

스마트시티 위험요인과 저항에 관한 연구*

박 현 애*, 유 영 천**, 이 환 수***

요 약

스마트시티는 기존 도시의 문제를 해결하고 새로운 부가 가치를 창출할 것으로 큰 기대를 받고 있으나, 보안위험 증가에 우려 또한 증가하고 있다. 보안위험 인식에 따른 스마트시티에 대한 부정적 태도는 4차산업혁명 기술 활성화 및 스마트시티의 발전을 위해서도 개선해야 하는 문제이다. 이에 본 연구는 지각된 위험 이론과 사용자 저항이론을 바탕으로 스마트시티 내 위험요인과 스마트시티 저항 태도 간 관계를 통계적으로 분석하였다. 288명의 연구 표본을 대상으로 한 실증 분석결과에 따르면, 보안 위험, 사회적 위험, 신체적 위험요인은 스마트시티 저항에 직접적인 영향을 미치는 반면, 경제적, 성능, 사생활 침해에 대한 위험은 유의미한 영향이 없는 것으로 나타났다. 또한, 보안위험이 다른 위험에 선행요인으로 작용할 수 있다는 것을 검증하였으며, 스마트시티 환경에서는 사생활 침해 위험과 보안 위험에 대해 구분해서 논의할 필요성이 있음을 확인하였다. 본 연구는 일반인들 관점에서 스마트시티 인식에 부정적인 영향을 미치는 위험요인을 논의함으로써, 스마트시티 활성화를 위해 보안 및 안전 문제와 더불어 사회적 교류를 위한 정책적 방안 마련이 필요함을 보여준다.

A Study on Smart City Risk Factors and Resistance

Hyunae Park*, Youngcheon Yoo**, Hwansoo Lee***

ABSTRACT

Smart City is highly anticipated to solve the problems of existing cities and create new added value, but there is also increasing concern about security risks. The negative view of smart city according to security risk awareness is a problem that needs to be improved in order to activate the fourth industrial revolution technology and develop smart city. This study examined risk factors in smart cities based on perceived risk and user resistance theory, and empirically analyzed the relationship with resistance attitudes. According to the empirical analysis with 288 research samples, security, social, and physical risk factors directly affect smart city resistance, while financial, performance, and privacy risk have no significant effect. In addition, it was verified that the security risk can be an antecedent factor for other risk factors, and it was confirmed that it is required to separately discuss the security and privacy risk in the smart city environment. This study shows that it is necessary to prepare policy supports for social interactions as well as security and physical safety issues in order to activate smart city by discussing the risk factors that negatively affect smart city perception from the public's point of view.

Key words : Smart City, Perceived Risk, Security Risk, User Resistance

접수일(2020년 5월 22일), 수정일(1차: 2020년 6월 12일)

계재확정일(2020년 6월 25일)

★ This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A3A2008438). 이 연구는 산업통상자원부 산업혁신인재성장지원사업의 지원을 받았다.

* 단국대학교 IT법학협동과정 석사과정(1저자)

** 단국대학교 IT법학협동과정 석사과정(공동저자)

*** 단국대학교 산업보안학과 교수(교신저자)

1. 서 론

전통적인 도시의 문제를 해결하고 혁신적인 서비스 제공을 위한 방안으로 스마트시티라는 개념이 등장하였다. 스마트시티는 미래학자들이 예측한 새로운 도시 유형으로 컴퓨터 기술의 발달로 도시 구성원들 간의 네트워크가 완벽하게 갖춰져 있고 교통망이 잘 연결되는 것을 주요 특징으로 한다. 연구자들은 현재 미국의 실리콘 밸리를 모델로 삼아 앞으로 다가올 스마트 시티의 모습을 그려 나가고 있다[1].

스마트시티는 도시문제를 해결하고 새로운 부가치를 창출할 것으로 기대되어왔다. 그러나 스마트시티에 대한 긍정적인 평가에 반해 부정적인 평가 또한 제기되고 있는 상황이다. 다양한 영역이 융합되어 공격 침입 경로가 많아지면서 보안 위협이 증가하기 시작하였으며[2], 정보시스템 오작동 문제, 개인정보 공개 문제에 대한 우려 수준 또한 높은 것으로 나타났다[3]. 스마트시티의 통합 시스템에 개인정보를 제공하면서 실제 사생활 침해 문제 또한 발생하는 등 부정적 시선도 증가하고 있다[4]. 이러한 스마트시티의 보안위험에 대한 부정적 평가는 스마트시티 자체에 대한 저항 인식을 형성하고 이는 스마트시티 주거 의도 및 활성화에 부정적 영향을 미칠 수 있다. 그러나 기존 연구들은 스마트시티 국내외 동향, 스마트시티 서비스, 스마트시티 발전 방향 등과 같은 현황 및 긍정적 내용에 대한 논의가 대다수이며, 보안에 대한 접근은 사이버보안에 관한 기술적 내용으로 이루어져 있다. 이처럼, 스마트시티에서 발생 가능한 보안위험의 영향을 체계적으로 접근하여 스마트시티 자체에 대한 저항 인식을 분석한 연구는 부족하다. 기존 연구에 따르면 저항 행동에는 서비스의 특성에 따라 다양한 위험요인들이 영향을 미칠 수 있다[5]. 스마트시티는 스마트 홈 및 자율주행 자동차 등 생활과 밀접한 관련이 있기 때문에 기존의 서비스와 비교했을 때 저항 요인이 다르게 나타날 수 있다.

이에 본 연구에서는 Bauer(1960)의 지각된 위험이론을 바탕으로 스마트시티 내 발생 가능한 위험요인을 체계화하고, 사용자 저항이론 관점에서 위험요인들은 저항 태도에 영향을 미칠 것이라는 가설에 대한 실증 분석을 수행하였다. 본 연구는 스마트 위험요인

과 저항 태도의 관계를 분석함으로써 스마트시티 활성화를 위해 우선적으로 개선되어야 하는 위험요인들을 제시하는데 목적이 있다.

2. 선행연구

2.1 스마트시티

스마트시티는 ‘도시의 경쟁력과 삶의 질의 향상을 위하여 건설·정보통신기술 등을 융·복합하여 건설된 도시기반 시설을 바탕으로 다양한 도시서비스를 제공하는 지속 가능한 도시(스마트 도시법 제2조)이다. 스마트시티는 각종 도시문제를 해결할 뿐만 아니라 4차 산업혁명의 융·복합 기술을 적용하여 혁신적인 산업 생태계를 구축하고 삶의 질을 높이는 미래 성장 동력으로서 큰 역할을 할 것으로 보인다[6].

우리나라는 송도, 청라, 영종 3구역으로 구성된 인천경제 자유 구역, 고양시 개방형 스마트시티, 부산 에코델타시티(EDC)와 세종시(5-1)를 대표적인 스마트 시티로 지정하고 각 지역에 추진단을 설립하는 등 스마트시티 조성에 속도를 내고 있다. 최근 2020년 2월 19일에는 주차 플랫폼 ‘아이파크’를 스마트시티의 주차 공유 사업자로 선정하면서 ‘스마트시티 챌린지’를 통해 민간업체와 협력하여 스마트시티를 점차 확산해나가고 있다[7]. 해외의 경우에는 ‘지속 가능한 발전을 위한 환경 도시 계획’을 기초로 2006년부터 EU 최초의 스마트시티를 추진하기 시작한 네덜란드의 암스테르담, 사용자 주도의 개방형 리빙 랩을 바탕으로 활성화되고 있는 헬싱키 등이 대표적인 사례이다[6].

