Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 10 pp. 598-609, 2023

https://doi.org/10.5762/KAIS.2023.24.10.598
ISSN 1975-4701 / eISSN 2288-4688

정보보안 이미지 및 인센티브 민감성의 역할: 조직 공정성과 역할 정체성에 대한 조절 효과

황인호
국민대학교 교양대학

The Role of Sensitivities to Information Security Image and Incentive: The Moderation Effects on Organization Justice and Role Identity

Inho Hwang
College of General Education, Kookmin University

요 약 정보보안이 조직을 넘어 사회적 문제로 확산하면서, 국가적으로 보안 관련 법률 및 정책이 제정 및 운영되고 있다. 특히, 최근에는 내부자, 즉 사람에 의한 정보 노출에 대한 위협 최소화를 위한 정책 및 시스템 구축을 요구하고 있다. 본 연구는 개인의 행동은 조직 환경과 행동 관련 민감성 수준에 영향을 받음을 고려하여, 정보보안 준수 이미지 및 인센티브 민감성, 조직 공정성, 그리고 역할 정체성을 연계한 개인의 보안 행동 메커니즘을 제시한다. 보안 행동 관련 메커니즘을 확인하기 위해, 선행연구를 통해 연구 모델을 제시하였으며, 정보보안 정책을 업무에 반영하고 있는 기업의 근로자에게 온라인 설문을 통해 데이터를 확보하였다. 그리고, 가설 검정은 AMOS 22.0의 구조방정식 모델링과 Process 3.1 매크로를 적용하였다. 검정 결과, 조직 공정성이 역할 정체성을 통해 제언 행동에 긍정적 영향을 주었으며, 이미지 및 인센티브 민감성이 제언 행동의 원인 요인과 상호작용 효과를 가지는 것으로 나타났다. 연구 결과는 내부자의 건설적인 보안 행동을 강화하는 방안을 제시함으로써, 조직 내부의 목표 달성을 위한 보안 전략 수립에 기여한다.

Abstract As the issue of information security (IS) extends beyond organizations and becomes a societal concern, national laws and policies are being implemented which require organizations to comply with measures aimed at minimizing the risk of information exposure by insiders. In this study, we propose a research model to examine the mechanisms underlying individual IS voice behavior, specifically focusing on the relationship between the IS compliance image and incentive sensitivity, IS organization justice, and IS role identity. To test our hypotheses, we collected data through an online survey of employees working in companies that adhere to IS policies. We utilized the SPSS® Amos™22.0 software and Process 3.1 macro for testing the hypothesis. Our findings revealed that IS organization justice positively influences the IS voice behavior through the IS role identity, and that image and incentive sensitivity interact with the antecedents of IS voice behavior. These results contribute to the development of strategies aimed at achieving IS objectives within organizations by suggesting ways to promote constructive IS behavior among insiders.

Keywords : Compliance Intention, Sensitivity to Incentive, Sensitivity to Image, Organization Justices, Role Identity

*Corresponding Author : Inho Hwang(Kookmin Univ.)
email: hwanginho@kookmin.ac.kr
Received September 1, 2023 Revised October 5, 2023
Accepted October 6, 2023 Published October 31, 2023

1. 서론

정보보안에 대한 관심이 높아지면서, 국가들은 조직의 정보보호 체계 구축에 대한 법규들을 속속히 도입하고 있다. 우리나라는 정보통신망법과 개인정보보호법을 제정하여 운영하고 있으며, 정보보호 및 개인정보보호 관리체계 인증(ISMS-P) 정책을 통해, 개인정보를 활용하는 기업의 인증을 법적으로 요구하고 있다[1]. 글로벌 기업들은 정보보호 관리체계 인증인 ISO 27001을 확보하여, 투자자, 소비자 등 이해관계자에게 정보보안 활동 수준을 증명하고 있으며[2], 미국 행정부는 제로 트러스트(Zero-trust) 관점의 접근을 요구하고 있다. 즉, 보안 관련 모든 상호작용이 신뢰 불가능한 상태에서 시작되어야 하며, 내외부의 정보 노출 가능성을 사전에 차단하는 노력을 요구한다[3]. 즉, 정보보안은 조직의 문제를 넘어, 이제는 국가적 이슈로 인식되며, 모든 이해관계자에 대한 엄격한 정보 관리를 요구하고 있다[4].

사람의 보안 준수 행동 중요성을 제기한 연구들은 외부 침입은 방화벽 등 관련 기술 강화를 통해 해결할 수 있으나, 정보시스템에 접근 가능한 사람은 언제든 정보 노출이 가능할 뿐 아니라 개인별 통제가 매우 어려움을 지적하며, 보안 준수 행동 강화를 위한 지원이 필요함을 주장하고 있다. 선행연구들은 제재 이론(Deterrence Theory), 합리적 선택이론(Rational Choice Theory), 보호 동기 이론(Protection Motivation Thoery), 계획된 행동이론(Theory of Planned Behavior)등 접근 방식의 차이는 있으나, 심리적 접근을 통해 보안 준수 의지를 높이는 노력이 선행되어야 함을 설명했다[1,5-8]. 최근에는 역설적으로 강압적이고 높은 수준의 보안 준수에 대한 요구는 조직원의 부정적 감정을 형성시켜 회피 행동을 발현시킬 수 있음을 지적하고 있다[9]. 선행연구는 개인의 보안 행동은 심리적으로 긍정적 또는 부정적 동기 형성에 기인하므로, 조직은 맞춤형 환경 및 지원 체계를 구축하는 것이 필요함을 제시한 측면에서 높은 시사점을 가진다.

반면, 조직 내 개인의 행동 원인을 확인한 연구들은 조직 환경 또는 개인의 동기 등이 행동에 영향을 주는 조건들은 개인 특성과 연계되어 반영됨을 밝히고 있다. 스트레스 환경에서 개인들은 자신만의 대처(Coping) 방식을 추진하거나[10], 상이한 문제 해결 방법인 조절 초점(Regulatory Focus) 유형에 따라 다른 행동 방식을 취하기도 한다[9]. 정보보안과 관련하여, 권한, 불확실성 회피, 그리고 개인주의/집합주의와 같은 개인차 요인[7], 또는 개인이 보유한 대인 간 민감성 수준[11] 등에 따라 개인의 보안 정책 준수 행동이 변화하기도 한다. 즉, 개인 특성 요인은 조직이 개인에게 요구하는 활동에 대한 선행 조건과 상호 영향 관계에 있을 수 있다. 하지만, 정보보안 선행연구는 보안 환경 또는 개인 동기를 설명함에 주력하여, 보안 행동에 영향을 줄 수 있는 개인 요인의 영향과 관련된 연구는 부족한 상황이다.

본 연구는 조직에서 개인들의 행동은 외부의 평판과 보상 평가가 중요한 요소가 되며 각각의 민감성의 수준에 따라 차별적 행동을 보일 수 있음을 고려하여[12], 정보보안에 이미지 민감성(Sensitivity to Image)과 인센티브 민감성을 반영하고, 능동적 보안 이슈에 대한 의견 개진 행동인 제언 행동의 원인 요소와의 관련성을 제시하고자 한다. 첫째, 보안 관련 조직 환경과 개인의 인식, 그리고 행동 간의 메커니즘을 제시한다. 개인의 특정 행동은 조직에서 지원 체계 및 보상이 공정할 때 높아질 수 있으며[2], 맡은 역할에 대한 정체성이 확립될 때 해당 역할에 대한 목표 달성 행동을 강화할 수 있다[13]. 즉, 보안과 관련된 공정 환경이 개인의 보안에 대한 역할 정체성을 통해 제언 행동으로 연계될 수 있으며, 관련 메커니즘의 관계를 증명하고자 한다. 둘째, 이미지 민감성과 인센티브 민감성이 제언 행동에 영향을 주는 선행 요인에 대해 조절 역할을 하는지 확인한다. 지식공유와 관련된 주위의 이미지와 행동 결과에 대한 인센티브의 민감성은 조직 환경 개인 인식 조건과 연계하여 행동을 변화시킬 수 있는데[12], 정보보안에도 적용될 수 있는지를 확인하고자 한다. 연구 결과는 정보보안 환경 및 개인의 인식, 그리고 개인 특성 조건이 상호 연계되어 영향을 줄 수 있음을 밝힘으로써, 조직 내부의 보안 목표 달성을 위한 맞춤형 전략 수립에 기여할 것으로 기대한다.

