



# KISA REPORT

2019 VOL.9

## CONTENTS

### ISSUE

- 01 한국의 인공지능 알고리즘 담론  
[심우민 / 경인교육대학교 교수]
- 02 아세안의 사이버보안 국제협력 현황  
[박성림 / 국립정치대학(대만) 정치학연구소 박사수료]
- 03 사이버보안에서 AI 활용 편익과 구현 방법  
[이용용 / ICT&Security 애널리스트]
- 04 빅 테크 기업에 대한 미국 정부와 의회의 움직임  
[한상기 / 테크프론티어 대표]

### TREND

- 01 IFA 2019 유럽 가전의 혁신 속도가 빨라지다  
[최필식 / 기술작가]
- 02 애플 아이폰11 발표 속 스마트폰 시장 흐름 읽기  
[최호섭 / 디지털 칼럼니스트]
- 03 미국과 중국의 인터넷 미래 전망: 5G 선점을 위한 경쟁  
[유성민 / IT 칼럼니스트]

# 한국의 인공지능 알고리즘 담론



심우민 (legislation21@ginue.ac.kr)

경인교육대학교 교수  
사이버커뮤니케이션학회 총무이사

## 알고리즘 시대의 서막

인공지능(artificial intelligence) 기술 활용의 일상화가 점점 가시권에 진입하면서, 그 활용으로 인한 다양한 윤리적, 규범적 사안들에 관한 관심도 높아지고 있다. 그런 의미에서 정부 및 공공영역을 주축으로 하는 다양한 입법 정책적 대안들도 제시되고 있으며,民間 영역에서는 윤리 기준들을 중심으로 하는 담론들이 형성되어 가고 있다.

이러한 상황에서 중요한 것은 궁극적으로 인공지능 기술을 우리 사회의 혁신과 관련하여 어떻게 활용할 수 있는 것인지, 그리고 다양하게 예견되는 역기능들을 어떻게 방지할 수 있을 것인지 여부라고 할 수 있다. 그런데 현재 우리사회의 인공지능 알고리즘 담론은 현존하는 규제법제의 핵심이 마치 거대한 수익을 올리는 사업자들의 영업활동을 제약하기 위한 것처럼 오인하고 있거나 또는 그래야 된다고 생각하는 경향이 있다. 따라서 현재 우리 사회의 알고리즘 담론은 균형성을 회복하면서도, 온전한 알고리즘 시대의 진척을 위해 노력하는 데 집중해야 할 필요가 있을 것으로 보인다.

인공지능 기술의 발전은 종국적으로 기계적 판단의 바탕을 이루는 알고리즘의 영향력을 확산시킬 것으로 보인다. 통상적으로 알고리즘(algorithm)이란 주어진 문제를 풀기 위한 절차나 방법을 기술한 것을 의미한다. 인공지능은 일종의 소프트웨어 또는 프로그램을 기반으로 구동되는 것으로서, 이는 데이터를 학습하고 그 결과물을 산출해 내는 알고리즘에 의해 구성된다.

인공지능의 사회적 의미는 다양할 수 있겠으나, 기본적으로는 인간의 판단을 기계적 판단으로 대체한다는 점이 가장 중요한 의미라고 할 수 있다. 이는 다른 표현으로 소위 자동화(automation)라고 할 수 있으며, 최신의 인공지능 수준을 아니더라도 인간은 오랜 시간 동안 판단 및 행위의 자동화를 추구해 왔다는 점은 쉽게 확인할 수 있다. 물론 현재 수준에서의 인공지능 담론은 단순 자동화를 넘어서서 인간의 합리적 판단과 유사한 기계적 판단을 기대하는 것이기는 하다. 다만 이 지점에서 인간은 기계적 알고리즘 판단에 상당 부분 의존하게 될 것이라는 점을 확인할 수 있다. 예를 들면, 인간은 아주 단순한 수치 계산도 계산기에 의존하는 경향성을 보인다.

이런 의미에서 인공지능의 일상적 활용이 이루어지는 초기라고 할 수 있는 현 단계는 이미 소위 “알고리즘 시대”라고 할 수 있는 상황이다. 즉 인간의 행위와 그 저변의 판단은 알고리즘에 기반이 된 판단이 중심적 지위를 차지하게 된다. 이는 달리 말하여 알고리즘 기반 규제(algorithmic regulation)를 의미하는 것이다. 종국적으로 인간의 행위를 규제 또는 제약하는 것은 알고리즘이라는 의미이다.

이러한 알고리즘 시대는 향후 더욱 가속화될 것으로 전망된다. 비단 인공지능의 활용뿐만 아니라, 세상의 모든 사물 등 존재들이 디지털화하여 연결되는 소위 디지털 전환(digital transformation) 시대가 급격하게 진척되고 있기 때문이다. 디지털 전화는 이제까지 정보통신기술을 바탕으로 급속하게 성장해 온 데이터 집적 기반과 함께, 그러한 데이터들을 분석하고 활용하는 방법이 혁신적이고 비약적인 발전에 터 잡고 있다. 이러한 분석 및 활용 방법은 종국에 알고리즘에 기반을 두고 있고, 이제 도처에서 알고리즘에 기반을 둔 판단들이 존재하게 될 것으로 보인다.

## 알고리즘의 인식론적 논제

알고리즘에 기반을 둔 판단은 다음과 같은 윤리적 쟁점을 가지고 있는 것으로 판단된다. 우선 인식론적 차원에서의 문제점을 정리해보면 다음과 같다.

### 1) 불확정성

인공지능 및 그 알고리즘은 불확정성(indeterminacy)을 가진다.<sup>1)</sup> 이는 안정적인 판단 준거 기준 설정 및 확인 상의 어려움이 발생한다는 점을 의미한다. 인공지능 및 그 알고리즘은 현재의 기술 방식에 따라 보자면 데이터의 학습을 통해 알고리즘을 구축하고 수정해 나가는 속성을 가진다. 그런데 종래 곳곳에 존재하는 데이터는 기준 자체를 도출하기 어려운 비선형적 속성을 가지고, 다양한 과정을 통해 생산되는 데이터 자체도 상당히 비체계적이거나 무질서한 현실을 반영하는 경우가 빈번하다. 따라서 이를 기준으로 구성되는 알고리즘도 이러한 속성을 반영할 수밖에 없다. 또한 데이터 학습을 통해 구성된 알고리즘도 실제 엔지니어의 의도를 넘어서서 새로운 판단 기준들을 정립해 나간다는 측면에서, 때에 따라서는 예견 가능성을 벗어나는 경우가 발생할 수 있다.

### 2) 이해 불가능성

인공지능 및 그 알고리즘은 이해 불가능성을 가진다. 이는 앞서와 마찬가지로 데이터 및 알고리즘에 대한 인간의 이해 불가능성을 의미한다. 인류는 그간 상당한 수준의 과학기술 문명을 이룩해 왔지만, 아직 모든 문제 사안에 대한 해답이 있는 것은 아니다. 좀 더 현실적으로 인간은 아직 세상에 대해 아주 미약한 부분만을 알고 있다고 할 수 있다. 즉 곳곳에 존재하는 데이터를 인간의 방식으로 이해하는 데에는 한계가 발생한다. 그리고 이에 따라 이러한 데이터를 통해 구성되는 알고리즘에 대한 이해에도 한계가 있을 수밖에 없다.

### 3) 의도적 왜곡 가능성

이상과 같은 불확정성과 이해 불가능성을 넘어서서, 상황을 더욱 복잡하게 만드는 것은 인간의 의도적인 의미의 왜곡 가능성이다. 즉 현존하는 데이터와 알고리즘은 그 자체가 자연적으로 존재하는 것이라기보다는 인간의 의도가 개입된 경우가 빈번하다. 이는 인간이 인위적으로 자신의 의도를 투영하기 위해 데이터와 알고리즘을 생산해 낸다는 의미이다. 그러나 일반적으로 데이터와 이에 대한 학습은 매우 객관적으로 이루어진다는 환상을 가지고 있다. 따라서 인간의 의도가 보이지 않게 데이터와 알고리즘에 개입하여, 보이지 않는 판단 기준으로 도처에서 작동할 수 있다는 가능성을 배제할 수 없는 상황이다. 이러한 문제는 최근 사회과학적 차원에서 논란이 되는 가짜뉴스(fake news)와 대형 포털 및 SNS의 기사 배열 등이 이와 연관성을 가지고 있는 사안이라고 할 수 있다.

1) 인공지능과 관련하여 이에 대해 직접적으로 언급하고 있는 문헌으로는 Jack M. Balkin, "The Path of Robotics Law", California Law Review Circuit 6, 2015이 있다. 물론 볼킨의 논의는 인공신경망 기술의 구조를 전제로 하고 있다기 보다는 다차원적인 데이터의 결합으로 불확정성이 증대된다는 설명을 하고 있는 특성이 있다.

## 알고리즘의 규범론적 논제

알고리즘에 기반을 둔 판단이 가지는 윤리적 차원의 문제와 직결되는 규범론적 논제들을 정리해 보면 다음과 같다.

### 1) 불법적인 결과 산출

규범론적 관점에서 가장 문제시되는 것은 알고리즘을 통한 판단이 산출해 내는 불법적인 결과이다. 인간이 개입하지 않은 상황에서 기계적 판단이 산출해 낸 결과가 불법적인 성격을 가지는 경우는 현 단계에서도 쉽게 상정할 수 있다. 예를 들어 자율주행 자동차가 자체적인 판단에 따라 운행하는 과정에서 사람을 다치게 하거나 사망에 이르게 하는 경우가 이에 해당할 수 있다. 이는 인간의 관점에서 보자면 과실로 인한 경우도 있을 수 있고 고의에 의한 경우도 있을 수 있다. 그러나 기계가 불법적인 결과를 산출하는 경우에는 고의 및 과실 여부를 판단할 수도 없고, 때에 따라서는 불필요할 수도 있다. 종국적인 판단의 책임은 그러한 불법적인 결과 산출에 인간이 어떠한 방식으로 개입할 여지가 있었는지가 될 것이다. 궁극적인 책임은 어쨌든 인간에게 귀속될 수밖에 없기 때문이다.

### 2) 산출 결과 영향의 불확정성

데이터와 이에 대한 학습을 통해 구성된 인공지능 알고리즘의 불확정성의 문제는 앞서 언급한 바와 같다. 그런데 더 큰 문제는 그러한 알고리즘을 통해 산출된 결과가 사회의 다양한 영역에 미치는 영향 또한 정확하게 예측하기 어렵다는 문제가 있다. 종래 인간의 판단 결과가 사회 등에 미치는 영향에 대해서는 오랜 시간을 거치면서 어느 정도 예측이 가능해졌고, 이로 인한 역기능 발생에 대해 인간은 상당 시간 동안 적절한 대응방안을 구축해 왔다. 그러나 인간 개입이 최소화되고 대규모적이고 매우 빠른 속성을 가지는 기계적 판단 결과로 인한 영향에 대해서는 아직 사회적인 예측 시스템이 완성되어 있지 않다고 볼 수 있다. 결국, 이러한 영향이 확정될 수 있을 때, 제도적인 관점에서의 대응방안을 마련해 볼 수 있을 것이다.

### 3) 인과관계 파악의 난관

이제까지 전통적임 법규범은 특정 사안에 관한 인과관계(因果關係) 파악을 핵심 요인으로 하는 체계를 취하고 있었다. 즉 특정인의 판단과 이에 근거한 행위가 다른 주체의 권리 또는 법익을 제약하는 경우에, 그러한 판단과 행위에 대해 법적 제한을 가하는 체계였다고 할 수 있다. 그러나 문제는 앞서 언급한 인공신경망(artificial neural network)의 구조상 그러한 인과관계를 명확하게 확정하는 데에 한계가 발생할 수 밖에 없다는 문제점이 발생한다. 즉 인공지능 알고리즘은 특정 데이터들을 학습하고 그 결과를 반영하여 자율적으로(인간의 개입 없이) 알고리즘을 수정해 나가는 구조로 되어 있다. 따라서 인공지능이 어떠한 데이터를 학습하고 또한 왜 그러한 판단을 하게 되었는지를 정확하게 파악하기 힘든 경우가 발생할 가능성이 크다.<sup>2)</sup>

## 상정 가능한 규범적 대응방식의 유형

### 1) 전문가 윤리적 접근

일반적으로 매우 빠른 기술 변화가 존재하거나, 사안의 파악을 위해 매우 전문적인 식견이 요구되는 경우에는 외부적 규제는 실효성을 가지기 힘든 측면이 있다. 전문가가 아닌 제3자적 지위에서 관련 사안의 정확한 실체적 관계를 파악하기도 힘들거나 이해하기도 어렵기 때문이다. 이럴 때 활용되는 것이 바로 윤리적인 접근이다. 즉 전문가 집단의 자발적인 참여와 협력을 전제로 스스로 전문가 통제를 달성할 수 있도록 하는 방안이라고 할 수 있다. 인공지능 연구의 경우 상당히 빠르게 변화를 거듭하는 영역일 뿐만 아니라 매우 전문적인 기술 영역이라고 볼 수 있어, 이러한 윤리적 차원의 접근이 타당한 측면이 있다.

이와 관련한 사례 중 하나는 「생명윤리 및 안전에 관한 법률」 제7조 등의 국가 생명윤리심의위원회 및 제10조 기관 생명윤리위원회 등의 규정이다. 생명윤리 분야는 인공지능 분야와 마찬가지로 매우 첨단 기술의 영역이라고 할 수 있을 뿐만 아니라, 관련 위험이 매우 전면화할 가능성이 높다고 할 수 있다. 따라서 국가적 차원의 전문가 윤리 통제 업무를 수행하는 국가생명윤리심의위원회를 규정하고 있으며, 개별 관련 연구 기관별로 기관생명윤리위원회를 두도록 규정하고 있다. 기관 위원회를 별도로 두도록 하는 것은 연구 기관의 자율성을 보장하여 연구의 수월성을 보장한다는 취지도 가지고 있는 것으로 볼 수 있다.

### 2) 인증체계의 구축

인증체계를 구축하는 방식의 접근은 최근 행정규제에 관한 일종의 흐름에 가깝다고 할 수 있다. 즉 인허가 또는 행위 규제 요건 등을 법령상 규정하여 직접 규제하는 방식이 아니라, 자발적인 인증 획득을 유도하여 관련 분야 위험 관리 등의 대응 체계를 구축할 수 있도록 유도하는 방식이다.

인증체계는 국가 및 공공기관 등이 주축이 되어 운영되는 경우도 있고, 법령상 근거 없이 민간 인증사업자들이 운영하는 경우도 있다. 우리나라의 경우에는 이제까지 민간의 자발적인 참여를 유도한다는 취지를 가지고 있음에도 불구하고,<sup>3)</sup> 국가 및 공공기관 주축으로 인증체계 및 제도가 운영됐기에 국가 중심적 행정 규제로서의 성격이 강한 측면이 있다.

일반적으로 주요 국가들의 인증 관련 제도화 동향은 민간 인증사업자들의 인증을 전제로 운영되는 경우가 대다수이다. 국가가 특정 인증(예. 개인정보 보호 등) 체계를 법률적으로 규정하는 때도, 관련 인증기관 및 인증업무에 있어 민간 인증사업자들의 자율성을 존중하는 방향으로 운영된다. 대표적으로 EU의 경우에는 개인정보 보호와 관련한 인증의 경우에도 민간에서 구성된 인증기준을 승인 및 활용하는 상황이라고 볼 수 있다.<sup>4)</sup>

2) 기술적으로는 인공지능 관련 서비스의 출시에 앞서 엔지니어들은 테스트 또는 실험 과정을 통하여 일부 파라미터 조정 등의 개입을 할 수 있는 것은 사실이다. 그러나 현재 인공지능 기술의 논의의 핵심을 그러한 인위적인 개입 자체가 줄어들 것이라는 관념이 전제되어 있는 것이다.

3) 물론 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 정보보호 관리체계 인증(ISMS)의 경우에는 특정 규모 이상 사업자들에게는 법률상 인증 의무를 부과하고 있다. 그러나 이는 인증체계의 기본 취지에 부합하지 않는다는 평가가 지배적이다.

### 3) 개인적 권리의 설정

이는 인공지능 알고리즘의 투명성을 확보하기 위하여, 그러한 알고리즘을 개발 및 서비스하는 사업자들에게 이용자들에게 알고리즘 구조와 영향을 알려주도록 하고, 이용자들로서는 그에 대한 설명을 요청할 수 있도록 하는 규제방식을 의미한다. 이는 전통적으로 개인정보 자기결정권을 보장하고 있는 법제들이 취하고 있는 보편적인 방식이라고 할 수 있다. 즉 개인정보를 정보주체로부터 수집, 이용 및 제공하기 위해서는 수집 목적 등 관련 사항에 관한 정보를 정보 주체에게 제공해 준 연후에 정보주체의 동의를 받아야 한다 (well informed consent). 물론 이러한 권리설정적 접근 방식은 비단 개인정보 보호규제 영역에 한정해서만 논해지는 것은 아니다. 종래 좀 더 포괄적인 이용자의 설명 요청권의 유형은 우리나라의 「약관의 규제에 관한 법률」을 예시로 확인할 수 있다.

세계적으로는 이 부분의 논의가 상당한 반향을 일으키고 있는데, 이는 EU GDPR을 기반으로 한 설명요청권(right to explanation) 담론이 상당한 영향을 미치고 있다. 설명요청권은 GDPR 프로파일링 관련 조항에 있어 특정 알고리즘이 가지는 로직과 그 영향을 정보 주체에게 알려주어야 한다는 규정 내용으로 비롯된 것이다. 물론 관련 규정 본문에 이에 대해 명확하게 권리성을 부여하고 있는 것은 아니지만, 해석 및 추론을 통해 그 권리성을 확인할 수 있다는 입장으로 이해해 볼 수 있겠다.

### 4) 직접적인 행정 규제 설정

더욱 직접적인 행정규제를 설정하는 방식은 현 단계에서 심도 있는 논의가 이루어지고 있지는 못하다. 그 이유는 아직 인공지능 기술의 기술 방식 중 보편적 지위를 가지고 있는 것이 존재하지 않을 뿐만 아니라, 향후 기술발전의 맥락이 어떠한 방향으로 흐를지도 명확하게 예측하기 힘들기 때문이다. 다만 인공지능 알고리즘 기술의 불확정성 또는 블랙박스적 성격에 주목하여, EU의 Civil Law Rules in Robotics에서는 이에 대한 규제방향을 포괄적으로나마 언급하고 있다.

이러한 직접적인 행정규제 조항들은 매우 다양한 내용과 수준에서 발견할 수 있지만, 인간의 개입 및 관리 가능성을 확보한다는 수준에서 활용 가능한 규정들은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하, 정보통신망법)에서 상당수 발견할 수 있다. 가장 대표적으로 동법 제29조는 정보통신서비스 제공자들이 개인정보를 처리할 때에는 개인정보의 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 기술적 · 관리적 조치를 하여야 한다고 규정하면서, 세부적으로는 △개인정보를 안전하게 처리하기 위한 내부관리계획의 수립 · 시행, △개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치 · 운영, △접속기록의 위조 · 변조 방지를 위한 조치, △개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술 등을 이용한 보안 조치, △백신 소프트웨어의 설치 · 운영 등 컴퓨터바이러스에 의한 침해 방지조치, △그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치 등과 같은 세부적인 기준들을 나열 및 명시하고 있다.

---

4) EU GDPR 제42조(인증) 및 제58조(권한)

## 법 패러다임 전환 관점의 수용 필요성

인공지능 기술의 도입 및 활용으로 인해 발생할 수 있는 역기능에 대비하기 위해 상정할 수 있는 다양한 규범적 대응방식은 좀 더 궁극적으로는 과거와 같은 법체계를 유지할 수 없는 상황을 보여주는 측면도 있다. 왜냐하면, 앞서 언급한 인공지능 알고리즘에 관한 인식론적 논제와 규범론적 논제를 고려해 본다면, 그 어떠한 대안도 현재 상황에서는 확정적이라고 논하기 힘들기 때문이다. 그렇다면 우리는 법 패러다임의 전환까지도 고려하는 대응책을 고민해 보아야 한다.

법진화론적 측면에서, 근대 초기의 법은 형식적 정의의 실현이라는 데에 초점을 맞추었다고 한다면, 비교적 최근의 다원주의 경향 하에서는 절차법적 정의의 실현이 강조되어 왔다. 형식적 정의 실현 요청은 근대 이전에 실질적 정의를 추구한다는 미명하에 정당화되었던 자의성 및 재량을 감소시키기 위해 등장했다고 할 수 있다. 형식적 정의에 치중한 나머지 사회의 다원적 가치를 수용하는 데에는 한계가 발생했고, 그러한 가치들을 수용하기 위해 형식과 실질이라는 가치의 중간지점에서 경쟁하는 가치들이 소통할 수 있는 절차가 강조되게 된 것이다. 근대 자유주의적 법규범은 모두에게 동일한 기준으로 적용된다는 일반성을 가지며, 이러한 속성은 형식적 정의에 입각한 기준 설정을 통해 달성될 수 있었다. 그러나 거시적인 관점에서 보면, 절차 그 자체도 일정 부분 형식적 정의로 재차 귀결된다고 볼 수밖에 없다.<sup>5)</sup> 즉 법의 일반성이라는 속성이 상당 부분 유지되는 상황에서 강조되는 절차는 사실상 절차에 관한 형식성 강조에 지나지 않는다. 결국, 현재 법의 진화 단계는 형식주의에서 또 다른 실질주의로 진화(변화)하는 과도기적 상황을 의미하는 것으로, 그것이 바로 절차주의라고 칭해지게 된 것이라고 선해해 볼 수도 있다.

물론 실질주의로의 법 진화가 근대 이전의 실질주의와 동일한 것은 아니다. 역사적 경험에 근거하여 향후 법의 진화는 과거와는 다른 차원과 방식의 실질주의로 흘러갈 가능성이 높다. 인공지능의 활용이 일상화되는 경우 규제 대상과 환경이 매우 유동적으로 변화할 것이기 때문에, 상황에 맞는 실질적 정의를 매우 빠르게 추구하면서도 과거 형식주의적인 법이 추구하던 가치들까지도 상당부분 보존할 수 있는 새로운 법의 역할이 요청된다.<sup>6)</sup>

이와 관련하여 언급할 수 있는 것은 노넷과 셀즈닉(Philippe Nonet & Philip Selznick)의 응답적 법(responsive law)에 관한 관념이다.<sup>7)</sup> 이들은 법의 진화 단계를 억압적 법(repressive law), 자율적 법(autonomous law), 응답적 법(responsive law)으로 구분한다.<sup>8)</sup>

5) Roberto Unger, 김정오(역), 『근대사회에서의 법』(삼영사, 1994), 252면.

6) Roberto Unger, 위의 책, 281-286면.

7) 노넷-셀즈닉의 법진화론에 관한 설명으로는 양건, 『법사회학』(아르케, 2004), 237-242면; 양천수, 앞의 논문, 177-179면 참조.

8) Philippe Nonet & Philip Selznick, *Law and Society in Transition: Toward Responsive Law*(Harper & Row, 1978). 이 책의 국문 번역본은 정동호·신영호(역), 『법과 사회변동』(나남, 1986)이 있다.

‘억압적 법’이란 억압적 권력에의 봉사자로서의 법을 의미한다. 여기에서 법은 원칙적으로 무제한 재량권을 가진 주권자의 명령일 뿐이다. ‘자율적 법’은 억압을 약화하고 사회통합을 보호할 수 있는 분화된 제도로서의 법을 의미하며, 일반적으로 ‘법의 지배’라고 칭해지는 통치체계를 말한다. 마지막으로 ‘응답적 법’이란 사회적 필요와 기대(aspiration)에 부응하는 촉진제(facilitator)로서의 법을 의미하며, 이는 실용주의적·합목적적 법을 강조하는 입장이라고 할 수 있다.<sup>9)</sup> 자율적 법은 근대사회 이후 발전해 온 전통적·지배적 법패러다임이라고 할 수 있고, 응답적 법은 향후 법적 진화의 방향이라고 할 수 있다.

이들이 응답적 법이라는 새로운 법 유형 또는 패러다임을 언급하고 있는 원인으로는 다음과 같은 것들이 있다. 첫째, 법적 추론에 있어 목적의 우위 또는 지배 현상(법형식주의 탈피), 둘째, 법적 권위의 약화(법적 의무 및 공공성 등의 관념 변화), 셋째, 법의 개방성과 융통성 요청에 따른 참여의 증가(법의 정치화), 넷째, 법의 정당성 보다는 역량(실질적 목적달성 가능성)의 중시(재판보다는 행정규제 중심)가 그것이다. 이러한 법패러다임 원인들은 기본적으로 앞서 언급한 인공지능 및 4차 산업혁명과 연관한 법규범적 차원에서의 난점들과 연계되어 있다고 볼 수 있다.

