JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 23, No. 10, pp. 2045-2056, Oct. 2022

Check for updates

조직 내 정보보안 작업 복잡성과 경쟁적 분위기에 따른 정보보안 가치 차이의 영향

황 인 호
국민대학교 교양대학 조교수

The Effect of IS Value Dissimilarity According to IS Task Complexity and Competitive Climate within the Organization

Inho Hwang

Assistant Professor, College of General Education, Kookmin University, Seoul 02707, Korea

[요 약]

조직 차원에서 조직 내부자의 업무 효율성 확대를 위한 정보시스템 활용이 증가하면서, 사람에 의한 정보보안 위협 또한 증가하고 있다. 사람에 의한 정보보안 사고 가능성은 정보 접근 권한이 높아지고 접근 횟수가 증가할수록 높아진다. 본 연구는 내부자의 정보보안 준수 활동은 당사자의 심리적 측면에 있다고 보고, 정보보안 준수 활동을 감소하는 정보보안 미준수 원인(작업 복잡성, 가치 차이)과 조직 업무 환경요인(경쟁적 분위기)을 제시한다. 본 연구는 정보보안 정책을 조직원의 업무에 적용하는 조직에 근무하는 직원들을 대상으로 설문을 하였으며, 확보된 표본을 활용하여 가설 검증을 하였다. 가설 검증 결과, 정보보안 작업 복잡성, 가치 차이, 그리고 정보보안 준수 의도 간의 연계된 부정적 영향 관계를 확인하였으며, 경쟁적 분위기가 정보보안 작업 복잡성과 가치 차이가 준수 의도에 미치는 부정적 영향을 강화하는 것을 확인하였다. 본 연구는 조직원의 관점에서 정보보안 준수 행동을 감소시키는 선행 조건을 제시하여, 역설적으로 내부의 정보보안 수준을 높이기 위한 조직의 정보보안 정책 수립 방안의 수립에 기여 한다.

[Abstract]

As the use of information systems to expand organizational work efficiency increases, the threat of information security(IS) by organizational insiders is also increasing. The possibility of a IS incident by an insider increases as the authority and access to information increases. This study judges that insiders' IS compliance is due to psychological factors and suggests causes of IS non-compliance and organizational work environment factors that reduce IS compliance intention. This study conducted a survey of employees working in organizations that apply IS policies to the work of employees and tested the hypothesis using the obtained sample. As a result of hypothesis testing, we confirmed the mechanism between IS task complexity, IS value dissimilarity, and IS compliance intention, and confirmed that competitive climate had an interactive effect on IS task complexity and value dissimilarity. This study contributes to the establishment of an organization's IS policies and strategies to increase the level of internal IS.

색인어 : 정보보안, 작업 복잡성, 가치 차이, 경쟁적 분위기, 준수 의도

Keyword : Information security, Task complexity, Value dissimilarity, Competitive climate, Compliance intention

http://dx.doi.org/10.9728/dcs.2022.23.10.2045

Received 09 September 2022; **Revised** 05 October 2022
Accepted 05 October 2022

***Corresponding Author; Inho Hwang**

Tel: +82-02-910-5794
E-mail: hwanginho@kookmin.ac.kr

Ⅰ. 서 론

코로나19는 우리 사회를 더욱 빠르게 디지털 기반 활동을 하도록 강제하고 있다. 특히, 코로나19 사태가 조금씩 완화하고 있음에도 불구하고, 기업 등 사회 구성원은 온라인 중심 운영 체계의 효율성을 극대화하기 위하여 노력하고 있다[1]. 예를 들어, 대면 기반 회의를 대처하기 위하여 도입한 Zoom과 같은 온라인 미팅 시스템은 간편성과 효율성이 인정되어 지속해서 활용되고 있으며, 재택근무 기반의 조직 내 인적자원 관리체계가 IT 기업들을 중심으로 자리 잡는 추세이다. 물리적 제약을 뛰어넘는 정보시스템의 활용은 업무 효율성을 극대화하여 성과 창출에 도움을 주지만, 역설적으로 정보시스템에 대한 접근 권한을 보유한 사람의 증가와 보이지 않는 장소에서의 정보 접근성의 증가는 정보를 명료하게 통제해야 하는 집단에게 있어 정보 노출 가능성과 같은 문제를 일으킬 수 있다[2]. 사람에 의한 정보 노출 가능성은 시간과 장소를 불문하고 정보시스템에 접근이 가능한 사람일 경우 발생할 가능성이 존재하는데, 조직 서버에 대한 물리적 접근에서부터 온라인에서의 의도적인 정보 이동 또는 비의도적인 노출 가능성까지 다양하다[3]. 따라서, 기업들은 내부자의 정보시스템 활용성 강화를 통한 지속적 성과 창출과 내부자의 정보시스템 오남용 최소화를 통한 정보보안이라는 목표 달성, 두 마리의 토끼를 한꺼번에 잡아야 하는 어려움이 존재하는 상황이다[4].

하지만, 내부자의 정보보안 사고 억제 및 예방 방법을 제안해온 연구들은 내부의 정보보안 목표 달성이 멀웨어, 바이러스와 같은 외부의 침입에 대한 방어 기술에 대한 투자보다 더욱 어려운 문제일 수 있음을 지적하고 있다. 일찍이 West[2008]는 사람에 의한 정보보안 문제가 심리인 측면에서 접근되는데, 기업이 사람의 정보보안 행동을 관리 및 통제하고자 하더라도 정보보안 관련 행동 정보는 언제나 기업보다 당사자가 더욱 많이 보유하고 있으므로, 정보 노출 가능성은 언제나 존재할 수 있다고 하였다[5]. 즉, 사람에 의한 정보 노출 위협에 대한 억제 또는 예방적 활동은 심리적으로 대상자가 강하게 정보보안을 지켜야 한다는 의식을 보유하도록 함으로써, 자발적인 정보보안 활동 및 행동을 공유할 수 있도록 하는 것이 필요함을 지적했다. 이와 유사한 관점에서, 사람의 정보보안 준수와 관련된 선행연구들은 정보보안 준수 인식을 증가시키기 위한 긍정적 동기 및 조직의 전략적 활동 조건을 제시해왔다[6-8]. 최근에는, 보상보다 처벌의 관점을 주시하고 있는 정보보안의 특성을 고려하여, 강력하고 엄격한 정보보안 정책과 기술의 도입은 정보보안을 본인의 일에 적용해야 하는 조직원에게 부정적 가치 또는 인식을 심어주어, 오히려 심리적으로 정보보안 활동을 회피하도록 하는 조건이 될 수 있음을 제시한 연구들이 나오고 있다[9]. 특히, 정보보안 환경 및 기술의 준수 어려움, 또는 업무의 과부하 등으로 인하여 스트레스를 발현시켜 부정적 행동을 일으킬 수 있음을 지적한 연구가 대표적이다[9-11]. 스트레스 관련 연구들은 조직 내부의 정보보안 목표는 결국 정보보안 정책을 이행해야 하는 사람의 관점에서 접근해야 달성할 수 있음을 지적하고, 조직원에게 정보보안을 요구하는 과정에서 그들의 어려움 등을 함께 해결해나가야 함을 제시한 측면에서 시사점을 가진다. 그러나, 정보보안 관점에서 개인의 부정적 상황 및 인식과 관련된 연구는 최근에야 스트레스 이론 등을 접목하여 제시되어, 아직 정보보안을 업무에 적용하는 과정에서 발생 가능한 부정적 인식 조건과 관련된 연구는 다각적으로 제시되지 않는 상황이다.

본 연구는 조직이 요구하는 보안 요구사항에 대한 수행 주체인 조직원의 관점에서 미준수 원인을 살펴보되, 특히, 정보보안 활동에 대한 개인과 조직의 가치 차이에 주목한다. 조직에서 조직원이 부여받은 역할은 자신의 업무적 성과 달성에 있으며, 목표 달성을 위해 개인은 정보시스템 등을 활용한 정보 교류 활동을 능동적으로 수행한다. 정보보안은 성과 창출을 위한 정보의 교환 활동에 허가와 같은 추가적인 절차를 요구하여 효율성을 감소시키는 조건으로 인식할 수 있으며[5], 기존 업무 외 추가로 수행해야 할 활동이면서 미준수 행동 시 강한 처벌을 일으키는 활동이므로[8], 쉽게 정보보안의 가치를 최소화할 가능성이 발생하며, 가치가 자신과 일치하지 않을 때 요구된 행동을 축소할 가능성이 존재한다[12].

