Journal of the Korea Academia-Industrial cooperation Society
Vol. 23, No. 11 pp. 594-607, 2022

https://doi.org/10.5762/KAIS.2022.23.11.594
ISSN 1975-4701 / eISSN 2288-4688

조직원의 정보보안 관련 동기 향상 방안 연구: 정보보안 인식 및 개인조직 적합성 관점

황인호
국민대학교 교양대학

The Study to Reinforce IS Related Motivation of Employee: A Perspective on IS Related Awareness and Person-organization fit

Inho Hwang
College of General Education, Kookmin University

요 약 코로나 19로 인해 변화된 조직 환경은 조직원의 효과적인 업무 수행을 위해, 온라인 미팅 시스템과 같은 비대면 지원 기술의 활용을 증가시키고 있다. 비대면 지원 기술은 조직원들의 정보, 노하우 등의 교환 활동을 효과적으로 지원함으로써 조직의 성과 창출에 기여하고 있다. 반면, 조직은 정보보안을 위해 정보에 대한 통제를 통해 정보 노출을 억제해야 하는데, 온라인 기술 활용의 증가는 정보보안에 위협 요인으로 작용한다. 본 연구는 개인의 정보보안 준수 활동이 정보보안과 관련된 다양한 동기 요인의 영향에 있다고 보고, 준수 동기 강화 요인을 제시하는 것을 목적으로 한다. 세부적으로 정보보안 정책과 처벌 인식이 개인의 동기와 개인조직 적합성을 통해 준수의도로 연계되는 매커니즘을 설명한다. 본 연구는 설문지 기법으로 정보보안 정책을 업무에 적용하는 근로자들을 대상으로 설문을 하였으며, 구조방정식 모형과 Process 3.1을 활용하여 가설 검증을 하였다. 분석 결과, 정보보안 정책 및 처벌 인식이 내적 동기와 외부 규제를 통해 준수 의도에 영향을 주는 것을 확인하였으며, 내적 동기와 준수 의도 간의 관계를 개인조직 적합성이 강화하는 것을 확인하였다. 본 연구는 조직원의 정보보안 준수 의도에 영향을 주는 매커니즘을 밝힘으로써, 내부자에 대한 성공적인 정보보안 관리를 위한 방향을 제언한다.

Abstract Organizational changes due to COVID-19 are increasing the use of non-face-to-face support technologies, such as online meeting systems. However, organizations must control access to and the use of information by employees to ensure information security (IS), and the increased use of online technology can threaten IS. We hypothesized that an individual's IS compliance activities are influenced by various motivational factors related to IS and motivational reinforcement factors related to IS compliance. We propose a mechanism whereby IS policy and sanction awareness are linked to IS compliance intention through motivation and person-organization fit (PO fit). We surveyed workers who apply IS policies during work and tested this hypothesis using the structural equation model and Process 3.1 macro. The results of this analysis confirmed that IS policy and sanction awareness affect IS compliance intention through intrinsic motivation and external regulation and that PO fit reinforces the relationship between intrinsic motivation and IS compliance intention. Furthermore, having identified mechanisms that influence IS compliance intention, we suggest directions for successful IS management.

Keywords : IS Compliance Intention, Motivation, Policy Awareness, Sanction Awareness, Person-organization Fit

*Corresponding Author : Inho Hwang(Kookmin Univ.)
email: hwanginho@kookmin.ac.kr
Received September 13, 2022 Revised October 19, 2022
Accepted November 4, 2022 Published November 30, 2022

1. 서론

온라인 미팅 시스템과 같은 비대면 기반 기술 활용의 증가는 사람들이 대면을 통해 수행하던 교류 활동을 급격히 대체하고 있다. 특히, 조직은 비대면 기반 업무 체계가 업무 효율성을 감소시키지 않음을 인식하면서, 웹 기반 연계 기술을 활발히 도입하고 있다[1]. 조직원이 다양한 위치에서 조직의 정보기술을 사용하는 것은 효율성 증대에 긍정적인 영향을 줄 수 있지만, 정보 노출을 통제하고 모니터링을 해야만 하는 정보보안 관점에서는 위협이 될 수 있다[2]. 일찍이, Loch et al.[1992]은 정보 노출 가능성, 즉 정보보안 위협 요인별 대처 및 예방 방안을 제시하면서 기술 관점의 외부 침입보다 사람에 의한 정보 노출 위협에 대한 방어가 더욱 어려울 수 있음을 지적하였다[3]. 또한, West[2008]는 사람에 대한 정보보안 관리의 어려움은 조직과 사람 간의 정보의 불균형 문제에서 발생한다고 보았다[4]. 즉, 사람에 의한 정보 노출 가능성은 언제 어디서든 조직의 정보시스템에 접속할 수 있거나 외부와 접속이 쉬워질수록 발생할 수 있으므로, 조직들의 관심과 통제가 필요한 부분이다[5].

내부자의 정보보안 준수와 관련된 선행연구는 심리적 관점에서 접근될 필요가 있음을 지적하고 있다. 사람은 정보보안 준수 행동에 대한 혜택과 미준수 행동에 대한 비용을 합리적으로 비교해서 의사결정을 한다고 본 연구[6,7], 정보가 노출될 때 발생 가능한 두려움, 위협에 대한 인식과 대처 방법과 같은 동기적 조건을 제시한 연구[8], 정보보안 미준수 결과에 대한 강력한 처벌이 개인에게 자극되어 준수 행동으로 이어진다고 본 연구[9,10] 등이 대표적으로 제시되고 있다. 선행연구는 정보보안 환경에서 조직원이 합리적 또는 차선 선택, 또는 감정적 대처 등 정보보안 행동을 결정하는 것을 밝혔다는 부분에서 높은 시사점을 가진다.

반면, 조직에서 개인의 행동 동기는 본인이 보유한 내면의 동기로 결정되기도 하지만, 외적 환경과의 연계를 통해 동기화되어 행동으로 진행되기도 한다[8]. 정보보안은 대표적인 조직 중심의 구조화된 환경조건이기 때문에, 개인의 정보보안 관련 활동은 조직이 구축한 체계에서 행동으로 이어질 가능성이 크다. 하지만, 조직이 구축한 보안 환경에 대한 준수 요구사항이 조직원에게 전달된 후, 조직원이 보안 준수를 결정하는 과정에서, 어떠한 매커니즘을 통해 개인이 의사결정을 하고, 외적 요건에 영향을 받는지에 대한 분석은 부족하다. 이에 본 연구는 특정 환경, 개인 동기, 그리고 행동으로의 전환을 체계적으로 설명하는 자기결정성 이론(Self-determination Theory)과 조직과 개인 간의 동일시 감정을 통해 행동을 강화는 개인-조직 적합성(Person-organization Fit)을 연계하고자 한다.

첫째, 자기 결정성 이론은 개인은 주어진 환경에 스스로 대처하고 발전할 수 있는 역량을 확보하고자 하고, 내면적 동기와 외부적 동기를 통합적으로 고려하여, 환경이 요구하는 행동을 한다는 관점이다[11,12]. 즉, 정보보안과 같이 엄격한 통제 환경에서 조직원이 어떻게 준수 행동을 결정하는지를 강하게 설명할 수 있는 이론이다. 그러나, 정보보안 분야에서는 자기 결정성 이론을 접목하여 의미를 부여했으나[8], 조직 외적 조건과 연계하여 개인의 자기결정성을 설명한 연구는 부족한 상황이다. 즉, 본 연구는 자기결정성 영향요인으로 정보보안 관련 인식(정책, 처벌) 요인을 제시하고, 개인의 자기 결정을 위한 동기 강화 방안을 제시하고자 한다.

둘째, 자기 결정을 위해 형성된 개인의 다양한 동기의 영향을 강화하는 방안을 제시하고자 한다. 이에, 본 연구는 개인조직 적합성 요인을 반영하여 동기와 준수의도 간의 영향적 관계를 강화할 수 있음을 밝히고자 한다. 개인조직 적합성은 가치와 목표가 개인과 조직 간에 상호 동일시를 가지는 상황으로, 동일시가 강화된 개인은 조직의 요구사항이 본인의 목표 달성에 기여한다고 판단하므로 긍정적 행동을 보인다고 본다[13]. 즉, 정보보안 행동에 영향을 주는 개인에게 형성된 동기가 적합성 요인과 연계 시, 긍정적 행동을 강화할 수 있을 것으로 판단된다. 이를 통해, 연구는 조직이 고려해야 할 조직원의 정보보안 동기 개선 방안을 다각적으로 제시함으로써, 내부의 정보보안 성과 달성을 위한 전략 수립에 기여할 것으로 기대한다.

