「정보시스템연구」 제29권 제1호
한국정보시스템학회
2020년 3월, pp. 23~50
http://dx.doi.org/10.5859/KAIS.2020.29.1.23

조직 내 정보보안 기술스트레스 완화와 준수의도*

황인호** · 허성호***

〈목 차〉

Ⅰ. 서 론

조직 내 정보 관리가 조직의 가치 향상에 중요한 관건으로 자리 잡으면서, 많은 조직들은 각종 정보보안 관련 하드웨어, 소프트웨어, 그리고 서비스 등에 투자 및 적용을 하고 있다(Hwang et al., 2017). 실제로, 전 세계 정보보안 관련 시장 규모는 2018년 1,165억 달러에 이르며, 2025년까지 연평균성장률 11.0%에 달할 것으로 판단되고 있다(Grandviewresearch, 2019). 또한, 전 세계의 정보보안 시장의 중심에는 약 50% 수준에 달하는 기업 정보보안 시스템이 있으며, 정보 가치의 중요성에 따라 기업들의 보안 기술 구축 수요는 지속적으로 증가하고 있다(Grandviewresearch, 2019). 하지만, 조직 정보보안 사고의 대부분은 정보보안 수준을 높게 가져가고 있는 공공부문, 금융 부문, 엔터테인먼트 부문 중심으로 발생하고 있어(Verizon, 2019), 정보보안을 위한 조직들의 관심이 더욱 필요한 상황이다.

* 이논문 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임. (NRF-2018R1D1A1B07050305)
** 한국산업기술대학교, inho1998@kpu.ac.kr(주저자)
*** 중앙대학교 심리학과, powerrcy@daum.net(교신저자)

조직의 정보보안 사고는 연구자별 다양하게 제시하고 있는데, 일찍이 조직의 정보 노출 위협 요인을 제시한 Loch et al.(1992)는 보안 사고 유형을 행위주체(인간, 비인간)와 침입 경로(내부, 외부)의 관점으로 총 4개의 유형을 제시하였다. 비인간-외부 유형은 일반적으로 자연재해에 의해 발생하는 유형으로 보안 관리를 위한 조직 노력 만으로 해결하기 어려운 유형이다. 비인간-내부 유형과 인간-외부 유형은 해킹 등 기술적 침입을 통하여 보안 사고 위협이 발생하는 경우로서, 사전 대응을 위한 시스템적 개선을 통하여 해결할 수 있다. 인간-내부 유형은 보안 사고 수준에 따라 차이가 있지만, 조직 내 구성원의 미준수 행동에 따라 발생하는 경우이다. West(2008)는 조직의 정보보안 사고 예방 노력 중 가장 어려운 것이 사람 행동에 대한 통제 및 관리라고 보았다. 그는 조직원의 정보보안 준수 행동은 조직과의 대리인 문제에 있으며, 보안 행동의 정보를 조직원이 조직보다 더욱 많이 가지고 있기 때문에 관리가 어렵다고 하였다. 또한, 그는 조직원에게 있어 정보보안의 목표가 개인에게 주어진 본연의 업무적 목표가 아니기 때문에 심리적인 관점에 의해 준수 행동을 결정할 가능성이 높아 보안 준수가 상대적으로 어렵다고 보았다. 즉, 내부자에 의한 정보보안 준수는 조직에서 도입한 기술 및 규정 등 조직의 요구사항을 구성원들이 고려하지만, 자신의 상황에 맞춰서 행동하고 의미를 부여하려는 심리적 의지가 있기 때문에, 조직원 개개인의 보안 행동을 통제 및 관리하기 어려워 정보보안 사고를 지속적으로 발생시키는 유형이다 (Siponen et al., 2010).

실제로 Verizon(2019)이 발표한 지난 10년간의 전 세계 조직들의 정보보안 사고 유형을 살펴보면, 가장 많은 보안 사고 원인은 해킹과 같이 외부 침입에 의한 유형으로 매년 전체의 60~70%의 수준을 유지하고 있다. 그리고 조직 내부자에 의한 보안 사고가 약 20~30% 수준, 외부 파트너에 의한 사고가 5%에 달하는 것으로 나타났다. 그런데, 최근 내부자에 의한 정보보안 사고가 증가하고 있는 추세이며, 해킹 등 침입에 의한 사고는 감소하는 추세인 것으로 나타났다 (Verizon, 2019). 즉, 정보보안 불활실성이 높은 주체인 내부 구성원에 의한 정보보안 사고에 대한 대응책을 마련할 필요가 있다.

조직원의 정보보안 준수 행동과 관련된 선행연구들을 살펴보면, 조직원의 정보보안 준수행동의 개선을 위한 동기적 관점에서 접근하고 있다. 조직원의 보안 미준수 행동에 대한 제재(deterrence)를 중심으로 보안 목표 수준을 달성하고자 하는 연구(D'Arcy et al., 2009; Guo et al., 2011; Hwang and Lee, 2016; Safa et al., 2019), 개인이 가지는 공포 소구(fear appeal)를 통한 보안 관련 행동 동기를 높이고자 하는 보호동기(protection motivation theory)기반의 연구(Safa et al., 2015; Sommestad et al. 2014), 조직과 개인의 환경적 관계에서 개인에게 주어지는 외재적, 내재적 동기 향상을 통해 준수행동을 높이고자 하는 연구(Herath and Rao, 2009; Safa and Von Solms, 2016)들이 대표적으로 제시되어 실무적으로 활용되고 있다. 이들 선행연구들은 조직원들의 보안 준수 행동의 원인을 다각적 관점에서 제시함으로써 보안 준수행동을 높이기 위한 방향을 제시한 관점에서 시사점을 가진다.

하지만, 기존 연구들은 조직 관점에서 조직원의 보안 준수 행동 제어를 위한 기술적 통제 및 규범의 엄격함의 중요성을 높게 평가하여 접근하

였기 때문에, 조직의 보안 관련 환경적 변화에 의해 조직원에게 발생 가능한 부정적 동기 또는 행동에 대한 부분을 체계적으로 설명하지 못하고 있다. 특히, 최근 스마트 업무 환경 등을 위하여 도입된 기술적 변화 및 이에 대응하기 위한 보안적 기술 및 규정의 엄격함은 실제 기술을 적용해야하는 조직원들에게는 스트레스를 발생시키는 환경일 수 있는데(D'Arcy et al., 2014), 보안 관련 스트레스 원인 및 대처 방안에 대한 연구가 부족한 실정이다.

조직에서 도입하는 IT 기술은 업무 효율성 향상을 통한 조직의 목표 성과를 달성시키는 도구로서 높은 역할을 하지만, 업무에 적용하는 조직원에게는 새로운 지식 확보 및 변화된 업무 표준 프로세스 적응 등 기존과는 다른 체계를 요구한다. 이때, 개인은 기술스트레스(techno stress)를 발생시키게 되는데(Brod, 1982), 개인 차원의 부정적 의미를 가지거나 성과 미달성 등 조직의 요구와는 다른 행동을 하게 하는 원인이 된다(Ragu-Nathan et al., 2008). 정보보안 분야는 특히 스트레스 발생 시 부정적 행동이 나올 가능성이 높은데, 정보보안 기술은 업무 공유 등 성과 향상을 위한 기존 IT 기술의 도구적 특성과는 달리 보안 목표에 따른 개인에 대한 행동적 통제를 요구하기 때문이다(Hwang and Cha, 2018; West, 2008). 즉, 보안 관련 기술의 도입을 통한 조직원 환경적 변화가 지속적으로 발생시 조직원은 관련 기술에 의한 스트레스가 발생할 가능성이 높고 이에 대한 해결책을 제시하여야 하는데, 스트레스의 부정적 영향과 스트레스 최소화를 위한 연구가 부족한 실정이다.

이에 본 연구는 정보보안 관련 기술 도입에 의한 스트레스 발생과 부정적 영향 관계, 그리고 스트레스 감소를 위한 방향을 제시하는 것을 목적으로 한다. 세부적으로, 정보보안 관련 기술 스트레스 요인(기술과부하, 불확실성)을 제시하고 보안 준수의도를 감소시키는 원인임을 찾는다. 이후, 정보보안 관련 기술 스트레스 완화를 위한 조직 차원의 노력 요인(정보보안 관련 기술적 지원)과 개인의 특성 요인(개인-조직 적합성)을 제시하고 영향 관계를 검증한다.

이를 통해 도출된 연구 시사점은 다음과 같다. 첫째, 정보보안 기술 도입 시 고려해야 할 구성원의 보안 준수 감소 요인(기술 스트레스)을 제시하고 실제 부정적 영향을 미치는지를 찾음으로써 보안 관련 기술스트레스 최소화의 필요성을 제시한다. 둘째, 조직 관점, 개인 관점에서 보안 관련 기술스트레스의 영향을 최소화하기 위한 방향을 제시하고 영향관계를 검증함으로써, 보안 관련 전략 수립의 방향을 제시한다.

Ⅱ. 이론적 배경

2.1 정보보안 준수의도

조직의 정보보안 시스템에 대한 투자가 지속적으로 증가하고 있지만, 정보보안 사고는 매년 높은 수준으로 발생하고 있다(Grandviewresearch, 2019). 조직의 정보보안 사고는 1차적으로 조직의 정보 노출이라는 문제를 발생시키지만, 2차적으로 관련 정보와 관련된 사람들의 프라이버시 침해 등 추가 문제를 발생시키기 때문에 특히 개인정보의 중요성이 높은 금융 및 공공 부문에서의 관심이 높다(Verzion, 2019). 그렇지만, 2018년 정보보안

사고의 16%가 공공 부문, 10%가 금융 부문일 정도로 높은 수준의 보안 관련 투자에도 불구하고, 지속적으로 보안 사고가 발생하고 있다. 정보보안 사고는 어느 하나의 요인만으로 발생하는 것이 아니라, 내부자의 협력과 외부 해킹 등이 연계되어서 발생하는 등 다양성이 매우 높다. 2018년 보안 사고 중 연계된 사고 중 사고의 주요 원인이 외부 해킹(69%)과 내부자에 의한 사고(34%)일 정도로 내부자 연계에 의한 보안 위협이 높은 상황이다(Verizon, 2019). 더욱이, 내부자에 의한 정보 노출 유형은 단순히 IT분야 근로자뿐만 아니라, 엔지니어, 임원, 사무직, 협력기업 직원 등 IT 시스템에 접속할 수 있는 권한이 부여된 사람이면 정보 노출이 가능하기 때문에 내부자에 대한 보안 관리 및 통제는 더욱 어려운 실정이다(유인진, 박도형, 2018; 황인호, 김상현, 2019; Hwang et al., 2017).

조직은 엄격한 정보보안 기술 및 정책을 도입하여 외부 해킹 등을 방어하고 내부 구성원들의 정보보안 준수 행동이 이루어지길 기대하지만, 조직원의 정보보안 준수 행동은 조직의 목표와 다르게 나타나는 등 내부자에 의한 불확실성이 존재한다(D'Arcy et al., 2014). 조직원들의 보안 관련 행동 통제의 불확실성이 높을수록 조직은 정보 관리에 어려움을 겪게 되고, 나아가 조직에 대한 수요자들의 반감 등의 문제로 발생되는 요인이 된다(황인호, 김승욱, 2017).

따라서, 조직원에 의한 정보 노출 위협 최소화를 위해서는 조직원의 자발적인 보안 준수 행동을 요구할 수 밖에 없으며, 보안 준수의도를 높이는 것이 중요하다(Chen et al., 2012).

