

2019 VOL.5

KISA REPORT



CONTENTS.

ISSUE & TREND

- 01 5G 네트워크 슬라이싱 – Network-as-a-Service (NaaS)를 향한 가상 네트워크 기술 (윤대균 / 아주대학교 교수)
- 02 클라우드와 블록체인의 만남 'BaaS' (유성민 / IT 칼럼니스트)
- 03 AI 기반 사이버보안 – 이용·인식현황 중심으로 (이용용 / ICT&Security 애널리스트)
- 04 스마트공장 보안 (김계근 / SK인포섹 DS컨설팅팀장)
- 05 스마트시티 서비스를 위한 플랫폼 주요 보안 기술 (김호원 / 부산대 교수)
- 06 의료기관 정보보호 강화를 위한 노력 (경우호 / 병원정보보안협의회 회장)
- 07 2019년 마이크로소프트 빌드, 페이스북 F8, 구글 I/O에서 발표한 인공지능 기술과 그 의미 (한상기 / 테크프론티어 대표)
- 08 중국과 미국의 기반기술 주도권 경쟁 (박성림 / 국립타이베이간호건강대학 강사)
- 09 디즈니의 OTT 시장 진출, 눈여겨 볼 지점들 (최홍규 / EBS 연구위원)

주제 제안 및 정기 매일 신청 | kisareport@kisa.or.kr

인터넷 정보보호 관련 이슈, 현안 등 궁금한 내용을 보내주시면 선별 후 보고서 주제로 선정됩니다.

또한, KISA Report 온라인 서비스 제공을 원하실 경우 신청해주시면 매월 받아보실 수 있습니다.

5G 네트워크 슬라이싱 - Network-as-a-Service (NaaS)를 향한 가상 네트워크 기술



윤대균 (dkyoon@gmail.com)

- (現) 아주대학교 소프트웨어학과 교수
- (現) 더블에이치 고문
- (前) 삼성전자 무선사업부 전무
- (前) 엔에치엔테크놀로지서비스 대표
- (前) 엔에이치엔 전략사업본부장

통신사업자의 5G 서비스가 시작되고 이에 발맞추어 5G를 지원하는 스마트폰들이 시장에 출시되면서, 이제 본격적으로 5G 시대를 실감하게 되었다. 지난 3G, 4G 시대를 경험했던 일반 사용자의 입장에서 5G의 도입은 빠른 전송속도에 대한 기대감을 준다. 4G, 즉 LTE가 도입되었을 때 "LTE급 속도"라는 표현을 "매우 빠르고 민첩함"을 나타내는 수단으로 즐겨 사용하였던 것을 쉽게 떠올릴 수 있다. 이러한 맥락을 이어간다면, 이젠 "LTE급 속도"라는 표현 대신, "5G급 속도"라는 표현을 써야 시대에 뒤떨어지지 않는 비유가 될 것이다.

그러나 5G는 이전의 3G, 4G와 비교했을 때 "속도"뿐만 아니라 몇 가지 중요한 목표를 가지고 탄생하였다. 4차 산업혁명 시대의 주요 키워드인 "초연결 시대의 지능화"를 실현하기 위한 인프라로서 갖추어야 할 요건을 정의한 것이다. 여기엔 "초고속"과 함께, "초연결", "초저지연" 목표가 포함되어 있다. 이 각각은 다음과 같은 세 가지 카테고리로 구분된다.

- eMBB (Enhanced Mobile Broadband): 초고속 전송속도를 지향하며, 화상회의, 원격진료, VR 스트리밍 등과 같은 데이터 전송량이 많은 어플리케이션을 주요 유즈케이스(Use case)로 한다.
- mMTC (Massive Machine Type Communications): 초연결을 목표로 하며, 스마트시티, 스마트빌딩, 센서

네트워크, 각종 태그 트래킹 등과 같이 매우 많은 기기 간 원활한 통신을 가능하게 한다.

- uRLLC (Ultra-Reliable and Low-Latency Communication): 초저지연을 목표로 하며, 자율주행 자동차, 원격수술, 공장 자동화 등, 전송지연을 최소화함과 동시에 신뢰도가 높은 통신을 가능하게 한다.

이 세 가지 카테고리의 목표에 따라 각각이 지향하는 응용 분야에서 실제 필요로 하는 정량적 요구사항도 각기 다르게 정의된다. eMBB에서는 10Gbps가 넘는 데이터 전송속도를 목표로 하고 있으나, mMTC는 1Kbps에서 100Kbps 전송속도가 기준이다. 대신 1km² 내에서 동시에 100만대 기기까지 연결될 수 있어야 하며, 배터리도 최고 15년까지 사용할 수 있을 정도의 초저전력 소모 등 매우 도전적인 요구사항을 제시하고 있다. 한편 uRLLC는 50Kbps에서 10Mbps 정도의 보수적인 전송속도를 제시하고 있지만, 사용자단, 즉 end-to-end 지연시간에 대해서는 1ms 내외의 초저지연(ultra low latency)을 요구한다. 자율주행 자동차나 원격수술과 같은 응용 분야에서는 반드시 필요한 요구사항이다.

하나의 물리적 인프라, 다수의 가상 네트워크

다양한 유즈케이스에 대한 목표를 하나의 네트워크 인프라로 구현하는 것이 과연 기술적으로 가능할까? 4G의 등장이 다양한 산업 분야에 적잖은 영향을 끼쳤으나 가장 많은 혜택을 본 영역은 높은 전송속도를 필요로 하는 스트리밍 영역이다. 음악 서비스는 주류가 기존 MP3 다운로드 서비스에서 스트리밍 서비스로 전환되었으며, 또한 유튜브와 같은 동영상 스트리밍 서비스가 보편화된 데에도 4G의 높은 전송속도가 큰 역할을 했다. 높은 전송속도를 지향하는 4G 네트워크에서 충분히 가능한 응용 분야들이다.

그러나 수많은 센서와 이로부터 데이터를 수집하고 분석하는 다양한 기기가 춤출하게 연결된 IoT (Internet of Things) 서비스의 경우 4G 네트워크만으로는 충분하지 않다. 국내 이동통신 사업자들은 IoT 서비스를 위한 전용망을 구축하여 이러한 요구사항에 대응하였으며, 그 예로 IoT 전용망인 로라(Lora) 전국망 구축을 들 수 있다. 기존 4G 네트워크로 지원하기 어려운 요구사항들을 수용하기 위해 IoT 기기 및 서비스 기업들과 연합하여 새로운 인프라를 구축한 것이다. 기존 4G망 장비나 시설들을 일부 활용하였다고 하더라도 4G와는 엄연히 다른 별도의 물리적 네트워크이다.

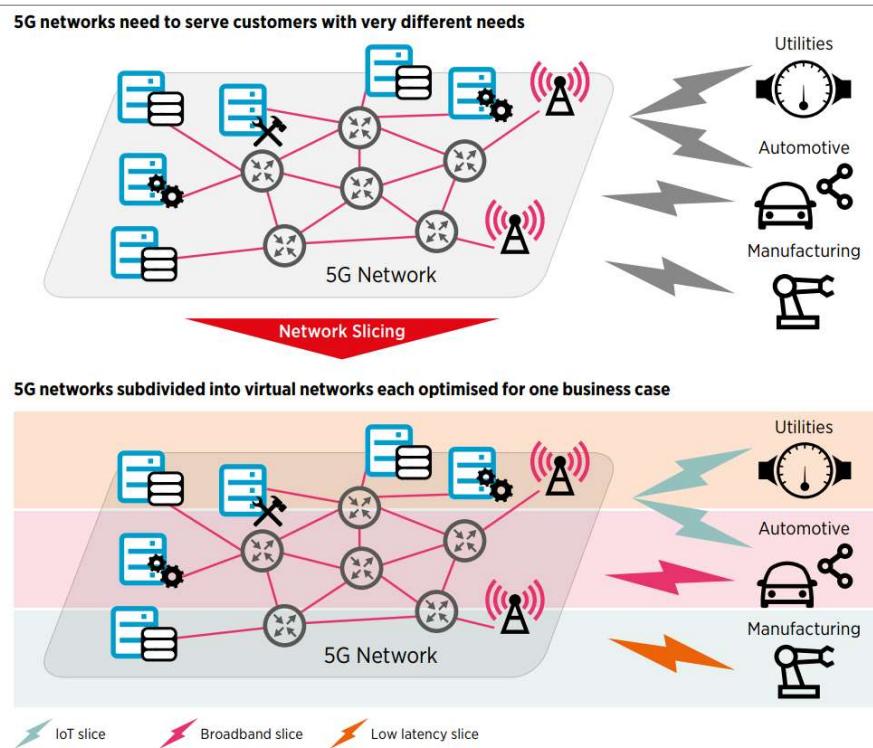
5G에서는 3G, 4G로 이어져 오던 초고속 데이터 전송과 함께 IoT의 초연결 요구사항도 모두 지원하는 것을 목표로 하고 있다. 여기에 자율주행 자동차와 같은 4차 산업혁명의 랜드마크 서비스들을 구현하기 위해서는 네트워크의 지연(latency)도 최소화하는 것이 필요하다. 이 각각의 서비스, 즉 각기 다른 성능 목표를 하나의 물리적인 네트워크로 가능하게 하는 것이 5G가 추구하는 가치이다.

동일한 물리적 네트워크상에서 각기 다른 속성의 가상 네트워크를 통해 다양한 카테고리의 서비스 구현을 가능하게 하는 것이 “5G 네트워크 슬라이싱”이다. 물리적 네트워크 인프라를 논리적으로 구분되는 다수의 네트워크로 분할, 앞서 언급된 5G 주요 유즈케이스들을 구현할 수 있도록 한다는 것이다. 예를

들면, IoT를 위한 초연결 서비스, 초고속 전송을 요구하는 서비스, 초저지연을 요구하는 서비스 이 각각의 카테고리에 적합한 별도의 네트워크 슬라이스를 구성하는 것이다. (그림 1) 각각의 슬라이스는 특정 비즈니스 케이스에 최적화된 네트워크 환경을 제공하며, 고객은 자신의 비즈니스 목적에 맞는 “슬라이스”를 활용하게 된다.

통신사업자의 경우 모든 용도의 슬라이스를 제공하는 것이 일반적이나, 경우에 따라선 일부 특정 목적에 부합하는 슬라이스를 제공할 수도 있다. 통신망을 임대하여 독자적인 이동통신 서비스를 제공하는 MVNO(Mobile Virtual Network Operator)의 경우 일부 도메인에 특화된 서비스를 표방하며 전문화된 슬라이스만을 제공할 수도 있다. 국내, 기존 MVNO들이 주로 차별화된 가격 정책으로 고객들을 유인하였다면, 앞으로는 특정 도메인에 전문화된 통신 서비스를 차별화 포인트로 시장에 등장할 가능성이 클 것으로 예상할 수 있다. 또한, 애플리케이션의 특성상 하나의 슬라이스가 아닌 여러 슬라이스를 필요로 할 수 있다. 대표적인 것이 자율주행 자동차인데 이는 광대역 폭의 데이터 전송과 초저지연 모두 필요로 하므로, 해당 용도에 맞는 두 개 이상의 슬라이스를 활용하게 된다.

네트워크 슬라이싱 개념 설명도



(출처: GSMA)

네트워크 슬라이싱에 기반을 둔 스마트 네트워크 – 새로운 B2B 사업기회

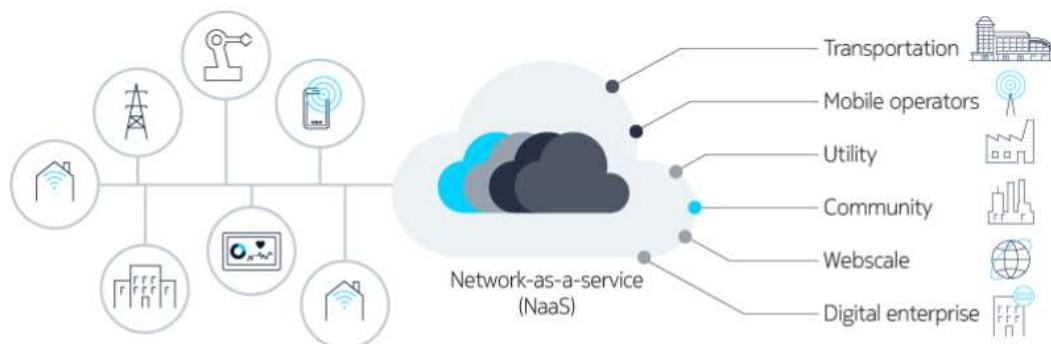
네트워크사업자의 주된 기능 및 가치는 정보를 안전하고 빠르게 특정 지점에서 다른 지점으로 전달할 수 있도록 하는 것이다. 특정 지점은 고정된 위치뿐만 아니라 스마트폰 사용자 위치와 같은 이동성이 있는 지점들을 모두 포함한다. 만일 기업이나 공공기관 같은 고객이 각자의 비즈니스 특성에 맞는 커스터마이즈된 형태의 네트워크가 필요하다면, 별도의 물리적인 네트워크 인프라 구축을 통해 고객의 요구를 충족시킬 수 있다. 그러나 네트워크 슬라이싱을 활용한다면 동일한 물리적 네트워크상에서도 각각 용도에 최적화된 “스마트한” 네트워크 솔루션 제공이 가능하다.

통신사업자는 단순히 정보 전달 수단을 제공하는 것이 아니라 기업의 비즈니스 애플리케이션을 호스팅하고, 비즈니스 수행을 통해 얻어지는 데이터를 수집하며, 이를 분석/가공하여 부가 가치를 제공하는 기능을 수행할 수 있게 된다. 기업마다 요구하는 네트워크 특성이 각기 다르고, 이를 슬라이싱에 기반한 스마트한 네트워크를 통해 지원하게 함으로써, 일반 퍼블릭 클라우드서비스에서 담보하기 어려운 네트워크 성능 요구사항에 대응할 수 있다는 것이 통신사업자가 가지고 있는 최대 강점이다. 통신사업자 입장에서는 별도의 인프라 투자 없이 기업 전용의 가상 네트워크를 제공함으로써 고부가가치의 서비스 창출이 가능하다는 얘기이다. 단, 기존 퍼블릭 클라우드 사업자들이 제공하는 다양한 서비스들을 통신사업자도 제공할 수 있어야 한다. 특히, 통신사업자가 장악하고 있는 네트워크 엣지에서의 서비스, 즉 엣지 컴퓨팅은 5G 확산과 함께 통신사업자들이 당면한 주요 과제이기도 하다. 또한, 논리적으로 완전히 분리된 네트워크 슬라이스를 기업 맞춤형으로 제공함으로써 기업 내에서 수행되는 프로세스와 이로 인해 생산되는 디지털 자산을 안전하게 보호할 수 있다는 것도 내세울 수 있는 주요 장점이다.

네트워크 슬라이스를 API(Application Programming Interfaces)를 통해 제공할 수도 있다. 네트워크와 관련된 형상 정보, 상태 정보들을 제공하는 것뿐만 아니라, 네트워크상에서 수행 가능한 많은 기능을 API를 통해 제공함으로써 전용 가상 망을 확보하기 어려운 소규모 기업의 비즈니스나 서비스 수요에 대응할 수 있다. 퍼블릭 클라우드에서 제공하는 백엔드 as-a-service와 유사한 개념이며, 기술적으로는 소프트웨어 정의 네트워크(SDN: Software Defined Network), 네트워크 함수 가상화(NFV: Network Function Virtualization) 기술 등에 기반하고 있다. API를 활용하면 이미 기업이 보유하고 있는 네트워크나 컴퓨팅 환경을 그대로 유지하면서 5G 네트워크 기능을 통합 운영하는 것도 용이해진다. 컴퓨팅 자원을 클라우드에서 가져다 쓰는 개념과 유사하게 무선 네트워크 기능을 서비스처럼 필요할 때 사용한다는 관점에서 클라우드 RAN(Cloud Radio Access Network)이라고 부르며, 이 클라우드 RAN은 네트워크 슬라이싱 구현의 핵심 요소이기도 하다.

스마트 네트워크는 곧 Network as-a-service(NaaS)의 전형적인 구현 예라고 볼 수 있다. 네트워크 슬라이싱이 5G에 기반한 NaaS를 본격화하는데 촉매가 될 것으로 전망되는 이유이기도 하다.

네트워크 as-a-service 개념도



(출처: Nokia)

주요 사업자 동향 및 과제

미국의 최대 이동통신 사업자인 버라이즌(Verizon)은 아직 정식으로 서비스를 시작하지는 않았지만, 실험적인 환경에서 네트워크의 모든 기저 대역(baseband) 기능을 완전하게 가상화하였다고 발표했다. 이는 특정 네트워크 장비들로 복잡하게 구성된 시스템이 없어도, 일반적으로 활용되는 표준 장비를 이용해 다양한 요구사항의 논리적 무선망 구성 및 활용이 가능하다는 것을 의미한다. 통신사업자가 아니더라도 서비스나 비즈니스에 필요한 무선 네트워크 인프라를 유연하게 구현할 수 있게 되고, 따라서 누구든지 네트워크상 “근처(vicinity)에서” 워크로드(workloads) 실행이 가능한 컴퓨팅 환경을 구축할 수 있게 된다. 방대한 데이터의 전송이 필요하거나, 또는 실시간 요구사항에 따른 저지연 컴퓨팅이 가능하다는 것을 강조하는 것이다. 인텔 및 노키아와의 협력을 통해 진행한 것으로 알려졌다.

AT&T는 에릭슨(Ericsson)과 함께 네트워크 슬라이싱 기술에 대한 검증을 실시한다고 밝힌 바가 있다. 비디오 스트리밍 서비스 품질(QoS)을 보장하기 위한 방편으로 각 사용자단에 네트워크 슬라이스를 적용한다는 것이 이 계획의 주요 골자이다. 유즈케이스 관점에서 완전히 다른 서비스를 대상으로 하는 것은 아니지만, 서비스 품질 달성을 위해 네트워크 슬라이싱을 활용한다는 측면에서는 의미가 있다고 볼 수 있다. 특히 ONAP(Open Network Automation Platform)이라는 오픈소스 프로젝트를 활용함으로써 ONAP을 함께 검증하는 것도 중요한 목표라고 발표했다. 다양한 오픈소스 프로젝트가 5G 네트워크 서비스에서 더욱 비중이 높아지고 있다는 것은 새겨볼 만하다.

국내 최대 이동통신 가입자를 보유하고 있는 SKT는 이미 2015년에 세계 최초로 네트워크 슬라이싱 기술 시연에 성공했다고 발표한 바가 있다. 이후 2017년에는 사업자 간 네트워크 슬라이싱 연동기술을

시연했다고 발표하기도 했다. 우리나라 최대 통신사업자인 KT도 5G 본격 상용화와 함께 네트워크 슬라이싱 및 가상화 기술의 시범 적용을 공표하고 나섰다.

국내 사업자들의 경우 이미 네트워크 슬라이싱 및 가상화 기술을 확보하고 있음을 시사하고 있으나, 이를 기반으로 한 에코시스템 구축이나 신규 B2B 서비스 추진과 관련된 활동에 대한 정보는 확인하기 어려운 상황이다. 5G 상용화 초기에 기업용 애플리케이션과 연계된 본격적인 서비스 추진은 향후 5G 확산을 위해 매우 중요하다. 국내 이동통신사들의 시범 서비스가 일반 사용자 대상의 엔터테인먼트 분야에서 활발하게 진행되고 있는 것은 그나마 다행스러운 현상이다. 하지만, 다양한 유즈케이스를 지향하는 5G 본래의 목적을 최대한 살리고, 또 이를 기반으로 한 에코시스템 활성화를 위해서는 좀 더 넓은 스펙트럼에서의 적극적인 시도가 필요한 시점이다.

전 세계 이동통신 사업자들의 협력기구인 GSMA에서 2017년에 작성한 네트워크 슬라이싱 자료에서는 네트워크 슬라이싱이 적용될 수 있는 10개의 산업군과 6개의 애플리케이션을 예시로 소개하고 있다. 시범사업을 시작하기 위한 좋은 레퍼런스라 여겨진다. 특히, 기업용 네트워크를 위한 슬라이스 애플리케이션 예는 좀 더 주시할 필요가 있다. 기업용 애플리케이션을 시범사업으로 추진하는 과정에서 네트워크 가상화 더 나아가 네트워크 as-a-service에 기반을 둔 사업 기회를 발굴할 수 있기 때문이다. 장비업체들과 특정 산업 도메인에 특화된 서비스를 전문으로 하는 기업/개인들을 모두 포함하는 에코시스템 구축도 이런 시범사업을 통해 거둘 수 있는 중요한 수확이 될 것이다. 통신사업자 입장에서는 성장성 정체를 해소할 수 있는 중요한 열쇠가 여기에 있을지도 모를 일이다.

[참고문헌]

- 매일경제, "SKT, 세계 첫 IoT 전국망 구축...가스 검침기 등 400만기기 연결", 2016년 7월 4일
- 윤대균, "5G 상용화와 함께 새로이 조명되는 엣지 컴퓨팅", 2019 KISA 리포트 Vol.3, 2019년 3월
- Verizon, "Verizon takes major step towards commercialization of Multi-Access Edge Compute (MEC) and Network Slicing with successful virtualization of baseband unit operations", May 8, 2019
- FierceWireless, "AT&T and Ericsson use ONAP for network slicing", Mar. 28, 2019
- Netmanias, "SK텔레콤, 에릭슨과 5G 핵심 기술 '네트워크 슬라이싱' 세계 최초 시연", 2015년 10월 22일
- ZDnet Korea, "SKT, 네트워크 슬라이스 연동기술 시연", 2017년 2월 15일
- 바이라인 네트워크, "KT, 노키아 5G 네트워크 가상화·슬라이싱 기술 시범 적용한다", 2019년 2월 25일
- GSMA, "An Introduction to Network Slicing", 2017

클라우드와 블록체인의 만남 'BaaS'



유성민 (dracon123@naver.com)

- (現) 동국대학교 국제정보보호대학원 외래교수
- (現) IT 칼럼니스트 (사이언스타임즈, 신동아, 더비체인 등 고정필진)
- (前) KT 융합기술원 연구원

블록체인은 암호화폐로 인해서 주목받은 기술이다. 이러한 이유로, 블록체인이 몇 년 전부터 주목받았다고 하지만, 대부분의 블록체인 관련 주제는 암호화폐 관련이었다. 그러나 블록체인에 대한 관심이 몇 년간 지속됨에 따라, 블록체인은 암호화폐를 벗어나서 자체 기술로서 주목받고 있다.

이러한 현상은 가트너의 10대 유망기술에서 확인할 수 있다. 가트너는 2017년부터 10대 유망기술로 블록체인을 꾸준히 선정해왔기 때문이다. 이는 블록체인이 수년간 지속해서 관심을 받고 있음을 보여준다. 그뿐만 아니라, LG경제연구원은 2016년 보고서에서 "블록체인이 암호화폐를 넘어서 발전할 것"으로 전망했다.¹⁾ 이러한 전망은 실질적으로 맞았다고 볼 수 있다.

4차 산업혁명 기술의 연평균 성장률을 조사한 적이 있었다. 블록체인의 성장률이 다른 4차 산업혁명 기술들보다 1.7배에서 5배 정도 높았다. 이를 한 번 살펴보자.

우선 블록체인을 살펴보면, '마켓 리포트 센터 (Market Report Center)'에 따르면 2018년의 블록체인 시장 규모는 7.08억 달러에 이를 것으로 분석했고, 2024년에는 607억 달러 성장할 것으로 전망했다. 연 평균 시장 성장률 (CAGR)이 무려 88.87%에 이른 셈이다.²⁾ 다른 시장 조사 전문 기관도 블록체인 성장률을 비슷하게 전망했다. '마켓스 앤드 마켓스 (Markets and Markets)'는 2018년부터 2023년까지의 CAGR이 80.2%에 이를 것으로 전망했다.³⁾ 글로벌 마켓 인사이트 (Global Market Insights)는 2018년부터

1) 한수연, "블록체인, 비트코인을 넘어 세상을 넘본다", LG경제연구원, 2016년 08월.

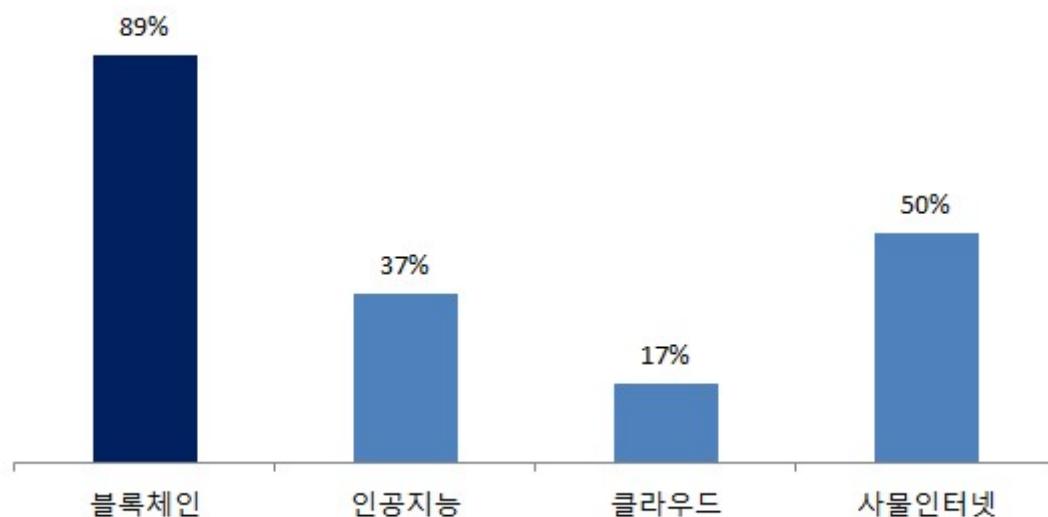
2) Market Reports Center, "Blockchain Market Size is anticipated to reach USD 60.7 billion by 2024", February 14, 2018.

3) Markets and Markets, "Blockchain Market worth \$23.3 billion by 2023", December, 2018.

