인공지능(AI) 보안 분야 국가별 대응 현황

오다인
더 리더블 편집장 | ohdain@thereadable.co

들어가며: AI가 앞당긴 보안 담론의 주류화

우리말로 보안(保安)은 보전해 편안한 상태를 뜻하며, 영문으로는 위험이나 공포로부터 자유로운 상태를 가리키는 '시큐리티(Security)'와 통용된다. 정보기술(IT) 분야에서는 정보보호의 의미로 쓰이는데, 2020년 이전까지 보안이 본격적인 사회 이슈로 거론된 적은 국내외를 아울러 거의 없었다. 헤드라인에 보안이 등장하는 경우는 청와대, 언론사, 은행 등 웹사이트를 만 3일 동안 마비시키며 약 360억 원에서 540억 원의 손해를 입힌 2009년 7.7 디도스(Distributed Denial of Service, 분산 서비스 거부) 공격 사건[1]이나 150개국 컴퓨터 30만 대를 감염시킨 2017년 5월 '워너크라이(WannaCry)' 랜섬웨어 공격[2]과 같이 피해 정도가 극심한 사고에 국한됐다. 대형 사고로 인해 보안 문제가 드물게 화두에 오르면 그동안의 허술함을 질타하는 기사가 쏟아지고 여론이 들끓어 보안 예산이 잠깐 늘어나기도 하지만, 이마저도 급속히 사그라드는 것이 십수 년간의 패턴이었다.

인공지능(Artificial Intelligence, 이하 'AI')의 부상은 보안 담론을 주류화하면서 이런 패턴에 균열을 일으키고 있다. '보안의 내재화(Secure by design)'는 AI가 제기하는 새로운 위협에 대한 가장 강력한 대응책으로 주목받고 있으며, 미국과 영국을 비롯한 세계 각국은 AI 기술 주도권을 쥐려는 경쟁에서 보안과 안전을 핵심 가치로 언급하고 있다. AI는 기술 역사상 인류에 대한 유례없는 파급력을 드러내며 기술의 사용자인 인간을 불안(Insecure)에 몰아넣고, 이로써 안전한 상태인 시큐리티를 갈급하게 만든다. AI 시대 보안은 더 이상 해도 그만, 안 해도 그만인 사족(蛇足)이나 예산 낭비가 아니라 각 기관과 기업, 심지어 개인이 최소한의 역량을 배양해야만 하는 국가 번영의 필수 요소로 떠올랐다.

AI 시대 새로운 위협, 가짜뉴스

AI는 기존 보안에서 고려되지 않았던 이슈들을 이 분야로 빠르게 흡수하고 있다. 대표적인 예가 가짜뉴스다. 뉴스는 여론을 만드는 1차 재료이자 역사의 기록물이기도 한데, 생성형 AI(Generative AI)가 폭발적으로 성장하면서 실제 처럼 보이는 가짜뉴스를 방대한 규모로 생산, 민주주의를 교란하고 일반 시민의 삶에 악영향을 끼치고 있다. 생성형 AI는 인터넷에서 수집·학습한 대규모 언어 모델(Large Language Model)을 바탕으로 마치 인간처럼 질문에 답하는 기술 서비스[3]다. 지난해 3월 신원미상의 공격자는 볼로디미르 젤렌스키 우크라이나 대통령이 러시아에 항복을 선언하는 영상을 AI로 사실처럼 꾸민 뒤 사회관계망서비스(SNS)를 통해 퍼뜨렸다. 음란물에 특정인의 얼굴을 입힌 뒤 유포하는 신종 범죄, 가족 구성원의 목소리를 베껴 긴급 상황을 조장 및 금전을 갈취하는 보이스피싱, 유명 배우의 이미지를 활용해 만든 광고 영상도 AI 기술 발전에 따라 실제와 구별하기 어려운

