Research Paper Informatization Policy Vol. 29, No.1 (2022), pp.024-037
https://doi.org/10.22693/NIAIP.2022.29.1.024

사이버 보안 강화를 위한 한국형 미래 인터넷 추진 방안에 관한 연구*

임 규 건** · 김 해 연*** · 안 재 익****

요 약

4차 산업혁명과 정보통신 기술의 발전 및 코로나 19로 ICT 환경이 급변하는 가운데 설계 초기에 보안성, 이동성, 관리성, QoS 등이 고려되지 않고 개발된 기존 인터넷은 기본 구조 위에 기능을 추가해야하는 한계성 때문에 인터넷 구조가 복잡해졌으며 보안성 취약, 안정성 취약, 신뢰성 취약 등의 문제가 지속적으로 발생하고 있다. 또한 인공지능, IoT 등 첨단 기술로 인한 디지털 트랜스포메이션 시점에 안정성과 신뢰성을 제공할 수 있는 새로운 개념의 인터넷이 요구되고 있는 실정이다. 이에 본 연구에서는 사이버 보안을 강화할 수 있는 한국형 미래 인터넷 구현 방안을 제시하기 위해 미래 인터넷 구현에 있어 중요한 핵심 요소를 분석하고 국내외 미래 인터넷 관련 연구 동향과 기술 적합성을 평가하여 한국의 사이버 환경에 적합한 미래 인터넷의 추진 방향 및 추진 전략을 도출하였다. 미래 인터넷 구현에 있어 핵심 요소의 중요도는 보안성, 무결성, 가용성, 안정성, 기밀성의 순으로 나타났다. 현재 미래 인터넷 프로젝트는 전 세계적으로 다양하게 연구되고 있는데 수많은 프로젝트 중 Bright Internet이 미래 인터넷 구현의 핵심 요소를 가장 적절히 만족하고 있으며 한국의 사이버 환경에 가장 적합한 기술로 평가되었다. Bright Internet을 한국형 미래 인터넷으로 추진하기 위해 기술적 이슈뿐만 아니라 전략적 이슈와 법률적 이슈도 같이 고려하여야 한다. 기술적 이슈로는 한국형 미래 인터넷의 표준으로 Bright Internet을 선정함에 있어 SAVA IPv6-NID 채택이 필요하고 데이터 센터 차원의 통합 데이터 관리와 국가 간 협력 체계 수립이 필요할 것이다. 전략적 이슈로는 안전한 관리 체계와 운영기관의 확립이 필요하고, 법률적 이슈로는 한국의 개정된 데이터 3법과 같은 국내법 준수를 포함한 GDPR(General Data Protection Regulation, 개인정보보호규정)의 요구 사항도 만족시켜야 한다.

주제어 : 미래 인터넷, 인터넷 보안, 한국사이버환경, 4차산업혁명, 밝은인터넷

A Study on the Korea Future Internet Promotion Plan for Cyber Security Enhancement*

Lim, Gyoo-Gun**·Jin, Hai-Yan***·Ahn, Jae-Ik****

Abstract

Amid rapid changes in the ICT environment attributed to the 4th Industrial Revolution, the development of information & communication technology, and COVID-19, the existing internet developed without considering security, mobility, manageability, QoS, etc. As a result, the structure of the internet has become complicated, and problems such as security, stability, and reliability vulnerabilities continue to occur. In addition, there is a demand for a new concept of the internet that can provide stability and reliability resulting from digital transformation-geared advanced technologies such as artificial intelligence and IoT. Therefore, in order to suggest a way of implementing the Korean future internet that can strengthen cybersecurity, this study suggests the direction and strategy for promoting the future internet that is suitable for the Korean cyber environment through analyzing important key factors in the implementation of the future internet and evaluating the trend and suitability of domestic & foreign research related to future internet. The importance of key factors in the implementation of the future internet proceeds in the order of security, integrity, availability, stability, and confidentiality. Currently, future internet projects are being studied in various ways around the world. Among numerous projects, Bright Internet most adequately satisfies the key elements of future internet implementation and was evaluated as the most suitable technology for Korea's cyber environment. Technical issues as well as strategic and legal issues must be considered in order to promote the Bright Internet as the frontrunner Korean future internet. As for technical issues, it is necessary to adopt SAVA IPv6-NID in selecting the Bright Internet as the standard of Korean future internet and integrated data management at the data center level, and then establish a cooperative system between different countries. As for strategic issues, a secure management system and establishment of institution are needed. Lastly, in the case of legal issues, the requirement of GDPR, which includes compliance with domestic laws such as Korea's revised Data 3 Act, must be fulfilled.

Keywords : future internet, internet security, south korea cyber environment, fourth Industrial revolution, bright internet

Received Jan 7, 2022; Revised Jan 14, 2022; Accepted Feb 17, 2022

* This work is prepared based on the contents of the 2020 Korea Internet & Security Agency Report (KISA2020-0334). The initial version was released in BIGS 2021.

** Professor, Business School, Hanyang University (gglim@hanyang.ac.kr)
*** Master's Degree, Business School, Hanyang University (jin1220@hanyang.ac.kr)
**** Ph.D Candidate, Business School, Hanyang University (anssane@hanyang.ac.kr), Corresponding Author

I. 서론

인터넷은 경제의 급속 성장뿐만 아니라 정치, 사회, 교육, 문화 등 다양한 방면에서 새로운 패러다임을 형성하였고 인터넷 공간은 IT 기술과 정보통신기술의 발전을 통하여 정보화시대를 넘어 지능정보사회로 진입하고 있다. 시간과 공간의 제약을 없애고 익명성과 비대면성이 보장된 사이버공간(Cyberspace)은 현실세계와는 또 다른 하나의 생활권을 형성하였다(Um & Kim, 2007). 그러나 현재 보안에 취약한 인터넷은 사이버 테러, 사이버 폭력, 사생활 침해, 개인정보 유출 그리고 다양한 고도화되고 지능화된 사이버 공격의 영향으로 인해 새로운 형태의 사이버 테러 및 범죄가 증가하고 있다(Lim, G. & Ahn, J., 2020a). 또한 국가뿐만 아니라 개인에 있어서도 전자상거래, 통신, 교통, 금융거래 등 일상생활에 직접적인 영향과 잠재적 피해에 노출되어 있는 상태이다.

코로나 19의 장기화로 인해 '사이버 팬데믹'으로 이어지고 있는 현재, 원격·비대면 환경이 증가하면서 온라인 활동이 급증하였고 사이버 공격자들의 접근이 쉬워졌다. 사회적 이슈를 이용한 피싱, 비대면 업무를 위한 커뮤니케이션으로 위장한 스피어피싱, 클라우드·IoT·분산근무로 내부 시스템의 외부 접점이 늘어나면서 확장된 공격표면, 쉽게 구할 수 있는 사용자·관리자 계정정보 등 '공격자 친화적' 환경이 조성되고 있다(Kim, 2021).

대표적 정보기술 중 하나인 사물인터넷(Internet of Things, IoT)은 수많은 데이터를 생성하고 초연결 사회를 구현할 수 있는 순기능을 보여주고 있지만 IoT의 증가 및 발전에 따라 발생할 수 있는 위협요소들도 급증하고 있다(Shin, 2017). 실제로 전 세계에서는 리눅스 달로즈 웜, Mozi봇넷 등 악성코드로 인해 보안 IP카메라, CCTV, 셋톱박스, 유무선공유기 등 사물인터넷 장비들이 감염된 사례가 보고되고 있다. 전문가들은 IoT 환경의 가속화 및 사용증가로 인한 사이버 공간에서의 보안 위협도 증가할 것이라고 주장하고 있다.

