JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 22, No. 5, pp. 855-866, May. 2021

정보보안 조직 불공정성이 정보보안 걱정 및 기피 행동에 미치는 영향: 피해자 공정 민감성의 조절 효과 분석

황 인 호[1]
[1]국민대학교 교양대학 조교수

The Effects of Information Security Organizational Injustice on Information Security Anxiety and Avoidance Behavior: Focusing on Moderation Effects of Victim Justice Sensitivity

Inho Hwang[1]
[1]Assistant Professor, College of General Education, Kookmin University, Seoul 02707, Korea

[요 약]

최근, 온라인 기반 업무가 다양해지면서, 조직들은 정보 관리를 엄격하게 할 필요성이 높아지고 있다. 특히, 내부자의 정보보안 활동에 대한 관리가 더욱 어려워지면서, 조직은 구성원의 미준수 행동을 통제할 필요성이 커지고 있다. 따라서, 본 연구는 조직원의 정보보안 기피 행동의 원인을 확인하고자 한다. 본 연구는 정보보안을 업무에 적용하는 근로자들을 대상으로 하였으며, 연구가설 검증은 설문을 통해 확보한 표본을 구조방정식모델링을 적용하여 실시하였다. 연구 결과, 정보보안 유형별 불공정성이 개인의 보안 준수 걱정을 높였으며, 보안 준수 걱정이 기피 행동에 영향을 미쳤다. 또한, 피해자 공정 민감성이 높은 집단이 낮은 집단보다 각 불공정성의 걱정에 미치는 부정적 영향을 강화하였다. 본 연구는 개인의 부정적 보안 행동에 영향을 주는 원인을 조직, 개인 차원에서 제시하였다는 측면에서 학술적, 실무적 시사점을 가진다.

[Abstract]

With the recent diversification of online-based work, organizations are increasingly required to strictly manage information. In particular, as it becomes more difficult to manage information security activities of insiders, the need for organizations to control the non-compliance behavior of employees is increasing. This study aims to present the causes of the information security avoidance behavior of employees. The study targets workers who apply information security to their work and hypothesis verification was conducted by applying structural equation modeling to samples obtained through questionnaires. As a result, information security injustice increased the avoidance behavior by compliance anxiety. Also, the victim justices sensitivity moderate the relationship between injustice and anxiety. The study has implications in terms of presenting the causes that affect negative security behavior at the organizational and individual levels.

색인어 : 정보보안, 기피 행동, 준수 걱정, 조직 불공정성, 피해자 공정 민감성
Key word : Information Security, Avoidance Behavior, Compliance Anxiety, Organizational Injustice, Victim Justice Sensitivity

http://dx.doi.org/10.9728/dcs.2021.22.5.855

Received 15 April 2021; **Revised** 10 May2021
Accepted 10 May2021

***Corresponding Author; Inho Hwang**

Tel: +82-02-910-6473
E-mail: hwanginho@kookmin.ac.kr

Ⅰ. 서 론

정보 자산이 조직의 중요한 가치로 인식되면서, 조직들은 조직의 정보를 체계적으로 관리하고 보호하기 위한 노력을 하고 있다[1]. 예를 들어, 정보보안 관련 국제 표준 인증 확보 및 정보보호 관리 법률 대처 차원의 정보보호관리 체계 인증과 같은 체계 구축 제도를 활용하거나, 자체적인 정보보안 정책 도입 또는 기술 적용을 통해 보안 체계 구축 노력을 하고 있다.

그럼에도 불구하고, 조직 정보보안 사고는 계속 발생하고 있다. 정보보안 사고의 특성상 해당 사고 발생 시 조직의 가치를 감소시키는 요인으로 인식되고 있어 문제를 숨기고자 하는 경향이 높다. 하지만, 세계적으로 보안 사고는 꾸준히 발생하고 있다[2]. 정보보안 사고들은 매년 유사한 빈도로 나타나는데, 외부의 기술적 침입(해킹, 피싱, 멀웨어 등)을 통한 정보 약탈 사고가 약 60~70% 수준이며, 조직 내부자(구성원 또는 파트너사)에 의한 정보 노출 사고가 약 20~30% 수준에서 발생하는 것으로 파악된다[2]. 일찍이 정보보안 대처 방안을 연구한 Loch et al.[1992]은 정보보안 사고는 유형별 맞춤형 접근이 필요하다고 보았다[3]. 즉, 외부의 기술적 침입을 통한 정보 약탈은 방화벽, 보안이 강화된 클라우드 시스템과 같은 최신의 보안 기술을 적용하여 대처할 수 있으나, 조직 내부의 사람에 의한 정보 노출 사고는 대부분 악의적이지 않은 정보 오·남용에 의해 발생하기 때문에 개인 차원에서는 정보 관리에 대한 의식을 꾸준히 가지고 있어야 하며, 조직 차원에서는 구성원이 보안 활동을 업무에 적용할 수 있도록 행동 기반의 예방 정책 및 대처 방안을 마련하는 것이 필요하다고 보고 있다[3].

실제로, 많은 정보보안 관련 선행연구들은 사람에 의한 정보 노출 사고 예방을 위한 조직의 대처는 구성원의 정보보안 준수 행동을 위한 동기 형성에 초점을 맞추어야 한다고 본다. 대표적으로, 범죄학, 사회학, 심리학 등에서 개인과 집단간의 관계에서 개인의 행동 방안을 예측한 이론들인 일반제재이론(general deterrence theory), 중화이론(neutralization theory), 동기이론(motivation theory), 계획된 행동이론(theory of planned behavior) 등을 유기적으로 적용하여, 조직 내 상황 및 특성별 구성원의 정보보안 행동 원인에 대한 측면과 조직의 대처 방향을 제시한 결과들이 다수 제시되었다[4-10]. 선행 연구들은 개인을 둘러싼 정보보안 환경 측면과 개인의 행동 사이에는 행동 원인을 결정할 단서가 있으며, 조직이 맞춤형으로 제시할 때 긍정적인 행동 의지를 보인다는 것을 제시한 측면에서 높은 시사점을 가진다.

최근에는 엄격하고 지키기 어려운 수준의 정보보안 정책 및 기술의 도입이 오히려 구성원들의 행동을 부정적으로 만든다는 연구가 제시되고 있다. 대표적으로 조직에서 개인이 보유한 역량을 초과한 상태가 유지될 때 발생하는 스트레스를 정보보안 분야에 접목하여, 구성원의 정보보안 관련 스트레스 발생 가능성을 최소화해야 한다는 관점을 제시한 연구 결과가 조금씩 나오고 있다[11,12]. 정보보안 분야에 스트레스를 적용한 연구들은 기술스트레스 이론(techno-stress theory), 스트레스 대처 이론(stress-coping theory)을 정보보안 분야에 탐색적으로 적용하여, 어떠한 정보보안 요구 상황이 개인의 정보보안 미준수행동에 영향을 주는지를 확인했다는 측면에서 높은 시사점을 가진다[13-15]. 하지만, 아직까지 관련 선행연구들은 탐색적 관점에서 대부분 접근되어, 정보보안 관련 다양한 스트레스 원인과 이를 개선하기 위한 방향을 제시한 연구는 부족한 상황이다.

본 연구는 정보보안 정책을 업무에 적용하는 조직원의 관점에서 관련 행동을 기피하게 만드는 스트레스 세부요인인 정보보안 준수 걱정 요인을 제시하고 걱정을 높이는 조직의 정보보안 환경을 검토하고자 한다. 세부적으로, 조직 공정성 이론을 정보보안 분야에 적용하되, 대표적인 부정적 원인인 불공정성 세부 요인들이 정보보안 준수 걱정을 통해 정보보안 기피행동으로 이어지는 매커니즘을 확인하고자 한다. 또한, 불공정성과 걱정간의 관계에 있어 개인의 공정 민감성 수준이 어떻게 악화시키는지를 추가적으로 확인함으로써, 조직이 접근해야 할 정보보안 공정성 대처 방향을 제시하고자 한다.

