

지능정보사회를 대비한 안전관리체계 리모델링에 관한 연구 - 총론

제1권

A Research on Remodeling of Safety Management System
for Intelligent Information Society - Introduction

송 지 환 / 서 영 희

2018.04.

이 보고서는 2017년도 과학기술정보통신부 정보통신·방송연구
개발사업의 연구결과로서 보고서 내용은 연구자의 견해이며,
과학기술정보통신부의 공식입장과 다를 수 있습니다.

제 출 문

과학기술정보통신부 장관 귀하

이 보고서를 『지능정보사회를 대비한 안전관리체계 리모델링에 관한 연구 - 총론』의 연구결과보고서로 제출합니다.

2017년 12월

연구기관 : 소프트웨어정책연구소

총괄책임자 : 송지환 선임연구원

참여연구원 : 서영희 선임연구원

참여기관 : 한국법제연구원

한국행정연구원

목 차

요 약 문	i
Summary	xiv
제1장 서론	1
제1절 연구의 배경 및 목적	1
1. 연구의 배경	1
2. 연구의 목적	3
제2절 연구의 구성 및 방법	3
1. 연구의 구성	3
2. 연구의 방법	4
제2장 기술 중심으로	7
제1절 개요	7
1. 추진 배경	7
2. 연구의 목적	8
제2절 교통 안전 : 자율주행차	8
1. 시장 및 정책 동향	9
2. 요소 기술	12
3. 안전 관리 현안 및 시사점	15
제3절 시설물 안전 : 스마트 빌딩	18
1. 시장 및 정책 동향	19
2. 요소 기술	22
3. 안전 관련 현안 및 시사점	25
제4절 사회기반 안전(금융) : 블록체인	26
1. 블록체인의 특징	26
2. 시장 및 정책 동향	29
3. 요소 기술	32
4. 안전 관련 현안 및 시사점	35
제5절 소결	40

제3장 행정관리 중심으로	44
제1절 개요	44
1. 추진 배경	44
2. 연구의 목적	45
제2절 교통 안전 : 자율주행차	46
1. 교통 안전분야의 지능정보기술에 따른 영향 검토	46
2. 교통 안전관리체계 현황 분석	47
3. 교통 분야 지능정보기술 적용 시 발생 가능한 위험성과 문제점	49
4. 교통 안전관리체계의 리모델링 방향 도출	50
5. 교통 분야 안전관리체계 개선방안 도출	51
제3절 시설물 안전 : 스마트 빌딩	53
1. 건축·시설물 안전분야의 지능정보기술에 따른 영향 검토	53
2. 건축·시설물 안전관리체계 현황 분석	54
3. 건축·시설물 분야 지능정보기술 적용 시 발생 가능한 위험성과 문제점 분석	56
4. 건축·시설물 안전관리체계의 리모델링 방향 도출	57
5. 건축·시설물 분야 안전관리체계 개선방안 도출	58
제4절 사회기반 안전(금융) : 블록체인	60
1. 금융 안전분야의 지능정보기술에 따른 영향 검토	60
2. 금융 안전관리체계 현황 분석	61
3. 금융 안전 분야에 지능정보기술 적용 시 발생 가능한 위험성과 문제점	64
4. 금융 안전관리체계의 리모델링 방향 도출	64
5. 금융 분야 안전관리체계 개선방안 도출	66
제5절 소결	68

제4장 법·제도 중심으로	70
제1절 개요	70
1. 추진 배경	70
2. 연구의 목적	71
제2절 교통 안전 : 자율주행차	72
1. 현행 교통 분야 안전관리체계 조사 및 분석	72
2. 자율주행차 등 지능정보기술의 상용화 과정의 문제점	73
3. 자율주행차 관련 해외 주요국 교통 안전관리체계	73
4. 법·제도 관점에서의 교통 안전관리체계 구축 방안	77
제3절 시설물 안전 : 스마트 빌딩	78
1. 스마트 빌딩 상용화에 따른 안전관리 문제	78
2. 현행 안전관리 법률에 근거한 시설물분야에 대한 안전관리 체계 분석	79
3. 지능정보기술을 활용한 스마트 빌딩의 상용화 과정에서 여러 문제점	79
4. 해외 시설물 안전관리체계 조사 및 분석	79
5. 법·제도 관점에서의 시설물 안전관리체계 구축 방안	83
제4절 사회기반(금융) 안전 : 블록체인	84
1. 암호화폐의 등장이 금융분야에 미치는 영향	84
2. 암호화폐 관련 국내 안전관리 법률체계 및 정책 조사 및 분석	85
3. 블록체인 신기술의 안전적 활용을 위한 관련 법령에 대한 검토	85
4. 블록체인(암호화폐) 관련 해외 안전관리 법체계 조사 및 분석	87
5. 법·제도 관점에서의 사회 기반(금융) 안전관리체계 구축 방안	90
제5절 소결	92
제5장 결론	93

표 목 차

〈표 2-1〉 블록체인 종류 비교	27
〈표 2-2〉 블록체인 기술의 단계별 발전 방향	28
〈표 2-3〉 금융 관련 블록체인 관련 해외 기업 동향	29
〈표 2-4〉 금융 관련 블록체인 관련 국내 기업 동향	30
〈표 2-5〉 대표적인 암호화폐 도난 사고 요약	36
〈표 3-1〉 교통 안전 : 자율주행차 연구 내용 요약표	52
〈표 3-2〉 시설물 안전 : 스마트 빌딩 연구내용 요약표	59
〈표 3-3〉 사회기반(금융) 안전 : 블록체인 내용 요약표	67

그 립 목 차

[그림 1-1] 협동 연구에 참여하는 전문 연구 기관	5
[그림 2-1] 미국 GSA의 Smart building 운영 정책	21

요 약 문

1. 제 목 : 지능정보사회를 대비한 안전관리체계 리모델링에 관한 연구 - 총론

2. 연구 목적 및 필요성

(1) 추진 배경

- 지식정보사회를 넘어 지능정보사회의 도래
 - 새로운 기술의 등장과 발전으로 사회가 급격히 변화하는 지능정보사회가 도래하여 이전에 없던 새로운 가치를 창출하고 있음
- 지능정보사회의 도래로 그간의 사회 변화보다 큰 변혁이 있을 것으로 전망
 - 지능정보사회는 본질적이고 전면적인 변혁(變革)을 우리에게 가져다주고 있으며 특히 자율주행차, 스마트 빌딩, 블록체인의 등장으로 인해 국민의 안전을 확보하고 강화하기 위한 안전관리 체계의 변화가 요구됨
 - 그간의 연구는 새로운 기술을 이용하여 안전을 확보하거나 보완하는 데 집중하여 새로운 기술로 변화가 필요한 안전관리체계에 대한 깊이 있는 연구는 미흡하였음
- 이에 국민 안전에 파급력이 클 것으로 예상하는 교통 안전, 시설물 안전, 사회기반(금융) 안전분야에 대해 안전관리 체계(틀) 변화에 대한 연구의 필요성 증대
 - 지능정보사회를 미리 대비하기 위해서는 국민의 안전을 확보하는 새로운 안전관리체계 구축이 밀바탕 되어야 하며 새로운 기술, 법·제도 및 행정관리에 대한 다양하고, 종합적이고, 전문성 있는 관계 연구기관의 협동 연구가 필요함

(2) 연구의 목적

- 신기술이 적용되어 국민의 안전을 확보·강화하는데 파급효과가 클 것으로 예상하는 세 분야(교통 안전, 시설물 안전, 사회기반(금융) 안전)를 대상으로 신기술의 출현에 효과적으로 대응하기 위한 변화 및 개선방안 등을

기술, 법·제도, 행정관리 측면에서 종합적으로 도출하여 제시하고자 함

3. 연구의 구성 및 방법

(1) 연구의 구성

- 본 협동 연구보고서는 총 4권으로 구성되며 제1권 총론에서는 제2권부터 제4권까지의 내용을 요약 기술함
- 제1장은 서론으로서 연구의 배경, 필요성, 목적 등을 기술함, 제2장은 기술 중심 보고서를 요약하고 제3장은 제3권 행정관리 중심 보고서를, 제4장에서는 제4권 법·제도 중심 보고서를 각각 요약하며, 제5장에서는 지금까지 내용을 정리함
 - 제2권(소프트웨어정책연구소 연구수행)에서는 자율주행차(제2장), 스마트 빌딩(제3장), 블록체인(제4장) 등 신기술에 대해 시장 및 정책 동향을 살펴보고 요소 기술에 관해 설명하며, 제5장에서는 해당 기술과 관련된 안전 현안을 정리하고 이를 바탕으로 시사점을 도출함
 - 제3권(한국행정연구원 연구수행)에서는 교통 안전(제2장), 시설물 안전(제3장), 사회기반(금융) 안전(제4장) 분야의 안전관리 추진체계를 분석하고, 지능정보기술로 인한 미래위험 대응 정책 현황을 분석하며, 제5장에서는 각 분야의 문제 해결과 향후 효과적인 대응을 위해 요구되는 변화관리 방향 및 정책과제, 그리고 장·단기적 추진 방안을 도출함
 - 제4권(한국법제연구원 연구수행)에서는 교통 안전(제2장), 시설물 안전(제3장), 사회기반(금융) 안전(제4장) 분야의 주요 법적 이슈와 쟁점을 분석하며, 제5장에서는 각 분야의 기존 안전관리체계 및 입법사례 분석을 통하여 도출된 문제를 해결하고, 향후 효과적인 대응을 위해 요구되는 변화관리 방향을 제시함

(2) 연구의 방법

- 지능정보사회의 변화에 대응 가능한 안전관리체계 구축을 위해 교통 안전, 시설물 안전, 사회기반 안전(금융) 분야를 대상으로 새로운 기술,

법·제도 및 행정관리에 대한 종합적이고 전문성 있는 관계 연구기관의 협동 연구를 수행함

- 소프트웨어정책연구소는 자율주행차, 스마트 빌딩, 블록체인 기술에 대한 시장 및 정책 동향, 요소 기술에 대해 조사하고 기술과 안전 간 관계 제시
 - 기본적으로 문헌연구를 중심으로 조사한 결과에 대해 전문가와의 인터뷰를 통해 연구의 적실성을 높이고, 참여 연구기관들과 정기적인 회의를 통해 필요한 정보를 공유하고 연구 방향을 조율함
- 한국행정연구원은 현재의 안전관리 추진체계를 분석하고 지능정보기술로 인한 미래위험 대응 정책의 현황 분석, 각 분야의 문제 해결과 향후 효과적인 대응을 위해 요구되는 변화관리 방향 및 정책 추진 방안을 제시
 - 적절성을 평가하기 위하여 연구의 관련성을 고려한 연구자문단을 구성·운영하여 연구의 품질을 보증
- 한국법제연구원은 기존 안전관리체계 및 입법사례 분석을 통하여 도출된 문제를 해결하고, 향후 효과적인 대응을 위해 요구되는 변화관리 방향을 도출
 - 다양한 신기술 분야 전문가, 안전관리관련 입법전문가, 관련 행정 실무자 등으로 구성된 자문위원회를 활용

4. 연구 내용 및 결과

1) 기술적 측면에서의 안전관리체계 리모델링 연구

(1) 교통안전 : 자율주행차와 안전

- 자율주행차의 특징
 - 자율주행차는 2025년부터는 사람의 개입 없이 독립적으로 운행이 가능할 것이라 예측되며, 다양한 사회·경제적 효과가 예상됨
- 자율주행차의 시장 및 정책 동향
 - 완전 자율주행차의 시장 규모는 2025년에 60만대 수준에 도달할 것이며 이후 2035년에는 2,100만대 수준으로 대폭 증가할 것으로 예상됨

- 주요 글로벌 자동차 제조업체 및 IT업체, 부품업체는 자율주행차 시장에서 경쟁력 확보를 위해 업체 간 인수 및 합병 등 적극적인 투자를 진행하고 있음
- 국내에서도 2010년부터 현대·기아자동차를 중심으로 연구가 진행되고 있고, 미국 자동차공학회(SAE) 기준 자율주행 레벨 3~4단계까지 개발되었으며, 완성차 기업뿐만 아니라 대학교 및 IT연구소, 부품 업체에서도 연구개발을 진행 중임
- 정부의 적극적인 개입을 통한 임시 운행제도 마련 및 법적 규제 근거 정비를 통해 국제 표준에 맞는 평가 절차를 구축해야 하고 교통사고 발생 시 책임 및 보험 등 이슈를 해결하기 위한 정부의 역할이 중요함

○ 자율주행차의 요소 기술

- 환경인식 기술은 차량 주행 관련 주변 교통 정보를 빠르게 수집하며 해석 및 의사결정을 신속히 실행하는 데 사용됨
- 측위 기술은 주변 환경 인식의 개선을 위한 기술로써 정밀한 자동차 위치를 추정하면 최적의 제어로 안전성 향상 및 연비 절감 효과가 있음
- V2X 기술은 차량 주행 중 유·무선망을 이용하여 다른 차량 및 도로 등 인프라가 구축된 사물과 서로 교통 상황 등의 정보를 교환하는 데 사용됨

○ 자율주행차의 안전 관련 현안 및 시사점

- 2016년 2월 구글의 자율주행차 사고 및 2016년 5월 테슬라 모델S 사망 사고 등 자율주행차 사고가 발생하면서 안전이 중요한 과제로 부상하였으며 해당 사례의 분석을 통해 향후 연구 방향의 제시가 필요
- 자율주행차는 기존 차량보다 더 많은 전자·통신 기능을 내장하여 보안 취약점 및 오작동의 위험이 증가하고 있으므로 이에 대한 보안적, 기술적 측면의 개선 노력이 필요

(2) 시설물 안전 : 스마트 빌딩

○ 스마트 빌딩의 정의와 특징

- 스마트 빌딩은 IT 기술을 통해 건물시스템을 제어하여 성능을 최적화하며, 건물의 사용자에게 쾌적하고 안전하며 건강한 환경을 제공함

- 스마트 빌딩은 초기 투자비의 회수 비용이 짧고, 건물의 세입자를 쉽게 구할 수 있는 등 경제적이며, 건물의 냉난방 및 조명 비용을 최대 50% 까지 감소하는 등 에너지 절약적인 특성이 있음

○ 스마트 빌딩의 시장 및 정책 동향

- 스마트 빌딩의 서비스 시장 규모는 전 세계적으로 2015년 130억 달러에서 2020년 320억 달러로 연간 22%의 성장이 예측됨
- 스마트 빌딩에서 IoT(Internet of Things)기기는 IoT 설치에 따른 보조금 지급, 기설치된 건물자동화시스템과의 연계 등으로 건물의 에너지 소비를 줄일 수 있어 IoT 관련 기기 및 서비스가 시장을 선도할 것으로 전망됨
- 미국은 총무부를 중심으로 건물의 에너지 소비 감소, 건물 관리의 효율 향상과 건물 사용자의 만족도 향상을 목표로 스마트 빌딩 정책을 운용 중임
- 우리나라는 국가 차원에서 스마트 빌딩의 구현을 위하여 ICT 및 IoT와 연계된 건물에너지관리시스템의 개발을 지원하고 있음

○ 스마트 빌딩의 요소 기술

- 스마트 빌딩은 다수의 서로 다른 제조사와 다양한 장비가 사용되며 이러한 장비를 하나로 통합 제어하기 위해서는 공통의 언어를 사용한 데이터의 송수신이 필수적이며 대표적인 통신방법은 BACnet과 Zigbee가 있음
- 스마트 빌딩의 주요 구성 요소와 기술은 건물 자동화 시스템, 냉난방공조시스템, 조명 시스템, 엘리베이터, 방재 시스템, 방범 시스템과 통신 시스템으로 구분되며 최근 빅데이터 기술과 인공지능 기술이 주목받고 있음

○ 스마트 빌딩의 안전 관련 현안 및 시사점

- 스마트 빌딩은 주요 제어시스템과 IoT 기기는 서로 연동이 되어 있어 IoT에 대한 보안이 매우 중요하며 외부 해킹에 대한 선제 대응이 필요함
- 또한 건물 사용자의 생명을 보호하고 안전을 확보하기 위해서는 방재 시스템과 다른 건물자동화 시스템과의 통합 및 상호 운용성을 향상하는

것이 요구됨

(3) 사회기반(금융) 안전 : 블록체인

○ 블록체인의 정의와 특징

- 블록체인이란 거래 내용을 저장한 블록을 특정한 서버가 아닌 네트워크를 통해 분산 저장하고 일정 시간마다 암호화 후 체인 형태로 연결하여 저장하는 기술로써 제3자의 신뢰 없이 이중 거래를 차단하여 확실하고 안전한 거래를 보장함

○ 블록체인(금융 분야)의 시장 및 정책 동향

- 블록체인 기술은 2020년 연간 성장률 120%를 기록하고 시장 규모는 2030년 3,400조 원 규모에 달할 것으로 예측됨
- 은행 및 증권, 대출, 자산 관련 분야에서 블록체인 기술을 활용한 다양한 서비스를 출시하거나 출시에 대한 계획을 수립하고 있음
- 미국, 일본 등 주요국은 금융 분야의 컨소시엄을 발족하여 국가별 실정에 맞도록 산업체와 정부의 협력을 통해 발전하고자 노력하고 있음
- 국내에서도 금융권 블록체인 협의회를 발족하여 은행 및 금융투자업권 컨소시엄 간 소통을 강화하고 정보 공유 및 제도 개선사항 등을 검토하고 있음

○ 블록체인의 요소 기술

- 암호기술로부터 블록체인의 신뢰성과 투명성이라는 특성이 확보되며 암호학적 해시함수(cryptography hash function)는 데이터가 변조되었는지를 확인하는 역할을 수행함
- 또한 전자서명(digital signature)은 데이터가 실제 주인(owner)에 의해 작성되거나 수정되었는지를 증명함
- P2P 네트워크를 통해 블록체인이 네트워크의 여러 노드에 분산 저장됨에 따라 변조는 더욱 어려워지고 투명성이 제고됨

○ 블록체인을 활용한 사회기반(금융)의 안전 관련 현안 및 시사점

- 블록체인의 활용 과정에서 많은 혼란과 피해가 발생하고 있으며, 암호화폐 탈취, ICO 관련 피해, 부정 거래와 스마트 거래의 취약점 등 대표적인 금융 분야의 사고 사례를 중심으로 안전 관련 현안을 도출함

- 각종 사고 사례를 살펴본 결과, 문제의 원인은 블록체인 자체라기보다는 이를 활용하는데 있어 낮은 보안 의식, 관련 정책 부재 및 미흡, 기술력 부족 등이 문제라고 볼 수 있음

2) 행정관리 측면에서의 안전관리체계 리모델링 연구

(1) 교통안전 : 자율주행차와 안전

- 교통 안전관리체계 현황 분석 및 개선방향 도출
 - 현재의 교통 안전관리체계는 다양한 법령이 관련되어 있으며, 교통 안전관리 주관 부처도 분산되어 있는 등 정책 추진을 위한 일관적인 체계가 취약한 편임
 - 지능정보기술 도입에 따른 위험관리 및 교통 안전관리체계 운영을 위한 전문인력 양성이 시급함
- 교통 안전분야의 지능정보기술 도입에 따른 영향 검토
 - 지능정보기술이 도입될 경우 교통 안전분야에 있어서 긍정적인 변화와 더불어 부정적인 변화도 함께 예상됨
 - 특히 기존의 교통 안전 위험요소와 지능정보기술 도입에 따라 새롭게 발생할 수 있는 위험요소의 혼재가 예상됨
 - 정보통신기술의 활용에 따라 교통 안전관리 시스템 및 개인정보의 관리와 관련한 위험 발생 가능성이 제기됨
- 교통 분야 국가안전관리체계 개선방안 도출
 - 기존 교통 안전관리체계의 한계를 극복하고 지능정보기술이 도입됨으로써 발생하게 될 다양한 위험에 대처하기 위한 통합적인 교통 안전 거버넌스 체계의 구축이 필요함
 - 교통분야 지능정보기술에 대한 이해도 높은 전문 안전관리 인력 양성을 위한 제도 도입이 요구됨
 - 지능정보기술 도입에 따른 교통 안전관리체계의 정보보안 및 개인정보 보호 문제에 대한 효율적인 대처방안의 마련이 필요함
 - 자율주행차와 관련해 선진국의 법제들을 검토하여 다양한 이슈들에 대응할 수 있는 준비가 필요함

(2) 시설물 안전 : 스마트 빌딩

○ 시설물 안전관리체계 현황 분석 및 개선방향 도출

- 시설물 안전관리체계와 관련한 법제 및 정책 현황에 대한 분석을 통해 문제점을 파악하고 개선방안을 제시함
- 국내 정책현황에 관한 최신 정부 간행물 및 국책 연구기관 보고서 등을 분석하고 전문가 자문을 통해 개선방안을 도출함

○ 지능정보기술에 따른 영향 검토

- 국내외 전문 문헌 분석 및 전문가 조사를 통해, 건축·시설물에 대한 영향을 분석함
- 지능정보기술 적용 시설물이 아직 안착되거나 일반화되지 못한 특성을 고려하여, 다양한 분야의 최신 동향을 분석하여 반영함
- 스마트 도시 등 거시적 관점에서의 영향에 대해 분석하여, 지능정보기술 사회의 특징인 초연결성 측면에 대해 고려하도록 검토함

○ 건축·시설물 분야 국가안전관리체계 개선방안 도출

- 건축·시설물의 생애주기(설계-시공-관리-개·보수 단계)별 맞춤형 안전관리 체계를 마련하여 최대의 효용을 창출하고, 안정적인 활용이 필요함
- 지능정보기술 도입에 따른 건축·시설물 안전관리 관련 법제의 마련과 기술변화에 따른 안전관리 체계 방안을 지속적으로 반영함
- 일관된 원칙과 시스템에 따른 정보 입수가 가능하도록 중앙정부, 지방자치단체, 그리고 관련 민간업체 등이 협력하는 체계가 요구됨
- 사회경제문화적인 측면과 기술적인 측면 등 다각적인 영향을 고려한 안전관리 체계의 구축이 필요함

(3) 사회기반(금융) 안전 : 블록체인

○ 사회기반(금융) 분야 안전관리체계 현황 분석 및 개선방향 도출

- 사회기반(금융) 안전 분야 안전관리체계와 관련한 법제 및 정책 현황에 대한 분석을 통해 문제점을 파악하고 개선방향을 제시함
- 국내 정책현황에 관한 최신 정부 간행물 및 국책 연구기관 보고서 등을

분석하고 전문가 자문을 통해 개선방향을 도출함

○ 지능정보기술에 따른 영향 검토

- 국내외 문헌 분석 및 전문가 조사를 통해, 사회기반(금융) 안전 분야에 대한 영향 분석 및 긍정적/부정적 변화 요소를 파악함
- 특히 기존의 사회기반(금융) 안전 분야 위험요소와 지능정보기술 도입에 따라 새롭게 발생할 수 있는 위험요소의 혼재가 예상됨

○ 사회기반(금융) 분야 국가안전관리체계 개선방안 도출

- 법령에서는 원칙만 제시하고 하부기관들이 지침 형태로 제정하여 운영하는 방안과 네거티브 접근 방법, 사후 규제, 샌드박스(sandbox) 등을 활용한 파일럿식 접근에 대한 고려가 필요함
- 금융 사고에 대한 보다 체계적이고 근본적 대응을 위한 전문가 양성 및 시스템이 필요함
- 금융 위험 파악과 관리에 블록체인, 빅데이터, AI 등의 기술을 활용하는 방안을 고려해야함
- 금융 안정을 위한 글로벌 차원의 위험관리 통제센터 네트워크 연계 및 공동 활용 방안 구축이 필요함

3) 법·제도 측면에서의 안전관리체계 리모델링 연구

(1) 교통안전 : 자율주행차와 안전

○ 현행 교통 분야 안전관리체계 조사 및 분석

- 재난안전 관리체계의 기본법인 ‘재난 및 안전관리 기본법’ 등 관련 법률상의 교통안전 분야에 대한 안전관리 체계를 분석함
- 자율주행차 안전관리제도 관련 법령에 대한 검토로 자동차관리법, 도로교통법, 제조물책임법, 자동차손해배상보장법, 보험법 등 기존 자동차 안전관리 관련 법령에 대한 검토를 수행함
- 자율주행차의 관리에 대한 개별 법률은 아직 없는 상황으로 2016년 자동차관리법을 개정하여 자율주행차에 대한 근거 규정을 마련하였으나 향후 추가적인 관련 법률에 대한 정비가 필요한 실정임

○ 자율주행차 등 지능정보기술의 상용화 과정의 문제점

- 신기술을 기반으로 하는 자율주행차의 제조과정에서의 기술적 결함, 운행 과정에서의 안전사고 등 많은 법적 문제의 발생 가능성이 있음
- 행정적 관점에서는 자율주행차를 위한 운전면허시험과 발급 등 운전면허제도의 변화가 필요하고, 책임보험 등 차량보험제도 등 안전관리 체계의 리모델링이 요구됨
- 신기술을 기반으로 자율주행차의 사용 및 이용 상의 안전확보와 운행 중 발생한 안전사고의 손해배상 등 책임분담 문제와 자율주행 시스템에 대한 해킹과 개인정보 침해 문제를 검토함
- 해외 현황과 교통안전관리체계 조사 및 분석
 - 미국, 일본, 독일, 프랑스 등 주요 국가의 자율주행기술의 교통 분야 활용 현황과 자율주행차의 안전한 이용을 위한 안전관리제도 정비 현황을 조사함
 - 국가마다 다소 차이가 있으나 아직 자율주행차를 규율하는 개별법은 없는 상황임
- 자율주행차 등 지능정보기술에 따른 교통안전관리체계 구축 방안 제시
 - 자율주행차에 대한 기술적 안전관리를 전담하는 부서의 확대와 범정부적 차원의 협력과 부처 간 업무를 명확히 수립하는 자율주행차 안전관리 체계 구축이 필요함
 - 교통안전 관련 개별 법령에 대한 제도 개선방향과 명확한 안전관리 기준의 설정, 자율주행자동차의 시스템 결함 가능성에 대비하고 각종 안전사고를 사전에 예방하기 위한 새로운 규정의 도입 등을 제시함

(2) 시설물 안전 : 스마트 빌딩

- 스마트 빌딩 상용화에 따른 안전관리 문제의 제기
 - 신기술을 바탕으로 현존 건축물·구조물을 통제·운영할 수 있는 스마트 빌딩에 대해 최근 각종 논의들이 진행되고 있으나 법제 지원적 관점의 접근은 전혀 없는 상황임
 - 또한 스마트 빌딩은 해킹에 의한 악의적 공격이나 시스템 자체의 기술적 취약점이 발생하는 경우를 대비하지 않는다면 오히려 스마트 빌딩을 구축하지 않는 것보다 더 심각한 피해가 발생할 가능성이 있음

- 현행 건축·시설물 분야 안전관리체계 조사 및 분석
 - 우리나라의 스마트 빌딩에 대한 정책은 기후변화에 대응한 저탄소정책과 에너지 효율화, 신재생에너지 정책 등의 한 분야로 추진되고 있음
 - 현행 안전관리제도 체계상 시설물 안전의 주무부처는 국토부이며, 산자부가 스마트 빌딩에 대한 지원 정책을, 과기정통부가 신기술과 관련한 지원정책을 담당하고 있음
 - 스마트 빌딩의 안전관리는 건축법, 시설물의 안전관리에 관한 특별법 등 기존의 시설물 안전 법률의 적용을 받으며, 스마트 빌딩을 규정한 개별 법률이나 규정이 없는 상황임
- 인공지능 센서 등 지능정보기술을 활용한 스마트 빌딩의 상용화 과정의 문제점
 - 기존 법·제도 한계로 제기될 관리상의 법적 문제를 스마트 빌딩 설계 및 건축과정에서의 안전관리, 스마트 빌딩 시스템의 보안과 개인정보보호를 중심으로 관련된 내용을 분야별로 검토함
- 스마트 빌딩 관련 해외 시설물 안전관리체계 조사 및 분석
 - 주요 국가의 스마트 빌딩 관련 법제정비 현황을 조사한 결과, 미국, 영국, 프랑스 등 대부분의 국가에서 스마트 빌딩 정책은 에너지 효율화, 기후변화 대응정책의 하나로 추진되고 있음
 - 입법 현황의 경우, 아직 스마트 빌딩을 대상으로 하는 법률은 없으며 에너지법이나 기후변화 대응 관련 법률에서 일부 규정하고 있음
- 스마트 빌딩의 등장에 따른 건축·시설물 안전관리체계 리모델링 방안 제시
 - 스마트 빌딩 정책의 경우, 기술적 안전관리가 핵심적 사항이므로 이를 전담하는 부서를 명확히 하고 이를 확대할 필요가 있음
 - 일본의 경우 스마트 빌딩과 주택에 대한 정책 추진과 관리는 경제산업성과 국토교통성이 담당하고 있으며, 미국은 스마트 빌딩 진흥법안을 마련하여 스마트 빌딩의 활성화를 지원하고 있음

(3) 사회기반(금융) 안전 : 블록체인

- 블록체인 등 신기술의 현황 및 이를 활용한 암호화폐의 등장이 금융분야에 미치는 영향 분석
 - 블록체인 기술을 활용한 암호화폐의 등장은 중앙은행이 발행하는 법정화폐 중심의 기존 금융제도 전반에 충격을 주고 있음
 - 중앙은행의 통제를 벗어나 지급 및 거래수단을 만들려는 시도는 통화의 가치와 안전성을 보장하는 기존의 금융제도를 와해시키고, 이를 이용해 투기적 수단으로 악용하려는 불법적 행위라는 시각이 일반적임
- 암호화폐 관련 국내 안전관리 법률체계 및 정책 조사 및 분석
 - 국가의 재난안전 관리체계의 하나인 사회기반안전(금융)분야에 대한 안전관리 체계를 분석함
 - 현재 정부 정책은 암호화폐가 투기적 수단으로 변질되고, 불법적인 투자자 모습과 불법적 거래가 문제되어 이를 규제하는 방향으로 정책 마련 중임
- 블록체인 신기술의 안전한 활용을 위한 관련 법령에 대한 검토
 - 블록체인 신기술을 활용한 암호화폐의 법적 개념과 법적 허용여부 검토
 - 암호화폐의 안전적 활용을 위한 전자문서 및 전자거래기본법, 전자금융거래법, 개인정보보호법, 전자서명법, 상법, 주식 및 사채 등의 전자등록에 관한 법률, 자본시장과 금융투자업에 관한 법률 등에 대해 검토함
- 블록체인 등 신기술의 활용 과정의 문제점 분석
 - 블록체인 기술에 기반을 둔 암호화폐의 등장으로 기존의 금융관리제도의 한계가 나타나 이로 인하여 많은 법적 문제가 발생할 것으로 예상됨
 - 암호화폐를 활용한 자금세탁 등 불법행위, 암호화폐에 대한 세금문제, 암호화폐를 가장한 불법자금모집이나 사기대출유인 등에서 법적 문제가 발생하고 있음
- 블록체인(암호화폐) 관련 해외 안전관리 법체계 조사 및 분석
 - 미국, 일본, 프랑스 등 주요 국가의 블록체인 기반의 암호화폐 현황 조사 및 관리제도 조사 및 분석함
 - 비트코인 등 암호화폐의 법적 허용에 대해서는 국가마다 다소 차이가 있으며 암호화폐에 대한 개별법은 존재하지 않음

- 블록체인 등 신기술의 활용에 따른 금융안전관리체계 구축 방안 제시
 - 투기적 목적을 가진 암호화폐 거래에 대한 규제의 필요성이 있으므로 향후 제도개선과 관련하여 암호화폐의 본질과 법적 성격에 대한 더 많은 연구가 요구됨
 - 암호화폐의 안전한 거래 및 최소한의 보호를 위해서 암호화폐 거래소에 대해서는 일정 거래량 이상을 부담할 수 있는 서버 증설 및 거래소 내부 규율, 보안 강화 등 이에 대한 규제방안을 마련하고, 동시에 암호화폐의 건전한 발전에 대한 지원이 필요함

5. 기대 효과

- 지능정보화사회의 도래로 파급력이 큰 교통 안전, 시설물 안전, 사회기반(금융) 안전 분야를 선정하여, 기술적 측면에서 지능정보기술의 도입 현황과 요소 기술 분석을 도출하고, 그 결과를 토대로 행정관리 및 법·제도 측면에서 리모델링 방향을 제시하여 새로운 안전관리체계의 효율성 강화와 안전관리 정책의 정합성 제고
- 분야별 국민 안전강화를 위한 기술적 발전방향과 행정 관리, 법령 및 제도 개선방안을 제시하여 신기술에 의한 사회변화에 적합한 안전관리체계 확립과 정책 구현에 대한 기초자료 마련

Summary

The study deals with the improvement of safety management system for traffic, facility, and social infrastructure (financial) safeties, which is expected to change drastically due to the advent of the intelligence information society. For comprehensive and specialized research from various perspectives, we, the Software Policy & Research Institute (SPRi), conducted collaborative research with the Korea Institute of Public Administration (KIPA) and the Korea Legislation Research Institute (KLRI).

The SPRi researches the core technologies of autonomous vehicles, smart buildings, and blockchain, which are representative technologies in the selected safety fields. Then the SPRi predicts social change in technology commercialization process and describes the relationship between the new technology and safety. The KIPA describes social change according to the emergence of the intelligence information society, analyzes the major issues expected when applying the new technology. Also, KIPA diagnoses the problems of the existing safety management system and suggests plans for effective response. The KLRI has drawn up problems through analysis of existing safety management systems and legislative cases in each safety field, and proposes directions in the perspective of the legal and institutional required for effective responses in the future. In particular, KLRI analyzes the major legal issues in intelligent information technology from the perspective of law system.

Autonomous vehicle is the technology that will have the greatest impact on traffic safety. Its elemental technologies are classified into three categories: environmental recognition, positioning, and V2X technologies. Based on these elemental technologies, major overseas countries have been responding and systematically improving their self-driving car safety. Predictions of the timing of commercialization of autonomous vehicles vary from research institutes to project, but they are expected to be within around 5 to 10 years. Autonomous vehicles can be considered to affect safety in two aspects, such as security

and technology itself. Particularly, although there are no official hacking accidents that have been confirmed or reported so far, it has proved that computer systems in vehicles can be hacked through numerous researches and experiments in various countries.

In order to improve the traffic safety management system in perspective of administrative management, it is necessary to establish a traffic safety governance system, nurture professional manpower, set up information security and personal information protection plan, and actively introduce advanced cases. Firstly, the establishment of integrated traffic safety governance system should be given priority to cope with the various risks that will arise from the advent of intelligent information technology. Secondly, it is necessary to foster traffic safety management professionals who are familiar with both transportation and intelligence information technology. Thirdly, when intelligence information technology is introduced into the traffic safety management system, measures for building a higher level information security system and protecting personal information should be prepared. Finally, it is necessary to review the legal systems of developed countries in relation to autonomous vehicles and be prepared to cope with various issues.

In perspective of the improvement of the legal system, it clarifies the responsibilities of the autonomous driving vehicle, reforms the regulations on the use of the vehicle, raises the safety of the autonomous driving system, and reorganizes the insurance system. Firstly, if a traffic accident occurs due to the operation of an autonomous vehicle, it may cause complicated problems about the criminal and civil liability of the related parties such as the driver, the manufacturer, and the software developer. Therefore, the responsibility for the autonomous vehicle must be clarified. Secondly, the current legislation focuses on how vehicles are used and maintained, so the framework of this legislation needs to be revised to allow the use of autonomous vehicle technology without test drivers and ensure that the technology is maintained correctly. Thirdly, it is necessary to establish a strong legal apparatus to

protect autonomous vehicles from potential cyber threats, and to apply stricter technical standards to autonomous vehicles. Fourthly, a separate insurance system with new compensation standards is needed to prepare for the special accidents that may occur during the operation of autonomous vehicles.

