Regular paper | Journal of the KIECS. pp. 931-940, vol. 16, no. 5, Oct. 31. 2021, t. 109, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2021.16.5.931

정보보안 기술스트레스가 스트레인을 통한 보안정책 저항에 미치는 영향: 업무기술 적합성의 조절 효과 중심

황인호*

The Influence on the Information Security Techno-stress on Security Policy Resistance Through Strain: Focusing on the Moderation of Task Technology Fit

In-Ho Hwang*

요 약

정보 관리가 조직의 주요 성공 요인으로 인식되면서, 조직은 엄격한 정보보안 정책 및 기술 도입 및 운영을 위한 투자를 높이고 있다. 그러나, 엄격한 정보보안 기술은 업무에 정보보안을 적용하는 조직원에게 기술스트레스를 발생시킬 수 있다. 본 연구의 목적은 정보보안 기술스트레스가 스트레인을 통해 정보보안 정책 저항에 미치는 영향을 제시하고, 업무기술 적합성이 기술스트레스의 영향을 완화하는 것을 확인하는 것이다. 본 연구는 선행연구를 통해 연구 모델 및 가설을 제시하였으며, 설문 조사를 통해 확보된 표본을 활용하여 구조방정식을 통한 가설검증을 하였다. 연구 결과는 정보보안 기술스트레스(과부하, 복잡성)가 정보보안 스트레인(걱정, 피로)을 통해 정보보안 정책 저항에 영향을 주었으며, 업무기술 적합성이 기술스트레스와 스트레인 간의 관계를 조절하는 것을 확인하였다. 본 연구는 정보보안 정책 및 기술의 적용 시 발생 가능한 조직원의 스트레스와 완화 방법을 제시한 관점에서 내부의 정보보안 수준 향상을 위한 전략적 방향을 제시한다.

ABSTRACT

As information security(IS) is recognized as a critical success factor for organizational growth, organizations are increasing their investment in adopting and operating strict IS policies and technologies. However, when strict IS technology is adopted, IS-related techno-stress may occur in the employees who apply IS technology to their tasks. This study proposes the effect of IS-related techno-stress formed in individuals on IS policy resistance through IS strain and proves that task-technology fit mitigates the negative effect of techno-stress. Research models and hypotheses were presented through previous studies, and the secured samples were used, and structural equation modeling was applied to verify hypothesis. As a result of the study, it was confirmed that IS-related techno-stress (overload, complexity) affected IS policy resistance through IS strain (anxiety, fatigue), and that task-technology fit moderated the relationship between techno-stress and strain. This study suggests a strategic direction for improving the level of internal IS from the viewpoint of suggesting ways to mitigate the stress of employees that may occur when IS policies and technologies are adopted.

키워드

Information Security, Security Policy Resistance, Strain, Task Technology Fit, Techno-stress
정보 보안, 보안 정책 저항, 스트레인, 업무 기술 적합성, 기술 스트레스

* 교신저자: 국민대학교
• 접 수 일 : 2021. 08. 11
• 수정완료일 : 2021. 09. 13
• 게재확정일 : 2021. 10. 17
• Received : Aug. 11, 2021, Revised : Sep. 13, 2021, Accepted : Oct. 17, 2021
• Corresponding Author : In-Ho Hwang
College of General Education, Kookmin University,
Email : hwanginho@kookmin.ac.kr

Ⅰ. 서 론

정보보안이 조직의 중요한 관리 요인으로 인식되면서, 조직은 엄격한 정보보안 정책 및 조직에 특화된 기술 도입을 통해 조직 내·외부의 보안 위협으로부터 보호하기 위한 노력을 하고 있다[1]. 실제, 전 세계 정보보안 시장은 2020년 1,671억 달러에서 2028년까지 연평균성장률 10.9%[1]에 이를 것으로 예측된다[2].

조직의 정보보안 위협은 조직 외부 또는 내부에서 정보에 접근 가능한 방식이 존재할 경우 언제든 발생할 수 있다. 실제 조직 외부 기술로 인한 침입(해킹, 멀웨어 등)으로 인한 사고가 매년 전체 보안 사고의 약 70~80% 내외를 차지하고 있으며, 내부의 침입(정보 오남용, 악의적 노출 등)으로 인한 사고가 약 20~30%를 차지하고 있다[3]. 일찍부터 정보보안 위협 요인을 연구한 선행연구들은 외부 침입의 경우 조직에 특화된 엄격한 보안 기술을 접목함으로써 문제를 최소화할 수 있다고 보았으며, 내부 정보 노출 문제의 경우 개인들의 자발적인 정보보안 행동에 의존할 수 밖에 없으므로, 심리학적으로 개인의 보안 행동 동기 형성을 위한 지원이 무엇보다 필요하다고 보고 있다[4-6]. 특히, 내부자의 정보보안 관련 행동은 범죄학, 사회학, 심리학 등에서 적용되던 조직과 개인 사이의 행동 이론(제재 이론, 합리적 선택이론, 보호동기이론, 계획된 행동 이론 등)들을 접목함으로써, 조직이 추구하는 보안 목표 수준 달성을 위해서 구성원(내부자)가 확보해야 할 다양한 동기적 요인을 제시한 관점에서 높은 시사점을 가진다.

