https://doi.org/10.33778/kcsa.2023.23.5.009

보안과 프라이버시 위험이 스마트카 안전과 신뢰에 미치는 영향★

권 순 범*, 이 환 수**

요 약

운전자의 주행 안전성과 편의성을 증가시키기 위하여 최근 자동차는 ICT 기술이 융합된 스마트카 형태로 진화하고 있다. 그러나 스마트카의 자율주행 기능을 구현하기 위해 존재하는 전자제어장치(Electronic Control Unit; ECU)와 차량용 네트워크의 취약성은 자동차 사이버보안에 대한 위험을 증가시키는 원인이 되고 있다. 스마트카 보안에 대한 운전자들의 불안 심리는 스마트카 확산에 부정적인 영향을 미칠 수 있으나 실제 스마트카 해킹이 현실에서 일어난 사례는 적은 상황으로 주로 연구를 통해서만 이러한 위험에 대해 논의되고 있는 상황이다. 향후 스마트카의 보급과 확산을 위해서는 스마트카의 실질적인 보안능력 향상과 더불어 운전자들이 인식하는 위험 요인과 이를 통해 형성된 스마트카에 대한 신뢰를 이해하는 것이 중요할 수 있다. 따라서 본 연구에서는 스마트카의 신뢰 형성에 영향을 미치는 위험 요인을 보안과 프라이버시를 중심으로 살펴보고 이러한 요인들이 스마트카 안전인식과 신뢰에 어떠한 영향을 미치는지 분석한다.

The impact of security and privacy risk on smart car safety and trust

Soonbeom Kwon*, Hwansoo Lee**

ABSTRACT

Smart cars, which incorporate information and communication technologies (ICT) to improve driving safety and convenience for drivers, have recently emerged. However, the increasing risk of automotive cybersecurity due to the vulnerability of electronic control units (ECUs) and automotive networks, which are essential for realizing the autonomous driving functions of smart cars, is a major obstacle to the widespread adoption of smart cars. Although there have been only a few real-world cases of smart car hacking, drivers' concerns about the security of smart cars can have a negative impact on their proliferation. Therefore, it is important to understand the risk factors perceived by drivers and the trust in smart cars formed through them in order to promote the future diffusion of smart cars. This study examines the risk factors that affect the formation of trust in smart cars, focusing on security and privacy, and analyzes how these factors affect safety perceptions and trust in smart cars.

Key words : Smart cars, security, privacy, safety, trust

접수일(2023년 10월 23일), 수정일(2023년 12월 11일), 게재확정일(2023년 12월 12일)

★ 이 논문은 2023년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임 (P0008703, 2023년 산업혁신인재성장지원사업)

* 단국대학교 과학기술정책융합학과 박사과정(주저자)

** 단국대학교 산업보안학과 교수(교신저자)

1. 서 론

운전자의 주행 안전성과 편의성을 증가시키기 위하여 최근 자동차는 ICT 기술이 융합된 스마트카 형태로 발전하고 있다. 특히, 운전자의 주행 안전성을 위해 개발되고 있는 운전자 보조 시스템과 자율주행 기능은 운행 중 발생하는 판단 오류와 실수를 줄여주어 교통사고를 줄여줄 것으로 예상된다[1]. 그러나 스마트카의 자율주행 기능을 구현하기 위해 존재하는 전자제어장치(Electronic Control Unit; ECU)와 차량용 네트워크의 취약성은 자동차 사이버보안에 대한 위험을 증가시키는 원인이 되고 있으며, 이에 따라 스마트카의 보안에 대한 소비자들의 불안 심리가 커지고 있는 상황이다[2].

실제로 스마트카의 해킹이 현실에서 일어난 사례는 아직 많지 않다. 스마트카에 대한 해킹 사례는 주로 학계와 업계의 연구를 통해서만 주로 보고되고 있는 상황으로 초기 시장 및 제품에 대한 소비자들의 막연한 우려일 수 있다. 그러나 이러한 우려들이 실제 스마트카 확산이나 산업 성장에 장벽이 될 수 있기 때문에 이러한 우려들이 어떻게 발생하는지에 대한 이해는 매우 중요하다. 자동차와 같이 사람의 안전과 직결된 제품의 경우 제품에 대한 신뢰형성이 필요하고 이러한 신뢰에 미치는 영향요인들을 논의하는 것은 학술적으로나 실무적으로 매우 중요하다. 선행연구들에서도 신기술에 대한 소비자의 신뢰는 소비자의 수용의도에 유의한 영향을 미치는 것으로 나타난 바 있다[3]. 이러한 관점에서 보안 우려가 있는 스마트카의 경우 시장 확산을 위해서 중요한 것은 실질적 보안능력의 향상과 더불어 스마트카의 보안과 위험 요인에 대한 운전자들의 인식과 그 결과로 나타나는 신뢰일 수 있다.

따라서 스마트카와 같은 혁신제품의 확산을 위해 중요한 것은 소비자의 신뢰를 향상시키는 것이며, 이를 위해서는 소비자의 신뢰 형성에 원인을 주는 요인을 분석할 필요가 있다. 현재 스마트카에 대한 선행연구들은 스마트카의 수용의도를 분석하기 위한 수단으로써 단순히 전통적인 기술수용이론들만 활용하고 있을 뿐[4][5], 스마트카의 수용의도에 영향을 미치는 신뢰 형성 요인에 대한 논의는 부족한 실정이다. 기존 연구들에서는 주로 스마트카 보안 이슈에 대한 기술적 측면의 논의는 활발했던데 반해, 스마트카 환경에서 운전자들이 우려할 수 있는 프라이버시 침해에 대한 논의는 상대적으로 부족하였다. 더욱이 보안과 프라이버시 뿐만 아니라 스마트카 신뢰에 미치는 영향요인들에 대한 파편화된 논의가 이루어져왔기 때문에 스마트카 운전자들의 인식하는 안전 관련 요인들 간의 구조적 관계에 대한 종합적 논의 또한 제한적이었다. 이에 본 연구는 스마트카의 신뢰 형성에 영향을 미치는 요인을 보안과 프라이버시 관점에서 살펴보고 이러한 세부 요인들이 스마트카의 안전과 신뢰 인식에 어떠한 영향을 미치는지를 분석한다.

