Information Systems Review
Vol. 22, No. 3 August 2020 http://dx.doi.org/10.14329/isr.2020.22.3.099

Bright Internet 신뢰네트워크 도입에 따른 지능정보사회의 사이버 역기능 해소에 대한 인식 분석

Analysis on the Perception of the Cyber Dysfunction in the Intelligent Information Society According to the Introduction of the Bright Internet Trust Network

임 규 건 (Gyoo Gun Lim) 한양대학교 경영대학 경영학부 교수
안 재 익 (Jae Ik Ahn) 한양대학교 경영대학 석사과정, 교신저자

요 약

현재 우리 사회는 4차 산업혁명의 물결 속에서 지능정보사회로 전개되고 있으며 이러한 변화는 모든 분야를 혁신시키는 긍정적 효과를 가져 올 것이다. 하지만 기술의 양면성으로 순기능과 동시에 역기능이 발생되고 있다. 지능화에 의해 해킹, 테러, 개인정보 침해, 불법콘텐츠 유통 등 사이버 역기능에 대한 위협은 더욱 심각해 질 것이다. 지금까지 인터넷의 보안 체계는 사후적(Proactive) 보안체계였으나 근래에 예방적(Preventive) 보안체계 방안인 신뢰네트워크에 대한 제안이 이루어지고 있다. 이에 본 연구에서는 신뢰네트워크 기술 중 하나인 Bright Internet에 대해서 지능정보사회의 사이버 역기능 해소 가능성을 분석하고자 한다. 본 연구에서는 지능정보사회의 사이버 역기능을 정의하고 Bright Internet 5대 원칙 도입에 대한 지능정보사회의 사이버 역기능 변화에 대한 인식을 분석한다. 연구결과 Brighit Internet 신뢰네트워크 도입으로 인한 지능정보사회의 역기능 해소가 가능하며 특히 사이버 범죄 및 테러, 권리침해 영역의 개선이 클 것으로 예측되었다. 5대 원칙 중에는 확인 가능한 익명성의 원칙과 국제 협력 조사 원칙이 역기능 해소의 기대치가 높게 나타나 효과가 클 것으로 분석되었다.

키워드: 지능정보사회, 사이버 역기능, 밝은인터넷, Bright Internet, 신뢰네트워크, 인공지능

† 이 논문은 2018년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2018S1A5A2A01035729). ㈜글로벌리서치가 실시한 설문조사 결과를 포함하고 있음. 초기 버전은 2019년 한국 춘계학술대회에 발표되었음.

Ⅰ. 서 론

현재 우리 사회는 4차 산업혁명의 물결 속에서 지능정보기술을 토대로 지능정보사회로 발전하고 있다. 이러한 변화는 인류 문명의 새로운 패러다임을 제시하고 모든 분야를 혁신시키는 긍정적 효과를 가져올 것이다. 하지만 기술의 양면성으로 순기능과 동시에 역기능이 발생되고 있다. 해킹 기술로 무장한 테러단체, 범죄자들의 공격은 미래 산업 전반의 위협요인이 되고 있으며, 개인정보 침해, 불법콘텐츠 유통, 사이버불링 등 다양한 역기능이 나타나고 있다(전영은, 김정연, 2014). 또한, 정보 보안에 대한 공격 수법이 지능화되고 이에 따른 피해 규모도 커지고 있다(전민서, 장항배, 2019). 특히 4차 산업 시대 혁신기술 중 하나인 블록체인 기반 암호화폐의 해킹사례나 빅데이터 기반 지능화 로봇 해커의 등장은 미래 사회의 사이버 위험이 기하급수적으로 증가하고 사이버 보안이 불가능에 가까울 정도로 어려워 질 것이라는 점을 경고하고 있다(임종인, 2018).

지금까지 지능정보에 대한 연구는 기술 자체의 발전에 초점이 주로 맞추어 졌으나 이제 지능정보기술로 인한 우리 생활과 사회의 변화 및 위협에 관심을 가져야 할 때이다(National Science and Technology Council Committee, 2016a, 2016b). 기술이 우리 사회에 순기능만 제공하는 것이 아니기 때문에, 혁신 기술로 인한 사회적 문화적 변화에 대해 고민하고 이에 대한 기술적, 사회적, 문화적, 정책적 대응을 통합적으로 준비해야 한다(김병운, 2016; 백승익 등, 2016; 이원태 등, 2015; 황종성, 2016). 또한, 기술적인 보안 대책은 정교하게 만들기 위해 많은 비용과 시간이 드는데 반해 이에 대한 해킹 기술은 비교적 정교하지 않은 방법으로도 기술적 보안을 무기력화 하는 경우가 상당히 많아 단순히 기술적인 접근만으로는 해결할 수 없기에 통합적인 대응을 통해 피해를 최소화 하는 것을 목적으로 두어야 할 것이다(윤일한, 권순동, 2015)

지금까지 인터넷 네트워크는 TCP/IP 자체가 보안에 대한 고려를 많이 하지 않아서 개별 시스템을 자기 스스로 보호해야하는 사건 발생 후에 보호하는 사후적(Proactive) 보안체계였다. 근래에 이러한 위협 원인을 예방적으로 근본적으로 제거할 수 있는 신뢰네트워크가 제안되고 있다. 그 중 Bright Internet(밝은 인터넷)은 세계정보시스템학회(Association for Information Systems, AIS)에서 이재규 교수의 제안으로 AIS 비전으로 채택되어 연구주제화 되었다(Lee *et al.*, 2018). Bright Internet은 예방적(Preventive) 보안체계로써 발생자 책임의 원칙, 전달자 책임의 원칙, 확인 가능한 익명성의 원칙, 국제 협력 조사의 원칙, 프라이버시 보호의 원칙으로 구성되는 5가지 원칙으로 설계하는 차세대 인터넷 네트워크이다(Lee *et al.*, 2018). 이와 관련하여 필요성과 기본적으로 필요한 요소기술 등에 대한 연구가 진행 중이다. 본 연구에서는 사이버 역기능을 해소 할 수 있는 방안인 Bright Internet 신뢰 네트워크의 5대 원칙에 대해서 역기능 해소 가능성에 대한 사회적 인식을 조사해 보고자 한다. 이를 토대로 적절한 신뢰 네트워크 구조와 실용적인 기술적 도입의 방향을 모색할 수 있을 것이다.

이를 위해서 제Ⅱ장 선행연구에서는 지능정보사회에서의 사이버 역기능과 Bright Internet을 중심으로 신뢰네트워크에 대해서 살펴본다. 제Ⅲ장에서는 연구 설계를 하며 제Ⅳ장에서 신뢰네트워크 도입에 따른 역기능 해소에 대한 인식을 분석하고 Bright Internet 5대 원칙별 인식을 분석하며 신뢰네트워크 도입으로 인한 미래 사이버 역기능 감소 효과를 살펴보고 제Ⅴ장에서 마무리 한다.

Ⅱ. 선행연구

2.1 지능정보사회의 사이버 역기능

지능정보사회의 근원은 4차 산업혁명으로의 사회 변화에 따라 발생된다. 제4차 산업혁명은 스위스 다보스에서 개최하는 세계경제포럼의 의장인 클

라우드 슈밥에 의하여 최초 주장되었고 46회 다보스포럼에서 “제4차 산업혁명의 이해”가 의제로 선정되면서 전 세계적인 화두로 등장하게 되었다(김재호, 김권일, 2017; 이원태, 강장묵, 2016). 대한민국 정부에서도 “제4차 산업혁명 촉진 기본법안”의 등장으로 4차 산업혁명을 통해 전개되는 지능정보사회 전반에 활용되는 지능정보기술을 인공지능과 데이터 활용을 융합하여 기계에 인간의 고차원적 정보처리를 구현하는 기술이라고 정의하고 있으며 AI(Artificial Intelligence), 빅데이터, IoT 등의 초연결, 초지능화 특성을 지닌 기술을 포함하고 있다(관계부처 합동, 2016; 김재호, 김권일, 2017)

지능정보사회로의 전개는 우리 사회의 전반적인 시스템을 변화시키고 개인의 실생활에도 혁신적인 변화를 가져오지만 기술 발전의 양면성에 따라 역기능도 발생시킬 수 있다(이홍재 등, 2018; 임규건 등, 2018). 4차 산업혁명의 대표적인 혁신기술인 블록체인 기반 암호 화폐 해킹사례와 랜섬웨어와 같은 지능형 악성코드로 기존 발생 되었던 사이버 역기능의 범위와 피해가 더욱 크다는 것을 확인할 수 있다. 하지만 지능정보기술의 순기능에 집중하여 역기능에 대한 관심이 상대적으로 적은 상황이며 관련 연구도 부족한 실정이다(송봉규, 2019). 이러한 상황에서 지능정보사회에 대한 기술적, 사회적, 문화적, 정책적 대응을 준비하는 것이 필요하며 사이버 공간의 중요 이슈인 신뢰성을 확보할 수 있는 기술적 요구도 반드시 준비해야할 것이다.