정보보안 준수의도에 대한 개념을 살펴보면, Bulgurcu et al.(2010)은 조직의 잠재적 보안 위협으로부터 정보 및 기술 자원을 보호하기 위한 조직원의 의도로 정의하고 있으며, Vance et al.(2012)은 조직의 정보 자원을 외부와 내부의 위협들로부터 보호하고자 하는 조직원의 의도로 정의하고 있다. 즉, 정보보안 준수의도는 조직 외부 및 내부의 위협으로부터 정보 자원을 보호하고자 하는 구성원들의 의도이기 때문에, 준수의도는 조직원이 능동적으로 조직의 정보 자원을 보호하고자 하는 개념이다. 따라서, 내부자의 정보보안 위협을 최소화하기 위해서는 조직원의 정보보안 준수의도를 높이기 위한 선행적 노력이 필요하며, 조직원이 이러한 노력을 인지할 때 준수의도는 높아진다.

2.2 정보보안 관련 기술스트레스

2.2.1 기술스트레스(Techno-stress)

최근 많은 조직들은 정보관리 및 조직 내 업무 효율성 증대를 위하여 다양한 IT 기술을 도입하고 있으며, 조직원들에게 IT 기반의 표준화된 업무 프로세스를 요구하고 있다(Tarafdar et al., 2014). 개인을 둘러싼 조직의 환경과 개인의 가치 및 행동, 결과간의 불균형이 높아질 때 스트레스가 발생하며, IT 기술 환경에 의하여 개인이 받는 불균형으로 인한 피로감 등을 기술스트레스라고 한다(Ayyagari et al., 2011). 기술스트레스란 용어를 처음 제시한 Brod(1982)는 기술스트레스를 개인이나 조직이 새로운 기술의 도입 및 운영에 적응할 수 없어서 발생하는 상태의 결과로 정의하였으며, 조직 내 정보 기술의 발전에 따라 관련 기술 활용에 대한 요구가 지속적으로 개인에게 발생할 때, 누군가는 적응하지 못하는 상황

이 발생하고 스트레스 수준은 높아지게 된다(Ragu-Nathan et al., 2008).

조직 및 구성원의 업무 효율성 및 성과 향상 등의 목적으로 도입된 정보기술이 개인에게 과하다고 판단될 경우 스트레스가 발생되는데, 스트레스는 정신적, 신체적 문제를 발생시켜 해당 기술에 대한 회피, 조직에 대한 불만 등을 일으키는 부정적 요인이다(Tarafdar et al., 2014).

따라서, 기술스트레스가 발생 되지 않도록 하는 것이 필요하다. 연구자별로 발생 가능한 기술스트레스에 대한 세부적인 상황 또는 유형을 다양하게 제시하고 있는데, Ragu-Nathan et al. (2008)은 기술스트레스가 발생되는 유형을 5가지(기술과부하, 기술침해, 기술 복잡성, 기술 불안정성, 기술 불확실성)로 제시하고 있다. 첫째, 기술 과부하(techno overload)는 정보기술의 도입 등으로 업무 패턴의 변화, 그리고 더 빠르게 요구되는 업무 성과 등을 의미한다. 둘째, 기술침해(techno invasion)는 정보기술의 도입으로 개인의 생활을 침해받고, 새로운 기술 습득을 위하여 소비하는 시간 등을 의미한다. 셋째, 기술 복잡성(techno complexity)은 복잡한 기술 도입으로 인하여 새로운 업무 형태에 대한 능력 부족을 의미한다. 넷째, 기술 불안정성(techno insecurity) 기술이 유발하는 직업에 대한 불안감을 의미한다. 다섯째, 기술 불확실성(techno uncertainty)은 자신을 둘러싼 기술의 지속적인 변화로 인하여 기술에 대한 불확실성이 높아지는 수준을 의미한다.

2.2.2 정보보안 관련 기술스트레스

정보보안 분야에서도 사용자들에게 정보보안 관련 기술스트레스는 발생한다. 정보보안에 대한 요구 수준이 높아지는 만큼 조직에서 도입하는 보안 관련 기술 및 정책 수준 또한 높아지고 전문화된다(Guo and Yuan, 2012). 더불어, 많은 조직은 투자한 정보보안 관련 기술 및 설정된 내부 표준에 대하여 조직원의 충분한 학습을 통한 이행을 요구하고 있으며, 정보보안 위협 최소화를 위하여 보안 관련 조직원에 대한 물리적 통제를 실시하고 있다.

실제로, 조직들은 조직 내 다양한 정보보안 기술을 조직원들에게 적용하고 있다. 매체 제어 기술(개인 PC, USB 등 디바이스 통제)를 통한 데이터 생성, 활용에 대한 통제를 실시하고 있으며, 정보 검색 및 유출 차단 기술(메신저 및 웹하드 등 정보 기술 차단)을 통해 조직 내의 정보가 외부로 유출되는 것을 차단하고 있다. 또한, 문서에 대한 암호화, 문서에 대한 사용자 접근 권한 통제, 개인 PC 암호화 정책 및 네트워크 접근 통제 기술 등 다각적인 정보보안 기술을 도입하고 조직원들이 업무에 적용하도록 요구하고 있다.

전문화된 정보보안 시스템의 조직 내 도입은 안정적인 보안 체계 기술 기반의 프로세스 표준화를 추구함으로써, 반강제적인 보안 수준 강화 성과를 도출할 수 있다(Hwang et al., 2019). 하지만, 과도하고 급격한 정보보안 기술의 도입 및 행동에 대한 요구는 조직원의 기술스트레스를 일으키며, 보안관련기술스트레스(security related techno stress)라 한다(D'Arcy et al. 2014; Hwang and Cha, 2018). D'Arcy et al.(2014)은 보안 관련 스트레스를 내부 또는 외부의 보안 관련 요구로 인하여 발생되는 개인의 인지 및 능력 평가에 관련된 심리적 스트레스 유형으로 정의하고 있으며, Hwang and Cha(2018)는 보안 관련 기술스트레서(security

related stress creator)를 제시하면서, 조직의 정보보안 기술적 행동 요구와 개인의 기술에 대한 능력 차이에 발생하는 심리적 스트레스를 일으키는 수준으로 정의하고 있다. 즉, 보안 관련 기술스트레스는 보안 관련 요구에 의해 발생되는 개인의 심리적 스트레스 수준이다.

보안 관련 기술스트레스를 일으키는 상황 또는 요인을 D'Arcy et al.(2014)는 기존 Ragu-Nathan et al.(2008)이 제시한 기술스트레스 5개 요인 중 기술과부하, 기술복잡성, 기술불확실성을 적용하여, 보안 스트레스 상황에 대한 실증검증을 하였다. 그들은 기술 침해와 기술 불안정성은 제외하였는데, 보안 분야에 적용하여 실증검증을 한 결과 기술과부하와 해당 요인들이 부분적으로 일치하였고, 정보보안 구성항목에 적절하지 않다고 보았기 때문이다.

본 연구는 조직원이 받는 정보보안 관련 기술스트레스의 하위 요인으로 기술과부하와 기술불확실성을 적용한다. 기술복잡성은 조직에 도입한 보안 관련 기술의 변화 및 복잡성으로 인하여 인식하는 보안 복잡성에 대한 스트레스 수준으로 정의할 수 있는데, 기술불확실성 또한, 자신을 둘러싼 보안 기술적 변화로 인하여 느끼는 불확실성 수준이기 때문에, 유사성이 높다고 판단했기 때문이다. 따라서, 정보보안 관련 기술과부하는 보안 기술 도입으로 인하여 개인의 업무 수준이 증가함으로써 발생하는 스트레스 수준으로 정의하며, 정보보안 관련 기술불확실성은 정보보안 기술의 지속적인 변경으로 인하여 개인이 인지하는 불확실한 상황으로 정의한다.

1) 정보보안 관련 기술과부하

정보보안 관련 기술과부하에 대하여, D'Arcy et al.(2014)은 정보보안 관련 요구사항이 조직원의 업무를 증가시키고, 결과적으로 관련 업무를 완수해야 하는데 소요되는 추가적인 시간 및 노력에 대한 압박감으로 정의하였으며, Hwang and Cha(2018)는 사용자가 다루거나 업무 과중을 개선하기 어려운 상태의 정보보안 기술로서 정의하였다. 즉, 기술과부하는 개인의 업무에 정보보안 기술 도입으로 인하여 추가적인 업무가 발생함에 따라, 노력 및 시간을 소요하는 압박의 수준이다.

조직 내 보안관련 기술과부하는 다양한 형태로 나타날 수 있는데, 예를 들어, 문서화 작업 시 기존 문서 생성-변경-보관 등의 업무 프로세스 이외에 보안 관점에서의 문서 보호를 위한 문서별 보안 등급 생성, 승인 등의 절차를 수행하거나, 외부 파트너와의 업무적 협업 시 필요한 정보 교환, 공동 작업 등에서 보안 부서 또는 관리 권한자에 의한 사전적 동의가 필요하거나 특정 보안 시스템을 설치하여 활용해야 하는 경우가 발생한다. 즉, 조직원이 자신에게 주어진 업무적 목표 달성을 위하여 필요한 정보 생성, 활용, 그리고 타인 등과의 공유적 활동을 함에 있어서, 정보보안 기술 및 정책 수준에 맞는 추가적인 기술적(특정 하드웨어, 소프트웨어 활용 등), 정책적(보안 관리자 또는 권한자에 대한 사전 승인 등) 노력이 필요한데, 보안 기술이 엄격하게 도입될수록 조직원에게는 스트레스로 나타날 수 있다.

조직 내 도입한 기술에 의해 발생되는 기술과부하는 조직원에게 부여된 관련 목표 및 만족도 등에 부정적인 영향을 미치고 나아가 생산성과 같은 업무적 성과를 감소시키는 원인이 되는 선행요인이다(Gaudioso et al., 2017; Hung et

al., 2015; Ragu-Nathan et al., 2008; Tarafdar et al., 2014). Ragu-Nathan et al.(2008)은 조직 내 특정 기술의 최종사용자에게 발생하는 기술스트레스가 개인의 직무 만족도를 감소시키고, 조직 몰입까지 축소시키는 것을 실증분석을 통해 확인하였으며, Tarafdar et al.(2014)은 조직내 영업사원들의 기술스트레스 환경에 대한 연구를 통해 기술스트레스가 업무 스트레스를 발생시키고, 기술에 의한 성과를 감소시키는 선행요인임을 증명하였다. 또한, 정보기술의 목적인 협력, 공유를 위한 기술적 환경에서도 기술스트레스는 발생하는데, Jena(2015)는 기술스트레스가 조직몰입과 직무만족도를 감소시키고, 목표에 대한 부정적 행동과 성과 감소를 일으키는 선행요인임을 증명하였다. 특히, 기술스트레스 세부 요인인 기술과부하도 부정적 영향을 미치는 선행 조건인데, Hung et al.(2015)은 조직의 모바일 환경에서 발생가능한 기술적 스트레스 상황 중 기술 과부하와 커뮤니케이션 과부하가 개인의 업무 생산성을 감소시키는 원인이 되는 것을 확인하였다.

