ISSN 1229-1889(Print)
ISSN 2287-9005(Online)
J Korean Soc Qual Manag Vol. 53, No.1: 75-91, March 2025
https://dx.doi.org/10.7469/JKSQM.2025.53.1.75

국방 지능형 사이버위협 대응시스템의 수용의도에 영향을 미치는 요인에 관한 연구: 인공지능 기술특성을 중심으로

정성미* · 신성제** · 최정일***†

* 숭실대학교 대학원 IT정책경영학과
** 숭실대학교 대학원 경영학과
*** 숭실대학교 경영학부

A Study on the Fators Affecting the Intention to Accept Defense Intelligent Cyber Threat Response System: Focused on AI Technology Characteristics

Jung, Sung Mi* · Shin, Seong Je** · Choi, Jeongil***†

* Department of IT Policy and Management, Graduate School of Soongsil University
** Department of Business Administration, Graduate School of Soongsil University
*** School of Business Administration, Soongsil University, Corresponding Author

ABSTRACT

Purpose: The purpose of this study is to examine the factors affecting the intention to accept Defense Intelligent Cyber Threat Response System based on AI Technology Characteristics from the user's point of view.

Methods: The study conducted a survey of experienced people targeting defense cyber personnel performing national defense cyber operations, and valid 357 data were analyzed by SPSS (ver 22.0) and R (ver 4.1.0) program packages.

Results: As a result of the empirical analysis, it was found that among the AI technological characteristics of the Defense Intelligent Cyber Threat Response System, speed, expertise, and reliability, in that order, had an impact on performance expectancy. In terms of effort expectancy, reliability, expertise, and accuracy were found to be the influencing factors. Additionally, social influence and performance expectancy were found to have a positive effect on the intention to adopt the Defense Intelligent Cyber Threat Response System.

Conclusion: This study is significant in that it structurally analyzes the factors affecting system adoption in the defense environment from a user perspective, thereby laying the foundation for the practical utilization and dissemination of the technology. Beyond merely improving technological performance, it is expected to

● Received 27 February 2025, 1st revised 5 March 2025, accepted 7 March 2025
† Corresponding Author(jichoi@ssu.ac.kr)
ⓒ 2025, The Korean Society for Quality Management
This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0) which permits unrestricted non-Commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

provide strategies for the effective adoption and utilization of the Defense Intelligent Cyber Threat Response System within actual defense organizations.

Key Words: AI Technology Characteristics, Cyber Threats, Defense Cyber Organization, Defense Cyber Threat Response System, UTAUT

1. 서 론

현대 국방 환경은 빠르게 발전하는 정보통신기술(ICT)과 함께 새로운 도전에 직면하고 있다. 특히, 사이버 공간은 기존의 물리적 전장과는 다른 특성을 가지며, 국가 안보와 밀접한 핵심 영역으로 부각되고 있다. 4차 산업혁명의 영향으로 인공지능, 클라우드 컴퓨팅, 빅데이터, 블록체인 등 첨단 기술이 국방 분야에 적극 도입되면서, 디지털 기술의 확산이 가속화되고 그 중요성 또한 커지고 있다(Kim et al., 2024). 이러한 변화는 국방 ICT 기술의 발전을 촉진하는 동시에, 사이버위협을 더욱 지능적이고 정교한 형태로 변화시키고 있다.

사이버위협은 단순한 해킹이나 정보 유출을 넘어 지능형 지속 공격(Advanced Persistent Threat, APT), 랜섬웨어, 인공지능을 활용한 공격 등 점점 더 고도화된 양상으로 진화하고 있다. 이러한 위협은 정교하고 지속적인 방식으로 이루어지며, 기존의 단순한 기술적 방어 체계로는 탐지하거나 차단하기가 어려워지고 있다(Kim, 2024). 더 나아가, 사이버 공간에서 발생하는 위협은 물리적 전장과는 다른 비대칭적인 특성을 가지며, 전통적인 군사 방어 방식으로는 대응하기 힘든 새로운 전장으로 부상하고 있다. 특히, 敵의 정교한 사이버 전략은 우리의 사이버 자산과 국방정보체계를 직접적으로 위협하고 있어, 이를 안정적이고 체계적으로 보호하기 위해 더욱 발전된 대응시스템과 전략적 사고를 요구하고 있다(Song, 2023).

국방 사이버조직은 이러한 위협에 대응하기 위해 기술적 방어 역량을 지속적으로 강화하고 있지만, 사이버위협의 복잡성과 공격의 범위가 확장됨에 따라 단일 조직의 역량만으로는 대응이 점점 더 어려운 현실에 직면하고 있다. 기존의 사이버위협 대응시스템은 주로 알려진 위협 패턴을 기반으로 설계되어, 신종 위협이나 변형된 공격에 대해 즉각적인 탐지와 방어를 수행하는 데 한계가 있다. 따라서 기존 시스템의 한계를 극복하고, 더 효과적이고 체계적인 사이버위협 대응시스템을 구축하는 것은 국가 안보와 군사작전의 성공을 위해 필수적이다.

사이버 공격이 점점 더 정교해짐에 따라 글로벌 보안 기업들은 최신 기술을 도입하여 사이버 보안 시스템을 강화하고 방어 역량을 지속적으로 향상시키고 있다. 그러나 국방 분야에서는 보안의 중요성과 안정적인 서비스 제공이 필수적이므로, 새로운 기술을 즉각적으로 적용하는 데 한계가 있다.

국방분야에서 미래 전장을 주도할 인공지능 기술은 지휘소 AI참모, 무인 자율 시스템, 표적 이미지 분석, 빅데이터 활용 2차전지 품질 분류(Huh et al., 2023) 등 일부 실 작전 현장에서 적극적으로 도입하여 활용하고 있다. 그러나 국방 사이버위협 대응을 위한 인공지능 기술은 여전히 사이버작전 현장에서의 실질적 적용보다는 사이버위협 정보 공유, 연구개발, 보안 전략 수립 등 기술적·정책적 연구에 초점이 맞춰져 있으며, 효과적인 사이버위협 대응을 위해 기술적 특성을 반영한 시스템의 수용 과정과 실효성을 검증하는 실증적 연구는 부족한 실정이다.

이에 본 연구에서는 사용자 관점에서 인공지능 기술이 적용된 시스템의 수용에 영향을 미치는 요인을 분석하기 위해 기존 선행연구를 체계적으로 검토하고, 기술적 특성을 구성하는 주요 요인을 도출하였다. 또한, 국방 사이버작전 임무를 수행하는 군인과 군무원을 대상으로 이러한 인공지능 기술특성이 시스템 수용의도에 미치는 영향을 실증적으로 분석하여 국방 지능형 사이버위협 대응시스템의 성공적인 도입과 활성화를 위한 실무적 시사점을 도출했다는 점에서 기존 연구와 차이가 있다. 이를 수행하기 위해 통합기술수용모델(UTAUT)의 선행연구를 검토하여 연구모델을 설계하였다.

2. 이론적 배경 및 선행연구

2.1 사이버위협

ICT 분야에서 '위협(threat)'은 한국정보통신기술협회(TTA) 정보통신 용어 사전에 따라 자산의 손실을 발생하게 하는 원인이나 행위, 또는 보안에 해를 미치는 행동이나 사건으로 정의된다. 이를 바탕으로, 사이버 공간에서 조직의 자산에 손실을 끼칠 수 있는 잠재적 위협을 사이버위협으로 정의할 수 있다. 사이버위협은 데이터 유출 및 위·변조, 시스템 파괴, 서비스 거부 공격(DoS)과 같은 다양한 사이버 공격 유형으로 나타나며, 이는 조직과 개인의 정보 자산을 심각하게 위협한다(Kim et al., 2017).

사이버위협은 정보통신기술(ICT)의 발전에 따라 양적으로 증가하고 질적으로 고도화되고 있다. 과거의 사이버 공격은 주로 금전적 이익이나 공격자 개인의 만족을 목적으로 한 비교적 단순한 형태의 공격이 주를 이루었다. 이러한 공격은 불특정 다수를 대상으로 수행되며 비교적 탐지와 방어가 용이했다. 그러나 최근 사이버위협은 특정 목표를 정밀하게 설정하고, 복합적이고 고도화된 기술을 사용하여 탐지와 방어를 어렵게 만든다. 특히 APT 공격은 체계적이고 조직적으로 수행되는 고도화된 공격을 말한다. 이 공격은 단순한 데이터 유출을 넘어 정치적·경제적 가치가 높은 조직의 목표 시스템에 장기적으로 침투하여 민감한 정보를 탈취하거나 시스템을 교란시키는 것을 목적으로 한다. 국방 분야에서도 APT 공격에 의해 군 내부망 해킹 사건과 같은 사이버 피해 사례가 증가하면서 국가 안보와 조직의 정보 자산에 심각한 위협으로 인식되고 있다.