Ⅱ. 이론적 배경

2-1 정보보안 기피 행동

세계적인 코로나 19사태는 우리 사회의 운영 형태를 급속도로 변화시키고 있다. 해당 바이러스 사태는 사회 구성원인 사람들간의 만남을 최소화하길 요구하고 있으며, 많은 조직들은 반강제로 조직 구성원의 재택근무 또는 온라인 미팅 등을 통해 어려움을 대처하고 있다. 하지만, 온라인 기반의 정보 기술 사용 확대는 정보에 대한 접근 방식을 다양화시켜 정보 노출 위협을 높일 수 있다. 실제로 정보보안 사고를 일으킨 내부자는 IT 부서 전문가 이외에 일반 사무직, 엔지니어, 영업직 등 세부 기술을 잘 모르더라도 정보시스템에 접근이 가능한 사람들로 구성된 것으로 나타났다[2]. 따라서, 조직이 내부 정보보안 수준을 꾸준히 유지하기 위해서는 악의적이지 않더라도 발생 가능한, 조직이 구축한 정보보안 정책에 대한 조직원들의 미준수 행동을 최소화하는 것이 필요하다[16,17]. 악의적이지는 않으나, 귀찮거나 자신과 맞지 않는 등 다양한 이유에서 조직이 요구하는 정보보안을 기피 하는 행동을 기피 행동이라 한다.

즉, 정보보안 기피 행동(avoid behavior)은 조직이 구축한 정보보안 정책, 규정, 기술 등을 통해 개인에게 부여된 요구사항을 민감한 환경 등의 이유로 기피 하는 행동을 말한다[9]. 즉, 기피 행동은 조직이 요구하는 특정 활동에 대하여 자신에게 불편하거나 민감한 상황이 발생했을 때, 그리고 타인이 해당 상황을 잘 인식하지 못할 때, 해당 상황을 기피 하는 것을 지칭한다[5]. 특히 정보보안은 개인에게 부여된 1차 업무적 성과 및 목표가 아니라, 업무 외 추가적 요구사항에 가까우므로, 조직원들은 자신의 업무 목표 달성에 정보보안이 피해를 발생시킨다고 판단할 때, 기피 하는 경향을 보인다. 따라서, 조직은 개인의 기피 행동을 최소화하는 것이 필요하며, 본 연구는 기피 행동을 높이는 선행요인을 제시하고 시사점을 제시하고자 한다.

2-2 정보보안 준수 걱정

조직원들은 조직의 특정 기술 도입이나 과도한 업무적 요구사항이 자신의 역량 수준을 넘어선다고 판단할 때 스트레스를 일으킨다[18]. 즉, 조직 내 구성원들의 스트레스 관련 선행 연구들은 개인의 기존 업무에 추가적인 활동을 요구함으로써 개인과 개인을 둘러싼 환경간의 균형이 깨지게 될 때, 스트레스가 발생할 가능성이 높다고 본다[12,19]. 해당 환경은 정보보안과 같은 정보 기술일 수 있고, 추가적인 업무일 수도 있다. Tarafdar et al.[2007]은 조직의 정보시스템 도입은 개인의 기술 관련 스트레스와 업무 스트레스를 높일 수 있다고 보았는데, 도입하는 기술 자체의 특성(복잡성, 불확실성 등)에 의해서도 스트레스가 발생가능하고, 새로운 기술 표준을 업무에 적용 시 개인은 반발감을 가지거나, 기존 업무와의 갈등을 발생시켜 스트레스를 일으킬 수 있다고 보았다[11]. 이와 같은 스트레스가 지속적으로 발현되면, 개인의 심리적 문제(걱정, 두려움)가 발생하거나, 육체적 문제(피로)가 나타나기도 하고, 나아가서는 조직의 업무 성과에 부정적 영향을 미친다[20-22].

조직 내 스트레스는 다양한 형태로 나타나는데, Salanova et al.[2013]은 기술 도입으로 인한 스트레스는 걱정, 피로, 무력감 등으로 발생하여 개인의 행동에 부정적인 영향을 미친다고 하였으며[23], Jena[2015]는 기술 스트레스로 인하여 걱정 등을 통합한 부정적 정서가 나타난다고 하였다[24]. 걱정(anxiety)은 정보 기술의 적용에 있어, 해당 기술을 명확하게 파악하지 못함으로 인해 발현되는 사용자의 두려움 또는 염려의 수준을 의미한다[23]. 즉, 걱정은 특정 행동에 대한 정보 또는 경험이 부족한 상황에서 행동으로 옮겨야 할 때 발생하는 심리적 부담감으로서, 걱정이 높아지면 두려움 또는 염려 수준이 커져 오히려 해당 행동을 기피하려는 속성을 보인다.

정보보안 관점에서 걱정은 기존 업무 또는 기술보다 더욱 잘 발생할 수 있는데, 조직은 지속적인 외부의 침입 등을 방지하기 위하여, 높은 수준의 보안 정책 또는 기술을 지속적으로 도입하고 구성원들에게 적용을 요구할 수 밖에 없으며, 이와 같은 상황이 지속적 발생 시 구성원들은 자신의 역량 수준을 넘어선 보안 관련 활동에 어려움을 느낄 가능성이 높다[18]. 즉, 정보보안 준수 걱정(information security compliance anxiety)은 조직이 도입한 정보보안 정책 또는 기술에 대한 적용이 어렵거나, 조직의 정보보안 정책과 다른 상황에 직면하는 등의 새로운 적용 상황이 발생할 때 발생할 수 있다.

걱정은 조직과 관련된 행동 측면에서 부정적 영향을 주는 선행 조건이다. Salanova et al.[2013]은 기술 스트레스 요인인 걱정, 피로, 무력감은 개인의 육체적 문제뿐만 아니라, 조직이 요구하는 업무 달성에 문제를 일으킬 수 있다고 하였으며, 기술 사용성을 높이는 것이 걱정을 최소화시킬 수 있음을 확인하였다[23]. 특히, 정보보안 준수 관련 걱정의 형성은 조직이 요구하는 정보보안 관련 행동을 따르지 않거나 기피하는 원인이 된다. 걱정이 형성되는 이유는 정보보안 관련 행동 방식과 예상 결과에 대한 정확한 정보가 부족하거나 경험이 부재할 때 발생하는데, 이때, 당사자는 관련 행동을 기피 하게 된다. Hwang et al.[2017]은 정보보안 준수의도에 걱정이 부정적인 영향을 미치는 것을 확인하였다. 그들은 걱정을 완화하기 위해서는 정보보안 활동에 대한 지식 확보를 위한 정책, 기술, 홍보 등의 지원이 필요하다고 보았다[18]. 즉, 구성원의 정보보안 준수에 대한 걱정의 발현은 조직이 요구하는 보안 행동을 기피 하는 원인이 될 수 있으므로, 연구는 정보보안 걱정과 기피 행동간의 관계를 확인하고자 한다.

H1 : 정보보안 관련 준수 걱정은 정보보안 기피 행동에 정(+)의 영향을 미칠 것이다.

2-3 정보보안 조직 불공정성

조직 공정성 이론(organization justice theory)은 집단과 개인 즉, 이해관계자 간의 공정한 관계가 상호 간 요구 행동에 긍정적 반응을 일으킨다는 관점이다[25]. 해당 이론의 기본적인 가정은 사람들은 상호 간의 관계 설정에 있어 공정한 상황 및 관계를 중요시 여기며, 공정성을 확보하기 위하여 노력하고, 확보된 공정성을 유지하기 위하여 상대방과 일체화한다는 것이다[26]. 또한, 조직 공정성에 대한 평가는 상대적 비교를 통해 이루어지는데, 개인이 조직에서 올바른 평가 및 대우를 받았다고 평가하는 것은 자신과 유사한 상황의 타인에 대한 조직의 대처와 비교를 통해 공정에 대한 적정성을 유추 및 판단한다[27]. 즉, 조직이 공정하다는 인식은 구성원 간에 개별적이고 상대적으로 평등하게 대우를 받았는지를 판단하는 것으로 나타나고, 형성된 공정성은 당사자로 하여 현재까지 받은 대우 또는 경험 등에 대한 손실을 발생시키지 않기 위하여 조직이 요구하는 행동 및 목표 등을 수행하도록 돕는 조건이 된다[28].

역으로, 조직 불공정성(organization injustice)은 조직이 개인에게 공평하게 대우하고 있지 않다고 판단하는 수준을 의미한다[26]. 즉, 조직원 본인에 대한 조직의 지원이 조직이 요구하는 행동 및 성과 목표보다 부족하거나, 행동 과정 등에서 주변 사람과 비교해서 상대적으로 피해를 받거나 부족하게 대우받는다고 판단할 때, 조직에 대한 불공정성이 형성된다. 개인이 조직으로부터 불공정한 대우를 받고 있다고 판단할 때, 개인은 부정적 감정을 가지게 되고 조직의 요구사항과 다른 행동으로 이어지는 경향을 보인다[29].

