Regular paper | Journal of the KIECS. pp. 741-752, vol. 19, no. 4, Aug. 31. 2024, t. 126, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2024.19.4.741

정보보안 기술 스트레스와 조직 공정성이 준수 의도에 미치는 영향: 계획된 행동이론을 중심으로

황인호*

The Influence of Information Security Techno-stress and Organizational Justice on Compliance Intention: Focusing on the Theory of Planned Behavior

In-Ho Hwang*

요 약

사회적으로, 정보보안에 대한 필요성이 증가하면서, 조직들은 정보보안을 위한 기술적 투자를 강화하고 있다. 본 연구는 상대적으로 관심이 부족한 내부자의 정보보안 준수 체계 강화를 위한 방안을 제시하였다. 특히, 조직에서 개인의 행동 원인을 설명하는 계획된 행동이론을 반영하여 기술 스트레스와 조직 공정성을 통해 행동이 변화할 수 있음을 밝히고자 하였다. 연구는 정보보안 도입 기업에 근무하는 조직원에 설문 조사를 하였으며, 383건의 표본을 활용하여 가설 검정을 하였다. 검정 결과, 정보보안 기술에 의한 스트레스(과부하와 불확실성)가 조직원의 태도를 감소시키고, 조직 공정성이 주관적 규범을 높였으며, 자기 효능감과 함께 준수 의도에 영향을 주었다. 더불어, 조직 공정성이 과부하 및 불확실성의 태도에 미치는 부정적 영향을 완화하는 것을 확인하였다. 연구 결과는 조직의 부정적 보안 환경을 개선하기 위한 조직 공정성 조건을 제시하여, 조직 내부의 보안 성과 달성을 위한 방안 마련에 도움을 줄 것으로 기대한다.

ABSTRACT

Organizations amplify their information security (IS) technical investments as the demand for IS escalates. This research suggests conditions for enhancing insider compliance with IS, focusing on the potential for behavior modification through techno-stress and organizational justice, based on the theory of planned behavior. To test the proposed hypothesis, this study utilized a survey methodology on 383 employees from companies with implemented IS. The test results showed that IS techno-stress (overload and uncertainty) caused by reduced attitudes of employees, and organizational justice increased subjective norms, influencing IS compliance intentions along with self-efficacy. Additionally, organizational justice has been found to alleviate the adverse effects of IS overload and uncertainty on attitudes. The findings are expected to help clarify measures for achieving IS performance within the organization by proposing organizational justice conditions to improve the negative IS environment of the organization.

키워드

Theory of Planned Behavior, Compliance Intention, Techno-overload, Techno-uncertainty, Organizational Justice
계획된 행동 이론, 준수 의도, 기술 과부하, 기술 불확실성, 조직 공정성

* 교신저자: 국민대학교 교양대학
• 접 수 일 : 2024. 06. 18
• 수정완료일 : 2024. 07. 15
• 게재확정일 : 2024. 07. 25
• Received : Jun. 18. 2024, Revised : Jul. 15. 2024, Accepted : Jul. 25. 2024
• Corresponding Author : In-Ho Hwang
College of General Education, Kookmin University,
Email : hwanginho@kookmin.ac.kr

Ⅰ. 서 론

조직의 정보 관리에 대한 사회적 요구가 지속해서 증가하면서, 조직들의 정보보안에 대한 기술적, 조직 구조적 투자가 증가하고 있다[1]. 특히, 국가 차원에서 정보보안 체계 구축에 대한 요구가 증가하고 있는데, 미국은 모든 환경에서 정보보안 신뢰를 높일 수 있는 기반을 요구하고 있으며[2], 국내는 정보통신망법과 개인정보보호법 등에서 조직들의 정보 자산관리에 대한 요구사항 수준을 높이고 있다[3]. 공통으로, 외부 침입에 대한 대비뿐 아니라, 내부자에 의한 정보 노출 가능성을 예방하는 체계 구축을 함께 요구한다. 반면, 전 세계적으로 보안사고는 지속해서 발생하고 있는데, 매년 발생하는 보안사고의 약 20~30%는 사람에 의해 발생하고 있어, 조직 내부자의 보안 준수를 위한 통제가 필요한 상황이다[4].

내부자의 보안 준수와 관련된 선행연구들은 조직원은 보안 준수에서 얻을 수 있는 혜택 및 비용을 고려하여 행동을 결정한다는 관점[5], 조직원은 사고에 대한 위협과 두려움에 기반하여 사고에 대한 대처 동기를 가지게 된다는 관점[6], 그리고 정보보안 정책, 기술 등의 운용이 엄격하고 과도할 때 조직원들의 부정적 인식 및 행동을 도출할 수 있다는 관점[7][8] 등을 제시했다. 선행연구들은 조직원의 보안 행동은 긍정적 또는 부정적 동기에 기반하여 준수 행동으로 연계됨을 밝힌 측면에서 시사점이 있다.

반면, 정보보안이 조직원의 준수 행동으로 연계되기 위해서는 조직 환경과 개인과 관계성을 명확하게 이해하고 개인을 지원하는 것이 요구된다[9]. 조직과 개인 간의 관계에서 조직 환경 또는 요구사항에 대한 개인의 행동 원인을 체계적으로 설명한 이론이 계획된 행동이론(Theory of Planned Behavior)이다. 계획된 행동이론은 개인의 행동은 대상에 대한 자기 통제 의식, 대상에 대한 호의적 태도, 그리고 주변 사람들의 행동을 복합적으로 고려하여 발현됨을 설명한 이론으로[10], 조직 구성원의 행동 원인에 대한 설명력이 높다. 정보보안과 관련하여 계획된 행동이론은 긍정적 측면의 조직 보안 환경과 개인행동 원인, 그리고 준수 행동으로 연계되는 구조를 밝히는 것에 주력하였다[5][11][12]. 하지만, 조직원은 엄격한 보안 정책 등에 의해 스트레스를 받을 수도 있다. 즉, 조직 환경에 의한 개인의 스트레스는 부정적 행동을 유발할 수 있는데[3][13], 계획된 행동이론을 기반으로 부정적 조건을 완화하기 위한 연구는 부족한 상황이다.