최근에는 조직원의 업무 효율성 및 성과 창출을 위해 도입한 정보 기술의 수준이 높을수록, 실제 사용자에게 부담이 될 수 있다는 관점의 연구 또한 제시되고 있는데, 대표적인 관점이 기술스트레스 이론(Techno-stress Theory)이다[7-9]. 특히, 기술스트레스 이론은 정보보안 기술과 연계되어, 조직 정보보안 수준 향상을 위해 도입하는 지속적이고 엄격한 보안 기술 및 정책이 긍정적인 행동을 추구하도록 하는 것이 아닌, 정보보안 정책 및 기술을 업무에 적용하는 구성원의 관점에서 역량의 한계성으로 인하여 스트레스를 일으켜 부정적 행동 또는 회피 행동을 일으킨다는 관점이 제기되고 있다[10,11]. 정보보안 분야에 기술스트레스를 제시한 연구들은 탐색적 관점에서 스트레스 발현 가능성을 제기한 관점에서 시사점을 가진다. 하지만, 선행연구들은 정보보안 기술스트레스 발현을 통해 부정적 행동으로 이어지는 과정을 명확하게 제시하지 못하였으며, 형성된 기술스트레스를 완화하기 위한 다각적인 조직 차원 또는 개인 차원의 조건 또는 방향을 제언하지 못하고 있다.

본 연구는 조직 차원의 엄격하고 체계적인 정보보안 기술 도입이 구성원에게 기술스트레스를 발현시킴으로써, 스트레인(걱정, 피로)을 일으켜 조직이 추구하는 정책에 부정적 영향을 줄 수 있음을 제시하고, 형성된 기술스트레스와 스트레인(걱정, 피로) 간의 관계를 업무기술 적합성이 완화할 수 있음을 확인하고자 한다. 이에 본 연구는 정보 기술 분야의 기술스트레스와 스트레인, 혁신 저항, 그리고 업무기술 적합성 관련 선행연구를 통해 연구가설을 제시하고, 가설 분석을 위한 변수 구성 및 표본 수집을 통해, 구조방정식 모델링을 통해 가설검증을 하고자 한다. 향후, 결과는 구성원 관점에서 엄격한 보안 기술 도입에 의한 스트레스의 예상 결과를 다각적으로 살피고, 기술스트레스의 부정적 영향을 완화하기 위한 방향을 제시함으로써, 조직 내부자의 보안 수준 달성을 위한 전략적 방향을 제시할 수 있다.

Ⅱ. 관련 연구

2.1 정보보안 정책 저항

조직 내 구성원들은 선행되었던 조직 내 표준 규범, 분위기 등과 결합하여 체화된 자신만의 업무적 체계를 가지고 있으며, 급격한 변화에 대한 저항(Resistance)을 통해 기존 균형을 유지하고자 한다[12]. 변화에 대한 저항은 현상을 변경하라는 외부적 압력에 있어 기존 현상을 유지하고자 하는 모든 기여적 행위로 정의된다[13]. 즉, 변화에 대한 저항은 환경적, 집단적 측면에 균형을 가지고자 하는 인간의 자연스러운 반응이기 때문에, 기술 도입, 혁신 정책 적용 등 급격한 변화를 추구하는 집단의 행동은 구성원의 행동적 저항을 이끌 수 있다.

특히, 정보보안 관점에서 조직은 외부의 급격하게

1) https://www.grandviewresearch.com/industry-analysis/cyber-security-market

변화하는 기술적 침입 및 국가적 정보보안 정책의 변화 등 환경적 변화에 대처하고 정보자산을 보호하기 위하여, 많은 자원을 투자하여 높은 수준의 정보보안 정책 및 기술을 도입하고자 한다[14]. 하지만, 정보보안에 의한 급격한 변화는 실제 업무에 정보보안 규정과 기술에 대한 적용을 요구받는 조직원의 관점에서 기존 형성된 균형을 흩트리는 역할을 하므로, 저항을 이끌 수 있다. 이와 같은 구성원들의 저항 의식은 높아질수록 조직이 추구하는 목표 및 요구 행동에 반하는 행동을 하도록 돕는다[6]. 따라서, 조직은 정보보안 정책 도입 시 조직원의 저항 수준을 판단하는 것이 필요하다. 본 연구는 정보보안 정책 저항에 영향을 주는 조건으로 기술스트레스와 스트레인을 제시한다.