개인의 조직에 대한 불공정성 판단은 조직 내 개인의 특정 활동을 위해 필요한 정보 확보, 활동 과정, 그리고 성과에 대한 배분 과정마다 발생할 수 있다. 즉, 조직 불공정성은 분배 불공정성, 과정 불공정성, 그리고 정보 불공정성이 있다[26].

분배 불공정성(distributive injustice)은 조직 내 개인의 행동 결과에 대한 평가 또는 분배가 불평등하다고 판단하는 수준으로 정의된다[30]. 사람들은 결과에 대한 분배는 상황적 특성에 따라 형평(equity), 평등(equality) 등 차별적으로 적용하는데, 상황적 특성을 감내하더라도 조직 내 행동 결과의 평가 및 결과 배분이 상대적으로 불합리하다고 판단할 경우 분배 불공정성

이 발현된다. 정보보안 관점에서 분배의 공정성은 개인이 올바르게 대우받고 있다고 판단하는 중요한 기준이 된다[31]. 조직은 구성원의 준수 행동의 결과 정보를 정확하게 확인하고 판단할 수 없으므로, 손쉬운 방법으로 미준수 행동에 대한 처벌, 제재 관점으로 결과를 이해하려는 경향을 보인다[32]. 만일, 특정 조직의 미준수 행동에 대한 처벌 관점의 정보보안에 대한 분배가 적절하지 않다는 것은 구성원들의 미준수 행동 결과에 대한 처벌이 상대적으로 불합리하다는 것을 의미하기 때문에, 높은 수준의 반발심을 일으킬 가능성이 높다.

절차 불공정성(procedural injustice)은 조직 내 행동 결과를 확보하는데 필요한 절차가 불공정하다고 판단하는 수준으로 정의된다[29]. 절차는 특정 활동에 대한 의사결정 과정 시 적용하는 정책, 규정, 그리고 과정에 대한 참여 수준이 적절한지에 대한 평가로서, 해당 과정이 불공정하여 자신이 결과를 명확하게 얻을 수 없다고 판단할 때 절차 불공정성이 발현된다[26]. 정보보안 관점에서 절차의 공정성은 개인에게 공정한 대우를 하고 있다고 판단하는 중요한 기준이 된다. 조직이 도입하는 정보보안 정책, 규정, 기술 등은 심리적인 측면에서 기술적 측면까지 개인이 조직에서 수행하는 활동 전반을 제어하는 것을 의미한다[31]. 만일 개인이 타인과 비교하여 자신이 정보보안 정책 등 필요 의사결정 절차 또는 참여가 불공평하여, 자신이 홀대받는다고 판단할 경우 불공정함을 인식할 가능성이 크다.

정보 불공정성(informational injustice)은 특정 활동에 대한 절차 및 결과 등에 대한 사전 정보 및 지식을 제공하는 수준이 불공정하다고 판단하는 수준이다[26]. 개인이 자신의 활동에 대한 성과를 확보하기 위해서는 해당 활동에 대한 경험 또는 지식을 보유하는 것이 필요하며, 결과에 대한 평가가 어떻게 이루어지는지 등 행동 수행 전반에 대한 정보가 필요하다[28]. 정보가 불공정하다는 것은 타인과 비교해서 적절한 행동을 할 수 없음을 의미하고 필연적으로 성과가 뒤처지게 된다는 것을 의미하기 때문에, 높은 수준의 불합리성을 경험하게 된다. 정보보안 관점에서 정보 공정성은 조직으로부터 개인이 적절히 대우를 받고 있는지에 대한 인식 기준이 된다[31]. 만일, 개인이 조직의 정보보안 정책, 규정 등에 대한 행동 정보를 명확하게 인식하지 못할 경우, 보안 미준수 행동으로 나타날 가능성이 커지기 때문에 조직원은 심리적, 경제적 피해를 받을 가능성이 있다. 즉, 정보보안 필요 정보를 상대적으로 적절히 확보하지 못하고 있다고 판단할 경우 불공정함을 인식할 가능성이 있다.

개인이 조직의 행동이 자신에게 불공정하다고 판단할 경우, 걱정과 같은 스트레스를 발현시켜 심리적, 육체적 문제를 일으키거나, 조직이 요구하는 특정 행동에 대하여 반하는 행동을 할 가능성이 높다. Khan et al.[2013]은 개인에 대한 조직의 불공정한 상황을 분배 불공정성과 절차 불공정성으로 구분하였으며, 각 불공정한 상황이 발생할 경우, 슬픔 또는 화남과 같은 스트레스를 발현시키고, 조직의 요구 업무적 행동을 미준수하는 것을 확인하였다[33]. Hystad et al.[2014]은 분배, 절차, 상호작용, 그리고 정보 불공정성으로 형성된 전체적인 조직 불공정성은 개인의 도덕적 일탈을 높이고 미준수 행동으로 이어짐을 확인하였다[26]. 또한, Johnson et al.[2010]은 공평(fair)의 관점에서 공정성을 측정하였는데, 불공평은 걱정을 높이고 공평은 행복을 높이는 관계에 있음을 확인하였으며[34], Rafferty et al.[2010]은 상급자의 불공정함은 개인의 심리적 스트레스를 일으켜 불면증에 영향을 주는 것을 확인하였다[30]. 정보보안 분야에서도 조직 공정성은 업무 스트레스를 감소시키는 원인이다. Hwang and Ahn[2019]은 조직 공정성이 업무 갈등 및 업무 모호성을 완화하여 준수행동을 높이는 선행 조건임을 확인하였다[35]. 즉, 정보보안 분배, 절차, 그리고 정보 불공정성이 높아지면 개인이 정보보안을 업무에 적용 시 걱정을 높일 수 있으므로, 연구는 정보보안 불공정성과 정보보안 준수 걱정 간의 영향 관계를 확인하고자 한다.

H2 : 정보보안 분배 불공정성은 정보보안 준수 걱정에 정(+)의 영향을 미칠 것이다.

H3 : 정보보안 절차 불공정성은 정보보안 준수 걱정에 정(+)의 영향을 미칠 것이다.

H4 : 정보보안 정보 불공정성은 정보보안 준수 걱정에 정(+)의 영향을 미칠 것이다.

2-4 공정 민감성

조직 공정성은 조직의 본인에 대한 대우에 대한 공평성에 대한 인식의 수준으로서, 특정 행동에 대해 주변 유사한 상황과 상대적으로 비교하여 사전 정보제공의 공정함, 행동 절차의 참여 및 의사결정 과정의 공정함, 그리고 결과에 대한 평가에 대한 공정함이 복합적으로 인식될 때 개인 차원의 직업 만족을 높이거나 업무 스트레스를 감소시키는 역할을 한다.

조직 공정성 판단은 조직에 소속된 구성원이 하는 것이기 때문에, 구성원의 성향에 따라 같은 상황이라도 공정성에 대한 다른 판단이 가능하다[36]. 즉, 사람마다 공정성에 대한 민감성이 다르므로, 조직에 대한 공정성 평가가 상이 할 수 있다.

공정 민감성(justice sensitivity)은 조직의 공정 또는 불공정한 상황에 대해 깊게 반응하는 수준으로서[37], 관점에 따라 다른 공정 민감성을 제시하고 있다. Liu and Berry[2013]는 공평 민감성(equity sensitivity)의 단일 요인을 제시하였으며[36], Schmitt et al.[2005]와 Gollwizer et al.[2009]은 공정 민감성을 피해자 관점(victim), 관찰자 관점(observer), 그리고 가해자 관점(perpetrator)으로 구분하여 제시하였다[37,38].

본 연구는 탐색적 관점에서 Schmitt et al.[2005]의 피해자 공정 민감성(victim justice sensitivity)을 적용한다. Schmitt et al.[2005]이 제시한 공정 민감성 중 피해자 관점은 본인이 조직으로부터 피해를 받는 상황에 대한 민감한 수준을 의미하고, 관찰자 관점은 타인이 조직으로부터 피해를 받는 상황에 대한 민감한 수준을 의미하며, 가해자 관점은 본인이 조직으로부터 월등히 혜택을 받는 상황에 민감한 수준을 의미한다[37]. 정보보안은 준수에 대한 성과의 개념이 아닌 미준수에 대한 피해의 개념으로 접근하며, 업무에 추가적인 보안 활동을 적용시키는 것을 중점적으로 고려하기 때문에, 자신 또는 타인의 보안 관련

행동을 명확하게 알 수 없는 경우가 많다. 따라서, 민감성 중 관찰자 또는 가해자 민감성 보다, 자신이 피해를 받는 상황에 대한 민감성이 정보보안 분야에 더욱 적절할 것으로 판단한다.