#### 노넷과 셀즈닉의 법진화론

	억압적 법	자율적 법	응답적 법
법의 목적	질서	정당화	권능(competence)
정당성	사회방위와 국익	절차적 공정성	실질적 정의
법적추론	자의적, 개별적	법적 권위 중시 (형식주의 및 법률주의)	목적적
재량	광범위	협소(입법에 의한 제한)	목적 구속의 전제 하에 확대

물론 이 글에서 응답적 법으로의 패러다임 전환을 모종의 법칙이나 진리라고 주장하는 것은 아니다. 다만 과거 전통적인 법의 속성인 형식성과 이를 근간으로 하는 법치행정의 원리는 상당한 변화에 직면하고 있다는 문제를 제기하고 있는 것이다. 물론 근대 자유주의 정립 이후 복지국가 및 조합국가 패러다임의 도입으로 자유주의 법체계의 형식성이 일정부분 약화된 측면이 없지 않지만, 인간의 내면으로 침투해 오는 인공지능 알고리즘 및 유관 기술들은 그러한 형식성의 약화를 더욱 가속화시킬 것으로 보인다. 즉 예측이 어려울 뿐만 아니라 복잡한 이해관계가 얹힌 상황에서, 빠른 기술 변화와 그로 인한 위험에 대응하기 위해서는 법집행기관이 현재보다는 다소 확대된 규제 재량을 보유해야 하고, 그에 다른 법패러다임 전환이 불가피하다.

이를 위해 법규범적 측면에서는 당해 법령의 목적을 명확히 하고, 이에 대한 구속을 전제로 법 집행기관의 대응 재량을 다소 포괄적으로 규정하는 방안이 요구된다.

9) 이에 관한 보다 구체화된 설명으로는 심우민, “인공지능과 법패러다임 변화 가능성: 입법 실무 거버넌스에 대한 영향과 대응 과제를 중심으로”, 「법과 사회」 제56호, 2017 참조.

실제로 다차원적이고 신속한 환경 변화가 전제된 상황에서는, 법치행정 원리에 입각한 전통적인 법적 규제와 같이 모든 규제 요건들을 사전에 법에 명확하게 규정해 두기 어려운 측면이 있다. 따라서 현대 입법에 있어서는 일반조항과 같은 다소 포괄적인 입법기술의 활용이 증가하고 있는 상황이다. 이는 입법 및 행정 편의라기보다는 변화하는 법현실에 대응하기 위한 불가피한 대응방식이라고 할 수 있다. 이렇게 될 경우 입법 문구(법문)의 명확성보다는 입법 ‘목적’의 명확성이 더 중요한 의미를 가진다고 할 수 있다.

## 변화에 대응하기 위한 담론전략의 우선성

### 1) 규범적 대응담론의 전환

앞서 언급한 바와 같은 응답적 법 패러다임으로의 전환은 인공지능 알고리즘 시대에서는 불가피할 것으로 보인다. 즉 형식적인 법적 대응방식에 관한 요건을 사전에 예측하고 명확히 규정하는 것이 어려운 상황이고, 이는 인공지능 기술이 보편화 된 이후에도 마찬가지로 발생할 수밖에 없는 문제라고 할 수 있다. 따라서 인공지능 알고리즘 시대의 입법정책 담론은 단순한 규제 강화나 완화(폐지)를 정답으로서 제시하려는 것이 아니라, 향후 관념적 변화가 어떤 방향으로 진화할 것인지에 대해 명확하게 인식할 수 있는 토대를 마련하는 데 주력해야 할 필요가 있다. 특히 응답적 법 패러다임으로의 진화 상황을 고려해 본다면, 입법정책 담론은 규범적 대응이 추구해야 하는 ‘목적’에 관한 합의에 기여할 수 있어야 한다.

이러한 측면에서 세계 주요 국가들은 법적 규제 강화 및 완화에 주력하기보다는 인공지능 알고리즘에 관한 윤리적 원칙이나 사회 운영의 원칙을 설정하기 위해 노력하고 있다. 물론 이들 국가에서도 입법적인 대안 모색에 관심이 없는 것은 아니지만, 먼저 윤리 기준과 원칙을 정립하고 이에 입각하여 세부적인 입법 대안들을 마련해 나가고자 하는 전략을 취하고 있다.<sup>10)</sup>

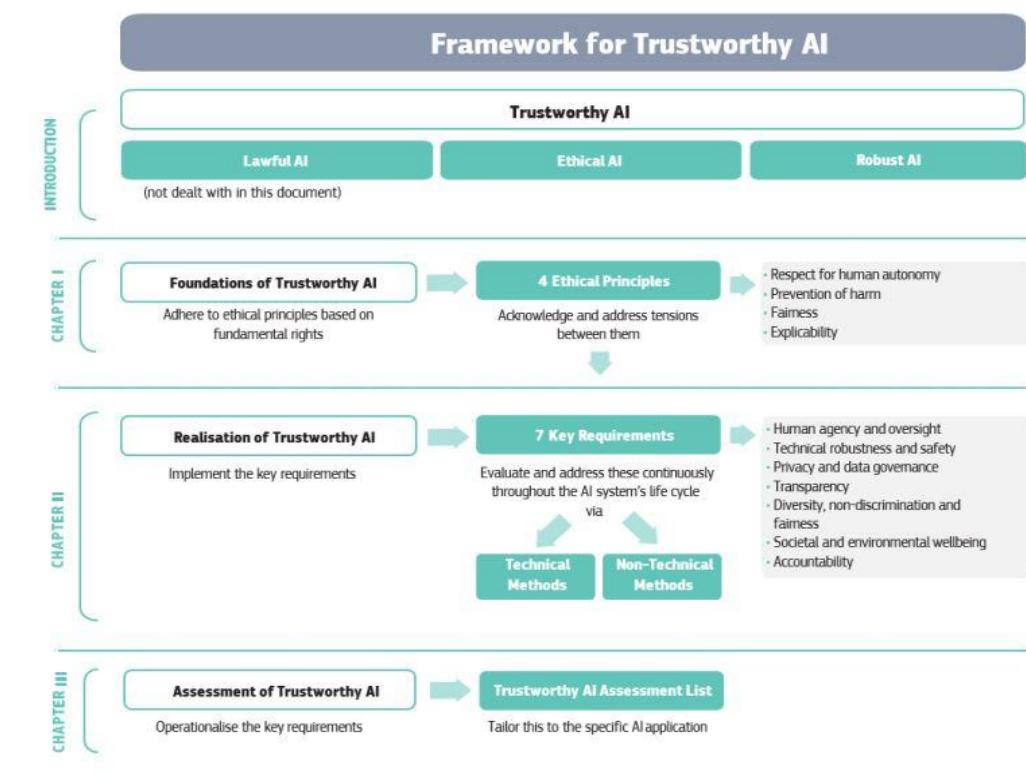
우리나라도 이와 유사한 정책적 동향이 존재하는 것이 사실이다. 대표적으로 정부부처 및 정부 출연 연구 기관들을 중심으로 다양한 인공지능 윤리 가이드라인 및 헌장 등을 제시하기 위해 노력해 왔으며, 정부의 4차산업혁명위원회는 해커톤 등의 과정을 거치면서 규범적 대응방안을 선도하기 위해 노력해 왔다. 그러나 문제는 해외 주요 국가들의 경우 입법적 해결 적이나 규범적 대안을 단기적으로 찾는 데 몰두하지 않고, 담론적 공감대를 형성해 나가기 위한 전략을 취하고 있다는 점에 주목할 필요가 있다.

10) 이러한 견지에서 주목할 만한 문헌들로는 다음과 같은 것들이 있다. The European Commission's High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019.4.8; Guidance: UK Department for Digital, Culture, Media & Sport, Data Ethics Framework, 2018.8.30; CNIL, The ethical matters raised by algorithms and artificial intelligence: how can humans keep the upper hand?, 2018.5 등.

## 2) 참조 사례로서의 유럽연합

이와 관련하여, 가장 좋은 참조 사례로 유럽연합이 있다. 유럽연합의 유럽위원회는 2018년 12월 18일 신뢰 가능한 AI 윤리지침(Ethics Guidelines for Trustworthy AI)을 공표하였다.<sup>11)</sup> 지침 안은 인공지능(AI)이 사회에 가져올 긍정적 요소를 최대화하면서도 위험성을 최소한으로 억제할 수 있는 ‘신뢰할 수 있는 AI’를 실현하기 위한 목적으로, 유럽위원회가 창설한 52명의 고위전문가그룹(High-Level Expert Group)으로 이루어진 전문 부회가 정리하였다. 해당 지침안은 내년 1월 18일까지 의견 공모를 거쳐 내용을 수정하고 이해관계자 간 협의를 통해 2019년 4월 8일 최종적인 윤리지침으로 발표하였다.<sup>12)</sup>

### 유럽연합의 신뢰 가능한 AI 프레임워크



[출처: The European Commission’s High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019.4.8., 8면.]

해당 지침은 개인과 사회에 엄청난 혜택을 가져다줄 가능성을 지닌 AI는 상당한 위험을 내포하기에 제대로 올바르게 관리되어야 함을 강조하고 있다.

11) The European Commission’s High-Level Expert Group on Artificial Intelligence, Draft Ethics Guidelines for Trustworthy AI, Brussels, 2018.12.18.

12) The European Commission’s High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019.4.8

나아가 전반적으로 AI를 통한 이득이 그에 따른 위험보다 크다는 점을 고려하여 AI의 장점을 극대화하는 동시에 위험을 최소화하는 방향으로 나아가기 위해서는 ‘인간 중심의 접근 방식’(Human-centric approach)을 통해 ‘신뢰할 수 있는 AI’를 개발해야 한다고 주장한다.<sup>13)</sup>

해당 지침은 3개의 장으로 나누어 신뢰할 수 있는 구조를 규정하고 있다. 제1장에서는 AI가 준수하여야 할 기본권, 원칙, 가치를 규정하여 AI의 윤리적 목적(Ethical Purpose)을 보장하고자 하였으며, 제2장에서는 윤리적 목적과 기술적 건전성을 모두 다룰 수 있는 ‘신뢰할 수 있는 AI 실현 지침’을 제공한다. 마지막으로 제3장에서는 신뢰할 수 있는 AI에 대한 구체적인 영향평가 목록을 제공하여 요구사항이 실제로 준수될 수 있도록 하였다.

위 신뢰 가능한 AI 윤리지침과 관련하여 우선 참조해야 하는 사항은 위 지침을 만들기 위해 단순히 전문가들의 의견 제시에 그친 것이 아니라, 다수의 이해관계자로부터의 의견을 공개 수렴하고 또한 그 결과를 공표하고 있다는 점이다.<sup>14)</sup> 즉 단순히 전문가 집단의 의견을 반영하여 결과를 알고 형식적인 청문 절차를 거지는 우리와는 사뭇 다른 접근이라고 할 수 있다. 물론 이러한 접근 방식은 유럽연합이나 서구 국가들에서는 새로운 것이 아니다. 대부분의 입법 및 정책 사안들에 관해서는 영향평가(impact assessment)가 이루어지고 있으며, 그 과정에서 공개적인 문서화를 통한 의견수렴(consultation)은 필수적인 절차이다.<sup>15)</sup>

또한, 위와 같은 지침은 확정적인 대안으로서 기능하는 것이 아니라, 지침 자체에 지속적인 영향평가 절차(Assessment of Trustworthy AI)를 규정하고 있으며, 이런 맥락에서 2019년 6월 26일부터 영향평가의 시범절차를 진행하고 있다. 이 과정은 역시 정량적인 측면에서의 영향평가는 물론이고 의견수렴 과정을 필수적으로 언급하고 있다.<sup>16)</sup>

## 담론전략으로서 영향평가 절차의 제도화 필요

인공지능 알고리즘 시대에 대비하기 위해 각국은 치열한 고민을 시작하고 점차 그 성과들을 제시하고 있다. 이는 우리나라로도 마찬가지인데, 개별 정부부처들은 물론이고 각 정부출연 연구기관들도 이러한 움직임에 동참하고 있다. 그러나 해외 주요 국가들의 대응방식과 우리의 대응방식에는 다소간에 상이함이 존재한다. 그 것은 바로 면밀한 영향평가 및 담론형성 절차가 존재하는지 여부라고 할 수 있다.

13) 인공지능 기술이 현재 상황에서는 초기 단계라는 것을 감안하여 개발 단계에서의 윤리적이거나 규범적인 기준을 강조하는 것은 또한 주요 국가들의 공통점이라고 할 수 있다. OSTP, The National Artificial Intelligence Research and Development Strategic Plan, 2016; 総務省 情報通信政策研究所 調査研究部『A.I開発ガイドライン』, 2016 등 참조.

14) 실제 유럽연합은 위 지침의 초안을 발표한 이후 500여 건의 의견을 접수하였고, 그 세부 내용과 이에 대한 피드백 사항들을 문서화하여 공개하고 있다. 이에 대해서는 <https://europa.eu/!cJ43wn> 사이트를 참조할 것.

15) 이에 대해서는 심우민 외, 『국정과제 이행을 위한 과학기술 법체계 중장기 발전방향 연구』(국가과학기술자문회의, 2018)를 참조할 것.

16) <https://europa.eu/!bC37vJ> 참조.

해외 주요 국가들의 경우에는 영향평가 결과를 사회에 제공하고, 이를 기반으로 더욱 발전적인 대안을 다소 장기적인 관점에서 형성하기 위하여 노력하고 있다. 앞서 살펴본 EU뿐만 아니라 영국, 미국, 일본, 프랑스 등 대부분 국가들은 이러한 전략을 취하고 있는 것으로 볼 수 있다.

우리나라의 경우에는 현 정부 출범 이후 4차 산업혁명이라는 기치 아래 규제혁신 정책을 추진해 나감과 아울러, 각종 윤리 가이드라인과 현장을 고민해 왔다. 그러나 다른 국가들과 다른 점이라고 한다면 즉자적인 대안 제시에만 주력해 왔다고 평가할 수 있겠다.

예를 들어, 4차산업혁명위원회에서는 이해관계 당사자들의 논의를 거쳐 개인정보 보호법제 등 입법적인 개선방안들을 정부에 제언하였고, 이를 마치 정부의 규제혁신 정책 추진의 성과인 것처럼 홍보하였다. 그러나 이는 궁극적으로 최근 데이터 3법 등에 관한 현실 입법 과정에서 확인할 수 있는 것처럼 시민사회의 강력한 반발에 부딪히고 있다. 이는 담론적 합의보다는 이해 당사자 간의 정치적 타협과 그 결과를 중시하는 맥락이 불러온 당연한 결과이다. 실제로 어떤 근거로 4차산업혁명위원회 해커톤에서 그런 결정을 하였는지, 세부적으로 어떤 이해관계 당사자가 어떤 발언을 하였는지 등도 공개되어 있지 않다. 더욱 심각하게는 그러한 대안들에 대해 시민사회 의견을 수렴하는 공개적이고 공식적인 절차도 없었다. 만일 4차산업혁명 위원회 해커톤의 입법적 건의 사항을 그대로 국회에서 의결한다고 하더라도, 이를 둘러싼 갈등은 향후에도 지속될 것이고, 또한 그런 맥락에서 매우 불안정한 규범적 상황은 지속될 것이다. 그러므로 담론적 공감대 형성 절차로서의 영향평가 절차의 제도화가 필수적이다.

물론 우리나라에도 다른 주요 국가들과 마찬가지로 정책 및 법안 등의 검토(영향평가) 절차와 이해관계자 의견수렴 절차(담론적 합의절차)가 형식적으로나마 일부 존재한다고 볼 수 있다. 그러나 우리나라에서 이러한 절차는 도출된 정책이나 법규범적 대안을 정당화시키기 위한 부수적인 절차로서의 의미만을 가질 뿐이다. 따라서 장밋빛 미래에 관한 전망을 제시하기에 앞서, 현실적·구체적인 전망과 이에 관한 사회적 공감대를 구축할 수 있는 담론절차로서의 영향평가 절차를 제도화하는 것이 현재로써는 가장 긴요한 국가적인 규범적 대응방안이다.

# 아세안의 사이버보안 국제협력 현황



박성림 (sunglimpark@naver.com)

국립정치대학(대만) 정치학연구소 박사수료  
(前) 국립타이베이간호건강대학 교양교육센터 강사

## 아세안: 서구와 비서구의 경쟁지대

2008년 세계금융위기가 발발한 지 10여 년이 지난 오늘날 사이버보안은 세계 각국 정부, 기업 및 사회가 가장 관심을 가지는 이슈로 떠오르고 있으며, 특히 탈냉전 시대에 접어들어 유일한 패권국인 미국과 미국 주도 질서에 대해 의문을 품고 있는 러시아, 중국과 같은 비서구 국가 간의 이익이 가장 첨예하게 충돌하는 이슈다. 이들의 의견충돌은 2017년 UN GGE 리포트 채택 실패뿐 아니라 이들 국가의 상이한 사이버보안 전략에서 드러나는 관점 차이에서 잘 드러난다.

아세안은 1960년대 중반 국제전으로 확산하는 베트남전과 인도차이나반도의 공산주의 무장 세력이 급격하게 점총하는 것에 대한 공동대응을 위해 인도네시아, 태국, 말레이시아, 필리핀 및 싱가포르 등 5개국이 창설한 지역공동체로, 2017년 기준 회원국은 10개국으로 증가했으며, 역내 인구는 약 6.4억 명에 달한다. GDP는 2조 7,615억 불(전 세계 GDP 3.45%)이며, 회원국들의 평균 경제성장률은 5%에 달하고, 인구의 60%가 35세 이하로 무궁한 성장잠재력을 가지고 있다. 회원국들의 대외관계를 살펴보면, 싱가포르, 인도네시아가 미국과 긴밀한 협력관계를 유지했지만, 캄보디아와 라오스는 전통적으로 중국의 우호 국가로 평가되고, 베트남의 경우 1990년대 미국과 수교한 동시에 기존 우방국인 러시아와 긴밀한 협력을 통해 미국과 비서구 국가 간의 균형을 유지하고 있다. 이같이 복잡한 아세안 국가들의 대외관계는 오늘날 서구-비서구 구도 중심의 사이버공간 논의의 현실과 매우 흡사하다. 그렇다면, 서구와 비서구의 힘이 교차하는 아세안이 오늘날 어떻게 사이버공간 협력을 추구하고 있는지를 알아보는 것은 작게는 아세안이라는 신흥 지역공동체의 사이버공간에 대한 인식과 협력을 확인하는 방법이 될 것이며, 크게는 서구-비서구 구도의 사이버공간 논의과정에서 아세안의 대응을 검토함으로써 우리의 방안을 구성하는데 참고할 가치가 있다고 본다.

본고는 아세안의 사이버보안 국제협력 현황을 검토함으로써 아세안이라는 신흥시장이자 제3의 길을 걷는 지역 협력체가 서구 국가와 비서구 국가와의 협력을 통해 어떠한 사이버보안을 구현하려는 지에 논의하고자 한다. 이를 위해서 제2절과 제3절에서는 아세안 차원에서의 사이버보안 협력 채널과 아세안과 싱가포르 간의 협력 채널인 사이버보안 장관회의를 검토하고자 하며, 제4절에서는 아세안과 일본, 중국, 유럽연합 간의 협력으로 세분화해서 아세안 내 주요 논의경로를 확인하고자 한다. 아세안은 현재 정례 정상회담과 더불어 아세안+3(한·중·일) 정상회담, 정보통신 장관회의에서 사이버보안 협력을 논의하고 있으며, 싱가포르 주도의 사이버보안 장관회의 또한 중요한 채널이다. 제5절에서는 이 같은 협력 현황이 보여주는 의의와 더불어 우리나라가 향후 아세안과 어떠한 사이버보안 협력을 추진할지에 관한 밑거름을 약술함으로써 본고를 마무리하고자 한다.

## 아세안의 사이버보안 국제협력(I): 아세안 내 협력 채널 현황

아세안의 사이버스페이스 협력은 △아세안 자체의 사이버공간 협력(정상회담-정보통신 장관회의 및 사이버보안 장관회의, ARF), △아세안-싱가포르 사이버공간 협력과 더불어 △아세안-미국, 일본, 중국 및 EU와의 국제협력으로 구분할 수 있다. 우선 아세안 정상회담(ASEAN Summit)은 매년 개최되는 아세안 회원국 및 유관국가 정상들이 회동하는 회의체이며, 2017년 제34차 정상회담에서 아세안 사이버보안 선언문(ASEAN Leaders' Statement on Cybersecurity Cooperation)을 채택한 바 있다. 2017년 제32차 정상회담에서 채택된 사이버보안 협력 선언(ASEAN Leaders' Statement on Cybersecurity Cooperation)에는 △사이버공간을 위협이자 경제성장의 기회로 인식, △다양한 분야의 각기 다른 주체들의 참여에 따른

조율, △회원국들의 사이버보안 정책, 역량구축, 국제협력 조율 및 협력체계 구성, △UN 현장 및 2015년 UNGGE 리포트의 사이버공간에 대한 적용, △국가 주권과 국제규범의 사이버 상 적용 인정, △공통적이고 자발적이며 비구속적인 사이버 상 국가 행위 규범 수용을 통한 신뢰 강화 등이 명시되었다.

우선 사이버공간을 “위협이자 기회”로 보는 인식은 사이버 상에서 증가하는 범죄, 테러리즘, 해킹 등을 지적하는 한편, 위협에만 매몰되지 않고 이 같은 위협을 해소하는 과정에서 관련 산업 성장 및 취업 증가를 지목한 것은 적어도 중국, 러시아와 같은 비서구 국가의 사이버공간에 대한 인식과 차이가 있으며, 또한 사이버공간의 안정적 이용에 방해가 되는 해킹, 테러, 범죄행위만을 언급하고 정치적 콘텐츠를 언급하지 않은 점도 비서구 국가들과는 확연히 다른 점이다. 두 번째로, 유엔현장과 2015년 UNGGE 리포트를 비롯한 현행 국제규범의 사이버공간에 대한 적용을 들 수 있다. 사이버공간을 기준 육상, 해상 및 공영과 다른 공간으로 보고 이에 관한 국제법을 제정해야 할지는 오랫동안 논의되어왔으며, 아세안은 미국, 유럽연합과 같이 기존 국제법의 적용 가능함을 인정했다. 마지막으로, 국가의 사이버공간에서의 행위 규제를 들 수 있으며, 협력 선언은 공통적이고 자발적이며 비구속적인 규범 수용을 방안으로 제시했다. 이는 기존 국제법 및 현재 국가들로부터 받아들여져서 규제를 할 수 있는 최소한의 틀을 인정하고, 여기에서 사이버보안 국제 거버넌스를 시작하자는 것으로 해석된다.

두 번째로, 아세안 정보통신 장관회의(ASEAN Telecommunications Ministers Meeting, Telmin 이하 ‘텔민’ 약칭, 2001~현재)를 들 수 있으며, 2005년에 개최된 제3회 장관회의에서 처음으로 사이버보안을 위해 △2004년까지 모든 회원국의 인터넷침해사고대응팀(Computer Emergency Response Team, CERT) 설치 및 운영 추진, △공동 사이버위협 및 취약점 진단 프레임워크 구축, △위협 정보교류 합의가 합의문에 명시되었다. 제6회 (2006) 회의부터 (2015) 회의까지는 △네트워크 보안 보장, △아세안 내 사이버보안 유관기구 활동성과 (아세안 정보통신 감독평의회, 아세안 인터넷침해사고대응팀, 아세안 네트워크보안 행동 평의회) 및 국제협력성과(아세안-일본 주요 정보통신 기반시설 보호 가이드라인 수립 및 아세안-일본 사이버 보안 협력 허브, 아세안-중국 CERT 사이버사고 유형 리스트 및 정보공유 프로토콜 처리 과정 합의), 아세안 사이버보안 협력전략(ASEAN Cybersecurity Cooperation Strategy), 사이버보안추진 방향(다양한 분야의 주요 주체들을 중심으로 하는 사이버보안 구현) 등이 논의되었다. 텔민에서 논의된 사항을 검토해보면, 구체적인 사안에 대한 확인과 더불어 향후 어떻게 회원국들이 자국 내에서 어떻게 사이버보안을 추진할지에 관한 방향 제시가 눈에 띈다. 2017년 회의에서는 정부, 기업, 학계, 비정부기구 등 다양한 분야의 다양한 주체들의 참여를 통한 사이버보안의 구현이 언급되었으며, 이는 기존의 활동 열거에서 벗어나 처음으로 아세안 국가들의 사이버보안 거버넌스 방향을 제시했다는 점에서 의미를 지닌다.