스마트시티는 교통, 환경, 생활·복지, 경제, 안전, 에너지 등 다양한 분야에서 ICT(Information and Communication Technology) 및 빅데이터 등 신기술을 접목한 서비스를 제공하고 있다<표 1>. 교통 분야에는 자율주행 및 무인 셔틀 서비스, 스마트 주차 서비스가 있으며 운전자에게 주변 교통상황과 급정거, 낙하물 등의 사고 위험 정보를 실시간으로 제공하는 차세대 지능형 교통시스템(C-ITS) 서비스가 있다[9]. 치안 분야로는 비상 대응 시스템, 치안관리용 드론, CCTV가 있으며 의료분야로는 스마트 의료기기, 의료 데이터 관리 센터가 있다. 이외에도 스마트 대피 시스템, 지

능형 도시 모니터링, 에너지 수집 센서 등이 있어서 스마트시티 내에서 더욱 편리한 생활을 보장하기도 한다.

<표 1> 스마트시티 서비스 종류[8]

구분	내용
교통	자율주행 및 무인 셔틀 서비스, 스마트 주차 서비스, 차세대 지능형 교통 시스템 (C-ITS)
치안	비상대응시스템, 치안관라용 드론, CCTV
의료	스마트 의료기기, 의료 데이터 관리 센터
안전	스마트 대피 시스템, 지능형 도시 모니터링
에너지	에너지 수집 센서, 관리 시스템
도시 데이터	빅데이터 처리 시스템

2.2 스마트시티 위험요인

스마트시티는 앞서 제시한 것과 같이 정보통신기술을 바탕으로 광범위한 서비스를 운영하고 있기 때문에 보안위험을 포함한 다양한 형태의 위험요인들이 존재한다. 스마트시티에서는 크게 교통, 치안, 의료, 에너지, CCTV·센서, 도시 데이터의 6가지 분야에서 보안 위험이 발생할 수 있다. 교통 분야의 경우, 자율주행 및 무인 셔틀 서비스 등 차량 사물 통신, 차세대 지능형 시스템이 해킹당하여 교통마비가 발생한다거나 차량의 제어권을 탈취당하여 교통 혼란을 초래할 수 있다. 치안 분야의 경우에는 자연재해 및 안전·재난 문제를 관리, 모니터링하는 센서가 해킹으로 경보 시스템 오작동과 시스템 마비를 일으킬 수도 있다. 의료 분야의 경우, 의료정보가 유출된다거나 스마트 의료기기가 해킹당하여 직접적으로 사람에게 피해를 발생시킬 수 있으며, 에너지 분야의 경우 스마트시티의 에너지 수집 센서, 관리 시스템이 해킹당해 작동을 멈추거나 공장에서 생산하는 유해한 물질에 시민들이 노출될 수도 있다. 도시 데이터 분야의 경우, 스마트시티 내 데이터 시스템이 해킹당하여 민감한 정보가 유출된다거나 변조될 수도 있다[10]. 이처럼, 스마트시티는 다양한 보안 위험들이 발생할 수 있는데 기존의 지각된 위험 이론을 기반으로 발생 가능한 위험을 설

명할 수 있다.

지각된 위험 이론은 오랜 시간 사회과학 연구에서 활용된 이론으로[10][11], 마케팅, 경제학, 심리학, 공공정책 및 금융 등의 다양한 분야에서 활용되면서 세분화되기 시작하였다[12]. Cunningham(1967)은 성능 위험, 경제적 위험, 기회/시간 위험, 안전성 위험, 사회적 위험, 심리적 위험이라는 6가지 위험으로 위험요인을 나누었으며[13], Jacoby & Kaplan(1972)은 지각된 위험을 경제적 위험, 성능 위험, 신체적 위험, 심리적 위험, 사회적 위험, 시간적 위험의 6가지 유형으로 나누었다[14]. 이후 다양한 연구들에서 지각된 위험의 요인들을 세분화하였는데 공통적으로 활용되는 위험요인들을 정리하면 <표 2>와 같다.

<표 2> 지각된 위험의 종류[15][16][17]

구분	내용
경제적 위험 (Financial Risk)	초기 구매 비용 및 후속 유지비용과 관련된 잠재적 비용에 대한 위험
성능 위험 (Performance Risk)	설계 및 광고된 것처럼 작동되지 않거나 고장의 가능성 때문에 원하는 효과를 가져오지 못할 위험
사회적 위험 (Social Risk)	사회적 집단에서의 개인의 지위에 대한 잠재적인 손실에 대한 위험
신체적 위험 (Physical Risk)	사고로 인해 질병 등 개인의 신체에 해를 끼칠 수 있는 위험
심리적 위험 (Psychological Risk)	구매 목표를 성취하지 못했을 때 잠재적 자존감의 상실에 따른 위험
시간적 위험 (Time Risk)	구매 결정 및 잘못된 구매에 따른 시간 낭비에 대한 위험
사생활 침해 위험 (Privacy Risk)	개인정보에 대한 통제와 관련된 잠재적인 손실 위험
보안 위험 (Security Risk)	시스템 취약성이나 외부의 공격으로 인해 데이터 보호에 영향을 미칠 수 있는 기술적 위험
기술 위험 (Technology Risk)	신뢰할 수 없는 장치 또는 기술로 인해 발생할 수 있는 잠재적 손실에 관한 위험

스마트시티에서 발생할 수 있는 위험 사례들과 스

마트시티를 지원하는 서비스 및 기술 등의 특징에 비추어 보면 스마트시티 내에서 발생할 수 있는 위험요인은 경제적 위험, 성능 위험, 사회적 위험, 신체적 위험, 사생활 침해 위험, 보안위험으로 정리할 수 있다. 경제적 위험의 경우, 스마트시티가 일반 거주지보다 비용이 높다는 점, 성능 위험의 경우, 시스템 오작동 및 마비가 발생할 수 있다는 점, 사회적 위험의 경우, 스마트시티가 다각화된 인공지능 서비스를 지원하기 때문에 일반 사람들과는 멀어질 수 있다는 측면에서 발생 가능하다. 신체적 위험의 경우, 의료기기 해킹으로 신체에 해를 끼칠 수 있다는 점과 사생활 침해의 경우, 수집한 데이터 중 민감한 정보가 유출될 수 있다는 점에서 발생할 수 있다. 보안위험의 경우, 스마트시티 내 다양한 정보시스템들이 존재하고 이들이 해킹당할 수 있다는 점에서 중요한 위험요인이다. 그러나 스마트시티와 관련해서 심리적 위험의 경우 사회적 위험이나 사생활 침해 위험과 유사성이 높고 기술 위험은 보안위험이나 성능 위험과 공통된 부분이 많아 별도의 위험 요인으로 간주하기에는 한계가 있다.

스마트시티의 초기 거주 비용이나 매달 관리 비용이 일반 거주지보다 지나치게 높을 수 있다는 점 등이 경제적 위험요인으로 볼 수 있다. 예를 들어 부산 에코델타 스마트시티의 경우, LWP(Learn Work and Play) 융합 커뮤니티 공간, 스마트 정수장, 연료전지 발전소, 스마트 스쿨, 스마트 쇼핑 단지, 헬스케어·빅데이터 센터, 스마트 주차장, 스마트 휴게시설 등의 다양한 편의시설 구축을 목표로 하고 있어 초기 구축 비용부터 관리 비용이 일반 거주지보다 높을 것으로 예상된다. 이러한 비용은 사람들에게 경제적 위험 인식을 증가시킬 수 있다[18].

성능 위험에 관한 요인으로는 각종 기기 및 서비스에서 오작동이 발생하여 거주자들이 불편을 겪을 수 있고, 서비스가 기대한 것보다 만족스럽지 않을 수 있다는 점을 들 수 있다. 스마트시티에서는 다양한 분야에서 자동화된 서비스를 활용하고 있는데, 예를 들어 냉난방 서비스 및 의료시스템 등의 오작동은 오히려 사용자들의 불편을 초래할 수 있는 요인이 된다[18].

