Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 7 pp. 435-448, 2021

https://doi.org/10.5762/KAIS.2021.22.7.435
ISSN 1975-4701 / eISSN 2288-4688

조직공정성과 조직 신뢰가 정보보안 기술 스트레스 완화에 미치는 영향 연구

황인호
국민대학교 교양대학

A study on the Effects of Organization Justice and Organization Trust on Mitigation of Techno-stress Related to Information Security

Inho Hwang
College of General Education, Kookmin University

요 약 정보보안이 조직의 중요한 가치로 인식되면서, 조직들은 엄격한 정보보안 기술 및 정책을 도입하여 정보 보안 사고를 예방하고자 한다. 그러나, 엄격한 정보보안 관련 기술은 정보보안을 실행에 옮겨야 하는 조직원에게 부정적 행동의 원인인 기술 스트레스를 일으킬 수 있다. 연구의 목적은 개인의 정보보안 준수의도에 부정적 영향을 미치는 정보보안 관련 기술 스트레스를 제시하고, 정보보안 관련 기술 스트레스 완화요인(조직 공정성, 조직 신뢰)을 제시하는 것이다. 설문 대상은 정보보안 정책과 기술을 적용하고 있는 조직의 조직원이며, 구조방정식 모델링을 통해 연구가설을 검증하였다. 연구 결과, 정보보안 관련 기술 과부하와 기술 복잡성이 정보보안 준수의도를 감소시켰으며, 정보보안 관련 조직 공정성이 기술 과부하와 기술 복잡성을 완화시켰다. 특히, 조직 신뢰는 기술 과부하와 준수의도간의 부정적 영향 관계를 조절하였다. 연구는 정보보안 기술 도입이 조직원에게 스트레스를 유발할 수 있음을 확인하였고, 기술 스트레스를 감소시키기 위한 전략적 방향을 제시한 측면에서 시사점을 가진다.

Abstract Because information security is judged to be among an organization's core values, organizations are trying to prevent security breaches by adapting strict security technologies and policies. However, strict information security-related technologies can cause techno-stress, which is a cause of negative behavior in employees of the organization. The purpose of this study is to identify information security-related techno-stress that negatively affects an individual's compliance intention, and to present techno-stress mitigation factors. Employees of an organization that was applying information security policies and technologies were surveyed, and the research hypothesis was verified through structural equation modeling. One result of the study shows that techno-overload and techno-complexity reduce compliance intention, but organizational justice mitigated techno-stress. In particular, organizational trust moderated the negative relationship between techno-overload and compliance intention. This study implies that adaption of strict information security technology can cause techno-stress in employees of an organization, but there is a strategic direction for reducing techno-stress.

Keywords : Compliance Intention, Techno Overload, Techno Complexity, Organization Justice, Organization Trust

이 논문은 2020년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2020S1A5A8040463)
*Corresponding Author : Inho Hwang(Kookmin Univ.)
email: hwanginho@kookmin.ac.kr
Received March 29, 2021 Revised April 19, 2021
Accepted July 2, 2021 Published July 31, 2021

1. 서론

정보보안이 조직의 핵심 운영관리 요인으로 인식되면서, 조직들은 다각적 관점에서 정보보안 수준 향상을 위한 노력을 하고 있다. 대표적으로, 많은 조직들이 ISO/IEC 27001 국제 인증을 통해, 정보보호 정책, 물리적 보호, 정보 통제 등 체계적으로 정보보안 수준을 높이고 있음을 증명하고 있으며, 자체적인 정보 관리 및 통제 정책 및 관련 시스템을 도입하기 위한 노력을 하고 있다. 그럼에도 불구하고, 정보 노출 사고는 지속적으로 발생하고 있다. 정보보안 사고 유형을 외부, 내부, 그리고 파트너로 구분한 Verizon[2020]은 매년 조직 외부(해킹, 멀웨어, 피싱 등)에 의한 정보 노출 사고가 50~70% 수준에서 발생하고 있으며, 내부(내부 근로자의 실수 등)에 의한 정보노출 사고는 20~30% 수준, 그리고 파트너에 의한 사고는 5% 이하 수준에서 발생하고 있음을 제시하고 있다[1]. Loch et al.[1992]은 정보보안 사고는 유형별 다르게 나타나며, 유형에 맞는 대처가 필요하다고 보았다[2]. 그들은 인간 또는 비인간적 요소들의 외부 침입은 방어벽과 같은 조직 내 보안 시스템의 강화를 통해 해결할 수 있다고 보았다. 반대로, 인간적 요소의 내부 침입은 조직 구성원 개개인의 행동적 문제이기 때문에, 심리적 관점에서 부정적 행동을 방지하기 위한 제재, 예방관점의 노력을 통해 해결할 수 있다고 보았다[2]. 즉, 조직이 지속적 관점에서 정보보안 관리 수준을 높이기 위해서는 정책, 기술과 같은 인프라 측면의 보안 구조 정립과 더불어 구성원 개인의 행동 통제를 위한 정책 수립 및 예방관리가 함께 이루어져야 한다[3]. 즉, 정보 노출 사고의 20~30%를 차지하고 있는 내부자의 보안 미준수 위협 예방을 위한 노력 또한 필요한 시점이다.

정보보안 내부자의 준수 행동과 동기 형성 관련 선행연구는 내부자의 정보보안 준수 행동은 개인 의지에 따라 다르게 나타나며 준수 행동에 대한 결과를 숨길 수 있는 반면, 조직은 모든 구성원의 보안 행동 정보를 알지 못하는 상황에 직면하기 때문에 구성원 스스로 정보보안을 지킬 수 있도록 하는 것이 필요하다고 보고 있다. 대표적으로, 선행연구는 범죄학, 심리학, 사회학 등에서 집단과 개인 간 관계 또는 개인의 행동 동기 관련 이론(합리적 선택이론, 보호동기이론, 제재 이론, 계획된 행동이론, 중화이론 등)들을 정보보안 분야에 적용하여 조직 내 부자의 미준수 행동을 최소화 또는 지속적 준수 행동 향상을 위한 동기적 요인들을 제시해왔다[4-8]. 즉, 선행연구들은 조직에서 개인의 보안 준수 행동 동기를 조직 행동 관점(정책, 제재 수립 등), 개인 의사결정 관점 등 다양한 측면에서 제시하여 조직 내부의 보안 수준 향상을 위해 추진해야 할 방향을 제시하였다는 측면에서 시사점을 가진다.

최근에는 조직이 도입한 기술과 정책에 대하여 복잡성 등의 이유로 형성되는 부정적 관점을 확인하는 스트레스 관련 연구들이 제시되고 있다[9,10]. 정보보안 분야에서도, 엄격한 정보보안 기술 도입이 조직원의 업무 진행에 방해되고, 엄격한 보안 준수에 어려움을 가질 수 있다는 정보보안 관련 스트레스 관련 연구들이 제시되고 있다[11-13]. 선행연구는 정보보안 관련 스트레스가 기술 관점, 또는 업무적 관점에서 발생하며, 정보보안 준수 행동에 부정적 영향을 미치는 것을 탐색적 관점에서 확인하였으나, 아직까지 정보보안 도입에 의해 발생 가능한 개인 차원의 스트레스를 완화시키기 위한 조건을 다양하게 제시하지 못하고 있다.

이에, 연구는 정보보안 준수의도에 부정적 영향을 미치는 정보보안 관련 기술 도입에 따라 발생가능한 스트레스 유형을 제시하고, 스트레스 완화를 위한 방안을 제시하는 것을 목적으로 한다. 세부적으로, 연구는 정보보안 관련 기술 과부하와 기술 복잡성이 정보보안 준수의도에 미치는 부정적 영향을 확인하고, 정보보안과 관련한 조직이 제공하는 공정성과 조직 신뢰가 정보보안 관련 기술 스트레스를 완화하는 것을 확인하고자 한다.

2. 이론적 배경

2.1 정보보안 준수의도

조직 내부에서 보안 사고는 내부자의 직업과 상황과 관계없이, 정보시스템에 대한 접근 권한만 있으면, 언제, 어디서나 발생할 수 있다. 실제로, 보안 사고를 일으킨 내부자의 직업은 IT 기술자, 사무직 근로자, 엔지니어, 영업직 근로자 등 다양하게 나타나고 있다[1]. 최근 전 세계적으로 확산하고 있는 코로나 사태는 조직 내 근로자들의 회의, 공동 사무실 활용과 같은 집단 모임을 최소화하길 요구하고 있어, 자연스럽게 외부에서 정보시스템에 대한 접근이 가능해지고 있다. 즉, 업무의 효율성 증대를 위한 정보 공유 & 연계 활동이 정보보안에는 취약점일 수 있는 문제점을 가진다[14].