2. 이론적 배경

2.1 스마트카와 보안

스마트카는 자율주행자동차와 커넥티드카를 모두 포함하는 개념이며, 자율주행자동차의 자율성과 커넥티드카의 연결성이 모두 포함된 자동차를 의미한다. 스마트카가 제공하는 핵심 기능은 크게 운전자보조시스템(Driving Assistance System), 차량용 인포테인먼트 시스템(Vehicle Infotainment System), 사물인터넷 허브(IoT Hub) 3가지로 구분 가능하며, 이는 운전자의 편리성을 증대시키는 역할을 하고 있다[6]. 그러나 스마트카가 제공하는 자율주행기능과 인포테인먼트 시스템 등은 차량 내부 네트워크와 외부 네트워크와의 연결성을 강화시키고 있으며, 이는 전통적인 자동차에서는 크게 문제되지 않았던 보안 문제를 증가시키는 원인이 되고 있다. 실례로 2010년 학계에서 최초로 자동차 해킹에 대한 가능성이 제기된 것을 시작으로 2011년에는 자동차에 탑재된 무선 통신을 해킹한 최초의 연구가 발표되었고, 2013년에는 화이트해커인 Miller와 Valasek이 Ford의 Escape 차량과 Toyota의 Prius 차량을 해킹하는데 성공한 바 있다. 이 외에도 자동차 해킹의 사례와 방법은 다양해지고 있으며, 학계와 실무에서는 이를 해결하기 위한 다양한 연구가 이루어지고 있다[7].

국내·외에서는 스마트카에 대한 해킹으로 인해 발생할 수 있는 문제를 사전에 예방하고 대응하기 위하여 자동차 사이버보안에 대한 다양한 가이드라인과

법·정책적 개선방안을 마련하고 있다, 실례로 유럽은 자동차 사이버보안을 강화하기 위하여 자동차 사이버 보안에 대한 규정인 「UN Regulation No. 155」를 채택하여 시행하고 있다. 또한, 국내에서는 자동차 사이버보안에 대한 규정이 정비되기 전까지 자동차 사이버보안에 대한 관리 방안을 참고할 수 있도록 국토교통부에서 「자동차 사이버 보안 가이드라인」을 제작하여 배포한 바 있다. 그러나 이들 규정과 가이드라인은 자동차에 대한 사이버보안에 초점이 맞추어져 있을 뿐 사이버보안에 대한 해킹으로 발생할 수 있는 프라이버시 관리 문제에 대한 논의는 부족한 실정이다.

하지만 스마트카에 대한 프라이버시 관리 문제는 소비자의 신뢰를 저해하는 요인이 된다는 점에서 보안 문제와 함께 중요하게 다루어질 필요가 있다. 실례로 스마트카에 대한 해킹 문제로 발생할 수 있는 개인정보 유출과 안전 위험 및 보안 관련 문제들은 스마트카에 대한 소비자의 신뢰를 낮추고 스마트카에 대한 소비자의 지각된 위험을 높여 스마트카에 대한 소비자의 제품선택 행동에 영향을 주는 것으로 나타났다. 즉, 스마트카 보안에 대한 불안 심리가 커질수록 스마트카에 대한 소비자의 수용의도는 낮아질 것이며, 스마트카에 대한 소비자의 수용의도를 높이기 위해서는 스마트 보안에 대한 문제가 선결되어야 한다[8]. 그러나 소비자의 행동 의도는 소비자가 느끼는 객관적인 상황보다는 주관적인 감정에 의해 결정되는 경우가 많기 때문에[9], 스마트카에 대한 소비자의 수용의도를 높이기 위해서는 스마트카 보안에 대한 실증연구와 함께 스마트카 보안으로 인한 불안 심리가 소비자에게 미치는 영향을 연구하는 연구도 함께 병행되어야 한다. 스마트카 보안이 소비자의 행동 의도에 어떠한 영향을 미치는지 분석한 선행연구가 일부 존재하나, 단순히 소비자의 행동의도에 영향을 미치는 하위요인으로써 보안 문제를 다루고 있을 뿐 스마트카 보안 문제로 발생할 수 있는 파생 위험이 소비자의 행동의도에 미치는 영향을 분석한 연구는 부족한 실정이다.

2.2 스마트카의 지각된 위험

지각된 위험 (Perceived Risk) 은 1960년대 Bauer (1967)에 의해 처음 소개된 개념으로 제품 사용 시 소비자가 느낄 수 있는 주관적인 손실 위험을 의미한다. Bauer (1967)에 따르면 소비자는 어떠한 행동을 할 때 위험을 감수한다고 하였으며, 이러한 위험 감수 행동이 소비자의 제품 선택 의도에 영향을 미친다고 하였다[10]. 이와 같은 Bauer의 지각된 위험 개념은 소비자의 행동의도를 파악하는 핵심적인 변수로 활용되어 왔으며, 소비자의 제품 구매 행동을 설명하는 연구에 활용되며 발전하였다. 특히, 마케팅, 경영학, 심리학 등과 같은 다양한 분야에 적용되며 이론적 발전을 이뤄왔으며, 선행연구들은 지각된 위험 개념을 제품의 특성과 환경에 따라 다양하게 분류하며 이론을 발전시켜 왔다[11].