사회적 위험에 관한 요인으로는, 스마트시티 내 생활로 인해 사람들과 소통하는데 어려워지거나 사회적 단절이 이루어져 스마트시티에 거주자를 부정적으로

바라볼 수 있다는 점을 들 수 있다. 스마트시티는 이동 보조 로봇, AI(Artificial Intelligence) 기반 돌봄 로봇, 케어 로봇, 가정 교육 로봇 등을 통해 인공지능 서비스를 지원한다[18]. 로봇 서비스가 편리할 수는 있으나, 모든 것을 인공지능을 통해 해결하기 때문에 실제 사람들과는 거리가 멀어질 수 있다는 점에서 사회적 위험이 존재할 수 있다.

스마트시티 내 장비 및 보안시스템은 해킹의 주요 목표가 될 수 있다는 점에서 보안위험은 발생 가능성이 높다. IoT(Internet of Things) 기기가 증가할수록 개인정보, 의료정보 등이 노출될 수 있는 데이터의 양도 증가하기 때문에 IoT 기기에 보안 기술이 적용되어 있어야 하지만 IoT 기기는 가격 대비 CPU, 메모리 등의 성능 제한으로 인해 보안 기술을 적용하지 못하는 취약성을 갖고 있다[19]. 또한, IoT를 위한 통신 네트워크는 과도한 네트워크 데이터 암호화 프로토콜(Secure Sockets Layer: SSL)에 의존하여 보안에 취약하다[20]. 이러한 기술적 취약성으로 인해 보안위험은 초기 스마트시티에서 발생 가능성이 높은 위험 중 하나이다.

신체적 위험은 전통적인 주거환경에 정보통신기술이 융합되면서 기존 위험보다 더 강화되어 발생 가능한 위험으로 고려할 수 있다[21]. 스마트시티 내 전자기기를 활용하여 테러 및 범죄를 일으킨다면 안전을 위협할 수도 있고, 도시 냉난방 서비스 및 의료시스템이 해킹되어 건강에 직접적으로 피해를 미칠 수도 있다. 특히 스마트 정수장, 연료전지발전소와 같은 기반 시설이 테러에 노출된다면 큰 인명피해로 이어질 수 있다[18].

사생활 침해에 관한 요인으로는 민감한 개인정보가 수집·유출·남용될 수 있고, 사생활이 감시당할 수 있다는 점을 들 수 있다. 스마트시티는 미래형 의료데이터 관리센터, 데이터 시스템을 구축하고 있기에 거주자의 민감한 개인정보, 의료정보들이 수집될 수 있으며 이 또한 유출 및 남용의 가능성이 있다. 2018년 싱가포르에서 의료그룹의 데이터베이스가 해킹당하였고, 2017년 미국 병원 네트워크인 아트리움 헬스(Atrium Health)에서 데이터베이스가 해킹당해 265만 명의 개인정보가 유출되기도 하였다[10].

2.3 스마트시티 저항

사용자 저항이론은 정보시스템 사용자가 사용 환경과 시스템과의 상호작용을 통해 위험을 지각하게 되면 이는 곧 저항행위로 이어지는 사용자 행태를 의미한다[22]. 사용자 저항은 새로운 서비스가 도입되면서 생기는 변화에 대한 사용자의 부정적인 반응 및 행위라고 할 수 있다. 이론에 따르면 사용자들은 조직 환경이나 대상 시스템과의 상호작용을 통해 위험을 지각하면 이는 저항행위로 이어진다. 이러한 저항행위의 특징은 상황 요인에 영향을 미치는 순환구조를 이룬다는 것이다[22].

사용자 저항이론은 스마트시티 저항을 이해하는 데에도 활용 가능하다. 위험을 지각하면 저항행위가 나타난다는 사용자 저항이론에 따라 스마트시티 위험요인들에 대한 논의는 스마트시티 확산을 이해하는데 도움이 될 수 있다. 이성근·김덕근·안성조(2015)는 주거지 선택 문제에는 사회적 요인(이웃관계, 안정성, 프라이버시), 기능적 요인(주택 구조 및 내부 성능), 환경적 요인(접근성, 교육 환경), 상황적 요인(거주 기간, 가족 수), 경제적 요인(주택비용), 이미지 요인, 경기 요인으로 나뉠 수 있다고 제시하였다[23]. 이처럼 주거 선택에 영향을 미치는 요인들은 지각된 위험 이론에서 논의하는 내용들과 대부분 유사한 것을 확인할 수 있다. 스마트시티의 상대적으로 높은 비용은 주거지 선택요인의 경제적 요인에 적용될 수 있을 것이고, 스마트시티에서 발생할 수 있는 기기 오작동은 기능적 요인에 적용될 수 있다. 이웃 관계가 멀어진다거나 신체에 해를 입힐 수 있음은 사회적 요인에 포함될 수 있고, 개인정보가 유출되거나 보안시스템이 해킹되는 것은 사회적 요인 및 기능적 요인에 적용될 수 있다. 이러한 요인으로 인해 스마트시티 내에서 부정적인 결과나 성과의 불확실성 지각된 부작용이 크게 나타난다면, 이에 대한 내용은 곧 스마트시티 위험요인과 이어질 수 있고, 스마트시티 거주 자체에 대한 부정적인 결과를 초래할 수 있다.

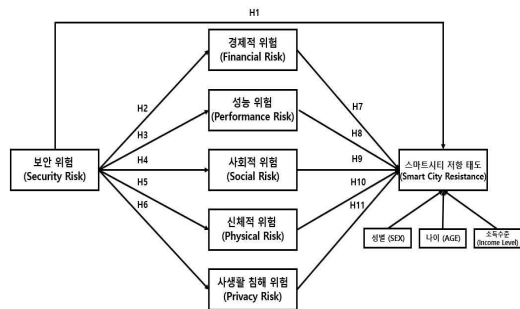
선택을 위한 의사결정을 내릴 때 사람들은 최대한 손실을 적게 입으려 하는 경향이 있다. 이런 점에서 지각된 위험은 사람들의 수용이나 저항행동을 설명할 수 있는 유용한 변수가 될 수 있다[24]. 마찬가지로,

스마트시티에서도 경제적, 성능, 사회적 위험 등이 미치는 영향을 이해하게 된다면 주거지로써 스마트시티를 선택하지 않는 저항 행동이 나타날 수 있다. 따라서, 본 연구에서는 스마트시티 내에서 부정적인 영향을 미칠 수 있는 위험요인을 우선 정리함으로써 정리된 요인과 저항 행동과 관계를 살펴보고자 한다.

3. 연구방법론

3.1 연구모형 및 가설

본 연구에서는 지각된 위험 이론과 사용자 저항이론을 바탕으로, 스마트시티 내에서 발생할 수 있는 위험이 저항 태도에 미치는 영향을 분석하는 연구모형을 제시하였다(그림 1). 스마트시티에서 발생할 수 있는 위험 중 보안위험은 경제적 위험, 성능 위험, 사회적 위험, 신체적 위험, 사생활 침해 위험에 직접적 영향을 미칠 수 있을 것으로 예상하여 연구모형을 설계하였다. 보안위험이 클수록 다른 위험요인들에 영향을 끼칠 것이라는 가설과 함께 이러한 위험요인들이 스마트시티 저항 태도에 영향을 미칠 것이라는 가설을 세워 이를 실증적으로 분석하였다.



