Journal of the Korea Convergence Society
Vol. 11. No. 9, pp. 229-242, 2020

ISSN 2233-4890 / eISSN 2713-6353
https://doi.org/10.15207/JKCS.2020.11.9.229

조직구성원의 정보보안 준수 및 미준수 원인에 대한 연구

황인호[1], 허성호[2*]
[1]국민대학교 교양대학 교수, [2]중앙대학교 심리학과 강사

A study on the information security compliance and non-compliance causes of organization employees

In-Ho Hwang[1], Sung-Ho Hu[2*]
[1]Professor, Department of General Education, Kookmin University
[2]Lecturer, Department of Psychology, Chung-Ang University

요 약 본 연구의 목적은 정보보안 준수의도에 영향을 주는 긍정적, 부정적 측면의 환경적 요인을 제시하고, 개인의 보안 준수의도와의 영향관계를 찾는 것이다. 연구대상은 정보보안 정책 및 기술을 적용하는 조직의 구성원들이며, 설문조사를 통하여 유효표본을 확보하였다. 분석과정에서 구조방정식모델링을 통해 연구모델에 대한 검증을 하였다. 측정변수는 정보보안 정책, 정보보안 시스템, 정보보안 기술적 지원, 업무장애, 비가시성, 조직몰입, 준수의도로 구성하여 분석에 활용하였다. 결과는 보안 준수요인인 정책, 시스템, 기술적 지원과 미준수 요인인 업무 장애가 각각 조직몰입에 영향을 주었으며, 준수의도로 이어지는 것을 확인하였다. 연구 모델의 검증 결과를 토대로 조직의 정보보안 준수 수준 향상을 위한 구성원들의 보안 준수 전략 수립의 방향성을 제시하였다.

주제어 : 준수의도, 조직몰입, 정보보안 정책, 정보보안 시스템, 정보보안 기술적 지원, 업무장애, 비가시성

Abstract The purpose of this study is to present the environmental factors of positive and negative aspects that affect the information security compliance intention, and reveals the relationship of the individual's the security compliance intention. The subjects of this study are employees of organizations that apply information security policies and technologies, and effective samples were obtained through surveys. In the process of analysis, the study model was verified through structural equation modeling. The measurement variables consisted of security policy, security system, technical support, work impediment, security non-visibility, compliance intention and organizational commitment and used for analysis. The results confirmed that security compliance factors such as policy, system, technical support, and non-compliance factors, work impediment, respectively, had an impact on organizational commitment, leading to compliance intention. The verification result of the research model suggests the direction of establishing a security compliance strategy for employees to improve the level of information security compliance of the organization.

Key Words : Compliance Intention, Organizational Commitment, Security Policy, Security System, Technical Support, Work Impediment, Security Non-visibility

*This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea(NRF-2018S1A5A8027420)
*Corresponding Author : Sungho Hu(powerrcy@daum.net)
Received July 16, 2020 Revised August 21, 2020
Accepted September 20, 2020 Published September 28, 2020

1. 서론

조직에서 보유한 정보 가치가 조직의 가치를 대변하는 시대가 되면서, 조직들은 필연적으로 핵심 자산인 정보를 보호하기 위한 노력을 해야하는 상황으로 접어들고 있다[1]. 실제로, 글로벌 정보보안 시장은 지난 2005년부터 2019년까지 30배 이상 성장하였으며, 2022년에는 1,330억 달러를 넘을 것으로 예상되고 있다[2].

조직들의 정보 보호를 위한 지속적인 투자에도 불구하고, 정보 노출 사고는 끊임없지 발생하고 있다. 버라이즌의 정보보안 침해 보고서(2019)에 따르면, 정보보안 사고는 발생하더라도 잘 드러나지 않는 경향이 있으나, 전 세계적으로 높은 수준으로 지속적으로 발생하고 있는 것으로 나타났다[3]. 세부적으로, 조직의 보안 사고는 매년 60~70% 정도가 해킹, 멀웨어 등을 통한 외부의 침입에 의해 발생하고 있으나, 조직 내부에 의한 사고 또한 매년 20~30% 발생하고 있는 것으로 나타났다. 실제, 2018년의 경우 보안 사고 유형의 15%가 권한이 부여된 사용자의 오용(misuse)에 의해 발생한 것으로 나타났으며, 보안사고 주체 중 34%가 내부자에 의한 사고인 것으로 나타났다[3].

최근 코로나19와 같은 환경적 변화에 의해 스마트워크 개념이 조직에 도입 및 확산되기 시작하면서, 내부자에 의한 정보보안 사고 위협은 더욱 높아지고 있다. 즉, 휴대성 디바이스 기술 도입 및 활용을 통한 업무 생산성 향상 요구는 조직구성원들의 정보 접근을 더욱 다양한 장소 및 채널을 활용하여 접근하도록 허용하고 있어, 내부자들의 보안 사고 위협은 결코 적지 않은 것으로 판단된다[4-6].

조직구성원 관점의 정보보안에 대한 선행 연구들은 심리적 관점에서 개인의 정보보안을 접근해야 한다고 보고 있다. 특히, West(2008)는 정보보안에 대한 조직과 개인 간의 관계는 대리인 관계가 형성되고 있다고 보았다. 개인의 정보보안 행동 정보의 양은 조직보다 많으며, 언제든 숨길수 있기 때문에 개인의 도덕적 해이가 발생할 수 있다고 보았다[7]. 그러므로, 내부인의 정보보안 준수 활동은 조직이 아닌 개인의 심리적 선택에 의해 결정된다고 주장하였다. 관련된 선행 연구에서도 조직 내 구성원의 정보보안을 심리적 관점에서 접근함으로써, 내부자의 보안 위협 문제를 해결하고자 하고 있다. 대표적으로, 일반억제이론(general deterrence theory)을 중심으로 개인의 정보보안 미준수에 대한 엄격하고 명확한 제재를 보여주는 것이 준수 행동에 영향을 준다는 연구가 제시되고 있으며[8,9], 예방동기이론(protection motivation theory)을 중심으로 정보보안 미준수에 대한 명확한 공포 메시지가 개인의 태도 또는 행동에 영향을 주기 때문에, 이를 기반으로 확장형 연구가 다양하게 제시되고 있으며[10,11], 계획된 행동이론(theory of planned behavior)을 활용하여 정보보안을 준수해야 하는 개인의 행동 원천을 찾는 연구가 제시되고 있다[12,13]. 최근에는 정보기술의 부정적 측면인 기술스트레스가 정보보안 분야에도 적용됨을 제시하는 연구들이 제시되고 있다[14,15]. 이와 같은 선행연구들은 조직구성원 정보보안 준수 행동에 영향을 주는 요인들을 개인 측면에서 사회과학 등 다양한 이론을 중심으로 제시하였다는 측면에서 시사점을 가진다.

반면, 조직구성원의 정보보안 준수 행동은 개인의 심리적 결정으로 이루어지기 때문에, 개인을 둘러싼 조직 내부의 환경적 특성에 영향을 많이 받게 된다[16]. 즉, 구성원의 보안 준수 행동에 긍정적, 부정적 영향을 주는 조직의 환경적 요인이 있으며, 개인은 자신을 둘러싼 환경적 특성을 종합적으로 판단하여 보안 행동 수준을 결정한다. 하지만, 보안 준수의도에 영향을 주는 조직 내 환경적 특성 및 구조를 제시하는 것이 필요함에도 불구하고 아직까지 조직원의 정보보안 준수와 관련된 선행연구들은 동기 형성에 초점을 맞추고 있어, 조직차원에서 제공해야할 보안 환경 및 지원체계에 대한 연구는 부족한 상황이다.

이에 본 연구는 조직원의 정보보안 준수의도에 영향을 주는 조직 환경 측면의 특성을 찾고 영향관계를 증명하고자 한다. 세부적으로, 조직원의 정보보안 준수의도에 긍정적인 영향을 주는 조직 환경 요인(정보보안 정책, 정보보안 시스템, 정보보안 기술적 지원)을 제시하고 준수의도에 미치는 영향 관계를 찾고자 한다. 더불어, 정보보안 준수의도에 부정적인 영향을 주는 조직 환경 요인(업무 장애, 보안 비가시성)을 제시하고 준수의도에 미치는 영향 관계를 찾고자 한다.

이를 통해, 연구는 조직 차원에서 조직원들에게 지속적으로 제공해야할 환경적 요인과 보완해야 할 환경적 요인을 제시함으로써, 조직원이 자발적으로 보안 준수 행동을 할 수 있는 조직의 보안 관련 전략적 방향을 제시하고자 한다.