사이버 역기능은 인터넷 등의 정보통신기술을 사용함에 있어 발생할 수 있는 모든 부작용을 의미한다(이윤배, 2013; 우매리, 2015). 사이버 역기능에 대해서는 미디어중독, 유해 콘텐츠, 사이버 폭력, 권리침해, 사이버테러, 판단장애 등 다양한 분류와 연구가 진행되었었다(권정인 등, 2011). 그러나 우리 사회는 지능정보사회로 전개되며 사이버 역기능의 위험성과 범위를 확대되고 있지만 기존의 연구는 정보사회에서의 사이버 역기능을 중심으로 전개되어 지능정보사회에서 발생할 수 있는 역기능, 즉 IOT, 인공지능, 빅데이터 등의 지능정보기술에 대한 역기능 연구가 부족한 실정이다(송봉규, 2019).

임규건, 안재익(2020)에서는 지능정보사회에서 발생할 수 있는 다양한 사이버 역기능들을 파악하기 위해 인터넷, 정보기술, 지능정보화와 관련된

〈표 1〉 지능정보사회의 사이버 역기능(임규건, 안재익, 2020)

5대 영역	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, 문자 메시지를 이용한 피싱 기법
	해킹	남의 컴퓨터 시스템에 허락 없이 침입하여 데이터를 빼내거나 파괴하는 행위
	금융사기	범행 대상자에게 인터넷메일, SMS 등을 이용해 금전적 피해를 야기하는 사기수법
	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

〈표 1〉 지능정보사회의 사이버 역기능(임규건, 안재익, 2020)(계속)

5대 영역	사이버 역기능	정의
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	
	지능 정보 격차	지능 정보에 대한 접근이 경제적, 성별, 연령별로 불균형하게 나타나는 현상을 의미함
	불건전 정보	사이버 상에 유포된 불건전한 정보(음란물 등)를 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 혼동되는 상태

‘국가정보화 기본법’, ‘지능정보사회 중장기 종합대책’, ‘국가정보화백서’의 법률 및 보고서 등을 분석하고 FGI 방법론을 통해 다섯 가지 유형으로 지능정보사회의 사이버 역기능을 분류하였다. 본 연구에서는 <표 1>과 같이 지능정보사회의 사이버 역기능을 사이버 범죄 및 테러, 권리 침해, 지능정보 이용 문화, 지능정보 신뢰성, 사회적 문제의 5대 영역으로 구분하였다. 사이버 범죄 및 테러는 스팸, 지능형 악성코드, 피싱, 파밍, 스미싱, 해킹, 금융사기, 사이버 테러, 사이버 폭력의 세부 항목으로, 권리 침해는 프라이버시 침해, 데이터 주권 침해, 인공지능 생산물에 대한 저작권 문제로, 지능정보 이용 문화는 허위사실 유포, 스마트폰 과의존, 인터넷 과의존, 지능 정보 격차, 불건전 정보, 지능정보기술 과의존으로, 지능정보 신뢰성은 인공지능판단 신뢰성 및 윤리성 문제, 인공지능 학습의 편향성, 사회적 문제는 대규모 실업 및 불안정한 고용 형태, 인간소외 및 정체성 문제 등의 세부 항목으로 구성된다. 본 연구에서는 이러한 유형분류를 채택하여 사이버 역기능을 해소할 수 있는 신뢰네트워크에 대한 사회적 요구를 확인한다.

2.2 Bright Internet 신뢰네트워크

기존의 인터넷 네트워크는 보안에 대한 고려를 많이 하지 않아 개별 시스템을 자기 스스로 보호하는 사건 발생 후에 보호하는 사후적 보안체계이다. 하지만 지능정보기술의 빠른 발전과 변화로 인하여 지능화된 사이버 공격으로부터 자기 방어를 실현하기는 예산과 기술적 한계로 점점 더 불

가능하게 될 것이다. 이에 위협 원인을 예방적으로 제거할 수 있는 신뢰네트워크가 제안되고 있다. 신뢰 네트워크 기술로 TIPN(Trusted IP Network), Bright Internet, Black Core Network, TOR(The Onion Routing), SDP(Software Defined Perimeter) 등이 제안되고 있다(Cloud Security Alliance, 2014; Reed *et al.*, 1998).

TIPN은 초연결 신뢰네트워크로 신뢰할 수 있는 사람-사물-데이터가 실시간, 온디맨드로 연결되는 네트워크이다. 이는 사물의 연결로 디바이스-네트워크-클라우드에 대해서 시공간 초월적으로 고신뢰 연결성을 제공하며 유통되는 정보에 대한 신뢰성을 보장할 수 있는 네트워크 기술이다(정부금 등, 2017).

Bright Internet은 세계정보시스템학회(Association for Information Systems, AIS)에서 이재규 교수의 주창으로 The Bright Internet(밝은 인터넷)이 비전으로 채택되며 최초 제안되었다. Bright Internet은 예방적(Preventive) 보안체계로써 발생자 책임의 원칙, 전달자 책임의 원칙, 확인가능한 익명성의 원칙, 국제 협력 조사의 원칙, 프라이버시 보호의 원칙으로 구성되는 5가지 원칙으로 설계하는 차세대 인터넷 네트워크이다(Lee *et al.*, 2018). 발송자 책임의 원칙은 온라인 악성 정보를 생성한 원인자 주체에 책임을 부여하는 것을 의미하며 악의적인 목적으로 불법 유해 콘텐츠를 생산하는 정보 발송자에게 책임을 질 수 있도록 이를 추적하고 관리할 수 있는 기술을 포함한다. 전달자 책임 원칙은 악성 정보를 중개하는 개인 혹은 기관에도 책임을 부여하는 것을 의미하며 예방적 보안 시스템 설계, 중개자 기반의 예방적 감시 시스템 설계 등의 기술을 포함한다. 확인가능한 익명성의 원칙은 평소에는 익명성을 보장하고 악의적 위협 상황 발생 시 적절한 과정을 통해 원인자(또는 실명)를 확인 할 수 있는 것을 의미하며 확인가능한 익명성 아키텍처, 직간접 실명 확인 기술 등을 포함한다. 국제 협력 조사 원칙은 국가 간의 공조와 협약을 통해 사이버 테러를 조사하고, 테러 발생 국가에 대해서 정해진 규칙을 통해 제재를 가하는 체계를 의미하며 국제적 범위의 블랙리스트 관리 체계, 사이버 범죄 및 평가자 평가 모델, 국제적 범위의 발송자 IP 추적 기술 및 표준체계 등의 기술을 포함한다. 프라이버시 보호의 원칙은 신뢰네트워크 구현과 운영 중 정보 유출의 위험과 수집기관의 악용 위험을 방지하여 프라이버시를 보호함을 의미하며 전달자 책임 원칙에 대한 프라이버시 보호 감사, 확인가능한 익명성 원칙에 대한 프라이버시 보호 감사 등을 포함한다(Lee *et al.*, 2018; Shin *et al.*, 2018).