2. 이론적 배경

2.1 조직 내부의 정보보안 사고 및 준수의도

미국의 바이든 행정부는 2021년 5월 행정명령을 통해 연방정부 및 관련된 기업에게 제로 트러스트 아키텍쳐(Zero Trust Architecture)로의 전환을 명령하였다[14]. 제로 트러스트 아키텍쳐는 말 그대로 '신뢰하지 말 것'을 의미하며, 조직의 정보보안 전략과 활동이 기존 외부자 중심의 침입 방지 체계에 방점이 있었다면, 이제는 내부자 또한 믿지 말고 외부자와 동일한 정보 접근체계를 가지고 관리하라는 의미이다[15]. 실제로, Verizon[2021]

보고서에 따르면, 매년 수집되어 드러난 조직의 정보보안 사고 중 내부자와 파트너에 의해 노출된 정보 사고는 전체 사고의 약 20%에서 30% 내외를 차지하고 있는 것으로 나타나고 있다[16]. 문제는 내부자에 의한 정보 노출 사고는 직위, 직무 등과 관계없이 발생 가능한 것으로 확인되고 있다. IT 부서의 기술 전문가, 사무직, 엔지니어, 영업직 등 정보 노출자는 다양한 직무를 가지고 있어, 정보 접근 가능성만 있으면 노출이 가능한 것으로 나타났다[16]. 즉, 내부의 정보보안 수준을 높이기 위해서는 조직원의 자발적인 정보보안 행동이 요구된다. 특히, 선행연구는 심리적 개선의 결과로서 정보보안 준수 의도 강화가 필요함을 지적한다[4,7]. 정보보안 준수 의도(IS Compliance Intention)는 외부의 침입으로부터 조직의 정보 자산 보호의 필요성을 인식하고, 조직의 정보 관리 체계를 통해 보안 관련 행동을 하고자 하는 의도를 지칭한다[6,8,17]. 즉, 조직의 정보 자산의 가치를 인식하고 외부로부터 보호하고자 하는 의식이 높아질수록 자발적인 준수 행동으로 이어진다[1]. 따라서, 본 연구는 정보보안 준수 의도 향상을 위한 개인 동기를 자기 결정성 이론에서 접목하고, 정보보안 정책 및 처벌 인식, 그리고 개인조직 적합성을 접목하여 정보보안 동기 강화 방안을 제시한다.

2.2 자기 결정성

자기 결정성 이론은 개인의 행동은 공동체 내 주어진 환경을 기반으로 스스로 행동 방식을 결정하기 위한 역량을 확보함으로써 이어질 수 있음을 제시하는 이론이다[18]. 즉, 집단에서 사람은 유기체로서 집단 환경에 대처하고 만족감을 얻기 위한 역량을 확보하고자 노력하는데, 자기실현을 위해 환경에 대처하는 역량을 확보했을 때 동기 및 행동으로 이어진다는 관점이다[11,19]. 특히, 자기 결정성 이론이 관심을 받는 이유는 집단의 구조적 특징이 자기실현을 위한 개인 역량 확보에 기여하고 행동으로 이어짐을 밝혔다는 측면이다[20]. 따라서, 조직은 조직원이 능숙하게 주어진 환경에 대처할 수 있는 역량을 확보할 수 있도록 다각적인 지원을 하는 것이 요구된다.

자기 결정성 이론은 개인이 조직의 요구사항을 이해하고 있을 때, 관련 요구사항에 대한 동기를 형성하고 긍정적 행동으로 이어지는 매커니즘을 제시한다[12]. 즉, 개인의 행동은 외부에 의해서 제시된 통제적 동기 조건과 본인의 결정에 기반하는 자율적 동기 조건이 복합적으로 작용하여 행동으로 이어진다[21]. 개인이 가지는 동기의 유형은 연구자 별 차이가 있는데, Fernet et al.[2008]과 Nie et al.[2015] 등은 조직 환경에서 개인의 동기를 내적 동기와 외적 동기로 구분하되, 외적 동기를 동일시 규제, 내사된 규제, 외적 규제로 구분하고 업무적 행동 변화 원인을 설명하였으며[20,22], Trépanier et al.[2015]은 통제된 동기와 자율적 동기로 구분하여 개인 행동 원천을 설명하였다[23]. 본 연구는 정보보안과 관련된 개인의 행동 동기를 설명하기 위하여, Fernet et al.[2008]의 동기 중 내적 동기(내재적 동기)와 외적 규제(외재적 동기)를 적용한다. 이유는 정보보안의 특성을 감안하였는데, 조직에서 정보보안 미준수 행동 결과에 대한 평가는 강력한 제재로 나타나기 때문에, 외재적 동기 중 가장 강력한 외적 규제에 따를 것이라 판단하였다. 더불어, 정보보안 관련 연구들은 개인의 내재적 동기 발현이 정보보안 준수 행동을 강화한다고 함께 제시하고 있다[9,24]. 즉, 본 연구는 정보보안 행동 결정에 영향을 주는 자기 결정 기반의 동기에 내적 동기와 외적 규제를 적용한다.

내적 동기(Intrinsic Motivation)는 자율적 동기, 즉 자기 결정적으로 행동을 결정하는 동기로서, 외부 환경으로부터 요구된 것을 이행함에 따라 확보가 가능한 즐거움, 만족감 등을 얻기 위하여 참여하고자 하는 동기를 지칭한다[22]. 즉, 개인이 대상 행동을 함으로써, 외부로부터 기대는 추가적인 보상이 아닌 내면의 변화 등을 기대하는 동기를 의미한다. 정보보안 측면에서, 정보보안이 조직의 요구와 이행에 따른 보상의 개념이 아닌 정보 관리가 즐겁거나, 본인 스스로 정보 관리 필요성이 강하게 인식된 경우를 지칭한다[9].

외적 규제(External Regulation)는 비자기 결정적 동기, 즉 통제된 환경에 따라 행동을 결정하는 동기로서, 행동의 예상되는 결과인 보상 또는 처벌에 대한 대처 관점에서 참여하고자 하는 동기를 지칭한다[22]. 즉, 개인이 환경이 제공하는 다양한 조건을 고려하여 최선의 이익을 위해 고려하는 수단으로서의 동기 개념이다. 정보보안 측면에서, 외적 규제는 조직이 추진하는 정책 일환으로서, 업무에 적용해야 할 보안 규정을 제공하고, 미준수 행동 적발 시 강력한 처벌을 보여줌으로써 조직원의 준수 행동을 유발한다[9].

특정 분야의 내적 동기와 외적 규제는 조직이 요구하는 활동에 대한 조직원의 준수 행동을 유발한다. 조직과 관련된 자기결정성 이론을 연구한 선행연구들은 조직의 외부 환경(업무 구조, 조직 문화, 업무 지원 활동 등)이 내재적 동기 및 외재적 동기를 기반으로 한 개인의 업무 동기에 영향을 미치고, 나아가 성과, 심리적 웰빙, 조직 신뢰, 직업 만족 등에 강한 영향을 주는 매커니즘이 존재

함을 밝혀왔다[11,20,22]. 정보보안과 관련하여, Padavachee[2012]는 정보보안 준수 행동에 영향을 주는 내적 동기와 외적 동기를 유형별로 세분화하였으며[25], Menard et al.[2017]은 정보보안에 대한 자기 결정 역량인 관계성, 역량, 자율성이 정보보안 관련 행동 의도에 영향을 주는 조건임을 밝혔다[8]. 또한, Son[2011]은 정보보안 행동 동기를 외재적 동기(처벌)와 내재적 동기(가치 일치, 인지된 합법성)로 구분하고[24], Chen et al.[2022]은 친 사회적 동기, 자기 규제 동기, 처벌 동기를 제시하여 조직이 고려해야 할 정보보안 행동 원인을 확인하였다[9]. 관련되어, 본 연구는 자기 결정성 이론에서 제시한 내적 동기와 외적 규제가 개인의 보안 행동에 긍정적 영향을 줄 것으로 판단하며, 다음 가설을 수립하였다.

H1 : 정보보안 관련 내적 동기는 정보보안 준수 의도에 긍정적 영향을 준다.

H2 : 정보보안 관련 외적 규제는 정보보안 준수 의도에 긍정적 영향을 준다.

2.3 정보보안 인식

조직원에 대한 정보보안 인식 제고는 조직이 내부의 정보보안 준수 전략을 위해 제공하는 다양한 프로그램의 주요 목적 중 하나이다[26]. 정보보안 인식(Awareness)은 정보 관리의 필요성을 이해하고, 정보보안 활동을 통해 도출되는 예상 결과와 부족 시 나타날 수 있는 잠재적인 문제에 대한 조직원의 전반적인 보안 지식과 이해를 의미한다[6,27,28].

정보보안과 관련된 인식은 상황별 다양한 관점에서 제시되고 있는데, Bulgurcu et al.[2010]은 정보보안 인식과 정보보안 정책 인식으로 구분하여, 일반적인 정보에 대한 인식과 조직이 도입한 보안 정책에 대한 인식으로 구분하였으며[6], D'Arcy et al.[2009]은 정보보안 준수를 위한 조직 활동과 관련된 관점에서 보안 정책 인식, 지원 프로그램 인식, 그리고 모니터링 인식으로 구분하여 제시하였다[27]. 또한, Park et al.[2017]은 건강 정보에 대한 보안과 관련된 인식으로 일반적 정보보안 인식, 규제 인식, 그리고 처벌 인식으로 구분하였다[26]. 즉, 연구에 적용된 상황에 따라, 개인이 인식하는 대상의 차이가 존재함을 의미한다. 본 연구는 조직원에게 정보보안 정책의 준수와 관련된 구조적 인식 조건을 확인하고자 하며, 정보보안 정책 인식과 처벌과 관련된 인식 요인을 적용한다.