특히, 공정 민감성은 불공정한 상황이 발생할 때, 조직에 대한 부정적 감정을 가지거나, 조직이 요구하는 활동과 반대되는 행동을 하도록 한다. Gollwitzer et al.[2009]은 조직의 불공정한 상황이 존재할 때, 공정 민감성은 더욱 크게 반응하여 의심적인 마인드 셋을 가지도록 하여, 공유 행동을 하지 않도록 한다고 하였으며[38], Schmitt et al.[2005]은 공정 민감성이 높을수록 불공정한 환경에 크게 반응하여 부정적 정서를 가지고, 업무에 영향을 준다고 하였다[37]. 또한, Liu and Berry[2013]는 조직 전반의 불공정성 상황이 조직일체감에 미치는 부정적 영향을 공평 민감성이 강화하는 것을 확인하였다[36]. 즉, 정보보안 관점에서 피해자 공정 민감성은 불공정성의 부정적 영향을 높일 것으로 판단하며, 분배, 절차, 그리고 정보 공정성이 정보보안 걱정을 높이는 과정에서 더욱 민감하게 반응할 것으로 판단하고 연구가설을 제시한다.

H5a : 피해자 공정 민감성은 정보보안 분배 불공정성과 정보보안 준수 걱정 간의 관계를 조절할 것이다.

H5b : 피해자 공정 민감성은 정보보안 절차 불공정성과 정보보안 준수 걱정 간의 관계를 조절할 것이다.

H5c : 피해자 공정 민감성은 정보보안 정보 불공정성과 정보보안 준수 걱정 간의 관계를 조절할 것이다.

Ⅲ. 연구 모델 및 방법

3-1 연구모델

본 연구는 조직의 정보보안 관련 유형별 불공정성이 개인의 정보보안 준수에 미치는 부정적인 측면을 확인하고, 공정 민감성에 의해 불공정한 상황이 증폭될 수 있음을 제시하는 것을 확인함으로써, 내부의 정보보안 관련 행동 향상을 위한 방향을 제시하는 것을 목적을 가지며, 선행연구를 기반으로 연구 모델을 제시한다(그림 1).

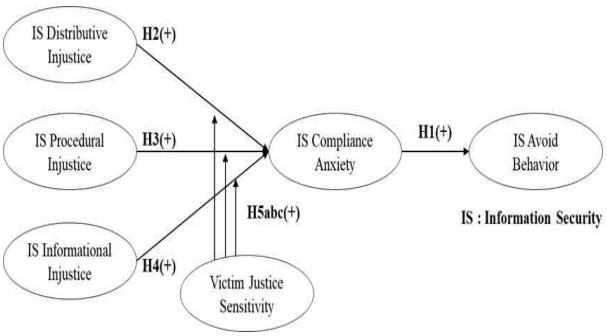

그림 1. 연구 모델
Fig. 1. Research Model

3-2 데이터 측정 및 수집

본 연구는 조직 내부의 정보보안 행동의 변화 요인을 설문방식으로 측정하고 데이터를 확보함으로써, 연구가설을 확인하고자 한다. 이에, 연구 대상은 정보보안 정책 및 규정을 적용하고 있는 기업의 근로자들을 대상으로 한다. 특히, 자신의 업무에 정보보안 행동 요구사항을 적용해야 하는 일반 근로자들을 대상으로 한다.

또한, 설문지 개발은 요인별 선행연구에서 적용한 설문항목을 적용하고, 정보보안 분야에 맞춰 변경하였으며, 7점 등간 척도로 구성하였다. 정보보안 불공정성은 Hystad et al.[2014]의 연구를 기반으로 분배 불공정성, 절차 불공정성, 정보 불공정성의 항목을 활용하되[26], 정보보안 특성에 맞게 재구성하였다. 정보보안 분배 불공정성은 정보보안의 결과의 불공정한 수준으로 정의하며, “정보보안 행동은 업무적 결과에 잘 반영되지 않음”, “정보보안 행동은 보안 관련 업무를 실행하는데 적절하지 않음”, “정보보안 행동은 조직의 정보보안 성과에 기여하는 것으로 보이지 않음”과 같이 3개의 항목을 적용하였다. 정보보안 절차 불공정성은 정보보안 관련 의사결정 절차의 불공정한 수준으로 정의하며, “조직의 보안 절차는 나의 보안 행동에 영향을 잘 주지 않음”, “보안 절차는 일관되지 않게 적용됨”, “조직의 정보보안 절차는 편견 없이 적용되고 있지 않음”과 같이 3개의 항목을 적용하였다. 정보보안 정보 불공정성은 정보보안 관련 정보 제공이 불공정한 상황의 수준으로 정의하며, “정보보안과 관련된 커뮤니케이션이 부족함”, “조직은 정보보안 절차를 정확하게 설명하지 않음”, “조직은 정보보안 준수에 대한 사항들을 상세히 제공하지 못함”과 같이 3개의 항목을 적용하였다.

정보보안 준수 걱정은 조직의 정보보안을 적용에 대한 우려 수준으로 정의하며[18], “나는 정보보안을 적용하는 방법에 대하여 우려”, “나는 실수로 정보 노출을 할 수 있다고 생각”, “보안 적용 시 해결할 수 없는 실수가 있을 수 있음”과 같이 3개의 항목을 적용하였다.

정보보안 기피 행동은 보안 준수가 어려운 상황을 기피 하는 행동으로 정의하며[9], “보안 준수가 어려운 상황 시, 지켜야 할 정보보안 행동을 기피”, “보안 준수가 어려운 상황 시, 정책 준수 행동을 감소”, “보안 준수가 어려운 상황 시, 정보보안 정책에 대한 적용 빈도를 줄임”과 같이 3개의 항목을 적용하였다.

마지막으로, 희생자 공정 민감성은 당사자가 불공정한 상황에 대하여 민감하게 반응하는 수준으로 정의하며[37], “나는 다른 사람들이 내 것이어야 할 무엇인가를 가져갈 때, 신경이 쓰임”, “ 나는 다른 사람들이 나로부터 이익을 취할 때, 견딜 수 없음”, “나는 다른 사람들의 부주의로 발생한 부적절한 업무 결과를 해결해야 할 때, 오랜 시간 견딜 수 없음”, “나는 다른 사람들이 나보다 더 나아질 때 화가 남”, “나는 다른 사람들이 나보다 더 잘 대우받고 있을 때, 그 상황이 오랫동안 잊혀지지 않음”과 같이 5개의 항목을 적용하였다.

표 1. 표본의 인구통계학적 특성
Table 1. Demographic Characteristics of Samples

Demographic Categories		Frequency	%
Industry	Manufacture	55	17.0
	Service	268	83.0
Gender	Male	205	63.5
	Female	118	36.5
Age	Under 30	100.0	31.0%
	31 – 40	111	34.4%
	Over 40	112	34.7%
Job Position	Under Manager	105	32.5
	Manager	139	43.0
	Over Manager	79	24.5
Total		323	100.0

도출된 설문의 응답은 정보보안 정책을 업무에 적용하고 있는 일반직 근로자들을 대상으로 하므로, 본 연구는 대학에서 재직자 전형으로 경영학과에 다니는 학생들에게 설문을 배포하였다. 설문을 배포하기 전, 정보보안 정책을 보유한 조직에서 정보보안을 업무에 적용하고 있는 부분과 설문의 목적과 통계적 활용 방향에 대하여 인지를 시켰고, 정보보안에 대하여 모르거나, 통계적 활용에 거부감을 보인 사람들을 제외하고 설문을 시행하였다. 표본 323개를 가설 검증에 활용하였으며, 표본의 인구통계학적 특성은 표 1.과 같다.

Ⅳ. 가설 검증

4-1 신뢰성 및 타당성 분석

본 연구는 구조방정식 모델링을 적용하여, 요인간의 구조적 영향 관계를 확인하고자 한다. 이에, AMOS 22.0과 SPSS21.0 툴을 활용하여 설문 항목들이 요인으로서 의미가 있는지를 확인하며, 신뢰성 및 타당성 분석을 실시한다.