### 아세안 사이버보안 주요 협력 채널

아세안 회의체	싱가포르-아세안 협력기구	아세안-해외국가 협력기구
아세안 정상회담		
아세안 국방장관회의		
아세안 정보통신 장관회의		아세안-인터폴 : 아세안 사이버역량개발 프로젝트
아세안 사이버보안 장관회의		아세안-일본 사이버보안 협력 허브
아세안지역안보포럼		
아세안 정보통신 감독평의회		
아세안 네트워크보안 행동평의회		
아세안 인터넷침해사고대응팀		

세 번째로, 아세안지역안보포럼이 있다. 2001년 7월 25일 베트남 하노이에서 개최된 제8회 ARF 외무장관회의 성명에 처음으로 사이버 범죄가 언급되었으며, 사이버 테러리즘(2002년과 2006년), 사이버보안 및 사이버 테러리즘 전문가 화상 회의체 구성(2008~2009년), 사이버 범죄 및 테러리즘 대응과 관련해 러시아를 선도국으로 선정(2010), 사이버보안 강화를 위한 협력(2012~2013년), 사이버 범죄(2014년, 2018~2019년) 등이 보도 자료에 명시된 바 있으며, 대체로 원론적인 입장 표명에 그치고 있다. 또한, ARF 지원을 통해 개최되는 사이버보안 세미나<sup>1)</sup>가 있으며, 우리나라는 2004년 및 2007년 제주 및 부산에서 개최한 바 있다. 주요 논의주제로는 △사이버 공격 및 테러리즘, △각국 정책(사이버테러 및 공격 대응, 정보통신 주요시설 보호) 및 기술소개, △CERT 현황 및 협력, △ARF 회원국 간 협력방안, △민간 기구 대응 현황 등이 있었다. 특이한 점으로는 2004년 세미나에 북한 외무성 관계자 4명이 참석한 바 있다. 관례로 북한은 남북한 회의 외에 남측에서 개최되는 국제회의에 정부 당국자를 파견한 예시가 없었으며, 2004년 회의 참석은 남북한이 모두 가입한 ARF가 지역 평화 조성뿐 아니라 남북한 교류 협력에 도움이 된다는 것을 보여준 사례이다.

### 아세안의 사이버보안 국제협력(II): 싱가포르의 역할

2016년부터 추진되고 있는 아세안 사이버보안 장관회의(The ASEAN Ministerial Conference on Cybersecurity)는 싱가포르 주도로 추진되는 회의체로 평가된다. 사이버보안 장관회의는 싱가포르 사이버보안원(Cyber Security Agency of Singapore)의 사이버보안주간 활동 내에 개최되며, 사이버보안의 성격, 인식 제고, 2015년 UN GGE리포트를 기반으로 한 규범 구성, 아세안 사이버역량구축 프로그램

1) ASEAN REGIONAL FORUM, LIST OF TRACK I ACTIVITIES YEAR 1994 - 2018(Classified by subject)  
<http://aseanregionalforum.asean.org/wp-content/uploads/2019/01/List-of-ARF-Track-I-Activities-1994-2018-by-Subject-as-of-August-2018-1.pdf> (검색 일자: 2019.8.20)

(ASEAN Cyber-Capacity Programme)이 논의되었다. 네 번째로는 아세안지역안보포럼(ASEAN Regional Security Forum)이다. 사이버보안과 관련한 기구로는 외무장관회의와 사이버보안 세미나를 들 수 있다. 아세안지역안보포럼은 1994년 5월에 창설되었으며, 아세안 회원국 10개국과 우리나라, 미국, 일본 등 10개 대화 상대국과 7개 기타 회원국 등 총 27개국으로 구성되어 있다. 주요 논의주제는 국제 및 역내 안보 정세와 더불어 역내 신뢰 구축 조치, 예방외교 등이 있으며, 주요 회의체로 외무장관회의와 고위관리 회의(SOM)가 있으며, 사이버보안과 관련해서 아세안 지역 포럼과 27개 구성국이 공동개최하는 사이버보안 세미나가 있다.

2018년에 설립된 아세안-싱가포르 사이버보안 전문센터(The ASEAN Singapore Cyber Security Centre of Excellence)는 아세안 사이버역량 프로그램(ASEAN Cyber Capacity Programme)의 일환으로 싱가포르의 사이버보안 규범 및 사고 대응 경험과 교육을 공유하는 매개체이다. 주 교육 분야로는 사이버보안 규범(△국제법, △국내 법규 및 정책 수립, △분쟁 대응 방안) 및 사고 대응 매뉴얼(△공격 대응 실무경험, △방어 대응 및 관련 훈련)이다.

### 아세안의 사이버보안 국제협력(III): 타국과의 협력

아세안은 비단 아세안 회원국 간의 협력뿐 아니라 비회원국가, 국제기구와도 긴밀한 협력관계를 통해 사이버역량 및 협력 채널 구축 강화에 나서고 있으며, 대표적으로 일본, 중국, 유럽연합, 미국 및 러시아 등이 있다. 우선 일본은 아세안과 긴밀한 협력관계를 유지하는 국가로서 2018년에 설립된 아세안-싱가포르 사이버보안 전문센터가 대표적인 협력사례라고 하겠다. 일본 주도로 이미 아세안-일본 주요 정보통신 기반 시설 보호 가이드라인(ASEAN-Japan Critical Information Infrastructure Protection Guideline)이 제정되었으며, 2017년 텔민에서 아세안-일본 사이버보안 역량강화센터(ASEAN-Japan Cybersecurity Capacity Building Centre) 설립이 확정되었고, 또한 아세안-일본 사이버보안 협력 허브(ASEAN-Japan Cybersecurity Cooperation Hub) 수립이 결정되었다. 마지막으로, 아세안 사이버역량발전(ASEAN Cyber Capacity Development Project)은 일본-아세안 협력 강화기금(Japan-ASEAN Integration Fund)의 지원을 받아 아세안과 인터폴(Interpol)에서 2016~2018년에 시행한 프로젝트이며, △국가별 사이버 정책 검토, △전문가 훈련(380명 교육 수료)과 더불어 세미나(사이버 범죄 및 위협 대응) 개최 및 경험 공유 등이 추진된 바 있다.

일본 외에 부각되는 국가로는 중국을 들 수 있으며, 중국은 인터넷침해사고 대응센터를 주도로 기술적 협력에 주력하고 있다. 2014년 9월 18일 광시좡족자치구 난닝에서 중국-아세안 사이버공간 포럼이 개최된 바 있고, 2016~2018년 인터폴 글로벌 혁신체계 일환으로 아세안 사이버역량발전 프로그램(ASEAN Cyber Capacity Development Project)이 시행되었다. 또한 아세안-중국 CERT 사이버사고 유형 리스트 및 정보 공유 프로토콜 처리 과정 합의(ASEAN-China Computer Emergency Response Teams(CERTs)

사이버사고 유형 리스트, 정보공유 프로토콜 및 처리 과정 수립이 핵심이 된 바 있다. 미국의 경우 다소 늦었는데, 2013년 7월 1일 브루나이에서 개최한 미국-아세안 장관급회의에서 해양안보와 사이버보안, 특히 사이버보안 및 사이버 범죄 대응에 관한 긴밀한 협력을 기대한다고 표명했으며, 이는 일본과 중국과 비교 시 아직 시작단계에 있다고 볼 수 있다.

## 의의 및 시사점

이렇듯, 아세안은 정보통신 장관회의 및 사이버보안 장관회의와 아시안 지역 안보 포럼을 통해 아세안 국가 모두가 수용 가능한 정책 개발뿐 아니라 인력훈련 및 사고 대응에 나서고 있으며, 또한, 일본과 중국을 통해 부족한 지원 자원을 수용하고 고급인력훈련에도 박차를 가하고 있다. 이 같은 국제협력에서 가장 중요한 채널로는 아세안 정상회의, 정보통신 장관회의, 사이버보안 장관회의와 아세안-일본 간의 협력이 있으며, 특히 협력의 방향과 구체적인 정책 기조가 정보통신 장관회의에서 논의되고 있다. 우선 정상회의에서 논의된 사이버공간의 성격은 “위협이자 기회”이며, 사이버공간은 열려있는 무한한 기회의 공간도, 부적절한 정보 유통에 따른 위협 증대도 아니다. 위협적 측면의 경우 사이버 범죄, 테러리즘 및 해킹으로 이는 비단 아세안뿐 아니라 서구, 비서구 국가 모두가 직면하는 이슈이며, 또한 아세안의 사이버보안이 여전히 성장단계에 머물러 있음을 보여주는 방증이라고 하겠다. 또한, 경제성장의 동력으로 보는 시각은 적어도 아세안이 사이버공간의 성장성을 주목하고 있고, 서구, 비서구의 특정 국가에 치우치지 않고 있음을 보여준다. 두 번째로, 사이버 범죄 및 테러리즘 문제를 들 수 있다. 아세안 구성 국가들을 들여다보면, 싱가포르처럼 경제, 사회적 발전 수준이 비약적으로 올라온 국가와 더불어 태국, 베트남, 인도네시아 등 개발도상국이 있고, 또한 라오스, 미얀마와 같은 저개발국가가 있다. 구성 국가 간의 경제, 사회적 발전의 차이로 인해 발생하는 사이버 범죄가 상이할 수 있고, 대응 인력 및 자원 또한 차이가 날 수밖에 없는 실정이다. 정보통신 장관회의 논의사항을 잠시 짚어보면 사이버위협 및 취약점 진단 프레임워크 구축, 사이버사고 유형 리스크 공유와 같이 실제 범죄 및 테러리즘에 대응하는 방안들이 제시된 것은 이 지역에서 가장 중요한 이슈는 기본적인 범죄 및 테러리즘 대응임을 보여준다. 세 번째로, 싱가포르의 역할이다. 앞서 언급했듯이, 싱가포르는 사이버보안 장관회의 개최의 실질적 구성원이며, 여기에서 논의된 사이버보안 성격과 인식 제고, 규범 구성을 아세안의 사이버보안의 수준을 제고시키는 동력이다. 향후 아세안의 사이버보안을 심층적으로 논의하기 위해서는 실질적 논의를 주도하는 싱가포르의 사이버보안 현황을 살펴볼 필요가 있으며, 특히 규범 구성을 주도하는 정부 및 학계를 주목해야 한다.

이를 볼 때, 아세안의 사이버보안은 성장기에 머물러 있음을 알 수 있고, 일본과 더불어 중국이 아세안과의 협력을 강화하고 있으나 여전히 협력 이슈는 다양하다고 하겠다. 우선, 사이버위협 대응에 관한 경험 공유 및 교육지원을 들 수 있다. 현재 싱가포르와 더불어 인터폴, 중국, 일본에서 사이버위협 대응 교육을 지원하고 있으나, 언론에서 보도된 훈련 인력 수는 백여 명 수준임을 확인해볼 때, 향후 아세안 관련 ODA

예산에 사이버보안 분야를 추가해서 아세안과의 사이버보안 협력을 추진할 필요가 있다. 우리나라는 2000년대에 들어 아세안과의 ICT 분야의 교육, 훈련을 지원하고 있으나, ICT 기술 분야에서 안정적 협력이 이루어지기 위해서는 기술보안은 절대적으로 필요하다. 이를 고려하면 기존 기술협력뿐 아니라 사이버보안 협력이 필요하고, 이를 공공기관뿐 아니라 민간 대학에 위탁하는 형식으로 아세안 국가의 공무원, 기업 관리자, 대학원생의 사이버보안 교육을 지원하는 방안을 검토해볼 필요가 있다. 마지막으로 싱가포르를 중심으로 논의되는 아세안 사이버보안 규범을 심층적으로 검토해야 한다. 필자는 본고를 쓰며 정보통신 장관회의 및 사이버보안 장관회의에서 정책 방향뿐 아니라 아세안 사이버보안 전략과 더불어 규범 제정에 관한 논의를 언론 보도로 확인했다. 그러나 구체적인 전략과 규범에 관한 문서가 검색되지 않아서 정리에 어려움을 겪었다. 향후 아세안의 사이버보안 전략, 규범에 관한 정책연구 및 조사 분석이 뒤따라야 하며, 이를 통해 “아세안의 사이버보안”에 관한 심층적인 이해가 있어야 우리나라와 아세안 간의 사이버보안 협력이 강화될 것이다.

#### [참고문헌]

- [1] 외교부, 『아세안 개황』(서울, 2018년), 14-17.
- [2] 신남방정책특별위원회, 신남방정책. <http://www.nsp.go.kr/policy/policy02Page.do> (검색 일자: 2019.8.19).
- [3] 최경희, 「2018년 아세안공동체 현황과 한·아세안 관계 그리고 2019년 전망」, 『정세와 정책』, 2018년 제20호(2018.12.17), P.2.
- [4] 주 아세안대표부, 2015.12.27., 「ASEAN 공동체[ASEAN Community]」 비전 2025.
- [5] ASEAN, 16 Oct, 2012, Joint Media Statement of the Third ASEAN Telecommunications & IT Ministers
- [6] ASEAN, September 18th, 2006, JOINT MEDIA STATEMENT Sixth ASEAN Telecommunications &IT Ministers Meeting, Brunei Darussalam
- [7] ASEAN, 24 August, 2007, Seventh ASEAN Telecommunications&IT Ministers Meeting(7<sup>th</sup> TELMIN).
- [8] ASEAN, 29 August, 2008, The 8<sup>th</sup> ASEAN Telecommunications&IT Ministers Meeting
- [9] ASEAN, 16 November, 2012, Joint Media Statement of the 12<sup>th</sup> ASEAN Telecommunications and IT Ministers Meeting and its Related Meetings with Dialogue Partners.
- [10] ASEAN, 11 Oct 2016, ASEAN Member States Call for Tighter Cybersecurity Coordination in ASEAN.
- [11] ASEAN, September 27th, 2018, Chairman's Statement of The 3rd ASEAN Ministerial Conference on Cybersecurity.
- [12] ASEAN, 6 November, 2017, ASEAN Leaders' Statement on Cybersecurity Cooperation.
- [13] Indo-Pacific Defense Forum, 2018.12.21., 「싱가포르, 지역 내 사이버 역량 강화를 위한 프로그램 추진」
- [14] CCDCOE, Keiko Kono ,ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working
- [15] OpenGov, Dean Koh, 24 November, 2017. Enhancing cybersecurity in ASEAN - Singapore announces three broad proposals at the ASEAN Ministerial Conference on Cybersecurity.
- [16] CCDCOE, Keiko Kono, ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working.
- [17] ASEAN, 1 August, 2019, ASEAN-EU Statement on Cybersecurity Cooperation.
- [18] Interpol, ASEAN Cyber Capacity Development Project(ACCDP).
- [19] ASEAN, 13 September, 2013, Joint ministerial statement of the ASEAN-Japan Ministerial policy meeting on Cybersecurity cooperation.

## 사이버보안에서 AI 활용 편익과 구현 방법



이응용 (david9631@gmail.com)

ICT&Security 애널리스트

오늘날 인공지능(AI)과 머신러닝 기술이 급속도로 발전하면서 산업 전반에 영향을 끼치고 있다. 사이버보안 영역도 예외일 수 없다. 공격자들은 AI 기술을 사용하여 자동화된 공격을 시도하고 있고, 방어자들도 신속하고 지능화된 대응을 위해 AI 기술에 대한 의존도가 증가하고 있다. 이러한 사이버 보안 환경변화에 따라 미래 사이버보안을 논의할 때 AI는 핵심적인 요소로 부상하고 있다. AI는 사이버 보안에서 기준의 탐지와 대응 역량뿐만 아니라 선제적 방어 역량을 강화할 수 있는 장점이 있는 반면, 악의적인 행위자들의 공격 속도를 증가시켜 오히려 공격의 성공 확률을 높이는 취약점을 보인다. 아울러 오픈소스 AI 라이브러리 및 소프트웨어의 확산은 신규 보안취약점을 증가시키고 있다.

최근 글로벌 컨설팅 기업인 캡제미니(Capgemini)는 소비재, 소매, 은행, 보험, 자동차, 유트리티, 통신 등 7개 산업 분야의 850명의 고위 임원을 대상으로 사이버보안에서의 AI 활용 관련 조사를 실시했다. 최고 정보책임자(CIO), 최고정보보호책임자(CISO)를 포함하여, 프랑스, 독일, 영국, 미국 등 10개 국가에 위치한 기업의 경영진 대상(850명) 설문조사와 기업·대학의 전문가 대상의 심층 인터뷰를 시행하고, 운영기술(OT) 및 정보기술(IT), 사물인터넷(IoT) 영역의 사이버보안에서 AI 활용사례를 분석하였다. 캡제미니는 조사연구와 분석 결과를 토대로 2019년 7월 “인공지능을 활용한 사이버보안의 재발견(Reinventing Cybersecurity with Artificial Intelligence)” 보고서를 발표하였다.

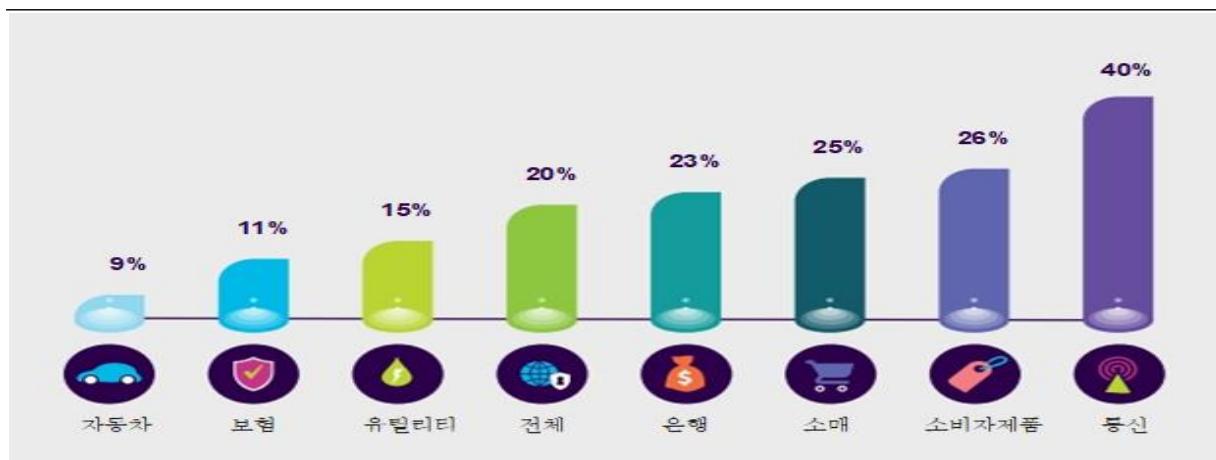
본고에서는 “인공지능과 사이버보안의 재발견” 보고서의 주요 내용을 기반으로 AI 기반 사이버보안 필요성, 사이버보안에서 AI 활용 편익, 사이버보안에서 AI 활용 중점분야, 사이버보안에서 AI 구현 로드맵 등에 대해 고찰해보고자 한다.<sup>1)</sup>

## AI 기반 사이버보안 필요성

### AI 발전에 따른 사이버위협 증가

오늘날의 기업들은 사이버보안 역량의 지속적인 강화라는 긴급하고도 중대한 도전과제에 직면해있다. 클라우드, IoT, 빅데이터, 5G, AI 등 다양한 ICT 기술의 발전과 함께 주변에 편재한 많은 기기, 네트워크, 소프트웨어 등이 복잡하게 연결되면서 사이버위협이 동시에 증가하고 있으며, 공격표면이 지속적으로 증가하고 공격의 정교성도 높아지고, 사이버 공격으로 인한 피해 규모도 증가하고 있다.

손실액 5천만 달러를 초과하는 사이버보안 침해사고



[출처: CAPGEMINI]

1) Capgemini Research Institute, Reinventing Cybersecurity with Artificial Intelligence The new frontier in digital security, 2019.7.; 본고는 이 보고서 내용을 기초로 작성하였으며, 이후 그림, 도표 등 이외에는 인용 표시 생략

캡제미니의 조사연구는 디지털 사업이 성장함에 따라 사이버 공격의 위험이 기하급수적으로 증가한다는 사실을 확인해주었다. 기업 중 21%는 자사 조직이 2018년에 불법접근으로 인한 사이버보안 침해를 경험하고, 사이버보안 위반에 대한 대가를 치르고 있는 것으로 나타났다. 기업들은 향후 1년 이내에 사이버 공격이 2배로 급증할 것으로 전망하였다. 사이버침해로 인한 피해도 대폭 증가하여, 기업 중 20%는 사이버침해로 인해 5천만 달러 이상의 손실을 입은 것으로 조사되었다. 특히 통신기업의 40%는 5천만 달러이상의 손해를 입어 피해 규모가 최대였다. 이러한 위협에 직면하여 대부분의 통신회사(80%)는 위협을 식별하고 공격을 막기 위해 AI에 의존하고 있는 것으로 조사되었다.

### 사이버보안에서 AI 의존도 증가

최근 급속히 발전한 AI는 해커 조직의 공격에 활용되는 등 사이버 위험을 한층 고조시키고 있다. 보안 기업인 ZeroFox의 데이터과학자는 실험을 통해 AI 시스템이 스피어피싱(spear phishing) 트윗(수신자가 민감한 정보를 공유하도록 속이는 개인화된 트윗)을 성공적으로 전송하는 것을 입증하였다. 이 실험에서 AI는 스피어피싱 트윗을 사람보다 약 6배 빠르게 전송하고, 약 2배 이상의 공격 성공률을 보이는 것으로 나타났다.<sup>2)</sup>

산업별 사이버위협 대응에서 AI 의존 비율



[출처: CAPGEMINI]

또한 네트워크 트래픽이 빠르게 증가하고, 보안로그 등 사이버보안 데이터도 급증하는 빅데이터 시대를 맞이하여 사이버보안 분석가들이 기존 보안 도구로는 현대의 사이버 공격을 신속히 탐지하고 대응하기 어려워지는 상황에 직면하고 있다. 기업 경영진 중 61%는 AI를 이용하지 않는다면 심각한 위협을 식별할 수 없다고 인정했다. 아울러 신속한 대처가 필요하거나 사이버보안 분석가가 신속하게 치료할 수 없는

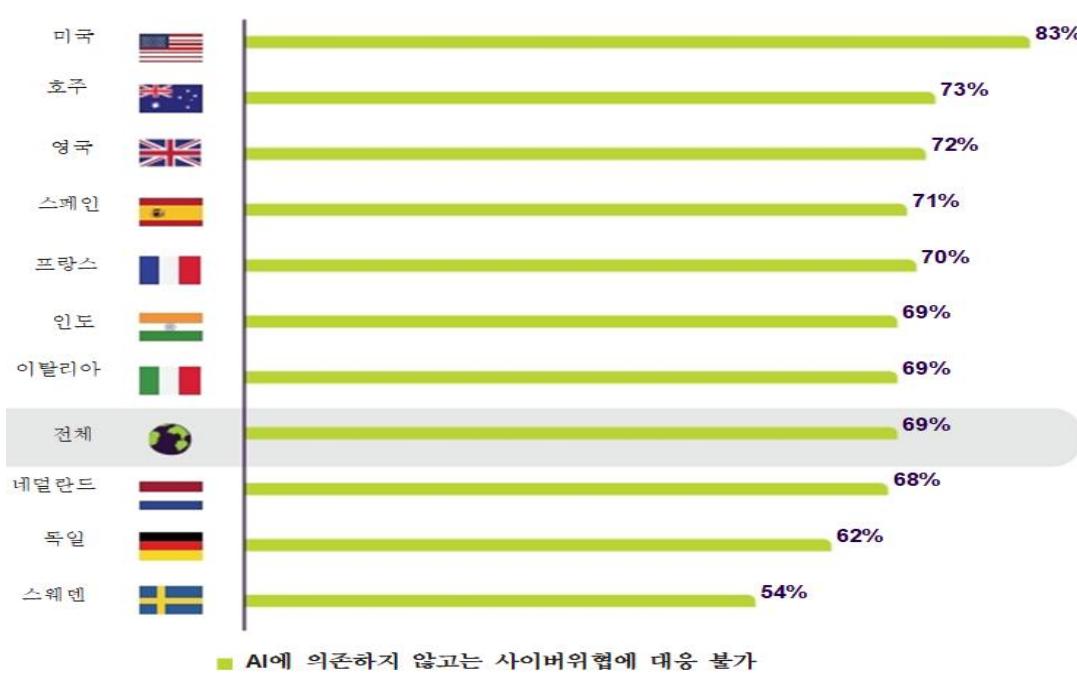
2) Raconteur, "AI in cybersecurity: a new tool for hackers?", 2019.2  
<https://www.raconteur.net/technology/ai-cybersecurity>

사이버 공격 유형도 증가하고 있다. 경영진 중 43%는 기계적인 속도의 사이버 공격이 증가하고 있다고 지적했으며, 기업들의 69%는 AI를 이용하지 않고는 신속한 공격에 대응할 수 없다고 인식하는 것으로 조사되었다. 아울러 사이버 공격 패턴의 변화로 기업 중 약 절반(48%)은 2020년도에 사이버보안에서 AI 예산을 평균적으로 29% 증액하고, 기업 중 약 1/4은 40% 이상 증액할 계획인 것으로 조사되었다.