정보보안과 같이 조직의 정책에 대한 조직원의 인식은 본인의 행동 조건에 영향을 준다. Bulgurcu et al.[2010]은 합리적선택이론의 선행 조건으로 정보보안 인식 요인을 밝혔으며, 인식을 통해 태도를 결정하는 정보보안 비용, 혜택 요인을 설정한다고 보았다[6]. 또한, Jaeger and Eckhardt[2021]은 시스템 관점에서 구축한 보안 경고 등의 지원 체계로 인한 상황적 정보보안 인식은 정보보안 보호 동기의 선행 조건이며, 인식이 강화될 때 보안 관련 행동으로 이어짐을 확인하였다[28]. 즉, 정보보안 관련된 상황별 인식은 개인의 정보보안 행동 동기를 통해 준수 활동으로 이어지는 매커니즘을 결정하는 선행 조건으로 인식할 수 있다. 이에, 본연구는 정보보안 정책 및 처벌 인식과 자기 결정성 관련된 정보보안 동기 요인, 그리고 준수의도 간의 관계를 확인하기 위하여 선행연구를 분석한다.

2.3.1 정보보안 정책 인식

정보보안 정책 인식(IS Policy Awareness)은 조직원이 조직의 정보보안 목적과 목표를 이해하고, 이상적으로 헌신하고자 하는 상태를 의미한다[6]. 정보보안 정책 인식은 조직이 그들의 특성에 맞추어 도입한 정책과 규정, 그리고 행동 요구사항 등, 정보보안 방향에서부터 수행 절차까지 이해하고, 행동의 필요성을 인식하고 있는 상황을 의미한다[28]. 따라서, 정보보안 정책 인식을 보유한 조직원은 정보보안 가치, 전략, 운영까지 인식하므로, 조직 차원의 보안 활동 지원이 유지될 경우 긍정적 행동으로 이어질 수 있다[2].

조직의 정보보안 정책에 대한 인식의 강화는 정보보안 활동에 대한 가치와 프로세스의 이해도를 높여 긍정적인 정보보안 행동을 유발할 수 있다. Da Veiga and Martins[2017]는 정보보안 문화에 따른 개인행동 변화 조건을 제시하면서, 정보보안 준수에 대한 긍정적인 조직 문화로 인해 형성된 인식은 개인의 행동에 영향을 주는 조건임을 제시하였다[29]. 또한, Momonov and Benbunan-Fich[2018]는 정보보안 위협에 대한 인식은 개인의 패스워드 강화 행동을 증가시킴을 확인하였다[30]. 동일한 맥락에서 정보보안 정책 인식과 조직원의 준수 의도 간에 긍정적 영향 관계가 형성될 것으로 판단하고, 가설을 수립하였다.

H3a : 정보보안 정책 인식은 조직원의 정보보안 준수 의도에 긍정적 영향을 준다.

또한, 조직원이 조직의 보안 관련 정책에 대하여 명확하게 인식할 때, 당사자는 정보보안 활동의 필요성을 느

끼는 내적 동기를 형성하거나, 통제 조건을 명확하게 이해함으로써 통제 조건에 대한 행동 동기를 형성한다. Ogbanufe[2021]은 정보보안 정책 인식이 조직원의 정보보안 업무 정체성을 강화하여, 정보보안 정책 관련 행동으로 이어지는 것을 확인하였으며[31], Xu et al.[2021]은 정보보안 정책에 대한 인식은 조직원의 조직에 대한 처벌의 명확성과 심각성 인식을 강화하여 정보보안 정책 준수로 이어지는 것을 확인하였다[2]. 또한, Jaeger and Eckhardt[2021]은 상황적 정보보안 인식은 정보 노출의 위협과 대처 효능감을 강화하여 정보보안 보호 동기를 높이는 것을 확인하였다[28]. 즉, 연구는 정보보안 정책 인식이 조직원의 내적 동기와 외적 규제에 긍정적 영향을 줄 것으로 판단하며, 가설을 수립하였다.

H3b : 정보보안 정책 인식은 정보보안 관련 내적 동기에 긍정적 영향을 준다.

H3c : 정보보안 정책 인식은 정보보안 관련 외적 규제에 긍정적 영향을 준다.

2.3.2 정보보안 처벌 인식

정보보안 처벌 인식(IS Sanction Awareness)은 정보보안 위반과 관련된 처벌 유형과 심각성에 대한 지식과 이해의 수준을 의미한다[26]. 처벌은 조직이 보편적으로 도입하는 보안 관련 규정으로서[24], 조직 내 특정 활동에 대한 구성원의 미준수 행동에 대하여 명확하고 강력한 처벌을 가할 때, 구성원이 미준수에 대한 우려를 통해 준수 행동으로 이어진다는 관점이다[2]. 따라서, 정보보안에 대한 처벌이 공정하고 명확하게 발생한다고 느끼는 사람은 미준수 행동과 관련된 결과의 두려움 또는 추가적 비용 발생에 대한 합리적 의사결정을 하고자 하며, 준수 행동을 하고자 한다[10].

정보보안 처벌은 조직의 정보보안 요구사항을 수용하도록 한다. Guo and Yuan[2012]은 조직 처벌, 팀 처벌, 그리고 개인 스스로 처벌에 따른 정보보안 준수 행동의 변화를 확인하였으며, 개인과 가까운 집단(팀)과 개인이 느끼는 인지된 처벌은 정보보안 회피 의도를 감소시킨다고 하였다[32]. 또한, Park et al.[2017]은 정보보안 처벌 인식이 환자의 건강 정보를 드러내는 행동과 부적 상관관계가 있다고 하였다[26]. 즉, 정보보안 처벌 인식은 정보보안 준수 의도와 긍정적 영향 관계를 형성할 것으로 판단하고, 가설을 수립하였다.

H4a : 정보보안 처벌 인식은 정보보안 준수 의도에 긍정적 영향을 준다.

또한, 정보보안 처벌 인식은 부분적으로 개인의 정보보안 동기, 태도 등 행동 원인 요소에 영향을 주어 준수 의도를 높인다. 선행연구는 처벌은 개인이 느끼는 심각성의 수준 등에 따라 개인의 받아들임의 차이가 발생한다고 보고 있다. D'Arcy et al.[2009]은 조직 차원에서 수행되는 정보보안 모니터링에 대한 인식은 조직원의 처벌에 대한 심각성과 명확성 인식을 높여 정보 오남용 의도를 감소시킨다고 하였다[27]. Jaeger and Eckhardt[2021]은 개인과 시스템 단위 요인을 통해 형성된 정보보안 인식은 인지된 두려움과 대처 효능감을 통해 조직원의 보호 동기를 강화하는 것을 확인하였다[28]. 반면, Guo et al.[2011]은 정보보안 미준수 행동에 대한 결과인 처벌에 대한 인식은 악의 없는 정보보안 침해 태도에 영향을 주지 못했는데, 그들은 외적 요인에 의한 동기보다 개인 스스로 위험에 대한 인식과 팀 규범이 더욱 크게 태도에 더욱 영향을 주기 때문이라고 하였다[33]. 하지만, 공통점은 개인이 받아들일 수 있는 처벌에 대한 적정한 인식 강화는 개인의 행동 원인에 긍정적 영향을 줄 수 있음을 밝히고 있다. 본 연구는 정보보안 처벌에 대한 인식이 형성된 조직원은 조직으로부터 받는 규제 동기의 인식과 본인의 내적 동기를 결정하도록 도움으로써 보안 관련 행동으로 이어지도록 도울 것으로 판단하고, 가설을 수립하였다.

H4b : 정보보안 처벌 인식은 정보보안 관련 내적 동기에 긍정적 영향을 준다.

H4c : 정보보안 처벌 인식은 정보보안 관련 외적 규제에 긍정적 영향을 준다.

2.4 개인조직 적합성

사람은 집단의 일원으로서 역할 및 소속감을 확보하고자 한다[34]. 적합성(Fit)은 개인을 둘러싼 특정 환경과 자신의 역량을 연계함으로써 균형감을 가지려고 하는 인식의 수준을 의미하며[13], 사람은 대상 환경에 포함된 개인은 환경의 요구사항에 대하여 자신만의 지식, 경험 등을 통해 확보한 역량을 적용하여, 균형점을 맞추고자 한다. 개인조직 적합성은 비전, 목표, 가치와 같이 조직이 설정하고 수행하는 무형의 조건이 개인이 보유한 가치와 동일하다고 판단하는 수준을 의미한다[34]. 즉, 조직은 조직원에게 조직 내 특정 역할을 부여할 때, 조직이 보유하고 있는 특정 가치에 기반한 역할 및 이에 따른 행동을 요구한다. 반대로, 개인은 본인이 보유한 가치를 달성하기 위해 조직에서 구성원으로서 역할을 하고, 관련

활동을 위한 지원을 조직에게 요구한다[35]. 조직과 개인 간의 상호 교환 관계에서 가치의 일치성이 발현될 때, 개인조직 적합성은 높아지게 되며 상호 역할을 인정하며, 동일한 목표를 위해 노력하게 된다는 관점이다[13,35].