이에, 본 연구는 정보보안 가치 차이를 적용하되, 조직의 정보보안 환경과 업무적 환경이 당사자의 정보보안 가치 차이에 어떠한 영향을 미쳐 정보보안 활동을 감소시키는지를 확인하고자 한다. 세부적으로, 본 연구는 조직의 정보보안 복잡성의 증대가 개인의 정보보안 가치 차이를 발현시켜 준수 의도에 어떠한 영향을 주는지를 확인하며, 업무 환경이 경쟁적 분위기가 형성될 때 가치 차이의 영향을 어떻게 조절하는지를 확인한다. 본 연구의 결과는 조직원의 관점에서 정보보안 준수 감소 요인을 제시하므로, 조직이 내부 정보보안 성과를 달성함에 있어 고려해야 할 내부자의 정보보안 가치 확립 전략 수립에 실질적으로 기여할 것으로 판단한다.

Ⅱ. 선행연구 및 가설설정

2-1 조직 내부의 보안 사고 유형 및 보안 준수 필요성

정보보안 사고는 발생 시 대상 조직 및 정보와 관련된 이해관계자들의 가치를 감소시키는 조건이다[5]. 정보보안 예방은 매우 중요한 관점이며, 조직들은 정보보안 관련 정책, 규정, 기술 등에 대한 투자를 높이는 추세이다[6]. 지금까지 조직들은 외부의 정보 침입의 방어를 위한 기술적 노력을 중점적으로 추진해왔다. 하지만, 전 세계적으로 드러난 정보보안 사고 유형을 기술적 침입과 사람에 의한 노출의 관점에서 살펴보면, 사람(내부자 및 파트너)에 의한 정보보안 사고는 매년 전체 사고의 20-30% 내외에서 발생하는 것으로 판명되

고 있다[13]. 단 한 건의 정보 노출 사고가 기업의 가치를 감소시키는 것을 고려하면, 사람에 의한 정보 노출 가능성을 최대한 억제하기 위한 노력이 필요한 시점이다. 더욱이, 내부의 정보보안 사고 위협은 이해관계자의 조직의 정보시스템 활용이 증가할수록 커질 수 있다. 즉 조직의 정보에 대한 접근이 가능한 사람이 많아질수록 정보보안에 대한 관리 포인트는 많아진다. 실제로, 내부자의 정보보안 사고는 IT, 사무직, 영업직, 엔지니어 등 직무와 관계없이 발생했으며, 최고 경영층에서 말단 직원 등 다양하게 발생한 것으로 나타났다[13].

따라서, 조직이 내부의 정보보안 수준 달성을 위한 전략 수립을 위해서는, 조직원에 대한 정보보안 관리체계를 새롭게 수립할 필요성이 있다. 특히, 조직은 사람들의 자발적인 보안 준수 행동을 유발할 필요성이 있으며, 전략적 접근이 요구된다. 정보보안 준수 의도(Compliance Intention)는 집단의 정보를 외부의 침입에 의한 위협으로부터 보호하고, 정보 노출 등 오남용을 최소화하고자 하는 의지를 지칭한다[7,14]. 즉, 준수 의도가 형성된 사람은 자신이 속한 조직의 정보 자산을 능동적으로 보호하고자 하는 활동을 하고자 한다[1]. 이에 본 연구는 개인의 준수 의도에 부정적 영향을 주는 주요 조건으로 정보보안 가치 차이를 제시하고, 정보보안 환경과 업무 환경에 따라 정보보안 가치 차이의 부정적 영향이 어떻게 변화하는지를 확인하고자 한다.

2-2 정보보안 관련 가치 차이

가치(Value)는 특정 환경에서 대상자가 의사결정을 하도록 돕는 요인으로서[15], 개인에게 본인의 행동에 의미를 부여하도록 돕는 내적 동기이며, 집단에게는 집단이 추구하는 목적을 설명하는 조건이다[4]. 즉, 조직은 조직으로서 나가고자 하는 방향이 존재하며, 조직 이해관계자들이 조직의 추진 방향을 이해하고 따르기를 원하는데, 가치는 이러한 목적을 달성하도록 돕는 조건이다[12].

또한, 상호 교환관계에 있는 이해관계자들은 자신이 보유한 가치와 교환 대상자의 가치를 평가한다. 즉, 당사자들은 가치 일치(Value Congruence)의 수준을 평가하는데, 상호 간에 추구하는 가치의 적합성이 충분히 존재한다고 판단할 때, 상대방을 이해하고 믿음을 형성하여, 상대방과 교류를 하도록 돕는다[16]. 특히, 조직과 조직원의 관점에서 조직 내 구축된 가치 및 가치의 전달은 조직원으로 하여 조직을 신뢰하고, 조직에 대한 매력을 인식하도록 하여 조직과 함께 나아가고자 하는 의도를 가지게 한다[16]. 나아가, 가치는 조직과 관련된 이해관계자(파트너, 고객 등)가 조직을 이해하고 동질성을 가져, 연계된 활동을 지속하도록 돕는 역할을 한다[15].

반대로, 교환 대상자(조직, 사람) 간 가치가 다르거나 갈등을 일으키는 조건으로 인식될 경우, 부족한 가치는 상호 간에 믿음을 상실시키고 반대되는 행동을 추구하도록 돕는다[17]. 조직에서 가치 차이(Value Dissimilarity)는 개인이 가치 측면에서 자신이 조직과 다르다고 인식하는 수준을 의미한다[12]. 조직 환경에서 개인은 업무의 목표와 절차가 왜 수행되어야 하는지에 대한 신념이 존재해야 능동적인 행동을 일으키는데, 조직과 가치 차이가 발생할 경우, 개인은 조직의 요구사항을 수행하는데 주저할 가능성이 있다[18].

정보보안 활동과 관련하여, 조직이 추진하는 정보보안 가치에 대한 이해는 조직원에게 정보보안 활동의 필요성을 느껴, 자발적인 정보보안 활동을 하도록 돕는다. Lian[2021]은 조직의 정보보안 지원 도구의 유용성이 가치를 형성하여 정보보호 의도를 형성시킨다고 하였으며[4], Doherty and Tajuddin[2018]은 사용자 중심의 정보보안 준수 모델을 제시하면서, 조직이 보유한 정보에 대한 가치 인식과 정보보안 활동에 대한 가치 인식이 사용자 행동을 강화한다고 하였다[19]. 즉, 조직의 정보 자산에 대한 중요성 인식과 정보보안 활동을 위해 조직이 추진하는 활동에 대한 가치가 상호 연동될 때, 조직원은 정보를 보호하기 위한 의지를 보유하게 된다. 따라서, 조직은 정보보안 활동에 대한 가치를 구성원이 이해하고 동질감을 가질 수 있도록 지원하는 것이 요구된다.

2-3 정보보안 관련 작업 복잡성

조직에서 조직원은 주어진 특정 환경 또는 이해관계자의 요구사항에 대하여 자신이 어떻게 해결할 수 있을지 판단한다. 당사자는 자신이 확보한 정보, 경험 등을 기반으로 대처하지만, 본인의 정보 부족, 조직의 과도한 요구사항 등이 발생할 때 예상되는 결과를 정확하게 판단할 수 없어 부정적 감정을 발현할 수 있다[20,21]. 대표적인 행동의 과정, 결과 예측을 어렵게 하는 조건이 복잡성이다. 복잡성(Complexity)은 조직 내 업무, 특정 행동 등 대상에게 요구되는 행위의 양과 정보의 출처, 대상과 관련된 복잡한 지식의 묶음으로 설명되는데[22], 요구되는 행동의 양과 행동을 위해 확보해야 할 정보가 많아 심리적으로 복잡하다고 느끼는 수준을 의미한다[23]. 즉, 복잡성 감정은 조직에서 개인에게 부여된 과업의 양과 과업을 해결하기 위해 요구되는 많은 정보로 인하여 추가적인 시간과 노력을 추가해야 한다고 느껴, 심리적으로 부담감을 느끼는 상황을 의미한다.

조직에서 복잡성의 대상은 기술, 업무, 프로젝트 등 다양하게 존재한다. Tarafdar et al.[2008]은 기술 스트레스 요인 중의 하나로 기술 복잡성을 제시하였으며, 지속적인 기술 도입 등으로 복잡한 기술을 배우거나 다루는 능력이 부족한 상황이라고 하였다[24]. Zhang et al.[2022]는 프로젝트와 같이 특별한 업무에 대한 복잡성을 제시하였으며, 대상 과제의 양과 필요 정보의 양의 과다로 인하여 느끼는 복잡성으로 정의하였다[25]. 본 연구는 작업에 대하여 개인이 느끼는 심리적 부담감을 정보보안 분야에 적용한다.