과학기술정보통신부에 따르면 2021년, 미국 최대 송유관 업체가 랜섬웨어 공격을 받아 시스템 마비로 인해 송유관 가동이 전면 중단되었고, 국내에서도 10위권 배달 대행 플랫폼 기업이 공격을 받아 전국 3만5천 곳의 점포와 만5천 명의 라이더 피해 발생 및 국내 자동차 부품 제조업 기업 침해사고 발생 등 랜섬웨어 침해사고가 집중적으로 발생하여 랜섬웨어를 최대 보안 위협으로 여기고 있다(Ministry of science and ICT, 2021).

인터넷을 통한 금융업무가 가능해지고 간편해지면서 간편결제, 인터넷 뱅킹 등 금융기관의 인터넷 서비스 사용률이 급증하는 반면, 악의적인 공격자에 의한 사고 사례도 지속적으로 발생하고 있기에 인터넷 서비스의 전반적인 구조를 분석하고 구조에 따른 보안위협 도출이 무엇보다 중요하다(Lee, et al., 2017).

전략국제문제연구소(CSIS)의 2020년 사이버 범죄의 간접적 비용 분석 보고서를 확인하여 보면 세계적으로 사이버 범죄에 인한 직접적인 피해액이 2018년에는 5,225억 달러(약 598조원)에 달하였고 2020년에는 9,450억 달러(약 1,030조원)에 달한다고 추산하였고 이러한 피해액은 지속적인 증가 추세를 보여주고 있다(Strategic International Research Institute, 2020). 여기에 사이버 보안에 지출한 비용 1,450억 달러(약 158조원)를 합치면 2020년에는 사이버 범죄에는 1조 달러 이상의 비용이 지출되고 있다고 추산하였다.

사이버 범죄는 공공의 안전을 해치고, 국가 보안에 피해를 주며, 경제를 파괴하는 비용을 발생시키는 것은 물론 기회의 상실과 자원 낭비, 사기 저하 등의 간접적 비용을 유발하기도 한다. 1,500개 기업에 대한 조사 결과, 4%만이 아무런 사이버 사고가 없었다고 응답하였으며 많은 경우 악성 프로그램과 스파이웨어의 피해를 입었다고 응답하였고, 생산성의 하락이나 근무 시간의 상실 등 비금전적인 피해 또한 막심했으며 최대 18시간의 근무 시간 상실로 평균 50만 달러(약 5억 4,500만원)의 피해를 입은 것으로 나타났다(Strategic International Research Institute, 2020). 막대한 비용이 발생하는 것에도 불구하고 다수의 조직은 사이버 리스크에 대한 이해 부족으로 보안 사고 감소에 대한 대응체계 및 계획이 미비한 실정이다(Lim, et al., 2018).

사이버 범죄가 사회기반 시설에 심각한 손상과 잠재적 피해를 초래하고 있고 4차 산업혁명으로 고도화되고 지능화된 기술사회에서는 점차 사이버 공격자를 색출하기 어려워지고 있어 인공지능, IoT 등 첨단 신기술로 인해 전반 산업이 디지털 전환을 추진하는 시점에 보안성과 신뢰성을 제공할 수 있는 차세대 인터넷이 요구되고 있다. 따라서 인터넷, 네트워크 연구 전문가들은 현존 인터넷 구조의 한계를 인식하고 장기적인 관점에서 기존의 인터넷을 다시 설계해야 하는 미래 인터넷에 대한 연구가 필요함에 동의하고 있다. 미래 인터넷이란 단순한 미래의 네트워크란 의미를 뛰어 넘어, 현재 인터넷 구조의 한계성을 극복하고 미래의 새로운 요구사항을 수용하기 위해, 기존과는 다른 혁신적인 개념(Clean-Slate)으로 설계/개발될 미래의 새로운 인터넷을 의미한다(Telecommunication Technology Association, 2009).

신뢰할 수 있고 안전한 미래 인터넷을 구현하기 위해 기존 인터넷의 구조적 문제점과 한계를 분석하고 선진국들의 사이버 보안 전략과 미래 인터넷 추진 전략에 대한 분석을 통해 차세대 인터넷에 대한 계획 수립이 필요한 시점이다. 또한 정보보안 트렌드와 선진국의 미래 인터넷 전략을 분석하여 한국 사이버 환경에 적합한 미래 인터넷의 구현방안 수립이 필요하다.

이에 본 연구에서는 사이버 보안을 강화할 수 있는 한국형 미래 인터넷의 구현 방안을 제시하기 위해 국내외 미래 인터넷 연구 동향을 분석하고 미래 인터넷 구현의 핵심 요소를 FGI 방법론을 통해 분석하며 대표적인 미래 인터넷 프로젝트의 한국 사이버 환경 적합성을 평가하여 한국 사이버 환경에 적합한 미래 인터넷의 추진 방향 및 추진 전략을 도출하고자 한다.

Ⅱ. 관련 연구

1. 미래 인터넷 연구 동향

세계 각국은 미래인터넷 표준화에 적극 대응하기 위해 국가별 자체적인 표준화 추진 단계를 수립하고 있으며 산학연 연계 컨소시엄을 구성하며 범국가적인 차원의 프로젝트 추진 포부를 밝히고 있다(Yoo, 2014). 주요 국가별 미래인터넷 추진 동향은 〈표 1〉과 같다.

미국은 2005년부터 국가과학재단(National Science Foundation, NSF)을 중심으로 미래인터넷 연구를 추진해오고 있으며 정부에서도 적극적인 정책적 지원을 실시하고 있다(Lee, 2020). 대표적인 연구 프로젝트로는 FIA(Future Internet Architecture), NDN(Named Data Networking), QIS(Quantum Information Science), XIA(eXpressive Internet Architecture) 등이 있다. 유럽연합(EU)는 유럽 위원회를 중심으로 정부의 주도하에

〈표 1〉 주요 국가별 미래 인터넷 추진 동향
〈Table 1〉 Future Internet Promotion Trends of Major Countries

Category	U.S.	EU	China	South Korea
Main institutions	NSF & FIA	NGI	Chinese government	Progressing individually
Proceeding method	Cooperation between government and private companies	Government-led	Government-led	Led by private companies
Main projects	NDN, MobilityFirst, XIA	Focused on NGI-affiliated project	NEW IP Projects	Bright Internet
Development goal	Network Flexibility & Security	Public interest (democracy) & security	Security	Security

미래 인터넷 기술 개발을 위해 연구를 진행하고 있다(Katja, 2020). EU의 대표적인 연구 프로젝트로는 NGI(Next Generation Internet) 및 산하 프로젝트들이 있다. 중국은 화웨이를 중심으로 정부 기관의 주도하에 사이버 테러 등의 문제를 예방할 수 있는 새로운 인터넷 구조체를 제안하는 'NEW IP' 프로젝트를 추진하고 있다. 한국은 2011년에 미래 인터넷 관련 5개년 추진 계획을 발표하였고 정부의 주도 하에 미래 인터넷 기술 개발을 도모하였으나 2015년 이후에는 정부 주도의 대규모 점진적/혁신적인 미래인터넷 추진 전략이 등장하지 않는 추세이며 현재는 개별 교육기관 및 기업 주도의 프로젝트만이 남아있는 상황이다. 한국의 대표적인 연구 프로젝트로는 OBelle(Atto Research), 쿨크라우드, Bright Internet(밝은 인터넷) 등이 있다(Lee, 2015; Lee, et al., 2018).