조직원 관점에서 개인조직 적합성의 인식은 조직의 가치 달성을 위한 활동이 본인의 가치 달성에 기여하도록 돕는 조건이라고 생각하도록 하므로, 조직 내 업무 만족도를 높이거나, 조직 몰입을 높여, 조직 성과 달성에 기여하는 조건이다. Jung et al.[2010]은 조직의 윤리적 가치에 대한 인식이 개인에게 개인조직 적합성을 높여, 이직의도를 낮춘다고 하였으며[36], Andrews et al.[2010]은 개인조직 적합성이 조직 몰입 및 만족도를 높인다고 하였다[34]. 또한, Wang and Li[2019]는 고등학교에서 개인과 수요, 역할, 사람 등 간의 다양한 적합성은 업무성과 달성에 기여함을 확인하였다[37].

정보보안 관점에서도 개인조직 적합성은 개인의 행동 전환에 도움을 줄 수 있다. 조직의 정보의 가치와 정보보안 활동의 가치는 결국 조직이 개인에게 필요성을 인식시키고, 관련 지원을 지속해서 제공하되, 개인이 보안 관련 요구사항을 받아들여야 하는데, 개인조직 적합성은 해당 가치 활동을 높이고, 조직 동일시를 강화하는 조건이다[38].

조직에서 개인이 특정 대상 및 환경에 대하여 느끼는 적합성은 개인이 조직으로부터 느끼는 특정한 동기가 관련된 행동 또는 결과에 미치는 영향을 조절한다. Lim et al.[2019]은 학교 조직에서, 개인이 직업 만족도를 가지기 위해서는 외재적 동기 개념인 보상이 선행되어야 한다고 보았다[39]. 특히, 그들은 개인조직 적합성이 보상과 상호작용 효과를 가져 직업 만족도에 미치는 영향을 증가시킴을 확인하였다. 반대로, Junaedi and Wulani[2021]은 개인조직 적합성이 개인이 업무적으로 느끼는 스트레스에 의한 부정적 영향을 조절하여, 부정적 행동을 최소화하는 요인임을 확인하였다[35]. 동일한 맥락에서, 본 연구는 개인조직 적합성은 정보보안에 대하여 조직원이 인식하는 다양한 동기 유형(내적 동기, 외적 규제)의 영향을 조절하여 긍정적 행동을 강화하는 요인이라 판단한다. 따라서, 연구는 개인조직 적합성과 동기간의 조절 효과에 대한 가설을 수립하였다.

H5a : 내적 동기가 정보보안 준수 의도에 미치는 영향은 개인조직 적합성을 통해 조절 된다.

H5b : 외적 규제가 정보보안 준수 의도에 미치는 영향은 개인조직 적합성을 통해 조절된다.

3. 연구모델 및 데이터 수집

3.1 연구모델

본 연구는 조직 내부자의 정보보안 준수 의도 강화를 설명하는 것을 목적으로 한다. 세부적으로, 자기 결정성 이론을 토대로 동기 요인(내적 동기, 외적 규제)을 적용하였으며, 정보보안 인식 요인과 개인조직 적합성을 반영한다. 연구 모델은 Fig. 1과 같다.

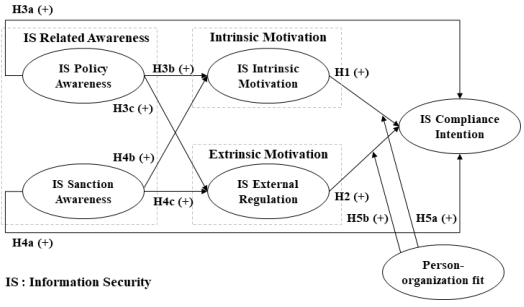

Fig. 1. Research Model

3.2 측정 도구 및 데이터 수집

본 연구는 조직원의 정보보안 준수 의도 향상 방안 관련 연구 모델의 검증을 위해, 적정 대상을 선정하고 설문지 기법으로 응답자의 인식을 확인하고자 한다. 이를 위하여, 정보보안 및 조직 분야의 선행연구에서 제시한 요인별 측정 문항을 정보보안 특성에 맞추어 변경하였다. 또한, 연구는 정보보안 설문 문항이 적절하게 구성되었는지를 확인하기 위하여 경영 대학원에 다니는 직장인 10명에게 도출된 설문 문항을 확인하고 수정 완료하였다. 측정 도구는 리커트 척도로 구성하였다(1점: 매우 그렇지 않다, 7점: 매우 그렇다).

정보보안 정책 인식은 합리적 선택이론을 정보보안에 적용한 Bulgurcu et al.[2010] 연구에서 항목을 확보하였으며[6], “우리 조직의 정보보안 정책에서 규정한 규칙을 알고 있음”, “우리 조직의 정보보안 정책에서 규정한 규칙을 이해하고 있음”, “조직의 정보보안을 강화하기 위해 보안 정책에 규정된 책임을 알고 있음”을 적용하였다. 정보보안 처벌 인식은 병원 내 정보보안 연구를 수행한 Park et al.[2017] 연구에서 항목을 확보하였으며[26], “나는 정보보안 정책을 위반할 경우 징계를 받을 것을 알고 있음”, “나는 정보보안 정책을 반복적으로 어길 때 엄중한 처벌을 받는 것을 알고 있음”, “나는 정보보안 정책을 위반할 경우 명확하게 처벌받는 것을 알고 있음”을 적

용하였다.

자기 결정성 기반 동기는 조직 행동에 동기 유형을 제시한 Fernet et al.[2008] 연구에서 내적 동기와 외적 규제의 항목을 확보하였으며[22], 내적 동기는 “나는 정보보안 정책을 업무에 적용하는 것을 즐겁다고 생각함”, “나는 정보보안 정책을 업무에 적용하는 것을 흥미롭다고 생각함”, “나는 정보보안 정책을 업무에 적용하는 것을 좋아함”을 적용하였으며, 외적 규제는 “나에게 주어진 업무는 정보보안 정책을 적용하는 것을 요구함”, “조직은 정보보안 정책을 업무에 적용하는 것을 의무적으로 요구함”, “나는 조직으로부터 정보보안 정책을 지키는 것을 요구받았음”을 적용하였다.

정보보안 준수 의도는 Bulgurcu et al.[2010] 연구에서 항목을 확보하였으며[6], “앞으로 우리 조직의 보안 정책과 관련된 요구사항을 준수할 의향이 있음”, “앞으로 우리 조직의 보안 정책의 요구사항에 따라 정보와 기술 자원을 보호할 의향이 있음”, “앞으로 정보기술 사용 시 조직에서 정한 규칙과 책임에 따라 행동할 의향이 있음”을 적용하였다. 개인조직 적합성은 조직과 개인 간의 관계에서 적합성의 중요성을 설명한 Valentine et al.[2002] 연구에서 항목을 확보하였으며[13], “개인적 가치가 우리 조직과 잘 맞는다고 느낌”, “우리 조직은 다른 사람과 관련된 관심에 대하여 나와 같은 가치를 보유하고 있음”, “우리 조직은 정직과 관련하여 나와 같은 가치를 보유하고 있음”, “우리 조직은 공정성과 관련하여 나와 같은 가치를 가지고 있음”을 적용하였다.

Table 1. Characteristics of Samples

Categories		Frequency	%
Gender	Male	209	49.2
	Female	216	50.8
Age	〈 30	98	23.1
	31 - 40	96	22.6
	41 - 50	109	25.6
	〉 51	122	28.7
Industry	Manufacture	125	29.4
	Service	300	70.6
Size	〈10	27	6.4
	10-50	106	24.9
	51-300	143	33.6
	〉300	149	35.1
Job Position	Under Manager	177	41.6
	Manager	164	38.6
	Over Manager	84	19.8
Total		425	100.0

설문 대상은 정보보안 정책을 수립하고, 정해진 규정과 활동을 개인들의 업무에 적용하는 것을 요구하는 조직의 근로자로 하였다. 본 연구는 선정한 설문 대상을 정확하게 확보하기 위하여, M리서치 기업이 보유한 직장인 회원을 대상으로 온라인 설문을 하였다. 특히, 연구는 직장인이면서 정보보안을 적용하고 있음을 확인하기 위하여, 설문 전 직업을 확인하고 정보보안 정책을 업무에 적용하는지를 확인하였다. 모든 요구사항에 충족한 사람만 설문에 참여하도록 하였으며, 추가로 설문 목적과 확보한 통계의 활용방법에 대하여 설명한 후 설문을 허가한 사람만 본 설문에 참여하도록 하였다.

본 연구는 총 425건의 유효 표본을 확보하였으며, 연구는 특히, 국내 기업 특성을 최대한 반영하기 위하여, 온라인 설문 시 표본을 특성별 조정하였는데, 성별과 나이는 비슷한 비중으로 확보하고자 하였으며, 업종은 제조업과 서비스업을 약 3대 7 수준으로 구분하고자 하였다. 특히, 조직 규모의 경우 국내 10인 미만의 소기업은 정보보안 정책이 낮은 수준이므로, 적게 확보하였으며, 규모가 클수록 더 많은 표본을 확보하도록 구조화하였다. 통계적 특성은 Table 1과 같다.

4. 가설 검증

4.1 신뢰성, 타당성 분석

본 연구는 연구 모델에 적용한 요인에 대하여 다 항목으로 구성된 측정 도구를 적용하였으므로, 적용 요인의 신뢰성 및 타당성 분석을 수행하였다.