첫째, 신뢰성 분석은 요인이 다 항목으로 구성되어 있을 때, 척도의 일관성을 확인하는 것이다. 본 연구는 우선 베리맥스 기법을 적용한 탐색적 요인분석을 실시하였으며, 그룹핑 된 결과를 기반으로 크론바흐 알파값을 도출하였다. 선행연구는 크론바흐 알파에 대하여 0.7 이상을 요구한다[39]. 탐색적 요인분석 결과, 공정 민감성 항목 1개(JS5)를 제외한 6개 요인의 19개 항목의 요인 적재값이 가장 낮은 항목은 분배 불공정성의 0.642로 나타났으며, 크론바흐 알파가 가장 낮은 요인은 분배 불공정성으로 0.785로 나타났다(표 2).

둘째, 타당성 분석은 관측변수와 잠재변수를 활용한 요인의 항목들의 일관성과 요인 간의 차별성이 있는지를 확인하는 분석으로 확인적 요인분석을 적용한다. AMOS 22.0을 활용하여 도출된 확인적 요인분석 결과 모델의 적합성은 구조방정식 적합성 요구사항을 충족시켰다($\chi 2/df$ = 1.566, RMSEA = 0.042, GFI = 0.938, AGFI = 0.914, NFI = 0.948, CFI = 0.980). 이에 연구는 집중타당성 분석을 실시하였다.

표 2. 구성요인 타당성 및 신뢰성 결과
Table 2. Result for Construct Validity and Reliability

Constructs		Factor Loading	Cronbach's Alpha	CR	AVE
DIJ	DIJ1	0.825	0.785	0.753	0.505
	DIJ2	0.642			
	DIJ3	0.714			
PIJ	PIJ1	0.765	0.842	0.799	0.570
	PIJ2	0.771			
	PIJ3	0.814			
IIJ	IIJ1	0.811	0.875	0.833	0.625
	IIJ2	0.848			
	IIJ3	0.838			
CA	CA1	0.805	0.872	0.839	0.636
	CA2	0.833			
	CA3	0.830			
AB	AB1	0.811	0.919	0.903	0.757
	AB2	0.912			
	AB3	0.875			
JS	JS1	0.792	0.906	0.904	0.703
	JS2	0.789			
	JS3	0.809			
	JS4	0.802			

DIJ(Distributive Injustice), PIJ(Procedural Injustice), IIJ(Informational Injustice), CA(Compliance Anxiety), AB(Avoid Behavior), JS(Justice Sensitivity)

집중 타당성은 개념신뢰도(CR)와 평균분산추출(AVE)를 구하여 확인하는데, 일반적으로 개념신뢰도는 0.7 이상, 평균분산추출은 0.5 이상을 요구한다[40]. 분석 결과, 요인들의 집중타당성은 확보하였다(표 2).

또한, 판별타당성 분석은 잠재변수간의 차별성을 확인하는 기법으로서, 상관계수와 평균분산추출 값을 비교하여 확인한다. 잠재변수의 평균분산추출의 제곱근 값이 상관계수보다 크면 판별타당성을 확보한다고 본다[41]. 결과는 판별타당성을 확보한 것으로 나타났다(표 3).

그리고, 본 연구는 설문지 기법으로 영향 관계에 있는 요인들을 측정하였기 때문에, 공통방법편의 문제가 있는지를 확인한다. 공통방법편의 분석 기법은 상황별 다양하게 적용하고 판단하는 기법들이 제시되고 있으며, 연구는 Podsakoff et al.[2003]이 사례로 제시한 방법 중 비측정 잠재방법 요인 측정 기법을 적용한다. 본 기법은 확인적 요인분석에 추가로 잠재요인을 적용하되, 적용하지 않은 구조 모델과 적용한 구조 모델의 항목의 변화량을 확인하는 기법이다. 분석 결과 잠재요인을 적용하지 않은 구조모델의 적합성($\chi 2/df$ = 1.566, RMSEA = 0.042, GFI = 0.938, AGFI = 0.914, NFI = 0.948, CFI = 0.980)과 적용한 구조 모델의 적합성($\chi 2/df$ = 1.364, RMSEA = 0.034, GFI = 0.951, AGFI = 0.922, NFI = 0.960, CFI = 0.989) 모두 적합도 요구사항보다 높은 것으로 나타났으며, 측정 항목간의 변화량은 0.3 이하로 나타나, 공통방법편의 문제는 높지 않은 것으로 판단된다.

표 3. 판별타당성 결과
Table 3. Result for Discriminant Validity

Constructs	1	2	3	4	5	6
DIJ	**0.710**					
PIJ	.597**	**0.755**				
IIJ	.516**	.429**	**0.791**			
CA	.520**	.426**	.472**	**0.798**		
AB	.450**	.429**	.335**	.384**	**0.870**	
JS	.603**	.626**	.454**	.513**	.406**	**0.838**

Note: Values in bold type = square root of the AVE
DIJ(Distributive Injustice), PIJ(Procedural Injustice), IIJ(Informational Injustice), CA(Compliance Anxiety), AB(Avoid Behavior), JS(Justice Sensitivity)
**: p < 0.01

4-2 주 효과 분석

본 연구는 조절 효과를 제외한 요인간의 영향 관계를 확인하는 주 효과 분석을 실시한다. 해당 분석은 AMOS 22.0을 활용하였으며, 구조방정식모델링을 적용하였기 때문에 적합성을 확인하였다. 적합성 분석 결과는 χ2/df = 2.265, RMSEA = 0.063, GFI = 0.933, AGFI = 0.902, NFI = 0.935, CFI = 0.963로 나타났다. 결과는 RMSEA가 요구사항인 0.5보다 약간 높은 것으로 나왔으나 그 외 값들은 적합성 판단을 위한 기준보다 높게 나타나, 경로 분석에 문제가 없다고 판단하여 연구가설을 검증한다.

연구가설 1은 정보보안 준수 걱정이 정보보안 기피행동에 정(+)의 영향을 준다는 것으로, 결과는 통계적으로 유의한 것으로 나타났다(H1: β= 0.385, p < 0.01). 이러한 결과는 정보보안 관련 걱정이 정보보안 준수의도에 부정적 영향을 미친다는 Hwang et al.[2017]의 연구와 유사한 결과이다. 즉, 정보보안 정책에 대한 행동을 업무에 적용해야 하는 조직원의 입장에서, 정보보안 정책이 자신의 역량을 넘어서거나 어렵다고 판단할 때 오히려 정보보안 준수 상황에서 기피 행동을 보일 수 있음을 의미한다. 따라서, 조직은 정보보안 정책 적용 시, 구성원의 보안에 대한 걱정을 최소화하기 위한 노력을 하는 것이 필요하다.

연구가설 2는 정보보안 분배 불공정성이 보안 준수 걱정에 정(+)의 영향을 미친다는 것으로, 결과는 통계적으로 유의한 것으로 나타났으며(H2: β= 0.310, p < 0.01), 연구가설 3은 정보보안 절차 불공정성이 보안 준수 걱정에 정(+)의 영향을 미친다는 것으로, 결과는 통계적으로 유의한 것으로 나타났다(H3: β= 0.153, p < 0.05).

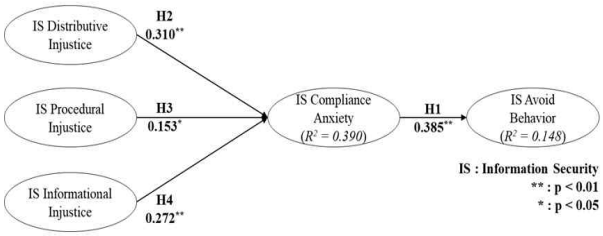

그림 2. 구조모델 결과 (주 효과)
Fig. 2. Results of the Structural Model (Main Effect)

표 4. 주효과 분석 결과
Table 4. Results of Main Effect Tests

	Path	Coefficient	t-value	Result
H1	CA → AB	0.385	6.405**	Support
H2	DIJ → CA	0.31	3.427**	Support
H3	PIJ → CA	0.153	1.959*	Support
H4	IIJ → CA	0.272	3.890**	Support

DIJ(Distributive Injustice), PIJ(Procedural Injustice), IIJ(Informational Injustice), CA(Compliance Anxiety), AB(Avoid Behavior)
**: p < 0.01, *: P < 0.05

그리고, 연구가설 4는 정보보안 정보 불공정성이 보안 준수 걱정에 정(+)의 영향을 미친다는 것으로, 결과는 통계적으로 유의한 것으로 나타났다(H4: β= 0.272, p < 0.01). 이러한 결과는 개인에 대한 불공평이 걱정을 높인다는 Johnson et al.[2010], 상급자의 불공정성이 당사자의 심리적 불안을 일으킨다는 Rafferty et al.[2010]의 결과와 유사하다. 즉, 정보보안 행동에 대하여 필요한 정보 제공, 의사결정 절차, 그리고 결과에 대한 불공정 판단은 당사자에게 불안감, 즉 걱정을 높일 수 있기 때문에, 조직들은 공정한 정보보안 활동에 대한 지원 및 결과를 예측할 수 있는 정보 등을 제공하는 것이 필요하다.