2.2. 정보보안 기술스트레스 및 스트레인

집단과 개인 간의 관계에서 스트레스 원인과 스트레스의 결과를 잘 설명하는 관점이 거래이론(Transaction Theory)으로서, 거래이론은 개인은 개인 환경의 요구에 대한 균형을 가지기 위한 대처 방법 등 역량을 보유하고 있다고 보고 있으나, 환경 변화로 인하여 환경이 요구하는 사항을 받아들이거나 이행할 수 없을 때 스트레스를 발현시키고, 발현된 스트레스는 개인에게 부정적 심리 반응을 일으킨다는 관점이다[7]. 여기서, 스트레스(Stress)는 개인이 직면한 사건, 자극의 속성으로 인하여 발생하는 거래 과정으로서, 외부 스트레스 발생 요인으로 인하여 개인의 거래 과정에서 발현되는 불균형을 의미한다. 스트레인(Strain)은 거래 과정의 스트레스로 인하여 발현된 개인의 심리적 반응을 의미한다[15].

현대 조직은 과거와 달리 조직의 성과 달성을 위해 IT 기술을 활발하게 적용하고 있다. 이와 같은 IT 기술을 도입한 조직의 환경은 구성원들에게 도입한 IT 기술로 인하여 변화된 조직 업무 프로세스, 기술 적용 체계 등 새로운 업무 표준을 적용하여 빠르게 성과를 창출하는 것을 요구하고 있다. 즉, 빠르게 변화하는 환경에 대처하기 위해 도입한 정보 기술은 구성원에게 기존 균형을 흩트리고, 새로운 지식 등을 학습하는 등 변화에 적응하는 것을 요구하며, 개인이 이를 받아들이지 못하는 환경이 지속할 때, 기술스트레스(Techno-stress)는 발생한다[8].

정보보안 관점에서 기술스트레스는 다양한 측면에서 발생할 수 있다[10]. 조직은 정보보안을 위하여 엄격한 기술을 도입함으로써 보안 수준을 유지하고자 하지만, 조직원은 기술 도입으로 인하여 추가로 요구되는 활동이 발생하며, 기술의 복잡성으로 인하여 역량의 한계를 가질 수 있다. 즉, 정보보안 관련 기술스트레스는 대표적으로 기술 과부하(Techno Overload)와 기술 복잡성(Techno Complexity)으로 인하여 발생할 수 있다[11]. 기술 과부하는 보안 기술 도입이 개인의 업무의 양을 높이는 상황을 의미하며, 대표적으로, 업무 문서에 대한 보안 규정 준수를 위한 허가의 절차 또는 보관 방식의 변화로 인한 추가적 과업 증가 등이 발생할 수 있다. 기술 복잡성은 도입한 보안 기술 습득 조건이 높은 상황으로서, 기술 용어, 절차, 예외 사항 등의 체화에 소요시간 등을 들 수 있다.

조직 내 형성된 보안 관련 기술스트레스 요인들은 구성원에게 필요 요구사항을 증가시켜 개인의 한계 역량의 문제를 일으키는 과정을 통해, 심리적 부정 반응인 스트레인을 발현시킨다[15]. 기술에 의한 스트레인은 다양하게 발현되는데, 대표적으로 걱정과 피로가 있다. 걱정(Anxiety)은 특정 환경에 대한 필요 정보 전체를 확보하지 못하여 발현되는 두려움 또는 염려를 의미한다[16]. 특히, 걱정은 조직의 기술에 대한 적용 가능성에 대한 두려움으로 자주 발현되며, 엄격하고 체계화된 정보보안 기술에 대한 활용 정보를 명확하게 확보하지 못할 때 걱정을 발현시킬 수 있다[5]. 즉, 정보보안 관련 기술의 어려움으로 인한 두려움이 형성될 때, 걱정이 발생할 수 있다. 피로는 신체적 및 심리적 요인의 복합적 상호작용으로 유도되는 자기 평가된 피로감으로서[17], 환경 내 개인의 주관적 경험을 통해 형성된 느낌을 의미한다. 정보보안과 관련하여, 다양한 보안정책 환경 및 엄격한 규정 등으로 인하여 발생한 갈등적 요인이 정보보안 피로를 일으킬 수 있으며, 부정적 행동을 야기한다[4]. 즉, 정보보안 정책준수와 관련된 갈등 등으로 인하여 개인의 부정적 평가가 지속할 때 피로는 형성된다.

정보보안 관련 스트레인(정보보안 기술 걱정, 정보보안 정책준수 피로)이 지속해서 형성되면, 조직이 요구하는 수준인 정보보안 준수 행동을 회피하는 행동을 할 가능성이 높다[7,10,11]. 따라서, 본 연구는 정보보안 준수 과정에서 발생한 스트레인이 정보보안 정책에 대한 저항을 일으킬 것으로 판단하며, 스트레인

과 저항 간의 가설을 제시한다.

H1: 정보보안 기술 관련 걱정은 정보보안 정책 저항에 정(+)의 영향을 미친다.

H2: 정보보안 준수 관련 피로는 정보보안 정책 저항에 정(+)의 영향을 미친다.

또한, 기술스트레스와 스트레인 간의 관계에서 개인을 둘러싼 정보보안 기술 과부하와 복잡성으로 인하여 발생 가능한 스트레스 과정이 다양한 스트레인을 발현시킨다[4,17]. 특히, 연구는 정보보안 기술 관련 걱정과 정보보안 준수 관련 피로감의 형성에 기술스트레스가 영향을 줄 것으로 판단하며, 기술스트레스와 스트레인 간의 가설을 제시한다.