본 연구는 정보보안 기술 도입으로 인하여 발생할 수 있는 개인의 스트레스가 계획된 행동이론에 반영되어 행동 의도로 연계되는 구조를 밝히고, 스트레스를 완화하기 위한 조건을 제시하는 것을 목적으로 한다. 이에, 기술 스트레스 이론, 조직 공정성 이론, 그리고 계획된 행동이론을 반영하되, 정보보안 관련 기술 스트레스가 태도를 감소시켜 준수 의도에 미치는 영향을 확인하고, 주관적 규범에 영향을 주는 조직 공정성이 기술 스트레스의 부정적 영향을 완화할 수 있음을 확인하고자 한다. 본 연구의 결과는 조직의 부정적 보안 환경을 개선하기 위한 조직 노력 조건을 제시함으로써, 내부적인 보안 목표 달성을 위한 방안을 제언할 수 있을 것으로 기대한다.

Ⅱ. 이론적 배경

2.1 조직 정보보안

미국 행정부는 조직의 정보보안 체계를 강화하기 위해, ‘제로 트러스트(Zero Trust)’에 기반한 보안 정책을 강화하도록 요구하고 있다[2]. 제로 트러스트는 조직의 정보보안 환경이 누구든 어떤 상황이든 신뢰하지 않음을 기반으로 하는 것으로, 기존에 외부의 침입에 기반한 정보보안 정책 및 기술을 적용하였다면, 내부 및 외부와 관련 없이 모든 환경에서 보안 체계를 엄격하게 유지하는 것을 의미한다[2]. 미국은 정부 주도의 정보보안 수준을 강화하는 노력을 하고 있으나, 국내의 경우 아직 조직의 정보보안 수준은 미약한 수준이다. 실제, 국내 기업들의 정보보호를 위한 정책은 약 38.6%만 구축한 상태이며, 기업 규모가 작을수록 정책 및 조직보유는 낮은 수준으로 나타나고 있다[1]. 특히, 침해사고 예방을 위한 기술 서비스의 이용은 다소 높은 수준이나 내부자를 위한 교육 수준은 32.9%만 수행하고 있어[1], 내부자에 의한 정보보안 예방을 위한 노력이 필요한 시점이다. 해당 관점에서 본 연구는 조직원의 준수 의도(Compliance Intention)를 향상하는 방안을 제시하고자 한다. 준수 의도는 조직이 보유하고 있는 정보 자원을 외부 및 내부의 위

험으로부터 보호하려는 행동 의지를 의미하며[5][14][15], 준수 의도를 높임으로써 내부자들의 보안 준수 활동을 증진할 수 있다[16]. 본 연구는 계획된 행동이론과 기술 스트레스, 그리고 조직 공정성을 반영하여 준수 의도 감소를 최소화하는 방안을 제시하고자 한다.

2.2 계획된 행동이론

사람은 특정 환경에서의 의사결정 및 행동을 위해 외재적, 내재적으로 형성된 요소를 복합적으로 고려하여 합리적 결정을 하는데[12], 이를 적절히 설명하는 이론이 계획된 행동이론이다. 본 이론은 개인의 행동은 대상에 대한 믿음을 기반으로 구축된 개인의 태도, 외부 환경으로부터 얻어진 행동 조건인 주관적 규범, 그리고 대상을 통제할 수 있다고 믿는 행동 통제 요소가 복합적으로 작용함으로써 행동으로 연계된다고 보기 때문에[10], 의사결정에 영향을 주는 환경과 개인의 인식 간의 관계성을 명료하게 제시한 측면에서 활용성이 높다. 특히, 계획된 행동이론은 적용 환경적 특성에 기반하여 외적 환경과 통제 요소를 다각적으로 제시하고, 행동에 영향을 주는 선행 요소를 변화시키는 조건으로 반영할 수 있어[6], 집단과 개인 간의 관계에서 행동 강화 전략 수립에 중점적으로 활용된다. 본 연구는 계획된 행동이론의 자기 효능감(Self-efficacy), 태도(Attitude), 주관적 규범(Subjective Norms)을 정보보안에 반영하되, 보안 정책이 반영된 조직 환경이 계획된 행동이론의 행동 원인에 영향을 주는 조건을 확인하고자 한다.

자기 효능감은 대상을 스스로 통제하거나, 문제를 해결할 수 있다고 판단하는 수준으로[5], 개인이 외부의 압력이나 요구에 기반한 의사결정을 하는 것이 아닌 스스로 대상을 통제 및 관리할 수 있다고 판단할 때 자기 효능감이 형성된다[12]. 정보보안과 관련하여 자기 효능감은 조직의 정책 및 기술에 대한 요구사항에 대하여 자신의 업무에 충분히 반영하여 스스로 해결할 수 있다는 믿음을 지칭하므로, 형성된 자기 효능감은 조직이 요청하는 수준의 준수 행동을 유발하는 조건이 된다[9]. 태도는 자신의 경험을 기반으로 형성된 대상에 대한 호의성을 의미한다[12]. 태도의 대상은 환경에서부터 사물 또는 서비스에 이르기까지 다양하며, 호의성은 본인에게 이익을 높이도록 돕는 조건이므로, 대상에 긍정적 태도를 형성한 개인은 대상에 긍정적 의도를 가진다[11]. 정보보안과 관련하여 형성된 긍정적 태도는 조직이 정보보안을 통해 자신에게 피해를 주지 않을 것이라는 믿음을 함께 보유하고 있으므로, 긍정적 준수 행동으로 연계될 가능성이 크다[16]. 주관적 규범은 행동 대상의 주변의 문화 또는 행동 양식 등에 의해 내재화된 수준을 의미한다[16]. 즉, 주관적 규범은 의사결정을 하는 대상을 둘러싼 환경에서 얻어진 행동 방식이며, 대표적으로 주변 사람들이 대상과 관련되어 보이는 행동 방식을 기반으로 생성된 규범이다[11]. 정보보안과 관련하여, 개인은 동료들의 정보보안 관련 행동으로부터 유사한 행동을 함으로써 조직 문화에 동조하려는 모습을 보인다. 즉, 보안 관련 주관적 규범은 개인의 준수 행동을 변화시킨다[17].