2024년까지의 CAGR이 75%에 이를 것으로 전망했다.⁴⁾

블록체인 외 4차 산업혁명 기술을 살펴보자. 마켓스 앤드 마켓스는 2018년부터 2025년까지의 인공지능(AI)의 CAGR이 36.62%일 것으로 전망했다.⁵⁾ 클라우드의 경우, 2018년부터 2023년까지 17%의 CAGR 추세를 보일 것으로 전망했다.⁶⁾ 사물인터넷 (IoT)의 시장은 2017년부터 2021년까지 연평균 50%의 성장률을 보일 것으로 전망했다.⁷⁾

4차 산업혁명 유망 기술의 CAGR 비교



이처럼 블록체인 시장 성장은 매우 가파르다. 그런데 이를 위해서는 넘어야 할 장벽이 있다. 그건 바로, 블록체인의 사업화이다. 수많은 블록체인 관련 기술개발이 이뤄지고 있다. 그런데 대부분의 개발 결과물은 사업화로 이어지지 않을 가능성이 높다.

딜로이트(Deloitte)는 블록체인 과제의 성공률을 분석한 적이 있다. 분석 방법은 공동 개발 프로젝트 관리 시스템 '깃허브(GitHub)'를 델프트공과대학에서 개발한 모니터링 툴로 블록체인의 과제 지속성을 계속 점검하는 식으로 이뤄졌다. 딜로이트는 2009년부터 2017년까지 86,034개의 과제가 생겨난 것으로 확인했는데, 연평균 8,600개나 생긴 셈이다. 그러나 놀라운 점은 그중 92%의 과제가 사라졌다는 것이다. 과제 수명 또한 1.22년밖에 되지 않는다. 이는 블록체인이 관심으로 많은 과제가 생겨나고 있으나, 과제 성공과 사업화로는 이어지기가 힘들음을 보여준다.

가트너는 기술 성장 단계를 표시하는 '하이프 사이클(Hype Cycle)'을 통해서 블록체인이 사업화를 모색

4) Finance Review, "Blockchain Market to grow at 75% CAGR from 2018 to 2024", September 25, 2018.

5) Markets and Markets, "Artificial Intelligence Market worth 190.61 Billion USD by 2025", February, 2018.

6) Markets and Markets, "Hybrid Cloud Market worth \$97.64 billion by 2023", August, 2018.

7) Forbes, "IoT Market Predicted To Double By 2021, Reaching \$520 B", August 16, 2018.

하는 단계에 이르렀음을 제시하고 있다⁸⁾. 이러한 분석은 가트너만이 내놓은 것은 아니다. 맥킨지 (McKinsey) 또한 가트너처럼 블록체인의 사업 성공사례가 없음을 지적했다. 그리고 이를 위한 준비가 필요하다고 주장했다⁹⁾.

그러므로 블록체인 사업화를 위한 시장 진입 전략이 중요하다. 이에 따라, 블록체인 시장 진입에 방해되는 요소를 파악해야 한다. 어떤 요소가 가장 큰 진입 장벽일까? 식품안전정보원은 식품 산업을 대상으로 블록체인의 진입 장벽을 조사했다. 그중 '구축/교체비용'이 식품 산업의 관련 업무에서 제약사항이 높은 편으로 조사됐다¹⁰⁾. 필자가 실제로 블록체인 관련 전문가를 만나거나 사업 기획을 할 때, 기존 시스템 구축의 문제가 종종 언급되곤 했었다.

그러나 다행히, 이러한 장벽의 해결책이 이미 나와 있다. 그건 바로 '서비스형 블록체인 (BaaS)'이다. BaaS는 '블록체인 애플리케이션 (Daap)'을 클라우드 플랫폼에 적용해서 제공하는 서비스이다. BaaS는 시장의 이러한 진입장벽을 낮춰줄 역할을 할 것으로 보이는데, 이에 따라 BaaS가 주목받을 전망이다. 본 글에서는 BaaS를 다루도록 하겠다.

클라우드 중심으로 변하는 ICT 서비스

BaaS를 이해하기 위해서는 클라우드 플랫폼을 우선 살펴볼 필요가 있다. 클라우드는 사용자 단말기 대신에 중앙 서버의 컴퓨팅 파워를 이용해서 서비스를 원격으로 제공하는 플랫폼이다. 플랫폼 사용 유형은 '서비스 사용자'와 '서비스 제공자'로 나눌 수 있다.

클라우드 서비스 유형 비교 (이용자와 제공자)

	서비스 이용자	서비스 제공자
정 의	- 서비스 이용 시에 클라우드를 활용하는 유형	- 서비스 제공 시에 클라우드를 활용하는 유형
제공범위	- SaaS	- IaaS, PaaS, SaaS
이용예시	- 드롭박스, 네이버 클라우드, 슬랙 등	- NBP, AWS, 애저 등

서비스 사용자는 말 그대로 사용자를 뜻하는데, 클라우드를 통해서 서비스를 받을 수 있다. 드롭박스를 예시로 들어보자. 드롭박스에 저장한 문서는 사용자 단말에 저장되지 않는다. 대신, 중앙 서버에 저장이 된다. 그러므로 해당 예시는 클라우드를 이용한 서비스 사용에 해당한다. 그 외 네이버 클라우드, 구글 클라우드, 슬랙 등이 있다. 참고로 클라우드는 서비스 제공 범위에 따라서 3가지로 나눌 수 있다. 서

8) 하이프 사이클은 기술 성숙도에 따라 5단계로 표현한 그래프이다. 기술 축발, 과장된 기대의 정점, 환멸의 저점, 기술 재조명 그리고 생산성 안정을 거친다. 현재 블록체인은 2018년 기준으로 과장된 기대의 정점과 환멸의 저점이 맞대어 있는 곳에 있다.

9) Matt Higginson, and etc., "Blockchain's Occam Problem", McKinsey, January, 2019.

10) 민경세 그리고 신예인, "미래 식품 안정망 강화를 위한 블록체인 활용 연구", 식품안전정보원, 2018년 12월.

비스 이용자는 소프트웨어를 클라우드 형태로 이용하는 경우가 많다. 따라서 서비스 이용자의 경우에는 '서비스형 소프트웨어 (SaaS)'인 경우가 많다.

서비스 제공자는 서비스 제공을 위해서 클라우드를 활용하는 유형을 뜻한다. 이러한 서비스 예시에는 '네이버 비즈니스 플랫폼 (NBP)', '아마존 웹 서비스 (AWS)', '마이크로소프트의 '애저(Azure)' 등이 있다. 이러한 예시의 클라우드 플랫폼은 서비스 제공 지원의 역할을 한다.

아울러, 서비스 제공자는 서비스 이용자 유형과 달리 서비스 이용 수준에 따라 '서비스형 인프라(IaaS)', '서비스형 플랫폼 (PaaS)' 그리고 '서비스형 소프트웨어 (SaaS)'가 있다. SaaS만을 주로 이용하는 서비스 이용자 유형보다 폭넓게 제공한다.

IaaS는 서비스 제공에 필요한 하드웨어 (혹은 서버)를 클라우드에서 제공하는 유형이다. PaaS는 인프라에 더해서 플랫폼까지 제공하는 유형을 뜻하고, SaaS는 플랫폼 위에 소프트웨어까지 덧붙여서 '응용프로그램인터페이스(API)'를 통해서 제공하는 유형을 뜻한다.

이처럼, 클라우드는 서비스 제공 필요도에 따라서 지원을 할 수 있다. 이러한 이유로, 클라우드가 주목받고 있다. 특히 AI가 주목받음에 따라, AI 서비스를 클라우드를 통해서 구현하는 사례가 늘고 있다. 예를 들어, 마이크로소프트는 AI 서비스를 간편하게 이용할 수 있다고 홍보하고 있다. 서비스 제공자는 이미 만들어진 AI를 SaaS 형태로 API를 통해서 제공받기만 하면 되기 때문이다.

이는 BaaS에서도 마찬가지이다. BaaS는 두 가지 클라우드 유형 중에서 서비스 제공자를 위해 만들어진 형태이다. 다시 말해, BaaS도 제공자가 원하는 범위에 따라서 IaaS, PaaS 혹은 SaaS 형태로 지원받을 수 있다. 참고로 AI의 경우에는 AlaaS라고 부른다.

BaaS 제공 개념도



클라우드 플랫폼별 BaaS 서비스 동향

지금까지 내용을 정리하면, BaaS는 서비스 제공자를 위해서 블록체인 플랫폼을 클라우드를 통해서 제공하는 서비스로 정의할 수 있다. 따라서 BaaS는 블록체인 성장과 함께 주목받고 있다. 이유는 두 가지이다. 첫 번째 이유는 앞서 언급한 데로 블록체인의 시장 진입 장벽을 낮추기 위함이다. BaaS 시장 평가에 관해서는 블록체인 종사자 사이에서도 호불호가 나뉘는 것 같다. 그러나 확실한 점은 BaaS가 블록체인의 시장 활성화에 도움을 준다는 점이다. 기존 시스템과의 연동 문제를 하드웨어 인프라 추가 구매 없이, 클라우드로 해결할 수 있기 때문이다. 그뿐만 아니라, 블록체인 구현 난이도가 낮아진다. IBM, KT, 램다256 등은 BaaS를 활용하면 블록체인 활용도가 낮아진다고 홍보하고 있다.

두 번째 이유는 클라우드 플랫폼 제공자가 시장 추세에 맞춘 것으로 볼 수 있다. 클라우드 플랫폼에서는 여러 AI 서비스를 제공하고 있다. AI 서비스의 인기가 높기 때문이다. 블록체인도 마찬가지이다. 클라우드 플랫폼은 자사 플랫폼에 인기 있는 블록체인을 제공하는 것은 당연한 추세이다. 그러므로 여러 클라우드 플랫폼에서 BaaS를 제공하고 있다. 이러한 동향을 한 번 살펴보자.

최초로 BaaS를 선보인 기업은 마이크로소프트이다. 2015년 마이크로소프트는 자체 클라우드 플랫폼 애저를 통해서 BaaS를 선보였다. 코다(Corda), 이더리움, 하이퍼레저 등 여러 블록체인을 클라우드를 통해 제공하고 있다. 3M, 불러 등 글로벌 기업이 마이크로소프트의 BaaS를 이용하고 있다. 그리고 2019년 5월에는 클라우드를 통해 블록체인 서비스 운영까지도 관리하는 '애저(azure) 매니지드 서비스'도 출시했다.

IBM의 푸드 트러스트



(출처: Flickr)

IBM도 BaaS를 제공하고 있다. 마이크로소프트보다 2년 늦은 2017년에 이를 출시했다. 그러나 IBM은 리눅스재단을 통해서 하이퍼레저라는 플랫폼에 많은 기여를 하고 있다. 마이크로소프트와 달리, 하이퍼레저를 통해 블록체인 사업에 진출한 셈이다. 따라서 IBM은 하이퍼레저를 통해서 BaaS 영역에 진출했고, 대부분의 실증 서비스는 BaaS를 통해 이뤄지고 있다. 참고로 IBM은 블록체인 기반 식품 이력 관리 서비스 '푸드 트러스트 (Food Trust)'를 BaaS 형태로 출시한 상태이다. 그 외 아마존은 2018년 4월부터 AWS를 통해 BaaS를 제공하고 있다. 이어 7월 오라클도 BaaS 출시를 발표했다.

중국 기업 또한 BaaS 시장에서 활약이 두드러진다. 화웨이와 알리바바에서 BaaS를 출시했기 때문이다. 화웨이는 2018년 11월 BaaS 출시를 정식으로 선언했다.

국내 기업 또한 2019년부터 BaaS 시장에 본격적으로 진출하고 있다. 2019년 1월 KT는 보도 자료를 통해 자체 클라우드 플랫폼 '유클라우드(uCloud)'를 통해서 자체 블록체인 플랫폼을 3월에 제공하기 시작했다고 밝혔다. 참고로 이를 기가 체인이라고 한다. 현재 KT는 레몬헬스케어와 함께 BaaS를 이용해 스마트 병원 서비스 출시를 계획하고 있다. 그 외, 2019년 3월 램다 256은 신규 블록체인 플랫폼 '루니버스'를 소개했다. 이와 함께 해당 블록체인을 BaaS로 지원한다고 밝혔다. LG CNS는 2019년 올해를 목표로 BaaS 출시를 준비하고 있다.

이처럼 여러 클라우드 기업에서 BaaS를 선보이고 있다. 이에 따라서, BaaS는 블록체인 산업에서 주목을 많이 받을 전망이다. 그뿐만 아니라, 블록체인 산업이 시장으로 진입하는 데에도 기여할 전망이다.

AI 기반 사이버보안 – 이용·인식현황 중심으로



이용용 (david9631@gmail.com)

- (現) ICT&security 애널리스트
- (現) 통신·정보보안 석사과정(University of Victoria)
- (前) KISA 조사분석팀장
- (前) KISA 수석연구원(인터넷/사이버보안정책)
- (前) 데이터 연구원(네트워크/소프트웨어공학)

개요

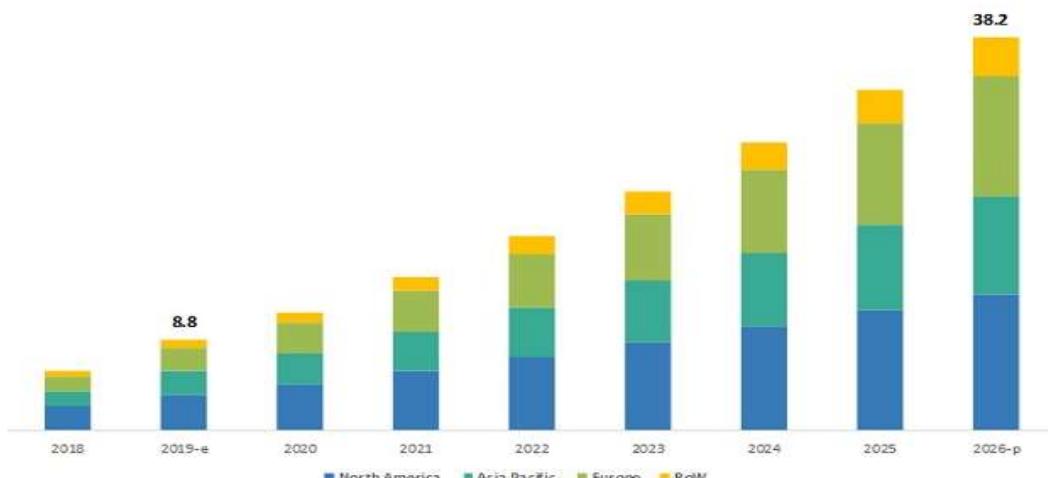
새로운 ICT 환경에서의 사이버위협도 끊임없이 변화하고 지능화하면서, 기업들의 사이버보안에 대한 관심이 증폭되고 있다. 그러나 전 세계적인 사이버보안 인력의 부족 등으로 인해 기업들은 점증하는 사이버위협에 효과적으로 대처하는 데 점점 더 어려움을 겪고 있다. 기업들은 사이버 위기에 직면한 상황에서, 최근 기계학습, 딥러닝 등의 발전으로 AI의 잠재력이 입증되면서 AI가 사이버위협 탐지, 예방, 대응 등 사이버보안 역량을 강화하고 기업이 직면한 인력난을 해결하는데 기여할 것으로 기대하고 있다. 이에 따라 기업의 최고경영층(CEO, CIO, CISO 등)은 AI를 활용한 사이버보안 제품에 대한 관심이 높아지고 있으며, 보안업체들은 AI 기능을 탑재한 사이버보안 솔루션을 연이어 출시하고 있다.

시장조사 기관인 마켓앤드마켓(MarketsandMarkets)의 2025 글로벌 예측보고서에서는 사이버보안에서 AI 시장 규모가 2017년에는 39억 6천만 달러에서 연평균 31.38% 성장하여 2025년까지 348.1억 달러에 이를 것으로 전망했다. 네트워크에 연결된 IoT 기기의 급증, 데이터 급증에 따른 빅데이터와 클라우드 기술의 발전과 함께, 사이버보안 분야도 보안데이터(트래픽, 보안로그)가 증가하면서 AI 기반의 보안에 대한 수요가 증가하고 있다. 또한 전 세계적으로 사이버보안 인력이 부족한 상황에서 AI 기반 솔루션을 사이버보안에 적용하면 사이버보안 전문가의 부족을 상당히 해소할 수 있을 것이라는 예상 등이 AI 기반 보안 시장의 성장을 촉진하고 있다. 기업들은 업무 연속성에 중요한 정보시스템을 보호하기 위해 사

이번보안 예산을 확대하고, 기업전략을 사이버보안과 연계하며 직원과 고객을 위한 사이버보안 교육을 강화하고 있다.

2025년까지 사이버보안에서 AI 시장은 하드웨어보다는 소프트웨어 분야의 성장률이 높을 것으로 예상된다. AI 시스템은 사이버보안을 위해 기계학습 알고리즘과 함께 언어처리, 시각인식, 음성인식 등 다양한 유형의 소프트웨어를 필요로 한다. 영국의 Darktrace, 미국의 Cylance, Securonix, IBM, Palo Alto Networks, Symantec 등이 기업들이 사이버보안에서 AI를 접목한 소프트웨어 제품을 연이어 출시하며 시장을 주도하고 있다. 특히 북미지역이 향후 몇 년간 AI 기반의 사이버보안 시장을 주도할 것으로 전망된다. 북미 지역은 정부 기관, 금융기관, 주요 기반시설 등에서 사이버위협이 급증하는 문제에 직면하면서 혁신적 보안기술에 대한 도입이 활발하다. 주요 AI 업체와 사이버보안업체들이 북미지역에 기반을 두고 있어 북미지역 기업들이 향후 수년간 사이버보안에서 AI 시장의 성장에 크게 기여할 것으로 전망된다.

지역별 사이버보안에서 AI 시장 규모(단위: 10억 달러)



[출처: Market and Market] ※ RoW: Rest of the world)

전 세계적으로 사이버보안 분야에서도 AI 시장이 급성장하고, 기업들이 AI 제품 도입이 확대될 것으로 예상됨에 따라, 본고에서는 사이버보안 분야에서의 AI 도입, 이용, 인식현황, AI 도입에 따른 이점과 장애 요인 등을 최근의 다양한 기관에서 발표한 연구조사 결과를 기반으로 살펴보고자 한다.

2019 경영층의 최상의 아젠더 – AI & 사이버보안

가트너는 2018년 10월 가트너 IT 심포지엄/XPO 2018에서 89개 국가의 3,102명의 최고정보책임자 (CIO; 정부 부문 CIO 528명 포함) 대상으로 설문 조사하여 2019년 CIO의 핵심 아젠더를 발표하였다. 가

트너는 조사 결과를 토대로 AI와 사이버보안이 2019년 CIO의 핵심적인 아젠더를 형성한다고 발표했다. 파괴적인(disruptive) 신흥기술들은 모든 조직의 경제를 변화시킬 때 비즈니스 모델을 재구성하는 데 중요한 역할을 한다. 가트너는 CIO와 IT 경영자에게 어떤 기술을 가장 파괴적일 것으로 기대하는지 질의했고, 이에 대해 CIO와 IT 경영자들은 언급된 기술 중 AI 기술이 가장 주목한다고 응답하였다. CIO 및 IT 경영자 중 37%는 디지털 기술 및 추세에 따라 조직에서 이미 AI 기술을 도입했거나 조만간 도입할 계획이라고 응답했다.

가트너의 설문조사 결과, 성숙도 측면에서 정부 부문은 디지털 서비스 설계와 공급에서 점진적으로 발전하여 민간 부분에 필적할 정도의 성숙도에 도달하고 있는 것으로 평가되었다. 투자 분야에서는 타 산업부문 CIO의 34%가 투자를 증가시킬 계획이지만, 정부부문 CIO 중 17%가 디지털 비즈니스에 대한 투자를 증액할 계획이 있는 것으로 나타났다. 정부 부문은 파괴적인 기술로 AI(27%)를 가장 많이 꼽았으며, 다음으로 데이터분석(22%)과 클라우드 기술(19%) 등의 순이었다. 정부 부문 CIO 중 10%는 이미 AI 솔루션을 배포했고, 39%는 향후 1-2년 내에 배포할 계획이 있었으며, 36%는 향후 2~3년 내 AI 솔루션을 배포할 계획이라고 응답했다. 정부 부문 CIO들은 BI(Business Intelligence)/데이터분석, 사이버/정보보안(43%), 클라우드서비스/솔루션(39%)이 2019년의 기술투자에서 집중한다고 응답했다. 정부 부문의 CIO들이 사이버보안에 중점을 두는 것은 조직과 고객을 보호하기 위해 안전한 디지털 비즈니스 기반 구축이 절실함을 반영하는 것으로 판단된다.

파괴적인 기술과 투자 중점 분야

2019 파괴적인 기술			2019 집중 투자 분야		
순위	정부 우선순위	응답자 비율 (%)	순위	정부 우선순위	응답자 비율 (%)
1	AI/기계학습	27	1	BI(Business Intelligence)/데이터 분석	43
2	데이터 분석	22	2	사이버/정보보안	43
3	클라우드	19	3	클라우드 서비스/솔루션	39
4	사물인터넷	7	4	코어 시스템 개선/트랜스포메인션	33
5	모바일(5G 포함)	6	5	소프트웨어 개발/업데이트	26
6	BI(Business Intelligence)	6	6	인프라/데이터센터	23
7	디지털 트랜스포메이션	6	7	AI/기계학습	22
8	블록체인	5	8	기술통합	21
9	자동화	3	9	고객/사용자 경험	20
10	고객관계관리	2	10	모바일 애플리케이션	19

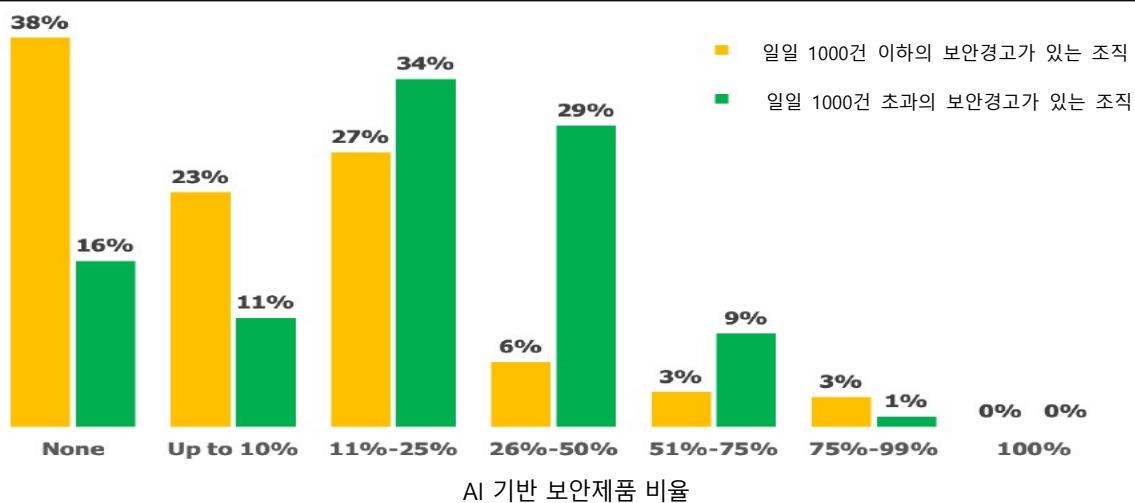
(출처: Gartner, dynamiccio.com 재인용)

설문조사에서는 또한 대부분의 기업에서 CIO가 여전히 사이버보안에 대한 책임을 담당하는 비율이 가장 높은 것으로 나타났다. 그러나 최신 기업환경에서 IT 조직만으로는 더 이상 사이버보안을 완전하게 제공하기 어려울 수 있으며, 피싱과 같은 사회공학적 공격의 범람은 조직 내 모든 직원의 광범위한 행동변화와 참여를 필요로 한다.

사이버보안에서 AI의 가치 분석

Osterman Research는 2018년 12월 발표한 '사이버보안에서의 AI – 이점, 한계, 진화하는 문제점' 연구 보고서에서 기업 전반의 AI 이용에 대한 현황과 한계점을 제시했으며, 특히 기업이 일상적으로 경험하는 보안경고의 규모에 따른 AI 도입 현황과 이점 등을 제시했다. Osterman은 직원 수 1,000명 이상의 400개 조직을 대상으로 조사했으며, 조사 결과에 따르면 기업 중 73%는 일정 수준 이상의 AI 기반의 보안 제품을 도입한 것으로 나타났다. 특히 하루에 1,000건 이상의 보안 경고를 접수하는 기업의 경우에는 상대적으로 AI 지원 보안제품을 이용하는 비율이 84%로 증가하는 것으로 나타나는데, 이는 의사 결정자들이 AI를 보안경고의 흥수를 해결하는데 유용한 도구로 간주하고 있음을 보여준다.

일일 보안경고 규모에 따른 AI 지원 보안제품 비율별 이용률



(출처: Osterman Research)

AI 제품 구매 의향 관련, 현재 AI를 이용하고 있는 기업들이 AI 이용에 따른 다양한 이점으로 인해 새로운 AI 지원 제품을 구매할 의향이 높은 것으로 나타났다. 설문조사에서 보안제품을 구매하는 의사결정 과정에서, AI 지원 보안제품 적용 비율이 10% 이하인 조직 중 11%만이 의사결정 과정에서 AI가 상당히 중요하거나 매우 중요한 역할을 있다고 응답했다. 반면 AI 지원 보안제품 적용 비율이 10%를 초과하는 기업 중 구매 결정에서 AI가 상당히 중요하거나 매우 중요한 역할을 있다고 응답한 비율은 40%에 이르

는 것으로 나타났다. AI 지원 보안제품 도입에 따른 긍정적인 측면 관련, 전체 조직 중 60%는 AI가 보다 신속하게 경고를 조사하도록 지원하고, 동일한 비율로 AI가 보안 직원의 효율성을 개선한다고 응답했다. 또한 조직 중 약 절반가량은 AI가 자동화된 초기 검사에 유리하고, 위협 식별을 최적화하는 이점이 있다고 응답했다.