조직 내 정보시스템에 대한 접근 방식과 주체가 다양해질수록, 조직원이 스스로 정보보안에 대한 필요성을 인식하고 행동하도록 하는 것이 필요하다[15,16]. 즉, 개인

이 정보보안에 대한 준수의도를 발현되도록 하여, 조직의 정보 관리를 위한 행동이 자연스럽게 나타나도록 하는 것이 필요하다[5]. 정보보안 준수의도(information security compliance intention)는 조직의 정보 자원에 대한 위협 요인들로부터 해당 자원을 보호하기 위한 개인들의 행동 의지로서[4], 현재 또는 미래에 조직 내 정보 관리를 위하여 몰입하고자 하는 개인의 정신적 상태이다[17]. 즉, 정보보안 준수의도는 조직이 구축한 정보를 언제든 능동적으로 보호하고자 하는 행동 의지이다. 따라서, 조직은 개인의 정보보안 준수의도 향상을 위한 동기 형성 또는 부정적 의도를 가지지 않도록 동기 형성할 수 있도록 지원하는 것이 필요하며[18], 연구는 부정적 영향을 미치는 동기적 요인인 정보보안 관련 기술 스트레스와 이를 완화하는 요인인 공정성, 조직 신뢰에서 준수의도 향상 방향을 제시하고자 한다.

2.2 정보보안 관련 기술 스트레스

기술 스트레스(techno stress)는 개인을 둘러싼 기술적 환경과 개인의 상황 또는 기술에 대한 인식의 차이에 의해 발생하는 개념으로서[19], 일찍이 Brod[1982]는 기술 스트레스를 개인 또는 조직에 도입되어 운영되는 새로운 기술을 활용할 수 없는 상태로 정의하였다. 그는 효율성 향상을 위한 새로운 기술의 투입은, 역으로 해당 기술에 대한 경험, 지식 확보를 위한 추가적인 자원 투입을 요구하기 때문에 스트레스로 나타날 수 있다고 보았으며, 이를 기술 스트레스라고 지칭하였다[20]. 즉, 조직에서 새로운 기술의 도입은 조직 전체의 표준 프로세스 등의 체계를 정립함으로써 효율성 및 성과를 높이는 중요 요인이지만, 해당 기술을 업무에 적용해야 하는 구성원에게 프로세스의 변화, 기술 경험 부재 등의 추가적인 문제를 발생시켜 업무 수행에 부정적 영향을 줄 수 있다[10,21,22].

조직에서 도입하는 기술은 특성별 스트레스를 다르게 발현시킨다. Tarafdar et al.[2007]은 기술 스트레스를 발현시키는 요인을 기술 스트레서(techno stressor)로 정의하였으며, 기술 과부하, 기술 침해, 기술 불안정성, 기술 복잡성, 그리고 기술 불확실성을 세부 요인으로 구성하여, 기술 스트레스 발현이 개인의 행동에 부정적 영향을 주는 외부 동기적 요인이 되는 것을 확인하였다[9].

정보보안 분야에서도 정보보안 정책과 기술의 도입이 구성원의 관련 스트레스를 발생시킬 수 있다. D'Arcy et al.[2014]은 조직의 정보보안 정책 및 활동을 통해 발생하는 스트레스를 정보보안 관련 스트레스로 정의하였으며, 정보보안 관련된 엄격하고 빠르게 변화하는 보안 정책 및 규정, 그리고 기술 도입 상황이 구성원에게 스트레스로 나타날 수 있음을 확인하였다[11]. 즉, 조직은 정보자원에 대한 내부 또는 외부의 침입을 방어하기 위하여, 더욱 엄격한 예방 정책을 수립하고 관련 시스템을 도입해야만 하는데, 실제 업무에 관련 보안 정책과 기술을 적용해야 하는 구성원은 새로운 보안 관련 표준이 제시될 때마다 새롭게 해당 기술을 이해해야 하는 상황에 직면할 수 있으며, 추가적으로 업무 적용 절차, 방식 등의 어려움을 호소할 수 있다. 이와 같이, 정보보안 관련 스트레스는 나타날 수 있으며, 스트레스 발생 시 구성원은 보안 행동을 회피하거나 숨길 수 있다[12].

정보보안 기술과 관련하여 개인에게 발생가능한 스트레스는 해당 기술 도입으로 업무에 과부하가 일어나거나, 복잡한 기술 도입으로 인한 걱정 등이 발생할 때 나타날 수 있다[12]. 첫째, 기술 과부하(techno overload)는 기술이 무의식적으로 구성원에게 더 많은 일을 하도록 유도하는 것으로서[22], 조직에 도입한 기술이 개인들의 업무를 늘리거나 더 빠르게 일하도록 함으로써 스트레스를 발생시키는 것을 의미한다[21]. 정보보안 관련하여 기술 과부하는 정보보안 관련 기술로 인하여 기존 업무의 양을 증가시키는 상황으로 설명할 수 있다[12]. 예를 들어, 정보보안 정책의 도입은 정보자산인 문서를 생성, 보관, 공유 시 접근 권한 또는 허가와 같은 새로운 프로세스를 요구할 수 있기 때문에, 개인의 업무에 추가적 활동을 부여할 가능성이 높으며, 기술 과부하 기반의 스트레스로 나타날 수 있다.

둘째, 기술 복잡성(techno complexity)은 직원들이 정보 기술의 높거나 어려운 품질 수준으로 인하여 무능력함을 가지는 수준을 의미하며[22], 엄격하고 복잡한 기술의 도입은 개인의 기술 습득에 어려움을 가져오며 스트레스로 나타나는 상황을 지칭한다[21]. 정보보안과 관련하여 기술 복잡성은 정보보안 기술 도입이 기존의 업무 프로세스의 변화, 이행 절차의 복잡한 상황, 그리고 엄격한 준수 조건을 가지는 것을 의미한다[12]. 예를 들어, 정보보안 기술은 기존 구성원이 이해하던 기술의 표준 정의와 달라, 새로운 표준화된 절차, 행동 정의 등의 이해를 요구하기 때문에 구성원들이 관련 기술을 이행하는데 걱정 또는 두려움을 가지도록 할 수 있다. 따라서, 정보보안 관련 기술 과부하와 기술 복잡성은 조직 구성원의 스트레스를 발생시키는 요인이며, 스트레스가 높아질수록 조직이 요구하는 보안 관련 행동을 회피할 가능성이 높아진다[11,12]. 이에 연구는 해당 요인들의 부정적 효과

와 완화 방향을 제시하고자 한다.

2.3 정보보안 관련 조직 공정성

조직공정성(organization justice)은 집단에서 개인이 특정 행동 및 결과에 대한 판단을 공정(fairness)을 기반으로 하는 수준을 의미한다[23]. 즉, 조직 공정성은 개인과 집단 간의 상호관계에서 개인의 행동이 집단 내의 판단과 비교 시 적절한지를 판단하는 개념이다[24]. 일찍이, 결과의 분배관점에서 공정성 개념을 제시한 Adams[1965]는 교환관계에 있는 이해관계자의 행동 결과에 대한 평가의 공정성은 상대적 비교를 통해, 즉 상대적 만족감의 수준을 통해 결정된다고 하였다[25]. 즉, 조직에서 개인이 받는 금전적, 비금전적 가치의 공정성은 자신과 비슷한 사례에서 발생한 가치의 수준과 비교할 때, 만족 또는 불만족을 결정하며, 만족 수준이 높아질 때 공정하다고 판단한다[26].

초기의 공정성 이론은 형평의 개념을 강조하여, 결과에 대한 분배에 대한 관점을 중점적으로 다루었으나, 최근에는 결과를 형성시키는 사전 절차와 정보 제공의 방식에 따라 결과가 달라지는 측면을 감안 하여, 다양한 공정성 관점이 제시되고 있다[27]. 즉, 보상에 대한 분배 관점의 공정성뿐만 아니라, 분배과정에서 발생하는 절차에 대한 적절성, 그리고 관련 행동에 필요한 정보 제공의 공정성 등이 제시되고 있다[24]. 즉, 공정성은 결과 중심의 행동 평가의 적정성에 대한 수준에서 결과를 도출하기 위한 과정과 사전 정보 제공 등의 공정성으로 분류되고 있으며, 특정 행동에 대한 동기 형성, 행동 과정, 그리고 결과까지 공정하다고 판단할 때, 조직이 자신에게 공정하다고 판단한다[28].

정보보안 분야에서도 조직 공정성은 구성원의 긍정적인 정보보안 행동의 동기적 요인이다. 정보보안 관련 정책과 기술에 대한 준수 행동은 조직 내부자는 직위, 직무와 관계없이 실행되어야 하며, 미준수 행동 시 발생하는 처벌과 같은 결과 또한 공정해야 한다[29]. 즉, 조직 구성원들의 정보보안 관련 행동에 대한 결과, 과정, 그리고 정보보안 준수에 필요한 정보 제공 등의 전체적인 활동이 공정할 때, 조직원들은 보안 준수에 대한 동기를 형성하고 미준수 행동을 억제한다[30].