계획된 행동이론의 세부 요인(자기 효능감, 태도, 그리고 주관적 규범)은 조직에서 개인이 조직의 요구사항에 맞는 행동 의도를 보이도록 돕는 선행 조건이다[11][16][17]. 즉, 정보보안에 대한 조직원의 자기 효능감, 태도, 그리고 주관적 규범이 준수 의도를 높이는 조건이라 판단하며, 다음의 가설을 제시한다.

H1a. 정보보안 관련 자기 효능감은 준수 의도에 양(+)의 영향을 준다.

H1b. 정보보안 관련 태도는 준수 의도에 양(+)의 영향을 준다.

H1c. 정보보안 관련 주관적 규범은 준수 의도에 양(+)의 영향을 준다.

2.3 정보보안 기술 스트레스

조직원은 자신을 둘러싼 환경 및 조직의 요구사항에 대하여 자신의 지식 등 역량을 활용하여 대처하며, 반대급수로 급여 또는 명성 등의 이익을 얻는다[13]. 하지만, 주어진 요구사항의 변화 등의 이유로 충분하게 대처하지 못하는 상황이 발생할 경우 불균형 상태가 발생하고 부정적인 반응을 일으킬 수 있다[8]. 스트레스(Stress)는 개인이 외부와 거래 과정에서 발생하는 요구사항 등의 불일치로 인하여 발생하는 불균형을 의미한다[18]. 특히, 현재 기업들은 생산성과 성과 향상을 위하여 IT 기술을 적극 투입하고 지속해서 개선하는 등의 노력을 하고 있는데, IT 기술의 과다한 변화 또는 요구사항으로 인하여 조직원에게 불균

형을 일으킬 수 있는데 이를 기술 스트레스(Techno-stress)라고 한다[19]. 즉, 기술 스트레스는 조직이 제공하는 기술적 환경에 대하여 개인이 받아들이지 못하는 환경에 직면하여 느끼는 불균형 상태를 의미한다[18]. 정보보안 관점에서도 기술 스트레스는 발현될 수 있는데, 정보보안 정책에 대한 표준화를 위하여 조직은 외부와의 차단 또는 보안 절차 등을 위하여 관련 기술을 적용하는데, 조직원에게 스트레스로 작용할 수 있다. 대표적인 기술 스트레스 유형으로 과부하와 불확실성이 있다. 첫째, 기술 과부하(Techno-overload)는 특정 기술의 도입이 개인의 업무 수준을 변화시켜 추가적인 활동을 요구하는 상태를 의미한다[20]. 둘째, 기술 불확실성(Tecnho-uncertainty)은 도입 기술을 환경 변화에 대처하기 위하여 지속해서 변화시킴으로써 기술에 대한 이해도가 감소하는 상태를 의미한다[3]. 이와 같은 과부하와 불확실성은 정보보안에서도 반영될 수 있는데, 정보보안 관련 기술을 반영함으로써 기존 업무 체계가 변화하게 되는데 과도한 경우 스트레스를 받을 수 있으며, 보안 기술을 빠르게 도입 및 변화시킬 때 조직원은 기술을 명확하게 이해하지 못하는 상태에 있을 수 있다[8].

조직의 환경에 대한 인식은 사용자의 태도에 영향을 미친다. Lee et al.[2016]은 외부의 보안 관련 위협 인식은 개인의 태도에 영향을 미친다고 하였으며[7], Safa and Von Solms[2016]은 조직 환경에 의한 외적 동기는 개인의 태도 형성에 영향을 준다고 하였다. 또한[16], Vakola and Nikolaou[2005]는 조직 변화에 대한 조직원의 태도는 업무적 과부하 같은 스트레스에 의해 부정적 영향을 받는 조건임을 설명하였다[13]. 즉, 선행연구는 스트레스와 같은 환경이 개인의 태도에 영향을 주는 조건임을 설명한다. 본 연구는 정보보안과 관련된 기술 과부하와 기술 불확실성이 개인의 태도에 부정적 영향을 줄 것으로 판단하고, 다음 가설을 제시한다.

H2. 정보보안 관련 기술 과부하는 정보보안 관련 태도에 음(-)의 영향을 준다.

H3. 정보보안 관련 기술 불확실성은 정보보안 관련 태도에 음(-)의 영향을 준다.

2.4 조직 공정성

조직에서 개인은 조직이 요구하는 업무 및 특정 활동에 대한 목표를 달성함으로써 성과를 지급받는데[21], 자신의 활동 결과에 대한 충분히 이해할 수 있는 결과를 보상받길 원한다[22]. 조직 내 공정함과 행동 간의 관계를 명확하게 설명하는 관점이 조직 공정성이다. 조직 공정성(Organizational Justice)은 조직과 개인 간의 교환 관계에서 교환이 상호 공평하다고 판단하는 관점이다[23]. 공정성은 상대적 개념으로 개인이 제공한 활동 및 결과에 대한 보상이 유사한 상황에서도 비슷하거나 충분히 인정할만한 보상으로 연계될 때 공정성을 높게 판단한다[24].

초기 공정성은 결과에 대한 보상의 공평함에 의해 형성된다고 보았으나, 최근에는 결과의 공평성이 이루어지기 위해서는 환경적으로 준비 및 수행 과정에서 공평함이 중요하다고 보며[23][25], 전체적인 맥락에서 개인은 공정함을 고려한다는 관점의 연구가 제시되고 있다[26]. 본 연구는 전체 조직 공정성을 반영한다. 정보보안과 관련하여 조직원은 보안 정책을 준수하는 과정과 결과 등에서 충분한 보상을 받을 수 있을 때 공정성을 높게 가질 수 있다. 즉, 보안 행동을 위한 사전 정보를 충분히 제공하고, 누구나 보안 절차를 동등하게 지켜야 하고, 미준수 또는 준수에 따른 결과를 동등하게 받을 때 공정하다고 판단한다[27][28].

