Journal of Digital Convergence
Vol. 19. No. 11, pp. 327-339, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.11.327

보안 정책 준수 동기에 관한 연구: 기술 위협 회피 관점에서

임명성
삼육대학교 경영학과 부교수

Security Policy Compliance Motivation: From Technology Threat Avoidance Perspective

Myung-Seong Yim
Associate Professor, Department of Business Administration, Sahmyook University

요 약 본 연구는 TTAT를 기반으로 정보보안 정책의 관점에서 보안 정책의 특성(정책의 취약성, 정책의 효과성, 정책 준수 비용, 정책 준수 효능감, 사회적 영향력)이 조직의 정보보안 정책 준수 동기에 미치는 영향을 살펴보기 위해 수행되었다. 분석 결과는 다음과 같다. 첫째, 보안 정책의 위협은 정책 준수 동기에 유의한 영향을 미치는 것으로 나타났다. 둘째, 정책의 효과성은 준수 동기에 통계적으로 유의한 영향을 미치지 못하는 것으로 나타났다. 셋째, 정책 준수 비용은 정책 준수 동기에 유의한 영향을 미치는 것으로 나타났다. 넷째, 정책 준수 효능감은 회피 동기에 유의한 영향을 미치지 못하는 것으로 나타났다. 마지막으로, 사회적 영향력은 준수 동기에 유의한 영향을 미치는 것으로 나타났다.

주제어 : 정보 보안, 보안 정책, 보안 효과, 준수 동기, 기술위협회피이론

Abstract The ultimate aim of this study is to examine the effect of security policy characteristics (policy threat, policy effectiveness, policy compliance cost, policy compliance self-efficacy, social influence) on organizational information security policy compliance motivation based on TTAT (Technology Threat Avoidance Theory). We found the following results. First, the security policy threat has a significant positive effect on policy compliance motivation. Second, it was found that the policy effectiveness has a statistically significant effect on the compliance motivation. Third, the policy compliance cost has an influence on the policy compliance motivation. Fourth, the policy compliance self-efficacy does not have an effect on compliance motivation. Finally, social influence has a significant effect on compliance motivation.

Key Words : Information Security, Security Policy, Security Effectiveness, Compliance Motivation, Technology Threat Avoidance Theory

1. 서론

1.1 연구배경

정보기술은 양날의 검이다[1]. 선한 목적으로 사용된다면 조직은 생산성 향상, 효율성 개선 등 다양한 긍정적 성과를 기대할 수 있다. 개인에게는 단순반복적 행동으로부터 해방, 편리함, 신속함, 연결성 등 다양한 측면에서 기술 사용의 혜택을 얻을 수 있다. 반면, 해킹,

*Corresponding Author : Myung-Seong Yim(msyim@syu.ac.kr)
Received August 27, 2021 Revised September 5, 2021
Accepted November 20, 2021 Published November 28, 2021

DDoS(Distributed Denial of Services), Spyware, Ransomware, Adware, e-mail spam, worms, viruses 등과 같이 악의적으로 사용된다면, 개인에게는 컴퓨터 자산 피해, 금전적 피해, 정신적 피해를 줄 수 있으며, 조직적 관점에서도 재산 피해, 업무 생산성 문제, 기업의 이미지와 명성의 훼손, 주가 피해 등 다양한 부정적 결과를 유발할 수 있다[2].

기술을 원래 도입 목적에 맞게 사용한다면 문제는 없으나 그렇지 않은 경우가 많기 때문에 오늘날과 같이 끊임없는 보안 사고와 대량의 피해자가 발생하고 있다. 2020년 국가·공공 분야에 대한 사이버 공격 시도 건수는 하루 평균 162만 건으로, 2016년 41만 건보다 약 4배 증가했다[1]. 문제는 기업이 주로 의존하는 기술 보안 솔루션은 조직 자산의 안전을 완벽히 보장하지 못한다는 것이다[3][4]. 2014년 IBM의 조사에 따르면, 성공적으로 구축된 시스템의 데이터 유출 사고의 70%가 인적 실패로 인해 발생했다[5]. 기업 보안 전문업체 Fortinet이 기업의 기술관리자들을 대상으로 시행한 조사에 따르면[1], 응답 기업 중에 42%가 악의적 내부자 공격(예. 직원이 악성 링크 클릭)을 경험했다고 응답했다. 또한, 31%는 우발적 내부자 보안 침해 사고를 경험했다고 응답했다.

이와 같이 인적 보안이 중요함에도 불구하고 인간의 보안 행동에 대한 연구는 여전히 초기단계이다[4]. 1996년부터 2018년까지 발간된 연구자료를 보면 약 4% 미만의 연구만이 인간의 보안 행동에 관심을 두었다[5].

조직은 구성원들이 조직의 정보 자산을 안전하게 관리하기 위해서 정보보안 정책을 수립하여 개인의 보안 행동을 유도한다. 하지만, 경영진들은 정책 수립에 관한 관심만 높을 뿐 정책을 준수하도록 구성원들의 행동을 유도하는 과정에 대한 이해와 관심은 여전히 부족하다. 구성원들의 정보보안 정책 준수는 다양한 조직 요인뿐만 아니라 개인적 요인과도 밀접하게 연관됨에도 불구하고 구성원들의 정책 준수 행동을 어떻게 유도할지는 여전히 많은 연구가 필요하다[6][7].

정보보안 정책은 조직의 보안을 강화할 수 있는 핵심 도구이다[3]. 보안 정책을 통해 구성원들은 자사의 정보자원을 보호하기 위해 어떻게 행동해야 하는지 알 수 있다[3]. 또한, 구성원들은 보안 정책을 통해 보안 사고의 예방, 탐지, 대응 방법도 알 수 있다[3]. 하지만, 구성원들이 보안 정책을 준수하지 않으면 보안 정책의 실효성은 상실된다[8]. Liu et al.[9]은 구성원들이 조직의 정보 자원을 활용하는 데 있어서 정보보안 정책의 미준수는 지속적인 보안 사고의 주된 원인이라고 지적했다.

1.2 선행연구

보안 정책은 조직의 정보 자원에 적절한 그리고 부적절한 사용이 무엇인지 판단할 수 있는 지침을 제공한다[10]. 정보보안을 위한 대책으로 보안 정책은 구성원들의 보안 위반 행위를 억제하는 수단으로 작용한다[10]. 선행연구에 따르면, 보안 정책은 조직의 정보기술 남용 수준을 낮추는 것으로 나타났다[10]. 따라서, 본 연구는 조직 구성원들의 정보보안 정책 준수 행동를 유도할 수 있는 방안을 마련하기 위해서 보안 정책 준수 동기에 미치는 선행요인을 탐구하고자 한다. 이를 위해서 TTAT(기술위협 회피 모형)를 이론적 배경으로 활용하고자 한다.

Chen and Liang[11]은 TTAT가 정보보안 행동을 설명하는 데 매우 유용하고 논리적인 모형임에도 불구하고 본 모형에 대한 실증적 검정은 많이 이루어지지 않고 있다고 지적했다. TTAT는 IT 위협에 직면하였을 때 기술 사용자의 동기를 이해하기 위해 개발되었다[2]. TTAT는 개인의 보안행위의 결정요인과 행위 결정 과정을 설명해 준다[12]. 따라서, 정보보안 측면에서 사용자의 행위를 설명하는 데 매우 유용한 모델이다. 하지만, 선행연구를 살펴보면, TTAT가 Malware, 앱, 기기를 기반으로 연구하였을 뿐, 구성원들의 보안 행동의 기반이 되는 보안 정책의 특성과 영향을 살펴보지 않았다.

Liang and Xue[1]는 Spyware의 위협과 대응 반응에 대해 살펴보았다. Young et al.[12]은 Malware(Malicious Software)의 위협과 반응을 연구했다. Arachchilage and Love[13]는 피싱(phishing) 공격의 위협 회피 행동에 대해 연구했다. Ikhalia et al.[14]은 Facebook app 사용자의 보안 인지 수준을 평가했다. Chen and Li[2]는 모바일 기기 사용자의 프라이버시 보안 확신 행위에 대해 실증분석했다. Cho and Ip[6]은 BYOD(Bring Your Down Device)의 수용을 TTAT에서 제시된 변수들을 사용하여 실증분석했다.