대부분의 미래인터넷 프로젝트들은 기존 인터넷 체계의 문제점에 집중하여 하나의 목적성(ex. 콘텐츠, 이동성, 보안)을 지닌 채로 프로젝트가 추진되고 있다. 현재 활발히 진행 중인 미래인터넷 후보 프로젝트들은 점점 더 늘어나는 데이터의 종류와 통신의 목적을 유연하게 관리하기 위해 패킷의 목적성을 밝히게 하거나 혹은 콘텐츠 중심의 네트워크 구조로 전환을 시도하고 있다. 또한 XIA, NEW IP를 포함한 거의 대부분의 프로젝트에서 보안성에 대한 강조가 재차 언급되고 있다.

2. 국내 사이버 위협 현황

급변하는 ICT 환경 변화 가운데, 사물과 공간, 사람 등이 인터넷으로 연결되어 정보를 생성 및 수집하고, 공유 및 활용하는 4차 산업혁명시대에 사이버위협은 나날이 증가되고 있는 추세이다. 사이버위협은 대체적으로 국가 및 개인정보를 탈취하는 정보유출, 금전적 이득을 위한 거래 및 금융사기, 시스템을 악의적으로 공격하여 마비시키는 서비스 중지 공격, 원격조정으로 장치를 파괴시키는 물리공격으로 분류할 수 있고 사이버위협의 증가는 내/외부 요인으로 나눌 수 있다(Korea Institute of Science and Technology Information, 2018). 스턱스넷, APT(advanced persistent threat), 키로깅, 크리덴셜 스터핑 등 사이버공격 자체의 고도화, 지능화는 사이버위협 증가의 내부요인이고, 성능이 낮은 센서, 내부 보안성, 쉬운 접근성 등 네트워크 자체의 보안 취약점 및 기존에 연결되지 않던 것들의 연결로 인한 보안 취약점이 사이버위협 증가의 외부요인이다(Seo, 2016).

SK인포섹 보안 시큐디움센터에서 공개한 통계 자료에 따르면 2020년 1월~ 5월 22일까지 하루 평균 20,375건의 사이버 공격이 탐지되었고 2019년 같은 기간에 비해 19%(3,238건) 증가로 폭발적인 사이버 공격의 증가를 확인할 수 있다. 코로나 19의 확산에 의해 비대면 및 재택근무가 증가하면서 사이버 공격으로 인한 외부에서의 접속 시도나 기술 및 정보 유출의 사례가 급증하고 있는 것으로 사이버 보안의 중요성이 나날이 높아지고 있다는 것을 알려준다.

3. 미래 사회의 사이버 위협

기기의 '초연결성', '지능화', '자동화'는 사람을 편리하게 해주고 빠른 정보처리가 가능하게 하는 순기능을 가지지만 기술의 양면성으로 순기능과 동시에 역기능이 존재하게 된다(Baek, et al., 2016). 사이버세계가 사물인터넷을 기반으로 이전과 비교할 수 없이 확장되어 사이버 공격의 피해가 더욱 커질 수밖에 없으며 블록체인 기반 암호화폐의 해킹사례, 빅데이터 기반 지능화 로봇 해커의 등장, 지능화된 사이버 공격 등은 미래 사회의 사이버 위협이 기하급수적으로 증가하고 사이버 보안이 불가능에 가까울 정도로 어려워 질 것으로 전망된다(Lim, 2018).

인터넷, 정보기술, 지능정보화와 관련된 '국가정보화 기본법', '지능정보사회 중장기 종합대책', '국가정보화 백서'의 법률 및 보고서를 분석하여 사이버 역기능 키워드를 1차적으로 추출하고 추출된 키워드의 분류 및 통합과정을 통하여 미래 지능정보사회에서 발생할 수 있는 사이버 역기능을 파악하였다. 국가정보화백서에서

〈표 2〉 대표적 미래 사이버 위협 유형
〈Table 2〉 Common Types of Cyber Threats in the Future

No.	Types of cyber threats	Details	References
1	Ransomware	Ransomware attacks targeting government agencies & medical facilities	Ministry of science & ICT
2	Infrastructure attacks	Intelligent attacks on infrastructures such as smart grids & banks	Mid-to-long-term comprehensive plan on intelligent information society
3	Personal information leakages	Stealing and leaking information from governments, companies, & individuals through cyberattacks, i.e. cloud hacking	Framework act on national informatization
4	Target attack using intelligent AI	Using artificial intelligence technology, cyberattacks target specific institutions	Mid-to-long-term comprehensive plan on intelligent information society
5	IoT device cyberattacks	Service paralysis occurs by hacking IoT devices such as self-driving cars & smart healthcare	National informatization white paper
6	Blockchain-based cryptocurrency	Blockchain-based crypto wallets & exchanges are hacked to steal cryptocurrency	National informatization white paper
7	Fake news	Unauthorized spread of false information such as fake news by exploiting technologies such as deepfake	National informatization white paper
8	Abuse of financial services	Unfair payment or leakage of financial/ personal information by exploiting financial services such as simple payments	Framework Act on National Informatization

추출한 사이버 위협 키워드는 IoT, 인공지능, 데이터 등 주요 기술들의 키워드였고 지능정보사회 중장기 종합대책에서는 사이버테러, 프라이버시, 사회적 변화 등 사회적 문제점들이 파악되었으며 국가정보화 기본법에서는 개인정보 침해, 정보격차, 불건전 정보 등 키워드가 추출하였다. 대표적 미래 사이버 위협 유형은 〈표 2〉와 같이 주요 시설 랜섬웨어, 사회기반시설 공격, 개인정보 유출, 지능화 AI 활용 타깃 공격, IoT 기기 공격, 블록체인 기반 암호화폐, 가짜뉴스, 금융 서비스 악용과 같은 8가지 유형으로 분류할 수 있다.

Ⅲ. 기존 인터넷 체계의 구조적 문제점

인터넷의 보급과 확산에 따라 새로운 패러다임의 사용자 요구를 충족하는데 있어 전송 품질, 보안성, 신속한 이동성 제공, 확장성 등 부분에서 기존 인터넷 체계의 한계성이 대두되고 있어 기존 인터넷의 연장이 아닌 새출발(Clean-Slate)하여 완전히 새로운 인터넷 아키텍처의 수립이 필요하다고 국제적으로 제기되고 있다(Lee, et al., 2009).

인터넷 개발 초기에는 보안성, 이동성, 관리성, QoS 등 부분이 고려되지 않아 사이버 환경에 새로운 요구사항들이 발생할 경우 필요에 따라 기능을 기존의 구조위에 추가하는 방식으로 진행되어 왔다. 이에 기본 구조위에 기능을 추가해야하는 한계성 때문에 인터넷의 구조는 더욱 복잡해졌으며 보안성 취약, 신뢰성 취약, 안정성 취약 등의 문제들이 지속적으로 발생하고 있다. 또한 인터넷 기술에 내재된 기술적 문제점인 주소 부족, 멀티-호밍, 혼잡 제어의 기술적 문제들도 점점 표출되고 있다(Kang, 2017).

기존 인터넷 체계는 다양한 유/무선 스마트 기기의 급속한 보급과 콘텐츠의 폭발적인 증가 등의 인터넷 이용 증가가 고려되지 않은 구조이기 때문에 네트워크 병목, 서비스 지연 등의 문제점이 지속적으로 발생하고 있으며 이러한 문제들을 해결하기 위해 물리적인 네트워크 설비를 확충하고 있지만 설비 확충이 투자대비 수익이 낮아 비용문제가 발생할 뿐만 아니라 급속도로 확대되는 네트워크 수요를 충족시킬 수 없다(Yeo, et al., 2007; Office of National Security, 2019). 특히 4차 산업혁명의 대표 기술인 사물인터넷의 발달은 네트워크 확산뿐만 아니라 규모 자체가 확장되는 구조이기 때문에 기존 사이버 공격에 대한 피해 범위뿐만 아니라 경제적, 사회적 문제도 걷잡을 수 없이 확대될 것으로 전망된다.