스마트카 분야에서 지각된 위험은 소비자의 행동의도를 파악하기 위한 수단으로써 활용되고 있다. 선행연구는 크게 지각된 위험의 세부 요인을 단일차원으로 분류하는 연구와 다차원적인 요소로 분류하는 연구로 구분 가능하며, 자동차의 소비자 행동의도를 분석하는 연구는 지각된 위험을 다차원적인 요소로 분석하는 연구가 주를 이루고 있다. 지각된 위험을 단일차원으로 접근한 연구로 Thilina et al. (2019)은 기술수용이론과 지각된 위험 개념을 활용하여 전기차의 사용의도에 미치는 영향을 분석하였다[12]. 그러나 이는 ICT 기술이 융합된 엄밀한 의미의 스마트카를 분석한 연구라기보다는 단순히 전기차의 사용의도를 분석한 연구로 스마트카와 관련한 시사점을 논의하는데는 한계가 있었다. Zhang et al. (2019)은 기술수용이론(TAM)과 초기 신뢰 형성 이론(Initial Trust Build Theory) 및 지각된 위험 이론을 활용하여 자율주행자동차의 수용의도에 미치는 영향을 분석하였으며, 지각된 위험의 하위 요인으로 지각된 안전 위험(Perceived Safety Risk)과 지각된 프라이버시 위험(Perceived Privacy Risk)을 제시하였다[13]. Kenesei et al. (2022)는 신뢰 이론과 지각된 위험 이론을 활용하여 자율주행자동차의 사용의도에 영향을 미치는 요인을 분석하였다. 위험 요인을 성능 위험(Performance Risk)과 프라이버시 위험(Privacy Risk)으로 분류하였으며, 프라이버시 위험이 자율주

행자동차의 사용의도에 유의한 영향을 미치는 것을 확인하였다[14].

기존 연구들은 주로 Bauer가 제시한 일반적 위험 요인들이 구매의도나 사용의도에 미치는 영향을 분석함으로써 제품 차원의 수용에 대한 논의를 주로 해왔다는 점에서 한계가 있다. 스마트카를 포함한 스마트 기술 환경에서는 해당 기술에 대한 신뢰관리가 매우 중요하며 이는 보안과 프라이버시에 대한 균형을 확보함으로써 가능해진다[15]. 기존 연구들에서 스마트카의 신뢰와 관련된 안전, 보안, 프라이버시 요인들의 영향이 파편적으로 논의되어 왔기 때문에 이러한 요인들의 구조적 관계나 통합적 영향에 대한 논의는 소비자들의 스마트카에 대한 인식을 이해하는데 유용하다.

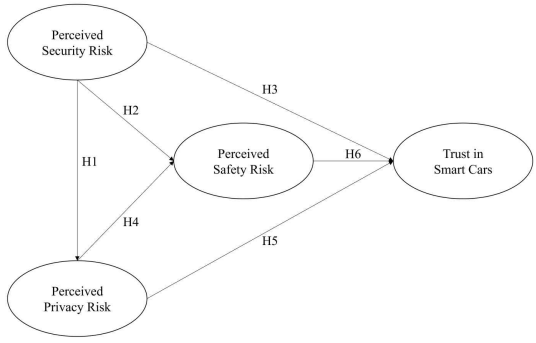
2.3 스마트카 신뢰

소비자의 지각된 위험과 행동 의도에 영향을 주는 신뢰는 소비자 행동 연구에 있어 주요 관심 주제가 되어가고 있다. 그러나 신뢰라는 개념이 가지고 있는 추상성과 측정의 어려움과 같은 특성은 신뢰에 대한 연구를 어렵게 하였으나 Mayer et al. (1995)는 기존에 연구되던 신뢰 개념을 통합하는 연구를 제시하였고, 이들이 제시한 신뢰 개념은 이후 사회과학 분야에 통용되며 적용되고 있다[16].

스마트카에 대한 신뢰는 스마트카 사용에 대한 소비자의 행동에 유의한 영향을 끼치는 중요한 개념이다[4][17]. 스마트카 분야에서 Choi & Ji (2015)는 신뢰와 지각된 위험이 자율주행자동차의 사용의도에 미치는 영향을 분석하는 연구를 수행하였다. 이들은 자율주행자동차의 신뢰 형성에 영향을 미치는 요인으로 시스템 투명성(System transparency), 기술적 능력(Technicalcompetence), 상황관리(Situation management)를 제시하였으며, 이들 요인 모두 자율주행자동차의 신뢰 형성에 유의한 영향을 미치는 것으로 나타났다[4]. Modliński et al. (2022)은 성별과 종교적 성향이 자율주행자동차의 신뢰형성에 미치는 영향을 분석하였으며[18], Chan & Lee (2021)는 기술수용이론의 일부 요인을 독립변수로 설정하고 신뢰를 매개요인로 설정하여 자율주행자동차의 사용의도에 어떠한 영향을 미치는지 분석하였다[19]. 이처럼 스마트카 분야에서 신뢰는 스마트카에 대한 소비자의 행동 의도를 파악하기 위한 도구로써 독립변수 및 매개변수로 다양하게 활용되어 왔다. 그러나 주로 성능적 측면에서 구매와 관련된 논의에 그쳐 보안이나 프라이버시와 같이 정보보호나 기기의 안전성 측면의 요인을 통합적으로 논의하지 못한 한계가 있다.

