KISA REPORT

2019 VOL.12

한국인터넷진흥원

KISA REPORT

CONTENTS

ISSUE

디지털 사회의 신뢰 제고를 위한 논의

01 **신뢰를 위한 인공지능 거버넌스가 왜 필요한가?**
[한상기/ 테크프론티어 대표]

02 **사회적 신뢰를 위한 새로운 ID 프레임워크의 필요성**
[최필식 / 기술작가]

03 **사회변화를 이끄는 '행동하는 인터넷정책'으로의 패러다임 전환**
[이원태 / 정보통신정책연구원 연구위원]

04 **기술, 사람을 돌아보다**
[최호섭 / 디지털 칼럼니스트]

05 **데이터 신뢰를 위한 합의 알고리즘**
[유성민/ IT 칼럼니스트]

TREND

01 **디지털패권 경쟁 속의 화웨이: 유럽과 아시아 국가들의 공조와 일탈**
[유인태 / 전북대학교 국제인문사회학부 조교수]

02 **주요국 사이버 공급망 위협관리 정책 동향 및 시사점**
[김소선 / 고려대학교 정보보호대학원 책임연구원]

03 **개인정보보호법 개정 후, 데이터 3법의 남은 과제**
[이창범 / 연세대학교 법무대학원 겸임교수]

신뢰를 위한 인공지능 거버넌스가 왜 필요한가?

한상기 (stevehan@techfrontier.kr)

테크프론티어 대표

인공지능 기술의 발전이 빠르게 진행되고 다양한 산업 분야와 사회 문제 해결에 사용되면서 인공지능의 역작용이나 사회 전반에 끼치는 영향, 기술만이 아니라 정치 경제 윤리적 관점에서의 논의가 지난 1~2년 사이에 매우 활발해지고 있다.

2020년에는 이런 논의 결과가 구체적으로 어떻게 모습을 만들어 낼 수 있는가에 관한 연구와 정책 방향 및 법제도 측면에서의 토의와 합의 과정이 국가 안에서 또는 국제적인 기관이나 조직을 통해서 이루어질 것이다.

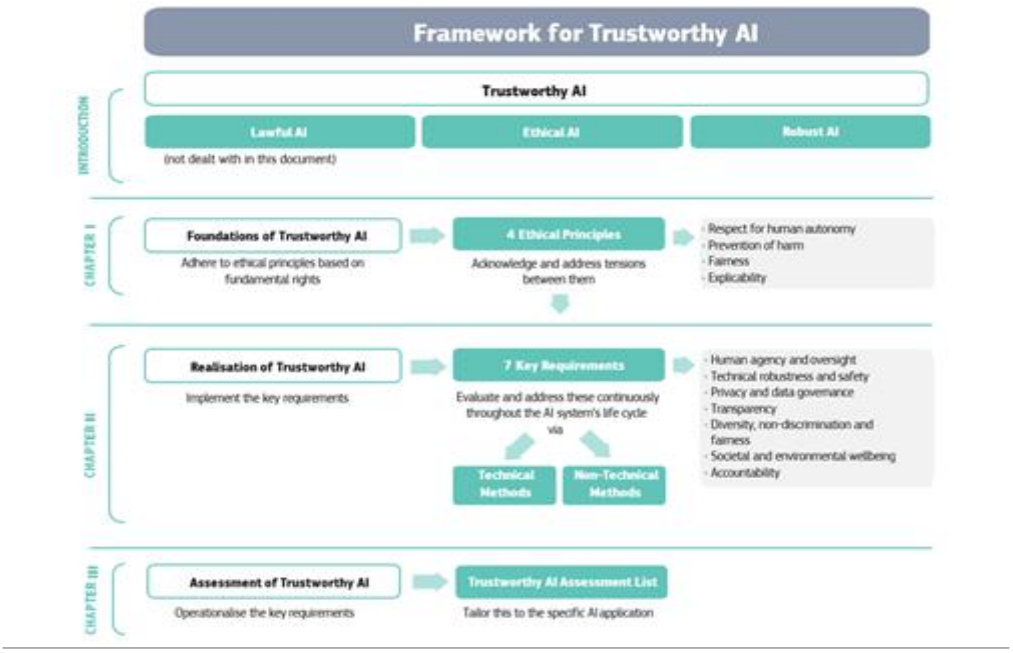
인공지능 기술 적용 결과가 공정하지 않은 문제, 예를 들어, 성별과 인종, 사회 집단에 대해 편향을 갖는 문제, 견고하고 안전하지 않은 문제, 설명 가능이나 투명성이 결여되어 있는 문제, 인간 가치 시스템에 부합하게 만들 수 있는가에 대한 질문 등 많은 잠재적 문제점과 해결해야 하는 이슈들이 제기되었다.

이제는 이런 문제를 모두 종합해 하나의 통합된 프레임워크로 이런 문제에 대해 대처하고, 인류가 어떻게 첨단 인공지능 시스템에 의해 변화하는 최적의 방법을 찾을 것인가 하는 문제를 '인공지능 거버넌스'라는 주제로 파악해야 한다.

지난 2017년에 생명의 연구소 주관으로 아실로마에서 '유익한 인공지능' 논의 결과 23개의 원칙을 선언한 이후, 2019년에는 인공지능이 사회에 엄청난 변환을 가져올 것이라는 판단에 단지 위험을 완화하는 것을 넘어 인류에게 최고의 미래를 만들어 낼 수 있게 인공 일반 지능 (AGI)을 어떻게 디자인할 것인가를 모색하기로 했다.

2018년 8월에는 옥스포드 대학의 인류 미래 연구소에서 '인공지능 거버넌스: 연구 어젠다' 보고서를 발행해서 기술, 정책, 이상적인 거버넌스에 대해 주요 이슈를 제시했다. 유럽 집행위는 인공지능 고급 전문가 그룹을 구성해서 신뢰성 있는 인공지능의 세 가지 구성 요소를 기반으로 이를 성취하게 할 수 있는 프레임워크를 제시했다. 이 프레임워크는 지금까지 나온 다양한 이슈를 신뢰성 있는 인공지능이라는 하나의 거대 담론 아래 모아서 기반과 구현, 평가를 위한 작업을 의미 있게 정리했다.

유럽 집행위가 제시하는 신뢰성 있는 인공지능을 위한 프레임워크



2019년에는 OECD 역시 인공지능 원칙을 만들어 일반 원칙과 정책 권고 사항을 제시했다.일반 원칙에는 포용성과 지속 가능성, 인간 가치와 공정성, 투명성과 설명 가능성, 견고성과 안전성, 책임성 주제가 있으며 이 원칙들이 인공지능 거버넌스를 생각할 때 가장 핵심이 되는 이슈들이다.[1)]

이런 움직임에서 대학, 연구 기관, 재단들의 움직임도 다양하게 이루어지고 있는데 최근 가장 눈에 띄는 조직이 'AI NOW 연구소'이다. 이 연구소는 포드 재단과 맥아더 재단이 지원한 연구소로 케이트 크로포드 교수와 메레디스 휘트테이커 교수가 공동 설립자로 활동하며, 뉴욕 대학이 운영하고 있다. 이 연구소는 인공지능이 어떻게 개발되고 사용되어야 하는가에 대한 국제 토론을 이끌고 있으며, 주요 연구 주제는 크게 권리와 자유, 노동과 자동화, 편향과 포용, 안전과 중요한 인프라로 구분하고 있다.

AI NOW는 2019년 12월에 연간 보고서를 발행했는데, 여기에는 해로운 인공지능에 대한 점증하는 반격, 2019년에 새롭게 등장한 긴급한 우려들 두 가지의 큰 주제로 현재 인공지능 산업에서 사회가 풀어내야 하는 이슈를 정리하고 있다.

이런 문제를 단지 기술이 아닌 21세기 인문학 연구로 풀어야 한다는 신념으로 세계적 사모펀드 운영회사인 블랙스톤 창업자인 슈워츠만은 MIT와 옥스포드에 각각 3억 5천만 달러와 1억 5천만 파운드를 기증해 새로운 연구 그룹을 만들기도 했다. MIT에는 컴퓨팅 칼리지를 세우고, 옥스포드 대학에는 인문학 센터를 만들었다. 인문학 센터 안에는 세계 최고 수준의 철학자와 인문학자들과 아카데미, 기업, 정부의 인공지능 사용자 및 기술 개발자들이 인공지능의 윤리와 거버넌스를 연구하도록 했다.[2)]

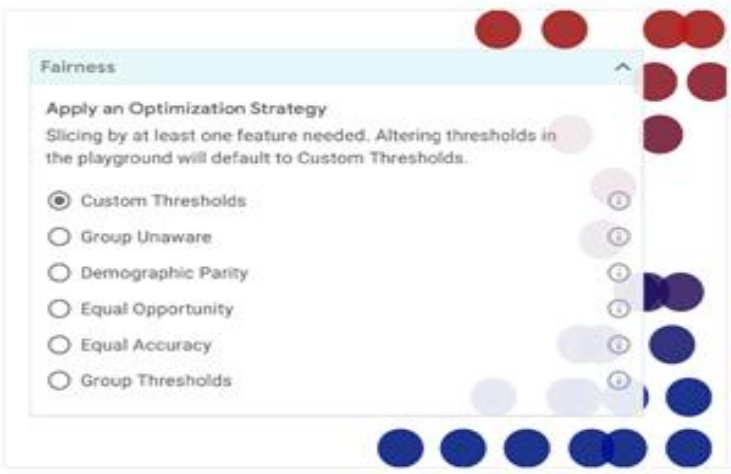
신뢰성을 위한 기업의 움직임

기업들의 움직임도 매우 빠르게 진행되고 있으며, 앞에서 말한 인공지능의 사회적 이슈나 원칙에 대응하기 위해 새로운 기술과 도구를 발표하고 있다. 구글이 수행하는 연구 프로그램 중 하나는 '페어(PAIR)'라는 프로그램으로 'People+AI Research'의 약자이다. 이는 인간 중심의 연구와 디자인으로 인공지능 파트너십이 생산적이고, 즐거우며 공정하게 되도록 하는 노력이다.[3)]

이 프로그램을 통해 구글이 2018년 9월에 소개한 것이 '왓이프 (What-If) 도구 (WIT)'이다. 텐서보드 웹 애플리케이션의 새로운 기능으로 사용자가 추가 코드 작성 없이 머신 러닝 모델을 분석할 수 있게 한다. 즉, 텐서플로우 모델과 데이터셋에 포인터를 주면 왓이프 도구는 모델의 결과를 탐색할 수 있는 비주얼 인터페이스를 인터랙티브하게 제공한다.

1) http://www.oecd.org/going-digital/ai/
2) https://www.schwarzmancentre.ox.ac.uk/Page/ethicsinai
3) https://ai.google/research/teams/brain/pair

WIT에서 5 가지 유형의 공정성에 맞춰 데이터를 정렬해 보는 기능



마이크로소프트는 ICML 2018년에 발표한 논문에 기반을 둔 방식으로 일반적인 분류기를 다양한 공정성 정의에 따라 공정한 분류기로 변화시키는 증명 가능하고 실용적인 확실한 방안을 제시한다.[4] 이 도구를 'fairlearn'이라는 이름으로 깃허브에 공개하고 있다.

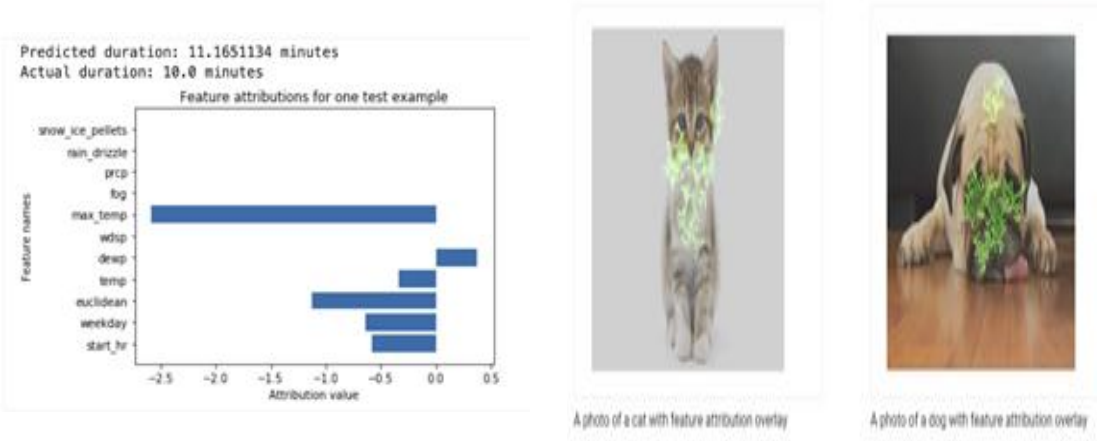
페이스북은 2018년 F8 컨퍼런스에서 머신 러닝 알고리듬이 편향되어 있는지를 결정하는 내부 프로젝트인 페어니스 플로우를 개발 중이라고 발표했으나,[5] 내부용으로 사용하는 중이다. IBM은 'AI 공정성 360 (AIF 360) 툴킷을 제시하고 있는데, 이는 알고리듬에 의한 원하지 않은 편향을 찾고, 이해하고, 완화하기 위한 확장 가능한 툴킷이다.[6]

설명과 해석을 위한 접근도 여러 방향으로 이루어지고 있다. 마이크로소프트가 인공지능의 '블랙박스' 문제를 해결하기 위한 시도로 내 놓은 오픈 소스 소프트웨어 툴킷인 인터프리트ML은 인공지능 시스템의 결과를 설명하기 위해 개발자가 여러 방법으로 실험할 수 있게 돕도록 한다.[7]

구글은 2019년 11월 런던에서 열린 '구글 넥스트' 이벤트에서 또 다른 방식의 설명 가능 인공지능 기능을 선 보였다. 아직 베타인 '설명 가능 인공지능(Explainable AI)'은 해석 가능하고 포용적인 머신 러닝 모델을 도입하기 위한 도구와 프레임워크이다.[8]

4) Agarwal, A., et. al., "A Reduction Approach to Fair Classification," arXiv, Jul 16, 2018
5) Quartz, "Facebook says it has a tool to detect bias in its artificial intelligence," May 4, 2018
6) R. Bellamy, et. Al., "AI Fairness 360: An Extensible Toolkit for Detecting, Understanding, and Mitigating Unwanted Algorithmic Bias," arXiv, Oct 3, 2018
7) Venture Beat, "Microsoft open-sources InterpretML for explaining black box AI," May 10, 2019
8) ZDNet, "Google's new AI tool could help decode the mysterious algorithms that decide everything," Nov 21, 2019

구글의 설명 가능 인공지능 주요 기능



IBM의 설명가능성 360 툴킷은 파이썬으로 작성한 확장 가능한 오픈 소스 툴킷으로 머신 러닝 모델이 인공지능 애플리케이션 전 생애 주기 동안 어떻게 레이블을 예견하는지를 다양한 수단을 통해서 이해하도록 한다.

그러나 이런 도구는 아직 개발자를 위한 설명과 해석이지 일반 사용자를 대상으로 하는 기능이 아니다. 모델을 이해하고 데이터를 조정하는 일을 지원하는 것이기 때문에 본격적인 설명 가능성에 대한 연구는 좀 더 설명 생성과 심리학적인 연구를 통한 접근이 필요한 상황이다.

우리의 방향

최근 정부가 발표한 인공지능 국가 전략을 보면 이런 이슈에 대해 파편적인 접근을 하고 있다. 인공지능과 조화 공존이라는 주제 하에 일자리 문제와 역기능 방지, 윤리 이슈를 제시했으며, 법제도 정비를 내세웠다. 그러나 이런 문제는 지난 2-3년을 지나면서 보다 통합적 시각으로 발전했으며, 명확한 주제들이 제시되었다.

따라서 이제는 신뢰할 수 있는 인공지능을 위한 거버넌스 차원에서 검토가 필요하며, 이에 대한 기술 개발과 정책 수립, 그리고 지원 체계와 감독 기관 지정 등의 문제가 필요하다.
또한, 이런 주제는 한 국가에서만 만들어 갈 수 없기 때문에, 국제적 협조와 공조가 필요하며, 연구 집단/정책 기관/시민 단체/정부 각 계층별로 국제 협력이 이루어져야 하며 동시에 이들을 엮어 내는 노력이 필요하다

또한, 민간 기업 간의 상호 협력을 위한 공동 연구 기관의 설립과 협력 연구 프로젝트를 구성해 공동 노력하는 자세가 필요하다. 우리가 앞으로 다루어야 할 문제는 하나의 기업이 대응하기에는 너무나 크고 너무나 중요한 과제들이기 때문이다.

사회적 신뢰를 위한 새로운 ID 프레임워크의 필요성

최필식 (choi4u@gmail.com)

기술작가
IT 블로그 'chitsol.com' 및 테크G(www.techg.kr) 운영자

대부분의 사람들은 물리적 공간에서 일상적인 삶을 사는 한편으로 디지털 세상과 공존하고 있다. 인간의 기본 욕구를 충족하기 위해 활동하는 물리적 세상만큼이나 여러 유형의 네트워크로 연결된 디지털 세상에서 실제 세계에 버금가는 많은 일을 할 만큼 밀접하게 연결된 것이다. 오히려 물리적인 이동이나 행동 없이 디지털 세계의 활동만으로 일을 끝낼 때도 있다.

그런데 5G 같은 더 빠른 네트워크와 수많은 데이터를 처리할 강력한 컴퓨팅 환경을 갖춰 나갈수록 물리적 공간과 디지털 세계의 경계가 희미해질 것으로 예상함에 따라 이용자를 증명하는 본인 확인에 대한 패러다임의 변화가 필요한 시점이다. 기존 서비스 사업자마다 이용자 본인 확인에 필요한 ID를 위해

수많은 개인정보를 받으면서 발생한 수많은 폐해에서 벗어나 민감한 개인정보의 유출 없이 온라인에서 쓸 수 있는 새로운 ID 프레임워크는 단순한 선언이나 법률적인 체계만으로 완성되는 것이 아닌 공동체가 함께 고민해야 할 과제다.

ID로 확인하던 이용 자격

소수의 전문가와 연구소, 대학교 등 일부 영역을 제외하고 일반 이용자들이 지금처럼 온라인에서 ID/비밀번호라는 단순 계정 체계가 대중화된 시점은 아마도 PC 통신이 시작된 이후일 것이다. PC에 설치한 모뎀에 전화선을 꽂고 다이얼 업 기반 PC 통신이나 전자 게시판(BBS) 등 접속해 자료실이나 동호회, 채팅 같은 데이터 기반 통신 서비스를 이용할 때 ID와 비밀번호를 입력하는 절차를 거치면서 그 방식에 익숙해지기 시작했으니 말이다.

하지만 PC 통신 시절의 ID와 비밀번호 체계는 자격을 확인하는 데 편한 방식이었을 뿐이다. 엄밀히 따지면 ID 이용자와 소유자가 같다고 말할 수 없고, 본인을 확인하는 수단이라고 보기도 어려웠다. 서비스에 접속하거나 이용하기 위한 가입 여부 및 필요한 자격을 확인하는 용도로는 충분했을지 몰라도 처음부터 이용자 본인을 확인하기 위한 목적을 충족하기 위한 개념과 체계는 잡혀 있지 않았기 때문이다.

ID에 대한 느슨한 개념으로 인해 서비스를 쓸 수 있는 자격을 가진 ID를 다른 사람과 공유하거나 빌려주는 장면을 보는 것은 어렵지 않았다. 또한 온라인의 개인정보 보호라는 개념이 강하지 않던 때라 생일이나 전화번호 같은 개인정보를 기반으로 ID를 만들기도 했고, 허위 정보를 기반으로 ID를 생성할 수 있었을 뿐만 아니라 다른 사람의 ID를 악용하거나 그럴 수 있는 위험성이 매우 높았다.

물론 당시 서비스의 한계로 ID를 본인 인증 목적으로 활용할 가치가 컸다고 보긴 어렵다. 다만 PC 통신을 벗어나 인터넷 시대로 변화를 겪으면서 ID의 쓰임새가 늘어나면서 ID가 가진 함의가 드러나게 된다.

ID와 소유자의 동일성 확인

초고속 네트워크가 집집마다 깔리면서 접어든 인터넷 시대에도 기존 ID 체계는 유지된다. 인터넷 서비스를 쓰기 위한 자격을 확인하기 위한 목적으로 ID와 비밀번호 체계는 그대로 이어진 것이다. 하지만 다양한 인터넷 서비스 증가는 단지 서비스를 이용할 수 있는 자격만 부여하는 것이 아니라 ID의 실제 이용자를 확인해야 할 필요성이 더욱 커졌다. 금융, 쇼핑, 게임, 메일, 카페 등 ID를 기반으로 접속한 사용자와 본인이 아닐 경우 타인의 명의도용이나 부정 사용 등 여러 문제를 야기할 가능성이 컸기 때문이다.

이러한 상황에서 서비스 사업자들은 인터넷을 통해 이용자들을 직접 확인할 수 없는 비대면 가입을 받을

때 어떻게 이용자의 자격을 확인할 수 있는지 방법을 찾아야 했다. 지금처럼 본인 확인 시스템이 개발되지 않은 상태에서 이용자를 확인할 공인된 정보가 필요했던 서비스 업체들은 이용자의 주민등록번호를 활용했다. 주민등록번호는 이용자의 생년월일과 성별, 출생지 등 개인정보가 들어 있는 민감 정보였으나, 객관적으로 이용자를 확인할 방법이 없다는 이유로 이 정보를 입력받아 저장한다. 이 외에도 ID의 소유자와 관련된 갖가지 개인정보를 원활한 서비스에 필요하다는 이유로 수집하는 곳도 적지 않았다.

하지만 ID 생성을 위해 서비스마다 입력받은 주민등록번호 같은 개인정보들은 형편없이 취급되고 관리된 결과 큰 후유증을 낳는다. 이용자 본인 확인이나 성인 인증, 중복 가입 방지 같은 목적으로 제공된 주민등록번호와 개인정보들이 대량으로 판매되거나 오픈 마켓, 정유사, 통신사에 보관 중인 개인정보들이 해킹 등으로 유출되는 사고가 끊이지 않았다. 암호화되지 않은 개인정보들이 유출되고 오프라인에서 명의도용에 악용되는 등 수많은 피해 사례가 등장하면서 이에 대한 대책을 요구하는 목소리가 커졌고 정부는 개인정보 보호에 관한 법률 제정을 통해 이를 관리하기 시작했다.

늘어난 본인 인증 수단과 남은 문제

2004년 입법논의가 시작된 개인정보보호법이 2011년 3월 29일 공포되고 6개월 뒤인 2011년 9월 30일부터 시행된다. 그리고 2012년 2월 18일 이후 온라인상 주민등록번호 수집이 금지된다. 개인정보보호법에 따라 개인정보를 수집 이용하는 경우 정보주체의 동의나 법령에 근거 규정이 경우만 가능하고 회원 탈퇴 때 지체 없이 파기토록 장치가 마련된 것이다. 개인정보보호 관리체계 인증 등 기업들의 개인정보 보호 인식 제고를 위한 교육과 제도를 만들어 나가는 등 개인정보보호에 대한 인식을 바꾸는 노력도 병행된다.

이처럼 개인정보보호법은 표면적으로 더 이상 주민등록번호 같은 민감한 개인정보를 서비스 사업자가 저장하지 못하도록 제약을 두는 데 의의가 있지만, 그렇다고 완전히 차단된 것은 아니다. 개인정보보호법 이후 서비스를 이용할 때 주민등록번호 같은 개인정보의 수집을 차단했어도 서비스 이용에 필요한 ID를 생성하려는 사람이 이용자 본인인지 아닌지를 확인하는 본인 확인 서비스는 예외로 뒀기 때문이다. 비록 가입하려는 인터넷 서비스는 이용자의 본인 여부만 한번 확인하면 그만이라 해도 이용자 본인을 확인할 수 있는 개인정보는 다른 인증 서비스에서 관리되는 것이다.

지금 공식적인 본인 인증 수단으로 쓸 수 있도록 허용된 것은 공인인증서나 아이핀, 휴대전화에 이어 최근 신용카드 등이다. 이러한 본인 인증 기관들은 이용자의 개인정보를 기반으로 인증 요청을 받으면 별도로 발급한 인증서에 비밀번호를 입력하거나 신용카드 정보, 휴대 전화로 받은 문자나 앱 인증을 통해 서비스에 본인 여부를 통보한다.

이처럼 본인 인증 수단은 늘어났지만 몇 가지 문제도 여전히 남아 있다. 인터넷 서비스마다 본인 인증

수단을 취사선택할 수 있는 터라 이용자는 특정한 서비스를 쓰기 위해 허용된 본인 인증기관에 개인정보를 넣어둬야 한다. 또한 중앙화 된 기관을 통한 본인 인증만 통과하면 서비스 이용에 문제가 없고 인터넷 서비스 사업자의 보안 사고가 발생할 때도 절차적 문제가 없고 사용자 피해를 입증하지 못한 경우 책임을 면하는 근거가 되기도 했다.

모바일이 바꾼 ID 패러다임

인터넷 서비스를 쓰기 위해 본인 인증을 거쳐 생성된 ID가 한 명의 이용자 또는 그 이용자가 관리하는 하더라도, ID는 온라인에서 이용자의 대신하는 용도 이상은 아니었다. 앱을 중심으로 다양한 서비스를 이용하는 초기 모바일 시대도 이러한 의미는 변하지 않았다.

하지만 모바일 시대는 ID의 새로운 면이 부각된다. 기존 인터넷 서비스는 이용자가 ID로 로그인한 뒤 서비스를 닫으면 로그아웃 되면서 서비스를 종료한 반면, 모바일은 서비스를 쓰지 않는 상태에서도 이용자가 계속 서비스를 쓰고 있는 것처럼 작동했다. 즉, 기존의 ID는 오프라인 이용자가 필요한 때만 활용했던 반면, 모바일에서 ID는 자동 로그인 등 훨씬 적극적인 방식으로 작동하면서 능동적으로 사용자 데이터를 수집해 클라우드나 서버로 전송한 것이다.

스마트폰이나 웨어러블 장치처럼 다양한 센서를 갖춘 장치들을 통해 수집한 데이터는 이용자의 위치를 포함해 센서로 감지된 운동 데이터와 심박수 같은 신체 데이터 등 민감한 데이터를 포함하고 있었다. 이용자의 동의 없이 민감한 개인정보들이 서비스 개선 및 마케팅에 활용되는 용도로 쓰였고, 이러한 정보를 서버에 저장하고 관리와 취급에 대한 안내도 빈약했다.

이용자 동의 없는 개인정보 수집과 활용이 늘어나자 더욱 강력한 개인정보 보호에 대한 요구가 높아졌다. EU를 비롯한 각국 정부는 모든 개인정보에 대해서 보호받을 권리를 주목하고 적법한 근거에 따라 규정된 목적에 맞게 이용자 동의에 따라 활용되고 이용자의 데이터에 접근하고 정정할 권리를 갖도록 하기 위한 원칙을 잡고 규제도 강화한 것도 이 때문이다. 결국 모바일로 불거진 개인정보에 대한 통제와 관리에 대한 문제가 부각되면서 온라인에서 이용자를 대신하던 ID에 대한 관점도 바뀌게 된다.