2.4 조직 신뢰

신뢰는 이해당사자 상호관계성에서 발생하는 호의적인 믿음의 수준으로서[31], 특정 대상자에게 대한 믿음이 형성될 때 상호 간에 이익이 되는 행동을 할 것이라는 심리적인 상태를 가진다는 관점이다. 즉, 신뢰는 상대방이 자신에게 불이익을 주지 않고 바른 행동을 할 것이라고 믿는 상태이기 때문에, 본인 또한 대상자에게 이익이 되는 행동을 하고자 하는 동기적 요인이다[32]. 조직 신뢰(organization trust)는 개인과 조직간의 관계에서, 조직이 자신에게 호의적이고 이익이 된다고 믿는 수준을 지칭한다[33].

조직, 개인 등 상호간에 신뢰가 형성되기 위해서는 신뢰 형성을 위한 무결성, 역량(능력), 호혜성과 같은 조건이 필요하다[34]. 무결성은 상대방이 자신에게 거짓이나 불이익이 되는 행동을 하지 않을 것이라는 믿음의 수준으로서, 상대방이 정직하다고 판단될 때 형성된다. 역량 또는 능력은 상대방의 행동이 전문성을 보유하고 있어 거짓이 없다고 판단하는 수준이다. 따라서, 특정 주제에 대한 지식을 충분히 가지고 있어, 행동 방식의 문제가 없다고 생각할 때 발생한다. 마지막으로, 호혜성은 상대방의 행동이 본인에게 호의적이라고 판단하는 수준을 의미한다[35]. 따라서, 조직에 대한 신뢰는 조직이 본인에게 이익이 되고 호의적이며, 전문성을 갖출 때 형성된다[34].

정보보안 분야에서도 조직 신뢰는 개인의 보안 행동 동기로 작용한다. 즉, 조직이 공정하고 개인 및 조직 전체에게 이익이 되는 정보보안 활동의 필요성을 제시할 때, 조직 신뢰가 형성되고 긍정적 행동을 할 수 있도록 돕는다[35]. 특히, 조직이 정보보안 활동의 필요성을 명확하게 정립하고, 모든 구성원에게 공정하게 운용함을 선포할 때(정보보안 비전 선포식 등), 조직원들은 조직에 대한 신뢰를 형성하게 되고, 조직이 요구하는 행동으로 이어진다[35].

3. 연구 모델 및 가설 설정

3.1 연구 모델

본 연구는 정보보안 관련 기술 스트레스가 개인의 정보보안 준수의도에 미치는 부정적 영향을 확인하고, 정보보안 관련 조직공정성과 조직 신뢰가 정보보안 관련 기술 스트레스를 완화시키는 것을 확인하고자 한다. 이에 다음 Fig. 1.의 연구 모델을 제시한다.

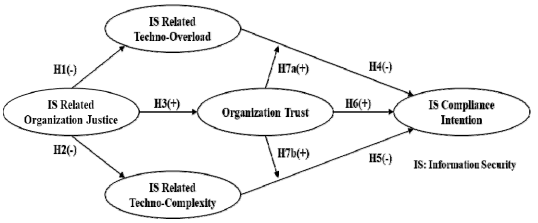

Fig. 1. Research Model and Proposed Hypotheses

3.2 연구 가설

3.2.1 조직 공정성과 기술 스트레스간의 관계

조직의 구성원에 대한 공정성은 개개인들의 특정 스트레스를 감소시킨다. 정보보안 관점에서 조직 공정성은 조직 내 모든 구성원에게 정보보안 관련 행동 정보를 명확하고 동등하게 제공하고, 행동 절차에 대한 피드백 등의 활동을 명확하게 하며, 행동 결과에 대한 긍정 또는 부정적 결과에 대한 혜택 또는 처벌을 정확하게 하는 전체적인 활동의 적정성을 의미한다[36]. 개인의 정보보안 준수 행동 과정과 결과에 대한 조직의 평가가 상대적으로 적정하다고 판단할 때, 공정성은 높아지며 개인에게 형성된 스트레스를 감소시킨다[24,27,37]. 또한, 형성된 조직 공정성은 정보보안 활동에 필요한 정보 등을 객관적으로 제공하고 있음을 의미하기 때문에, 조직 내 정보보안 관련 업무를 적용할 때 발생하는 개인의 걱정, 두려움을 감소시킨다[38]. 더불어, Cho et al.[2019]은 정보보안 관련 직업 스트레스가 개인의 이직의도에 미치는 부정적 영향을 조직이 공정하다고 믿을 때 완화하는 것을 확인하였다[29]. 즉, 정보보안 관련 공정성은 정보보안 기술 도입으로 발생하는 기술 과부하와 기술 복잡성에 의한 스트레스를 감소시킬 것으로 판단하며, 다음의 연구가설을 제시한다.

H1. 정보보안 관련 조직 공정성은 정보보안 관련 기술 과부하에 부(-)의 영향을 줄 것이다.

H2. 정보보안 관련 조직 공정성은 정보보안 관련 기술 복잡성에 부(-)의 영향을 줄 것이다.

3.2.2 조직 공정성과 조직 신뢰간의 관계

신뢰는 이해관계자의 상호 교환관계에서 형성되기 때문에, 공정성이 중요한 선행 조건이다[31]. 조직이 구성원에게 신뢰를 형성시키기 위해서는 전문성을 기반으로, 상대방인 조직원에게 이익과 호의성을 보이는 것이 필요하며[32], 공정성은 과정과 결과에 대한 평가가 자신에게 피해를 주지 않는다는 개념이기 때문에, 특정 활동 및 결과 타인과 공정하다고 판단할 경우 조직에 대한 신뢰를 형성할 수 있다[39,40]. Zeinabadi and Salehi[2011]는 교환관계에서 절차적 공정성과 조직 신뢰가 직업 만족 및 조직시민행동에 미치는 영향을 확인하였으며, 절차적 공정성이 신뢰를 높이는 것을 확인하였다[41]. Hwang[2020]은 정보보안 관련 조직 공정성이 있음을 구성원에게 제시할수록 구성원의 조직 신뢰를 높여 정보보안 관련 회피행동을 감소시키는 것을 확인하였다[42]. 즉, 정보보안 관련 공정한 행동이 조직에 대한 구성원들의 신뢰를 형성시킬 것으로 판단하고 연구가설을 제시한다.

H3. 정보보안 관련 조직 공정성은 조직 신뢰에 정(+)의 영향을 줄 것이다.

3.2.3 기술 스트레스와 준수의도간의 관계

조직은 내부자들의 정보보안 준수 수준 향상을 위하여 엄격한 기술 및 정책을 도입함으로써 해결하길 원하지만, 조직원들은 해당 기술 및 정책을 업무에 적용함에 있어, 적용 결과의 불확실성, 걱정 등의 스트레스를 발생시킬 수 있다[11]. 형성된 기술 스트레스는 조직원의 부정적 행동 동기로서, 개인의 만족을 감소시키거나 조직이 요구하는 행동 수준을 회피하고자 하는 원인이 된다. Jena[2015]는 조직이 제공하는 엄격한 기술이 스트레스를 발생시키고 개인의 만족 감소와 더불어 조직에 대한 몰입을 감소시켜 나아가 조직에 피해를 준다고 하였으며[10], Fuglseth and Sørebø[2014]는 기술 스트레스가 개인의 걱정, 두려움 등에 영향을 주어, 부정적 행동성을 높인다고 하였다[22]. 더욱이, Hwang and Cha[2018]는 정보보안 관련 기술 스트레스가 업무 스트레스를 높여, 조직 몰입 및 정보보안 준수의도를 감소시키는 원인이 됨을 확인하였으며[12], D'Arcy et al.[2014]은 정보보안 스트레스가 감정 대처에 영향을 주어 보안 회피의도를 높이는 요인임을 확인하였다[11]. 즉, 정보보안 관련 기술 스트레스(기술 과부하, 기술 복잡성)는 조직이 요구하는 정보보안 수준을 감소시키는 원인이며, 다음과 같은 연구가설을 제시한다.

H4. 정보보안 관련 기술 과부하는 정보보안 준수의도에 부(-)의 영향을 줄 것이다.

H5. 정보보안 관련 기술 복잡성은 정보보안 준수의도에 부(-)의 영향을 줄 것이다.

3.2.4 조직 신뢰와 준수의도간의 관계

조직 신뢰의 형성은 개인 수준에서의 만족감을 형성시키며, 조직에 대한 충성도가 높아져 긍정적 행동을 하도

록 한다. Top et al.[2015]은 병원 조직에서 구성원들의 조직에 대한 신뢰가 높아질수록 조직 몰입이 높아진다고 하였으며[43], Krosgaard et al.[2002]은 조직 신뢰가 조직에 대한 이타적 행동인 조직시민행동을 높이는 선행요인임을 확인하였다[44]. 정보보안 분야에서도 조직 신뢰는 조직의 보안 요구수준을 달성하는 선행 조건인데, Lowry et al.[2015]은 정보보안 정책 이니셔티브 및 행동을 통해 형성한 조직 신뢰가 정보보안 미준수의도를 감소시킨다고 하였으며[35], Hwang[2020]은 조직 신뢰는 조직이 구성원에게 피해를 주지 않을 것이라는 속성을 포함하기 때문에, 조직의 성과와 본인의 성과를 동일시함으로써 긍정적 행동으로 이어진다고 하였다[42]. 선행연구를 기반으로 조직 신뢰는 정보보안 준수의도에 긍정적인 영향을 주며, 다음의 연구가설을 제시한다.

