

2100호

2023.07.19.

ISSN 1225-6447

Weekly ICT Trends

주간기술동향



- 「주간기술동향」은 과학기술정보통신부 「ICT 동향분석 및 정책지원」 과제의 일환으로 정보통신기획평가원 (IITP)에서 발간하고 있습니다.
- 「주간기술동향」은 인터넷(<http://www.itfind.or.kr>)을 통해 서비스를 이용할 수 있으며, 본 고의 내용은 필자의 주관적인 의견으로 IITP의 공식적인 입장이 아님을 밝힙니다.
- 정보통신기획평가원의 「주간기술동향」 저작물은 공공누리 "출처표시-상업적 이용금지" 조건에 따라 이용할 수 있습니다. 즉, 공공누리의 제2유형에 따라 상업적 이용은 금지하나, "별도의 이용 허락"을 받은 경우에는 가능하오니 이용하실 때 공공누리 출처표시 지침을 참조하시기 바랍니다.
(<http://www.kogil.or.kr/info/license.do> 참고)

예시) "본 저작물은 '000(기관명)'에서 '00년' 작성하여 공공누리 제0유형으로 개방한 '저작물명(작성자:000)'을 이용하였으며, 해당 저작물은 '000(기관명), 000(홈페이지 주소)'에서 무료로 다운받으실 수 있습니다."



Weekly ICT Trends

주간기술동향

2100호

ISSN 1225-6447



기획시리즈:

차세대보안

OT/ICS 보안 이슈 및 기술 동향

이대성_부산가톨릭대학교 교수

- | | |
|--------------------------------|----|
| I. 서론 | 2 |
| II. OT/ICS 보안 개황 | 3 |
| III. 우크라이나 전쟁에서의 사이버전 동향 | 5 |
| IV. 독일 BSI의 OT/ICS 보안 동향 분석 | 7 |
| V. OT/ICS 보안 강화를 위한 NIST 표준 동향 | 9 |
| VI. 맺음말 | 13 |

ICT 신기술

심리상담 분야의 생성형 AI 도입에 관한 기술 동향

이장원_럽디(주) CTO

- | | |
|-------------------------------|----|
| I. 서론 | 15 |
| II. 심리상담에 대한 생성형 AI 진영의 주장 | 16 |
| III. 실제 심리상담/치료 산업 분야와의 괴리 | 17 |
| IV. 심리상담의 보조도구로는 생성 AI가 매우 유용 | 24 |
| V. 결론 | 26 |

ICT R&D

동향

양자 다이아몬드 자기장 현미경

오상원_한국표준과학연구원 책임연구원

- | | |
|--|----|
| | 27 |
|--|----|

단위 디지털트윈 연합을 위한 고신뢰 실시간 양방향 동기화 엔진 기술

송민환_한국전자기술연구원 책임연구원

- | | |
|--|----|
| | 31 |
|--|----|

Chapter

01

OT/ICS 보안 이슈 및 기술 동향

이대성_부산가톨릭대학교 교수

지난 3년 간 계속되었던 팬데믹의 영향으로 기업의 디지털 전환이 가속화되고, O2O 등 시민들의 생활이 플랫폼 의존적으로 변화됨에 따라 사이버 공간에서의 내외부 위협이 크게 증가하고 있다. 또한, 2022년 2월에 시작된 우크라이나의 전쟁에서 사이버전이 수반된 하이브리드 전쟁의 양상이 뚜렷해짐에 따라 주요 정보통신 기반 시설의 핵심 영역인 OT/ICS 보안이 기존 사이버 보안의 개념을 넘어서 국가 안보의 중요한 축으로 인식되고 있다. 본 고에서는 최근 OT/ICS 보안 영역에서 제기되고 있는 기술적 이슈와 동향을 분석하기 위해 지난 1년 간 우크라이나 전쟁에서 드러난 사이버전의 양상과 독일 BSI의 ICS 보안 동향 분석, 그리고 사이버 공간 보호와 관련된 미 NIST의 사이버보안 표준 정책 동향 등을 살펴봄으로써 향후 OT/ICS 보안의 발전 방향을 전망한다.

I. 서론

OT/ICS(Operational Technology/Industrial Control System)는 산업 생산 기반시설의 핵심 운용기술 영역이며, 4차 산업혁명이 급진전됨에 따라 AI 등 첨단기술과 융합된 이른바 「스마트 X」가 전 산업으로 확산되면서 사이버보안 전체에서 차지하는 비중이 더 커지고 있다. 본 고에서는 OT/ICS 보안 기술의 이슈를 팬데믹(pandemic)의 종식과 2022년 2월 러시아의 침공으로 시작된 우크라이나 전쟁에서 접근함으로써 주요 변화의 흐름을 파악하고자 한다.

첫째, 사이버보안 일반 동향으로, APT 공격의 빈도 및 강도 증대, IIoT, 소프트웨어 공급망에 대한 랜섬웨어 공격 확산, Log4j 등 오픈소스 프로그램 보안 취약점의 노출, 원격업무 솔루션, 메타버스 기기, 가상사설망(VPN)에 대한 취약점 공격 등이 지속적으로 늘어나면서

* 본 내용은 이대성 교수(☎ 051-510-0653, dslee@cup.ac.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

이에 대한 기술적 대응이 보안 이슈가 되고 있다.

둘째, 2020년 초에 발생한 코로나19는 국가 사회·경제 전반에 걸쳐 온라인 비대면 문화를 일상화시켰다. 이러한 현상은 기업들의 디지털 전환(DT/DX)을 더 앞당기는 계기가 되었으며, 시민들의 비대면 플랫폼 이용 증가로 공격자 입장에서는 사이버 공격 표면이 확장되어 자신들에게 크게 유리한 환경이 조성되었다고 볼 수 있다.

셋째, 2022년 2월에 시작된 우크라이나 전쟁에서는 물리적 군사행동과 사이버전(cyber warfare)이 동시에 전개됨으로써 전형적인 하이브리드전(hybrid warfare)의 양상을 보여주고 있다. 이번 하이브리드전에서는 전쟁 당사자 및 지원국들이 군(軍)은 물론 정부가 지원하는 민간 해커집단이 사이버전을 수행하고 있으며, 주요 공격 목표는 적대국의 산업 기반시설 운용 교란, 시스템 파괴, 심리전 등에 두어지고 있다.

이하에서는 국가 주요 기반시설들의 안정적인 보호와 급성장하고 있는 스마트 X 산업 발전에 필수적인 OT/ICS 보안 이슈와 기술 동향을 분석한다.

II. OT/ICS 보안 개황

미 NIST(National Institute of Standards and Technology)는 OT/ICS 네트워크를 구성하는 SCADA(Supervisory Control And Data Acquisition), DCS(Distributed Control Systems), PLC(Programmable Logic Controller) 등에 대한 사이버 공격 의도를 다음과 같이 정의하고 있다.

- ICS 네트워크에서 정보의 흐름을 차단하거나 지연시켜 ICS의 정상적인 운용을 방해
- 명령어나 경보 임계값을 무단으로 변경하여 장비를 손상 또는 정지시켜 시스템에 치명적 영향을 주거나 인명에 위협 초래
- 시스템 운영자에게 부정확한 정보를 전달하여 비인가 변경을 유도하거나 운영자의 부적절한 행동을 유발하여 다양한 부작용 유발
- ICS 소프트웨어나 형상을 변경하거나 ICS 소프트웨어를 악성코드에 감염시켜 다양한 부작용 유발
- 보안시스템의 정상적 운용을 방해하여 교체가 어려운 고가의 장비에 위협 유발
- 안전시스템의 정상 운용을 방해하여 인명에 위협 초래

이들에 대한 공격기법으로는 주요 정보통신 기반시설 자체가 분리망을 사용하기 때문에 USB 등 이동 저장매체를 사용하여 OT/ICS에 운용되는 소프트웨어나 장비에 스틱스넷(stuxnet)이나 트라이톤(triton)과 같은 전용 악성코드를 감염시키는 방법이 주로 사용되고 있다. 하지만 최근에는 클라우드, 액티브 디렉토리(active directory) 등의 IT 기술과 연동되면서 랜섬웨어나 원격 접속 프로그램 등 공개된 소프트웨어나 오픈소스를 활용한 공격 사례가 증가하고 있으며, 보안 경계 밖에 위치한 IoT 기기를 통해 ICS 망에 접근할 수 있는 액세스 점점이 늘어남으로써 사이버 공격 시도는 더욱 증가할 것으로 예상된다[6].

이 밖에 기반시설 OT/ICS에 대한 사이버 공격이 유발할 수 있는 피해 규모를 예측하여 국가 지원을 받는 해킹그룹들의 활동이 두드러지고 있다. 러시아 해커 조직 다크사이드(DarkSide)가 수행한 것으로 추정되는 미국 송유관 해킹 공격은 세계 경제에 막대한 영향을 끼쳤으며, 북한 해커 조직도 국내 기반 시설과 주요 인사들을 대상으로 사이버 공격을 수행하고 있다. 이러한 추세를 감안해 보면 앞으로 OT/ICS에 대한 보안 위협과 공격은 계속 증가할 것으로 전망된다[2]-[4].

OT/ICS 기술영역에서 가장 중요한 비중을 차지하고 있는 국내 주요 정보통신 기반시설에 대한 공격은 지난 20년(2003.1~2021.6) 간 꾸준히 증가하여 총 31건이 발생한 것으로 보고 되었으며, 산업 분야별로는 에너지 분야가 14건으로 전체 사고의 45%를 차지하고 있다. 에너지 분야 14건을 다시 세분화하면, 전력 7건, 원자력 4건, 에너지 3건이다.

해외에서도 2010년 이란 대규모 산업시설 제어시스템의 오작동을 유발한 스틱스넷을 시작으로 에너지 기반시설에 대한 조직적인 공격이 증가하였다. 2015년 블랙에너지(black energy), 2016년 크래쉬 오버라이드(crash override), 2017년 트라이톤, 2018년 TSMC (Taiwan Semiconductor Manufacturing Co.) 워너크라이 랜섬웨어, 2019년노르스크 하이드로 록커고(NorskHydro LockerGoga), 2021년 플로리다 수도인프라 공격 등이 지속적으로 보고되고 있다[1].

최근 10여 년간 국내외에서 발생한 OT/ICS 공격 사례는 [표 1]과 같다.