새로운 ID 프레임워크 필요성

인터넷과 모바일 시대를 거쳐 디지털 중심 네트워크 사회로 진화를 가속하는 상황에서 ID는 단순히 서비스를 쓸 수 있는 자격을 넘어 소유자를 가리키는 수단이 됐다. 이 때문에 과거의 신원 확인 시스템을 기반으로 개선해 온 오늘날의 ID는 5G로 가속화되는 디지털 사회에서 쓰임새와 기능을 재점검할 필요가 있다.

먼저 지금처럼 서비스마다 중앙화된 본인 인증 방식을 통한 ID 생성을 계속해야 하는가에 대한 문제다. 앞서 지적한 대로 서비스별로 ID를 만들면서 이용자를 인증하는 방식은 본인 인증에 필요한 중요한 개인정보를 통제하고 관리하는 권한을 이용자가 아니라 외부에 맡기는 것이어서 대안이 필요하다.

개인정보의 관리와 책임을 이용자가 갖는 자기주권신원지갑(Self Sovereign IDentity)에 대한 관점에서 나온 것이 분산 ID다. 지금처럼 특정 서비스의 서버 안에 자격 증명을 담아 두는 것이 아니라 이용자의 신원을 확인하거나 자격을 증명하는 증명서를 네트워크로 연결된 다양한 장치에 저장하고 이용자의 지문이나 홍채 등 고유 정보를 동원해 이를 확인하는 신원 관리 체계다. 분산 ID를 구현하고 운영하는 방법에 대해선 블록체인을 비롯한 여러 기술을 응용하지만, 적어도 지금처럼 중앙화된 기관을 통하지 않고도 이용자의 신원을 인증할 수 있는 특징이 있어 국내외 IT 기업이 이에 대한 실증 작업을 진행 중이다.

그렇다고 분산 ID가 무조건적인 해결책이라고 할 수 없다. 단지 이용자의 본인 확인에 중점을 두던 기존 오프라인 신원 증명에 기반을 둔 ID 체계에서 하기 어려웠던 개인정보 통제와 관리의 권한을 이용자에게 돌려주고 ID에 대한 복잡성을 줄이는 장점은 분명히 있다. 그러나 이용자에게 개인정보의 통제와 관리 권한을 돌려주는 일이라도 공동체가 이를 받아들일 수 있는 논의와 준비가 없으면 새로운 ID 체계에 대한 혼란만 키울 가능성도 있다. 하지만 이 논의는 피할 수 없다. 디지털 세계에서 이용자를 안전하게 증명하는 새로운 ID 프레임워크는 데이터 기반 사회로 가는 가장 중요한 열쇠이기 때문이다.

사회변화를 이끄는 '행동하는 인터넷정책'으로의 패러다임 전환

이원태

정보통신정책연구원 연구위원

2019년 타임즈의 '올해의 인물'로 선정된 16세 환경운동가 그레타 툰베리(Greta Thunberg)는 우리 인류가 직면한 '기후 위기'에 대해 더 이상 침묵하지 말고 '기후 행동'에 나서야 할 중요한 시기가 바로 2020년이라고 말했다. UN과 같은 국제기구를 비롯해 전 세계 국가들도 '기후 위기' 또는 '기후 변화'를 2020년의 중요한 정책의제로 삼고 이산화탄소배출 감소 등 지속가능한 대응전략 마련에 부심하고 있으며, 2020년에 예정된 주요국의 선거들에서도 기후 문제가 중점 의제로 부각되고 있다.

그런데 2020년은 기후행동의 전 지구적 요구만큼이나 인터넷의 영역에서도 중요한 전환점이 될 것으로 보인다. 최근 인터넷 기술의 미래를 전망하거나 인터넷의 사회적 영향과 관련한 이슈를 다루는 상당수의 연구자들이 기술적 솔루션에 대한 과잉의존 경향에서 탈피해 사회변화(social chage)에 좀 더 큰 비중을 두고 논의하기 시작했기 때문이다. 그들은 신기술의 사회적 책무성을 추상적으로 논의하는데 그치지 않고 구체적인 실행방법론을 마련하거나 책임 있는 정치사회적 실천까지 요구하기도 했다.

예컨대 알고리듬 편견이나 차별과 같은 이슈뿐만 아니라 기후 위기와 같은 글로벌 현안에 대해서도 인터넷과 관련한 정부, 기업, 학계가 보다 적극적이고 구체적인 문제해결에 나서야 한다는 공감대가 형성되고 있다. 오랫동안 인터넷이 인간의 행동 데이터를 추적해서 비즈니스화 하는데 유용한 수단으로만 간주되었다면, 올해는 인터넷을 사회변화를 추동하는 행동규범의 기제로 포섭하려는 움직임이 더욱 가시화될 것으로 보인다. 그런 문제의식에서 이 글은 최근 사회 변화의 관점에서 인터넷의 책임과 역할을 전망하는 다양한 논의들을 소개하고, 향후 알고리듬 시대의 인터넷 정책 과제는 무엇인지를 논의하고자 한다.

기술은 사회변화를 위한 책임성을 가져야 한다

주지하다시피 기술과 사회의 관계를 바라보는 관점에는 기술결정론(technological determinism)과 사회구성론(Social Construction of Technology)이 대립하고 있었고 인터넷 초기에는 기술이 사회를 바람직하게 바꿀 것이라는 낙관론이 지배했었다. 그러나 인터넷과 소셜미디어의 확산 속에서 인터넷을 통한 여론 왜곡과 디지털 포퓰리즘이 일상화되고 민주주의를 위협하는 요소로 변질됨에 따라 인터넷 기술에 대한 초기의 낙관론은 크게 신뢰를 잃게 되었다. 이같은 인터넷 낙관론의 퇴조와 비관론의 부상은 객관적인 사실(fact)마저 부정하고 알고리듬 기반의 가짜뉴스(fake news)를 더 신뢰하는 이른바 '진실의 쇠퇴(truth decay)'[1] 현상을 배경으로 하는데 이는 인터넷 기술에 대한 최소의 기대마저 붕괴했다는 것을 의미한다.

그렇다고 해서 기술의 사회적 맥락을 강조하는 사회구성론의 관점이 상대적으로 힘을 얻고 있는 것은 아니다. 기술혁신이나 기술변화의 과정이 정치사회적 시스템과 상호작용하는 상황을 중시하는 사회구성론은 인공지능이라는 새로운 기술의 압도적 영향력 앞에 새로운 규제체계의 미정립, 이해관계 상충의 제도적 조율 실패 등의 한계를 드러냈기 때문이다. 오히려 인공지능 단계의 인터넷 기술이 알고리듬으로 모든 것을 결정함에 따라 그러한 기술을 사용하는 개인과 집단 사이의 불평등을 더욱 심화되고 있는 실정이다. 어쩌면 비관론의 무게가 실린 기술결정론이 다시 부활한 것처럼 느껴진다. 물론 이는 디지털 기술의 엄청난 발전 및 압도적 지배에 비해 이를 규제할 규범력이나 능동적으로 대응하기 위한 사회적 힘이 취약하다는 뜻이다.

1) '진실의 부패(Truth Decay)' 현상을 연구하는 미국 RAND 연구소에 의하면, 진실의 부패는 "공공적 삶에서 사실과 데이터의 역할이 감소하는 현상"을 의미하며 사실과 데이터의 분석적 해석에 대한 거부, 여론과 사실의 혼동, 사실에 대한 개인적 경험의 우위 등의 특징을 지닌다고 한다. https://www.rand.org/research/projects/truth-decay.html

그러나 이 같은 인터넷 담론 지형의 변화는 오히려 기술의 사회적 책임을 좀더 강조하는 학계의 논의를 촉발시키고 있다. 이러한 논의의 가장 대표적인 예가 인공지능의 사회적 영향을 연구하는 미국 뉴욕대 인공지능연구소(AI Now Institute)가 최근 발간한 보고서 "AI Now 2019"(2019.12)이다. 이 보고서는 인종차별, 성차별 등 사회적 불평등을 심화시키는 인공지능의 부작용을 크게 우려하면서 기술전문가 및 정부관계자들에게 인공지능 기술의 사회적 책임성 강화와 함께 보다 강력한 알고리듬 규제 정책을 권고하고 있다. 특히 안면인식기술(face recognition technology) 등과 같이 사람들의 생활과 관련한 의사결정에 중대한 영향을 미치는 인공지능 기술의 사용 금지를 촉구하기도 했다.[2)]

뿐만 아니라 작년 12월초에 캐나다 밴쿠버에서 열린 "NeurIPS 2019"라는 데이터과학자 국제학술대회에서는 우리 모두가 직면한 알고리듬의 편견과 차별 문제가 기술적 접근으로는 미흡하고 사회적 구조를 바꾸는데 과학자들도 나서야 한다는데 공통된 의견을 모았다.[3)] 또한 영국 옥스퍼드대 옥스퍼드인터넷연구소(OII: Oxford Internet Institute)가 지난해 연말 향후 2020-2022년의 새로운 연구프로젝트로 인공지능, 기계학습 등 '신흥기술의 거버넌스(Governance of Emerging Technologies)'로 정하고 알고리듬 블랙박스의 설명가능성, 자동화된 의사결정(automated decision making)의 윤리적 조사 등의 이슈를 연구하는 이유도 그러한 맥락이라고 할 수 있다.[4)]

그리고 세계 최대 컴퓨터과학자들의 모임인 국제전기전자기술협회(IEEE)가 발행하는 저널 <<기술과 사회(Technology and Society)>> 2019년 12월호 특집도 "(기술적) 유용성을 넘어서"(Beyond Usability)라는 주제 하에서 인공지능 등 새롭게 급부상하는 디지털 기술의 영향을 '복합적인 사회기술체제(complex socio-technical system)'라는 관점에서 기술의 윤리적 설계(ethical design)를 중점적으로 다룬 이유도 기술의 사회적 책임성을 강조하는 최근의 상황 변화를 반영하는 것이라 하겠다.[5)]

'정치 행위로서의 데이터 과학' 그리고 인터넷 정책

그러면, 최근 인터넷 기술을 연구하는 과학자들이 사회변화, 특히 인공지능 등 새로운 인터넷 기술에 의해 심화하거나 고착되는 불평등의 정치사회적 조건을 바꾸는 문제에 대해서도 어떻게 목소리를 내고 있는지를 살펴보자.

첫째, 정부의 정책을 변화시키는데 적극 개입해야 한다는 것이다. 우리는 오랫동안 기술결정론의 압도적 우위 속에서 인터넷 경제의 급속한 발전을 가져온 인터넷 인프라, 인터넷 산업, 인터넷 정책(정부)의 삼위일체, 달리 말해 공공-사기업 기술동맹(public-private tech partnerships)을 너무 당연한 것으로 간주해왔다.

2) https://ainowinstitute.org/AI_Now_2019_Report.pdf
3) https://www.wired.com/story/sobering-message-future-ai-party/
4) https://www.oii.ox.ac.uk/news/releases/new-research-to-explore-governance-of-emerging-technologies/
5) https://technologyandsociety.org/technology-and-society-magazine/current-issue/

그런데 기술혁신의 주인공이나 책임을 모두 기업이 맡는 사이에 정부의 기술책임성은 모호하거나 은폐됐다. 예를 들면 최근 행정당국의 CCTV와 인터넷 기업의 안면인식기술이 통합되는 사례가 늘어났지만 기업의 책임론에 비해 정부의 책임론은 상대적으로 미흡했다. 기술의 부작용에 따른 사회적 피해에 대해 공급자인 기업에 전폭적으로 책임을 지우고 정부와 정치권의 면책은 당연시되는 규범 문화가 지배했던 셈이다. 사실상 정부의 알고리듬 기술 오남용에 대한 윤리적, 법제도적 책임 메커니즘이 존재하지 않는다는 뜻이다.

그러나 인공지능 등 신기술의 사회적 영향에서 기업의 책임에 비해 상대적으로 소홀히 다뤄진 정부의 책임성을 더욱 명확히 하고 문제의 정책은 개선하려는 논의 및 움직임이 과학자들 사이에서 지속적으로 나타나고 있다. 대표적인 논의가 뉴욕대의 케이트 크로포드(Kate Crawford) 교수와 제이슨 슐츠(Jason Schultz) 교수가 말하는 '국가행위자로서의 인공지능 시스템(AI System as State Actors)'론이다.[6] 그들은 최근 들어 정부 차원의 알고리즘의 공적 사용이 증가하고 있으나 인권, 기본권, 공정성 등 헌법적 가치에 미치는 영향을 제대로 평가한 적도 없고 인공지능 이용에 따른 공공과 민간의 경계가 모호할 경우 국가의 책임 범위도 명확하지 않으며, 더구나 정부의 책임에 대한 공적인 감독 프로세스도 부재하다면서 인공지능과 관련한 국가의 역할을 명확히 할 필요가 있다고 강조한다.

학술적 논의와 더불어 최근 정부 등 공공차원에서 인공지능 기반의 자동화된 의사결정을 동결하거나 제한하는 미국 과학자들의 캠페인도 전개되고 있다. 특히 안면인식기술을 금지하는 캠페인이 매사추세츠, 오클랜드, 샌프란시스코 등에서 일어났는데, 일부의 연구 프로젝트가 중단되기도 했다. 또한 정부와 기업의 인공지능 알고리듬 정책에 대한 시민사회의 법률적 저항(즉 소송투쟁) 및 일상적인 감사(감시) 요구를 통해 정부의 정책을 변경한 일도 있었다.[7]

요컨대, 종전까지는 구글, 페이스북 등 글로벌 테크 기업들에 대한 규제에 초점을 두었으나, 최근에서야 정부의 인공지능 알고리듬 이용 및 공공기관의 '자동화된 의사결정(ADS)'에 대한 통제를 과연 누가, 어떻게 할 것인가에 대한 논의가 급부상하기 시작한 셈이다. 이 때문에 알고리듬의 사회적, 민주적 통제를 둘러싸고 시민사회와 전문가 공동체의 정부에 대한 정치사회적 압력이 크게 증대할 것이므로, 알고리듬 거버넌스 형성과정에서 정부의 정책 조율 역량은 더욱 중요해질 것으로 예상한다.

둘째, 기술이 정치적 이슈라는 점을 분명히 드러내자는 것이다. 기술의 정치적 성격은 기술이 선거운동을 위한 수단이 되거나 정치적 기능을 대체한다는 것이 아니라 기술이 정치적 의사결정 방식에 영향을 미치고 더 나아가 국가와 시장의 관계, 법 제도와 같이 한 사회의 규칙을 변경하는 힘을 지니고 있다는 뜻

6) https://columbialawreview.org/content/ai-systems-as-state-actors/
7) 호주 정부(보건복지부)는 복지수당 수령자를 대상으로 한 인공지능 알고리듬 기반의 자동화된 부채회수(즉 빚독촉) 프로그램인 'robo-debt'을 시행하려다가 시민들의 저항에 부딪히자 관련 정책을 변경한 바 있다. 이 사례에 대해서는 Pasquale, Frank(2019), "The Second Wave of Algorithmic Accountability" https://lpeblog.org/2019/11/25/the-second-wave-of-algorithmic-accountability/?fbclid=IwAR3MKPuL5rD6r9O2IInsCbXX6PKywvTOMM 참조.

이다. 특정한 정파나 정당의 입장에 선다는 것이 아니라 기술의 '탈정치화', 즉 기술과 정치의 관계를 분리하지 말고 알고리듬의 영향평가 등 과학적 데이터로 입법, 정부 등의 정책에 적극적으로 개입함으로써 제도적 조건을 변경하는 행위로서의 정치를 말하는 것이다. 즉 인공지능 등 신기술이 초래하는 인종차별, 성차별 등 불평등의 자동화에 대해서 기술적 해결에만 초점을 두지 않고 불평등의 사회적 구조를 바꾸는 데에도 대안과 실천을 요구하는 목소리를 내자는 뜻이다.

이러한 주장의 대표적인 과학자는 하버드대학의 '인터넷 사회를 위한 버크먼클라인센터'의 벤 그린(Ben Green) 교수인데, 그는 과학자와 기업들이 기술혁신의 목표를 '사회적 선(social good)'으로 막연하고 추상적으로 설정하고 정치적인 문제를 회피하는 것을 비판하면서 데이터 과학을 정치행위의 하나로 적극 규정할 것을 강조한다.[8] 그는 데이터 윤리, 알고리듬 윤리 등의 추상적인 윤리원칙은 광범위한 사회 정의의 문제를 다루는 데 적합하지 않다면서 윤리 대신 사회 전체의 자원 분배에 영향을 미치는 정치가 더 필요하다고 주장한다. 그런 맥락에서 데이터를 추출해서 분석만 하지 말고 데이터 분석과 활용에 정치사회적 권한을 부여(empowering)해서 시민들의 보다 책임 있는 행동을 견인하는 '데이터 정치(data politics)' 혹은 '데이터 행동주의(data activism)'도 그러한 관점과 맥을 같이 한다고 볼 수 있다.[9] 대규모의 데이터 속에서 알고리듬 차별이나 편견을 분석하고 드러내고 기술적 개선책(업데이트 등)을 제시하는 것도 중요하지만, 편견을 넘어 정의를 실현하기 위한 사회변화 전략도 고민하는 것도 과학자들의 책임이라는 것이다.

사회정의를 위한 포용적 기술로서의 인터넷

셋째, 인터넷 기술과 정책에서 공정성(fairness)의 문제를 적극적으로 포함해야 한다는 것이다. 이 문제가 중요해지는 이유는 그동안 우리가 엄청난 정보화의 진전을 이룩했으나 정보격차 또는 디지털 격차의 현안이 알고리듬 단계에 와서 오히려 더욱 심화하였기 때문이다. 그래서 알고리듬 윤리, 데이터 윤리와 같은 기술 윤리적 원칙이나 관련 정책이 매우 중요해진다는 것이다. 하지만 더블린대학의 아베바 버헤인(Abeba Birhane) 교수가 지적했듯이, 알고리즘 편견을 기술적, 윤리적으로 해결할 수 있다는 믿음[10]은 '인공지능 과잉 서사(AI over-hype narrative)', 즉 데이터 맹신주의에 불과하다. '디지털 넛징(digital nudging)'이라는 말이 있듯이, 사람들이 무의식적으로 자신의 습성이나 생활양식 등 개인의 행위를 알고리듬 기반의 자동화 메커니즘에 스스로 맞추도록 훈육되는 기제, 즉 '알고리즘적 식민주의화(algorithmic colonization)'는 기술적 수정이나 윤리적 선언으로 해결할 수 없다는 것이다.[11]

8) Green, Ben (2019). Data Science as Political Action: Grounding Data Science in a Politics of Justice, https://arxiv.org/abs/1811.03435
9) Beraldo, Davide & Milan, Stefania (2019), "From Data Politics to the Contentious Politics of Data" Big Data & Society. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3487477
10)알고리듬 편견이나 부작용을 기술적, 윤리적으로 교정할 수 있다는 과학자들의 주장에 대해서는 https://www.nytimes.com/2019/12/06/business/algorithm-bias-fix.html#click=https://t.co/lkLEpfDwF9 참조.

이와 관련해서 플로리디 교수는 지금까지 우리가 두 가지의 규범적 접근방식, 즉 도덕적 평가에 기반을 둔 디지털 윤리(digital ethics)와 법규준수(legal compliance)에 초점을 둔 디지털 규제(digital regulation)에 치중해 왔는데, 정보사회가 올바르게 작동하도록 디지털 정책을 조율하고 또 정치사회적 조건의 변화까지 수반하는 정책 결정에 초점을 둔 디지털 거버넌스(digital governance)의 형성에 대해서도 과학자들의 적극적 관심이 필요하다고 주장한다(Floridi, 2018).[12)]

또한 앞에서 소개한 뉴욕대 인공지능 연구소(AI Now Institute)의 보고서도 알고리듬 편견 연구가 단순히 기술적 오류 수정을 넘어 정치적, 사회적 구조 변화에도 관여해야 한다고 주장한다. 인공지능의 편견이나 공정성 연구는 기술 통계적으로 엄격한 솔루션을 추구하는 수학적 접근방식의 한계를 넘어 인종주의, 사회적 약자, 다양성 등의 비기술적(non-technical)이고 사회적인 맥락(특히 사회정의)들에 관한 연구와 해결방안도 함께 지향해야 한다는 것이다.

그리고 기후문제라는 전 지구적 정의의 문제에 대해서도 인터넷의 적극적 관여가 요구된다. 기후 위기에 대응한 기후 행동이 본격화하는 상황에서 인터넷 기술 또한 기후 문제의 기술적, 사회적, 환경적 책임에서 자유롭지 못하다는 문제의식 아래서 이에 대응한 인터넷 기반의 적극적인 기후정책을 제시하지 않으면 안 될 것이다. 이미 일부 인공지능 과학자들은 인공지능 연구와 개발의 이산화탄소 배출량을 계산해 탄소 감소의 기후정책에 적극적으로 부응하려는 움직임이 가시화하고 있다.[13)] 즉 기후문제 또는 환경문제를 알고리즘 책무성의 영역으로 간주하고 이에 책임 있는 연구와 정책을 제시하려는 노력인 것이다.

알고리듬 시대의 인터넷 정책 전망

앞에서 살펴본 바와 같이 인터넷 기술이 알고리듬 기반의 새로운 발전 단계에 이르면서, 기술과 사회의 관계를 근본적으로 다시 설정할 것을 요구하고 있다. 지금까지 우리는 새로운 인터넷 기술이 사회에 큰 영향을 미치고 또 역으로 사회가 신기술의 성격을 규정하는 등 기술과 사회의 상호작용에 대해 주로 일반론적으로 논의해왔다. 그러나 알고리듬화하는 인터넷 기술의 부작용이 기술적, 윤리적으로 통제하기 어려운 상황까지 간다면, 새로운 기술이 민주주의 사회를 지탱하는 최소한의 가치나 원칙을 약화시키거나 배제

11) Birhane, Abeba (2019), "The Dark Side of Digitisation and the Dangers of Algorithmic Decision-Making", https://www.theelephant.info/ideas/2019/08/08/the-dark-side-of-digitisation-and-the-dangers-of-algorithmic-decision-making/

12) Floridi, Luciano (2018), "Soft Ethics and the Governance of the Digital", Philos. Technol. (2018) 31:1-8.

13) 이들 인공지능 공학자들은 기계학습과 관련한 연구의 탄소영향(ML CO2 Impact)을 알려주는 소위 '머신러닝 이산화탄소 배출량 계산기(Machine Learning Emissions Calculator)'를 만들어 공개 서비스하고 있다. 만약 연구자나 개발자들이 머신러닝 연구의 탄소영향을 추정하려면 자신의 연구환경에서 사용되는 하드웨어(hardware type), 사용시간(hours used), 클라우드 제공업체(provider), 컴퓨팅 지역(region of compute) 등을 선택하면 탄소배출량이 자동 계산되어 나온다. 연구자들은 앞으로 이러한 결과를 토대로 인공지능 연구의 탄소배출량을 줄이기 위한 실천방안의 일환으로 논문, 블로그 게시물 및 출판물 등에 탄소배출량 표시를 일반화하는 것을 제안한다. 이에 대해서는 https://mlco2.github.io/impact/#compute 참조.

하지 않도록 하는 실질적인 노력이 더욱더 중요해지고 있다. 이제는 인터넷의 사회적 영향에 대한 분석과 정책 참조라는 정태적인 접근이 아니라 사회문제 해결 또는 사회변화를 추동하는 행위자로서 인터넷을 자리매김하는 동태적 정책 프레임워크가 그 어느 때보다 필요하다는 뜻이다.

그러나 그동안 우리의 인터넷 영역은 신기술의 차별적 권력 효과에 따른 공정성의 문제를 적극 제기하는데 매우 소극적이었고, 자율성, 투명성, 공정성 등의 원칙(principle) 중심의 What에만 초점을 두었지, 신기술의 위험성이나 부작용을 실제적으로 줄이기 위한 How에는 인색해 사회를 변화시킬 행동(action) 역량이 축적될 기회가 그리 많지 않았다. 특히 사회적 약자를 위한 보편적 디자인(Universal Design)의 기술적 프로그램만 있었을 뿐 그러한 문제를 반영한 사회조건의 변화를 가져오기 위한 구체적 실천력은 미흡했다. 사실상 인터넷 등 우리나라 IT 영역에는 '정치적 중립'으로 포장된 탈정치적 태도가 만연해 있었다고 해도 과언이 아니었다.

하지만 알고리듬 시대가 오면서, 인터넷 관련 연구자들은 기술적 문제를 추상화 하는데 머물기 보다는 인터넷 연구를 오히려 사회적 개입의 수단으로 간주해야 할 단계에 진입했다고 볼 수 있다. 알고리듬 단계의 인터넷 기술이 초래하는 경제적, 사회적 불평등이라는 근본적 문제는 단순히 기술적 개선의 차원을 훨씬 뛰어넘는 이슈이기 때문이다. 따라서 앞으로 신기술의 부작용을 해결하는데 기술적, 윤리적 접근의 한계를 인식하고 사회적 변화를 이끄는 행위자로서 자각하는 일이 중요하며, 더 나아가 인터넷 기술과 관련된 다양한 행위자들 간의 더욱 적극적인 상호작용, 대화와 토론, 숙의를 통해 사회의 변화와 혁신을 이끌어야 할 것이다. 프랑크 파스퀘일 교수가 말한 것처럼, 우리도 인터넷의 사회적 부작용을 기술적으로 개선하는 차원을 넘어 기술의 구조적인 문제도 적극적으로 다룰 수 있는 '알고리듬 책무성의 두 번째 물결(second wave of algorithmic accountability)'을 적극적으로 맞이할 필요가 있다.

기술, 사람을 돌아보다

최호섭 (work.hs.choi@gmail.com)

디지털 칼럼니스트

새로운 기술에 대해 기대하고, 환호하는 이유는 무엇일까? 기술은 그 자체로 흥미롭고 재미있기도 하지만 결과적으로 삶에 이전과 다른 변화를 만들어주기 때문이다. '혁신'으로 대변되는 기술 발전의 목표는 결국 사람에 있다는 이야기다.

하지만 기술은 과연 우리와 얼마나 가까이에 있었을까? 많은 사람이 밤을 새워가며 지켜보던 미국 IT 기업들의 개발자 컨퍼런스, 그리고 CES나 MWC로 대표되는 전시회는 여전히 가장 최신 기술이 소개되는 자리지만 그 관심은 피부로 느껴질 만큼 줄어들고 있다. 단순히 '혁신이 없다'는 말로 표현되지만 사실 최근의 기술은 그 어느 때보다 빠르게 발전하고 있고, 또 구체화하고 있다. 하지만 그 변화와 혁신이 잘 와 닿지 않는 것도 사실이다. 기술이 우리와 그만큼 멀리 있기 때문이다.

기술의 발전, 그리고 멀어지는 사람과의 거리

돌아보면 기술들은 그리 가까이 있지도 않았을 뿐 아니라 오히려 더 멀어져 간 게 사실이다. 친절하지 않았다. 기술과 사람 사이의 간극이 멀어질수록 이를 이용하는 경우도 많아진다. 어렵고 불확실한 기술들을 바탕으로 불안감을 만드는 비즈니스다. 두려움은 가장 잘 팔리는 상품이고 인공지능이나 빅데이터, 5G, 4차 산업혁명 등 기술이 어렵고 개념적일 때 불안은 더 커진다.

