

내부자의 정보보안 준수를 위한 정보보안 환경 및 지원 체계 구축: 정보보안 공정성 분위기 강화 관점

황인호*

Building an IS Environment and Support Structure for Insiders to Comply with IS:
A Perspective on Improving the IS Related Justice Climate

In-Ho Hwang*

요 약

정보 관리가 조직의 핵심 역량으로 인식되면서, 조직들은 정보 관리 및 보호를 위한 정책 및 기술에 대한 자원 투입을 높이고 있다. 특히, 정보보안 활동의 경우, 내부자에 의한 정보 노출 사고가 지속해서 발생함에 따라 조직 내부자 관리에 관심 수준이 높아지고 있다. 본 연구는 조직이 구축한 정보보안 환경 및 지원 구조가 정보보안 준수 의도에 미치는 영향을 확인하고자 한다. 본 연구는 조직이 구축한 정보보안 환경 및 지원 구조가 정보보안 준수 의도에 미치는 영향을 확인하고자 정보보안 정책 운용 조직 실무자의 설문조사로 수행하였으며, 421개의 표본을 활용하여 구조방정식 모델과 Process 3.1을 활용하여 가설 검증을 하였다. 분석 결과, 정보보안 환경 구축 요인인 진성 리더십과 공정성 분위기, 정보보안 준수 지원 요인인 커뮤니케이션과 피드백이 보안 준수 의도에 긍정적인 영향을 주었다. 또한, 진성 리더십, 처벌, 커뮤니케이션, 그리고 피드백이 정보보안 공정성 분위기의 긍정적 영향을 강화하는 것으로 나타났다. 연구 결과는 조직 차원에서 내부자의 보안 행동 강화를 위해 추진해야 할 구조 설계 방향을 전체적으로 제시하였다는 측면에서 조직 정보보안 수준 달성에 기여한다.

ABSTRACT

As information is recognized as a core competency of organizations, organizations are increasingly investing in policies and technologies for information security (IS). Recently, as information exposure accidents by people have occurred continuously, interest in IS behaviors of organization insiders is increasing. This study aims to confirm the effect of the IS environment and support structure established by the organization on the intention of individuals to comply with IS. We conducted a survey of employees in organizations with IS policies and tested the hypothesis using the structural equation of AMOS 22.0 and Process 3.1 using 421 samples. As a result of the analysis, authentic leadership and justice climate, which are factors that build an IS environment, and communication and feedback, which are factors supporting IS compliance, have a positive effect on employees' compliance intention. In addition, authentic leadership, punishment, communication, and feedback were found to reinforce the positive impact of IS justice climate. As the study suggested the overall structural design direction to be pursued to reinforce insider's IS behavior, and the results help to achieve the IS goal.

키워드

Compliance Intention, Authentic Leadership, Justice Climate, Sanction, Communication, Feedback
준수 의도, 진성 리더십, 공정성 분위기, 처벌, 커뮤니케이션, 피드백

* 교신저자: 국민대학교 교양대학

• 접수일 : 2022. 08. 12
• 수정완료일 : 2022. 09. 11
• 게재확정일 : 2022. 10. 17

• Received : Aug. 12, 2022, Revised : Sep. 11, 2022, Accepted : Oct. 17, 2022

• Corresponding Author : In-Ho Hwang
College of General Education, Kookmin University,
Email : hwanginho@kookmin.ac.kr

1. 서 론

정보가 조직의 지속적인 성장을 위한 핵심 가치로 인지되면서, 조직은 자사의 정보를 체계적으로 관리하기 위해 높은 수준의 정보 기술을 도입하고 있으며 자사의 정보가 외부에 노출되지 않도록 다양한 보안 정책 및 기술을 적용하고 있다[1]. 그렇지만, 조직의 정보보안 사고는 끊임없이 발생하고 있다. 특히, 보안 사고의 경우 발생할 경우, 조직의 가치를 감소시킬 뿐 아니라 해당 정보와 관련된 이해관계자까지 추가 피해를 발생시킬 수 있어 사회적으로도 관심이 높은 상황이다[2]. 실제로, 정보보안 사고는 다양한 채널로 발생하고 있는데, Verizon[2021]에 따르면, 멀웨어, 소셜 침입 등 조직 외부로 통한 기술 침입을 통해 발생한 정보 탈취 사고가 매년 드러난 전체 사고의 약 2/3 수준에서 발생하고 있으며, 조직과 관련된 파트너 및 내부자에 의한 노출 기반의 보안 사고가 약 1/3 수준에서 발현됨을 지적하고 있다[3]. 지금까지 정보 보호를 위한 관심은 대부분 외부의 침입 방지를 위한 정보보안 기술 도입에 주력해왔으나, 2021년 9월 바이든 행정부가 제로-트러스트(Zero-trust) 행정 명령을 내릴 정도로 내부자에 의한 보안 사고를 방지하기 위한 관심 또한 높아지는 상황이다. 제로-트러스트는 조직의 정보보안 보호 정책과 규제가 외부와 동일하게 내부자에게도 적용해야 함을 의미한다[4].

조직 내부의 정보보안 사고 예방을 위한 선행연구는 내부자, 즉 조직원의 정보보안 준수 행동 강화를 위한 심리적 접근에 주목해왔다. 즉, 조직이 엄격한 정보보안 정책을 도입하더라도, 정보보안 활동을 업무에 적용해야 하는 조직원이 동의하지 않는다면 언제든지 정보를 노출할 수 있음을 고려하고 있으며, 조직은 조직원의 이타적이고 능동적인 정보보안 활동 수준을 증진하기 위한 노력을 해야 한다고 본다. 대표적으로, 정보보안 정책과 규정을 지킴에 있어 엄격하고 심각한 수준의 처벌 및 제재를 제시할 때 조직원의 참여를 유도할 수 있다는 관점의 연구[2][5], 조직원에게 정보 가치에 대한 이해와 정보 노출 시 발생할 수 있는 위협, 그리고 대처의 필요성을 인식시키는 것이 보안 행동으로 이어진다는 관점의 연구[1], 정보보안 준수 행동에 대한 개인의 이익과 손해에 대한 인식이 정보보안 행동으로 이어진다는 관점의 연구[6] 등이

대표적이다. 최근에는 리뷰 연구를 중심으로 조직과 개인의 관계에서 개인은 조직이 구축한 특정 환경 및 구조에 의해 영향을 받고 행동으로 이어지기 때문에 조직의 전체적인 정보보안 환경 구축이 무엇보다 중요하다라는 관점이 제시되고 있다[7]. 그러나, 조직의 전반적인 정보보안 정책 구축 환경 및 조직원의 정보보안 준수 행동 강화를 위한 지원 체계 관련 연구는 다각적으로 제시되고 있지 않은 상황이다.

본 연구는 조직의 정보보안 환경 구축 및 지원 체계를 다각화하여 조직의 어떠한 정보보안 준수 지원 요인이 조직원의 정보보안 준수 활동에 기여할 수 있는지를 확인하고자 한다. 세부적으로, 조직이 전체적인 보안 환경 구축을 위해 노력하는 요인으로 진성 리더십과 공정성 분위기를 제시하였고, 조직의 정보보안 정책 이행 관점에서 처벌을 제시하였다. 그리고, 정보보안 준수 지원 체계 요인으로 커뮤니케이션과 피드백을 제시하였다. 더불어, 본 연구는 전체적으로 형성된 조직 내 정보보안 공정성 분위기를 강화하는 방안을 함께 논의함으로써, 조직 내부의 정보보안 수준 달성에 분위기가 미치는 영향을 제시하고자 한다. 즉, 연구는 진성 리더십, 처벌, 커뮤니케이션, 그리고 피드백의 공정성 분위기가 미치는 긍정적 영향을 어떻게 강화하는지를 제시한다. 연구의 결과는 조직 차원에서 조직원의 보안 행동 강화를 위해 추진해야 할 구조적 설계 방안을 전체적으로 제시함으로써, 내부보안 목표 달성에 기여할 것으로 판단한다.