H6. 조직 신뢰는 정보보안 준수의도에 정(+)의 영향을 줄 것이다.

3.2.5 조직 신뢰의 조절 효과 관계

조직 신뢰는 전체적인 조직의 행동이, 구성원에게 도움이 된다고 믿을 때 형성되기 때문에, 조직에 대한 신뢰를 보유한 조직원은 조직의 특정한 요구가 본인에게 불평등하거나 피해를 준다고 판단하지 않는 경향이 있다[32]. 그러므로, 조직이 특정한 행동이나 업무에 추가적인 활동을 구성원에게 요구하는 경우가 발생하더라도, 조직에 대한 신뢰가 높으면 해당 상황에 의한 스트레스를 적게 받는다[42]. Guinot et al.[2014]은 조직 내 구성원 간 형성된 신뢰가 개인들의 업무 스트레스를 완화시켜 직업만족도를 높이는 것을 확인하였으며[45], Top and Tekingunduz[2018]는 구성원에게 공정하고 신뢰받는 조직은 구성원들의 업무 스트레스를 감소시키는 것을 확인하였다[46]. 특히, Hwang[2020]은 정보보안 도입으로 인하여 발생한 업무적 갈등을 조직 신뢰가 감소시키는 것을 확인하였다[42]. 선행연구는 조직 신뢰가 부정적 행동을 발생시키는 스트레스를 완화시키는 요인임을 제시하고 있다. 본 연구는 조직 신뢰가 기술 스트레스가 정보보안 준수의도에 미치는 부정적 영향에 대하여 조절효과를 가질 것으로 판단하고 다음의 연구가설을 제시한다.

H7a. 조직 신뢰는 정보보안 관련 기술 과부하와 정보보안 준수의도간의 영향관계를 조절할 것이다.

H7b. 조직 신뢰는 정보보안 관련 기술 복잡성과 정보보안 준수의도간의 영향관계를 조절할 것이다.

3.3 데이터 측정 도구 및 수집

연구는 정보보안 관련 기술 스트레스와 완화요인, 그리고 정보보안 준수의도간의 관계를 확인하기 위하여 서베이 기법을 적용하여 구조방정식 모델링 기반의 양적 분석을 실시하고자 한다. 이에, 연구는 정보보안 분야 및 타 분야에서 적용되던 선행 요인들을 국내 정보보안 특성에 맞추어 7점 리커트 척도로 구성된 다 항목 기반의 설문 항목으로 재구성하였다.

정보보안 관련 조직 공정성은 조직이 정보보안 활동과 관련하여 전체적으로 공정하다고 판단하는 수준으로서[28], 선행연구를 기반으로 정보보안 특성에 맞게 재구성하여, “전체적으로, 정보보안과 관련하여 공정하게 대우를 받음”, “나는 정보보안에 대하여 우리 조직이 공정하다고 판단”, “일반적으로 조직의 정보보안 활동은 공정함”, “조직은 정보보안 활동에 대하여 공평하게 대우”와 같이 4개 항목으로 구성하였다. 정보보안 관련 기술과부하는 정보보안 관련 기술로 인한 더 많은 업무를 수행하도록 만드는 수준으로서[9], 선행연구를 기반으로 정보보안 특성에 맞게 재구성하여, “정보보안 기술 때문에, 처리할 수 있는 것보다 더 많은 작업을 요구받음”, “정보보안 기술 때문에 업무일정에 방해받음”, “정보보안 기술 적응을 위해 나의 작업 행동을 변화 받도록 요구받음”과 같이 4개 항목으로 구성하였다. 정보보안 관련 기술복잡성은 정보보안 기술이 복잡해짐에 따라 본인의 능력이 부족하다고 느끼는 수준으로서[9], 선행연구를 기반으로 정보보안 특성에 맞게 재구성하여, “나는 새로운 보안 기술을 이해하고 사용하는데 시간이 필요”, “나는 보안 기술을 배우기 위한 충분한 시간이 없음”, “정보보안 기술이 종종 어려운 부분이 있음”과 같이 3개 항목으로 구성하였다. 조직 신뢰는 조직이 약속을 지키고 자신의 이익에 도움이 된다고 믿는 수준으로서[32], 선행연구를 기반으로, “조직은 약속을 지키기 위해 노력”, “조직은 조직원을 의견을 고려하여 의사결정”, “조직은 나의 일을 성취할 수 있도록 도움”, “나는 조직 구성원을 위한 조직 결정에 기꺼이 따를 것”과 같이 4개의 항목으로 구성하였다. 마지막으로, 정보보안 준수의도는 조직 정보에 대한 위협요인으로부터 정보를 보호하고자 하는 의지 수준으로서[5], 선행연구를 기반으로, “정보보안 정책을 기꺼이 따를 것”, “정보보안 정책을 지속적으로 준수할 것”, “정보시스템 접속 시, 보안 정책을 지속적으로 준수할 것”, “업무 수행할 때마다 보안 절차를 따를 것”과 같이 4개 항목으로 구성하였다. 구성한 다 항목 기반의 설문은 사전에 정

보보안 관련 정책을 보유한 조직에서 근무하는 대학원생 10명을 대상으로 설문 항목의 적절성 및 이해도를 파악하여 수정하였다.

설문 대상은 연구 모델에서 제시한 정보보안 정책에 대한 조직원의 준수의도와 스트레스, 완화적 관계를 확인하기 위하여, 정보보안 정책을 도입한 기업에 다니는 근로자들을 대상으로 하였다. 설문은 대학의 주말반 재직자 전형에 다니는 경영학과 학생들을 대상으로 하되, 조직의 정보보안 정책을 알고 있는 사람들로 한정하였으며, 2019년 12월에 실시하였다. 설문 전 학생들에게 설문의 목적과 통계 활용 방법에 대하여 정확하게 고지한 후, 응답을 거절한 사람들을 제외하였으며, 333개의 응답을 분석에 적용하였다.

4. 가설 검증

4.1 기초 통계

연구가설 검증에 활용한 표본은 333개로 다음과 같은 인구통계학적 특성을 가진다. 첫째, 업종의 경우, 제조업은 58개(17.4%), 서비스업은 275개(82.6%)로 나타났다. 이러한 특성은 국내 서비스업의 비중과 비슷한 상황인 것으로 판단 되었다. 둘째, 응답자의 성별은 남성이 210개(63.1%), 여성이 123개 (36.9%)로 6:4의 비중인 것으로 나타났다. 셋째, 응답자의 연령의 경우 30세 미만은 103개(30.9%), 31-40세는 116개(34.8%), 41-50세는 83개(24.9%), 그리고 51세 이상은 31개 (9.3%)로 나타났다. 즉, 30-40세의 연령이 가장 많아 사회생활을 활발히 하는 연령층의 응답을 확보하였다. 마지막으로, 직급의 경우 사원급은 106개 (31.8%), 대리급은 92개(27.6%), 과장급은 52개 (15.6%), 차부장급은 50개 (15.0%), 그리고, 임원급은 33개(9.9%)를 확보하였다.

4.2 신뢰성 및 타당성 분석

연구는 구조방정식모델링을 통하여 연구 모델에 적용한 요인간의 관계성을 확인하기 때문에, 다 항목 기반 요인에 대한 신뢰성 및 타당성 분석을 실시한다. 신뢰성과 타당성 분석은 SPSS 21.0과 AMOS 22.0을 활용하였다. 신뢰성 분석은 다 항목 기반의 요인들이 내적인 일관성을 가지는가를 확인하는 기법으로, 연구는 탐색적 요인분석과 크론바흐 알파 값을 구함으로써 확인한다. 5개 요인 18개 항목에 대하여 탐색적 요인 분석 후 항목들이 각 요인으로 정확하게 묶인 것을 확인하였으며, 크론바흐 알파 분석을 실시하였다. Nunnally[1978]은 0.7이상의 크론바흐 알파 수준을 요구하였으며[47], 분석 결과 모든 요인들이 0.7이상으로 나타나 신뢰성을 확보하였다 (Table 1.).