2. 이론적 배경

2.1 정보보안 제언 행동

조직의 정보보안에 대한 중요성이 높아지면서, 일찍부터 대상별 맞춤형 정보보안 예방 및 제어 체계의 필요성이 제기되어 왔다. Loch et al.[1992]은 인간-비인간(기술), 내부-외부가 반영된 프레임워크를 제시하고 예방 절차를 제시하였다. 비인간에 의한 내부 침입과 인간에 의한 외부 침입은 보안 기술의 강화를 통해 해결할 수 있으며, 비인간에 의한 외부 침입은 자연재해와 관련된 개념이므로 발생하기 어려운 문제라 보았다[14]. 반면 인간의

내부 침입은 정보시스템을 활용하여 업무의 효율성을 높이고자 하는 이슈와 연계되며, 업무 과정에서 보안 활동이 반영되므로, 보안행동 정보 전반을 조직이 파악하지 못하는 문제가 발생함을 지적하였다[14]. West[2008]는 정보보안에 대한 개인들의 긍정적 심리 형성을 통한 조직원의 준수 행동을 확보하고, 정보 자원을 보호해야 함을 지적하였다[15].

본 연구는 개인 중심의 보안 준수 행동에서 벗어나, 조직 전체의 보안 수준 확립을 위해 업무 수행 과정에서 발생 가능한 이슈에 대한 건설적 의견 개진 행동인 제언 행동(Voice Behavior)을 정보보안에 적용한다. 제언 행동은 공동의 목표에 대해 발생 가능한 문제점을 확인하고, 주변 동료들과 교류하여 문제를 해결하는 행동 전반을 말한다[16,17]. 내부의 정보보안 목표를 지속해서 유지하기 위해서는 개인 중심의 준수 행위를 벗어나, 환경 변화 과정에서 발생할 수 있는 보안 이슈를 능동적으로 해결하는 행동이 필요하다[2]. 이에, 본 연구는 조직 공정 환경, 역할 정체성, 그리고 개인의 보안 관련 민감성이 제언 행동에 미치는 영향 관계를 제시하여 조직의 보안전략 수립에 기여하고자 한다.

2.2 정보보안 역할 정체성

정체성(Identity)은 사회 구조에서 개인이 차지하는 부분에 부여된 일련의 의미로서, 집단과 개인 간의 상호작용 관점에서 유래된 인식의 개념이다[18]. 즉, 개인은 집단과의 상호작용 과정에서 본인의 위치를 결정하도록 의미를 부여하는데, 유사한 특성의 공유하는 관계 또는 역할 등에서 본인의 의미를 확립하게 된다[19]. 역할 정체성(Role Identity)은 개인이 사회 구조에서 어떠한 역할을 하고 있는지를 확인하고 자신에게 의미를 부여하는 개념으로서, 특정 역할에 대해 나는 누구이며, 어떻게 행동함으로써 사회 구조에 포함되는지를 확인하는 관점이다[20]. 조직에서 역할 정체성은 개인이 조직으로부터 요구받은 역할에 대해 어떻게 행동하는 것이 맞은 가에 대한 의미를 부여하는 과정이며, 역할에 대한 정체성을 확립함으로써 조직 구성원으로서 인식 및 행동을 하게 된다[21]. 정보보안 역할 정체성(IS Role Identity)은 동일한 맥락에서 정보보안 상황에서 개인이 어떠한 행동을 하는 것이 조직과 개인에게 의미가 있을지를 고려하는 것으로서, 조직이 요구하는 정보 자원 관리 정책의 준수에 대한 역할의 필요성을 인식하는 상황을 의미한다[13].

역할 정체성이 확립된 사람은 조직이 개인에게 요구하는 역할에 대한 행동을 보여줌으로써, 구성원임을 인식시키고자 한다. Ma and Agarwal[2007]은 온라인 커뮤니티에 대한 개인의 정체성 확립은 커뮤니티에서 지식 기여 활동을 함으로써, 구성원임을 다른 사람들에게 알리고자 함을 확인하였으며[21], Ray et al.[2014] 또한 온라인 커뮤니티에 대한 동일성과 정체성 확립은 커뮤니티 만족도를 형성하여 나아가 긍정적인 지식 기여 행동을 보임을 확인하였다[22]. 정보보안과 관련하여, Ogbanufe[2021]은 정보보안에 대한 조직원의 역할 정체성 확립이 조직에서 개인의 위치를 확립시키기 위하여 정보보안 정책 행동을 보임을 확인하였다[13]. 선행연구는 조직에서 개인이 부여받은 역할에 대한 의미부여 등을 통해 확립한 정체성은 긍정적 행동을 유발하는 원인임을 설명한다. 이에, 정보보안 역할 정체성이 조직을 위한 보안 관련 제언 행동에 긍정적 영향을 줄 것으로 판단하며, 다음의 가설을 제시한다.

H1 : 정보보안 역할 정체성은 정보보안 제언 행동에 긍정적 영향을 준다.

2.3 정보보안 조직 공정성

조직 공정성(Organization Justice)은 조직이 조직원에게 제공한 역할, 활동, 결과 등에 대한 행동적 반응의 수준으로서[23], 조직에 대해 개인이 인식하는 거래 과정 및 결과에 대한 공정함의 평가를 지칭한다[24]. 공정성은 상황 또는 결과에 대한 상대적 비교를 수행하는 것을 가정한다[25]. 즉, 개인은 교환과정에서 확보된 결과를 평가하기 위해 유사한 환경 또는 상황에서 제시되었던 결과를 비교하며, 상대적으로 박탈감 또는 만족도 수준을 평가한다. 즉, 박탈감을 높게 판단할 때 불공정한 대우를 받았다고 판단하며, 만족도를 높게 판단할 때 공정한 대우를 받았다고 판단한다[26].

초기 공정성은 결과의 공평성(Fairness)을 중심으로 연구되었다[25]. 즉, 거래의 보상이 충분하게 제공되었는지에 대한 기준을 중심으로 사람들은 공정성을 판단한다고 보았다. 이후, 선행연구는 거래 과정에서 필요한 정보, 절차 등이 공평하게 제공될 때, 개인은 상대방이 요구하는 결과를 충분히 제공할 수 있고, 이에 맞는 보상을 받을 수 있음을 지적하면서 다양한 공정성 조건을 제시했다. 즉, 결과의 보상 개념인 분배 공정성, 거래 과정에서의 절차가 공평해야 함을 설명한 개념인 절차 공정성, 결과 도출에 필요한 정보의 공평한 제공에 대한 관점의 정보 공정성, 그리고 의사결정에 필요한 소통의 과정에서 받게 되는 공평함인 대인 간 공정성 등이 제시되었다[24,26,27]. 나아가, 조직원이 조직에 대하여 느끼는 공

정성은 모든 환경 및 지원 체계 등을 통합하여 평가하게 되며, 통합된 공정성에 기반하여 행동이 결정된다는 연구가 제시되었다[28]. 본 연구는 정보보안 조직의 공정성은 전체적인 환경 및 지원의 개념으로 평가할 것으로 판단하고 통합된 조직 공정성 개념을 반영한다.