II. 선행연구

2.1 진성 리더십

리더십은 조직 행동 연구에서 일찍부터 조직 내부자들의 행동 전환에 영향을 주는 조건으로 활용되었던 요인으로, 정보시스템의 발전과 기업의 사회적 책임이 중요해지면서, 새로운 조건의 리더십이 강조되고 있다[8]. 이중 진성 리더십(Authentic Leadership)은 리더의 투명성과 도덕적 신념, 그리고 믿을 수 있는 행동의 중요성을 강조한 리더십을 의미한다[9]. 즉, 기업의 사회적 책임은 리더에서부터 나오고, 리더가 제시하는 행동이 진실할 때, 구성원들의 리더에 대한 믿음이 형성되고 기업의 바람직한 성장을 위해 노력한

다는 관점이다[10].

진성 리더십은 리더가 구성원에게 보여줘야 할 조건을 하나의 형태가 아닌 복합적 차원으로 구성되어 있음을 제시하고 있다[9-10]. 즉, 내재화된 도덕적 관점(Internalized Moral Perspective), 균형 잡힌 정보처리(Balanced Processing of Information), 자기인식(Self-awareness), 관계적 투명성(Relational Transparency)이라는 4가지 측면의 차원을 복합적으로 내재화하고 제시하는 것을 요구한다. 첫째, 내재화된 도덕적 관점은 리더가 사회가 요구하는 윤리 및 도덕적 신념에 따라 행동하는 모습을 의미한다. 이와 같은 도덕적 관점은 구성원들의 윤리적 가치와 일치하여 조직 전체의 윤리적 분위기를 형성에 기여할 수 있다. 둘째, 균형 잡힌 정보처리는 리더의 의사결정이 주관적이지 아니하고 객관적 정보에 기반하여 행동하는 모습을 의미한다. 즉, 객관적 정보를 통해 의사결정이 이루어지므로, 조직 내 특정 행위의 과정과 결과가 공정하게 나타날 수 있다. 셋째, 자기인식은 리더는 본인이 보유한 강점과 약점을 명확하게 인식하고 강점의 강화와 약점의 보완을 위해 노력하는 것을 의미한다. 마지막으로, 관계적 투명성은 집단의 구성원과의 관계가 명료하고 투명하여 진솔한 모습을 보이는 수준을 의미한다. 즉, 특정 행동에 있어 리더가 구성원과 교류를 통해 협력적으로 해결하는 모습의 수준을 의미한다.

2.2 정보보안 공정성 분위기

공정성은 특정 사회 또는 집단에 소속되어 있는 개인과 개인, 개인과 집단 간의 공평함에 대한 인식과 관련 행동의 결과에 대한 반응을 의미한다[11]. 초기의 공정성은 특정 활동의 결과에 대한 분배 관점에서 공평성 평가를 기준으로 논의되는데, 개인과 집단 간의 관계에서 분배의 결과에 대하여 대상자가 느끼는 상대적 만족감과 박탈감을 중심으로 공평성을 판단한다고 보았다[12]. 이후, 조직 공정성은 결과의 분배에 대한 공정함에서, 결과가 이루어지는 절차에 대한 공정함, 집단 내 교환 대상자 간의 공정함, 그리고 결과에 필요한 정보를 명확하게 제공하는 공정함 등으로 구분되어 활용되어 왔다[13].

공정성 분위기(Justice Climate)는 집단 내 구성원들이 느끼는 공정함에 대한 전체적인 인식으로서, 집단이 추구하는 공정함에 대한 가치에서부터 구성원들의 공정한 활동을 수행하려는 의지까지 포함되는 개

념이다[14]. 그러므로, 공정성 분위기는 특정 목표에 대한 정책 개발과 같이 조직의 단일 노력만으로 형성되는 것이 아닌, 대상 목표에 대한 공정성 가치 선언에서부터, 구성원들의 참여하려는 의지 및 지속적 행동으로 인해 형성된 암묵적인 행태까지 포함되어 공정성 분위기를 형성한다[15]. 또한, 형성된 공정성 분위기는 구성원 및 조직의 행동 가치를 결정하기 때문에 개인에게는 목표 달성 과정에 영향을 주고, 조직 전체의 성과를 향상하는 조건이다[16].

특히, 정보보안 분야에서 조직 공정성은 조직원의 정보보안 준수율에 긍정적 영향을 주는 조건으로 인식되어 왔다[4]. 조직이 도입한 정보보안 정책을 시행하는 과정에서 조직원은 자신에게 부여된 역할 및 결과에 대한 상대적 평가를 하며, 대우가 만족스러울 때 조직에 대한 믿음을 형성하여 정보보안 준수 행동으로 이어진다. 따라서, 정보보안 공정성 분위기를 형성하는 것은 구성원들의 자발적인 보안 행동을 기대하도록 한다.

2.3 정보보안 처벌

처벌은 조직의 특정 정책에 대한 구성원의 행동 강화와 관련되어 오랫동안 논의되었던 요인이다. 처벌(Sanction)은 개인이 집단이 요구하는 특정 활동에 대한 미준수 시 개인에게 부여된 페널티에 대한 언급 수준을 의미한다[2]. 처벌과 관련된 연구들은 처벌이 엄격하고 명료할수록, 대상자들은 자신의 이익을 극대화하기 위해서 또는 미준수 시 필요한 비용은 최소화를 위하여 요구사항을 이행하려는 경향을 보인다고 본다[17]. 특히, 정보보안은 조직이 직원에게 부여한 업무적 성과 달성과 같은 우선적 목표가 아닌 업무 수행과정에서 추가로 수행해야 할 행동 지침으로 인식되고 있고, 정보보안 준수에 의한 가치 확립보다 미준수에 의한 정보 노출에 대한 우려가 크기 때문에, 인센티브보다 페널티를 강조함으로써 개인의 행동 전환을 기대할 수 있다고 본다[18].

또한, 조직원의 정보보안 정책 준수에 대한 처벌은 공정성과 밀접한 관련이 있는데, 정보보안과 관련된 모든 사람이 동일한 문제에 대해 공정한 처벌을 받지 않을 경우, 조직 내 불공정성에 대한 우려를 발현시켜 조직에 대한 믿음을 상실하게 되는 경향을 보인다[5]. 따라서, 조직은 정보보안 규정 및 결과에 대한 행위를

문서화하고 명료한 행동을 통해 공정성을 확립함으로써, 모든 구성원이 당연히 정보보안 정책을 준수해야 한다는 믿음을 가지도록 하는 것이 요구된다[19].

2.4 정보보안 관련 커뮤니케이션

커뮤니케이션(Communication)은 집단의 구조 및 집단 내 행동에 대하여, 개인이 건설적이고 능동적인 행동을 지원하는 정보 지원 활동으로서[20], 조직 커뮤니케이션이 추구하는 목표는 구성원이 조직의 비전, 가치, 목표에서부터 조직이 구성원에게 요구하는 일상적 업무에 이르기까지 방향에 맞게 행동하도록 지원하는 것을 의미한다[21]. 즉, 커뮤니케이션은 조직의 특정 목표 달성을 위해서 조직원에게 달성을 위한 사전 정보 제공에서부터 상호 교환 활동을 지원함으로써 내부자들 간에 능동적으로 교류할 수 있도록 하는 것을 의미한다[22]. 정보 기술의 발전은 조직 내 구성원 간에 원활하고 쉽게 교류 활동을 할 수 있도록 하고 있다. 많은 조직이 온라인 미팅 시스템, 인트라넷, 소셜네트워크서비스 등을 지원하여 교환 대상자 간에 정보 및 지식을 교환하고 성과를 달성할 수 있도록 돕고 있다. 즉, 커뮤니케이션 활동의 증대는 대상자가 더욱 쉽게 목표를 달성할 수 있도록 돕는다[21].

정보보안과 관련하여, 개인의 보안 준수 행동은 정보보안에 대한 행위 정보를 명확하게 이해하고 있는 것이 요구되는데, 조직 차원의 커뮤니케이션 활성화는 정보보안의 가치와 행위 정보를 쉽게 확보할 수 있도록 돕는다[23]. 즉, 정보보안에 필요한 지식 등을 교류하고 쉽게 확보할 수 있도록 커뮤니케이션을 활성화할 때 조직 내 보안 수준을 높게 유지할 수 있다[24].