사이버보안 기술의 부족으로 사이버 공격의 수와 복잡성이 증가하고 있는 반면, 기계학습 등의 분야에서는 AI를 활용하여 사이버보안 인력 부족을 일정 부분 해소할 수 있을 것으로 기대된다. 기업의 69%는 사이버 공격에 대응하기 위해 AI가 필요하다고 응답하였다. 특히 통신업계는 5천만 달러가 넘는 손실이 발생하면서 심각한 사이버침해에 대응하기 위한 AI 활용에 매우 적극적으로 나서고 있다.

국가별 사이버보안에 AI 의존 비율을 측정해보면, 미국 기업들은 사이버위협 대응에서 AI 기반 사이버 보안 애플리케이션 및 플랫폼을 최우선 순위로 두면서 AI 의존 비율이 전 세계 평균보다 14% 이상 높게 나타났다. 미국뿐만 아니라 호주, 영국, 스페인, 프랑스 주요 선진국들도 사이버보안에서 AI를 의존하는 비율이 70% 이상인 것으로 나타났다.

국가별 사이버위협 대응에서 AI 의존 비율

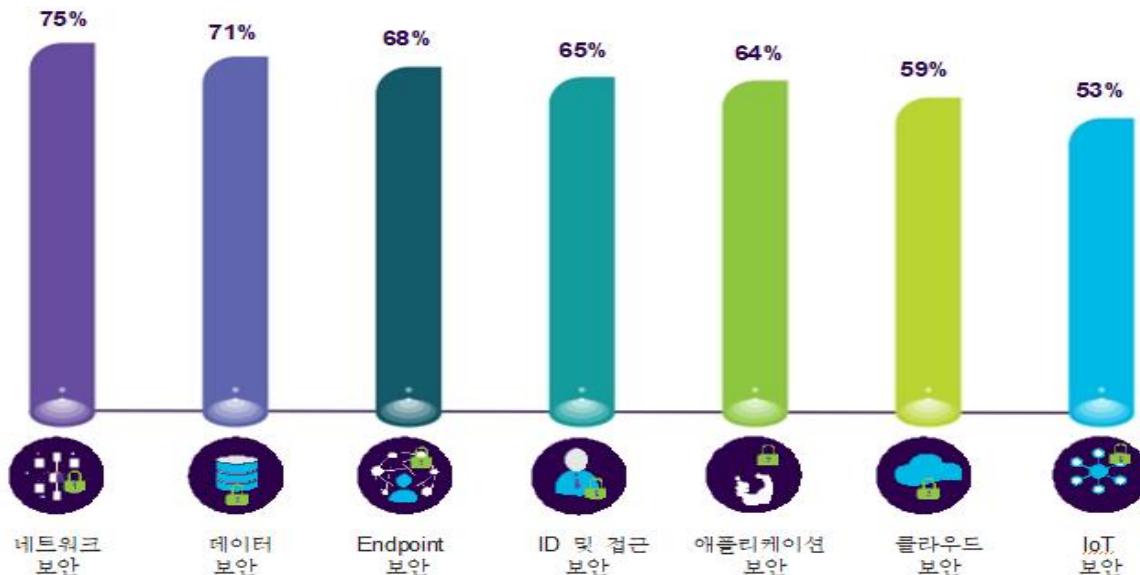


[출처: CAPGEMINI]

## 사이버보안에서 AI 활용 분야

기업들이 네트워크 보안을 위해 AI 활용 사례를 시험하는 경우가 많아졌는데, AI 활용 사이버보안 분야 중에는 네트워크 보안 분야(73%)가 가장 높았다. 데이터 기반 경제, 개인정보보호 등 데이터의 중요성이 증가하여 데이터 보안이 두 번째 순위를 차지했으며, 2021년까지 엔드포인트 기기가 250억 개 이상으로 증가할 것으로 전망되고<sup>3)</sup> (가트너), 사물인터넷(IoT) 및 산업사물인터넷(IIoT) 센서가 기하급수적으로 확대하여 위협 표면이 급증할 것으로 예상되면서 엔드포인트 보안 분야가 세 번째를 차지하였다.

기업의 사이버보안에서 AI 활용 분야

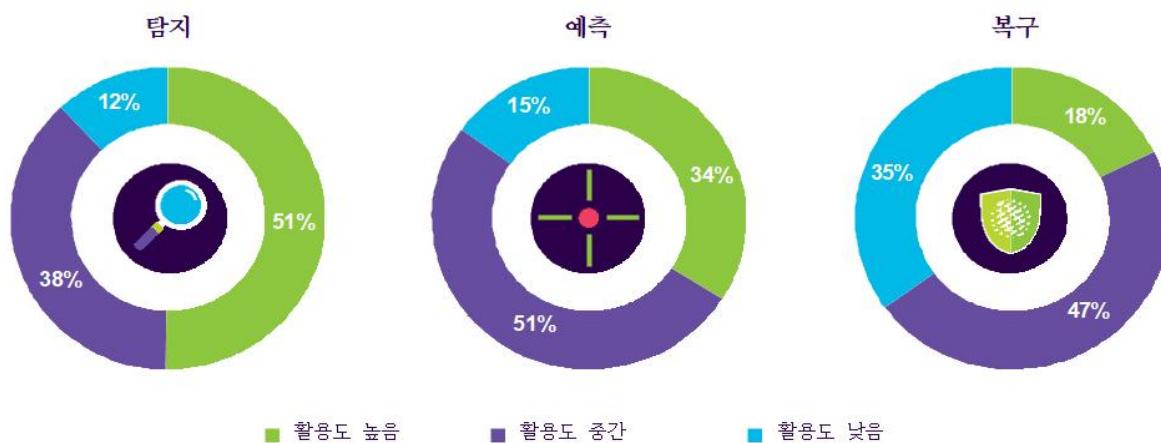


[출처: CAPGEMINI]

기업들은 사이버위협 탐지, 예측, 대응에 광범위하게 AI를 적용하고 있으며, 특히 탐지 영역에서의 AI 활용에 더욱더 많은 예산과 시간을 투자하는 것으로 나타났다. 기업 경영진들의 사이버위협 탐지 영역에서 AI를 집중적으로 활용하는 비율이 51%인 것에 비하여 예측은 34%, 복구는 14% 수준으로 상대적으로 낮았다. 기업이 사이버보안 노력의 일환으로 AI를 사용하고 채택함에 따라 기계학습의 기술이 발전하면서 예측 및 복구 분야도 점진적으로 증가할 것으로 예상된다.

3) CIO, "Top 10 strategic IoT technologies and trends: Gartner," 2018.11  
<https://www.cio.in/media-releases/top-10-strategic-iot-technologies-and-trends-gartner>

### 사이버보안 영역(탐지, 예측, 복구)별 AI 활용 비율



[출처: CAPGEMINI]

### 사이버보안에서 AI 활용 편익

사이버보안에서 AI 활용은 조직이 사이버위협 패턴을 파악하여 이용함으로써 신규 위협을 탐지하고 예측하는 기능을 개선하며, 사고 식별과 조사, 복구하는 데 필요한 시간과 비용을 절감할 수 있다. 기업 중 약 2/3인 64%는 AI가 보안 침해를 탐지하고 대응하는 비용과 시간을 단축할 수 있으며 AI는 사이버보안에 대한 투자회수율(ROI)이 높다고 인식했다. 사이버보안에 AI를 활용한 대다수 기업의 비용 절감 효과는 평균 12%로 1~15%대를 보였지만, 일부 기업은 15% 이상의 높은 비용 절감 효과를 보이는 것으로 나타났다.

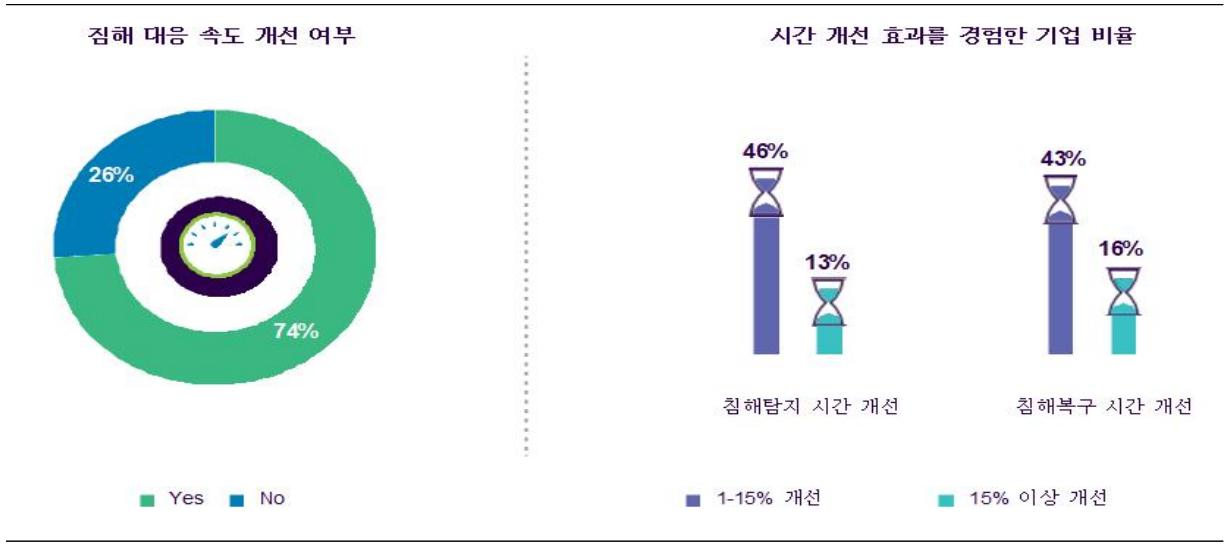
#### AI 사이버보안의 침해 탐지 및 복구 관련 비용감소 효과



[출처: CAPGEMINI]

기업에서 사이버 공격으로부터 조직을 보호하기 위해 신속한 복구가 필수적이다. 사이버보안에서 AI를 활용하면 사이버위협 및 침입을 탐지하는 데 걸리는 전체 시간을 최대 12%까지 단축할 수 있고, 침해치료, 보안 패치 등 복구에 필요한 시간도 12%까지 줄일 수 있는 것으로 나타났다.

AI 사이버보안의 침해 탐지 및 복구 관련 시간 개선 효과



[출처: CAPGEMINI]

사이버보안 시간 단축은 알려진 또는 알려지지 않은 이상 행위나 공격 패턴 등을 지속해서 모니터링하여 달성을 할 수 있다. 예를 들어 미국의 전문소매업체인 PetSmart는 Kount와의 파트너십을 통해 사기 탐지 AI를 사용하여 수백만 건의 거래와 결과를 분석하는 AI/ML(머신러닝) 기술을 구현해 최대 1,200만 달러를 절감할 수 있었다.<sup>4)</sup> 이 기술은 각 거래정보를 타 모든 거래와 비교하여 각 거래의 적법성을 판단하는 방법으로, 사기 주문이라고 확인되면 주문을 취소하여 회사의 비용을 절약하고 브랜드 손상을 피할 수 있었다.

AI를 활용한 사기 방지는 기계학습을 활용하여 이상 행위, 상관관계, 주요 변수 등을 분석함으로써 구현될 수 있다. 기계학습은 사이버 사기를 방지하는데 다음과 같은 역할을 할 수 있다.<sup>5)</sup>

- 사기 예방을 과거 경험에만 의존하지 않고 새로 등장한 활동, 행위, 예외적 거래 경향 검사
- 지급 거부가 시작될 때까지 오래 기다리지 않고, 실시간으로 사기 감지

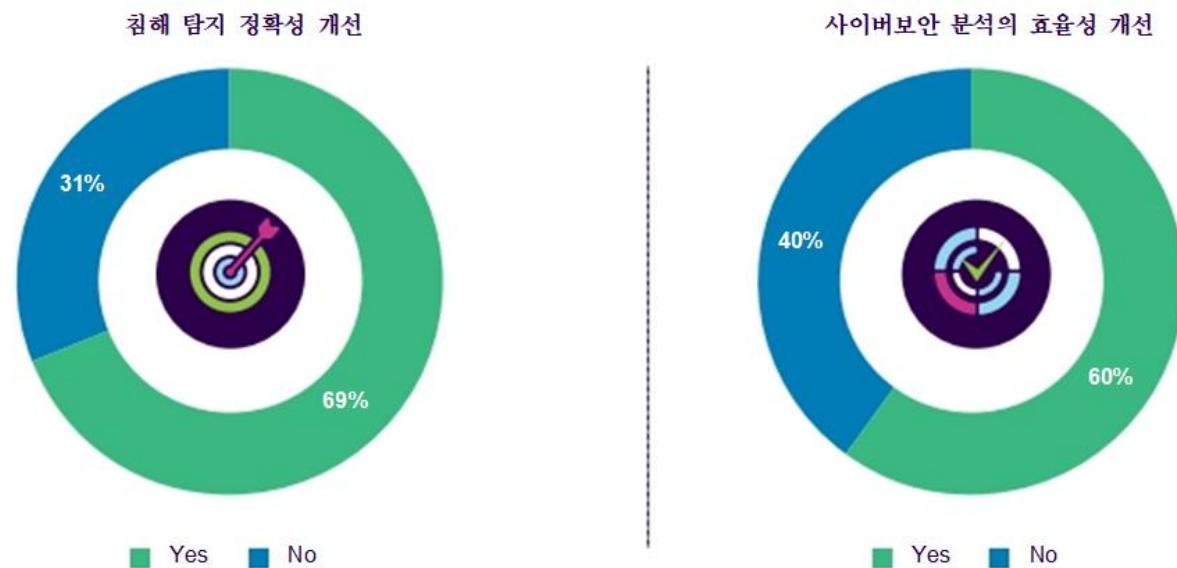
4) ZDNet, "How technology is saving PetSmart millions by eliminating sales fraud," 2018.7  
<https://www.zdnet.com/article/how-technology-is-saving-petsmart-millions-by-eliminating-sales-fraud/>

5) Forbes, Top 9 Ways Artificial Intelligence Prevents Fraud, 2019.7.9.  
<https://www.forbes.com/sites/louiscolumbus/2019/07/09/top-9-ways-artificial-intelligence-prevents-fraud/#657b322814b4>

- 친구 사칭, 판촉 남용 또는 등 정교하고 정교한 오남용 공격 방지
- 사기 분석가에게 실시간 위험정보를 제공하고 사기 손실 최소화를 위한 적정 임계값 정보 제공
- 디지털 기업이 지급거부 비율, 운영비용 등을 보다 효과적으로 통제할 수 있도록 지원
- 연중무휴 게임 등의 가상현실(VR) 상품 판매로 일관된 고품질 사용자 경험 제공
- 판매자의 쉬운 온라인 구매 승인과 AI의 탐지 오류 감축으로 고객 경험 향상
- 내부 비즈니스 정책, 규제 기관의 정책, 유통업체와의 계약 준수 등으로 AI 기반 사기 예방
- 이익에 직접적인 영향을 미치는 지불 거절 수준을 통제하여 비즈니스의 수익성 개선

사이버보안 분석가는 보안로그, 사고기록 등을 검토하는 데 상당한 시간이 소요된다. AI가 간단하고 시간이 많이 소요되는 작업을 진행하면, 사이버보안 분석가는 AI 기반 사이버보안 시스템이 파악한 사고를 분석하는 데 보다 많은 시간과 노력을 투입할 수 있다. 기업이 사이버보안 분야의 인재를 확보하기 어려운 상황에서 AI 활용은 좋은 대안이 될 수 있다. 실제로 기업 중의 약 2/3가 AI 활용이 사이버보안 분석가의 정확성과 효율성을 개선하고 있다고 인식하고 있다.

#### AI의 사이버침해 분석의 정확성과 효율성

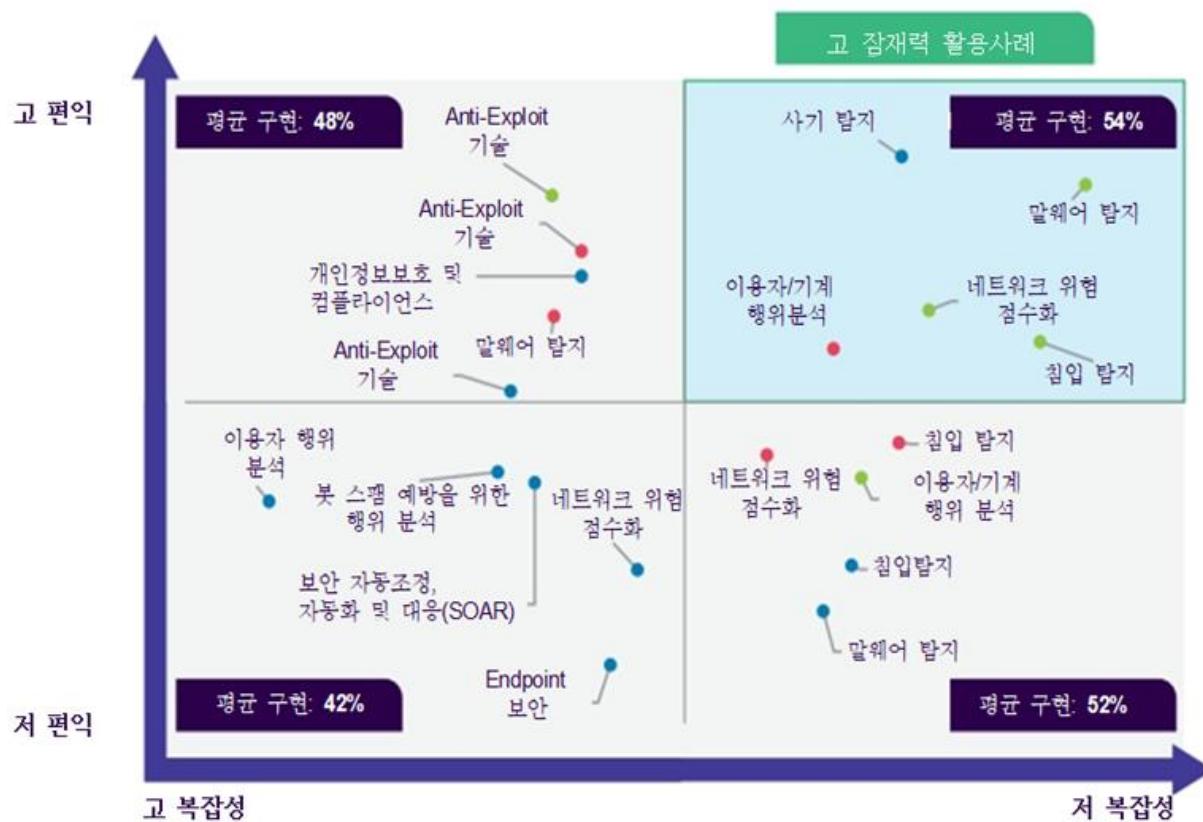


[출처: CAPGEMINI]

## 사이버보안에서 AI 활용 중점분야

AI 기반 사이버보안 시스템 가치를 최적화하고, 추가적인 투자의 정당성을 확보하고자 하는 기업에서 잠재력이 높은 활용사례를 찾는 것은 사이버보안에서 AI의 성공을 성취하는데 핵심적 요소이다. 기업의 경영진 중 57%는 구현은 쉬우면서 높은 편익을 제공하는 우수한 잠재력의 활용사례에 대한 이해가 부족하며, 이는 AI 기반 사이버보안 구현에서 도전과제라고 지적했다. 캡제미니는 정보기술(IT), 운영기술(OT) 및 사물인터넷(IoT)에 걸쳐 20개의 사용사례를 분석하고 구현상의 복잡성 및 시간 단축 측면과 같은 구현에 따른 편익에 따라 순위를 매겼다. 이를 통해 구현 복잡성은 낮으면서 편익성은 우수한 5가지 잠재적 활용사례로 사기 탐지(IT), 멀웨어 탐지(OT), 침입 탐지(OT), 네트워크 위험 점수화(OT), 이용자/기계 행위분석(IoT)을 제시하고, 기업에서 활용할 것으로 권장하였다. 조사대상 기업 중 54%가 이러한 5개의 활용사례를 이미 구현한 것으로 조사되었다. 고 잠재력 분야를 도출하기 위해 다양한 활용사례를 편익과 복잡성 수준에 따른 분류는 다음과 같다.

사이버보안에서 AI 활용사례(복잡성-편익성 매트릭스)



[출처: CAPGEMINI]

상기 도표에서 파악한 복잡성은 낮은 반면 편익은 높은 5가지 우수한 활용사례에 대한 상세한 설명과 산업계의 구현사례들은 다음과 같다.

#### 사이버보안에서 AI 활용하는 경우 권장되는 사용사례

높은 잠재력의 활용사례	설명	산업 구현 사례
네트워크 위험 점수화 (OT)	<ul style="list-style-type: none"> <li>데이터 기반으로 정량적인 위험 등급 점수 산정</li> <li>네트워크 위험 점수는 데이터 기반의 불확실성 범위뿐만 아니라 위험 수준 추정치를 제공하여 고위험을 신속히 지정</li> </ul>	<ul style="list-style-type: none"> <li>Verizon은 보안 관리 서비스에 AI 기반 Endpoint 보안 인텔리전스 기능을 적용함으로써 기업이 다양한 평가 수준에 따라 위험을 식별, 우선순위 설정, 즉각적인 보안 조치가 필요한 위험 분야에 집중하도록 지원</li> </ul>
침입 탐지 (OT)	<ul style="list-style-type: none"> <li>악의적 활동에 대해 정교하고 자동화된 통찰력을 통해 실시간으로 사이버 공격을 신속하게 탐지, 분석 및 방어</li> </ul>	<ul style="list-style-type: none"> <li>스마트 그리드(Smart Grid)에서 침입 탐지 프레임워크 및 연구 진행 중</li> <li>버클리연구소 연구팀은 사이버보안 방법론, 기계학습 알고리즘 및 센서기술을 전력망 보안 모니터링 및 분석 프레임워크에 결합하여 IP 네트워크를 통해 전력망의 침입을 탐지하는 프레임워크 구축 중</li> </ul>
이용자/기계 행위 분석 (IoT)	<ul style="list-style-type: none"> <li>인간 행위 식별을 통해 새로운 형태의 사이버 공격을 실시간으로 정확하게 탐지, 차단, 의심스러운 이용자 행위분석을 통한 침해 계정 탐지 및 시스템 보안 개선</li> </ul>	<ul style="list-style-type: none"> <li>유럽의 자율주행차 기업인 ISFM은 AI 기반의 행동 프로파일링 및 접근통제를 활용하여 해킹으로부터 자율주행차 전자 제어시스템을 보호하는 기능 강화</li> </ul>
사기 탐지 (IT)	<ul style="list-style-type: none"> <li>머신 러닝을 사용하여 거래를 실시간으로 분석하면서 동시에 사기 위협을 탐지, 금전 손실을 줄이면서 사용자 경험 향상</li> </ul>	<ul style="list-style-type: none"> <li>PayPal은 거래를 실시간으로 분석하는 정교한 딥러닝 시스템을 사용하여 사기 비율을 매출의 0.32%로 감축</li> </ul>
말웨어 탐지 (OT)	<ul style="list-style-type: none"> <li>이전에 식별한 맬웨어 특성을 사용하여 시그니처(Signature) 기반 접근방식으로는 탐지할 수 없는 잠재적 말웨어 감염 예측</li> </ul>	<ul style="list-style-type: none"> <li>Duke Energy, BP, Honeywell 등 주요 석유 및 가스 기업은 AI를 사용하여 기계의 실시간 센서 데이터를 활용하여 잠재적인 문제점과 장애를 방지하며, AI 제품은 인간의 뇌처럼 작동하여 다양한 침입을 탐지</li> </ul>

[출처: CAPGEMINI]

### 사이버보안에서 AI 구현 로드맵

사이버보안에서 AI가 제공하는 편익은 상당하지만, 많은 기업은 AI 솔루션을 구현하는 데에 어려움을 겪고 있다. 기업들은 사이버보안에서 AI 구현 관련 다양한 도전과제에 직면하고 있으며, 특히 AI의 활용 사례에 대한 개념적인 이해부터 실제적인 구현 완료 단계까지 어떻게 수행할 것인지에 대한 이해가 부족한 것으로 조사되었다. 이에 따라 캡제미니는 시스템 구현과 마찬가지로 계획단계의 중요성을 강조하면서, 사이버보안에서 AI를 구현하기 위한 체계적인 로드맵 6개 활동을 제시했다.