2.2 국방 사이버 조직

2009년 7.7 DDoS 공격이 북한의 소행으로 잠정 결론이 내려지면서 국방부는 사이버전에 대응하기 위한 조직의 신설과 강화를 본격적으로 시작했다(Eom, 2013). 현재 국방부의 사이버작전 조직은 합참의 예하 부대인 사이버작전사령부를 중심으로, 국군지휘통신사령부와 작전사급 부대들이 각각 작전통제, 지휘감독, 작전지휘 역할을 맡아 사이버전 임무를 총괄·지휘하고 있다. 특히 사이버작전사령부는 국방 사이버 공간에서의 사이버작전 수행과 이를 지원하는 업무를 총괄하기 위해 2010년 1월 '사이버사령부'로 창설되었다. 초기에는 국방정보본부 예하 사령부로 시작되었으나 2011년 9월 국방개혁에 따라 국방부 직속 사령부로 배속 전환 및 증편되었다. 이후 2018년 8월에는 조직과 기능을 전면 개편하며 '사이버작전사령부'로 명칭을 변경하고 그 역할과 기능을 더욱 강화했다(Shin, 2020). 사이버작전사령부는 전·평시 사이버 작전계획을 수립하고 시행하며, 사이버교리 및 전력발전업무, 평시 사이버위협 대응작전, 전시 합동사이버작전 수행, 전문인력 육성과 기술 개발 등 다양한 임무를 수행하고 있다. 각 군 본부에서도 사이버작전 관련 조직이 체계적으로 구성되어 있다. 육군본부와 예하 야전군 내에는 각급 제대별로 정보보호 조직이 마련되어 있으며, 제대의 규모와 성격에 따라 서로 다른 임무를 수행한다. 육군본부는 사이버작전 관련 합참의 지도·감독을 받으며 작전부대의 사이버작전을 지원한다. 육군본부 정보화기획참모부와 사이버작전센터는 침해사고 예방과 대응 및 복구, 긴급대응반 통제, 자원체계 보호정책 수립, 정보보호기술에 관한 업무, 국방정보시스템의 취약점 분석 및 평가, 정보보호책임자 및 개인 정보관리 책임관을 지정하여 운영한다. 각 야전군사령부는 지휘통신참모부 사이버방호과에서 사이버작전을 계획하고 예하부대를 조정·통제하며, 사이버작전에 대한 제반사항을 협조하고 지원한다. 야전군사령부 예하 군단 및 사·여단은 각각 정보체계보호, 침해사고 발생 시 조치 및 복구, 전장 및 자원 관리 체계 운용, 취약점 점검 및 보완, 시스템 운영자 교육 등 사이버작전을 수행하기 위한 사이버방호실을 운영한다.

2.3 국방 지능형 사이버위협 대응시스템

국방 사이버위협 대응시스템은 사이버위협이 점점 정교해짐에 따라 보다 종합적인 시각에서 보안 위협을 식별하고 효과적으로 대응할 수 있는 통합 관리 체계의 필요성이 강조되면서 발전해왔다. 초기에는 방화벽(Firewall), 침입방지 시스템(IPS), 위협관리체계(TMS)등 개별적인 보안 솔루션을 기반으로 운영되었으나, 점차 정보보호체계의 핵심 기능을 통합하고 대응 역량을 강화한 통합 보안 관리 시스템(ESM)으로 발전하였다. 또한, 다양한 정보보호 시스템에서 발생하는 로그 데이터를 수집하고 이상 행위를 분석하여 보안 위협을 식별하는 보안 정보 이벤트 관리 시스템(SIEM)으로 진화하였다. SIEM은 빅데이터 기술을 이용하여 대용량 데이터를 분석하고 있으며, 이를 통해 로그 데이터로부터 유의미한 보안 위협들을 찾아내고 있다(Jeon, 2019).

사이버 공격이 점차 지능화·고도화됨에 따라, 기존 국방 보안 솔루션만으로는 효과적인 대응에 한계가 드러나고 있다. 이를 개선하기 위하여 국방 지능형 사이버위협 대응시스템은 기존 사이버 보안 시스템에서 발전된 개념으로, 다양한 형태의 사이버 공격과 위협을 실시간으로 탐지하고 분석 및 대응하는 통합 사이버위협 대응시스템이다. 이 시스템은 통합 위협 관리 시스템(UTM), 네트워크 접근 통제 시스템(NAC), 침입 방지 시스템(IPS) 등과 같은 국방 정보보호체계의 주요 기능을 통합할 뿐만 아니라, 이벤트에 대한 상관관계를 분석하고 보안 위협에 자동화된 대응 및 조치 등의 기능을 통해 보다 정교하고 신속한 사이버위협 대응을 가능하게 한다. 이를 통해 국방 분야의 사이버작전 환경에서 실시간 위협 대응 역량을 강화하고, 지속적으로 변화하는 보안 위협에 대한 선제적 방어가 가능하다.

2.4 인공지능 기술특성

인공지능 기술이 빠르게 발전함에 따라 다양한 분야에서 인공지능 시스템이 활용되고 있다. 대표적인 응용 사례로는 자율주행 차량(AV, Autonomous Vehicles), 컴퓨터 비전, 음성 인식, 인공지능 기반 의료 전문가 시스템 등이 있으며, 이러한 시스템이 대규모로 실전에 도입되기 전에 신뢰성과 안전성을 평가하는 것이 필수적이다(Jie Min et al., 2022). 국방 인공지능은 민간분야에 적용된 인공지능 기술을 단순 적용하는 것이 아니라 국방분야가 가진 혹독한 운용환경, 비정형화된 데이터 등 고유의 특성을 고려하여 설계된 특수한 인공지능을 의미한다. 따라서, 인공지능 기술을 국방환경에 효과적으로 구현하기 위해서는 국방분야의 특수성이 반영되어 일반적인 인공지능 기술보다 신뢰성 높은 데이터의 수집과 대용량 데이터의 정확한 분석 및 활용 기술이 필수적이다(Moon et al., 2020). 인공지능 기술의 특성을 도출하기 위해 인공지능 기술의 주요 키워드들을 KJ법을 활용하여 산업계와 학계의 전문가들과 논의한 결과, 인공지능 서비스의 주요 특성은 그룹으로 분류되었으며 이는 개인맞춤화, 전문성, 편의성, 다양성, 시공간성, 신뢰성, 실시간성으로 도출하였다(Baek et al., 2019). 또한 Kim, Y. (2022)는 인공지능을 활용한 신약 개발 플랫폼 특성 변수를 연구하여 전문성, 풍부성, 정확성을 분석하였고, Choi, J. W. (2021)은 인공지능 스마트양식 시스템 연구에서 신뢰성, 반응성, 전문성, 가용성, 보안성을 고려하여 사용자의 수용의도를 분석하였으며, Jang(2022)은 정부의 인공지능 기반 보안관제 시스템 도입에 영향을 미치는 요인을 실증적으로 분석하며 신뢰성, 가용성, 전문성을 주요 시스템 특성으로 도출하였다(Jang, 2022). 이러한 연구들은 인공지능 기술이 다양한 분야에서 성공적으로 도입되기 위해 신뢰성과 전문성, 정확성, 신속성 등이 중요한 요소임을 시사한다.