3. 연구모형 및 가설설정

본 연구의 목적은 스마트카의 보안이 운전자의 지각된 위험과 스마트카 신뢰에 미치는 영향을 분석하는 것이다. 이를 위하여 문헌 연구를 통해 스마트카의 지각된 위험 요인을 재정립하고 (그림 1)과 같은 연구모형을 설정하였다. 본 연구에서 제시하는 스마트카의 지각된 위험과 관련한 세부 요인은 보안 위험(Security risk)과 프라이버시 위험(Privacy risk), 안전 위험(Safety risk)으로 구성되어 있다.



(그림 1) 연구모형

3.1 보안 위험과 프라이버시 위험

보안은 프라이버시와 밀접한 관련이 있다. 이는 프라이버시라는 개념의 특성 자체가 일반적으로 대중에게 알려지지 않은 정보를 의미하며, 보안은 이러한 프라이버시의 침해를 막아주는 역할을 하기 때문이다[20]. 실례로 정보보호 분야에서의 선행연구에 따르면 소비자의 지각된 보안은 프라이버시 위험에 유의한 영향을 미치는 것으로 나타난 바 있다[21]. 또한, 스마트카 내에 존재하는 인포테인먼트 시스템과 자율주행 시스템은 차량 운전자의 위치 정보 및 민감정보를 다

루기 때문에, 스마트카에 대한 보안 위험은 프라이버시 위험에 유의한 영향을 미칠 것으로 분석할 수 있다. 이에 따라 본 연구는 다음과 같은 가설을 설정하였다.

H1. 스마트카의 지각된 보안 위험은 지각된 프라이버시 위험에 유의한 영향을 미칠 것이다.

3.2 보안 위험과 안전 위험

스마트카에 대한 보안은 운전자의 생명과 직접적인 관계가 있다. 이는 스마트카의 보안 취약점을 이용한 해킹이 발생할 경우 심각한 경우는 차량 제어권을 빼앗기게 되어 운전자에게 직접적인 인적 피해를 일으킬 수 있기 때문이다. 실례로 스마트카에 대한 사람들의 심리를 분석한 Prasetio & Nurliyana (2023)의 연구에 따르면 스마트카의 지각된 보안은 지각된 안전에 유의한 영향을 미치는 것으로 나타났다[22]. 이에 따라 본 연구는 다음과 같은 가설을 설정하였다.

H2. 스마트카의 지각된 보안 위험은 지각된 안전 위험에 유의한 영향을 미칠 것이다.

3.3 보안 위험과 신뢰

스마트카의 보안 위험에 대한 인식은 스마트카의 신뢰에 유의한 영향을 미칠 수 있다. 실례로 정보보호 분야의 선행연구에 따르면 소비자의 지각된 보안 위험은 서비스에 대한 소비자의 신뢰를 낮추는 요인으로 작용하는 것으로 나타났으며[23], 자동차 분야에서의 선행연구에 따르면 스마트카의 보안이 스마트카의 신뢰에 유의한 영향을 미치는 것으로 나타났다[24]. 즉, 보안 위험은 제품이나 서비스의 신뢰를 낮추는 요인으로 작용할 수 있으며, 스마트카의 보안 위험은 스마트카에 대한 운전자의 신뢰를 낮추는 요인이 될 수 있다. 이에 따라 본 연구는 다음과 같은 가설을 설정하였다.

H3. 스마트카의 지각된 보안 위험은 신뢰에 유의한 영향을 미칠 것이다.

3.4 프라이버시 위험과 안전 위험

자율주행기능과 인포테인먼트 기능이 탑재된 스마트카는 운전자의 거래내역 및 활동내역, 위치경로 등을 저장하고 이용한다. 따라서 스마트카 내에 존재하는 프라이버시가 해커에게 유출되었을 경우에는 이에 대한 내용이 악용될 수 있으며 심각한 경우에는 운전자에게 신체적 피해를 입히거나 범죄의 수단으로 활용하는 등 운전자의 안전에 위협을 줄 수 있다[25]. 이에 스마트카 내부에 존재하는 프라이버시는 해킹 등과 같은 방법으로 위험에 노출되면 운전자의 안전이 위험해질 수 있다. 실례로 Prasetio & Nurliyana (2023)의 연구에 따르면 스마트카에 대한 사람들의 지각된 프라이버시 요인은 스마트카에 대한 지각된 안전 요인에 유의한 영향을 미치는 것으로 나타났다[22]. 이에 따라 본 연구는 다음과 같은 가설을 설정하였다.

H4. 스마트카의 지각된 프라이버시 위험은 지각된 안전 위험에 정(+)의 영향을 미칠 것이다.

3.5 프라이버시 위험과 신뢰

정보보호 분야에서의 선행연구에 따르면 정보보호 주체가 개인정보를 잘 보호해 주지 못하면 사람들은 정보보호 주체에 대한 신뢰가 낮아지는 것으로 나타나며, 이와 유사한 맥락 하에 프라이버시 위험과 신뢰와의 관계를 분석한 자동차 분야에서의 선행연구에 따르면 스마트카의 지각된 개인정보 위험은 신뢰에 유의한 영향을 미치는 것으로 나타났다[13]. 즉, 스마트카의 지각된 개인정보 위험은 운전자의 스마트카에 대한 신뢰에 유의한 영향을 미칠 것으로 분석된다. 이에 따라 본 연구는 다음과 같은 가설을 설정하였다.

H5. 스마트카의 지각된 프라이버시 위험은 신뢰에 유의한 영향을 미칠 것이다.