정보보안 작업 복잡성(IS Task Complexity)에 대하여, 본 연구는 정보보안 관련 조직의 요구사항을 개인의 업무에 추가로 반영하는 상황에서, 정보보안 활동 요구사항의 양과 확보해야 할 정보의 수준이 다양하여, 업무에 적용하기 힘들다

고 느끼는 수준으로 정의하였다. 즉, 엄격한 정보보안 규칙과 행동 규정 등으로 인하여, 기존 업무를 크게 변화시켜야 하거나, 추가적인 정보 확보에 어려움을 겪어, 정보보안을 반영한 업무수행에 불편함을 겪을 때, 복잡성이 높다고 느낄 수 있다.

특정 목적 달성에 필요한 활동이 복잡하다고 느낄 경우, 당사자는 활동을 회피하거나, 숨기려는 경향을 보인다. Zhang et al.[2022]은 팀 프로젝트 복잡성이 높아질수록 팀원들은 각각의 지식을 은폐하려 하고 프로젝트 성과를 감소시키는 원인이 된다고 하였다[25]. Tarafar et al.[2008]은 기술 불확실성이 포함된 기술 스트레스 원인은 업무 스트레스를 높여, 조직 내 개인의 업무 생산성을 감소시킨다고 하였다[24]. 정보보안과 관련하여 D'Arcy et al.[2014]는 과부하, 복잡성, 그리고 불확실성으로 구성된 정보보안 관련 스트레스 원인은 감정적 대처를 통해, 정보보안 회피 의도를 강화한다고 하였다[10]. 즉, 업무에 정보보안 작업을 부여 시, 개인이 복잡하다고 느낄 경우, 개인은 정보보안 준수 행동을 줄이고자 한다. 이에, 연구는 복잡성과 준수 의도 간의 관계를 확인하기 위한 가설을 수립하였다.

H1: 정보보안 관련 작업 복잡성은 정보보안 준수 의도를 낮춘다.

또한, 조직 내 특정 활동에 대한 복잡성은 대상에 대한 가치 차이를 강하게 인식하도록 하여, 대상과 관련된 조직의 요구를 따르지 않으려는 경향을 보이도록 한다.

첫째, 개인에게 스트레스를 발생시킬 수 있는 조직 내 조건은 대상의 가치를 감소시킨다. Lv et al.[2021]은 갈등과 불신, 그리고 커뮤니케이션이 발생하지 않는 조직 조건이 강화될수록, 대인 간의 혜택 중심의 가치 인식을 감소시켜 부정적 업무 행동을 높이는 것을 확인하였다[26]. Semerci[2018]는 조직 내 업무 갈등과 역할 갈등으로 인하여 형성된 경쟁에 대한 인식은 개인의 가치와 차이를 일으켜 지식 은폐를 강화한다고 하였다[27]. Taradfar et al.[2008]은 기술 관련 갈등, 복잡성 등을 통합하여 기술 스트레스 조건으로 제시하였으며, 스트레스는 개인에게 부정적 영향을 주는 요인임을 확인하였다. 즉, 갈등, 복잡성과 같은 부정적 조건은 특정 대상에 대한 가치 차이를 발현시킬 수 있다.

둘째, 가치 적합성을 감소시키는 상황 및 그로 인한 가치 차이에 대한 인식은 조직의 가치 향상과 관련된 개인의 행동을 감소시킨다. Cooper[2013]는 팀의 가치 차이가 팀에 대한 동일시를 감소시키고 팀 학습 활동을 감소시키는 조건임을 제시하였으며[12], Hobman et al.[2003]은 조직에 대한 가치 차이 인식이 본인의 업무 및 관계 갈등을 일으키는 원인이라고 하였다. 정보보안과 관련하여[17], Hedström et al.[2011]은 정보보안에 대한 가치 차이 발생할 경우, 당사자의 정보보안 활동에 부정적 행동을 일으키는 조건임을 제시하였다[28]. 즉, 선행연구는 복잡성 등 스트레스 발현 환경이 대상에 대한 가치 차이를 발생시켜 부정적 행동을 일으킨다. 본 연구는 정보보안 관련 조직 복잡성이 조직원의 정보보안 가치 차이를 일으켜, 준수 의도에 부정적 영향을 미칠 것으로 판단한다. 이에, 연구는 복잡성, 가치 차이, 그리고 준수 의도 간의 매커니즘을 확인하기 위한 가설을 수립하였다.

H2: 정보보안 관련 작업 복잡성은 정보보안 가치 차이를 높여, 정보보안 준수 의도를 낮춘다.

H2a : 정보보안 관련 작업 복잡성은 조직원의 정보보안 가치 차이를 높인다.

H2b : 정보보안 관련 가치 차이는 정보보안 준수 의도를 낮춘다.

2-4 조직의 경쟁적 분위기

조직에서 개인은 본인을 둘러싼 환경에 영향을 받으며, 환경과의 균형성을 유지함으로써 안정감을 느끼고자 한다[29]. 특히, 환경은 조직이 도입한 기술, 정책과 같은 업무에 적용해야 하는 업무적 환경 조건에서부터, 가치, 분위기와 같이 눈에 보이지 않으나, 오래전부터 구성원들이 수행해왔던 행동 방식 등과 같은 환경적 조건에 이르기까지 다양하게 존재한다[30].

경쟁적 분위기(Competitive Climate)는 집단 구성원들이 보상을 추구하기 위해, 주변 동료들과 비교된 성과를 적극적으로 활용하는 수준을 인식하는 것을 의미한다[29]. 경쟁심은 사람이 가지는 본질적 특성이기에, 개인은 특정 행동에 대한 물질적 보상 또는 목표 달성을 통한 만족감 등을 확보하고자 한다. 이에, 조직에서 개인은 자신의 목표 달성을 위해 경쟁을 통해 인센티브, 권력 등을 확보하고자 하므로, 경쟁적 분위기는 조직 전체의 성과에 긍정적 영향을 주는 조건이다[30]. 따라서, 현대 조직은 보상의 개념을 적극적으로 채용하고 있으며, 개인에게 부여된 목표 달성 수준에 따라 유무형의 보상을 위한 정책을 마련하고 있다. 하지만, 과도한 수준의 경쟁적 분위기는 조직 전체의 성과 달성을 위한 활동보다는 조직원 개인만의 관점에서 성과 창출을 위한 활동을 증가시키는 역할을 한다[31]. 즉, 경쟁적 분위기가 주변에 형성되고 동료 간의 상대적 비교가 지속할 경우, 개인은 조직 환경에 대처하기 위하여 본인 중심의 사고와 행동 방식을 결정하고 활동을 한다. 조직이 지속해서 성장하기 위해서는 개인 중심의 사고 이외에 집단적 사고가 필요한데 경쟁적 분위기는 이를 감소시키는 역할을 한다.

정보보안은 준수 행동에 대한 보상의 개념보다 미준수 행동에 대한 처벌의 개념을 적극적으로 반영할 수밖에 없다. 한 번의 실수로 인하여 노출된 정보는 기존에 준수를 통해서 얻은 성과보다 큰 문제를 일으킬 수 있어 보안 사고에 대한 경각심을 일깨우기 위한 강력한 제재가 뒤따르기 때문이다[8]. 경쟁적 분위기는 조직원에게 성과 창출을 위한 지식교류 행동과 정보보안을 위한 행동에 대한 딜레마를 인식하도록 할 가능성이 있다[5]. 즉, 성과 달성에 대한 경쟁이 심화할 경우, 개인은 성과 달성을 위해 행동 결과가 눈에 띄지 않는 정보보안 활동을 최소화할 가능성이 존재한다[32]. 정보보안 문화, 분위기 등 환경과 관련된 선행연구는 긍정적 환경이 구축되

어 있을 때 준수 행동을 강화함을 제시해왔다. Xue et al.[2021]은 윤리적 리더십에 의해 형성된 조직 내 정보보안 준수 분위기는 조직원의 정보보안 정책 회피 의도를 약화하는 것을 확인하였으며[8], Lin et al.[2022]은 사람 중심 문화를 구축한 조직은 능동적인 보안 행동을 기대할 수 있음을 확인하였다[2]. 즉, 조직 환경은 개인의 특정 활동 변화를 기대할 수 있다. 본 연구는 선행연구를 기반으로 경쟁적 분위기와 정보보안 준수 의도 간에 부정적 영향 관계가 존재할 것으로 판단하며, 가설을 수립하였다.

H3: 조직의 경쟁적 분위기는 조직원의 정보보안 준수의도를 낮춘다.

또한, 조직에 형성된 경쟁적 분위기는 관련된 업무, 요구사항과 관련된 활동에 부담감을 일으켜, 정보보안 관련 미준수 원인의 부정적 영향을 조절할 수 있다.