H3a. 정보보안 기술 과부하는 정보보안 기술 관련 걱정에 정(+)의 영향을 미친다.

H3b. 정보보안 기술 과부하는 정보보안 기술 관련 걱정에 정(+)의 영향을 미친다.

H4a. 정보보안 기술 과부하는 정보보안 정책준수 관련 피로에 정(+)의 영향을 미친다.

H4b. 정보보안 기술 과부하는 정보보안 정책준수 관련 피로에 정(+)의 영향을 미친다.

2.4. 업무기술 적합성

오늘날 조직은 정보 기술의 효과적 활용을 통해 구성원 및 조직 차원의 성과 창출을 추구하고 있다. 구성원이 업무에 기술을 효과적으로 적용하고 활용하기 위해서는 기술이 조직의 특성에 맞게 구축됨으로써, 기술의 유용성을 인식하는 것이 필요하다[18]. 이와 같은 조직에 적합한 기술의 성과에 대한 관점이 업무기술 적합성이다. 업무기술 적합성(Task Technology Fit)은 조직 및 개인의 업무 특성과 기술 특성의 적합성이 높아야 기술 유용성이 높아져 업무 성과를 높인다는 개념이다[19].

업무기술 적합성은 개인의 기술에 대한 인식을 변화시킴으로써 정보 기술의 활용성을 높이기 때문에, 개인 성과 목표 달성에 기여할 뿐 아니라 기술에 의한 스트레스를 감소시키는 역할을 한다[20]. 특히, 정보보안은 조직의 업무적 특성에 맞추어 정책을 도입하고, 맞춤형 기술을 적용하는 경향이 있으므로, 정보보안 관련 기술이 업무와 적합함을 알리기 위한 조직 차원의 노력이 필요하다[21,22]. 즉, 정보보안 관련 기술이 업무와 높은 적합성을 가진다고 인식할수록 기술에 의한 스트레스 발현이 감소할 것으로 판단한다. 이에 본 연구는 업무 정보보안 기술 적합성이 기술스트레스와 스트레인 간의 관계에 조절 효과를 가질 것으로 판단하고, 연구가설을 제시한다.

H5a. 업무-정보보안 관련 기술 적합성은 기술 과부하와 걱정 간의 관계를 조절한다.

H5b. 업무-정보보안 관련 기술 적합성은 기술 과부하와 피로 간의 관계를 조절한다.

H5c. 업무-정보보안 관련 기술 적합성은 기술 복잡성과 걱정 간의 관계를 조절한다.

H5d. 업무-정보보안 관련 기술 적합성은 기술 복잡성과 피로 간의 관계를 조절한다.

III. 연구 모델 및 자료 수집

본 연구는 그림 1과 같이 정보보안 수준 향상을 위해 도입한 조직의 보안 기술로 인하여 구성원에게 발생할 수 있는 기술스트레스가 스트레인을 통해 보안 정책 저항에 이르는 관계를 확인하고, 기술업무 적합성의 완화 효과를 확인하는 것을 목적으로 한다.

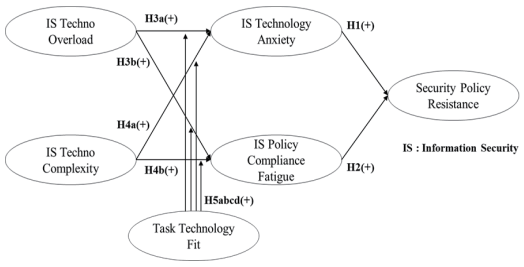

그림 1. 연구 모델
Fig. 1 Research model

연구 모델 검증은 선행연구를 통해 도출한 요인들의 영향 관계를 정보보안 분야에 적용하고자 하며, 설문지 기법을 통해 확보한 표본을 AMOS 22.0 기반의 구조방정식모델링을 실시한다.

연구 모델에 적용한 6개의 요인의 설문항목은 정보기술 및 혁신 분야에 적용된 항목들을 정보보안 특성을 반영하여 설문을 도출하였다. 설문 문항은 7점 리커트 척도(1점: 매우 그렇지 않다 - 7점: 매우 그렇