정보보안 분야에서도 기술과부하에 의해 발생한 스트레스는 개인의 정보보안 준수에 부정적인 영향을 준다(D'Arcy et al., 2014; Hwang and Cha, 2018). D'Arcy et al.(2014)은 조직의 정보보안 요구에 대한 개인들의 스트레스가 정보보안 회피의도에 미치는 영향 관계를 제시하였으며, 그들은 보안관련스트레스를 기술과부하, 기술복잡성, 기술불확실성을 활용한 2차요인을 도출하였으며, 보안관련스트레스가 회피의도에 긍정적 영향을 주는 요인임을 증명하였다. 또한, Hwang and Cha(2018)은 보안관련기술스트레서가 직무몰입을 감소시켜 보안 준수의도를 떨어뜨리는 영향관계를 제시하였으며, 실제 부정적 영향을 미치는 것을 확인하였다. 즉, 보안 관련 기술스트레스 세부요인인 기술과부하 또한 직접적으로 보안 준수의도에 부정적인 영향을 미칠 것으로 판단하고, 선행연구를 기반으로 다음과 같은 연구 가설을 제시한다.

H1. 정보보안 관련 기술과부하는 정보보안 준수의도에 음(-)의 영향을 줄 것이다.

2) 정보보안 관련 기술불확실성

정보보안 관련 기술 불확실성에 대한 개념을 살펴보면, D'Arcy et al.(2014)은 조직이 조직원의 업무와 관련된 보안 요구사항을 지속적으로 업데이트 하고 변경하는 상황 또는 수준으로 정의하였으며, Hwang and Cha(2018)은 조직에서 도입한 정보보안 기술의 지속적인 수준 향상 등으로 발생하는 기술에 대한 불확실성 수준으로 정의하였다. 즉, 보안 기술불확실성은 지속적으로 확대 또는 변경되는 보안 기술로 인하여 발생하는 불확실한 상황으로 정의할 수 있다.

조직의 정보관리에 대한 요구는 단순히 조직만의 문제가 아닌 사회적, 정책적 관점의 영향을 받는다(D'Arcy et al., 2019). 조직 외부 환경 변화 및 정보 보호에 대한 지속적인 요구사항의 발생은 국가 정책적으로 조직의 보안 관련 기술 및 규정의 변화를 요구한다. 예를 들어, 조직관점에서 스마트 워크나 모바일 기반의 직무의 증가는 통신 등 보안 관련 기술적 표준(가상 서버, 인증 등)을 요구하고, 제정된 기술적 표준은 조직의 보안 기술을 변경해야함을 의미한다. 산업분야에 새롭게 적용된 보안 기술은 주기적인 보안 교육 및 훈련이 필요하며, 적용된 보안 기술에 적정한 표준 프로세스 및 보안 요구사항을 조직원에게

요구한다.

또한, 사회적 관점에서 개인의 사생활과 관련된 소셜미디어의 활용 증대는 정보 노출 위협도를 증가시켰으며, 많은 조직은 자체 소셜미디어를 개발하거나 대표적인 소셜미디어의 활용을 조직 내 금지하는 규정을 시행하고 있다. 하지만, 개인들은 또 다른 소셜미디어를 활용하고 있으며, 조직은 이에 대한 제재 또는 기술적 향상을 통한 정보노출 방지를 위한 노력을 한다. 즉, 다양한 요인에 의한 조직 내외부의 정보 환경의 변화는 보안 기술의 변화를 가져오고, 점차 빨라지는 변화는 조직원의 기술불확실성을 야기한다(D'Arcy and Teh, 2019).

조직 내 지속적인 기술 변화로 인하여 발생되는 기술불확실성은 조직원의 부정적 행동을 야기하고 성과를 감소시키는 원인이 된다(Ayyagari et al., 2011; Jena, 2015; Oh and Park, 2016; Yan et al., 2013). Ayyagari et al.(2011)은 개인-기술의 부적합성에 의한 차이의 발생이 스트레스를 일으키고, 준수 행동에 영향을 준다고 하였으며, Yan et al.(2013)은 병원 내 원격 의료 커뮤니케이션 기술이 기술 수용 및 성과를 높이는 요인이지만, 과도한 기술적 변화는 스트레스를 일으켜 부정적 결과를 가져오는 원인이 된다고 보았다. Oh and Park(2016)은 기술스트레스는 개인의 업무와 삶의 갈등을 일으켜, 직무만족도를 감소시키는 원인임을 증명하였으며, Jena(2015)는 기술스트레스가 부정적 행동 및 기술관련 성과에 부정적 영향을 주는 선행 조건임을 증명하였다.

정보보안 분야에서도 기술불확실성은 조직원의 준수행동에 부정적인 영향을 주는 요인이다. D'Arcy et al.(2019)는 보안관련스트레스가 정신적 반응을 통해 정보보안 준수의도를 감소시키는 원인임을 개인이 가지는 반응의 유형별(피로(fatigue), 좌절(frustation)) 차이 분석을 함으로써 상호간의 관련성이 있음을 증명하였다. 또한, Hwang and Cha(2018)는 보안관련기술스트레스의 요인으로 기술불확실성을 적용하였으며, 보안관련 기술스트레스가 직무스트레스를 통한 조직몰입 간에 부분적인 매개효과가 있음을 증명하였다. 즉, 보안관련 기술스트레스 세부요인인 기술불확실성 또한 직접적으로 보안 준수의도에 부정적인 영향을 미칠 것으로 판단하고, 선행연구를 기반으로 다음과 같은 연구 가설을 제시한다.

H2. 정보보안 관련 기술불확실성은 정보보안 준수의도에 음(-)의 영향을 줄 것이다.

2.3 정보보안 기술적 지원

효율적인 정보관리 및 보호를 위해서는 정보보안 관련 기술 및 업무 표준 프로세스 등 규정 도입은 필수적이나(Steinbart et al., 2018), 엄격한 보안 기술의 도입 및 지속적 변경은 실 수요자이며 보안 관련 행동 주체인 조직원들에게는 보안 관련된 기술적 스트레스를 일으킬 수 있다. 조직원에게 발생 가능한 보안 관련 기술스트레스를 감소시켜 부정적 행동을 최소화하기 위해서는 조직 차원의 보안 기술에 대한 지원이 필요하다.

기술스트레스이론에서는 기술스트레스 억제를 위한 조직 차원의 노력을 완화요인(inhibitors)이라 명명하고 스트레스 완화를 위한 다각적 요인을 제시하고 있다(Fuglseth and Sørebø, 2014; Ragu-Nathan et al., 2008; Jena, 2015). Ragu-Nathan et al.(2008)과 Fuglseth

and Sørebø(2014)는 스트레스 완화요인을 이해증진(literacy facilitation), 기술적지원(technical support provision), 참여촉진(involvement facilitation) 3가지로 제시하였는데, 사용자가 컴퓨팅시스템에 대한 이해를 할 수 있도록 조직차원에서의 독려(이해증진), 관련 기술 활용 효율성 증대를 위한 헬프데스크 운영(기술적지원), 사용자들이 기술 도입 등에 대한 참여를 통한 사용자 관점의 기술 도입 촉진(참여 촉진)이 기술스트레스를 감소시킬 수 있다고 보았다. Jena(2015)는 단일의 완화요인을 제시하면서 기술적 문제를 해결하도록 지원하는 조직의 노력 및 충분한 시간 제공 수준이 높을수록 기술스트레스에 대한 완화효과가 있음을 증명하였다.

본 연구는 지속적으로 변화하는 조직의 보안환경에서 조직원이 체감할 수 있는 정보보안 지원 요인으로서, 기술적 지원이 우선시 되어야 할 것으로 보고, 보안관련 기술스트레스 완화요인으로 제시한다. 조직 내 헬프데스크 운영 등 정보보안 지원 정책이 활발할수록, 조직원들이 관련 보안 기술 및 준수 범위를 명확하게 모르더라도 보안 행동으로 옮길 수 있으며, 직접적인 행동 성과를 도출할 수 있기 때문이다.

정보보안 관련 기술적 지원은 Ragu-Nathan et al.(2008)의 기술적지원에 대한 정의를 정보보안 분야에 반영하여, 헬프데스크 등 정보보안 관련 기술의 효과적인 사용을 위한 조직의 지원으로 정의한다. 기술적 지원을 위한 헬프데스크 운영의 주요 목적은 개인이 관련 기술적 문제에 대하여 빠른 시간안에 해결하는데 있다(Tarafdar et al., 2011). 그렇기 때문에, 조직에 도입한 개별 기술요소별 맞춤형 기술 지원이 헬프데스크가 추구하는 기술적 범위이다. 정보보안 분야에서, 보안 기술 지원을 위한 헬프데스크의 역할은 최종수요자가 보안 기술 적용 시 필요한 기능 해결 조치와 더불어, 보안 기술을 반영한 기술적 프로세스 관리 및 행동 방식을 제시하는 것까지 포함된다.

정보보안 관련 기술적 지원은 스트레스를 직·간접적으로 감소시키거나 조직에 대한 만족을 높이는 요인이다. Tarafdar et al.(2014)은 영업사원의 기술스트레스가 업무스트레스에 영향을 주고 기술에 의한 성과에 부정적 영향을 미친다고 하였으며, 기술스트레스 완화요인이 기술스트레스와 업무스트레스간의 관계를 완화하는 조절효과를 가진다고 하였다. Fuglseth and Sørebø(2014)는 기술스트레스는 IT 사용만족도를 감소시키고 사용의도를 감소시키는 원인인데, 완화요인이 기술스트레스와 만족도 사이를 완화하고, IT사용의도를 높이는 요인이라고 하였다. Tarafdar et al.(2011)은 기술스트레스의 부정적 영향(심리적 영향 및 부정적 행동)을 완화요인이 직접적으로 기술스트레스를 감소시킨다고 하였다. 즉, 기술스트레스 관련 선행연구를 바탕으로, 정보보안 관련 기술적 지원은 보안 관련 기술스트레스인 기술과부하와 기술불확실성을 완화할 것으로 판단하고, 다음과 같은 연구가설을 제시한다.

H3. 정보보안 기술적 지원은 정보보안 관련 기술과부하에 음(-)의 영향을 줄 것이다.

H4. 정보보안 기술적 지원은 정보보안 관련 기술불확실성에 음(-)의 영향을 줄 것이다.

2.4 개인-조직 적합성

인간은 자신을 둘러싼 다양한 환경(직업, 조직, 집단 등) 내에서 끊임없는 상호작용을 통해 환경에 대처하려고 하는데(Lauver and Krisof-Brown, 2001), 개인-조직 적합성은 환경에 대한 인간의 태도 또는 행동을 예측하기 위하여 제시된 이론이다. 개인을 둘러싼 환경적 특성에 따라 적합성은 보다 세분화되어 제시되고 있다. 실제로, 개인-직무 적합성(person-job fit), 개인-조직 적합성(person-organization fit), 개인-직업 적합성(person-vocation fit) 등 환경적 조건에 따라 다양하게 적합성을 제시하고 있으며, 다양한 환경별 개인들의 행동 및 예측 관점으로 활용되고 있다(Krisof-Brown et al., 2005). 그 중, 개인-조직 적합성은 조직 내 개인의 행동 예측에 가장 대표적으로 활용되는 개념이며, 개인-조직 적합성은 개인과 조직간에 적어도 하나의 개체가 다른 개체가 필요로 하는 것을 제공하거나 유사한 기본 특성을 공유하거나 둘 다를 공유할 때 발생하는 호환성을 의미한다(Kristof, 1996). 개인-조직적합성은 개인이 조직이 보유한 가치(value), 목표(goal), 사명(mission)과 어떻게 일치하는지와 관련되며, 두 개체들이 추구하는 방향이 일치하거나 호환될 때 적합성이 높다고 할 수 있다(Lauver and Krisof-Brown, 2001).