2. 이론적 배경

2.1 정보보안 준수의도

조직 내부자에 의한 정보보안 사고는 다양한 상황에서 발생하고 있는데, 조직 정보시스템에 대한 접속이 가능한 상황이면 언제든 발생할 수 있다[17]. 실제로 정보보안 사고를 일으킨 내부자는 정보시스템 관리자 이외에 임직원, 사무직 등 다양한 직무에서 나타나고 있어[3], 조직원의 정보 노출 위협을 최소화하는 것이 필요하다. 하지만, 정보보안 준수 행동에 대한 정보는 조직원이 조직보다 많이 보유하고 있으며, 언제든 숨기려고 하면 상황을 감출 수 있기 때문에[7], 엄격한 보안 기술을 적용하는 것만으로 내부자의 정보보안 준수 행동을 명확하게 이끌어내기 어렵다[9,11]. 따라서, 조직은 개인의 자발적인 행동을 높이기 위한 지원체계를 구축하는 것이 필수적이며, 이를 통해 조직원의 정보보안 준수 의도를 높이는 것이 필요하다.

의도는 현재 또는 미래에 특정한 행동을 실행하겠다는 다짐을 보여주는 정신 상태를 의미한다[18]. 즉, 조직에서 개인의 의도는 특정 목적에 대한 달성 의지에 대한 정신 상태이기 때문에 긍정적 행동을 기대하는 요인이다. 특히 정보보안 준수의도는 내부 및 외부의 위협으로부터 조직의 정보 자원을 보호하려는 개인의 행동의지 이기 때문에[17], 준수의도가 높은 조직원은 조직에서 추구하는 보안 목표에 대한 수행 행동을 할 가능성이 매우 높다. 따라서, 조직이 내부의 보안 위협을 최소화하고, 정보보안 목표 수준을 달성하기 위해서는, 구성원의 자발적인 정보보안 행동이 필요한 상황이며, 준수의도 향상을 위한 조직차원의 노력이 필요하다. 본 연구는 조직원의 보안 준수의도에 영향을 주는 조직의 긍정적 요인과 부정적 요인을 찾고 관련성을 검증함으로써, 준수의도 향상 방안을 제시하고자 한다.

2.2 조직 몰입

조직 몰입에 대한 개념은 연구자별 조금씩 차이가 있으나, 개인 스스로가 조직과 동일시 하거나 헌신하고자 하는 성향으로 정의되거나[19], 조직의 목표 및 가치에 대하여 조직과 동일시 또는 관여하고자 하는 개인의 상대적 강도의 수준으로 정의하고 있다[20]. 즉, 조직 몰입은 조직의 목표 또는 추구하는 가치를 인지하고 동일시하고자 하는 개인의 성향으로 정의할 수 있다.

조직 몰입 수준을 높게 보유한 조직원은 규정된 자신 과업 수준을 넘어서 자발적으로 조직에 도움이 되는 행동을 하려는 경향이 강하다[21]. 즉, 조직의 특정 목표에 대한 믿음을 형성한 조직원은 대상 목표를 동일시하기 때문에 지속적으로 목표를 달성하고자 한다[22].

조직 몰입은 조직 차원에서 몰입을 위한 환경을 구축해서 조직원에게 제공할 경우, 개인들의 몰입 수준은 높아진다[21]. 즉, 조직 몰입은 동일시 강도가 상대적이기 때문에 개인별 차이가 있을 수 있으나, 조직의 목표를 이해시키고 목표 달성의 당위성을 인정하는 등의 활동이 선행될 경우 개인은 조직이 추구하고자 하는 가치를 인식하고 동일시 할 가능성이 높아진다[19].

정보보안 관점에서도 조직몰입은 조직원의 자발적인 보안 준수를 위한 중요한 요인이다. 합리적 선택이론 관점에서 살펴보면, 조직원에게 정보보안 정책 및 관련 기술은 자신의 성과 달성을 위한 장애 요인으로 인식되는데, 정보보안 준수를 통해 얻을 수 있는 혜택이 준수 행동으로 인한 비용보다 커야 준수의도를 가진다[17]. 하지만, 조직 몰입은 개인의 조직에 대한 믿음의 수준이기 때문에, 조직의 보안 목표에 대한 몰입 수준이 높은 조직원은 준수의도가 강화된다[18]. 즉, 조직 몰입은 비록 정보보안 준수 행동이 자신의 업무 달성에 불편한 행동일지라도, 조직의 핵심 정보 보호를 위하여 필요한 행동으로 인식하게 하는 요인이다[15].

조직 몰입이 높아진 조직원은 조직에서 요구하는 정보보안 수준을 달성하기 위한 노력을 한다. Hwang and Cha(2018)는 정보보안 관련 기술스트레스와 준수의도 간의 관계분석에서, 높아진 보안 기술에 의한 스트레스는 조직몰입을 통해 준수의도까지 부정적 영향을 미치는 것을 확인하였다[15]. Safa et al.(2018)은 내부자의 보안 위협을 감소시키기 위한 통합모델을 제시하였으며, 몰입이 미준수행동의도를 감소시키는 것을 확인하였다. Herath and Rao(2009)는 동기이론과 제재이론을 기반으로 개인들의 정보보안 정책 수용 통합 프레임워크를 제시하였다. 그들은 조직 몰입이 정보보안 정책에 대한 준수의도를 높이는 요인이기 때문에, 조직에 대한 관여 수준이 높아지도록 관리하는 것이 필요하다고 보았다[18]. Sharma and Warkentin(2019)은 업무 절차에서 필요한 조직의 정보보안 규칙을 준수하는 정도를 조직원의 조직몰입 수준에 따라 파악하였으며, 높은 수준의 조직 몰입을 가진 조직원일수록 정보보안 관련 행동의 필요성을 인식하고 있는 것으로 나타났다[25]. 즉, 선행연구는 조직 목표 및 가치 에 대한 개인의 관여 수준인 몰입의 형성이 정보보안 준수의도에 긍정적인 영향을 미치는 것으로 제시하고 있다.

2.3 정보보안 준수 요인

2.3.1 정보보안 정책 지원

정보 정책은 조직 내에서 정보시스템 자원을 적절히 사용하기 위한 규칙 및 가이드라인으로서[26], 정보보안 정책은 정보보안과 관련된 조직의 기술 등 자원을 사용하기 위한 규정을 의미한다[16]. 정보보안 정책에는 조직의 정보보안 목표, 조직의 보안 관련 표준, 규칙에 대한 준수 요구 사항 등의 행동 방식에 대한 상세 설명, 보안 준수 행동에 대한 책임, 그리고 보안 사고 시 처리 방법 등이 포함된다[27].

조직의 환경에 적합한 정보보안 정책 수립 및 보급은 조직원들의 정책에 대한 신뢰를 확보할 수 있기 때문에, 조직에 맞는 보안 정책을 수립하는 것이 중요하다[28]. 따라서, 조직은 외부 환경 요인(기술발전, 산업 표준, 관련 법적 요구사항 등)과 내부 환경 요인(사업 목표, 조직 문화, 기술 아키텍처, 내부 반발 등)을 종합적으로 고려하여 정보보안 정책 수준을 결정하고 구체화하는 것이 필요하다[29].

더불어, 조직의 정책은 조직원들의 조직 몰입에 긍정적인 영향을 준다. Chung and Chang(2005)은 조직의 인적자원관리의 효과를 높이기 위해서는 가족친화적인 인사제도를 구축하는 것이 필요하며, 가족친화적 제도가 조직 몰입에 긍정적인 영향을 미치는 것을 확인하였다[30]. 마찬가지로 Eaton(2003)은 조직의 업무가 개인의 삶과 균형 있게 유지될 수 있도록 조직의 관련 정책을 수립하는 것이 필요하다고 보았으며, 업무-개인의 삶에 대한 균형 잡힌 정책은 조직 몰입을 높여 성과에 영향을 주는 것을 확인하였다[31]. 즉, 조직의 명확한 정책 수립 및 제공은 조직원의 신뢰를 높이고 몰입에 영향을 준다.