Table 1. Result for Construct Validity and Reliability

Construct	Item	Factor Loading	Cronbach's Alpha	CR	AVE
Organization Justice	OJ 1 OJ 2 OJ 3 OJ 4	0.834 0.823 0.815 0.822	0.934	0.881	0.713
Techno Overload	TO 1 TO 2 TO 3	0.805 0.836 0.836	0.892	0.846	0.647
Techno Complexity	TC 1 TC 2 TC 3	0.793 0.774 0.746	0.854	0.811	0.589
Organization Trust	OT 1 OT 2 OT 3 OT 4	0.834 0.834 0.812 0.806	0.914	0.889	0.667
Compliance Intention	CI 1 CI 2 CI 3 CI 4	0.780 0.832 0.822 0.775	0.948	0.932	0.774

타당성 분석은 집중타당성 분석과 판별타당성 분석을 실시한다. 집중타당성은 요인의 구성 항목들이 요인에게 구성되어 있는지를 확인하는 기법으로 개념신뢰도와 평균분산추출에 대한 산출 식을 활용하여 확인한다. 개념신뢰도는 0.7이상, 평균분산추출은 0.5이상의 값을 요구한다[48]. 타당성 분석은 AMOS 22.0을 활용하여 확인적 요인분석을 실시하는데, 우선 구조모델의 적합성을 확인하였다. 구조 모델의 적합성 검증은 GFI는 0.9 이상, AGFI는 0.9 이상(0.8이상 가능), CFI는 0.9 이상, NFI는 0.9 이상, 그리고 RMSEA는 0.05 이하(0.1 가능)를 요구한다. 분석 결과, 확인적 요인분석의 적합성에 대한 문제는 없는 것으로 나타났다(x^2/df = 1.421, GFI = 0.944 AGFI = 0.923, NFI = 0.966, CFI = 0.990, RMSEA = 0.036). 이후, 개념신뢰도와 평균분산추출을 산출하였으며, 모든 요인이 요구수준을 충족하였다(Table 1).

판별타당성은 요인간 얼마나 차별성을 가지는지를 확인하는 기법으로서, 구조방정식모델링에서는 상관계수와 평균분산추출 값을 활용하여 확인한다. 판별타당성은 평균분산추출 제곱근들이 요인간의 상관계수보다 모두 클 때 판별타당성을 확보했다고 본다[49]. 분석 결과, 상관계수보다 평균분산추출 제곱근이 높은 것으로 나타나,

판별타당성 문제는 없는 것으로 나타났다(Table 2.).

Table 2. Result for Discriminant Validity

Constructs	1	2	3	4	5
Organization Justice	***0.844***				
Techno Overload	-.497**	***0.804***			
Techno Complexity	-.545**	.657**	***0.768***		
Organization Trust	.568**	-.447**	-.527**	***0.816***	
Compliance Intention	.644**	-.586**	-.633**	.619**	***0.880***

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

연구는 추가적으로 공통방법편의 문제를 확인하였다. 공통방법편의는 설문지 기법으로 수준을 판단하여 분석할 때 자주 발생하는 문제로서, 독립변수와 종속변수를 같이 측정할 때 사회적 바람직성 또는 편의성의 문제로 두 변수 간의 상관관계의 변이가 발생하는 문제이다. 본 연구는 Podsakoff et al.[2003]이 제시한 기법 중 가장 널리 활용되는 단일공통방법분석(single common method)기법을 활용하였다[49]. 해당 방법은 확인적 요인분석으로 적용된 구조 모델에 단일 요인을 추가하였을 때, 측정항목의 변화량을 살피는 기법으로 일반적으로 측정항목의 변화량이 0.2 이하이면, 공통방법편의 문제가 낮다고 판단한다. 분석 결과, 단일 요인 적용 전 구조모델의 적합도(x^2/df = 1.421, GFI = 0.944 AGFI = 0.923, NFI = 0.966, CFI = 0.990, RMSEA = 0.036)와 단일 요인 적용 후 구조모델의 적합도(x^2/df = 1.258, GFI = 0.956 AGFI = 0.929, NFI = 0.974, CFI = 0.995, RMSEA = 0.028)는 요구사항을 충족하였으며, 각 측정항목의 변화량이 0.2 이하로 나타나 공통방법편의 문제는 낮다고 판단한다.

4.3 주 효과 검증

연구는 조절효과 검증을 제외한 주 효과 검증을 실시한다. 구조방정식 모델링을 통한 주효과 검증은 구조방정식 모델의 적합성 검증 단계, 요인간의 경로(β) 검증 단계, 그리고 요인간의 영향력(R^2) 검증 단계로 실시한다. 첫째, 주 효과 분석에 적용한 구조모델의 적합성 검증을 실시하였다. 분석 기준은 앞서 확인적 요인분석에서 적용한 기준을 동일하게 적용하였으며, 분석 결과는 전체적 관점에서 분석에 문제가 없는 것으로 나타났다(x^2/df = 2.354, GFI = 0.904, AGFI = 0.873, NFI = 0.942, CFI = 0.965, RMSEA = 0.064).

둘째, 연구 모델에서 적용한 요인간의 경로(β) 검증을 통해 연구가설을 확인한다. 연구가설 1은 정보보안 관련 조직공정성이 정보보안 관련 기술 과부하에 부(-)의 영향을 미친다는 것으로, 경로 분석 결과 통계적으로 유의한 것으로 나타나 가설은 채택되었다(H1: β= -0.549, p<0.01). 이러한 결과는 조직이 공정할수록 구성원들의 업무 스트레스가 감소된다는 Tziner and Sharoni[2014]의 연구결과와 동일하다. 즉, 정보보안에 대한 조직차원의 공정한 규정 및 활동이 구성원의 기술 과부하에 의한 스트레스를 감소시키기 때문에, 정보보안 적용에 공정성을 반영할 수 있도록 노력하는 것이 필요하다. 연구가설 2는 정보보안 관련 조직공정성이 정보보안 관련 기술 복잡성에 부(-)의 영향을 미친다는 것으로, 경로 분석 결과 통계적으로 유의한 것으로 나타나 가설은 채택되었다(H2: β = -0.619, p<0.01). 이러한 결과는 조직의 공정성이 개인의 업무-가족간의 갈등을 감소시킨다는 Judge and Colquitt[2004]의 연구와 유사한 결과이다. 즉, 조직 차원의 공정성을 확립하기 위한 노력이 선행될 때, 개인의 스트레스를 감소시켜 내부의 보안 수준을 향상시킬 수 있다.

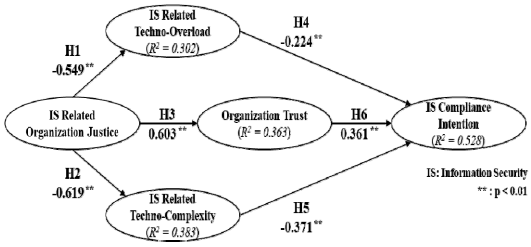

Fig. 2. Results of the Structural Model

Table 3. Summary of Hypothesis Tests (Main Effect)

Path		Coefficient	t-value	Results
H1	OJ → TO	-0.549	-9.608**	Support
H2	OJ → TC	-0.619	-10.198**	Support
H3	OJ → OT	0.603	11.128**	Support
H4	TO → CI	-0.224	-4.519**	Support
H5	TC → CI	-0.371	-6.759**	Support
H6	OT → CI	0.361	7.082**	Support

OJ(Organization justice), TO(Techno overload), TC(Techno complexity, OT(Organization trust), CI(Compliance intention)
**: p < 0.01

연구가설 3은 정보보안 관련 조직공정성이 조직 신뢰에 정(+)의 영향을 미친다는 것으로, 경로 분석 결과 통계적으로 유의한 것으로 나타나 가설은 채택되었다(H3: β= 0.603, p〈0.01). 이러한 결과는 조직의 활동이 공정하다고 판단될 때 조직에 대한 구성원의 신뢰가 형성된다는 Seifert et al.[2014]의 연구 결과와 유사하다. 즉, 정보보안 관련한 조직의 정보제공, 절차, 결과 등의 종합적인 공정함이 조직 신뢰를 형성하여 긍정적 행동으로 이어지도록 하기 때문에, 조직 공정성을 강조하는 전략을 수립하는 것이 필요하다. 연구가설 4는 정보보안 관련 기술과부하가 정보보안 준수의도에 부(-)의 영향을 미친다는 것으로, 경로 분석 결과 통계적으로 유의한 것으로 나타나 가설은 채택되었다(H4: β= -0.224, p〈0.01). 이러한 결과는 기술 스트레스가 조직 몰입에 부정적인 영향을 미친다는 Jena[2015]의 연구와 유사한 결과이다. 즉, 정보보안 기술 도입으로 인하여 추가적으로 발생하는 업무적 과부하가 조직의 요구 행동을 감소시키기 때문에, 업무 과부하를 완화시키기 위한 노력을 요구한다. 연구가설 5는 정보보안 관련 기술복잡성이 정보보안 준수의도에 부(-)의 영향을 미친다는 것으로, 경로 분석 결과 통계적으로 유의한 것으로 나타나 가설은 채택되었다(H5: β = -0.371, p〈0.01). 이러한 결과는 정보보안 기술 복잡성이 개인의 만족도를 감소시킨다는 Fuglseth and Sørebø[2014]의 결과와 유사하다. 즉, 정보보안 관련한 기술이 어려울수록 조직원에게 걱정 등 부담을 가져 부정적 행동을 유도하기 때문에, 기술에 대한 지식 향상을 위한 지원이 필요하다. 연구가설 6은 조직 신뢰가 정보보안 준수의도에 정(+)의 영향을 미친다는 것으로, 경로 분석 결과 통계적으로 유의한 것으로 나타나 가설은 채택되었다(H3: β= 0.361, p〈0.01). 이러한 결과는 조직 신뢰가 정보보안 미준수행동을 감소시킨다는 Lowry et al.[2015]의 연구 결과와 유사하다. 즉, 조직 신뢰는 조직에 대한 전체적인 호의적인 믿음이기 때문에, 신뢰가 형성될 경우 조직에 대한 이타적인 행동을 할 가능성이 높음을 의미하며, 조직차원에서 신뢰를 가질 수 있도록 노력하는 것이 필요하다.

