경제·인문사회연구회 협동연구총서 17-26-01
정보통신정책연구원 기본연구 17-11-01

초연결사회의 지속가능성을 위한 사회문화적 조건과 한국사회의 대응(III)

총괄보고서

손상영/이시직/오태원 외

2017. 12.

Korea Information Society Development Institute

KISDI 정보통신정책연구원
KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE

경제·인문사회연구회 협동연구총서 17-26-01
정보통신정책연구원 기본연구 17-11-01

초연결사회의 지속가능성을 위한 사회문화적 조건과 한국사회의 대응(III)

총괄보고서

손상영/이시직/오태원 외

2017. 12

KISDI 정보통신정책연구원
KOREA INFORMATION SOCIETY DEVELOPMENT INSTITUTE

경제·인문사회연구회 협동연구총서

“초연결사회의 지속가능성을 위한 사회문화적 조건과 한국사회의 대응(Ⅲ)”

1. 협동연구총서 시리즈

협동연구총서 일련번호	연구보고서명	연구기관
17－26－01	초연결사회의 지속가능성을 위한 사회문화적 조건과 한국사회의 대응(Ⅲ): 총괄보고서	정보통신정책연구원 경일대학교
17－26－02	초연결사회의 안전성과 사이버 복원력 확보를 위한 대책	정보통신정책연구원 상명대학교
17－26－03	초연결사회의 기술기반 창작도구의 활용에 따른 사회문화제도 고찰	정보통신정책연구원 대구대학교 마크로밀엠브레인(주)

2. 참여연구진

연구기관		연구책임자	참여연구진
주관 연구 기관	정보통신정책연구원	손상영 연구위원 (총괄책임자)	조성은 연구위원 이시직 연구원 김희연 부연구위원 양수연 연구원
협동 연구 기관	경일대학교	오태원 교수 (연구책임자)	-

서 언

글로벌-모바일-사물 커뮤니케이션 환경은 정보사회의 고도화를 넘어 초연결사회로의 근본적인 변화를 추동하고 있습니다. 초연결사회의 지속가능성을 위한 제반환경을 한 발 앞서 진단하고 이에 참여하는 플레이어들의 역할 및 사회변동에의 함의에 관한 심층적 접근이 필요한 시점입니다. 일부에서는 우리 사회의 준비가 연결의 속도와 양에만 집중하고 연결의 질에는 상대적으로 소홀해 '네트워크의 실패'를 보완할 장치를 마련하지 못한 채 초연결사회를 맞을 가능성이 있다는 우려도 있습니다. 따라서 초연결사회의 시스템 위험 및 사회조직과 구성원의 점증하는 불안에 주목하고 초연결사회로 가는 길에서 발생할 수 있는 새로운 문제에 대비함과 동시에 신뢰에 기반한 건강한 연결망을 갖춘 지속가능한 초연결사회로의 전환을 모색해야 할 필요가 있습니다.

본 연구는 3개연도로 기획되어 2015년부터 진행되었습니다. 3차 연도인 올해 연구의 결과는 총 3권의 보고서로 이루어졌습니다. 제1권은 총괄보고서로서 2개 세부과제별 연구결과를 종합적으로 정리하고 인공지능, 빅데이터와 같은 와해적 기술의 확산이 초래할 충격과 갈등을 수용하고 해소함으로써 초연결사회의 상부구조의 지속가능성을 담보할 수 있는 새로운 규범정립 방향을 제시하였습니다. 제2권은 "초연결사회의 안전성과 사이버 복원력 확보를 위한 대책" 연구로서 초연결사회의 정보 시스템들이 지속적인 외부 공격을 견디면서도 정상적으로 작동하는 초연결사회의 물리적 기반의 지속가능성을 확보할 수 있는 방안을 모색하는 연구를 진행하였습니다. 제3권인 "초연결사회의 기술기반 창작도구의 활용에 따른 사회문화제도 고찰" 연구는 새로운 기술이 열어가는 새로운 문화가 기존의 가치관과 조화를 이루면서 지속적으로 발전해 갈 수 있는, 즉 초연결사회의 새로운 문화의 지속가능성을 위한

사회문화제도를 모색하는데 기여할 것으로 생각합니다.

이러한 다학제적인 접근을 통해 초연결사회로의 전환에 대한 우리 사회의 준비사항 및 예상되는 부작용을 사전에 진단함으로써 지속가능한 커뮤니케이션 환경을 제안하고자 합니다. 또한 본 연구에서 다루는 다양한 주제들이 초연결사회의 도래에 따른 변화를 사전에 포착하는 데 도움이 되고 유연하고 통합적인 정책의 틀을 확보하는데 기여할 수 있을 것으로 기대합니다.

본 연구 보고서는 “초연결사회의 지속가능성을 위한 사회문화적 조건과 한국사회의 대응(Ⅲ) 총괄보고서”입니다. 본 연구는 정보통신정책연구원의 손상영 박사가 총괄책임을 맡아 수행하였고 조성은 연구위원, 이시직 연구원, 김희연 부연구위원, 양수연 연구원이 함께 수고해 주셨습니다. 함께 연구를 수행해주신 경일대학교 오태원 교수와 세부과제의 협동연구진 여러분께 감사드립니다. 협동연구기관의 연구책임자로 참여하여 초연결사회 사이버보안 교육프로그램 설계 연구를 함께 해주신 상명대학교의 유지연 교수와 공동연구진에도 감사를 드립니다. 무엇보다 각 전문분야의 연구기관과 연구진이 초연결사회의 지속가능성을 위한 사회문화적 조건과 한국사회의 대응연구에 참여하여 협동연구를 진행할 수 있도록 기회를 마련해 주신 경제·인문사회연구회에도 깊은 감사의 말씀을 드립니다. 끝으로 향후 이 보고서를 바탕으로 초연결사회와 관련된 학문적 성과가 축적되고 국민의 삶의 질 향상에 보탬이 되는 정책개발이 이루어지기를 희망합니다.

2017년 12월

정보통신정책연구원

원 장 김 대 희

목 차

표 목 차

그 림 목 차

제1장 서 론

제1절 연구의 배경 및 목적

1. 연구의 배경

글로벌－모바일－사물 커뮤니케이션 환경은 정보사회의 고도화를 넘어 초연결사회로의 근본적인 변화를 추동하고 있다(이호영 외, 2016). 초연결사회의 지속가능성을 위한 제반환경을 한 발 앞서 진단하고 이에 참여하는 플레이어들의 역할 및 사회변동에의 함의에 관한 심층적 접근이 필요한 시점이다(이호영 외, 2016). 이에 초연결사회의 시스템 위험 및 사회조직과 구성원의 점증하는 불안에 주목하고 초연결사회로 가는 길에서 발생할 수 있는 새로운 문제에 대비함과 동시에 신뢰에 기반한 건강한 연결망을 갖춘 지속가능한 초연결사회로의 전환을 모색해야할 필요가 있다(이호영 외, 2016).

본 연구는 사물인터넷(Internet of Things: IoT)과 빅데이터(Big Data), 인공지능(Artificial Intelligence) 등 초연결성에 의존한 기술이 전 사회로 확산되는 시대의 사회문화적 변동에 관한 관심으로부터 시작되었다(이호영 외, 2016). 이에 본 연구는 기술주도의 사회가 가져올 수 있는 유토피아 비전에 매몰되지 않고 초연결사회의 시스템 위험과 사회적 지배 문제 등에 대해 비판적인 관점에서 살펴보고 미래 사회의 순기능과 역기능을 종합적으로 검토하는 다학문적 연구로서 사회와 기술의 공진화적 관점을 견지하고 있다.

우리는 1, 2차연도 연구 결과를 통해 초연결사회의 지속가능성을 위해서는 이처럼 경제적 변화 이외에도 문화, 조직, 규범, 일자리 등 사회적 변화에 대한 고려가 반드시 필요하다는 것을 알게 되었다(이호영 외, 2016). 특히 지난 해 구글의 알파고가 이세돌 9단과의 대국에서 인공지능 알파고가 4승 1패로 승리한 이후, 초연결사회에

서 인공지능과 사물인터넷, 빅데이터 등 지능정보기술이 야기할 사회경제적 영향에 대한 분석과 4차 산업혁명에 대응한 정부의 역할이 무엇보다 중요해지고 있다.

이미 주요국들은 저상장이 고착화된 '뉴노멀(New Normal)시대'를 극복하기 위해 인공지능 등 소위 '지능정보기술' 기반의 4차 산업혁명을 통해 산업・경제 활성화를 도모하고, 나아가 사회, 법・제도 등 모든 영역에서 선제적으로 국가 차원의 전략 및 정책을 마련하고 있다(이시직, 2017). 우리나라도 지난 2016년 12월에 4차 산업혁명에 대응하여 기술, 산업 그리고 사회분야를 아우르는 '지능정보사회 중장기 종합대책'을 발표한데 이어, 올해 11월 '혁신성장을 위한 사람중심의 4차 산업혁명 대응계획'을 발표한 바 있다. 이처럼 정부는 기술기반의 거대한 구조변화 속에서 산업 인프라 및 생태계 조성 그리고 미래사회 변화에 대한 선제적 대응으로 4차 산업혁명을 혁신성장의 새로운 기회로 삼아야 한다.

초연결사회라는 것은 자발적인 연결, 나아가 자동화된 연결에 기초하는 것처럼 보이지만 당연히 주어진 '사회구조'를 반영하며 동시에 그 구조를 변화시키기도 한다(이호영 외, 2016). 다양한 해외 사례를 참조하는 것은 필수불가결하지만 더 이상은 캐치업 전략으로 성장하는 것이 불가능한 시대이기 때문에 기술적 환경과 우리에게 주어진 사회적 환경을 동시에 고려하는 발전 전략을 구사해야 하며 사물인터넷 등 초연결성을 제고하는 기술을 활용할 공동체의 직간접적 수요에도 관심을 기울여야 한다(이호영 외, 2016). 사회적 기술이자 와해적 기술(disruptive technology)로서의 인공지능, 사물인터넷, 빅데이터는 따라서 4차 산업혁명으로 인한 경제적 결과는 물론이고 사회적, 문화적 변동을 야기할 수밖에 없기 때문이다. 따라서 정부는 그 확산 속도와 강도, 그리고 기술이 주는 성장의 기회에 주목하면서도 사회의 준비 정도와 부대효과를 동시에 고려해야 한다(이호영 외, 2016).

이러한 이유로 본 연구는 초연결사회의 지속가능성에 초점을 맞추고 있다. 원래 지속가능성은 1972년 로마클럽이 발표한 '성장의 한계(The Limits to Growth)' 라는 보고서에서 언급된 이후 인간 활동, 경제나 경영, 기후와 환경, 국가정책 등에 광범위하게 사용되었다.[1] 최근 사회적 지속가능성은 개인, 지역공동체와 사회가 서로

함께 살아가는 방법과 관련이 있으며, 형평성, 의료보건 등 전통적인 사회정책 영역과 참여, 니즈, 사회적 자본, 경제, 환경, 그리고 행복과 삶의 질 등의 새로운 영역을 통합하고 있다(Colantonio and Dixon, 2009). 또한 지속가능성을 주요 가치로 추구하는 '사회ㆍ기술전환론(Socio-technical Transition)'에서 지속가능성이란 사회문제의 근본적 해결을 위한 시스템 자체의 개선을 의미하며, 그 효과의 중장기적 지속성을 의미한다(송위진, 2013). 본 연구는 사회적 지속가능성의 한 측면에서 와해적 기술들이 초래할 잠재력을 가진 경제사회적 갈등과 시스템 위험이 지속적으로 완화되고, 자율적인 인공물들이 사회적으로 수용되어 인간의 삶과 조화를 이루면서, 마침내 신기술의 발전이 지속적으로 사회 발전으로 이어지는 사회문화적 조건을 탐구한다.

2. 연구의 목적

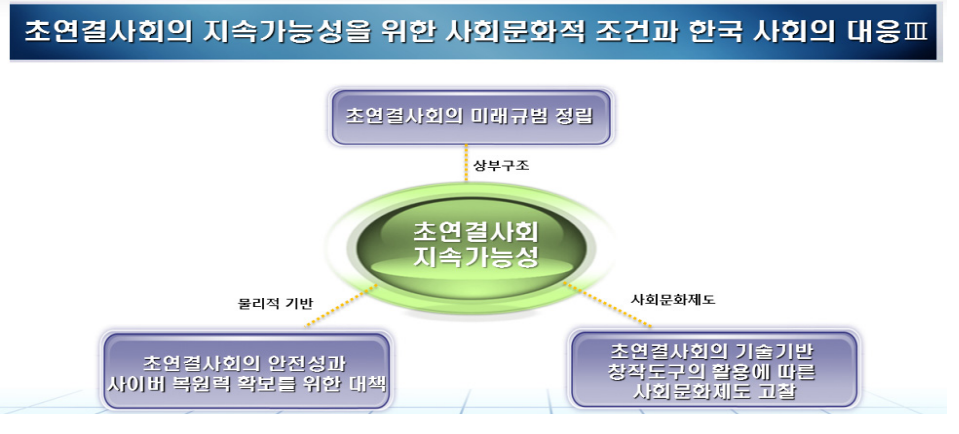
본 연구는 초연결사회로의 전환에 대한 우리 사회의 준비사항과 예상되는 부작용을 사전에 진단함으로써 지속가능한 커뮤니케이션 환경과 사회적 삶의 조건들을 제안하고자 한다(이호영 외, 2015). 이를 위해 사물인터넷, 빅데이터, 인공지능 등 초연결성에 의존한 기술이 전 사회로 확산되는 초연결사회의 기술변동의 파급력에 관한 사회경제적, 문화적 분석을 기반으로 관련 ICT전략을 마련하고자 한다. 또한 센서와 엑추에이터가 모든 지식과 정보, 공간, 사물을 연결시킬 새로운 네트워크 환경에서 기술의 안정성과 사회의 지속가능성의 조건을 인문사회과학적인 관점에서 검토하고 특히, 초연결사회의 단계로 접어든 한국 사회가 간과하고 있는 사회적, 문화적,

1) 그 중에서도 가장 주목받은 사례를 들자면, 1987년 세계환경발전위원회(World Commission on Environment and Development: WCED)는 성장 일변도로 치달아온 산업화로 인해 환경오염 및 파괴가 심각해지는 상황을 타개해나가는 전략적 대응방안을 논의하기 위해 『우리공동의 미래(Our Common Future)』라는 보고서를 내면서 '지속가능한 발전'이란 "미래 세대의 욕구를 충족시킬 수 있는 능력을 위태롭게 하지 않으면서 현 세대의 욕구를 충족시키는 발전"이라고 정의했는데 이는 많은 이론의 여지에도 불구하고 가장 보편적인 개념으로 받아들여지고 있다(윤순진, 2002).

법적 문제점을 검토하고 이에 대한 정책적 시사점을 도출하고자 한다.

특히, 3차 연도 연구에서는 초연결사회의 지속가능성을 공통분모로 삼고 새로운 상부구조(규범), 물리적 기반, 사회문화제도를 모색함으로써 사회 각 부문의 균형발전 및 지속가능한 성장을 위한 정책방향을 제시함을 목적으로 한다. 이를 위해 첫째, 대표적인 규범이론인 목적론적 윤리론, 의무론적 윤리론, 정의론을 초연결사회를 구성하는 각 계층(C-P-N-D)에 적용한 결과를 바탕으로 인간중심의 초연결사회를 구현하기 위한 미래규범 정립방향을 제시한다. 둘째, 항시적인 사이버 보안 위협에 대응하여 시스템 작동 중에도 시스템을 보호하고 필수 기능을 유지할 수 있도록 인공지능을 활용하는 방안과 필요한 솔루션들을 결합하는 방안을 제시하고, 국가 차원의 사이버 복원력 확보를 위해 국가 사이버 복원력 기반의 개념을 제시하고 관련 기관들의 협력 및 네트워킹 방안을 제안하고자 한다. 셋째, 사이버 위험에 대응하기 위해 기술위주의 보안대책이 아닌 보편적 시민을 대상으로 한 사이버 보안교육의 정책방향을 도출하고, 나아가 사이버보안위협 및 이슈에 대응하면서도 국내 교육환경에 적절한 한국형 사이버보안 교육체계를 제시한다. 넷째, 초연결기술 환경이 문화영역에 미치는 영향을 고려하여 디지털 콘텐츠의 유통, 이용, 창작에서의 새로운 정책 및 제도적 개선방안을 도출하고자 한다.

〔그림 1－1〕 3차연도 연구목표

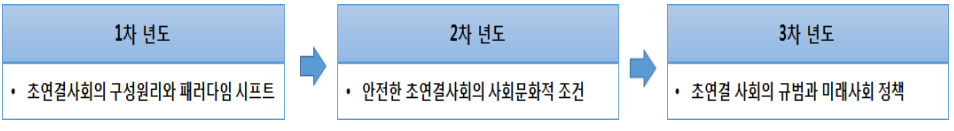


제 2 절 연구사업의 내용과 추진체계

1. 연구사업의 내용

본 연구는 센서와 액추에이터가 모든 지식과 정보, 공간, 사물을 연결시킬 새로운 네트워크 환경에서 기술의 안정성과 사회의 지속가능성의 조건을 인문사회과학적 관점에서 연구하고자 3개년 프로젝트로 기획되었다(이호영 외, 2015).

〔그림 1－2〕 전체 연구사업의 추진 내용



1차연도(2015년)에는 스마트 디바이스의 전면화와 무선통신의 질적 수준 제고에 따른 전방위 연결(All-connected) 사회가 어떤 양상을 띠고 우리 사회에 나타나며 사회조직 원리의 기본 축을 어떤 방식으로 재편하는지에 대한 광범위한 조사와 구조분석을 통해 초연결사회의 구성 원리와 미래상에 대해 연구하였다(이호영 외, 2015). 2차연도(2016년)에는 초연결사회를 위한 정치, 경제, 사회, 문화 각 영역의 준비 정도와 초연결사회의 안정성과 신뢰성 제고를 위한 사회문화적 조건에 관해 연구한 후, 3차연도(2017년)에는 초연결사회의 규범과 관련된 제반 사회적 이슈 및 지속가능한 초연결시대를 위한 미래사회의 정책을 구상하고자 한다(이호영 외, 2015).

구체적으로 3차연도(2017년)인 올해 연구는 3개년 프로젝트의 마지막 연구로서 총 3개의 과제로 나누어 진행된다. 먼저, 첫 번째 연구인 총괄보고서에서는 기존 1, 2차연도의 연구결과를 종합정리하고, 3차연도 연구의 기본방향을 설정한다. 또한 고도화된 초연결사회의 기술 환경변화에 따라 사회규범적 패러다임 전환도 함께 요

청되고 있는 바, 2차연도에서 논의한 ‘초연결사회에서의 법・제도 이슈’를 토대로 규범이론 분석을 통해 초연결사회의 미래규범 정립방향을 제시한다.

두 번째 “초연결사회의 안전성과 사이버 복원력 확보를 위한 대책 개발” 연구에서는 최근 초연결사회에 대비하는 세계적인 추세에 따라서 초연결사회의 안전성과 신뢰를 위협하는 새로운 위협 요인들에 대한 대책 및 안전한 초연결사회로의 이행을 위한 사회문화적 조건을 충족시키기 위한 정책방안을 마련한다. 이를 위해 구체적으로 초연결사회에 적합한 보안 및 프라이버시 보호 정책을 개발하고, 구미 주요 기관의 사이버 복원력 시스템을 비교분석하여 국가차원에서 사이버 복원력 시스템 기반 구현을 위한 정책과제를 제시하며, 초연결사회의 기본적 소양으로서 정보보안 교육 추진전략을 개발한다.

세 번째 “초연결사회의 기술기반 창작도구 활용에 따른 사회문화제도 고찰” 연구에서는 초연결사회의 기술 환경이 문화 영역에 미치는 영향을 살펴보고 그에 대응하기 위한 제도의 개선 방향에 대한 시사점을 제시한다. 이를 위해 초연결사회의 기술 환경에 따른 디지털 콘텐츠의 유통·소비 이슈에서부터 최근의 창작 이슈까지, 그와 관련한 문화현상과 각국의 정책방향, 법리적 논쟁 등을 고찰하여 초연결사회의 지속가능성을 모색한다. 특히 초연결사회가 지능화 단계로 진화하면서 최근 인공지능 기반 창작물에 대한 이슈가 제기된 것에 주목하고 이에 대한 각국의 정책 방향과 법리적으로 수용가능한 방안, 전문가 의견 조사 등을 통해 향후 사회적 논의 방향의 지침을 제시한다.

2. 연구사업의 추진체계

본 연구 사업은 ICT 및 디지털 사회정책분야의 전문성과 연구의 체계성을 확보하고자 전문성을 갖춘 대학, 연구소 등과 공동연구를 추진하였다. 정보통신정책연구원은 “초연결사회의 지속가능성을 위한 사회문화적 조건과 한국 사회의 대응(III)” 과제의 총괄 연구기관으로서 본 연구 결과를 도출하는 과정에서 보다 입체적인 논의와

함의를 도출하기 위해 연구협력회의, 워크숍, 중간보고 및 최종보고회를 개최하는 등 협동연구진과 유기적인 네트워크를 형성하여 지속적인 의견교류 및 연구진행상황을 점검하는 한편 전문가 간담회, 세미나, 토론회 등을 다수 개최하여 각 계 전문가로부터 본 협동연구의 타당성 및 연구결과에 대한 검증과정을 거쳤다.

〈표 1－1〉 연구수행기관의 역할

구분	담당	내용
연구총괄	정보통신정책연구원	– 협동연구과제 총괄기관으로 융합연구주제 선정, 범위, 구성 체계, 주요 이슈 등을 설정 – 협동연구진과 유기적인 네트워크를 형성하여 본 연구 결과를 도출하는 과정에서 보다 입체적인 논의와 함의를 도출
협동연구	세부과제별 전문연구기관 및 과제자문위원과 협동연구	– 상명대학교 산학협력단을 비롯한 협동연구기관 및 과제자문위원은 KISDI가 제시한 각 세부 연구내용과 관련하여 해당기관 및 전문가의 전문성을 충분히 발휘하여 연구에 참여

3차 연도 협동연구과제의 추진체계는 다음 〔그림 1－2〕와 같다.

〔그림 1－3〕 3차연도 협동연구과제 추진체계

구체적으로 ‘초연결사회의 미래규범 정립방향’ 연구는 초연결사회에서 상부구조(규범)의 지속가능성을 담보할 수 있는 새로운 규범과 윤리를 모색하기 위하여 법철학 및 규범이론 전문가인 경일대학교 오태원 교수팀과 함께 규범이론 분석을 통한 초연결사회의 미래규범 방향을 모색하였다.

둘째, ‘초연결사회의 안전성과 사이버 복원력 확보를 위한 대책 개발’ 연구는 2차 연도에서 도출한 사이버보안 교육의 중요성과 정규 교육화 필요성에 대한 연구 결과를 수용하였다. 이에 정보통신정책연구원은 사이버보안 교육에 대한 전문성을 보유한 상명대학교 산학협력단 유지연 교수팀(사이버보안 전공)과 함께 사이버보안 교육 프로그램의 기본 틀을 기획하고 교육 내용의 적합성에 대해서 함께 검토하였다.

셋째, ‘초연결사회 기술기반 창작도구 활용에 따른 사회문화제도 고찰’ 연구는 초연결사회 기술 환경이 문화영역에 미치는 영향을 살펴보고 그에 대응하는 제도적 개선 방향을 제시하고자 하였다. 이를 위해 디지털 콘텐츠의 유통, 이용, 창작에서의 새로운 현상과 정책, 법리적 논쟁 등을 고찰한다. 제도 개선은 법리적 합리성과 밀접하다는 점에서 대구대학교 법학과 최진원 교수팀과 협업하여 현실적으로 합리적인 정책 시사점을 도출하고자 하였다.

이러한 과정을 통해 확보된 결과는 지속가능한 초연결사회에 대해 인문－사회과학적 입장에서 접근할 수 있는 기반을 마련하고, 그 사회문화적 영향력을 가늠하여 국지적 공간을 넘어서 지속가능한 초연결사회를 만들어가는 중장기적 정책방향을 마련하는데 이바지할 것으로 기대된다(이호영 외, 2015).

제 2 장 선행연구 검토 및 금년 연구방향

제 1 절 1・2차연도 연구결과 종합[2)]

본 연구는 2015년부터 2017년까지의 3년 연구 중 마지막 연도의 연구에 해당한다. 본 장에서는 지난 2년 동안 수행한 연구 결과를 간략하게 정리하고 금년 연구 방향에 대해서 기술한다.

1. 1차연도 연구의 주요내용 및 결과

1차연도 연구(2015)는 초연결사회로의 전환에 대한 우리 사회의 준비사항과 플랫폼 기업에 의한 승자독식, 데이터리치와 데이터푸어 사이의 양극화 문제, 개인정보 보호와 프라이버시 문제, 보안 및 연결의 안전성 등 '네트워크의 실패'를 사전에 대비할 방안을 모색하였다(이호영 외, 2015). 이를 위해 초연결사회가 만들어내는 사회구조의 변동과 정체성의 변화, 특히 연결의 양적 폭발이 낳는 효과 등을 복잡계 이론, ANT 이론 등을 이용하여 분석하고, 인터넷 이용자에 대한 설문조사와 전문가 인터뷰 등을 통해 사물인터넷에 대한 기대와 우려를 동시에 파악하였다(이호영 외, 2015).

먼저, 1차연도 첫 번째 연구 주제인 '초연결사회의 복잡계적 특성' 연구에서는 먼저, 사물인터넷, M2M과 같은 개념들이 사물들과 기계들 간의 연결만을 의미했던 반면, 인간, 사물, 기계가 모두 연결되는 초연결사회를 정의내리고 초연결사회에 대한 각계의 전망을 소개하고, 초연결사회의 네트워크적 특성을 이론적으로 검토하였

2) 1, 2차연도 연구의 결론을 중심으로 본 보고서의 맥락에 맞게 재정리하였다.

다(이호영 외, 2015).

1차연도 두 번째 연구 주제인 ‘커넥티드 사회의 구조변동’ 연구에서는 모든 것이 연결되는 커넥티드 세상에서 연결의 크기와 빈도, 강도가 변함에 따라 그 안에서 살게 되는 사람과 사회가 겪게 될 구조적 변동을 설명하였다(이호영 외, 2015). 이를 위해 사물인터넷 환경에서 인간 존재에 대한 성찰을 통해 사회구성 논리의 변화가 인간, 사회, 세계 구성에 미치는 영향과 의미에 대한 심층적 이해를 시도하였다(이호영 외, 2015). 본 연구에서는 새로운 기술의 도입과 진화로 인해 사적 자아의 차원에서, 공동체 차원에서, 그리고 사회적 차원에서 어떠한 유의미한 변화 및 재구성이 진행되는지에 관한 거시적 조망을 제공하였다(이호영 외, 2015). 특히, 커넥티드 사회의 사회경제적 구조변동 중 플랫폼 경제, 플랫폼 비즈니스로 대변되는 네트워크 비즈니스는 수확체증의 법칙이 존재하는 비즈니스로, 수확체증이 존재하는 비즈니스, 산업 또는 시장에는 승자독식과 독점이 존재한다는 점을 주목할 필요가 있다(이호영 외, 2015). 승자독식 사회에서 선점, 변화와 혁신의 중요성을 되새겨볼 때 새로운 초연결 IT 산업이 발전할 수 있도록 글로벌 경쟁에 맞는 법과 규제체제를 개편하고, 자국의 기업에 변화와 혁신의 기회를 열어주는 것을 정부의 과제로 제시하였다(이호영 외, 2015).

1차연도 마지막 연구 주제인 ‘지속가능한 초연결사회를 위한 준비’ 연구에서는 먼저, 초연결사회로의 전환기에 사회 각 분야는 무엇을 준비해야 하며 어떻게 대비해야 하는가를 생각해야 하는 상황에서 다른 나라들이 초연결사회에 어떻게 대비하고 있는지 파악하였다(이호영 외, 2015). 또한 앞서 검토한 해외 사례를 바탕으로 사물인터넷의 도입에 따른 초연결사회의 미래사회 이슈로 사라지는 일자리 문제, 기술사회적 엔지니어링, 양극화로 인한 시민 공간의 상실, 디지털 디바이드의 중층화, 인간능력의 쇠퇴와 인공지능의 인간화, 프라이버시 문제 등을 다루었다.

이를 종합하여 지속가능한 초연결사회를 위한 다음과 같은 정책적 시사점을 제시하였다. 첫째, 초연결사회의 도래와 함께 시작된 연결의 폭발적 증가에만 주목할 것이 아니라 연결의 구조와 시스템에 관심을 기울여야 한다(이호영 외, 2015). 둘째,

사물인터넷은 복잡계적 특성으로 인해 승자독식으로 나아가기 쉬우며 네트워크 외부성으로 인해 후발자에게 불리한 시장을 형성하는 경향이 있는데 이러한 '네트워크 실패'를 교정하기 위해 정부는 노력해야 한다(이호영 외, 2015). 셋째, 사물인터넷의 공공성에 대한 이해를 높여야 하고, 넷째, 사물인터넷은 거시적 사회문제에 대한 대응은 물론이고 미시적인 사회문제나 현안에 대한 해결을 위해 적극적으로 동원되어야 한다(이호영 외, 2015).

2. 2차연도 연구의 주요내용 및 결과

2차연도 연구(2016)에서는 기술철학 및 미디어철학을 포함하여 사회학, 경제학, 커뮤니케이션학, 법학 등 다양한 학문적 영역에서 논의되고 있는 사물인터넷과 빅데이터 기반의 초연결사회에 대한 관점들을 담아내고자 했다(이호영, 2016).

먼저, 2차연도 첫 번째 연구 주제인 '연결된 사물의 세계: 사물인터넷의 철학적, 사회과학적 이해' 연구에서는 최근 테크놀로지의 발전에 힘입어 우리 사회가 '초연결 사회'로의 진입을 눈앞에 둔 시점에서 사물 인터넷을 중심으로 사물 또는 기기 사이의 연결이 갖는 철학적, 사회과학적 함의를 논의하고자 하였다(이호영 외, 2016). 이른바 '연결된 사물의 세계'에 대한 이해를 위해서는 사물이란 무엇인가, 연결 또는 관계란 무엇인가, 인간과 사물 사이의 관계는 어떠한가와 같은 철학적인 질문들에 대한 답을 출발점으로 삼아, '연결 사회'에서 '초연결 사회'로의 이행을 사회과학적 관점에서 전망하였다(이호영 외, 2016). 구체적으로 사물의 개념, 그리고 사물과 사물 사이의 관계가 갖는 의미를 논의하고, 사물 인터넷이 이끄는 사회 변화의 경향을 몇 가지 하위영역으로 나누어 고찰하였다(이호영 외, 2016).

2차연도 두 번째 연구 주제인 '안전한 초연결사회의 사회문화적 조건'에 대해서 논의하는 중에 연구진은 초연결사회의 안전성을 구성하는 주요 요소로서 사이버보안에 주목하였다. 이에 따라 세부과제 중 하나는 초연결사회에서 사이버보안 역량을 강화하기 위한 사회문화적 조건들을 탐구해 보기로 했다. 그 주요 내용은 다음과

같다. 초연결사회의 사이버보안은 크게 기술적 차원, 조직적 차원 그리고 사회문화적 차원으로 구분해서 논할 수 있다. 우선 기술적 차원의 논의는 〈표 2-1〉로 요약된다.[3)]

〈표 2－1〉 초연결사회 사이버보안 기술

기술 분야	대응 기술 또는 대책
물리적 IoT 보안	차폐(shielding), 적발용 센서 설치 등 간섭방지(anti-tampering), security-by-obscurity, masking 또는 투입(input) 데이터의 무작위화 등
디바이스 위의 정보보안	AES(Advanced Encryption Standard),해시함수(Hash functions), ECC(Elliptic Curve Cryptography) 비대칭 키에 의거한 시그너처 체제 사용 데이터의 최소화
관측될 수 없는 통신	proxy chain을 이용한 네트워크 익명화 TOR(The Onion Router)
정책 관리 기반 접속 제어	SecKit(The Security Toolkit) 보안규칙 원형(template): 사건(Event)－조건(Condition)－조치(Action)의 규칙들로서 조치 부분은 허용, 거부, 수정, 지연 등의 집행 행위
IoT 클라우드에서 정보보안	Verifiable computing homomorphic signatures, message authentic codes redactable and sanitizable signatures
정보 보안을 위한 인공지능	인공면역체계(Artificial Immune system) 침입탐지 및 제거체계(Intrusion Detection and Prevention System) 인공신경망(Artificial Neural Networks)

출처: 손상영 외(2016) pp. 32-41을 재구성.

다음으로 조직 차원에서의 사이버보안 논의는 다음과 같다. 초연결 세계에 대한 침입은 가장 취약한 지점에서 이루어지기 때문에 취약한 지점들을 강화시켜주는 것이 중요하다. 따라서 일부가 정보보안을 등한시하면 그 영향이 다수의 건전한 부분에도 미치기 때문에, 초연결 세계의 정보보안은 모든 구성원이 함께 보조를 맞추어 실행해야 한다. 이와 같은 실행에 있어서 최고 경영진의 역할이 중요하다. 최고 경

3) 자세한 내용은 손상영 외(2016) pp. 32-41 참조.

영진은 사이버 위험에 대비하는 것이 조직의 생존과 번영에 핵심적인 업무임을 항상 명심하고 구체적인 사이버 위험관리 프로그램을 개발해서 실전에 대비한 훈련을 실행해야 하며 이것이 사이버 복원력으로 확대 내지는 진화되도록 해야 한다. 앞서 언급한 바와 같이 초연결 세계의 모든 구성원이 보조를 맞추기 위해서는 모두가 사이버 복원력의 원칙과 지침을 공유하고 함께 준수해야 한다(손상영 외, 2016: 89). 또한 사회문화적 차원에서 사이버보안 논의는 초연결사회의 각 주체별로 최선 행동과 사회문화적 조건에 초점이 맞추어졌다. 그 주요 내용은 〈표 2-2〉로 요약된다.[4)]

〈표 2－2〉 초연결사회에서의 최선 행동과 사회문화적 조건

참여 주체	최선 행동	사회문화적 조건
하드웨어 제조자	하드웨어가 제공하는 사양을 최소화	다양한 화려한 사양에 대한 욕구는 자제
솔루션 개발자	모든 단계에 걸쳐 정보 보안을 유념하고 구현	소형 디바이스에서 발생할 수 있는 속도 지연의 문제를 고려해서 설계되어야 하며 솔루션 이용자도 정보 보안을 위해서 기다리고 인내
솔루션 운영자	일반 사용자들을 설득해서 자발적으로 정보 보안업무에 참여	일반인을 대상으로 하는 사이버 보안교육의 도입
사용자	모든 사용자가 예외 없이 사이버 보안교육을 충실히 받고 정보 보안업무에 참여	사이버 보안수준의 상향평준화

출처: 손상영 외(2016).

2차연도 세 번째 연구 주제인 ‘네트워크를 통한 창의적 협력과 탈경계의 문화확산’ 연구는 초연결사회 기술 인프라를 통해 구현할 수 있는 문화 영역의 생활 서비스에 대한 가능성을 고찰하고 향후 초연결사회 기술 인프라를 십분 활용하는 문화생활을 위해 지금 무엇을 해야 하는지에 대한 시사점을 도출하였다. 세부 연구내용을

4) 자세한 내용은 손상영 외(2016) pp. 71-82 참조.

보면, 먼저 초연결사회의 기술 인프라에서 도시의 각 요소들을 연결, 도시 전체를 게임 공간화하는 유럽의 시범 프로젝트를 검토하였고, 국내 스마트시티 시범도시로 선정된 서울시와 대구시의 스마트시티 전략 사례를 조사하였으며, 그 결과들을 종합하여 초연결사회 도시문화생활에 대한 잠재성을 고찰하였다. 또 데이터 기반의 문화 기획 및 제작 사례, e-Tourism에서 스마트관광으로 진화하는 기술 기반 관광문화 고찰 등을 통해 초연결사회 생활문화의 진화상을 살펴보았다. 그리고 설문조사를 통해 초연결사회의 생활문화상에 대한 이용자의 수용태도를 분석하였다. 그 결과들을 종합하여 향후의 생활문화상의 원활한 수용을 위해 현재 무엇에 중점을 두어야 하는지에 대한 시사점을 도출하였다. 그 내용은 데이터 활용이 일상화한 사회환경 조성, 스마트시티 전략에 고려되어야할 디지털 문화생활 프로젝트 등이다.

2차연도 네 번째 연구 주제인 '초연결사회에서의 법・제도적 이슈 및 개선방안' 연구에서는 초연결환경에서의 정보보호 패러다임 변화에 따라 제기되는 현행 정보보호법・제도상의 문제점을 검토하고 개선방안을 도출하는 한편 미래성장동력으로서 사물인터넷 산업・서비스 활성화를 저해하는 규제이슈 및 대응방안을 살펴보았다(이호영 외, 2016). 먼저, 초연결환경에서 제기되는 현행 법・제도상의 문제점으로는 크게 5가지로 나눌 수 있다. 첫째, 초연결환경에서 사물인터넷 서비스는 단일 사업자가 아닌 다양한 유형의 주체가 해당 서비스를 제공하므로 개인정보처리자의 법적 책임소재가 불분명해 진다. 둘째, 수많은 개인정보처리자들에 의해 수집된 다양한 유형의 정보들이 공유 및 활용되는 사물인터넷 환경에서는 이용자 스스로 자신의 개인정보가 수집 및 이용되고 있음을 인식하기 어렵거나 수집목적과 최소한의 범위 내에서 잘 처리되고 있는지 확인하기가 쉽지 않다(이호영 외, 2016). 나아가 기업들도 이용자에게 사물인터넷 환경에서 수집되는 개인정보의 수집・이용 목적, 항목, 이용 및 보유기간 등을 명확히 고지하여 동의를 받거나, 이 중 변동사항이 발생할 때마다 새롭게 개별적인 동의를 받는다는 것이 사실상 불가능하다(이호영 외, 2016). 셋째, 기업이 정보주체의 개인정보를 비식별 조치를 하더라도 정보주체는 해당 기업이 보유한 다른 정보와의 결합을 통해 재식별화될 가능성은 없는지, 사물인

터넷 가치사슬에 관계된 다양한 사업자들 모두가 비식별화 조치를 통해 활용하고 있는지 여부 등을 명확하게 확인하기 힘든 측면이 있어 실질적인 개인정보자기결정권 보장에도 한계가 발생한다(이호영 외, 2016). 넷째, 사물인터넷, 클라우드 컴퓨팅, 빅데이터 등의 등장으로 국경 간 개인정보의 이전과 유통은 더욱 증가할 수 밖에 없는 상황에서 개인정보 관련 유출이나 정보주체 권리침해 등의 사고가 국경 간 발생할 경우 정보주체의 피해구제, 이에 따른 분쟁조정 등이 어려우며 일부의 경우 외교적 분쟁으로도 확대될 수 있다(김범수 외, 2014). 다섯째, 현재 사물인터넷의 진흥 및 규제와 관련한 통합적인 단일법이 부재한 상황에서 사물인터넷 분야는 기존 산업 및 서비스에 ICT가 융합되는 특성 상 해당 사업이나 서비스를 규율하는 분야별 다양한 개별규제들의 적용을 받는다(이호영 외, 2016). 이와 관련하여 먼저, 개인정보보호법제의 개선사항으로는 개인정보의 개념과 범위를 명확히 하고, 사전적・개별적 동의방식에서 정보주체의 사후적 통제권이 보장된 묵시적・포괄적 동의방식으로 전환하는 한편 개인정보의 국외이전을 위한 판단기준이 마련될 필요가 있다고 주장하였다(이호영 외, 2016). 또한 현행「정보통신융합특별법」상 신속처리 및 임시허가 제도의 개선방안으로는 신속처리 신청 사유를 명확히 하고, 임시허가 유효기간 내 소관부처의 본 허가 규정 마련을 의무화하는 한편, 임시허가 심사절차에 소관부처 소속 공무원의 참여를 의무화하도록 제안하였다(이호영 외, 2016).

2차연도 다섯 번 째 연구 주제인 ‘초연결 기술과 직업세계의 관련성’에서는 초연결사회에서 기술 발전과 이로 인한 자동화가 가져올 수 있는 직업의 미래에 대한 국민적 관심을 반영하여 전문가들을 대상으로 하는 델파이 조사를 통해 초연결 기술과 관련한 일자리 전망을 조사 분석하였다(이호영 외, 2016). 직업지표를 통해 전도가 유망하면서 일자리가 증가하는 직업들의 특성들을 적시함으로써 구체적이고 신뢰할 만한 결과를 도출하였다(이호영 외, 2016). 분석 결과 초연결 기술은 일차적으로 직업세계의 양적인 변화에 큰 영향을 미치며 향후에는 직업세계의 질적 변화를 주도해갈 것으로 예측되었다(이호영 외, 2016). 창업까지를 고려한다면 초연결 기술이 절대적인 일자리 감소를 가져오는 극단적 상황은 연출되지 않을 것이지만 전반적으로는 일

자리의 증가보다는 감소 쪽으로 영향력이 더 클 것으로 예상되었다(이호영 외, 2016). 분석 결과는 질적으로는 더 좋은 일자리가 초연결 기술과 관련하여 등장할 것으로 내다보고 있지만 궁극적으로 일자리의 양극화를 피하기는 어려울 것으로 예측하고 있다(이호영 외, 2016). 따라서 정부는 이러한 직업 전환과 일자리 감소라는 과도기적 상황의 피해가 사회적 약자에게 집중되지 않도록 인력 양성, 직업 전환, 사회안전망 등의 정책 수단을 적극적으로 도입하여야 할 것이다(이호영 외, 2016).

제 2 절 타 선행연구과제와의 차별성 검토

본 연구와 타 선행연구과제의 차별성은 〈표 2-3〉과 같이 검토 및 정리하였다.

〈표 2－3〉 타 선행연구과제와의 차별성

구 분	선행연구와의 차별성		
	연구목적	연구방법	주요 연구내용
주요 선행연구	- 과제명:The promise and peril of hyperconnectivity for organizations and societies - 연구자(연도):Fredette, J. et al. (2012) - 연구목적: 기술발달이 가져온 기업조직과 시회의 초연결성에 대한 탐색	- 문헌연구	- 기업 조직과 현대 사회에 초연결성이 미치는 긍정적, 부정적 영향에 대한 고찰 - 초연결성에 대한 여섯 가지 주요 특성에 대해 범주화
	- 과제명: Impact of Global Hyperconnectivity and Increased Smartphone Usage on the Delivery and Structure of IT Organizsation in Transport Logistics - 연구자(연도): Linke, M..(2013) - 연구목적: IT 기술발달에 따른 글로벌 초연결 효과 연구	- 문헌연구	- IT와 상품, 서비스가 추동하는 초연결에 대한 전 지구적 현상에 대한 논의 - IT 기술발달에 따라, 사람, 공간, 상품, 기술 등 각각의 차원이 초연결상태를 전 지구적 확산에 대한 탐구

구 분	선행연구와의 차별성		
	연구목적	연구방법	주요 연구내용
	- 과제명:Social Inclusion in a Hyperconnected World - 연구자(연도): Carter, M., et al. (2013) - 연구목적: 초연결 세계에서의 사회적 포섭 현상 탐색	- 문헌연구	- 기존의 digital divide 논의를 넘어 IT 발전이 평행적 현실(parallel reality)를 실현시켰음을 주장 - 초연결세계에서 정보, 기관, 사람에 의한 즉각적인 접근적 특성은 공개된 디지털 세계에서 참여의 확장을 가능하게 함
	- 과제명:Emerging Issues for our Hyperconnected World - 연구자(연도): Biggs, P. (2012) - 연구목적: 초연결 세계에 발생하는 이슈 검토	- 문헌연구	- 인터넷과 연결된 디바이스의 급속한 증가로 사물인터넷의 중요성과 이를 기반한 초연결세계에서의 사회변화에 대한 연구
	- 과제명:The Hyperconnected World: A New Era of Opportunity - 연구자(연도): Akamai Technologies, Inc. (2013) - 연구목적: World Economic Forum, 2012 Insight Report	- 문헌연구 - 정책연구 - 사례연구	- ICT에 기반한 새로운 초연결사회의 도래에 대한 현황분석 및 관련한 미래정책 논의 - 초연결 사회에서 기업이 새로운 마켓에 적응하기 위한 정책적 대안제시
	- 과제명: 창조적 가치연결, 초연결사회의 도래 - 연구자(연도): 윤미영·권정은(2013) - 연구목적: 새로운 패러다임으로서의 초연결사회에 대한 탐색	- 문헌연구	- 미래의 새로운 패러다임으로서의 초연결사회에 대한 동향분석 - 초연결사회의 새로운 모습과 이를 실현하는 핵심 기술 탐색
	- 과제명: 초연결 시대로의 변화와 대응 방향 - 연구자(연도): 김현중(2012) - 연구목적: 초연결 시대에 대한 문헌연구를 통해 미래대응전략마련	- 문헌연구 - 정책연구	- 초연결시대의 변화 동인과 IT의 변화, 핵심가치와 역량을 분석하고 정책적 대응마련
본 연구	- 본 연구는 센서와 액추에이터가 모든 지식과 정보, 공	- 문헌 조사 - 서베이 조사	- 1차연도(2015년)에는 스마트 디바이스의 전면화와 무

구 분	선행연구와의 차별성		
	연구목적	연구방법	주요 연구내용
	간, 사물을 연결시킬 새로운 네트워크 환경에서 기술의 안정성과 사회의 지속가능성의 조건을 인문사회과학적 관점에서 연구 - 본 연구는 기술주도의 사회가 가져올 수 있는 유토피아 비전에 매몰되지 않고 초연결사회의 시스템 위험과 사회적 배제 문제 등에 대해 비판적인 관점에서 살펴볼 것이며 미래 사회의 순기능과 역기능을 종합적으로 살펴보는 다학문적 연구로서 사회와 기술의 공진화적 관점을 견지함 - 정치학/행정학, 경제학, 사회학, 문화연구 등을 아우르는 학제적 연구 - 개별분과 학문 차원의 다양한 연구방법론을 미래정책연구와 유기적으로 결합	- 이용자 심층면접 조사 - 전문가(개발자) 델파이 조사	선통신의 질적 수준 제고에 따른 All-connected 사회가 어떤 양상을 띠고 우리 사회에 나타나며 사회조직 원리의 기본 축을 어떤 방식으로 재편하는지에 대한 광범위한(extensive) 질적 조사와 구조 분석을 통해 초연결사회의 구성 원리와 미래상에 대해 연구 - 2차연도(2016년)에는 초연결사회를 위한 정치, 경제, 사회, 문화 각 영역의 준비 정도와 초연결사회의 안정성과 신뢰성 제고를 위한 사회문화적 조건에 관해 연구 - 3차연도(2017년)에는 초연결사회의 규범과 관련된 제반 사회적 이슈 및 지속가능한 초연결시대를 위한 미래사회 정책 구상을 통해 초연결사회의 도래에 따른 새로운 정책이슈들을 개발하고 대안을 제시한 점이 선행연구와의 차별성이 있음

제 3 절 금년 연구의 기본방향

본 연구는 3개연도로 기획되어 2015년부터 진행되었다. 금년 3차연도 연구의 기본방향 및 주요내용은 다음과 같다.

우선, 제3장에서는 지난 2차연도 연구에서 분석한 초연결사회에서 제기되는 법률적 이슈를 바탕으로 대표적 규범이론인 목적론적 윤리론, 의무론적 윤리론 그리고

롤즈의 정의론을 초연결사회의 특성에 적용하여 그 결과를 바탕으로 초연결사회의 미래규범은 어떠한 방향을 지향하여야 하는지를 모색하고자 한다. 이를 위해 초연결사회를 분석하는 틀로써 각 계층(C-P-N-D)에 규범이론을 적용한 결과를 바탕으로 초연결사회를 규율할 규범형식과 기본원칙을 도출하고자 한다.

제4장에서는 초연결사회에 대비하는 세계적인 추세에 따라서 초연결사회의 안전성과 신뢰를 위협하는 새로운 위협 요인들에 대한 대책 및 안전한 초연결사회로의 이행을 위한 사회문화적 조건을 충족시키기 위한 정책방안을 마련하고자 한다. 이러한 목표하에 본 연구는 초연결사회에 적합한 보안 및 프라이버시 보호 정책, 초연결사회의 정보보안 교육 추진 전략, 사이버 복원력 시스템 구현을 위한 정책과제를 제시하고자 한다.

제5장에서는 초연결사회의 기술 환경과 연결하여 디지털 콘텐츠의 유통·소비 이슈에서부터 최근의 창작 이슈까지, 그와 관련한 문화현상과 각국의 정책방향, 법리적 논쟁 등을 고찰하여 초연결사회의 지속가능성을 모색하고자 한다. 문화 영역에 영향을 미치는 핵심 제도를 저작권으로 보고 지금의 저작권 제도가 어떤 방향으로 어떻게 개선되어야 초연결사회의 안정적 정착에 기여할 수 있을지를 고찰하는 것이다. 특히 초연결사회가 지능화 단계로 진화하면서 최근 인공지능 기반 창작물에 대한 이슈가 제기된 것에 주목하고 이에 대한 각국의 정책 방향과 법리적으로 수용가능한 방안 등을 분석한다. 또 전문가 의견조사를 거쳐 인공지능 기반 창작물에 대한 제도적 수용을 어떤 방식으로 처리할 것인지에 대한 사회적 논의 방향의 지침을 제시한다.

이상에서 소개한 3개의 세부과제는 초연결사회의 지속가능성을 공통분모로 삼고 있다. 초연결사회의 미래 규범을 다루는 첫 번째 과제는 인공지능, 빅데이터와 같은 와해적 기술의 확산이 초래할 충격과 갈등을 수용하고 해소함으로써 초연결사회의 상부구조의 지속가능성을 담보할 수 있는 새로운 규범과 윤리를 모색한다. 두 번째 과제는 초연결사회의 정보 시스템들이 지속적인 외부 공격을 견디면서도 정상적으로 작동하는 초연결사회의 물리적 기반의 지속가능성을 확보할 수 있는 방안을 모

색한다. 세 번째 과제는 새로운 기술이 열어가는 새로운 문화가 기존의 가치관과 조화를 이루면서 지속적으로 발전해 갈 수 있는, 즉 초연결사회의 새로운 문화의 지속가능성을 위한 사회문화제도를 모색한다.

제 3 장 규범이론 분석을 통한 초연결사회의 미래규범 정립방향 모색

제 1 절 논의의 배경

디지털 네트워크를 통하여 모든 사람과 사물이 연결되어 상호작용하는 초연결사회는 인터넷이 개발되면서 정보사회로 변화를 시작하는 때에 이미 예상된 미래라고도 할 수 있다. 하지만 막상 초연결사회로 빠르게 진보하는 현대 사회에서 우리는 어떤 사회규범을 준비해야 하고 그것은 어떤 방향을 지향해야 하는지에 대한 논의는 다소 지체되고 있는 것이 사실이다. 더군다나 인공지능에 대한 폭발적인 관심으로 인하여 미래 정보사회의 가장 중요한 기반이라고 할 수 있는 초연결사회에 대한 규범적 논의는 인공지능과 관련된 규범논의에 비해 상대적으로 적었다. 본 장에서는 초연결사회에서 과연 우리가 어떤 규범을 생각할 수 있는지, 그 규범은 어떤 방향으로 정립해야 할 것인지에 대하여 논의해보고자 한다.

먼저 초연결사회의 기본 성격에 대하여 알아본다. 본 연구의 대상으로 하는 초연결사회의 개념은 무엇이고 어떻게 구성된 사회인지 탐구함으로써 초연결사회의 특성을 파악할 수 있다. 특히 초연결사회가 정보통신 기술 등 첨단 기술을 바탕으로 구현되는 사회인 만큼 초연결사회를 구성하는 주요 기술과 그것들의 상호관계를 분석함으로써 초연결사회의 전체적인 특성을 파악할 수 있을 것이며, 그에 어울리는 규범이론을 생각해볼 수 있다.

이어서, 1차연도에서 연구한 초연결사회의 특성에 대표적인 규범이론을 적용해보고자 한다. 규범이론으로는 윤리이론의 대표적 두 이론인 목적론적 윤리론과 의무론적 윤리론, 그리고 롤즈의 정의론을 초연결사회에 적용해보고자 한다. 물론

이 외에도 아리스토텔레스, 샌델의 정의론이나 법경제학적 윤리이론과 같이 다른 규범이론을 적용해볼 수 있으나 가장 전형적인 규범이론으로 논의를 한정하고자 한다.

마지막으로, 초연결사회 특성에 대한 규범이론의 적용결과를 바탕으로 초연결사회는 어떠한 규범형식으로 구체화되어야 하는지, 그 규범 설정 시 고려해야할 기본원칙과 주요내용은 무엇인지에 대하여 논의한다.

제 2 절 초연결사회의 개념 및 주요특징[5)]

1. 초연결사회의 개념

초연결사회가 일의적으로 규정될 수 없음은 이미 잘 알려져 있다. 초연결사회를 구성하는 기술에 중점을 두고 초연결사회를 정의하기도 하며, 인간과 인간간의 정보와 사상의 연결을 중시하는 사회적 개념으로서 초연결사회를 정의하기도 한다. 일단 근원적 개념을 먼저 살펴볼 필요가 있다. '초연결'이라는 용어는 캐나다 사회과학자인 Anabel Quan-Haase와 Barry Wellman에 의해 시작된 용어[6)]라고 알려져 있으나, 실제로는 2000년대 중반 이후 인터넷 솔루션기업인 시스코에서 사물인터넷의 기술적 기반 위에 제시한 미래 사회상으로서 초연결사회를 언급하고, 세계경제포럼에서 2012년 처음 논의된 이후 매년 주요 안건으로 다뤄지면서 본격적으로 정부와 학계의 관심을 끌게 되었다는 의견도 있다(이호영 외, 2015). 용어의 시작에 대한 논란에 비하여 초연결에 대한 설명은 대동소이하다. 일반적으로 초연결이란 네트워크를 통해 사람-사람, 사람-사물, 사물-사물이 연결되어 커뮤니케이션 할 수 있는 상태를 말한다고 정의한다. 이러한 초연결성은 기존과 다른 사회서비스를

5) 본 절은 초연결사회의 미래규범 방향을 논하기에 앞서 독자들의 이해를 돕기 위해 1차연도 연구결과를 바탕으로 재구성하였다.

6) 위키백과(http://en.wikipedia.org/) (검색일: 2017.5.7.).

만들어내고 이를 통해 새로운 문화와 가치를 형성해 나가는 기반이 된다고 한다. WEF의 2012년『글로벌 IT 리포트(Global Information Technology Report)』는 초연결사회는 다음과 같은 여섯 가지 주요 속성을 가진다고 요약하였다. 첫째, 항상 연결된 상태(Always on), 둘째, 상시적 접근가능성(Readily accessible), 셋째, 개개인의 소비 능력을 뛰어넘는 정보풍요(Information rich), 넷째, 상호작용성(Interactive), 다섯째, 사물인터넷으로 대표되는 사람을 넘어서는 연결(Not just about people)이라고 한다(이호영 외, 2015). 즉, 초연결사회는 네트워크를 통해 사람-사람, 사람-사물, 사물-사물이 연결되어 커뮤니케이션 할 수 있는 사회로서 항상 연결되어 접근가능하고 풍요로운 정보와 다양한 상호작용이 이루어지는 사회라고 정의할 수 있을 것이다.

2. 초연결사회의 특징

물론 이러한 현상중심의 초연결사회에 대한 정의는 가장 일반적으로 초연결사회를 표현하고 있기는 하지만 초연결사회의 구체적인 특성을 모두 보여주고 있지는 못하다. 발전된 정보통신기술을 바탕으로 하고 있는 초연결사회의 특성을 구체적으로 분석하기 위해서는 초연결사회를 구성하고 있는 기술들에 대하여 알아보아야 할 것이다. 초연결사회를 구성하는 것이라고 대표적으로 논의되는 기술들은 센서, 모바일, 클라우드, 빅데이터를 들 수 있다. 이른바 4차 산업혁명의 한 축이라고 일컬어지는(심진보 외, 2017) 초연결사회에서는 인간뿐만 아니라 사물에도 컴퓨팅 파워가 접목되고 인터넷을 기반으로 모든 객체가 연결됨으로써 사람과 사물의 운영프로세스가 고스란히 저장ㆍ관리되게 된다고 표현된다(박정은 외, 2014).

초연결사회가 매우 기술에 의존하여 파생된 사회라는 점에는 크게 이견이 없을 것이다. 그렇다고 해서 초연결사회가 완전히 기술결정론[7]적인 사회라고 보기는 어

7) 기술결정론은 기술이 사회에 미치는 영향에 초점을 두고 기술이 자율적인 작동 방식을

렵다. 현대사회에서 크게 주목받는 공유와 활용의 사회적 가치를 생각한다면 그러한 기술의 진보를 가져온 근원에는 사람들의 사회적 욕구가 충분히 반영되었다고 보아야 한다. 물론 이 또한 완전한 사회구성론[8]을 의미하는 것은 아니다. 기술과 사회의 상호작용에 의해 기술이 사회변화를 이끌기도 하고 사회수요에 의해 기술이 진화하기도 한다고 보아야 한다.

여기에서 초연결사회의 복잡성의 첫 번째 근원을 찾을 수 있다. 웨어러블 디바이스의 경우를 생각해 보자. 반도체 기술의 발전으로 인한 고집적 반도체의 가격하락과 센서의 가격하락, 무선통신 기술의 발전 등은 웨어러블 디바이스의 탄생을 가져왔다. 스마트폰이라는 물리적 플랫폼도 중요하게 작동하였다. 그렇다고 웨어러블 디바이스가 기술의 발전만을 바탕으로 개발되었는가를 생각해본다면 그렇지 않다는 것을 알 수 있다. 대부분의 웨어러블 디바이스는 사회의 수요에 맞추어 개발되었고, 수요에 부응하지 못한 디바이스는 빠르게 소멸되었다. 물론 그 반대로 완전히 새로운 기술이 사회적으로 새로운 수요를 창출하는 경우도 있다. 결론적으로, 기술이 사회의 변화를 이끄는 경우와 사회의 수요가 기술을 진화시킨 경우에 대하여 복합적으로 분석할 필요가 있다.

가지고 오직 자체적인 내부 작동 원리에 의해 발전한 다고 가정한다(Smith and Marx, 1994).

8) 기술은 사회의 모습/관계를 설명하고 구현하는 수단이라고 보고 사회가 기술에 미치는 영향에 대하여 주목하여 사회가 자율적인 작동원리가 있다고 설명힌디(MacKenzie and Wajcman, 1985).

제 3 절 초연결사회와 규범이론

1. 초연결사회와 목적론적 윤리론[9)]

목적론적 윤리론은 공리주의를 바탕으로 하여 이른바 '최대 다수의 최대 행복'을 추구하는 가치관이다. 대부분의 기술은 '최소 비용으로 최대 효과'라는 효율성을 바탕으로 최대 행복을 추구하는 목적론적 윤리론에 기반하고 있다고 할 수 있다. 초연결사회를 구현하는 필수 기술들의 경우에도 마찬가지이다. 항상 연결되어 있음으로써 정보를 전달하기 위하여 소요되는 비용을 절감하고 많은 사람들이 누리게 함으로써 행복의 최대를 추구한다고 할 수 있다. 또한 많은 데이터를 바탕으로 하여 보다 좋은 서비스를 가능하게 함으로써 행복치를 증대하고자 한다.

기술이 대부분 공리주의적이니 초연결사회는 목적론적 윤리론에 입각한 공리주의 사회라고 단순하게 결론내리기는 어렵다. 초연결사회에서도 '소수의 희생을 바탕으로 한 다수의 폭리 문제'와 같이 목적론적 윤리론이 해결하지 못하는 문제가 발생할 수 있기 때문이다. 최소의 비용을 추구하는 기술이 사회 전체적 공리를 증대시켰지만 소수를 외면하거나 소수의 인권을 침해하는 현상이 나타날 수 있다. 사회적으로 초연결사회의 지속가능성을 논의하고, 프라이버시 보호의 문제, 승자독식의

9) '의무론'이라는 용어는 영국의 철학자 브로드(Broad, C. D.)가 윤리 이론들을 크게 두 가지로 구분하여 의무론적 이론과 목적론적 이론으로 부른 데서 비롯하였다. 그에 따르면, 의무론적 이론은 어떤 종류의 행동이 언제나 어떤 종류의 환경에서 그 행동의 결과와 상관없이 옳거나 그르다고 주장하는 이론이다. 목적론적 이론은 행위의 옳고 그름은 언제나 본래적으로 좋거나 나쁜 어떤 결과들을 낳게 될 그 경향성에 의해 결정된다고 주장하는 이론이다. 목적론적 윤리란, 말 그대로 우리가 추구하고 또 추구해야 할 어떤 궁극적인 목적이 있음을 전제하는 윤리인데, 그 궁극적인 목적은 넓은 의미로는 행복이고 좁은 의미로는 쾌락이다. 여기서는 최선의 결과를 가져오는 행위가 선하고 옳은 행위이다. 반면, 의무론적 윤리란, 우리가 추구해야 할 어떤 궁극 목적보다는 언제 어디서나 지켜야 할 행위의 근본원칙에 주목하는 윤리이다. 예를 들어 행복과 의무가 충돌할 경우, 목적론자는 행복 쪽을 선택한다면 의무론자는 의무 쪽을 선택한다고 볼 수 있다.

문제, 기울어진 운동장의 문제 등을 논의하는 것은 단순히 공리주의적 윤리론이 전체를 해결하지 못한다는 것을 이미 인식하고 있기 때문이라고 할 수 있다.

2. 초연결사회와 의무론적 윤리론

의무론적 윤리론으로 가장 대표적으로 설명되는 이론은 칸트의 윤리론이다. “너의 의지의 준칙이 보편적 입법의 원리에 타당하도록 행동하라”는 칸트의 도덕법칙은 합리적 이성을 바탕으로 가장 합당한 행동을, 즉 의무를 파악할 수 있으며 인간은 그 의무를 행하여야 하며, 또한 할 수 있다는 것이다. 또한 기술과 사회의 관계를 중심으로 보았을 때 매우 중요한 칸트의 두 번째 도덕법칙이 있는데 이는 “네 자신에게나 다른 사람에게 있어서 인격을 언제나 동시에 목적으로 대우하고 수단으로 대하지 말라”는 것이다.

기술 자체가 의무론적이냐를 묻는다면 이는 상당히 어리석은 질문이 될 것이다. 기술 자체는 대부분 기본적으로 효율성을 추구하기 때문이다. 그러나 기술이 추구하는 방향이 어떠한지를 묻는다면 이는 충분히 논의해볼 수 있게 된다. 기술은 결국 인간이 개발하는 것이며 그 기술을 개발하는 인간이 어떠한 목적으로 그 기술을 개발하는지, 기술의 작동 과정에서 어떠한 점을 고려하는지를 생각한다면 의무론적 윤리론이 초연결사회에 여전히 그 의미를 가지고 있음을 알 수 있다. 초연결사회를 구현하는 기술들이 과연 인간을 수단으로 대하고 있는지, 인간을 목적으로 대하고 있는지에 대하여 성찰해본다면 초연결사회의 미래규범에 대한 아이디어를 생각해낼 수 있다.

3. 초연결사회와 롤즈의 정의론

롤즈의 정의론은 자연권 이론의 바탕이 된 고전적 사회 계약 이론을 일반적 논변 형식으로 발전시켜 정의관을 제시하고 있다(존 롤즈, 2015). 롤즈는 정의의 원칙들을 평등한 최초의 입장에서의 합의의 대상으로 여기고 있다. 롤즈는 이러한 방식을

공정으로서의 정의라고 부르고 있다(김정오 외, 2017).

원초적 입장은 '무지의 베일(veil of ignorance)'에 싸인 상태로서 일정한 정의관에 이르게 하도록 규정된 순수한 가상적 상황이다(존 롤즈, 2015). 원초적 입장이 가진 본질적 특징은 ① 각각의 개인이 자신의 특수한 사실을 알지 못하며, ② 각각의 개인은 합리적이고 상호 무관심하다는 것이다(존 롤즈, 2015). 자신의 특수한 사실을 알지 못한다는 것을 무지의 베일이라고 하며, 이러한 특징은 원초적 입장을 공정하게 만들어준다(존 롤즈, 2015). 이 때문에 순수 절차적 정의로서 공정으로서의 정의라는 말이 성립한다(존 롤즈, 2015). 결국 원초적 입장에서의 합의는 공정한 것이 된다(존 롤즈, 2015). 각각의 개인이 합리적이며 상호 무관심하다는 것은 서로 타인의 이해관계에 관심이 없으며, 자신의 이익을 위해 노력한다는 것으로 이해되어야 한다(존 롤즈, 2015). 즉 개개인은 타인에 대한 시기심 때문에 자신의 이익을 무시하는 행위를 하지 않는다(존 롤즈, 2015).

이러한 원초적 입장에서 정의의 두 원칙을 채택하게 된다(존 롤즈, 2015). 제1원칙은 기본적 권리와 의무의 할당을 평등하게 요구하는 원칙이며, 제2원칙은 사회적 경제적 불평등의 허용은 사회의 최소 수혜자에게 그 불평등을 보상할 만한 이득을 가져오는 경우에만 정당하다는 것을 주장한다(존 롤즈, 2015). 따라서 어떤 불평등이 불운한 사람의 처지를 개선한다면, 그로 인해 소수의 사람이 더 큰 이익을 취하는 것은 정당하게 된다(존 롤즈, 2015). 그러나 전체적인 선을 증대시킨다고 해도 평등한 기본적 권리를 침해하는 제도는 부당하다(존 롤즈, 2015). 왜냐하면 정의의 두 원칙은 제1원칙을 제2원칙보다 우선한다는 것을 인정하고 있기 때문이다(존 롤즈, 2015).

의무론적 윤리론과 마찬가지로 초연결사회를 구현하는 기술들이 롤즈의 정의론에 입각하여 정의로운지를 분석하는 것은 어려울 것이다. 그러나 초연결사회가 과연 정의로운가의 문제는 다르다. 초연결사회가 기술 기반의 사회라고 해서 그 사회가 정의롭지 않아도 된다고 생각하지는 않기 때문이다. 사회적 약자를 위한 웨어러블 디바이스 기술의 개발, 개인의 프라이버시권 보호, 평등한 정보 이용 기회의 보

장 등 이미 논의되고 있는 초연결사회 관련 문제를 보아도 초연결사회를 구현함에 있어서 롤즈의 정의론에 입각한 정의로운 초연결사회를 위한 노력이 필요하다는 것을 쉽게 인식할 수 있다.

제 4 절 초연결사회에 대한 규범이론의 적용

1. 초연결사회와 계층 모형

초연결사회에 규범이론을 적용하기 위해서는 초연결사회의 필수적인 기술들을 구분할 필요성이 있다. 단순하게 사물인터넷이라고 표현하지만 거기에는 매우 다양한 기술들이 복잡하게 작동하고 있기 때문이다. 간단하게 생각해보더라도, 사물이 작동하는 기술(데이터가 생성되는 기술), 통신하는 기술(데이터가 전송되는 기술), 데이터가 분석되는 기술, 데이터가 활용되는 기술 등 단계에 따라서 적용되는 기술이 다를뿐더러 그 특성도 다르다. 따라서 이를 효과적으로 분석하려면 계층 모형(Layer Model)을 적용할 필요가 있을 것이다. 여기에서는 계층 모형 중 CPND 모형을 적용해보고자 한다. 물론 CPND 모형은 계층을 구분하는 모형보다는 ICT 또는 사물인터넷의 패러다임 또는 생태계라고 표현된다(최계영, 2012; 최창현, 2014; 정법근, 2015). 우선 CPND로 구분하는 것이 초연결사회에서 데이터가 생성, 전송, 분석, 활용되는 단계에 대하여 적절히 구분하고 있기 때문에 초연결사회의 기술과 규범을 연결하는 데에 좋은 선긋기를 해주고 있다. 또한 CPND 생태계라고 표현되는 바에서 볼 수 있는 것처럼 기술적이나 분석적으로 이렇게 나누어지기는 하지만 서로 긴밀하게 상호작용할 수밖에 없으며 궁극적으로 하나의 사회(생태계)를 구성한다는 점에서 초연결사회를 분석하는 틀로 적절하다고 생각한다.