기존 인터넷의 구조적 문제점으로 다음과 같이 보안성, 안정성, 관리성, 이동성, 확장성을 제시할 수 있으며 미래인터넷 구현에 있어 반드시 보완되고 고려되어야 할 사항이라고 할 수 있다.

1. 보안성

기존 인터넷에서 가장 대두되는 문제점은 보안성이 취약하다는 점이다. 초창기 인터넷 사용자들은 서로 신뢰할만한 연구자들이었기 때문에 악성 해커에 대한 보안은 크게 고려되지 않았는데 인터넷은 누구든지 누구에게나 패킷을 보낼 수 있으며 악의적 유저가 본인의 패킷 주소를 변조하는 것도 막지 못하는 구조이기 때문에 악성 트래픽의 근원지조차 찾아내기 어려운 상황이다(Byun, 2009). 따라서 보안성을 강화하기 위해서는 인터넷 사용자의 행위에 대한 추적가능성과 확인가능성을 확보해야 하며 동시에 사용자의 익명성과 프라이버시를 존중할 수 있는 방안을 도입해야 할 필요가 있다.

2. 안정성

인터넷이 VoIP와 같이 전화와 방송까지 수용할 뿐만 아니라 산업 전반에 걸쳐 사용되고 있기에 안정성과 신뢰성은 반드시 보장되어야 하는데 기존 인터넷의 경우 체계상의 구조적 문제점들로 인하여 안정성을 추구하기에는 현실적 어려움이 많다. 특히 인터넷의 기능 대부분이 네트워크보다는 단말에 집중되어 있어 해킹당한 호스트에 의해 대량의 패킷이 생성되었을 때는 네트워크가 심각하게 영향을 받으며 마비될 수 있다. 따라서 안정성을 강화하기 위해서는 네트워크 아키텍처 설계부터 근본적으로 안정성과 신뢰성을 고려해야하며 이는 네트워크 관리능력과 보안성을 반드시 포함하고 있어야 할 필요가 있다.

3. 관리성

기존 인터넷의 경우 상당히 복잡한 구조 때문에 네트워크 분리, 라우팅 설정, 보안설정 등 숙련된 관리자의 직접 설정이 요구되는데 이에 네트워크 사고 대부분이 관리자의 잘못된 네트워크 설정으로부터 비롯되며 네트워크 서비스 중단까지 발생될 수 있다. 또한 네트워크 설정 외에도 네트워크에 문제가 발생했을 때 원인을 진단할 방법이 부족하며 단순히 관리자의 경험적 관점에서 문제를 해결하고 있다. 따라서 관리성 확보를 위해 네트워크 설정 및 관리의 자동화와 비교적 간결하게 네트워크 아키텍처가 설계될 필요가 있다.

4. 이동성

스마트폰과 사물인터넷의 급속한 보급으로 무선 네트워크의 사용도와 중요도가 확대되고 있는데 초기에 고려되지 않았던 무선 네트워크를 구성하기 위해 Mobile IP, Fast Handover 등의 기술을 도입하였으나 기존 인터넷의 근본적인 구조적 한계점, 무분별한 개방형 무선 네트워크 등 유선네트워크에 비해 보안성과 안정성이 매우 떨어지는 실정이다. 따라서 장치가 이동함에 따라 무선 통신 안정성이 확보되어야 하며 무선 장치 특성상 저전력, 저성능의 특징을 충분히 커버해야 할 필요가 있다.

5. 확장성

시대의 발전에 따라 다양한 단말이 출현하였고 단말의 수가 급증했을 뿐만 아니라 4차 산업혁명의 초연결성을 기반으로 하는 사물인터넷의 발달도 네트워크 전체의 복잡도가 커져가고 이전과는 비교할 수도 없을 정도로 구모가 확장되고 있기 때문에 네트워크의 확장성은 반드시 확보되어야 한다.

Ⅳ. 미래 인터넷 추진방향

1. 미래 사이버 위협 대응 솔루션

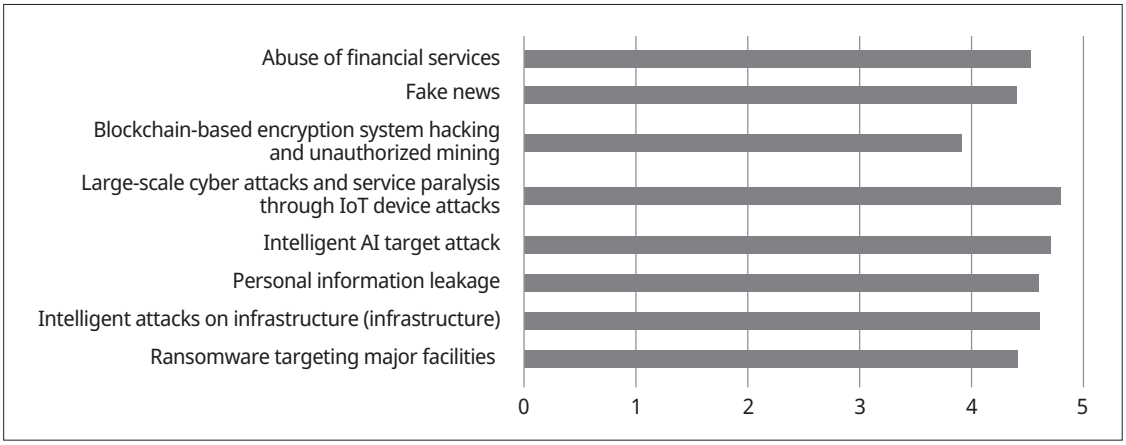
미래 사이버 위협에 대한 위험 전망을 살펴보기 위하여 선행연구를 통하여 제시한 미래 사이버 위협 8대 유형에 대해 정보 보호, 인터넷 전문가 16인의 의견을 전문가 워크숍과 설문조사를 통해 조사하였다. 2020년 12월 9일에 전문가 워크숍과 이후 한 달간 설문조사를 실시하였다. 자문위원단 및 전문가 구성원은 국내외 대학(중국청화대학교, 중국시안교통대학교, KAIST, 고려대, 한양대, 경희대) 교수, 국방부 정보화기획관, ETRI 책임급 연구원, 한국인터넷진흥원 (KISA) 팀장, Penta Security 상무, 한글과 컴퓨터 CTO 등을 전문가로 구성하였다.

전문가들의 의견을 조사한 결과 〈그림 1〉과 같이 전 유형에 있어 4점(위험)이상으로 나타났으며 특히 IoT, 지능화된 AI 활용한 타깃 공격에 대한 사이버 위협 위험도가 높게 나타났다.