마지막으로, 선행 변수의 영향력인 결정계수(R^2)를 확인하였다. 분배. 절차, 그리고 정보 불공정성은 정보보안 준수 걱정에 39.0%의 영향을 미치는 것으로 나타났으며, 준수 걱정은 정보보안 기피 행동에 14.8%의 영향을 미치는 것으로 나타났다.

4-3 조절 효과 분석

본 연구는 정보보안 관점에서 피해자 공정 민감성(victim justice sensitivity)이 불공정성과 걱정 간의 관계를 조절하는 것을 확인한다. 요인들은 등간 척도로 구성되어 있으므로, 구조방정식모델링의 조절효과는 독립변수와 조절 변수간의 상호작용항을 도출하고, 상호작용 항의 결과변수에 미치는 영향을 측정한다. 연구는 상호작용 항 도출의 방법으로 독립변수와 조절변수의 측정 항목을 모두 연계한 직교화접근법(orthogonalizing approach)을 적용하였으며[43], 결과는 표 5와 같다.

표 5. 조절 효과 분석 결과
Table 5. Results of Moderating Effect Tests

	Path	Coefficient	t-value	Result
H5a	DIJ → CA	0.284	3.407**	Support
	SJ → CA	0.399	4.987**	
	DIJ x SJ → CA	0.253	4.861**	
H5b	PIJ → CA	0.106	1.316	Support
	SJ → CA	0.516	6.115**	
	PIJ x SJ → CA	0.253	4.792**	
H5c	IIJ → CA	0.302	5.011**	Support
	SJ → CA	0.447	7.122**	
	IIJ x SJ → CA	0.239	4.783**	

DIJ(Distributive Injustice), PIJ(Procedural Injustice), IIJ(Informational Injustice), CA(Compliance Anxiety), JS(Justice Sensitivity)
**: p < 0.01

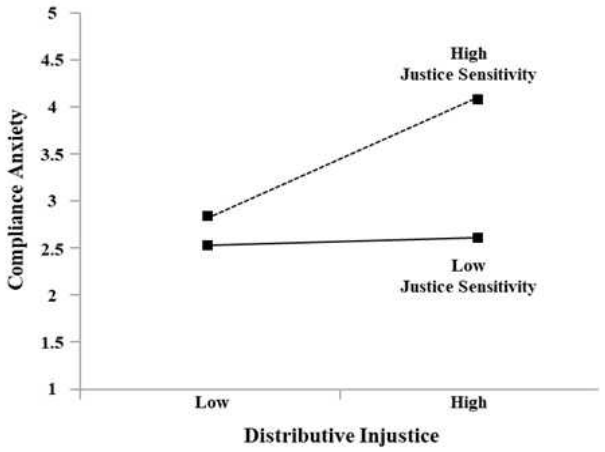

그림 3. 공정 민감성의 조절효과 (H5a)
Fig. 3. Moderation Effect of Justice Sensitivity (H5a)

연구가설 5a는 공정 민감성이 정보보안 분배 불공정성과 정보보안 준수 걱정 간을 조절한다는 것으로, 상호작용항이 통계적으로 유의한 것으로 나타났다(H5a: β= 0.253, p < 0.01). 조절효과의 영향 관계를 명확하게 알아보기 위하여 그래프로 표현하였다. 분석 결과, 분배 불공정성은 준수 걱정을 높이며, 분배 불공정성 집단 내에서 공정 민감성이 높은 집단이 낮은 집단보다 보안 준수 걱정을 더욱 크게 형성하는 것을 확인하였다.

연구가설 5b는 공정 민감성이 정보보안 절차 불공정성과 정보보안 준수 걱정 간을 조절한다는 것으로, 상호작용항이 통계적으로 유의한 것으로 나타났다(H5b: β= 0.253, p < 0.01). 조절효과의 영향 관계를 명확하게 알아보기 위하여 그래프로 표현하였다. 분석 결과, 절차 불공정성은 자체만으로 준수 걱정을 높이지 않으나, 조절 효과 분석 시 절차 불공정성 집단 내에서 공정 민감성이 높은 집단이 낮은 집단보다 보안 준수 걱정을 더욱 크게 형성하는 것을 확인하였다.

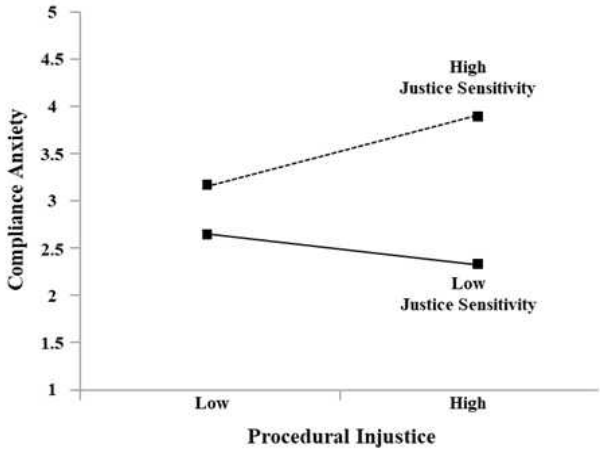

그림 4. 공정 민감성의 조절효과 (H5b)
Fig. 4. Moderation Effect of Justice Sensitivity (H5b)

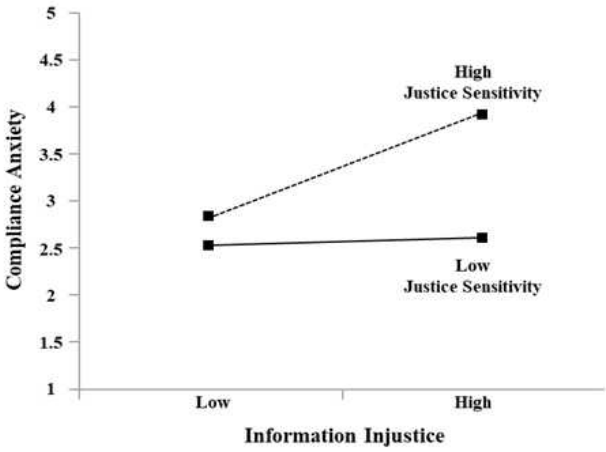

그림 5. 공정 민감성의 조절효과 (H5c)
Fig. 5. Moderation Effect of Justice Sensitivity (H5c)

연구가설 5c는 공정 민감성이 정보보안 정보 불공정성과 정보보안 준수 걱정 간을 조절한다는 것으로, 상호작용항이 통계적으로 유의한 것으로 나타났다(H5c: β= 0.239, p < 0.01). 조절효과의 영향 관계를 명확하게 알아보기 위하여 그래프로 표현하였다. 분석 결과, 정보 불공정성은 준수 걱정을 높이며, 정보 불공정성 집단 내에서 공정 민감성이 높은 집단이 낮은 집단보다 보안 준수 걱정을 더욱 크게 형성하는 것을 확인하였다.

조절 효과 검증 결과, 정보보안에 대한 조직 불공정성이 구성원의 보안 걱정에 미치는 영향은 개인의 공정 민감성에 따라 조절하는 것을 확인하였다. 즉, 조직원들이 조직의 불공정한 상황을 나쁘게 인식할수록 정보보안 준수에 대한 걱정이 높아짐을 의미하기 때문에, 조직은 정보보안 공정성에 대한 인식을 높이기 위한 노력을 해야 함을 의미한다.