클라우드 서비스 유형 비교 (이용자와 제공자)

이점	전체 조직	AI 적용비율 10% 이하인 조직	AI 적용비율 10% 초과인 조직
보안 경고에 대한 신속한 조사	60%	49%	69%
AI가 보안직원의 효율성 개선	60%	46%	70%
자동화된 초기 검사	49%	41%	54%
위협 식별 최적화	47%	41%	51%
위협 완화 가속화	44%	33%	53%
긍정오류(False Positives) 감소	38%	28%	47%
자동화된 치료 및 격리	23%	17%	28%

(출처: Osterman Research)

한편, AI 지원 보안제품 도입 관련 문제점 관련 조사대상 기업 중 46%는 규칙 개발과 구현이 부담스럽다고 표시했으며, 25%는 향후 AI 지원 보안솔루션을 추가로 구현할 계획이 없다고 응답했다. 이러한 조사 결과는 사이버보안에서 AI의 실제적인 활용이 실제로 초기 단계에서 머무르고 있어, 그 잠재력을 충분히 활용하지 못하고 있음을 시사한다. 보안기술 솔루션들은 AI 기술의 적용에 따른 장점을 많이 마케팅하고 있으나, 현재 AI가 보안에 어떤 긍정적인 효과를 낼 것인지에 대한 입증은 충분하지 않은 상황이다. Osterman Research의 연구에서 조사 응답자들은 보안팀이 직면한 제로데이(Zero-day), 고수준 위협 등 다양한 위협을 완화하는데 AI 기술이 아직은 크게 도움이 되지 않는다고 지적했다. 그러나 향후에는 사이버보안 분야에서 AI 활용 방법이 개선되면서 점진적으로 기업의 이익을 실현하고 사이버보안을 향상하는데 AI의 기여도가 전반적으로 개선될 것으로 예상된다. AI 기술을 사이버보안에 적용하면서 새로운 공격 유형을 빠르게 분류하고, 학습하여 대처할 수 있도록 지원할 것으로 예상된다.

클라우드 서비스 유형 비교 (이용자와 제공자)

문제점	전체 조직	AI 적용비율 10% 이하인 조직	AI 적용비율 10% 초과인 조직
정확한 경고를 제공하는 도구 구입의 어려움	50	28	67
규칙 생성과 구현의 어려움	46	27	61
조직의 네트워크에 맞추어 과도한 조정 필요	39	23	51
부정확한 결과 생성	36	30	41
고가의 제품	35	32	37
사용 편리성 부족	21	16	25

(출처: Osterman Research)

시장조사기관인 포네몬(Ponemon)은 2018년 7월 미국의 IT 및 보안 실무자 600여명을 대상을 설문 조사하여 발표한 '사이버보안에서 AI 가치(The Value of Artificial Intelligence in Cybersecurity)' 연구보고서에서 AI가 사이버보안에서 위협 분석 속도의 향상, 침해 확산 방지, 애플리케이션 취약점 식별 등의 이점을 제공한다고 설명했다. 포네몬은 AI를 사용하지 않는 기업이 연간 약 330만 달러 이상을 사이버침해를 해결하는데 평균적으로 지출하고 있으나, AI 기술을 보유한 기업들은 동일한 위협에 대처하는데 연간 평균 80만 달러를 지출하여 연간 2백만 달러 이상을 절감한다고 발표했다.

사이버침해 해결에 AI 이용에 따른 비용 절감

구분	AI 미적용	AI 적용	시간과 비용 차이
사이버방어에 대한 조직 및 계획	25.32	16.05	9.27
사이버침해와 말웨어 감염에 대한 실행가능한 정보 포착	80.20	41.11	39.09
애플리케이션 취약성 조사 및 탐지	195.88	70.48	125.40
사이버침해나 말웨어에 대한 실행가능한 정보 조사	66.28	24.23	42.05
사이버침해나 말웨어로 인한 손상이나 침해를 입은 네트워크, 애플리케이션, 디바이스 치료	212.89	39.63	173.26
정책이나 의무사항 등 준수하여 사이버사고에 따른 보고서 작성 및 보고	25.07	15.91	9.16
오류, 긍정오류를 추적하는데 보안인력이 소모하는 시간	400.83	41.42	359.41
말웨어에 감염된 네트워크, 애플리케이션, 디바이스를 치료에 따른 계획에 없던 시스템 중단	3.95	1.90	2.05
주별 전체 시간	1,010.42	250.73	759.69
연간 전체 시간	52,541.84	13,037.96	39,503.88
연간 전체 비용 추정치	\$3,283,865.00*	\$814,872.50*	\$2,468,992.50*

* \$62.50/시간 (출처: Ponemon Institute)

사이버침해가 증가하면서 기업들이 침해 징후를 감지해 자동으로 정보를 제공하여 관련하여 많은 양의 경고가 지속적으로 발생하는 상황이다. 따라서 보안팀이 AI를 활용하게 되면 업무효율성을 개선할 수 있다. 기업관리협회(Enterprise Management Associates, EMA)에 따르면 과도하게 많은 경고로 인해 적어도 64%의 경고를 조사하지 못하고 있는 실정이다. 그러나 AI를 사용하면 AI는 정보를 분석하고, 의미 있는 정보를 추출하고, 경고를 결정하고 우선순위 설정 등 보안 분석가의 업무 중 일부를 대신함으로써 보안직원들이 다른 중요한 작업에 집중할 수 있도록 할 수 있다. AI는 보안전문가가 반복적인 작업을 최

소화하고, 분석 스킬을 향상하고 새로운 도구, 기술을 사용하는 방법을 배우는 기회와 시간을 제공함으로써 사이버보안 관련 작업의 생산성을 대폭 개선할 수 있을 것이다. 아직 사이버보안에서 AI 활용이 초기 단계에 있기 때문에 AI 잠재력 활용의 효과를 완전히 실현되지 못하고 있으나, 기업이 사이버보안에서 AI 기술 투자를 지속하고, AI 기술이 발전함에 따라 사이버보안에서 AI 기술의 비중이 증가하고 기술력이 향상되면서 그 영향력도 높아질 것으로 예상된다.

산업별 AI 지원 보안제품 활용

2019년 3월, SANS 연구소는 사이버보안을 위한 AI의 기본적인 기능에 대한 인식, 보안을 위해 AI 구현 여부, 구현 시기와 방법 등에 대해 사이버보안 커뮤니티를 대상으로 조사했다. SANS는 기술(17%), 사이버보안 서비스 공급자(14%), 금융(11%), 교육(8%), 정부(7%) 부문의 전문가들을 대상으로 설문 조사했으며, 주요 결과는 다음과 같다.

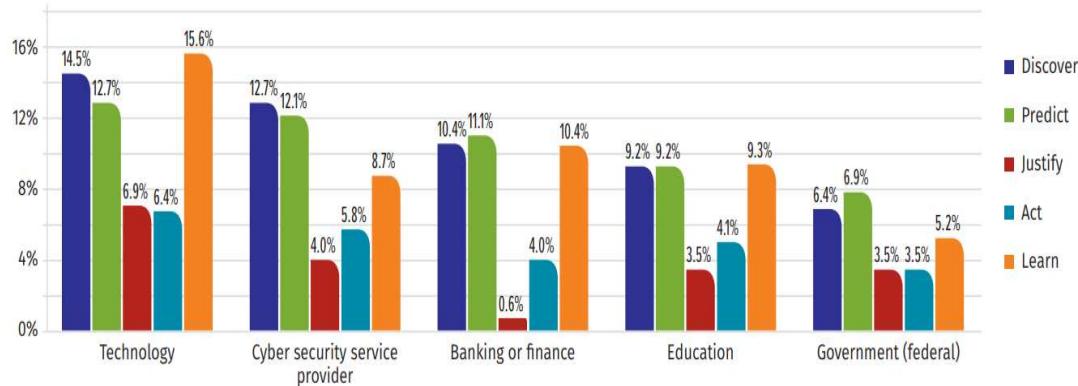
1) AI 지원 보안의 기본적인 기능

SANS는 AI 보안 솔루션의 기본적인 기능을 아래의 5개 영역(발견, 예측, 설명, 행동, 학습)으로 구분하고, 이중에서 어떤 기능이 AI 보안솔루션의 갖추어야 할 기본적인 기능인지에 대해 조사하였다.

- 발견(Discover) – 사람의 개입 없이 데이터에서 학습
- 예측(Predict) – 지적 발견을 통한 데이터의 이해를 기반으로 미래에 발생할 일에 대한 대안을 제시
- 설명(Justify) – 결과를 인식할 수 있고 믿을 수 있도록 행동을 설명(투명성은 이용자가 어떤 알고리즘과 매개변수를 사용할 것인지를 알리는 측면이 반면, 설명은 행동에 대한 적정한 이유를 제시)
- 행동(Act) – 업무절차에서 지능형 애플리케이션에 대한 사용자 경험을 제공
- 학습(Learn) – 데이터가 진화하면서 감지하고 대응

조사응답자들은 AI 보안솔루션의 기본적인 기능으로 학습(81.3%), 발견(80.2%), 예측(79.1%)을 주로 꼽았고, 다음으로 행동(39%), 설명(20%)을 중요하다고 응답했다. 아래의 도표와 같이 산업 부문별로 AI 솔루션의 기본적인 기능을 다소 다르게 인식하는 것으로 나타났다. 기술 부문은 다른 산업을 지원하는 데 필요한 제품 개선에 중점을 두어 학습을 중요하게 인식하는 반면, 금융 부문은 발견 및 예측을 중요하게 인식했다. 이는 금융 부문이 금융사기에 대한 발견과 신속한 대응력이 필요한 것에 기인한 것으로 판단된다.

산업별 AI 지원 솔루션의 기본적인 기능으로 고려하는 사항

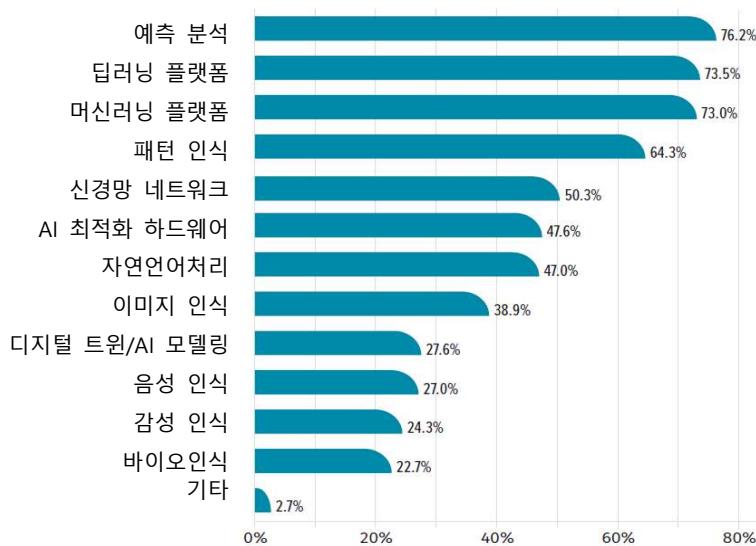


(출처: sans.org)

2) AI 지원 보안을 위한 주요 기술

많은 응답자가 인식하는 AI 지원 보안을 위한 최상위 기술로는 예측분석(76.2%), 딥러닝(73.5%), 머신러닝(73%)인 것으로 나타났다. 다음으로는 패턴인식(64.3%), 신경망 네트워크(50.3%)의 순이었다. 이에 비해 자연어처리(47%), 이미지 처리(38.9%), 음성 인식(27%) 등과 같은 통계적 처리기술은 AI 지원 기술로 고려하는 비율이 상대적으로 낮은 것으로 나타났다. 응답자들은 AI에 대해 신경망 학습, 예측분석과 같은 심층학습 기술을 포함하는 것으로 인식하는 경향이 높았다. 이러한 기술들은 문제 해결을 위해 대규모 데이터를 수집, 분석하고 문제를 분석하여 예측정보를 제공할 수 있다.

AI 지원 보안을 위해 고려하는 기술

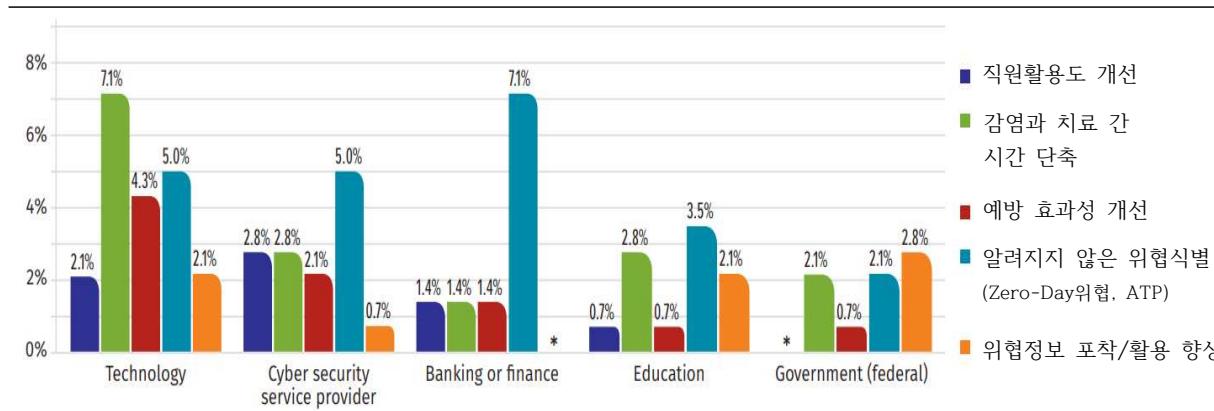


(출처: sans.org)

3) 사이버보안에 AI 활용에 따른 이점

보안전문가의 입장에서 응답자의 57%는 AI를 사용하는 보안솔루션을 사용하거나 사용하려고 계획하고 있지만 35%만이 이러한 플랫폼에 대한 직접적인 경험이 있는 것으로 나타났다. 사이버보안에서 AI 활용영역은 조직에 따라 다양하게 나타났으며, 이중 최상위 3개 분야는 사이버 방어(75.2%), 말웨어 예방(75.5%), 지능형 위협탐지와 예방(68.6%)인 것으로 나타났다. 전체 응답자의 85%는 AI를 향상된 보안을 위한 원동력으로 인식했으며, 대다수(67%)는 기존의 사이버보안 도구를 대체하기보다는 보완한다고 인식했다. AI 지원 사이버보안 솔루션에 대한 견해는 산업부문에 따라 다르게 나타났다. 기술 부분은 감염 후 치료에 걸리는 시간 감축에 중점을 두는 반면, 금융 분야는 알려지지 않은 위협을 식별하는 것에 집중하고 있는 것으로 나타났다. 이러한 조사 결과는 조직이 보안 태세를 향상하는데 있어 AI를 활용하는 최상의 방법은 필연적으로 해당 조직의 임무와 기존의 기능에 크게 좌우될 것임을 시사한다.

산업별 사이버보안을 개선하는데 AI 활용에 따른 이점

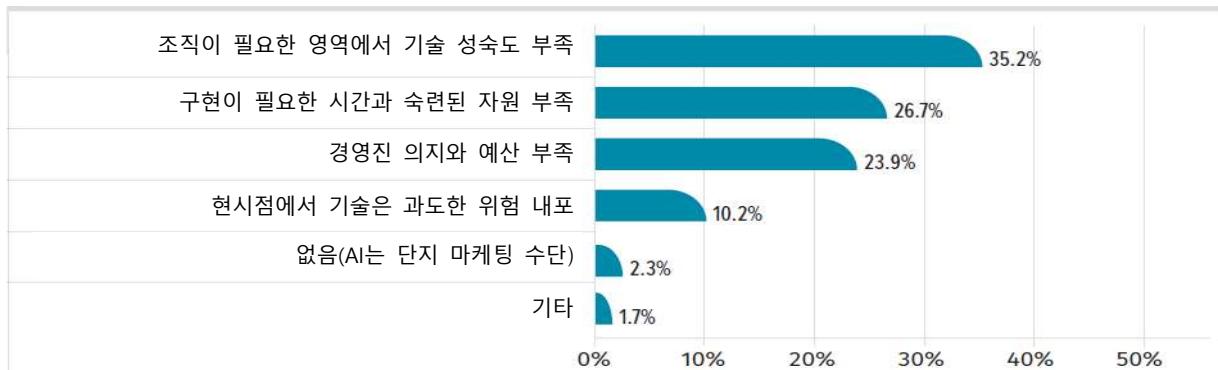


(출처: sans.org)

4) 사이버보안의 AI 도입 관련 장애 요인

AI는 사이버보안 전문가가 최신 위협에 보다 정교하고 신속하게 대응하도록 지원하지만, AI 기술을 사이버보안에 도입하는데 여러 장애 요인이 발생하는 것으로 조사되었다. 사이버보안 전문가 중 35%는 구현에서 직면한 최우선 장벽으로 AI의 성숙도 부족을 언급했다. 또한 사이버보안 전문가 중 46%는 AI의 기술이 여전히 성숙하지 못했다고 인식했으며, 단지 5%만이 고도로 성숙했다고 인식하는 것으로 나타났다. 설문응답자 중 기술 실무 직원은 경영진보다 AI 솔루션의 성숙도에 보다 높은 신뢰도를 나타냈으며, 이러한 요인들은 AI 구현을 모색하고 있는 사이버보안 전문가들에게 중요한 역할을 할 것으로 기대된다. 응답자 중 27%는 AI 구현에 필요한 시간과 숙련 자원이 부족하다고 응답했고, 24%는 경영진의 의지와 예산 부족을 지적했다. 응답자 중 10%는 AI가 현시점에서는 사이버보안에 너무 많은 위험을 초래할 수 있다고 지적했다.

사이버보안 애플리케이션에 AI 도입 관련 장애요인



(출처: sans.org)

응답자의 피드백을 기반으로 연구보고서는 AI를 사이버보안에 활용하는 것과 관련해서 잠재적 위험으로 1) 소비할 데이터의 규모와 유형으로 인한 개인정보 침해 2) 단일 마스터 AI 알고리즘에 대한 과도한 의존, 3) 알고리즘의 한계에 대한 이해 부족, 4) 데이터 및 메타 데이터 보호가 충분하지 않음, 5) 부적절한 교육 훈련, 6) AI를 통한 의사 결정에서 가시성 부족, 7) 특정 문제에 대한 잘못된 알고리즘 사용 등을 제시하였다.

시사점

사이버보안에서 AI를 활용하면 새로운 사이버위협에 대해 기존의 방식보다 훨씬 신속하고 효과적으로 위협을 예측하고 대응할 수 있을 것으로 기대를 모으고 있다. 전 세계 주요 IT 및 보안 전문기업들은 AI를 사이버보안에 적용한 솔루션 개발에 박차를 가하고 있으며, 정부 기관과 기업의 경영층들은 올해의 핵심적인 경영 의제로 AI와 사이버보안에 집중하여 투자를 확대하고 있다. 이러한 상황을 고려할 때 향후 수년간 정부 기관 및 민간 기업은 점증하는 사이버위협은 증가하나 사이버보안 전문 인력이 부족한 상황에서 사이버보안을 강화하는데 AI 적용을 확대할 것으로 전망된다.

현시점에서는 보안경고 등 침해위협이 높은 기업을 중심으로 AI 기반의 사이버보안 제품을 도입이 활발하다. 이들 기업은 AI 지원 보안제품 도입에 따라 보안 위협에 대한 신속한 대처, 보안직원의 효율성 향상 등을 경험하면서, 새로운 보안제품을 도입하는 구매 결정에서 AI 지원 여부가 중요한 요소로 인식했다. 이에 따라 기업들의 AI 기술 적용에 대한 요구가 증가할 전망이며, 기업의 요구를 반영하여 사이버보안 업체들은 딥러닝, 신경망 네트워크 등 다양한 AI 관련 기술을 적용한 보안제품 개발과 출시가 증가할 전망이다.

산업부문별로는 조직의 임무와 기능에 따라 사이버보안에서 AI를 활용하는 목적과 방법, 도입하는 기

술에서 차이를 발생했다. 기술기업의 경우에는 침해해결 시간 단축, 금융기업의 경우에는 알려지지 않은 위협 식별, 정부 분야의 경우에는 위협정보 포착과 활용에 중점을 두는 것으로 나타났다. 이처럼 다양한 고객의 요구에 부합하기 위해 AI 기반 사이버보안 제품이 다양화될 전망이다.

아울러 아직은 AI 지원 보안제품 도입 관련, AI 기술의 성숙도 부족, 숙련 인력 부족 등의 다양한 문제점이나 장애 요소들을 여전하므로, 정부, 기업, 대학 등은 협력하여 사이버보안에 적용되는 AI 기술개발, 전문인력 양성 등 AI 기반 사이버보안 역량 강화를 위해 적극적 참여가 노력이 요구된다.

[참고문헌]

- SANS, Security Gets Smart with AI, 2019.05. 20;
<https://www.sans.org/reading-room/whitepapers/analyst/security-smart-ai-38867>
- Techrepublic, Top 5 barriers to AI security adoption, 2019. 3. 26
<https://www.techrepublic.com/article/top-5-barriers-to-ai-security-adoption/>
- Market and Market, Artificial Intelligence in Cybersecurity Market by Offering (Hardware, Software, and Service), Deployment Type, Security Type, Technology (ML, NLP, and Context-Aware), Application (IAM, DLP, and UTM), End User, and Geography- Global Forecast to 2026,
<https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html>
- Gartner Survey of More Than 3,000 CIOs Reveals That Enterprises Are Entering the Third Era of IT
<https://www.gartner.com/en/newsroom/press-releases/2018-10-16-gartner-survey-of-more-than-3000-cios-reveals-that-enterprises-are-entering-the-third-era-of-it>
- 2019 CIO Agenda: Secure the Foundation for Digital Business
<https://enterprisecloud/ngw/globalassets/en/information-technology/documents/trends/gartner-2019cio-agenda-key-takeaways.pdf>
- Data Analytics and Cybersecurity Top Tech Investments of Government CIOs in 2019: Says Gartner
<https://www.dynamiccio.com/data-analytics-and-cybersecurity-top-tech-investments-of-government-cios-in-2019-says-gartner/>
- Security Intelligence, Are Applications of AI in Cybersecurity Delivering What They Promised?, 2019. 2. 12
<https://securityintelligence.com/are-applications-of-ai-in-cybersecurity-delivering-what-they-promised/>
- Osterman Research, The State of AI in Cybersecurity, 2018. 12
<https://info.protectwise.com/osterman-state-of-ai-in-security>
- Ponemon Institute, The Value of Artificial Intelligence in Cybersecurity, 2018.
<https://www.ibm.com/downloads/cas/EX0P6YPO>

스마트공장 보안



김계근 (toproach@gmail.com)

- (現) 제어시스템보안연구회 산업분과위원
- (前) 롯데정보통신 통합보안센터 보안정책팀장
- (前) 이니텍/시큐어소프트 모의해킹팀장
- (前) 고등기술연구원 방산기술연구센터 연구원

들어가면서

“스마트공장” 수년 전까지만 해도 없던 용어지만 최근 4차 산업혁명, 5G와 함께 언론에서 쉽게 노출되는 단어이다. 쉽게 말하면 공장이 똑똑해졌다는 의미이다. 이는 ICT 기술과 전통 제조업이 결합하면서 산업간 융합을 통해 제조 공장에서 혁신이 일어났음을 의미한다. 이러한 스마트공장으로의 변화를 이끈 것은 단연 ICT 기술이며 우리는 스마트공장에 대해서 대부분 잘 알고 있다고 생각한다. 실제로 그럴까? 어떤 이는 공장 자동화를 다른 이는 공장의 빅데이터 분석을 통한 공정 개선을 스마트공장이라고 여기는 경우가 많다. 따라서 본 기고에서는 스마트공장에 대해 먼저 알아보고 이후 제조업에서 발생한 보안 사고 사례를 살펴보면서 스마트공장의 보안 사고를 대비한 동향정보와 대응 방안에 대해서 알아보고자 한다.

스마트공장 개념

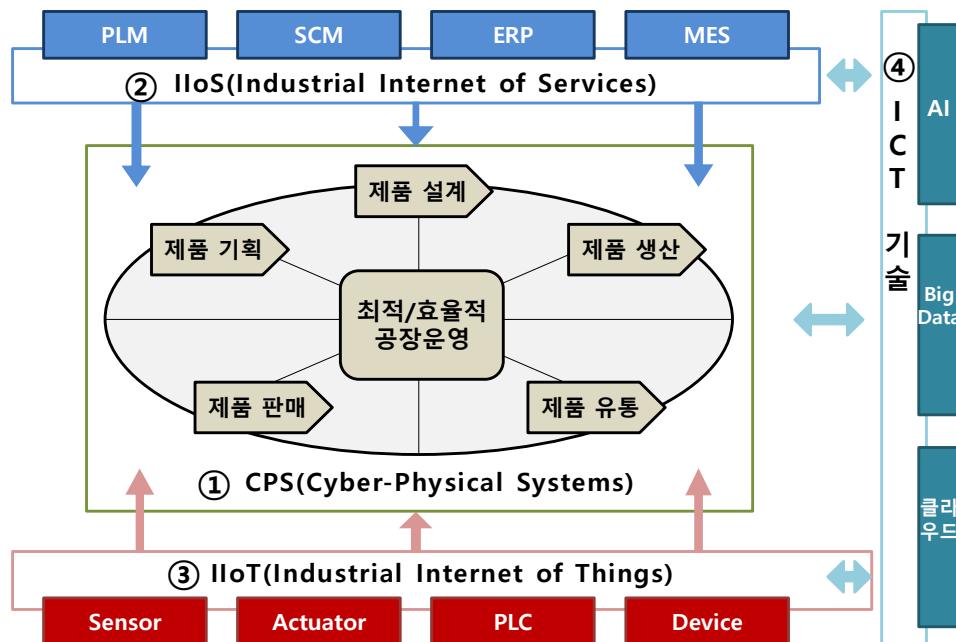
스마트공장 개념에 대해서 기술표준원의 KS X 9001-1 (스마트공장 – 제1부: 기본 개념과 구조) 표준에서는 다음과 같이 정의하고 있다.