2.3.2 정보보안 시스템 지원

조직은 핵심 자산인 정보 노출을 방지하고 손실을 최소화하기 위해, 그리고 조직 내·외부의 보안 위협으로부터 조직의 정보를 보호하기 위하여 정보보안 활동을 조직에 구현하고자 한다[29]. 효과적인 정보보안 활동은 조직 내 모든 구성원들의 통일된 정보 생성, 운영, 보호를 위한 물리적 시스템을 개발 및 도입하는 것이다[16]. 정보보안 시스템은 조직원의 정보 자원에 대한 접근을 제한하고 통제할 목적으로 구축하는 기술을 의미한다[27]. 핵심 정보에 대학 접근 제어 밑 통제를 위해서는 중요 정보를 관리하는 시스템의 물리적 출입 통제, 데이터 센터 및 컴퓨터실에 대한 보안, 케이블과 관련 장비와 같은 물리적 접근에 대한 관리 시스템을 구축하는 것이 필요하다[32]. 최근에는 개인 보유 정보의 관리 및 손실을 최소화하기 위한 보안 클라우드 시스템, 정보보안이 적용된 모바일 컴퓨팅 시스템 등을 도입 및 활용함으로써 조직의 정보 관리 수준을 높이고 있다[33].

정보 관리를 위한 보안 시스템 도입은 표준화된 정보 관리 체계를 포함하기 때문에, 조직의 정보 관리 문화 형성 및 준수행동에 도움을 준다. Yildirim et al.(2011)은 조직 내 도입한 물리적 보안 시스템은 조직원의 보안 행동에 대한 방향을 제시하기 때문에 조직 차원의 보안 문화 형성에 도움을 준다고 하였으며[34], DeVeiga and Eloff(2010)은 정보보안 관련 물리적 기술 도입은 조직원의 보안 행동 방향을 제시하기 때문에, 정보보안 준수 문화형성에 도움을 준다고 하였다. Hwang et al.(2017)은 조직구성원의 정보보안 미준수 원인과 조직차원의 개선을 위한 노력요인을 제시하였는데, 정보보안 시스템 구축 및 지원이 개인들의 미준수원인을 감소시켜, 보안 준수의도를 높인다고 하였다[16]. 즉, 정보보안 시스템 도입은 조직 구성원의 표준화된 정보 행동을 요구하고 관리할 수 있기 때문에 조직의 보안 수준은 높아질 수 있다.

정보시스템 도입은 조직 몰입에 긍정적인 영향을 준다. Shum et al.(2007)은 조직의 고객관리시스템 도입 관점에서, 조직원의 조직 목표에 맞는 행동 변화를 위해서는 관련된 시스템 도입을 통해 업무 표준을 달성하는 것이 필요하다고 보았다[36]. 특히, 그들은 고객관리시스템 도입이 조직원들의 조직 몰입을 높이는 것을 확인하였다[36]. Cardoso and Caldeira(2012)는 병원정보시스템의 도입이 조직 구성원들의 조직 몰입에 미치는 영향 수준을 파악하였다. 그들은 병원 내 정보시스템 도입이 구성원들의 업무에 대한 인식을 높이고 관여 수준을 높여 조직 몰입에 긍정적인 영향을 준다고 하였다[37].

2.3.3 정보보안 기술적 지원

기술적 지원은 조직의 제도화된 기술에 대한 이해 향상을 위한 조직 차원의 기술지원 매커니즘이다[38]. 기술적 지원은 조직 내 도입 한 기술을 조직원이 효율적으로 활용할 수 있도록 돕는 체계로서, 일반적으로 기업들은 IT 시스템에 대한 헬프데스크를 운영함으로서, 기술 활용성을 높이도록 돕는다[39]. 이와 같은 기술적 지원은 실제 사용자인 조직원의 관점에서 정보 기술 사용 시 발생하는 문제점을 해결해줌으로서, 개인들에게 발생 가능한 기술적 어려움(기술적 복잡성, 기술적 불확실성 등)을 최소화하여 업무 생산성 향상에 도움을 준다[40]. 특히, 최근에는 급변하는 환경적 변화에 대응하기 위한 조직들의 신 기술 도입이 잦아들면서, 개인들의 기술스트레스 발생 문제가 조직의 이슈가 되고 있다. 기술 도입에 의한

스트레스를 완화하기 위해서는 개인들의 눈높이에 맞는 기술적 지원 체계를 구축하는 것이 필요하다[41].

기술적지원은 조직몰입, 준수의도와 같은 조직 목표에 대한 능동적인 행동원천 요인들에게 긍정적인 영향을 준다. Fuglseth and Sørebø(2014)는 기술스트레스가 조직원의 ICT 사용 만족도 및 지속적인 사용의도를 감소시키는 선행 조건이라고 하였으며, 헬프데스크와 같은 사용자 관점의 기술적 지원은 관련 지식 형성 등을 통해 사용의도에 긍정적인 영향을 주는 요인임을 제시하였다[38]. Ragu-Nathan et al.(2008)은 정보관리 중요성이 높아지면 질수록, 조직 내 기술스트레스가 높아지게 되는데, 기술적 지원이 기술스트레스를 완화시키며, 조직 몰입에 긍정적인 영향을 주는 요인임을 증명하였다[39]. 특히 Tarafdar et al.(2011)은 성과에 긍정적인 영향을 주는 기술도입의 부정적인 부분을 모델화하였으며, 기술스트레스 완화요인인 기술적 지원이 개인의 심리적 결과물인 조직 몰입, 만족도와 같은 요인에 긍정적인 요인임을 제시하였다[40].

2.4 정보보안 미준수 요인

2.4.1 정보보안 관련 업무 장애

조직원들은 개인에게 주어진 목표를 달성하기 위하여 노력한다. 정보기술은 개인에게 주어진 업무의 효율을 높이고 성과달성에 도움을 주는 핵심 요인이다[42]. 반면, 정보보안은 조직원의 행동을 통제하는 요인으로, 성과 달성을 위한 활동을 제한할 수 있는 요인이다. 예를 들어, 조직원은 업무 효율을 위하여 자유롭게 정보 공유를 하고자 하나, 보안 승인 절차는 관리자의 승인이 사전에 필요함을 의미하기도 한다. 또한, 개인적 활동을 위하여 조직 내 허가되지 않는 메신저 프로그램을 사용하여 내부 정보자원을 동료들과 공유하기도 한다[43]. 즉, 정보보안 목표는 정보보안 부서의 조직원을 제외하고, 개개인의 목표와 동일하지 않는 경우가 대부분이며, 조직원들은 업무성과 달성을 위해 절차의 편의성을 추구하는 경향이 높다.

정보보안 관련 업무 장애는 보안 정책 준수 규정으로 인한 개인들의 업무 절차와 조치에 대한 제한 수준으로 정의된다[17]. 심리적 요인이 강한 정보보안 관련 행동은 보안을 실행에 옮기는 개인의 상황에 따라 결정될 가능성이 높은데[7], 보안 관련 행동이 업무 절차 등 성과 달성에 부정적인 영향을 미친다고 판단할 경우 정보보안을 어길 가능성이 높아진다[9].

정보보안 관련 업무 장애는 미준수 행동을 일으키는 선행 조건이다. Bulgurcu et al.(2010)은 정보보안 준수 행동은 개인의 합리적 선택에 의해 결정된다고 보았으며, 개인은 보안 준수 시 발생하는 비용과 혜택을 비교한다고 보았다[17]. 그들은 정보보안에 의해 발생되는 업무장애를 비용으로 보았으며, 보안 준수의도에 부정적인 영향을 미치는 요인임을 증명하였다. Hwang et al.(2017)은 정보보안 준수의도는 조직과 개인간의 상호 관계에서 발생한다고 보고 개인의 미준수원인을 업무장애로 보았으며, 준수의도를 감소시키는 원인임을 확인하였다[16].

2.4.2 정보보안 비가시성

조직은 사전에 정보보안 목표 및 수준을 결정하고, 내부 구성원들에게 관련 행동 준수를 요구한다. 즉, 조직이 정해놓은 방향에 따라 조직원들은 준수행동을 하여야 한다. 정해진 보안 관련 행동을 요구받는 개인이 바람직한 행동을 하기 위해서는 관련 보안 정책 및 규정, 절차, 보안 행동 방식, 그리고 예상되는 성과 등을 지속적으로 제공하는 것이 필요하다. 보안 관련 정보를 제공하는 조직 차원의 노력이 없을 경우 조직원들은 자신이 획득한 제한된 정보만을 기반으로 보안 행동을 하게 되고 합리화하고자 한다[7].

