Regular paper | Journal of the KIECS. pp. 165-176, vol. 18, no. 1, Feb. 28. 2023, t. 117, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2023.18.1.165

정보보안 기술 및 커뮤니케이션 불확실성이 제언 행동에 미치는 영향: 개인의 정보 영향 민감성의 역할

황인호*

The Influence of IS Technology and Communication Uncertainty on IS Voice Behavior: The Role of Susceptibility to Informational Influence of Employee

In-Ho Hwang*

요 약

조직 내부의 정보 노출 위협에 대한 관리가 조직 전체의 정보보안 목표 달성에 기여할 수 있음이 밝혀지면서, 조직들은 내부자에 적용되는 정보보안 정책을 엄격하게 구축하고, 보안 시스템에 대한 투자를 높이고 있다. 하지만, 정보보안 사고는 한 명의 고의적인 정보 노출에 의해서도 조직에 피해를 주므로, 심리적 측면에서 내부자의 정보보안 준수 행동 강화를 위한 노력을 하는 것이 요구된다. 본 연구는 정보보안에 대한 불확실한 조직 환경이 어떻게 개인의 정보보안 관련 행동에 영향을 주는지를 확인하는 것을 목적으로 한다. 연구는 정보보안 정책 구축 및 활용하는 조직의 내부자를 대상으로 설문하였으며, 440개의 표본을 활용하여 가설을 검증하였다. 검증 결과, 정보보안 기술 및 커뮤니케이션 불확실성이 정보보안 예상 불안을 통해 정보보안 제언 행동을 감소시켰으며, 개인의 정보 영향 민감성이 정보보안 기술, 커뮤니케이션, 그리고 예상 불안에 의해 변화되는 제언 행동을 조절하였다. 연구의 결과는 실무적으로 불확실한 정보보안 환경의 보완 필요성과 개선 방향을 제시한다.

ABSTRACT

As the reduction of information exposure threats by organization insiders contributes to achieving information security(IS) goals, organizations are establishing strict IS policies applicable to insiders and increasing investment in IS systems. However, since IS incidents cause damage to an organization even by malicious information exposure by one person, psychological support for strengthening IS compliance behavior by insiders. This study aims to confirm how the uncertain organizational environment related to IS affects individual IS-related behavior. We surveyed insiders of organizations operating IS policies and tested the hypothesis using 440 samples. As a result, IS technology and communication uncertainty reduced IS voice behavior through IS prospective anxiety, and individuals' susceptibility to information influence moderated the relationship between IS technology, communication, and prospective anxiety and IS voice behavior. Our results suggest the necessity and direction of supplementing the uncertain IS environment in practice.

키워드

Voice Behavior, Technology Uncertainty, Communication Uncertainty, Prospective Anxiety, Susceptibility to Informational Influence

제언 행동, 기술 불확실성, 커뮤니케이션 불확실성, 예상 불안, 정보 영향 민감성

* 교신저자: 국민대학교 교양대학
• 접 수 일 : 2022. 11. 23
• 수정완료일 : 2023. 01. 02
• 게재확정일 : 2023. 02. 17
• Received : Nov. 23, 2022, Revised : Jan. 02, 2023, Accepted : Feb. 17, 2023
• Corresponding Author : In-Ho Hwang
College of General Education, Kookmin University,
Email : hwanginho@kookmin.ac.kr

Ⅰ. 서 론

조직 내부자 중심의 정보 노출 위협 가능성에 대한 사회적 관심이 높아지면서, 공공기관들을 중심으로 내부자에 대한 정보 운용 및 통제 체계를 처음부터 다시 검토하는 노력을 하고 있다. 대표적으로 미국은 2021년 “제로 트러스트 아키텍처(Zero Trust Architecture)” 정책을 반영하고 있다. 특히, 정부 기관과 연계된 민간 기업까지 기본으로 돌아가, 조직 내부자에 대한 정보 통제 체계가 외부자에 대한 정보 통제 체계 수준까지 이루어지도록 정보보안 체계를 운용하도록 강제하고 있다[1]. 하지만, 아직 조직원, 파트너사와 같이 사람에 의한 정보 노출 사고는 세계적으로 지속해서 발생하고 있으며, 전체 정보보안 사고의 약 30%에 달하는 것으로 나타나고 있다[2]. 사람을 통해 발생하는 정보 노출 사고는 악의적 관점에서 정보 노출을 통해 이익을 얻는 사례도 있으나, 비의도적으로 정보 노출 사건을 일으켜 조직에 피해를 발생시키는 사례도 빈번한 것으로 나타나고 있다[2]. 즉, 내부자가 업무 과정에서 발생하는 정보보안 관련 행동에 대한 조직 차원의 명시적인 정보 제공을 통해, 정보보안 필요성과 절차를 명료하게 판단하도록 지원하는 것이 요구되고 있다. 실제로, West[2008]는 정보보안 활동에 대한 행동 정보는 조직보다 조직원이 언제나 더욱 많이 보유하고 있으므로, 조직원 스스로 정보보안 활동을 할 수 있도록 심리적 지원의 필요성을 강조하였으며[3], 관련 선행연구가 내부자의 정보보안 준수 행동 강화를 위해서는 긍정적인 행동 동기가 필요하며, 동기 개선을 위한 조직 내 정보보안 문화 등 선제적으로 정보보안 환경 구축의 필요성을 제시해왔다[4-6]. 최근에는 조직원이 정보보안 준수를 위해서는 정보 확보, 학습 등과 같은 추가적인 노력과 시간이 필요하므로, 정보보안 활동이 조직원과 조직 간에 초기 계약 시 수립했던 본연의 업무 목표 달성에 부담감을 주는 요인으로 작용할 수 있음을 지적하면서, 조직원의 미준수 원인이 엄격하고 변화하는 정보보안 정책과 규범 등에 있음을 밝히는 연구도 제시되고 있다[7-9]. 선행연구는 조직원의 정보보안 준수 또는 미준수 행동의 원인을 설명했다는 측면에서 시사점을 가진다. 특히, 그들은 조직과 조직원의 관계에서 조직원의 정보보안 준수를 위한 조직 환경, 문화 구축이 무엇보다 중요함을 제시하고, 자연스럽게 조직원이 정보보안 준수 동기를 구축하도록 지원하는 것이 중요함을 제언하였다. 하지만, 최근 활발하게 이루어지고 있는 정보보안 미준수 행동 원인 관련 연구는 정보보안이 스트레스를 일으킬 수 있음을 확인함에 그쳐, 개인을 둘러싼 조직 업무 환경 중 정보보안 관련 스트레스를 일으키는 세부 조건이 무엇인지를 밝히는 연구는 부족한 상황이다.