첫째, 신뢰성은 요인별 측정 도구들의 일관성을 확인하는 것으로서, 본 연구는 SPSS 21.0 패키지의 크론바흐 알파를 통해, 신뢰성을 확인한다. 선행연구는 신뢰성 확보를 위해 요인별 0.7 이상의 크론바흐 알파를 요구한다[40]. 본 연구에 적용된 6개의 요인은 총 25개의 문항으로 구성되어 있으며, 신뢰도에 문제를 가진 1개 문항(ISIM1)을 제외한 24개의 문항을 적용하였다. 요인별 확인한 크론바흐 알파는 Table 2와 같으며, 모든 요인이 요구사항을 충족하였다.

둘째, 타당성은 적용된 측정항목이 요인별 일관성을 보유하고, 요인별 차별성을 지니는지를 확인하는 것으로서, 본 연구는 AMOS 22.0 툴의 확인적 요인분석을 구하고, 각각의 타당성을 확인하고자 한다. 우선, 연구는 확인적 요인분석 모형의 적합도가 요구수준에 일치하는지를 확인하였다. 결과는 $x2/df$ = 1.604, NFI = 0.964,

CFI = 0.986, RMSEA = 0.038, RMR = 0.044, GFI = 0.954, AGFI = 0.935와 같이 나타났다. 즉, 구조모형에서 요구하는 적합도 수치에 대하여 모든 요구사항이 충족된 것으로 나타났다. 이후, 연구는 요인별 측정항목의 일관성 확인하기 위하여 집중 타당성을 확인하였다. AMOS 22.0에서 집중 타당성은 개념 신뢰도(CR)와 평균분산추출(AVE)을 구하여야 하는데, 선행연구는 0.7 이상의 개념 신뢰도와 0.5 이상의 평균분산추출 값을 요구한다[41]. Table 3은 집중 타당성 분석 결과를 보여주며, 적용된 모든 요인의 개념 신뢰도와 평균분산추출은 요구사항을 충족한 것으로 나타났다.

Table 2. Validity of Variables

Variables		Estimate	SRW Estimate	Standard Error	Critical Ratio	Cronbach's Alpha
ISPA	ISPA3	1.000	0.871			0.884
	ISPA2	0.967	0.870	0.044	22.19**	
	ISPA1	0.917	0.804	0.046	19.93**	
ISSA	ISSA3	1.000	0.846			0.908
	ISSA2	1.039	0.922	0.042	24.47**	
	ISSA1	0.918	0.870	0.041	22.65**	
ISIM	ISIM3	1.000	0.885			0.866
	ISIM2	0.965	0.862	0.051	18.85**	
ISER	ISER3	1.000	0.856			0.808
	ISER2	0.931	0.733	0.060	15.40**	
	ISER1	0.883	0.734	0.057	15.42**	
ISCI	ISCI3	1.000	0.852			0.898
	ISCI2	1.064	0.905	0.045	23.61**	
	ISCI1	1.018	0.836	0.048	21.17**	
PO fit	PO fit4	1.000	0.807			0.899
	PO fit3	1.001	0.871	0.049	20.44**	
	PO fit2	0.961	0.833	0.050	19.31**	
	PO fit1	0.977	0.821	0.052	18.95**	

ISPA(IS Policy Awareness), ISSA(IS Sanction Awareness), ISIM(IS Intrinsic Motivation), ISER(IS External Regulation), ISCI(IS Compliance Intention), PO fit(Person-organization fit)
SRW(Standard Regression Weight), **: p < 0.01

그리고, 연구는 요인 간의 차별성을 확인하기 위하여 판별 타당성을 확인하였다. 선행연구는 요인의 상관계수와 평균분산추출의 제곱근을 비교하되, 평균분산추출 제곱근이 상관계수보다 모두 클 때, 판별 타당성이 존재한다고 본다[41]. 판별 타당성 확인 결과는 Table 3과 같으며, 요구사항을 충족하였다.

마지막으로, 연구는 설문지 기법으로 응답자의 설문 당시의 인식을 영향 관계에 있는 모든 변수를 측정하였는데, 응답 과정에서 편향이 발생할 수 있어, 공통방법편의 문제를 확인하였다. 공통방법편의 문제 확인은 Podsakoff et al.[2003]이 제시한 다양한 기법 중 일반적으로 활용되는 비측정 잠재방법 요인 기법을 적용하였다. 해당 기법은 확인적 요인분석 모델에 단일 요인을 추가하여 측정항목과 연결한 모델을 만들고, 두 모델 항목의 결과치를 비교하는 방법이다[42]. 우선, 확인적 요인분석 모델($x2$/df = 1.604, NFI = 0.964, CFI = 0.986, RMSEA = 0.038, RMR = 0.044, GFI = 0.954, AGFI = 0.935)과 단일 요인을 추가한 모델의 적합도($x2$/df = 1.311, NFI = 0.975, CFI = 0.994, RMSEA = 0.027, RMR = 0.029, GFI = 0.968, AGFI = 0.946)를 확인하였으며, 모두 적합도 요구사항을 충족하여, 두 모델의 측정치를 비교하였다. 모든 값이 0.3 미만의 차이를 보여 공통방법편의 문제는 크다고 판단되지 않아, 가설 검증을 수행하였다.

Table 3. Discriminant Validity

Variable	CR	AVE	1	2	3	4	5	
ISPA	0.870	0.692	**0.83[a]**					
ISSA	0.880	0.710	.60**	**0.84[a]**				
ISIM	0.846	0.648	.48**	.41**	**0.81[a]**			
ISER	0.759	0.513	.44**	.44**	.50**	**0.71[a]**		
ISCI	0.875	0.699	.54**	.56**	.56**	.58**	**0.83[a]**	
PO fit	0.814	0.686	.45**	.35**	.61**	.46**	.46**	**0.82[a]**

ISPA(IS Policy Awareness), ISSA(IS Sanction Awareness), ISIM(IS Intrinsic Motivation), ISER(IS External Regulation), ISCI(IS Compliance Intention), PO fit(Person-organization fit)
a: square root of the AVE, **: p < 0.01

4.2 경로검증

본 연구는 주 효과와 조절 효과를 분리하여 검증한다. 주 효과는 AMOS 22.0의 구조방정식 모형을 적용하였으며, 조절 효과는 Hayes의 Process 3.1을 적용하였다. 구조방정식 모형을 반영한 주 효과 검증을 위해, 본 연구는 확인적 요인분석에 적용한 수치와 동일한 적합도 검증을 하였다. 주 효과 모형의 적합성 분석 결과는 $x2$/df = 2.049, NFI = 0.966, CFI = 0.982, RMSEA = 0.05, GFI = 0.958 그리고, AGFI = 0.935와 같이 나타났다.

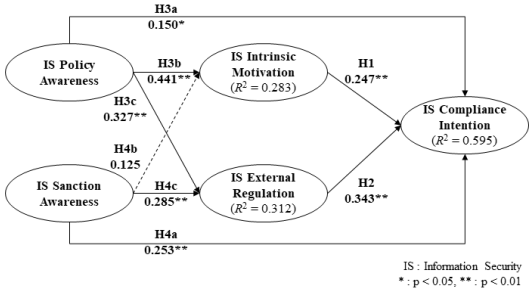

Fig. 2. Results of Direct Effects

Table 4. Results of Direct Effects

Path		Coefficient	t-value	Results
H1	ISIM → ISCI	0.247	5.081**	Supported
H2	ISER → ISCI	0.343	6.541**	Supported
H3a	ISPA → ISCI	0.150	2.388*	Supported
H3b	ISPA → ISIM	0.441	6.038**	Supported
H3c	ISPA → ISER	0.327	4.65**	Supported
H4a	ISSA → ISCI	0.253	4.442**	Supported
H4b	ISSA → ISIM	0.125	1.810	Not Supported
H4c	ISSA → ISER	0.285	4.113**	Supported

ISPA(IS Policy Awareness), ISSA(IS Sanction Awareness), ISIM(IS Intrinsic Motivation), ISER(IS External Regulation), ISCI(IS Compliance Intention)
**: $p < 0.01$

적합도 결과는 전체적인 형태의 적합도를 확인하는 구조방정식 모형 특성상 모든 요구 수치가 적합하게 나타났기 때문에, 요인 간의 경로 분석(β)을 하였다. 연구가설 검증 결과는 Fig. 2, Table 4와 같다.

가설 1은 정보보안 내적 동기가 조직원의 정보보안 준수 의도에 긍정적 영향을 준다는 것으로, 내적 동기와 준수 의도 간의 경로 분석 결과는 통계적으로 유의하였다(H1: β = 0.247, $p < 0.01$). 또한, 가설 2는 정보보안 관련 외적 규제가 조직원의 정보보안 준수 의도에 긍정적 영향을 준다는 것으로, 외적 규제와 준수 의도 간의 경로 분석 결과는 통계적으로 유의하였다(H2: β = 0.343, $p < 0.01$). 이러한 결과는 정보보안에 대한 개인의 자기 결정성이 조직이 요구하는 정보보안 활동에 중요한 선행 조건이 됨을 밝히는 Menard et al.[2017]의 연구와 유사하다[8]. 즉, 정보 관리와 보호가 개인에게 도움이 되고 보호의 필요성을 자체적으로 인식하는 내적 동기와 정보보안 정책이 제시하는 규제적 관점을 받아들이는 외적 동기가 보안 관련 행동에 영향을 줌을 의미한다. 따라서, 조직은 단기적으로는 정보보안 규제를 명확하게 인식할 수 있도록 하고, 중장기적으로 조직원의 자발적 참여를 유도할 수 있는 활동을 수행하는 것이 요구된다.