보안 관련 다양한 정책, 행동 방법 등 정보를 조직원에게 제공하는 것을 가시성이라 한다[16]. 조직의 보안 가시성 활동은 조직원들의 정보보안 정책 준수에 영향을 미친다. 보안 정책에 대한 설득력 있는 메시지는 조직 전체가 지속적으로 볼 수 있도록 표시되는 것이 필요하다. 예를 들어 정보보안 관련 캠페인, 포스터, 커피잔에서의 광고 등이 있을 수 있는데 가시적인 활동은 개인의 보안 관련 정보를 확보할 수 있도록 돕는다[44].

정보보안에 대한 가시적 행동은 보안 기술 도입 이외에 추가적으로 소요 되는 비용과 같고, 효과성에 대한 증명이 쉽지 않기 때문에 가시적인 정보 제공 활동은 지속되기 쉽지 않다[16]. 즉, 정보보안 비가시성이 높아질수록 조직원들은 잘못된 보안 정보를 확보하게 되어 조직의 보안 목표 수준과 다른 행동을 할 가능성이 높다. 또한, 특정 정보에 대한 비가시성은 조직에 대한 개인의 몰입을 감소시키는 요인이다. Aryeetey and Sanda(2010)는 개인의 조직 내 업무 생활의 질적 향상은 조직원의 몰입에 의해서 결정되는데, 조직에서 업무에 대한 다양한 정보를 제공하지 않을 때 몰입 수준이 낮아져 질적 업무 생활수준이 낮아진다고 하였다[45].

3. 연구 모델 및 방법

3.1 연구 모델

본 연구는 조직원들의 정보보안 준수 의도 형성에 긍정적, 부정적 영향을 주는 선행 요인을 제시함으로써, 자발적인 정보보안 준수 행동 방향을 찾는 것을 목적으로 한다. 세부적으로, 조직에 대한 조직원들의 몰입 형성이 준수의도를 높일 것으로 판단하고, 조직몰입에 긍정적, 부정적 영향을 주는 조직원의 조직 내 환경적 요인을 제시함으로써, 조직 내 보안 관련 다각적 상황을 검토하고자 하였다. 연구에서 제시하는 연구모델은 Fig. 1과 같다.

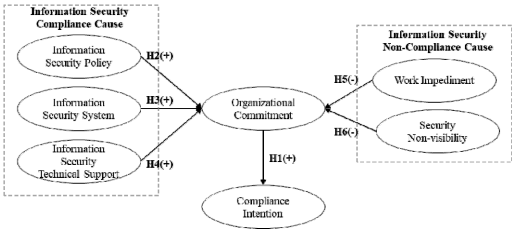

Fig. 1. Research Model and Proposed Hypotheses

3.2 데이터 측정 방법 및 수집

본 연구의 목적인 구성원들의 정보보안 환경에 대한 평가 및 준수에 대한 생각을 파악하기 위하여, 설문지 기법을 적용하여 연구 모델 및 가설을 검증하고자 하였다.

설문 구성은 Table 1과 같이 연구 모델에 적용된 7개 요인에 대하여 각각 선행 연구에서 도출된 세부 문항들을 정보보안 상황에 맞추어 재구성하였으며, 다항목 기반의 설문을 구성하여 분석의 내적 타당성을 높이고자 하였다.

도출된 설문문항은 타당성 확보를 위하여, 정보보안 정책을 보유한 기업에서 근무하며 대학원에 다니는 학생 10명에게 사전 인터뷰 및 설문항목 검증을 실시하였다. 설문문항에 문제가 없다고 판단되어, 본 설문을 실시하였다. 설문 항목에 대한 구성은 응답의 편의성과 분석의 다양성을 위하여 7점 등간척도를 활용하여 구성하였다.

설문 대상은 정보보안 정책을 실시하고 있는 기업에 재직 중인 직장인을 대상으로 하되, 정보보안 정책 확산을 주 업무로하는 IT부서나 보안 부서를 제외한 일반 업무 부서로 한정하였다. 대상을 제한적으로 설정한 이유는 본 연구의 목적이 보안 업무가 자신의 주 업무가 아닌 구성원들의 준수 행동의 원인을 파악하기 위한 것이기 때문이며, 조직 내 정보보안 부서의 목적은 보안 관련 관리가 주 목적이기 때문에, 연구목적과 상이하다고 판단하였다.

Table 1. Questionnaire

Constructs	Items		Source
Security Policy	SP1	Our organization has detailed instructions for usage of e-mail.	[27]
	SP2	Our organization has a rule for utilization of computer resources (ex: pc, server, etc).	
	SP3	Our organization has official policy of prohibiting the access of unauthorized computer system	
	SP4	Our organization has detailed guidelines to explain how to use computer password.	
Security System	SSI	Our organization's information security system is constructed to be efficiently utilized.	[46]
	SS2	Our organization appropriately invests in the construction of an information security system.	
	SS3	Our organization allots sufficient expenses on an information security system.	
Technical Support	TS1	Our end-user help desk does a good job of answering questions about information security.	[39]
	TS2	Our end-user help desk is well staffed by knowledgeable individuals(Drop).	
	TS3	Our end-user help desk is easily accessible.	
	TS4	Our end-user help desk is responsive to end-user requests(Drop).	
Work Impediment	WI1	Complying with the requirements of the security policy keeps me from doing my actual work .	[17]
	WI2	Complying with the requirements of the security policy slows down my response time to my peers, customers, managers, etc.	
	WI3	Complying with the requirements of the security policy hinders my productivity at work.	
	WI4	Complying with the requirements of the security policy impedes my efficiency at work.	
Non visibility	NV1	In my organization, information security activities are not advertised widely.	[44]
	NV2	Information security is not very visible in my organization.	
	NV3	Information security incidents are visible in public (R) (Drop).	
Organizational Commitment	OC1	I would be happy to spend the rest of my career in this organization.	[24]
	OC2	I enjoy discussing my organization with people outside it.	
	OC3	I really feel as if this organization's problems are my own.	
Compliance Intention	CI1	IIt is likely that I would continuously comply with security policy in order to protect the organization's security system.	[24]
	CI2	I am willing to comply with security policy during work.	
	CI3	I feel certain about my attitude toward compliance with the organization's security policy.	

설문 조사는 대학 내 사회인들을 위하여 도입한 과정인 주말반 경영학 학사 과정에 다니는 직장인들을 대상으로 실시하였다. 2019년 11월~12월 2개월 동안 재직자 전형 수업의 학생들에게 사전 양해를 구하고 설문을 실시하였으며, 설문 실시 전 연구의 목적 및 데이터 활용

방법 등 개인 정보관련 내용의 활용에 대한 동의를 구하고 설문을 실시하였다. 총 500부를 배포하였으며, 응답을 거절한 학생 88명을 제외한 412개의 결과를 Table 2와 같이 확보하였다. 이중 설문 응답을 부실하게 하는 등 문제가 있는 결과를 제외한 346개의 자료를 연구 가설 검증에 활용하였다.

Table 2. Demographic Characteristics

Demographic Categories		Frequency	%
Total		346	100.0%
Gender	Male	194	56.1%
	Female	152	43.9%
Age	〈 30	93	26.9%
	31~40	140	40.5%
	41~50	102	29.5%
	〉 50	11	3.2%
Type of Industry	Manufacturer	80	23.1%
	Service	266	76.9%
Job Position	Staff	144	41.6%
	Assistant Manager	92	26.6%
	Manager	55	15.9%
	General Manager	55	15.9%

3.3 연구 가설

지금까지의 내용을 종합하여 본 연구는 다음과 같은 가설을 수립하였다.

H1 : 조직원의 조직 몰입은 정보보안 준수의도에 긍정적 영향을 미칠 것이다.

H2 : 정보보안 정책 지원은 조직몰입에 긍정적 영향을 미칠 것이다.

H3 : 정보보안 시스템 지원은 조직몰입에 긍정적 영향을 미칠 것이다.

H4 : 정보보안 기술적 지원은 조직몰입에 긍정적 영향을 미칠 것이다.

H5 : 정보보안 관련 업무 장애는 조직몰입에 부정적 영향을 미칠 것이다.

H6 : 정보보안 비가시성은 조직몰입에 부정적 영향을 미칠 것이다.

4. 연구 결과

4.1 신뢰성 및 타당성 분석

연구 모델 및 가설 검증은 구조방정식모델링을 통해 실증 분석을 하고 시사점을 제시하고자 한다.