물론, Cho and Ip[6]은 BYOD 정책의 효과성, BYOD 정책 준수 비용, BYOD 정책 준수 효능감 등을 연구모형에 반영하였으나 본 모형에 포함된 사회적 영향력은 BYOD 사용에 대한 개념이며, 종속변수도 위협 회피 동기나 위협 회피 행동이 아닌 BYOD 수용이라는 점에서 보안 정책의 특성을 제대로 반영했다고 보기 어렵다.

1) Fortinet (2021). 2021년 운영기술 및 사이버 보안 현황 보고서.

1.3 연구목적

TTAT가 보안 행동에 관한 이론적 기반을 제공하고 다양한 연구에서 본 모형을 기반으로 정보보안 관련 연구를 수행했음에도 불구하고 정보보안의 핵심 요소인 보안 정책에 관한 학술적 연구는 아직 시도되지 않았다. 따라서, 본 연구는 선행 연구의 이러한 한계점을 보완하기 위해서 정보보안 정책의 정황을 반영한 연구를 수행하고자 한다. 특히, 선행 연구에서 시도되지 않았던 TTAT를 기반으로 보안 정책 준수 동기에 미치는 영향을 보안 정책 요인들을 기반으로 실증적으로 검정하고자 한다.

2. 이론적 배경

2.1 정보보안 정책

정보보안에 있어서 사용자가 보안 정책을 수용(준수)하도록 유도하는 요인에 대안 이해는 정보보안 문제를 해결하는 데 있어서 기본단계이다[15]. 정보보안 정책이란 조직 내 보안 강화를 위한 사회적, 정치적, 법률적, 경제적, 기술적 규정을 말한다[16]. 따라서, 보안 정책은 조직의 내부 및 외부의 위협으로부터 조직의 정보 자산을 보호하기 위한 조직적 계획을 포함하며, 보안 구현 방법을 제시하며, 정보보안을 위한 경영진과 구성원의 행동 지침이 된다[16].

기업의 정보보안 정책은 경영진에 의해 작성된다[17]. 이 관점에서 보안 정책은 보안에 대한 경영진의 기대가 조직의 정보 보안 요구사항에 맞는 구성원들의 행동으로 이어지도록 해주는 도구이다[16]. 사용자 차원에서 보안 정책은 구성원들의 적절한 보안 행동을 위한 지침이 된다[16].

2.2 기술 위협 회피 이론

그동안 정보보안 관련 연구에서 사용된 기반 이론은 주로 조직적 수준에서 제시된 이론들이다[1]. 즉 개인 수준에서 구성원들의 기술 위협 회피를 설명해주는 이론은 부재하다[1]. Liang and Xue[1]는 개별 IT 사용자의 위협 회피 행동을 설명할 수 있는 기술 위협 회피 모형(TTAT: Technology Threat Avoidance Theory)을 제안했다. 본 모형은 인공두뇌학 이론(cybernetic theory)과 스트레스 대응 이론(coping theory)을 기반으로 개발되었다.

인공두뇌학 이론의 기본 가정은 기술 사용자의 위협 회피는 현재 상태와 예상치 못한 결과 상태 간의 불일치를 확장해주는 역동적 양의 피드백 순환(dynamic positive feedback loop)으로 설명할 수 있다는 점이다[18][19]. 양의 피드백 순환에서, 현재 상태가 지나치게 예측불가능한 결과 상태와 연관될 때 인간의 행동은 활성화된다[18]. 반면, 이 두 상태 간의 불일치 정도가 지나치게 클 경우 행동의 단절(중단)이 활성화된다[18]. 이처럼, 기술 사용자의 회피 행동은 양의 피드백 순환이라는 프로세스 관점에서 설명된다[1].

대응 이론 관점에서 개인은 자신이 직면한 (기술) 환경 위협을 평가하기 위해서 두 가지 인지적 평가 과정인 위협 평가(1차 평가)와 대응 평가(2차 평가)를 수행하며, 이 평가 과정을 통해 위협을 어떻게 피할 것인지 결정한다[1]. 여기서 개인이 사용할 수 있는 회피(대응) 방법은 문제 기반 대응(problem focused coping)과 감정 기반 대응(emotion focused coping)이다. 문제 기반 대응은 주어진 문제를 직접 해결하는 노력이다. 감정 기반 대응은 감정적 회피 노력이 해당한다.

TTAT 관점에서 기술 사용자가 IT 위협을 인지하였을 때, 사용자는 자신에게 주어진 위협을 피할 수 있는 가용한 안전장치가 준비되어 있다고 판단될 경우 능동적으로 안전장치를 활용하여 위협을 회피할 동기(문제 기반 대응)를 갖는다[1]. 반면, 가용한 안전장치가 없거나, 주어진 안전장치가 자신이 직면한 위협을 회피하는 데 유용하지 못하다고 판단되면, 감정 기반 대응을 활용하여 수동적으로 위협을 회피하려 할 수 있다[1].

TTAT에서 사용자의 위협 인식은 위협 발생 가능성에 대한 인지와 위협 발생으로 인한 부정적 결과의 인지된 심각성에 의해 결정된다[1]. 본 모형은 대응 이론과 다르게 정보보안 측면에서 위협을 회피할 방법을 평가할 수 있는 세 가지 요인을 제시했다[1]. 이는 대응 수단의 효과성(effectiveness of the measure), 대응 수단의 비용(costs of the measure), 대응 수단을 활용할 효능감(self-efficacy) 등이다[1]. 정리하면, TTAT는 IT위협에 대한 사용자의 위협 회피 행동의 결정요인과 행동 과정을 설명해준다[1].

3. 연구모형 및 가설

TTAT에 따르면, 개인의 동기에 영향을 미치는 요인은 보안에 대한 인지된 위협과 회피 가능성(avoidability)이다[12]. 회피 가능성은 보안 대책의 효

과성, 보안 대책의 비용, 자기 효능감 수준으로 구성된다[1][12]. Boysen et al.[20]은 이 세 가지 요인이 고른 중요도로 회피 동기를 결정한다고 언급했다. 회피 동기(avoidance motivation)란 “안전 대책을 활용하여 직면한 IT 위협에서 벗어나고자 하는 기술 사용자의 동기”를 말한다[4]. 따라서, 개인의 보안 행위 동기는 인지된 위협, 보안 대책의 효과성, 보안 대책의 비용, 자기 효능감 등에 의해 결정된다. Liang and Xue[1], Carpenter et al.[21] 등의 연구에 따르면, 위의 4가지 요인이 모두 위협 회피 동기에 유의한 영향을 미친다는 것을 실증적으로 규명했다.

TTAT의 초기 모형에서 인지된 위협에 영향을 미치는 요인으로 제시된 인지된 취약성과 인지된 심각성을 본 연구에 포함하지 않은 이유는 두 변수에 대한 관점이 통일되지 못하고 연구 결과의 차이가 크기 때문이다. 예를 들어, Boysen et al.[20]은 인지된 취약성을 인지된 위협의 선행변수가 아니라 인지된 심각성의 선행변수로 보았다. Carpenter et al.[21]은 인지된 취약성을 인지된 위협뿐만 아니라 인지된 심각성에 모두 영향을 미치는 선행요인으로 보았다. Vance et al.[22]의 연구에서는 인지된 심각성과 인지된 취약성이 위협에 어떠한 영향도 미치지 못하는 것으로 나타났다. Jasen and van Schaik[23]은 인지된 심각성이 예방적 온라인 행동에 유의한 영향을 미치는 반면, 인지된 취약성은 예방 행동에 유의한 영향을 미치지 못한다는 것을 규명했다. Gillam and Foster[5]는 두 요인이 모두 회피 동기에 아무런 영향을 미치지 못한다는 것을 규명했다. Gillam and Waite[24]의 연구에서도 두 요인이 회피 동기에 아무런 영향을 미치지 못하는 것으로 나타났다. 이처럼 두 잠재변수의 역할의 불일치한 결과로 인해 본 연구에서 배제했다.