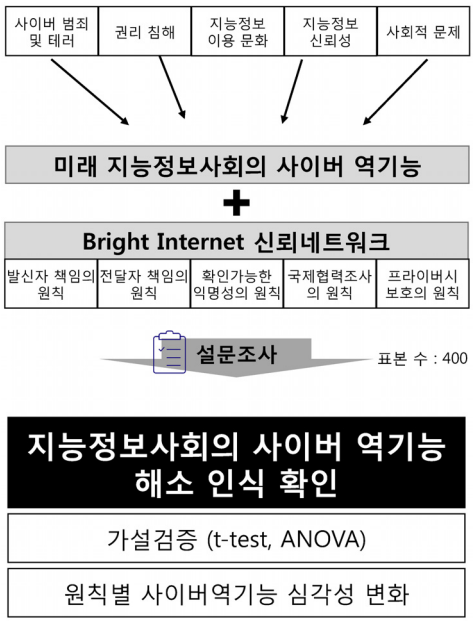
본 연구에서는 현재 연구진행 중인 Bright Internet의 효과성에 대해서 검증해 보고자 한다. 본 연구에서는 Bright Internet의 5대 원칙을 토대로 지능정보사회에서 사이버 역기능이 어느 정도 해소될 수 있는지에 대해서 사회적 인식을 조사하고 기술적 요구를 반영하여 신뢰네트워크 구현을 위한 실용적인 기술적 연구 방향을 제시한다.

Ⅲ. 연구 설계

3.1 연구 절차

본 연구에서는 신뢰네트워크 기술 중 Bright Internet을 기반으로 차세대 네트워크 보안체계를 수립하는데 도움이 되고자 지능정보사회의 사이버 역기능 해소를 위한 신뢰네트워크의 사회적 인식을 <그림 1>과 같은 절차로 확인한다. 이를 위해서 선행연구의 유형분류를 채택하여 지능정보사회의 사이버 역기능을 사이버 범죄 및 테러, 권리침해, 지능정보 이용 문화, 지능정보 신뢰성, 사회적 문제의 5대 영역으로 나누고 하위 역기능들에 대하여 신뢰네트워크 도입 시 역기능 해소 가능성을 설문조사를 통해 확인한다. Bright Internet 각 원칙별 역기능 해소에 대한 인식을 분석하여 기술적, 사회적 요구를 반영하고 미래 사회가 준비해야 할 신뢰네트워크의 연구 방향을 제시한다. 또한 이와 함께 신뢰네트워크의 도입으로 지능정보사

회 사이버 역기능 문제가 얼마나 해결될지에 대해서 그 심각성에 대한 인식 정도를 추정해 본다.



〈그림 1〉 연구 방법 및 절차

일반적으로 남녀 성별에 따른 정보처리 및 판단의 차이와 인지 능력에 대한 차이가 있으므로 사회과학적 분석에서 성별 차이를 고려해야 한다고 한다(이진권, 2016; 최성수, 2015). 본 연구에서는 신뢰네트워크의 도입에 따른 지능정보사회 사이버 역기능 해소에 대해서 성별, 연령별 차이 없이 모든 국민이 이러한 변화를 요구하고 있음을 확인하기 위하여 다음의 연구 가설들을 설정하였다.

H1: Bright Internet 신뢰네트워크의 도입은 지능정보사회 사이버 역기능 해소에 긍정적인 영향을 줄 것이다.

H2: Bright Internet 신뢰네트워크 도입으로 인한 지능정보사회 사이버 역기능 해소에 대한 성별에 따른 인식 차이는 없을 것이다.

H3: Bright Internet 신뢰네트워크 도입으로 인한 지능정보사회 사이버 역기능 해소에 대한 연령별 인식 차이는 없을 것이다.

3.2 데이터 수집 및 분석 방법

본 설문은 만 19세 이상의 성인을 대상으로 하였으며 표본의 수는 총 400개 이다. 전문조사기관인 ㈜글로벌리서치를 통해 표본은 남자 200명, 여자 200명을 대상으로 하였으며 인구통계학적 연령대는 다음 <표 2>와 같다.

〈표 2〉 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 대한 측정 문항은 Bright Internet 5대 원칙에 대하여 총 5가지로 설정하였으며 지능정보사회의 사이버 역기능 심각성과 신뢰네트워크 도입을 통한 지능정보사회 사이버 역기능 해소의 사회적 인식은 다중항목 척도인 리커트 5점 척도(1: 훨씬 더 악화됨, 3: 큰 변화 없음, 5: 훨씬 더 개선됨)를 이용하여 측정하였다.

분석은 역기능 개선 영향력이 비슷한 집단을 확인하기 위해 IBM SPSS Statistics 25를 활용하여 k-means 군집분석을 통해 군집을 3개로 나눠 신뢰네트워크의 개선효과를 비교분석하였다. 또한 성별에 따른 역기능 해소 인식 차이를 검증하기 위하여 독립표본 t-test를 실시하여 가설을 검증하였고, 연령별 역기능 해소 인식 차이를 검증하기 위하여 ANOVA 분석을 실시하여 가설을 검증하였다. 신뢰네트워크 도입으로 인한 지능정보사회의 사이버 역기능 심각성 변화는 5점 척도의 설문을 -100~100까지 스케일링한 후 각 원칙별 역기능 해소 정도에 대해서 추정하였다. 다만, 본 연구에서는 역기능 해소에 대한 정확한 값을 산출할 수 없어 역기능별 감소 비율을 확인하여 신뢰네트워크의 개선 영향력을 확인하였다.

Ⅳ. 분석 및 결과

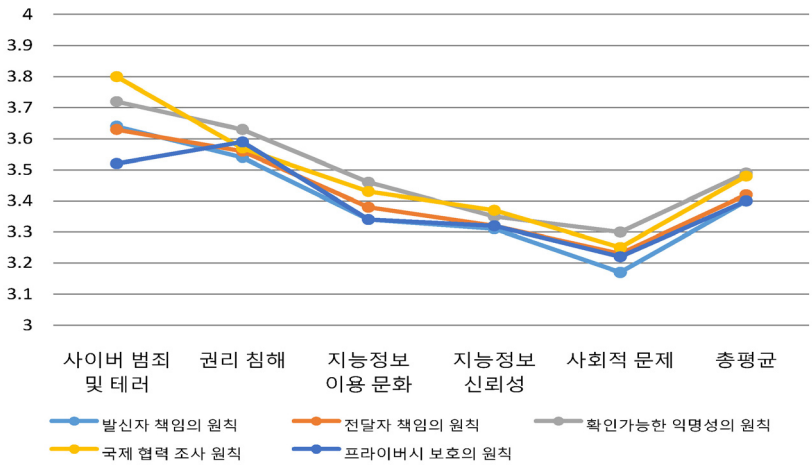
4.1 신뢰네트워크 도입으로 지능정보사회 사이버 역기능 해소에 대한 인식

본 연구에서는 설문조사를 통해 신뢰네트워크 도입으로 인한 지능정보사회의 사이버 역기능 해소의 인식을 확인하였다. 설문조사의 신뢰수준은 95%에서 표본오차 ±4.90%이다. 신뢰 네트워크의 도입은 <표 3>과 <그림 2>와 같이 지능정보사회의 사이버 역기능 5대 전 영역에 대해 사이버 역기능 개선에 긍정적인 영향이 있을 것(μ = >3)으로 나타났다. 그 중, 사이버 범죄 및 테러, 권리침해의 영역에서 개선 영향이 클 것으로 나타났으며 지능정보이용문화 영역 중 불건전 정보 또한 영향이 클 것으로 나타났다. 이것은 Bright Internet 체계의 주요 목적이 사이버 범죄와 테러의 원인 제공자를 확인할 수 있는 체계를 갖추어 범죄의 원인을 근원적으로 억제하는 것이기 때문일 것으로 사료된다. 원인자가 발생시킨 사이버 공격에 대한 대책이 주가 되고 기술적, 비즈니스적 문제들에 대한 방안은 다수 포함하고 있지만 사회적, 문화적 문제 해결은 약하다는 것을 확인할 수 있다.