가설3은 정보보안 정책 인식이 동기와 준수 의도에 긍정적 영향을 준다는 것으로, 준수 의도(H3a), 내적 동기(H3b), 그리고 외적 규제(H3c)에 미치는 정보보안 정책 인식의 영향은 통계적으로 유의하였다(H3a: β = 0.150, $p < 0.05$, H3b: β = 0.441, $p < 0.01$, H3c: β = 0.327, $p < 0.01$). 이러한 결과는 정보보안 정책 인식이 개인의 합리적 선택에 조건에 영향을 주어 준수의도로 이어진다는 Bulgurcu et al.[2010]의 연구와 유사한 결과이다[6]. 즉, 정보보안 정책을 명확하게 인식한 개인은 스스로의 정보 관리의 필요성을 확립하고, 조직이 추진하는 보안 정책에서 지켜야할 규제적 조건을 인식함을 의미한다. 따라서, 조직은 자사의 정보보안 정책에 대한 정보를 명확하게 조직원에게 전달하는 노력이 요구된다.

가설 4는 정보보안 처벌 인식이 동기와 준수 의도에 긍정적 영향을 준다는 것으로, 준수 의도(H4a)와 외적 규제(H4c) 에 미치는 정보보안 정책 인식의 영향은 긍정적 영향을 주었으나, 내적 동기(H4b)는 유의수준 10%에서만 영향을 주어 영향력이 약한 것으로 나타났다(H4a: β = 0.253, $p < 0.01$, H4b: β = 0.125, n.s, H4c: β = 0.285, $p < 0.01$). 처벌은 개인의 행동에 영향을 주는 대표적인 외적 동기 인식 요인으로 미준수 행동에 대한 비용으로 인지되므로[6], 처벌이 외적 동기인 외적 규제에 영향을 준 결과와 정보보안 준수의 의도에 긍정적 영향을 준 것은 처벌 관련 선행연구와 유사하다. 반면, 내적 동기에는 영향을 주지 않았는데, 이러한 결과는 처벌 인식, 인지된 위험과 달리 태도에 영향을 주지 않았다는 Guo et al.[2011]의 연구와 유사한 결과이다[33]. 즉, 엄격한 수준의 처벌은 외부의 환경적 조건에 대한 개인의 강한 받아들임 요소임을 의미한다. 다만, 대상 요인들의 관계는 적게나마 영향을 주는 것으로 나타났기 때문에, 개인의 내면 동기 변화 관점에서 처벌이 중요한 조건임은 맞는 것으로 판단된다. 즉, 조직은 정보보안 처벌이 단순히 엄격한 수준과 부정적 영향만을 주는 것이 아니라, 처벌을 통해 조직 전체의 정보 관리 체계가 완성될 수 있음을 제시하는 것이 필요하다.

마지막으로, 연구는 경로 검증에 적용된 변수들의 영향력(R^2)을 확인하였다. 정보보안 정책과 처벌 인식은 정보보안 내적 동기에 28.3%의 영향을 주었으며, 정보보안 정책과 처벌 인식은 외적 규제에 31.2%의 영향을 주었다. 그리고, 정보보안 정책, 처벌 인식과 내적, 외적 동기는 준수 의도에 59.5%의 영향을 주었다.

4.3 조절 효과 검증

가설 5는 개인조직 적합성이 정보보안 관련 동기(내적 동기, 외적 규제)가 준수 의도에 미치는 긍정적 영향을 조절한다는 것으로, 본 연구는 Hayes[2017]의 Process 3.1을 적용하여, 조절 효과를 검증하였다[43]. 이에, 연구는 Hayes의 모델 1을 적용하였으며, 부트스트래핑 5,000과 신뢰도 95%를 적용하였다. 개인조직 적합성의 조절 효과 검증 결과는 Table 5와 같다.

Table 5. Results of Moderating Effect of PO fit

		Coefficient	t-value	Result
ISIM x POfit → ISCI (H5a)	Constant	5.1720	114.6667**	Supported
	Usef	0.4271	8.6258**	
	Terr	0.1461	3.0296**	
	Interaction	-0.1180	-3.7934**	
	F = 79.8504, R2 = 0.3627			
ISER x POfit → ISCI (H5b)	Constant	5.1228	122.1048**	Not Supported
	JC	0.4717	10.7581**	
	AL	0.2139	5.0787**	
	Interaction	-0.0602	-1.9193	
	F = 92.1498, R2 = 0.3964			

ISIM(IS Intrinsic Motivation), ISER(IS External Regulation), ISCI(IS Compliance Intention), PO fit(Person-organization fit)
**: p 〈 0.01, *: p 〈 0.05

세부적으로, 개인조직 적합성이 내적 동기와 준수 의도 간의 긍정적 영향 관계를 조절한다는 가설 5a는 유의수준 5%를 기준으로 채택되었으나, 개인조직 적합성이 외적 규제와 준수 의도 간의 긍정적 영향 관계를 조절한다는 가설 5b는 유의수준 5%를 기준으로 기각되었다. 하지만, 가설 5b는 유의수준 10%에서 채택되어, 어떠한 영향을 적게나마 영향을 주는지 세부 가설(H5a, H5b)의 영향을 단순 기울기 그래프를 통해 확인하였다.

Fig. 3과 Fig. 4는 개인조직 적합성의 조절 효과 영향 그래프이다. 그래프를 확인한 결과, 내적 동기가 준수 의도에 미치는 긍정적 영향에 개인조직 적합성은 내적 동기가 높은 집단에서는 영향의 큰 차이는 없었으나, 내적 동기가 낮은 집단에서는 개인조직 적합성이 강한 영향을 주어, 개인의 준수 의도를 높이는 것으로 나타났다. 외적 규제의 경우 내적 동기와 유사한 패턴을 보였으나, 영향의 차이는 크지 않았다.

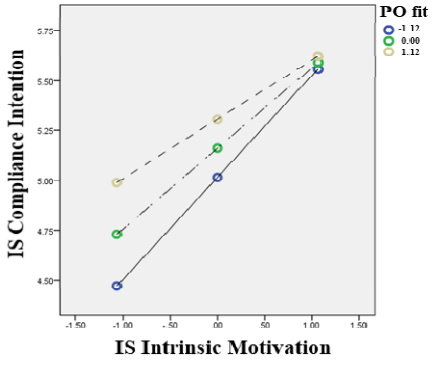

Fig. 3. Moderating Effect of PO fit (H5a)

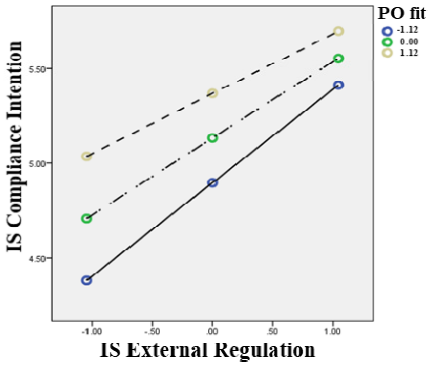

Fig. 4. Moderating Effect of PO fit (H5b)

개인조직 적합성의 조절효과 분석 결과는 조직원이 보유한 정보보안 동기가 행동에 미치는 영향을 강화함을 의미한다. 개인조직 적합성이 높은 사람은 조직에 대한 동질성을 강하게 인식하고 있으므로, 자신의 이익을 위하여 조직이 요구하는 활동에 대하여 적극적으로 참여하려는 의도를 가진다. 본 연구에 따르면 해당 상황에 대한 동기를 가진 사람은 개인조직 적합성과 연계하여 강한 영향을 줄 수 있음을 의미한다. 따라서, 조직은 조직원에게 조직이 추진하는 가치와 목적을 명확하게 알림으로써, 조직원이 조직과 함께하여 성장할 수 있음을 인식하게끔 지원하는 것이 요구된다.

5. 결론

5.1 요약

비대면에 대한 업무적 대처의 일환인 온라인 교류 기술과 같은 새로운 시스템의 도입은 조직원들의 업무 생산성을 높이는 요인으로 인식되고 있으나, 정보시스템에 대한 접근 및 통제가 어려운 비대면 상황에서의 정보 교류 활동 등과 같은 다각적인 이유로 정보보안에 대한 우려 또한 커지고 있다. 특히, 내부자의 정보보안 준수 활동은 당사자의 심리적 관점에서 접근해야 하는데, 심리적 개선을 통하지 않은 내부자의 정보 접근 권한의 강화는 정보 노출 위협을 커지게 한다.

본 연구는 자기 결정성 관점에 주목하여, 정보보안 관련 개인의 행동 동기를 자율적 동기 측면과 통제적 동기 측면으로 구분하고, 동기 강화를 위한 조건을 제시하는 것을 목적으로 하였다. 세부적으로 본 연구는 정보보안 정책 인식과 처벌 인식이 개인의 정보보안 내적 동기와

외적 규제를 통해 정보보안 준수 의도 향상에 미치는 매커니즘을 확인하고자 하였으며, 개인조직 적합성이 정보보안 관련 동기의 영향을 어떻게 조절하는지를 확인하고자 하였다.