3.6 안전 위험과 신뢰

스마트카 분야에서의 선행연구에 따르면 지각된 안전은 신뢰와 밀접한 관련이 있는 것으로 나타난다. 이는 사람들의 신체적 안전과 밀접한 관련이 있는 자동

차의 특성상 안전이 보장되지 않는 자동차는 사람들이 신뢰하지 않기 때문이다[26]. 실례로 Zhang et al. (2019)의 연구에 따르면 스마트카의 지각된 안전 위험은 신뢰에 유의한 영향을 미치는 것으로 나타난 바 있다[13]. 이에 따라 본 연구는 다음과 같은 가설을 설정하였다.

H6. 스마트카의 지각된 안전 위험은 신뢰에 유의한 영향을 미칠 것이다.

4. 연구방법

4.1 자료수집 및 설문지구성

본 연구는 데이터 수집을 위하여 온라인 설문조사 전문업체인 Open Survey를 통하여 일반인 300명을 대상으로 설문을 실시하였다. 설문 문항은 신뢰성과 타당성이 확보된 기존의 선행연구를 토대로 개발되었으며, 측정문항은 모두 리커드 7점 척도로 구성되었다. 변수들의 측정을 위하며 개발된 설문 문항은 <표 1>과 같다.

<표 1> 측정 문항

변수	측정문항		
Perceived Security Risk	PSE1	나는 스마트카가 해킹으로 인한 보안문제가 발생할 수 있다고 생각한다.	[27]
	PSE2	나는 스마트카의 보안시스템이 개인정보를 지켜주지 못할 것이라 생각한다.	[28]
	PSE3	나는 해커가 스마트카의 정보를 탈취해 갈 수 있다고 생각한다.	
	PSE4	나는 해커가 스마트카 내에 악성 프로그램을 설치하고 해킹할 가능성이 있다고 생각한다.	[29]
Perceived Privacy Risk	PPR1	나는 스마트카가 너무 많은 정보를 수집할까봐 걱정된다.	[13]
	PPR2	나는 스마트카가 허용된 목적과 다르게 나의 개인정보를 사용할까봐 걱정된다.	
	PPR3	나는 스마트카가 나의 허락없이 내 개인정보를 공유할까봐 걱정된다.	
	PPR4	나는 스마트카가 위치추적 및 데이터와 관련한 프라이버시 문제를 일으킬 것이라 생각한다.	[27]
Perceived Safety Risk	PSA1	나는 스마트카를 이용하여 목적지까지 안전하게 가는 것이 어렵다고 생각한다	[30]
	PSA2	나는 스마트카가 안전하지 않다고 생각한다	[13]
	PSA3	스마트카 기술은 나를 안전하게 지켜주지 못할 수 있다고 생각한다	[31]
	PSA4	나는 스마트카가 일반 자동차보다 안전하지 않다고 생각한다	[32]
Trust in Smart Cars	TRS1	전반적으로 나는 스마트카를 신뢰한다.	[4]
	TRS2	나는 스마트카의 보안성을 신뢰한다.	[33]
	TRS3	나는 스마트카의 안전성을 신뢰한다.	
	TRS4	나는 스마트카의 성능을 신뢰한다.	

4.2 분석방법

본 연구는 수집된 데이터의 분석을 위하여 통계 분석 프로그램인 SPSS 23과 Smart PLS 4를 활용하였다. 우선 표본의 인구통계학적 특성을 분석하기 위하여 기술통계 분석을 활용하였으며, 연구모델에 포함된 변수들의 신뢰성과 타당성을 검증하기 위하여 탐색적 요인 분석을 실시하였다. 또한, 가설의 검증을 위하여 부분최소자승법 기반의 구조방정식 분석 기법(PLS-SEM)을 활용하였다.

5. 분석결과

5.1 표본의 인구통계학적 특성

표본의 구체적인 인구통계학적 특성은 <표 2>와 같다. 우선, 응답자들의 성별은 남성 50.0%, 여성 50.0%로 동일한 것으로 나타났으며, 나이는 20대 25.3%, 30대 25.3%, 40대 24.7%, 50대 24.7%인 것으로 나타나 거의 유사한 비율로 수집된 것으로 나타났다. 학력은 고졸 13.7%, 초대졸 13.0%, 대졸 65.0%, 석사졸 8.3%인 것으로 나타났다. 또한, 차량 소유 여부는 소유 66.3%, 미소유 33.7%인 것으로 나타나 차량을 소유한 응답자의 비율이 높은 것으로 나타났으며, 운전경력은 2년 미만 37.7%, 2년 이상 4년 미만 8.0%, 4년 이상 6년 미만 6.3%, 6년 이상 8년 미만 5.0%, 8년 이상 43.0%인 것으로 나타났다.

<표 2> 표본의 인구통계학적 특성

구분		명(%)
성별	남성	150(50.0%)
	여성	150(50.0%)
나이	20대	76(25.3%)
	30대	76(25.3%)
	40대	74(24.7%)
	50대	74(24.7%)
최종학력	고졸	41(13.7%)
	초대졸	39(13.0%)
	대졸	195(65.0%)
	석사	25(8.3%)
차량소유 여부	소유	199(66.3%)
	미소유	101(33.7%)
운전경력	2년 미만	113(37.7%)
	2년 이상 4년 미만	24(8.0%)
	4년 이상 6년 미만	19(6.3%)
	6년 이상 8년 미만	15(5.0%)
	8년 이상	129(43.0%)
총		300(100.0%)

5.2 신뢰성 및 타당성 분석 결과

본 연구모형의 측정 문항에 대한 신뢰성과 타당성을 확인하기 위하여 탐색적 요인 분석을 실시하였다. 우선, 측정모형의 검증을 위해 내적일관성 평가 지표인 Cronbach's alpha와 집중타당도 평가 지표인 평균분산 추출값(Average Variance Extracted; AVE)과 외부적재값을 확인하였다. 일반적으로 Cronbach's alpha는 0.7 이상일 때 내적일관성이 확보된 것으로 보며[34], AVE 값은 0.5 이상[35], 외부적재값은 0.7 이상일 때 집중타당성이 확보된 것으로 본다[36]. <표 3>에 따르면 모든 변수가 기준치를 상회하는 것으로 내적일관성과 집중타당성이 확보된 것으로 나타났다.