또한 지능정보사회의 주된 이슈인 인공지능 문제에 대해서도 해소의 영향이 크지 않는 다는 것을 확인할 수 있다. 이는 현재 Bright Internet 신뢰네트워크 연구가 본질적으로 네트워크 개선점에 초점이 맞춰져 있기 때문에 인공지능을 원인으로 발생하는 역기능과 사회적 변화를 포함하지 못하고 있다는 것을 나타낸다.

〈표 3〉 신뢰네트워크 도입으로 인한 지능정보사회 역기능 해소에 대한 사회적 인식

지능정보사회의 사이버 역기능	발신자 책임의 원칙	전달자 책임의 원칙	확인가능한 익명성의 원칙	국제 협력 조사 원칙	프라이버시 보호의 원칙	평균
사이버 범죄 및 테러	3.64	3.63	3.72	3.80	3.52	3.66
권리 침해	3.54	3.56	3.63	3.57	3.59	3.58
지능정보 이용 문화	3.34	3.38	3.46	3.43	3.34	3.39
지능정보 신뢰성	3.31	3.32	3.35	3.37	3.32	3.33
사회적 문제	3.17	3.23	3.30	3.25	3.22	3.24
평균	3.40	3.42	3.49	3.48	3.40	3.44



〈그림 2〉 Bright Internet 도입으로 인한 지능정보사회 역기능 해소에 대한 인식

이에 미래 지능정보사회의 신뢰네트워크 구성 시 기술적 문제뿐만 아닌 사회적, 문화적 문제 또한 포함시켜야 하며 지능정보기술의 역기능들로 인한 역기능과 사회 변화를 포함시킬 수 있는 통합적인 사이버 공간 관리 체계를 고안할 필요가 있을 것으로 사료된다.

4.1.1 발송자 책임의 원칙

발송자 책임의 원칙의 적용으로 역기능 해소에 대한 사회적 인식에 대해서 역기능별 군집분석을 <표 4>와 같이 분석하였다. 표에서 쉐도우 처리한 부분은 함께 군집으로 묶인 것으로 역기능 해소가 잘 되는 항목들이다. 사이버 범죄 및 테러(μ = 3.64, σ = 0.94)와 권리침해(μ = 3.54, σ = 0.87)에 대해서 사이버 역기능이 효과적으로 개선될 것(μ = >3.5)이라고 인식하고 있다. 특히 하위 역기능에서 스팸이 평균 3.74(σ = 0.84)로 가장 높았고 다음으로 허위사실유포(μ = 3.69, σ = 1.02), 피싱, 파밍, 스미싱(μ = 3.68, σ = 0.95), 지능형 악성코드(μ = 3.66, σ = 0.90), 사이버 폭력(μ = 3.66, σ = 1.00) 순으로 결과가 나타나 사이버 범죄 및 테러와 권리침해의 하위 역기능과 지능정보이용문화의 허위사실유포, 불건전 정보는 발송자 책임의 원칙을 통해 역기능 해소가 가능할 것이라 인식하지만 그 외 타 영역

〈표 4〉 발송자 책임의 원칙의 적용으로 역기능 해소에 대한 사회적 인식

지능정보사회의 역기능		평균	표준편차
사이버 범죄 및 테러	스팸	**3.74****	0.84
	지능형 악성코드	**3.66****	0.90
	피싱, 파밍, 스미싱	**3.68****	0.95
	해킹	3.54*	0.93
	금융사기	**3.62****	0.98
	사이버 테러	**3.62****	0.97
	사이버 폭력	**3.66****	1.00
평균		3.64**	0.94
권리 침해	프라이버시 침해	**3.61****	0.93
	데이터 주권 침해	3.51*	0.86
	인공지능 생산물에 대한 저작권문제	3.51*	0.83
평균		3.54*	0.87
지능정보 이용문화	허위사실유포(가짜뉴스)	**3.69****	1.02
	스마트폰 과의존	3.17	0.85
	인터넷 과의존	3.21	0.84
	지능 정보 격차	3.22	0.81
	불건전 정보	3.51*	0.94
	지능정보기술 과의존	3.26	0.79
평균		3.34	0.87
지능정보 신뢰성	인공지능 판단 신뢰성 및 윤리성 문제	3.35	0.80
	인공지능 학습의 편향성	3.26	0.78
평균		3.31	0.79
사회적 문제	대규모 실업 및 불안정한 고용 형태	3.15	0.81
	인간소외 및 정체성 문제	3.19	0.79
평균		3.17	0.80
전체 평균		3.40	0.86
군집 A(Centroid = 3.66)**	군집 B*(Centroid = 3.52)	군집 C(Centroid = 3.23)	

에서는 큰 변화는 없을 것으로 추정할 수 있다.

사이버 범죄 및 테러와 권리침해의 영역은 발송자에 대한 기술적 방안으로 해소가 가능한 사이버 역기능으로 판단하고 발신자 책임의 원칙이 사이버 역기능에 대하여 개선이 가능할 것이고 인식하고 있음이 파악되었다. 지능정보이용문화의 허위사실유포(가짜뉴스)와 불건전 정보 또한 해당 영역의 타 역기능들과 다르게 기술적으로 해결 가능한 역기능으로 인식하고 있다고 볼 수 있다.

이는 기존에 수신자 책임을 중심으로 전개되었던 역기능 방지에 대하여 발송자에게 책임을 부여함으로써 역기능 개선의 새로운 패러다임을 제시한다. 또한 발송자에게 책임을 부여하여 이용자들이 기술 안정성에 대해 신뢰성을 높일 수 있음을 의미한다.

4.1.2 전달자 책임의 원칙

전달자 책임의 원칙 적용으로 역기능 해소에 대한 사회적 인식과 역기능별 영향력 군집을 <표 5>와 같이 분석하였다. 지능정보사회 사이버 역기능 5대

〈표 5〉 전달자 책임의 원칙의 적용으로 역기능 해소에 대한 사회적 인식

지능정보사회의 역기능		평균	표준편차
사이버 범죄 및 테러	스팸	**3.72****	0.85
	지능형 악성코드	**3.66****	0.88
	피싱, 파밍, 스미싱	**3.66****	0.93
	해킹	3.55*	0.93
	금융사기	**3.65****	0.91
	사이버 테러	3.59*	0.96
	사이버 폭력	**3.62****	0.98
평균		3.63**	0.92
권리 침해	프라이버시 침해	**3.64****	0.95
	데이터 주권 침해	3.52*	0.84
	인공지능 생산물에 대한 저작권문제	3.52*	0.87
평균		3.56*	0.89
지능정보 이용 문화	허위사실유포(가짜뉴스)	**3.66****	0.97
	스마트폰 과의존	3.25	0.83
	인터넷 과의존	3.29	0.79
	지능 정보 격차	3.27	0.76
	불건전 정보	3.51*	0.87
	지능정보기술 과의존	3.32	0.77
평균		3.38	0.83
지능정보 신뢰성	인공지능 판단 신뢰성 및 윤리성 문제	3.31	0.85
	인공지능 학습의 편향성	3.32	0.77
평균		3.32	0.81
사회적 문제	대규모 실업 및 불안정한 고용 형태	3.23	0.78
	인간소외 및 정체성 문제	3.23	0.78
평균		3.23	0.78
전체 평균		3.42	0.85
군집 A(Centroid = 3.66)**	군집 B*(Centroid = 3.54)	군집 C(Centroid = 3.28)	

영역에서 사이버 범죄 및 테러와 권리침해 영역이 효과적으로 개선될 것(μ = >3.5)으로 인식되고 있으며, 특히 하위 역기능에서 스팸(μ = 3.72, σ = 0.85), 지능형 악성코드(μ = 3.66, σ = 0.88), 허위사실유포(μ = 3.66, σ = 0.97), 파싱, 파밍, 스미싱(μ = 3.66, σ = 0.93), 금융사기(μ = 3.65, σ = 0.91)가 본 원칙을 통한 역기능 개선 가능성이 높게 평가되고 있다.