특히, 조직 공정성은 환경 요소이므로, 개인의 주관적 규범과 같은 환경에 대한 인식을 강화하는 조건이다. Yoon[2011]은 조직의 디지털 정책에 대한 조직원의 주관적 규범은 조직 전체에 형성된 공정성에 의해 영향을 받는다고 하였다[21]. 또한, Jacobs et al.[2014]는 조직 공정성이 개인의 감정 및 상사와 조직 지원에 긍정적 영향을 미쳐 긍정적 행동으로 연계됨을 밝혔다[25]. 즉, 정보보안과 관련하여 조직 차원에서 공정성 제공 노력은 조직원의 주관적 규범에 영향을 줄 것으로 판단하며, 다음의 가설을 제시한다.

H4. 정보보안 관련 조직 공정성은 정보보안 관련 주관적 규범에 양(+)의 영향을 준다.

또한, 조직 공정성은 스트레스와 같은 부정적 인식 조건이 행동에 미치는 영향을 완화하는 효과를 가진다. Alam[2016]은 조직원이 업무에 도입한 기술로 인하여 스트레스를 받게 될 때 생산성이 감소하며, 업무

적 공정성이 스트레스와 상호 조절하여 생산성 감소를 완화하는 것을 밝혔다[22]. 또한, Son and Park[2016]은 조직에서 개인이 느끼는 프라이버시 우려는 절차적 공정성과 상호작용 효과를 가져 컴퓨팅 준수에 영향을 주는 것을 밝혔다[24]. 즉, 조직 공정성은 스트레스의 부정적 영향을 스트레스와 연계하여 완화할 수 있는 조절 조건이다. 이에, 본 연구는 조직 공정성이 기술 스트레스 요인(과부하, 불확실성)과 상호작용 효과를 가져 스트레스가 태도에 미치는 부정적 영향을 완화할 것으로 판단하고 다음의 가설을 제시한다.

H5a. 조직 공정성은 기술 과부하가 태도에 미치는 영향에 완화 효과를 가진다.

H5b. 조직 공정성은 기술 불확실성이 태도에 미치는 영향에 완화 효과를 가진다.

III. 연구모델 및 측정

3.1 연구모델

본 연구는 조직 내 도입된 보안 정책 및 기술에 대한 조직원의 행동 조건을 밝히는 것이 목적이다. 계획된 행동이론, 기술 스트레스 이론, 그리고 조직 공정성 간의 연계성을 제시함으로써 행동 원인을 밝히고자 하며, 제시한 연구모델은 그림 1과 같다.

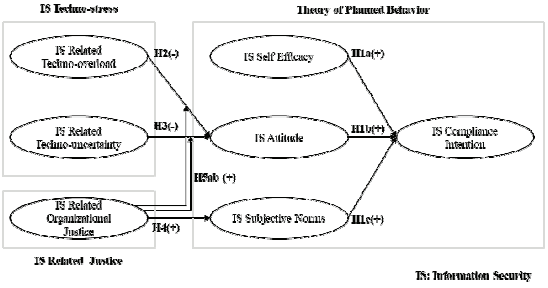

그림 1. 연구모델
Fig. 1 Research Model

3.2 측정 도구 및 표본 확보

본 연구는 조직 구성원의 행동 원인을 밝히기 위해, 계획된 행동이론 등 적용 이론들과 관련된 설문 문항을 정보보안 분야에 맞게 수정하여 적용하였다. 즉, 요인별 2개 이상의 설문 문항을 구성하되, 내용 타당성을 확보하기 위해 타당성을 확보한 선행연구에서 문항을 제시하고 7점 리커트 척도로 적용하였다.

최종적으로 적용된 변수별 측정 문항은 다음과 같다. 보안 관련 기술 과부하는 Tarafdar et al.[2007] 연구에서 제시하였으며[19], “회사로부터 정보보안 기술 정책에 맞게 업무를 보도록 요구받음(제외)”, “회사의 보안 기술로 인해, 처리할 수 있는 것보다 많은 일을 요구받음”, “회사의 정보보안 기술로 인해 업무 수행에 어려움을 겪음”, “회사의 정보보안 기술에 적응하기 위하여 업무수행 방법을 변경하도록 요구받음”과 같다. 보안 관련 불확실성은 Tarafdar et al.[2007] 연구에서 제시하였으며[19], “회사에 적용된 보안 기술은 변화하고 있음”, “회사의 보안 시스템은 지속해서 업그레이드가 됨”, “회사에서 내 업무는 기술적으로 새로운 보안 관련 요구 사항이 발생함”과 같다. 보안 관련 조직 공정성은 Ambrose and Schminke[2009] 연구에서 제시하였으며[26], “나는 회사에서 정보보안에 대하여 전반적으로 공정하게 대우받음”, “나는 우리 회사가 정보보안 활동에 대하여 공정하다고 믿음”, “우리 회사의 정보보안 정책 및 활동은 일반적으로 공정함”, “우리 회사는 정보보안 활동에 대하여 공평하게 대우함”과 같다. 정보보안 태도는 Bulgrucu et al.[2010] 연구에서 제시하였으며[5], “회사의 보안 기술과 방법을 받아들이는 것은 중요함”, “회사의 보안 기술과 방법을 받아들이는 것은 나에게 혜택이 있음”, “회사의 보안 기술과 방법을 받아들이는 것은 나에게 도움이 됨”과 같다. 정보보안 자기 효능감은 Ifinedo[2012] 연구에서 제시하였으며[6], “나는 보안 위반으로부터 나를 보호하는데 필요한 기술을 보유하고 있음”, “나는 나의 기밀 정보를 노출하지 않도록 예방할 수 있는 지식을 보유하고 있음”, “나는 업무 과정에서 정보를 보호하기 위한 예방할 수 있는 기술을 가지고 있음”, “나는 보안 위반을 억제하는 것이 나의 통제 범위에 있다고 믿음”, “나는 참조할 수 있는 정보가 있을 때, 충분히 보안 조치를 할 수 있음”과 같다. 정보보안 주관적 규범은 Ifinedo[2012] 연구에서 제시하였으며[6], “나의 상사는 내가 회사의 보안 정책을 따라야 한다고 생각함”, “동료들은 내가 회사의 보안 정책을 따라야 한다고 생각함”, “회사의 IT 부서는 내가 보안 정책을 따르도록 압력을 가함”,

