Regular paper | Journal of the KIECS. pp. 241-248, vol. 19, no. 1, Feb. 29. 2024, t. 123, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2024.19.1.241

정보보안 정책, 기술, 그리고 커뮤니케이션 불확실성의 영향: 정보보안 역할 정체성의 역할

황인호*

The Influence of Information Security Policy, Technology, and Communication Uncertainties: The Role of Information Security Role Identity

In-Ho Hwang*

요 약

사회적으로, 조직이 보유한 정보 자원에 대한 엄격한 관리를 요구하고 있다. 조직들은 기술적으로 외부 정보 침입에 대처해야 할 뿐 아니라, 내부자에 의한 정보 노출 가능성까지 관리해야 하는 상황에 직면해 있다. 하지만, 조직이 도입한 정보보안 정책, 기술 등은 조직 내부의 보안 수준 달성에 도움을 주지만, 과도하거나 체계적이지 못한 보안 구조는 조직원의 불확실성을 높일 수 있다. 본 연구는 정보보안 관련 조직의 구조적인 불확실성 요인을 제시하고 행동에 미치는 영향을 제시한다. 즉, 정보보안 정책, 기술, 그리고 커뮤니케이션 불확실성이 구조적으로 존재할 수 있음을 밝힌다. 정보보안 환경 관련 선행연구를 통해 연구 모델과 가설을 제시하였으며, 구조방정식 모델링을 적용하여 가설을 검정하였다. 가설 검정 결과, 정보보안 정책, 기술, 그리고 커뮤니케이션 불확실성이 조직원의 역할 정체성과 준수 의도를 감소시켰다. 연구 결과는 조직 내 정보보안 관련 구조적인 불확실성 개선 조건을 제시하였기 때문에, 조직 내부의 정보보안 목표 달성을 위한 환경 전략 방향을 제언한다.

ABSTRACT

Socially, organizations are required to effectively manage their information resources, both in terms of acquiring information from external sources and safeguarding against potential breaches by insiders. While information security policies and technologies implemented by organizations contribute to achieving internal security, an overly complex or disorganized security structure can create uncertainty among employees. In this study, we identify factors of structural information security (IS)-related uncertainty within organizations and propose that they contribute to non-compliance. We develop a research model and hypotheses based on previous studies on the information security environment and test these hypotheses using structural equation modeling. Our findings indicate that uncertainties related to IS policy, technology, and communication decrease employees' IS role identity and their intention to comply with IS measures. By addressing these uncertainties, organizations can improve their IS environment and work towards achieving their IS goals.

키워드

Communication Uncertainty, Policy Uncertainty, Technology Uncertainty, Role Identity, Compliance Intention
커뮤니케이션 불확실성, 정책 불확실성, 기술 불확실성, 업무 동일시, 준수 의도

* 교신저자: 국민대학교 교양대학
• 접 수 일 : 2023. 11. 19
• 수정완료일 : 2023. 12. 31
• 게재확정일 : 2024. 02. 17
• Received : Nov. 19, 2023, Revised : Dec. 31, 2023, Accepted : Feb. 17, 2024
• Corresponding Author : In-Ho Hwang
College of General Education, Kookmin University,
Email : hwanginho@kookmin.ac.kr

Ⅰ. 서 론

정보 관리가 조직의 중요한 성장 요인으로 인식되고, 조직이 보유한 정보 자산이 단순히 조직만의 문제가 아닌 정보와 관련된 사회 구성원에게 직접적인 피해를 주는 것으로 판단되면서, 국가 차원에서 조직의 정보보안 및 개인 프라이버시 보호를 위한 법률 등을 도입하고 있다[1]. 이에, 조직들은 생성된 정보 자원들을 안전하게 보호하기 위해 정보보안 정책과 기술의 도입 및 활용을 위한 투자를 높이고 있다[2]. 조직에서 발생할 수 있는 보안 사고의 유형을 살펴보면, 사고의 약 70~80%가 악의적 형태로 외부의 기술적 침입을 통해 발생하고 있으나, 조직과 관련된 내부자 또는 파트너에 의한 정보 노출 사고 또한 20~30% 수준에서 발생하고 있다[3]. 즉, 조직은 외부 침입을 억제하기 위한 기술적 도입 외, 내부자의 정보 오남용 등을 최소화하기 위한 보안 정책 및 행동 정보 지원까지 요구되는 실정이다.