1 국회입법조사처, 「'7.7 DDoS 사고' 대응의 문제점과 재발방지 방안」, 현안보고서 제48호, 2009, 2쪽
2 김진, "美 국토안보부 '랜섬웨어 공격자 7800만원 챙겨'", 뉴스1, 2017.05.16., https://m.news1.kr/articles/?2994562
3 한정훈, 「생성형 AI 시대의 개막」, 한국방송통신전파진흥원, 미디어 이슈 & 트렌드 제55호, 2023, 이슈 리포트 1쪽

수준까지 정교화[4]됐다. 올해 5월 미국은 국방부 청사 인근에서 대규모 폭발이 발생했다는 가짜뉴스가 합성 사진과 함께 퍼지는 바람에 다우존스, S&P 등 주요 증시가 하락[5]하는 사태도 벌어졌다. 개인의 삶과 평판을 피폐화하고 경제적 권리를 갉아먹으며 국가 경제와 안보에 영향을 끼치는 AI 악용 사례가 이미 일상과 세계 곳곳에서 발견된다.

AI 기반의 딥페이크(Deepfake) 영상은 이제 약 3만 원이면 제작해주는 서비스까지 나온 상황이지만, 처벌은 고사하고 탐지조차 쉽지 않은 것으로 알려졌다[6]. 사회적 피해가 커짐에 따라 국가별 AI 정책에서 가짜뉴스 대응은 상당히 비중 있게 언급된다. 일례로 윤석열 대통령은 지난 9월 국무회의에서 "AI와 디지털 오남용이 가짜뉴스 확산을 만들어내고 있다"면서 "가짜뉴스 확산을 방지하지 못한다면 자유민주주의와 시장경제가 위협받고 우리 미래와 미래 세대 삶 또한 위협받게 된다[7]"고 말했다. 이보다 8일 앞서 대통령실은 성명을 내고 "가짜뉴스는 민주주의 최대 위협 요인"이라고 밝히기도 했다. AI로 인해 가짜뉴스 판별이 갈수록 어려워지는 가운데 정보의 무결성은 국가 안보의 축이자 사회 근간으로 인식된다. AI를 악용한 가짜뉴스의 생성 및 확산은 여론 조작, 선거 개입, 사회 분열을 조장하는 새로운 위협으로 등장하면서 각국 위기의식도 높아졌다.

AI 보안 위협과 국가별 대응책 1: 미국과 영국 현황

매년 미국 샌프란시스코와 라스베이거스에서 열리는 RSA, 블랙햇(Black Hat), 데프콘(DEF CON) 등 국제 보안 콘퍼런스에서는 AI 보안 위협을 둘러싼 정책적, 기술적 논의가 집중적으로 펼쳐지며, 위협 행위자(Threat Actor)가 AI를 활용할 때 어떤 시나리오가 가능한지, 나아가 실제로 구현될 가능성은 있는지 탐색하는 발제 및 토의의 시간이 마련된다. 보안 기업 체크포인트가 발표한 보고서에 따르면, 올해 1월 오픈AI의 '챗GPT(ChatGPT)'를 사용해 악성코드와 피싱 이메일 등 해킹 도구를 개발[8]한 사례가 포착됐다. 해커들은 챗GPT를 활용해 랜섬웨어, 키로거(사용자가 키보드를 통해 입력한 데이터를 중간에서 가로채는 해킹 기술) 등을 만들고 이 같은 방법을 다크웹 등 사이버 범죄 커뮤니티에서 공유했다. 체크포인트는 보고서에서 "챗GPT 언어모델이 정교해지면 사이버 범죄자들은 간단한 명령어만으로 악성코드나 피싱 이메일 프로그램을 쉽게 개발할 수 있다"면서 "초보 해커도 손쉽게 피싱 범죄에 가담하는 등 사이버 범죄 진입 장벽이 대폭 낮아질 것"이라고 우려했다.