[표 1] 국내외 OT/ICS 공격 사례(2013~2021년)

시기	발생국	사고 내용	비고
2013.03.	한국	방송 및 금융 등 다수 기업 전산망에 악성코드로 인한 시스템 파괴 등 장애가 발생하여 PC 및 시스템 4만 8,000여 대 피해 발생	방송 금융

시기	발생국	사고 내용	비고
2014.01.	일본	후쿠이현 몬주 핵발전소 내 관리자 PC가 바이러스에 감염되어 교육·훈련 보고서, 조직변경 홍보 메일 등 사내 데이터 유출	원자력
2014.12.	독일	철강회사의 용광로 제어시스템에 장애 발생	철강
2015.12.	우크라이나	전력발전소에 악성코드 침투로 제어시스템 서비스가 중단되어 8만여 가구에 정전 발생	전력
2016.10.	미국	호스팅업체 Dyn사의 DNS 서비스가 디도스 공격으로 웹사이트 접속 장애 발생	통신
2017.06.	일본	혼다모터스 사야마 공장에 워너크라이 랜섬웨어가 유포되어 48시간 동안 생산 중단	일본
2018.01.	일본	가상화폐거래소 코인체크사가 해킹되어 580억 엔 피해 발생	금융
2018.05.	멕시코	은행 5곳이 해킹되어 1,540만 달러가 가짜계좌로 인출되는 사고 발생	금융
2018.11.	미국	HSBC은행 미국 지점에서 신원 미상의 해커가 고객의 온라인 계정에 불법 접근하여 일부 정보 유출	금융
2019.01.	미국	오클라호마 보안부에서 rsync 서비스를 통해 FBI 수사자료 등 유출	행정
2019.03.	미국	태양광·풍력 에너지 공급기업 에스파워가 시스코 방화벽 취약점으로 디도스 공격을 받아 발전설비 및 12개 회사와 연결 중단	에너지
2019.05.	미국	볼티모어에서 랜섬웨어 공격을 받아 파일이 암호화되는 피해 발생	행정
2019.07.	남아공	요하네스버그 전력공급사 시티파워를 대상으로 랜섬웨어 공격이 발생, 대부분 지역에서 정전사태가 발생하고 전기로 납세 행정처리 마비	전력
2020.09.	독일	신원 미상의 해커가 뒤셀도르프 대학병원 망에 랜섬웨어를 감염시켜 서비스 중단 및 중증환자 1명을 다른 병원으로 후송 도중 사망 사고 발생	병원
2020.10.	인도	뭄바이시가 사이버공격으로 송전시스템, 교통시스템, 열차 운행이 마비되었으며, 도시 운영에 꼭 필요한 시스템을 복구하는 데 2시간, 나머지 영역을 복구하는 데 12시간 이상 소요	전력
2020.12.	영국	스코틀랜드 지역 전력공급 업체 피플에너지사가 해킹 공격을 받아 27만 명의 개인정보 유출	전력
2021.02.	미국	플로리다주 올즈마시 상수도 공급 시설이 해커 공격에 노출되어 화학물질 농도가 급격히 높아졌으나 직원이 마우스 움직임을 감지한 후 차단	수자원
2021.05.	미국	송유관 업체 콜로니얼 파이프라인사가 랜섬웨어에 감염되어 며칠 동안 송유관 가동 중단	에너지
2021.05.	한국	한국원자력연구원을 대상으로 사이버공격 발생, 연구로 핵연료부를 포함한 직원 이메일, rods, 휴대전화 번호, 계정정보 등이 도난	원자력
2021.06.	오스트레일리아	세계 최대 육가공 업체 JBS푸드사가 랜섬웨어 공격을 받아 육류 가공 생산 차질	육가공

〈자료〉 국가정보원 외, 2022 국가정보보호백서, 2022. 5, pp.93-106. 재구성

III. 우크라이나 전쟁에서의 사이버전 동향

군사적 무력이 동원되는 전시 하의 사이버전에서는 군의 지휘 계통과 주요 기반시설 운영 마비 시도가 주요 공격 표적이 된다. 2022년 2월에 시작된 우크라이나 전쟁은 재래식 군사 작전과 함께 사이버전이 동시에 진행되는 하이브리드 전쟁 중에 있다. 특히, 이번 전쟁에서는 당사국의 사이버군 외에 각국을 지지하는 민간 해커집단들이 참여하고 있는 것이 특징이다[2],[7].

개전 전인 1월 덴버 국제공항에서 1월에 33시간 동안 간섭상황이 발생했으며, 글로벌 위성항법시스템(Global Navigation Satellite System: GNSS)에 신호 교란이 발생했다. 그리고 개전 전날에는 러시아가 우크라이나의 군사, 금융, 항공, IT 서비스 등 주요 기반시설에 대해 HermeticWiper로 시스템을 삭제하는 사이버 공격을 감행했고, 2월 27일에는 민간 전문가들이 포함된 우크라이나 IT군이 러시아 수십 개 조직에 사이버 공격을 가했다.

이 후 개전 1개월 동안 독일과 동유럽을 연결하는 ViaSat사의 위성통신 모뎀 1만 여대에 장애가 발생했으며,¹⁾ 독일 국내의 Enercon사 풍력 터빈 약 5,800대(총 최대 발전 능력: 11GW)가 원격 제어기능이 마비되어 위성모뎀을 1대씩 초기화/재설정하여 복구했다.

2월 28일에는 해커비스트 그룹 어나니머스가 우크라이나 침공에 반대하여 벨라루시 철도 회사의 내부망에 침입하여 러시아군의 철도 이동을 저지했다고 발표했는데, 벨라루스 철도 회사는 수동 모드로 운영을 전환하여 기차운행이 지연되었던 것으로 보인다. 이 밖에도 친 러시아, 친 우크라이나 양측의 해커비스트들이 DoS 공격으로 웹 사이트를 다운시키는 등 서로 사이버 공격을 감행했다.

2022년 1월부터 2023년 3월 사이에 러시아와 우크라이나 간의 사이버전에는 91개 조직이 관여되었고, 1,537건의 사이버 사고가 있었던 것으로 분석된다. 이번 사이버전의 주요 공격 표적은 [표 2]와 같이 일부 심리전을 제외하고는 대부분 주요 기반 시설에 대한 사이버 공격이었음을 알 수 있다[7].

1) VPN 설정을 악용하여 네트워크 관리 인터페이스에 침입한 뒤 설정을 지우는 악성코드(AcidRain)를 위성 모뎀에 이식하였는데, 이는 우크라이나 국내 통신을 혼란시키려고 한 것으로 추정

[표 2] 우크라이나 전쟁에서의 사이버전 현황

피해국가	총피해 건수	공격주체	주요 표적
우크라이나	360건	- 피플스 사이버아미(99) - NoName057(16)(40) - 어나니머스 러시아(26) - 샌드웜(19) 및 DEV-0586(12)	- 행정(81) - 금융(43) - 미디어(34) - ICT(33) - 교통(18) 및 에너지(18)
러시아	241건	- 우크라이나 육군(59) - 어나니머스(49) - 어나니머스 이탈리아(37)	- 금융(42) - 행정(39) - 미디어(25) - ICT(21) - 에너지(18)
기타 국가	936건	- NoName057(16)(431) - 어나니머스 러시아(100) 및 킬넷(88)	- 주요 표적 분야 * 행정(284) * 교통(161) * 금융(93) - 주요 표적국가 * 폴란드(173) * 라트비아(92) * 미국(83)

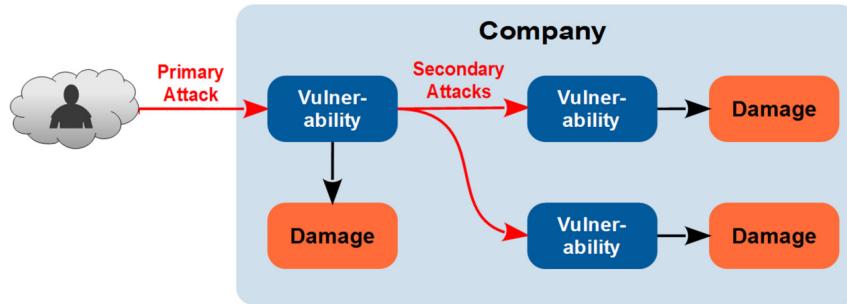
〈자료〉 Cyber Peace Institute, Cyber Dimensions of the Armed Conflict in Ukraine, Q1 Analysis Report, 2023. 3, pp.3-14.

IV. 독일 BSI의 OT/ICS 보안 동향 분석

독일의 정보기술보안청(Bundesamt für Sicherheit in der Informationstechnik: BSI)²⁾은 2016년부터 OT/ICS 보안 중심의 동향 보고서를 발표하고 있는데, 이 보고서의 동향분석 방법론은 사이버보안 훈련 프로그램 설계 시에 매우 유용한 시사점을 주고 있다.

이 분석 보고서는 세 개의 파트로 구성되는데, 첫째는 보안 위협 사례별로 위협의 원인 제시, 취약점이나 위협상황이 존재하는 결정적인 요인을 설명하고, 둘째는 공격실행의 구체적인 가능성을 설명하여 위협의 범위를 추정하도록 한다는 점에서 가상 위협 시나리오를 설정하는데 유용하다. 셋째는 위협사례별 보안대책으로 위협 대응과 미해결 리스크의 최소화를 위한 대안을 제시함으로써 사이버 보안 위협의 대응 방향을 설정하는데 의미있는 데이터를 제공하고 있다.

2) BSI는 미국 NSA(National Security Agency), 영국 CESG(Communications-Electronic Security Group)에 해당



[자료] BSI, Industrial Control System Security: Top 10 threats and countermeasures, 2022, 3, pp.1~20.

[그림 1] BSI의 사이버 공격과 피해 측정 연관도

또한, BSI는 [그림 1]과 같이 사이버 공격을 최초 공격(primary attack)과 후속 공격(secondary attack)으로 구분하고 이에 따른 피해 발생을 측정하고 있는데, 후속 공격의 특징과 보안대책을 다음과 같이 제시하고 있다.

- 권한 상승을 위한 인증 정보를 수집하기 위해 OS, 응용 서버, DB 등 표준 IT 컴포넌트의 버그나 취약점을 공격
- 내부 시스템 침입에 성공하면 업무망이나 제어망의 취약한 인증/인가체계를 탐색하여 지속 공격
- Field Bus 통신 조작: 대부분의 제어기기는 일반적으로 비보안 텍스트 프로토콜을 채택하고 있기 때문에 제어 명령어 조작이 용이
- 공격자는 보안체계를 무력화하거나 데이터 트래픽의 경로를 재설정하기 위해 라우터나 방화벽 등 네트워크 기기를 불법 조작
- 랜섬웨어 감염에 대비하여 반드시 백업체계 구축

한편, 사이버 공격에 의한 피해 발생은 생산시설에 물리적 손실 발생, 안전 절차나 시스템 조작, 인적/물적 손해 발생, ICS 가용성의 전체 혹은 부분적 파괴에 의한 생산 손실 발생, 데이터 유출로 인한 노하우(지적재산권 등) 유출 발생, 시스템이나 파라미터 조작에 의한 기기 성능의 저하로 측정하고 있다.

2022년에 발표된 10대 보안위협 사례 순위는 [표 3]과 같다. 보안위협 1순위인 이동식 저장매체나 모바일 기기를 통한 악성코드 감염은 기반시설이 폐쇄망이라 할지라도 언제라도 악성코드에 의해 감염될 수 있다는 것을 보여 준다. 2위 인터넷이나 인트라넷을 경유한 악성

코드 감염, 4위 외부망 및 클라우드 컴포넌트 공격, 7위 인터넷에 접속된 제어기기, 8위 원격 유지보수를 이용한 내부시스템 침입은 외부에서 네트워크를 경유하여 침입하는 경우로, 기반 시설의 IoT화, 부품의 디지털화 등으로 인해 매년 사이버 공격 위협이 증가할 것으로 전망된다[8].

[표 3] 2022년 OT/ICS 보안 10대 위협

구분	10대 위협	2019년 이후 추세
1	이동식 저장 매체 및 모바일 기기를 경유한 악성코드 감염	→
2	인터넷 및 외부망을 경유한 악성코드 감염	↑
3	직원 실수(human error) 및 방해 행위(sabotage)	→
4	외부망 및 클라우드 컴포넌트 공격	↗
5	사회공학적(social engineering) 공격과 피싱	→
6	DoS/DDoS 공격	→
7	인터넷에 접속된 제어기기 공격	↗
8	원격 유지보수를 이용한 침입	↗
9	기술적 장애나 불가항력적 사고(force majeure)	→
10	공급망 내 SW/HW 취약점 공격	↑

〈자료〉 BSI, Industrial Control System Security: Top 10 threats and countermeasures, 2022, 3, pp.1-20.