개인-환경간의 적합성 수준에 대한 평가는 초기에는 환경적 관점에서 개인과 환경 적합성 수준을 판단하였다(French et al., 1982). 즉, 개인이 환경과 유사한 요인을 확보하고 있을 때 상호적합성(supplementary fit)이 일어나거나, 환경이 요구하는 것을 개인이 보완할 때 보완적합성(complementary fit)이 일어난다고 보았다. 하지만, 최근에는 개인과 환경, 즉 개체 간의 요구사항에 대하여 상호간에 충족시킬 때 대상 간 적합성이 있다고 본다(Krisof, 1996). 개인-조직 적합성 관계에서, 조직은 개인에게 가치, 목표, 문화, 규범 등의 충족을 요구하고, 개인은 자신의 목표 달성에 대한 기회, 자원 지원 등을 요구한다. 즉, 조직원은 조직으로부터 업무에 대한 기회, 커뮤니케이션 기회, 개인적 목표 달성에 대한 기회 등을 제공 받을 때 적합한 조직으로 판단하고(Valentine et al., 2002), 조직은 개인의 지식, 역량, 태도, 노력 등과 같이 조직의 가치와 일치하거나 향상시키는 개인의 능력을 확보할 때 적합하다고 판단한다(Cable and Judge, 1996).

개인-조직 적합성은 개인 관점에서 만족도를 높이거나 이직의도를 감소시키는 선행요인이며, 조직 관점에서는 조직 몰입, 조직시민행동을 향상시켜 장기적으로 조직의 이익에 도움을 주는 요인이다. Wheeler et al.(2007)은 개인-조직 적합성이 일치하지 않을 경우 발생하는 부정적 영향을 찾고자 하였는데, 개인-조직적합성의 불일치가 만족도를 감소시키고 이직의도에 영향을 주는 것을 확인하였다. Netemeyer et al.(1997)은 영업 조직의 조직시민행동에 영향을 주는 선행요인을 제시하였는데, 개인-조직 적합성, 리더십 지원, 보상의 공정성이 영업조직 근로자들의 만족도를 높여 조직시민행동에 긍정적인 영향을 주는 것을 확인하였다. 더불어, Andrews et al.(2011)은 조직의 도덕적 가치가 개인-조직 적합성을 통해 조직에 대한 만족도 및 조직 몰입에 긍정적인 영향을 주는 개인-조직 접합성의 매개 프로세스를 제시하였다. 그

들은 조직의 바람직한 윤리적 가치 및 달성 활동이 개인-조직 적합성을 향상시키고, 조직에 대한 만족 및 몰입 수준을 높이는 것을 확인하였다. 즉, 개인-조직 적합성은 조직에 대한 긍정적인 태도 및 의도를 부여하는 선행요인이다.

본 연구는 개인-조직 적합성의 관련 선행연구를 바탕으로, 정보보안 분야에서도 개인-조직 적합성이 개인의 태도 및 의도에 긍정적 영향을 줄 것으로 판단하고 다음과 같은 가설을 제시한다.

H5. 개인-조직 적합성은 정보보안 준수의도에 정(+)의 영향을 줄 것이다.

개인-조직 적합성은 조직의 특정 환경에 의한 조직원들의 행동간의 관계에 조절효과를 가진다. Ruiz-Palomino and Martinez-Canas (2014)는 조직의 윤리적 문화 형성을 위한 노력이 조직에서 요구하는 윤리 수준까지 개인에게 형성시킬 수 있을 것인가에 대한 연구를 수행하였다. 그들은 조직의 윤리적 문화가 개인들의 윤리적 행동 및 조직시민행동을 높이는 선행요인임을 밝혀냈으며, 나아가, 개인-조직 적합성이 윤리적 문화와 윤리적 행동간의 관계에서 강화효과를 가지는 것을 증명하였다. 즉, 개인-조직적합성이 높은 조직원은 조직에서 형성하는 윤리적 문화에 의한 윤리적 행동의도가 개인-조직 적합성이 낮은 조직원보다 높아짐을 발견하였다. 또한, Alniaçik et al.(2013)은 긍정적인 몰입, 직업 만족도가 이직의도를 감소시키며, 개인-조직 적합성이 긍정적 몰입과 직업 만족도에 의한 개인의 이직의도 감소를 더욱 높일 수 있는 것을 증명하였다. 즉, 개인-조직 적합성은 조직의 특정 환경이 개인의 행동에 미치는 긍정적, 부정적 영향을 조절한다. 본 연구는 개인-조직 적합성의 이러한 특징이 정보보안 분야에서도 적용될 것으로 판단한다. 즉, 정보보안 관련 기술과부하와 기술불확실성이 준수의도에 미치는 부정적 영향을 개인-조직 적합성이 완화할 것이라 판단하며, 다음과 같은 가설을 제시한다.

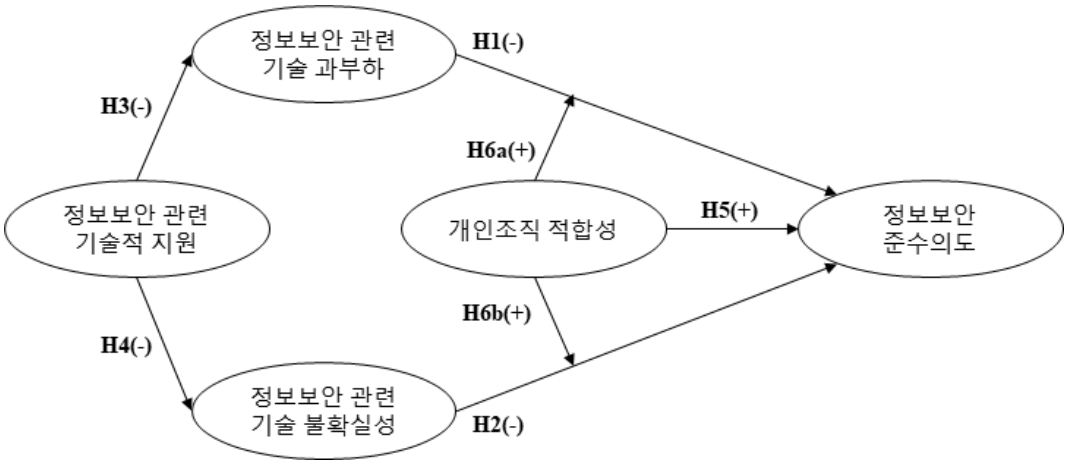
H6a : 개인-조직 적합성은 기술과부하와 준수의도간의 음(-)의 관계를 완화할 것이다.

H6b : 개인-조직 적합성은 기술불확실성과 준수의도간의 음(-)의 관계를 완화할 것이다.

Ⅲ. 연구 방법

3.1 연구 모델

본 연구는 정보보안 관련 기술스트레스 요인(기술 과부하, 기술 불확실성)이 조직원의 정보보안 준수에 미치는 부정적 영향 관계를 파악하고, 보안 관련 기술 스트레스 완화를 위한 조직차원의 선행요인(기술적 지원)과 개인적 특성 고려요인(개인-조직 적합성)을 찾는 것을 목적으로 한다. 이를 위하여 <그림 1>의 연구모델을 제시하였으며, 실증검증을 통하여 연구목적을 달성하고자 한다.



<그림 1> 연구 모델

3.2 연구 변수 구성

연구 모델에서 제시한 구조기반의 연구가설들을 검증하기 위하여, 본 연구는 설문지 기법을 실시하여 관련 데이터를 확보하고자 한다.

정보보안 관련 기술스트레스와 기술적 지원은 IT 기술 스트레스 관련 선행연구를 통해 설문항목을 도출하였으며, 개인-조직적합성은 인사조직 분야 선행연구를 통해 설문항목을 도출하였다. 이후 정보보안 분야에 맞게 요인별 설문항목을 재구성하였다. 또한, 설문문항의 척도는 리커트척도를 적용하였으며, "매우 그렇지 않다(1점)"에서 "매우 그렇다(7점)"으로 7점 리커트를 사용하여 설문을 구성하였다.

세부적으로, 정보보안 관련 기술과부하는 "정보보안 기술 도입으로 인하여 조직원의 업무가 과해지는 수준"으로 정의하며, Ragu-Nathan et al.(2008)의 연구를 기반으로 4개의 설문항목을 도출하였다. 정보보안 관련 기술 불확실성은 "조직에 도입된 정보보안 기술 수준이 지속적으로 높아지고, 변화하는 수준"으로 정의하며, D'Arcy et al.(2014)의 연구를 기반으로 3개의 설문항목을 도출하였다. 정보보안 관련 기술적 지원은 "조직원의 정보보안 기술 습득 및 활용에 대한 조직차원의 기술적 지원 수준"으로 정의하며, Ragu-Nathan et al.(2008)의 연구를 기반으로 4개의 설문항목을 도출하였다.

조절변수인 개인-조직적합성은 "개인의 가치와 조직의 가치가 동일한 수준"으로 정의하며, Valentine et al.(2002)의 연구를 기반으로 4개의 설문항목을 도출하였다. 종속변수인 정보보안 준수의도는 "조직의 정보보안 요구사항을 준수하고자 하는 의도"로 정의하며, Chen et al.(2012)의 연구를 기반으로 4개의 설문항목을 도출하였다.

다음으로, 설문문항의 내적 타당성(content validity)를 높이기 위하여, 도출된 5개 측정 요인을 정보보안 정책을 적용하는 기업에 다니는 대학원생 10명에게 항목에 대한 사전 검증을 실시하였다. 항목 구성 내용들이 문제가 발생하지 안하 최종적으로 요인별 설문문항을 확정하였으며, 다음 <표 1>과 같다.

<표 1> 연구 변수 구성 항목

변수	구성 항목	관련문헌
정보보안 관련 기술과부하	나는 조직의 정보보안 기술 정책에 맞추어 일을 하도록 요구 받는다. 나는 조직의 정보보안 기술 때문에, 처리할 수 있는 것보다 더 많은 업무를 요구 받는다. 나는 정보보안 기술 때문에 업무 수행 일정에 방해를 받는다. 나는 정보보안 기술 요구 수준에 적응하기 위하여 업무 습관을 바꾸도록 요구 받는다.	Ragu-Nathan et al.(2008)
정보보안 관련 기술불확실성	회사의 정보보안 관련 기술은 변화하고 있다. 회사의 정보보안 시스템은 지속적인 업그레이드가 되고 있다. 내 직업은 정보보안에 대한 새로운 요구사항이 지속적으로 발생하고 있다.	D'Arcy et al. (2014)
정보보안 관련 기술적 지원	조직의 보안 데스크는 조직원 보안 문제에 대한 답변을 한다. 조직의 보안 데스크는 조직원이 보안 지식을 가지도록 지원한다. 조직의 보안 데스크는 쉽게 접근이 가능하다. 조직의 보안 데스크는 조직원의 요청에 응답을 한다.	Ragu-Nathan et al.(2008)
개인-조직 적합성	나는 나의 개인적 가치가 조직에 잘 맞는다고 생각한다. 우리 조직은 다른 사람들에 대한 관심과 관련하여 나와 동일한 가치를 가지고 있다. 우리 조직은 정직함과 관련하여 나와 동일한 가치를 가지고 있다. 우리 조직은 공정성과 관련하여 나와 동일한 가치를 가지고 있다.	Valentine et al. (2002)
정보보안 준수의도	나는 우리 조직의 정보보안 정책을 지속적으로 따를 것이다 나는 우리 조직의 정보시스템을 보호하기 위해 조직의 정보시스템 보안 정책을 지속적으로 준수할 가능성이 높다. 나는 우리 회사의 정보 시스템을 접속할 때마다 정보보안 정책을 준수할 것이다. 나는 업무를 수행할 때마다 정보보안 절차를 준수할 것이다.	Chen et al. (2012)

3.3 자료 수집

본 연구는 조직의 정보보안 관련 기술에 의해 발생가능한 조직원의 스트레스 요인을 제시하고 완화하기 위한 조직차원, 조직원 개인 특성차원의 요인을 제시하는 것을 목적으로 한다. 따라서, 설문대상은 정보보안 정책 및 기술을 엄격하게 도입하고 있는 기업에 다니는 조직원을 대상으로 하며, 개인의 업무 및 조직 생활에 정보보안 행동을 요구받는 일반적인 업무를 보는 조직원을 대상으로 한다. 반면, 조직의 정보보안 부서에서 근무하는 조직원들은 제외하였다. 이유는 정보보안 부서의 업무 목표가 일반적 업무를 보는 부서와 달리, 정보보안 정책 및 기술을 조직에 적용하는데 있어 받을 수 있는 스트레스 요인이 틀릴 수 있다고 판단하였기 때문이다. 또한, 정보보안 부서의 조직원과 그 외 부서의 조직원은 정보보안 기술에 대한 이해도 및 관여도 수준 등의 차이가 높게 발생할 수 있다고 보았기 때문이다.