(그림 1) 연구모형

보안위험이란, 스마트시티 내 장비가 해킹을 당하고 공유되는 데이터가 외부로부터 공격을 받는 것과 같은 정보에 대한 통제와 관련된 잠재적인 손실로, 스마트시티 서비스에서 대표적으로 나타날 수 있는 위험이다. 스마트시티는 전통적인 주거 형태와 달리 다양한 ICT 기술이 집목함과 더불어 기술유출의 경로가

늘어나 보안위험이 더욱 증가한 주거 형태이다[2]. 또한, 부정적 보안인식은 지각된 위험과 사용자저항 간의 관계를 강화시키는 것으로 나타났다[24]. 따라서, 본 연구에서는 스마트시티에 대한 보안위험 정도가 높을수록 저항 태도에 영향을 미칠 것이라는 가설을 설정하였다.

가설 1 (H1): 스마트시티의 보안위험은 저항 태도에 정(+)¹의 영향을 미칠 것이다.

보안시스템 및 보안 기기의 취약성으로 인해 해킹을 당하고 악성코드에 감염되는 등 보안위험을 통해 경제적 위험, 성능 위험, 사회적 위험, 신체적 위험, 사생활 침해 위험이 결과로서 발생할 수 있다. Zhao et al.(2008)은 IBS(Intelligent Building System) 시스템의 보안위험의 정도가 높을수록 사람들은 경제적 위험으로 인한 재정 손실에 대한 우려가 커진다는 관계를 입증한 바 있으며[25], 손영성·박준희(2015)는 홈 IoT 시스템이 수많은 센싱 정보 및 제어 명령이 유통되기 때문에 사생활 침해 위험, 성능 위험 등 다양한 위험이 발생할 수 있음을 주장하였다[26]. 홈 IoT 시스템 외에도 스마트시티에 접목된 기술 및 서비스들은 주거 생활의 질을 높여주었으나 보안 측면에서는 취약하다는 단점이 있다. 따라서, 본 연구에서는 스마트시티에 대한 보안위험 정도가 높을수록 경제적 위험, 성능 위험, 사회적 위험, 신체적 위험, 사생활 침해 위험의 정도 또한 높을 것이라는 가설을 설정하였다.

가설 2 (H2): 스마트시티의 보안위험은 경제적 위험에 정(+)¹의 영향을 미칠 것이다.

가설 3 (H3): 스마트시티의 보안위험은 성능 위험에 정(+)¹의 영향을 미칠 것이다.

가설 4 (H4): 스마트시티의 보안위험은 사회적 위험에 정(+)¹의 영향을 미칠 것이다.

가설 5 (H5): 스마트시티의 보안위험은 신체적 위험에 정(+)¹의 영향을 미칠 것이다.

가설 6 (H6): 스마트시티의 보안위험은 사생활 침해 위험에 정(+)¹의 영향을 미칠 것이다.

Mauricio(2003)은 e-서비스 제공업체에서 소비자가

제품 및 서비스를 구매할 때 경제적 위험이 구매 의도에 영향을 미치는 것을 확인한 바 있으며[17], 김홍범 외(2010)는 관광객의 경제적 위험지각이 관광객 거정에 유의한 영향을 미치는 것으로 입증되었다[27]. 스마트시티의 경우, 대개 전통적인 주거 형태보다 분양 금액이 높고 다양한 편의시설이 마련되어 있어 관리 비용이 높을 것으로 예상되기 때문에 저항 태도가 형성될 수 있다.

가설 7 (H7): 스마트시티에 대한 경제적 위험은 저항 태도에 정(+)¹의 영향을 미칠 것이다.

Mauricio(2003)은 제품 및 서비스가 오작동하거나 서버가 제대로 작동하지 않아 결제가 잘못 처리되는 것과 같은 성능 위험의 정도가 높을수록 구매를 망설인다는 내용을 실증한 바 있으며[17], Park(2016)은 스마트폰으로 예약했던 여행 상품을 평가할 때, 성능 위험에 관한 인식이 높을수록 부정적인 평가를 하는 것으로 확인하였다[16]. 스마트시티 내에도 각종 기기 및 서비스의 종류가 많아 고장 및 오작동의 가능성이 충분히 크며 이는 스마트시티 저항에 영향을 미칠 수 있다.

가설 8 (H8): 스마트시티에 대한 성능 위험은 저항 태도에 정(+)¹의 영향을 미칠 것이다.

김홍범 외(2010)의 연구에 따르면 현지인들과의 마찰, 의사소통 문제 등 관광객의 사회적 위험지각이 관광객의 위험 인식에 유의한 영향을 미치는 것으로 확인하였다[27]. 스마트시티의 경우, 자율주행 주차 서비스, 가정교사 로봇 등 인공지능 서비스를 제공하여[18] 이웃 간의 대화 없이도 충분히 일상생활이 가능하므로 스마트시티 내 생활로 인해 이웃들과의 소통이 적어질 수도 있다. 이러한 사회적 위험은 스마트시티 저항 태도에 영향을 미칠 수 있다.

가설 9 (H9): 스마트시티에 대한 사회적 위험은 저항 태도에 정(+)¹의 영향을 미칠 것이다.

스마트시티에서는 의료시스템 및 의료기기를 IoT와 접목하여 환자의 상태를 기록하고 인공지능을 기반으로 의료서비스를 제공한다[28]. 인터넷에 연결되어 있어 의료시스템 및 의료 기기가 해킹에 노출될 경우

환자의 생명과 직결되어 인명피해를 발생시킬 수 있다. 실제로, 2018년 싱가포르에선 한 의료그룹의 데이터베이스가 멀웨어에 감염돼 현지 총리, 장관을 포함한 약 1만 6,000명의 처방전이 유출되기도 하였다[10]. 이러한 신체적 위험은 스마트시티에 부정적 인식을 초래할 수 있다.

가설 10 (H10): 스마트시티에 대한 신체적 위험은 저항 태도에 정(+)^{의 영향을 미칠 것이다.}

Park(2016)은 스마트폰으로 모바일 여행 상품을 예약할 때, 개인정보 유출과 같은 사생활 침해 위험 인식과 구매 의도와 의 유의미한 관계를 입증한 바 있다 [16]. 실제로 대구 수성구 수성 알파 시티의 '5G 스마트시티 통합관제센터'는 무단 횡단하는 보행자와 불법 주정차, 범죄 발생 여부, 통과 차량 수, 유동 인구 숫자 등을 파악하여 100여 개의 서버에서 정보를 수집하고 인공지능이 이를 분석한다. 결국, 거주자의 개인정보는 실시간으로 수집되고 분석되며 이는 유출 또는 남용될 수 있다[29]. 이러한 사생활 침해 위험은 스마트시티에 대한 저항 인식을 형성할 수 있다.

가설 11 (H11): 스마트시티에 대한 사생활 침해 위험은 저항 태도에 정(+)^{의 영향을 미칠 것이다.}

3.2 측정문항

스마트시티 내에서 발생 가능한 위험요인 간의 관계와 이들이 스마트시티 저항 태도에 미치는 영향을 파악하기 설문 문항을 구성하였다. 경제적 위험 4개, 성능 위험 4개, 사회적 위험 4개, 신체적 위험 4개, 사생활 침해 위험 4개, 보안위험 6개, 주거 저항 의도 4개, 총 30개 문항으로 구성하였으며, 응답은 ①매우 그렇지 않다, ②그렇지 않다. ③보통이다. ④ 그렇다. ⑤매우 그렇다, 와 같이 리커트 5점 척도를 활용하였다. 문항은 기존의 지각된 위험요인과 관련된 설문조사를 바탕으로 스마트시티에 맞게 일부 변형하여 측정 문항을 개발하였다. 변수의 조작적 정의 및 측정항목을 개발하는데 참고한 기존 연구는 <표 3>과 같다.