Smart buildings that can affect the safety of facilities can be divided into communication technology and new emerging technology. BACnet and Zigbee are typical communication technologies. They are mainly used for short distance communication in smart buildings. Recently, a smart building has been transformed into an intelligent building that is combined with the emerging technologies such as big data, artificial intelligence, and IoT technology. As ICT technology is applied to building automatic control system, which is a core element of smart building, real-time monitoring of various types of data produced in smart buildings. Smart buildings have opportunities and crises associated with building safe societies. Smart Building's IoT-based communication system enables the fire detection and the organic connection of the suppression facility and the air conditioning system to detect and evolve the fire prematurely. On the other hand, IoT devices widely used in smart buildings are interlocked with the main control system of buildings, so that security threats in IoT environment are various, such as device loss and physical destruction, signal disturbance, information leakage, data modulation.

Improvement for facility safety in administrative management are as follows. Firstly, a customized safety management system for each life cycle (design - construction - management - maintenance - repair phase) of buildings and facilities should be established to create the maximum utility in its use and to utilize buildings and facilities for users in a stable state. Secondly, in order to ensure the safety management of buildings and facilities, it is necessary to continue to support the legal system so that such intelligent information technology can be introduced and operated. Thirdly, a system in which central government, municipal governments, and related private companies cooperate is required to enable the acquisition of information based on consistent principles

and systems. Finally, it is required to construct a safety management system considering various effects.

In perspective of the legal system, the ways to improve the safety of facilities are as follows. Firstly, Smart Building utilizes cutting edge ICT. Urban planning is an important factor in building social infrastructure, so it is necessary to build an integrated network for smart building management. Secondly, mitigation plans are needed to solve the problem of initial investment cost related to building of smart buildings. Thirdly, there is no legal definition of smart building in current law, and related laws such as existing building law require builders to withstand typical risks such as earthquake and typhoon. However, it is necessary to prepare laws related to smart building.

The blockchain technology, which has the greatest influence on the social infrastructure, especially financial sector, consists of cryptography and P2P network technologies. From a technical point of view, the greatest risks to social infrastructure security are hacking the cryptographic exchange, fraud using ICO, leakage of personal information, and smart contract hacking. In all cases of accidents, rather than the problem of the blockchain itself, it was a problem of insufficient security consciousness, lack of relevant policy and technology in utilizing it in the financial sector.

The improvement of the social infrastructure (financial) in the aspect of administration management are as follows. Firstly, there is a need to adapt centralized and vertical regulation to a distributed system of blockchains. Secondly, we need to develop a more systematic and fundamental system and educate experts in preparation for security incidents such as financial leaks and personal information leakage. Thirdly, we must consider the use of the blockchain technology actively in the identification and management of financial risks. The blockchain can be utilized for the creation of public information sharing infrastructure, expansion of collaboration among agencies, public service certification, and public data transactions. Fourthly, in order to stabilize the financial system, it is necessary to consider the linkage with the global network

based on digital technology and the common utilization plan. In the future, it will be impossible to manage individual factors affecting national safety. Therefore, there will be a way to establish a network between national and regional risk management and control centers so that national management and regional plans can be organized.

In perspective of legal system, the ways to improve the social infrastructure (financial) are as follows. Firstly, since the advent of cryptocurrency is not that long, we need more legal study on the legal nature of cryptocurrency. Secondly, we need to regulate the current situation of trading in cryptocurrency for speculative purposes. The effect of the cryptocurrency law is that the scope of the regulation will vary depending on how strictly the control and supervision of the regulation is achieved. However, it is expected that the risk of capital and speculative fraud will be greatly reduced through the Japanese cryptocurrency law regulation. It can also lead to healthy development of the cryptocurrency exchange industry.

The analysis of market and policy status and element technology in traffic, facility, and social infrastructure (finance) safeties that are considered to be influential in the coming of the intelligent information society. Based on the results of this study, the remedial direction is suggested in terms of administrative management and legal system to enhance the efficiency of the new safety management system and the consistency of the safety management policy. Finally, the technical development direction for the national safety enhancement in each field and administrative management, laws and regulations and system improvement plans were laid out, and the basic data on the establishment of the safety management system and the policy implementation suitable for the social change by the new technology were prepared.

CONTENTS

Chapter 1. Introduction	1
Chapter 2. Focused on Technology	5
Chapter 3. Focused on Administrative Management	94
Chapter 4. Focused on Legal System	138
Chapter 5. Conclusion	199

제1장 서론

제1절 연구의 배경 및 목적

1. 연구의 배경

알파고와 같은 인공지능 기술의 비약적인 발전, 모든 사물이 연결되는 IoT(Internet of Things, 사물인터넷)의 대중화, 세상에 없던 블록체인 기술의 등장 등 새로운 기술의 등장과 발전으로 우리 사회는 급격히 변하고 있다. 혹자는 이러한 사회를 ‘지능정보사회’라 부르기도 하고 ‘제4차 산업혁명’이 도래했다고도 말한다. 이 사회가 어떻게 불리든 간에 새로운 기술로 새로운 사회가 도래하였음은 자명해 보인다. 경제, 사회, 일상의 삶 등 모든 분야에서 신기술은 보편적으로 사용되고 이전에 없던 새로운 가치를 창출하고 있다.

지능정보사회의 도래는 그간의 사회 변화와는 다른 엄청난 변혁(變革)을 우리에게 가져다주고 있다. 예를 들어, 교통 분야의 경우 자율주행차의 등장으로 인해 기존의 교통 안전관리체계의 새로운 ‘디자인(design)’이 필요하다. 도로 교통체계부터 관련 법령, 보험제도, 관리체계까지 모든 영역에 대해 재설계를 해야 한다. 스마트 빌딩의 등장은 그간의 시설물 안전 관리체계의 변화를, 블록체인의 등장은 금융 분야의 사회기반 안전 관리체계의 변화를 요구하고 있다. 이러한 분야야말로 지능정보사회의 변화 요구에 따라 국민의 안전을 확보하고 강화하는데 파급효과가 클 것으로 예상된다.

지금까지의 연구들은 새로운 기술을 이용하여 좀 더 안전을 확보하거나 보완하는 데 집중하였다¹⁾²⁾. 인공지능과 빅데이터 기술을 이용하여 CCTV로 촬영한 실시간 영상에서 범죄 패턴을 분석하여 범죄 발생을 예측해 준다. 재난망을 통해 지진이나 해일에 대한 경보를 해당 지역 주민들에게 거의 실시간으로 알려주기도 한다. 그간의 안전 연구에서는 신기술을 이용한 안전 확보가 대부분이었다. 그러나, 새로운 기술로 변화가 필요한 안전관리체계에 대한 깊이 있는 연구는 미흡하다.

1) 최선화 외, “빅데이터를 활용한 재난관리 역량 강화”, 국립재난안전연구원, 2015

2) 최호진 외, “첨단기술을 활용한 스마트형 생활안전 관리방안 연구”, 한국행정연구원, 2014

따라서, 지능정보사회의 도래를 대비하여 기존 안전관리체계의 재설계가 필요한 시점이다. 특히, 국민의 신체와 생명, 재산에 직접적인 영향을 줄 교통 안전, 시설물 안전, 사회기반(금융) 안전에 대해 우선적인 검토가 필요하다. 이러한 분야에 대해 새로운 기술, 법·제도 및 행정관리 등 다양한 관점에서 종합적이고 전문성 있는 연구가 필요하다. 기술, 법·제도, 행정관리에 대한 구체적인 연구의 필요성은 다음과 같다.

첫째, 기술 중심의 연구에서는交通安全 분야의 자율주행차, 시설물 안전 분야의 스마트 빌딩, 사회기반 안전(금융) 분야의 블록체인 기술에 대해 깊이 있는 분석과 이해가 필요하다. 이러한 요소 기술의 이해를 바탕으로 해당 분야의 기술 상용화 과정에서의 사회 변화를 예측하고 안전과의 관계를 분석하는 데 필요하다. 또한, 법·제도 및 행정 관리 측면에서의 기존 체계 재설계 시 기초 자료로 활용될 수 있다.

둘째, 행정관리 중심의 연구에서는 지능정보사회 출현에 따른 사회변화 내용 분석, 신기술 적용 시 예상되는 주요 쟁점 분석, 기존 안전관리체계의 문제점 진단, 그리고 효과적인 대응을 위한 변화 및 개선방안 등을 정부 행정 차원에서 종합적으로 도출이 필요하다. 이를 위해 각 분야의 안전관리 추진체계 분석, 지능정보기술로 인한 미래위험 대응 정책 현황 분석, 안전관리체계 리모델링 방향의 도출이 필요하다. 또한, 각 분야의 문제 해결과 향후 효과적인 대응을 위해 변화관리 방향 및 정책과제, 그리고 장·단기적 추진 방안의 도출이 요구된다.

셋째, 법·제도 중심의 연구에서는 신기술에 의한 변화요구에 적극적으로 대응하고 국민들이 믿을 수 있는 정보를 보다 안전하게 활용할 수 있는 사회 기반 시설의 마련이 필요하다. 또한 신기술의 사용과정에서 발생하는 위험으로부터 안전할 수 있도록 새로운 관점에서의 법·제도적 안전관리체계를 구축하기 위해 지능정보기술 적용 시 예상되는 주요 법적 이슈 및 쟁점 분석이 필요한 상황이다.

인공지능, 빅데이터, IoT, 블록체인 등 다양한 신기술이 사회의 혁신을 이끄는 지능정보사회를 미리 대비하기 위해서는 국민의 안전을 확보하는 새로운 안전관리체계 구축이 밀바탕 되어야 한다. 이러한 분야에 대해 기술, 법·제도 및 행정관리에 대한 다양하고, 종합적이고, 전문성 있는 관계 연구기관의 협동 연구

가 필요한 시점이다. 본 연구를 통해 지능정보화사회에 적합한 교통 안전, 시설물 안전, 사회기반(금융) 안전 분야 등 분야별 안전관리체계의 리모델링 방안제시와 관련 기초자료로 활용할 수 있을 것이다.

2. 연구의 목적

상기에서 살펴본 바와 같이 지능정보사회의 도래로 기존 안전관리체계를 개선해야 하는 압력에 직면해 있다. 기존의 안전관리체계는 새로운 지능정보기술로 인한 사회 변화를 적극적으로 반영하지 못하고 있다는 지적을 받는 실정이다. 이러한 변화를 가져온 새로운 기술에 대한 깊이 있는 이해가 절실하다. 또한, 법·제도적인 측면과 행정관리 측면에서의 기존 안전관리체계의 개선 방안 연구 역시 요구되고 있다.

이에 본 연구에서는 지능정보사회 변화 요구에 따라 신기술이 적용되어 국민의 안전을 확보·강화하는데 파급효과가 클 것으로 예상하는 세 분야(교통 안전, 시설물 안전, 사회기반(금융) 안전)를 대상으로 신기술(지능정보기술)의 출현에 효과적으로 대응하기 위한 변화 및 개선방안 등을 기술, 법·제도, 행정관리 측면에서 종합적으로 도출하여 제시하고자 한다.

제2절 연구의 구성 및 방법

1. 연구의 구성

본 협동 연구보고서는 총 4권으로 구성된다.

제1권 총론에서는 제2권부터 제4권까지의 내용을 요약 기술한다. 제1장에서는 서론으로서 연구의 배경, 필요성, 목적 등을 기술한다. 제2장은 제2권 기술 중심 보고서를 요약한다. 제3장에서는 제3권 행정관리 중심 보고서를, 제4장에서는 제4권 법·제도 중심 보고서를 각각 요약한다. 제5장에서는 지금까지 내용을 정리한다.

제2권(소프트웨어정책연구소 연구수행)에서는 자율주행차(제2장), 스마트 빌딩(제3장), 블록체인(제4장) 등 신기술에 대해 시장 및 정책 동향을 살펴보고 요

소 기술에 관해 설명한다. 제5장에서는 해당 기술과 관련된 안전 현안을 정리하고 이를 바탕으로 시사점을 도출한다.

제3권(한국행정연구원 연구수행)에서는 교통 안전(제2장), 시설물 안전(제3장), 사회기반(금융) 안전(제4장) 분야의 안전관리 추진체계를 분석하고, 지능정보기술로 인한 미래위험 대응 정책 현황 분석한다. 제5장에서는 각 분야의 문제 해결과 향후 효과적인 대응을 위해 요구되는 변화관리 방향 및 정책과제, 그리고 장·단기적 추진 방안을 도출한다.

제4권(한국법제연구원 연구수행)에서는 교통 안전(제2장), 시설물 안전(제3장), 사회기반(금융) 안전(제4장) 분야의 주요 법적 이슈와 쟁점을 분석한다. 제5장에서는 각 분야의 기존 안전관리체계 및 입법사례 분석을 통하여 도출된 문제를 해결하고, 향후 효과적인 대응을 위해 요구되는 변화관리 방향을 제시한다.

2. 연구의 방법

지능정보사회의 변화에 대응 가능한 안전관리체계 구축을 위해 다양한 측면에서 기술, 법·제도 및 행정관리에 대한 종합적이고 전문성 있는 관계 연구기관의 협동 연구를 수행한다. 그림 1-1에서와 같이 기술, 행정관리, 법·제도 분야에서 각각 전문성을 갖는 소프트웨어정책연구소, 한국행정연구원, 한국법제연구원 간의 협동 연구를 통해 본 연구를 수행한다. 각 기관의 연구 방법은 다음과 같다.

[그림 1-1] 협동 연구에 참여하는 전문 연구 기관



소프트웨어정책연구소는 교통 안전, 시설물 안전, 사회기반 안전(금융) 분야를 대상으로 새롭게 등장한 신기술인 자율주행차, 스마트 빌딩, 블록체인 기술에 대한 시장 및 정책 동향, 요소 기술에 대해 조사와 안전과의 관계를 제시한다. 기본적으로는 문헌연구를 중심으로 해당 기술 분야의 활용 현황과 각국의 정책 및 국내 현황에 대해 조사를 수행한다. 국내외의 정책문서, 정책보고서, 연구보고서, 학술논문 등이 주된 대상이다. 국내 자율주행차, 스마트 빌딩, 블록체인 기술의 전문가와의 인터뷰를 통해 연구보고서의 적실성을 높인다. 협동 연구의 목적을 달성하기 위해, 참여 기관들은 정기적인 회의로 필요한 정보를 공유하고 연구 방향을 조율해 나간다.

한국행정연구원은 교통 안전, 시설물 안전, 사회기반(금융) 안전 분야의 안전관리 추진체계를 분석하고, 지능정보기술로 인한 미래위험 대응정책 현황을 분석하고, 각 분야의 문제 해결과 향후 효과적인 대응을 위해 요구되는 변화관리 방향 및 정책과제, 그리고 장·단기적 추진 방안을 제시한다. 또한, 연구의 품질 제고 및 연구 추진 방법, 개발 내용 등의 적절성을 평가하기 위하여 본 연구의 관련성(재난/안전관리, ICT 기술, 정책 개발 및 진단/평가 등)을 고려하여 연구자문단을 구성·운영한다. 연구자문단의 수시 자문 기능을 활용하여 연구의 적절성 및 효과성 등을 평가, 환류하여 품질을 보증한다.

한국법제연구원은 교통 안전, 시설물 안전, 사회기반(금융) 안전 분야의 기존 안전관리체계 및 입법사례 분석을 통하여 도출된 문제를 해결하고, 향후 효과적

인 대응을 위해 요구되는 변화관리 방향을 도출한다. 특히, 미국, 영국, 프랑스, 독일, 일본 등 해외 지능사회대비 현황과 이에 따른 안전관리 정책 및 입법사례 조사 및 분석한다. 또한, 원내 연구진 이외에 인공지능 등 다양한 신기술 분야 전문가, 안전관리제도 입법전문가, 안전관리 분야 정책전문가, 관련 행정 실무자 등으로 구성된 자문위원회를 적극적으로 활용하여 정책 반영도를 높인다.

제2장 기술 중심으로

제1절 개요

본 장에서는 소프트웨어정책연구소에서 “지능정보사회를 대비한 안전관리 체계 리모델링에 관한 연구 - 기술 중심으로”라는 주제로 작성한 제2권의 내용을 요약 정리한다.

1. 추진 배경

지능정보사회로의 도래로 국민 안전에 파급력이 클 것으로 예상하는 교통 안전, 시설물 안전, 사회기반 안전(금융)의 체계 변화에 지대한 영향을 줄 것으로 예상하는 자율주행차, 스마트 빌딩, 블록체인 기술에 대한 깊이 있는 이해와 안전에 미치는 영향에 대한 연구가 필요한 시점이다.

자율주행차 기술은 주변을 인식하는 환경 인식 기술에서부터 정확한 위치를 파악하는 측위 기술, 주변 자동차나 인프라와 통신하는 V2X 기술 등으로 지능정보기술의 거의 모든 영역에 해당한다. 하나의 부품 고장이나 인공지능의 잘못된 판단은 큰 사고로 이어질 수밖에 없다. 이에 자율주행차 기술이 안전에 미치는 영향에 대해 분석이 필요하다. 또한, 자율주행차의 사고 사례 분석을 통해 향후 교통 분야의 안전 확보를 위한 시사점 도출이 중요하다.

스마트 빌딩의 등장은 시설물 안전에도 영향을 주고 있다. 각종 센서와 빅데이터 기술은 빌딩 내 각종 데이터를 수집할 수 있게 되었고 이를 분석하여 적절한 의사결정을 내릴 수 있게 되었다. 또한, 네트워크 기술의 발달은 빌딩 내 모든 사물 간 통신이 자유롭게 이루어지고 필요한 액션(action)이 네트워크를 통해 전달된다. 이에, 센서의 오동작이나 네트워크의 단절 혹은 해킹은 빌딩 안전에 영향을 줄 수 있다. 안전과 보안 측면에서 스마트 빌딩 기술의 검토가 요구된다.

블록체인 기술은 금융 분야의 사회기반 안전에 대한 체계의 재설계를 요구하고 있다. 기존 은행 등 금융 분야의 사회기반 안전은 중앙집권적인 형태의 안전관리체계에 최적화되어 있다. 블록체인 기술은 이러한 중앙집권적인 체계를 완전히 부정하는 분산된 개념을 선보였다. 특히, 최근 블록체인 기반 암호화폐의

높은 관심으로 이를 이용한 사기 등이 발생하여 큰 피해가 발생하고 있다. 따라서, 블록체인 기술을 금융 분야에서 안전하게 활용하기 위한 연구가 필요하다.

인공지능, IoT, 빅데이터, 블록체인 등 다양한 신기술이 사회의 혁신을 이끄는 지능정보사회를 미리 대비하기 위해서는 국민의 안전을 확보하는 새로운 안전관리체계 구축이 밀바탕 되어야 한다. 이러한 안전관리체계 구축을 위해서는 기반이 되는 기술에 대한 이해가 필요하며, 요소 기술과 안전과의 관계에 대한 연구가 필요하다. 각 분야의 사고사례를 조사하여 이를 바탕으로 시사점 도출이 중요한 시점이다.

2. 연구의 목적

지능정보사회의 도래로 기존 안전관리체계를 개선해야 하는 상황에 직면해 있다. 즉, 기존의 안전관리체계는 새로운 지능정보기술로 인한 사회 변화를 적극적으로 반영하지 못하고 있다는 지적을 받는 실정이다. 법·제도적인 측면과 행정관리 측면에서의 기존 안전관리체계의 개선 방안을 협동으로 연구하기에 앞서 이러한 변화를 가져온 새로운 기술에 대한 깊이 있는 이해가 절실하다. 또한, 이러한 기술과 안전과의 관계를 분석한 연구가 선행되어야 한다.

본 연구에서는 지능정보사회의 변화 요구에 따라 국민의 안전을 확보하고 강화하는데 파급효과가 클 것으로 예상하는 교통안전, 시설물 안전, 사회기반 안전(금융) 분야를 대상으로 새롭게 등장한 신기술에 대한 시장 및 정책 동향, 요소 기술에 대한 이해와 안전과의 관계를 제시하고자 한다.

제2절 교통 안전 : 자율주행차

자동차 산업은 향후 10~20년의 자율주행차 기술 혁신이 지난 100여 년간 이뤄진 일반 자동차의 기술 변화보다 더 큰 상황에 직면해있으며, 자율주행차는 자율주행 시스템 기술의 발전으로 전 세계적인 큰 이슈로 급부상하고 있다.

미국의 구글 자동차는 2016년 총 50여대의 자율주행차가 도로를 활보하고 있으며, 국내의 경우에도 2017년 국토부로부터 임시자율주행 허가를 취득하여 총 20대의 자율주행차를 보유중이다. 국내외의 주요 자동차 제조업체들은 2017

년 미국 자동차공학회(SAE) 기준 자율주행 레벨 3~4단계의 자율주행자동차를 출시하고 있으며, 업체 대부분은 2020년 자율주행차 상용화 계획 및 2030년에 자율주행 레벨 5단계의 기술개발을 목표로 하고 있다. 자율주행 시스템 기술의 발전은 향후 교통 정체의 완화 및 환경부하의 경감 등 수많은 기대효과를 창출 할 것이라 예상된다.

그러나 2016년 2월 구글의 자율주행차 사고 및 2016년 5월 테슬라 모델S 사망 사고 등 자율주행차 사고 사례가 많이 발생하면서 중요한 과제로 ‘안전’ 이 새로 떠올랐다. 현재 많은 자동차 제조업체들이 자율주행차의 연구개발에 박차를 가함에도 불구하고 시판에 대해서는 조심스러운 입장을 취하고 있는데, 그 이유는 자율주행차 사고는 곧 운전자 및 상대방의 안전과 직결되기 때문이다. 이와 같이 안전에 관한 중요성이 제고되는 만큼 사고의 원인이 되는 요인을 다각도로 검토하고 사고의 예방 및 대처 방안 마련이 필요한 상황이다.

1. 시장 및 정책 동향

가. 해외 시장 동향

주요 글로벌 조사기관인 IHS Automotive는 대략 2025년부터 ‘완전 자율주행차’의 보급 및 시장 규모가 대폭 증가하여 60만대 수준에 도달 할 것이며, 이후 2035년에는 2,100만대 수준으로 늘어날 것으로 예상³⁾하고 있다. 구체적인 전망은 기관별로 조금씩 차이를 보이지만 2020년에서 2025년 사이에 NHTSA 3단계의 차량이 보급될 것으로 전망한다. 보스턴 컨설팅 그룹에 의하면, 자율주행차 시장 규모는 2025년에는 420억 달러까지 증가하며 2035년에는 770억 달러로 10여 년간 대폭 상승할 것으로 예상하며 2035년의 자율주행차의 생산 규모는 전체의 25% 규모로 총 3,000만대 중 완전 자동주행 자율주행차는 1,200만대, 부분 자율주행차는 1,800만대에 이를 것으로 전망⁴⁾하고 있다.

해외 ICT업체 중 하나인 구글은 자동차 업계와의 제휴를 확대하고 있고, 구글의 모기업 알파벳은 ‘Waymo’라는 타이틀을 내걸고 자율주행차 프로젝트를 위해 따로 자회사를 독립시킴으로써 상용화에 한걸음 다가갔다. 미국의 실리콘

3) IHS Markit, IHS Clarifies Autonomous Vehicle Sales Forecast, 2016.06.

4) Navigant Research(2013), 한국정보화진흥원, 자율주행 자동차산업의 빛장을 열다(2017) (재인용)

벨리를 기반으로 한, 주요 자동차 제조업체 중 하나인 Tesla는 2015년 Model S/IX에 Auto Pilot(Autosteer, Autopark 등의 기능)을 탑재하였다. GM(General Motors Corporation)은 2016년 1월, 차량 공유 회사인 리프트(Lyft)와 자율주행 택시 사업을 협력하기로 했으며 Ford는 2016년, 2021년부터는 완전 자율주행차 단계의 자동차 생산 및 본격적인 시험에 돌입할 예정이다.

위와 같이 글로벌 주요 자동차 제조업체 및 IT업체는 현재 자율주행차 시장의 경쟁력 확보를 위해 기술 개발 및 기업의 인수 합병 등 적극적인 투자를 하고 있는 상황이다. 또한 효율적인 자율주행차 개발을 목표로 IT, 통신, 자동차 부품 등의 다른 산업군의 선도 업체들과 협력중이다. 자율주행 기술은 크게 고정밀 지도, 센서 및 인공지능(AI) 등으로 구분하며, 주로 완성차 업체가 핵심 기술의 확보를 위해 ICT업체와 협력 발전 방향을 모색 중이다.

나. 국내 시장 동향

국내 자동차 내수시장의 수입차 시장 규모가 확대되고 있는 추세이며, 주요 자동차 제조업체의 친환경 자동차의 상용화를 위한 노력으로 전기 자동차 및 하이브리드 자동차의 보급이 증가하고 있다. 또한 노년층의 승용차 이용량이 증가함에 따라 향후에는 안전할 뿐만 아니라 운행조작이 쉽고 간편한 자동차의 수요가 늘어날 것으로 전망된다. 국내 자동차 판매량의 경우, 수출 비중이 높고 자동차 보급은 포화되고 있는 추세이다.

국내 기업의 경우, 2010년부터 현대·기아자동차를 중심으로 연구가 진행되고 있다. 현재는 SAE기준에서 자율주행 레벨 3~4단계까지 개발되었으며, 국내 자동차 부품업체중 현대모비스는 2016년 처음으로 국내 자율주행차 임시운행 허가를 취득했다. 2019년에 양산을 준비 중이며, 2020년과 2022년에는 각각 레벨3 이상의 자율주행기술의 개발 및 상용화를 목표로 하고 있다. 이에 뒤이어 LG이노텍, 세코닉스, 엠씨넥스 등 전자 부품 업체들도 핵심 센서 기술을 개발하고 있다. 2017년에는 국내 ICT업체에서 네이버가 처음으로 자율주행차 임시운행 허가를 받음과 동시에 자체개발 중인 자율주행 차량을 최초로 공개했다. 이처럼 완성차 기업뿐만 아니라 대학교 및 IT연구소, 부품 업체 등에서도 연구 개발이 활발하게 진행 중이다.

다. 해외 정책 동향

전 세계적으로 자율주행차가 급부상하고 있으며, 그에 따른 정책 및 인프라, 규제 등이 이목을 끌고 있다. 현 정책은 인간의 운전을 전제로 다루고 있기 때문에, 법적인 주체가 아닌 인공지능 및 소프트웨어 시스템 등 컴퓨터로 발생한 사고의 책임 해결을 위해서 많은 논의와 분석이 필요하다. 또한 자율주행차의 상용화를 위해서는 기업의 연구·개발도 중요하지만 정부의 적극적인 개입을 통한 임시 운행제도 마련하고, 법적 규제 근거를 정비하여 국제 표준에 맞는 평가 절차를 구축해야 한다. 또한 교통사고 발생 시 책임 및 보험 등의 문제에 있어서도 정부의 역할이 매우 중요하다.

미국은 자율주행차 관련하여 선도적인 대응을 하고 있다. 자율주행차 및 교통시스템 개발을 위해 교통부(DOT), 국방부(DOD), 과학재단(NSF)등을 통해 연방 정부 및 주정부 지원을 하고 있다. 또한 자율주행차의 취약 분야인 사이버 보안에 관한 대응책으로 조직을 개편하였으며, 업계와 정보 공유 및 분석을 위해 ISAC(Information Sharing and Analysis Center) 활동 지원을 추진함으로써 사이버 보안을 공동으로 해결하기 위한 대응체계를 강화하였다.

유럽의 정책 동향을 살펴보면 ‘도쿄의정서’를 토대로 친환경적인 CO2 배출감소를 위해 자율주행차 기술 개발에 착수하였고 EU 주도 및 유럽 국가 개별의 연구로 구분되어 진행 중이다. EU 집행위원회(European Commission, EC) 주도의 연구는 정보통신총국(DG-CONNECT)⁵⁾ 및 연구혁신총국(DG-RTD)⁶⁾에 의해 자율주행차 기술개발을 위한 대형 프로젝트가 진행 중이며 자율주행차 관련 R&D를 다양하게 지원하고 있다.

라. 국내 정책 동향

기술 선진국인 미국, 유럽에 비해 국내의 자율주행차의 기술 수준은 평균 약 4.6년의 격차를 보이며 위치추적 기능, 경로 계획(Path Planning) 능력, 주변 환

5) EC 산하 정보통신총국 (Directorate-general for Communications Networks, Content and Technology), ICT분야 정책 수행은 커뮤니케이션 네트워크 콘텐츠·기술 총국이 담당

6) 연구혁신총국 (Directorate-General for Research and Innovation), 총국의 R&D관련 정책을 총괄 관리

경 인지능력, 자동차 제어기술 등 총 4가지 핵심 기술 중 주변 환경 인지능력을 제외한 나머지 3가지 기술은 세계 선진국과 비슷한 수준에 도달했다고 평가받고 있다. 그러나 자율주행차의 완성을 위해서는 다양한 산업의 융·복합을 통한 개발이 필요하나 국내 R&D는 자동차와 도로, ICT 기술 등을 부처별로 독립적으로 추진 중인 실정이다. 산업통상자원부는 자동차선변경시스템 등 자율주행 기술개발은 진행 중이나 부품산업 기반조성의 부족 및 제도적, 정책적 문제 등으로 상용화 계획에 차질이 생기고 있다. 또한 현행 자동차관리법에서는 자율주행차의 일반도로 운행이 금지였으나, 산업 발전을 목표로 2014년 미래부(현 과기정통부)와 국토부 등은 자율주행차 운행을 위한 규제를 개선하였다. 현재 국내는 첨단 운전자보조시스템(Advanced Driver Assistance System, ADAS)안전기준을 적용하고 있다.

2017년 11월에는 관계부처 합동으로 ‘혁신성장을 위한 사람 중심의 4차 산업혁명 대응계획’을 통해 자율주행차의 글로벌 경쟁 심화에 대응하기 위해 2020년 고속도로 준자율주행차 상용화(레벨3: 고속도로 등 자율주행, 돌발상황 시 운전자 개입)로 교통문제를 해결하고, 고령자·장애인 등 교통약자 배려 및 자동차 신시장을 선도하기 위한 정책을 수립하였다. 2017년부터 2022년까지 고해상도 카메라, 레이더, 라이다 등 9대 핵심부품, 자율주행 SW, 통신 및 보안 등 자율주행차 핵심기술을 개발하고 2018년을 목표로 세계 최고 수준의 테스트베드 ‘K-City’⁷⁾ 조기 구축과 자율주행을 지원한다. 또한 2020년까지 검사 리콜 및 사고 시 책임배분 보험 제도를 마련하고 ‘운전자’를 전제하고 있는 도로 교통 법령 정비 추진을 계획하고 있다.

2. 요소 기술

자율자동차와 관련된 요소 기술은 3가지로 구분할 수 있다. 첫 번째는 첨단 운전자지원시스템(ADAS), 카메라, 레이더, 라이다와 같은 환경인식기술이고 두 번째는 주변 환경 인식의 개선을 위한 GPS와 같은 측위기술이다. 세 번째는 차량 주행 중 다른 차량 및 도로 등과 네트워크를 통한 상호 통신으로 정보를 공유하는 V2X(Vehicle to Everythings) 기술이다.

7) 경기 화성에 32만㎡ 규모로 고속도로, 도심, 교외 등 5개 실제 환경을 재현한 ‘실험도시’

가. 환경인식 기술

자동차용 센서는 차량 주행 관련 주변 교통 정보를 빠르게 수집하며, 이를 해석하고 의사결정을 신속히 실행하기 위한 자율주행차의 핵심 기술로 자리 잡고 있다. 또한 주행 중 주변 환경에 대한 정확한 인지가 불가능하다면 자율주행 시스템 자체가 불가능하다고 말할 수 있을 만큼 중요하며 과거에 단순히 차량의 주행상황 등을 측정하기 위한 목적과는 다르게 최근에는 차량 및 신호등 등 주행 중 외부 환경에 대한 데이터를 수집/분석하는 역할을 한다.

최근에는 완성차 제조업체 및 부품업체뿐만 아니라 IT업체도 첨단운전지원시스템(Advanced Driver Assistance System, ADAS)개발에 주력하고 있으며 해외 자율주행차의 선도국들은 교통으로 인한 사고를 줄이기 위해 안전 규제를 강화하는 등의 노력을 하고 있다. 또한 그에 따른 외부 환경을 인지해야하는 자율주행 센서 시스템은 현재 핵심 사업으로 급부상하고 있다.

ADAS라 함은 차량 내·외부의 탑재된 각종 센서들이 안전과 위험회피를 목적으로 운전자를 지원하는 첨단보조 시스템이다. 초기에는 차량에 잠재 위험 발생 시, 단순한 경고로 운전자의 전방 주시를 유도하는 기술적이고 수동적인 경고에 불과했으나, 최근에는 능동적인 간섭 기술로 발전하고 있다. 이 기술은 자율주행을 위한 필수적 과정으로 최근에는 ADAS 센서와의 융합이 활발해졌으며, 향후에는 정교한 기능의 구현을 예상하고 있다. ADAS용 센서는 크게 카메라(camera), 레이더(radar), 레이저(laser), 초음파 센서(ultrasonic)로 나뉠 수 있다.

카메라는 레이저와 라이다보다 정밀도가 떨어지며 날씨와 시간의 영향을 받는 반면 형태의 인식은 가능하다는 점에서 주목받고 있다. 물체 식별이 관건인 자율주행에서 카메라는 중요한 역할을 한다.

레이더는 물체 방향으로 전자기파(radio waves)를 발사 후 반사되는 신호를 분석하여 거리, 높이, 속도 등의 주변정보를 얻는다. 자동긴급제동, 전·후방 충돌경보 등 ADAS에 사용되는 자율주행 기초의 센서로 날씨와 시간의 영향을 덜 받는다는 장점이 있다.

레이저는 에너지 파동의 변화를 해석해 주변 사물을 인식하는 장치로서 긴 상용화 역사를 가지고 있으며 가격이 저렴하다. 또한 적외선 이용 시 야간에도

물체의 식별이 가능하다. 그러나 레이더(Radar)에 비해 인식거리가 짧으며 (20~50m) 날씨의 영향이 크며 형태 인식이 어렵다는 단점이 있다.

초음파(Ultrasonic Sensor)는 간단함과 동시에 저렴하다는 장점을 갖춘 센서로써 가청 주파수 영역 밖인(20KHz 이상)음파를 발사한 뒤 반사되어 돌아오는 신호를 감지 및 시간을 측정하여 거리를 계산한다. 음파는 빛에 비해 느려 상대속도 측정 과정에 문제가 있고, 측정 거리(3~4m)가 짧은 이유로 주로 정차 시 혹은 저속 주행 시에 활용된다.

나. 측위기술

자율주행차와 첨단 운전자 보조 시스템(ADAS)에 있어서 정밀한 자동차 위치를 추정하는 고정밀 측위 기술은 핵심 기술 중 하나이다. 자차의 위치 추정이 가능하면 이를 통한 주변 환경 인식의 개선 및 주변 지형을 고려한 최적의 제어로 안전성 향상 및 연비 절감 효과를 볼 수 있으나, 고정밀 측위 기술의 상용화 측면에서 고가의 장비와 센서를 활용하고 있어 충분한 연구가 필요하다. 측위 기술 중 현재는 GNSS(Global Navigation Satellite System)기반 GPS(Global Positioning System), GLONASS(Global Navigation Satellite System) 등의 위성 항법 시스템을 활용하는 전파항법(Radio Navigation)방식이 두루 사용되고 있다. GNSS(Global Navigation Satellite System)는 다수의 위성을 이용해 각 국(미국의 GPS, 러시아의 GLONASS, 유럽의 GALILEO, 일본의 GZSS 등)의 위성측위 시스템들을 통칭한 항법 시스템으로 3차원 위치·시각 정보를 전 지구적으로 제공하는 시스템을 의미하며 현재는 GPS, GLONASS가 가장 활발하게 서비스를 제공하고 있다. 이러한 위성항법(Satellite navigation) 측위 시스템은 전 세계적으로 활용 범위가 넓어지고 있으며 다양한 분야(민간, 항공기, 선박, 군 관련 등)에 사용되고 있다.