## 사이버보안에서 AI 구현 로드맵



[출처: CAPGEMINI]

### ① AI 운영을 위한 데이터 자료 및 데이터 플랫폼 개발

사이버보안에서 AI는 데이터 자료가 플랫폼에 연결되고 AI 알고리즘에 대한 입력으로 제공될 때 성공할 수 있다. 많은 기업은 AI 인프라 지원이 기존의 인프라, 데이터 시스템 및 애플리케이션 환경과의 통합문제로 인해 어렵다고 지적한다. 상당수의 경영진은 사이버보안 분야에서 AI를 통해 달성하려는 목표를 알고 있다고 말하지만, 기업 중 겨우 절반(54%)만이 AI 알고리즘을 운영하는데 필요한 데이터 세트를 파악하고 있는 것으로 나타났다.

기업들이 데이터 식별뿐만 아니라 고품질 결과를 원한다면 데이터를 현행화하고, 안전하게 유지해야 한다. 경영진의 절반 정도만이 데이터 세트를 AI 알고리즘의 입력으로 사용하기 위해 데이터의 현행화 및 안전성을 보장하기 위한 품질 검사를 수행하는 것으로 나타났다.

### ② 편익을 가속화하고 극대화하기 위해 적합한 활용사례 선택

투자를 정당화하는 데에 필요한 편익을 확보하려면 올바른 활용사례를 선택하여 구현하는 것이 매우 중요하다. 활용사례 선택은 사이버보안에서 AI를 활용하는 데 있어서 지속적인 과정이며, 최적의 결과에 도달하기 위해 반복 수행에 따른 시간이 소요된다. 기업들은 다음과 같은 작업 수행이 요구된다.

- 상당한 편익을 제공하지만, 구현 복잡성이 낮은 활용사례부터 시작
- 사용 가능한 데이터가 완전하고 최신인 활용사례에 초점을 맞추어 진행
- 알고리즘을 적절히 조정할 수 있도록 테스트 활용사례로부터 결과를 검증할 수 있는 전문가 확보

### ③ 위협 인텔리전스를 향상하기 위해 대외적으로 협업

크라우드 소스 플랫폼을 통한 위협 분야 연구원, 보안전문가와의 협업이 중요하다. 이를 통해 기업은 경험하고 있는 위협에 다양한 보안전문가가 신속하게 대처할 수 있고, AI 알고리즘의 논리를 개선하여 위협을 효율적으로 탐지하는 데 중요한 역할을 수행할 수 있다.

기업은 데이터 플랫폼을 구축하여 다른 조직과 최신 위협 데이터를 공유할 수 있다. 예를 들어 페이스북의 Threat Exchange 및 IBM의 X-Force Exchange는 기업이 편리한 형식으로 위협 인텔리전스를 공유하고 이용할 수 있도록 지원한다. 캡제미니 조사에서는 단지 2명의 경영진만이 크라우드 소싱 플랫폼을 통해서 외부의 기업과 위협 인텔리전스를 공유하고 있는 것으로 나타났다.

#### ④ 보안 관리를 향상하기 위해 보안 자율조정, 자동화, 복구(SOAR) 적용

보안 자율조정, 자동화, 대응(SOAR<sup>6)</sup>)은 조직이 다양한 소스에서 보안 데이터 및 경고를 수집할 수 있도록 지원하는 기술이다. SOAR 기술을 통해 인적 및 기계 능력의 조합을 활용하여 사고분석을 수행할 수 있으며, 이를 통해 데이터 자료 및 플랫폼에 대한 연결을 통해 표준적인 업무 흐름에 따라 사고 대응 활동을 정의하고 우선순위를 지정하고 추진할 수 있다. 경고 품질 향상, 사이버보안 분석가의 시간 단축, 보안 및 운영센터의 관리를 향상하는 SOAR은 사이버보안에서 AI의 최적 결과를 보장하기 위한 필수적 요소이지만 조직의 36%만이 적용하고 있는 것으로 나타났다.

#### ⑤ AI 준비를 위해 사이버 분석가에 대한 교육 훈련

기업 중 절반은 효율적으로 위협을 탐지하기 위한 AI 알고리즘을 구성하고 그 논리를 개선할 수 있는 우수한 사이버보안 전문가가 부족한 것으로 조사되었다. AI 알고리즘의 잠재적 취약점을 제거하기 위해 조직의 주요 프로세스에 대한 지식이 필요하고, 공격을 분석할 때 보안전문가뿐만 아니라 문제를 이해하는 업무 전문가 참여가 요구된다. 이러한 문제를 해결하는 한 가지 방법은 기술 발전에 따른 영향을 받은 직원들에 대한 교육을 강화하는 것일 수 있다. 사이버 분석가의 효율성을 향상하는 또 다른 방법은 직원들이 AI 도구 및 사고 경보를 활용할 수 있는 인터페이스를 구축하는 것이다.

#### ⑥ 투명하고, 윤리적으로 장기적인 개선을 성취하기 위해 사이버보안의 AI 거버너스 구축

기업은 AI 지원 사이버보안을 위한 거버넌스 메커니즘이 필요하며, 보안 및 운영센터는 다음 사항들을 지속해서 관리해야 한다.

마지막으로 행정명령 8항(AI 기술에서 미국의 우위를 유지하기 위한 실행계획)에서는 대통령 국가안보보좌관<sup>7)</sup>은 과학기술정책실(OSTP) 등과 협력하여 AI에서 미국의 우위를 유지하고, 경쟁국과 적대국들로부터 미국의 경제 및 안보 이익에 중대한 AI 기술을 보호하기 위한 실행계획 개발을 조정하도록 하였다.

이 실행계획은 AI 행정명령 발효 120일 이내에 대통령에게 보고되어야 하며 필요시 전부 또는 일부를 기밀로 유지할 수 있다.

- 사이버보안 분석가의 역할 및 책임 정의
- 작업을 실행하기 전에 사이버 분석가를 통해 AI 알고리즘 결과 모니터링 실시

6) Security Orchestration, Automation and Response

7) the Assistant to the President for National Security Affairs

- AI 알고리즘이 정상적으로 작용하는지 모니터링하기 위한 통제 절차 마련
- AI 알고리즘으로 생성된 결과에 대한 위험 허용 범위 식별
- AI 알고리즘의 결과의 논리 및 현행화를 모니터링하는 메커니즘 구현
- AI 알고리즘이 실패하거나 변조된 경우 대체 방법 마련
- 성공 여부를 측정할 수 있는 핵심 성능 지표 구현

## 사이버보안에서 AI 구현 로드맵

현대와 미래의 사이버보안에서 AI 활용은 선택이 아니라 필수로 자리매김하고 하고 있다. 주요국 및 기업들은 현대의 정교한 사이버위협에 신속하게 대응하기 위해 AI에 의존하고 있다. 많은 경영진은 사이버보안에서 AI 활용이 비용과 시간 감축 등 다양한 편익을 제공한다고 인식하고 있으며, 이에 따라 사이버 보안에서 AI 도입에 적극적이고, 투자를 확대할 계획이다.

한편 많은 기업은 사이버보안에서 AI를 활용하는 데 있어서 전문인력이 부족하고, 우선적으로 집중할 AI 활용 분야, AI 활용을 위한 체계적인 방법 등에 대한 지식과 이해가 부족하여 사이버보안에 AI를 구현하는데 어려움을 겪고 있다. 이러한 기업들은 AI 구현의 복잡성과 편익을 분석하여 조직이 집중할 분야를 선정하여 먼저 구현을 추진할 필요가 있다. 아울러 사이버보안의 구현 로드맵에서 제시한 데이터 플랫폼 개발, 고 영향 활용사례 선택, 대외적으로 협업, 자율조정·자동화·복구(SOAR) 적용, 사이버보안 분석가 훈련, 거버넌스 구축 등 6개 활동을 종합적으로 수행하면서 사이버보안에서 AI를 구현하는 것이 바람직하다.

정부 기관 및 민간기업들은 해킹 기술의 진화뿐만 아니라 신경망 기술, 컴퓨터 비전, 로봇 등 AI 관련 다양한 기술의 급속한 발전에 따라 사이버보안에서 AI 활용을 적극적으로 추진하기 위해 전문인력을 확보하고, 사이버보안 프로세스를 지속적으로 개선할 필요가 있다. 국내 보안업체들은 AI 기술 개발뿐만 아니라 기업들이 사이버보안에서 AI를 보다 편리하게 도입할 수 있도록 고객의 요구사항 분석 및 계획단계부터 시스템 구축 단계까지 종합적으로 지원할 수 있는 서비스 역량을 개발할 필요가 있다.

### [참고문헌]

- [1] Capgemini Research Institute, Reinventing Cybersecurity with Artificial Intelligence The new frontier in digital security, 2019.7.
- [2] CIO, “Top 10 strategic IoT technologies and trends: Gartner,” 2018.11
- [3] Forbes, Top 9 Ways Artificial Intelligence Prevents Fraud, 2019.7.9
- [4] Forbes, m Why AI Is The Future Of Cybersecurity, 2019.7.14
- [5] Raconteur, “AI in cybersecurity: a new tool for hackers?,” 2019.2
- [6] ZDNet, “How technology is saving PetSmart millions by eliminating sales fraud,” 2018.7

# 빅 테크 기업에 대한 미국 정부와 의회의 움직임



한상기 (stevehan@techfrontier.kr)

테크프론티어 설립자 겸 대표  
(前) 세종대학교 ES 센터 교수

## 반독점 위반, 프라이버시 침해, 사회적 책임 회피

미국 의회와 정부가 모두 나서서 하나의 주제에 일치단결하는 일은 매우 드문 일이다. 그러나 지금 미국에서는 구글, 페이스북, 아마존, 애플과 같은 소위 빅 테크 기업의 지나친 권력과 사업 실행 과정의 문제, 프라이버시 침해, 정치적 편향 등 사회적 책임에 대해 전 방위적인 조사가 이루어지고 있다.

연방 정부와 의회는 4개의 빅 테크 기업 모두에 대해 조사를 하고 있으며, 주 정부는 주로 페이스북과 구글에 대해 조사를 하는 상황이다. 연방 정부의 경우는 서로 역할 분담을 하고 있는데, 법무부는 구글과 애플에 대해서, 연방 무역 위원회(FTC)는 페이스북과 아마존에 대해 반독점 문제를 조사하고 있다.

현재 발표되고 있는 움직임만 정리해도 다음과 같은 일이 벌어지고 있다. 원래 특정 기업에 대한 조사는 대외적으로 공표하지 않는 게 관행이었지만, 이들에 대한 많은 조사를 공개적으로 선언하고 진행하고 있다.

- 구글은 기본적으로 검색 결과와 안드로이드에서 자사의 서비스와 제품에 우선권을 준다는 의심을 받고 있으며, 온라인 광고 영역을 주도하는 것이 소규모 사업자에게 불공정하다는 점이 조사 대상이다.
- 페이스북은 프라이버시 처리 문제, 허위 정보와 혐오 발언의 확산 문제로 비난받아 왔으며, 지나치게 많은 개인 데이터를 갖고 있기 때문에 사용자들이 다른 서비스를 선택할 수 없게 하고 있다는 비판을 받고 있다.
- 아마존은 자사의 플랫폼에서 사업하는 독립 상인에 대한 지식을 더 경쟁력 있는 자체 상품을 만드는 데 사용하고 있다는 의심을 받고 있으며, 애플의 경우 아이폰 앱을 만드는 외부 개발자들에 대한 문지기 역할이 지나치다는 의심과 앱 스토어 검색에서 자사 제품에 유리한 알고리즘을 사용하고 있다는 의심을 받는다.
- 2019년 2월 FTC는 테크 산업의 잠재적 반독점 위반에 대한 조사를 위해 새로운 태스크 포스를 결정했다.
- 2019년 6월 미국 법무부는 애플의 반독점법 위반에 대해 정식으로 조사에 들어갔다고 발표했다. 유럽에서도 스포티파이가 애플이 불공정한 행위를 한다고 유럽 규제 당국에 고소함으로써 애플의 앱스토어나 애플 뮤직의 독점적 위치에 문제를 제기했다.
- 2019년 7월 페이스북은 FTC가 페이스북의 반독점법 위반에 대해 조사를 시작했다고 발표했다.
- 유럽 집행위는 7월부터 아마존 플랫폼에서 판매하는 독립적인 소매상으로부터 얻은 민감 데이터를 아마존이 사용하고 있는지 평가하는 조사에 들어갔다고 발표했다.<sup>1)</sup>
- 구글의 모회사 알파벳은 8월 30일에 법무부로부터 미 정부와 다른 나라에서 있었던 과거 조사에 대한 정보와 문서를 요청받았음을 공시했다. 증권위원회에 공시한 내용에는 각 주의 법무부로부터 비슷한 조사 요청을 받을 수 있다는 예측이 있었다.
- 2019년 9월 6일 뉴욕주를 포함한 8개 주와 워싱턴 DC의 법무부 장관이 페이스북의 반독점 문제를 조사한다고 발표했다.<sup>2)</sup>

1) European Commission, “Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon,” Jul 17, 2019.

2) New York Times, “New Google and Facebook Inquiries Show Big Tech Scrutiny Is Rare Bipartisan Act,” Sep 9, 2019.

- 2019년 9월 9일 48개 주와 워싱턴 DC, 푸에르토리코의 법무 장관들이 구글의 반독점법 위반 여부를 공동 조사하겠다고 밝혔다.<sup>3)</sup> 여기에 캘리포니아와 앨라배마주는 빠졌다. DI 조사는 텍사스주의 공화당 소속 켄 팍스톤 법무부 장관이 이끌 것이며 주로 구글의 광고와 검색 서비스 비즈니스에 초점을 맞추고 있다.
- 2019년 9월 11일 연방 무역 위원회 (FTC)는 빅 테크 기업의 반독점 문제에 대해 고도의 조사를 하겠다 밝혔으며, 먼저 소수의 팀 주도로 이들의 비즈니스 실행과 잠재적 위험을 특정하기 위한 조사가 이루어졌다.<sup>4)</sup> 아마존의 경우 소규모 기업을 인터뷰하면서 기업들이 아마존에 얼마나 의존하는가를 문의하기로 했다. 많은 기업이 90% 이상의 판매를 아마존에 의존하고 있기에 아마존의 요구나 정책의 급격한 변화에 매우 취약할 수 있기 때문이다. 아마존이 유사한 제품으로 작은 상인들과 불공정하게 경쟁하고 있는가? 역시 조사 대상이다.
- 9월 12일에는 하원의 반독점 패널에서 소비자 데이터 수집의 영향에 대한 청문회가 열렸다.
- 2019년 9월 13일에는 하원 사법위원회 소속 리더와 반독점 소위원회 의원들이 4개 기업에 각각 공식 문서를 보내서 중요 정보 제출을 요구했다. 이에는 조직도, 주요 제품과 서비스, 시장에서의 점유율, 상위 10위에 속하는 경쟁자 정보, 10대 고객, 재무 정보, 과거 미국 정부나 다른 나라 정부로부터 조사 관련 문서, 인수 합병에 관련된 정보, 과거 십여 년 동안의 최고 경영자 사이의 내부 이메일 등 매우 민감한 모든 정보를 요청했다. 시한은 10월 14일까지이다. 또한, 80여 개의 기업에 정보 요청을 했는데, 자기들의 비즈니스가 4대 거대 기업에 의해 어떤 영향을 받았는지, 독점적 지위로 관여했는지를 요청했다.<sup>5)</sup>
- 미 상원은 9월 17일 빅 테크 기업에 대한 반독점 조사가 제대로 이루어지고 있는지, 적절한 자원이 투입되고 있는지 관련하여 행정부 반독점 규제 당국에 강한 압력을 주기 위한 청문회를 열었다.<sup>6)</sup> 또 다른 청문회는 극단주의가 온라인에서 확산하는 문제에 대한 것이다.

이러한 움직임은 빅 테크 기업이 시장에서의 권력을 남용하는 것이 아니냐는 우려에서 비롯되었다. 그동안 혁신의 상징이고 미국 경제를 이끄는 새로운 엔진이라고 칭송했던 기업이 이런 상황에 처하게 것은 계속되는 데이터 유출, 프라이버시 침해, 허위정보 확산 등에 연관된 사건들 때문이라고 봐야 한다. 특히 과거 2016년 대선에서의 문제로 인해 정치권의 관심이 높아졌고, 내년 예정된 다음 대선까지 이런 문제를 사전에 최소화해야 한다는 여론의 요구에 대응하는 움직임으로 이해할 수 있다.

3) The Verge, “Google under antitrust investigation by 50 attorneys general,” Sep 9, 2019.

4) CNN, “FTC ramping up its Big Tech antitrust investigations,” Sep 11, 2019

5) New York Times, “Congress Asks More than 80 Companies for Big Tech Complaints,” Sep 20, 2019.

6) New York Times, “Lawmakers Urge Aggressive Action From Regulators on Big Tech,” Sep 17, 2019.

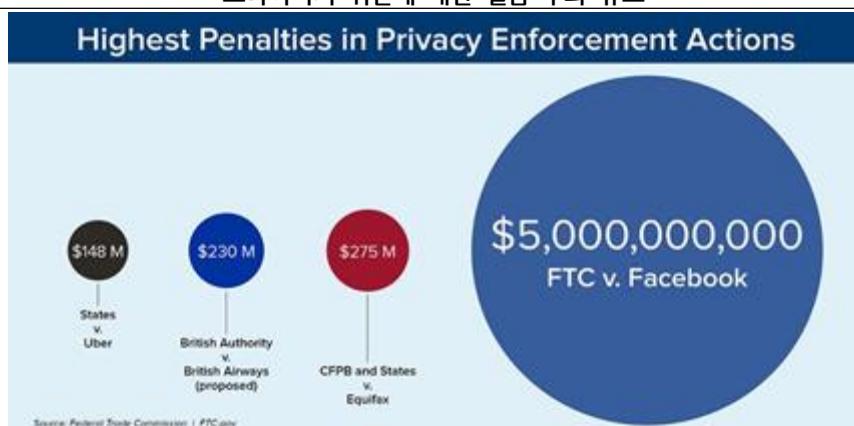
구글은 현재 5개의 조사를 받고 있는데, FTC가 프라이버시 이슈로 (일단 유튜브에서 아이들의 프라이버시 위반 문제로 벌금을 부과했다) 인하여 법무부, 의회 사법위, 주 법무부 등에서 반독점 위반 혐의로 4건의 조사가 이루어지고 있다.

페이스북은 이보다 많은 11건이 진행 중인데, 위에 거론한 기관 외에 증권 거래 위원회, 주택 도시 개발부, 상원 은행 위원회, 각 주의 법무부에서 다양한 조사가 진행 중이다. 조사 주제는 프라이버시, 반독점, 차별, 암호화폐 등으로 다양하다. 애플은 3건의 반독점 위반 혐의에 대해 조사받는 중이며, 아마존 역시 3건의 반독점 위반 건이 진행 중이다.<sup>7)</sup> .총합하면 연방 기관에서 8건, 주나 지역 정부에서 6건, 의회에서 2건이 있다.

## 다양한 벌금 부과와 합의

최근에는 유럽에서도 빅 테크 기업에 처벌이나 벌금을 부여한 사례가 지속해서 발생하고 있다. 2019년 7월 FTC는 페이스북이 개인정보를 잘못 다루었다는 이유로 약 50억 달러에 달하는 벌금을 부과했는데, 이는 기술 기업에 부과한 벌금 중 가장 큰 규모에 해당한다.<sup>8)</sup>

프라이버시 위반에 대한 벌금 부과 규모



[출처: 포브스, FTC]

FTC는 이를 통해 페이스북이 프라이버시를 다루는 문화 자체를 완전히 바꾸겠다는 계획이다. 특히 이 합의준수를 앞으로 20년간 유지하겠다는 의지로 임원 수준의 변화를 포함해 제3의 개발자들과 이런 정보를 다루는 방식을 바꾸고, 향후 어떤 프라이버시 위반에 대해서 회사가 어떻게 책임을 져야 하는지에 대한 가이드라인을 수립했다고 평가받는다.

7) New York Times, “16 Ways Facebook, Google, Apple and Amazon Are in Government Cross Hairs,” Sep 9, 2019.

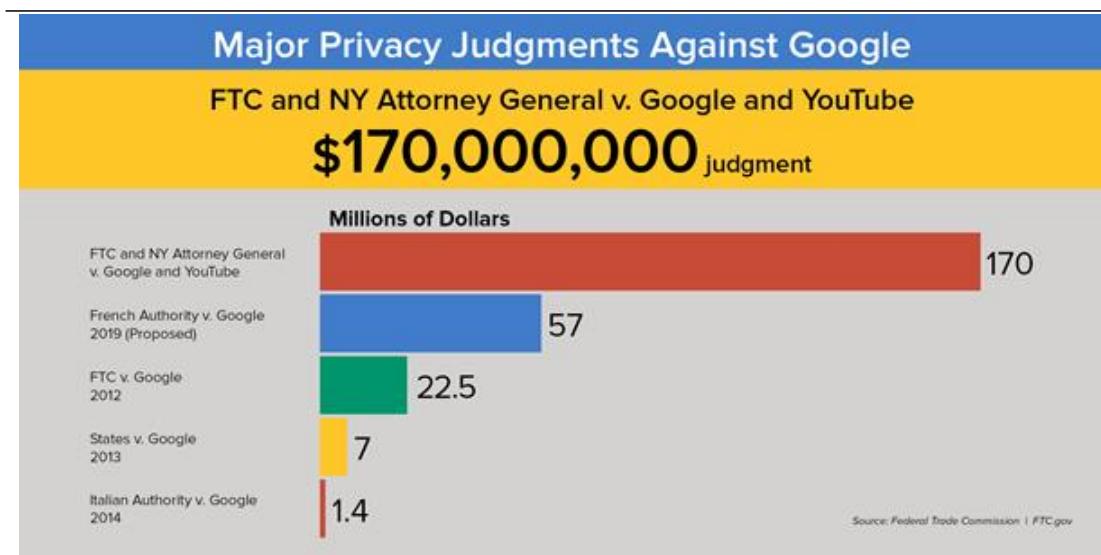
8) Forbes, “FTC Slaps Facebook With \$5 Billion Fine, Forces New Privacy Controls,” Jul 24, 2019.

추가로 마크 저커버그의 힘을 제한하고 이사회에 독립적인 프라이버시 위원회를 만들도록 했는데, 이 프라이버시 위원회 위원은 투표권을 갖는 주식의 2/3가 찬성해야만 해고할 수 있도록 해서 저커버그가 마음대로 할 수 없게 했다. 저커버그는 또한 이런 동의안대로 실행하고 있는지에 대한 보고서를 매 분기 및 연마다 FTC에 제출해야 한다.

이에 따라 저커버그는 페이스북 페이지에 완전히 새로운 표준을 만들겠다고 밝혔다. 그는 수백 명의 엔지니어와 수천 명의 인력을 동원하여 데이터를 사용하는 새로운 기능을 공개할 때나 기존 기능을 수정해서 데이터를 새로운 방식으로 사용하는 경우, 이용할 때 잠재하는 위험과 이를 완화하려는 조치를 문서화할 것이라고 말했다. 또한, 가장 경험이 많은 리더가 제품의 최고 프라이버시 담당 임원 역할을 하도록 배정하고, 새로운 제품을 만드는 것에 더 많은 시간이 걸리는 것을 감수할 것이라고 발표했다.

구글은 최근 유튜브에서 어린아이들의 프라이버시를 침해했다는 이유로 1억 7천만 달러의 벌금을 부과 받았다.<sup>9)</sup> 아이들로부터 불법적으로 개인정보를 수집하고 이를 타깃 광고에 사용해 이익을 얻었다는 이유다. 이는 FTC와 뉴욕주 법무부의 조사에 의해 FTC에 1억 3,600만 달러, 뉴욕주에 3,400만 달러를 내기로 합의 한 것으로, 어린이 온라인 프라이버시 보호법 (COPPA) 위반이다. 지금까지 구글이 프라이버시 위반으로 판결을 받은 것은 이탈리아, 미국 주 정부, FTC (2012년), 프랑스 정부에 이어 5번째이다.