AI 보안 분야 국가별 대응은 크게 AI 발전에 따른 보안 위협 대응과 AI를 활용한 보안 기술 개발 등 두 가지 갈래로 나타난다. AI가 산업 전반에 급속히 적용되는 가운데 이용자 보호를 위한 규제는 어떻게 마련할지, 효과가 있을지, AI와 보안에 대한 기술 리터러시 및 인식은 어떤 방식으로 제고할지 정책적 움직임이 활발하다. 개인정보 보호, 프라이버시 영역도 AI 보안 이슈에서 빠지지 않고 거론된다. AI가 학습하는 데이터에는 개인정보가 포함되는데, 단순한 보호를 넘어 기술과 사회 발전을 위해 민감 정보라도 적정한 활용이 필요하다는 의견이 있으며, 챗GPT 관련 논란에서 불거졌듯 기밀 정보, 유료 정보를 노출하는 생성형 AI를 어떻게 규제할 것인지도 아직 해결되지 않은 화두로 남아 있다. 국가 안보와 국방의 영역에서 AI는 더욱 엄정하게 검토된다. AI 조력자의 판단을 어느 정도로 신뢰할 수 있을지, 그 근거와 기준은 무엇으로 만들 수 있을지 다국적 회의체와 수면 아래 대화가 급격하게 늘어났다. 일례로 네덜란드는 군사 AI에 관한 국제회의를 신설하고 이 분야에서 책임 있는 AI 사용을 촉구[9]하기 시작했다. 아직 국제사회에서 AI와 안전에 관한 규범이 확립되지 않은 시기인 만큼 미국과 영국, 유럽에서 이 분야 주도권을 가져가기 위한 노력도 포착된다.

미국은 최근 싱가포르에서 폐막한 '싱가포르 인터내셔널 사이버 위크(SICW)' 행사에서 보안 내재화 가이드라인 '사이버보안 리스크의 균형 전환: 보안 내재화 소프트웨어를 위한 원칙과 접근(Shifting the balance of cybersecurity risk: principles and approaches for secure by design software)' 업데이트를 발표하고 생성형 AI가 하나의 소프트웨어로 간주되는 만큼 이 가이드라인에 포함된다고 선언[10]했다. 젠 이스털리(Jen Easterly) 미국 사이버보안및인프라보안국(CISA) 국장은 지난 10월 17일 SICW의 고위급 패널 세션에 참석해 "AI는 현시대 가장 강력한 무기가 될 것이며 안전과 보안을 고려해 제작돼야 한다"고 강조했다. 이날 발표에 따르면 미국이 주도하는 보안 내재화 가이드라인에는 기존 6개 파트너에 체코, 이스라엘, 싱가포르, 한국, 노르웨이, 일본을 포함한 7개 파트너가 새롭게 추가되면서 총 13개 국제 파트너들이 참여한다.

미국 바이든 행정부는 지난 10월 30일 안전하고 신뢰할 수 있는 AI에 관한 행정명령에

4 이상덕·황순민, "전쟁 가짜뉴스 온상 지적에 SNS 부랴부랴 대책 쏟아내", 매일경제, 2023년 10월 18일, A5면

5 김대은, "생성형 AI가 연 판도라 상자…'가짜가 세상을 흔든다'", 매일경제, 2023.06.18., https://www.mk.co.kr/news/it/10762679

6 이상덕·송경은·황순민, "3만원이면 AI영상 찍어내는데…범죄악용 처벌근거 찾기 하세월", 매일경제, 2023년 10월 18일, A5면

7 김동하, "尹 '가짜뉴스 못막으면 자유민주주의에 위협'", 조선일보, 2023.09.13., https://www.chosun.com/politics/politics_general/2023/09/13/C626FI4CUZET5MYEZEKFH5RZRA/

8 배한님, "비밀번호 털어간 초보 해커, 공범은 '챗GPT'?", 머니투데이, 2023.02.06., https://news.mt.co.kr/mtview.php?no=2023020516292249550