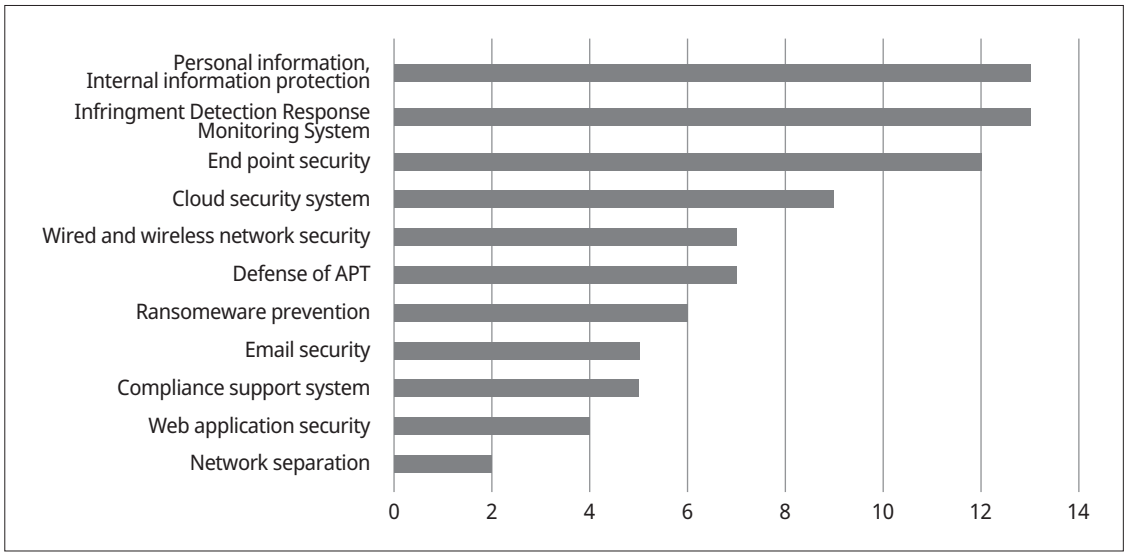
미래 사이버 위협의 대응 솔루션으로는 초연결 시대 네트워크 안정성 제공을 위한 인프라 보호 및 다양한 융·복합 서비스의 신뢰성 있는 제공을 위한 보안 기술, AI 활용 사이버 공격 대응 기술 개발 및 AI 신기술을 활용한 보안 기술 고도화, 사회 안전망 구축 등 방안들이 제기되고 있다. 미래 사이버 위협 대응 솔루션에 대한 전문가 의견을 조사한 결과 〈그림 2〉와 같이 개인정보 내부 정보 보호가 가장 중요한 것으로 나타났으며 침해 탐지 대응 모니터링 시스템, 엔드포인트 보안의 순으로 중요 솔루션으로 나타났다.

2. 미래 인터넷 구현의 핵심 요소

미래 인터넷은 기존 인터넷과 네트워크를 포괄하는 새로운 개념의 네트워크 구축이 필요하고 새로운 요구사항을 수용하는 서비스응용 및 구조화 등 새로운 인터넷 기



〈그림 1〉 미래 사이버 위협에 대한 위험도
〈Fig. 1〉 Risk of future cyber threats



〈그림 2〉 미래 사이버 위협 대응 솔루션 중요도(중복 선택)
〈Fig. 2〉 The Importance of Future Cyber Threat Solutions(multiple choice)

술 필요하다(Jeon, 2012). 이에 본 연구에서는 선행연구를 통해 선정한 인터넷의 5가지 핵심요소와 전문가들이 추가로 선정한 5가지 미래 인터넷 핵심 요소, 총 10가지를 FGI 방법론을 활용하여 중요도를 평가하였다. 평가방법은 미래 인터넷 구현의 핵심 요소 순위는 전문가들에게 미래 인터넷에 반드시 포함되어야할 정보보안의 요소들에 대해 순위를 정하게 하였고 1위 10점, 2위 8점, 3위 6점, 4위 4점, 5위 2점의 점수를 부여 후 산출하였다. 평가결과는 〈표 3〉과 같이 미래인터넷 구현에 있어 보안성이 가장 중요한 핵심 요소로 나타났고 이어서 무결성,

〈표 3〉 미래 인터넷 구현의 핵심 요소 순위
〈Table 3〉 Rankings of Key Elements of Future Internet Implementation

Rank No.	Key elements	Score
1	Security	122
2	Integrity	94
3	Availability	66
4	Stability	64
5	Confidentiality	64
6	Scalability	30
7	Manageability	16
8	User-centeredness	10
9	Trust chain	8
10	Mobility	6

가용성, 안정성의 순으로 나타났다. 이는 기존 인터넷에서 가장 큰 취약점으로 여겨지고 있는 보안성과 무결성에 대한 요구가 나타난 결과라 판단할 수 있다.

3. 미래 인터넷 구현의 방향성

미래 인터넷은 기존의 인터넷 기술과 환경을 발전적으로 보완·개선하거나 새로운 개념 및 구조 측면에서 완전히 새롭게 재설계하는 차원에서의 접근이 필요하다(Jeon, et al., 2012). 미래 인터넷 구현에 있어 가장 중요한 부분은 보안성과 무결성을 보장하는 안전한 신뢰 네트워크를 구성하는 것이다. 인터넷은 사회를 구성하는 필수적인 요소로써 사회 전반에 걸쳐 높은 보안성이 요구되는 영역으로 안전하게 활용하기 위하여 보안성을 갖추어야 할 것이다. 또한 다양한 응용 도메인의 서비스 요구사항을 만족시켜줄 수 있도록 구조적인 면에서 유연성 및 확장성을 갖추어야 할 것이다. 그 외 빅데이터 및 AI 기반의 운영의 자동화, 인터넷의 무결성, 관리의 편의성 등을 위한 관리성과 보안위협에 대한 사전예방적인 대응을 위한 국제적 협력 또한 고려되어야 할 것이다.

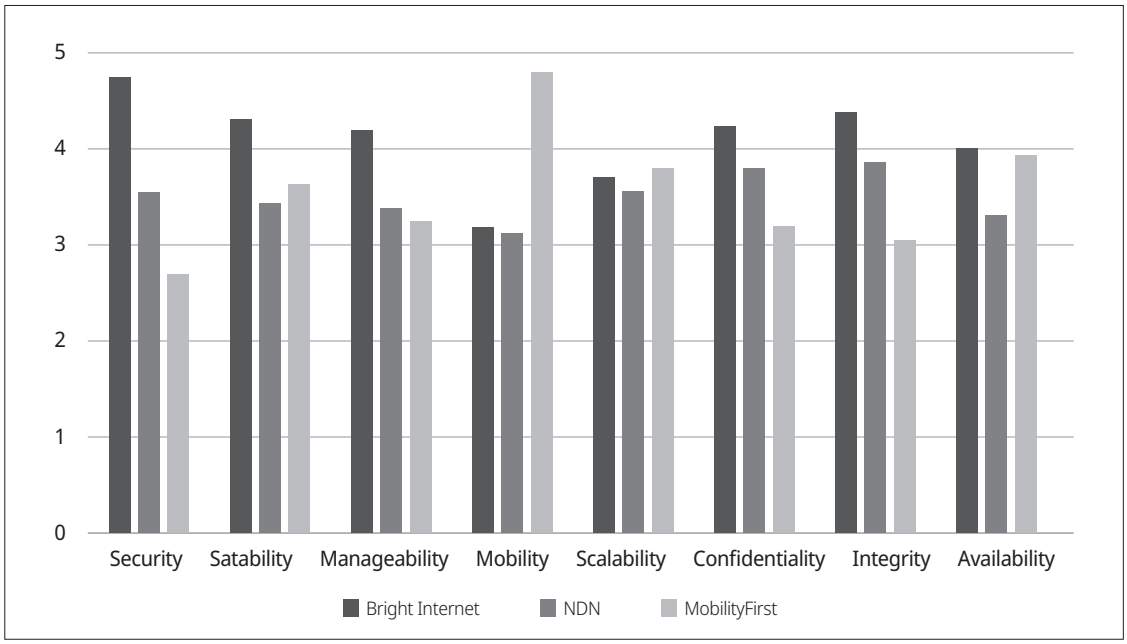
V. 한국형 미래 인터넷

1. 주요 미래 인터넷 기술별 적합성 비교

현재 활발히 연구되고 있는 대표 미래 인터넷 프로젝트(Bright Internet, NDN, MobilityFirst)를 한국 환경에 대한 적합 여부를 비교하고 FGI 방법론을 통해 적

