

지능정보사회의 사이버 역기능 분류와 사회적 인식 분석*

임규건** · 안재익***

A Study on the Classification of Cyber Dysfunction and the Social Cognition Analysis in the Intelligent Information Society*

Gyoo Gun Lim** · Jae Ik Ahn***

■ Abstract ■

The Internet cyber space has become more important as it enters the intelligent information society of the 4th Industrial Revolution beyond the information age through the development of ICT, the expansion of personalized services through mobile and SNS, the development of IoT, big data, and artificial intelligence. The Internet has formed a new paradigm in human civilization, but it has focused only on the efficiency of its functions. Therefore, various side effects such as information divide, cyber terrorism, cyber violence, hacking, and personal information leakage are emerging. In this situation, facing the intelligent information society can lead to an uncontrollable chaos. Therefore, this study classifies the cyber dysfunction of intelligent information society and analyzes social cognition, suggests cyber dysfunction standard of intelligent information society, and examines the seriousness of dysfunction, and suggests technical research directions for future technologies and services. The dysfunctional classification of the intelligent information society was classified into five areas of cyber crime and terrorism, infringement of rights, intelligent information usage culture, intelligent information reliability, and social problems by FGI methodology. Based on the classification, the social perception of current and future cyber dysfunction severity was surveyed and it showed female is more sensitive than male about the dysfunction. A GAP analysis confirmed social awareness that the future society would be more serious about AI and cyber crime.

Keyword : Artificial Intelligence, Intelligent Information Society, Cyber Dysfunction, 4th Industrial Revolution, Security

Submitted : February 4, 2020

1st Revision : February 19, 2020

Accepted : February 22, 2020

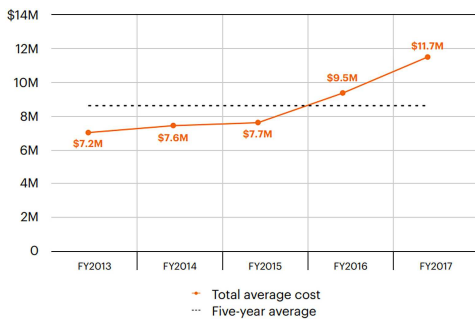
* 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018S1A5A2A01035729). 한국IT서비스학회 2019 추계학술대회에서 우수연구로 선정되어 ㈜글로벌리서치가 실시한 설문조사 결과를 포함하고 있음.

** 한양대학교 경영대학 교수

*** 한양대학교 경영대학 석사과정, 교신저자

1. 서 론

인터넷 사이버 공간은 정보통신기술 발전과 모바일, SNS를 통한 개인화 서비스 확대, IoT, 빅데이터, 인공지능 등 기술 발전을 통해 정보화시대를 넘어 4차 산업혁명의 지능정보사회로 접어들면서 그 중요성이 더욱 강화되고 있다. 그동안 인터넷은 정치, 경제, 사회, 문화, 교육 등 인류문명에 새로운 패러다임을 형성하였지만 그 기능의 효율성에 집중하여 순기능에만 주목한 면이 있다 (Lee et al., 2018, Shin et al., 2018). 그러나 최근 정보격차, 사이버테러, 사이버폭력, 해킹, 개인정보 유출 등 다양한 역기능이 나타나고 있다(권문주 외, 2010; 임규건 외, 2018; 양승돈과 김형욱, 2018). Ponemon Institute의 2017년 사이버 범죄 비용 연구 보고서에 따르면 2016년에 보고된 950만 달러에서 23% 증가한 1,170만 달러로 증가하였다고 한다(Ponemon Institute, 2017).



[그림 1] 최근 5년간 사이버 범죄 비용 평균(Ponemon Institute, 2017)

4차 산업 혁명의 대표적인 혁신기술 중 하나인 블록체인 기반의 암호화폐의 해킹 사례와 같이 혁신 산업마다 고도화된 해킹기술로 범죄자들, 테러단체들의 위협이 심해지고 있다. 4차 산업혁명시대의 혁신 이면에는 인공지능과 빅데이터 기술에 기반한 자동화되고 지능화된 해킹기술 같은 파괴적인 기술 혁신이 또한 존재하는 것이다(임종인, 2018). 이 때문에 사이버위험은 기하급수적으로 더욱 증가할 것으로 예측된다.

이렇듯 사이버 공간에서의 안전한 생활 보장, 새로운 사회 질서 정립에 필요성이 강하게 요구되고 있지만 지능정보 사회로의 전개에 따른 종합적 역기능 대응 전략은 미흡한 상황이다. 그동안 이운배(2013), 우매리 등(2015) 사이버 역기능과 관련한 다양한 연구가 다수 진행되고 있으나 지능정보 사회의 새로운 패러다임을 반영한 역기능 연구는 아직 부족한 실정이다. 4차 산업혁명의 지능정보화 사회를 대비해서 역기능에 대한 체계적인 연구가 필요한 시점이다.

이에 본 연구에서는 지능정보 사회의 사이버 역기능에 대해서 파악하고 역기능을 분류하고자 한다. 이를 위해서 기존에 제시되었던 인터넷 역기능을 분석하고 지능정보 사회 관점에서의 사이버 역기능에 대하여 현재 제정된 법률과 관련 부처의 보고서 등의 문헌 분석을 통해 지능정보사회의 사이버 역기능 키워드들을 추출한다. 그리고, FGI 방법론을 통해 지능정보사회의 사이버역기능에 대하여 정의 및 분류하고자 한다.

또한 도출한 지능정보사회의 사이버 역기능 분류 기준을 기반으로 사이버 역기능에 대한 사회적 인식을 조사한다. 현재와 미래의 인식 차이를 분석함으로써 역기능의 심각성을 파악하여 미래 기술 및 서비스 등에 대한 기술적 연구 방향을 제시하고자 한다(서인주, 정지영, 2017).

제 2장 선행연구에서는 사이버역기능, 지능정보 사회, 남녀간 성별차이에 대한 인지차이에 대해서 살펴본다. 제 3장에서는 지능정보 사회의 사이버 역기능을 추출 및 분류한다. 제 4장에서는 가설 검증과 사이버 역기능 인지조사 결과에 대한 분석하고 제 5장에서 마무리 한다.

2. 선행연구

2.1 지능정보사회

지능정보사회는 인공지능 기술과 데이터 활용기술의 발전에 따라 새로이 부상하는 사회 모습을 지칭한다(관계부처 합동, 2016). 즉, 지능정보기술이

사회 전반에 활용되어 새로이 발전하고 변화하는 사회를 의미한다.

기존 정보사회는 계산능력이 증시되고 아날로그와 디지털이 분리된 사이버공간을 전반으로 ICT가 중점이 된 특성을 가졌다면 지능정보사회는 생각하는 능력이 증시되고 아날로그의 디지털화가 된 현실세계 전반으로 로봇, 알고리즘, 사물인터넷 등 지능정보기술이 중점이 되어 만물의 데이터화, 실시간 반응, 자율 진화, 무인 의사결정의 특성을 지닌다(이원태, 2018).