첫째, 분위기와 같은 조직의 환경 조건은 스트레스 조건인 복잡성과 행동 간의 관계를 조절한다. Peng et al.[2021]은 조직의 경쟁 환경이 심화할수록, 조직 내 대인 간 관계 갈등이 지식 은폐에 미치는 영향을 높일 수 있음을 지적하였다. 정보보안과 관련하여[31], Nasirpouri Shadbad and Biros[2021]은 정보보안 관련 갈등, 과부하, 모호성 조건으로 구성된 스트레스가 정보보안 정책 행동에 미치는 부정적 영향에 대해, 조직이 구축한 지원 환경을 통해 감소시킬 수 있다고 하였으며[9], Trang and Nastjuk[2021]은 정보보안 활동 준수에 소요 시간의 증가로 인한 스트레스가 미준수 행동에 미치는 영향을 조직 차원에서 설계한 정보보안 정책 준수를 위한 구조 체계(처벌, 보상)가 조절 효과를 가진다고 하였다[32]. 즉, 조직의 경쟁적 환경은 불안감 등을 일으킬 수 있는 특정 조건에 영향을 주어 행동의 변화를 일으킬 수 있다.

둘째, 경쟁적 분위기는 가치와 같은 내적 동기와 행동 간의 관계를 조절한다. Han et al.[2020]은 경쟁적 분위기가 개인의 지식 은폐 행동에 미치는 부정적 영향을 개인의 낙관주의가 감소시킨다고 하였으며[29], Vedadi et al.[2021]은 조직의 요구사항에 대한 정보 불확실성 환경에 의해 형성된 불확실성 인식은 정보 관리에 대한 자기효능감이 행동에 미치는 영향을 감소시킨다고 하였다[33]. Semerci[2019]는 지식 공유 활동에 있어 개인이 느끼는 지식 가치에 대한 인식은 갈등 상황이 지식 은폐에 미치는 영향을 조절하기 때문에, 갈등과 관련된 조직 환경의 변화가 요구됨을 지적하였다[27]. 즉, 분위기는 대상 목표에 대한 가치의 영향을 변화시킬 수 있다.

선행연구를 기반으로 본 연구는 경쟁적 분위기가 정보보안 관련 작업 복잡성과 가치 차이가 준수 의도에 미치는 부정적 영향을 각각 조절할 것으로 판단하고, 연구가설을 수립하였다.

H4a: 경쟁적 분위기는 정보보안 관련 작업 복잡성이 정보보안 준수 의도에 미치는 영향을 조절한다.

H4b: 경쟁적 분위기는 정보보안 관련 가치 차이가 정보보안 준수 의도에 미치는 영향을 조절한다.

Ⅲ. 연구 모델 및 데이터 수집

3-1 연구 모델

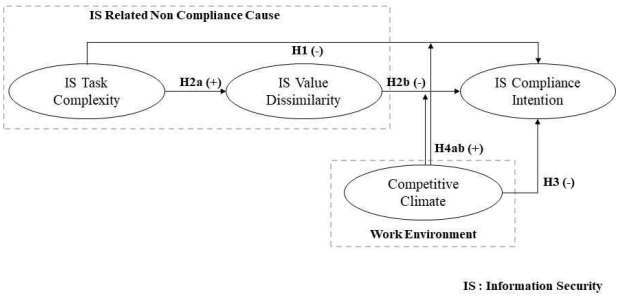

그림 1. 연구 모델
Fig. 1. Research Model

본 연구는 조직 내부의 정보보안 준수에 부정적 영향을 주는 정보보안 관련 요인과 조직 업무 환경요인을 확인한다. 선행연구를 통해, 정보보안 관련 작업 복잡성, 가치 차이, 그리고 준수 의도 간의 매커니즘과 경쟁적 분위기의 영향 관계를 제시하였으며, 연구 모델로서 제시하였다<그림 1>.

3-2 설계 및 데이터 수집

표 1. 설문 문항
Table 1. Questionnaire Items

Construct	Items	Reference
ITC	I have found that applying IS to work is a complex task.	[22]
	Applying IS to work requires additional problem-solving capabilities.	
	Applying IS to work requires additional mental action.	
ISVD	I think my values for IS are different from other peers.	[12] [18]
	I think that the principle of complying with IS is different from other peers.	
	I often disagree with other peers about IS goals.	
ISCI	I intend to comply with the IS policy.	[7]
	I intend to recommend other peers to comply with the IS policy.	
	I intend to support other peers to comply with the IS policy.	
CC	My organization compares my performance with my peers.	[29]
	The performance I receive in my organization is reflected in comparison with other peers.	
	All members of the organization are interested in achieving work goals.	

ITC(IS Task Complexity), ISVD(IS Value Dissimilarity), ISCI(IS Compliance Intention), CC(Competitive Climate)

연구는 설문지 기법으로 확보한 요인별 설문 결과를 기반으로 가설을 검증하고자 한다. 또한, 연구가설은 주 효과에 대하여 AMOS 22.0 툴을 적용한 구조방정식 모형으로 검증하고, 조절 효과에 대하여 Process 3.1을 적용하여 검증한다.

이를 위해, 연구는 연구 모델에 제시한 요인과 관련된 선행연구로부터 다 항목 기반의 설문 문항을 확보하고, 정보보안 특성에 맞추어 재정리하였다. 또한, 도출된 설문 문항이 정보보안 관련자들에 적정한 설문인지를 확인하기 위하여, 경영학과 대학원에 다니는 직장인 10명을 대상으로 설문의 내용 타당성을 확인하였으며, 최종 수정 후 설문을 수행하였다. 요인별 설문 문항은 표 1과 같으며, 7점으로 구분된 등간 척도(1점: 매우 그렇지 않다. 4점: 보통이다. 7점: 매우 그렇다)를 적용하여 설문을 수행하였다.

설문 대상은 정보보안 관련 정책을 구축하고, 구성원의 업무에 정보보안 규정을 적용하여 행동하도록 하는 조직의 근로자로 선정하였다. 선정된 대상을 정확하게 확보하기 위하여, 본 연구는 직장인 표본을 다수 보유하고 있는 M 리서치 기업을 통해 온라인 설문을 수행하였다. 특히, 연구는 온라인 설문 설계 시, 설문 대상에 적정한 표본을 확보하기 위한 작업을 하였다. 첫째, 응답자의 직업을 확인한 후, 직장인만 다음 설문에 참여하도록 하였으며, 정보보안 정책을 업무에 반영하고 있는지를 추가 확인한 후, 해당자만 본 설문에 참여하도록 하였다. 또한, 본 설문 시작 전 연구의 목적 통계적 활용에 대하여 다시 설명하였으며, 활용 방법에 대하여 허가한 사람만 설문을 수행할 수 있도록 하였다.

표 2. 표본 특성
Table 2. Characteristics of Samples

Demographic Categories		Frequency	%
Gender	Male	199	50.3
	Female	197	49.7
Age	Under 30	90	22.7
	31 – 40	94	23.7
	41 – 50	106	26.8
	Over 50	106	26.8
Industry	Manufacture	114	28.8
	Service	282	71.2
Firm Size	Under 10	23	5.8
	11~50	102	25.8
	51~300	126	31.8
	Over 300	145	36.6
Job Position	Staff	162	40.9
	Assistant Manager	90	22.7
	Manager	64	16.2
	Over Manager	80	20.0
Total		396	100.0

설문을 통해 확보한 유효 표본은 396건으로서, 표본의 특성은 표 2와 같다. 연구는 특히 설문 확보 시, 성별, 연령, 업종, 기업 규모를 다르게 확보했다. 성별과 연령은 비슷한 비율로 확보하였으며, 업종은 제조업과 서비스업이 3:7 수준으로 맞추었다. 그리고 기업 규모의 경우, 10인 미만 기업은 최대한 적게 받고자 하였는데, 정보보안 정책, 기술을 적용하고 있는 국내 기업의 경우 규모가 클수록 많아지는 특성을 고려하였다. 즉, 표본의 특성은 국내 산업 특성을 대체로 반영하였다고 판단된다.

Ⅳ. 가설 검증

4-1 신뢰성 및 타당성

본 연구는 설문을 통해 요인별 응답자의 인식을 확보하되, 각 요인은 다 항목 기반의 문항을 적용하였다. 따라서, 연구는 각 문항이 요인을 정확하게 구성하고 있는지 신뢰성과 타당성을 확인하였다.