사람에 의한 정보 노출 사고의 예방 및 억제를 위한 방향을 제시한 선행연구는 정보보안 활동에 대한 개인의 활동 정보에 대하여, 개인이 조직보다 관련 정보를 많이 보유하고, 시스템 활용의 증대로 언제든 보안 사고를 일으킬 가능성이 존재하므로, 심리적 관점에서 보안 준수를 위한 동기 형성과 준수 행동 강화를 위한 환경 구축이 무엇보다 중요함을 제시하고 있다[4-6]. 즉, 선행연구들은 능동적인 보안 행동을 강화할 수 있는 조직 환경 및 지원 체계의 구축이 조직에 선행되어야 함을 중점적으로 제시해왔다. 반면, 조직원 관점에서 조직의 구조적 측면에서 보안 지원 체계에 대한 부족이 어떻게 보안 준수 활동에 부정적 영향을 미칠 수 있는지를 설명하는 연구는 부족하다.

연구 목적은 개인을 둘러싼 특정 환경에 대한 과도한 걱정의 상황 개념인 불확실성(Uncertainty)을 적용하여[7], 조직의 정보보안 지원 체계에서 불확실성이 발생할 수 있는 조건을 다각적으로 살피고, 개인의 보안 준수에 미치는 영향을 확인하는 것이다. 조직은 정보보안 활동 강화를 위해, 보안 정책과 기술의 도입에 높은 수준의 자원을 투입하고, 조직원이 해당 기술 또는 활동을 충분히 할 수 있도록 커뮤니케이션 체계를 지원하고 있다. 역설적으로, 정보보안 정책, 기술, 그리고 커뮤니케이션 활동으로 인한 정보가 개인에게 충분하게 전달되지 않을 때, 조직원은 불확실성을 느낄 수 있으며, 부정적 행동 의도를 보일 가능성이 존재한다. 연구는 정보보안 관련 정책, 기술, 그리고 커뮤니케이션 불확실성이 조직원의 정보보안 관련 역할 정체성을 통해 준수 의도에 부정적 영향을 미칠 수 있음을 확인함으로써, 조직이 제공해야 할 정책, 기술 등의 정보 불확실성 감소를 위한 방향성을 제안하고자 한다.

Ⅱ. 이론적 배경

2.1 정보보안 현황

정보보안에 대한 조직의 관리 요소는 더욱 강화되고 있다. 미국은 2021년 공공기관을 중심으로 “제로트러스트(Zero-trust)” 아키텍처 적용을 요구하였는데, 조직 외부에 적용된 보안 체계를 내부에도 동일하게 적용하여, 내부로부터의 정보 노출 가능성을 최소화하길 요구하고 있다[8]. 한국은 정보통신 분야 등 개인정보를 엄격하게 관리해야 하는 산업을 중심으로 정보보호 및 개인정보보호 관리체계 인증(ISMS-P)을 법적으로 요구하고 있다[9]. 실제, 국내 정보보안 시장은 2022년 6조 7천억 원에서 2024년 7조 3천억 원으로 가파르게 성장할 것으로 기대되고 있으며, 조직 규모가 큰 기업을 중심으로 정보보안 정책 및 기술을 도입하고, 관리 조직을 운영하여 발생 가능한 이슈를 최소화하길 기대하고 있다[9]. 하지만, 정보보안은 한 건의 실수가 큰 사고로 이어진다. 특히, 조직 내부의 보안 사고는 조직이 쉽게 발견하지 못할 가능성이 크므로, 조직 구성원에 대한 보안 준수 의식 강화를 통한 자발적 참여가 무엇보다 필요하다[10]. 이에, 본 연구는 조직원의 보안 준수 의도 약화 원인을 제시하여 역설적으로 행동 강화 전략을 제안하고자 한다. 준수 의도(Compliance Intention)는 개인이 관리하는 정보자산에 대한 주변의 위협으로부터 보호하고자 하는 의지를 지칭한다[4]. 따라서, 준수 의도가 감소한 개인은 조직보다 개인 중심의 행동을 할 가능성이 크다.