〈표 4〉 대표 미래 인터넷 프로젝트 비교
〈Table 4〉 Comparison of Common Future Internet Projects

Category	Bright Internet	MobilityFirst	NDN
Network design method	IPv6 gradual design	ICN innovative design	ICN innovative design
Network compatibility	Compatibility guaranteed design	Does not guarantee compatibility based on ICN	Does not guarantee compatibility based on ICN
Transmission method	Packet based	Packet based	Packet based
Identifier	Addresses hosts	Addresses data (Flat Structure)	Addresses data (Hierarchical structure partially accepting flat structure)
Routing	Asymmetric routing	Hybrid ID-LOC routing / GSTAR	Symmetric routing
Caching	Supporting ordinary caching function	In-network caching	In-network caching
Forwarding	Stateless forwarding	Multi-hop forwarding	Multi-path forwarding
Security	Able to trace contribution principle of sender responsibility	Object security	Data-centric security
Mobility	Mobile IPv6	Mobility supported	Implicit mobility supported
Scalability	Supporting various ID systems, i.e. IPv4, IPv6	GUID	New ID
Adoption	Preceding new test bed establishment	Preceding new test bed establishment	Preceding new test bed establishment



〈그림 3〉 정보보안 요소별 미래 인터넷 평가
〈Fig. 3〉 Future Internet Evaluation by Key Element

합성을 평가하였다(Lim, et al., 2018; Zhang, et al., 2010). 전문가 16인의 설문은 60여 개의 설문 문항으로 이루어져 있고 5단계 척도를 사용하였다. 3가지 미래 인터넷 프로젝트가 정보보안 요소를 어느 정도 포함하고 있는 지 확인한 결과는 〈표 4〉, 〈그림 3〉과 같다.

정보보안 요소별 3가지 미래 인터넷 프로젝트를 비교 평가한 결과 Bright Internet 프로젝트는 다른 프로젝트보다 긍정적인 평가를 받았다. 그 중 보안성이 가장 뛰어나게 나타났고 안정성, 관리성, 기밀성, 무결성, 가용성 부분이 모두 4점 이상으로 높게 나타났다. 그러나 확장성과 이동성 부분이 비교적 부족한 모습을 보여주었다.

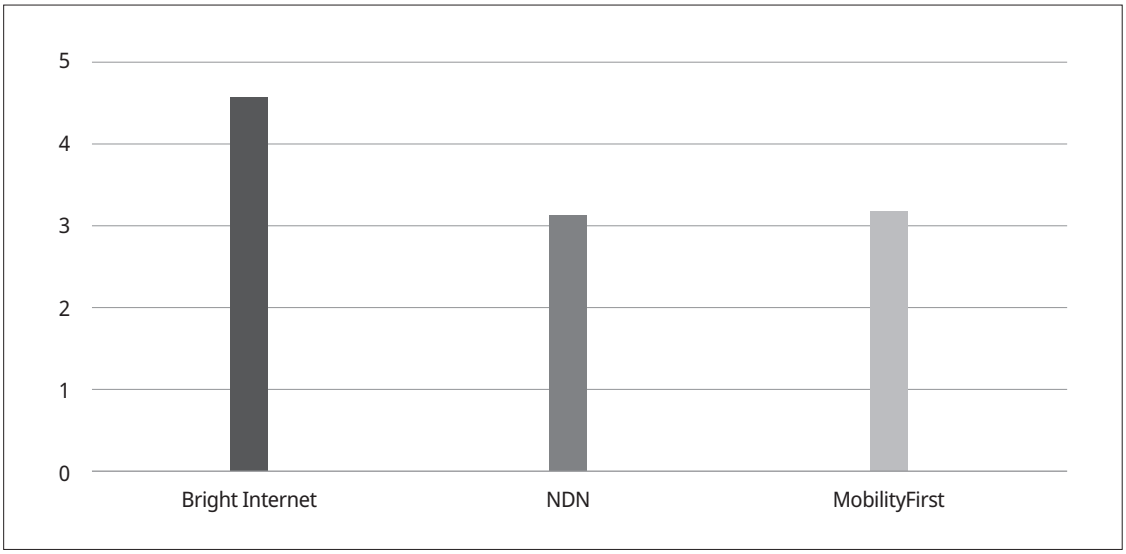
NDN 프로젝트는 여러 정보보안 요소별로 보았을 때 모두 3점 전후로 중간 정도의 수준을 포함하고 있다. 그 중에서 이동성과 가용성 방면이 다소 부족한 모습을 보여주었다.

MobilityFirst 프로젝트는 무선통신장치에 초점을 둔 프로젝트로 이동성 방면이 4.81점으로 매우 뛰어나지만 기타 요소는 모두 3점 전후로 약한 편인데 그 중에서 보안성이 2.69점으로 가장 취약하게 나타났다.

2. 한국 사이버 환경에서의 미래 인터넷 적합성 평가

3가지 미래 인터넷 프로젝트가 한국 사이버 환경에서의 적합성 평가 결과는 다음의 〈그림 4〉와 같다.

Bright Internet 프로젝트가 4.56점으로 한국의 사이버 환경에 가장 적절하다는 것을 확인할 수 있다. Bright Internet 프로젝트는 책임 소재에 대한 부분, 차세대 인터넷 환경에 적합한 다양화된 보안 정책을 제안하는 등 기존 인터넷 체계에 있어서의 근본적 한계점들을 보완하는 방향으로 접근하며, 미래 인터넷의 적용에 필수적인 기술, 법제도적 개편 등 요소를 포함하고 있다. 또한 국내 인터넷 환경이 5G/6G등의 차세대 이동통신 및 엣지 컴퓨팅, 고도화된 유선통신 인프라 구축이 병행해서 진행되며, 새로운 기술들이



〈그림 4〉 한국 사이버 환경에서의 적합성 평가
〈Fig. 4〉 Evaluation of Suitability in the Korean Cyber Environment

동시에 접목되면서 기존 인터넷 환경이 진화하고 있기에 Bright Internet이 한국의 사이버 환경에 가장 적합하다고 판단된다.

NDN과 MobilityFirst 프로젝트는 모두 3점 전후로 나타났는데 해당 프로젝트들은 TCP/IPv6를 대체하는 IP관리방식으로 특정 구조가 필요하고 글로버 규모의 식별자 기반 라우팅, 포워딩, 매핑 기술 문제, 자가인증 식별자 이용 인증 및 신뢰 도메인 구성 기술 문제, 빠른 패킷 포워딩 메커니즘, 콘텐츠 및 프라이버시 보호 관련 문제 등 해결하여야 할 이슈가 존재하기에 한국의 사이버 환경에서 프로젝트를 설계하고 추진하기에 제한적일 수 있다.