2.5 통합기술수용모형(UTAUT)

기술수용모델은 Ajzen & Fishbein(1975)의 합리적 행동이론(Theory of Reasoned Action, TRA)의 심리학 이론

에 근거한 신념, 태도, 행동 개념을 적용한 것이다(Fishbein & Ajzen, 1975). 기술수용이론은 초기에는 사회심리학적 관점에서 개인의 행동 의도와 실제 행동을 연구하는 데서 출발하였는데, 이후 IT 정보기술을 비롯한 신기술에 대한 개인 및 조직의 기술수용을 연구하는 방향으로 확장되면서, 다양한 분야에서 활용되며 발전해 왔다. 기술수용이론 중 TAM은 그동안 다양한 연구에서 새로운 기술수용을 설명하는 데 널리 활용되었으며, 현재까지 검증된 연구모형으로 발전해왔다. 하지만 신기술 수용을 설명하는 데에는 한계가 있으며, 정보기술의 다변화된 환경을 충분히 반영하지 못하는 제한점이 있다. 이에 따라, Venkatesh et al.(2003)은 1980년대 이후 급속히 확산된 첨단 기술이 조직과 개인의 기술수용에 미치는 영향을 분석하기 위해, 8개의 정보시스템 모델을 비교 분석하는 실증 연구를 진행하였다. 그 결과, 행동의도에 영향을 미치는 주요 요인으로 성과기대와 노력기대, 사회적영향을 도출하였으며, 사용행위에 영향을 미치는 요인으로는 촉진조건을 제시하였다. 또한, 성별, 나이, 경험, 자발성을 조절변수로 포함하여 통합기술수용이론(UTAUT)을 <Figure 1>과 같이 제안하였다. UTAUT 모델은 합리적 행동이론(Theory of Reasoned Action: TRA), 기술수용모형(Technology Acceptance Model: TAM), 계획된 행동이론(Theory of Planned Behavior: TPB), PC활용모형(Model of PC Utilization: MPCU), 혁신확산이론(Innovation Diffusion Theory: IDT), 동기모형(Motivational Model: MM), TAM-TPB 통합모형(Combined TAM-TPB : C-TAM-TPB), 사회인지이론(Social Cognitive Theory: SCT) 정보기술에 관련된 8개의 이론을 토대로 그 구성 개념을 분석하여 모형을 구성하였다(Venkatesh et al., 2003). UTAUT는 최신 정보기술의 수용의도를 검증하는 데 유용한 모델로 평가되며, 신기술을 도입하고 활용하는 과정에서 발생하는 다양한 요인을 고려할 수 있어 여러 연구에서 널리 활용되고 있다(Lee, 2018). 특히, 첨단 기술을 조직이나 개인이 효과적으로 수용하고 실무에 적용하는 과정에서 영향을 미치는 요소들을 분석하는 데 유용한 이론적 모델을 제공한다.

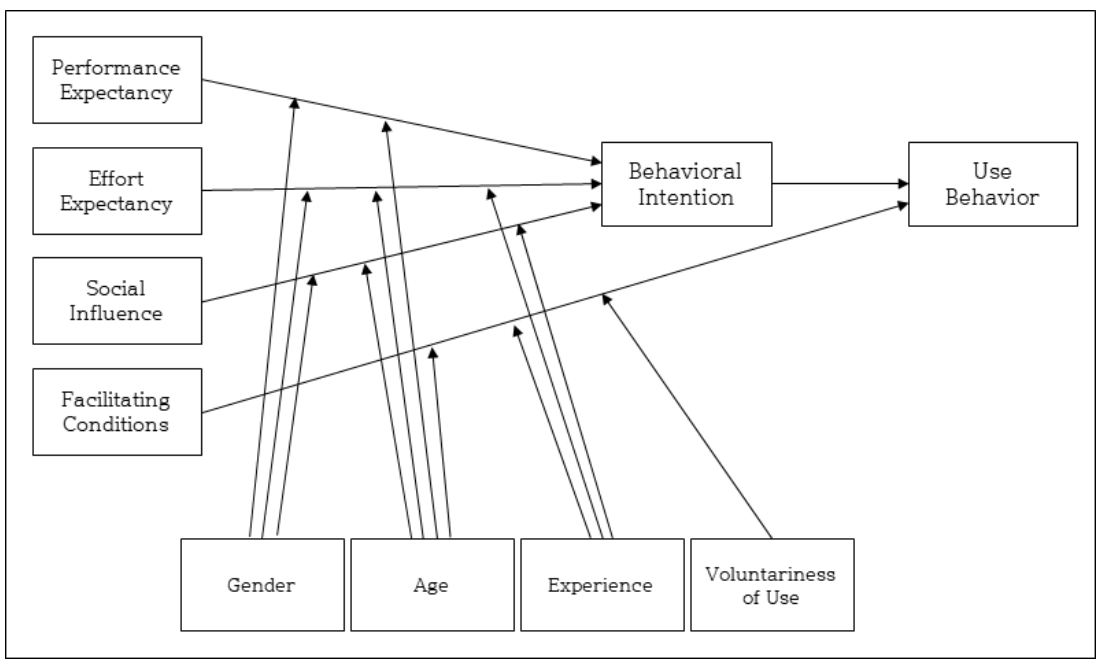

Figure 1. Unified Theory of Acceptance and Use of Technology Model

3. 연구모형 및 가설

3.1 연구모형

본 연구는 정보기술 수용의도와 관련된 선행연구를 바탕으로, 국방 지능형 사이버위협 대응시스템의 인공지능 기술특성에 대한 수용의도를 분석하는 것을 목표로 한다. 국방 정보체계 시스템을 비롯하여 공공서비스, 통신, 금융 등 다양한 분야에서 신기술이 활용되고 있으며, 이러한 분야에서 UTAUT 모형의 타당성이 실증적으로 검증되었다. 기존 기술수용모델(TAM)의 설명력이 약 40% 수준인 반면, UTAUT는 다양한 예측 변수를 포함함으로써 모델의 설명력을 약 70%까지 향상시킨 것으로 보고되었다(Venkatesh et al., 2003). 따라서, 최신 정보기술 트렌드를 보다 효과적으로 반영할 수 있는 UTAUT가 본 연구의 분석에 적합하다고 판단하였으며, 이를 기반으로 연구모형을 설계하였다.

UTAUT의 성능기대와 노력기대는 TAM의 인지된 유용성과 인지된 용이성과 비슷한 개념으로 보았다(Lee, 2016). 인공지능 기술특성의 선행연구를 참고하여 본 연구목적에 적합한 지능형 사이버위협 대응시스템의 인공지능 기술특성인 신뢰성, 전문성, 정확성, 신속성의 4개의 독립변수를 도출하였고 UTAUT의 성과기대와 노력기대, 사회적영향이 수용의도에 영향을 주는 것으로 변수를 구성하였다. 또한 국방 사이버 인력의 개인적 특성이 국방 지능형 사이버위협 대응시스템 수용의도에 미치는 차이를 분석하기 위해 성별, 나이, 계급, 근속년수, 복무제대를 인구통계학적 통제변수로 설정하였다, 이러한 논의를 바탕으로 국방 지능형 사이버위협 대응시스템의 수용의도에 영향을 미치는 요인을 파악하고자 <Figure 2>와 같이 연구모형을 설계하였다.