AI, IoT, Big Data, Cloud 등을 대표적인 주요 지능정보기술로 정의할 수 있으며 지능정보기술은 정확한 데이터 분석을 통한 초연결성, 초지능화의 특성이 사회 객체들을 상호 연결하고 지능화시켜 우리 사회의 전반적인 시스템을 네트워크로 연결하고 자동제어를 가능하게 한다(주윤경, 2018; 이홍재 외, 2018).

지능정보기술은 교통, 노동, 교육, 의료, 안전 등 우리 일상생활을 변화시키고 있으며 이외 사회 전 분야에 보편적으로 활용되어 지능정보사회로의 변화를 주도하고 있다(백승익 외, 2016). 향후 기계와 사람의 상호작용이 극대화 되면서 자동화의 속도와 범위가 확대되고 인간이 아닌 기계가 스스로 생각하고 판단하는 사회로 인공지능이 주체가 될 것이다(이정아, 2016).

이러한 지능정보사회로의 패러다임 전환은 사회 전반적으로 새로운 기회와 혁신적 변화를 제공하

지만 기술 발전의 양면성에 따라 다양한 역기능을 초래할 수도 있다(이홍재 외, 2018). 하지만 사회는 긍정적으로 창출되는 사회적 변화에 집중하여 역기능에 대한 관심이 상대적으로 적은 상황이며 이와 관련한 연구도 부족한 실정이다(송봉규, 2019).

2.2 사이버 역기능

인터넷의 발전은 인류 문명에 새로운 패러다임을 형성하고 삶의 질을 향상시키는 등 긍정적인 사회 변화를 이끌었지만 초기부터 인터넷의 순기능에만 주목하였고 TCP/IP 프로토콜이 보안을 고려하여 만들어진 것이 아니라서 인터넷으로 인한 다양한 사회의 부작용이 발생하였다. 현재 사이버 상에서 발생할 수 있는 통신사기, 명예 훼손, 사이버 성폭력, 개인정보 침해, 저작권 침해, 인터넷 중독 등의 부작용을 통칭하는 개념으로 사이버 역기능이 정의되고 있다(이윤배, 2013, 우매리, 2015).

사이버 역기능의 발생 요인으로는 정보 수집과 전달의 속도, 프라이버시와 익명성, 전자 매체의 본질, 심미적 매료, 국제적 사용 범위, 정보통신 기술의 파괴력 등이 제시되고 있다(이윤배, 2013).

기존 연구에서 제시하는 사이버 역기능 분류 표준은 다음 [그림 2]와 같다. 미디어중독, 유해 콘텐츠, 사이버폭력, 권리침해, 사이버테러, 판단장애 등 총 6가지 항목으로 대분류하였다(권정인 외, 2011).



[그림 2] 인터넷의 역기능 분류 표준(권정인 외, 2011)

지능정보사회에서는 지능정보기술이 다양한 산업분야와 연결되며 가상과 현실의 경계가 소멸되고 융합이 이루어지게 된다(정보통신전략위원회, 2018; 이원태 외, 2017). 이러한 공간 패러다임의 변화는 더욱 역기능의 위험을 증폭, 확대시킬 것이며 이중적이고 복합적인 위험을 가져올 수 있다(이정아, 2016; 성지은, 정병걸, 2007).

하지만 기존의 연구는 정보사회에서의 사이버 역기능에 대한 정의 및 분류에 그치고 다가오는 지능정보사회에서 발생할 수 있는 역기능은 포함하지 못하고 있다.

이에 본 연구에서는 지능정보기술로 인하여 발생할 수 있는 역기능을 정의하고 분류하고자 한다. 잘 알려진 사이버 테러, 해킹, 사이버 범죄, 개인정보 유출뿐만 아니라 SNS 활성화, 1인 미디어 성장으로 인한 사이버 명예훼손, 인공지능 발전으로 인한 인간성 상실 및 인지장애, 초연결 시대의 발전으로 인한 Life Log 권리 침해 등을 반영하고자 한다.

2.3 남녀 간 성별 차이에 의한 인지 차이

남녀 간 성별 차이에 대한 생리학적, 심리학적, 마케팅과 관련한 연구가 다수 수행되어 왔다. 일반적으로 남성보다 여성이 상대적으로 위험에 대해서 기피하고자 하는 경향이 있고 특히 부정적인 감정에 대하여 예민하게 반응한다(Bajtelmsmit and VanDerhi, 1997; Johnson and Powell, 1994; Harbaugh et al., 2002). 이러한 성향은 의사결정자가 속한 사회와 문화, 그리고 위험 수준 등에 따른 구체적 상황에 따라 달라질 수 있다(Weber et al., 2002; Vieider et al., 2015).

또한 남녀 성별에 따른 정보처리 및 판단의 차이가 있고 인지 능력에 차이가 있으므로 사회과학적 분석에서 성별 차이도 고려되어야 한다(이진권, 2016; 최성수, 2015).

본 연구에서는 남녀 간 지능정보사회의 사이버 역기능 위험성 인식차이를 확인해 봄으로써 미래

사회가 대처해야 할 지능정보사회의 역기능을 사회보편적으로 수용할 수 있는 기술, 서비스의 기반을 마련하고자 한다.

3. 본 론

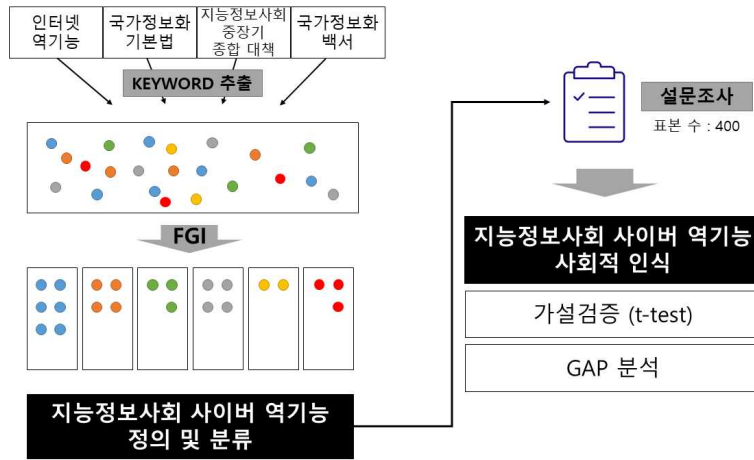
3.1 연구 절차

본 연구에서는 지능정보사회의 사이버 역기능을 정의하기 위하여 국가정보화 기본법(2019), 지능정보사회 중장기 대책(관계부처 합동, 2016), 국가정보화백서(한국정보화진흥원, 2018)로부터 지능정보사회 역기능 키워드를 1차 추출한 후 분류 및 통합 과정을 거쳐 지능정보사회의 사이버 역기능을 2차로 추출하였다. 이후 FGI 방법론을 활용하여 정보사회와 MIS 전공 전문가로 구성된 패널을 통해 다섯 가지 유형으로 분류하고 지능정보사회의 역기능 유형을 제시하였으며 기존 선행연구와 관련 문헌을 분석하여 지능정보사회의 사이버 역기능 분류를 구체화하였다.