“주변 사람들은 내가 회사의 보안 정책을 따라야 한다고 생각함”과 같다. 준수 의도는 Chen et al.[2012] 연구에서 제시하였으며[15], “나는 회사의 보안 정책을 계속 따를 것임”, “나는 업무를 수행 과정에서 보안 절차를 준수할 예정임”, “나는 회사의 보안 정책을 준수하고자 하는 나의 태도에 확신을 가짐”과 같다.

본 연구가 조사하고자 하는 대상은 정보보안 정책과 기술을 도입하여, 조직원 업무에 반영하고 있는 기업의 근로자이다. 이에, 설문은 대학의 사회교육원의 경영학과에 다니는 직장인을 대상으로 온라인 및 오프라인 설문을 동시에 진행하여 직업을 보유하고 있으며, 회사에서 정보보안 기술을 도입한 사람만 설문에 참여하도록 하였다. 또한, 설문 시작 전 확보된 표본의 통계적인 활용 방법과 목적을 제시하고 이를 허가한 사람만 실제 설문에 참여하도록 하였다.

3.3 표본 특성

가설 검정을 위해 확보한 표본은 383건으로서, 표본에서 나타난 특성은 표 1에 제시하였다. 성별의 경우 남성이 약 61%로 나타났으며, 나이의 경우 연령대별 비슷한 규모로 확보된 것으로 나타났다. 업종은 서비스업이 약 80%로 나타났으며, 직위 또한 위치별 비슷한 비중을 가진 것으로 나타났다.

표 1. 표본 특성
Table 1. Sample Characteristics

Categories		Frequency	%
Total		383	100.0
Gender	Male	235	61.4
	Female	148	38.6
Age	Under 30	109	28.5
	31 - 40	125	32.6
	41 - 50	109	28.5
	Over 51	40	10.4
Industry	Service	309	80.7
	Manufacturing	74	19.3
Job Position	Staff	123	32.1
	Assistant Manager	102	26.6
	Manager	115	30.0
	Over Manager	43	11.2

Ⅳ. 분 석

4.1 신뢰성 및 타당성 분석

연구모델에 반영된 변수들은 측정 문항들이 다 항목들로 구성되어 있으므로, 측정 문항의 변수에 대한 신뢰성 및 타당성을 확인하였다.

표 2. 타당성 및 신뢰성
Table 2. Construct Validity and Reliability

Constructs		Factor Loading	Construct Reliability	Average Variance Extracted	Cronbach's Alpha
OJ	OJ4	0.887	0.910	0.718	0.943
	OJ3	0.907			
	OJ2	0.908			
	OJ1	0.889			
TO	TO4	0.894	0.854	0.662	0.910
	TO3	0.884			
	TO2	0.858			
TU	TU3	0.889	0.877	0.703	0.920
	TU2	0.912			
	TU1	0.873			
SE	SE5	0.816	0.899	0.641	0.923
	SE4	0.852			
	SE3	0.885			
	SE2	0.875			
	SE1	0.778			
Atti	Atti3	0.912	0.885	0.719	0.915
	Atti2	0.861			
	Atti1	0.880			
SN	SN4	0.921	0.899	0.689	0.926
	SN3	0.901			
	SN2	0.856			
	SN1	0.800			
CoI	CoI3	0.930	0.921	0.795	0.945
	CoI2	0.953			
	CoI1	0.888			

OJ(Organizational Justice), TO(Techno-Overload), TU(Techno-uncertainty), SE(Self-efficacy), Atti(Attitude), SN(Subjective Norms), CoI(Compliance Intention)

첫째, 신뢰성은 적용된 측정 문항들을 반복해서 확인하더라도 일관성 있게 결과가 도출되는 것을 확인하는 것으로, SPSS 21.0 툴에서 크론바흐 알파 값(Cronbach's alpha)을 확인하여 신뢰성을 측정하였다. 크론바흐 알파 값은 적용 변수에 대하여 0.7 보다 큰

값을 요구한다[29]. 분석 결과는 표 2에 제시하였으며, 신뢰성이 확보된 것으로 나타났다.

둘째, 타당성은 잠재변수에 대한 측정변수의 일관성과 잠재변수 간의 차별성이 존재하는지 확인하는 것으로, 본 연구는 AMOS 22.0 툴을 활용하되 확인적 요인분석을 통해 타당성을 확인하였다. 우선 분석에 반영한 모델링의 적합도를 확인하였으며, χ^2/df = 1.497, RMSEA = 0.036, RMR = 0.038, GFI = 0.928, AGFI = 0.908, NFI = 0.958, 그리고 CFI = 0.986으로 나타났다. 선행연구는 모델 적합도에 대해 RMSEA, RMR은 0.05보다 낮은 것을 요구하고, CFI, NFI, GFI, 그리고 AGFI은 0.9보다 높은 것을 요구한다[30]. 분석 결과 모든 적합도 수치가 요구수준을 충족하였다.

잠재변수에 대한 일관성의 확인은 집중 타당성 분석을 통해 확인한다. 집중 타당성은 개념 신뢰도(Construct Reliability), 평균분산추출(Average Variance Extracted)을 변수별로 확인하되, 0.7보다 높은 개념 신뢰도를 요구하며, 0.5보다 높은 평균분산추출을 요구한다[30]. 결과는 표 2에 제시하였으며, 모든 잠재변수에 대한 집중 타당성이 확보되었다.