특정 역할에 대한 조직 차원의 지원 및 보상 등의 공정성은 조직원의 역할 준수를 넘어 이타적 행동을 추구하는데 도움을 준다. Colquitt[2001]은 분배, 절차, 정보, 대인 간 공정성이 결과 만족도, 역할 준수, 그리고 협력적 행동을 높임을 밝혔으며[24], Chou et al.[2013]은 조직 공정성은 개인에게 부여된 역할의 달성을 넘어 이타적 행동인 조직 시민행동에 영향을 줌을 밝혔다[26]. 정보보안과 관련하여, Xue et al.[2011]은 정보보안 처벌 중심의 공정성을 제시하면서, 공정한 처벌 환경이 조직원의 처벌 인식과 준수 행동을 강화함을 확인하였으며[6], Hwang[2021]은 정보보안 분배, 절차, 정보 공정성이 조직 내 개인 간의 관계적 사회 자본을 형성하여 준수 의도를 높임을 확인하였다[29]. 역으로, Alshare et al.[2018]은 조직 공정성이 개인의 회피 행동을 축소하는 환경 조건임을 제시하였다[30]. 즉, 조직 공정성은 조직에 대한 개인의 이타적 행동을 강화한다. 연구는 동일한 맥락에서 제언 행동에 영향을 줄 것으로 기대하며, 다음의 가설을 제시한다.

H2 : 정보보안 조직 공정성은 조직원의 정보보안 제언 행동에 긍정적 영향을 준다.

조직이 개인에게 요구하는 역할에 대한 환경 구축 또는 지원 활동의 증가는 정체성을 확립하도록 돕는다. Zhao et al.[2014]은 조직 내 상호작용 공정성이 시민행동과 연계하여 조직원의 조직 정체성 확립에 기여함을 확인하였으며[27], 역으로 Liu and Berry[2013]은 조직 불공정성 환경이 높아질 때, 조직 정체성에 부정적 영향을 줌을 확인하였다[31]. Ma and Agarwal[2007]은 온라인 커뮤니티에서 공존성을 느낄 때 커뮤니티 정체성을 확립할 수 있음을 밝혔다[21]. 또한, Ogbanufe[2021]은 조직이 관리하는 정보의 위협 요인, 정책 방향을 충분히 알리고, 그리고 보안 준수를 위한 지원을 할 때, 조직원의 정보보안 역할 정체성을 확립할 수 있음을 제시하였다[13]. 즉, 선행연구는 공정한 환경 구축이 조직에 대한 개인의 정체성 확립에 도움을 줌을 밝히고 있다. 동일한 맥락에서 본 연구는 정보보안 조직 공정성이 역할 정체성에 긍정적 영향을 줄 것으로 기대하며, 다음의 가설을 제시한다.

H3 : 정보보안 조직 공정성은 조직원의 정보보안 역할 정체성에 긍정적 영향을 준다.

2.4 정보보안 준수 민감성

조직이 요구하는 특정 활동에 대한 인식 또는 행동은 개인의 민감성(Sensitivity)에 따라 다르게 발현된다[11]. 민감성은 대상으로부터 확보하는 유무형의 가치에 매력을 느끼는 수준을 의미한다[32]. 정보보안과 관련하여 개인의 대인 간 영향 민감성은 개인의 정보보안 준수 행동에 영향을 줄 수 있는데, 조직 내 형성된 보안 관련된 규범과 제공되는 정보를 받아들이는 개인의 민감성 수준에 따라, 조직 중심의 선택 또는 개인 중심의 선택을 하려는 모습을 보인다[11].

Venkatesh et al.[2022]은 조직의 지식관리 활동 및 성과에 영향을 주는 개인 특성 요인으로 인센티브 민감성과 이미지 민감성을 제시하였다[12]. 그들은 조직 요구에 대한 개인의 행동은 요구사항 준수에 따른 성과의 보상 조건에 영향을 받으며, 준수 활동에 따른 주변 동료들의 인식 또는 평판으로 형성된 영향력 조건에 영향을 받을 수 있음을 제시하였다[12]. 본 연구는 정보보안 관련 조직의 역할 요구에 대해, 개인의 행동은 이미지 및 인센티브 민감성에 의해 변화할 것으로 기대하며, 해당 요인들을 반영한다. 첫째, 이미지 민감성(Sensitivity to Image)은 조직으로부터 요구받은 역할에 참여 또는 참여하지 않음으로써 형성되는 대중적 또는 사회적 이미지에 대한 우려의 수준으로 정의된다[12]. 즉, 집단에서 개인은 집단 구성원에게 영향을 주거나, 구성원들로부터 인정을 받음으로써, 집단의 일원으로 인식을 하는 모습을 보이는데[13], 이미지 민감성은 외부의 평판 또는 인식 등에 민감하게 반응하여 행동하려는 수준을 의미한다. 따라서, 이미지 민감성이 높은 개인은 조직이 요구하는 지식제공 행동, 업무적 행동 등을 능동적으로 함으로써 주변 동료들로부터 인정을 받길 원하는 경향이 있다[12]. 둘째, 인센티브 민감성(Sensitivity to Incentive)은 조직으로부터 요구받은 역할에 대한 수행 보상 또는 가치에 매력을 느끼는 수준으로 정의된다[12]. 개인은 조직으로부터 행동 결과로서 금전적 또는 비금전적 보상을 확보하길 원하며, 보상은 개인이 부여받은 역할에 대한 성과 창출에 높은 영향을 주는 요인이다. 특히, 인센티브 민감성이 높은 사람은 조직의 요구사항 또는 역할을 달성함으로써 추가적인 보상을 확보하길 기대하기 때문에, 능동적인 참여 행동을 보인다[32].

조직 내 역할 참여와 관련된 개인의 민감성은 역할에 대한 개인의 인식과 상호작용 효과를 가져 행동을 변화시킨다. Venkatesh et al.[2022]는 지식관리와 관련된 인센티브 민감성은 개인의 조직에서의 장기적 활동 지향성 및 불확실성 회피 인식과 상호작용 효과를 가져 지식제공 행동을 강화함을 밝혔으며, 이미지 민감성은 개인이 인식한 권한 수준과 상호작용 효과를 가져 지식제공 및 검토 행동을 변화시키는 것을 확인하였다[12]. Yazdanmehr et al.[2020]은 정보보안과 관련된 개인의 자율적 의식인 자기 규제에 대한 인식과 대인 간 영향 민감성이 상호작용 효과를 가져 보안 정책 준수에 영향을 준다고 하였다[11]. 즉, 개인의 민감성은 요구 활동에 대한 개인의 인식과 조절 효과를 가지며, 행동을 변화시킨다. 동일한 맥락에서 정보보안 준수 관련 이미지 및 인센티브 민감성은 역할 정체성과 조절 효과를 가져 제언 행동을 변화시킬 것으로 판단하며, 다음 가설을 제시한다.

H4a : 정보보안 준수 관련 이미지 민감성은 역할 정체성과 제언 행동의 관계를 조절한다.

H4b : 정보보안 준수 관련 인센티브 민감성은 역할 정체성과 제언 행동의 관계를 조절한다.

또한, 개인의 민감성은 역할 수행에 필요한 조직 환경과 상호작용 효과를 가져 행동을 변화시킨다. Lee and Hwang[2021]은 조직의 절차 및 정보 관련 공정성이 보안 준수 원인 및 행동에 미치는 영향에 대해, 개인의 공정 민감성이 조절 효과를 가져, 행동 변화를 일으킨다고 하였다[2]. Yazdanmehr et al.[2020]은 정보보안을 위한 조직의 명령과 통제 조건이 보안 정책 준수에 미치는 영향에 조절 효과를 가지는데, 조직이 구축한 보안 환경과 개인이 확보한 규범 및 정보를 어떻게 받아들일 것인지에 대한 개인의 민감성이 환경과 연계되기 때문이라고 보았다[11]. 즉, 조직 공정성과 관련된 환경적 조건과 개인의 민감성은 조절 효과를 가지며 행동을 변화시킨다. 본 연구는 조직 공정성과 제언 행동 간의 관계를 이미지 민감성과 인센티브 민감성이 조절할 것으로 판단하며, 다음의 가설을 제시한다.