이후 본 연구에서 제시하는 지능정보사회의 사이버 역기능 유형을 기반으로 사이버 역기능에 대한 사회적 인식을 설문조사하여 우리 사회가 바라보는 사이버 인식의 현 주소를 가설검증과 현재와 미래에 대한 GAP분석을 실시하였다.

3.2 지능정보사회의 사이버 역기능 추출

지능정보사회에서 발생할 수 있는 다양한 사이버 역기능들을 파악하기 위해 본 연구에서는 인터넷, 정보기술, 지능정보화와 관련된 ‘국가정보화 기본법’, ‘지능정보사회 중장기 종합대책’, ‘국가정보화백서’의 법률 및 보고서를 분석하여 1차적으로 키워드를 추출하였다. 이후 유사한 특징 혹은 성질을 가진 요소들은 통합하고 그 반대의 경우를 2차로 추출하고 FGI 방법론을 통해 다섯 가지 유형으로 분류하여 지능정보사회의 사이버 역기능을 제시하였다.



[그림 3] 연구 프레임워크

3.2.1 국가정보화백서

국가정보화백서는 지난 국가정보화 현황과 실적 뿐만 아니라 미래 지능정보사회에 대한 각 분야의 현황과 전망을 포함하고 있다(한국정보화진흥원, 2018). 특히 2018년 국가정보화백서는 데이터 경제를 특별 기획으로 미래 지능정보사회의 데이터 기반 혁신 및 전략을 담고 있다.

국가정보화백서에서 1차적으로 추출한 지능정보사회의 사이버 역기능 키워드는 <표 1>과 같다. 인공지능, IOT, 데이터, 사이버테러 등과 같은 지능정보사회 주요 기술들의 키워드가 주를 이뤘고 그 외 정보사회에서 발생했던 인터넷 역기능도 다수 존재하였다.

<표 1> 국가정보화백서 사이버 역기능 키워드

국가정보화백서
신뢰성 및 안전성, 법적·윤리적 문제, 사고시 책임소재, 해킹, 보안위협, 사이버 멀미, 개인정보 유출, 인공지능 저작물에 대한 저작권 문제, 인공지능으로 인한 일자리 문제, 인공지능 판단에 대한 윤리적인 문제, 인공지능 판단의 신뢰성 문제, 학습의 편향, 법적 체계 미비, IOT로 인한 사이버 공격 증대, 과도한 개인정보 수집, 데이터 기반 특성 분석 및 차별, 인터넷 과의존, 스마트폰 과의존, 지식재산권 침해, 사이버 폭력, 음란물, 불법사이트, 피싱, 파밍, 스미싱, 사이버 국가안보 위협, 허위사실 유포, 데이터 주권

3.2.2 지능정보사회 중장기 종합대책

제4차 산업혁명에 따른 지능정보사회 중장기 종합대책은 미래창조과학부를 주축으로 10개 부처 및 민간 전문가 30여 명으로 구성된 지능정보사회 민관합동 추진협의회를 구성하고 지능정보기술이 사회 경제 전반의 구조적인 변화를 일으킬 것으로 전망되어 중장기적인 종합대책을 수립하여 관련 내용을 담고 있다. 인간 중심 지능정보사회 실현을 국가 비전으로 세우고 기업, 국민, 정부, 전문가 및 학계에서의 역할을 제시하고 있으며 이와 관련한 사회적 요구를 반영하고 있다(관계부처합동, 2016).

지능정보사회 중장기 종합대책에서 1차적으로 추출한 지능정보사회의 사이버 역기능 키워드는 <표 2>와 같다. 프라이버시, 인공지능, 사이버테러, 사회적 변화 등과 같은 사회적인 문제들이 주를 이뤘고 특히 타 보고서와 달리 기술 외적인 역기능들이 다수 추출되었다.

<표 2> 지능정보사회 중장기 종합대책 사이버 역기능 키워드

지능정보사회 중장기 종합대책
해킹, 인간소외, 프라이버시 침해, 소득 하락, 소득 양극화, 지능정보격차, 안정성 및 신뢰성 문제, DDOS, 악성코드, 사이버 위협, 인공지능 오작동, 고용구조 변화, 인공지능 개발자 및 이용자의 윤리, 인공지능에 대한 사회적 편견

3.2.3 국가정보화 기본법

국가정보화 기본법은 국가정보화의 기본적인 방향과 관련 정책의 수립 및 추진에 필요한 사항을 규정하고 지속가능한 지식정보사회를 실현하며 국민의 삶의 질을 높이고자 제정된 법이다. 국가정보화 기본법은 제 1장 총칙, 제 2장 국가정보화 정책의 수립 및 추진체계, 제 3장 국가정보화의 추진, 제 4장 국가정보화의 역기능 방지, 제 5장 정보통신기반의 고도화, 제 6장 보칙, 총 6장으로 구성되어 있으며 법률적으로 지능정보사회의 사이버 역기능을 정의하고 있다.

국가정보화 기본법에서 1차적으로 추출한 지능정보사회의 사이버 역기능 키워드는 <표 3>과 같다. 정보격차, 개인정보침해, 불건전 정보, 지식재산권 침해, 명예·생명·재산상의 위해 등의 키워드를 포함하였다. 제정된 법률이기 때문에 최소한의 단위를 가지고 있는 키워드들이 주를 이루었다.

<표 3> 국가정보화 기본법 사이버 역기능 키워드

국가정보화 기본법
정보격차, 개인정보침해, 불건전 정보, 지식재산권 침해, 명예·생명·재산상의 위해

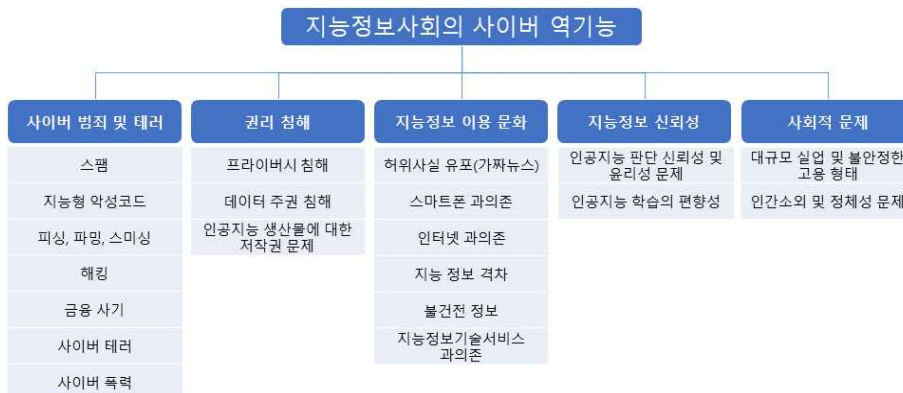
3.3 지능정보사회의 사이버 역기능 분류

기존 정의 및 분류되었던 인터넷 역기능과 각 범

<표 4> 지능정보사회의 사이버 역기능 2차 추출 키워드

인터넷 역기능	미디어중독, 유해콘텐츠, 사이버폭력, 권리침해, 사이버테러, 판단장애
국가정보화 기본법	정보격차, 불건전 정보, 지식재산권 침해
지능정보사회 중장기 종합대책	해킹, 인간소외, 프라이버시 침해, 지능정보격차, 안정성 및 신뢰성 문제, 사이버 위협, 인공지능 오작동, 인공지능 개발자 및 이용자의 윤리, 인공지능에 대한 사회적 편견
국가정보화 백서	해킹, 개인정보 유출, 인공지능 저작물에 대한 저작권 문제, 인공지능으로 인한 일자리 문제, 인공지능 판단에 대한 윤리적인 문제, 인공지능 판단의 신뢰성 문제 법적 체계 미비, 과도한 개인정보 수집, 인터넷 과의존, 스마트폰 과의존, 지식재산권 침해, 사이버 폭력, 음란물, 불법사이트, 피싱, 파밍, 스미싱, 허위사실 유포, 데이터 주권