기술이 사람을 돌아볼 필요가 있다. 기술의 목표는 신기한 것이 아니다. 주가를 올리기 위해서, 누구에게 보여주기 위해서 만드는 것이 아니라 얼마나 더 편리한 삶을 만들어줄 수 있느냐에 따라 가치가 결정되는 것이 기술이다. 그 틈을 좁힐 필요가 있다.

기술에 가장 예민한 IT 기업들도 이를 알고 있다. 2019년의 기술 흐름은 드디어 뒤를 돌아보기 시작했다. 인공지능, 클라우드, 가상현실, 5G, 반도체 등 그동안 쏟아 놓았던 수많은 기술이 그 자체로 받아들여지고, 목표와 방향성을 이해하는 이들이 많지 않기 때문이다.

늘 새로운 것을 빠르게 쏟아내고 사람들의 반응을 중요하게 살피는 구글을 돌아보면 흥미롭다. 구글은 개발자 컨퍼런스인 구글I/O에서 '모두에게 쓸모 있는 구글을 만들 것(Building a more helpful Google for everyone)'이라고 발표했다. 큰 의미가 있나 하고 볼 수 있지만 쉽고 명확한 비전이다. 새로운 기술들의 의미를 돌아보고 있다는 이야기다.

구글이 쏟아놓은 것들도 이를 충실하게 반영하고 있다. 구글이 공개한 '라이브 속기(Live transcribe)'는 켜 두면 음성 인식 기술을 통해 말을 알아듣고 이를 글자로 받아 적는다. 단순한 STT(Speech to Text) 기술로 볼 수 있지만 사실 이를 효과적으로 해주는 서비스는 이제까지 거의 없었다. 정확도는 말할 것도 없다. 하지만 이 기술은 구글에 가장 쉬운 것 중 하나다. 그동안 구글 어시스턴트를 비롯해 오토ML 등 많은 곳에서 음성 인식 기술을 개발하고 활용했다. 받아쓰기는 구글에 기술적으로 아무것도 아닐 수 있지만 이를 꺼내 놓지 못했을 뿐이다. 그 생각의 전환이 바로 사람을 돌아보는 데에서 나오는 것이다.

다시 보는 '혁신'의 의미

바로 1년 전인 2018년 구글은 똑같은 자리에서 같은 기술을 이용한 '듀플렉스(Duplex)'를 발표했다. 인공지능이 사람의 말을 알아듣고, 그에 따라 적절한 답을 한다는 아이디어로 시작한 이 기술은 음성 인식, 문장 해석, TTS(Text to Speech) 등 대화와 관련된 온갖 인공지능 기술을 품고 있는 결정체였다. 이 기술은 세상을 깜짝 놀라게 했고 큰 관심을 받았다.

하지만 컴퓨터가 너무 능숙하게 대화를 이끌어가는 것에 대해 사람들은 적잖은 불안과 불편함을 느꼈다. 위협적이라고 받아들이기도 했다. 기술의 완성도는 흠잡을 데 없었지만 사람과의 거리는 그만큼 더 멀어진 기술이라고 할 수 있다. 그에 비해 라이브 속기는 너무나도 단순한 기술이지만 그 정확도가 높아지고, 쓰기 쉬워지면서 '쓸 만하다'는 인상을 주었고 그만큼 가깝게 쓰이고 있다. 구글은 최근 이 라이브 속기에 번역 기술을 더 해 실시간 번역 기술을 발표하기도 했다. 이 역시 음성인식, 번역 등 구글이 오랫동안 다져왔던 기술이고 너무 쉬운 기술이지만 간단한 조합만으로 그 가치가 달라지는 것이다.

스마트폰, PC 등 우리가 쉽게 접하는 기술들만 봐도 이 흐름은 쉽게 나타난다. 최근 안드로이드와 iOS를 비롯한 운영체제의 방향성은 새로운 기술을 더 하기보다 경험에 더 집중하고 있다. 기존의 기능들을 더 원활하게 쓸 수 있도록 가다듬어서 사용성을 높이고 스마트 기기를 더 안정적으로 쓸 수 있도록 하는 것이다. 예를 들어 메시지 앱을 더 편하게 쓰고, 음성 인식의 정확도와 활용도를 높이는 식이다. 그 기술은 장애인들을 위한 접근성으로 나타난다. 애플은 음성으로 맥을 다룰 수 있도록 보이스 콘트롤을 향상했고 구글도 발음 때문에 의사소통이 어려운 장애인들의 목소리나 움직임을 머신러닝으로 학습해 의사를 정확히 전달해주는 기술을 공개하기도 했다.

스마트폰에 대한 의존도가 높아지는 것에 대한 고민도 지속해서 고민되는 주제다. 안드로이드의 디지털 웰빙이나 iOS의 스크린 타임처럼 사용 습관을 보여주고, 화면을 아예 흑백으로 만드는 등 새로운 기술들로 해결되고 있다. 더 많이, 오래 쓰게 하는 것이 기술과 비즈니스의 목표가 아니라 얼마나 더 효과적으로, 건강하게 쓰느냐로 관심이 움직이고 있다는 이야기다.

기술의 본질적 목표, '사람'

2019년 가장 큰 기대와 실망을 샀던 기술은 단연코 5세대 이동통신이다. 국내 이동통신사들과 스마트폰 제조사들은 세계에서 처음으로 5세대 이동통신을 서비스하기 위해 막대한 노력을 기울였다. 그리고 4월 3일 사실상 상용 서비스는 아니지만 각 통신사가 선별한 셀러브리티들을 대상으로 제한적 서비스를 시작했다. 그렇게 우리나라는 세계에서 처음으로 5세대 이동통신을 서비스하는 국가가 됐다. 지표도 나쁘지 않다. 현재 우리나라에서 팔리는 스마트폰들의 절반 가까이는 5세대 이동통신에 접속할 수 있는 기기다.

하지만 5G는 우리 가까이에 얼마나 가까이 있을까? 현장의 반응은 그리 긍정적이지 않다. 그 가치가 제대로 전달되지 않기 때문이다. 제 속도를 내기는커녕 잘 터지지 않거나, 이 때문에 배터리 소모가 더 빨라지는 경우도 많다. 물론 이제까지 망 설비 초기에 3G나 LTE도 비슷하게 겪었던 일이긴 하다. 하지만 5G는 너무 서두른 느낌이 있고, 무엇보다 LTE 이상의 '그 무엇'을 보여주지 못하고 있다.

5G는 차세대 IT 기술의 밑거름으로 꼽혀 왔다. 인공지능, 자율주행, 가상현실 등 모든 기술이 바로 5G에서 시작된다. 하지만 현재 5G는 그저 '조금 더 빠른 인터넷망' 그 이상의 가치를 만들어내지 못하고 있다. 그마저도 완전하지 못하기 때문에 '경험'이 썩 좋지 않다. 결국 공급자들의 의도와 달리 적지 않은 이용자들은 지난 한 해 동안 더 비싼 요금을 물면서도 5G를 끄고 썼고, 기본 약정 기간이 끝나면서 5G 가입을 해지하고 LTE로 넘어가는 움직임도 있다. 막대한 투자와 기대로 시작했지만 환영받지 못하는 기술이 된 셈이다.

물론 5G는 초기 단계고, 앞으로 새로운 기술이 더 많이 개발될 것이다. 네트워크는 기반 기술이기 때문에 황무지에 가장 먼저 깔리는 기술이라는 변명도 해 본다. 하지만 준비되지 않은 기술이 한 번 이용자들과 멀어지면 다시 그 간극을 좁히는 데에는 더 오랜 시간이 걸리게 마련이다.

기술의 발전은 당연하고 필요한 일이다. 하지만 기술이 고도화될수록 이유와 명분은 더 필요하다. 사람이 중심에 있을 필요가 있다. 인공지능의 민주화, 프라이버시, 기술의 윤리 등 세상은 기술만큼 그 주변의 환경들에 관심이 쏠리고 있다. 기술이 발전하면서 자연스럽게 사람과 함께 하는 방법이 고민되는 단계로 접어들고 있다. 기술의 목표는 결국 사람이기 때문이다.

데이터 신뢰를 위한 합의 알고리즘

유성민 IT 칼럼니스트 (dracon123@naver.com)

서강대학교 정보통신대학원 대우교수

디지털 사회와 블록체인

블록체인이 등장한지 10년이 넘었다. 2007년 사토시 나카모토(Satoshi Nakamoto)는 비트코인을 소개하면서 블록체인을 최초로 언급했다[1]. 이후, 블록체인은 주목받기 시작했고, 인공지능(AI)과 함께 미래 유망 기술로 자리 잡았다.

1) Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2007, pp. 1-9.

주목받는 이유는 블록체인의 세 가지 제공 가치를 제공하기 때문이다[2]. 첫째는 투명성과 공유성이다. 블록체인은 개인 간(P2P) 네트워크를 통해 참여자인 노드에 데이터를 공유한다. 블록체인의 데이터 공유는 거의 모든 노드에 투명하게 보여준다. 그러므로 투명성을 가진다.

그런데 블록체인은 이러한 데이터를 공유하는 데에서만 끝내지 않는다. 공유된 데이터의 일치된 합의를 가져와 데이터 신뢰성도 보증한다. 다시 말해, 데이터의 무결성을 보증해 데이터 신뢰성을 높인다. 무결성과 신뢰성을 제공하는 셈이다. 끝으로 블록체인은 두 가지 가치를 기반으로 탈 중앙선을 가진다.

블록체인은 모든 노드에 데이터를 공유하고, 이러한 데이터에 합의를 해 신뢰성을 자동으로 보증한다. 중앙 시스템 혹은 중개자 없이 말이다. 이는 블록체인 내 시스템이 탈중앙 형태로 운영하게 한다. 비트코인을 예로 들어보자. 비트코인 거래를 중개하는 중앙 시스템이 없다. 노드가 참여해 거래 이력을 공유하고 합의를 통해 탈중앙 형태로 무결성을 보증하기 때문이다.

블록체인 제공 가치

제공가치	내 용
투명성 & 공유성	데이터를 노드에 투명하게 공유함
무결성 & 신뢰성	공유된 데이터의 합의를 통해 무결성과 신뢰성을 보증함
탈중앙성	자체적으로 시스템 운영이 가능함

블록체인의 이러한 특성은 디지털 신뢰가 중요한 사회에서 주목받게 한다. 블록체인 방식은 기존보다 더 나은 신뢰성을 제공하기 때문이다. 첫 번째 이유는 중앙 시스템의 조작 위험이 없다. 두 번째 이유는 분산 형태이기 때문에 장애 내구성이 높다. 중앙 시스템이 마비되면 시스템에 미치는 악영향이 크다. 그러나 블록체인은 탈중앙 형태이므로 중앙 시스템의 마비 문제가 없다. 마지막 이유는 다수가 보증하기 때문에 중앙 시스템보다 더 신뢰성이 높다. 중앙 시스템이 불투명하게 데이터를 처리하는 것보다 다수에게 투명하게 합의를 통해 데이터를 처리하는 블록체인의 신뢰성이 더 높을 수밖에 없다.

정리하면, 블록체인은 디지털 신뢰가 중요한 사회에 탈중앙 형태라는 새로운 패러다임을 제시하고 있다. 그러나 여기서 한 가지 화두가 있다. 블록체인을 적용했다고 해서 데이터 신뢰성을 충분히 보증한다고 할 수 있을까? 혹은 데이터 신뢰성을 가진다고 무조건 믿어야 할까? 이는 기술 찬양론에 불과하다. 디지털 신뢰 보증을 위해서는 블록체인을 정확히 분석하고 개선을 위한 연구가 필요하다.

2) 유성민), “미래 사회에 지능을 더하다: 블록체인과 혁신 서비스”, AI 플러스, 한국정보화진흥원(NIA), 1-94쪽, 2019년 02월.

블록체인의 오해와 합의 알고리즘의 대두

블록체인과 인공지능은 상당히 많은 공통점을 가지고 있다. 그중 가장 큰 공통점은 기존 사회를 개선하는 것이다. 블록체인은 디지털 사회에 신뢰성을 높여주고, 인공지능은 데이터 분석 범위와 정확성을 높여준다. 그러나 기술 적용에만 초점을 둬서는 안 된다.

인공지능은 개념적 기술로 사람의 지능을 흉내 내는 기술이다. 실질적으로 연구되는 분야가 아니다. 엄밀히 말해, 이를 동작하는 알고리즘이 연구되고 있을 뿐이다. 최근에는 기계학습 알고리즘이 주목받고 있다. 그리고 이에 관해 연구하고 있다. 다시 말해, 같은 인공지능이라도 기계학습 알고리즘 설계에 따라 데이터 분석 범위와 정확도가 달라진다.

이는 블록체인에서도 마찬가지이다. 블록체인도 개념적 기술이다. 실질적으로 연구되는 분야가 아니다. 블록체인은 P2P 네트워크와 합의 알고리즘에 의해서 움직인다. 여기서 합의 알고리즘은 블록체인에서 중요한 역할을 한다. 데이터 신뢰성 보증하는 역할을 담당하기 때문이다. 합의 알고리즘은 P2P 네트워크에 의해서 분산된 데이터를 합의에 따라서 일관된 데이터가 모든 노드에 저장될 수 있도록 만드는 알고리즘으로 정의할 수 있다.

결국, 합의 알고리즘은 블록체인에 무결성&신뢰성과 탈중앙성을 가지는 데에 중요한 역할을 한다. 블록체인에 합의 알고리즘이 없다면, 데이터는 단순히 분산돼 있다. 분산형 데이터 구조일 뿐이다. 그렇게 되면, 디지털 신뢰에 있어 블록체인은 아무런 의미가 없다.

이를 잘 보여주는 논문 제목이 있다. “블록체인은 = 분산형 원장 + 합의 알고리즘”이라는 제목의 논문이 있다. 이러한 논문에서도 알 수 있듯이 블록 체인은 탈중앙 방식의 신뢰에서 중요한 역할을 한다[3].

블록체인에 관해 몇 가지 오해가 있다. 그중 하나로 블록체인을 사용하면 전력 소모가 발생하는 점이다. 이는 비트코인에 사용되는 작업증명알고리즘(PoW)에 해당하는 말이다. 그리고 블록체인 내에 저장된 데이터 조작을 위해서 50%를 초과한 컴퓨팅 파워가 필요하다는 말이 있다. 이 또한 오해이다. 우선, 블록체인 내에 저장된 데이터를 조작하는 것은 거의 불가능에 가깝다. 블록체인 이전 값을 기반으로 블록을 만들어 체인 구조를 형성하고 있다. 해시 알고리즘을 사용하고 있기 때문이다. 해시 알고리즘은 임의 값을 함수 기능에 의해 특정 값으로 변환하는 알고리즘이다. 참고로 비트코인에 적용된 해시 알고리즘은 SHA-256이다. 16진수 값으로 변환한다. 해시 알고리즘 특징은 임의 값이 변하면 해시 함수에 의한 결과 값도 변한다는 것이다. 그리고 역은 불가능하다. 결과 값으로 나온 16진수 값을 가지고 투입된 값을 알아낼 수 없다. 비트코인은 이를 기반으로 PoW 알고리즘을 고안해냈다.

3) Andreas Meier and Henrik Stormer, “Blockchain = Distributed Ledger + Consensus”, HMD Praxis der Wirtschaftsinformatik, 55(6), pp.1139-1154, December 2018.

비트코인은 노드가 특정 블록을 생성할 수 있는 조건으로 블록의 해시 결과값이 제시된 16진수 값보다 작은 값을 가장 먼저 발견할 때로 한정하고 있다. 다시 말해, “주어진 16진수 값보다 작은 블록을 빨리 만들어내”라는 문제를 가장 빠르게 맞히면 블록 생성권이 주어진다. 그리고 보상을 받게 된다. 블록에는 이전 블록의 해시값, 거래 이력 그리고 난수값이 있다. 난수값 조절로 문제를 풀 수 있다. 여기서 중요한 점은 이전 블록의 해시값이다. 블록에는 이전 블록의 해시값이 들어있다. 그러므로 이전 블록을 변경할 수 없다. 이전 블록을 변경하면 이전 블록의 해시값도 변한다. 그러면 연쇄적으로 블록이 모두 변하기 때문이다. 그래서 이전 블록의 해시값을 변경하지 않으면서 블록 데이터 변경이 가능은 하다. 해시 충돌(Hash Collision)을 유발하게 말이다. 해시 충돌은 임의 값을 넣었을 때, 해시에 의한 결과값 중복을 말한다. 비유하면, 생일이 똑같은 사람이 두 명이 있는 경우이다. 결론부터 말하면, 해시 충돌은 가능은 하다. 다만, 이를 위해서는 막대한 시간이 필요하다. 해시 충돌을 위해서는 2^256번의 연산이 필요하다. 그러나 생일 패러독스 가능성에 의해서 2^130번[4] 연산 정도면 충분히 해시 충돌을 일으킬 수 있다. 그런데 이는 세계 최고 슈퍼 컴퓨터보다 1900배 좋은 슈퍼 컴퓨터로 돌리면 1천만 초 걸려서 99.8% 확률로 해킹할 수 있다.

그럼 컴퓨팅 파워 50% 초과는 어디에서 나온 말일까? 신규 블록 생성에만 해당한다. 비트코인 내에서 이중 지불 공격이 일어날 수 있다. 악의 노드 A가 100 비트코인을 가지고 있다고 생각해보자. 노드 A는 거래를 위해 노드 B에게 100 비트코인을 지불했다. 본인의 100 비트코인을 모두 소진한 셈이다. 그런데 노드 A는 사기 치기 위해서 자신이 만든 또 다른 노드 C에게 100 비트코인을 중복으로 비트코인을 지불했다고 가정해보자. 이러한 공격이 이중지불공격이다. 노드 A 입장에서는 노드 C쪽과의 거래한 데이터가 남아야 한다. 노드 A는 노드 C쪽의 거래가 블록으로 인정받기를 기대해야 한다.

그러나 이러한 일이 발생할 가능성은 매우 적다. 대부분 블록 생성자 노드는 블록 생성 시에 검증을 통해 이중지불공격임을 알아내기 때문이다. 그리고 비트코인의 블록체인은 대다수 블록 생성자가 본인의 비트코인 안정성 등 이해관계에 따라 성실하게 블록 생성을 할 것으로 가정하고 있다. 이러한 가정에 따라, 노드 C의 거래는 무산될 가능성이 크다. 따라서 노드 A는 블록 생성을 직접 해야 한다. 이때, 노드 A는 직접 참여해 노드 C와의 거래 데이터를 블록으로 만들 수 있어야 한다. 그런데 현실적으로 가능해지려면 노드 A가 블록 생성에 차지하는 컴퓨팅 파워 비중이 높아야 한다. 그리고 등장한 용어가 50% 초과이다. 다시 말해, 노드 A는 성실한 노드 전체의 컴퓨팅 파워를 초과해야 한다. 쉽게 말해, 노드 A와 성실 블록 생성자가 50대 50으로 이루는 것을 초과해야 한다. 그러면 이중지불공격이 일어날 수 있다.

그러나 반드시 50% 초과해야지 이중지불공격 발생 확률이 높을까? 이러한 생각은 356명이어야만 중복된 생일인 사람이 나온다고 생각하는 것과 같다. 실질적으로 시뮬레이션을 통환 여러 연구에 따르면,

4) 생일 패러독스: 생일이 같은 사람이 있기 위한 사람의 수를 확률적으로 계산함. 이론적으로는 1년보다 숫자가 큰 366명이 있어야지 같은 생일자가 나올 수 있음. 그러나 실제로는 그 보다 더 적은 숫자가 있어도 확률저으로 같은 생일자가 나올 확률이 있음.

컴퓨팅 파워 20%를 초과한 노드가 등장하면 이중지불공격을 충분히 일으킬 수 있다. 어떤 연구에서는 25%를 초과하면 이중지불공격을 일으켜 블록 데이터 생성 신뢰성에 악영향을 미칠 수 있다[5]. 그래서 해외의 여러 유명 블록체인 학계에서는 PoW의 블록체인 데이터 신뢰성 혹은 장애 허용률(악의 노드 대응성)을 51%가 아닌 25%까지로 보고 있다.

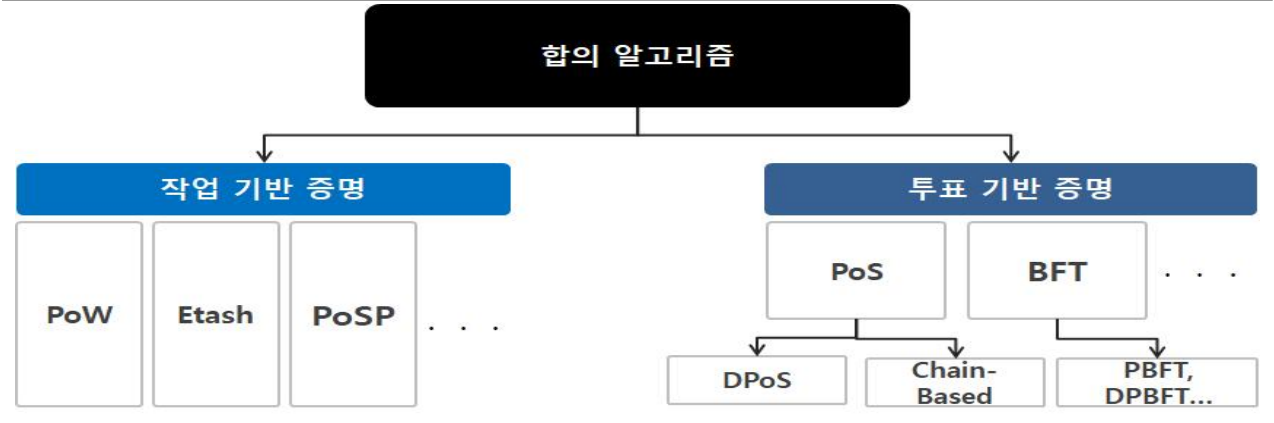
정리하면, 합의 알고리즘은 블록체인이 디지털 신뢰 사회 형성에 활용될 수 있도록 중요한 역할을 한다. 그러므로 합의 알고리즘에 관해 구체적으로 연구할 필요가 있다. 그리고 블록체인을 적용했다고 해서, 디지털 신뢰성을 완벽하게 보증하는 것은 아니다.

현재 합의 알고리즘이 직면한 문제는 데이터 신뢰성을 어떻게 탈중앙 형태로 제대로 보증할 수 있는지가 중요하다. 그리고 탈중앙 형태에서 성능을 끌어올리는 것도 중요하다.

두 가지 유형으로 나뉘는 합의 알고리즘

현재 합의 알고리즘에 관해 상당히 많은 연구가 진행되고 있다. 의 알고리즘은 블록 생성 방식에 따라 '작업 기반 증명(Work Based Proof)'과 '투표 기반 증명(Voting Based Proof)'으로 나눌 수 있다. 전자는 컴퓨팅 파워와 같은 물리적 자원을 소모해서 합의 하는 방식이다. 작업증명알고리즘(PoW), 이대시(Ethash), 용량증명알고리즘(PoC) 등이 있다. 후자는 컴퓨팅 자원을 활용하지 않고 투표 혹은 지분이라는 방식을 통해 물리적 자원을 활용하지 않고 증명하는 방식이다. 이러한 유형에는 지분증명알고리즘(PoS), 위임형 지분증명알고리즘(DPoS), 비잔틴장애허용알고리즘(BFT), 중요증명알고리즘(PoI) 등이 있다.

블록 생성 방식에 따른 합의 알고리즘 구분



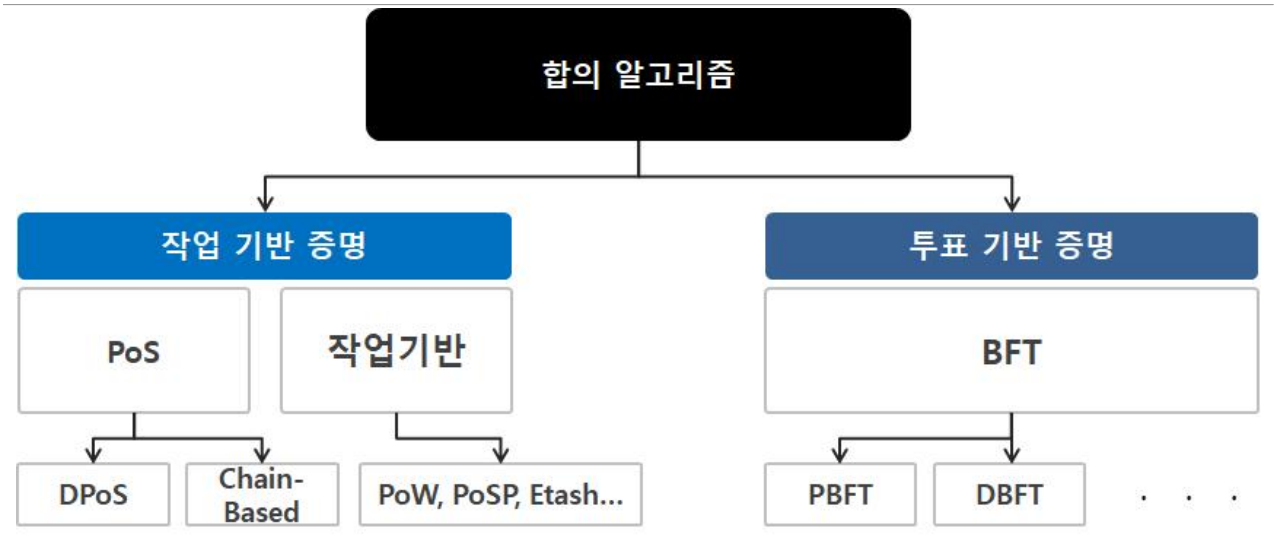
[출처: 유성민(2019), 합의알고리즘강의자료(서강대)]

5) Ittay Eyal and Emin Gün Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable", Communications of the ACM, Volume 61, Issue 7, 2018, pp.95-102.

또 다른 구분 방법으로는 생성된 블록의 검증 방식이다. 두 가지 유형으로 나눌 수 있다. 첫 번째로 블록 생성 후의 검증이 있다. '실시간성 우선(Liveness over Safety)'이라고 부른다. 말 그대로, 블록을 생성한다면 검증하는 방식이다. 두 번째로 블록 검증 후에 블록을 생성하는 것이다. '안정성 우선(Safety over Liveness)'이라고 부른다. 참고로 전자에는 PoW, PoS, Etash, PoSP, PoI 등이 속한다. 후자에는 BFT 계열이 속한다. 학계에서는 블록의 검증 방식으로 합의 알고리즘을 구분하는 것을 선호한다. 차이가 명확하기 때문이다.