먼저 웨어러블 디바이스에 대한 기술과 사물인터넷의 물리적 부분에 대한 영역은 가장 기본 계층인 디바이스 계층(Device Layer)이 적용될 것이다. 사물인터넷의 통

신영역과 클라우드 및 빅데이터의 통신영역은 네트워크 계층(Network Layer)에 적용될 수 있을 것이다. 사물인터넷과 클라우드 등의 운영체제 및 상호운용과 연결된 부분은 플랫폼 계층이 될 것이다. 마지막으로 빅데이터를 비롯하여 인공지능 등 데이터를 분석하고, 활용하는 부분은 콘텐트 계층(Content Layer)이라고 할 것이다. 이렇게 각각의 계층으로 나누어지는 기술들이 복합적으로 작동하여 초연결사회가 구현되는 것이기 때문에 초연결사회를 한마디로 표현하기도, 초연결사회를 관통하는 가치나 규범을 도출하기도 어렵다. 오히려 계층을 나누어 파악하게 되면 각 계층에서 주도적으로 작동하는 가치나 규범이 다를 수 있다는 것을 이해할 수 있으며 보다 실제적인 미래규범을 생각해낼 수 있다.

2. 디바이스 계층(Device Layer)

디바이스 계층에는 웨어러블 디바이스 기술이 대표적으로 적용될 것이며, 사물인터넷의 물리적 부분도 여기에 상당부분 포섭될 수 있다. 디바이스 영역에서 초연결사회의 진화방향은 어떠할 것인가 생각해보자. 가트너(Gartner)의 초연결 시대의 ICT 기술변화 트렌트 전망(윤미영 외, 2013)을 보면 ① 인간 능력 향상: 웨어러블을 주축으로 한 기술 발달은 육체, 감성, 인지 분야에 걸친 인간의 능력치 향상에 기여, ② 인간 대체형 기계: 고위험군 또는 단순 반복작업의 신속한 처리를 통해 생산성 증대, ③ 인간-기계 간 협업: 기계가 지니는 생산성, 속도라는 장점과 인간의 감성지능과 문제해결 능력을 결합하여 작업 효율 극대화의 방향으로 기술이 발전되어 갈 것으로 전망하고 있다.[10]

기술변화 방향의 설명만을 단순히 보면 이는 최대 다수의 최대 행복치를 높이기 위한 방향으로 보일 수 있다. 기술은 기본적으로 효율성을 바탕으로 최대 행복치를 추구하기 때문에 어찌 보면 당연하게 보일 것이다. 그러나 디바이스 관련 기술들은

10) 그 외에 ④ 인간과 환경에 대한 기계 이해 증진, ⑤ 기계에 대한 인간 이해 증진, ⑥ 기계와 인간의 스마트화 등이 있다.

기본적으로 인간을 향하고 있음을 간과해서는 안 된다. 웨어러블 디바이스의 안전성의 문제나 웨어러블 디바이스가 송출하는 데이터의 프라이버시 문제 등 인간의 기본적인 권리를 침해해서는 안 된다는 것이다. 이는 인간을 수단이 아닌 목적으로 대해야 한다는 칸트의 도덕률에서 파생한다고 보는 것이 더 적절할 것이다. 또한 장애인이나 고령자 등 사회적 약자를 위한 웨어러블 디바이스 기술 개발(엄주희, 2017)의 경우 공리주의적 윤리관에만 의존한다면 기술 개발이 이루어지지 않을 수도 있다. 물론 현재에도 사회적 약자를 위한 디바이스의 개발이 이루어지고 있지만 이 또한 상대적으로 수익성을 기대할 수 있는 고령자를 대상으로 하는 경우가 많고 수요가 적은 디바이스에 대한 개발은 활발하게 이루어지고 있지 못하다. 초연결사회에서 인간의 특정 능력을 보완하거나 대체하는 디바이스가 그러한 능력에 대한 장애가 있는 사람을 장애가 없는 사람과 동등한 사람으로 만들어줄 수 있다는 점을 고려한다면, 롤즈의 정의론에 입각하여 정의로운 초연결사회를 구현하려는 노력이 있어야 하고, 이는 사회적 약자를 위한 웨어러블 디바이스의 개발 등으로 이어질 수 있다.

기술적인 측면에서는 사물인터넷으로 대변되는 초연결사회는 사물인터넷이 실시간 수집하고 처리하는 데이터와 인공지능을 이용하여 인간이 처해 있는 복잡성의 세계에서 고도의 최적화가 이루어진다. 그런데 이러한 최적화는 인간의 제어 범위를 벗어나 지능을 가진 기계의 자율성에 맡겨지는 경우가 흔히 발생하게 되면서 인간은 의사결정 과정에서 제외되어 사회의 주체로서의 존재방식을 상실할 위험에 처하게 된다. 한 사회에서 인간의 자율성과 주체성의 상실은 인권의 존중마저 위태롭게 되어 궁극적으로 우리의 민주주의 사회가 심각한 위협을 받을 수도 있다. 따라서 인간과 기계의 협업에 있어서도 칸트의 도덕률이 중요한 윤리 원칙으로 적용되어야 하며, 기계가 인간의 역할을 대체하는 것이 아니라 인간의 부족한 점을 보완하여 인간이 더 커다란 성취를 이루어 초연결사회에서 더욱 굳건한 자율적 주체로 발전하도록 인간을 지원하도록 관련 기술이 발전해 나가야 한다.

두 번째로 어떤 규범이 작동할 것인가에 대한 질문을 던져야 한다. 물리적 계층

(Physical Layer)으로 분류하는 이론에 입각한다면 디바이스 계층인 웨어러블 디바이스 및 사물인터넷의 물리적 영역에는 우선 제조물과 관련된 법리가 중심적으로 적용된다. 실체가 있는 디바이스에 대한 규율이니 기본적으로 법규범에 의할 것이다. 그러나 정말 법규범만으로 모든 사안을 해결할 수 있을 것인가에 대한 의문은 여전히 남는다. 특히 국경의 의미가 매우 약해지는 ICT 환경에서 법적 관할권을 넘는 문제에 대하여 범규범만으로 모든 사안을 해결하기는 어려울 것이다. 예를 들어 스마트폰으로 사진을 촬영할 때 촬영음이 나도록 강제되어 있는 규범을 생각해보자. 이는 이른바 '몰카'를 방지하기 위한 규범으로 우리나라에서 강제되고 있다. 그러나 우리나라를 제외한 대부분의 국가에서 스마트폰에서 사진을 촬영할 때 촬영음이 나도록 강제하고 있지 않다. 해외에서 판매되는 스마트폰을 구매하여 사용한다면 실효성이 없는 규범이 되고 마는 것이다.[11] 더군다나 앱스토어에는 카메라 무음앱이 얼마든지 있어서 누구나 원한다면 무음으로 촬영할 수 있다. 카메라 촬영음을 강제하는 규범이 실효성이 떨어지는 잘못된 규범이라고 결론을 내리려고 하는 것이 아니다. 초연결사회에서 디바이스에 대한 법규범적 규율이 반드시 모든 사안을 해결할 수 있는 것은 아니며, 이와 관련된 인터넷 윤리에 대하여 복합적으로 생각해야 한다는 것이다.

정리하자면 먼저 초연결사회의 디바이스 계층에서 미래 규범은 단순히 목적론적 윤리론에만 의존하는 것이 아니라 인간을 목적으로 대하는 의무론적 윤리론과 롤즈의 정의론이 복합적으로 작동하는 방향으로 정립되어야 할 것이다. 특히 디바이스를 통하여 장애가 극복될 수 있는 분야와 같이 디바이스가 장애 여부, 연령, 성별 등의 차이와 관계없이 평등한 사회를 구성하는 데 도움을 주는 분야에 롤즈의 정의론에 입각한 규범의 정립이 필요하다. 또한 규범의 형태에 있어서도 물론 법규범이 주도적인 역할을 하겠지만, 해외에서 개발, 제작된 디바이스가 우리 법규범에 따라 정상적인 수입과정을 거쳐서 들어오는 것이 아니라 얼마든지 '직구'될 수 있다는 점을

11) 연합뉴스, "카메라 셔터 소리 싫어서... 아이폰 해외 직구매 는다." 2016.5.16.

고려하여 인터넷 윤리를 통한 규율에 대하여 고민하여야 한다.

3. 네트워크 계층(Network Layer)

네트워크 계층에는 사물인터넷 중 통신 기술, 클라우드 기술 등이 포섭될 것이다. 물론 사물인터넷 기술은 네트워크와 웨어러블 디바이스가 중첩되는 부분이 있어서 인간과 접목되는 부분이 있겠지만 여기에서는 순전히 네트워크 영역에서의 문제로 국한하기로 한다. 또한 네트워크 외부성이나 기울어진 운동장 이론 등 네트워크의 실패라 불리는 문제(이호영 외, 2015)는 네트워크라 표현되기는 하지만 네트워크 계층에서 말하는 망으로서의 네트워크라기보다는 연결로 인한 영향으로서의 네트워크이므로 그 다음에서 설명할 플랫폼의 문제라고 보는 것이 타당하다.

여기서 네트워크 계층은 개념상 인간과의 접점이 없기 때문에 기본적으로 목적론적 윤리론에 입각한 효율성과 최대 행복을 추구하면 될 것이다.[12] 즉 성능의 향상, 저비용 고효율, 안정적 기능 등이 추구될 것이다. 초연결을 위해서 수많은 네트워크의 연결과 확장이 필요하며, 유선망 도매제공제도가 이를 위한 하나의 해결책으로 제안되는 것도 이러한 맥락에서 이해할 수 있다(김병운 외, 2015). 유선망 도매제공제도가 고려해야 하는 기존 사업자의 투자 유인 요소, 효율적인 사업자의 진입 유도 방법을 볼 때 공리주의적 윤리관으로 충분히 해석할 수 있다. '망 중립성' 논의와 같이 다소 의무론적으로 보이는 문제도 있지만, 이 또한 경쟁의 활성화를 통하여 결과적으로 공리의 증진을 추구하는 목적론적 윤리론으로 충분히 해석될 수 있을 것이다.

네트워크 계층을 주도하는 규범은 법규범이라고 보아야 한다. 망 자체가 국내에 존재하는 것으로 법규범의 관할권 범주 안에 들어오는 것으로 분석된다. 또한 행위규제 요소의 측면에서 '시장원리'가 가장 크게 작동하겠지만 이 시장원리를 조정하

12) 네트워크 계층에서 목적론적 정의론과 배치되는 전통적 규범으로 보편적 접속(universal access)을 들 수 있다. 그러나 보편적 접속은 초연결사회의 이슈는 아니므로 여기서 다루지는 않는다.

는 것은 결국 법규범이기 때문에 법경제학적 논증을 하지 않더라도 쉽게 이해될 수 있다. 물론 네트워크에는 프로토콜과 같이 '코드'라는 규범요소가 작동하는 영역이 분명 존재한다. 그러나 이러한 코드가 범규범이 추구하는 방향이나 가치와 배치되는 경우를 찾기는 쉽지 않을 것이다. 특정한 코드에 의하여 네트워크 시장의 불균형이나 왜곡이 발생할 수 있겠지만 이는 네트워크의 문제라기보다는 플랫폼의 문제라고 보아야 하기 때문이다. 결론적으로 네트워크 계층은 4가지 계층 중 가장 명쾌하게 규율될 수 있는 영역으로 목적론적 윤리론에 입각한 법규범이 주요한 규범정립 방향이라고 하겠다.

4. 플랫폼 계층(Platform Layer)

초연결사회에서는 플랫폼의 중요성은 매우 커지며 이에 대한 경쟁력을 확보해야 한다는 논의(류한석, 2016; 김대호 외, 2015)는 많았던 반면에, 플랫폼 계층의 규범문제는 지금까지 활발히 논의되고 있지는 못하지만 초연결사회로의 진행이 가속화될수록 중대한 문제로 등장할 가능성이 크다. 네트워크 계층은 사물인터넷과 빅데이터, 클라우드가 연결되는 영역이라고 할 수 있는 반면 플랫폼은 그 형태가 매우 다양하게 나타나는 만큼 정확하게 어떤 부분이라고 규정할 수 있는 것은 아니지만 데이터의 생성과 활용이 연결되는 과정에서 작동하는 프로그램 영역 또는 단계라고 할 것이다.

플랫폼 계층의 규범적 문제는 플랫폼 기술의 발전을 효율성에 입각한 시장원리에 맡겨둘 경우 지배적 플랫폼의 영향력이 지속적으로 강대해져서 법을 뛰어넘는 코드에 의한 지배가 이루어질 가능성이 높다는 것이 핵심이다. 퍼스널 컴퓨터 및 프로그램 시장에서 마이크로소프트가 OS를 바탕으로 구축한 플랫폼의 영향력이 얼마나 강대한지, 애플이 구축한 플랫폼의 영향력이 얼마나 강해지고 있는지를 생각한다면 쉽게 이해할 수 있다. 더군다나 초연결사회에서 사물인터넷은 복잡계적 특성으로 인해 승자독식으로 나아가기 쉬우며 네트워크 외부성으로 인해 후발자에게 불리한

시장을 형성하는 경향이 있다(이호영 외, 2015). 이는 부분적으로 네트워크 자체의 선호적 연결과 유유상종 효과에 기인하는 것으로 이를 네트워크의 실패라고 부를 수 있다(이호영 외, 2015). 복잡계적 특성이 아니더라도 사물인터넷의 4원칙(커넥팅랩, 2014) 중 2원칙인 '모든 사물은 표준어로 소통해야 한다'라는 것을 생각한다면, 초연결사회에서 플랫폼은 필수불가결한 것이고, 이로 인하여 승자독식의 문제, 불평등의 문제, 참여자의 선택의 제한 문제가 발생할 수밖에 없는 구조라는 것이다. 이러한 문제는 목적론적 윤리론이나 의무론적 윤리론, 롤즈의 정의론 중 어느 것을 적용하여도 옳지 않은 것으로 분석될 것이다. 결국 플랫폼 계층의 규범문제는 어떤 규범으로 이를 규율할 수 있는가의 문제이다.

1차적으로 법규범에 의한 규율이 있어야 할 것이다. 대부분의 연구에서 플랫폼 문제의 해결책으로서 정부의 역할을 강조(이호영 외, 2015; 커넥팅랩, 2014)하는 것도 결국 범규범의 필요성을 인식하고 있는 것이라고 볼 수 있다. 시장 경쟁이 공정하게 이뤄질 수 있도록 정부가 제대로 감시하면서 불공정 행위에 대해 적시에 적절한 조치를 취한다면, 독과점으로 인해 발생하는 문제를 최소화할 수 있을 뿐만 아니라, 새로운 경쟁자가 등장할 수 있는 토대를 마련할 수 있다(커넥팅랩, 2014). 2차적으로는 제작자 윤리 또는 코드에 대한 관심과 노력이다. 마이크로소프트가 구축한 플랫폼도, 애플이 구축한 플랫폼도 우리 법규범의 관할권을 넘는 것이다. 그 플랫폼을 기반으로 개발되고 유통되는 코드들은 일차적으로 그 플랫폼에 맞추어 개발되는 것이지 우리의 법규범에 맞추어 개발되는 것이 아니다. 이른바 윤리적 코드에 대한 관심과 노력이 병행되어야 플랫폼의 규범문제를 해결할 수 있다.

정리하자면, 플랫폼 계층의 규범문제는 어떤 규범이론을 적용하는가의 문제라기보다는 어떤 규범의 형태를 중시하느냐의 문제라고 분석된다. 1차적으로는 공정한 시장 환경을 조성하기 위한 법규범의 역할, 즉 정부의 역할이 요구될 것이며, 2차적으로는 공정 경쟁을 지향하는 인터넷 윤리와 코드가 발전되고 강화될 수 있도록 관심과 노력이 요청된다.

5. 콘텐트 계층(Content Layer)

콘텐트 계층에는 빅데이터 기술, 각종 프로그램과 애플리케이션, 콘텐츠, 포괄적으로 인공지능 기술이 포함될 것이다. 즉, 초연결사회이면서 지능정보사회인 영역이라고 할 것이다. 규범이론적으로 가장 복잡한 계층이라고 할 수 있다. 콘텐트 계층에서는 워낙 다양한 데이터가 다양한 프로그램을 통하여 다양한 목적으로 활용될 것이기 때문에, 사안에 따라서 다른 윤리론이, 즉 다른 가치관이 적용될 수도 있을 것이다. 따라서 개별 사안에 대하여 어떠한 규범이론이 적용되어야 하는지 논의하기보다는 궁극적으로 초연결사회가 어떤 가치를 추구하는 사회인가 하는 것을 생각해볼 필요가 있다.

초연결사회는 기본적으로 공유와 협력을 추구하는 사회라고 판단된다. 데이터의 공유를 통하여 인간과 인간, 인간과 기계가 연결되어 협력함으로써 더 나은 사회를 만들어나가는 것이라고 할 것이다. 물론 이러한 과정을 통하여 최대 행복을 추구하는 것은 당연하다. 그러나 그 중심에 인간이 있다는 것을 잊어서는 안 된다(김대호 외, 2015). 사물인터넷시대에 정보인권 보장을 논의한다거나(이준복, 2015), 현대 초연결사회와 새로운 인격권 보호체계를 논의하는 것은 결국 초연결사회에서 인간이 소외되거나 인간의 권리가 침해되지 않아야 한다는 것을 공감하고 있다는 것이다. 즉, 인간을 수단이 아닌 목적으로 대하는 의무론적 윤리론이 강하게 요구되는 것이다. 초연결사회에 대한 논의에서 프라이버시 문제가 가장 많이 논의되는 것도 규범이론적으로는 의무론적 윤리론으로 설명할 수 있다.

콘텐트 계층의 주도적 규범도 일단 법규범이라고 해야 할 것이다. 그러나 4가지 계층 중 법규범의 역할이 가장 축소되어가는 영역이라고 보인다. 국내에서 개발되고 사용되는 각종 프로그램은 1차적으로 우리 법규범에 입각하여 개발되고 사용될 것이지만 초연결사회에서 국내에서 개발된 기기와 프로그램만 사용될 것이라고 생각하는 사람은 없을 것이다. 간단한 예로, 샤오미에서 개발ㆍ판매하는 제품을 사용하기 위하여 인터페이스가 중국어로 구성된 프로그램을 사용하는 경우를 생각하면

쉽게 이해할 수 있다. 윤리적 논의가 가장 활발하게 이루어지는 인공지능의 경우에도 마찬가지이다. 인공지능 기술의 선두를 달리고 있다는 구글은 우리 법규범의 관할권이 미치지 않는다. 최근 들어 인터넷 윤리, 개발자 윤리, 윤리적 코드에 대한 논의가 활발하게 전개되는 것은 같은 맥락에 있는 것이다.

콘텐트 계층에서는 공리주의적 윤리론이 여전히 작동하겠지만 인간을 수단이 아닌 목적으로 대하라는 의무론적 윤리론을 강조함으로써 인간 중심의 초연결사회가 구현될 수 있도록 노력할 필요가 있다. 아울러 법규범의 작용이 약해지거나 무력화될 수 있는 사안이 많이 발생할 수 있는 만큼 인터넷 윤리에 대한 관심과 노력이 반드시 이루어져야 하는 영역이다.

제 5 절 초연결사회의 규범형식 및 기본원칙

1. 초연결사회의 규범형식

초연결사회를 규율할 미래규범을 정립함에 있어 가장 먼저 초연결사회에서 규범이 과연 필요한 것인가, 필요하다면 어떠한 규범형식으로 접근해야 하는지에 대한 논의가 필요하다. 왜냐하면 인공지능・빅데이터・블록체인 등 신기술의 도입기나 발전기에는 어느 누구도 해당 기술이 어떠한 방향으로, 어느 정도 속도로 발전해 나아갈 것인지를 예측하기 어렵고, 급격히 변화하는 기술적 환경에 따라 선제적으로 법규범을 통해서 이를 규율할 경우 자칫 혁신을 저해할 수 있는 단초를 제공할 수도 있기 때문이다.

다만, 기술도입기나 기술발전기와 같이 아직 법규범을 제・개정하기에는 이르지만 사회적으로 규율의 필요성이 큰 영역에서는 과도기적으로 행위자에게 구체적인 행위지침을 제시하여 그에 따른 행위를 유도하는 윤리규범이나 가이드라인의 규범형식을 고려할 필요가 있다.[13] 예를 들어 이러한 윤리규범이나 가이드라인 등의 연

13) IEEE는 ‘윤리적인 디자인(Ethically Aligned Design)’을, 일본 총무성 산하 AI네트워크사

성법(soft law)은 향후 시간이 흐름에 따라 실정법(hard law)으로 발전하여 그 분야에서 중요한 규범으로 작용할 개연성이 그 만큼 높아진다는 점에서 중요한 의미를 가진다(정필운・고인석, 2017).

또한 사회・경제(산업)・삶 전반에 혁신과 총체적 변화가 예상되는 4차 산업혁명에 대응하여 선제적인 법규범의 제・개정이 불가피한 경우에는 먼저, 해당 신기술 혁신에 따른 사회적 변화가 전혀 새로운 현상이거나 개별적으로 달리 대응해야 하는 특수성이 있다면 새롭게 입법을 통해 규율하고[14], 동일한 사회현상에 대하여 유사하거나 중복되는 규범이 존재하는 상황이라면 기존 법령의 개정[15]을 통해 이를 보완하는 입법전략이 요구된다.

초연결사회의 발전단계를 고려해볼 때, 독일의 Industry 4.0에서 OECD의 차세대 제조혁명으로 그리고 최근 다보스포럼에서 논의된 4차 산업혁명까지 이러한 일련의 시간적 흐름과 기술적 진화에 맞추어 4차 산업혁명과 초연결사회의 개념이 점차 확대되고 있으며, 초연결사회를 구성하는 핵심기술을 포함한 4차 산업혁명을 이끄는 기술의 범위 또한 다양해지고 있다.

앞서 제4절에서는 전통적 규범이론을 C-P-N-D계층에 각각 적용하여 초연결사회의 규범이 어떠한 방향을 지향하여야 하는지 살펴보았다. 다만, 초연결사회에 대한 규범이론의 적용결과를 바탕으로 각 초연결사회의 단계에 적합한 규범형식을 모색하기 위해서는 다소 평면적으로 구성되어 있는 C-P-N-D계층에 시간적 개념을 적용

회추진회의 사무국과 인공지능학회에서는 ‘AI개발윤리 가이드라인’을 제시하였고, 우리나라도 과학기술정보통신부가 ‘지능정보사회 윤리 가이드라인’을 발표할 예정이다.

14) 유럽의회 법사위원회(Committee on Legal Affairs)가 로봇, 인공지능의 개발 및 확산에 따라 제기되는 법적・윤리적 이슈에 대한 법제화 방향을 담은 ‘로봇법 규칙 초안을 위한 보고서(Draft Report)’를 제시하였고, 우리나라에서도 강효상 의원(자유한국당)이 ‘지능정보사회 기본법안’을, 박영선 의원(더불어민주당)이 ‘로봇기본법안’등을 대표발의 하였다.

15) 과학기술정보통신부는 기존 정보화 사회 중심법률인「국가정보화기본법」을 ‘지능정보화기본법’으로 전면 개정하는 방안을 추진 중에 있다.

하여 보다 입체적으로 접근할 필요가 있다.

왜냐하면 C-P-N-D계층에 규범이론을 적용한 결과에 따라 제시된 규범형식을 살펴보면, 법・윤리・코드 등이 모두 포함되고 어느 규범형식이 더 중요하게 작용할 것인가에 대한 경중의 차이만 있을 뿐 계층별 규범형식에는 큰 차이가 없기 때문이다. 아래 <표 3-1>은 제4절에서 초연결사회를 구성하는 각 계층(C-P-N-D)에 대표적인 규범이론을 적용한 결과를 바탕으로 도출한 규범형식이다.

〈표 3－1〉 규범이론 적용을 통한 계층별 규범형식

생태계	계층	대상	규범형식
초연결 사회	콘텐트	빅데이터 분석·활용 인공지능의 데이터 분석·활용	윤리와 코드 > 법규범
	플랫폼	사물인터넷 운영체제·상호운용 클라우드 운영체제·상호운용	법규범(공정) > 윤리와 코드
	네트워크	사물인터넷 통신영역 클라우드 통신영역 빅데이터 통신영역	법규범(공정) > 윤리와 코드
	디바이스	웨어러블 디바이스 기술 사물인터넷 물리적 부분	법규범 > 윤리와 코드

하지만 <표 3-2>과 같이 규범이론을 적용한 각 계층(C-P-N-D)에 시간적 개념을 추가적으로 고려해보면 초연결사회에서 적합한 규범형식은 계층별로 다르게 나타남을 알 수 있다.

우선, 각 계층에 시간적 개념을 적용해보면 다음과 같다. 먼저, 플랫폼은 인간이 사물을 지배하기 위한 통로로써 필수적인 기재이지만, 서로 다른 기계에 대한 서로 다른 플랫폼은 인간에게 별도의 학습을 요하고, 사물과 사물 간의 합종연횡이 어려워 생산성 향상에 장애가 되는 단점이 있었다. 독일이 이러한 문제점을 해결하고 인간-사물, 사물-사물 사이의 지배관계를 위한 플랫폼의 상호운용과 효율성 극대화를 위해 추진한 ‘Industry 4.0(Smart Factory)’은 플랫폼 계층에 해당하고, 플랫폼 간의

상호운용을 향상시키기 위해 기존의 클라우드와 빅데이터를 넘어 사물인터넷 통신 영역을 발전시켰다는 점에서 네트워크 계층에도 해당한다. 또한 2030년 전후로 펼쳐질 제조혁명의 생산기술에서 중요한 기술로 웨어러블과 사물인터넷의 물리적 부분을 지목한 OECD의 차세대 제조혁명은 디바이스 계층에 해당한다. 마지막으로 인공지능, 빅데이터 등 지능정보기술이 인간의 지적능력과 경쟁하고, 초지능・초연결・융합화가 가속화되는 4차 산업혁명은 콘텐트 계층에 해당한다.

이러한 시간적 개념을 각 계층에 적용하여 초연결사회의 적합한 규범형식을 생각해볼 때, 네트워크・디바이스 계층의 경우 3차 산업혁명의 연장선에 위치하고 있으므로 기존 법규범 틀 내에서 개정 및 보완을 통해 여전히 규율이 가능하나, 사회, 산업(경제), 삶의 방식 등을 총체적으로 변화시키는 초연결사회와 4차 산업혁명시대의 플랫폼과 콘텐트 계층에서는 4차 산업혁명에 따른 위험을 최소화하고 기회와 혜택을 보다 많은 사람들이 향유할 수 있도록 하는 한편 시장에서 공정한 경쟁이 이뤄질 수 있도록 법, 윤리, 코드 등 다양한 형태의 규범형식을 통해 초연결사회를 규율할 필요가 있다.

〈표 3－2〉 시간적 개념을 고려한 초연결사회의 규범형식

생태계	시간 개념	계층	대상	규범형식
초연결사회	4차 산업혁명	콘텐트	빅데이터 분석·활용 인공지능의 데이터 분석·활용	법규범, 윤리, 코드
	Industry 4.0	플랫폼	사물인터넷 운영체제·상호운용 클라우드 운영체제·상호운용	법규범, 윤리, 코드
		네트워크	사물인터넷 통신영역 클라우드 통신영역 빅데이터 통신영역	법규범
	차세대 제조혁명	디바이스	웨어러블 디바이스 기술 사물인터넷 물리적 부분	법규범

특히, 각 계층에 시간적 개념을 적용할 경우 기존의 법규범뿐만 아니라 다양한 규범형태가 강력히 요청되는 플랫폼 계층과 콘텐트 계층을 주목할 필요가 있다. 먼저, 플랫폼 계층은 복잡계적 특성으로 인해 시장에서 승자독식, 불평등, 참여자의 선택제한 등 다양한 불공정 문제가 발생할 가능성이 높은 만큼, 1차적으로 공정한 시장경쟁 환경을 조성하기 위한 법규범의 역할이 중요하며 다만, 국내법의 역외적용의 한계를 고려하여 2차적으로는 공정 경쟁을 지향하는 윤리와 코드를 마련하기 위한 국제사회의 노력이 병행될 필요가 있다. 또한 인공지능, 로봇 등 기계적 알고리즘이 인간의 가치판단과 행위에 지대한 영향을 미칠 것으로 예상되는 콘텐트 계층에서는 법규범은 물론 사전 예방원칙에 입각하여 지능정보기술의 잠재적 위험으로부터 사회시스템을 보호하고 관련 윤리적 또는 코드의 규율이 필요한 영역에 대하여 구체적인 행위지침을 제공하는 등의 초연결사회가 추구하는 가치에 따라 개별 사안에 대하여 다양한 규범형태를 마련하여 초연결사회를 규율하여야 한다.

2. 초연결사회 규범의 기본원칙 및 주요내용

인간중심의 초연결사회를 구현하기 위해 관련규범 정립 시 고려되어야할 기본원칙과 주요가치는 다음과 같다. 첫째, 초연결사회는 지능정보기술을 개발 및 활용함에 있어 인간의 존엄과 가치의 존중을 최우선 기본원칙으로 설정하여야 한다.「헌법」 제10조는 “모든 국민은 인간으로서의 존엄과 가치를 가지며 행복을 추구할 권리를 가진다.”라고 규정하고 있으며, 이러한 인간의 존엄과 가치는 헌법질서에서 반드시 준수되어야 하는 최고의 가치지표이다. 초연결사회는 인간의 지적 능력과 경쟁하는 단계로서 그 어떤 기술보다 인간의 존엄과 가치에 대한 본질적 문제와의 충돌이 불가피할 가능성이 높다(김민호 외, 2016). 따라서 인간의 존엄과 가치를 존중하는 초연결사회를 구현하기 위해서 지능정보기술・서비스는 인간에 의해 자율적으로 통제 및 제어가 가능하여야 하며, 인간의 윤리적 가치를 벗어나지 않도록 연구・설계・제작・관리・이용되어야 한다.

둘째, 초연결사회는 알고리즘에 의한 차별 등 인공지능이 야기할 사회적 역기능 발생을 방지하여야 한다. 인공지능, 로봇 등 지능정보기술의 발전이 인간의 사회적・경제적 편익을 증대시킬 것으로 예상되는 가운데 인공지능 기술에 의한 차별성, 비도덕성, 편향성, 인종차별 등 알고리즘 기반의 평가시스템이 야기할 차별과 편견 등 새로운 사회적 이슈가 끊임없이 제기되고 있다. 따라서 정부는 4차 산업혁명에 따른 사회적 역기능을 해소하고, 취약계층을 포함한 보다 많은 사람들이 지능정보기술의 기회와 혜택을 향유할 수 있도록 지능정보기술의 보편성, 편의성, 접근성을 확보하기 위한 노력이 필요하며, 국제 협력을 통해 세계적 보편성에 입각한 글로벌스탠다드 마련에 적극 참여하여야 한다.

셋째, 초연결사회는 4차 산업혁명이 가져올 노동・고용구조 변화에 따른 사회보장 및 복지제도의 개선을 통해 지속가능한 발전의 토대를 제공하여야 한다. 초연결사회는 노동・고용과 관련하여 근로시간・장소의 유연화, 노동플랫폼 기업의 등장, 프리랜서・1인 자영업자 등의 독립형 노동자 증가, 근무형태의 다양화, 근로자대표제도 등 다양한 변화를 초래할 것으로 예측되고 있다. 따라서 현행 노동법제 하에서 '근로자'와 '자영업자'와 같은 이분법적인 접근이 아니라, 다양한 고용형태를 포괄할 수 있는 '근로자'의 개념을 정립하여 '일하는 사람'에 대한 다차원적인 사회적 안전망을 구축하여야 한다. 또한 디지털화에 따른 근로자의 고용불안을 해소하고, 심리적・정신적 부담을 완화하는 한편 근로자의 인격권과 프라이버시를 보호할 수 있는 새로운 사회적 보호장치가 필요하며, 근로자측의 협상과 교섭력 확대를 위해 새로운 방식의 근로제대표제를 마련할 필요가 있다(박지순, 2017). 나아가 획일적인 근로시간 및 장소, 근로조건, 해고 규제 등에서 탈피하여 4차 산업혁명이 가져올 총체적 변화에 신속하게 대응하고 기업과 근로자의 개별 업무특성에 맞는 다양한 근로조건을 설정할 수 있도록 자율규제방식으로의 전환을 모색할 필요가 있다.

넷째, 초연결사회에서 민간의 창의와 자율성을 보장하여야 한다. 초연결사회의 기반이 되는 지능정보기술・서비스는 기존 산업 및 기술과 융합하여 새로운 기술・서비스를 창출하고 있다. 하지만 우리나라의 경우 포지티브(positive)법체계, 칸막이식

진입규제, 그림자 규제, 오프라인 중심의 시설・설비규제, 활동규제 등은 ICT융합 신산업 활성화와 혁신을 저해하는 대표적인 문제로 지적되고 있다. 따라서 정부와 국회는 규제패러다임을 '사전허용-사후규제'방식으로 전환하고, 신속처리・임시허가, 신기술・제품 적합성 인증제도 등 대안적 규제개선제도의 개선을 통해 신속한 시장출시를 적극 지원하는 한편, 기존 규제에도 불구하고 혁신적인 ICT융합 신기술・서비스를 시장에서 실험할 수 있는 '규제 샌드박스(Regulatory Sandbox)'를 도입하여 민간의 창의적인 아이디어가 혁신으로 이어질 수 있도록 적극 지원해야 한다.

다섯째, 초연결사회에서 지능정보기술이 초래할 위협으로부터 이용자의 안전과 사생활은 보호되어야 한다. 안전한 초연결사회로의 안착을 위해서는 지능화된 사이버위협과 AI 오작동 등으로 발생 가능한 문제에 대응하여 사전 예방체계를 구축하고, 국가 차원에서 사이버위협 예방 및 대응을 체계적으로 수행할 수 있도록 제도, 방법, 절차 등을 마련하여 국가 사이버침해사고 대응체계를 확립하여야 한다. 또한 새로운 기술 환경 변화에 대응하여 이용자 권리 강화 및 사생활 보호를 위해 이용자의 선택권을 확대하는 한편 이용자 주도의 초연결사회 생태계를 조성하기 위한 이용자 정책방향을 정립할 필요가 있다.

제4장 초연결사회의 안전성과 사이버 복원력 확보를 위한 대책

제 1 절 초연결사회를 위한 보안 및 프라이버시 보호 정책

1. 초연결사회의 새로운 위협의 트렌드와 침해 대응

가. 최근의 트렌드와 침해사례

사물 인터넷(IoT)과 함께 보급되는 새로운 소형 디바이스와 센서들은 보안에 취약하며 사물 인터넷의 특성상 침해당했을 때 피해 규모가 매우 클 수가 있다. 최근 이러한 속성을 반영한 듯 사이버 범죄가 지속적으로 증가하고 있으며 피해 규모도 날로 커지고 있다.

2015년 McAffee 랩의 위협 예측(Threat Predictions)에 의하면 사이버 첩보(espionage), 사이버 전쟁(cyber-warfare)이 증가할 것으로 예상되며, 해킹 기술의 발전에 의해 해커를 색출하기가 더욱 어려워지고 민감한 정보의 도난을 막기도 어려워질 것이라고 했다. 또한 연결된 사물(connected objects)의 기하급수적 증가, 부실한 보안 대책, 그리고 IoT 디바이스가 지니고 있는 데이터의 높은 가치 때문에 IoT 디바이스에 대한 공격이 급격히 늘어날 것으로 전망했다(Bendovschi, 2015).

최근의 사이버 공격에 대한 분석 결과 중 주목할 만한 것으로서 Bendovschi (2015)을 들 수 있다. 그는 2013~2015년 사이에 발생한 1,500만 건의 사이버 공격을 분석해서 트렌드를 도출하고 이러한 사이버 공격에 대한 대응 방안을 제시했다. 여기서는 이 연구 결과를 살펴보고 시사점을 도출하고자 한다.

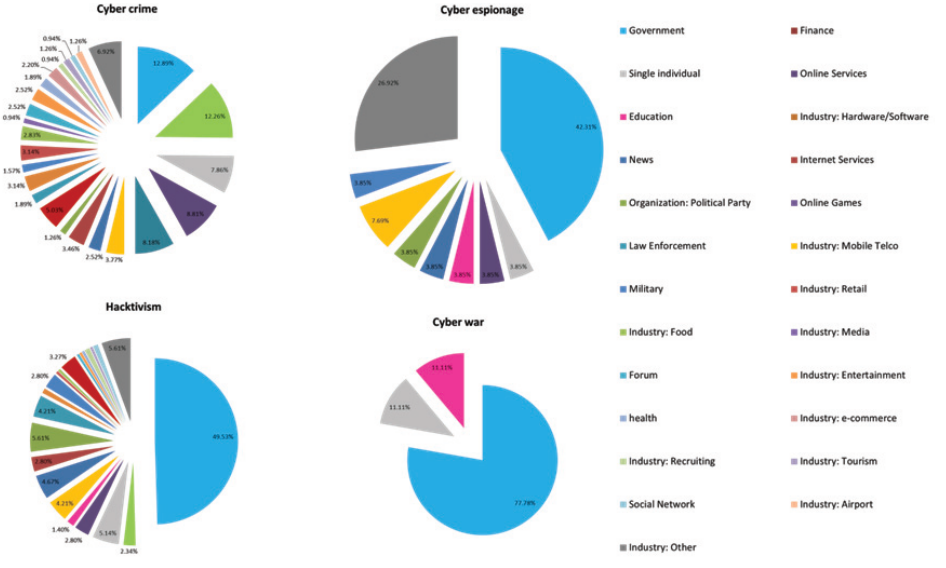
우선 침해의 원인은 크게 범죄자의 의도된 공격, 인간의 실수 그리고 시스템 내 취약점으로 나누어지는데 첫 번째 원인의 비중이 50%에 못 미친다. 또한 피해자들 중 96%가 한 개 이상의 시스템 취약점을 가졌던 것으로 분석되었다. 실제로 사이버

공격의 유형은 매우 다양하지만 이 연구에서는 크게 사이버 범죄(cyber-crime), 사이버 첩보, 사이버 전쟁 그리고 해킹(hacktivism)의 4대 유형으로 분류한다. 공격의 유형과 공격 대상 사이에는 유의미한 상관관계가 발견되었다. 예를 들면, 사이버 첩보는 주로 정부기관, 미디어 그리고 법집행 기관에 집중되었다([그림 4-1] 참조). 또한 분석 결과는 몇 가지 트렌드를 시사하고 있다. 첫째, 불법적 비인가 접근의 경우 물리적 접근에 비해 논리적 접근의 비중이 늘어나고 있는 추세이다. 둘째, 스마트폰에 대한 사이버 공격이 증가하고 있다. 스마트폰은 인터넷에 상시적으로 접속되어 있고, 앱, 소셜 네트워크 등 접근 경로도 다양하며 많은 개인정보도 지니고 있기 때문에 사이버 범죄의 대상으로 주목받고 있다(Bendovschi, 2015).

위에서 소개한 최근의 사이버 공격의 패턴과 트렌드에 대응해서 Bendovschi (2015)는 다음과 같은 대응책을 권유했다. 사이버 공격에 대비하여 조직들은 우선 내부적으로 지속적인 위험 사정(risk assessment)을 실시해야 한다. 또한 내부에서 사용하는 모든 하드웨어, (보안용을 포함한) 소프트웨어들은 업데이트되고 최신 보안 패치가 설치되어야 한다. 유지보수와 업그레이드를 위해 제삼자가 제공하는 소프트웨어도 같은 규칙이 적용되어야 한다. 조직 외부에서 접속하거나 웹 기반 애플리케이션의 경우 2단계 이상의 인증(authentication) 절차를 적용하는 것이 바람직하다. 조직 내부의 취약성과 위험은 내부 직원의 부적절한 행동에 의해 야기되는 경우가 매우 많기 때문에 업무 절차를 명확한 방법으로 공식화하고 정책화하는 것이 필요하다. 퇴직자, 계약자, 감사역, 다른 제삼자 등 조직의 네트워크에 접속할 필요가 있는 외부자들에 대해서는 접속을 제한하거나 한시적으로 허용하는 것이 바람직하다. 현재의 업무에 사용되지 않는 데이터는 조직의 네트워크로부터 제거하는 것이 좋다. 조직 외부적으로는 사이버 공격에 대응하는 비영리단체들의 도움을 얻거나 사이버 공격으로 인한 피해를 보상해 주는 보험에 가입하는 것도 새로운 대응책이 된다.[16]

16) AXA는 사이버 공격으로 인한 피해를 보상해주는 보험상품을 개발해서 판매하고

〔그림 4－1〕 사이버 범죄 유형별 대상 산업의 비중



출처: Bendovschi (2015) p.28

IoT 단말, 센서 등은 많은 부가가치를 창출하지만 대부분 단순한 기능을 수행하므로 연산 및 저장용량이 작기 때문에 보안조치를 취하는 데 한계가 있다. IoT를 많이 활용하는 산업제어시스템은 보안이 특히 취약하다. 산업제어시스템의 교체 또는 업데이트 도중에 설비 가동이 멈추는 위험이 있기 때문에 보안 위협에도 불구하고 보안강화 조치를 적시에 실시하기 어렵다. 노후한 저사양의 OS를 사용하고 있는 경우에는 보안 업데이트 자체가 불가능하다.

과거 사이버 공격은 주로 자신의 해킹 능력을 과시하거나 안보를 위협하는 것을 목적으로 했지만 최근에는 금전을 목적으로 하는 공격이 빈번해지고 있다. 2015년 2월 국내외 사업가 이메일을 해킹한 후 거래은행으로부터 거액을 편취하는 스피어 피싱(spear-phishing) 사기 조직이 검거되었는데 피해액은 총 224억 원에 이르렀

있으며, 고객의 사이버 위험 관리를 지원해주는 서비스도 출시했다.

다.[17] 2016년 11월에는 불법 도박 사이트를 해킹해서 40여 억 원의 부당이익을 챙긴 해킹 조직이 검거되기도 했다(보안뉴스, 2016. 11. 17.). 2017년 5월에는 워너크라이 랜섬웨어가 전 세계를 상대로 대대적인 공격을 실행했고 우리나라도 약 2,000 건의 피해가 발생했다. 워너크라이는 약 300 달러 상당의 비트코인을 요구했던 것으로 알려졌다.[18] 2017년 6월에는 국내 최대 가상화폐 거래소인 '빗썸'이 해킹당해서 수십억 원의 피해가 발생했다(경향비즈, 2017. 7. 3.).

최근 랜섬웨어는 협박 요구에 취약한 의료기관을 자주 공격하며 상대적으로 높은 금액을 요구하고 있다. 2016년 3월 미국의 3개 대형병원이 랜섬웨어의 공격을 받았으며 그 중 한 병원은 열흘간 시스템이 마비되어 공격자에게 1만 7,000 달러를 지불하고 시스템을 복구했다(안랩, 2016. 5. 2.).

초연결사회의 도래로 IoT가 산업에 확산되면서 보안에 취약한 산업제어 시스템에 대한 랜섬웨어 공격이 우려되고 있다. 산업제어 시스템에 문제가 생기면 병원 정보시스템 못지않게 심각한 문제가 발생하기 때문에 공격자의 요구에 신속히 반응하지 않을 수 없다. 산업제어 시스템에 대한 랜섬웨어 공격은 2016년에 시작되었다. 2016년 4월 미국 미시간주의 수력발전소 시스템이, 11월에는 샌프란시스코 시영철도 시스템이 랜섬웨어 공격을 받았다(아이뉴스24, 2017. 7. 7.). 보안업계에서는 산업제어 시스템이 랜섬웨어 공격의 보다 높은 목표가 될 것으로 전망하고 있으며 특히 IoT 환경 아래 제조 현장에서 인터넷에 연결되어 있는 수많은 설비자동제어장치(PLC)가 손쉬운 공격 목표가 될 것으로 전망했다.

미국의 정보시스템감시통제협회(ISACA)의 조사에 의하면 2017년에 성행할 사이버보안 위협 유형을 빈도 순서로 나열하면 랜섬웨어, IoT 공격, DDoS, 피싱, 악성 사이트와 Malvertising 등이다. 또한 59%의 기업이 작업 환경에 있는 IoT 설비에 대한 사이버 공격 우려를 표명했고, 78%의 기업이 악성 코드 공격을 경험했고 그중

17) http://greenjournal.co.kr/220273179905 (검색일: 2017. 7. 10.)

18) http://blog.naver.com/facemaker111/221006130150 (검색일: 2017. 7. 10.)

62%가 랜섬웨어였으며, 53%의 기업은 랜섬웨어 공격에 대한 공식적인 대응 프로세스를 마련했다고 답했다. 사이버 공격의 의도로는 금전 목적이 50%, 서비스 교란이 45%, 개인정보 절도가 37%였다. 금전 목적의 사이버 공격이 향후 랜섬웨어를 더욱 정교하게 만들 것으로 예상되었다.

사이버보안 전문기업인 Symantec은 '2017 인터넷보안위협 보고서(Internet Security Threat Report)'를 발표했는데 2016년에는 사이버 범죄자들의 단순한 전술과 혁신적인 범죄 수법이 수백만 달러에 달하는 가상은행의 예금을 강탈하고, 국가적인 지원을 받는 해커 집단이 미국 대통령 선거에 혼란을 초래하는 등 전 세계적으로 사상 유래 없는 충격을 주었다고 했다. 위 보고서에서 Symantec은 2016년에 전 세계적으로 발생한 사이버 공격들을 특징짓는 5개의 트렌드를 제시했는데 그 내용은 다음과 같다.[19)]

정치에 대한 표적 공격: 경제적 첩보행위에서 정치적 방해 공작과 전복 기도로 이동하고 있다. 미국 민주당에 대한 사이버 공격으로 인한 정보 유출은 조직과 국가를 불안하게 하고 혼란을 초래했다. 과거에는 방해 공작을 위한 사이버 공격은 거의 없었으나 2016년 미국 대선에서 드러났듯이 정치적으로 영향을 미치려고 하는 사이버 공격의 트렌드가 확대되고 있다.

이메일이 사이버 공격의 무기: 이메일이 이용자들에게 위험하고 효과적인 위협이 되었다. 2016년 평균적으로 131개 이메일 중 1개는 악성코드를 지니고 있었다. 업무 메일을 가장한 피싱공격이 매일 400여 개의 기업을 공격하고 있고, 이로 인해 지난 3년간 30억 달러의 손실이 발생했다.

조직, 국가에 의한 사이버 공격: 2016년에는 범죄 조직에 의한 사이버 공격으로 은행들이 강탈당했으며, 최초로 국가가 사이버 공격에 관여했다는 증거가 발견되었다. 북한은 방글라데시, 베트남, 에콰도르, 폴란드의 은행을 공격해서 최소 9,400만 달러를 강탈했다.

---

19) https://www.symantec.com/security-center/threat-report (검색일: 2017. 7. 10.)

미국은 랜섬웨어의 쉬운 표적: 랜섬웨어가 전 세계적으로 사이버 범죄의 수입원이 되고 있다. 특히 미국은 랜섬웨어의 가장 크고도 쉬운 표적이 되었다. 미국인 중 64%가 '몸값(ransom)'을 지불할 의사가 있는 것으로 조사된 반면 이에 대한 세계 평균치는 34%이다. 범죄자들이 요구하는 평균 몸값은 건당 1,077 달러이다.

클라우드는 위험한 곳: 클라우드는 보안 취약점으로 인해 사이버 범죄의 다음 전선이 될 것이다. 클라우드 서비스에 대한 의존도의 증가는 조직들에게 취약점을 만들어 준다. 2016년 클라우드 사용자들이 오래된 앱 버전들을 인가 장치도 없이 방치하는 바람에 수만 개의 Mongo 클라우드 DB가 랜섬웨어의 공격을 받아 몸값을 요구받았다. 현실적으로 CIO들은 자신의 조직에서 몇 개의 클라우드 앱이 사용되고 있는지도 모른다. 통제되지 않는 접속과 관리되지 않는 IT 자산은 심각한 위험을 초래한다. CIO들이 클라우드 앱에 대한 접속과 사용을 철저히 관리하지 않으면 공격자들은 클라우드의 취약점을 노릴 것이다.

나. 사이버 침해 트렌드 전망

매년 다수의 사이버보안 전문기관들은 향후 발생할 사이버 침해의 주요 트렌드들을 발표해왔다. 여기서는 2017년도에 발표된 트렌드들을 각 기관별로 살펴보고 공통된 트렌드들과 초연결사회와 관련성이 높은 트렌드들에 대해서 논의하고자 한다.

CIO를 주 고객으로 하는 영국의 IT 전문사이트인 'Information Age'는 2017년에 등장할 10대 사이버보안 트렌드를 발표했다. 그 주요 내용은 다음과 같다.[20]

① 사이버보안 관련 규제의 지속적인 개선: 지금까지 규제는 단지 규제만 준수하고 보안에 대한 잘못된 감각만 키우는 문화를 형성해왔다.

② 데이터 절도에서 데이터 조작으로: 공격자는 데이터 절도와 웹사이트 해킹에서 데이터 무결성(integrity)을 공격하는 방향으로 전환한다.

---

20) http://www.information-age.com/10-cyber-security-trends-look-2017-123463680/ (검색일: 2017. 6. 15.)

③ 기업 내 사이버보안 전문가 고용이 늘어남에 따라 사이버보안 기술에 대한 수요는 지속 증가: 사이버보안 기술에 대한 전 세계적 부족으로 기업들 간 사이버보안 전문가 확보 경쟁이 치열해질 것이며 기업들은 외주보다는 기업 내부에 전문가를 확보하려고 할 것이다.

④ IoT 디바이스에서 설계에 의한 보안(Secure by design)은 지연: 설계에 의한 보안은 2018년 이후에 가능할 것으로 전망되며, 인공지능을 장착한 공격은 특정 사용자들의 행동을 모방함으로써 숙련된 보안요원들조차 농락할 수 있을 것이며, 복잡하고 맞춤형의 피싱 공격을 통해서 사이버 공격에 경각심을 가진 사람들까지도 성공적으로 유린할 수 있을 것으로 예상된다.

⑤ 소비자 디바이스가 공격 표적: 2017년 이후에는 연결된 사물들을 통해서 소비자들이 랜섬웨어의 공격 표적이 될 것으로 전망된다.

⑥ 더욱 대담해지고 상업화되고 추적하기 어려운 공격자들: 해커들은 더욱 조직화되고 상업화되며(데이팅 서비스 사례에서 이미 등장한 바와 같이) 콜센터를 설치하기도 한다. 사이버 범죄가 거의 범죄로 인식되지 않는 국가에 근거지를 둠으로써 경찰의 치안영역을 벗어난다.

⑦ 더욱 똑똑해진 공격자들: Dark Web을 이용하여 자신의 신분을 감추고 다른 범죄자들과 소통한다.[21]

⑧ 더욱 교묘해진 사이버 침해: 사이버 범죄자들은 더욱 우회적인 방법으로 활동을 넓혀간다. 침해 소프트웨어가 피해자를 다시 공격자로 전환시켜 피라미드 형태의 공격자 집단을 만들어가는 혁신적 시스템이 이미 발견되었다.

⑨ 사이버 위험 보험의 보편화: 사이버 공격의 피해를 보상해주는 보험상품이 향후 보편화될 것이다. 피해에는 기업의 평판과 신뢰의 실추, 부정적인 미디어 노출로 인한 미래 수입의 감소 등이 포함된다. 보험상품은 고객의 필요에 따라

21) 웹 중에서 검색엔진에 의해 인덱스되어 있지 않은 부분을 Deep Web이라고 하며 Dark Web은 Deep Web의 작은 부분으로서 특정 소프트웨어나 접속 승인을 통해야만 접근이 가능하다(https://en.wikipedia.org/wiki/Dark_web, 검색일 2017. 6. 15.).

맞춤형이 될 것이다.

⑩ CCO(Chief Cybercrime Officer)라는 신 직업 등장: 조직들은 사이버 침해를 방지하고 침해 발생 시 작전을 지휘하고 조직의 이사회와 그 나머지 부분을 굳건히 연결하는 책무를 담당한 CCO를 선임할 것이다.

보안 전문업체인 Upwork는 2017년 3대 사이버보안 트렌드와 대응책을 발표했다. 그 내용은 다음과 같다.[22]

주입 공격(injection attacks): 데이터베이스의 농락. 이 공격은 기본적으로 데이터를 필요로 하는 웹 애플리케이션을 표적으로 한다. SQL 주입 공격은 해커의 데이터베이스 교본을 앱을 통해 주입함으로써 해커가 마음대로 데이터베이스를 조작하고 데이터를 절도, 삭제, 변조하는 것이다. 이 공격을 막기 위해서는 비준(validation), 회피(escaping), SQL의 견고한 코딩과 같은 기초적인 초치가 필요하며, 해킹 발생 시에는 이용자의 권리를 최소화하는 최소특전원칙(Least Privilege Principle)을 실행한다.

인간을 해킹하기: 사회공학(social engineering)과 피싱 사기. 이용자가 신뢰하는 어떤 사람인 척하든지 공공기관인척 하든지 채팅으로 인간관계를 맺는 방법 등으로 신뢰감을 주고 이용자로부터 필요한 정보를 얻어내는 것이 사회공학적 해킹이다. 피싱 공격은 회사 업무 메일 등 의심받지 않는 메일을 가장하여 첨부파일을 열어보게 하는 방법으로 공격하여 필요한 정보를 훔쳐가는 공격이다. 이러한 공격에 가장 효과적인 대응 방법은 수상한 메일을 경계하고 당국에 보고하는 방법을 숙지하는 등 이용자들을 교육하는 것이다.

사이버 범죄자의 무기 선택: 악성코드. 악성코드를 컴퓨터에 내려받으면 컴퓨터 내에서 벌어지는 모든 활동을 관찰하고, 개인정보에 접근하며 비인가 이용자도 접속할 수 있는 '뒷문(backdoor)'를 설치한다. 뒷문은 대규모 공격의 통로가 된다. 악성코드를 방지하는 기본적인 방법은 모든 운영체제를 업데이트하고 방화벽(firewall)을

22) https://www.upwork.com/hiring/development/trends-in-cyber-security-threats-and-how-to-prevent-them/ (검색일: 2017. 6. 15.)

설치하는 것이다. 악성코드의 신종 수법으로서 ‘malvertising’이 등장했는데 이는 악성코드가 온라인 광고를 가장해서 컴퓨터에 침입하는 것이다. 이를 차단하려면 브라우저를 정기적으로 업데이트하고 ‘ad blocker’를 설치한다.

· ISF (2017) Threat Horizon 2019

정보보안포럼(Information Security Forum: ISF)은 2019년 위협 지평(threat horizon)에서 향후 2~3년간 전 세계 조직들이 처하게 될 9개의 위협들을 다음과 같이 3개의 주제로 분류해서 발표했다.

〈표 4－1〉 ISF(2017)의 2019년 위협 지평

주제	위협
1. 파괴(disruption): 취약한 연결에 대한 과도한 의존이 파괴를 초래	1.1 사전 계획된 인터넷 파괴 공격으로 경제 혼란을 초래(일부 국가나 테러 집단이 적국의 경제적 혼란을 초래하기 위해 핵심 인터넷 인프라가 공격의 표적이 될 것이다.) 1.2 IoT가 랜섬웨어에게 납치(랜섬웨어는 이미 조직들이 디지털 정보에 부여하는 가치를 가로채는 주된 방법이 되었으며 랜섬웨어는 스마트 디바이스 분야로 진출해서 인간의 생명을 위협할 것이다.) 1.3 권한을 가진 내부자를 위협해서 중요 정보를 탈취(임무 수행에 핵심적인 정보에 접근권을 가진 자를 전통적인 범죄 방식으로 위협을 가해서 핵심 정보를 획득한다.)
2. 왜곡(distortion): 정보의 무결성에 대한 신뢰 상실	2.1 자동화된 거짓 정보로 즉각적인 신뢰를 얻음(인공지능에 의한 가상 인격체의 발달로 의도적으로 허위 정보를 유포하면서 상업적인 기관들을 공격 표적으로 한다.) 2.2 위조된 정보가 조직의 성과를 약화시킴(조직의 내부 정보의 무결성에 대한 공격이 수적으로, 규모나 복잡성 측면에서 증가할 것이다.) 2.3 파멸된 블록체인이 신뢰를 파괴(블록체인은 사기나 돈세탁에 이용되면서 파멸되어 이에 대한 신뢰가 산산조각날 것이다. 그 결과 블록체인은 폐기되고 그 프로세스 효율성이 상실된다.)

주제	위협
3. 악화(deterioration): 규제와 기술 때문에 제어 능력 상실	3.1 감시 관련 법들이 기업 비밀을 노출시킴(공격자들은 통신 사업자들이 수집한 산적된 정보에 대한 적절한 보안 조치를 할 능력이 없는 점을 노릴 것이다.) 3.2 프라이버시 규제는 내부 위협에 대한 관찰에 장애가 됨(개인에 대한 프로파일링에 대한 규제는 조직에게는 수수께끼가 되면서 내부 위협을 관찰할 능력을 상실하거나 규제를 위반한다. 어떤 경우도 부정적인 결과를 초래한다.) 3.3 인공지능의 보급을 위한 황급한 질주는 예상하지 못한 결과를 초래(인공지능의 사용은 기업의 지도자, 개발자 그리고 시스템 관리자의 이해를 초월하는 결과를 낳으면서 새로운 취약점을 창출한다.)

출처: ISF(2017) 재구성

위에서 제시된 9개의 위협은 인터넷과 정보 시스템이 운영되는 사회에는 공통적으로 적용될 수 있는 것이라고 본다. 그러나 위협의 현실성, 즉 실현가능성은 각 사회의 특성에 따라 달라질 수도 있다. 예컨대, 1.1과 같은 인터넷 인프라에 대한 물리적 테러 가능성은 우리나라와 같이 테러 공격이 발생한 사례가 적은 국가에서는 큰 위협이 되지는 않을 것이다.

다. 소결

2017년을 기준으로 그 때까지 발생한 사이버 공격의 유형과 그 이후의 사이버 공격의 유형에 대한 예측을 종합적으로 검토해 보면 2010년대 중후반의 사이버 위협의 트렌드를 파악할 수 있다. 하지만 2015년도에 예측한 결과와 사후적인 결과를 비교해 보면 다소 거리가 있는 경우도 있으므로 2017년 이후에 대한 예측 결과의 신뢰 수준은 다소 하향 조정할 필요가 있다.

2017년 이전 사이버 공격의 중심적인 트렌드는 금전 목적의 공격이라고 할 수 있다. 그리고 공격 대상이 개인으로부터 랜섬이 높은 의료기관, 가상화폐 거래소 그리고 보다 수준 높은 공격 대상인 산업제어 시스템으로 상향 조정되는 추세를 보였다.

2016년 미국 대선을 계기로 정치적 목적의 사이버 공격이 새로운 사이버 위협의

유형으로 등장했지만 이는 중요한 정치적 이벤트가 있을 때 발생하는 공격이므로 새로운 트렌드로 자리잡기에는 지속성이 부족하다. 그 밖에도 McAffee 랩은 사이버 전쟁을 2010년 중후반 주요 사이버 위협으로 예측했지만 이 예측은 다소 빗나간 것으로 보인다.

2017년 이후 사이버 침해에 대한 3개 기관의 예측 결과 중에서 공통된 트렌드가 데이터 무결성에 대한 공격이다. 단순한 데이터 절도나 데이터 접근 봉쇄의 수준을 넘어 공격 대상의 데이터를 위변조함으로써 상대방의 시스템을 교란하여 이에 대한 반사 이익을 취하는 것이다. 인공지능이 상업적 용도로 활용됨에 따라 데이터 무결성은 인공지능에 의한 의사결정에 매우 중요하다. 예컨대, 경쟁 상대방의 인공지능 시스템에 입력되는 데이터를 은밀히 조작함으로써 상대방이 인지하지 못한 상태에서 상대방 시스템을 교란 또는 조작할 수 있다. 이러한 방법으로 상대방이 잘못된 의사 결정을 하도록 유도하여 커다란 금전적 이득을 취할 수 있다.

또 하나의 공통된 트렌드는 공격 방법이 더욱 교묘해진다는 것이다. 정보시스템 이용자와 관리자들이 사이버 위협에 대한 경각심을 강조함에 따라 공격자들은 다양한 기술과 수법을 동원해서 일반 이용자는 물론 보안 전문가마저 기만하고자 한다. 이를 위해 흔히 사용되는 방법이 사회공학적 해킹과 인공지능을 이용한 가상인격체의 개발이라고 할 수 있다. 이제는 일반 이용자뿐만 아니라 전문가들도 항시적인 보안 업그레이드 교육이 필요하다.

결론적으로, 지금까지는 사이버 공격이 시스템 마비에 대한 위협으로 금전적 이득을 취해왔지만 향후 초연결사회에서는 데이터 조작 공격을 통한 상대방 시스템의 교란을 통해 더욱 지속적이고 은밀하게 금전적 이득을 노릴 것으로 예상된다. 예컨대, 과거에는 업무 메일을 가장한 피싱 공격이 주된 해킹 방법이었다면 지금부터는 다양한 사회공학적 해킹, 피라미드식 공격자 양성 등 교묘한 사이버 침해가 이용자들을 노릴 것이므로 일반 이용자들에게도 이제는 전방위적 해킹 대응 방법에 대한 이해와 훈련이 요구된다.

2. 초연결사회를 위한 사이버보안 정책

가. 미국과 EU의 사이버보안 정책

1) 미국 연방정부의 사이버보안 정책

미국은 2002년 연방정부기관의 사이버보안을 규율하는 「연방정보보안관리법(Federal Information Security Management Act(FISMA) of 2002)」을 제정했다. 그런데 이 법은 바로 2002 「국토안보법(Homeland Security Act)」에 흡수되었다. FISMA 이전에도 일부 산업에서 사이버보안을 규율하는 연방 법제가 존재했다. 1996년 보건의료 관련기관의 정보보안을 규율하는 「의료정보보호법(Health Portability and Accountability Act:HIPAA)」이 제정되었고, 1999년에는 금융기관들의 사이버보안을 규율하는 「Gramm-Leach-Bliley Act」가 제정되었다.

1980년대에도 미국에는 사이버보안과 관련된 법제가 있었다. 예를 들면 1984년 제정된 「위장접근수단·컴퓨터사기 및 컴퓨터남용법(Counterfeit Access Device and Computer Fraud and Abuse Act)」은 전산 조직에 대한 무단 접속이나 컴퓨터 사기와 남용과 같은 행위를 범죄로 규정했으며 1996년 개정되면서 「국가정보기반보호법(National Information Infrastructure Protection Act)」으로 대체되었다. 1987년에는 연방 컴퓨터 시스템의 보안과 프라이버시를 향상하기 위해 「컴퓨터 보안법 (Computer Security Act)」이 제정되었다가 나중에 FISMA로 대체되었다.

FISMA는 현대적인 사이버 위협에 대비하여 위험 분석, 인증(certification)과 승인(accreditation) 절차 등을 포함하는 NIST가 개발한 사이버보안 프레임워크의 실행을 모든 연방기관에게 의무화하고 있다. 그러나 그 실효성에 대해서 보안 전문가들은 다음과 같은 의문을 제기하고 있다.

FISMA의 내용은 나쁘지 않지만 측정 시스템에 문제가 있다. 측정해야 하는 것이 사이버보안 계획의 존재 여부가 아니라 실제로 보안을 개선하는지 여부가 확인되어야 한다. FISMA의 집행은 서류작업의 수준에 머물러 있어서 실제로 사이버보안을 개선하는지는 의문이다(Government Computer News, 2007. 3. 18.). 사이버보안 전문

가들은 FISMA를 사이버보안을 위한 하나의 체크 리스트로 보고 있다. 사이버보안 책임자가 이 체크 리스트를 충족했다고 해서 자만하면 안 된다(Government Computer News, 2009. 6. 10.).

위에서 소개한 법제 이외에 많은 법안들과 정책들이 제안되었으나 무산되었다. 그 중 주목할 만한 것으로서 2003년 발표된 '사이버공간 보안을 위한 대통령의 국가전략(President's National Strategy to Secure Cyberspace)'을 들 수 있다. 이 전략은 사이버 공격에 비상 대응하고 국가적인 사이버 취약점을 감소시키기 위해서 정부와 산업계의 협력적 노력을 강조했다. 2004년에는 미국 의회가 4억 달러의 예산을 책정하여 이 전략의 일부 목표를 달성하기도 했으나 보안 전문가들은 다음과 같은 문제를 지적하고 있다.

이 전략은 국가의 사이버보안을 위한 좋은 출발이지만 미흡하다. 이 전략의 목적이 정부가 사이버보안의 문제를 책임지고 해결하는 것이 아니라 컴퓨터 시스템의 소유자들이 그들의 보안을 개선하는 프레임워크를 마련하는 것이지만 실제로 참여기업들이 개발된 보안 솔루션들을 채택하도록 하지는 않았다.[23]

2009년 오바마 행정부가 출범하면서 '사이버공간 정책리뷰(Cyberspace Policy Review)'를 발표하고 국토안보부(HSD)에서 담당한 국가 사이버보안 업무를 대통령 중심의 백악관에서 주도하기 시작했다. 또한 사이버보안을 위한 민·관 협력과 공동책임을 강조하고 보안 교육과 전문인력 양성, 혁신 촉진 등을 위한 시책을 제시했다(배병환·송은지, 2014).

사이버보안의 위협이 날로 증가하고 있음에도 불구하고 2002년 이후 최근까지 일부 개정 법률을 제외하고는 사이버보안에 대한 종합적인 법률이 제정되지 못했다. 개정 법률들은 주로 연방정부 기관들의 사이버보안과 관련된 임무나 조직에 관한 것이었다(송담대학교, 2015).

사이버보안에 관한 입법이 의회에서 지연되는 가운데 주요 기반시설이 사이버 공

23) https://en.wikipedia.org/wiki/Cyber-security_regulation (검색일: 2017. 10. 8.)

격에 노출되자 오바마 대통령은 2013년 2월 주요 기반시설 강화를 위한 행정명령(Executive Order 13636)과 정책지침(PDD 21)을 발표하고 주요 기반시설 보호를 위한 사이버보안 프레임워크를 개발하고 연방 정부기관의 역할과 의무를 규정했다(배병환·송은지, 2014).

오바마 대통령의 임기가 종료됨에 따라 위의 행정명령과 정책지침도 더 이상 유효하지 않게 되었으나 의회에서는 「국가사이버공간 및 핵심기반시설 보호법(National Cyberspace and Critical Infrastructure Protection Act of 2013)」이 2014년 7월 미국 의회 하원을 통과했다. 이 법은 「국토안보법(Homeland Security Act of 2002)」을 개정해서 국토안보부의 사이버보안과 관련된 역할을 법으로 규정하고 국토안보부 장관이 연방, 주, 지방 정부, 주요 기반시설 소유자와 운영자 등을 국가 사이버보안을 위해 조율할 수 있게 규정하고 있다.

또 하나 주목할 만한 것으로는 민간에게 사이버보안 관련 의무를 규정한 「사이버보안법(Cybersecurity Act)」를 들 수 있다. 이 법안은 2012년에 발의되어 계속 의회를 통과하지 못하다가 여러 번의 타협과 법안 개정 후 2015년에 비로소 통과되면서 미국 연방정부의 사이버보안 관련 법제의 중심적인 위치에 서게 되었다.

2012년에 발의된 법안은 국토안보부로 하여금 핵심기반시설(critical infrastructure)를 보유하고 있는 산업들에게 사이버보안에 관한 업계 최선행동(best practices)에 대한 표준을 개발하고 의무화하고자 했다. 그러나 업계의 반대로 의무 표준을 자발적 표준(voluntary standards)로 완화하고 표준을 채택하는 기업들에게는 법적 책임에 대한 면제(liability protection), 사이버 위협에 대한 지원, 위협에 대한 비밀정보에 접근권 부여 등의 유인을 제공했다.