설문 문항에 대한 신뢰성 및 타당성 분석을 실시하였다. 신뢰성 분석은 한 요인을 유사한 다항목의 설문으로 측정하였을 때 실시하는 분석으로 항목들의 일관성을 파악하고자 할 때 적용한다. 본 연구는 SPSS 26.0을 활용하여 Cronbach's alpha 값을 도출함으로써 검증하였으며, Cronbach's alpha 값이 요인별 0.7 이상일 때 신뢰성을 확보하였다고 판단한다[47]. 분석 결과, 신뢰성에 문제가 있는 요인 3개(기술적지원 2개, 비가시성 1개)를 제외한 21개의 문항을 적용하였으며, 가장 낮은 신뢰성을 가진 요인인 비가시성이 0.848로 나타나 신뢰성에 문제가 없는 것으로 나타났다.

타당성은 다중 항목으로 구성된 지표가 일정한 방향으로 구성되어 있는지(집중타당도(convergent validity)), 다른 지표와의 차별성이 있는지(판별타당도(discriminant validity))하는 분석 기법이다. 집중타당도는 일반적으로 개념신뢰도(construct reliability)와 평균분산추출(average variance extracted)을 통해 검증한다. 집중타당도 검증을 위해서는 AMOS 22.0을 활용하여 확인적 요인분석을 실시하여야 하며, 개념신뢰도는 0.7이상의 값을, 평균분산추출은 0.5이상의 값을 요구한다[48].

구조모형에 대한 모델의 적합도는 복합적으로 적합지수를 활용하며, 적용지수별 요구사항의 차이가 있다. GFI는 0.9 이상, AGFI는 0.9이상(0.8이상 허용), NFI는 0.9이상, CFI는 0.9이상, RMSEA는 0.05이하(0.1이하 수용가능)를 요구한다. 7개 요인(21개 문항)에 대한 확인적 요인분석을 실시한 결과 모형의 적합도는 요구사항에 적합한 수준인 것으로 나타났다(χ^2/df = 1.725, GFI = 0.931, AGFI = 0.904, CFI = 0.986, NFI = 0.968, RMSEA = 0.044). 이후, Table 3과 같이 개념신뢰도와 평균분산추출 값을 구하였으며, 개념신뢰도가 가장 낮은 요인은 비가시성(0.706), 평균분산추출이 가장 낮은 요인은 업무장애(0.545)로 나타나 집중타당성 문제는 없는 것으로 제시되었다.

추가적으로, 판별타당성 분석을 실시하였다. 판별타당성은 지표간의 차별성이 있는지를 판단하기 위한 분석 기법이다. 판별타당성은 상관관계 분석을 통해 도출된 요인들의 상관계수들과 평균분산추출의 제곱근 값을 비교함으로써 판단한다[49]. 7개 요인에 대한 상관관계 분석 값과 타당성 분석에 활용한 평균분산추출의 제곱근 값을 비교한 결과, Table 4에서처럼 상관관계분석 값이 작은 것으로 나타나 판별타당성 문제가 적은 것으로 나타났다.

Table 3. Result for Construct Validity and Reliability

Construct	Item	Factor Loading	Cronbach's Alpha	CR	AVE
Security Policy	SP1 SP2 SP3 SP4	.838 .848 .827 .855	.934	.908	.711
Security System	SSI SS2 SS3	.824 .862 .866	.934	.908	.768
Technical Support	TS1 TS3	.940 .941	.911	.751	.601
Work Impediment	WI1 WI2 WI3 WI4	.939 .946 .922 .912	.946	.827	.545
Non visibility	NV1 NV2	.879 .888	.848	.706	.546
Organizational Commitment	OC1 OC2 OC3	.869 .893 .844	.927	.904	.758
Compliance Intention	CI1 CI2 CI3	.761 .762 .782	.954	.939	.836

Table 4. Result for Discriminant Validity

Constructs	1	2	3	4	5	6	7
Security Policy	***.843***						
Security System	.658**	***.876***					
Technical Support	.283**	.249**	***.775***				
Work Impediment	-.410**	-.371**	-.180**	***.739***			
Non visibility	-.100	-.152**	-.130*	.223**	***.738***		
Organizational Commitment	.484**	.454**	.280**	-.263**	-.215**	***.871***	
Compliance Intention	.668**	.569**	.219**	-.350**	-.172**	.707**	***.914***

Note: Values in bold type along the diagonal indicate the square root of the AVE
**: p 〈 0.01

마지막으로, 공통방법편의(common method bias) 문제에 대한 검증을 실시하였다. 공통방법편의는 설문조사를 통한 실증 분석 시 잘 나타나는 문제로서, 다중 항목을 통해 하나의 요인을 측정하고, 독립변수와 종속변수를 동일한 측정도구를 활용하였을 때 결과의 이상치가 발생하는 문제를 지칭한다. 공통방법편의 문제에 대한 검증 기법은 연구자별 다양하게 제시하고 있으나, 일반적으로 활용되는 단일방법요인기법(single-method-factor approaches)을 적용하였다[50]. 본 기법은 확인적요인분석에 단일요인을 추가 적용했을 때, 측정도구들의 변화량을 통해 문제 수준을 파악하는 기법이다. 분석 결과, 단일 요인을 적용하지 않았을 때와 적용했을 때의 모형의 적합도는 요구사항에 적합한 것으로 나타났으며(단일요인 미적용 모델 적합도(x^2/df = 1.725, GFI = 0.931, AGFI = 0.904, CFI = 0.986, NFI = 0.968, RMSEA = 0.044), 단일모형 적용 모델 적합도(x^2/df = 1.407 GFI = 0.951, AGFI = 0.922, CFI = 0.993, NFI = 0.977, RMSEA = 0.033)), 각 모델의 측정 도구들의 차이가 0.2보다 낮게 나타나 공통방법편의 문제는 낮은 것으로 판단되어, 구조방정식모델링을 통한 가설검증을 실시한다.

4.2 구조모형 평가

가설검증을 위한 구조모형 평가는 우선 연구 모델을 구조화한 모형의 적합도 분석을 실시한다. 적합도 분석에 문제가 없을 경우, 경로계수(β) 기반의 연구 모델의 영향관계를 상호간에 분석하고, 종속변수가 가지는 영향력 분석을 제시하기 위한 경로계수(R^2) 분석을 실시한다. 첫째, 공변 통제 없이 적합도 검증을 실시하였다. 구조모형 평가를 위한 적합도 요구사항은 앞서 실시한 확인적 요인분석의 요구사항과 동일한 기준으로 검토하였으며, 구조 모형의 적합도는 AGFI와 RMSEA값이 조금 낮게 나타났으나, 전체적으로 적정한 것으로 나타났다(x^2/df = 2.402, GFI = 0.908, AGFI = 0.877, CFI = 0.973, NFI = 0.954, RMSEA = 0.061).

둘째, Table 5에서와 같이 경로계수 분석을 통한 연구 모형 기반의 가설검증을 실시하였다.

연구가설 1은 조직원의 조직몰입은 정보보안 준수의도에 긍정적인 영향을 준다는 것으로서, 경로분석을 실시한 결과 조직 몰입과 준수의도간에는 긍정적 영향관계를 형성하는 것으로 나타났다(H1: β= 0.654, p〈0.01). 이러한 결과는 개인과 조직간의 관계에서 개인이 조직의 목표와 일치하고자 하는 조직몰입 수준이 높아질수록, 능동적으로 자신의 업무 등 성과달성을 위한 노력을 더 많이 한다는 선행연구[15]와 동일한 결과이다. 이러한 결과는 조직원의 정보보안 준수행동이 단순히 조직차원의 지원에 의해서 발현되는 것이 아니라, 조직구성원으로서 조직과 함께하는 공동의 목표의식을 보유하고 있을 때, 조직이 제시하는 정보보안 목표 행동을 자발적으로 할 수 있음을 의미한다. 따라서, 개인의 정보보안 행동은 조직과 동일시하고자 하는 개인의 의식 전환이 이루어질 때 형성될 수 있으며, 조직 몰입을 높이기 위한 조직차원의 노력이 필요함을 제시한다.