본 연구는 개인의 정보보안 활동과 관련된 정보 부족이 정보보안 행동에 부정적 영향을 일으킬 것으로 판단하고, 정보 부족과 관련된 정보보안 환경 불확실성 요소를 탐색적으로 살펴보고자 한다. 즉, 연구는 조직원이 조직의 정보보안 정책, 규칙, 기술을 본인 업무에 반영할 때, 부족한 정보 수준에 의해 형성된 불확실성 조건이 중요한 미준수 행동 원인이라고 판단한다. 이에, 연구는 조직원이 불확실하다고 판단할 수 있는 정보보안 환경 요인을 기술, 커뮤니케이션 관점에서 제시하고, 불확실성이 정보보안 걱정 형성을 통해 조직을 위해 이타적으로 행동하는 개념인 제언 행동에 부정적 영향을 일으킬 수 있음을 확인하고자 한다. 또한, 개인은 동료들과 다양한 상호작용을 하면서 그들과 사회성을 유지하고자 하는데, 주변에서 제공하는 정보를 받아들이고 활용하는 수준의 차이가 존재할 것으로 판단하고 정보 영향 민감성이 불확실성의 영향 조건을 조절하는지 확인하고자 한다. 본 연구의 결과는 정보보안 미준수에 대한 조직 환경 요소와 개인의 성향 조건을 밝히고 조직원의 정보보안 관련 활동에 영향을 줄 수 있음을 확인함으로써, 조직 내부자의 정보보안 미준수 행동을 최소화하기 위한 조직 전략적 방향을 제언한다.

Ⅱ. 이론적 배경

2.1 정보보안 제언 행동

2021년 기준 국내 조직들의 정보보안 현황을 살펴보면, 응답 조직의 89.9%가 체계적인 정보보안 관리의 필요성을 인지하고 있으나, 현실적으로 정보보호 정책을 보유한 조직은 응답 기업의 27.0%에 불과하고, 실제 정보 침해사고 발생 시 72.3%의 조직이 해당 문제 또는 추가적 해결을 위해 별다른 움직임을

보이지 않은 것으로 나타났다[10]. 즉, 국내 조직들은 정보보호에 대한 중요성을 인지하나, 이슈 해결과 관련된 관심은 상대적으로 저조한 상태이다. 반면, 미국 등 선진국은 국가 차원에서 국가와 연계된 글로벌 조직들의 정보 노출에 대한 체계적 관리를 요구하는 상황이므로[1], 앞으로 정보보안과 관련된 조직 차원의 정책 및 기술적 구축, 그리고 조직원 관리가 요구된다. 특히, 사람에 의해 발생할 수 있는 정보 노출은 시간, 장소와 무관하게 정보시스템 접근 가능성 수준에 따라 다르게 발생할 수 있으므로, 구성원 모두가 자발적인 정보관리 활동을 할 수 있도록 조직 차원의 지원 전략 수립이 요구된다[11].

이에, 본 연구는 조직 내 구성원들의 자발적인 정보보안 준수 문화를 구축하기 위해서는 구성원들의 이타적이고 능동적인 참여가 무엇보다 중요하다고 판단하였다. 이에, 연구는 본인에게 주어진 정보보안 요구사항에 대한 행동 준수를 넘어, 동료들에게 보안 관련 도움을 주고 이타적으로 보안 활동의 필요성을 개진하도록 돕는 행동인 제언 행동(Voice Behavior)을 연구에 반영하고자 한다. 제언 행동은 개인이 특정 환경에서 본인과 집단의 목표 및 성과 창출을 위해 건설적으로 대상 문제에 대한 의견을 제시하는 행동을 지칭한다[12]. 특히, 긍정적 상황에 대한 독려 행동뿐 아니라, 부정적 상황에서 문제점 개선을 위한 의견 개진과 같은 행동을 포함하기 때문에[13], 정보보안과 같이 미준수 행동이 발생 시, 조직 전체의 손실을 발생할 수 있는 조건에서 제언 행동의 필요성은 높아질 수 있다[14]. 따라서, 개인들의 정보보안 제언 행동을 감소시키는 심리적 조건들을 확인함으로써, 역설적으로 정보보안 제언 행동 강화 방안을 제언하고자 한다.

2.2 정보보안 예상 불안

조직에서 사람들은 조직 내 환경, 분위기, 동료 등 자신을 둘러싼 외적 조건의 변화에 대하여 본인이 가지고 있는 역량을 활용하여 대처하여 안정적 상황을 유지하고자 하는 속성을 가진다[15]. 특히, 조직 내 새로운 기술, 정책, 규정 등이 도입될 경우, 개인은 기존 경험 등에서 확보한 정보 등을 활용하여 발생할 수 있는 이슈를 선제적으로 해결하고 변화에 적응하고자 한다. 하지만, 개인에게 주어진 정보, 역량 등의 부족은 대상에 대한 행동 결과를 명확하게 예측하지 못하게 할 수 있다[16]. 즉, 개인은 불안감을 형성할 수 있는데, 불안(Anxiety)은 미래의 특정 시점에 발생할 수 있는 잠재적 위협에 대한 반응을 의미한다[17]. 불안감은 복잡한 환경에서 발현될 수 있는데, 복합적으로 형성되어 높은 불안감이 형성될 경우, 대상에 대한 두려움, 신체적 약화 등의 문제로 이어질 수 있으며, 나아가 부정적 행동 의도를 가지도록 한다[16]. 특히, 불안감은 아직 발생하지 않았으나 발생할 수 있는 우려로서 형성되기도 한다. Carleton et al.[2007]은 발생하지 않았으나 두려움 등을 일으킬 가능성이 존재한다는 관점에서 예상 불안(Prospective Anxiety) 개념을 제시하였다[17].

정보보안과 관련하여 불안감은 특정 업무가 이루어진 이후에 발생할 수 있다. 현재 많은 조직이 조직원의 정보보안 준수 여부를 특정 이슈가 발생한 이후 결과를 통해 실행하고 있으며, 준수 행동에 대한 보상보다는 미준수 행동에 대한 처벌을 중심으로 운용하고 있다. 특히, 조직들은 급변하는 외부 환경에 빠르게 대응하기 위해 관련 기술 또는 규정을 지속해서 변화시키는 상황이다[3, 18]. 즉, 정보보안 준수 여부는 개인의 업무 수행 결과에 대한 조직의 판단으로 결정되고 처벌 중심의 정책으로 운용되며 업무 환경은 빠르게 변화하기 때문에, 조직원에게 정보보안 문제는 언제든 자신에게 불리한 상황을 일으킬 수 있는 이슈로 반응할 수 있다. 따라서 정보보안 활동은 개인에게 아직 일어나지 않았으나 향후 발생할 수 있는 불안 요소로 작용할 수 있으며, 본 연구는 예상 불안을 정보보안에 반영한다.