보안을 위한 안전 대책들은 조직의 정보보안 정책에 기술되어 있다[12]. 따라서, IT 보안 행위의 궁극적 목적은 구성원들의 정보보안 정책 준수를 통해 보안 위협을 회피하는 것이다[12]. 이러한 관점에서 구성원들의 정보보안 위협 회피 행위는 구성원들의 정보보안 정책 준수 행위라고 볼 수 있다[12]. 정보보안 정책 준수란 “조직 구성원들이 조직의 정보기술과 정보 자원을 적절히 활용하기 위해서 정보보안 정책을 따르는 정도”를 말한다[12].

본 연구에서는 정보보안 정책 준수 동기를 보안 위협 회피 행위의 동기로 보고 해당 동기에 영향을 미치는 요인을 TTAT에서 제시한 4가지 요인과 Liang and Xue[1]가 TTAT를 제시할 때 포함한 사회적 영향력으로 보고 해당 요인들 간의 인과관계를 살펴보기 위해 아래와 같은 가설과 연구모형을 제시했다.

3.1 정책의 위협

Abraham H. Maslow의 욕구 단계설에 따르면, 개인의 자원과 자산에 대한 안전성은 인간의 기본 욕구이다[4]. 이 관점에서 IT 위협은 개인의 프라이버시와 재정적 손실을 유발할 수 있다[4]. 따라서, 기술 사용자들은 IT 위협에서 벗어나고 싶은 동기를 가지게 된다[4]. 위협의

Table 1. Demographic Information of Respondents

Criteria		Freq.	%	Criteria		Freq.	%
Gender	Male	100	69.9	Education	High School	1	0.7
	Female	41	28.7		2yrs College	11	7.7
	Missing	2	1.4		4yrs College	96	67.1
Age Group	18-24	2	1.4		Master Degree	26	18.2
	25-34	69	48.3		Ph.D	4	2.8
	35-44	59	41.3		ETC.	1	0.7
	45-54	13	9.1		Missing	4	2.8
Position	Technical	43	30.1	Employment type	Regular worker	118	82.5
	Managerial/Clerical	45	31.5		Temporary Employment	1	0.7
	Middle Manager	37	25.9		Worker by the hour	2	1.4
	Professional	15	10.5		Contract worker	20	14.0
	ETC	3	2.1		Missing	2	1.4
Years of employment (avg.)		5.9085 yrs		Main Workpalce	Office	139	97.2
Time spent on computers at work		approx. 8.8759 hour/day			Home	2	1.4
Subjective computer literacy level(1-7)		5.2624			ETC	1	0.7
					Missing	1	0.7

강도가 높아질수록 더 강한 회피 동기를 가지게 된다[4]. 조직의 정보보안 정책은 조직 구성원들이 조직자원을 안전하게 활용할 수 있는 방법뿐만 아니라 보안 사고 전후에 자신이 취해야 하는 행동의 지침을 제공한다.

회사의 정보보안 정책 수립은 대부분 조직의 경영진과 정보시스템 부서의 상위 관리자에 해당하는 사람들이 주로 담당한다[3]. 따라서, 일부 Bottom-up 방식의 정책 수립 절차도 존재할 수는 있으나 많은 경우 Top-down 방식으로 정책이 작성되는 것이 일반적이다[25]. 문제는 이와 같은 절차가 현장의 목소리를 제대로 반영하지 못할 수 있다는 점이다. 이와 같은 문제는 견고한 정보보안을 보장하는 것이 아니라 정책의 허점을 만들어 조직의 정보보안이 취약하게 만들 수 있다. 즉 조직에서 수립한 정보보안 정책을 구성원들이 이해하기 어렵고 장황하며 의미가 명확하게 전달되지 못한다면 구성원들은 보안사고 전후로 자신이 취해야 하는 보안행동을 결정하지 못하게 된다. 예를 들어, 조직이 수립한 BYOD 정책은 구성원들이 개인 모바일 장비로 어떻게 기업 정보에 접근하고 어떻게 자신의 업무를 수행하는지를 안내하는 지침서가 된다[6]. 따라서, 보안 정책은 구성원들의 관점에서 설득력 있고, 이해하기 쉬우며, 행동으로 옮기는 데 문제없이 명료하게 작성되어야 한다.

Liang and Xue[1]는 인지된 위협이 회피 동기에 유의한 영향(정의 영향)을 미치는 것으로 나타났다. 반면, Young et al.[12]의 연구에서는 인지된 위협이 회피 동기에 유의한 영향을 미치지 못하는 것으로 나타났다. 마찬가지로, Liu et al.[9]의 연구에서 인지된 위협이 보안 정책 준수 행위에 유의한 영향을 미치지 못하는 것으로 나타났다.

H1: 정책의 위협은 정책 준수 동기에 음(-)의 영향을 미칠 것이다.

3.2 정책의 효과성

안전대책의 효과성(safeguard effectiveness)이란 "악의적 IT 위협을 피하기 위해서 활용할 수 있는 안전대책의 개인적 평가"를 말한다[13].

보안 장치(대안)의 유용성(usesulness)은 인지된 효과성으로 평가된다[2]. Ikhalia et al.[14]은 보안의 유용성은 유용해야 하고, 도움이 돼야 하고, 이해하기 쉬워야 하고, 정확해야 한다고 주장했다.

Goel and Chengalur-Smith[16]는 간결성(brevity), 명확성(clarity), 포괄성(breadth, thoroughness) 등을 정보보안 정책 효과성의 기준으로 제시했다. 간결성은 보안 정책에 사용된 단어의 중독, 왜곡, 오해, 모호함, 중언부언, 동어반복 등이 없이 작성된 정도를 말한다[16]. 명확성은 수립된 정책의 내용이 얼마나 읽기 쉽고, 이해하기 쉬운지를 반영한다[16]. 지나치게 많은 전문 용어를 사용하거나, 이해하기 힘든 기술적 용어를 사용하는 경우, 장황하게 쓰여있는 경우 명확성이 낮다고 볼 수 있다. 포괄성은 정보 보안과 관련된 요소를 얼마나 많이 반영하고 있는지를 나타낸다[16]. 즉 정책의 내용이 얼마나 구체적인지를 나타내는 것이 포괄성이다.

보안 정책을 수립하는 데 있어서 이 3가지 요인이 중요함에도 불구하고 다음과 같은 문제점이 있다. 첫째, 세 요인 간의 상관관계가 높다는 것이다. 세 요인이 통계적으로 구분되기보다는 하나 혹은 두 개의 개념으로 나뉘는 경우 많다. 둘째, 세 요인뿐만 아니라 더 많은 요소가 반영되어야 한다. 예를 들어, 기술의 발전은 지속적이다. 모바일 기술이 대중화되고, 새로운 기술이 대중화될 경우 기업은 새로운 기술환경을 조직에 반영한다. 따라서, 새로운 기술환경에 맞추어 보안 정책은 지속적으로 갱신되어야 한다. 따라서, '최신성'과 같은 요소들이 정책의 효과에 반영되어야 한다. 그럼에도 불구하고 중요한 것은 정보 보안 정책의 효과성에 대한 평가이다.

그동안 보안 정책이 존재하는지 그리고 구성원들이 정보보안 정책을 인지하고 있는지만 관심을 두어왔다. 이제는 존재의 여부에서 한 발 더 나아가 정책을 명확히 이해하고 있는지를 평가해야 한다. 우리 회사에 정보보안 정책이 '있다'가 중요한 것이 아니라 구성원들이 정보 보안 정책을 '잘 알고 있다'가 더 중요하기 때문이다. 정보보안 정책이 효과적으로 작성되어 구성원들이 잘 이해하고 있다면 구성원들의 보안 정책 준수 가능성도 커질 것이다. Liang and Xue[1], Young et al.[12]의 연구에서는 보안 위협에 대한 안전장치의 효과성이 회피 동기에 유의한 영향을 미치는 것으로 나타났다. Chen and Li[2]의 연구에서도 모바일 기기 보안에 대한 인지된 효과성이 확신 동기에 유의한 영향을 미치는 것으로 나타났다. Cho and Ip[6]의 연구에서는 BYOD 보안 정책의 인지된 효과성이 BYOD 수용에 유의한 영향을 미치는 것으로 나타났다. 반면, Liu et al.[9]의 연구에서는 인지된 효과성이 보안 정책 준수 행위에 유의한 영향을 미치지 못하는 것으로 나타났다. 이와 같은 상반된 결과를 검증하기 위해서 다음의 가설을 제시할 수 있다.