Ⅴ. 결 론

5-1 연구의 요약

코로나 19로 인한, 사람 간의 연계 활동이 제약되면서, 조직 내 온라인 기반의 업무들이 다양하게 진행되고 있다. 많은 조직들은 사회적 문제 대처와 업무 효율 감소 최소화를 위하여 온라인 미팅 등을 추진하고 있지만, 정보보안 관점에서는 조직의 중요 정보에 대한 외부 노출 방식이 다양해짐을 의미하기 때문에 조직 내부의 보안 사고의 우려도 함께 커지고 있다. 본 연구는 조직의 내부 정보보안 수준에 문제가 되는 구성원들의 정보보안 기피 행동에 미치는 영향 요인을 제시함으로써, 조직이 추진해야 할 방향을 제시하고자 하였다. 세부적으로, 정보보안 불공정 요소(분배, 절차, 정보적 관점)들이 실제 업무에 정보보안을 적용해야 하는 구성원들에게 불안감 등 걱정을 일으켜 정보보안 상황에서 기피행동으로 이어지는 관계를 확인하고자 하였

으며, 정보보안 불공정성이 걱정에 미치는 영향을 개인의 공정 민감성이 강화하는 것을 확인하고자 하였다.

연구 대상은 조직에 도입된 정보보안 정책을 업무에 적용해야 하는 근로자들로 하였으며, 323개의 표본을 확보하여 AMOS 22.0 툴을 활용한 구조방정식모델링을 실시하였다.

분석 결과, 정보보안 분배 불공정성, 절차 불공정성, 그리고 정보 불공정성이 개인의 정보보안 준수 걱정을 높였으며, 정보보안 기피행동으로 이어지는 관계가 있음을 확인하였다. 또한, 피해자 공정 민감성이 정보보안 불공정성과 걱정 간의 관계를 강화하는 것을 확인하였다. 특히, 공정 민감성은 높은 집단이 낮은 집단보다 불공정성에 의해 받는 준수 걱정을 더욱 높이는 것을 확인하였다. 본 연구는 조직 내부자들의 정보보안 미준수 행동에 미치는 부정적 영향 관계를 확인함으로써, 조직이 고려해야 할 방향을 제시하였다는 측면에서 시사점을 가진다.

5-2 연구의 시사점 및 향후 연구

본 연구는 정보보안 기피 행동 원인을 제시한 관점에서 다음의 학술적 시사점을 가진다. 첫째, 본 연구는 조직 내 정보보안 관련 행동을 업무에 적용하는 구성원의 관점에서 상황을 회피하고자 하는 행동 개념인 기피 행동을 정보보안 분야에 적용하고, 형성된 개인의 정보보안에 대한 걱정이 기피 행동을 높이는 요인임을 확인하였다. 정보보안 정책 및 기술은 특정 정보시스템 도입처럼 한번 도입으로 끝나는 것이 아니라, 추가적 업데이트 또는 물리적 준수 요구 등 조직의 외부 환경적 변화에 맞추어 대응해야 하는 어려움이 있다. 조직원들은 정보보안 준수 행동에 어려움을 겪거나 불안감을 가지게 될 때 미준수 행동을 보일 수 있는데, 본 연구는 정보보안으로 형성된 걱정과 기피행동 간에 영향관계가 있음을 확인하였다. 즉, 학술적 관점에서 연구는 정보보안 미준수의 유형인 기피 행동을 적용하여 원인을 제시하였다는 측면에서 시사점을 가진다.

둘째, 본 연구는 조직 공정성 이론을 부정적 관점으로 적용한 조직 차원의 불공정성과 개인의 걱정 간의 관계가 성립됨을 확인하였다. 조직 불공정성은 결과에 대한 분배, 의사결정 과정의 절차, 그리고 사전 정보 제공이라는 측면의 활동이 구성원들에게 공정하지 못하게 인식되는 관점으로서, 불공정성이 높아지면 스트레스로 발현된다. 본 연구는 정보보안 분야에 조직 불공정성을 적용하여 개인의 부정적 행동 원인인 걱정에 미치는 영향을 확인하였다. 즉, 학술적 관점에서 연구는 정보보안 분야에 불공정성 요인들을 반영하여 부정적 영향을 줄 수 있는 선행조건임을 확인하였다는 측면에서 시사점을 가진다.

셋째, 본 연구는 개인의 공정성에 대한 민감한 수준인 공정 민감성을 적용하여, 불공정한 상황에 대한 걱정의 변화를 측정하였다. 세부적으로, 본 연구는 당사자가 불공정함으로 인하여 피해를 받을 때 형성되는 거부감인 민감성을 적용하였으며, 정보보안 분배 불공정성, 절차 불공정성, 그리고 정보 불공정성이 걱정을 형성시키는데 있어, 강화 효과를 가지는 것을 확인하였다. 즉, 학술적 관점에서 연구는 개인의 공정에 대한 민감성 수준에 따라, 정보보안 부정적 원인에 영향을 줄 수 있다는 것을 확인하였다는 측면에서 탐색적 시사점을 가진다.

또한, 본 연구는 조직의 정보보안 관련 준수 수준 향상 관점에서 다음의 실무적 시사점을 가진다. 첫째, 본 연구는 조직 내부의 정보보안 목표 달성에 결정적인 영향을 주는 조직원의 미준수 행동 유형 중의 한 가지인 기피 행동을 높이는 부정적 원인(정보보안 준수 걱정)을 제시하였다. 정보보안 준수 걱정은 자신의 보안 환경과 요구사항이 자신의 역량보다 높을 때 발생하는 것으로 준수할 수 있을지에 대한 두려움, 불안감의 발현이다. 자산 보호를 위하여 지속적으로 변화를 추구할 수 밖에 없는 정보보안 정책의 특성 상 개인의 걱정이 높아질 수 밖에 없는데, 걱정 수준이 높아지면 개인은 정보보안 상황에 대한 기피 행동으로 발현되는 것을 확인하였다. 즉, 실무적 관점에서 조직이 내부의 보안 목표 달성을 위해 고려해야 할 조직원의 감정을 확인하고 적정한 대처를 해주는 것이 필요함을 제시하였다는 측면에서 시사점을 가진다.

둘째, 본 연구는 정보보안 불공정성 세부요인을 적용하였으며, 분배 불공정성, 절차 불공정성, 그리고 정보 불공정성이 개인의 정보보안 준수 걱정을 높이는 것을 확인하였다. 세부적으로, 정보보안 분배 불공정성은 정보보안 행동 결과에 대한 불공정성으로 보상보다는 처벌의 개념이 강한 정보보안 관점에서 결과의 불공정성은 개인의 불안감을 높일 수 있다. 정보보안 절차 불공정성은 정보보안 의사결정 및 참여 과정에서 제외되는 등 불공평한 대우를 받았다고 판단하는 수준으로 과정의 불평등은 걱정을 높일 수 있음을 의미한다. 정보보안 정보 불공정성은 정보보안 행동에 필요한 각종 정보를 사전에 동등하게 받지 못한다는 개념으로서 정보 불공정성이 발생하면, 결과 또한 다르게 나타나기 때문에 정보보안을 업무 적용에 어려움이 발생할 수밖에 없다. 본 연구는 실무적 관점에서 조직이 추진하는 정보보안 정책의 적용에 있어, 사전 정보제공, 과정, 그리고 결과 전반에 걸친 조직원의 불공정성에 대한 고려가 함께 존재하며 스트레스 요인으로 발생 될 수 있음을 제시한 측면에서 시사점을 가진다.

마지막으로, 본 연구는 공정성에 대한 민감성 수준이 불공정성에 의한 부정적 영향을 강화하는 것을 확인하였다. 특히, 정보보안 분야에 피해자 공정 민감성을 적용하여 민감성이 높을수록 정보보안 불공정 요인별(정보, 절차, 분배) 걱정에 미치는 영향이 높아지는 것을 확인하였다. 따라서, 조직이 개인의 공정 민감성을 낮추는 것은 현실적으로 어려우므로, 조직이 제공하는 정보보안 요구사항에 맞게 구성원들에게 공평한 대우를 하고 있음을 지속적으로 알리는 것이 필요하다.