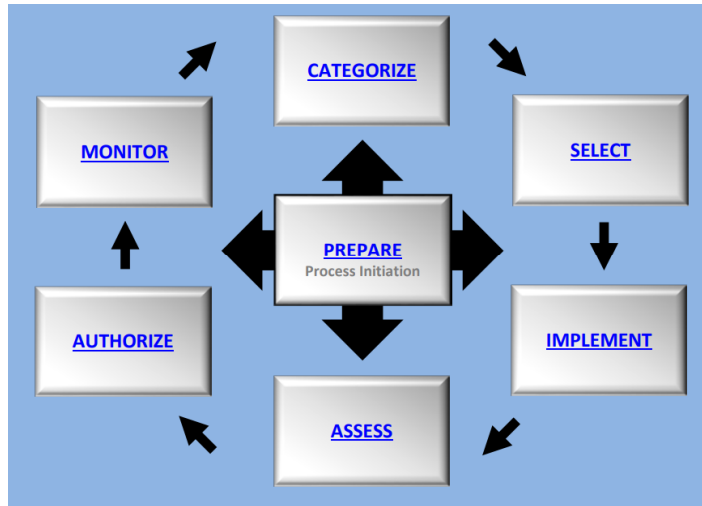
V. OT/ICS 보안 강화를 위한 NIST 표준 동향

1. NIST 위험관리체계(RMF)

RMF(Risk Management Framework)는 미 국방부가 2007년부터 적용해오던 DIACAP (DoD Information Assurance Certification and Accreditation Process)을 대체하기 위한 차세대 사이버보안 프레임워크이며, 사이버보안 대책을 체계적으로 수립, 구현, 평가, 관리하기 위한 활동이다.

NIST가 제시하는 RMF는 6개의 위험 프로세스에 1개 준비 프로세스가 연계되는 체계로 구성되어 있다([그림 2] 참조).

1단계(prepare)는 준비로서 조직의 위험관리 전략을 수립하고 조직전체의 위험평가를 실



〈자료〉 NIST, Risk Management Framework for Information Systems and Organizations, SP 800-37 Rev.2, 2018. 12, pp.6-22.

[그림 2] NIST RMF의 7단계 프로세스

시하여 여러 개의 시스템을 공통 지원할 수 있는 보안대책을 개발하고, 보호 대상 시스템 간의 경계를 명확히 하여 위험 관리의 우선 순위를 설정하는 등 조직 수준 및 시스템 수준 관점에서 RMF를 실행할 준비를 한다.

2단계(categorize)는 시스템 분류로서 CNSSI 1253, NIST SP 800-60과 관련한다. 이 단계에서는 체계에 요구되는 기밀성, 무결성, 가용성의 수준을 상, 중, 하로 결정한다. 보안 분류, 시스템 설명, 시스템 등록으로 구성되며, RMF 담당자를 지정한다.

3단계(select)는 보안 통제항목의 선정으로 CNSSI 1253, NIST SP 800-53과 관련한다. 이 단계에서는 보안 통제항목을 식별하고 보안 계획에 통제 항목을 선택하며, 공통 통제항목 식별과 보안 통제항목 선정, 모니터링 전략, 보안계획(SP) 승인으로 구성되어 있다. 단, 공통 보안통제항목이 부족하거나 과다한 경우에는 오버레이 적용을 통해 조정 가능하다.

4단계(implement)는 보안통제항목 구현으로서 NIST SP 800-30과 관련한다. 이 단계에서는 사이버보안 아키텍처에 따른 보안통제 솔루션을 구현하며, 보안 계획에 보안통제항목을 구현할 수 있도록 문서화한다.

5단계(assess)는 보안통제 평가로서 NIST SP 800-53A와 관련된다. 이 단계에서는 보안 통제평가자(SCA)와 보안평가계획(SAP)을 승인책임자(AO)가 승인을 위해 평가가 진행되며,

보안계획(SP), 보안평가보고서(SAR), 조치일정계획(POA&M)을 준비하되, 보안통제 평가자(SCA)는 보안평가계획서(SAP)를 작성하고 초기 개선조치를 수행한다.

6단계(authorize)는 RMF 체계 인가로서, NIST SP 800-39와 관련한다. 이 단계에서는 추진일정계획(POA&M)을 준비하고, SP, SAR, POA&M을 승인책임자(AO)에게 제출한다. AO는 운용승인, 임시시험승인, 운용승인거부 중에서 하나를 결정한다.

7단계(monitor)는 지속 감시로서 NIST SP 800-137과 관련한다. 이 단계에서는 시행중인 보안통제항목의 연간 평가, 개선조치사항 식별, SP/SAR/PO&M 갱신, 보안상태 보고 등의 활동을 수행한다.

또한, RMF는 시스템 개발 라이프사이클(SDLC)과 연계되어 있다. SDLC는 SP 800-64 Rev.2(정보 시스템 개발 수명 주기의 보안 고려 사항)에 표시된 수명 주기로 정의되며 시작 → 개발 및 조달 → 구현 및 평가 → 운영 및 유지 관리 → 사용 중단의 5단계로 구성된다. 새로운 시스템은 SDLC의 시작 → 구현 및 평가 → RMF 위험 관리의 준비 → 정보 시스템의 운영 승인의 프로세스를 적용한다.

운영 및 유지보수가 시작되면 보안관계 조치를 모니터링하지만, 그 이후에는 기존 시스템이 되고, 시스템 변경 등의 이벤트가 발생하면 처음부터 RMF를 실행한다. RMF의 첫 번째 단계인 위험관리 준비는 시스템을 대상으로 SDLC 시작 단계부터 실행한다. 조직 수준의 준비는 SDLC 실행 전에 조직이 수행해야 할 사항을 준비하는 것이다[9].

2. NIST 사이버보안체계(CSF)

주요 기반시설들은 IP 환경을 운영하고 있고, 인터넷을 사용하는 업무망과 연결된 지점도 존재하며, 무선망의 연결도 증가하면서 시설 보안의 난이도가 높아지고 있다. 오래된 설비가 많아 안티바이러스를 적용하거나 제어나 분석을 수행할 수도 없는 환경을 운영하고 있다. 또한, 설비 제조사들마다 전용 산업 프로토콜을 사용하고 있어 형상 관리는 물론 전체 설비나 제어 네트워크에 대한 모니터링이나 보안 취약점 점검에도 많은 어려움이 있다.

따라서 일단은 핵심 자산 분석을 통해 보호할 자산을 식별하여 리스크를 분석하고 그에 따른 보호대책을 수립해야 한다. 계측, 전기, ICT, 방재 등에 사용되는 장비를 식별하고, 이를 대상으로 지속적인 가시성을 확보해 비정상·이상징후를 탐지해야 한다. 또한, 사고가 발생하더라도 원인 파악이 가능한 환경을 운영하고, 대응과 복구방안도 수립해야 한다. 결과

적으로 식별 → 보호 → 탐지 → 대응 → 복구로 이어지는 사이버보안체계가 마련되는 셈이다([그림 3] 참조).

이를 위해 NIST는 2014년에 사이버보안 프레임워크(Cyber Security Framework: CSF) 버전 1을 공표하였으며, 2018년 4월에는 버전 1.1을 발표하였는데, 이 버전에는 자체평가 개선방안(The changes include guidance on how to perform self-assessments), 공급망 위험관리 추가사항(additional detail on supply chain risk management), 공급망 관계사와의 접촉규칙(guidance on how to interact with supply chain stakeholders), 취약점 공개 절차(vulnerability disclosure process) 등이 추가되었다[10],[11].



〈자료〉 NIST, Cybersecurity Framework Version 1.1, 2018. 4. pp.3-6.

[그림 3] NIST의 사이버보안체계 5단계 활동 프로세스

3. NIST 사이버보안 통제체계

NIST 800-53은 미국 정부기관이 사용하는 정보시스템에 대한 보안 통제항목³⁾을 구체화하고 이를 지정하기 위한 지침이다. 각 기관은 FIPS(Federal Information Processing Standard) 200⁴⁾을 기반으로 각 기관의 정보시스템 등급을 구분하고, 등급에 따른 보안통제 항목은 FIPS 200을 준수하기 위해 발행된 NIST SP 800-53을 참고하여 수립하게 된다. FIPS 200에서는 “이 표준에서 지정된 최소한의 보안 요구사항은 최신 버전의 NIST SP 800-53에 설명된 보안통제를 구현할 것”을 명시하고 있다.

NIST SP 800-53의 최초 버전은 2006년 12월 발행되었으나, 4차례의 개정을 거쳐 2020년 9월에 Rev.5가 발행되었다. Rev.5에서는 범용 컴퓨터 시스템, 사이버 물리시스템(CPS), 클라우드, 모바일 시스템, 제어시스템(ICS) 및 사물인터넷(IoT) 보호가 강조되었으며, ISO/IEC

3) 여기서 보안 통제항목이라 함은 정보시스템 및 그 정보의 기밀성, 무결성, 가용성을 보장하기 위해 해당 정보시스템에 설치되거나 운영되는 기술적, 관리적, 운영적 보안대책을 의미한다.

4) 2006년 3월에 발행된 FIPS(Federal Information Processing Standard) 200은 미 상무성 장관이 연방표준으로 승인한 문서로, 17개 보안 통제 분야에 대한 최소한의 보안 요구사항을 지정하고 있다.

27001 표준이나 사이버보안 프레임워크(CSF) 가이드라인과도 연관성을 갖고 있다.

통제사항은 크게 두 가지로 구분된다. 개인정보보호와 관련해서는 권한 및 목표, 데이터 품질 및 완전성, 개인 참여 및 개인 구제, 투명성, 책임·감사 및 위험관리, 데이터 최소화 및 보존, 안전 사용 제한의 8개 보안통제 분야를 다룬다. 기술적 통제에서는 모바일 컴퓨팅, 클라우드 컴퓨팅, 애플리케이션 보안, 신뢰성, 보안보증, 정보시스템의 리질리언스, 내부자 위협, 공급망 보안, APT 공격 등 9개 통제 분야를 다루고 있다. NIST SP 800-171은 민간기업이나 조직에 적용되고, NIST SP 800-53은 연방정부 정부에 적용되므로 두 표준은 긴밀한 관계에 있다. 따라서 어느 쪽 보안담당자이든 이 두 가지 표준을 모두 이해할 필요가 있다.

NIST SP 800-53(2020)은 20개 보안 통제 분야, 321개 통제항목으로 구성되어 있다. 또 867개 세부 통제항목을 제시하여 각 조직의 특성에 적합한 세부 보안 통제항목으로 적용할 수 있도록 하였다[12].

VI. 맺음말

OT/ICS 보안의 핵심영역인 국내 주요 정보통신 기반 시설은 2012년 186개에서 2021년 424개로 지속적으로 증가하고 있다. 이 중 공공 분야는 277개, 민간 분야는 147개가 정보통신기반보호법에 의해 주요 정보통신 기반시설로 지정되어 있으며, 향후 「스마트 X」 산업의 활성화로 민간의 비중이 증가할 것으로 예상된다.