H2: 정책의 효과성은 정책 준수 동기에 정(+)의 영향을 미칠 것이다.

Table 2. Exploratory Factor Analysis

Construct (Cronbach's α)	Measurement Variales	Factor						Communaity	
		1	2	3	4	5	6	Initial	Extraction
Policy Effectiveness (α=0.931)	PolicyEffect1	**0.807**	0.134	0.112	0.036	0.063	0.105	0.782	0.681
	PolicyEffect2	**0.777**	0.172	−0.046	0.004	−0.033	0.149	0.783	0.649
	PolicyEffect3	**0.811**	−0.151	−0.024	0.032	0.004	−0.029	0.781	0.720
	PolicyEffect4	**0.852**	0.048	−0.083	−0.056	−0.018	−0.009	0.811	0.742
	PolicyEffect5	**0.790**	0.030	−0.136	−0.075	−0.055	0.011	0.783	0.664
	PolicyEffect6	**0.697**	−0.087	−0.015	0.060	0.045	0.038	0.673	0.568
	PolicyEffect7	**0.664**	−0.297	−0.058	0.072	0.107	−0.190	0.751	0.614
	PolicyEffect8	**0.721**	−0.003	0.068	−0.044	0.172	0.065	0.737	0.649
Policy Threat (α=0.850)	PolicyEffect9	0.191	−0.037	0.135	−0.024	**0.585**	0.078	0.576	0.461
	PolicyEffect10	0.097	−0.162	−0.014	0.044	**0.795**	−0.054	0.749	0.771
	PolicyEffect11	−0.162	0.056	−0.047	0.051	**0.960**	0.004	0.731	0.849
	PolicyEffect12	0.059	0.096	−0.143	−0.043	**0.669**	−0.071	0.609	0.535
Compliance Cost (α=0.929)	PerBenefit1	−0.038	0.061	−0.119	**0.642**	0.015	0.048	0.577	0.440
	PerBenefit2	0.033	0.035	0.018	**0.891**	−0.038	0.022	0.799	0.793
	PerBenefit3	−0.055	−0.050	−0.024	**0.905**	−0.016	0.039	0.812	0.799
	PerBenefit4	0.078	−0.001	0.056	**0.934**	−0.005	−0.047	0.894	0.890
	PerBenefit5	0.001	0.013	0.071	**0.879**	0.052	−0.057	0.852	0.808
Compliance Motivation (α=0.947)	PerIntent1	0.014	**−0.835**	0.034	−0.041	0.006	0.132	0.872	0.843
	PerIntent2	−0.022	**−0.888**	0.032	−0.022	0.007	0.097	0.886	0.883
	PerIntent3	0.023	**−0.886**	0.051	−0.035	−0.024	0.061	0.850	0.857
	PerIntent4	0.021	**−0.888**	−0.008	−0.016	−0.065	0.004	0.814	0.794
	PerIntent6	−0.074	**−0.730**	−0.106	−0.020	0.077	0.070	0.675	0.605
Social Influence (α=0.950)	SubNorm1	−0.003	−0.106	0.148	0.045	0.007	**0.799**	0.861	0.716
	SubNorm2	−0.083	−0.044	0.004	0.030	0.037	**0.928**	0.884	0.858
	SubNorm3	0.127	−0.080	−0.108	−0.017	0.021	**0.791**	0.885	0.807
	SubNorm4	0.068	−0.017	−0.103	−0.072	−0.056	**0.884**	0.914	0.891
	SubNorm5	0.107	−0.105	−0.063	−0.009	−0.072	**0.806**	0.858	0.823
Self−Efficacy (α=0.941)	PBC3	−0.029	0.014	**−0.685**	−0.060	0.067	0.171	0.662	0.530
	PBC4	0.008	0.033	**−0.918**	0.025	0.008	−0.044	0.845	0.848
	PBC5	−0.062	0.014	**−0.920**	−0.009	0.060	0.022	0.861	0.846
	PBC6	−0.022	−0.010	**−0.915**	0.027	0.017	0.021	0.846	0.840
	PBC7	0.087	−0.035	**−0.825**	0.043	−0.059	−0.081	0.810	0.698
	PBC8	0.131	−0.035	**−0.804**	0.016	−0.006	−0.022	0.813	0.711
Eigenvalue		8.724	5.898	3.822	3.354	2.408	1.468	Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalization.	
% of Variance		26.437	17.874	11.581	10.165	7.297	4.448		
Cumulative %		26.437	44.311	55.892	66.057	73.353	77.802		
KMO and Bartlett's Test									
Kaiser−Meyer−Olkin Measure of Sampling Adequacy						0.845			
Bartlett's Test of Sphericity			Approximate Chi−Square			4645.190			
			degree of freedom			528			
			Significance			0.000			

3.3 정책 준수 비용

정책 준수 비용(costs of compliance)이란 "구성원들이 정보보안 정책 준수로 인해 발생할 것으로 예상되는 전반적인 부정적 결과물"을 말한다[7]. 예를 들어, 보안 정책 준수에 소요되는 시간과 노력이 해당한다[7].

조직 구성원들의 정보보안 정책 준수는 기업의 보안 강화를 위한 첫걸음이지만 보안 정책의 준수가 쉬운 것은 아니다. 합리적 선택 이론(Rational Choice Theory)에 따르

면, 모든 사람은 어떠한 선택을 하는 데 있어서 해당 선택으로 얻을 수 있는 이익과 비용의 두 가지 측면을 모두 평가한다. 즉 인간은 의사결정을 하는 데 있어서 긍정 혹은 부정 중 하나의 측면만 보는 것이라 아니라 두 가지 측면을 모두 검토한 후 자신의 행동을 결정한다.

정보보안 분야에서도 정책의 준수와 연관된 비용과 이익에 대한 인지적 평가를 통해 정보보안 정책 준수 행위를 예측할 수 있다[7]. 정보보안 측면에서 개인의 정책 준수가 조직의 정보보안을 강화한다는 장점이 있는 반면, 보안 정책을 준수하는 데 따르는 부정적 비용도 발생한다[8]. 선행연구에 따르면, 정보보안 정책의 준수와 개인의 업무 생산성은 일정 부분 상충하기 때문에 정책 준수가 조직 내에서 원활하게 이루어지지 않는다[16][25]. 또한, 보안 정책을 준수하는 과정 자체가 불편함을 유발하기 때문에 구성원들이 정책 준수에 소홀할 수 있다[26]. D'Arcy and Lowry[7]는 보안 정책 준수로 인해 발생하는 업무 장애가 보안 정책 준수 태도에 부정적 영향을 미친다는 것을 규명했다. 일부 구성원들은 보안 정책을 자신들의 행동을 감시 및 통제하기 위한 도구라고 인식하기도 한다[3][16]. 이처럼, 조직의 정보보안 정책을 준수하는 데 유·무형의 비용이 발생한다면 구성원들은 정책 준수에 소극적일 수 있다. Young et al.[12]의 연구에 따르면, 안전대책 비용이 회피 동기에 부(−)의 영향을 미치는 것으로 나타났다. Chen and Li[2]의 연구에서도 모바일 기기의 안전성에 대한 인지된 비용이 확신 동기에 부정적 영향을 미치는 것으로 나타났다. Liu et al.[9]의 연구에는 인지된 비용이 보안 정책 준수 행위에 음(−)의 영향을 미치는 것으로 나타났다. 반면, Boysen et al.[20]의 연구에서는 안전 대책 비용이 회피 동기에 유의한 영향을 미치지 못하는 것으로 나타났다. Cho and Ip[6]의 연구에서도 BYOD 보안 정책의 준수 비용이 BYOD 수용에 유의한 영향을 미치지 못하는 것으로 나타났다. 이와 같은 불일치한 결과의 원인 중 하나는 연구 정황의 차이에 있다. 본 연구에서는 보안 정책의 특성을 중심으로 연구를 수행하기 때문에 선행연구와 다른 결과가 도출될 수 있다. 따라서, 다음의 가설을 제시할 수 있다.

가설 H3: 정책 준수 비용은 정책 준수 동기에 음(−)의 영향을 미칠 것이다.