일반적으로 남성의 경우, 생활편의와 직장과의 접근성이 주거선택에 우선시되는 반면, 여성은 주택 주변의 이웃이나 재해나 방법 문제를 중요시하는 등 성별

에 차이가 존재한다[30]. 또한, 20, 30대 전자기기 사용시간과 의존도가 40, 50대보다 높기 때문에 사생활 침해 및 보안위험에 관한 우려가 상대적으로 높을 것으로 예상되며[31], 소득수준이 높을수록 거주지 주변 문화 환경 만족도가 높고 경제적인 부담을 덜 느끼기 때문에 비교적 경제적 위험이 적다[32]. 이처럼, 인구통계학적 변수들이 스마트시티 저항에 미칠 수 있는 영향을 최소화하기 위해서 통제 변수로 성별, 나이, 소득수준을 모델에 투입하였다.

<표 3> 측정항목

구분	측정내용	참고 문헌
경제적 위험	FR1: (스마트시티에 살게 된다면) 스마트시티는 주거비용이 높을 것이다.	[33]
	FR2: 스마트시티에 매달 지불하는 관리 비용은 많을 것이다	
	FR3: 스마트시티에서는 일반 거주지보다 비용이 많이 들 것이다.	
	FR4: 스마트시티에 거주하게 된다면 예상치 못한 추가 비용이 있을 것이다.	
성능 위험	PFR1: 스마트시티 내 기기, 서비스(예시: 스마트대피시스템, 각종 로봇 서비스, 의료서비스) 오작동 및 고장의 가능성이 있을 것이다.	[34]
	PFR2: 스마트시티 내 각종 서비스의 오작동 및 고장이 생기면 해결하기 어려울 것이다.	
	PFR3: 스마트시티의 기기 및 서비스의 잦은 오작동 및 고장으로 인해 일상생활이 불편할 수 있을 것이다.	
사회적 위험	SOR1: 스마트시티가 사람들과 소통하는데에 적합하지 않은 환경이라고 생각한다.	[18]
	SOR2: 스마트시티에 거주한다면 다른 사람들과 어울리기 어렵다고 생각한다.	
	SOR3: 스마트시티 내에서 생활한다면 사회적 단절이 이루어질 것이라고 생각한다.	

	SOR4: 스마트시티에서 거주한다면 다른 사람들이 나를 부정적으로 바라볼 것이다.	
신체적 위험	PHR1: 스마트시티에 산다면 나의 건강을 위협할 수 있을 것이다.	[34]
	PHR2: 스마트시티 내 사고는 신체에 해를 끼칠 수 있다고 생각한다.	
	PHR3: 스마트시티에 살지 않는 것이 오히려 더 안전할 것이다.	
사생활 침해 위험	PVR1: 스마트시티 내 시스템에는 나의 민감한 정보들이 수집될 수 있다.	[34]
	PVR2: 스마트시티에서는 나의 사생활이 감시당할 수 있을 것이다.	
	PVR3: 스마트시티 내 시스템에서 나의 개인정보가 유출될 수 있을 것이다.	
	PVR4: 스마트시티에서 수집된 개인정보는 내가 원하지 않는 방향으로 남용될 수 있을 것이다.	
보안 위험	SER1: 스마트시티 내 장비들은 해킹에 취약할 것이다.	[33]
	SER2: 스마트시티 내 사물인터넷 기기는 보안에 취약할 것이다.	
	SER3: 스마트시티의 보안시스템은 전반적으로 완벽하지 않을 것이다.	
	SER4: 스마트시티 내 시스템들은 외부로부터 해킹 위험이 있을 것이다.	
	SER5: 스마트시티에서 공유되는 데이터는 외부로부터 공격에 의해 유출될 수 있을 것이다.	
	SER6: 스마트시티 내 장비들은 해커들에 의해 공격을 받을 가능성이 높을 것이다.	
스마트 시티 저항	SCR1: 스마트시티에 사는 것에 거부감이 있다.	[35]
	SCR2: 스마트시티에 사는 것에 부정적이다.	
	SCR3: 스마트시티에 살게 된다면 불안할 것 같다.	
	SCR4: 스마트시티에 사는 것에 반대하는 편이다.	

3.3 연구 데이터

연구 데이터는 전문 모바일 설문업체인 Open Survey를 활용하여 2020년 5월에 300명의 응답을 수집하였다. 그중 불성실한 응답 12건을 제외하여 총 288건을 분석에 활용하였다. 표본의 인구통계학적 특성은 <표 4>와 같다. 표본 중 남성은 146명(50.7%)이고 여성은 142명(49.3%)으로 성비의 균형을 유지하였다. 응답자의 연령대는 설문의 성격을 고려하여 10대를 모집 대상에서 제외하였고, 그 결과 20대가 71명(24.7%), 30대가 71명(24.7%), 40대가 72명(25.0%), 50대가 74명(25.7%)으로 고르게 분포되었다. 소득은 월 100만 원 미만이 42명(14.6%), 월 100만 원 ~ 200만 원이 40명(13.9%), 월 200만 원 ~ 300만 원이 78명(27.1%), 월 300만 원 ~ 400만 원이 55명(19.1%), 월 400만 원 이상이 73명(25.3%)으로 소득이 월 200만 원 ~ 300만 원인 응답자가 가장 많은 것으로 나타났다.

<표4> 표본의 인구통계학적 특성

구분	항목	빈도	비율
성별	남성	146	50.7%
	여성	142	49.3%
연령	20대	71	24.7%
	30대	71	24.7%
	40대	72	25.0%
	50대	74	25.7%
학력	고졸 이하	54	18.8%
	대학 재학	22	7.6%
	대학 졸업	180	62.5%
	대학원 재학	8	2.8%
	대학원 졸업	24	8.3%
소득	월 100만 원 미만	42	14.6%
	월 100 ~ 200만 원	40	13.9%
	월 200 ~ 300만 원	78	27.1%
	월 300 ~ 400만 원	55	19.1%
	월 400만 원 이상	73	25.3%
전체 표본 수(N)		288	

4. 분석결과

4.1 측정모형의 검증

본 연구에서는 연구모델의 검증을 위해 다른 구조방정식 도구보다 상대적으로 장점이 있는 PLS 구조방정식 분석 기법을 활용하였다. 측정모형의 검증을

<표 5> 신뢰성 및 타당성 분석결과

변수	측정항목	요인적재량	평균	표준편차	α	C. R.	AVE	제거 항목
경제적 위험 (FR)	FR1	0.687	3.893	0.763	0.805	0.858	0.603	
	FR2	0.871						
	FR3	0.754						
	FR4	0.782						
성능 위험 (PFR)	PFR1	0.740	3.270	0.992	0.676	0.822	0.607	Q13
	PFR2	0.758						
	PFR3	0.835						
사회적 위험 (SOR)	SOR1	0.777	2.510	1.010	0.808	0.874	0.635	
	SOR2	0.831						
	SOR3	0.851						
	SOR4	0.723						
신체적 위험 (PHR)	PHR1	0.821	2.383	0.899	0.708	0.837	0.631	Q21
	PHR2	0.780						
	PHR3	0.782						
사생활 침해 위험 (PVR)	PHR1	0.821	3.746	0.910	0.914	0.939	0.794	
	PHR2	0.780						
	PHR3	0.782						
보안위험 (SCR)	PVR1	0.863	3.471	0.938	0.914	0.933	0.699	
	PVR2	0.895						
	PVR3	0.912						
	PVR4	0.894						
주거 저항 (RR)	RR1	0.889	2.346	0.795	0.901	0.931	0.772	
	RR2	0.914						
	RR3	0.843						
	RR4	0.868						