를 혹은 보고서에서 추출한 키워드에서 중복되는 내용의 의미를 가진 키워드를 제외하여 재분류한 결과는 <표 4>와 같다. 이어 <표 4>에서 추출한 키워드를 통합하여 중복되는 내용 혹은 의미를 가진 키워드는 전문가 집단의 FGI 방법론을 통하여 통합하고 다른 성격을 지닌 그룹을 분리하여 5가지 그룹의 역기능을 정의하고 해당하는 역기능들을 정리하였다. 크게 [그림 4]와 같이 사이버 범죄 및 테러, 권리 침해, 지능정보 이용 문화, 지능정보 신뢰성, 사회적 문제



[그림 4] 지능정보사회의 사이버 역기능 분류

<표 5> 지능정보사회의 사이버 역기능 정의

사이버 범죄 및 테러	
스팸	불필요한 인터넷 메일, 불필요한 휴대전화, SMS 등을 보내는 행위
지능형 악성코드	해커가 프로그램 등에 다양한 보안 위협을 만들어 배포하여 특정 기업이나 조직의 네트워크에 지속적 지능적으로 가하는 공격
피싱, 파밍, 스미싱	피싱 : 개인정보와 낚시의 합성어, 이메일 등을 수신자가 신뢰할만한 출처로 위장하여 보내 개인정보를 빼내는 해킹 기법
	파밍 : 공식적으로 운용하고 있는 도메인 자체를 중간에서 탈취하여 개인정보를 빼내는 해킹기법
	스미싱 : 문자와 피싱의 합성어, 문자메세지를 이용한 피싱 기법
해킹	남의 컴퓨터 시스템에 허락 없이 침입하여 데이터를 빼내거나 파괴하는 행위
금융 사기	범행 대상자에게 인터넷메일, SMS 등을 이용해 금전적 피해를 야기하는 사기 수법
사이버 테러	상대방 컴퓨터나 정보기술을 해킹하거나 악성프로그램을 이용해 컴퓨터 시스템과 정보통신망을 무력화하는 테러리즘
사이버 폭력	사이버불링(모욕, 따돌림, 협박 등)과 사이버 상에서 발생하는 명예훼손, 언어폭력, 성폭력 등을 의미
권리 침해	
프라이버시 침해	개인 사생활 혹은 정보가 개인의 의사와 관계없이 공개되거나 간섭받은 경우를 의미
데이터 주권 침해	활동을 통해 무분별하게 생산되는 빅데이터의 주인된 권리를 침해하는 것을 의미
인공지능 생산물에 대한 저작권 문제	인공지능을 통해 만들어진 저작물에 대한 저작권을 정의하는 문제를 의미
지능정보 이용 문화	
허위사실유포 (가짜뉴스)	허위사실을 사이버 공간에 유포하는 것을 의미 (가짜뉴스 포함)
스마트폰 과의존	스마트폰, 인터넷 사용에 대한 금단을 유발시키고 이로 인해 일상생활에 장애가 유발되는 상태를 의미
인터넷 과의존	의미
지능 정보 격차	지능 정보에 대한 접근이 경제적, 성별, 연령별로 불균형하게 나타나는 현상을 의미함
불건전 정보	사이버 상에 유포된 불건전한 정보(음란물 등)을 의미
지능정보기술서비스 과의존	개별적 요구에 맞는 선별적 정보를 제공함으로써 신기술에 더욱 의존하게 만드는 현상을 의미, 인간의 인지적 판단을 지능정보기술이 대신하게 됨으로써 주도적인 의사결정이 어려운 것을 의미
지능정보 신뢰성	
인공지능 판단 신뢰성 및 윤리성 문제	인공지능의 판단의 신뢰성 여부와 그 판단을 통해 발생될 수 있는 윤리적인 문제를 의미
인공지능 학습의 편향성	편향된 학습(Training)으로 균등하고 합리적인 판단이 불가능한 것을 의미
사회적 문제	
대규모 실업 및 불안정한 고용 형태	지능정보기술을 통해 일자리가 대체되어 대규모 실업과 불안정한 고용 형태가 발생됨을 의미
인간소외 및 정체성 문제	인간이 필요에 의해 만든 지능정보기술에 의해 인간이 지배되는 현상, 소통의 대상이 인간인지 기계인지 판단이 불가하여 인간의 주된 정체성이 혼돈되는 상태

위와 같은 지능정보사회의 사이버 역기능 5대 영역 분류에 대하여 적절성을 설문조사를 통해 확인하였다. 전체 400명 중 69.3%가 적절하다고 답변하였으며 그렇지 않다고 답변한 비율(3.3%)보다

월등히 높아 본 연구에서 제시한 분류 기준이 적절하다고 판단하였다. 이후 본 분류 체계를 기초로 하여 사이버 역기능에 대한 사회적 인식을 조사하였다.

4. 조사분석 및 결과

4.1 가설

본 연구에서는 도출된 지능정보사회의 사이버 역기능 분류 기준을 기반으로 현재와 미래정보사회의 사이버 역기능에 대한 사회적 인식 차이를 조사하기 위하여 다음의 연구가설을 설정하였다.

H1 : 현재와 미래의 지능정보사회 사이버 역기능 문제에 대한 심각성에 차이가 있을 것이다.

여기서 지능정보사회의 사이버 역기능은 본 연구에서 제안한 사이버 범죄 및 테러, 권리 침해, 지능정보 이용 문화, 지능정보 신뢰성, 사회적 문제 다섯 가지의 유형으로 구분하였다.

H1-1 : 현재와 미래의 지능정보사회 사이버 범죄 및 테러 문제에 대한 심각성의 차이가 있을 것이다.

H1-2 : 현재와 미래의 지능정보사회 권리 침해 문제에 대한 심각성의 차이가 있을 것이다.

H1-3 : 현재와 미래의 지능정보사회 지능정보 이용문화 문제에 대한 심각성의 차이가 있을 것이다.

H1-4 : 현재와 미래의 지능정보사회 지능정보 신뢰성 문제에 대한 심각성의 차이가 있을 것이다.

H1-5 : 현재와 미래의 지능정보사회 사회적 문제에 대한 심각성의 차이가 있을 것이다.

두 번째 가설은 지능정보사회 사이버역기능에 대해서 남녀 간의 인식차이에 대해서 살펴보았다.