본 고에서는 국가 산업경제의 핵심시설인 OT/ICS 보안과 관련된 사이버 공격의 유형을 우선순위별로 살펴 보았고, 우크라이나 전쟁에서 발생하고 있는 OT/ICS의 공격대상이 행정, 에너지, 교통, 금융에 집중되고 있음을 확인하였다.

또한, 급증하는 OT/ICS 보안 위협에 대처하기 위해서는 OT/ICS 운용기관들의 사이버 보안사고 대응체계를 강화해야 하며, 이에 필요한 동향으로 글로벌 사이버보안 표준을 주도하는 미국 NIST의 위험관리체계(RMF/SP 800-37), 사이버보안체계(CSF), 연방정부 사이버보안 통제체계(SP 800-53) 등 현재 제개정이 이루어지고 있는 사이버 보안 표준 동향을 소개하였다.

본 고에서 다룬 OT/ICS 보안기술 동향이 해당 분야 사이버보안 담당자들의 사이버 복원

력(cyber resilience) 중심의 사고대응 대책 개선방향 수립에 도움이 되기를 기대한다.

● 참고문헌

- [1] 국가정보원 외, 2022 국가정보보호백서, 2022. 5, pp.93-106.
- [2] 이글루시큐리티, 우크라이나 러시아 전쟁으로 보는 사이버전 동향 및 대응방안, 2022. 5.
- [3] KISA, 러시아-우크라이나 하이브리드 전쟁, 또 하나의 전쟁터가 된 사이버 공간, 사이버 위협 동향 보고서, 2022. 12, pp.8-11.
- [4] 안랩, 2023년 5대 사이버 보안 위협 전망, 2023. 1.
- [5] 이대성, 팬데믹 시대의 사이버 보안 기술 및 표준화 동향, KIST 융합연구리뷰, 2022. 11, pp.10-14.
- [6] NIST, Guide to Industrial Control Systems Security, SP 800-82 Rev.2, 2015. 5, pp.2-1.
- [7] Cyber Peace Institute, Cyber Dimensions of the Armed Conflict in Ukraine, Q1 Analysis Report, 2023. 3, pp.3-14.
- [8] BSI, Industrial Control System Security: Top 10 threats and countermeasures, 2022, 3, pp.1-20.
- [9] NIST, Risk Management Framework for Information Systems and Organizations, SP 800-37 Rev.2, 2018. 12, pp.6-22.
- [10] NIST, Cybersecurity Framework Version 1.1, pp.3-6.
- [11] NIST, Discussion Draft of the NIST Cybersecurity Framework 2.0 Core, 2023. 4, pp.1-5.
- [12] NIST, SP 800-53 Rev.53, Security and Privacy Controls for Information Systems and Organizations, 2020. 9, pp.1-15.

Chapter
02심리상담 분야의 생성형 AI 도입에
관한 기술 동향

이장원_럽디(주) CTO

I. 서론

ChatGPT와 심리상담에 대해 검색해보면, “우리는 ChatGPT로 심리상담을 가능하게 했다”라는 주장들이 많다. 미국 온라인 정신건강 서비스인 코코(KOKO)의 공동창업자 로버트 모리스는 “GPT를 사용하여 약 4,000명에게 정신건강 지원을 제공했다”[1]라고 주장하고 있으며, 이런 내용들을 통해 “ChatGPT로 심리상담 분야를 대체했다(혹은 곧 대체 가능하다)”라는 주장들이 퍼지고 있다.

이러한 주장의 상당수는 현재 기업들의 “새로운 분야에 먼저 깃발 꽂아놓기”, 즉 선점 효과를 노리는 데서 발생한다. 아직 완성되지 않은 서비스에 대해 일단 “우린 할 수 있다”고 주장해놓고, 실제 구현은 나중에 하는 관습에서 발생한다. 사실 이런 사례는 거의 모든 분야에서 옛날부터 있었던 마케팅이며, ChatGPT가 보여준 성능이나 파급효과가 워낙에 크다보니 쉽게 부정하기도 힘들고, “정말 가능할지도 모른다”는 기대감이 존재한다.

하지만, 심리학적으로 적합성 및 체계성을 가진 심리상담을 생성형 AI를 통해 진행하는 건 현재 시점에서는 불가능하며, 가까운 시일 내에는 심리치료의 보조 도구 역할은 할 수 있어도 주 상담사/치료가 되는 것은 어려울 것으로 전망된다.

‘선점효과’ 마케팅을 심리상담/치료 분야에 사용하는 것은 대단히 위험한 행위이다. 대부분의 분야는 생성형 AI가 제공하는 “유사한 답변”이면 충분하지만, “아주 정확한 답변”을 필요로 하는 의료 분야 등 일부 분야에서는 생성형 AI의 위력도 약해지며, 오남용의 위험성도 매우 크기 때문이다.

* 본 내용은 이장원 CTO(☎ 02-588-0720, jwlee@lud.co.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

본 고에서는 심리상담 및 관련 분야에 생성형 AI를 도입한 사례나 연구결과를 알아보고, 이런 전망과 달리 생성형 AI를 심리상담에 도입했을 때의 문제점과 한계에 대해 알아보고자 한다. 또한, 생성형 AI가 심리상담의 주체가 아닌, 보조 도구로서 활용된 사례와 그 유용함과 전망에 대해 살펴본다.

II. 심리상담에 대한 생성형 AI 진영의 주장

StabilityAI의 대표인 에마드 모스타크는 2023년 5월 미국 실리콘밸리에서 열린 “Cerebral Valley Summit” 콘퍼런스에서 “GPT-4는 최고의 상담 심리 치료사다”[2]고 말해 주목 받았다. 모스타크는 자신의 신경발달 장애와 ADHD에도 GPT를 ‘치료사’로서 적극 활용 중이라고도 밝혔다. 이미 미국의 커뮤니티 플랫폼 레딧엔 모스타크와 같은 이들이 증가 추세이다.

미국 샌디에이고 캘리포니아의 존 에어즈 웰컴연구소 교수 연구팀은 “대화형 챗봇 ‘ChatGPT’가 내놓는 의료 상담의 만족도가 의사를 능가한다”라는 분석을 의학학술지 “미국의사협회지 (JAMA) 내과”에 발표했다[3]. 연구팀은 레딧의 “의사에게 물어보세요(AskDocs)”란 게시판에 올라온 질문 195개를 무작위로 뽑아 ChatGPT에도 제시했다. 그런 다음 이 답변과 의사의 답변을 의사 면허를 지닌 전문가 패널들이 비교하게 했다. 그 결과 ChatGPT의 답변이 우수하다는 응답이 의사 답변이 우수하다는 응답보다 3.6배 높았다. 환자를 공감하는 답변이란 평가도 ChatGPT가 9.8배 더 높았다. 에어즈 교수는 “AI를 통해 의료를 개선할 수 있는 기회는 엄청나다”며 “ChatGPT는 환자에게 내리고 싶은 처방전과 같다”고 발언했다.

“ChatGPT로 이미 심리상담이 가능하다”라고 주장하는 서적들도 출간되고 있다. 한국만 해도 “ChatGPT 인생의 질문에 답하다”, “ChatGPT 연애학개론” 등의 서적이 ChatGPT를 저자로 하여 출간되었으며, 이들 서적은 “ChatGPT 인간심리까지 파고들다” 등의 표어를 내세우며 심리분석이나 상담을 ChatGPT로 수행할 수 있는 것처럼 주장하고 있다.

이런 상황이다 보니 서울디지털재단에서 발간한 “ChatGPT 활용 사례 및 활용 팁[4]” 역시 ChatGPT 활용 분야로 ‘심리상담’ 항목을 “상담분야는 잘못된 정보를 도출 할 수 있기 때문에 주의 요망”이라는 단서와 함께 추가했다. 워낙에 많은 언론이나 기업들이 “심리상담도 ChatGPT로 가능해질 거다”라고 말하니 이를 긍정할 수도 부정할 수가 없기에 고민 끝에 붙인 단서로 보인다.

III. 실제 심리상담/치료 산업 분야와의 괴리

하지만, 이러한 호평에도 불구하고 현 시점에서 생성형 AI가 심리학적으로 제대로 된 상담을 주도하는 것은 거의 불가능하며 가까운 시일 내에는 심리치료의 보조 도구 역할은 할 수 있어도 주 상담사/치료자가 되기는 어려울 것으로 전망된다. 영국 심리학회 회원인 폴 마스텐 박사는 정신건강 개선을 목표로 하는 앱에 대해서 “앱은 대면 치료의 보조 수단으로만 사용해야 하며, 대면 치료를 대체할 수 없다는 것이 중론이다”[5]라고 말했다. 또한, 뉴욕대 아서 캐플런 생명윤리학과 교수는 “이번 코크 사태처럼 사용자에게 알리지 않고 AI 기술을 사용하는 비윤리적인 행태가 앞으로 지속될 것이다”며 “특히 ChatGPT 등 챗봇을 통한 정신적 진단과 판단은 아직 표준 치료법이 아니다”고 지적했다. 그는 “지금까지 어떤 정신의 학자나 심리학자들도 ChatGPT나 GPT-3 등을 통한 심리 치료의 효능을 검증하거나 옹호하지 않은 상태다”[6]고도 강조했다.

1. 현재의 AI는 인간 심리를 이해하고 답변을 내는 것이 아니다.

1966년 MIT에서 개발한 심리상담을 모방한 세계 최초의 챗봇, ELIZA의 사례가 이를 보여준다(그림 1) 참조). ELIZA는 당시 유행하던 “내담자 중심 상담”을 모방한 챗봇이었다. 내담

```
=====
EEEEEEEE L      IIIIIII ZZZZZZZ      AAA
E      L      I      Z
E      L      I      Z      A      A
EEEEEE L      I      Z      A      A
E      L      I      Z      A      A
E      L      I      Z      A      A
EEEEEEEE LLLLLLLL IIIIIII ZZZZZZ      A      A
=====
ELIZA > (PLEASE TYPE IN ALL CAPS) WHAT'S YOUR NAME DEAR ?
AMIT
ELIZA > HI, I'M ELIZA. WHAT DO YOU WANT TO TALK ABOUT ?
AMIT > CAN I TALK ABOUT MY PROBLEM ?
ELIZA > SURE... !
AMIT > DUE TO ON GOING EXAMS IN COLLEGE, I HAVE A LOT OF STRESS.
ELIZA > PLEASE RELAX A LITTLE. SLEEP WELL.
AMIT > THANKS FOR YOUR ADVICE.
ELIZA > NO MENTION.
AMIT > BYE
ELIZA > BYE AND KEEP IN TOUCH...
=====
```

〈자료〉 기술과 혁신, 세계 최초의 심리상담 챗봇 ELIZA 대화 화면, KOITA, Vol.459, 2023.

[그림 1] 세계 최초의 심리상담 챗봇 ELIZA 대화 화면

자 중심 상담이란 상담치료사가 내담자의 행동이나 발언에 가치판단을 전혀 하지 않고 긍정하고 공감하는 방식의 상담을 말한다. 상담치료사의 역할을 해결책을 제시하는 것이 아니라, 내담자가 스스로 문제를 파악하고 해결방법을 찾아내도록 환경을 조성하는 것에 있다.