마지막으로, 연구는 요인 간의 영향력(R^2) 검증을 실시하였다. 조직 공정성은 기술 과부하에 30.2%의 영향력을 가지는 것으로 나타났으며, 기술 복잡성에는 38.3%의 영향력을 가지는 것으로 나타났다. 또한 조직 신뢰에는 36.3%의 영향력을 가졌다. 또한, 기술과부하, 기술복잡성, 그리고 조직 신뢰는 정보보안 준수의도에 52.8%의 영향력을 가졌다.

4.4 조절효과 검증

연구 가설 7a와 7b는 조직 신뢰가 기술 스트레스와 준수의도 사이의 부정적 관계를 조절할 것이라는 것으로서, 연구 내 변수들이 리커트 척도로 구성되어 있기 때문에 요인간의 상호작용항을 만들어 상호작용효과를 확인함으로써 조절효과를 검증한다. 조절효과에 대한 상호작용항을 만드는 방법은 여러 가지가 있으나, 엄격한 방법 중의 하나인 직교화접근법(orthogonalizing approach)을 적용하여 조절효과 검증을 실시하였다[51]. 분석 결과는 Table 4.와 같다.

Table 4. Summary of Moderating Effect Tests

Path		Coefficient	t-value	Results
H7a	TO → CI	-0.37	-6.914**	Support
	OT → CI	0.445	8.183**	
	TO x OT → CI	0.106	2.004*	
H7b	TC → CI	-0.453	-7.334**	Reject
	OT → CI	0.362	6.327**	
	TC x OT → CI	0.058	1.321	

TO(Techno overload), TC(Techno complexity), OT(Organization trust), CI(Compliance intention)
* p 〈 0.05, ** p 〈 0.01

첫째, 조직 신뢰가 기술 과부하와 준수의도간의 부정적 관계를 조절할 것인지를 검증한 결과, 기술 과부하와 조직신뢰의 상호작용항이 채택되어 조직 신뢰의 조절효과가 있는 것으로 나타났다. 상세한 조절효과를 확인하기 위하여, 그래프로 표현하였으며, 결과는 Fig. 3.과 같다. 정보보안 관련 기술 과부하가 높은 집단에서 조직 신뢰가 높은 집단이 낮은 집단보다 준수의도에 미치는 부정적 영향을 높게 완화시키는 것으로 나타났다.

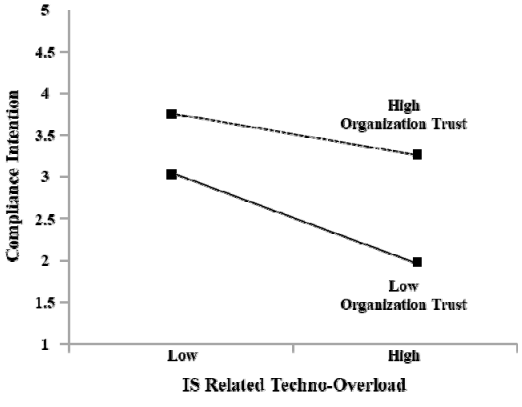

Fig. 3. Moderation Effect of Organization Trust

둘째, 조직 신뢰가 기술복잡성과 준수의도간의 부정적 관계를 조절할 것인지를 검증한 결과, 기술복잡성과 조직신뢰의 상호작용항이 기각되어 조직 신뢰의 조절효과가 없는 것으로 나타났다.

조절효과 분석 결과, 조직 신뢰는 정보보안 기술 도입으로 인하여 추가적으로 발생하는 업무적 문제에 의한 스트레스의 준수의도에 미치는 부정적 영향을 완화시키는 것으로 나타났다. 특히, 과부하가 높게 나타날 때, 조직 신뢰의 완화효과가 큰 것을 확인하였다. 따라서, 조직은 조직원들의 조직에 대한 신뢰 형성을 위한 지속적 정보 제공, 활동 등을 지속적으로 실시함으로써, 스트레스 완화를 유도하는 것이 필요한 것으로 판단된다.

5. 결론

5.1 연구 요약

최근 정보가 조직의 중요한 가치 관리요인으로 인식되면서 보안에 대한 기술적 투자가 많아지고 있다. 하지만, 엄격한 정보보안 기술에 대한 투자는 정보보안 활동을 업무에 적용하는 조직원들에게 스트레스로 작용할 수 있어, 스트레스 감소를 위한 요인을 제시하는 것이 필요한 상황이다.

본 연구는 정보보안 기술 도입에 의해 발생가능한 스트레스 요인인 기술 과부하와 기술 복잡성을 제시하고 정보보안 준수의도에 미치는 부정적 영향 및 스트레스 완화를 위한 조직공정성과 조직 신뢰의 영향력을 확인하고자 하였다. 이에, 정보보안 정책을 도입한 조직에 근무하는 조직원들을 대상으로 정보보안에 대한 설문을 실시하였으며, 구조방정식모델링을 기반으로 연구가설을 검증하였다. 결과는 정보보안 관련 기술 과부하와 기술 복잡성이 준수의도를 감소시키며, 정보보안 관련 조직 공정성이 기술 스트레스 요인을 완화시키는 것을 확인하였다. 또한, 정보보안 관련 조직 공정성이 조직 신뢰를 높여 준수의도에 긍정적 영향을 주는 것을 확인하였다. 추가적으로, 조직 신뢰가 정보보안 기술 과부하와 준수의도간의 부정적 관계를 조절하는 것을 확인하였다.

5.2 연구 시사점 및 한계

연구는 조직 내부의 정보보안 수준 향상을 위한 관점에서 다음과 같은 학술적 관점에서의 시사점을 가진다. 첫째, 연구는 정보보안 분야에 기술 스트레스를 적용하여, 기술 스트레스 관련 세부 요인을 제시하고 부정적 행동원인이 됨을 밝혔다. 세부적으로, 기술 스트레스 요인을 정보보안 관련 기술 과부하와 기술 복잡성으로 구분하여 제시하였는데, 정보보안 기술 도입으로 인하여 발생하는 추가적인 업무에 의해 발생하는 스트레스와 엄격하고 세밀한 기술 도입이 구성원에게 기술 사용의 어려움 등의 스트레스를 발생시켜 정보보안 준수의도에 부정적 영향을 주는 것을 확인하였다. 즉, 학술적 관점에서 기술 스트레스가 정보보안에 적용되는 것을 확인하였으며, 준수의도에 부정적 영향 요인을 제시한 관점에서 시사점을 가진다.

둘째, 연구는 조직 공정성의 역할을 정보보안 분야에 적용하여, 정보보안 관련한 조직의 공정한 활동으로 인한 인식형성이 어떠한 영향을 미치는지를 확인하였다. 세부적으로 정보보안 관련 정보 제공, 절차, 그리고 결과에 대한 복합적 의미인 조직 공정성은 어렵고 엄격한 수준의 기술 도입으로 인해 발생하는 스트레스를 감소시키는 요인임을 확인하였으며, 조직원이 조직에 대한 긍정적인 믿음을 형성할 수 있도록 돕는 요인임을 확인하였다. 즉, 학술적 관점에서 정보보안 활동이 조직 전체에 반영되어 믿을 수 있는 환경이 구축될 때 개인의 부정적, 긍정적 행동 동기에 영향을 준다는 것을 제시하였다는 측면에서 동기 개선 요인으로서의 시사점을 가진다.

셋째, 연구는 조직 신뢰가 미치는 긍정적 영향을 정보보안 분야에 적용하고, 확인하였다는 측면에서 시사점을 가진다. 세부적으로, 연구는 조직 신뢰가 정보보안 준수의도를 높이는 것을 확인하였으며, 조직 신뢰가 정보보안 관련 기술 과부하와 준수의도간의 부정적 관계를 조절하는 것을 확인하였다. 즉, 연구는 조직이 구성원에게 호의적이고 이익을 줄 수 있다는 믿음인 조직 신뢰의 형성은 조직이 요구하는 행동에 긍정적인 의도를 가질 수 있도록 하는 것을 확인하였기 때문에, 내부자의 정보보안 수준 향상의 선행 요인을 도출하였다는 측면에서 학술적 시사점을 가진다.