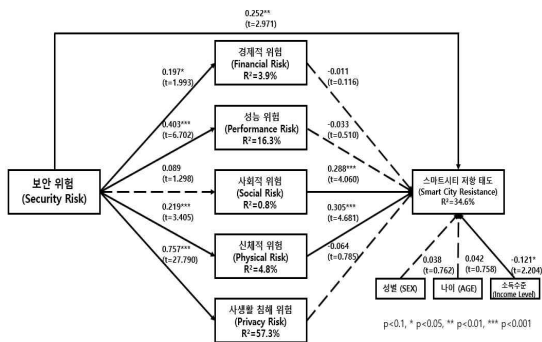
위하여 Cronbach's alpha 값을 비롯하여 합성 신뢰도 (Composite Reliability; CR), 평균 분산 추출(average variance extracted; AVE) 및 연구모형 검증을 수행하였다. 먼저 신뢰도와 내적 일관성을 검증하기 위해서 합성 신뢰도(Composite Reliability)와 Cronbach's alpha를 확인하였다. 일반적으로 Cronbach's alpha와 합성 신뢰도(Composite Reliability; CR)의 값이 0.7 이상이면 변수에 대한 측정항목들의 신뢰성이 높다고 할 수 있는데[36], PFR4: '스마트시티 서비스가 기대한 것보다 만족스럽지 않을 것이다.'와 SER7: '스마트시티 내 전자기기를 활용한 테러 및 범죄는 안전을 위협할 수 있을 것이다.' 문항은 Cronbach's alpha와 합성 신뢰도를 저하시키는 문항으로 확인되어 해당 항목을 분석에서 제외하였다. 데이터 분석결과, 모든 변수에 대한 Cronbach's alpha와 합성 신뢰도 값이 각각 0.805와 0.858 이상임을 확인하였다.

다음으로는 집중타당도와 판별 타당도를 확인하였

다. 먼저 집중타당도 검증을 위해서 설문항목의 요인적재량들을 확인하였다. 집중타당도는 각 변수 항목들의 요인적재량이 0.7 이상일 때 확보된 것으로 보는데 본 연구의 항목들은 경제적 위험 FR1을 제외하고 모두 기준치 이상을 나타내고 있고[36], 또한 추가로 평균 분산 추출(Average Variance Extract)이 0.5 이상일 때 집중타당도를 확보하는 것으로 보는데 본 연구의 변수들의 평균 분산 추출의 값들도 모두 0.6 이상을 기록하므로 집중타당도를 확보하는 것으로 보인다. 판별 타당도를 위해서는 각 변수의 평균 분산 추출의 제곱근 값과 종과 횡에 있는 다른 변수들과의 값을 비교하여 이 값들보다 클 때 판별 타당성을 확보하는 것으로 보는데 모든 변수의 평균 분산 추출의 제곱근 값이 다른 변수들의 값들보다 크므로 판별 타당성 또한 확보하는 것으로 나타났다[36].

4.2 연구 가설의 검증

본 연구에서 제안하고 있는 연구모형의 경로 분석을 위해서 부트스트랩 재 표본 방법으로 1000개의 재 표본 과정을 통하여 본 연구에서 제시한 11개의 가설을 검증하였다[36]. 전체 288개의 표본을 대상으로 한 경로 분석에서 11개의 가설 중 7개의 가설 (H1, H2, H3, H5, H6, H9, H10)이 유의한 것으로 나타났다. 추가로, 연구모형의 모델 적합도를 보기 위해 Tenenhaus et al.(2004)가 제안한 방법을 활용하여 본 연구의 모델 적합도를 검증하였다. PLS에서의 모델 적합도 지수는 R²값의 평균과 AVE(평균 분산 추출)값 평균의 기하 평균값을 통해 산출되며, 값이 클수록 적합도가 높은 것으로 판별한다. 적합도 지수 계산을 한 결과 본 연구모형의 적합도 지수는 36.6%로 양호한 것으로 나타났으나 전반적인 분산 설명력(R²)이 낮아 추가적인 외생 변수 투입을 통한 모델 확장은 필요한 것으로 보인다. 통제 변수로 투입된 세 가지 변수 중 성별, 나이는 스마트시티 저항에 유의미한 영향을 주지는 않았으나 소득수준과는 유의미한 관계가 있는 것으로 나타났다. 이는 소득수준이 높을수록 스마트시티에 대한 경제적 부담이 적기 때문에 부정적 인식이 낮은 것으로 판단된다.



(그림 2) 가설검증 결과

5. 결론

5.1 연구 시사점

본 연구 결과에 따른 스마트시티는 상호 연결된 기기를 바탕으로 다양한 편의 서비스를 지원하는 이점이 있으나 보안위험이 다른 위험 요소에 미치는 영향이 크고, 이를 통한 스마트시티에 대한 부정적 저항 태도 형성에도 기여한다는 것을 본 연구를 통해 확인하였다. 최근에는 스마트시티의 상호 연결 특성으로 오히려 보안 위험이 더 커지고 있다는 것은 많은 학술적 논의를 통해 이미 대안을 마련할 필요성을 보여 준다[4]. 실제 사례로 2017년 미국 병원 네트워크의 데이터베이스 시스템이 해킹되어 개인정보가 유출되거나 2018년 우리나라의 가정집에서도 IP 카메라가 해킹되어 약 5천 명이 불법 촬영 피해를 받는 사례들이 나타났다[10]. 이러한 사례들로부터 사람들은 스마트시티 내에 위험이 존재한다고 인식할 수 있으며, 이는 곧 스마트시티에 대한 부정적 인식에 영향을 줄 수밖에 없다[22].

본 연구 결과가 제시하는 시사점을 정리하면 다음과 같다. 첫째, 스마트시티 환경에서 경제적 위험과 성능 위험, 사생활 침해 위험에 대한 인식은 낮은 것으로 나타났다. 경제적 위험의 인식이 낮은 것은, 이미 스마트시티 분양 비용에 대해 인식한 후 거주 비용을 지불하였고 스마트시티에 거주한다는 것 자체가 본인에게 경제적 부담이 덜 하기 때문인 것으로 판단된다. 성능 위험에 대해서도 이미 최신식으로 스마트시티가 지어졌기 때문에 CCTV, 보안시스템 고장의 가능성을 크게 인식하지 않아 위험을 느끼지 않는다는 것으로 보인다. 사생활 침해 위험 인식이 낮은 것은 스마트시티라고 하더라도 기존에 온라인상에서 발생하던 사고와 환경에 큰 차이가 없다고 인식하여 스마트시티의 사생활 침해가 더 위험하다고 인식하지 못한 것으로 판단된다. 일부의 경우에는 이미 개인정보가 유출된 적이 있어서 사생활 보호의 한계에 대해서 인식하고 있기 때문에 사생활 침해 위험을 크게 인식하지 않았을 수도 있다.

둘째, 먼저 스마트시티 저항에 신체적 위험이 미치는 영향 또한 큰 것으로 나타났다. 이는 스마트시티라는 특수성 때문일 수도 있다. 기존의 사이버보안 사고 같은 경우, 온라인상에서 개인정보를 가져가거나 시스템에 침투하여 데이터를 빼가는 유형이었다면 스마트시티에서 발생하는 보안사고는 실제로 사람들에게 직

접적인 영향을 줄 수 있다는 점에서 다르다. 예를 들어, 이동성이 높은 ‘치안관리용’ 드론이 해킹당해 시민들을 적으로 간주하고 공격하거나 생명과 직결되는 의료기기가 해킹당했을 경우 환자의 목숨이 위협할 수 있으며[10], 스마트 정수장, 연료전지발전소와 같은 기반시설을 해킹하여 테러를 일으킨다면 더 큰 인명 피해가 나타날 수 있다. 이처럼 현실과 직결되어 있다는 스마트시티의 특수성 때문에 사람들은 안전에 대한 위협을 느끼고 신체적 위협을 가장 크게 인식하였을 수 있다. 스마트시티의 거주에 대한 문제뿐만 아니라 방문 및 유입을 위해서는, 신체적 위협 인식을 줄이기 위하여 안전 문제에 대한 문제를 최우선으로 해결해야 한다.