잠재변수 간 차별성의 확인은 판별 타당성을 통해 확인하며, 선행연구는 모든 변수가 반영된 상관계수를 평균분산추출과 비교하되 평균분산추출 제곱근이 상관계수보다 클 때 차별성이 존재한다고 본다[30]. 결과는 <표 3>에 제시하였으며, 판별 타당성이 존재하는 것으로 나타났다.

표 3. 판별 타당성 분석 결과
Table 3. Result for Discriminant Validity

	1	2	3	4	5	6	7
OJ	**0.84**[a]						
TO	-.57**	**0.81**[a]					
TU	-.50**	.65**	**0.83**[a]				
SE	.37**	-.34**	-.32**	**0.80**[a]			
Atti	.51**	-.50**	-.40**	.41**	**0.84**[a]		
SN	.55**	-.44**	-.38**	.36**	.45**	**0.83**[a]	
CoI	.69**	-.62**	-.52**	.52**	.58**	.58**	**0.89**[a]

OJ(Organizational Justice), TO(Techno-overload), TU(Techno-uncertainty), SE(Self-efficacy), Atti(Attitude), SN(Subjective Norms), CoI(Compliance Intention)
a = square root of the AVE, **: p < 0.01

4.2 가설 검정

가설 검정은 AMOS 22.0 툴과 Process 3.1 매크로를 적용한다. 첫째, 기술 스트레스와 조직 공정성이 개인의 계획된 행동이론에 적용되는 관계는 전체적인 맥락을 살피는 구조방정식 모델링을 수행하며, 둘째, 조직 공정성이 기술 스트레스의 부정적 영향을 완화한다는 조절 효과는 상호작용 효과를 그래프로 지원하는 Process 3.1을 적용함으로써, 명확하게 영향 수준을 확인하고자 한다.

가설 1~4까지의 검정에 필요한 모델링을 하였으며, 적용 모델의 적합도는 χ^2/df = 1.981, RMSEA = 0.051, RMR = 0.179, GFI = 0.901, AGFI = 0.879, NFI = 0.936, 그리고 CFI = 0.967로 나타났다. RMSEA와 RMR, 그리고 AGFI가 요구사항보다 부족한 것으로 나타났으나, 크게 부족하지 않았으며 그 외 수치가 적합했기 때문에, 모델을 통해 가설 검정을 하였다. 검정 결과는 그림 2, 표 4에 제시하였다.

가설 1은 계획된 행동이론의 자기 효능감(H1a), 태도(H1b), 그리고 주관적 규범(H1c)이 준수 의도를 높인다는 것으로, 각 가설은 유의수준 5%에서 채택되었다(H1a: β= 0.277, p < 0.01; H1b: β= 0.399, p < 0.01; H1c: β= 0.448 p < 0.01). 가설 2와 3은 정보보안 관련 기술 과부하(H2)와 불확실성(H3)이 개인의 태도를 감소시킨다는 것으로 가설 2는 유의수준 5%에서 채택되었으나, 가설 3은 기각되었다(H2: β= -0.477, p < 0.01; H3: β= -0.126, n.s.). 가설 4는 정보보안 관련 조직 공정성이 개인의 태도를 높인다는 것으로 유의수준 5%에서 채택되었다(H4: β= 0.615, p < 0.01).

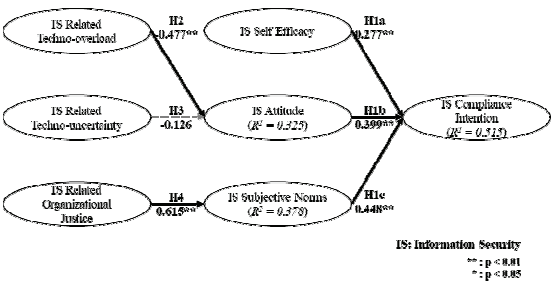

그림 2. 가설 검정의 결과 (H1~H4)
Fig. 2 Results of Hypothesis Tests (H1~H4)

표 4. 가설 검정의 결과 (H1~H3)
Table 4. Results of Hypothesis Tests (H1~H3)

	Path	Coefficient	t-value	Result
H1a	SE → CoI	0.277	6.467**	Supported
H1b	Atti → CoI	0.399	9.029**	Supported
H1c	SN → CoI	0.448	10.132**	Supported
H2	TO → Atti	-0.477	-6.715**	Supported
H3	TU → Atti	-0.126	-1.827	Rejected
H4	OJ → SN	0.615	12.777**	Supported

OJ(Organizational Justice), TO(Techno-overload), TU(Techno-uncertainty), SE(Self-efficacy), Atti(Attitude), SN(Subjective Norms), CoI(Compliance Intention)
**: $p < 0.01$

가설 5는 조직 공정성이 기술 스트레스(과부하, 불확실성)로 인한 태도 감소를 완화한다는 것으로, 적용된 잠재변수들이 리커트 척도이므로 Process 3.1의 모델 1을 적용하였다(붓스트래핑 5,000, 유의수준 5% 반영)[31]. 스트레스와 조직 공정성의 상호작용 항이 태도에 미치는 영향의 결과는 표 5와 같으며, 조직 공정성의 조절 효과가 존재하는 것으로 확인되었다 (H5a: t= 3.800, $p < 0.01$; H5b: t= 4.741, $p < 0.01$).

표 5. 가설 검정의 결과 (H5)
Table 5. Results of Hypothesis Tests (H5)

		Coefficient	t-value	Result
H5a	Constant	4.903	97.530**	Supported
	TO	-0.244	-4.976**	
	OJ	0.240	4.750**	
	Interaction	0.105	3.800**	
	F = 68.8178, R^2 = 0.3559			
H5b	Constant	4.905	99.215**	Supported
	TU	-0.127	-2.769**	
	OJ	0.298	6.110**	
	Interaction	0.122	4.741**	
	F = 63.3062, R^2 = 0.3338			

OJ(Organizational Justice), TO(Techno-overload), TU(Techno-uncertainty)
**: $p < 0.01$

조직 공정성이 과부하(H5a)와 불확실성(H5b)과 태도 간의 관계에 영향이 있는 것으로 나타났으므로, SPSS 21.0을 활용하여 그래프로 영향 수준을 확인하였으며, 결과는 그림 3과 그림 4와 같다. 기술 과부하와 불확실성이 조직원의 태도를 감소시키는 조건에서, 조직 공정성이 높은 집단에서 태도 감소가 완화되는 것을 확인하였다.