3.4 정책 준수 효능감

자기 효능감(self−efficacy)이란 "대응 행동을 수행할 수 있는 자신의 능력에 대한 개인적 판단"을 말한다[2][6]. 보안 관점에서, 정책 준수 효능감(Compliance Self−efficacy)이란 "정보보안 정책 준수를 위한 요구사항을 충족하기 위해 필요한 기술, 지식, 역량에 대한 개인적 평가"를 말한다[7]. 즉 효능감은 보안 대책을 활용할 수 있는 개인의 신념이다[2].

정보시스템 분야에서 자기 효능감은 사용자의 컴퓨터 보안 행위, 정보 보안 정책 준수 의도, 정보보안 도구 활용 의도 등에 영향을 미치는 강력한 선행요인으로 인식되어 왔다[2]. 하지만, 자기 효능감의 역할이 항상 일치하는 것은 아니다. D'Arcy and Lowry[7]는 정책 준수 효능감이 개인의 정책 준수 행위에 긍정적 영향을 미친다는 것을 규명했다. Young et al.[12]의 실증연구에서도 자기 효능감이 회피 동기에 유의한 영향(+)을 미치는 것으로 나타났다. Johnston et al.[27]은 인지된 자기 효능감과 인지된 대응 효능감이 보안 정책 준수 의도에 유의한 영향을 미친다는 것을 규명했다. Chen and Li[2]의 연구에서는 모바일 기기 안전에 대한 자기 효능감이 확신 동기에 유의한 영향을 미치는 것으로 나타났다. Cho and Ip[6]은 BYOD 보안 정책 준수 자기 효능감이 BYOD 수용에 유의한 영향을 미친다는 것을 규명했다. 반면, Carpenter et al.[21]의 연구에서 자기 효능감은 회피 동기에 유의한 영향을 미치지 못하는 것으로 나타났다. 따라서, 다음의 가설을 제시할 수 있다.

가설 H4: 정책 준수 자신감은 정책 준수 동기에 정(+)의 영향을 미칠 것이다.

3.5 사회적 영향력

사회적 영향력(social influence)은 기술 사용자의 위협 회피 행동에 영향을 미치는 일반적 요인이다[1]. 사회적 영향력이란 "자신에게 중요한 주변 사람들이 내가 그 기술을 반드시 사용해야 한다고 생각하는 정도"를 말한다[28]. 개인의 행동은 자신이 속한 집단, 조직, 혹은 사회와 밀접하게 연관된다[1]. 마찬가지로, 기술 사용자의 회피 행동도 자신이 속한 사회적 환경의 영향에서 벗어날 수 없다[1].

사회적 영향력은 주관적 규범과 마찬가지로 개인의 행동 의도에 직접적인 영향을 미치는 결정요인이다[28]. Venkatesh et al.[28]은 사회적 영향력이 기술 사용자의 행동 의도에 유의한 영향을 미친다는 것을 규명했다. Cho and Ip[6]의 연구에서, 사회적 영향력이 구성원들의 BYOD 수용에 유의한 영향을 미치는 것으로 나타났다. 하지만, D'Arcy and Lowry[7]의 연구에서 주관적 규범이 정

보보안 준수 행위에 유의한 영향을 미치지 못하는 것으로 나타났다. 따라서, 다음의 가설을 제시할 수 있다.

가설 H5: 사회적 영향력은 정책 준수 동기에 정(+)의 영향을 미칠 것이다.

지금까지 제시한 5가지 가설을 기반으로 연구모형을 제시하면 아래의 [그림 1]과 같다.

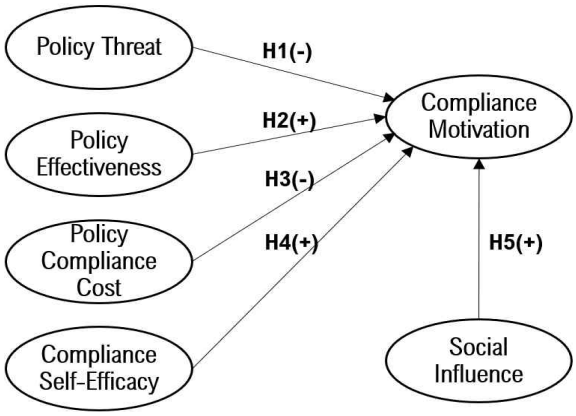

Fig. 1. Research Model

4. 분석

4.1 자료 수집

본 연구에서는 모형 분석에 필요한 실증 자료를 수집하기 위해서 설문기법을 사용했다. 설문 기법에 사용된 모든 항목은 선행연구에서 신뢰성이 확보된 지표들을 참고한 후에 본 연구의 정황에 맞게 수정했다.

정책 위협은 Goel and Chengalur-Smith[16]에서 4개의 항목을 차용했다. 정책 효과성은 Goel and Chengalur-Smith[16]에서 8개의 항목을 차용했다. 정책 준수 비용은 Cho and Ip[6], Liang and Xue[1], Young et al.[12]에서 5개의 항목을 차용했다. 정책 준수 효능감은 Cho and Ip[6], Liang and Xue[1], Young et al.[12]의 연구에서 6개의 항목을 차용했다. 사회적 영향력은 Chen and Liang[11], Venkatesh et al.[28]의 연구에서 5개의 항목을 차용했다. 정책 준수 동기 Chen and Liang[11], Liang and Xue[1], Young et al.[12]의 연구에서 5개의 항목을 차용했다.

설문에 대한 응답은 Likert-type 7점 척도법을 사용했다. 1점은 "전혀 동의하지 않음"을 의미하며, "7점은 전적으로 동의함"을 의미한다.

본 연구에서 각각의 지표의 신뢰성(내적 일관성, Cronbach's α)을 평가한 결과, 정책 위협은 0.850, 정책 효과성은 0.931, 정책 준수 비용은 0.929, 정책 준수 효능감은 0.941, 사회적 영향력은 0.950 등으로 모두 기준 값인 0.7 이상으로 나타났다[30].

총 200개의 설문을 배포했고, 175개의 응답을 회수했다. 이 중에서 불성실한 응답(예. lining, 5개 이상의 항목에 같은 번호로 응답, 중간번호로 5개 이상 항목에 응답 등)을 제외하고 143개의 응답을 최종 분석에 사용했다.

4.2 탐색적 요인 분석

본 연구에서는 수집된 데이터 속에서 잠재적 요인 구조를 식별하기 위해서 탐색적 요인 분석(EFA, Exploratory Factor Analysis)을 수행했다.

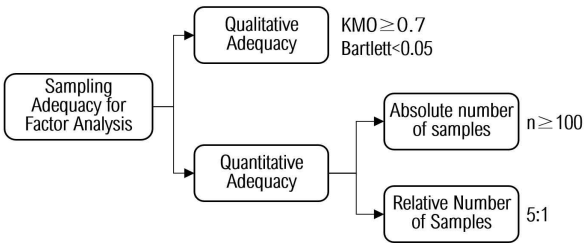

Fig. 2. Sampling Adequacy for Factor Analysis

Table 3. Correlation Analysis

	Mean	Std. Deviation	Policy Effectiveness	Policy Threat	Compliance Cost	Social Influence	Self Efficacy	Avoid Motivation
Policy Effectiveness	4.0822	0.97877	1	.429**	0.017	.310**	.286**	.193*
Policy Threat	3.9231	0.98681	.429**	1	0.107	−0.007	.201*	0.111
Compliance Cost	3.6755	1.18579	0.017	0.107	1	−0.151	0.037	−.198*
Social Influence	5.1147	1.09660	.310**	−0.007	−0.151	1	0.139	.570**
Self-Efficacy	3.6958	1.19095	.286**	.201*	0.037	0.139	1	0.026
Avoid Motivation	5.6308	0.98189	.193*	0.111	−.198*	.570**	0.026	1

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

EFA 전에 수집된 데이터가 EFA에 적합한지 여부를 판단했다(그림 2). 양적 판단으로 연구에 사용된 관측변수의 수 대비 수집된 데이터의 수가 적정한가를 판단했다[30]. 일반적 기준에 따르면, 상대적 표본 기준으로 5:1을 사용한다[30]. 본 연구에서는 33개의 측정항목이 사용되었기 때문에 165개의 표본이 필요하다. 하지만, 143개 표본이 사용되었기 때문에 기준보다 다소 표본이 부족하다. 추가적으로 절대적 기준을 살펴보았다. 선행연구에 따르면, 100개가 EFA를 위한 최소 표본이다[31]. 본 연구에서는 이 기준을 충족했다. 다음으로 질적 특성을 살펴보았다. 질적 특성은 수집된 데이터로 EFA에 적합한 행렬식을 도출할 수 있는지를 점검하는 절차로 KMO(Kaiser-Meyer-Olkin)와 Bartlett 검정을 보고 판단한다[32]. KMO는 최소 0.7 이상이 되어야 한다[32]. Bartlett 검정은 통계적으로 유의($p<0.05$)해야 한다[32]. 본 연구에서 KMO는 0.845, Bartlett의 0.000으로 EFA를 수행하기에 적합한 것으로 나타났다.