H2 : 지능정보사회 사이버 역기능 문제에 대한 남녀의 심각성 인식 차이가 있을 것이다.

세 번째 가설은 지능정보사회 사이버역기능에 대해서 세대별 인식차이에 대해서 살펴보았다.

H3 : 지능정보사회 사이버 역기능 문제에 대한 세대별 심각성 인식 차이가 있을 것이다.

4.2 데이터 수집 및 분석 방법

본 연구에서 진행한 지능정보사회의 사이버 역기능 분류를 토대로 지능정보사회의 사이버 역기능 사회적 인식을 설문조사를 통해 확인하였다. 본 설문은 만 19세 이상의 성인을 대상으로 하였으며 수집한 표본의 수는 남자 200명, 여자 200명 총 400개이다. 이외 인구통계학적 변수는 다음 <표 6>과 같다.

<표 6> 인구통계학적 변수

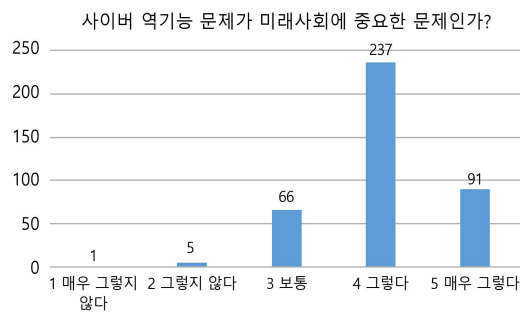
연령	20대	30대	40~50대	60세 이상
표본 수	100	100	140	60
비율	25.0%	25.0%	35.0%	15.0%

변수에 관한 측정 문항은 질문에 따라 총 두 가지로 설정하였다. 지능정보사회의 사이버 역기능에 대한 사회적 인식과 본 연구에서 제안한 지능정보사회의 사이버 역기능 분류 기준의 적절성은 다중항목 척도인 리커트 5점 척도(1 : 매우 그렇지 않다, 5 : 매우 그렇다)를 이용하였고, 지능정보사회의 사이버 역기능 심각성은 다중항목 척도인 리커트 5점 척도(1 : 매우 낮음, 5 : 매우 높음)를 이용하여 변수를 측정하였다.

본 연구에서 집단 간의 차이를 확인하기 위해 수집된 데이터의 분석을 IBM SPSS Statistics 25를 활용하였다. 현재와 미래의 사이버 역기능 인식 차이를 검증하기 위해서 대응표본 t-test를 실시하여 본 연구에서 제시한 가설을 검증하였고 성별에 따른 역기능 인식 차이를 확인하기 위해 독립표본 t-test를 실시하여 실증분석을 진행하였다. 또한 세대별 역기능 인식 차이를 확인하기 위해 ANOVA와 사후검증을 통해 실증분석을 진행하였다.

4.3 지능정보사회의 사이버 역기능에 대한 사회적 인식

본 연구에서는 설문조사를 통해 지능정보사회의 사이버 역기능에 대한 사회적 인식을 조사하였다. 지능정보사회의 사이버 역기능에 대한 사회적 인식에 대하여 조사한 결과 [그림 5]와 같이 전체의 82.1%(4 : 그렇다, 5 : 매우 그렇다의 합계)가 지능정보사회의 사이버 역기능 문제가 미래사회에 중요한 문제라고 답하였다.



[그림 5] 미래 지능정보사회에서의 사이버 역기능의 중요성

현재 발생하고 있는 사이버 역기능에 대한 심각성과 미래의 지능정보사회의 사이버 역기능에 대한 심각성을 <표 7>과 같이 비교 분석하였다. 현재의 경우 전체 평균 3.87($\sigma = 0.51$)로 전반적으로 심각성이 높다고 답하였다. 사이버 범죄가 평균 4.08($\sigma = 0.57$)로 가장 높았고 다음으로 지능정보 이용 문화($\mu = 3.83, \sigma = 0.63$), 권리 침해($\mu = 3.77, \sigma = 0.67$), 사회적 문제($\mu = 3.69, \sigma = 0.77$), 지능정보 신뢰성($\mu = 3.57, \sigma = 0.75$) 순으로 결과가 나타났다. 세부적으로는 <표 12>와 같이 사이버 범죄 및 테러 영역에서 피싱, 파밍, 스미싱($\mu = 4.20, \sigma = 0.80$), 허위 사실유포($\mu = 4.16, \sigma = 0.83$), 사이버 폭력($\mu =$

<표 7> 지능정보사회 사이버 역기능 5대 영역에 대한 현재 및 미래 심각성 평균

사이버역기능	현재		미래지능정보사회	
	평균	표준편차	평균	표준편차
사이버 범죄 및 테러	4.08	0.57	4.14	0.64
권리침해	3.77	0.67	3.91	0.69
지능정보이용문화	3.83	0.63	3.91	0.65
지능정보신뢰성	3.57	0.75	3.78	0.79
사회적 문제	3.69	0.77	3.81	0.83
전체	3.87	0.51	3.96	0.57

4.14, $\sigma = 0.84$)이 가장 심각하다고 나타났다.

미래 지능정보사회의 사이버역기능 심각성은 평균 3.96($\sigma = 0.57$)로 현재보다 더욱 심각할 것이라고 답하였다. 미래 지능정보사회 또한 사이버 범죄 및 테러가 평균 4.14($\sigma = 0.64$)로 가장 높은 결과가 나타났고 다음으로 권리침해($\mu = 3.91, \sigma = 0.69$), 지능정보 이용 문화($\mu = 3.91, \sigma = 0.65$), 사회적 문제($\mu = 3.81, \sigma = 0.83$), 지능정보 신뢰성($\mu = 3.78, \sigma = 0.79$) 순으로 결과가 나타났다. 세부적으로는 <표 12>와 같이 사이버 범죄 및 테러 영역에서 해킹($\mu = 4.26, \sigma = 0.81$)과 피싱, 파밍, 스미싱($\mu = 4.20, \sigma = 0.81$)이 가장 심각할 것이라고 나타났다.

4.4 가설 검증

본 연구에 제시한 가설인 현재의 심각성과 미래 지능정보사회의 사이버 역기능 심각성에 대한 차이가 통계적으로 유의한지 확인하기 위하여 t-test를 통해 검증하였다. <표 8>과 같이 현재와 미래 지능정보사회의 심각성의 차이에 대한 검증 결과 t값이 -6.302로 나타났으며 유의 수준이 $p < 0.05$ 에 속함으로 심각성에 대한 인식 차이가 존재하는 것으로 나타났으며 미래에 더욱 심각해 질 것으로 예측되었다.

<표 8> 현재와 미래지능정보사회의 사이버 역기능 심각성 인식 차이

독립변수	평균	표준편차	상관관계	GAP	t	P
현재	3.87	.510	0.845	0.09	-6.302	.000
미래지능정보사회	3.96	.573				

또한 지능정보사회의 사이버 역기능 유형별로 현재의 심각성과 미래 지능정보사회의 심각성에 대한 차이를 통계적으로 유의한지 확인하기 위하여 위와 동일하게 t-test를 통해 <표 9>와 같이 검증하였다. 검증결과는 모두 유의 수준이 $p < 0.05$ 에 속함으로서 모든 세부 유형들이 인식 차이가 있음을 알 수 있었다.