2.5 정보보안 관련 피드백

조직의 목표에 대한 조직원의 바람직한 행동을 이끌기 위해서는 당사자의 특정 활동에 대한 다각적 분석 등을 통해 정보를 제공함으로써, 특정 활동에 대한 이슈를 개선하여 중장기적으로 성과 달성에 기여하는 것이 필요하다[25]. 피드백(Feedback)은 개인에게 요구한 활동에 대한 과정, 결과를 정보화하여 제공하는 것을 지칭한다[25]. 피드백은 조직 내 동료(상사, 부하 등), 고객 및 파트너 등 본인과 연계된 다양한 이해관계자로부터 받을 수 있으며, 단순 정보부터 행동에 대한 성과, 평가 등을 포함하기 때문에, 특정 상황에서

개인의 행동 변화에 높은 영향을 주는 조건이다[26].

정보보안과 관련하여, 조직은 높은 수준으로 투자한 정보보안 정책, 기술 등을 내부자들이 체계적으로 활용하는 것을 기대하는데, 피드백 활동은 중장기적으로 당사자의 정보보안 준수 행동을 높일 수 있다[27]. 즉, 피드백은 정보보안 정책의 목표와 가치를 이해하도록 돕고, 정보보안 준수 행동 결과의 적정성과 개선 행동의 가이드라인까지 제공하기 때문에, 피드백이 체계적이고 높은 수준의 정보를 제공할수록 높은 수준의 내부 정보보안에 기여할 수 있다[28].

III. 연구가설 및 측정

3.1 연구모델

연구는 조직 내부자의 보안 준수를 위하여, 조직이 추진해야 할 구조적 방향성을 제언하는 것을 목적으로, 다음의 그림 1의 연구모델을 제시한다.

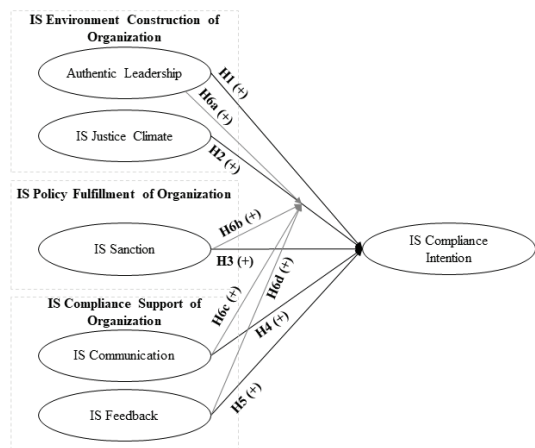


그림 1. 연구모델
Fig. 1 Research model

3.2 연구가설

3.2.1 진성 리더십과 준수 의도

조직에서 리더가 자신의 수준을 명확하게 인식하고, 구성원들과의 투명한 관계를 유지하고, 객관적 정보에 기반한 의사결정을 하고, 윤리적으로 바람직한 형태를 가질 때, 조직원들은 리더의 행동 가치를 자신

과 동일하게 판단하여, 조직 및 리더가 요구하는 목표를 달성하기 위해 기여하는 모습을 보인다[10]. 특히, 진성 리더십의 강화는 조직원 본인의 성과 달성에 도움을 줄 뿐 아니라[29], 조직의 혁신에 기여한다[30].

반대로, 진성 리더십은 조직 구성원들이 조직 환경으로부터 받는 스트레스를 완화하여 만족도를 높이거나 이직 의도를 감소시키는 역할을 한다[31]. 즉, 진성 리더십은 조직원의 행동을 조직의 목표와 동일하게 행동하도록 하는 역할을 한다. 따라서, 조직원의 정보보안 관련 행동에 대해 진성 리더십이 영향을 줄 것으로 판단하고, 연구가설을 제시한다.

H1. 진성 리더십은 내부자의 정보보안 준수 의도에 긍정적 영향을 미친다.

3.2.2 정보보안 공정성 분위기와 준수 의도

조직 내 특정 목표에 대해 형성된 전체적인 공정성 분위기는 참여자들의 긍정적인 행동을 기대하도록 한다. Walumbwa et al.[2010]은 리더십에 의해 형성된 조직 공정성 분위기는 조직원의 이타적 행동 개념인 조직시민행동을 높인다고 하였으며[14], Shin et al.[2015]은 조직 단위에서 형성시킨 공정성 분위기가 기업 단위의 재무적 성과까지 영향을 주는 것을 확인하였다[15].

특히, 정보보안과 관련하여 조직 공정성은 조직원 보안 준수에 영향을 준다. Lee and Hwang[2021]은 정보보안 관련 절차 및 정보 공정성은 개인의 정보보안 준수 동기에 영향을 주어 정보보안 제인 행동에 영향을 준다고 하였으며[4], Alshare et al.[2018]은 조직 공정성이 정보보안 회피 행동을 감소시킨다고 하였다[32]. 즉, 형성된 정보보안 관련 전체적인 공정성 분위기는 내부자의 보안 준수에 긍정적 영향을 줄 것으로 판단한다.

H2. 정보보안 공정성 분위기는 내부자의 정보보안 준수 의도에 긍정적 영향을 미친다.

3.2.3 정보보안 처벌과 준수 의도

정보보안 정책에 대한 명확하고 공정한 처벌은 조직원에게 미준수 행위에 대한 손해를 인식시켜 정보보안 준수 의도를 향상하는 역할을 한다. Sarkar et al.[2020]은 조직 내 처벌이 명확하고 심각할수록 정보보안 정책 준수 회피 행동을 감소시킨다고 하였으며

[18], Xue et al.[2011]은 정보보안 처벌에 대한 공정한 기대가 정보보안 준수 의도를 형성시킨다고 하였다[5]. 반대로, Vance et al.[2020]은 너무 엄격한 공식적, 비공식적 형태의 정보보안 처벌은 오히려 조직원의 반발을 일으켜 오히려 정보보안 정책을 회피하는 역할을 한다고 보았다[2]. 선행 연구를 요약하면, 정보보안 처벌이 충분히 지킬 수 있으며 공정한 형태로 제시될 경우 개인의 보안 준수 의도를 높일 수 있다. 이에 따라 다음의 연구가설을 제시한다.

H3. 정보보안 처벌은 내부자의 정보보안 준수 의도에 긍정적 영향을 미친다.

3.2.4 정보보안 커뮤니케이션과 준수 의도

조직이 특정 활동에 대한 목표를 달성하기 위해서는 당사자들의 능동적인 참여 행동이 무엇보다 요구된다. 조직 차원의 커뮤니케이션 제공은 관계자들의 상호 교류를 쉽게 할 수 있도록 함으로써, 관련 정보 및 지식 확보에 도움을 주며, 목표 달성에 기여한다[20]. 특히, 정보보안 정책, 기술 등과 관련된 다양한 정보에 대한 교류 활동의 제공(예: 캠페인, 동영상 제공, 이메일 지원 등)은 조직원의 정보보안 준수 의도를 높이는 데 기여한다[33]. 또한, 정보보안에 대한 커뮤니케이션 지원은 조직의 정보보안 문화를 형성시켜 개인의 정보보안 준수 행동 향상에 기여하며[24], 조직의 정보보안 관리체계를 확립시켜 정보보안 준수 성과 달성에 기여한다[34]. 따라서, 정보보안 커뮤니케이션 지원은 내부자의 정보보안 준수 의도 향상에 기여할 것으로 판단한다.

H4. 정보보안 커뮤니케이션 지원은 내부자의 정보보안 준수 의도에 긍정적 영향을 미친다.

3.2.5 정보보안 피드백과 준수 의도

조직 차원의 조직원에 대한 정보보안 활동 피드백 지원은 정보보안 준수 활동을 높이는 조건이다. D'Arcy and Lowry[2019]는 조직원의 정보보안 활동에 대한 지속적인 모니터링 및 행동 결과의 제공 활동은 조직원의 정보보안 준수 의도를 높이는 것을 확인하였으며[28], Hwang et al.[2017]은 정보보안 관련 장애로 인한 스트레스를 정보보안에 대한 기술적 지원이 완화할 수 있으며, 정보보안 준수 의도로 이어질 수 있음을 확인하였다[35]. Solomon and Brown[2021]

은 정보보안 문화 형성을 위해서는 정보보안 행동에 대한 모니터링을 통한 정보 피드백이 무엇보다 중요하며, 행동 개선에 기여한다고 하였다[24]. 즉, 정보보안 피드백 지원은 내부자의 정보보안 준수에 긍정적인 영향을 줄 것으로 판단한다.