실시간성 우선의 경우 블록 생성에 초점이 맞춰져 있다. 그러므로 생성된 블록의 안정성이 낮다. 블록이 중복으로 발생할 수 있기 때문이다. 참고로 이를 '포크(Fork)'라고 한다. 포크는 이중지불공격 등과 같이 블록이 중복으로 발생하는 상황을 뜻한다. 실시간성 우선은 합의 되지 않은 블록이 생성되고 전파되는 과정을 거친다. 그리고 블록 생성자는 검증한다. 이러한 검증 과정 시간 동안에 또 다른 블록을 생성할 수 있게 한다. 그래서 블록 안정성이 명확하지 않다. 대신, 생성된 블록에서 많이 블록이 쌓일수록 안정성이 높아진다. 검증된 블록이 쌓이기 때문이다. 이러한 이유로, 실시간성 우선 합의 알고리즘은 '확률성(Probability)'을 가진다고 부르기도 한다. 참고로 이러한 합의 알고리즘은 경쟁 방식을 가진다. 블록 생성의 실시간성에 맞춰져 있기 때문에 경쟁 방식을 유도해 블록을 빠르게 생성하게 한다. 또한, 비허가형 블록체인에 적합하다. 경쟁자가 많은 수록 악의 생성자의 블록 생성에 대응할 수 있기 때문이다. 비트코인을 예로 들어보자. 10명의 블록 생성자보다 1만 명의 블록 생성자가 많을수록 1명의 악이 생성자에 대응성이 높아진다. 그만큼 성실한 블록 생성자의 컴퓨팅 파워가 커지기 때문이다.

블록 생성 방식에 따른 합의 알고리즘 구분



[출처: 유성민(2019), 합의알고리즘강의자료(서강대)]

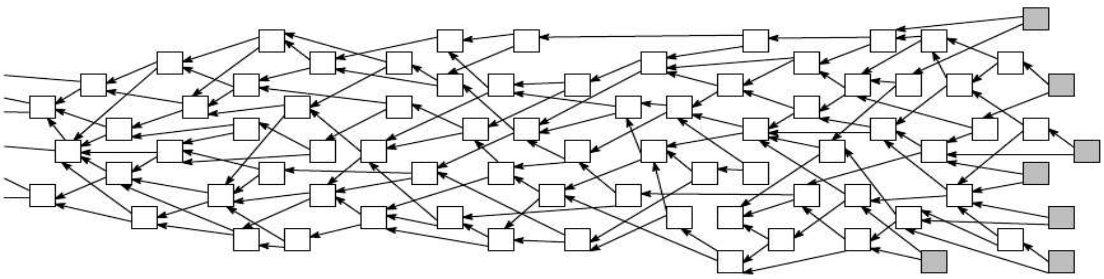
안정성 우선은 생성된 블록의 안정성이 거의 완벽하다. 이미 거의 모든 참여자에 의해서 블록 생성의 동의를 얻었기 때문이다. 따라서 안정성 우선은 '완결성'을 가지고 있다. 포크 발생도 없다. 다만, 비허가형 블록체인에 적용은 어렵다. 안정성 우선은 대다수 생성자에 허락을 받고 블록을 생성한다. 그런데 비허가형은 블록 참여자가 많다. 그럼 블록 생성의 시간이 너무 오래 걸린다. 이러한 이유로, 허가형 블록체인에 적용할 수밖에 없는 한계가 있다. 또한, 안정성 우선은 실시간성 우선과 달리 협력 기반으로 블록을 생성한다. 투표 등의 방식으로 동의를 얻어 블록을 생성하기 때문이다.

이러한 유형에 속하지 않은 합의 알고리즘도 있다. 아이오타(IoTA)에 적용된 블록체인 플랫폼인 탱글(Tangle)이 대표적인 유형이다. 탱글은 블록체인 노드 중에서 거래 생성자가 직접 데이터 블록을 생성하고 검증하게 한다. 합의 방식을 간소화했기 때문에 속도 측면에서는 매우 빠르다. IoTA는 용어에서도 유추할 수 있듯이 사물인터넷(IoT) 서비스 전용 블록체인으로 속도를 우선시 한다. 탱글은 데이터 생성자가 이전 블록 두 개를 최소한으로 증명 받게 한다. 참고로 인정받지 않은 블록을 팁(Tip)이라고 부른다. 탱글은 신규 블록 생성자가 팁의 검증을 유도하도록 가중치 계산법을 적용했다. 해당 계산법은 팁을 검증한 신규 블록 생성자를 우선적으로 검증 받도록 하는 계산법이다.

안정성 우선과 실시간성 우선 합의 알고리즘 비교

구 분	안정성 우선	실시간성 우선
정 의	검증된 블록 생성	블록 생성후 검증
적용 블록체인	BFT 계열	PoW, PoS, DPoS, Ethash 등
블록 안정성	완결성	확률성
포크 발생	X	O
생성 방식	협력적 구조	경쟁적 구조
적합 블록체인 유형	허가형 블록체인	비허가형 블록체인

이전 블록을 검증하는 방식의 탱글 구조



[출처: 위키피디아]

디지털 신뢰 시대의 합의 알고리즘 연구

인공지능은 지능형 혹은 자동화의 대표 기술로 떠오르고 있다. 마찬가지로, 블록체인은 신뢰성과 탈중앙성을 대표하는 유망 기술로 떠오르고 있다. 따라서 디지털 신뢰 시대에는 블록체인 적용이 필수이다. 그런데 블록체인 적용만으로 디지털 신뢰 시대를 구현 했다고 말하기 어렵다. 원천 기술인 합의 알고리즘 연구가 필요하다. 합의 알고리즘 구현에 따라 블록체인 기반의 디지털 신뢰성이 결정되기 때문이다. 따라서 지능형 시대에 기계학습 알고리즘 연구가 필요하듯이, 디지털 신뢰 시대에 합의 알고리즘 연구가 필요하다.

디지털패권 경쟁 속의 화웨이: 유럽과 아시아 국가들의 공조와 일탈

유인태 (ityoo@jbnu.ac.kr)

전북대학교 국제인문사회학부 조교수

미국의 화웨이에 대한 압박이 거세다. 이는 단지 하나의 중국 기업에 대한 것이라기보다는 중국을 기술 패권의 최대 경쟁자로 보는 미국의 시각에서 비롯된다고 할 수 있다. 미국은 동맹국들을 중심으로 중국과 화웨이를 지속적으로 압박하려 들고 있다. 그러나 파이브 아이즈를 비롯한 미국의 주요 동맹국들마저 최대 교역국으로 부상한 중국의 위상을 고려해 이해관계를 따지며 적극적으로 미국에 동조하지만은 않고 있는 양상이다. 우리나라 역시 자국 선도 산업의 육성과 이와 결부된 이익의 측면을 명확히 파악하고, 이에 맞는 외교적 노력을 펼쳐야 할 것이다.

I. 큰 그림에서 화웨이 사태 보기

애초에 화웨이에 대한 '파이브 아이즈(Five Eyes, FVEY)'의 대응은 미국의 이니셔티브에 기인하는 바가 크다. 2012년 미국 하원 정보위원회는 중국의 화웨이, ZTE 통신장비 제조 그룹에 대해 미국 국가안보가 그들의 스파이 활동 그리고 산업첩보활동에 의해 침해될 수 있음을 경고하였고, 이에 따라 이들 회사가 미 정부와의 계약에서 배제되도록 하였다. 이는 미국의 대 중국 위협인식에 기인한다. 2017년 『국가안보전략(National Security Strategy of the United States of America)』에 나타나듯, 중국은 미국의 안보와 주권을 침해하는 경제적 경쟁자로 규정된다.

미국의 대 중국 위협인식은 단순히 트럼프 대통령 그 자신에만 기인한 것이라기보다는 미국 지도자 계층에서 널리 공유된 인식으로 볼 수 있다. 의회에서는 거대 양당에 의해 그리고 국무부, 안보·첩보 관련 부서와 그 외의 기타 부서에서도 공유되고 있다. 그 근거로서 2017년 트럼프 대통령 취임 이후에는 국제무역위원회(USITC), 외국인투자심의위원회(CFIUS), 미국무역대표부(USTR), 상무부, 법무부, 재무부도 화웨이 제품 사용 금지에 가세하고 있다. 나아가 2018년 2월에는 중앙정보국(CIA), 국가안보국(NSA), 국가정보국(DNI), 연방수사국(FBI)을 포함한 6개 미 정보기관 수장들이 미 상원 정보위 청문회에서 해킹 가능성을 거론하며 화웨이와 ZTE 제품을 사용해서는 안 된다고 주장하였다.

이러한 범정부적 인식의 공유는 같은 해 8월 국제적으로 확산되는데, 미국은 파이브 아이즈 회원국을 국제적 확산을 위한 최초의 토대로 삼는다. 미국은 자국의 인식과 행보를 파이브 아이즈 회원국 외에도 특히 군사적 동맹국 혹은 정치외교적 우방국들에게 영향을 미치려고 시도하였다. 이러한 미국의 공조 체제 확산의 노력에, 중국 내부의 법체제 변화가 또 다른 구실을 제공한다. 법체계 변화란 2016년 11월에 중국 전국인민대표대회를 통과한 '사이버보안법(네트워크안전법)' 그리고 2017년 6월에 통과된 첩보 관련의 '국가정보법' 제정이다. '사이버보안법'은 2018년 11월에 새로운 조항들이 추가되며, 기업들의 데이터국지화와 중국 정부의 요구가 있을 경우 암호 해독 정보를 언제든 제공해야 하며, 인터넷 검열과 접속 차단하는 권한을 정부에 부여한다. '국가정보법'은 중국의 전기통신회사들에게 국가의 첩보 활동을 지지하고, 협동하며, 협조할 것을 의무화 하고 있으며, 이 중국의 법안들은 화웨이에 대한 파이브 아이즈의 반대 공조체제 형성의 이유를 한층 더 공고히 하였다.

미국의 화웨이 제재가 단순한 국가의 기업에 대한 제재로만으로 파악되지 않는 이유는, 현재 진행 중인 미·중 간의 통상마찰 때문이다. 이는 미국이 자국 중심의 통상질서를 재편하려는 노력의 일환이지만, 부상하는 강대국 혹은 잠재적 패권경쟁국인 중국이라는 점에서 그 파급력과 함의는 전 지구적이다. 미국 정부는 무역제재를 통해 중국의 기술력을 억제함으로써 중국의 국력 신장에 제동을 걸어 패권경쟁에서 이기려는 의도를 감추지 않는다. 미국은 2018년 4월 4일에 25% 고율관세를 부과할 중국산 제품 1,300개 품목을 발표하면서, 중국이 미래산업 육성을 위해 추진하고 있는 '중국 제조 2025'를 공개적으로 지칭한 바 있다.

이는 중국의 미래 성장 가능성을 주요 공격 대상으로 삼은 것을 숨기지 않은 것이다. 화웨이가 주목을 받는 이유는 바로 미래 성장 가능성의 핵심이 되는 5G 네트워크 기술을 보유하고 있는 회사이기 때문이다.

상기한 바와 같이, 화웨이와 ZTE 부품에 대한 미국의 제재는, 그 자체만 가지고 독립적으로 파악될 수 없고 여러 구조적 요인이 수반되고 있다. 대표적 세 가지 요인은, 첫째, 미국 국내에서의 대중국 인식의 악화와 패권경쟁의식 고조, 둘째, 중국 내에서의 권위주의적 법제도의 개정, 그리고 셋째, 미·중 간의 통상 마찰이 그 구조적 요인들이다. 게다가 미국과 중국이라는 거대한 국가들 간에 일어나는 갈등이기 때문에, 이러한 구조적 요인들은 패권경쟁, '기술전쟁(Tech War)', '무역전쟁(Trade War)'라는 자극적인 용어로 지칭되고, 이들 용어들이 서로 엮이며 교차되어 사용될 수 있는 시기를 불러왔다.

그러나 이러한 전쟁은 과거 냉전 시기에 결속되었던 동맹국 혹은 우방국들 사이 국제정치와는 다른 양상을 보인다. 특히, 화웨이 제재와 관련한 전통적 우방국 혹은 군사 동맹국들 간의 국제공조의 불안정성(아래 표 참조)은 전통적으로 안보로 치중되었던, 혹은 안보 이슈만이 '상위정치(high politics)'였던 냉전시기와는 확연히 구분된다. 2018년까지만 해도 상당 부분 미국의 공조 체제에 동승하는 분위기였지만, 2019년 들어서부터 각국이 차례차례 일탈한다.

화웨이 제제 공조와 동맹의 국제 정치

Alliance Politics On Huawei Ban	Relationships	Changing Policy on Huawei Ban	
		2018	2019
U.K.	Five-Eyes	With U.S.	Partial
Australia	Five-Eyes	With U.S.	With U.S.
New Zealand	Five-Eyes	With U.S.	Partial
Canada	Five-Eyes	Ambiguous	Partial
Germany	Military Alliance	Ambiguous	Partial
Japan	Military Alliance	With U.S.	With U.S.
South Korea	Military Alliance	Ambiguous	Partial

[출처: 저자 작성]

2019년부터의 이런 변화를 어떻게 설명할 것인가. 무엇이 전통적인 동맹정치에서의 응집성과는 다른 이러한 양상을 낳는가. 여러 요인을 생각해 볼 수 있지만, 잠정적으로 5가지 요인을 들 수 있다.

① 불확실성: 미국 전략의 가변성
② 상호의존성: 국가들의 미국과의 (그리고 중국과의) 정치외교적 그리고 통상적 관계
③ 인식의 상이성: 국가들의 중국 위협 인식은 정도의 차이가 있음. 이에는 상호의존성뿐만 아니라, 지역적 근접성의 영향력도 있음

④ 국내의 이해관계 다양성: 국내 이해당사자들이 화웨이 제품을 어느 정도 의존하는가. 그리고 그 행위자들의 정책과정에서의 영향력이 국가마다 다름

⑤ 기업전략이 차이성: 화웨이의 사업 전략 상, 대응 방법이 다름. 시장이 큰 국가들에게는 검증을 제시함

II. 화웨이 사태와 각국의 대응

화웨이 제재를 위한 미국의 국제적 공조체제 구축은 '파이브 아이즈'를 중심으로 전개되었다. '파이브 아이즈'는 군사 동맹을 넘어, 첩보 영역에서도 협력하는 첩보 동맹이기 때문에, 미국에게 있어 그 어느 나라들보다도 가깝게 공조 관계를 유지하고 있는 국가들이다. 이들 국가들을 단초로 국제적인 화웨이 제재 체제를 구축하려고 했던 것은 당연하게 보인다. 더욱이 제재의 이유가, 화웨이 부품을 통한 중국 정부에 의한 국가 기밀의 탈취 및 변경 가능성이었기 때문에, '파이브 아이즈'는 적절한 장(場)이였다.

'파이브 아이즈'를 통한 공조는 2018년 7월의 회동에서부터 비교적 명확히 보이기 시작한다. 7월의 캐나다 노바스코샤에서 회원국들의 첩보 기관들의 장들이 회동한 이후로, 5개 회원국들은 화웨이가 차세대 5G 무선 네트워크 공급 사업에서 배제되어야 한다는 데에 뜻을 같이 하였다(Keall 2018). 그 이후 화웨이에 대한 공조의 분위기가 고조되는 가운데, 파이브 아이즈 내 공조 체제는 2018년 8월 호주 골드코스트의 회동에서 한 차례 더 강조되었다(Barkin 2018). 그리고 이즈음에 전 지구적 공조체제를 촉구하며, 공식적 협조 요청이 독일과 일본에게도 확장되었다.

미국의 화웨이 부품 사용 금지 조치 요구에 대해 우선, 호주 정부가 가장 먼저 동의한다. 그에 이어 뉴질랜드가 대(對) 화웨이 정책에 동승하는 듯 했다. 영국은 초반에는 공조의 자세를 취하다가 2019년에 공조 일탈로 선회했다. 그에 비해 캐나다는 2018년부터 완전한 공조체제에 가담하지 않았으며, 파이브 아이즈 공조체제를 완전히 무시하지 않는 선에서 적당한 협력을 보였으나, 최종 결정을 내리지 않고 유보한 상태였다. 그러나 2019년에는 영국, 뉴질랜드, 캐나다, 세 나라 모두 화웨이 부품의 완전한 배제가 아닌 부분적 허용으로 전환한다. 이하에서는 이들 각국 나라들의 화웨이에 대한 움직임을 상론한다.

1. 호주

2018년 8월 호주 골드코스트 회동시기에, 호주의 턴불 수상은 트럼프 대통령에게 전화하여 화웨이와 ZTE가 호주의 5G에서 제외되었음을 알렸다. 외국 정부로부터 치외법권적인 지침을 받을 수 있는 회사들을 제외한다는 명분에 기인한다. 뒤이어 같은 해 10월에는 호주정보국(Australian Signals Directorate, ASD)의 수장 마이크 버제스(Mike Burgess)가 5G의 중요성을 언급하며 화웨이와 ZTE가 미칠 수 있는 국가안보 우려를 시사했다. 이처럼 첩보기관의 수장이 나서서 공적으로 언급한 경우는 70년간의 기관의 역사에서 유례가 없었던 사건이었다(Beams 2018). 이는 호주가 어느 정도로 미국과 긴밀히 협조하고 있는가를 보여주는 일례를 보인다.

호주의 이러한 중국 기업인 화웨이에 대한 견고한 거부 입장은 호주와 상황이 유사한 여러 나라와 비교해 볼 때, 여러 의문을 낳는다. 우선, 첫째, 호주는 영국, 캐나다 뉴질랜드와 같은 다른 파이브 아이즈 회원국 그리고 독일, 프랑스와 같은 서방 민주주의 선진국이 2019년도에 들어 화웨이 장비 사용을 허가하는 방향으로 선회한 것과 달리 계속해서 화웨이 사용 금지 입장을 견지한다. 나아가, 둘째, 2019년도 말에 되어서는 화웨이 장비 금지의 입장을 견지한 나라는 호주 외에 일본 정도일 정도로 호주에서는 고립에 대한 우려의 목소리도 나온다. 고립은 화웨이 제품을 대체할 마땅한 대안이 없는 경우 곧 5G 경쟁에서의 낙오를 의미할 수 있다. 셋째, 호주는 동남아시아와 지리적으로 가까우며, 중국과도 유럽 우방국들에 비해 상대적으로 가까우며, 중국의 잠재적 위협이 전략상으로 중요한 고려 요인이다. 그럼에도 불구하고, 지리적으로 가까운 동남아시아 국가들, 예를 들어 미국과의 군사동맹국인 필리핀과 태국은 5G 네트워크 장비로 화웨이 제품을 사용하기로 하였다. 넷째, 호주와 중국의 상호의존도는 상당했음에도, 교역의 압박이 작용하지 않은 것으로 보인다. 중국은 호주의 가장 큰 수입국이다. 그리고 석탄은 호주에게 있어 가장 이윤이 남는 수출인데, 중국의 석탄 구입은 호주 GDP의 4%에 육박한다. 중국의 호주에 대한 무역보복이 결코 가볍게 넘겨질 수 있는 사안이 아닌 것이다. 다섯째, 마지막으로, 호주의 경우도 다른 여러 나라의 경우와 같이 이전 기술에 대한 화웨이 의존도가 결코 낮지 않았다. 화웨이가 사실상 4G 네트워크 서비스의 반을 제공하고 있는 상황이기도 했다. 화웨이 금수 결정은 이동통신사(carrier)들이 적응할 시간도 없이 빠르게 결정되었다. 그리고 호주는 2019년 5월부터 텔스트라(Telstra)가 5G 서비스를 개시했고 이미 수만 명의 가입자를 받았다. 호주에서의 화웨이는 그 사업 진입 가능성이 희박해 보이고, 향후 기회를 노리며 기다리는 동안에, 다른 분야, 예를 들어 교통, 광산, 농업 및 교육 쪽으로 관심을 전환하고 있다.

사실상 상기한 여러 상황들이 화웨이 5G 장비 사용으로 전환한 국가들과 유사함에도 불구하고, 호주의 이러한 결정은 어떻게 유지되고 있는 걸까. 2019년의 세계적인 추세에도 불구하고 호주가 화웨이를 배제하고 있는 것을 보면, 미국의 압박만이 아닌 다른 이유가 있을 수 있음을 짐작케 한다. 왜냐하면 다른 모든 나라들도 미국의 압박을 느끼고 있었지만, 전환했었기 때문이다.

사실 호주의 결정은 미국의 압박에 의한 것이 아닐 수 있다. 이를 입증하듯, 오히려 호주의 입장이 보다 더 견고할 수 있는데, 미중무역협상 가운데 화웨이 제품을 카드로 쓰는 미국을 보면, 미국은 오히려 화웨이에 대해 상대적으로 유연한 태도를 보이고 있다. 오히려 미국의 화웨이 제품 금수 공조 체제도 호주에 의해 시작되었을 수도 있다는 주장도 있다. 호주는 미국이 화웨이 제품 금수 공조 체제를 형성하기 위해 본격적으로 움직이기 전에 이미 2011년에 화웨이 제품을 국가 브로드밴드 네트워크 사업에서 제외한 바 있다. 그 금수 조치가 2018년에 백도어 존재 가능성 때문에 5G 네트워크 사업으로 연장되었을 뿐이라 볼 수 있다. 그리고 호주는 미국보다도 더 강력한 제재형식을 취하며, 단순히 정부 네트워크 뿐 아니라 모든 네트워크에서 금지하고 있다. 한때, ASD 수장인 마이크 버제스는 2017년에 핵심과 비핵심 인프라의 차이는 모호해질 수 있다고 언급했다.

이는 영국이 비록 화웨이 부품을 기밀 데이터를 취급하는 네트워크로부터 당장은 떨어뜨릴 수 있다고 하더라도, 장차 떨어뜨리기 어려워진다는 의미이다.

이러한 호주의 정책 방향은 호주의 대(對) 중국 인식 특히 중국 위협을 강하게 느끼는 정책결정자들에 의한 것일 가능성이 크다. 호주의 화웨이 5G 장비 사용 금지는 2018년에 결정이 내려졌는데, 말콤 턴불(Malcom Turnbull) 정권 시기이다. 그는 같은 해 8월에 퇴임하였으나, 그는 국가 첩보 활동을 도와야할 의무가 있는 기업에는 5G 네트워크 사업을 맡길 수 없다는 견해를 가지고 있었으며, 불확실한 세상에서는 대비책(hedge)을 마련해두어야 한다고 피력한 바 있다. 즉, 중국이 현재 평화적으로 보인다고 해서 화웨이에 의존하게 되면 나중에 국가 안보에 큰 위협이 될 수 있다는 의미이다. 그리고 중국에 모든 것을 의존할 수 없으며 5G 장비의 전적인 의존은 피해야 한다는 의미로 해석될 수 있다. 턴불은 중국을 동아시아에서의 지정학적 불안정의 근원임을 그리고 국가안보에의 가장 큰 위협이 될 수 있다고 강하게 의식하고 있었다고 볼 수 있다. 따라서, 화웨이 장비 사용 금지는 여러 나라의 경우, 특히 미국과 가까울 경우, 미국과의 관계에서 비롯되는 압력이 주요 이유로 지목되지만, 호주의 경우 미국의 압박 없이 자체적인 결정의 결과로 볼 수 있다. 실제, 턴불은 중국 기업들과의 거래를 금지하는 것과 관련해서 미국이나 파이브 아이즈의 어느 국가로부터 압력을 받은 적이 없다고 부인했다. 심지어 턴불은 은퇴한 후에도 영국 수상 테레사 메이(Theresa May)에게 화웨이의 위험성을 경고했을 정도이다. 턴불의 후임인 스콧 모리슨(Scott Morrison) 수상도 강경한 우파로서 친미 성향의 대 중국 강경책을 선호하며, 호주의 대(對) 화웨이 정책은 호주의 대(對)중국 정책과 함께 한동안 유지될 것으로 보인다.

물론, 호주 정부의 향후 행방은 어느 정도 중국과의 경제적 관계로부터 영향을 받지 않을 수 없다. 영국의 화웨이 부품의 부분적 도입이, 브렉시트와 결부되며, 상당 부분 화웨이 부품이 가져다주는 경제적 이익을 고려하지 않을 수 없듯이, 호주에게도 중국과의 경제적 상호의존에서 비롯되어 치러야 하는 비용이 호주의 정치인들에게도 압박이 될 수 있다. 그러나 호주는 중국의 무역 영역에서의 대항 조치를 호주의 화웨이 금지와 별개로 인식하여, 화웨이 기업 부품 제재 방침을 유지해 왔으며, 화웨이의 지속적인 탄원에도 불구하고 향후 계속될 것으로 보인다.

2. 뉴질랜드

앞서 언급된 2018년 8월과 10월의 첩보 기간 수장들의 회동을 거쳐, 파이브 아이즈 내에서의 화웨이에 대한 우려가 공유되고, 대응 공조에 대한 논의가 고조되면서, 뉴질랜드의 노동당 정부도 이러한 흐름에 신속히 동승하였다. 단적인 예로, 뉴질랜드는 2018년 호주의 마이크 버제스가 공표한 이후 불과 7일 만에 화웨이가 스파크(Spart New Zealand) 공영 전화회사로 5G 장비 공급을 금지하는 결정을 내렸다. 이 결정은 뉴질랜드의 첩보기관인 정부통신보안국(Government Communications Security Bureau)이 국가 안보상의 이유로 내린 것이다. 이러한 정부통신보안국의 결정으로 스파크는 2018년 11월에 이미 화웨이

장비를 5G 네트워크에 사용할 수 없다고 보았다. 다른 한편, 2019년 2월이 되자, 저신다 아던(Jacinda Ardern) 뉴질랜드 수상은 자국 정부는 아직 절차를 진행 중이며, 스파크가 정보통신보안국의 우려를 불식시킬 수 있다면, 화웨이가 여전히 참여할 수 있다고 언급하였다. 즉, 확정된 결정은 아직 없다고 말하며, 뉴질랜드의 유연한 입장을 수상이 직접 시사 하였다.

뉴질랜드의 정부통신보안국의 결정은 호주의 결정에 이어 공표되었으며, 이러한 결정들의 이면에는 미국의 압박이 있었다. 그러나 동시에, 아던 수상의 언급에서 보이듯, 뉴질랜드 수상의 입장에는 중국과의 관계에서 비롯되는 우려가 작용하였다고 할 수 있다. 즉, 뉴질랜드는 화웨이를 완전히 제외하지 못하고 있는데, 이는 중국과의 깊은 경제적 관계에 기인한다. 중국은 뉴질랜드의 가장 큰 무역국이며, 중국인 관광 유입도 크다. 따라서 화웨이를 금지할 경우, 야기될 수 있는 경제적 보복에 대한 우려가 컸다(Withers 2019). 이를 방증하듯, 뉴질랜드의 화웨이에 대한 입장을 피력한 후에는 수상 자신이 중국과의 어떠한 마찰도 없다는 것을 역설하기까지 하였고, 더욱이 뉴질랜드는 비록 파이브 아이즈 첩보 동맹의 일국이지만, 동맹국과는 상관없이, 즉 미국이나 호주로부터의 압박 없이, 독자적으로 결정을 내린다고 말한다.