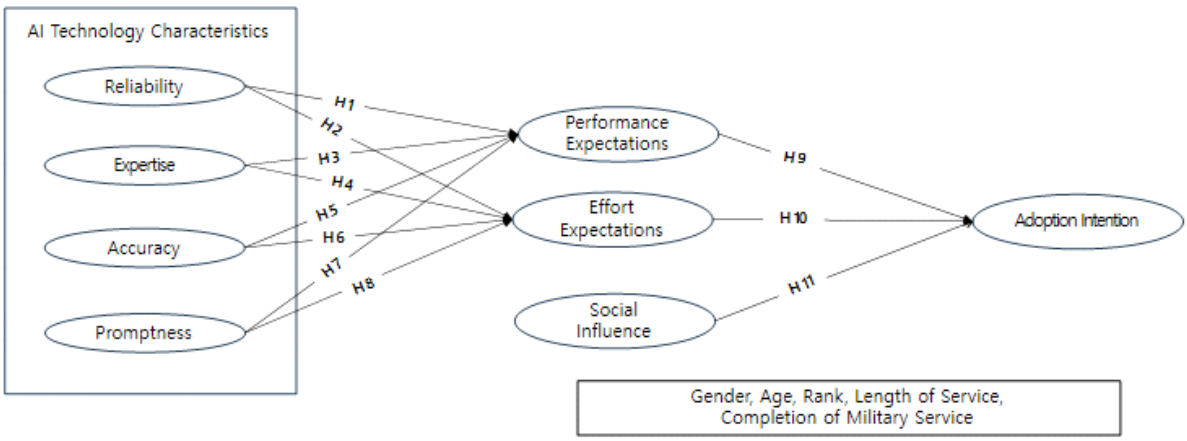

Figure 2. Research Model

3.2 연구가설 설정

3.2.1 국방 지능형 사이버위협 대응시스템의 인공지능 기술특성에 대한 가설

혁신 기술인 인공지능 도입에서 신뢰(Trust)는 사용자의 기술수용과 행동에 결정적인 영향을 미치는 핵심 요소로

작용한다. 혁신 기술은 본질적으로 불확실성과 위험을 동반하기 때문에, 사용자는 신뢰를 기반으로 해당 기술을 도입할지 여부를 판단한다. 신뢰는 불확실성을 완화하고, 사용자가 기술을 안전하고 유용하다고 인식하도록 함으로써 기술 도입에 긍정적인 영향을 미친다. 특히, 인공지능과 같은 복잡한 기술은 신뢰가 확보되지 않으면 사용자의 채택이 어려워지고, 이는 기술 도입의 성공을 저해할 가능성이 크다(Kim, 2024). Chichilnisky(1999)는 사회를 유지하는 윤활유로 신뢰를 비유였으며, 신뢰가 거래 비용을 절감하고 경제적 가치를 증대시킬 뿐만 아니라, 경제 활동과 기술 수용에서도 핵심적인 역할을 한다고 강조하였다. 국방 지능형 사이버위협 대응시스템은 사이버 보안 업무의 자동화 및 통합을 목표로 하며, 국방 정보보호체계에서 수집된 대량의 데이터를 분석하고, 탐지된 위협에 대해 자동화된 대응을 수행하는 기술이다. 이러한 시스템이 정확한 데이터 분석 및 처리 역량을 갖추고, 敵의 사이버위협으로부터 국방 정보체계를 효과적으로 보호할 수 있어야 신뢰성이 보장된다. 관련 선행연구를 살펴보면 Lee et al.(2022)의 연구에서는 블록체인 기술의 수용의도에 영향을 주는 요인들을 분석한 결과, 신뢰성이 성과기대, 노력기대에 긍정적인 영향을 미친다고 확인하였다. Kim(2024)의 인공지능 기반 사이버위협 대응시스템 도입 연구 및 Jang(2022)의 정부 인공지능 기반 보안관제 시스템 도입 연구에서도 신뢰성이 성과기대, 노력기대 및 시스템 도입의도에 중요한 영향을 미친다고 분석되었다. 이와같은 선행연구를 바탕으로 신뢰성을 국방 지능형 사이버위협 대응시스템이 제공하는 기능이 안전하게 수행될 수 있다고 믿는 신뢰의 정도로 정의하며, 신뢰성이 높을수록 성과기대와 노력기대가 증가하고, 기술 활용이 더욱 쉬울 것으로 예상된다. 이를 기반으로하여 다음과 같은 가설을 설정하였다.

H1. 국방 지능형 사이버위협 대응시스템의 신뢰성은 성과기대에 정(+)의 영향을 미칠 것이다.
H2. 국방 지능형 사이버위협 대응시스템의 신뢰성은 노력기대에 정(+)의 영향을 미칠 것이다.

국방 지능형 사이버위협 대응시스템은 다양한 데이터 출처에서 정보를 수집하고 이를 분석하여 위협을 탐지하는 역할을 수행한다. 전문성을 갖춘 시스템은 이 과정에서 높은 정확성을 유지하여 오탐과 과탐을 최소화할 수 있으며, 과거 데이터를 학습하고 새로운 위협을 신속하게 파악하여 적절한 대응 방안을 제시할 수 있다. 따라서 시스템의 전문성은 사용자가 업무 효율성이 향상될 것이라는 기대를 형성하게 하며, 이는 시스템에 대한 신뢰도를 높이는 요인으로 작용할 것이다. 관련 연구에서도 이러한 영향이 확인된 바 있다. 인공지능 기반 부동산 가치 평가 프롭테크 서비스 연구에서는 전문성이 성과기대와 사용의도에 유의미한 영향을 미친다는 사실을 검증하였으며(Kim, S., 2022), Kim(2024)의 인공지능 기반 사이버위협 대응시스템 도입 연구와 Jang(2022)의 정부 인공지능 기반 보안관제 시스템 도입 연구에서도 전문성이 성과기대와 노력기대, 시스템 도입에 중요한 영향을 미치는 요인으로 분석되었다. 이와같은 선행연구를 바탕으로 국방 지능형 사이버위협 대응시스템의 전문성을 기존의 보안관제 시스템보다 수행력측면에서 더 높은 수준의 결과를 제공할 것이라는 믿음의 정도로 정의하며 이를 기반으로 다음과 같은 가설을 제시하였다.

H3. 국방 지능형 사이버위협 대응시스템의 전문성은 성과기대에 정(+)의 영향을 미칠 것이다.
H4. 국방 지능형 사이버위협 대응시스템의 전문성은 노력기대에 정(+)의 영향을 미칠 것이다.

국방 지능형 사이버위협 대응시스템은 대규모 국방 네트워크 환경에서 발생하는 다양한 사이버위협을 탐지하고 분석하여 신속하게 대응하는 역할을 수행한다. 이 시스템의 핵심 요소 중 하나는 정확성으로, 위협 탐지 및 대응 과정에서 오탐과 미탐을 최소화하는 것이 필수적이다. 만약 시스템이 위협 정보를 정확하게 식별하지 못한다면 오탐으로 인해 불필요한 경보가 발생하거나, 실질적인 위협을 탐지하지 못해 치명적인 보안 사고로 이어질 가능성이 있다.

따라서 정확한 위협 탐지와 대응이 이루어질수록 국방 정보체계의 보안성과 업무 효율성이 향상될 수 있다. 정확성에 대한 선행연구를 살펴보면 Stinivasan(1985)는 정보시스템이 정확한 정보를 제공해야 한다고 강조하였으며, Lee(2024)는 시스템의 정확성을 제안하기 위해서 데이터의 질적 확보가 전제조건이라고 하였다. ETRI(2020)의 연구에서는 안면인식 기술도입에 대한 사회적 논란과 시사점을 분석하면서, 안면인식 기술의 정확성을 중요한 편익 요소로 정의하였다(Choi, J. Y., 2021). Kim, Y. (2022)의 인공지능 신약개발 플랫폼 도입의도 연구에서는 정확성과 전문성이 사용자의 신뢰 형성과 최종 수용의도에 중요한 영향을 미친다고 확인되었으며, Kim(2019)의 국방 스마트워크 사용의도 연구에서는 정확성이 노력기대에 유의미한 영향을 미치는 요인으로 분석되었다. 또한, 국방 실시간 안면인식 기술 도입의도에 관한 실증 연구에서는 정확성이 성과기대와 노력기대에 긍정적인 영향을 미친다고 분석되었다(Choi, J. Y., 2021). 선행연구 결과를 바탕으로 국방 지능형 사이버위협 대응시스템의 정확성을 위협정보를 정확하게 식별하여 차단할 것이라는 기술 수준 정도로 정의하였으며, 이를 기반으로 다음과 같은 가설을 제시하였다.

H5. 국방 지능형 사이버위협 대응시스템의 정확성은 성과기대에 정(+)의 영향을 미칠 것이다.
H6. 국방 지능형 사이버위협 대응시스템의 정확성은 노력기대에 정(+)의 영향을 미칠 것이다.

사이버 공격은 빠른 속도로 진화하며, 탐지 및 대응 지연이 보안 위협을 심화시킬 수 있기 때문에 신속한 정보처리와 즉각적인 대응이 필수적이다. 이러한 시스템의 신속성은 사이버위협이 발생하는 즉시 대응책을 마련하고, 정보가 지연 없이 처리될 수 있도록 보장하는 중요한 요소로 작용한다. 또한, 정보의 신속성은 정보 이용 시기의 적합성과 직결되는 중요한 요인으로, 적시에 제공되는 정보가 사용자에게 유용성과 신뢰성을 높이는 역할을 한다. 신속성에 대한 선행연구를 살펴보면 국방 실시간 안면인식 기술 도입의도에 관한 실증 연구에서는 신속성이 성과기대와 노력기대에 긍정적인 영향을 미친다고 분석되었다(Choi, J. Y., 2021). Chae et al.(2014)는 신속성이 비즈니스 운영 환경에서 데이터 활용에 영향을 미치는 중요한 요인임을 강조하였으며, Kang(2018)의 SNS 특성과 조직 커뮤니케이션 문화가 군의 사기에 영향을 미치는 요인에 관한 연구에서는 정보 기술력을 바탕으로 정보를 빠르게 제공 가능한 속도의 정도로 신속성을 정의하였다(Kang, 2018). 이러한 선행연구를 바탕으로, 국방 지능형 사이버위협 대응시스템의 신속성을 시스템의 정보 생성 과정이 신속하여 사이버위협 대응에 대한 적시성을 높이는 정도로 정의하며, 이를 기반으로 다음과 같은 가설을 설정하였다.