다. V2X

도로 위의 자동차는 항상 위험이 존재하고 있으며, 세계보건기구(WHO)는 도로 인프라 시설이 개선되고 있음에도 불구하고 매년 전 세계에서 교통사고로 인한 125만 명의 인명 손실이 발생한다고 발표했다. 자동차는 인명과 직접적으로 결부되어 있으므로 자율주행차의 개발에 있어서 교통 사고율 감소를 위한 대책

이 시급하다. 이러한 부분들을 고려하기 위해 다양한 시도를 한 결과 ESP(Electronic Stability Program, 전자식 자세자세제어장치)와 ABS(Anti-lock Brake System, 잠김 방지 브레이크 시스템) 등과 같이 전자장비들을 유기적으로 통제하는 최상위의 안전 시스템들이 산출물이라고 볼 수 있다. 또한 최근 국내에서 이슈가 된 양재 IC부근과 봉평 터널에서의 버스 사고원인은 운전자의 졸음 운전으로 규명된 바 있는데, 이에 대한 대책으로 주목받고 있는 졸음운전 방지나 전방 주시 태만을 줄이기 위한 HUD 네비게이션 도입 등 사용자 인터페이스 측면의 방안이 등장하고 있다.

그러나 위와 같은 방안은 특정 서비스를 도입한 차량과 운전자만을 대상으로만 적용되는 것으로, 실제 상황을 실시간으로 완벽하게 고려하여 정보를 제공하는 것은 불가능하다. 즉, 아무리 차량 자체 내 센서가 훌륭하다 하더라도 자율주행 기술을 100% 도입하기에는 한계가 있다. 이러한 이유로 양방향으로 상호 통신을 하며 교통정보를 공유 할 수 있는 V2X(Vehicle to Everything)가 부각되고 있다.

3. 안전 관리 현안 및 시사점

지금까지 자동차의 기술 개발은 물리적인 혁신을 거듭함과 동시에 기술 범주가 가상적인 부분까지 확대되면서 자동차 시장은 유례없이 빠르게 변하고 있다. 자동차 주요업체들은 자율주행차 시장에서의 경쟁력 확보를 위해 각자의 핵심 기술을 바탕으로 협력 체계를 구축하고 있으며 정부 차원에서의 정책적, 경제적 지원 및 투자도 활발히 이루어지고 있다. 그러나 자율주행차 시장에서의 치열한 경쟁 속에서 근본적인 이슈에 대해 검토가 필요하다. 최근 주요 자동차 업체인 구글 및 테슬라 자율주행차의 대표적인 사고 사례의 분석을 통해 기술 개발에 따른 한계와 그에 따른 법·정책적 현안 및 안전 관련 이슈를 면밀하게 검토 후 향후 연구 방향을 제시하는 과정이 필요한 시점이다.

가. 안전관리현안

1) 구글 사례 분석

구글 자율주행차의 사고는 2016년 미국 캘리포니아 주에서 렉서스(RX450h)를 개조해 만든 자율주행차와 버스 간 가벼운 접촉 사고였다. 구글 자율주행차

가 우회전을 위해 우측 연석 쪽으로 접근 후 모래주머니를 인지하였다. 인지 후 전방의 모래주머니를 회피하기 위해 왼쪽으로 차선을 변경하는 과정에서 옆 차선에서 주행 중인 버스와 사고가 발생했다. 사고의 원인은 버스가 감속할 것이라는 자율주행 차량의 판단과는 다르게 주행속도를 그대로 유지하여 충돌이 발생했다. 구글은 자율주행 차량의 도로 교통법을 엄정하게 지켜 도로의 흐름을 방해한다는 잣은 지적을 받기도 하였으며 버스가 양보하지 않을 수 있다는 점을 소프트웨어에 주입 및 수정이 필요하다고 인지하였다. 개선방안으로서 자율주행 기능 알고리즘을 사람의 운전습관을 모방하도록 변경하였다.

이번 사고를 통해 구글은 자율주행차 시험 운행이 지니고 있는 위험성을 인정하였으며 그와 동시에 위험 상황 및 안전성 확보를 위한 노력은 계속 진행 중이다. 자율주행 시험운행을 통해 인공지능(AI)기반 교통 흐름 및 예측 불가능한 상황 등에 운전 하는 방법을 학습중이며, 안전에 이상이 있을 경우 수동 모드로 전환하여 위험을 방지하고 있다. 구글의 자율주행차 총책임자 크리스 엄슨 역시 현재의 자율주행 기술의 한계에 대해서 인정한 바 있으며, 향후 몇 년 내에 해결을 목표로 하고 있다. 구글 자율주행차 사고 사례에서도 확인할 수 있듯이 사람의 수신호 인지 및 사물의 유형구분(예, 돌 vs. 종이박스)은 아직 극복해야 할 대상이다.

2) 테슬라 사례 분석

구글의 사고 발생년도와 같은 해(2016), 미국 플로리다주 고속도로에서 테슬라의 모델 S는 자율주행 중 운전자 첫 사망 사고를 일으켰다. SW에 자동차 제어의 기능을 부분적으로 위임하는 자율주행모드인 ‘오토파일럿(Auto Pilot)’ 기능은 주변 환경의 인식 부족으로 대형트레일러와 해당 차량과의 충돌로 확인되었다. 테슬라 측은 사고 원인에 대해 충돌 사고 당시 차량의 자율주행 센서가 햇빛을 정면으로 받는 역광 상태에서 트레일러의 백색 옆면을 하늘로 착각한 채 인식하지 못했던 것이라고 밝혔다. 또한 오토파일럿(Auto Pilot)기능을 사용하면 자동으로 차선 유지 및 차로 변경이 가능하며 교통 혼잡 구간에서는 능동형 트래픽 크루즈 컨트롤을 이용한 속도 조절 등이 가능하기 때문에 차선을 올바르게 인식하는 것이 중요하다. 테슬라 측은 자율주행모드(Auto Pilot) 기능 사용구간에서는 운전자의 전방 주시 의무를 지켜야 한다고 강조했다.

향후 자율주행차의 조기 상용화를 위해 경제성, 소비자의 인식전환, 안전성 입증과 관련된 기술 및 법·정책제도의 개선이 필요하며 자율주행차 확산 속도는 앞서 말한 현안들의 개선 정도에 따라 좌우될 것이다.

나. 시사점

구글과 테슬라의 사고를 전후로 자율주행차 안전을 목표로 각국의 대응 및 제도 정비를 본격화하고 있다. 유럽 국가 중 네덜란드는 테슬라의 자율주행 기능을 차량 내 장착을 허가한 반면 독일 연방자동차위원회는 테슬라 자율주행(AutoPilot)기능이 불완전한 시험 버전(Beta-phase version)이라는 이유로 차량 내 적용을 허가하지 않고 개선의 필요성을 강조했다. 또한 한국, 일본 및 유럽은 유엔 전문가회의(2016.7.10)에서 차량 추월 및 차선 합류 등이 가능한 자율주행차 운행 공통기준 제정 논의를 하였으며, 2018년 중으로 운전자가 핸들 조작을 하지 않고 차선 변경 및 추월을 할 수 있는 차량 조건 등과 같은 기준을 만들어 국가별로 채택할 예정이라고 밝혔다.

현재까지 공식적으로 확인되거나 보고된 자동차 관련 해킹 침해 사고는 없지만, 각국의 많은 연구원들의 수많은 연구 및 실험에 걸쳐 차량 내 컴퓨터 시스템이 해킹 가능함을 증명하기도 했다. 자율주행차는 기존 차량에 비해 더 많은 전자·통신 기능을 내장하고 있으며 이에 따라 해킹하기 쉬운 보안 취약점 및 오작동의 위험이 증가하고 있다. 이에 대응하여 유럽, 미국 등 주요 자동차 선도국에서는 보안위협에 대한 대응책과 더불어 연구 개발에 박차를 가하고 있으며 자동차 업계 및 ICT업체 역시 이를 방지하기 위해 많은 노력을 기울이고 있다.

자율주행차의 상용화는 기관마다 다르나 대략 5~10년으로 예상하고 있다. 종합해보자면 현재 화두가 되고 있는 자율주행차 중에서도 크게 기술적, 보안적 두 가지 측면에서 안전에 영향을 미친다고 볼 수 있다. 앞서 언급한 구글의 사고에서는 기술적 측면에서 발생한 사고라 볼 수 있다. 현재까지 자율주행차가 없는 이유는 노선을 유지하거나, 장애물 피하기 등 어느 정도 기술적인 부분이 해결됐다고 볼 수 있으나 돌발적인 상황까지 고려하는 부분에 있어서는 기술적으로 보완되어야 한다. 최근 알파고(구글 내의 인공지능 기술 개발업체인 구글 딥마인드로부터 만들어진 시스템)라는 AI(Artificial Intelligence, 인공지능)와 같이 발생한 돌발 상황을 인지한 뒤에 향후에 벌어질 상황을 미리 예측해 최선의 선

택을 하는 의사 결정 체계가 필요하다. 이는 기술적 측면에서 향후의 방향을 제시한다.

또한 보안적 측면에서는 지금까지 발생한 자율주행차 해킹 사고는 아직 없으나 보안은 사람의 생명과 직결되며 향후 개발에 꼭 고려해야 할 사항중 하나이다. 현재는 네트워크로 모든 것이 연결되는 ‘초연결 사회’로서 이와 같은 기술의 발전은 자율주행차 또한 해킹의 위협에서 자유롭지 않으며 오동작 및 인명피해로까지 이어질 수 있음을 확인 할 수 있다. 이와 같이 다양한 특성을 가진 기기가 상호 연결되는 IoT 환경에서는 PC 중심의 기존 환경과는 달리 해커가 노릴만한 침투 경로와 공격 방법이 다양화 될 수 있을 뿐만 아니라 신속하게 공격을 인지하거나 대응하기 쉽지 않다. 다시 말해 기획 및 개발 단계에서부터 IoT 보안성 확보를 위한 노력이 필요하다. 또한 자율주행차에서 지원되는 보안 및 다수의 소프트웨어를 선제적으로 개발할 필요가 있으며 이는 새로운 시장을 확보 할 수 있는 좋은 계기가 될 것이다.

현재의 자율주행차 수준으로는 안심하고 탑승하는 것에 무리가 있다는 판단이 전반적이며 자율 주행에 대한 편익이 많은 반면 안전성의 미확보로 생명에 위협이 될 수 있는 우려의 시선도 있다. 향후의 ‘무사고’와 ‘안전’을 목표로 기술적, 보안적 측면의 개선 및 문제 해결에 대한 노력이 시급하다.

제3절 시설물 안전 : 스마트 빌딩

스마트 빌딩 혹은 인텔리전트 빌딩이란 용어는 1984년 미국 코네티컷주 하트포드의 시티 플레이스 건물의 특징을 설명하면서 처음 등장하였다. 이후 스마트 빌딩에 대한 관심이 증가함에 따라 다양한 개념 정의가 이루어졌다. 1990년 Powell의 정의⁸⁾에 따르면 스마트 빌딩은 건물의 실내 환경을 완전히 제어할 수 있으며, 냉방, 난방, 조명, 방재, 방범, 통신 및 승강기 등의 제어가 중앙 컴퓨터에 의하여 이루어지는 건물로 정의되었다. 또한 스마트 빌딩은 건축, 통신, 자동화 등의 기술을 유기적으로 통합하여 경제성, 효율성, 쾌적성, 기능성, 신뢰성, 안전성을 추구한다.

8) Powell, J.A., “Intelligent design teams design intelligent buildings”, Habitat International, Vol. 14 Nos 2/3, pp. 83-94. 1990.

이 절에서는 스마트 빌딩의 시장 및 정책 동향, 요소 기술에 대한 분석, 안전 관련 현안 및 시사점을 기술한다.

1. 시장 및 정책 동향

가. 시장 동향

최근 스마트 빌딩은 ICT를 기반으로 설비 시스템 기기 간의 연결성과 사용자와 시스템 간의 연결성이 강조되는 경향을 보인다⁹⁾. 스마트 빌딩의 이러한 연결성은 사용자의 재실 패턴에 따라 건물의 기기를 효율적으로 운전할 수 있게 한다. 스마트 빌딩은 건물 사용자의 건물 재실 패턴을 파악하고 기기를 운전함으로써 에너지 비용을 절감할 수 있다. 예를 들어 미국 맨해튼에 위치한 뉴욕 타임스 건물은 스마트 센서를 설치하여 이를 기반으로 조명 시스템을 운전함으로써 조명에너지의 70%를 절감하였다¹⁰⁾. 또한, 전기 단가의 변동에 따른 기기의 최적 제어로 에너지 비용을 절감하는 수요 대응 제어 기술도 스마트 빌딩의 능동적 그리드 연결성으로 인하여 가능하다. 이처럼 스마트 빌딩은 ICT를 기반으로 건물 내에서의 연결성에서 벗어나 스마트 시티의 주요 요소로 점차 그 기능이 확대되고 있다.

Memoori의 전망에 따르면, 스마트 빌딩의 서비스 시장 규모는 전 세계적으로 2015년 130억 달러에서 2020년 320억 달러로 연간 22%의 성장을 할 것으로 예측되었다.¹¹⁾ 스마트 빌딩에서 IoT 기기는 IoT 설치에 따른 보조금 지급, 이미 설치된 건물자동화시스템과의 연계 등으로 건물의 에너지 소비를 절감할 수 있어서 IoT 관련 기기 및 서비스가 시장을 선도할 것을 예측된다. Gartner에 따르면 대형 건물은 IoT의 설치로 인하여 건물의 에너지 효율 및 건물 관리 비용을 약 30% 절감할 수 있는 것으로 나타났으며, 전 세계적으로 상업용 건물에 설치된 IoT의 기기의 숫자는 2017년 730만 개에서 2018년에는 1,070만 개에 달할 것으로 예상하였다.¹²⁾

9) Building Efficiency Initiative, What is a smart building?, 2011

10) Braendrecht, A., The future is now: five smart building features transforming today's workplace, Forbes, 2017.

11) Memoori, Big data for smart buildings 2015 to 2020, 2015.

12) Gartner, Gartner says smart cities will use 1.6 billion connected things in 2016, Gartner, 2015.12.

IBM은 IBM Cognitive Building solution을 개발하여 Building Information Model (BIM)을 이용하여 건물의 운영 데이터 정보를 가시화하고, 건물의 사용 패턴을 학습하며, 일기예보 정보와 연동하여 Watson IoT 플랫폼을 통하여 최적의 건물 제어가 이루어지는 서비스를 제공하고 있다. IBM의 솔루션은 최적화와 자동화를 통하여 건물을 효율적으로 관리하고, 공간 운영과 실의 관리를 효과적이고 쾌적하고자 하고 있다. 국내에서는 삼성전자에서 스마트 빌딩 통합 관리 솔루션인 b.IoT를 개발하였으며, 공조설비, 조명, 전력 및 펠드 디바이스, CCTV, 온습도 센서, 웨어러블 기기 및 신재생 시스템을 IoT 및 스마트 컨트롤러로 연동하여 빌딩 내 효율성 및 운영 최적화를 절감시켜주는 솔루션을 제공하고 있다.

나. 정책 동향

우리나라는 국가 차원에서 스마트 빌딩의 구현을 위하여 ICT 및 IoT와 연계된 건물에너지관리시스템의 개발을 지원함으로써 정부 주도로 스마트 빌딩의 구현을 적극적으로 지원하고 있다.

국토교통부는 장기 주택종합계획에서 에너지 절약적이고 환경 친화적인 주거 환경의 조성을 위하여 ICT를 활용한 스마트홈 보급 확대 정책을 공표하여 미래형 주택공급을 유도하고 있으며, 구체적으로 이동통신, 원격제어 보안 등 관련 첨단 기술을 융합한 스마트홈 보급을 위한 지원을 확대하고 있다. 이를 위하여 미래형 스마트홈 기술개발사업에 대한 연구를 2017년 착수하였으며, 해당 연구과제를 통해 ICT 융합 공동주택의 관리 및 운영과 재해 및 재난 대응형 스마트 안전 주택 기술을 개발하고 있다.

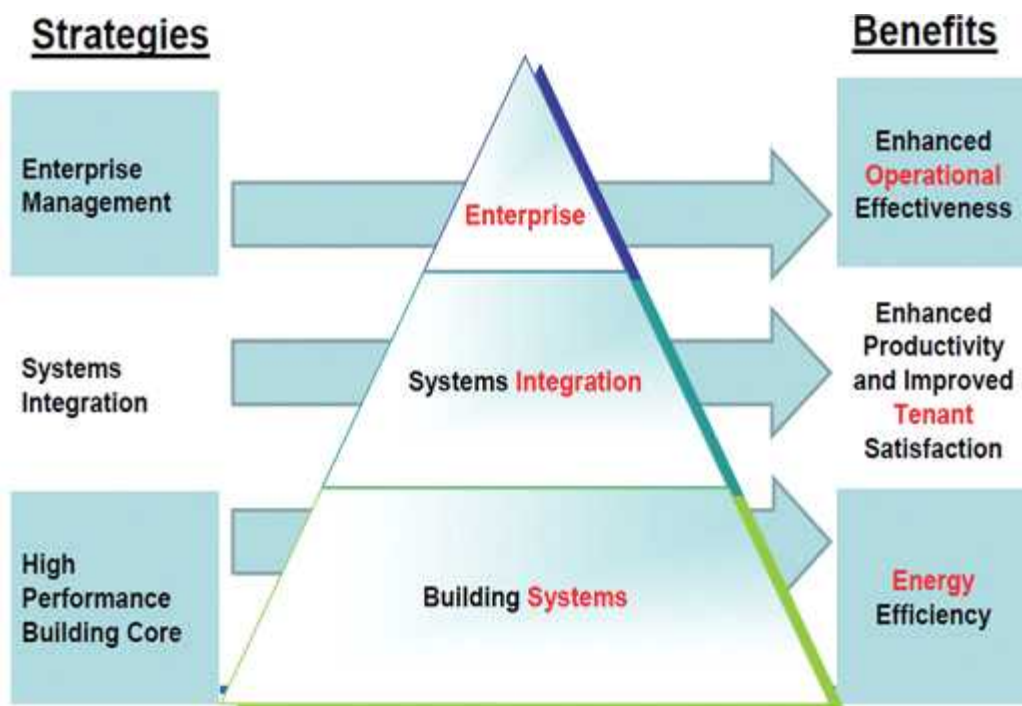
2015년 6월, 미래창조과학부 (현 과학기술정보통신부)에서는 ICT와 타 산업과의 융합을 촉진하기 위한 K-ICT 사물인터넷 융합 실증 사업을 착수하여 개방형 스마트 홈 기술개발 및 실증을 진행하고 있다. 다양한 스마트 홈 제품 및 서비스가 호환되는 개방형 API 개발 및 테스트 하우스의 구축을 통하여 기술개발 및 검증을 진행하고 있다.

산업통상자원부에서는 미래산업 선도 기술 개발사업의 목적으로 K-MEG 과제를 지원하여 스마트 그린 빌딩의 에너지 생산과 사용을 효율적으로 운영하여 제로 에너지 건물을 구현할 수 있는 체계적 솔루션을 구축하여 실제 건물에 적

용할 수 있도록 하고 있다.

미국은 총무부(GSA: General Services Administration)를 중심으로 건물의 에너지 소비 감소, 건물 관리의 효율 향상과 건물 사용자의 만족도 향상을 목표로 스마트 빌딩 정책을 운용하고 있다. GSA의 스마트 빌딩 추진 정책은 특히 일반적인 전력망계의 기능에 지능적인 부가 기능이 포함된 스마트 미터링의 설치 및 운영을 강조하고 있다.

[그림 2-1] 미국 GSA의 Smart building 운영 정책



GSA 발표자료, "Integration of SMART BUILDINGS Technology in GSA PBS", 2010

출처 : 이태원, 개방형 에너지관리시스템(EMS) 운영체계, 설비저널 45(10), 2016.

미국의 에너지성(Department of Energy)에서는 스마트 빌딩의 건물에서 설비 기기들의 통신 모듈의 표준화, 호환성, 에너지 절감을 위한 디맨드(demand) 제어 기술의 개발 및 검증에 지원하고 있다. 이를 통하여 스마트 빌딩과 스마트 그리드를 연계하여 기존의 전력망을 개선하고, 건물의 에너지 소비의 절감을 도모하고 있다.

유럽은 EU의 EPBD (Energy Performance of Building Directive)를 중심으로

스마트 빌딩 정책을 추진하고 있다. 특히 스마트 빌딩의 활성화를 위한 재정적인 지원과 더불어 범유럽 연구 과제인 Horizon 2020 프로그램¹³⁾을 통하여 스마트 빌딩의 연구 및 기술 개발에 대한 지원도 적극적으로 하고 있다. 특히, 스마트 빌딩이 갖춰야 할 특징을 첫째, 스마트 그리드와 연계하여 건물의 에너지 공급과 에너지 소비가 유연화되고, 둘째, 건물이 신재생에너지 및 에너지 저장 장치 등을 이용하여 에너지 수급의 자율성을 확보하며, 마지막으로 건물 사용자의 건강 및 안전을 적극적으로 확보하는 것으로 정의하였다.¹⁴⁾ 특히, 유럽 연합의 건물 부분의 환경 정책 즉, 2050년까지 건물부분의 탄소배출을 90% 감축시키고, 신재생에너지 사용량을 2030년까지 30% 증가시키는 것을 달성하기 위하여 스마트 빌딩 정책을 적극적으로 추진하고 있다. 유럽 연합은 스마트 빌딩을 통해 5백만 가구에 PV를 설치하고, 오피스 건물의 에너지 소비를 23% 감소시킬 뿐만 아니라 최대 전력 부하를 55% 감소시키려고 계획하고 있다. 또한, 스마트 빌딩을 통하여 실내 환경을 향상해 근무 효율을 11% 증가시키고, 질병으로 인한 병가를 35% 감소시키는 등의 목표를 세우고 있다.

위에서 살펴본 바와 같이 우리나라를 포함한 선진국에서는 건물로부터 발생하는 온실가스 배출량을 감축시키고, 건물의 경제성을 향상하며, 건물 재실자의 건강을 향상할 수 있는 스마트 빌딩의 보급 확대를 위하여 정부 차원의 활성화 정책을 추진하고 있으며, 스마트 빌딩의 기술 개발을 위한 연구도 정부주도로 적극적으로 지원하고 있다.

2. 요소 기술

가. 스마트 빌딩의 통신 기술

건물 규모의 근거리 통신망(LAN: Local Area Network)에서 사용되는 통신 방법에는 IEEE 802.3 규정에 따른 Ethernet, ANSI 878.1 표준인 ARCnet, Echelon 회사가 처음 개발하여 ANSI/EIA 709.1로 발전된 LonTalk와 ISO 16484-5의 규격인 BACnet이 대표적이다. 이중 BACnet은 건축설비분야에 가장 널리 사용되고

13) Horizon 2020 프로그램은 2014년부터 2020년까지 7년 동안 약 786억 유로를 투자하는 유럽연합의 연구혁신 프로그램으로 유럽의 글로벌 경쟁력을 강화하고 지식기반 경제 활성화를 목적으로 한다.

14) Frances Bean et al., Opening the door to smart buildings, Building Performance Institute Europe, 2017.

있는 산업계의 표준이며, 개별 기기 레벨과 통합 제어 레벨의 호환성 및 통합이 유리하다. 또한, 최근에는 무선 통신을 기반으로 한 센서 및 건물 자동화 시스템의 개발 및 보급이 이루어지고 있다. 스마트 빌딩의 대표적인 통신방법은 BACnet과 Zigbee이다.

1) BACnet

BACnet의 특징 중의 하나는 인터넷과의 연결이 쉽다는 것이다. BACnet은 BACnet Virtual Link Layer (BVLL)를 이용하여 BACnet 기기와 Internet Protocol (IP) 기기의 통신을 IP 신호로 가능하게 한다. IANSI/ASHRAE 135-2001에 규정된 BACnet/IP 통신 기준에 따라 BACnet 신호를 주고받는 개별 기기들은 어디서라도 IP 네트워크에 연결할 수 있다. 즉, 이러한 기능으로 인하여 인터넷이 연결된 곳이라면 어디에서라도 시스템에 쉽게 접속할 수 있게 된다.

2) ZigBee

ZigBee 통신 기술은 조명, 냉난방 및 방재의 통합 관리가 무선으로 가능하며, 이를 통한 에너지 절감과 더불어 설비 기기들의 개보수 및 확장이 쉬운 장점이 있다. ZigBee 방식은 Schneider, Johnson Controls, Phillips 등과 같은 세계 유수의 업체에서 채택되었으며, 국내에서는 포스코 건설에서 국내 건설사에서는 최초로 아파트 세대 내에서 ZigBee 방식의 무선 네트워크 환경을 구축하여 무선 통합 제어를 하고 있다.

나. 스마트 빌딩의 신기술

스마트 빌딩의 주요 구성 요소와 기술은 건물 자동화 시스템, 냉난방공조시스템, 조명 시스템, 엘리베이터, 방재 시스템, 방범 시스템과 통신 시스템으로 구분할 수 있다. 건물자동화 시스템은 통신 규격으로 주로 BACnet을 사용하며, 최근에는 인터넷을 통한 원격 제어가 가능하다. 냉난방공조시스템은 효율적인 시스템의 운영을 위하여 야간환기, 엔탈피 제어¹⁵⁾, 외기보상제어, 냉난방 플랜트 대수 제어 등을 적용한다. 구성 요소로는 공기조화기, 보일러, 냉동기, 온도, 압

15) 엔탈피 제어는 건축물의 냉방에 적용되는 방법으로써, 실내 공기와 실외 공기의 엔탈피를 비교하여 실외 공기의 엔탈피가 낮은 경우에는 냉동기를 가동하지 않고 환기 시스템만을 운전하여 실외 공기를 실내로 공급하여 건축물을 냉방 하는 방법을 말한다.

력, 유량 센서 등이 있다. 냉난방공조시스템은 재실자의 인원을 자동으로 파악하여 공실 여부를 판단하고, 사용되지 않는 공간에 대해서는 건물관리자가 공조를 일시적으로 제한하는 기능이 가능해졌다. 조명시스템은 실의 사용 여부에 따른 조명의 제어 등이 인터넷 기반으로 가능하다. 스마트 빌딩의 방법 및 방재 시스템은 출입제어기, 감시용 CCTV, 침입 방지 기능을 갖추고 있으며, 이러한 기능이 원격으로 중앙에서 인터넷 기반으로 가능하다.

1) 빅데이터

스마트 빌딩의 최신 관심사 중의 하나는 바로 빅데이터 기술의 응용이다. 스마트 빌딩은 특히 건물의 운전 정보, 즉 실내외 온도, 습도, CO₂, 기기 운전 스케줄 및 가동시간 등에 대한 방대한 데이터가 발생하며, 최근에는 IT 기술의 발전으로 저장에 쉬워졌다. 특히, 무선 통신 네트워크 및 통신 속도의 발달과 오픈 소스 형태의 소프트웨어가 발전함에 따라 실시간으로 방대한 데이터의 수집, 저장 및 분석이 가능해졌다.

2) 인공지능

스마트 빌딩의 또 다른 관심사 중의 하나는 바로 인공지능 기술의 응용이다. 스마트 빌딩은 건물 운전과 관련된 다양한 형태의 대량 데이터에 대한 접근 및 저장을 할 수 있다. 특히, 무선 통신 네트워크 및 통신 속도의 발달과 오픈 소스 형태의 소프트웨어가 발전함에 따라 실시간으로 방대한 데이터의 수집, 저장 및 분석이 가능해졌다.

인공지능 기반의 빅데이터 응용 기술은 특히 스마트 빌딩의 건물에너지 및 설비 제어 분야에 적용되고 있다. 대표적인 인공지능의 응용 분야는 예측제어(Predictive control), 고장예지진단(Fault Detection and Diagnostics)이 있다. 예측제어는 미래의 스마트 빌딩의 에너지 소비 및 신재생에너지의 생산량을 예측하고 이를 반영하여 건물의 에너지 관리를 하는 것을 말한다. 인공신경망을 이용한 경우, 태양광발전의 신재생에너지 예측 및 건물 에너지 소비량을 정확도 90% 이상으로 예측이 가능한 것으로 알려져 있다.

3) IoT

최근 급속도로 발전하고 있는 IoT 기기는 특히 스마트 빌딩의 보급과 발달에 기여하고 있다. IoT 센서 및 기기들은 기기 간의 데이터 공유는 물론 다른 정보 시스템들로의 데이터 송수신이 가능하여 기존에 불가능했던 데이터 기반의 효율적인 건물자동화관리가 가능해졌다.

3. 안전 관련 현안 및 시사점

스마트 빌딩은 ICT 기술이 본격적으로 적용되기 시작하면서 비약적인 발전을 하게 된다. 스마트 빌딩의 핵심 요소인 건물자동제어 시스템에 ICT 기술이 적용됨에 따라 스마트 빌딩에서 생산되는 다양한 형태의 데이터를 실시간으로 모니터링하고, 이를 바탕으로 건물의 사용자 및 시스템의 특성이 반영된 데이터 기반의 예측 제어가 가능하게 되었다. 이에 따라서 스마트 빌딩은 일반 건물 대비 에너지 소비량이 약 20% 감소함과 동시에 건물 사용자에게 쾌적하고 건강한 환경을 제공하여 건물 재실자의 생산성도 증대시키는 것으로 알려져 있다.

스마트 빌딩의 전 세계 시장 규모는 2015년 130억 달러에서 2020년 320억 달러로 연간 22%씩 성장할 것으로 예측되는 등 미래 시장을 선도할 기술이다. 이에 따라 우리나라를 포함한 선진 각국에서는 스마트 빌딩의 보급 확대를 위한 정부 차원의 활성화 정책과 관련 기술 개발을 적극적으로 지원하고 있다. 또한, 세계 굴지의 IT기업인 IBM, Google 및 삼성전자 등은 인공지능 기반의 빅데이터 응용 기술을 건물자동화시스템에 적용하여 발빠르게 시장을 선점하고 있다.

스마트 빌딩은 안전한 사회의 구축과 관련된 기회와 위기를 동시에 지니고 있다. 예를 들어 스마트 빌딩의 IoT 기반 통신 시스템은 화재 탐지와 진압 설비와 공기조화설비 시스템의 유기적 연계가 가능하게 하여 화재를 조기에 감지하고 진화할 수 있다. 또한, 건물 사용자의 스마트 폰과의 통신을 통하여 화재 발생 시 위치 파악과 맞춤형 피난 안내도 가능하게 하는 등 스마트 빌딩은 더욱 안전한 환경을 제공한다.

반면, 스마트 빌딩에 광범위하게 사용되는 IoT 기기들은 건축물의 주요 제어 시스템과 연동이 되어 있어 IoT 기기에 대한 보안이 매우 중요하다. IoT 환경의 보안 위협은 기기 손실 및 물리적 파괴, 신호 교란, 정보 유출, 데이터의 변조, 기기의 오작동 유발 등 다양하다. 이에 따라 스마트 빌딩의 통신 네트워크의 보

안을 위한 경량화된 암호화 통신 및 보안 관리 서비스 기술이 안전을 지키기 위한 필수요소가 된다.

정부는 제4차 산업혁명의 신산업 플랫폼으로 스마트 시티를 선정하고 글로벌 건설 시장의 아젠다를 선점하고자 노력하고 있다. 우리나라는 도시화의 진행률이 이미 90% 이상이 진행되어 있어, 스마트 시티의 보급은 정체된 도시의 회복력을 향상하고 지속적인 도시 개발이 가능한 새로운 비즈니스 기회를 도출할 것으로 예상된다. 스마트 빌딩은 스마트 시티 생태계의 근간으로 시장에서 차지하는 중요성과 경제 효과가 더욱 증가할 것으로 전망된다.

앞으로 글로벌 스마트 빌딩 시장을 선점하기 위해서는 산업 주도권을 획득하기 위한 적극적인 정책지원이 필요하다. IoT 및 인공지능 기반의 새로운 건물자동화시스템의 기술 개발을 정부 차원의 연구 지원, 스마트 빌딩 IT 서비스 관련 기업에 대한 세제 지원 및 인센티브 제공도 중요하다. 또한, 스마트 빌딩의 사이버 위협에 따른 사회적 부작용이 최소화될 수 있도록 외부 해킹 공격에 대한 시스템의 파괴, 오작동, 개인 정보 유출 등에 대한 선제적 대응이 필요한 시점이다.

제4절 사회기반 안전(금융) : 블록체인

이 절에서는 미래 혁신 기술로 주목받고 있는 블록체인의 등장에 따른 금융분야의 변화를 중심으로 살펴보고자 한다. 블록체인 기술의 특징, 시장 및 정책동향, 요소 기술에 대한 분석, 안전 관련 현안 및 시사점을 도출한다.

1. 블록체인의 특징

가. 블록체인의 개념

블록체인이란 거래(transaction) 내용을 저장한 블록을 특정한 서버가 아닌 네트워크를 통해 분산 저장하고 일정 시간마다 암호화 후 체인 형태로 연결하여 저장하는 기술이다. 이를 통해 제3자의 신뢰 없이 이중 거래를 차단하여 확실하고 안전한 거래를 보장한다. 공인된 제3의 중개기관에 대한 의존성이 높은 분야에 블록체인을 적용하면 효율성이 높아지고, 중앙 서버가 아닌 분산 저장방식으

로 인한 보안성 및 투명성 제고 등의 장점으로 다양한 분야에서 주목받고 있다.

나. 블록체인의 특징

1) 블록체인의 종류

블록체인 종류는 크게 세 가지 형태로 분류할 수 있다. 이는 공개(public) 블록체인과 개인(private) 블록체인 그리고 컨소시엄(consortium 또는 hybrid) 블록체인이다. 각각의 특징은 아래 표 2-1로 정리하였다.

〈표 2-1〉 블록체인 종류 비교

구분	공개 블록체인 (public Blockchain)	개인 블록체인 (private Blockchain)	컨소시엄 블록체인 (consortium Blockchain)
거버넌스	한번 정해진 법칙을 바꾸기 매우 어려움	중앙기관의 의사결정에 따라 변경 가능	컨소시엄 참여자들의 합의에 따라 변경 가능
데이터 접근	누구나 접근 가능	허가받은 사용자만 접근가능	허가받은 사용자만 접근가능
거래증명	알고리즘으로 동작(PoW, PoS), 익명의 거래 증명자	중앙기관에 의하여 거래증명이 이루어짐	사전에 합의된 규칙에 따라 거래검증, 인증된 거래 증명자 존재
암호화폐	필요	불필요	불필요
장점	안정성, 신뢰성, 익명성, 투명성 보장	- 높은 효율성과 확장성 - 처리속도 빠름 - 기업별 특징에 특화 가능	- 높은 효율성과 확장성 - 처리속도 빠름 - 민감 정보를 처리하는 역할 부여 가능
단점	- 확장성이 낮음 - 거래 속도 느림	- 보안성이 낮음	- 개입이 필요할 수 있음 - 투명성과 보안성이 낮음
활용 예	비트코인, 이더리움	나스닥 Linq	R3 CEV, 하이퍼레저

2) 블록체인 발전 방향

블록체인 기술은 가장 먼저 비트코인과 같은 공개(public) 형태에서 확장성과 효율성을 보완한 개인(private) 블록체인으로 발전하였으며 향후 산업간 융합과 사회 기반구조로써 확산되어 활용될 것으로 보인다. 특히 블록체인의 발전기로 볼 수 있는 2014년부터 공개 블록체인의 단점을 개선한 개인 블록체인과 스마트 계약이 추가된 공개 블록체인(이더리움)이 등장하여 다양한 활용이 가능해졌다.

개인 블록체인은 모든 거래가 추적 가능한 개방성과 실시간, 대용량 처리가 어려운 공개 블록체인의 한계점을 개선하여 기업 내 플랫폼을 구축할 수 있게 한다. 이더리움 플랫폼에서는 튜링완전(turing-complete)¹⁶⁾한 프로그래밍 언어의 사용이 가능하다. 그러므로 개발자는 직접 계약 조건과 내용을 코딩하여 원칙적으로는 상상하는 모든 종류의 계약을 스마트 계약으로 표현할 수 있다는 의미와 같다. 즉, 스마트 계약은 일정한 조건을 만족하는 경우 거래가 자동으로 실행될 수 있도록 프로그래밍 된 자동화 계약을 의미한다.