3. 한국형 미래 인터넷 추진 방향

본 연구에서는 한국의 사이버 환경에서 Bright Internet 프로젝트를 설계하고 추진하기 가장 적합하다는 의견을 확인할 수 있는데 Bright Internet을 한국의 미래 인터넷으로 추진하려면 고려하여야 할 사항들이 존재한다. 첫번째 고려사항은 바로 Bright Internet의 기술적 이슈이다. 텔레그램과 같은 익명성이 보장되는 소프트웨어와 사용자의 데이터를 제공하는 것을 거부할 수 있는 해외 서비스에서 사이버 범죄자의 신원확보를 위해 레이어 하단의 SAVA IPv6 - NID 채택이 필요하고, 개별 Bright Internet Data Center(BIDC) 차원의 통합 데이터 관리와 국가별 BIDC 간의 협력 체계가 필요할 것이다. 또한 사후적/방어적(Reactive) 형태를 이루는 기존의 인터넷 보안체계는 추후 예방적 형태로 바꾸고 사이버 위협의 원인을 근본적으로 제거할 수 있는 신뢰 네트워크가 필요할 것이다. 다음으로 고려해야 할 사항은 Bright Internet 구현의 전략적 이슈이다. 익명성의 훼손으로 인한 개인정보 노출, “빅브라더” 등 이슈에 대한 우려를 잠식시킬 수 있는 안전한 관리체계와 기관의 확립이 선행 되어야 한다. 또한 정책 및 보안에 대한 공조체계의 수립이 필요하고 미래 사이버 위협에 대응하기 위한 Task Force, 실시간적 협조 및 대응체계의 수립이 필요하며 지능정보기술의 역기능들로 인한 영향과 사회 변화를 포함시킬 수 있는 통합적인 사이버 공

간 관리체계의 고안이 필요하다. 마지막으로 고려해야 할 사항은 Bright Internet의 법률적 이슈이다. 한국에서의 미래 인터넷을 추진하고 나아가 국제 표준 기준을 달성하기 위해서는 EU의 GDPR과 한국의 개정된 데이터 3법의 요구사항을 만족시켜야 할 것이다. Bright Internet 확인가능한 익명성 프로토콜의 경우 원인지 식별 시 개인정보에 대한 이용 및 처리 부분이 GDPR 규제에서 벗어날 수 없기에 사전에 보완해야 한다. 또한 Bright Internet Data Center의 운영 방면에서 운영 방안 및 정책 수립에 있어 개인정보보호 이슈를 해소하기 위해 GDPR의 요구사항을 만족시켜야 한다.

4. 한국형 미래 인터넷 추진 전략

한국의 사이버 환경에 적합한 Bright Internet을 추진하기 위해서는 우선 기존 인터넷과 구분되는 완전히 새로운 인터넷 아키텍처에 대한 고안을 통해 보안측면에서 완전한 무결성을 지닌 혹은 다양한 보안 단계를 구현/서비스할 수 있는 인터넷 구조의 설계가 필요하다.

이어서 인터넷은 한 국가가 독점하는 형태의 인프라가 아닌 세계적인 합의와 표준이 필요하기 때문에 한국 단독의 추진 보다 중국, 미국 등 인터넷 생태계에 큰 영향력을 갖고 있는 국제사회와 긴밀히 협력하여 사이버 역기능을 해소를 위한 장기적 관점의 국제적 연구개발 교류를 진행하고 신기술 공동기획, 민관협동 등 기술협력을 추진하여 표준화를 선도해야 한다. 이 과정 중에 국가 간 협력이 불가피하지만 미래 인터넷 상용화 및 기술 표준화 경쟁에 대비하여 주요 중점기술에 대한 한국 주도의 상용화 계획 및 표준화 대응전략 수립이 필요하며, 미래 인터넷 인프라 구축 및 서비스응용모델 발굴을 위해 대단위 테스트 베드를 구축하고 원천기술의 사전 연구개발 추진해야 한다.

특히 Bright Internet은 신뢰네트워크로써 사이버 위협의 원인 제공자를 파악하여 사이버 공격을 사전에 해결할 수 있는 해결책이 될 수 있지만, 인터넷 특성상 사회적 문제, 인공지능을 통한 지능화 등의 문제를 근본적으로 해결할 수 없다. 즉, 지능정보기술의 발전과 사회 변화에 따른 역기능을 포괄적으로 해결할 수 있는 정책 혹은 제도가 뒷받침 될 수 있도록 관련 연구 및 체계를 함께 고민해야할 것이다.

Ⅵ. 결론

4차 산업혁명과 코로나 사태로 인한 비대면이 일상화 되는 시점에서 개발 초기에 보안성, 관리성, 이동성, QoS 등 부분을 고려하지 않고 설계한 기존 인터넷은 신뢰성, 확장성 등 다양한 부분이 부족한 체계상의 문제점들을 지니고 있으므로 신뢰기반의 미래 인터넷 개발 및 추진이 무엇보다 시급한 상황이다. 특히 보다 다양해지고 고도화된 미래 사이버 위협들이 발생 및 증가하고 있기에 미래 인터넷 구현에 적극적으로 나서야 할 시점이다.

이에 본 연구에서는 미래 인터넷에 대한 연구 동향을 분석하고 미래 인터넷 구현에 있어 중요한 구성 요소를 확인하고 평가하며 이에 따라 연구되고 있는 미래 인터넷 기술, 프로젝트의 적합성을 평가하여 한국 사이버 환경에 적합한 미래 인터넷 기술과 추진 방향 및 추진 전략을 제시하였다.

미래 인터넷 구현의 핵심요소의 중요도는 보안성, 무결성, 가용성, 안정성, 기밀성, 확장성 순서로 나타났고 미래 인터넷의 구현에 있어 이러한 요소들을 보장하는 신뢰 네트워크의 구현이 필요할 것 이다. 핵심요소들을 만족 시킬 수 있는 미래 인터넷 기술로는 Bright Internet이 한국형 사이버 환경에 가장 적합한 미래 인터넷 프로젝트로 선정되었다. Bright Internet이 NDN, MobilityFirst 프로젝트보다 보안성, 가용성 등 부분에서 신뢰 네트워크로서의 적합도가 타 프로젝트에 비해 상대적으로 높게 평가되었다. Bright Internet 프로젝트는 개선전략의 일환으로 완전히 새로운 인터넷 설치가 아닌, 현재의 인터넷을 개선하는 개념이어서 수용성이 상대적으로 높게 평가되었다.

한국 사이버 환경에서의 미래 인터넷 Bright Internet

프로젝트 추진에 있어, SAVA IPv6 - NID 채택이 필요하고, BIDC 차원의 통합데이터 관리와 국가별 BIDC 간의 협력체계가 필요할 것으로 예상된다. 그리고 기술적 이슈뿐만 아니라 국경이 존재하지 않는 인터넷의 특성도 고려하여 사이버 범죄자의 추적, 검거 및 인도를 위해 긴밀한 국제적 공조가 필수적이다. 특히, 인터넷은 국제 협력을 통한 원인지에서의 원인제거가 가능한 협력 체계 수립이 필수 불가결한 사항이기에 보안 모니터링, 효과적 관리체계 분배 및 국제적 공조체계 수립을 위해 정부 및 민간의 전략적 협조가 반드시 동반되어야 할 것이다.

■ References

Baek, S., Lim, G. & Yu, D. (2016). "Exploring Social Impact of AI." *Informatization Policy, 23*(4), 3-23.

{백승익·임규건·여등승 (2016). 인공지능과 사회의 변화. 〈정보화정책〉, 23권 4호, 3-23.}

Byun, S. (2009). "Future Internet Architecture Research Trend." *Electronic and Telecommunication Trend, 24*(3), 1-12.

{변성혁 (2009). 미래인터넷 아키텍처 연구동향. 〈전자통신동향분석〉, 24권 3호, 1-12.}

Jeon, E., Lee, D., Lee, S., Seo, D. & Kim, J. (2012). "Analyzing Future Internet Security Research Trends: Focusing on FIA." *Information Security Paper, 12*(1), 79-87.