다)로 구성하였다. 정보보안 기술스트레스는 조직 내 도입된 정보보안 관련 기술로 인하여 발생 가능한 스트레스 원인으로서[9], 정보보안 기술 과부하는 선행연구로부터 3개의 측정 문항을 도출하였으며, 일례로 “나는 정보보안 기술 정책에 맞추어 일하도록 요구받음”과 같이 적용하였다. 정보보안 기술 복잡성은 선행연구로부터 4개의 측정 문항을 도출하였으며, 일례로 “정보보안 기술을 이해하고 적용하기 위해 시간이 필요함”과 같이 적용하였다. 정보보안 스트레인은 정보보안 관련 기술 등으로 인하여 발생한 스트레스의 심리적 반응으로서 연구는 걱정과 피로를 적용하였다. 정보보안 기술 걱정은 선행연구로부터 4개의 측정 문항을 도출하였으며[16], 일례로 “정보보안 시스템을 사용하는데 우려를 느낌”과 같이 적용하였다. 정보보안 행동 피로는 선행연구를 통해 4개의 측정 문항을 도출하였으며[17], 일례로 “정보보안 활동으로 인해 긴장을 풀기가 힘듦”과 같이 적용하였다. 보안정책 저항은 정보보안 정책으로 인한 변화에 대한 주저함 수준으로서 선행연구를 통해 3개의 측정 문항을 도출하였으며[6], 일례로, “보안정책 변화가 개인적으로 이익이 되지 않는다고 생각함”과 같이 적용하였다. 업무 정보보안 기술 적합성은 도입된 보안 기술의 기능이 업무에 적합한 수준으로서[18], 선행연구를 통해 4개의 측정 항목을 도출하였으며, 일례로 “정보보안 기술(방화벽, 문서관리&보호 기술 등)은 유용함”과 같이 적용하였다.

표 1. 표본의 인구통계학적 특성
Table 1. Demographic characteristics of samples

Demographic Categories		Frequency	%
Industry	Manufacture	69	16.4
	Service	352	83.6
Gender	Male	328	77.9
	Female	93	22.1
Age	Under 30	59	14.0
	31 - 40	162	38.5
	Over 40	200	47.5
Job Position	Under Manager	162	68.2
	Manager	125	29.7
	Over Manager	134	31.8
Total		421	100.0

연구 대상은 정보보안 정책 및 관련 기술을 도입한 조직에 근무하는 근로자들을 대상으로 하며, 온라인 설문을 하였다. 연구는 M리서치가 보유한 직장인 패널 중 정보보안 정책 및 관련 기술을 업무에 적용하는지를 사전 질문하고, 해당하는 직장인만 설문에 참여하도록 구조화하였다. 설문 전 연구목적 및 통계 활용의 방법을 고시하였으며, 사용에 허가한 사람만 설문하도록 하였다. 설문은 2021년 4월 말에 실시하였다. 총 421명의 표본을 확보하였으며, 표본의 특성은 표 1과 같다.

Ⅳ. 분 석

4.1 신뢰성 및 타당성 분석

본 연구는 요인별 측정 항목이 2개 이상으로 구성되어 있으므로, 요인별 일관성 확인 방법인 신뢰성 분석과 요인 내 항목의 적정성과 요인 간 차별성을 측정하는 타당성 분석을 하였다.

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

Constructs		Factor Loading	Cronbach's Alpha	CR	AVE
TO	TO1	0.843	0.877	0.784	0.645
	TO2	0.758			
TC	TC1	0.730	0.900	0.834	0.557
	TC2	0.777			
	TC3	0.771			
	TC4	0.758			
ISA	ISA1	0.753	0.924	0.861	0.608
	ISA2	0.788			
	ISA3	0.785			
	ISA4	0.699			
ISF	ISF1	0.716	0.937	0.857	0.666
	ISF3	0.703			
	ISF4	0.727			
PR	PR1	0.751	0.906	0.825	0.612
	PR2	0.729			
	PR3	0.721			
TF	TF1	0.874	0.944	0.911	0.719
	TF2	0.888			
	TF3	0.891			
	TF4	0.893			

TO(Techno Overload), TC(Techno Complexity), ISA(IS Anxiety), ISF(IS Fatigue), PR(Policy Resistance), TF(Task Technology Fit)

신뢰성은 SPSS 21.0을 활용하여 베리맥스 기법을 적용한 탐색적 요인 분석을 실시하고, 크론바흐 알파 값을 도출하여 확인하였다. 6개 요인(22개 항목) 중 신뢰성에 문제가 있는 2개 요인(TO3, ISF2)를 제외하였으며, 표 2와 같이 최종적으로 도출된 크론바흐 알파 값은 0.7 이상으로 나타나 신뢰성을 확보하였다[23].

타당성은 확인적 요인분석을 실시하여 집중 타당성과 판별 타당성을 확인한다. 집중 타당성은 요인 측정 항목의 일관성을 측정하는 것으로서 개념 타당성(CR)과 평균분산추출(AVE)을 확인한다. 확인적 요인분석에 대한 구조모델의 적합성을 확인한 결과는 χ^2/df = 1.947, RMSEA = 0.047, GFI = 0.931, AGFI = 0.906, NFI = 0.962, 그리고 CFI = 0.981로 나타났으며, 표 2와 같이 집중 타당성인 CR(0.7 이상 요구), AVE(0.5 이상 요구) 모두 타당성을 확보하였다[24].

판별 타당성은 요인의 상관계수와 평균분산추출의 제곱근을 비교하되 평균분산추출보다 상관계수가 낮을 경우 판별 타당성을 확보했다고 본다[24]. 분석 결과 표 3과 같이 판별 타당성을 확보하였다.