H5a : 정보보안 준수 관련 이미지 민감성은 조직 공정성과 제언 행동의 관계를 조절한다.

H5b : 정보보안 준수 관련 인센티브 민감성은 조직 공정성과 제언 행동의 관계를 조절한다.

3. 연구 모델 및 데이터 수집

3.1 연구 모델

연구는 조직원이 정보보안 활동 과정에서 개인 특성 요인인 이미지 및 인센티브 민감성의 영향을 확인하는 것을 목적으로 한다. 이에, 연구는 조직 공정성 - 역할 정체성 – 제언 행동에 대한 메커니즘에 민감성의 조절 효과를 제시하며, 연구 모델은 Fig. 1과 같다.

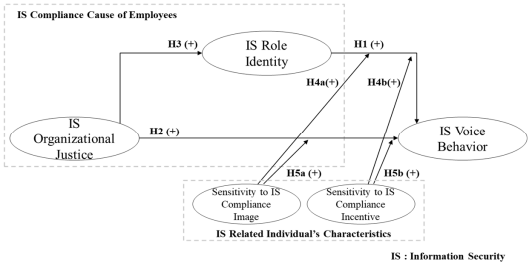

Fig. 1. Research Model

3.2 측정 도구 및 표본 수집

가설 검정은 설문지 기법으로 확보한 표본을 활용하되, AMOS 22.0, SPSS 21.0, 그리고 Process 3.1 도구를 검정에 적용한다. 설문 문항 도출을 위하여, 첫째, 조직 내 조직원 활동과 관련된 선행연구에서 요인별 측정 문항을 확보하고, 정보보안 관점으로 문항들을 변경하였다. 둘째, 측정 문항들의 내적 타당성을 확보하기 위하여, 도출된 문항들을 정보보안을 업무에 반영하고 있는 직장인이면서 경영 대학원에 다니고 있는 10명의 사람에게 문항의 적절성을 확인하고 수정 및 보완하였다. 최종적으로 확보한 문항의 척도는 7점 리커트 척도를 적용하였다(7점: 매우 그렇다 – 1점: 매우 그렇지 않다).

최종 적용된 설문 문항은 다음과 같다. 정보보안 조직 공정성은 Ambrose and Schminke[2009]의 측정 문항을 반영하였으며[28], “(ISOJ1) 전체적으로, 나는 조직으로부터 보안 활동과 관련하여 공정한 대우를 받고 있음”, “(ISOJ2) 나는 정보보안에 대해 조직이 공정하게 대우하고 있다고 믿음”, “(ISOJ3) 조직의 정보보안 활동들은 일반적으로 공정함”, “(ISOJ4) 정보보안 활동에 대해 조직은 동료들을 공평하게 대우함”을 적용하였다. 정보보안 관련 역할 정체성은 Ogbanufe[2021]의 측정 문항을 반영하였으며[13], “(ISRI1) 정보보안 정책을 따르는 것은 나에게 정말 중요함”, “(ISRI2) 조직에서 내가 보유한 정보를 보호하는 것은 내가 누구인지를 결정하도록 하는

중요한 부분임", "(ISRI3) 업무에서 정보보안 정책을 준수하는 능력은 내가 누구인지를 설명하는 중요한 부분임"을 적용하였다. 정보보안 제언 행동은 Svendsen and Joensson[2015]의 측정 문항을 반영하였으며[16], "(ISVB1) 나는 조직의 정보보안 목표 달성을 위해 의견을 제시함", "(ISVB2) 나는 조직의 정보보안 관련 문제에 대하여 동료의 참여를 독려함", "(ISVB3) 나는 조직의 보안 정책에 대한 아이디어를 제시함"을 적용하였다. 정보보안 준수 이미지 민감성은 Venkatesh et al.[2022]의 측정 문항을 반영하였으며[12], "(SCIm1) 정보보안과 관련된 지식 부족을 드러내는 것은 불편함", "(SCIm2) 정보보안과 관련되어, 나의 평판을 손상할 수 있는 것은 하지 않을 것임", "(SCIm3) 정보보안과 관련되어, 나의 이미지를 손상하는 것을 하지 않을 것임"을 반영하였다. 정보보안 준수 인센티브 민감성은 Venkatesh et al.[2022]의 측정 문항을 반영하였으며[12], "(SCIn1) 정보보안을 지키는데, 준수 활동에 따른 인센티브가 중요하다고 생각함", "(SCIn2) 정보보안을 지키는데, 추가적인 보너스가 중요하다고 생각함", "(SCIn3) 정보보안을 지키기 위해서는 교육 등의 혜택을 제공하는 것이 중요하다고 생각함"을 반영하였다.

측정 대상은 구축된 정보보안 정책을 조직원의 업무에 반영하고 있는 기업의 근로자로 설정하였다. 설정된 대상에 맞도록 표본을 확보하기 위하여, 직장인 회원을 다수 확보한 M리서치에 의뢰하여 설문을 받았다. 첫째, 응답자의 직업과 나이를 우선 확인하였다. 사무직이면서, 20세 이상인 사람만 다음 설문으로 넘어가도록 하였다. 둘째, 조직이 조직원에게 제공 또는 요구하고 있는 정책을 지식관리 정책, 정보보안 정책, 인사관리 정책, 기타로 제시하고 정보보안 정책에 응답한 사람만 본 설문으로 넘어가도록 하였다. 최종적으로, 연구에서 확보한 통계 자료에 대한 활용 목적과 방법을 설명하였으며, 통계적 활용을 허가한 사람만 본 설문에 접근하도록 구조화하였다.

총 437건의 표본을 확보하였으며, 표본이 보유한 특성은 Table 1과 같다. 응답자의 성별은 5대 5 비중으로 확보되었으며, 연령 또한 세대별 약 23%내외로 비슷한 비중으로 확보한 것으로 나타났다. 응답자의 조직은 서비스업이 제조업보다 많은 7대 3의 비중으로 나타났으며, 기업 규모는 50인 이상 기업이 전체의 68%인 것으로 나타났다. 응답자의 직위는 사원 및 대리급에서 가장 많은 것(41.2%)으로 나타났다. 표본의 특성은 사무직 특성을 적절히 반영한 것으로 판단되었다.

Table 1. Characteristics of Samples

Categories		Frequency	%
Gender	Male	218	49.9
	Female	219	50.1
Age	〈 30	101	23.1
	31 - 40	101	23.1
	41 - 50	114	26.1
	〉 51	121	27.7
Industry	Manufacture	126	28.8
	Service	311	71.2
Size	〈10	27	6.2
	10-50	113	25.9
	51-300	144	33.0
	〉300	153	35.0
Job Position	Under Manager	180	41.2
	Manager	175	38.6
	Over Manager	82	18.8
Total		437	100.0

4. 가설 검정

4.1 신뢰성, 타당성 분석

설문을 통해 확보한 표본의 데이터들은 리커트 척도로 측정되었으며, 요인별 다 항목으로 구성되어 있으므로, 측정 항목들이 요인을 충분히 설명할 수 있는지 신뢰성과 타당성을 확인하였다.

첫째, 신뢰성은 측정 도구를 반복 측정하더라도 일관성 있게 요인을 설명하고 있는지를 확인하는 것으로, 본 연구는 SPSS 21.0 패키지의 신뢰성 분석 도구인 크론바흐 알파 값을 통해 확인하였다. 선행연구는 적용 요인 모두에 0.7 이상의 크론바흐 알파를 요구한다[33]. 5개 요인에 반영된 16개 측정 항목 중 신뢰성에 문제가 있는 1개 항목(ISOJ4)을 제외하였으며, 신뢰성 분석 결과는 Table 2와 같다. 모든 측정 항목들은 요인에 대해 신뢰성을 확보한 것으로 나타났다.