지능정보 이용 문화의 허위사실 유포와 불건전 정보는 발송자 책임의 원칙과 유사한 원인으로 사이버 범죄 및 테러, 권리 침해의 영역과 함께 전달자 책임의 원칙이 개선 가능할 것으로 인식하고 있음을 분석할 수 있다.

지금까지는 사이버 범죄에 대하여 수신자 방어를 기조로 발송자에 대한 책임 부여 및 추적을 가장 중요시 하여 정보 중개자인 전달자에 대한 책임이 비교적 작았다. 하지만 지능정보사회로 전개되면서 정보 통신의 중요성이 부각되고 있어 직접적 관여자인 전달자에 대해서도 책임 부여가 필요하다는 사회적 인식을 확인할 수 있다.

4.1.3 확인가능한 익명성의 원칙

확인가능한 익명성의 원칙 적용으로 역기능 해소에 대한 사회적 인식과 역기능별 영향력 군집을 <표 6>과

〈표 6〉 확인가능한 익명성의 원칙의 적용으로 역기능 해소에 대한 사회적 인식

지능정보사회의 역기능		평균	표준편차
사이버 범죄 및 테러	스팸	**3.77****	0.91
	지능형 악성코드	3.69*	0.93
	피싱, 파밍, 스미싱	**3.72****	0.97
	해킹	3.63*	0.98
	금융사기	**3.74****	0.93
	사이버 테러	**3.75****	0.96
	사이버 폭력	**3.76****	1.00
평균		**3.72****	0.96
권리 침해	프라이버시 침해	**3.73****	1.00
	데이터 주권 침해	3.59*	0.92
	인공지능 생산물에 대한 저작권문제	3.58*	0.88
평균		3.63*	0.93
지능정보 이용 문화	허위사실유포(가짜뉴스)	**3.81****	0.99
	스마트폰 과의존	3.31	0.84
	인터넷 과의존	3.30	0.77
	지능 정보 격차	3.31	0.78
	불건전 정보	3.66*	0.92
	지능정보기술 과의존	3.35	0.78
평균		3.46	0.85
지능정보 신뢰성	인공지능 판단 신뢰성 및 윤리성 문제	3.36	0.80
	인공지능 학습의 편향성	3.33	0.74
평균		3.35	0.77
사회적 문제	대규모 실업 및 불안정한 고용 형태	3.26	0.78
	인간소외 및 정체성 문제	3.34	0.75
평균		3.30	0.77
전체 평균		3.49	0.86
군집 A(Centroid = 3.75)**	군집 B*(Centroid = 3.63)	군집 C(Centroid = 3.32)	

같이 분석하였다. 사이버 범죄 및 테러, 권리침해 영역이 효과적으로 개선될 것(μ = >3.5)이라고 인식하고 있고, 하위 역기능에서 허위사실유포(μ = 3.81, σ = 0.99), 스팸(μ = 3.77, σ = 0.91), 사이버 폭력(μ = 3.76, σ = 1.00), 사이버테러(μ = 3.75, σ = 0.96), 금융사기(μ = 3.74, σ = 0.93), 프라이버시 침해(μ = 3.73, σ = 1.00), 피싱, 파밍, 스미싱(μ = 3.72, σ = 0.97), 지능형 악성코드(μ = 3.69, σ = 0.93), 불건전 정보(μ = 3.66, σ = 0.92)가 확인가능한 익명성의 원칙을 통한 역기능 개선 가능성을 높게 평가하고 있다.

정보사회에서 익명성으로 발생되는 역기능들을 본 설문조사 결과에서도 다수 포함되고 있음을 확인할 수 있었다. 인터넷 실명제가 2012년 위헌 판결이 내려지면서 익명성 보장과 인터넷 실명제 실시 사이에 여전히 많은 토론과 연구들이 진행되고 있는 가운데, 지능정보사회로 전개되는 현 시점에서 확인가능한 익명성의 원칙 도입 등과 같은 대안을 통해 역기능 해소가 필요하다는 사회적 요구를 확인할 수 있는 것으로 사료된다.

4.1.4 국제 협력 조사 원칙

국제 협력 조사 원칙 적용으로 역기능 해소에 대한 사회적 인식과 역기능별 영향력 군집을 <표 7>과

〈표 7〉 국제 협력 조사 원칙의 적용으로 역기능 해소에 대한 사회적 인식

지능정보사회의 역기능		평균	표준편차
사이버 범죄 및 테러	스팸	**3.79****	0.84
	지능형 악성코드	**3.82****	0.92
	피싱, 파밍, 스미싱	**3.85****	0.90
	해킹	**3.83****	0.95
	금융사기	**3.80****	0.91
	사이버 테러	**3.80****	0.91
	사이버 폭력	**3.73****	0.90
평균		**3.80****	0.91
권리 침해	프라이버시 침해	3.58*	0.89
	데이터 주권 침해	3.58*	0.85
	인공지능 생산물에 대한 저작권문제	3.57*	0.80
평균		3.57*	0.85
지능정보 이용 문화	허위사실유포(가짜뉴스)	3.61*	0.95
	스마트폰 과의존	3.33	0.78
	인터넷 과의존	3.34	0.78
	지능 정보 격차	3.35	0.79
	불건전 정보	3.57*	0.88
	지능정보기술 과의존	3.37	0.78
평균		3.43	0.83
지능정보 신뢰성	인공지능 판단 신뢰성 및 윤리성 문제	3.39	0.80
	인공지능 학습의 편향성	3.34	0.77
평균		3.37	0.78
사회적 문제	대규모 실업 및 불안정한 고용 형태	3.25	0.75
	인간소외 및 정체성 문제	3.26	0.76
평균		3.25	0.75
전체 평균		3.48	0.82
군집 A(Centroid = 3.80)**	군집 B*(Centroid = 3.58)	군집 C(Centroid = 3.33)	

같이 분석하였다. 지능정보사회 사이버 역기능 5대 영역에서 전반적으로 사이버 범죄 및 테러와 권리 침해 영역이 효과적으로 개선될 것(μ = >3.5)으로 인식되고 있다. 국제 협력 조사의 원칙이 군집A(스팸, 지능형 악성코드, 피싱, 파밍, 스미싱, 해킹, 금융사기, 사이버 테러, 사이버 폭력)에서 가장 효과적일 것으로 인식되고 있으며 군집B(프라이버시 침해, 데이터 주권 침해, 인공지능 생산물에 대한 저작권 문제, 허위사실유포(가짜뉴스), 불건전 정보)에서도 효과적일 것으로 인식되고 있다.

하위 역기능에서는 피싱, 파밍, 스미싱(μ = 3.85, σ = 0.90), 해킹(μ = 3.83, σ = 0.95), 지능형 악성코드(μ = 3.82, σ = 0.92), 금융사기(μ = 3.80, σ = 0.91), 사이버 테러(μ = 3.80, σ = 0.91), 스팸(μ = 3.79, σ = 0.84), 사이버 폭력(μ = 3.73, σ = 0.90)이 본 원칙을 통한 역기능 개선 가능성을 높게 평가하고 있다. 또한 역기능 해소에 대한 인식이 다른 원칙들 보다 전반적으로 더욱 높게 나타난다. 특히 사이버 범죄 및 테러 영역의 평균값이 3.80 이상이고 하위 역기능들도 모두 높은 수치를 나타내고 있다.

해외에서 국내로 유입되는 사이버 테러가 더욱 증가하고 있지만 현존하는 국내법, 국제법으로 추적이 어려울 뿐만 아니라 이해관계에 얽혀 근본적인 역기능 원인을 해결하기 어려운 상황이다. 이러한 가운데 국가 간의 공조와 협약을 통한 사이버 테러 조사 및 테러 발생 국가에 대한 제재로 사이버 역기능을 해소하고자 하는 사회적 요구를 확인할 수 있다. 또한 타 원칙들 보다 역기능 해소의 기대치가 높은 만큼 적극적으로 해결해야하는 사회적 요구로 판단할 수 있다.