<표 3> 내적일관성 및 집중타당성 검증 결과

변수	항목	외부적재값	α	AVE
Perceived Security Risk	PPE1	0.861	0.903	0.777
	PPE2	0.816		
	PPE3	0.930		
	PPE4	0.913		
Perceived Privacy Risk	PPR1	0.880	0.906	0.780
	PPR2	0.915		
	PPR3	0.901		
	PPR4	0.836		
Perceived Safety Risk	PSA1	0.773	0.883	0.742
	PSA2	0.921		
	PSA3	0.893		
	PSA4	0.852		
Trust in Smart Cars	TRS1	0.902	0.916	0.787
	TRS2	0.947		
	TRS3	0.953		
	TRS4	0.727		

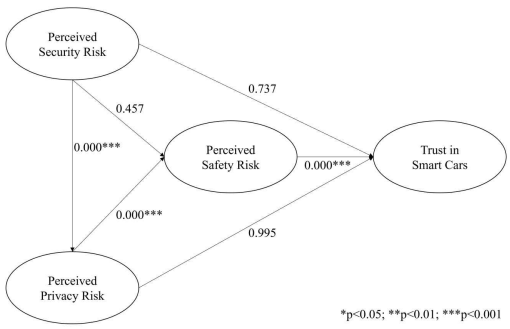
다음으로, 측정문항의 판별타당성을 검증하기 위하여 Fornell-Larcker criterion를 확인하였다. Fornell-Larcker criterion에 따르면 각 개별 요인의 AVE 제곱근 값이 종과 횡의 잠재변수들보다 크면 판별타당성이 확보된 것으로 보며[35], <표 4>는 모두 기준치를 상회하는 것으로 확인되어 판별타당성에도 문제가 없는 것으로 나타났다.

<표 4> 판별타당성 검증 결과

변수	PPR	PSA	PSE	TRS
PPR	0.883			
PSA	0.346	0.862		
PSE	0.741	0.223	0.881	
TRS	-0.170	-0.298	-0.139	0.887

5.3 가설 검증 결과

본 연구는 가설을 검증하기 위하여 300개의 샘플에 대한 부트스트래핑(Boot Strapping) 재표본 기법(n=5000)을 활용하였다. 이를 통해 검증한 가설의 결과는 (그림 2)와 같다. 우선, 지각된 보안 위험은 지각된 프라이버시 위험(경로계수=0.741, t=22.818, p<0.001)에 유의한 영향을 미치는 것으로 나타났으나, 지각된 안전 위험(경로계수=-0.073, t=0.743)과 신뢰(경로계수=-0.032, t=0.336)에는 유의한 영향을 미치지 않는 것으로 나타났다. 또한, 지각된 프라이버시 위험은 지각된 안전 위험(경로계수=0.0400, t=4.073, p<0.001)에 유의한 영향을 미치는 것으로 나타났으나, 신뢰(경로계수=-0.001, t=0.006)에는 유의한 영향을 미치지 않는 것으로 나타났다. 마지막으로, 지각된 안전 위험은 신뢰(경로계수=-0.341, t=4.580, p<0.001)에 유의한 영향을 미치는 것으로 나타났다.



(그림 2) 가설 검증 결과

6. 논의 및 결론

본 연구의 목적은 지각된 위험 이론을 활용하여 보안과 프라이버시 위험이 운전자의 스마트카 신뢰에 미치는 영향을 분석하는 것이다. 분석결과를 요약하면 다음과 같다 첫째, 지각된 보안 위험은 지각된 프라이버시 위험에 유의한 영향을 미치는 것으로 나타났다. 이는 스마트카 내에 존재하는 운전자의 위치 정보 및 민감정보의 보호를 위하여 운전자들은 스마트카의 보안이 중요하다고 생각하는 것으로 해석할 수 있다.

둘째, 지각된 보안 위험은 지각된 안전 위험과 신뢰에 유의한 영향을 미치지 않는 것으로 나타났다. 이는 스마트카의 보안 요인이 안전 요인에 유의한 영향을 미친다는 기존의 연구[22]와 스마트카의 보안이 스마트카의 신뢰에 유의한 영향을 미친다는 기존의 연구결과[24]를 부정하는 결과이다. 이는 자율주행기술이 고도화되지 않은 스마트카의 특성상 아직까지는 스마트카의 보안 위험이 프라이버시 위험과 스마트카 신뢰에 영향을 미치지 못한 것으로 분석된다. 그러나 기술통계 결과, 스마트카의 보안에 대한 운전자의 우려는 높은 것으로 나타났기 때문에 자율주행 레벨3 이상의 스마트카가 상용화되는 시기에는 지금과 다를 수 있어 이에 따른 후속 연구의 필요할 것으로 보인다.