본 연구는 정보보안 정책을 조직 내 업무에 적용하고 있는 조직에 근무하는 사람을 대상으로 설문 조사를 하였으며, 확보한 425건의 유효 표본을 AMOS 22.0과 Process 3.1에 적용하여 가설을 검증하였다. 결과는 정보보안 정책 인식이 내적 동기와 외적 규제를 통해 준수 의도에 영향을 주었으며, 정보보안 처벌 인식이 외적 규제를 통해 준수 의도에 영향을 주었다. 그리고, 개인조직 적합성이 정보보안 관련 내적 동기가 준수 의도에 미치는 긍정적 영향을 강화하였다.

5.2 연구의 시사점 및 향후 연구

본 연구는 심리적 관점에서 정보보안 행동 강화를 위한 연구를 진행함으로써, 이론적 측면에서의 시사점을 제시한다. 첫째, 본 연구는 조직과 개인 간의 관계에서 개인이 성장을 위해 조직으로부터 요구된 특정 항목에 대한 역량을 확보하고 동기를 부여하여 행동으로 이어지는 것을 체계적으로 설명하는 자기 결정성 이론을 정보보안에 적용하였다. 기존 정보보안 관련 연구는 개인의 정보보안 인식과 관련된 조건이 보호동기 이론, 합리적 선택이론 등과 연계하여 행동 변화를 측정하는 모델로서 활용할 수 있음을 밝혔다면[6,28], 본 연구는 자기결정성 이론의 다양한 동기 조건을 정보보안 분야에 적용하되, 특히 인식 요인과 동기 요인 간의 영향 관계가 직접적으로 존재할 수 있음을 밝히고자 하였다. 특히, 본 연구는 자기 결정성이 제시하는 동기 요소 중 자율적 측면의 동기 개념인 내적 동기와 통제적 측면의 동기 개념인 외적 규제를 정보보안 분야에 적용하여, 요인으로 도출하였으며, 조직원의 행동 의도에 미치는 영향을 확인하였다. 즉, 이론 관점에서 본 연구는 개인의 정보보안 활동에 영향을 주는 동기 요인을 다각적으로 구분하여 제시한 측면에서 의미가 있다.

둘째, 본 연구는 조직원의 정보보안 준수 활동에 복합적으로 영향을 주는 동기 요인을 향상하는 관점에서 정보보안 인식 요인을 적용하였다. 동기 개선과 관련하여, 조직 환경과 관련된 선행연구는 조직이 제공해야 할 목적, 가치, 모니터링 체계, 교육 프로그램 등 조직 활동 단위의 접근을 시도했다면[1,27], 본 연구는 조직이 제공한 정보보안 관련 특정 정보에 대한 개인 인식의 중요성을 제시하고 영향 관계를 확인하였다. 세부적으로, 연구는 조직이 구축한 정보보안에 대한 인식을 분류하여, 정책 인식과 처벌 인식으로 구분하여 동기에 미치는 영향을 확인하였다. 특히, 정보보안 정책 인식은 개인의 내적, 외적 동기에 영향을 주는 요인이며, 처벌 인식은 주로 외적 동기에 영향을 주는 요인임을 확인하였다. 선행연구에서 처벌의 영향은 상황별 차이가 있음을 밝혔다면[6,33], 본 연구는 처벌인식은 적게나마 내적 동기에 영향을 주긴 하지만, 외적 규제에 대한 동기 인식 중심으로 정보보안 동기를 형성시켜 정보보안 준수의도로 이어지는 매커니즘을 밝혔다는 측면에서 의미를 가진다. 따라서, 단기적으로 동기 강화를 위해서는 조직원의 처벌 인식을 강화하는 노력이 요구되며, 전체적인 정책에 대한 방향성을 이해하도록 조직원을 훈련시키는 노력이 요구된다. 이론 관점에서 본 연구는 정보보안 정책과 처벌에 대한 개인의 인식이 어떻게 동기를 통해 행동으로 이어지는지를 체계적으로 설명한 관점에서 자기 결정성을 정보보안 분야에 접목한 선행연구로서의 의미가 있다.

셋째, 본 연구는 개인조직 적합성을 적용하여, 개인에게 형성된 정보보안 관련 동기가 준수 의도에 미치는 영향을 강화하는 것을 확인하였다. 정보보안 선행연구는 개인에게 형성된 동기 또는 태도를 강화하기 위해 독립변수로서 조직 환경 조건 등을 중점적으로 제시해왔다[10,31]. 반면, 본 연구는 개인과 조직 간에 가치의 일치로 발현된 적합성이 정보보안에 대한 동기의 영향까지 변화를 일으킬 수 있음을 확인하였다. 즉, 본 연구는 정보보안 동기와 행동 간의 관계에 정보보안이 아닌 다른 감정에 의해 영향을 받을 수 있음을 제시하였기 때문에, 선행연구로서 이론적 의미가 있다.

본 연구는 조직이 내부의 정보보안 목표를 달성하기 위해 추진해야 할 활동 방향을 정립한 관점에서 조직 행동적 의미가 있다. 첫째, 본 연구는 조직원의 정보보안 준수 활동에 영향을 주는 내적 동기를 제시하고, 내적 동기 강화 방안을 마련하였다. 내적 동기는 개인이 외부의 특정 조건을 통해 행동 변화를 추구하는 것이 아니라, 스스로 필요성에 의해 추진하려고 하는 개념이다. 정보보안과 관련하여 정보의 가치를 이해하고, 정보보안 활동의 필요성을 스스로 인식할 때, 개인은 내적 동기를 형성할 수 있다. 특히, 연구는 내적 동기 강화는 결국 정보보안 정책에 대한 이해와 내재화가 무엇보다 중요한 선행개념임을 제시하였다. 즉, 연구는 조직 보안 환경에 대한 개인의 인식, 동기, 그리고 행동으로 이어지는 매커니즘을 설명하고자 하였다. 따라서, 조직은 구성원에게 조직의 정보보안 정책에 대하여 정확하게 이해하고, 지식으

로 받아들일 수 있는 정보 제공 프로그램을 강화하는 것이 필요하다. 정보보안 캠페인, 교육 및 훈련, 가이드라인 제공 등 언제든 정보보안의 필요성을 스스로 인식할 수 있도록 정보를 제공한다면, 조직원의 자발적인 보안 행동을 도출할 수 있을 것이다.

둘째, 본 연구는 조직의 정보보안 규제 환경에 의해 동기적 영향을 받을 수 있음을 확인하고, 외적 동기 강화를 위한 인식 조건을 제시하였다. 처벌은 조직이 우선적으로 추진할 수 있는 명료한 행동 강화 조건이다. 즉, 정보보안 미준수 행동에 대한 예상되는 결과가 명료하며 강력한 처벌로 이어짐을 이해시킨다면 조직원은 비용의 최소화를 위한 행동을 할 가능성이 존재한다. 특히, 본 연구는 외적 동기 강화를 위한 요인으로 정보보안 정책 인식과 정보보안 처벌 인식이 존재함을 제시하였다. 따라서, 조직은 구성원이 정보보안 정책 및 규정에 대하여 이해하는 것뿐 아니라, 미준수 시 발생 가능한 처벌을 이해할 수 있도록 정보화하여 제공하는 것이 요구된다.

마지막으로, 본 연구는 개인에게 형성된 정보보안 관련 동기의 영향을 강화하기 위한 조절적 조건인 개인조직 적합성을 제시하였다. 즉, 정보보안과 관련된 요소가 아닌 조직과 개인 간의 가치적 일치성이 강화될수록 조직원은 조직이 추진하는 보안 방향에 대하여 자신의 가치와 동일하게 생각하고 행동으로 이어지는 것을 의미한다. 특히, 개인이 보유한 내적 동기와 높은 상호작용 효과를 발휘하는데, 정보보안에 대한 개인적 필요성과 조직에 대한 가치가 연계된 것으로 판단된다. 따라서, 조직은 정보보안을 넘어 조직이 성장을 위해 추진하는 가치에 대하여 조직원이 이해하고 일체화하도록 지속해서 정보를 제공하는 것이 요구된다.

본 연구는 조직이 구축한 정보보안 정책, 처벌과 같은 인식이 동기를 통해 행동으로 이어지는 매커니즘을 발견하고, 동기 강화 방안을 마련한 측면에서 의미가 있으나, 다음의 연구적 한계가 존재한다. 첫째, 본 연구는 조직의 정보보안에 대한 준수 의도를 개인이 느끼는 인식 수준 기반의 설문을 통해 확보하였다. 조직의 정보보안 규정, 처벌 등은 명확하게 수준이 정해져 있는 경우가 많은데, 본 연구는 개인이 생각하는 수준을 기반으로 연구를 진행하였다. 향후 연구에서는 정보보안 처벌 등 구축 수준에 따라, 개인의 인식 차이를 확인한다면 정보보안 처벌 등 정책이 가지는 의미를 보다 명확하게 설명할 수 있을 것으로 판단한다. 둘째, 본 연구는 정보보안 행동을 일으키는 개인의 인식을 확인하였으나, 행동의 차이를 발현시키는 개인차 변인을 적용하지 않았다. 특히, 조직에서 개인의 위치나 권력에 따라 정보보안 인식의 차이가 발생할 수 있으며, 특정 문제에 대한 개인의 대처 역량에 따라 동기 및 행동의 차이가 존재할 수 있다. 따라서, 향후 연구에서는 개인차 변인을 적용하여, 개인의 특성에 따른 정보보안 행동 차이가 존재함을 밝힌다면, 내부자의 정보보안 전략 수립을 위한 시사점을 제공할 수 있을 것으로 판단한다.