“내담자 중심 상담”이라는 기법 자체는 현재도 사용되고 있지만, 어쨌든 이 상담기법에서는 상대방이 이야기를 계속 이어나갈 수 있도록 격려하기만 하면 되었기에 1960년대의 컴퓨팅 기술로도 심리상담의 모방이 가능했다.

환자: 나는 X가 필요합니다.

ELIZA의 답: 왜 X가 필요한가요? / X가 정말 도움이 될까요? / X가 꼭 필요하다고 생각하세요?

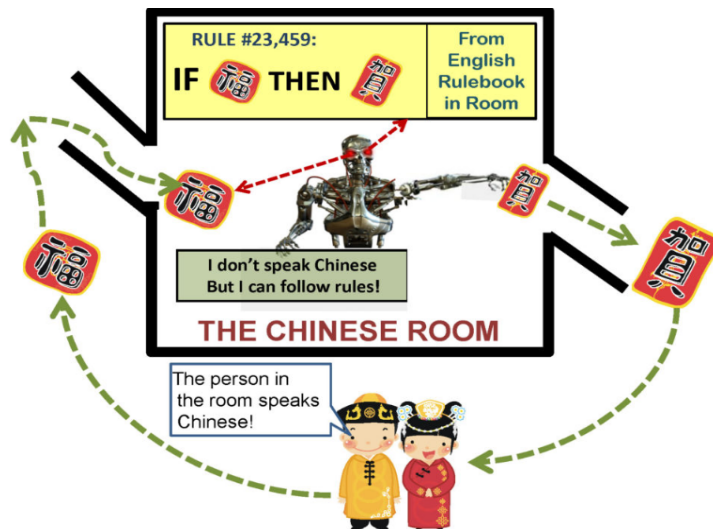
환자: 뭐가 그렇죠?

ELIZA의 답 : 왜 물어보시죠? / 당신은 어떻게 생각하세요?

환자의 말에 규칙을 적용할 수 없는 경우

ELIZA의 답 : 계속 말씀해 보세요 / 정말 흥미롭네요 / 그렇죠, 어떤 뜻인지 조금 더 말씀해주실까요?[7]

예시 대화를 보면 짐작하겠지만, ELIZA는 입력받은 문장에 대해 미리 설정된 키워드에 따라 특정한 답변만을 내놓았던 것이다. 하지만 적지 않은 이들이, 심지어 ELIZA를 개발한 엔지니어조차도 ELIZA를 ‘대화상대’처럼 생각했다. 이로 인해 “일라이자 효과”라는 신조어까지 생겼는데, 이는 “사용자가 무의식적으로 컴퓨터의 행위를 인간의 행위와 유사한 것으로



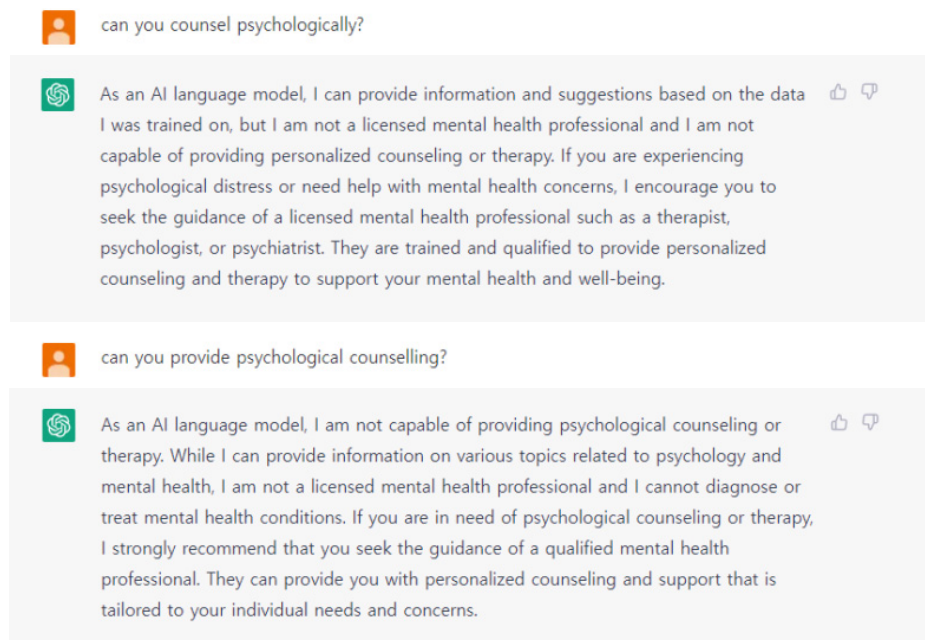
〈자료〉 Richard Golden, LM101-006: How to Interpret Turing Test Results, Learning Machines 101, 2014.

[그림 2] “중국어 방” 실험 개요 도식도

추정하고 의인화하는 경향”[8]을 말한다. 영화 ‘HER’이나 현재 서비스되고 있는 ‘레플리카’ 등의 예시를 생각하면 쉬울 것이다.

미국의 철학자 존 설의 “중국인 방 문제”는 인공지능 중 인공일반지능(AGI)을 실험하는 척도로 유명한 튜링 테스트로는 인공지능에게 사람과 같은 지능이 존재하는지를 판별할 수 없음을 보여주는 사고 실험이다. [그림 2]와 같이 안을 볼 수 없는 방 안에 중국어를 전혀 모르는 작업자를 앉혀 놓고, 이 작업자에게는 중국어에 대한 해석은 전혀 없이 제시된 중국어 문장에 따라 적합한 중국어 답을 정리한 표만 주어진다. 누군가가 종이에 중국어로 쓴 문장을 적어서 방에 넣으면, 작업자는 표를 보고 그에 맞는 답을 표에 적힌 모양 그대로 그려서 내놓는다. 이 경우 작업자가 중국어를 전혀 이해하지 못하는데도 방 밖의 사람은 중국어로 소통한다고 생각할 것이다[9].

1966년의 ELIZA도, 2023년의 ChatGPT도 결국 이 점에서는 마찬가지이다. 문장을 이해하고 공감해서 답변을 주는 것이 아니라, 모델과 알고리즘에 따라 답을 주는 것이고 그 ‘답안’이 ChatGPT는 매우 정교화 되었을 뿐이다. 물론 “문장을 이해하는 것처럼 보인다”라는 것



〈자료〉 ChatGPT, ChatGPT에게 심리 상담이 가능하냐고 질문했을 때 ChatGPT 답변, ChatGPT, 2023.

[그림 3] 전문적 심리상담은 불가하니 전문가를 찾으라는 챗 GPT 답변

만으로도 대단한 수준이고 위대한 진보이기는 하지만, 심리상담 현장에 상담사로서 직접 도입하기에는 매우 문제가 많다고 할 수 있다.

이러한 문제는 ChatGPT의 개발사인 OPEN AI도 인지하고 있는 문제라, 심리상담에 대해 문의하면 [그림 3]과 같이 “공인된 전문가를 찾으라”는 답변이 올라오게 만들고 있다[10].

2. 인간 심리에 대한 정확한 데이터 수집과 연구의 어려움

이렇게 반론할 수도 있을 것이다. 2023년 현재의 생성형 AI는 심리상담을 이해하기 어렵지만 계속해서 데이터를 분석하면 가까운 미래에 가능해지지 않겠냐고 말이다. 필자 역시 기본적으로는 동의하지만, 할루시네이션(AI가 맥락과 관련 없거나 사실이 아닌 내용을 마치 옳은 답처럼 내놓는 현상) 등의 문제 때문에 심리상담 분야에 대한 정확한 상담과 진단 데이터를 수집해야 하는데, 현재 심리상담 분야는 그 점에 있어서 어려운 점이 많다는 것을 지적하고 싶다. AI, 정확히는 머신러닝 계열의 AI가 성공적인 성과를 창출한 분야들은 대부분 ① 바둑과 같이 데이터 수집이 매우 쉬운 분야거나(바둑의 ‘기보’는 그 자체로 데이터셋이라고 할 수 있다), ② 그 결과물이 정확하지 않아도 빅데이터를 통해 경향성을 제대로 잡아낼 수 있거나, ③ 오랜 시간과 비용을 들여 데이터를 가공하고 이를 통해 AI 모델링을 진행한 분야들인데, 심리상담은 3가지 모두 해당이 되지 않는 분야이다.

한국의 심리상담 분야의 현황을 살펴보면, 왜 심리상담의 데이터 수집이 제대로 이루어지지 않는지 알 수 있다.

가. 심리상담 분야는 디지털 전환이 매우 미비한 분야라 정확한 데이터 수집/분석이 어렵다.

2021년 통계청 통계에 따르면 한국의 심리상담센터(정신과 의료기관을 제외한 일반 심리상담센터)는 약 5,800개, 심리상담 종사자는 약 2만 5,000명이다[11].

이 데이터가 의미하는 것은 다음과 같다.

- 심리상담이라는 분야 자체가 매우 영세한 분야임을 의미한다.
- 따라서 데이터 수집/분석에 대한 체계가 제대로 정립되어 있지 않으며, 그럴 여력이 없는 심리상담 센터가 대부분이다.

이런 문제로 인해 심리상담 분야의 디지털 전환률 자체가 극히 낮다. 2023년 현재도, 심리

상담 분야의 대부분은 아직도 상담기록을 수기나 개별 문서파일로 관리한다. 고객관리의 기본이라는 CRM(고객관계관리) 프로그램조차도 사용하는 심리상담센터가 드물다.

현재 많은 대학들이 심리 분야 연구를 진행하고 있지만, 심리상담센터와 협약 하에 그 데이터를 활용하는 곳은 극히 적다. 2021년에 한국에서 진행된 심리상담만 213만 건인데, 그 데이터 대부분이 무용지물이 된 것이다. 위의 문제들 때문에 제대로 된 데이터를 수집하기도 힘들고, 사전에 미리 내담자 동의 등의 절차와 준비를 해놓지 않으면 상담윤리에도 문제가 있으니, 대부분의 대학들이 좌담회 형식으로 연구대상을 따로 모집해서 실험하는 것이다.

나. 위의 문제로, 데이터 분석을 통해 정확한 상담/치료에 관한 모델을 만들기가 어렵다.

결국, 생성형 AI도 본질적으로 학습이 필요한 AI이며, AI를 학습시키려면 정확하고 많은 데이터가 필요하다. 문제는 심리상담 분야의 기존 데이터는 정확하지도 분량이 많지도 않은 데, 정작 결과물은 ‘정확하게’ 나와야 하는 의료 분야라는 것이다.

다. 의료 분야의 규제를 뚫기도, 비즈니스 모델(BM)을 만들기도 매우 어렵다.

위에서 설명한 이유로 의료 분야에서는 생성형 AI 기반 서비스들이 규제를 돌파하기 어렵다. 한 예로 세계적인 컨설팅 기업 딜로이트는 2018년 5월, ‘D. Predict’라는 신약 임상시험의 성공률을 예측하는 머신러닝 기반 솔루션을 발표했었다[12]. 딜로이트는 발표 당시 기사에서 “해당 솔루션을 의료분야에서도 활용할 수 있을 것”이라 자평했지만 이 솔루션은 결국 본격적으로 쓰이지 못했다. 해당 솔루션이 금방 자취를 감춘 것은 여러 가지 이유가 있지만 당시 자체 기술평가에서도 정확도가 73%에 그쳤기에 의료 분야에 도입하기엔 정확도의 문제가 컸다는 점이 있다.