셋째, 지각된 프라이버시 위험은 지각된 안전 위험에 유의한 영향을 미치는 것으로 나타났다. 이는 스마트카의 지각된 프라이버시 요인이 지각된 안전 요인에 유의한 영향을 미친다는 기존의 연구결과[24]를 지지하는 결과이며, 운전자들은 거래내역 및 활동내역, 위치경로와 같은 개인정보의 유출이 안전과 밀접한 관련이 있다는 여기는 것으로 해석할 수 있다.

넷째, 지각된 프라이버시 위험은 신뢰에 유의한 영향을 미치지 않는 것으로 나타났다. 이는 최근 연속적으로 발생하는 개인정보 유출이 개인정보에 대한 사람들의 인식을 무뎌지게 만들었을 수도 있으며, 이에 대한 관련 연구는 후속 연구를 통해 검증될 필요가 있다.

다섯째, 지각된 안전 위험은 신뢰에 유의한 영향을 미치는 것으로 나타났다. 이는 스마트카의 지각된 안전 위험이 신뢰에 유의한 영향을 미친다는 기존의 연구결과를 지지하는 결과이며[13], 스마트카의 신뢰도를 향상시키기 위해서는 스마트카의 안전에 대한 인식이 개선되어야 함을 의미한다.

본 연구의 학술적 및 실무적 의의는 다음과 같다. 우선, 학술적 측면에서 본 연구는 자율주행기술이 탑재된 스마트카의 기술이 가속화되는 시점에서 스마트카의 수용의도에 기초가 되는 스마트카의 신뢰 형성 요인을 분석하였다는 점에서 의의가 있다. 또한, 스마트카에 대한 기존의 선행연구들은 단순히 기술수용이론과 같은 전통적인 이론들을 활용한 연구만이 주를 이뤘는데 본 연구는 지각된 위험 요인을 스마트카의 특성에 맞게 재분류하여 분석하였다는 점에서도 의의

가 있다. 또한, 기존의 선행연구들은 스마트카의 보안이나 프라이버시, 안전 요인이 스마트카의 신뢰에 미치는 영향에 대해 포괄적으로 살펴본 연구가 부족하였는데, 본 연구에서는 이들 요인의 실증적 관계에 대해 고찰하였다는점에서 학술적 의의가 있다. 다음으로, 실무적 측면에서는 스마트카의 신뢰 형성을 위해서는 운전자의 지각된 안전 요인을 고려하는 것이 중요하다는 점을 확인하였으며, 이는 향후 스마트카의 인식 제고는 물론 스마트카 보급을 위한 정책의 기초자료로 활용될 수 있다는 점에서 의의가 있다. 그러나 본 연구의 한계로 아직 스마트카가 확산되지 못한 시점의 분석이다 보니 향후 활성화 시점에 재연구를 통한 분석 결과의 확인 및 논의의 확장은 필요할 것이다.

참고문헌

[1] 장승주, “자율 주행 자동차 관련 SW기술 동향”, 정보와 통신, 제33권, 제4호, pp. 27-33, 2016.

[2] Kyriakidis, M., Happee, R., & de Winter, J. C., “Public opinion on automated driving: Results of an international questionnaire among 5000 respondents”, Transportation research part F: traffic psychology and behaviour, Vol. 32, pp. 127-140, 2015.

[3] Luo, X., Li, H., Zhang, J., & Shim, J. P., “Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services”, Decision support systems, Vol. 49, No. 2, pp. 222-234, 2010.

[4] Choi, J. K., & Ji, Y. G., “Investigating the importance of trust on adopting an autonomous vehicle”, International Journal of Human-Computer Interaction, Vol. 31, No. 10, pp. 692-702, 2015.

[5] Yuen, K. F., Cai, L., Qi, G., & Wang, X., “Factors influencing autonomous vehicle adoption: An application of the technology acceptance model and innovation diffusion theory”, Technology Analysis & Strategic Management, Vol. 33, No. 5, pp. 505-519, 2021.

[6] Park, J., Nam, C., & Kim, H. J., “Exploring the key services and players in the smart car marke”t. Telecommunications Policy, Vol. 43, No. 10, pp. 101819, 2019.

[7] 최원석, "국제 학술대회를 중심으로 자동차 보안 기술 동향", 通信情報保護學會誌, 제30권, 제6호, pp. 91-99, 2020.

[8] Jing, P., Xu, G., Chen, Y., Shi, Y., & Zhan, F., “The determinants behind the acceptance of autonomous vehicles: A systematic review”. Sustainability, Vol. 12, Np. 5, pp. 1719, 2020.

[9] Zauner, A., Koller, M., & Hatak, I., “Customer perceived value—Conceptualization and avenues for future research”, Cogent psychology, Vol. 2, No. 1, pp. 1061782, 2015.

[10] Bauer, R. A., “Consumer behavior as risk taking”, Marketing: Critical perspectives on business and management, pp. 13-21, 1967.

[11] Wang, S., Wang, J., Li, J., Wang, J., & Liang, L., “Policy implications for promoting the adoption of electric vehicles: Do consumer’s knowledge, perceived risk and financial incentive policy matter?”, Transportation Research Part A: Policy and Practice, Vol. 117, pp. 58-69, 2018.

[12] Thilina, D. K., & Gunawardane, N., “The effect of perceived risk on the purchase intention of electric vehicles: an extension to the technology acceptance model”, International Journal of Electric and Hybrid Vehicles, Vol. 11, No. 1, pp. 73-84, 2019.

[13] Zhang, T., Tao, D., Qu, X., Zhang, X., Lin, R., & Zhang, W., “The roles of initial trust and perceived risk in public’s acceptance of automated vehicles”, Transportation research part C: emerging technologies, Vol. 98, pp. 207-220, 2019.