전통 제조산업에 ICT를 결합하여 제품의 기획, 설계, 생산, 유통, 판매 등 전 과정을 ICT 기술로 통합함으로써, 최소 비용과 시간으로 고객맞춤형 제품 생산을 지향하는 공장

※ KS X 9001 9001(스마트공장) 표준

주목해야 할 것은 ICT 기술이 제품 제조 전 과정에 통합되었고 이를 통해 고객 맞춤형 제품 생산을 한다는 점이다. 그렇다면 어떤 형태로 ICT 기술이 통합되었기에 스마트공장이라고 이름을 짓는 것일까? 다음 그림은 스마트공장의 개념을 도식화한 것으로 IT, OT, IoT 등의 기술이 통합된 형태를 가지고 있다.

스마트공장 개념



위 그림에서 스마트공장은 ① CPS 영역 ② IIoS 영역 ③ IIoT 영역 ④ ICT 기술 영역으로 표현할 수 있으며, 각 영역의 기능을 살펴보고 적용 기술을 아래 표와 같이 나누어 볼 수 있다.

스마트공장 기술 구성요소

구분	적용 기술
CPS	제품 기획, 양산 기술
IIoS	IT 정보화 기술
IIoT	IoT 기술 (센싱, 통신)
ICT 기술	빅데이터, AI, 클라우드

그림에서 ①번 영역은 제조 프로세스로 공장 자동화를 포함하는 영역이다. CPS로 표현된 것은 해당 부분의 물리적 제품의 기획과 생산과정에서 가상공간에서의 모델링, 시뮬레이션을 통하고 실제 시제품 혹은 양산품을 생산할 때 컴퓨터를 통해 입력된 3D 설계 파일을 3D 프린터가 제품으로 만들어내는 과정을 포함한다. 이렇게 만들어진 제품은 유통과정을 통해 최종 소비자에게 판매되는 것을 표현한 것이다. 일반적으로 FA (공장 자동화)는 제품의 생산과정에서 효율을 높이고 자동화하는 데 중점을 두고 있다.

②번은 IIoS (Industrial Internet of Service) 영역으로 일반적인 IT 영역으로만 볼 수 있지만, 그 의미는 크게 다르다고 생각 한다 . 그림에서 보면 ①②③ 번의 모든 데이터가 ④번 영역을 통해 공유되고 이를 다시 ②번 영역인 IIoS 가 받아서 제조 공정에 영향을 미치는 것을 볼 수 있다. 즉 IIoS 영역은 제조 공정의 모든 영역에서 오는 데이터를 ICT 기술을 이용하여 분석하고 이를 바탕으로 제조 과정에 실시간으로 개입하게 된다. 즉, 공정의 전체 효율을 최적화시킬 수 있다는 점이다. 그뿐만 아니라 해당 영역은 단일 공장에서의 제조 효율 개선이 아니라 유관한 타 제조공장 (혹은 기업)과 연계되어 단일 기업을 넘어서 다수 기업을 연계하는 하나의 거대한 제조시스템을 만들 수 있는 기반이 되는 점점 역할을 수행할 수 있는 중요한 부분이다.

③번은 IIoT (Industrial Internet of Things) 영역으로 제조현장 내부에 위치한 수많은 센서, 밸브, 액츄에이터 등 다양한 기기(Devices)류로 이루어져 있으며 다양한 시리얼 통신(DNP-3, Modbus 등) 및 무선 통신(Zigbee, z-wave, RFID 등)으로 상호 연결되어 있으며 제품 생산과정에서 발생하는 다양한 데이터 (생산장비의 데이터 및 공장 설비환경을 담당하는 Utility로부터의 데이터)를 수집하고 이를 상위 시스템으로 전달하는 역할을 한다.

④번은 ICT 기술이 접목된 것으로 ③번에서 수집된 모든 데이터를 취합하는 빅데이터 수집과 AI의 다양한 기법을 이용하여 제품 생산과정의 품질 검사 및 공정 개선, 효율 최적화 등을 수행하는 역할을 하는 최신 ICT 기술이 접목되고 있는 부분이기도 하다. 일반적으로 IT 회사에서는 ④번 영역과 ②번 영역을 주 영역으로 사업을 진행하고 있다.

결론적으로, 스마트공장은 ICT 기술, OT/ICS¹⁾ 기술, IoT 기술이 모두 접목되어 운영되는 제조산업과 IT

1) OT : Operation Technology, 운영기술로 24x365 지속적으로 멈추지 않고 운영이 되어야 하는 영역의 운영기술로 주로 사회기반시설(교통, 정수, 발전 등)이 이 부분에 포함된다.

ICS : Industrial Control System, 산업제어시스템을 의미하며 OT 영역에 포함된다.

산업이 융합된 형태의 제조업으로 4차 산업혁명의 특징인 초 연결성(Super connectivity)과 Big Data/AI 기술이 융합된 형태라고 볼 수 있다.

제조업에서의 (보안) 사고

앞에서 설명한 바와 같이 스마트공장은 모든 영역이 상호 연결되는 초 연결성을 가지고 있다. 이는 외부에서 접근이 가능한 경로를 물리적으로 생성해 놓고 있다는 의미가 되는데 이러한 제조공장에서 보안 사고는 없었을까? 실제 공장이 아닌 산업체어시설 전반을 보게 된다면 실제 사고 사례는 미국 기준으로 2016년 290건이 넘으며, 이 중 제조업에서 발생한 사고는 63건으로 전체의 21.7%를 차지한다. (출처 : ICS-CERT) 국내의 경우는 사고 통계 및 조사가 발표된 적이 없다.

실제 제조업에서 발생한 보안사고 중 주요 보안 사고는 다음과 같다.

제조업 주요 보안사고 사례 (최근 5년)

발생 연도	발생 국가	제조업 유형	공격 대상	공격 방식	결과
2018	대만	반도체	생산정보 PC	랜섬웨어 (워너크라이)	웨이퍼 생산 차질
2017	사우디	화학공장	비상안전장치	트리톤 (악성코드)	가스 유출 시도 차단
2017	다수 국가	석유, 철강, 선박, 자동차 등	윈도우 OS (PC, 서버 등)	랜섬웨어	주요 정보의 암호화로 사용 불능
2017	일본	반도체	생산정보 PC/서버	랜섬웨어 (워너크라이)	반도체 생산 차질(웨이퍼 폐기) 매출 2% 손실
2014	독일	철강	용광로 제어시스템	해킹 (OA → FA)	제어시스템 기능 차단 용광로 제어권 상실

사고 사례를 통해 보면 주로 랜섬웨어 및 악성코드에 의한 감염이 많은 것을 볼 수 있으며, 감염이 생산에 차질을 주었다는 것은 앞에서 설명한 스마트공장의 초 연결성으로 인한 결과로 볼 수 있다. (제조업에서 생산영역(FA 영역)이 네트워크와 연결되는 것은 스마트공장 이전부터 진행되어 오던 것이므로 위 사례가 꼭 스마트공장에서만 일어날 수 있는 것은 아니다.)

또한, 공격 방식이 트리톤 악성코드와 해킹인 두 건의 경우에는 공격대상을 정하고 해당 공장의 시스템에 대한 이해를 바탕으로 타겟팅 공격을 한 결과이다. 실제로 OT 영역에 대한 보안 침해의 경우 그 비중이 제조업으로 많이 움직이고 있음을 최근의 사고 사례에서 알 수 있다.

보안사고 증가율

구분	2010년	2016년	증가율
OT 보안 사고건수	41 건	290 건	607%
제조업 보안사고 건수	2 건	63 건	3,050%

(출처 : ICS CERT, 미국 기준)

이러한 제조업의 보안 침해 사고의 증가율과 4차 산업혁명에 의한 스마트공장으로의 전환은 제조업 전반에 걸쳐서 다양한 침해사고를 유발할 수 있을 것으로 보인다. 하지만 스마트공장의 보안 침해를 OT/ICS 영역에서만 발생하는 것으로 생각해서는 안 된다. 앞에서도 이야기했지만, 스마트공장은 산업간 융합의 제조 분야의 결과물이다. 따라서 스마트공장의 보안을 살펴보려면 IT, OT/ICS, IoT, 물리 보안의 4대 영역을 모두 포함하는 보안을 고려해야 한다. 이제 남은 지면은 스마트공장의 보안 동향과 스마트 공장 보안을 위해 고려해야 할 사항에 관해서 기술하도록 한다.

스마트공장 보안 동향

스마트공장에 대한 보안은 스마트공장 참조모델인 RAMI (Reference Architecture Model for Industry) 4.0²⁾ 을 기반으로 보안을 적용하려는 유럽의 움직임과 ISA (International Society of Automation) – 95³⁾ 를 기반으로 ISA/IEC 62443을 통해 보안을 적용하려는 미국의 움직임으로 크게 볼 수 있다. 다만 미국의 경우에는 반드시 스마트공장을 대상으로 하는 것이 아니라 ICS (산업제어시스템) 영역 전반에 걸친 보안 기준을 마련하려고 한다.

각 국의 이러한 보안 노력은 ICS 분야에서 보안 인증 제도를 적용하여 ISASecure, IEC/ISA 62443 인증을 산업제어시스템 장비, 소프트웨어, 보안 프로세스 등에 대해 각 국가별로 제품, 사업자, 제조사를 대상으로 보안 인증 제도를 실시하고 있다. 또한 기업에서도 자체적으로 ICS 보안 인증 기준을 두고 이를 통과한 제품을 출시하고 있다. 다만, 대부분이 산업제어장비 위주의 인증으로 이루어져 있어 스마트 공장에 맞는 보안인증이라고 여기기에는 맞지 않는 부분이 있지만, 스마트공장을 구축할 때 들어가는 장비들이기 때문에 참조할만한 가치는 충분히 있다고 볼 수 있다.

2) RAMI 4.0

스마트 제조 참조모델로 독일 기계설비 공업협회(VDMA)가 구축, 국제표준화기구인 IEC 산하 SG8(전략 그룹 8, 스마트제조)에서 발표함. 독일에서 인더스트리 4.0을 추진하는 데 상이한 표준과 산업환경의 일반적인 이해를 돋기 위한 목적으로 개발되었으며 스마트그리드 참조 구조 모델(SGAM)을 참고하였음

3) ISA 95

엔터프라이즈(IT 영역)와 제어시스템 간의 자동화 된 인터페이스를 개발하기 위한 국제자동화 협회(ISA)의 국제표준으로 MES 설계의 기본방향을 분석하고 MES와 ERP를 운영할 수 있는 인터페이스, 객체 모델, 용어 등을 정의하고 MES를 기반으로 하는 표준안을 제시

아래의 표는 스마트공장에 대한 보안 인증제도는 아니지만, 산업 제어시스템에 대한 인증제도를 운용하는 주요 국가의 산업제어시스템 인증 명과 인증기관을 정리한 내용이다.

보안사고 증가율

인증 구분	국가	인증 명	인증 기관	적용 표준	내용
설비, 제품 및 안전 강제 인증	미국	UL	UL Inc.	UL 규격	전기/전자, 각종 기계의 제품 안전시험 및 인증 발행, 환경시험, 제품 성능시험
	유럽	CE	EOTC	EN 규격	전기, 가스, 의료, 기계 등 건강, 안전, 위생 및 환경 차원에서의 위험성 시험
	중국	CCC	CNCA	GB 규격	전기/전자, 기계장치, 정보통신 장비 등 사람 및 동식물 안전 및 환경 보호를 위한 시험
ICS 보안 인증	미국	ISASecure	ISCI	IEC/ISA 62443	제어기기 및 제어소프트웨어, 제어 시스템, 개발 프로세스에 대한 보안 인증
	독일	ISASecure	TÜV Rheinland	IEC/ISA 62443	제어기기 및 제어소프트웨어, 제어 시스템, 개발 프로세스에 대한 보안 인증
	독일	IEC-624 43 인증	TÜV SÜD	IEC/ISA 62443-3-3, 62443-2-4	IACS 사이버 보안 인증, 시스템 통합 사업자 인증, 제조사 인증
	일본	ISASecure	CSSC	IEC/ISA 62443	제어기기 및 제어소프트웨어, 제어 시스템, 개발 프로세스에 대한 보안 인증

(출처 : ICS CERT, 미국 기준)

스마트공장에 대한 보안에 대해서는 국내에서도 5G+ 중기 전략에서도 그 중요성을 인식하고 스마트 공장 보안 등 융합보안과 관련하여 제도개편(법 개정 포함), 산업육성 지원, 인력 양성 등 다양한 측면에서 산업 활성화를 위해 노력하고 있다.

그렇다면 현장에서의 보안에 대한 요구는 어떠할까? 실제로 스마트공장으로 전환하려고 하는 기업과 이를 지원하는 공공기관, 지자체 등에서는 스마트공장의 보안에 대해서 잘 이해하지 못하기에 이에 대한 준비도 미흡하다고 볼 수 있다. 현장에서는 스마트공장의 보안에 관해 관심이 없거나 있더라도 정보 보호 관리체계인 ISMS 인증으로만 해결하려고 하는 경우가 대부분이다. 이는 앞서 이야기한 스마트공장의 특징을 모르기 때문에 기존 정보보호 인력들이 IT 보안만을 적용하려 하거나 정보통신망 법에서 이야기하는 ISMS 인증만 받으면 보안에 대한 견제가 없을 것이라는 판단 아래에서 일어난다고 본다. 이는 반드시 개선되어야 한다.

스마트공장 보안 대책

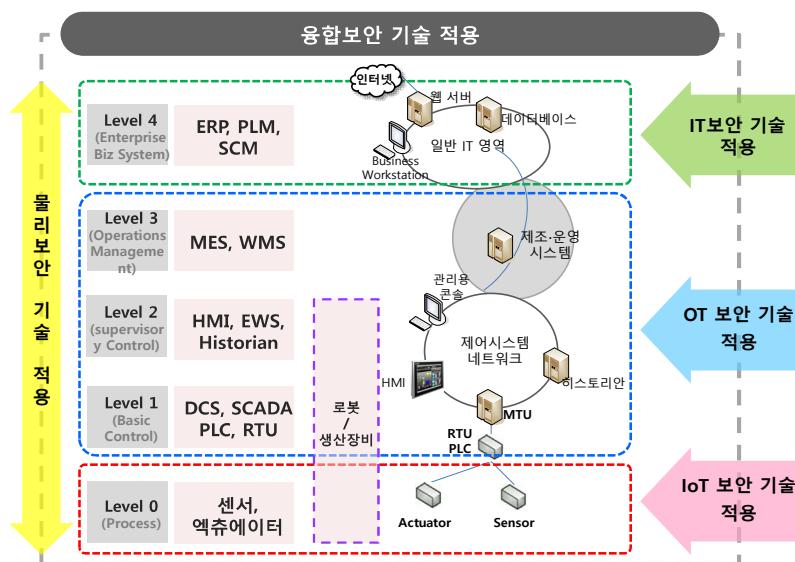
스마트공장과 관련된 보안 위협에 대해서 유럽 사이버 보안 조직인 ECSO(European Cyber Security Organization)의 WG3에서는 Industry 4.0 and ICS Sector Report에서 다음과 같이 6개의 주요 보안 과제를 언급하고 있다.

Industry 4.0 and ICS Sector Report 6가지 보안 과제

- 안전과 보안의 융합 (Safety-Security Convergence)
- 산업용 IoT에 대한 사이버 보안 (Cyber security of Industrial IoT)
- 산업용 제어시스템에 대한 침입 탐지 (Intrusion detection on Industrial Control Systems)
- 사이버-물리 위협 통합 관리 (Manage cyber-physical threats)
- 조직 및 역할의 변화 (Organisational and behavioural changes)
- 밸류체인을 포함하는 보안 (Security throughout the value chain)

따라서, 스마트공장의 보안은 IT/OT/IoT/물리 보안의 4개 영역의 보안을 모두 고려하여 설계되어야 하며, 이를 도식화하면 아래 그림과 같이 나타낼 수 있다.

스마트공장 계층별 적용 보안 대책



위 그림은 ISA/IEC 62443의 계층모델을 기반으로 스마트공장에 적용되어야 할 보안기술을 도식화한 것으로 실질적으로는 각 계층에 존재하는 장비에서 차이가 있을 수 있다. 상위 관점에서는 변화가 없을지라도 제조업의 공정의 다양성에 따라서도 변화가 됨은 분명한 사실이다.

물리 보안 측면에서는 스마트공장의 각 구역을 통제구역, 제한구역, 일반구역 등으로 나누어 공장의 외곽에서부터 내부 생산라인, 통합 제어실, 공조실 등을 중요도에 따라 나누어 관리하고 이를 출입하기 위한 절차 및 통제시스템의 적용을 고려해야 한다. 외곽의 경우에는 사람과 차량의 출입통제 외에 최근에는 드론에 대한 대비책도 마련되어야 한다.

IT 보안 측면에서는 서비스 거부 공격, 악성코드 및 랜섬웨어 감염, APT 공격, 정보 유출 등 다양한 보안 위협을 정의하고 이에 대한 대비책을 수립하는 것이 필요하다. 또한, 공급망을 통한 사이버 공격 등에 대한 대비책도 마련되어야 할 것이다. 공급망 공격은 IT 측면뿐 아니라 OT/ICS 분야에도 해당한다.

OT/ICS 보안 측면에서는 IT 시스템과의 연계를 고려하여 보안을 고려하여야 하는데 이때 공정절차에 대한 이해를 바탕으로 사용되고 있는 산업용 장비와 산업용 네트워크를 파악하는 것은 필수이다. 보통 그림 2를 기준으로 IT 네트워크인 이더넷은 Level 4, 3영역에서, 산업용 네트워크인 EtherCAT, Ethernet/IP, Profinet 등은 Level 2에서, 시리얼 통신인 Profibus, ModBus 등은 Level 1, 0에서 많이 사용된다. 하드웨어적인 구성 외에도 사용되는 Protocol에 대한 이해가 필요하며, IT 영역의 IDS처럼 해당영역에서 산업 보안 침해를 탐지 할 수 있는 산업용 IDS 혹은 산업용 보안 이상 징후 탐지 시스템을 운영하는 것이 좋다. 추가적으로 OT/ICS 영역에서 필요한 보안 기술 및 솔루션만 적용되는 것이 아니라 공장의 생산정보시스템과 생산 장비의 연계구조, 설비(Utility)에 대한 이해 등을 바탕으로 하는 보안체계의 구축을 고려해야 한다. 무엇보다 우선해야 할 것은 이러한 보안을 적용함에 있어 OT/ICS 영역이 IT 보안과 같은 위험(Risk)을 가지고 있다고 생각한다면 큰 오산이다. 공장에서의 제어시스템(ICS)의 고장, 장애, 보안 사고는 단순히 기기의 멈춤, 생산 차질만을 가져오는 것이 아니라 물리적인 대형사고로 연계된다. 즉, 인명의 사상, 폭발, 화재 등 실세계에 영향을 미치는 중대한 사고의 원인이 될 수 있기에 안전과 관련하여 접근해야 한다. 즉, 가용성이 우선시되어야만 한다.

IoT 보안 측면에서는 IoT 기기 자체에 대한 보안성과 Level 0인 현장 장치(Field Device)로부터 상위 Level로의 침투 가능성에 대한 분석, 현장 장치 인증, 통신 간의 위·변조 등의 보안 사항을 고려해야 한다.

마지막으로 4대 영역 전반을 포함하여 융합의 관점에서 위협을 탐지하고 대응할 수 있는 기술적, 관리적 체계가 필요할 것이다.

결언

스마트공장에 적용되는 보안은 단순히 정보보안, OT/ICS 보안, IoT 보안, 물리 보안의 한 가지만을 강조해서 되는 것은 아니다. 스마트공장의 탄생배경이 4차 산업혁명에 의해 제조 분야에서 나타난 IT와 제조업 간의 산업간 융합의 결과물이기 때문에 보안을 적용함에서도 해당 제조업의 특성을 이해하고 그에

맞는 융합관점의 보안을 적용해야 하기 때문이다.

이를 조직, 기술, 절차의 세 가지 관점에서 볼 때 다음과 같은 사항을 고려해야 할 것이다.

조직 측면에서는 해당 제조 분야의 업무절차, 공정 등을 이해하는 것을 전제로 스마트공장에 적용되는 4대 영역의 보안 기술을 모두 이해할 수 있는 가칭 CFSO(Chief Factory Security Officer)를 두고 4개 분야의 각 영역을 담당하는 조직이 그 산하에 있어야 할 것이다.

기술 측면에서는 분야별 보안 기술이 적용되어야 함은 물론이고, 각 영역간의 연계 및 상호 연동을 고려하는 융합보안 기술이 개발, 적용되어야 할 것이다.

절차 측면에서는 각 영역 특히 OT/ICS 분야의 생산 장비 및 Utility의 Life Cycle 전반에 걸쳐 보안이 고려되어야 한다. 장비의 입고, 설치, 운영, 폐기 등에 있어서 단계별 보안 기준과 점검 절차가 운영되어야 할 것이다.

스마트공장의 보안은 이제 시작이지만 개별 보안영역에서의 많은 경험과 전문가를 보유하고 있다. 따라서 이를 하나로 잘 엮을 수 있다면 단순히 스마트공장의 보안 침해를 방비한다는 점 외에도 스마트공장 보안(스마트 시티 보안 등 다양하게 변형 적용될 수 있다고 본다.)이라는 신산업분야를 선도해 나갈 수 있으리라 판단한다.

스마트시티 서비스를 위한 플랫폼 주요 보안 기술

김호원 (howonkim@pusan.ac.kr)



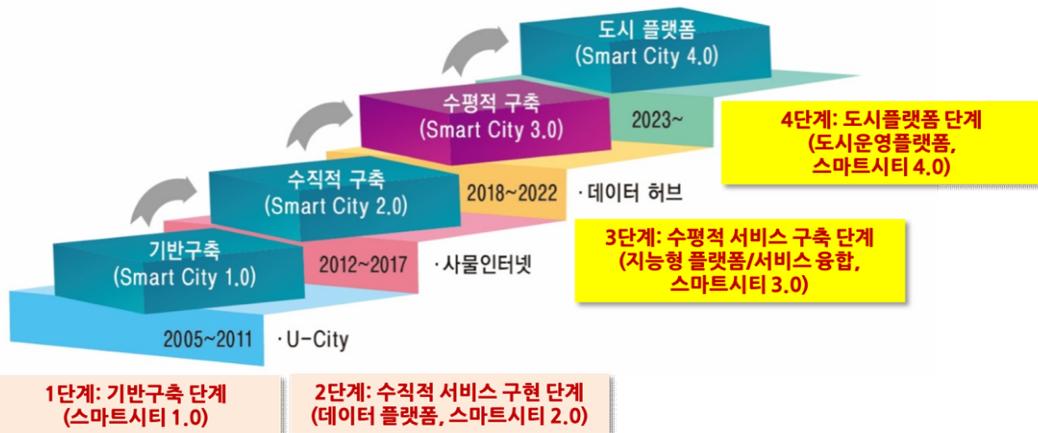
- (現) 부산대 사물인터넷 연구센터 센터장
- (現) 한국정보보호학회 상임이사
- (現) 한국통신학회 평의원, 정보처리학회 이사, 멀티미디어학회 이사

국내 스마트시티 동향 및 플랫폼 개발 현황

■ 국내 스마트시티 동향

- 스마트시티는 ICT 기술 공급자와 사용자 간에 조화를 이루는 것이 중요하며, 미래 스마트시티는 지속 가능한 스마트시티 서비스 생태계 조성이 되도록 진행된다.
- 국내에서는 부산의 에코델타시티, 세종 스마트시티, 대구와 시흥의 스마트시티 등 국토교통부 중심의 스마트시티 사업이 추진 중이며, 이외에도 서울과 창원시 등 여러 지자체에서 다양한 스마트시티 사업을 추진 중에 있다.
- 스마트시티 사업은 기존에는 사물인터넷과 유무선 통신/네트워크 등 기술 실증 중심이었지만, 현재는 도시재생 및 기존 도시문제 해결 등, 실질적인 스마트시티 조성을 위한 노력을 수행 중이다.
- 스마트시티 기술에서 활용되는 대표적인 ICT 기술로는 IoT와 AI, 플랫폼, 블록체인 등이 있음. IoT는 데이터의 센싱/수집 및 전송, 저장하며, AI와 플랫폼에서는 데이터의 처리/가공/활용, 블록체인은 데이터에 대한 신뢰성을 제공함. 일련의 모든 과정이 데이터와 관련되어있는 즉, 스마트시티를 데이터시티로 간주해도 무방하다는 것을 의미한다.

데이터 기반 스마트시티 개념도



스마트시티 플랫폼과 보안

■ 스마트시티 플랫폼과 보안

스마트시티 플랫폼은 IoT, AI, 블록체인 등 최신 IT 기술들이 종합적으로 융합되어 탄생한 기술이라고 할 수 있다. 융합 기술이라는 특징은 서비스의 확장성, 정확성, 편의성 등 많은 점에서 강점으로 작용하지만, 보안 관점에서 보았을 때 이러한 특징은 불리하게 작용한다. 그 이유는 스마트시티 플랫폼에 적용된 요소 기술의 취약점이 스마트시티 플랫폼에 동일하게 발생할 수 있기 때문이다. 그렇기에 스마트시티 플랫폼을 제공함에 있어, 보안은 설계에서 개발 단계까지 전 과정에서 반드시 고려되어야 할 부분 중 하나이다. 또한 시민의 생활과 밀접하게 관련되어 서비스를 제공하고 있다는 점으로 미루어보았을 때 보안 위협 및 사고가 발생하였을 경우 그 피해는 스마트시티 서비스가 제공되고 있는 도시의 시민이 될 수 있다. 그러므로 스마트시티 플랫폼 보안은 선택이 아닌 필수이며, 스마트시티 기술에서 핵심 중추 역할을 수행하는 부분 중 하나라고 할 수 있다.