그럼에도 관련 업계는 이 법안이 사이버보안을 개선하지 못하고 혁신만 저해한다고 비판했다. 이러한 업계의 주장은 헤리티지 재단의 한 보고서가 다음과 같이 대변하고 있다. 첫째, 정당성이 있는 사업상 이유로 자발적 표준을 채택할 수 없는 핵심기반시설을 보유한 기업에게 위협에 대한 정보를 제공하지 않는 것은 공공의 이익에 반하는 것이다. 둘째, 법적 책임을 면제해준다는 것은 징벌적 손해배상만 피하게

하는 것이다. 또한 정부의 표준은 소송에 있어서 판단 기준으로 작용할 것이다. 셋째, 표준이 작성되고 채택되는 다년간의 과정에서 사이버보안 제품에 대한 투자와 혁신은 중단된다. 기업은 표준에 부합되는 않는 기술에 투자하지 않을 것이기 때문이다. 또한 사이버보안과 같은 역동적 기술 환경에서 정부가 올바른 표준을 설정할 수 있는지에 대해서도 회의적이다. 넷째, 자발적 표준을 채택하지 않는 기업에게 자발적 표준을 강제한다면 이미 자발성을 상실한 것이다.[24]

다년간에 걸친 이해당사자간 타협 끝에 2015년 10월 「사이버보안법(Cybersecurity Act of 2015)」이 미 의회 상원을 통과했다. 이 법은 4개의 타이틀로 구성되어 있는데 Title Ⅰ은 같은 해 통과된 「사이버보안 정보공유법(Cybersecurity Information Sharing Act: CISA)」이 차지하고 있고 Title Ⅱ의 Subtitle A에는 「국가 사이버안보 보호 선진화법 2015(National Cybersecurity Protection Advancement Act of 2015」가[25] 들어가 있다. 이 법은 국토안보부 내부의 민간 조직인 국가사이버보안통신통합센터(National Cybersecurity and Communications Integration Center: NCCIC)에게 정보공유 메커니즘의 시행을 맡겼으며, 분야별 정보공유분석센터들(ISACs)과 민간기구들과의 정보공유를 촉진하는 조치를 취하도록 규정하고 있다. Title Ⅲ는 연방 「사이버보안 인력평가법(Federal Cybersecurity Workforce Assessment Act of 2015)」으로서 사이버보안 역량이나 관련 기능을 요구하는 직책을 찾아내기 위해 연방 인력에 대한 광범위한 평가를 규정하고 있다. Title Ⅳ는 핵심 정보 시스템과 네트워크에 대한 위협을 발견하고 공개하기 위해 개발된 다양한 수단들을 제공한다. 이상 4개의 타이틀 중에서 핵심이라고 할 수 있는 「사이버보안 정보공유법」의 주요 내용은 다음과 같다.[26]

---

24) http://www.heritage.org/defense/report/cybersecurity-act-2012-revised-cyber-bill-still-has-problems (검색일: 2017. 6. 15.)

25) 이 법안은 2015년 4월 23일 미국 상원에서 기각된 바 있다. (https://www.govtrack.us/congress/ bills/114/hr1731, 검색일: 2017. 6. 15.)

26) https://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015 (검색일: 2017. 6. 15.)

① 민간 부문과 연방정부 사이의 정보공유 게이트웨이는 국토안보부의 국가사이버보안통신통합센터에서 그 역할을 담당한다. 또한 접수된 정보가 실시간으로 다른 연방기관들에게 전달될 수 있는 자동전달시스템을 구축·운영한다.

② 사이버 공격을 당한 기업들의 경험은 미래의 사이버보안을 위한 중요한 자산이기 때문에 정부와 민간이 공유하는 것이 바람직하다. 그러나 공격을 당한 기업 입장에서는 그러한 경험의 공유가 자칫 민사적 또는 형사적 책임을 야기할 수도 있으며 기업의 신뢰도를 저하시킬 수도 있기 때문에 공유를 주저하지 않을 수 없다. 따라서 민간기관에게 정보 공유의 유인을 제공할 필요가 있는데 이 법에서는 민간기관이 CISA의 정보공유 규정을 준수한 경우에는 정보공유 행위로부터 발생한 민사적 책임을 면할 수 있는 피난처(safe harbor)가 제공된다. 비록 악의적인 의도에 의한 정보공유 행위라고 할지라도 CISA의 기술적인 요구조건에 의거한 객관적인 준수 검증을 통과하면 법적 책임을 면한다. 피난처는 민사적 책임뿐만 아니라, 규제 및 반독점 책임도 포함되며, 중과실이나 의도적 위법행위의 경우도 책임 면제에서 예외라고 명시하지 않았다.

③ 비연방기관은 정보를 공유하는 시점에서 사이버보안과 직접적인 관련성이 없는 개인정보는 제거할 수 있다.

④ 규제를 받는 기관들이 연방 규제당국과 사이버보안 위협에 대한 대화를 해도 책임 면제를 박탈당하지 않는다. 사이버보안 정보를 제공하지 않거나 정부 계약에서 배제하는 등 불이익을 주겠다는 위협으로 정보공유를 강제하지 않는다.

⑤ 제공된 정보에 의거하여 경고를 하거나 행동을 취해야 하는 의무를 지우지 않는다. 또한 선의로 행동을 취하지 않음으로써 발생한 손실에 대한 법적 책임을 면제하지도 않는다.

⑥ 이 법은 민간 기관이 사이버보안의 목적으로 자신의 정보 시스템과 동의를 구한 타 기관의 정보 시스템에 대해 방어적 조치를 취하는 것을 승인한다. 그러나 '역해킹'과 같이 관련 법에서 불법으로 규정하고 있는 조치는 승인하지 않는다.

그동안 민간기관이 사이버보안 관련 정보를 연방기관들과 공유하도록 하기 위해서 국토보안부를 거칠 것인지 아니면 FBI나 NSA로 바로 직행할 것인가에 대해 오랜 기간 동안 논쟁이 있었으나 민간 기관에는 법적 책임의 면제라는 유인을 제공하고 보안 관련 기관들에는 실시간 공유 정보의 제공이라는 조건을 제시하면서 타협한 결과 최종적으로 국토안보부가 사이버보안 정보포털과 같은 역할을 맡게 되었다. 법적 책임의 면제 범위에 대해서도 그 동안 논란이 있었지만 선의든 악의든 정보공유의 의도에 상관없이 공유의 기술적인 요건만 충족하면 면제시켜줌으로써 민간기관에게 매우 유리한 결정이 내려졌다. 프라이버시 보호 측면에서는 '직접적인 관련성이 없는'과 '정보를 공유하는 시점'이라는 표현이 모호하기 때문에 남용될 가능성이 있어 이 조항에 의한 프라이버시 보호 수준이 프라이버시 옹호 단체들이 원하는 수준에 못 미칠 가능성이 높다. 한편 사이버보안 관련 공유정보의 활용 목적이 사이버보안 위협 외에는 사망 또는 심각한 신체 부상 또는 심각한 경제적 손해의 위협에 대한 대응에만 제한된 점은 프라이버시 옹호자들에게 만족스러운 결과라고 할 수 있다.[27]

2) EU의 사이버보안 정책

EU는 2001년 '네트워크와 정보 보안에 대한 선언(Communication on Network and Information Security)'을 출발점으로, 사이버 공격에 대한 인식 제고와 대처 방안에 대한 '안전한 정보사회를 위한 전략(Strategy for a secure information society)' 수립, 2008년 사이버 테러에 대응하기 위한 '사이버방위센터' 설립 등을 추진해왔다. EU에서 사이버보안에 대한 체계적인 논의는 유럽의 지속가능한 경제성장을 위해 2010년 발표된 유럽의 디지털 의제(Digital Agenda for Europe) 중 하나인 'EU 사이버보안 전략 및 지침 제안'에 의해서 촉발되었다. 이에 따라 유럽연합집행위원회(European Commission: EC)는 2013년 2월 'EU 사이버보안 전략(Cybersecurity Strategy of the European Union)'과 'EU 네트워크 및 정보보안 지침(안)(Directive on Network

27) https://www.lawfareblog.com/cybersecurity-act-2015 (검색일: 2017. 6. 15.)

and Information Security: NIS)'을 발표했다.

우선 전자의 주요 내용을 살펴보면, EU 사이버보안 전략은 사이버보안의 원칙, EU의 비전이 반영된 전략적 우선 추진과제와 조치 그리고 관련 기관들의 역할과 책무로 구성되어 있다. 사이버보안의 원칙으로는 'EU의 핵심가치를 물리적 공간과 디지털 공간에 동일하게 적용한다'를 비롯해서 5대 원칙이 제시되었고, 전략적 우선 추진과제로는 '사이버 복원력의 확보'를 비롯한 5대 과제가 제시되었으며[28] 과제 수행을 위해 집행위원회가 직접 추진할 사항들과 관련 기관들에게 의무 또는 권고의 성격으로 위임할 사항들을 제시했다.

NIS 지침은 EU 사이버보안 전략의 핵심적인 부분을 법제화한 것으로서 2016년 7월 EU 의회에서 통과되었다. 그 주요 내용은 다음과 같다. 첫째, 회원국은 '컴퓨터 보안사고 대응팀(Computer Security Incident Response Team: CSIRT)'과 국가 NIS 당국을 설치한다. 둘째, 회원국들 사이에 전략적 협력과 정보교환을 지원하고 촉진하기 위해 '협력그룹(Cooperation Group)'을 설치하고, 특정 사이버보안 사고에 대한 신속하고 효과적인 업무 협조와 위험에 대한 정보 공유를 장려하기 위해 CSIRT 네트워크를 설치한다. 셋째, 에너지, 교통, 수자원, 은행, 금융시장 인프라, 보건, 디지털 인프라 분야의 기업들은 적절한 보안 조치를 취하고 심각한 보안사고 발생 시에는 CSIRT에게 보고해야 한다.[29]

사이버보안 관련 불법행위를 EU 차원에서 내린 결정으로는 2005년 '정보시스템 공격에 대한 이사회 기본결정(Council Framework Decision on attacks against information systems)'이 있다. 여기서는 정보시스템에의 불법 접근, 시스템에의 불법 침입, 데이터에의 불법 침입을 범죄로 규정하고 있다. 이 결정은 사이버보안에 대한 구체적인 입법 방향을 제시함으로써 EU의 사이버보안 법제의 발전에 중요한 기여를 하고 있다(송담대학교, 2015). 2013년 EU의 '정보시스템 공격에 관한 지침(Directive

28) 자세한 내용은 배병환·송은지(2014) p.6 참조.

29) https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-initiatives-working-towards-more-secure-online-environment (검색일: 2017. 6. 15.)

on attacks against information systems)'은 대규모 사이버 공격에 대응하기 위해 회원국의 사이버 범죄 관련 법들을 강화하고 더 무거운 형벌을 도입할 것을 요구했다.[30] 2015년 유럽연합 집행위원회에 의해서 채택된 '안보에 관한 신 유럽 의제(the New European Agenda on Security 2015-2020)'는 '더 효과적인 사이버 범죄와의 전쟁'을 3대 우선 추진과제 중 하나로 설정하고 전 유럽 차원에서 조율된 대응을 강조했다. 또한 비현금 지불방식에 관한 사기나 위조를 처벌하는 입법을 추진하고 사이버 범죄에 대한 수사를 가로막는 장애요인들을 검토할 것을 요구했다.

2015년에는 Digital Single Market Strategy가 발표되었는데 그 안에는 '사이버보안에 대한 공공-민간 파트너십'이 포함되어 있었다. 여기에는 대기업, 중소기업, 스타트업, 연구기관, 대학, 소비자, 협회 그리고 정책 당국들이 참여했다. 이 파트너십의 목적은 혁신과 회원국들과 업계들 사이의 신뢰 제고 그리고 사이버보안 제품과 솔루션에 대한 역내 수요자와 공급자의 연계를 통해서 사이버보안 시장의 파편화를 극복하고 유럽의 경쟁력을 제고하는 것이다.

EU는 사이버보안 정책의 수립과 실행을 실무 차원에서 지원하고, 사이버보안 관련 기관들의 협력을 촉진하며 사이버 범죄에 대한 법 집행을 효과적으로 추진하기 위해 각각의 목적에 부합하는 전문기관들을 설립해서 운영하고 있다. EU 산하 사이버보안 관련 조직들을 살펴보자.

ENISA(European Union Agency for Network and Information Security)는 유럽연합 내부의 고도의 네트워크 및 정보 보안에 적극적으로 기여하기 위해 설립한 기관이다. 2004년 ENISA는 유럽의회와 이사회 Regulation (EC) No 460/2004에 의해서 설립되었고 현재는 대체 regulation인 Regulation (EU) No 526/2013에 의거하고 있다. ENISA의 활동 영역은 주로 ⅰ) 보안사고 대응책 등에 대한 권고, ⅱ) 정책 수립과 실행 지원, ⅲ) EU 역내 작전팀들에게 실무 지원 등이다.[31]

---

30) https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-initiatives-working-towards-more-secure-online-environment (검색일: 2017. 6. 15.)

31) https://en.wikipedia.org/wiki/Cyber-security_regulation (검색일: 2017. 10. 8.)

2012년 EU 산하기관들에 대한 사이버보안 사고나 위협에 효과적으로 대응하기 위해서 EU는 침해사고대응팀(CERT-EU)을 설립했다. 공공 및 민간 기관들과의 협력과 정보공유를 위해서 CERT-EU는 EU 역내외의 CERT들과 CSIRT들 그리고 민간 사이버보안 기업들과 협조 네트워크를 구축·운영하고 있다. 향후 NIS 지침이 실행되면 CERT-EU의 역할이 강화될 것으로 전망된다.

2013년 EU 경찰(Europol)은 EU 역내의 사이버 범죄에 대한 법 집행을 위하여 유럽사이버범죄센터(European Cybercrime Center: EC3)를 설립했다. EC3는 조직화된 범죄 집단에 의한 사이버범죄, 피해자에게 심각한 위해를 가하는 사이버범죄, 필수 기반설비와 정보기반을 공격하는 사이버범죄에 초점을 맞추고 있다. EC3는 각 범죄 분야에서 범죄 정보와 첩보에 관한 중심 허브의 역할, 회원국의 수사와 작전 지원, 정보 기반의 의사결정을 지원하는 전략분석 기법의 제공, 회원국 당국의 역량 강화와 훈련 지원, 디지털 포렌식 지원 등을 수행하고 있다.[32)]

나. 미국과 EU의 사이버보안 정책 비교 및 시사점

최근 미국과 EU의 사이버보안 정책의 차이점은 크게 2가지를 지적할 수 있다. 첫째는 사이버보안 사고의 접수창구가 다르다. 둘째는 사고 신고의 자발성 여부이다. 여기서는 이러한 차이점으로 인해 야기될 결과를 예상해보고 장단점을 비교한다. 또한 우리나라 사이버보안 정책에 주는 시사점을 논의해보기로 한다.

미국의 경우 어떤 기관 또는 기업이 사이버 공격을 당했을 때 관련 정보를 국토안보부 내의 NCCIC에 보고하도록 보고창구가 일원화되어 있는 반면, EU의 경우 해당 국가가 설치한 CSIRT에 보고하도록 되어 있다. 미국은 NCCIC에 보고된 정보가 자동전달 시스템에 의해서 다른 연방기관에 실시간으로 제공되도록 제도화되어 있지만 EU는 CERT-EU가 각국의 CSIRT들과 협조 네트워크를 운영하고 있기 때문에 보고를 받은 CSIRT와 CERT-EU 사이의 소통이 얼마나 원활한가에 따라 정보공유의

32) https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (검색일: 2017. 11. 11.)

속도와 범위가 달라질 수 있다. 따라서 EU의 경우는 광범위한 사이버 공격의 경우 대응이 다소 지연될 수도 있다.

어떤 기업이 사이버 공격을 당했을 때, EU에서는 해당 기업이 의무적으로 신고해야 하지만 미국은 신고 의무는 없으나 신고 시에는 법적 책임 면제를 비롯한 여러 건의 혜택을 부여한다. 앞에서도 언급한 바와 같이 미국의 제도는 기업에게 매우 유리하기 때문에 사건이 발생했을 때 자발적 신고를 기대할 수 있지만 EU의 제도 하에서 기업은 신고에 따르는 손실과 신고의무 위반에 따른 손실을 비교해서 전자가 더 크면 사건을 은폐하려고 할 것이다. 따라서 정보공유의 효율성 측면에서는 미국의 제도가 우월하다고 판단된다. 즉 사이버 침해 사건에 대한 데이터가 커질수록 데이터 분석을 통해 더 유용한 정보를 추출할 수 있을 것이다. 그러나 법적 책임의 면제는 결국 손실의 전가를 의미하기 때문에 과연 사회적으로 바람직한가라는 문제가 제기된다.

다. 초연결사회 도래에 따른 사이버보안 정책 동향

초연결사회의 진전에 따라 미국과 EU에서는 IoT, 빅데이터, 인공지능 등 초연결사회를 지원하는 핵심 기술요소들의 보안을 위한 정책을 개발하고 있다. 이러한 새로운 기술들은 기존의 전통적인 사이버보안의 과제들에서 다루지 않았던 새로운 이슈들을 제기하고 있다. 여기서는 미국과 EU의 관련 정책 부서에서 발표한 보고서의 주요 내용을 살펴보면서 그들의 정책 방향을 파악해 보기로 한다.

2016년 미국 국토안보부는 '사물 인터넷 보안을 위한 전략적 원칙들(Strategic Principles for Securing the Internet of Things(IoT)'이라는 보고서를 발표했는데 여기서는 사물 인터넷 보안을 위한 6대 원칙이 제시되었다.[33] 또한 이 보고서는 IoT 개

33) 6대 원칙은 다음과 같다. ⅰ) 설계 단계에서 보안을 구현할 것, ⅱ) 보안 업데이트와 취약점 관리를 독려할 것, ⅲ) 검증된 보안 행동(security practices)들에 의존할 것, ⅳ) 잠재적 영향력에 따라 보안 대책들의 우선순위를 정할 것, ⅴ) IoT 전반에 걸쳐 투명성을 제고할 것, ⅵ) 연결은 주의 깊게, 그리고 연결의 필요성을 의도적으로 점검할 것(U.S. Department of Homeland Security, 2016).

발자, 서비스 제공자 등 이해 당사자들이 취해야 할 IoT 보안을 위한 행동들도 제안했다.

국토안보부는 이 보고서가 IoT 보안을 위한 다른 정부 기관과 민간 기관의 노력을 지원하는 첫발에 해당하며 다음과 같은 정책적 노력을 취할 예정임을 밝혔다. 첫째, IoT가 제기하는 위험을 완화하기 위한 길을 정부와 민간이 함께 모색하기 위해 국토안보부는 연방 기관들과 IoT 관련 이해 당사자들을 조율하는 역할을 하겠다. 둘째, 국토안보부는 IoT 관련 위험에 대한 인식을 제고하고 교육ㆍ훈련을 강화하겠다. 셋째, IoT 보안을 제고하기 위한 유인을 마련하기 위해 관련 정책 및 입법 기관과 이해 당사자들과 함께 노력하겠다. 넷째, IoT의 국제 표준화를 위한 국제기관 및 민간의 노력을 지원하고 그들도 IoT 관련 혁신 및 보안을 위한 노력에 동참하도록 유도하겠다(U.S. Department of Homeland Security, 2016).

2016년 10월 미국 대통령 산하 국가과학기술평의회(National Science and Technology Council)는 '국가 인공지능 연구개발 전략계획(National Artificial intelligence Research and Development Strategic Plan)'을 발표했다. 이 계획에는 7개의 인공지능 관련 연구개발 전략이 포함되어 있고 그 중 하나가 '인공지능 시스템의 안전성과 보안성 확보'이다. 그 주요 내용은 다음과 같다.

인공지능 시스템들은 다음과 같은 이유로 중대한 안전 및 보안 과제들에 직면해 있다. 첫째, 인공지능 시스템은 복잡한 환경에서 작동하도록 설계되며 그 중 상당수의 상태(state)들은 미리 검증되지 않기 때문에 설계 당시에 고려되지 않았던 상황에 직면할 수도 있다. 둘째, 비지도 학습(unsupervised learning)에 의해 결정되는 인공지능의 행동은 예측하기가 어렵다. 셋째, 인간의 목표를 컴퓨터 명령어로 번역하기가 어렵기 때문에 인공지능 시스템에 프로그램화된 목표들이 프로그래머가 의도한 목표와 일치하지 않을 수도 있다. 넷째, 많은 경우에 인공지능 시스템의 작동 결과는 인간의 상호작용에 의해 영향을 받는다. 이 경우 인간의 반응의 변이가 시스템 안전성에 영향을 준다. 이와 같은 이슈들에 대해 인공지능의 안전성과 보안성을 제고하기 위해서는 인공지능의 설명가능성(explainability), 투명성, 신뢰, 검증 및 타당성

(verification and validation) 그리고 공격에 대한 보안, 장기적인 인공지능 안전성과 가치 일치(value-alignment) 등의 이슈에 추가적인 투자가 필요하다(National Science and Technology Council, 2016a).

또한 2016년 10월 국가과학기술평의회는 '인공지능의 미래에 대한 준비(Preparing for the Future of Artificial Intelligence)'라는 보고서를 발표했다. 여기서는 National Science and Technology Council (2016a)에서 제기한 이슈들 외에도 인간의 의사 결정을 대신하는 인공지능의 결정이 어떻게 정의, 공정성, 책임성을 담보할 수 있는지에 대해 의문을 제기했다. 사실 이러한 의문은 빅데이터에 대한 미국 정부 보고서들에서 제기된 의문의 연장선에 있다(Executive office of the president, 2014).

의사 결정의 투명성은 데이터, 알고리즘뿐만 아니라 의사 결정에 대한 설명가능성도 포함하는 것인데 많은 인공지능 전문가들은 진보된 인공지능의 행태를 이해하고 예측하는 데는 태생적인 어려움이 있음을 경고하고 있다. 최근 인공지능을 이용한 자율적 또는 반 자율적 무기들이 개발되면서 인간의 제어를 벗어난 무기들에 대한 법적, 윤리적 문제가 제기되고 있다. 이 보고서에서 국가과학기술평의회는 자율적 또는 반 자율적 무기의 개발은 인도주의에 대한 국제법을 준수해야 함을 강조했다(National Science and Technology Council, 2016b).

2015년 12월 유럽네트워크정보보호원(ENISA, 2015a)은 '빅데이터 보안(Big Data Security)'라는 보고서를 발표했는데 여기서 빅데이터 보안과 관련된 핵심과제들을 다음과 같이 제시했다. 첫째는 접근 제어와 비준이다. 데이터 접근을 원하는 다양한 이용자의 보안 수준 때문에 필요한 접근 제어와 비준의 수준을 유지하기 어렵다. 둘째, 빅데이터 환경에서 수집되는 대량의 로그 데이터를 안전하게 저장하고 관리하는 것이 큰 과제이다. 셋째, 빅데이터 시스템은 다양한 정보 출처로부터 데이터를 수집하는데 일부 출처들은 신뢰성이 검증되지 않는다. 따라서 검증되지 않은 데이터를 이용하는 빅데이터 분석은 잠재적으로 부정확한 결과를 초래한다(ENISA, 2015a).

위 보고서는 데이터의 수집과 저장 및 접근과 관련된 보안 문제에 초점을 두고 있

는 반면 최근 네덜란드의 정부 자문기구의 빅데이터 보안정책 관련 보고서는 데이터의 분석 및 활용 단계에서의 보안 문제로 초점을 이동시키면서 미국 정부가 제시한 빅데이터 보완 이슈와 유사한 과제를 제기했다. 2017년 네덜란드 정부의 과학 협의회(Netherlands Scientific Council for Government Policy)는 정부 기관이 사용하는 빅데이터 분석에 대한 규제의 초점이 데이터 수집에서 데이터 분석 및 이용으로 이동해야 한다고 주장하면서 그 이유와 대응책을 다음과 같이 설명하고 있다.

데이터 분석 단계에서는 알고리즘, 데이터 소스와 범주, 다양한 데이터에 대한 가중치 등에 대한 선택이 이루어지지만 현행 법 체계에서는 분석 단계는 규제의 사각지대이고 알고리즘의 책임성은 결여되어 있다. 이러한 문제에 대응해서 데이터 품질, 방법론의 건전성, 그리고 사용된 알고리즘의 직관성 등에 대한 기본적인 요구조건을 고려할 수 있다. 데이터의 최신성과 무결성을 유지하는 것은 기본이지만 알고리즘과 방법론이 과학적 방법론의 기준에 부합해야 하며 그 검증은 소관 감사당국에 의해 공개적으로 이루어져야 한다. 그리고 데이터 분석 주체는 어떻게 자신의 분석 결과를 도출했는지를 증명할 수 있어야 한다(WWR, 2017).

빅데이터 보안 분야에서 데이터 수집 및 보관과 관련된 보안 문제는 전통적인 사이버보안 이슈 중 하나인 데이터 무결성에 관한 것으로 볼 수 있다. 그러나 데이터 분석 단계에서 소위 '블랙 박스' 안에서 벌어질 수 있는 자의적인 알고리즘 및 방법론의 선택에 의한 분석 결과의 왜곡 문제는 인공지능 보안문제와 같이 초연결사회에서 새롭게 등장한 사이버보안 문제라고 할 수 있다. 그 동안 미국과 EU의 관련 정책 보고서를 통해서 문제의 본질이 드러나고 있지만 아직도 연구의 여지가 많이 남아 있어서 연구 결과가 정책으로 전환되기까지는 더 많은 논의가 필요할 것이다.

3. IoT 환경에서의 설계에 의한 프라이버시

수많은 기기들이 연결된 초연결사회에서 우리의 삶은 점점 더 많은 기술과 기기들을 활용하여 더욱 풍성해질 것이라는 긍정적 기대와 함께 한편에서는 우리의 정

보를 수집하고 분석한 수많은 결과들에 대한 프라이버시 관점에서의 우려도 증가하고 있다. 다양한 데이터가 수집되고 처리되는 과정에 대한 사람들의 지속적 인식의 어려움과 수집된 정보의 과용 또는 오용에 대한 일반인들의 입증의 어려움(ENISA, 2014)은 서비스의 초기 기획 단계에서부터 이용자의 프라이버시와 데이터를 보호하는 '설계에 의한 프라이버시(Privacy by Design)'의 도입에 대한 당위성을 부여한다.

설계에 의한 프라이버시를 최초로 주장한 Cavoukian은 OECD의 공정한 정보관행 원칙(Fair Information Practice Principles: FIPPs)[34]에 기초하여 정보기술, 사업관행, 네트워크 인프라에 선제적으로 프라이버시를 내재화하는 것을 통해 개인은 개인정보보호의 안전대책을 걱정하지 않고 그들의 프라이버시가 큰 틀 안에서 보장되고 있음을 확신하는 위치에 놓이게 된다고 하였다(Cavoukian et al., 2014; Cavoukian, 2014).

이러한 설계에 의한 프라이버시는 사물인터넷 시대에 이용자의 프라이버시 보호와 보안뿐만 아니라 기업 차원에서도 스스로를 보호할 수 있는 유일한 방안이라는 주장도 있다. Coraggio(2015. 12. 31.)는 사물인터넷 기술과 관련하여 적용가능한 개인정보보호 의무가 여전히 불확실한 규제환경에서 데이터 유출 사고 등이 발생하였을 때 기업이 스스로를 보호하기 위한 유일한 방법이 설계에 의한 프라이버시임을 주장하였다. 이처럼 소비자와 기업 모두에게 필수적인 설계에 의한 프라이버시는 정보보호에 대한 인식이 높아지고 연결된 수많은 기기들간의 데이터 전송이 이루어지는 초연결 사회에서 더욱 주목받을 것으로 예상된다.

가. 설계에 의한 프라이버시와 GDPR

설계에 의한 프라이버시는 일반적 원칙과 개인정보보호 기술을 동시에 다루는 중

34) OECD가 발표한 프라이버시 가이드라인(Privacy Guideline)에 포함되어 있는 8가지 원칙, 즉 수집제한, 정보정확성, 목적명확성, 이용제한, 안정성 확보, 공개, 정보주체의 참여, 수집기관 책임의 원칙을 말한다(손상영 외, 2016).

요한 개념이지만 이를 채택하도록 하는 인센티브 제공이 없다는 점(ENISA, 2014), 시스템 설계자의 역할이 관련 법에 명시되어 있지 않으므로 법적 근거가 없다는 점[35] 등의 한계가 지적되었다. 그러나 2018년 5월부터 발효되는 EU의 GDPR(General Data Protection Regulation)이 설계에 의한 프라이버시 보호(Privacy by design), 기본 설정에 의한 데이터 보호(Data protection by default), 그리고 설계에 의한 데이터 보호(Data protection by design)가 직접 언급되고 이러한 개념에 기초하여 작성되었기에 법적 근거도 마련된 상황으로(European Commission, 2016; Cavoukian, 2016; Mahan, 2016. 8. 9.; 보안뉴스, 2016. 10. 6.) 향후 더욱 확대될 것으로 예상된다.[36] 더욱이 글로벌 기업들은 유럽연합 거주자를 상대로 서비스나 상품을 제공하고 행동을 모니터링하는 경우 GDPR의 적용대상이 되기 때문에 개인정보보호 규범의 수준을 유럽연합에 맞추는 수준으로 상향평준화될 것으로 예상된다(이은우, 2016. 7. 10.).

1) GDPR 25조(Data protection by design and by default)

GDPR에서는 제4장 정보처리자와 수탁처리자(Controller and processor), 제1절 일반적 의무(General obligations)의 제25조에 “Data protection by design and by default”를 명시하고 있다. 주요 내용은 다음과 같다.

· 제25조 1항. “최신 기술과 실행 비용, 처리의 성격과 범위, 상황, 목적뿐 아니라 처리로 인해 개인의 권리와 자유에 대해 발생할 수 있는 변경 가능성과 중대성의 위험성을 참작하여, 정보처리자는 처리 수단을 결정한 시점과 처리 당시 시점에서 데이터 최소화 등 개인정보보호의 원칙을 이행하고 본 규정의 요건을 충족하고 정보주체의 권리를 보호하기 위해 처리에 필요한 안전조치를 포함하기 위해 고안된 가명처리 등 적절한 기술 및 관리조치를 이행해야 한다.”

---

35) Wikipedia, “Privacy by Design”(https://en.wikipedia.org/wiki/Privacy_by_design, 검색일: 2017. 8. 1.)

36) GDPR의 채택에 따라, EU 회원국은 2018년 5월 6일까지 개정규정을 자국법에 적용시켜야 하며, 규정은 2018년 5월 25일부터 발효된다(Tech M, 2016. 8. 11.).

· 제25조 2항. “정보처리자는 기본 설정을 통해 처리의 개별 특정 목적에 필요한 정도에 한하여 개인정보가 처리될 수 있도록 보장하기 위한 적절한 기술 및 관리조치를 이행해야 한다. 이러한 의무는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보관기간 및 접근용이성에 적용된다. 특히, 이러한 조치는 개인정보가 관련 개인의 개입없이 불특정 다수에게 열람되지 않도록 기본 설정을 통해 보장한다.”
· 제25조 3항. “제42조에 근거한 공식 인증 메커니즘은 본 조항의 제1항 및 제2항에 규정된 요건의 준수를 입증하는 요소로 이용될 수 있다.”

GDPR 안내서를 발간한 행정자치부·한국인터넷진흥원(2017)은 정보처리자(controller)가 최신 기술, 실행 비용, 개인정보 처리의 성격과 범위, 상황, 목적, 개인정보 처리로 인해 개인의 권리와 자유에 대해 발생할 수 있는 변경 가능성, 중대성 및 위험성을 고려하여 취할수 있는 적절한 기술적·조직적 조치에는 개인정보처리의 최소화(data minimisation), 처리에 필요한 보호조치(safeguards), 가명화(pseudonymisation) 등이 해당된다고 설명하고 있다.[37] 또한 정보처리자(controller)가 기본 설정을 통해 처리 목적에 필요한 범위 내에서 개인정보가 처리될 수 있도록 적절한 기술적·조직적 조치를 실시해야 함과 동시에 이러한 조치는 수집되는 개인정보의 양, 해당 처리의 범위, 개인정보의 보유기간 및 접근 가능성(accessibility)에 대해서도 적용된다고 안내하고 있다(행정자치부·한국인터넷진흥원, 2017).

이러한 GDPR의 설계에 의한 데이터 보호 및 기본 설정에 의한 데이터 보호는 유럽의 개인정보보호정책을 근본적으로 변화시키는 주요 개념 중 하나이다. 설계에 의한 데이터 보호는 개인의 데이터 처리와 관련된 새로운 제품과 프로세스, 서비스의 초기개발 단계에서부터 전체 개발 과정의 전반에 걸쳐 기업이 개인정보보호를

37) 행정자치부·한국인터넷진흥원(2017)은 “기업이 모든 프로젝트의 초기단계에서 개인정보 보호를 중요한 고려사항으로 하고, 전체 라이프 사이클에서 전반에 걸쳐 개인정보를 보호하는 것을 권장”하고 있다.

고려해야 한다고 주장한다. 기본 설정으로서의 데이터 보호는 시스템이나 서비스에서 개인이 다른 사람과 공유하는 개인정보의 양에 대해 선택할 때 기본 설정이 가장 프라이버시 친화적이어야 한다는 것을 의미한다.

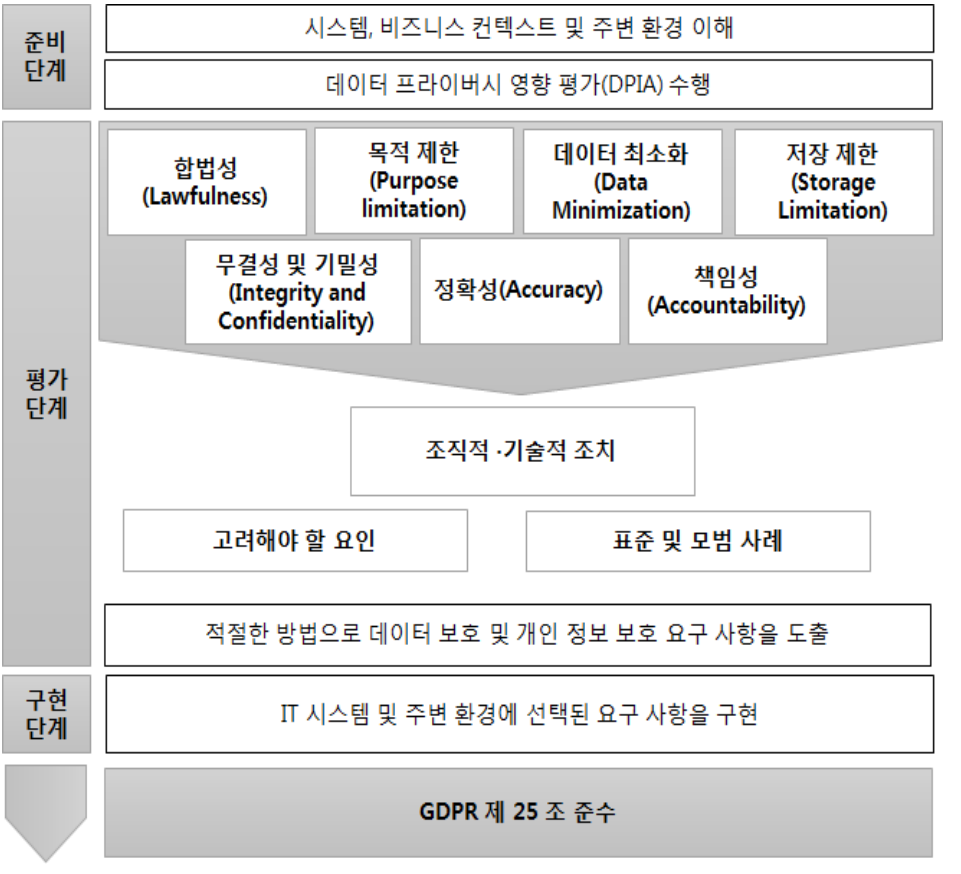
2) 설계에 의한 프라이버시에 기초한 GDPR 25조 적용 프레임워크

GDPR의 실제적 적용 논의는 아직 초기단계이다. 여기에서는 새로운 GDPR을 준수하도록 돕기 위해 수행된 작업이 아직까지 없었음을 지적하며, 유럽의 일반 데이터 보호 규정 (GDPR)의 프라이버시 정책이 IT 시스템에 어떻게 구체적으로 구현되어야 하는지를 연구한 ElShekeil & Laoyookhong (2017)의 논의를 소개하고자 한다. 이들은 GDPR 25조와 다른 조항에 제시되어 있는 데이터 보호 원칙을 분석하여 다음과 같이 GDPR의 7대 데이터 보호 원칙을 책임성(Accountability), 목적 제한(Purpose Limitation), 저장 제한(Storage Limitation), 무결성 및 기밀성(Integrity and Confidentiality), 데이터 최소화(Data Minimization), 정확성(Accuracy), 합법성, 공정성 및 투명성(Lawfulness, Fairness and Transparency)으로 정리하고 여기에 기반하여 APSIDAL 프레임워크를 제시하고 있다(ElShekeil and Laoyookhong, 2017).[38)]

ElShekeil and Laoyookhong(2017)가 제시한 프레임워크는 준비 단계, 평가 단계, 구현 단계의 세 단계로 구성된다. 먼저, 준비 단계에서는 시스템, 비즈니스 컨텍스트 및 주변 환경을 조사하여 범위를 올바르게 이해하는 과정과 개인 데이터 처리가 데이터 주체에 미치는 영향을 확인하기 위해 데이터 프라이버시 영향 평가(Data Privacy Impact Assessment, DPIA)를 수행하는 과정으로 구성된다.

38) GDPR 데이터 보호를 구현하기 위해 제안된 APSIDAL 프레임워크는 법적인 요구사항을 파악하여 7개 데이터 보호 원칙과 목표를 달성하기 위해 필요한 조직적 및 기술적 조치의 제안하고 있다.

〔그림 4－2〕 APSIDAL 프레임워크



출처: ElShekeil and Laoyookhong(2017) p.13

다음으로 평가단계에서는 개인 데이터 처리 전에 법적 근거의 고려 등 앞서 제시된 GDPR의 7대 데이터 보호 원칙과 관련된 GDPR의 규정, 목표, 조직적 조치와 기술적 조치 등 핵심 요소를 제시하고 있다.[39]

39) GDPR의 7대 데이터 보호원칙과 관련된 조직적 조치와 기술적 조치의 상세한 내용은 ElShekeil and Laoyookhong(2017)를 참고하라.

〈표 4－2〉 GDPR의 7대 데이터 보호 원칙과 관련 규정

	7대 원칙	GDPR 규정	목표
1	합법성, 공정성 및 투명성 (Lawfulness, Fairness and Transparency)	GDPR Art.5.1 (a) “정보 주체와 관련하여 합법적으로, 공정하게 투명하게 처리”	개인 데이터 처리는 확고한 법적 근거에 따름. 데이터 컨트롤러는 데이터 수집 및 처리 전에 정보주체에 대한 결과에 관해 명확한 견해를 제시해야 함
2	목적 제한 (Purpose Limitation)	GDPR Art.5.1 (b) “명시적이며 적법한 특정 목적을 위해 수집되고 해당 목적과 양립하지 않는 방식으로 추가적 처리 되어서는 안됨. 공익적인 기록보존 목적 또는 과학 및 역사 연구 또는 통계 목적을 위한 추가적 개인정보처리는 제 89조 (1)항에 따라 최초의 목적과 양립되지 않는다고 간주되지 않음”	데이터 컨트롤러가 데이터 수집 및 처리의 이유를 정의하고, 원래 목적에 따라 데이터 처리. 또한 처리의 목적 제한의 확인을 위해 데이터 수명주기 전반에 걸친 데이터 추적성의 확보
3	데이터 최소화 (Data Minimization)	GDPR Art. 5.1 (c) “개인정보가 처리되는 목적과 관련하여 적절하고 타당하고 필요한 범위로 제한”	수집된 데이터의 양을 줄이는 것
4	정확성 (Accuracy)	GDPR Art. 5.1 (d) “정확하고, 필요시 최신 정보이어야 함; 처리 목적과 관련하여 부정확한 개인 정보는 지체 없이 삭제 또는 정정되도록 합리적인 일체의 조치가 취해져야 함”	데이터 컨트롤러는 수집한 데이터의 정확성을 확인하고 데이터 소스를 확인하는 필요조치를 취해야 함. 또 필요시 정보의 정확성에 대한 모든 문제를 고려하여 최신 정보를 유지
5	저장 제한 (Storage Limitation)	GDPR Art. 5.1 (e) “개인정보의 처리목적에 필요한 기간에 한해서 정보주체가 식별될 수 있는 형태로 보관되어야 함. 개인정보는 정보주체의 권리와 자유를 보호하기 위해 본 규정에서 요구하는 적절한 기술 및 관리조치를 규정하는 제89조 (1)항에 따라 공익적인 기록보존 목적 또는 과학 및 역사연구	데이터가 목적을 달성하는 기간 동안만 식별가능한 데이터를 유지. 데이터 컨트롤러는 원래 목적으로 더 이상 처리되지 않는 정보의 추적 및 제거에 책임이 있음

	7대 원칙	GDPR 규정	목표
		목적이나 통계목적에 한해 개인정보를 처리하는 경우, 해당 개인정보는 보유기간 연장 가능”	
6	무결성 및 기밀 유지 (Integrity and Confidentiality)	GDPR Art. 5.1 (f) “적절한 기술 및 관리조치를 이용하여, 무단(unauthorized) 또는 불법적 처리나 사고로 인한 손실이나 파기, 손상에 대한 보호조치를 포함한 개인정보의 적절한 보안을 보장하는 방식으로 처리”	무결성 및 기밀성은 정보 보안 기반의 일부. 이 원칙에 대한 조치는 데이터 수명주기 전반에 걸쳐 구현되고 운영되어야함
7	책임성 (Accountability)	GDPR Art. 5.2 “정보처리자는 제1항의 준수를 책임지고 이에 대한 준수를 입증할 수 있어야 함”	책임성은 GDPR에 도입된 새로운 개념. 데이터 컨트롤러는 규정의 조항을 준수함을 입증하고 책임져야함. 이는 합법적이지 않은 개인 데이터의 미처리, 개인 정보 보호 원칙의 IT 시스템 구현 등으로 수행가능

출처: ElShekeil and Laoyookhong(2017) 재구성

또한 프레임워크의 사용자가 참조할 수 있는 표준 및 모범 사례를 다음과 같이 제시하고 있다.

〈표 4－3〉 데이터 보호, 프라이버시 및 보안 조치 관련 표준 및 모범사례

구분	표준 및 모범사례	
조직적 조치	ISO 27000	조직이 정보 자산을 보호하는 데 도움이 되는 표준 세트
	ISO 29100	개인 식별 정보를 처리하는 조직을 위한 프레임워크 및 일련의 통제
	ISO 27018	공공 클라우드에서 개인 식별 정보를 보호하기 위한 컨트롤 세트
	UCF	통합 컴플라이언스 프레임워크는 조직 및 기술 요구에 모두 적용할 수 있는 포괄적인 컨트롤 세트를 유지 관리하는 라이브러리

구분	표준 및 모범사례	
	COBIT 5	민감한 개인 데이터 또는 정보 보안 (SPDI)을 위한 다양한 원동력을 포함하는 ISACA에서 제작 한 비즈니스 프레임워크
기술적 조치	NIST 800-53	정보 시스템을 위한 기술 보안 통제
	ENISA(2015b)	프라이버시 강화 기술 가이드로 개인 정보 보호를 위한 일련의 기술 개인 정보 보호 조치 제시

출처: ElShekeil and Laoyookhong(2017) pp.22-23

ElShekeil and Laoyookhong(2017)은 개발중이거나 운영중인 모든 IT 시스템에 적용할 수 있도록 IT 시스템의 설계 단계에서는 LINDDUN, 위협모델링, 공통기준(ISO/IEC 15408) 등을 활용할 것을, 그리고 IT 시스템이 이미 작동중인 경우에는 정적 및 동적 코드 검토 또는 침입 테스트와 취약점 테스트를 통해 해결가능한 결함을 식별할 것을 제안하고 있다.

〈표 4－4〉 데이터 보호, 프라이버시 및 보안 요구 사항 도출을 위한 접근방식

구분	기술/방법	주요 내용
설계중인 시스템	LINDDUN	LINDDUN은 소프트웨어 기반 시스템에서 개인 정보 위협을 식별하기위한 포괄적인 프레임워크
	위협 모델링 (Threat Modelling)	위협 모델링은 위협이 식별될 수 있는 시스템의 설계 단계에서 사용
	공통 기준 (Common Criteria, ISO/IEC 15408)	공통 기준 (ISO / IEC 15408)은 정보 시스템의 보안 요구 사항에 대한 국제 표준
운영 시스템	침투 및 취약점 테스트 (Penetration and Vulnerability testing)	시스템이 운영 단계에 있는 경우 침투 테스트 및 취약점 검색을 사용하여 공격자의 관점에서 시스템 결함을 식별가능
	정적 및 동적 코드 검토 (Static and Dynamic Code Reviews)	정적 및 동적 코드 검토는 소프트웨어를 검토하는 또 다른 방법

출처: ElShekeil and Laoyookhong(2017) pp.23-24

ElShekeil and Laoyookhong(2017)은 앞서 제시된 여러 조치들을 평가단계에서 이행하면 GDPR의 데이터 보호원칙은 준수될 것이며, IT 시스템은 GDPR의 준수를 위

해 제시된 요구 사항을 보장해야 한다고 주장한다. 이들의 연구는 실제로 IT 시스템에 제안된 기술 조치의 적용 가능성을 깊이 다루고 있지는 않지만 법적 의무 준수 여부에 초점을 맞추어 조직 및 IT 시스템 수준에서 GDPR의 데이터 보호원칙 준수를 통한 프라이버시 보호 구현에 있어 참고할만한 가치가 있다.

나. 설계에 의한 프라이버시와 IoT에의 적용

1) IoT 시대의 설계에 의한 프라이버시 원칙

설계에 의한 프라이버시의 7대 원칙은 2차연도 연구(손상영 외, 2016)에서 정리한 바 있다. 여기서는 이 7대 원칙을 사물인터넷 시대에 적용하여 소개한 Cavoukian and Popa(2016)의 논의를 소개한다.

〈표 4－5〉 설계에 의한 프라이버시의 7대 원칙과 IoT에의 적용

구분	설계에 의한 프라이버시의 7대 원칙	IoT에의 적용
1	사후대응이 아닌 사전 대응(Proactive not Reactive; Preventive not Remedial)	남용의 기회를 예상하고 제거(Anticipate and Eliminate Opportunities for Abuse)
2	프라이버시를 기본 설정으로 (Privacy as the Default Setting)	프라이버시를 기본 설정으로(Configure Privacy by Default)
3	설계에 배태된 프라이버시(Privacy Embedded into Design)	무결성을 설계에 배태하는 것(Embed Integrity into Design)
4	최대의 기능성－제로섬이 아닌, 포지티브 섬 (Full Functionality-Positive Sum, not Zero-Sum)	최적화된 경험을 최대의 기능성에 통합(Fuse Optimized Experiences to Full Functionality)
5	End-to-End 보안－데이터 생애주기 보호 (End-to-End Security-Full Lifecycle Protection)	보호 설계를 명확하고 단순화(Clarify and Simplify for Protective Design)
6	가시성과 투명성－공개 (Visibility and Transparency-Keep it Open)	모니터링 및 인식의 제어(Control Monitoring and Awareness)
7	이용자 프라이버시 존중－이용자 중심 (Respect for User Privacy-Keep it User-Centric)	이용자를 피해자가 아닌 이해관계자로 포함 (Include Users as Stakeholders, not Victims)

출처: Cavoukian et al.(2014); Cavoukian,(2014); Cavoukian and Popa(2016) 재정리.

먼저, ‘사후대응이 아닌 사전 대응(Proactive not Reactive; Preventive not Remedial)’과 관련하여 IoT의 프라이버시 개념은 ‘남용의 기회를 예상하고 제거(Anticipate and Eliminate Opportunities for Abuse)하는 것이다. 선제적 예방을 목표로 한다는 점에서 그 맥을 같이하며 동의 절차가 미래의 프라이버시 침해 예방에 가장 큰 도움이 될 것으로 보고 있다.

둘째, ‘프라이버시를 기본 설정으로(Privacy as the Default Setting)’와 관련하여 IoT의 프라이버시 개념도 ‘프라이버시를 기본 설정으로(Configure Privacy by Default)’라는 점에서 동일하다. IoT라고 해서 전혀 다른 새로운 프로세스를 추구하는 것이 아니라 개인들이 아무런 조치를 취하지 않아도 프라이버시가 보호되도록 시스템에 기본 설정으로 구축하는 것에서 출발해야 한다.

셋째, ‘설계에 배태된 프라이버시(Privacy Embedded into Design)’와 관련하여 IoT의 프라이버시 개념은 ‘무결성을 설계에 배태하는 것(Embed Integrity into Design)’이다. IoT에 프라이버시 보호를 레이어링하고 삽입하는 것은 추후의 악용이나 남용을 방지하고 초기에 보호를 하는 데 중요하다.

넷째, ‘최대의 기능성－제로섬이 아닌, 포지티브 섬(Full Functionality-Positive Sum, not Zero-Sum)’과 관련하여 IoT의 프라이버시 개념은 ‘최적화된 경험을 최대의 기능성에 통합(Fuse Optimized Experiences to Full Functionality)’하는 것이다. 이용자들이 프라이버시와 보안 둘 중 하나를 선택하거나 안전대책으로 감시를 받아들여야 하는 것은 긍정적 해결책이 아니며 ‘윈－윈’ 시나리오를 만들어내기 위해 프라이버시와 보안을 유지하며 이용자 경험을 극대화하는 혁신을 도입해야 한다.

다섯째, ‘End-to-End 보안－데이터 생애주기 보호(End-to-End Security-Full Lifecycle Protection)’와 관련하여 IoT의 프라이버시 개념은 ‘보호 설계를 명확화 및 단순화(Clarify and Simplify for Protective Design)’ 하는 것이다. 복잡성은 유용성을 약화시키므로 사물인터넷에서의 설계에 의한 디자인은 전체 디자인 및 사용자 경험을 통해 분명하고 쉽게 접근 가능한 단순한 메시지로 시작되어야 한다.

여섯째, ‘가시성과 투명성－공개(Visibility and Transparency-Keep it Open)’와 관련

하여 IoT의 프라이버시 개념은 '모니터링 및 인식의 제어(Control Monitoring and Awareness)'이다. 사물인터넷은 열린 설계에 기초하고 있다. 정보의 이용자와 공급자 모두에게 그 구성요소와 운영과정은 가시적이고 투명함을 원칙으로 하는 것에 기초하여야 하며 기술자들은 보호를 위한 모니터링과 감시 사이의 경계를 분명히 알아야 하며 책임성 있는 모니터링을 수행하여야 한다.

마지막으로, '이용자 프라이버시 존중－이용자 중심(Respect for User Privacy-Keep it User-Centric)'과 관련하여 IoT의 프라이버시 개념은 '이용자를 피해자가 아닌 이해관계자로 포함(Include Users as Stakeholders, not Victims)'하는 것이다. 사물인터넷에서 모든 개인은 콘텐츠 생성의 노드라는 개념을 가진다면 혁신가들이나 기술자들이 프라이버시 보호의 길에서 이탈하는 것을 방지할 수 있다. 또한 이용자를 이해관계자로 인식함으로써 신뢰기반의 생태계를 구성해나갈 수 있을 것이다.

사물인터넷 공간에서의 제품과 솔루션 설계는 혁신적이고, 유용하고 효과적이어야만 한다. 그러나 좋은 디자인 원칙을 준수하려면 철저해야 하고, 상세해야 하며, 거슬리지 않고 심미적이어야 하며, 사회적으로 책임성 있고 정직해야 한다(Cavoukian and Popa, 2016). 이러한 차원에서 IoT 환경에서의 설계에 의한 프라이버시 전략의 준수는 더욱 중요할 것이다.

2) 설계에 의한 프라이버시의 적용

설계에 의한 프라이버시의 적용이 이루어지기 위해서는 개발 과정의 초기에 서비스와 제품에서 프라이버시를 어떻게 다룰 것인지 선택을 하는 것이 필수적이다.[40]

설계에 의한 프라이버시 적용이 성공적으로 이루어지려면 신제품 및 서비스 개발에 참여하는 직원들이 프라이버시와 관련된 지식이 충분해야 한다. 이를 위해 데이

40) 개인정보영향평가(Privacy Impact Assessment)를 실행하는 것이 프라이버시 위험을 판별하고 관련 의사 결정에 도움이 된다. 또한 데이터 주체가 개인 데이터 처리 및 권리 행사 방법에 대해 알고 싶을 때 소통할 수 있는 곳이 명확해야 하며, 적절한 보안 조치, 데이터 품질을 보장할 수 있는 방법, 그리고 제품 또는 서비스를 폐기할 때 데이터로 수행 작업 등을 미리 생각하고 설계하는 것이 중요하다.

터 보호와 관련된 명확한 정책, 지침 및 작업 지침을 개발해야 하며, 그 과정을 이끌어줄 개인정보보호 전문가가 있어야 한다.

· IoT에서의 설계에 의한 프라이버시 가이드라인

IoT에서의 설계에 의한 프라이버시의 실제적 적용과 관련하여서는 아직 관련된 논의와 연구가 초기 단계이다. ENISA(2015a) 등 일부 연구들에서 설계에 의한 프라이버시의 구현을 위한 전략을 제시하고는 있지만 아직까지는 Cavoukian이 정리한 7대 원칙의 실제적 적용이나 구현이 제대로 이루어지지는 못한 것으로 파악된다. 이러한 문제의식의 연장선상에서 Perera et al.(2016)은 지금까지 IoT 응용 프로그램과 미들웨어 플랫폼에 프라이버시 문제가 고려되지 못하였고, 기존의 설계에 의한 프라이버시 프레임워크가 IoT 애플리케이션 및 미들웨어 플랫폼을 설계하는 데 사용 가능한 가이드라인에 적용되어 소프트웨어 엔지니어들에게 제공하지 않았음을 지적하며, IoT에서 소프트웨어 개발 프로세스를 안내할 수 있는 체계적 방법으로 초기 단계의 가이드라인을 소개하고 있다. 여기에서는 이들의 논의를 소개하여 IoT에서의 설계에 의한 프라이버시 가이드라인의 출발점으로 삼고자 한다.

Perera et al.(2016)은 구조화된 가이드라인의 제시를 위해 먼저 IoT 애플리케이션에서의 데이터 흐름을 분석하고 데이터 수명주기를 5단계로 구분하였다.

〈표 4－6〉 IoT 애플리케이션에서의 데이터 수명주기

데이터 수명주기	내용
동의 및 데이터 수집 (CDA)	특정 노드에 의한 라우팅 및 데이터 읽기
데이터 전처리 (DPP)	다른 처리 절차를 준비하기 위해 원시 데이터에 대해 수행되는 모든 유형의 처리
데이터 처리 및 분석 (DPA)	의미있는 정보를 산출하기위한 데이터 항목의 수집 및 조작
데이터 저장소 (DS)	나중에 검색 할 수 있도록 처리 된 정보의 원시 데이터 저장소
데이터 보급 (DD)	외부로 데이터를 전송

출처: Perera et al.(2016) p.2 재구성

여기서 데이터 수명주기의 5단계는 동의 및 데이터 수집, 데이터 전처리, 데이터 처리 및 분석, 데이터 저장소, 데이터 보급이다.

또한 이들은 기존에 논의되고 있는 설계에 의한 프라이버시 프레임워크를 검토한 후 8가지 설계 전략을 검토하여 30개의 가이드라인을 제시하고[41], 이 가이드라인을 따르지 않을 경우 결과적으로 발생가능한 2가지 프라이버시 위험으로 2차적 사용과 무단엑세스를 적시하고 있다. Perera et al.(2016)이 제시한 가이드라인을 요약하면 다음 표와 같다.

41) 8개 설계전략은 최소화(Minimise), 숨기기(Hide), 분리하기(Seperate), 총계(Aggregate), 고지(Inform), 통제(Control), 강제하기(Enforce), 실행(Demonstrate)전략이며, 이 전략에 대한 상세 내용은 손상영 외(2016)에 정리되어 있다.

〈표 4－7〉 설계에 의한 프라이버시 프레임워크 분석

	가이드라인	데이터 수명주기					설계전략								프라이버시 위험	
		DA	DPP	DPA	DS	DD	최소화	숨기기	분리하기	총계	고지	통제	강제하기	실행		
1	데이터 수집 최소화 (Minimise data acquisition)	v	v				v	v							x	-
2	데이터 소스 수 최소화 (Minimise number of data sources)	v					v								x	-
3	원시 데이터raw data 유입 최소화 (Minimise raw data intake)	v	v				v			v					x	
4	지식 발견 최소화 (Minimise knowledge discovery)			v			v								x	-
5	데이터 저장 최소화 (Minimise data storage)				v		v								x	-
6	데이터 보존 기간 최소화 (Minimise data retention period)				v		v	v								-
7	데이터 라우팅 숨기기 (Hidden data routing)	v				v		v								
8	데이터 익명화 (Data anonymisation)	v	v	v		v		v								-
9	암호화된 데이터 통신(Encrypted data communication)	v				v		v								-
10	암호화된 데이터 처리 (Encrypted data processing)		v	v				v								-
11	암호화된 데이터 저장소 (Encrypted data storage)							v							x	
12	데이터 세분성 감소 (Reduce data granularity)	v	v	v		v									x	
13	쿼리 응답 (Query answering)					v	v	v							x	
14	반복되는 쿼리 차단 (Repeated query blocking)					v	v	v							x	-
15	분산 데이터 처리 (Distributed data processing)			v					v						x	-

	가이드라인	데이터 수명주기					설계전략								프라이버시 위험	
		DA	DPP	DPA	DS	DD	최소화	숨기기	분리하기	총계	고지	통제	강제하기	실행		
16	분산 데이터 저장소 (Distributed data storage)				v				v						x	
17	지식 발견 기반 집계 (Knowledge discovery based aggregation)	v	v	v	v	v				v					x	
18	지리 기반 집계 (Geography based aggregation)	v	v	v	v	v				v					x	
19	체인 집합 (Chain aggregation)	v	v	v	v	v				v					x	
20	시간대별 집계 (Time-Period based aggregation)	v	v	v	v	v				v					x	
21	카테고리 기반 집계 (Category based aggregation)	v	v	v	v	v				v					x	
22	정보 공개 (Information disclosure)	v	v	v	v	v					v			v	x	
23	제어 (Control)	v	v	v	v	v						v	v		x	
24	로깅 (Logging)	v	v	v	v	v								v	x	-
25	감사 (Auditing)													v		
26	오픈 소스 (Open source)													v		
27	데이터 흐름 (Data flow)													v		
28	인증 (Certification)													v		
29	표준화 (Standardisation)													v		
30	규정 준수 (Compliance)													v	x	-

주: 프라이버시 위험에서 2차적 사용은 (x), 무단 엑세스는 (-)로 표기

출처: Perera et al. (2016: 6)

Perera et al.(2016)이 제시한 가이드라인은 좋은 출발점이 될 수 있지만, 모든 IoT 애플리케이션이나 플랫폼을 비교하거나 일괄적으로 적용할 수 있는 것은 아니다. 왜냐하면 IoT 플랫폼은 각각의 용도와 목적에 맞도록 설계되기 때문이다. 그럼에도 불구하고 이 가이드라인은 설계에 의한 프라이버시의 적용을 위해 소프트웨어 엔지니어들이 참고할 만한 사항들을 정리하고 있기 때문에 충분한 가치가 있다고 판단된다.

· IoT 환경에의 설계에 의한 프라이버시 적용 노력들

설계에 의한 프라이버시의 적용과 관련된 움직임은 여러 사례에서 포착되고 있다. EU의 사물인터넷 혁신연합(Alliance for Internet of Things Innovations: AIOTI)은 IoT에서의 보안과 프라이버시에 관한 워크숍을 진행한 결과를 2017년 1월에 발표했다(AIOTI, 2017). 워크숍은 초연결 기기의 시장 출시 시간이 단축되면서 설계에 의한 보안과 설계에 의한 프라이버시 조건을 정의하는 지침이 매우 필요하다는 인식하에 유사한 다양한 분야에서 전체 네트워크 아키텍처 및 가치사슬에 대한 최소한의 보안 및 프라이버시 조건을 논의하는 것을 목표로 진행되었다. 그중 일부를 소개하면 다음과 같다.

먼저, 웨어러블 및 스마트 카와 관련한 7개의 기본 보안 및 프라이버시 조건은 다음과 같다.

〈표 4－8〉 웨어러블 및 스마트카 관련 보안 및 프라이버시 조건

구분	웨어러블 및 스마트카 관련 보안 및 프라이버시 조건
1	이용자에 의한 데이터 제어
2	투명성 및 사용자 인터페이스 제어
3	암호화를 기본 설정으로
4	비교적 높은 기준선의 설정
5	보안, 안전, 프라이버시 보호를 전체 생애주기 동안 제공
6	권한있는 자에 의한 신뢰할 수 있고 투명한 업데이트
7	설계에 의한 신원 보호(개인신원정보를 기기 신원과 분리)

출처: AIOTI(2017) p.5 재구성

커넥티드/자율주행차와 관련된 개인 데이터 및 프라이버시의 조건과 관련해서는 다음을 제시하였다.

〈표 4－9〉 커넥티드/자율주행차 관련 개인 데이터 및 프라이버시 조건

구분	커넥티드/자율주행차 관련 개인 데이터 및 프라이버시 조건
1	데이터 세분화, 개인 데이터 영역에서의 데이터 세분화
2	다양한 이해관계자에 따라 정의된 대로 데이터 통제, 평가, 이용
3	투명성을 제1 조건으로 함
4	이용자 선택 및 제어(개인 데이터에 대한 접근 권한 등 전체 보안 관련)
5	설계에 의한 프라이버시 및 프라이버시를 기본 설정으로

출처: AIOTI(2017) pp.5-6 재구성

또한 IEEE의 인터넷 기술 커뮤니티와 기술 및 정책 전문가들은 IoT 환경에서의 보안과 프라이버시와 관련하여 End-to-End 보안과 설계에 의한 프라이버시(Privacy by Design)를 위한 프로포절 개발을 위해 협력할 것이라 발표해 향후 상당한 변화가 예상된다(IEEE, 2016. 11. 16.).

뿐만 아니라 2017년 3월 미국의 캘리포니아주 상원에서는 IoT 기기에 설계에 의한 프라이버시를 요구하는 법안을 발의했는데 기본 골자는 웹으로 연결된 기기 제조업체들은 적절한 보안 기능을 갖춘 기기 및 소비자 정보 이용에 대한 동의 획득을 해야 한다는 것이다(Bonner, 2017. 4. 27.). 캘리포니아주 상원 법안 327호(California Senate Bill 327)는 IoT 기기 제조업체가 소비자 데이터 보안에 대한 책임을 지도록 하는 주정부 및 연방정부의 입법 및 규제 트렌드와 맞닿아 있다. 이 법안은 IoT 기기 제조업체가 추후에 패치를 도입하거나 선택적 또는 반응적으로 업계 모범사례를 취하는 것이 아니라 제품 개발 과정의 초기단계에 선제적으로 '설계에 의한 보안'을 구현하는 최초의 입법명령일 것으로 보이며, 결과적으로 이 법안에 근거한 요구사항들은 향후 IoT 기기 개발에 있어 R&D 및 예산에 상당한 영향을 미칠 것으로 보인다. 제출된 법안의 내용이 그대로 제정된다면 다음과 같은 내용들이 요청될 것으

로 보인다.

- 기기가 수집·보관·전송하는 정보 관련 적절한 보안 기능을 기기에 갖출 것
- 정보를 수집할 때 소비자에게 알려주도록 기기를 설계할 것
- 기기가 정보를 수집하고 전송하기 전에 소비자 동의를 구할 것(사용자 인터페이스를 통해)
- 어떤 데이터가 기기에서 수집되고 있는지 소비자에게 분명한 개인정보보호 고지를 제공할 것
- 기기의 보안을 강화하기 위해 지속적으로 보안 패치와 업데이트를 소비자에게 직접 알릴 것

또한 이 법안은 소매점에서 판매시점에서의 해당 기기의 정보수집 기능에 대한 짧고 분명한 서면 고지를 제공할 것을 요구하도록 하는데, 이 고지서에는 '기기가 오디오, 비디오, 위치정보, 생체정보, 건강 또는 기타 개인/민감한 소비자 정보를 수집할 수 있음'과 기기에 적용되는 프라이버시 정책을 어디에서 찾을 수 있는지의 내용이 포함된다. 아직까지 캘리포니아주 상원 법안 327호의 통과 및 시행 여부는 불확실하지만 분명한 것은 IoT 기기와 관련하여 프라이버시, 데이터 보안을 다루는 데 있어 설계의 초기 단계부터 이용자의 프라이버시와 데이터를 보호하는 트렌드가 확산될 것임은 분명해 보인다.

이처럼 IoT에의 설계에 의한 프라이버시 구현 또는 GDPR의 데이터 보호 원칙 준수 등 사전에 프라이버시를 생각하는 절차는 결과적으로 효율성을 증대시킬 것으로 기대된다(Danon, 2017). GDPR은 초기 단계에서부터 프라이버시를 고려하도록 요구한다는 점에서 설계에 의한 프라이버시 원칙에 기초하고 있다. 이에 따라 IoT에의 적용 프레임워크에서 확인할 수 있듯이 프라이버시는 마지막 단계에서 추가로 고려되는 요소가 아닌 새로운 제품이나 서비스의 주요 요소 중 하나가 된다는 점에서 큰 의미가 있다. 초기 단계에 고려사항이 많아 복잡해 보일 수 있지만, 실제로는 설계가 완료된 후 프라이버시 관련 고려 사항을 적용하는 것은 불가능한 경우가 생기기

도 하고 비용도 더 들기 때문에 초기의 설계단계에서 적용하는 것이 실제로는 더 쉬우며 개발 프로세스도 보다 효율적이 된다. 향후 현재 진행중인 IEEE의 End-to-End 보안과 설계에 의한 프라이버시 프로포절 개발, 미국의 캘리포니아주 상원의 IoT 기기에 설계에 의한 프라이버시를 요구하는 법안의 진행 등 여러 노력들과 더불어 2018년 5월 GDPR의 발효 시점 이후에는 설계에 의한 프라이버시에 기초한 데이터 보호 및 프라이버시 보호가 보안과 프라이버시를 다루는데 있어 매우 중요한 트렌드가 될 것이다.

제 2 절 사이버 복원력 관련 정책 및 국가 사이버 복원력 기반

1. 해외 사이버 복원력 관련 정책 동향

가. 미국

미국은 2006년 국가인프라보호계획(2006 National Infrastructure Protection Plan: NIPP)을 발표하면서 테러 공격이나 사고 발생 시 국가 주요 기능의 복원 능력을 인프라 보호 개념의 일부로 강조하기 시작했다. NIPP는 원래 국가적인 필수 인프라와 핵심자원(Critical Infrastructure and Key Resources: CIKR)의 보호 노력을 통합하려는 의도로 설계되었다. 우선 NIPP의 최우선의 목표는 다음과 같다.

“테러리스트의 의도적인 노력의 효과의 예방, 저지, 무력화 또는 약화하고, 적의 공격, 자연 재해 또는 다른 비상 상황이 발생한 경우에 국가적인 준비성, 적시 대응 그리고 신속 복구 능력을 강화하여 국가의 필수 인프라와 핵심 자원의 보호 수준을 제고함으로써 더욱 안전하고 확고하며 복원력이 강화된 미국을 건설하는 것”이다 (U.S. Department of Homeland Security, 2006: p.1).

2006 NIPP의 거의 모든 부분에 걸쳐서 복원력이라는 용어가 등장하는데 그 공식

적인 정의는 다음과 같다.

“NIPP의 맥락에서 복원력이란 자산, 시스템 또는 네트워크가 테러리스트의 공격 또는 다른 사고 시에 자신의 기능을 유지하거나 복구할 수 있는 역량을 의미”한다 (U.S. Department of Homeland Security, 2006: p.104).

2006 NIPP는 국가적인 필수 인프라나 핵심 자원에서 사이버 인프라적 요소들에 대한 보호를 별도로 분리하지 않고 일반적인 인프라와 통합해서 논하고 있기 때문에 사이버 복원력이라는 용어를 사용하지 않는다. 그러나 분야별로 위험 사정을 수행할 때는 사이버 인프라도 개별적으로 파악되어야 하고 대규모 자산, 시스템 또는 네트워크의 사이버적 요소로서 포함되어야 한다고 했다. 그런데 2006 NIPP가 예시한 사이버 인프라는 ERP, 이메일과 같은 비즈니스 시스템, SCADA와 같은 산업제어시스템, 일반적인 접근제어 시스템 그리고 전화 기반의 경고 시스템 등으로서 시스템 위주의 관점을 보이고 있다. 즉 복원력의 대상을 주로 정보 시스템으로 보고 있다고 할 수 있다.

2009년에는 2006 NIPP를 개정한 2009 NIPP가 발표되었다. 여기에는 ‘partnering to enhance protection and resiliency’라는 부제가 추가됨으로써 복원력이 보호의 개념으로부터 떨어져 나와서 보호와 대등한 위상을 가지게 되었다. 실제로 2009 NIPP의 여러 곳에서 보호와 복원력이라는 용어가 병렬적으로 사용됨으로써 복원력은 NIPP에서 하나의 세부 목표에서 주요 목표로 격상되었다.