현재와 미래의 지능정보사회 사이버 역기능 심각성에 대해서 남녀별 인식 차이가 존재하는지 확인하기 위하여 t-test를 통해 검증하였다. <표 10>과 같이 현재의 지능정보사회 사이버 역기능 심각

성의 남녀별 인식 차이에 대한 검증 결과 t값이 -4.169로 나타났으며 유의수준이 $p < 0.05$ 이므로 성별에 따른 인식 차이가 존재하는 것으로 나타났다. 또한 미래의 지능정보사회 사이버 역기능 심각성의 남녀별 인식 차이에 대한 검증 결과도 t값이 -3.912($p < 0.05$)로 성별에 따른 인식 차이가 존재하는 것으로 나타났다. 남녀 간의 평균값을 보았을 때 현재의 경우 남성이 3.77, 여성이 3.98로, 미래의 경우 또한 남성이 3.86, 여성이 4.08로 여성이 사이버 역기능 문제에 대하여 더욱 심각하게 인식함을 확인 할 수 있다.

<표 9> 5대 역기능 유형별 현재와 미래지능정보사회의 사이버 역기능 심각성 인식 차이

독립변수	시대	평균	표준편차	상관관계	GAP	t	P
사이버 범죄 및 테러	현재	4.08	0.57	0.758	0.06	-2.789	.006
	미래지능정보사회	4.14	0.64				
권리침해	현재	3.77	0.67	0.642	0.14	-4.8	.000
	미래지능정보사회	3.91	0.69				
지능정보이용문화	현재	3.83	0.63	0.787	0.08	-3.67	.000
	미래지능정보사회	3.91	0.65				
지능정보신뢰성	현재	3.57	0.75	0.61	0.21	-6.043	.000
	미래지능정보사회	3.78	0.79				
사회적문제	현재	3.69	0.77	0.672	0.12	-3.59	.000
	미래지능정보사회	3.81	0.83				

<표 10> 남녀별 현재와 미래지능정보사회의 사이버 역기능 심각성 인식 차이

독립변수	성별	평균	표준 편차	t	P
현재	남	3.77	0.49	-4.169	.000
	여	3.98	0.51		
미래지능정보사회	남	3.86	0.54	-3.912	.000
	여	4.08	0.59		

<표 11> 세대별 현재와 미래지능정보사회의 사이버 역기능 심각성 인식 차이

변수	제공함	평균제공	F	P	
현재	집단-간	1.275	0.425	1.641	0.179
	집단-내	102.597	0.259		
	전체	103.873			
미래지능정보사회	집단-간	0.764	0.255	0.772	0.510
	집단-내	130.539	0.330		
	전체	131.303			

세대별 차이 또한 ANOVA 방법론을 통해 차이를 검증 하였으나 전 항목에 대해 유의 수준이 $p > 0.05$ 로 나타나 차이를 확인할 수 없었다.

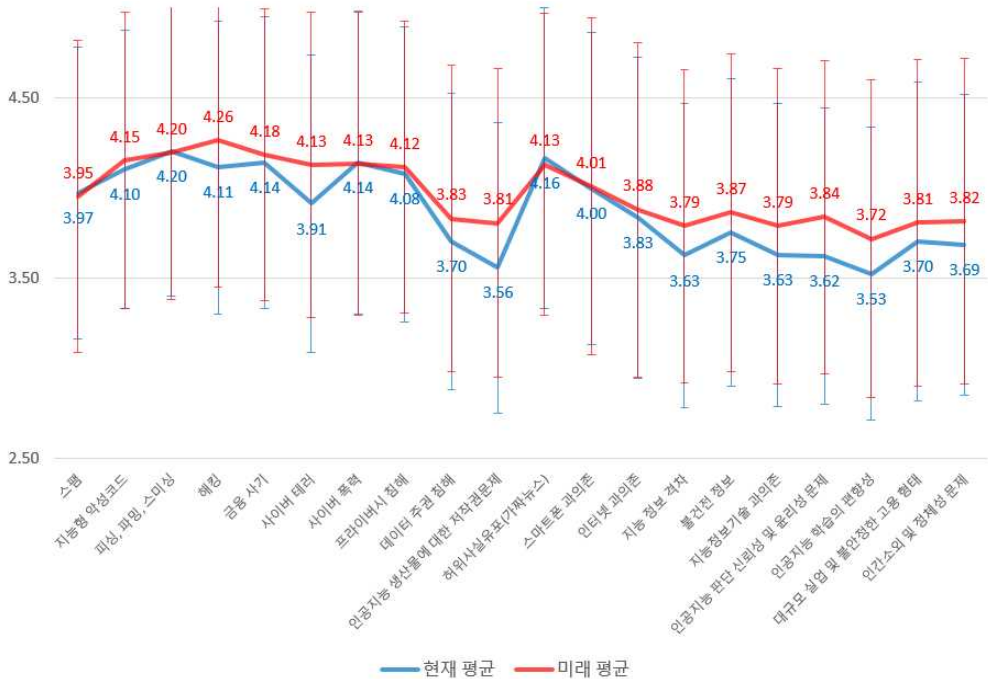
4.5 현재와 미래 지능정보사회의 사이버 역기능 심각성 GAP 분석

현재와 미래 지능정보사회의 사이버 역기능별 심각성 차이를 <표 12>와 [그림 6], [그림 7]과 같이 GAP분석을 실시하였다. [그림 7]에서 모든 사이버 역기능들이 미래 지능정보사회에서 더욱 심각할 것이라는 결과를 확인할 수 있다. 특히 권리침해, 지능정보 신뢰성 영역에서 비교적 큰

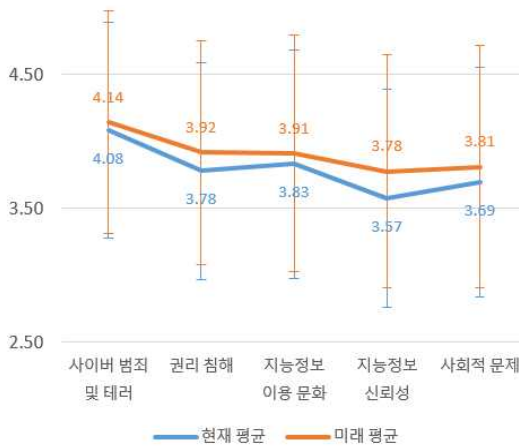
차이가 있음을 확인할 수 있다. [그림 6]에서는 피싱, 파밍, 스미싱, 사이버 폭력, 스팸, 허위사실 유포(가짜뉴스)를 제외한 모든 역기능들이 미래 지능정보사회에서 더욱 심각할 것이라는 결과를 확인할 수 있다. 특히 인공지능 생산물에 대한 저작권문제, 인공지능 판단 신뢰성 및 윤리성 문제, 사이버 테러, 인공지능 학습의 편향성 부분에서 차이가 크게 나타남($GAP > 0.19$)을 알 수 있다. 또한, 지능 정보 격차, 지능정보기술 과의존, 해킹, 인간소외 및 정체성 문제, 데이터 주권 침해, 불건전 정보, 대규모 실업 및 불안정한 고용 형태에서 차이($GAP > 0.1$)가 있음을 확인할 수 있다.