■ 스마트시티 플랫폼의 보안 기술

- 식별 및 인증, 인가

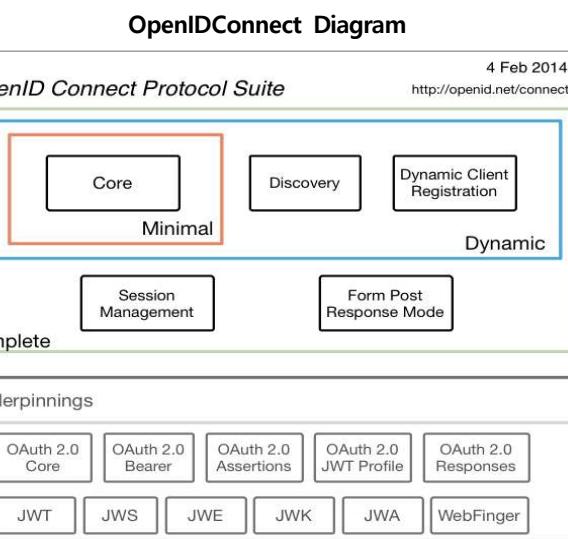
대부분의 스마트시티 플랫폼이 Micro service Architecture 형태로 제공되며 이에 따라 각각의 API 서버들은 API 클라이언트에 대한 식별(Identification) 및 인증(Authentication)과 인가(Authorization)를 위한 메커니즘이 필요하게 되었다.

식별(Identification)이란 어떠한 주체가 본인을 누구라고 스스로 주장하는 것이다. 식별과 인증은 떼려야 뗄 수 없는 관계이며, 이러한 식별은 인증이라는 과정을 거쳐 자신의 주장과 인증 내용이 부합한다는 것을 상대방 측에게 확인시킨다.

인증(Authentication)이란 서비스 사용자의 신원을 증명하는 행위라고 할 수 있다. 인증 방법의 분류로는 지식기반(Type 1, Something you know), 소유기반(Type 2, Something you have), 존재기반(Type 3, Something you are)로 분류할 수 있다. Something you know의 경우 사용자가 알고 무엇을 알고 있느냐에 관한 내용으로 패스워드, 패스워드 구문이 대표적이며, Something you have의 경우 스마트카드, 신분증, 열쇠 등이 있다. 마지막으로 Something you are는 본인 자신의 어떤 것을 인증하는 방식으로 지문인식, 장형 인식, 홍채인식 등의 방법이 존재한다. 위에서 언급한 방법 중 서로 다른 두 가지 이상의 타입을 이용하여 인증하는 것을 다중 인증(Multi-Factor Authentication)이라고 하며, 조직 전체의 보안성을 한층 더 높일 수 있는 효과적인 인증 방법이다.

인가(Authorization)란 사용자가 일련의 인증과정을 거쳐 인증을 받은 후, 접근제어 기술에 따른 전체 혹은 부분적으로 보호된 리소스에 접근할 수 있는 권한을 부여하는 행위이다. 접근제어라는 용어는 경우에 따라 인증과 인가를 합쳐서 혹은 인가를 접근제어라고 부르는 경우도 있다.

- OIDC와 OAuth2.0



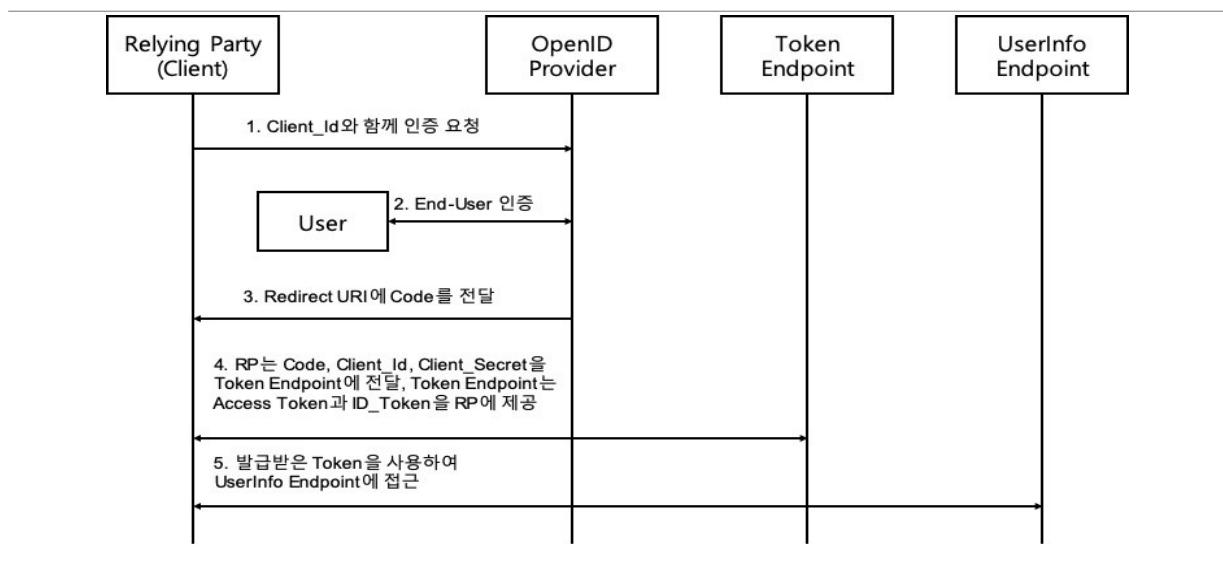
OIDC(OpenID Connect)는 OAuth 2.0 프로토콜을 기반으로 하는 Identity Layer이다. OAuth2.0은 보호된 리소스에 접근하기 위해 접근 토큰을 가져오고 사용하는 메커니즘을 정의하지만 ID 정보를 제공하는 표준 메서드는 정의하지 않는다. 그러한 의미에서 OIDC(OpenID Connect)는

SSO(Single-Sign-On)를 목적으로 OAuth2.0 권한 부여 절차와 더불어 Google, Microsoft 등의 공인된 IdP(ID공급자)에 로그인할 수 있도록 지원하는 표준 인증 프로토콜이다. 또한, OIDC는 기존의 Application에 추가로 mobile 디바이스, Native App(흔히 말하는 Mobile Application)에서의 인증/인가를 지원한다는 점에서 미래 지속적으로 사용 가능하다는 장점이 있다.

- 서비스 인증 & 인가 흐름도

앞서 언급한 식별과 인증, 인가 등 일련의 모든 과정이 OIDC와 OAuth 2.0 프로토콜에 의해서 수행된다. 클라이언트는 OpenID Provider로부터 인증을 요청하고, 응답으로 인가 Code를 받게 된다. 인가 Code와 자신의 정보를 포함하여 Token Endpoint에 Token을 요청하고 접근 허가 시 응답으로 Access Token을 획득하게 된다. Access Token은 보호된 리소스에 대한 접근 권한을 포함하고 있는 일종의 접근 허가권으로써, 클라이언트는 해당 Access Token을 포함한 요청을 Resource Endpoint에 보내고, 리소스를 제공받을 수 있게 된다.

OpenIDConnect 인증/인가 흐름도



- 접근제어(Access Control) 기술

접근제어 메커니즘은 주체로부터 오브젝트에 대한 접근 요청을 수신하고 접근허가를 결정하고 집행하는 논리적 구성요소로 정의할 수 있다. 이러한 접근제어 메커니즘은 고전적인 방법부터 최신 방법까지 다양한 방법이 존재한다.

- ACL(Access Control List)

ACL 모델은 리소스에 대한 접근 권한을 가진 사용자 또는 사용자그룹을 리스트에 기록하여 관리한다. 시스템은 접근제어 리스트를 참조하여 사용자에 대한 리소스 접근제어를 실시한다.

- DAC(Discretionary Access Control)

DAC 모델은 리소스의 소유권에 기반을 둔다. 사용자 또는 그룹이 리소스에 대한 소유권을 가지고 있을 때 다른 사용자나 그룹에 해당 리소스의 접근 권한을 부여할 수 있게 된다. 이러한 모델은 임의적 접근통제라고도 불린다.

- MAC(Mandatory Access Control)

MAC 모델은 관리자 중심의 접근제어 기술이다. 관리자는 리소스에 대한 보안 등급을 설정하고, 사용자에게 보안등급에 따른 리소스 접근 권한을 부여한다.

- RBAC(Role-Based Access Control)

RBAC이란 사용자의 역할에 기반하여 접근 통제하는 기법이다. RBAC을 사용하기 위해서는 역할 할당(Role Assignment), 역할에 따른 권한 부여(Role Authorization), 권한 부여(Permission Authorization)의 과정이 필요하며, 큰 조직 또는 그룹에 적합한 접근제어 모델이다.

- ABAC(Attribute Based Access Control)

ABAC모델에서 객체에 대한 접근제어는 사용자가 가진 속성을 기반으로 하며, 주체가 객체에 접근하기 위해 만족시켜야 할 속성에 대해 정의하고 있다. 주체는 접근 권한을 획득하기 위해 자신의 속성이 규칙에 부합함을 증명하여야 한다.

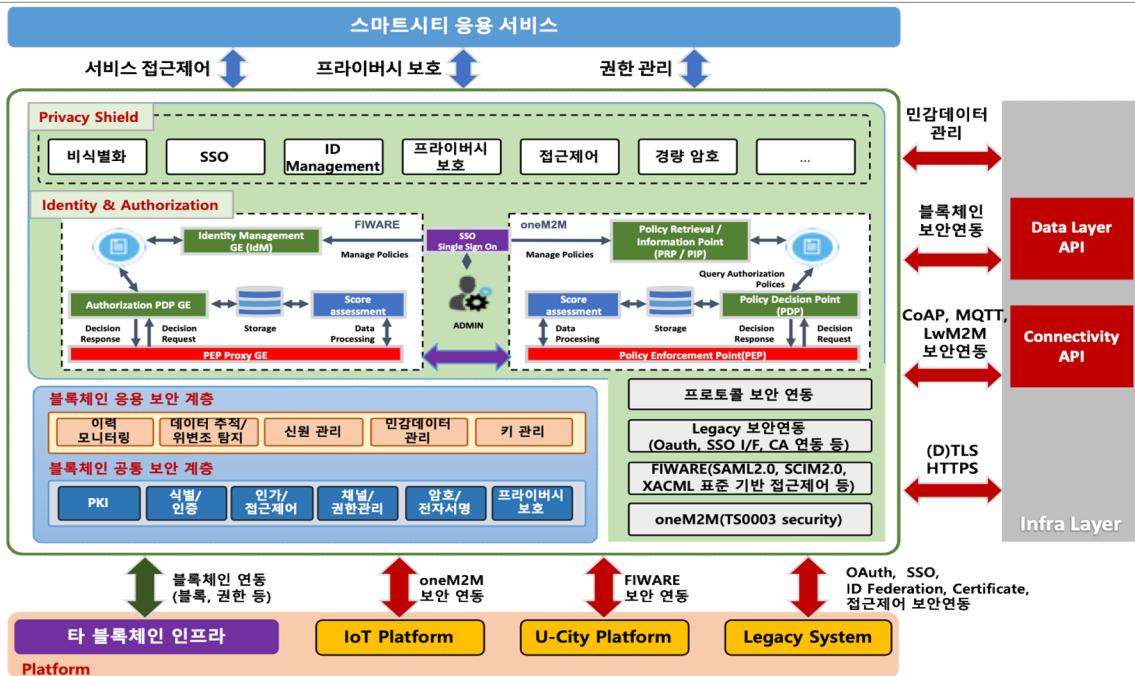
- CapBAC(Capability Based Access Control)

CapBAC은 IoT 환경을 위한 접근제어 방식으로 IoT 환경에서 RBAC이 디바이스에 적용될 경우 많은 Role을 수용하기 어려운 단점이 있으며, ABAC의 경우 IoT 환경의 속성들을 동일하게 일치시키기 어렵다는 단점이 있다. 이러한 한계점을 극복하고자 CapBAC은 주체에게 최소한의 권한 규칙과 권한 위임기능을 부여하여 자신이 접근제어를 관리할 수 있도록 한다.

■ 스마트시티 플랫폼에서의 통합보안 기술

스마트시티 플랫폼은 IoT, AI, 플랫폼, 블록체인 등 다양한 최신 IT 기술이 적용된 기술이므로 근본적으로는 각 요소 기술에 대한 보안 기술이 근간이 된다. 스마트시티 플랫폼 관점에서의 통합 인증/인가 보안, IoT 플랫폼에서의 디바이스 보안 및 플랫폼 보안 연동, 블록체인의 데이터 무결성 보장 등 스마트시티 플랫폼에서의 통합보안 기술이란 복합적인 요소 기술들의 보안 통합이라고 할 수 있다.

스마트시티 플랫폼 통합보안 구조도



스마트시티 보안 기술이 나아가야 할 방향

스마트시티는 기존의 응용 서비스와는 달리 최신 IT 기술들이 적용되어 탄생한 융합 기술이라는 특성을 가지며 보안 기술을 포함한 여러 요소 기술의 복합체라는 사실을 알게 되었다. 스마트시티의 특성에 의한 보안 취약성과 프라이버시 침해 문제는 어렵고 복잡한 문제이다. 이러한 스마트시티 보안 문제를 해결하기 위해서 먼저 정보보호 법령을 정비하고, 심화되고 있는 사이버 보안 위협에 대한 제도적 정책적 대응 역량을 대폭 강화해야 하며, 보안 위협으로부터 침해사고 발생 시 신속히 대응할 수 있는 체계적이고 조직화된 침해 대응 체계를 구축하고 고도화해야 할 것이다. 또한 스마트시티 기술이 현실에서 성공적으로 적용되기 위해서는 근본이 되는 요소 기술의 보안 기술 수준을 글로벌 수준의 경쟁력을 갖추도록 체계적으로 준비하고 관리해야 할 것이다.

[참고문헌]

- 서화정, 이동건, 김지현, 최종석, 김호원, "사물인터넷상에서의 보안과 프라이버시 보호 이슈," 정보처리학회지, v.21, no. 2, pp.48~60, 2014년3월
- 김호원, "스마트시티 인프라 보안기술", NetSec-KR, pp.374~390, 2019년 4월
- "OpenID", <https://openid.net/connect/>, 2019년 05월

의료기관 정보보호 강화를 위한 노력



경우호 (whkyung@amc.seoul.kr)

- (現) 병원정보보안협의회 회장
- (現) 서울아산병원 정보보호UM
- (現) 대한병원정보협회 정보보안이사
- (現) 스마트의료보안포럼 정책분과간사

시작하는 말

의료정보는 일반적인 개인정보 보다 훨씬 민감한 정보로서, 유출이나 훼손 시 환자 생명에 치명적인 위협을 가할 수 있을 만큼 파급효과가 크다. 때문에 의료기관은 의료정보를 잘 관리하고 안전하게 보호하기 위한 엄격한 정보보호 관리체계를 구축하고 운영해야 한다.

하지만 지속해서 발생하고 있는 의료기관의 환자 개인정보 유출 사고 사례에서 볼 수 있듯이 아직도 대다수의 의료기관은 안전한 정보보호체계 구축을 위한 비용 투자나 정보보호 활동이 부족하며, 이를 잘 운영하기 위한 전담조직 구성이나 인력 확보에도 소극적이다.

의료기관은 환자의 개인정보 및 의료정보를 안전하게 보호할 책임과 의무가 있다. 특히 최근에는 의료정보가 진료 목적뿐만 아니라 연구 목적으로도 다양하게 활용되고 있는 만큼 더욱 신중하고 체계적인 관리가 필요하기 때문에 현재 의료기관이 내포하고 있는 보안 위험요소들을 알아보고자 한다.

또한 이러한 문제점을 해결하는 데 도움이 될 수 있도록 병원 정보보안협의회 활동에 대해 안내하고 앞으로 나아갈 방안을 제시하여 의료기관의 정보보호 수준 향상에 도움이 되었으면 한다.

의료기관 및 연구원 전경



(출처: 서울아산병원)

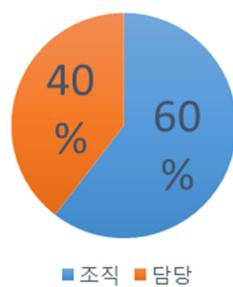
의무화된 ISMS 인증과 병원정보보안협의회 출범

2016년 개정된 정보통신망법 및 시행령에 의해 연간 매출액 1,500억 원 이상의 상급종합병원이 ISMS(Information Security Management System) 인증 신규 의무대상으로 지정됨에 따라 이에 해당하는 43개 병원이 ISMS 인증을 받았다. 의무대상을 기준 정보통신기술(ICT) 사업자에 한정하지 않고 민감한 정보를 다루는 의료기관까지 확대함으로써 정보보호 사각지대에 있던 의료기관도 정보보호 수준 개선을 위한 발판을 마련했다고 할 수 있다.

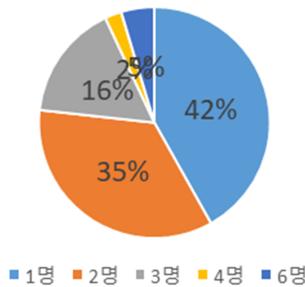
그렇지만 ISMS 인증을 받은 상급종합병원도 자세히 들여다보면 아직 부족한 부분이 많다고 여겨진다. 인증 필수항목인 정보보호 조직을 완벽히 갖춘 병원은 절반 정도에 지나지 않고 있으며 전담조직 없이 정보보호 담당자만을 두고 운영하는 병원도 많은 현실이다.

상급종합병원 정보보호 조직 및 인력 현황

정보보호조직



인원수



(출처: 병원정보보안협의회)

그나마 상급종합병원은 ISMS 인증을 받으면서 일정 수준 이상의 정보보호 관리체계를 구축, 운영하고 있지만, 그 외 종합병원이나 요양병원 등 중소 규모의 의료기관들은 규제 내에서 관리를 받지 못하다 보니 정보보호 업무를 수행하기 쉽지 않은 상황이다.

ISMS 인증을 받으면서 병원 상호 간의 정보 및 타 병원 사례 등을 공유하고, 공통된 의견을 모아 정부 기관에 건의하고자 2018년 7월에 병원 정보보안협의회를 출범하였다. 상급종합병원을 비롯한 종합병원 50곳의 정보보안 실무자 150여명이 회원으로 운영 중이며, 향후 협의회는 상급종합병원뿐만 아니라 모든 병원급 의료기관을 포함하여 구성할 예정으로 의료기관 전체의 정보보호 업무를 지원할 예정이다.

의료장비에 연결된 PC 보안 취약

랜섬웨어는 전 세계에서 심각한 사회적 문제로 떠오르고 있으며, 의료기관의 경우에는 의료장비를 연결하는 게이트웨이 PC의 보안 취약점으로 인해 랜섬웨어에 큰 피해를 입고 있다. 의료장비를 연결하는 게이트웨이 PC는 대다수가 기술지원이 종료된 운영체제를 사용하고 있으며 윈도우즈 보안패치 및 백신 프로그램을 설치 시 오작동이 발생하기도 한다.

그렇기 때문에 보안패치나 백신을 설치하지 않고 운영하는 경우가 많아 랜섬웨어에 쉽게 감염된다. 특히 2017년부터 5월부터 등장한 워너크라이 랜섬웨어는 운영체제의 취약점을 이용하여 네트워크에 연결된 모든 PC를 감염시켜 중요 파일을 암호화하고 시스템을 마비시킨다. 환자의 생사를 위해 촌각을 다투는 의료기관에서 랜섬웨어로 인해 의료장비 가동에 문제가 발생하면 환자의 생명도 위협받게 된다.

의료장비와 게이트웨이 PC



(출처: 서울아산병원)

이를 예방하고자 많은 의료기관이 랜섬웨어 방어시스템 도입, 백신 상시 업데이트, 보안 위협 모니터링 등 지속해서 노력하고 있지만, 게이트웨이 PC의 보안은 자동으로 관리가 어려운 상황이다.

그렇다면 의료장비의 랜섬웨어 감염을 막을 수 있는 방법은 무엇일까? 운영체제 보안패치 및 백신 프로그램 설치가 불가능한 의료장비 PC 운영 현황에 대해 전수조사를 시행해 인터넷 등 불필요한 서비스를 차단하고 보안 위협 발생 시 긴급 패치 적용 등의 조치가 가능하도록 준비해야 할 것이며 정부에서도 의료장비 PC에 대한 보안정책이나 가이드라인을 제시하여야 한다.

의료기관 개인정보보호 자율점검

정부가 민간기업 전체의 개인정보보호를 효율적으로 규율하지 못하는 문제점 해소를 위해 관련 사업 분야의 협회 및 단체에 제도적 지원을 통해 개인정보 관리의 효율성 제고 목적으로 개인정보 자율점검 제도를 시행하였다. 의료분야 자율규제 단체로 2016년 10월 행정안전부(이하 행안부)로부터 개인정보 보호 자율규제 및 점검 능력을 인정받아 대한병원협회가 최초 지정되었다.

2019년 개정된 개인정보보호 자율점검 규약은 지금까지 수동적인 형태의 점검에서 자율규제단체를 통한 적극적인 점검을 요구하게 개정되었다. 개정된 규약을 수행하기 위하여, 대한병원협회와 병원정보 보안협의회는 공동으로 자율규제점검 안을 만들고 적용하고자 한다.

자율규제단체 운영의 자문을 위하여 분야별(법률, 학계, 현업) 전문가로 구성된 운영 TFT를 구성하였으며 자율규제 심사원을 양성하여 회원사 대상으로 현장 심사를 5년 주기로 의무적으로 시행하고자 한다. 자율점검을 수행한 의료기관 중 우수한 기업은 표창하고 행안부 개인정보보호 실태점검 대상에서 제외되며 개인정보 유출 사고 발생 시에도 정상참작이 이루어지는 등 많은 혜택이 주어진다.

클라우드 서비스 유형 비교 (이용자와 제공자)

구분	대한병원협회	병원정보보안협의회	비고
역할	정책수립	심사원 운영	
업무	<ul style="list-style-type: none"> ▲ 개인정보보호 현장심사원 전문 교육 실시 ▲ 개인정보보호 자체 현장 이행확인 및 컨설팅 수요조사확인 ▲ 자체수행 개인정보보호 처리 프로그램 현장 확인 ▲ 자체수행 개인정보보호 현장 이행 확인 및 컨설팅 실시 	청구소프트웨어 보안기능 18개 포함	

(출처: 대한병원협회)

행안부에서 개인정보보호 실태점검을 나가면 과태료 받을 의료기관이 많을 것으로 예상된다. 개인정보 보호 자율점검을 규제나 간섭으로 생각하지 않고 모든 의료기관이 자율규제 단체의 현장 심사를 수행하게 되면 의료기관의 정보보호 수준도 많이 향상되고 정보보호 업무에도 많은 도움이 될 것이다.

맺음말

최근 증가하고 있는 의료기관 해킹 등 각종 보안 위협으로부터 의료기관은 환자의 개인정보 및 의료정보를 안전하게 보호하고 체계적으로 관리하기 위하여 주요 정보 자산에 대한 취약점 분석·평가, 보호 대책 수립 및 이행, 감독기관의 주기적인 점검 등 정보보호 관리체계 강화에 적극적으로 임해야 한다. 의료기관은 환자의 생명과 직결된 민감한 정보를 많이 보유하고 있다. 환자의 정보를 보호하는 노력은 의료의 질 향상 못지않게 중요하기에 정보보호는 선택이 아닌 필수업무로 인식하고 수행해야 할 것이다.

그러나 의료기관 자체 자율적인 부분으로는 한계가 있으니 개인정보보호 자율규제 단체의 자율점검을 성실히 수행하는 것이 바람직하다고 본다. 마지막으로 자율적으로 구성하고 노력하는 병원정보보안협의회가 잘 추진할 수 있도록 정부와 관계기관의 적극적인 지원을 해주시기 바란다.

2019년 마이크로소프트 빌드, 페이스북 F8, 구글 I/O에서 발표한 인공지능 기술과 그 의미



한상기 (stevehan@techfrontier.kr)

- (現) 테크프론티어 설립자 겸 대표
- (前) 세종대학교 ES 센터 교수
- (前) KAIST 문화기술대학원 교수
- (前) 다음커뮤니케이션 전략 대표

들어가며

최근 우리나라를 필두로 서비스를 개시한 5G 서비스는 차세대 무선 네트워크 기술로 다양한 네트워크를 통한 고속 데이터 전송, 대기시간 축소, 수많은 IoT 기기에 대한 끊김 없는 서비스 등 통신 서비스를 획기적으로 개선할 것으로 기대되고 있다. 5G의 도입은 지능형 로봇, 증강현실, 스마트시티 등 전후방의 산업 발전을 가속할 것으로 예상된다. 또한 5G 기술의 진화는 인공지능, 기계학습과 접목하며 디지털 기술 전반에 융합되면서 ICT 생태계 전반의 변혁을 촉진할 가능성이 높다.

4월 말에서 5월 초에는 미국의 대표적 테크 기업인 마이크로소프트, 페이스북, 구글이 개발자 컨퍼런스를 열면서 각종 새로운 기술과 전략을 소개한다. 이를 통해 앞으로 2~3년 동안 해당 기업이 어떤 기술 방향과 사업전략을 추구하는지 확인할 수 있으며, 개발자 커뮤니티 또한 자사에 호의적이고 풍성한 생태계를 구축하고자 한다. 이런 노력은 우리 기업이 아직은 더 보고 배울 점이 많지만, 국내에서도 몇 년 전부터 이런 활동이 이루어지고 있어 고무적이라고 볼 수 있다.

이번 보고서에서는 위의 세 가지 행사에서 발표한 기술 중에서 인공지능과 관련된 기술을 정리함으로써, 세 회사의 인공지능 기술 전략의 방향을 이해하고, 국내 기업이 이에 능동적으로 대처할 수 있기를 기대한다.