H7. 국방 지능형 사이버위협 대응시스템의 신속성은 성과기대에 정(+)의 영향을 미칠 것이다.
H8. 국방 지능형 사이버위협 대응시스템의 신속성은 노력기대에 정(+)의 영향을 미칠 것이다.

3.2.2 국방 지능형 사이버위협 대응시스템의 성과기대, 노력기대, 사회적영향에 대한 가설

통합기술수용모형(UTAUT)을 적용한 다양한 연구에서는 성과기대, 노력기대, 사회적영향이 정보시스템의 사용의도에 영향을 미친다는 점을 확인하였다(Venkatesh et al., 2003; Fuksa, 2013; Kang et al., 2016). 이러한 연구결과와 유사하게 모바일오피스를 중심으로 국방 스마트워크 사용의도에 영향을 미치는 요인에 관한 연구에서도 성과기대, 노력기대, 사회적영향이 사용의도에 유의미한 영향을 미치는 것으로 나타났다(Kim, 2021). 또한, 인공지능 기반 사이버위협 대응시스템의 도입의도에 영향을 주는 요인을 분석한 연구에서도 성과기대, 노력기대, 사회적영향이 시스템 도입의도에 중요한 역할을 한다는 점이 밝혀졌다(Kim, 2024). 성과기대는 새로운 기술이 개인의 업무 성

과 향상에 기여할 것이라는 기대를 의미하며(Venkatesh et al., 2003), 이는 기술수용모델(TAM)의 인지된 유용성과 밀접한 관련이 있다. 기존 연구에서도 성과기대는 신기술의 수용과 시스템 도입의도를 설명하는 핵심 요인으로 확인되었다(Hong, 2021). 한편, 노력기대는 새로운 기술을 사용하는 것이 얼마나 용이한지에 대한 믿음을 의미하며, 이는 TAM의 '인지된 사용 용이성' 개념을 기반으로 도출된 변수이다(Venkatesh et al., 2003). 노력기대는 정보기술 사용의도를 설명하는 데 중요한 요소로 작용하며(Venkatesh et al., 2003), 연구에 따르면 스마트폰 잠재적 수용자의 노력기대가 수용의도에 유의미한 영향을 미쳤다는 결과가 도출되었다(Kwon, 2010). 또한 Jang(2022)은 정부의 인공지능 기반 보안관제 시스템 연구에서 성과기대와 노력기대가 중요한 요인임을 확인하였으며, Shin(2022) 역시 인공지능 기반 설비관리 시스템 연구에서 성과기대와 노력기대가 수용의도에 영향을 미친다고 분석하였다. 이처럼, 여러 선행연구에서 성과기대, 노력기대, 사회적영향이 시스템 도입의도에 유의미한 영향을 미친다는 점이 입증되었다. 이러한 연구 결과를 바탕으로 본 연구에서는 국방 지능형 사이버위협 대응시스템 시스템과 관련하여 성과기대, 노력기대, 사회적영향을 다음과 같이 정의하였다. 성과기대는 국방 지능형 사이버위협 대응시스템을 이용하면 사이버 보안 관제 정탐율 향상 등 사이버위협 대응 업무를 처리하는데 유용할 것이라는 믿음의 정도, 노력기대는 사이버 보안 관제 등 사이버위협 대응 업무를 위해 국방 지능형 사이버위협 대응시스템을 쉽게 이용할 수 있을 거라는 믿음의 정도, 사회적영향은 사회적으로 국방 지능형 사이버위협 대응시스템의 도입이 필요하다고 믿는 정도로 정의하고 이를 바탕으로, 본 연구에서는 위 변수들이 수용의도에 미치는 영향을 규명하기 위해 연구가설을 다음과 같이 설정하였다.

H9. 국방 지능형 사이버위협 대응시스템의 성과기대는 수용의도에 정(+)의 영향을 미칠 것이다.
H10. 국방 지능형 사이버위협 대응시스템의 노력기대는 수용의도에 정(+)의 영향을 미칠 것이다.
H11. 국방 지능형 사이버위협 대응시스템의 사회적영향은 수용의도에 정(+)의 영향을 미칠 것이다.

4. 실증분석

4.1 자료의 수집

본 연구에서는 국방 사이버위협 대응시스템을 사용한 경험이 있는 국방 사이버 조직(군인 및 군무원)을 대상으로 자료를 수집하였다. 설문 조사는 총 44개 문항으로 구성되었으며, 이 중 39개는 측정 항목, 5개는 인구통계학적 정보를 포함하는 문항이다. 응답은 7점 리커트 척도로 수집되었으며, 조사 기간은 2024년 12월 15일부터 2025년 2월 10일까지 진행되었다. 총 357부의 응답이 확보되었으며, 표본은 국방 사이버작전 임무를 수행하는 군인과 군무원으로 한정하였다. 이는 연구 대상자들이 국방 사이버위협 대응시스템에 대한 정확한 이해를 바탕으로 응답할 수 있도록 하기 위함이다.

4.2 인구통계학적 분석

본 연구에서는 총 357명의 설문 데이터를 수집하여 분석을 진행하였으며, 표본의 인구통계학적 특성을 파악하기 위해 SPSS(ver 22.0)를 활용하여 빈도분석을 실시하였다. 설문 응답자의 군사 경험, 기술 이해도 등을 고려하여 가능한 다양한 집단을 포함하여 대표성을 확보하였으며 표본의 균형성과 편향성 최소화를 위해 자료의 정규성 검정은

R(ver 4.1.0)을 이용하여 진행하였다. 설문 응답자 357명의 인구통계학적 특성은 <Table 1>과 같다. 표본의 특성을 살펴보면 먼저 남성은 259명으로 72.7%, 여성은 98명으로 27.3%로 국방의 특성상 남성과 여성의 비율이 2배이상 높게 나타났다. 연령의 경우 20세~29세가 14.7%, 30세~39세 49.9%, 40세~49세 31.2%, 50세 이상이 4.2%로 30~39세가 가장 높은 비중을 차지하였으며, 계급은 영관장교 25.6%, 위관장교 24.3%, 부사관 21.6%, 군무원 28.5%로 계급별 비율은 균등한 결과가 나타났다. 근속연수는 1년 미만 5.69%, 1년 이상~5년 미만 10.6%, 5년 이상~10년 미만 23.3%, 10년 이상~15년 미만 28.2%, 15년 이상~20년 미만 16%, 20년 이상 16%로 1년 미만이 가장 적었고, 10년 이상~15년 미만이 28.2%로 비율이 높게 나타났다. 복무제대는 정책부서 44.7%, 사단급 이상 전술제대 비율은 55.3%로 나타났다.

Table 1. Demographic Characteristics of the Sample

Sortation		Frequency	Percentage
Gender	Male	259	72.7
	Female	98	27.9
	Total	357	100.0
Age	20 to 29	53	14.7
	30 to 39	178	49.9
	40 to 49	111	31.2
	Above 50	15	4.2
	Total	357	100.0
Rank	Field-grade Officers	91	25.6
	Company-grade Officers	87	24.3
	Non-Commissioned Officer	77	21.6
	Defense civillian	102	28.5
	Total	357	100.0
Length of Service	Duration < 1 year	21	5.9
	≥ 1 year and < 5 years	38	10.6
	≥ 5year and < 10 years	83	23.3
	≥ 10year and < 15 years	101	28.2
	≥ 15year and < 20 years	57	16
	≥ 20 years	57	16
	Total	357	100.0
Completion of Military Service	Policy Office	160	44.7
	Division and Higher Tactical Units	197	55.3
	Total	357	100.0

4.3 신뢰도 및 타당도 분석

신뢰도 평가는 내적 일관성 신뢰도(Internal Consistency Reliability)와 지표 신뢰도(Indicator Reliability)로 평가할 수 있다. 내적 일관성 신뢰도는 Cronbach's α 계수 값이 0.7 이상을 충족했을 경우, 관측변수들의 내적 신뢰도를 확보한다(Nunnally & Bernstein, 1994). PLS 모델 분석 시 합성 신뢰도는 DG.rho 값이 0.7 이상일 때 신뢰도가 확보되었다고 할 수 있다(Bagozzi & Yi, 1988).