둘째, 타당성은 측정 항목들이 요인을 얼마나 정확하게 측정했는가를 판단하는 것으로, 본 연구는 AMOS 22.0 패키지의 확인적 요인분석을 통해 타당성을 확인하였다. 특히, 측정치 간에 높은 상관관계를 가져 요인을 대표할 수 있는지를 확인하는 집중 타당성과 요인들이 서로 상이한 수준을 가지는지 확인하는 판별 타당성을 확인하였다. 우선, 확인적 요인분석 모델에 대한 적합도 수준을 확인하였다. 선행연구는 적합도 수치에 대하여 RMSEA와 RMR에 대하여 0.05보다 낮은 값을 요구하고, GFI, AGFI, NFI, 그리고 CFI에 대하여 0.9보다 높

은 값을 요구한다[34]. 모델의 적합도 확인 결과, $\chi 2/df$ = 1.891, NFI = 0.967, CFI = 0.984, RMSEA = 0.045, RMR = 0.044, GFI = 0.956, 그리고 AGFI = 0.934와 같이 나타나, 적합도 요구수준을 충족하였다.

Table 2. Validity and Reliability of Variables

Variables		Estimate	SRW Estimate	Standard Error	Critical Ratio	Cronbach's Alpha
ISOJ	ISOJ3	1.000	0.885			0.867
	ISOJ2	0.904	0.818	0.045	19.93**	
	ISOJ1	0.878	0.789	0.046	19.05**	
ISRI	ISRI3	1.000	0.875			0.896
	ISRI2	0.976	0.879	0.041	23.59**	
	ISRI1	0.993	0.837	0.045	21.98**	
ISVB	ISVB3	1.000	0.839			0.909
	ISVB2	1.041	0.901	0.044	23.82**	
	ISVB1	1.008	0.897	0.043	23.66**	
SCIm	SCIm3	1.000	0.840			0.861
	SCIm2	0.967	0.816	0.052	18.60**	
	SCIm1	0.905	0.792	0.05	17.99**	
SCIn	SCIn3	1.000	0.838			0.857
	SCIn2	0.982	0.848	0.049	20.02**	
	SCIn1	0.955	0.784	0.052	18.22**	

ISOJ(IS Organization Justice), ISRI(IS Role Identity), ISVB(IS Voice Behavior), SCIm(Sensitivity to IS Compliance Image), SCIn(Sensitivity to IS Compliance Incentive)
SRW(Standard Regression Weight), **: p 〈 0.01

집중 타당성은 개념 신뢰도와 평균분산추출을 확인한다. 개념 신뢰도는 요인별 0.7보다 높은 값을 요구하며, 평균분산추출은 요인별 0.5보다 높은 값을 요구한다[34]. 분석 결과는 Table 3과 같으며, 모든 요인이 집중 타당성 요구사항을 확보한 것으로 나타났다.

Table 3. Discriminant Validity

Variable	CR	AVE	1	2	3	4	5
ISOJ	0.841	0.639	**0.800[a]**				
ISRI	0.877	0.704	.498**	**0.839[a]**			
ISVB	0.888	0.726	.512**	.628**	**0.852[a]**		
SCIm	0.838	0.634	.488**	.418**	.535**	**0.796[a]**	
SCIn	0.834	0.627	.552**	.527**	.604**	.635**	**0.792[a]**

ISOJ(IS Organization Justice), ISRI(IS Role Identity), ISVB(IS Voice Behavior), SCIm(Sensitivity to IS Compliance Image), SCIn(Sensitivity to IS Compliance Incentive)
CR(Construct Reliability), AVE(Average Variance Extracted)
a: square root of the AVE, **: p 〈 0.01

판별 타당성은 요인 간의 차별성을 확인하기 위해, 상관계수가 적을 것을 요구하는데, 선행연구는 평균분산추출의 제곱근이 전체 상관계수보다 클 경우, 판별 타당성이 존재한다고 본다[34]. 결과는 Table 3과 같으며 판별 타당성을 확보하였다.

그리고, 본 연구는 동일방법편의 문제를 확인하였다. 해당 문제는 측정 도구를 동일 시점에 측정했을 때, 선행변수에 의해 후행 변수의 응답을 왜곡할 수 있는 문제를 말한다. 연구는 여러 동일방법편의 문제 확인 방법 중 비측정잠재방법요인 기법을 적용하였다. 본 기법은 모든 요인이 공분산으로 반영된 모델에 단일 요인을 추가하고 측정 항목에 연결한 모델을 만들어, 두 모델 간의 측정값의 변화량을 확인하는 것이다[35]. 공분산이 반영된 모델의 적합도($\chi 2/df$ = 1.891, NFI = 0.967, CFI = 0.984, RMSEA = 0.045, RMR = 0.044, GFI = 0.956, AGFI = 0.934)와 단일 요인이 반영된 모델의 적합도($\chi 2/df$ = 1.261, NFI = 0.982, CFI = 0.996, RMSEA = 0.024, RMR = 0.022, GFI = 0.975, AGFI = 0.954)가 요구사항을 충족하였으며, 측정값의 변화량이 각각 0.3보다 낮은 것으로 나타나, 동일방법편의 문제는 크지 않아 가설 검정을 하였다.

4.2 가설 검정

본 연구는 주 효과 분석과 조절 효과 분석을 개별적으로 수행한다. 주 효과 분석은 조직 공정성이 역할 정체성을 통해 제언 행동으로 연계되는 메커니즘을 확인하는 것으로서, AMOS 22.0을 적용하여 구조방정식 모델링 기반의 경로 검정을 한다. 조절 효과 분석은 정보보안 준수 활동과 관련된 이미지와 인센티브 민감성이 제언 행동의 선행 요인과 상호작용 효과를 가지는지를 확인하는 것으로서, Process 3.1 매크로를 통해 확인한다.

가설 1에서 가설3까지의 경로 검정을 위해 구조 모델을 제시하였으며, 제시한 구조 모델의 적합도를 확인하였다. 결과는 $\chi 2/df$ = 2.705, NFI = 0.977, CFI = 0.985, RMSEA = 0.063, RMR = 0.047, GFI = 0.969, 그리고 AGFI = 0.941과 같이 나타났다. 비록 RMSEA가 요구사항인 0.05보다 조금 큰 것으로 나타났으나, 그 외 수치가 적합도 요구사항을 충족하여, 경로 분석(β)을 하였다. 결과는 Fig. 2와 Table 4와 같다.

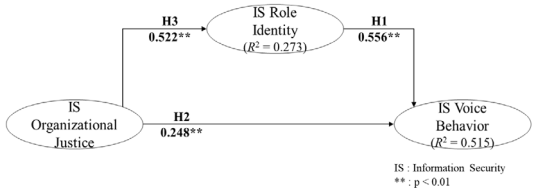

Fig. 2. Results of Hypothesis Testing (H1-H3)

Table 4. Results of Hypothesis Testing (H1-H3)

Path		Coefficient	t-value	Results
H1	ISRI → ISVB	0.556	10.544**	Supported
H2	ISOJ → ISVB	0.248	4.988**	Supported
H3	ISOJ → ISRI	0.522	10.020**	Supported

ISOJ(IS Organization Justice), ISRI(IS Role Identity), ISVB(IS Voice Behavior)
**: p < 0.01