심리상담 분야에서 생성형 AI를 활용한 수익성 있는 BM을 만들기가 극히 어렵고, 관련 기업의 진출이나 투자도 별로 없다는 점도 장벽이다. 위에서 말한 정확도 등의 문제를 넘어서려면 많은 시간과 자금이 필요한데, 실제로 심리상담 분야에서 활동하고 있는 기업들은 소수의 스타트업들에 불과하며, 대규모 투자를 유치한 기업은 거의 없다. 심리상담 분야의 스타트업 중에 AI에 손대보지 않은 기업은 거의 없지만, AI를 통해 수익성 있는 BM을 개발한 곳도 아직 없다. 그만큼 위의 장벽들이 생각보다 넘어서기 힘들다는 반증이다.

심리상담 역시 인간 대상의 의료 분야이며, 따라서 부정확한 내용이나 상담을 진행하는 것은 위험한 일이다. 미국의 심리학자 조나단 세들러는 AI 챗봇의 상담 치료 확장 가능성을 긍정하는 기사를 트위터에 공유하며 비판했다. “AI 챗봇은 당신이 세상에서 제대로 역할을 하고 다른 사람과 관계를 맺도록 가르치지 않는다”며 “나르시스즘적 환상에 빠지는 방법은 가르쳐준다”고 했다[13].

ChatGPT와 같은 생성형 AI는 질문을 해석한다. 그리고 답변이 될 만한 유사 텍스트를 학습해 그럴듯하게 말해준다. 이 과정이 사실 알게 모르게 스스로 생각했던 걸 꺼내주는 과정에 불과할 수 있다고도 했다. 고민은 해결되지 않고, 상담자 본인의 생각과 고민만 계속 발전할 수도 있다는 비판이다. 쉽게 말하면 자신의 성공에 대한 확신이 많은 사람이 ChatGPT로 상담하면 자기 성공에 대한 확신이 점점 늘어날 수 있지만 절망에 빠진 사람에게서는 오히려 부정적 생각을 더 심화시킬 수 있다는 것이다.

실제로 2023년 3월에 기후위기에 대한 절망에 빠진 벨기에 30대 남성이 AI 챗봇의 부추김에 스스로 목숨을 끊는 일도 발생했다는 보도도 있었다[14]. 배려와 공감에 결여된 생성형 AI 상담은 자기 상태에 대한 급진만 가속화하는데, 이러한 문제에 대한 고민이나 배려가 없이 생성형 AI의 더 강력해진 “일라이자 효과”를 악용하려는 이들이 늘어나고 있다.

3. 인간을 동의 없이 생성 AI의 실험상대로 삼는 사기업들

코코(KOKO)의 공동창업자 로버트 모리스가 “GPT를 사용하여 약 4,000명에게 정신건강 지원을 제공했다”고 트위터에 공표한 후 일어난 논쟁은, AI 기술이 심리상담에 적용될 때 일어날 수 있는 윤리적 논쟁과 위험성을 미리 보여준다.

우선, 위의 정신건강 지원은 고객의 동의도 받지 않고, 고객들에게 그 메시지가 AI로 작성되었다는 것을 숨긴 채 진행되었다. 그 때문에 학계나 언론에서는 “정신건강 지원이 필요한 취약한 사람들을 본인들의 동의 없이 실험 대상이 되도록 속였다”라고 비판했다.

연구 윤리 분야의 교육자인 조지아 주립대학 법학 교수 레슬리 울프는 “AI가 검토되지 않은 편향되거나 부주의한 텍스트를 생성할 경우 정신적 고통에 시달리는 사람들의 기분이 더 나빠질 수 있다”[15]면서 KOKO가 AI로 답변을 제공한 것을 숨긴 것에 대해 비판했다.

2012년, 페이스북(현 메타)은 68만 9,000명을 대상으로 심리 실험[16]을 실시하여 사람들의 뉴스피드 콘텐츠를 변경함으로써 전염병처럼 부정적 또는 긍정적 감정을 확산시킬 수

있다는 사실을 밝혀내고 해당 논문을 미국 국립과학원 회보(Proceedings of the National Academy of Sciences: PNAS)에 등재했다. 이 실험에서 페이스북은 대상 유저들의 뉴스피드에 등장하는 포스트와 사진의 종류를 조작하여 긍정적인 포스팅이나 부정적인 포스팅 중 한 가지만 보여지도록 했다. 그 결과 유저들은 평소처럼 친구들의 다양한 포스팅을 보는 것이 아니라 페이스북사에서 조작한 뉴스피드를 보게 되었다. 페이스북 측은 사용자가 직접 친구의 페이지를 방문할 경우 그들의 포스팅을 볼 수 있도록 해 두었다고 설명했지만, 중요한 건 페이스북이 고의적으로 대부분의 사람들이 읽는 뉴스피드에 올라가는 특정 콘텐츠를 편집하거나 강조했다는 것이다.

이렇게 실험결과보다 긍정적인 포스트에 노출된 사용자들이 스스로도 보다 긍정적인 댓글을 다는 경우가 많으며, 역의 관계 역시 성립한다는 사실을 확인했다. 연구는 직접적 접촉이나 안면이 없는 사이에서도 감정의 동조를 이끌어낼 수 있다는 “감정 전염”이라는 과학적 개념에 초점을 맞춰 기획하고 진행되었다.

이 연구가 논란이 되자 페이스북은 “우리의 목적은 어디까지나 심리학적 연구의 일환이며, 사용자들을 스팸이나 중복 콘텐츠로부터 보호하는데 있다”면서 “페이스북 가입 시 유저들이 동의한 페이스북 이용 조건 항목 중에 뉴스피드 내용을 조작하는 것에 동의하는 항목이 있으므로 이는 합법이다”라는 입장을 밝혔다. 이에 대해 애널리틱스 제프 케이건은 “가장 큰 문제는 페이스북의 사고방식이다. 그들은 고객과 고객의 프라이버시에 관해서는 전혀 생각하지 않는다. 그들은 지속적으로 사용자를 무시하는 비열한 활동을 해나가고 있다”라면서, 분명 법적으로는 문제가 없지만 윤리적으로는 문제가 많음을 지적했다.

미 정부 연구원들이 매독에 걸린 흑인들에게 생체 실험을 하다 사망자가 나왔던 터스커키 사건 이후, 미 의회는 1974년 인간 피실험자들과 관련된 테스트에 대한 감독을 의무화했다. 현재 미국에서는 연방 지원을 받는 대학이나 기관들은 인간 주제에 대한 실험을 수행할 때 생명윤리심의위원회(IRB)로 알려진 엄격한 규칙을 따라야 한다.

하지만, 미 연방 정부의 지원을 받지 않고 식품의약품의 승인을 받지 않는 민간 기업이나 비영리 단체의 경우 이러한 법적 의무가 없다. 코코도, 페이스북도 위의 문제로 어떤 법적 처벌도 받지 않았다. 이런 선례들이 있기에 상담윤리에 저촉되거나 심리학에 대한 고찰이 없는 유사 서비스들은 앞으로도 나올 것으로 예상된다.

IV. 심리상담의 보조도구로는 생성 AI가 매우 유용

앞서 말한 것처럼 생성형 AI가 심리상담 분야에서 주 상담자가 되기에는 많은 문제들이 있다. 그러나 반대로 심리상담 및 치료의 보조도구로는 매우 유용하며, 디지털 전환(DT)이 열악한 심리상담 분야의 디지털 전환을 이루고 장차 심리 분야에 대한 정확한 데이터 수집을 위해 필요하다고 본다. “심리상담의 보조도구”로 사용하자는 이야기는 다시 말하면 “생성형 AI가 만드는 결과물을 바로 고객(내담자)에게 전달하지 말고, 그 중간에 심리상담사를 검수 역할로서 두라”는 이야기이다. 이는 단순히 규제를 피하는 수준이 아니라, 생성 AI를 심리상담사로 활용했을 때 발생할 수 있는 문제 대부분을 해결할 수 있다.

1. 전문가에 의한 필터링을 거침으로서, 정확도가 떨어지는 문제를 피할 수 있다.

의료 분야는 “아주 정확한 답변”을 요구하기 때문에 생성형 AI가 생성한 답변을 내담자에게 그대로 전달하는 건 문제가 있다. 하지만, 중간에 심리상담사가 검수하고 생성형 AI는 내담자에게 해야 할 답변을 ‘제안’만 하는 방식이라면, 정확도나 할루시네이션 문제를 효과적으로 회피할 수 있다.

2. 심리상담의 업무 프로세스 개선에는, 생성형 AI가 매우 효과적이다.

생성형 AI가 해줄 답변의 ‘제안’ 그리고 상담기록의 ‘요약’ 등의 기능은 심리상담에 있어 매우 니즈가 높은 기능들이다. 현행 심리상담에서는 상담시간보다 상담 후 처리업무가 더 많은 시간을 차지한다. 상담 축어록(상담 내용을 문서로 만드는 것) 작성, 상담 내용의 분석 및 토의, 내담자에게 적절한 답변을 보내는 것 전부가 현재는 수작업으로 이루어지고 있기 때문이다.

이 문제들 전부가 ChatGPT의 응용으로 해결 가능한 일이다. 심리상담 분야에서 “상담내용을 녹음해서 STT(Speech To Text)로 바꾸면 된다”라는 발상을 못해서 제한적으로 사용하고 있는 것이 아니다. 현재 한국 STT 솔루션 중 가장 널리 쓰이는 제품들조차도 아직은 STT 변환 후 수작업으로 고쳐야 할 부분이 너무 많아서 안 쓰는 것이다. 그런데 생성형 AI를 이용하면 이러한 수정 작업을 자동으로 할 수 있게 되어 상담기록 작성에 도움이 된다.

상담기록 요약은 ChatGPT가 가장 잘하는 “텍스트 요약”이니 더 설명할 필요가 없을 것이며, 내담자에게 적절한 답변을 만드는 것 역시 미리 데이터를 학습시키고, 적절한 프롬프트를 사용한다면 불가능한 것도 아니다. 이미 심리상담 분야 스타트업에서는 시험적으로 이런 기능들을 활용하려는 기업들도 있다.

3. 생성형 AI를 필두로 심리상담 분야의 디지털 전환(DT)을 이루는 과정에서, 심리 분야 데이터를 수집할 수 있게 된다.

생성형 AI와 웹 솔루션, CRM, 챗봇 등의 기술을 적절히 결합하면, 심리상담 업계에서도 환영받을만한 심리상담 보조 솔루션의 제작이 가능하다. 그런데 이러한 솔루션을 도입한다는 것은 심리상담 기록들이 드디어 데이터로 저장되기 시작한다는 뜻이며, 심리상담 솔루션 개발 시에 데이터를 정형화하는 것을 전제로 기획 및 설계를 진행하여 적절한 UX를 갖추게 되면, 심리상담 데이터를 약간의 가공만으로 데이터셋으로 바꾸는 것 역시 꿈만은 아니다. 즉, 그간 심리 분야 연구에 있어 큰 장벽이었던 심리상담 데이터의 가공에 필요한 시간과 비용이 대폭 줄어드는 것을 의미한다. 물론, 적절한 절차를 거쳐야겠지만, 개인정보 비식별화된 심리상담 데이터를 연구목적으로 활용할 수 있다면 심리연구에도, 향후 생성형 AI가 심리상담/치료를 위한 정확한 데이터 분석에도 크게 도움이 되리라 생각된다.