설문은 대학의 평생교육원에서 대학 학위를 받기 위하여 수업을 듣는 직장인들을 대상으로 받았다. 설문을 위하여 연구진이 직접 수업 전에 방문하여 연구의 취지를 설명하고, 통계적

용도로만 데이터를 활용한다고 명확하게 설명함으로써 설문당사자들의 개인 정보 노출에 대한 우려를 제거한 후 설문을 실시하였다. 그럼에도 설문을 거절하거나, 정보보안 정책이 조직에 도입되었는지 모르는 직장인들은 제외하고 설문을 확보하였다.

설문 기간은 2018년 12월 한달동안 진행되었으며, 총 500부를 배포하였다. 설문 결과 총 385개의 샘플이 수집되었으며, 이 중 응답을 상이하게 하거나 응답이 없는 샘플들을 제외하고 346개의 결과를 연구 가설 검증 데이터로 활용하였다.

Ⅳ. 가설 검증

4.1 설문응답자의 표본특성

346개의 유효 설문응답치의 인구통계학적 결과는 다음 <표 2>와 같다. 총 346개의 응답 중 성별로 구분 시, 남성은 194개(56.1%), 여성은 152개(43.9%)로 나타났으며, 연령으로 구분 시, 30세 미만은 93개(26.9%), 31~40세는 140개(40.5%), 41~50세는 102개(29.5%), 50세 이상은 11개(3.2%)로 나타났다. 업종은 제조업에서 80개(23.1%), 서비스업에서 266개(76.9%)가 응답하였으며, 직급으로 구분 시, 사원・대리는 144개(41.6%), 과장은 92개(26.6%), 차・부장은 55개(15.9%), 임원은 55개(15.9%)로 나타났다. 성별, 연령, 직급은 고르게 나타났으며, 업종은 서비스업이 더 많은 것으로 나타나 국내 업종별 특성을 잘 반영한 것으로 판단된다.

<표 2> 인구통계학적 특성

구분		빈도	비율(%)
합계		346	100.0%
성별	남성	194	56.1%
	여성	152	43.9%
연령	< 30	93	26.9%
	31~40	140	40.5%
	41~50	102	29.5%
	> 50	11	3.2%
업종	제조업	80	23.1%
	서비스업	266	76.9%
직급	사원&대리	144	41.6%
	과장	92	26.6%
	차부장	55	15.9%
	임원	55	15.9%

4.2 신뢰도 및 타당성 분석

연구 모델의 검증은 구조방정식모델링(structural equation modeling)을 적용한다. 구조방정식모델링 기반 가설검증을 위하여 사전에 신뢰성 및 타당성 분석을 실시한다.

첫째, 신뢰성 분석은 측정 요인들의 반복 측정에 따른 일관성을 파악하는 개념으로서, 내적 일관성(internal consistency)을 활용하여 신뢰성을 파악한다. 내적 일관성은 요인의 설문이 다항목으로 구성될 때 cronbach's alpha 계수를 활용하여 신뢰성을 감소시키는 항목을 제외함으로써 항목들의 일관성을 확보하는 방법이다. Nunnally(1978)은 각 요인의 신뢰성 확보를 위해서는 cronbach's alpha가 0.7이상이 되어야 한다고 하였다. 본 연구모델의 요인은 5개로서 총 19개의 설문항목으로 구성되어 있다. SPSS 21.0을 활용하여 분석한 결과 기술과부하 구성항목(TO1)을 제외한 18개의 항목에서 내적일관성을 가지는 것으로 나타났다 <표 4>.

둘째, 타당성분석은 측정 요인들이 서로 상

이한 개념으로 구성되어 있는지를 검증하는 것으로 확인적요인분석을 적용하여 집중타당성(convergent validity)과 판별타당성(discriminant validity)를 통해 검증한다. 확인적요인분석은 AMOS 22.0을 적용하여 모수추정법을 기반으로 실시하였으며, 구조모델의 적합도는 <표 3>과 같이 권고 사항에 적합하게 나타나 우선 집중타당성을 분석하였다.

<표 3> 확인적 요인분석 적합도 분석결과

변수	χ2/df	GFI	AGFI
분석 결과	1.333	0.955	0.936
권고 사항	< 3	> 0.9	> 0.8
변수	CFI	NFI	RMSEA
분석 결과	0.994	0.978	0.031
권고 사항	> 0.9	> 0.9	< 0.1

집중타당성은 개념신뢰도(construct reliability)와 평균분산추출(average variance extracted)를 통해 검증하며, Wixom and Watson(2001)은 개념신뢰도는 0.7이상, 평균분산추출이 0.5이상 일 경우 집중타당성이 있다고 보았다. 분석결과 개념신뢰도 및 평균분산추출이 가장 적은 요인이 준수의도로서 각각 0.706(개념신뢰도) 0.546(평균분산추출)로 나타나 집중타당성이 존재하는 것으로 나타났다<표 4>.

추가적으로, 판별타당성은 연구모델에 적용된 요인들이 상호간에 독립적으로 구별되는것에 대한 수준을 측정하는 분석으로서, 평균분산추출과 상관관계분석의 값을 비교하여 측정한다. Fornell and Lacker(1981)은 판별타당성을 평균분산추출 제곱근 값과 요인들의 상관관계 값을 구하여, 상관관계 값이 평균분산추출 제곱근 값보다 작으면 각 요인들이 독립적인 것으로 판단하였으며, 분석 결과 판별타당성이 존재하는 것으로 나타났다<표 5>.

<표 4> 측정 모형의 신뢰성 및 타당성 검증

변수	측정 항목 명	평균	표준편차	표준 적재치	Cronbach's Alpha	개념 신뢰도	분산추출 지수
기술과부하	TO2	2.89	1.12	.813	0.903	0.858	0.669
	TO3			.853			
	TO4			.825			
기술불확실성	TU1	2.76	1.33	.848	0.936	0.881	0.711
	TU2			.856			
	TU3			.848			
기술적지원	TS1	5.21	1.19	.829	0.939	0.902	0.697
	TS2			.772			
	TS3			.813			
	TS4			.819			
개인-조직 적합성	PO1	5.13	1.18	.829	0.921	0.891	0.732
	PO2			.845			
	PO3			.842			
	PO4			.691			
준수의도	CI1	5.61	1.12	.866	0.977	0.706	0.546
	CI2			.856			
	CI3			.860			
	CI4			.857			

<표 5> 확인적 요인분석에서 구성 개념간 상관관계

변수	1	2	3	4	5
기술과부하	***0.818***				
기술불확실성	.544**	***0.843***			
기술적지원	-.558**	-.561**	***0.835***		
개인-조직적합성	-.550**	-.481**	.613**	***0.856***	
준수의도	-.557**	-.558**	.610**	.609**	***0.739***

주) * = p<0.05 / 대각선의 볼드체 값은 분산추출지수의 제곱근

더불어, 본 연구는 연구 모델 및 가설 검증을 위하여 요인에 대한 다항목 중심의 설문 문항을 적용함으로써, 설문응답자의 요인에 대한 생각을 질문하고 데이터를 확보하였기 때문에, 공통방법편의(common method bias) 문제에 대한 검증을 실시한다. Podsakoff et al.(2003)은 공통방법편의는 연구과정에서 다양한 문제로 발생 가능하다고 보았으며, 검증 기법별 조금씩의 문제가 존재하기 때문에 상황별 적정기법을 적용하는 것이 필요하다고 보았다. 본 연구는 일반적으로 활용되는 단일방법요인(single-common-method-factor)을 적용하여 공통방법편의 문제를 찾고자 한다. 본 방법은 단일요인을 추가로 적용한 구조모델과 요인들만 적용한 구조모델간의 측정항목의 변화량을 살펴봄으로써 차이가 없는지 확인하는 방법이다. 단일요인을 적용하지 않은 구조모델의 적합도(χ^2 = 145.3 (*df* = 109, p<0.01), GFI = 0.955, AGFI = 0.936, CFI = 0.994, NFI = 0.978, and RMSEA = 0.031)와 단일모형을 적용한 구조모델의 적합도(χ^2 = 101.7 (*df* = 92, p<0.01), GFI = 0.967, AGFI = 0.945, CFI = 0.998 NFI = 0.984, and RMSEA = 0.018) 모두 권장 사항에 적합하였으며, 측정요인의 구성항목들의 변화량이 0.2이하로 나타나 공통방법편의 문제는 적은 것으로 나타났다.

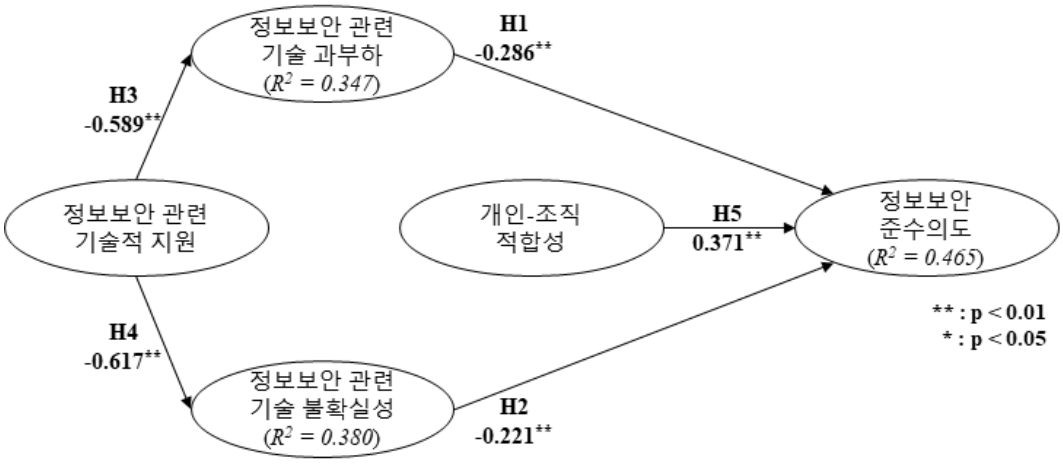
4.3 주효과 분석

구조방정식모델링 기반의 연구모델 검증을 위한 분석은 모델의 적합도 검정, 경로계수(β) 분석, 그리고 결정계수(R^2)분석 3단계의 절차로 진행된다. 첫째, 구조모델의 적합도 검증은 앞서 확인적요인분석에서 실시한 적합도 분석 기준을 동일하게 적용하였으며, 분석 결과 연구모델 구조는 적합한 것으로 나타났다<표 6>.