셋째, 스마트시티 저항에 사회적 위협이 미치는 영향 또한 큰 것으로 나타났다. 스마트시티의 경우, 다양한 ICT 기술이 접목되어 자율주행 주차 서비스, 가정교사 로봇 등 인공지능 서비스를 제공하여 이웃 간의 대화 없이도 충분히 일상생활이 가능하기에 사람들을 대면할 기회가 적어 사람들과의 사이가 멀어질 수도 있다. 이러한 상황으로 보아 사회적 위협을 인식하였다고 판단된다. 사회적 위협을 해결하기 위해서는 스마트시티에 내에서도 문화 활동을 할 수 있는 프로그램을 개설하거나, 입주민들과 교류할 수 있는 장이 마련되어야 할 것이다.

넷째, 기존 연구들은 연구 목적이나 연구자의 의도에 따라 보안위협과 사생활 침해 위협의 개념을 분리하기도 하고 하나의 개념으로 통합해서 다루기도 한다. 본 연구에서 보안 위협과 프라이버시 위협이 저항 태도에 미치는 영향이 다른 것을 볼 때 스마트시티 환경에서는 두 개념은 분리되는 것이 적절하다는 것을 알 수 있다.

다섯째, 위험요인들 사이에도 각각의 인과관계가 존재할 수 있음을 본 연구를 통해 검증하였다. 기존 연구들은 지각된 위험요인들을 병렬적인 선행요인으로 고려하여 서로 간의 인과관계에 대해서는 논의가 부족하였다. 한 예로, 보안시스템 및 보안기기가 해킹을 당하고 악성코드에 감염되는 등 보안위협을 통해 계좌에 돈이 빠져나가거나 보안사고가 발생하여 개인이 안전에 위협을 받을 수 있으며 개인정보가 남용·유출될 수도 있다. 보안시스템의 위험 정도가 높을수록 사

람들이 인식하는 경제적 위험 또한 커진다는 관계를 입증한 연구 또한 존재한다[25]. 이처럼 보안위협이 선행요인으로서 작동하고, 이의 결과로 경제적 위험, 성능 위험, 사회적 위험, 신체적 위험, 사생활 침해 위험 등을 인지하게 될 수도 있다. 따라서 연구모델을 제시함에 있어서 위험요인들 간에 관계 또한 고려하는 것이 바람직하다고 볼 수 있다.

5.2 연구의 의의 및 한계점

본 연구의 학술적 의의는 이론적 기여와 실무적 기여로 나뉠 수 있다. 이론적 기여로서는 첫째, 스마트시티 인식에 대해서 부정적인 영향을 미치는 위험요인을 분석하였다. 기존 연구들은 스마트시티의 기술 분석, 스마트시티 동향, 스마트시티 사이버보안에 대한 내용이 주를 이루며, 스마트시티 인식에 관하여 분석한 연구는 부족하다. 본 연구는 실증적 분석을 통해 스마트시티 위험요인을 분석하고 개선방안을 모색했다는 점에서 의의가 있다. 둘째, 위험요인 간의 계층적인 부분을 확인했다. 보안위협이 선행적인 요인으로 작용하고 나머지 다섯 가지 위험요인이 결과로서의 요인으로 나타났다. 셋째, 연구 주제에 따라서 유의한 위험 요소가 달라질 수 있다는 것을 확인하였다. 김홍범 외(2010)의 연구에서는 사회적 위협이 관광객 태도에 영향을 미치는 것으로 나타났으나[27] 양지윤 외(2006)의 연구에서는 모바일 뱅킹 사용에 있어 사회적 위협은 비교적 영향이 없는 것으로 분석되었다[37]. 오히려 스마트시티 상황에서 사회적 위협 인식이 높게 나타나고 경제적 위험 인식은 낮은 것으로 확인되었다. 저항에 있어서 전통적인 위험요인은 항상 유의하지 않고 상황에 따라 달라진다는 것이다.

실무적 기여로서는 스마트시티 인식에 대하여 부정적인 영향을 미치는 위험요인을 파악하여 해결방법을 모색했다는 데에 있다. 연구 결과, 부정적인 영향을 미치는 위험요인은 사회적 위협과 신체적 위협으로 나타났다. 사회적 위협 인식에 대한 방안으로, 사람들과의 교류 활동을 통한 문화 활동을 할 수 있는 환경 마련해야 한다는 것과 신체적 위협 인식에 대한 방안으로, 스마트시티 안전에 대한 정책적인 차원의 논의가 필요하다는 것을 주장하였다.

그럼에도 불구하고 이 연구는 다음과 같은 한계점이 있다. 첫째, 스마트시티 저항의 선행요인으로 전통적인 위험요인에 대해서만 분석하였다는 점이다. 주거선택요인은 사회적 변수(이웃 관계, 안정성, 프라이버시), 물리적 변수(유지관리, 소음, 편리성, 주차시설, 조경과 수목, 미, 주택형태, 주택 규모 등), 개인적 변수(연령, 소득, 수입, 교육수준, 거주 기간, 주택 소유형태, 가족 수), 서비스 변수(대중교통수단, 어린이 놀이터, 공공시설), 근린주거 변수(접근성, 주변 환경, 공해 정도, 위치, 학군)로 나누어 설명할 수 있다[38]. 주택 주변의 소음, 대중교통수단, 공공시설, 위치, 주변 환경 등이 주거를 선택하는데 큰 변수로 작용할 수 있음에도 불구하고 본 연구에서는 전통적인 위험요인과 관련된 요인만을 파악하였다. 향후 연구에서는 위험요인 외에 다양한 개인적 요인이나 환경적 요인들을 고려한 통합 모델이 검증된다면 스마트시티 저항을 이해하는데 도움이 될 것이다.

둘째, 위험요인 간에 상관관계를 살펴보기 하였으나 이들 간의 설명력이 높진 않다. 위험요인 간에 미세한 차이는 있으나 설명력이 부족하므로, 위험요인 간에 관계에 대한 추가적인 논의 및 연구가 필요하다. 마지막으로, 스마트시티에 거주한 적이 없거나 스마트시티에 대해서 잘 모르는 사람들을 대상으로 위험요인을 파악했다는 한계점이 있다. 스마트시티에 거주한 적이 없고, 이에 대해 잘 모르는 사람들은 위험요인을 실제로 겪어보지 못했기 때문에 상상에 빚대어 응답하였을 가능성이 있다. 스마트시티에 거주한 적이 있거나, 실제 거주 중인 사람들을 중심으로 위험요인을 파악한다면, 현실적인 개선방안이 도출될 수 있을 것이다.