マイクロソフト ビルド 2019

マイクロソフトのビルト 2019は5月6日から8日まで米国シアトルで開催され、6千人以上の来場者が参観した。¹⁾サティヤ・ナデラは、世界中の企業がAI技術を活用する時代であると述べた。また、開発者がAI技術を活用して、AIクラウドとAIエッジ時代のプラットフォームを強化した。²⁾

このビルトで、マイクロソフトが示したAI関連技術の中でも注目されたのは、自走型ロボット開発用のクラウド基盤である。これを構築したのは、マイクロソフトの子会社であるボンサイ(Bonsai)である。ボンサイは、自走型システムの学習に有用な強化学習分野に特化したスタートアップである。³⁾

この発表は、まだレビュー段階の技術であり、Azure⁴⁾を基盤とした開発者たちが自走型ロボット開発用のモジュールシステムを学ぶためのツールである。すでにマイクロソフトは、エアシム(AirSim)シミュレーターやドローン用のサービス、機械学習とティ칭用のツールなどを提供している。同時に、既存の機器ネットワークサービスやオープンソースのロボットOS(ROS)と一緒に利用できる。

アーティクルス・ガイア Sの小型車両検査ロボットとドクターマーテリアル・ハンドリングの自走型車両を開発した初期開発事例を示した。

アーティクルスのガイア Sロボット



マイクロソフト 365は、マイクロソフトのオフィス 365、Windows 10、企業用モビリティとセキュリティを組み込んだ製品群である。このビルトでは、人々の生産性を高めるためのAI技術によるAIがマイクロソフト 365のスイートにどのように組み込まれるかを見ることができた。⁴⁾

1) <https://news.microsoft.com/build2019/> 参照

2) Microsoft Blog, "Microsoft to acquire Bonsai in move to build 'brains' for autonomous systems," Jun 20, 2018

3) マイクロソフトが提供するパブリッククラウドサービス <https://azure.microsoft.com/> 参照

일단 마이크로소프트 서치가 일반에게 공개되는데 이는 Bing(Bing)과 마이크로소프트 그래프의 인공지능 기능을 활용해 검색의 수준을 올리고자 한다. 특히 마이크로소프트 그래프는 조직의 모든 내부 데이터 망이나 공공 인터넷에 존재하는 데이터를 활용하도록 한다. 특히 Bing에서 검색하든 윈도우 10에서 검색 바를 이용하든 가장 현재 문맥에 맞는 결과를 제시한다고 한다.

또 다른 지능으로는 기계 독해인데, 우리가 제시하는 질문에 명확히 일치하는 구문을 문서에서 추출해준다. 불명확한 정보에 기반해 기업 내부에서 사람을 검색하는 기능 역시 추가되었다.

올해 가을부터는 워드 온라인을 제공해 문서 작성은 더 좋게 만드는 방안을 제시한다. 워드의 아이디어스라는 기능으로 마이크로소프트 그래프의 지능, 머신 러닝을 활용해 뛰어난 문장이나 더 프로다운 문서를 만들고, 다른 사람이 만든 문서를 효과적으로 둘러보게 한다. 이미 파워포인트나 엑셀에서 제공하고 있는 지능형 기능의 워드 버전이라고 볼 수 있다. 특히 워드의 '다시 쓰기' 기능은 신경망을 이용해 문장을 다른 방식으로 작성할 수 있음을 제시하는 기능이다.

지능형 비서에 대한 미래 비전으로는 2018년 인수한 시맨틱 머신즈의 기술을 대화형 엔진으로 발전시키고 있다. 대부분의 지능형 비서가 어떤 질의응답이나 사용자 요구를 수행하기 위해서 일일이 손으로 코딩한 스텝을 따라가지만, 이번에 발표한 기술은 데이터를 통해서 대답을 얻거나 이렇게 학습된 방식을 여러 문맥에 사용해 좀 더 일반화할 수 있음을 보여주었다. 예를 들어, 축구 경기 점수를 알아내는 방식은 일기 예보나 교통 상황에 대한 정보를 알아내는 데에도 적용할 수 있다는 것이다.

이를 통해 좀 더 쉽게 동적인 대화가 가능해 서로 연관된 내용, 문맥, 개념을 별개의 소스를 통해 연결해 대답하고, 옵션을 제공하고, 결과를 제시할 수 있다. 또한, 대화의 문맥을 따라가면서 기억할 수 있도록 해서 말을 하면서도 듣기를 수행하는 풀 듀플렉스 기능을 갖게 했다. 이 기능은 현재 코타나 위에 구현되며, 오피스 패키지에서 필요로 하는 일을 좀 더 사용자의 선호나 의도에 맞게 수행하도록 도와줄 수 있다. 마이크로소프트 봇 프레임워크에서도 사용하게 될 것이다.

페이스북 F8 발표

매년 열리는 F8은 올해 열 번째로, 4월 30일부터 5월 1일 산호세에서 열렸다. 인공지능, 오픈 소스, 증강현실과 가상현실, 개발자 프로그램, 새로운 개발 도구 등을 소개했지만, 가장 큰 변화는 향후 페이스북의 중심을 프라이버시에 초점을 맞추는 플랫폼으로 가져가겠다는 것이다.⁴⁾ 저커버그는 그의 키노트에서 '미래는 프라이빗이다'라는 비전을 제시했다.

인공지능 기술은 CTO인 마이크 슈로퍼가 발표한 두 번째 날 발표의 주요 주제였다. 특히 그동안 페이스북을 곤란하게 만든 허위정보나 폭력, 차별적 포스팅에 대한 처리를 인공지능으로 하겠다고 선언한 저커버그의 약속이 어떻게 실현되고 있는지를 보여주었다.

4) Microsoft AI Blog, "How AI is making people's workday more productive," May 6, 2019

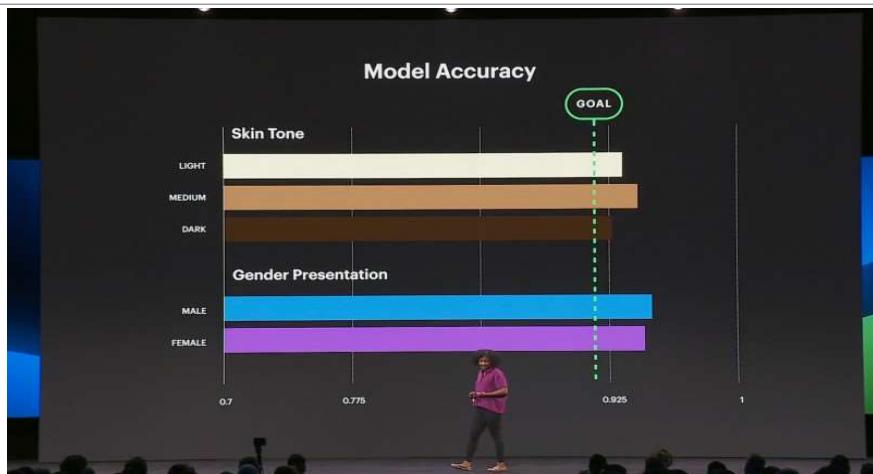
5) VentureBeat, "Everything Facebook announced at F8 2019," May 2, 2019

페이스북의 기술과 사회 문제를 다루기 위한 프레임워크



특히 허위 계정, 거짓 정보, 남용과 편향의 문제를 기술적 접근과 함께 외부 전문 기관과 협력을 통해 풀어가겠다고 선언했다. 그동안 많이 거론된 피부색과 젠더에 따라 인식률이 달라지는 얼굴 인식 문제도 새로운 알고리듬으로 8.5배 빠르게 수행하면서도 목표 정확도를 넘었음을 선언했다.

얼굴 인식의 편향 문제 해결



또한, 언어에 구애받지 않는 인공지능 모델 개발로 93개의 언어와 30가지의 방언을 처리할 수 있게 학습한 모델과 비디오 상에서 중요한 부분을 빠르게 스캔하고 처리하도록 함으로써 6,500만 비디오에서 1만 개 이상의 서로 다른 행위를 인식할 수 있음을 보여줬다. 이를 기준 벤치마크 비디오 데이터를 통해 확인한 결과 82.8%의 뛰어난 인식률을 보였다.

페이스북은 인공지능 학습 테크닉을 자기-지도학습 기술로 전환하고 있는데, 이는 적은 양의 레이블

데이터와 다량의 레이블이 안 붙은 데이터를 함께 사용해서 정확도를 높이는 기술로, 과거 12,000시간 분량의 수동으로 레이블을 붙인 데이터와 비교해 단지 80시간의 데이터만으로 더 정확도를 올렸다고 발표했다.

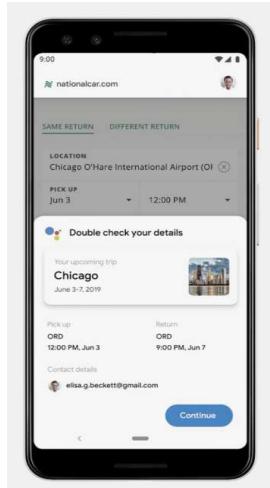
새로운 머신 러닝 도구인 Ax도 발표했는데, 이는 파이토치(PyTorch) 위에서 돌아가는 머신 러닝 실험 관리를 위한 플랫폼이다.⁶⁾ Ax는 인공지능 모델의 정확도를 올리기 위해 학습률과 드랍아웃을 조정하기 위한 실험을 작동시키는 플랫폼이다. Ax는 이번에 발표한 베이스 최적화 패키지인 보토치(Botorch)와도 작동한다.

구글 I/O

구글 I/O 역시 매해 열리는 개발자 컨퍼런스로 올해는 5월 7일부터 9일까지 마운틴 뷰의 앰피씨어터에서 개최했다. 올해에는 7천 명 이상이 참여했다고 한다.

작년에 듀플렉스를 발표해 놀라움을 제공한 구글은 올해는 '듀플렉스 온 더 웹'을 발표했다.⁷⁾ 이미 44개 국가에서 사용 가능한 듀플렉스는 전화와 음성을 넘어 웹으로 확장하겠다는 의미이다. 현재는 차량 렌탈 예약과 영화 티켓 구매와 같은 사례에 국한한다. 예를 들어, 자동차를 렌트하려고 하면 듀플렉스가 렌탈 회사 웹사이트에 접근해 필요한 정보를 사용자를 대신해서 작성해 준다. 웹 버전의 자세한 내용을 올해 하반기에 공개할 예정이다.

자동차 렌트 양식을 대신 채워주는 듀플렉스



6) VentureBeat, "Facebook launches machine learning experimentation tool Ax," May 1, 2019

7) TechCrunch, "Google is bringing AI assistant Duplex to the web," May 7, 2019

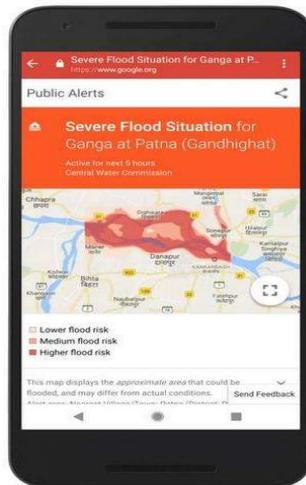
구글 렌즈는 구글 검색과 더 통합되어 이제 14가지 언어를 핸드폰에서 인식하고, 크게 읽어 주고, 번역을 할 수 있다. 구글 어시스턴트 역시 이제 기기 자체에서 동작하면서 속도가 10배 정도 향상되었고, 웨이즈(Waze)에서 사용할 수 있는 드라이빙 모드를 제공한다.⁸⁾ 구글 렌즈는 식당의 메뉴나 종이에 있는 정보를 인식하고 정보를 제공할 수 있으며, 메뉴에 나온 음식 사진을 구글 맵스에 있는 정보로 제공해 주문에 참고하게 하고, 계산서를 인식해 계산을 도와주고, 팁을 계산하거나 음식값을 나눠 계산하도록 도와준다.

구글은 이제 연합 학습 (federated learning)이라는 분산 머신 러닝 기술을 통해 서로 다른 지역에 있는 모바일 폰이 협력적으로 머신 러닝 모델을 학습할 수 있게 함으로써 핸드폰에 있는 개인 데이터를 전송하지 않게 만들었다.⁹⁾

구글은 말하기나 듣기 장애가 있는 사람들을 위해서 라이브 캡션, 라이브 릴레이, 프로젝트 유포리아 등을 발표했는데, 라이브 캡션은 안드로이드 Q 버전에서 지원할 예정으로 안드로이드 기기에서 보는 모든 비디오에 자막을 제공한다. 라이브 릴레이이는 구글 어시스턴트를 통해 문자로 작성한 내용을 전화로 상대방에게 음성 전달하고, 상대방 얘기도 다시 문자로 바꿔 준다. 프로젝트 유포리아는 언어 장애가 있는 사람들의 음성 샘플을 모아서 그런 사람들의 음성을 향상할 예정이다.

'환경 지능'이라는 이름의 기술로 사회 복지를 위한 인공지능의 적용 사례 중 하나는 인도에서의 홍수 예측이다. 인도의 중앙 수자원 위원회와 같이 협력해 파트나 지역에 대한 홍수 예측을 통해 피해 지역의 주민을 미리 대피시키거나 전력 중단 등에 대해 대비할 수 있게 했다. 정확도는 90%에 달해 다른 지역으로도 확대할 예정이다.

홍수 예측을 위한 인공지능



정리하며

8) Androidcentral, "Google I/O 2019: Top 12 announcements!," May 9, 2019

9) Synced, "I/O 2019 Your Data Stays on Your Phone: Google Promises a Better AI," May 7, 2019

이번 세 회사의 발표의 핵심 중 하나는 프라이버시에 대한 접근과 스마트 기기 자체에서 제공하는 옛지 컴퓨팅이다. 이는 개인 데이터를 더 이상 클라우드로 가져오지 않고 보호함으로써 그동안 많은 문제를 일으킨 프라이버시 문제에 보다 근원적인 해결 방안을 찾아내겠다는 의미이다. 동시에, 그동안 인공지능 학습을 위해 수집한 데이터가 이미 충분히 확보되었기 때문에 지금까지 제시한 지능은 이제 서비스로만 제공할 수 있다는 자신감이다. 구글이 그동안 100GB 크기의 음성 인식 모델을 단지 0.5 기가바이트로 줄였다는 것이 그 증거이다.

구글은 특히 사회 복지를 위한 기능에 많은 접근을 제시했으며, 페이스북은 공정성이나 폭력, 허위정보에 본격적으로 대응하겠다는 자세를 나타냈다. 마이크로소프트는 자사가 강점을 가진 오피스 생산성을 크게 향상하는데 인공지능을 본격적으로 투입하겠다는 의지를 보였다.

중국과 미국의 기반기술 주도권 경쟁



박성림 (sunglimpark@naver.com)

- (現) 국립타이베이간호건강대학 교양교육센터 강사
- (現) 국립정치대학(대만) 정치학연구소 박사과정 수료
- (前) 주타이베이 한국대표부 연구원

중국과 미국 간 ICT 기반기술 주도권 다툼

미국과 중국 사이에 무역전쟁 외에 새로운 갈등이 전개되고 있다. 바로 “사이버공간 주도권 경쟁”이며, 그 시작은 미국 정부로부터 시작되었다. 미국 백악관은 2019년 5월 15일 도널드 트럼프 대통령이 미국 내 정보통신 기술 및 서비스 보호를 위한 국가비상사태를 선포했다고 발표했으며, 미국 언론들은 이번 조치가 사실상 중국 정보통신 장비 제조사인 화웨이(Huawei)를 겨냥한 것이라고 지적했다. 수년 전에만 해도 화웨이는 장비 제조사로서 업계 관계자들에게는 익숙한 이름이었지만, 이제는 ICT 분야 전문가가 아니어도 “들어 본” 이름이 되었다. 2018년 12월 2일 명 완저우 화웨이 CFO가 미국의 대이란 재재 위반으로 캐나다에서 체포되었고 중국 외교부는 12월 7일 정례 브리핑에서 브리핑의 70%를 명 완저우 체포 관련에 할애하며 캐나다와 미국 정부에 항의를 표명했다. 반면, 미국 국무부는 이는 대이란 재제위반에 따른 조치이며 순수하게 법적 이슈라고 반박하였다. 미·중 정부 간 갈등에 이어 미국 학계 또 한 화웨이와 거리를 두고 있다. 올해 4월 UC 버클리, 스탠포드대, 미네소타대는 화웨이와의 연구 협력을 중단할 것을 선포했으며, MIT 또한 화웨이로부터 연구지원금 수령을 중단한다고 발표한 바 있다.

양국의 갈등은 비단 화웨이 뿐만 아니라 첨단 기술 분야에서도 첨예하게 드러나고 있으며, 인공지능

과 5G 기술에서 매우 확연하다고 하겠다. 2019년 2월 트럼프 대통령은 인공지능 개발증진을 위한 행정명령에 서명했으며, 구체적으로 1) 전문가 교육 강화, 2) 인공지능 체제구축을 위한 클라우드 서비스 및 정보 접근 개선, 3) 국제 협력 등이 포함되었다. 이뿐만 아니라 국방부에 인공지능 전담부서를 만들어 약 7,500만 달러를 투입하고 있고, 기타 연방 부처도 인공지능 기술개발과 진흥에 뛰어들고 있다. 그러나 미국 전문가들은 이는 중국 정부 주도의 인공지능 진흥에 비해 턱없이 못 미친다는 비판을 제기하고 있다. 2016년 기준 중국 인공지능 논문 저자 인용 수는 2000년 대비 44% 증가했으며, 2017년 한국 소프트웨어 정책연구소 보고에 따르면 중국의 인공지능 연구역량은 양적 지표(연구 건수, 피인용 횟수)에서 이미 미국을 능가했으며, 2017년 칭화대학 인공지능 및 로봇학습과정 등록자가 2010년 대비 160% 증가했다. 비단 인공지능 뿐만 아니라 5G에서도 중국의 움직임은 세계의 주목을 끌고 있다. 상술한 화웨이는 5G 네트워크 구축 및 관련 장비 분야 모두에서 수준 높은 기술을 갖추고 있으며, 이는 5G 소프트웨어 분야에서만 강점을 지닌 구글과 대비되는 측면이 있다. 화웨이는 2000년도부터 아프가니스탄, 노르웨이 등 악천후가 상시 존재하는 세계 각지에서 통신 네트워크 시공의 경험이 풍부하고, 이와 더불어 5G 특허, 반도체, 연결 장비 측면에서도 높은 수준의 기술과 저렴한 가격 및 기술경쟁력을 갖추고 있다.

상기에서 논의한 화웨이 논쟁과 5G 및 AI 개발 경쟁은 이러한 기반기술이 향후 세계 각국의 경제 및 사회 질서를 주도하는 일종의 “룰”的 역할을 한다는 점이며, 화웨이는 5G 네트워크 구성 및 장비 제조 사로 경쟁자인 에릭슨, 노키아 및 삼성보다 압도적으로 풍부한 경험, 기술특허 및 가격경쟁력을 갖추고 있는 반면, 미국은 이를 주도할 기업이 없는 실정이다. 화웨이의 세계적인 확장은 시진핑 지도부 하에서 아시아를 비롯해 유럽, 중동, 남미 등 전 방위로 진출하는 중국 외교의 흐름을 연상하게 하며, 미국에게는 자국의 위상을 위협하는 신호로 보이게 한다. 루치르 샤르마(Ruchir Sharma) 모건스탠리 부사장은 2018년 6월 뉴욕타임스 칼럼에서 향후 세계 각국 경제의 GDP 중 80%는 신기술의 개발과 응용에 따른 생산력 증대에 좌우될 것이라고 지적했다. 특히 그는 베이징에 도착했을 때 구글과 페이스북 같이 서구 사회에서 매일 접하는 웹사이트를 더 이상 사용할 수 없고, 바이두(Baidu)와 위챗(WeChat)을 사용해야 함을 지적하며 양측의 차이를 확연히 지적했다.

즉, 화웨이를 둘러싼 미국의 경계감과 중국의 우려는 향후 어떤 나라가 세계 경제 및 사회질서를 주도할 기술을 장악하고 이 “규칙”을 만드느냐에서 나온 것이다. 이에, 본고는 이런 시각에서 제2절에서 화웨이 논쟁을 우선적으로 검토하고, 이어 제3절에서 인공지능 및 5G 분야에서 양국의 진흥정책 및 기술개발 현황을 논의할 예정이다. 제4절에서는 이 같은 중국과 미국의 5G 및 인공지능 기술과 관련된 논쟁이 1) 첨단기술 개발 선점 경쟁, 2) 세계 경제 및 사회질서의 주도권 선점에 대한 우려에서 비롯됨을 제시하고, 이 같은 양국의 경쟁은 향후 다른 기술 분야에서도 발발할 수 있다는 점과 더불어 우리에게 시사 하는 바를 제시하고자 한다. 특히, 양국의 기술 경쟁 및 관점의 차이는 중국과 미국에 경제와 안보 분야에서 크게 의존하고 있는 우리에게 재차 “제2의 사드 사태”를 불러일으킬 소지가 있으며, 이를 위해서는 1) 중국과 미국의 사이버공간 관점 차이에 대한 정확한 이해, 2) 지속적인 현황 모니터링과 더불어 3) 다양한 소통 채널을 통해 우리의 곤경과 입장을 명확하게 소개함으로써 불필요한 오해를 줄이는 방

안을 고려해볼 것을 제안하고자 한다.

화웨이를 바라보는 미국과 중국

화웨이는 창업자 런 정페이(Ren Zhengfei)가 1987년 홍콩 인근의 션전(Shenzhen)에 설립한 ICT 장비 및 솔루션 전문기업이다. 1997년부터 저개발 국가 및 농촌 지역 등 세계 170개국에서 뛰어난 기술력과 저렴한 가격경쟁력에 기반해서 유선 네트워크 인프라 구축 및 관련 장비, 개인 통신 단말기 개발 및 판매로 세계 통신업계의 강자로 부상하고 있다. 화웨이의 주력제품은 텔레콤 네트워크(5G 포함), 클라우드 서비스이며, 유무선 네트워크 매출이 전체 매출의 절반을 차지하고 있다. 화웨이에 관한 의혹은 2011년 블룸버그에서 보다폰의 화웨이 공유기 관련 백도어 이슈를 보도하면서 불거졌다. 당시 보다폰 내부 문서에 따르면 화웨이 가정용 공유기에 네트워크에 무단 접속이 가능한 '백도어'가 발견되었으며, 화웨이 측은 수정 후 문제를 해결했다고 통보했지만, 추가 테스트에서 여전히 일부 취약점이 해결되지 않음이 확인되었다고 한다. 당시 화웨이 측은 기술적 실수였으며, 보안을 우회하기 위해 의도적으로 숨겨진 통로를 지칭하는 백도어가 아니라고 주장했다. 이 문제가 발생한 후에도 보다폰은 여전히 화웨이 장비를 사용하고 있으며, 이 외에 구체적인 보안 리스크가 확인된 사례가 발견한 바 없다.

이와 불어, 화웨이가 중국 정부 주도의 사회통제 시스템 구축에 기술지원을 제공하고 있다는 비판도 제기되고 있다. 텐왕(Tian-Wang)으로 통칭되는 사회안전망은 중국 전 지역에 인공지능 카메라 기반의 치안 모니터링 시스템으로 화웨이는 AI 카메라, 모니터링 시스템을 종합한 스마트 시티 솔루션을 제공하고 있으며, 중국 남부의 션전(Shenzhen)시 롱강구 행정센터에 화웨이의 솔루션을 적용한 모니터링 시스템이 활용되고 있음이 언론에 확인되었다. 또한, 신장 위구르(Xinjiang Uygur) 자치구에 소재하는 무슬림 교화캠프로 알려진 수용소의 감시 시스템에 화웨이 제품이 공급되었다는 주장이 있다.

화웨이에 관한 비판과 더불어 화웨이의 배후에 중국 정부가 있다는 주장이 제기되고 있다. 여기에는 1) 창업자 런 정페이 회장의 경력(전 중국군 통신장교), 2) 비상장회사에 따른 공개정보 부족, 3) 중국공산당 주도의 중국정치경제 현실상 중국 정부의 지시에 따른 정보활동 가능성 등이 근거로 제시되고 있다. 그러나 화웨이는 회사 종업원들이 주식을 소유하고 있고, 중국 정부에 고객 정보를 제공하거나 정부로부터 제공요청을 받지 않았다고 이 같은 의혹에 항변했다. 또한, 런 회장의 중국군 장교 출신과 더불어 비상장사로서 공개정보가 부족한 것을 들어 "화웨이=중국군 기업"으로 보는 것은 다소 논리적인 무리가 따르며, 양자 간의 협력관계가 명백히 존재한다고 보기에는 이같은 논리와 사례만으로는 여전히 부족한 측면이 있다.

그러나 미국은 2018년을 기점으로 화웨이에 대한 강경한 입장을 고수하고 있으며, 올해 5월 트럼프 대통령의 행정명령은 화웨이를 비롯하여 광범위하게 중국 ICT 기업의 제품 및 서비스의 수입을 거부하겠다는 것이다. 또한, 트럼프 대통령 외에 이미 존 볼턴 백악관 국가안보회의 보좌관은 2019년 1월 이스라엘 방문 당시 중국의 이동통신 장비에 대한 우려를 베냐민 네타냐후 이스라엘 총리에게 제기한 바

있다. 또한, 마이크 폼페오 미국 국무장관은 2월 11일 헝가리 방문 당시 미국은 동맹국에 화웨이 장비 사용의 위험성을 경고할 책임이 있고, 미국의 중요한 시스템이 있는 곳에 화웨이 장비가 설치돼 있다면 이들과 협력이 어려워질 수 있다고 경고했다.