<표 6> 연구모델의 적합도 결과

변수	χ^2/df	GFI	AGFI
분석 결과	2.078	0.920	0.894
권고 사항	< 3	> 0.9	> 0.8
변수	CFI	NFI	RMSEA
분석 결과	0.979	0.961	0.056
권고 사항	> 0.9	> 0.9	< 0.1

둘째, 연구가설 검증을 실시한다. 연구가설 검증은 경로계수(*β*) 분석을 통하여 측정 요인간에 영향관계를 검증한다. 경로계수 분석(*β*)을 통해 도출된 연구가설 검증 결과는 <그림 2>, <표 7>과 같다.



<그림 2> 가설검정 결과

<표 7> 가설검정 결과

가설	경로	경로 계수	t-value	결과
H1	기술과부하 → 준수의도	-0.286	-5.825**	채택
H2	기술불확실성 → 준수의도	-0.221	-4.454**	채택
H3	기술적 지원 → 기술과부하	-0.589	-10.577**	채택
H4	기술적 지원 → 기술불확실성	-0.617	-11.709**	채택
H5	개인-조직적합성 → 준수의도	0.371	7.197**	채택

연구가설 1은 정보보안 관련 기술 과부하가 정보보안 준수의도에 음(-)의 영향을 준다는 것으로, 가설 검증 결과 기술 과부하와 준수의도가 부정적 영향관계에 있는 것으로 나타났다(H1: β = -0.286, p < 0.01). 이러한 결과는 IT 시스템 도입이 사용자의 기술스트레스를 발생시키고 관련 목표 행동에 부정적인 영향을 준다는 Galluch et al.(2015)와 Tarafdar et al.(2011)의 선행연구와 같은 결과이다. 즉, 조직 정보보안 기술 도입 및 활용 요구사항이 높아져 조직원의 관점에서 기술활용의 어려움이 발생한다고 판단될 때, 당사자의 정보보안 준수의도를 감소시킨다. 따라서, 조직에 도입한 정보보안 기술이 조직원의 업무 등에 과부하가 되지 않도록 지원하는 것이 필요하다.

연구가설 2는 정보보안 관련 기술 불확실성이 정보보안 준수의도에 음(-)의 영향을 준다는 것으로, 가설 검증 결과 기술 불확실성과 준수의도가 부정적 영향관계에 있는 것으로 나타났다(H2: β= -0.221, p<0.01). 이러한 결과는 조직에 도입한 기술이 지속적으로 변화하여 구성원의 기술관련 불확실성이 높아지면 피로 등에 의해 직무 만족도를 감소시킨다는 Ragu-Nathan et al.(2008)의 결과와 부분적으로 일치한다. 즉, 조직에서 개인이 급작스런 정보보안 기술의 변화에 대하여 스트레스로 인식할 경우 조직에 대한 불만 또는 피로감 등이 높아져 스트레스화된다는 것을 의미하며, 이러한 결과는

준수의도 감소와 같은 부정적 행동요인으로 이어진다. 따라서, 정보보안 기술 도입 시 불확실성을 감소시키기 위한 조직 차원의 노력을 하는 것이 필요하다.

연구가설 3은 정보보안 기술적 지원이 정보보안 관련 기술 과부하에 음(-)의 영향을 준다는 것으로, 가설 검증 결과 기술적 지원이 기술과부하를 완화시키는 것으로 나타났다(H3: β= -0.598, p<0.01). 이러한 결과는 협력적 학습환경 향상을 위한 IT 도입 과정에서 발생하는 기술스트레스 요인을 조직 차원의 기술 지원 노력이 감소시킨다는 Jena(2015)의 연구와 동일한 결과이다. 즉, 지속적으로 변화하는 정보보안 환경에 대응하기 위한 시스템 도입 등 조직의 노력은 개인의 스트레스 환경에 노출시킬 수 있지만, 사용자 지원을 위한 기술적 헬프데스크 운영은 기술과부하 스트레스를 감소시키기 때문에 사용자 맞춤형 기술적 지원 체계 구축이 필요하다.

연구가설 4는 기술적 지원이 정보보안 관련 기술 불확실성에 음(-)의 영향을 준다는 것으로, 가설 검증 결과 기술적 지원이 기술 불확실성에 부정적 영향을 주는 것으로 나타났다(H4: β = -0.617, p<0.01). 이러한 결과는 조직에 도입한 기술의 변화 수준에 따라 발생가능한 기술스트레스 요인을 기술스트레스 완화 매커니즘이 작용을 한다는 Tarafdar et al.(2015)의 연구와 동일한 결과이다. 즉, 조직 차원의 보안 관련 기술적 지원이 급변하는 외부 환경에 대응하기 위한 조직의 보안기술 도입에 의한 기술불확실성 스트레스를 완화시키기 때문에, 조직은 사용자 관점의 보안 기술 매뉴얼 및 헬프데스크를 운영함으로써, 기술적으로 충분히 지원하고 있음을 제시하는 것이 필요하다.

연구가설 5는 개인-조직 적합성이 정보보안 준수의도에 양(+)의 영향을 준다는 것으로, 가설 검증 결과 개인-조직 적합성이 정보보안 준수의도에 긍정적 영향을 주는 것으로 나타났다(H5: β= 0.371, p<0.01). 이러한 결과는 조직원과 조직의 개인-조직 적합성이 일치할 때, 직무만족도를 높여 조직시민행동에 긍정적인 영향을 준다는 Netemeyer et al.(1997)의 연구와 부분적으로 일치한다. 즉, 정보보안 분야에서도 조직원과 조직이 추구하는 가치가 일치할 때, 조직원은 조직의 가치 및 목표 달성을 위하여 노력하는 것이 증명되었다. 따라서 개인-조직 적합성이 정보보안 준수의도를 높이는 중요한 선행요인이기 때문에, 조직의 가치를 지속적으로 제시하고 개인이 인지할 수 있도록 지원하는 것이 필요하다.

셋째, 구조모형에서 결과변수에 대한 선행변수들의 영향력을 측정하기 위하여 결과변수별 결정계수(R^2) 분석을 실시하였다. 정보보안 준수의도는 정보보안 관련 기술과부하와 불확실성, 그리고 개인-조직적합성의 선행변수들에 의해 46.5%의 설명력을 가지는 것으로 나타났다. 기정보보안 기술적지원은 정보보안 관련 기술과부하에 34.7%의 설명력을 가지는 것으로 나타났으며, 정보보안 관련 불확실성에 38.0%의 설명력을 가지는 것으로 나타났다.

4.4 조절효과 분석

연구가설 6a와 6b는 정보보안 관련 기술스트레스(기술과부하, 불확실성)가 정보보안 준수의도에 미치는 부정적인 영향 관계에서, 개인-

조직적합성에 의한 조절효과(완화효과)가 발생할 것이라는 관점이다.

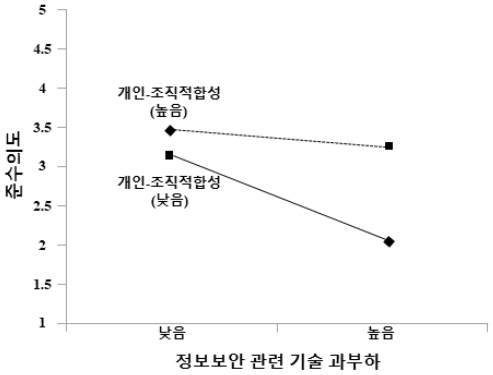
조절변수가 연속형 변수일 때, 구조방정식모델링을 통한 조절효과 검증은 대상 요인들의 상호작용효과(interaction effect)분석을 통하여 실시한다. 본 연구는 상호작용효과 분석 중 엄격하게 평가하는 방법인 Little et al.(2007)의 직교화접근법(orthogonalizing approach)을 적용하여 조절효과분석을 실시하였으며, 분석 결과는 <표 8>과 같다.

<표 8> 조절효과 분석 결과

구분	경로	경로 계수	t-value	결과
H6a	TO → CI	-0.325	-6.107**	채택
	P-O fit → CI	0.414	7.898**	
	TO x P-O fit → CI	0.246	5.696**	
H6b	TU → CI	-0.361	-7.133**	채택
	P-Ofit → CI	0.41	8.101**	
	TU x P-Ofit → CI	0.161	3.815**	

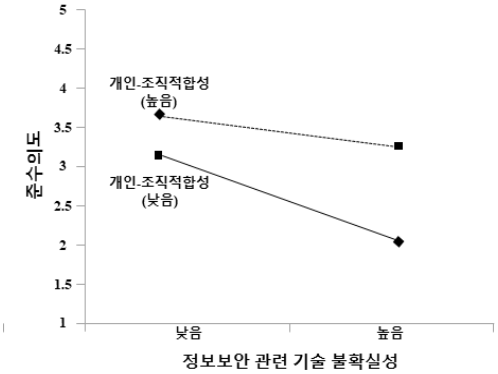
**: p < 0.01
TO(기술과부하), TU(기술불확실성),
P-O fit (개인-조직적합성), CI(준수의도)

기술과부하와 준수의도간의 부정적 영향관계를 개인-조직적합성이 완화하는가를 검정한 결과(H6a), 개인-조직적합성이 기술과부하의 준수의도에 미치는 부정적 영향을 완하는 것으로 나타났다. 추가적으로, 개인-조직적합성의 조절효과 영향관계를 보다 명확하게 분석하기 위하여 상호작용항 그래프(interpreting interaction effects)를 제시하였다(Dawson, 2014). 정보보안관련 기술과부하가 준수의도를 감소시키지만, 개인-조직적합성이 높을 경우 준수의도 감소를 완화하는 것으로 나타났다 <그림 3>.



<그림 3> 기술과부하 조절효과 분석 결과

기술불확실성과 준수의도간의 부정적 영향관계를 개인-조직적합성이 완화하는가를 검정한 결과(H6b), 개인-조직적합성이 불확실성의 준수의도에 미치는 부정적 영향을 완하는 것으로 나타났다. 더불어, 개인-조직적합성의 조절효과 영향관계를 보다 명확하게 분석하기 위한 상호작용한 그래프를 적용한 결과, 정보보안관련 기술불확실성이 준수의도를 감소시키지만, 개인-조직적합성이 높을 경우 준수의도 감소를 완화하는 것으로 나타났다 <그림 4>.



<그림 4> 기술불확실성 조절효과 분석 결과

Ⅴ. 결 론

본 연구의 목적은 조직의 정보 가치 중요성에 따라, 지속적으로 증가하는 정보보안 기술에 대한 투자 및 도입이 가지는 부정적인 부분을 제시하고 부정적 측면을 완화함으로써, 조직의 지속적인 정보보호를 위한 방향을 제시하는 것에 있다.