참고문헌

- [1] 최봉문, “스마트 용어의 적용사례 분석을 통한 ‘스마트시티’의 개념정립을 위한 연구”, 한국콘텐츠학회논문지, 제11권, 제12호, pp. 943-949, 2011.
- [2] 김현진, 손태식, “스마트시티의 보안을 위한 사이버보안위협정보 활용 연구”, 한국디지털콘텐츠학회 논문지, 제20권, 제6호, pp. 1173-1180, 2019.
- [3] 김용국, 송유미, 조상규, “유비쿼터스도시 거주민 인식조사를 통한 스마트도시 정책 개선 방향 연구”, 한국도시설계학회지 도시설계, 제20권, 제3호, pp. 83-93, 2019.
- [4] Adel S. Elmaghraby, Michael M. Losavio, “Cyber security challenges in Smart Cities: Safety, security and privacy”, Journal of Advanced Research, Vol. 5, No. 4, pp. 491-497, 2014.
- [5] 박현선, 김상현, “간편 결제 서비스의 지각된 위험과 기술적 특성이 사용갈등과 수용저항에 미치는 영향에 관한 연구”, 인터넷전자상거래연구, 제17권, 제4호, pp. 119-138, 2017.
- [6] 조대연, “스마트시티 개념과 이슈”, 도시문제, 제52권, 제580호, pp. 22-25, 2017.
- [7] https://www.molit.go.kr/USR/NEWS/m_71/dtl.js?p?lcmstage=1&id=95083430
- [8] 이면성, “사물인터넷(IoT) 기반 스마트시티 실증 서비스 주요 현황 및 사례”, 한국통신학회지(정보와 통신), 제34권, 제9호, pp. 3-8, 2017.
- [9] <https://www.c-its.kr/introduction/introduction.do>,
- [10] <https://www.boannews.com/media/view.asp?id=79250>
- [11] Bauer, Raymond A, “Consumer behavior and risk taking, in Dynamic Marketing for a Changing World”, R.S.Hancock, Ed., American Marketing Association, Chicago, pp. 389-398, 1960.
- [11] Bauer, Raymond A, “Consumer behavior as risk taking, in Risk Taking and Information Handling in Consumer Behavior”, Donald F. Cox, ed., Harvard University Press, Boston, pp. 23-33, 1967.
- [12] Margy p. Conchar, George M. Zinkhan, Caraperters, and Sergio Olavarrieta, “An integrated framework for the conceptualization of consumers’ perceived-risk processing”, Academy of Marketing Science, pp. 418-438, 2004.
- [13] Cunningham, S., “The major dimensions of perceived risk. In: D. Cox (Ed.), Risk Taking and Information Handling in Consumer Behavior”,

- Harvard University Press, 1967.
- [14] Jacoby, J., & Kaplan, V, "The components of perceived risk in product purchase: A cross-validation", *Journal of Applied Psychology*, Vol. 59, No. 3, pp. 287-291, 1972.
- [15] 최지은, 강주영, 이환수, "증강현실 게임에서 연령에 따른 위험 인식 차이 연구", *예술인문사회융합멀티미디어논문지*, 제7권, 제3호, pp. 401-410, 2017.
- [16] Sangwon Park, "Multidimensional Facets of Perceived Risk in Mobile Travel Booking", *Journal of Travel Research*, 2016.
- [17] Mauricio S. Featherman, Pavlou, "Predicting e-services adoption: a perceived risk facets perspective", *International Journal of Human-Computer Studies*, pp. 451-474, 2003.
- [18] <https://www.busan.go.kr/ecodelta>
- [19] 이기성, 안효범, 이수연, "개인정보 노출을 예방하는 방법에 관한 연구", *융합보안논문지*, 제12권, 제1호, pp. 71-77, 2012.
- [20] 신영진, "사물인터넷시대에 적합한 개인정보보호정책의 우선순위분석", *한국지역정보화학회지*, 제22권, 제2호, pp. 25-57, 2019.
- [21] 유우영, "IoT 보안에 대한 국내외 연구 동향 분석", *융합보안논문지*, 제18권, 제1호, pp. 61-67, 2018.
- [22] 이환수, 임동원, 조항정, "빅데이터 시대의 개인정보 과잉이 사용자 저항에 미치는 영향", *한국지능정보시스템학회 지능정보연구*, 제19권, 제1호, pp. 125-139, 2013.
- [23] 김문선, 김현정, 김문오, 김효진, "IPTV 사용자 저항에 관한 연구", *한국전자거래학회지*, 제15권, 제2호, pp. 205-217, 2010.
- [24] 김상현, 박현선, "개인 및 기술 특성이 모바일 결제 서비스의 지각된 위험과 수용저항에 영향에 관한 연구", *디지털융복합연구*, 제15권, 제12호, pp. 239-253, 2017.
- [25] Anita Lifan Zhao, Stuart Hanmer Lloyd, Philippa Ward, Mark M.H. Goode, "Perceived risk and Chinese consumers' internet banking services adoption", *International Journal of Bank Marketing*, Vol. 26, No. 7, pp. 505-525, 2008.
- [26] 손영성, 박준희, "홈 IoT 기술 현황과 발전 방향", *한국통신학회지(정보와 통신)*, 제32권, 제4호, pp. 23-28, 2015.
- [27] 김홍범, 임지영, 김나은, "위험지각이 관광객의 걱정과 태도에 미치는 영향", *호텔경영학연구*, 제19권, 제6호, pp. 171-19, 2010.
- [28] 노시춘, "u-헬스케어시스템의 정보보안 체계 확보를 위한 5단계 보안위협도 평가모델 설계", *융합보안논문지*, 제13권, 제4호, pp. 11-17, 2013.
- [29] <https://news.imaeil.com/InnerColumn/2020051416405058069>
- [30] 정연택, 김재태, 김종원, "소형주택 주거만족 요인 연구: 인구통계변인에 따른 고객특성그룹 중심으로", *한국콘텐츠학회*, 제17권, 제4호, pp. 488-499, 2017.
- [31] 정만수, "연령과 인지욕구가 스마트폰 사용행동에 미치는 영향에 관한 탐색적 연구: 스마트폰 의존도, 앱 활용도, 앱 호감도, 사생활침해 우려, 광고회피행동을 중심으로", *광고학연구*, 제25권, 제6호, pp. 105-133, 2014.
- [32] 정보람, 진인수, 소득수준과 문화적 여건이 행복감에 미치는 영향. *문화정책논총*, 제31권, 제1호, pp. 30-51, 2017.
- [33] 송재호, 고승식, "관광호텔기업 위기관리 연구", *관광경영연구*, 제12권, 제3호, pp. 21-43, 2008.
- [34] Harridge March, S., Lifan Zhao, A., Hanmer Lloyd, S., Ward, P. and Goode, M, "Perceived risk and Chinese consumers' internet banking services adoption" *International Journal of Bank Marketing*, Vol. 26, No. 7, pp. 505-525, 2008.
- [35] <http://www.smartcity1st.com/survey/intro.php>
- [36] Chin, w. w., "The partial least squares approach to structural equation modeling", *Modern methods for business research*, Vol. 295, No. 2, pp. 295-336, 2008.
- [37] 양지윤, 안중호, 박철우, "인지된 위험이 모바일 뱅킹 수용 의도에 미치는 영향", *기술혁신연구*,

제14권, 제3호, pp. 183-208, 2006.

- [38] 이주택, “주거환경만족도 요인구조분석에 관한 연구”, 동국대학교 박사학위논문, 제31권, 1994.

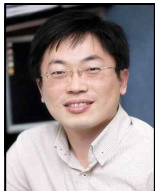
[저자 소개]



박 현 애 (HyunAe Park)
2019년 8월 한세대학교 산업보안학과
학사
2019년 ~ 현재 단국대학교 IT법학협동
과정 산업보안법 전공 석사과정
email : gusdo7272@naver.com



유 영 천 (YoungCheon Yoo)
2020년 2월 한세대학교 산업보안학과
학사
2020년 ~ 현재 단국대학교 IT법학협동
과정 산업보안법 전공 석사과정
email : y2c206@naver.com



이 환 수 (Hwansoo Lee)
2005년 2월 연세대학교 산업정보시스
템 공학과 석사
2014년 2월 KAIST 기술경영학과 박
사
2017년 ~ 단국대학교 융합보안학과
교수
email : hanslee992@gmail.com