H5. 정보보안 피드백 지원은 내부자의 정보보안 준수의도에 긍정적인 영향을 미친다.

3.2.6 정보보안 공정성 분위기 향상 조건

조직은 조직마다 특정한 분위기를 가진다. 분위기는 조직의 가치, 조직원들의 행동 등이 모여서 형성되지만, 형성된 분위기는 지속해서 소속되어 있는 사람들에게 영향을 준다[14]. 즉, 조직 내 문화, 분위기 등의 형성은 단순히 어느 하나의 조건에 의해 형성되는 것이 아니라 리더의 노력, 조직의 목표 및 정책, 분위기 형성을 위한 조직의 노력 등이 연계되고, 조직원이 받아들였을 때 높아질 수 있다[15]. 즉, 공정성 분위기는 조직 내 다양한 환경적 조건에 의해 영향을 받는다. Ja'afaru Bambale [2014]은 조직의 공정성 분위기가 구성원의 조직시민행동에 미치는 긍정적 영향을 조직에 대한 개인들의 동일시 및 적합성을 일으키는 요인들에 의해 조절적 영향을 받는다고 보았으며[36], 이러한 적합성에 대해 Kristof[1996]는 조직이 개인에게 적절한 정보 등 업무적 자원과 기회를 제공할 때, 보완적 적합성이 발현됨을 제시하였다[37]. 즉, 공정성 분위기는 추가로 조직이 개인에게 제공하는 업무적 환경, 자원, 그리고 기회 등으로 인한 동으로 인하여 동일시 환경이 갖추어질 때 행동의 변화를 일으킬 수 있다. 이에 본 연구는 조직 환경 및 구조, 그리고 지원 요소로 제시한 진성 리더십, 처벌, 커뮤니케이션, 그리고 피드백이 공정성 분위기가 개인의 준수의도에 미치는 긍정적 영향을 강화할 수 있을 것으로 판단한다.

H6a. 진성 리더십은 공정성 분위기가 준수의도에 미치는 영향을 조절한다.

H6b. 정보보안 처벌은 공정성 분위기가 준수의도에 미치는 영향을 조절한다.

H6c. 정보보안 커뮤니케이션은 공정성 분위기가 준수의도에 미치는 영향을 조절한다.

H6d. 정보보안 피드백은 공정성 분위기가 준수의도에 미치는 영향을 조절한다.

3.2 측정 도구 및 측정 방법

연구모델의 검증은 설문지 기법으로 확보한 데이터를 기반으로 양적 검증을 수행하고자 한다. 이에, 연구는 정보보안 및 조직 관련 선행연구에서 적용되었던 요인별 다항목 기반의 설문 문항을 정보보안 특성에 맞게 보완하여 활용하였다. 특히, 연구는 각 설문 문항을 리커트 척도를 적용하였으며, 매우 그렇지 않다(1점) - 매우 그렇다(7점)를 설문에 반영하였다.

진성 리더십은 2차 요인으로서, Neider and Schriesheim[2011] 연구를 바탕으로 문항을 도출하였다[10]. 자기인식은 4개 문항으로 구성되며, 우리 회사의 대표는 1) 본인의 문제를 인식하는 편임, 2) 본인의 강, 약점을 잘 인식하는 편임, 3) 본인의 능력을 잘 인식하는 편임, 4) 본인의 행동이 구성원에게 미치는 영향을 알고 있음과 같이 구성된다. 관계적 투명성은 4개 문항으로 구성되며, 우리 회사의 대표는 1) 본인의 특정 행동 이유를 제시하는 편, 2) 본인의 실수를 명확하게 인정하는 편, 3) 구성원들과 지식을 교류하는 편, 4) 공개로 본인의 생각을 표현하는 편으로 구성된다. 균형 잡힌 정보처리는 4개 문항으로 구성되며, 우리 회사의 대표는 1) 본인의 의견에 반대되는 것을 확인하는 편, 2) 다양한 의견을 잘 듣는 편, 3) 데이터를 활용하여 의견을 결정하는 편, 4) 구성원의 반대 의견을 청취하는 편으로 구성된다. 내재화된 도덕적 관점은 4개 문항으로 구성되며, 우리 회사의 대표는 1) 생각과 행동이 일치하는 편, 2) 믿음을 기반으로 의견을 결정하는 편, 3) 도덕적 믿음에 어긋난 것을 하는 것을 싫어하는 편, 4) 자신의 도덕적 신념에 따라 행동하는 편으로 구성된다. 공정성 분위기는 Ambrose and Schminke[2009]의 연구를 바탕으로 [13], “우리 회사는 구성원에게 공정한 정보보안에 대해 대우를 하고 있음”, “나는 우리 회사가 공정한 정보보안 관련 활동을 하고 있다고 믿음”, “우리 회사는 정보보안에 대하여 구성원에게 공평하게 대우하고 있음”과 같이 3개 문항을 반영하였다. 처벌은 Guo et al.[2011]의 연구를 바탕으로 [19], “우리 회사는 구성원의 보안 비준수 행위에 대한 제재를 엄격하게 시행함”, “회사의 정보보안 정책을 위반할 경우 제재를 받을 수 있음”, “우리 회사는 정보보안 정책을 위반할 경우 제재가 따름을 명시적으로 전달함”과 같이 3개 문항을 반영하였다. 커뮤니케이션은 Jiménez-Castillo

and Sánchez-Pérez[2013]의 연구를 바탕으로[21], “우리 회사는 정보보안 활동 정보를 전달하는 채널 또는 도구를 제공함”, “우리 회사는 정보보안의 필요성과 가치를 제공함”, “우리 회사는 다양한 내부 도구(그룹웨어 등)를 통해 정보보안 지침을 제공함”과 같이 3개 문항을 반영하였다. 피드백은 Wright[2004]의 연구를 바탕으로[25], “정보보안에 대한 성과 평가는 나의 업무를 개선하는 데 도움이 되었음”, “나는 정보보안 규정 준수를 위해 회사로부터 도움을 받음”, “나는 정보보안 규정을 수행하는 것에 대해 주변 동료들로부터 유용한 정보를 얻음”, “나는 정보보안 준수에 대한 강·약점 등의 평가를 받음”과 같이 4개의 문항을 반영하였다. 정보보안 준수 의도는 Chen et al.[2012]의 연구를 바탕으로[38], “나는 우리 회사의 정보보안을 지속해서 지킬 것”, “나는 우리 회사의 중요 정보를 보호할 가능성이 높음”, “나는 우리 회사의 보안 정책과 규정을 준수할 가능성이 있음”과 같이 3개 문항을 반영하였다.

표 1. 표본 특성
Table 1. Characteristics of samples

Categories		Frequency	Percentage
Gender	Male	328	77.9
	Female	93	22.1
Age	Under 30	59	14.0
	31 - 40	162	38.5
	41 - 50	156	37.1
	Over 51	44	10.5
Industry	Manufacturing	69	16.4
	Service	352	83.6
Job Position	Staff	162	38.3
	Assistant Manager	125	29.7
	Manager	128	30.4
	Over Manager	6	1.4
Firm Size	Under 10	67	15.9
	10~49	139	33.0
	50~299	53	12.6
	Over 300	162	38.5
Total		421	100.0

본 연구는 연구 대상을 정보보안 정책을 자사의 특성에 맞추어 개발하고, 조직 전반에 정책을 반영하고

있는 조직의 구성원으로 설정하였다. 설정된 연구 대상에 대한 설문을 명확하게 확보하기 위하여, 마크로 밀 엠브레인 리서치가 보유한 직장인 회원을 활용하였다. 연구는 설문을 수행하기 전, 본인의 회사가 정보보안 정책을 본인에게 적용하여 업무적으로 반영하는 것을 요구하는지를 확인한 후 설문에 응답하도록 구조화하였다. 특히, 연구는 온라인 설문을 설계하였으며, 설문 대상으로 선정된 사람들에게 연구의 목적, 데이터의 통계적 활용에 대한 정보를 제공하고, 이를 허가한 사람들만 본 설문에 참여하도록 하였다. 표본은 총 421개를 확보하였으며, <표 1>과 같은 표본의 특성을 확인하였다.