요인 회전은 Oblimin with Kaiser Normalization, 요인 추출은 PAF(Principal Axis Factoring)를 사용했고, 최소 요인 적재값은 0.5 이상이면서 교차 요인(0.4 이상의 적재값을 갖는 요인)이 없는 요인을 기준으로 총 6개의 요인을 추출했다. 요인의 총 분산은 77.802로 최소 기준인 60%를 상회하는 것으로 나타났다[31].

본 연구에서는 CMV(Common Method Variance)의 영향이 결과의 왜곡을 유발할 정도로 심각한지 여부를 살펴보았다. CMV를 검정하기 위한 사후 검정 기법 중에 Harman[32]이 제시한 단일 요일 검정법(single factor test)을 수행했다. 본 분석을 위해서 모든 관측변수가 포함된 EFA를 수행하고, 첫 번째 요인(요인 회전 전)의 분산의 양을 보고 CMV의 영향력을 평가한다[33]. 만약, 첫 번째 요인의 분산이 50%가 넘을 경우 CMV의 심각하다고 판단한다. 본 연구에서는 EFA 수행 후 도출된 첫 번째 요인의 분산이 26.437%로 매우 낮은 수준을 나타냈기 때문에 CMV로 인한 결과 왜곡이 발생하지 않을 것이라고 예상할 수 있다.

다음으로 잠재변수 간에 상관관계를 분석했다. 표 3을 보면 본 연구에서 제시한 변수 간에 일정 수준의 상관관계가 존재하는 것으로 나타났다. 그뿐만 아니라 다중공선성을 의심할 만큼 지나치게 높은 상관관계 계수는 존재하지 않는 것으로 나타났다.

4.3 가설검정

적정 표본 수를 결정하기 위해서 G*Power v3.1.9.7을 사용하여 최적 표본 수를 계산했다. 계산 결과 최소 134개의 표본이 필요한 것으로 나타났다(α error probability=0.05, two-tailed, Critical t=1.9780988). 본 연구에서는 143개의 표본을 사용하였기에 회귀분석을 위한 최소 표본 기준을 충족하고 있다.

다음으로 독립변수 간의 다중공선성을 살펴보기 위해서 VIF(Variane Inflation Factors)를 살펴보았다. 본 값은 5 이하가 되어야 한다[34]. 본 연구에서는 최대 VIF 값이 1.281로 독립변수 간에 다중공선성이 존재하지 않는다고 볼 수 있다.

다음으로 오차항 간의 자기 상관성(auto-correlation)을 살펴보기 위해서 durbin-watson d값을 살펴보았다. durbin-watson d값은 2일 경우 자기상관의 문제가 없다고 판단한다. 본 연구에서 d값은 2에 근사한 2.161로 나타났기 때문에 오차항 간의 자기상관의 문제는 심각하지 않다고 볼 수 있다.

Cohen[35]에 따르면, R^2값이 0.02는 낮은 수준, 0.13은 중간 수준, 0.26 이상은 높은 수준의 효과 크기라고 정의했다. 본 연구에서 종속변수인 정책 준수 동기의 R^2는 0.360으로 나타났고, 독립변수의 수를 반영한 Adjusted R^2도 0.337로 높은 수준으로 나타났다.

가설검정을 위해 회귀분석을 수행했다. 분석 결과는 표 4와 그림 3과 같다.

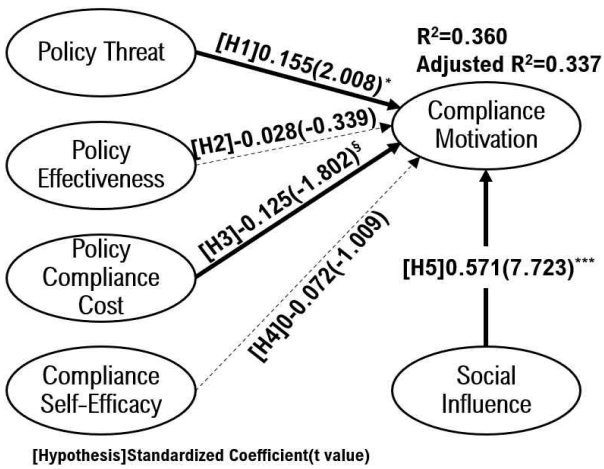

Fig. 3. Results of Regression Path Analysis

회귀분석 결과, 보안 정책의 위협은 준수 동기에 유의한 영향을 미치는 것으로 나타났다($\beta=0.155$, $t=2.008$, $p<0.05$). 정책의 효과성은 준수 동기에 유의한 영향을 미치지 못하는 것으로 나타났다($\beta=-0.028$, $t=-0.339$). 정책 준수 비용은 준수 동기에 유의한 영향을 미치는 것으

Table 4. Results of Regression Analysis

	Unstandardized Coefficients		Standardized Coefficients	t value	Significance	Collinearity Statistics		Results
	B	Standard Error	Beta			Tolerance	VIF	
(Constant)	3.127	0.492	-	6.355	0.000	-	-	-
Policy Effectiveness	−0.028	0.082	−0.028	−0.339	0.735	0.692	1.445	Rejected
Policy Threat	0.155	0.077	0.155	2.008*	0.047	0.781	1.281	Rejected
Compliance Cost	−0.104	0.058	−0.125	−1.802§	0.074	0.964	1.037	Accepted
Social Influence	0.511	0.066	0.571	7.723***	0.000	0.855	1.170	Accepted
Self-Efficacy	−0.060	0.059	−0.072	−1.009	0.315	0.905	1.105	Rejected

Dependent Variable: Avoidance Motivation
*** p<0.001, **p<0.01, *p<0.05, §p<0.1

로 나타났다(β=−0.125, t=−1.802, p<0.1). 정책 준수 효능감은 정책 준수 동기에 영향을 미치지 못하는 것으로 나타났다(β=−0.072, t=−1.009). 마지막으로, 사회적 영향력은 정책 준수 동기에 유의한 영향을 미치는 것으로 나타났다(β=0.571, t=7.723, p<0.001).

5. 결론 및 함의

5.1 연구의 의의

본 연구는 TTAT를 기반으로 정보보안 정책의 관점에서 보안 정책의 특성(정책의 취약성, 정책의 효과성, 정책 준수 비용, 정책 준수 효능감, 사회적 영향력)이 조직의 정보보안 정책 준수 동기에 미치는 영향을 살펴보기 위해 수행되었다.

분석 결과, 첫째, 보안 정책의 위협은 정책 준수 동기에 유의한 영향을 미치는 것으로 나타났다. 단, 본 연구에서 가설로 제시한 방향과 반대 방향으로 나타났다. 정책의 위협이 준수 행동에 부(−)의 영향을 미치는 것이 아니라 정(+)의 영향을 미치는 것으로 나타났다. 위험보상이론(Risk Compensation Theory)에 따르면 새로운 안전장치가 마련되었거나 기존의 위험이 사라졌다고 생각할 때 개인은 더 위험한 행동을 취할 가능성이 크다. 예를 들어, 자동차의 ABS(Anti-lock braking system)가 개발되었을 때 과속 사고는 오히려 증가했다. 기존의 위험이 안전함으로 바뀌면 또 다른 위험한 행동을 취하여 항상성(homeostasis)을 유지한다. 반대로 위험이 존재할 때 안전을 추구하여 항상성의 균형을 유지할 수 있다. 즉 정책이 불안전하고 취약할 때 정책 준수 동기로 항상성을 유지할 수 있다. 이는 조직이 취약한 정책을 취해야 한다는 것을 의미하는 것은 아니다. 오히려, 견고한 정책을 수립하되, 구성원들이 취할 수 있는 또 다른 위험 행동을 사전에 예상하고 이를 예방하는 조처를 해야 한다는 것을 의미한다.