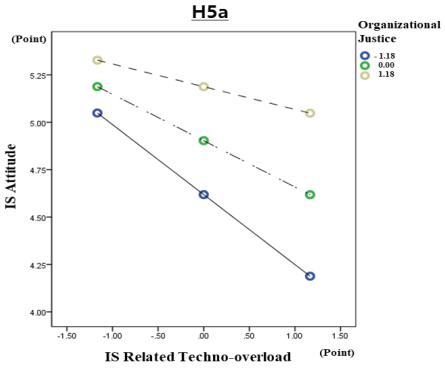

그림 3. 조절 효과의 결과 (H5a)
Fig. 3 Results of Moderation Effect (H5a)

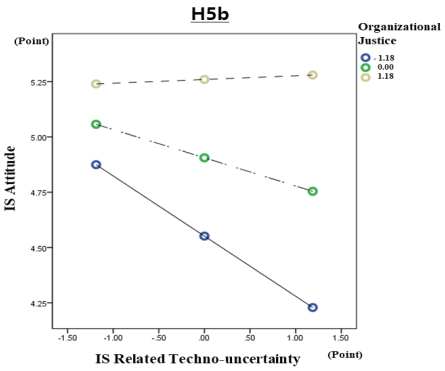

그림 4. 조절 효과의 결과 (H5b)
Fig. 4 Results of Moderation Effect (H5b)

V. 결 론

5.1 연구의 요약

사회적으로, 조직의 체계적인 정보보안에 대한 필요성이 높아지면서, 조직들은 정보보안 수준 강화를 위한 투자 수준을 높이고 있다. 본 연구는 상대적으로 관심이 부족한 분야인 내부자의 정보보안 준수 체계 강화를 위한 방안을 제시하였다. 특히, 조직과 개인 간의 연계성에서 개인의 행동 원인을 설명하는 계획된 행동이론을 기반으로 스트레스에 따른 영향과 조

직 공정성을 중심으로 개선 방안을 마련하고자 하였다. 연구는 정보보안 정책과 기술을 업무에 반영하고 있는 기업에 근무하는 조직원에 설문 조사를 하였으며, 383건의 표본을 활용하여 가설 검정을 하였다. AMOS 22.0 툴과 Process 3.1 매크로를 통해 확인한 가설 검정 결과는, 정보보안 기술에 의한 스트레스(과부하와 불확실성)가 조직원의 태도를 감소시키고, 조직 공정성이 주관적 규범을 높였으며, 태도, 주관적 규범, 그리고 자기 효능감이 준수 의도에 영향을 주었다. 더불어, 조직 공정성이 과부하 및 불확실성의 태도에 미치는 부정적 영향에 대해 완화 효과를 가지는 것을 확인하였다.

5.2 논의

본 연구 결과의 시사점은 다음과 같다. 첫째, 조직에서 개인의 행동 원인을 체계적으로 밝히는 계획된 행동이론을 반영하되, 부정적 환경에 의해 발생할 수 있는 기술 스트레스가 연계될 수 있음을 밝혔다. 즉, 보안 기술의 과부하와 불확실성의 인식은 개인의 태도에 부정적 영향을 주는 조건임을 밝혔다는 측면에서 선행연구로서 의미를 지닌다. 따라서, 조직은 조직원의 보안에 대한 태도 강화를 위하여 역설적으로 보안 기술 도입으로 인하여 발생할 수 있는 부정적 인식을 최소화하는 것이 필요하다. 예를 들어, 도입 기술에 대한 전략적 방향을 소개하고, 교육 및 훈련 프로그램을 통해 기술의 내재화가 가능하도록 돕는 것이 요구된다. 둘째, 정보보안에 대한 조직 차원의 공정성 확립이 개인의 정보보안 행동 원천 중 주관적 규범에 영향을 주는 조건이며, 기술 스트레스가 태도에 미치는 부정적 영향을 완화하는 조건임을 밝힌 측면에서 선행연구로서 학술적 시사점을 지닌다. 즉, 보안 정책이 모든 구성원에게 동일하게 적용됨을 제시할 때, 개인은 주변 동료들의 행동 방식에서 보안 행동의 필요성을 인지하는 주관적 규범을 형성함을 의미한다. 또한, 공정한 보안 준수 활동에 대한 조직의 지원은 새로운 기술이 도입되더라도 목적에 맞게 모든 구성원에게 행동을 요구하는 것이므로 태도 감소를 억제할 수 있음을 의미한다. 따라서, 조직은 정보보안 관련 정보를 모든 구성원에게 동일하게 제공하고, 정보보안 준수 결과에 대해 보상 또는 처벌을 공정하게 적용하고, 해당 활동 내용을 내부적으로 공개하여 준수 활동을 증진하는 것이 요구된다.

본 연구는 조직 내 개인의 보안 행동 강화 방안을 제시한 측면에서 시사점이 있으나, 다음의 연구 한계가 있다. 첫째, 본 연구는 산업 또는 업종별 특성을 고려하지 않았다. 즉, 정보보안 관련 관심과 중요도는 업종 등에 따라 차이가 존재할 수 있는데, 표준화 관점에서 접근하여 해당 차이를 고려하지 않았다. 따라서, 향후 연구에서는 정보보안 시각 차이를 고려한 업종별 내부자 행동 원인을 밝히는 것이 요구된다. 둘째, 본 연구는 기술 스트레스가 개인의 행동 의도에 미치는 영향을 확인하였다. 스트레스에 대한 대처는 개인들의 특성에 따라 다를 수 있는데, 본 연구는 해당 사항을 고려하지 않았다. 따라서, 향후 연구에서는 개인 대처 등의 방식에 따라 스트레스 반응의 차이를 제시함으로써, 내부자의 정보보안 수준 강화를 위한 방안을 세부적으로 제시하는 것이 요구된다.