수상의 언급은 파이브 아이즈 국가로서 뉴질랜드가 보였던 결속력과는 다르며, 뉴질랜드는 유연한 입장을 취하고 있는 것으로 볼 수 있다. 이러한 뉴질랜드의 입장 변화는 중국과의 관계로부터 많은 영향을 받았다. 뉴질랜드는 중국과의 긴밀한 교역관계를 가지고 있었으며, 이로부터 비롯되는 사회로부터의 압박이 작지 않았기 때문이다. 그리고 같은 파이브 아이즈인 영국의 정책 전환도 호기로 작용했다. 영국도 화웨이를 5G 사업 계획에 포함시킬 수 있다는 가능성은 수상으로 하여금 첩보기관과는 다른 발언을 할 수 있게 하였다. 즉, 뉴질랜드가 놓인 국제 구조적인 제약과 국제 환경의 변화는 기존 2018년의 강경한 뉴질랜드 입장으로부터 2019년의 유연한 태도로의 전환을 가능케 한 것이다.

다른 한편, 화웨이도 영국의 결정이 변화함에 따라 여러 나라에 새로운 제안을 제시하는데, 뉴질랜드에게도 유연한 태도를 주문한다. 화웨이는 2019년 4월에 뉴질랜드가 영국과 같이 제한된 역할이라도 승인할 것을 요구한다. 영국은 화웨이가 5G 네트워크의 핵심 부분에의 참여는 금지하지만 비핵심 부분은 허락하기로 방침을 선회한 것이다. 이러한 방침은 영국 뿐 아니라 독일도 동일했다. 영국과 독일의 이러한 방침은 미국이 화웨이 제품의 스파이행위(espionage) 가능성을 제기하고, 미국과 중국 간에 갈등이 고조하는 가운데 취한 중도노선이라 할 수 있다. 모든 나라가 미국과의 좋은 정치적 관계와, 중국과의 경제적 관계에서 비롯되는 혜택, 양자를 갖고 싶어 하기 때문에, 영국과 같은 종류의 중도노선은 미국의 우방국에 계속해서 확산될 것으로 보인다.

세계적인 흐름과 뉴질랜드의 중국과의 관계 속에서, 화웨이의 사업 가능성은 뉴질랜드의 5G 네트워크 사업에서 다시 부상하고 있다. 스파크는 작년에 화웨이를 베이스 스테이션(base stations)에 유일한 공급자로 전면에 내세운 계획을 세웠지만, 정부는 국가안보를 이유로 이를 거절한 바 있다. 그러나 2019년 11월 18일에 다시 한 번 화웨이를 삼성과 노키아와 더불어 하나의 선호하는 사업자로 지명한 것이다.

이러한 큰 기업의 움직임은 서방 우방국들의 움직임과 뉴질랜드 내에서의 움직임을 반영하는 것으로 볼 수 있다.

3. 캐나다

2018년 12월에는 캐나다에서 파이브 아이즈 회동이 있었으며, 이는 최고위 정보 장관들의 연례 모임이었다. 여기에서는 화웨이를 회원국의 5G 모바일 폰 네트워크 사업 참여에서 배재하기 위해 조율할 것이 결정되었다. 미국의 6개 첩보 기관들의 장은 화웨이를 세계에서 가장 위험한 사이버첩보(cyberintelligence) 위협으로 간주하고, 화웨이의 5G 기술이 원격 스파이, 정보의 탈취와 변형, 그리고 심지어 시스템 셧다운까지 가능할 것으로 보았다(Chase and Fife 2018). 그러나 캐나다의 태도는 미국, 호주 그리고 뉴질랜드와 같이 전면적으로 명백한 금지를 나타내지 않았다. 캐나다 안보정보청(Canadian Security Intelligence Service)의 수장은 국가 지원의 정보탈취행위가 늘어나고 있는 추세는 언급하였으나, 중국을 구체적으로 언급하지는 않았다.

캐나다의 트뤼도 자유당 정권은 2018년 12월 이전까지 다른 파이브 아이즈 구성 국가들과는 달리 화웨이에 대해 결정적 태도를 취하지 않고, 여러 선택지들이 열린 잠정적 상태를 유지하는 자세를 취했다. 예를 들어 2018년 11월까지도 화웨이가 5G 네트워크 모바일 사업에 참여할 수 있는 가능성을 열어 놓았었다. 이런 결정이 캐나다 연방 정보기관인 캐나다 통신보안기구(Communications Security Establishment, CSE)의 권고에 따른 것인 점도 주목해야 한다(Bussoletti 2018). 그 전 10월 달에는 파이브 아이즈, 특히 미국으로부터 캐나다의 화웨이 제품 사용 우려가 표출되었는데, 오히려 스콧 존스(Scott Jones) 캐나다 사이버 안보 센터(Canadian Centre for Cyber Security)장은 캐나다가 화웨이의 위협에 대응할 수 있는 역량이 있음을 강조하였다(Freeze 2018).

그러자 미국 상원의원들이 캐나다 총리에게 캐나다의 5G 네트워크 사업으로부터의 화웨이 배제 청원서한을 보냈다. 이들은 캐나다가 미국과 호주의 선례를 따르기를 촉구했다(Chase and Fife 2018). 당시 호주와 뉴질랜드도 화웨이 사용 금지에 참여하던 상황이었고, 이런 상황은 이미 화웨이 제품을 많이 사용하고 있던 캐나다에 압박이 되었다(Desjardins 2018). 화웨이 제품 사용금지를 택한 국가들은 화웨이 제품에 중국 정부에 의한 '백도어' 설치의 위험을 공유하고 있었고, 만일 캐나다가 화웨이 제품을 사용할 경우, 파이브 아이즈 공조망에 연결되어 있는 캐나다를 통해 중국이 첩보 정보를 빼내어 갈 수 있는 위험이 있었기 때문이다. 캐나다는 첩보 공조에서 배제될 수 있다는 위기를 고려하지 않을 수 없었다.

그리하여 2018년 12월 이후 캐나다는 파이브 아이즈와의 중국 화웨이에 대한 공조체제를 취한다. 그러나 캐나다는 호주나 뉴질랜드에서처럼 화웨이의 5G 네트워크 사업 참여를 금지하지 않았다. 이는 지금까지 취해온 캐나다의 신중한 태도와 배치될 뿐 아니라, 자국의 민간 영역에도 이익이 되지 않기 때문이다. 대신 다른 형태로 공조를 취하는데, 캐나다는 미국의 요청에 따라 화웨이 창업자의 딸이자 최고재무책임자

(Chief Financial Officer)인 멍완저우를 2018년 12월 5일 체포한다. 비록 화웨이는 중국 정부와 공조하여 불법적 감시를 하고 있다고 비난 및 의심을 받고 있긴 했지만, 표면적인 체포의 이유는 북한 경제재제에 대한 위반 혐의 때문이며, 스파이행위(espionage)에 의한 것은 아니었다. 멍완저우의 체포에 보복하듯이 중국 당국도 캐나다 출신 전 외교관과 대북사업가를 체포했다.

캐나다는 미국과 중국으로부터 양쪽의 압박을 받게 되는 상황에서 절묘한 균형을 취할 것을 요구받았다. 미국은 중국과의 첨단 기술 경쟁의 구조 속에서 캐나다를 압박하고 있었으며, 중국은 멍완저우의 체포에 항의하고 나섰을 뿐 아니라, 만일 화웨이가 금지 될 경우 캐나다에 부정적인 결과가 있을 것이라고 강력히 경고했다. 게다가 중국은 중국내 캐나다 주요 인물들을 구류하며, 캐나다에 추가적인 압박을 가했다. 캐나다는 중국에 압박을 받고 있지만 이에 굴하는 자세를 보이고 있지 않다. 멍완저우를 두둔하던 주중캐나다 대사는 공조체제의 강화 맥락 가운데 해임되었고, 멍완저우의 미국 송환절차는 시작되었다. 그러나 2019년 3월까지도 캐나다는 미국의 요구에 호주나 뉴질랜드와 같이 명확히 응하지는 않았다. 캐나다의 중도노선 운영(maneuvering)의 기술을 엿볼 수 있다.

양쪽에서 캐나다에 가하는 압력은 여전하다. 한편으로 멍완저우 체포라는 협조는 미국 하원에서의 결의안('19.10월)에서 보이듯 미국의 찬사를 받는다. 캐나다는 미국과의 범죄인 인도 협약에 의해 체포하였고, 미국은 결의안이라는 당근을 통해, 캐나다의 행위에 간접적인 영향을 미치려고 한다. 다른 한편으로 캐나다는 중국으로부터 여러 보복(위협)을 받아 왔다. 상기한 바와 같이 중국은 캐나다인 2명을 스파이 혐의로 구류하고 그리고 다른 두 명에게 사형을 선고한 바 있다. 그리고 티벳, 위구르, 홍콩의 민주주의 운동과 관련한 캐나다인들은 중국을 지지하는 자들부터 여러 괴롭힘을 당하고 있다. 더욱이 중국은 캐나다에게 두 번째로 큰 교역국가인데, 2019년 3월에 카놀라 반입을, 2019년 6월말에는 캐나다산 돼지고기와 쇠고기 수입을 중단했다. 무역보복의 전체적 규모로는 현재 캐나다의 3.8억 달러에 이르는 농산품들의 수입이 제한되었다('19.11월 기준). 피해를 받은 농부들은 캐나다 총리에겐 국내로부터의 정치적 압박이다.

이런 미국과 중국의 이중 압박 가운데, 영국이 중국 화웨이의 5G 장비 도입 결정을 한다. 이 결정은 파급효과가 있었다. 유럽에서는 독일, 스위스, 네덜란드 등 유럽 주요국도 잇따라 화웨이 장비 도입 의사를 밝힌다. 파이브 아이즈 국가들에게도 그 효과가 있었는데, 뉴질랜드가 2019년 2월 중순 즈음에, 기존의 화웨이 제품 사용 금지 입장에서 선회하여, 화웨이가 들어올 수 있음을 공표하였다. 이어 2019년 5월 캐나다 정부도 화웨이 장비 도입 검토에 들어간 것이다. 캐나다 정부의 이런 입장 결정에는 화웨이의 적극적인 움직임도 있었다.

캐나다가 미국에 의한 화웨이 제재 공조체제를 일탈하게 된 데에는, 유럽 국가들의 움직임도 있었지만, 캐나다의 대(對) 중국 입장과도 관련이 있다. 캐나다 총리 쥐스탱 트뤼도(Justin Trudeau)는 캐나다의 중국에의 관여(engagement) 정책을 계속 지지해온 인물이며, 자신이 중국으로의 특사로까지 파견된 적이 있을 정도로 중국과의 관계를 중시 여겨왔다. 물론 국내적으로 반대 세력이 있으며, 자유당의 중국 경도에

대해 보수당은 비판적이다. 극단적으로 한 인사는 중국과의 완전한 재시작을 요구하기도 했다.

또 다른 일탈을 촉진한 이유로 국내 이해당사자들의 목소리를 들 수 있다. 캐나다의 경우, 다수의 그리고 거대 전기통신회사들로부터 화웨이 제품에 대한 지지가 있었다(Liao 2019). 캐나다의 삼대 전기통신회사 중에, 텔루스(Telus Corp.), 벨 캐나다(BCE Inc.'s Bell Canada)는 이미 화웨이와 상당히 공동 투자한 상황이었고, 로저 통신회사(Rogers Communications Inc.)만이 에릭슨을 주로 사용하고 있었다. 화웨이를 금지할 경우, 노키아나 에릭슨만이 가능하게 된다. 더욱이 미국의 압박 하에서도 화웨이는 캐나다에 지속적으로 연구 개발에 투자하고 있었으며, 이로 인해 새로운 일자리가 기대되고 있었다(Horowitz 2019).

이와 같은 화웨이 기술에 의존도가 높은 대내적 상황은, 화웨이에 유연한 태도로 선회한 다른 나라에서도 유사하게 발견된다. 캐나다와 유사하게 영국의 많은 기업 또한 이미 화웨이 제품을 사용하고 있다. 이런 상황이 영국의 선회에 영향을 미쳤다고 볼 수 있다. 독일 또한 유사하며, 이미 모든 5G 참여 기업들이 화웨이 기술들을 사용하고 있다(Buck 2019).

상기와 같은 조건에서 파이브 아이즈의 또 다른 회원국이자 인접국인 캐나다마저 화웨이 제재 공조에서 빠지는 듯하자, 미국은 캐나다에 새로운 압박을 이어간다. 미국 국가안보고문 로버트 오브라이언(Robert O'Brien)이 2019년 11월 23일 캐나다의 화웨이의 5G 장비 사용을 경고하였고, 만일 사용할 경우 캐나다와 미국의 정보 공유를 허가하지 않겠다고 밝혔다. 국가안보고문은 미국의 동맹국이 트로이목마인 화웨이 5G 통신 네트워크를 들이면 정보 공유에 영향을 받을 것이라고 언급하면서, 미국의 화웨이에 대한 인식을 단적으로 드러내었다. 이에 대해 캐나다 국방부 장관인 하진 싸쟌(Harjit Sajjan)은 화웨이 도입 여부 결정까지는 더욱 많은 시간을 소요할 예정이며, 캐나다의 통신업체가 서로 다른 의견을 갖고 있는 상황에서 벨캐나다(BCE)와 텔러스(Telus)는 화웨이 장비를 금지하는 것은 5G 네트워크 발전에 영향을 준다는 입장이지만, 오타와 정부가 최종 결정을 내리기까지는 5G 계획을 잠정 보류키로 했다고 언급하였다. 벨캐나다(BCE)와 텔러스(Telus)는 화웨이의 4G 장비를 사용하고 있으며, 화웨이의 5G 장비 도입을 금지할 경우 막대한 장비 교체 비용 등을 우려하고 있다.

캐나다는 화웨이의 5G 모바일 네트워크 사업 참여 가능 여부에 대해 결정을 계속해서 유보하여 왔으며, 특히 2019년 10월 21일에 있었던 연방선거 이후로 연기해 왔다. 그러나 아직 캐나다 정부의 결정은 내려지지 않았다('19.12.1 기준). 이는 앞서 언급한 바와 같이 미국의 입장이 확고하지 않으며, 발표하기에 정치적 부담감이 가장 적은 적기를 기다리고 있기 때문이다. 영국이 2020년에야 결정을 내릴 것이라 예상되기 때문에, 국내 정치 상황을 고려하며 비슷한 시기에 내려질 것으로 예상된다.

요약하자면, 캐나다는 미국과 거리를 조절하며 화웨이에 대한 입장을 견지해왔다. 캐나다는 사이버 안보 영역에서 민주적 절차의 수호라는 가치를 내걸고 연합 형성에 이니셔티브를 취하였다. 더욱이 영국과 독일 그리고 뉴질랜드의 선회로 인해 캐나다를 향한 미국의 압박은 경감되었다. 이러한 화웨이에 대한 캐나다의

정책에는 국내 이익단체들의 지지도 존재했다. 따라서 캐나다가 견지해온 미국과 중국 간의 미묘한 균형 감각과 조심스러운 국익 추구 외교 노선은 유지될 것으로 보인다.

4. 영국

2019년 2월 18일에 영국의 국가사이버보안센터(National Cyber Security Center, NCSC)가 중국 통신 장비업체 화웨이 제품을 차세대 통신망인 5G 네트워크에서 사용하는 데 따른 보안 리스크가 관리 가능한 수준이라고 판단을 내린 것이 알려지면서, 반(反) 화웨이 공조 체제에 금이 가기 시작했다. 정보기관 MI6 수장도 영국이 화웨이에 대해 미국보다 유화적인 조치를 취할 수 있으며, 각국은 문제 해법을 모색할 주권을 가지고 있다고 언급하기도 했다. 이 당시 미국은 이미 정부부처에 화웨이 장비 사용을 금지한 상황이었으며, 호주와 뉴질랜드도 정부 차원에서의 장비 배제를 선언했었고, 프랑스와 독일은 '주의해야 한다'는 경고를 내놓으며 신중한 입장이었다.

이에 화웨이의 안정성 검사를 위해 영국에서는 화웨이의 소프트웨어 기술력과 보안성을 검사하는 기관인 '화웨이 사이버 보안 평가 센터(Huawei Cyber Security Evaluation Centre, HCSEC)'를 설립한다. 여기서 3월 말에 보고서를 내놓는데, 이에는 화웨이 제품의 기술적 결함을 우려하는 내용이 담겨져 있었다. 그러나 정치적 판단은 포함되지 않았다.

4월 중순이 지나자 영국 5G 망 구축 사업에 화웨이가 참여하는 것이 명확히 보도된다. 테레사 메이 수상이 화웨이가 영국 망 중 비핵심 부분 구축 작업에 참여하도록 허락하는 문건에 서명한 것이다. 이 결정은 4월 23일 영국 국가안전보장회의에서 내려진 것이며, 수상은 이 회의의 의장이다. 즉, 메이 수상과 장관들에 의해 내려진 정치적 결정이며, 정보 부처나 국방부는 여전히 국가안보 차원에서 회의적이었다. MI6 수장은 안보적 위협을 계속해서 언급하였으며, '데일리 텔레그래프'에 국가안전보장회의에서의 합의 내용을 유출한 것으로 해임된 윌리엄슨 국방장관도 이를 반영한다. 미국의 최우방국인 영국이 선회하면서 '반 화웨이 전선'은 붕괴로 향한 연쇄 일탈이 일어났다는 것은 상기한 바와 같다.

이렇게 여러 나라들이 동맹국 미국에 반대하면서까지 그리고 잠재적으로는 외교·안보에서의 관계 악화까지 감안하며, 기존의 입장에서 선회하여 화웨이에 대해 유화적인 태도로 바뀔 수 있었던 것은 국내적인 이유도 있다. 즉, 영국 내 관련 이해당사자들의 화웨이 제품에 대한 수요가 있었고, 이들의 목소리가 작용했기 때문에, 정부로서도 외부의 압박에 대항할 수 있었던 면도 있다.

현재 화웨이 5G 사용의 임시적 허용은 영국은 12월 12일 선거 이후로 화웨이에 대한 최종적 결정을 내리기로 연기했으나 정치적 혼란 가운데 2020년까지 연기할 가능성이 크다. 보리스 존슨 수상은 5G 네트워크에서 논쟁적이지 않은 부문에 화웨이 제품을 허용할 것임을 언급한 바 있다('19.11.19.) 이는 테레사 메이 전 수상의 입장을 그대로 계승한 것이다. 두 수상에게 정치적으로 불안정한 시기에 최종적 결정을 내리기에는 정치적 부담이 크게 작용했을 것이고 판단을 유보하는 정무적 판단이 현재의 잠정적 허용으로

귀착된 것으로 볼 수 있다. 잠정적 허용도 부분적 허용을 수용했다. 즉, 2019년 4월에 기존의 화웨이에 대한 “전면 금지(blanket ban)”를 통한 미국과의 견고한 공조체제에서 선회하여, 화웨이 제품이 차세대 모바일 네트워크의 핵심 부분을 공급하는 것은 제한되지만, 그 밖의 ‘에지(edge)’에는 부품을 공급할 것을 허용하였다.

5. 유럽연합, 독일, 프랑스, 러시아

유럽연합(EU)은 영국보다 약간 앞서 2019년 3월에, 화웨이 장비 사용을 막아달라는 미국 요청을 무시할 것이라는 의사 표명을 하였다. 앤드루스 안십 EU 디지털 부문 총괄 책임자는 이 같은 내용의 권고안을 제출하였다. 권고안은 회원국에 법적인 강제력이 없지만, EU 회원국들의 정책 방향에 중요한 잣대가 된다.

독일은 2019년 4월 중순 즈음에 5G 이동통신망 구축 사업에서 화웨이를 포함시킬 것을 명확히 하였다. 미국은 유럽연합의 맹주국인 독일에게도 화웨이를 배제하지 않을 경우 기밀 정보 제공 등 군 통신선 단절로 경고한 바 있다. 그럼에도 독일은 가격 경쟁력과 기술력을 확보한 화웨이를 배제할 경우, 이미 상당히 뒤쳐진 무선망 사업에서 뿐 아니라, 차세대 디지털 네트워크 구축 사업에서까지 크게 뒤처질 수 있다고 판단하여, 기존 입장에서 선회하였다. 그 뿐 아니라 미국과의 관계도 어느 정도 영향을 미친 것으로 볼 수 있다.

프랑스도 독일과 마찬가지로 화웨이를 배제 않기로 했다. 2019년 11월 26일 프랑스 재정경제부의 아녜스 파니에뤼나셰 정무차관은 이와 같은 내용을 방송 인터뷰에서 다시 한 번 확증했다.

러시아는 2019년 6월, 5G 개발에 중국의 화웨이와 손을 잡기로 하였다.

6. 일본, 한국, 인도

일본은 2018년 12월 화웨이와 ZTE를 정부의 5G 제품 조달 과정에서 제외하면서, 미국 그리고 호주와 뉴질랜드와 보조를 같이 했다. 그러나 화웨이는 이미 민간 부문에서는 KDDI Corp.와 NTT Docomo의 네트워크 장비에 부품들을 제공하고 있었다. 2019년 6월 일본에서의 G20은 2010년 이후 처음으로 중국 정상의 일본 방문이 이루어진 행사이기 때문에 변화가 있지 않을까하는 예측들이 있었지만, 일본의 입장은 그 이후로도 변화하지 않았다.

한국은 두 개의 가장 큰 모바일 사업자 SK텔레콤과 KT는 초기 5G 네트워크에 있어 화웨이 장비를 사용하지 않았다. KT는 2018년 2월 평창올림픽 때 화웨이의 도움 없이 5G를 선보인바 있다. 2019년 4월에는 삼성이 5G 기술이 내장된 세계 최초의 모바일 스마트폰을 내놓기도 하였다. 그러나 LG유플러스는 네트워크에 화웨이 기술을 포함하였다. 동 회사는 2018년 10월 26일 국회에서 열린 과학기술정보통신부 종합감사에서는 화웨이의 5G 장비를 도입 예정이라고 밝힌 바도 있다.

한국 정부는 2018년 불명확했던 화웨이 기업 부품사용에 대한 정부 방침을, 2019년도에 어느 장비를 쓸 것인지는 개별 회사에 달려 있다고 밝힘으로써 화웨이 기업에 대한 입장을 정리했다고 할 수 있다. 2019년 2월부터 보인 유럽과 동남아시아에서의 화웨이 배제 거부는 한국 기업 및 정부의 화웨이 장비 사용에 부담을 덜어 주었다.

인도는 가입자 수로 보면 세계에서 두 번째로 가장 큰 전기통신(telecom) 시장이지만 전통적으로 새로운 기술을 받아들이는 데에는 속도가 늦다. 45 퍼센트의 모바일 사용자가 2019년 2월 기준으로 3G나 4G를 사용 중이며, 대부분의 사람들이 2G를 여전히 사용하고 있다. 전문가들은 5G는 2023년에야 대중적인 사용이 이루어질 것이라 본다. 이 와중에 인도의 화웨이에 대한 입장은 아직 미정이며('19.4월 기준), 화웨이를 포함해서 노키아, 에릭슨, 삼성 등을 5G 테스트에 초대했다.

그러나 인도는 기본적으로 중국 제품에 대한 불신이 있으며 이는 과거 경험에서 비롯된다. 2010년에는 국가 안보의 우려에서 중국 전기 통신 장비를 금지한 바 있으며 2014년에는 화웨이가 국영 전기통신 네트워크 회사인 Bharat Sanchar Nigam를 해킹했다는 주장에 대해 조사를 개시한 바 있다. 2018년에는 이미 화웨이의 장비 진입이 금지되어 있는 상태였다. 그러나 최근 보도에 따르면 인도 정부도 브라질 정부와 함께 순전히 경제적으로 고려할 때 화웨이 장비 구매를 배제할 이유가 없다는 입장을 밝힌 바 있다.

7. 태국, 필리핀, 말레이시아

대부분의 동남아시아 국가들은 미국의 우려를 공유하지 않는 분위기이다. 태국은 2020년까지 화웨이 주도의 5G 서비스를 내놓기를 희망하며, 이미 화웨이와 합작 연구를 수행하고 있다. 필리핀도 마찬가지로 5G 네트워크 장비로 화웨이 제품을 사용하기로 하였다.

화웨이는 2019년에 태국 최대 이동통신사업자 AIS(Advanced Infor Service)와 그리고 필리핀의 글로브 텔레콤과 5G 계약을 체결하였다('19.10월 기준). 그리고 싱가폴의 M1 서비스, 말레이시아의 맥시스(maxis), 인도네시아의 텔콤셀(Telkomsel)은 모두 화웨와 시험 서비스를 하기로 계약했다('19.4월 기준). 캄보디아 주요 이동통신사들도 모두 중국의 화웨이 장비로 5G 네트워크를 구축할 계획이며, 2019년 4월에는 화웨이와 5G 인프라 개발 협력 협약을 체결한 바 있다.

그러나 오직 베트남만이 중국 화웨이를 배제할 것으로 알려진 가운데, 자체 장비 개발에 나설 뿐 아니라 에릭슨과 노키아와 협력을 할 예정이다. 이러한 베트남의 방향은, 중국과의 갈등 특히 남중국해에서의 긴장과 베트남의 미국과 안보 및 경제 관계를 강화하고 싶은 선호하고도 관련이 있어 보인다. 베트남 최대 통신사 비엣텔은 베트남 군부가 운영한다. 비엣텔은 4G 서비스에서도 화웨이 제품을 사용하지 않았었다.

Ⅲ. 향후 전망

미국과 중국과의 1차 무역 협상이 연내에 마무리가 지어지지 않을 수 있는 가능성이 언급되는 가운데, 그와 연관된 미국의 화웨이 입장은 계속 견지될 것으로 보인다. 이는 미국의 화웨이 제재 공조체제의 압박이 특히 동맹국들에게 계속적으로 있을 것으로 예상할 수 있다. 이런 거시적 맥락에서, 화웨이에 대한 각국의 입장은 지금 현 상황 유지가 지속될 것으로 보인다. 물론, 미국의 대외정책 방향성이 급격히 선회하거나, 화웨이 부품의 치명적 위험성이 발견되지 않는다는 전제에서이다.

거시적인 맥락에서 현재 상황이 당분간 연기될 것으로 보이지만, 각국의 국내 상황을 보아도, 불안한 시기를 겪고 있는 나라들은 특히 현 잠정적 상황의 연장이 불가피하다. 영국과 같은 나라가 대표적인 경우이다. 브렉시트라는 초유의 상황을 놓고, 더 이상의 불안정을 야기하는 사항에 대해 결정을 내리기 어려운 상황이다. 다른 동맹국들도, 영국의 결정을 기다리고 있다. 영국의 최종 결정이 그들의 정치적 결정의 부담을 덜어줄 수 있기 때문이다. 즉, 현재 최종 결정을 유보하고 있는 동맹국들은, 미중 무역협상에 촉각을 세우는 한편, 자국의 정치적 상황에 따라, 최종 결정을 내릴 적절할 시기를 노리고 있다. 화웨이 부품이 가지는 안보상의 성격 때문에, 최종 결정에는 정치적 부담이 따르기 때문이다. 그러나 최종 결정을 내리기 전에는 현재와 같은 잠정적 허용 방침이 지속될 것이며, 새로운 큰 문제가 대두되지 않는 한, 현 방침이 고착될 가능성이 커 보인다.