조직에서 특정 환경 또는 대상에 대한 개인의 불안감이 형성될 경우, 대상에 대한 행동을 회피하려는 모습을 보인다. Hwang et al.[2017]은 정보보안 정책 준수에 대한 걱정이 발생할 경우, 구성원들은 보안 관련 행동 결과를 숨기려는 행태를 가질 수 있음을 확인하였으며[18], Siponen and Vance[2010]는 정보의 불균형으로 인한 조직원의 정보보안 정책에 대한 불안감의 형성은 정보보안 미준수 행동으로 이어질 수 있음을 밝혔다[19]. 즉, 정보보안 활동과 관련된 예상되는 불안감은 준수 행동을 감소시키는 조건이다. 본 연구는 불안감이 능동적으로 의견을 제시하는 개념인 제언 행동에도 부정적 영향을 줄 것으로 판단하고, 예상 불안과 제언 행동 사이에 다음 가설을 제시한다.

H1. 정보보안 예상 불안은 정보보안 관련 제언 행동에 부정적 영향을 준다.

2.3 불확실성

불확실성은 특정 환경, 상황 등에 대한 과도한 걱정, 상태 불안과 같은 인식을 형성하는 조건으로, 대상 환경에서 본인에게 부정적인 사건을 일으킬 수 있다고 판단되는 조건을 의미한다[20]. 특정 환경에 대한 불확실성을 용납하지 않는 사람의 경우 불확실성과 관련된 모호한 정보적 상황 등 외부 환경 요소를 위협적인 요소로 인식하고 육체적으로 스트레스 반응을 일으킬 수 있으며[7], 나아가 불확실성을 최소화하기 위해 대상과 관련된 행동을 실행하지 않고 모호하게 회피하려는 행동을 보이기도 한다[17].

특히, 정보보안 정책 및 기술 등의 도입은 조직원에게 조건별 불확실성을 높게 인식시킬 수 있는데, 조직이 정보보안을 위해 도입한 특정한 시스템 등 환경적 조건이 개인이 보유한 역량(지식, 경험 등)을 넘어서거나, 제대로 관련 정보를 확보하지 못하는 환경이 지속하고 있다고 판단할 때, 행동에 대한 걱정 등을 유발할 수 있다[9]. 본 연구는 정보보안 불확실성 조건으로 기술 불확실성과 커뮤니케이션 불확실성을 제시하며, 불확실성 요소들이 개인의 심리적 불안감을 형성하여 어떻게 정보보안과 관련된 행동을 감소하는지를 확인하고자 한다.

2.3.1 정보보안 기술 불확실성

기술 불확실성은 조직 내 특정 목적을 위해 도입된 기술이 지속해서 변화되는 상황을 의미한다[19]. 정보보안과 관련하여 기술 불확실성은 조직원에게 높게 인식될 수 있다. 조직은 외부 침입으로부터 정보자원을 보호하기 위해, 지속해서 높은 수준의 보안 기술을 적용하고자 한다. 반면, 조직원은 자신의 역량 이상의 기술적 이해를 요구받게 된다고 판단할 때 기술에 대한 불확실성을 일으킬 수 있다[21]. 예를 들어, 스마트워크와 같은 미래면 업무 체계의 증가는 조직의 정보자산 보호를 위해 새로운 기술의 도입과 업무 표준, 규칙 등을 변화시키게 된다. 더불어, 정보자원 보호를 위해 조직은 현재보다 엄격한 정보보안 정책과 기술 수준을 적용할 가능성이 존재한다. 조직원은 스마트워크 업무를 통한 효율적 성과 달성과 정보보호를 위해 기대 이상의 지식 확보 활동을 수행해야 한다. 즉, 정보보안 수준 강화를 위한 조직의 노력은 조직원에게 관련 기술에 대한 불확실성을 야기할 수 있다[22].

기술 환경의 변화로 인한 불확실성 인식이 증가할 경우, 개인은 정보보안 관련 행동을 회피하거나 미준수 행동을 일으킬 가능성이 있다. Jena[2015]는 불확실성을 포함한 기술 스트레스의 형성은 개인의 관련 기술에 대한 불만족을 일으키고 기술 관련 성과 달성에 부정적 영향을 준다고 하였으며[23], Tarafdar et al.[2007]은 조직 내 기술 불확실성 등 변화로 인한 기술 스트레스 환경은 업무 스트레스를 일으켜 개인의 생산성에 문제를 일으킬 수 있다고 하였다. Hwang and Cha[2018]는 정보보안 분야에 기술 스트레스 상황은 조직몰입과 준수 의도를 감소시킬 수 있음을 확인하였다[9].

또한, 기술 불확실성은 개인의 심리적 감정을 감소시켜 부정적 행동으로 이어지도록 한다. D'Arcy and Teh[2019]는 불확실성 등 보안 관련 스트레스 상황이 지속할 경우, 개인에게 피로, 좌절 등과 같은 정신적 상태를 일으켜 개인에게 부정적 영향을 준다고 하였으며[8], D'Arcy et al.[2014]은 정보보안 불확실성, 복잡성, 과부하 상황은 개인의 도덕적 이탈 심리를 형성하여 정보보안 회피 의도를 일으킨다고 하였다[7]. 즉, 정보보안 관련 기술에 대한 불확실성의 증가는 부정적 심리 상황을 일으키고, 정보보안에 대한 부정적 의도를 형성할 수 있다. 본 연구는 기술 불확실성, 예상 불안, 그리고 제언 행동 간에도 동일한 관점이 형성될 것으로 판단하고 가설을 제시한다.

H2a. 정보보안 기술 불확실성은 정보보안 관련 제언 행동에 부정적 영향을 준다.

H2b. 정보보안 기술 불확실성은 정보보안 예상 불안에 긍정적 영향을 준다.

2.3.2 정보보안 커뮤니케이션 불확실성

커뮤니케이션(Communication)은 이해관계자들이 상호 간에 다양한 지식, 정보 등과 같은 가치 자원들을 인식하고 이해할 수 있도록 돕는 역할을 하는 것으로[24], 조직 내 커뮤니케이션은 조직이 보유한 가치, 목표와 같은 중장기적 계획에서부터, 업무 생산성 향상에 필요한 현실적 정보, 경험과 같은 무형의 지식 등을 확보하도록 돕는 기능을 한다[25]. 즉, 커뮤니케

이션은 상호 이해하고 가치를 확보에 필요한 지식 자원을 제공하는 수준을 의미한다. 조직은 공식적으로 조직원이 정보를 교류할 수 있도록 커뮤니케이션 도구를 제공하고 있으며, 최근에는 스마트워크 등 변화하는 업무구조에 맞추어 커뮤니케이션 채널을 다양하게 제공하고 있다[26]. 정보보안과 관련하여 커뮤니케이션은 조직의 정보보안 정책의 목적과 정보관리의 가치가 무엇인지 조직 구성원에게 제공하는 역할을 하며, 실질적 정보보안 행동을 위해 필요한 정보를 교류하고 응원하는 역할을 한다[4]. 따라서, 공식적인 정보보안 커뮤니케이션 지원은 조직원의 정보보안에 대한 활동 참여를 높일 수 있다[27].