IV. 분 석

4.1 신뢰성 및 타당성

연구모델에 적용된 요인들은 선행연구에서 확보한 멀티 항목으로 구성된 측정 도구를 활용하였으므로, 우선 요인의 신뢰성 및 타당성 수준을 확인한다.

첫째, 신뢰성은 적용 요인이 일관성을 보유하고 있는지를 확인하는 것으로서, 본 연구는 사회과학에서 주로 활용되는 SPSS 21.0 툴에서 제공하는 크론바흐 알파 값을 활용하여 신뢰성을 확인한다. 관련 선행연구는 요인의 구성 항목들의 크론바흐 알파 0.7 이상의 값을 요구한다[39]. 신뢰성에 대한 결과는 <표 2>와 같으며, 연구모델에 적용된 모든 요인의 크론바흐 알파가 0.7 이상의 값인 것으로 나타났다.

둘째, 타당성은 적용 요인의 내적 일관성(집중 타당성)과 요인들의 차별성(판별 타당성)을 확인하는 것으로서, 본 연구는 AMOS 22.0 패키지를 적용하되, 2차 확인적 요인분석을 실행하여 집중 타당성과 판별 타당성을 확인하고자 하였다.

우선 모든 요인을 적용한 2차 확인적 요인분석 구조 모델의 적합성을 확인하였다. 결과는 $\chi^2/df = 1.588$, RMSEA = 0.037, GFI = 0.905, AGFI = 0.887, NFI = 0.948, TLI = 0.978, 그리고 CFI = 0.980과 같이 나타나, 구조방정식 모형의 적합도 요구사항을 모두 충족하였다.

표 2. 타당성 및 신뢰성
Table 2. Construct validity and reliability

Constructs		Loading	Cronbach's Alpha	CR	AVE
SA	SA1	0.801	0.888	0.807	0.511
	SA2	0.821			
	SA3	0.831			
	SA4	0.818			
RT	RT1	0.880	0.931	0.867	0.620
	RT2	0.882			
	RT3	0.869			
	RT4	0.883			
BP	BP1	0.878	0.932	0.867	0.620
	BP2	0.902			
	BP3	0.842			
	BP4	0.898			
MP	MP1	0.895	0.941	0.893	0.676
	MP2	0.912			
	MP3	0.878			
	MP4	0.889			
JC	JC1	0.894	0.935	0.892	0.733
	JC2	0.940			
	JC3	0.899			
San	San1	0.908	0.913	0.872	0.694
	San2	0.860			
	San3	0.876			
Com	Com1	0.872	0.923	0.883	0.717
	Com2	0.907			
	Com3	0.905			
Feed	Feed1	0.881	0.931	0.874	0.634
	Feed2	0.830			
	Feed3	0.905			
	Feed4	0.898			
CI	CI1	0.773	0.858	0.848	0.652
	CI2	0.882			
	CI3	0.856			
AL ^a	SA	0.945	0.931	0.928	0.763
	RT	0.932			
	BP	0.868			
	MP	0.915			

SA(Self Awareness), RT(Relational Transparency), BP(Balanced Processing), MP(Internalized Moral Perspective), JC(Justice Climate), San(Sanction), Com(Communication), Feed(Feedback), CI(Compliance Intention), AL(Authentic Leadership)

a = second construct (SA, RT, BP, MP)

집중 타당성은 평균분산추출(AVE)과 개념 신뢰도(CR) 값을 요인별 개별적으로 구하여 확인하는데, 선행연구는 요인의 평균분산추출이 0.5 이상, 개념 신뢰도가 0.7 이상의 값을 가질 때 집중 타당성을 확보했다고 본다[40]. 진성 리더십을 포함하여 모든 요인이 집중 타당성을 가진 것으로 나타났다<표 2>.

판별 타당성은 요인들이 상호 간 차이를 가지는지를 확인하는 것으로서, 선행연구는 적용 요인들의 상관계수와 평균분산추출을 비교하되 평균분산추출의 제곱근이 상관계수 전체보다 각자 크게 나타날 때, 판별 타당성을 확보하였다고 본다[40]. 판별 타당성을 확인한 결과는 <표 3>이며, 요인 간의 판별 타당성을 충족하였다.

표 3. 판별 타당성 결과
Table 3. Result for discriminant validity

Constructs	1	2	3	4	5	6
AL ^a	0.873 ^b					
JC	.66**	0.856 ^b				
San	.61**	.60**	0.833 ^b			
Com	.75**	.66**	.59**	0.847 ^b		
Feed	.67**	.54**	.52**	.61**	0.796 ^b	
CI	.62**	.58**	.51**	.61**	.59**	0.807 ^b

AL(Authentic Leadership), JC(Justice Climate), San(Sanction), Com(Communication), Feed(Feedback), CI(Compliance Intention)
a = second construct, b = square root of the AVE, **: p < 0.01

본 연구는 독립변수와 종속변수를 단일 시점에 설문지 기법으로 확인하였으므로, 각 변수의 편향 문제인 공통방법편의 문제가 있을 수 있다. 연구는 공통방법편의 수준 확인을 위하여 단일공통방법편의 방법을 적용하였다[41]. 방법은 기본 확인적 요인분석 모델에 추가로 단일 요인을 적용하고 측정치에 연계하였을 때, 모델 간의 측정값의 변화량이 작은지를 확인하는 것이다. 분석 결과, 두 모델 모두 요구사항을 충족하였으며, 항목별 측정값의 변화량이 0.3 미만으로 나타나 공통방법편의는 큰 문제가 아닌 것으로 나타났다.

4.2 주 효과

조직의 정보보안 구조 요인과 개인의 정보보안 준수의도 간의 관계 검증은 AMOS 22.0의 구조방정식 모형을 적용하였으며, 정보보안 공정성 분위기에 미치는 조절 효과 영향은 SPSS 21.0의 Process 3.1을 적

용하였다. 구조방정식 모형을 통한 검증은 주 효과 모델의 적합성, 연구모델 내 설정된 요인의 경로 분석의 절차를 수행한다.

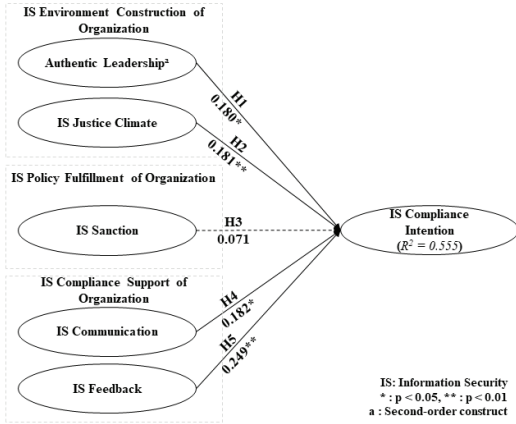


그림 2. 경로 분석(주 효과) 결과
Fig. 2 Results of main effect tests

표 4. 경로 분석(주 효과) 결과
Table 4. Results of main effect tests

	Path	Coefficient	t-value	Result
H1	AL ^a → CI	0.180	2.105*	Support
H2	JC → CI	0.181	2.845**	Support
H3	San → CI	0.071	1.183	Not Support
H4	Com → CI	0.182	2.284*	Support
H5	Feed → CI	0.249	4.006**	Support

AL(Authentic Leadership), JC(Justice Climate), San(Sanction), Com(Communication), Feed(Feedback), CI(Compliance Intention)
a = second construct
*: p < 0.05, **: p < 0.01

본 연구는 우선 주 효과 모델의 적합도를 확인하였다. $\chi^2/df = 1.603$, RMSEA = 0.038, GFI = 0.944, AGFI = 0.925, NFI = 0.969, TLI = 0.985, 그리고 CFI = 0.988과 같이 나타나, 모든 수치가 적합도 요구 사항을 충족하였다.