Table 2. Results of Reliability Evaluation

Observed variable	MVs	C.alpha	DG.rho	Observed variable	MVs	C.alpha	DG.rho
Reliability	5	0.952	0.963	Performance Expectations	5	0.944	0.957
Expertise	5	0.947	0.960	Effort Expectations	5	0.957	0.967
Accuracy	3	0.882	0.927	Social Influence	5	0.942	0.956
Promptness	4	0.945	0.961	Adoption Intention	5	0.950	0.961

<Table 2>는 내적 일관성 신뢰도 평가 결과이다. 잠재변수들의 Cronbach's α 계수 값을 확인했을 때 기준치 0.7을 크게 넘었고, 합성 신뢰도 DG.rho 값이 역시 기준치 0.7을 넘었으며, 고유치인 Eigen value 값 역시 기준치 1.0 이상으로 나타났다. 모든 잠재변수의 기준은 내적 일관성 신뢰도와 합성 기준치를 크게 넘어 측정지표가 내적 신뢰도를 확보했다고 할 수 있다.

PLS-SEM 구조방정식 모형의 타당도 평가는 집중타당도(Convergent Validity)와 판별타당도(Discriminant Validity) 평가로 이루어진다. 판별타당도 평가는 AVE 제곱근 값의 확인과 교차적재기준 값을 확인하는 것으로 각 변인의 AVE 제곱근 값이 잠재변수와 다른 잠재변인 간의 상관계수 값에 비해 높으면 판별타당도가 확보되었다고 할 수 있다(Gefen & Straub, 2005). <Table 3>에서 대각선에 있는 AVE 제곱근 값이 잠재변수와 다른 잠재변인 간 상관계수 값에 비해 높게 나타나므로 판별타당도를 충족한 것으로 확인되었다.

Table 3. Results of Convergent Validity and Discriminant Validity Analysis

	RL	EP	AC	PR	PE	EE	SI	AI	AVE
RL	0.916								0.839
EP	0.860	0.909							0.826
AC	0.790	0.834	0.900						0.810
PR	0.738	0.794	0.845	0.927					0.859
PE	0.747	0.794	0.772	0.820	0.904				0.818
EE	0.770	0.774	0.723	0.670	0.689	0.923			0.852
SI	0.672	0.734	0.736	0.819	0.804	0.603	0.901		0.813
AI	0.680	0.728	0.701	0.765	0.803	0.611	0.861	0.912	0.832

* RL: Reliability, EP: Expertise, AC: Accuracy, PR: Promptness, PE: Performance Expectations, EE: Effort Expectations, SO: Social Influence, AI: Adoption Intention

4.4 경로분석 결과

경로분석에 있어 경로계수는 통계적으로 유의성을 갖으며, 이를 판단하기 위해 부트스트래핑(Bootstrapping)에 의한 비모수 평가 방법을 적용 분석한다(Hair et al., 2014). 본 연구에서는 구조방정식 분석을 R의 PLSPM Package를 사용하여 2,000번의 부트스트래핑 재샘플링을 통하여 경로계수의 유의성을 검증하였다.

경로계수(Path Coefficients)는 두 변수 간의 상관계수 값과 표준화된 변수 값(Standardized Values)의 관계에서 계산된 값을 갖는다. 추정된 경로계수 값이 +1에 가까울수록 통계적으로 유의한 강한 정(+)의 관계를 나타내며, -1에 가까울수록 강한 부(-)의 관계를 나타내고, 0에 가까울수록 그 관계가 약하다고 볼 수 있다. 경로계수 값의 유의성은 부트스트래핑에 의한 표준오차(Standard Error)에 따라 달라지는데, 부트스트랩 표준오차를 이용한 산출된 t값(Empirical t value)을 계산할 수 있고, 그 수식은 아래와 같다.

$$t = \frac{p_i}{se_i}$$

산출된 t 값이 임계치(Critical Value)보다 크면 계수 값이 특정 오류의 확률(유의수준)에서 유의적이라고 할 수 있으며, 양측검정(Two-tailed Test)에서 일반적 사용이 되는 임계치(t-value)는 1.96(유의수준 5%)으로 나타낼 수 있다(Hair et al., 2014). 본 연구의 경로분석 결과는 <Table 4>와 같다.

Table 4. Results of Path Analysis

Research hypothesis		Hypothetical path			Estimate	t-value	p-value	Result
H1	H1-1	RL	→	PE	0.135	2.409	0.017 *	Adopted
	H1-2	EP			0.268	4.212	0.000 ***	Adopted
	H1-3	AC			0.043	0.714	0.476	Rejected
	H1-4	PR			0.471	8.709	0.000 ***	Adopted
H2	H2-1	RL	→	EE	0.350	5.441	0.000 ***	Adopted
	H2-2	EP			0.327	4.468	0.000 ***	Adopted
	H2-3	AC			0.157	2.242	0.026 *	Adopted
	H2-4	PR			0.021	0.332	0.740	Rejected
H3	H3-1	PE	→	AI	0.282	6.039	0.000 ***	Adopted
	H3-2	EE			0.054	1.557	0.120	Rejected
	H3-3	SI			0.601	14.151	0.000 ***	Adopted

※ Significance Level : *p<0.05, **p<0.01, ***p<0.001

* RL: Reliability, EP: Expertise, AC: Accuracy, PR: Promptness, PE: Performance Expectations, EE: Effort Expectations, SO: Social Influence, AI: Adoption Intention

국방 지능형 사이버위협 대응시스템의 기술특성요인과 성과기대 사이의 경로분석에서는 신속성(t=8.709, p=0.000), 전문성(t=4.212, p=0.000), 신뢰성(t=2.409, p=0.017)으로 나타나 신속성 및 전문성, 신뢰성이 성과기대에 정(+)의 영향을 미치는 것으로 확인되었으며, 정확성은 기각되어 영향을 미치지 않는 것으로 확인되었다. 이는 국방 데이터의 활용에 대한 군의 엄격한 보안 및 제도적 규제로 인공지능 기술 적용을 위한 외부망 접속 불가, 데이터의 시험 제한, 비정형 데이터가 대부분인 국방 분야의 특성상 국방 데이터 정보를 빅데이터화하여 활용하는 데 어

려움이 많으며, 국방 데이터가 비밀 유통 구조로 운용되기 때문에 국방정보시스템 등에 적용하는데 한계가 있다고 여기고 있는 것으로 확인할 수 있다. 따라서 국방 지능형 사이버위협 대응시스템 도입시 시스템의 정확성을 높이기 위해 다양한 국방 사이버방호체계로부터 수집된 정보를 종합하여 양질의 데이터를 제공함으로써 국방 사이버 인력의 사이버위협 대응 능력 향상을 위한 시스템 개발 및 제공하는 것에 중요한 시사점을 제공할 수 있다.

국방 지능형 사이버위협 대응시스템의 기술특성요인과 노력기대 사이의 경로분석에서는 신뢰성(t=5.441, p=0.000), 전문성(t=4.468, p=0.000), 정확성(t=2.242, p=0.026)으로 나타나 신뢰성, 전문성, 정확성은 노력기대에 정(+)의 영향을 미치는 것으로 확인되었으며, 신속성은 기각되어 영향을 미치지 않는 것으로 확인되었다. 이는 현재 국방 시스템에서는 데이터의 호환성 문제, 경직된 시스템 구조 등으로 인하여 체계적인 데이터 습득 및 공유가 쉽지 않은 상황이므로 신속성보다는 데이터의 정확성과 시스템 간 연계성 확보가 더 중요한 과제로 인식될 수 있으며 (Moon et al., 2020), 국방 분야에서의 시스템은 정보의 정확성과 기밀성 등 운용되는 정보에 대한 정보보증이 다른 분야보다 절대적으로 필요하므로 이는 신속성보다 정보의 질적 측면이 더 중요하게 고려됨을 시사한다.

국방 지능형 사이버위협 대응시스템의 성과기대, 노력기대, 사회적영향이 수용의도에 미치는 영향을 분석한 결과, 사회적영향(t=14.151, p=0.000)과 성과기대(t=6.039, p=0.000)는 수용의도에 긍정적인 영향을 미치는 것으로 확인되었으나, 노력기대는 유의한 영향을 미치지 않는 것으로 나타났다.