[14] Kenesei, Z., Ásványi, K., Kökény, L.,

Jászberényi, M., Miskolczi, M., Gyulavári, T., & Syahrivar, J., “Trust and perceived risk: How different manifestations affect the adoption of autonomous vehicles”, Transportation research part A: policy and practice, Vol. 164, pp. 379-393, 2022.

[15] Nixon, P. A., Wagealla, W., English, C., & Terzis, S., “Security, privacy and trust issues in smart environments”, Smart Environments: Technologies, Protocols, and Applications, pp. 249-270, 2004.

[16] Mayer, R. C., Davis, J. H., & Schoorman, F. D., “An integrative model of organizational trust”, Academy of management review, vol. 20, Np. 3, pp. 709-734, 1995.

[17] Dirsehan, T., & Can, C., “Examination of trust and sustainability concerns in autonomous vehicle adoption”, Technology in Society, Vol. 63, pp. 101361, 2020.

[18] Modliński, A., Gwiaździński, E., & Karpińska-Krakowiak, M., “The effects of religiosity and gender on attitudes and trust toward autonomous vehicles”, The Journal of High Technology Management Research, Vol. 33, No. 1, pp. 100426, 2022.

[19] Chan, W. M., & Lee, J. W. C., “5G connected autonomous vehicle acceptance: The mediating effect of trust in the technology acceptance model”, Asian Journal of Business Research, Vol. 11, No. 1, pp. 40-60, 2021.

[20] Liu, N., Nikitas, A., & Parkinson, S., “Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach”, Transportation research part F: traffic psychology and behaviour, Vol. 75, pp. 66-86, 2020.

[21] Shin, D. H., “The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption”, Interacting with computers, Vol. 22, No. 5, pp. 428-438, 2010.

[22] Prasetio, E. A., & Nurliyana, C., “Evaluating perceived safety of autonomous vehicle: The influence of privacy and cybersecurity to cognitive and emotional safety”, IATSS Research, Vol. 47, No. 2, pp. 160-170, 2023.

[23] Fogel, J., & Nehmad, E., “Internet social network communities: Risk taking, trust, and privacy concerns”, Computers in human behavior, Vol. 25, No. 1, pp. 153-160, 2009.

[24] Kaur, K., & Rampersad, G., “Trust in driverless cars: Investigating key factors influencing the adoption of driverless cars”, Journal of Engineering and Technology Management, Vol. 48, pp. 87-96, 2018.

[25] Taeihagh, A., & Lim, H. S. M., “Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks”, Transport reviews, Vol. 39, No. 1, pp. 103-128, 2019.

[26] Nordhoff, S., Stapel, J., He, X., Gentner, A., & Happee, R., “Perceived safety and trust in SAE Level 2 partially automated cars: Results from an online questionnaire”, Plos one, Vol. 16, No. 12, pp. e0260953, 2021.

[27] Mack, E. A., Miller, S. R., Chang, C. H., Van Fossen, J. A., Cotten, S. R., Savolainen, P. T., & Mann, J., “The politics of new driving technologies: Political ideology and autonomous vehicle adoption”, Telematics and Informatics, Vol. 61, pp. 101604, 2021.

[28] Klobas, J. E., McGill, T., & Wang, X., “How perceived security risk affects intention to use smart home devices: A reasoned action explanation”, Computers & Security, Vol. 87, pp. 101571, 2019.

[29] Park, C., Kim, Y., & Jeong, M., “Influencing factors on risk perception of IoT-based home energy management services”, Telematics and

Informatics, Vol. 35, No. 8, pp. 2355-2365, 2018.

[30] Koul, S., & Eydgahi, A., “The impact of social influence, technophobia, and perceived safety on autonomous vehicle technology adoption”, Periodica Polytechnica Transportation Engineering, Vol. 48, No. 2, pp. 133-142. 2020.

[31] Jabbari, P., Auld, J., & MacKenzie, D., “How do perceptions of safety and car ownership importance affect autonomous vehicle adoption?”, Travel behaviour and society, Vol. 28, pp. 128-140, 2022.

[32] Ljubi, K., & Groznik, A., “Role played by social factors and privacy concerns in autonomous vehicle adoption. Transport policy, Vol. 132, pp. 1-15, 2023.

[33] Ribeiro, M. A., Gursoy, D., & Chi, O. H., “Customer acceptance of autonomous vehicles in travel and tourism”, Journal of Travel Research, Vol. 61, No. 3, pp. 620-636, 2022.

[34] Nunnally, J.C., & Bernstein, I.H., ‘Psychometric Theory (3rd Ed.)’. McGraw-Hill., 1994.

[35] Fornell, C., & Larcker, D. F., “Structural equation models with unobservable variables and measurement error: Algebra and statistics”, Journal of Marketing Research, Vol. 18, No. 3, pp. 382-388, 1981.

[36] Hair, J. F., Ringle, C. M., & Sarstedt, M., “PLS-SEM: Indeed a silver bullet. Journal of Marketing theory and Practice”, Vol. 19, No. 2, pp. 139-152, 2011.

〔저자소개〕

권 순 범 (Soonbeom Kwon)
2022년 2월 단국대학교 법학과 학사
2023년 8월 단국대학교 IT법학협동과정 석사
2023년 9월 ~ 단국대학교 과학기술정책융합학과 박사과정
email : kwonsb777@naver.com

이 환 수 (Hwansoo Lee)
2005년 2월 연세대학교 산업정보시스템 공학과 석사
2014년 2월 KAIST 기술경영학과 박사
2017년 ~ 단국대학교 산업보안학과 교수
email : hanslee992@gmail.com