IDAP INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2022, Vol. 5, No. 1, 5-33. https://doi.org/10.37944/jams.v5i1.138

Factors affecting information security compliance intention of military officer

Kim, Sangyoung* · Lee, Taebok**

ABSTRACT

The purpose of this study is to analyze the factors that influence the information security compliance intention of Korean military officers. For this purpose, a research model was constructed focusing on information security compliance attitude and perceived control, which are the main variables of the theory of planned behavior. In addition, security sensitivity, organization trust, information security work impediment, and sanction, were selected as independent variables. The research model was analyzed through a survey targeting Korean army officers, and the results are as follows. First, security sensitivity, organization trust, and sanctions had a significant effect on information security compliance attitude. However, the effect of information security work impediment had not been identified. Second, it was analyzed that security sensitivity and organization trust had a positive effect on perceived information security compliance control, but the effect of information security work impediment and sanction had not been verified. Third, it was confirmed that the information security compliance attitude and perceived control affect the information security compliance intention, which reconfirmed the results of previous studies. This study is meaningful in that it can improve the information security level of the military organization by suggesting a way to manage these factors.

Keywords : military officer's information security, perceived information security compliance control, security sensitivity, organization trust, sanction

* (First Author) Unit under the direct control of the 3corps, tkddud829@naver.com, https://orcid.org/0000-0001-5313-0114

** (Corresponding Author) Korea National Defense University, Department of Defense Management, Ph.D. Student, taebok88@gmail.com, https://orcid.org/0000-0002-5310-4490

Ⅰ. 서론

최근 과학기술의 급속한 발달은 개인의 일상생활뿐만 아니라 조직환경에도 영향을 미치고 있으며, 군에서도 다양한 정보기술을 적용하여 조직의 체계와 구성원들의 업무환경을 변화시키고자 하는 노력을 지속하고 있다. 그러나 그 과정에서 해킹이나 내부침해 행위로 인한 정보 및 기밀 유출 등의 정보보안 위협 역시 증가하고 있다. 이러한 위협은 정보기술 자체의 결함 및 취약성뿐만 아니라 군 내부구성원의 일탈과 부주의에 의해 발생하게 된다. 실례로 2019년 전방 부대의 정보장교가 군 시설과 무기 배치 등의 기밀자료를 모바일 메신저로 주고받다가 처벌받은 사례가 있다.[1] 또한, Warkentin & Willson(2009)은 바이러스와 같은 기술적 요인보다 조직 내・외부의 인적자원 요소가 더 큰 위협 요소라고 지적하였으며, 정보보안 사고의 상당수가 내부 인원에 의해 발생한다는 연구결과도 있다(Crossler et al., 2013). 이런 사례와 연구는 조직의 정보보안 수준을 향상하기 위해 구성원의 보안 준수 행동을 이끌어내기 위한 조치가 필요하다는 점을 시사한다. 그래서 국방부는 군 부대 및 국방 관련 기관의 정보 유출을 차단하기 위해 각종 규정 및 지침을 제정하고, 정기 및 수시 보안 점검, 보안 관련 각종 경연대회를 개최하는 등 보안사고 예방을 위한 다양한 노력을 기울이고 있다. 이런 노력에도 불구하고 개인의 미숙 및 행정착오에 의한 비밀 오인 파기, 비인가 정보통신 장비 반입, 비밀 분실 등의 보안사고가 발생하고 있으며, 이 중 대부분이 구성원의 보안정책 미준수나 부주의로 인해 생겨나고 있다.

이러한 문제 인식을 계기로 군 장병의 보안 준수와 관련된 연구도 다양하게 진행되고 있다. Park & Oh(2016)는 군 조직문화와 정신전력이 장병의 보안 준수 의지에 영향을 미친다는 점을 분석하였고, Kim, Shin, & Kim(2018)은 군 정보통신부대원을 대상으로 정보보안 정책준수 태도 및 의도에 영향을 미치는 요인을 연구하였다. 특히, Kim & Kim(2020)은 계획된 행동이론을 토대로 군 구성원이 군사보안 행동에 영향을 미치는 정보보안 정책준수 의도와 태도, 주관적 규범 등의 관계를 통계적으로 분석하여 내재적 동기인 윤리의식의 주요 영향요인을 밝혔다. Kim, Seong, & Kim(2020)은 육군 장교의 윤리적 성향이 보안정책 준수 태도와 의도에 영향을 미친다는 연구결과를 제시하였다. 이처럼 선행연구는 대부분 계획된 행동이론을 활용하여 바탕으로 군내 구성원의 행동 의도에 영향을 미치는 보안정책 준수 태도 및 주관적 규범의 요인을 확인하는 데 집중하고 있다. 반면에 계획된 행동이론에서 추가된 주요 변수인 지각된 행동 통제감에 영향을 미치는 요인을 고려한 연구는 많지 않은 실정이다. 이는 개인이 보안을 준수하면서 발생할 수 있는 각종 제약사항을 해결하거나 통제할 수 있는지를 설명하는 지각된 통제감이 ‘보안업무 수행능력이나 지식수준’의 성격을 가진 변수로 태도나 주관적 규범에 비해 다양한 영향요인을 고려하는 것이 쉽지 않기 때문에 관련 실증연구도 부족한 원인으로 볼 수 있다.

---

1) 조선일보(2019.10.01.). 군사기밀 주고받은 군장교・경찰 연인...남녀 모두 징역형. https://www.chosun.com/site/data/html_dir/2019/10/01/2019100101012.html

본 연구는 지각된 행동 통제감이 보안 준수 의도뿐만 아니라 실제 행동에도 영향을 미칠 수 있는 중요한 변수라는 점을 고려하여 해당 영향관계를 장교 집단으로 연구대상을 한정하여 분석하고자 한다. 기존 연구는 주로 장병 전체를 대상으로 군 장병의 보안 준수에 영향을 미치는 요인을 탐색하고 있어 군의 위계적 명령 체계를 고려하여 장교 계급에 주어진 권한과 역할에 따른 조직 구성의 특수성을 반영하는데 한계점이 있다고 볼 수 있다. 특히, 최근 군사기밀 유출 사례(Eom, J. H. & Kim, N. U., 2020)를 살펴보면, 대부분이 군 비밀취급 인가를 갖고 있고, 더 중요한 정보를 취급하는 간부인 장교에 의해 발생하고 있는 것으로 나타났다(예: 비행실습용 훈련기 구매계획을 외국계 군수업체에 전달, 잠수함발사탄도미사일 수중 사출시험 정보를 외부 기자에 누설). 군 장교는 크게 장성・영관・위관급 장교로 구분되는데 장성 및 영관급 장교는 대대급 이상 주요 부대의 지휘관이나 부서장으로서 전반적인 부대관리뿐만 아니라 보안 업무에 대한 지휘・감독 책임을 부여받고 있다.[2)]

구체적으로 위관급 장교는 기술 및 기능 전문가로서 주로 정비 및 조종 등의 분야에서 근무하는 준사관을 제외한 대부분이 소부대의 지휘관(자) 및 제대별 지휘통제기구의 구성원으로서 다양한 군사자료 및 민감자료를 취급하기 때문에 보안 업무를 폭넓게 수행하는 계층이다. 특히 정보병과 장교들은 제대별 정보 및 보안부서의 관리자 또는 실무자로서 정보보안 업무를 계획 및 주도하는 역할을 주로 수행하고 있다. 따라서 현재 연구는 보안 업무를 관리하는 직책에서 주로 근무하는 영관급 이상 장교, 중・소대장 및 지휘통제기구의 구성원을 대상으로 보안 업무 수행에서 장교들의 정보보안 준수 의도에 미치는 영향을 밝힘으로써 군 부대와 국방기관의 보안수준 향상을 위한 정책수립이나 시행지침 개선 등에 활용할 수 있는 기초조사로 학문적인 시사점이 크다고 볼 수 있다.

상기한 연구목적을 달성하기 위해 본 연구는 계획된 행동이론을 바탕으로 하여 군 장교들의 정보보안 준수 의도에 영향을 미치는 요인을 태도와 지각된 통제감을 중심으로 분석하고자 한다. 특히 지각된 통제감은 의도가 행동으로 이어지기 위해서 상황적 제약을 극복하기 위한 능력이 필요하다는 관점에서 추가된 요인으로, 군 장교의 정보보안 준수 의도를 보안업무를 수행하는데 필요한 지식 및 능력 차원에서 설명할 수 있다는 점을 고려하여 본 연구의 주요 변수로 포함하였다. 이러한 연구목적의 달성을 위해 선행연구를 바탕으로 보안 준수 태도와 지각된 통제감에 영향을 미칠 수 있는 변수들을 식별하여 연구모형을 구성하고, 이를 실증적으로 확인하고자 육군 장교를 대상으로 설문조사를 실시하여 그 결과를 분석하였다. 본 연구의 구성은 1장에서 연구의 필요성과 의의를 제시하고, 2장에서는 정보보안 준수 의도와 관련된 선행연구를 분석하였다. 이를 바탕으로 3장에서 연구모형과 가설을 구성하고, 4장에서 분석결과를 제시한 뒤, 마지막 5장에서 연구의 결론 및 시사점을 제시하였다.

2) 국방보안업무훈령(국방부훈령 제2425호, 2020. 5. 11)은 소속부대 및 기관의 전반적인 보안에 대한 지휘・감독 책임이 각급부대의 장에게 있음을 명시하고 있다.

Ⅱ. 이론적 배경

2.1 계획된 행동이론과 정보보안 준수 의도

계획된 행동이론은 합리적 행동이론을 보완하여 태도, 주관적 규범, 지각된 행동 통제감을 세부 요인으로 적용한 이론이다(Ajzen, 1991). 계획된 행동이론에서 각 개인은 자신의 행동에 대한 긍정적 또는 부정적인 태도, 개인 행동에 대한 주변 사람들의 평가나 압력을 의미하는 주관적 규범, 개인이 어떠한 행동을 얼마나 잘 수행하고 통제할 수 있는지에 대한 인식이 행동 의도에 영향을 미친다고 설명한다. 이 중 태도와 지각된 통제감은 행동에 대한 내적 인식을 나타내는 개인적 요인이며, 주관적 규범은 어떠한 행동을 수행하면서 개인이 느끼는 사회적 의무 및 압박감으로서 환경적 요인으로 구분될 수 있다(Kim, Shin, & Kim, 2018). 이러한 계획된 행동이론은 특정 행동에 대한 의도를 개인 및 환경적 요인으로 구분하여 체계적으로 설명할 수 있어 사회과학의 다양한 분야에서 활용되고 있다. 특히 정보보안과 관련된 연구는 조직 구성원의 정보보안 준수 의도에 영향을 미치는 요인을 분석하기 위한 이론으로 활용되고 있다. 정보보안 준수 의도는 다양한 보안 위협으로부터 조직 내 주요 정보를 보호하고자 하는 구성원의 의지로 구성원 개인의 정보보안 준수 의도가 높을수록 보안 행동에 정적인 영향이 나타났다(Vance & Siponen, 2012). 다시 말해 정보보안 준수 의도는 조직의 보안수준 향상을 위해 중요하게 관리되어야 할 요인이라고 할 수 있다. 이와 관련하여 Al-Omari et al.(2013)는 정보보안 주관적 규범과 태도, 통제감이 정보보안 준수 의도와 긍정적인 관계를 밝혔다. 또한, 조직원의 주관적 규범과 태도가 정보보안 준수 의도에 영향을 미친다는 연구결과(Hwang, I. H. & Hu, S. H., 2018)를 제시하는 등 계획된 행동이론을 바탕으로 정보보안 준수 의도를 설명하기 위한 연구가 활발하게 진행되고 있다.