반면, 커뮤니케이션 불확실성은 커뮤니케이션 상황에서 개인이 대처할 수 있는 정보를 충분히 받지 못하는 상태를 의미한다[28]. 즉, 커뮤니케이션 불확실성은 정보 취득을 위한 커뮤니케이션을 추가로 필요한 상황임을 의미한다. 정보보안과 관련하여 커뮤니케이션 불확실성은 정보보안 활동 관련 필요 정보를 충분히 받지 못하는 상황을 말하므로, 조직원은 행동에 대한 예측 불가능성을 가질 가능성이 존재한다.

커뮤니케이션은 이해관계자에게 요구되는 활동에 대한 정확한 정보를 제공하는 것을 의미하기 때문에, 행동 가능성을 높인다. 공식적 커뮤니케이션과 관련하여 Jiménez-Castillo and Sánchez-Pérez[2013]는 조직원이 대상에 대한 가치와 목표를 이해하도록 돕는 조건이기 때문에, 조직 차원의 커뮤니케이션 전략 수립의 중요성을 제시하였다[26]. 또한, Solomon and Brown[2021]은 정보보안 정책 및 행동 방법에 대한 커뮤니케이션 채널의 제공은 정보보안 관련 행동을 높이는 조직 전략 조건이라고 하였으며[4], Barlow et al.[2018]은 정보보안을 위한 조직 차원의 커뮤니케이션 제공은 구성원의 보안 준수 행동을 강화하는 요인이라고 하였다[27]. 반대로, Jo and Jo[2012]는 커뮤니케이션 불확실성은 조직원의 직업 만족도와 구성원에 대한 신뢰도를 감소시키는 조건이라고 하였다[28]. 즉, 커뮤니케이션 확실성은 개인의 특정 행동과 밀접한 상관관계를 가진다. 본 연구는 정보보안 관련 커뮤니케이션 불확실성이 강화될수록 행동에 대한 불안감을 형성하고, 부정적 행동으로 이어질 것으로 판단하고, 커뮤니케이션 불확실성, 예상 불안, 그리고 제언 행동 간의 관계성을 확인하기 위한 가설을 제시한다.

H3a. 정보보안 커뮤니케이션 불확실성은 정보보안 관련 제언 행동에 부정적 영향을 준다.

H3b. 정보보안 커뮤니케이션 불확실성은 정보보안 예상 불안에 긍정적 영향을 준다.

2.4 정보 영향 민감성

조직 구성원들은 개인적 경험 또는 성과 달성 등의 다양한 목적달성을 위하여, 다른 동료들과 상호작용하여 정보를 확보하는 노력을 한다[29]. 하지만, 사람들이 확보한 정보를 받아들여 행동으로 옮기는 수준은 차이가 존재한다[30]. 즉, 사람들은 주변과의 상호작용을 통해 확보한 정보에 대하여 받아들여 행동으로 옮기고자 하는 인식의 차이가 있다. 정보 영향 민감성(Susceptibility to Informational Influence)은 대인 간 상호작용에서 확보한 정보에 대한 개인이 반응하는 수준으로서[29], 정보 영향 민감성이 높은 개인은 상호작용을 통해 정보 확보를 높이고자 하며, 깊은 수준으로 인식하여 행동으로 옮기거나, 다른 사람들에게 인정받고자 하는 욕구가 강하게 나타난다[30].

정보보안과 관련하여 다른 사람들의 행동을 모방하는 것은 정보보안 정책을 이해하고, 요구사항에 대하여 정확하게 행동하도록 돕는다[6]. 즉, 조직 내 동료들의 정보보안 관련 행동과 유사한 행동을 보임으로써, 타인에 대한 부정적 평가를 최소화하고자 하는 경향을 보인다[31]. 반대 맥락에서, 본 연구에서 제시한 정보보안 커뮤니케이션과 기술 불확실성에 의해 발현된 정보보안 행동에 대한 걱정은 조직 내 동료와 조직 구조에서 정보보안 준수를 감소시키는 조건으로 인식될 것으로 판단한다. 즉, 정보 영향 민감성이 높은 사람은 주변 동료들의 인식과 인정을 중요하게 판단하기 때문에, 주변에서 정보보안에 대한 준수 활동이 부족하다고 판단할 경우 미준수 행동으로 이어질 가능성이 클 것으로 판단한다. 따라서, 본 연구는 정보 영향 민감성 수준에 따라, 정보보안 기술 불확실성, 커뮤니케이션 불확실성, 예상 불안이 정보보안 제언 행동에 미치는 영향을 조절할 것으로 판단하며, 탐색적으로 영향 관계가 존재하는지를 확인하고자 하며, 다음의 연구가설을 제시한다.

H4a. 정보 영향 민감성은 예상 불안과 제언 행동 간의 관계에 조절 효과를 가진다.

H4b. 정보 영향 민감성은 기술 불확실성과 제언

행동 간의 관계에 조절 효과를 가진다.

H4c. 정보 영향 민감성은 커뮤니케이션 불확실성과 제언 행동 간의 관계에 조절 효과를 가진다.

III. 연구모델 및 측정

3.1 연구모델

본 연구는 정보보안 관련 불확실성 요소가 조직원의 예상 걱정 발현을 통해, 능동적이고 이타적으로 의견을 제시하는 개념인 제언 행동을 감소시키고, 개인이 받아들인 정보에 대한 민감성 수준에 따라 조절할 것으로 판단하며, 선행연구를 통해 그림 1과 같은 연구모델을 제시한다.

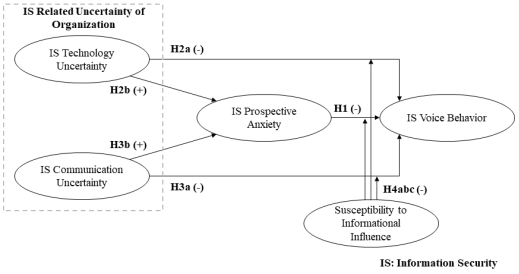

그림 1. 연구모델
Fig. 1 Research Model

3.2 측정 도구

연구 대상은 정보보안 정책을 운용하고 있는 기업에서 근무하고 있는 근로자들이다. 연구가설 검증은 선행연구를 통해 확보한 다항목 기반의 설문을 기반으로 요인별 설문 측정을 하여, 연구모델에서 제시한 요인 간의 관계에 대한 정량적 분석을 하고자 한다. 본 연구는 연구모델에 적용된 5개 요인별 선행연구 기반의 설문 문항을 다항목으로 도출하였으며, 정보보안 특성에 맞게 변경하고 7점 리커트 척도를 적용하여 설문에 활용하였다.