2009 NIPP에서는 효과적인 CIKR 보호 프로그램과 복원력 전략이 가져야 할 특성들을 다음과 같이 제시하고 있다.

〈표 4－10〉 CIKR 보호 프로그램과 복원력 전략의 특성

특성	내용
포괄적 (comprehensive)	• 효과적인 프로그램은 CIKR의 물리적, 사이버적 그리고 인간과 관련된 요소들을 적절히 제시해야 하며 장기, 단기 그리고 지속가능한 행동들을 고려해야 함 • 분야 고유의 계획들은 분야 내부에서 CIKR의 보호를 위한 다수의 프로그램과 정책들을 제시해야 함
조율됨 (coordinated)	• 다양한 CIKR 분야들은 고도로 분산되어 있고 복잡하기 때문에 CIKR 보호에 대한 책임은 잘 조율되어야 함 • CIKR 소유자와 운영자는 복원력을 더욱 강화하고 더욱 효과적인 손실 예방을 보장하는 조치를 통해서 재산, 정보 그리고 인력을 보호할 의무가 있음. 이러한 조치로는 테러리스트 위협에 대한 의식 제고, 취약점 감소를 위한 대응작전의 실행 등이 있음 • 주, 지방, 자치구 당국은 자신의 관할구역 내 대중들에게 필수적인 자산, 시스템 그리고 네트워크를 위한 보호 조치를 제공 또는 강화해야 할 의무가 있음. 그들은 보호 프로그램을 개발하고 연방 지침 및 지식을 보완하고 관련된 연방 프로그램을 실행하며, 필요시 법 집행 역량도 제공하며 관할구역의 우선적인 보호 수요에 부응하기 위해 연방 자원에도 접근할 수 있음 • 연방기관들은 국가의 핵심적인 CIKR의 보호 강화 및 CIKR 파트너들의 노력과 상이한 예산 출처로부터 생성된 자원들을 조율해야 할 의무가 있음 • 분야 고유의 기관(Sector-Specific Agency)들은 가장 효과적인 장기 보호 전략에 대한 정보를 제공하고 보호 프로그램을 개발하고 프로그램의 실행을 조율함 • 국토안보부는 다른 유관기관과 협력하면서 국가적으로 필수적인 자산들을 위한 위험관리, 보호 프로그램 및 복원력 전략의 중심점 역할 수행
비용효과적 (cost-effective)	• 효과적인 CIKR 프로그램과 전략은 주어진 지출 규모를 가지고 위험을 최대한 완화할 수 있는 조치들에 집중함으로써 자원을 효율적으로 사용해야 함. • 비용효과성과 공익 추구를 위한 평가요소들: - 완전한 정보를 가지고 업무수행 위협과 그에 상응하는 보호 조치에 대한 정보를 사용할 수 있는 메커니즘 제시 - CIKR 보호에 대한 효과적인 장기적 접근이 가능한 절차와 조율 구조 제시 - CIKR 파트너가 자신의 이익을 위해 자발적으로 조치를 취하도록 하고 부족한 부분만 보완하는 시장 기반의 경제적 유인을 지지 - CIKR 파트너의 이익의 범위를 넘어가는 공익을 위한 지출에 대해서는 공공예산 지원의 우선순위가 부여
위험 고지됨 (risk-informed)	• 보호 프로그램과 복원력 전략의 실행 후 완화된 위험을 평가하는 메커니즘은 상이하므로 다음과 같은 공통의 요소를 포함해야 함

특성	내용
	- 결과: 보호 프로그램과 복원력 전략의 실행은 피해를 감소시킴으로써 결과를 제한하거나 관리할 수 있게 함 - 취약점: 보호 프로그램은 약점을 감소 또는 강화함으로써 취약점을 감소 - 위협: 보호 프로그램과 복원력 전략은 자산, 시스템, 네트워크를 테러리스트들에게 덜 매력적인 표적으로 만들어줌으로써 위협을 감소시킴

출처: U.S. Department of Homeland Security(2009) 재구성

2013년 2월 미국의 대통령 정책지침 PPD-21 “Critical Infrastructure Security and Resilience”가 발표됨에 따라 2009 NIPP도 업데이트되었다. 우선 복원력의 개념은 PPD-21을 따라서 다음과 같이 재정의했다.

“복원력은 변화하는 상황에 대비하고 적응하며 파괴적인 사건들을 견디고 신속하게 복구하는 능력이다. 이것은 의도적인 공격, 사고, 자연적인 위협과 사건들을 견디고 복구하는 능력도 포함”한다(U.S. Department of Homeland Security, 2013: p.7).

2013년 2월 미국 대통령은 행정명령(Executive Order) 13636 “Improving Critical Infrastructure Cybersecurity”를 발표했는데, 주요 내용으로 연방정부는 필수 기반시설 소유자 및 운영자와 조율해서 사이버보안 관련 정보공유를 촉진하고, 사이버보안에 대한 위험 기반의 접근법을 이들과 협력해서 개발하고 실행할 것을 요구했다. 또한 행정명령은 필수 기반시설에 대한 사이버 위험을 줄이기 위해서 기술중립적 사이버보안 프레임워크를 개발하고, 강력한 사이버보안 행동의 채택을 장려하고 이를 위한 인센티브를 제공하며, 사이버 위협 관련 정보공유의 양, 적시성, 품질을 제고하고 프라이버시와 국민 기본권을 필수 기반시설 보안 및 복원력 정책에 포함시킬 것을 요구했다(U.S. Department of Homeland Security, 2013: p.9).

사이버보안 관련 정책에 있어서 2009 NIPP는 비록 사이버보안 관련 대상을 전체 필수 기반시설로부터 분리해냈지만 사이버보안 정책은 전체 보안정책에 통합되어 다루고 있었다. 그러나 행정명령 13636은 사이버보안 프레임워크의 개발을 비롯하여

사이버보안 정보공유 정책들을 언급하는 등 사이버보안 관련 정책이 독자적 영역에 자리 잡고 있다.

2013 NIPP는 국가 기반시설 보호를 위한 국가적인 노력의 진전을 위한 12개의 실천 과제를 제시했는데 그중 사이버보안과 관련된 내용은 다음과 같다. 두 번째 "공동 계획을 통해 집단행동을 결정하라."의 세부 항목으로 분야별 계획(Sector-Specific Plan)에는 현행 그리고 계획 중인 사이버보안 노력을 기술하되, 사이버보안 프레임워크의 활용, 사이버보안 정보공유 정책, 프로그램화된 조치들, 위험 사정, 훈련, 사고 대응 및 복구 노력, 사이버 측정기법 개발 등을 포함할 것을 요구했다(U.S. Department of Homeland Security, 2013: p.22). 열 번째 "연구개발 해법을 발전시켜 필수 기반시설 보안 및 복원력을 증진시켜라."의 세부 내용으로 사이버보안 투자에 대한 인센티브 부여 정책의 촉진을 요구했다(U.S. Department of Homeland Security, 2013: p.25). 또한 이와 같은 분야별 위험 감소를 위한 활동에 필수 기반시설 소유자 및 운영자의 참여를 독려했다.

대통령 행정명령 13636과 이에 대한 후속조치인 2013 NIPP의 발표를 계기로 사이버보안 정책은 기존의 보안정책의 영역에서 어느 정도 분리되어 독자적인 영역을 확보했지만 복원력의 개념은 여전히 보안 개념과 결합되어 논의되고 있으므로 '사이버 복원력'도 사이버보안의 개념 안에서 논의되고 있다. 2013 NIPP의 사이버보안의 개념도 다음과 같이 사이버 복원력의 개념을 포함하는 2009 NIPP에서 제시된 정의를 그대로 사용했다.

"사이버보안(cybersecurity)이란 전자적 정보통신 시스템과 그 안에 포함된 정보의 훼손, 비인가된 사용 또는 남용을 방지하고, 필요시 복구하여, 정보의 기밀성, 무결성 그리고 가용성을 보장하는 것으로서 유무선망, 위성망, 공공안전 응답소, 911 통신 시스템, 제어 시스템 등의 정보 네트워크의 보호 및 필요시 복구를 포함"한다(U.S. Department of Homeland Security, 2009: p.109).

정책 차원에서는 사이버 복원력이 사이버보안에 포함되어 있지만 개별 조직 차원에서 사이버 복원력에 대한 평가는 독립적으로 수행할 수 있게 준비되어 있다. 미국의 국토안보부는 필수 기반설비 운영자들과 각급 지방정부들이 자체적으로 사이버 복원력에 대한 사정을 실시할 수 있는 Cyber Resilience Review(CRR)라는 방법론을 배포했다.

2009년에 처음 도입된 후 2014년에 대폭 개정된 CRR은 42개의 목표와 141개의 구체적 행동으로 구성되어 있는데, 이들은 미국 카네기멜론 대학의 CERT 복원력 관리모형(Resilience Management Model)으로부터 도입되었고 CRR 행동들에 대한 판단 기준은 미국 표준기술연구소(NIST)의 사이버보안 프레임워크(Cybersecurity Framework)로부터 도입되었다.[42)]

결론적으로 미국의 경우 사이버 복원력은 아직 독자적인 국가 정책의 대상이라기보다는 개별 조직 차원의 과제라고 판단된다. 그럼에도 사이버보안 정보공유 정책, 복원력 관련 연구개발 정책 등은 개별 조직 차원을 넘어 국가 차원의 정책 과제라고 할 수 있다.

나. EU

유럽연합 집행부는 유럽연합 의회와 이사회에 "복원력에 대한 유럽연합의 접근법: 식량안보 위기로부터 배우기(The EU Approach to Resilience: Learning from Food Security Crises)"라는 보고서를 제출하면서 복원력 전략은 다양한 정책들, 특히 식량안보, 기후변화 적응 그리고 재난위험 감소 등에 기여해야 한다고 주장했다. European Commission(2012)은 복원력을 다음과 같이 정의했다.

"복원력이란 압박과 충격을 견디고, 적응하고 신속히 회복할 수 있는 개인, 가구, 지역 사회, 국가 또는 지구촌의 한 지역의 능력"이다.

---

42) https://en.wikipedia.org/wiki/Cyber_Resilience_Review (검색일: 2017. 10. 15.)

European Commission (2012)에 의하면 복원력의 개념에는 두 측면이 있다. 하나는 압박과 충격에 더 잘 저항할 수 있는 개인, 가구, 지역사회 또는 더 큰 조직 등 복원력 주체의 타고난 강점이고 다른 측면은 충격으로부터 신속히 회복하는 역량이다. 또한 복원력의 향상은 주체의 강점을 더 강화하거나 충격의 강도를 감소시키거나 또는 두 방법을 동시에 사용하여 달성할 수 있다. 이것은 어떤 위기 속에 존재하는 다중 위험을 감소시키면서, 동시에 지역 사회, 국가 그리고 지구촌의 한 지역 수준에서 대처 및 적응 메커니즘을 향상시킬 것을 요구한다.

식량 위기의 문제에서 시작된 EU의 복원력에 대한 정책적 논의는 여러 분야로 확산되어가면서 사이버보안 정책에서도 복원력에 대한 논의가 시작되었고 2013년 EU의 사이버보안 전략에서 사이버 복원력이 주요 정책과제로 다루어졌다.[43] EU 사이버보안 전략에서 제시한 5대 전략과제 중 첫 번째 과제가 '사이버 복원력의 확보'이다. 특히 EU 전반에 걸친 사이버 복원력을 확보하기 위해서는 정책 당국과 민간 부문의 역량 강화와 상호간 효과적인 협력을 강조했다. 그 주요 내용을 살펴보기로 한다.

모든 회원국이 갖추어야 할 NIS를 위한 공통의 최소 요구사항을 설정하고 이를 충족하도록 요구한다. 또한 국가 차원의 NIS 전략을 수립하고, 국가 차원의 협력 계획을 수립하도록 하며, 2012년에 설립된 CERT-EU가 이를 실무적으로 지원한다.

각 회원국의 NIS 당국간 정보공유와 상호협력이 가능한 조율된 방지·탐지·약화·대응 등의 사이버 복원력 메커니즘을 개발한다. 민간 부문은 기본적으로 스스로 사이버 복원력을 개발하고 최선 행동을 공유하는 등 민간의 자발적인 참여가 절실하지만 민간은 위험관리 문화의 조성과 사이버보안에 대한 투자의 유인이 부족하므로 핵심 산업 분야에서는 위험관리 당국과 정보공유를 의무화한다. 보안 수준의 향상, 정보 공유, 최선 행동 공유를 위해서 민간의 자발적, 비공식적 협력이 중요하다. 또

43) 비록 EU 사이버보안 전략에서 사이버 복원력에 대한 명시적인 정의는 제시되지 않았지만 그 개념은 2016년 영국 정부의 다음과 같은 사이버 복원력 정의와 거의 같을 것으로 본다. "사이버 복원력이란 시스템과 조직이 피해가 초래되는 사이버 사건을 견디고 회복하는 전반적 능력을 의미한다."(HM Government, 2016).

한 NIS 당국은 다른 규제 당국, 법집행 당국 등과 정보를 공유한다. 사이버 복원력을 위한 '유럽 공공·민간 파트너십(European Public-Private Partnership for Resilience: EP3R)은 매우 중요한 플랫폼의 역할을 수행한다. 여기서는 핵심 자산, 자원, 기능, 복원력을 위한 기본 요구사항 등이 발굴되고 협력이 필요한 사항들이 논의되고, 대규모 공격에 대응하는 메커니즘 등이 개발된다.

ENISA에게는 회원국의 사이버 복원력 역량 강화 활동을 지원하고, 산업제어 시스템의 보안을 위한 CSIRT 설립 필요성과 가능성을 타진하며 범유럽 사이버침해훈련을 실시할 것 등을 요구했다. 산업계에는 높은 수준의 사이버보안을 위해 투자하고, 최선 행동을 개발하며 산업계 차원의 정보 공유, 공공당국과의 정보 공유 그리고 EP3R과 TDL(Trust in Digital Life)에 적극 참여할 것을 요청했다.

ENISA는 EU 각 회원국들의 국가 사이버보안 전략의 수립을 지원하기 위해서 EU 내부 및 외부 국가들이 수립한 국가 사이버보안 전략들에서 공통된 요소들과 대책들을 파악하고 이들이 구조나 내용 측면에서 보안과 복원력 증진에 적합한 것들인지를 연구하고 종합해서 ENISA(2012)를 발표했다. 이 보고서는 국가 사이버보안 전략의 개발과 실행을 위한 18개의 정책과제를 제시했는데 (비록 사이버 복원력이라는 용어는 명시적으로 사용되지는 않았으나) 그 중에 일부는 사이버 복원력과 밀접한 관련이 있다.

그 주요 내용을 살펴보면, 우선 사이버보안 전략의 목표를 국가나 사회 전반의 핵심 기능을 지원하는 국가 ICT 자산의 복원력과 보안의 증진으로 삼았다. 다양한 사이버보안을 실시함으로써 서로 다른 분야 간의 협력을 증진하고 상호의존성을 인지하고 서로 협력하는 문화를 조성하고 궁극적으로는 복원력의 향상을 도모한다. 공공-민간의 파트너쉽 형성을 통해서 공통의 목표를 가지고 보안과 복원력의 여러 측면들(저지, 방지, 탐지, 대응, 복구 등)에서 효율적으로 대처한다. 공공-민간 파트너쉽의 효율적인 운영을 위해서는 참여기관 간의 신뢰할 수 있는 정보공유 메커니즘이 수립되어야 한다.

ENISA(2012) 보고서는 EU 회원국들의 국가 사이버보안 전략 수립을 지원하기 위

한 연구의 결과물이지만 그 연구 내용은 2013년 발표된 EU의 사이버보안 전략의 기초가 되었다. 또한 사이버 복원력이 국가 사이버보안 전략의 목표로 인식됨으로써 2013년에 사이버 복원력이 명시적으로 주요 정책과제에 포함된다.

2. 사이버 복원력 시스템

가. 사이버 복원공학 프레임워크

초연결사회는 수많은 사물들이 네트워크에 연결되어 있고 그 중 상당수는 항시적 관리를 받지 못해 사이버 공격에 취약하기 때문에 초연결사회는 사이버 위협으로부터 안전을 보장받을 수 없다. 그럼에도 불구하고 초연결사회의 많은 부분이 수많은 IoT 기반의 자동화 시스템에 의해서 항시적으로 운영되기 때문에[44] 사이버 공격을 받는 도중에도 그 자동화 시스템의 핵심기능은 정상적으로 작동해야 할뿐만 아니라 공격에 의해 훼손된 부분도 복구되어야 한다. 이러한 이유로 초연결사회의 사이버 보안에 있어서 사이버 복원력의 확보가 중요한 과제가 된다.

사이버 복원공학에 대한 Bodeau and Graubart (2011)의 MITRE 보고서가 발표된 이후 관련 업계에서는 단위 조직 차원에서 사이버 복원공학 프레임워크가 제시한 원칙들을 구현하기 위한 알고리즘을 개발하는 데 주력해왔다. 본 연구에서는 설계에 의한 보안과 인공지능 기반의 보안 그리고 사이버 복원력 알고리즘을 결합하여 조직 차원의 사이버 복원력 시스템을 구현하는 방법을 제시하고 단위 조직 차원의 사이버 복원력 시스템을 국가 차원으로 확장하는 방법을 제안하고자 한다.

본 연구는 손상영 외(2016)의 사이버 복원력에 대한 연구의 연장이므로 독자들의 편의를 위해서 앞서 언급한 연구 결과의 일부를 다시 소개하고자 한다.[45] Bodeau and Graubart (2011)에 의하면 사이버 복원력(cyber resilience)이란 기능을 수행해야 할 사이버 자원에 대한 열악한 상황, 압박, 공격에 직면해서 이를 예상하고, 견뎌내

44) 대표적인 사례로 산업제어시스템을 들 수 있다.

45) 자세한 내용은 손상영 외(2016) pp.91~98을 참조하라.

고, 회복하고 역량을 개선하는 방향으로 나아갈 수 있는 국가, 조직, 임무 또는 비즈니스 과정의 능력이다. 여기서 열악한 상황이나 압박이란 사이버 공격은 아니지만 기계적 오류나 자연재해로 인한 정전과 같은 상황을 포함한다. 여기서 사이버 복원력은 사이버 위협에 직면한 주체들의 복원력과 사이버 위협의 대상인 사이버 자원들의 복원력을 모두 지칭한다. 사이버 복원력의 구성요소들은 크게 사이버 복원력의 목적, 그 아래 좀 더 구체화된 목표 그리고 그 목표를 달성하기 위한 행동으로 구분될 수 있다.

〈표 4－11〉 사이버 복원력의 목적

목적	개념
예상하기 (anticipate)	적의 공격으로 임무 또는 비즈니스 기능이 무력화되는 것을 미리 방지하기 위해 정보가 주어진 대비태세를 유지하는 것이다
견디기 (withstand)	성공적인 적의 공격에도 불구하고 핵심적인 임무 또는 비즈니스 기능을 지속하는 것이다
회복하기 (recover)	적의 공격이 성공한 이후 임무/비즈니스의 기능을 가능한 최대한 복구하는 것이다
진화하기 (evolve)	실제적인 또는 예상되는 적의 공격으로부터 피해를 최소화하기 위해서 임무/비즈니스 기능들과 이를 지원하는 사이버 역량을 변화시키는 것이다

출처: Bodeau and Graubart (2011)에서 재구성, 손상영 외(2016) p.92로부터 재인용

〈표 4－12〉 사이버 복원력의 목표

목표	개념
이해하기 (understand)	임무 또는 비즈니스 기능의 사이버 자원에 대한 의존성 그리고 적의 행동과 관련된 사이버 자원의 현 상황 등에 대한 유용한 정보력을 유지하는 것이다
준비하기 (prepare)	예상되는 사이버 공격에 대처할 현실적인 사이버 방책들을 확보하는 것이다
방지하기 (prevent)	사이버 자원에 대한 성공적인 공격을 미리 막는 것이다
지속하기 (continue)	공격을 받으면서도 필수적인 임무/비즈니스 기능들을 최대한 유지하고 활성화하는 것이다

목표	개념
제한하기 (constrain)	적의 공격으로부터 피해를 제한하는 것이다
복원하기 (reconstitute)	적의 성공적인 공격 이후 임무/비즈니스 기능들을 가능한 완전하게 제공하기 위해서 사이버 자원들을 재배치하는 것이다
전환하기 (transform)	과거, 현재 그리고 미래의 적의 공격에 대응해서 조직행동의 양상들을 변화시키는 것이다
재설계하기 (re-architect)	사이버 복원 행동을 더욱 효과적으로 적용하기 위해서 설계를 수정하고 적의 역량, 의도 그리고 공격목표들에 대한 장기적 변화를 다루고 사이버 복원력을 개선하는 새로운 기술들을 수용하는 것이다

출처: Bodeau and Graubart (2011)에서 재구성, 손상영 외(2016) p.93로부터 재인용

〈표 4－13〉 사이버 복원력의 행위

행위	개념
적응적 반응 (adaptive response)	공격의 성격에 의거하여 공격이 진행되고 있다는 징후에 대응하여 조치를 취하는 것이다
분석적 관찰 (analytic monitoring)	잠재적 취약점, 적의 동정 그리고 피해를 찾아내기 위해 상시 체제로 그리고 조율된 방법으로 데이터를 수집하고 분석하는 것이다
조율된 수비 (coordinated defense)	적의 행동에 대항하여 핵심 자원들을 방어하기 위한 다수의 구별되는 기제를 적응적으로 그리고 조율된 방법으로 관리하는 것이다
기만 (deception)	적을 혼동시키기 위해서 혼란과 오도를 사용하는 것이다
다양성 (diversity)	공격 효과를 최소화하고 적들로 하여금 다수의 상이한 기술들을 공격하게 만들기 위해서 이질적인 기술들을 사용하는 것이다
역동적 자리잡기 (dynamic positioning)	핵심 자산들과 센서들을 분산 처리하고 역동적으로 재배치하는 것이다
동태적 표현 (dynamic representation)	구성요소, 시스템, 서비스, 임무 의존성, 적의 동정 그리고 대안적 사이버 방책(cyber courses of action:CCoA)의 효과 등을 동태적으로 보여준다는 것이다
비지속성 (non-persistence)	한정된 시간 동안만 정보, 서비스 그리고 연결성을 유지함으로써 적이 취약점을 활용하고 지속적인 거점을 설치할 기회를 감소시킨다는 것이다

행위	개념
특전 제한 (privilege restriction)	위험 상황과 사용자 신뢰도 각각의 유형과 정도에 따라서 사이버 자원을 사용하기 위해 요구되는 특전과 사용자와 사이버 존재에 할당된 특전을 제한함으로써 적의 행동의 잠재적 결과를 최소화하는 것이다
재정렬 (realignment)	사이버 자원을 임무/비즈니스 기능들의 핵심 측면들과 열을 맞추어 공격당한 표면을 줄이는 것이다
중복 (redundency)	핵심 자원들은 보호되는 여러 벌(instance)을 유지하는 것이다
분할 (segmentation)	구성요소들을 계통 또는 중요도에 따라 논리적 또는 물리적으로 갈라놓음으로써 성공적인 공격의 확산이나 피해를 제한하는 것이다
입증된 무결성 (substantiated integrity)	핵심적인 서비스, 정보 저장장치, 정보 스트림 그리고 구성요소들은 적에 의해 변조되지 않았음을 확인하는 것이다
예측불가능성 (unpredictability)	적의 행동에만 대응하지 않고 수시로, 무작위로 변화를 실행하는 것이다

출처: Bodeau and Graubart (2011)에서 재구성, 손상영 외(2016) p.94로부터 재인용

나. 설계에 의한 보안

설계에 의한 보안(Security by Design)이란 가능한 한 취약성을 제거하여 공격을 받지 않도록 응용 프로그램을 개발하는 것이다. 이를 위해서 시큐어 코딩, 지속적 테스트, 자격증명, 암호화 기법 등이 사용된다(Kreizman and Robertson, 2006).

이 개념이 구체화되는 과정은 다음과 같다. 산업별 보안에 대한 요구사항, 보안 규제사항, 보안 최선행동, 거래당사자간 계약 등이 정형화, 패턴화 과정을 거쳐 OWASP, ISO 등 보안 관련 단체에 전달되고 이러한 보안 관련 단체는 전달 내용의 핵심을 추출하여 설계에 의한 보안 원칙을 수립한다. 보안업체들은 원칙을 구현하는 행동을 개발한다.

설계에 의한 보안의 실행 방법의 한 사례로서 다음과 같은 Hewlett Packard Enterprise의 솔루션을 들 수 있다. 이 솔루션은 시큐어 코딩(secure coding)과 런타임 애플리케이션 자기방어(runtime application self-protection)로 구성된다.

시큐어 코딩은 프로그램 개발단계에서 정적 코드 분석을 실시한다[46]. 보안 약점 리스트로 프로그램의 취약점을 발견하고 개발자와 운영자가 함께 소통하고 협력하면서(DevOps) 취약점을 개선한다. 그럼에도 정적 코드 분석의 정확도는 대부분 80% 이하이며 리콜률도 50% 이하이므로 시큐어 코딩만으로는 설계에 의한 보안을 달성할 수 없다.

런타임 애플리케이션 자기방어는 시큐어 코딩의 한계를 극복하기 위해 도입된다. 이 기술은 응용 프로그램의 런타임 도중에 응용 프로그램의 실행을 통제하고 실시간으로 공격을 탐지하고 방어하는 보안기술로서 이미 성숙단계에 진입해 있다. 런타임이 시작되면 애플리케이션 서버에 자기방어 에이전트가 로드되고, 취약지점이나 중요 실행지점에 보호로직을 삽입한다. 공격자가 해당지점을 공격하면, 자기방어 에이전트는 대신 공격을 저지하고 보안 서버에 보고한다. 이 기술은 애플리케이션 수정 없이 보안 확보가 가능하며, 서비스 중단 없이 런타임에서 작동하므로 사이버 복원력 측면에서 장점이 있다.

런타임 애플리케이션 자기방어가 적이 나타날 만한 길목을 지키는 전술이라면 이를 보완할 수 있는 전술은 전장 전체를 레이더로 감시하면서 이상 징후를 찾아내는 것이라고 할 수 있다. 후자에 해당하는 보안기술로서 '네트워크상에서 이상 징후 탐지'를 들 수 있으며 대표적인 솔루션으로서 보안전문업체인 Darktrace의 Immune system이 있다.

네트워크상에서 이상 징후 탐지는 네트워크 구성요소, 사용자, 디바이스 등의 정상적인 행위에 대한 기계학습을 통해서 정상과 비정상 상태를 실시간으로 식별하고 위협을 감지하여 대응하는 것이다. 인체의 면역기능을 응용한 네트워크 면역체계를 구축하는 데 지도학습(supervised learning)과 비지도학습(unsupervised learning)을 함께 사용하면서 네트워크상의 모든 사용자, 장치 등을 실시간으로 학습하고 상관관

46) 미국은 2002년 제정한 FISMA에서 시큐어 코딩을 의무화했으며, 한국은 2012년 12월부터 공공기관 정보화사업에서 시큐어 코딩을 의무화했다.

계를 분석하면서 스스로 개선해 나간다. 특히 네트워크 내부와 외부의 적을 모두 찾아낼 수 있다는 것이 장점이라고 할 수 있다.

다. 사이버 복원력 시스템의 구현

이제 시스템 차원에서 사이버 복원력의 개념을 구현해보기로 한다. 사이버 복원력은 확고한 사이버보안 및 침입 탐지 역량의 기반 위에 구현되어야 하므로 우리는 사이버 복원력 시스템을 설계에 의한 보안과 네트워크상 이상 징후 탐지 시스템 그리고 사이버 복원력 행위가 학습된 시스템 내부 인공지능으로 구성한다. 이를 위해 사전에 핵심 자산과 자원, 정보시스템이 제공해야 할 필수 기능, 복원력을 위한 기본 요구사항 등 사이버 복원력 행위를 실천하기 전에 미리 결정되어야 할 사항들을 결정한다. 사이버 복원력 행위로는 Bodeau and Graubart (2011)의 14개 행위를 네트워크상에서 이상 징후 탐지 시스템에 내재되어 있는 인공지능을 이용해서 구현한다.

- **사이버 복원력의 행위(practices):** '적응적 반응(adaptive response)', '분석적 관찰(analytic monitoring)', '조율된 수비(coordinated defense)', '기만(deception)', '다양성(diversity)', '역동적 자리잡기(dynamic positioning)', '동태적 표현(dynamic representation)', '비지속성(non-persistence)', '특전 제한(privilege restriction)', '재정렬(realignment)', '중복(redundancy)', '분할(segmentation)', '입증된 무결성(substantiated integrity)', '예측불가능성(unpredictability)'의 14개의 행위로 구성(손상영 외, 2016).

위의 복원력 행위 중 적응적 반응, 분석적 관찰 등 일부는 이미 이상징후 탐지시스템에 구현되어 있을 것으로 판단된다.

라. 국가적 사이버 복원력 기반

EU의 사이버 복원력 확보 전략을 참조로 할 때 국가적 사이버 복원력은 개별 기관들의 확고한 사이버 복원력 시스템과 이들의 협력을 가능하게 하는 정보 공유 및 협력 대응 체계를 통해서 확보될 수 있다. 즉 국가적 사이버 복원력 기반은 기관 단위 사이버 복원력 시스템의 집합과 공공/민간 합동 침해사고 관련 정보 공유 및 협력 대응 체계의 총합이라고 할 수 있다. 공공/민간 합동 침해사고 관련 정보 공유 및

협력 대응 체계는 침해사고를 통지 또는 신고 받은 기관과[47] 취약점 분석기관과[48] 민관합동조사단을[49] 연결하는 폐쇄 네트워크로 구성할 수 있다.

침해사고를 통지 또는 신고 받은 기관은 모든 취약점 분석기관과 민관합동조사단에 신고 받은 침해 관련 정보를 즉시 공유하도록 제도화한다. 네트워크 참여 기관들은 경쟁과 협력을 통해 침해사고의 원인과 대응 방안을 제시하며, 필요시 한국침해사고대응팀협의회 등 전문가 시민단체의 협조도 요청할 수 있다. 초연결사회에서 침해사고의 범위가 확대되고 있으므로 침해사고 신고 의무기관의 범위가 확대될 필요가 있으며, 신고에 대한 인센티브도 마련될 필요가 있다.

위에서 제안된 국가적 사이버 복원력 기반은 침해사고 신고 창구가 단일화되어있는 미국 시스템보다는 각 회원국 CSIRT의 우선권을 인정하고 있는 EU 시스템에 가깝다고 할 수 있다. 이와 같은 전략은 기존의 우리나라 사이버보안 거버넌스의 틀 안에서 정보 공유와 협력 체계에 대한 관계기관 사이의 합의만으로 구현할 수 있기 때문에 실현 가능성이 높다고 할 수 있다. 다만 그 성공 여부는 정보 공유와 협력이 얼마나 신속하고 활발하게 이루질 것인가에 달려 있다.

제 3 절 초연결사회의 정보보안 교육 추진전략

1. 사이버보안 교육체계의 필요성

가. 사이버보안 교육의 필요성

초연결사회는 사물인터넷, 빅데이터 등 관련 기술의 발전으로 연결성, 전역성, 상호연계성, 상호운용성, 상호의존성 등을 가지게 되었으며 이러한 특성의 확대로 사이버보안이 국가·국민의 안보·안전과 직결되는 요소로 부상하게 되었다. 또한 사이

47) 정보통신기반보호법 13조, 정보통신망법 48조, 전자금융거래법 21조에 규정되어 있다.
48) 정보통신기반보호법 9조에 규정되어 있다.
49) 정보통신망법 48조에 규정되어 있다.

버 위험에 대한 개인의 소홀함이 개인을 넘어 사회와 국가 안보 위협으로 확대되는 ‘최소량 법칙(리비히 법칙)’이 적용되어 대다수 국민의 사이버보안 기본 지식의 결핍이 사이버보안 사고를 유발하기 때문에 점점 지능화되고 복합적으로 행해지는 사이버 위험에 대응하기 위해서는 현재의 단순한 기술 위주의 보안대책이 아닌 보편적인 시민들을 대상으로 한 사이버보안 교육이 필요해지고 있다(McGettricket al., 2014; Kirlappos and Sasse, 2012; Irvine, 2011; Dodge and Ragsdale, 2005).

특히 청소년들의 경우 사이버 공간 내 활동이 다양하게 증가하고 있는 반면 아직 윤리 및 보안 관련 가치관이 형성되지 않아 사이버 위험에 직접적 노출될 수 있으며, ‘사이버 불링’ 및 ‘사이버 범죄’ 등의 악의적인 활동에 개입하게 될 우려가 있어 이를 통제하기 위한 교육의 필요성이 더욱 증가된다(Giannakas et al., 2016).

이처럼 사이버 위험에 대응하기 위한 종합적인 보안대책의 일환으로 사이버보안 교육의 필요성이 증가하고 있는 가운데, 사이버보안 교육은 초연결사회의 구성원이 취해야 할 최선의 행동은 무엇인지에 대해 효율적으로 학습할 수 있도록 전체적인 차원에서 구성되어야 하며, 이에 걸맞은 교육과정 및 교육 내용의 개발이 요구된다.

교육과정으로는 자신을 보호할 수 있는 안전한 온라인 이용 방법 및 디지털 시민으로서 필요한 ‘디지털 시민권’에 대해 학습하는 내용이 수반되어야 하며, 이때 디지털 시민권이란 법을 준수하고, 타인의 권리를 존중하는 등 디지털 세계의 시민으로서 현명하고 책임감 있게 행동하는 방법을 배우는 것을 의미한다. 더불어 이러한 교육과정을 직접 실천할 수 있도록 도와주는 차원에서 기술교육을 함께 구성해야 한다.

나. 사이버보안 교육의 정규화 필요성

대다수 국민의 사이버보안 기본 지식의 결핍은 사이버보안 사고를 유발하기 때문에(佐藤謙二, 2016), 전문 인력 외 보편적인 시민들을 대상으로 한 사이버보안 교육의 중요성이 점점 더 증가하고 있다(McGettrick et al., 2014; Kirlappos and Sasse, 2012; Irvine, 2011; Dodge and Ragsdale, 2005). 특히 청소년에게 사이버보안 교육은

초연결사회 내의 사이버 위협에 대응할 수 있을 뿐만 아니라 사이버 공간 내 '디지털 시민'으로서의 권리를 지키고 보호할 수 있는 능력을 향상시킨다(Hunt, 2016; Crompton et al., 2016).

그러나 현재 청소년들이 사이버보안 교육을 받을 수 있는 공간은 거의 없으며, 또한 학교 및 교사의 차원에서도 의무적으로 가르쳐야 하는 교과과정 이외의 주제인 사이버보안을 다루기가 부담스러운 실정이다. 따라서 사이버보안 교육은 초·중등 교육과정에서 정규과목으로 편성되어야 하며, 구체적인 이유는 아래와 같이 크게 세 가지로 정리할 수 있다.

첫째, 사이버보안 교육을 지속적으로 수행하려면 교과목의 정규화가 필요하다. 우리에게 사이버 공간 및 정보기술은 점점 더 삶의 중요한 부분이 되고 있다. 이러한 정보기술의 발전은 모두에게 편의성을 제공하였지만 그것이 부적절하게 사용된다면 의도와 상관없이 큰 위험에 처하게 된다. 이처럼 사이버 공간에서의 행위가 국가·국민의 안보·안전과 직결되는 요소임을 고려한다면, 사이버보안 교육은 마치 길을 건너기 전 양 옆을 살피거나, 차 안에서 안전벨트를 매는 것과 같이 아주 자연스러워질 때까지 시행될 필요가 있다(Pruitt-Mentle, 2008). 무엇보다도 신체적·인지적으로 성장 발달이 왕성하게 이루어지는 초·중등 시기에는 성인에 비해 교육을 통한 행동변화를 유도하기 쉽기 때문에 이 시기에 이루어지는 지속적인 사이버보안 교육은 안전한 온라인 행동과 디지털 시민으로서의 자아를 형성시켜줄 수 있다.

둘째, 사이버보안 교육은 개인부터 사회 및 국가의 안전과 직결되는 요소이기 때문에 국가 차원에서 교육의 큰 틀을 가지고 체계적으로 교육할 필요가 있다. 초·중등 교육과정에서부터 체계적인 사이버보안 교육은 청소년들이 초연결사회의 구성원으로서 취해야 할 올바른 결정을 내리고, 관련 기술을 책임감 있게 사용 할 수 있는 능력을 향상시킨다.

그러나 국내 교육과정 내의 사이버보안 교육은 사이버보안 위협에 대응하고, 전반적인 사이버보안에 대한 기본 지식을 함양하기 위한 니즈와는 상당한 거리가 있으며, 일관된 교육체계 없이 대개 일회성 이벤트 중심으로 이루어지고 있다. 또한

커리큘럼 측면에서 초등학교는 물론이거니와 중·고교 과정에서도 개인정보와 저작권 보호, 저작권 활용, 사이버 윤리 등 피상적인 학습에 치중되어 있고, 하나의 큰 체계에서 유기적으로 시행하는 것이 아니라 단편적으로 시행하는 상황이다. 실제로 공교육 정상화 교육 개혁 과제 일환으로 확정된 '2015 개정 교육과정'을 살펴보면, 대부분의 과정이 학생들의 정보윤리 의식 함양, 소프트웨어 저작권에 대한 이해, 정보기술의 올바른 사용법 등 단기간이고 단발적인 경우에 한정되어 있는 문제를 드러내고 있다.

이를 해결하기 위해서는 일관된 교육 과정에 근거한 교육체계가 필요하며, 이를 효과적으로 구현하기 위해서는 사이버보안이 학교 내 단발적인 활동으로만 수행될 것이 아니라 정규 교과목으로 제공되어야 한다(佐藤謙二, 2016; HM Government, 2014; Bishop, 2010). 이때의 사이버보안 교육은 사이버보안 위협으로부터 하드웨어 및 소프트웨어 보호를 위한 엔지니어링 기반의 기술적 지식보다는 특정 보안 문제를 이해하고 그 파급 효과를 감소시키기 위해 올바른 행동을 취하기 위한 '사이버 리터러시'에 관한 교육을 중심으로 하며, 기술 교육의 경우 기본적인 개념 및 문제를 해결할 수 있는 능력을 향상시킬 수 있는 정도의 기술 교육으로 제공되어야 한다(Kessler and Ramsay, 2014).

셋째, 청소년의 전체적인 사고력 향상을 위해 사이버보안 교육이 필요하다. 초·중등학생의 사이버보안 관련 학습은 컴퓨팅적 사고(Computational Thinking)를 향상시킬 수 있다. 이 개념은 컴퓨터 공학적 사고를 차용하여 문제를 해결하고 시스템 설계나 인간의 행동을 이해하는 역량이라고 정의할 수 있는데(Wing, 2006), 단순한 컴퓨팅의 활용이 아닌 창의적이고 융합적인 차원에서 사고하는 방법, 해결과정을 컴퓨팅 시스템으로 처리될 수 있는 형태로 구조화·알고리즘화하는 논리적인 사고 방법이다. 사이버보안 교육은 관련 학습내용을 위해 논리적 사고력, 분석력, 문제해결력을 활용하여야 하므로 컴퓨팅적 사고를 증진시키는 데 효과적일 수 있다(박남제, 2016).

또한 사이버보안 자체가 명확히 정의된 것이 아니라 IoT 등 기술 발전과 함께 점

차 발전·확장되고 있는 개념이기 때문에, 사이버보안 교육은 기준 및 표준처럼 정해진 내용을 교육하는 대신 사이버 공간 내 행동에 대한 올바른 결정과 책임 있는 기술사용을 위한 사고력 향상 교육으로 제공될 수 있다(Pruitt-Mentle, 2008).

이처럼 사이버보안 교육은 교육적 활용도 측면에서 융합적 사고력 및 고등사고력을 배양할 수 있다는 큰 장점을 지닌다.

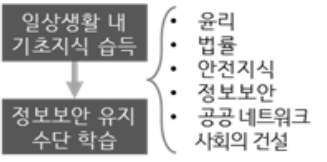
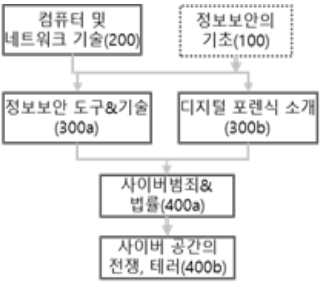
2. 사이버보안 교육체계(안) 구축

가. 사이버보안 교육체계의 기본 방향 설정

초·중등학교에서부터 사이버보안 교육을 체계적으로 수행하기 위해서는 큰 틀의 사이버보안 교육체계 내에서 일관된 교육과정이 수립되어야 하며, 이를 통해 정규 교과목으로 제공될 필요가 있다. 그러나 '사이버보안' 자체가 구체적으로 무엇인지 명확히 정의된 것이 아니라, IoT 등 기술 발전과 함께 점차 발전·확장되고 있는 개념이기 때문에 이를 교육하기 위한 공통적인 체계 또한 존재하지 않는다.

따라서 본 연구에서는 한국형 사이버보안 교육체계의 구축을 위해 사이버보안 교육을 실시하고 있는 주요국(미국, 일본, 호주 등)을 분석하였다. 그리고 그 결과 나라마다 다른 교육 목표 및 교육 체계를 구축하여 운영하고 있음을 인지하였으며, 국내 사이버보안 교육체계의 기본 방향 설정을 위해 가장 두드러지는 특징을 지닌 3가지 교육체계(일본의 사이버보안 교육 커리큘럼, 규슈대학의 사이버보안 교육안, 미국 국토안보부에서 수행하고 있는 사이버보안 인력양성 프로그램)의 주요 구성, 교육 내용 및 특징을 아래의 표와 같이 정리하였다.

〈표 4－14〉 사이버보안 교육 커리큘럼(안)

구분	주요 구성	주요 내용 및 특징
[일본] 사이버보안 교육 기본안		• 정보윤리 중심의 사이버보안 교육 프로그램 • 정보 기반 사회 윤리, 법률의 이행 및 준수 등 보안 의식제고를 목표로 함
[일본] 규슈대학의 사이버보안 교육안		• 사이버보안 역량 및 활용능력의 향상 차원의 교육 • 학년 및 전공에 상관없이 향후 ICT 국제 사회에서 생존하기 위한 사이버보안 능력 및 개인의 사이버 위기에 대처 능력 향상을 목표로 함
[미국] 국토안보부 (DHS) 사이버보안 인력양성안		• 사이버보안과 관련한 기술 기반의 교육과 사이버 공간에서의 국제관계, 테러, 전쟁 등 안보를 중점적으로 다루고 있음

첫째, 일본의 사이버보안 교육 기본안은 일상생활에 필요한 정보보안 관련 지식의 이해 및 습득을 통해 자신을 보호할 수 있는 수단 학습을 목표로 하는 정보윤리 중심의 사이버보안 교육이다. 세부 내용으로는 윤리, 법률, 안전지식, 정보보안 개념의 학습 등이 있으나 교육 자체가 기본적인 지식 습득에서 끝나는 저차원 프로그램이다. 둘째, 규슈대학의 사이버보안 교육안은 학년 및 전공에 상관없이 개인이 사이버 위기에 효과적으로 대응할 수 있는 사이버보안 역량 및 활용 능력을 향상시키고자 한다. 또한 기본적인 정보보안 윤리 및 기본 지식부터, 기술, 법률 및 저작권, 개인정보 보호 등 다양한 관련 분야를 교육하고 있다는 것이 특징이다.

마지막으로 미국 국토안보부(DHS)의 사이버 인력양성 교육은 기술 기반의 교육과 함께 사이버 공간에서의 외교 및 국제관계, 테러, 전쟁 등 안보내용을 중점적으로 다

루고 있으나 전문 인력 양성을 위한 교육 프로그램이라는 점에서 한계가 존재한다.

위와 같은 세 가지의 교육안 모두 각각의 사이버보안 교육 목표를 달성하기 위해 구체적인 체계를 구축하고 이를 교육프로그램에 반영하고 있으나, 사이버보안 전반에 대한 이해를 포괄적으로 다루고 있는 것이 아니라 한정된 영역을 중심으로 교육이 진행되는 한계를 지닌다.

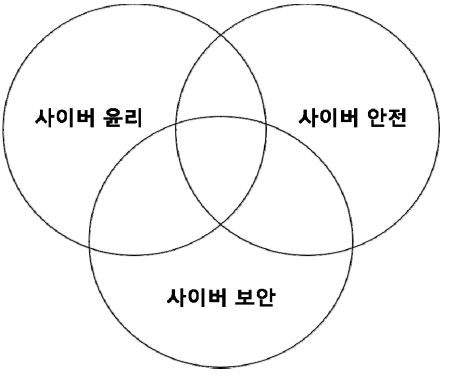
사이버보안에 대한 전반적 이해와 초연결사회에서 발생할 수 있는 사이버보안 위협을 관리·대응하기 위한 능력을 향상시키기 위해서는 사이버 안전, 윤리, 기술적인 교육 등 어느 한쪽 영역에 치우치지 않고 모든 교육을 받을 수 있는 포괄적인 사이버보안 교육체계의 구축이 필요하다. 이를 위해 미국에서는 C3 프레임워크를 개발하여, 초·중·고를 대상으로 한 교육체계로 사용하고 있다. C3 프레임워크는 C3 개념(사이버 윤리, 사이버 안전, 사이버보안)을 모두 아우르는 포괄적인 개념의 교육체계로 본 연구에서는 이를 기반으로 새로운 한국형 사이버보안 교육체계를 구축하고자 한다.

나. 사이버보안 교육체계의 구성

C3 프레임워크를 기반으로 현재의 사이버보안 위협 및 이슈에 대응하면서도 국내 교육환경에 적절한 한국형 사이버보안 교육체계를 구축하기 위해, 기존의 C3(사이버 윤리, 사이버 안전, 사이버보안) 개념과 각 개념의 교육 목표를 다음과 같이 새롭게 정의하였다.

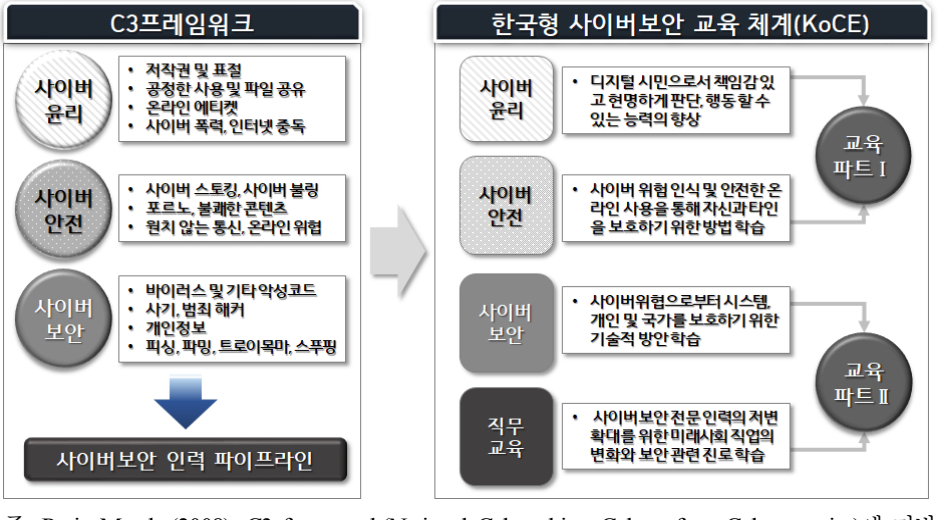
- 사이버 윤리: 법을 준수하고, 다른 사람을 존중하며, 온라인상의 디지털 시민으로서 책임감 있고 현명하게 판단·행동할 수 있는 능력의 향상을 목표로 한다.
- 사이버 안전: 온라인 위험을 인식하고, 정보에 입각한 의사 결정과 기술 시스템·미디어·정보 기술의 안전한 사용을 통해 자신과 타인을 보호하기 위한 적절한 조치방법의 학습을 목표로 한다.
- 사이버보안: 초연결사회에 새롭게 등장하고 있는 사이버 위협으로부터 작게는 시스템 및 네트워크, 크게는 개인 및 국가를 보호하기 위한 기술적 방안의 학습을 목표로 한다.

〔그림 4－3〕 C3 프레임워크 학습영역



또한 기존 C3 프레임워크에 새롭게 정의한 C3 개념을 반영하여 다음과 같이 교육 파트Ⅰ,Ⅱ로 나누어지는 한국형 사이버보안 교육체계(Korea Cybersecurity Education, KoCE)의 큰 틀을 구성하였다.

〔그림 4－4〕 한국형 사이버보안 교육체계의 구성

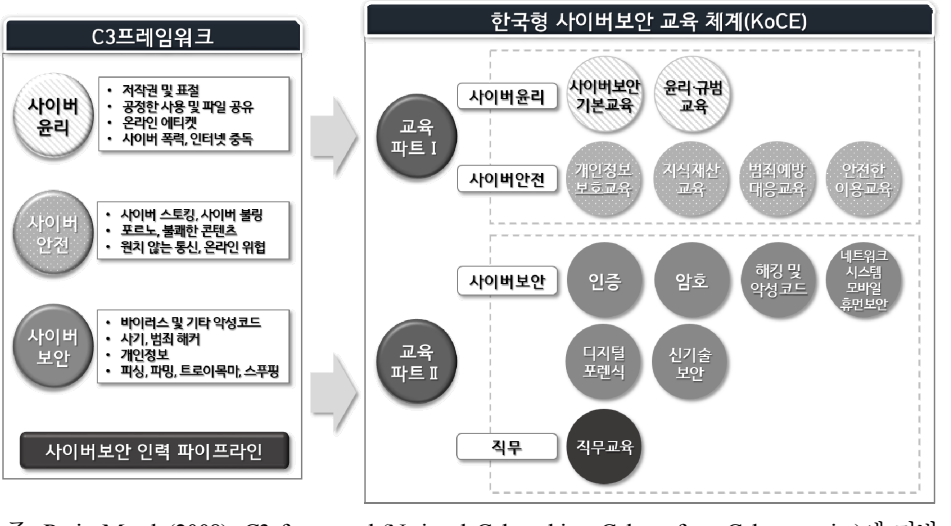


주: Pruitt-Mentle.(2008). C3 framework(National Cyberethics, Cybersafety, Cybersecurity)에 기반하여 새로이 구성함.

- 교육파트 Ⅰ(사이버 윤리+사이버 안전 교육)은 사이버 윤리 및 사이버 안전과 관련한 기본 교육으로 구성되며, 초연결사회의 구성원으로서 사이버 공간 내에서의 정보 관리 및 타인과의 관계 형성 등을 위해 취해야 할 최선의 행동에 대해 학습하는 것을 목표로 한다.
- 교육파트 Ⅱ(사이버보안+직무교육)에서는 사이버 공간 내에서 발생하는 사이버 위협으로부터 시스템, 개인 및 국가를 보호하기 위해 필요한 기술 교육과 미래 사이버보안 전문 인력의 저변 확대를 위한 직무교육을 목표로 한다.

이후 각 사이버보안 교육파트 및 파트 별 학습목표에 알맞은 세부 교과목을 다음 그림과 같이 13개로 설정하였다.

〔그림 4－5〕 한국형 사이버보안 교육체계의 세부 교과목



주: Pruitt-Mentle(2008). C3 framework(National Cyberethics, Cybersafety, Cybersecurity)에 기반하여 새로이 구성함.

- 교육파트 Ⅰ: 초연결사회의 구성원 및 디지털 시민으로서 취해야 할 최선의 행동을 배우기 위한 사이버보안 기본 교육과 윤리·규범 교육, 안전한 사

이버 공간의 이용을 위한 범죄예방 대응교육과 안전한 이용교육, 개인 및 타인의 권리를 보호하기 위한 개인정보보호교육, 지식재산 교육으로 구성한다.

- 교육파트 Ⅱ: 사이버보안 위협에 대응하고, 적절한 보호조치 관련 지식 및 방법을 학습하기 위한 기술 관련 주제를 6가지(인증, 암호, 해킹 및 악성코드, 네트워크·시스템·모바일 휴먼보안, 디지털 포렌식, 신기술 보안)로 구성하고 미래 사이버보안 전문 인력의 저변을 확대하기 위한 직무교육으로 구성한다.

다. 사이버보안 교과목별 세부주제 구성

13개 교과목에 해당하는 주요 학습 목표, 내용을 구성하기 위해 국내외에서 실시하고 있는 사이버보안 교육 및 관련 교육 프로그램의 구성 요소 및 내용을 분석하였다. 분석에 사용된 국내외의 사이버보안 교육 및 관련 교육 프로그램은 다음과 같다.

〈표 4－15〉 국내외 사이버보안 관련 교과

국가	교육 유형	주요 내용
한국	정규교과	- 초·중·고에서 실시하는 교과목 중 정보보호교육과 관련한 교과목 · 초등학교: 사회, 도덕, 실과 교과 · 중학교: 정보 교과 · 고등학교: 정보 및 정보 과학 교과목, 컴퓨터일반(특성화고)
	비교과	- 한국정보화진흥원(NIA)에서 개발하여 제공하고 있는 인터넷 윤리교육 내 교육프로그램 - 사이버인성 교재(중/고등), 스마트 사회의 이해 교재, 인터넷 미디어& 윤리교재, 소셜 미디어 리터러시 교육 프로그램 교재
	대학교육	- KOCW(Korea Open CourseWare) K-MOOC에 게시된 강의 중 정보보호 이론 및 정보보호 개론 수준의 교과목
미국	중등교육	- 사이버보안 교육 체계인 NICE 전략의 일환으로 수행되는 K-12사이버보안 교육
	고등교육	- 국토안보부에서 제공하는 비기술적인 주제 중심의 사이버보안 인력양성 프로그램

국가	교육 유형	주요 내용
	일반교육	- TEEX(Texas Engineering Extension Service)에서 일반 시민을 대상으로 제공하는 보편적인 사이버보안 교육
일본	정규교육	- 일본 문부과학성에서 발표한 초·중·고등학교의 사이버보안 교육 커리큘럼
	대학교육	- 규슈대학의 사이버보안 커리큘럼
호주	정규교육	- eSafety 위원회(Office of the eSafety Commissioner)가 교육부와 협력하여 정규 교육 하에서 이루어지는 원격수업인 eSafety 가상 교실
	기타교육	- 호주 연방 경찰(AFP)에서 제공하는 범죄 예방 프로그램 'ThinkUknow'

위에서 언급한 국내·외의 사이버보안 교육 프로그램 내용을 분석한 결과, 다음과 같이 13개 교과목에 해당하는 주제가 도출되었다.

〈표 4－16〉 국내외 사이버보안 교육의 비교

분류		정규교과			비교과			국내 대학	미국			일본				호주	
		초	중	고	초	중	고		K-12	DHS	TEEX	초	중	고	대	가상 교실	Think U Know
사이버 보안 기본 교육	정보혁명	○	○	○		○	○	○	○								
	4차 산업혁명					○											
	디지털 시민					○	○										
	사이버 공간과 국제관계*									○							
	사이버보안의 이해			○						○			○	○	○		
윤리·규범 교육	사이버 자아정체성					○	○										○
	사이버 공간에서의 커뮤니케이션	○		○		○	○	○	○							○	○
	인터넷 윤리		○	○				○		○	○				○		○
개인 정보	프라이버시 보호							○			○					○	

분류		정규교과			비교과			국내 대학	미국			일본				호주	
		초	중	고	초	중	고		K-12	DHS	THEX	초	중	고	대	가상 교실	Think U Know
보호 교육	개인정보 보호	○	○			○	○	○	○		○		○			○	○
	평판관리					○	○									○	○
지식 재산권 교육	지식재산권의 개념 및 보호대상*										○						
	저작권		○			○	○	○	○						○		
	특허							○									
범죄 예방 대응 교육	사이버 범죄	○		○		○	○	○		○	○				○		○
	사이버 폭력		○			○	○									○	○
안전한 이용	사이버안전의 기본	○					○	○	○		○	○			○		○
	인터넷, 스마트폰 중독	○	○			○		○									
	온라인 상 유해 정보 및 콘텐츠			○		○		○								○	○
인증*	사용자 인증*								○			○					
암호	암호의 역사							○							○		
	대칭키와 공개키 암호							○			○				○		
	암호기술의 역기능							○							○		
해킹 및 악성 코드	해킹의 위협 요인 및 대응	○		○				○							○	○	
	바이러스 및 웜							○				○			○		
	랜섬웨어							○							○		
시스템, 네트워크, 모바일	시스템 보안 위협 및 대응방안*								○	○	○				○		
	네트워크 보안								○	○	○				○		

분류		정규교과			비교과			국내 대학	미국			일본				호주	
		초	중	고	초	중	고		K-12	DHS	THEX	초	중	고	대	가상 교실	Think U Know
휴먼 보안	위협 및 대응방안*																
	모바일 보안 위협 및 대응방법					○	○								○		
	사회공학적 공격*								○								
디지털 포렌식	디지털 포렌식의 개념							○		○	○						
	디지털 포렌식의 목적 및 절차							○		○	○						
	디지털 증거와 수집							○		○	○						
신기술 보안																	
직무 교육	미래사회의 직업과 진로		○														
	직무수행 역량		○														

* 주: *은 사이버보안 교육과 관련하여 주요국(미국, 일본, 호주 등) 교육내용에는 반영되어 있으나 인터넷윤리, 정보보호, 정보리터러시 등 국내 정규 및 비정규 교과내용에는 포함되어 있지 않은 주제임.

이외에도 전문가 자문을 통해 국내·외의 사이버보안 교육에서는 다루고 있지 않으나 최근 관련 이슈 및 교육의 필요성이 증가하는 항목을 새롭게 추가하여 최종적으로 도출하였다.

최종 도출된 교과목에 대한 세부 주제는 다음과 같다.

〈표 4－17〉 사이버보안 교과목 파트별 세부 주제(최종)

교육 파트		세부 주제
사이버보안 기본교육	학습 목표	• 변화하는 환경에 대해 학습하고, 기본적인 사이버보안에 대한 이해를 통해 ‘디지털 시민’으로 거듭나는 것을 목표로 함
	세부 주제	• 정보혁명, 4차 산업혁명, 디지털 시민, 사이버 공간과 국제관계*, 사이버보안의 이해, 정보보호 리터러시**
윤리·규범 교육	학습 목표	• 사이버 공간 내에서 올바른 자아를 확립하고, 원활한 커뮤니케이션을 위한 윤리에 대해 학습함 • 또한 새로운 보안 패러다임으로 초기(설계) 단계에서부터 역기능을 통제하기 위해 보안을 고려한 코드/알고리즘 개념에 대해 학습함
	세부 주제	• 사이버 자아정체성, 사이버 공간에서의 커뮤니케이션, 인터넷 윤리, 코드 윤리와 알고리즘 윤리**
개인정보 보호 교육	학습 목표	• 개인 및 타인의 프라이버시 및 정보를 보호하는 방법에 대해 학습하고, 온라인에서 자신의 평판을 관리하기 위해 개인이 가질 권리인 잊힐 권리, 연결되지 않을 권리에 대해 학습함
	세부 주제	• 프라이버시 보호, 개인정보 보호, 평판관리
지식재산권 교육	학습 목표	• 정보제공자 및 제작자의 인터넷상의 재산권인 지식재산권과 저작권의 개념에 대해 학습하고, 이를 올바르게 사용하는 방법과 정보 제작자 및 이용자의 권리를 보호하기 위한 법·제도 및 라이선스에 대해 학습함
	세부 주제	• 지식재산권의 개념 및 보호대상*, 저작권, 공정이용**, 특허
범죄예방 대응교육	학습 목표	• 사이버범죄의 이해 증진 및 예방·대응에 필요한 지식수준 향상을 목표로 하며, 신고 및 상담 등 도움을 요청하는 방법에 대해서도 학습함
	세부 주제	• 사이버 범죄, 사이버 폭력
안전한 이용	학습 목표	• 컴퓨터와 스마트폰 등을 안전하게 사용하기 위한 방법을 학습하며 사이버 공간 이용의 부작용인 인터넷/스마트폰 중독 및 유해정보로부터 자신을 지키는 방법에 대해 파악함
	세부 주제	• 사이버안전의 기본, 인터넷, 스마트폰 중독, 온라인상 유해정보 및 콘텐츠
인증*	학습 목표	• 계속해서 증가하고 다양화되는 보안 위협에 대응하기 위해 사용자, 장비, 기업 및 단체, 서비스에 대한 보안을 인증하기 위한 방법 및 제도에 대해 학습함
	세부 주제	• 사용자 인증*, 장비 인증**, 인증제도**

교육 파트		세부 주제
암호	학습 목표	• 암호에 대한 기본적인 이론과 실제 활용 분야, 암호기술의 역기능에 대해서 학습함
	세부 주제	• 암호의 역사, 대칭키와 공개키 암호, 암호기술의 역기능
해킹 및 악성코드	학습 목표	• 개인 차원에서 피해를 줄일 수 있도록 해킹과 악성코드에 대한 개념을 명확하게 인지하고 해킹과 악성코드로 인한 침해 사고 등 보안에 대한 문제를 예방하기 위한 방안에 대해 학습함
	세부 주제	• 해킹의 위협 요인 및 대응, 바이러스 및 웜, 랜섬웨어
시스템, 네트워크, 모바일 휴먼보안	학습 목표	• 시스템·네트워크·모바일 측면에서 발생할 수 있는 보안 위협과 대응방안에 대해 학습함
	세부 주제	• 시스템 보안 위협 및 대응방안*, 네트워크 보안 위협 및 대응방안*, 모바일 보안 위협 및 대응방법, 사회공학적 공격*
디지털 포렌식	학습 목표	• 현대 사회의 정보화가 고도화되면서 과학수사 분야에서 디지털 기기를 매개체로 한 디지털 증거 자료를 수집·분석하는 기술이 요구되는 배경을 이해함 • 디지털 포렌식이 무엇인지에 대해 이해하고 기본적인 절차와 방법에 대해 학습함
	세부 주제	• 디지털 포렌식의 개념, 디지털 포렌식의 목적 및 절차, 디지털 증거와 수집, 디지털 포렌식 활용사례**
신기술 보안**	학습 목표	• 4차 산업혁명과 함께 나타나고 있는 새로운 기술과 활용 사례들을 알아보고, 이와 관계된 새로운 보안 위협과 대응방안에 대해 학습함
	세부 주제	• 4차 산업혁명과 ICBM**, 사물인터넷**, 빅데이터**, 클라우드**, 로봇**, 스마트시티**, 지능형 자동차**
직무교육	학습 목표	• 초·중등 교육 과정에서부터 사이버보안과 관련한 직업이 무엇이 있으며, 사이버보안 전문가가 되기 위해서는 어떠한 지식과 능력이 요구되는지에 대해 학습하고자 함
	세부 주제	• 미래사회의 직업과 진로, 직무수행 역량, 전문가 윤리**

주: *은 사이버보안 교육과 관련하여 주요국(미국, 일본, 호주 등) 교육내용에는 반영되어 있으나 인터넷윤리, 정보보호, 정보리터러시 등 국내 정규 및 비정규 교과내용에는 포함되어 있지 않은 주제임.

: **은 국내·외에서 다루고 있지 않은 교육내용이나, 최근 관련 이슈 및 중요성이 증가함에 따라 본 연구에서 새롭게 추가한 내용임.

라. 최종 교육체계 및 세부 교과목 구성

1) 교육파트 I

(1) 사이버보안 기본교육

정보가치의 증대와 4차 산업혁명으로 사이버 공간의 역할과 그 속에서의 국제관계가 중요해지고 있다. 따라서 변화하는 환경에 대해 인식하며, 기본적인 사이버보안 지식에 대한 이해를 통해 '디지털 시민'으로 거듭나기 위한 역량을 키우는 교육이 필요해졌다. 이에 사이버보안 기본 교육에서는 변화하는 환경 및 디지털 시민으로서 가져야 할 권리에는 무엇이 있는지에 대해 학습한다.

〈표 4－18〉 사이버보안 기본교육 교안

수업 주제	정보와 정보혁명, 사이버공간에 대한 이해	
학습 목표	• 변화하는 환경에 대해 학습하고, 기본적인 사이버보안에 대한 이해를 통해 '디지털 시민'으로 거듭나는 것을 목표로 함	
교과 구성	정보혁명	가. 정보사회 일반 - 정보사회의 특징 나. 정보의 의미와 가치 - 정보의 개념 - 정보의 중요성 변화 - 정보의 가치 다. 정보과학기술의 이해 - 정보과학기술의 개념, 특징 - 정보과학기술의 발달과정 - 새로운 기술이 갖는 특징 라. 사이버 공간의 등장 - 사이버 공간의 개념 - 사이버 공간의 성격
	4차 산업혁명	가. 4차 산업혁명 - 1-3차 산업혁명과 4차 산업혁명 간의 차이 - 4차 산업혁명의 특징 - 4차 산업혁명을 통한 변화 나. 4차 산업혁명의 긍정적 효과와 부정적 효과 - 디지털시대 정보소통구조 변화에 따른 명암 - 디지털시대의 헌법적 가치의 보호

수업 주제	정보와 정보혁명, 사이버공간에 대한 이해	
	디지털 시민	가. 디지털 시민과 디지털 시민권 - 디지털 시민 - 디지털 시민의식 - 디지털 시민권 나. 디지털 기회와 정보격차 - 디지털 기회 - 디지털 정보격차 - 디지털 정보격차의 해결
	사이버 공간과 국제관계	가. 사이버공간의 국제적 위치와 세계질서 - 사이버공간의 국제관계 - 국가 간 신뢰를 위한 협정 - 사이버공간에서의 전쟁, 테러
	사이버보안의 이해	가. 사이버보안의 기본 지식 - 사이버보안의 개념 - 사이버보안의 3요소 나. 사이버보안의 필요성 - 사이버보안 영역의 확대
	정보보호 리터러시	가. 정보보호 리터러시의 의의
주요 키워드	정보의 가치, 정보혁명, 4차 산업혁명, 디지털 시민과 디지털 시민권, 디지털 기회와 정보격차, 사이버 공간의 국제관계, 사이버보안, 정보보호 리터러시	

(2) 윤리·규범 교육

오늘날 정보 사회에서는 상상할 수 없을 정도로 많은 양의 정보가 사이버 공간 내에서 빠른 속도로 유통되고 있으며, 익명성·개방성 등 사이버 공간 특성에 따른 새로운 문화가 형성되고 있다. 이러한 사이버 공간의 변화는 새로운 문화의 형성과 함께 수많은 역기능을 가지게 되었으나 모든 역기능에 대해 법·제도화 할 수 없는 사안이 많아지면서 윤리·규범의 역할이 더욱 중요해지고 있다.

따라서 윤리·규범 교육에서는 사이버 공간 내에서 올바른 자아를 확립하고, 타인을 존중할 수 있는 커뮤니케이션에 대해 학습한다. 또한 새로운 보안 패러다임으로 초기(설계) 단계에서부터 역기능을 통제하기 위해 보안을 고려한 코드/알고리즘 개념에 대해 학습한다.

〈표 4－19〉 윤리·규범 교안

수업 주제	사이버 공간 내 윤리·규범에 대한 이해	
학습 목표	• 사이버 공간 내에서 올바른 자아를 확립하고, 원활한 커뮤니케이션을 위한 윤리에 대해 학습하며, 새로운 보안 패러다임으로 초기(설계) 단계에서부터 역기능을 통제하기 위해 보안을 고려한 코드/알고리즘 개념에 대해 학습함	
교과 구성	사이버 자아정체성	가. 사이버공간에서의 자아정체성 - 사이버공간의 특성과 자아정체성 - 사이버 자아의 불완전성 나. 사이버공간과 현실의 차이 - 사이버 공간이 내 삶에 미치는 영향 - 사이버 공간 속의 나와 현실 속의 나를 비교해보기
	사이버공간에서의 커뮤니케이션	가. 사이버공간소통의 특징 - 사이버 공간의 특성으로 인한 소통 방식의 변화 - 사이버 공간 특성에 따른 새로운 문화 형성 나. 사이버 공간에서 나와 상대를 존중하기 - 네티켓 - 모바일 에티켓 - SNS 에티켓
	인터넷 윤리	가. 인터넷 윤리의 이해 - 인터넷 윤리의 개념 - 인터넷 윤리의 필요성 나. 인터넷 윤리와 관련된 법률/제도 - 정보통신망법, 전기통신기본법, 위치정보의 보호 및 이용 등에 관한 법률, 게임 산업 진흥에 관한 법률, 통신 비밀 보호법, 유해정보 심의제도 등
	코드 윤리와 알고리즘 윤리*	가. 코드/알고리즘 윤리의 이해 - 코드/알고리즘 윤리의 등장 - 코드/알고리즘 윤리의 필요성 나. 코드/알고리즘 윤리의 적용
주요 키워드	인터넷 윤리, 사이버 공간의 문화, 네티켓, 소셜미디어, 사이버 공간과 자아정체성, 코드/알고리즘 윤리	

주: *은 사이버보안 교육과 관련하여 주요국(미국, 일본, 호주 등) 교육내용에는 반영되어 있으나 인터넷윤리, 정보보호, 정보리터러시 등 국내 정규 및 비정규 교과내용에는 포함되어 있지 않은 주제임.

(3) 개인정보 보호 교육

정보화 시대의 도래와 함께 개인의 참여가 증가함에 따라 행위의 주체로서 개인의 영향력이 강화되었다. 이러한 맥락에서 개인정보에 대한 가치와 중요성이 크게 증가하였고, 개인정보를 보호하기 위하여 다각적인 차원의 노력이 필요해졌다. 따라서 개인정보 보호교육에서는 개인 및 타인의 프라이버시 및 정보를 보호하는 방법에 대해 학습하고, 온라인에서 자신의 평판을 관리하기 위해 개인이 가질 수 있는 권리인 잊힐 권리, 연결되지 않을 권리에 대해 학습한다.