연구 목적 달성하기 위하여, 정보기술에 의한 스트레스 요인을 정보보안 분야에 적용하였다. 세부적으로 정보보안 기술과부하와 불확실성이 정보보안 기술에 의해 발생되는 스트레스 요인임을 제시하고 보안 준수에 미치는 부정적인 영향을 찾고자 하였다. 더불어, 부정적 행동 발생 요인인 스트레스를 완화시키기 위한 요인을 제시하였는데, 조직 관점에서 수행해야할 접근 방향(기술적 지원)과 개인의 특성 요인(개인-조직적합성)으로 구분하여 제시함으로써, 다각적 관점의 준수의도 감소에 대한 최소화 방안을 찾고자 하였다.

선행연구를 통해 도출된 연구모델에 대한 검증은 구조방정식모델링을 활용하였으며, 서베이를 통해 데이터를 확보하였다. 설문대상은 정보보안 기술을 도입하여 활용하고 있는 조직에 근무하는 조직원들을 대상으로 하였으며, 유효샘플 346개를 확보하였다.

가설 검정 과정은 구조방정식모델링 검증을 위한 신뢰성 및 타당성 분석을 실시하였으며 문제가 없어, 주효과 및 조절효과 분석을 실시하였다. 주효과 분석 결과, 정보보안 관련 기술스트레스 요인(기술과부하, 불확실성)이 준수의도에 부정적인 영향을 미치고 개인-조직적합성이 준수의도에 긍정적인 영향을 미치는 것으로 나타났다. 또한, 조직차원의 기술적 지원(헬프데스크 운영 등)이 기술스트레스를 감소시키는 것으로 나타났다. 더불어, 정보보안 기술스트레스와 준수의도간의 부정적관계를 개인-조직적합성이 완화할 것인가에 대한 조절효과분석을 실시하였다. 분석 결과, 기술과부하 및 불확실성에 의한 보안관련 기술스트레스는 준수의도를 감소시키지만, 개인-조직적합성이 높을 때가, 개인-조직적합성이 낮을 때보다 준수의도에 미치는 부정적 영향이 낮아지는 것을 확인하였다.

5.1 연구의 시사점

본 연구는 정보보안 분야에 다음과 같은 이론적, 실무적 시사점을 가진다.

첫째, 기술스트레스가 가지는 부정적 측면을 정보보안 분야에 적용하였으며, 조직원의 보안 준수를 감소시키는 것을 확인하였다. 조직의 보안 위협은 지속적으로 증가하고 있을 뿐 아니라, 스마트 업무를 통한 직무의 효율성을 높이고자하는 조직이 증가하면서 보안 사고 가능성은 높아지고 있다. 이에, 조직들은 더욱 강화된 보안기술을 도입하고 있어, 결과적으로 엄격해지고 강화된 정보보안기술에 의해 조직원들은 보안 관련 스트레스를 일으킬 가능성이 높다(Hwang and Cha, 2018). 본 연구는 정보보안 관련 기술 스트레스 요인을 파악하기 위하여 기술스트레스 관련 선행연구를 통해 기술과부하와 불확실성 요인들을 제시하였다. 기술과부하는 정보보안 기술에 의해 자신의 본연 업무의 양을 증가시키는 상황을 의미하며, 불확실성은 지속적인 보안 기술의 도입으로 관련 기술

습득 등의 불확실성이 커지는 것을 의미한다. 이론적 측면에서, 정보보안 분야에 기술스트레스가 발생하는 것을 증명하였으며, 구성원들의 준수의도를 감소시키는 것을 확인하였기 때문에, 향후 정보보안 기술의 부정적 측면의 연구 분야에 있어, 본 연구의 결과는 이론적 시사점을 줄 것으로 판단된다. 또한, 조직의 정보보안 시스템은 결구 실제 사용자인 조직원들의 관점에서 도입되어야 한다는 것을 스트레스 관점에서 제시하였으며, 정보관리를 위한 조직의 노력이 훼손되지 않기 위해서는 보안기술에 의한 스트레스를 최소화하기 위한 방안을 마련해야 함을 제시하였다.

둘째, 정보보안의 기술스트레스(기술과부하, 불확실성)을 최소화하기 위한 조직차원의 노력요인(기술적 지원)을 제시하고 관련성을 검증하였다. 기술스트레스 이론은 기술스트레서(발생 원인)가 개인의 조직에 대한 만족도 또는 몰입 등을 감소시킨다고 보았으며, 기술스트레서가 개인에게 부정적 영향을 주는 과정을 감소시키기 위해서는 기술스트레스 완화 매커니즘이 중요하다고 보았다(Ragu-Nathan et al., 2008). 본 연구는 조직차원의 보안 관련 기술적 지원이 직접적으로 높아진 보안 기술 수준에 의해 발생한 스트레스를 완화할 수 있다고 보았으며, 선행연구를 통해 정보보안 관련 기술적 지원 요인을 제시하고, 스트레스와의 음(-)의 영향관계가 있음을 증명하였다. 즉, 이론적 관점에서 조직원의 보안 기술에 대한 이해 및 행동적 지원과 같은 조직차원의 보안 기술 지원 노력이 기술스트레스에 부정적인 영향을 미치는 것을 증명함으로써, 준수의도에 부정적 영향을 미치는 요인을 완화하기 위한 선행 조건을 제시하였다는데 의미를 가진다. 또한, 실무적 관점에서, 조직원의 보안 행동 불안감 등을 해소함으로써 스트레스를 감소시킴으로써 준수의도에 긍정적인 영향을 주는 선행 요인임을 증명하였다.

따라서, 정보보안 관련 기술 도입을 통해 정보 관리 및 조직원의 보안 위협 최소화를 위해서는 조직원이 이해할 수 있는 보안 기술 지원 서비스가 선행되어야 한다. 즉, 조직은 정보보안 관련 기술 및 조직의 정보보안 규정에 대한 해석 및 적용 방법, 그리고 보안 행동에 옮기 위한 관련 매뉴얼을 도입하여 배포하기 위한 교육 훈련 등을 실시하는 것이 필요하다. 또한, 조직원의 적정 보안 행동을 위한 보안관련 헬프데스크 운영을 실시함으로써 언제든 조직원이 보안 관련 도움을 받을 수 있도록 시스템을 구축하는 것이 필요하다.

셋째, 정보보안의 기술스트레스(기술과부하, 불확실성)가 개인의 정보보안 준수의도에 미치는 부정적 영향을 완화하기 위한 조절요인인 개인-조직적합성을 제시하고 상호작용효과 검증을 통해 조절효과를 가지는 것을 확인하였다. 개인은 자신만의 가치를 가지고 있으며, 조직에서 조직의 가치가 본인의 가치와 일치할 때, 조직의 목표 및 성과를 달성하고자 하는 동기가 높아진다(Wheeler et al. 2007). 본 연구는 경영학의 인사 조직 분야 및 심리학, 사회학 분야에서 중점적으로 다루었던 개인과 조직간의 관계를 설명하는 이론인 개인-조직적합성 이론을 정보보안 분야에 적용하였다. 즉, 이론적 측면에서, 조직원에게 부여된 정보보안 행동이 보안 관련 기술들에 의해서 스트레스를 일으켜 감소되더라도, 개인이 조직의 가치를 명확하게 인지

하고 동일시를 할 경우 부정적 행동이 완화되는 것을 증명하였다. 즉, 엄격한 보안 기술에 의한 스트레스를 완화하기 위한 개인적 특성 요인을 제시하였다는 측면에서 의미를 가진다. 또한, 실무적 관점에서, 개인이 조직에 대한 의미 및 가치에 대한 인식이 개인에게 발생하는 기술적 스트레스의 부정적 영향을 감소시킬 수 있음을 증명하였다.

이에 따라 조직은 조직이 추구하는 가치 및 목표가 개인과 일치함을 지속적으로 교육 및 캠페인 등을 통해 가시성을 높이고, 함께 정보관리를 해나간다는 일체감을 형성시키기 위한 활동을 하는 것이 필요하다. 이를 통해 지속적으로 보안 관련 기술스트레스가 조직원들에게 발생하더라도, 조직의 보안 관련 가치 달성을 위하여 조직원 스스로가 해야할 행동이라고 판단하도록 제시하는 것이 필요하다.

5.2 연구의 한계점

본 연구는 다음과 같은 한계점을 가지며, 향후 연구에서의 보완될 필요가 있다. 본 연구는 정보보안 기술에 의해 발생 가능한 조직원의 스트레스와 완화를 위한 요인을 제시함으로써, 조직 내부 구성원들의 자발적인 보안 준수를 위한 방향을 제시하는 것을 목적으로 하였다. 이에, 정보보안 기술 및 정책을 도입한 조직에 근무하는 조직원들을 대상으로 설문지 기법을 통해 실증분석을 하였다. 설문지 기법 특성 상 응답 당시의 조직 도입 기술들의 스트레스 상황, 조직의 기술적 지원 체계 등에 대한 응답자 본인의 인지를 기반으로 현황을 분석하였는데, 보다 명확한 분석을 위해서는 조직에 도입한 기술 수준에 대한 객관적 측정 및 개인적 특성을 비교 분석함으로써, 시사점을 제시하는 것이 필요하다. 또한, 설문 대상을 국내에 정보보안 기술을 도입한 조직의 구성원을 대상으로 하였으나, 응답자의 조직적 특성별 분석을 실시하지는 못하였다. Verizon(2019) 보고서에 의하면, 전 세계 정보보안 사고가 가장 많은 업종이 금융, 공공, 엔터테인먼트 분야인데, 각각 업종별 특성과 도입한 정보보안 기술 수준&표준, 정책 등이 상이하다. 정보보안 기술을 도입한 업종별 특성을 반영한 연구를 진행한다면, 보다 체계적인 실무적인 관점에서의 도움이 될 것으로 판단된다. 그리고, 정보보안 기술 관련 스트레스 완화 요인으로 조직 요인인 기술적 지원과 개인 특성 요인인 개인-조직 적합성을 적용하였으나, 조직차원의 노력요인이 다양하게 제시되어야 할 필요가 있으며, 개인-보안기술 적합성, 개인-집단 적합성 등 보다 세부적 관점에서의 적합성 특성에 대한 연구가 이루어진다면, 개인들의 정보보안 준수 방안 수립에 도움이 될 것으로 판단된다.

참고문헌

유인진, 박도형 “중소기업 프로파일링 분석을 통한 기술유출 방지 및 보호 모형 연구,” 정보시스템연구, 제27권, 제1호, 2018, pp. 171-191.

황인호, 김승욱, “조직원의 정보보안 관련 업무 스트레스에 대한 억제 및 업무대처에 대한 연구: 금융 비즈니스를 중심으로,” e-비즈니스연구, 제18권, 제3호, 2017,

pp. 147-165.

황인호, 김상현, “SCO Framework 을 적용한 조직과 조직원의 정보보안 준수 관계 연구,” 정보시스템연구, 제28권, 제4호, 2019, pp. 105-129.

Alniaçik, E., Alniaçik, Ü., Erat, S., and Akçin, K., “Does Person - Organization Fit Moderate the Effects of Affective Commitment and Job Satisfaction on Turnover Intentions?,” *Procedia-Social and Behavioral Sciences*, Vol. 99, 2013, pp. 274-281.

Andrews, M. C., Baker, T., and Hunt, T. G., “Values and Person-Organization Fit: Does Moral Intensity Strengthen Outcomes?,” *Leadership & Organization Development Journal*, Vol. 32, No.1, 2011, pp. 5-19.