정보보안 기술 불확실성은 Tarafdar et al. [2007] 연구에서 4개 문항을 확보하였으며[20], “정보보안 기술에 대하여 충분히 이해하지 못하고 있음”, “새로운 기술 이해에 시간이 필요”, “정보보안 기술 학습에 필요한 시간 부족”, “정보보안 기술을 잘 알고 있는 다른 직원을 종종 찾음”으로 적용하였다. 정보보안 커뮤니케이션 불확실성은 Jo and Jo [2012] 연구에서 4개 문항을 확보하였으며[28], “정보보안 관련 메시지를 받을 때, 정보를 잘 받았다고 느끼지 못함”, “조직으로부터 받은 정보보안 메시지가 불충분하다고 느낌”, “받은 정보보안 메시지가 불명확하다고 느낌”, “조직으로부터 받은 정보보안 메시지에 대한 반응을 판단하기 어려움”으로 적용하였다. 정보보안 예상 불안은 Carleton et al. [2007] 연구에서 4개 문항을 확보하였으며[17], “필요한 모든 정보보안 정보가 없다는 것은 나를 좌절시킴”, “정보보안 준수 계획을 잘 세웠더라도 예상치 못한 작은 사건이 모든 것을 망칠 수 있음”, “언제나 정보보안 행동 결과를 예측할 수 있길 바람”, “예상치 못한 정보보안 사고는 나를 당황시킴”으로 적용하였다. 정보보안 제언 행동은 Svendsen and Joensson [2016] 연구의 3개 문항을 확보하였으며[12], “우리 조직의 정보보안을 위하여 의견을 제시함”, “ 우리 조직의 정보보안에 영향을 미치는 문제에 대하여 직원들이 참여하도록 노력함”, “조직의 정보보안 정책에 대한 변경사항에 대한 아이디어를 제시함”으로 적용하였다. 정보 영향 민감성은 Yazdanmehr et al. [2020] 연구에서 4개 문항을 확보하였으며[29], “정보보안 정책을 올바르게 따르기 위해 종종 다른 사람들의 행동을 관찰함”, “종종 정보보안 정책을 준수하는 올바른 방법을 선택하는데 도움을 주기 위해 다른 사람들과 상의함”, “내 행동이 정보보안 정책을 위반하는지 불확실할 때 동료들에게 종종 이에 대해 질문함”, “특정 정보보안 정책을 어떻게 준수해야 할지 모를 때, 친한 동료에게 물어봄”으로 적용하였다.

3.3 측정 대상 및 표본 특성

본 연구에서 선정된 연구 대상에 맞는 표본을 확보하기 위하여, M리서치 기업이 보유한 회원 집단 중 직장인 그룹에 대하여 설문을 구조화하고 온라인 설문을 수행하였다. 온라인 설문 설계 시, 회원들에게 직장인 여부, 정보보안 정책의 업무 적용 여부를 사전에 확인하였으며, 대상에 맞는 사람들만 설문에 참여하도록 하였다. 또한, 연구에서 확보한 표본과 통계적 결과에 대한 활용 방법, 목적을 사전에 제공하고 이를 허가한 사람들만 본 설문에 참여하도록 하였다. 총 유효 표본 440개를 확보하였으며, 반영된 표본이 보유한 특성은 표 1과 같다.

표 1. 표본의 특성
Table 1. Characteristics of Samples

Categories		Frequency	%
Gender	Male	218	49.5
	Female	222	50.5
Age	Under 30	102	23.2
	31 - 40	102	23.2
	41 - 50	114	25.9
	Over 51	122	27.7
Industry	Manufacturing	126	28.6
	Service	314	71.4
Job Position	Staff	183	41.6
	Assistant Manager	101	23.0
	Manager	74	16.8
	Over Manager	82	18.6
Firm Size	Under 10	27	6.1
	10~49	113	25.7
	50~299	144	32.7
	Over 300	156	35.5
Total		440	100.0

Ⅳ. 분 석

4.1 신뢰성 및 타당성

본 연구는 주 효과 분석은 구조방정식 모델링을 위한 AMOS 22.0 패키지를 활용하고, 조절 효과 분석은 Process 3.1 패키지를 활용하였다. 우선, 연구모델에 반영된 요인들은 다 항목으로 측정되었으므로, 요인별 적절하게 측정되었는지를 확인하기 위한 신뢰성 및 타당성 분석을 수행하였다.

첫째, 신뢰성은 SPSS 21.0 패캐지를 활용하되 탐색적 요인분석과 크론바흐 알파를 통해 적절성을 확인하였다. 크론바흐 알파는 요인별 0.7 이상의 값을 요구하며[32], 표 2는 신뢰성 분석에 적용된 요인 측정치와 크론바흐 알파를 보여준다. 결과적으로 모든 요인이 요구사항을 충족하여 요인에 대한 일관성 확인 요소인 신뢰성을 확보하였다. 둘째, 타당성은 AMOS 22.0 패키지를 활용하되 확인적 요인분석을 수행하고, 집중 타당성과 판별 타당성을 함께 확인하였다. 집중 타당성은 요인 구성 항목들이 요인별 일관성 및 항목적 타당성을 가지는지 확인하는 것으로 개념 신뢰도(CR)와 평균분산추출(AVE)을 구한다. 우선 확인적 요인분석 모델의 적합성을 확인하였으며, χ^2/df = 2.148, RMR = 0.048, RMSEA = 0.051, GFI = 0.931, AGFI = 0.908, NFI = 0.950, TLI = 0.967, 그리고 CFI = 0.972과 같이 나타나 적합성 요구사항을 충족하였다. 집중 타당성 관련 선행연구는 개념 신뢰도 0.7 이상, 평균분산추출 0.5 이상의 값을 개별적으로 요구한다[33]. 표 2는 집중 타당성 결과를 보여주며, 모든 요인이 집중 타당성 요구사항을 충족하였다.