표 3. 판별타당성 결과
Table 3. Result for discriminant validity

Constructs	1	2	3	4	5	6
TO	**0.803**					
TC	.69**	**0.746**				
ISA	.57**	.66**	**0.780**			
ISF	.72**	.69**	.71**	**0.816**		
PR	.62**	.61**	.75**	.73**	**0.782**	
TF	-.31**	-.42**	-.45**	-.46**	-.47**	**0.848**

Note: Values in bold type = square root of the AVE
TO(Techno Overload), TC(Techno Complexity), ISA(IS Anxiety), ISF(IS Fatigue), PR(Policy Resistance), TF(Task Technology Fit)
**: $p < 0.01$

연구는 적용 요인 모두를 동일시점에 설문으로 측정하였기 때문에, 독립변수와 종속변수 간의 편차가 발생할 가능성이 있다. 이에, 연구는 공통방법편의 문제를 확인하였다. 연구는 비측정잠재방법요인 측정 기법을 적용하였다[25]. 해당 방법은 확인적 요인분석 모델과 공통 요인을 추가 적용한 모델 간의 측정 항목의 변화량의 크기를 확인하는 기법이다. 확인적 요인분석 모델과 공통 요인을 추가한 모델 간의 측정 항목의 변화량을 측정한 결과, 차이 값이 0.2 이하로 나타나 공통방법편의 문제는 높지 않았다.

4.2 구조방정식모델링 결과

연구 모델은 조절 효과가 포함되어 있으므로, 조절 효과를 제외한 모델에 대한 주 효과 분석을 우선적으로 실시하고, 조절 효과 검증을 추가로 실시한다. 주 효과 검정은 구조모델의 적합성 검정, 연구 모델 상 경로 분석(β), 그리고 결과변수에 대한 영향력(R^2)을 실시한다. 첫째, 주 효과 검증을 위한 연구 모델의 구조 모형 적합도 분석 결과는 χ^2/df = 2.746, RMSEA = 0.064, GFI = 0.932, AGFI = 0.902, NFI = 0.960, CFI = 0.974와 같이 나타났다. 다소 RMSEA 값이 요구사항보다 높으나 0.1 이하까지 허가하기 때문에, 주 효과 분석에 문제가 없는 것으로 파악되었다.

표 4. 주 효과 분석 결과
Table 4. Results of main effect tests

	Path	Coefficient	t-value	Result
H1	ISA → PR	0.523	11.073**	Support
H2	ISF → PR	0.415	9.155**	Support
H3a	TO → ISA	0.209	3.410**	Support
H3b	TO → ISF	0.402	7.290**	Support
H4a	TC → ISA	0.593	9.184**	Support
H4b	TC → ISF	0.496	8.910**	Support
R^2: PR = 71.6%, CA = 57.0%, CF = 69.0%				

TO(Techno Overload), TC(Techno Complexity), ISA(IS Anxiety), ISF(IS Fatigue), PR(Policy Resistance)
**: $p < 0.01$

둘째, 연구 모델에 적용된 경로 간의 검증을 하였다. 가설 1은 정보보안 기술 관련 걱정이 보안정책 저항을 높인다는 것으로, 가설검증 결과 신뢰 수준 95% 기준에서 유의하였다(H1: β= 0.523, $p < 0.01$). 가설 2는 정보보안 정책준수 관련 피로가 보안정책 저항을 높인다는 것으로, 가설검증 결과 신뢰 수준 95% 기준에서 유의하였다(H2: β= 0.415, $p < 0.01$). 가설 3은 정보보안 기술 과부하가 정보보안 걱정 및 피로를 높인다는 다는 것으로, 가설검증 결과 신뢰 수준 95% 기준에서 유의하였다(H3a: β= 0.209, $p < 0.01$; H3b: β= 0.402, $p < 0.01$). 가설 4는 정보보안 기술 복잡성이 정보보안 걱정 및 피로를 높인다는 것으로, 가설검증 결과 신뢰 수준 95% 기준에서 유의하였다(H4a: β = 0.593, $p < 0.01$; H4b: β= 0.496, $p < 0.01$).

마지막으로, 결과변수의 결정력을 확인하였다. 보안정책 저항은 걱정과 피로로부터 71.6%의 영향을 받았

으며, 걱정은 기술 과부하와 기술 복잡성으로부터 57.0%, 피로는 기술 과부하와 기술 복잡성으로부터 69.0%의 영향을 받는 것으로 나타났다.

추가로, 연구는 업무기술 적합성이 정보보안 기술스트레스와 스트레인 간의 긍정적 영향 관계를 조절할 것으로 판단하고 조절 효과를 확인하였다. 본 연구는 적용 요인 모두 리커트 척도로 구성되어 있으므로, 상호작용 항을 도출하여 상호작용 항의 결과변수에 미치는 경로 수준을 통하여 확인한다. 구조방정식을 통한 상호작용 항 도출 방법은 여러 가지가 있으나, 본 연구는 독립변수와 조절변수를 모두 연결하되, 비표준화잔차 값을 활용하는 기법인 직교화접근법을 적용하고자 한다[26]. 분석 결과는 표 5와 같다.