#### 구글이 프라이버시 침해로 벌금을 내야 하는 사례들



[출처: FTC]

9) New York Times, "Google Is Fined \$170 Million for Violating Children's Privacy on YouTube," Sep 4, 2019

구글은 유럽 연합에서도 이미 지난 3월 온라인 광고 시장 독점 방지를 위반한 혐의로 15억 유로 벌금을 부과받았다. 이는 2017년부터 진행된 구글에 대한 세 번째 벌금 집행으로, 이번에는 유럽 웹사이트에 사용되는 검색 바에서 불공정한 조건을 강요했다는 이유이다.

또한 애플은 유럽에서 불공정 경쟁과 세금 회피로 인해 2016년에 130억 유로의 세금을 부과하겠다는 유럽 경쟁 위원회의 주장에 맞서기 위해 CFO가 류셈부르크를 방문해 어필하고 있다.<sup>10)</sup>

그러나 최근 미국 두 연방기관 간의 불화로 진행이 빠르지 못하다는 불만이 나타나 이에 대해 의회가 규제 당국의 활동을 강화하도록 압박하는 중이다.<sup>11)</sup> 중복된 조사 가능성과 주 법무부의 일반 조사는 오히려 문제를 더 복잡하게 만들 수 있다는 의견이 의회에서 나오고 있다.

## 기업의 대응과 전망

이러한 위기에 대응하기 위한 각 기업의 움직임도 매우 빠르게 나타나고 있다. 아마존의 제프 베저스와 페이스북의 마크 저커버그는 워싱턴에 나타나 여러 활동을 하며 여론을 돌리기 위한 노력을 하고 있다. 특히 저커버그는 트럼프 대통령을 만나 선거 보안, 프라이버시 등의 이슈에 대해 논의한 것으로 알려졌다.<sup>12)</sup>

현재 민주당의 유력 대통령 후보인 엘리자베스 워런 상원의원이 아마존에 대해 한 말이 매우 의미심장하다. 워런 상원의원은 ‘당신은 심판이 되거나 선수가 될 수 있다. 그러나 두 가지 모두를 할 수는 없다’는 말로 빅 테크 기업이 우월적 지위를 약용하고 있음을 강조했다.

이런 정부와 의회의 움직임의 결과는 어떻게 나타날 것인가? 일단 가장 강력하게 나타나는 의견은 이런 거대 기업을 분할해 경쟁을 촉발하고 독점을 막자는 것이다. 워런 상원의원은 이미 민주당 프라이머리에서 이런 기업을 분할하는 정책을 만들겠다고 선언했다.

이미 2018년에 콜롬비아 로스쿨의 법학자 팀 우<sup>13)</sup>나 하버드 대학의 경제학자 케네스 로고프는 빅 테크 기업이 이미 너무 커졌기 때문에 분할할 필요가 있다고 주장했다.<sup>14)</sup> 심지어 페이스북의 공동 창업자인 크리스 휴즈조차 FTC나 법무부와의 미팅에서 페이스북이 분할되어야 한다고 주장했다.<sup>15)</sup>

10) CNet, “Apple prepares for \$14 billion tax battle in EU court,” Sep 16, 2019.

11) WSJ, “U.S. Antitrust Enforcers Signal Discord Over Probes of Big Tech,” Sep 16, 2019.

12) New York Times, “Bozos and Zuckerberg Take Their Pitches to Washington,” Sep 19, 2019.

13) CNN, “Big Tech is way too big,” Dec 17, 2018.

14) Market Watch, “Opinion: Has Big Tech gotten too big for our own good?” Jul 11, 2018.

15) New York Times, “Chris Hughes Worked to Create Facebook. Now, He Is Working to Break It Up,” Jul 25, 2019.

최근 ‘진보를 위한 데이터’와 유거브(YouGov)가 공동으로 조사한 여론조사에서도 미국인 2/3가 빅 테크 기업을 분할하는 안에 대해 찬성한다는 조사가 나왔다.<sup>16)</sup> 흥미로운 점은 민주당이나 공화당 지지자는 상관 없이 모두 동의하고 있다는 점이다.

빅 테크 기업도 이런 위험에 적극 대응을 하기 시작했다. 워싱턴을 대상으로 로비와 여론 전환을 꾀하면서도 동시에 각종 정책을 강화하고, 대응 방안을 제시하기 시작했다.

9월 20일 페이스북은 사용자 개인정보와 다른 범법행위가 의심되는 수만 개의 앱을 중단시켰는데, 지난 2018년 8월에 400개의 앱을 중단하도록 한 것에 비해 엄청 커진 숫자다. 정확한 수치는 매사추세츠주 법무부 조사의 일환으로 보스턴 주 법원에 제출한 자료에서 밝혀졌는데 그 숫자는 69,000개라고 한다.<sup>17)</sup>

페이스북은 또한 콘텐츠에 대한 문제를 검증하고 포스팅을 내려야 하는 결과를 자사 내부에서 판단하지 않고 다양한 외부위원으로 구성된 관리위원회(Oversight Board)를 통하여 판단하겠다는 정책을 발표했다.<sup>18)</sup> 40명으로 구성되는 이 관리위원회는 지나치게 폭력적이거나 인종 차별적인 내용, 비정상적인 행위를 판단하게 되며 외부의 다양한 채널을 통해 위원을 선정한다고 했다.

구글은 9월 12일 검색 알고리즘을 변경해 오리지널 뉴스 기사에 우선권을 부여하기로 했다.<sup>19)</sup> 이를 1만 명이 넘는 인간 리뷰어에게 주지시켜 구글 알고리즘이 이에 맞게 훈련되도록 할 예정이다. 이는 왜곡되거나 조작되는 허위 정보나 가짜 뉴스에 대한 대응으로 이해할 수 있으나, 반대로 좀 더 깊이 있고 충실한 뉴스가 나중에 나올 수 있다는 점에서 비판을 받고 있다.

7월 23일에는 월스트리트 저널, 9월 9일에는 뉴욕 타임스가 애플이 앱 스토어 운영에서 어떻게 경쟁자들을 교묘하게 몰아내고 자사의 앱을 가장 높은 순위에 제시되게 만들었는지 연도별로 그 변화를 상세히 분석한 자료를 공개한 적이 있다.<sup>20)</sup>

이런 문제점 지적에 애플은 앱 스토어 검색 알고리즘을 변경해 자사의 앱이 검색 상위에 나오는 비율을 줄이도록 했다.<sup>21)</sup> 그러나 앱 스토어 차트나 검색 결과에 애플 제품이 나타나는 것이 과연 올바른 것인가 하는 문제 제기는 계속된다. 차라리 자체 소프트웨어 다운로드를 독립적인 섹션으로 놓고, 앱 스토어는 제3자 소프트웨어로만 구성하는 것이 옳다는 의견이 있다.

---

16) Vox, “Poll: Two-thirds of Americans want to break up companies like Amazon and Google,” Sep 18, 2019.

17) New York Times, “Facebook’s Suspension of ‘Tens of Thousands’ of Apps Reveals Wider Privacy Issues,” Sep 20, 2019.

18) The Atlantics, “Finally, Facebook Put Someone in Charge,” Sep 18, 2019.

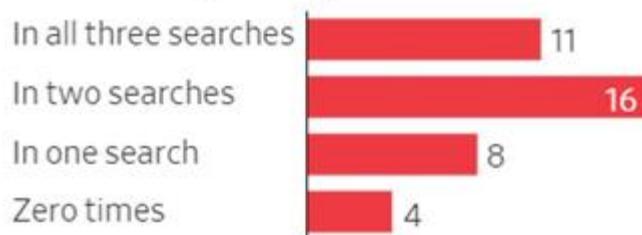
19) The Verge, “Google is changing its search algorithm to prioritize original news reporting,” Sep 12, 2019.

20) New York Times, “How Apple’s Apps Topped Rivals in the App Store It Controls,” Sep 9, 2019.

21) TechCrunch, “Apple tweaks its App Store algorithm as antitrust investigations loom,” Sep 10, 2019.

### 인기 키워드로 앱 스토어에서 검색할 때 애플 앱이 처음에 나오는 경우

**Number of Apple's apps that ranked first:**



Note: The study's more than 600 searches were conducted in June. Searches excluded Apple apps that weren't discoverable in the App Store such as Safari, as well as apps specific to Apple products such as Apple Support.

Source: WSJ analysis of Apple's App Store

[출처: WSJ]

반독점법 위반 행위로 조사를 받는다고 바로 어떤 결과를 기대할 수는 없다. IBM에 대해 조사가 13년, AT&T도 십여 년이 걸렸고, 마이크로소프트는 12년 동안 추적했지만, 항소심에서 정리가 되었다. 이는 대기업의 수많은 로비스트, 법률가, 의회와 관련된 기관의 직원들이 적극적인 방어에 나서기 때문이다. 또한, 독점을 규제하면서 작은 경쟁 기업을 보호하는 것이 소비자들에게 비효율적이거나 가격 인상을 가져올 수 있다는 비판도 있다.

그러나 지금 테크 분야의 거대 기업이 가진 상상 이상의 권력과 이를 악용해 불공정한 행위를 저지르는 것, 의도하지 않아도 벌어지는 수많은 데이터 유출과 프라이버시 침해, 민주주의에 큰 위협이 되는 허위 정보의 빠른 유포와 확산에 대해서 공공기관과 규제 당국이 시민을 위해 무엇인가 나설 때라는 것에 대해서는 모두 공감하고 있다.

# IFA 2019 유럽 가전의 혁신 속도가 빨라지다



최필식 (choi4u@gmail.com)

기술작가  
IT 블로그 'chitsol.com' 및 테크G([www.techg.kr](http://www.techg.kr)) 운영자

CES가 새로운 해를 여는 소비자 기술 전시회라면 IFA는 한 해를 정리하는 소비자 제품 전시회다. 새해 벽두에 열리는 CES가 미국 중심적이면서 뜨거운 일출 같은 전시회라면, 가을 무렵의 IFA는 유럽 특유의 정서가 반영된 화려한 노을로 비유할 수 있을 만큼 두 전시회는 비슷한 듯해도 지역적 특수성이 반영된 다른 모습을 보여 왔다. 다만 신기술로 시선을 끄는 CES에 비하면 IFA는 유럽 소비자를 위한 제품 이외의 소식을 얻기 힘든 전시회인 것이 사실이다.



IFA 2019 전시회가 열리는 메세 베를린의 남쪽 입구 모습

[출처: IFA 공식 자료]

이러한 비판적 시각에서 벗어나기 위해 IFA 주최 측은 올해 미국과 다른 유럽의 지역적 색채를 더욱 강화하는 한편, CES와 다른 프로그램을 더 준비했다. 기존 맥락 없는 기조연설 대신 IFA에서 잘 다루지 않던 모바일에 초점을 맞춘 기업의 연사를 준비하는 한편, 자동차 분야의 미래를 모색하는 'SHIFT' 이벤트를 추가하며 모빌리티 업계를 끌어들였다. 또한, ODM 상품의 수출 상담을 위한 IFA 글로벌 마켓을 3년째 IFA 기간 내에 운영하면서 더 많은 기업과 고객들에게 IFA가 기업 제품을 선보이는 상징성을 넘어 실리를 추구할 수 있는 전시회로 자리 잡도록 지원을 아끼지 않았다.

이러한 IFA의 노력은 2천 개 가까운 전시업체를 유치하는 한편 행사 기간 동안 24만5천 명이 다녀가는 성과로 이어졌다. 수많은 참관객과 다양한 업계의 관계인들이 IFA 2019에서 무엇을 보고 갔는지 주요 키워드를 정리한다.

## 키워드 1. 8K TV, 가속도를 불이다.

사실 TV라는 전통적인 영상 가전의 한 아이템을 소비자 전시회의 첫 키워드로 꼽는 것은 상투적일 수 있다. 그렇더라도 IFA 2019의 8K TV는 곱씹어 볼 의미가 있는 키워드다. 이미 대중화의 길에 접어들었다고 볼 수 있는 4K TV와 달리 8K TV는 여전히 시기상조라는 견해를 가진 이들이라면, 특히 CES 2019에서 IFA 2019로 이어지는 8K TV의 흐름을 지켜본 이라면 이제 그 견해를 수정할 필요가 있어 보여서다.

IFA 2019에서 확인한 8K TV는 한국과 일본, 중국 가전 제조사뿐 아니라 유럽 영상 가전 업체까지 빠짐 없이 가세한 형국이다. 이는 대형화되고 있는 디스플레이의 추세에 맞춰 시장이 빠르게 확산될 것으로 예상하기 때문이다. 시장 조사 기관 IHS는 2019년 30여만 대의 규모에서 2022년에 500만 대 시장으로 성장할 것이라는 전망을 내놓기도 했다



각 제조사의 8K TV. 왼쪽 상단부터 시계 방향 순서로 코니카, LG, 소니, TCL, 삼성, 하이센스 순.

이처럼 8K TV가 대중화를 서두르는 이유는 60인치 이상 대형 TV의 부족한 화소를 메워 화질을 개선하고 몰입감을 높이는 가장 좋은 해결책이라서다. 8K TV는 가로 7,680, 세로 4,320개의 물리적 화소를 가진 디스플레이를 쓰는데, 화면이 대형화될수록 떨어지는 화소 밀도를 보완해야만 실제로 화질을 개선하는 효과를 얻을 수 있다.

하지만 8K TV가 생각보다 빨리 기지개를 켜면서 급해진 것은 콘텐츠다. 8K TV에 대응할 수 있는 콘텐츠는 거의 찾아보기 힘든 현실이 기다리고 있다. 그러나 8K TV를 위한 샘플 수준의 콘텐츠는 찾을 수 있지만, 이미지 크기와 프레임, 색 정보를 담은 8K 방송이나 장편 영상물은 거의 없다. 이는 고화질 TV 시장이 시작될 때마다 반복되는 문제여서 시간을 두고 기다리면 해결될 문제다. 일한 장치가 가상 현실 헤드셋이라는 점에서 그 중요도는 더욱 높아진다. 현실의 움직임을 감지해야만 가상 현실의 자유도(Degree of Freedom)를 높일 수 있기 때문이다.

또한 8K로 송출할 예정인 2020년 하계 도쿄 올림픽 같은 대형 스포츠 이벤트를 거치면 8K 콘텐츠는 좀 더 빨리 늘어날 가능성이 크다.

그렇더라도 지금 당장은 4K 콘텐츠를 8K TV에서 볼 수밖에 없는 상황이다. 8K TV에 충분한 정보를 담고 있지 않더라도 전용 콘텐츠가 없는 만큼 이를 활용해야 한다. 물론 4K 콘텐츠가 8K TV에서 무조건 보기 흉한 것은 아니다. TV 제조사들이 이에 대비한 기술을 쓰고 있어서다. 4K 콘텐츠를 8K TV에서 화질 저하 없이 볼 수 있는 업스케일링을 위한 기술과 부품이 8K TV에 들어 있다.

실제 8K TV는 8K 콘텐츠의 정보를 처리하고 4K 콘텐츠를 8K 콘텐츠처럼 속이는 업스케일링을 위한 전용 인공 지능 기반 프로세서가 들어간다. 이러한 AI 프로세서는 기계 학습을 통해 찾아낸 영상의 화질 개선 알고리즘을 담고 있다. 원본 영상의 화질에 있는 노이즈를 잡아내고 4K 콘텐츠의 업스케일링에서 부족한 정보를 채워 넣는 역할을 한다. LG전자는 IFA 2019에 전시한 OLED TV에 개선된 2세대 알파 9 8K 프로세서를 넣었고, 삼성전자는 8K TV에 넣은 퀸텀 프로세서 8K의 실물을 전시장에 공개했다. 물론 인공 지능 기반 프로세서가 아닌 8K 처리를 위한 프로세서를 탑재한 8K TV도 많다.



샤프는 소비재용 8K TV의 단순 전시 대신 활용처에 필요한 솔루션을 공개했다.

IFA 2019에서 볼 수 있는 8K 관련 제품은 대부분 TV지만, 일부 8K 편집 환경과 5G를 활용한 솔루션을 공개한 곳도 있다. 일본 샤프는 고밀도 8K TV를 박물관이나 비디오 월로 활용하면서 5G를 결합해 섬세한 영상을 봐야 하는 원격 수술에 활용하는 샘플을 전시했다. 실제 8K 콘텐츠가 당장 없는 상황에서 기업 및 산업 현장에서 고밀도 화소를 가진 8K TV는 매우 유용할 수 있을 것으로 보인다.

## 키워드 2. 모바일, 조금 다른 5G를 말하다

해마다 모바일 전략과 기술에 관한 가장 굵직한 소식이 쏟아지는 행사라면 1초의 고민도 없이 모바일

월드 콩그레스라 말할 것이다. 그런데 IFA 2019에서 예상 밖 현상이 벌어졌다. 모바일 컴퓨팅의 핵심인 모바일 프로세서와 관련한 새 발표들이 IFA를 기점으로 잇달아 나온 것이다. 퀄컴을 비롯해 삼성과 화웨이 등 모바일 프로세서의 경쟁자들이 새로운 프로세서와 전략을 쏟아낸 것은 이전 IFA 전시회 역사에서 찾아보기 힘든 광경이다.

그 원인은 역시 ‘5G’다. IFA가 비록 가전 전시회이기는 해도 유럽에서 열리는 소비자 전시회 가운데 가장 큰 규모라는 점을 볼 때, 5G 상용화를 준비하는 유럽 각 나라에 필요한 스마트폰 같은 소비자용 5G 장치를 위한 메시지가 잘 전달될 수 있는 분위기는 갖추고 있다.



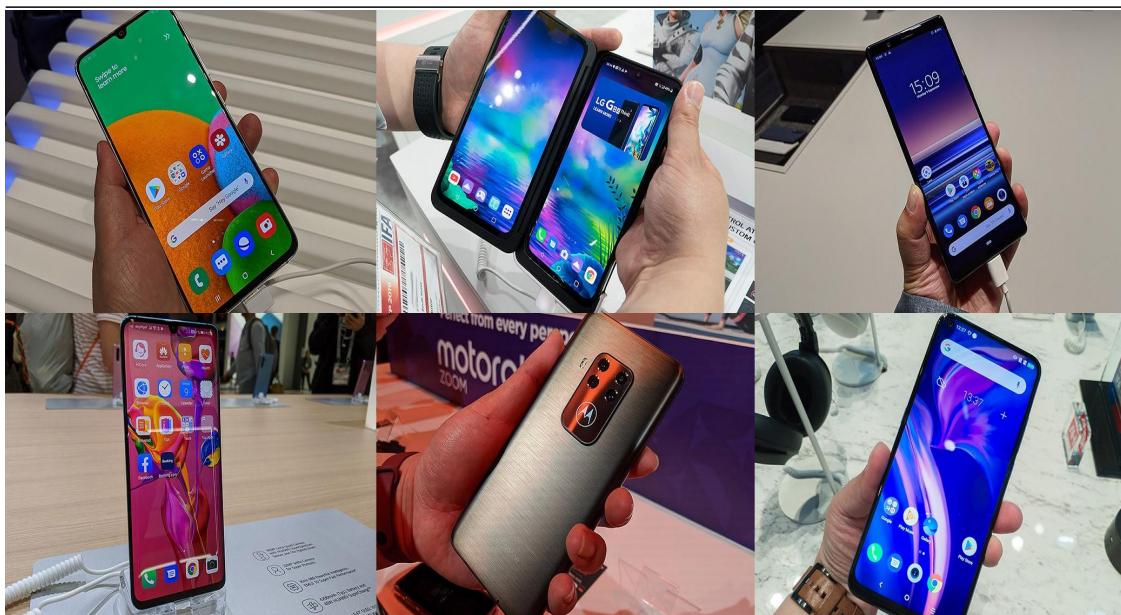
퀄컴과 화웨이, 삼성 등 5G 모바일 솔루션과 전략을 공개했다. 퀄컴은 차기 중급형 프로세서에 대한 전략, 화웨이는 고급형 5G 프로세서, 삼성은 중고급형 5G 통합 프로세서를 발표했다

하지만 IFA 2019에서 5G 스마트폰이 아니라 5G 스마트폰용 모바일 프로세서의 작은 경쟁이 일어난 것은 2년 전부터 IFA 공식 키노트의 단골 연사가 된 화웨이가 새로운 모바일 프로세서를 발표하면서 소비자 제품의 기술 리더십으로 연결되는 효과를 무시할 수 없어서다. 화웨이는 애플이나 퀄컴보다 앞서 IFA에서 신경망 코어를 내장한 플래그십 프로세서인 기린 970을 2017년에 발표해 놀라움을 안겼고 이듬해에도 경쟁사보다 먼저 IFA에서 기린 980을 발표했다. 모바일 프로세서에 따른 스마트폰의 기술 리더십에 대한 이미지 경쟁이 일어날 수 있는 분위기 속에서 결국 삼성과 퀄컴도 IFA를 통해 새 5G 모바일 프로세서와 전략에 관한 메시지를 풀며 분위기를 내주지 않으려는 듯한 인상이다.

올해 IFA 2019의 5G 프로세서로 모바일 뉴스를 장식한 기업은 화웨이와 퀄컴, 그리고 삼성이다. 그런데 먼저 포문을 연 곳은 화웨이가 아니라 삼성이었다. IFA 개막 이틀 전인 9월 4일에 5G 모뎀을 처음 통합한 8나노 팬펫 공정 프로세서인 엑시노스 980을 공개하고 IFA 행사장인 시티큐브에서 실제 샘플을 공개할 것이라는 예상은 거의 없었기 때문이다. 다만 엑시노스 980은 5G 모뎀을 통합한 최초의 칩이긴 해도 아키텍처를 볼 때 플래그십이 아닌 플래그십에 가까운 스마트폰을 위한 용도로 출시할 것으로 예상한다.

화웨이는 지난 해와 변함없이 플래그십용 프로세서를 들고 왔다. 9월 6일 오전 진행된 IFA 2019 공식 키노트에서 차기 모바일 프로세서인 기린 990 5G를 공개한 것이다. 그런데, 화웨이 소비자 제품 부문

CEO 리차드 유의 프레젠테이션은 매우 공격적이었다. 새로운 5G 모뎀 통합 7nm 공정의 기린 990의 특징을 소개하는 것에서 멈추지 않고 앞서 출시된 퀄컴이나 애플, 삼성 등 경쟁 구도의 제품과 일일이 성능을 비교하며 상대적 우위를 강조했다.



IFA 2019에서 공개된 스마트폰들. 왼쪽 상단부터 시계 방향으로 삼성 갤럭시 A90, LG V50S(G8X) 씽큐, 소니 엑스페리아 5, TCL 플렉스, 모토롤라 줌, 화웨이 P30 프로.

퀄컴은 예상 밖의 전략을 공개했다. 플래그십용 제품인 스냅드래곤 8 시리즈뿐 아니라 준플래그십 및 중급형 제품에 탑재되는 스냅드래곤 7 시리즈 및 6 시리즈까지 모두 5G를 지원한다고 공식 발표한 것이다. 중급형 제품에 5G를 위한 mmWave 및 6GHz 이하 주파수, TDD 및 FDD 모드를 포함한 모든 주요 지역 및 주파수 대역, 5G+LTE 다중 심을 지원하겠다는 발표로 올해 말부터 가격을 좀더 낮춘 5G 스마트폰을 기대할 수 있게 된 것이다. 이와 함께 퀄컴은 글로벌 생태계의 역할론을 더욱 강조했다. 제조사와 유럽 이통사와 협력 관례를 통해 5G 생태계 구축을 위해 함께 노력 중이라는 메시지를 내보냈다. 기술리더십을 앞세운 화웨이나 텁새시장 공략에 나선 삼성과 다른 자세였다.

이러한 모바일 뉴스와 더불어 가격을 낮춘 고급형 5G 스마트폰과 새로운 LTE 스마트폰도 쏟아졌다. LG 전자가 5G 스마트폰인 V50과 거의 같은 제원에 카메라 사양과 가격을 낮춘 V50S 씽큐를 공개했고, 삼성은 플래그십 프로세서를 탑재한 갤럭시 A90을 깜짝 발표했다. 화웨이는 광학 5배, 디지털 포함 50배 줌이 되는 P30 프로를 공개했고, 소니도 엑스페리아 5라는 플래그십 라인을 확장했다. 레노버와 노키아, TCL이 중급형 시장을 위한 새로운 스마트폰을 내놓는 등, 역대 IFA 전시회 가운데 모바일 전략과 제품에 관한 뉴스가 많이 쏟아졌다.