2.2 정보보안 역할 정체성

집단에서 개인은 집단 또는 다른 사람들과 상호작용을 통해서 본인의 위치를 인식하게 되는데, 정체성

(Identity)은 상호작용 과정에서 관계, 역할 등에 대한 집단 내 본인의 존재 의미를 부여하는 수준을 의미한다[11]. 역할 정체성(Role Identity)은 집단에서 개인이 수행하는 역할을 확인하고 본인에게 의미를 부여하는 개념이다[12]. 즉, 개인이 특정 집단에서 부여된 역할에 대한 인식을 통해 내가 누구인지를 판단하도록 하고, 해당 집단에 어떤 행동을 할 것인지를 의사결정을 하도록 돕는 요소이다. 조직에서 개인은 주어진 업무 등에서 역할을 인식하고, 역할을 충분히 하여 조직 또는 동료들로부터 인정을 받고, 구성원임을 느끼게 된다[11], [13]. 정보보안 관점에서 역할 정체성(Information Security Role Identity)은 정보 관리 상황에서 개인이 수행하는 행동이 조직과 본인에게 이익이 되고 공동체로서 역할을 하는지를 인식하는 수준을 의미한다[14].

역할 정체성을 수립한 사람은 집단의 구성원임을 알리고, 본인과 집단의 이익을 위한 행동을 보인다. Ogbanufe[2021]은 정보보안 분야에서 정체성을 확립한 사람은 자신의 위치를 명료하게 알리기 위하여, 보안 준수 행동을 보인다고 하였으며[14], Ma and Agarwal[2017]은 커뮤니티 참여자의 정체성 인식은 커뮤니티 구성원들에게 본인의 지식 공유 활동을 높이는 행동을 하는 것을 확인하였다[11]. Hwang[2022]은 조직원이 조직에 대해 사회적 정체성을 확립할 경우, 정보보안 관련 제언 행동을 보임을 증명하였다[13]. 즉, 선행연구는 집단에서의 역할 관점의 정체성을 확립한 사람은 역할을 강화함으로써 본인의 위치를 인식시키려는 모습을 보임을 설명한다. 이에, 본 연구는 정보보안 역할 정체성이 보안 준수 의도에 영향을 줄 것으로 기대하며, 다음 가설을 제시한다.

H1. 정보보안 역할 정체성은 조직원의 보안 준수 의도에 긍정적 영향을 미친다.

2.3 정보보안 불확실성

불확실성(Uncertainty)은 외부의 특정 조건에 대한 불확실한 정보 등으로 명확하게 미래를 예측하기 어려운 상태로서[15], 과도한 걱정, 불안 등의 부정적 인식을 형성시키는 조건이다[7]. 특히, 불확실성을 높게 받아들이는 사람은 대상 조건을 위협 요소로 인식하여 감정적 관점의 스트레스를 발현시키거나 육체적 문제를 일으키기도 하고, 나아가 불확실성 문제 해결을 위해 회피하려는 모습을 보이기도 한다[16]. 정보보안에 대하여, 조직이 도입한 정보보안은 미준수 행동에 대한 엄격한 처벌을 기반으로 하고 있으며, 외부 환경 변화에 따라 관련 필요 정보의 변화가 빠르게 일어난다[17]. 즉, 조직원이 업무에 적용해야 하는 정보보안 관련 불확실성은 환경 변화에 대처하는 과정에서 지속해서 발현될 가능성이 있다.

본 연구는 정보보안 관련 불확실성 발현 조건을 조직 구조적 관점에서 살펴본다. 조직 내 구조적 측면에서 불확실성 발생 조건을 살펴보면, 정보보안 정책과 기술이 현실 업무의 특성 명확하게 반영되지 않거나, 기존 체계를 빠르게 변화시켜 조직원이 주어진 체계에서 정확하게 보안 관련 활동을 수행하기 힘들다고 판단되는 상황에서 발현될 수 있으며, 조직과 구성원 간 소통이 충분히 이루어지지 못하여 정보를 적절히 확보하지 못하는 상황에서 발현될 수 있다. 첫째, 정보보안 정책 불확실성(Information Security Policy Uncertainty)은 조직 내 보안 활동을 수행하기 위해 구현된 정책이 불충분하다고 판단되는 수준을 의미한다[18]. 최근, 조직 업무 환경이 온라인과의 연계 등으로 빠르게 변화하고 있는데, 정보보안 정책이 해당 환경의 특성에 맞게 변화하지 못하였다면 조직의 보안 정책에 대한 의구심을 가질 가능성이 있으며, 정책 불확실성으로 발현될 수 있다. 둘째, 정보보안 기술 불확실성(Information Security Technology Uncertainty)은 정보보안을 위해 도입한 기술이 계속 변화하여 개인의 업무에 적용이 불충분하다고 판단되는 수준을 의미한다[7]. 예를 들어, 재택 근무 등을 위해 도입한 보안 기술에 대하여 조직원은 이해가 부족한 상황에서 기술을 업무에 적용해야 하는 상황에 직면하게 되고, 조직원은 기술 불확실성을 인식할 수 있다. 셋째, 정보보안 커뮤니케이션 불확실성(Information Security Communication Uncertainty)은 이해관계자 간 정보보안 관련 지식, 정보 등의 가치 자원을 충분히 제공받지 못하고 있다고 판단되는 수준을 의미한다[19]. 조직에서 개인은 특정 활동 및 성과 달성을 위해 다양한 정보 자원을 충분히 확보해야 하는데, 조직은 공식적, 비공식적 채널 및 도구 등을 제공한다. 하지만, 정보보안 제공 방식과 정보의 수준이 충분히 제공되지 않을 때, 조직원들은 커뮤니케이션 부족으로 인하여 적절히 대처하지 못하는 상황에