본 연구는 정보보안 조직 불공정성, 정보보안 준수 걱정, 그리고 기피 행동 간에 긍정적 영향 관계가 있음을 제시한 측면에서 시사점을 가지지만, 다음과 같은 한계점이 있으며, 향후 보완될 필요가 있다. 첫째, 본 연구는 정보보안 행동과 관련된 조직의 노력 요인과 개인의 동기적 측면을 확인하기 위하여 정보보안을 도입한 조직에 근무하는 직장인을 대상으로 설문을 하였다. 즉, 정보보안에 대한 직장인의 생각을 확인함으로써, 조

직이 추진해야 할 방향을 제시하였다. 하지만, 조직의 공정성에 대한 평가는 조직의 특성별 차이가 높을 것으로 판단한다. 예를 들어, 개인주의 조직과 집단주의 조직은 공정성에 대한 관점이 틀릴 수 있다. 따라서, 향후 연구에서 조직 문화적 특성에 따른 개인의 행동과 조직의 추진 노력을 다양하게 제시한다면 보다 높은 시사점을 가질 수 있을 것으로 판단한다. 둘째, 본 연구는 개인차에 의한 요인을 공정 민감성 관점에서 접근하여 불공정성과 걱정 간의 관계를 조절하는 것을 확인하였다. 공정 민감성은 선행 연구 별로 다양하게 제시되고 있다. 예를 들어 Liu and Berry[2013]는 공평성을 기반으로 민감성을 제시하였으며, 본 연구에 적용한 피해자 공정 민감성 이외에 관찰자, 가해자 민감성도 존재한다[37]. 따라서, 향후 연구에서 다양한 개인 차 변인을 정보보안 분야에 적용하여 확인한다면, 높은 현실적 시사점을 제시할 수 있을 것으로 판단한다.

감사의 글

이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구(NRF-2018R1D1A1B07050305)로서, 관계부처에 감사드립니다.

참고문헌

[1] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, “Information Security Governance Challenges and Critical Success Factors: Systematic Review,” *Computers & Security*, Vol. 99, pp. 102030, 2020.

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

[3] K. D. Loch, H. H. Carr, and M. E. Warkentin, “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding,” *MIS Quarterly*, Vol. 16, No. 2, pp. 173-186, 1992.

[4] 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, pp. 523-548, 2010.

[5] H. Liang and Y. Xue, “Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective,” *Journal of the Association for Information Systems*, Vol. 11, No. 7, pp. 394-413, 2010.

[6] J. Y. Son, “Out of Fear or Desire? Toward a Better Understanding of Employees’ Motivation to Follow IS Security Policies,” I*nformation & Management*, Vol. 48, No. 7, pp. 296-302, 2011.

[7] Y. Chen, K. Ramamurthy, and K. W. Wen, “Organizations' Information Security Policy Compliance: Stick or Carrot Approach?,” *Journal of Management Information Systems*, Vol. 29, No. 3, pp. 157-188, 2012.

[8] C. Posey, T. L. Roberts, and P. B. Lowry, “The Impact of Organizational Commitment on Insiders’ Motivation to Protect Organizational Information Assets,” *Journal of Management Information Systems*, Vol. 32, No. 4, pp. 179-214, 2015.

[9] Y. Chen and F. M. Zahedi, “Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China,” *MIS Quarterly*, Vol. 40, No. 1, pp. 205-222, 2016.

[10] 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, pp. 37-46, 2019.

[11] M. Tarafdar, Q. Tu, B. S. Ragu-Nathan, and 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.

[12] R. Ayyagari, V. Grover, and R. Purvis, “Technostress: Technological Antecedents and Implications,” *MIS Quarterly*, Vol. 35, No. 4, pp. 831-858, 2011.

[13] J. D'Arcy, T. Herath, and 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.

[14] 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, pp. 282-293, 2018.

[15] J. D'Arcy, A. Hovav, and D. Galletta, “User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach,” *Information Systems Research*, Vol. 20, No. 1, pp. 79-98, 2009.

[16] S. Ha and H. Kim, “The Effects of User’s Security Awareness on Password Security Behavior,” *Journal of Digital Contents Society*, Vol. 14, No. 2, pp. 179-189, 2013.

[17] H. J. Lee, H. S. Kho, E. H. Roh, and K. S. Han, “A Study on the Factors of Experience and Habit on Information Security Behavior of New Services-based on PMT and UTAUT2,” *Journal of Digital Contents Society*, Vol. 19, No. 1, pp. 93-102, 2018.

[18] I. Hwang, D. Kim, T. Kim, and 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.

[19] I. Hwang, “The Effect of Information Security Delivery

Activities and Feedback on Work Impediment and Compliance Intention," *Journal of Digital Contents Society*, Vol. 21, No. 9, pp. 1653-1663, 2020.

[20] M. Y. Leung, Y. S. I. Chan, and C. Dongyu, C, "Structural Linear Relationships between Job Stress, Burnout, Physiological Stress, and Performance of Construction Project Managers," *Engineering, Construction and Architectural Management*, Vol. 18 No. 3, pp. 312-328, 2011.

[21] F. Gaudioso, Q. Turel, and C. Galimberti, "The Mediating Roles of Strain Facets and Coping Strategies in Translating Techno-Stressors into Adverse Job Outcomes," *Computers in Human Behavior*, Vol. 69, pp. 189-196, 2017.

[22] I. Hwang, "Analysis of the Effects of Information Security Sanction and Role Ambiguity on Compliance Intention: Focusing on Moderation Effects of Technical Support and Task Coping," *Journal of Digital Contents Society*, Vol. 22, No. 2, pp. 271-280, 2021.

[23] M. Salanova, S. Llorens, and E. Cifre, "The Dark Side of Technologies: Technostress among Users of Information and Communication Technologies," *International Journal of Psychology*, Vol. 48, No. 3, pp. 422-436, 2013.

[24] 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.

[25] P. M. Muchinsky, *Psychology Applied to Work: An Introduction to Industrial and Organizational Psychology*. Wadsworth/Thomson Learning, 2014.

[26] S. W. Hystad, K. J. Mearns, and J. Eid, "Moral Disengagement as a Mechanism between Perceptions of Organisational Injustice and Deviant Work Behaviours," *Safety Science*, Vol. 68, pp. 138-145, 2014.

[27] T. A. Judge and 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.

[28] 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.

[29] L. Jiang and C. Wagner, "Perceptions of Justice or Injustice as Determinants of Contributor Defections from Online Communities," *Journal of the Association for Information Science and Technology*, Vol. 66, No. 7, pp. 1477-1493, 2015.

[30] A. E. Rafferty, S. L. D. Restubog, and N. L. Jimmieson, "Losing Sleep: Examining the Cascading Effects of Supervisors' Experience of Injustice on Subordinates' Psychological Health," *Work & Stress*, Vol. 24, No. 1, pp. 36-55, 2010.

[31] 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 Journal*, Vol. 24, No. 6, pp. 479-502, 2014.

[32] 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.

[33] A. K. Khan, S. Quratulain, and J. R. Crawshaw, "The Mediating Role of Discrete Emotions in the Relationship between Injustice and Counterproductive Work Behaviors: A Study in Pakistan," *Journal of Business and Psychology*, Vol. 28, No. 1, pp. 49-61, 2013.

[34] R. E. Johnson, C. H. Chang, and C. C. Rosen, "Who I Am Depends on How Fairly I'm Treated: Effects of Justice on Self-Identity and Regulatory Focus," *Journal of Applied Social Psychology*, Vol. 40, No. 12, pp. 3020-3058, 2010.

[35] I. Hwang and 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.

[36] Y. Liu and C. M. Berry, "Identity, Moral, and Equity Perspectives on the Relationship Between Experienced Injustice and Time Theft," *Journal of Business Ethics*, Vol. 118, No. 1, pp. 73-83, 2013.

[37] M. Schmitt, M. Gollwitzer, J. Maes, and D. Arbach, "Justice Sensitivity: Assessment and Location in the Personality space," *European Journal of Psychological Assessment*, Vol. 21, No. 3, pp. 202–211, 2005.

[38] M. Gollwitzer, T. Rothmund, A. Pfeiffer, and C. Ensenbach, "Why and When Justice Sensitivity Leads to Pro- and Antisocial Behavior," *Journal of Research in Personality*, Vol. 43, No. 6, pp. 999-1005, 2009.

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

[40] B. H. Wixom and H. J. Watson, "An Empirical Investigation of the Factors Affecting Data Warehousing Success," *MIS Quarterly*, Vol. 25, No.1, pp. 17-41, 2001.

[41] C. Fornell and 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.

[42] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee, and 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.

[43] G. C. Lin, Z. Wen, H. W. Marsh, and 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.

황인호(Inho Hwang)

2007년 : 중앙대학교 대학원 (경영학석사)
2014년 : 중앙대학교 대학원 (경영학박사)

2014년～2018년: (사)한국창업경영연구원
2018년～2020년: 한국산업기술대학교
2020년～현 재: 국민대학교 교양대학 조교수
※관심분야 : IT 핵심성공요인(IT CSF), 디지털 콘텐츠(Digital Content), 정보보안(Information Security), 프라이버시(Privacy) 등