군은 국가안보와 직결되는 군사기밀과 정보를 다루기 때문에 이를 보호하기 위한 정보보안의 중요성이 중요한 조직[3]으로 고도의 보안기술과 복잡한 보안정책을 적용하고 있다. 하지만, 최근까지도 군 내부구성원의 보안 규정 미준수와 부주의로 인한 정보유출 위협이 증가함에 따라 정보보안 준수 의도를 높이기 위한 관련 연구가 활발하게 진행되고 있다(Table 1). 예를 들어, Park & Oh(2016)는 장병의 보안 준수 의지를 높이는 주요 요인으로 군 조직문화와 군인정신・국가관・안보관 등의 정신전력을 강조하였다. Kim, Shin, & Kim(2018)은 군 정보통신부대원을 대상으로 정보보안 준수의도에 정보보안 준수 태도와 규범이 긍정적인 영향을 미치며, 이런 영향관계에서 내재적 이익과 보안 안전성 등이 정보보안 준수 태도를 높이는 요인이라는 것을 밝혔다. 또한, Kim(2020)은 군사보안 준수에 대한 태도와 주관적 규범에 영향을 미치는 내・외적동기(군 조직원의 윤리의

3) 국방부 소관 법령인 군사기밀 보호법(법률 제13503호, 2015. 9. 1. 시행)은 누설될 경우 국가안전보장에 명백한 위험을 초래할 우려가 있는 문서, 기록 등의 군사기밀을 보호하기 위한 목적으로 제정되어 시행되고 있는데, 이는 군 조직 내 정보보안의 중요성을 나타내는 대표적인 사례라고 할 수 있다.

식, 보안교육, 처벌 명확성)의 역할을 제시하였다. 특히, Kim, Seong, & Kim(2020)은 군 장교를 대상으로 도덕성과 책임감 등의 윤리적 성향이 보안 준수 태도에 영향을 미친다는 점을 실증적 분석을 통해 검증하였다. 가장 최근 연구(Park, E. C. & Jeon, K. S., 2021)에서는 과중한 업무가 보안 스트레스를 유발하고 보안 스트레스는 보안 준수 행동에 부정적 영향을 미친다는 점을 확인하였다. 선행연구 고찰 결과, 군 구성원의 보안 준수와 관련된 연구는 다양하게 이뤄지고 있으나, 주로 합리적 행동이론의 주요변수인 태도와 주관적 규범에 영향을 미치는 요인에 대해 분석하고 있다. 그러나 기존 합리적 행동이론의 제한점을 보완하고자 추가된 변수인 지각된 행동 통제감의 영향요인에 대한 연구는 부족한 실정이다. 지각된 행동 통제감은 의도가 행동으로 이어지는 과정에서 상황적 제약을 극복할 수 있는 자원에 대한 고려가 필요하다는 측면에서 추가된 변수인데, 군 장교가 정보보안을 준수하는데 필요한 보안 업무 능력이나 지식 등의 차원에서 설명할 수 있게 해주는 변수가 될 수 있다.

<Table 1> Military-related information security research

Researcher	Main Variable	Analysis Method	Result
Park & Oh (2016)	Psychological military strength. Culture of military organization. Security compliance intention. Security performance.	Structural Equation Modeling (SEM)	Psychological military strength has a positive effect on security compliance and performance. Culture of military organization has a positive (+) effect on security performance.
Kim, Shin, & Kim (2018)	Information security policy-compliance (ISPC) intention, attitude, subjective norm. Perceived security safety. Security vulnerability. Intrinsic benefits. Loyalty to the military.	Structural Equation Modeling (SEM)	ISPC intention was affected by subjective norms and ISPC attitude. Then, the ISPC attitude was affected by one's perceived security safety or security vulnerability, intrinsic benefits, and the loyalty to the military.
Kim, Seong, & Kim (2020)	Ethical disposition. Perceived work environment. Turnover intention. Information security policy-compliance(ISPC) attitude, intention.	Structural Equation Modeling (SEM)	Ethical disposition has a positive effect on ISPC attitude and Perceived work environment affects turnover intention. Turnover intention has a negative effect(-) on ISPC attitude, ISPC attitude and intention have a positive (+) relationship.
Kim, D. H. (2020)	Internal motives External motives Military Security attitude, subjective norm, perceived control, and intention	Structural Equation Modeling (SEM)	Internal and external motives of military members are related to military security attitude, subjective norm, and perceived control. Military security attitudes, subjective norms, and perceived control influence intention, and intention are related to behavior.

Park & Jeon (2021)	Task overload, complexity, uncertainty, and conflict. Security stress. Security compliance behavior.	Structural Equation Modeling (SEM)	Task overload has a positive (+) effect on security stress, and security stress has a negative effect on security compliance behavior.

이를 고려하여 본 연구에서는 계획된 행동이론의 변수를 중심으로 군 장교의 정보보안 준수 의도와 관련된 요인을 분석하고자 하며, 특히 개인적 요인인 태도와 지각된 행동 통제감에 영향을 주는 변수 분석에 중점을 두고자 한다. 이러한 연구목적 달성을 위해 다양한 선행연구 분석을 통해 보안 준수와 관련된 개념으로 확인된 보안 감수성, 조직 신뢰, 정보보안 업무 장애, 제재를 개인적 요인 변수로 식별하였다. 본 연구에서는 특정 행동을 수행하기 위한 동기는 즐거움을 추구하고자 하는 접근 동기와 고통을 피하고자 하는 회피 동기의 두 가지 차원으로 구분될 수 있다는 선행연구 결과(Cornwell, Franks, & Higgins, 2014)를 바탕으로 보안 감수성과 조직 신뢰는 부대의 정보보안 목표 달성의 긍정적 측면과 관련 있는 접근 동기 측면의 변수로, 정보보안 업무 장애와 제재는 보안 미준수로 발생할 수 있는 위험과 관련된 회피 동기 측면의 변수로 제시하였다. 이를 바탕으로 구성원의 보안 준수를 위한 접근과 회피 측면의 설명변수가 태도와 지각된 행동 통제감에 어떠한 영향을 주는 살펴보기 위한 연구모형을 구성하였으며, 환경적 요인이라고 할 수 있는 주관적 규범은 통제변수로 연구에 포함하였다.

2.2 보안 감수성

일반적으로 감수성은 외부환경 및 타인의 자극에 대한 반응 능력을 말하는데, 사회과학 분야에서는 성인지 감수성, 인권 감수성, 문화 간 다양성 감수성 등의 개념으로 다양하게 활용되고 있다. 보안 감수성은 보안 업무를 수행하면서 발생 가능한 보안 위협을 예방하기 위한 보안정책 및 기술에 대해 인식하고 행동하고자 하는 개인의 민감성이라고 정의될 수 있는데, 보안 위협 및 수단의 필요성에 대한 인식, 보안 수단을 사용하도록 만드는 다양한 동기, 보안 수단의 효과적인 사용을 위해 필요한 지식 등의 세 가지 하위요인으로 구성될 수 있다(Das et al., 2014). 조직에서 발생하는 정보보안 위반 사례의 50% 이상이 내부 구성원에 의해 발생한다는 Crossler et al.(2013)의 연구결과는 조직 구성원이 지닌 보안 감수성에 따라 조직 전체의 보안 위반사례 및 보안 수준이 달라질 수 있다는 점을 시사한다. 이와 관련하여 Lee & Kim(2021)은 보안 감수성이 군 구성원의 지각된 처벌과 국방보안 준수 의도 간의 관계를 조절하는 변수라는 점을 실증적으로 분석함으로써, 보안 감수성이 정보보안 준수 의도에 미치는 영향에 대해 설명하였다. 본 연구에서는 이러한 개념과 선행연구 결과를 바탕으로 보안 감수성을 정보보안 준수 태도 및 행동 통제감 등의 개인적 요인에 영향을 미칠 수 있는 변수 중 하나로 선정하였다.

2.3 조직 신뢰

신뢰는 조직구성원 및 개인 간 친밀성을 가지고 긍정적인 믿음을 형성하고 있는 수준으로서(Nachmias, 1985), 상대방이 특정 행동 또는 목표에 대하여 자신과 유사한 행동을 할 것이라는 심리적 믿음(Gillespie & Dietz, 2009; Hwang, I. H. & Hu, S. H., 2021a)으로 정의될 수 있다. 조직신뢰는 구성원이 조직에 대하여 가지는 긍정적 믿음의 수준으로 정의되는데(Kim, H. G., 2008), 조직구성원이 조직 활동에 자발적으로 참여하게 해주며, 각종 위기 상황에서 효과적으로 대응하도록 하는 심리적 기반이 되는 중요한 요인이라고 할 수 있다(Kim, C. J. & Yoon, C. S., 2008).

정보보안 분야에서 조직 신뢰는 조직의 보안 규정 및 정책 등에 대한 구성원의 믿음을 바탕으로 형성되며(Lowry et al., 2015), 조직에 대한 신뢰는 조직의 정보보안 체계가 자신을 포함한 구성원들에게 이익이 될 것이라고 믿고 행동하도록 해준다(Hwang, I. H., 2021b). 즉, 조직의 정보보안에 대한 신뢰를 지닌 구성원은 조직의 정보보안 정책 및 기술을 따르려는 경향이 커짐에 따라 이를 준수하고자 하는 의도 역시 높아질 수 있다(Hwang, I. H. & Hu, S. H., 2021a). 이와 관련하여 Kim, H. S.(2016)은 국내 창업교육센터 입주기업을 대상으로 조직 신뢰가 보안정책 준수 의지에 긍정적인 영향을 미친다는 점을 분석하였고, Lee & Lee(2019)는 민간 경비원의 조직 신뢰와 보안정책 준수 의지가 긍정적 관계가 있음을 실증적으로 확인하였다. 이를 바탕으로 본 연구에서는 조직에 대한 신뢰를 군 장교의 보안 준수와 관련 있는 변수로 포함하였다.

2.4 정보보안 업무 장애

업무 장애는 특정 정책 및 기술 도입에 따른 새로운 요구사항으로 인해 업무에 장애가 있다고 느끼는 정도(Bulgurcu, Cavusoglu, & Benbasat, 2010)를 의미하는데, 추가적인 보안정책 및 기술을 기존 업무에 적용해야 하는 정보보안과 같은 분야에서 자주 나타날 수 있는 문제이다(Hwang, I. H. & Kim, S. W., 2017). 다시 말해 조직의 정보보안 정책 및 기술을 적용하는 과정에서 업무에 장애가 있다고 느끼는 것을 정보보안 업무 장애라고 정의할 수 있다. 이러한 정보보안 업무 장애는 개인의 보안 준수 행동에 부정적 영향을 미치는 요인이 될 수 있는데, 이와 관련하여 Hwang(2020)은 금융업에 근무하는 직장인을 대상으로 정보보안 업무 장애가 준수 의도에 부정적 영향을 미친다는 점을 확인하였고, Hwang & Hu(2021b)는 정보보안 업무 장애가 정보보안 준수 걱정에 영향을 미침으로써 준수 의도에도 부정적 영향을 미친다는 점을 실증 분석하였다.