한국은 어떻게 해야 하는가. 화웨이 사태는, 미중의 기술패권 다툼의 맥락에서 벌어지고 있다는 것을 이해해야 한다. 화웨이 제품의 실제 기술 보안적 문제는 이미 부차적인 문제가 되는 양상을 보아도 이를 알 수 있다. 선도 산업 분야의 기술과 표준 세우기, 그리고 이와 연결된 경제적 이익이 미국에게 중요하기 때문에, 화웨이 사태는 국제정치적 논란이 되고 있다. 한국은 미국이 중국과 선도 부문에서의 우위를 걸고 싸우고 있는 화웨이 사태의 민감성을 잘 파악하고, 조심스럽게 향후 행보를 정해 나갈 필요가 있다. 한국은 자국 선도 산업의 육성과 이와 결부된 이익의 측면을 명확히 파악하고, 이에 맞는 외교적 노력을 펼쳐야 할 것이다.

[참고 문헌]

유인태. 2019. 캐나다 사이버 안보와 중견국 외교: 화웨이 사례에서 나타난 안보와 경제·통상의 딜레마 속에서. 문화와 정치. 6(2):263-298.

Barkin, Noah. 2018. “Exclusive: Five Eyes intelligence alliance builds coalition to counter China.” https://www.reuters.com/article/us-china-fiveeyes/exclusive-five-eyes-intelligence-alliance-builds-coalition-to-counter-china-idUSKCN1MM0GH (accessed 2019/03/27).

Bauman, Zygmunt et al. 2014. “After Snowden: Rethinking the Impact of Surveillance.” International Political Sociology. 8(2): 121-144.

Beams, Nick. 2018. “‘Five Eyes’ Intelligence Agencies Behind Drive Against Chinese Telecom Giant Huawei.” https://www.globalresearch.ca/five-eyes-intelligence-agencies-behind-drive-against-chinese-telecom-giant-huawei/5662933 (accessed 2019/03/27).

Buck, Tobias. 2019. “German Regulators Syas Huawei Can Stay in 5G Race.” https://www.ft.com/content/a7f5eba4-5d02-11e9-9dde-7aedca0a081a (accessed 2019/06/03).

Bussoletti, Francesco 2018. “All Five Eyes countries, except Canada, ban Huawey over security fears.” https://www.difesaesicurezza.com/en/cyber-en/all-five-eyes-countries-exept-canada-ban-huawey-over-security-fears/ (accessed 2019/03/27).

Chase, Steven and Robert Fife. 2018. “U.S. senators urge Trudeau to block Huawei from 5G.” https://www.theglobeandmail.com/politics/article-us-senators-urge-trudeau-to-block-huawei-from-5g/ (accessed 2019/03/27).

Desjardins, Lynn. 2018. “Huawei ban in Australia increases pressure on Canada.” http://www.rcinet.ca/en/2018/08/24/china-telecom-giant-spy-concern/ (accessed 2019/03/27).

Freeze, Colin. 2018. “Ottawa’s top cybersecurity official: Canada has ‘layers’ to protect against Huawei threat.” https://www.theglobeandmail.com/canada/article-ottawas-top-cybersecurity-official-canada-has-layers-to-protect/ (accessed 2019/03/27).

Horowitz, Julia. 2019. “Huawei Is Growing in Canada Despite Pressure There.” https://edition.cnn.com/2019/02/21/business/huawei-canada-hiring/index.html (accessed 2019/06/03)

Liao, Rita. 2019. “Canada’s Telus Says Partner Huawei si ‘Reliable’.” https://techcrunch.com/2019/01/20/telus-backs-huawei/ (accessed 2019/06/06).

Whithers, Trace. 2019. “New Zealand Syas China’s Huawei Hasn’t Been Ruled Out of 5G.” https://www.bloomberg.com/news/articles/2019-02-18/new-zealand-says-china-s-huawei-hasn-t-been-ruled-out-of-5g-role (accessed 2019/03/23).

주요국 사이버 공급망 위협관리 정책 동향 및 시사점

김소선 (ssosuny@korea.ac.kr)
고려대 정보보호대학원
사이버보안정책센터 책임연구원

1. 서론

공급망(Supply Chain)은 제품이나 서비스를 고객에게 제공하는 과정에서 조직, 자원, 인력, 정보 등에 대한 전반적인 시스템을 의미한다. 정보통신기술(ICT) 제품의 생명주기와 비교하면 수요자의 요구사항에 따라 S/W 및 H/W를 설계한 후 개발업체 또는 제조업체를 통해 개발하고, 배포(Distribution), 획득(Acquisition) 및 배치(Deployment), 운영 및 유지보수, 파기 과정을 거치게 되는데, 이러한 공급망에 침투하여 사용자에게 전달하는 S/W 또는 H/W를 변조하는 공급망 공격이 지속적으로 발생하고 있다. 국내·외에서 발생한 공급망 공격을 살펴보면, 공격자는 S/W 업데이트 서버나 상대적으로 보안이 취약한 개발업체의 개발환경에 침투하여 정상적인 S/W를 변조하여 악성코드를 유포하는 사례가 많았다.

그러나 최근 ICT 글로벌 공급망이 복잡해지고, 화웨이·ZTE 등 중국 장비에 대한 보안 우려가 높아지면서 주요국에서는 정부차원 또는 산업 분야별로 S/W 및 H/W, 서비스를 포함한 사이버 공급망 위험관리 방안을 마련하고 있다. 국내에서는 국가·공공기관이 정보보호시스템 및 네트워크 장비 등 보안기능이 있는 IT제품을 도입하는 경우, 도입 대상제품이 CC 인증 등 사전 도입 요건을 만족하였는지를 확인하고 검증이 필요한 제품에 대해서는 보안적합성 검증을 신청하여 미비한 점이 발견되면 조치 후에 제품을 운용한다. 민간 분야의 경우에는 S/W나 정보시스템 개발·구축단계에서의 보안위협을 최소화하기 위한 보안활동이 정의되어 있으며, 주요정보통신기반시설 취약점 분석·평가, 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 등에서 외부자 보안, 정보시스템 도입 및 개발보안 등에서 개별 제품 중심의 보안대책을 요구하고 있다. 그러나 이와 같은 보안관리체계는 5G, IoT 기기, 클라우드 서비스 등 모든 ICT 제품과 서비스를 포함하여 전반적인 공급망 위험을 관리하기에는 한계점이 있다.

따라서 본고에서는 사이버 공급망 위험관리(Cyber Supply Chain Risk Management, 이하 C-SCRM)를 IT/OT 제품 및 서비스를 안전하게 공급하기 위해 공급망에서의 발생 가능한 위험을 식별하고 평가·완화하는프로세스로 정의하고, 미국과 일본을 중심으로 정부기관 및 산업 분야별 사이버 공급망 위험관리 정책 동향을 살펴본다. 또한 주요국의 공급망 보안 관련 지침 분석을 통해 C-SCRM의 주요 활동을 파악하여 사이버 공급망 위험관리체계 수립 시 고려사항 등을 도출하고자 한다.

2. 주요국 사이버 공급망 위험관리(C-SCRM) 정책 동향 분석

(1) 미국

미국 정부는 2008년부터 사이버보안 관련 국가계획·전략, 대통령 행정명령 등에 따라 연방정부기관 중심의 정보통신기술 공급망 위험관리(ICT SCRM) 정책을 추진하였다. 즉 연방정부기관이 관리하는 S/W 및 H/W를 포함한 모든 ICT 제품과 서비스의 전 생명주기를 대상으로 공급망의 무결성을 확보하기 위한 위험관리체계를 구축하는데 초점을 맞추었다. 또한 ICT 공급망 위험을 제품의 무단 생산, 변조, 도난, 악성 S/W 및 H/W 삽입, 제조 및 개발 보안실무 미흡 등으로 지정하고, 시스템 통합구축 사업자(System Integrator), 공급자(Supplier), 외부 서비스 제공자(External Service Provider) 등 공급망 관계자를 포함하여 공급망 위험을 완화하는 절차와 방안을 마련하고자 하였다. 따라서 연방정부는 먼저 계약에 따라 정부기관의 정보에 접근·처리하는 민간 등 공급자들을 대상으로 조달 요건을 강화하고, 미 국방부(DoD)는 조달계약 참여업체에게 관련 보호지침 준수를 의무화하고 있다.

〈표 1〉 미국 사이버 공급망 위험관리 정책의 주요 현황

구분		주요 내용
공공 부문 (연방 정부)	CNCI[1] ('08)	▪ 글로벌 공급망 위험관리를 위한 다방면의 접근방식 개발 (CNCI #11) - NIST IR 7622('12) ⇒ NIST SP800-161('15) (연방정부기관 SCRM 실무)
	OMB Circular A-130('16)	▪ 연방정부기관은 NIST SP800-161에 따라 공급망 위험관리 계획 수립
	EO-13556 ('10)	▪ 연방정부와 계약을 체결한 민간 등 공급자들이 처리하는 CUI(Controlled Unclassified Information)[2] 에 대한 정부차원에서의 보호 프로그램 실시 - NIST SP800-171 Rev.1('16) (민간 등 비연방기관에서 처리하는 CUI에 대한 보호지침)
	EO-13833 ('18)	▪ 정부기관의 CIO에 IT 투자와 조달에 관한 책임 부여
	국가사이버 전략 ('18)	▪ 연방정부의 공급망 위험관리 향상 - 공급망 위험관리 프로세스, 공급망 위협정보 공유, 공급망 위험이 있는 벤더사 및 제품, 서비스 배제 등
	EO-13873 ('19)	▪ 정보통신기술 및 서비스 공급망 확보 - 국가안보에 위협이 되는 특정 기업의 정보통신기술과 서비스에 대해 미국 정부 및 기업에서도 취득·설치·거래 및 사용 금지
민간 부문	S/W	▪ SAFECode for S/W Supply Chain Integrity Papers
	IT/OT	▪ Open Trusted Technology Provider ▪ ISO/IEC 27036 (공급자와의 관계에서의 보안요구사항) ▪ IEC 62443-2-4 (IACS[3] 서비스 제공자에 대한 보안요구사항)
	전력	▪ NERC CIP-013-1 공급망 위험관리 ▪ APPA[4] & NRECA[5] 공급망 위험관리 시 고려사항 및 모범사례
민·관 협력	주요기반시설	▪ NIST Cybersecurity Framework(NIST CSF) Ver.1.1 - ID.SC(공급망 위험관리): 조직의 우선순위, 제약사항, 위험허용도 등을 고려하여 공급망 위험을 식별 및 평가, 관리하는 프로세스를 마련
	ICT	▪ CISA 산하 ICT SCRM Task Force - 정부와 산업계 간의 양방향 공급망 위험정보 공유를 위한 공통된 위험관리 프레임워크 개발 - ICT 공급 및 제품, 서비스의 위협을 식별·평가하기 위한 프로세스와 기준 수립 - 적격 입찰자 및 제조업체 목록을 작성하기 위한 업계와 평가 기준 수립 - OEM 또는 공인된 판매업자로부터 ICT 구매 장려, 위·변조된 ICT 조달을 방지하기 위한 정책 권고안 작성

민간 부문은 산업계 또는 ISO/IEC 등 국제표준 단체를 중심으로 S/W, IT/OT 등 개별적으로 지침을 개발하거나 관련 표준을 제정하고, 공급망의 무결성과 신뢰성을 확보하고자 노력하였다. 예를 들어, 민간

1) Comprehensive National Cybersecurity Initiative
2) CUI는 비기밀등급(Unclassified Information) 정보 중에서 관련 법률, 규정, 정부 정책에 따라 반드시 보호해야 하는 정보를 말함
3) Industrial Automation and Control System
4) American Public Power Association
5) National Rural Electric Cooperative Association

IT 벤더사는 ICT 제품 및 클라우드 서비스를 포함하여 수요기관과 공급자 간의 보안요구사항을 규정한 국제 표준인 ISO/IEC 27036을 도입하였다. 또한 전력 분야의 경우에는 전력산업의 규제기관인 '연방에너지규제위원회(FERC[6])의 지시에 따라 공급망 위험관리 기준 개발이 시작되었는데, SW 무결성 및 진정성(Authenticity), 공급자의 원격접근 관리, 정보시스템 계획, 공급자 위험관리 및 조달 통제 등을 고려할 것으로 요구하였다. 이에 따라 NERC[7]에 대규모 전력시스템(BES[8]) 운영과 관련된 ICS의 H/W, S/W, 컴퓨팅 및 네트워크 서비스에 대한 공급망 위험관리 기준을 개발하고, FERC는 해당 기준을 전력 C-SCRM 표준(CIP-013-1)으로 채택하였다. 이와 같이 민간 부문의 ICT 공급망 위험관리 정책은 전력 등 일부 분야를 제외하고는 정부기관이 직접 개입하기 보다는 민간 시장에서의 자발적인 참여에 의해 추진되었음을 알 수 있다.

그러나 미국 의회에서 중국 정부가 화웨이 등 자국의 통신장비에 설치된 백도어를 이용하여 스파이 활동을 하고 있다는 의혹을 제기하면서 트럼프 정부에서는 ICT 공급망 위험이 국가 안보는 물론 민간 부문에도 심각한 위협이 될 수 있다고 간주하였다. 2018년 발표된 국가사이버전략을 살펴보면, 연방정부 기관의 사이버보안 강화를 위해 공급망 위험관리 향상을 우선 추진과제로 언급하고, 조달 및 위험관리 프로세스 상에 공급망 위험관리 포함, 공급망 위협에 대한 정보공유, 공급망 위험이 있는 벤더사·제품·서비스는 배제하도록 하는 등 공급망의 투명성 확보 및 위험관리에 대한 책임이 강조되었다. 또한 정부기관은 산업계와 ICT SCRM TF를 구성하여 민·관 공동으로 ICT 공급망 위험관리 방안을 마련하기 위한 활동을 시작하였고, 이후 EO-13873을 통해 미국 정부기관은 물론 기업에서도 특정 기업이 설계·개발·제조·공급하는 정보통신기술과 서비스에 대해 취득 및 설치·거래·사용을 금지하면서 국가 안보 차원에서 민간 부문의 ICT 공급망 위험관리 활동에 정부기관이 개입하기 시작한 것을 알 수 있다.

(2) 일본

일본 사이버 공급망 위험관리 정책은 크게 정부기관의 IT 제품 및 서비스에 대한 공급망 보안과 4차 산업혁명 정책 기조인 'Society 5.0' 및 'Connected Industries[9]' 실현과 연계하여 민간 산업분야의 사이버보안 강화 정책으로 구분할 수 있다.

6) Federal Energy Regulatory Commission
7) North American Electric Reliability Council
8) Bulk Electric System
9) 제4차 산업혁명으로 일본 산업의 목표로 IoT 등에 의해 다양한 사물이 연결되고, 고객이나 사회의 과제해결에 도움이 되는 새로운 부가가치를 창출하는 산업사회를 의미함

<표 2> 일본 사이버 공급망 위험관리 정책의 주요 현황

구분		주요 내용
공공부문 (정부기관[10])	▪ IT 제품 또는 서비스의 조달방침 및 절차에 관한 합의[11]('18)	▪ 23개 정부기관은 정보시스템·기기·서비스 조달 시의 발생 가능한 공급망 위험에 사전 대응 (IT 종합전략실 및 NISC에 검토·자문 요청)
민간부문	▪ 제2차 사이버보안전략('18) ▪ 산업사이버보안 강화를 위한 이행계획(Action Plan)('18)	▪ 사이버-물리 보안대책 프레임워크(CPSF) 수립 및 분야별 대응 구체화, 국제화 추진 (경제산업성) ▪ 공급망을 공유하는 ASEAN 국가의 사이버보안 역량 강화 지원 (미국과 연계하여 공동 훈련 추진, 경제산업성) ▪ 사이버-물리 보안에 관한 연구개발 추진 (내각부, 총무성, 경제산업성) ▪ 정부기관 및 산·학 연계를 통해 공급망 위험에 대응하기 위한 기술검증체계 방안 마련 (내각관방) ▪ 중소기업 사이버보안대책 촉진 (내각관방, 총무성, 경제산업성) - 중소기업 대상 사이버보안대책 사례 등 가이드라인 개발, 사이버보험 활용, 사고 발생 시 지원, 인센티브 제공 등 보안투자 촉진

먼저, 공급망 위험을 정보통신기장비 등 개발이나 제조 과정에서 정보탈취·파괴, 정보시스템의 정지 등 악의적인 기능이 삽입되거나 도입 이후에도 운영·유지보수 과정에서 공급자의 프로그램 등으로 인해 비인가변조가 발생할 수 있는 가능성으로 정의하고, 사이버보안전략을 통해 공급망 위험에 관한 대책 수립의 중요성을 언급하였다. 또한 정부기관의 정보보호 대책 수립 가이드라인[12]을 살펴보면, 개발 또는 조달 과정에서 악의적인 기능이 포함될 우려가 있는 기기와 공급망 위험 발생 우려가 있는 기업의 장비들을 도입하지 않도록 규정하고 있다. 그러나 일본 정부는 정부기관들이 공급망 위험에 대해 보다 적극적으로 대응하도록 총 9종의 정보시스템 및 기기, 서비스[13]에 대한 조달 절차를 강화하였다.

10) 내각관방, 내각법제국, 인사원, 내각부, 궁내청, 공정거래위원회, 개인정보보호위원회, 경찰청, 금융청, 소비자청, 부흥청, 총무성, 법무성, 외무성, 재무성, 문부과학성, 후생노동성, 농림산업성, 경제산업성, 국토교통성, 환경성, 방위성, 회계감사원

11) IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ

12) 政府機関等の対策基準策定のためのガイドライン(平成30年度版)の解説 (遵守事項5.1.2(1)(a))

13) ① 통신회선장치(허브, 스위치, 라우터(VPN 등 서비스 통합형 포함), FW(FW, WAF), IDS, IPS, UTM), ② 서버장비(메일 서버, 웹 서버, DNS 서버, FW 서버, DB서버, 인증 서버, 관리서버(AD 서버 등), Proxy 서버, NAS(Network Access Server)), ③ 단말기(데스크톱 PC, 노트북, 모바일 단말기(노트북, 스마트폰, 태블릿 단말기)), ④ 복합기(프린터(프린터, 네트워크 프린터)), ⑤ 특정용도 기기(화상 회의시스템 구성 기기, IP 전화시스템 구성 기기, 네트워크 카메라 시스템 구성 기기 및 각종 센서, 출입관리시스템 구성 기기), ⑥ 소프트웨어(OS, 어플리케이션(업무용 포함) 및 웹 콘텐츠, 미들웨어, 펌웨어(펌웨어 동작에 의해 CPU 등 제어가 가능)), ⑦ 주변기기(키보드, 마우스), ⑧ 외부 전자기록매체(외장용 하드 디스크, USB 메모리), ⑨ 서비스(시스템 개발, 운용·보수, 통신 서비스, 클라우드 서비스 제공)

따라서 정부기관은 국가안전보장 및 치안 관련 업무를 수행하는 시스템이나 기밀성이 높은 정보나 대량의 개인정보를 취급하는 시스템, 장애 발생 시 정부기관의 업무수행에 현저한 영향을 미치는 기반 시스템 등에 대해서는 보다 적극적으로 공급망 위험을 고려해야 하며, 공급망 위험 대응에 필요한 조치사항 수립 시에는 IT 종합전략실과 내각사이버보안센터(NISC[14])에 지원을 요청할 수 있다.

일본 정부기관은 이와 같은 신규 조달 규제 정책을 기업 등 민간 부문에게는 강제화하고 있지 않다. 그러나 「주요기반시설 정보보호대책에 관한 제4차 시행계획」에서 주요기반시설 사업자들의 경영층을 대상으로 공급망(비즈니스 파트너, 자회사, 관련 회사)을 포함한 정보보호대책을 마련할 것으로 요구하고 있으므로 정보통신, 전력 등 14개 분야 주요기반시설 사업자를 중심으로 특정 기업의 제품과 서비스를 배제하는 등의 공급망 보안대책을 마련할 가능성이 있다.

민간 부문의 사이버 공급망 위험관리 정책은 일본의 경제사회 활성화를 위해 산업 분야의 사이버보안 강화 정책 중 하나로 추진되고 있으며, 대표적으로 사례로 경제산업성 산하 산업사이버보안연구회가 개발한 '사이버-물리 보안대책 프레임워크(Cyber-Physical Security Framework, 이하 CPSF)'을 들 수 있다.

미국, 영국 등에서는 기존의 공급망, 즉 ICT 제품 및 서비스의 생명주기(설계, 개발 및 생산, 배포, 획득 및 배치, 운영 및 배치, 파기) 상에서 기업들 간의 관계에 따른 정보, 산출물 등의 무결성과 신뢰성, 책임추적성에 초점을 맞추었다면, 일본의 CPSF는 IoT 등으로 제4차 산업혁명 기술을 활용하면서 사이버 공간과 물리적 공간을 모두 고려한 새로운 형태의 공급망을 정의하였다. 이는 기존의 공급망의 개념이 확장된 것으로 ① 기업들 간의 연결(예. IoT 기기 제조 → 판매 → 소비자 구입)뿐만 아니라 ② 사이버 공간과 물리적 공간 간의 연결(예. IoT 기기를 통한 수집한 정보가 클라우드에 저장), ③ 사이버 공간에서의 데이터 연결(예. 맞춤형 서비스 제공을 위해 클라우드에 저장된 정보 분석)이 동시에 발생하면서 공급망을 구성하는 모든 구성요소들(기업, 데이터, 시스템 등) 간에 상호 영향을 미치는 것을 의미한다. 이와 같이 동적 형태의 공급망을 CPSF에서는 '가치창출 프로세스'로 정의하고, 이 프로세스의 신뢰성을 확보하기 위해 보안대책을 마련할 것을 요구하고 있다. 또한 CPSF는 발생 가능한 위험을 식별하여 보안대책을 수립하기 위해 3개의 계층으로 구분하고, 가치창출 프로세스(즉, 공급망)의 구성요소를 조직[15], 인력[16], 사물[17], 데이터[18], 절차[19], 시스템[20]으로 정의하였다. 이와 같은 3계층 모델을 기반으로 가치창출 프로세스 전체의 보안을 확보하기 위해서는 각 계층별로 신뢰성을 확보하고, 각 주체들은 위험관리 프로세스를 기반으로 계층별 구성요소에 대해 보안대책을 적용해야 한다.

14) National center of Incident readiness and Strategy for Cybersecurity
15) 공급망에 참가하는 기업·단체·조직
16) 조직에 소속된 인력 및 공급망 상에 직접 참가하는 인력
17) H/W, S/W, H/W 등 부품을 조작하는 기기 포함
18) 물리적 공간에서 수집된 정보, 공유·분석·시뮬레이션을 통해 가공된 정보
19) 정의된 목적을 달성하기 위한 일련의 활동들
20) 목적을 실현하기 위해 사물로 구성된 체계 및 인프라

〈표 3〉 일본 CPSF을 활용하여 공급망의 신뢰성을 확보하기 위한 기본방향

계층	주요 대상	각 주체가 수행해야 하는 보안대책
3계층: 사이버 공간에서의 데이터 연결 (사이버 공간)	데이터	▪ 조직·산업계들 간의 데이터 송수신, 가공·분석, 저장 과정에서의 조직, 인력, 시스템, 절차 등에 대한 보안성 확보
2계층: 사이버 공간과 물리적 공간 간의 연결	규칙에 따라 물리 -사이버 공간 간의 변환하는 기능	▪ 물리적 공간의 정보를 사이버 공간의 데이터로 정확하게 변환하는 기능을 포함한 사물(S/W, H/W), 시스템 등에 대한 보안성 확보 (안전성(Safety) 포함)
1계층: 기업들 간의 연결 (물리적 공간)	조직	▪ 조직이 관리하는 인력, 사물, 데이터, 절차, 시스템에 대해 적절한 보안 관리체계 수립 및 유지

따라서 CPSF을 활용하여 신뢰성을 확보하기 위해서는 각 구성요소에 대해 보안요구사항이 만족되었는지 여부(예. 보안요구사항을 충족하는 사물·데이터 생성, 이에 대한 기록 유지, 제3자의 의한 검증 등)를 확인하고, 이와 관련된 사항을 조회(예. 신뢰성 목록 작성 및 관리 등)할 수 있어야 하며, 이와 같은 상호 간의 신뢰 관계를 구축·유지(예. 상호 검증을 통해 추적성 확보, 구축된 신뢰 관계를 위협하는 공격 탐지·대응 등)하는 것이 필요하다.

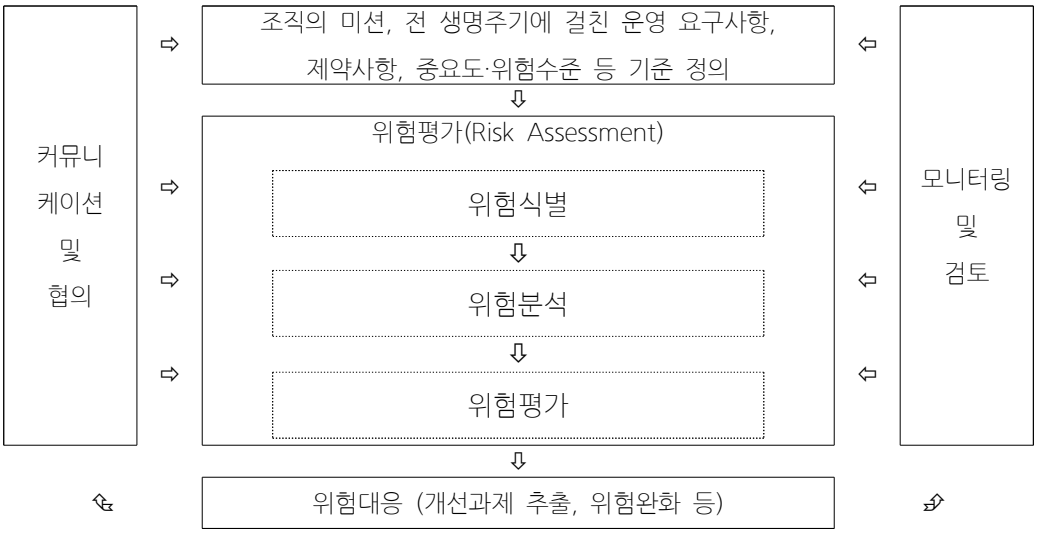
3. 주요국 사이버 공급망 위험관리(C-SCRM) 프레임워크 분석

〈표 4〉 주요국 사이버 공급망 위험관리에 관한 주요 지침 및 가이드라인

구분	국제표준	국내	미국	일본	영국	호주
조직 사이버 보안	▪ ISO/IEC27001 ▪ ISO/IEC27002	▪ 정보보호 및 개인정보보호 관리체계 (ISMS-P) ▪ 주요정보통신 기반시설 취약점 분석·평가 기준	▪ NIST RMF[21] ▪ NIST SP 800-53 ▪ NIST CSF Ver1.1. (ID.SC)	▪ NISC 정부기관 정보보호 대책에 관한 공통규범 ▪ 경제산업성 사이버보안 경영가이드라인 V2.0 ▪ 경제산업성 CPSF (CPS.SC)	▪ NCSC Cyber Assessment Framework (Supply Chain)	▪ Cyber security guidelines (Outsourcing)
사이버 공급망 보안	▪ ISO/IEC 27036 ▪ ISO/IEC 20243 ▪ IEC 62443-2-4	▪ 클라우드 보안인증제 (클라우드 서비스제공자) ▪ IoT 보안인증 (IoT제품)	▪ NIST SP 800-161 ▪ NISTIR 8179 ▪ FedRAMP (클라우드 서비스제공자) ▪ NIST SP 800-171	▪ JASA[22] 공급망 정보보호 관리	▪ NCSC Supply Chain Security Guidance ▪ NCSC Cloud Security Principles	▪ Cyber Supply Chain Risk Management ▪ Cyber Supply Chain Risk Management Practitioner Guide

주요국은 공공-민간 부문의 조직이 사이버 공급망 위험을 효과적으로 관리할 수 있도록 관련 지침이나 가이드라인을 개발하여 제공하고 있다. <표 4>에 볼 수 있듯이 조직의 사이버보안 프레임워크의 하위 항목으로 사이버 공급망 보안관리 활동을 제시하거나 또는 별도의 공급망 보안 관련 지침을 개발하였다. 그러나 공급망 위험관리의 필요성이 대두되면서 NIST CSF 등 일부는 개정 과정을 거쳐 '공급망 위험관리'를 하위항목을 신설하고, 제3자가 제공하는 제품 및 서비스 등 공급망 전체의 현황을 파악하여 대응 방안을 마련하도록 요구하고 있다.