〈표 2-2〉 블록체인 기술의 단계별 발전 방향

세대	Blockchain 1.0	Blockchain 2.0	Blockchain 3.0
단계	도입기	발전기	확산기
시기	2009-2013	2013-2016	2017-2022
설명	공개 블록체인 (누구나 열람)	- 개인(기업형) 블록체인 등장 - 스마트 계약	산업과의 융합
활용 예	비트코인	나스닥 장외 주식거래, 이더리움	SCM, 에너지, 물류 등

자료 : SPRi, 블록체인(Blockchain) 기술의 산업적·사회적 활용 전망 및 시사점, 2017.09.

다. 암호화폐로서의 블록체인

암호화폐(cryptocurrency)란 암호화를 통해 거래를 보호하고, 추가적인 단위의 생성을 제어하며 자산의 교환을 검증하도록 설계된 디지털 자산¹⁷⁾을 의미한다. 암호화폐를 활용하는 경우, 국가 간 간편한 지급이 가능하며 별도의 은행 계좌의 개설이나 신용카드를 발급하지 않아도 자금이체와 같은 거래가 가능하다. 또한 제3의 중개기관이 없으므로 기존의 금융 네트워크를 통한 자금의 거래보다 낮은 수수료로 거래가 가능하다. 그러나 암호화폐는 기존 화폐에 비해 가격 변동성이 매우 크다. 암호화폐 자체의 위조나 이중 사용은 기술적으로 어렵지만 암호화폐 거래소 해킹이나 개인지갑의 보안 관련 문제의 발생 가능성이 존재한다. 또한 거래가 익명으로 진행되고 은행 계좌가 불필요하며 보고의 의무가 존재하지 않으므로 탈세의 가능성이 높다.

16) 튜링 완전이란 어떤 프로그래밍 언어나 추상 기계가 튜링 기계와 동일한 계산 능력을 가진다는 의미로 계산적인 문제를 프로그래밍 언어나 추상 기계로 풀 수 있다는 의미

17) wikipedia, Cryptocurrency

2. 시장 및 정책 동향

가. 시장 동향

1) 해외 시장 동향

블록체인 기술은 미래 핵심 기술로써의 기대감이 점차 높아지고 있으며 향후 5년에서 10년 내 실제 적용 가능성이 높을 것으로 예측된다. 시장조사기관인 가트너의 블록체인 사업의 부가가치 분석에 의하면, 블록체인 기술은 2020년 연간 성장률 120%를 기록하고 시장 규모는 2030년에 3조 달러 규모(한화 3,400조)에 달할 것으로 예측된다. 세계경제포럼(WEF)은 2027년 기준 전 세계 GDP의 10%인 8조 달러가 블록체인 플랫폼에서 발생할 것으로 전망¹⁸⁾하였다. 또한 금융업계는 블록체인 기술로 인한 비용 절감 규모가 2022년 기준으로 약 200억 달러에 달할 것으로 기대¹⁹⁾하고 있다. 금융업계 참가자 중 80%는 분산원장 기술이 업계를 변화시킬 것이며 2020년 내 도입될 것으로 예측²⁰⁾하고 있다. 표 2-3은 블록체인을 활용하려는 금융 관련 해외 기업의 동향을 정리한 내용이다.

〈표 2-3〉 금융 관련 블록체인 관련 해외 기업 동향

구분	회사명	설명
미국	나스닥 OMX그룹	- 블록체인을 기반으로 장외주식 거래소를 만들어 기업 및 투자자들을 연결시킬 계획 - 2015년부터 전문투자자용 장외시장인 'Nasdaq private market'에 블록체인 기술을 시범적으로 적용하여 실제 거래 시간을 3일에서 10분으로 단축시킴
	Ripple	- 블록체인 기술을 기반으로 한 지급결제 및 송금서비스를 통해 거래시간을 단축하고 저렴한 수수료 비용으로 제공
영국	런던 증권거래소	- 블록체인을 도입하기 위한 관련 워킹그룹 조직
	Propy	- 2016년 9월에 온라인으로 글로벌 부동산을 구매할 수 있도록 이더리움을 기반으로 프로젝트를 진행 - 중국의 O2O(Online to Offline) 부동산 서비스 제공업체인 Leju Holdings Limited와 제휴

18) WEF, “Deep Shift - Technology Tipping Points and Societal Impact”, 2015.09.

19) IDC, “Is the Future of Financial Services orgs in Blockchain?”, 2017.03.

20) Bain & Company, “Blockchain in Financial Markets: How to Gain an Edge”, 2017.02.

구분	회사명	설명
		- 2017년 9월에는 ICO를 통해 1500만 달러(한화 약 170억 원)를 자금을 유치
일본	증권거래소 그룹	- 일본 노무라 종합연구소, IBM과 협력하여 블록체인 기술의 실증 테스트를 위한 연구를 진행
싱가포르	금융 감독청	- 블록체인 기술 관련 'Project Ubin'을 발표, 첫 번째 단계로 은행 간 블록체인 기술을 활용한 지불을 위한 개념증명 설계를 위한 것으로 2017년 초에 완료 - 2단계로 이더리움을 활용하여 주정부가 암호화폐를 발행하고 실제 거래를 수행하고 자산을 구매할 예정

자료 : 뉴스 기사 및 금융업의 블록체인 활용과 정책과제, 한국금융연구원(2017) 참고

2) 국내 시장 동향

국내에서도 은행 및 증권, 대출, 자산 관련 분야에서 블록체인 기술을 활용한 다양한 서비스를 출시하거나 출시에 대한 계획을 수립하고 있다. 금융 업계 뿐만 아니라 IT서비스 업계에서도 금융/증권/자산 관리 분야 등을 중심으로 블록체인의 상용화 및 연구 개발에 적극적으로 나서고 있음을 알 수 있다.

〈표 2-4〉 금융 관련 블록체인 관련 국내 기업 동향

구분	회사명	설명
은행권	KB금융그룹	- 2015년 9월 고객이 보유한 포인트를 암호화폐인 비트코인으로 전환할 수 있는 「포인트리-비트코인 전환 서비스」 제공 - 2016년 4월 핀테크 기업인 코인플러그와 협업하여 국내 최초로 비대면 실명확인정보를 블록체인에 기록하는 기술 도입
	하나금융 지주	- 2016년 11월에 글로벌 블록체인 컨소시엄인 R3에서 국내 지급 결제와 인증 관련 프로젝트를 진행하여 기술 검증 완료
	KEB하나은행	- 블록체인에 기반을 둔 글로벌 통합 결제 플랫폼을 2018년 5월 정도에 공개 예정
	신한은행	- 2017년 12월에 글로벌 결제 전문 기업 비자(VISA)의 해외 기업 송금 서비스인 VISA B2B 커넥트 시범사업에 국내 은행 최초로 참여
대출	페이게이트 (PayGate)	- 핀테크 오픈 बैं킹 플랫폼인 세이퍼트(Seyfert)를 통해 P2P 대출 제공 - 2016년 8월에 부동산 핀테크 기업인 씨피핀테크와 기술교류 업무제휴 양해각서(MOU)를 맺고 ²¹⁾ 협력 관계 구축
IT기업	LG CNS	- P2P 장외 주식거래 서비스인 'B-트레이딩(B-Trading)' 개발
	삼성 SDS	- 블록체인 업체인 블로코와 국내외 공동 사업추진 및 기술 개발 시너지를 위한 전략적 MOU 체결 - 삼성카드 블록체인 구축사업을 비롯해 송금, 인증, 지급결제 등 블록체인

구분	회사명	설명
		관련 다양한 서비스를 발굴하고 신사업을 적극 추진 계획
	카카오뱅크	- 글로벌 금융 그룹인 씨티(Citi)와 세계 최대 P2P송금업체인 트랜스퍼와이즈(TransferWise)와 업무협약 체결

자료 : 관련 기사 정리

나. 정책 동향

1) 해외 정책 동향

먼저 해외의 정책 동향을 살펴보면, 미국, 일본 등 주요국은 금융 분야의 컨소시움을 발족하여 나라별 실정에 맞도록 산업체와 정부의 협력을 통해 발전하고자 노력하고 있다. 또한 해외 송금이나 증권과 관련한 다양한 금융 서비스를 개발하고 있으며, 자산거래 분야에 스마트 계약 기능을 도입하려는 노력과 함께 유통·물류, 공공서비스 등 여러 가지 분야에 블록체인을 도입하고자 하는 시도를 수행하고 있다.

미국의 연방 및 주 정부는 블록체인 기술이 금융을 포함한 산업과 사회 서비스 등에 가져올 파급효과에 주목하고 기관 간 협력을 통해 해결하고자 노력하고 있다. 중화인민공화국의 중앙은행인 중국인민은행(Bank of People of Bank of China, PBoC)은 2017년 1월에 블록체인 기반의 가상화폐를 시험하였다. 또한 2017년 6월에는 블록체인 및 인공지능과 같은 신기술 개발을 적극적으로 추진할 계획으로 다섯 가지 목표를 제시²²⁾하는 5개년 개발 계획을 발표하였다.

일본의 경우에는 2016년 10월에 지역 금융 기관 및 인터넷 전용 은행을 포함한 42개 은행이 일본 은행 중앙 컨소시엄(“The Japan Bank Consortium to Central Provide Domestic and Cross-border Payment”)에 가입²³⁾하였다. 이 컨소시엄은 금융 서비스 그룹 SBI(Strategic Business Innovator)와 분산원장 신생기업인 Ripple의 합작 투자로 시작되었으며 컨소시엄 내 협력을 통해 자국 및 외환 서비스를 통합하여 24시간 실시간 송금 인프라를 구축하겠다는 계획을 발표하였다.

21) 아이뉴스,페이게이트, 부동산 P2P 대출 씨피핀테크와 MOU, 2016.08.

22) coindesk, China's Central Bank Vows to Push for Blockchain in Five-Year Plan, 2017.06.

23) “42 Banks Join Blockchain Consortium in Japan”, coindesk, 2016.11.

2) 국내 정책 동향

금융권에서는 2016년 11월에 감독기구인 금융위원회와 금융감독원의 주도로 은행연합회, 금융투자 협회, 핀테크 산업협회가 참여하는 ‘블록체인 협의회’가 출범하였다. 이를 통해 블록체인 플랫폼의 상호호환성을 고려하여 초기 연구 단계부터 은행 및 금융투자업권 컨소시엄 간 소통을 강화하고 정보 공유 및 제도 개선사항 등을 검토하고자 한다. 자문그룹으로는 금융연구원, 핀테크지원센터, 금융보안원, 신용정보원과 전문가 등이 구성되었다.

또한 정부와 지자체를 중심으로 자산에 대한 전자계약 및 디지털 공공 서비스 분야에 블록체인을 활용하고자 하는 시도가 이루어지고 있다. 행정자치부는 2017년 2월에 블록체인 기술을 전자정부에 도입하는 방안을 모색하기 위한 전자정부 정책토론회 개최하였다. 이 자리에서 전자투표, 전자계약, 부동산 등기, 전자 문서 관리 등 행정 서비스에 블록체인 도입 방안에 대해 논의되었다.

3. 요소 기술

블록체인의 요소 기술은 크게 암호기술(cryptography)과 P2P 네트워크(peer-to-peer network) 기술로 구성된다. 이러한 요소 기술의 이론은 이미 수십 년 전에 정립되어 통신 암호화, 데이터 무결성 확인, 파일 분산 공유 시스템 등 여러 분야에서 활용되고 있다. 블록체인 기술은 기존의 요소 기술의 특성을 극대화하여 ‘신뢰성(reliability)’과 ‘투명성(transparency)’이라는 특징을 확보하였다. 여기에서는 블록체인을 이해하는 데 필요한 요소 기술인 암호기술과 P2P 네트워크 기술에 대해 설명한다.

가. 암호기술

블록체인 기술을 기반으로 하는 가상화폐를 암호화폐라 부를 정도로 암호기술은 블록체인의 핵심 요소 기술이다. 암호기술로부터 블록체인의 신뢰성과 투명성이라는 특성이 확보되었다고 말하는 것이 과언은 아니다. 특히, 암호기술 중 암호학적 해시함수(cryptography hash function)는 데이터가 변조되었는지를 확인하는 역할을 하고, 전자서명(digital signature)은 데이터가 실제 주인(owner)에 의해 작성되거나 수정되었는지를 증명한다.

1) 암호학적 해시함수 (Cryptography Hash Function)

암호학적 해시함수를 설명하기에 앞서 ‘해시함수’에 대해 먼저 설명한다. 해시함수는 “임의의 길이의 입력값을 고정된(fixed) 길이의 결과값으로 매핑하는 함수”이다. 해시함수에 의해 계산된 결과값을 보통 ‘해시’ 혹은 ‘해시값’이라 부른다. 해시함수는 같은 입력에 대해 항상 같은 해시값을 만들어내기 때문에 해시값을 해당 입력의 ‘지문(fingerprint)’이라고도 말한다. 암호학에서는 긴 입력으로부터 짧고 일정한 길이의 값을 ‘소화(digest)하듯’ 출력하기 때문에 ‘메시지 다이제스트(message digest)’라고도 한다.

해시함수에서 서로 다른 입력값에 대해 동일한 해시값이 나올 경우 이를 ‘충돌’이라 부른다. 해시함수를 실제 사용하려면 충돌이 발생할 가능성이 매우 낮아야 한다. 물론 결과값(해시값)으로부터 입력값이 쉽게 유추되며 안되고 해시함수 알고리즘 자체가 쉽게 파악되어서도 안 된다. 일반적인 해시함수는 입력값의 범위가 한정된 경우 결과값으로부터 입력값을 비교적 쉽게 유추할 수 있으며 몇 개의 입력과 결과만 있으면 누구나 해시 알고리즘을 알아낼 수 있다. ‘암호학적 해시함수’는 일반적인 해시함수에 비해 충돌 가능성이 낮으며 결과값을 유추하거나 알고리즘을 쉽게 파악할 수 없는 조건을 최대한 만족하도록 만들어졌다.

암호학적 해시함수는 입력값이 조금만 바뀌어도 결과값이 완전히 달라지는 특성을 갖는다. 이러한 특성으로 인해 연결된 데이터 블록의 어떤 값이라도 변경되면 해당 데이터 블록 이후로 연결된 모든 블록의 해시 포인터가 전부 바뀌게 된다. 따라서 가장 마지막 데이터 블록의 해시값만 알고 있으면 데이터 변조를 쉽게 알 수 있게 된다.

2) 전자서명 (Digital Signature)

전자서명은 디지털 환경에서 누가 데이터를 작성하였고 다른 누군가에 의해 변조되지 않았음을 보장하는 데 주로 사용된다. 전자서명은 비대칭키 암호화²⁴⁾의 특징을 응용해 ‘서명(sign)’과 ‘확인(verify)’이라는 개념을 구현한 방법

24) 비대칭키 암호화는 암호화하는 키와 복호화하는 키가 서로 다르며, 암호화키와 복호화키를 포함한 키쌍을 생성

이다. 비대칭키 암호화를 위해서는 키쌍을 생성해야 한다. 전자서명에서는 생성된 키쌍에서 하나를 개인키(private key)라 하고 나머지 하나를 공개키(public key)라 부른다. 개념상으로는 키쌍 중 어느 키도 개인키나 공개키가 될 수 있지만, 실무에서는 서명 작업보다는 확인 작업이 빈번하기 때문에 확인 작업 성능을 높이기 위해 키쌍 생성 때부터 용도를 구분하여 사용한다.

전자서명에서 서명(sign)이란 개인키를 소유한 사람이 개인키로 데이터를 암호화하는 작업을 말한다. 해당 서명은 개인키를 소유한 사람만 할 수 있기 때문에 마치 서류에 실제 서명하는 것과 같다고 하여 서명 작업이라고 한다. 하지만 실제 서류는 서명을 받은 후에도 변조가 쉽기 때문에 공증 등의 추가 절차가 필요하다. 반면 전자서명은 개인키 유출만 없다면 다른 사람은 해당 개인키로 암호화할 수 없다. 따라서 전자서명된 데이터는 사실상 변조가 불가능하다.

전자서명에서 확인(verify)이란 공개키(서명 시 사용된 개인키의 짝)로 데이터를 복호화하는 작업을 말한다. 개인키를 소유한 사람이 알려준 공개키로 서명된 데이터가 복호화된다면 해당 데이터는 틀림없이 소유한 사람이 전자서명 했다고 볼 수 있다. 이는 마치 실제 서류의 서명 진위를 확인하는 것과 비슷하다 하여 확인 작업이라고 부른다.

나. P2P 네트워크 기술

Peer-to-peer(P2P) 네트워크는 분산된 환경에서 노드(node) 간 데이터를 효율적으로 공유하기 위한 기술이다. P2P 네트워크에서는 하나의 노드가 서버와 클라이언트 역할을 모두 수행한다. 즉, 노드는 필요한 데이터를 다른 노드로부터 받거나, 데이터를 소유한 노드는 이를 다른 노드에 전송한다. 참고로 서버-클라이언트 네트워크에서는 서버가 중앙에서 모든 데이터를 소유하고 있으며, 클라이언트는 필요한 데이터를 서버에 요청하여 받는다.

블록체인 기술에서 P2P 네트워크는 중요한 역할을 수행한다. 신뢰성과 투명성이라는 블록체인의 특성을 보장하기 위해서는 앞에서 설명한 암호기술과 더불어 P2P 네트워크 기술 역시 필요하다. 블록체인이 P2P 네트워크의 여러 노드에 분산 저장됨에 따라 변조는 더욱 어려워지고 투명성은 올라가게 된다. 특히, 공개 블록체인의 경우 P2P 네트워크의 안정적인 구성이 더욱 중요해지고 있다. 비

트코인과 같은 암호화폐 분야에서는 P2P 네트워크를 유지하기 위해 일정 보상(예, 코인 지급 등)이 이루어진다.

4. 안전 관련 현안 및 시사점

블록체인 기술의 등장은 지금까지의 금융에 대한 개념을 송두리째 변화시켰다. 기존 금융은 모든 거래가 중앙의 통제를 받는 방식이었다면, 블록체인 기술은 완전히 분산된 방식으로 금융의 개념을 바꾸고 있다. 블록체인 기반의 암호화폐는 누구의 간섭도 없이 거래를 진행할 수 있게 하고, 해외 송금 역시 비교적 저렴한 수수료로 단 몇 분 만에 가능케 한다. 기존 방식을 고수하던 금융 기관 역시 새로운 블록체인 기술을 도입하기 위해 온 힘을 다하고 있다.

블록체인의 수많은 장점에도 불구하고 금융 분야의 블록체인 활용에서 많은 혼란과 피해가 발생하고 있다. 이에 대표적인 사고 사례 등을 살펴보고 이를 바탕으로 법·제도 개선 및 거버넌스의 정비에 필요한 시사점을 도출하고자 한다.

가. 안전 관련 현안

블록체인 기술은 아직 발전 과정에 있는 기술이다. 이로 인해 금융 분야의 활용에서 여러 문제가 발생하고 있다. 최근 암호화폐의 가치 급상승으로 암호화폐 탈취를 목적으로 한 거래소 해킹 사고가 빈번히 발생하고 있다. 블록체인 기반의 새로운 투자방식인 ICO를 이용한 투자사기는 또 다른 선의의 피해자를 양산하고 있다. 익명성을 보장하는 블록체인의 특성과는 달리 암호화폐를 법정화폐로 교환할 때 의도치 않게 발생하는 개인정보 침해도 문제가 되고 있다. 또한, 불법 자금 거래 등 부정 거래 가능성도 높은 편이다. 마지막으로 블록체인을 이용한 스마트 계약 역시 여러 취약점으로 인해 큰 피해가 발생하기도 하였다.

1) 암호화폐 거래소 해킹 사례 분석

2009년 암호화폐의 등장 이후 암호화폐 거래소의 대량 도난 사고가 발생하여 막대한 피해가 발생하고 있다. 암호화폐 거래소의 해킹은 고객의 개인키가 유출되어 발생한다. 많은 거래소가 고객의 편의를 위해 거래에 필요한 개인키를 보관해 주는 ‘지갑(wallet)’ 서비스를 제공한다. 비트코인과 같은 암호화폐 자

체는 해킹이 거의 불가능하지만 거래소의 지갑에 보관된 개인키는 보안 정도에 따라 해커나 내부자에 의해 유출될 수 있다. 결국, 거래소의 암호화폐 도난 사고는 지갑에 보관 중인 고객의 개인키가 유출되어 소유자의 의사와는 상관없이 암호화폐가 누군가의 소유로 바뀔 경우가 대부분이다.

<표 2-5> 대표적인 암호화폐 도난 사고 요약

거래소	피해 규모 (암호화폐)	피해 규모 (당시시세, USD)	사고 발생 일시	비 고
Mt. Gox	850,000 BTC	474,000,000	2011년 후반부터 지속 발생	최대 규모의 비트코인 거래소 해킹 사례
BitStamp	18,866 BTC	5,000,000	2015. 1. 4.	Mt.Gox와 달리 보상 약속
BitFinex	119,756 BTC	72,000,000	2016. 8. 2.	Mt.Gox 이후 최대 피해 사례
Yapizon	3,831 BTC	5,000,000	2017. 4. 22.	국내 첫 피해 사례

출처 : 뉴스 기사 정리

PC나 스마트폰에 저장된 개인키가 악성 코드에 의해 유출되는 경우도 있지만, 대량 유출 사고는 암호화폐 거래소의 지갑에 저장된 고객의 개인키가 유출되어 발생한다. 즉, 암호화폐 거래소가 지갑에 저장된 고객의 개인키를 안전하게 보호하지 못해 해커의 공격이나 내부자의 소행으로 개인키가 유출되어 막대한 피해가 발생하게 된다.

2) ICO 투자 사기 사례 분석

ICO(Initial Coin Offering)는 블록체인 기술을 이용하여 기술력 있는 스타트업에 투자하는 방식이다. 그러나 최근 ICO가 피싱(phishing), 신용사기(scam), 다단계 사기(Ponzi scheme)에 이용됨에 따라 투자자에게 피해를 주고 있다. 2017년 9월 캐나다의 유명 무료 모바일 메신저 앱인 ‘Kik19’의 ICO에서도 정체불명의 제삼자가 소셜미디어에 Kik의 ICO 참여 URL이라며 가짜 웹주소를 유포한 사례도 있었다. 미국 증권감독위원회는 투자자들에게 ‘치고 빠지기(pump and dump)’ 전략을 구사하는 사기꾼들을 주의할 것을 당부한 바 있다. 영국 금융감독청도 ICO는 매우 위험하고 투기적인 투자이며 투자자 보호가 불가능하고, 합법적인 프로젝트들도 개발 정도가 매우 초기 단계이므로 경험 많은 투자자들

도 신중히 해야 한다고 경고하였다. ICO로 투자금을 받고 기업 활동을 제대로 하지 않아도 법적으로 처벌할 근거가 현재로서는 미흡하다. 아직은 암호화폐에 대한 법·제도가 제대로 준비되어 있지 못하기 때문에 투자자가 손실을 보거나 사기를 당해도 제도적으로 보호할 장치가 마땅히 없다. 더 나아가 암호화폐의 광풍과 함께 유사수신행위나 다단계 피해자가 늘고 있다.²⁵⁾

3) 개인정보 유출 및 부정 거래 사례 분석

암호화폐 거래소의 관리자의 미흡한 보안 의식으로 인해 대량의 개인정보 유출되거나 암호화폐를 활용한 부정 거래 사례가 발생하는 사례가 발생하고 있다. 2017년 6월, 국내 최대 가상화폐 거래소²⁶⁾인 빗썸(Bithumb)에서 직원(비상임이사)의 PC가 해킹되어 고객 정보가 유출되는 사고가 발생하였다. 방송통신위원회(이하 방통위) 조사 결과, 빗썸 거래소 운영회사인 비티씨코리아닷컴은 개인정보 파일을 암호화 하지 않은 상태로 개인 PC에 보유하고 있었고, 백신 소프트웨어의 업데이트도 하지 않은 것으로 드러났다. 이번 사건으로 인해 암호화폐 관련 사업자의 보안의식 제고와 함께 시스템 보안 조치 및 인증절차를 강화할 필요가 있음을 알 수 있다.

4) 스마트 계약 해킹 사례 분석

스마트 계약은 블록체인을 기반으로 금융거래나 부동산 계약 등 다양한 형태의 계약을 체결하고 자동으로 실행할 수 있는 기능을 제공한다. 스마트 계약은 이더리움 플랫폼의 특성인 튜링완전(turing-complete)한 프로그래밍 언어를 사용하여 직접 계약 조건과 내용을 코딩할 수 있다. 사실상 원하는 모든 종류의 계약을 구현할 수 있다는 장점을 가지나 오류가 발생할 가능성도 동시에 증가하였다고 볼 수 있다.

이러한 스마트 계약의 특성을 해킹 사례는 2016년 6월에 발생한 더 다오(The Dao) 프로젝트와 2017년 7월에 발생한 이더리움 플랫폼에서 동작하는 클라이언트인 패리티 지갑(Parity Wallet) 사건²⁷⁾이 있다. 이더리움의 스마트 계약

25) ‘가짜 비트코인 가상화폐 유사수신행위 56건 적발’, 아이뉴스24, 2017.10.18.

26) MBN 뉴스, 국내 1위 가상화폐 거래소 ‘빗썸’, 세계에서 1위, 2017.12.14.

27) <http://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/> 참고

기능으로 개발된 더 다오는 클라우드 세일로 판매한 다오 토큰을 이더로 환급하는 로직에 재귀 호출 버그(recursive calling vulnerability)가 포함되었다. 해커는 이 취약점을 이용하여 당시 가치로 약 500억 원에 해당하는 360만 이더(ETH)를 탈취하였다. 패리티는 다중서명(Multi-Sig)²⁸⁾ 지갑의 취약점으로 인해 3개의 ICO 프로젝트에서 153,037이더(약 3200만 달러 규모)를 도난당했다. 원래 지갑의 소유자를 지정하는 코드는 거래 생성자에 의해 제일 처음에만 실행되어야 하지만 패리티 지갑의 경우, 라이브러리로 작성한 해당 함수를 모든 사람이 언제든지 호출 가능한 문제점을 가지고 있었다. 이러한 취약점을 악용하여 해커는 해당 계약의 소유자를 해커의 주소로 변경하는 공격으로 토큰 세일 때 펀드 금액을 저장하는 다중서명 계약에서 대량의 이더를 탈취할 수 있었다.

이와 같이 스마트 계약은 코드에 취약점이 존재할 가능성이 있으며 해당 취약점이 해커에 의해 악용된다면 막대한 금전적 손실이 발생하는 사고로 이어질 가능성이 매우 크다. 스마트 계약에 대한 보안 수준은 개발자 역량에 좌우되며 별도의 검증 기능은 존재하지 않는 것이 현재의 실정이다. 앞으로 스마트 거래에 대한 활용이 증가하게 되는 경우를 대비하여 이에 대한 충분한 검토가 필요한 상황이다.

나. 시사점

블록체인의 금융 적용에서 발생하는 문제로 암호화폐 거래소 해킹, ICO를 이용한 사기, 개인정보 유출과 부정 거래, 스마트 거래 해킹 등을 찾을 수 있었다. 모든 사고 사례에서 블록체인 자체의 문제이기 보다는 이를 금융 분야에 활용하는데 있어 낮은 보안 의식, 관련 정책 부재 및 미흡, 기술력 부족 등이 문제였다.

암호화폐 거래소의 해킹은 대부분 낮은 보안 의식 때문에 발생하였다. 암호화폐 거래소의 지갑 서비스는 편리하지만, 서버 해킹으로 개인키가 유출될 수 있음을 주의하여야 한다. 서버가 아닌 PC나 USB 등에 지갑을 암호화하여 보관하는 것이 대량 도난 사고로부터 비트코인을 안전하게 보호하는 방법이다. 그러

28) 다중서명(Multisignature, Multi-Sig) 지갑이란 여러 명의 지갑 소유자의 동의를 얻어 암호화 자산을 관리하도록 설계된 스마트 계약,
(<https://cointelegraph.com/news/parity-multisig-wallet-hacked-or-how-come>. 참고)

나 PC나 USB의 도난, 파손 등으로 개인키를 잃어버리는 경우 자신의 암호화폐를 영원히 사용할 수 없음을 주의해야 한다. 만일 개인키가 유출된 것 같다면 새로운 지갑을 생성하고 새 지갑으로 비트코인 즉시 이동해야 한다. 새로운 지갑으로 비트코인이 옮겨지면 유출된 이전 개인키로는 해커가 해당 비트코인을 탈취할 수 없게 된다.

ICO는 기술력은 있으나 자금 조달이 어려운 스타트업이 전 세계 누구에게나 손쉽게 투자를 받을 수 있게 하는 암호화폐 기반의 새로운 투자 방법이다. 크라우드 펀딩, VC, IPO보다 투자 절차가 간단하고 비용이 적게 들지만, 일부 부도덕한 기업들의 신용 사기(scam), 다단계, 유사수신행위 등으로 투자자들에게 손해를 입히는 경우가 발생하고 있다. ICO 투자 시 해당 기업의 기술력과 미래 가치를 자세히 고려하여 손해가 발생하지 않도록 주의해야 한다. 블록체인 기술이 갖는 다양한 가능성이 발현될 수 있도록 해외 각국의 가상통화 및 ICO에 관한 정책변화를 적극 모니터링하면서 국내에 적합한 정책을 구사해 나가는 것이 필요하다.

빗썸(2017.06.) 개인정보 유출사건, 야피존(2017.04.) 해킹 등으로 인해 가상화폐 거래소에 대한 정보 보안의 불안감이 높아지고 있다. 개인정보 유출 및 해킹을 방지하기 위한 의무사항 준수 여부를 확인하고 지속적으로 관리 감독하는 역할이 강화되어야 할 뿐만 아니라 가상화폐 거래소 스스로 개인정보 유출이나 각종 해킹의 피해를 줄이기 위한 노력이 요구된다. 아직까지는 블록체인을 통한 부정거래나 자금세탁관련 거래 등 비정상적인 거래가 발생하여도 거래 취소 등의 대응이 어려우므로 사전에 탐지 및 차단하기 위한 노력도 필요하다. 이상금융거래 탐지 시스템(Fraud Detection System, FDS)의 방식을 참조하여 접속정보, 거래내용 등을 종합적으로 분석하여 불법 의심거래를 탐지하고 차단하기 위한 연구를 수행할 수 있다. EU 집행위원회의 경우, 공개키 기반구조(public key infrastructure, PKI)의 자금세탁방지 기술을 연구하여 거래소와 같은 블록체인의 문지기 역할을 수행할 주체에게 적용하고자 노력하고 있다.

스마트 계약의 취약점을 보완하기 위해서 기술과 제도적 관점의 검토가 모두 필요하다. 먼저 기술적으로는 스마트 계약 코드를 배포하기 전에 코드리뷰를 통해 보안 취약점 존재 여부와 악성코드 감염 여부를 사전에 확인하는 과정이 필수적이다. 금전적 거래와 관련된 스마트 계약을 개발하는 경우에는 배포 전에

시간을 갖고 사전 코드 리뷰 및 단위 테스트(Unit Test)²⁹⁾ 등의 검증방식을 통해 충분한 검토가 이루어 져야 할 것이다. 일반적으로 많이 사용되는 함수의 경우, 효과적이고 안전하게 구현될 수 있도록 표준 라이브러리로 개발/배포하여 검증된 스마트 계약 코드 사용을 권고할 수 있다. 또한 스마트 계약의 완결성을 제고할 수 있도록 코드의 취약성을 보완할 수 있는 스마트 계약 관련 가이드라인을 만들어 배포하는 것도 하나의 방안이 될 수 있다. 그리고 제도적으로는 개인 간 스마트 계약에서 당사자 간 이슈가 존재하는 경우, 피해에 대한 법적인 보호 조치를 마련하고 문제를 예방하기 위한 기존 법·제도 개정을 위한 검토 역시 필요하다.

제5절 소결

이 연구에서는 새로운 기술로 인해 변화가 클 것으로 예상하는 교통 안전, 시설물 안전, 사회기반(금융) 안전 분야를 선정하였다. 선정된 분야는 새로운 기술의 등장으로 법·제도에서부터 행정관리까지 전반적인 수정을 요구한다. 각 안전 분야에 지대한 영향을 주는 자율주행차, 스마트 빌딩, 블록체인 기술에 대한 특징과 시장 및 정책에 대한 동향을 조사하였고, 각 기술을 구성하는 요소 기술에 대해서도 분석하였다. 마지막으로 각 분야의 사고사례를 조사하여 이를 바탕으로 시사점을 도출하였다.

자율주행차는 2025년부터는 사람의 개입 없이 독립적으로 운행이 가능할 거라 예상된다. 시장 규모도 대폭 증가하여 60만대 수준에 도달할 것이며 이후 2035년에는 2,100만대 수준으로 늘어날 것으로 예상된다. 자율주행차의 상용화를 위해서는 기업의 연구·개발도 중요하지만, 정부의 적극적인 개입을 통한 임시 운행제도 마련 및 법적 규제 근거 정비를 통하여 국제 표준에 맞는 평가 절차를 구축해야 한다. 또한, 교통사고 발생 시 책임 및 보험 등의 문제에서도 정부의 역할이 매우 중요하다.

자율주행차는 환경인식 기술과 측위 기술, V2X 기술 등이 핵심 요소 기술이다. 환경인식 기술은 차량 주행 관련 주변 교통 정보를 빠르게 수집하며 해석 및 의사결정을 신속히 실행하는 데 사용된다. 측위 기술은 정밀한 자동차 위치

29) 컴퓨터 프로그래밍에서 소스 코드의 특정 모듈이 의도된 대로 정확히 작동하는지 검증하는 절차

를 추정하는 데 필수요소이다. 이를 통한 주변 환경 인식의 개선 및 주변 지형을 고려한 최적의 제어로 안전성 향상 및 연비 절감 효과를 볼 수 있다. 마지막으로 V2X는 차량 주행 중 유/무선망을 이용하여 다른 차량 및 도로 등 인프라가 구축된 사물과 서로 교통 상황 등의 정보를 교환하는 데 사용된다.

자율주행차를 개발하고 있는 구글 및 테슬라의 대표적인 사고 사례를 통해 기술 개발에 따른 한계에 대해 알아보았다. 특히, 자율주행차가 개발됨에 따라 기존 차량보다 더 많은 전자·통신 기능을 내장하고 있으며 이에 따라 해킹하기 쉬운 보안 취약점 및 오작동의 위험들이 증가하고 있다. 이에 대응하여 보안 위협에 대한 대응책과 더불어 연구 개발에 박차를 가해야 한다. 마지막으로 돌발 상황을 인지한 뒤에 앞으로 벌어질 상황을 예측해 제일 나은 선택을 하는 인공지능 기반의 의사 결정 체계의 고도화가 필요하다.

스마트 빌딩에 대한 개념은 1980년대에 등장하였지만, IoT 등의 발달로 최근 주목을 받기 시작했다. 스마트 빌딩의 서비스 시장 규모는 전 세계적으로 2015년 130억 불에서 2020년 320억 불로 연간 22%의 성장을 할 것으로 예측되었다. 스마트 빌딩에서 IoT기기는 IoT 설치에 따른 보조금 지급, 이미 설치된 건물자동화시스템과의 연계 등으로 건물의 에너지 소비를 감축할 수 있어서 IoT 관련 기기 및 서비스가 시장을 선도할 것을 예측된다. 이에 우리나라를 포함해 해외 주요국들은 스마트 빌딩에 대한 적극적인 정책을 펴고 있다.

스마트 빌딩은 다수의 서로 다른 제조사와 다양한 장비가 사용되며 이러한 장비를 하나로 통합 제어하기 위해서는 공통의 언어를 사용한 데이터의 송수신이 필수적이다. BACnet과 ZigBee 등이 대표적인 통신 기술로 사용되고 있다. 이와 더불어 스마트 빌딩의 건물 자동화 시스템, 냉난방공조시스템, 조명 시스템, 엘리베이터, 방재 시스템, 방범 시스템 등이 주요 기술이다. 인공지능 기반의 빅데이터 응용 기술은 특히 스마트 빌딩의 건물에너지 및 설비 제어 분야에 예측 제어, 고장예지진단 등을 위해 적용되고 있다.