〈표 4－20〉 개인정보 보호 교안

<table>
<tr><td>수업 주제</td><td colspan="2">개인정보 보호 및 프라이버시 보호</td></tr>
<tr><td>학습 목표</td><td colspan="2">• 개인 및 타인의 프라이버시 및 정보를 보호하는 방법에 대해 학습하고, 온라인에서 자신의 평판을 관리하기 위해 개인이 가질 수 있는 권리인 잊힐 권리, 연결되지 않을 권리에 대해 학습함</td></tr>
<tr><td rowspan="3">교과 구성</td><td>프라이버시 보호</td><td>가. 프라이버시권에 대한 이해
- 프라이버시권의 개념
- 고전적 의미의 프라이버시
- 현대적 의미의 프라이버시
- 우리나라 헌법상 프라이버시권의 인정
나. 프라이버시를 보호하기 위하여 고려해야 할 사항
- 프라이버시의 법적 권리: 개인정보자기결정권
- 사이버 공간에서 발생 가능한 프라이버시 이슈</td></tr>
<tr><td>개인정보보호</td><td>가. 개인정보의 의미
- 개인정보의 개념과 특징
- 개인정보 중요성의 증가
나. 개인정보를 보호해야 하는 이유
- 개인정보 유출 방법의 증가, 다양화
- 개인정보 유출 시 발생할 수 있는 문제에 대한 이해
다. 개인정보를 보호하는 방법
- 개인적 차원의 방안
- 국가/제도적 차원의 방안</td></tr>
<tr><td>평판관리*</td><td>가. 온라인 평판 관리의 의미</td></tr>
</table>

수업 주제	개인정보 보호 및 프라이버시 보호	
		- 사이버 특성에 따른 개인 기록의 형성 - 소셜 미디어 등을 통한 평판의 형성 나. 잊힐 권리 - 잊힐 권리의 의미 - 잊힐 권리의 인정 - 잊힐 권리의 명과 암 다. 연결되지 않을 권리 - 연결되지 않을 권리의 의미 - 연결되지 않을 권리와 관련한 논의 및 법제화 라. 통신비밀의 보호 - 통신비밀의 보호 - 통신비밀보호법의 제정
주요 키워드	프라이버시, 개인정보보호, 개인정보 보호원칙, 온라인 평판 관리, 잊힐 권리, 연결되지 않을 권리, 통신비밀의 보호	

주: *은 사이버보안 교육과 관련하여 주요국(미국, 일본, 호주 등) 교육내용에는 반영되어 있으나 인터넷윤리, 정보보호, 정보리터러시 등 국내 정규 및 비정규 교과내용에는 포함되어 있지 않은 주제임.

(4) 지식재산권 교육

IT 기술이 발전함에 따라 정보화 사회가 도래하였으며, 넘쳐나는 정보들로 인하여 사람들은 원하는 자료를 검색하여 활용하고 있다. 이렇게 활용되는 자료들은 모두 누군가의 손에 의해서 생성된 정보로 하나의 재산으로 인정받고 있으나 자료를 손쉽게 얻을 수 있다 보니 정보의 제공자 및 제작자와 재산권적 권리를 고려하지 않고 무분별하게 사용되는 일이 빈번하다.

사이버보안은 정보의 올바른 활용 및 보호에서 출발함에 따라 정보제공자 및 제작자의 인터넷상 재산권인 지식재산권과 저작권의 개념에 대해 학습하고, 이를 올바르게 사용하는 방법과 보호하기 위한 법·제도 및 라이선스에 대해 학습한다. 또한 지나친 디지털 저작권 보호 기술이 소비자 권리를 침해할 수 있음을 인식하고, 이를 해결하기 위해 등장한 공정사용 개념 및 제도에 대해 학습한다.

〈표 4－21〉 지식재산권 교안

수업 주제	인터넷상 정보의 소유권에 대한 이해	
학습 목표	• 정보제공자 및 제작자의 인터넷상의 재산권인 지식재산권과 저작권의 개념에 대해 학습하고, 이를 올바르게 사용하는 방법과 정보 제작자 및 이용자의 권리를 보호하기 위한 법·제도 및 라이선스에 대해 학습함	
교과 구성	지식재산권의 개념 및 보호대상	가. 지식재산권의 이해 - 지식재산권의 개념 및 보호목적 - 기존의 지식재산권과 사이버공간상의 지식재산권의 차이 - 사이버 지식재산권의 필요성 증가 나. 지식재산권의 보호대상 및 범위 - 지식재산권 범위의 확장 - 새로운 지식재산권의 등장 다. 지식재산권의 보호방법 - 법률에 의한 보호
	저작권	가. 저작물 - 저작권법의 보호대상 - 저작물의 종류 - 공동저작물 - 보호받지 못하는 저작물 나. 저작권의 발생과 보호기간 다. 저작권의 종류 - 저작인격권의 종류 - 저작재산권의 종류 라. 저작권의 제한 - 권리제한의 의의 - 저작재산권 제한 - 법정허락에 의한 제한 마. 저작권 침해 유형 바. 저작권의 보호를 위한 방법 - 개인 차원 - 법·제도적 차원 - 기술적 차원
	공정이용	가. 공정이용과 소비자의 권리 - 공정이용의 개념

수업 주제	인터넷상 정보의 소유권에 대한 이해	
		- 공정이용의 필요성 - 공정이용의 예 나. CCL - CCL의 개념 - CCL의 종류 다. 오픈소스 SW - 오픈소스 SW의 정의 - 오픈소스 SW 라이선스 - 오픈소스 SW 라이선스의 종류
	특허	가. 특허의 이해 - 특허의 개념 - 특허의 요건 - 특허의 효력 나. 특허 심사절차 다. 국제특허출원 - 해외출원의 필요성 - 해외출원 방법
주요 키워드	지식재산권의 개념, 지식재산권 관련 법률, 보호방법, 저작권, 저작권 침해 유형, 저작권 보호방안, 공정이용, CCL, 오픈소스 SW, 특허	

(5) 범죄 예방·대응 교육

일상생활과 경제활동에서 인터넷 없는 세상을 생각하기 힘들지만 인터넷은 범죄자에게도 익명성을 유지한 채 범죄를 저지를 수 있는 기회를 제공한다. 범죄는 법으로 엄격하게 금지하는 행위이고 처벌 대상이므로 자칫 사소한 실수로라도 범죄를 저지르게 되거나 범죄피해를 당하지 않도록 조심할 필요가 있다.

이에 범죄 예방·대응 교육은 사이버범죄에 대한 인식을 통해 피해 예방·대응에 필요한 지식수준 향상을 목표로 하며, 신고 및 상담 등 도움을 요청하는 방법에 대해서도 학습한다.

〈표 4－22〉 범죄 예방·대응 교안

수업 주제	사이버 범죄 예방과 대응	
학습 목표	• 사이버범죄의 이해 증진 및 예방·대응에 필요한 지식수준 향상을 목표로 하며, 신고 및 상담 등 도움을 요청하는 방법에 대해서도 학습함	
교과 구성	사이버 범죄	가. 사이버범죄의 개념과 특징 - 사이버범죄의 개념 - 사이버범죄의 특징 나. 사이버범죄의 유형 및 대응방안 - 사이버범죄의 유형 - 사이버범죄의 예방 및 대응방안 - 범죄 피해를 당했을 경우
	사이버 폭력	가. 사이버폭력의 개념과 특징 - 사이버폭력의 개념 - 기존 학교폭력과 사이버폭력의 차이 나. 사이버폭력의 유형 다. 사이버폭력의 대응방안 - 가해자가 되지 않기 - 피해를 당했을 경우
주요 키워드	사이버범죄, 사이버범죄의 특징 및 유형, 사이버범죄의 예방 및 대응방안, 범죄 피해 신고 및 상담, 사이버폭력, 사이버폭력의 유형 및 대응방안	

(6) 안전한 이용 교육

현실공간과 사이버공간의 경계가 허물어짐에 따라 일상에서도 인터넷에 접속하기 위하여 다양한 도구가 활용되고 있다. 그러나 다양한 도구의 활용은 중독 및 과의존을 불러일으킬 수 있으며, 유해 콘텐츠의 접근이 쉬워지는 등 많은 부작용을 초래하기도 한다.

따라서 안전한 이용 교육에서는 가장 많이 사용하는 컴퓨터와 스마트폰, 그리고 그 속에서 구동되는 웹과 전자메일 등을 안전하게 사용하기 위한 방법에 대한 지식 향상을 목표로 하며, 사이버 공간 이용의 부작용인 인터넷/스마트폰 중독 및 유해정보로부터 자신을 지키는 방법에 대해 학습한다.

〈표 4－23〉 안전한 이용 교안

수업 주제	사이버 공간의 안전한 이용	
학습 목표	• 컴퓨터와 스마트폰 등을 안전하게 사용하기 위한 방법을 학습하며 사이버 공간 이용의 부작용인 인터넷/스마트폰 중독 및 유해정보로부터 자신을 지키는 방법에 대해 파악함	
교과 구성	사이버안전의 기본	가. PC의 안전한 사용 - 계정 관리 - 패스워드 관리 - 윈도우 업데이트 수행 - 백신 프로그램 설치 - 백업/복원 관리 나. 인터넷 안전한 사용 - 전자메일 보안 - 브라우저 보안 - 무선네트워크 보안 다. 스마트폰의 안전한 사용 - 분실/도난 대책 - 패스워드 설정 - 백업/복원 관리 - 안전한 애플리케이션 사용
	인터넷, 스마트폰 중독	가. 인터넷, 스마트폰 중독의 이해 - 신개념 중독과 인터넷 과의존의 개념 및 현황 - 신개념 중독의 종류 나. 중독의 증상 및 진단 - 인터넷/스마트폰 중독 증상 - 인터넷/스마트폰 중독의 진단 방법 다. 중독의 예방 및 치료방법 - 스마트폰·인터넷 이용 조절력과 자기통제력 기르기 - 건강한 스마트폰 사용 실천약속 - 일상생활에서의 적절한 스마트폰 사용방법
	온라인상 유해정보 및 콘텐츠	가. 유해정보의 개념 및 종류, 식별방법 - 불법 유해정보와 청소년 유해정보 나. 유해정보의 종류와 실태 - 유해정보의 종류 - 관련 이슈 다. 유해정보 대응 방안 - 인터넷 내용 등급서비스 - 부적절한 콘텐츠 신고방법
주요 키워드	PC, 네트워크, 스마트폰의 안전한 사용, 인터넷 중독, 스마트폰 과의존, 불법 유해정보와 청소년 유해정보	

2) 교육파트 Ⅱ

(1) 인증

계속해서 증가하고 다양화되는 보안 위협에 대응하기 위해 사용자, 장비, 기업 및 단체, 서비스에 대한 보안을 인증하기 위한 다양한 방법이 등장하고 있다. 특히 사용자 인증에는 지문인식 기술 및 홍채인식 기술을 활용한 금융 서비스 등 스스로를 증명, 인증하는 수단이 빠르게 변화하고 있다.

따라서 인증 교육에서는 사용자를 인증하는 방법에는 무엇이 있으며, 최근 새롭게 떠오르고 있는 이슈에는 무엇이 있는지 학습한다. 또한 사용자 외에도 장비, 기업 및 단체, 서비스의 보안을 인증하는 방법과 관련한 제도는 무엇이 있는지 학습한다.

〈표 4－24〉 인증 교안

수업주제	인증에 대한 이해	
학습 목표	• 계속해서 증가하고 다양화되는 보안 위협에 대응하기 위해 사용자, 장비, 기업 및 단체, 서비스에 대한 보안을 인증하기 위한 방법 및 제도에 대해 학습함	
교과 구성	사용자 인증	가. 사용자 인증의 개념 - 사용자 인증이란 - 사용자 인증을 위한 요건 나. 사용자 인증 방법 - 지식기반 인증 - 소유기반 인증 - 생체기반 인증 다. 새로운 인증 방식의 등장 - Usable Security 인증 - 행위기반 인증 - FIDO
	장비 인증	가. CC 인증 - 국제 CC 인증 평가요소 - 국내 CC 인증

수업주제	인증에 대한 이해	
	인증제도	가. ISMS 정보보호 관리체계 - 개요 - ISMS의 목적 및 기대효과 - 인증대상 - 인증요소 및 범위 나. PIMS 개인정보보호 관리체계 - 개요 - PIMS의 목적 및 기대효과 - 인증요소 및 범위 다. 클라우드 서비스 보안인증제도 - 개요 - 클라우드 인증의 목적 및 기대효과 - 인증요소 및 범위
주요 키워드	사용자 인증, 인증의 종류, Usable Security, 행위기반 인증, FIDO, CC 인증, ISMS, PIMS, 클라우드 서비스 보안인증제도	

(2) 암호

우리가 평소에 사용하는 메신저는 암호화를 통해 친구나 가족들과 주고받는 메시지를 남들이 볼 수 없게 보호되고 있다. 이외에도 암호는 인터넷뱅킹에서 사용하는 인증서, 전자투표 등에서 사용되고 있다.

따라서 암호 교육에서는 정보의 보호를 위해, 우리의 실생활에서 가깝고 필수적으로 사용되고 있는 암호에는 무엇이 있는지 학습하고, 이에 대한 기본적인 이론과 실제 활용 분야, 암호기술의 역기능에 대해서 학습한다.

〈표 4－25〉 암호 교안

수업 주제	암호의 개념과 원리 및 암호기술	
학습 목표	• 암호에 대한 기본적인 이론과 실제 활용 분야, 암호기술의 역기능에 대해서 학습함	
교과 구성	암호의 역사	가. 암호의 발달과정 - 최초의 암호

수업 주제	암호의 개념과 원리 및 암호기술	
		- 고대 암호 - 근대 암호 - 현대 암호 나. 현대의 암호이론 - 암호의 기본 원리 - 현대 암호의 원리와 안전성
	대칭키와 공개키 암호	가. 대칭키와 공개키의 원리 및 특징 - 대칭키 암호 - 공개키 암호 나. 암호의 종류 및 활용 사례 - 대칭키 암호의 종류 - 공개키 암호의 종류
	암호기술의 역기능	가. 암호기술의 악용 사례
주요 키워드	암호의 역사, 고대 암호, 근대 암호, 현대 암호, 현대 암호의 원리와 안전성, 대칭키 암호, 공개키 암호, 암호기술의 역기능	

(3) 해킹 및 악성코드

일상의 많은 부분이 사이버 세상과 공유됨에 따라 사이버 공간 내 범죄 또한 크게 증가하고 있다. 따라서 해킹 및 악성코드 교육에서는 개인 차원에서 피해를 줄일 수 있도록 해킹과 악성코드에 대한 개념을 명확하게 인지하고 해킹과 악성코드로 인한 침해 사고 등 보안에 대한 문제를 예방하기 위한 방안에 대해 학습한다.

〈표 4－26〉 해킹 및 악성코드 교안

수업 주제	해킹 및 악성코드의 개념과 대응방안	
학습 목표	• 개인 차원에서 피해를 줄일 수 있도록 해킹과 악성코드에 대한 개념을 명확하게 인지하고 해킹과 악성코드로 인한 침해 사고 등 보안에 대한 문제를 예방하기 위한 방안에 대해 학습함	
교과 구성	해킹의 위협 요인 및 대응	가. 해킹의 개념 및 역사 - 해킹의 개념 - 해킹의 역사 나. 해킹의 유형

수업 주제	해킹 및 악성코드의 개념과 대응방안	
		- 해킹의 유형 - 해킹을 유발하는 행위 다. 해킹의 증상 및 대응방법 - 온라인 계정 - 단말기 - 데이터
	바이러스 및 웜	가. 바이러스와 웜에 대한 이해 - 악성 프로그램의 개념 - 바이러스의 개념 나. 바이러스와 웜의 증상 및 예방법 - 바이러스의 증상 및 예방법 - 웜의 증상 및 예방법
	랜섬웨어	가. 랜섬웨어의 개념 및 특징 - 랜섬웨어의 개념 - 랜섬웨어의 특징 나. 랜섬웨어 감염경로의 이해 다. 램섬웨어의 대응방법 - 5대 예방수칙 - 랜섬웨어 복구
주요 키워드	해킹의 역사, 해킹의 개념, 해킹의 유형, 악성 프로그램, 바이러스, 웜, 랜섬웨어	

(4) 시스템, 네트워크, 모바일 휴먼보안

인터넷을 통한 네트워크의 연결로, 컴퓨터 및 모바일 사이에 주고받는 데이터의 양이 증가함에 따라 네트워크의 보안 문제 발생 시 컴퓨터 시스템이나 모바일의 보안 문제와 맞물려 하나의 시스템을 넘어서 국가의 시스템까지도 장애가 발생할 수 있다. 따라서 시스템·네트워크·모바일 측면에서 발생할 수 있는 보안 위협과 대응방안에 대해 학습한다.

〈표 4－27〉 시스템, 네트워크, 모바일 휴먼보안 교안

수업 주제	시스템·네트워크·모바일에 대한 이해
학습 목표	• 시스템·네트워크·모바일 측면에서 발생할 수 있는 보안 위협과 대응방안에 대해 학습함

수업 주제	시스템·네트워크·모바일에 대한 이해	
교과 구성	시스템 보안 위협 및 대응방안	가. 시스템의 이해 - 컴퓨팅 시스템의 발전 - 인간과 컴퓨팅 장치의 상호작용 나. 시스템 환경에서 발생할 수 있는 위협 - 시스템 환경에 대한 위협의 유형 - 시스템 환경에 대한 위협요소의 특성 다. 시스템 위협의 예방 및 대응방법
	네트워크 보안 위협 및 대응방안	가. 네트워크의 이해 - 네트워크의 구조 - 네트워크의 종류 - 네트워크 프로토콜 나. 네트워크 환경에서 발생할 수 있는 위협 - 네트워크상의 데이터로 인한 위협 - 발생 가능한 공격 유형 다. 네트워크에 대한 위협의 예방 및 대응방법 - 네트워크에 대한 지속적인 모니터링 - 무선 네트워크보안/방화벽
	모바일 보안 위협 및 대응방법	가. 모바일의 이해 - 모바일 개념 - 모바일의 영향력 및 보안 필요성 - 보안관점에서의 안드로이드 및 iOS의 차이 나. 모바일 환경에서 발생할 수 있는 위협 - 사용자/단말 - 네트워크 - 응용서비스 - 모바일 콘텐츠 다. 모바일 위협의 예방 및 대응방법
	사회공학적 공격	가. 사회공학적 공격의 이해 - 사회공학적 공격 - 사회공학적 공격의 방식 나. 사회공학적 공격의 영향력 - 기존 사이버공격과의 차이 다. 사회공학적 공격의 대응방법 - 공격의 탐지 방법 - 예방 방법 - 공격 시 대응 방법
주요 키워드	시스템 보안, 네트워크 보안, 모바일 보안, 사회공학적 공격	

(5) 디지털 포렌식

최근에는 경찰이 압수한 범죄자의 스마트폰에서 통화내역이나 문자메시지 등을 복구하여 증거로 삼았다는 내용의 뉴스를 종종 접하곤 한다.[50] 이처럼 현대 사회의 정보화가 고도화되면서 과학수사 분야에서 디지털 기기를 매개체로 한 디지털 증거 자료를 수집·분석하는 기술이 요구되고 있다. 이러한 배경을 이해하면서, 디지털 포렌식이 무엇인지에 대해 이해하고 기본적인 절차와 방법에 대해 학습한다.

〈표 4－28〉 디지털 포렌식 교안

수업 주제	디지털 포렌식의 개념 및 절차	
학습 목표	• 현대 사회의 정보화가 고도화되면서 과학수사 분야에서 디지털 기기를 매개체로 한 디지털 증거 자료를 수집·분석하는 기술이 요구되는 배경을 이해함 • 디지털 포렌식이 무엇인지 이해하고 기본적인 절차와 방법에 대해 학습함	
교과 구성	디지털 포렌식의 개념	가. 디지털 포렌식의 역사 - 법·과학을 이용한 최초의 수사기록 - 과학수사의 발전 나. 디지털 포렌식의 필요성 다. 디지털 포렌식의 활용 분야 - 디지털 포렌식 적용 분야 - 주요 활용사례 라. 안티 포렌식 - 등장배경 및 개념 - 주요 활용 사례
	디지털 포렌식의 목적 및 절차	가. 디지털 포렌식의 목적과 원칙 - 디지털 포렌식의 목적 - 디지털 포렌식의 원칙 나. 디지털 포렌식의 진행 절차
	디지털 증거와 수집	가. ‘디지털 증거’란? - 디지털 증거의 개념 - 디지털 증거의 특징 나. 디지털 증거의 수집과 보관 - 디지털 증거의 수집절차

50) https://blog.naver.com/with_msip/220996692452 (검색일: 2017. 7. 10.)

수업 주제	디지털 포렌식의 개념 및 절차	
		- 디지털 증거 보관 시 유의사항
주요 키워드	과학수사, 디지털 포렌식, 안티 포렌식, 디지털 포렌식의 진행 절차, 디지털 증거, 디지털 증거의 수집과 보관	

(6) 신기술 보안

제4차 산업혁명이 이루어지고 지능정보기술이 적용됨에 따라 사람과 기계가 함께 일하고, 고부가가치를 창출하는 새로운 일자리가 생기며, 단순 반복 업무 등의 직업들이 점차 사라지고 있다. 이로 인해 삶의 질 향상, 이전과는 다른 새로운 형태의 일자리 창출, 노동생산성의 향상 등 긍정적 측면에서의 효과도 예상되지만, 그 이면에는 간과해서는 안 될 요소들이 존재하는데 사이버보안 위협이 대표적이다(장우식, 2017. 5. 10.). 디지털 혁명의 고도화는 해킹공격으로 인한 사고 발생 시 위협을 넘어 우리에게 상상할 수 없는 큰 피해를 줄 수 있다.

따라서 신기술 보안 교육에서는 4차 산업혁명과 함께 나타나고 있는 새로운 기술과 활용 사례들을 알아보고, 이와 관계된 새로운 보안 위협과 대응방안에 대해 학습한다.

〈표 4－29〉 신기술 보안 교안

수업 주제	신기술 보안 이해	
학습 목표	• 4차 산업혁명과 함께 나타나고 있는 새로운 기술과 활용 사례들을 알아보고, 이와 관계된 새로운 보안 위협과 대응방안에 대해 학습함	
교과 구성	4차 산업 혁명과 ICBM	가. ICBM 개념 및 특징
	사물인터넷	가. 개요 - 등장 배경 및 개념 - 적용 사례 및 기대효과 나. 새로운 보안 위협 및 대응방안 - 기존 보안위협의 업그레이드 및 새로운 보안 위협의 등장 - 보안 위협의 대응방안
	빅데이터	
	클라우드	
	로봇	
	스마트시티	
	지능형 자동차	
주요 키워드	4차 산업혁명, ICBM, 사물인터넷, 빅데이터, 클라우드, 로봇, 스마트시티, 지능형 자동차, 신기술 보안	

(7) 직무교육

직업 세계는 기술발전과 사회변화, 경제활동의 변화 등에 의해 영향을 받기 때문에 그 변화는 직업을 가지고 살아가는 성인은 물론 준비하고 있는 학생들과 청년들에게도 매우 중요하다.

특히 4차 산업혁명 시대의 도래와 함께 개인과 기업, 국가의 정보가 해킹당할 위험도 높아지면서 사이버보안전문가의 역할이 무척 중요해지고 있다. 따라서 초·중등 교육 과정에서부터 사이버보안과 관련한 직업이 무엇이 있으며, 사이버보안 전문가가 되기 위해서는 어떠한 지식과 능력이 요구되는지에 대해 학습한다.

〈표 4－30〉 사이버보안 직무교육 교안

수업 주제	사이버보안 직무교육	
학습 목표	• 초·중등 교육 과정에서부터 사이버보안과 관련한 직업이 무엇이 있으며, 사이버보안 전문가가 되기 위해서는 어떠한 지식과 능력이 필요한지에 대해 학습하고자 함	
교과 구성	미래사회의 직업과 진로	가. 직업의 변화 - 직업 환경의 변화 요인 - 사이버/정보기술로 인한 직업의 변화 나. 사이버보안 관련 직업 [참고자료] 사이버군·경찰
	직무수행 역량	가. 국가직무능력표준(NCS) 나. 정보보호 관련 자격증
	전문가 윤리	가. 전문가 윤리의 필요성
주요 키워드	직업의 변화, 사이버보안 관련 직업, 전문가 윤리, 정보보호 관련 자격증, 국가직무능력 표준(NCS), 사이버군·경찰	

3. 사이버보안 교육의 정규교육화 방안

2018년부터 중학교 교과 과정에서 소프트웨어 교육이 의무화된다. 이에 대해서 학생들의 학습 부담 문제, 강사 확보의 문제 등이 제기되고 있기 때문에 사이버보안 교육의 경우도 동일한 문제가 발생할 것으로 예상된다. 따라서 가까운 시점에 별도의

사이버보안 교과 과정을 정규 교과목으로 도입하기는 매우 어렵다고 본다.

한 가지 다행스러운 점은 소프트웨어 교육과 사이버보안 교육은 이론적인 측면에서 공통분모가 많다는 것이다. 따라서 사이버보안 교육 체계 중에서 기술적인 분야는 소프트웨어 교육의 한 응용 분야로 다루면 된다. 사이버 윤리와 사이버 안전 분야는 기존의 초중등 교육과정에 있는 정보윤리 및 정보화 역기능에 대한 교육 내용을 사이버보안 교육 체계의 수준으로 강화하면 굳이 새로운 과목이나 교과 과정을 개설할 필요는 없다. 중등학교 수준의 사이버보안 기술교육을 위한 강사 인력은 소프트웨어 강사 인력을 활용하면 된다. 즉 소프트웨어 강사 인력에게 사이버보안 기술 관련 약간의 추가적인 연수 기회를 제공하면 사이버보안 강사를 겸할 수 있을 것이다.

하지만 아직 소프트웨어 강사 인력도 확보되지 않은 것이 현실이다. 따라서 소프트웨어 교육이 정상적인 궤도에 진입할 즈음에 사이버보안 기술교육을 추진하는 것이 무리가 없을 것이다. 그러나 사이버보안 기술교육이 소프트웨어 교육의 일부로서 포함되기 위해서는 소프트웨어 교육 과정 설계에 사이버보안 기술교육이 반영되어야 하며 이에 대한 소프트웨어 교육 정책당국의 동의가 필요하다. 사이버보안 교육 체계의 분야별 도입 시점을 예정하고 이에 따라 강사 인력을 위한 연수 계획도 미리 세워두는 것이 바람직하다.

`

제 5 장 초연결사회의 기술기반 창작도구 활용에 따른 사회문화제도 고찰

이번 장에서는 초연결사회의 문화영역에서 전통적 기준이 어떤 기술적 도전에 직면해 있으며 이를 해결하기 위해 현재의 법·제도를 어떤 방향으로 수정·보완해야 하는지를 고찰한다. 2000년대 중반 디지털화와 방송과 통신이 융합하면서 이미 법·제도의 주목할 만한 변화가 있었다. 이른바 '디지털 혁명'으로 명명된 당시의 기술 발전으로 인해 디지털 환경에서 새로운 콘텐츠 유통·소비 형태가 등장하면서 이를 제어하던 저작권법에 대한 논쟁이 일어났다. 그리고 지금, 기술의 발전과 초연결사회로의 전환은 유통과 소비뿐만 아니라 창작의 영역에까지 새로운 개념과 형태를 확장시켜 다시 한 번 저작권과 관련한 법·제도에 대한 논쟁을 일으키고 있다. 이에 디지털 혁명으로부터 제기된 유통·소비 이슈에서부터 최근의 창작 이슈까지 초연결사회의 기술 환경과 연결된 디지털 콘텐츠에 대한 법·제도 이슈를 다루며 초연결사회의 지속가능성을 모색하고자 한다. 특히 창작 이슈는 초연결사회가 지능화단계로 진화하면서 새롭게 등장한 인공지능 기반의 창작물 관련 이슈로써 지금까지 축적된 사회적 논의가 거의 없다는 점에서 문헌 및 법리적 고찰 이외에 전문가 조사를 병행하였다.

제 1 절 ICT 고도화와 초연결사회의 진화

1. ICT 고도화와 기술-문화 경계의 융합

ICT의 고도화는 기술과는 별도의 영역으로 간주되어 온 문화 영역을 적극적으로 포섭하여 둘 사이의 경계를 모호하게 하는 한편, 서로가 각 영역의 발전을 촉진하는

동력이 되어 왔다. 하드웨어와 소프트웨어 형태로 개발된 기술은 그 안에 담을 콘텐츠를 필요로 하였으며 문화 영역은 문화 콘텐츠를 생산하는 도구이자 유통 수단으로써 기술을 활용하여 왔다. 이 두 영역 간의 상호작용으로 인한 경계의 모호성은 뚜렷한 경계를 기초로 한 사회 규범 및 제도와 충돌을 야기하며 전통 방식으로 각 영역에 종사해 온 사람들에게까지 영향을 미치게 된다. 역사적으로 기술은 기존의 전통을 와해하고 새로운 규범과 제도를 형성하는 계기가 되어 왔다. 반면에 전통을 쌓아온 기존 영역은 전통적 원칙과 기준을 지키되 기술에 따른 사회의 변화를 유연하게 수용할 방법을 찾아왔다.

특히 최근의 기술 환경의 변화는 문화콘텐츠의 유통과 이용, 창작의 형태를 변화시키며 기존 제도의 현대화를 요구해 왔다. 먼저 물리적 매체에 담겨 제한적으로 유통되던 콘텐츠가 디지털화하여 인터넷을 통해 보다 쉽게 이동하고 복제되며 결합하고 변형가능한 디지털 콘텐츠로 확장되었다. 하나의 콘텐츠를 원본 손실 없이 복제하여 다양한 매체를 통해 동시다발적으로 제공할 수 있게 되었으며 그 과정에서의 비용도 현저하게 감소되었다. 물리적 기반에서는 일단 소비하면 상품가치가 하락하였지만 디지털 세계에서는 상품가치를 보존하면서 무한 재생이 가능하다. 시장 범위도 물리적 경계를 넘어서게 되면서 글로벌 시장으로의 진출이 용이해졌다. 디지털화된 콘텐츠는 다양한 서비스 플랫폼을 통해 소비자에게 전달된다.

소비 형태에서도 변화가 있었다. 서비스되는 콘텐츠를 수동적으로 받아들였던 이용자들은 서비스 플랫폼에서 제공하는 피드백 채널을 통해 콘텐츠에 대해 적극적으로 논평하거나 의견을 제시하거나 지인들과 공유하기 시작하였다. 고정된 컴퓨터를 벗어나 스마트폰 등의 모바일 기기를 주로 사용하게 되면서 콘텐츠의 소비와 피드백은 언제 어디서든 가능한 일상의 소통이 되었다. 콘텐츠에 대한 논평이나 공유를 넘어 패러디한 콘텐츠를 만들어 올리거나, 자신의 소비 반응을 콘텐츠화하여 스스로가 콘텐츠를 만들어 내는 창작자가 되기도 하였다. 서비스 플랫폼은 이들에게 콘텐츠를 올리고 유통할 수 있는 개인 채널을 제공해주었고 나아가 수익창출을 위한 비즈니스 모델도 지원하기 시작하였다. 이러한 문화콘텐츠의 유통, 소비, 창작 형태

의 변화는 사회제도적 이슈와도 연결된다. 예를 들어, 거대 ICT 기업의 서비스 플랫폼에서 승자독식 구조를 벗어난 대안적 플랫폼이 등장하고 새로운 산업으로 떠오르거나 그동안 저작권과 관련이 없던 일반 이용자들이 저작권에 관련되면서 관련법을 알아야 필요가 생겼다.

2. 초연결사회의 진화

초연결사회는 사물인터넷(IoT)과 클라우드(Cloud computing), 빅데이터(Big data)와 모바일(Mobile)로 대표되는 네트워크 기반과 이를 통해 데이터의 수집, 저장, 분석, 활용 과정이 유기적으로 이루어지는 데이터 기반의 사회이다(이호영 외, 2015). 모든 사물에 컴퓨터를 내재하고 인터넷으로 경로를 잇고 데이터의 흐름을 통해 기존 경계를 통합·융합해 온 초연결사회는 2017년 현재 인공지능·머신러닝의 범용화 경향과 함께 초연결을 넘어 초지능으로 전진하는 양상을 보이고 있다. 이와 함께 인간이 개입하는 부분은 더욱 축소되고 인간의 고유 영역이라고 여겨왔던 범위는 더욱 좁아진다. 인간의 개입 없이 사물과 사물이 연결되고 상호작용하며 상호작용의 결과로 나온 데이터를 유통하여 새로운 가치를 만들어내는 데 인간의 개입을 최소화해 왔던 기술은 스스로 판단하고 통제하고 학습하여 개선할 수 있는 능력까지 갖추게 되었다.

이렇게 기술이 유통과 소비뿐만 아니라 창작의 영역에도 관여하면서 인간 중심으로 형성된 사회문화 제도에 근본적인 이슈가 발생하였다. 즉, 문화 영역에서 인간만이 창작 주체가 될 수 있는지에 대한 질문이 제기되었으며, 기술 의존도가 높아진 창작 과정에서 누가 어느 정도의 저작권을 행사할 수 있는지에 대한 논의가 시작되는 시점이다.

다음에는 ICT 고도화에 따른 기술-문화 경계의 융합과 초연결사회의 진화과정에서 나타나는 문화 현상을 살펴보고, 즉 초연결사회의 기술 환경이 문화 영역에 미치는 영향을 살펴보고 그에 대응하기 위한 제도의 개선 방향에 대한 시사점을 제시하

고자 한다. 이를 통해 지금의 사회문화적 제도가 새롭게 도래하는 초연결사회의 문화 구현을 방해하지 않고 초연결사회의 안정적 정착과 지속가능성을 위한 사회시스템을 정립하는 방향으로 개선되기를 기대한다.

제 2 절 ICT 기반 디지털 콘텐츠의 유통·이용·창작

1. 서비스 플랫폼의 다양화

인터넷의 등장은 우리 사회를 아날로그 사회에서 디지털 사회로 전환하는 시작점이었다. 아날로그 사회에서는 각 영역의 경계가 뚜렷하였다. 경계가 뚜렷한 만큼 각 영역의 특징도 분명하였기 때문에 어떤 콘텐츠를 전달하는 매체가 곧 그 콘텐츠의 특징을 규정하였다. 즉, 신문, 사진, 라디오, 텔레비전, 영화 등이 문화의 영역이자 콘텐츠를 전달하는 매체였으며 콘텐츠였다. 반면에 디지털 사회에서는 각 영역의 경계를 넘나드는 것이 용이하게 되었으며 하나의 콘텐츠가 다양한 매체로 유통되고 매체의 특징을 띤 콘텐츠들이 서로 융합하여 새로운 창작물이 등장하기 시작하였다.

가. 웹·모바일 기반 서비스 플랫폼의 다양화

웹·모바일 기반으로 동영상 콘텐츠를 제공하는 여러 서비스 플랫폼이 있다. 서비스 플랫폼의 출발점에 따라 구분을 해보면, ① 포털사이트: 네이버(TV캐스트), 카카오(다음TV팟) 등; ② 소셜 미디어: 페이스북, 트위터 등; ③ 동영상 서비스 채널: 아프리카TV, 유튜브 등; ④ 콘텐츠 사업자 서비스: 티빙(tving), 푹(pooq) 등; ⑤ 통신사 OTT(over the top) 서비스: 올레TV(KT), Btv모바일(SKT), U+HDTV(LGT) 등이 있다.

2016년 한국 시장에 진출한 넷플릭스(Netflix)는 처음부터 콘텐츠 유통 플랫폼으로 출발하였으며 기존에 제작된 방송 및 영화 콘텐츠를 주로 유통시켰다는 점에서 이용자 중심의 동영상 서비스 채널로 출발한 아프리카TV나 유튜브와 차이가 있다. 한국의 서비스 플랫폼 시장의 후발주자로서 아직 시장을 충분히 장악하지는 못했지만 직접 제작한 독자적 콘텐츠를 주요 공략 포인트로 하여 시장을 넓혀 가고 있다.

2017년 자체 제작한 영화 '옥자'를 유통시키면서 국내 이용자가 2배 이상 증가한 것이 하나의 징표이다(한국일보, 2017. 7. 18.).

음악·음원 서비스 플랫폼으로는 멜론, 엠넷, 지니, 벅스 등이 있다. 카카오가 로엔을 인수하면서 멜론 사이트를 소유하게 되었지만 카카오뮤직이라는 플랫폼을 따로 가지고 있기도 하다. 네이버도 네이버뮤직으로 음원 서비스를 제공하고 있다. 지니는 KT 자회사가 운영하고 있으며 엠넷은 CJ E&M이 소유하고 있다. 결과적으로 국내 콘텐츠 사업자, 통신사, 포털사이트가 대표적인 음악·음원 서비스 플랫폼을 소유하고 있는 것이다.

다양한 콘텐츠를 종합적으로 서비스하는 플랫폼으로는 네이버와 카카오가 대표적이다. 영화, 음악, 웹툰, 책, 뉴스, 증권, 부동산, 지도, 쇼핑 등을 비롯해 블로그와 지식서비스를 제공하고 있다. 페이스북은 사람 사이의 연결 관계를 지원하는 소셜 네트워크 사이트로 출발하여 IT 포털사이트만큼이나 다양한 유형의 콘텐츠 서비스를 지원하는 플랫폼으로 성장하였다. 구글은 검색엔진이라는 기본 형태는 유지하면서 구글 계정으로 연결된 여러 개의 개별 애플리케이션을 통해 다양한 서비스를 제공하는 플랫폼이다.

나. 서비스 플랫폼의 콘텐츠 제작

1990년대 초중반까지 방송 콘텐츠는 허가받은 소수의 방송국을 중심으로 제작되고 공중파에 의해 한정된 형태로 유통되었다. 1990년대 중반 이후 케이블, IPTV, 위성 등의 도입으로 콘텐츠의 유통채널이 확장되었으며, 2000년대 들어와서는 콘텐츠의 디지털화와 함께 휴대폰, 스마트폰, 태블릿 등 유통 매체도 확장되면서 이용자의 콘텐츠 접근성도 향상되었다. 하지만 텔레비전에 최적화된 방송콘텐츠를 모바일 기기로 소비하는 경우가 보편화되면서 모바일 기기에 최적화된 콘텐츠에 대한 수요가 증가하였다. 이에 서비스 플랫폼은 웹·모바일 기반의 콘텐츠를 제작하거나 서비스하는 비중을 늘려왔다. 드라마·웹예능 등 동영상 형식의 웹콘텐츠는 10분 내외의 짧은 에피소드 단위로 제작된 동영상 시리즈를 말한다(송진·이영주, 2015). 웹드라마,

웹예능의 콘텐츠는 보통은 편당 길이가 15분을 넘지 않을 만큼 짧다. 길게 제작되어도 30분이 최고이고 방송 콘텐츠 제작비용보다 훨씬 낮은 비용이 들 것이다. 또 공공성을 가진 공중파를 이용하는 것이 아니라 전통적으로 사적 커뮤니케이션 채널로 인식되어 온 인터넷, 즉 통신의 형태로 배포되기 때문에 사회적 책무가 덜하고 그에 따라 방송사 콘텐츠에 비해 더 자유로운 내용을 담을 수 있다. 종합 서비스 플랫폼인 네이버와 카카오는 각각의 포털사이트에 이미 제공하고 있는 웹툰, 웹소설을 다시 동영상 콘텐츠로 제작하는 등 원소스 멀티유즈(one-source multi uses: OSMU) 전략에 유리하다.

최근에는 웹·모바일 기반의 플랫폼이 직접 콘텐츠 제작에 참여하는 사례가 증가하고 있다. 네이버는 2017년 한 해 동안 25억 7,000만 원을 투자한다고 밝혔다(디지털타임즈, 2017. 4. 14.). 2016년 웹드라마 10편, 웹예능 35편 등 54편에 약 11억 원을 투자하였고 2017년에는 132편을 지원한다고 한다(디지털타임즈, 2017. 8. 24.). 카카오도 자회사 로엔엔터테인먼트를 중심으로 자체 동영상을 제작한다.

모바일 사용자의 증가로 수요가 급증하면서 서비스 플랫폼의 다양화만큼이나 경쟁이 치열해지고 플랫폼이 직접 제작하는 콘텐츠는 더욱 증가할 것으로 본다. 유튜브가 광고 없는 유료 서비스 채널인 유튜브 레드를 시작하면서 자체 콘텐츠를 제작한 것도 사용자를 유튜브 레드로 유입할 독자적 콘텐츠가 필요하였기 때문이다. 이러한 전략은 넷플릭스가 '하우스 오브 카드' 등의 드라마 제작으로 이미 성공한 전략이다. 유튜브 레드는 영상을 다운로드해서 오프라인에서도 볼 수 있다. 일반 유튜브 서비스의 경우 콘텐츠 제공자는 구글 애드센스와 연동해서 수익을 창출할 수 있고 이용자는 광고를 보는 대가로 콘텐츠를 무료로 이용한다.

페이스북은 2016년 페이스북 라이브 서비스를 시작하였다. 이용자들은 페이스북 라이브를 통해 실시간 방송을 할 수 있는데, 앱 메뉴 중 '방송하기' 버튼을 클릭하는 것만으로 간단히 실시간 방송을 시작할 수 있다. 방송 시청자 범위를 조정할 수도 있고 시청자들은 방송을 보다가 동영상 터치만으로 댓글을 쓰고 실시간 피드백 제공도 가능하다. 실시간으로 방송된 내용은 그대로 타임라인에 남아 있어 페이스북

친구들은 언제든 다시 해당 방송을 볼 수 있다. 결국 페이스북 라이브 서비스는 단순히 실시간 방송 서비스를 제공하는 것이 아니라 이용자가 직접 올리는 콘텐츠 형태를 동영상으로까지 확대하여 자체 콘텐츠를 풍부하게 하는 데 기여한다.

동영상 서비스 채널 아프리카TV는 페이스북 라이브가 시작되기 십수 년 전부터 사용자 제작 방송을 유통해 온 플랫폼이다. 최근에는 유튜브와의 경쟁에서 밀리는 양상도 보이지만 오랜 시간동안 국내의 대표적 인터넷 방송 플랫폼이었다. 이용자들은 아프리카TV에서 방송을 하면서 수익도 창출할 수 있다. 별풍선 등 유료 아이템 덕분인데, 시청자는 유료 구매한 별풍선으로 방송 진행자를 후원할 수 있다.

다. 개인방송과 수익창출

유튜브와 아프리카TV는 사용자에게 개인방송을 할 채널을 준다. 페이스북 라이브도 개인이 실시간 방송을 할 수 있지만 방송을 위한 독자 채널을 갖는 것이 아니라는 점에서 방송 특화된 서비스 플랫폼은 아니다. 국내 IT 포털사이트인 네이버와 카카오도 네이버V앱과 카카오TV에서 생중계 서비스를 제공하지만 아이돌이나 다른 유명인 중심이며 일반 이용자는 생중계 서비스를 이용하지 못한다. 카카오TV는 2017년 2월 다음tv팟을 통폐합하면서 인터넷 개인방송 서비스를 가져왔지만 개인방송 플랫폼으로 아직 두각을 나타내지 못하고 있다. 아프리카TV는 2016년 10월 인기 있던 유명 1인 방송 진행자들이 이탈하여 유튜브로 이동하면서 타격을 받았으나 수년 동안 1인 방송을 이끌어온 서비스 플랫폼이다(블로터넷, 2016. 10. 26.). 최근에는 유튜브가 더 선호되고 있다는 진단도 나오지만 2017년 1/4분기 실적 개선과 함께 다시 안정화되고 있다는 의견도 있다(비즈니스포스트, 2017. 4. 28.). 사태가 벌어지기 전 아프리카TV의 월평균 방문객은 700만 명 정도였고 2016년 9월에는 누적 시청자 수가 3억 5,000만 명이었으며, 저녁 6시 이후부터 자정까지 동시 방송 채널 수는 5,000개 전후이고 매일 10만 개의 방송이 나갔다(한국저작권보호원, 2016).

한국경제매거진(2017. 6. 21.)에 따르면 1인 방송 사업은 10대, 20대 등 한정된 연령층을 넘어 3세부터 70세까지 연령층이 확대되고 있으며 콘텐츠도 게임 중심에서

교육, 캠핑, 반려동물 등 전 방위로 확장되고 있다. 1인 방송 시청자는 방송 중에 언제든 자신의 의견을 1인 방송인에게 전달할 수 있고 1인 방송인은 즉각적인 피드백을 전달하는 등 생생한 쌍방향 소통을 경험할 뿐만 아니라 쌍방향 소통 내용이 방송으로 생생하게 중개되면서 방송 콘텐츠 제작에 참여하는 경험도 한다. 1인 방송 산업의 성장은 다중 채널 네트워크(multi-channel networks, 이하 MCNs) 산업의 성장과 연결된다. MCNs는 1인 방송인과 제휴하여 프로그램 기획과 투자, 마케팅과 제작 시설 및 장비 공급, 저작권·홍보·교육·광고·수익관리 등을 지원한다(유재흥·김윤명, 2015).

2. 이용자 지위의 변화

가. 콘텐츠 생산자로서의 이용자

인터넷 등장 이전까지 문화콘텐츠를 전달하는 기술 매체는 신문, 사진, 축음기, 영화, 라디오, 방송 등이었고 콘텐츠가 제작되어 매체를 통해 전달하는 과정은 일방향이었다. 이용자는 엄밀하게 콘텐츠를 이용하기보다는 일방적으로 수용하는 수용자였다. 반면에 인터넷은 등장 초기부터 쌍방향 매체로 주목받았는데, 수동적으로 콘텐츠를 소비해 온 이들에게 피드백을 전달할 기회, 즉 쌍방향 소통의 기능을 더함으로써 수용자를 보다 능동적인 위치의 이용자로 전환시키는 계기가 되었다. 그러나 초기 인터넷은 콘텐츠를 다운로드하는 속도에 비해 업로드하는 속도가 확연히 느렸으며 네트워크 기술의 한계 때문에 기본적 웹 환경에서 텍스트 중심의 피드백만 허용하는 등 소통의 한계도 컸다.

팀 오라일리(Tim O'Reilly)가 웹 2.0 시대를 선언한 2000년대 중반에 들어서면서 쌍방향성은 좀 더 제 기능을 하기 시작한다. 이용자는 스스로 웹 기반의 매체를 만들고 콘텐츠 생산자의 지위를 획득하였으며 간편한 디지털 편집도구를 이용할 수 있는 기술 환경 덕분에 자기만의 소비 양식을 만들어갔다. 즉, 텍스트 중심에서 벗어나 이미지뿐만 아니라 동영상 형식의 콘텐츠를 스스로 만들어 올리거나 다른 이가

올린 콘텐츠를 변형시켜 다시 공개하는 등 콘텐츠 확산에 보다 적극적으로 참여하였다. 한 단계 업그레이드된 인터넷에서 비전문가, 즉 아마추어들도 쉽게 참여할 수 있는 디지털 환경이 조성되면서 콘텐츠 생산 영역이 확대되었고 콘텐츠를 생산하는 동시에 소비하는 프로슈머라는 신용어도 등장시켰다. 프로슈머는 생산자(producer)와 소비자(consumer)가 결합된 신조어로 생산자이자 동시에 소비자라는 의미를 갖는다.

프로슈머의 등장은 일부 전문영역에서만 영향을 미쳤던 저작권법이 일반 이용자에게도 영향을 주는 일상의 법으로 전환되는 계기가 되었다(박유리 외, 2009). 그러나 이후 10여 년간 일반 이용자의 저작권법 위반 사례가 급속하게 증가하였을 뿐 당시 제기되었던 이슈는 아직 온전하게 해결되지 못한 상태이다. 사회시스템의 변화 속도가 기술에 따른 콘텐츠 이용형태의 변화 속도를 따라가지 못한 것이다.

콘텐츠 생산에 이용자의 참여가 거의 없던 과거에는 다른 이의 창작물을 불법적으로 이용해 경제적 이익을 취하는 계획된 범죄가 대부분이었다. 그러나 최근 10년간은 저작권자의 경제적 이익을 해할 의도가 없는 비자발적 저작권 침해 사례도 발생하고 있다. 대부분의 일반 이용자는 온라인에서 쉽게 이용가능한 콘텐츠를 재활용하여 자신만의 표현양식으로 가공하는 과정이 누군가의 창작물을 훼손하거나 경제적 이익에 해를 준다는 점을 이해할 기회가 사회적으로 거의 없었으며 지금도 크게 나아지지 않았다.

2009년 우리나라에서 5살 꼬마의 동영상을 블로그에 올렸다가 동영상에 부른 노래의 저작권이 문제되어 차단된 사례가 언론을 통해 널리 알려지면서 저작권 논쟁을 일으킨 적이 있다(한겨레, 2009. 6. 24.). 유사한 분쟁은 물론 해외에서도 있었다. 2007년 프린스의 노래 ‘Let’s go crazy’에 맞춰 춤을 추는 세 살 아들의 비디오를 올린 부모가 저작권 소유자 유니버설 뮤직 그룹으로부터 저작권 침해 통지서를 받은 것이다(Mullin, 2017. 6. 20.). 우리나라와는 달리 해당 비디오는 복원되었고, 저작권 소유자는 오히려 ‘공정이용’ 권한을 무시하였다는 이유로 또 다른 법적 소송을 받게 되었다가 최근 소송 기각 판결을 받았다.

나. 이용자 지위 변화에 따른 저작권 이슈

콘텐츠 소비자였던 일반 이용자가 콘텐츠 생산자 지위를 획득한 이후 다양한 수준의 디지털 콘텐츠가 기하급수적으로 증가한 것은 창작자 혹은 저작권 보유자에 대한 보상 체계를 흔드는 요인 중 하나가 되었다. 이용자가 접근할 수 있는 플랫폼에서 제공하는 다양한 미디어 채널과 콘텐츠 편집 도구는 창작자의 수준을 타고난 전문가 수준에서 누구나 시도해볼 수 있는 일상 수준으로 낮추었고, 소셜 미디어를 통한 사회관계의 연결성은 아마추어 창작자의 콘텐츠를 쉽고 빠르게 전달할 수 있는 효율적인 유통 경로로 기능하였다. 이용자는 본인의 일상 경험이나 감성을 공유하는 데서 나아가 자신의 취미나 특기, 전공 분야에 특화된 정보를 전달하는 채널로 소셜미디어를 이용한다. 생산자의 지위로 확장한 일반 이용자는 스스로 혹은 MCNs를 통해 수익 모델[51]을 적극적으로 모색하기도 한다. 비상업적 의도의 콘텐츠 제작과 업로드 활동에서 상업적 이익 추구로 진전되면서 일반 이용자와 관련된 저작권법 이슈 역시 강도를 더한다. 기존 저작물 이용 대가가 경제적 이익으로 연결될수록 원저작자의 경제적 이익 침해 논쟁을 일으키게 되기 때문이다.

수익 창출을 목적으로 한 개별 방송 채널 이외에 사적으로 사이트를 운영하는 일반 이용자들도 무지 혹은 (법) 무시에 의한 저작권 침해 문제가 발생하기도 한다. 예를 들어, 동영상을 찍어 올릴 때 기술적으로 배경 음악 삽입이 쉬워졌지만 저작권이 있는 음악을 그대로 사용하면 안 된다는 것을 배울 기회는 드물다. 게다가 저작권을 의식하고 대가를 지불하고 이용하려고 해도 그 방법과 절차가 알려지지 않아 현실

51) 대표적으로 구글이 제공하는 구글 애드센스를 들 수 있는데, 개인 블로그나 홈페이지, 유튜브 등에 구글이 계약을 맺은 광고가 노출되는 애드센스를 설치하여 사이트의 방문정도에 따라 광고 노출의 대가로 구글로부터 일정 수익을 보장받는 형식이다. 방문자가 광고를 클릭하면 보상은 더 커진다. 사이트 운영자는 방문자에게 매력적인 콘텐츠를 제공하여 방문객수를 늘리고 그만큼 구글로부터 대가를 받는 구조이다. 최근 급증하고 있는 1인 방송채널은 시청자로부터 선물을 받는 형식, 타기업과의 협약에 따른 직간접 광고 수익 등 다양한 경로로 수익을 창출한다.

적으로 어려운 경우도 많다. 이에 기술 환경 및 이용형태의 변화와 함께 일반 이용자들에게 저작권에 대한 이해를 넓힐 기회를 마련하고자 한국저작권위원회 등이 교육서비스[52]를 하고 있지만 사회적 인식은 여전히 낮은 수준이다.

제 3 절 기술기반 창작도구와 비인간 창작자의 등장

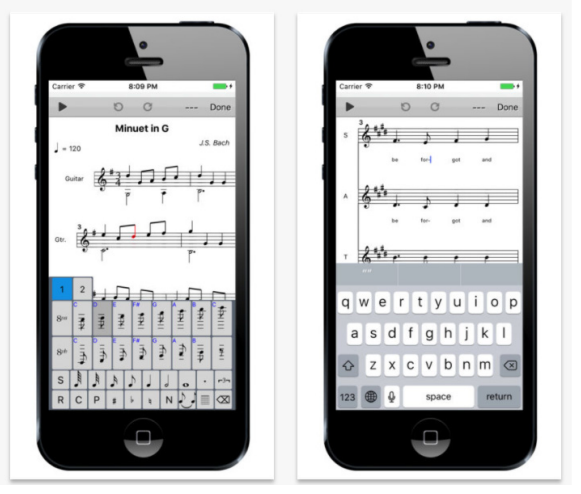
1. 디지털 창작도구

일반 이용자들의 접근과 활용이 용이한 디지털 창작도구는 계속해서 진화하고 있다. 최근 델(Dell)은 윈도우 10을 창작 도구로 하는 디스플레이인 캔버스 27을 선보였다(ITWorld, 2017. 1. 6). 디스플레이는 마우스나 키보드 대신에 손을 이용한다. 구글의 틸트 브러시 툴킷은 3D환경에서 창작할 수 있게 지원하는 창작도구이다. 오픈소스로 공개되었기 때문에 원하는 창작자는 누구나 사용할 수 있다(블로터, 2017. 1. 24). 펜과 터치 기능의 창작용 태블릿은 이미 많은 웹툰 작가나 아티스트, 디자이너, 사진작가 등이 사용하고 있으며 일반 이용자들도 취미 활동을 창작용 태블릿을 구입해 이용하기도 한다.

모바일 앱스토어에서 구입할 수 있는 Score Creator는 작곡을 도와주는 앱이다. 음표 키보드와 코드 키보드가 가상환경에서 구현되어서 마치 텍스트를 입력하듯 음표와 코드를 입력할 수 있다.

52) 한국저작권위원회는 범국민 대상의 저작권 평생교육원을 운영하면서 맞춤형 교육지원, 산업현장의 필수 저작권 직무능력 개발 지원, 교육콘텐츠 개발 보급 등의 임무를 수행한다(한국저작권위원회 원격평생교육원(http://edulife.copyright.or.kr) 참조).

〔그림 5－1〕 Score Creator 스크린샷



자료: 애플스토어 Score Creator 스크린샷.

이러한 창작도구는 인간의 창작 활동을 지원하는 도구이다. 즉, 인간이 창작욕구와 아이디어를 좀 더 용이하게 표현할 수 있게 보조한다. 도구의 활용은 인간임을 증명하는 하나의 특징이며 도구로서의 기술의 발전은 곧 인간의 외부적 능력이 어떻게 증가해왔는가를 보여주는 기록이다(멈퍼드, 1952; 박홍규 역, 2011).

그러나 초연결사회는 문화와 기술의 영역이 모호해지는 사회일 뿐만 아니라 과거부터 지금까지 문화영역에서 기술이 수행해온 역할을 넘어서는 새로운 이슈를 가져온다. 네트워크 기반으로 연결되는 사물의 수가 무한증대하고 그 사물을 이용하는 사용자와의 상호작용뿐만 아니라, 연결된 사물 간 상호작용으로 끊임없이 디지털 정보를 생성하며 그 디지털 정보조차도 연결망에서 교류되도록 작동하는 초연결사회에서는 인간의 통제를 벗어난 영역이 증대한다(박유리 외, 2016). 초연결사회에 들어서서 인간은 이미 거대한 데이터의 양에서부터 통제의 어려움을 경험하였고, 이에 빅데이터 분석 기술 등을 통해 외부적 능력으로 보완하고자 하였다. 지금은 인공지능 기반의 지능형 서비스의 등장으로 인간의 통제가 불필요한 지능형 자동화

영역이 확장되고 있다. 이러한 변화는 문화 영역에서는 비인간에 의해 생산된 창작물이라는 지금까지 논의되지 않았던 새로운 이슈를 가져왔다.

2. 비인간 창작자의 등장과 협업적 창의성

초연결사회는 인간과 상호작용하는 일상의 사물뿐만 아니라 인간의 개입 없이 사물 간 상호작용만으로 현상이 일어나는 경우가 빈번한 사회이다(박유리 외, 2016). 예를 들어, 카네기 멜론의 교통체증 개선을 위한 스마트 인프라는 인간의 개입 없이 기술의 작동만으로 최적의 교통 흐름을 구현한다.[53] 현재의 교통상황을 파악하고 최적화된 교통 흐름을 유지하기 위해 신호체계를 통제하며 자동차들의 흐름 속도에 맞춰 다음 신호체계와 상호 소통하여 현 상황과 연계된 조치를 대기시키는 과정이 센서기술, 인공지능 등을 기반으로 한 컴퓨팅 사물 간의 상호작용만으로 판단되고 결정되는 식이다.

이처럼 비인간 행위자 간 상호작용으로 사회 시스템이 지능화하고 스스로 작동하는 초연결사회에서도 창작의 영역은 한동안 인간 행위자만이 할 수 있는 고유한 영역으로 보는 인간중심주의적 시각이 쉽게 사라지지는 않을 것이다. 그러나 인공지능 기반의 미술, 음악, 소설, 기사 등이 생산되기 시작하면서 창작의 영역에서도 인간의 통제를 벗어난 비인간 행위자의 역할이 부각되고 있다.

인공지능 알고리즘은 인간 개발자가 만든다. 알고리즘의 학습을 위한 기초 자료는 기존 데이터로 충당하며 그 데이터는 개개인이 생성한 정보이다. 무엇인가를 생

53) 2012년부터 카네기 멜런 대학에서 주관하고 있는 스마트 인프라 구축 프로젝트는 피츠버그 간선도로를 중심으로 교통체증 개선을 위한 시스템을 개발하기 위한 것인데, 여기에 사물인터넷과 센서 기술, 인공지능 등 초연결사회의 근간이 되는 기술이 적용된다. 스마트 인프라 시스템은 먼저 ① 센서 데이터 시스템으로 현재의 교통 상황에 대한 정보를 추출하고, 그다음 ② 최적화한 교통상황을 위한 조치(명령)를 신호체계에 전송하며 ③ 다음 신호체계와 소통하여 현 상황과 연계된 조치를 대기시키고 ④ 매초 이 스케줄 주기를 반복한다(Smith, 2016).

성하려는 목적을 가진 이용자가 개발된 인공지능 알고리즘에 필요한 데이터를 재료로 투입하여 창작물을 추출하였다면 그 결과물은 협업적 창의성이 발휘된 결과물이라고 볼 수 있을까? 협업적 창의성이란 천재의 재능으로서의 창의성과 비교되는 것으로 사회적 상호작용과 협업의 결과물이다(이종관, 2017). 엄밀하게 인공지능의 창작활동에서는 협업적 창의성의 과정이 개입한다고 할 수 없다. 주체들 간에 생각을 주고받고 자신의 생각과 타인의 생각을 연결하여 생각의 핵심을 변형시키거나 새로운 생각으로 진전시키는 과정이 없기 때문이다. 다만 단계마다 참여하는 주체가 달라진다. 알고리즘 개발 단계에서는 개발자가, 기계학습 단계에서는 수많은 개별 행위자가, 그리고 최종단계에서 알고리즘을 사용하는 사용자가 각 단계의 주체이지만 이들 간 상호적 협업은 없다. 더구나 최종 결과물은 누구나 접근가능한 공유물이 아니다. 사실 이 최종 결과물에 대한 성격과 법적 권한, 소유권을 주장할 대상과 사회적 책무를 질 주체가 사회적으로 명확하게 정의되지 않은 상태이다.

3. 지능형 창작도구와 비인간의 창작물

여기서는 현실의 사례를 통해 인공지능 기반의 지능형 창작도구가 인간의 의도가 거의 개입되지 않는 상황에서 협업 과정을 통해 스스로 창작물을 생성하는 데까지 진화한 사례를 고찰한다. 앞서 언급하였듯이 인공지능 기반의 창작도구는 콘텐츠 생산에 직접 관여한다는 점에서 기존의 기술 창작도구와 다른 잠재성을 가지고 있다. 도구의 기능을 넘어서 인간이 주도해온 창작과정에 개입하는 것이다. 즉, 이미 개발된 인공지능 알고리즘과 투입하는 데이터에 따라 창작물이 생성되는 과정에서 인간의 개입은 최소한으로 축소된다.

이와 관련하여 먼저 뉴스 기사가 인간이 아니라 기술에 의해 작성되고 이를 독자들이 이질감 없이 받아들이는 로봇저널리즘을 이야기해볼 수 있다. 기사 작성을 위해 개발된 로봇저널리즘 알고리즘은 2009년 첫선을 보인 이후 최근 영향력 있는 뉴스서비스 기업에서 활용되고 있다. 예를 들어, 뉴욕타임스는 스태츠멍키

(StatsMonkey)라고 불리는 로봇저널리즘 알고리즘을 사용하고 있다. 2014년 미국 LA타임스의 퀘이크봇(Quakebot)은 지진 속보를 8분 내에 직접 작성하여 화제가 되었으며, 그밖에 AP통신의 워즈스미스(Wordsmith), 포브스의 퀼(Quill), 텐센트의 드림라이터(Dreamwriter) 등이 현재 유력 뉴스 서비스 기업이 사용하는 로봇 저널리즘 알고리즘이다. 국내 최초의 로봇저널리즘에 의한 기사는 2016년 IamFNBOT가 쓴 파이낸셜 뉴스의 "코스피 4.92포인트 하락, 1840.53포인트 거래 마감"이다(파이낸셜 뉴스, 2016. 1. 21.). 그밖에 국내에는 매일경제의 엠로보(M-Robo), 전자신문의 로봇 ET 등이 있다.

현재 로봇저널리즘은 주어진 정보를 가지고 단순 사실 기사를 작성하며 인간의 검수가 필요한 수준이다. 즉, 현재의 로봇 저널리즘은 기사 작성에 사고와 통찰이 개입되지 않는 단순 사실 기사를 빠른 시간 내에 생산해냄으로써 기자의 역량을 보다 가치 있는 기사 작성에 집중할 수 있게 지원하는 역할에 제한되어 있다. 로봇 저널리즘 알고리즘이 사고와 통찰이 필요한 칼럼이나 탐사보도까지 가능한 수준으로 발전하는 시기는 현재로서는 가늠할 수 없지만 언젠가 실현될 것으로 전망된다. 인간의 지능과 사고, 통찰이 표현되어 온 뉴스 기사 영역까지도 데이터 기반의 지능형 로봇이 처리할 수 있게 될 미래가 그리 멀지 않았다는 것이다.

인공지능 기반의 작사·작곡 알고리즘도 상용화되었다. 일본에서 개발한 '오르페우스'는 리듬과 곡조를 설정한 후 단어 몇 개를 삽입하면 자동으로 가사를 만든다고 한다. 웹사이트 형태로 서비스되고 있으며 누구나 무료로 사용할 수 있다. 가사 데이터베이스와 음악 이론으로 학습한 알고리즘으로 하루 200여 곡을 만들어 낸다고 한다(전자신문, 2016. 1. 26.). 인공지능 헤드폰은 인공지능 기반 작곡 알고리즘인데 역시 일본에서 개발되었다. 인공지능 헤드폰을 쓴 사람이 특정 음악을 들을 때 변하는 뇌파 기록으로 학습하고 헤드폰 사용자의 뇌파 정보만으로 그 사람의 기분에 맞는 음악을 1분 만에 만들어낸다고 한다(디지털타임스, 2017. 4. 5.). 미국의 에밀리 하월(Emily Howell)은 협주곡을 몇 개 들려주고 악보를 입력하면 악보의 패턴을 분석해서 새로운 음악을 작곡한다. 에밀리 하월이 만들어낸 음악은 실제로 아이튠즈,

아마존 등의 온라인·모바일 플랫폼에서 판매되기도 하였다. 그밖에 쿨리타(Kulitta), 라무스(Lamus) 등이 있다. 스페인 말라가대학에서 개발한 인공지능 '라무스(Lamus)'가 작곡한 음악은 오케스트라가 연주하여 CD로 판매되기도 하였다(한국저작권보호원, 2017).

인공지능 알고리즘은 뮤직비디오까지 만들어낸다(The Verge, 2017. 4. 12.). 디지털 이미지로 구성된 뮤직비디오로 꽃, 잔디, 건물 등의 이미지가 노래와 함께 점점 정교해지는 정도여서 인간이 제작한 뮤직비디오의 수준에는 현저히 미치지 못한다. 그러나 노래의 오디오 데이터를 기초로 특정 모양과 조명, 질감을 선택하고 작동시켰다는 점에서 주목받았다.

구글의 인공지능 기반 미술 창작 알고리즘인 딥드림(Deep Dream)은 미술작품 전시회에 선보인 후 약 10만 달러의 판매수익을 올리기도 하였다. 딥드림 사이트[54]에 가면 딥드림 알고리즘을 이용하여 누구나 이미지를 생성할 수 있으며 자기가 생성한 이미지를 공개하는 사이트도 따로 있다.[55] 이미 있는 이미지 파일을 딥드림에 투입하면 투입한 이미지들의 혼합으로 새로운 이미지 파일이 생성된다. 딥드림의 결과물은 사실상 원본이 따로 있는 2차 저작물인 셈이다. 딥드림의 생성물은 창작물이라기보다는 이미지 합성 알고리즘에 의한 합성물이 더 맞는 표현일 수도 있다. 이미지 변형은 정해진 알고리즘으로 규정되기 때문에 딥드림으로 생성된 이미지인지 아닌지 구분하는 것은 어렵지 않다. 구글은 딥드림으로 생성된 이미지들을 하나의 미술사조인 것처럼 하여 인셉셔니즘(inceptionism)이라는 사조 이름도 정해 주었다.

비슷한 이미지 변형 알고리즘으로 프리즈마가 있다. 인공지능 기반으로 사진 이미지를 특정 화풍의 회화 이미지로 변형시킨다. 프리즈마도 창작 미술을 한다기보다는 '아주 간단한 사진 편집 앱'으로 평가되는 수준이다(뉴스위크, 2016. 8. 8.).

---

54) Deep Dream Generator(http://deepdreamgenerator.com/).

55) Deep Dream web interface(http://psychic-vr-lab.com/deepdream/).

〔그림 5－2〕 프리즈마로 형성된 이미지샷

자료: 뉴스위크(2016. 8. 8.).

암스테르담에서 공개된 새로운 ‘렘브란트’ 화풍의 그림은 사람이 아닌 인공지능과 3D 프린팅 등 기술의 융합 작품이었다. 페인트 기반의 UV 잉크를 사용해 렘브란트가 사용한 그림의 질감이나 붓터치를 재현, 3D 인쇄로 출력한 결과물로서 딥러닝 알고리즘을 이용해 346점의 유명한 렘브란트 그림을 분석하고 렘브란트의 그림 주제와 스타일을 모방하되 새로운 작품을 만들어내었다. ‘넥스트 렘브란트(The Next Rembrandt)’라고 명명된 이 작품은 백인 남성의 초상화로 렘브란트 작품과 유사하다. 총 18개월이 걸린 이 프로젝트는 네덜란드의 광고 회사 월터 톰슨(J. Walter Thompson)이 기획했으며 ING, 마이크로소프트 등이 협업했다.[56]

56) The Next Rembrandt(https://www.nextrembrandt.com/).

〔그림 5－3〕 넥스트 렘브란트

자료: The Next Rembrandt(https://www.nextrembrandt.com/).

인공지능으로 쓴 시나리오로 단편영화가 제작되기도 하였는데, 1980년대부터 90년대에 나온 SF 드라마와 영화 수백 편의 대본으로 학습한 후 완성한 대본으로 8분짜리 SF물인 영화 ‘선스프링(Sunspring)’을 만들었다. 영화 제작 후 공상과학영화 축제에도 참가하여 상위 10위 안에 들기도 하였으며 유튜브를 통해 배포되었다. 학습용 대본은 온라인에서 구할 수 있는 대본이었다(곽노필, 2016. 6. 14.).