4.1.5 프라이버시 보호의 원칙

프라이버시 보호의 원칙 적용으로 역기능 해소에 대한 사회적 인식과 역기능별 영향력 군집을 <표 8>과 같이 분석하였다. 마찬가지로 지능정보사회 사이버 역기능 5대 영역에서 권리침해(μ = 3.59, σ = 0.95)와 사이버 범죄 및 테러(μ =

〈표 8〉 프라이버시 보호의 원칙의 적용으로 역기능 해소에 대한 사회적 인식

지능정보사회의 역기능		평균	표준편차
사이버 범죄 및 테러	스팸	3.57*	0.90
	지능형 악성코드	3.48*	0.94
	피싱, 파밍, 스미싱	3.53*	0.98
	해킹	3.50*	0.94
	금융사기	3.52*	0.97
	사이버 테러	3.52*	0.96
	사이버 폭력	3.53*	0.96
평균		3.52*	0.95
권리 침해	프라이버시 침해	**3.72****	1.02
	데이터 주권 침해	3.56*	0.95
	인공지능 생산물에 대한 저작권문제	3.49*	0.87
평균		3.59*	0.95
지능정보 이용 문화	허위사실유포(가짜뉴스)	3.51*	0.94
	스마트폰 과의존	3.27	0.76
	인터넷 과의존	3.26	0.73
	지능 정보 격차	3.28	0.72
	불건전 정보	3.41*	0.87
	지능정보기술 과의존	3.29	0.75
평균		3.34	0.80

〈표 8〉 프라이버시 보호의 원칙의 적용으로 역기능 해소에 대한 사회적 인식(계속)

지능정보사회의 역기능		평균	표준편차
지능정보 신뢰성	인공지능 판단 신뢰성 및 윤리성 문제	3.31	0.78
	인공지능 학습의 편향성	3.33	0.72
평균		3.32	0.75
사회적 문제	대규모 실업 및 불안정한 고용 형태	3.21	0.76
	인간소외 및 정체성 문제	3.24	0.78
평균		3.22	0.77
전체 평균		3.40	0.84
군집 A(Centroid = 3.72)**	군집 B*(Centroid = 3.51)	군집 C(Centroid = 3.27)	

3.52, σ = 0.95) 영역이 효과적으로 개선될 것이라고 인식하고 있고 하위 역기능에서는 프라이버시 침해(μ = 3.72, σ = 1.02)가 본 원칙을 통해 역기능 개선 가능성이 높다고 평가되었다. 그런데, 전반적으로 역기능 개선에 영향을 미친다는 결과가 나타났지만 영향요인이 비교적 큰 군집A와 보통인 군집B 모두 타 원칙과 비교했을 때 비교적 낮은 평균값을 나타내고 있어 사이버 역기능 전반을 포용할 수 있는 사회적 요구를 포함시키는 것이 필요할 것으로 사료된다.

4.2 성별과 연령에 따른 신뢰네트워크 도입으로 인한 지능정보사회의 사이버 역기능 해소 인식 차이

본 연구에서 제시한 가설인 성별에 다른 신뢰네트워크 도입으로 인한 지능정보사회 사이버 역기능 해소 인식 차이가 통계적으로 유의한지 확인하기 위해 독립표본 t-test를 실시하였다. <표 9>와 같이 성별에 따른 역기능 해소 인식차이를 검증하였으나 전 항목에 대해 유의수준이 $p > 0.05$로 나타나 차이를 확인할 수 없어 본 가설을 채택하였다.

또한, 본 연구에서 제시한 가설인 연령대에 다른 신뢰네트워크 도입으로 인한 지능정보사회 사이버 역기능 해소 인식 차이가 통계적으로 유의한지 확인하기 위해 ANOVA를 실시하였다. <표 10>과 같이 연령대에 따른 역기능 해소 인식차이를 검증하였으나 전 항목에 대해 유의수준이 $p > 0.05$로 나타나 차이를 확인할 수 없어 본 가설을 채택하였다.

〈표 9〉 성별에 따른 신뢰네트워크 도입으로 인한 지능정보사회의 사이버 역기능 심각성 해소 인식 차이

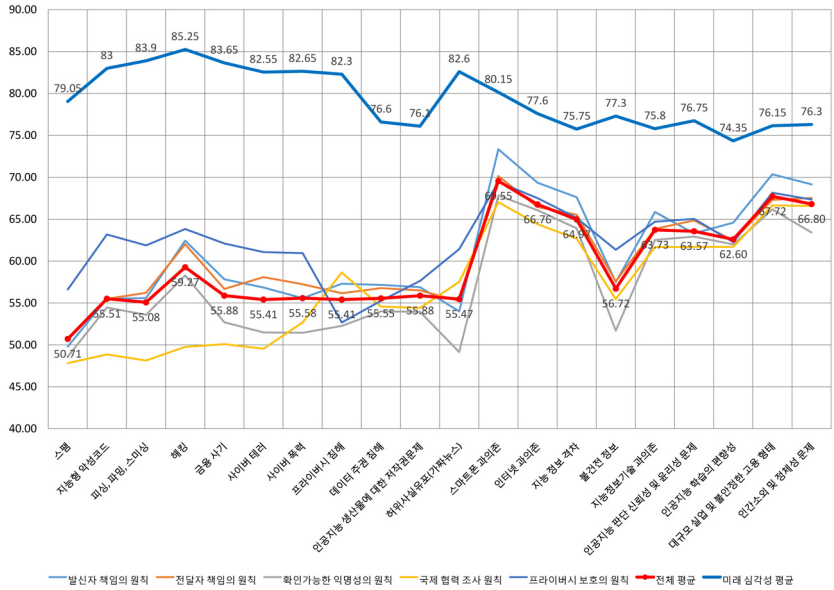
독립변수	성별	평균	표준편차	GAP	t	P
발신자 책임의 원칙	남	3.44	0.63	-0.024	-0.402	0.625
	여	3.46	0.59			
전달자 책임의 원칙	남	3.43	0.65	-0.070	-1.121	0.834
	여	3.50	0.59			
확인가능한 익명성의 원칙	남	3.52	0.65	-0.059	-0.933	0.439
	여	3.57	0.61			
국제협력조사의 원칙	남	3.51	0.57	-0.089	-1.504	0.217
	여	3.60	0.61			
프라이버시 보호의 원칙	남	3.37	0.63	-0.104	-1.637	0.581
	여	3.47	0.64			

〈표 10〉 연령에 따른 신뢰네트워크 도입으로 인한 지능정보사회의 사이버 역기능 심각성 해소 인식 차이

		제곱합	자유도	평균제곱	F	유의확률
발신자 책임의 원칙	집단-간	1.518	3	0.506	1.369	0.252
	집단-내	146.406	396	0.370		
	전체	147.924	399			
전달자 책임의 원칙	집단-간	0.950	3	0.317	0.817	0.485
	집단-내	153.615	396	0.388		
	전체	154.565	399			
확인가능한 익명성의 원칙	집단-간	1.015	3	0.338	0.845	0.470
	집단-내	158.500	396	0.400		
	전체	159.515	399			
국제협력조사의 원칙	집단-간	0.127	3	0.042	0.120	0.948
	집단-내	139.953	396	0.353		
	전체	140.080	399			
프라이버시 보호의 원칙	집단-간	0.657	3	0.219	0.538	0.656
	집단-내	161.023	396	0.407		
	전체	161.680	399			

4.3 신뢰네트워크 도입으로 인한 지능정보사회의 사이버 역기능 심각성 변화

본 연구에서는 설문조사를 통해 지능정보사회의 사이버 역기능 심각성의 사회적 인식과 신뢰네트워크 도입으로 인한 지능정보사회의 사이버 역기능 해소에 대한 인식을 확인하여 기술 도입으로 인한 인식 변화를 <그림 3>과 <표 11>과 같이 확인하였다.