첫째, 적용 요인에 대한 신뢰성 분석은 요인의 일관성을 측정하는 것으로서, 본 연구는 SPSS 21.0 툴을 활용하여 요인별 크론바흐 알파를 측정하여 신뢰성을 확인하였다. 크론바흐 알파는 요인별 0.7 이상의 값을 가질 때 신뢰성이 있다고 판단한다[34]. 연구 모델에 적용된 총 4개의 요인에 대한 크론바흐 알파 값은 표 3에 제시하였으며, 모든 요인에 대한 요구사항을 충족했다.

표 3. 신뢰성 및 확인적 요인분석 결과
Table 3. Reliability and Confirmatory Factor Analysis

Constructs		Estimate	SRW Estimate	SE	CR	Cronbach's Alpha
ITC	ITC3	1.000	0.857			0.868
	ITC2	1.005	0.883	0.049	20.585**	
	ITC1	0.919	0.805	0.049	18.664**	
ISVD	ISVD3	1.000	0.825			0.896
	ISVD2	1.037	0.897	0.053	19.490**	
	ISVD1	0.925	0.774	0.055	16.931**	
ISCI	ISCI3	1.000	0.854			0.901
	ISCI2	1.015	0.856	0.049	20.718**	
	ISCI1	1.001	0.876	0.047	21.290**	
CC	CC3	1.000	0.840			0.884
	CC2	1.070	0.903	0.048	22.505**	
	CC1	1.026	0.884	0.047	21.906**	

ITC(IS Task Complexity), ISVD(IS Value Dissimilarity), ISCI(IS Compliance Intention), CC(Competitive Climate)
SRW(Standardized Regression Weights), SE(Standard Error), CR(Critical Ratio)
**: $p < 0.01$

표 4. 집중 타당성 및 판별 타당성 결과
Table 4. Convergent Validity and Discriminant Validity

Constructs	CR	AVE	1	2	3	4
ITC	0.837	0.632	**0.795[a]**			
ISVD	0.853	0.658	.453**	**0.811[a]**		
ISCI	0.885	0.719	-.546**	-.581**	**0.848[a]**	
CC	0.871	0.692	.394**	.394**	-.464**	**0.832[a]**

Note: a = square root of the AVE, **: $p < 0.01$
ISC(IS Task Complexity), ISVD(IS Value Dissimilarity), ISCI(IS Compliance Intention), CC(Competitive Climate)
CR(Construct Reliability), AVE(Average Variance Extracted)

둘째, 적용 요인에 대한 타당성 분석은 요인의 구성항목의 일관성을 확인하고, 요인 간에 차별성을 지니는지를 확인하는 것으로서, 본 연구는 AMOS 22.0 툴을 활용하여 확인적 요인분석 모형을 구조화하고, 집중 타당성(일관성 확인)과 판별 타당성(차별성 확인)을 확인함으로써 타당성을 측정하였다. 우선 확인적 요인분석은 구조모형을 적용하였으므로, 모형의 적합도를 확인하였다. 해당 모형의 적합도는 $\chi 2/df = 1.465$, RMSEA = 0.034, RMR = 0.041, TLI = 0.990, CFI = 0.993, GFI = 0.971, 그리고 AGFI = 0.953로 나타났다. 모든 적합도 요구 수치가 요구사항을 충족하였다<표 3>.

집중 타당성은 개념 신뢰도(CR)와 평균분산추출(AVE) 값을 구하는데, 선행연구는 개념 신뢰도 0.7 이상의 값을 요구하고 있으며, 평균분산추출 0.5 이상의 값을 요구한다[35].

연구 모델에 적용된 요인들의 집중 타당성을 확인한 결과는 표 4와 같다. 모든 요인이 개념 신뢰도와 평균분산추출에 대한 요구사항을 충족하였다. 더불어, 본 연구는 판별 타당성을 확인하였다. 판별 타당성은 요인 간의 차별성을 확인하므로, 상관계수와 평균분산추출을 상호 비교하여 확인한다. 즉, 평균분산추출의 제곱근 중 가장 작은 값이 요인들의 상관계수보다 클 때, 판별 타당성이 있다고 판단한다[35]. 결과는 표 4와 같으며, 판별 타당성에 대한 요구사항을 충족하였다.

마지막으로, 본 연구는 공통방법편의 문제를 확인하였다. 연구는 설문지 기법으로 설문 대상자의 응답 당시의 정보보안에 대한 독립 변수와 종속 변수 등을 측정하였으므로, 응답의 편향 문제가 있을 수 있다. 공통방법편의 문제 확인은 여러 기법이 있으나, 본 연구는 일반적으로 활용되는 단일방법요인 기법을 적용하였다. 해당 기법은 확인적 요인분석 구조모형에 단일 요인을 추가하되, 단일 요인을 측정 항목에 연결한 구조모형을 구하고, 두 모형 간의 측정치의 변화량으로 확인하는 기법이다[36]. 확인적 요인분석 모형과 단일 요인을 추가한 모형의 적합도 모두 요구사항을 충족하였으며, 두 모델 간의 측정치의 변화량이 0.3 이하로 나타났다. 즉, 공통방법편의 문제는 높게 나타나지 않아, 가설을 검증하였다.

4-2 주 효과 분석

주 효과 분석은 정보보안 작업 복잡성, 정보보안 가치 차이, 그리고 정보보안 준수 의도 간의 매커니즘을 확인하는 것으로서, AMOS 22.0 툴을 활용하여 경로 검증을 수행하였다.

주 효과 분석 또한 구조모델을 적용하였으므로, 적용 모형의 적합도를 확인하였다. 적합도 확인은 타당성 분석과 동일한 수치 및 기준을 적용하였으며, $\chi 2/df = 1.893$, RMSEA = 0.048, RMR = 0.083, TLI = 0.982, CFI = 0.986, GFI = 0.961, AGFI = 0.938로 나타났다. 비록, RMR은 요구사항인 0.05보다 약간 높으나, 그 외 수치들이 요구사항을 충족하였다.

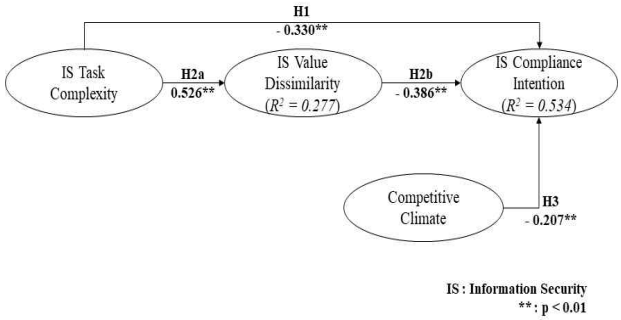

그림 2. 주 효과 분석 결과
Fig. 2. Results of the Main Effect Tests

표 5. 주 효과 분석 결과
Table 5. Results of Main Effect Tests

	Path	Coefficient	t-value	Result
H1	ITC → ISCI	-0.330	-5.672**	Supported
H2a	ITC → ISVD	0.526	9.526**	Supported
H2b	ISVD → ISCI	-0.386	-7.325**	Supported
H3	CC → ISCI	-0.207	-4.285**	Supported

ISC(IS Task Complexity), ISVD(IS Value Dissimilarity), ISCI(IS Compliance Intention), CC(Competitive Climate)
**: $p < 0.01$

가설 1은 정보보안 작업 복잡성이 개인의 정보보안 준수 의도를 낮춘다는 것으로서, 경로계수(β)를 확인한 결과 유의수준 1%에서 통계적으로 영향 관계가 수립되는 것으로 나타났다(H1: $\beta = -0.330$, $p < 0.01$). 결과는 복잡한 정보보안을 적용할 때 느끼는 스트레스가 조직 몰입을 통해 준수 의도에 부정적 영향을 준다는 Hwang and Cha[2018] 연구와 유사한 것이다. 즉, 엄격하고 수준 높은 정보보안은 외부의 침입은 억제할 수 있으나, 내부자에게 부정적 감정을 일으킬 수 있으며, 조직이 요구하는 정보보안 활동에 대한 부정적 의도를 발현시킬 수 있음을 의미한다. 가설 2는 정보보안 작업 복잡성이 정보보안에 대한 가치 차이를 통해(H2a), 정보보안 준수

의도를 낮춘다(H2b)는 것으로서, 경로계수(β)를 확인한 결과 유의수준 1%에서 통계적으로 영향 관계가 수립되는 것으로 나타났다(H2a: β = 0.526, p < 0.01, H2b: β = −0.386, p < 0.01). 결과는 조직 내 갈등 및 불신의 상황이 조직원 간의 연계된 가치를 감소시켜 부정적 행동을 유발한다는 Lv et al.[2021] 연구와 유사한 것이다. 즉, 개인에게 복잡하거나 갈등을 발생시키는 조건은 관련된 행동에 대한 필요성 및 가치 차이를 발생시킬 수 있으며, 이렇게 발현된 가치 차이는 조직보다는 개인 중심의 행동을 추진하도록 도울 수 있음을 의미한다. 즉, 조직은 조직원을 고려한 정보보안 정책을 마련하고, 업무에 효과적으로 적용할 수 있는 지원 체계를 구축함으로써, 조직원들이 정보보안의 필요성과 가치를 인식할 수 있도록 지원하는 것이 요구된다.