가설 1은 정보보안 역할 정체성 확립이 보안 이슈에 대한 제언 행동에 긍정적 영향을 준다는 것으로, 요인 간의 경로(β)는 통계적으로 유의하였다(H1: β = 0.556, p < 0.01). 결과는 정보보안 역할 정체성을 확립한 조직원은 조직이 요구하는 보안 정책 관련 행동을 높임을 밝힌 Ogbanufe[2021] 연구와 유사하다. 즉, 개인이 조직에서 관리하는 정보 자원에 대한 관리의 필요성 인식을 확립했을 때, 자신과 조직을 위해 준수 행동을 하게 됨을 의미한다. 따라서, 조직은 조직원에게 정보 자원 관리의 필요성을 높일 수 있는 보안 위협 요인과 활동 방법 등의 정보를 지속해서 제공하는 노력이 요구된다. 가설 2는 정보보안 조직 공정성 확립이 개인의 보안 이슈에 대한 제언 행동에 긍정적 영향을 준다는 것으로, 요인 간의 경로(β)는 통계적으로 유의하였다(H2: β = 0.248, p < 0.01). 결과는 정보보안 행동 결과에 대한 처벌의 공정성이 개인의 보안 준수 활동에 긍정적 영향을 준다는 Xue et al.[2011] 연구와 유사하다. 즉, 조직의 지원이 모든 조직원에게 공평하게 정보를 제공하고, 절차가 객관적이며, 처벌과 같은 결과에 대한 상대적 공정함을 인식할 때, 조직원의 참여 활동을 증진할 수 있다. 가설 3은 정보보안 조직 공정성 확립이 정보보안 역할 정체성 확립에 긍정적 영향을 준다는 것으로, 요인 간의 경로(β)는 통계적으로 유의하였다(H3: β = 0.522, p < 0.01). 이러한 결과는 상호작용 관련 공정성이 조직에 대한 정체성을 높임을 설명한 Zhao et al.[2014] 연구와 유사한 결과이다. 즉, 특정 정책 또는 활동에 대한 조직의 지원 과정과 평가 체계 등의 공정성에 대한 인식은 대상에 대한 일체감 또는 정체성을 확립하도록 돕는다. 따라서, 조직은 조직원이 정보보안을 반영한 역할의 필요성을 느낄 수 있도록 공정한 보안 환경을 구축하고 지원 체계를 유지하는 노력이 요구된다.

가설 4는 정보보안 준수 관련 이미지 및 인센티브 민감성이 정보보안 관련 개인의 인식 요인과 조절 효과를 가진다는 것으로, 측정 항목이 리커트 척도로 구성되어 있으므로 Process 3.1의 모델 1(붓스트래핑 5,000)을 반영하였다[36]. 조절 효과 검정 결과는 Table 5와 같다. 역할 정체성과 이미지 민감성 간의 조절 효과(H4a)는 유의수준 5% 기준으로 두 요인의 상호작용 항이 제언 행동에 미치는 영향이 없었으며, 역할 정체성과 인센티브 민감성 간의 조절 효과는 상호작용 항이 영향을 주는 것으로 나타났다(H4a: t = -1.916, n.s., H4b: t = -3.733 p < 0.01). 추가로, 역할 정체성과 인센티브 민감성 간의 조절 효과 관계를 명확하게 확인하기 위하여, SPSS 21.0의 단순기울기 검정을 하였으며, Fig. 3과 같다.

Table 5. Results of Hypothesis Testing (H4)

		Coefficient	t-value	Result
ISRI x ISIm → ISVB (H4a)	Constant	5.332	137.721**	Not Supported
	ISRI	0.481	11.757**	
	ISIm	0.365	8.793**	
	Interaction	-0.070	-1.916	
	F = 137.8512, R^2 = 0.4885			
ISRI x ISIn → ISVB (H4b)	Constant	5.373	135.866**	Supported
	ISRI	0.407	9.733**	
	ISIn	0.400	9.353**	
	Interaction	-0.135	-3.733**	
	F = 152.0561, R^2 = 0.5130			

ISRI(IS Role Identity), ISVB(IS Voice Behavior), SCIm(Sensitivity to IS Compliance Image), SCIn(Sensitivity to IS Compliance Incentive)
**: p < 0.01, *: p < 0.05

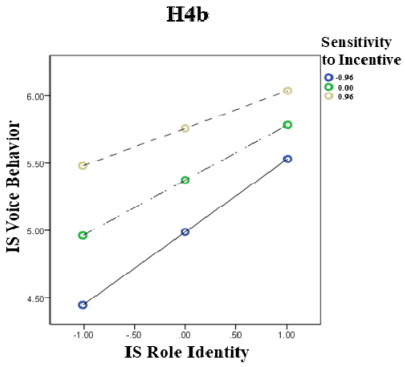

Fig. 3. Moderating Effect (H4b)

분석 결과, 역할 정체성이 제언 행동에 미치는 긍정적 관계에서, 인센티브 민감성이 낮은 집단이 높은 집단보다 역할 정체성과 상호작용 효과를 높게 가져 제언 행동을 높이는 것으로 나타났다. 인센티브 민감성의 경우 행동에 대한 보상에 대한 개인의 인식이며, 조직에서 수행한 결과에 대한 보상은 개인의 기본적인 욕구이기 때문에, 역할 정체성과 같은 내적 동기와 상호작용 효과를 가진 것으로 판단된다.

가설 5는 정보보안 준수 관련 이미지 및 인센티브 민감성이 조직 공정성과 조절 효과를 가진다는 것으로, 가설 4와 동일한 방법으로 측정하였다. 각 민감성의 조절 효과 검정 결과는 Table 6과 같다. 조직 공정성이 이미지 민감성(H5a), 인센티브 민감성(H5b)과 조절 관계에 있음을 확인한 결과, 개별적으로 각각 상호작용 항이 제언 행동에 영향을 주는 것으로 나타났다(H5a: t = -2.298, p 〈 0.05, H5b: t = -2.441, p 〈 0.05). 추가로, 민감성이 미치는 조절 효과의 영향을 확인하기 위하여, SPSS 21.0의 단순기울기 검정을 하였으며, Fig. 4, Fig. 5와 같다.

조직 공정성은 이미지 및 인센티브 민감성과 각각 비슷한 패턴의 영향을 가지는 것으로 나타났다. 즉, 독립변수들이 제언 행동에 대한 긍정적 영향에 대해, 이미지 및 인센티브 민감성이 낮은 집단이 높은 집단보다 조직 공정성과 상호작용 효과를 높게 가져 제언 행동을 높이는 것으로 나타났다. 즉, 정보보안의 환경이 공정하다고 판단될 때, 개인은 올바른 평판과 보상을 받을 수 있을 것으로 판단하여 각 민감성의 영향을 높게 받는 것으로 판단된다.

Table 6. Results of Hypothesis Testing (H5)

		Coefficient	t-value	Result
ISOJ x ISIm → ISVB (H5a)	Constant	5.341	125.062**	Supported
	ISOJ	0.334	7.591**	
	ISIm	0.406	8.516**	
	Interaction	-0.078	-2.298*	
	F = 87.2665, R^2 = 0.3768			
ISOJ x ISIn → ISVB (H5b)	Constant	5.350	125.876**	Supported
	ISOJ	0.257	5.781**	
	ISIn	0.485	10.144**	
	Interaction	-0.083	-2.441*	
	F = 103.9618, R^2 = 0.4187			

ISOJ(IS Organization Justice), ISVB(IS Voice Behavior), SCIm(Sensitivity to IS Compliance Image), SCIn(Sensitivity to IS Compliance Incentive)
**: p 〈 0.01, *: p 〈 0.05

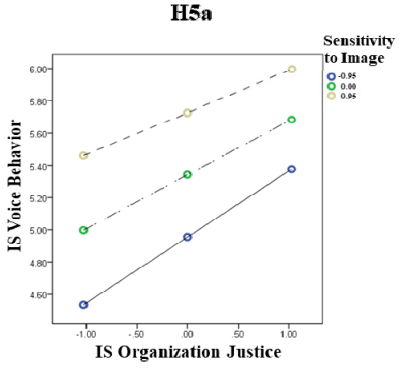

Fig. 4. Moderating Effect (H5a)

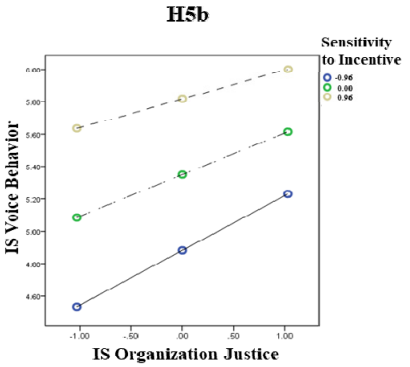

Fig. 5. Moderating Effect (H5b)

5. 결론

5.1 연구의 시사점

연구에서 확인한 가설 검정의 결과는 다음의 학술적, 실무적 시사점을 가진다.