이는 국방 사이버위협 대응시스템이 다양한 기술적 요소와 복잡한 연계성을 포함하고 있어, 제공되는 정보가 지나치게 기술적이고 상세할 경우 비전문가인 사용자가 이를 해석하는 데 어려움을 겪을 가능성이 높기 때문으로 해석된다(Rudin, 2019). 국방 사이버 인력이 기대하는 이상적인 시스템은 숙달이 용이하며, 높은 정확성과 간결성을 제공하는 시스템이다. 그러나 시스템이 사이버위협 대응 과정을 지나치게 기술적으로 상세히 제공하면, 사용자의 이해를 돕기보다는 오히려 운용 부담을 증가시키는 요인으로 작용할 수 있다.

즉, 사용자는 시스템이 사이버위협을 정확하게 식별하고 직관적으로 정보를 제공할 것을 기대하지만, 시스템의 조작이 복잡하거나 학습 부담이 크다면 숙달하는 데 많은 노력이 필요하게 되어 기대와 어긋날 수 있다는 것이다. 이러한 점이 반영되어 노력기대가 수용의도에 영향을 미치지 않는 것으로 나타난 것으로 볼 수 있다.

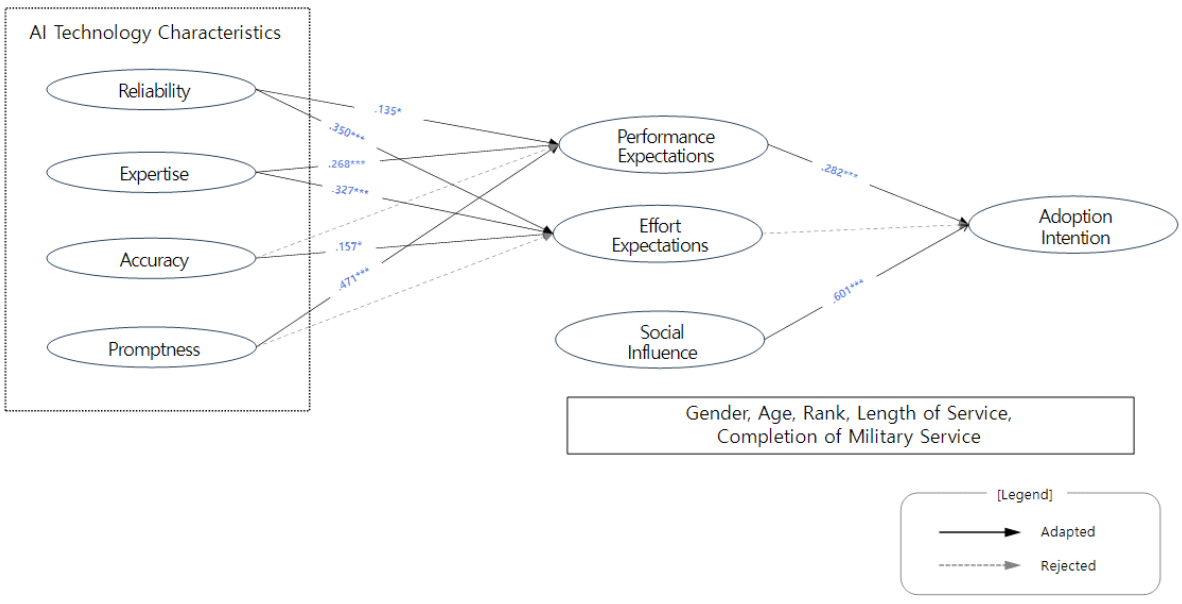

Figure 3. Result of Path Analysis

결과적으로, 국방 지능형 사이버위협 대응시스템을 개발하고 도입할 때 사용자의 운용 환경을 고려한 직관적인 인터페이스를 제공하고, 시스템 사용 매뉴얼을 시각적으로 구성하는 것이 중요하다. 또한, 원활한 운용을 위해 사용자 교육 및 지원 프로그램을 마련하는 것이 필수적이라는 시사점을 도출할 수 있다.

본 연구의 가설을 바탕으로 도출된 경로분석 결과는 <Figure 3>에 제시된 연구모형을 통해 확인할 수 있다.

5. 결 론

전 세계적으로 사이버위협이 급증하는 가운데, 국방 분야에서의 사이버 공간 보호는 국가 안보의 핵심 과제로 부각되고 있다. 특히, 국방 ICT 환경이 발전함에 따라 사이버위협은 더욱 지능화·고도화되고 있으며, 기존 보안 솔루션만으로는 효과적인 대응이 어려운 상황이다.

국방 영역에서의 사이버위협은 단순한 해킹이나 정보 유출을 넘어, 군사 작전 수행 및 국가 주요 인프라 보호에 직결되는 문제이기 때문에 보다 정밀하고 즉각적인 대응이 요구된다. 이에 따라, 실시간 위협 분석과 자동화 대응이 가능한 국방 지능형 사이버위협 대응시스템의 도입이 필수적이며, 본 연구는 해당 시스템의 수용의도에 영향을 미치는 요인을 규명하는 것을 목표로 하였다.

본 연구의 학문적 시사점은 다음과 같다. 첫째, 기존 연구가 인공지능 기술의 국방 적용 가능성과 기술적 발전에 초점을 맞추었던 것과 달리, 본 연구는 사용자 관점에서 인공지능 기술특성이 국방 환경에서 시스템 수용의도에 미치는 영향을 구조적으로 분석하였다는 점에서 차별성이 있다. 이를 통해, 단순한 기술 성능 개선을 넘어 국방 조직 내 인공지능 기반 사이버위협 대응시스템이 효과적으로 도입되고 활용될 수 있는 방안을 모색하였다.

둘째, 본 연구는 선행연구를 기반으로 국방 지능형 사이버위협 대응시스템의 핵심 기술특성으로 신뢰성, 전문성, 정확성, 신속성의 네 가지 요소를 도출하였으며, 분석 결과 이들 요인이 성과기대와 노력기대에 긍정적인 영향을 미치는 것으로 나타났다. 이는 인공지능 기술을 활용한 보안 시스템 도입 시, 해당 기술특성이 사용자의 수용의도 결정에 중요한 기준이 될 수 있음을 시사한다.

셋째, 본 연구의 결과는 국방 분야뿐만 아니라 금융, 제조, 의료, IT 등 다양한 산업에서 유사한 정보기술(IT) 시스템 도입 시에도 적용될 수 있는 시사점을 제공한다. 산업별로 보안 수준이 중요한 분야에서는 인공지능 기술특성이 시스템의 도입과 수용의도에 중요한 판단 기준이 될 수 있으며, 특히 정확한 위협 탐지, 신속한 대응, 신뢰성 높은 데이터 분석이 필수적인 산업군에서 본 연구의 결과가 활용될 수 있음을 보여준다.

본 연구의 결과를 통해 도출할 수 있는 실무적 시사점은 다음과 같다. 첫째, 인공지능 기술특성 중 성과기대에 가장 큰 영향을 미치는 요인은 신속성, 전문성, 신뢰성 순으로 나타났으며, 이는 국방 환경뿐만 아니라 위기 대응이 중요한 산업군에서도 신속하고 신뢰성 있는 인공지능 기술 적용이 필요함을 의미한다.

둘째, 인공지능 기술특성 중 노력기대에 가장 큰 영향을 미친 요인은 신뢰성, 전문성, 정확성 순으로 나타났다. 이는 국방 사이버 공간에서 신뢰성 높은 데이터 활용과 정확한 위협 탐지가 필수적임을 의미한다. 특히, 전문성을 갖춘 국방 지능형 사이버위협 대응시스템은 과거 공격 패턴을 학습하여 새로운 위협을 정확히 탐지하고, 최적의 대응 전략을 수립함으로써 작전 수행의 정밀도를 향상시킬 수 있다. 본 연구는 이를 통해 국방 지능형 사이버위협 대응시스템 도입 시 고려해야 할 핵심 요소를 규명하고, 이러한 요소가 국방 사이버작전뿐만 아니라 금융 보안, 의료 데이터 보호, 제조업의 스마트 팩토리 보안 등에서도 인공지능 기반 보안 시스템 도입 시 중요한 요인이 될 수 있음을 시사한다.