화웨이 논쟁 일지(2011. 2 ~ 2019. 5)

2011.02	화웨이 제조 가정용공유기에서 보안리스크 발견 및 백도어 우려 제기
2012.10	미 하원, 화웨이 및 ZTE 안보위협 제기
2018.01	미 하원, 화웨이 및 ZTE 장비 사용 중단법안 발의
2018.08	트럼프 대통령, 화웨이 및 ZTE 장비 사용 금지 내용이 포함된 국방수권법 서명
2018.11	호주, 화웨이 및 ZTE 5G 구축사업에서 배제
2018.12	뉴질랜드, 화웨이 5G장비 사용금지 결정
2019.01	명 완저우 화웨이 부회장이 미국의 대이란 재제 위반으로 캐나다에서 체포 프랑스, 독일 등 유럽 주요 통신사에서 화웨이 등 중국 통신장비 사용금지 발표
2019.05	폴란드 당국, 스파이 혐의로 화웨이 중국인 직원 체포

(출처: 경향신문 2019.2.10. 및 필자 내용보충)

이처럼 강경한 미국과 달리, 냉전 시대부터 유지된 유럽과 아시아 동맹국들의 입장은 각양각색이다. 우선 화웨이 제품 배제의 입장에 선 국가로 호주(2018.8), 뉴질랜드(2018.11)는 자국 5G망에서 화웨이 장비 사용 배제를 확정했다. 트럼프 정부의 행정명령 발표 후, 수많은 세계 각국 기업이 화웨이와 거래 중단을 결정했으며, 컴퓨터 및 스마트폰 프로세서 설계 및 반도체기술 사용권 대여를 하는 영국의 ARM 또한 화웨이와 거래 중단을 결정했다고 BBC에서 보도했다. 애플, 삼성, 화웨이 스마트폰의 애플리케이션 프로세서뿐만 아니라 화웨이의 5G 통신네트워크 장비는 대다수 ARM의 설계에 기반한다는 점에서 사태가 장기화될 경우 화웨이가 어려움에 처할 것이라는 전망이 다수이다. 2019년 2월 17일 영국 정보통신 본부(GCHQ) 산하 국가사이버보안센터(NCSC)는 5G 네트워크에서 화웨이 장비의 보안리스크를 경감시키는 방안이 있다는 결론을 냈다고 영국 파이낸셜타임스가 보도했으며, 이는 화웨이 제품사용을 배제할 것을 촉구하는 미국과 정면 배치되는 것이다. 량 화(Liang Hua) 화웨이 순회 회장은 올해 5월 화웨이와 영국 정부는 화웨이 제품에 대한 보안 우려를 해소하고자 “스파이 금지협정” 체결을 고려하고 있다는 입장을 밝혔으며, 이는 화웨이 제품이 중국 정부가 활용할 수 있는 백도어가 설치되어 있을 것이라는 세간의 우려를 해소하기 위한 것으로 보인다. 영국과 더불어 독일 정부 역시 지난 2월 6일 5G 구축과정에서 특정 기업을 배제하지 않되, 모든 장비업체에 엄격한 보안규정을 적용하겠다는 입장을 표명했다. 요약하자면, 화웨이를 둘러싼 미국과 중국 간의 갈등은 2011년 보다폰 백도어 논쟁에서 출발해서 2018년부터 격화되어 2019년 5월 현재 미국 내 화웨이 제품 판매가 어려움에 처해 있다.

중국과 미국의 5G 및 인공지능 기술경쟁

우선 5G의 데이터 전송속도가 최대 20Gbps(초당 2.5GB)를 목표로 하고, 1Gbps가 최대치인 LTE보다

20배가 빠르다는 점에서 기존 3G, 4G는 비교 자체가 어렵다. 이는 기술혁신에 따른 더욱 편리한 서비스를 이용할 수 있다는 점과 더불어 누가 주도권을 장악할 것인가라는 물음을 제기한다. 현재 5G 네트워크 및 관련 장비 분야에서 화웨이는 1,481개의 기술특허를 보유하고 있으며, 이는 전체 5G 특허의 29%에 달한다. 또한, 세계 150여개 통신사에서 화웨이의 5G 장비를 시험 사용 중이며, 유럽(23개국), 중동(10개국), 아시아(6개국) 및 아프리카(1개국) 등 세계 40개국과 5G 장비도입 계약을 체결했다고 한다. 화웨이는 2009년부터 5G 연구에 나서 라우터, 통신탑 및 단말기 칩 기술을 보유하고 있고, 세계 최초로 3GB 상업용 5G 반도체 Balong 5G01을 개발한 바 있다. 또한, 화웨이는 5G NR 기술 분야에서 1,481건의 특허를 출원했으며, 5G 무선 주파수 밴드 인터페이스 제어 채널의 공식 코드인 폴라 코드(Polar Code) 분야 특허의 50%를 가지고 있다.

이미, 화웨이는 5G 서비스 및 스마트 의료분야에서 본격적인 서비스 추진을 준비하고 있다. 태국의 아시아 타임스(Asia Times)는 화웨이의 본사가 소재한 선전은 화웨이 및 ZTE의 5G 비즈니스 지원 차원에서 올해 3분기 이내에 7,000개의 5G 기지국 설치를 마무리할 예정이라고 보도했다. 또한, 광동성 인민병원 및 중국 이동통신과 2019년 3월 9일 5G 스마트 의료전략협력 협의서를 체결했으며, 병원 도착 전 5G 네트워크 기반 긴급네트워크 접속을 통해 환자 상태 확인 및 처치 준비를 하는 스마트 의료는 긴급 환자 처치에 큰 도움이 될 것이라고 발표했다.

5G 분야에서 화웨이를 제외한 네트워크 구축 및 장비 제조사로는 ZTE, 에릭슨, 노키아와 삼성을 들 수 있으며, 미국의 경우 현재 관련 기업이 없는 것으로 확인된다. 화웨이를 "5G 분야의 최강자이자 중국 기업"으로 규정한다면, 미국의 입장에서 화웨이의 세계적인 확장은 우려의 요인으로 볼 수 있다. 2019년 2월 워싱턴에서 나토 외무장관 회의 개최 시 6명의 전직 미국 장성들은 5G 네트워크가 기존 통신과 확연히 다르고 빠르다는 점을 강조하는 한편, 이 같은 5G 네트워크가 화웨이의 제품으로 구성 시 중국 정부 주도의 정보수집, 사이버 공격 또는 군사작전 목적으로 악용될 수 있다는 점을 지적했다.

화웨이 연구소 소재 및 제품판매 금지 현황



여기에서 “**확연히 다르고 빠르다**”는 점은 5G가 기존 통신기술과 차원이 다른 첨단기술임을 보여주는 대목이며, 5G를 중심으로 기존 경제, 사회 시스템이 재편되고, 고도의 보안이 요구되는 군사, 외교, 안보 네트워크 또한 영향을 받는 것은 매우 자연스러운 현상이다. 이런 5G 네트워크 구성에 신뢰하기 어려운 중국의 장비를 쓰는 것 자체가 우려하게 하는 것이며, 동일한 정치이념과 교류사가 있는 유럽, 한국 기업의 5G 장비에 관해서는 언급 자체가 없었고, 여기에 관한 논의도 없는 실정이다. 즉, 이들의 우려는 다름 아닌 “**중국**”이라는 “**신뢰하기 어려운 나라**”에 관한 것이다. 두 번째로, 패트릭 샐러핸 미국 국방부장관 대리는 화웨이의 5G 네트워크 구축이 중국 정부의 세계적 영향력 확산 측면에서 볼 수 있다고 지적했다. 샐러핸 장관 대리의 지적은 2008년 세계금융위기 이후 급격히 추락했던 서구 경제와 대비되게 고속성장과 힘의 세계적 투사를 추진하는 중국에 대한 미국 사회의 우려를 잘 반영한 것이다. 특히, 2013년 시진핑 국가주석 취임 이후 중국은 남중국해에 인공섬 조성 및 군사기지 설치를 강행해 베트남, 필리핀 등 주변국과 갈등을 빚고 있으며, 또한 일대일로 프로젝트를 통해 동남아 지역을 비롯해 중앙아시아, 유럽, 중동 지역까지 자국의 경제력을 확장하고자 하고 있다. 이 같은 중국의 영향력 확산이 5G 분야에서도 지속되고, 화웨이의 5G 장비가 미국의 영향력 내에 있는 지역 및 미국 본토로 유입되는 것 자체가 미국에게는 사실상 “**위협**”으로 볼 수밖에 없는 점이 있다.

또한 중국의 인공지능 진흥에 관해서는 1) 정부 주도의 진흥정책, 2) 기업의 자구노력, 3) 기반연구 강화로 정리할 수 있다. 우선, 중국의 2015년 5월 인터넷플러스 인공지능 3개년 추진계획방안과 2017년 7월 인공지능진흥 규획, 2018년 11월 차세대 인공지능산업혁신 중점추진업무 방안은 중국 정부의 체계적인 인공지능 진흥계획을 잘 보여준다. 상기 정책에 따르면, 중국은 2030년까지 지금의 인공지능 기초 및 산업기술을 세계적인 수준으로 도약시키는 것을 목표로 하며, 산업 규모를 100조 위안(한화 약 16,000조 원)으로 확장하고자 한다.

2017년 5월 27일 뉴욕타임스는 미국의 인공지능 연구예산이 감축되고 있고, 미국 및 유럽에서 학위를 마친 박사 또는 연구진들이 중국 대학으로 옮겨가고 있다고 지적했다. 중국은 중앙정부 뿐만 아니라 지방 정부도 중국 대학을 비롯해 관련 해외기업에도 투자하고 있으며, 일례로 중국 후난성 샹탄시는 소규모 도시임에도 불구하고, 로봇 및 인공지능 연구에 20억 달러를 투자할 예정이며, 장수성 쑤저우 시 경내의 유망한 인공지능 기업은 회사 설립 시 미화 80만 달러의 보조금을 받을 수 있다고 하며, 이는 중국 정부의 인공지능 분야에 대한 적극적인 정책지원과 투자를 보여주는 예시라고 하겠다.

두 번째로, 비단 중국 정부뿐만 아니라 중국 기업들 또한 빠르게 움직이고 있다. 중국 인공지능산업은 2015년을 기점으로 매년 30% 성장하고 있으며, 시장 규모는 2017년 기준 전년 대비 51.2% 성장한 152.1억 위안(한화 약 2.5조 원)에 달한다. 바이두, 알리바바, 텐센트 등이 ICT 대기업이 각각 커넥티드카, 스마트 물류, 게임 분야의 연구를 추진하고 있다. 우선, 커넥티드카 분야에서는 바이두가 앞서가고 있으며, 바이두는 2017 CES Asia에서 현대자동차와 함께 무인주행차량 기술개발에 합의했고, 바이두 측에서 바이두 맵오토(Baidu MapAuto), 음성인식 구동 서비스, 첨단 운전자지원시스템 등 무인주행차량 S/W 개발을 담당할 것을 합의했다. 또한, 바이두는 2017년 6월부터 포드, 다임러 벤츠, 인텔, 엔비디아 등 해

외 50개 기업과 자율주행차량 개발 프로젝트인 아풀로 프로젝트 구성에 합의 후, 2018년 4월 아풀로 차량 정보보안실험실을 창설했다. 2019년 1월 아풀로 무인주행차량은 홍콩-마카오-중국 광동성 주하이를 연결하는 강주아오 대교에서 시험 운행을 마쳤고, CES 2019에 무인 커넥티드카로 중국에서 라스베가스까지 상품 운송을 하며 상용화를 준비하고 있음을 과시한 바 있다.

이와 더불어, 스마트 의료 분야에서는 알리바바와 바이두가 이미 상용서비스를 시행하고 있다. 알리바바는 인공지능 기술을 접목해 서비스를 추진하고 있으며, 2017년 7월부터 실시되고 있는 알리바바 헬스사의 “닥터 유(Doctor You)” 진단 서비스는 CAT 스캔을 통해 염증 세포를 확인해 질병 유무 및 암 발병 여부를 확인해준다. 또한, 바이두는 2016년부터 AI 기술에 기반을 둔 채팅 로봇을 개발해서 환자와 이야기하고 의사에게 처방 제안을 제공하는 서비스를 시행하고 있다. 마지막으로, 물류 및 금융 분야에서는 알리바바가 선도하고 있으며, AI 관련 자회사로 앤트 금융서비스(Ant Financial Services, 판테크), 알리익스프레스(물류 배송)를 두고 있다. 알리바바는 지난 2015년 8월 AI 플랫폼 'DT PAI'를 출시했으며, 2016년 3월 소비자의 행동패턴을 사전 분석 및 예측하는 알리 샤오미(Ali Xiaomi)를 출시했다. 또한, 앤트 금융은 2017년 7월 초 AI 기반 이미지 인식시스템을 출시했으며, 이 시스템은 각기 다른 12개의 보험청구사례를 동시에 분석한다. 2017년 9월에 출시된 스마일 투 페이'라는 얼굴인식 결제 시스템은 고객이 단말기에서 메뉴 선택 후 전화번호 입력을 마친 후 기기 카메라를 보고 웃으면 결제가 완료되는 방식이다. 이처럼 중국의 5G 기술과 인공지능 기술은 상용화 단계로 접어들고 있다.

중국의 기술적 부상에 대한 미국의 우려가 최대 원인

정리하자면, 미국이 화웨이에 대한 우려와 긴급행정명령까지 발동하며 화웨이 제품의 미국 내 유입 및 사용을 차단하는 것은 비단 화웨이에 대한 우려만이 아니라 “중국의 기술적 부상”에 대한 우려에서 나온 조치이다. 향후 세계 경제 및 사회의 규칙을 바꿀 5G 및 인공지능 분야에서 중국은 정부의 적극적 정책과 기업의 자구적 노력으로 선도적 위치에 올랐으며, 특히 화웨이는 여기에서 핵심 기업이라고 평가할 수 있다. 화웨이가 세계 각지에서 5G 네트워크 구축 및 장비 공급을 하는 것은 미국의 시각에서 볼 때 새로운 질서가 만들어지고 있다고 볼 수 있고, 반면 미국이 주장하는 백도어 설이나 보안 우려를 뒷받침 할만한 충분한 실증 사례가 발견되지 않고 있다.

그러나, 중요한 것은 미국의 주장이 옳다, 그르다가 아니라 국제정치에서 패권국인 미국이 신흥 강국인 중국에 대해 조처를 취했다는 점이며, 특히 품페오 미국 국무장관이 언급했듯이 미국은 동맹국에서 화웨이 제품이 사용되는 것을 허용하지 않겠다는 점을 분명히 밝혔다는 것이다. 여기에서 하나 떠올려 볼 사례로는 단연 2017년 사드 사건이며, 당시 북핵에 대응하기 위해 도입된 사드에 대한 우리나라와 중국 간의 인식 차이와 더불어 충분치 않은 소통으로 중국 관광객 대폭 감소와 중국에서 사업을 영위하는 우리 기업인들이 유무형의 압박에 놓였었다. 당시 사드를 둘러싼 중국과 우리나라, 미국 간의 입장차는 매우 첨예했으나, 화웨이 논쟁과 비교 시 미국의 대 화웨이 압박은 더욱 거세고, 중국 또한 미국의

압박에 대해 근대 초기 서구 열강의 중국 침략에 비유할 만큼 격양되어 있다.

이런 상황에서 한쪽으로 입장을 선회할 경우에는 그 반대쪽으로부터 역풍은 자연히 불어오는 것이며, 이는 화웨이 이슈에서도 예외가 아니다. 오히려 금번 화웨이를 둘러싼 중미 갈등은 사드 이슈를 훨씬 능가하는 바, 먼저 세계 각국과 아시아 역내 국가들의 대응 상황을 신중히 모니터링할 필요가 있다. 두 번째로, 중국은 비단 경제 이슈뿐만 아니라 한반도 비핵화 및 평화체제 구축에서 미국과 더불어 반드시 협력해야 하는 파트너라는 점을 염두에 두고 정부, 기업 및 학계 등 다양한 분야에서 소통 채널을 구축해서 서로 간의 입장을 교환해서 우리가 취할 수 있는 최대한의 선의를 보이면서 중미 양국의 갈등 소재에서 벗어나야지, 여기에 자칫 얹매일 경우 분쟁의 씨앗으로 양측 모두에게 피해를 볼 수 있다.

[참고문헌]

- South China Morning Post, 4 April, 2019, MIT cuts funding ties with Huawei and ZTE citing US investigations.
-]VOA 코리아, 미 의회, 지출안 원칙적 합의...트럼프, 'AI 연구'행정명령 서명
- 중앙일보, 2019.2.18., 13억 인구 빅데이터가 무기... 중국 AI, 미국에 1.4년차 추격
- The New York Times, Ruchir Sharma , June 28, 2018 , The Coming Tech Battle With China
- 서울경제, 2019.2.18., 화웨이 손 들어준 英...'파이브 아이즈'에 금가나
- The Guardian, 14 May, 2019, Huawei' prepared to sign no-spy agreement with UK
- 大公報(香港), 2019.3.10., 攜手華為中移動 粵建5G應用醫院
- 이응용, Kisa Report, 2019.4, 글로벌 5G 도입 논쟁과 정보보호
- The Gear, 황승환, 2019.5.2., "공유기 백도어?" 화웨이 즉 기술적 실수, 이미 해결 해명
- South China Morning Post, 4 Apr, 2019, 'Grave concerns': US ex-military leaders warn that allies' use of Chinese 5G tech poses unacceptable risk
- Foreign Policy, Kara Frederick, May 3, 2019, The 5G future is not just about Huawei
- Asia Times, May 7, 2019, Shenzhen 5G stations plan to help Huawei, ZTE
- MIT Technology Review, Will Night, Feb 8, 2019, The real reason America is scared of Huawei: internet-connected everything
- The New York Times, 27 May, 2017, Is China Outsmarting America in A.I.?
- South China Morning Post, 15 Oct, 2017, Artificial intelligence use poised for rapid growth in Chinese hospitals
- 한국정보화진흥원, 2017.9, 중국의 인공지능(AI) 전략 : '차세대 인공지능 발전계획'을 중심으로
- 박성림, KISA Report, 2019.1, 중국 CES 2019 기업 동향

디즈니의 OTT 시장 진출, 눈여겨 볼 지점들

최홍규 (think.bc399@gmail.com)



- (現) EBS 미래교육연구소 연구위원
- (前) 한국인터넷진흥원 선임연구원
- 언론학 박사
- 저서 : 소셜 빅데이터 마이닝을 활용한 미디어 분석 방법(2017), 콘텐츠 큐레이션(2015), 방송의 진화(공저)(2018) 등

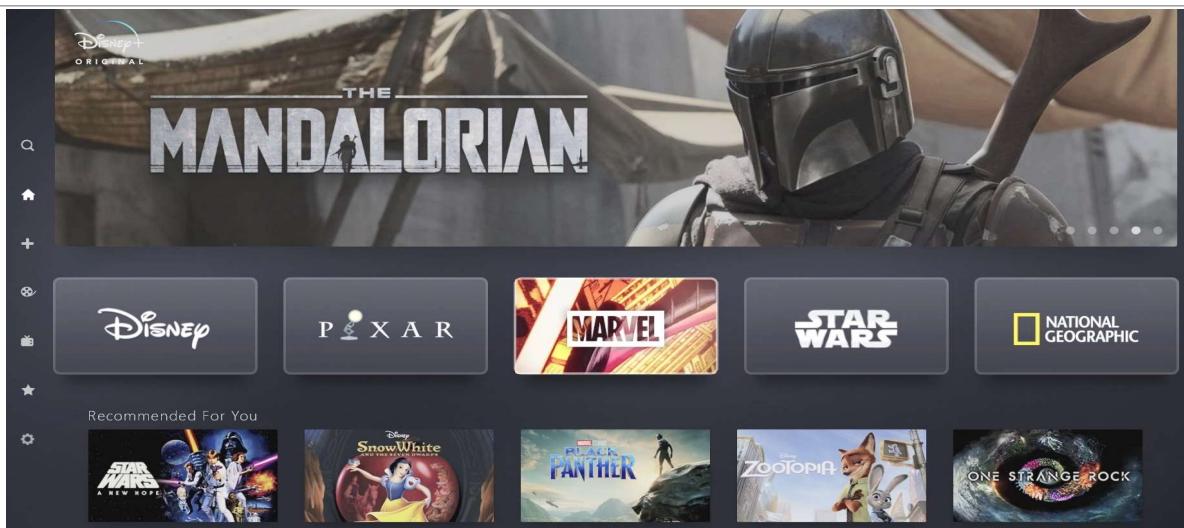
1923년 설립된 월트 디즈니 컴퍼니(The Walt Disney Company, 이하 디즈니)는 설립 100년을 앞둔 시점에서 새로운 미디어 산업으로의 진출을 선언한다. 2019년 11월부터 월정액 기반으로 소비자들에게 직접 콘텐츠를 제공하는 DTC(Direct-To-Consumer) 형 동영상 스트리밍 서비스를 게시한다는 것이다. 서비스 이름은 '디즈니+(Disney+)'라고 한다. 애플이 애플 TV+로 동영상 스트리밍 시장 진출을 선언하고 난 후 한 달도 채 지나지 않아 발표된 내용이라 시장의 관심이 뜨거웠다. 발표 시점은 11일 목요일이었는데, 이 발표 이후 하루 지난 12일 금요일에는 디즈니의 주가가 전날 대비 11% 이상 급등했다. 2009년 이후로 단 하루에 이만큼 주가가 오른 적이 없었으니, 디즈니에게 디즈니+는 최근 10년 동안에 가장 크게 시장의 주목을 끈 서비스라고 할 만하다.¹⁾

넷플릭스가 주도하는 소위 동영상 OTT(Over The Top) 스트리밍 시장을 디즈니의 진출로 어떻게 달라질 수 있을까? 영화를 좋아하는 사람이라면 확연히 달라진다고 느낄 것이다. 어벤져스, 스타워즈, 심슨가족 같은 시리즈물을 디즈니+에서만 볼 수 있다고 하면 태도를 바꿀 이용자는 많다. 게다가 가격도 넷플릭스보다 저렴하다면 얘기가 또 달라진다. 실제로 이번 발표에서 디즈니는 기존에 디즈니가 보유한 콘텐츠를 디즈니+에서만 공급할 방침이라고 못 박았다. 넷플릭스에 제공하던 기존 디즈니 콘텐츠도 다 끊고 디즈니+에만 공급하며 가격은 월 6.99달러(연간 69.99달러)로 저렴하게 제공하겠다고도 했다. 이용자 입장에서는 반가운 소식이 아닐 수 없다.

콘텐츠 라인업을 들어보면 이용자들의 구미가 더 당길 수밖에 없다. 마블 스튜디오(Marvel Studios, 이

하 마블), 월트 디즈니 애니메이션 스튜디오(Walt Disney Animation Studios), 픽사 애니메이션 스튜디오(Pixar Animation Studios, 이하 픽사), 내셔널 지오그래픽(National Geographic), 디즈니 TV 애니메이션(Disney Television Animation) 등 쟁쟁한 곳에서 제작한 영화 500편과 TV 시리즈를 7,500편을 제공해준다는 것은 참으로 구미가 당긴다. 대규모로 제작된 오리지널 콘텐츠도 선보일 예정인데, 예를 들면 스타워즈 시리즈에서 스핀 오프(spin-off)한 '더 만달로리안(The Mandalorian)'이 대표적이다. 이미 10여편의 시리즈가 만들어져 강력한 팬덤이 형성되어 있는 스타워즈 시리즈, 그 팬들의 입장에서도 이와 같은 콘텐츠 라인업은 열광할만한 것이다.

디즈니 보도자료를 통해 공개된 디즈니+(Disney+) 서비스 화면



(출처 : thewaltdisneycompany.com²⁾

이번 디즈니+가 제시한 콘텐츠나 서비스는 여타 동영상 OTT 서비스가 제공하거나 제공할 것으로 예측되는 서비스들과 별반 차이는 없다. 그러나 기존에 워낙 많은 영화나 TV 시리즈를 보유하고 있던 미디어사가 스트리밍 시장에 뛰어든다는 차원에서 몇 가지 눈여겨 볼만한 지점들이 발견된다.

디즈니+만의 머니 게임과 번들링 경제

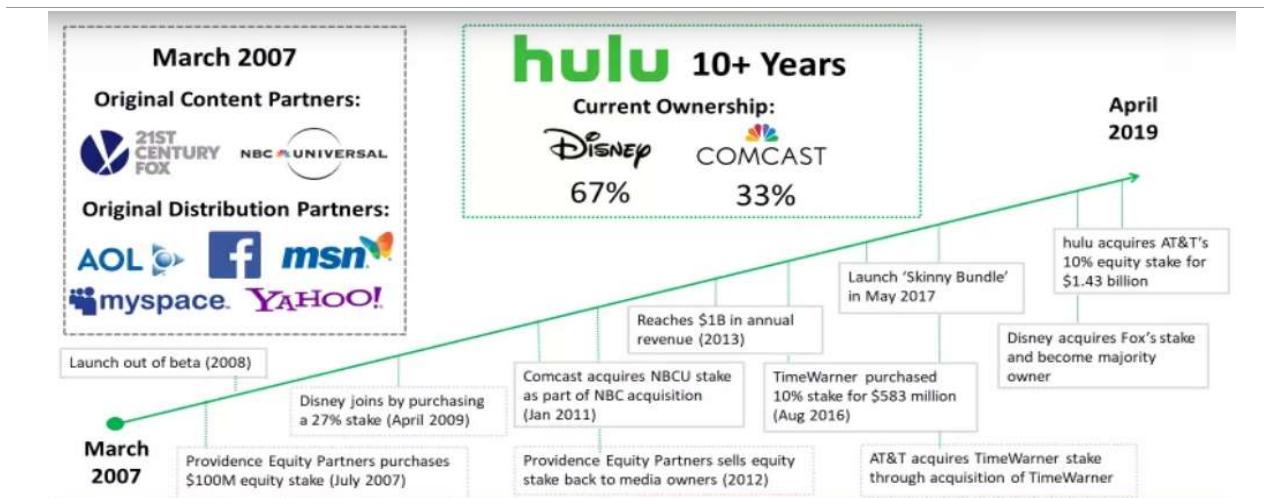
디즈니+는 갑자기 생겨난 서비스가 아니다. 그간 디즈니가 숱하게 진행해 온 미디어 서비스 기업에 대한 인수와 주식 보유 등이 축적된 결과다. 디즈니의 CEO인 로버트 아이거(Robert A. Iger)는 2005년에 임명되었는데 이듬해인 2006년에 픽사를 74억 달러에 인수한다. 3년 후인 2008년에는 마블을 42억 4천만 달러에 인수하고 다시 2012년에는 스타워즈를 만든 루카스필름(Lucasfilm)을 40억 5천만 달러에 인수한다. 다시 6년이 지난 2018년에는 21세기 폭스(21st Century Fox Inc.)를 인수하며 영화와 TV 부문의

라인업을 완성했다. 그런데 여기서 끝이 아니다. 디즈니+ 서비스 론칭을 위해 중요한 지분 인수가 2017년 여름에 있었는데, 바로 스트리밍 기술 사업자 벤테크(BAMTech)를 인수한 것이다. 이 회사는 2018년부터 ESPN+의 스트리밍 서비스를 운영하였으며 디즈니+의 스트리밍 서비스도 여기서 운영할 것으로 전해졌다.