표 5. 조절 효과 분석 결과
Table 5. Results of moderating effect tests

	Path	Coefficient	t-value	Result
H5a	TO → ISA	0.496	9.685**	Support
	TF → ISA	-0.321	-7.019**	
	TOxTF→ISA	-0.070	-2.095*	
H5b	TO → ISF	0.656	14.282**	Support
	TF → ISF	-0.282	-7.184**	
	TOxTF→ISF	-0.069	-2.447*	
H5c	TC → ISA	0.635	12.254**	Not Support
	TF → ISA	-0.185	-3.998**	
	TCxTF→ISA	-0.066	-1.628	
H5d	TC → ISF	0.688	13.847**	Not Support
	TF → ISF	-0.169	-3.937**	
	TCxTF→ISF	-0.056	-1.487	

TO(Techno Overload), TC(Techno Complexity), ISA(IS Anxiety), ISF(IS Fatigue), TF(Task Technology Fit)
*: $p < 0.05$, **: $p < 0.01$

업무기술 적합성은 기술 과부하와 스트레인(걱정, 피로) 간의 관계를 조절하였으나, 기술 복잡성과 스트레인(걱정, 피로) 간의 관계는 조절하지 않는 것으로 나타났다. 상세히 업무기술 적합성의 조절 효과를 확인하기 위하여 평균을 기준으로 구분된 그래프를 표현하였다. 업무 과부하는 스트레인(걱정, 피로)을 높이는 요인이나, 업무-기술 적합성이 높은 집단에서 스트레인을 낮추는 역할, 즉 그림2, 그림 3과 같이 완화효과를 가지는 것으로 나타났다.

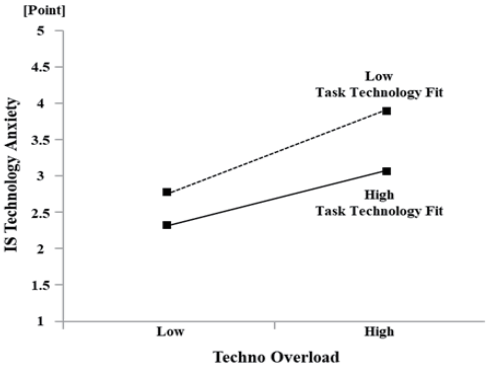

그림 2. TTF의 조절효과 (H5a)
Fig. 2. Moderation Effect of TTF (H5a)

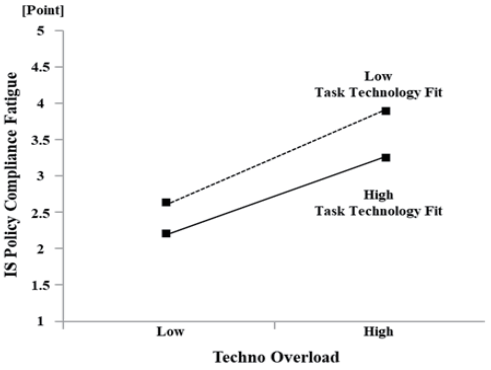

그림 3. TTF의 조절효과 (H5b)
Fig. 3. Moderation Effect of TTF (H5b)

V. 결 론

정보자원관리 중요성의 증가에 따라 조직 차원의 정보보안 정책 및 기술에 대한 투자는 높아지고 있다. 조직은 더욱 엄격하고 체계적인 정보보안 정책 및 기술을 도입하고 있으나, 해당 정책 및 기술을 업무에 적용해야 하는 조직원의 관점에서 발생 가능한 기술 차원의 스트레스에 대한 관심은 부족하다.

본 연구는 정보보안 기술 도입에 따라 형성 가능한 기술스트레스가 스트레인을 형성하여 정보보안 정책 저항에 미치는 영향을 제시함으로써, 조직 내 정보보안 기술이 미치는 부정적인 측면을 강조하였다. 또한, 연구는 업무-기술 적합성을 정보보안 기술스트레스가 주는 스트레인(걱정, 피로)을 완화하기 위한 요인으로

적용하고 관련성을 확인하였다.

연구는 가설검증을 위하여 정보보안 정책 및 기술을 운용하고 있는 조직에 근무하는 근로자들을 대상으로 온라인 설문을 하였으며, 구조방정식모델링을 통해 가설검증을 하였다. 결과적으로 구성원에게 형성된 정보보안 기술 과부하와 기술 복잡성이 정보보안 기술 걱정과 정보보안 준수 활동 피로를 통해 정보보안 정책 저항을 높이는 것을 확인하였으며, 업무 정보보안 기술 관련 적합성이 형성될 때, 기술스트레스와 스트레인 간의 관계를 완화하는 것을 확인하였다.