Ayyagari, R., Grover, V., and Purvis, R., “Technostress: Technological Antecedents and Implications,” *MIS Quarterly*, Vol. 35, No. 4, 2011, pp. 831-858.

Brod, C., *Technostress: The Human Cost of the Computer Revolution*. Reading, MA: Addison-Wesley, 1984.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I., “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *MIS Quarterly*, Vol. 34, No. 3, 2010, pp. 523-548.

Cable, D. M., and Judge, T. A., “Person‐Organization Fit, Job Choice Decisions, and Organizational Entry,” *Organizational Behavior and Human Decision Processes*, Vol. 67, No. 3, 1996, pp. 294-311.

Chen, Y., Ramamurthy, K., and Wen, K. W., “Organizations' Information Security Policy Compliance: Stick or Carrot Approach?,” *Journal of Management Information Systems*, Vol. 29, No.3, 2012, pp. 157-188.

D'Arcy, J., Herath, T., and Shoss, M. K., “Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective,” *Journal of Management Information Systems*, Vol. 31, No. 2, 2014, pp. 285-318.

D'Arcy, J., Hovav, A., and Galletta, D., “User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterrence Approach,” *Information Systems Research*, Vol. 20, No. 1, 2009, pp.79-98.

D’Arcy, J., and Teh, P. L., “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, 103151.

Dawson, J. F., “Moderation in Management Research: What, Why, When and How,” *Journal of Business and Psychology*, Vol. 29, No. 1, 2014, pp. 1-19.

Fornell, C., and Larcker, D. F., "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, Vol. 18, No. 1, 1981, pp. 39-50.

French, J. R. P., Caplan, R. D., and Harrison, R. V., *The Mechanisms of Job Stress and Strain*. New York: Wiley, 1982.

Fuglseth, A. M., and Sørebø, Ø., "The Effects of Technostress within the Context of Employee Use of ICT," *Computers in Human Behavior*, Vol. 40, 2014, pp. 161-170.

Galluch, P. S., Grover, V., and Thatcher, J. B., "Interrupting the Workplace: Examining Stressors in an Information Technology Context," *Journal of the Association for Information Systems*, Vol. 16, No. 1, 2015, pp. 1-47.

Gaudioso, F., Turel, O., and Galimberti, C., "The Mediating Roles of Strain Facets and Coping Strategies in Translating Techno-Stressors into Adverse Job Outcomes," *Computers in Human Behavior*, Vol. 69, 2017, pp. 189-196.

Grandviewresearch, 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, 2019.

Guo, K. H., and Yuan, Y., "The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model," *Information & Management*, Vol. 49, No. 6, 2012, pp. 320-326.

Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E., "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model," *Journal of Management Information Systems*, Vol. 28, No. 2, 2011, pp. 203-236.

Herath, T., and Rao, H. R., "Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness," *Decision Support Systems*, Vol. 47, No. 2, 2009, pp. 154-165.

Hung, W. H., Chen, K., and Lin, C. P., "Does the Proactive Personality Mitigate the Adverse Effect of Technostress on Productivity in the Mobile Environment?," *Telematics and Informatics*, Vol. 32, No. 1, 2015, pp. 143-157.

Hwang, I., and Cha, O., "Examining Technostress Creators and Role Stress as Potential Threats to Employees' Information Security Compliance," *Computers in Human Behavior*, Vol. 81, 2018, pp. 282-293.

Hwang, I., Kim, D., Kim, T., and Kim, S., "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.

Hwang, I. H., and Lee, H. Y., "The Employee's Information Security Policy Compliance Intention: Theory of Planned Behavior, Goal Setting Theory, and Deterrence Theory Applied," *Journal of Digital Convergence*, Vol. 14, No. 7, 2016, pp. 155-166.

Hwang, I., Wakefield, R., Kim, S., and Kim, T., "Security Awareness: The First Step in Information Security Compliance Behavior," *Journal of Computer Information Systems*, 2019, pp. 1-12.

Jena, R. K., "Technostress in ICT Enabled Collaborative Learning Environment: An Empirical Study among Indian Academician," *Computers in Human Behavior*, Vol. 51, 2015, pp. 1116-1123.

Kristof, A. L., "Person‐Organization Fit: An Integrative Review of its Conceptualizations, Measurement, and Implications," *Personnel Psychology*, Vol. 49, 1996, pp. 1-49.

Kristof-Brown, A. L., Zimmerman, R. D., Johnson, E. C., and Henry, B., "Consequences of Individuals' Fit at Work: A Meta-Analysis of Person-Job, Person-Organization, Person-Group, and Person-Supervisor Fit," *Personnel Psychology*, Vol. 58, No. 2, 2005, pp. 281-342.

Lauver, K. J., and Kristof-Brown, A., "Distinguishing Between Employees' Perceptions of Person‐Job and Person‐Organization Fit," *Journal of Vocational Behavior*, Vol. 59, No. 3, 2001, pp. 454-470.

Little, T. D., Card, N. A., Bovaird, J. A., Preacher, K. J., and Crandall, C. S., "Structural Equation Modeling of Mediation and Moderation with Contextual Factors," *Modeling Contextual Effects in Longitudinal Studies*, Vol. 1, 2007, pp. 207-230.

Loch, K. D., Carr, H. H., and Warkentin, M. E., "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly*, Vol. 16, No. 2, 1992, pp.173-186.

Netemeyer, R. G., Boles, J. S., McKee, D. O., and McMurrian, R., "An Investigation into the Antecedents of Organizational Citizenship Behaviors in a Personal Selling Context," *Journal of Marketing*, Vol. 61, No. 3, 1997, pp. 85-98.

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

Oh, S. T., and Park, S., "A Study of the Connected Smart Worker's Techno-stress," *Procedia Computer Science*, Vol. 91, 2016, pp. 725-733.

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

2003, pp. 879-903.

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., and Tu, Q., "The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation," *Information Systems Research*, Vol. 19, No. 4, 2008, pp. 417-433.

Ruiz-Palomino, P., and Martínez-Cañas, R., "Ethical Culture, Ethical Intent, and Organizational Citizenship Behavior: The Moderating and Mediating Role of Person‐Organization Fit," *Journal of Business Ethics*, Vol. 120, No. 1, 2014, pp. 95-108.

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., and Sookhak, M., "Deterrence and Prevention Based Model to Mitigate Information Security Insider Threats in Organisations," *Future Generation Computer Systems*, Vol. 97, 2019, pp.587-597.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T., "Information Security Conscious Care Behaviour Formation in Organizations," *Computers and Security*, Vol. 53, pp. 65-78, 2015.

Safa, N. S., Von Solms, R., and Futcher, L., "Human Aspects of Information Security in Organisations," *Computer Fraud & Security*, Vol. 2016, No. 2, 2016, pp. 15-18.

Siponen, M., Pahnila, S., and Mahmood, M. A., "Compliance with Information Security Policies: An Empirical Investigation," *Computer*, Vol. 43, No. 2, 2010, pp.64-71.

Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J., "Variables Influencing Information Security Policy Compliance: A Systematic Review of Quantitative Studies," *Information Management & Computer Security*, Vol. 22, No. 1, 2014, pp. 42-75.

Steinbart, P. J., Raschke, R. L., Gal, G., and Dilla, W. N., "The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes," *Accounting, Organizations and Society*, Vol. 71, 2018, pp. 15-29.

Tarafdar, M., Bolman Pullins, E., and Ragu-Nathan, T. S., "Examining Impacts of Technostress on the Professional Salesperson's Behavioral Performance," *Journal of Personal Selling & Sales Management*, Vol. 34, No. 1, 2014, pp. 51-69.

Tarafdar, M., Pullins, E. B., and Ragu Nathan, T. S., "Technostress: Negative Effect on Performance and Possible Mitigations," *Information Systems Journal*, Vol. 25, No. 2, 2015, pp. 103-132.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., and Ragu-Nathan, T. S., "The Impact of

Technostress on Role Stress and Productivity," *Journal of Management Information Systems*, Vol. 24, No. 1, 2007, pp. 301-328.

Tarafdar, M., Tu, Q., Ragu-Nathan, T. S., and Ragu-Nathan, B. S., "Crossing to the Dark Side: Examining Creators, Outcomes, and Inhibitors of Technostress," *Communications of the ACM*, Vol. 54, No. 9, 2011, pp. 113-120.

Valentine, S., Godkin, L., and Lucero, M., "Ethical Context, Organizational Commitment, and Person-Organization Fit," *Journal of Business Ethics*, Vol. 41, No. 4, 2002, pp. 349-360.

Vance, A., Siponen, M., and Pahnila, S., "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, Vol. 49, No. 3, 2012, pp. 190-198.

Verizon, Verizon 2019 Data Breach Investigations Report, 2019.

West, R., "The Psychology of Security," *Communications of the ACM*, Vol. 51, No. 4, 2008, pp. 34-40.

Wheeler, A. R., Coleman Gallagher, V., Brouer, R. L., and Sablynski, C. J., "When Person-Organization (mis) Fit and (dis) Satisfaction Lead to Turnover: The Moderating Role of Perceived Job Mobility," *Journal of Managerial Psychology*, Vol. 22, No. 2, 2007, pp. 203-219.

Wixom, B. H., and Watson, H. J., "An Empirical Investigation of the Factors Affecting Data Warehousing Success," *MIS Quarterly*, Vol. 25, No. 1, 2001, pp. 17-41.

Yan, Z., Guo, X., Lee, M. K., and Vogel, D. R., "A Conceptual Model of Technology Features and Technostress in Telemedicine Communication," *Information Technology & People*, Vol. 26, No. 3, 2013, pp. 283-297.

황 인 호 (Inho Hwang)

현재 한국산업기술대학교 연구교수로 재직하고 있다. 중앙대학교 경영학 박사학위를 수여하였다. 기업가정신, IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야에 관심을 가지고 연구를 진행 중이다.

허 성 호 (Sungho Hu)

중앙대학교 사회문화심리 전공으로 박사학위를 수여하였으며, 현재 중앙대학교에서 연구방법론과 심리통계를 주로 담당하고 있다. 주요 관심사는 정보문화, 문화격차, 디지털콘텐츠, 고령화, 성인교육 분야에 관심을 두고 있다.

<Abstract>

The Mitigation of Information Security Related Technostress and Compliance Intention

Inho Hwang · Sungho Hu

Purpose

As information management grows in importance around the world, organizations are investing in information security technology. However, the higher the level of information security technology in an organization, the higher the techno-stress of employees. The purpose of this study is to suggest stress factors related to information security technology that affect the reduction of employees' intention to comply with information security and to suggest ways to alleviate stress.

Design/methodology/approach

The research presented a model for mitigating technical stress related to information security based on technical stress theory and person-organization fit theory. 346 questionnaire data were analyzed from the members of the organization who applied the information security technology, and the research hypothesis was verified through the structural equation modeling.

Findings

The hypothesis test confirms that security-related techno-stress reduces the information security compliance intention of employees, organizational technical support mitigates technical stress, and person-organization fitness mitigates the negative relationship between techno-stress and compliance intention. The results of the study contribute to the organization's strategy for minimizing the reduction of the information security compliance intention of employees, and are meaningful in that the theoretical basis for mitigating techno-stress is provided in the field of information security.

Keywords: Information Security Related Techno-stress, Compliance Intention, Person-Organization Fit, Technical Support

* 이 논문은 2020년 1월 10일 접수, 2020년 2월 1일 1차 심사, 2020년 2월 1일 게재 확정되었습니다.