디즈니 최고 경영자인 로버트 아이거의 이와 같은 인수 전략과 그로 인한 동영상 스트리밍 사업은 디즈니를 더 이상 오프라인 공간에 두지 않겠다는 의지로 해석된다. 미래의 영화와 TV 시청을 위한 공간은 온라인이라는 것이다. 한편으로는 구글, 넷플릭스, 아마존, 페이스북 등 온라인 동영상 영역에서 급성장하고 있는 ICT 기업에 대한 전통적인 미디어 그룹의 반격이기도 하다.³⁾ 기존 ICT 기업들이 온라인 네트워크 기술을 기반으로 콘텐츠를 취득하는 구조로 사업을 확장하는 방식을 취했다면, 디즈니는 이제껏 확보한 콘텐츠를 기반으로 팬덤을 굳히고 이를 통해 이용자 네트워크를 확대하는 방식을 구사하고 있다.

이 과정에서는 머니 게임(money game) 형태로 막대한 자금을 투입해 기업이나 지분 인수 방식을 취하기도 했다. 디즈니의 스트리밍 서비스 확대를 완성시킨 거래는 21세기 폭스사 인수로 여겨지는데, 이때 폭스의 인수를 통해 스트리밍 서비스인 훌루(hulu)의 지분 67%를 취득해 대주주의 위치에 올랐다. 이로써 디즈니는 디즈니+, 훌루, ESPN+ 등 동영상 스트리밍 서비스의 네트워크를 견고하게 꾸릴 수 있게 됐다. 디즈니의 자금력이 뒷받침되지 않았다면 취할 수 없었던 전략이다.

훌루(hulu)의 소유권 변화 양상



(출처: devoncroft.com⁴⁾)

디즈니가 21세기 폭스사를 사들이면서 훌루의 경영권을 확보한 것은 디즈니가 동영상 OTT 사업을 바라보는 관점을 잘 드러낸다. 디즈니에게 OTT 사업은 최대한 많은 소비자에게 많은 콘텐츠를 제공하는 일종의 번들링 경제(Economic of Bundling)가 작용하는 사업 영역이다.⁵⁾ 번들링 경제는 넷플릭스를 통해

이미 경험된 바 있는 사업 모델이다. 넷플릭스는 콘텐츠 하나하나를 개별 고객에게 제공하지 않으며 번들로 고객들에게 다양한 콘텐츠를 제공한다. 고객들은 번들의 가격을 통해 콘텐츠 가격을 평균화해 인식하기 때문에 판매자는 이러한 콘텐츠 평균 가격을 적절하게 책정해 고객들에게 번들 가격을 제시해야 한다. 이들 번들에는 품질이 확보된 콘텐츠가 적절히 포함되어 있어야 하며 번들 가격이 이 품질 높은 콘텐츠에 합당한다고 판단하는 고객들만 서비스 이용을 중단하지 않게 되는 원리다.

디즈니+도 마찬가지다. 현재 자사가 소유하고 있는 다수의 영화와 TV 프로그램을 제공하기로 했는데 이 콘텐츠들은 디즈니+, 헐루, ESPN+ 등에서만 공유될 수 있도록 했다. 번들의 가격은 월 6.99달러로 상대적으로 오리지널 콘텐츠 숫자가 많은 넷플릭스에 비해 적게 책정됐는데, 이렇게 가격이 책정된 이유는 이용 고객이 넷플릭스 콘텐츠의 평균 이용 대금을 더 높게 인식하기 때문으로 풀이된다. 디즈니+가 이제 넷플릭스와 마찬가지로 고객을 직접적으로 만나는 동영상 스트리밍 서비스를 채택한 이상, 폐쇄적인 콘텐츠 유통 시스템 안에서 자사 콘텐츠를 유통하겠다고 선언한 것과 마찬가지다.⁵⁾ 이는 디즈니+의 번들링 경제 효과를 자사 이용 고객들에게 각인시키고 향후에 점차적으로는 넷플릭스의 번들링 서비스 고객을 유입시키겠다는 전략이다.

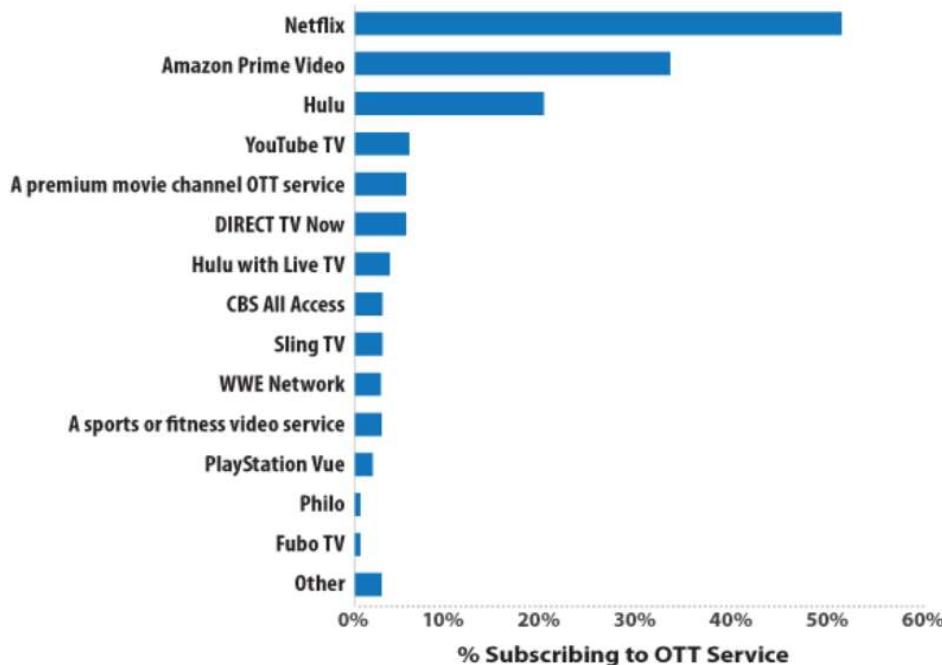
넷플릭스와의 정면승부

디즈니+가 종국에 이겨내야 하는 대상은 뻔하다. 넷플릭스다. 미국 인터넷 광대역망 가구의 91%는 빅3 OTT로 불리는 넷플릭스 (Netflix), 아마존 프라임 비디오 (Amazon Prime Video), 헐루 (Hulu) 중 하나의 OTT 서비스에 가입하고 있다.⁷⁾ 현재 헐루는 디즈니의 영향력 하에 있으니 결국 넷플릭스를 잡으면 시장에서 승기를 잡을 수 있게 된다. 또한 가격 면에서 디즈니+는 넷플릭스의 가장 저렴한 옵션(월 7.99달러), 아마존 프라임 서비스(연간 119달러), 헐루의 광고지원형 서비스(5.99달러)와 비교해도 가장 낮은 가격으로 승부를 펼칠 수 있게 되어서 초기에 고객들의 이목을 집중시킬 것으로 보인다.

사실 디즈니+ 서비스가 론칭되면 디즈니 계열의 사업자들과 서비스를 연계할 수 있기 때문에 시장에서는 위협적인 존재로 부각될 수밖에 없다. 아예 처음 시장에 진입하는 사업자가 아니라 계열사 사업자들의 서비스를 등에 업고 더욱 가입자를 늘려나갈 수 있는 전략이 가능한 것이다. 빅3 OTT 사업자 중에서 그 어떤 사업자도 처음부터 디즈니 애니메이션, 마블 시리즈, 픽사 애니메이션, 내셔널 지오그래픽 등의 콘텐츠를 완전히 확보한 채로 시장에 진입한 사업자는 없다.

디즈니+가 기존 사업자와 다른 이유가 여기에 있다. 요약하자면 디즈니+는 OTT 플랫폼으로는 헐루와 ESPN+와 제휴가 가능할 뿐만 아니라, 기존 미국의 안방 TV 프로그램 및 할리우드 유명 영화들을 모두 섭렵한 채로 시장 진입이 가능한 것이다. 생각해보자! 디즈니는 올해로 30번째 시즌을 맞이하는 “심슨가족(The Simpsons)” 시즌 30의 에피소드 전편을 디즈니+ 서비스 론칭과 함께 제공할 것이라 전했는데, 이만큼 매력적인 형태로 콘텐츠 제공을 시도했던 기존의 OTT 사업자들이 있었는가 말이다. 한마디로 디즈니의 동영상 OTT 사업은 기존 사업자들보다는 매우 좋은 조건으로 시작한다는 얘기다.

미국 OTT 서비스 가입 비율
(미국 내 인터넷 가입가구 조사, 2018년도 3분기)



(출처: parksassociates.com⁷)

이처럼 올해 하반기인 11월에 론칭할 디즈니+의 상황을 곱씹어 보면, 넷플릭스와 단순 비교하는 것이 어렵다. 그래도 한번 대략적인 내용을 비교해 보자면 이미 확보한, 혹은 향후 확보하여 제공할 오리지널 콘텐츠에서는 큰 차이가 있다. 넷플릭스의 오리지널 시리즈물은 대략 700편 이상에 달하지만 디즈니+는 25편 정도로 28배 정도 차이가 난다. 오리지널 영화도 마찬가지다. 넷플릭스는 200편인데 비해 디즈니는 10편에 불과하여 20배 정도의 차이가 난다.

즉 오리지널 콘텐츠에서 20~28배의 차이를 두고 넷플릭스와 디즈니+가 경쟁하는 것이다. 앞서 언급한 번들링 경제의 측면에서 오리지널 콘텐츠가 번들링 가격 책정의 요소라면 넷플릭스는 확실히 우월적 지위에 있다. 더 높은 번들링 가격을 매겨도 이용자 이탈률이 낮을 수 있기 때문이다. 이런 면에서는 디즈니+ 월정액은 초기 유인책으로 기능하지 못할 가능성도 있다.

콘텐츠 종류에서도 넷플릭스와 디즈니+는 차이를 보인다. 넷플릭스는 전 연령대에 제공 가능한 장르나 내용의 콘텐츠를 확보하고 있다. 반면 디즈니+의 콘텐츠는 유아·어린이, 가족 위주의 콘텐츠가 주를 이룬다. 여기서 고려해볼 만한 점은 디즈니+를 운영하는 디즈니 측면에서는 훌루나 ESPN+가 디즈니+에 머무르지 않는 연령대의 고객들을 대신 붙잡아둘 수 있다는 이점이 있다. 따라서 넷플릭스와 디즈니+의 콘텐츠 종류를 단순 비교하여 디즈니 그룹 전체의 OTT 사업을 평가하기에는 무리가 따른다.

동영상 OTT 서비스 비교(디즈니+ VS. 넷플릭스)

Category	<u>Disney</u>	<u>Netflix</u>
Price	\$6.99	\$12.99
Content	Family	Broad
Original Series	25+	700+
Original Movies	10+	200+
Launch	Nov-19	Jan-07

(출처: tdgresearch.com⁸)

결론적으로 말하면, 넷플릭스가 디즈니+에 비해 나은 점은 월등히 많은 분량의 오리지널 콘텐츠와 12년간 축적된 서비스 노하우, 1억 5천만 명에 육박하는 유료가입자라고 할 수 있다. 특히 동영상 OTT 서비스의 근간을 이루는 오리지널 콘텐츠는 당분간 디즈니+가 따라잡기 어려워 보인다. 그러나 디즈니+는 훌루와 ESPN+ 등 계열사의 OTT 서비스들과 협력이 용이하고, 기존에 강력한 팬덤을 형성하고 있는 콘텐츠를 이미 확보하고 있어 새로운 오리지널 콘텐츠의 흥행 성공 확률도 어느 정도는 확보하고 있다는 부분이 이점이다. 둘 중에서 승자는 뚜껑을 열어봐야 알고 시간이 지나 봐야 안다는 얘기다.

포화상태의 월정액 주문형 비디오(SVOD) 시장에서 살아남기

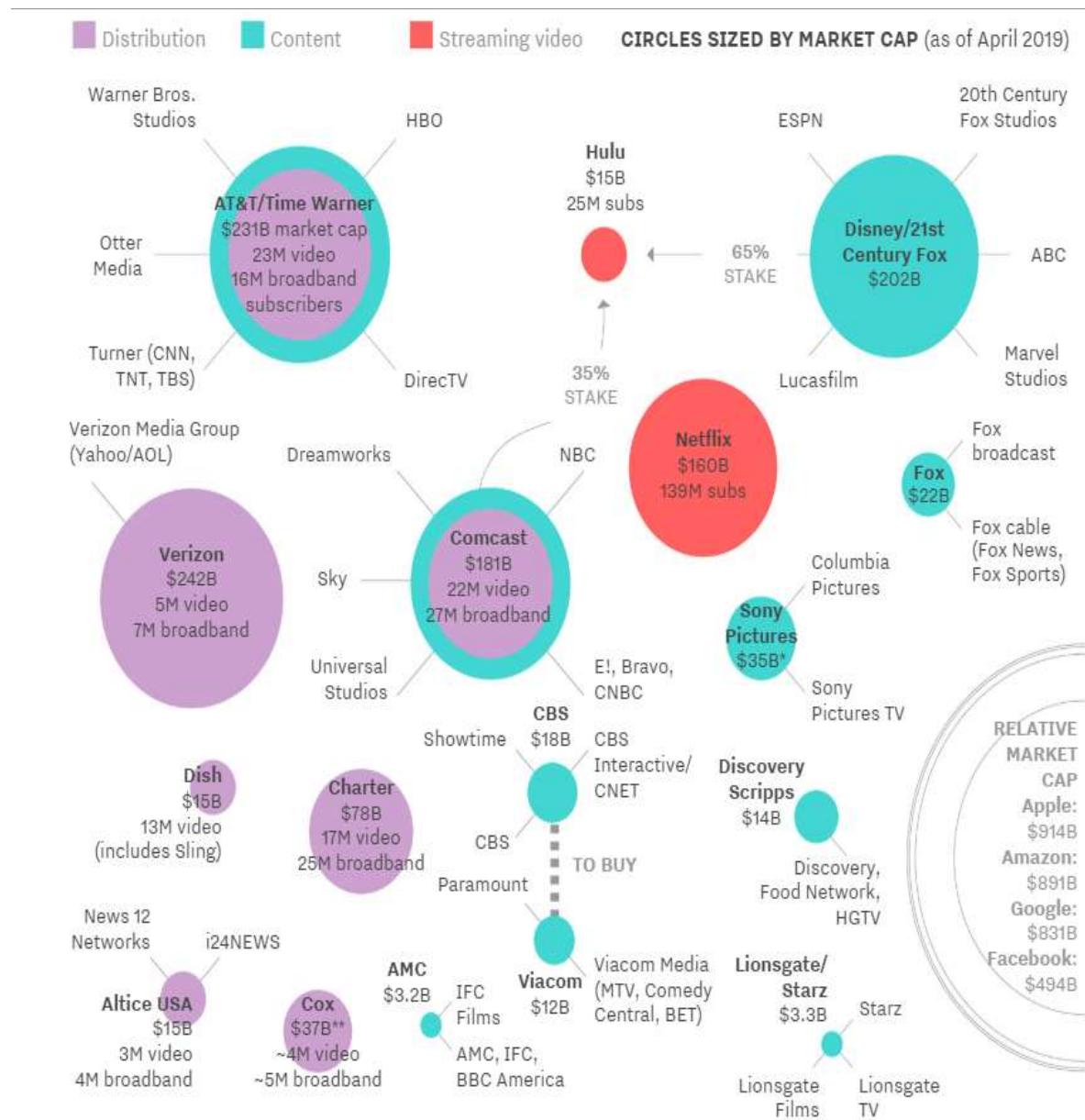
이번 디즈니+의 서비스 론칭 계획으로 2019년 하반기는 그야말로 미디어 시장의 전쟁터가 될 예정이다. 특히 디즈니에 앞서 서비스 계획을 발표한 애플TV+까지 가세하면 월정액 주문형 비디오(SVOD, Subscription Video On Demand) 시장은 무한경쟁 시장이자, 서비스 포화 상태로 가고 있다고 해도 과언이 아니다. 전체 가입자 수가 한정된 상황에서 서비스의 숫자가 늘어나는 상황으로 가고 있기 때문에 사업자 간 경쟁은 더욱 치열해질 수밖에 없다. 기본적으로는 월정액 가격, 오리지널 콘텐츠 제작, 인기 콘텐츠 확보 등에서의 경쟁은 불 보듯 뻔하다.

동영상 OTT 시장으로 한정하지 않고 콘텐츠 제작, 미디어 유통, 스트리밍 서비스 등으로 영역을 넓히면 더욱 복잡하다. AT&T와 타임워너(Time Warner) 계열사들이 콘텐츠 확보 기업으로는 가장 큰 규모의 시가총액을 기록하며 시장에서 영향력을 갖추고 있다. 2천3백10억 달러의 시가총액을 기록하고 있는 이 그룹사는 HBO, 워너브라더스 스튜디오(Warner Bros. Studios), CNN, TNT, TBS, DirecTV 등 라인업도 다양하다.

그런데 시가총액 2위 사업자는 디즈니와 21세기 폭스사 계열이라는 점을 주목해야 한다. 시가총액 2

전20억 달러를 기록하고 있는 이 그룹은 업계 2위를 기록하고 있다. 자금력에서 1위 사업자와 큰 차이를 보이지 않으면서도 대중에게 어필할 수 있는 많은 콘텐츠를 다수 확보하고 있다. 컴캐스트(Comcast)나 넷플릭스보다는 시가총액도 우위에 있다. 디즈니+가 론칭되면 이러한 산업 지형상 우위에 있는 기업으로서 가지게 되는 이점도 분명히 존재할 것이다.

콘텐츠 제작·미디어 유통·스트리밍 서비스의 지형(금액: 시가총액)



(출처: vox.com⁹)

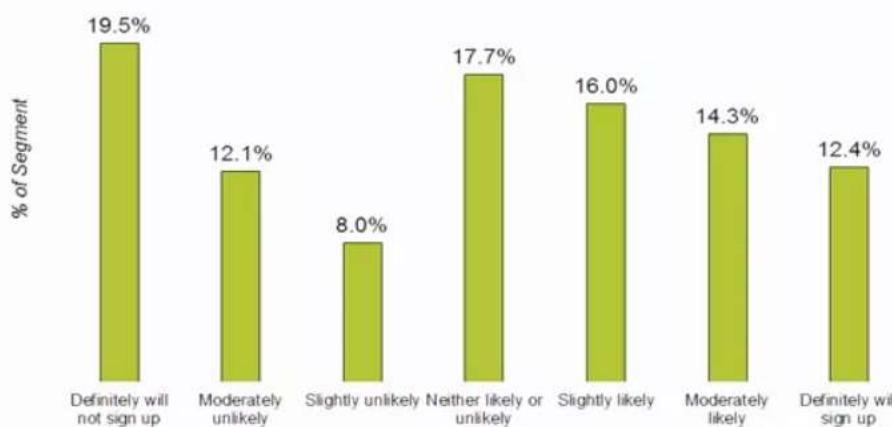
하지만 이러한 콘텐츠 제작, 미디어 유통, 스트리밍 서비스에 한정된 사업자들 외에 애플, 아마존, 구글, 페이스북 같은 ICT 사업자들을 더 주목해야 한다. 이들의 시가총액은 이미 기존 미디어 그룹사들의 시가총액을 훌쩍 뛰어넘는다. 규모 측면에서는 비교하기 힘들고 기존 사업자들과 유사한 동영상 스트리밍 서비스를 제공하고 있다. 언제든 유사한 서비스로 경쟁 대열에 들어설 수 있다.

디즈니+가 올해 11월 이후 유념해야 할 부분은 바로 이러한 포화상태의 시장에서 어떻게 살아남을 수 있는가이다. 단순히 기존 미디어 사업자들을 제압해서 사업적 성과를 거두기 어려운 실정에서 어떠한 전략을 통해 시장에서 성공을 거둘 것이냐는 점이다. 넷플릭스가 동영상 OTT 시장의 강자라서 넷플릭스와 경쟁이 가능해진다고 해도 애플도 구글도 아마존도 페이스북도 다 경쟁자로 부각할 것인데 이 상황을 디즈니가 어떻게 극복할 것이냐는 점이다. 결국 기존 콘텐츠들의 인기에 힘입어 시장을 조금씩 늘려나가야 할 것인데 이것은 예측이 불가하며, 한편으로 기업과 주식에 대한 인수 카드를 언제까지 쓸 수 있을지 미지수다.

이러한 상황에도 불구하고 최근 미국의 인터넷 가입 고객 1,949명을 대상으로 디즈니+ 서비스 가입 가능성에 관해 물어본 조사 결과는 다소 긍정적이다. 이용자의 43%는 다양한 가격으로 가입할 가능성이 높고, 27% 정도는 가입 가능성이 있거나 틀림없이 가입하는 정도의 수준으로 나타났다. 디즈니+에 대한 잠재적 이용자 군의 규모를 짐작할 수 있게 하는 결과다.

디즈니+ 서비스 가입 가능성에 관한 이용자 인식조사 결과

Prices randomly, evenly, and exclusively assigned, including \$5.99, \$7.99, and \$9.99/month)
 (among adult broadband users, n=1,949)



(출처: broadbandtvnews.com¹⁰⁾

디즈니+도 애플TV+와 마찬가지로 넷플릭스가 주도했던 동영상 OTT 사업 영역에 진입하는 서비스다. 시장의 평가는 갈리겠지만 디즈니는 2008년부터 2018년까지 10여 년간 매출이 거의 60%가 증가한 회사다. 2018년에는 순수한 마진만 21% 정도를 기록해 미디어 엔터테인먼트 분야에서는 매우 높은 수익

성을 보였다. 이러한 면모 때문에 디즈니는 애플과 함께 2019년 하반기 동영상 OTT 사업 영역의 판세를 바꿀 강력한 사업자로 여겨지는 것이다. 디즈니+는 애플TV+와 함께 시장의 지형을 바꿀 것이다. 이제 문제는 그 규모다.

[참고문헌]

- CNN(2019. 4. 12.). Disney's stock has its best day in nearly a decade.
<https://edition.cnn.com/2019/04/12/investing/disney-stock/index.html>
- The Walt Disney Company(2019. 4. 11). Disney Spotlights Comprehensive Direct-to-Consumer Strategy at 2019 Investor Day
<https://www.thewaltdisneycompany.com/disney-spotlights-comprehensive-direct-to-consumer-strategy-at-2019-investor-day>
- New York Times(2017. 12. 14.). Disney Makes \$52.4 Billion Deal for 21st Century Fox in Big Bet on Streaming
<https://www.nytimes.com/2017/12/14/business/dealbook/disney-fox-deal.html>
- Devoncroft(2019. 4. 17.). Analysis of Hulu's latest Valuation
<https://devoncroft.com/2019/04/17/analysis-of-hulus-latest-valuation>
- Havard Business Review(2019. 2. 25.). Netflix and the Economics of Bundling.
<https://hbr.org/2019/02/netflix-and-the-economics-of-bundling>
- DEG(2019. 1. 28.). Two Media Giants, Two Approaches to DTC
<https://www.degonline.org/nathanson-two-media-giants-two-approaches-to-dtc>
- Parks Perspectives(2019. 4. 15.). Disney+ Making Strong Case to Break into Big Three OTT Services.
<http://www.parksassociates.com/blog/article/disney--making-strong-case-to-break-into-big-three-ott-services>
- Tdg(2019. 4. 17.). A True Disruptor? Thoughts on Disney+.
<https://www.tdgresearch.com/a-true-disruptor-thoughts-on-disney>
- Recode(2019. 4. 3.). Here's who owns everything in Big Media today.
<https://www.vox.com/2018/1/23/16905844/media-landscape-verizon-amazon-comcast-disney-fox-relationships-chart>
- Broadband TV news(2019. 3. 15.). TDG: streaming OTT service Disney+ likely to be well received.
<https://www.broadbandtvnews.com/2019/03/15/tdg-streaming-ott-service-disney-likely-to-be-well-received>

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.2

이슈 & 트렌드

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

2019년 Vol.4

이슈 & 트렌드

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

2019년 Vol.1 CES 2019

이슈 & 트렌드

- CES 2019 주요 이슈 분석(서동우)
- CES 2019에 등장한 인공지능 기술과 제품 동향(한상기)
- CES 2019 자율주행 주요 동향(정구민)
- CES 2019가 보여준 '컴퓨팅의 현재와 미래'(이석원)
- CES2019, 다음 단계로 발걸음 옮긴 가상현실 헤드셋 기술(최필식)
- CES 2019 디스플레이의 변화, '화질에서 공간으로'(최호섭)
- 중국 CES 2019 기업 동향(박성림)
- CES 2019 전시회, '유레카'가 사라진, 그러나 꾸준히 발전하는 '유레카 존'(김태진)

2019년 Vol.3 MWC 2019 & RSA Conference 2019

이슈 & 트렌드

- MWC 2019에서 확인한 5G 시대, 모든 컴퓨팅 장치가 달라진다(최필식)
- MWC 2019, 상용화 준비 끝난 5세대 이통통신 생태계와 서비스(최호섭)
- MWC 2019, 서비스를 위한 스마트카의 다양한 진화(정구민)
- MWC 2019, 4YFN에서 살펴본 스타트업 기술 동향(이유환)
- MWC 2019 주요 이슈 분석(신민준)
- RSA Conference 2019를 통해 본 위협 그리고 인공지능과 자동화(정일욱)
- RSA Conference 2019& 인공지능 이슈(이용용)
- RSA Conference 2019에서 살펴본 클라우드 기반 보안 서비스 동향(윤승원)
- RSA Conference 2019에서 살펴보는 OT 보안 현황(유성민)
- RSA Conference 2019 주요 이슈 분석(오성택)



발 행 일 2019년 5월

발 행 행 한국인터넷진흥원

기획및편집 한국인터넷진흥원 미래정책연구실 미래정책팀

발 행 처 전라남도 나주시 진흥길 9

본지에 실린 내용은 필자의 개인적 견해이므로,

한국인터넷진흥원의 공식 견해와 다를 수 있습니다.

KISA Report의 내용은 무단 전재를 금하며, 기공/인용할 경우

반드시 [한국인터넷진흥원, KISA Report] 라고 출처를 밝혀주시기 바랍니다.