표 2. 타당성 및 신뢰성
Table 2. Construct Validity and Reliability

Constructs		Factor Loading	Cronbach's Alpha	CR	AVE
TU	TU1	0.747	0.886	0.880	0.649
	TU2	0.782			
	TU3	0.808			
	TU4	0.748			
CU	CU1	0.782	0.891	0.862	0.609
	CU2	0.780			
	CU3	0.788			
	CU4	0.696			
PA	PA1	0.647	0.856	0.816	0.528
	PA2	0.812			
	PA3	0.848			
	PA4	0.803			
VB	VB1	0.787	0.910	0.889	0.727
	VB2	0.776			
	VB3	0.725			
SII	SII1	0.803	0.906	0.886	0.660
	SII2	0.834			
	SII3	0.799			
	SII4	0.724			

TU(Technology Uncertainty), CU(Communication Uncertainty), PA(Prospective Anxiety), VB(Voice Behavior), SII(Susceptibility to Informational Influence)

판별 타당성은 연구모델에 적용된 요인들이 차별성을 보유하고 있는지를 판단하는 것으로, 판별 타당성 관련 연구는 상관계수와 평균분산추출 계수를 비교하는 방법을 제안하였다[33]. 평균분산추출 계수의 제곱근 값이 요인들의 상관계수보다 클 때, 판별 타당성이 존재한다고 판단한다. 결과는 표 3과 같으며, 요구되는 수준을 충족한 것으로 나타났다.

표 3. 판별 타당성 결과
Table 3. Result for Discriminant Validity

Constructs	1	2	3	4	5
TU	**0.805[a]**				
CU	.614**	**0.781[a]**			
PA	.467**	.440**	**0.726[a]**		
VB	-.624**	-.607**	-.560**	**0.853[a]**	
SII	.592**	.557**	.482**	-.600**	**0.813[a]**

TU(Technology Uncertainty), CU(Communication Uncertainty), PA(Prospective Anxiety), VB(Voice Behavior), SII(Susceptibility to Informational Influence)
a = square root of the AVE, **: $p < 0.01$

마지막으로, 연구는 설문지 기법에서 일반적으로 발생하는 설문 측정 과정에서 발생하는 편의 문제인 공통방법편의에 대한 수준을 확인하였다. 현재 다양한 방식의 공통방법편의 측정 기법이 제시되나, 연구는 단일공통방법편의 확인 기법을 적용하였다. 본 측정 기법은 확인적 요인분석 모델에 단일 요인을 추가하고, 두 모델 내 측정치 변화량의 수준을 확인하는 것으로, 변화량이 적을수록 공통방법편의 문제가 낮다고 본다[34]. 분석 결과 두 모델의 측정치의 변화량 차이는 0.2보다 모두 작게 나타나, 공통방법편의 문제를 고려할 수준은 아닌 것으로 나타났다.

4.2 주 효과 분석

정보보안 관련 불확실성 요소가 개인의 정보보안 관련 예상 불안을 통해, 제언 행동으로 이어지는 주 효과 분석을 우선 수행하였다. 요인별 관계 검증은 구조방정식 모델링을 반영하였으며, 우선 적용 모델의 적합도를 확인하였다. 모델의 적합도는 χ^2/df = 2.065, RMR = 0.046, RMSEA = 0.049, GFI = 0.948, AGFI = 0.926, NFI = 0.962, TLI = 0.975, 그리고 CFI = 0.980으로 나타나, 모든 수치가 적합도 요구사항을 충족하였다. 이후, 연구는 구조방정식 모델링을 수행하였으며, 변수별 경로 분석을 통해 가설 채택 여부를 판단하였으며, 결과는 그림 2, 표 4와 같다.

가설 1은 정보보안 예상 불안이 정보보안 제언 행동을 감소시킨다는 것으로, 구조방정식 내 두 요인 간의 경로를 확인한 결과는 5%의 유의수준을 기준으로 채택되었다(H1: β= -0.286, $p < 0.01$). 가설 2는 정보보안 기술 불확실성이 예상 불안을 증가시키고(H2b), 정보보안 제언 행동을 감소시킨다는 것으로(H2a), 구조방정식 내 두 요인 간의 경로를 확인한 결과는 5%의 유의수준을 기준으로 채택되었다(H2a: β= -0.337, $p < 0.01$; H2b: β= 0.344, $p < 0.01$).

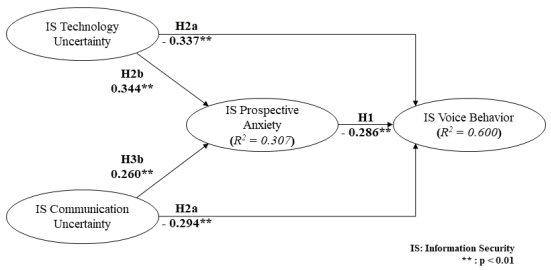

그림 2. 주 효과 (경로 분석) 결과
Fig. 2 Results of Main Effect Tests

표 4. 주 효과 (경로 분석) 결과
Table 4. Results of Main Effect Tests

	Path	Coefficient	t-value	Result
H1	PA → VB	-5.961	-0.286**	Support
H2a	TU → VB	-5.725	-0.337**	Support
H2b	TU → PA	4.805	0.344**	Support
H3a	CU → VB	-5.142	-0.294**	Support
H3b	CU → PA	3.689	0.26**	Support

TU(Technology Uncertainty), CU(Communication Uncertainty), PA(Prospective Anxiety), VB(Voice Behavior)
**: $p < 0.01$

가설 3은 정보보안 커뮤니케이션 불확실성이 예상 불안을 증가시키고(H3b), 정보보안 제언 행동을 감소시킨다는 것으로(H3a), 구조방정식 내 두 요인 간의 경로를 확인한 결과는 5%의 유의수준을 기준으로 채택되었다(H3a: β= -0.294, $p < 0.01$; H3b: β= 0.260, $p < 0.01$).

최종적으로, 독립변수가 종속변수에 미치는 영향력 수준을 확인하였다. 기술 및 커뮤니케이션 불확실성과 예상 불안은 제언 행동에 60.0%의 영향을 주었으며, 기술 및 커뮤니케이션 불확실성은 예상 불안에 30.7%의 영향을 주었다.

4.3 조절 효과 분석

개인이 보유한 정보 영향 민감성이 제언 행동 선행변수에 의한 영향을 조절할 것이라는 가설 4는 Hayes[2017]의 Process 3.1 패키지를 활용하여 분석하였다. Process 3.1 패키지에서 조절효과 분석은 모

델 1(부트스트래핑 5,000, 신뢰수준 95%)을 반영하였다. 정보 영향 민감성의 조절 효과 결과는 표 5와 같다. 가설 4a는 예상 불안과 제언 행동 간의 조절 효과 검증이고, 가설 4b는 기술 불확실성과 제언 행동, 가설 4c는 커뮤니케이션 불확실성과 제언 행동 간의 조절 효과 검증이다. 모든 관계에서 독립변수와 조절변수를 반영한 상호작용 변수의 영향이 5%의 유의수준을 기준으로 채택되었다(H4a: t= -2.033, $p < 0.05$; H4b: t= -2.780, $p < 0.01$; H4c: t= -2.956, $p < 0.01$). 정보 영향 민감성의 조절 효과 영향을 명확하게 판단하기 위하여, SPSS 21.0 패키지를 활용하여 단순 기울기 그래프를 적용하였다. 그림 3은 예상 불안과 제언 행동 간의 영향에 대한 조절 효과 검증 결과이고, 그림 4는 기술 불확실성과 제언 행동 간의 영향에 대한 조절 효과 검증 결과이고, 그림 5는 커뮤니케이션 불확실성과 제언 행동 간의 영향에 대한 조절 효과 검증 결과이다.