직면할 수 있다.

특정 환경에 대한 불확실성의 증가는 개인의 부정적 인식 수준을 높인다. D'Arcy and Teh[2019]는 불확실성이 높은 정보보안 환경은 개인의 부정적 상태인 피로, 좌절감 등을 높이는 조건이라고 하였으며[20], Hwang[2022]은 조직이 정보보안을 위해 공식적으로 제공하는 기술 및 커뮤니케이션 채널에 대한 불확실성은 개인들의 정보보안에 대한 걱정 인식 수준을 높이는 요소임을 확인하였다[13]. 즉, 불확실성 조건은 대상에 대한 개인의 인식을 부정적으로 발현하도록 돕는다. 이에, 연구는 정보보안 정책, 기술, 그리고 커뮤니케이션 불확실성이 역할 정체성에 부정적 영향을 미칠 것으로 판단하며, 다음 가설을 제시한다.

H2a. 정보보안 정책 불확실성은 정보보안 역할 정체성에 부정적 영향을 미친다.

H2b. 정보보안 기술 불확실성은 정보보안 역할 정체성에 부정적 영향을 미친다.

H2c. 정보보안 커뮤니케이션 불확실성은 정보보안 역할 정체성에 부정적 영향을 미친다.

또한, 조직원이 업무 수행과정에서 적용해야 할 정보보안에 대하여, 조직이 정책, 기술, 그리고 커뮤니케이션 관점에서 충분히 서비스하지 못할 때, 보안 준수 활동에 부정적 영향을 줄 수 있다. Tarafdar et al.[2007]은 불확실성이 포함된 기술 스트레스 환경은 개인의 생산성에 부정적 영향을 준다고 하였다[7]. D'Arcy et al.[2014]은 통합된 관점에서의 정보보안 불확실성 인식은 조직원에게 심리적 이탈을 높여 구축된 보안 체계를 회피하려는 의도를 가질 수 있다고 하였으며[21], Hwang and Cha[2018]은 정보보안 기술 불확실성이 조직원의 조직 몰입 및 준수 의도를 줄이는 선행 조건임을 밝혔다[2]. 즉, 정보보안 지원 체계의 불확실성은 개인의 정보보안 관련 행동에 부정적 영향을 미치게 된다. 이에, 연구는 정보보안 정책, 기술, 그리고 커뮤니케이션의 불확실성이 준수 의도에 부정적 영향을 줄 것으로 판단하여, 다음의 가설을 제시한다.

H3a. 정보보안 정책 불확실성은 보안 준수 의도에 부정적 영향을 미친다.

H3b. 정보보안 기술 불확실성은 보안 준수 의도에 부정적 영향을 미친다.

H3c. 정보보안 커뮤니케이션 불확실성은 보안 준수 의도에 부정적 영향을 미친다.

III. 연구 모델 및 측정

3.1 연구 모델

본 연구는 정보보안 준수 활동에 부정적 영향을 줄 수 있는 조직 내 불확실성 요인을 제시하고, 조직원의 역할 정체성 및 준수 의도에 미치는 영향을 확인하기 위해, 그림 1의 연구 모델을 제시한다. 그리고, 적용 요인 간의 전체적인 연계성을 확인하기 위하여 구조방정식 모델링을 통해 가설을 검정하며, AMOS 22.0 패키지를 반영한다.