둘째, 연구는 모형 내 적용된 요인 간의 경로 검증(β)을 수행하였으며, 연구가설의 결과를 확인하였다. 가설 1은 진성 리더십이 조직 내부자의 정보보안 준수 의도에 영향을 준다는 것으로 요인 간의 경로를 확인한 결과, 신뢰수준 95%를 기준으로 채택되었다(H1: $\beta = 0.180$, $p < 0.05$). 가설 2는 정보보안 공정성 분위기가 조직 내부자의 정보보안 준수 의도에 영향을 준

다는 것으로 요인 간의 경로를 확인한 결과, 신뢰수준 99%를 기준으로 채택되었다(H2: $\beta = 0.181$, $p < 0.01$). 가설 3은 정보보안 처벌이 조직 내부자의 정보보안 준수 의도에 영향을 준다는 것으로 요인 간의 경로를 확인한 결과, 신뢰수준 95%를 기준으로 기각되었다(H3: $\beta = 0.071$, n.s.). 가설 4는 정보보안 커뮤니케이션이 조직 내부자의 정보보안 준수 의도에 영향을 준다는 것으로 요인 간의 경로를 확인한 결과, 신뢰수준 95%를 기준으로 채택되었다(H4: $\beta = 0.182$, $p < 0.05$). 가설 5는 정보보안 피드백이 조직 내부자의 정보보안 준수 의도에 영향을 준다는 것으로 요인 간의 경로를 확인한 결과, 신뢰수준 99%를 기준으로 채택되었다(H5: $\beta = 0.249$, $p < 0.01$).

마지막으로, 연구는 진성 리더십, 공정성 분위기, 처벌, 커뮤니케이션, 그리고 피드백이 정보보안 준수 의도에 미치는 영향력(R^2)을 확인하였다. 정보보안 준수 의도는 선행 요인으로부터 55.5%의 영향을 받았다.

4.3 조절 효과

본 연구는 정보보안 관련 공정성 분위기가 개인의 준수 의도에 미치는 영향을 조직 환경 구축의 타 요인(진성 리더십, 처벌, 커뮤니케이션, 그리고 피드백)이 조절 효과를 가져, 공정성 분위기에 의한 영향을 강화할 것으로 판단하였다.

연구는 Hayes[2017]가 제시한 Process 3.1을 활용하여, 요인들의 공정성 분위기와 준수 의도 간의 관계에 대한 조절 효과를 확인하였다[42]. Process 3.1에서 조절 효과 검증은 모델 1을 적용하였으며, 부트스트래핑 5,000(유의수준 5%)을 반영하였다. 결과는 진성 리더십, 처벌, 커뮤니케이션, 그리고 피드백 요인들은 각각 정보보안 공정성 분위기가 정보보안 준수 의도에 미치는 긍정적 영향에 조절 효과를 가지는 것으로 나타났다<표 5>.

연구는 진성 리더십, 처벌, 커뮤니케이션, 그리고 피드백이 공정성 분위기가 결과에 미치는 영향을 어떻게 조절하는지를 확인하기 위해, Process 3.1의 단순 기울기 그래프를 제시하였다.

표 5. 조절 효과 결과
Table 5. Results of moderating effect tests

		Coefficient	t-value	Result
H6a	Constant	5.009	115.392**	Support
	JC	0.240	6.062**	
	AL	0.310	6.651**	
	Interaction	-0.054	-2.226*	
	$F = 109.3734, R^2 = 0.4404$			
H6b	Constant	5.007	114.604**	Support
	JC	0.323	8.036**	
	San	0.204	4.854**	
	Interaction	-0.057	-2.374*	
	$F = 87.4448, R^2 = 0.3862$			
H6c	Constant	5.015	115.449**	Support
	JC	0.241	6.044**	
	Com	0.316	7.314**	
	Interaction	-0.059	-2.491*	
	$F = 108.1062, R^2 = 0.4375$			
H6d	Constant	5.014	124.824**	Support
	JC	0.274	7.767**	
	Feed	0.283	8.351**	
	Interaction	-0.065	-3.184**	
	$F = 118.1317, R^2 = 0.4594$			

AL(Authentic Leadership), JC(Justice Climate), San(Sanction), Com(Communication), Feed(Feedback), CI(Compliance Intention)
*: $p < 0.05$, **: $p < 0.01$

첫째, 공정성 분위기가 준수의도에 미치는 긍정적 영향에 있어, 공정성 분위기가 높은 집단에서 진성 리더십이 높을수록 준수의도가 강화되는 것을 확인하였다<그림 3>. 둘째, 공정성 분위기가 준수의도에 미치는 긍정적 영향에 있어, 공정성 분위기가 높은 집단에서 처벌 인식이 높을수록 준수의도가 강화되는 것을 확인하였다<그림 4>.

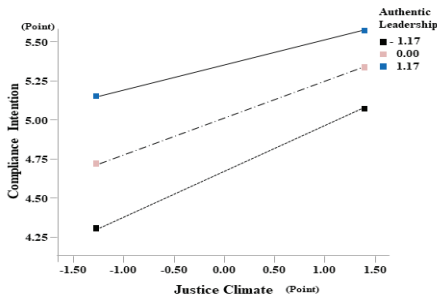


그림 3. 진성 리더십 조절 효과 (H6a)
Fig. 3 Moderation effect of al (H6a)

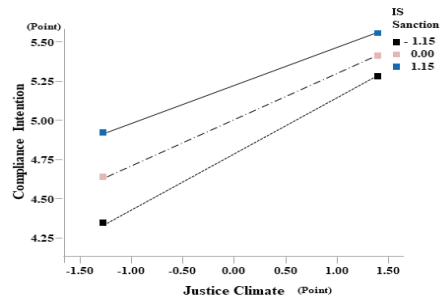


그림 4. 처벌 조절 효과 (H6b)
Fig. 4 Moderation effect of sanction (H6b)

셋째, 공정성 분위기가 준수의도에 미치는 긍정적 영향에 있어, 공정성 분위기가 높은 집단에서 커뮤니케이션 지원 수준이 높을수록 준수의도가 강화되는 것을 확인하였다<그림 5>. 마지막으로, 공정성 분위기가 준수의도에 미치는 긍정적 영향에 있어, 공정성 분위기가 높은 집단에서 피드백 수준이 높을수록 준수의도가 강화되는 것을 확인하였다<그림 6>.

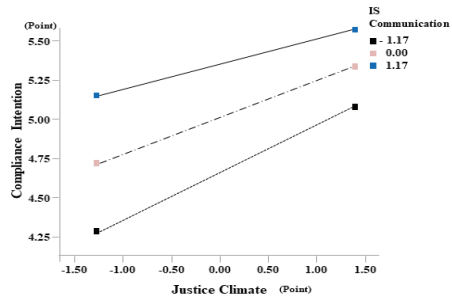


그림 5. 커뮤니케이션 조절 효과 (H6c)
Fig. 5 Moderation effect of communication (H6c)

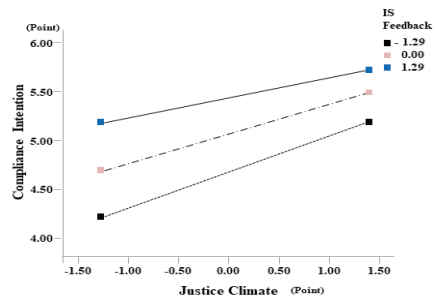


그림 6. 피드백 조절 효과 (H6d)
Fig. 6 Moderation effect of feedback (H6d)

V. 결 론

본 연구는 내부자의 정보보안 관리 체계에 대한 사회적 요구가 높아지는 상황에서, 조직 차원에서 구축한 정보보안 정책 및 기술을 조직원의 업무에 능동적으로 적용할 수 있도록 지원하기 위한 조직의 노력 체계를 제시하고자 하였다. 이를 위해, 연구는 정보보안에 대한 조직 환경 구축 측면(진성 리더십, 정보보안 공정성 분위기), 정보보안 정책 이행 측면(처벌), 그리고 정보보안 준수 지원 측면(커뮤니케이션, 피드백)으로 구분하여 개인의 보안 준수 행동에 영향을 주는 조건을 제시하고, 정보보안 공정성 분위기가 개인의 보안 행동에 미치는 영향을 강화할 수 있는 요인이 무엇인지 앞서 제시한 조직 보안 환경 및 지원 체계 요인을 적용하여 확인하고자 하였다.