가설 3은 조직 환경 요소인 경쟁적 분위기가 개인의 정보보안 준수 의도를 낮춘다는 것으로서, 경로계수(β)를 확인한 결과 유의수준 1%에서 통계적으로 영향 관계가 수립되는 것으로 나타났다(H3: β = −0.207, p < 0.01). 결과는 정보보안 준수 분위기가 정보보안 부정적 행동을 약화한다는 Xue et al.[2021] 연구와 역설적으로 유사성을 가진다. 즉, 긍정적 분위기와 같은 조직의 환경은 동질성을 중심으로 개인의 행동을 유발하는데, 경쟁적 분위기는 개인 중심의 사고를 유발하여, 정보보안 활동보다 본인 성과 중심의 행동을 유발할 수 있음을 의미한다. 따라서, 조직은 경쟁심을 유발하되, 팀 또는 조직 중심의 활동 또한 보상으로서 역할을 할 수 있도록 전략을 수립하는 것이 요구된다.

또한, 선행 요인의 결정력인 결정계수(R^2)를 확인하였다. 정보보안 작업 복잡성은 정보보안 가치 차이에 27.7%의 영향을 주었으며, 정보보안 작업 복잡성과 정보보안 가치 차이는 정보보안 준수 의도에 53.4%의 영향을 주었다.

4-3 조절 효과 분석

가설 4는 경쟁적 분위기가 정보보안 관련 미준수 원인(작업 복잡성, 가치 차이)가 정보보안 준수 의도에 미치는 부정적 영향을 조절하여, 부정적 영향을 강화한다는 것으로서, 본 연구는 Hayes[2017]의 Process 3.1을 적용하였다. 세부적으로, Process 3.1의 모델 1을 적용하되 부트스트래핑 5,000과 신뢰수준 95%를 적용하였다. 경쟁적 분위기의 조절 효과에 대한 분석 결과는 표 6과 같다.

가설 4a는 작업 복잡성과 경쟁적 분위기가 상호작용 효과를 가져 준수 의도에 영향을 준다는 것으로, 유의수준 1%에서 통계적으로 영향 관계가 수립되는 것으로 나타났으며, 가설 4b는 가치 차이와 경쟁적 분위기가 상호작용 효과를 가져 준수 의도에 영향을 준다는 것으로, 유의수준 1%에서 통계적으로 영향 관계가 수립되는 것으로 나타났다. 이에, 본 연구는 경쟁적 분위기의 조절 효과가 어떠한 방식으로 발현되는지 확인하기 위하여 Process 3.1의 단순 기울기 그래프를 제시하였다.

표 6. 경쟁적 분위기의 조절 효과 결과
Table 6. Results of Moderating Effect of CC

Path		Coefficient	t-value	Result
H4a	Constant	5.402	123.706**	Supported
	ITC	−0.409	−9.032**	
	CC	−0.306	−6.540**	
	Interaction	−0.105	−2.884**	
	F = 81.6508, R^2 = 0.3846			
H4b	Constant	5.397	127.129**	Supported
	ISVD	−0.399	−9.441**	
	CC	−0.285	−6.230**	
	Interaction	−0.086	−2.745**	
	F = 0.92.2583, R^2 = 0.4139			

ISC(IS Task Complexity), ISVD(IS Value Dissimilarity), ISCI(IS Compliance Intention), CC(Competitive Climate)
**: p < 0.01,

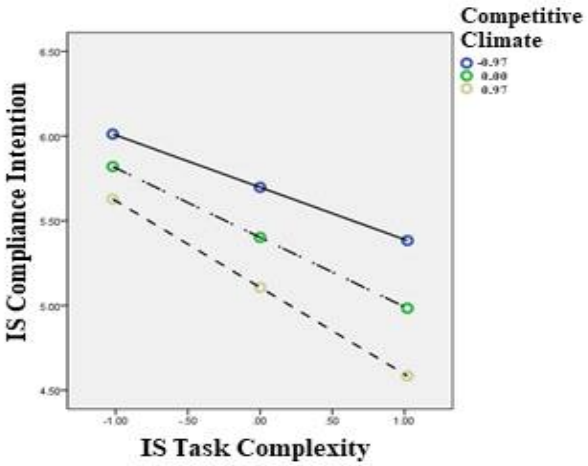

그림 3. 경쟁적 분위기의 조절 효과 결과(H4a)
Fig. 3. Results of Moderating Effect of CC(H4a)

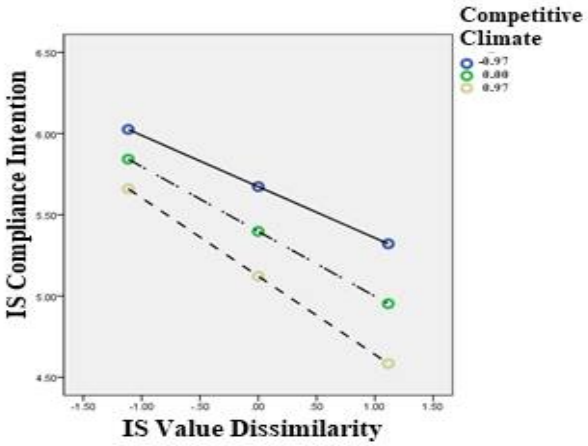

그림 4. 경쟁적 분위기의 조절 효과 결과(H4b)
Fig. 4. RResults of Moderating Effect of CC(H4b)

경쟁적 분위기는 작업 복잡성과 연계하여, 경쟁적 분위기가 높아질수록 정보보안 준수 의도를 감소시키는 것으로 나타났으며<그림 3>, 가치 차이와도 동일한 결과를 보여주는 것으로 나타났다<그림 4>. 즉, 정보보안을 업무에 반영하는 과정에서의 복잡성과 정보보안에 대한 가치 차이를 인식하는 과정에서 조직 내 업무적 환경이 경쟁성을 강화할 때, 개인은 정보보안 준수 행동보다, 본인 중심적 행동을 보일 수 있음을 시사한다. 따라서, 조직은 정보보안 복잡성을 감소시키는 노력과 동시에 경쟁적 분위기에 대한 조직원의 인식을 감소시키기 위한 노력을 함께 하는 것이 요구된다.

V. 결 론

5-1 연구의 요약

조직 내 비대면 기반 정보시스템의 활용이 지속해서 증가하면서, 내부자에 의한 정보 노출 가능성의 우려가 커지고 있다. 본 연구는 조직 내부자에 대한 정보보안 성과 달성은 심리적 접근 및 행동 개선에 있다고 보고, 조직원의 정보보안 준수 의도를 감소시키는 정보보안 미준수 원인과 조직 업무 환경요인을 제시하고자 하였다. 세부적으로, 연구는 정보보안 작업 복잡성, 정보보안 가치 차이, 그리고 경쟁적 분위기 환경이 정보보안 준수에 미치는 부정적 영향의 매커니즘을 확인하고자 하였으며, 조직의 경쟁적 분위기가 정보보안 준수 의도 감소 요인(작업 복잡성, 가치 차이)의 영향을 높이는 효과를 가지는 것을 확인하고자 하였다. 연구는 정보보안 정책을 조직 내 업무에 적용하여, 정보보안 활동을 요구하는 조직의 근로자들에게 설문을 수행했으며, 396개의 유효 표본을 활용하여, 주 효과 분석과 조절 효과 분석을 수행하였다.

주 효과 분석은 정보보안 작업 복잡성, 정보보안 가치 차이, 그리고 정보보안 준수 의도 간의 연계 매커니즘을 확인하는 것으로, 분석 결과 작업 복잡성이 개인의 정보보안에 대한 가치 차이를 높여, 준수 의도를 낮추며, 경쟁적 분위기가 준수 의도에 부정적 영향을 주는 것을 확인하였다. 조절 효과 분석은 조직의 경쟁적 분위기가 작업 복잡성과 가치 차이가 미치는 부정적 영향을 강화하는 것으로, 분석 결과 경쟁적 분위기는 작업 복잡성, 가치 차이와 각각 상호작용 효과가 있음을 확인하였으며, 작업 복잡성과 가치 차이의 부정적 효과를 더욱 강화하는 것으로 나타났다.