본 연구의 한계점으로는, 응답자가 실제 시스템을 사용해본 경험이 부족하여 수용의도에 대한 평가가 일부 주관적일 가능성이 있다는 점이 있다. 따라서, 향후 연구에서는 시스템 도입 후 사용자 경험을 기반으로 지속사용의도를 분석하는 연구가 필요하다. 또한, 본 연구는 국방 사이버작전 실무자를 대상으로 설문을 진행하였으나, 최종적으로 정책을 결정하는 국방 사업 담당 부서의 관점이 충분히 반영되지 않은 한계가 존재한다. 이에 따라, 향후 연구에서는 의사결정권자를 포함하여 보다 포괄적인 분석을 수행함으로써, 국방뿐만 아니라 다양한 산업군에서 인공지능 기반 보안 시스템의 효과적인 도입과 운영을 위한 정책적 시사점을 도출할 필요가 있다.

REFERENCES

Ajzen, I. and Fishbein, M. 1975. A Bayesian Analysis of Attribution Processes. Psychological Bulletin 82(2):261-277.

Baek, ChangHwa, Lim, SungUk, Choe JaeHo. 2019. A Study on Major Characteristic Analysis and Quality Evaluation Attributes of Artificial Intelligence Service. Journal of the Korean Society for Quality Management 47(4):837-846.

Bagozzi, R. P. and Yi, Y. 1988. On the Evaluation of Structural Equation Models. Journal of the Academy of Marketing Science 16(1):74-94.

Chae, B., Yang, C., Olson, D., and Sheu, C. 2014. The Impact of Advanced Analytics and Data Accuracy on Operational Performance: A Contingent Resource Based Theory(RBT) Perspective. Decision Support Systems 59:119-126.

Chichilnisky. G. (Eds.). 1999. Markets. Information and Uncertainty. Cambridge University Press.

Choi, JooWon. 2021. A Study on Factors Affecting Acceptance Intention to Use Smart Fish Farming System based on Artificial Intelligence. PhD diss., Soongsil University.

Choi, JungYoung. 2021. An Empirical Study on Factors Affecting the Intention to Adoption of Real-time Facial Recognition Technology in Defense. PhD diss., Soongsil University.

Eom, JunHo. 2013. A Preemptive Cyber Deterrence Strategy to Ensure Cyber Warfare Defense Capabilities. Security Journal 24:125-204.

Fishbein, M. and Ajzen, I. 1975. Belief, Attitude, Intention, and Behavior : An Introduction to Theory and Research. Reading, MA: Addison-Wesley.

Fuksa, M. 2013. Mobile Technologies and Services Development Impact on Mobile Internet Usage in Latvia. Procedia Computer Science 26:41-50.

Gefen, D. and Straub, D. 2005. A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example. Communications of the Association for Information Systems 16(1):91-109.

Hair J. F., Hult, G. T. M., Ringle, C. M. and Sarstedt, M. 2014. A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Thousand Oaks, CA: Sage Publications.

Hong, SooHee. 2021. A Study on Factors Affecting the Construction of Big Data-based Intelligent Integrated Forest Fire Disaster Prevention Platform. PhD diss., Soongsil University.

Huh, HyoungJo, Ko, Sujin, Baek, SeungHyun. 2023. A Study on the Big Data Analysis and Predictive Models for Quality Issues in Defense C5ISR. Journal of Korean Society for Quality Management 51(4):551-571.

Jang, SangHyun. 2022. An Empirical Study on Factors Affecting the Introduction of AI-Based Security Control Systems in Government. PhD diss., Soongsil University.

Jeon, HyeongJu. 2019. A Study on Efficient Security Control Measures Using SIEM and Threat Systems. PhD diss.,

Sungkyunkwan University.

Kang, SungYoon. 2018. The Effects of Social Media Characteristics and Organizational Communication Culture on Military mmorale. Journal of Digital Convergence 16(7):79-88.

Kang, SunHee and Kim, HaKyun. 2016. The Moderating Effects of Old and Innovation Resistance on the Intention to Accept and Utilize Easy Payment Services. Focusing on the Moderating Effects of Old and Innovation Resistance. Management and Information Research 35(2):167-183.

Kim, DongHee, Park, SangDon, Kim, SoJung, and Yoon, OhJun. 2017. A Study on How to Build a Cyber Threat Information Sharing System: Focusing on the US Case. The Journal of the Convergence Security 17(2):53-68.

Kim, JinMin. 2024. A Study on the Factors Affecting the Intention to Adopt Artificial Intelligence-based Cyber Threat Response System. PhD diss., Soongsil University.

Kim, JinTae. 2019. Factors Influencing the Intention to Use Defense Smartwork. Defense Smartwork Usage Intention: Focusing on Mobile Office. PhD diss., Soongsil University.

Kim, SangJin. 2022. A Study on Factors Affecting the Intention to Use Proptech Services for Artificial Intelligence-based Real Estate Valuation. PhD diss., Soongsil University.

Kim, Ye-eun, Song, Ho Jun, and Shin, Wan Seon 2024. Analysis of machine learning research patterns from a quality management perspective. Journal of Korean Society for Quality Management 52(1):77-93.

Kim, YoungDae. 2022. A Study on the Factors Affecting the Intention to Adopt an AI-based Drug Discovery Platform Factors Affecting Acceptance Intention of AI-based Drug Development Platform. PhD diss., Soongsil University.

Kwon, OhJoon. 2010. An Empirical Study of Potential Adopters' Acceptance of Smartphones. Internet and Information Security 1(1):55-83.

Lee, DonHee. 2024. Does Artificial Intelligence (AI)-based Applications Improve Operational Efficiency in Healthcare Organizations?: Opportunities and Challenges. Journal of Korean Society for Quality Management 52(3):557-574.

Lee, HongJe. 2018. A Study on the Factors Influencing the Intention to Invest in Information Security. PhD diss., Soongsil University.

Lee, KyoungJin, Kim, YongHwan, Lee, JiOne and Gim, GwangYong. 2022. A Study on the Factors Affecting the Intention to Adopt of Blockchain-Based Identity Certification Services in the Defense Sector. The Journal of Korean Institute of Communications and Information Sciences 47(1):113-131.

Min, J., Hong, Y., King, C. B., and Meeker, W. Q. 2022. Reliability Analysis of Artificial Intelligence Systems Using Recurrent Events Data from Autonomous Vehicles. Journal of the Royal Statistical Society Series C: Applied Statistics 71(4):987-1013.

Moon, JaeWoong, Park, JangYong, Lee, JinHa and Song, JaeSeung. 2020. Analysis of Cyber Defense Information Security Systems for the Utilization of Artificial Intelligence Technology. The Journal of the Digital Contents Society 21(5):891-900.

Nunnally, J. C. and Bernstein, I. H. 1994. Psychometric Theory. 3rd Edition. New York, NY: Tata McGraw-Hill Education.

Rudin, C. 2019. Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead. Nature Machine Intelligence 1(5):206-215.

Shin, HeeKyung. 2022. A Study on Acceptance Intention of AI-based Facility Management System. PhD diss., Soongsil University.

Shin, KyungSoo. 2020. Military Response Issues in the Cyber Operational Environment. Defense Policy Research 36(1):71-99.

Song, TaeEun. 2023. North Korea Cyber Threats: Current Status and Strategic Responses. Korea Nagtional Diplomatic Academy(KNDA).

Stinivasna, A. 1985. Alternative Measures of System Effectiveness: Associations and Implications. MIS Quarterly 9(3):243-253.

Venkatesh, V., Morris, M. G., Davis, G. B. and Davis, F. D. 2003. User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly 27(3):425-478.

저자소개

정성미 숭실대학교 일반대학원 IT정책경영학과 박사과정에 재학 중이며 현재 육군 정보통신병과 장교로 복무중이다. 주요 관심분야는 Software, AIoT, AI, Big Data 분석, Metaverse 및 정보보호 등이다.

신성제 숭실대학교 일반대학원 경영학 박사과정에 재학 중이며, ㈜엠지테크윈 대표로 재직중이다. 주요 관심분야는 MIS, ISO 인증평가, 빅데이터, 무인시스템 등이다.

최정일 미국 University of Nebraska-Lincoln에서 경영학 박사학위를 취득하였으며, 프랑스 인시아드(INSEAD)에서 초빙연구원과 미국 Merrimack 대학에서 경영학부 교수를 역임한 후 현재 숭실대학교 경영학부 교수로 재직 중이다. 주요 연구 관심 분야는 운영관리, 서비스 품질평가, IT기반의 혁신전략 및 품질 4.0 등이다.