현재의 수준에서 인공지능 알고리즘 기반의 창작도구는 기본적으로 학습용 데이터가 필요하다. 기사 작성이든 작사·작곡이든 회화 이미지 창작에서 뮤직비디오, 영화시나리오 구성까지 사전에 학습이 필요하다. 인간은 알고리즘 개발과정과 학습용 데이터 투입과정 등에 관여한다. 생성된 결과물이 인간의 온전한 의지와 능력으로 만들어진 것이 아니라 인공지능의 자동화 과정을 거쳤다는 점에서 창작의 주체 논쟁이 일어난다. 인공지능을 통한 창작물을 온전히 인간의 창작물로 인정할 수 있는지, 새로운 기준을 세워 인공지능의 창작물로 봐야 하는지, 혹은 협력적 창의성의 결과물이라고 보고 인간과 인공지능 둘 다의 역할을 인정해야 하는지 등에 대한 논쟁이 있다. 또 창작 과정마다 개입한 인간이 다르기 때문에 어떤 과정에서 어떤

역할을 한 인간에게 어느 정도의 권리를 부여하는지에 대한 논의도 필요하다. 즉, 이 생산물을 저작권이 있는 창작물로 인정할지, 창작물로 본다면 저작권은 누구에게 부여되는지, 저작권한은 얼마나 지속될 수 있는지 등에 대한 제도적 논의가 필요할 것이다. 이와 관련해서는 뒤에 인공지능 기반 창작도구를 이용한 창작물의 저작권한을 논할 때 다시 다룬다.

제 4 절 기술 환경 변화와 주요국의 정책 방향

초연결사회의 연결성은 데이터의 무한생성으로 이어지고 데이터로부터 고부가가치를 창출하는 데이터경제를 이끌었다. 초연결사회의 이러한 특성은 데이터의 또 다른 형태로써의 디지털 콘텐츠를 활용을 통한 가치창출의 원천으로 보는 경향을 강화시킨다. 세계 각국은 저작권의 현대화를 통해 기술 환경 변화에 따라 등장한 새로운 사회문화 경향을 수용하고자 한다. 다음에서는 주요국의 저작권에 대한 사회 및 정책적 논의를 고찰하여 디지털 콘텐츠에 대한 제도적 지향이 어디를 향해 있는지를 구체적으로 살펴본다.

1. 디지털 콘텐츠의 이용 활성화 정책

디지털 콘텐츠는 ICT 기반의 신산업·디지털 경제의 경쟁력을 높일 핵심 요인으로 주목받고 있다. 이에 각국은 창작자의 권리보호를 통해 질 좋은 콘텐츠 생산을 독려하는 한편, 콘텐츠 유통 시장을 활성화하여 산업경제 경쟁력의 향상을 추구하는 것을 정책 방향으로 설정하고 있다. 이와 관련하여 최근 각국에서 추진한 정책과 향후 계획을 살펴본다.

가. 미국

미국 정부는 2016년 6월 30일 최종 개정된 미국의 저작권법이 1976년의 저작권법의 기본 틀을 따른다고 명시하고 있지만(U.S. Copyright Office, 2016), 미국 저작권법은

디지털 시대를 반영한 시발점인 1998년 개정된 이른바 디지털 밀레니엄 저작권법(Digital Millennium Copyright Act: DMCA)에서부터 논해진다. 법령의 첫 타이틀은 '온라인 저작권 침해에 대한 책임 제한(Online Copyright Infringement Liability Limitation Act)'으로, 불법 저작물 유통에 대한 온라인 서비스 제공자(OSP)의 면책 조항을 담고 있다. 저작권자로부터 불법 저작물의 삭제 요청을 받아 해당 콘텐츠를 삭제하면 저작권 침해로부터 면책된다. 또한 불법 복제에 대한 기술적 방어 보장, 컴퓨터 유지·보수를 위해 필요한 복제 행위에 대한 면책 등이 주요 내용으로 포함되어 있다.(U.S. Copyright Office, 1998).

켈러(Keller, 2017)에 따르면, DMCA의 목적은 ① 소송 없이 온라인에서의 저작권 침해를 저지할 수 있는 절차 마련, ② 온라인 서비스 제공자에게 예측 가능한(명확한) 법 조항 제공, ③ 저작권자와 온라인 서비스 제공자에게 처리 절차에 대한 의무를 부여하는 대신 이용자의 합법적 콘텐츠에 대한 삭제 조치가 남용되지 않도록 처리, ④ 합법적(이고 수익창출이 가능한) 온라인 콘텐츠 유통을 위한 기술 및 비즈니스 모델 개발 촉진 등이다. 1998년 이후 온라인을 통한 콘텐츠 유통의 증가와 디지털 콘텐츠 자체의 양적 증가 등 기술 환경 변화와 함께 온라인 서비스 제공자에 의한 과잉 삭제나 로봇에 의해 대리되는 통지 절차에서의 오류 등 여러 문제가 제기되어 왔다.

2010년 이후 저작권 개혁에 대한 사회적 논의가 시작되었다.[57] 2010년 미국 상무부가 정책 조정의 필요성을 제기하고 '개인 정보 보호 정책, 저작권, 글로벌 정보의 자유로운 흐름, 사이버 보안에 대한 포괄적인 검토 및 인터넷 경제에서의 혁신' 등을 다룰 태스크 포스를 운영하고, 그 결과를 「디지털 경제에서의 저작권 정책, 창의, 그리고 혁신(Copyright Policy, Creativity, and Innovation in the Digital Economy)」

57) 2010년 '저작권 원칙 프로젝트: 개혁의 방향(The copyright principles project: Directions for reform),' 2013년 '넥스트 그레이트 저작권법(The Next Great Copyright Act),' 2013년 '디지털 경제에서의 저작권 정책, 창의, 그리고 혁신(Copyright Policy, Creativity, and Innovation in the Digital Economy)' 등에서 개혁 논의를 확인할 수 있다.

보고서를 통해 발표하였다(U.S. The Department of Commerce, 2013). 보고서의 주요 내용은 저작물에 대한 권리와 활용 간의 균형 정책 제안, 온라인 저작권 침해 방지, 적법하게 서비스 성장을 촉진하는 집행 수단 마련 등이다. 흥미로운 것은 저작권에 대한 논의를 미국 상무부가 주도한 사실이다. 미국 중앙부처에는 우리나라 문화체육관광부에 해당하는 부처가 없으며 상무부가 문화산업의 측면에서 저작권 기반 산업을 다루기 때문이다. 따라서 미국의 저작권 정책은 일관되게 기술 혁신에 따른 문화산업 발전의 기회를 최대한 보장하는 데 초점을 맞출 수 있었다.

2015년 미국 컴퓨터와 통신산업협회(Computer & Communications Industry Association: CCIA)가 발표한 「디지털 경제를 위한 저작권 개혁(Copyright Reform for a Digital Economy)」 보고서에서는 보다 직접적으로 초연결사회의 경제·산업적 측면에서 접근하는 저작권 정책의 기조를 확인할 수 있다. 이 보고서는 지금까지의 저작권 정책은 경제적 보상을 통해 창작자의 창작활동을 장려하는 데 중점을 두어 왔지만, 기술 발전 덕분에 '누구나 전 세계 이용자를 잠재 고객으로 하는 콘텐츠 제작자'가 될 수 있는 현실에서는 신산업·신서비스 창출에 대한 장벽을 최소화하는 것이 바람직하다고 주장한다. 그리고 이와 관련하여 저작권 개혁에 중요한 두 가지 원칙을 제시한다. 첫째, 모든 라이선스 사용자와 소비자가 비자발적 저작권 침해를 하지 않도록 신기술 혁신을 수용하는 것과 둘째, 콘텐츠 산업만이 아니라 저작권법의 영향을 받는 어떠한 비즈니스에서도 관련 법제도의 예측가능성을 높이는 것이다(CCIA, 2015).

〈표 5－1〉 '디지털 경제를 위한 저작권 개혁' 원칙

원칙	내용
(1) 새로운 기술 혁신의 수용을 위한 원칙	1) 공정이용(fair use) 보장은 저작권법의 핵심이며 관련 입법안의 핵심 고려사항임 2) 계약상의 제약이 상품의 자유로운 유통을 제한하지 않도록 보장하기 위해 최초 판매 원칙을 유지해야 함 3) 저작권 소유에 대한 투명성을 높이고 반경쟁 행위를 단속하기 위

원칙	내용
	한 라이센스 제도를 개혁해야 함. 또 저작물과 관련한 데이터의 품질과 이용 가능성을 향상시키기 위해 저작권 사무국을 개혁해야 함
(2) 비즈니스 확실성 제공을 위한 원칙	1) 클라우드 컴퓨팅 및 소셜 미디어 등의 온라인 서비스에 대한 DMCA(Digital Millennium Content Act, 디지털밀레니엄저작권법)의 세이프하버(safe harbor)를 유지해야 함 2) 예측 가능성을 더 높일 수 있도록 불균형적인 법적 손해배상을 개혁해야 함 3) 합리적이고 효과적인 처벌조항을 포함하여 고의적인 저작권 오용을 방지하기 위한 법령을 제정해야 함 4) 기업의 임원 또는 주주가 기업의 저작권 침해 행위에 관여하거나 2차적 책임 원칙에 따른 책임이 있을 때 기업이 감추고 있는 것을 복원해야 함

자료: CCIA(2015).

새로운 기술혁신 수용에 대해서 CCIA(2015)는 클라우드 컴퓨팅과 개방형 비즈니스 모델, 새로운 창작 모델 등을 예로 든다. 먼저 클라우드 컴퓨팅은 사용자 컴퓨터에서 로컬로 처리하던 파일 저장, 백업, 온갖 데이터 처리 행위가 '클라우드'에서 원격으로 수행가능하게 되면서 '사적 이용'에 대한 판단을 어렵게 한다. 이와 관련하여 CCIA(2015)는 기술 혁신을 수용하는 태도라면 로컬 컴퓨터에서의 사적 이용과 마찬가지의 기준이 클라우드 컴퓨팅에서도 적용되어야 한다고 주장한다. 또 오픈소스 소프트웨어는 공동 혁신 모델의 개발을 가능하게 하며 소프트웨어가 아니라 소프트웨어를 이용한 서비스 제공으로 수익을 얻는 개방형 비즈니스 모델이 정착되는 과정이라고 본다. 따라서 소프트웨어를 저작물로 보는 개념도 변해야 한다는 것이다. 마지막으로 새로운 창작 모델이란 크리에이티브 커먼스 라이선스(creative commons license), 즉 라이선스의 개방과 공유를 통해 창작물의 유통을 자유롭게 하는 대신 크라우드 펀딩이나 창작물을 매개로 얻는 광고, 콘서트 등의 수익으로 충당하는 방식이다. 크리에이티브 커먼스 라이선스는 창작자가 어느 정도의 수준으로 라이선스를 허용할지를 결정[58]하고 그 내용을 기호로 표시한 후 자신의 창작물을

배포하는 것이다.

최근 미국의 정책 기조를 살펴볼 수 있는 자료로 2016년 대선 당시 공표되었던 민주당과 공화당 정강에서의 지식재산권 관련 정책 내용이 있다. 미국 민주당은 국내외 예술가, 창작자, 발명가 등의 지식재산권 보호에 대한 지지를 표명하는 한편 쿼터제, 차별조치, 데이터현지화 등의 요구에 반대하는 입장을 보였다(The Democratic Platform Committee, 2016). 창작자 보호와 함께 디지털 콘텐츠의 유통 활성화에 중점을 두었는데, 주목할 것은 유통활성화 정책이 다른 나라의 보호 정책과 밀접하다는 점이다. 쿼터제나 자국 콘텐츠 우대 정책 등은 우리나라를 비롯해 자국의 문화를 보호하려는 여러 나라들이 채택해 온 정책들이다. 데이터현지화는 초연결시대에 자국민의 개인정보를 보호하겠다는 취지로 개인정보를 저장하는 물리적 서버의 위치를 자국 내로 한정하는 것이다. 이 역시 글로벌 ICT에 의한 자국민 개인정보의 유출을 막으려는 국가들이 채택하는 정책이다. 결과적으로 미국 민주당의 정책 방향은 자국 저작권자의 권리 보호를 통해 창작 활동을 장려하면서 해외의 원활한 콘텐츠 유통을 저해하는 정책을 저지하려는 의도가 분명하다. 민주당과는 달리 공화당은 지식재산권에 대한 뚜렷한 정책을 발표하지 않았지만, 중국 등 해외 저작권 침해에 대응하여 자국의 자산 보호에 강조점을 두겠다는 의사가 표명되었다(The Republican Platform Committee, 2016). 민주당과 공화당의 정강이 미국 대선 당시에 발표된 만큼, 자국민에게 호소할 만한 내용이 필요했을 것이다. 따라서 더욱 미국 중심의 정책이 나올 수밖에 없다는 점을 고려하더라도, 미국이 전 세계를 디지털 콘텐츠 유통 시장으로 보고 각국의 유통 시장을 미국 내 콘텐츠의 자유로운 유통 수준에 맞춰 미국 기업의 성장을 꾀하고 있음을 양 당의 정강을 통해 확인할 수 있다.

---

58) 저작자 표시만 의무화, 저작자 표시와 비영리 이용만 허용, 저작자 표시와 창작물 변경 금지, 저작자 표시와 동일조건 변경 허락, 저작자 표시와 비영리 이용 및 동일조건 변경 허락, 저작자 표시와 비영리 이용, 변경금지 등 6가지 종류가 있다(CCKorea - CC라이선스(http://ccl.cckorea.org/about/) 참조).

나. 유럽

유럽연합(EU)은 2015년 5월부터 논의를 시작한 디지털 단일시장(Digital Single Market) 전략에서 저작권법의 현대화를 주요 과제로 꼽았다. 디지털 무역을 통해 유통될 디지털 콘텐츠에 대한 EU 내 각국 법 규제의 차이를 최소화하고 창작자의 권리를 보호하면서 유통을 활발히 할 전략을 모색하려는 의도이다. 2017년 5월 16일 EU는 디지털 시대에 적합한 최신 저작권 원칙을 필요로 한다는 판단하에 유럽연합 집행위원회(European Commission)가 소비자와 제작자가 디지털 사회를 최대한 활용할 수 있도록 하는 입법안을 제출하였다(European Commission, 2017. 5. 16.). 검토된 EU 저작권 원칙은 디지털 단일시장에서의 저작권에 관한 규정과 지침으로 구성된다. 주요 목표는 〈표 5－2〉와 같다.

〈표 5－2〉 디지털 단일시장(Digital Single Market)에서 EU 저작권 원칙의 주요 목표

목표	내용
1) 온라인 콘텐츠에 대한 국경 간 접근 확대	- 유럽 전역의 사람들을 대상으로 이용 가능성을 향상시키고 창작자를 위한 새로운 유통 채널을 제공하여 EU의 문화유산을 최우선시 - 이러한 목표를 달성하기 위해 EU 위원회가 제안한 조치 · 텔레비전 및 라디오 프로그램의 온라인 배포에 유리한 조건 조성 · VoD 플랫폼에서 시청각 작업의 가용성 증대 · 상거래가 아닌 작품의 디지털화 및 보급을 용이하게 함
2) 교육, 연구, 문화 유산에 대해 저작권이 있는 자료를 사용할 수 있는 기회 확대	- EU 법상 대부분의 저작권 예외는 현재 선택사항이며 국경을 넘어서 적용되지 않음. 그중 일부는 오늘날의 기술적 현실에 비추어 재평가 필요 - 제안된 지침의 목적은 디지털 및 국경 간 사용에 초점을 둔 문화유산의 교육, 조사 및 보존 분야의 주요 예외 및 제한 사항에 적용할 수 있는 EU 규칙을 현대화하는 것 - 제안된 지침이 발표하는 필수 예외 사항은 다음과 관련됨: 교습 활동, 텍스트 및 데이터 마이닝, 문화유산 보존
3) 저작권 시장 기능의 향상	- 제안된 조치는 언론 매체, 온라인 플랫폼, 저자 및 공연자의 보상에 대한 온라인 콘텐츠를 위한 더 공정한 시장 창출을 목표로 함 - 제안된 지침의 주요 요소

목표	내용
	· 언론사 관련 또는 '인접' 권리 · 권리 보유자의 강화된 지위를 통해 비디오 공유 플랫폼의 온라인 이용에 대해 협상하고 보상받도록 함 · 새로운 투명성 원칙을 통해 작가 및 공연자에 보상

자료: European Commission(2017. 5. 16.) 재구성.

유럽연합의 개입과 중재가 필요한 부분으로 특히 교육 목적의 디지털 콘텐츠의 국경 간 사용, 과학연구와 관련한 텍스트 데이터 사용, 문화유산의 디지털화와 보존 등을 주요 논의 대상으로 하고 있다. 창작자 측면에서는 디지털 환경 변화에도 창작자와 저작권자에게 공정한 분배가 돌아가도록 보장해야 하며 이를 위해 창작자가 업로드하는 다양한 디지털 콘텐츠 창작물에 대한 합당한 보수 지불 방안 논의가 요구된다. 이용자 측면에서는 다양한 디지털 창작물에 대한 접근을 보장하기 위해 복잡한 승인과정(complex clearance process)을 조정할 필요가 있다.

다. 일본

일본은 2016년 6월 '지식재산추진계획'[59]에 이어 2017년에도 '지식재산추진계획'[60]을 발표하였다. 매해 발표하고 있지만 특히 2016년 계획에 사물인터넷, 빅데이터, 인공지능 등 지능정보기술이 발전할수록 콘텐츠가 창출할 혁신의 가능성을 높게 평가하고 지식재산으로 적극 활용할 수 있는 방안을 모색하고 있다(유계환·김아름, 2016). 이 계획에는 ICT 발전에 대응하는 지식재산 시스템 정비와 관리를 통해 4차 산업혁명 시대를 대비하는 저작권 시스템 구축을 강조하고 있다. 일본의 애니메이션과 만화를 비롯해 영화, 음악, 게임 등의 콘텐츠가 전 세계 시장에 이미 진출

59) 일본 "2016년 지식재산추진계획(2016 知的財産推進計畫)" https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20160509.pdf (검색일: 2017. 7. 18.)

60) 일본 "2017년 지식재산추진계획 (2017 知的財産推進計畫)" https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20170516.pdf (검색일: 2017. 7. 18.)

해 있는 만큼 지속적인 해외 유통을 지원하여 산업 성장의 동력으로 삼는다는 계획도 포함되어 있다. 2017년 계획에는 4차 산업혁명 기반이 될 지식재산 시스템 구축과 함께 문화산업 콘텐츠 역량 강화를 강조하고 있는데, 콘텐츠 해외 진출 확대 및 산업 기반 강화, 영화 산업 진흥, 디지털 아카이브 구축 등의 내용을 담고 있다(권용수, 2017). 인공지능 창작물을 저작권으로 보장하는 지식재산으로 분류할 것인지에 대한 검토는 2016년부터 시작되었으며, 2017년에는 콘텐츠 활용을 촉진할 수 있게 분야별 콘텐츠 권리정보를 집약한 데이터베이스 이용 활성화에 방점을 두었다. 〈표 5－3〉은 2016년과 2017년의 지식재산추진계획을 비교한 것이다.

〈표 5－3〉 일본의 지식재산추진계획(2016~2017)

구분	2016년	2017년
배경	사물인터넷, 빅데이터, 인공지능 등 지능정보기술이 발전함에 따라 콘텐츠를 지식재산으로 적극 활용할 수 있는 방안 모색	4차 산업혁명 기반이 될 지식재산시스템 구축과 함께 문화산업 콘텐츠 역량 강화
목표	1) 4차 산업혁명 시대 지식재산 혁신 2) 지식재산 교육·인재 양성 3) 콘텐츠 산업기반 강화 4) 지식재산 시스템 정비	1) 4차 산업혁명 기반인 지식재산시스템 구축 2) 지역 창생·혁신 촉진 3) 문화산업 콘텐츠 역량 강화
내용	ICT 발전에 대응하는 지식재산 시스템 정비와 관리를 통해 4차 산업혁명 시대를 대비하는 저작권 시스템 구축	콘텐츠 해외 진출 확대 및 산업 기반 강화, 영화 산업 진흥, 디지털 아카이브 구축 등

자료: 유계환·김아름(2016), 권용수(2017) 재구성.

라. 중국

중국 역시 최근 「2017 중국 인터넷 저작권 산업 발전보고」를 발표하였다. 보고서 자체는 공개되지 않았으나 대외경제정책연구원(2017. 4. 26.)에 따르면, 2016년 중국 인터넷 저작권 산업 규모는 5,000억 위안(약 82조 8,500억 원) 이상으로 전년

동기 대비 31.3% 성장하였다. 그러나 디지털 음원의 유료 서비스 소비문화가 아직 정착되지 않는 등 디지털 콘텐츠 활성화 촉진을 위한 지속적 지원이 필요한 상황이다. 2015년 중국 음원 시장 규모는 63억 7,000만 위안(약 1조 551억 원), 2016년 96억 2,000만 위안(약 1조 5,935억 원) 등으로 증가하고 있지만 실제 음원 유통 규모에 비해 아직 유료 서비스 기반의 소비모델이 형성되지 않았다. 텐센트가 보유한 중국 최대 음악 플랫폼 QQ뮤직을 비롯해 음원 플랫폼들은 광고수익이나 연예인 파생상품 판매를 통한 수익창출에만 머물러 있었다. 그러나 지난 2016년 거대 플랫폼을 가진 텐센트와 중국 음원 스트리밍 업체 CMC(Chian Music Corporation)가 합병하면서 플랫폼을 통한 음원 유통산업의 활로를 찾았다고 평가받았다. 음원 저작권을 내세운 폐쇄적 음원 유통 체계가 거대 플랫폼과 결합하여 저작권 독점이 아닌 저작권 라이선스 체계로 전환하고 시장 접근성을 증가시킨 것이다(이정진, 2016. 7. 27.). 이러한 시장의 흐름과는 별도로 중국 정부는 디지털 음악 창작물의 저작권 보호를 강화하는 방향으로 저작권법을 개정하였으며 2015년 발표한 「중국 음악 산업 발전을 위한 몇 가지 의견」에서 음악 창작물에 대한 저작권 침해와 복제 행위를 엄단할 것이며 음원 저작권 보호를 위한 환경을 조성해 음원 정품화를 정착시켜 나가겠다는 정부 지원 방향을 밝혔다(백지연, 2016). 시장에서 저작권 라이선스 체계로 유통 활성화 환경이 조성되는 한편, 제도적으로는 저작권 보호 강화를 통해 디지털 콘텐츠 시장 발전에 균형을 꾀하고 있는 것이다.

마. 한국

우리나라는 2017년 4월 미래창조과학부가 온라인으로 유통되는 콘텐츠 거래의 투명성과 공정성을 확보하고 콘텐츠 유통을 활성화하기 위해 콘텐츠 거래 사실 인증사업을 확대, 실시한다고 밝혔다(지디넷, 2017. 4. 18.). 이 인증사업은 2014년부터 시행하고 있는데, 인증시스템을 통해 유통과정에서 일어날 수 있는 고의적 불법 유통과 정산누락 등을 감시하여 콘텐츠 유통의 공정성을 확보하고자 한 것이다. 지금까지는 웹하드를 통한 유통 중심으로 인증시스템을 활용하였고 최근 방송콘텐츠,

전자책, 애니메이션, 영화 등으로 인증 범위를 확대하고 있다.

미래창조과학부는 2014년 12월 디지털콘텐츠 불공정거래 예방을 위한 '표준계약서'를 만들고 상생협력지원센터를 통해 운영해오고 있다(과학기술정보통신부, 2017. 11. 14.). 국내 디지털콘텐츠산업 규모는 2012년 23조 9,209억 원이었으며 2017년에는 29조 1,575억 원 규모로 성장할 것으로 전망하였다(중기이코노미, 2016. 8. 24.). 콘텐츠의 생산과 유통이 오프라인에서 온라인, 다시 모바일 영역으로 넘어오면서 디지털콘텐츠산업의 규모가 성장하고 있으며, 이에 따라 디지털콘텐츠 거래에서의 불공정사례도 증가하고 있어 이에 대한 대응책으로 표준계약서를 마련된 것이다.[61]

디지털콘텐츠 표준계약서란 미래창조과학부장관이 디지털콘텐츠의 공정한 거래와 유통질서를 확립하기 위해 공정거래위원회, 문화체육관광부, 방송통신위원회와 협의해 마련한 디지털콘텐츠 거래에 관한 표준계약서로 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」 제22조에 따른 디지털콘텐츠 유통질서 확립을 위한 것이다. 구성은 도급, 하도급, 위탁판매, 중개, 퍼블리싱 등 5종으로 되어 있다.

2016년 9월에는 한국저작권보호원이 설립되었다. 이는 "저작권 보호를 위한 시책 수립지원 및 집행과 저작권 보호와 관련한 사항을 심의하며 저작권 보호에 필요한 사업을 수행하여 문화 및 관련 사업의 향상 발전에 이바지함을 목적"[62]으로 한 것이다.

저작권 관련 기술 개발 분야에서는 정부 주도로 2017년 3월 UHD(초고화질) 2D 영상과 3D 영상, 360도 VR(가상현실) 영상 등 여러 기술로 구현된 디지털 콘텐츠의 저작권 보호를 위해 적합한 디지털 워터마킹 기술을 개발할 계획이다(디지털타임스, 2017. 2. 26.). 또한 문화체육관광부는 2017년 말까지 인공지능 기반 창작물에 대

61) 미래창조과학부가 2014년 콘텐츠산업 사업체들을 대상으로 한 불공정거래 조사결과에 따르면, 56.9%의 기업이 불공정거래를 경험한 것으로 나타났다. 디지털콘텐츠의 불공정거래 유형은 ① 규정된 비용을 지급하는 대가로 저작권 포기를 강요 ② 재계약 시 갑이 모든 저작권을 소유 ③ 원작자의 저작권 권리 미인정 ④ 을의 동의 없이 갑의 저작권 등록 ⑤ 동일 내용을 활용한 갑의 일방적인 타 장르 콘텐츠 재생산 등이었다(중기이코노미, 2016. 8. 24.).

62) 한국저작권보호원 설립목적 및 연혁(https://www.kcopa.or.kr/lay1/S1T9C71/contents.do)

한 저작권 보호를 규정하는 개정안을 제시할 계획이며, 그 계획의 일환으로 문체부 산하 한국저작권위원회 역시 영화, 음악, 도서 등 문화 창작 분야에서 인공지능이 활약할 수 있는 분야를 검토하고, 인공지능의 창작 과정에서 발생할 수 있는 저작권 침해 문제와 처벌 규정, 인공지능 창작물의 저작권 귀속주체 및 보호 기간 등을 검토할 계획이다(디지털타임스, 2017. 4. 5.).

2. 인공지능 창작물에 대한 법제도 이슈

현행 저작권법상 저작물은 사람의 사상 감정의 표현이어야 하고, 민법상 권리능력을 부여받으려면 인(人)이어야 하는데 이러한 인(人)에는 자연적 생물로서의 사람인 자연인이거나 일정한 목적을 가진 사람이나 재산의 모임에 법인격을 부여한 법인이어야 한다(민법 제2장 및 제3장). 따라서 현행법상으로는 인공지능의 법적 지위를 정함에 있어 법적으로 포섭되기 어려우며 이는 다른 국가에서도 유사한 상황이다. 다만 인공지능에 의한 창작도 누군가의 노력과 비용이 수반되는 것임은 물론이다. 그 결과물이 문화 발전에 도움이 될 수 있을 것이라는 점도 부인하기 어렵다. 그렇다면 저작권법에서 관심을 가지고 인공지능의 창작을 장려하는 것이 법목적에 부합하지 않은지 검토가 필요하다. 다음에서는 이와 관련하여 주요국의 논의를 살펴본다.

가. 미국

기술적 진보에도 불구하고 미국 내에서 인공지능에 대한 입법은 아직 포괄적으로 이루어지지 않고 있다. 드론, 자율주행자동차, 의료 소프트웨어 등 약한 인공지능을 이용한 특정 장치나 기기에 관한 규제 입법이 부분적으로 이루어졌거나 검토되고 있는 정도이다(윤혜선, 2016). 최근 관련 논의에 속도를 내고 있는데, 초기에는 학계 및 기업이 시작하였지만 정부차원에서 추진되는 프로젝트로 주도권이 넘어가고 있는 것이 특징이다.

행정부는 2016년 5월 3일 인공지능에 관련된 연방 활동을 조정할 수 있도록 기계

학습 및 인공 지능에 관한 새로운 국가과학기술위원회(National Science and Technology Council, NSTC) 소위원회를 구성한다고 발표하였다(Felten, 2016. 5. 3.). 이후 소위원회는 2016년 10월 「인공지능 국가 개발 연구 전략」과 「인공지능의 미래를 위한 준비」 등의 보고서를 발표하고, 이어서 2016년 12월에 「인공지능과 자동화가 경제에 미치는 영향」이라는 제목의 보고서를 발표하여 초연결·초지능 시대를 준비하기 시작하였다. 이 보고서들은 인공지능의 경제적 효과와 공공성, 윤리적 문제들을 포괄적으로 다루고 있고 법적 지위에 대해서도 검토하고 있다는 점이 주목할 만하다(Federal Register, 2016. 6. 27.).

특히 미국 도로교통안전국(The National Highway Traffic Safety Administration)은 2016년 2월 구글의 자율주행차 인공지능 시스템을 연방법 체제에서 '운전자'로 인정할 수 있다고 밝힌 바 있다(Reuters, 2016. 2. 10.). 인공지능이 운전자라는 법적 주체성을 인정받는다면 이는 권리의무의 행위 주체로 인정될 여지가 있다.

나. 유럽

EU에서는 인공지능의 법적 지위를 전자인간으로 규정하는 것을 고려하는 결의안을 채택하는 등 가장 급진적으로 인공지능의 발전에 대응하고 있다. 2014년 로봇법(Robot Law) 프로젝트를 진행하여 로봇규제가이드라인(Guidelines on Regulating Robotics)를 제정한 바 있으며(차상육, 2017), 유럽의회 법무위원회(the Committee on Legal of the European Union)에서는 최근 발전하는 로봇과 인공지능 문제에 따른 윤리적 문제들을 검토하고자 2015년에 실무자 그룹(working group)을 마련하여 법을 적용하기 위한 방안을 마련하였다(Nevejans, 2016). 2016년에는 로봇에 대하여 EU법을 적용하는 방안을 놓고 초안 보고서가 발표되기도 하였다(European Parliament, 2016. 5. 31.). 이 보고서에서는 지능형 자율 로봇의 책임능력을 인정하는 방향으로 언급하고 있다. 구체적으로, ① 센서를 통해 자율성을 지니고(acquire autonomy through sensors) ② 주변에서 정보를 교환하며 정보를 분석하며(trades and analyses data) ③ 스스로 학습하고(self-learning) ④ 물리적 도움을 받으며(has a physical

support) ⑤ 주변 환경에 따라 행동을 하는(adapts its behaviours and actions to its environment) 특성을 지닌 로봇을 지칭한다.

로봇에 법인격을 부여하려면 '법적인' 생명을 부여할 수밖에 없다(grant a legal life)(Nevejans, 2016). 그렇다면 로봇에 부여되는 법적인 의미의 주체는 로봇 뒤에 숨겨진 법적 행위자인 물리적 인간이 진실된 주체가 되거나 혹은 로봇 그 자체가 법적인 주체가 되어야 한다(Nevejans, 2016).

보다 직접적으로 인공지능의 법적 지위가 2017년 1월 유럽연합 법무위원회에서 정해졌다. 본 위원회에서는 향후 입법 시 AI의 법적 지위를 '전자인간(electronic persons)'으로 규정하는 것을 고려하도록 하는 내용의 결의안을 통과시켰다(강태욱, 2017. 1. 23.). 이는 인공지능에 대하여 법적 지위를 규정하는 것을 고려하도록 하는 수준이기에 법적 강제력은 없으나 인간에 비견할 만한 법적 지위를 논했다는 점에서 의미를 갖는다. 이번 결의안에 따라 종래 자연인과 법인 외 새로운 법인격이 도출될 가능성이 높아진 것으로 보인다(차상육, 2017).

하지만 전자인간의 법적 권한과 의무의 범주가 아직 명확하게 정하여진 것은 아니다. EU법 내에서 전자인간이라는 새로운 법인격의 법적 지위를 어느 정도 선까지 인정하여야 할 것인지에 대해서는 추후 더 많은 논의가 필요한 상황이다.

다. 일본

일본에서는 아직 법인격을 인정할 정도로 구체화된 내용은 없다. 하지만 2016년 지식재산추진계획을 통해 인공지능 창작물의 저작권 문제를 검토하는 등 인공지능의 법적 쟁점을 검토하기 위하여 정부 차원의 대응이 진행 중이다. 일본 지식재산전략본부는 인공지능을 비롯한 첨단 기술의 고도화에 대비한 새로운 지식재산전략인 '2016년 지식재산추진계획'을 결정한 바 있다(권용수, 2016). 본 추진계획에 따르면 일본 정부는 2016년 지식재산추진계획을 통하여 인공지능의 창작물에도 저작권을 인정하는 법 정비를 실시한다고 한 바 있다.[63] 2016년 1월부터 지식재산전략본부

63) 영국은 1988년 저작권법에서 컴퓨터 산출 저작물(computer-generated works)에 대해

‘차세대 지식재산 시스템 검토위원회’를 통해 AI 창작물에 대한 권리 인정 및 침해 대응 등에 대한 검토를 실시하고 4월 8일 AI 창작물을 인간의 창작물과 달리 볼 필요가 없으며 법적으로도 역시 보호할 필요가 있다는 보고서를 공개하였다.

라. 한국

2017년 2월 정부는 4차 산업혁명 시대를 견인할 인공지능과 그 응용 분야의 선제적 규제개선을 위하여 지능정보사회 기본법 제정을 추진하기로 하였다(미래창조과학부, 2017. 2. 17.). 현재 지능정보사회에 대한 방향과 일관된 제도의 기준 등을 위한 기본법이 부재하고 인공지능의 안전성과 사고 시 법적책임 등 법제도 이슈가 등장하고 있다. 그러나 정부 차원의 정비방향 제시 등이 미흡한 점을 감안하여 ① (가칭) 지능정보사회 기본법 제정을 추진하고 ② 인공지능 확산 관련 핵심 법제도 이슈(인공지능 안전성, 사고 시 법적책임, 기술개발 윤리, 데이터·지재권 보호) 관련 정비방향을 제시하기로 한 것이다(미래창조과학부, 2017. 2. 17.).

국가지식재산위원회에서도 미래 지식재산 이슈에 대비하고자 동 위원회에 ‘차세대 지식재산 특별전문위원회’를 설치하고 본 위원회에서 인공지능, 빅데이터 등 신기술 IP의 보호 체계를 정립하고 IP 이슈(인공지능 창작물의 권리인정 문제 등)에 선제적으로 대응하기로 한 바 있다(미래창조과학부, 2016. 12. 22.).[64]

창작에 필요한 조치를 한 자에게 저작권이 귀속된다고 규정한 바 있다.

64) 미래창조과학부 보도자료(2016. 12. 22.)에 따르면 2017년 지식재산 주요 정책이슈는 다음과 같다.

정책이슈	관계부처
1. 특허침해 손해배상액 확정에 있어 기여도 산정 기준 확립	특허청
2. 지식재산집약산업의 지식재산 활용을 위한 전문기관(산업별) 육성	복지부, 미래부
3. 직무발명 공동발명자의 지분율 관련 권리 보호방안	특허청
4. 정부 R&D 수행단계에서의 IP-R&D 확대 방안	미래부, 특허청
5. 정부 R&D 국외 특허 활성화 방안	미래부, 특허청
6. 인공지능 기술 및 산업 관련 지재권 심층분석 및 대응방안	미래부, 특허청
7. 사적복제보상금제도 도입방안	문체부

제 5 절 ICT 고도화에 따른 법제도 이슈

이번 절에서는 초연결사회의 기술 환경으로 인한 법·제도 이슈를 살펴본다. 크게 유통, 이용, 창작 형식의 변화에 따른 이슈를 살펴본다.

1. 매체 기술의 발전과 유통·이용 형태의 변화

가. 사적 이용과 저작권 제도

1) 사적복제에 대한 저작권 제한

저작권법 제30조에 따르면 공표된 저작물을 영리를 목적으로 하지 아니하고 개인적으로 이용하거나 가정 및 이에 준하는 한정된 범위 안에서 이용하는 경우에는 그 이용자는 이를 복제할 수 있다. 이 규정에 의하여 타인의 저작물을 자유이용하는 자는 그 저작물을 번역·편곡 또는 개작하여 이용할 수도 있으며(저작권법 제36조 제1항), 출처의 명시의무도 면제된다(저작권법 제37조 제1항). 이러한 법 조항은 먼저 저작물의 이용이 개인적 또는 가정과 같은 한정된 범위에서만 이루어지는 것을 요건으로 하고 있고 대외적인 이용을 전제로 한 것이 아니기 때문에 출처명시를 할 필요성가 없고, 또한 현실적으로도 출처명시의무 부과는 타당성이 없다고 본 것이다(오승종, 2015). MP3를 복제하여 핸드폰에 넣고 다닌다거나 영상저작물을 VCR로 복제하는 것, 개인감상 목적으로 촬영하는 것 등이 모두 복제에는 해당하지만 이 조항에 근거하여 면책된다.

복제권은 저작재산권에서 중심적인 권리이고 사적복제 조항은 이를 포괄적으로

정책이슈	관계부처
8. 국가공무원 및 지방공무원의 지식재산 전담인력 전문성 강화 방안	인사혁신처
9. 토종식물자원의 재평가를 통한 창조적 활용 방안	미래부, 환경부, 해수부, 복지부
10. 공적개발원조사업 연계를 통한 신지식재산 개발 및 활용 방안	외교부, 농림부, 환경부, 해수부, 산림청

제한하는 규정이므로 저작권자의 이익을 지나치게 제약하지 않도록 유의할 필요가 있다. 사적복제 조항이 마련될 당시에는 지금과 같이 복제가 용이해진 상황을 고려하지 못하였는데, 특히 디지털 환경 네트워크 기술의 발전으로 권리자의 이익이 크게 위협받게 되었다. 이에 따라 저작권자 보호를 위해 사적복제 조항을 조정할 필요가 제기된다.

애초에 사적복제는 개인 혹은 가정 등 한정된 범위에서 타인의 저작물 이용을 제한하는 것으로, 저작권자의 경제적 이익을 저해하지 않으면서 일일이 이용허락을 받기 어려운 현실적 제약을 고려한 조항이다. 그러나 기술 환경의 변화로 이 전제가 성립되지 않게 되었다. 복제기기는 흔해졌고 원본과 동일한 품질의 복제물을 누구나 쉽게 만들 수 있게 되었다. 때문에 저작권자에게는 경제적 대가없는 자유로운 이용으로 직업군의 존립을 위태롭게 하는 위협이 되었고, 이는 헌법상 기본권 침해 및 국제협약 위반 가능성을 내포하고 있다.

2) 불법 다운로드와 사적이용

최신 개봉 영화 파일이나 방송프로그램 파일을 웹하드 등에서 어렵지 않게 찾을 수 있다. 이때 인터넷에서 불법 저작물을 다운로드하는 것은 저작권 침해에 속한다. 저작권자의 경제적 이익을 침해할 수 있기 때문이다. 실제로 2008년에 원본이 불법이라면 사적복제에 관한 제30조를 적용할 수 없다며 “다운로더 입장에서 복제의 대상이 되는 파일이 저작권을 침해한 불법파일인 것을 미필적으로나마 알고 있었다면 위와 같은 다운로드 행위를 사적이용을 위한 복제로서 적법하다고 할 수는 없다”는 판결이 나온 적이 있다(서울중앙지방법원 2008. 8. 5. 선고 2008카합968 판결).

3) 엄격한 해석과 이용의 장애

저작권법 제30조와 관련해서는 저작재산권자의 이익을 고려하여 엄격하게 해석·운용할 필요가 있음에도 우리나라는 사적복제에 해당하면 아무런 대가 없이 자유로운 이용을 쉽게 허용하는 경향이 있다. 이는 오늘날과 같은 저작권 환경에서 저작권자에게 가혹한 결과를 가져올 수 있다. 사적복제는 아날로그 영역에서는 그 인정근

거에 맞게 적절하게 적용될 수 있지만 디지털 환경에서 원본과 같은 수준으로 대량 복제가 가능한 상황에서는 법 적용의 적합성을 면밀하게 살펴볼 필요가 있다(이대희, 2010).

그러나 엄격한 해석이 이용의 장애를 가져올 수도 있다. 서비스 제공자가 플랫폼을 만들어 이용자에게 특정 저작물을 선택해서 저장하도록 서비스한다고 하였을 때, 복제하는 실질적 주체는 이용자가 된다. 또 서비스 제공자와 개인 이용자 간 통신의 형태로 파일을 주고받은 것으로 볼 수 있다. 어떤 경우이든 서비스 제공자는 처벌 대상에서 벗어날 여지가 생긴다. 그리고 이용자는 기술적으로 가능한 서비스를 이용하는 데에도 심리적 제약이 발생할 수 있다. 결과적으로 엄격한 해석이 이용자의 이용을 제약하는 장애가 되는 것이다.

4) 새로운 균형의 모색 - 보상금 제도의 검토

디지털 환경에서 저작권자의 권한을 해하지 않는 범위에서 사적 복제 조항을 해석하는 한편, 엄격한 법 해석으로 이용자의 콘텐츠 이용을 저해하는 경우를 최소화하기 위한 균형 있는 대안이 필요하다. 이와 관련한 절충안으로 유럽은 일찍이 사적 복제 보상금 제도를 도입하였다. 기술 발전으로 사적 복제 면책 조항 자체를 삭제해야 한다는 주장에 대하여 사적 복제를 허용하는 대신 보상금을 징수하는 것이다. 지금은 대부분의 유럽연합 회원국과 미국, 일본을 비롯하여 남미와 아프리카까지 40여 개국이 넘는 나라에서 사적 복제 보상금 제도를 도입, 운영하고 있다(이상정·이영록·최진원, 2016). 보상금 제도가 완벽한 대안이라고 할 수 없겠지만 가급적 자유로운 복제허용을 통해 이용자의 자유로운 정보 교환과 창작 활동에의 참여를 보장해주면서 저작권자에게 최소한의 보상을 하도록 조정한 대안으로서 현재 가장 널리 활용되고 있다.

나. 유형물 논리의 종말 - 클라우드 환경과 링크

1) 링크의 가치와 법적 판단

과거 지식재산권은 지식재산이 체화된 유형물을 중심으로 이해관계를 조정해 왔

으나 ICT가 소유와 유통 형태를 변화시켰다. 콘텐츠의 디지털화와 함께 물질의 직접적 소유가 스트리밍과 링크 형식으로 대체되고 있다.

링크는 인터넷의 기본 속성이다. 세상을 바꾼 인터넷의 중심에는 하이퍼링크(hyperlink, '링크')가 있기 때문이다. 그러나 모든 매체기술이 그러하였듯이 링크 역시 불법적 이용에 악용될 소지가 있다. 얼마 전까지 불법저작물에 대한 링크나 이를 모아놓은 사이트를 쉽게 발견할 수 있었는데, 이때 링크 형식 때문에 사이트 운영자가 저작물을 업로드하였다고 보기 어려운 문제가 있었다. 링크는 경로 정보를 줄 뿐이라고 생각할 수 있기 때문이다.

초연결사회의 커넥티드 환경에서 이용자는 이제 접속과 공유만으로도 충분한 만족을 느낄 수 있으며, 서버에 업로드 되어 있는 사이트와 링크로만 정리된 사이트의 차이를 느끼지 못한다. 제도와 산업 현실 역시 이를 반영할 필요가 있다. 그러나 우리나라 법원은 여전히 링크에 대하여 과거와 크게 다르지 않은 입장을 보이고 있다. 심층링크(deep link)나 직접링크(direct link)가 복제나 전송이 되지는 않는다고 하였으며(대법원 2009. 11. 26. 선고 2008다77405 판결), 휴대전화 문자메시지를 통한 링크나(대법원 2015. 8. 19. 선고 2015도5789 판결) 모바일 애플리케이션에서 인터넷 링크와 유사하게 제3자가 관리·운영하는 모바일 웹페이지로 이동하도록 연결하는 경우에도 저작권 침해의 정범은 아니라고 보았다(대법원 2016. 5. 26. 선고 2015도16701 판결).

2) 새로운 균형의 모색 - 불법 링크에 대한 제재

링크에 대하여 아무런 책임을 지우지 않는 것은 오늘날 매체 환경에서 재고될 필요가 있다. 이용자 입장에서는 서버에 업로드된 콘텐츠를 이용하는 경우와 링크로 연결된 콘텐츠를 이용하는 것의 차이를 인식하지 못한다는 점에서 업로드와 링크를 전혀 다른 사항으로 볼 수 없다. 예외적인 경우로 국한해야 한다는 전제는 필요하며 링크와 관련하여 마치 저작물을 직접 업로드한 것과 동일한 법적 판단을 내려야 하는 상황을 사전에 배제할 필요가 없다고 본다. 중장기적인 시각에서 링크의 법적 판단 자체를 재고할 시점이 되었다.

다음으로 저작권 침해가 아니라고 하더라도 타 법에 의한 균형 조정 방법을 찾아보는 것을 제안한다. 불법저작물에 대한 링크를 통하여 사람들을 모으고 여기에서 막대한 수익을 올리는 사업모델은 대부분이 문제가 있다고 인식한다. 법 제도가 사회의 인식을 반영해야 한다는 측면에서 보더라도 이를 합법적 비즈니스모델로 인정해주는 것은 적절치 않기 때문이다. 우선 불법행위에 의한 손해배상책임을 물을 수 있는지에 대한 검토가 필요하다(최진원, 2017). 불법행위의 성립은 반드시 저작권 등 법률에 정해진 엄밀한 의미에서의 권리 침해의 경우에만 제한하지 않고, 법적으로 보호할 가치가 있는 이익이 위법하게 침해된 것으로 충분하다(서울중앙지방법원 2008. 11. 14. 선고 2007가단70153 판결).

다음으로 부정경쟁방지법에 의한 통제를 고려해볼 수 있다. 2014년 부정경쟁행위의 보충적 일반조항인 차목을 신설하였다. “타인의 상당한 투자나 노력으로 만들어진 성과 등을 공정한 상거래 관행이나 경쟁질서에 반하는 방법으로 자신의 영업을 위하여 무단으로 사용함으로써 타인의 경제적 이익을 침해하는 행위(제2조 제1호 차목)”를 부정경쟁행위로 규정하고 있다. 이 규정은 지식재산권 개별법의 보호요건이나 침해요건 충족 여부가 모호했던 영역에 대하여 보완재의 역할을 할 것으로 기대되었다(최진원 외, 2017).

물론 이와 같은 통제가 링크에 대한 위축효과를 일으키지 않도록 유념해야 한다. 일본에서는 2016년 3월 이후 문화청의 「문화심의회법제·기본문제소위원회」에서 리치사이트(リーチサイト)에 대한 입법적 조치를 적극적으로 검토하고 있다. 여기에서 리치사이트를 사이트형과 앱형으로 분류하고(文化審議會著作權分科會法制‧基本問題小委員會, 2016), 악질성·대량성·계속성 등이 있는 경우에만 규제하는 방안을 제언하고 있다(知的財産戰略本部檢証‧評価‧企畵委員會, 2016). 이들을 ‘긴급히 대응할 필요성이 높은 행위 유형의 요소’라고 하였는데, 표현의 자유와의 균형을 고려하여 과도한 규제가 되지 않도록 주의하고 있음을 보여준다.

2. 저작물 이용시 권리처리 방법의 모색 - 롱테일과 프로슈머

가. 롱테일과 고아저작물

1) 롱테일과 고아저작물

초연결사회의 매체기술 발전이 가져다준 장점 중 상징적인 두 가지 단어로 롱테일과 프로슈머를 꼽을 수 있다. 과거에는 시장 수요가 어느 정도 확보되지 않으면 해당 콘텐츠는 절판되어 시장에서 사라졌다. 하지만 디지털 환경 덕분에 재고나 물류비용이 감소하였고 그로 인해 니치마켓이 활성화되는 현상으로 이어졌다. 이미 시장에서 사라진 콘텐츠들이 디지털 콘텐츠로 다시 선보이기도 한다. 이러한 롱테일 현상은 초연결사회의 긍정적 현상이라고 볼 수 있다. 롱테일 시장에서의 어려움은 저작권 처리 문제일 것이다. 저작권료가 비싸서가 아니라 해당 저작물의 저작권자를 찾아 이용허락을 받는 데 드는 비용이 크기 때문이다.

2) 법정허락 제도의 한계

저작권자를 찾을 수 없는 이른바 고아저작물의 이용을 위해 법정허락 제도의 정비가 논의되어야 한다. 1957년에 제정된 국내 저작권법은 처음부터 저작물의 저작자를 알 수 없는 경우에 강제허락을 인정하였다. 한국저작권위원회의 심사를 거쳐 승인을 받아야 이용할 수 있으므로 '강제허락'에 해당한다(하상익, 2003).[65] 연혁으로 살펴보면 1986년 '공표된 저작물'로 대상을 한정하였고, 2000년 개정에서는 '상당한 노력'의 요건을 대통령령이 정하는 기준에 해당하는 상당한 노력으로 구체화하였다(최진원, 2011).[66]

법문상으로는 법정허락의 절차는 문화체육관광부 장관이 주관하게 되어 있으며 현재 한국저작권위원회가 업무 위탁을 받아 수행하고 있다(저작권법 제130조). 고아

---

65) 저작재산권자와 저작물 이용 희망자 사이에 협의가 성사되지 못하였을 때, '권한 있는 제3자'가 보상금을 받는 대가로 해당 저작물의 이용 허락을 강제하는 것, 혹은 그렇게 하여 강제로 의제된 허락 자체를 의미한다(이영록·최진원, 2010).

66) 2006년에는 외국인 저작물을 대상에서 제외하였다.

저작물을 이용하려면 먼저 승인신청을 하고 심사를 받는다. 심사 후 승인통지를 받으면 바로 보상금을 공탁하고 해당 저작물을 이용하면 절차는 끝난다. 그러나 이러한 절차가 결코 수월하게 끝나는 것이 아니며 저작물 하나를 이용하기에는 복잡하고 많은 시간을 필요로 한다는 점에서 크게 효율적이지 않다.

나. 프로슈머와 권리처리

1) 정보 발신자로서의 일반 이용자

인터넷은 누구나 정보의 발신자가 될 수 있는 환경을 만들었다. 과거 저작권에 문외한이었던 일반인들은 이제 저작권법에 대해 어느 정도 이해가 필요한 상황이 되었다. 이용자와 창작자의 경계가 모호해지는 소위 프로슈머이자 정보의 발신자가 되면서 이용자 개개인은 저작권 권리처리에 직접 관여하게 된 것이다. 뉴스 페이지 링크를 블로그에 가져오거나 시 한 편을 적어서 올리는 것으로도 저작권 침해 논쟁에 휘말릴 수 있다.

그러나 저작권법은 1957년 제정 이후 최근까지 교육 콘텐츠로 다뤄진 경우가 거의 없었다. 최근에 초등학교 교과서에 저작권 관련 사항을 삽입하거나 일반인 대상의 저작권법 교육 서비스[67]가 운영되는 등 그 대응방법이 모색되고 있다.

2) 집중관리와 저작권 거래소

또 다른 문제는 저작권 제도에 대하여 충분한 알고 있는 이들조차도 합법적 이용을 위한 권리처리가 쉽지 않은 경우가 많다는 것이다. 사용료를 지불하고 싶지만 어디에 어떻게 지급하면 되는지 알기 어려운 경우가 종종 있기 때문이다. 예를 들어, 스스로 제작한 동영상(UCC)에 음악 배경을 넣고자 할 때, 작곡가와 작사가, 편곡자는 물론, 가수와 연주자, 음반제작자의 허락을 받아야 한다. 하지만 이들의 연락처를 알 방법은 현실적으로 쉽지 않다.

67) 한국저작권위원회 원격평생교육원(http://edulife.copyright.or.kr/).

3) 권리처리방법의 대안

이에 대한 대안으로 집중관리제도를 활성화하는 방안을 제안한다. 저작권 이용허락은 거래비용으로 인하여 시장 실패가 나타나기 쉬운 시장이다. 저작권사용료보다 거래비용이 높은 경우를 해결하기 위한 현실적 대안으로 집중관리가 역할을 수행해 오고 있다. 권리자 입장에서는 저작물 이용을 일일이 확인하고 사용료를 청구하는 수고를 덜어줄 수 있고 이용자 입장에서도 권리자를 탐색하여 교섭하고 개별적으로 사용료를 납부하는 불편을 줄일 수 있다.

우리의 저작권법은 저작권 집중관리와 관련하여 법문에서 저작권위탁관리업으로 표현하고 있으며, 저작권신탁관리업과 저작권대리중개업으로 구분하여 규정하고 있다. 간단한 신고만으로 가능한 대리중개업은 수백 개 업체가 영업하고 있지만,[68] 문화체육관광부 장관의 허가를 받아야만 업무 수행이 가능한 위탁관리업의 경우에는 현재 단지 13개 단체만이 있다(안태숙 외, 2013).

우리나라는 상대적으로 집중관리단체의 역사가 일천하고 신뢰도 역시 높지 않다. 그 결과 신탁률도 높지 않아서 음악저작권과 음악실연권을 제외하면 대표단체라고 칭할 만한 사례가 매우 제한적이다. 때문에 집중관리단체를 통한 권리처리 역시 현재로서는 완전한 대안이 되지 못한다.

저작권을 쉽고 편리하게 권리처리할 수 있는 저작권거래소가 정부 차원에서 기획되었고 적지 않은 투자가 이루어진 상태이지만, 앞으로는 마이크로라이선스 등 이용자가 편리하게 이용허락을 받을 수 있는 방안을 좀 더 모색해 보아야 할 것이다. 중장기적으로는 일부 권리에 대해서 권리의 배타성을 약화시키는 방법도 고려해 볼 수 있다.

68) 실제로 운영 중인 대리중개업자는 288개로 조사되었다(안태숙 외, 2013).

3. 공정이용에 대한 재고

가. 공정이용의 범위 확대

새로운 창작을 위해서는 선행 저작물을 이용할 수 있어야 한다. 타인의 저작물을 이용하여 새로운 창작, 그리고 문화 발전이 이루어지기 때문이다. 저작권법으로 보호를 받는 저작자도 자신의 저작물을 선인들이 쌓아 놓은 문화유산의 바탕 위에서 창작하였을 것이다. 문화 발전을 최종 목적으로 하는 저작권법은 권리의 보호 못지 않게 공정하고 원활한 이용에 관심을 가진다. 시장실패 등의 사유로 이용허락을 받을 수 없어 저작물 이용의 필요성이 인정된다면 이를 공정이용의 형태로 포섭할 수 있어야 한다.

우리나라에는 저작권법 제23조 이하에서 저작재산권을 제한하는 규정을 가지고 있다. 그리고 한미 FTA 논의 과정에서 권리자의 보호 강화에 대응하고 이용자 입장을 대변하여 2011년 이른바 '공정이용 일반조항'을 도입하였다(저작권법 제35조의 3). 당시 기술의 발달과 저작물 이용환경의 변화로 저작물 이용이 다양화되고 있어 개별적 저작재산권 제한 규정만으로는 구체적인 상황에 대응하기 어려울 수 있고, 저작권 보호 기간의 연장 등 저작권 보호가 강화됨에 따라 상대적으로 저작물 이용자의 지위가 저하될 수 있다는 우려에 대응하기 위하여 도입된 것이다.

그리고 2016년 동 조항을 개정하였는데, 공정이용의 범위를 확대하는 방향으로 문구 수정이 이루어졌다. 즉 '포괄적 공정이용'에 대한 저작물 이용 목적상의 제한('보도·비평·교육·연구 등')을 삭제하고, '포괄적 공정이용' 판단 시 고려사항인 '영리성 또는 비영리성 등 이용의 목적 및 성격'에서 '영리성 또는 비영리성'을 삭제하였다(국회검토보고서, 2013). 이러한 목적에 국한하지 않고 공정이용을 인정할 수 있다는 취지이다.

나. 공정이용 여부의 판단 기준

일반 조항의 도입으로 공정이용 해당 여부를 최종적으로 법원이 판단하게 되었다.

공정이용 여부는 DRM 등 기술적 요소를 포함하여 다양한 요인을 종합적으로 판단하게 된다. 그러나 그 기준은 모호하여 공정이용 여부를 미리 판단하는 것이 어렵다. 공정이용 조항은 미국 저작권법 제107조의 내용을 거의 그대로 가져온 것인데, 미국에서도 공정이용의 기준이 명확하게 제시되지는 못하고 있다. 다만 미국 대법원은 공정이용을 판단할 때 첫 번째 고려 사항인 이용의 목적 및 성격(The Purpose and Character of the Use)을 가장 중요하고 결정적인 사항으로 보고 있다는 점은 공정이용 조항에 새로운 창작을 도모하는 역할을 기대하고 있음을 살펴볼 수 있게 한다.

미국 대법원은 구체적으로 새로운 작품이 단순히 원저작물의 대상을 대체하는 것인지 아니면 더 큰 목적 또는 다른 성격을 수반하며 새로운 표현, 의미 또는 메시지를 통해 원창작물을 변형시키거나 새로운 것을 더하는지, 즉 새로운 작품이 변형적(transformative)인지를 판단의 기준으로 제시하였다. 이는 원저작물이 이차적 이용의 재료로 이용되면서 새로운 정보, 미학, 통찰력을 통해 원저작물의 가치를 더해 줘야 한다는 뜻이라고 설명되기도 한다.[69]

우리나라 법원의 판례는 아직 충분히 축적되지 못한 상태이기 때문에 앞으로 많은 연구와 더불어 이해관계자의 의견을 수렴하여 기준을 마련해 나가야 한다. 공정이용의 이론적 근거는 공평의 원칙이다. 현대의 저작자가 저작물을 창작하는 것은 완전한 무에서 유를 창조하는 것이 아니라 처음에는 저작자도 역시 이용자의 입장에서 자기보다 앞선 저작자들의 창작물을 보고, 배우고, 느낀 후에 자신의 저작물을 창작한 셈이기 때문에 역시 마찬가지로 자신의 저작물도 다른 사람이 공정하게 이용하는 것을 허용하는 것이다(최상필, 2012). 공정이용의 기준을 마련해 나가는 과정에서 이용은 곧 새로운 창작을 위한 것이라는 정책적 고려가 반영되어야 한다. 프로슈머의 창작을 장려하려면 특히 공정이용이 되는 변형적 이용과 2차적저작물작성권의 침해 사이의 기준을 마련하는 것이 중요하다(이해완, 2012; 문일환, 2013;

69) Blanch v. Koons, 467 F.3d 244 (2d Cir. 2006).

Leval, 1990).

4. 인공지능 기반 창작물과 저작권 이슈

초연결사회의 진화를 상징하는 인공지능 기술 수준은 아직 약한 인공지능 단계이지만 그 파급효과는 이미 현실이 되고 있다. 저작권 차원에서 인공지능에 대한 쟁점은 크게 인공지능 학습과 창작 단계에서 타인의 저작물을 이용하는 문제와 그 결과 창작된 저작물에 대한 법적 보호 문제로 나눠볼 수 있다.

가. 인공지능 창작 과정에서의 저작물 이용

1) 학습을 위한 데이터 이용과 저작권

(1) 인공지능 학습을 위한 저작물의 이용

인공지능을 활용하려면 인공지능의 학습을 위한 데이터가 필요하며, 이때 인공지능이 처리하는 데이터 중에 저작물이 포함될 수 있다. 만약 저작물이 포함된 데이터라면 수집되어 저장되고 공유 또는 분석을 위하여 전달되는 과정에서 복제권, 공중송신권 침해 등이 문제가 될 수 있다(김병일, 2017). 데이터에서 원하는 정보를 추출하는 과정에서 일시적 복제 문제도 제기된다. 나아가 학습을 위한 데이터셋을 만드는 과정에서 동일성유지권 침해와 같은 저작인격권 문제도 발생할 수 있다. 해석상으로 '부득이한 사유'의 범위를 조정할 여지는 있으나 저작재산권과 같은 공정이용 일반조항은 현행법상 마련되어 있지 않다는 점을 고려해야 한다. 향후 제도적으로 공정이용의 범위를 넓혀주거나 법정허락의 대상으로 관련 조항을 신설하는 방안도 논의해 볼 수 있을 것이다.

〈표 5－4〉 학습용 데이터셋 생성과정에서 제기될 수 있는 저작권법 이슈

저작권법

제12조(성명표시권) ①저작자는 저작물의 원본이나 그 복제물에 또는 저작물의 공표매체에 그의 실명 또는 이명을 표시할 권리를 가진다.

②저작물을 이용하는 자는 그 저작자의 특별한 의사표시가 없는 때에는 저작자가 그의 실명 또는 이명을 표시한 바에 따라 이를 표시하여야 한다. 다만, 저작물의 성질이나 그 이용의 목적 및 형태 등에 비추어 부득이하다고 인정되는 경우에는 그러하지 아니하다.

제13조(동일성유지권) ①저작자는 그의 저작물의 내용·형식 및 제호의 동일성을 유지할 권리를 가진다.

②저작자는 다음 각 호의 어느 하나에 해당하는 변경에 대하여는 이의(異議)할 수 없다. 다만, 본질적인 내용의 변경은 그러하지 아니하다. 〈개정 2009.4.22.〉

1. 제25조의 규정에 따라 저작물을 이용하는 경우에 학교교육 목적상 부득이하다고 인정되는 범위 안에서의 표현의 변경
2. 건축물의 증축·개축 그 밖의 변형
3. 특정한 컴퓨터 외에는 이용할 수 없는 프로그램을 다른 컴퓨터에 이용할 수 있도록 하기 위하여 필요한 범위에서의 변경
4. 프로그램을 특정한 컴퓨터에 보다 효과적으로 이용할 수 있도록 하기 위하여 필요한 범위에서의 변경
5. 그 밖에 저작물의 성질이나 그 이용의 목적 및 형태 등에 비추어 부득이하다고 인정되는 범위 안에서의 변경

더불어 실무자들이 저작권과 그 매체의 이용허락을 혼동하는 경우가 있는데, 이는 교육과 홍보가 필요하다. 저작권에 대하여 대가를 지불하고 이용허락을 받은 콘텐츠라고 하더라도 모든 이용을 허락하는 것은 아니므로 그 계약조건을 상세하게 살펴보아야 한다. 계약조건을 위반한 경우에는 계약위반으로 인한 손해배상 책임뿐 아니라, 경우에 따라서는 저작권 침해로 인한 책임을 부담할 수도 있다(박성호, 2014).

(2) 데이터셋 제작과 저작재산권

데이터셋을 만들어 공개하는 것은 더욱 복잡한 저작권 문제에 관심을 가져야 한다. 인공지능 내부에서 이용되는 것과 달리 외부에 공개하는 학습용 데이터셋은 원저작자의 저작권을 침해할 가능성이 높아진다. 상대적으로 공정이용에 해당할 가능성이 작아진다는 의미로도 이해할 수 있다.

반면 데이터셋 자체가 저작권법의 보호를 받을 가능성도 크다. 따라서 제3자가 공개한 데이터셋을 인공지능 학습에 사용하는 경우, 데이터셋 제작자에 대해서도 권리처리가 필요할 수 있다는 점을 주의해야 한다. 먼저 DB 제작자의 권리가 있다. 개별 저작물에 대한 이용이 아닌 데이터셋을 이용하는 것이라면 DB로서의 법적 보호도 고려해야 한다. 개별 데이터로서는 창작성이 없어 저작물에는 해당하지 않는 경우에도 수집 및 처리 과정에서 인적·물적인 투자를 하여 체계적으로 배열 또는 구성되었고, 이용자들이 개별적으로 그 소재에 접근하거나 소재를 검색할 수 있다면 저작권법상 데이터베이스로 보호될 수 있다.

창작성이 없더라도 인공지능이 데이터베이스의 전부 또는 상당한 부분을 복제·배포·방송 또는 전송하는 경우 데이터베이스 제작자의 권리를 침해하게 된다(저작권법 제93조). 예컨대 정보 또는 사실의 분석(collation of facts)을 제공하는 행위는 데이터베이스 제작자의 권리 침해가 될 수 있다. 유사한 법리에 따라 콘텐츠산업 진흥법에 따른 보호 가능성도 있다.

그 밖에 가공된 정도에 따라 데이터셋 제작자에게 편집저작물 또는 2차적저작물 작성자의 권리가 부여될 수 있다. 학습용 데이터는 일반인의 시각에서는 의미 없는 수준으로 가공될 수도 있지만 사상, 감정 등 저작물성의 요건을 충족할 가능성도 배제할 수 없다.

현재 인공지능 산업 발전에 학습용 데이터셋의 부족이 커다란 장애가 되고 있다. 단견으로는 데이터셋의 이용 제약을 없애는 것이 좋을 것처럼 보이지만, 데이터셋 제작에 비용과 시간을 투자한 자에 대한 법적 보호가 중장기적으로는 도움이 될 것으로 보인다. 따라서 창작성이 없더라도 투자에 대한 보호와 관련된 법제도 정비를 검토할 필요가 있다.

2) 표절 등 윤리적인 문제

저작권법은 엄밀히 모방을 금지하는 제도가 아니다. 타인의 생각을 자신의 것처럼 표절하더라도 저작권 침해에는 해당하지 않는 사례도 많다. 대표적으로 저작권법에

서는 아이디어를 베끼는 것이 문제가 되지 않는다. 미국의 저작권법 102조(b)는 "저작자의 원저작물에 대한 저작권의 보호는 그 형태 여하를 불문하고 당해 저작물에 기술, 설명, 예시 또는 구현된 아이디어, 절차, 과정, 작동 방식, 원칙 또는 발명에 대하여는 적용하지 아니한다"고 명시하고 있기도 하다(U.S. Copyright Office, 2016).

인공지능에 의한 창작은 미술, 어문, 음악 분야에서 선도적으로 이루어지고 있다. 이들은 빅데이터를 기반으로 기존의 저작물을 변형하여 새로운 저작물을 만들어내고 있다. 이 과정에서 저작물 이용이 일어날 수밖에 없고 결과물에도 기존 저작물의 흔적이 남아 있게 된다. 정도의 차이가 있을 뿐이지 사람이 창작한 저작물도 유사한 과정과 결과를 가져오고 있다. 이 과정에서 2차적저작물작성권 침해에 해당하지 않더라도 아이디어 표절 등 윤리적인 문제를 야기할 수 있고 이는 곧 불법행위나 부정경쟁방지법상 위법한 행위로 평가받을 위험도 있다.

하지만 현실에서 사람에 의한 창작에도 다른 사람의 창작물을 활용하거나 아이디어를 차용하는 새로운 미술사조가 등장하면서, 법제도 역시 유연하게 접근해야 한다는 주장이 힘을 얻고 있다. 예를 들어, '차용미술'이라는 영역에서 기존 작품들을 활용하여 새로운 창작에 이르는 방식을 법적으로 용인한 사례들이 존재한다(Fisher III et al., 2012).

나. 인공지능 창작물의 보호

1) 비인간 창작물에 대한 법적 판단

인공지능의 창작물은 인간이 아닌 비인간의 창작물이다. 따라서 현행법상 창작물로 인정되지 않으며 저작권을 부여할 수 없다. 비인간이라도 법적으로 인간으로 간주하는 법인격이라는 개념이 있지만 현재로서는 인공지능에 대하여 법인격 인정을 논하는 단계까지 나아가지 못하였다. 그러나 인공지능이 사람처럼 창작을 할 수 있게 된다면 문화발전이라는 저작권법 목적에 도움이 되는 것은 분명하다. 현재 수준의 약한 인공지능 역시 누군가의 노력과 비용이 수반되어 창작이 이루어지고 있는 바 투자에 대한 보상도 도외시할 수 없다. 투자를 보존하기 위한 법적 조치에서 저

작권한 부여도 하나의 방법으로 논할 수 있기 때문에 인공지능을 법인격으로 인정하는 사안에 대해 쉽게 결론을 내릴 수는 없다. 또 다른 대안으로는 저작권이 아니라 다른 법 조항을 통해 투자를 보상해줄 방법을 찾아볼 수 있다.

2) 대안 모색을 위한 고려사항

앞서 언급하였듯이 자연인, 법인에 이어 '전자인간(인공지능)'을 법적인 사람의 개념으로 인정하는 문제는 쉽게 풀 수 있는 것이 아니다. 어떤 결론에 도달하려면 수많은 쟁점과 복잡한 이해관계를 풀어야 한다. 다행히 인공지능의 현 기술 수준에서는 아직 충분히 논의할 시간이 있다고 본다. 지금 시점에서 분명한 것은 인공지능 기반의 기술도구로 창작물이 생성되고 상용화 단계에 있는 현재의 수준에서 필요한 조치를 강구해야 한다는 것이다. 예를 들어, 투자자, 사용자, 프로그램 개발자 등에게 권리를 부여하는 방안, 부정경쟁행위로서 규제하는 방안 등을 고려해 볼 수 있다.