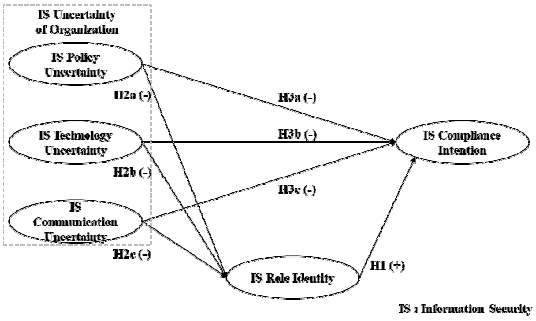

그림 1. 연구모델
Fig. 1 Research model

3.2 측정 도구 및 표본 확보

가설 검정은 설정한 연구 대상에게 설문하여 확보한 데이터를 활용한다. 또한, 설문에 적용된 모든 요인은 정보보안 또는 조직 연구에서 적용된 다항목 기반의 측정 도구를 반영하되, 정보보안 특성을 반영하여 수정된 문항에 대해 7점 리커트 척도를 적용하여 최종적으로 구성하였다.

독립변수인 정보보안 정책 불확실성은 Vedadi et al.[2021] 연구에서 도출하였으며, "나는 정보보안 정책이 무엇에 관한 것이며, 그것이 나를 위해 무엇을 할 수 있는지 잘 모르겠음" 등 4개 문항을 적용하였다. 정보보안 기술 불확실성은 Tarafdar et al. [2007] 연구에서 도출하였으며, "나는 도입된 정보보안 기술에 대해 충분하게 이해하지 못하고 있음" 등 4개 문

항을 적용하였다. 정보보안 커뮤니케이션 불확실성은 Jo and Jo [2012] 연구에서 도출하였으며, “조직으로부터 받은 보안 관련 메시지에 대해, 잘 받았다고 판단하기 어려움” 등 4개 문항을 적용하였다. 매개 변수인 정보보안 역할 정체성은 Ogbanufe[2021] 연구에서 도출하였으며, “조직의 보안 정책을 준수하는 것은 나에게 중요함” 등 3개 문항을 적용하였다. 종속변수인 준수 의도는 Chen et al.[2012] 연구에서 도출하였으며, “나는 요구받은 보안 관련 정책을 따를 의도가 있음” 등 3개 문항을 적용하였다.

연구 목적에 맞는 표본을 확보하기 위하여, 연구 대상은 정보보안 정책을 도입한 기업에서 근무하며, 정보보안 준수 활동을 요구받고 있는 직장인으로 설정하였다. 설문은 M리서치의 직장인 회원을 대상으로 온라인으로 진행하였다.

표 1. 표본의 특성
Table 1. Characteristics of samples

Categories		Frequency	%
Gender	Male	195	47.9
	Female	212	52.1
Age	Under 30	82	20.1
	31 - 40	100	24.6
	41 - 50	111	27.3
	Over 51	114	28.0
Industry	Manufacturing	112	27.5
	Service	295	72.5
Job Position	Staff	160	39.3
	Assistant Manager	95	23.3
	Manager	72	17.7
	Over Manager	80	19.7
Firm Size	Under 10	24	5.9
	10~49	108	26.5
	50~299	131	32.2
	Over 300	144	35.4
Total		407	100.0

적정 표본 확보를 위해, 설문 참여 전, 회원들은 직업, 나이, 성별에 응답하였으며, 직장인이라고 응답한 사람 중 조직이 정보보안 정책을 보유하고 있다고 응답한 사람만 참여하도록 설계하였다. 응답 대상자들은 본 설문에 앞서 설문 목적과 표본의 통계적 활용 정보를 확인하였으며, 그럼에도 참여하겠다고 응답한 사람만 설문을 수행하였다. 확보된 표본은 407건이며, 응답자들의 특성은 표 1과 같다.

Ⅳ. 분 석

4.1 신뢰성 및 타당성

가설 검정에 적용할 데이터는 요인별 다 항목으로 구성되어 있으므로, 측정 도구들이 요인을 대표할 수 있는지 요인별 신뢰성과 타당성을 확인하였다.

표 2. 타당성 및 신뢰성의 결과
Table 2. Result for construct validity and reliability

Constructs		Factor Loading	Cronbach's Alpha	CR	AVE
PU	PU4	0.878	0.913	0.899	0.690
	PU3	0.874			
	PU2	0.859			
	PU1	0.792			
TU	TU4	0.738	0.885	0.877	0.641
	TU3	0.847			
	TU2	0.836			
	TU1	0.829			
CU	CU4	0.762	0.872	0.855	0.596
	CU3	0.827			
	CU2	0.813			
	CU1	0.778			
RI	RI3	0.861	0.894	0.879	0.708
	RI2	0.884			
	RI1	0.836			
CI	CI3	0.813	0.867	0.869	0.688
	CI2	0.878			
	CI1	0.793			

PU(Policy Uncertainty), TU(Technology Uncertainty), CU(Communication Uncertainty), RI(Role Identity), CI(Compliance Intention)
CR: Construct Reliability, AVE: Average Variance Extracted

첫째, 신뢰성은 측정 문항들을 반복 측정 시, 요인을 일관성 있게 설명하는지를 확인하는 것으로, SPSS 21.0 패키지의 크론바흐 알파 값을 통해 판단한다. 요인별 요구되는 크론바흐 알파는 0.7 이상이다 [22]. 측정 도구들의 요인에 대한 신뢰성은 결과는 표

2와 같으며, 모든 요인의 신뢰성을 확보하였다.