〈그림 3〉 신뢰네트워크 도입으로 인한 지능정보사회의 심각성 변화

〈표 11〉 신뢰네트워크 도입으로 인한 심각성 감소율 및 순위

	기존 미래 심각성	신뢰네트워크 도입으로 인한 개선된 심각성	심각성 감소율	심각성 감소율 순위
스팸	79.05	50.71	0.36	1
지능형 악성코드	83.00	55.51	0.33	4
피싱, 파밍, 스미싱	83.90	55.08	0.34	2
해킹	85.25	59.27	0.30	9
금융사기	83.65	55.88	0.33	3
사이버 테러	82.55	55.41	0.33	5
사이버 폭력	82.65	55.58	0.33	7
프라이버시 침해	82.30	55.41	0.33	8
데이터 주권 침해	76.60	55.55	0.27	10
인공지능 생산물에 대한 저작권문제	76.10	55.88	0.27	12
허위사실유포(가짜뉴스)	82.60	55.47	0.33	6
스마트폰 과의존	80.15	69.55	0.13	18
인터넷 과의존	77.60	66.76	0.14	17
지능 정보 격차	75.75	64.97	0.14	16
불건전 정보	77.30	56.72	0.27	11
지능정보기술 과의존	75.80	63.73	0.16	14
인공지능 판단 신뢰성 및 윤리성 문제	76.75	63.57	0.17	13
인공지능 학습의 편향성	74.35	62.60	0.16	15
대규모 실업 및 불안정한 고용 형태	76.15	67.72	0.11	20
인간소외 및 정체성 문제	76.30	66.80	0.12	19
평균	79.39	59.61	0.25	

가장 심각성이 개선된 사이버 역기능은 스팸이었으며(36% 감소), 피싱, 파밍, 스미싱, 금융사기, 지능형 악성코드, 사이버 테러의 순으로 나타났다. 사이버 범죄 및 테러, 권리 침해, 지능정보이용문화의 허위사실유포, 불건전 정보의 역기능들에 대해 심각성이 감소 한 것을 확인할 수 있다. 하지만, 대규모 실업 및 불안정한 고용 형태, 인간소외 및 정체성 문제, 스마트폰 과의존, 인터넷 과의존 등의 역기능은 개선 효과가 비교적 적은 것으로 나타났다. 해당 역기능들은 주로 사회적, 문화적 문제를 포함하고 있어 네트워크의 기술적 개선 방안인 신뢰네트워크로 해결하는데 부족함이 있음을 확인할 수 있다. 다만, 신뢰네트워크 도입으로 인해 적은 폭의 감소를 확인할 수 있어 해당 역기능들에 대한 기술 외적인 문제를 보완한다면 큰 효과가 있을 것이다. Bright Internet과 같은 신뢰네트워크의 도입으로 전체적으로는 약 25% 정도의 심각성을 줄일 수 있을 것으로 추정된다.

Ⅴ. 결 론

본 연구에서는 지능정보사회의 사이버 역기능을 해소할 수 있는 신뢰네트워크 중 Bright Internet의 5대 원칙을 토대로 신뢰네트워크에 대한 사회적 인식과 요구를 확인하고 신뢰네트워크를 통한 사이버 역기능 해소의 인식을 분석하여 미래지능정보사회의 적절한 신뢰네트워크 구조와 실용적 기술도입 방향을 제시하였다.

신뢰네트워크 도입으로 지능정보사회의 역기능 해소에 대한 인식은 Bright Internet 5대 원칙에 대하여 설문조사를 통해 분석하였다. 지능정보사회의 사이버 역기능 5대 영역 중 사이버 범죄 및 테러, 권리 침해 영역이 역기능 개선에 영향이 큰 것을 확인할 수 있었고 지능정보 이용 문화 영역의 허위사실유포(가짜뉴스)와 불건전 정보의 역기능도 개선의 영향이 있음을 확인할 수 있었다. 하지만, 지능정보 이용 문화, 지능정보 신뢰성, 사회적 문제 영역의 역기능들은 개선 영향이 보통인 것으로 나타났고, 프라이버시 보호의 원칙 중 지능형 악성코드, 불건전 정보, 인공지능 생산물에 대한 저작권 문제의 역기능들도 개선 영향이 적은 것으로 나타났다.

세부적으로 발송자 책임의 원칙은 사이버 범죄 및 테러와 권리 침해 영역에 대해 기술적으로 역기능 해소가 가능하다고 인식하고 있다. 이는 수신자 책임 중심으로 전개되었던 역기능 방지를 발송자에게도 책임을 부여하여 역기능 개선의 새로운 패러다임을 제시하고 지능정보기술 이용자들이 기술 안정성에 대한 신뢰성도 높일 수 있음을 해석할 수 있다. 전달자 책임 원칙도 사이버 범죄 및 테러와 권리 침해 영역에 대해 역기능 해소가 가능할 것으로 인식하고 있다. 이를 통해 사이버 범죄에 대해 발송자에 대한 책임 부여 및 추적을 가장 중요시하여 정보 중개자인 전달자에 대한 책임이 작았던 문제에 대해 직접적 관여자인 전달자에 대해서도 책임 부여가 필요하다는 사회적 인식을 확인할 수 있다. 확인가능한 익명성의 원칙은 5대 원칙 중 사이버 범죄 및 테러와 권리 침해 영역뿐만 아니라 전체 역기능에 대해 개선 가능성이 가장 높게 평가되고 있다. 이는 인터넷 실명제 위헌 판결 후 익명성 보장과 인터넷 실명제 실시 사이의 논란이 지속되고 있는 가운데, 지능정보사회로 전개되는 현 시점에서 해당 역기능 해소 방안이 강력히 요구되고 있다는 것으로 해석할 수 있다. 국제 협력 조사 원칙은 사이버 범죄 및 테러와 권리 침해 영역에 대해 역기능 해소가 가능할 것으로 인식되고 있다. 이는 해외에서 국내로 유입되는 사이버 테러가 증가하고 있지만 현존 국내법과 국제법으로는 추적에 한계가 있어 역기능 원인을 해결하기 어려운 현 상황을 국가 간 공조와 협약을 통해 사이버 테러 조사를 시행하고 발생 국가에 대한 제재를 가함으로써 사이버 역기능을 해소하고자 하는 사회적 요구를 확인할 수 있었다. 특히, 타 원칙들보다 역기능 해소의 기대치가 높아 가장 우선적이고 적극적으로 해결해야하는 사회적 요구로 해석할 수 있다. 프라이버시 보호의 원칙은 권리 침해와 사이버 범죄 및 테러 영영에 대해 역기능 해소가 가능할 것으로 인식되고 있다. 전반적으로 역기능 개선에 영향을 있음을 확인할 수 있지만 타 원칙에 비해 낮은 평균값을 가져 사이버 역기능 전반을 포용할 수 있는 사회적 요구를 포함시키는 과정이 필요할 것이다.

또한 성별, 연령대별 신뢰네트워크 도입으로 인한 지능정보사회 사이버 역기능 해소 인식에 차이를 확인한 결과 성별, 연령별 차이 없이 모든 국민이 이러한 변화를 요구하고 있음을 확인 할 수 있었다.

신뢰네트워크 도입으로 인한 지능정보사회의 역기능 심각성 해소의 가능성은 전체 평균 25%정도의 변화를 가지고 올 수 있음을 예측할 수 있었다. 스팸, 피싱, 파밍, 스미싱, 금융사기, 지능형 악성코드, 사이버 테러의 순으로 심각성 감소율이 높았으며 사이버 범죄 및 테러, 권리침해, 지능정보이용문화의 허위사실 유포, 불건전 정보의 역기능들의 심각성이 감소한 것을 확인할 수 있었다. 하지만 사회적, 문화적 문제를 포함하고 있는 대규모 실업 및 불안정한 고용 형태, 인간소외 및 정체성 문제, 스마트폰 과의존 등의 역기능은 개선효과가 비교적 적어 네트워크 기술적 개선 방안인 신뢰네트워크의 보완점을 확인할 수 있었다.