스마트 빌딩의 주요 제어시스템과 IoT 기기는 서로 연동이 되어 있어 IoT에 대한 보안이 매우 중요하다. IoT 환경에서 발생할 수 있는 보안 위협요소는 단말 분실 및 물리적 파괴, 무선신호 교란, 정보 유출, 데이터 변조 등이 있다. 또한, 스마트 빌딩에서는 특히 통신 네트워크의 보안이 중요하다. 스마트 빌딩에서

많이 사용되는 ZigBee는 단말 성능이 경량화되어 고도의 암호화가 어려운 측면이 있으며, ZigBee의 모든 통신구간에 대한 암호화가 이루어지는 것이 아니므로 이에 대한 대책이 필수적이다.

블록체인 기술은 기존 금융에서와 같이 공인된 제3의 중개기관에 대한 의존성이 높은 분야에 적용 시 높은 효율성을 기대할 수 있다. 특히, 중앙 서버가 아닌 분산 저장방식으로 인한 보안성 및 투명성 제고 등의 장점으로 다양한 분야에서 주목받고 있다. 블록체인 기술은 2020년 연간 성장률 120%를 기록하고 시장 규모는 2030년 3,400조 원 규모에 달할 것으로 예측된다. 미국, 일본 등 주요국은 금융 분야의 컨소시엄과 협의체를 발족하여 나라별 실정에 맞도록 산업체와 정부의 협력을 통해 발전하고자 노력하고 있다.

블록체인의 요소 기술은 암호기술과 P2P 네트워크 기술이다. 암호기술로부터 블록체인의 신뢰성과 투명성이라는 특성이 확보된다. 특히, 암호기술 중 암호학적 해시함수(cryptography hash function)는 데이터가 변조되었는지를 확인하는 역할을 하고, 전자서명(digital signature)은 데이터가 실제 주인(owner)에 의해 작성되거나 수정되었는지를 증명한다. 또한, P2P 네트워크는 블록체인이 네트워크의 여러 노드에 분산 저장됨에 따라 변조는 더욱 어려워지고 투명성은 올라가게 된다.

블록체인 기술의 금융 분야 활용에서 여러 문제가 발생하고 있다. 최근 암호화폐의 가치 급상승으로 암호화폐 탈취를 목적으로 한 거래소 해킹 사고가 대표적이다. 블록체인 기반의 새로운 투자방식인 ICO를 이용한 투자사기는 또 다른 선의의 피해자를 양산하고 있다. 익명성을 보장하는 블록체인의 특성과는 달리 암호화폐를 법정화폐로 교환할 때 의도치 않게 발생하는 개인정보 침해도 문제가 되고 있다. 또한, 불법 자금 거래 등 부정 거래 가능성도 높은 편이다. 블록체인을 이용한 스마트 거래 역시 여러 취약점으로 인해 큰 피해가 발생하였다. 모든 사고 사례에서 블록체인 자체의 문제이기 보다는 이를 금융 분야에 활용하는 데 있어 낮은 보안 의식, 관련 정책 부재 및 미흡, 기술력 부족 등이 문제였다.

지능정보사회의 도래로 국민의 안전을 확보하고 강화하는데 과급력이 클 것으로 예상하는 교통 안전, 시설물 안전, 사회기반 안전(금융) 분야의 신기술에

대해 알아보았다. 추후 관련 분야에서의 법·제도 측면과 행정 관리 측면에서의 개선방안 및 정책과제에 기초 자료로 활용되기를 기대한다.

제3장 행정관리 중심으로

제1절 개요

이 장에서는 협동 연구 기관인 한국행정연구원에서 “지능정보사회를 대비한 안전관리체계 리모델링에 관한 연구 - 행정관리 중심으로”라는 주제로 작성한 제3권의 내용을 요약 정리한다.

1. 추진 배경

최근 지식정보사회를 넘어 지능정보사회가 도래하고 있으며, 새로운 가치가 창출되고 발전하고 있다. 이러한 지능정보사회의 도래는 역사상 유례가 드문 거대한 스케일의 변화를 요구하고 있으며 지능정보사회에 효과적으로 대응하기 위해서는 새로운 과제와 정책적 대응 또한 요구되고 있는 실정이다. 이에 따라 민간은 물론 공공부문에서도 지능정보기술을 적극 활용한 선진화된 지능형 정부로의 변화의 필요성이 커지고 있다. 특히, 선진화된 지능형 정부로의 변화 요구 중 재난 및 안전관리 분야에 있어서 국민을 보다 안심·안전하게 보호해 줄 수 있는 새로운 국가안전관리체계의 구축이 요구된다.

한편, 우리나라의 안전수준을 경제수준과 비교하여 판단해 보았을 때 아직도 미흡하다고 볼 수 있다. 우리나라는 2015년 기준 1인당 GDP 2만 8,000달러, 세계경제순위 11위의 경제대국으로 성장했으나 세월호 사고에서 확인할 수 있듯이 아직까지 안전 수준은 높지 않은 형편이다. 이처럼 높지 않은 우리나라의 안전수준을 선진국 수준으로 끌어 올리고자 국민안전처(現 행정안전부)는 2014년 11월 출범 후 “안전혁신 마스터플랜”을 수립하여 재난 및 안전 관리 전반에 걸친 혁신을 주도하는 노력을 추진해왔다. “안전혁신 마스터플랜”은 2014년 4월 발생한 세월호 사고를 계기로 재난 및 안전관리체계를 원점에서 재검토하여 근본적인 안전 혁신방안을 추진하는 것을 목표로 하고 있다. 우리 정부는 안전대진단 등을 통해 국민들의 적극적인 참여를 유도하고, 재난안전 전 분야, 전 과정에 걸친 종합적, 중장기적 혁신계획을 추진하고 있다.

문재인 대통령은 2017년 5월 10일 치러진 제19대 대통령 선거 시 후보자 10

대 정책 공약 중 하나로 ‘안전하고 건강한 대한민국’을 제시하였다. 이 공약에는 국가가 국민의 생명과 안전을 책임진다는 내용을 포함하고 있으며, 이를 위해 4대 목표와 5대 이행방법을 발표하였다. 4대 목표에는 깨끗하고 안전한 사회의 건설하고, 자연재해와 사회적 재난으로부터 국민을 보호하겠다는 내용을 포함하고 있다. 또한, 5대 이행방법에는 청와대 중심의 재난대응 컨트롤 타워를 구축하고, 재난사건에 대한 대응체계를 강화하겠다는 내용을 포함한다. 또한, 문재인 대통령 취임 이후 새 정부는 국정기획자문위원회를 통해 “국정운영 5개년 계획”을 발표하였다. 동 계획에서 재난 및 안전과 관련한 내용은 ‘내 삶을 책임지는 국가(5대 국정목표)’의 전략 3. ‘국민안전과 생명을 지키는 안심사회(20대 국정전략)’에 포함되어 있다. 따라서 이러한 변화 요구에 부응하고 지능정보사회의 변화에 적극적으로 대응하기 위하여 다양한 관점(기술, 행정, 법·제도)에서 거시적 관점의 국가안전체계 연구 수행이 요구된다.

2. 연구의 목적

본 연구는 지능정보사회 변화 요구에 따라 신기술이 적용되어 국민의 안전을 확보·강화하는데 파급효과가 클 것으로 예상되는 교통 안전, 시설물 안전, 사회 기반(금융) 안전 분야를 중심으로 지능정보사회 출현에 따른 사회변화 내용 분석, 신기술 적용시 예상되는 주요 쟁점 분석, 기존 국가안전관리체계의 문제점 진단, 그리고 효과적인 대응을 위한 변화 및 개선방안 등을 정부 행정 차원에서 종합적으로 도출하여 제시하고자 한다.

첫째, 현재 교통 안전관리체계는 개별법 위주의 법률체계에 따라 다양한 법령이 연관되어 있으며, 교통 안전 관리를 위한 다양한 관리 주체가 존재한다. 기존 교통 안전관리체계에 신기술인 자율주행차가 도입될 경우 교통환경 변화에 따른 대응전략의 마련 및 이를 관리하기 위한 주체의 확립이 필요하다. 기존의 문헌 분석 및 전문가 조사를 통해 자율주행차 도입에 따른 위험요인을 분석하고, 위험요인에 대한 대응을 위한 교통 안전관리체계의 개선방안을 제시한다.

둘째, 시설물/건축물 안전관리는 1995년 제정된 「시설물의 안전관리에 관한 특별법」(이하 시특법)에 따라 이루어지고 있으나 시설물 붕괴 등의 사고가 잇따라 발생하며, 노후 시설물 안전관리에 대한 관심이 높아지고 있으며, 이에 따라 안전관리체계의 패러다임 전환(건설(공급) 중심에서 유지보수(관리) 중심으로)이

요구되고 있다. 현행 안전관리 체계의 개선과 더불어, 지능정보기술이 도입된 형태인 스마트 빌딩, 스마트 건축이 등장하고 있어, 이에 대한 미래지향적 위험관리 체계에 대한 고려가 필요한 실정이다. 문헌분석 및 전문가 조사를 통해 스마트 빌딩, 스마트 건축 등의 활성화에 따른 위험요인에 대해 분석하고 이를 반영하는 안전관리체계의 전환 방안을 제시한다.

셋째, 사회기반 안전관리(금융) 분야의 경우, 현재 관련법이나 규제체계가 정부부처별로 다기화 되어 있어 블록체인과 같은 신기술이 법적 허용공간으로 진입하는 것 자체가 매우 어려운 상황이다. 지금의 기술적 발전(블록체인 기술 등)은 단기적 효과가 과도하게 부각되는 반면, 잠재적 위험이나 문제에 대한 대응에 관한 충분한 검토가 결여된 바 이를 누가 담당할 것인가에 관한 이슈도 상존한다. 이에 따라 문헌분석 및 전문가 조사를 통해 블록체인의 활성화에 따른 위험요인에 대해 분석하고 이를 반영하는 안전관리체계의 전환에 대한 방안을 제시한다.

제2절 교통 안전 : 자율주행차

1. 교통 안전분야의 지능정보기술에 따른 영향 검토

교통 안전 분야에 지능정보기술(자율주행차, IoT 등)의 적용이 확대됨에 따라 나타나는 가장 두드러진 변화상(특징)을 교통인프라, 교통이용자 행태, 스마트 교통수단, 그리고 안전관리 정보시스템 등으로 구분하여 분석하였다. 교통 분야에서 지능정보기술이 적용될 경우 긍정적인 부분과 부정적인 부분이 함께 나타나게 될 것이다.

첫째 교통인프라에 지능정보기술 도입은 ① 기존 인프라 이용 효율 최대화와 디지털 인프라 확대, ② 인프라 관리 측면에서 비용절감 등의 긍정적인 측면이 있는 반면에, 부정적으로는 ① 보안 및 개인정보 침해, ② 기존 인프라 첨단화를 위한 대규모 투자 요구 등의 부정적인 측면도 함께 나타날 것으로 보고 있다.

둘째, 지능정보기술 도입에 따라 교통이용자 행태 변화로는 ① 교통수단 간 연계 확대 및 공유형 교통수단의 편의성 증대로 인한 접근성 높은 통행 가능, ② 사고 감소 및 무운전으로 인한 운전자의 운전 스트레스 완화와 이동 중 차량

내 다양한 활동 가능 등과 같은 긍정적인 부분이 있는 반면에, ① 자율주행차가 대중교통이 아닌 개인 승용차 위주로 적용이 될 경우 장거리 통행이 증가할 가능성이 높음, ② 개인 위치정보와 이동정보 노출로 사생활 침해 우려 등이 있다.

셋째, 지능정보기술(자율주행, IoT 등)을 활용한 ‘스마트 교통수단’에서는 ① 수요 맞춤형 교통수단으로 통행에 시·공간적 제약 감소, ② 초소형·개인형 이동수단의 등장으로 교통 접근성 개선, ③ 자율주행차와 전기자동차의 등장으로 교통 안전과 환경 개선 등의 긍정적인 부분이 있다. 하지만 ① ICT에 대한 수용성이 높은 이용 계층에 스마트 교통수단이 편중될 수 있음, ② 초소형·개인형 이동수단의 안전 기준 마련이 미흡하여 사고 발생을 줄이는데 한계, ③ 스마트 교통수단과 비스마트 교통수단과의 상충 증가 등의 문제가 우려된다.

마지막으로, 교통 분야에서 지능정보기술(자율주행, IoT 등)을 활용한 안전관리 정보시스템은 ① 위험요인에 대한 실시간 모니터링이 가능해져서, 안전 위험요인에 사전적으로 대응이 가능, ② 사고 발생 위치와 시간을 신속히 알 수 있어 대처 시간 단축, ③ 안전관리 정보의 자동화로 관리 효율성 증대 등의 긍정적인 측면이 있다. 한편, 교통 분야의 안전관리 시스템은 ① 다량의 정보가 하나의 정보시스템을 통해 관리될 경우 해킹에 노출 시 재난상황 발생 가능, ② 시스템의 에러 발생에 대한 원인 규명 및 대처 지연, ③ 전문가의 종합적 판단 능력 배제 등의 부정적인 측면이 있을 것으로 보인다.

2. 교통 안전관리체계 현황 분석

교통수단·시설 또는 교통체계의 운행·운항·설치 또는 운영은 중앙행정기관(국토교통부)이 관장하고 있고, 교통 안전 관리 체계 역시 중앙집권적인 특징을 가지고 있다. 즉, 교통 인프라와 운영, 그리고 안전관리체계까지 교통 관련해 거의 모든 권한이 중앙정부에 집중되어 있다. 이와 같이 중앙집중식의 비효율적인 교통 인프라와 안전관리 체계로 인해 비용과 부담이 지속적으로 증가하고 있는 실정이다.

제4차 산업혁명 시대의 도래로 교통 부문의 급속한 변화가 있을 것으로 예측되고 있지만, 현행의 방식을 고수할 경우 교통 부문은 새로운 서비스의 제공에서 뒤떨어질 수 있다. 제4차 산업혁명을 선도하는 지능정보기술에 의해 초연결

사회 혹은 환경이 조성되면서 새로운 접근방식이 절실해지고 있다. 특히 제4차 산업혁명 시대를 맞이하여 자율주행차와 같은 스마트 센서(Smart Sensor)에 의한 교통수단의 등장은 전통적인 교통 인프라뿐만 아니라 교통 안전 관리체계에 서 변화를 요구하고 있다. 그렇지만 우리는 물리적인 교통 인프라가 이들 기득 권 위주로 편중되어 있어 미래의 교통 안전 관리 체계의 마련을 위한 노력에 있 어 소극적인 편이다. 특히 제4차 산업혁명 시대에 걸맞은 교통 안전관리체계를 구축하기 위한 협력보다는 기득권을 지키기 위해 개방과 협업에는 소극적인 자 세를 취하고 있다.

한편, 현재 「교통 안전법」이나 「도로교통법」 등과 같은 교통 안전 관리 체계를 뒷받침하는 법률들은 지능정보기술이 반영되어 있지 않은 아날로그 시대 의 교통 안전 관리체계에 초점을 두고 있다. 또한 지능정보기술의 도입에 따른 교통환경 변화에 대응하는 전략을 마련하고 관리하기 위한 주체가 확립되어 있 지 못하다. 즉, 제4차 산업혁명 시대의 도래로 교통 부문에서 지능정보기술이 도 입되면서 등장한 자율주행차에 대한 교통 안전 관리 방안을 찾기가 어렵다는 것 을 의미한다.

현재 우리나라의 교통 안전 관리 행정시스템은 새로운 지능정보기술들을 포 함하는 기술적 요인의 전면적 변화를 수용할 준비가 되어 있지 않은 실정이다. 제4차 산업혁명에 선제적으로 대응하기 위해 기술적 요인을 앞세운 새로운 자율 주행차 업체 등을 중심으로 관련자들이 지능정보기술을 반영한 교통 안전 관리 체계를 만들기 위해 기존 법체계의 완화나 변화를 말하고 있지만 상황은 여의치 않다. 즉 자율주행차 등 지능정보기술이 포함된 부분에 대한 관련법이나 규제체 계가 정부부처별로 다변화 되어 있어 법적 허용공간으로 진입하는 것 자체가 매 우 어려운 상황이다. 중앙정부는 패러다임 변화의 시대에 부응하기 위해 기존의 법체계를 수정·보완하는데 있어 아주 소극적인 자세를 취하고 있는 실정이어서 교통 안전 관리 체계의 변화에 대한 논의 여건이 성숙하지 못한 상황이다.

지능정보기술은 하루가 다르게 진화를 거듭하고 있고, 이러한 기술의 대변혁 시기에 사회전반의 변화를 초래할 수 있는 상황에 대한 수용이 필요한 실정 이다. 물론 새로운 기술을 통해 과거 교통 안전 관리 체계의 이슈들에 대한 대대 적인 변화가 필요하고, 이로 인한 위험요인이 존재하는 것은 부인할 수 없다. 특 히 자율주행차 등 상용화가 완전히 이루어지 않아 교통 안전 관리 체계를 위협

하는 새로운 요인들에 대한 식별조차 이루어지지 않은 상태에서 이를 관리하기 위한 제반준비의 결여는 현 기술적 요인에 대한 전반적 차원의 판단을 어렵게 하는 요인으로 작용할 수 있다. 즉, 기술발전을 수용할 수 있는 사회적 인프라가 구축되기 전까지는 많은 관심과 노력, 그리고 해당 기관뿐만 아니라 정부 차원의 가이드라인 마련이 절대적으로 필요하다. 이를 바탕으로 법제를 구체화 하고 미래의 교통 안전 이슈들에 대한 대비가 가능할 것이다.

3. 교통 분야 지능정보기술 적용 시 발생 가능한 위험성과 문제점

제4차 산업혁명으로 인해 교통 분야 역시 많은 영향을 받게 되고, 기존의 안전관리 체계는 지능정보기술의 적용으로 인해 위험성과 문제점을 보일 것이다. 교통 안전분야에 지능정보기술(자율주행차, IoT 등)이 적용되었을 때 나타날 수 있는 위험으로는 ① 교통 안전 관리 시스템의 오류, ② 정보보안 및 개인정보보호, ③ 교통 안전 관리 능력 문제 등이 있다. 즉 지능정보기술 도입으로 교통 분야는 편의성과 안전성이 증대하지만, 해킹 및 바이러스 등에 의한 정보보안이나 개인정보 침해 등의 위험성도 증가할 것이다.

먼저, 기술적 측면에서 보면, 한국산업기술평가관리원 산업기술수준조사에 따르면 최고수준의 원천기술을 보유한 유럽과 비교하여 한국은 1.4년 정도(유럽의 83.8%, 세계4위 수준)의 격차가 있는 것으로 나타났다. 원천기술수준 2위인 일본이나 3위인 미국의 경우 유럽과 실질적으로 차이가 없으나, 한국의 경우 완성차·부품제조, 소프트웨어, 통신 등 자율주행차를 구성하는 개별기술이 경쟁력을 보유했음에도, 상용화 시점이 기술수준 격차 대비 약 7.2배 뒤쳐져 있는 상황이다.

다음으로, 규제 및 인프라 측면에서는 미국, 일본 등 선진국은 자율주행차의 자유로운 도로 테스트를 위해 상기와 같은 규정을 규제로 간주하여 완화 중이며, 추가 규제 발굴을 위해 노력하고 있다. 또한, NHTSA에서 발표한 자율주행차 5단계에 따라 사고에 대한 책임여부가 이미 정립되어 있으나 국내 학계에서는 여전히 책임 주체에 대하여 논쟁 중이다. 이와 같은 인프라의 부재와 규제는 자율자동차 산업의 진입 장벽을 높이고, 성능개선 및 개발속도를 저하시켜, 기술산업발전에 장애가 될 가능성이 있다.

마지막으로, 교통 안전 측면에서의 자율주행차의 도입에 따른 대표적인 변화는 교통 사고량의 변화를 예상할 수 있다. 자율주행차의 도입에 따른 변화로 교통사고 감소 가능성과 증가 가능성이 동시에 예상된다. 자율주행차가 도입되면 도로 안내 및 규제를 준수하여 교통사고의 약 90%를 차지하는 운전자 과실에 의한 교통사고 감소에 크게 기여할 것으로 예상된다. 반면에, 자율주행차가 완벽하게 교통사고를 예방할 수 없으며, 운전자들의 자율주행차에 대한 과신, 교통약자 부주의 등으로 인해 교통사고 가능성이 증가할 수 있다.

4. 교통 안전관리체계의 리모델링 방향 도출

가. 안전관리 거버넌스 변화 방향

지능정보기술이 접목된 새로운 교통수단인 자율주행차가 도입되면 교통 안전관리를 위해서는 현행의 법·제도 및 관련 기관의 역할 등 전반적인 교통 안전관리체계의 정비가 필수적으로 이루어져야 한다. 그러나 자율주행차와 비자율주행차가 함께 운용될 것이기 때문에 기존의 교통 안전 관련 법제의 틀을 크게 훼손하지 않으면서 시대적인 변화에 부응하는 교통 안전 관리체계를 만드는 것은 쉽지 않은 일이다. 지능정보기술이 도입되어 편의성과 안전성의 혜택을 증대시키고, 위험요인들을 줄이기 위해서는 교통 안전 전반에 걸쳐 새롭게 접근해야 한다. 즉 법제와 인프라 등 교통 안전 환경 측면뿐만 아니라 관련된 모든 요인들을 충분히 검토하여 균형 잡힌 안전관리 체계 구축이 될 때 가능한 것이다.

제4차 산업혁명으로 인해 지능정보기술의 발달에 따른 미래 교통 안전 분야 관리체계는 ① 환경변화에 따른 변화에 능동적 대응, ② 법제의 정비 및 마련, ③ 교통 안전관리 거버넌스 체계 구축 등이 필요한 것으로 나타났다.

나. 교통 분야 안전관리 대응 전략

교통 분야에 있어서 지능정보기술의 보다 광범위한 적용을 위해서는 필요한 법이나 제도, 가이드라인이 마련되어야 한다. 또한, 현재의 교통 안전 관리시스템이 자율주행차와 관련된 안전 이슈들을 포함하고 자율주행차 운행에 충분히 대응할 수 있는지를 검토해야 한다. 또한, 최근의 패러다임 변화(제4차 산업혁명, 지능정보기술 등의 출현)에 대응하여, 교통 분야 안전관리 추진체계와 관련

한 대응전략으로는 ① 교통 안전 관리에 있어 일원화된 관리 주체 필요, ② 교통 안전 추진체계의 수정·보완, ③ 정보보안 및 개인정보보호, ④ 교통 안전 관리 전문가 양성 및 활용 등이 있다.

5. 교통 분야 안전관리체계 개선방안 도출

지능정보기술을 적용한 자율주행차는 교통수단에서 가장 주목 받고 있고, 교통 부문 전반에 걸쳐 큰 변화를 초래할 잠재력을 가지고 있다. 그러므로 미래형 교통수단과 운영체계로서 우리 사회의 모든 분야에 걸쳐 상당한 영향력을 행사할 것으로 전망된다. 자율주행차는 기존의 자동차 및 정보통신기술 분야 등 산업부문의 생태계를 흔드는 파괴력이 큰 이슈이지만, 새로운 교통인프라의 구축과 정보보안·개인정보 침해 등의 위험성까지 동시에 내포하고 있다. 특히 자동차 및 정보통신기술 산업은 자율주행차 등의 교통부문에 지능정보기술을 적극적으로 수용하려는 움직임을 활발히 보이고 있으나, 여전히 공급자 중심의 시각과 시장 흐름에 수동적이고 소극적으로 협조하는 분위기가 있다. 이러한 대응태도는 법제나 관리 체계가 새로운 기술의 적용과 관련하여 어떠한 판단을 내리기 어려운 상황과 직결되어 있으며, 실제로 최근 들어 소개되고 있는 기술들은 체계적인 차원의 변화를 내포하므로 특정 법률이나 제도의 판단을 적용하는데 어려움이 있는 실정이다.

따라서 자율주행차 등의 스마트 교통수단이나 인프라를 도입할 경우 발생하는 여러 가지 문제점을 보완하는 과정에서 전반적인 법제나 안전관리 체계가 구축될 것으로 보인다. 교통 분야의 안전관리 체계 개선을 위해서는 교통 안전 거버넌스 체계의 구축, 전문인력 양성, 정보보안 및 개인정보보호 방안 수립, 선진 사례의 적극적인 도입이 필요하다.

첫째, 통합적인 교통 안전 거버넌스 체계의 구축이 필요하다. 기존 교통 안전 관리체계는 지능정보기술의 도입에 따른 안전관리에 있어 적합하지 않은 측면이 있는데, 대표적으로 자율주행차와 비자율주행차가 동시에 주행을 할 경우에 현행의 교통 안전 관리체계로는 충분하지 않다. 따라서 지능정보기술의 도입으로 발생할게 될 다양한 위험에 대처하기 위한 통합적인 교통 안전 거버넌스 체계의 구축이 우선되어야 한다.

둘째, 지능정보기술에 대한 높은 이해력을 가진 전문 인력의 양성이다. 제4차 산업혁명으로 인해 IoT, AI, 빅데이터 같은 지능정보기술이 교통 분야에 적용될 경우 교통과 지능정보기술에 대한 이해를 가진 인력이 필요하다. 그렇지만 대부분의 교통 분야의 종사자들은 지능정보기술에 대한 이해가 낮아 안전관리체계의 원활한 수행을 위해서는 전문 인력이 필요하다. 따라서 교통 분야와 지능정보기술 모두를 알고 있는 교통 안전 관리 전문 인력을 시급히 육성해야 할 것이다.

셋째, 지능정보기술의 도입으로 인해 정보보안 문제와 개인정보 침해와 같은 문제가 발생할 수 있다. 지능정보기술의 도입으로 보다 수준 높은 서비스의 제공이 가능하지만, 해킹으로 인해 정보보안이 불안해지고, 이로 인해 개인의 많은 정보가 유출되는 문제가 발생할 수 있다. 교통 안전 관리체계에 지능정보기술이 도입될 때, 보다 수준 높은 정보보안 체계의 구축과 개인정보보호를 위한 방안을 마련해야 한다.

마지막으로, 자율주행차와 관련해 선진국의 법제들을 검토하여 다양한 이슈들에 대응할 수 있는 준비가 필요하다. 교통 분야의 안전관리를 위한 자율주행차와 같은 지능정보기술의 도입을 수용할 수 있는 제도적 인프라가 구축되기 전까지는 많은 관심과 노력, 그리고 해당 기관뿐만 아니라 중앙 및 지방 정부 차원의 계획이 있어야 한다.

<표 3-1> 교통 안전 : 자율주행차 연구 내용 요약표

문제점 및 위험성 분석	리모델링 방향	개선방안
[현행 체계 문제] - 교통 안전 관리체계의 미비 - 교통 안전 관리 평가지표의 미흡 및 법률 간의 관계가 모호 - 교통 안전 관련자 책임소재가 모호 - 지능형 교통 안전 관리를 위한 전문기술인력 부족 - 교통 안전 관리 대상의 범위 확대	① 자율주행차에 맞춘 법제 정비 - 자율주행차에 맞춘 도로교통법, 보험관련 조항 마련 - 안전사고에 대한 책임소재 명확화 ② 교통 안전 시스템의 보안 강화 체계 - 정보보안 강화를 위한 신기술 도입 - 개인정보 보호 법·제도 강화 생애주기별 안전관리체계 ③ 주행 데이터 신뢰성 검증 체계 - 데이터 관리 시스템 구축 - 시스템 오류를 줄이기 위한 정확	① 기술적 측면 - 해킹 등에 대비한 정보보안 기술 개발 및 강화 - 자율주행차의 레벨에 따른 위험성 검증을 위한 단계별 시범적용 후 제도화 ② 의식적 측면 - 시스템 오류에 대비한 사람 중심 관리체계 구축 - 지능정보기술 적용 확대 및 위험성 관리를 위한 관련 기관 간 협력과 협업체계 구축

문제점 및 위험성 분석	리모델링 방향	개선방안
[지능정보기술 위험성] - 교통 안전 관리 시스템의 오류 - 정보보안 및 개인정보보호 침해에 대한 대응 문제 - 교통 안전 관리 능력의 문제	한 데이터 확보 ④ 사람에 의한 관리체계 병행 - 안전관리 시스템의 오류에 대비한 안전관리 전문인력 확보	- 지능정보기술 및 위험성에 대한 교육 ③ 제도적 측면 - 통합화된 안전관리체계의 책임관계 명확화 - 교통 안전 이슈별 해당 기관 간 협력체계 구축 - 교통 안전관리에 민간의 책임 소재 명확화

제3절 시설물 안전 : 스마트 빌딩

1. 건축·시설물 안전분야의 지능정보기술에 따른 영향 검토

건축·시설관리 시스템의 변화가 이루어지고 있는데, 최근 빌딩, 도시 인프라 등의 시설 관리 산업은 ICT 기술과 융합을 통해 스마트 산업으로 전환이 가속화되고 있다. 기존 시설관리 산업은 인력 중심의 산업이었으나 최근 센서, 네트워크, 컨트롤러, 소프트웨어 등 기술의 발전으로 자동화, 지능화가 가속화되고 있는 중이다. 이와 더불어 전력 소비의 급증에 따른 전력난이 이슈화되고 세계적으로 그린(Green) 트렌드가 확산되면서 빌딩 내 설비의 효율적인 에너지 관리가 가능한 스마트 빌딩에 대한 수요가 빠르게 확산되고 있다. 한편, 국가 차원에서는 주택 및 빌딩뿐만 아니라 도시 전체 시설물 및 인프라의 커넥티드 환경 조성 및 지능화를 추진하고 있고, 각국 정부의 스마트시티 정책 추진으로 도시의 안전성, 시민 편의성, 에너지/자원 효율성 등이 제고될 것으로 기대하고 있다. 또한 지능정보기술의 적용으로 건축·시설물 생애주기별(설계, 시공, 관리, 개·보수 단계) 영향 분석이 가능해진다.

첫째, 설계단계에서는 ① 수요예측의 정확성 제고 및 리스크 검토·관리용이, ② 지능화된 설계가 가능하고 원가분석 기술 혁신 가능 등의 효과가 있지만, ① 일자리 감소, ② 지나친 표준화로 창의성 실종 같은 문제도 나타날 것으로 보고 있다.

둘째, 시공단계의 변화는 긍정적인 측면에서 ① 시공과정 오류 검토 및 리스

크 관리의 용이함, ② AR/VR 기반의 현장 시공 첨단화 가능 등이 있는 반면, 부정적 응답으로는 ① 일자리는 감소하는 반면에 기업의 수익은 상승, ② 지나친 자동화에 따른 오류가 전체로 확산될 우려가 있다.

셋째, 지능정보기술(IoT, AI 등)을 활용한 건축·시설물 관리단계의 긍정적 측면으로는 ① 상시적 진단이 자동적으로 수행되어 체계적이고 지속적인 관리 가능, ② 사용·관리과정에서 예방적 관리기술을 적용해 건축·시설물의 내구성과 사용연한 증대, ③ AR/VR을 활용한 시설물 유지 관리 및 이력 관리가 가능이 있는 반면, ① 일자리는 감소하는데 반해 기업의 수익만 상승할 것임, ② 지능정보기술 적용 가능한 건물과 불가한 건물 간 기술격차 확대, ③ 기기 오류 시 관리인력 축소에 따른 초기 대응 실패 우려 등의 부정적인 측면도 함께 있다.

넷째, 개·보수단계에서는 ① 건축·시설물의 개·보수 범위 및 방법, 그리고 비용의 예측의 정확성 제고, ② 기존 건축물 정보의 활용을 통한 구성요소의 생애주기(내구성) 확인 가능, ③ AR/VR을 활용한 지하 시설물 모니터링 가능 등의 좋은 점이 있지만, ① 일자리는 감소하는데 반해 기업의 수익만 상승할 것임, ② 생활 불편함 개선을 위한 개·보수 과정에서 개인생활과 관련한 사생활정보가 유출될 가능성이 높음, ③ 지나친 시스템 의존에 따른 판단 오류 우려 등이 있다.

2. 건축·시설물 안전관리체계 현황 분석

건축·시설물 관리 분야에서 빌딩, 도시 인프라 등의 시설 관리 산업은 ICT 기술과 융합을 통해 스마트 산업으로 전환이 가속화되고 있다. 기존 시설관리 산업은 인력 중심의 산업이었으나 최근 센서, 네트워크, 컨트롤러, 소프트웨어 등 기술의 발전으로 자동화, 지능화가 가속화되고 있는 중이다. 이와 더불어 전력 소비의 급증에 따른 전력난이 이슈화되고 세계적으로 그린(Green) 트렌드가 확산되면서 빌딩 내 설비의 효율적인 에너지 관리가 가능한 스마트 빌딩에 대한 수요가 빠르게 확산되고 있다. 한편, 국가 차원에서는 주택 및 빌딩뿐만 아니라 도시 전체 시설물 및 인프라의 커넥티드 환경 조성 및 지능화를 추진하고 있고, 각국 정부의 스마트시티 정책 추진으로 도시의 안전성, 시민 편의성, 에너지/자원 효율성 등이 제고될 것으로 기대하고 있다.

건축·시설물의 설계-시공-관리-개·보수의 전 단계에 걸쳐서 지능정보기술이 도입되면 새로운 환경에 맞춘 안전 관리를 위해서는 시특법 등 현재의 법률과 제도는 적합하지 않은 부분이 많다고 할 수 있다. 시설물은 다양한 분야(구조체, 각종 설비 등)가 어우러진 복합체이고 공간을 다루어야 하므로 관리체계가 복잡한 특성을 가지고 있다. 현행 시설물 안전 관리 체계를 살펴보면, 중앙부처 간 역할분담, 중앙부처-지방자치단체 간의 역할 수행, 그리고 안전점검 민간업체의 전문성 등으로 구분하여 설명할 수 있다.

첫째, 시설물 안전관리체계에 대한 중앙부처 간 역할분담이 분산되어 있다. 현행 시설물 안전관리체계의 총괄기능은 국토교통부와 행정안전부로 분리되어 있는데, 시설물 안전관리 시스템도 국토교통부의 시설물정보관리시스템(FMS), 소규모 취약시설 안전관리시스템(SFMS)과 국민안전처의 국가재난관리시스템(NDMS)으로 분산되어 있다. 현재 국회(국토교통위원회와 안전행정위원회)는 시설물의 안전 관리체계를 국토교통부로 일원화하기 위하여 「재난 및 안전관리 기본법」상의 특정관리대상시설을 「시설물의 안전관리에 관한 특별법」상 제3종 시설물로 소관과 명칭을 변경하는 내용의 법률개정안을 심사하고 있다. 그러나 법률개정 이후에도 소규모 공공시설 등의 안전관리 및 유지관리는 여전히 행정안전부 소관으로 남아있게 된다. 「재난 및 안전관리 기본법」 제10조의3에 따른 재난 및 안전관리 사업의 효과성 및 효율성 평가 등 시설물 안전관리에 대한 국민안전처의 역할도 국토교통부와 별도로 계속된다.

둘째, 중앙부처-지방자치단체의 역할수행은 보수·보강 등 후속조치 이행 관리에 부적정한 측면이 있다. 「시설물의 안전관리에 관한 특별법」 제14조제3항에 따라 1·2종시설물 안전점검 및 정밀안전진단 실시결과 긴급한 조치가 필요하다고 인정되면 특별자치도지사·시장·군수 또는 구청장은 시설물 사용제한 등의 조치를 명할 수 있다. 조치를 하지 않을 경우 지방자치단체의 장은 「시설물의 안전관리에 관한 특별법」 제15조제2항에 따라 보수·보강 이행 및 시정을 명할 수 있다. 그러나 일부 지방자치단체의 경우 후속조치 이행에 대한 관리감독이 부실하여 중대결함이 있는 시설물임에도 불구하고 장기간 보수·보강되지 아니한 채 방치되고 있는 사례가 발생한다.