9 Kuksung Nam, "[REAIM 2023] International community calls for responsible use of AI in military", The Readable, 2023.02.17., https://thereadable.co/reaim-2023-international-community-calls-for-responsible-use-of-ai-in-military/

10 Kuksung Nam, "US aims to secure generative AI with updated guideline", The Readable, 2023.10.18., https://thereadable.co/us-aims-to-secure-generative-ai-with-updated-guideline/

서명[11]했다. 이날 연설에서 바이든 대통령은 딥페이크의 정교함을 언급하면서 AI 규제 필요성[12]을 강조했다. 미국 바이든 행정부는 올해 AI 선도기업이 자율적인 책임을 지도록 촉구하면서 해당 기업과 연방정부 협업을 기축으로 한 이니셔티브를 마련하기도 했다. 지난 7월 바이든 행정부는 AI가 제기하는 위협에 대해 AI 선도기업의 자율적인 헌신을 요청하면서 아마존, 앤트로픽, 알파벳, 인플렉션, 메타, 마이크로소프트, 오픈AI 등 7개 기업이 AI 시스템의 보안과 기능을 테스트하고 기술이 사회에 미치는 위험에 관한 연구에 투자하며 시스템의 취약성에 대한 외부감사를 촉진하기로 하는 데 자발적으로 합의[13] 했다고 밝혔다. 이른바 'AI 안전 서약'에는 AI를 책임 있고 안전하게 사용할 것을 약속하는 8개 조항이 포함됐다. 약 2주 뒤에는 'AI 사이버 챌린지(AI Cyber Challenge)[14]'를 잇달아 내놨다. 이는 미국 기반시설과 인터넷을 보호하기 위해 미국 정부가 출범시킨 AI 보안 분야 최신 이니셔티브로 AI 선두기업 네 곳(앤트로픽, 구글, 마이크로소프트, 오픈AI)과 방위고등 연구계획국(DARPA)이 파트너십을 맺고 향후 2년간 AI를 활용해 소프트웨어 취약점을 식별 및 해결하는 대회로 구성됐다.

영국은 지난 8월 '국가 위험 등록부(National Risk Register) 2023'을 발간하면서 AI를 영국에 대한 보안 위협으로 명시[15]했다. 이어 지난 9월에는 정부 공식 발표를 통해 두 달 뒤인 11월 AI 안전에 관한 국제 회담(AI Safety Summit)을 개최한다고 발표했다. AI 보안과 안전 분야에서 주도권을 잡으려고 하는데, 회담의 목표를 다섯 가지로 아래와 같이 제시[16]했다.

[표 1] AI 안전에 관한 국제 회담(AI Safety Summit)의 5대 목표

1. AI 신기술에 따른 리스크와 필요한 행동에 관한 공통된 이해
2. 국가 및 국제 프레임워크를 비롯한 AI 신기술 안전 분야 국제 협력 추진
3. AI 신기술 안전성 제고를 위해 각 조직이 취해야 할 조치들
4. AI 안전성 연구에 대한 잠재적 협력 분야: 모델 역량 평가, 거버넌스 지원을 위한 새로운 표준 개발 등
5. AI 개발 안전성 확보는 AI를 세계와 공익을 위해 활용하는 방안이라는 것을 제시

11 The White Hose, "President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence", https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

12 오로라, "'AI 훈련부터 서비스까지 정부 통제' 바이든, 초강력 행정명령 서명", 조선일보, 2023.10.31, https://www.chosun.com/economy/tech_it/2023/10/31/NHTF6SQKRJCW5OFX3IZXBK5USI/

13 The White House, "Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI", https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/

14 The White House, "Biden-Harris Administration Launches Artificial Intelligence Cyber Challenge to Protect America's Critical Software", https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/09/biden-harris-administration-launches-artificial-intelligence-cyber-challenge-to-protect-americas-critical-software/

15 Michael Hill, "영국, AI를 장기적 보안 위협으로 공식화", CIO, 2023.08.04., https://www.ciokorea.com/news/302215#csidxfdb5a29258dd18299e8bd55e8383152.