우리나라에서는 아직 인공지능 결과물에 대한 법적 보호 방안이 구체적인 법률 개정안으로 발의된 바는 없다. 다만 2017년 2월 '신산업 규제혁신 관계장관회의'에서 4차 산업혁명 시대를 견인할 인공지능과 그 응용 분야의 선제적 규제개선의 일환으로 인공지능 확산 관련 핵심 법제도 이슈를 제시하기로 한 바 있다(미래창조과학부, 2017. 2. 17). 또한 국가지식재산위원회에서도 '차세대 지식재산 특별전문위원회'를 설치하고 인공지능, 빅데이터 등 신기술 IP의 보호 체계 정립과 IP 이슈(인공지능 창작물의 권리인정 문제 등) 등에 대한 계획을 발표하였다(미래창조과학부, 2016. 12. 22).

(1) 인공지능 소유자에게 권리를 주는 방안

현재의 저작권법은 인공지능이 만든 결과물에 대한 보호를 고려하지 않고 있지만 향후 개정안을 검토한다면 크게 세 가지 경우를 생각해 볼 수 있다. 먼저 인공지능의 소유자인 사람에게 권리를 주는 방안이다. 인공지능이 법적 주체로 인정되는 경우 컴퓨터 소유자가 인공지능을 '사실상(de facto)' 고용한 것과 같은 관계라는 주장

에 따른 것이기도 하다(김윤명, 2016).

이와 관련하여 업무상 저작물과 관련된 조항이 인공지능 창작물 보호에 대한 시사점을 줄 수 있다. 국내 저작권법은 제2조 제31호에서 '업무상저작물'에 대하여 "법인·단체 그 밖의 사용자(이하 '법인 등'이라 한다)의 기획 하에 법인 등의 업무에 종사하는 자가 업무상 작성하는 저작물을 말한다"고 정의한 후 제9조에서 "법인 등의 명의로 공표되는 업무상저작물의 저작자는 계약 또는 근무규칙 등에 다른 정함이 없는 때에는 그 법인 등이 된다. 다만, 컴퓨터프로그램저작물(이하 '프로그램'이라 한다)의 경우 공표될 것을 요하지 아니한다"고 규정하고 있다. 업무상 저작물을 귀속을 규정하는 제9조가 업무상 저작물에 대한 저작권의 귀속에 대하여 저작권법이 창작자 원칙의 예외를 두는 것은 단체명의 저작물은 법인 등이 기획·공표하며, 그 이름으로 사회적인 책임을 지는 것이 일반적이므로, 법인 등에 저작자의 지위를 인정하여 법률관계를 명확하게 하고 거래의 편의를 도모하며 저작자 특정의 곤란을 해소하기 위함이다(이해완, 2015).

(2) 프로그램 개발자에게 권리를 주는 방안

두 번째로 고려해볼 수 있는 것은 프로그램 개발자에게 권리를 주는 방안인데 프로그램 개발자는 인공지능이 구동될 수 있도록 프로그램을 만들었을 뿐, 인공지능을 통한 창작과정에는 별로 관여하지 않는다. 인공지능을 '도구'로 보는 시각에서는 현행법에서도 프로그램 개발자에게 권한을 부여하는 것이 가능하다. 하지만 인공지능이 스스로 학습능력을 통해 지식재산을 창출하는 수준에 이르게 되면 개발자에게 권리를 주는 방식은 저작권법의 기존 논리로는 이해하기 어렵다.

(3) 인공지능에 권리를 주는 방안

마지막으로 인공지능 그 자체에 권리를 부여하는 방안이다. 그러나 이를 위해서는 인간과 분리된 온전한 법적 주체임을 인정하는 것이 선행되어야 한다. 아직은 실현 가능성이 높지 않은 가정이다. 그러나 미래를 대비해 대안의 하나로 고려한다면, 이 경우 기존의 법체계에서 소유자 혹은 사용자에게 책임과 권한을 적용하는 단계에서 법인 체계, 예컨대 특수목적법인(Special Purpose Company)에 관한 사항을 규

율하는 특별법을 마련하거나 민법상 한정후견인을 두는 것과 유사한 것으로 파악해 보는 것이 하나의 방안이 될 수 있다.

나아가 독자적인 권리와 의무의 주체로서 법에 편입되는 단계를 검토해 볼 수 있다. 같은 취지에서 부정경쟁방지법의 개정이나 지능사회 관련 새로운 법률 제정에 투자자 보호 관련 규정을 마련하는 것도 대안이 될 수 있다.

제 6 절 초연결사회 기술기반 창작 이슈에 대한 전문가 의견

여기서는 기술기반의 창작과정 이슈에 대해 따로 수행한 전문가 의견조사를 다룬다. 앞에서 다룬 이슈들은 수년간의 사회적 논의와 법리적 논쟁이 축적됐던 반면 창작 관련 이슈는 사회적 논의가 이제 막 시작된 단계로써 사회적 합의에 기반을 둔 결론을 내리기 부족한 상황이다. 이번 의견조사의 목적도 어떤 결론을 내린다기보다는 관련 전문가들의 의견을 들어보고 향후 논의의 방향을 좁히는 데 의의를 두고자 한다.

1. 전문가 의견조사 개요

디지털 환경의 변화에 따라 저작권법 예외 조항을 활용하여 저작물 이용범위를 확대할 필요가 있다는 이슈와 아직 사회적 합의점을 찾지 못한 인공지능 창작물의 저작권 이슈에 대해 전문가 의견을 조사하였다.

이 조사는 2017년 11월 약 2주간 진행되었다. 사전에 조사 주제와 관련 전문가 리스트를 작성하고 일일이 전화를 걸어 의견조사 참여 여부를 확인하였다. 최종 선정된 전문가 20명의 분야는 저작권 관련 기관 3명, 대학의 문화콘텐츠학과 교수 3명, 법학과 3명, IT 포털사이트 종사자 2명, 법무법인 변호사 2명, 정책기관 2명, 공학·기술 분야 개발자 4명, 언론 분야 1명으로 구성되었다. 참여한 전문가의 신분은 가급적 익명 처리하였으며 이에 따라 의견조사에 참여한 이들의 정보를 보고서에서 일

관되게 밝히지는 않았다.(표 5－5).

〈표 5－5〉 인공지능 창작물에 대한 전문가 의견조사 응답자

번호	분야	소속	지위
1	언론	-	기자
2	저작권 관련 기관	한국음악저작권협회	-
3		한국저작권위원회	
4		한국저작권보호원	
5	대학 (문화콘텐츠)	한림대학교	교수
6		순천향대학교	
7		서울예술대학교	
8	IT 포털	C사	-
9		N사	
10	대학(법학)	한양대학교	교수
11		상명대학교	
12		강원대학교	
13	법무법인	-	변호사
14		-	
15	정책기관	국회의원실	보좌관
16		한국소비자원	연구위원
17	대학·연구기관·민간산업 (공학/기술)	한국전자통신연구원	책임연구원
18		광주과학기술원	교수
19		인하대학교	교수
20		엘에스웨어	연구소장

전문가 의견조사를 위해 객관식과 주관식으로 구성된 구조화된 웹 설문지를 만들어 온라인으로 응답을 받았다. 의견조사 내용은 인공지능 학습용 데이터셋 구축 시 저작권 이슈와 인공지능 창작물에 대한 저작권 이슈 등 두 가지이다.

조사 내용의 세부 항목은 아래 〈표 5－6〉와 같다.

〈표 5－6〉 인공지능 창작물에 대한 전문가 의견조사 내용

항목	세부 항목
데이터셋 저작권 이슈	인공지능 학습용 데이터에 대한 저작권법 예외
	데이터셋 제작자의 법적 권한
	이용된 저작물의 창작자 성명이나 출처 표시의 필요
	이용된 저작물의 동일성유지권 침해 이슈
	2차적저작물작성권(번역권)의 침해 이슈
인공지능 창작물 저작권 이슈	인공지능의 추론을 거친 창작물에 대한 저작권 인정 수준
	인공지능의 새로운 창작물에 대한 저작권 인정 수준
	인공지능의 저작권 대리인
	저작권 인정 기간

자료: 직접 작성.

2. 저작물 이용범위 확대에 대한 전문가 의견

저작물 이용범위 확대에 대해 전문가 의견조사는 인공지능 학습용 데이터에 저작물이 포함되는 경우 저작권 예외 조항으로 규정하는 데 대한 의견조사로 한정해서 질문하였다.

가. 인공지능 학습용 데이터 구축 시 저작권법 예외 조항 여부

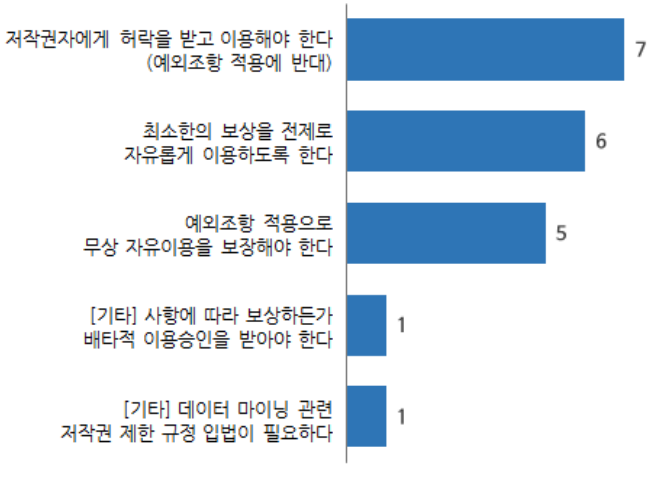
인공지능 학습용 데이터 구축을 위한 데이터 마이닝을 저작권법 예외 조항으로 하는 방안에 대해 7명이 ② ‘저작권자에게 허락을 받고 이용해야 한다(예외조항 적용에 반대)’고 응답하였으며, 6명이 ③ ‘최소한의 보상을 전제로 자유롭게 이용하도록 한다’고, 5명이 ① ‘예외조항 적용으로 무상 자유이용을 보장해야 한다’고 응답하였다. 조사 결과는 신기술·신서비스를 수용하는 과정에서도 기존 법률을 따를 필요성에 무게가 더 실려 있기는 하지만, 사실상 예외조항 불가에서부터 일정 조건에서의 허용, 그리고 무상 자유이용에까지 의견이 거의 균등하게 갈렸다고 볼

수 있다.

기타 의견으로 '기존 저작물의 종류에 따라 보상권을 처리해야 할 것도 있을 것이고, 배타적 이용허락을 받아야 하는 것도 있어야 한다'는 의견과 '데이터 마이닝 관련 저작권 제한 규정의 입법 필요성'을 제안한 의견이 있었다. 즉, 사안에 따라 저작권 적용 여부가 달라질 수 있다는 것과 현재의 저작권법에서보다는 새로운 조항으로 데이터 마이닝에 대한 저작권 제한 규정을 따로 두자는 의견이 제시되었다.

〔그림 5－4〕 인공지능 학습용 데이터 구축 시 저작권법 예외 조항 여부

(단위: 명)



나. 인공지능 학습용 데이터셋에 대한 저작권 인정 여부

다음으로 영상저작물 등 저작물 일부를 가공하여 인공지능 학습용 데이터셋을 구축한 경우 2차적저작물로서 저작권을 인정하는 데 대한 전문가 의견을 수렴하였다. 이와 관련하여 응답자 중 13명이 일정 정도 권리를 인정해야 한다는 의견을 제시하였다. 13명의 의견을 개별적으로 살펴보면, 저작권법이 이미 창작성이 없는 데이터

베이스 제작자의 권리를 규정하고 있으며 인공지능 학습용 데이터셋도 데이터베이스와 같은 수준으로 적용되어야 한다는 의견이 다수였다.

반면에 데이터셋 자체가 독창성이 있다면 권한을 인정해야 한다는 주장도 있었다. 즉, 모든 데이터셋이 독창성이 있지는 않겠지만 일부 인정될 수 있다면 권한을 줘야 한다는 것이다.

> 독창성이 있는 경우에는 데이터셋 제작자에게도 일정한 법적 지위를 인정해야 할 것이다. 다만, 기존의 저작물에 대한 허락이나 보상을 전제로 제작해야 독자적인 권리가 인정되어 그에 따른 허락권한과 보상을 받을 수 있다고 사료된다. (법학자F)

그밖에 데이터셋 제작과정을 창작과정의 일부라고 판단해서 의견은 비창작물로서의 제한적 권리 보장이 아니라 아예 창작물로 간주하고 저작권을 보장해야 한다는 것이다. 이와 관련하여 데이터셋의 창작성을 정도로 판단하고 권리도 그에 비례하여 주어져야 한다는 주장이 있었다.

한 응답자는 창작성 여부와는 별도로 산업적 관점에서 인공지능 학습용 데이터 분야가 활성화되어야 기술 및 산업이 발전할 수 있다는 점에서 보상체계가 필요하다는 점을 지적하였다.

> 학습용 데이터셋 산업 자체가 활성화되어야 인공지능 기술도 그 기반 위에 발전할 수 있다고 판단된다. (IT 포털N)

응답자 4명은 데이트셋에 대한 저작권을 인정할 수 없다는 점을 분명히 하였다. 그 이유에 대해서, 먼저 데이터셋이 인공지능 학습과정에 필요한 도구적 목적을 가졌다는 주장이다. 학습과정에서 창작능력을 획득하는 것은 인공지능 기술이지 데이터셋나 데이터셋 제작자가 아니라는 것이다. 교육을 위한 저작물 이용에 대해 저작료를 지불하지 않듯이 학습을 위한 데이터셋을 이용할 때 저작료를 지불할 필요가 없다는 것이다.

> 실제 인간이 특정 창작 관련 분야에서 성장하는 과정을 보더라도, 즉 아무런 지식이 없는 학생이 기존 저작물을 보고 배우고 하는 과정을 통해 창작인으로 성장해 가

는데, 이때 교육 자체에 있어 (교육으로 지불되는 비용은 제외하고) 저작물에 대한 권리로 이에 대한 저작료를 지불하거나 그러지는 않는다. 사실 인공지능이 학습하는 절차도 어찌 보면 사람이 기존 데이터(저작물)로 학습하는 과정과 일맥상통하는 관점으로 해석할 수 있기 때문이다. (기술J)

데이터셋을 저작물로 인정하는 것에 찬성하든 반대하든, 혹은 판단을 유보하든 대부분의 전문가가 기존 저작물을 정당하게 사용하였는가에 대한 문제의식과 우려를 표명했다. 이와 관련하여 법학자A는 최근 법학계의 논의 사항을 전하였다. 데이터셋에 대한 저작권 예외 조항이 적용되더라도 해당 데이터셋이 외부에 공개되지 않고 내부용으로 사용 후 폐기하는 제한된 요건에서만 인정되어야 한다는 것이다.

아울러, 단순히 빅데이터를 인공지능의 내부에서 이용되는 학습용 데이터셋이 아닌 외부에 공표되는 학습용 데이터셋인 경우에는 원저작자의 저작권을 침해할 수 있다는 점에서 위의 인공지능 내부의 학습용 데이터로 이용하는 경우인지를 명확히 해야 합니다. 예외조항(공정이용) 적용은 내부에서 이용되는 학습용 데이터셋에만 경우에 한정된다는 것이 최근 논의의 내용이기 때문입니다. (법학자A)

다. 데이터셋 제작과정 및 인공지능 학습과정에서의 저작인격권 보호

저작권법 제12조와 제13조는 저작인격권에 대한 조항으로 각각 창작자 성명표시권과 저작물의 동일성유지권을 보장하고 있다. 성명표시권은 저작물의 원본이나 그 복제물, 또는 저작물 공표 매체에 저작자가 본인의 실명이나 이명(본 이름 외 달리 부르는 이름)을 표시할 권한이다.[70] 동일성유지권은 저작자가 자신의 저작물의 내용과 형식, 제호 등의 동일성을 유지하고자 할 때 보장받는 권리이다.[71]

---

70) 한국저작권위원회 용어사전 - 성명표시권
https://www.copyright.or.kr/information-materials/dictionary/view.do?glossaryNo=396&pageIndex=10&searchLangType=&searchkeyword=&pageDisplaySize=10&searchIdx=&searchText=&clscode=01&searchTarget= (검색일: 2017. 11. 1)

71) 한국저작권위원회 용어사전 - 동일성유지권
https://www.copyright.or.kr/information-materials/dictionary/view.do?glossaryNo=379&pageIndex=9&searchLangType=&searchkeyword=&pageDisplaySize=10&searchIdx=&

이 조항들과 관련하여 먼저 원저작자의 권한을 보호한다는 차원에서 학습용 데이터셋 저작과정이나 인공지능의 학습과정에서 사용된 저작물의 창작자 성명과 출처를 표시해야 할 의무에 대해 물었다. 이에 대해 13명이 긍정적으로 응답하였다. 6명이 그럴 필요가 없다고 보았고 1명이 판단을 유보하였다.

데이터셋 제작과정에서 원저작물을 허락 없이 변형하여 이용하는 것이 이른바 동일성유지권을 침해하는 문제가 되는지에 대한 질문에서는 그렇다고 응답한 전문가가 10명, 그렇지 않다고 한 전문가가 9명이었다. 1명은 판단을 유보하였다.

〈표 5－7〉 학습용 데이터셋에 대한 저작인접권 적용 여부

성명이나 출처 표시	동일성유지권	응답자수(명)
해야 된다	침해문제 있다	10
	침해문제 없다	3
	잘 모르겠다	-
하지 않아도 된다	침해문제 있다	-
	침해문제 없다	5
	잘 모르겠다	1
잘 모르겠다	침해문제 있다	-
	침해문제 없다	1
	잘 모르겠다	-

이러한 결과는 앞서 데이터셋 제작자의 법적 권한을 인정하기에 앞서 데이터셋 제작 과정이 원저작물의 저작권 침해가 될 수 있다는 점에 대다수가 우려를 표명하였던 것과 일관된 것이다. 전문가의 판단 과정에서 향후 추진할 정책 방향에 대한 어떤 함의를 얻을 수 있을 것을 기대하고 판단 기준 혹은 이유를 자세히 서술해 줄 것을 요청하였다.

기본적으로 저작물을 사용할 때는 창작자의 권리를 존중해야 하고 현행법에서 저

searchText=&clscode=01&searchTarget= (검색일: 2017. 11. 1)

작인접권으로 보장하기 때문에 성명표시권과 동일성유지권은 지켜져야 한다는 의견이 다수였다. 총 10명이 성명 등은 표시되어야 하고 원저작물의 변형은 동일성유지권과 밀접하므로 원저작자로부터의 사전 승인이 필요하다고 보았다.

> 저작물이라 하면 창작자의 사상과 감정이 반영되어 있고, 이를 존중해줘야 한다고 생각합니다. 따라서 변형을 위해서는 사전 허락이 필요하다고 생각합니다. 다만, 인공지능 산업발전을 위해서라면 공유저작물을 활성화하고 이용하는 것이 적절해 보입니다. (기술C)

특히 성명표시권은 다양한 편집이 가능해진 기술 환경에서 창작물의 본래 창의성을 드러낸다는 점에서 지켜져야 한다고 주장하기도 하였다.

> 특히 디지털 시대가 되면서 특수 기술을 활용해 다양한 편집 등이 용이하게 될 수 있지만 창작물 본연의 창의력은 훼손되어서는 안 된다고 본다. (문화콘텐츠K)

성명표시권과 관련해서는 지식 출처와 가공과정에 대한 정보를 남기는 의미도 있다고 한다.

> 지식정보사회에서 지식의 출처와 가공과정은 필수 정보이다. 인공지능이 창작하게 되고 저작물을 빅데이터 형태로 활용하게 되면서 효율성과 개발 편의를 이유로 저작물 이용 표시를 생략하거나 기계식 문법으로 간소화할 수 있는데 이는 창작의 가치를 훼손하고, 저작물의 형성과정을 불투명하게 만들어버릴 수 있다. (언론E)

다음은 성명 혹은 출처는 표시되어야 하나 동일성유지권을 지키는 것은 현실적으로 불가능하거나 불필요하다는 의견이다.

> 기술적으로 불가능하다. 저작물의 본질적인 것을 이용하는지에 따라 달라질 수 있다. (법학자H)

대조적으로 5명이 성명표시권 및 동일성유지권 모두 적용될 필요가 없다는 견해를 드러냈다. 저작권법의 예외 사유에 해당될 수 있다거나 데이터베이스 관련 저작권에서 인격권이 없는 상황과 마찬가지로 봐야 한다는 의견이다.

우리 저작권법 제12조와 제13조는 성명표시권과 동일성유지권의 예외 사유를 규정하고 있습니다. 딥러닝을 위한 데이터의 수집 및 가공의 경우에는 부득이한 경우로 보는 것이 적절한 것 같습니다. (기관D)

5년 이하의 단기간의 저작권으로 보호해야 한다고 생각하지만, 데이터베이스도 인격권이 없는 상황에서 인공지능이 만든 창작물에 인격권을 부여하는 것은 논리적 일관성이 없습니다. (법학자P)

또 학습과정에서 사용하는 것뿐이라서 필요가 없다고도 하였다.

학습과정에서 출처를 확인할 필요는 없다고 봅니다. 사람이 책을 보거나, 공부하는 것과 다름이 없다고 보는 것이지요. 따라서 동일성유지권에 대한 문제도 필요하다고 보지 않습니다. (법학자R)

라. 2차적저작물작성권(번역권) 침해에 대한 의견

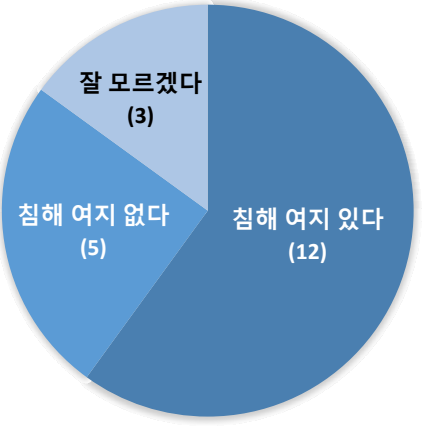
인공지능 학습용 데이터셋 구축과 관련한 직접적인 저작권 이슈는 아니지만 초연결사회의 신기술 서비스와 관련된 이슈로서 인공지능 기반의 번역서비스에 대한 저작권 문제를 질문하였다. 즉, 인공지능 기반의 번역서비스가 저작권법상의 2차적저작물작성권[72](번역권)의 침해라고 판단할 여지가 있는지에 대한 문항이다. 이와 관

72) 2차적저작물작성권이란, 원저작물을 번역·편곡·변형·각색·영상제작 그 밖의 방법으로 작성한 창작물을 2차적저작물이라고 하는데, 원저작물의 저작자는 자신의 저작물을 원저작물로 하는 2차적저작물을 작성할 권리와 작성된 2차적저작물을 이용할 권리를 가진다. 원저작자의 이러한 권리를 2차적저작물작성권이라 한다. 즉, 자신의 저작물을 원저작물로 하는 2차적저작물을 작성할 권리는 원저작자의 배타적 권리이므로 원저작자의 허락 없이 2차적저작물을 작성하였다면 원저작자의 2차적저작물작성권을 침해한 것이다. 다만, 이러한 허락 없이 2차적저작물작성권을 침해하면서 작성된 2차적저작물일지라도 제3자와의 관계에서는 독립된 저작물로 보호받는다(한국저작권위원회 용어사전 - 2차적저작물작성권 (https://www.copyright.or.kr/information-materials/dictionary/view.do?glossaryNo=446&pageIndex=1&searchLangType=&searchkeyword=&pageDisplaySize=10&searchIdx=&searchText=&clscode=01&searchTarget=) 참조).

련하여 12명이 침해라고 판단할 여지가 있다고 응답하였으며 5명이 아니라고 응답하였다. 그리고 3명이 판단을 유보하였다.

〔그림 5－5〕 인공지능 번역물의 2차적저작물작성권 침해 여지에 대한 의견

(단위: 명)



원저작자의 2차적저작물작성권을 침해할 여지가 있다고 본 이유로는 행위의 주체가 사람이냐 기계냐의 차이만 있는 사항으로 본래의 법 취지가 적용되어야 한다는 점을 주로 꼽았다.

> 행위의 주체가 사람이냐 기계냐의 차이만 있을 뿐이기 때문에 저작물 번역 서비스는 저작권법상 권리 침해라고 판단한다. (기관B)

> 전문 번역가를 고용하여 저작권자의 허락 없이 번역하는 것과 다르지 않기 때문이다. (변호사G)

저작물을 단순 번역하는 것은 창작 행위가 아니기 때문에 창작 행위의 보호 차원에서라도 원저자의 2차적저작물작성권은 보호되어야 한다고 주장한다. 또 그러한 단순 번역이 오히려 원저작자의 의도와는 별도로 작품 이미지 왜곡에 영향을 줄 수

도 있기 때문에 원저작자의 권리 행사가 중요하다고도 하였다.

> 번역은 저작물을 창작하는 것과는 다른 관점이다. 즉, 이미 (누군가-기계 혹은 사람-에 의해) 창작된 저작물을 다른 언어로 단순 변경하는 것이므로 저작권 허락이 반드시 필요하다고 생각된다. (기술J)

위의 의견과는 달리 창작물의 번역과 단순 텍스트의 번역을 구분해서 판단할 필요성을 제기한 응답자도 있었다.

> 출판물을 번역하는 것과 단순 번역에 인공지능을 이용하는 것과는 구분지어 판단하여야 할 것 같습니다. 인공지능을 이용하여 소설과 같은 기존 저작물을 번역하여 서비스를 제공한다면, 기존과 같이 번역에 대한 허락을 받아야 한다고 생각합니다. 즉, 2차 저작물 생성을 위해 사용된 인공지능 번역은 원저작권자의 권리 침해 여지가 있다고 생각합니다. (기술L)

의도적으로 기술혁신이 가져올 사회갈등 요인의 작동을 최대한 지연시키자는 의견도 있었다.

> 알고리즘에 따른 번역서비스가 저작권이 있는 콘텐츠를 무분별하게 번역해 낼 수 있다면 (조금은 다른 관점에서) 인간의 일자리 침해와도 맞닿아 있는 이슈이기 때문에 더욱 번역권이 보호되어야 합니다. 이러한 이유로 해당 이슈는 더 면밀한 검토가 필요할 것 같습니다. (IT 포털I)

원저작자의 2차적저작물작성권 침해가 아니라는 입장에서는 주로 인공지능 번역서비스 이용 행위가 기타 컴퓨터 소프트웨어를 이용하는 행위와 별반 다르지 않다는 점을 이유로 내세웠다.

> 약한 AI를 전제로 답을 합니다. 우선 인공지능 번역서비스를 제공한 사람과 인공지능에 번역을 지시한 사람을 나누어 생각해야 합니다. 번역서비스를 제공한 사람은 범용적 컴퓨터 프로그램을 제공한 사람과 마찬가지로 2차적저작물 작성에 대해 침해책임이 없습니다. (기관D)

인공지능을 이용한 번역서비스의 활용으로 공정이용의 범위에 해당하는 경우에는

침해가 되지 않고, 이를 이용해서 이득을 얻는 경우에는 번역권의 침해라고 보아야 하지 않을까 한다. (법학자F)

그 밖에 책임을 묻는 대상이 모호하다는 점, 원저작자의 경제적 이익을 해하지 않는 한에서 문제가 없다는 점을 들었다. 마지막으로 비경제적, 사적 이용에 따른 저작권법 예외 이유를 넘어 인공지능 기반의 번역서비스가 범용화되는 시점에서는 누구든지 자유롭게 이용할 수 있도록 하는 것이 낫다는 의견이다.

그러나 번역서비스가 고도화되면 번역은 개별적으로 가능한 시점이 되므로 단순히 책을 번역해 읽거나 리포트를 작성하는 경우에도 번역권 침해로 보는 것은 무리이고 이런 시점에 이르면 누구든지 자유롭게 이용할 수 있도록 해야 할 것으로 본다. (법학자F)

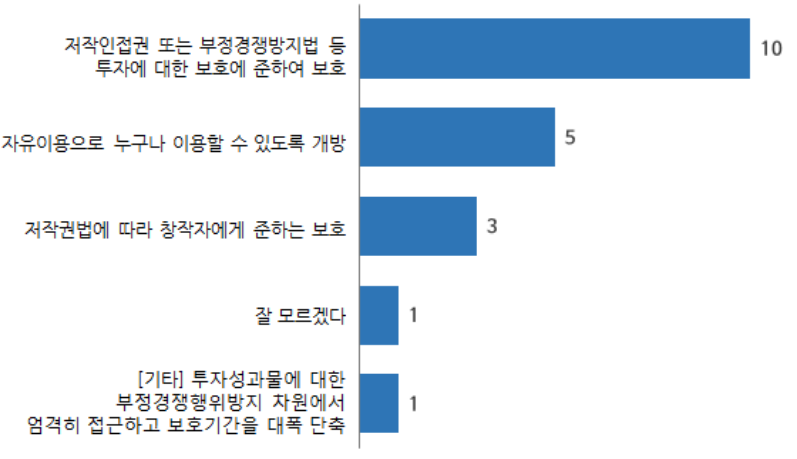
3. 인공지능 창작물에 대한 전문가 의견

가. 인공지능 창작물에 대한 법정 보호 수준

먼저 저작물이 포함된 기존 데이터 학습을 거친 인공지능이 추론 과정을 거쳐 새로운 결과물을 생성하였을 때 이 결과물에 대한 저작권을 인정한다면 어느 정도가 적당한지를 물었다. 가장 많은 응답은 10명이 선택한 ② '저작인접권 또는 부정경쟁방지법 등 기존 법에서 투자에 대한 보호에 준하여 보호할 수 있는 수준'이었다. 기타 의견으로 나온 '부정경쟁행위 방지를 위해 투자성과물에 대한 보상은 해야 하나 저작권 보호기간을 대폭 단축하는 등의 조정이 필요'하다는 의견도 투자에 대한 보상이 필요하다는 점에서 앞의 10명과 같은 의견으로 볼 수 있다. 그밖에 5명이 ③ '누구나 자유롭게 이용할 수 있도록 개방해야 한다'는 데 동의하였으며, 3명은 ① '저작권법에 따라 창작자에 준하는 보호 수준'을 선택하였다. 나머지 한 명은 판단을 유보하였다.

〔그림 5－6〕 인간 통제 및 학습과정을 거친 AI 창작물에 대한 법정 보호 수준

(단위: 명)



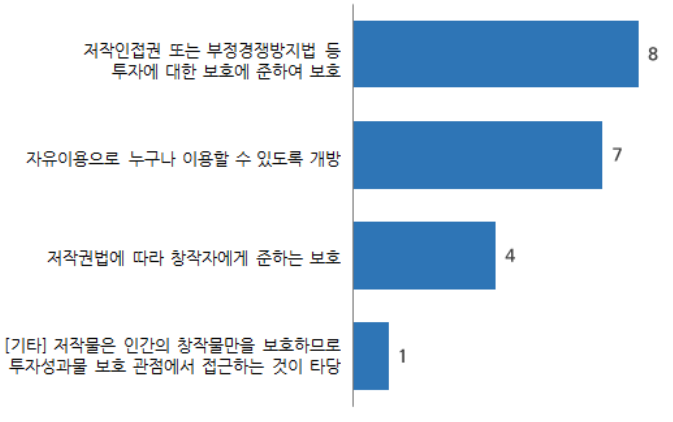
다음으로 보다 진전된 인공지능 기술을 가정하였다. 즉, 저작물이 포함된 데이터를 이용한 학습 과정을 거치지 않고 각 분야의 기본 원리만 학습한 상태에서 새로운 콘텐츠를 제작하였을 경우이다. 인공지능이 회화의 기본 원칙을 입력받고 스스로 그림을 그려내거나 음악 작곡의 기본 원칙의 학습만으로 음악을 작곡하는 것으로 인간의 개입이 감소하고 인공지능의 자율적 판단 영역이 증가한 상황을 가정하였다. 이렇게 가정을 약간 달리하였을 때, 응답 결과는 다음과 같았다.

먼저 ② ‘투자에 대한 보호에 준하는 수준’을 선택한 이는 8명으로 역시 가장 많은 응답을 받았다. 기타 의견인 ‘저작물은 인간의 창작물만을 보호하므로 어느 경우에나 투자성과물 보호 관점에서 접근하는 것이 타당’하다는 의견은 투자에 대한 보호 수준이라는 점에서 역시 앞의 8명과 동일한 의견으로 간주할 수 있다. 그 밖의 응답에서 그 결과물을 ③ ‘누구나 이용할 수 있게 해야 한다’는 의견은 7명으로 늘어난 반면, ① ‘저작권법에 따라 창작자에 준하는 수준’을 선택한 이는 1명이 더 늘어난 4명에 불과하였다.

결과적으로 인공지능 기술 수준이 더 높아져 인간의 통제에서 좀 더 벗어나 콘텐츠를 생성해도 창작자에 준하는 인공지능의 저작권 인정에는 대체로 부정적이라고 볼 수 있다. 오히려 개입하는 인간의 영역이 줄어든 만큼 공공재로서 자유롭게 이용하도록 개방하자는 의견이 늘었다. 가장 적정한 기준은 인공지능 개발을 위한 투자를 보호하는 수준에서 성립되는 것이었으며, 보상을 받아야 할 인간의 개입 정도가 감소할수록 공공재로 활용하는 데 동의하는 의견이 증가한 것이다.

〔그림 5－7〕 인간 통제 및 학습과정 없이 생성된 AI 창작물에 대한 법정 보호 수준

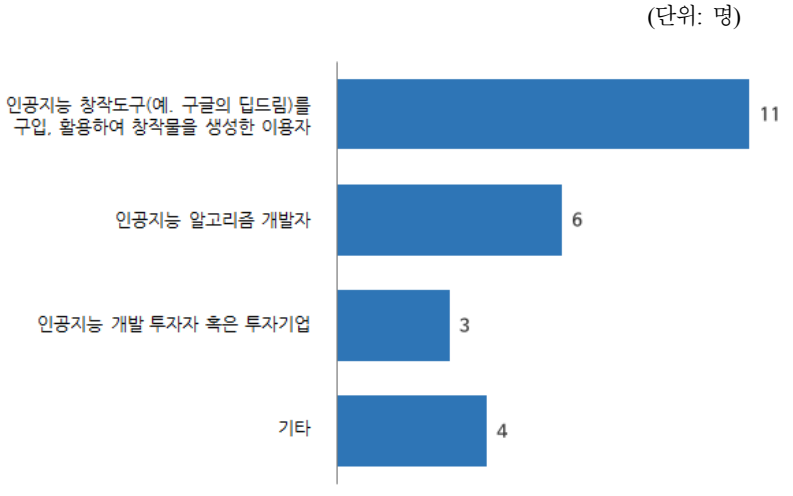
(단위: 명)



나. 인공지능 창작물의 법적 대리인

인공지능 창작물에 대한 저작권을 인정할 때 인공지능을 대신해 법적 권리를 행사할 주체를 규정할 필요가 있다. 전문가들에게 이 경우 누가 인공지능 대리인으로 저작권을 행사하는 데 가장 적합하다고 생각하는지를 물었다.

〔그림 5－8〕 인공지능 창작물의 법적 대리인에 대한 의견



이 문항에서는 중복응답을 허용하였으며 응답자의 이해를 돕기 위해 구글의 인공지능 기반 그림 생성 소프트웨어인 딥드림의 예[73]를 들었다. 그 결과, 11명이 ③ ‘인공지능 창작도구를 구입, 활용하여 창작물을 생성한 이용자’로 응답하였고, 6명이 ① ‘인공지능 알고리즘 개발자’, 3명이 ② ‘인공지능 개발 투자자 혹은 투자기업’을 선택하였다. 그밖에 4개의 기타의견이 나왔는데, ④ ‘개발자, 투자자(투자기업), 이용자 간의 적정한 분배’, ⑤ ‘인공지능 창작도구를 구입한 소유자’, ⑥ ‘창작물을 생성하도록 인공지능에 최종 명령을 내리고 자료를 정리한 자’, ⑦ ‘추가적인 논의가 필요’ 등이었다. 이 중 ⑤ ‘인공지능 창작도구를 구입한 소유자’와 ⑥ ‘인공지능에 최종 명령을 내리고 자료를 정리한 자’는 ③ ‘인공지능 창작도구를 구입, 활용하여 창작물을 생성한 이용자’일 수도 있다는 점에서 다수가 ③ 의 경우를 선택하였

73) 응답자가 설문 응답 중에 참고할 사이트로 방문할 수 있게 하이퍼링크하였다. 해당 사이트는 구글의 딥드림 소프트웨어를 활용해 이용자들이 만들어낸 사이키델릭한 그림들을 볼 수 있는 곳이다(Deep Dream Generator (https://deepdreamgenerator.com/feed/) 참조).

다고 볼 수 있다.

객관식에 응답한 이후 인공지능 생성물의 저작권 대리인 응답의 판단 이유를 주관적으로 기술해 줄 것을 요청하였다.

1) 법적 대리인으로서 인공지능 이용자

먼저 ③ '인공지능 창작도구를 구입, 활용하여 창작물을 생성한 이용자'로 응답한 대부분은 인공지능을 창작도구로 이해하고 창작도구를 활용한 이용자의 창작성을 인정해야 한다는 의견을 냈다.

> 워드프로세서나 필기도구를 활용하여 작품을 만든 사람에게 저작권을 주는 것이지, 워드프로세서 제작자에게 작품에 대한 저작권을 주지 않는 것과 같은 이치라고 하겠습니다. 인공지능 도구를 활용하여 인공지능이 무엇을 생성하도록 명령을 하는 주체이므로, 창작물을 생성한 이용자에게 저작권을 행사할 권한을 주는 게 맞다고 봅니다. (기관B)

> 인공지능 개발자는 단순히 창작할 수 있는 기술을 실현한 것뿐이고 실제 본인의 취향 혹은 스타일에 맞는 창작물을 생성하는 데 직접 기여한 실체는 이를 구입해서 실행, 사용한 사람/사용자이기 때문이다. (기술J)

인공지능은 창작도구일 뿐이라는 의견과는 별도로 인공지능 알고리즘 개발 능력이 월등히 뛰어난 거대 글로벌 ICT 기업에게 저작권한이 몰리는 불균형 현상을 우려하는 의견도 있었다.

> 인공지능 알고리즘 개발자나, 인공지능 개발 투자자에게 저작권을 조금이라도 인정하게 된다면 전 세계의 창작물에 대한 모든 권리를 Google, Amazon, IBM 등의 대기업이 인공지능에 대한 저작권을 전부 가지므로 대기업에 종속될 가능성이 크기 때문입니다. (법학자P)

또 하나 눈길을 끄는 의견으로 약한 인공지능 수준에서 도구로 기능하는 것을 넘어서 인간의 통제를 벗어나 인공지능의 자율적 판단으로 콘텐츠가 생성되는 단계에 이르면 그 생성물은 특정 유형의 것으로 관리해야 한다는 것이었다. 이는 앞서 응답

에서 인공지능의 자율성이 커질수록 그 결과물을 공공재로써 누구나 활용할 수 있도록 해야 한다는 의견이 증가한 것과 어느 정도 통하는 응답으로 보였다. 창작에 기여한 '사람'이 없는 경우는 기존의 법 제도가 아니라 다른 유형의 제도와 기준이 요구된다고 볼 수 있다.

> 위의 질문에서 의도한 AI는 약한 AI로 보이는데, AI를 학습시키고 활용한 사람이 있으면 그 사람이 저작자가 되는 것이 합리적이고, 그렇지 않고 강한 AI 창작의 경우에는 창작에 기여한 사람이 없으므로 저작권이 아니라 창작성 없는 데이터베이스제작자의 권리처럼 저작권법상 특별한 권리(sui generis rights)의 형태로 권리를 부여하거나, 아니면 특별법으로 규율하여야 할 것입니다. (기관D)

2) 법적 대리인으로서 알고리즘 개발자 그리고 투자자

① '알고리즘 개발자만'을 대리인 자격으로 꼽은 3명의 응답 내용을 보면 저작권의 대상을 인공지능이 산출한 콘텐츠가 아니다. 저작권 대상은 콘텐츠를 산출한 인공지능 알고리즘으로 간주하고 있다.

> 지재권 기본원칙인 창작자주의 원칙에 가장 근접… 나아가 책임도 물을 수 있어야 한다. (법학자H)

> 빅데이터 등 자료를 수집하는 역할은 창작의 수준이 아니고 주어진 데이터를 논리적으로 알고리즘을 설계하고 최적화하는 것이 창작, 즉 저작권으로 간주된다고 본다. (문화콘텐츠K)

알고리즘 개발자와 인공지능 이용자를 모두 꼽은 한 명의 응답자는 인공지능을 플랫폼으로 보고 그 플랫폼을 통해 생성된 콘텐츠는 개발자와 이용자 간 협업의 결과물이며 따라서 법적 권리는 둘 모두에게 속한 것으로 판단하였다.

> 알고리즘 자체가 플랫폼이므로 기술 개발자와 이를 활용한 이용자가 공유하는 게 타당하다. (언론E)

알고리즘 개발자와 투자자를 동시에 꼽은 응답자 2명은 역시 인공지능 알고리즘

을 창작물로 보고 창작물 생성에 기여한 이들도 개발자와 투자자를 법적 권한의 대상으로 보았다.

> 알고리즘 스스로 진화해 나간다 하더라도 초기 셋업을 한 주체인 개발자와 개발이 가능하도록 지원한 투자자가 저작에 대한 권리를 인정받아야 한다고 생각합니다. 때에 따라 오픈소스를 기반으로 작업이 진행됐을 수도 있으나, 이 경우에도 알고리즘 제작을 위한 설계와 디자인 등 최소한의 리소스는 들기 때문에 이에 대한 최소한의 보상 장치는 만들어져야 할 것입니다. 또한, 이들에 투자한 투자자들 역시 최소한의 권리 보장을 통해, 더 많은 창작 활동이 일어날 가능성에 대한 지속적 관심과 지원이 일어날 수 있다고 생각합니다. (IT 포털I)

② '인공지능 개발 투자자 혹은 투자기업'만 선택한 한 명의 응답자 역시 인공지능 알고리즘 자체가 창작물이며, 이 창작물이 생성되도록 지시하고 명령한 투자자가 그 자격이 있다고 보았다.

> 알고리즘 개발자보다는 개발 투자자 혹은 투자 기업이 대부분 창작을 지시하거나 명령한 주체가 될 것이므로 알고리즘 개발자가 종업원의 자격으로 개발한 인공지능 알고리즘이 만들어낸 창작물의 경우는 개발 투자자 혹은 투자 기업에 저작권이 귀속되는 게 맞는 것 같습니다. (IT 포털N)

3) 기타 의견

기타 의견으로 ④ '개발자, 투자자(투자기업), 이용자 간의 적정한 분배', ⑤ '인공지능 창작도구를 구입한 소유자', ⑥ '창작물을 생성하도록 인공지능에 최종 명령을 내리고 자료를 정리한 자', ⑦ '추가적인 논의가 필요'하다는 의견 등이었다. 이 중 ⑤ '인공지능 창작도구를 구입한 소유자'와 ⑥ '인공지능에 최종 명령을 내리고 자료를 정리한 자'는 ③ '인공지능 창작도구를 구입, 활용하여 창작물을 생성한 이용자'에 포함할 수 있다. 따라서 다수가 ③의 경우를 선택하였다고 볼 수 있다.

다. 인공지능 창작물 보호기간

이미 앞 문항들의 결과를 통해 의견조사에 참여한 전문가 대부분이 인공지능 생

성물을 창작물로 보거나 저작권 보호 대상으로 보는데 긍정적이지 않다는 것을 확인하였다. 마찬가지로 창작물로 인정한다고 가정하였을 때 적정한 저작권 보호기간을 묻는 질문에서도 가장 많은 응답은 ③ '현행법에서 창의성이 없지만 노력과 자원을 투입했기에 5년간의 단기 권리 존속 기간을 인정한 데이터베이스권과 같은 기준으로서 창작물을 생산한 직후부터 5년 정도로 제한하는 것'이었다.

〈표 5－8〉 인공지능 창작물 보호기간

질문	문항	응답(명)
인공지능 창작물을 인정한다고 가정하였을 때 적정한 저작권 보호기간	③ 현행법에서 창의성이 없지만 노력과 자원을 투입했기에 5년간의 단기 권리 존속 기간을 인정한 데이터베이스권과 같은 기준으로서 창작물을 생산한 직후부터 5년 정도로 제한해야 한다	7
	④ 인공지능 창작물 생산은 데이터베이스(DB) 제작보다 창작성·창의성이 있으므로 5년 이상의 권리 존속 기간을 인정해야 한다	4
	① 순수 창작물로 간주하여 인간 저작권자의 권한과 동일하게 (법적권한대행자가) 살아 있는 동안 및 사후 70년까지 저작권의 보호를 받아야 한다	2
	② 업무상저작물로 간주하여 공표한 다음 해 1월 1일부터 70년간 보호받아야 한다	1
	⑤ 인공지능의 생산물은 창작물이 아니므로 저작권을 단 하루도 인정할 수 없다	1
	[기타] 최단 기간이 성립하도록 새로운 형태의 합의가 필요하거나 5년 이하의 권리보호기간(예. 3년) 등 기간 단축을 제시	5

7명이 '데이터베이스에 준하는 단기 권리 존속 기간'을 선택하였고(③) 4명이 ④ '데이터베이스(DB) 제작보다 창작성·창의성이 있으므로 5년 이상의 권리 존속 기간을 인정해야 한다'고 보았다. 다시 말해서 11명이 데이터베이스에 준하거나 그보다

약간 나은 정도로 권리 존속 기간을 인정해야 한다고 응답했다. ① ‘순수 창작물로 간주하여 인간 저작권자의 권한과 동일하게 (법적권한대행자가) 살아 있는 동안 및 사후 70년까지 저작권의 보호를 받아야 한다’는 데는 2명만이 동의하였고 ② ‘업무상저작물로 간주하여 공표한 다음 해 1월 1일부터 70년간 보호받아야 한다’는 데는 1명이 선택하였다. 즉 3명만이 인간 저작권자와 동일하거나 비슷한 수준으로 보호기간을 규정해야 한다고 응답하였다. 그리고 한 명이 ⑤ ‘인공지능의 생산물은 창작물이 아니므로 저작권을 단 하루도 인정할 수 없다’고 하였다. 5명이 기타의견을 제시하였는데, 모두 최단 기간이 성립하도록 새로운 형태의 합의가 필요하거나 5년 이하의 권리보호기간(예. 3년) 등 기간 단축을 제시하였다. 즉, 창작성은 인정할 수 없지만 부가가치 창출이나 투자에 대한 보호차원에서 최단기간 보호 혹은 다른 방법의 보상을 고려해봐야 한다는 것이다.

제 7 절 소 결

본 장에서는 초연결사회의 기술 환경에 따라 문화영역에서 일어나는 현상과 정책 및 제도적 이슈를 살펴보았다. 먼저 초연결사회 기술 환경에 따른 디지털 콘텐츠의 유통, 이용, 창작 과정에서의 새로운 현상을 고찰하였다. 그다음으로 초연결사회에 대응하는 주요국의 제도 개선 논의와 정책 방향을 살펴보았다. 저작권 제도는 창작자의 배타적 권리를 보장해서 창작 활동을 도모하고 궁극적으로 문화 창달을 달성할 목적으로 정립된 것이다. 그러나 주요국의 정책 기조는 배타적 고립보다 공유와 개방을 통한 소통과 상호 작용에 더 가치를 두고 있다.

이어서 초연결사회의 기술 환경에 따른 디지털 콘텐츠의 유통, 이용, 창작 형태의 변화를 수용하기 위한 법적 논쟁을 고찰하였다. 저작권 제도의 많은 부분이 아날로그 시대의 유산인 만큼 디지털 사회에서 기존 제도가 수용하지 못하는 여러 상황과 법리 논쟁이 발생하였다. 여기서는 사적 복제, 클라우드 환경과 링크, 롱테일 시장과

고아저작물 권리처리, 공정이용 등 기술 환경 변화로 새롭게 해석되거나 개선이 필요한 기존 저작권 제도를 고찰하고 법리적 대안을 제시하였다. 또한 인공지능 창작 과정에서의 저작물 이용 이슈와 인공지능 창작물의 저작권 보호 수준에 대해 최근 제기되고 있는 논의를 살펴보았다.

그리고 최근 이슈인 인공지능 창작 과정에서의 저작물 이용 이슈와 인공지능 창작물의 저작권 보호 수준에 대해 전문가 의견 조사 결과를 기술하였다. 이 이슈는 최근 제기되고 있는 이슈로서 기존의 문헌과 현상, 사회적 논의만으로 어떤 결론을 끌어내기 어려웠다. 따라서 이 두 이슈에 대해 관련 전문가의 의견을 들어보고 앞서 고찰한 법리적 타당성 검토 결과를 더해서 향후 사회적 논의를 위한 몇 가지 방향을 다음 장에서 제시하였다.

제 6 장 결론 및 정책적 시사점

본 연구는 ‘초연결사회의 지속가능성을 위한 사회문화적 조건과 한국사회의 대응’의 3개년 프로젝트 중 마지막 연구로서, 3차 연도의 연구결과와 정책적 시사점을 요약하면 다음과 같다.

첫째, 제3장에서는 초연결사회의 미래규범 정립방향을 제시하였다. 이를 위해 초연결사회를 분석하는 틀로 각 계층(C-P-N-D)에 대표적인 규범이론인 목적론적 윤리론, 의무론적 윤리론 그리고 정의론을 적용하고, 초연결사회에 대한 규범이론의 적용결과를 바탕으로 초연결사회의 규범형식과 원칙 및 주요내용을 도출하였다.

구체적인 내용은 다음과 같다. 고대나 중세와 같이 단순하지 않은 현대 사회에 있어서 어떤 사회가 하나의 가치관, 하나의 규범이론을 가지고 운영되지는 않는다. 물론 기술의 영향이 많이 작용하는 사회인만큼 효율성을 바탕으로 최대행복을 추구하는 목적론적 윤리론에 입각하여 많은 사안이 결정될 가능성이 높고, 또한 법치주의 사회에서 법규범에 의한 권리와 의무의 규율이 이루어지는 것은 당연하다.

그러나 본 장에서 지적하고자 하는 바는 먼저, 초연결사회가 그렇게 하나의 가치관으로 모든 문제를 해결할 수 있는 사회가 아니며, 계층에 따라서 구체적으로 구분하여 사회적 문제에 접근하여야 한다는 것이다. 디바이스 계층에서는 롤즈의 정의론에 대한 고려가 강조되어야 한다고 분석되며, 네트워크 계층에서는 목적론적 윤리론에 입각한 효율성의 가치관이 일관성 있게 적용될 것이다. 플랫폼 계층에서는 어떤 규범이론을 적용하는가의 문제보다 어떤 규범을 통하여 규율할 것인가를 고민하여야 하며, 콘텐츠 계층에서는 의무론적 윤리론에 입각하여 인간을 목적으로 대하는 가치관이 강조되어야 한다.

또한 초연결사회의 문제들이 법규범만으로 해결될 수 있지 않다는 것이다. 이 또한 각 계층에 따라서 시간적 개념을 고려하여 분석해야 하며, 경우에 따라 법 이외

의 다른 규범에 관심을 더 기울여야 할 수도 있는 것이다. 디바이스 계층과 네트워크 계층에서는 정의롭고 안전한 초연결사회를 구현하기 위한 법규범이 기본적으로 작동하고, 특히 콘텐츠 계층과 플랫폼 계층은 인간 중심의 초연결사회를 구현하고, 공정한 경쟁을 보장하는 법규범은 물론이고, 인터넷 윤리나 윤리적 코드가 매우 강조되어야 한다. 나아가 초연결사회 규범 정립 시 고려해야할 기본원칙으로는 ①인간의 존엄과 가치 존중, ②정보격차, 사회적 차별 등 사회적 역기능 방지, ③노동·고용구조변화에 따른 사회적 안전망 및 사회보장제도 확충, ④민간의 창의와 자율성 보장, ⑤이용자의 안전과 사생활 보호를 제시하였다.

본 장의 연구를 통해 인간중심의 정의로운 초연결사회라는 가치관이 공허한 글귀로 취급될 수도 있겠지만 특정한 사안에서 정책을 결정하거나 기술의 발전을 유도하는 방향타가 될 수도 있을 것이다.

둘째, 초연결사회 안전성의 중심적인 요소로 지목된 사이버보안에 관한 연구가 2차 및 3차연도에 추진되었다. 2차연도는 사이버보안의 기술적 차원, 조직적 차원 그리고 사회문화적 차원에서 논의가 진행되었다. 이러한 논의로부터 여러 가지 시사점이 도출되었는데 그 중에서 사이버보안 교육과 사이버 복원력 확보의 중요성이 3차연도 정책 연구의 초점이 되었다.

우선 4장에서 논의한 사이버 침해의 트렌드 변화를 요약해 보면, 초기 정보사회에서는 해킹 능력의 과시가 사이버 침해의 주된 목적이었으나 2010년대 중반부터는 금전 목적으로 트렌드가 변화했으며 이러한 트렌드는 그 이후에도 견지될 것으로 전망되었다. 초연결사회의 진전에 따라 인공지능 기반의 자동 의사결정 기제가 널리 활용되면서 사이버 침해의 방법이 종래의 일회성 랜섬 웨어 공격에서 공격 대상이 이용하는 데이터 변조를 통한 의사결정 시스템의 교란으로 전환될 것으로 전망되었다. 이에 따라 향후 사이버 침해의 효과는 일회성에 그치지 않고 은밀하게 지속될 것이다. 이처럼 교묘한 침해 수법에 대응할 수 있는 기본적인 대책은 사이버보안에 대한 기초교육과 함께 항시적인 업그레이드 교육의 실시라고 생각된다.

초연결사회에서 작동하고 있는 주요 정보시스템들은 사이버 공격을 받고 있는 상

황에서도 그 핵심 기능이 작동해야 하며 침해당한 부분도 자기 치유를 통해 회복되어야하기 때문에 사이버 복원력의 중요성이 대두되었다. 사이버 복원공학의 원론격인 MITRE 보고서가 발표된 이후 관련 업계에서는 사이버 복원력을 위한 행동들을 알고리즘으로 구현하는 연구를 추진해 왔으나 사이버 복원력을 하나의 구체적인 시스템으로 구현하는 시도는 찾아보기 어렵다. 본 연구에서는 최근 사이버보안 분야에서 개발된 솔루션들과 MITRE 보고서에서 제안된 사이버 복원력 행동들을 결합한 인공지능 기반의 사이버 복원력 시스템의 개념을 제안했다. 이 개념은 새 정부 100대 국정과제 중 세부과제에 포함된 '인공지능 기반 사이버보안 위협 대응체계 구축'을 실현하는 데 도움이 될 것으로 본다.

지금까지 사이버 복원력은 단위 조직 차원에서 논의되어 왔다. 최근 사이버 공격에 대응하기 위해서는 국가, 나아가 글로벌 차원에서의 공조가 중요하므로 사이버 복원력 시스템도 적어도 국가적 차원으로 확장될 필요가 있다. 본 연구에서 제안한 '국가 사이버 복원력 기반'은 이와 같은 취지로 개발된 것으로서 새로운 물리적 인프라를 구축할 필요 없이 기존의 법제도 틀 안에서 사이버보안 관련 정책당국들 간 정보공유를 통해 구현할 수 있는 것이다.

제4장에서 제안한 사이버보안 교육 교안을 기반으로 정규 사이버보안 교육용 교재를 용이하게 개발할 수 있을 것으로 생각된다. 사이버보안 교육이 정규 교과과정에 편입되는 데 있어서 가장 큰 장애 요인은 새로운 교과목이 추가되어 학생들의 학습 부담이 가중된다는 것이다. 앞에서 언급한 바와 같이 사이버보안 교육은 현재 실시되고 있는 소프트웨어 교육의 일부로서 정규 교과과정에 진입시키고 향후 성과를 지켜보면서 확대 방향을 모색하는 것이 바람직하다.

셋째, 5장에서는 초연결사회 기술 환경으로 인한 문화영역의 특징적 현상과 그에 대응하는 정책적, 법·제도적 이슈와 대응을 살펴보았다. 문화 영역에 영향을 미치는 핵심 제도를 저작권으로 보고 지금의 저작권 제도가 어떤 방향으로 어떻게 개선되어야 초연결사회의 안정적 정착에 기여할 수 있을지를 모색해본 것이다. 특히 초연결사회가 지능화 단계로 진화되면서 최근 인공지능 기반 창작물에 관련한 이슈가

제기된 것에 주목하였다. 문헌 고찰이나 법리 논쟁 모두 아직 충분한 자료가 축적되지 않은 최신 이슈로서 본 연구에서는 향후 논의 방향에 대한 틀을 제시하는 데 의의를 두었다. 지금까지의 고찰을 기초로 정책적 시사점을 제시한다.

무엇보다 디지털 환경에서 발생하는 저작물의 생성과 유통, 이용 비중이 현저하게 증가하였으며 앞으로 더욱 큰 비중을 차지할 것을 고려하면 디지털 시대에 적합한 법으로의 개정은 필수적이다. 이와 관련하여 몇 가지 세부사항에 대한 대안을 제시한다. 첫째, 모호해진 사적복제의 범위와 개념에 따른 저작권 이슈에 대한 해결방안으로 사적복제 보상금 제도를 제안한다. 저작권자에게는 창작에 대한 보상을 보장하고 이용자에게는 자유로운 정보 교환과 창작 활동을 보장해주는 방안이다. 둘째, '링크'와 관련된 법적 제재조치를 완화하여 이용을 자유롭게 하는 반면, 저작물의 불법 링크를 통한 이익 추구를 저지하기 위해 다른 법을 활용하는 방안, 즉 손해배상책임이나 불공정거래의 책임을 묻는 방안을 제안한다. 셋째, 저작자가 불명확한 저작물을 이용할 방안을 마련하는 것이다. 디지털 형태로 수명이 길어진 콘텐츠를 저작자 불명으로 이용할 수 없다면 문화 발전과 산업 진흥 모두에 손해가 된다. 따라서 저작권리 처리의 편의를 위한 집중관리제도를 정비하고 강화할 필요가 있다. 중장기적으로는 일부 권리에 대해 권리의 배타성을 약화시키는 방안도 고려해야 한다. 마지막으로 공정이용의 범위를 확대하는 것이다. 공정이용 범위가 확대되면 기존 창작물을 토대로 자신의 창작물을 생성할 기회가 증가할 것이다. 아래에 언급하듯이 공정이용은 또한 신기술 개발에도 밀접한 이슈이다.

다음은 초연결사회 지능형 기술과 관련한 신규 이슈에 대한 것이다. 먼저 세계 각국이 논의하고 있는 공정이용 범위에 데이터 마이닝을 포함하는 안이다. 본 연구의 전문가 의견조사 결과, 기술 발전을 위한 유연한 대응보다는 현행 저작권법 원칙을 지키는 데 다수가 동의하였다. 이는 인공지능 기술 발전을 이유로 공정이용 범위를 확대하는 데는 사회적 합의를 위한 시간이 필요함을 함의한다. 따라서 현재는 현행법이 허용하는 한에서 학습용 데이터셋 구축 시 저작물을 제한적으로 이용하되 향후 제도적으로 공정이용 범위를 확대하거나 법정허락의 대상으로 관련 조항을 신설

하는 방안을 제안한다.

다음으로 인공지능 기반 창작물의 법적 권한에 대한 것이다. 사용자(소유자), 개발자, 인공지능 등 세 가지 방안에 대해 살펴보았다. 첫째, 전문가 의견조사 결과는 인공지능 사용자가 권한을 가져야 한다는 의견이 다수였다. 이때 사용자는 곧 소유자일수도 있고 엄밀하게는 소유자와 구분될 수도 있다. 이는 업무상 저작물에 대한 조항에서 시사점을 얻을 수 있다. 둘째, 프로그램 개발자의 경우 '인공지능 기반 창작도구'를 만든 저작권자로 이해된다. 그러나 인공지능이 스스로 학습하여 창작물을 생성하는 경우에는 논리적 타당성이 부족하다. 셋째, 인공지능 자체에 권리를 부여하기 위해서는 인간과는 별도의 온전한 법적 주체임을 먼저 인정받아야 하며 이 과정은 꽤 오랜 시일을 필요로 할 것이다. 기존 법체계에서 논리를 찾는다면, 특수목적법인에 관한 사항을 규율하는 특별법을 제정하거나 민법상 한정후견인을 두는 것과 유사한 것으로 보는 것이다.

본 연구는 초연결사회의 지속가능성을 공통분모로 삼고 상부구조, 물리기반, 사회문화 제도의 지속가능한 발전을 위한 대책을 논의하였다. 기술결정론 기반의 트랜스휴머니즘이 초래하는 인간과 기계의 갈등, 사이버 위협의 증가와 첨단화, 자율적인 기계가 초래할 새로운 위험, 신기술과 기존 창작문화 제도와의 갈등 등 초연결사회의 지속가능성을 와해할 수 있는 요인들에 대해서 논의하고 그 중 일부에 대해서 대책을 제시하였다. 그러나 이 연구가 파악하지 못한 복잡하고 다층적인 초연결사회의 지속가능성을 위협하는 요인들이 산적해 있을 것이며 초연결사회의 진전에 따라 새로이 등장할 요인들도 있을 것이다. 따라서 본 연구의 뒤를 잇는 후속 연구가 추진되어야 할 것으로 본다. 초연결사회가 초래할 새로운 기술문명의 지속가능성은 신기술이 만들어낼 인공물들의 사회적 수용성에 달려 있다고 볼 수 있으므로 향후 초연결사회의 지속가능성에 대한 연구는 신기술의 사회적 수용성에 대한 연구로 이어질 것으로 기대된다.

참 고 문 헌

강태욱(2017. 1. 23), “로봇의 법적 지위”, 《법률신문》, Retrieved from https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial=107556 (검색일: 2017. 6. 15).

과학기술정보통신부(2017. 11. 14.), “디지털콘텐츠 공정거래 콘퍼런스 개최”, 과학기술정보통신부 보도자료.

곽노필(2016. 6. 14.), “[AI] 인공지능, 시나리오 작가 데뷔…“창작이 별거냐””, 곽노필의 미래창, Retrieved from http://plug.hani.co.kr/futures/2663739 (검색일: 2017. 8. 8.).

국회검토보고서(2013), “저작권법 일부개정법률안”, 이군현의원 대표발의.

권용수(2016), “일본 정부, 인공지능(AI)의 창작물에도 저작권을 인정하는 법 정비 실시”, 《저작권 동향》, 제10호, 한국저작권위원회.

_____(2017), “[일본] 지식재산전략본부, 제4차 산업혁명의 기반이 되는 지식재산 시스템의 구축 방안을 담은 계획 발표.”, 《저작권 동향》, 제6호, 한국저작권위원회.

김대호 외(2015), 『인간, 초연결 사회를 살다』, 커뮤니케이션북스.

김범수 외(2014), “스마트기기 보급 확대에 따른 개인정보보호방안 연구 - 사물인터넷 환경을 중심으로”, 개인정보보호위원회.

김병운・고창열(2015), “초연결사회 도래에 따른 유선가입자망 도매제공 법제화 소고 - 접속유형 및 도매요금을 중심으로 -”, 《과학기술법연구》 제21집 제2호, 한남대학교 과학기술법연구원.

김병일(2017), “빅데이터 분석과 데이터 마이닝을 위한 저작권 제한”, 저작권법 60

주년 기념 세미나 발표집.

김수연 외(2010), “상용화전략을 위한 웨어러블 컴퓨터의 개념 연구”,《디지털디자인학연구》10(2), 한국디지털디자인협의회.

김윤명(2016), “인공지능(로봇)의 법적 쟁점에 대한 시론적 고찰”,《정보법학》, 제20권 제1호.

김정오 외(2017), 『법철학: 이론과 쟁점』, 박영사.

대외경제정책연구원(2017. 4. 26.), “2016년 인터넷 저작권 산업 규모 전년 대비 31.3%↑”, Retrieved from http://csf.kiep.go.kr/news/M001000000/view.do?articleId=23328 (검색일: 2017. 7. 3.).

류한석(2016), 『플랫폼, 시장의 지배자』, ㈜대성 KOREA.COM.

멈퍼드, 루이스(1952), 박홍규 역(2011), 『예술과 기술』, 텍스트.

문일환(2013),『저작권법상 공정이용 판단기준과 그 적용』, 동아법학.

미래창조과학부(2016. 12. 22.), “지식재산(IP)과 R&D연계전략으로 제4차 산업혁명 선도”, 미래창조과학부 보도자료.

_____(2017. 2. 17.), “「인공지능, 가상현실, 핀테크 규제혁신」방안 발표-4차 산업혁명, 지능정보사회를 견인할 핵심동력 및 유망 산업분야에 대한 선제적 규제개선 추진-”, 미래창조과학부 보도자료.

박남제(2016), “모의해킹 놀이 활동을 통한 초등 정보보호교육 STEAM 프로그램 개발 및 적용”,《정보교육학회논문지》제20권 제3호, pp. 273~282

박성호(2014),『저작권법』, 박영사.

박유리・최진원・김정언・이경남(2009), “방송통신콘텐츠 저작권의 효과적 보호에 관한 연구”, 방송통신위원회.

박유리・손상영・김창완・강하연・오정숙・김희연・정원준・신정우・문상현(2015), “인터넷의 진화와 사회경제적 패러다임 변화 연구: 사물인터넷을 중심으로,” 정보통신정책연구원.

박정은 외(2014), “초연결사회와 미래서비스”,《정보와 통신》제31권 제4호, 한국통

신학회.

박지순(2017), “4차 산업혁명 시대 일자리 확대를 위한 제도 개선 방안”, 지능정보사회 법제도 세미나 자료집, 한국정보화진흥원・지능정보사회 법제도 포럼.

배병환·송은지(2014), “주요국 사이버보안 전략 비교·분석 및 시사점”,《정보통신방송정책》, 제26권 제21호, 정보통신정책연구원.

백지연(2016), “[중국] 국가판권국, 〈2016년 중국 음악 산업 발전 보고서> 발표”,《저작권 동향》, 제24호, 한국저작권위원회

손상영·이원태·김희연·문정욱(2016), 『안전한 초연결사회를 위한 사회문화적 조건』, 경제인문사회연구회 협동연구총서 16-31-02 정보통신정책연구원.

송위진(2013),『창조도시의 혁신정책: 지속가능한 도시를 위한 시민참여형 혁신전략』, 과학기술정책연구원.

송담대학교 (2015), 『사이버보안체계 강화를 위한 정보보호법제 비교법 연구』, 한국인터넷진흥원.

송진·이영주(2015), 『방송영상 웹콘텐츠 현황 및 활성화 방안』, KOCCA 연구보고서 15-36, 한국콘텐츠진흥원.

심수민(2014),『웨어러블 디바이스 산업백서』, Digieco Focus, KT경제경영연구소.

심진보・최병철・노유나・하영욱(2017), 『대한민국 제4차 산업혁명, -새로운 미래를 위한 전략과 통찰, IDX』, 콘텐츠하다.

안태숙·이종민·박차욱·이형주·이수영(2013), 『저작권대리중개업체 사업현황 조사』, 저작권정책연구 2013-07, 한국저작권위원회.

양천수(2016), “현대 초연결사회와 새로운 인격권 보호체계”,《영남법학》제43집, 영남대학교 법학연구소.

엄주희(2017), “고령사회를 위한 사물인터넷 융합 디지털 헬스케어 사용자 경험 디자인 연구”, 박사학위논문, 한양대학교 대학원.

오승종(2016), 『저작권법』, 박영사.

유계환·김아름(2016), “일본 「지적재산 추진계획 2016」 의 주요내용 및 시사점”,

《심층분석 보고서》, 한국지식재산연구원.

유재홍·김윤명(2015), “온라인 개인 방송 플랫폼 확산 동향”,《월간 SW 중심사회》, 11월호, 소프트웨어정책연구소, pp.42~46.

윤미영・권정은(2013), “창조적 가치의 연결, 초연결사회의 도래”,《IT & Future Strategy》 제10호, 한국정보화진흥원.

윤순진(2012), “지속가능한 발전과 21세기 에너지정책”,《한국행정학보》 36권 3호, 한국행정학회.

윤혜선(2016), “인공지능을 둘러싼 법의 관심과 그 지향점에 관한 일고(一考)-미국의 인공지능과 법에 관한 논의 동향을 중심으로”,《KISO저널》, 제23호, 한국인터넷자율정책기구, pp. 23~28.

이대희(2010), “전자출판 및 디지털도서관 실현 방안” ,《계간 저작권》, 제23권 제1호, pp. 4~25.