표 5. 조절 효과 결과
Table 5. Results of Moderating Effect Tests

		Coefficient	t-value	Result
H4a	Constant	5.336	129.920**	Support
	PA	-0.460	-9.490**	
	SII	-0.360	-7.873**	
	Interaction	-0.073	-2.033*	
	F = 132.0276, R^2 = 0.4760			
H4b	Constant	5.345	133.362**	Support
	TU	-0.415	-9.163**	
	SII	-0.383	-8.672**	
	Interaction	-0.090	-2.780**	
	F = 132.5168, R^2 = 0.4769			
H4c	Constant	5.346	133.276**	Support
	CU	-0.376	-8.965**	
	SII	-0.445	-10.586**	
	Interaction	-0.104	-2.956**	
	F = 127.0429, R^2 = 0.4664			

TU(Technology Uncertainty), CU(Communication Uncertainty), PA(Prospective Anxiety), SII(Susceptibility to Informational Influence)
*: $p < 0.05$, **: $p < 0.01$

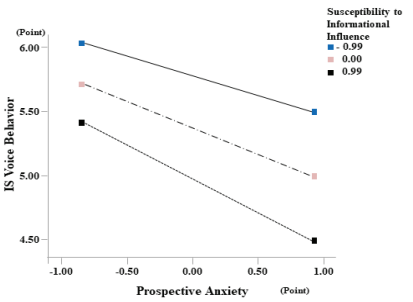

그림 3. 정보 영향 민감성 조절 효과 (H4a)
Fig. 3 Moderation Effect of SII (H4a)

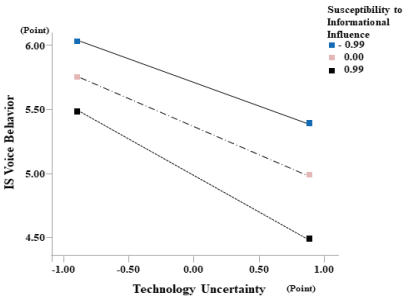

그림 4. 정보 영향 민감성 조절 효과 (H4b)
Fig. 4 Moderation Effect of SII (H4b)

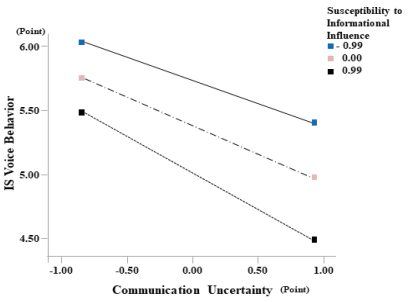

그림 5. 정보 영향 민감성 조절 효과 (H4c)
Fig. 5 Moderation Effect of SII (H4c)

V. 결 론

조직 내부자에 대한 정보 통제 등 정보보안에 대한 노력 요구가 강력해지면서, 조직들은 엄격한 정보보안 정책을 도입하고 있다. 하지만, 정보보안 준수 활동은 개인의 선택으로 인해 발생하기 때문에, 개인들의 자발적 정보보안 준수 활동을 위한 전략적 접근이 요구된다. 본 연구는 정보보안에 대한 내부자의 제언 행동

에 부정적 영향을 주는 조직 환경 요소를 확인하고, 개인의 정보 영향 민감성에 의한 영향의 차이가 존재할 수 있음을 확인하고자 하였으며, 정보보안 정책을 운용하는 조직의 구성원들을 대상으로 설문하였다. 또한, SPSS 21.0과 AMOS 22.0 패키지를 활용하여 가설을 검증하였다. 가설 검증 결과, 정보보안 기술 및 커뮤니케이션 불확실성은 개인의 정보보안 예상 불안을 통해 정보보안 제언 행동을 감소시키는 선행 조건임을 확인하였다. 또한, 개인이 보유하고 있는 정보 영향 민감성은 정보보안 기술 불확실성, 정보보안 커뮤니케이션 불확실성, 그리고 정보보안 예상 불안이 제언 행동에 미치는 영향을 조절하였다.

본 연구를 통한 시사점은 다음과 같다. 첫째, 본 연구는 정보보안 관련 개인의 행동에 있어, 본인에게 주어진 정보보안 관련 행동 이외 추가로 주변 동료 및 조직에 정보보안 관련 의견을 적극적으로 개진하는 개념인 제언 행동을 적용하고 행동 원인을 확인하였다. 즉, 본 연구는 정보보안 관련 행동 연구에서 결과변수를 다양화한 측면에서 학술적 시사점을 가지며, 조직 내부의 자발적이고 이타적인 의견 개진 행동을 감소시키는 원인 요소를 제시한 관점에서, 실무적으로 조직의 내부 정보보안 전략 수립 방향성에 기여한다.

둘째, 본 연구는 정보보안 정보 부족 등의 이유로 발생할 수 있는 심리적 불안을 세밀하게 접근하여, 정보보안 미준수 행동에 대한 불안정한 미래 예측으로 인한 불안감 요소인 예상 불안을 반영하였다. 즉, 본 연구는 정보보안에 대한 처벌은 밝혀진 결과를 통해 결정되므로, 현재에 대한 문제보다는 미래에 불안한 예상에서 개인의 심리적 문제를 일으킬 것으로 판단하였으며, 예상 불안의 원인을 밝히고 부정적 결과로 이어질 수 있음을 확인한 측면에서 학술적 시사점을 지닌다. 또한, 조직 차원에서 개인의 예상 불안이 어떻게 영향을 주는지를 확인하였기 때문에, 불안 최소화 전략 수립 측면에서 실무적 시사점을 지닌다.

셋째, 본 연구는 개인의 정보보안 불안 형성에 영향을 주는 조직 환경적 조건에 대한 개인의 인식 요인을 제시하였다. 특히, 불확실성 개념을 반영하여, 조직 내 정보보안 관련 활동 시 발생할 수 있는 불확실성 요소를 다각적으로 제시하고자 하였다. 기술 불확실성은 정보보안 기술의 변화로 인하여 개인이 기술을 정밀하게 활용하기 어렵다고 판단하는 상황이며, 커뮤니케이션 불확실성은 제공되는 정보보안 관련 정보가 충분하지 않다고 인식하는 상황을 의미한다. 이러한 상황은 현재 조직에서 충분히 발생할 수 있는 조건이므로, 실무적 차원에서 개선점으로서 제언했다는 측면의 시사점을 가지고, 불확실성을 다각화한 측면에서 학술적 시사점을 지닌다.