마지막으로, 민간업체의 안전점검 부실이 문제가 되고 있는 실정이다. 「시설물의 안전관리에 관한 특별법」 제11조의3은 국토교통부장관(한국시설물안전공

단)으로 하여금 정밀점검 또는 정밀안전진단의 부실을 방지하기 위하여 민간업체의 진단결과를 평가할 수 있도록 규정하고 있다. 2015년 기준 민간업체의 정밀안전진단 및 안전점검 시장 점유율은 90.7%(수주금액 약 1,875억 원)이고, 한국시설안전공단 점유율은 9.3%(수주금액 약 191억 원)이다. 국토교통부로부터 평가업무를 위탁받은 한국시설물안전공단은 2015년에 부실진단 우려가 있다고 판단되는 진단결과 26,247건 중 5,600건(21.3%)을 평가하였는데, 이 중 265건(5.5%)이 시정·부실 판정을 받았다. 시정·부실 판정 비율이 2009년에는 17.4%였는데 2010년에 15.5%, 2011년에 10.4%, 2012년에 11.2%, 2013년에 11.6%, 2014년에 6.2%, 2015년에 5.1%로 감소하여 현행 평가제도가 부실진단을 예방함에 있어서 일정 수준 기여한 것으로 보였으나, 미흡·부실 판정사유를 살펴보면 필수시험항목 누락, 적정 평가 기준 미반영 등 안전과 직결되는 매우 중대한 사항들이 포함되어 있어 계속 엄격하게 평가할 필요가 있다. 시·도지사는 점검·진단을 부실하게 수행한 것으로 평가받은 민간업체에 대하여 「시설물의 안전관리에 관한 특별법」 제9조의4에 따라 영업정지 등의 행정처분을 하여 관리감독을 강화할 필요가 있다.

3. 건축·시설물 분야 지능정보기술 적용 시 발생 가능한 위험성과 문제점 분석

건축·시설물 안전관리의 전 과정에 제4차 산업혁명 시대의 지능정보기술 도입으로 긍정적인 변화가 이루어질 것이라는 의견이 있는 반면에, 오히려 지능정보기술의 오류나 외부 공격에 의한 위험요인의 증가로 현재보다 안전관리 수준이 떨어질 것이라는 지적도 많은 편이다. 지능정보기술이 바탕이 된 건축·시설물 안전관리가 설계-시공-관리-개·보수라는 전 과정에 걸쳐서 확산될수록 기존 건축·시설물의 안전관리 체계를 개선하거나 구축하기 위한 초기 비용이 늘어날 것이라는 것은 누구나 공감하는 부분이다. 또한, 지능정보기술을 지속적으로 진화를 거듭하고 있지만 건축·시설물 안전관리에 적용되는 기술 표준을 위한 법제의 제정·보완은 바로 이루어질 수 없는 상황에서 안전관리 시스템을 일관성 있게 유지하는 것은 쉽지 않은 일이라고 할 수 있다. 그리고 건축·시설물의 용도, 크기 등은 규격화 되어 있지 않아 지능정보기술을 적용한 안전관리의 표준화 마련도 어려운 실정이다. 더불어 도입된 지능정보기술 간에 호환되지 않는 기술들의 난립에 따른 어려움이 발생할 수 있어 이에 대한 준비도 필요하다. 전문가 인터뷰에서도 지적했듯이, 지능정보기술을 매개로 하여 연결되어 해킹이나

사이버 공격으로 인해 개인의 사생활 정보가 유출과 시스템 오류가 발생할 수 있기에 보안에 대한 대비가 필수적이다.

한편, 위험성 분석을 보면, 건축·시설물 안전관리의 전 과정에 제4차 산업혁명 시대의 지능정보기술 도입으로 긍정적인 변화가 이루어질 것이라는 의견이 있는 반면에, 오히려 지능정보기술의 오류나 외부 공격에 의한 위험요인의 증가로 현재보다 안전관리 수준이 떨어질 것이라는 지적도 많은 편이다. 즉, 건축·시설물 안전관리 분야에 지능정보기술(IoT, AI 등)이 적용되면, ① 지능정보기술 기반 시스템의 오류 발생, ② 개인정보보호 및 정보보안, ③ 시스템의 신뢰성 문제, ④ 기술 적용의 차별화 등을 언급했다. 전체적으로 건축·시설물 안전관리에 지능정보기술 도입으로 안정성과 대응성이 증대하지만, 시스템 오류나 해킹 및 바이러스 등에 의한 정보보안이나 개인정보 침해 등의 위험요인에 대한 우려가 있다.

4. 건축·시설물 안전관리체계의 리모델링 방향 도출

제4차 산업혁명 시대의 도래로 시설물 안전관리 부문의 급속한 변화가 있을 것으로 예측되고 있지만, 현행의 방식을 고수할 경우 시설물 안전 부문의 경우 그 위험성이 높아질 수 있다. 따라서 제4차 산업혁명을 선도하는 지능정보기술에 의해 초연결사회 혹은 환경이 조성되면서 새로운 접근방식이 절실해지고 있다. 따라서 안전관리의 추진 방향을 추진체계와 추진과제로 나누면 다음과 같다.

안전관리 추진체계의 측면에서 보면, 제4차 산업혁명 시대로 접어들면서 지능정보기술이 우리의 일상에 깊숙이 영향을 미치고 있다. 이러한 사회 전반에 걸쳐서 일어나는 패러다임의 변화는 기존의 상식을 뛰어 넘어 새로운 관점에서 모든 상황을 판단해야 하고, 광범위한 법제의 변화와 대비가 이루어져야 한다. 건축·시설물의 안전관리는 일상생활과 깊숙이 연결되어 있고, 어느 부문보다 안전관리가 중요한 분야이다. 지능정보기술의 순기능을 확대하고 역기능을 최소화하기 위해서는 안전관리를 담당하는 부처/부서 간, 정부-민간 기업 간의 긴밀한 협력 체계 구축이 필요하다. 또한 관리 시스템의 체계적이고 안정적인 관리를 통해 예측 가능한 리스크를 줄이는 노력이 이루어져야 한다. 종합하면, ① 안전관리 패러다임 변화에 대응, ② 부처/부서 간 협력체계 구축, ③ 안전관리 데이터 축적과 관리시스템 체계화 등이 필요하다.

한편, 추진 과제측면에서 볼 때, 현행 시설물 안전관리체계에는 IoT나 AI 등을 적용한 건축·시설물 안전관리에 관한 규정은 거의 없는 실정이기에 법제의 보완·정비와 함께 관련 기관의 역할 규정 등과 같은 안전관리 체계의 구축이 필수적으로 이루어져야 한다. 특히 지나치게 안전을 중시하는 건설 산업의 특성상 중앙정부 및 민간 기업에서는 신기술 도입에 대해 매우 보수적이기 때문에, 지능정보기술이 접목된 신기술을 신뢰할 수 있는 기관의 검증 및 정부 주도의 적극적인 도입이 함께 이루어져야 한다. 건축·시설물의 안전관리에 지능정보기술이 도입되어 안전성과 대응성이 높아지겠지만, 시스템 오류나 정보보안 등의 부정적인 요인들을 충분히 고려하여 법제와 시스템을 마련할 필요가 있다. 종합하면, ① 통합적 정보관리 시스템 구축, ② 시스템 관리 책임의 명확화, ③ 신기술 도입 등이 필요하다.

5. 건축·시설물 분야 안전관리체계 개선방안 도출

현재 많은 기업들과 정부기관들은 건축·시설물 안전관리 체계에 지능정보기술을 적극적으로 수용하려는 움직임을 활발히 보이고 있으나, 관련 법제나 관리체계가 새로운 기술적용과 관련하여 어떠한 판단을 내리기 어려운 상황과 직결되어 있다. IoT, AI, 그리고 빅데이터 같은 새로운 지능정보기술들의 진화는 지속적으로 이루어지고 있기에 특정 법률이나 제도를 마련하는데 한계가 있다. 따라서 건축·시설물의 안전관리 체계에 지능정보기술이 도입되고 있는 지금 법률의 제·개정과 함께 맞춤형 가이드라인을 우선적으로 제시하여 여러 가지 문제점을 보완하는 과정이 필요할 것이다.

첫째, 건축·시설물의 생애주기(설계-시공-관리-개·보수 단계)별 맞춤형 안전관리 체계를 마련하여 그 이용에 있어 최대의 효용을 창출하고, 건축물 및 시설물의 이용자가 안정적인 상태에서 활용하기 위한 대책이 필요하다.

둘째, 건축·시설물의 안전관리가 안정적으로 이루어지기 위해서는 이러한 지능정보기술을 도입할 수 있고 운용할 수 있도록 법제적인 뒷받침을 지속적으로 지원해야 할 필요가 있다. 제4차 산업혁명으로 인해 새롭게 등장한 지능정보기술들은 건축·시설물의 안전관리 체계의 틀을 바꾸어야 하는 큰 변화를 수반하고 있다.

셋째, 일관된 원칙과 시스템에 따른 정보 입수가 가능하도록 중앙정부, 지방자치단체, 그리고 관련 민간업체 등이 협력하는 체계가 요구된다. 전문가들이 지적했듯이 현재 건축물의 물리적·사회적 안전 수준 진단과 문제도 제대로 파악하지 못하는 실정에서 적용 가능한 신기술이 무엇인지, 적용 범위와 우선순위 등 세부 전략 수립이 불가한 것을 제대로 인식해야 한다. 따라서 IoT나 AI 등의 지능정보기술을 활용하여 시설물의 안전관리 체계를 새롭게 하기 위해서는 안전관리체계 거버넌스의 구성이 요구된다.

마지막으로, 다각적인 영향을 고려한 안전관리 체계의 구축이 요구된다. 현행 안전관리체계는 기술 중심의 안전관리체계로 지능정보기술의 도입으로 다양한 시작, 즉 사회경제적 측면까지 고려된 안전관리를 포함하지 못한다. 따라서 기술적인 측면뿐만 아니라 사회경제적인 측면까지 고려된 안전관리 체계 구축이 되어야 한다.

〈표 3-2〉 시설물 안전 : 스마트 빌딩 연구내용 요약표

문제점 및 위험성 분석	리모델링 방향	개선방안
[현행 체계 문제] - 대규모 건축물 중심의 안전관리 체계 - 통합 안전관리 체계 부재(개별법에 의한 안전관리) - 건축생애단계별 안전진표 및 점검 체계 미흡(관리 시점: 건축물 준공 이후 중심) - 사람 중심 안전관리체계(사람 거주 건축물과 비거주건축물의 분리) - 안전점검/진단의 결과 신뢰성 제고 및 자료 관리 내실화 필요(점검 기술자의 역량 부족, 안전관리 대상 시설물의 미등록 발생)	① 통합적 안전관리체계 - 안전관리 분야 간 연계 관리 - 소규모 건축·시설물을 포함한 안전관리 ② 생애주기별 안전관리체계 - 준공 전 단계를 포함하는 안전관리체계 - 노후화 관리 시스템 ③ 보안 강화 체계 - 보안 강화를 위한 신기술 도입 - 개인정보 보호 법·제도 강화 ④ 데이터 신뢰성 검증 체계 - 데이터 관리 시스템 구축 ⑤ 사람에 의한 관리체계 병행 - 안전관리 인력 확보 - 단계별 안전관리 가외성 확보	① 기술적 측면 - 보안 기술 개발 및 강화 - 기술 위험 관리를 위한 단계별 시범적용 후 제도화 - 대지 단위 건축물 관리를 위한 DB 구축 ② 의식적 측면 - 사람 중심 시설물 관리체계 구축 - 지능정보기술 적용 확대 및 위험성 관리를 위한 정부 전략 강화 - 지능정보기술 및 위험성에 대한 교육 ③ 제도적 측면 - 통합화된 안전관리체계의 책임 관계 명확화 - 현장 중심 분야 간 협력 체계 구축 - 시설물 안전관리 민간 역량 강
[지능정보기술 위험성] - 시스템 연계에 따른 연쇄적 사고		

문제점 및 위험성 분석	리모델링 방향	개선방안
- 정보 보안/ 개인정보 노출 위험 - 데이터 및 기술 신뢰성 - 인간에 대한 고려 배제(기술 중심 시설물) - 시스템 간 충돌 - 적절치 못한 기술 적용에 따른 위험		화(전문가 양성 등)

제4절 사회기반 안전(금융) : 블록체인

1. 금융 안전분야의 지능정보기술에 따른 영향 검토

핀테크 혁명의 촉매제가 된 분산화 시스템의 가장 중요한 핵심 기술은 암호 화키와 분산장부다. 은행 없이 개인 간(P2P) 거래가 활성화되면서 은행점포가 거의 사라질 수 있으며, 해외송금과 대출(클라우드 펀딩)도 블록체인을 기반으로 한 가상화폐를 활용해 실행이 가능해질 것이다. 이는 상당한 비용절감 효과와 투명성, 보안성 및 신속성의 제고, 그리고 금융포용(financial inclusion) 확대 등의 효과도 기대할 수 있게 한다. 클라우드 컴퓨팅 기술이나 빅데이터, 오픈 API 기술, 인공지능 등의 신기술도 금융권으로의 도입이 확산되고 있다.

사회기반(금융) 안전 분야에 지능정보기술의 적용 확대는 아래 8가지 변화를 가져올 수 있으며 각 변화상이 갖는 긍정적 측면과 부정적 측면은 다음과 같다.

첫째, 블록체인 등 분산시스템의 대두로 인한 신뢰토대 와해는 ① 투명하고 빠르게 금융 업무를 진행할 수 있음, ② 저비용으로 이용이 가능함 등의 긍정적 측면이 있으며, ① 금융 산업의 와해가 예상, ② 현재 실험단계이며 유지비용이 많이 듦, ③ 소비자 데이터 보호 문제가 대두될 가능성 있음 등의 부정적인 측면이 나타날 수 있다.

둘째, 가상화폐의 출현과 기존 통화의 변화에 대해서는 ① 금융중개비용 축소, ② 금융 포용성 확대 등의 긍정적 측면과 ① 통화정책과 경제정책에 어려움을 가중시킬 수 있음, ② 추적이 힘들, ③ 디지털 소외계층이 금융소외계층이 될

수 있음 등의 부정적 측면이 나타날 수 있다.

셋째, 빅데이터 기술, 고객 맞춤형 서비스 제공, 플랫폼 형성은 ① 많은 고객에게 맞춤형 금융 서비스 제공 가능, ② 고객 만족도 증가, ③ 신규 서비스 기업의 시장 진입용이 등의 긍정적 측면과 ① 개인정보 유출, ② 서비스 및 상품 내용이 복잡해지면서 이해도 저하 등의 부정적 측면이 있다.

넷째, 인공지능, 머신러닝 등의 산업분야 활용에 대해서는 ① 한계에 부딪혔던 분야에 대하여 극복 가능, ② 생산성 향상, ③ 인건비 절감 등의 긍정적 측면과 ① 소수 기업의 독과점, ② 고용 감소 등의 부정적 측면이 있다.

다섯째, 스마트 인증 및 새로운 기술 기반의 보안, 인증 방식의 제공은 ① 좀 더 편리한 인증시스템 등장 가능, ② 보안의 강화 등의 긍정적 측면과 ① 소비자 피해 보상 절차 및 관련 규정 보완 필요, ② 해킹의 위험성은 여전히 존재 등의 부정적 측면이 예상된다.

여섯째, 암호화기술 기반의 원산지증명, 재산권 및 등기등본 서비스에 대해서는 ① 신속하고 저렴한 비용으로 서비스 이용 가능, ② 위조, 변조 예방 등의 긍정적 측면과 ① 보안 강화 필요, ② 보편화가 힘들 등의 부정적 측면이 있을 수 있다.

일곱째, 다양한 금융서비스 출현은 ① 금융 혜택을 받지 못했던 사람들에게도 혜택 부여 가능, ② 경쟁에 따른 금융비용 절감 등의 긍정적 측면과 ① 금융산업 체계의 불안정성 및 큰 변화 예상, ② 시스템, 법 등 보완해야 될 부분이 많음, ③ 안정화에 시간 필요 등의 부정적 측면이 있다.

마지막으로 고객중심의 서비스 전달체계는 ① 금융산업의 성장, ② 고객의 접근성 및 만족도 상승 가능, ③ 양질의 서비스 제공 가능 등의 긍정적 측면과 ① 독과점 가능성 높음, ② 새로운 금융 리스크 발생 가능, ③ 규제 사각지대 출현으로 불법 금융거래 가능성 높음 등의 부정적 측면이 발생할 수 있다.

2. 금융 안전관리체계 현황 분석

과거의 금융 인프라는 전통적으로 중앙집권적인 특징과 비 암호화된 hub

and spoke³⁰⁾ 데이터베이스 구조를 가지고 있어 비용이 많이 들고 종종 사이버 공격에 노출되기도 했다. 그에 따라 금융안정을 위한 관리 비용은 지속적으로 늘어나고 자본요구량이 커지며 거래상대방, 운영, 사이버 공격 위험 등에 대한 기술적 관리부담도 기하급수적으로 늘어 왔다. 이는 복잡하게 얽혀진 네트워크의 특성상 위험요인이 증폭되는 데 비해 이를 관리할 수 있는 주체는 극소수인 중앙집권적 구조 때문으로 볼 수 있다.

초연결 환경이 자리 잡고 있는 4차 산업혁명시대의 금융 변화는 이와 같이 과거방식으로 전달되는 금융서비스의 제반 요소에 대해 본질적인 의문을 던지면서 변화를 촉구하고 있다. 이는 연결로 초래되는 시장구조의 변화, 시장참여자들의 행동방식, 변화된 인센티브 구조 등을 감안하면 더 이상 과거의 통제방식만으로는 대응하기 어려우며 점차적으로 분산구조를 수용하면서 진화할 필요가 절실했기 때문이다.

즉, 제4차 산업혁명 시대의 스마트 센서(Smart Sensor)는 다수의 민간이 그 역할을 담당해야 하지만, 우리의 시장 신뢰는 여전히 전통 인프라(legacy infra)와 기득권 위주로 편중되어 있다. 실제로 사회적 공감대 형성의 주도계층이 폐쇄적 자세를 견지하고 있으며, 개방과 협업에는 소극적인 자세를 취하고 있다.

게다가 감독기관은 지능정보기술(블록체인 등)을 기반으로 한 금융 산업이 전자기술을 활용한다는 점에서 현행 전자금융거래법에 적용하고자 하는데, 현재 우리나라 전자금융거래법은 중앙집중형 전산시스템을 기본으로 가정하여 설비 등 각종 규제들을 구체적으로 적시하고 있다. 따라서 이 법을 새로운 기술을 기반으로 한 금융 서비스에 적용하게 되면 법적 해석에 있어 적용대상, 전자자금 거래계약의 효력, 안전성 확보의 의무, 정보보호최고책임자의 지정, 전자금융기반시설 취약점 분석 및 평가 등과 관련된 다양한 쟁점사항들이 존재한다. 또한 개인정보보호법의 경우에도 각 부처별 소관의 다양한 개별법이 존재해 데이터를 활용하는 지능정보기술 발전에 장애물이 될 수 있다. 외국환 거래법의 경우도 전자적으로 화폐가 개인 간 자유롭게 이동할 수 있는 상황을 고려하지 않은 법체제로 앞으로의 신기술 적용 시 상충되는 부분에 대한 고려가 필요하다.

30) Hub-and-Spoke는 중앙(hub)에 외곽지점을 연결하는 스포크(spoke)의 시리즈로 구성된 교통 노선을 가리키는 말. 즉, 중앙집중식 모델을 의미함. 1955년 델타 항공이 이 방식을 통해 운송물류업계에 혁명을 일으켰고, 1970년대 후반 정보통신 기술 부문에도 채택됨(wikipedia).

블록체인 기술이라는 것의 핵심은 분산원장이고 제3의 신뢰기관이 필요 없는 것을 전제로 개인 간(P2P) 거래가 가능한 것이므로 중앙집권적 형태의 감독기관과 시스템은 블록체인과는 쉽게 조화되기 어렵다. 게다가 현행 금융 안전 관리 체계는 금융정책 및 감독 기구 간 역할 혼선 및 중복의 문제와 금융 감독의 독립성 및 중립성이 결여될 수 있다는 점, 소비자보호에 소홀해질 수 있다는 점 등의 문제가 제기되어 있다.

그럼에도 불구하고 현재 우리나라는 신기술에 대한 규제 방침을 명확히 하지 않고 있으며, 기존의 법을 바탕으로 신기술을 규율하고자 한다. 일례로 2016년 말 기획재정부에서는 핀테크 업체가 은행에 대한 의존 없이 독자적으로 해외 송금을 서비스할 수 있도록 '외국환거래법 시행령' 개정을 추진했다. 당시 정부에서는 자금세탁방지를 위한 외환전산망 보고의무 부과 및 고객확인 의무 요건 부과, 외국환거래법 개정을 통한 규율, 자본금 요건 및 전산설비와 전문 인력 등을 요구했다. 그러나 업계에서는 해외 송금업을 위해서는 해외 업체와의 파트너십이 중요한데 진입장벽을 높이면 등록이 어려울 것이고 파트너를 구하기 어려우므로 오히려 시장이 음성화될 가능성이 있다며 가능한 한 시장 진입장벽을 낮춰 공정한 경쟁을 유도해야 한다고 주장했다. 결국 자본금은 하향 조정되긴 하였지만, 핵심문제는 그것이 아니다. 송금서비스의 근간인 가상화폐의 법적 성격을 명확히 하여 국경을 넘을 수 있는 업무에 관한 법적 적용을 포괄적으로 이행하는 등의 노력이 필요한 것이다. 그러나 가상화폐에 관한 판단이나 각종 비트코인 거래소에 관한 규율방침은 여전히 오리무중이다. 게다가 분산원장을 기반으로 한 블록체인 기술을 금융권에 도입하려면 개인정보보호에 대한 부분도 새롭게 고려해야 할 것이다. 그러나 우리나라의 금융권 개인정보보호 규제 체계만 보아도 알 수 있듯이 현행 금융 안전 관리 체계는 굉장히 복잡한 양상을 띠고 있다.

전반적으로 볼 때 우리나라의 금융안정을 위한 행정체계는 그동안 정치적으로 발달해온 수직적(silo) 의사전달구조로 인해 초연결 환경의 위험요인에 대응하는 데는 근본적인 한계를 보일 수밖에 없는 구조이다. 물론 이러한 체계 자체가 다양한 법체계 기반 위에서 구현된 만큼 이를 변경하거나 개편할 수 있는 법적근거를 마련하는 것 자체가 쉽지 않은 것도 사실이다. 그러나 이러한 체제적인 효율성의 한계는 향후 점차 심각해질 것이 분명하기 때문에 환경변화에 걸맞은 유연한 조직과 체계로 진화하려면 상당한 준비가 선행되어야 한다.

3. 금융 안전 분야에 지능정보기술 적용 시 발생 가능한 위험성과 문제점

사회기반(금융) 안전 분야에 지능정보기술의 적용에 따라 기존 안전관리체계의 문제점은 기술을 따라오지 못하는 법, 제도, 규정과 제도 간 중복, 상충되는 부분, 그리고 규제완화에 대한 부분이 향후 안전관리에 큰 문제점이 있다. 그리고 신기술 적용으로 발생할 수 있는 위험으로는 지능정보기술에 대한 맹목적 믿음과 기술을 따라오지 못하는 법체계, 보안문제가 있다. 지능정보기술 도입으로 금융 분야는 전체적으로 발전을 하지만 그만큼 위험성도 커지고 있다고 하겠다.

구체적으로는 블록체인 기술이 확산될수록 체인 관리에 드는 비용이 급증할 수 있으며, 특정 서버(Server)가 해킹 등에 공격당할 경우 보안에 취약해질 가능성이 있다. 또한 여러 가지 블록기술들이 난립함에 따른 표준화 정착의 지연의 문제와 네트워크 상의 모든 참여자에게 거래 관련 정보가 공개될 수 있기 때문에 금융거래가 요구하는 보안성과 익명성과의 배치 가능성도 인식해야 한다. 블록체인 기술의 통화관리정책, 자금세탁 방지와 같은 금융안정 관련 제도 및 정책과의 상충 가능성과 이 외에도 불충분한 거래 처리 능력, 네트워크의 참여를 이미 검증된 사람들에게 국한시키기 어려운 한계, 알려지지 않은 네트워크 참여자들 간의 담합가능성, 결제의 최종성에 관련된 완전성이 미흡한 문제, 공감대형성도 확정하기 어려움 등은 여전히 남아있는 기술적인 문제다. 블록체인은 이중거래 방지에 탁월한 기능을 보유하고 있는 반면, 거래가 승인된 이후 취소가 불가능하게 설계되었다는 기술적 한계와 작업증명에 소요되는 재원이 과도하게 투입되어야 하는 한계도 존재한다. 또한 금융은 사소한 보안 사고만으로도 막대한 손실로 이어질 수 있는 특수 산업이라는 점에서 핀테크 서비스를 제공할 때는 보안을 우선 요소로 인식하는 것이 중요하다.

이 외에도 빅데이터 활용에 따른 프라이버시 문제도 제기되고 있으며, 오픈 API를 위해서는 오류 및 예외사항의 완벽한 처리, 다양한 운영체제 등 이질적인 전산환경에서의 호환성 검증이 필요하다. 또 인공지능을 금융 분야에 적용하였을 때에는 수익의 배분이나 법적 책임문제 등에 관한 논란이 있을 수 있다.

4. 금융 안전관리체계의 리모델링 방향 도출

가. 안전관리 거버넌스 변화 방향

우리나라의 행정시스템은 새로운 기술요인의 전면적 변화를 수용하기도 어렵고 점진적인 진화를 도모하기도 쉽지 않은 상황이다. 우리나라의 금융안정을 위한 행정체계는 그동안 정치적으로 발달해온 수직적(silo) 의사전달구조로 인해 초연결환경의 위험요인에 대응하는 데는 근본적인 한계를 보일 수밖에 없는 구조이다. 또한 관련법이나 규제체계가 정부부처별로 다기화 되어 있어 법적 허용 공간으로 진입하는 것 자체가 매우 어려운 상황이다. 이러한 체제적인 효율성의 한계는 향후 점차 심각해질 것이 분명하기 때문에 환경변화에 걸맞은 유연한 조직과 체계로 진화하려면 상당한 준비가 선행되어야 한다.

전문가를 통한 심층 인터뷰에 따르면 제4차 산업혁명 지능정보기술의 사회기반 안전(금융) 분야 적용에 대한 안전관리체계는 금융 산업의 발전을 위해 금융체계의 네거티브 전환이 필요하다. 또한 금융회사들이 업무수행의 유연성과 자율성을 발휘하고, 경쟁력을 증진시킬 수 있도록 원칙중심의 포괄주의체제를 도입하고 미래 금융 관리체계에 대해 정책적 목표의 확실성이 요구된다.

나. 사회기반(금융) 안전 분야 안전관리 대응 전략

앞으로의 문제는 미래로의 전환과 현 시스템의 조화를 어떻게 이루어낼 것인가이며, 이는 결국 정책노력이 아닌 구성원과 시장의 움직임에 따라 결정될 것으로 보인다. 지능정보기술의 보다 광범위한 적용 과정에서 소위 와해와 재구성을 통해 새로운 질서와 공동체 형성이 이루어질 것이다. 이 과정에서 사회구성원들은 디지털 변화에 대해 바른 식견과 판단, 그리고 건전한 의식을 가지고 대응해야 할 것이다. 또한 현 금융시스템 인프라가 제공하는 처리능력을 블록체인 기술도 제공할 수 있는가의 문제에 대해서도 고민해 보아야 한다.

최근의 패러다임 변화(제4차 산업혁명, 지능정보기술 등의 출현)에 대응하여, 우리나라 사회기반(금융) 분야 안전관리 추진체계와 관련한 대응전략은 ① 국제적 경쟁력을 갖추기 위해서는 시대 흐름에 맞는 규제 필요, ② 관련 부처의 협업 필요, ③ 소비자 보호를 위한 포용적 금융 확대(기술발전에 따른 미래 금융 불평등 해소) 필요, ④ 자발적 조정기능을 통한 정부의 개입 최소화, ⑤ 관리체계 개선 등이 있다.

5. 금융 분야 안전관리체계 개선방안 도출

블록체인 기반 위의 사회기반(금융) 안전 분야 안전관리는 금융 분야 고유의 수직 조직과 각종 규제나 법률의 차이로 인해 상당기간 분열된 양상이 개별적으로 이루어질 가능성이 높다. 그러나 미래의 위험요인들은 그 자체가 복잡적이고 다양한 요소를 내포하고 있으므로 대응체제도 가급적 분산되고 탈중앙화된 방향으로 진화하는 것이 중요하다. 이를 수용하고 촉진할 수 있는 행정체제는 개방형과 참여형의 특징을 모두 가져야 하지만 지배구조상 컨트롤 타워 역할을 다른 방식으로 전가시키거나 분산시키기 어려운 특징을 가지고 있다. 따라서 우리는 기존 레거시(legacy infrastructure)와의 조화로운 운영 내지 발전적 진화의 이슈를 어떻게 해결해 나갈 것인지에 대한 준비가 필요하다.

먼저, 우리는 중앙집중형, 수직적 법 규제를 4차 산업혁명 분산 시스템에 어울리게 정비해야 할 필요가 있다. 그렇지 않으면 기존 법과 와해성 특징을 가진 신기술과의 상충 문제가 계속해서 발생할 것이다. 즉, 우리는 법령에서는 원칙만 제시하고 하부 기관들이 수시로 개정할 수 있는 지침(guidance) 형태로 제정하여 운영하는 방안을 고려해야 하며, 네거티브 접근 방법과 사후 규제를 통해 감독과 규제 업무를 수행할 수 있는 방안을 강구해야 한다. 이는 당장에 실행 가능한 것이 아니므로 기술의 위험성과 가능성, 그리고 그에 적합한 규제를 알기 위해서라도 샌드박스(sandbox) 등을 활용한 파일럿식 접근(pilot approach)이 필요할 것으로 보인다.

둘째, 미국의 경우 금융사고 전문가(PCI Forensic Investigator)를 육성하고 있는데, 우리도 금융사고나 개인정보유출 등에 따른 보안사고에 대비해 보다 체계적이고 근본적인 시스템 마련과 전문가 양성이 필요할 것으로 보인다. 지능정보 기술을 활용한 금융 시스템은 디지털 기술을 활용하는 것으로 해킹 등의 위협에서부터 자유로울 수 없고 따라서 더욱더 철저한 사고 대비와 사고 처리가 필요할 것이기 때문이다.

셋째, 블록체인 기술을 금융 위험의 파악과 관리에 적극 활용하는 방안을 고려해보아야 한다. 블록체인은 행정정보 공동이용 기반 조성, 기관 간 협업 확대, 공공서비스 인증, 공공데이터 거래 등에 활용할 수 있다. 또 블록체인 기술은 효

율적인 운영, 즉각적인 서비스, 향상된 데이터 보안 등의 제공도 가능하다. 이외에도 다양한 위험들의 연관은 빅데이터와 AI 등을 동원하여 파악할 수도 있다. 이렇듯 기술을 규제 감독에 활용하는 것을 레그테크(RegTech)라고 하는데 이를 시스템 모델 구축과 시나리오 분석 및 예측, 데이터 수집, 고객 신원정보 확인, 금융 시스템 감시 등에 사용함으로써 준법감사 업무를 효율적으로 처리할 수 있으며, 금융 안정에도 기여할 수 있을 것이다.

넷째, 금융안정을 위해 글로벌 차원의 위험관리 통제센터 네트워크 연계 및 공동 활용 방안도 고려해볼 수 있다. 앞으로 국민안위에 영향을 주는 요인들을 개별 관리하는 것은 불가능하므로 국내 및 역내 차원의 위험관리 통제센터 간의 네트워크를 구축하여 국가별 관리와 역내 차원의 조치가 유기적으로 이루어질 수 있도록 하는 방법도 있을 것이다.

〈표 3-3〉 사회기반(금융) 안전 : 블록체인 내용 요약표

문제점 및 위험성 분석	리모델링 방향	개선방안
[현행 체계 문제] - 금융정책 및 감독 기구 간 역할 혼선 및 중복의 문제와 금융 감독의 독립성 및 중립성이 결여 - 관련법이나 규제체계가 정부부처별로 다기화 되어 있음. - 전통 인프라와 기득권 위주의 폐쇄적 자세, 개방과 협업에 소극적 - 소비자 보호에 소홀할 가능성 - 화폐가 전자적으로 개인 간 자유롭게 이동할 수 있는 상황을 고려하지 않은 법체제로 앞으로의 신기술 적용 시 상충되는 부분 존재 - 그럼에도 불구하고 신기술에 대한 규제 방침을 명확	① 연결을 상정한 여건에 적합한 대응 체계를 구축 - 블록체인 기반의 자발적 대응여건 마련 - 모니터링을 통한 규제 감독과 익명성이라는 블록체인 고유의 특징을 조화시킬 방안 고려 ② 개인프라이버시를 해치지 않으면서 데이터의 광범위한 활용을 통해 사회구성원들의 효용을 증진 - 데이터 기술의 발전 필요 ③ 법·제도 및 감독체계의 정비 - 변화 방향에 부합하고 와해비용을 최소화하는 방향을 모색 - 이해관계자(Stakeholders)의 합의는 매우 중요 - 기존 레거시(legacy infrastructure)와의 조화로운 운영 내지 발전적 진화 ④ 민간주체들이 정책방향에 대해	① 기술적 측면 - 블록체인 분산기술 및 빅데이터, AI 등을 금융 위험의 파악과 관리에도 적극적으로 활용 - 시스템 모델 구축과 시나리오 분석 및 예측, 데이터 수집, 고객 신원정보 확인, 금융 시스템 감시 등에 레그테크(Regtech)를 사용 - 금융 안정을 위해 글로벌 차원의 위험관리 통제센터 네트워크 연계 및 공동 활용 방안도 고려 ② 의식적 측면 - 사회구성원들의 다양한 실험과 관심을 통한 공감대 형성 - 국가는 개방플랫폼의 역할을 강조하면서 포괄적이며 안전한 서비스를 제공 ③ 제도적 측면 - 법령에서는 원칙만 제시하고 하부 기관들이 수시로 개정할 수

문제점 및 위험성 분석	리모델링 방향	개선방안
히 하지 않고 있음. - 환경변화에 걸맞은 유연한 조직과 체계로 진화 필요 [지능정보기술 위험성] - 체인 관리에 드는 비용 급증 가능성 - 해킹을 통한 피싱(Phishing), 사기, 정보 탈취 등으로 손실 발생 우려 등 보안 문제 - 여러 가지 블록기술들이 난립함에 따른 표준화 정착의 지연 가능성 - 금융거래가 요구하는 보안성과 익명성과의 배치 가능성 - 불충분한 거래 처리 능력, 네트워크의 참여자 검증의 문제, 네트워크 참여자들 간의 담합가능성, 완전성이 미흡한 문제, 공감대형성도 확정하기 어려움 등 기술적인 문제 - 거래가 승인된 이후 취소가 불가능하게 설계되었다는 기술적 한계 - 프라이버시 문제 - 인공지능을 금융 분야에 적용하였을 때에는 수익의 배분이나 법적 책임문제 등에 관한 논란 - 금융안정 관련 제도 및 정책과의 상충	자발적으로 원활하게 준비할 수 있는 여건 형성 - 정부는 직접적으로 개입하지 않으면서 필요한 자발적 조정노력을 원활히 구현할 수 있도록 제반 여건을 점검	있는 지침(guidance) 형태로 제정하여 운영하는 방안 - 샌드박스(sandbox) 등을 활용한 파일럿식 접근(pilot approach) - 네거티브 접근 방법, 사후 규제 - 금융 사고나 개인정보유출에 따른 보안 사고에 대한 보다 체계적이고 근본적인 대응을 위한 전문가 양성 및 시스템 마련

제5절 소결

교통안전, 시설물안전, 사회기반 안전(금융)의 세 분야 모두 지능정보기술의 도입에 따른 안전 관련 공통의 문제 해결과 향후 효과적인 대응을 위해 다음과 같은 정책적 노력을 기울여야 할 것으로 판단된다.