V. 결론

코로나 이후 심리상담의 숫자가 크게 증가한 것에 비해 한국의 심리상담 인프라는 여러 지점에서 부족함을 보이고 있다. 이런 문제를 해결하기 위해 심리상담의 디지털 전환이 반드시 필요하지만, 관련된 예산이 적고, 심리학이나 상담윤리에 대한 충분한 고찰이 없는 서비스들이 심리상담의 이름을 걸고 나오고 있는 상황이다. 특히, ChatGPT를 비롯한 생성형 AI들은 강력한 일라이자 효과를 통해 유사 서비스들에게 사용자들이 현혹되게 하는 결과를 낳을 수 있어, 규제에 대한 고민을 하지 않을 수 없다.

다만, 그렇다고 해서 생성형 AI들을 심리상담에서 배제시키는 것은 옳지 않다. 심리상담사나 전문가들의 검수와 조언을 통해 보조 기능으로는 충분히 훌륭하게 동작할 수 있고, 이러

한 움직임이 결과적으로 심리 분야의 연구에도 기여할 수 있을 것이라 생각한다. 본 고에서 다룬 내용들이 심리상담과 생성형 AI 분야의 활용에 관심을 가진 이들에게 도움이 되길 바란다.

● 참고문헌

- [1] NBC NEWS, A mental health tech company ran an AI experiment on real users. Nothing's stopping apps from conducting more, NBC NEWS 보도자료, 2023.
- [2] 한국경제신문, 생성 AI와의 상담...어떨 때는 맞고, 어떨 때는 틀리다, 2023. 6. 13.
- [3] 동아일보, 의료상담 만족도에서도 의사 뛰어넘은 ChatGPT, 2023.
- [4] 서울디지털재단 ChatGPT 활용연구 TFT, "ChatGPT 활용 사례 및 활용 팁", 2023. p.5.
- [5] BBC, "제인 웨이크필드, 챗봇 치료사에게 마음을 열 수 있을까?", 보도자료, 2023. 4. 3.
- [6] Zdnet Korea, "ChatGPT, 정신 치료 가능할까...전문가 '시기상조'", 2023.
- [7] KOITA, "ChatGPT에는 정말로 지능이 있을까?, 기술과 혁신", Vol.459, 2023.
- [8] 경향신문, "기계가 사람으로 느껴질 때", 2023.
- [9] 통계청, 분류코드 87294(사회복지 상담 서비스 제공업) 21년 통계, 2021.
- [10] Richard Golden, LM101-006: How to Interpret Turing Test Results, Learning Machines 101, 2014.
- [11] ChatGPT, "전문적 심리상담은 불가하니 전문가를 찾으라는 ChatGPT 답변", 2023.
- [12] 데일리팜, "딜로이트, 인공지능 신약가치평가 솔루션 개발", 2018. 5. 2.
- [13] 한국경제신문, "생성 AI와의 상담...어떨 때는 맞고, 어떨 때는 틀리다", 2023. 6. 13.
- [14] Zdnet Korea, "AI 챗봇과 대화 하다 목숨 끊은 男...'천국서 살 수 있다'", 2023. 5. 18.
- [15] NBC NEWS, A mental health tech company ran an AI experiment on real users, Nothing's stopping apps from conducting more, 2023.
- [16] CIO, "페이스북 심리 실험에 관한 7가지 사실", 2014.

Chapter

03

양자 다이아몬드 자기장 현미경

오상원_한국표준과학연구원 책임연구원

I. 결과물 개요

개발목표시기	2024. 06.	기술성숙도 (TRL)	개발 전	개발 후
결과물 형태	HW-Module, HW-System, Patent		4	6
Keywords	다이아몬드 양자자기장센서, 자기장 현미경, 다이아몬드 질소 빈자리 quantum diamond magnetometer, magneto-microscope, DNV			

II. 기술의 개념 및 내용

1. 기술의 개념

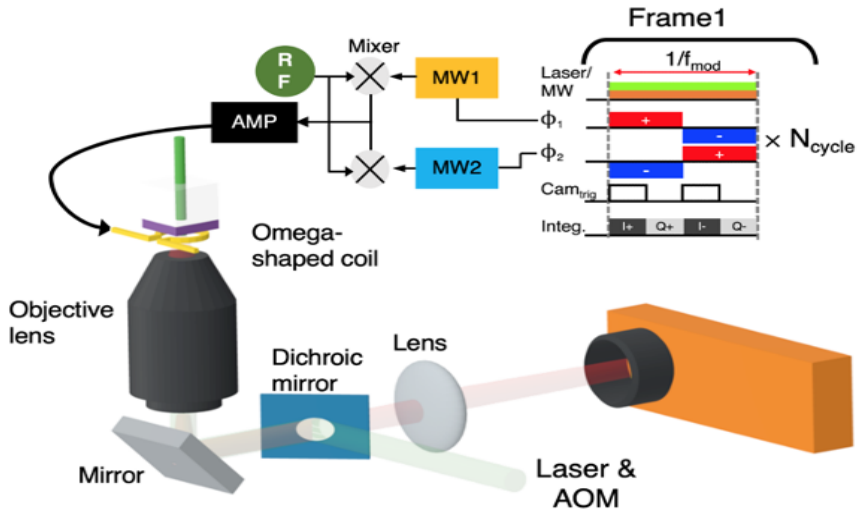
- 다이아몬드 양자 자기장 센서를 이용한 자기장 측정이 가능한 자기장 현미경

2. 기술 특징

- 다이아몬드 내부 불순물(nitrogen vacancy)을 이용한 자기장 측정
- 카메라 혹은 포토다이오드 등을 이용한 광학적 측정

* 본 내용은 오상원 책임연구원(☎ 042-604-1053, sangwon.oh@kriss.re.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.



〈자료〉 한국표준과학연구원 자체 작성

[그림 1] 기술개념도

- 카메라 이용 시 각 넓은 영역을 동시에 측정이 가능
- 시료와 수백 나노미터 ~ 수 마이크로미터까지 근접이 가능해 뛰어난 자기장 공간 분해능을 가짐

III. 국내외 기술 동향 및 경쟁력

1. 국내 기술 동향

- 국내 대학교 및 연구소 등에서 다이아몬드 양자 센서를 이용하여 자기장 및 온도 측정 연구가 활발히 진행 중
- 다이아몬드 자기장 현미경 구성 시 Lock-in이 가능한 카메라를 사용하여 뛰어난 자기장 민감도를 확보

2. 국외 기술 동향

- 양자자기장 현미경을 사용하여 집적회로의 불량 분석 기술 개발
- 그래핀 등 2차원 물질에서의 전류흐름 측정을 통해 다양한 물질 특성 연구 진행 중

3. 경쟁기술 동향 및 현황

- 마이크로미터 수준의 공간 분해능과 수십 나노 테슬라 수준의 민감도를 동시에 확보

경쟁기술	본 기술의 우수성/차별성
홀센서 스캐너	- 홀센서 대비 뛰어난 자기장 민감도(nT)와 홀센서 스캐너와 다르게 대면적을 마이크로미터 수준의 공간 분해능으로 동시에 측정할 수 있어 매우 빠르게 측정 속도를 가짐
초전도간섭계(SQUID) 기반 스캐너	- SQUID 센서는 뛰어난 민감도(수십fT)를 갖는 큰 장점을 갖고 있지만 SQUID 구성을 위해 시료와 근접할 수 없는 단점(공간 분해능 열화)과 점 위치만을 측정하는 스캐너 특성상 측정 속도가 느린 단점을 가짐 - SQUID 센서는 극저온 냉매를 주기적으로 공급해야 하는 문제가 있어 장비운용 비용이 높은 단점을 가짐

4. 특허 동향

No.	국가	출원 · 등록번호(출원 · 등록일)	상태	명칭
1	대한민국	10-2021-0150446(2021.11.04)	출원 중	DNV 센서 모듈을 이용한 대면적 자기장 및 온도 측정 장치 및 방법
2	PCT	PCT/KR2020017360(2020.12.01)		Apparatus for sensing temperature using diamond nitrogen vacancy sensor and method for fabrication the same

IV. 국내외 시장 동향 및 전망

1. 국내외 시장 동향 및 전망

- 양자자기장 전체 시장 전망

- 세계 양자자기장 센서는 2022년 551.6백만 USD에서 2028년 1,029백만 USD로 평균 10.8% 성장할 것으로 예상(Inside Quantum Technology, Quantum Sensor Markets. 2019)
- 국내 양자자기장 센서의 시장도 2022년 418억 원에서 2028년 879억 원으로 연평균 13% 성장할 것으로 예상(ETRI 기술정책연구본부)

2. 제품화 및 활용 분야

➤ 반도체 불량 탐지

제품/서비스	제품 및 활용 야 세부내용
반도체 불량 탐지	다층 패키징된 반도체의 단락 등 검사
자성체 연구 장비	연구기관에서 자성체 연구에 활용 가능한 자기장 현미경

V. 기대효과

1. 국내외 시장 동향 및 전망

- 우리나라는 반도체 생산에 있어 세계적 선도국가로 기술 수준이 높은 다층 패키징 방법의 신뢰도를 높이는데 자기장 현미경이 기여할 수 있음

Chapter

03

단위 디지털트윈 연합을 위한 고신뢰 실시간 양방향 동기화 엔진 기술

송민환_한국전자기술연구원 책임연구원

I. 결과물 개요

개발목표시기	2026. 12.	기술성숙도 (TRL)	개발 전	개발 후
결과물 형태	SW-Patent		3	6
Keywords	디지털트윈, 고신뢰 동기화, 대용량 동기화, 양방향 동기화, 지능형 동기화 Digital Twin, High-reliability synchronization, Massive synchronization, Bidirectional synchronization, Intelligent synchronization			

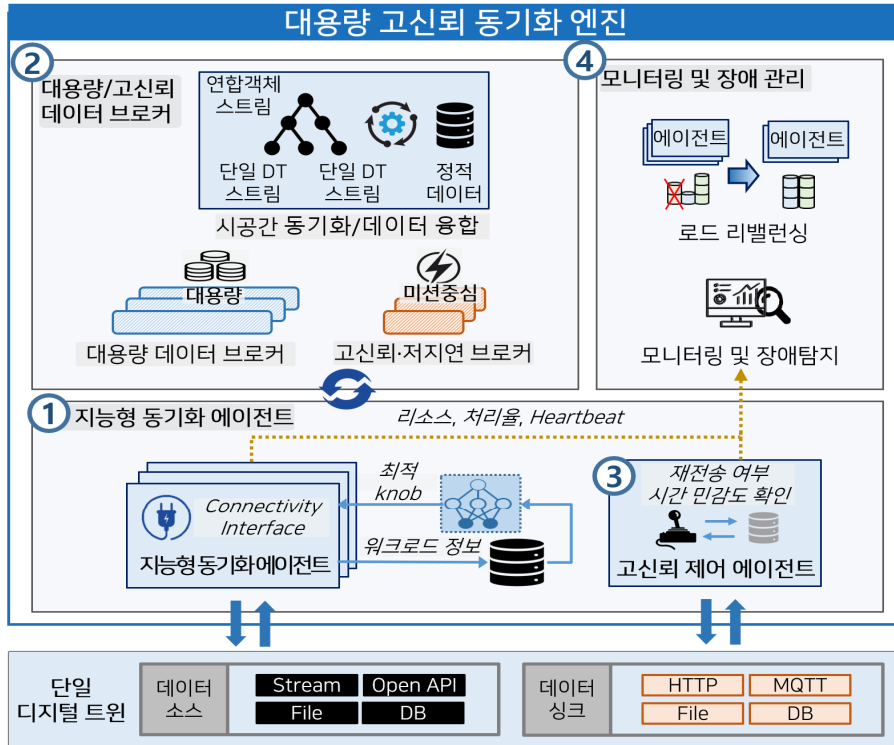
II. 기술의 개념 및 내용

1. 기술의 개념

- 단위 디지털트윈 연합을 위한 고신뢰 실시간 양방향 동기화 엔진 기술은 단위 디지털트윈들이 수집하는 실시간으로 발생하는 사물인터넷 데이터와 그로부터 파생되는 인공지능·서비스 데이터를 수집하여 디지털 연합 트윈의 다양한 융합 서비스에 전달해 주기 위한 동기화 엔진 및 에이전트 기술을 의미
- 단위 디지털트윈은 현실 세계에서 다양한 특성의 데이터를 수집하고 파생 데이터를 생성

* 본 내용은 송민환 책임연구원(☎ 031-789-7582, mhsong@keti.re.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.