16 The U.K. Government Department for Science, Innovation and Technology, "UK government sets out AI Safety Summit ambitions", 2023.09.04., https://www.gov.uk/government/news/uk-government-sets-out-ai-safety-summit-ambitions

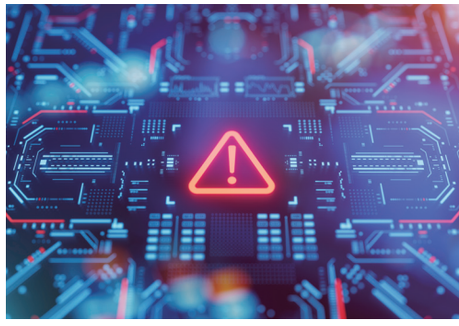
AI 보안 위협과 국가별 대응책 2: 아태지역과 유럽 현황

호주는 2019년 11월 연방과학산업연구기구(CSIRO)를 통해 AI 로드맵을 발표하면서 보안을 AI 시대 핵심 요인으로 꼽았다. 이 로드맵은 AI 개발 지원을 위한 사이버보안 요구사항을 언급하고 AI 데이터 보안에 관한 새로운 표준이 필요하다고 언급했다.

유럽연합은 지난 6월 세계 최초로 인공지능법(AI Act)을 채택[17]했다. AI에 관한 광범위한 규제로, AI를 활용하는 모든 제품과 서비스가 규제의 대상이 된다. 2021년 처음 제안된 이 법은 AI 시스템을 위험 수준에 따라 네 단계로 구분하며, 어린이 등 취약계층을 대상으로 한 앱일수록 더 강력한 규제를 적용하도록 설계됐다.

캐나다는 일원화한 사이버안보 컨트롤타워인 '캐나다 사이버보안 센터(Canadian Centre for Cyber Security)'를 운영하면서 일반 국민이 이해할 수 있는 언어로 보안 정책을 알리고 있다. 인공지능(AI)과 생성형 AI 부상에 따른 위기 요인도 함께 설명하고 있다.

중국, 일본, 싱가포르에서도 AI 보안 대응을 위한 움직임이 최근 급속도로 진전하고 있다. 중국은 2023년 9월 클라우드 보안 연맹(CSA)의 자국 내 'AI 보안 워킹그룹'을 결성[18]했다. 이는 AI 보안 기술 연구를 위한 중국 대기업과 연구기관 간 협업 이니셔티브로서 차이나텔레콤, 앤트그룹, 화웨이, 바이두, 바이트댄스, 시안전자과기대학, 국가금융평가센터 등 30여 개 기업 및 기관이 참여하는 것으로 알려졌다. 두 달 앞선 7월에는 중국 국가인터넷정보판공실이 '생성형 AI 산업 관리 임시규정'을 발표하면서 생성형 AI 서비스 제공자가 서비스를 당국에 등록하고 제품 출시 전 보안 평가를 수행해야 한다고 밝혔다.



일본은 2022년 6월 사이버 보안에 관한 행동계획[19]을 발표했다. 2013년 동북아 국가 중 최초로 사이버 위협 주체와 대상을 명시한 '사이버 안보 전략'을 발표한 바 있으며 해당 전략에서 일본 정부는 "일본은 동맹 및 선진국과의 사이버 방어, 억지, 공세적 능력구축 협력과 함께, 동남아시아에 대한 역량구축 지원을 정보기술, 인공지능, 로봇공학 등의 기술경쟁과 연계해 추진"한다고 선언했다.