{전은아·이도건·이상우·서동일·김점구 (2012). 미래 인터넷 보안 연구 동향 분석 : FIA를 중심으로. 〈정보보안논문지〉, 12권 1호, 79-87.}

Jeon, S. (2012). "Direction of R&D on Understanding and Focusing Technologies of the Future Internet." *Korean Information Processing Society, 19*(3), 101-109.

{전승수 (2012). 미래인터넷의 이해와 중점기술에 대한 연구개발 방향. 〈한국정보처리학회〉, 19권 3호, 101-109.}

Kang, H. (2017). *Is the current Internet structure evolving into the future*. Telecommunications Technology Association.

{강현국 (2017). 〈현재의 인터넷 구조가 미래로 진화하고 있는가〉. 한국정보통신기술협회.}

Katja B. (2020). *A vision for the future Internet*. NGI.

Kim, S. (2021). "2021 Cyber Threat Trend Analysis and Response Technology." *DATANET*, December 6.

{김선애 (2021). 2021 사이버 위협 동향 분석과 대응 기술. 〈DATANET〉. 12월 6일.}

Korea Institute of Science and Technology Information (2018). *Analyzing the latest cyber threat trends and countermeasures*. Korea Institute of Science and Technology Information.

{한국과학기술정보연구원 (2018). 〈최신 사이버위협 동향 및 대응 방안 분석〉. 한국과학기술정보연구원.}

Lee, E. (2020). "The U. S. Government's Trends in Quantum Information Communication and Security Policy." *Korea Internet & Security Agency, 4*(7), 1-15.

{이응용 (2020). 미국 정부의 양자정보통신 및 보안 정책 추진 동향. 〈한국 인터넷진흥원〉, 4권 7호, 1-15.}

Lee, H., Lee, W., Kim, S., Shin, Y. & Park, H. (2009). "A Study on the Characteristics and Development of Korean Internet Culture." *Korea Information Society Development Institute*, 1-125.

{이호영·이원태·김사혁·신유림·박현유 (2009), "한국 인터넷 문화의 특성과 발전방안 연구", 〈정보통신정책연구원〉, 1-125.}

Lee, J. (2015). "Research framework for AIS grand vision of the bright ICT initiative." *MIS quarterly, 39*(2), iii-xii.

Lee, J. (2016). "Invited commentary—reflections on ICT-enabled bright society research." *Information Systems Research, 27*(1), 1-5.

Lee, J., Cho, D., & Lim, G. (2018). "Design and validation of the bright internet." *Journal of the Association for Information Systems, 19*(2), 3, 63-85.

Lee, K., Lee, S. & Yim, K. (2017). "Analysis and Classification of Security Threats based on the Internet Banking Service." *Informatization Policy, 24*(2) 20-42.

{이경률·이선영·임강빈 (2017). 인터넷 뱅킹 서비스에서의 보안 위협 분류 및 분석. 〈정보화정책〉, 24권 2호, 20-42.}

Lim, G. & Ahn, J. (2020a). "A Study on the Classification of Cyber Dysfunction and the Social Cognition Analysis in the Intelligent Information Society."

Journal of Information Technology Services, 19(1), 55-69.

{임규건·안재익 (2020a). 지능정보사회의 사이버 역기능 분류와 사회적 인식 분석. 〈한국IT서비스학회〉, 19권 1호, 55-69.}

Lim, G. & Ahn, J. (2020b). "Analyzing the Perception of Cyber dysfunction in the Intelligent Information Society by the introduction of Bright Internet Trust Network." *Information Systems Review, 22*(3), 99-118.

{임규건·안재익 (2020b). Bright Internet 신뢰네트워크 도입에 따른 지능정보사회의 사이버 역기능 해소에 대한 인식 분석. 〈Information Systems Review〉, 22권 3호, 99-118.}

Lim, G., Liu, M. & Lee, J. (2018). "A Study on the Damage Cost Estimation Model for Personal Information Leakage in Korea." *Journal of The Korea Institute of Information Security & Cryptology, 28*(1), 215-227.

{임규건·류미나·이정미 (2018). 개인정보유출 피해 산출 모델에 관한 연구. 〈정보보호학회논문지〉, 28권 2호, 215-227.}

Lim, H., Ni, A., Kim, D., Ko, Y. B., Shannigrahi, S. & Papadopoulos, C. (2018). "NDN construction for big science: Lessons learned from establishing a testbed." *IEEE Network, 32*(6), 124-136.

Lim, J. (2018). [Forum] "Preparing for global cyber security regulations." *Digital Times*, February 13.

{임종인 (2018). [포럼] "글로벌 사이버보안 규제 대비해야." 〈디지털타임스〉, 2월 13일.}

Ministry of science and ICT (2021). *Organize and operate Ransomware Response Support Team.* Ministry of science and ICT.

{과학기술정보통신부 (2021). 〈'랜섬웨어 대응 지원반' 구성·운영〉. 과학기술정보통신부.}

Office of National Security (2019). *National Cyber Security Strategy*. Office of National Security.

{국가안보실 (2019). 〈국가 사이버안보 전략〉. 국가안보실.}

Seo, B. (2016). *4th Industrial Revolution and Cyber Security Measures*. NIA Future planning center.

{서병조(2016). 〈4차 산업혁명과 사이버 보안대책〉. 한국정보화진흥원 정책본부 미래전략센터.}

Shin, Y. (2018). "A Study on Developing Policy Indicators of Personal Information Protection for Expanding Secure Internet of Things Service." *Informatization Policy, 25*(3), 29-51.

{신영진 (2018), 안전한 사물인터넷 서비스 확산을 위한 개인정보보호정책평가지표 개발에 관한 연구. 〈정보화정책〉, 25권 2호, 29-51.}

SK Infosec (2020). *EQST security issue in the first half of 2020*. SK Infosec.

{SK인포섹 (2020). 〈EQST 2020년 상반기 보안 이슈〉. SK인포섹.}

Strategic International Research Institute (2020). *Indirect Cost Analysis of Cybercrime.* Strategic International Research Institute.

{전략국제문제연구소 (2020). 〈사이버 범죄의 간접적 비용 분석〉. 전략국제문제연구소.}

Telecommunication Technology Association (2009). *Future Internet*. Telecommunication Technology Association.

{한국정보통신기술협회 (2009). 〈미래인터넷〉. 한국정보통신기술협회.}

Um, M. & Kim, M. (2007). "An Exploratory Study on Factors affecting Efforts for Information Protection in Cyber Space." *Informatization Policy, 14*(1) 125-143.

{엄명용·김미량 (2007). 사이버공간에서 정보보호 예방활동에 영향을 미치는 요인에 관한 탐색적 연구. 〈정보화정책〉, 14권 1호, 125-143.}

Yeo, H. , Um, K. & Cho, S. (2007). "QoS-based multimedia service provision plan and performance evaluation in a portable Internet environment." *Journal of Advanced Navigation Technology, 11*(3), 306-312.

{여현·엄기복·조성언 (2007). 휴대 인터넷 환경에서 QoS 기반 멀티미디어 서비스 제공 방안 및 성능 평가. 〈한국항행학회〉, 11권 3호, 306-312.}

Yoo, J. (2014). *Global Future Internet Promotion Trend*. Korea Internet & Security Agency.

{유재필 (2014). 〈전 세계 미래인터넷 추진 동향〉. 한국인터넷진흥원.}

Zhang, L., Jacobson, V., Zhang, B. & Tsudik, G. (2010). *Named Data Networking (NDN) Project.* Named Data Networking.