5-2 연구의 시사점 및 향후 연구

본 연구는 정보보안 미준수 조건과 업무 환경 조건이 개인의 정보보안 활동에 미치는 영향을 확인하였으며, 학술적 측면에서 다음과 같은 의미를 지닌다. 첫째, 본 연구는 정보보안 미준수 원인으로 작업 복잡성을 적용하였다. 복잡성 개념은 조직 및 사회학에서 중점적으로 다루던 요인으로서, 역할의 양과 필요 정보에 대한 과다 등으로 인하여 역할 수행에 어려움을 겪을 수 있음을 설명한다. 본 연구는 정보보안 활동이 가지는 특성과 복잡성을 연계하였는데, 정보보안은 기존 개인이 수행하던 업무에 추가로 수행해야 할 처벌적 활동 개념이므로, 당사자는 관련 활동 수행을 위해 추가적 정보를 확보해야 하며, 업무 프로세스를 개선해야 하는 어려움을 가질 수 있다. 복잡성은 해당 상황을 잘 설명할 수 있는 용어이며, 본 연구는 정보보안 작업 복잡성이 정보보안 준수 의도를 낮추는 요인임을 확인하였다. 따라서, 학술적으로, 정보보안에 대한 개인의 부정적 감정을 유발하는 요인인 복잡성을 제시한 측면에서 의미를 지닌다.

둘째, 본 연구는 정보보안을 업무에 반영하는 조직원의 관점에서 정보와 보안 준수 활동이 가지는 가치에 의해 행동 변화가 일어날 수 있음을 고려하고, 정보보안 가치 차이의 부정적 영향을 확인하였다. 정보보안 행동 관련 연구는 정보보안 동일시, 몰입과 같은 조직 관점에서 긍정적 행동을 강화하는 내적 동기 요인을 지속해서 연구해왔다면[6], 본 연구는 정보보안 요구로 인해 업무적 복잡성이 강화될 때, 정보보안에 대한 가치 차이가 발현될 수 있음을 고려하였다. 특히, 연구는 정보보안 가치 차이의 선행 요인(복잡성)과 결과를 복합적으로 확인한 관점에서, 선행연구로서의 시사점을 지닌다.

셋째, 본 연구는 조직의 업무적 환경이 개인의 정보보안 관련 준수 활동에 영향을 줄 수 있음을 확인하였다. 특히, 연구는 경쟁적 분위기의 형성이 가지는 부정적 효과를 고려하여, 정보보안 분야에 적용하였다. 즉, 경쟁적 분위기는 개인의 성과 창출에 기여하지만, 과할 때는 개인 중심의 행동을 유발하는데, 성과 창출을 위한 손쉬운 정보 공유 활동과 정보보호 관점에서 억제적 활동 중 개인은 정보보호 활동을 감소시킬 가능성이 존재할 것으로 판단하였다. 즉, 학술적으로 본 연구는 경쟁적 분위기가 개인의 정보보안 준수 의도를 감소시키는 것을 확인하였으므로, 단순히 정보보안 관련 문화 등 환경적 조건이 아닌 일반적인 조직 환경까지 고려된 요인을 제시한 관점에서 선행연구로서의 의미를 지닌다.

본 연구는 조직 내부의 정보보안 목표 달성에 반드시 요구되는 조직원의 보안 준수에 부정적 영향을 주는 조건을 다각적으로 확인한 관점에서 현실에서 조직 전략 수립에 시사점을 제언한다.

첫째, 본 연구는 정보보안 작업 복잡성 개념을 적용하여, 조직원이 느낄 수 있는 정보보안 활동의 부담감이 준수 행동에 어떠한 영향을 주는지를 확인하였다. 즉, 정보보안 작업 복잡성은 기존 업무에 정보보안을 반영함에 있어, 업무의 양과 관련 업무를 수행하는데 필요한 정보 등이 복합적으로 작용하여, 정보보안 활동의 어려움을 겪는 상황을 지칭한다. 조직이 엄격한 정보보안 정책과 규정을 수립하였지만, 조직 구성원들의 동의 또는 업무적 상황을 고려하지 않은 활동에 대한 요구사항이 증대될수록 조직원은 정보보안 작업 복잡성을 느끼게 되어, 정보보안 준수에 어려움을 겪게 된다. 따라서, 조

직은 정보보안을 반영한 업무 수행과정에 대한 정확한 지침을 마련하고, 정보보안 교육 및 훈련 등을 통해 조직원이 느끼는 복잡성을 최소화하는 것이 요구된다.

둘째, 본 연구는 정보보안 가치 차이 개념을 적용하여, 조직이 추진하는 정보보안에 대한 가치가 본인의 가치와 차이가 존재할 때 발생 가능한 문제점을 확인하였다. 즉, 조직이 추진하는 정보보호에 대한 필요성과 가치가 본인의 업무 또는 활동에 도움이 되지 않거나, 정보보안 가치를 명확하게 이해하지 못할 때, 가치 차이가 발생할 수 있는데, 정보보안 가치 차이는 정보보안 관련 행동을 하지 않도록 하는 조건이 된다. 특히 본 연구는 가치 차이가 발생하는 원인으로, 정보보안 작업 복잡성에 있음을 지적하였는데, 과도하거나, 사전 정보가 부족한 정보보안 요구사항은 개인에게 복잡함을 형성하여, 정보 관리의 가치를 상실하도록 돕는 조건이 됨을 확인하였다. 따라서, 조직은 정보보안 활동의 필요성과 활동을 통해 얻을 수 있는 혜택 등 가치를 조직원이 명확하게 이해할 수 있도록 지원하는 것이 요구되며, 특히, 정보보안 활동에 필요한 사전 정보와 수준을 체계적으로 제공함으로써, 정보보안 가치를 이해할 수 있도록 하는 것이 필요하다.

셋째, 본 연구는 조직 업무 환경 요소가 조직원의 정보보안 활동에 영향을 주는 조건임을 제시하였다. 특히, 경쟁적 분위기는 개인 중심의 사고 및 성과 창출 행동을 강하게 유발하는 조건인데, 정보보안과 연계하여 준수 행동에 부정적 영향을 미치는 환경적 조건임을 확인하였다. 따라서, 조직은 경쟁심이 가지는 긍정적 효과를 유지하되, 조직 전체를 위한 활동이 개인에게 주어지는 보상과 혜택에 도움이 될 수 있도록 인적자원 전략을 수립하는 것이 필요하다. 즉, 개인에게 주어진 본연의 업무 성과 달성을 위해서, 당사자는 정보보안 활동을 의도적으로 회피할 수 있는데, 보상 체계가 조직 전체를 위한 활동으로 확장될 경우, 이러한 경쟁적 행동을 감소시킬 수 있을 것으로 판단된다. 또한, 경쟁적 분위기는 정보보안 미준수 원인(복잡성, 가치 차이)이 준수 의도에 미치는 부정적 영향을 강화하는 조절적 요인임을 확인하였다. 즉, 개인이 느끼는 정보보안 관련 행동 조건이 업무적 환경과 떨어져 있는 것이 아님을 제시하므로, 조직은 정보보안 목표 달성을 위해, 조직원의 업무 환경을 함께 고려하는 것이 요구된다.

본 연구는 정보보안 미준수 원인을 설명하는 매커니즘을 체계적으로 제시하였으나, 다음의 연구적 한계를 가지며 향후 보완될 필요성이 있다. 첫째, 본 연구는 설문지 기법을 적용하여 연구가설을 검증하였다. 특히, 응답자가 조직의 정보보안 상황과 개인의 특성에 대한 인식을 측정하여 결론을 제시하였다. 즉, 연구는 조직 특성에 대하여 개인 인식을 기반으로 측정하였다. 비록 표본의 양에 문제는 없으나, 경쟁적 분위기와 관련된 조직 특성을 명확하게 파악하기 위해서는 분위기 특성에 따른 집단 분석이나, 조직 정보보안 지원 수준에 대한 집단 분석 등을 통해 개인의 행동 변화를 측정한다면, 관련된 조직 특성별 차별화된 결론을 제공할 수 있을 것으로 판단한다. 둘째, 본 연구는 정보보안 복잡성과 가치 차이 관점의 부정적 조건을 제시하고 영향 관계를 파악하였다. 하지만, 본 연구는 조직에서 개인의 권한, 위치 등 특성의 차이를 고려하지 않았으며, 개인이 특정 문제를 해결하는데 적용되는 차별적 특성을 반영하지 않았다. 즉, 개인이 가지고 있는 환경적 차이점과 개인의 문제에 대한 대처의 차별성 등은 행동의 변화를 일으키는 중요한 조건이다. 따라서, 향후 연구에서 개인차 변인을 활용하여 정보보안 행동 변화를 연구한다면, 개인 맞춤형 전략 수립에 도움을 줄 것으로 기대한다.