싱가포르는 2019년 11월 국가 AI 전략을 발표하고 이를

17 Kelvin Chan, "How Europe is leading the world in the push to regulate AI", AP News, 2023.06.14, https://apnews.com/article/ai-act-artificial-intelligence-europe-regulation-94e2b38703b38fdbfabc9580f845ef9a

18 유효정, "中 화웨이·바이두·바이트댄스 등 'AI 보안 그룹' 결성", 지디넷코리아, 2023.09.08., https://zdnet.co.kr/view/?no=20230908012515

19 글로벌 과학기술정책정보 서비스, "일본, 「사이버 보안에 관한 행동계획」 발표", 2022.06.17., https://now.k2base.re.kr/portal/trend/mainTrend/view.do?poliTrndId=TRND0000000000046882&menuNo=200004&pageIndex=

전담하는 '스마트네이션 및 디지털 정부청(SNDGO)'을 출범[20]시켰다. 이를 통해 2025년까지 싱가포르 전역에 적용 가능한 독립형 5G를 구축하고 차세대 통신 인프라 구축을 위한 인공지능과 사이버보안 연구를 지원하겠다고 밝혔다.

우리나라는 지난 4월 AI 주도권 확보를 위한 대통령 발표가 나온 이후 디지털플랫폼정부위원회, 개인정보보호위원회를 주축으로 한 AI 기술개발 및 보안 대응이 활발하다. AI 시대에 발맞춰 데이터 보호 정책 방향으로 '규정' 중심에서 '원칙' 중심으로 규제 패러다임을 전환한다고 선언한 것이다. 국가정보원은 지난 6월 챗GPT 보안 가이드라인을 발표[21]했다. 앞서 우리 정부는 2019년 10월 AI 국가 전략을 발표한 바 있으며, 세부적으로는 2021년 사이버작전사령부와 국가정보자원관리원 간 'AI 등을 활용한 최신 사이버 보안기술 및 위협정보 공유를 위한 업무협약'이 체결되는 등 국가 안보와 국방을 위한 AI 보안 기술 개발 사업도 추진돼 왔다.

[표 2] AI 보안 분야 국가별 대응 현황

국가	내용
미국	• 2023년 10월 바이든 행정부 "안전하고 신뢰할 수 있는 AI에 관한 행정명령"에 서명 • 2023년 10월 싱가포르 인터내셔널 사이버 위크(SICW) 보안 내재화 가이드라인 업데이트 발표 시 생성형 AI가 소프트웨어의 일종으로서 해당 가이드라인에 포함된다고 선언 • 2023년 8월 DARPA와 AI 기업 간 취약점 발굴 이니셔티브 'AI Cyber Challenge' 발표 • 2023년 7월 오픈AI 등 7개 AI 선두기업과 'AI 안전 서약' 발표
영국	• 2023년 8월 '국가 위험 등록부(National Risk Register)'를 발간하면서 AI를 영국에 대한 보안 위협으로 명시 • 2023년 11월 정부 주도의 'AI Safety Summit' 개최, 이른바 "블레츨리 선언"에서 28개국 대표단 합의 발표. AI 안전에 관한 다섯 가지 주요 목표 제시
호주	• 2019년 11월 연방과학산업연구기구(CSIRO), 'AI 로드맵' 발표. 로드맵에서 AI 개발 지원을 위한 사이버보안 요구사항을 언급하고 AI 데이터 보안에 관한 새로운 표준이 필요하다고 강조
유럽연합	개인정보보호, 책임 있는 AI를 중심으로 한 지속적인 법 제·개정 • 2019년 4월 신뢰할 수 있는 AI를 위한 윤리 지침 • 2019년 6월 신뢰할 수 있는 AI를 위한 정책 및 투자 권장 사항 • 2020년 2월 "AI에 대한 우수성과 신뢰에 대한 유럽의 접근방법" 백서 • 2023년 6월 인공지능법(AI Act) 채택: AI 시스템을 위험 수준에 따라 네 가지로 분류. 2026년 시행 예정
캐나다	• 캐나다는 일원화한 사이버안보 컨트롤타워인 '캐나다사이버보안센터(Canadian Centre for Cyber Security)'를 운영하면서 일반 국민이 이해할 수 있는 언어로 보안 대응 정책 등을 알리고 있음. 해당 센터에서 AI와 생성형 AI에 대한 위기 요인도 설명
중국	• 2023년 9월 7일 클라우드 보안 연맹(CSA)의 중국 'AI 보안 워킹그룹' 결성. AI 보안 기술 연구를 위한 중국 대기업과 연구기관 협업 이니셔티브. 차이나텔레콤, 앤트그룹, 화웨이, 바이두, 바이트댄스, 시안전자과기대학, 국가금융평가센터 등 30여 개 기업 및 기관이 참여 • 2023년 7월 중국 국가인터넷정보판공실, '생성형 AI 산업 관리 임시규정'을 발표하면서 생성형 AI 서비스 제공자가 서비스를 당국에 등록하고 제품 출시 전 보안 평가를 수행해야 한다고 규제
일본	• 2022년 6월 사이버 보안에 관한 행동계획 발표 • 2013년 동북아 국가 중 최초로 사이버 위협 주체와 대상을 명시한 사이버 안보 전략을 발표: "일본은 동맹 및 선진국과의 사이버 방어, 억지, 공세적 능력구축 협력과 함께, 동남아시아에 대한 역량구축 지원을 정보기술, AI, 로봇공학 등의 기술경쟁과 연계해 추진"
싱가포르	• 2019년 11월 국가 AI 전략 발표. 이를 전담하는 '스마트네이션 및 디지털정부청(SNDGO)' 출범: 2025년까지 싱가포르 전역에 적용 가능한 독립형 5G 구축을 목표(2022년까지 50% 목표)로 차세대 통신 인프라 구축을 위한 AI와 사이버보안 연구 지원
한국	• 2019년 10월 AI 국가 전략 발표 • 2021년 사이버작전사령부-국가정보자원관리원, 'AI 등을 활용한 최신 사이버 보안기술 및 위협정보 공유를 위한 업무협약' 체결. • 2023년 4월 대통령실 발표. AI 시대 데이터 보호 정책 방향으로 '규정' 중심에서 '원칙' 중심으로 규제 패러다임 전환