둘째, 정책의 효과성은 준수 동기에 유의한 영향을 미치지 못하는 것으로 나타났다. 본 연구에서 살펴본 정책의 효과성은 형식이다. 정책의 효과성은 형식(form)과 내용(content)의 두 가지 측면에서 볼 수 있다. 하지만 내용의 경우 조직마다 다르고 산업의 유형에 따라서도 달라지기 때문에 정책의 형식에 대한 평가 기준은 마련되어 있는 반면에 정책의 내용을 평가할 수 있는 지표가 개발되어 있지는 않다. 따라서, 정책의 형식뿐만 아니라 내용의 효과성 혹은 정책의 내용 효과성이 준수 동기에 미치는 영향을 검증한다면 다른 결과를 기대할 수도 있다.

셋째, 정책 준수 비용은 정책 준수 동기에 유의한 영향을 미치는 것으로 나타났다. 본 결과는 조직의 정책 준수가 개인의 생산성 하락 혹은 업무 수행의 장벽이 될 경우 정책 준수 동기를 유발하지 못할 수 있다는 점을 의미한다. 따라서, 현실성 있는 정책 마련을 위해 구성원들의 업무 생산성과의 상충관계를 고려하여 기존 정책을 현장에 맞게 수정하는 것이 구성원들의 정책 준수 동기를 높이는 방법이다.

넷째, 정책 준수 효능감은 회피 동기에 유의한 영향을 미치지 못하는 것으로 나타났다. 이와 같은 결과에 대한 원인을 성별에 따른 차이에서 찾을 수 있다. 선행 연구에 따르면, 자기 효능감과 회피 동기 간에 성별의 차이가 있는 것으로 나타났다. 남성의 경유 자기 효능감과 회피 동기 간에 유의한 관계가 없었으나 여성의 경우 유의한 관계가 존재했다. 또한, 준수 효능감과 행동 간의 괴리가 존재하기 때문에 나타난 결과라고 볼 수 있다. 조직의 정책을 충분히 이해하고 있고 행동으로 옮길 수 있음에도 항상 보안 행동을 취하는 것은 아니다. 따라서, 경영진은 이

러한 간극을 줄이기 위해 구성원들에게 보안 행동을 솔선수범하고, 정책 준수를 위한 분위기를 조성해야 한다.

마지막으로, 사회적 영향력은 준수 동기에 유의한 영향을 미치는 것으로 나타났다. 자신의 주변 사람들이 보안 정책에 대해 중요하게 생각하고 있을 때 보안 행동에 대한 동기가 유발되는 것으로 해석할 수 있다. 전언하였듯이, 이를 현장에서 적용하기 위해서 경영진들은 보안 분위기를 조성해야 한다.

5.2 이론적 함의

본 연구는 보안 정책의 특성 관점에서 TTAT를 활용했다는 점에서 TTAT의 연구 정황을 확장했다는 의의가 있다. 지금까지 TTAT는 특정한 공격, 기기의 활용, 앱의 활용에 대해서만 적용되어 왔을 뿐, 조직의 보안 행동의 기본이 되는 보안 정책 준수에 대한 연구는 부재했다. 본 연구는 보안 정책의 특성을 TTAT의 각 요인에 적용하여 정책 준수 동기를 살펴보았다는 점에서 의의가 있다.

5.3 실무적 함의

본 연구는 현실적인 보안 정책을 개발할 때 고려해야 할 요소를 제시했다는 점에서 의의가 있다. 경영진이 보안 정책의 개발에 있어서 형식과 내용을 모두 고려해야 한다. 정책의 입안자가 아니라 준수자의 입장에서 이해하기 쉽고, 현실적이며, 업무 수행에 장해가 되지 않도록 정책을 수립해야 한다. 또한, 불가피하게 업무 수행 절차에 일부 불편함이 발생하더라도 업무 생산성과 상충되지 않고, 장기적 관점에서 조직에 이익이 된다는 점을 이해시킬 필요가 있다. 그뿐만 아니라, 전체 구성원들의 정책 준수 동기를 유발하기 위해서 경영진의 솔선수범과 보안 분위기를 조성하는 노력도 수반되어야 한다.

5.4 연구의 한계점과 향후 연구방향

응답자가 조직에서 혹은 자신에게 발생한 IT 위협을 인지하였는지 혹은 경험하였는지 여부를 사전에 물어보지 않았다. 본 연구에서 모든 조직은 예외 없이 보안 사고에 직면하게 되고 이에 따라 응답자도 보안 사고를 직·간접적으로 경험했다고 가정하고 연구를 수행했으나 직접적으로 보안 사고를 경험한 사람과 간접적으로 경험한 사람 간에 차이가 존재할 수 있다. 따라서, 향후 연구에서 사전에 보안 사고의 직접 경험자를 대상으로 조사하거나 직접 경험자와 간접경험자를 비교해서 연구한다면 더 의미 있는 연구 결과를 얻을 수 있을 것으로 판단된다.

스트레스에 대한 인지적 평가는 두 단계로 이루어진다. 1차 평가에서는 직면한 스트레스가 자신에게 기회 혹은 위협이 되는지를 평가한다. 2차 평가에서는 자신이 직면한 스트레스를 스스로 통제할 수 있는지를 평가한다. 이 과정이 끝나면 문제 기반 대응을 활용할지 감정 기반 대응을 활용할지를 결정한다. 즉, 1차 평가에서 스트레스는 기회와 위협으로 나뉜다. 본 연구는 스트레스를 위협으로 가정했다. 하지만, 스트레스가 기회일 수도 있다. 스트레스가 기회라고 인식한 경우 대응 과정은 위협과 다를 수 있다. 본 연구에서는 기회의 관점을 고려하지 않았다는 점에서 한계라고 할 수 있다. 또한, 2차 평가에서 통제력(예. 자기 효능감)에 따라 스트레스 수준은 달라질 수 있다. 따라서, 스트레스 연구에서 자기 효능감을 선행변수로 사용할 수 있지만, 조절변수로도 사용할 수 있다. 향후 연구에서 스트레스에 대한 개인의 통제 수준에 따른 차이를 탐색하는 것도 의의가 있을 것으로 판단된다.

TTAT의 실증 모형은 문제 기반 대응을 결과변수로 본다. 대응이론에 따르면, 스트레스에 대한 대응 기법은 문제 기반 대응과 감정 기반 대응이 있다. 따라서, 문제 기반 대응뿐만 아니라 감정 기반 대응도 함께 본다면 연구의 관점을 더 확장할 수 있을 것으로 기대할 수 있다. 그뿐만 아니라, 기술 사용자가 가용한 기술의 수준 혹은 유형(예. 사회적 지원)에 따라 위협 회피 성향은 달라질 수 있다. 따라서, 향후 연구에서 사회적 지원을 또 다른 대응 전략으로 보고 모형에 추가한다면 더 확장된 모형을 도출할 수 있을 것으로 예상된다.

TTAT는 자발적 기술 사용 상황을 가정한다. 하지만, 본 모형의 확장을 위해서 의무적 사용 상황에서 적용할 수 있는 경쟁모형을 개발하는 것도 의미가 있을 것이다. 향후 연구에서는 의무적 기술 사용 상황과 자발적 기술 사용 상황을 비교한다면 이러한 한계점을 보완할 수 있을 것으로 기대할 수 있다.

본 연구에서 실증분석을 위해 사용한 표본 수는 143개이다. 실증분석을 위해서 미리 정해진 '적정 수준'의 표본 수가 있는 것은 아니지만, 개인 차원의 연구에서 충분한 표본 수라고 보기는 어렵다. 따라서, 더 많은 표본을 수집하여 분석할 경우 결과에 차이가 발생할 수 있다.