둘째, 타당성은 측정 도구가 요인을 정확하게 측정하는지를 확인하는 것으로서, 구성 개념을 충분히 설명하는지를 확인하는 집중 타당성과 요인 간의 차이를 확인하는 판별 타당성을 적용한다. 이를 위해, AMOS 22.0 패키지를 활용하여 확인적 요인분석을 하였다. 해당 모델의 적합도는 χ^2/df = 1.534, RMR = 0.031, RMSEA = 0.036, GFI = 0.950, AGFI = 0.931, NFI = 0.961, 그리고 CFI = 0.986으로 나타나, 0.05 이하의 값을 요구하는 RMR, RMSEA와 0.9 이상의 값을 요구하는 GFI, AGFI, NFI, CFI 모두 요구사항을 충족하였으므로[23], 모델의 측정치를 활용하였다. 집중 타당성은 개념 신뢰도(CR)와 평균분산추출(AVE) 값을 구하여 확인하되, 요인별 개념 신뢰도는 0.7 이상, 요인별 평균분산추출은 0.5 이상의 값을 요구한다[23]. 분석 결과는 표 2와 같으며, 모든 요인의 집중 타당성을 확보한 것으로 나타났다.

판별 타당성은 요인 간 차이 수준을 확인하기 때문에, 요인들의 상관계수와 평균분산추출 값을 비교하여 확인한다. 선행연구는 평균분산추출 값의 제곱근이 모든 요인의 상관계수보다 클 때, 판별 타당성을 확보했다고 본다[23]. 표 3에 분석 결과를 제시하였으며, 요인 간의 차별성이 확인되었다.

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

Constructs	1	2	3	4	5
PU	**0.830[a]**				
TU	.47**	**0.801[a]**			
CU	.51**	.587**	**0.772[a]**		
RI	-.46**	-.47**	-.49**	**0.841[a]**	
CI	-.41**	-.43**	-.45**	.43**	**0.830[a]**

PU(Policy Uncertainty), TU(Technology Uncertainty), CU(Communication Uncertainty), RI(Role Identity), CI(Compliance Intention)
a = square root of the AVE, **: $p < 0.01$

4.2 가설 검정

가설 검정은 모든 요인을 동시에 반영하여 요인 간의 연계성을 확인하는 구조방정식모델링을 적용하여 확인한다. 우선, 구조모델의 적합도를 확인하였다. 적합도 확인 기준은 확인적 요인분석과 동일하게 하였다. 결과는 χ^2/df = 1.460, RMR = 0.031, RMSEA = 0.034, GFI = 0.953, AGFI = 0.935, NFI = 0.963, 그리고 CFI = 0.988로 나타나, 가설 검정에 측정치들을 반영하였다. 구조방정식 모델링을 적용한 결과는 그림 2와 표 4와 같다.

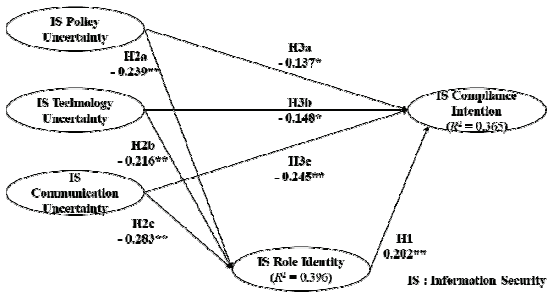

그림 2. 구조방정식 모델링의 검증 결과
Fig. 2 Results of structural equation modeling tests

표 4. 구조방정식 모델링의 검증 결과
Table 4. Results of structural equation modeling tests

	Path	Coefficient	t-value	Result
H1	RI → CI	0.202	3.159**	Support
H2a	PU → RI	-0.239	-4.031**	Support
H2b	TU → RI	-0.216	-3.117**	Support
H2c	CU → RI	-0.283	-3.779**	Support
H3a	PU → CI	-0.137	-2.187*	Support
H3b	TU → CI	-0.148	-2.039*	Support
H3c	CU → CI	-0.245	-3.055**	Support