References

[1] 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

[2] J. Xu, X. Wang, L. Yan, "The Moderating Effect of Abusive Supervision on Information Security Policy Compliance: Evidence from the Hospitality Industry," Computers & Security, Vol. 111, pp. 102455, 2021. DOI: https://doi.org/10.1016/j.cose.2021.102455

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

[4] 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

[5] 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

[6] 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

[7] M. Kajtazi, H. Cavusoglu, I. Benbasat, D. Haftor, "Escalation of Commitment as an Antecedent to Noncompliance with Information Security Policy," Information & Computer Security, Vol. 26 No. 2, pp. 171-193, 2018. DOI: https://doi.org/10.1108/ICS-09-2017-0066

[8] P. Menard, G. Bott, R. E. Crossler, "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-determination Theory. Journal of Management Information Systems, Vol. 34, No. 4, pp. 1203-1230, 2017.

DOI: https://doi.org/10.1080/07421222.2017.1394083

[9] Y. Chen, W. Xia, K. Cousins, "Voluntary and Instrumental Information Security Policy Compliance: An Integrated View of Prosocial Motivation, Self-regulation and Deterrence," Computers & Security, Vol. 113, pp. 102568, 2022.
DOI: https://doi.org/10.1016/j.cose.2021.102568

[10] X. Wang, J. Xu, "Deterrence and Leadership Factors: Which are Important for Information Security Policy Compliance in the Hotel Industry," Tourism Management, Vol. 84, pp. 104282, 2021.
DOI: https://doi.org/10.1016/j.tourman.2021.104282

[11] M. Gagné, E. L. Deci, "Self-Determination Theory and Work Motivation," Journal of Organizational Behavior, Vol. 26, No. 4, pp. 331-362, 2005.
DOI: https://doi.org/10.1002/job.322

[12] R. M. Ryan, E. L. Deci, "Self-determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-being," American Psychologist, Vol. 55, pp. 68-78, 2000.
DOI: https://doi.org/10.1037/0003-066X.55.1.68

[13] S. Valentine, L. Godkin, M. Lucero, "Ethical Context, Organizational Commitment, and Person-organization Fit," Journal of Business Ethics, Vol. 41, No. 4, pp. 349-360, 2002.
DOI: https://doi.org/10.1023/A:1021203017316

[14] The White House, Executive Order on Improving the Nation's Cybersecurity, Available From: https://www.whitehouse.gov. (accessed May 12, 2021)

[15] Gartner, Zero Trust Architecture and Solutions, 2020.

[16] Verizon, Data Breach Investigations Report, 2021.

[17] I. Hwang, "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

[18] Manganelli, L., Thibault-Landry, A., Forest, J., & Carpentier, J. (2018). Self-determination theory can help you generate performance and well-being in the workplace: A review of the literature. Advances in Developing Human Resources, 20(2), 227-240.
DOI: https://doi.org/10.1177/1523422318757210

[19] H. Kang, S. Han, J. Ku, "Study of Adolescents' Academic Personality Types, Learning Behavioral Types and Self-determinative Learning Motivations," Journal of the Korea Academia-Industrial cooperation Society, Vol. 15, No. 8, pp. 4919-4929, 2014.
DOI: http://dx.doi.org/10.5762/KAIS.2014.15.8.4919

[20] Y. Nie, B. Chua, A. Yeung, R. Ryan, W. Chan, "The Importance of Autonomy Support and the Mediating Role of Work Motivation for Well-Being: Testing Self-Determination Theory in a Chinese Work Organisation," International Journal of Psychology, Vol. 50, No. 4, pp. 245-255, 2015.
DOI: https://doi.org/10.1002/ijop.12110

[21] I. Hwang, "Reinforcement of IS Compliance of Employees: A Perspective on Improving Self-determination of Organization Justice and Person-job Fit," Journal of the Korea Academia-Industrial cooperation Society, Vol. 23, No. 6, pp. 360-371, 2022.
DOI: https://doi.org/10.5762/KAIS.2022.23.6.360

[22] C. Fernet, C. Senécal, F. Guay, H. Marsh, M. Dowson, "The Work Tasks Motivation Scale for Teachers," Journal of Career Assessment, Vol. 16, No. 2, pp. 256-279, 2008.
DOI: https://doi.org/10.1177/1069072707305764

[23] Trépanier, S. G., Forest, J., Fernet, C., & Austin, S. (2015). On the psychological and motivational processes linking job characteristics to employee functioning: Insights from self-determination theory. Work & Stress, 29(3), 286-305.
DOI: https://doi.org/10.1080/02678373.2015.1074957

[24] J. Son, "Out of Fear or Desire? Toward a better Understanding of Employees' Motivation to Follow IS Security Policies," Information & Management, Vol. 48, No. 7, pp. 296-302, 2011.
DOI: https://doi.org/10.1016/j.im.2011.07.002

[25] K. Padayachee, "Taxonomy of Compliant Information Security Behavior," Computers & Security, Vol. 31, No. 5, pp. 673-680, 2012.
DOI: https://doi.org/10.1016/j.cose.2012.04.004

[26] E. Park, J. Kim, Y. Park, "The Role of Information Security Learning and Individual Factors in Disclosing Patients' Health Information," Computers & Security, Vol. 65, pp. 64-76, 2017.
DOI: https://doi.org/10.1016/j.cose.2016.10.011

[27] J. D'Arcy, A. Hovav, 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.
DOI: https://doi.org/10.1287/isre.1070.0160

[28] L. Jaeger, A. Eckhardt, "Eyes Wide Open: The Role of Situational Information Security Awareness for Security-Related Behaviour," Information Systems Journal, Vol. 31, No. 3, pp. 429-472, 2021.
DOI: https://doi.org/10.1111/isj.12317

[29] A. Da Veiga, N. Martins, "Defining and Identifying Dominant Information Security Cultures and Subcultures," Computers & Security, Vol. 70, pp. 72-94, 2017.
DOI: https://doi.org/10.1016/j.cose.2017.05.002

[30] S. Mamonov, R. Benbunan-Fich, "The Impact of Information Security Threat Awareness on Privacy-protective Behaviors," Computers in Human Behavior, Vol. 83, pp. 32-44, 2018.
DOI: https://doi.org/10.1016/j.chb.2018.01.028

[31] 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

[32] K. H. Guo, Y. Yuan, "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model," Information & Management, Vol. 49, No. 6, pp. 320-326, 2012.
DOI: https://doi.org/10.1016/j.im.2012.08.001

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

[34] M. C. Andrews, T. Baker, T. G. Hunt, "Values and person-Organization Fit: Does Moral Intensity Strengthen Outcomes?," Leadership & Organization Development Journal, Vol. 32, No. 1, pp. 5-19, 2011.
DOI: https://doi.org/10.1108/01437731111099256

[35] M. Junaedi, F. Wulani, "The Moderating Effect of Person-organization Fit on the Relationship between Job Stress and Deviant Behaviors of Frontline Employees," International Journal of Workplace Health Management, Vol. 14, No. 5, pp. 492-505, 2021.
DOI: https://doi.org/10.1108/IJWHM-06-2020-0103

[36] H. Jung, Y. Namkung, H. Yoon, "The Effects of Employees' Business Ethical Value on Person-organization Fit and Turnover Intent in the Foodservice Industry," International Journal of Hospitality Management, Vol. 29, No. 3, pp. 538-546, 2010.
DOI: https://doi.org/10.1016/j.ijhm.2009.08.005

[37] X. Wang, B. Li, "Technostress among University Teachers in Higher Education: A Study Using Multidimensional Person-environment Misfit Theory," Frontiers in Psychology, Vol. 10, pp. 1791, 2019.
DOI: https://doi.org/10.3389/fpsyg.2019.01791

[38] I. Hwang, "The Influence of Organization Trust and Person Organization Fit on Information Security Compliance Intention Through Role Stress Mitigation," Korean Review of Corporation Management, Vol. 12, No. 3, pp. 131-151, 2021.
DOI: https://doi.org/10.20434/KRICM.2021.08.12.3.131

[39] S. Lim, K. Lee, K. Bae, "Distinguishing Motivational Traits between Person-organization Fit and Person-job Fit: Testing the Moderating Effects of Extrinsic Rewards in Enhancing Public Employee Job Satisfaction," International Journal of Public Administration, Vol. 42, No. 12, pp. 1040-1054.
DOI: https://doi.org/10.1080/01900692.2019.1575665

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

[41] 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

[42] 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

[43] A. F. Hayes, Introduction to Mediation, Moderation, and Conditional Process Analysis: A Regression-based Approach, 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