본 연구는 정보 보호를 위해 관련 정책과 기술을 도입한 기업에 근무하는 사람을 연구 대상으로 하였으며, 설문지 기법으로 확보한 421개의 유효 표본을 활용하여 가설 검증을 하였다. 주 효과 분석은 구조방정식 모형을 적용하였으며, 조절 효과 분석은 Process 3.1을 적용하였다. 결과는 진성 리더십, 정보보안 공정성 분위기, 정보보안 커뮤니케이션, 그리고 피드백이 개인의 준수도에 긍정적 영향을 주었으며, 진성 리더십, 처벌, 커뮤니케이션, 그리고 피드백이 정보보안 공정성 분위기가 개인에게 주는 영향을 강화하였다.

본 연구의 결과는 다음의 연구적, 실무적 의미를 지닌다. 첫째, 연구는 조직 환경 구축 요인으로 진성 리더십을 제시하였다. 진성 리더십은 오늘날 사회가 기업에 요구하는 윤리적, 정보적 활동 등을 리더가 충분히 보유하고, 행동으로 보여주는지를 확인하는 요인으로서, 리더가 자신의 강점과 약점을 명확하게 인지하고, 조직원과 함께하려고 하며, 객관적 정보에 기반한 공정한 행동을 하며, 윤리적으로 문제가 없는 리더십을 의미한다. 진성 리더십 관련 선행연구가 조직 만족도 및 성과 분야에 중점적으로 관심을 두었다면, 본 연구는 정보보안 분야에 진성 리더십을 반영하여 조직원의 행동 변화에 영향을 주는 조건임을 확인한 차원에서 연구적 의미를 지닌다. 또한, 실무적 관점에서 꼭 정보보안과 관련된 조건이 아니더라도 리더가 사회적 바람직성과 공정성에 기반한 행동 가치를 조직원에게 보여줄 필요가 있음을 확인한 측면에서 의미

를 지닌다.

둘째, 연구는 조직 보안 환경 구축 요인으로 정보보안 공정성 분위기를 제시하였다. 동일 업종의 기업이라도 조직 내 분위기의 차이는 구성원의 행동 차이를 발생시킨다. 정보보안과 관련 공정성 선행 연구가 공정성의 직접적인 영향을 중점적으로 확인하였다면, 본 연구는 본 연구는 공정성 분위기의 긍정적 영향을 확인하고, 공정성 분위기 향상을 위한 조절 조건을 확인한 측면에서 연구적 의미를 지닌다. 또한, 실무적 관점에서 정보보안 관련 공정성 분위기 형성을 위해 조직이 제공해야 할 사전 정보, 절차, 그리고 결과의 공정함의 중요성을 인식할 때 행동을 강화할 수 있다는 것을 확인한 측면에서 의미를 지닌다.

셋째, 연구는 보안 정책 이행 관점에서 정보보안 처벌 요인을 적용하였다. 처벌은 조직이 가장 손쉽게 수행하고 단기적으로 성과를 확인할 수 있는 보안 이행 조건으로 알려져 있다. 하지만, 몇몇 선행연구와 유사하게 본 연구에서는 처벌이 명확하고 심각할수록 보안 준수도에 영향을 주지 못하는 것으로 나타났다. 이러한 결과는 처벌은 단기적으로 영향을 줄 수 있으나 장기적으로 개인에게 부담을 가질 수 있는 요인으로 회피 행동으로 이어질 수 있음을 의미한다. 따라서 조직 차원에서 정보보안 처벌의 수준을 명확하게 인식하고 문제 대처를 할 수 있도록 하는 것이 요구된다. 즉, 처벌로 인해 변화하는 개인행동을 확인한 측면에서 연구적 의미를 가진다. 또한, 실무적 관점에서 본 연구는 조직이 정보보안 처벌에 대한 인식을 전환하고 조직원 관점에서 고려해야 함을 제시하였다. 따라서, 조직은 조직의 환경과 보안 관리체계에 맞는 처벌 체계를 구축하는 것이 요구된다.

넷째, 연구는 정보보안 수행 지원 관점에서 정보보안 커뮤니케이션을 적용하였다. 커뮤니케이션은 교환대상자 간 정보, 지식 등의 교류가 활발하게 이루어지도록 돕는 전체적인 수준으로서, 커뮤니케이션 활동이 강화될수록 대상에 대한 개인들의 지식, 경험 수준이 높아지게 된다. 커뮤니케이션 관련 선행 연구가 지식 관리 또는 조직 운영 쪽에 관심을 두었다면, 본 연구는 정보보안에 대한 조직의 커뮤니케이션 활동이 개인에게 영향을 줄 수 있음을 확인한 측면에서 연구적 의미를 지닌다. 또한, 실무적으로, 조직은 조직원이 정보보안 정보를 명확하게 파악하고, 현장에서 어떻게

보안 행동을 할지를 결정할 수 있도록, 공식적, 비공식적인 보안 정보 제공 채널을 확대할 필요가 있음을 확인하였으며, 정보보안 관련 캠페인 등 정보보안의 필요성과 가치를 인식시키기 위한 노력이 요구됨을 제시하였다.

다섯째, 연구는 정보보안 지원 관점에서 정보보안 피드백을 제시하였다. 피드백은 개인이 특정 활동에 대한 수준, 평가까지 포함하므로 중장기적으로 성과에 기여하는 요인이다. 특히, 정보보안 준수 활동은 보안 환경의 급격한 변화에 능동적인 대처를 요구하는데, 피드백 활동은 조직원의 대처를 강화할 수 있다는 관점에서 의미를 지닌다. 피드백 관련 선행연구가 개인 성과 관점에서 주된 관심을 보였다면, 본 연구는 정보보안 분야에 피드백이 준수 수준을 높일 수 있음을 확인한 관점에서 연구적 의미를 지니며, 정보보안 활동에 대한 모니터링 및 결과에 대한 객관적 정보 제공, 행동 개선 방향 등을 제시하는 피드백 활용의 필요성을 제시한 측면에서 실무적 의미를 지닌다.

마지막으로, 본 연구는 정보보안 공정성 분위기 강화 방안을 제시하였다. 정보보안 선행연구는 공정성의 직접적인 영향을 중점적으로 제시했다면, 본 연구는 앞서 제시한 진성 리더십, 처벌, 커뮤니케이션, 그리고 피드백이 각각 공정성 분위기와 상호작용 효과를 가져, 개인 보안 행동에 미치는 영향을 강화할 수 있는 조건임을 확인하였다. 특히, 처벌의 경우 개인의 정보보안 준수에는 영향을 주지 못했지만, 정보보안 공정성 분위기가 형성된 상태에서 처벌의 명확성이 연계될 경우 개인의 행동을 전환할 수 있음을 확인하였다. 즉, 조직의 정보보안 공정성 분위기는 한 부분의 노력만으로 강화되는 것이 아니라, 리더십, 정책 이행, 커뮤니케이션 및 피드백과 같은 전반적인 보안 행동 강화를 위한 조직의 다각적 지원이 있을 때, 높은 영향을 발휘할 수 있음을 의미한다.