군은 국가안보와 직결되는 중요하고 민감한 정보를 다루는 조직으로 이를 보호하기 위한 고도의 보안기술 및 엄격하고 복잡한 보안 절차를 적용하고 있다. 따라서 군 구성원 역시 정보보안에 따른 업무 장애를 지각하고 있을 가능성이 높으며, 이는 보안 준수의도에 부정적인 영향을 미칠 수 있다. 따라서 본 연구에서는 군 복무 장교의 정보보안 업무 장애 인식을 보안 준수에 영향을 미칠 수 있

는 요인으로 선정하였다.

2.5 제재

제재는 억제이론에서 정보보안에 대한 개인의 인식을 높이는 주요 접근 방법 중 하나로 제시되는 개념이며, 처벌이나 페널티 등의 용어로 사용되기도 한다. 억제이론은 조직의 보안정책을 준수하지 않을 때 적용 가능한 제재의 유형 및 강도를 구성원에게 인식시키고, 이를 지속적으로 통제하고 확인함으로써 보안 위협요소를 최소화할 수 있다고 제시한다(Onwudiwe, Odo, & Onyeozili, 2005). 또한, 제재의 하위요인으로 엄격성・확실성・신속성 등이 제시되는데 엄격성은 위반행위를 충분히 단념시킬 수 있을 정도의 엄격함을 의미하며, 확실성은 보안정책을 준수하지 않으면 반드시 제재를 받게 될 것이라는 점을 인식시키는 것이다. 신속성은 위반행위 이후 즉각적인 제재가 이루어질 때 그 효과가 발휘될 수 있다는 점을 제시해준다. 이와 관련하여 Kim & Song(2011)은 제재의 강도가 정보보안 준수 의도와 긍정적인 관계를 보인다고 설명하였으며, Hwang(2021a)는 제재의 심각성과 확실성이 보안 준수 의도에 영향을 미칠 수 있음을 확인하였다. 또한 Kim, D. H.(2020)은 군 조직원이 지각하는 처벌 명확성이 보안 준수 태도와 주관적 규범에 긍정적 영향을 미친다는 점을 확인하였으며, Lee & Kim(2021)은 군 장교의 처벌에 대한 지각이 국방보안 준수 의도와 관계가 있다는 점을 실증 분석하였다. 이렇듯 제재는 조직 구성원의 정보보안 준수 의도를 설명하는 변수로 활용되어왔으며, 이를 고려하여 본 연구에서도 제재를 주요 변수로 포함하였다.

Ⅲ. 연구모형 및 가설 설정

3.1 연구모형

본 연구는 군 장교의 정보보안 준수 의도에 영향을 미치는 요인에 대해 알아보기 위한 연구모형을 구성하였다(Figure 1). 계획된 행동이론에서 행동 의도에 영향을 미치는 것으로 제시된 주요 변수 중 개인적 요인을 중심으로 연구모형을 구성하였고, 환경적 요인인 주관적 규범은 통제변수로 포함하였다. 또한, 선행연구에서 조직구성원의 보안 준수에 영향을 미치는 것으로 확인된 보안 감수성, 조직 신뢰, 정보보안 업무 장애, 제재를 선행변수로 제시하여 정보보안 준수 태도와 지각된 통제감에 미치는 영향에 대해 분석하고자 하였다.

3.2 연구가설

3.2.1 접근 측면의 요인(보안 감수성・조직 신뢰)과 정보보안 준수 태도 및 지각된 통제감

동기와 관련된 연구에서 접근 동기는 어떠한 이점이나 즐거움을 얻기 위해 특정 행동을 수행한다고 바라보는 관점이다. 조직에서 요구하는 정보보안 정책이나 기술을 사용하는 것에 대한 긍정적 인식과 관련된 보안 감수성과 조직 신뢰는 접근 측면의 요인이라고 볼 수 있으며, 이는 정보보안 준수에도 영향을 미칠 수 있을 것이다. 특히 보안 감수성은 보안 위협에 따라 적절한 보안 수단을 사용해야한다는 인식과 이와 관련된 지식, 보안정책 및 규정을 준수하고자 하는 동기 등의 하위요인으로 설명될 수 있다. 따라서 높은 수준의 보안 감수성을 지닌 조직 구성원은 정보보안을 준수해야 하는 필요성을 명확하게 인식하고 있다. 이를 위한 수단과 관련된 지식을 갖추고 있어 보안 준수에 대한 태도도 긍정적으로 나타날 수 있으며, 이는 군 구성원의 보안 감수성이 국방보안 준수에 영향을 미친다는 연구를 통해 확인되기도 하였다(Lee, T. B. & Kim, S. Y., 2021). 그리고 보안 감수성이 높은 구성원은 조직의 보안정책이나 기술을 준수해야 하는 필요성에 대해 명확히 인식할 뿐 아니라 이를 활용하기 위한 지식이나 능력의 수준도 높기 때문에 지각된 통제감에도 긍정적인 영향을 미칠 것으로 추론할 수 있다.

조직 신뢰는 구성원이 조직에서 요구하는 행동이나 절차에 긍정적으로 반응하는데 도움을 주는 것으로 알려져 있다. 따라서 조직의 정보보안 정책에 대한 높은 신뢰를 지닌 구성원은 조직의 정보보안 절차 및 기술에 대해 긍정적으로 인식할 뿐만 아니라 적극적으로 준수하고자 할 것이며, 이는 다양한 선행연구를 통해 검증되었다(Hwang, I. H., 2021b; Hwang, I. H. & Hu, S. H., 2021a). 또한 조직 신뢰가 형성된 개인은 조직 내 모든 구성원이 요구되는 보안정책 및 절차를 준수하고 있을 것이라는 믿음을 가지게 될 것이다. 이러한 믿음은 조직 내에서 개인의 보안 업무를 용이하게 수행할 수 있다는 인식을 가지게 함으로써 지각된 통제감에 영향을 미칠 수 있을 것이다. 본 연구에서는 이러한 논거와 선행연구 결과를 바탕으로 다음과 같은 연구가설을 구성하였다.

가설1(H1) : 정보보안 접근 동기 측면의 요인은 준수 태도와 통제감에 영향을 미칠 것이다.
가설1a(H1a) : 보안 감수성은 정보보안 준수 태도에 정(+)의 영향을 미칠 것이다.
가설1b(H1b) : 보안 감수성은 정보보안 준수 통제감에 정(+)의 영향을 미칠 것이다.
가설1c(H1c) : 조직 신뢰는 정보보안 준수 태도에 정(+)의 영향을 미칠 것이다.
가설1d(H1d) : 조직 신뢰는 정보보안 준수 통제감에 정(+)의 영향을 미칠 것이다.

3.2.2 회피 측면의 요인(정보보안 업무 장애・제재)과 정보보안 준수태도 및 지각된 통제감

회피 동기는 개인이 고통이나 어려움을 피하기 위해 행동한다고 이해하는 관점인데, 보안 절차나 기술을 따르면서 겪게 되는 업무 장애와 정보보안 미준수 시 가해질 수 있는 제재는 정보보안

준수와 관련된 회피 측면의 동기라고 볼 수 있다. 그리고 이러한 회피 측면의 동기 역시 정보보안 준수 행동에 영향을 미칠 수 있는 변수로 고려해볼 수 있다. 우선 정보보안 업무 장애는 기존 업무에 정보보안 업무를 추가로 수행하면서 겪게 되는 어려움이나 부정적 감정 등을 의미하기 때문에 구성원이 지각하는 업무 장애 수준이 높을수록 정보보안 정책 준수에 대한 부정적 태도가 형성될 수 있는데, 이는 선행연구를 통해 실증적으로 입증되었다(Hwang, I. H., 2020; Hwang, I. H. & Hu, S. H., 2021b). 게다가 정보보안 업무 장애는 본연의 업무를 수행하는 과정에서 보안 업무가 추가됨에 따라 겪게 되는 어려움이기 때문에, 보안 준수와 관련된 주변 상황을 쉽게 통제할 수 있다는 인식에 부정적인 영향을 미치게 될 것이라는 점도 고려해볼 수 있다. 다음으로 제재는 정보보안 정책을 준수하지 않을 때 가해지는 물리적 또는 사회적인 억제 수단인데, 조직 구성원이 조직 내에서 제재가 명확하고 확실하게 이행되고 있다는 점을 인식할 경우 보안을 준수하는데 긍정적인 반응을 보일 수 있으며, 나아가 지각된 행동 통제감과 밀접한 관련이 있는 실제 행동에도 영향을 미칠 수 있다는 점이 다수의 선행연구를 통해 확인되었다(Kim, D. H., 2020; Kim, S. H. & Song, Y. M., 2011; Lee, S. H. & Lee, J. L., 2019). 이를 토대로 본 연구는 다음과 같은 연구가설들을 설정하였다.

가설2(H2) : 정보보안 회피 동기 측면의 요인은 준수 태도와 통제감에 영향을 미칠 것이다.
가설2a(H2a) : 정보보안 업무 장애는 정보보안 준수 태도에 부(−)의 영향을 미칠 것이다.
가설2b(H2b) : 정보보안 업무 장애는 정보보안 준수 통제감에 부(−)의 영향을 미칠 것이다.
가설2c(H2c) : 제재는 정보보안 준수 태도에 정(+)의 영향을 미칠 것이다.
가설2d(H2d) : 제재는 정보보안 준수 통제감에 정(+)의 영향을 미칠 것이다.

3.2.3 정보보안 준수 태도・지각된 통제감과 정보보안 준수 의도

행동에 대한 태도와 지각된 통제감이 의도에 영향을 미칠 수 있다는 점은 계획된 행동이론을 활용한 다양한 선행연구를 통해 실증적으로 확인되었으며, 정보보안과 관련된 연구에서도 정보보안에 대한 태도와 통제감이 준수 의도에 긍정적 영향을 미치는 것으로 나타났다(Jeong, H. I. & Kim, S. J., 2018; Kim, D. H., 2020; Kim, J. K. & MOU JIAN, 2020). 다시 말해 정보보안 준수에 대한 긍정적인 태도와 이를 잘 수행하고 통제할 수 있다는 믿음이 있으면 보안 준수에 대한 의도도 높아질 수 있는 관계를 가정하여 다음과 같은 가설을 구성하였다.