결과는 첫째, 체계적인 정보보안 기술 및 정책 도입이 실제 사용자인 조직원의 기술스트레스를 발현시킬 수 있음을 제시하였다. 조직 내부자에 의한 정보노출 사고는 전체 사고의 20~30%를 차지하고 있을 정도로 높은 수준이기 때문에, 보안 기술이 내부자의 부정적 행동 동기를 형성시키는 것을 사전에 인식하여 대처를 위한 전략 수립에 도움이 될 수 있을 것으로 판단한다. 둘째, 형성된 기술스트레스의 부정적 심리 발현을 감소시키기 위한 요인을 제시하였다. 업무기술 적합성은 개인이 판단할 수 있는 기술의 효용성이 업무적 활동과 연관성이 높은 것을 의미한다. 따라서, 결과는 업무기술 적합성에 대한 인식 수준을 향상하기 위한 노력이 필요함을 제시한다. 즉, 조직은 정보보안 기술이 개인의 업무와 무관하지 않음을 홍보, 캠페인, 교육 등으로 알리는 활동을 다각적으로 실행하는 것이 필요하다.

연구는 정보보안 관련 기술스트레스의 부정적 측면과 완화 관점을 제시하였다. 향후 연구에서는 조직 관점, 개인 관점 등 다각적인 기술스트레스 완화요인을 제시하는 것이 필요하다.

References

[1] W. Seo, "A study on the optimized balance module of security policy to enhance stability in the service-based information system," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 13, no. 6, 2018, pp. 1155-1160.

[2] Grandviewresearch, "Cyber security market size, share & trends analysis report by component, by security type, by solution, by services, by deployment, by organization, by application, by region, and segment forecasts, 2021 - 2028," *Report,* 2021.

[3] Verizon, "2020 data breach investigations report," *Report,* 2020.

[4] H. Chen, Y. Li, L. Chen, and J. Yin, "Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): The roles of information security-related conflict and fatigue," *J. of Enterprise Information Management*, vol. 34, no. 3, 2020, pp. 770-792.

[5] 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.

[6] M. J. Merhi and P. Ahluwalia, "Examining the impact of deterrence factors and norms on resistance to information systems security," *Computers in Human Behavior*, vol. 92, 2019, pp. 37-46.

[7] A. M. Fuglseth and Ø. Sørebø, "The effects of technostress within the context of employee use of ICT," *Computers in Human Behavior*, vol. 40, 2014, pp. 161-170.

[8] 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.

[9] 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.

[10] 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.

[11] I. Hwang and O. Cha, "Examining technostress creators and role stress as potential threats to employees' information security compliance," *Computers in Human Behavior*, vol. 81, 2018, pp. 282-293.

[12] S. Oreg, "Personality, context, and resistance to organizational change," *European J. of Work and Organizational Psychology*, vol. 15, no. 1, 2006, pp. 73-101.

[13] Y. Bao, "Organizational resistance to performance

enhancing technological innovations: A motivation threat ability framework," *J. of Business & Industrial Marketing*, vol. 24, no. 2, 2009, pp. 119-130.
[14] W. Seo, "A study on the application of modularization technique to standard security policy to protect information assets and the securement of confidentiality and integrity," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 14, no. 1, 2019, pp. 111-118.
[15] R. Ayyagari, V. Grover, and R. Purvis, "Technostress: Technological antecedents and implications," *MIS Quarterly*, vol. 35, no. 4, 2011, pp. 831-858.
[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] A. Lee, S. Son, and K. Kim, "Information and communication technology overload and social networking service fatigue: A stress perspective," *Computers in Human Behavior*, vol. 55, 2016, pp. 51-61.
[18] T. C. Lin and C. C. Huang, "Understanding knowledge management system usage antecedents: An integration of social cognitive theory and task technology fit," *Information & Management*, vol. 45, no. 6, 2008, pp. 410-417.
[19] D. L. Goodhue and R. L. Thompson, "Task-technology fit and individual performance," *MIS Quarterly*, vol. 19, no. 2, 1995, pp. 213-236.
[20] A. Shirish, "Cognitive-affective appraisal of technostressors by ICT-based mobile workers and their impacts on technostrain," *Human Systems Management*, vol. 40, no. 2, 2021, pp. 265-285.
[21] C. C. Angolano, I. R. Guzman, M. S. Garmon, and C. J. Navarrete, "Information technology security task-technology fit based on the technology-to-performance chain theory," In *Proc. of the 50th annual conf. on Computers and People Research* (17-26), Milwaukee, Wisconsin, USA, 2012.
[22] H. Kim, "A Study on cloud-based secure file management security," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 14, no. 1, 2019, pp. 243-250.
[23] J. C. Nunnally, *Psychometric theory (2nd ed.)*. New York: McGraw-Hill, 1978.
[24] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of Marketing Research*, vol. 18, no. 1, 1981, pp. 39-50.
[25] 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," *Journal of Applied Psychology*, vol. 88, no. 5, 2003, pp. 879-903.
[26] G. C. Lin, Z. Wen, H. W. Marsh, and H. S. Lin, "Structural equation models of latent interactions: Clarification of orthogonalizing and double-mean-centering strategies," *Structural Equation Modeling*, vol. 17, no. 3, 2010, pp. 374-391.

저자 소개

황인호(Inho 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