본 논문은 2024년 한국전자통신학회 춘계학술대회에 발표한 논문임

References

[1] Ministry of Science and ICT, Korea Information Security Industry Association, “2023 survey on information security,” *Report*, Feb. 2024.

[2] Nettgov, “Biden administration releases draft zero-trust guidance,” *Report*, Sept. 2021.

[3] I. Hwang, “The Influence of IS technology and communication uncertainty on IS voice behavior: The role of susceptibility to informational influence of employee,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 18, no. 1, 2023, pp. 165-176. http://dx.doi.org/10.13067/JKIECS.2023.18.1.165

[4] Verizon, “2022 data breach investigations report,” *Report*, Des. 2022.

[5] 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. https://doi.org/10.2307/25750690

[6] P. Ifinedo, “Understanding information systems

security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, vol. 31, no. 1, 2012, pp. 83-95.
https://doi.org/10.1016/j.cose.2011.10.007

[7] C. Lee, C. Lee, and S. Kim, "Understanding information security stress: Focusing on the type of information security compliance activity," *Computers & Security*, vol. 59, 2016, pp. 60-70.
https://doi.org/10.1016/j.cose.2016.02.004

[8] I. Hwang and O. Cha, "Examining technostress creators and role stress as potential threats to employees' information security compliance," *Computers in Human Behavior*, vol. 81, 2018, pp. 282-293.
https://doi.org/10.1016/j.chb.2017.12.022

[9] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," *MIS Quarterly*, vol. 34, no. 3, 2010, pp. 549-566.
https://doi.org/10.2307/25750691

[10] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, 1991, pp. 179-211.
https://doi.org/10.1016/0749-5978(91)90020-T

[11] J. Cox, "Information systems user security: A structured model of the knowing–doing gap," *Computers in Human Behavior*, vol. 28, no. 5, 2012, pp. 1849-1858.
https://doi.org/10.1016/j.chb.2012.05.003

[12] T. Sommestad, H. Karlzén, and J. Hallberg, "The sufficiency of the theory of planned behavior for explaining information security policy compliance," I*nformation & Computer Security*, vol. 23, no. 2, 2015, pp. 200-217.
https://doi.org/10.1108/ICS-04-2014-0025

[13] M. Vakola and I. Nikolaou, "Attitudes towards organizational change: What is the role of employees' stress and commitment?," *Employee Relations*, vol. 27, no. 2, 2005, pp. 160-174.
https://doi.org/10.1108/01425450510572685

[14] 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.
http://dx.doi.org/10.13067/JKIECS.2022.17.2.375

[15] 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.
https://doi.org/10.2753/MIS0742-1222290305

[16] N. S. Safa and R. Von Solms, "An information security knowledge sharing model in organizations," *Computers in Human Behavior*, vol. 57, 2016, pp. 442-451.
https://doi.org/10.1016/j.chb.2015.12.037

[17] W. R. Flores and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," *Computers & security*, vol. 59, 2016, pp. 26-44.
https://doi.org/10.1016/j.cose.2016.01.004

[18] R. K. Jena, "Technostress in ICT enabled collaborative learning environment: An empirical study among Indian academician," *Computers in Human Behavior*, vol. 51, 2015, pp. 1116-1123.
https://doi.org/10.1016/j.chb.2015.03.020

[19] M. Tarafdar, Q. Tu, B. S. Ragu-Nathan, and T. S. Ragu-Nathan, "The impact of technostress on role stress and productivity," J. *of Management Information Systems*, vol. 24, no. 1, 2007, pp. 301-328.
https://doi.org/10.2753/MIS0742-1222240109

[20] M. Tarafdar, E. B. Pullins, and T. S. Ragu Nathan, "Technostress: Negative effect on performance and possible mitigations," *Information Systems J.*, vol. 25, no. 2, 2015, pp. 103-132.
https://doi.org/10.1111/isj.12042

[21] C. Yoon, "Theory of planned behavior and ethics theory in digital piracy: An integrated model," *J. of business ethics*, vol. 100, 2011, pp. 405-417.
https://doi.org/10.1007/s10551-010-0687-7

[22] M. A. Alam, "Techno-stress and productivity: Survey evidence from the aviation industry," *J. of Air Transport Management*, vol. 50, 2016, pp. 62-70.
https://doi.org/10.1016/j.jairtraman.2015.10.003

[23] 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.

https://doi.org/10.1037/0021-9010.89.3.395
[24] J. Son and J. Park, "Procedural justice to enhance compliance with non-work-related computing (NWRC) rules: Its determinants and interaction with privacy concerns," *Int. J. of Information Management*, vol. 36, no. 3, 2016, pp. 309-321.
https://doi.org/10.1016/j.ijinfomgt.2015.12.005
[25] G. Jacobs, F. D. Belschak, D. N. Den Hartog, "(Un) ethical behavior and performance appraisal: The role of affect, support, and organizational justice," *J. of business ethics*, vol. 121, 2014, pp. 63-76.
https://doi.org/10.1007/s10551-013-1687-1
[26] 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.
https://doi.org/10.1037/a0013203
[27] 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.
https://doi.org/10.1287/isre.1090.0266
[28] I. Hwang, "The impact of IS policy and sanction perceptions on compliance intention through justice: The role of justice sensitivity," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 18, no. 2, 2023, pp. 337-348.
http://dx.doi.org/10.13067/JKIECS.2023.18.2.337
[29] J. C. Nunnally, *Psychometric theory (2nd ed.)*. New York: McGraw-Hill, 1978.
[30] 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.
https://doi.org/10.1177/002224378101800104
[31] 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 한국산업기술대학교 연구교수
2020년 ~현재 국민대학교 교양대학 조교수
※ 관심분야 : IT 핵심성공요인(IT CSF), 디지털 콘텐츠(Digital Content), 정보보안(Information Security), 프라이버시(Privacy) 등