마지막으로, 본 연구는 정보보안과 관련된 정보, 지식 등의 확보 및 활용은 개인의 성격에 의해 영향을 받을 것으로 판단하고, 정보 영향 민감성 요인을 반영하여, 불확실성과 불안 요소가 제언 행동에 주는 부정적 영향을 추가로 어떻게 감소시킬 수 있는지를 확인하였다. 즉, 학술적 관점에서 연구는 개인 특성화 요인을 정보보안 분야에 반영한 측면에서 시사점을 가지고, 조직원별 정보보안 불안 속성에 대한 받아들임의 차이가 있음을 인식하고 맞춤형 대처가 필요함을 제시한 측면에서 조직 실무적 시사점을 가진다.

본 연구는 정보보안 불확실성 요소의 정보보안 행동 감소에 미치는 영향을 확인한 관점에서 의미가 있지만, 다음의 한계점을 가진다. 첫째, 연구는 정보보안 조직 환경 측면에서 불확실성 요소를 제시하고 개인의 인식 수준을 측정하였다. 하지만, 이러한 지표는 개인의 설문 당시의 응답 인식 수준이기 때문에, 명확성 측면에서 문제를 일으킬 수 있다. 따라서, 향후 연구에서는 정보보안 기술 수준과 커뮤니케이션 제공 수준을 객관화함으로써, 조직 단위의 요소의 영향을 명료하게 측정하는 것이 요구된다. 둘째, 본 연구는 정보보안 관련 정보의 교환 시, 개인이 인식하는 정보 영향 민감성 요소를 조절 변수로 활용하였다. 개인차 요소는 민감성 이외 정보보안 문제 관련 대처 이론 등 다양하게 제시되고 있다. 향후 연구에서는 개인이 정보보안 이슈에 대하여 받아들이는 요소를 다각화함으로써, 개인의 행동 원인을 설명하는 지침으로 활용하는 것이 요구된다.

본 논문은 2022년 한국전자통신학회 추계학술대회에 발표한 논문임

References

[1] Nettgov, "Biden administration releases draft zero-trust guidance," *Report*, Sept. 2021.

[2] Verizon, "2021 data breach investigations report," *Report,* Des. 2021.

[3] R. West, "The psychology of security," *Communications of the ACM*, vol. 51, no. 4, 2008, pp. 34-40.

[4] G. Solomon and I. Brown, "The influence of organisational culture and information security culture on employee compliance behaviour," *J. of Enterprise Information Management*, vol. 34, no. 4, 2021, pp. 1203-1228.

[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] A. Vedadi, M. Warkentin, and A. Dennis, "Herd behavior in information security decision-making," *Information & Management*, vol. 58, no. 8, 2021, pp. 103526.

[7] 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.

[8] 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.

[9] 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.

[10] Korea Information Security Industry Association, "2021 survey on information security," *Report*, Jan. 2022.

[11] W. Lee and I. Hwang, "Sustainable information security behavior management: An empirical approach for the causes of employees' voice behavior," *Sustainability*, vol. 13, no. 11, 2021, pp. 6077.

[12] M. Svendsen and T. S. Joensson, "Transformational leadership and change-related voice behavior," *Leadership & Organization Development J.*, vol. 37, no. 3, 2016, pp. 357-368.

[13] L. Van Dyne and J. A. LePine, "Helping and voice extra-role behaviors: Evidence of construct and predictive validity," *Academy of Management J.*, vol. 41, no. 1, 1998, pp. 108-119.

[14] 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.

[15] V. Greco and D. Roger, "Coping with uncertainty: The construction and validation of a new measure," *Personality & Individual Differences*, vol. 31, 2001, pp. 519-534.

[16] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, vol. 27, no. 3, 2003, pp. 425-478.

[17] R. N. Carleton, M. P. J. Norton, and G. J. Asmundson, "Fearing the unknown: A short version of the intolerance of uncertainty scale," *J. of Anxiety Disorders*, vol. 21, no. 1, 2007, pp. 105-117.

[18] I. Hwang, D. Kim, T. Kim, and S. Kim, "Why not comply with information security? An empirical approach for the causes of non-compliance," *Online Information Review*, vol. 41, no. 1, 2017, pp. 2-18.

[19] M. Siponen and A. Vance, "Neutralization: New insights into the problem of employee information systems security policy violations," *MIS Quarterly*, vol. 34, no. 3, 2010, pp. 487-502.

[20] 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.

[21] Z. Yan, X. Guo, M. Lee, and D. R. Vogel, "A

conceptual model of technology features and technostress in telemedicine communication," *Information Technology & People*, vol. 26, no. 3, 2013, pp. 283-297.

[22] 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.

[23] R. K. Jena, "Technostress in ICT enabled collaborative learning environment: An empirical study among Indian academician," *Computers in Human Behavior*, vol. 51, 2015, pp. 1116-1123.

[24] K. Ruck and M. Welch, "Valuing internal communication; Management and employee perspectives," *Public Relations Review*, vol. 38, no. 2, 2012, pp. 294-302.

[25] M. Welch and P. R. Jackson, "Rethinking internal communication: A stakeholder approach," *Corporate Communications: An Int. J.*, vol. 12, no. 2, 2007, pp. 177-198.

[26] D. Jiménez-Castillo and M. Sánchez-Pérez, "Nurturing employee market knowledge absorptive capacity through unified internal communication and integrated information technology," *Information & Management*, vol. 50, no. 2, 2013, pp. 76-86.

[27] J. B. Barlow, M. Warkentin, D. Ormond, and A. Dennis, "Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance," *J. of the Association for Information Systems*, vol. 19, no. 8, 2018, pp. 689-715.

[28] 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.

[29] A. Yazdanmehr, J. Wang, and Z. Yang, "Peers matter: The moderating role of social influence on information security policy compliance," *Information Systems J.*, vol. 30, no. 5, 2020, pp. 791-844.

[30] E. Bonabeau, "The perils of the imitation age," *Harvard Business Review*, vol. 82, no. 6, 2004, pp. 45-54.

[31] J. Wang, Z. Yang, and S. Bhattacharjee, "Same coin, different sides: Differential impact of social learning on two facets of music piracy," *J. of Management Information Systems*, vol. 28, no. 3, 2011, pp. 343 - 384.

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

[33] 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.

[34] P. M. Podsakoff, S. B. MacKenzie, J. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies," *J. of Applied Psychology*, vol. 88, no. 5, 2003, pp. 879-903.

[35] A. F. Hayes, *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York: Guilford Publications, 2017.

저자 소개

황인호(In-Ho Hwang)

2007년 중앙대학교 대학원 졸업(경영학석사)
2014년 중앙대학교 대학원 졸업 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