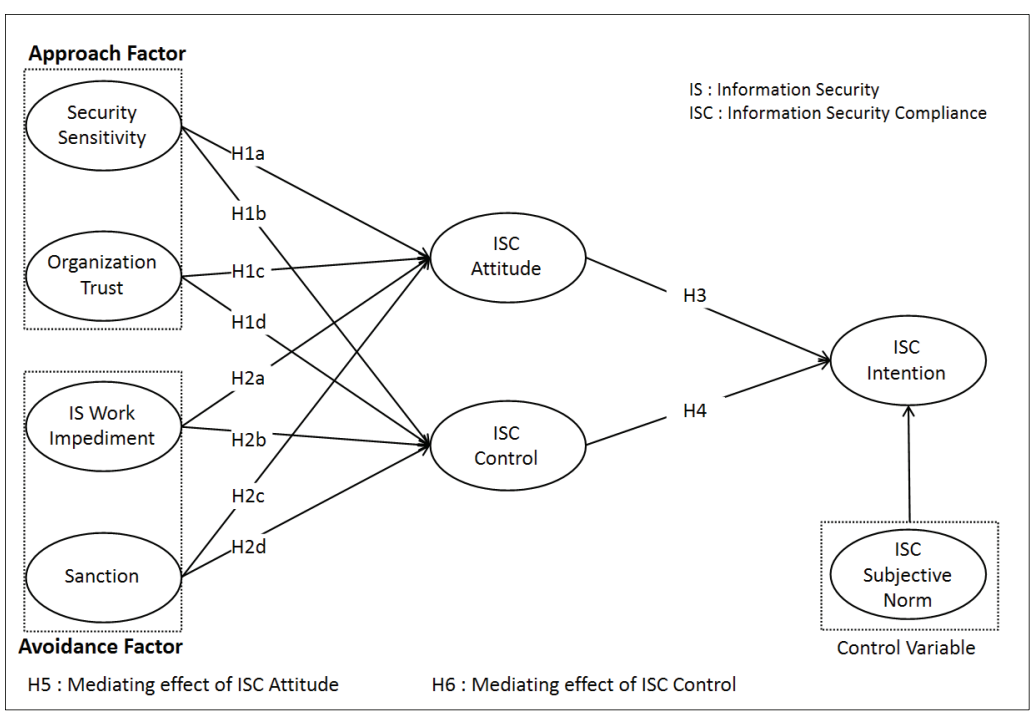
가설3(H3) : 정보보안 준수 태도는 정보보안 준수 의도에 정(+)의 영향을 미칠 것이다.
가설4(H4) : 정보보안 준수 통제감은 정보보안 준수 의도에 정(+)의 영향을 미칠 것이다.

한편 계획된 행동이론을 바탕으로 다수의 선행연구에서 다양한 설명변수와 행동 의도와의 관계에서 태도와 지각된 통제감의 매개효과가 확인되었다(Kwon, Y. S. & Nam, J. M., 2021; Kim,

Shin, & Kim, 2018). 본 연구에서는 정보보안 준수와 관련된 분석에서도 정보보안 준수 태도와 지각된 통제감이 보안 감수성, 조직 신뢰, 정보보안 업무 장애, 제재 등의 독립변수와 정보보안 준수 의도와의 관계를 매개하는 효과가 있는지 확인하기 위해 다음과 같은 가설을 구성하였다.

가설5(H5) : 정보보안 준수 태도는 설명변수와 정보보안 준수 의도의 관계를 매개할 것이다.
가설5a(H5a) : 정보보안 준수 태도는 보안 감수성과 준수 의도의 관계를 매개할 것이다.
가설5b(H5b) : 정보보안 준수 태도는 조직 신뢰와 준수 의도의 관계를 매개할 것이다.
가설5c(H5c) : 정보보안 준수 태도는 정보보안 업무 장애와 준수 의도의 관계를 매개할 것이다.
가설5d(H5d) : 정보보안 준수 태도는 제재와 준수 의도의 관계를 매개할 것이다.

가설6(H6) : 정보보안 준수 통제감은 설명변수와 정보보안 준수 의도의 관계를 매개할 것이다.
가설6a(H6a) : 정보보안 준수 통제감은 보안 감수성과 준수 의도의 관계를 매개할 것이다.
가설6b(H6b) : 정보보안 준수 통제감은 조직 신뢰와 준수 의도의 관계를 매개할 것이다.
가설6c(H6c) : 정보보안 준수 통제감은 정보보안 업무 장애와 준수 의도의 관계를 매개할 것이다.
가설6d(H6d) : 정보보안 준수 통제감은 제재와 준수 의도의 관계를 매개할 것이다.



<Figure 1> Research Model

Ⅳ. 연구방법 및 결과

4.1 자료수집 및 참가자 특성

본 연구는 군 장교의 정보보안 준수 의도에 영향을 미치는 요인을 실증적으로 분석하기 위해 설문조사 기법을 활용하였다. 설문대상의 범위는 보병사단 예하부대에서 지휘자(관) 및 부서장, 참모 장교로 근무하는 영관급 및 위관급 장교로 한정하였다. 다만, 기술 및 기능 분야에서 주로 업무를 수행하는 준사관은 연구목적을 고려하여 설문 대상에서 제외하였다. 설문조사는 군 인트라넷 메일과 SNS를 통해 육군의 2개 상비사단[4]에서 근무하는 702명의 장교에게 설문지를 배포하였으며, 223부의 설문지가 회수되었다(응답률 : 31.7%). 이 중 불성실하게 작성이 되었거나, 결측값 등의 오류가 있는 설문지를 제외한 214부의 유효 데이터를 연구분석에 활용하였다. 설문 응답자의 특성(Table 2)은 살펴보면, 조직구성원의 다수를 차지하고 있는 군의 구조 특성과 같이 남성이 91.1% 여성이 8.9%를 차지하고 있다. 계급별 분포는 위관장교 73.7%, 영관장교 26.3%이며, 직책은 지휘관 29.4%, 참모 72.6%의 분포로 나타났다. 군 장교 전체 정원 7만여 명 중 영관급 이상 장교가 2만여 명(약 29%)이라는 점을 고려할 때,[5] 분석을 위해서 수집한 표본이 군 장교의 전체 분포와 비교적 유사한 특성을 나타내고 있어 모집단을 대표하는 데 무리가 없는 것으로 판단하였다.

<Table 2> Survey respondents

Category			Frequency (N)	%
Gender	Male		195	91.1
	Female		19	8.9
Rank	Company officer	2nd lieutenant	11	5.1
		1st lieutenant	21	9.8
		Captain	126	58.8
	Field officer	Major	36	16.9
		Lieutenant colonel	17	8.0
		Colonel	3	1.4
Position	Commander		63	29.4
	Staff		151	70.6
Total			214	100

4) 상비사단은 평시 편제병력의 대부분이 현역으로 구성되어 즉각적인 전투력 발휘가 가능한 사단이다. 따라서 상비사단에서 근무하는 장교들은 경계 및 전투태세와 관련된 민감정보 및 군사기밀을 상시 다루고 있어 본 연구의 목적에 부합한 설문대상이라고 할 수 있다.

5) 와이드안보(2021.02.01.). 2021년 국방예산 분석 및 정책적 함의. Rok Angle, 232호. https://kookbang.dema.mil.kr/newsWeb/20210201/1/BBSMSTR_000000100003/view.do

4.2 변수의 조작적 정의 및 측정문항

본 연구에서는 군 장교의 정보보안 준수 의도에 영향을 미치는 변수를 측정하기 위해 선행연구에서 검증된 설문 항목을 응답 대상자의 특성을 고려하여 군 조직의 정보보안 환경 특성 및 군대 용어에 맞게 수정하여 사용하였다. 각 문항은 7점 리커트 척도로 측정하였으며, 세부적인 측정문항 정보는 부록 1과 같다.

보안 감수성은 '보안 위협을 예방하기 위한 보안정책 및 기술에 대해 인식하고 행동하고자 하는 개인의 민감성 정도'를 의미하며(Das et al., 2014), 이를 측정하기 위해 Lee & Kim(2021)의 연구에서 사용한 8개의 설문 문항을 활용하였다. 조직 신뢰는 '구성원이 조직에 대하여 가지는 긍정적 믿음의 수준'으로 정의되는데(Kim, H. G., 2008), 이를 측정하기 위해 Agarwal(2013)의 연구를 바탕으로 Hwang(2021b)가 사용한 4개의 설문 항목을 사용하였다. 정보보안 업무 장애는 '조직의 정보보안 정책 및 기술을 적용하는 과정에서 업무에 장애가 있다고 느끼는 정도'로 정의할 수 있으며, Hwang & Hu(2021b)가 선행연구를 통해 도출한 3개의 설문 문항에 정보보안 준수가 업무 효율에 미치는 영향을 측정하기 위한 1문항을 추가하여 활용하였다. 제재는 '정보보안을 준수하지 않았을 때 발생하는 물리적・사회적 처벌의 정도'라고 정의할 수 있으며, Hwang(2021a)의 연구에서 사용한 6개의 설문 문항을 수정한 후 사용하였다. 정보보안 준수 태도는 '구성원이 정보보안 준수를 긍정적으로 인식하는 정도'로 정의되며, Kim, D. H.(2020)이 사용한 5개의 설문 문항을 수정하여 활용하였다. 정보보안 준수 통제감은 '구성원이 보안정책 및 절차의 준수를 잘 수행하고 통제할 수 있다고 믿는 정도'로 Kim, Shin, & Kim(2018)의 연구에서 지각된 통제감을 측정하기 위해 사용한 3개 문항을 활용해서 측정하였다. 정보보안 준수 주관적 규범은 '구성원이 정보보안 준수에 대해 느끼는 사회적 압력의 정도'라고 정의할 수 있으며, Kim, Shin, & Kim(2018)이 사용한 4개 문항을 연구목적에 맞게 수정하여 활용하였다. 정보보안 준수 의도는 '조직의 정보보안 정책을 준수하고자 하는 자발적 의지의 정도'로 정의하였으며, Herath & Rao(2009)가 보안정책 준수 의도 측정을 위해 사용한 3개의 설문 문항을 사용하였다.

4.3 분석방법 및 결과

PLS는 복잡한 연구모형을 검증(Hair et al., 2010)하거나 이론개발의 초기 단계에서 사용하기에 적합한 분석기법으로(Barclay, Higgins, & Thomson, 1995), 자료의 표본 분포에 관한 가정이나 제약으로부터 비교적 자유롭다는 특성이 있다(Chin, 1998). 본 연구는 정보보안 준수 의도와 관련된 다양한 변수들의 관계를 분석하고자 하는 복잡한 연구모형이며, 214건의 비교적 적은 표본으로 경로계수 유의성 검증을 해야 한다는 점을 고려하여 PLS 분석기법을 사용하였다. 분석 프로그램은 SmartPLS 3.0을 활용하였고, 측정모형 분석과 구조방정식 모형 분석의 두 단계로 나누어 분석하였

다. 먼저 측정모형 분석 단계에서 변수 측정의 타당도와 신뢰도를 검증하고, 구조방정식 모형 분석 단계에서는 경로계수 분석을 통한 가설검증을 실시하였다.