이동철(2010), “사물지능통신관련 국내 사례 및 사업 추진 현황”,《Digieco Focus》, KT 경제경영연구소.

이상정·이영록·최진원(2016), “사적복제보상금제도 도입방연 연구”, 지식재산위원회.

이영록·최진원(2010), “법정허락제도 개선방안 연구”, 저작권연구., 한국저작권위원회.

이정진(2016. 7. 27.), “중국 음원시장에 부는 변화의 바람”, 대외경제정책연구원 중국 전문가포럼, Retrieved from http://csf.kiep.go.kr/issueInfo/M002000000/view.do?searchCategory=&articleId=19093&page=&searchKey=&searchString= (검색일: 2017. 9. 22.).

이종관(2017), “4차산업혁명을 향한 반성과 기획(가제),” 자문보고서 in 조성은 외(in press)《2017년 ICT 기반 사회현안문제 해결방안 연구》, 정보통신정책연구원.

이준복(2015), “사물인터넷시대에서 정보인권 보장을 위한 법적 고찰”,《홍익법학》 제16권 제3호, 홍익대학교 법학연구소.

이해완(2012),『저작권법』, 박영사.

_____(2015),『저작권법 3판』, 박영사.

이호영·김희연·김사혁·최항섭(2015),『초연결사회의 지속가능성을 위한 사회문화적 조건과 한국 사회의 대응(I): 총괄보고서』, 기본연구 15-14-01, 정보통신정책연구원.

이호영·이시직·이재현·김영생(2016),『초연결사회의 지속가능성을 위한 사회문화적 조건과 한국 사회의 대응(Ⅱ): 총괄보고서』, 기본연구 16-14-01, 정보통신정책연구원.

장우식 (2017. 5. 10.), "제4차 산업혁명 시대의 도래와 사이버 보안 위협", IGLOO SECURITY.

전승수(2012), "초연결 사회의 빅데이터 생태계 분석과 시사점",《KISTEP Issue Paper》2012-10, 한국과학기술기획평가원.

전재림·정진근·김창화·유지혜(2014),『네트워크 저장 서비스의 저작권법상 쟁점에 관한 연구』, 한국저작권위원회.

정법근(2015), "사물인터넷 시대의 C-P-N-D 생태계 동향",《정보통신방송정책》제27권 3호, 정보통신정책연구원.

정필운・고인석(2017), "인공지능윤리 가이드라인의 필요성과 제정 방향", 인공지능 윤리가이드라인, 그 필요성과 내용 토론회 자료집.

존 롤즈(2015),『정의론』, 홍성우 역, 새창미디어.

차상육(2017), "인공지능(AI)과 지적재산권의 새로운 쟁점-저작권법을 중심으로-",《2017 국제학술대회: 최근의 산업계 혁신과 지적재산권에 관한 국제적 논의》,［대구: 경북대학교］(개최일: 2017. 2. 7.).

최계영(2012), "스마트 시대 ICT 패러다임의 변화",《TTA Journal》Vol.143, 한국정보통신기술협회.

최상필(2012), "저작재산권 제한사유의 예시주의로의 전환에 관한 소고",《재산법연구》, 제29권 제3호, 한국저작권위원회.

최진원(2011), "권리자불명 저작물 활용 방안에 대한 비교법적 연구",《정보법학》, 제15권 제2호, pp. 217~254.

_____(2017), “저작물에 대한 링크와 법적책임에 관한 小考 - 사례 분석을 통한 합법과 위법 경계의 탐색 -”, 계간 저작권

_____·차세대콘텐츠재산학회 편(2017), 『디자인과 법』, 도서출판 채움.

최창현(2014), “C-P-N-D 생태계와 ICCT”, 《디지털융복합연구》 제12권 제3호, 한국디지털정책학회.

커넥팅랩(2014), 『사물인터넷, -클라우드와 빅데이터를 뛰어넘는 거대한 연결』, 미래의창.

하상익(2003), “저작권법상 법정허락제도에 대한 고찰-법경제학적 관점에서”, 서울대학교 대학원 법학과 석사학위논문.

한국저작권보호원(2016), 《저작권보호통계전문지 C STORY》, 제1호, 한국저작권보호원 침해예방기반팀.

_____(2017), 『2017 해외 저작권 보호 동향』, 한국저작권보호원 침해예방팀.

행정자치부·한국인터넷진흥원(2017), 『우리 기업을 위한 ‘유럽 일반 개인정보 보호법’ 안내서』.

2. 국외 문헌

文化審議會著作權分科會法制‧基本問題小委員會(2016). “リーチサイト等による侵害コンテンツへの誘導行爲の行爲類型”, 文化審議會著作權分科會法制‧基本問題小委員會（第４回）平成２８年１２月２７日, 配布資料.

佐藤謙二(2016). IT リテラシー教育の一環としての情報セキュリティ教育の要件について. 國士舘大學紀要情報科學第37号.

知的財産戰略本部檢証‧評価‧企畵委員會(2016). “次世代知財システム檢討委員會報告書”, 平成２８年４月, 41面.

AIOTI(2017). *Report on Workshop on Security & Privacy in IoT.*

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787-2805.

Bendovschi, A.(2015). "Cyber-attacks – trends, patterns and security countermeasures," *Procedia Economics and Finance, 28*, 24-31.

Bishop, M.(2010). Technology, training, and transformation. *IEEE Security & Privacy*, *8*(5), 72-75.

Bodeau, D. J. and Graubart R.(2011). *Cyber Resiliency Engineering Framework.* MITRE Technical Report, MTR110237.

Bonner, D.(2017. 4. 27.). *California Bill Mandates Privacy By Design For IoT Devices.* http://www.wcsr.com/Insights/Alerts/2017/April/California-Bill-Mandates-Privacy-By-Design-For-IoT-Devices(검색일: 2017. 6. 1.).

Cavoukian, A.(2014). Evolving FIPPs: proactive approaches to privacy, not privacy paternalism. In S. Gutwirth, R. Leenes and P. de Hert(eds.) *Reforming European Data Protection Law.* Volume 20 of the series Law, Governance and Technology Series pp. 293~309.

_____.(2016). *Embed Privacy by Design, or Risk losing Privacy Forever.* Retrieved from https://www.law.berkeley.edu/wp-content/uploads/2016/03/Ann-Cavoukian.pdf (검색일: 2017. 1. 7.).

_____ and Popa, C.(2016). *Embedding Privacy into What's Next: Privacy by Design for the Internet of Things.* Ryerson University Privacy & Big Data Institute, April 2016.

_____, Dix, A. and El-Emam, K.(2014. 3.). *The Unintended Consequences of Privacy Paternalism.* Information and Privacy Commissioner, Ontario, Canada.

Coraggio, G.(2015. 12. 31.). IoT in 2016: Privacy by design is the only way. Retrieved from https://inform.tmforum.org/features-and-analysis/2015/12/iot-in-2016-privacy-by-

design-is-the-only-way/

CCIA(2015). *Copyright Reform for a Digital Economy*.

Crompton, B., Thompson, D., Reyes, M., Zhao, X. and Zou, X.(2016). *Cybersecurity Awareness Shrewsbury Public Schools*. Clark University Clark Digital Commons.

Danon(2017). GDPR top ten #6: Privacy by Design and by Default . Retrieved from https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html (검색일: 2017. 11. 20.).

Dodge, R., and Ragsdale, D.(2005). Technology Education at the US Military Academy. *IEEE Security & Privacy*, *3*(2), 49-53.

ElShekeil, S. A., and Laoyookhong, S.(2017. 11.). *GDPR Privacy by Design.* Retrieved from http://www.isaca.org/chapters4/Sweden/OmOss/Documents/Stipendie2017_ElShekeil-Laoyookhong.pdf (검색일: 2017. 12. 20.).

ENISA(2012). *National Cyber Security Strategies: Practical Guide on Development and Execution.*

_____(2014). *Privacy and Data Protection by Design - From Policy to Engineering.*

_____(2015a) *Big Data Security: Good Practices and Recommendations on the Security of Big Data Systems.*

_____(2015b) *Privacy and Data Protection by Design -from Policy to Engineering.*

European Commission(2012). *The EU Approach to Resilience: Learning from Food Security Crises.* Communication from the Commission to the European Parliament and the Council.

_____(2016). Reform of EU data protection rules. Retrieved from http://ec.europa.eu/justice/data-protection/reform/index_en.htm (검색일: 2017. 2. 10.).

European Parliament(2016. 5. 31.). "Draft Report with recommendations to the Commission on Civil Law Rules on Robotics." Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%

2BV0//EN (검색일: 2017. 8. 18.).

Executive Office of the President(2014. 5). *Big Data: Seizing Opportunities, Preserving Values*. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (검색일: 2017. 11. 20.).

Federal Register(2016. 6. 27.). "Request for Information on Artificial Intelligence." Retrieved from https://www.federalregister.gov/documents/2016/06/27/2016-15082/request-for-information-on-artificial-intelligence (검색일: 2017. 8. 8.).

Felten, E.(2016. 5. 3.). "Preparing for the Future of Artificial Intelligence." The White House Blog. Retrieved from https://obamawhitehouse.archives.gov/blog/2016/05/03/preparing-future-artificial-intelligence (검색일: 2017. 10. 5.).

Fisher III, W. et al.(2012). Reflections on the Hope Poster Case, 25 HARV. J.L. & TECH. 243, 313 (Quoting William M. Landes & Daniel B. Levine, The Economic Analysis of Art Law, 1 HANDBOOK OF THE ECONOMICS OF ART AND CULTURE 211, 217 (2006)).

Giannakas, F., Kambourakis, G., Papasalouros, A. and Gritzalis, S.(2016). Security education and awareness for K-6 going mobile. *iJIM*, *10*(2), 41-48.

HM Government(2014). *Cyber Security Skills - Business Perspectives and Government's Next Steps*.

_____(2016). *National Cyber Security Strategy 2016 to 2021*. UK. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss- map/national_cyber_security_strategy_2016.pdf (검색일: 2017. 6. 15.)

Hunt, T.(2016). *Cyber Security Awareness in Higher Education*. Symposium Of University Research and Creative Expression(SOURCE).

IEEE(2016. 11. 16). *End-to-end Security and Privacy by Design for IoT*. Retrieved from http://sites.ieee.org/futuredirections/tech-policy-ethics/november-2016/end-to-end-security-and-privacy-by-design-for-iot/ (검색일: 2017. 6. 1.).

ISF(2017) *Threat Horizon 2019.* Information Security Forum

Irvine, C.(2011). The value of capture-the-flag exercises in education: an interview with Chris Eagle. *IEEE Security & Privacy*, *9*(6), 58-60.

Jeremy Rifkin(2000), The age of access : the new culture of hypercapitalism, where all of life is a paid-for experience, Putnam Publishing Group.

Keller, D.(2017). "OSPs and the DMCA", Seoul Copyright Forum 2017.

Kessler, G. C. and Ramsay, J. D.(2014, January). A proposed curriculum in cybersecurity education targeting homeland security students. In *2014 47th Hawaii International Conference on System Sciences (HICSS),* IEEE, 4932-4937.

Kirlappos, I. and Sasse, M. A.(2012). Security education against phishing: a modest proposal for a major rethink. *IEEE Security & Privacy*, *10*(2), 24-32.

Kreizman G. and Robertson B.(2006). *Incorporating Security Into the Enterprise Architecture Process.* Gartner.

Leval, P. N.(1990). "Toward a Fair Use Standard." *Harvard Law Review*. Vol. 103, pp. 1105~1136.

MacKenzie, Donald and Wajcman, Judy (1985). The Social Shaping of Technology, Milton Keynes: Open University Press.

Mahan, P.(2016. 8. 9). "Privacy by Design and the GDPR." Retrieved from https://www.isaca.org/chapters3/Atlanta/AboutOurChapter/Documents/GW2016/0809%20130-PMahan-PbD_and_GDPR.pdf (검색일: 2017. 1. 7.).

McGettrick, A., Cassel, L. N., Dark, M., Hawthorne, E. K. and Impagliazzo, J.(2014). Toward curricular guidelines for cybersecurity. In *Proceedings of the 45th ACM technical symposium on Computer Science Education* (pp. 81~82). ACM.

Mullin(2017. 6. 20.). Supreme Court turns down EFF's "Dancing Baby" fair use case," https://arstechnica.com/tech-policy/2017/06/supreme-court-wont-hear-dancing-baby-copyright-case;/.

Nevejans, N.(2016). *European Civil Law Rules in Robotics*. European Parliament.

National Science and Technology Council(2016a). *National Artificial intelligence Research and Development Strategic Plan.* Networking and Information Technology Research and Development Subcommittee, Executive Office of the President. Retrieved from https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf (검색일 : 2017. 11. 20.).

_____(2016b). *Preparing for the Future of Artificial Intelligence*. National Science and Technology Council committee on Tech nology, Executive Office of the President. Retrieved from https://obamawhite house.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/prepar ing_for_the_future_of_ai.pdf (검색일 : 2017. 11. 20.).

Perera, C., McCormick, C., Bandara, A. K., Price, B. A. and Nuseibeh, B.(2016. 11). Privacy-by-Design framework for assessing Internet of Things applications and platforms. In *Proceedings of the 6th International Conference on the Internet of Things* (pp. 83-92). ACM.

Pruitt-Mentle, D.(2008). 2008 National Cyberethics, *Cybersafety. Cybersecurity Baeline Study*. National Cyber Security Alliance.

Smith, Merritt Roe and Marx, Leo(1994). Does Technology Drive History? The Dilemma of Technological Determinism, Cambridge, MA: MIT Press.

Smith, S.(2016). “Smart Infrastructure for Urban Mobility.” Retrieved from https://cra.org/ccc/wp-content/uploads/sites/2/2016/06/Stephen-Smith-AI-slides.pdf (검색일: 2017. 10. 11.).

The Democratic Platform Committee(2016). “2016 Democratic Party Platform.” Retrieved from http://www.presidency.ucsb.edu/papers_pdf/117717.pdf (검색일: 2017. 6. 1.).

The Republican Platform Committee(2016). “2016 Republican Party Platform” Retrieved from https://prod-cdn-static.gop.com/static/home/data/platform.pdf (검색일: 2017. 6. 1.).

Thomas H. Davenport (2014). Big Data at Work: Dispelling the Myths, Uncovering the Opportunities, Harvard Business School Publishing..

U.S. Copyright Office(1998). “The Digital Millennium Copyright Act of 1998.” Retrieved from https://www.copyright.gov/legislation/dmca.pdf (검색일: 2017. 10. 11.).

_____(2016). “Copyright Law of the United States.” Retrieved from https://www.copyright.gov/title17/title17.pdf (검색일: 2017. 10. 11.).

U.S. Department of Commerce(2013). *Copyright Policy, Creativity, and Innovation in the Digital Economy*.

U.S. Department of Homeland Security(2006). National Infrastructure Protection Plan.

_____(2009). National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency.

_____(2013). National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience.

_____(2016). *Strategic Principles for Securing the Internet of Things(IoT) Version 1.0*. Retrieved from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINApdf (검색일 : 2017. 11. 20.).

Wing, J. M. (2006). Computational thinking. *Communications of the ACM*, *49*(3), 33-35.

WWR(2017). *Big Data Security policies: Serving Security, Protecting Freedom*. WRR-Policy Brief 6. Retrieved from https://www.wrr.nl/publicaties/policy-briefs/2017/01/31/big-data-and-security-policies-serving-security-protecting-freedom (검색일: 2017. 11. 20.).

3. 기타 자료

《경향비즈》 (2017. 7. 3.), “국내 최대 가상화폐 거래소, ‘빗썸’ 해킹의 전말”. Retrieved

from http://biz.khan.co.kr/khan_art_view.html?artid=201707031758001&code=920100#csidx80691a4837058d29949af2564a054e5 (검색일: 2017. 11. 10.).

《뉴스위크》(2016. 8. 8.), “내 사진이 몇 초만에 인상파 작품으로”, Retrieved from http://newsweekkorea.com/?p=4646 (검색일: 2017. 9. 13.).

《디지털타임스》(2017. 2. 26.), ““360도 VR영상 등 저작권 보호하자”, 디지털 워터마킹 기술개발 가속도”, Retrieved from http://www.dt.co.kr/contents.html?article_no=2017022702101560753001 (검색일: 2017. 5. 20.).

《디지털타임스》(2017. 4. 5.), ““인공지능 vs 인간’ 저작권 분쟁시대 온다”, Retrieved from http://www.dt.co.kr/contents.html?article_no=2017040602100151102001 (검색일: 2017. 6. 16.).

《디지털타임즈》(2017. 4. 14.), “웹 콘텐츠 강화하는 네이버 … 자회사 제작 웹드라마 인기”, Retrieved from http://www.dt.co.kr/contents.html?article_no=2017041402101331043001 (검색일: 2017. 5. 25.).

《디지털타임즈》(2017. 8. 24.), “카카오, ‘로엔’ 주축 자체 제작 동영상 강화” Retrieved from http://www.dt.co.kr/contents.html?article_no=2017082502101231043001 (검색일: 2017. 10. 11.).

《보안뉴스》(2016. 10. 6.), “도입 20개월 남은 GDPR, 실제로 바뀌어야 하는 것들”. Retrieved from http://www.boannews.com/media/view.asp?idx=51967&kind=4 (검색일: 2017. 3. 2.).

《보안뉴스》(2016. 11. 17.), “도박 사이트 타깃으로 일확천금 노리는 해커들 어쩌나”. Retrieved from http://www.boannews.com/media/view.asp?idx=52402 (검색일: 2017. 3. 2.).

《블로터》(2016. 10. 26.), ““대도서관 사태’로 보는 아프리카TV…플랫폼인가, 미디어인가”, Retrieved from http://www.bloter.net/archives/266251 (검색일: 2017. 4. 29.).

《블로터》(2017. 1. 24.), “구글, VR 창작도구 ‘틸트브러시 툴킷’ 오픈소스로 공개”, Retrieved from http://www.bloter.net/archives/271061 (검색일: 2017. 9. 29.).

《비즈니스포스트》(2017. 4. 28.), “아프리카TV, BJ 이탈 수습해 1분기 매출 신기록”, Retrieved from http://www.businesspost.co.kr/BP?command=print&idxno=48266 (검색일: 2017. 6. 17.).

《아이뉴스24》(2017. 7. 7.), “산업제어시스템(ICS)까지…랜섬웨어 '경보'”. Retrieved from http://news.inews24.com/php/news_view.php?g_serial=1034165&g_menu=02020 (검색일: 2017. 10. 2.).

안랩 (2016. 5. 2.), “랜섬웨어의 표적형 공격, 의료기관 겨냥하나”. Retrieved from http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=24948 (검색일: 2017. 10. 2.).

《연합뉴스》(2016. 5. 16), “카메라 셔터 소리 싫어서…아이폰 해외 직구매 는다”, Retrieved from http://www.yonhapnews.co.kr/bulletin/2016/05/15/0200000000AKR20160515043500017.HTML?input=1195m (검색일: 2017. 10. 17).

이은우 (2016. 7. 10.), “유럽은 지금 통합개인정보보호 법규(GDPR)로의 이행기”. 《보안뉴스》, Retrieved from http://www.boannews.com/media/view.asp?idx =51126 (검색일: 2017. 8. 1.).

일본 “2016년 지식재산추진계획(2016 知的財産推進計畫)”, Retrieved from https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20160509.pdf (검색일: 2017. 7. 18.).

일본 “2017년 지식재산추진계획(2017 知的財産推進計畫)”, Retrieved from https://www.kantei.go.jp/jp/singi/titeki2/kettei/chizaikeikaku20170516.pdf(검색일: 2017. 7. 18.).

《전자신문》(2016. 1. 26.), “인공지능이 만든 음악...저작권은 누구에게?”, Retrieved from http://www.etnews.com/20160126000269 (검색일: 2017. 10. 20.).

《중기이코노미》(2016. 8. 24.), “‘표준계약서’로 디지털콘텐츠 불공정거래 예방”, Retrieved from http://www.junggi.co.kr/article/articleView.html?no=16216&cate1=2&cate2=4&prevPagename=articleList.html&page=6 (검색일: 2017. 11. 1.).

《지디넷》(2017. 4. 18.), “미래부, 콘텐츠 거래사실 인증사업 확대 실시”, Retrieved from http://www.zdnet.co.kr/news/news_view.asp?artice_id=20170418111238 (검색일: 2017. 11. 11.).

《파이낸셜뉴스》(2016. 1. 21.), “코스피 4.92포인트 하락, 1840.53포인트 거래 마감”, Retrieved from http://www.fnnews.com/news/201601211516540123 (검색일: 2017. 4. 3.).

《한겨레》 (2009. 6. 24.), “5살 꼬마 동영상도 저작권 침해?”, Retrieved from http://www.hani.co.kr/arti/society/society_general/362163.html#csidxf76bc3907ef79cd91ce5a4653662790 (검색일: 2017. 10. 2.).

《한국경제매거진》 (2017. 6. 21.), “1인방송 산업, 한계는 없다”, Retrieved from http://magazine.hankyung.com/business/apps/news?popup=0&nid=01&c1=1003&nkey=2017061901125000201&mode=sub_view (검색일: 2017. 9. 5.).

《한국일보》 (2017. 7. 18.), “‘옥자’의 힘… 넷플릭스 이용자 2주 새 2배 뛰었다”, Retrieved from http://www.hankookilbo.com/v/999cc8f8f7664b36b6bbee3919ee4187 (검색일: 2017. 8. 21.).

《ITWorld》(2017. 1. 6.), ““모든 윈도우 10 PC를 창작 도구로” 델, 캔버스 27 공개”, Retrieved from http://www.itworld.co.kr/print/102882 (검색일: 2017. 9. 6.).

《Tech M》(2016. 8. 11.) “강력한 EU 개인정보보호법 시행 대비 가이드라인 만든다”. Retrieved from http://techm.kr/bbs/board.php?bo_table=article&wr_id=2458 (검색일: 2017. 6. 1.).

한국저작권위원회 원격평생교육원(http://edulife.copyright.or.kr) (검색일: 2017. 10. 3.).

한국저작권보호원 - 설립목적 및 연혁(https://www.kcopa.or.kr/lay1/S1T9C71/contents.do) (검색일: 2017. 10. 3.).

한국저작권위원회 용어사전 - 2차적저작물작성권(https://www.copyright.or.kr/information-materials/dictionary/view.do?glossaryNo=446&pageIndex=1&searchLangType=&searchkeyword=&pageDisplaySize=10&searchIdx=&searchText=&clscode=01

&searchTarget=) (검색일: 2017. 11. 29.).

한국저작권위원회 용어사전 - 동일성유지권(https://www.copyright.or.kr/information-materials/dictionary/view.do?glossaryNo=379&pageIndex=9&searchLangType=&searchkeyword=&pageDisplaySize=10&searchIdx=&searchText=&clscode=01&searchTarget=) (검색일: 2017. 11. 1.).

한국저작권위원회 용어사전 - 성명표시권(https://www.copyright.or.kr/information-materials/dictionary/view.do?glossaryNo=396&pageIndex=10&searchLangType=&searchkeyword=&pageDisplaySize=10&searchIdx=&searchText=&clscode=01&searchTarget=) (검색일: 2017. 11. 1.).

Blanch v. Koons, 467 F.3d 244, 251-252 (2d. Cir. 2006).

CCKorea - CC라이선스(http://ccl.cckorea.org/about/) (검색일: 2017. 10. 20.).

Deep Dream Feed(https://deepdreamgenerator.com/feed/) (검색일: 2017. 10. 3.).

Deep Dream Generator(http://deepdreamgenerator.com/) (검색일: 2017. 9. 8.).

Deep Dream web interface(http://psychic-vr-lab.com/deepdream/) (검색일: 2017. 10. 17.).

Government Computer News(2007. 3. 18.). "FISMA efficiency questioned, 2007". Retrieved from https://gcn.com/Articles/2007/03/18/FISM As-effectiveness-questioned.aspx?Page=2 (검색일 : 2017. 1. 12.).

Government Computer News(2009. 6. 10.). "Keith Rhodes | Effective IT security starts with risk analysis, former GAO CTO says". Retrieved from https://gcn.com/articles/2009/06/15/interview-keith-rhodes-it-security.aspx (검색일 : 2017. 1. 12.).

Reuters(2016. 2. 10.). "Exclusive : In boost to self-driving cars, U.S. tells Google computers can qualify as drivers." Retrieved from https://www.reuters.com/article/us-alphabet-autos-selfdriving-exclusive/exclusive-in-boost-to-self-driving-cars-u-s-tells-google-computers-can-qualify-as-drivers-idUSKCN0VJ00H (검색일: 2017. 4. 20.).

The Next Rembrandt(https://www.nextrembrandt.com/) (검색일: 2017. 10. 22.).

The Verge(2017. 4. 12.). "This music video was created by an algorithm that turns soun

d frequencies into landscapes.” Retrieved from https://www.theverge.com/tldr/2017/4/12/15270026/music-video-algorithm-victor-doval-howler-monkey (검색일: 2017. 8. 31.).

Wikipedia, ‘Privacy by design’. Retrieved from https://en.wikipedia.org/wiki/Privacy_by_design (검색일: 2017. 8. 1.).

「전자금융거래법」 제21조. (국가법령정보센터, Retrieved from http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B1%B0%EB%9E%98%EB%B2%95).

「정보통신기반보호법」 제9조, 제13조. (국가법령정보센터, Retrieved from http://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EA%B8%B0%EB%B0%98%20%EB%B3%B4%ED%98%B8%EB%B2%95).

「정보통신망법」 제48조. (국가법령정보센터, Retrieved from http://www.law.go.kr/lsInfoP.do?lsiSeq=123210#0000).

대법원 2009. 11. 26. 선고 2008다77405 판결.

대법원 2015. 8. 19. 선고 2015도5789 판결.

대법원 2016. 5. 26. 선고 2015도16701 판결.

서울중앙지방법원 2008. 8. 5. 선고 2008카합968 판결.

서울중앙지방법원 2008. 11. 14. 선고 2007가단70153 판결.

Blanch v. Koons, 467 F.3d 244 (2d Cir. 2006).

http://blog.naver.com/facemaker111/221006130150 (검색일: 2017. 7. 10.).

https://blog.naver.com/with_msip/220996692452 (검색일: 2017. 7. 10.)

http://greenjournal.co.kr/220273179905 (검색일: 2017. 7. 10.).

http://www.heritage.org/defense/report/cybersecurity-act-2012-revised-cyber-bill-still-has-problems (검색일: 2017. 6. 15.).

http://www.information-age.com/10-cyber-security-trends-look-2017-123463680/ (검색일:

2017. 6. 15.).

https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-initiatives-working-towards-more-secure-online-environment (검색일: 2017. 6. 15.).

https://en.wikipedia.org/wiki/Cyber-security_regulation (검색일: 2017. 10. 8.).

https://en.wikipedia.org/wiki/Cyber_Resilience_Review (검색일: 2017. 10. 15.).

https://en.wikipedia.org/wiki/Dark_web (검색일: 2017. 6. 15.).

https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (검색일: 2017. 11. 11.).

https://www.govtrack.us/congress/ bills/114/hr1731 (검색일: 2017. 6. 15.).

https://www.law360.com/articles/745523/a-guide-to-the-cybersecurity-act-of-2015 (검색일: 2017. 6. 15.).

https://www.lawfareblog.com/cybersecurity-act-2015 (검색일: 2017. 6. 15.).

https://www.symantec.com/security-center/threat-report (검색일: 2017. 7. 10.).

https://www.upwork.com/hiring/development/trends-in-cyber-security-threats-and-how-to-prevent-them/ (검색일: 2017. 6. 15.).

정보통신정책연구원 기본연구 안내

▌2015 기본연구

기본연구 15－01 인터넷의 진화와 사회경제적 패러다임 변화 연구: 사물인터넷을 중심으로(박유리, 손상영, 김창완, 강하연, 오정숙, 김희연, 정원준, 신정우, 문상현)

기본연구 15－02 방송영상산업 생산요소시장의 구조와 거래유형에 대한 연구(황유선, 박동욱, 김호정)

기본연구 15－03 빅데이터 시대 개인 행태 정보 수집 및 활용에 대한 정책 연구(조성은, 이시직)

기본연구 15－04 ICT 무역 글로벌 패러다임 변화에 따른 대응 방안(강하연, 윤승환, 박은지, 박영덕, 김재형)

기본연구 15－05 한중 ICT기업의 해외진출 방식 비교와 시사점(김성옥, 전민경, 한동교, 김준연)

기본연구 15－06 우체국 MVNO 위탁판매사업의 소비자 효용 증대 효과 추정(최중범, 김민진, 심송보)

기본연구 15－07 ICT 벤처기업의 생애주기 추적조사 연구(조유리, 강유리)

기본연구 15－08 주파수 공동사용 현황 및 도입 방안 연구(김지환, 정아름, 임동민)

기본연구 15－09 미디어 상품의 문화적 할인 지수 개발에 대한 연구(곽동균, 정은진, 장원호, 남기범, 김상현)

기본연구 15－10 비선형적(Non-linear) TV 시청환경에서 수용자의 매체 이용행태 변화 및 파급효과에 관한 연구(심홍진, 주성희, 임소혜, 이해미)

기본연구 15－11 거시경제 및 제조업 구조와 ICT 산업 간 관계분석 모형(주재욱, 김욱준, 하형석)

기본연구 15－12 우정사업의 신사업 추진을 위한 조직민첩성 진단(이용수, 안명옥, 김종근)

협동연구총서 15－13－01 과학기술과 ICT 활용을 통한 생산성 향상 방향 연구 및 경제 통계 구축(I) 총괄보고서: 과학기술과 ICT 활용을 통한 생산성 향상 방향 연구 및 경제 통계 구축(김정언, 정현준, 진홍윤, 신우철, 문성배, 신석하, 전현배, 조태형, 이영수, 양현석)

협동연구총서 15－14－01 초연결사회의 지속가능성을 위한 사회문화적 조건과 한국 사회의 대응(I): 총괄보고서(이호영, 김희연, 김사혁, 최항섭)

▌2016 기본연구

기본연구 16－01 O2O 비즈니스 확산에 따른 시장 변화 및 정책 방안 연구(박유리, 오정숙, 양수연, 임세실, 최 충, 최동욱)

기본연구 16－02 ICT 혁신에 대응하는 플랫폼 육성 전략연구(최계영, 김민식, 최주한)

기본연구 16－03 모바일 웹과 앱의 이용패턴 비교와 모바일 인터넷 서비스의 생태계(정광재, 이보겸)

기본연구 16－04 방송영상산업 생산요소시장의 계약유형에 대한 연구－예능오락부문을 중심으로(황유선, 김호정)

기본연구 16－05 모바일 인터넷 시대의 방송콘텐츠 서비스 활성화 방안 연구(심홍진, 주성희, 임소혜, 이주영)

기본연구 16－06 ICT산업 정책의 거시경제적 효과 분석을 통한 정책 방향 연구(고동환, 정부연)

기본연구 16－07 우체국보험 수익구조 진단 및 개선 방안 연구(이석범, 이경은, 최승재, 류근옥, 박성용, 류성경)

기본연구 16－08 기업의 개방형 혁신전략이 ICT융합 성과에 미치는 영향력 분석(남충현, 정원준, 김규남)

기본연구 16－09 지능정보사회의 규범체계 정립을 위한 법·제도 연구(이원태, 문정욱, 이시직, 심우민, 강일신)

기본연구 16－10 이동통신사업자의 투자 결정 요인에 관한 연구(정 훈, 박상미, 전홍민, 김인혜)

기본연구 16－11 불확실성하에서의 이동통신요금제 선택에 관한 연구(이민석, 이솔희)

기본연구 16－12 우체국 특성 분석에 따른 미래 우체국 운영 방안(이용수, 안명옥, 김영규)

협동연구총서 16－13－01 과학기술과 ICT 활용을 통한 생산성 향상 방향 연구 및 경제통계 구축(Ⅱ): 총괄보고서 (김정언, 정현준, 김경훈, 진홍윤, 신우철)

협동연구총서 16－14－01 초연결사회의 지속가능성을 위한 사회문화적 조건과 한국 사회의 대응(Ⅱ): 총괄보고서(이호영, 손상영, 이원태, 조성은, 문정욱, 김희연, 이시직, 양수연, 이재현, 이정엽)

협동연구총서 16－15－01 ICT 벤처생태계의 변화 분석을 위한 패널데이터 구축 및 정

책방향 연구(I): 총괄보고서(조유리, 남충현, 이은민, 손가녕, 김도훈, 오동현)

협동연구총서 16－16－01 조사환경 변화에 대응한 ICT 통계 생산체계 혁신 방안 연구(Ⅰ): 총괄보고서(정용찬, 주재욱, 이원태, 김윤화, 유선실, 김욱준, 오윤석, 박민규, 황용석, 황선웅)

▌2017 기본연구

기본연구 17－01 지능정보사회의 공공정보화 패러다임 변화와 미래정책 연구(이원태, 문정욱, 류현숙)

기본연구 17－02 ICT가 고용구조에 미치는 영향 분석(이학기, 이경남)

기본연구 17－03 ICT 융합 대중소기업 상생을 위한 생태계 조성 방안 연구(강준모, 김민식, 이슬기)

기본연구 17－04 ICT 정책에서 빅데이터 분석의 활용방안 연구(김경훈, 이선희, 오윤석, 양수연, 송태민)

기본연구 17－05 사물인터넷 생태계의 경쟁 이슈와 정책과제(이민석, 박상미, 김성준)

기본연구 17－06 비면허 대역 주파수의 활용 동향 및 경제적 가치 추정 방법론 연구(김희천, 임동민, 정아름, 김인희)

기본연구 17－07 모바일 동영상 서비스의 광고효과에 관한 연구(주성희, 심홍진, 김청희)

기본연구 17－08 유료방송서비스 간 대체성에 관한 연구: 수요함수 추정을 통한 실증분석(황유선, 육은희)

기본연구 17－09 ICT 수출 주요 결정요인과 그 영향 분석(고동환, 최지혜)

기본연구 17－10 컨조인트 분석을 통한 우체국 제휴사업 효과 분석(박재석, 김민진, 김지혜)

협동연구총서 17－11－01 초연결사회의 지속가능성을 위한 사회문화적 조건과 한국사회의 대응(III): 총괄보고서 (손상영, 박유리, 이호영, 조성은, 김희연, 양수연, 이시직)

협동연구총서 17－12－01 ICT 벤처생태계의 변화 분석을 위한 패널데이터 구축 및 정책방향 연구(Ⅱ): 총괄보고서(조성은, 조유리, 강준모, 이학기, 민대홍, 이은민, 손가녕)

협동연구총서 17－13－01 과학기술과 ICT 활용을 통한 생산성 향상 방향 연구 및 경제 통계 구축(III): 총괄보고서(정현준, 김정언, 김경훈, 남충현,

신우철, 김도완)

협동연구총서 17－14－01 조사환경 변화에 대응한 ICT 통계 생산체계 혁신 방안 연구(Ⅱ): 총괄보고서(정용찬, 이원태, 정혁, 김윤화, 유선실, 정부연, 오윤석, 박민규, 권헌영, 오형나)

정보통신정책연구원 정책연구 안내

▌2015 정책연구

정책연구 15－01 SW융합 핵심기술분야의 현황 및 전망 (김규남, 이경선, 이경남, 이대호)

정책연구 15－02 과학기술・ICT 융합 유망분야 진흥 및 성과측정을 통한 창조경제 구현방안 (최계영, 이경선, 김규남, 김민식, 이경남, 허성욱)

정책연구 15－03 ICT 산업 현황 분석과 대응방향 연구 (정현준, 박유리, 진홍윤, 이인수)

정책연구 15－04 공영 TV홈쇼핑의 운영 차별화 방안 (이종원, 박민성, 김혜성)

정책연구 15－05 ICT통계 관리체계 개선방안 연구 (정용찬, 정 혁, 신지형, 김윤화, 하형석)

정책연구 15－06 남북 ICT(통신・우편・방송) 통합인프라 구축방안 (김철완, 김성옥, 최중범, 박재석, 서소영, 이우섭, 정아름)

정책연구 15－07 환경변화에 대응한 배달 최적화 모델 연구 (최중범, 이영종, 황병일)

정책연구 15－08 우정IT 조직의 역할 재정립과 발전전략 마련 (이용수, 안명옥)

정책연구 15－09 재난안전통신망 구축 총사업비 검증 (손상영, 김사혁)

정책연구 15－10 방송콘텐츠 기반확충을 위한 국내외 사례분석 및 정책방향 연구 (박동욱, 심홍진, 황준호, 정은진)

정책연구 15－11 주요국의 과학기술벤처 창업환경과 정책지원체계 비교 연구 (최계영, 강유리, 김민식, 송민선, 정원준, 이두진, 김대환)

정책연구 15－12 통신시장 경쟁상황 평가(2015년도) (정진한, 김득원, 김상용, 김용재, 김창완, 김현수, 이민석, 이종화, 정광재, 정 훈, 강인규, 김대건, 김주현, 김진호, 나상우, 송용택, 오기석, 임동민, 홍현기)

정책연구 15－13 인터넷 경제 시대의 정책방향 정립에 관한 연구(박유리, 이경선, 이경남, 송민선, 정원준, 오인하, 이상직)

정책연구 15－14 중소SW기업의 M&A 활성화 방안(나성현, 강유리)

정책연구 15－15 창업생태계 선순환을 위한 연쇄창업가 지원방안 연구(조유리, 고동환, 정원준)

정책연구 15－16 통신시장의 IP화와 C-P-N-D 생태계 확산에 대응한 중장기 통신정책방안 연구 (이종화, 김민철, 송용택)

정책연구 15－17 신규사업자 진입 정책사례 연구 (정진한, 김창완, 김득원, 나상우, 이보겸)

정책연구 15－18 ’16～’17년도 접속원가 산정 및 유・무선 데이터 이용 확산을 고려한

통화량 예측 모형 개선방안 연구 (김민철, 오기석, 김진호, 김대건)

정책연구 15－19 ICT 생태계 확산에 대응한 보편적 역무 제도 개편 방향 연구 (정 훈, 나상우)

정책연구 15－20 MVNO 시장의 경쟁력 강화를 위한 정책방향 수립 및 서비스 다양화 가능성에 대한 연구 (정광재, 김대건)

정책연구 15－21 단말기 유통구조 정상화 및 이용자 편익 증진을 위한 제도개선방안 연구 (김민철, 이종화, 강인규, 이보겸)

정책연구 15－22 데이터 기반 이동통신 요금제 정착을 위한 요금체계 개선방안 및 이용자 편익 증대방안 연구(김용재, 오기석, 김인혜)

정책연구 15－23 규제비용총량제 도입을 위한 비용분석 방안 연구 (초성운, 정광재, 황유선, 오기석, 박희영)

정책연구 15－24 지역방송발전지원 특별법의 실효적 시행방안 연구 (심홍진, 황준호, 박희영)

정책연구 15－25 방송매체 환경 변화에 따른 방송평가 지표 연구 (주성희, 성욱제, 이미라)

정책연구 15－26 보도 콘텐츠의 구성요소 분석 및 법제 정비방안 연구 (김남두, 우혜진)

정책연구 15－27 미디어 다양성 지표의 시범적용 분석 (성욱제, 김남두, 이미라, 정은진)

정책연구 15－28 방송－ICT 융합 시대의 매체간 합산 영향력지수 정책방안 연구 (곽동균, 김남두, 우혜진)

정책연구 15－29 지상파 다채널방송 도입을 위한 정책방안 연구: 단계별 정책목표와 실행방안을 중심으로 (김태오, 김호정)

정책연구 15－30 개인정보보호 이슈의 지형변화와 국제규범의 형성 연구 (이원태, 이시직, 심우민, 강일신)

정책연구 15－31 통일대비 남북 방송통신 교류협력센터 추진방안 연구 (김철완, 김성옥, 서소영, 이우섭, 서홍수)

정책연구 15－32 FTA 시대 국내제작물 규제 정비방안 (강하연, 주성희, 노은정)

정책연구 15－33 공정경쟁 활성화를 위한 방송・통신 결합판매 규제제도 개선방안 연구 (김창완, 강준석, 강인규)

정책연구 15－34 인터넷 동영상 서비스에 대한 합리적 제도화 방안 연구 (곽동균, 권용재, 김호정, 박희영)

정책연구 15－35 디지털사이니지 산업 규제개선 및 진흥정책 연구(김태오, 곽동균, 김호정)

정책연구 15－36 통합 시청조사 결과의 제도화 및 활용방안에 관한 연구 (성욱제, 김태오, 정은진, 박상진)

정책연구 15－37 사물인터넷 실증사업의 경제적 파급효과 분석 (김규남, 이은민, 정원준, 최남희)

정책연구 15－38 계좌이동제 시행에 따른 우체국예금의 대응전략 및 실행방안 (박재석, 김민진, 황병일, 하정랑)

정책연구 15－39 ICT 기업 성장 요인 및 특성 분석 (정현준, 정 혁, 진홍윤, 신우철)

정책연구 15－40 ICT 산업분야 한・중・미・일 경쟁력 비교분석과 대응방안 (이경선, 남충현, 김민식, 신우철, 이대호)

정책연구 15－41 ICT 산업 중장기 전망(2016~2020년) 및 대응전략 (정 혁, 최계영, 정용찬, 김창완, 정현준, 고동환, 남충현, 이은민, 김민식, 오정숙, 이경남, 강유리, 진홍윤, 유선실, 나상우, 김대건)

정책연구 15－42 정부 창업지원사업의 효과성 제고방안 연구 (나성현, 김민식, 강유리 진홍윤)

정책연구 15－43 IT・금융 융합 규제개선 연구 (조유리, 송민선, 이준희)

정책연구 15－44 방송통신 결합판매 규제 개선방안 연구 (김현수, 정 훈, 김대건, 송용택)

정책연구 15－45 미디어 환경변화에 따른 방송정책의 기본방향과 과제 (황준호, 성욱제, 주성희, 김호정, 우혜진, 이해미)

정책연구 15－46 방송 서비스 고도화를 위한 지상파 UHD 방송 및 방송주파수 정책방안 연구 (김남두, 이종원, 김상용, 정광재, 김주현, 박상진)

정책연구 15－47 2016년 방송통신 분야 시장 전망 및 정책 방안 연구 (초성운, 정용찬, 정 훈, 정 혁, 유선실, 권용재)

정책연구 15－48 방송 콘텐츠 공정거래환경 조성방안 연구: 외주제작사의 간접광고 시행방안 및 스포츠 중계권거래 제도개선을 중심으로 (주성희, 임세진, 정은진)

정책연구 15－49 매체환경 변화에 대응한 규제개선 연구 (이종원, 김태오, 권용재)

정책연구 15－50 방송시장 환경변화에 대응한 유료방송 요금 규제 및 수신료 배분 체계 개선 방안 연구 (강준석, 황유선, 권용재)

정책연구 15－51 유료방송 제도개선을 위한 시장현황 분석 (이재영, 유선실, 박선영)

정책연구 15－52 주요 통신서비스별 시장상황 자료 수집・분석 (김현수, 정 훈, 강인규, 홍현기, 김대건)

정책연구 15－53－01 2015 방송통신통상협상력강화 사업 결과보고서 (강하연, 윤승환, 박은지, 김재형, 노은정)

정책연구 15－53－02 2015 FTA 협상대상국 방송통신서비스 시장개방 및 규제제도 현황

(강하연, 박은지, 김재형, 노은정)

정책연구 15－54 2015년도 남북 정보통신 교류협력 촉진사업 결과보고서 (김철완, 김봉식, 서소영, 이우섭)

정책연구 15－55 ICT 인문사회 혁신기반 구축(Ⅲ) 총괄보고서 (조성은, 이호영, 손상영, 이원태, 강홍렬, 한은영, 김사혁, 김희연, 이시직, 홍성욱, 이종관, 남 영)

정책연구 15－56 ICT 인문사회 혁신기반 구축(Ⅲ): 디지털 세대와 미래기술 수용(이호영, 김희연, 김석호, 이윤석)

정책연구 15－57 ICT 인문사회 혁신기반 구축(Ⅲ): 디지털 기술・매체환경에서 창작의 변화 (이원태, 김희연, 유승호, 류한석)

정책연구 15－58 ICT 인문사회 혁신기반 구축(Ⅲ): 웰니스케어 확산과 미래 의료시스템 (조성은, 이시직, 이일학, 정지훈)

정책연구 15－59 ICT 인문사회 혁신기반 구축(Ⅲ): 공유경제 비즈니스 모델과 새로운 경제 규범 (손상영, 김사혁)

정책연구 15－60 2015년도 우정동향 조사 분석 (정진하, 이석범, 최중범, 안명옥, 이영종, 이경은, 박소연, 김민진, 최승재)

정책연구 15－61 국가 간 정산제도 및 UPU우편사업 전략 연구 (정진하, 최중범, 이경은)

정책연구 15－62 우체국 국제물류사업 진출 전략 (정진하, 이용수, 이영종, 박소연, 황병일, 김윤관)

정책연구 15－63 우체국금융 핀테크 도입을 위한 실증적 추진 전략 (정진하, 박재석, 김민진, 황병일, 하정랑)

정책연구 15－64 우체국보험 영업조직 효율적 운영 방안 (정진하, 이석범, 안명옥, 최승재, 심송보)

▌2016 정책연구

정책연구 16－01 ICT 발전에 따른 산업 및 기술수준별 고용효과 분석 및 정책방향 정립 (주재욱, 정부연)

정책연구 16－02 신규 이용 주파수의 효율적 활용관리・방안 연구(김상용, 김주현, 정아름)

정책연구 16－03 스마트시대에 대응한 방송광고분류체계 개선방안 연구(강준석, 주성희, 이미라, 정은진)

정책연구 16－04 SDGs체제 하에서 과학기술 ODA의 역할 및 효과성 제고방안 연구

(강인수, 김태은, 유성훈, 김진주, 정유미, 조수미)

정책연구 16－05 기술중립성 확보를 위한 방송제도 개선방안 연구(이종원, 김태오, 권용재)

정책연구 16－06 SW중심사회의 일자리 정책방향 연구(정 혁, 이경선, 이경남, 남충현, 이경남, 손가녕, 이 호, 임영모, 서영빈, 이동현, 최창옥)

정책연구 16－07 All-IP 네트워크로의 이전과 ICT 생태계 출현에 따른 전기통신사업법상 역무・사업자 분류체계 (이민석, 이종화, 송용택)

정책연구 16－08 ICT 개발협력 성과제고 및 전략적 이행방안 연구(강인수, 김태은, 유성훈, 송영민, 심수민, 조수미)

정책연구 16－09 데이터 기반 디지털 경제의 미래예측 방법론 연구(주재욱, 정용찬, 이원태, 신지형, 정부연, 김욱준, 이성호, 이대호, 김문조, 이왕원, 정지연, 김도훈, 김학준, 김남혁, 조문래, 나영민, 권영민, 조수진, 김근진)

정책연구 16－10 통일준비 ICT 통합기반 조성을 위한 정책과제 연구(김철완, 서소영, 이우섭, 서홍수)

정책연구 16－11 지능사회 구현을 위한 정보화 추진전략 개편방안 연구(최계영, 박유리, 이은민, 김규남)

정책연구 16－12 ICT 벤처지원 정책 개선방안 및 글로벌 벤처 생태계 조성방안 연구(남충현, 이은민, 손가녕, 오승환, 김규남)

정책연구 16－13 데이터 중심으로의 이동통신 패러다임 전환에 따른 미래 주파수 정책 방향 연구(김지환, 김득원, 김상용, 임동민, 김주현, 정아름, 김 철)

정책연구 16－14 5G 시대를 대비한 주파수 대가 산정 및 할당절차에 대한 연구(김지환, 김인희, 정아름)

정책연구 16－15 재난안전통신망 시범사업결과에 따른 총사업비 재검증－단말기 경제성 확보방안을 중심으로－(강홍렬, 한은영)

정책연구 16－16 OTT 동영상 시장 현황 파악 방안 연구(곽동균, 육은희)

정책연구 16－17 통신시장 경쟁상황 평가(2016년도)(여재현, 김민철, 김상용, 김용재, 김지환, 김창완, 김현수, 이민석, 이상우, 정광재, 정 훈, 강인규, 김대건, 김성준, 김인혜, 나상우, 송용택, 이보겸, 임동민, 홍현기)

정책연구 16－18 단말기 유통법 성과 분석 및 제도 개선방안 연구(김현수, 강인규, 이솔희, 김인혜)

정책연구 16－19 지상파방송 재송신 분쟁 관련 쟁점 및 개선방안 연구(김태오, 김호정)

정책연구 16－20 방송법상 금지행위 위반에 대한 과징금 부과 기준의 세분화에 관한 연구(김태오, 송민선)

정책연구 16－21 스마트미디어 시대 지역방송의 차별화 및 경쟁력 확보 방안 연구 (심홍진, 주민정, 이주영)

정책연구 16－22 국민관심행사 고시의 합리적 개선을 위한 실증연구(심홍진, 육은희)

정책연구 16－23 국내제작 방송프로그램 인정기준 개선방안 연구(주성희, 이주영)

정책연구 16－24 방송통신 융합 환경에 따른 방송사업자의 소유겸영 규제 개선 정책방안 연구(김남두, 진전은영)

정책연구 16－25 방송분야 정책통계의 효율적 관리 및 활용방안 연구(김남두, 정용찬, 신지형, 진전은영)

정책연구 16－26 방송프로그램 시청자평가 개선방안 연구(주재욱, 강현철, 박은희, 정부연, 이선희)

정책연구 16－27 브렉시트의 ICT 산업 파급효과와 정책방향 연구 (고동환, 강하연, 나성현, 진홍윤, 최지혜, 박은지, 박선우)

정책연구 16－28 RCEP, TISA, 한중일・한중미 FTA 등 방송통신시장 규제현황 분석 및 통상협상 방안 마련(강하연, 박은지)

정책연구 16－29－01 창조경제 글로벌 혁신협력모델 개발 연구(기본형모델)(강하연, 김성옥, 박지현, 남상열, 김성웅, 김진주, 최효민, 정아영, 박정은)

정책연구 16－29－01 창조경제 글로벌 혁신협력모델 개발 연구(특화형모델)(강하연, 김성옥, 박지현, 김진주, 최효민, 김은경, 김정민, 박승찬, 신윤정, 최준환)

정책연구 16－30 국제우편서비스 구조개편 및 요금안 마련 연구(최중범, 이영종, 박소연, 정일량)

정책연구 16－31 우체국 펀드판매 취급을 위한 실행 방안 마련 연구(박재석, 안명옥, 김민진, 황병일, 정경오, 이재석)

정책연구 16－32 기술변화와 인적자원 운영 연구(강홍렬, 한은영, 최승재, 허재준, 김형만)

정책연구 16－33 방송통신 결합상품 제도개선 효과분석 및 후속조치 연구(김민철, 김현수, 정 훈, 송용택, 이보겸)

정책연구 16－34 인터넷플랫폼사업자 이용자이익저해행위 개선방안 연구(김현수, 강인규, 홍현기, 김대건)

정책연구 16－35 시설관리기관 설비의 이용활성화를 위한 이용대가 산정방식 연구(이상우, 송용택, 이솔희)

정책연구 16－36 TDD 주파수의 효율적 활용방안 및 이동통신용 주파수 중장기 공급방안에 대한 연구(김상용, 김득원, 김지환, 임동민, 김인희)

정책연구 16－37 ’16년 주요 통신서비스별 시장상황 자료 수집・분석(김현수, 정 훈, 강인규, 홍현기, 김대건)

정책연구 16－38 전기통신사업 영업보고서 정보 유용성 제고방안 연구(정 훈, 박상미, 송용택, 이민석, 김대건)

정책연구 16－39 광고총량제 등 광고규제 개선 효과 분석(강준석, 황유선, 김호정, 홍석영)

정책연구 16－40 매체별 광고 규제체계 개선방안 연구(황준호, 김경은, 정은진)

정책연구 16－41 방송통신 분야 국내외 동향 분석 및 ’17년 시장전망 연구(초성운, 정용찬, 이민석, 정 혁, 유선실, 홍현기, 권용재, 홍석영)

정책연구 16－42 방송통신 분야 규제비용 연구(초성운, 황유선, 정광재, 김경은, 이보겸, 홍석영)

정책연구 16－43 방송통신 융합시대에 부응하는 규제체계 정비방안 연구(황준호, 성욱제, 정은진, 이주영)

정책연구 16－44 지상파다채널 시대의 합리적인 규범정립에 관한 연구(김태오, 송민선)

정책연구 16－45 외주제작시장의 공정거래 환경조성을 위한 평가방법론 개발(김경은, 심홍진, 황유선, 진전은영)

정책연구 16－46 공적서비스방송의 해외제도 비교 연구(이종원, 황준호, 성욱제, 김태오, 육은희)

정책연구 16－47 2016년도 미디어다양성 모니터링 연구(성욱제, 김남두, 강준석, 정은진, 이주영, 진전은영)

정책연구 16－48 ICT 통계 발전전략 수립(나성현, 정용찬, 주재욱, 정 혁, 정현준, 고동환, 김경훈, 유선실, 정부연, 김욱준, 진홍윤, 이선희, 신우철, 박선영, 박선우, 최지혜)

정책연구 16－49 ICT 통계조사 품질진단(정용찬, 김경훈, 정 환, 유선실)

정책연구 16－50 ICT 산업 통계분석 프레임워크 구축(나성현, 김욱준, 이선희, 진홍윤)

정책연구 16－51 ICT 통계 분류체계 개선방안 연구(정현준, 진홍윤, 김욱준)

정책연구 16－52 ICT 통계조사 기여도 평가(주재욱, 김경훈, 김욱준, 이동희)

정책연구 16－53 ICT 및 인터넷 경제 통계의 조사 모집단 및 표본설계 표준화(정현준, 김욱준, 오윤석, 신우철, 한근식)

정책연구 16－54 ICT 및 인터넷 경제통계분석(정혁, 고동환, 김경훈, 김민식, 김욱준, 나성현, 박선우, 신우철, 오윤석, 오정숙, 유선실, 이경남, 이선희, 이은민, 정부연, 정원준, 정현준, 진홍윤, 최지혜)

정책연구 16－55 남북 정보통신 교류협력 촉진(김철완, 강하연, 김윤도, 서소영, 이우섭)

정책연구 16－56 2017 ITU 텔레콤월드 개최국 협정 협상 대응방안 연구(서보현, 김태은, 전선민)

정책연구 16－57 2016년도 우정정책 출연연구－우정동향 조사 분석(정진하, 이석범, 한은영, 안명옥, 이영종, 이경은, 박소연, 최승재)

정책연구 16－58 2016년도 우정정책 출연연구－TPP 등 배달서비스 통상협상 대응 방안 수립(정진하, 최중범, 한은영, 이영종)

정책연구 16－59 2016년도 우정정책 출연연구－세계우편전략 이행을 통한 국제우편 경쟁력 강화방안 연구(정진하, 최중범, 이경은)

정책연구 16－60 2016년도 우정정책 출연연구－사업환경 변화에 따른 우체국예금 대응 전략 수립(정진하, 박재석, 이용수, 이영종, 김민진, 김지혜, 선정훈)

▌2017 정책연구

정책연구 17－01 통계 모형을 이용한 ICT 일자리 중심정책 효과 및 방향 연구(정혁, 정부연, 최지혜, 전병유)

정책연구 17－02 신창조경제 글로벌 역량 및 기업 해외진출 강화방안 연구(김성옥, 박지현, 박은지, 최효민)

정책연구 17－03 창업지원 효율화 및 창업기업 진입장벽 해소 방안 연구(최계영, 박유리, 문정욱, 정원준, 손가녕, 김민식)

정책연구 17－04 통합시청조사결과 합산을 위한 가중치 연구(황준호, 성욱제, 문혜리)

정책연구 17－05 ICT 신산업 활성화와 효율적 규제개혁 추진을 위한 정책방안 연구(김정언, 박유리, 이원태, 염수현, 조유리, 강준모, 이학기, 김민식, 이은민, 정원준, 이시직, 손가녕, 최주한)

정책연구 17－06 아시아스타트업 허브 조성을 위한 글로벌 정책 협력방안 연구(남충현, 이경남, 손가녕, 최주한)

정책연구 17－07 ICT 벤처・스타트업 관련 제도 효율화 방안 연구(조유리, 조성은, 김

민식, 손가녕)

정책연구 17－08 초연결 지능망 사회의 네트워크 투자 관리 체계 연구(이상우, 여재현, 정 훈, 나상우, 송용택, 이솔희, 이용진, 나성욱, 김병희, 조대근, 이종기)

정책연구 17－09 MVNO의 경쟁력 강화를 위한 시장분석 및 완전 MVNO 진입 가능성에 관한 연구(정광재, 김대건)

정책연구 17－10 All-IP, 융합형 서비스 활성화 등 시장환경 변화에 따른 통신서비스개선 및 이용자 편익확대 방안 연구(김용재, 김민철, 김창완, 이민석, 강인규, 나상우, 박상미, 이보겸)

정책연구 17－11 자가전기통신설비의 공익목적 활용 촉진을 위한 제도개선 방안 연구(이상우, 송용택, 이솔희)

정책연구 17－12 Mega FTA 시대의 신유형 서비스(스마트미디어, 광고 등) 규범체계 및 스마트미디어 콘텐츠 규제에 관한 연구(이종원, 주성희, 곽동균, 홍석영, 송민선, 진전은영)

정책연구 17－13 국내외 유료방송 규제개편 사례 및 정책동향 분석(이종원, 김호정)

정책연구 17－14 플랫폼 수익구조 개선을 통한 유료방송시장 생태계 선순환 기반조성을 위한 연구(강준석, 김남두, 권용재, 이주영, 홍석영)

정책연구 17－15 ICT산업 중장기 전망(2017～2021) 및 대응전략(정혁, 정용찬, 김창완, 고동환, 유선실, 정부연, 이경남, 오정숙, 이은민, 나상우, 김욱준, 김대건, 진홍윤, 이선희)

정책연구 17－16 ICT기반 사회현안 해결방안 연구(이호영, 손상영, 이원태, 조성은, 김희연, 문정욱, 이시직, 양수연, 류현숙, 최은창, 한상기)

정책연구 17－17 통신시장 경쟁촉진을 위한 규제 체계 및 정책방안 연구(김창완, 여재현, 이민석, 송용택, 이보겸)

정책연구 17－18 창조경제 글로벌협력 환경분석 및 의제대응 방안 연구(남상열, 김성웅, 박정은)

정책연구 17－19 일자리 창출 중심의 창조경제정책 수립・추진방안 연구(이학기, 이경남, 최주한)

정책연구 17－20 제4차 산업혁명 선도를 위한 과학기술-ICT 기반 국가정책방안 연구(김정언, 최계영, 조유리, 강준모, 이학기, 김민식, 이은민, 이시직,

정원준, 손가녕, 양수연, 최주한, 손병호, 신민수)

정책연구 17－21 우체국 서민대출 추진 시 예금사업 영향도 사전 분석(박재석, 김민진, 김지혜, 안명옥)

정책연구 17－22 합리적이고 공정한 PP-플랫폼 간 채널 계약을 위한 제도 개선 조사(강준석, 권용재)

정책연구 17－23 클라우드 도입에 따른 전자정부예산 운영의 혁신(강홍렬, 권헌영, 한은영, 김지혜, 엄석진)

정책연구 17－24 국제우편 관련 국내 시행 법령 전면 개정안 마련(최중범, 정진하, 박소연, 이진경)

정책연구 17－25 ICT 기업 글로벌 진출 활성화 방안 연구(조유리, 김성옥, 김정언, 손가녕)

정책연구 17－26 통신시장 경쟁상황 평가(2017년도)(정진한, 김민철, 김용재, 김창완, 김현수, 여재현, 이민석, 이상우, 정광재, 정훈, 강인규, 김대건, 김성준, 나상우, 박상미, 송용택, 이보겸, 이솔희, 홍현기)

정책연구 17－27 방송시장 상생 발전을 위한 사후규제 개선방안 연구(강준석, 김태오, 권용재)

정책연구 17－28 주파수 경매 시뮬레이션 Tool 개발(김희천, 김상용, 김득원, 김지환, 임동민, 정아름, 김인희)

정책연구 17－29 창조경제 글로벌 정책동향 분석 및 기본전략 수립(강하연, 박지현, 김성옥, 최효민, 강반디, 오태현)

정책연구 17－30 공공・민간 데이터 유통・거래 환경 기반 조성 연구(이원태, 문정욱, 양수연, 왕재선)

정책연구 17－31 ICT기반 사회현안 해결방안 연구(조성은, 손상영, 이원태, 김희연, 문정욱, 이시직, 양수연, 이종관)

정책연구 17－32 지능정보사회에서의 이용자보호 이슈 및 정책 방안 연구(이원태, 문정욱, 양수연)

정책연구 17－33 미래부 창업(재도전)・벤처 지원사업 참여기업 실태조사 및 지원정책 효율화 방안 연구(최계영, 김성옥, 김민식, 이가희)

정책연구 17－34 한・중 ICT 벤처・스타트업 및 공동연구 협력방향 연구(김성옥, 강하연, 서소영, 정인선, 강반디, 이슬기, 김준연)

정책연구 17－35 ICT 분야에서의 4차 산업혁명 활성화를 가로막는 경쟁 제한적 규제 발굴을 위한 연구(강준모, 조성은, 민대홍, 오정숙, 이시직)

정책연구 17－36 주요 통신서비스별 시장상황 자료 수집・분석(김현수, 정 훈, 강인규, 김대건, 송용택, 홍현기)

정책연구 17－37 부가통신서비스시장의 신유형 불공정행위 조사 방안 연구(김현수, 강인규, 홍현기)

정책연구 17－38 규제 환경 변화에 따른 이동통신 단말장치 유통구조 개선 방안 연구(김현수, 강인규, 이보겸)

정책연구 17－39 신규 통신서비스 활성화를 위한 도매제도 정비 및 합리적 트래픽 관리기준 개선 방안 연구(이상우, 정훈, 김대건, 이솔희, 송용택, 조대근)

정책연구 17－40 IoT 환경에서의 가입자식별모듈 이동성 제도 및 번호정책 연구(정광재, 김민철, 이보겸)

정책연구 17－41 ’18～’19년 접속원가 산정 및 통화량 예측모형 개선방안 연구(김민철, 송용택, 김대건, 김성준)

정책연구 17－42 5G 시대의 주파수 할당대가 산정 제도 연구(김지환, 김상용, 김득원, 김희천, 임동민, 정아름, 김인희)

정책연구 17－43 진입규제 완화에 대비한 전파법 체계 개선방안 연구(김득원, 김상용, 김희천, 임동민, 김인희)

정책연구 17－44 지능정보사회의 주파수 공급 및 이용제도 개선방안 연구(김지환, 김상용, 김득원, 김희천, 임동민, 김인희)

정책연구 17－45 방송통신 분야 환경변화에 따른 주요 이슈 분석 및 정책방향 연구(초성운, 황준호, 이재영, 이민석, 유선실, 홍현기, 권용재)

정책연구 17－46 방송통신 분야 규제비용 관리방안 연구(초성운, 황유선, 김지환, 정광재, 송민선)

정책연구 17－47 방통융합 서비스 해외제도 분석을 통한 미래지향적 규제체계 개선 연구(황준호, 성욱제, 김호정, 육은희)

정책연구 17－48 방송의 미래 전망과 규제 개선을 위한 정책 과제 연구(이재영, 정은진)

정책연구 17－49 지상파 AM라디오방송 효율화 정책방안 연구(이종원, 김태오, 김상용, 정은진)

정책연구 17－50 방송통신 결합판매 경쟁상황 평가 방법론 및 지표 개발(곽동균, 황유선, 권용재)

정책연구 17－51 정보통신망법상 개인정보보호 제도의 정책효과 분석(김태오, 이재영,

성욱준, 이원태, 조성은, 송민선)

정책연구 17－52 방송광고 전반에 대한 제도개선 방안 마련을 위한 연구 - 현행 비대칭규제에 대한 추가적 규제완화 시 효과 분석 등(강준석, 황유선, 김호정)

정책연구 17－53 신유형광고 제도화 및 매체별 차등규제 개선을 위한 입법안 연구(황준호, 심홍진, 송민선)

정책연구 17－54 방송한류 활성화 및 경쟁력 강화 방안 연구(주성희, 육은희)

정책연구 17－55 외주제작 시장구조 및 경쟁상황 실태평가 및 관련 제도 정비방안 연구(심홍진, 김청희)

정책연구 17－56 방송매체 환경변화에 따른 편성제도 실효성 제고 방안 연구(주성희, 김청희)

정책연구 17－57 공영방송의 독립과 공정성 제고를 위한 법제도 개선방안 모색(김남두, 이종원, 황준호, 정은진, 송민선)

정책연구 17－58 지상파・유료방송 방송광고 유형에 대한 시청자평가 및 인식조사(강준석, 곽동균, 황유선, 김호정, 송민선)

정책연구 17－59 매체 및 통상환경 변화에 따른 방송법제 대응방안 연구(이종원, 주성희, 곽동균, 육은희)

정책연구 17－60 유료방송 시장 집중현상 개선방안 연구(이재영, 육은희)

정책연구 17－61 방송통계 통합정보 제공체계 구축(신지형, 김윤화, 이선희, 김상우)

정책연구 17－62 인터넷 경제 및 ICT 통계 분석(정혁, 나성현, 고동환, 김경훈, 유선실, 정부연, 진홍윤, 이선희, 신우철, 노희윤, 오윤석, 최지혜, 김민식, 이경남, 오정숙, 이은민)

정책연구 17－63 인터넷 경제 및 ICT 관련 통계 표준화(정현준, 신우철, 박선영, 한근식)

정책연구 17－64 ICT 통계체계 기획 및 개선방안 연구(최계영, 정현준, 정용찬, 정혁, 신지형, 고동환, 남충현, 나성현, 김경훈, 유선실, 정부연, 김욱준, 이선희, 신우철, 노희윤, 오윤석, 최지혜, 김상우, 박선영, 진홍윤)

정책연구 17－65 지능정보산업 시장규모 추정을 위한 연구(고동환, 나성현, 최계영, 오윤석, 유선실, 이대호)

정책연구 17－66 ICT 통계조사 품질진단(정용찬, 유선실, 정환)

정책연구 17－67 ICT 통계조사 기여도 평가(신지형, 이선희, 김경훈, 김욱준, 주재욱)

정책연구 17－68 남북 정보통신 교류촉진(강하연, 김봉식, 서소영)

정책연구 17－69 APEC 인터넷경제 협력 논의 및 대응 방안(남상열, 김성웅, 박정은)

정책연구 17－70 OECD 고잉디지털(Going Digital) 프로젝트 분석 및 대응방안(고상원, 김성웅, 김병우)

정책연구 17－71 국제기구를 통한 중남미지역 ICT 협력방안 연구(남상열, 김성웅, 김병우)

정책연구 17－72 2017년도 우정정책 출연연구 － 우정동향 조사 분석(정진하, 이석범, 이용수, 한은영, 안명옥, 이영종, 이경은, 박소연, 김민진)

정책연구 17－73 2017년도 우정정책 출연연구 － 경쟁에 대응한 우편서비스 구조 개편과 이를 위한 법령개정 및 요금 체계 정비 방안 연구(정진하, 최중범, 한은영, 이영종)

정책연구 17－74 2017년도 우정정책 출연연구 － 우체국예금 전략고객 확보 방안(정진하, 박재석, 이용수, 안명옥, 김민진, 김지혜)

정책연구 17－75 2017년도 우정정책 출연연구 － 우편・배달서비스 관련 통상협상 대응 방안 수립(정진하, 최중범, 한은영, 이영종, 이진경)

● 저 자 소 개 ●

손 상 영
· 미국 로체스터대 경제학 박사
· 현 정보통신정책연구원 선임연구위원

이 시 직
· 연세대 법학 석사(박사과정)
· 현 정보통신정책연구원 연구원

조 성 은
· 미국 럿거스대 언론학 박사
· 현 정보통신정책연구원 연구위원

김 희 연
· 이화여대 사회학 석사
· 현 정보통신정책연구원 부연구위원

양 수 연
· 미국 럿거스대 언론학 박사
· 현 정보통신정책연구원 연구위원

오 태 원
· 연세대 법학 박사
· 현 경일대학교 교수

경제·인문사회연구회 협동연구 17-26-01
기본연구 17-11-01

총괄보고서: 초연결사회의 지속가능성을 위한 사회문화적 조건과 한국사회의 대응(Ⅲ)

2017년 12월 일 인쇄
2017년 12월 일 발행

발행인 김 대 희
발행처 정 보 통 신 정 책 연 구 원
충청북도 진천군 덕산면 정통로 18
TEL: 043-531-4114 FAX: 043-535-4695～6
인 쇄 크리홍보주식회사
ISBN 979-11-7000-174-4 94320
ISBN 979-11-7000-173-7 (전 3권)

보급가 10,000원