본 연구는 조직의 정보보안 목표에 대한 관리 체계 관점에서 조직원의 보안 행동 개선에 대한 방향을 제시한 시사점이 있으나, 다음의 연구적 한계를 지니고 있으며 향후 보완될 필요성 있다. 첫째, 연구는 표준화 관점에서 정보보안 정책을 보유한 집단에 소속된 조직원을 대상으로 설문하였다. 비록 결과 분석을 통해 유의미한 시사점을 제언하였으나, 조직 내 개인의 위치(직무, 업력 등)에 따라 정보 관리 이해도 등의

차이가 있을 수 있으며, 개인이 보유한 성향에 따라 정보보안에 접근하는 방식의 차이가 존재할 수 있다. 따라서, 향후 연구가 조직 내 개인의 위치 및 성향 등을 세분화하여 접근한다면 세심한 결론 및 접근 방향을 제공할 수 있을 것이다. 둘째, 연구는 조직 구분을 서비스업과 제조업으로 구분하였다. 하지만, 서비스업에서도 금융, 엔터테인먼트, 공공 등 성격이 상이하고 관리하는 정보의 유형이 다른 업종이 존재한다. 따라서, 향후 연구가 업종별 분화된 접근을 통해 개인의 행동 변화를 연구한다면, 업종별 접근 방향을 달리할 수 있는 정보를 제공할 수 있을 것이다. 마지막으로, 본 연구는 설문을 통해 개인의 행동 의도를 측정하였으나, 사회적 바람직성 등에 의한 편차를 무시할 수 없다. 따라서, 향후 연구에서는 행동 변화를 실제로 측정할 수 있는 연구를 진행하여 정보 관리 상황에서 개인의 행동 변화를 확인하는 것이 요구된다.

References

- [1] X. Ma, "IS professionals' information security behaviors in Chinese IT organizations for information security protection," *Information Processing & Management*, vol. 59, no. 1, 2022, pp. 102744.
- [2] V. Vance, M. T. Siponen, and D. W. Straub, "Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures," *Information & Management*, vol. 57, no. 4, 2020, pp. 103212.
- [3] Verizon, "2021 data breach investigations report," *Report*, Dec. 2021.
- [4] W. Lee and I. Hwang, "Sustainable information security behavior management: An empirical approach for the causes of employees' voice behavior," *Sustainability*, vol. 13, no. 11, 2021, pp. 6077.
- [5] 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.
- [6] M. Kajtazi, H. Cavusoglu, I. Benbasat, and D. Haftor, "Escalation of commitment as an antecedent to noncompliance with information security policy," *Information & Computer Security*,

- vol. 26, no. 2, 2018, pp. 171-193.
- [7] L. Dahabiyeh, "Factors affecting organizational adoption and acceptance of computer-based security awareness training tools," *Information & Computer Security*, vol. 29, no. 5, 2021, pp. 836-849.
- [8] I. Hwang, "The influence on the information security stressor on information security compliance intention: Focusing on the moderation of authentic leadership," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 16, no. 6, 2021, pp. 1101-1112.
- [9] F. O. Walumbwa, B. J. Avolio, W. L. Gardner, T. S. Wernsing, and S. J. Peterson, "Authentic leadership: Development and validation of a theory-Based measure," *J. of Management*, vol. 34, no. 1, 2008, pp. 89-126.
- [10] L. L. Neider and C. A. Schriesheim, "The authentic leadership inventory (ALI): Development and empirical tests," *The Leadership Quarterly*, vol. 22, no. 6, 2011, pp. 1146-1164.
- [11] J. A. Colquitt, R. A. Noe, and C. L. Jackson, "Justice in teams: Antecedents and consequences of procedural justice climate," *Personnel Psychology*, vol. 55, no. 1, 2002, pp. 83-109.
- [12] J. S. Adams, *Inequity in social exchange*, In *Advances in Experimental Social Psychology*. New York: Academic Press, 1965.
- [13] 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.
- [14] F. O. Walumbwa, C. A. Hartnell, and A. Oke, "Servant leadership, procedural justice climate, service climate, employee attitudes, and organizational citizenship behavior: A cross-level investigation," *J. of Applied Psychology*, vol. 95, no. 3, 2010, pp. 517-529.
- [15] Y. Shin, S. Sung, J. Choi, and M. Kim, "Top management ethical leadership and firm performance: Mediating role of ethical and procedural justice climate," *J. of Business Ethics*, vol. 129, no. 1, 2015, pp. 43-57.
- [16] I. Hwang, "The effect on the IS psychological empowerment on the mitigation of IS policy resistance through IS role stress: Focusing on the moderation of IS justice climate," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 17, no. 1, 2022, pp. 1-12.
- [17] G. D. Moody, M. Siponen, and S. Pahlila, "Toward a unified model of information security policy compliance," *MIS Quarterly*, vol. 42, no. 1, 2018, pp. 258-311.
- [18] S. Sarkar, A. Vance, B. Ramesh, M. Demestihas, and D. T. Wu, "The influence of professional subculture on information security policy violations: A field study in a healthcare context," *Information Systems Research*, vol. 31, no. 4, 2020, pp. 1240-1259.
- [19] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: A composite behavior model," *J. of Management Information Systems*, vol. 28, no. 2, 2011, pp. 203-236.
- [20] J. R. Edwards and D. M. Cable, "The value of value congruence," *J. of Applied Psychology*, vol. 94, no. 3, 2009, pp. 654-677.
- [21] D. Jiménez-Castillo and M. Sánchez-Pérez, "Nurturing employee market knowledge absorptive capacity through unified internal communication and integrated information technology," *Information & Management*, vol. 50, no. 2, 2013, pp. 76-86.
- [22] M. Welch and P. R. Jackson, "Rethinking internal communication: A stakeholder approach," *Corporate Communications: An Int. J.*, vol. 12, no. 2, 2007, pp. 177-198.
- [23] R. West, "The psychology of security," *Communications of the ACM*, vol. 51, no. 4, 2008, pp. 34-40.
- [24] G. Solomon and I. Brown, "The influence of organisational culture and information security culture on employee compliance behaviour," *J. of Enterprise Information Management*, vol. 34, no. 4, 2021, pp. 1203-1228.
- [25] B. E. Wright, "The role of work context in work motivation: A public sector application of goal and social cognitive theories," *J. of Public Administration Research and Theory*, vol. 14, no. 1, 2004, pp. 59-78.
- [26] M. C. Andrews and K. M. Kacmar, "Confirmation and extension of the sources of feedback scale in service-based organizations," *J. of Business Communication*, vol. 38, no. 2, 2001, pp. 206-226.

- [27] I. Hwang, "The effect of information security delivery activities and feedback on work impediment and compliance intention," *J. of Digital Contents Society*, vol. 21, no. 9, 2020, pp. 1653-1663.
- [28] J. D'Arcy and P. B. Lowry, "Cognitive affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study," *Information Systems J.*, vol. 29, no. 1, 2019, pp. 43-69.
- [29] H. Leroy, M. E. Palanski, and T. Simons, "Authentic leadership and behavioral integrity as drivers of follower commitment and performance," *J. of Business Ethics*, vol. 107, no. 3, 2012, pp. 255-264.
- [30] H. Elrehail, O. L. Emeagwali, A. Alsaad, and A. Alzghoul, "The impact of transformational and authentic leadership on innovation in higher education: The contingent role of knowledge sharing," *Telematics and Informatics*, vol. 35, no. 1, 2018, pp. 55-67.
- [31] M. Weiss, S. Razinskas, J. Backmann, and M. Hoegl, "Authentic leadership and leaders' mental well-being: An experience sampling study," *The Leadership Quarterly*, vol. 29, no. 2, 2018, pp. 309-321.
- [32] K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance: A higher education case study," *Information & Computer Security*, vol. 26 no. 1, 2018, pp. 91-108.
- [33] M. Siponen, S. Pahlila, and M. A. Mahmood, "Compliance with information security policies: An empirical investigation," *Computer*, vol. 43, no. 2, 2010, pp. 64-71.
- [34] L. Alzahrani and K. P. Seth, "The impact of organizational practices on the information security management performance," *Information*, vol. 12, no. 10, 2021, pp. 398.
- [35] 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, 2017, pp. 2-18.
- [36] A. Ja'afaru Bambale, "Relationship between servant leadership and organizational citizenship behaviors: Review of literature and future research directions," *J. of Marketing & Management*, vol. 5, no. 1, 2014, pp. 1-16.
- [37] A. L. Kristof, "Person organization fit: An integrative review of its conceptualizations, measurement, and implications," *Persomel Psychology*, vol. 49, no. 1, 1996, pp. 1-49.
- [38] 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.
- [39] J. C. Nunnally, *Psychometric theory (2nd ed.)*. New York: McGraw-Hill, 1978.
- [40] 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.
- [41] P. M. Podsakoff, S. B. MacKenzie, J. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *J. of Applied Psychology*, vol. 88, no. 5, 2003, pp. 879-903.
- [42] 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
(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