<표 12> 지능정보사회 사이버 역기능 현재 및 미래 심각성 평균 GAP

지능정보사회 사이버 역기능	현재 평균	미래 평균	현재 표준편차	미래 표준편차	GAP
스팸	3.97	3.95	0.81	0.864	-0.02
지능형 악성코드	4.10	4.15	0.77	0.821	0.05*
피싱, 파밍, 스미싱	4.20	4.20	0.802	0.815	-0.01
해킹	4.11	4.26	0.81	0.813	0.15**
금융 사기	4.14	4.18	0.811	0.81	0.04*
사이버 테러	3.91	4.13	0.823	0.844	0.22***
사이버 폭력	4.14	4.13	0.839	0.841	-0.01
프라이버시 침해	4.08	4.12	0.816	0.808	0.04*
데이터 주권 침해	3.70	3.83	0.819	0.85	0.13**
인공지능 생산물에 대한 저작권문제	3.56	3.81	0.805	0.854	0.25***
허위사실유포(가짜뉴스)	4.16	4.13	0.832	0.834	-0.03
스마트폰 과의존	4.00	4.01	0.866	0.933	0.01*
인터넷 과의존	3.83	3.88	0.89	0.926	0.05*
지능 정보 격차	3.63	3.79	0.843	0.868	0.16**
불건전 정보	3.75	3.87	0.85	0.88	0.11**
지능정보기술 과의존	3.63	3.79	0.84	0.873	0.16**
인공지능 판단 신뢰성 및 윤리성 문제	3.62	3.84	0.82	0.868	0.22***
인공지능 학습의 편향성	3.53	3.72	0.81	0.88	0.19***
대규모 실업 및 불안정한 고용 형태	3.7	3.81	0.884	0.904	0.11**
인간소외 및 정체성 문제	3.69	3.82	0.832	0.902	0.13**
GAP > 0.19***	GAP > 0.11**		GAP > 0*		GAP < 0



[그림 6] 지능정보사회의 사이버 역기능 현재 및 미래 심각성-사이버 역기능 요소별



[그림 7] 지능정보사회의 사이버 역기능 현재 및 미래 심각성-사이버 역기능 분류별

5. 결 론

본 연구에서는 우리 사회의 변화에 따른 지능정보사회 사이버 역기능을 분류하고 이를 토대로 현재와 미래 지능정보사회의 사이버 역기능 심각성

에 대한 인식을 분석하여 역기능 심각성 차이와 남녀별 심각성 인식 차이를 검증하였다. 이를 위해 크게 세 가지 가설을 설정하여 모형을 수립하고, 설문조사 데이터로 실증적 분석을 실시하였다.

지능정보사회의 사이버 역기능 분류는 현재 제정된 법률과 관련 부처의 보고서 등의 문헌분석을 통해 키워드를 추출하고 FGI 방법론을 통하여 최종적으로 사이버 범죄 및 테러, 권리 침해, 지능정보 이용 문화, 지능정보 신뢰성, 사회적 문제로 총 5대 영역으로 유형을 분류하였다.

이후 본 연구에서 제시한 지능정보사회의 사이버 역기능 분류 기준을 토대로 현재와 미래 지능정보사회의 사이버 역기능 심각성에 대한 인식을 설문조사를 통해 분석하였다. 지능정보사회에서의 사이버 역기능 문제가 미래사회에 중요한 문제임을 확인 할 수 있었고 현재보다 미래 지능정보사회에서 심각성이 더욱 높을 것이라는 연구 결과를 확인할 수 있었다.

현재 사이버 범죄를 가장 심각하게 생각하고

있으며 그중에서도 피싱, 파밍, 스미싱과 허위사실 유포가 가장 높은 심각성이 나타났다. 또한 미래 지능정보사회에서는 사이버 범죄가 가장 심각하게 나타났으며 그중에서도 해킹과 피싱, 파밍, 스미싱이 가장 높은 심각성을 나타내었다. GAP 분석 결과, 인공지능 생산물에 대한 저작권 문제, 인공지능 판단 신뢰성 및 윤리성 문제, 사이버 테러 순으로 심각성이 더욱 심화될 것이라는 연구 결과를 확인할 수 있었다. 미래 지능정보사회의 심각성과 GAP을 종합적으로 분석하면 인공지능 생산물에 대한 저작권 문제, 사이버테러, 인공지능 판단 신뢰성 및 윤리성 문제, 해킹, 지능형 악성코드가 심각성이 높아질 것으로 나타났다.

이를 통해 앞으로 지능정보사회에서 인공지능 역기능 문제가 가장 중요한 문제로 대두되고 있으며 인공지능에 대한 신뢰성과 안전성을 확보하여 사회적 요구를 충족시켜야 한다고 해석할 수 있다. 또한 지능화되고 있는 사이버 범죄에 대해서도 해결 방안을 도출하여 사회적 요구를 충족시켜야 한다. 이 외에도 5대 영역에 대하여 미래 사회에 대한 불안감을 개선하기 위하여 우리 사회가 노력해 나가야 할 것이다.

다만, 지능정보사회의 사이버 역기능 요소 중 피싱, 파밍, 스미싱, 사이버 폭력, 스팸, 허위사실 유포(가짜뉴스)에 대해서는 미래사회에서의 심각성이 현재보다 소폭 감소되는 양상을 확인할 수 있었다. 이 요소들은 현재 사회에서 가장 심각한 사이버 역기능으로 제시되고 있는 문제들이지만 미래 사회에서는 인공지능, 지능적 사이버 테러에 비하여 비교적 기술적, 사회적 변화를 가져올 수 있다는 인식으로 해석할 수 있으며 지능정보기술의 순기능으로 해석할 수도 있다.

또한 남녀 간의 지능정보사회의 사이버 역기능 심각성 인식 차이도 확인할 수 있었다. 여성이 위험 기피적인 경향이 있고 부정적 감성에 대하여 예민하게 반응한다는 기존연구와 같이 여성이 현재와 미래 사회에 대한 사이버 역기능 심각성을 더욱 민감하게 인식하고 있었다. 그러나, 세대별

인식의 차이는 나타나지 않았다.

추후 지능정보사회의 사이버 역기능을 해소할 수 있는, 특히 인공지능과 사이버 테러를 해소할 수 있는 기술과 서비스에 대한 연구가 필요하며 한 요소의 해결이 아닌 미래사회의 사이버 역기능 전체를 해소할 수 있는 기술적, 사회적, 문화적 시도가 필요하다. 또한 사이버 공간의 가장 중요한 이슈인 신뢰성을 확보할 수 있는 연구도 시도되어야 할 것이다.