연구는 조직 내부의 정보보안 준수 수준 향상관점에서 다음과 같은 실무적 시사점을 가진다. 첫째, 연구는 정보보안 수준 향상을 위해 도입한 정보보안 기술이 실제 업무에 해당 기술을 적용해야 하는 조직원에게는 부정적 효과로 다가올 수 있음을 제시하고 확인하였다. 즉, 정보보안과 관련하여 도입한 기술이 엄격할수록, 업무에 추가적인 활동을 부여할수록 조직원에게는 해당 기술을 적용하는데 어려움을 가져와 스트레스를 발생시켜, 조직이 요구하는 보안 수준을 회피할 수 있다는 것을 실무적 관점

에서 확인하였다. 따라서, 조직은 정보보안 기술을 도입할 때, 구성원이 해당 기술을 어떻게 받아들일 것인지를 사전에 고려하고, 기술을 받아들일 수 있는 정보를 제공하거나, 기술에 의해 발생가능한 스트레스를 최소화하기 위한 노력이 필요하다.

둘째, 연구는 정보보안 관련 기술 스트레스를 완화시키기 위한 요인으로 정보보안 관련 조직 공정성을 제시하였다. 조직 공정성은 특정한 행동의 결과와 더불어, 대상 행동을 실행하기 위한 사전 정보 제공, 절차 등에 대한 전반적인 공평한 수준을 의미한다. 특히, 정보보안 관련 행동에 대한 결과가 누구에게나 반영되고 실행할 수 있는 정보를 명확하게 제공한다면 정보보안 공정성이 발현될 수 있다. 이 경우 해당 개인은 조직이 도입한 정보보안 기술이 모든 조직 구성원에게 필요하다고 인식함으로써 스트레스를 완화시킬 수 있다. 즉, 연구는 실무적 관점에서 도입한 기술에 의해 발생 가능한 정보보안 관련 스트레스를 완화하기 위한 조직 차원의 노력 요인을 공정성 관점에서 제시하였다는 측면에서 높은 시사점을 가진다.

셋째, 연구는 조직 신뢰가 조직이 요구하는 정보보안 관련 준수 활동에 긍정적 영향을 주고, 부정적 영향을 완화하는 것을 확인하였다. 즉, 조직에 대한 신뢰가 형성된 개인은 조직이 요구한 기술에 대하여 스스로 필요성을 인식하고, 행동 의지를 가지게 됨을 확인하였다. 따라서, 실무적 관점에서 조직이 내부의 정보보안 수준을 지속적으로 유지하기 위해서 확보해야 할 요인인 신뢰를 제시하였다는 측면에서 높은 시사점을 가진다.

본 연구는 내부의 정보보안 수준 감소 최소화를 위한 측면에서 학술적, 실무적 시사점을 제시하였으나, 다음과 같은 측면에서 연구적 한계를 가지며 추가적인 연구가 필요하다. 첫째, 연구는 조직과 개인간의 관계에서 정보보안 준수 의지 향상을 위한 요인을 제시하기 위하여 적정 대상을 선정하여 응답자의 생각을 측정하였다. 특히, 조직의 공정성, 신뢰 요인을 측정하기 위하여 해당 응답자의 응답 당시의 조직에 대한 생각을 측정할 수 밖에 없었다. 하지만, 명확한 조직의 공정성 수준과 신뢰 수준을 측정하고, 개인의 행동에 미치는 영향을 확인하기 위해서는 공정성 수준에 따라 분류된 집단별 분석, 즉 실험 또는 실제 사례 연구가 추가적으로 필요할 것으로 판단되며 향후 연구에서 이러한 부분을 보완한다면 보다 높은 실무적 시사점을 제시할 수 있을 것으로 판단한다. 둘째, 최근 정보보안 연구들도 보다 세밀한 관점에서 집단별 특성 분류, 개인의 특성 분류를 통해 특정 집단에서 정보보안 준수에 미치는 영향의 차이를 제시하고 있다. 대표적으로 Vance et al.[2020]은 개인주의-집합주의를 기반으로 집단 간 차이를 확인한바 있다[14]. 이렇듯 집단의 다양한 특성에 기반하여 내부자의 정보보안 준수에 미치는 영향 요인을 제시하고 결과를 확인한다면 보다 심도 있는 결과를 제시할 수 있을 것으로 판단한다.

References

[1] Verizon, 2020 Data Breach Investigations Report, 2020.

[2] K. D. Loch, H. H. Carr, M. E. Warkentin, "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly, Vol. 16, No. 2, pp. 173-186, 1992. DOI : https://doi.org/10.2307/249574

[3] R. West, "The Psychology of Security," Communications of the ACM, Vol. 51, No. 4, pp. 34-40, 2008. DOI : https://doi.org/10.1145/1330311.1330320

[4] B. Bulgurcu, H. Cavusoglu, I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness," MIS Quarterly, Vol. 34, No. 3, pp. 523-548, 2010.

[5] Y. Chen, K. Ramamurthy, K. W. Wen, "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?," Journal of Management Information Systems, Vol. 29, No. 3, pp. 157-188, 2010. DOI : https://doi.org/10.2753/MIS0742-1222290305

[6] K. H. Guo, Y. Yuan, N. P. Archer, C. E. Connelly, "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model", Journal of Management Information Systems, Vol. 28, No. 2, pp. 203-236, 2011. DOI : https://doi.org/10.2753/MIS0742-1222280208

[7] T. Sommestad, H. Karlzén, J. Hallberg, "The Sufficiency of the Theory of Planned Behavior for Explaining Information Security Policy Compliance," Information & Computer Security. Vol. 23, No. 2, pp. 200-217, 2015. DOI : https://doi.org/10.1108/ICS-04-2014-0025

[8] I. Hwang, R. Wakefield, S. Kim, T. Kim, "Security Awareness: The First Step in Information Security Compliance Behavior," Journal of Computer Information Systems, pp. 1-12, 2019. DOI : https://doi.org/10.1080/08874417.2019.1650676

[9] M. Tarafdar, Q. Tu, B. S. Ragu-Nathan, T. S. Ragu-Nathan, "The Impact of Technostress on Role Stress and Productivity," Journal of Management Information Systems, Vol. 24, No. 1, pp. 301-328, 2007. DOI : https://doi.org/10.2753/MIS0742-1222240109

[10] R. K. Jena, "Technostress in ICT Enabled Collaborative Learning Environment: An Empirical Study among Indian Academician," Computers in Human Behavior, Vol. 51, pp. 1116-1123, 2015.
DOI : https://doi.org/10.1016/j.chb.2015.03.020

[11] J. D'Arcy, T. Herath, M. K. Shoss, "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," Journal of Management Information Systems, Vol. 31, No. 2, pp. 285-318, 2014.
DOI: https://doi.org/10.2753/MIS0742-1222310210

[12] I. Hwang, O. Cha, "Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance," Computers in Human Behavior, Vol. 81, pp. 282-293, 2018.
DOI : https://doi.org/10.1016/j.chb.2017.12.022

[13] J. D'Arcy, 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, pp. 103151, 2019.
DOI : https://doi.org/10.1016/j.im.2019.02.006

[14] A. Vance, M. T. Siponen, D. W. Straub, "Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations across Cultures. Information & Management, Vol. 57, No. 4, pp. 103212, 2020.
DOI : https://doi.org/10.1016/j.im.2019.103212

[15] I. Hwang, D. Kim, T. Kim, S. Kim, "Why not Comply with Information Security? An Empirical Approach for the Causes of Non-compliance," Online Information Review, Vol. 41, No. 1, pp. 1-17. 2017.
DOI : https://doi.org/10.1108/OIR-11-2015-0358

[16] S. Hu, I. Hwang, "Analysis of The Effects of Information Security Policy Sanction, Perceived Threat, and Perception of Information Security Climate on Compliance Behavioral Intention: Focusing on Prospect and Goal Orientation," Journal of the Korea Academia-Industrial Cooperation Society, Vol. 22, No. 1, pp. 595-602, 2021.
DOI: https://doi.org/10.5762/KAIS.2021.22.1.595

[17] N. S. Safa, C. Maple, S. Furnell, M. A. Azad, C. Perera, M. Dabbagh, M. Sookhak, "Deterrence and Prevention-based Model to Mitigate Information Security Insider Threats in Organisations," Future Generation Computer Systems, Vol. 97, pp. 587-597, 2019.
DOI: https://doi.org/10.1016/j.future.2019.03.024

[18] J. Choi, M. Che, "An empirical study on the relationship of personal optimistic bias and information security awareness and behavior in the activity of information ethics," Journal of the Korea Academia-Industrial Cooperation Society, Vol. 17, No. 5, pp. 538-547, 2016.
DOI: http://dx.doi.org/10.5762/KAIS.2016.17.5.538

[19] R. Ayyagari, V. Grover, R. Purvis, "Technostress: Technological Antecedents and Implications," MIS Quarterly, Vol. 35, No. 4, pp. 831-858, 2011.
DOI: https://doi.org/10.2307/41409963

[20] C. Brod, "Managing Technostress: Optimizing the Use of Computer Technology," Personnel Journal, Vol. 61, No. 10, pp. 753-757, 1982.