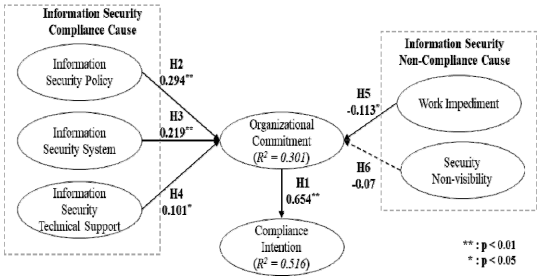

Fig. 2. Results of the Structural Model

연구가설 2는 정보보안 정책 지원이 조직원의 조직 몰입에 긍정적인 영향을 미친다는 것으로서, 경로분석을 실시한 결과 정보보안 정책과 조직 몰입간에는 긍정적 영향관계를 형성하는 것으로 나타났다(H2: β= 0.294, p〈0.01). 이러한 결과는 정보보안 정책 및 규정 정립이 조직원의 조직동일시 및 가치 형성에 긍정적인 영향을 준다는 선행연구[30]와 동일한 결과이다. 즉, 조직 내 엄격하고 누구나 동일하게 지켜야하는 보안 정책이 제정되고 실시될 경우, 조직원은 조직 내 구성원으로 지켜야할 가치 및 목표를 더욱 잘 이해할 수 있고, 조직에 몰입할 수 있게 되는 것을 의미한다. 따라서, 보안 정책을 명확하게 제시하고 지원하는 것이 조직원의 몰입 형성에 도움을 준다.

연구가설 3은 정보보안 시스템 지원이 조직원의 조직 몰입에 긍정적인 영향을 미친다는 것으로서, 경로분석을 실시한 결과 정보보안 시스템과 조직 몰입간에는 긍정적 영향관계를 형성하는 것으로 나타났다(H3: β= 0.219, p〈0.01). 이러한 결과는 조직 내 정보보안 시스템 구축 및 지원은 조직원의 보안 관련 태도 형성에 긍정적인 영향을 준다는 선행연구[36]와 유사한 결과로서, 조직 내 모든 구성원이 표준화된 보안 시스템을 통한 보안 행동을 요구받을 경우, 조직이 요구하는 보안 관련 행동 수준을 명확하게 알 수 있어 보안 관련 몰입 수준이 높아지는 것을 의미한다.

Table 5. Summary of Hypothesis Tests

	Path	Coefficient	t-value	Results
H1	OC → CI	.654	15.743**	Support
H2	SP → OC	.294	4.65**	Support
H3	SS → OC	.219	3.562**	Support
H4	TS → OC	.101	2.02*	Support
H5	WI → OC	-.113	-2.464*	Support
H6	NV → OC	-.07	-1.269	Reject

**: p 〈 0.01, *: p 〈 0.05
SP(Security Policy), SS(Security System), TS(Technical Support), WI(Work Impediment), NV(Non visibility), OC(Organizational Commitment), CI(Compliance Intention)

연구가설 4는 정보보안 기술적 지원이 조직원의 조직 몰입에 긍정적인 영향을 미친다는 것으로서, 경로분석을 실시한 결과 정보보안 기술적 지원과 조직 몰입간에는 긍정적 영향관계를 형성하는 것으로 나타났다(H4: β= 0.101, p〈0.05). 이러한 결과는 조직 내 IT 시스템에 대한 기술적 지원이 개인의 조직에 대한 몰입을 높여, IT 만족도 및 직업 만족도에 긍정적인 영향을 미친다는 선행연구[41]와 동일한 결과이다. IT 기술에 대한 효율적 활용을 위해서는 헬프데스크 및 매뉴얼 등을 지속적으로 보급하고 지원함으로써 조직원들이 IT 기술에 대한 가치를 인식하게 하는 것이 필요하다. 정보보안의 경우 보다 다각적인 절차적 행동을 요구하기 때문에, 정보보안 기술에 대한 지원을 실시할수록 조직의 보안 목표 및 행동 수준에 대한 명확한 이해를 할 수 있음을 의미한다.

연구가설 5는 정보보안 관련 업무장애는 조직 몰입에 부정적인 영향을 미친다는 것으로서, 경로분석을 실시한 결과 정보보안 관련 업무장애와 조직 몰입간에는 부정적 영향관계를 형성하는 것으로 나타났다(H5: β= -0.113, p〈0.05). 이러한 결과는 정보보안에서 업무 장애가 보안 관련 비용을 발생시켜 준수의도에 부정적인 영향을 미친다는 선행연구[17], 업무장애가 보안 관련 태도를 감소시킨다는 선행연구[16]과 유사한 결과이다. 개인에게 주어진 본연의 업무와 정보보안 업무는 일반적으로 일치하지 않는 경향이 있는데, 이러한 부분을 개인들은 보안 관련 비용으로 인식하는 경향이 있다. 또한, 추가적으로 발생한 업무는 기존 본인의 업무 성과 달성에 어려움을 줄 수 있는데, 이럴 때, 보안 관련 업무 때문에 장애가 발생한다고 판단한다. 업무장애는 보안 준수에 부정적인 영향을 주는데, 연구 분석 결과 조직 몰입을 감소시킴으로써, 보안 준수 행동을 낮추는 역할을 한다. 따라서, 조직은 정보보안이 개인의 업무에 장애로서 인식되지 않도록 지원하는 것이 필요하다.

연구가설 6은 정보보안 비가시성은 조직 몰입에 부정적인 영향을 미친다는 것으로서, 경로분석을 실시한 결과 정보보안 관련 비가시성과 조직 몰입간에는 부정적 영향관계를 형성하지 않는 것으로 나타났다(H6: β= -0.07, p〉0.05). 이러한 결과는 정보보안 가시성이 조직원의 정보보안 미준수 행동 원인을 감소시킨다는 선행연구[16]와 일치하지 않은 결과이다. 조직의 정보보안 요구사항은 지속적으로 조직원들에게 노출됨으로써, 조직원들이 보안 정책 및 행동 방식에 대하여 이해할 수 있도록 하는 것이 중요한데[44], 본 연구 결과는 조직 내 정보보안 관련 정보 노출의 부족한 상황이 조직 몰입에 큰 영향을 주

지 못한다는 것을 의미한다. 이러한 결과는 우리나라의 경우 일반적으로 정보보안 관련 캠페인이 지속적으로 이루어지기 보다는, 보안 시스템 기반 행동 억제 요인 기반의 정책을 통해 정보보안을 추구하려는 경향이 있기 때문에 정보보안 관련 메시지의 중요성을 고려하지 않기 때문인 것으로 판단된다.

마지막으로, 종속변수가 가지는 영향 분석을 실시하였다. 연구는 결정계수 분석을 통하여 구조모형에서 종속변수에 대한 독립변수들의 영향력을 도출하였다. 정보보안 준수의도는 조직몰입의 51.6%의 설명력을 가지고 있는 것으로 나타났으며, 조직몰입은 정보보안 정책, 정보보안 시스템, 정보보안 기술적 지원, 그리고, 업무 장애의 30.1%의 영향력을 가지는 것으로 나타났다.

5. 결론

5.1 연구의 요약

세계적으로 조직의 정보보안 기술에 대한 투자의 증대는 정보 관리 중요성이 높아지고 있음을 제시하는 것으로, 조직들은 정보 보호를 위한 시스템 구축 등 다각적 노력을 하고 있다. 하지만, 조직 내부의 보안 노출 사고 위협은 지속적으로 발생하고 있어, 조직구성원들의 정보보안 준수 향상을 위한 방법을 제시하는 것이 필요한 상황이다.

본 연구는 조직 내 환경적인 특성에 따라, 조직원의 정보보안 준수 및 미준수에 영향을 미치는 요인을 복합적으로 살펴봄으로써, 구성원들의 자발적인 정보보안 행동을 위한 지속적 지원 조건과 제어 조건을 제시하는 것을 목적으로 한다. 정보보안 준수 요인으로서 조직에서 구축 및 지원하는 정보보안 정책, 정보보안 시스템, 정보보안 기술적 지원 요인을 제시하였으며, 정보보안 미준수 요인으로서 정보보안으로 인한 업무장애 요인과 조직 내 정보보안 비가시성요인을 제시하였다. 각 선행요인들은 조직 몰입에 긍정 및 부정적 영향을 미쳐 준수의도에 영향을 줄 것으로 판단하여, 연구모델 및 가설을 제시하였다.

연구가설 검증은 구조방정식모델링을 적용하여 실증분석을 하고자 하였으며, 설문지 기법을 적용하되, 정보보안 정책을 도입한 기업에서 근무하는 조직원들을 주요 대상으로 설문을 실시하였다. 총 346개의 데이터를 활용하여 실증검증을 실시하였으며, 설문의 신뢰성 및 타당성 검증 결과 문제가 없어 AMOS 22.0을 활용하여 구조 모델을 검증하였다. 분석 결과 조직원의 보안 준수요인인 보안 정책, 보안 시스템, 보안 기술적 지원은 조직몰입에 긍정적인 영향을 미치는 것을 확인하였으며, 업무장애가 조직몰입을 감소시키는 요인임을 확인하였다. 또한, 복합적으로 형성된 조직 몰입은 정보보안 준수의도에 긍정적인 영향을 주는 요인임을 도출하였다.