참고문헌

- 관계부처 합동, “제4차 산업혁명에 대응한 지능정보 사회 중장기 종합대책”, 관계부처 합동, 2016.
- 국가법령정보센터 “국가정보화기본법 법률 제15369호”, 2019, Available at <http://www.law.go.kr/> 법령/국가정보화기본법(Accessed February 22, 2019).
- 권문주, 최연숙, 김태웅, “정보격차 해소 차원에서의 전자정부 서비스 이용촉진 연구 : 장노년층 사례를 중심으로”, *한국IT서비스학회지*, 제9권, 제2호, 2010, 73-92.
- 권정인, 이성철, 안성진, “사회현상학 관점에서의 인터넷역기능 분류체계 표준화 연구”, *컴퓨터교육학회 논문지*, 제14권, 제6호, 2011, 1-10.
- 백승익, 임규건, 여등승, “인공지능과 사회의 변화”, *정보화정책저널*, 제23권, 제4호, 2016, 3-23.
- 서인주, 정지영, “생활주기에 따른 현재와 미래 주거 선택 요인”, *예술인문사회융합멀티미디어논문지*, 제7권, 제4호, 2017, 315-327.
- 성지은, 정병길, “脫주격형 혁신체제에서의 기술 위협 관리”, *과학기술학연구*, 제7권, 제1호, 2007, 33-66.
- 송봉규, “제4차 산업혁명기술과 범죄에 대한 탐색적 연구”, *한국테러학회보*, 제12권, 제2호, 2019, 73-98.
- 양승돈, 김형욱, “사이버테러의 정세변화와 대응방안 연구”, *한국테러학회보*, 제11권, 제2호, 2018,

- 84-98.
- 우매리, “인터넷의 역기능과 인터넷 윤리 활성화 방안”, *신학과 목회*, 제43권, 2015, 297-318.
- 이원태, 문정욱, 양수연, “지능정보사회에서의 이용자보호 이슈 및 정책 방안 연구”, 방송통신위원회 방통융합정책연구, 2017.
- 이원태, “지능정보사회의 전개와 대응”, 경제·인문사회연구회 현신성장연구단, 2018.
- 이윤배, “인터넷 역기능 예방을 위한 인터넷 윤리 교육 개선 방안”, *한국정보통신학회논문지*, 제17권, 제6호, 2013, 1432-1440.
- 이정아, “지능화 시대, 새로운 대한민국으로 빅데이터 인하라”, 한국정보화진흥원, 2016.
- 이진권, “위험기피도 및 성격속성의 남녀 간 성별 차이에 관한 실험 연구”, *인문사회과학연구*, 제17권, 제1호, 2016, 565-588.
- 이흥재, 박미경, 차용진, “4차 산업혁명 역기능 대응 방안의 정책우선순위 분석”, *한국공공관리학보*, 제32권, 제4호, 2018, 27-50.
- 임규건, 류미나, 이정미, “개인정보유출 피해 비용 산출 모델에 관한 연구.” *정보보호학회논문지*, 제28권, 제1호, 2018, 215-227
- 임종인, “[포럼] 글로벌 사이버보안 규제 대비해야”, *디지털타임스*, 2018.
- 정보통신전략위원회, “지능정보사회 구현을 위한 제6차 국가정보화 기본계획(2018년~2022년)”, 정보통신전략위원회, 2018.
- 주윤경, “지능정보사회와 정보불평등”, *한국인터넷 자유평정기구*, 제33호, 2018, 33-37.
- 최성수, “남녀 성별에 따른 인지 행동적 차이에 관한 연구”, *디지털디자인학연구*, 제15권, 제4호, 2015, 307-318.
- 한국정보화진흥원, “2018 국가정보화백서”, 한국정보화진흥원, 2018.
- 한국정보화진흥원, “지능화 연구 시리즈 지능정보사회의 새로운 과제와 대응 방안”, 한국정보화진흥원, 2017.
- Bajtelsmit, V.L. and J.L. VanDerhi, “Risk Aversion and Pension Investment Choices”, *Positioning Pensions for the Twenty-First Century*, 1997, 45-66.
- Harbaugh, W.T., K. Krause, and L. Vesterlund, “Risk attitudes of children and adults : Choices over small and large probability gains and losses”, *Experimental Economics*, Vol.5, No.1, 2002, 53-84.
- Johnson, J.E.V. and P.L. Powell, “Decision making, risk and gender : Are managers different?”, *British Journal of Management*, Vol.5, 1994, 123.
- Lee, J.K., D.G. Cho, and G.G. Lim, “Design and Validation of the Bright Internet”, *Journal of the Association for Information Systems*, Vol.19, No.2, 2018, 63-85.
- Ponemon Institute, “2017 Cost of Cyber Crime Study”, Ponemon Institute, 2017.
- Shin, Y.Y., J.K. Lee, and M.Cl Kim, “Preventing State-Led Cyberattacks Using the Bright Internet and Internet Peace Principles”, *Journal of the Association for Information Systems*, Vol.19, No.3, 2018, 152-181.
- Vieider, F.M., T. Chmura, T. Fisher, T. Kusakawa, P. Martinsson, F.M. Thompson, and A. Sunday, “Within-versus between-country differences in risk attitudes : Implications for cultural comparisons”, *Theory and Decision*, Vol.78, No.2, 2015, 209-218.
- Weber, E.U., A.R. Blais, and N.E. Betz, “A domain-specific risk-attitude scale : Measuring risk perceptions and risk behaviors”, *Journal of Behavioral Decision Making*, Vol.15, 2002, 263-290.

◆ About the Authors ◆



임 규 건 (gglim@hanyang.ac.kr)

한양대학교 경영대학 임규건 교수는 KAIST 전산학 학사, POSTECH 컴퓨터 석사, KAIST 경영공학 박사학위를 취득하였고, 삼성전자, KT, 국제전자상거래연구센터(ICEC) 연구위원, 세종대학교 경영학과 교수를 역임하였다. 관심 분야는 혁신 비즈니스모델, IT서비스 혁신, 인공지능과 경영, e-Business 등이며, 2018년 IT서비스 우수연구인상을, 2009년 IT Innovation 유공자 지식경제부 장관 표창과 2007년 SW산업발전 유공자 정통부 장관 표창을 수여하였다. 주요 저서로는 '경영을 위한 정보기술', 'e-비즈니스 경영', '디지털경제시대의 경영정보시스템' 등 전문서적과 다수의 논문과 특허가 있다. 또한, 아시아최초 상용인터넷인 KORNET상용화, 중국 Shanghai Telecom SI사업전략, 한국 영화기술 로드맵, KTI 사업전략, 나라장터(G2B) 효과평가, 행정정보화(G4C) 성과분석, 국가정보보호지수개발, 국방정보화 수준평가모형, IT혁신인력양성종합대책, 국가디지털식별체계(UCI) 개선방안, 저작권정품인증제도, SW사업자신고제도개선, SW기술자신고제도개선 등 다양한 IT혁신 분야의 프로젝트를 수행하였다.



안 재 익 (anssame@hanyang.ac.kr)

한양대학교 경영대학 비즈니스인포매틱스학과 석사과정에 재학 중이다. 관심 분야는 빅데이터 분석, 디지털마케팅, 혁신비즈니스모델, e-비즈니스 등이다.