[21] T. S. Ragu-Nathan, M. Tarafdar, B. S. Ragu-Nathan, Q. Tu, "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation," Information Systems Research, Vol. 19, No. 4, pp. 417-433, 2008.
DOI: https://doi.org/10.1287/isre.1070.0165

[22] A. M. Fuglseth, Ø. Sørebø, "The Effects of Technostress within the Context of Employee Use of ICT," Computers in Human Behavior, Vol. 40, pp. 161-170, 2014.
DOI: https://doi.org/10.1016/j.chb.2014.07.040

[23] R. H. Moorman. "Relationship between Organizational Justice and Organizational Citizenship Behaviors: Do Fairness Perceptions Influence Employee Citizenship?," Journal of Applied Psychology, Vol. 76, No. 6, pp. 845-855, 1991.

[24] J. A. Colquitt. "On the Dimensionality of Organizational Justice: A Construct Validation of a Measure," Journal of Applied Psychology, Vol. 86, No. 3, pp. 386-400, 2001.

[25] J. S. Adams, Inequity in Social Exchange, In Advances in experimental social psychology (Vol. 2, pp. 267-299). Academic Press, 1965.

[26] C. B. Meyer, "Allocation Processes in Mergers and Acquisitions: An Organizational Justice Perspective," British Journal of Management, Vol. 12, No. 1, pp. 47-66, 2001.
DOI : https://doi.org/10.1111/1467-8551.00185

[27] T. A. Judge, J. A. Colquitt, "Organizational Justice and Stress: The Mediating Role of Work-family Conflict," Journal of Applied Psychology, Vol. 89, No. 3, pp. 395-404, 2004.
DOI: https://doi.org/10.1037/0021-9010.89.3.395

[28] M. L. Ambrose, M. Schminke, "The Role of Overall Justice Judgments in Organizational Justice Research: A Test of Mediation," Journal of Applied Psychology, Vol. 94, No. 2, pp. 491-500, 2009.
DOI : https://doi.org/10.1037/a0013203

[29] J. Cho, J. Yoo, J. Lim, "An Impact Analysis of Information Security Professional's Job Stress and Job Satisfaction to Turnover Intention: Moderation of Organizational Justice," Journal of Society for e-Business Studies, Vol. 24, No. 3, pp. 143-161, 2019.
DOI: https://doi.org/10.7838/jsebs.2019.24.3.143

[30] H. Li, R. Sarathy, J. Zhang, X. Luo, "Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance," Information Systems Journal, Vol. 24, No. 6, pp. 479-502, 2014.

DOI : https://doi.org/10.1111/isj.12037

[31] R. C. Mayer, J. H. Davis, F. D. Schoorman, "An Integrative Model of Organizational Trust," Academy of Management Review, Vol. 20, No. 3, pp. 709-734, 1995.
DOI : https://doi.org/10.5465/amr.1995.9508080335

[32] V. Agarwal, "Investigating the Convergent Validity of Organizational Trust," Journal of Communication Management, Vol. 17, No. 1, pp. 24-39, 2013.
DOI : https://doi.org/10.1108/13632541311300133

[33] N. Gillespie, G. Dietz, "Trust Repair After an Organization-Level Failure," Academy of Management Review, Vol. 34, No. 1, pp. 127-145, 2009.
DOI: https://doi.org/10.5465/amr.2009.35713319

[34] H. H. Tan, C. S. Tan, "Toward the Differentiation of Trust in Supervisor and Trust in Organization," Genetic, Social, and General Psychology Monographs, Vol. 126, No. 2, pp. 241-260, 2000.

[35] Y. Xie, S. Peng, "How to Repair Customer Trust after Negative Publicity: The Roles of Competence, Integrity, Benevolence, and Forgiveness," Psychology & Marketing, Vol. 26, No. 7, pp. 572-589, 2009.
DOI : https://doi.org/10.1002/mar.20289

[35] P. B. Lowry, C. Posey, R. B. J. Bennett, T. L. Roberts, "Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust," Information Systems Journal, Vol. 25, No. 3, pp. 193-273, 2015.
DOI: https://doi.org/10.1111/isj.12063

[36] Y. Xue, H. Liang, and L. Wu, "Punishment, Justice, and Compliance in Mandatory IT Settings," Information Systems Research, Vol. 22, No. 2, pp. 400-414, 2011.
DOI : https://doi.org/10.1287/isre.1090.0266

[37] A. Tziner, G. Sharoni, "Organizational Citizenship Behavior, Organizational Justice, Job Stress, and Workfamily Conflict: Examination of their Interrelationships with Respondents from a non-Western Culture," Revista de Psicología del Trabajo y de las Organizaciones, Vol. 30, No. 1, pp. 35-42, 2014.
DOI : https://doi.org/10.5093/tr2014a5

[38] I. Hwang, S. Ahn, "The Effect of Organizational Justice on Information Security-Related Role Stress and Negative Behaviors," Journal of The Korea Society of Computer and Information, Vol. 24, No. 11, pp. 87-98, 2019.
DOI: https://doi.org/10.9708/jksci.2019.24.11.087

[39] Y. T. Wong, H. Y. Ngo, C. S. Wong, "Perceived Organizational Justice, Trust, and OCB: A Study of Chinese Workers in Joint Ventures and State-owned Enterprises," Journal of World Business, Vol. 41, No. 4, pp. 344-355, 2006.
DOI : https://doi.org/10.1016/j.jwb.2006.08.003

[40] D. L. Seifert, W. W. Stammerjohan, R. B. Martin, "Trust, Organizational Justice, and Whistleblowing: A Research Note," Behavioral Research in Accounting, Vol. 26, No. 1, pp. 157-168, 2014.
DOI : https://doi.org/10.2308/bria-50587

[41] H. Zeinabadi, K. Salehi, "Role of Procedural Justice, Trust, Job Satisfaction, and Organizational Commitment in Organizational Citizenship Behavior (OCB) of Teachers: Proposing a Modified Social Exchange Model," Procedia-Social and Behavioral Sciences, Vol. 29, pp. 1472-1481, 2011.
DOI : https://doi.org/10.1016/j.sbspro.2011.11.387

[42] I. Hwang. "A Study on Mitigation of Information Security Related Work Stress," Journal of Convergence for Information Technology, Vol. 10, No. 9. pp. 123-135, 2020.

[43] M. Top, M. Akdere, M. Tarcan, "Examining Transformational Leadership, Job Satisfaction, Organizational Commitment and Organizational Trust in Turkish Hospitals: Public Servants Versus Private Sector Employees," The International Journal of Human Resource Management, Vol. 26, No. 9, pp. 1259-1282, 2015.
DOI : https://doi.org/10.1080/09585192.2014.939987

[44] M. A. Krosgaard, S. E. Brodt, E. M. Whitener, "Trust in the Face of Conflict: The Role of Managerial Trustworthy Behavior and Organizational Context," Journal of Applied Psychology, Vol. 87, No. 2, pp. 312–319.
DOI : https://doi.org/10.1037/0021-9010.87.2.312

[45] J. Guinot, R. Chiva, V. Roca-Puig, "Interpersonal Trust, Stress and Satisfaction at Work: An Empirical Study. Personnel Review," Vol. 43, No. 1, pp. 96-115, 2014. DOI : https://doi.org/10.1108/PR-02-2012-0043

[46] M. Top, S. Tekingunduz, "The Effect of Organizational Justice and Trust on Job Stress in Hospital Organizations," Journal of Nursing Scholarship, Vol. 50, No. 5, pp. 558-566, 2018.
DOI : https://doi.org/10.1111/jnu.12419

[47] J. C. Nunnally, "Psychometric Theory (2nd ed.)," New York: McGraw-Hill, 1978.

[48] B. H. Wixom, H. J. Watson, "An Empirical Investigation of the Factors Affecting Data Warehousing Success," MIS Quarterly, Vol. 25, No. 1, pp. 17-41, 2001.
DOI : https://doi.org/10.2307/3250957

[49] C. Fornell, D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," Journal of Marketing Research, Vol. 18, No. 1, pp. 39-50, 1981.
DOI: https://doi.org/10.2307/3151312

[50] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee, N. P. Podsakoff, "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies," Journal of Applied Psychology, Vol. 88, No. 5, pp. 879-903, 2003.

DOI : https://doi.org/10.1037/0021-9010.88.5.879

[51] G. C. Lin, Z. Wen, H. W. Marsh, H. S. Lin, "Structural Equation Models of Latent Interactions: Clarification of Orthogonalizing and Double-mean-centering Strategies," Structural Equation Modeling, Vol. 17, No. 3, pp. 374-391, 2010.
DOI : https://doi.org/10.1080/10705511.2010.488999

황 인 호(Inho Hwang) [종신회원]

- 2004년 8월 : 건국대학교 경영학과(경영학사)
- 2007년 6월 : 중앙대학교 경영학과(경영학석사)
- 2014년 2월 : 중앙대학교 경영학과(경영학박사)
- 2020년 9월 ~ 현재 : 국민대학교 교양대학 조교수

〈관심분야〉
IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야 등