### 키워드 3. 스마트 홈, 구글과 아마존이 유럽 가전을 삼킨다

지난 몇 년 동안 CES에서 구글과 아마존의 존재감은 상당했지만, IFA의 주요 전시 공간을 차지하고 있는 유럽 가전 업체들은 IT 공룡이 만든 플랫폼에 적극적인 느낌을 받지 못했다. 대부분의 유럽 가전 제조사도 스마트폰이나 태블릿 등 모바일 장치를 활용해 가전제품을 다루는 커넥티드 기능은 제공해 왔지만, 상대적으로 인공 지능 음성 비서로 제어할 수 있는 기능의 구현과 적용 다소 늦는 느낌이었다.

하지만 유럽에서 음성으로 가전제품을 제어하는 이용자가 늘면서 유럽 가전 업체도 AI 기반 음성 제어를 놓고 고민했다. 2018년 기준으로 독일서 810만이 넘는 이용자가 인공 지능 음성 비서를 쓰고 있고 그 수가 빠르게 증가한다는 비트콤 및 딜로이트의 조사 결과는 모바일의 연결성에 자연어 인터페이스를 갖춰야 할 당위성을 가전 업체에 상기시켰다. 그 때문에 유럽 가전 업체는 물론 유럽 시장에 제품을 출시하는 한국과 중국의 가전 업체들은 다양한 인공 지능 음성 인식 기술을 더 한 제품을 선보여 왔다.



유럽 가전 업체는 물론 거의 모든 가전 업체가 구글 또는 아마존의 음성 비서 플랫폼과 호환되는 제품을 전시했다.

그런데 지난해에 이어 올해 IFA에서 구글과 아마존을 적극적으로 끌어들인 가전 업체가 상당히 늘어났다는 점이 인상적이다. 일부의 저항이 남아 있기는 하나 구글과 아마존을 제외한 AI 플랫폼을 더는 찾아보기 힘든 상황이다. 특히 구글과 아마존이 유럽 가전의 AI 플랫폼으로 강세를 보였던 것이 아니라는 점에서 이번 IFA는 매우 큰 변화다. 2년 전만 해도 독일 가전 업체나 아시아 가전 제조사들이 독립적인 AI 플랫폼을 적용한 가전제품을 내놓거나 앞으로 내놓기 위해 준비 중이라는 발표를 빼놓지 않았다. 보쉬가 주방용 AI 어시스턴트인 마이키(Mykie)를 내놓으면서 독자적 생태계를 구축하는가 싶었다.

그러나 올해 보쉬나 지멘스 등 유럽 가전 업체들은 자체 플랫폼 대신 홈 커넥트에 기반을 둔 음성 인식 플랫폼을 연동하는 데 집중했다. 이전부터 유럽 가전제품들에 탑재되고 있는 커넥티드 플랫폼인 홈 커넥트가 구글과 아마존의 인공 지능 음성 비서와 연동되면서 이들의 가전제품도 자연스럽게 관련된 기능을 제어 할 수 있게 됐다.

이와 더불어 LG전자는 구글 어시스턴트와 강력하게 결합한 스마트홈을, 중국 하이얼은 같은 그룹으로 편입시킨 후버 및 캔디 등과 함께 아마존, 구글의 음성 비서는 물론 아마존 대시까지 지원하는 가전제품을 전시했다. 지난해 자체적으로 개발한 인공 지능 음성 비서 기능인 빅스비를 강하게 추진했던 삼성은 이번 IFA에서 스마트씽스를 기반으로 하는 가전제품으로 스마트홈 시연장을 구성했지만, 그 어디에도 빅스비의 존재감을 찾을 수 없었다. 오히려 세탁기 등 일부 장치에 아마존 대시를 넣는 등 지난 해와 확실히 다른 분위기로 스마트 홈을 강조하는 분위기였다.

이처럼 구글과 아마존의 영향력이 그 어느 때보다 강해진 것을 이번 IFA 2019에서 어렵지 않게 확인할 수 있다. 비록 개방성과 유연성을 앞세웠다고는 하나 이처럼 빠르게 구글과 아마존의 플랫폼이 유럽 가전 시장에 침투하게 된 이유는 더 분석할 필요가 있다. 또한, 구글과 아마존의 침투가 단순히 가전 업체의 대응이 어려운 전통 가전제품만 목표로 삼은 게 아니라는 점에서 향후 방향도 함께 살펴봐야 한다.



예년 보다 가짓 수가 늘어난 아마존 파이어 TV를 내장한 가전 업체의 TV들. 앱 기반 TV 시청 환경의 변화로 인해 구글 안드로이드 TV를 내장한 TV와 함께 스마트 TV 시장에 도전 중이다.

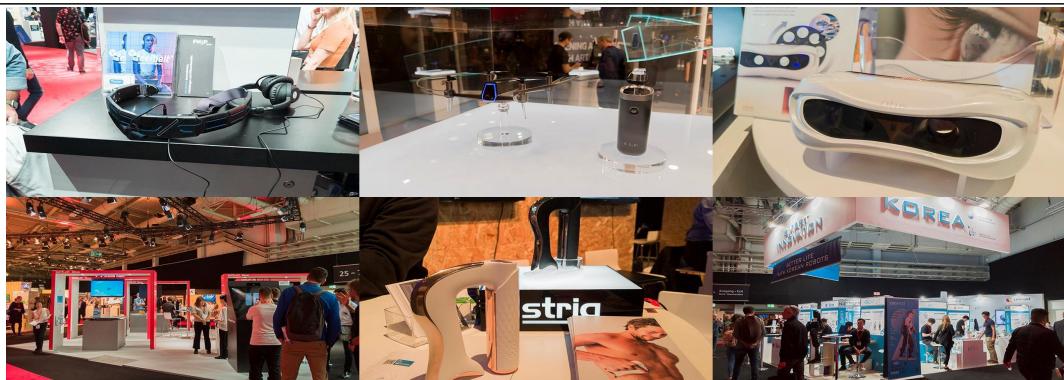
무엇보다 IFA 2019에서 구글과 아마존은 거의 모든 사물 인터넷 제품군까지 영향력을 넓히는 동시에 기존 TV의 스마트 플랫폼으로도 영향력을 확대했다. 구글 안드로이드TV와 아마존 파이어TV를 스마트TV

플랫폼으로 채택한 TV도 적잖게 등장한 것이다. 이는 유럽의 TV 시청 방식이 종전 채널 중심에서 앱 기반 스트리밍으로 변하면서 이에 따른 변화로 예상되는데, 이처럼 이용자 경험의 빠른 변화에 대응하지 못하고 있는 유럽의 가전 업체에 이미 준비된 플랫폼을 가진 구글과 아마존에 대한 종속은 더욱 심화할 것으로 보인다.

#### 키워드 4. 스타트업, IFA 넥스트가 혁신의 허브로 자리 잡다

수십 년 동안 새로운 소비재 제품을 전시해 고객에게 홍보하고 새로운 구매자를 연결해 주던 대형 전시회의 기능성이 하락하면서 위기를 거론한 적이 있다. 새로운 기업은 거의 없고 늘 같은 공간에 같은 기업의 전형적인 소비재 제품 전시회의 틀을 유지하다 보니 IFA도 몇 년 전 소비자의 관심을 끌어내지 못하고 점차 상황이 악화하는 위기를 맞이했다. 그런데 위기를 겪었던 대규모 전시회들이 다시 활력을 찾은 데는 공통점이 하나 있다. 전시회의 틀에 박히지 않은 '새로움'과 '혁신'이라는 두 가지 요소를 모두 충족할 수 있는 스타트업을 유치한 이후다.

IFA도 2년 전부터 IFA 넥스트라 불리는 스타트업 공간을 열었다. 주요 전시장과 거리가 먼 데다 키노트를 위한 씨어터를 제외하면 참관객이 거의 찾지 않던 26홀 전체를 스타트업을 위한 공간으로 개편한 것이다. 2년 전 첫 시작 때 이 공간은 IFA의 전시 성격과 다소 낯설었으나 지난해 다양한 스타트업 및 국가관이 자리를 펴면서 활기를 불어넣기 시작했다. 공간 특성상 매우 작은 부스를 배정받을 수밖에 없는 데도 아직 판매처나 투자자를 구하지 못한 수많은 스타트업들의 열띤 홍보로 인해 기존 IFA 전시 공간에서 볼 수 없는 흥미로움을 선사했다.



현재 양산을 준비하고 있거나 곧 정식 판매를 앞둔 수많은 스타트업의 제품들이  
IFA에 새로운 활력을 불어넣었다.

올해도 IFA 넥스트는 독일은 물론 한국과 일본, 프랑스, 중국, 이탈리아에서 엄선된 100개의 스타트업이 참여해 인공 지능과 디지털 헬스케어, 1인 이동 수단, 로봇, 푸드 테크와 관련된 흥미로운 제품들을 전시

하고 세계 여러 나라의 언론을 대상으로 수많은 혁신을 홍보했다. 특히 이번 IFA 넥스트는 일본을 최초의 글로벌 혁신 파트너 국가로 채택했다. 특별히 장식한 일본 파빌리온에서 기계와 인간의 상호 작용 방식에 대한 최신 아이디어와 혁신이 담긴 제품과 서비스를 공개한 것이다. 우리나라도 한국관 및 한국혁신센터 유럽(KIC Europe)에서 스타트업 부스를 마련했는데, 인공 지능, 로보틱스, 드론, 건강 관리, 웨어러블 등 다양한 분야의 아이디어 상품으로 관심을 모았다.

세계 주요 국가의 스타트업 전시와 함께 스타트업을 위한 IFA 넥스트 이노베이션 엔진 프로그램을 새로 선보였다. 이 프로그램은 IFA의 트렌드를 업계 전문가들이 직접 설명하는 것으로 이노베이션 엔진 레드와 이노베이션 엔진 블루로 나누어 9월 6일, 8일, 10일에 진행됐다. 이노베이션 레드는 올해 8K TV와 관련 기술, 인공 지능, 5G에 대한 업계 전문가 토론과 강연이 이어졌고, 이노베이션 블루는 지속 가능하고 누구나 접근 가능한 미래 베를린 생활 프로젝트에 관한 이야기를 공유했다.

이처럼 IFA 넥스트는 한 공간을 스타트업에게 내준 프로그램에 그치지 않고, 가장 혁신적인 사람들과 다양한 주제의 이야기를 공유하는 프로그램을 멈춤 없이 진행함으로써 IFA에서 가장 활발한 공간으로 자리 잡고 있음을 입증했다. 이는 결국 IFA를 단순한 가전 전시회의 틀에 가둘 것이 아니라 유럽에 진출해야 할 스타트업이 활용할 좋은 기회로써 확장되는 또 다른 의미도 담고 있다. IFA 넥스트 프로그램이 안정적으로 운영된 IFA 2019로 인해 지루한 IFA에 대한 편견은 조금은 날릴 수 있게 됐다.

# 애플 아이폰11 발표 속 스마트폰 시장 흐름 읽기



최호섭 (work.hs.choi@gmail.com)

디지털 칼럼니스트

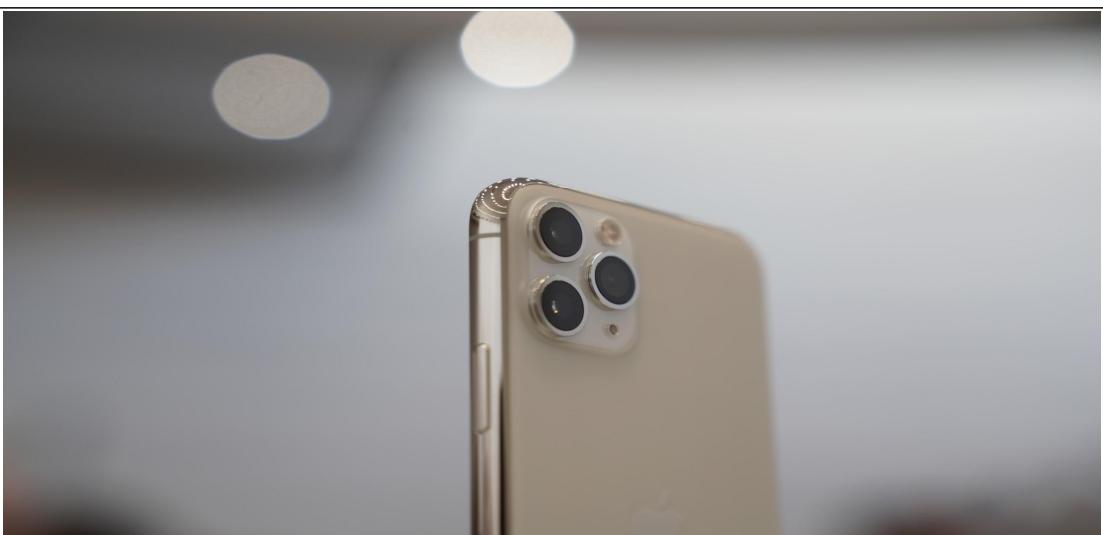
1년에 쏟아지는 스마트폰의 수는 셀 수 없이 많지만, 그 중에서도 애플의 아이폰 발표는 여전히 스마트폰 이용자, 그리고 업계의 큰 관심을 받고 있다. 애플은 여느 때와 마찬가지로 9월 초 애플 본사가 있는 쿠퍼티노의 애플 파크 스티브 잡스 극장에서 신제품을 발표했다.

눈에 띄는 것은 현장 생중계를 자체 홈페이지에서 뿐만 아니라 유튜브 라이브로도 중계했다는 점이다. 애플은 특히 유튜브를 중심으로 한 커뮤니티의 변화를 중요하게 여기는 것으로 보인다. 유튜브 라이브에는 최대 190만 명이 모여서 생중계를 지켜봤다. 애플도 애플이지만 전 세계를 대상으로 하는 유튜브의 막대한 영상 데이터 처리 능력은 놀라웠다.



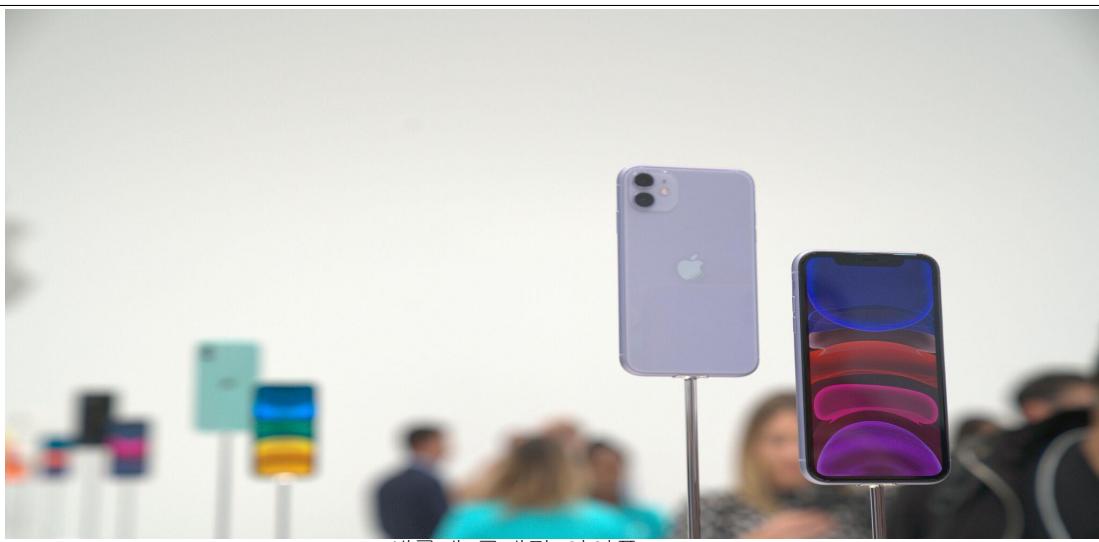
## 비슷한 디자인, 차별점은 카메라

애플은 세 가지 제품을 내놓았다. ‘아이폰11’, 그리고 ‘아이폰11 프로’, ‘아이폰11 프로 맥스’ 등으로 나뉜다. 기본이 되는 아이폰11은 6.1인치 LCD 화면에 표준 화각과 광각 렌즈를 갖춘 제품이다. 케이스는 알루미늄과 유리로 씌웠다. 아이폰11 프로는 스테인리스 스틸 케이스에 5.8인치 OLED 화면과 표준, 광각, 망원 렌즈 등 3개의 카메라를 넣었다. 아이폰11 프로 맥스는 화면 크기를 6.5인치로 늘린 제품이다.



각각 지난해 아이폰XR, 아이폰XS, 아이폰XS 맥스의 후속 제품으로 볼 수 있다. 카메라의 모양을 빼고는 케이스의 기본 디자인도 거의 그대로 닮았다. 모델명에 숫자가 붙는 넘버링 제품에는 전반적인 디자인이 바뀌는 경우가 많은데, 아이폰 6부터 6S, 7, 8까지 비슷한 디자인 톤을 유지했던 것처럼 애플은 11시리즈에서도 이전과 같은 품팩터를 적용했다.

전면 디스플레이 스마트폰 디자인에 큰 변화를 주는 것이 쉽지 않고, 아이폰11은 지난해 아이폰XR로 처음 등장한 디자인이기 때문에 서둘러 바꿀 필요는 없다. 어쨌든 애플은 디자인을 급격하게 바꾸는 대신 아이폰X의 디자인을 아직 쓸 만하다고 판단한 듯하다. 다만 베젤이 극단적으로 사라지고, 아예 제품 옆까지 흘러나오는 스마트폰 디자인이 많고, 노치 역시 다른 형태로 바뀌는 유행과 비교하면 지금 아이폰11 시리즈의 디자인은 아이폰X 출시의 파격에서 보수적인 느낌으로 다가오기도 한다.



새롭게 공개된 아이폰 11

## 아이폰XR의 자연스러운 합류, 정리되는 브랜드

기기의 구성은 지난해와 비슷하지만 이름에는 큰 변화가 생겼다. 올해 애플은 브랜드를 새로 정리했다. 아이폰XR의 후속 제품을 아이폰11로 이름 붙이고, 아이폰XS 계열의 후속 제품은 ‘아이폰11 프로’로 부른다.

지난해에는 아이폰XS를 중심으로 아이폰XS 맥스로 화면을 확장하고, 디스플레이와 카메라에 차이를 둔 아이폰XR 등으로 갈렸다. 아이폰XR은 결과적으로 지난 1년 동안 가장 많이 팔린 스마트폰이자, 전체 아이폰 판매량의 절반 이상을 차지한 제품이다. 하지만 아이폰XR에 대한 마니아층의 반응은 뜨뜻미지근했다. 이를 때문이다.

아이폰XR은 똑같이 A12 바이오닉 프로세서를 넣고 운영체제나 소프트웨어 지원 등 전체적으로 성능과 경험에 큰 차이가 없었지만 ‘R’이라는 이름 때문에 정식 시리즈에 들어가지 못하는 느낌을 주었다. 이는 제품을 선택하는 데에도 영향을 끼칠 수밖에 없다. 하지만 아이폰XR은 흥행에 성공한 기기였고, 애플 역시 이 기기에 의미를 부여하고 싶어 하는 것으로 보인다.

애플로서도 지난해에는 중심을 아이폰XS에 둘 수밖에 없는 일이었다. 어쩌면 애플은 지난해 아이폰XR을

발표하면서 지금과 같은 이름을 고민했을 수 있다. 하지만 'S'가 붙는 아이폰XS는 아이폰X의 후속 제품이기 때문에 그 이름을 쓸 수밖에 없다.

11로 이름을 바꾸면서 아이폰XR 계열은 자연스럽게 정식 라인업에 포함됐다. 그리고 자연스럽게 고가 라인업에 가치를 더 높일 수 있는 '프로'를 더했다. 누구도 불만을 느끼지 않을 교통정리다. 간단한 것처럼 보이지만 브랜드를 바꾸기는 쉽지 않은 일이다. 디자인이 파격적으로 바뀌지 않았기 때문에 부담스러울 수도 있다. 하지만 이 이름 변화는 제품 전체에 대한 인상을 바꾸는 데에 큰 영향을 끼친다. 결과적으로 아이폰7, 아이폰8을 쓴 이들이 자연스럽게 아이폰11로 넘어갈 수 있는 계기가 된다.

## 아이폰 진화의 중심에 프로세서와 카메라가 있는 이유

최근 아이폰 진화의 중심에는 프로세서가 있다. 아이폰X과 함께 등장했던 'A11 바이오닉' 프로세서는 지난해 아이폰XS의 'A12 바이오닉'을 거쳐 올해 'A13 바이오닉' 프로세서로 진화했다. 이를 뒤에 붙는 수식 어로 바이오닉을 고집하는 이유는 애플의 프로세서 개발 지향점이 뉴럴 엔진, 즉 머신 러닝에 있다는 것을 강조하는 것으로 풀이된다.

새 A13 프로세서도 기본 구조는 A12와 크게 다르지 않다. 기본 프로세서 성능은 20% 정도 높아졌고 전력 소비 효율도 크게 올라갔다. 사실상 A12 프로세서는 발표 1년이 지난 지금까지도 가장 빠른 프로세서의 자리를 지키고 있다. A13으로 그 기록이 경신된 것뿐이다. 애플은 전체적으로 성능은 20%, 효율은 40%까지 높아졌다고 한다.

하지만 여러 벤치마크 테스트를 통해 아이폰11의 A13 바이오닉 프로세서가 A12 바이오닉 프로세서보다 그렇게 인상적으로 빠르지 않다는 분석도 나오고 있다. 실제 피크 성능은 더 좋지만, 앱을 실행하고 구동하는 상황에서는 A12 바이오닉 프로세서와 비슷하다는 것이다. 이는 애플이 즐겨 쓰는 방법이기도 하다. 피크 성능만큼 애플이 중요하게 여기는 것이 바로 전력 효율이다. 애플은 매년 같은 비슷한 전력 소비량의 반도체로 더 높은 성능을 내도록 하고 있다. 그다음 이를 적절히 튜닝하면 비슷한 성능을 훨씬 적은 전력으로 처리할 수 있다. 그 적정선을 찾아내고, 이질감 없이 작동하도록 하는 것이 바로 iOS의 힘이다.

애플의 임원들이 와이어드와 나눈 인터뷰에서도 이 프로세서 설계 과정에서 전력 소비 효율에 특히 큰 공을 들였다는 것을 알 수 있다. 필립 실러 마케팅 수석 부사장은 85억 개 트랜지스터를 효율적으로 운영해서 새 아이폰들이 한 번 충전으로 지난 세대 제품보다 5시간을 오래 쓸 수 있도록 하는 것에 중심을 두었다고 밝히기도 했다.

반도체 기술에서 처리 속도와 전력 소비량 사이의 미묘한 줄다리기는 필연적인 요소다. 애플은 넉넉한 성능을 기반으로 균형을 찾은 셈이다.

애플은 이번에도 세 가지 제품을 내놓았고, 가격과 성격도 약간씩 다르지만 프로세서는 모두 A13 바이오닉을 넣어 성능을 똑같이 맞췄다. 물론 메모리를 4GB와 6GB로 구분해서 전반적인 시스템 성능에는 차이가 있을 수 있지만 세 제품은 똑같은 세대의 제품이고 할 수 있는 일과 그 결과물, 즉 경험은 다르지 않다.

## 애플에 중요한 것은 하드웨어에 지속성 줄 수 있는 ‘플랫폼’

애플에 가장 중요한 것은 당장의 하드웨어보다 생태계 중심의 플랫폼 영향력이다. ‘아이팟’이 다른 MP3 플레이어와 차별점을 둘 수 있었던 것은 바로 ‘아이튠즈’라는 음악 생태계가 있었기 때문이고, 아이폰이 여느 스마트폰과 가장 다른 경험을 만들어 준 것이 바로 ‘앱스토어’다. 결국 기기의 효용성은 더 좋은 기기 그 자체가 아니라 기기의 성능을 충분히 이용하고 잠재력을 끌어내는 소프트웨어, 앱 생태계에 달려 있다는 것을 애플은 누구보다 잘 알고 있다.

이 때문에 애플은 최근 개발자 콘퍼런스 WWDC를 비롯해 새 하드웨어를 내놓을 때 뉴럴 엔진과 머신러닝 도구 ‘ML킷’을 강조한다. 또한 공간을 새로 해석하는 증강현실에 대한 부분도 빠지지 않는다. 결국 머신 러닝과 증강현실이 앞으로의 앱 생태계에 큰 영향을 끼칠 것이라는 확신에서 나오는 판단이다. 그 과정에서 하드웨어, 소프트웨어, 운영체제, 플랫폼 모두가 같은 방향을 바라보고 체계적으로 움직이는 것은 애플의 강점이기도 하다.