나오며: 보안 인력난과 AI

AI 보안 대응책에서 빠지지 않는 이슈는 인력난이다. 보안 인력난은 지난 20년간 정보보호 산업의 고질적인 문제로 지적됐지만, AI 발전에 따라 더욱 복잡해졌다. 기존에 보안 직종은 업무의 중요성에 비해 대우가 현격히 떨어지는 문제가 있고, 사물인터넷(IoT) 확대 등 공격 표면이 급증하면서 보안 경보와 업무 과부하가 일상이 됐다, 보안 인력난을 마땅히 해결하지 못한 상황에서 AI 변수가 더해졌다. 이런 가운데 일각에서는 AI의 순기능을 활용할 경우 보안 업무와 경보 과부하의 돌파구가 마련될 것으로 기대[22]한다. 양날의 검인 AI를 보안의 위기로 남길지, 진화할 기회로 활용할지 가르는 시기, AI 보안 인력 양성을 위한 중장기 예산 증액을 기대한다.

20 대외경제정책연구원, 「스마트 국가 실현을 위한 최근 싱가포르 정부의 추진 현황」, 2023.06.20., https://www.emerics.org:446/businessDetail.es?brdctsNo=348608&mid=a30400000000&search_option=&search_keyword=&search_year=&search_month=&search_tagkeyword=&systemcode=03&search_region=&search_area=&currentPage=10&pageCnt=10

21 Dain Oh, "ChatGPT security guideline is published by Korean intelligence agency", The Readable, 2023.06.29., https://thereadable.co/chatgpt-security-guideline-is-published-by-korean-intelligence-agency/

22 Dain Oh, "'AI is an advantage to defenders,' says Mandiant CEO Kevin Mandia", The Readable, 2023.09.21., https://thereadable.co/ai-is-an-advantage-to-defenders-says-mandiant-ceo-kevin-mandia/