첫째, 새로운 기술의 성공적인 도입 및 활용을 위하여 관련 법·제도를 적시성 있게 마련함은 물론, 기술변화 내용을 모니터링하면서 필요한 내용을 지속적으로 수정·보완해 나가는 노력을 추진해야 할 것이다. 이와 관련하여, 현재 존재하는 다수의 관련 법령들과 새롭게 제정하는 법령 간에 내용상의 불일치 및 상충이 없도록 명확하게 조정해 나가는 노력도 병행해야 할 것이다.

둘째, 새로운 기술의 도입으로 인한 영향요인을 고려한 효과적인 안전관리와 관련하여 관련 법·제도를 통해 권한과 책임을 부여받은 기관들 간의 유기적인 협업을 기반으로 한 통합적인 안전 거버넌스를 구축하고 운영해 나가는 노력이 요구되고 있다. 이에 잘 대응하기 위해서는 관련 법·제도를 통해 관련 기관들에게 명확한 권한과 책임의 부여되어야 하며, 원활한 협업을 이끌어 낼 수 있는 다양한 유인기제를 마련해야 할 것이다. 또한, 협력은 반드시 신뢰를 기반으로 하는 만큼 국가와 사회 내 구성원 간에 신뢰를 제고시키기 위한 지속적인 노력을 추진해야 할 것이다.

셋째, 제4차 산업혁명의 출현과 지능정보사회의 진전과 같은 거대한 시대적 조류를 잘 헤쳐 나가기 위해서는 무엇보다도 지식과 전문성을 갖춘 전문 인력의 양성이 중요한 과제라고 할 수 있다. 따라서 중장기적 차원에서 이들 세 분야에서 창의적이고 발전적인 아이디어를 기반으로 한국사회의 변화관리를 이끌 미래 인재의 발굴 및 육성을 위한 투자와 노력을 집중해야 할 것이다.

넷째, 기술의 고도화 및 지능화에 따라 모든 사물과 인간이 연결되는 초연결성 사회를 맞이하면서 생활의 편리성이 향상되는 긍정적인 면도 있지만, 그 이면에는 해킹 등으로 인한 정보 및 데이터 유출, 사생활 침해, 데이터의 위·변조 등과 같은 안전을 위협하는 부정적인 요소도 늘어나고 있다. 따라서 이들 세 분야에서 엄청난 규모와 속도로 생성 및 축적되는 데이터와 정보를 안전하게 관리하여 개인과 기관이 편리하고 안전하게 지능정보사회의 혜택을 누리면서 생활할 수 있도록 정부가 정책적인 노력을 기울여나가는 것도 중요한 과제라고 할 것이다.

제4장 법·제도 중심으로

제1절 개요

본 장에서는 협동 연구 기관인 한국법제연구원에서 “지능정보사회를 대비한 안전관리체계 리모델링에 관한 연구 - 법·제도 중심으로”라는 주제로 작성한 제4권의 내용을 요약 정리한다.

1. 추진 배경

AI, 빅데이터 등 신기술에 의한 변화요구에 적극적으로 대응하고 국민들이 믿을 수 있는 정보를 보다 안전하게 활용할 수 있는 사회 기반시설의 구축이 요구되고 있다. 신기술의 사용과정에서 발생하는 위험으로부터 안전할 수 있도록 새로운 관점에서의 안전관리체계 구축을 위한 연구 수행이 필요하다. 특히, 법·제도 관점에서 지능정보기술 적용 시 예상되는 주요 법적 이슈 및 쟁점 분석이 필요한 상황이다.

기존의 안전관리체계는 최근의 기술변화를 반영하지 못하고 있다. 이에 새로운 관점에서의 거시적 측면에서의 안전관리체계의 구축과 함께 지능정보 등 신기술이 반영으로 인한 사회 분야별 변화 예측이 필요하다. 또한, 이를 반영한 분야별 안전관리 체계의 리모델링이 시급한 상황이다. 즉, 지능사회로의 패러다임 전환과정에서 국민의 안전을 확보·강화하는데 파급효과가 클 것으로 예상되고 시급성이 인정되는 교통 안전, 시설물 안전, 사회기반(금융) 안전에 대한 안전관리체계의 개선에 대한 법·제도 관점에서의 연구가 필요하다.

교통 안전 분야의 경우 자율주행차의 등장으로 새로운 교통수단이 빠르게 상용화가 진행되고 있다. 이뿐만 아니라, 무인 이동체의 활용도 급속히 증가하고 있어서 기존의 교통안전 체계의 한계가 나타나고 있다. 이에 새로운 기술을 반영한 법·제도의 개선과 교통안전 관리체계의 구축이 요구되고 있다.

시설물 안전 분야의 경우 인공지능을 활용한 클라우드 컴퓨팅기술에 다양한 ICT 기술들을 접목한 스마트 빌딩이 등장하고 있다. 시설물을 관리하면서 국민이 더욱 안전하게 생활할 수 있도록 신기술을 반영한 법과 제도의 개선이 필요

하다. 이를 반영한 시설물 분야 안전관리체계의 구축 마련이 시급한 상황이다.

사회기반(금융) 안전 분야의 경우 비트코인의 등장으로 블록체인(blockchain) 등 신기술의 활용에 대한 사회적 관심이 커지고 있다. 암호화폐 규제에 관한 찬반논란이 증폭되고 있으나 이에 대한 제도적 연구가 미흡하다. 이에 기존의 금융 분야에 대한 안전관리 체계의 한계가 발생하고 있다.

2. 연구의 목적

자율주행차, 스마트 빌딩, 블록체인 등의 신기술로 인해 발생하는 교통 안전, 시설물 안전, 사회기반(금융) 안전 등의 분야에서 안전관리체계에 대한 법·제도 관점에서의 리모델링 방향을 제시한다.

첫째, 자율주행자동차에 대한 사회적 관심이 매우 높고 자율주행 기술도 급속하게 발달하고 있어서 곧 상용화를 앞두고 있다. 하지만, 도입에 따른 법적 허용성과 안전문제, 사고 발생 시의 책임과 처리 방법 등에 대해서 검토해야 할 과제가 산적해 있다.

교통안전 분야를 법·제도 관점에서 기존의 안전관리체계 및 입법사례 분석을 통하여 도출된 문제를 해결하고, 향후 효과적인 대응을 위해 요구되는 변화 관리 방향을 제시한다. 또한, 법·제도 차원에서 신기술을 기반으로 하는 자율주행차의 제조단계에서의 품질 관리, 제품의 사용 및 이용 과정에서의 안전사고 등 안전관리체계의 법·제도적 개선을 위한 장·단기적 추진 방안을 제시한다.

둘째, 지능정보기술이 시설물 안전 분야에 미치는 영향을 분석하고, 지능정보기술의 활용 단계와 이를 반영한 스마트 빌딩 등 새로운 시설물의 현황, 현행 시설물 안전관리체계 등을 조사·분석한다. 이 결과를 바탕으로 시설물 안전관리정책 및 제도의 문제점을 제시하고, 국외 건축·시설물 안전관리체계 및 입법사례 분석을 통하여 지능정보기화 사회에 적합한 건축·시설물 안전관리체계 구축 방안을 제시한다.

스마트 빌딩에 대한 산업적 관심이 매우 높고 인공지능과 빅데이터 등 신기술도 급속하게 발달하고 있어서 이에 대한 상용화 논의가 활발하다. 하지만, 기술에 대한 지원과 안전문제, 스마트 빌딩에 대한 관리와 사고발생시의 책임과

처리 방법 등에 대해서 검토해야 할 과제가 있다. 시설물 안전 분야를 법·제도 관점에서 기존의 안전관리체계 및 입법사례 분석을 통하여 도출된 문제를 해결하고, 향후 효과적인 대응을 위해 요구되는 변화관리 방향을 제시한다.

셋째, 블록체인 등 신기술을 기반으로 하는 비트코인 등 암호화폐가 등장함에 따라 기존의 금융 분야에 대한 안전관리 체계의 한계가 발생하고 있다. 이에 신기술 사회를 대비한 금융 분야 안전관리 체계의 구축이 필요하다.

블록체인 등 신기술이 활용한 암호화폐가 금융 분야에 미치는 영향을 분석하고, 신기술의 활용 단계와 이를 반영한 암호화폐의 현황, 현행 금융 분야 안전관리체계 등을 조사·분석하여 금융 분야 안전관리정책 및 제도의 문제점을 제시한다. 또한, 해외 금융 분야 안전관리체계 및 입법사례 분석을 통하여 지능정보 사회에 적합한 금융 분야 안전관리체계의 구축방안을 제시한다.

제2절 교통 안전 : 자율주행차

자율주행차의 등장에 따른 교통 안전관리체계의 법·제도 관점에서 리모델링 연구 다음과 같은 내용을 포함한다. 우선 자율주행차의 개념과 현재 자율주행차의 상용화 추이, 상용화에 따른 안전관리 문제를 제기한다. 이후, 자율주행차의 법적 허용 여부, 자동차 관리법·도로교통법 등 현행 자동차 안전관리 법률 개관, 자율주행차 안전관리 조직체계 및 정책 동향 등을 분석한다. 다음으로 자율주행차 상용화에 따른 분야별 법적 과제를 제시하고, 미국, 영국, 독일, 프랑스, 일본 등 해외 주요 국가의 자율주행차 안전관리제도를 조사 및 분석하여 시사점을 도출한다. 마지막으로, 현행 자율주행차 안전관리체계의 한계를 인식하고, 제도적 개선을 위한 법·제도 관점의 리모델링 방향을 제시한다.

1. 현행 교통 분야 안전관리체계 조사 및 분석

재난안전 관리체계의 기본법인 ‘재난 및 안전관리 기본법’ 등 관련 법률상의 교통안전 분야에 대한 안전관리 체계를 분석한다. 자율주행의 제조과정에서의 기술적 결함 등 제조공정상의 품질 등 안전관리와 개인 교통수단의 취득과 실제 도로에서 주행하는 과정에서의 운전면허제도와 차량보험제도, 대중교통 수단의 이용과 관련한 도로교통 체계상의 안전관리제도를 주된 연구대상으로 한

다.

자율주행차 안전관리제도 관련 법령에 대한 검토로 자동차관리법, 도로교통법, 제조물책임법, 자동차손해배상보장법, 보험법 등 기존 자동차 안전관리 관련 법령에 대한 검토를 수행하였다. 자율주행차의 관리에 대한 개별 법률은 아직 없는 상황이며 2016년 자동차관리법을 개정하여 자율주행차에 대한 근거 규정을 마련하였으나 향후 추가적인 관련 법률에 대한 정비가 필요한 실정이다.

2. 자율주행차 등 지능정보기술의 상용화 과정의 문제점

인공지능 등 신기술을 기반으로 하는 자율주행차의 제조과정에서의 기술적 결함, 운행 과정에서의 안전사고 등 많은 법적 문제가 발생할 우려가 있다. 행정적 절차로는 자율주행차가 인공지능 기술 등 신기술을 기반으로 하고 있어서 기존의 자동차 사용을 위해 필요한 운전면허시험과 발급 등 운전면허제도의 변화가 필요하고, 책임보험 등 차량보험제도 등 안전관리 체계의 리모델링이 요구된다.

3. 자율주행차 관련 해외 주요국 교통 안전관리체계

미국, 일본, 독일, 프랑스 등 주요 국가의 자율주행기술의 교통 분야 활용 현황과 자율주행차의 안전한 이용을 위한 안전관리제도 정비 현황을 살펴보면, 국가마다 다소 차이가 있으나 아직 자율주행차를 규율하는 개별법은 없는 상황이다.

가. 미국

미국에서 자율주행자동차에 관한 안전관리제도는 현재 미국의 법률 및 규제 체계에 맞추기 어려운 문제를 안고 있다. 왜냐하면, 연방 교통부가 자동차가 어떻게 만들어져야 하는지(에어백, 안전벨트, 크럼플 존 등) 그 기준(연방자동차안전기준)을 제시하여 관리하고, 주는 이러한 기준에 따라 만들어진 자동차의 운행과 관련한 사항(등록, 자격부여, 보험, 교통법, 안전점검 등)을 규제하는 시스템이다. 이처럼 이원화된 규제체계에서는 자율주행차에 대한 통일적 관리가 어렵다.

연방 차원에서는 자율주행자동차의 안전한 개발을 위한 고속도로교통안전위원회(National Highway and Transportation Safety Administration, NHTSA, 이하 “NHTSA”)의 지침(가장 최근의 것이 2016년 9월) 이외에 통일된 법이 별도로 존재하지 않는 상황에서 주마다 각기 다른 자율주행자동차의 시험과 실제 주행에 관해 각기 다른 목적, 정의와 우선순위로 혼재된 규제를 운영하는 상황이었다.

이러한 상황에서 2017년 7월 27일, 주법의 적용을 자율주행자동차의 안전에 관한 규정의 적용을 선점(preemption)하고 NHTSA가 새롭게 제정될 안전 규제를 할 권한을 부여하는 자율주행법(Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act, 또는 Self Drive Act)이 하원의 에너지 및 상업위원회(Energy and Commerce Committee)를 통과하여 2017년 9월 6일, 여야의 합의로 하원을 통과하여 상원에 회부된 상황이다. 만약 양원을 통과한다면 자율주행자동차에 관한 주법의 개별 규제에는 제동이 걸리게 될 것으로 보인다.

나. 영국

영국 정부는 자율주행차 기술 발전의 미래를 실현하기 위한 법·제도적인 환경을 조성하는 데 있어서 적극적인 노력을 기울이고 있다. 세계 어느 나라보다 자율주행차의 개발이나 운영을 자유롭게 시도할 수 있는 규제 환경을 갖추겠다는 목표를 세우고 있다. 이를 통해 자율주행차 관련 기술의 발전에 있어서 우위를 점하겠다는 확고한 의지를 보여주고 있다.

법·제도적 측면에서는 자율주행차의 시험운행이나 자율주행차의 안전한 운영을 담보할 수 있는 법·제도적 기반을 마련하고, 형사상 및 민사상 책임을 배분하는 타당한 근거를 제공하기 위하여 법률에서 추가적인 기준을 마련하는 계획을 밝히고 있다. 이는 자율주행차의 안전성에 관한 요건, 자율주행차가 유발한 사고를 둘러싼 책임의 배분 등이 향후 자율주행차의 상용화에 있어서 법적으로 해결해야 할 가장 핵심적인 과제가 될 것을 보여주는 것이다.

현재의 제한적 자율주행 단계에서 영국은 전국의 공공도로에서 자율주행차의 시험운행이 큰 어려움이 없이 이루어질 수 있도록 관련 법제를 탄력적으로 운용하면서 흥미로운 기술 발전의 미래를 실현하는 데 법·제도적인 환경을 조성하

는 데도 적극적인 노력을 하고 있다.

다. 독일

현재 자율주행차와 관련된 독일의 기술 수준에서는 제한된 영역과 특별한 상황에서만 주행 기능이 자동화된 시스템으로 전환될 수 있는 것으로 보인다. 우리나라에서는 지금까지 자율주행차의 시험운행을 위해서 자동차관리법, 같은 법 시행령, 같은 법 시행규칙을 개정하였고, 도로 및 도로교통 관련 법제의 개정은 이루어지지 않았다. 이와 달리 독일에서는 도로교통 관련 법제의 개정을 통해 해결하고 있다.

최근 독일은 도로교통법을 개정하여 자율주행차에 대한 규정을 신설하였다(2017년 6월). 도로교통법(StVG)상 자율주행차의 법제화는 자율주행차 유형 및 발전 단계에 관련 민·관·학간 합의를 통해 이루어졌다는 점에서 의미가 있다. 개정 법률은 고도 또는 완전 자율 주행 기능 자동차를 정의하면서 요구되는 기술적 장비를 명시하여 자율주행차의 개념요소를 마련하였다. 독일은 법률에 대한 입법평가를 하고 있어서 도로교통법 제1c조에 따르면, 자율주행차에 관한 기술이 빠르게 발전하고 있음을 고려하여 2년 후인 2019년 이 법률의 검토를 하여 개정할 것을 법률에 명시하고 있어 향후 추가적인 법률의 개정될 것으로 예상된다.

라. 프랑스

프랑스는 자율주행차의 도입을 새로운 산업육성 차원에서 접근하기보다는 도로교통의 안전과 에너지 효율을 높이는 측면에서 접근하고 있다. 여기에 탄소 배출 저감을 위한 장기적인 대안으로서 자율주행차를 고려하고, 장애인 및 노령자와 같이 대중교통 접근이 어려운 사람에 대한 편의 제공 등 공익적 측면에서 자율주행차 상용화에 대한 정책적인 노력을 기울이고 있음을 알 수 있다.

자율주행차의 운행에 따른 안전을 확보하기 위한 법·제도적 측면에서 보면 ‘성장을 위한 에너지전환 법률’ 제37조에서 법률명령에서 실험 목적의 개인용 자동차, 화물운송 자동차 또는 대중교통 수단의 자동화에 대한 규정과 이용자의 안전을 보장하기 위한 조건 및 필요한 경우 적절한 배상책임에 대하여 규정할

것을 명시적으로 요청하였다. 그러나, ‘공공도로에서의 자율주행차 시험운행에 관한 오르도낭스’는 자율주행 시험운행 허가에 대한 근거 규정만을 두고 허가 요건 및 적용 조건에 대해서는 여전히 규정이 모자란 상황이다. 즉, 어떤 이유에 선지 충분한 입법을 하지 못한 것이다. 그런데도, 동 오르도낭스가 총 4개 조항을 규정된 것을 고려할 때 동 오르도낭스에서 자율주행차의 시험운행에 대한 주무부서를 수상, 기후에 관한 국제관계를 담당하는 환경·에너지·해양 장관, 내무부 장관으로 명확히 규정한 점은 안전관리체계의 법적 근거를 마련하였다는 점에서 의미가 있다.

마. 일본

일본의 경우 자동차 산업은 관련 산업을 포함하여 500만 명이 넘는 고용을 창출하는 등 국가를 대표하는 산업이다. 따라서 자율주행차에 대한 일본의 접근은 적극적라고 볼 수 있다. 2015년을 기점으로 일본 정부는 아베노믹스가 2단계에 진입한 것으로 판단하고, 도쿄올림픽에 맞춘 민관 협력 프로젝트인 ‘개혁 2020’을 개정하여 성장 전략으로 채택하였다. 그 중 차세대 도시 교통 시스템 및 자동 주행 기술의 활용은 6개의 프로젝트 중 하나로 설정하여 자율주행 기술을 활용하기 위한 정책지원에 나서고 있다.

동시에 자율주행차의 등장으로 나타날 안전문제 등 자동차의 안전관리제도에 체계적 접근을 하고 있다. 이미 2013년 도요타 자동차가 자율주행의 실험상황을 공개하였을 때 운전자가 핸들을 잡고 있지 않은 것이 문제가 되자 정부에서는 국토교통성의 오토파일럿시스템에 관한 검토회 및 경제산업성의 자율주행 비즈니스 연구회 등을 조직하여 정부 스스로 자율주행에 대한 안전관리 문제를 검토한 바 있다.

또한, 일본의 경찰청은 핸들이나 브레이크를 조작하지 않아도 주행이 가능한 자율주행차의 법률상 문제 및 일반 도로 실험 가이드라인 작성에 대한 협의 등을 실시하는 검토위원회를 설치하여 도로교통법 개정 등의 법령 정비를 진행하기 위해 자율주행에 대한 사고 발생 시의 책임 소재 등 법적인 문제 발생 및 과제 도출을 통한 가이드라인을 만들었다. 특히 이를 위해 자율주행의 제도적 과제 등에 관한 인터뷰 조사를 하고 이를 참고로 심층된 논의를 거쳐, 현재 일본에서의 자율주행 시스템에 대한 법적·운영상의 과제를 선정하여 이를 연구하고

안전관리제도 개선에 반영하고 있다. 여기에는 자율주행차의 운행으로 인한 형사상의 책임, 행정법규상의 의무, 민사상의 책임, 기타 문제 등을 다루고 있다.

이처럼 일본은 자율주행차의 등장으로 나타날 여러 법적 문제를 안전관리제도의 체계 속에서 정부가 지속적이고 체계적인 조사와 개선에 앞장서고 있다는 점에서 시사하는 바가 크다.

4. 법·제도 관점에서의 교통 안전관리체계 구축 방안

교통안전의 경우 자율주행차의 등장으로 새로운 교통수단이 빠르게 상용화가 진행되고 무인 이동체의 활용도 급속히 증가하고 있어서 이 보고서에서 연구한 다른 분야들보다 기존의 교통안전 체계의 한계가 나타나 신기술을 반영한 법·제도의 개선이 시급하고, 그에 대한 연구도 가장 많이 진행된 상황이다. 향후 제도개선과 관련하여 자율주행차 운행상의 책임의 명확화, 차량 이용에 대한 규제 개혁, 자율주행 시스템의 안전성 제고, 보험제도 개편 등에 대해 제언한다.

첫째, 자율주행차 운행상의 책임을 명확화하여야 한다. 자율주행차의 운행으로 교통사고가 발생할 경우 운전자나 제조사, 소프트웨어 개발자 등 관련 당사자의 형사상 및 민사상 책임을 둘러싸고 매우 복잡한 문제가 발생할 수 있다. 여기서 운전자의 기대가능성, 제조상의 부주의, 기술적 한계 등이 주된 쟁점이 될 수 있다. 그러나, 현행 법적 체계 아래에서는 법원이 그러한 점에 대해 개별 사안마다 다르게 판단할 수밖에 없다. 따라서 형사상 및 민사상 책임을 배분하는 타당한 근거를 제공하기 위하여 법률에서 추가적인 기준을 마련하여 책임의 명확성을 높여야 한다. 또한, 향후 운전자가 탑승하지 않은 상태에서 운행하는 완전 자율주행의 단계에서 발생할 수 있는 책임의 문제를 해결하기 위한 입법적 조치도 마련하여야 한다.

둘째, 차량 이용에 대한 규제의 개혁이다. 현행 법령에서는 차량이 어떻게 이용되고 유지되는지 규율하는 데 주안점을 두고 있다. 이러한 법령의 체계는 시험운전자 없이 자율주행차 기술의 사용을 허용하고 그 기술이 정확하게 유지되도록 보장하기 위하여 개정될 필요가 있다. 예컨대 도로에 대한 적합성을 점검하기 위한 자동차안전검사(MOT) 테스트에 대한 개선과 자율주행차 기술의 일부를 포함하기 위해 도로교통법의 개정이 있어야 할 것이다.

셋째, 자율주행 시스템의 안전성 제고이다. 도로교통에 있어서 안전성은 무엇보다도 가장 중요한 요소이다. 따라서 일반적인 운전자에게 기대되는 것보다 얼마나 더 고양된 수준의 ‘운전’이 자동화된 모드에서 작동되는 차량에 요구되어야 하는지에 대한 분석과 연구가 선행되어야 한다. 또한, 자율주행차가 잠재적인 사이버 위협으로부터 보호되게 하려고 강력한 법적 장치를 마련하고, 자율주행차에 더욱 엄격한 기술기준을 적용하여야 한다.

넷째, 보험제도의 개편이다. 앞서 검토한 바와 같이 자율주행차도 제3자에 대한 책임보험의 가입이 의무화되어야 한다. 하지만 그러한 자동차보험으로는 자율주행시스템의 결함이나 오작동 또는 외부의 해킹으로 인하여 발생한 사고에 대해서까지 감당하기 어렵다. 따라서 자율주행차의 운행 중에 발생할 수 있는 특수한 사고에 대비하기 위하여 새로운 보상 기준을 갖춘 별도의 보험체계가 필요하다. 이와 관련하여 국토교통부에서 보험제도에 대한 개선을 준비 중이나 운전자의 보험가입이 의무화되어 있는 현행의 제도를 확대하여 자율주행차의 소유자에 대한 보험 가입도 고려하여야 한다.

제3절 시설물 안전 : 스마트 빌딩

스마트 빌딩의 등장에 따른 시설물 분야 안전관리체계의 법·제도적 리모델링 연구는 다음과 같이 구성된다. 우선, 스마트 빌딩 개념과 특징, 현재 상용화 추이, 상용화에 따른 안전관리 문제를 제기한다. 이후, 스마트 빌딩에 대한 법제 정비의 필요성과 건축법·시설물의 안전관리에 관한 특별법 등 현행 시설물 안전관리 법률 개관, 스마트 빌딩 안전관리체계 및 정책 동향 등을 분석한다. 다음으로, 스마트 빌딩 등장에 따른 분야별 법적 과제를 제시하고, 미국, 영국, 독일, 프랑스, 일본 등 해외 주요 국가의 스마트 빌딩 안전관리체도를 조사 및 분석하고 시사점을 도출한다. 마지막으로, 현행 스마트 빌딩 안전관리체계의 한계를 인식하고, 제도적 개선을 위한 법·제도 관점의 리모델링 방향을 제시한다.

1. 스마트 빌딩 상용화에 따른 안전관리 문제

스마트 빌딩에 대한 합의된 개념이 없으나 현존 건축물·구조물에 사물인터넷(IoT) 분야 등의 신규 기술을 접목해 건물의 환경을 개선하려는 다양한 시도가

이루어지고 있다. 특히, 에너지 효율화의 측면에서 활발하다. 특히, 제4차 산업혁명시대를 맞이하여 건축 분야에서도 정보통신기술(ICT)을 바탕으로 한 자율제어시스템을 구축하여 건축물·구조물을 통제·운영할 수 있는 스마트 빌딩(인텔리전트 빌딩)에 대해 최근 각종 논의가 진행되고 있다. 그러나, 법제 지원적 관점의 접근은 전혀 없는 상황이다.

스마트 빌딩은 ICT 기술의 지원을 필수불가결 요소로 하는바 ICT 시스템 환경을 위협할 수 있는 요소들, 즉 해킹에 의한 악의적 공격이나 시스템 자체의 기술적 취약점 발생의 경우를 대비하지 않는다면 오히려 스마트 빌딩을 아예 구축하지 않는 경우보다 더 심각한 피해가 발생할 우려가 있다.

2. 현행 안전관리 법률에 근거한 시설물분야에 대한 안전관리 체계 분석

현행 안전관리제도 체계상 시설물 안전의 주무 부처는 국토교통부로 건축물·시설물 등에 대한 안전관리에 대한 정책을 추진하고 있으며 산업통상자원부가 스마트 빌딩에 대한 지원 정책을, 과학기술정보통신부가 인공지능 등 신기술과 관련한 지원정책을 담당하고 있다.

우리나라의 스마트 빌딩에 대한 정책은 기후변화에 대응한 저탄소정책과 에너지 효율화, 신재생에너지 정책 등의 한 분야로 추진되고 있다. 스마트 빌딩의 안전관리는 건축법, 시설물의 안전관리에 관한 특별법, 초고층 및 지하연계 복합건축물 재난관리에 관한 특별법 등 기존의 시설물안전법률의 적용을 받는다. 하지만 스마트 빌딩을 규정한 개별 법률이나 규정이 없는 상황이다.

3. 지능정보기술을 활용한 스마트 빌딩의 상용화 과정에서 여러 문제점

스마트 빌딩의 등장으로 기존의 시설물 안전관리제도의 한계로 인하여 많은 법적 문제가 발생할 것으로 예상된다. 이에 기존 법·제도 한계로 제기될 관리상의 법적 문제를 스마트 빌딩 설계 및 건축과정에서의 안전관리, 스마트 빌딩 시스템의 보안과 개인정보보호를 중심으로 관련된 내용을 분야별로 검토가 필요하다.

4. 해외 시설물 안전관리체계 조사 및 분석

미국, 영국, 프랑스 등 대부분의 국가에서 스마트 빌딩 정책은 에너지 효율화, 기후변화 대응정책의 하나로 추진되고 있다. 다만, 독일의 경우 스마트 빌딩보다 스마트 팩토리를 중심으로 정책을 추진하고 있는 것이 특징이다. 입법 현황에 있어서도 아직 스마트 빌딩을 대상으로 하는 법률은 없으며, 에너지법이나 기후변화 대응 관련 법률에서 일부 규정하고 있다. 다만, 2017년 처음으로 미국에서 개별 법률로 ‘스마트 빌딩 진흥법’을 상원에 발의한 상황이다.

가. 미국

미국은 2017년 세계 최초로 연방 법률로 스마트 빌딩에 대한 법적 정의와 개념 요소를 규정하고 이에 대한 지원을 규정한 스마트 빌딩 진흥법안을 마련하였다. 이러한 점에서 미국은 법·제도적으로 가장 앞서있다고 할 수 있다. 스마트 빌딩 도입 사례를 보더라도 대표적 사례인 2012년도에 건축된 샌프란시스코 공공 유틸리티 위원회(San Francisco Public Utilities Commission)건물의 경우 자연광(태양광) 수집 및 풍력 발전을 활용한 에너지 절감 시스템을 구축하고 있어서 에너지 효율화 측면에서 접근하는 측면도 있다. 더 나아가 건물 내의 데이터 이동을 조망할 수 있는 통합 건물 운영시스템을 내부에 구축하는 사례(미시건 주, 플린트 시의 대중교통국 건물)도 있어서 에너지 효율화는 물론 빌딩 리노베이션을 통해 감시카메라 및 네트워킹 신기술을 건물 내에 도입함으로써 범죄율이 높은 다운타운 지역에서 버스 승객의 환승에 안전을 확보하는 등 보다 확장된 모습을 보인다.

나. 영국

영국에서의 스마트 빌딩은 프랑스나 일본 등 다른 국가들과 유사하게 건물에 대한 에너지 효율성 제고 및 환경 개선을 위해 시작되었다. 따라서 스마트 빌딩에 대한 법적 정의나 개념요소 등을 직접 규정한 법률은 없다. 다만, 관련 법령은 없지만, 기후변화 대응을 위한 법률 등에서 관련 내용을 일부 규정하고 있다.

스마트 빌딩 정책의 추진도 정부에서 직접 나서기보다는 민간에서의 진행 상황을 지켜보고 있는 단계라 할 수 있다. 영국 내 스마트 빌딩을 포함하여 기술 관련 분야에 있어 공적 기관보다는 민간 수준의 기관이 더욱 적극적인 역할을 수행하고 있는 것이 사실이지만 공적 기관도 그 역할을 하고 있다. 영국에서는

이미 2014년 2월에 정부 내 기업혁신기술부(Department for Business, Innovation and Skills)는 스마트시티의 규제 및 표준화를 위한 각종 제안 사항을 제시하고 있는 스마트시티 프레임워크 - 스마트시티와 커뮤니티를 위한 전략 수립 가이드(Smart city framework - Guide to establishing strategies for smart cities and communities) 25라는 문서를 발행한 바 있기 때문이다. 영국에서의 스마트 빌딩에 대한 관심은 사적 분야에서 본격화되고 있는 것이 사실임은 앞서 본 바와 같지만, 공적 당국 역시 관련 상황을 예의 주시하며 일정 정도의 협업을 도모하며 본격적인 지원을 제공하고 있는 것 역시 사실이다.

스마트 빌딩 관련 주요한 역할을 자임하고 있었던 기업혁신기술부는 2016년 7월에 기업, 에너지 및 산업 전략부(Department for Business, Energy & Industrial Strategy)로 개편된 바 있다. 더욱이 기업혁신기술부(BIS)뿐만 아니라 에너지 및 기후변화부(the Department of Energy and Climate Change, DECC) 역시 기업, 에너지 및 산업 전략부(BEIS)에 편입됨에 따라 기술 분야에서 정부는 향후 이전보다는 적극적인 입장을 견지할 것으로 생각된다.

특히 기구 개편으로 기업, 에너지 및 산업 전략부는 스마트 기술 정책과 관련한 적지 않은 역할을 수행하고 있는 것으로 보이는데 그중 대표적인 것이 Green Deal (정책)이다. 이는 영국 내 거주자들이 가정에서 에너지를 절약할 수 있도록 유도할 뿐만 아니라(energy-saving improvements) 그에 대한 가장 합리적인 지불 방법을 찾도록 지원하는 정책을 말한다. 특히 최대한 에너지 절약을 할 수 있도록 하는 Green Deal이라는 당해 향상 기제(improvements)는 각 개인의 가정 상황에 따라 달리 적용할 수 있도록 하고 있어서 탄력적인 운영 방향성을 확보하고 있는 영국만의 획기적인 스마트 관련 정책이라고 볼 수 있다.

다. 독일

독일은 스마트 빌딩에 대한 정책은 명확하게 논의되는 바는 없으나 프랑스나 영국 등 주변 유럽 국가들이 빌딩의 에너지 효율화와 온실가스 감소 등 환경적 측면에서 접근하고 있는 것에 비추어 그 범주를 벗어나지는 않을 것으로 판단된다. 다만, 스마트 팩토리에 대한 정책추진에 있어서 사물인터넷(IoT)과 서비스 인터넷(IoS)을 구성요소로 하는 인더스트리 4.0의 실현방식을 취하고 있어서 향후 스마트 빌딩에서도 이러한 신기술을 접목할 것으로 보인다.

안전관리제도 시스템도 스마트 빌딩을 직접 대상으로 하는 법률은 없으나 시설물 안전관리는 일반적으로 연방환경의 보호 목적으로 제정되어 통합적인 연방 법전으로 인정되는 연방임미시온방지법에서 다루고, 일부는 시설물 관련 법령에 개별적으로 규정하고 있으므로 이러한 법률체계에서 관리된다고 하겠다. 아직 이러한 법률에서 스마트 빌딩에 대한 규정은 없다.

라. 프랑스

프랑스의 스마트 빌딩 정책 및 법제는 기후변화 및 에너지전환정책과 밀접한 연관을 맺고 있다. 이에 프랑스에서는 스마트 빌딩을 에너지 소비의 최적화, 재생에너지의 활용 등의 관점에서 접근하고 있는 것으로 보인다. 그 결과 2015년 에너지전환법에 따라서 현재는 우선 공공건물을 대상으로 하여 ‘에너지수행 우수 건물’ (bâtiment à énergie positive, positive energy buildings) 또는 ‘환경수행 우수 건물(bâtiment à haute performance environnementale)’의 증진을 목표로 하여 관련 법령을 마련하여 신축 건물의 에너지 및 환경적 성능(performance)의 개선에 힘쓰고 있다.

마. 일본

일본의 스마트 빌딩과 홈은 에너지를 효율화하자는 입장에서 이 제도를 적극적으로 추진하고 있다. 현재 일본의 스마트 빌딩과 주택에 대한 정책과 법·제도에 대한 특징과 시사점은 다음과 같이 요약할 수 있다. 첫째, 스마트 빌딩과 홈의 도입 목적은 “에너지의 효율화”에 있다는 것이다. 에너지 절감과 효율화를 위하여 정보통신을 이용하여, 에너지를 절감하려는 것이다. 둘째, 스마트 빌딩과 주택에 대한 관리부서는 중앙정부인 “경제산업성과 국토교통성”이다. 이들 부서의 구분은 경제산업성은 스마트 빌딩과 주택에 대한 비용 지원을 주된 것으로 하고, 이에 반하여 국토교통성은 에너지 효율화에 대한 관리시스템으로 인정제도를 도입하여 시행하고 있다는 것이다. 셋째, 스마트 빌딩과 주택에 대한 구체적인 근거법을 가지고 있지 않다는 것이다. 단지 에너지 효율화를 위하여 건축물 등에 대하여 「건축물에너지 소비성능의 향상에 관한 법률(建築物のエネルギー消費性能の向上に関する法律)」에 따라 인정제도를 도입하여 시행하고 있다. 넷째, 스마트 빌딩과 주택 도입을 위하여 정부는 적극적으로 총리대신의 지

도로 지원하고 계획을 수립하여 시행하고 있다.

이처럼 일본에서 스마트 빌딩과 주택은 정보통신을 활용하여 에너지를 효율화하는데 중점을 두고 지원하는 특징을 보인다.

5. 법·제도 관점에서의 시설물 안전관리체계 구축 방안

스마트 빌딩 등 시설물 안전과 관련한 현행 국가적 안전관리체계의 구조적 문제점은 아직 판단하기 어려운 상황이다. 그 이유는 스마트 빌딩의 활용이 아직 초기 단계이어서 이에 대한 안전관리체계 구성이 쉽지 않기 때문이다. 이러한 현상은 우리나라뿐만 아니라 미국, 일본, 유럽의 주요 국가도 동일하다.