4.3.1 측정모형 분석

측정모형의 신뢰성과 타당성은 Cronbach's α계수, 복합신뢰도, 평균분산추출지수(AVE: Average Variance Extracted) 등으로 검증 가능하며, 본 연구의 신뢰성 및 타당성 분석결과는 Table 3과 같다. Cronbach's α계수는 현상이나 대상을 일관성 있게 측정하였는지를 검증하는 값으로 0.7보다 클 때 내적일관성을 충족한다고 볼 수 있는데(Koo, D. M., 2017), 본 연구에서 사용된 변수들의 Cronbach's α값은 0.891~0.955에 분포하고 있어 내적일관성이 있는 것으로 확인되었다. 복합신뢰도 역시 내적일관성을 검증하는 수단으로 0.7 이상이면 신뢰도 또는 집중타당도가 높은 것으로 해석하는데(Koo, D. M., 2017), 변수들의 복합신뢰도는 0.932~0.963으로 0.7을 넘어서고 있다. 평균분산추출지수(AVE)가 0.5보다 클 때 모델이 타당한 것으로 판단하는데(Barclay, Higgins, & Thomson, 1995), 연구에서 사용된 모든 변수의 평균분산추출지수가 0.5 이상으로 이를 충족하고 있다.

한편 판별타당도는 각 변수의 평균분산추출지수의 제곱근이 다른 변수와의 상관계수보다 클 때 적절한 것으로 판단한다(Fornell & Larcker, 1981). Table 4를 통해 확인할 수 있듯이 평균분산추출지수의 제곱근이 변수 간 상관계수보다 큰 것으로 나타났다. 한편 PLS 구조방정식 모형은 평균자승잔차제곱근(SRMR)이 0.08보다 작을 경우 적합한 것으로 해석하는데(Henseler, Hubona, & Ray, 2016), 본 연구모형의 SRMR은 0.056으로 모형의 적합도가 있는 것으로 판단하였다.

<Table 3> Reliability and validity of measurement tools

Variable		Average	Standard Deviation	Factor loading	Cronbach's α	Composite Reliability	AVE
Security Sensitivity (SS)	SS1	5.556	1.236	0.799	0.939	0.950	0.703
	SS2	5.519	1.210	0.869			
	SS3	5.379	1.351	0.825			
	SS4	5.449	1.327	0.883			
	SS5	5.327	1.386	0.856			
	SS6	5.224	1.429	0.882			
	SS7	5.425	1.120	0.816			
	SS8	5.341	1.204	0.768			
Organization Trust (OT)	OT1	5.150	1.593	0.873	0.955	0.963	0.787
	OT2	5.056	1.582	0.911			
	OT3	4.963	1.654	0.902			
	OT4	4.841	1.536	0.883			
Information Security Work Impediment (ISWI)	ISWI1	5.201	1.589	0.926	0.941	0.956	0.845
	ISWI2	5.509	1.472	0.914			
	ISWI3	5.533	1.493	0.917			
	ISWI4	5.509	1.555	0.921			

Sanction (SC)	SC1	5.724	1.302	0.826	0.916	0.935	0.706
	SC2	5.636	1.274	0.892			
	SC3	5.607	1.281	0.913			
	SC4	5.449	1.399	0.834			
	SC5	5.949	1.250	0.747			
	SC6	5.551	1.266	0.819			
Information Security Compliance Attitude (ISCA)	ISCA1	5.701	1.201	0.834	0.917	0.938	0.752
	ISCA2	5.411	1.420	0.883			
	ISCA3	5.547	1.299	0.897			
	ISCA4	5.402	1.481	0.907			
	ISCA5	4.991	1.745	0.813			
Information Security Compliance Control (ISCC)	ISCC1	5.164	1.478	0.885	0.891	0.932	0.822
	ISCC2	5.533	1.175	0.918			
	ISCC3	5.547	1.194	0.916			
Information Security Compliance Subjective Norm(ISCSN)	ISCSN1	5.794	1.217	0.884	0.925	0.947	0.817
	ISCSN2	5.780	1.243	0.904			
	ISCSN3	5.757	1.263	0.912			
	ISCSN4	5.729	1.185	0.916			
Information Security Compliance Intent(ISCI)	ISCI1	5.864	1.146	0.905	0.915	0.946	0.854
	ISCI2	5.883	1.144	0.927			
	ISCI3	5.776	1.206	0.940			

<Table 4> Discriminant validity evaluation results

Variable	SS	OT	ISWI	SC	ISCA	ISCC	ISCSN	ISCI
SS	**0.838**							
OT	0.604	**0.887**						
ISWI	0.135	0.079	**0.919**					
SC	0.706	0.564	0.182	**0.840**				
ISCA	0.728	0.675	0.128	0.675	**0.867**			
ISCC	0.625	0.573	0.128	0.573	0.617	**0.906**		
ISCSN	0.634	0.474	0.254	0.640	0.635	0.555	**0.904**	
ISCI	0.738	0.520	0.205	0.666	0.683	0.617	0.687	**0.924**

* The bold underlined diagonal values represent the square root of the AVE.
Note. SS (Security Sensitivity), OT (Organization Trust), ISWI (Information Security Work Impediment), SC (Sanction), ISCA (Information Security Compliance Attitude), ISCC (Information Security Compliance Control), ISCSN (Information Security Compliance Subjective Norm), ISCI (Information Security Compliance Intention)

4.3.2 구조방정식 모형 분석

SmartPLS 3.0을 이용한 구조모형의 경로계수 분석결과는 Figure 2를 통해 확인할 수 있다. 구조모형에서 설명되는 보안준수 태도와 통제감의 R^2값이 각각 0.674와 0.548로 나타나 선행변수인 보안 감수성, 조직 신뢰, 정보보안 업무 장애, 제재와의 관계를 나타내는 설명력이 크다고 볼 수 있다.

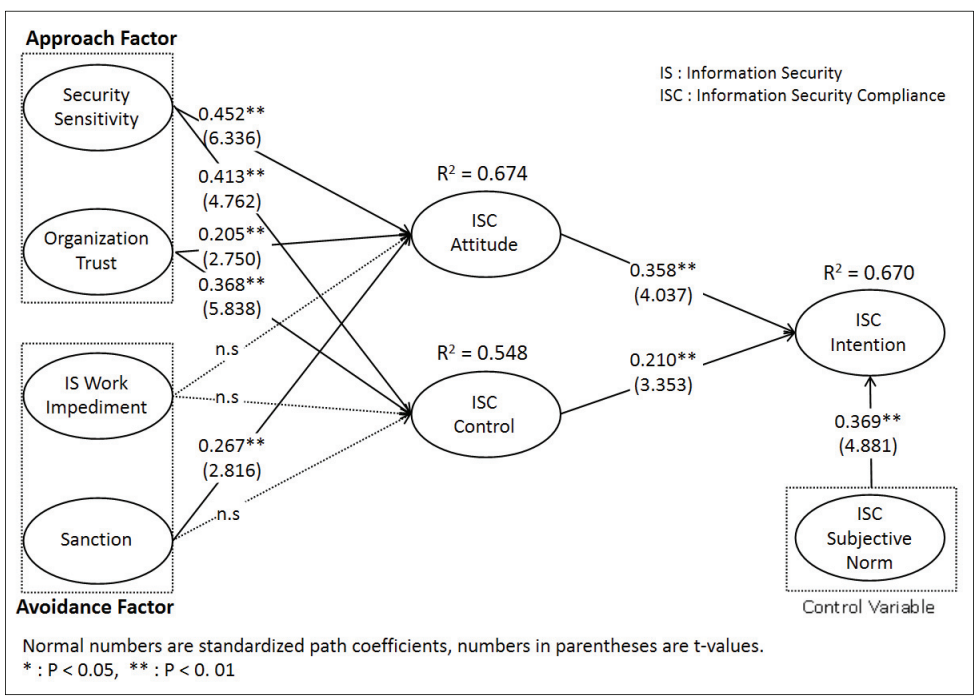
또한, 보안준수 태도와 통제감, 주관적 규범과 의도 간 관계에 대한 설명력을 나타내는 R^2값도 0.670으로 크게 나타났다. 본 연구의 가설은 부트스트랩 리샘플링 기법을 활용한 경로계수 분석을 통해 검증하였으며, 그 결과는 다음과 같다.

첫째, 정보보안 준수에 대한 접근 동기 측면의 요인인 보안 감수성과 조직 신뢰는 정보보안 준수 태도와 통제감에 긍정적인 영향을 미친다는 점을 확인하였다. 가설 검증 결과를 세부적으로 살펴보면 우선 보안 감수성과 정보보안 준수 태도의 관계를 설명하는 가설1a(H1a)는 통계적으로 유의한 영향이 있어 채택되었다(β=0.452, t=6.336, p=0.000). 이는 구성원의 보안 감수성이 높을 경우 정보보안 준수에 대해 긍정적인 태도를 보인다는 점을 의미한다. 다음으로 보안 감수성과 정보보안 준수 통제감 간의 관계를 분석한 가설1b(H1b)는 통계적으로 유의하여 채택되었으며(β=0.413, t=4.762, p=0.000), 이를 통해 보안 감수성이 높은 구성원은 정보보안 준수를 쉽게 해낼 수 있다는 믿음이 커진다는 점을 알 수 있다. 조직 신뢰가 정보보안 준수 태도에 미치는 영향을 확인한 가설1c(H1c)는 통계적으로 유의한 결과를 보여 채택되었으며(β=0.205, t=2.750, p=0.006), 구성원의 조직 신뢰가 정보보안 준수 태도에 긍정적인 영향을 미치는 것으로 나타났다. 마지막으로 조직 신뢰가 정보보안 준수 통제감에 미치는 영향을 확인한 가설1d(H1d)는 통계적으로 유의한 결과를 보였고(β=0.368, t=5.838, p=0.000), 이는 조직에 대한 신뢰가 구성원이 자신의 보안 준수 행동을 통제할 수 있다고 인식하는 데 도움을 줄 수 있다는 점을 의미한다.

둘째, 정보보안 준수와 관련된 회피 동기 측면의 요인과 정보보안 준수 태도 및 통제감 간의 관계를 분석한 결과 제재와 정보보안 준수 태도와의 관계를 설명하는 가설2c(H2c)만 채택되었고, 나머지 가설은 통계적으로 유의미한 결과를 보이지 않아 기각되었다. 이를 구체적으로 살펴보면, 우선 정보보안 업무 장애와 정보보안 준수 태도의 관계에 대해 분석한 가설2a(H2a, β=0.002, t=0.036, p=0.972)와 정보보안 준수 통제감과의 관계를 다룬 가설2b는 모두 통계적으로 유의한 결과가 나타나지 않아 기각되었다(H2b, β=0.035, t=0.637, p=0.524). 이는 군 구성원의 정보보안 업무 장애 인식이 정보보안 준수에 대한 태도와 통제감에 영향을 미치지 않는다는 점을 의미한다. 즉, 국가 안보 및 군사적 위협과 관련 있는 민감한 정보를 다루고 있어 업무의 효율보다는 중요 정보의 보호에 더 가치를 두는 군 장교 계층의 특수성이 반영된 결과라고 해석할 수 있을 것이다. 한편 제재가 정보보안 준수 태도에 영향을 미칠 것이라는 가설2c(H2c)는 통계적으로 유의하여 채택되었다(β=0.267, t=2.816 p=0.005). 이는 제재가 구성원의 정보보안 준수에 대한 긍정적 태도를 유도할 수 있다는 점을 시사한다. 마지막으로 제재와 정보보안 준수 통제감의 관계를 확인한 가설2d(H2d)는 통계적으로 유의하지 않아 기각되었고(β=0.047, t=0.614 p=0.539), 이는 제재가 군 구성원 스스로가 보안 규정이나 절차를 잘 수행하고 통제할 수 있다는 믿음에는 영향을 미치지 못한다는 점을 의미한다. 회피동기 성향일 경우 상대적으로 소극적인 학습전략을 택한다는 연구결과를 고려할 때(Higgins, 1998; as cited in Jin S. J. & Lee, J. S., 2018), 구성원이 제재를 회피하기 위한 목적으로 정보보안 업무를 수행할 경우 관련 규정 숙지 및 절차 숙달을 위한 노력이 적어지며, 이에 따라 보

안을 잘 해낼 수 있다는 믿음 수준이 낮아지기 때문에 유의미한 관계를 보이지 않은 것으로 판단된다.