PU(Policy Uncertainty), TU(Technology Uncertainty), CU(Communication Uncertainty), RI(Role Identity), CI(Compliance Intention)
**: $p < 0.01$

가설 1은 정보보안 역할 정체성이 확립된 조직원은 보안 준수 의도를 높인다는 것으로서, 해당 가설은 유의수준 5%를 기준으로 채택되었다(H1: β= 0.202, $p < 0.01$). 가설 2는 조직 내 정보보안 관련 불확실성 요소(정책(H2a), 기술(H2b), 커뮤니케이션(H2c))들은 조직원의 정보보안 역할 정체성 확립에 부정적 영향을 준다는 것으로, 유의수준 5%를 기준으로 세부 가설들이 채택되었다(H2a: β= -0.239, $p < 0.01$; H2b: β= -0.216, $p < 0.01$; H2c: β= -0.283, $p < 0.01$). 가설 3은 조직 내 정보보안 관련 불확실성 요소(정책(H3a), 기술(H3b), 커뮤니케이션(H3c))들은 개인들의 보안 준

수 의도 확립에 부정적 영향을 준다는 것으로, 유의수준 5%를 기준으로 세부 가설들이 채택되었다(H3a: β = −0.137, $p < 0.05$; H3b: β= −0.148, $p < 0.05$; H3c: β= −0.245, $p < 0.01$).

Ⅴ. 결 론

본 연구는 조직의 정보보안 정책, 기술, 그리고 커뮤니케이션 활동에 대한 불확실성 인식이 조직원 개개인의 보안 관련 활동에 미치는 영향을 확인하고자 하였다. 이에, 정보보안 정책, 기술, 커뮤니케이션 불확실성이 조직원의 정보보안 역할 정체성을 통해 준수 의도로 연계되는 부정적 영향을 설명하는 연구 모델을 제시하였다. 정보보안 정책 및 관련 기술을 도입하여, 업무에 적용하길 요구하는 조직의 구성원에게 설문하여, 407건의 표본을 확보하였다. 구조방정식 모델링을 통한 검정 결과, 정보보안 관련 정책, 기술, 그리고 커뮤니케이션 불확실성은 조직원의 역할 정체성에 부정적 영향을 주었으며, 나아가 보안 준수 의도까지 부정적 영향을 미쳤다.

결과의 학술적 시사점은 다음과 같다. 보안 행동 관련 선행연구가 개인들의 자발성을 높일 수 있는 조직 문화 및 환경 구축의 필요성을 중점적으로 제시했다면, 본 연구는 개인의 준수 행동을 축소하는 조직원인을 제시하고 결과를 확인한 측면에서 차별성과 학술적 시사점을 가진다. 세부적으로 불확실성 관점에서 개인이 정보보안 환경에서 느낄 수 있는 불확실성 요소를 정책, 기술, 그리고 커뮤니케이션 관점에서 제시한 측면에서 선행연구로서 의미가 있다. 또한, 단순히 보안 준수에 영향을 미치는 부정적 요소가 아닌, 보안 준수 행동을 강화할 수 있는 역할 정체성 인식 요소까지 부정적 영향을 미치는 요소임을 밝혔다는 측면에서 연구의 의미가 있다. 또한, 결과의 실무적 시사점은 다음과 같다. 조직이 내부자의 보안 수준을 달성하기 위해 구축 및 제공해야 할 기본 요소(정책, 기술 등)가 조직원에게 충분히 전달되지 않을 수 있음을 고려해야 함을 제시한다. 즉, 조직이 제공한 보안 관련 정보가 불확실하다고 인식될 때, 조직원은 오히려 보안 준수 행동을 줄이는 경향이 있음이 확인되었다. 따라서, 조직은 정보보안 정책, 기술 관련 정보가 충분히 커뮤니케이션될 수 있도록 시스템을 구조화하고, 지속해서 조직원이 해당 정보들을 이해하고 활용할 수 있는 수준을 달성했는지를 확인하는 노력이 요구된다.

본 연구는 보안 환경에 대한 불확실성 요소를 다각적으로 제시한 측면에서 시사점을 가지나, 조직원 개인이 불확실성을 인식할 때 받아들이는 감정 또는 대처의 차이 등의 개인 특성 요인, 제조업 또는 금융업 등과 같이 정보에 대한 관심 차이가 있는 업종에서의 영향 관계 등을 확인하지 못했다. 따라서, 향후 연구에서는 개인 또는 기업의 특성 요인을 종합적으로 고려하여 영향 관계를 확인할 필요가 있다.