<그림 1> C-SCRM의 위험관리 프로세스



주요 지침에서 규정하고 있는 C-SCRM는 <그림 1>와 같이 위험관리 프로세스를 기반으로 공급망 위험을 식별 및 평가하여 대응하고 모니터링을 통한 지속적인 개선활동을 실시한다. C-SCRM의 대상 범위를 살펴보면, 기존에는 정보시스템, S/W 등 ICT 제품 및 서비스, S/W개발·유지보수 등을 수행하는 외부 인력 등에 초점을 맞추었으나, ICT 융합 환경을 고려하여 IT 및 ICS, CPS[23], IoT 등 네트워크상에 연결된 장치 공급자와 구매자, 조직의 보안 상태에 영향을 미치는 파트너(Non-IT 및 OT 파트너)까지 포함하고 있다. 그러나 조직의 자원은 한정되어 있으므로, 식별한 시스템과 구성요소, 이해관계자들을 대상으로 중요도를 분석하여 우선순위를 선정하는 것이 필요하다. 이 때 중요도를 판단하는 기준으로 시스템의 상호의존성, 개인식별정보 등과 같은 데이터 민감도, 데이터 접근의 용이성, 시스템의 수명, 국가사회적 중요성 등을 들 수 있다. 따라서 미국 NIST CSF, 일본 CPSF, NCSC 및 호주의 공급망 보안 등에서 제시한 공급망 위험관리 활동을 분석하면 <표 5>와 같이 정리할 수 있다.

21) Risk Management Framework
22) Japan Information Security Audit Association
23) Cyber-Physical Systems

〈표 5〉 C-SCRM의 주요 활동

구분	주요 내용
공통 사항	▪ 사이버 공급망 위험관리 프로세스의 수립·운영 및 이해관계자와의 합의 ▪ 위험평가(Risk Assessment)를 통한 정보시스템 및 구성요소, 공급자, 제3의 파트너 식별·우선순위 선정, 평가 ▪ 공급자와 제3의 파트너와의 공식적인 계약을 따라 사이버보안대책 수행 (예. 보안사고 보고 등) ▪ 정기적 감사 또는 점검 등을 통해 계약상에서 규정한 의무사항 이행 여부 확인 ▪ 사고대응 및 복구 계획을 수립하거나 훈련 등 테스트를 수행할 때는 공급자와 제3자의 파트너 포함
추가 사항	▪ 공급자와의 책임 범위의 명확화 ▪ 공급망 보안에 관한 교육 및 인식제고 ▪ 공급자와의 계약 시 제공하는 제품·서비스가 적합한지 확인 ▪ 위탁업무를 수행하는 인력에 대한 보안 요구사항 수립·운영 ▪ 감사 또는 점검 등을 통해 결함 발견 시의 조치절차 수립·운영 ▪ 계약상에서 규정한 의무사항을 이행하고 있음을 증명하기 위한 정보 수집 및 안전하게 보관, 필요 시 적정한 범위 안에서 공개 ▪ 계약 종료 시(예. 계약기간 만료, 지원 종료)에 수행해야 하는 절차 수립·이행 ▪ 공급망에 대한 보안대책 기준 및 관련 절차 등 지속적으로 개선 ▪ 공급업체와의 전략적 파트너십 구축 및 정보공유

4. 시사점 및 결론

최근 ICT 글로벌 공급망이 복잡해지고, 화웨이·ZTE 등 중국 장비에 대한 보안 우려가 높아지면서 사이버 공급망 위험관리의 필요성이 증대되고 있다. 따라서 미국, 일본, EU 등 주요국은 정부차원 또는 산업 분야별로 공급망의 무결성 및 신뢰성을 확보하기 위해 다양한 분야의 모범사례를 토대로 관련 지침 등을 마련하고 있다. 먼저 미국과 일본을 중심으로 정부기관 및 산업 분야별 사이버 공급망 위험관리(C-SCRM) 정책 동향을 분석한 결과 다음과 같은 특징을 도출할 수 있다.

첫째, 정부기관은 사이버 공급망 위험으로 인해 국가 안보에 심각한 위협이 될 수 있다고 인식하고, S/W, H/W를 비롯하여 모든 ICT 제품과 서비스에 대한 조달 요건을 강화하였다. 미국은 연방정부의 사이버보안 강화 우선 추진과제 중 하나로 공급망 위험관리 향상을 우선 추진과제로 언급하고, 공급망의 투명성 확보와 위험관리에 대한 책임을 강조하였다. 또한 일본은 조달 규제 대상이 되는 모든 ICT 제품과 서비스, 공급망 위험을 고려해야 하는 시스템 등 기준을 구체적으로 제시하고, 각 정부기관들이 보다 적극적으로 공급망 위험에 대응하도록 절차를 강화하였다. 따라서 정부기관의 C-SCRM 정책은 제품 및 서비스에 대한 위험평가 프로세스 수립·운영, 조달 시의 공급자에 대한 평가기준 강화 등 규제를 기반으로 사이버 공급망 위험관리체계를 구축하고 있음을 알 수 있다.

둘째, 민간 부문은 전력 등 일부 분야를 제외하고는 정부기관이 직접 개입하기 보다는 산업계 또는 국제표준 단체를 중심으로 자발적 참여에 의해 공급망 위험관리 정책이 추진되었다. 그러나 일본은 주요 기반시설 분야의 사업자들을 대상으로 정부기관의 공급망 위험관리 방침을 전달함으로써 간접적으로 민간 부문에서도 공급망 보안대책을 마련할 것을 요구하였다. 또한 미국 정부기관은 사이버 공급망 위험 문제를 해결하기 위해 민·관 협력체계를 기반으로 TF팀을 구성하여 활동을 시작하고, 행정명령을 통해 정부기관은 물론 민간 기업에서도 특정 기업의 정보통신기술과 서비스에 대한 취득·설치·거래 및 사용을 금지함으로써 정부기관이 민간 부문의 ICT 공급망 위험관리 활동에 직·간접적으로 개입하기 시작한 것을 알 수 있다.

셋째, 일본 CPSF 사례 분석을 통해 IoT 등 제4차 산업혁명 기술에 의해 구성된 ICT 융합 환경을 고려하여 기존의 공급망 개념을 확장하여 조직, 인력, 정보, 사물에 이르기까지 통합적인 관점에서의 공급망 위험관리 접근방식을 확인할 수 있었다. CPSF은 사이버공간과 물리적 공간을 모두 고려하여 동적 형태의 공급망을 정의하고, 이와 같은 공급망에서의 발생 가능한 위험을 식별하여 보안대책을 수립하기 위해 3계층 모델과 6개의 구성요소(조직, 인력, 사물, 데이터, 절차, 시스템)를 정의하였다. 공급망 전체의 보안을 확보하기 위해서는 각 계층별로 신뢰성을 확보하는 것이 필요하며, 각 주체들은 위험관리 프로세스를 기반으로 계층별 구성요소에 대해 보안대책을 적용해야 한다. 따라서 스마트시티, 스마트교통 등과 같은 ICT 융합 환경에서의 단일 공급망 위험관리체계 구축 시, 이와 같은 사이버-물리보안의 통합적인 접근방식의 도입을 고려할 수 있다.

다음으로 조직에서 수행할 사이버 공급망 위험관리 활동을 파악하기 위해 주요국의 사이버 공급망 위험관리(C-SCRM) 프레임워크를 분석한 결과, 조직은 위험관리 접근방식을 기반으로 공급망 위험을 식별·평가하고 완화하는 프로세스를 구축·운영하고, 제품 및 서비스의 전 생명주기를 고려해야 한다. 따라서 조직은 사이버 공급망 위험관리 프로세스에 따라 먼저 공급망을 구성하는 IT 및 ICS, CPS, IoT 등 네트워크상에 연결된 장치, 공급자, 조직의 보안에 영향을 미칠 수 있는 제3의 파트너(예. 재위탁자) 등을 식별하고, 조직 내 중요도를 고려하여 우선순위를 선정하여 공급망 위험평가의 대상 범위를 보다 명확하게 한다. 위험분석 및 평가과정을 거쳐 위험을 완화하는 적절한 보호대책을 수립·운영하고, 모니터링과 검토를 통해 공급망에 대한 보안대책 기준 및 절차를 지속적으로 개선할 수 있는 절차를 마련한다.

조직은 공급자와의 공식적인 계약을 체결할 때, 공급자가 준수해야 하는 보안요구사항과 사고발생 시의 보고의무, 보안위협과 관련된 정보공유, 역할 및 책임, 위반 시의 제재 사항 등을 계약서에 명시하고, 공급망 상에 있는 이해관계자들이 이행할 수 있도록 한다. 또한 공급자와의 계약 시 제공하는 제품·서비스가 보안요구사항을 만족하였는지 여부를 확인하기 위해 조직 내부에서의 검증 절차를 마련하거나 제3자에 의한 평가·인증(예. 클라우드 보안인증제, IoT 보안인증 등)을 활용한다. 주기적으로 감사 또는 점검 등을 통해 계약상에서 규정한 의무사항 이행여부를 확인하고, 취약점 등 보안상의 결함 발견 시의 조치

실시, 증빙자료의 수집 및 확보 방안 등을 마련한다. 계약기간 만료, 지원종료 등에 따라 계약 종료 시에 수행해야 하는 절차(예. OT 환경에서 유지보수 기간이 종료되었으나, 부득이하게 해당 시스템 또는 기기를 사용해야 하는 경우 등)를 수립·이행해야 한다.

최근 IoT, 클라우드 등 제4차 산업혁명 기술이 본격적으로 도입되면서 다양한 사물과 서비스, 조직, 시스템 등이 빠르게 공급망에 포함될 것이다. 그러나 아웃소싱의 확대, ICT 글로벌 공급망의 복잡도 증가, 개발·제조 과정 등 공급망의 불투명성 등과 같이 내·외적 요인으로 인해 공급망 위험의 발생 가능성이 높아지고 있다. 따라서 주요국은 정부기관을 중심으로 선제적으로 대응하고자 사이버 공급망 위험관리체계를 구축하고, 관련 지침이나 가이드라인 개발 등을 통해 민간 부문에서도 공급망 위험에 대응할 수 있도록 지원하고 있다. 현재 국내에서는 클라우드 서비스, IoT 등 개별 제품을 중심으로 공급망 보안 활동을 수행하고 있으며, 이는 ICT 융합 환경에서의 다양한 제품 및 서비스, 공급자 등 공급망 전체를 포괄하여 위험에 대응하기에는 한계점가 있다. 따라서 IT/OT 환경 제품 및 서비스에 대한 전 생명주기를 고려하여 전반적인 공급망의 무결성과 신뢰성을 확보하기 위한 사이버 공급망 위험관리체계를 구축하고, 이를 지속적으로 개선하고 유지하는 방안을 마련하여 향후 변화하는 공급망 위험에 대비해야 할 것이다.

[참고문헌]

[1] 미국 정부 - 정보통신기술 및 서비스 공급망 확보에 대한 행정명령 시행, 인터넷 법제동향 제140호, 2019.05
[2] 공급망 공격 사례 분석 및 대응 방안, 한국인터넷진흥원, 2019.07
[3] 손효현, 김광준, 이만희, 미국 공급망 보안관리체계 분석, 정보보호학회논문지 Vol.29, No.5, 2019.10
[4] Supply Chain Risk Management Practices for Federal Information Systems and Organizations(NIST SP800-161), NIST, 2015.04
[5] National Cyber Strategy of the United States of America, White House, 2018.09
[6] Cyber Supply Chain Risk Management Practitioner Guide, ACSC, 2019.06
[7] ICT Supply Chain Risk Management Task Force: Interim Report, CISA, 2019.09
[8] Ariel (Eli) Levite, ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies, Carnegie Endowment for International Peace, 2019.10
[9] Cyber Supply Chain Risk Management, ACSC, 2019.11
[10] サイバーセキュリティ経営ガイドラインVer 2.0, 経済産業省, 2017.11
[11] 政府機関等の対策基準策定のためのガイドライン（平成 30 年度版), NISC, 2018.07
[12] IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ, NISC, 2018.12
[13] サイバー·フィジカル·セキュリティ対策フレームワーク Ver1.0, 経済産業省 商務情報政策局, 2019.04
[14] サイバーセキュリティ2019（2018年度報告·2019年度計画), サイバーセキュリティ戦略本部, 2019.05
[15] https://cisa.gov/
[16] https://www.cyber.gov.au/
[17] https://csrc.nist.gov/Projects/Cyber-Supply-Chain-Risk-Management
[18] https://www.ncsc.gov.uk/
[19] https://www.nerc.com/
[20] https://www.nisc.go.jp/
[21] https://www.meti.go.jp/

개인정보보호법 개정 후, 데이터 3법의 남은 과제

이창범 (miso4all@naver.com)

연세대학교 법무대학원 겸임교수

Ⅰ. 들어가는 글 : 데이터 3법과 4차 산업혁명

많은 사람들의 기대와 열망에도 불구하고 “데이터 3법(개인정보보호법, 정보통신망법, 신용정보법)” 개정안의 연내 국회 통과는 어려울 것 같다. 개정안은 각각 지난 1년 간 격론을 거쳐 어렵사리 국회 소관 상임위원회 전체회의를 통과하였으나 법제사법위원회에 발목이 잡혀 있는 상태이다. 4차 산업혁명의 강력한 추동을 위해 개정안을 신속하게 처리되어야 한다는 정·재계의 주장과 개정안을 “개인정보 도둑법”이라고 비판하며 국회 통과를 저지하려는 일부 시민사회단체의 주장이 충돌하면서 해를 넘길 전망이다.

개인정보의 활용 필요성에 대해서는 이전부터 논의가 되어 왔으나 지지부진하다가 2018년 2월과 4월에 개최된 대통령 직속 4차산업혁명위원회의 '규제·제도 혁신 해커톤'에서 정부, 시민단체, 산업계, 전문가 등 사이에 개인정보의 활용성 확대에 대한 공감대가 형성되면서 데이터 3법 개정안으로 발전하게 되었다. 「개인정보 보호법」 개정안은 더블어민주당 인재근 의원이, 「정보통신망법」 개정안은 같은 당 노웅래 의원이, 「신용정보법」 개정안은 같은 당 김병욱 의원이 각각 2018년 11월 15일 대표 발의하였다.

개인정보의 활용 촉진을 목적으로 한 「개인정보 보호법」 개정안은 사실 인재근 의원 이외에도 여러 여야 의원들에 의해서 발의되었다. 2018년 3월에 바른미래당 소속의 오세정 의원이 "가명 정보"의 활용 등을 주된 내용으로 하는 「개인정보 보호법」 개정안을 맨 처음 발의했고, 2018년 11월 22일에는 자유한국당 소속의 민경욱 의원이 「개인정보 보호법」 개정안을 발의했으며, 그 외에도 여러 여야 의원들이 개정안을 발의하였다.

이하에서는 2020년 1월 1일부터 시행될 미국 CCPA의 제정 동향을 간략히 살펴본 다음, 다소 이른 감이 없지 아니하나 데이터 3법 개정안의 국회 통과를 전제로 하여 데이터 3법 개정안의 주요 특징과 개정안 시행 후 남게 될 주요 법정책 과제에 대해서 살펴보는 것으로 한다.

Ⅱ. 미국 CCPA의 제정 배경과 주요 내용 및 특징

1. CCPA의 제정 배경

유럽연합이 2016년 5월 24일 디지털 싱글마켓 전략(Digital Single Market Strategy)[1]의 일환으로 28개 회원국 시민 모두에게 공통적으로 적용될 일반개인정보보호규정(General Data Protection Regulations, GDPR)[2]을 공표한 이후, 이에 영향을 받은 미국에서도 일반 개인정보보호법의 제정 논의가 활발하게 전개되었다. 이와 같은 환경에서 2018년 6월 캘리포니아주가 미국 역사상 처음으로 민간부문에 보편적으로 적용될 소비자 프라이버시보호법(California Consumer Privacy Act, CCPA)을 제정·공표하였다(2020. 1. 1. 시행).

미국은 원래 불문법주의 국가로 개인정보 보호 영역도 예외는 아니다. 때문에 미국은 개인정보보호를 위한 포괄적인 법률 없이 분야별로 최소한의 개별법을 제정해 대응해 왔다. 이렇게 해서 제정된 연방 개인정보보호 관련 법률은 금융현대화법, 의료정보법(HIPAA), 아동온라인프라이버시보호법(COPA) 등을 비롯해 20여개에 이른다.

그러나 이들 개별법만으로는 정보주체의 권리를 보호하는데 한계가 있기 때문에 미국 연방거래위원회

1) 2020년 디지털 싱글마켓 전략은 유럽연합이 오프라인 시장 통합에 이어 온라인상에서의 시장 통합을 목표로 2015년 5월에 수립·발표한 것으로 개인정보보호, ePrivacy 보호, 전자상거래, 소비자피해구제, 저작권보호 등 18개 로드맵으로 구성되어 있다.

2) GDPR은 2012년 1월 유럽위원회가 초안을 작성·제안하고, 2016년 4월 유럽의회와 유럽이사회가 이에 최종적으로 동의함으로써 제정되었다(2016년 5월 24일 발효). 이후 2년간의 준비를 거쳐 2018년 5월 25일부터 GDPR이 본격적으로 시행되었다.

(FTC)는 1970년대부터 FTC법 제5조를 적극적으로 활용하여 소비자의 개인정보와 사생활을 보호해 왔다. FTC법 제5조는 사업자의 불공정(unfair)하거나 기만적인(deceptive) 행위를 금지하고 있는데, FTC는 2019년 7월 12일에도 개인정보 유출에 대한 책임을 물어 페이스북에게 약 6조원(50억 달러)에 이르는 과징금을 부과하였다.

연방의회가 포괄적인 개인정보보호법 제정을 주저하는 사이 미국 최대 주 중 하나인 캘리포니아주가 사물인터넷 및 빅데이터 시대를 맞아 주민들에게 자신의 개인정보에 대한 보다 폭넓고 강화된 통제권을 부여하기 위해 일반법을 제정한 것이다. CCPA는 유럽연합 GDPR과 마찬가지로 ① 개인정보처리의 투명성(Transparency) 강화, ② 정보주체의 개인정보자기 통제권(Control) 강화, ③ 사업자의 책임성(Accountability) 강화를 입법의 3대 목표로 하고 있었다.

CCPA 제정으로 급해진 곳은 연방의회와 다른 주의회들이다. CCPA 제정 이후 네바다주, 뉴욕주, 워싱턴 DC 등 여러 다른 주에서도 유사한 입법이 시도됨에 따라 주마다 다른 개인정보보호법이 제정되는 것에 큰 우려를 느낀 연방의회 의원들이 다수의 포괄적인 개인정보보호법안을 발의하고 있다.

2. CCPA의 주요 내용 및 특징

CCPA는 사물인터넷 환경에 대비하여 보호대상을 소비자[3]뿐만 아니라 가정(a household)으로 까지 확대하고, 개인정보의 개념도 필명·별명, 계정이름, 기기ID, IP주소, 온라인 식별자(쿠키·beacon·pixel tags·모바일 광고ID·그밖에 이와 유사한 추적기술), 인터넷 활동정보(브라우징 내역, 검색 기록, 웹사이트·애플리케이션·광고 이용내역 등), 프로파일 목적의 추론정보 등까지 포함해 매우 광범위하게 정의 하고 있다. 또한 식별성의 정도에 따라 데이터를 개인정보, 가명정보, 비식별정보, 총계정보 등으로 구분하고 규정하고 있다.

CCPA는 캘리포니아에서 비즈니스를 수행하고 있는 한 역외의 사업자에게도 적용되고 해당 사업자와 공동 브랜드를 공유하는 모회사 및 자회사에게도 적용된다. 다만, 사업자의 상업행위가 캘리포니아 주 밖에서만 이루어지는 경우 소비자의 개인정보 수집·판매에 대해서는 동 법이 적용되지 않는다.

CCPA의 두드러진 특징 중 하나는 투명성 원칙의 강화이다. 소비자로부터 직접 개인정보를 수집할 때에는 수집 시점 또는 그 이전에 소비자가 합리적으로 접근할 수 있는 방식으로 수집할 개인정보의 범주, 이용목적, 삭제요구권 등을 알려야 하고, 소비자 이외로부터 개인정보를 수집할 때에는 수집한 개인정보의 범주, 수집출처의 범주, 사업상 또는 상업적 목적, 공유하는 제3자의 범주, 삭제요구권, 수집한 개인정보의 항목 등을 공개해야 한다. 무엇보다, 사업자가 수집한 개인정보를 판매하거나 공개하고자 할 때에는 개인정보가 제3자에게 팔릴 것이라는 사실, 판매거부권에 관한 설명 등을 소비자가 "합리적으로 접근할 수 있는 방식"으로 고지하고, "판매중단 지시(Do Not Sell My Personal

3) 여기서 '소비자'라 고유식별자에 의해서 식별이 되는 캘리포니아 주민인 자연인을 의미한다. 자연인이면 되므로 물건을 구입하는 구매자 이외에 근로자, 협력업체 또는 공급업체 임직원, 개인사업자 등도 소비자에 포함된다.

Information)" 링크를 인터넷 홈페이지를 통해 알기 쉽게 제공해야 한다.

또한, CCPA는 개인정보처리에 대한 소비자의 권리를 대폭 강화하고 있다. 정보공개 요구권, 개인정보 열람권(이전권), 삭제 요구권, 판매 거부권(opt-out), 차별취급을 받지 않을 권리 등을 보장하고 있으며, 16세 미만 아동 및 청소년 소비자의 개인정보 처리에 대해서는 옵트인(opt-in) 방식을 적용하고 있다. 그 중 가장 큰 특징은 차별취급을 받지 않을 권리라고 할 수 있다. 사업자는 소비자가 판매 거부권, 삭제 요구권 등의 권리를 행사했다는 이유로 차별적인 취급을 해서는 안 되며 모든 소비자에게 동등한 품질과 가격으로 재화 또는 서비스를 제공해야 한다. 우리나라에서는 서비스 제공 거부만 금지하고 있다.

Ⅲ. 데이터 3법 개정안의 주요 내용 및 특징

데이터 3법 개정안의 특징은 가명정보 및 익명정보의 활용 근거 명시, 제한적 범위 내에서 개인정보의 목적외 이용 허용(양립 가능성 원칙), 정보집합물의 결합 허용, 정보전송요구권(MyData) 신설, 법정 고지사항의 고지방법 유연화, 법집행 체계의 일원화, 벌칙규정의 정비 등을 통해서 개인정보의 활용성을 확대했다는데 있다.

1. 개인정보보호법 개정안의 주요 내용 및 특징

가. 가명정보의 활용 근거 명시

개정안은 개인 식별 정도에 따라 데이터의 유형을 ① 식별정보 ② 식별 가능정보 ③ 가명정보 ④ 익명정보로 구분하고 있다. 개정안은 "가명정보"를 원상태로 복원하기 위한 추가 정보의 사용·결합없이는 특정 개인을 알아볼 수 없는 정보로 정의하고, 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 처리하는 경우에는 정보주체의 동의가 필요 없다고 규정하고 있다.

나. 정보집합물의 결합 허용

개정안은 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 필요한 경우 개인정보처리자간 정보집합물의 결합을 명시적으로 허용하고 있다. 다만, 정보집합물의 결합은 대통령령으로 정하는 기준에 따라 보안시설을 갖춘 전문기관에서 수행해야 하며, 결합된 정보집합물을 전문기관 밖으로 반출하려면 가명정보나 익명정보로 처리한 뒤 전문기관의 장의 승인을 받도록 하고 있다. 비식결정보간 데이터 결합을 허용하고 있다는 점에서 특징적이라 할 수 있다.

다. 목적외 이용·제공의 제한적 허용

개정안은 당초 수집 목적과 합리적으로 관련된 범위 내에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령이 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용하거나 제공할 수 있게 하고 있다. 이른바 유럽연합 GDPR 및 미국 CCPA가 도입하고 있는 양립가능성(compatibility) 원칙을 반영한 것이다.

다. 정보통신서비스제공자등에 대한 특례 신설

개정안은 정보통신서비스제공자등에 대한 특례규정을 두고 있다. 특례규정은 새로운 규제를 신설한 것은 아니고 현행 정보통신망법 중 개인정보보호 관련 규정의 일부를 이전한 것이다. 그러나 개인정보 제공 제한, 개인정보처리 위탁, 영업양도등에 따른 개인정보 이전통지, 동의받는 방법, 개인정보보호책임자 지정, 개인정조처리방침 공개, 기술적·관리적 보호조치, 손해배상, 벌칙규정 등 「개인정보 보호법」과 중복되면서 충돌 소비자가 있다고 지적돼 온 일부 조항은 특례에서 배제하고 있다.

라. 개인정보보호 관련법의 집행체계 일원화

개정안은 개인정보보호위원회를 국무총리 소속의 중앙행정기관으로 격상하여 현재 행정안전부, 방송통신위원회, 개인정보보호위원회에 분산되어 있는 개인정보 보호 업무를 일원화하고 있다. 또한 개인정보보호위원회의 사무 및 심의·의결의 독립성을 보장하기 위하여 「정보조직법」 제18조에서 규정하고 있는 중앙행정기관의 장에 대한 국무총리의 행정감독권을 적용하지 않도록 규정하고 있다.

2. 정보통신망법 개정안의 주요 내용 및 특징

가. 개인정보 관련 규정의 이관

정보통신망법 제4장, 제8장, 제9장, 제10장 등에 규정된 개인정보보호 관련 조항을 삭제하고 이를 개인정보보호법으로 이관하고 있다. 이에 따라 개정안이 통과되면 정보통신망을 통한 정보통신서비스 제공자등의 이용자 개인정보 처리에 대한 관리·감독 권한도 방송통신위원회에서 개인정보보호위원회로 이전하게 된다.