마지막으로, 근무지에 따라 응답자를 구분하지 않은 한계점도 있다. 재택근무자, 사무실 근로자, 파트너사 근로자(파견 근로자), 혹은 하이브리드(재택과 사무실 근로 혼합) 근로 형태에 따라서 기술 위협 회피 행동은 달라질 수 있다. 응답자의 근무지를 구분하여 차이를 분석한다면 더 의미 있는 결과를 도출할 수 있을 것으로 사료된다.

REFERENCES

[1] H. Liang & Y. Xue (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, 33(1), 71-90.
DOI: 10.2307/20650279

[2] H. Chen & W. Li (2017). Mobile Device Users' Privacy Security Assurance Behavior: A Technology Threat Avoidance Perspective. *Information & Computer Security*, 25(3), 330-344.
DOI: 10.1108/ICS-04-2016-0027

[3] W. A. Cram, J. F. Proudfoot & J. D'Arcy (2017). Organizational Information Security Policies: A Review and Research Framework. *European Journal of Information Systems*, 26, 605-641.
DOI: 10.1057/s41303-017-0059-9

[4] H. Liang & Y. Xue (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.
DOI: 10.17705/1jais.00232

[5] A. R. Gillam & W. T. Foster (2020). Factors Affecting Risky Cybersecurity Behaviors by U.S. Workers: An Exploratory Study. *Computers in Human Behavior*, 108, 106319.
DOI: 10.1016/j.chb.2020.106319

[6] V. Cho & W. H. Ip (2018). A Study of BYOD Adoption from the Lens of Threat and Coping Appraisal of Its Security Policy. *Enterprise Information Systems*, 12(6), 659-673.
DOI: 10.1080/17517575.2017.1404132

[7] J. D'Arcy & P. B. Lowry (2019). Cognitive-affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study. *Information Systems Journal*, 29, 43-69.
DOI: 10.1111/isj.12173

[8] M. S. 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

[9] C. Liu, N. Wang & H. Liang (2020). Motivating Information Security Policy Compliance: The Critical Role of Supervisor-Surbordinate Guanxi and Organizational Commitment. *International Journal of Information Management*, 54, 102152.
DOI: 10.1016/j.ijinfomgt.2020.102152

[10] J. D'Arcy, A. Hovav & D. Galletta (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misue: A Deterrence Approach. *Information Systems Research*, 20(1), 79-98.
DOI: 10.1287/isre.1070.0160

[11] D. Q. Chen & H. Liang (2019). Wishful Thnking and IT Threat Avoidance: An Extension to the Technology Threat Avoidance Theory. *IEEE Transactions on Engineering Management*, 66(4), 552-567.
DOI: 10.1109/TEM.2018.2835461

[12] D. Young, D. Carpenter & A. McLeod (2016). Malware Avoidance Motivations and Behaviors: A Technology Threat Avoidance Replication. *AIS Transactions on Replication Research*, 2, 1-17.
DOI: 10.17705/1atrr.00015

[13] N. A. G. Arachchilage & S. Love (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. *Computers in Human Behavior*, 38, 304-312.
DOI: 10.1016/j.chb.2014.05.046

[14] E. Ikhalia, A. Serrano, D. Bell & P. Louvieris (2019). Online Social Netwokr Security Awareness: Mass Interpersonal Persuasion Using a Facebook App. *Information Technology & People*, 32(5), 1276-1300.
DOI: 10.1108/ITP-06-2018-0278

[15] G. P. Z. Montesdioca & A. C. G. Maçada (2015). Measuring User Satisfaction with Information Security Practices. *Computers & Security*, 48, 267-280.
DOI: 10.1016/j.cose.2014.10.015

[16] S. Goel & I N. Chengalur-Smith (2010). Metrics for Characterizing the Form of Security Policies. *Journal of Strategic Information Systems*, 19, 281-295.
DOI: 10.1016/j.jsis.2010.10.002

[17] M. S. Yim (2016). A Study on the Level of Perception about Information Security Countermeasures: Differences between Managers and Non-Managers. *Korean Management Consulting Review*, 16(4), 33-41.

[18] C. S. Carver & M. F. Scheier (1982). Control Theory: A Useful Conceptual Framework for Personality-Social, Clinical, and Health Psychology. *Psychological Bulletin*, 92(1), 111-135.
DOI: 10.1037/0033-2909.92.1.111

[19] J. R. Edwards (1992). A Cybernetic Theory of Stress, Coping, and Well-being in Organizations. *Academy of Management Review*, 17(2), 238-273.
DOI: 10.5465/amr.1992.4279536

[20] S. Boysen, B. Hewitt, D. Gibbs & A. McLeod (2019). Refining the Threat Calculus of Technology Threat Avoidance Theory. *Communications of the Association for Information Systems*, 45, 95-115.
DOI: 10.17705/1CAIS.04505

[21] D. Carpenter, D. K. Young, P. Barrett & A. J. McLeod (2019). Refining Technology Threat Avoidance Theory. *Communications of the Association for Information Sytems*, 44, 380-407.
DOI: 10.17705/1CAIS.04422

[22] A. Vance, B. B. Anderson, C. B. Kirwan & D. Earle (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG). *Journal of the*

Association for Information Systems, 15(10, 679-722. DOI: 10.17705/1jais.00375

[23] J. Jansen & P. van Schaik (2017). Comparing Three Models to Explain Precautionary Online Behavioural Intentions. I*nformation & Computer Security*, 25(2), 165-180. DOI: 10.1108/ICS-03-2017-0018

[24] A. R. Gillam & A. M. Waite (2021). Gender Differences in Predictors of Technology Threat Avoidance. *Information & Computer Security*, 29(3), 393-412. DOI: 10.1108/ICS-01-2020-0008

[25] M. Chan, I. Woon & A. Kankanhalli (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy & Security*, 1(3), 18-41. DOI: 10.1080/15536548.2005.10855772

[26] T. Herath & H. R. Rao (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, 18, 106-125. DOI: 10.1057/ejis.2009.6

[27] A. C. Johnston, M. Warkentin & M. Siponen (2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric. *MIS Quarterly*, 39(1), 113-134. DOI: 10.25300/MISQ/2015/39.1.06

[28] V. Venkatesh, M. G. Morris, G. B. Davis & F. D. Davis (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3), 425-278. DOI: 10.2307/30036540

[29] J. Nunnally (1978). *Psychometric Theory*, 2nd eds. New York: McGraw-Hill.

[30] M. S. Yim (2018). Factor Analysis for Exploratory Research in the Distribution Science Field. *Journal of Distribution Science*, 13(9), 103-112. DOI: 10.15722/jds.13.9.201509.103

[31] M. S. Yim (2019). A Study on Factor Analytical Methods and Procedures for PLS-SEM (Partial Least Squares Structural Equation Modeling). *Journal of Industrial Distribution & Business*, 10(5), 7-20. DOI: 10.13106/ijidb.2019.vol10.no5.7.

[32] D. Harman (1976). A Single Factor Test of Common Method Variance. *Journal of Psychology*, 35, 359-379.

[33] C. M. Fuller, M. J. Simmering, G. Atinc, Y. Atinc & B. J. Babin (2016). Common Methods Variance Detection in Business Research. *Journal of Business Research*, 69, 3192-3198. DOI: 10.1016/j.jbusres.2015.12.008

[34] J. F. Hair, G. T. M. Hult, G. Ringle & M. Sarstedt (2016). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 2nd eds. Thousand Oaks: Sage.

[35] J. Cohen (1988). *Statistical Power Analysis for the Behavioral Sciences*, Hillside, NJ: Lawrence Erlbaum.

임 명 성(Myung-Seong Yim) [정회원]

· 2002년 2월 : 삼육대학교 경영정보학과(BA)
· 2004년 2월 : 한국외국어대학교 경영정보대학원(MS)
· 2011년 8월 : 서강대학교 경영전문대학원(Ph.D.)
· 2011년 9월 ~ 2012년 2월 : 서강대학교 경영대학 대우교수
· 2012년 3월 ~ 현재 : 삼육대학교 경영학과 부교수
· 관심분야 : ICTs problems, paradox, and side effects, Service Innovation, New Research Methods, New Field of ICTs
· E-Mail : msyim@syu.ac.kr