첫째, 본 연구는 개인의 정보보안 준수 및 의견 개진 행동은 본인이 관리하는 정보 자원에 대한 보호의 필요성을 강하게 인식할 때 발현될 수 있음을 확인하였다. 특히, 정보보안 역할 정체성을 반영하되 자발적으로 의견을 개진하는 개념인 제언 행동과의 연계성을 확인하였다. 관련 선행연구가 개인에게 요구된 업무적 보안 활동의 준수 관점에 주목하였다면[8], 본 연구는 개인이 확립한 정보보안의 필요성과 정체성이 조직 전체를 위한 보안 강화를 위해 필요한 의견을 제기하는 행동에 영향을 줌을 밝혔다는 측면에서 연구적 차별성과 학술적 시사점을 가진다. 또한, 실무적 관점에서 개인이 인식한 정보보안 관리에 대한 인식의 강화가 이타적 보안 활동에 영향을 줌을 밝혔다. 즉, 정보 자원의 관리가 개인 본인 및 조직을 위해 필요하며, 관리를 통해 조직에서 본인의 정체성을 확립할 수 있다고 판단하도록 조직 차원의 지원이 필요함을 제시한다. 예를 들어, 정보 자원에 대한 기술적, 비기술적 위협 요인 및 예측되는 결과 등의 정보를 명확하게 제공하고, 정보 자원 관리를 위해 조직이 구축한 정책 및 지원 체계를 이해하도록 지원할 때, 조직원은 정보 자원 관리의 필요성을 인식할 수 있으며, 제언 행동을 통해 조직 전체의 보안 분위기 및 수준을 강화할 수 있다.

둘째, 본 연구는 조직원의 정보보안 역할 정체성의 확립과 능동적인 제언 행동을 위한 조직 환경 조건으로 조

직 공정성을 제시하였다. 정보보안 처벌 등 분야별 조직 공정성 관련 선행연구가 보안 정책에 대한 개인의 준수 행동에 영향을 줄 수 있음을 밝혔다면[6], 본 연구는 공정한 정보보안 환경의 구축이 조직원의 정보 자원 관리에 대한 정체성 확립과 나아가 보안 활동에 대한 의견 개진 행동에 긍정적 영향을 줄 수 있음을 밝힌 측면에서 차별성과 학술적 시사점을 가진다. 실무적 관점에서, 연구는 정보보안 정책을 관리하는 조직 관점에서 조직원에게 공정한 환경을 제공하고 있음을 알리는 것이 중요함을 밝혔다. 특히, 본 연구는 공정성에 대한 조직원의 평가가 활동에 대한 전체적인 평가에 기반함에 관점을 두었기 때문에, 조직은 정보보안 정책 관리 활동 전반에서 조직원들이 공정함을 느낄 수 있도록 지원하는 것이 필요함을 제시한다. 예를 들어, 정보보안 정책과 업무별 준수 활동에 대한 필요 정보를 명료하게 제공하고, 정보보안 준수 활동의 과정이 조직 내 직위 또는 권한과 관련 없이 누구나 동일하게 적용되고 있음을 알리고, 정보보안 결과에 대한 평가 및 상벌이 명확하게 이루어지고 있음을 알리는 노력이 필요하다.

셋째, 본 연구는 조직원의 정보보안 제언 행동에 영향을 주는 선행 변수가 정보보안 준수 관련 이미지 민감성에 영향을 받음을 확인하였다. 정보보안 관련 선행연구가 표준화 관점에서 조직 환경 및 인식의 행동에 미치는 영향을 중점적으로 밝혔다면[4], 본 연구는 개인차 요인이 보안 준수 활동에 변화를 일으킬 수 있음을 제시한 측면에서 차별성 및 학술적 시사점을 가진다. 실무적 관점에서, 개인은 조직이라는 집단에 소속된 공동체 의식을 가지는데, 동료 또는 외부 파트너들의 평판 등이 개인의 행동 과정에 영향을 미치게 된다. 특히, 정보보안 준수 과정에서 개인이 외부로부터 받게 되는 이미지의 민감성이 조직 환경 요소(조직 공정성)와 상호작용 효과를 가질 수 있다. 조직은 이미지 민감성이 높은 집단은 조직 공정성을 조금만 제공하더라도 긍정적 행동을 보이므로, 공동체 구성원으로 인식을 낮게 가진 조직원의 제언 행동을 강화하는 방안인 정보보안 관련 공정 환경을 구축하고 조직 전체에 확산하기 위한 전략을 수립하는 것이 필요하다.

넷째, 본 연구는 정보보안 준수 활동의 보상 개념인 인센티브 민감성이 조직 공정성과 역할 정체성과 상호작용 효과를 가지는 것을 확인하였다. 정보보안 선행연구가 보안 준수 활동에 대한 가치 또는 혜택을 중심으로 행동 원인을 밝히고, 조직의 보안 강화 전략 수립의 필요성을 제시해왔다면[5], 본 연구는 개인의 정보보안 활동에 대한 인센티브 민감성 개념을 정보보안에 적용하고 제언 행동 변화에 조절 효과를 가짐을 확인한 측면에서 선행연구로서의 학술적 시사점을 가진다. 실무적 관점에서, 개인은 조직과의 계약 관계에서 역할 수행 결과에 대한 보상을 확보하길 바라는데, 본 연구는 추가적인 인센티브가 개인의 행동 변화를 유도하는 조건이며, 정보보안 분야에 적용될 수 있음을 밝혔다. 특히, 정보보안 준수 인센티브 민감성이 정보보안 역할 정체성과 조직 공정성과 각각 상호작용 효과를 가져 행동을 변화시킴을 확인하였다. 조직의 공정한 보안 환경은 개인이 활동에 대한 공정한 대우를 받고 있음을 인식하는 조건이고, 정보보안 역할 정체성은 보안 활동을 통해 개인 또한 조직의 구성원으로 인정받는 무형의 보상을 의미한다. 즉, 조직이 조직원에게 구축된 보안 정책의 준수를 요구하기 위해, 공정한 보안 환경을 구축하고, 조직원에게 정보 관리의 필요성과 정체성을 확립하도록 지원하더라도 보상 체계가 부족하면 개인의 행동은 부정적으로 변화할 수 있음을 시사한다. 따라서, 조직은 공정하며 충분한 보상 체계에 기반한 보안 환경의 구축과 정체성 확립을 지원함으로써, 인센티브 민감성과 연계하여 제언 행동을 강화하기 위한 전략을 수립하는 것이 요구된다.