따라서 스마트 빌딩에 대한 안전관리 제도개선도 기존의 시설물의 화재나 붕괴 등과 같은 고전적 안전문제에 대한 접근보다는 기후변화 및 에너지전환정책, 에너지 효율화와 밀접한 연관을 맺고 있어서 이에 대한 기술적 연구에 대한 지원에 중점을 두고 있는 것이 일반적 추세이다. 법·제도 관점에서 시설물 안전관리체계 구축 방안은 다음과 같다.

첫째, 스마트 빌딩 관리를 위한 통합네트워크 구축이 필요하다. 스마트 빌딩은 최첨단 IT를 활용한 것으로 이러한 도시계획은 사회 인프라를 구축하는데 중요한 요소가 되고 있다. 예컨대, 스마트 빌딩은 감시 카메라나 입·퇴실 관리 등의 보안과 함께 조명, 공기조절, 방재 등의 설비가 상호 제휴하면서, 휴일 없이 가동되고 있다. 또한, 디지털 전자 게시판이나 화상회의 등의 이용도 급증하고 있어, 빌딩의 복합화와 대규모화에 적극적이다.

스마트 빌딩의 경우 일반적으로 설비 시스템이 독립하여 설치되어 있어, 대형 빌딩에서는 설비 중복에 따른 비용 증가가 발생할 수 있다. 이러한 비용의 문제를 해결하는 것이 스마트 빌딩의 부가가치를 향상할 수 있으며, 이를 위해 통합네트워크 방식이 요구된다. 감시카메라나 입·퇴실 관리 등 복수의 시스템을 단일 네트워크로 통합하는 것은 비용절감, 편리성 향상, 에너지 절약을 가져올 수 있다. 따라서 스마트 빌딩의 구축하기 위해서는 통합네트워크 구축이 전제되어야 한다.

둘째, 스마트 빌딩 건축과 관련한 초기 투자비용 증가문제이다. 스마트 빌딩

에 있어 건물주는 다양한 시스템을 통합화하기 위하여 초기 투자비용이 증가하게 된다. 이러한 투자비용 저감을 위한 노력이 없이는 스마트건물과 주택에 대한 보급이 어렵다. 스마트 빌딩의 보급이 없이는 안전한 관리체계를 구축하기 어렵다.

셋째, 스마트 빌딩 관련 법률이 마련되어야 한다. 현행 법률에서는 스마트 빌딩에 대한 법적 정의는 없으며, 기존의 건축법 등 관련 법률에서는 건설업자에게 내진과 태풍 등 전형적인 위험에 견딜 수 있도록 요구하고 있으나, 에너지 효율화나 절약을 위해 스마트 빌딩에 요구되는 기준 등에 대해서는 흠결되어 있다. 아직 이에 대한 구체적인 관련 법적 근거도 마련하고 못 하고 있다.

제4절 사회기반(금융) 안전 : 블록체인

블록체인 등 신기술의 등장에 따른 금융 분야 안전관리체계의 법·제도 관점에서의 리모델링 연구로 다음과 같이 구성된다. 우선, 블록체인 등 신기술의 발달과 이를 기반으로 하는 암호화폐의 등장에 따른 관리 문제를 서술한다. 다음으로, 암호화폐의 개념과 특징, 암호화폐에 대한 정책 및 전자금융거래법 일부 개정안 등 법제화 동향 등을 분석한다. 이후, 암호화폐 등장에 따른 자금세탁 등 불법행위, 세금부과 등 분야별 법적 과제를 제시하고, 미국, 영국, 프랑스, 일본 등 해외 주요 국가의 블록체인(암호화폐) 관리 제도를 조사 및 분석하고 시사점을 도출한다. 마지막으로 블록체인 기반의 암호화폐에 대한 현행 금융관리체계의 한계를 인식하고, 제도적 개선을 위한 법·제도 관점의 리모델링 방향을 제시한다.

1. 암호화폐의 등장이 금융분야에 미치는 영향

블록체인 등 신기술을 기반으로 인터넷을 통하여 전자적 거래되는 암호화폐가 등장하였다. 그 대표적인 예인 비트코인의 경우 전 세계에서 2017년 10월 시점에서 시가총액은 약 940억 달러에 하루 거래액이 약 15억 달러에 달하고 있다. 블록체인 기술을 기반으로 하는 암호화폐의 등장은 기존 중앙은행을 기반으로 하는 법정화폐를 중심으로 하는 금융제도 전반에 충격을 주고 있다. 중앙은행의 통제를 벗어나 지급 및 거래수단을 만들려는 시도는 통화의 가치와 안전성을 보장하는 기존의 금융제도를 와해시켰다. 이를 이용해 투기적 수단으로 악용

하려는 불법적 행위라는 시각이 일반적이다.

2. 암호화폐 관련 국내 안전관리 법률체계 및 정책 조사 및 분석

현행 안전관리체계상 금융안전은 사회기반안전의 한 분야로 기획재정부, 금융위원회를 중심으로 관리를 하고 있다. 2017년 9월에는 금융위원회가 7개 관계부처(기획재정부, 국무조정실, 공정거래위원회, 법무부, 방송통신위원회, 국세청, 경찰청) 및 3개 관계기관(한국은행, 금융감독원, 한국인터넷진흥원) 등의 10개 기관과 ‘관계기관 합동 TF’ 구성을 통하여 향후 가상화폐(Virtual Currency)에 대한 정책적 대응방안과 관련 법규 개정의 필요성과 방향을 제시하였다.

현재 정부 정책은 암호화폐가 투기적 수단으로 변질되고, 불법적인 투자자 모습과 불법적 거래가 문제되어 이를 규제하는 방향으로 정책을 마련 중이다.

3. 블록체인 신기술의 안전적 활용을 위한 관련 법령에 대한 검토

암호화폐의 안전적 활용을 위한 전자문서 및 전자거래기본법, 전자금융거래법, 개인정보보호법, 전자서명법, 상법, 주식 및 사채 등의 전자등록에 관한 법률, 자본시장과 금융투자업에 관한 법률 등에 대한 검토가 필요하다.

가. 암호화폐를 활용한 자금세탁 등 불법행위

암호화폐의 익명성을 바탕으로 자금세탁, 탈세, 마약·무기밀매 등 불법거래에 악용하거나, 규제 사각지대에 있는 점을 노려 유사수신 등 범죄를 저지르는 경우가 발생할 가능성이 매우 높다. 그 밖에도 해킹 등 불법행위의 대가로 디지털통화를 요구하거나 유사 디지털통화 투자로 고수익이 가능하다고 현혹하는 사례도 나타난다. 암호화폐 거래소를 통한 거래에 있어서 본인확인 절차가 의무화되어 있지 않으며, 거래소를 통하지 않은 직접 거래방식도 사용 가능한 상황이기 때문에 자금세탁의 방법으로 암호화폐가 사용되는 것이다.

나. 암호화폐에 대한 세금문제

암호화폐에 대한 세금부과 문제는 위의 자금세탁을 하는 이유에 조세회피를

위한 경우가 많다는 점과 암호화폐 거래를 통한 수익에 대한 세금을 부과할 필요가 있는가, 암호화폐 관련 영업을 하는 거래소에 관련 세금을 부과할 필요가 있는가 등 다양한 법적 이슈가 발생할 수 있어 이에 대한 법적 검토가 필요하다. 이에 관하여 자금세탁방지기구(Financial Action Task Force; FATF)의 2015년 암호화폐와 법정화폐를 교환하는 거래소에 등록·면허제를 부과하는 지침내용을 추가한 바 있으며, 일본은 비트코인 거래에 관한 소비세법 시행령 개정으로 소비세는 폐지하는 한편, 소득세는 유지하는 태도를 취하고 있다.

우리나라 국세청은 암호화폐가 부가가치세 과세대상인지 여부에 대한 질의와 관련하여 “비트코인이 화폐로서 통용되는 경우에는 부가가치세 과세대상에 포함되지 아니하는 것이나, 재산적 가치가 있는 재화로서 거래되는 경우에는 부가가치세 과세대상에 해당하는 것”이라는 유권해석(서면부가-21616, 2015.12.29)을 한 바 있다.

다. 불법자금모집, 사기대출유인 등

공인된 암호화폐인 것처럼 가장하며 자금을 모집하거나 코인(암호화폐)에 투자하면 원금 보장과 고수익 보장을 약속하는 불법자금모집의 사례가 발생하고 있다. 코인의 가격이 급등하여 투자금 이상의 수익을 보장할 수 있으며 현금으로 100% 환전이 가능하다고 제시하는 사례도 나타나고 사기대출 유인의 문제도 나타나고 있는데, 고금리대출로 어려움을 겪는 대출수요자(피해자)에게 햇살론 등 정부정책상품으로 대환대출을 안내해 주는 것으로 유인하여 수수료 명목의 비트코인을 갈취하는 소비자 피해 등도 발생하고 있다.

그 밖에도 암호화폐 관련 프로젝트를 인터넷상에 게시하여 자금을 모집하는 ICO(Initial Coin Offering)가 등장하여 증권규제를 받지 않은 상황에서 자금을 모집하는 형태로 활용되기도 한다. ICO를 이용한 자금조달은 그 자금모집의 형태가 기존의 증권규제 범주에 포함되지 않기 때문에 중국의 경우에는 불법으로 규정하고 있는 한편, 싱가포르 금융당국에서는 자본시장법상 집합투자증권 또는 채무증권으로 분류할 수 있다고 하면서 규제가능성을 제기하였다.

현재 「전자금융거래법 일부 개정 법률안」이 발의 되어 있다. 동 법률안은 암호화폐에 대한 정의와 관련 서비스 유형별 업태 규정을 통한 암호화폐 이용자

보호를 위한 암호화폐 거래 및 암호화폐 취급업자에 대한 의무와 금지행위 규정을 두고 있다.

라. 블록체인 등 신기술의 활용 과정의 문제점

블록체인 기술에 기반을 둔 암호화폐의 등장으로 기존의 금융관리제도의 한계가 나타났다. 이로 인하여 많은 법적 문제가 발생할 것으로 예상된다. 그 중에서 특히 논란이 되고 있는 암호화폐를 활용한 자금세탁 등 불법행위, 암호화폐에 대한 세금문제, 암호화폐를 가장한 불법자금모집이나 사기대출유인 등이 문제가 된다.

암호화폐의 익명성을 바탕으로 자금세탁, 탈세, 마약·무기밀매 등 불법거래에 악용하거나, 규제 사각지대에 있는 점을 노려 유사수신 등 범죄를 저지르는 경우가 발생할 가능성이 매우 높다. 그 밖에도 해킹 등 불법행위의 대가로 디지털통화를 요구하거나 유사 디지털통화 투자로 고수익이 가능하다고 현혹하는 사례도 나타나고 있다.

4. 블록체인(암호화폐) 관련 해외 안전관리 법체계 조사 및 분석

비트코인 등 암호화폐의 법적 허용에 대해서는 국가마다 다소 차이가 있으며 암호화폐에 대한 개별법은 존재하지 않았다. 다만, 일본에서는 2017년 4월 비트코인을 포함한 암호화폐를 대상으로 한 개정 자금결제법이 시행이 되고 있으며, 미국은 2017년 7월 통일가상화폐업규제법(Uniform Regulation Of Virtual Currency Businesses Act)이 통과되어 법적인 규제를 하게 된다. 영국은 비트코인 등 암호화폐에 대한 입법에 아직은 소극적이며, 금융소비자보호차원에서 암호화폐와 관련한 자금세탁방지법 준수여부 규제만 하고 있다. 구체적인 내용은 다음과 같다.

가. 미국

미국의 경우에는 규제당국에서 비트코인 등 관련 암호화폐의 거래에 있어서 긍정적 측면을 인정하면서도 상당한 리스크를 감안하여 이에 대한 규제가 필요하다고 보고 있다. 이에 미국 국세청에서는 2014년 3월에 비트코인에 대한 과세

기준에 대한 가이드라인을 공포하였다. 이는 비트코인이 법정화폐는 아니지만, 그 거래로 생긴 이득에 대해서는 주식이나 채권처럼 자본소득세를 부과하겠다는 취지로 이해될 수 있다. 아울러 2015년 9월 상품선물거래위원회(Commodity Futures Trading Commission, CFTC)는 비트코인을 투자의 대상이 될 수 있는 상품으로 규정하면서 CFTC로부터 플랫폼 사용에 대해 승인 신청을 하지 않은 비트코인 옵션거래 업체에 대해 운영 중단을 명령한 바 있다.

2016년 9월 19일 뉴욕주 법원에서 비트코인을 불법적으로 유통하여 연방자금세탁법 위반 및 무인가 자금송금업체를 운영한 혐의 등으로 기소된 사건에서 비트코인이 재화화 서비스의 지급수단이라는 점에서 화폐성이 인정된다는 판결은 향후 비트코인 등과 같은 암호화폐의 상용 범위에 따라 그 법적 성격이 달라질 수 있다는 점에서 우리 제도 상에도 시사점을 주는 사례로 보다 면밀한 검토가 요구된다.

나. 영국

영국에서는 금융소비자 보호와 관련해서 자금세탁방지법상의 규제만 받는 것으로 하여 규제상 매우 제한적인 태도를 취하고 있다. 이에 대해 업계는 지속적으로 규제를 명확히 해달라는 요청을 하면서, 한편으로 자율규제차원에서 전통적인 지급결제기관과 유사하게 규제를 준수함으로써 금융소비자의 신뢰를 얻기 위하여 노력하고 있다.

일각에서는 전통적인 지급결제기관과 동일한 규제가 부과될 필요가 있다는 주장도 하고 있고, 적어도 암호화폐 관련 거래위험성을 고지하도록 하고, 분쟁시 관련 처리절차를 안내하도록 의무화하여야 한다는 주장도 제기되고 있다. 그러나 영국정부는 암호화폐 기술의 발달정도와 암호화폐 사용률 등의 비중을 고려하여 이러한 산업에 진입하려는 창업에 장애가 되지 않고 보다 혁신적인 서비스를 제공할 가능성이 많다고 전망하고 있으며 금융소비자보호와 관련하여 기존의 보호방식 그대로 제공하는 것에는 다소 신중한 태도를 보이고 있다.

그런데 이러한 영국의 태도는 국제적으로 암호화폐와 관련하여 입법을 한 국가와 비교하여 볼 때 금융소비자보호면에서 큰 차이가 있는 것으로 평가할 수 있다. 대표적으로 일본의 경우 자금결제법의 개정을 통해 암호화폐교환업을 등

록제로 하되 이에 대해서는 행위규제를 통해(정보의 안전관리, 암호화폐업의 일부를 제3자에게 위탁한 경우 위탁기관에 대해서도 지도할 의무를 부과) 이용자 보호조치의 강구를 요구하고 있기 때문이다.

현재 암호화폐 관련 산업과 거래에 대한 영국의 유연한 태도는 향후 암호화폐 기술의 발전과 이용도에 따라 달라질 가능성이 없지 않으나 현재의 태도가 상당 기간 유지될 것으로 전망할 수 있다. 요컨대 암호화폐 관련한 영국정부의 태도는 ‘금융소비자 이익 증대’와 ‘혁신’을 비교형량하면서 결정·유지될 것으로 판단된다. 다만, 영국에서 시도되고 지원하는 혁신은 일명 ‘파괴적 혁신’을 목표로 하는 것으로 기존 업계의 구도를 질적으로 변화시킬 수 있는 상품과 서비스의 혁신을 가져오는 것을 목표로 하고 있음을 간과해서는 안 될 것이다.

다. 프랑스

비트코인에 대한 프랑스의 법적 규제의 내용을 정리하면, 우선 비트코인은 프랑스에서도 다른 나라의 경우와 마찬가지로 법정통화는 아니지만 대체지불수단의 하나로서 인정되고 있다는 점이다. 그리고 비트코인에 관한 조세정책도 강화하여 상속 및 부유세의 일종인 ISF(재산에 대한 연대성 세금), 그리고 전매목적의 비트코인 획득에 있어서 비트코인을 조세부과의 대상으로 삼고 있다. 다만, 비트코인은 유형재산은 아니므로 비트코인에 대한 부가가치세의 부과는 면제되고 있다.

이와 함께 비트코인의 유통이 점차 활발해 지면서, 비트코인에 관한 비공식적 경제가 차지하는 비중도 점차 감소하여 현재는 비트코인 전체 거래의 3~6%에 불과하게 되는 등 점차로 비트코인은 합법적인 거래의 지불수단으로서 인정되고 있음을 알 수 있다.

한편, 프랑스에서는 최근에는 비트코인과 같은 사이버화폐(Cybermonnaie)를 활용하여 새로운 사업에 대한 자금조달을 실시하는 ICO에 대해서, 그로 인한 위험으로부터 일반인 투자자들을 보호할 수 있는 법적 장치를 마련하기 위한 조사작업이 진행 중이다. 이와 관련해서 프랑스 금융안전위원회는 현재 UNICORN 프로그램을 실시하고 있다. 이 프로그램은 ICO에 대한 법적 규제와 관련해서 기존의 법률규정의 적용범위를 확대하는 방안과 새로운 법률규정을 제정하는 방안

을 두고 논의를 진행하고 있는데, 2017년 12월 22일까지 국민의견조사를 실시하는 등 이번 프로그램의 결과에 따라서 향후 프랑스에서 비트코인 및 ICO에 대한 법적 규제의 기본방향과 구체적인 내용들이 결정될 수 있을 것으로 보인다.

라. 일본

일본은 2017년 4월부터 시행되는 개정 자금결제법이 나오기 까지 2015년 7월부터 관련된 분야의 각계 전문가들로 구성된 금융청 내의 금융심의회 전문워킹그룹 활동(결제업무 등의 고도화에 관한 워킹그룹, 총 7회)을 통하여 암호화폐의 현재 문제점과 앞으로의 기대 및 기술 발전 저해 등의 우려 등에 대해서도 충분히 논의하여 그 결과를 반영하여 암호화폐의 정의 및 환전 거래 규제에 관한 법률을 제정하고 공표하였다. 이러한 입법과정의 노력도 시사점이라 하겠다.

우리나라에서도 법무부를 중심으로 금융위원회, 기획재정부, 공정거래위원회 등 관계 부처와 함께 ‘암호화폐 관계기관 합동 태스크포스(TF)’를 만들어 암호화폐 투자를 사칭한 유사수신행위의 처벌 근거를 명확히 하고 처벌을 강화하는 내용의 법령 개정을 추진하고 있어 현재 늘어나는 암호화폐 투기 관련 범죄를 방지하는 측면에서는 꼭 필요한 일이지만 모든 형태의 신규 ICO 금지 조치는 앞으로의 국내 블록체인 기술과 관련 산업 발전을 저해 및 위축 시킬 수도 있기 때문에 일본과 같은 업계의 자율규제 제도 도입, 국민공동감시기구 설립 등도 고려하여 선제적으로 대응하면서 발전할 수 있는 환경을 만들어야 할 것이다.

5. 법·제도 관점에서의 사회 기반(금융) 안전관리체계 구축 방안

블록체인 기술을 활용한 암호화폐의 등장과 거래량의 급속한 증가와 개인의 투기적 접근으로 인하여 규제의 필요성이 증가하고 있다. 그러나 아직 암호화폐에 대한 법적 개념도 없고 이에 대한 체계적인 연구도 없는 실정이어서 현행 금융안전관리체계에 대한 구체적 개선방안을 도출하기가 어려운 것이 현실이다. 향후 제도개선과 관련하여 암호화폐에 대한 법적 측면에서의 연구의 필요성과 투기적 목적으로 암호화폐를 거래하는 현재의 상황에 대한 규제의 필요성이 있다. 향후 제도개선과 관련하여 암호화폐에 대한 법적 측면에서의 연구의 필요성과 투기적 목적으로 암호화폐를 거래하는 현재의 상황에 대한 규제의 필요성 등

에 대해 다음과 같이 제언한다.

첫째, 암호화폐에 대한 법적 연구가 필요하다. 암호화폐의 등장이 얼마 되지 않아 아직 암호화폐의 실체가 모두 드러났다고 할 수는 없다. 따라서 암호화폐의 본질과 법적 성격에 대한 더 많은 법적 연구가 필요하다. 지금까지 우리가 접하고 있는 암호화폐, 예를 들어 비트코인(BTC)이나 이더리움 플랫폼의 이더(ETH)와 같은 것들은 지급수단으로서의 성격을 가지고 있다는 점은 분명해 보인다. 다만 이들은 가치가 확정된 통상적인 지급수단이 아니라 가치가 수요와 공급의 원리에 따라 변화하는 금융상품형 전자지급수단이고 이들은 분산형으로 발행되어 채권성을 보유하지 않고 배타적 지배는 인정되므로 물권성을 제한적으로 가지고 있다고 본다. 요컨대 암호화폐는 제한적 물권성을 가진 금융상품성 전자지급수단으로 볼 수 있다.

둘째, 투기적 목적으로 암호화폐를 거래하는 현재의 상황에 대한 규제의 필요성이다. 암호화폐법의 영향은 실제로 규제에 대한 관리 및 감독이 얼마나 엄격하게 이루어지는가에 따라서 그 범위가 다르겠지만 일본의 암호화폐법 규제를 통하여 자금 및 투기 사기 등의 리스크가 크게 경감될 것으로 예상되며 암호화폐 환전업계의 건전한 발전을 이끌 수도 있다.

우리나라에서도 법무부를 중심으로 금융위원회, 기획재정부, 공정거래위원회 등 관계 부처와 함께 암호화폐 관계기관 합동 태스크포스(TF)를 만들어 암호화폐 투자를 사칭한 유사수신행위의 처벌 근거를 명확히 하고 처벌을 강화하는 내용의 법령 개정을 추진하고 있어 현재 늘어나는 암호화폐 투기 관련 범죄를 방지하는 측면에서는 꼭 필요한 일이지만 모든 형태의 신규 ICO 금지 조치는 앞으로의 국내 블록체인 기술과 관련 산업 발전을 저해 및 위축 시킬 수도 있기 때문에 일본과 같은 업계의 자율규제 제도 도입, 관민공동감시기구 설립 등도 고려하여 선제적으로 대응하면서 발전할 수 있는 환경을 만들어야 할 것이다.

또한 암호화폐라는 명칭에 대한 사용 규제가 없기 때문에 법률상으로 암호화폐가 아님에도 불구하고 미등록 업체가 암호화폐라는 표현으로 유의한 상품을 판매하면 법률상의 암호화폐 환전업을 하는 것이 아니기 때문에 규제 등을 받지 않기 때문에 이용자에 대한 피해도 예상된다. 따라서 용어 사용에 대한 규제 등도 고려하며 범죄로 악용되지 않도록 해야 할 것이다.

제5절 소결

인공지능, 빅데이터, IoT, 클라우드 등 다양한 신기술이 활용되어 사회의 혁신을 유도하는 지능정보사회가 빠르게 도래하고 있다. 이러한 추세는 우리나라 뿐만 아니라 여러 국가에서 당면한 현상으로 변화된 미래 환경에서의 주도권을 잡기위한 국가 간 경쟁도 더욱 치열해지고 있다. 정보통신기술에 근거한 신기술 사회의 도래는 피할 수 없는 상황이 되었고, 일부는 이미 사회적 현상으로 받아들여지고 있다.

이러한 신기술의 지능정보사회에서는 빠르게 진화하는 기술과 이를 반영하여야 하는 사회적 시스템 사이에 현실적 괴리가 발생할 수밖에 없다. 그 이유는 기존의 사회적 제도, 특히 법·제도가 급변하는 기술적 요인을 수용하기가 쉽지 않기 때문이다. 그 중에서도 국민의 안전과 관련된 분야는 더욱 그러하다. 이미 신기술 사회가 도래하고, 이를 현실에서 반영하고 있더라도 이러한 신기술에 대한 사회적 합의가 없거나 기존의 안전체계가 기술변화를 반영하지 못하면 아무런 의미가 없다.

따라서 변화된 신기술 사회가 실질적으로 도래하기 위해서는 다른 분야도 그러하지만 특히 안전 분야는 기술과 법·제도가 함께 발전하여야 한다. 이러한 취지에서 지능사회로의 패러다임 전환과정에서 국민의 안전을 확보·강화하는데 파급효과가 클 것으로 예상되고 시급성이 인정되는 교통안전, 시설물 안전, 사회 기반 안전(금융)에 대한 안전관리체계의 리모델링에 대한 연구를 수행하였고, 각각의 제도개선 방향에 대해 연구하였다. 각 분야별 안전관리체계 리모델링의 방향을 정리하면서 향후 관련 분야 연구에 대한 정책적 제언을 하였다.

제5장 결론

이 연구에서는 지능정보사회의 도래로 급격한 변화가 예상되는 교통 안전, 시설물 안전, 사회기반(금융) 안전 분야에 대한 안전관리체계 개선 방안에 대해 다루었다. 다양한 관점에서 종합적이고 전문성 있는 연구를 위해 소프트웨어정책연구소는 한국행정연구원, 한국법제연구원과 협동 연구를 수행하였다.

소프트웨어정책연구소는 선정된 안전 분야의 대표적인 기술인 자율주행차, 스마트 빌딩, 블록체인 기술에 대해 조사하였고, 해당 분야에서 기술 상용화 과정에서의 사회 변화를 예측하고 기술과 안전과의 관계를 분석하였다. 한국행정연구원은 지능정보사회 출현에 따른 사회변화 내용 분석, 신기술 적용 시 예상되는 주요 쟁점 분석, 기존 안전관리체계의 문제점 진단, 그리고 효과적인 대응을 위한 변화 및 개선방안 등을 정부 행정 차원에서 종합적으로 도출하였다. 마지막으로 한국법제연구원은 각 안전 분야의 기존 안전관리체계 및 입법사례 분석을 통하여 문제를 도출하고, 향후 효과적인 대응을 위해 요구되는 법·제도 관점에서 변화 방향을 제시하였다. 특히, 법·제도 관점에서 지능정보기술 적용 시 예상되는 주요 법적 이슈와 쟁점을 분석하였다.

자율주행차 기술은 교통 안전 분야에 가장 큰 영향을 미칠 기술이다. 자율자동차와 관련된 요소 기술은 환경인식기술, 측위기술, V2X 기술 등 3가지로 구분하였다. 이러한 요소 기술을 바탕으로 자율주행차 안전을 목표로 해외 주요국들은 대응 및 제도 정비를 본격화하고 있다. 자율주행차의 상용화 시점에 대한 예측은 연구기관마다 다르나, 그 시점은 대략 5~10년 정도로 예상한다. 자율주행차는 보안과 구글 자율주행차 사고에서와 같은 기술 두 가지 측면에서 안전에 영향을 미친다고 볼 수 있다. 특히, 현재까지 공식적으로 확인되거나 보고된 자동차 관련 해킹 침해 사고는 없지만, 각국의 많은 연구원의 수많은 연구 및 실험에 걸쳐 차량 내 컴퓨터 시스템이 해킹 가능성을 증명하기도 했다.

행정관리 측면에서의 교통 안전관리체계 개선을 위해서는 교통 안전 거버넌스 체계의 구축, 전문 인력 양성, 정보보안 및 개인정보보호 방안 수립, 선진사례의 적극적인 도입이 필요하다. 좀 더 구체적으로 설명하면 다음과 같다. 첫째, 지능정보기술의 도입으로 발생할게 될 다양한 위험에 대처하기 위한 통합적인

교통 안전 거버넌스 체계의 구축이 우선되어야 한다. 둘째, 교통 분야와 지능정보기술 모두를 알고 있는 교통 안전 관리 전문 인력을 시급히 육성해야 한다. 셋째, 교통 안전 관리체계에 지능정보기술이 도입될 때, 보다 수준 높은 정보보안 체계의 구축과 개인정보보호를 위한 방안을 마련되어야 한다. 마지막으로 자율주행차와 관련해 선진국의 법제들을 검토하여 다양한 이슈들에 대응할 수 있는 준비가 필요하다.

제도개선과 관련하여 자율주행차 운행상의 책임의 명확화, 차량 이용에 대한 규제의 개혁, 자율주행 시스템의 안전성 제고, 보험제도 개편 등에 대해 제언하였다. 첫째, 자율주행차의 운행으로 교통사고가 발생할 경우 운전자나 제조사, 소프트웨어 개발자 등 관련 당사자의 형사상 및 민사상 책임을 둘러싸고 매우 복잡한 문제가 발생할 수 있기 때문에 자율주행차 운행상의 책임을 명확화하여야 한다. 둘째, 현행 법령에서는 차량이 어떻게 이용되고 유지되는지 규율하는데 주안점을 두고 있어, 이러한 법령의 체계는 시험운전자 없이 자율주행차 기술의 사용을 허용하고 그 기술이 정확하게 유지되도록 보장하기 위하여 개정될 필요가 있다. 셋째, 자율주행차가 잠재적인 사이버 위협으로부터 보호되게 하려고 강력한 법적 장치를 마련하고, 자율주행차에 더욱 엄격한 기술기준을 적용하여야 한다. 넷째, 자율주행차의 운행 중에 발생할 수 있는 특수한 사고에 대비하기 위하여 새로운 보상 기준을 갖춘 별도의 보험체계가 필요하다.

시설물 안전에 영향을 줄 스마트 빌딩은 크게 통신 기술과 신기술로 나눌 수 있다. 통신 기술은 BACnet과 Zigbee가 대표적이며 스마트 빌딩 내 근거리 통신에 주로 사용된다. 최근에는 빅데이터, 인공지능, IoT 기술과 접목되어 인텔리전트 빌딩으로 점차 변모하고 있다. 스마트 빌딩의 핵심 요소인 건물자동제어 시스템에 ICT 기술이 적용됨에 따라 스마트 빌딩에서 생산되는 다양한 형태의 데이터를 실시간으로 모니터링하고, 이를 바탕으로 건물의 사용자 및 시스템의 특성이 반영된 데이터 기반의 예측 제어가 가능하게 되었다. 스마트 빌딩은 안전한 사회의 구축과 관련된 기회와 위기를 동시에 지니고 있다. 스마트 빌딩의 IoT 기반 통신 시스템은 화재 탐지와 진압 설비와 공기조화설비 시스템의 유기적 연계가 가능하게 하여 화재를 조기에 감지하고 진화할 수 있다. 반면, 스마트 빌딩에 광범위하게 사용되는 IoT기기들은 건축물의 주요 제어시스템과 연동이 되어 있어 IoT 환경의 보안 위협은 기기 손실 및 물리적 파괴, 신호 교란, 정보

유출, 데이터의 변조, 기기의 오작동 유발 등 다양하다.

행정관리 측면에서 시설물 안전에 대해 개선 방안은 다음과 같다. 첫째, 건축·시설물의 생애주기(설계-시공-관리-개·보수 단계)별 맞춤형 안전관리 체계를 마련하여 그 이용에 있어 최대의 효용을 창출하고, 건축물 및 시설물의 이용자가 안정적인 상태에서 활용하기 위한 대책이 필요하다. 둘째, 건축·시설물의 안전관리가 안정적으로 이루어지기 위해서는 이러한 지능정보기술을 도입할 수 있고 운용할 수 있도록 법제적인 뒷받침을 지속해서 지원해야 할 필요가 있다. 셋째, 일관된 원칙과 시스템에 따른 정보 입수가 가능하도록 중앙정부, 지방자치단체, 그리고 관련 민간업체 등이 협력하는 체계가 요구된다. 마지막으로, 다각적인 영향을 고려한 안전관리 체계의 구축이 요구된다.

법·제도 측면에서 시설물 안전에 대해 개선 방안은 다음과 같다. 첫째, 스마트 빌딩은 최첨단 IT를 활용한 것으로 이러한 도시계획은 사회인프라를 구축하는데 중요한 요소가 되고 있기 때문에 스마트 빌딩 관리를 위한 통합네트워크 구축이 필요하다. 둘째, 스마트 빌딩 건축과 관련한 초기 투자비용 증가 문제를 해결할 수 있는 저감 대책이 필요하다. 셋째, 현행 법률에서는 스마트 빌딩에 대한 법적 정의는 없으며, 기존의 건축법 등 관련 법률에서는 건설업자에게 내진과 태풍 등 전형적인 위험에 견딜 수 있도록 요구하고 있으나, 에너지 효율화나 절약을 위해 스마트 빌딩에 요구되는 기준 등에 대해서는 흠결되어 있기 때문에 스마트 빌딩 관련 법률이 마련되어야 한다.

사회기반 안전 특히 금융 분야에 가장 큰 영향을 주는 블록체인 기술은 암호학 기술과 P2P 네트워크 기술 등으로 구성된다. 기술적인 측면에서 사회기반 안전에 가장 큰 위험은 암호화폐 거래소 해킹, ICO를 이용한 사기, 개인정보 유출과 부정 거래, 스마트 거래 해킹 등이 있다. 모든 사고 사례에서 블록체인 자체의 문제이기 보다는 이를 금융 분야에 활용하는데 있어 낮은 보안 의식, 관련 정책 부재 및 미흡, 기술력 부족 등이 문제였다.

행정관리 측면에서 사회기반(금융) 안전 분야의 개선 방안은 다음과 같았다. 첫째, 중앙집중형, 수직적 법 규제를 블록체인의 분산 시스템에 어울리게 정비해야 할 필요가 있다. 둘째, 미국의 경우 금융사고 전문가(PCI Forensic Investigator)를 육성하고 있는데, 우리도 금융사고나 개인정보유출 등에 따른 보

안 사고에 대비해 더욱 체계적이고 근본적인 시스템 마련과 전문가 양성이 필요하다. 셋째, 블록체인 기술을 금융 위험의 파악과 관리에 적극적으로 활용하는 방안을 고려해보아야 한다. 블록체인은 행정정보 공동이용 기반 조성, 기관 간 협업 확대, 공공서비스 인증, 공공데이터 거래 등에 활용할 수 있다. 넷째, 금융 안정을 위해 글로벌 차원의 위험관리 통제센터 네트워크 연계 및 공동 활용 방안도 고려해야 한다. 앞으로 국민안위에 영향을 주는 요인들을 개별 관리하는 것은 불가능하므로 국내 및 역내 차원의 위험관리 통제센터 간의 네트워크를 구축하여 국가별 관리와 역내 차원의 조치가 유기적으로 이루어질 수 있도록 하는 방법도 있을 것이다.

법·제도 측면에서 사회기반(금융) 안전에 대한 개선 방안은 다음과 같다. 첫째, 암호화폐의 등장이 얼마 되지 않아 아직 암호화폐의 실체가 모두 드러났다고 할 수는 없기 때문에 암호화폐의 본질과 법적 성격에 대한 더 많은 법적 연구가 필요하다. 둘째, 투기적 목적으로 암호화폐를 거래하는 현재 상황에 대한 규제의 필요성이다. 암호화폐법의 영향은 실제로 규제에 대한 관리 및 감독이 얼마나 엄격하게 이루어지는가에 따라서 그 범위가 다르겠지만 일본의 암호화폐법 규제를 통하여 자금 및 투기 사기 등의 리스크가 크게 경감될 것으로 예상하며 암호화폐 환전업계의 건전한 발전을 이끌 수도 있다.

지능정보화사회 도래를 대비하여 영향력이 크다고 판단한 교통 안전, 시설물 안전, 사회기반(금융) 안전 분야에서의 시장 및 정책 현황과 요소 기술을 분석하였다. 도출한 결과를 토대로 행정관리 및 법·제도 측면에서 리모델링 방향을 제시하여 새로운 안전관리체계의 효율성 강화와 안전관리 정책의 정합성 제고하였다. 마지막으로 각 분야별 국민 안전강화를 위한 기술적 발전방향과 행정 관리, 법령 및 제도 개선방안을 도출하여 신기술에 의한 사회변화에 적합한 안전관리체계 확립과 정책 구현에 대한 기초자료를 마련하였다.

주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.



[소프트웨어정책연구소]에 의해 작성된 [SPRI 보고서]는 공공저작물 자유이용허락 표시기준 제 4유형(출처표시-상업적이용금지-변경금지)에 따라 이용할 수 있습니다.
(출처를 밝히면 자유로운 이용이 가능하지만, 영리목적으로 이용할 수 없고, 변경 없이 그대로 이용해야 합니다.)