References

[1] 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, 2018, pp. 282-293.

[2] Fortune Business Insights, “The global cyber security market size is projected to grow from $172.32 billion in 2023 to $424.97 billion in 2030, at a CAGR of 13.8%,” *Report*, Apr. 2023.

[3] Verizon, “2021 data breach investigations report,” *Report,* Dec. 2021.

[4] Y. Chen, K. Ramamurthy, and K. W. Wen, “Organizations’ information security policy compliance: Stick or carrot approach?,” *J. of Management Information Systems*, vol. 29, no. 3, 2012, pp. 157-188.

[5] 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, 2021, pp. 101572.

[6] P. Ifinedo, “Exploring personal and environmental factors that can reduce nonmalicious information security violations,” *Information Systems Management*, vol. 40, no. 4, 2023, pp. 1-21.

[7] M. Tarafdar, Q. Tu, B. S. Ragu-Nathan, and T. S. Ragu-Nathan, “The impact of technostress on role stress and productivity,” *J. of Management*

Information Systems, vol. 24, no. 1, 2007, pp. 301-328.
[8] Z. Adahman, Z. W. Malik and Z. Anwar, "An analysis of zero-trust architecture and its cost-effectiveness for organizational security," *Computers & Security*, vol. 122, 2022, pp. 102911.
[9] Korea Information Security Industry Association, "2021 survey on information security," *Report*, Jan. 2022.
[10] I. Hwang, "The influence of competitive psychological climate and IS related anxiety: The role of IS related value dissimilarity," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 18, no. 4, 2023, pp. 649-660.
[11] M. Ma and R. Agarwal, "Through a glass darkly: Information technology design, identity verification, and knowledge contribution in online communities," *Information Systems Research*, vol. 18, no. 1, 2007, pp. 42-67.
[12] S. M. Farmer, P. Tierney, and K. Kung-McIntyre, "Employee creativity in Taiwan: An application of role identity theory," *Academy of Management J.*, vol. 46, no. 5, 2003, pp. 618-630.
[13] I. Hwang, "Reinforcement of IS voice behavior within the organization: A perspective on mitigating role stress through organization justice and individual social-identity," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 17, no. 4, 2022, pp. 649-662.
[14] O. Ogbanufe, "Enhancing end-user roles in information security: Exploring the setting, situation, and identity," *Computers & Security*, vol. 108, 2021, pp. 102340.
[15] P. A. Pavlou, H. Liang, and Y. Xue, "Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective," *MIS Quarterly*, vol. 31, no. 1, 2007, pp. 105-136.
[16] I. Hwang, "The influence on the information security techno-stress on security policy resistance through strain: Focusing on the moderation of task technology fit," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 16, no. 5, 2021, pp. 931-939.
[17] A. Vedadi, M. Warkentin, and A. Dennis, "Herd behavior in information security decision-making," *Information & Management*, vol. 58, no. 8, 2021, pp. 103526.
[18] H. Chen, M. Liu, and T. Lyu, "Understanding employees' information security‐related stress and policy compliance intention: The roles of information security fatigue and psychological capital," *Information and Computer Security*, vol. 30, no. 5, 2022, pp. 751-770.
[19] I. Jo and J. Jo, "Differentiation of uncertainty and ambiguity in communication within the organization: On Antecedent Variables and Influences of Uncertainty and Ambiguity," *J. of Communication Research*, vol. 49, no. 1, 2012, pp. 220-258.
[20] J. D'Arcy and P. L. Teh, "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization," *Information & Management*, vol. 56, no. 7, 2019, pp. 103151.
[21] J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding employee responses to stressful information security requirements: A coping perspective," *J. of Management Information Systems*, vol. 31, no. 2, 2014, pp. 285-318.
[22] J. C. Nunnally, *Psychometric theory (2nd ed.)*. New York: McGraw-Hill, 1978.
[23] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. of Marketing Research*, vol. 18, no. 1, 1981, pp. 39-50.

저자 소개

황인호(In-Ho Hwang)

2007년 중앙대학교 대학원 졸업 (경영학석사)
2014년 중앙대학교 대학원 졸업 졸업(경영학 박사)
2018년 한국산업기술대학교 연구교수
2020년 ~현재 국민대학교 교양대학 조교수
※ 관심분야 : IT 핵심성공요인(IT CSF), 디지털 콘텐츠(Digital Content), 정보보안(Information Security), 프라이버시(Privacy) 등