5.2 연구의 시사점

본 연구는 조직 내부의 정보보안 준수 행동관점에서 이론적, 실무적 시사점을 지닌다.

첫째, 정보보안 준수 관련 선행요인을 조직 보안 환경 관점에서 다각적으로 제시하였다. 정보보안 준수요인으로 정보보안 정책 지원, 정보보안 시스템 지원, 그리고 정보보안 기술적 지원 요인으로 세분화하여 제시하였다. 정보보안 정책은 구성원들이 공통적으로 행동하고 지켜야 할 규정으로서, 명확한 보안 정책 수립 및 지원은 조직원의 정보보안 준수에 긍정적인 영향을 미치는 것을 확인하였다. 정책과 더불어, 조직 특성을 반영한 시스템 개발 및 지원은 업무의 표준 프로세스에 정보보안 분야를 적용한 것이기 때문에, 조직원들이 반 강제적으로 보안 기술을 업무에 적용해야하는 것을 의미하며, 조직 몰입에 긍정적인 영향을 주는 것을 확인하였다. 더불어, 정보보안 관련 기술적 지원이 조직몰입을 거쳐 정보보안 준수의도에 긍정적인 영향을 주는 것을 밝혔는데, 보다 효율적으로 정보보안 정책 및 기술을 업무에 적용하기 위한 헬프데스크 운영의 중요성을 제시한 것이다. 다시 말해, 조직원들이 조직에서 추구하는 정보보안 방향 및 목적을 이해하고 맞추어 행동할 수 있도록 보안 정책, 시스템, 그리고 기술적 지원을 지속적으로 지원하는 것이 개개인의 보안 관련 조직 몰입 수준을 높여, 준수의도를 향상시키는 것을 증명하였다.

따라서, 이론적 관점에서 본 연구는 정보보안 준수에 긍정적 영향을 주는 환경적 특성 요인을 제시하고 조직몰입-준수의도간의 연관성을 검증하였다는 측면에서 연구적 시사점을 가진다. 또한, 실무적 관점에서 정보보안 정책, 시스템, 그리고 기술적 지원과 같이 조직이 추구하는 보안 관련 목표 및 행동적 절차 등의 정보를 체계적으로 제공할 경우 개인의 조직 몰입을 통해 준수의도에 긍정적 영향을 주는 것을 확인하였다. 즉, 보안 관련 표준 프로세스 구축(정책, 시스템) 및 효율적 활용(헬프데스크)을 위한 조직차원의 지원이 개인의 자발적인 보안 준수에 필요함을 제시하였다는 측면에서 실무적 시사점을 가진다.

둘째, 정보보안 미준수 선행요인을 개인을 둘러싼 조직 환경적 측면에서 제시하였다. 업무 장애와 보안 비가시성 요인을 선행연구를 통해 도출하였으며, 업무장애가 조직몰입을 감소시켜 준수의도에 부정적 영향을 미치는 요인임을 증명하였다. 조직 내 개인에게 주어진 업무 성과는 일반적으로 보안 준수가 아닌 개별 직무의 목표달성에 있다. 따라서, 정보보호를 위하여 보안 정책, 시스템 등의 구축은 개인의 업무 환경을 복잡하게 만드는 요인이 된다. 결과는 업무장애의 부정적 영향을 검증하였다.

이론적 관점에서 연구는 정보보안을 위하여 추가적으로 발생하는 업무적 특성이 정보보안 준수행동에 부정적 영향을 줄 수 있는 요인임을 증명하였다는 측면에서 시사점을 가진다. 또한, 조직에서 정보보안 기술에 대한 투자는 보다 엄격한 보안 정책 및 시스템 구축 등을 보장한다. 하지만, 조직원에게는 업무장애를 일으킬 수 있는 요인이 될 수 있다. 따라서, 조직은 정보보안 기술 및 정책 도입 시, 개인의 업무에 대한 효율성과 보안 업무의 효과성을 함께 고려하고 전략을 수립해야함을 조직 보안 실행 측면에서 제시하였다.

본 연구는 다음과 같은 측면에서 연구의 한계점을 가지며, 향후 연구의 방향을 제시하고자 한다. 첫째, 본 연구는 조직원의 정보보안 준수의도에 미치는 준수요인과 미준수요인을 복합적으로 살펴보고 시사점을 제시하기 위하여, 설문 대상을 정보보안 정책을 도입한 기업에서 재직중인 근로자들을 선정하고, 임의적으로 대상기업에 근무하는 근로자로부터 데이터를 확보하였다. 하지만, 업종별, 직무별 정보보안 정책 및 시스템 구축의 수준 차이가 발생할 수 있으며, 이에 따라 조직원의 준수 행동은 차이가 발생할 수 있다. IT 기업의 경우 데이터가 기업에게 매우 높은 가치를 발생시키는 요인이지만, 제조업의 경우 정보의 가치가 상대적으로 적다. 또한, 영업부서와 기업 내근직 등은 정보의 가치와 성과의 가치를 다르게 인식할 수 있다. 따라서, 업종별, 직무별 차별화된 연구를 실시한다면, 보다 깊이 있는 연구의 시사점을 가질 수 있을 것으로 판단된다.

둘째, 연구는 조직 환경적 관점에서의 정보보안 준수, 미준수요인을 제시하였다. 조직에서 지원하는 보안 관련 현황을 파악하기 위하여, 설문대상자의 응답 당시의 생각을 기반으로 수준을 파악하고 연관성을 제시하였다. 하지만, 보다 명확한 조직의 보안 환경 특성의 영향력을 파악하기 위해서는 실험적 환경 기반의 행동을 파악하는 것이 필요할 것으로 판단된다. 따라서, 향후 연구에서는 보안 정책, 시스템 지원, 기술적 지원, 업무장애, 비가시성과 같은 선행 조건에 대한 상황 기반의 연구를 통해 시사점을 제시하는 것이 필요하다.

마지막으로, 국내 조직 환경은 일반적으로 수직적 조직 구조를 기반으로 운영하고 있다. 최근 IT기업들을 중심으로 수평적 조직을 구축하고 혁신을 추구하는 기업들이 배출되고 있다. 이렇게 변화하는 조직 환경에 따라 개인들의 정보보안 준수행동은 변화할 것으로 판단된다. 따라서, 향후 연구에서는 조직 문화를 결정하는 구조, 특성 등을 고려한 연구가 필요하며, 각 연구별 세부적 시사점을 제시할 수 있을 것으로 판단된다.

REFERENCES

[1] Grandviewresearch. (2019). Cyber security market size, share & trends analysis report by component, by security type, by solution, by service, by deployment, by organization, by application, and segment Forecasts. 2019 - 2025. https://www.globenewswire.com

[2] Gartner. (2019). A look at cyber-security spending in 2019: Where budgets are increasing and why.

[3] Verizon. (2019). 2019 data breach investigations report.

[4] J. D'Arcy & P. L. Teh. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management, 56(7),* 103151. DOI : 10.1016/j.im.2019.02.006.

[5] I. Hwang, R. Wakefield, S. Kim & T. Kim. (2019). Security awareness: The first step in information security compliance behavior. *Journal of Computer Information Systems,* 1-12. DOI: 10.1080/08874417.2019.1650676

[6] H. Lee & J. Kim. (2018). A convergence study on the structural relationships among emotional labor and work performance of information security professionals. *Journal of the Korea Convergence Society, 9(1),* 67-74. DOI : 10.15207/JKCS.2018.9.1.067.

[7] R. West. (2008). The psychology of security. *Communications of the ACM, 51(4),* 34-40. DOI : 10.1145/1330311.1330320.

[8] M. I. Merhi & P. Ahluwalia. (2019). Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior, 92,* 37-46. DOI : 10.1016/j.chb.2018.10.031

[9] N. S. Safa, C. Maple, S. Furnell, M. A. Azad, C. Perera,

M. Dabbagh & M. Sookhak. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organizations. *Future Generation Computer Systems, 97,* 587-597. DOI : 10.1016/j.future.2019.03.024.

[10] H. L. Chou & C. Chou. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65,* 334-345. DOI: 10.1016/j.chb.2016.08.034.

[11] C. Posey, T. L. Roberts & P. B. Lowry. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32(4),* 179-214. DOI : 10.1080/07421222.2015.1138374.