셋째, 계획된 행동이론을 바탕으로 정보보안 준수 태도와 통제감이 정보보안 준수 의도에 미치는 영향에 관한 가설은 모두 채택되었다. 정보보안 준수 태도가 정보보안 준수 의도에 영향을 미친다는 가설3(H3)은 통계적으로 유의한 결과를 보였으며(β=0.358, t=4.037, p=0.000), 정보보안 준수 통제감과 준수 의도의 관계를 확인한 가설4(H4)에 대한 분석결과도 통계적으로 유의하였다(β=0.210, t=3.353 p=0.001). 환경적 요인으로서 통제변수로 고려한 정보보안 준수 주관적 규범은 준수 의도와 유의한 영향관계를 보였으며(β=0.369, t=4.881, p=0.000), 통제변수가 포함된 연구 모형에서도 정보보안 준수 태도와 통제감이 준수 의도에 유의한 영향을 미치고 있었다.



<Figure 2> Structural equation model analysis result

마지막으로 정보보안 준수 태도와 통제감의 매개효과에 대한 가설 분석결과는 Table 5를 통해 확인할 수 있다. VAF(Varianc account for)는 변수 간 관계에서 총효과에 대비한 간접효과의 크기를 나타내는 값인데, 0.2보다 작을 경우에는 매개 효과가 없는 것으로 판단하고, 0.2~0.8일 때는 부분매개, 0.8보다 큰 경우에는 완전매개 효과가 있다고 해석할 수 있다(Hair et al., 2014). 이를 바탕으로 매개효과를 검증해본 결과 정보보안 준수 태도는 보안 감수성, 조직 신뢰, 제재와 준수 의도 간의 관계에 대해 부분적인 매개효과를 나타냈으며, 정보보안 준수 통제감은 조직 신뢰와 준수 의도 간의 관계를 부분적으로 매개하는 것으로 확인하였다.

<Table 5> Mediation effect analysis result

Hypothesis	Path	Direct effect	Indirect effect(A)	Total effect(B)	VAF (A/B)	Result
5a	SS → ISCA → ISCI	0.568	0.162	0.730	0.222	Acceptance (partial mediation)
5b	OT → ISCA → ISCI	0.028	0.073	0.101	0.723	Acceptance (partial mediation)
5c	ISWI → ISCA → ISCI	0.080	0.001	0.081	0.012	Rejection
5d	SC → ISCA → ISCI	0.258	0.096	0.354	0.271	Acceptance (partial mediation)
6a	SS → ISCC→ ISCI	0.568	0.087	0.655	0.132	Rejection
6b	OT → ISCC → ISCI	0.028	0.077	0.105	0.733	Acceptance (partial mediation)
6c	ISWI → ISCC → ISCI	0.080	0.007	0.087	0.081	Rejection
6d	SC → ISCC → ISCI	0.258	0.010	0.268	0.038	Rejection

Note. SS (Security Sensitivity), OT (Organization Trust), ISWI (Information Security Work Impediment), SC (Sanction), ISCA (Information Security Compliance Attitude), ISCC (Information Security Compliance Control), ISCI (Information Security Compliance Intention)

V. 결론 및 논의점

5.1 연구결과 요약

본 연구의 목적은 군 조직에서 정보보안 계획 및 관리 업무를 수행하며, 군사비밀 및 민감한 자료를 다양하게 취급하는 군 장교 계층의 정보보안 준수 의도에 영향을 미치는 요인에 대해 분석하는 것이다. 이를 위해 계획된 행동이론을 바탕으로 하되, 다양한 선행연구를 통해 군 구성원의 정보보안 준수 태도 및 통제감에 영향을 미칠 것이라고 판단되는 변수들을 중심으로 연구 모형을 구성하였다. 이를 검증하기 위해 육군 장교를 대상으로 한 설문조사를 실시하였고, 조사결과를 바탕으로 연구가설을 검증하였다. 우선 정보보안 준수에 대한 접근동기 측면의 요인이라고 할 수 있는 보안 감수성과 조직 신뢰는 정보보안 준수 태도와 통제감에 긍정적인 영향을 미쳤다. 즉 보안 감수성을 갖추고 조직에 대한 신뢰가 있는 구성원은 높은 수준의 정보보안 준수 태도와 통제감을 보이고 있었다. 하지만 회피 차원의 변수로 고려한 정보보안 업무 장애와 제재와 정보보안 준수 태도 및 통제감과의 관계를 분석한 결과 제재는 정보보안 준수 태도에 긍정적인 영향을 미쳤으나, 나머지 가설은 통계적으로 유의한 결과를 보이지 않았다. 정보보안 업무 장애는 준수 태도와 통제감에 영향을 미치지 않는 것으로 나타났는데, 국가 안보와 직결되는 정보를 다루기 때문에 업무 효율보다는 정보보호에 더 중점을 두는 군 장교 계층의 특수성이 반영된 결과라고 할 수 있다. 한편 제재는

정보보안 준수 태도와는 긍정적인 관계를 보였으나, 통제감과의 관계는 확인되지 않았다. 이는 제재를 회피하기 위한 목적으로 정보보안 업무를 수행하는 구성원은 관련 규정 및 절차를 익히는데 소극적이고, 이에 따라 보안준수와 관련된 정책이나 절차를 통제할 수 있다는 믿음의 정도가 낮아지기 때문이라고 해석할 수 있다. 다음으로 계획된 행동이론에서 구성원의 개인적 요인이라고 할 수 있는 정보보안 준수 태도와 통제감은 정보보안 준수 의도에 긍정적인 영향을 미치며, 설명변수와 정보보안 준수 의도 간 관계를 부분적으로 매개한다는 점을 확인하였다. 이를 통해 다수의 선행연구에서 검증된 계획된 행동이론의 주요 변수가 군 조직의 정보보안 연구에도 적용될 수 있다는 점을 확인할 수 있었다.

5.2 연구의 시사점

본 연구의 결과는 다음과 같은 시사점을 갖는다. 첫째, 보안사고 발생의 주요 원인이 조직 구성원의 일탈과 부주의이며, 조직 내 인적 보안 분야가 취약하다는 점이 알려져 있음에도 불구하고 이와 관련된 연구는 상대적으로 적은 실정이다. 특히, 군 조직의 보안 관리에서 주요한 역할을 수행하는 장교 계층만을 대상으로 한 연구는 거의 없었다. 따라서 본 연구는 군 장교의 정보보안 준수 행동과 관련이 있는 요인을 접근 및 회피 동기 차원의 변수로 구분하여 실증적으로 분석했다는 점에서 의의가 있다.

둘째, 개인의 행동 의도 및 행동 예측과 관련된 연구에서 널리 활용되고 있는 계획된 행동이론을 중심으로 정보보안 준수 의도에 영향을 미치는 요인을 분석하였다. 특히 정보보안 준수 태도와 통제감이라는 개인적 요인을 중심으로 군 장교 계층의 정보보안 준수 의도에 영향을 미칠 수 있는 설명변수에 대해 세부적으로 확인할 수 있었다.

셋째, 군 구성원의 보안 준수 행동을 장려하기 위해 관리되어야 할 요인으로 보안 감수성이라는 개념을 제시하였다. 보안 감수성은 구성원이 보안을 준수해야 할 필요성을 인식하고 이를 준수하기 위해 요구되는 지식을 갖추고 있는지에 대해 종합적으로 확인할 수 있는 변수라고 할 수 있다. 본 연구는 이러한 보안 감수성이 군 장교의 정보보안 준수 태도 및 통제감에 긍정적인 영향을 미친다는 점을 실증적으로 확인하여 군 조직 내 보안 감수성 관리의 필요성을 제시했다는 점에서 의의가 있다.

넷째, 군 조직의 보안 수준 향상 및 군 조직 구성원, 특히 장교 계층의 보안 준수의도를 높이기 위해 실무적으로 집중하고 관리해야 할 분야를 제시해주고 있다. 우선 군 장교의 보안 감수성을 관리하기 위한 방안이 필요하다. 기존에 군에서는 성 관련 사고를 예방하기 위해 구성원의 성인지 감수성을 향상시키기 위한 교육 및 공모전 등을 시행해 왔으며, 이러한 활동이 성인지 감수성에 긍정적인 영향을 미친다는 분석결과도 제시되고 있다(Kim, Y. R., 2019; Jung, B. S., 2021). 이러한 연구결과에 근거하여 군에서 교육이나 공모전 등의 방법을 통해 군 장교의 보안 감수성을 높일 수 있다

면 보안 준수 의도 및 행동을 유도하여 부대의 보안 수준을 높일 수 있을 것이다. 또한 군 장교가 부대의 정보보안 정책에 대한 신뢰를 갖도록 월 1회 실시하는 사이버・보안 진단의 날 행사를 이용해 정보보안 활동 결과를 공개하거나 보안 관련 주요 변화사항을 소개하는 등의 주기적인 의사소통을 강화하고, 공정하고 일관성 있는 보안지침의 관리를 위한 노력이 필요하다. 마지막으로 보안 미준수에 대한 제재가 정보보안 준수 태도 및 의도에 영향을 미칠 수 있기 때문에 보안위반 발생 시 엄정한 신상필벌을 가하는 것은 보안 준수 의도 향상에 도움이 될 수 있다는 점을 시사하고 있다.

5.3 연구의 한계 및 향후 연구방향

이러한 시사점에도 불구하고 본 연구는 다음과 같은 한계점도 가지고 있다. 첫째, 본 연구는 장교가 군 정보보안의 관리책임자이며, 보안 관련 실무를 담당하는 주요 계층인 점을 고려하여 주요 분석대상으로 삼았다. 하지만 향후 연구는 지속적인 보안 수준의 유지를 위해서 관리책임자뿐만 아니라 모든 구성원이 보안을 준수하고 예방해야 한다는 점을 고려한 연구설계의 확대 적용이 필요하다. 예를 들어 관리책임자와 구성원의 역할 관계를 고려할 수 있는 팀 조직 수준의 변수(i.e, leadership: Yammarino, Mumford, Connelly, & Dionne, 2010)를 고려한 다수준 연구 접근이나 정보보안의 다층적 구조(multilevel information security architecture: Jin & Shen, 2012)를 고려한 연구모형 설계를 진행할 필요가 있다.