참고문헌

[1] Z. Tang, A. S. Miller, Z. Zhou, and 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, April, 2021. https://doi.org/10.1016/j.giq.2021.101572

[2] C. Lin, J. L. Wittmer, and X. Luo, “Cultivating Proactive Information Security Behavior and Individual Creativity: The Role of Human Relations Culture and IT Use Governance,” *Information & Management*, Vol. 59, No. 6, pp. 103650, September, 2022. https://doi.org/10.1016/j.im.2022.103650

[3] I. Hwang, “The Effects of Information Security Organizational Injustice on Information Security Anxiety and Avoidance Behavior: Focusing on Moderation Effects of Victim Justice Sensitivity,” *Journal of Digital Contents Society*, Vol. 22, No. 5, pp. 855-866, May, 2021. http://dx.doi.org/10.9728/dcs.2021.22.5.855

[4] J. W. Lian, “Understanding Cloud-based BYOD Information Security Protection Behaviour in Smart Business: In Perspective of Perceived Value,” *Enterprise Information Systems*, Vol. 15, No. 9, pp. 1216-1237. September, 2021. https://doi.org/10.1080/17517575.2020.1791966

[5] R. West, “The Psychology of Security,” *Communications of the ACM*, Vol. 51, No. 4, pp. 34-40, April, 2008. http://doi.acm.org/10.1145/1330311.1330320

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

[7] M. Siponen, S. Pahnila, and M. A. Mahmood, “Compliance with Information Security Policies: An Empirical Investigation,” Computer, Vol. 43, No. 2, pp. 64-71,

February, 2010. https://doi.org/10.1109/MC.2010.35

[8] B. Xue, F. Xu, X. Luo, and M. Warkentin, “Ethical Leadership and Employee Information Security Policy (ISP) Violation: Exploring Dual-mediation Paths,” *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 1, No. 1, pp. 5-23, August, 2021. https://doi.org/10.1108/OCJ-02-2021-0002

[9] F. Nasirpouri Shadbad and D. Biros, “Understanding Employee Information Security Policy Compliance from Role Theory Perspective,” *Journal of Computer Information Systems*, Vol. 61, No. 6, pp. 571-580, March, 2021. https://doi.org/10.1080/08874417.2020.1845584

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

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

[12] D. Cooper, “Dissimilarity and Learning in Teams: The Role of Relational Identification and Value Dissimilarity,” *International Journal of Intercultural Relations*, Vol. 37, No. 5, pp. 628-642, September, 2013. https://doi.org/10.1016/j.ijintrel.2013.06.005

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

[14] I. Hwang, “The Effect on Psychological Empowerment on IS Compliance Intention: Focusing on the Moderating Effect of Trust and Justice,” *Journal of Digital Contents Society*, Vol. 22, No. 10, pp. 1683-1694, October, 2021. http://dx.doi.org/10.9728/dcs.2021.22.10.1683

[15] P. Jiménez, A. Dunkl, and S. Peißl, “Workplace Incivility and Its Effects on Value Congruence, Recovery-Stress-State and the Intention to Quit,” *Psychology*, Vol. 6, No. 14, pp. 1930-1939, November, 2015. http://dx.doi.org/10.4236/psych.2015.614190

[16] J. R. Edwards and D. M. Cable, “The Value of Value Congruence,” *Journal of Applied Psychology*, Vol. 94, No. 3, pp. 654-677, September, 2009. https://doi.org/10.1037/a0014891

[17] E. V. Hobman, P. Bordia, and C. Gallois, “Consequences of Feeling Dissimilar from Others in a Work Team,” *Journal of Business and Psychology*, Vol. 17, No. 3, pp. 301−325, March, 2003. https://doi.org/10.1023/A:1022837207241

[18] K. A. Jehn, G. B. Northcraft, and M. A. Neale, “Why Differences Make a Difference: A Field Study of Diversity, Conflict, and Performance in Workgroups,” *Administrative Science Quarterly*, Vol. 44, pp. 741−764, December, 1999. https://doi.org/10.2307/2667054

[19] N. F. Doherty and S. T. Tajuddin, “Towards a User-centric Theory of Value-driven Information Security Compliance,” *Information Technology & People*, Vol. 31, No. 2, pp. 348-367, April, 2018. https://doi.org/10.1108/ITP-08-2016-0194

[20] I. Hwang, “Analysis of the Effects of Information Security Sanction and Role Ambiguity on Compliance Intention: Focusing on Moderation Effects of Technical Support and Task Coping,” *Journal of Digital Contents Society*, Vol. 22, No. 2, pp. 271-280, February, 2021. http://dx.doi.org/10.9728/dcs.2021.22.2.271

[21] K. Lee and S. Lee, "The Effect of Popularity and Manual Service of Smartphone on Technostress," *Journal of Digital Contents Society*, Vol. 18, No. 6, pp. 1079-1089, October, 2017. http://dx.doi.org/10.9728/dcs.2017.18.6.1079

[22] Z. Zhang and M. Min, “Organizational Rewards and Knowledge Hiding: Task Attributes as Contingencies,” *Management Decision*, Vol. 59, No. 10, pp. 2385-2404, September, 2021. https://doi.org/10.1108/MD-02-2020-0150

[23] S. H. Chan, Q. Song, and L. J. Yao, “The Moderating Roles of Subjective (Perceived) and Objective Task Complexity in System Use and Performance,” *Computers in Human Behavior*, Vol. 51, pp. 393-402, October, 2015. https://doi.org/10.1016/j.chb.2015.04.059

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

[25] Z. Zhang, M. Min, X. Cai, and H. Qiu, “Mitigating the Negative Performance Effect of Project Complexity Through an Informal Mechanism: The Conditional Mediating Role of Knowledge Hiding,” *International Journal of Project Management*, Vol. 40, pp. 192-204, April, 2022. https://doi.org/10.1016/j.ijproman.2022.01.002

[26] X. Lv, R. Zhang, and Q. Li, “Value Co-destruction: The Influence of Failed Interactions on Members’ Behaviors in Online Travel Communities,” *Computers in Human Behavior*, Vol. 122, pp. 106829, September, 2021. https://doi.org/10.1016/j.chb.2021.106829

[27] A. B. Semerci, “Examination of Knowledge Hiding with

Conflict, Competition and Personal Values," *International Journal of Conflict Management*, Vol. 30, No. 1, pp. 111-131, January, 2018. https://doi.org/10.1108/IJCMA-03-2018-0044

[28] K. Hedström, E. Kolkowska, F. Karlsson, and J. P. Allen, "Value Conflicts for Information Security Management," *The Journal of Strategic Information Systems*, Vol. 20, No. 4, pp. 373-384, December, 2011. https://doi.org/10.1016/j.jsis.2011.06.001

[29] M. S. Han, K. Masood, D. Cudjoe, and Y. Wang, "Knowledge Hiding as the Dark Side of Competitive Psychological Climate," *Leadership & Organization Development Journal*, Vol. 42, No. 2, pp. 195-207, June, 2020. https://doi.org/10.1108/LODJ-03-2020-0090

[30] M. Oubrich, A, Hakmaoui, L. Benhayoun, K. S. Söilen, and B. Abdulkader, "Impacts of Leadership Style, Organizational Design and HRM Practices on Knowledge Hiding: The Indirect Roles of Organizational Justice and Competitive Work Environment," *Journal of Business Research*, Vol. 137, pp. 488-499, December, 2021. https://doi.org/10.1016/j.jbusres.2021.08.045

[31] H. Peng, C. Bell, and Y. Li, "How and When Intragroup Relationship Conflict Leads to Knowledge Hiding: The Roles of Envy and Trait Competitiveness," *International Journal of Conflict Management*, Vol. 32, No. 3, pp. 383-406, September, 2020. https://doi.org/10.1108/IJCMA-03-2020-0041.

[32] S. Trang and I. Nastjuk, "Examining the Role of Stress and Information Security Policy Design in Information Security Compliance Behavior: An Experimental Study of In-task Behavior," *Computers & Security*, Vol. 104, pp. 102222, May, 2021. https://doi.org/10.1016/j.cose.2021.102222

[33] A, Vedadi, M. Warkentin, and A. Dennis, "Herd Behavior in Information Security Decision-making," *Information & Management*, Vol. 58, No. 8, pp. 103526, December, 2021. https://doi.org/10.1016/j.im.2021.103526

[34] J. C. Nunnally, *Psychometric Theory*, 2th ed. New York: McGraw-Hill, 1978.

[35] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, Vol. 18, No. 1, pp. 39-50, February, 1981. https://doi.org/10.1177/002224378101800104

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

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

황인호(Inho Hwang)

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

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