[12] Z. Ahmad, T. S. Ong, T. H. Liew & M. Norhashim. (2019). Security monitoring and information security assurance behavior among employees. *Information & Computer Security, 27(2),* 165-168. DOI : 10.1108/ICS-10-2017-0073

[13] S. Aurigemma & T. Mattson, (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information and Computer Security, 25(4),* 421-436. DOI : 10.1108/ICS-11-2016-0089.

[14] J. D'Arcy, T. Herath & M. K. Shoss. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems, 31(2),* 285-318. DOI : 10.2753/MIS0742-1222310210.

[15] I. Hwang & O. Cha. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior, 81,* 282-293. DOI : 10.1016/j.chb.2017.12.022.

[16] I. Hwang, D. Kim, T. Kim & S. Kim. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance, *Online Information Review, 41(1),* 1-17. DOI : 10.1108/OIR-11-2015-0358

[17] B. Bulgurcu, H. Cavusoglu & I. Benbasat. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly, 34(3),* 523-548.

[18] N. S. Safa & R. Von Solms. (2016). An information security knowledge sharing model in organizations, *Computers in Human Behavior, 57,* 442-451. DOI : 10.1016/j.chb.2015.12.037

[19] L. J. Williams & S. E. Anderson. (1991). Job satisfaction and organizational commitment as predictors of organizational citizenship and in-role behaviors. *Journal of Management, 17(3),* 601-617. DOI : 10.1177/014920639101700305.

[20] R. Mowday, L. Porter & R. Steers. (1982). *Employee-organizational linkages: The psychology of commitment, absenteeism and turnover.* New York: Academic Press.

[21] N. J. Allen & J. P. Meyer. (1996). Affective, continuance, and normative commitment to the organization: An examination of construct validity. *Journal of Vocational Behavior, 49(3),* 252-276. DOI : 10.1006/jvbe.1996.0043.

[22] J. P. Meyer, D. J. Stanley, L. Herscovitch & L. Topolnytsky. (2002). Affective, continuance, and normative commitment to the organization: A meta-analysis of antecedents, correlates, and consequences. *Journal of Vocational Behavior, 61(1),* 20-52. DOI : 10.1006/jvbe.2001.1842.

[23] N. S. Safa, C. Maple, T. Watson & R. Von Solms. (2018). Motivation and opportunity based model to reduce information security insider threats in organizations. *Journal of Information Security and Applications, 40,* 247-257. DOI : 10.1016/j.jisa.2017.11.001.

[24] T. Herath & H. R. Rao. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems, 18(2),* 106-125. DOI : 10.1057/ejis.2009.6.

[25] S. Sharma & M. Warkentin. (2019). Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security, 87,* 101397. DOI : 10.1016/j.cose.2018.09.005.

[26] M. E. Whitman. (2004). In defense of the realm: understanding the threats to information security. International *Journal of Information Management, 24(1),* 43-57. DOI : 10.1016/j.ijinfomgt.2003.12.003.

[27] J. D'Arcy, A. Hovav & D. Galletta. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach, *Information Systems Research, 20(1),* 79-98. DOI : 10.1287/isre.1070.0160

[28] M. Yim. (2018). An exploratory research on factors influence perceived compliance cost and information security awareness in small and medium enterprise, *Journal of the Korea Convergence Society, 9(9),* 69-81, DOI : 10.15207/JKCS.2018.9.9.069.

[29] K. J. Knapp, R. F. Morris Jr, T. E. Marshall & T. A. Byrd. (2009). Information security policy: An organizational-level process model. *Computers & security, 28(7),* 493-508. DOI : 10.1016/j.cose.2009.07.001.

[30] K. Chung & E. Chang. (2005). Family-friendly polices and employee's organizational commitment, *Family and Culure, 17(1),* 59-84

[31] S. C. Eaton. (2003). If you can use them: Flexibility policies, organizational commitment, and perceived performance. *Industrial Relations: A Journal of Economy and Society, 42(2),* 145-167. DOI : 10.1111/1468-232X.00285

[32] L. F. Kwok & D. Longley. (1999). Information security

management and modeling. *Information Management & Computer Security, 7(1),* 30-39.
DOI : 10.1108/09685229910255179.

[33] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius & M. Pattinson. (2017). Individual differences and information security awareness. C*omputers in Human Behavior, 69,* 151-156.
DOI : 10.1016/j.chb.2016.11.065.

[34] E. Y. Yildirim, G. Akalp, S. Aytac & N. Bayram. (2011). Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management, 31(4),* 360-365.
DOI : 10.1016/j.ijinfomgt.2010.10.006.

[35] A. Da Veiga & J. H. Eloff. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29(2),* 196-207.
DOI : 10.1016/j.cose.2009.09.002.

[36] P. Shum, L. Bove & S. Auh. (2008). Employees' affective commitment to change. *European Journal of Marketing, 42(11/12),* 1346-1371.
DOI : 10.1108/03090560810903709.

[37] I. Cardoso & M. Caldeira. (2012). *Users' commitment in information system implementation: The role of technological frames*. In Mediterranean Conference on Information Systems (pp. 254-266). Springer, Berlin, Heidelberg.

[38] A. M. Fuglseth & Ø. Sørebø. (2014). The effects of technostress within the context of employee use of ICT. *Computers in Human Behavior, 40,* 161-170.
DOI : 10.1016/j.chb.2014.07.040.

[39] T. S. Ragu-Nathan, M. Tarafdar, B. S. Ragu-Nathan & Q. Tu. (2008). The consequences of technostress for end users in organizations: Conceptual development and empirical validation. *Information Systems Research, 19(4),* 417-433.
DOI : 10.1287/isre.1070.0165.

[40] M. Tarafdar, Q. Tu, T. S. Ragu-Nathan & B. S. Ragu-Nathan. (2011). Crossing to the dark side: Examining creators, outcomes, and inhibitors of technostress. *Communications of the ACM, 54(9),* 113-120. DOI : 10.1145/1995376.1995403.

[41] R. K. Jena. (2015). Technostress in ICT enabled collaborative learning environment: An empirical study among Indian academician. *Computers in Human Behavior, 51,* 1116-1123.
DOI: 10.1016/j.chb.2015.03.020.

[42] N. G. Carr. (2003), IT doesn't matter. *Harvard Business Review, 81(5),* 41-49.

[43] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen & A. Vance. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems, 18(2),* 126-139.
DOI : 10.1057/ejis.2009.10.

[44] M. Siponen, S. Pahnila & M. A. Mahmood. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43(2),* 64-71.
DOI : 10.1109/MC.2010.35.

[45] M. Aryeetey & A. Sanda. (2012). Understanding Employees' Perspective of Quality of Work Life Indicators in Ghanaian Organizations. *International Journal of Contemporary Business Studies, 3(3),* 17-30.

[46] S. M. Lee, S. G. Lee & S. Yoo. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41(6),* 707-718.
DOI : 10.1016/j.im.2003.08.008

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

[48] B. H. Wixom & H. J. Watson. (2001). An empirical investigation of the factors affecting data warehousing success. *MIS Quarterly, 25(1),* 17-41.
DOI : 10.2307/3250957.

[49] C. Fornell & D. F. Larcker. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18(1),* 39-50.
DOI: 10.2307/3151312.

[50] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee & N. P. Podsakoff. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88(5),* 879-903.
DOI : 10.1037/0021-9010.88.5.879.

황 인 호(Hwang, In Ho) [종신회원]

· 2004년 8월 : 건국대학교 경영학과(경영학사)
· 2007년 6월 : 중앙대학교 경영학과(경영학석사)
· 2014년 2월 : 중앙대학교 경영학과(경영학박사)
· 2018년 7월 ~ 2020년 8월 : 한국산업기술대학교 창업교육센터 연구교수
· 2020년 9월 : 국민대학교 교양대학 조교수
· 관심분야 : IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야 등
· E-Mail : hwanginho@kookmin.ac.kr

허 성 호(Hu, Sung Ho) [종신회원]

· 2004년 2월 : 홍익대학교 신소재공학과(공학사)
· 2006년 2월 : 중앙대학교 심리학과(문학석사)
· 2012년 8월 : 중앙대학교 심리학과(문학박사)
· 2016년 3월 ~ 현재 : 한양대학교 산업융합대학원 겸임교수
· 2020년 3월 ~ 현재 : 블라인드 공채 채용심사 전문요원
· 관심분야 : 정보문화, 융합연구, 고령화, 빅데이터, 채용경향, 공동체 분야 등
· E-Mail : powerrcy@hanmail.net