둘째, 본 연구에서는 정보보안 준수 태도와 통제감에 영향을 미칠 수 있는 변수로 보안 감수성, 조직 신뢰, 정보보안 업무 장애, 제재의 4가지 변수만을 제시하였다. 이는 선행연구 검토를 통해 군 조직의 보안환경을 고려하여 영향력이 있을 것올 판단되는 변수를 위주로 선정하였다. 하지만, 이외에도 조직 공정성, 정보보안 스트레스, 정보보안 정책 목표 등 정보보안 준수와 관련된 다양한 심리적 변수 등과 군 조직의 안전문화(Hu, S. H., 2020) 등의 환경적인 맥락을 고려한 연구가 추가된다면 군 구성원의 정보보안 준수에 대한 종합적인 분석이 가능할 것이다.

셋째, 본 연구에서는 자기보고 형식의 설문조사법을 통해 자료를 수집하였다. 자기보고식 측정방법은 응답자들이 실제 현상보다 긍정적 또는 바람직한 방향으로 응답하는 반응편향 문제가 발생할 수 있다(Lebek et al., 2013). 따라서 추후 연구에서는 보안 준수 태도나 의도에 영향을 미치는 요인에 대해서는 개인이 지각하는 바를 설문식으로 측정하되, 이에 따른 보안 준수 행동이나 조직의 보안 수준은 관리자가 평가하게 하는 등의 노력으로 반응 편향 문제를 줄이기 위해 노력할 필요가 있다.

넷째, 계획된 행동이론은 행동 의도가 행동에 미치는 영향까지 분석하고 있는데, 본 연구에서는 실제적인 정보보안 준수 행동을 측정하기가 쉽지 않다는 점을 고려하여 정보보안 행동 의도까지만 살펴보았다. 이는 기존의 정보보안 연구들에서도 나타난 문제점이기도 한데, 정보보안 준수 행동에

대한 분석을 포함한 후속 연구가 진행된다면 더욱 설득력 있는 연구가 될 수 있을 것이다.

다섯째, 본 연구는 육군의 영관 및 위관급 장교를 대상으로 분석하였다. 부대 및 부서장으로서 전반적인 보안업무를 관리하고, 군사기밀을 주로 취급하고 있는 장교라는 계급의 특성상 공군 및 해군(해병대)에서도 대체로 육군과 유사한 결과가 나타날 것으로 예상된다. 그럼에도 각 군별 근무지역이나 근무환경, 부여된 임무에 따라 정보보안에 대한 인식의 차이가 발생할 수 있으므로 본 연구결과를 타군에 적용할 때에는 각 군별 특성에 대해 심도있게 고려할 필요가 있다.

끝으로 최근 군에서 드론과 로봇, AI 등의 4차 산업혁명 기술의 적용을 확대하고 있고, MZ세대의 군 입대가 본격화되면서 군내 모바일이나 스마트 기기 사용이 활성화되고 있다. 특히, 우리 군 조직의 병사 비율의 70% 수준을 차지하는 20대 초반 인원(MZ세대)에 대한 안보인식 강화 측면에서 군 정보보안의 강화 측면에서 인공지능을 활용한 정신교육(Choi, E. S., 2021)의 역할과 효과성을 연구할 필요가 있다. 이런 환경변화를 고려하여 군 구성원이 겪을 수 있는 정보보안 관련 기술스트레스나 정보보안 정책에 대한 저항 등에 대한 연구가 추가로 진행된다면 기술 발전 수준을 고려한 보안정책의 적용이 가능해질 것이다.

Acknowledgements

We would like to thank Editage (www.editage.co.kr) for English language editing.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Reference

Agarwal, V. (2013). Investigating the Convergent Validity of Organizational Trust. *Journal of Communication Management, 17*(1), 24-39. https://doi.org/10.1108/13632541311300133

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-t

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013). Information Security Policy Compliance: An Empirical Study of Ethical Ideology. System Sciences (HICSS), 2013 46th *Hawaii International Conference on System Sciences*, 3018-3027. https://doi.org/10.1109/hicss.2013.272

Barclay, D. Higgins, C., & Thomson, R. (1995). The Partial Least Squares(PLS) Approach to Causal Modeling : Personal Computer Adoption and Use as an Illustration. *Technology Studies, 2*(2), 44-59. https://www.researchgate.net/publication/313137896

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research, 295*(2), 295-336. https://www.researchgate.net/publication/311766005

Choi, E. S. (2021). Military Spiritual Education According to Environmental Changes in the Advanced Military Culture: Focusing on the Characteristics of New Generation (MZ Generation). *The Korean Journal of Unification Affairs, 33*(1), 29-63. https://doi.org/10.46561/KUA.2021.33.1.02

Cornwell, J. F., Franks, B., & Higgins, E. T. (2014). Truth, control, and value motivations: the "what," "how," and "why" of approach and avoidance. *Frontiers in Systems Neuroscience, 8*, 1-15. https://doi.org/10.3389/fnsys.2014.00194

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security, 32*(1), 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Das, S., Kim, T. H. J., Dabbish, L. A., & Hong, J. I. (2014). The effect of social influence on security sensitivity. In 10th Symposium On Usable Privacy and Security, 143-157. https://www.usenix.org/sites/default/files/soups14_proceedings.pdf#page=150

Eom, J. H., & Kim, N. U. (2020). Measures to Prevent the Leakage of Military Internal Information through the Analysis of Military Secret Leakage Cases: Focusing on Insider Behaviors. *Journal of Convergence Security, 20*(1), 85-92. https://doi.org/10.33778/kcsa.2020.20.1.085

Fornell, C. & Larcker. D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research, 18*(3), 382-388. https://doi.org/10.2307/3150980

Gillespie, N. & Dietz, G. (2009). Trust repair after an organization-level failure. *The Academy of Management Review, 34*(1), 127-145. https://doi.org/10.5465/amr.2009.35713319

Hair J., J.F., Sarstedt, M., Ringle, C.M., & Hult, G.T. (2014). *A Primer on partial least squares structural equation modeling*. California: Sage publications.

Hair, J., W. Black, B. Babin, & R. E. Anderson. (2010). *Multivariate Data Analysis*. Englewood Cliffs, Nj: Prentice Hall.

Henseler, J., Hubona, G., & Ray, P. (2016). Using PLS Path Modeling in New Technology Research: Updated Guidelines. *Industrial Management & Data Systems, 116*(1). 2-20. https://doi.org/10.1108/IMDS-09-2015-0382

Herath, T. & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 54-165. https://doi.org/10.1016/j.dss.2009.02.005

Higgins, E. T. (1998). Advances in experimental social psychology. Vol. 30. Academic Press. https://www.elsevier.com/books/advances-in-experimental-social-psychology/zanna/978-0-12-015230-8

Hu, S. H. (2020). Analysis of the impact of military organization's safety culture on safety behavior: Focusing on the mediating effect of safety leadership. *Journal of Advances in Military Studies, 3*(2), 63-81. https://doi.org/10.37944/jams.v3i2.70

Hwang, I. H. & Hu, S. H. (2018). A Study on the Influence of Information Security Compliance Intention of Employee: Theory of Planned Behavior, Justice Theory, and Motivation Theory Applied. *Journal of Digital Convergence, 16*(3), 225-236. https://doi.org/10.14400/JDC.2018.16.3.225

Hwang, I. H. & Hu, S. H. (2021a). The Influence of Security Motivation and Organization Trust on Information Security Compliance: Focusing on Moderation Effects of Work Promotion Focus. *Journal of the Korea Society Industrial Information System, 26*(3), 23-39. https://doi.org/10.9723/jksiis.2021.26.3.023

Hwang, I. H. & Hu, S. H. (2021b). Influence of Work Impediment and Compliance Anxiety on

Information Security Compliance Intention: Analysis of Moderating Effect on Involvement and PO fit. *Journal of Korea Service Management Society, 22*(2), 1-27. https://doi.org/10.15706/jksms.2021.22.2.001

Hwang, I. H. & Kim, S. W. (2017). A Study on the Inhibitors and Task Coping of Information Security Related Work Stress of Employees in Finance Industry. *The e-Business Studies, 18*(3), 147-165. https://doi.org/10.20462/tebs.2017.06.18.3.147

Hwang, I. H. (2020). The Effect of Information Security Delivery Activities and Feedback on Work Impediment and Compliance Intention. *Journal of Digital Contents Society, 21*(9), 1653-1663. https://doi.org/10.9728/dcs.2020.21.1.1653

Hwang, I. H. (2021a). Analysis of the Effects of Information Security Sanction and Role Ambiguity on Compliance Intention: Focusing on Moderation Effects of Technical Support and Task Coping. *Journal of Digital Contents Society, 22*(2), 271-280. https://doi.org/10.9728/dcs.2021.22.2.271

Hwang, I. H. (2021b). The Effect on Psychological Empowerment on IS Compliance Intention: Focusing on the Moderating Effect of Trust and Justice. *Journal of Digital Contents Society, 22*(10), 1683-1694. https://doi.org/10.9728/dcs.2021.22.10.1683

Jeong, H. I. & Kim, S. J. (2018). Influence on Information Security Behavior of Members of Organizations: Based on Integration of Theory of Planned Behavior (TPB) and Theory of Protection Motivation (TPM). *Korean Security Journal, 56*, 145-164. https://doi.org/10.36623/kssa.2018.56.7

Jin, J., & Shen, M. (2012). Analysis of Security Models Based on Multilevel Security Policy. *2012 International Conference on Management of e-Commerce and e-Government*. https://doi.org/10.1109/icmecg.2012.72

Jin, S. J. & Lee, J. S. (2018). The effect of approach-avoidance motivation on academic self-regulation: The mediating effect of self-efficacy. *The Journal of Learner-Centered Curriculum and Instruction, 18*(7), 547-563. https://doi.org/10.22251/jlcci.2018.18.7.547

Jung, B. S. (2021). Mixed Method Study on the Effect of Gender Equality Education for Military Cadets. *The Journal of Learner-Centered Curriculum and Instruction, 21*(15), 459-473. https://doi.org/10.22251/jlcci.2021.21.15.459

Kim, B. R. & Seong, K. S., & Kim, B. S. (2020). Effect of Military Officer's Ethical Disposition and Perceived Work Environment on Organizational Security Policy Compliance. *Information Systems Review, 22*(3), 31-58. https://doi.org/10.14329/isr.2020.22.3.031

Kim, B. R. & Shin, J. H., & Kim, B. S. (2018). What Influences Soldier's Intention and Attitude on the Information Security Policy Compliance?: A Case Study of One Signal Brigade

Unit. *The Quarterly Journal of Defense Policy Studies, 34*(2), 7-46. https://doi.org/10.22883/jdps.2018.34.2.001

Kim, C. J. & Yoon, C. S. (2008). A Study on the Relationship between Justice Perception and Organizational Trust in Contingent Workers. *Journal of Industrial Economics and Business, 21*(2), 759-782. http://uci.kci.go.kr/resolution/result.do?res_cd=G704-001438.2008.21.2.004