아이폰 11 프로 및 아이폰 11 프로 맥스

그 경험이 당장 만들어지는 것은 아니다. 애플도 이를 잘 알고 있다. 어쨌든 그 과정에 더 좋은 카메라와 더 빠른 프로세서가 필요한 것은 사실이. 그래서 애플은 할 수 있는 한 뉴럴 엔진의 성능을 모든 기기에 똑같이 넣으려고 하는 것이다. 언젠가 이 두 열쇠로 만들어진 앱들이 활발하게 쓰아지기 시작하면 이제까지의 기기들에서 거의 비슷한 경험을 만들어줄 것이고, 이는 곧 앱 개발자들에게 가장 강력한 동기 부여가 된다. 누구나 찾아와서 돈을 벌어가라고 ‘판’을 깔아주는 것이다. 앱스토어의 기본 기조이기도 하다.

여기에서 카메라의 확대도 단순한 광각 렌즈의 확보가 목표는 아니라는 것을 읽을 수 있다. 증강현실은 애플이 가장 공을 들이는 콘텐츠 중 하나다. 증강현실은 우리의 세상과 가상공간을 연결해주는 기술인데, 그 과정에서 세상을 더 정확하게 받아들이고, 공간에 대해 더 많은 정보를 확보하려면 결국 더 좋은 카메라가 필요하다. 카메라의 개수도 중요할 뿐만 아니라 공간을 더 넓게 바라보는 광각 카메라의 역할도 놓칠 수 없다.



게임 구독 서비스 ‘애플 아케이드’

애플이 모든 아이폰11에 광각 카메라를 더하고 여기에 머신 러닝 기반으로 사진을 매만지는 ‘딥 퓨전 (Deep Fusion)’을 더한 것이 바로 그 증거다. 물론 이 카메라 기술은 자연스럽게 ‘카메라의 기술에도 머신 러닝이 더해지면 기존과 다른 결과물을 만들어낼 수 있다’는 것을 스스로 증명하는 과정이기도 하다. 그리고 카메라가 사물을 그냥 바라보기만 하는 것이 아니라 직접 그 내용을 읽고 판단하기 때문에 증강현실에도 훨씬 유리할 수밖에 없다.

결국 애플이 최근에 내놓고 있는 하드웨어는 더 나은 스마트폰, 태블릿 등의 형태보다 새로운 흐름의 생태계를 더 확장할 수 있는 토대가 되는 플랫폼 하드웨어에 가깝다고 볼 수 있다. 아이폰과 함께 공개된 ‘애플 아케이드’나 ‘애플TV+’ 등의 서비스 역시 또 다른 형태의 독점 서비스이기도 하다.

# 미국과 중국의 인터넷 미래 전망: 5G 선점을 위한 경쟁



유성민 (dracon123@naver.com)

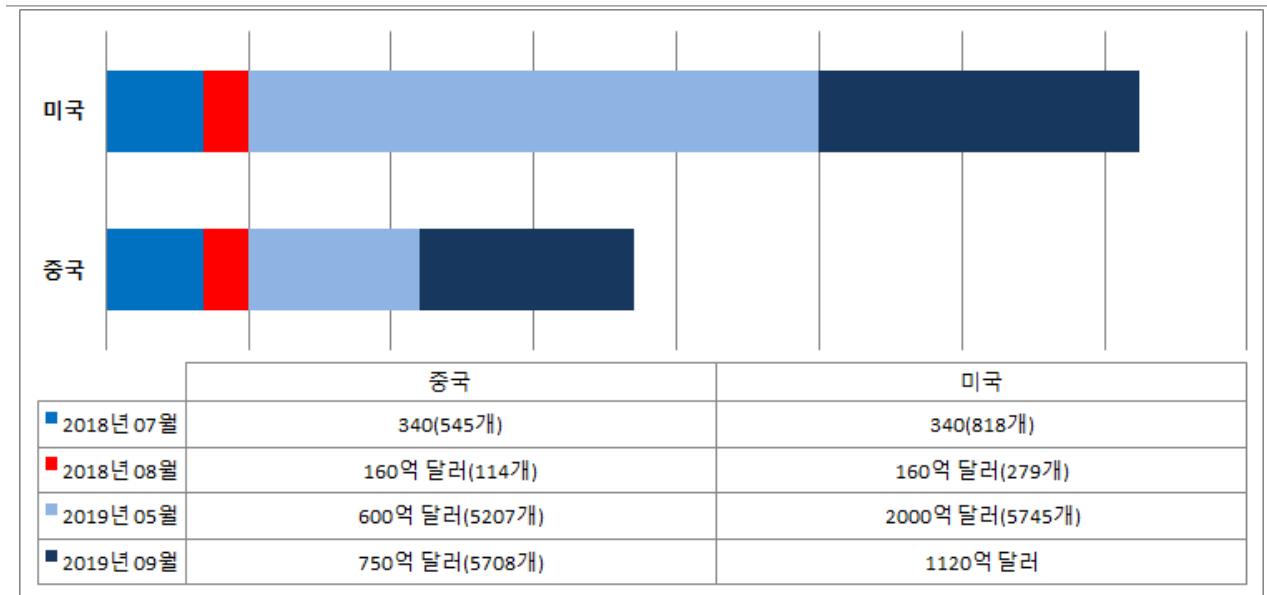
동국대학교 국제정보보호대학원 외래교수  
IT 칼럼니스트

미·중 무역 충돌은 세계적인 주요 화두이다<sup>1)</sup>. 두 국가의 무역 충돌은 세계 경제에 큰 영향을 미치기 때문이다. 무역 충돌은 2018년 7월로 거슬러 올라간다.

당시 미국은 중국에서 오는 수입품목 관세율을 10%에서 25%로 상향했다. 대상 품목은 818개로 340억 달러(약 40조 8,000억 원)에 달하는 수치였다. 중국도 미국과 똑같은 방법으로 대응했다. 중국은 미국에서 수입하는 545개 품목에 관세율을 똑같이 25%를 적용했다. 규모도 340억 달러(약 40조 8,000억 원)로 비슷하다. 이어 8월에 양국은 추가로 상대국으로부터 오는 160억 달러(약 19조 2000억 원) 규모의 수입 품목에 25% 추가 관세를 부과했다.

1) 신동아, “中 판매 국산 스마트폰, 화웨이 OS로 만들 판”, 2019년 06월.

미국과 중국의 관세 부과 금액 규모



미국과 중국은 주고받은 형태로 관세 전쟁을 중심으로 한 무역 갈등을 올해까지 유지하고 있다. 이는 1년이 지난 올해 9월까지도 유지하고 있다. 지난 5월 미국은 추가로 5천 745개 수입 품목(2,131억 300만 달러)에 25% 추가 관세율을 부과했다. 이어 중국도 6월에 5천 140개 수입 품목에 25% 추가 관세율을 부과했다. 9월에는 미국이 1,120억 달러(약 130조 원) 규모의 중국 수입품에 15% 관세를 부과했고, 중국은 이에 750억 달러(약 90조 원) 규모의 미국 수입품에 5%와 10% 추가 관세를 부과했다.

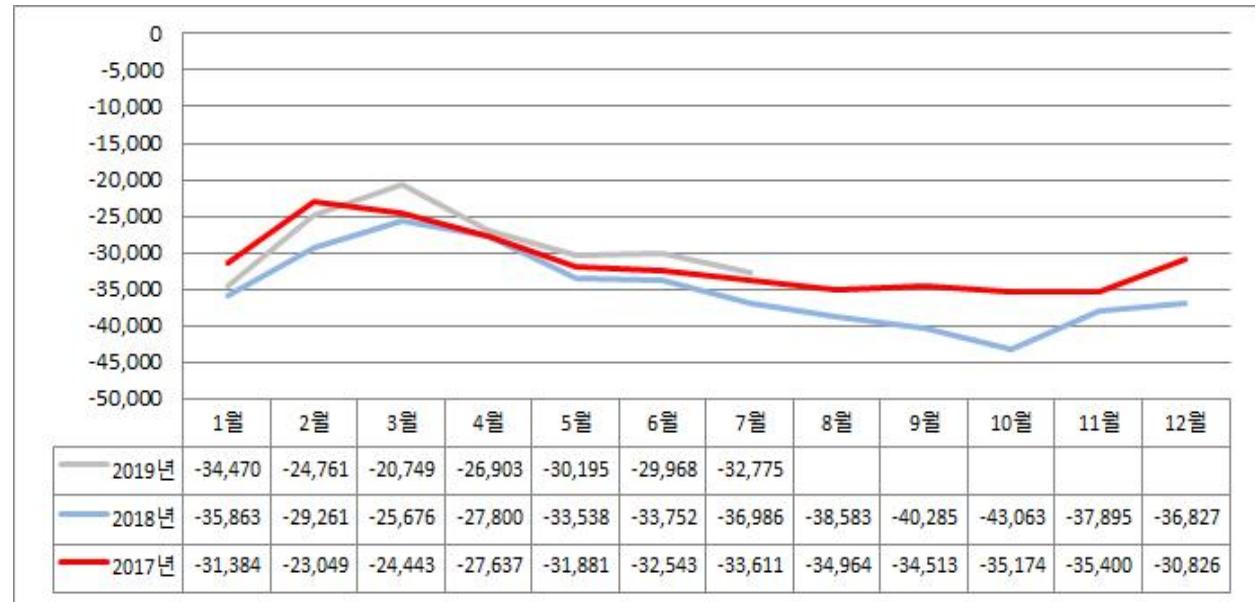
## 무역 전쟁의 원인은 기술 패권 경쟁

이처럼 미국과 중국은 한 치의 양보 없이 무역 갈등을 유지하고 있다. 이러한 갈등은 서로에게 득이 될 것이 없다. 그런데도 무역 충돌을 벌이는 까닭이 무엇일까? 일부 전문가는 미국이 무역 적자를 줄이기 위한 것으로 해석하고 있다. 타당성이 있어 보인다. 그러나 생각보다 효과가 없다. 중국도 미국으로부터 수입에 대해 대응했기 때문이다. 다시 말해, 미국이 중국으로부터 수입 의존도를 줄인 만큼, 중국으로 가는 수출 품목도 줄어든다.

실제로 미국 무역 수지 데이터를 보면 이를 알 수 있다. 미국 통계국(USCB)은 미국이 중국과의 무역 수지에 관한 데이터를 제공하고 있다<sup>2)</sup>. 미중 무역 충돌이 없었던 2017년과 충돌이 시작한 2018년을 비교하면, 오히려 2018년의 미국 무역 적자가 더 컸다. 물론 무역 충돌이 본격화된 2019년은 2017년보다 무역 적자가 더 적다. 그러나 수치상으로 봤을 때 큰 차이는 없다.

2) 미국 통계국(USCB), “Trade in Goods with China”, <https://www.census.gov/foreign-trade/balance/c5700.html>.

### 중국과의 무역에서 미국 무역 수지 현황 (2019년 8월 기준) USCB 데이터 인용)



[출처: USCB 데이터를 인용해 그래프로 표현]

그래서 대부분 전문가는 이번 무역 충돌을 기술 패권을 위한 갈등으로 해석하고 있다. 국가안보전략연구원은 미·중 무역전쟁을 첨단 기술 확보 선점을 위한 기술전쟁으로 분석했다<sup>3)</sup>. 이러한 사실은 지난 5월 추가 관세 품목에서 확인할 수 있다. 미국은 2,131억3000만 달러(255조7000억 원)의 추가 관세 품목 중 972 억6000만 달러(116조7000억 원)의 기계·전자류 항목에 추가 관세를 부과했다. 또한, 중국은 화웨이, 중심 통신(ZTE) 등에 수입 제재를 가하기도 했다.

정리하면, 미국과 중국의 기술 패권 경쟁은 무역 갈등으로 보이고 있다. 그럼 이러한 갈등이 심화될 산업은 어디일까? 5세대 무선통신(5G)이 심화할 영역으로 보일 전망이다. 5G는 기존 4세대 무선통신(4G)보다 20배 더 빠르고, 지연 시간은 10분의 1가량으로 적다. 따라서 5G는 4차 산업혁명의 고품질 서비스에 핵심 인프라로 간주되고 있다.

퀄컴(Qualcomm)은 피에스비(PSB)라는 시장 조사 기관과 함께 5G가 시장에 미치는 영향력을 비교했다<sup>4)</sup>. 퀄컴은 2035년에 5G가 산업에 미칠 영향력이 12.3조 달러(약 1.47경 원)에 이를 것으로 분석했다<sup>5)</sup>. 세계 총생산량(GDP)로 환산하면, 3조 달러(약 3,600조 원)에 달한다. 그리고 2,200만 개의 직업을 창출할 전망이다.

3) 박병주, “미·중 무역전쟁의 배경과 시사점”, 국가안보전략연구원, 이슈브리프 18(48), 2018.

4) PSB, “5G Economy Global Public Survey Report Commissioned by Qualcomm”, December 2016.

5) Qualcomm, “The 5G Economy”, <https://www.qualcomm.com/invention/5g/economy>.

## 미국과 중국의 5G 정책 비교

5G가 미치는 영향력이 커짐에 따라, 5G는 세계적으로 주목받고 있다. 미국과 중국도 마찬가지로 주목하고 있다. 미국 대통령 ‘도널드 트럼프’는 연설문에서 현재 미국 통신업자가 2,750억 달러(330조 원) 규모로 5G 산업에 투자하고 있다고 주장했다. 이어서 300만 개의 일자리 창출과 5천억 달러(약 600조 원)의 경제 가치를 유발할 것으로 전망했다<sup>6)</sup>. 도널드 트럼프 대통령은 이러한 이유로 5G 산업에 집중적으로 투자해야 한다고 주장했고, 이를 놓치면 미래 정보통신기술(ICT) 분야를 선동할 수 없다고 주장했다.

트럼프 대통령의 연설문에서도 알 수 있듯이, 미국은 5G 산업을 미래 유망 산업으로 육성하려 하고 있다. 실제로 연방통신위원회(FCC)는 산업 활성화를 위해 시외 지역에도 5G 인프라에 투자할 계획이라고 밝혔다. 이를 위해 십 년간 204억 달러(약 24.4조 원)를 투자 한다<sup>7)</sup>.

중국은 5G를 미래 성장 동력으로 바라보고 있으며, 중국 공업정보화부 중심으로 이를 추진하고 있다<sup>8)</sup>. 2013년 2월 5G 활성화를 위해서 정부, 민간, 학계가 협력할 수 있는 IMT-2020 추진 조직을 발족했다. 또한, 중국 정부는 5G 상용화를 위해서 2단계로 나눠서 사업을 추진하고 있다. 1단계(2016~2018)에서는 핵심 기술 개발 및 시험 단계에 초점을 둘 사업을 진행했고, 2단계(2018~2020)에서는 5G 상용화를 목표로 추진한다.

미국과 중국의 관세 부과 금액 규모

국 가	대상기업	특허 비율
중국	화웨이, ZTE, CATT, 오포	35.51%
유럽	노키아, 에릭슨, 시스벨, 이노베이션 테크놀로지	23.1%
한국	삼성, LG, KT	21.42%
미국	퀄컴, 인텔, 인터디지털, 애플, 옵티스	14.29%
일본	샤프, 후지쯔, 소니, NEC	5.4%

출처: CGS Global Focus(University of Bonn)

6) WhiteHouse, “Remarks by President Trump on United States 5G Deployment”, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-united-states-5g-deployment/>, April 2019.

7) Engadget, “FCC announces 5G airwave auction and \$20 billion rural broadband fund”,

<https://www.engadget.com/2019/04/12/fcc-5g-airwave-auction-rural-broadband-funding/>, December 2019.

8) 이규복, “중국의 5G 이동통신 정책 추진 현황”, 과학기술정책연구원, 과학기술정책 27(8), 2017년 08월, 38-43쪽.

이처럼 미국과 중국은 5G 산업 육성에 적극적이다. 그럼 두 국가를 비교하면, 현재 어느 국가가 좀 더 우위에 있을까? 본 대학교(University of Bonn)는 5G 관련 대표 기업 25곳을 선정하고, 5G 관련 특허 보유수를 분석했다<sup>9)</sup>. 중국(35.51%), 유럽(23.1%), 한국(21.42%), 미국(14.29%), 일본(5.3%) 등 순을 이었다.

영국 시장 조사 전문 기관 ‘애널리시스 메이슨(Analysis Mason)’은 국가별 5G 준비도를 조사했다. 그리고 미국과 중국이 19점으로 비슷한 순위를 유지했다. 이어 한국(18점), 일본(17점), 이탈리아(15점), 영국(15점), 홍콩(14점), 호주(13점), 스페인(11점) 등 순을 이었다<sup>10)</sup>.

정리하면, 특히 보유수에서는 중국이 미국보다 앞선 듯하다. 그러나 조사 대상 기업이 제한적이므로 이러한 결과를 무조건 신뢰하기 어렵다. 5G 준비도 측면에서는 미국과 중국이 서로 비슷한 위치에 놓여있다. 이에 따라, 미국과 중국이 5G 선점을 위한 경쟁이 불가피함을 보여준다.

미국과 중국의 5G 기술 수준을 분야별로 좀 더 세분화해서 봤을 때는 어떨까? 5G 통신 상용화, 5G 장비 업체 그리고 5G 스마트 폰으로 나눠서 바라볼 수 있다. 이에 관해 좀 더 살펴보자.

## 5G 통신 상용화 비교

5G 통신 상용화 수준은 미국이 앞서고 있다. 미국은 5G 주파수 경매를 2018년 11월에 최초로 시작했다. 그래서 미국 여러 통신사는 올해를 목표로 상용화를 준비하고 있다. 다만, 버라이즌 통신사는 독특하게 5G를 출시했다. 2018년 10월 스마트홈 전용 5G를 출시했다. 그러나 전문가는 이를 5G 상용화로 보지 않고 있다. 실질적인 5G 상용화는 4월 4일에 이뤄졌다. 한국 다음으로 바로 상용화했다. 도시는 시카고와 미니애폴리스 등 일부 지역을 대상으로 하고 있다<sup>11)</sup>. 이어 스프린트는 지난 5월 말에 5G를 상용화했다. 애틀란타, 휴스턴 등 지역에 제공한다. 2019년 6월 T-mobile은 6개 지역을 대상으로 5G 서비스를 상용화했다. AT&T는 지난 8월이 돼서야 뉴욕시 등 일부 지역을 대상으로 5G를 상용화했다<sup>12)</sup>.

중국은 미국과 비교하면 5G 상용화 속도가 느리다. 5G가 중국은 8월을 목표로 5G 상용화를 준비했다. 그러나 9월 25일 기준으로 5G 서비스가 제공된 중국 도시는 아직 없다. 중국 상하이에서 5G가 최초로 상용화될 것으로 전망되고 있다<sup>13)</sup>.

9) Xuewu Gu and etc., “Geopolitics and the Global Race for 5G CSG Global Focus”, CGS Global Focus, pp.1-84, May 2019.

10) Analysis Mason, “Global Race to 5G”, April 2019.

11) 매일경제, “‘2시간 차이’…한국, 미국 버라이즌에 앞서 ‘세계 최초 5G’”, <https://www.mk.co.kr/news/it/view/2019/04/206981/>, 2019년 4월.

12) Lifewire, “When Is 5G Coming to the US?”, <https://www.lifewire.com/5g-availability-us-4155914>, September 2019.

13) KOTRA, “5G 우선 시범 도시 상하이와 중국 5G 시대”, <https://news.kotra.or.kr/user/globalBbs/kotranews/782/globalBbsDataView.do?setIdx=243&dataIdx=174069>,

중국이동, 중국전신, 중국연통 등 중국 3대 통신사가 5G를 준비하고 있고, 베이징, 항저우 등 여러 지역에 5G 서비스를 상용화할 계획이다. 특히 중국이동은 50개 도시를 대상으로 5G를 상용화하는 방향으로 준비하고 있다<sup>14)</sup>.

## 5G 통신 장비와 5G 스마트폰 현황 비교

5G 통신 장비 시장도 5G 산업에서 중요하다<sup>15)</sup>. 시장 조사 전문 기관인 마켓스앤드마켓스에 따르면, 5G 장비 시장은 2020년부터 2027년까지 46.7%의 연평균 시장 성장률(CAGR)을 보인다. 다시 말해, 2010년 28.6억 달러(약 3.43조 원)에서 418.7억 달러(약 50.16조 원)로 성장할 전망이다.

5G 통신 장비 부분에서는 중국이 앞서는 듯이 보인다. 중국 5G 통신 장비 기업으로 화웨이를 들 수 있다. 현재 화웨이는 유럽 일부 국가, 한국, 인도 등에서 제공되고 있다. 미국 5G 통신 장비는 시스코와 퀄컴이 있다. 특히 화웨이는 5G 통신 장비 시장에서 다른 경쟁사를 압도하려는 계획을 품고 있다. 화웨이는 세계 시장 3분의 1을 점유하겠다고 밝혔다. 참고로 화웨이는 2019년 6월 기준으로 30여 국의 46개 통신사에 5G 동시 장비를 납품했다<sup>16)</sup>.

5G 스마트폰 시장은 어떨까? 현재 중국은 여러 5G 스마트폰을 출시했다. 오포(레노), ZTE(엑손 10), 샤오미(MiMix3), 화웨이(Mate20X) 등이 5G 스마트폰 모델이다. 이어 중국 스마트폰 제조 기업은 5G 스마트폰 보편화에도 주력하고 있다. 저가형 5G 스마트폰 출시를 준비하고 있기 때문이다. 미국은 모토로라(Moto z3)가 전부이다. 그러나 모토로라 모기업이 중국 기업인 레노버임을 고려하면, 모토로라 또한 중국 기업으로 볼 수 있다. 그렇게 되면, 미국 기업 중 1곳도 5G를 제공하는 기업이 없다. 현재 애플이 5G 스마트폰 출시에 서두르고 있다. 애플은 퀄컴과 특허 사용료 분쟁을 2년간 벌여오다가, 지난 4월에야 막을 내렸다. 사유는 5G 스마트폰 출시로 보인다.

지금까지 보면, 5G 스마트폰 영역은 중국이 압도적으로 우위에 있는 것처럼 보인다. 그러나 이를 세부적으로 살펴보면, 그렇지 않다. 스마트폰에 제공되는 5G 칩이 퀄컴에서 제조된 것이기 때문이다. 중국에서 출시한 5G 스마트폰 전부가 퀄컴에서 제조한 5G 칩(스냅 드래곤)을 사용하고 있다. 원천 기술은 미국이 우위에 있고, 활용 측면에는 중국이 우위에 있는 셈이다.

---

2019년 04월.

14) China Daily, “China Mobile plans to offer 5G commercial services in over 50 cities”, <http://www.chinadaily.com.cn/a/201906/25/WS5d120038a3103dbf1432a2b2.html>, June 2019.

15) MarketsandMarkets, “5G Infrastructure Market”, [https://www.marketsandmarkets.com/Market-Reports/5g-technology-market-202955795.html?gclid=EA1aIQobChMljMbcqZ3s5AlVVWLaWCh1foArIEAYASAAEgJOfD\\_BwE](https://www.marketsandmarkets.com/Market-Reports/5g-technology-market-202955795.html?gclid=EA1aIQobChMljMbcqZ3s5AlVVWLaWCh1foArIEAYASAAEgJOfD_BwE).

16) DigiAnalysis, “List of 5G contracts bagged by Huawei”, <https://www.digianalysys.com/list-of-5g-contracts-bagged-by-huawei/>, June 2019.

샤오미의 5G 전용 스마트폰(MiMix3)



[출처: Flickr]

## 결론

미국과 중국은 5G 선점에 주력하고 있다. 5G 산업 경쟁력 수준은 시장 조사 기관이 분석한 것처럼 비슷하다. 5G 통신 상용화 서비스에서는 미국이 앞서고 있다. 반면 통신 장비 부분에서는 중국이 앞서고 있다. 5G 스마트폰 부분에서는 대등한 수준에 놓여있다. 이러한 점을 봤을 때, 중국이 ICT 수준이 크게 발전됐음을 알 수 있다. 결국, 5G 선점은 중국이 기술력에서 미국을 넘을지를 가늠하게 하는 지표가 될 수 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 양도마차로 내달리는 엣지 컴퓨팅

## 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.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 인증체계 출범
- 「개인정보보호법」과 명확성 등의 요구

## 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.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.5

### 이슈 & 트렌드

- 5G 네트워크 슬라이싱-Network-as-a-Service(NaaS)를 통한 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

VOL.9

2019  
KISA  
REPORT

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



## 주제 제안 및 정기구독 신청 | [kisareport@kisa.or.kr](mailto: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 9월
발 행 처	한국인터넷진흥원 (전라남도 나주시 진흥길 9)
기 획	한국인터넷진흥원 ICT미래연구소
편 집	(주) 해리