〈자료〉 한국표준과학연구원 자체 작성

[그림 1] 기술개념도

하며, 이러한 단위 디지털트윈을 활용하는 디지털 연합 트윈 서비스는 서비스별 요구사항에 맞게 최적화된 데이터 동기화를 요구. 본 기술은 디지털 연합 서비스가 요구하는 문제를 해결하기 위한 지능형 동기화 에이전트 및 동기화 엔진 기술

- ▶ 또한, 본 기술은 지능형 동기화 에이전트 기술 외에 디지털 연합 트윈에서 수행되는 다양한 서비스를 지원하기 위해, 이종의 브로커로 구성된 양방향/대용량 고신뢰 동기화를 지원하는 엔진과 최적 동기화 경로를 제공하는 지능형 동기화 에이전트를 포함

2. 기술 특징

▶ 지능형 동기화 에이전트 기술

- 단위 디지털트윈 이종 데이터 소스를 지원하기 위한 동기화 에이전트 및 인터페이스

기술, 워크로드별 최적 동기화 지원 지능형 에이전트 기술, 서버 리소스에 따른 지능형 로드밸런싱 기술을 포함

- 대용량/고신뢰 데이터 브로커 기술
 - 이중 목적 기반 통합 데이터 브로커 기술, 시공간 동기화 및 데이터 융합용 분산처리 엔진 기술을 포함
- 고신뢰 제어 보장 기술
 - 시간 민감도 기반 고신뢰 동기화 기술, 서비스 요구사항에 따른 데이터 재전송 매커니즘을 포함
- 동기화 에이전트 모니터링 및 장애 관리 기술
 - 동기화 브로커 및 에이전트 리소스 모니터링 기술, 동기화 에이전트의 장애 탐지 및 로드 리밸런싱 기술을 포함

III. 국내외 기술 동향 및 경쟁력

1. 국내 기술 동향

- 국내 디지털트윈 기술은 글로벌 기업에 대비해 디지털트윈 플랫폼 등 관련 원천 기술에 대한 개발 사례가 부족하나, 국내의 기업이 IoT, 3D 모델링 등 디지털트윈 요소 기술과 관련된 자사의 특화 역량을 활용하여 디지털트윈으로 비즈니스 영역을 확대하고자 하는 시도는 많이 보임
- 국내의 기업들은 제조 공정의 최적화와 물류 흐름 운영 효율성 제고 등의 서비스를 위해 글로벌 대기업의 제품을 기반으로 디지털트윈 도입을 시도 중
- 현재 국내 디지털트윈 기술의 경우, 단위 디지털트윈의 핵심 요소 기술 개발에 집중하고 있어 디지털트윈의 연계 및 동기화 기술과 관련한 연구는 미흡

2. 해외 기술 동향

- 주요 선진국이 주도하며 초기 제조업 중심의 디지털트윈 시장에서 다양한 산업 분야로

- 확대되고 있으며 최근 디지털 전환에 대한 관심도가 높아지며 세계적으로 급성장 중
- 글로벌 디지털트윈 솔루션 기업인 미국 GE, 독일 Siemens, 프랑스 Dassault는 헬스케어, 자동차, 에너지, 항공 등 산업 전반의 다양한 분야로 디지털트윈 시장을 확대
 - 이종의 단위 디지털트윈의 연합 및 동기화와 관련된 원천 기술의 경우, 다양한 응용 도메인 디지털트윈 간 다이나믹한 로직 처리가 가능하도록 지원하는 Azure Digital Twin 버전 2와 Twin Federation 기능을 제공하는 Bentley Systems의 iTwin.js를 제외하고는 사례가 미흡

3. 경쟁기술 동향 및 현황

경쟁기술		본 기술의 우수성/차별성
Predix, General Electric(GE)	- 기계에서 발생하는 대규모의 데이터를 수집·분석하고 사물인터넷으로 연결하여 디지털트윈을 구현해주는 Predix 공개 - GE가 제조·판매하는 장비의 센서에서 수집한 데이터를 모아 분석하고, 디지털트윈으로 구현하여 가상 모니터링·제어 등의 서비스 제공 - 가스, 증기, 풍력 터빈 등을 클라우드 환경에서 디지털화하고 제어	- 본 기술은 단일 응용에 한정되어 있는 기존 단위 디지털트윈의 한계를 극복하여 이종의 단위 디지털트윈으로부터 입력되는 다양한 특성의 실시간 데이터를 연계하고 디지털 연합 트윈 생성을 지원할 수 있는 동기화 에이전트 및 엔진 기술 - 다양한 단위 디지털트윈의 특징과 디지털 연합 트윈 서비스의 요구사항에 맞게 최적화된 데이터 동기화를 지원하는 에이전트 및 엔진으로 구성
PlantSight, Siemens	- 제조 플랜트의 실시간 운영 상황을 3D 시각화 모델로 제공하고 고신뢰 데이터를 제공하는 PlantSight를 공동 개발 - 제조 공정의 디지털화 및 자동화 기능 제공	- 단위 디지털트윈의 특성에 따라 최적 동기화 파라미터로 구성된 에이전트를 생성하며 서비스의 요구사항에 따라 대용량의 동기화와 고신뢰 동기화를 선택하여 제공이 가능

IV. 국내외 시장 동향 및 전망

1. 국내외 시장 동향 및 전망

- 글로벌 시장조사 업체 가트너는 주목해야 할 “10대 기술 트렌드”로 디지털트윈을 선정하였으며 혁신적인 잠재력을 갖고 있고, 폭넓은 영향력을 보이며 급성장세를 나타낼 것으로 예상
- 시장조사업체 Markets and Markets의 디지털트윈 시장 보고서에 따르면 디지털트윈의

세계 시장의 규모는 2020년 31억 달러(3조 4,000억 원)에서 2026년 482억 달러(53조 8,000억 원)으로 성장할 것이라 전망(연평균 성장률 57.6%)

- 국내 시장 규모는 약 690억 원 규모로 미약하나 북미, 유럽 등 해외 주요국 대비 높은 성장률을 달성할 것으로 예측. 국내 디지털트윈 시장은 글로벌 대비 시장 개척 초기 단계로 규모가 작으나 성장 잠재력이 매우 크다고 평가

[표 1] 디지털트윈 기술의 국내외 시장

(단위: 10억 달러)

구분	2020년	2026년	CAGR
세계 시장규모	3.15	48.27	57.6%
한국 시장규모	0.06	1.53	70%

2. 제품화 및 활용 분야

- 본 기술을 기반으로 다양한 응용 분야가 혼재된 복합 플랫폼 환경에서 데이터 및 서비스를 효과적으로 연계하는 데 활용 가능
- 다양한 지능형 플랫폼들이 연계된 연합 응용 서비스를 제공하기 위한 지능형 데이터 수집 및 공급 솔루션으로 활용

제품/서비스	제품 및 활용 분야 세부내용
디지털트윈	본 기술은 수요처가 보유한 디지털트윈과 활용 가능한 외부 디지털트윈을 연계할 수 있도록 지원함으로써 서비스의 응용 분야를 확장하고 새로이 도출한 융합 서비스를 운용 가능한 환경을 구축하는 데 활용
스마트시티	본 기술은 지자체가 보유한 다양한 빅데이터 플랫폼과 IoT 데이터 기반의 디지털트윈 및 실시간 서비스를 실시간으로 연동하여 스마트시티에서 제공하는 서비스를 개선 및 발전하는 데 활용 가능
스마트 재해재난 대응	본 기술은 기상 및 지형 정보 등 여러 응용 분야가 연계된 정보가 필요한 재해재난 대응 분야에서 재난·재해의 다양한 원인 및 영향을 분석하고자 하는 데 활용 가능

주간기술동향 원고 공모

정보통신기획평가원은 주간기술동향의 ICT 기획시리즈에 게재할 “메타버스” 분야 원고를 모집하고 있습니다.

관심 있는 전문가 분들의 많은 참여를 바랍니다.

□ 원고 주제 : 차세대보안 관련 기술·시장·정책 동향

(※ 제목과 목차는 저자가 자율적으로 결정)

□ 제출 자격 : 원고 모집 분야의 전문가

□ 접수 기간 : 2023년 7월 16일 ~ 2023년 9월 15일(수시접수)

□ 제 출 처 : 주간기술동향 원고접수메일(wttrends@iitp.kr)로 제출

□ 원고 양식 : 파일참조(원고양식)

□ 원고 분량 : 12페이지 내외

□ 기타

- 원고 심의절차를 통과한 원고만 게재되므로 원고제출 시 반드시 원고심의의뢰서(첨부파일참조)를 함께 제출하여 주시기 바랍니다.
- 게재된 원고에 대하여 소정의 원고료 지급(200자 원고지 10,000원/1매, 최고 40만 원)
- 기획시리즈 칼럼은 매주 1편씩 발간 예정
- 게재된 원고로 인해 지적재산권 침해문제가 발생할 경우, 원고저자는 원고료 반환, 게시물 삭제 및 정보통신기획평가원이 입게 될 손실·비용에 대한 배상 등의 불이익을 받을 수 있습니다.

□ 제출 및 문의처

- (34054) 대전광역시 유성구 유성대로 1548 정보통신기획평가원
미래정책단 동향분석팀 주간기술동향 담당
- Tel : 042-612-8296, 8241 / Fax : 042-612-8209 / E-mail : wttrends@iitp.kr

- 사업책임자: 임진국(미래정책단장)
- 과제책임자: 허창희(동향분석팀장)
- 참여연구원: 이효은, 조성선, 도승희, 고은영, 임양섭, 최동렬,
유영신, 반치호, 장예지, 김채리, 김도현, 윤종혁

주간기술동향

통권 2100호(2023-24)

발행년월일 : 2023년 7월 19일

발행소 :  정보통신기획평가원

편집인겸 발행인 : 전성배

등록번호 : 대전 다-01003

등록년월일 : 1985년 11월 4일

인쇄인 : 예송미디어

 정보통신기획평가원

(34054) 대전광역시 유성구 유성대로 1548(화암동 58-4번지)

전화 : (042) 612-8296, 8241 팩스 : (042) 612-8209



깨끗한 IITP, 신뢰받는 IITP

IITP 정보통신기획평가원
<http://www.iitp.kr>



IITP 부정비리 신고센터