Kim, D. H. & Kim, D. K. (2020). A Study on the Effect of the Internal Motivation on Security Behavior of Military Members: Focusing on the Theory of Planned Behavior Model. *Korean Journal of Public Safety and Criminal Justice, 29*(3), 25-52. https://doi.org/10.21181/kjpc.2020.29.3.25

Kim, H. G. (2008). Relationships between Supervisor Trust, Organizational Trust and Organizational Citizenship Behavior: The Mediational Role of Organizational Commitment. *Korean Journal of Public Administration, 46*(1), 177-209. UCI : G704-000826.2008.46.1.001

Kim, H. S. (2016). Leadership, Corporate Entrepreneurship, Organization Trust, and Support of the CEO on the Compliance of the Organizational Security Policy: Focus on Business Incubator Firm. *Korean Journal of Industrial Security, 6*(2), 111-141. https://www.earticle.net/Article/A296678

Kim, J. K. & MOU JIAN (2020). Meta-analysis of Information Security Policy Compliance Based on Theory of Planned Behavior. *Journal of Digital Convergence, 18*(11), 169-176. http://doi.org/10.14400/JDC.2020.18.11.169

Kim, S. H. & Song, Y. M. (2011). An Empirical Study on Motivational Factors Influencing Information Security Policy Compliance and Security Behavior of End-Users(Employees) in Organizations. *The e-Business Studies, 12*(3), 327-349. https://doi.org/10.15719/geba.12.3.201109.327

Kim, Y. R. (2019). The Influence of Female Sport Leaders Education on Gender Sensitivity. *Journal of Korean Physical Education Association for Girls and Women, 33*(4), 1-14. https://doi.org/10.16915/jkapesgw.2019.12.33.4.1

Kim. D. H. (2020). A Study on the Effect of Internal and External Dynamics of the Military Members on Security Behavior: Focusing on the Theory of Planned Behavior Model. *Journal of Defense and Security, 2*(1), 1-63. https://www.dssc.mil.kr/dssckr/173/subview.do

Koo, D. M. (2017). Research methodology for basic, control, and mediating effect analysis, Changmyeong.

Kwon, Y. S. & Nam, J. M. (2021). Effects of Franchise Headquarters Support Services and Franchise Entrepreneurship on Multi-unit franchising Intention: Focusing on Mediated

Effects of Theory of Reasoned Action Factors. *The Journal of Korean Career · Entrepreneurship & Business Association, 5*(3), 25-60. https://doi.org/10.48206/kceba.2021.5.3.25

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' information security awareness and behavior: A literature review. *In 2013 46th Hawaii International Conference on System Sciences*, 2978-2987.

Lee, S. H. & Lee, J. L. (2019). A Study on Private Security Officers' Willingness to Comply with Security Policies. *Korean Security Journal, 61*, 137-162. https://doi.org/10.36623/kssr.2019.61.6

Lee, T. B. & Kim, S. Y. (2021). The Relationship between Military Officer's Perception of Punishment and Defense Security Compliance Intention. *Journal of Defense and Security, 3*(2), 199-220. https://www.dssc.mil.kr/dssckr/173/subview.do

Lowry, P. B., Posey, C., Bennett, R. J., & Roberts, T. L. (2015). Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies : An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust. *Information Systems Journal, 25*(3), 193-273. https://doi.org/10.1111/isj.12063

Nachmias, D. (1985). Determinants of trust within the federal bureaucracy. In D. H. Rosenbloom (Ed.), *Public personnel policy: The politics of civil service*. Port Washington, NY: Associated Faculty Press.

Onwudiwe, I., J. Odo, & E. Onyeozili. (2005). Deterrence Theory. In: Bosworth, M. (Ed.), Encyclopedia of Prisons & Correctional Facilities. California: Sage Publications.

Park, E. C. & Jeon. K. S. (2021). A Study on the Effects of Influencing Factors in the Security Environment of Military Organizational Members on Information Security Stress and Security Compliance Behavior Intention. *Journal of convergence security, 21*(3), 93-104. https://doi.org/10.33778/kcsa.2021.21.3.093

Park, J. K. & Oh, Y. K. (2016). A Study on the Effect of Military Security Performance on the Psychological military strength (As for Mediated Effect of Military Organizational Characteristics & Culture). *Journal of National Defense Studies, 59*(3), 75-106. http://doi.org/10.23011/jnds.2016.59.3.004

Vance, A., & Siponen, M. T. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing, 24*(1), 21-41. https://doi.org/10.4018/joeuc.2012010102

Warkentin M. & Willison R. (2009). Behavioral and Policy Issues in Information Systems

Security: The Insider Threat. *European Journal of Information Systems, 18*, 101-105. https://doi.org/10.1057/ejis.2009.12

Yammarino, F. J., Mumford, M. D., Connelly, M. S., & Dionne, S. D. (2010). Leadership and team dynamics for dangerous military contexts. *Military Psychology, 22*(sup1), S15-S41. https://doi.org/10.1080/08995601003644221

원 고 접 수 일 2022년 03월 18일
원 고 수 정 일 2022년 04월 19일
게 재 확 정 일 2022년 04월 25일

<부록 1> 변수의 조작적 정의 및 측정 문항

변수	정의	측정 문항
보안 감수성	보안 위협을 예방하기 위한 보안정책 및 기술에 대해 인식하고 행동하고자 하는 개인의 민감성 정도	. 나는 보안 문제가 발생 가능한 상황을 구분할 수 있다 . 나는 부대의 보안 규정 및 지시에 대해 잘 알고 있다 . 나는 최근 부대에서 발생하는 보안사고들을 알고 있다 . 나는 부대의 보안정책이 보안사고 예방에 중요하다고 생각한다 . 나는 누가 시키지 않더라도 부대의 보안정책에 따라 업무를 수행할 것이다 . 부대 보안정책을 준수하는 것은 나와 부대에 도움이 된다 . 나는 인트라넷 PC 보호 프로그램을 사용할 지식이 있다 . 나는 비밀문서 열람, 갱신 등 절차를 잘 알고 실시한다
조직 신뢰	조직에 대하여 가지는 긍정적 믿음의 수준	. 우리 부대는 부대원들을 공정하게 대우한다 . 우리 부대는 약속을 지키기 위해 노력을 한다 . 나는 우리 부대가 의사결정을 할 때, 부대원들의 의견을 고려한다고 믿는다. . 우리 부대는 개인이 하는 일을 성취하도록 도와준다
정보보안 업무장애	조직의 정보보안 정책 및 기술을 적용하는 과정에서 업무에 장애가 있다고 느끼는 정도	. 보안정책을 준수하면 업무수행에 지장을 미친다 . 보안정책을 준수하면 지휘관, 동료 등에 대한 응답이 느려진다 . 보안정책을 준수하는 것이 업무생산성을 저해한다 . 보안정책을 준수하면 업무효율이 저하된다
제재	정보보안을 준수하지 않았을 때 발생하는 물리적·사회적 처벌의 정도	. 내가 부대의 보안정책을 위반하면 반드시 처벌받을 것이다 . 상관이 나의 위반 사실을 안다면 공식적으로 처벌할 것이다 . 상관이나 동료가 보안정책을 위반하면 반드시 처벌될 것이다 . 내가 보안정책을 위반하면 동료들에게 신뢰를 잃을 것이다 . 내가 보안정책을 위반하면 상관에게 신뢰를 잃을 것이다 . 내가 보안정책을 위반하면 진급에 부정적 영향을 받을 것이다
정보보안 준수 태도	정보보안 준수를 긍정적으로 인식하는 정도	. 부대 보안정책을 준수하는 것은 당연하다 . 부대 보안정책을 준수하는 것은 바람직하다 . 부대 보안정책을 준수하는 것은 가치있는 일이다 . 부대 보안정책을 준수하는 것은 현명한 일이다 . 부대 보안정책을 준수하는 것은 긍정적인 일이다
정보보안 준수 통제감	보안정책 및 절차의 준수를 잘 수행하고 통제할 수 있다고 믿는 정도	. 나는 부대의 보안정책을 준수하는 것이 쉽다 . 나는 부대의 보안정책 준수와 관련된 지식이 있다 . 나는 보안정책을 준수할 적절한 교육을 받았고 능력이 있다
정보보안 준수 주관적규범	정보보안 준수에 대해 느끼는 사회접 압력의 정도	. 지휘관은 내가 부대의 보안정책을 준수해야 한다고 생각한다 . 상관은 내가 부대의 보안 관련 규정을 따라야 한다고 생각한다 . 부대의 보안부서에는 내가 보안정책을 준수하도록 요구한다 . 동료들은 내가 부대의 보안 규정을 준수하도록 요구한다
정보보안 준수 의도	조직의 정보보안 정책을 준수하고자 하는 자발적 의지의 정도	. 나는 부대의 보안정책을 준수할 의향이 있다 . 나는 정보보호를 위해 보안정책을 계속해서 준수할 것이다 . 나는 보안 규정에 명시되어 있는 책임을 준수할 의향이 있다

IDAP 광운대학교 방위사업연구소 INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2022, Vol. 5, No. 1, 5-33.

https://doi.org/10.37944/jams.v5i1.138

군 장교의 정보보안 준수 의도에 영향을 미치는 요인

김상영* · 이태복**

국문초록

본 연구의 목적은 군 장교의 정보보안 준수 의도에 영향을 미치는 요인을 분석하는 것이다. 이를 위해 계획된 행동이론의 주요 변수인 정보보안 준수 태도와 통제감, 선행연구 분석을 통해 군 구성원의 정보보안 준수에 영향을 미칠 것으로 판단되는 보안 감수성, 조직 신뢰, 정보보안 업무 장애, 제재의 네 가지 요인을 중심으로 연구모형을 구성하였다. 연구모형은 육군 장교를 대상으로 실시한 설문조사를 통해 분석하였고 그 결과는 다음과 같다. 첫째, 보안 감수성과 조직 신뢰는 정보보안 준수 태도와 통제감에 긍정적인 영향을 미쳤다. 둘째, 정보보안 업무 장애는 준수 태도 및 통제감과 유의한 관계를 보이지 않는 것으로 나타났다. 셋째, 제재는 정보보안 준수 태도에는 긍정적인 영향을 미쳤으나, 통제감에는 영향을 미치지 않는 것으로 확인되었다. 넷째, 정보보안 준수 태도와 통제감은 정보보안 준수 의도에 영향을 미치는 것으로 확인되었으며 이는 다수의 선행연구 결과를 재확인한 것이다. 본 연구는 군 조직의 정보보안 분야에서 주요한 역할을 수행하는 장교 계층의 정보보안 준수 의도에 영향을 미치는 요인을 확인하고, 이를 관리해야 할 필요성을 제기함으로써 군 조직의 정보보안 수준을 높일 수 있는 방안을 제시했다는 측면에서 의의가 있다.

주제어 : 군 장교의 정보보안, 정보보안 준수 통제감, 보안 감수성, 조직 신뢰, 제재

* (제1저자) 3군단 직할부대, 중대장, tkddud829@naver.com, https://orcid.org/0000-0001-5313-0114

** (교신저자) 국방대학교 국방관리학과 박사과정, taebok88@gmail.com, https://orcid.org/0000-0002-5310-4490