5.2 연구의 한계 및 향후 연구

본 연구는 정보보안 공정 환경과 개인의 역할 정체성 인식, 그리고 민감성 요소의 연계된 메커니즘을 밝힌 측면에서 시사점이 있으나, 다음과 같은 연구적 한계가 있으며 향후 보완될 필요가 있다. 첫째, 본 연구는 정보보안 제언 행동의 원인을 밝히기 위해, 정보보안 정책을 보유한 기업 관점의 조건을 제시하였다. 결과는 표준화 관점에서 의미를 지니나, 기업이 보유한 정보 가치는 업종별, 기업 특성별 차이가 있을 수 있다. 예를 들어, 금융업과 제조업에서 정보의 가치에 대한 인식 차이가 있을 수 있다. 이러한 차이는 조직 및 조직원의 보안 관련 행동의 차이를 발현시킬 수 있다. 따라서, 향후 연구에서는 세부 기업 특성별 내부자 준수 활동 강화 방안을 제시할 필요가 있다. 둘째, 본 연구는 개인차 요인으로 인센티브 및 이미지 민감성을 적용하였다. 조직에서 개인은 권력, 직위 등에 따라 정보보안 관련 인식의 차이가 있을 수 있으며, 특정 위협에 대한 대처 방식 등의 차이가 있을 수 있다. 즉, 개인의 위치 또는 개인의 대처 방식과 같은 개인차 요인에 따라 보안 행동의 차이가 발생할 수 있다. 따라서, 향후 연구에서는 세분화된 개인차 요인을 반영하여 행동 변화 원인을 밝힘으로써, 맞춤형 보안 전략 수립에 기여하는 것이 요구된다.

References

[1] I. Hwang, "The Study to Reinforce IS Related Motivation of Employee: A Perspective on IS Related Awareness and Person-organization fit," Journal of the Korea Academia-Industrial cooperation Society, Vol. 23, No. 11 pp. 594-607, 2022.
DOI: https://doi.org/10.5762/KAIS.2022.23.11.594

[2] W. Lee, I. Hwang, "Sustainable Information Security Behavior Management: An Empirical Approach for the Causes of Employees' Voice Behavior," Sustainability, Vol. 13, No. 11, pp. 6077, 2021.
DOI: https://doi.org/10.3390/su13116077

[3] The White House, Executive Order on Improving the Nation's Cybersecurity, 2021. Available From: https://www.whitehouse.gov

[4] Z. Tang, A. S. Miller, Z. Zhou, M. Warkentin, "Does Government Social Media Promote Users' Information Security Behavior towards COVID-19 Scams? Cultivation Effects and Protective Motivations," Government Information Quarterly, Vol. 38, No. 2, pp. 101572, 2021.
DOI: https://doi.org/10.1016/j.giq.2021.101572

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

[6] Y. Xue, H. Liang, 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

[7] 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

[8] X. Ma, "IS Professionals' Information Security Behaviors in Chinese IT Organizations for Information Security Protection," Information Processing & Management, Vol. 59, No. 1, pp. 102744, 2022.
DOI: https://doi.org/10.1016/j.ipm.2021.102744

[9] I. Hwang, S. Kim, C. Rebman, "Impact of Regulatory Focus on Security Technostress and Organizational Outcomes: The Moderating Effect of Security Technostress Inhibitors," Information Technology & People, Vol. 35, No. 7, pp. 2043-2074, 2022.
DOI: https://doi.org/10.1108/ITP-05-2019-0239

[10] N. S. Endler, J. D. Parker, "Assessment of Multidimensional Coping: Task, Emotion, and Avoidance Strategies," Psychological Assessment, Vol. 6, No. 1, pp. 50-60, 1994.
DOI: https://doi.org/10.1037/1040-3590.6.1.50

[11] A. Yazdanmehr, J. Wang, Z. Yang, "Peers Matter: The Moderating Role of Social Influence on Information Security Policy Compliance," Information Systems Journal, Vol. 30, No. 5, pp. 791-844, 2020.
DOI: https://doi.org/10.1111/isj.12271

[12] V. Venkatesh, F. D. Davis, Y. Zhu, "A Cultural Contingency Model of Knowledge Sharing and Job Performance," Journal of Business Research, Vol. 140, pp. 202-219, 2022.
DOI: https://doi.org/10.1016/j.jbusres.2021.07.042

[13] O. Ogbanufe, "Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity," Computers & Security, Vol. 108, pp. 102340, 2021.
DOI: https://doi.org/10.1016/j.cose.2021.102340

[14] K. K. Loch, 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

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

[16] M. Svendsen, T. S. Joensson, "Transformational Leadership and Change-related Voice Behavior," Leadership & Organization Development Journal, Vol. 37, No. 3, pp. 357-368, 2016.
DOI: https://doi.org/10.1108/LODJ-07-2014-0124

[17] J. Song, J. Wu, J. Gu, "Voice Behavior and Creative Performance Moderated by Stressors," Journal of Managerial Psychology, Vol. 32, No. 2, pp. 177-192, 2017.
DOI: https://doi.org/10.1108/JMP-03-2016-0078

[18] J. E. Stets, C. F. Biga, "Bringing Identity Theory into Environmental Sociology," Sociological Theory, Vol. 21, No. 4, pp. 398-423, 2003.
DOI: https://doi.org/10.1046/j.1467-9558.2003.00196.x

[19] A. N. Mishra, C. Anderson, C. M. Angst, R. Agarwal, "Electronic Health Records Assimilation and Physician Identity Evolution: An Identity Theory Perspective," Information Systems Research, Vol. 23, Np. 3, pp. 738-760, 2012.
DOI: https://doi.org/10.1287/isre.1110.0407

[20] S. M. Farmer, P. Tierney, K. Kung-McIntyre, "Employee Creativity in Taiwan: An Application of Role Identity Theory," Academy of Management Journal, Vol. 46, No. 5, pp. 618-630, 2003.
DOI: https://doi.org/10.2307/30040653

[21] M. Ma, R. Agarwal, "Through a Glass Darkly: Information Technology Design, Identity Verification, and Knowledge Contribution in Online Communities," Information Systems Research, Vol. 18, No. 1, pp. 42-67, 2007.
DOI: https://doi.org/10.1287/isre.1070.0113

[22] S. Ray, S. S. Kim, J. G. Morris, "The Central Role of Engagement in Online Communities," Information Systems Research, Vol. 25, No. 3, pp. 528-546, 2014.
DOI: https://doi.org/10.1287/isre.2014.0525

[23] 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

[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.
DOI: https://doi.org/10.1037/0021-9010.86.3.386

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

[26] T. Y. Chou, T. C. Seng-cho, J. J. Jiang, G. Klein, "The Organizational Citizenship Behavior of IS Personnel: Does Organizational Justice Matter?," Information & Management, Vol. 50, No. 2, pp. 105-111, 2013.
DOI: https://doi.org/10.1016/j.im.2013.02.002

[27] H. Zhao, Z. Peng, H. K. Chen, "Compulsory Citizenship Behavior and Organizational Citizenship Behavior: The Role of Organizational Identification and Perceived Interactional Justice," The Journal of Psychology, Vol. 148, No. 2, pp. 177-196, 2014.
DOI: https://doi.org/10.1080/00223980.2013.768591

[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] I. Hwang, "A study on the Effects of Information Security Social Capital and Organization Justice on Compliance Intention of Insiders," Journal of the Korea Academia-Industrial cooperation Society, Vol. 22, No. 8 pp. 511-522, 2021.
DOI: https://doi.org/10.5762/KAIS.2021.22.8.511

[30] K. A. Alshare, P. L. Lane, M. R. Lane, "Information Security Policy Compliance: A Higher Education Case Study," Information & Computer Security, Vol. 26, No. 1, pp. 91-108, 2018.
DOI: https://doi.org/10.1108/ICS-09-2016-0073

[31] Y. Liu, C. M. Berry, "Identity, Moral, and Equity Perspectives on the Relationship between Experienced Injustice and Time Theft," Journal of Business Ethics, Vol. 118, pp. 73-83, 2013.
DOI: https://doi.org/10.1007/s10551-012-1554-5

[32] W. Jiacheng, L. Lu, C. A. Francesco, "A Cognitive Model of Intra-organizational Knowledge-sharing Motivations in the View of Cross-culture," International Journal of Information Management, Vol. 30, No. 3, pp. 220-230, 2010.
DOI: https://doi.org/10.1016/j.ijinfomgt.2009.08.007

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

[34] 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

[35] 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

[36] A. F. Hayes, Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-based Approach, New York: Guilford Publications, 2017.

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