나. 사생활 보호규정은 그대로

「정보통신망법」 중 개인정보 보호와 직접 관련이 없는 사생활 보호 조항은 여전히 정보통신망법에 그대로 남겨져 있다. 즉 앱 접근권한 제한, 본인확인기관 지정제도, 개인정보보호 관리체계인증 등에 관한 규정은 「개인정보 보호법」으로 이전하지 않고 「정보통신망법」에 그대로 남겨 두었으며, 광고성 정보(스팸) 전송에 관한 규정도 「정보통신망법」에 그대로 남겨져 있다.

3. 신용정보법 개정안의 주요 내용 및 특징

가. 가명조치 및 익명조치의 정의 신설

개정안은 추가정보를 사용하지 아니하고는 특정 개인을 알아볼 수 없도록 개인신용정보를 처리하는 것을 가명조치로 정의하고, 가명조치한 개인신용정보는 신용정보주체의 동의 없이도 통계작성(시장조사 등 상업적 목적의 통계작성을 포함), 연구(산업적 연구를 포함), 공익적 기록보존 등을 위해 이용. 및 제공할 수 있도록 하고 있다. 또한 신용정보제공 · 이용자는 상거래관계가 종료된 날부터 최장 5년 이내에 해당 개인신용정보를 관리대상에서 삭제하여야 하나, 가명정보를 이용하는 경우에는 가명정보의 이용

목적 및 가명조치의 기술적 특성, 정보의 속성 등을 고려하여 대통령령으로 정하는 기간 동안 보존할 수 있다. 또한 더 이상 특정 개인을 알아볼 수 없도록 개인신용정보를 처리하는 것을 “익명조치”로 정의하고, 금융위원회가 위탁한 데이터전문기관의 적정성 심사를 통해 적정하게 익명조치가 이루어졌다고 인정한 경우 더 이상 해당 개인인 신용정보주체를 알아볼 수 없는 정보로 추정한다.

나. 이종 산업간 정보집합물 결합 허용

개정안은 이종 산업간 개인정보결합을 허용하고 있다. 다만, 신용정보회사 등이 자신이 보유한 정보집합물을 제3자가 보유하는 다른 정보집합물과 결합할 경우에는 데이터전문기관을 통해서 결합해야 한다. 다만, 데이터전문기관이 결합된 정보집합물을 해당 신용정보회사등 또는 제3자에게 전달하는 경우에는 가명조치 또는 익명조치가 된 상태로 전달해야 한다. 이에 따라 정보집합물의 결합을 위한 개인신용정보의 이용 또는 제공의 경우에는 정보주체의 동의가 필요 없고, 가명화 또는 익명화도 요구되지 않으며, 결합의 목적에도 제한이 없다.

다. 동의없는 개인정보 수집, 이용 및 제공

신용정보회사등이 개인신용정보를 수집하는 때에는 원칙적으로 해당 신용정보주체의 동의를 받아야 하나, 공개정보 즉 법령에 따라 공시(公示)되거나 공개된 정보, 출판물이나 방송매체 또는 「공공기관의 정보공개에 관한 법률」 제2조제3호에 따른 공공기관의 인터넷 홈페이지 등의 매체를 통하여 공시 또는 공개된 정보, 신용정보주체가 스스로 사회관계망서비스 등에 직접 또는 제3자를 통하여 공개한 정보, 그 밖에 이와 유사한 정보로서 대통령령으로 정하는 정보는 개인신용정보주체의 동의를 받지 않고 수집이 가능하도록 하고 있다.

또한 신용정보회사등이 개인신용정보를 이용하거나 제공하려는 경우에는 원칙적으로 신용정보주체로부터 개인신용정보를 이용·제공에 대하여 동의를 받아야 하지만, 당초 수집한 목적과 상충되지 아니하는 범위에서 신용정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 개인신용정보를 이용.제공하는 경우, 개인이 직접 제공한 개인신용정보를 제공받은 목적으로 이용하는 경우에는 개인신용정보주체의 동의를 받을 필요가 없도록 하고 있다.

라. 본인신용정보관리업 및 정보전송요구권의 도입

개정안은 개인신용정보주체의 신용관리를 지원하기 위하여 해당 신용정보주체의 신용정보를 통합하여 그 신용정보주체에게 제공하는 행위를 주된 영업으로 하는 “본인신용정보관리업” 이른바 마이데이터사업을 도입하고 있다. 마이데이터사업자는 개인신용정보주체를 대신하여 개인정보 자기결정권을 대리 행사할 수 있고 금융회사 등으로부터 전송받은 개인신용정보를 이용하여 신용정보주체에게 데이터 분석 및 컨설팅, 개인신용정보를 관리 · 사용할 수 있는 계좌 제공, 투자일임·투자자문 등의 서비스를 제공할 수 있게

된다. 또한, 마이데이터사업이 가능하도록 개인신용정보주체는 자신에 관한 개인신용정보를 보유하고 있는 신용정보제공·이용자 및 정부·공공기관에 대하여 자신에 관한 개인신용정보를 자신이나 본인신용정보관리회사, 다른 신용정보제공·이용자, 개인신용평가회사, 그 밖에 대통령령으로 정하는 자에게 전송하여 줄 것을 요구할 수 있는 개인신용정보 전송요구권을 인정받게 된다.

마. 법정 고지사항의 고지방법 유연화

신용정보회사등이 개인신용정보 활용에 대한 동의를 받을 때에는 「개인정보 보호법」 제15조제2항, 제17조제2항 및 제18조제3항에 따라 신용정보주체에게 해당 각 조항에서 규정한 "고지사항"을 알리고 동의를 받아야 하지만, 대통령령으로 정하는 신용정보제공·이용자는 고지사항 중 그 일부를 생략하거나 중요한 사항만을 발췌하여 그 신용정보주체에게 알리고 정보활용 동의를 받을 수 있도록 하고 있다. 다만, 개인신용정보주체가 고지사항 전부를 알려줄 것을 요청한 경우에는 그러하지 아니한다.

바. 신용정보주체의 권리 강화

개정안은 신용정보 활동 동의 등급제, 신용정보 관리체계의 강화, 자동화평가에 대한 권리 신설, 개인신용정보 전송요구권 등을 통해 신용정보주체의 권리를 강화하기 위한 일부 조치도 도입하고 있다. 개인정보 활용과 균형을 맞추기 위한 것으로 보인다.

사. 개인정보보호위원회의 집행 권한

금융회사 등을 제외한 신용정보제공·이용자인 "상거래 기업 및 법인"에 대해서는 금융위원회를 대신하여 개인정보 보호위원회가 자료제출요구·검사권·출입권·질문권 및 시정명령, 과징금 및 과태료 부과 등의 권한을 해상할 수 있게 함으로써 상거래기업 및 법인의 개인정보보호에 대한 관리감독체계를 개인정보보호위원회로 일원화하고 있다.

Ⅳ. 개정 후, 데이터 3법의 남은 과제

데이터 3법 개정안이 국회 본회의를 통과하여 시행되더라도 여전히 해결되지 않고 남아 있는 문제점이 적지 않다. 그 중 몇 가지는 시급히 해결해야 할 과제가 될 수 있다.

1. 산업별·업종별 차별 적용 문제

가. 정보통신서비스 제공자등에 대한 차별 적용

「개인정보 보호법」 개정안이 정보통신서비스 제공자등에 대한 특례 규정을 남겨 둠으로써 정보통신서비스 제공자등은 법 개정 이후에도 계속해서 차별적인 취급을 받아야 한다. 정보통신서비스 제공자등은 여전히 일반 개인정보처리자들은 부담하지 않은 개인정보 수집·이용에 대한 동의 원칙(동의 예외사유의

차별 적용), 이용내역 통지의무, 개인정보 유효기간제(휴면계정 삭제·분리 보관 의무), 배상책임보험 가입 의무, 국내대리인 지정의무, 국외 이전 제한 및 보호조치 의무, 유출사고 신고·통지 지연사유 소명 의무 등의 규제를 받아야 한다. 국내대리인 지정제도와 같이 나름대로 차별화의 합리적인 이유가 있는 것도 있지만 합리적인 근거를 찾기 어려운 것이 많아 관련 업계 또는 업종의 저항이 예상된다.

또한, 개정법 하에서도 정보통신서비스 제공자등은 여전히 동일한 법위반 행위에 대하여 차별적인 벌칙을 적용받아야 하는 경우가 많다. 예컨대, 개정안에 따르면 일반 개인정보처리자가 제15조 제1항을 위반하여 개인정보를 수집하거나 제22조 제6항을 위반하여 법정대리인의 동의를 받지 않고 아동의 개인정보를 수집한 경우 5천만원 이하의 과태료 처분을 받게 되지만, 정보통신서비스 제공자등이 동일한 법위반을 하게 되면 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하게 된다. 또한, 개인정보처리자가 제21조제1항을 위반하여 개인정보를 파기하지 아니한 경우에는 3천만원 이하의 과태료 처분을 받게 되지만, 정보통신서비스 제공자등이 동일한 법위반을 하게 되면 2년 이하의 징역 또는 2천만원 이하의 벌금에 처하게 된다. 과태료 부과기준에 있어서도 차이가 있다. 개인정보처리자가 제22조 제1항부터 제4항까지의 규정을 위반하여 구분해서 동의를 받지 아니한 경우에는 1천만원 이하의 과태료 처분을 받지만, 정보통신서비스 제공자등이 동일한 법위반을 한 경우에는 2천만원 이하의 과태료 처분을 받게 된다. 또한, 개인정보처리자는 개인정보 유출사고 신고 및 통지 의무 지연에 대한 소명 의무가 없지만, 정보통신서비스 제공자등은 소명의무 위반시 3천만원 이하의 과태료 처분을 받게 된다.

나. 의료·사회보장 기관·단체 등에 대한 차별 적용

「개인정보 보호법」 개정안은 일반 개인정보에 대해서는 가명처리 등의 예외를 인정하면서 민감정보에 대해서는 가명처리 등의 예외를 명시적으로 인정하고 있지 아니함으로써 의료계, 사회보장기관 등으로부터 차별화 논란이 예상된다. 개정안은 개인정보처리자가 개인정보를 가명 처리한 경우 정보주체의 동의 없이 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 처리할 수 있도록 허용하고 있고(제28조의2), 또한 당초 수집한 목적과 합리적으로 관련된 범위 내에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 정보주체의 동의 없이 개인정보를 이용하거나 제공할 수 있게 하고 있다(제15조 제3항 및 제17조 제4항).

그러나 「개인정보 보호법」 제23조에 따른 민감정보(사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보)가 가명처리의 대상이 될 수 있는지 여부 및 가명처리된 민감정보를 정보주체의 동의 없이 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 처리할 수 있는지 여부가 불분명하다. 또한, 당초 수집한 목적과 합리적으로 관련된 범위 내라면 정보주체의 동의 없이 개인정보를 이용하거나 제공할 수 있는지 여부도 불분명하다.

「개인정보 보호법」 제23조는 민감정보의 처리를 원칙적으로 금지하면서, 예외적으로 ① 다른 개인정보의 처리에 대한 동의와 별도로 정보주체의 동의를 받은 경우와 ② 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에만 민감정보를 처리할 수 있도록 제한하고 있어, 민감정보는 가명처리의 대상에 해당하지 않고 당초 수집한 목적과 합리적으로 관련된 범위 내라도 정보주체의 동의 없이는 민감정보를 이용하거나 제공할 수 없다고 해석될 여지가 크다. 이 경우 의료정보, 장애정보 등 건강정보(민감정보)의 처리가 불가피한 의료계, 제약업계, 사회보장기관 등으로부터 차별화 논란이 예상된다.

2. 「개인정보 보호법」과 신용정보법의 충돌 문제

「신용정보법」의 적용 대상은 신용정보회사등(신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관, 신용정보·이용자)이지만, 그 중 핵심 적용대상은 신용정보제공·이용자이다. 「신용정보보법」 개정안은 "신용정보"를 금융거래 등 상거래에서 거래 상대방의 신용을 판단할 때 필요한 정보라고 넓게 정의하고 있고(제2조제1호), "신용정보제공 · 이용자"를 고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻거나 만들어 낸 신용정보를 타인에게 제공하거나 타인으로부터 신용정보를 제공받아 본인의 영업에 이용하는 자와 그 밖에 이에 준하는 자로서 대통령령으로 정하는 자를 말한다고 규정하고 있다(제2조제7호).

개정안은 “신용정보”의 유형을 시행령에서 법률로 상향 입법한 것 이외에 "신용정보제공 · 이용자"의 정의나 범위에 대해서는 특별히 확대하거나 그밖의 수정을 가한 것이 없으므로 원칙적으로 현행 「신용정보법」의 적용 범위와 달라질 것이 없다. 그럼에도 불구하고 개정안 제45조 제1항과 제45조의3 제1항은 금융위원회의 감독을 받지 아니하는 신용정보제공·이용자의 하나로 “상거래기업 및 법인”을 상정하고 있고 이종 산업간 정보집합물의 결합을 허용하고 있다. 이는 곧 「신용정보법」 제2조제7호에서 규정하고 있는 신용정보제공 · 이용자의 개념을 보다 적극적으로 확대해서 해석하겠다는 의미로 이해될 수 있다.

이 경우 ‘상거래를 위하여 본인의 영업과 관련하여 얻거나 만들어 낸 신용정보를 타인에게 제공하거나 타인으로부터 신용정보를 제공받아 본인의 영업에 이용하는 자’는 모두 「신용정보법」의 적용대상이 되며, 개정안에 의해서 새로 추가된 규정들까지 금융회사 등이 아닌 일반 “상거래기업 및 법인”들에게까지 확대 적용됨으로써 그동안에도 해석상 논란이 되어 온 「개인정보 보호법」과 의 중복 적용 문제가 심화될 것으로 예상된다. 이는 데이터 3법 개정의 취지와 달리 「개인정보 보호법」의 적용 범위를 대부분 침식하게 되어 법 해석 및 적용상 적지 않은 충돌 문제가 발생할 것으로 예상된다.

3. 정보통신망법과 위치정보법의 정비 문제

「정보통신망법」 중 개인정보 보호와 관련된 조항이 모두 「개인정보 보호법」으로 이전한다고 하더라도 개인정보 보호와 직접 관련이 없는 앱 접근권한 제한, 본인확인기관 지정제도, 개인정보보호 관리체계

인증, 광고성 정보(스팸) 전송 제한 등에 관한 규정은 「정보통신망법」에 그대로 남게 된다. 또한 「위치정보의 보호 및 이용 등에 관한 법률」도 여전히 방송통신위원회의 소관으로 남게 된다. 그러나 앱 접근권한 제한 등이 모두 개인정보의 처리를 매개로 하고 있어 「개인정보 보호법」과 분리하기 어렵고, 위치정보는 사물인터넷(IoT) 환경에서 가장 주도적인 역할을 담당하고 있는 바 위치정보를 제외한 「개인정보 보호법」은 상상하기 어렵다. 이에 따라 사업과 관련된 부분은 개별법에 남겨 두더라도 개인정보 또는 위치정보의 보호에 대해서는 「개인정보 보호법」 체계 내에서 통일적으로 관리·감독되도록 관련 법률을 정비해야 한다는 주장이 제기될 것으로 보인다.

4. 정보주체의 권리 보호 및 실질화 문제

데이터 3법 개정안은 개인정보의 활용에 초점이 맞추어져 있어 정보주체의 권리 보호에 대해서는 선진국 수준에 미치지 못하고 있다. 우리나라 개인정보보호법은 어느 선진국 못지 않게 정보주체에게 강력한 권리를 부여하고 있고 다른 나라들과 달리 법 위반행위에 대해서 다수의 형사처벌 규정까지 두고 있지만, 정보주체가 실제 권리를 행사하는데 어려움이 많고 법위반에 대해서도 제대로 처벌이 이루어지고 있지 않아 종이호랑이에 불과하다는 비판을 받고 있다. 개인정보의 활용이 쉬워진 만큼 정보주체의 권리 행사도 쉽게 행사할 수 있도록 개선하여야 하고, 법위반 행위에 대한 벌칙도 사업자들의 법위반 행위를 실질적으로 억제할 수 있는 방향으로 현실화해야 할 과제가 남아 있다.

Ⅴ. 맺음말

데이터 3법 개정안이 데이터 경제 또는 4차 산업혁명과 관련된 모든 문제를 해결해 주는 것은 아니다. 데이터 3법 개정안은 데이터 경제의 서막을 여는 시작에 불과하다. 제대로 된 데이터 활용 환경을 만들고 데이터 경제의 성공을 이루기 위해서는 가명·익명 처리, 정보집합물 결합, 마이 데이터, 양립성 원칙 등에 대한 합리적이고 글로벌 스탠다드에 맞는 기준 설정이 필요하며, 산업간 또는 업종간 불합리한 차별화 정책도 재고되어야 한다. 또한, 무엇보다 시급한 것은 정보주체의 권리를 실질화 할 수 있는 조치가 뒤 따라야 할 것이다. 이를 위해서는 유럽연합 GDPR은 물론 미국의 CCPA가 많은 참고가 될 것이다.

GDPR은 민감정보도 사회보장 관련법에 따라 민감정보의 처리가 필요한 경우, 사회복지 시스템을 위하여 민감정보의 처리가 필요한 경우, 공익을 위한 기록보존 목적/과학적·역사적 연구 목적/통계적 목적으로 민감정보의 처리가 필요한 경우에는 정보주체의 동의 없이 처리할 수 있음을 명시하고 있다. CCPA는 비지니스 목적(business purpose)과 커머셜 목적(commercial purpose)을 구분해 개인정보의 보호 수준을 달리하고 있으며, 고유식별정보, 의료정보, 건강정보 등이 포함된 민감정보의 무단 접근·침입·도난·공개에 대해서는 법정손해배상을 인정하지만, 일반 개인정보의 유출 등에 대해서는 법정손해배상청구를 허용하지 않음으로써 개인정보보호에 유연하게 대응하고 있다. 그 대신 개인정보의 범위는 개인 추적이 가능한 모든 정보로 확대하고 정보주체가 언제 어디서나 권리를 쉽게 행사할 수 있도록 정보주체의 권리를 대폭 강화하고 있다.

2019 인터넷 10대 이슈 전망

- 1인 미디어 생산자가 경제적 주체가 되는 크리에이터 경제
- 디지털 경제의 중심축으로 자리잡는 데이터 경제
- 머니게임에서 실질적 활용을 추구하는 블록체인
- 상상에서 대중 수단이 되는 스마트 모빌리티
- 본격 상용화 시대를 여는 5G
- 우려에서 기대로 무게중심의 변화가 기대되는 디지털 헬스케어
- 지나친 기대에서 냉정한 현실로 다가오는 인공지능
- 경험의 지평을 넓히는 실감형 콘텐츠
- ICT 신산업 혁신의 장, 규제 샌드박스
- 클라우드와 양두마차로 내달리는 엣지 컴퓨팅

2019년 Vol.1 CES 2019

이슈 & 트렌드

- CES 2019 주요 이슈 분석
- CES 2019에 등장한 인공지능 기술과 제품 동향
- CES 2019 자율주행 주요 동향
- CES 2019가 보여준 '컴퓨팅의 현재와 미래'
- CES 2019, 다음 단계로 발걸음 옮긴 가상현실 헤드셋 기술
- CES 2019 디스플레이의 변화, '화질에서 공간으로'
- 중국 CES 2019 기업 동향
- CES 2019 전시회, '유레카'가 사라진, 그러나 꾸준히 발전하는 '유레카 존'

2019년 Vol.2

이슈 & 트렌드

- 5G 상용화와 함께 새로이 조명되는 엣지 컴퓨팅
- 2018 'AI 인덱스' 보고서 제시하는 주요 의미
- 인공지능의 윤리적 이슈 및 정책 시사점
- 인공지능 음성인식 시장의 현황과 전망
- 넷플릭스<킹덤>과 온라인 동영상 서비스 환경의 격변기
- 사업 실현성에 좀 더 가까워진 '블록체인' 전망
- 중국 사회보장제도시스템 동향 및 기업 대응
- 스마트시티의 보안 이슈 및 시사점
- 사이버보안 전문인력 양성 관련 국외 사례 분석 및 시사점
- 공개서비스를 통한 개인정보 위협 사례 분석 및 시사점

2019년 Vol.3 MWC 2019 & RSA Conference 2019

이슈 & 트렌드

- MWC 2019에서 확인한 5G 시대, 모든 컴퓨팅 장치가 달라진다
- MWC 2019, 상용화 준비 끝난 5세대 이동통신 생태계와 서비스
- MWC 2019, 서비스를 위한 스마트카의 다양한 진화
- MWC 2019, 4YFN에서 살펴본 스타트업 기술 동향
- MWC 2019 주요 이슈 분석
- RSA Conference 2019를 통해 본 위협 그리고 인공지능과 자동화
- RSA Conference 2019 & 인공지능 이슈
- RSA Conference 2019에서 살펴본 클라우드 기반 보안 서비스 동향
- RSA Conference 2019에서 살펴보는 OT 보안 현황
- RSA Conference 2019 주요 이슈 분석

2019년 Vol.4

이슈 & 트렌드

- 글로벌 5G 도입 논쟁과 정보보호
- 'Apple TV+'로 애플은 새로운 성장 국면을 맞이할까
- 스마트폰 생체 인식기술 동향
- 도약하는 중국 산업 인터넷 및 정책 현황
- 인더스트리 4.0으로 살펴본 디지털 트윈
- EU 공통의 사이버보안 인증체제 출범
- 「개인정보보호법」과 명확성 등의 요구

2019년 Vol.5

이슈 & 트렌드

- 5G 네트워크 슬라이싱-Network-as-a-Service(NaaS)를 향한 가상네트워크 기술
- 클라우드와 블록체인의 만남 'BaaS'
- AI 기반 사이버보안 - 이용·인식현황 중심으로
- 스마트공장 보안
- 스마트시티 서비스를 위한 플랫폼 주요 보안 기술
- 의료기관 정보보호 강화를 위한 노력
- 2019년 마이크로소프트 빌드, 페이스북 F8, 구글 I/O에서 발표한 인공지능 기술과 그 의미
- 중국과 미국의 기반기술 주도권 경쟁
- 디즈니의 OTT 시장 진출, 눈여겨볼 지점들

2019년 Vol.6

이슈 & 트렌드

- 허위정보, 가짜 뉴스, 폭력 및 혐오 발언과 싸우는 각국 정부
- 게임 지형의 변화를 가져올 클라우드 게이밍
- 도약기에 접어든 중국의 5G 시장 및 정책
- 5G++; Security++; Privacy--;
- 화자인식: 음성인식의 보이지 않는 보안 기술
- ITU 분산원장기술 포커스 그룹 표준화 추진
- 지역 중소기업의 정보보호 실천력 제고를 위한 소고
- 중국 개인정보보호 동향
- 개인정보자기결정권과 동의의 관계에 대한 이해
- Privacy Global Edge 2019 및 Asia Privacy Bridge Forum 리뷰

2019년 Vol.7

이슈 & 트렌드

- 일본 정보은행 인정 제도
- 5G 네트워크 시대 정보보호 기술 동향
- 국가 주도형 사이버보안 거버넌스의 확장
- 4차 산업혁명은 데이터 시대, XAI가 중요한 이유
- 〈WWDC 2019〉 '프라이버시 보호'에 또 한 발 앞서는 애플
- 메리 미커의 2019 인터넷 트렌드 보고서에 대한 리뷰
- 2019년 중국 인터넷 트렌드 리뷰 - 메리 미커 보고서를 중심으로
- 아마존의 상업 드론 배송은 무엇을 바꿔놓을까?
- 우버(Uber)로 돌아보는 이동의 패러다임 변화
- 무엇이 좋은 대화(Good Conversation)를 만드는가? : 페이스북 연구 네트워크 '좋은 대화 요건' 연구 리뷰

2019년 Vol.8

특별호 'MOVIE IT'

- 로봇과 사랑할 수 있을까? - SF 영화를 중심으로
- 영화 속 생체인증 - 사람의 운명이 몸에 새겨지는 미래
- 〈레디 플레이어 원〉 미래를 만든 가상현실의 현재
- 인공지능과 킬 스위치
- 〈하우스 오브 카드〉에 표현된 텍스트 마이닝 기술, 그 현재와 미래

이슈 & 트렌드

- 개인정보의 기술적·관리적 보호조치 기준 고시에 관한 법원 판결 동향
- 상하이협력기구 국가들의 사이버 협력: 규범 제정 및 공동 훈련을 중심으로
- 트럼프 행정부의 최신 인공지능(AI) 동향
- 해외에서 개인정보가 이용될 때 개인정보보호를 도와줄 수 있는 자율보호제도: APEC CBPRs와 PRP 인증

2019년 Vol.9

이슈 & 트렌드

- 한국의 인공지능 알고리즘 담론
- 아세안의 사이버보안 국제협력 현황
- 사이버보안에서 AI 활용 편익과 구현 방법
- 인공지능과 킬 스위치
- 빅 테크 기업에 대한 미국 정부와 의회의 움직임
- IFA 2019 유럽 가전의 혁신 속도가 빨라지다
- 애플 아이폰11 발표 속 스마트폰 시장 흐름 읽기
- 미국과 중국의 인터넷 미래 전망: 5G 선점을 위한 경쟁

2019년 Vol.10

이슈 & 트렌드

- AI 넥스트 캠페인: 미국 방위고등연구계획국(DARPA)의 차세대 인공지능 연구
- 인공지능은 소비자 장치에 어떤 모습으로 파고들었나?
- AI 민주화(Democratization of AI)
- 유네스코 보고서를 통해 살펴본 '교육 분야 AI 적용과 과제'
- 게임의, 게임을 위한, 게임에 의한 AI
- 중국의 AI 윤리 논의 현황
- 중국의 인공지능(AI) 산업의 움직임
- 캐나다의 인공지능(AI) 정책 추진 동향
- 금융 클라우드 정보보호조치에 대한 통상법적 소고
- 미국과 중국의 인터넷 미래 전망: 블록체인 추진 동향

2019년 Vol.11

이슈 & 트렌드

- 구독형 전자상거래(Subscription E-commerce)란 무엇인가?
- 구독 서비스로 스마트하게 스마트 홈을 구축할 수 있을까?
- 2020년 동영상 OTT 구독 번들링 경제 환경에서 경쟁적 요소는?
- 게임 구독, 새로운 기술과 콘텐츠 끌어안는 플랫폼의 역할과 기대
- 양자컴퓨터 현황 분석: 미국과 중국을 중심으로
- MIT College of Computing 설립 의미와 시사점
- 주요국 주요기반시설 사이버보안 정책 분석 및 시사점

주제 제안 및 정기구독 신청 | kisareport@kisa.or.kr

인터넷, 정보보호 및 개인정보보호와 관련한 각종 이슈와 동향 등 궁금한 사항을 이메일로 보내주시면 선별하여 KISA REPORT의 주제로 선정합니다.

KISA REPORT의 정기 구독을 원하시는 경우 이메일로 신청해주시면 매월 이메일로 받아보실 수 있습니다.

발 행 일	2019년 12월
발 행 처	한국인터넷진흥원 (전라남도 나주시 진흥길 9)
기 획	한국인터넷진흥원 ICT미래연구소
편 집	㈜ 해리

KISA 한국인터넷진흥원