본 연구 결과를 통해 신뢰네트워크인 Bright Internet이 사이버 범죄와 테러의 원인 제공자를 확인할 수 있는 체계를 갖춤으로 범죄의 원인을 근원적으로 억제하여 미래 지능정보사회에서 원

인자가 발생시킨 사이버 공격에 대한 해결책이 될 수 있다고 해석할 수 있다. 다만, Bright Internet이 사이버 공격 중 네트워크 개선점에 초점이 맞춰져 있어 사회적 문화적 문제를 포함하지 못하고 있으며 지능정보사회의 주된 이슈인 인공지능 관련 역기능에 대해서도 개선 영향이 적어 인공지능을 원인으로 발생하는 역기능과 사회적 변화를 포함하지 않고 있다는 것을 확인할 수 있다.

이에 미래 지능정보사회의 신뢰네트워크 구조 설계 시 기술적 문제 외에도 사회적, 문화적 문제도 함께 고려해야하며 지능정보기술의 역기능들로 인한 사이버 역기능과 사회 변화를 해소할 수 있는 통합적인 사이버 공간 관리 체계를 고안해야 할 것이다.

참 고 문 헌

[1] 관계부처 합동, *제4차 산업혁명에 대응한 지능정보사회 중장기 종합대책*", 관계부처 합동, 2016.

[2] 권정인, 이성철, 안성진, "사회현상학 관점에서의 인터넷역기능 분류체계 표준화 연구", *컴퓨터교육학회논문지*, 제14권, 제6호, 2011, 1-10.

[3] 김병운, "인공지능 동향분석과 국가차원 정책 제언", *정보화정책*, 제23권, 제1호, 2016, pp. 74-93.

[4] 김재호, 김권일, "지능정보사회에서의 규제", *한국토지공법연구*, 제79권, 2017, pp. 737-760.

[5] 백승익, 임규건, 여등승, "인공지능과 사회의 변화", *정보화정책*, 제23권, 제4호, 2016, pp. 3-23.

[6] 송봉규, "제4차 산업혁명기술과 범죄에 대한 탐색적 연구", *한국테러학회보*, 제12권, 제2호, 2019, pp. 73-98.

[7] 우매리, "인터넷의 역기능과 인터넷 윤리 활성화 방안", *신학과 목회*, 제43권, 2015, 297-318.

[8] 윤일한, 권순동, "정보보안 컴플라이언스와 위기대응이 정보보안 신뢰에 미치는 영향에 관한 연구", *Information Systems Review*, 제17권, 제1호, 2015, pp. 141-169.

[9] 이원태, 강장묵, "인공지능 기술/서비스 기반의 개인정보 보호 모델에 대한 연구", *한국인터넷방송통신학회논문지*, 제16권, 제4호, 2016, pp. 1-6.

[10] 이원태, 민희, "소셜미디어 시대 사회갈등의 재탐색", *21세기정치학회보*, 제25권, 제1호, 2015, pp. 265-284.

[11] 이윤배, "인터넷 역기능 예방을 위한 인터넷 윤리 교육 개선 방안", *한국정보통신학회논문지*, 제17권, 제6호, 2013, 1432-1440.

[12] 이진권, "위험기피도 및 성격속성의 남녀 간 성별 차이에 관한 실험 연구", *인문사회과학연구*, 제17권, 제1호, 2016, pp. 565-588.

[13] 이홍재, 박미경, 차용진, "4차 산업혁명 역기능 대응방안의 정책우선순위 분석", *한국공공관리학보*, 제32권, 제4호, 2018, pp. 27-50.

[14] 임규건, 류미나, 이정미, "개인정보유출 피해비용 산출 모델에 관한 연구", *정보보호학회논문지*, 제28권, 제1호, 2018, pp. 215-227.

[15] 임규건, 안재익, "지능정보사회의 사이버 역기능 분류와 사회적 인식 분석", *한국IT서비스학회지*, 제19권, 제1호, 2020, pp. 55-69.

[16] 임종인, *[포럼] 글로벌 사이버보안 규제 대비해야*, 디지털타임스, 2018.

[17] 전민서, 장항배, "ICT기반 보안개념 정의와 범위에 관한 설계연구", *Information Systems Review*, 제21권, 제3호, 2019, pp. 49-61.

[18] 전영은, 김정연, "금융회사의 사이버 보안 위협에 따른 개인정보보호 실태에 관한 연구", *한국IT서비스학회지*, 제13권, 제1호, 2014, pp. 79-89.

[19] 정부금, 이형규, 박혜숙, 박종대, "초연결 신뢰네트워크 기술", *전자통신동향분석*, 제32권, 제1호, 2017, pp. 35-45.

[20] 최성수, "남녀 성별에 따른 인지 행동적 차이에

관한 연구", *디지털디자인학연구*, 제15권, 제4호, 2015, pp. 307-318.

[21] 황종성, "지능사회의 패러다임 변화 전망과 정책적 함의", *정보화정책*, 제23호, 제2호, 2016, pp. 3-18.

[22] Cloud Security Alliance, *SDP Specification 1.0*, Cloud Security Alliance, 2014.

[23] 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, pp. 63-85.

[24] National Science and Technology Council Committee, *Preparing for the Future of Artificail Intelligence*, Executive Office of the President of United States, 2016a.

[25] National Science and Technology Council Committee, *The National Artificial Intelligence Research and Development Strategic Plan*, Executive Office of the President of United States, 2016b.

[26] Reed, M. G., P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing", *IEEE Journal on Selected Areas in Communications*, Vol.16, No.4, 1998, pp. 482-494.

[27] Shin, Y. Y., J. K. Lee, and M. C. 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, pp. 152-181.

Information Systems Review
Volume 22 Number 3
August 2020

Analysis on the Perception of the Cyber Dysfunction in the Intelligent Information Society According to the Introduction of the Bright Internet Trust Network

Gyoo Gun Lim* · Jae Ik Ahn**

Abstract

At present, our society is developing into the intelligent information society in the wave of the 4th industrial revolution, and this change will have the positive effect of innovating all industry fields. However, due to the duality of technology, there will be positive and negative effects. With intelligence, threats to cyber dysfunction such as hacking, terrorism, privacy infringement, and illegal content distribution will become more serious. Until now, the security system of the Internet has been a proactive security system, but in recent years, a proposal for a trust network, a preventive security system, has been introduced. Therefore, this study aims to analyze the possibility of resolving cyber dysfunction of intelligent information society about Bright Internet, one of trust network technologies. This study defines the cyber dysfunction of the intelligent information society and analyzes the perceptions of changes in the cyber dysfunction of the intelligent information society on the introduction of the five principles of the Bright Internet. The change of cyber dysfunction severity of the intelligent information society due to the introduction of the trust network is analyzed to reflect the technical and social demands. This work will guide the structure of the trust network and the direction of practical technological introduction and its influence.

Keywords: ***Intelligent Information Society, Cyber Dysfunction, Bright Internet, Trust Network, Artificial Intelligence***

* Professor, Professor, Business School, Hanyang University
** Corresponding Author, Master's Students, Business School, Hanyang University

◐ 저 자 소 개 ◑

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. 관심분야는 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 KORNET 상용화, 중국 Shanghai Telecom SI사업전략, 한국영화기술 로드맵, KTI 사업전략, 나라장터(G2B) 효과평가, 행정정보화(G4C) 성과분석, 국가정보보호지수개발, 국방정보화 수준평가모형, IT혁신인력양성종합대책, 국가디지털식별체계(UCI), 저작권정품 인증제도, SW사업자신고제도개선, SW기술자신고제도개선 등 다양한 IT혁신 분야의 프로젝트를 수행하였다.

안 재 익 (anssame@hanyang.ac.kr)

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

논문접수일 : 2020년 03월 12일 **게재확정일 : 2020년 04월 14일**
1차 수정일 : 2020년 04월 12일