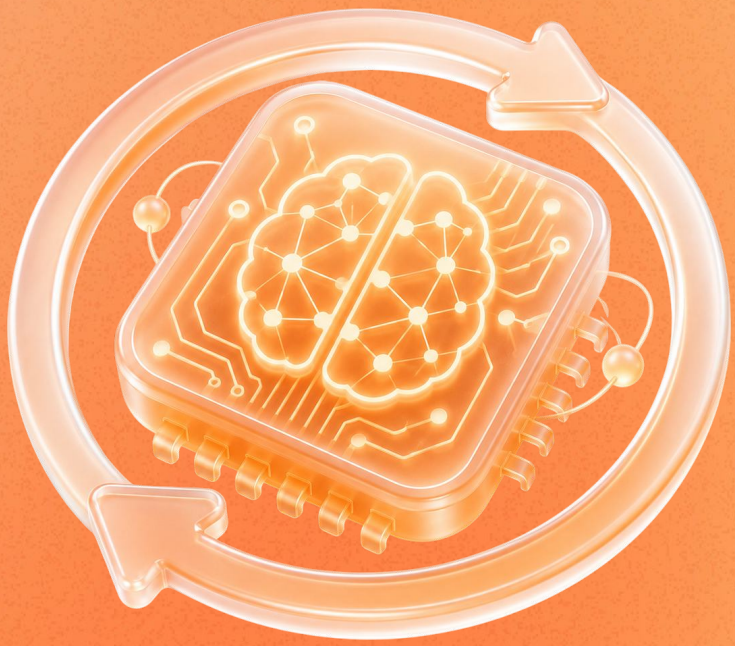
KISTEP 브리프 I 이슈페이퍼



알파고 등장 이후 10년, AI 패러다임 전환에 따른 7대 주요 이슈와 과학기술적 역할

저자 | KISTEP 전략기술정책센터 박노언 외

KISTEP

KISTEP 브리프

알파고 등장 이후 10년, AI 패러다임 전환에 따른 7대 주요 이슈와 과학기술적 역할

2026.11.13. 전략기술정책센터 박노언 센터장, 성장동력투자전략센터 채명식 연구위원, 성장동력투자전략센터 김주일 선임전문관리원, 정두엽 부연구위원, 허아람 선임전문관리원, 김동혁 연구원, 박윤경 연구원

요약문

□ 작성 배경

○ 알파고 등장('16) 이후 AI는 지난 10년 간 분석·예측 도구에서 생성형·에이전틱·피지컬 AI로 진화하며, 국가 혁신체계 전반의 경쟁을 촉발

○ 경쟁의 단위가 개별 모델의 성능·규모에서 컴퓨팅·반도체·데이터·인재·전력·안전·국제규범으로 확대되고, 산업·공공서비스 혁신을 넘어 과학적 발견·국가안보·공급망에 영향을 미치는 전략자산으로 부상

○ 미국은 AI 기술의 글로벌 우위를 기반으로 가치사슬 전반의 지배력을 강화하고 있으며, 중국은 글로벌 사우스를 중심으로 AI 외교 추진 및 최근에는 AI 기술의 수출 제한 및 통제 확대

○ 우리나라도 AI 기본법과 범정부 추진체계를 기반으로 AI 경쟁력을 높이고, 글로벌 거버넌스·공급망 협력 및 국제표준 개발에 참여하여 국제 대응역량 제고 추진

○ 기술주도 성장과 경제안보의 핵심 기술인 AI 분야의 국내 현주소를 진단하여 과학기술의 역할과 방향을 구체화할 필요

○ 본고는 최근 정부의 정책방향과 언론보도 등을 종합적으로 분석하여 AI 분야 7대 이슈*를 선정하고, 이슈별 국내외 동향과 우리나라의 현주소를 진단하여 과학기술적 대응방향을 제시

* ① 독자 AI 모델·인프라 확보를 통한 AI 주권 경쟁 심화, ② AI 기반 사이버·안보 위협의 지능화, ③ (산업 AX) 피지컬 AI 확산 및 AI-산업 융합 본격화, ④ (공공 AX) 국민체감 및 문제해결형 공공 AI 서비스 확대, ⑤ AI for Science와 과학기술 R&D 패러다임 전환, ⑥ AI 지식자원의 전략 자산화, ⑦ AI 지정학 블록화와 글로벌 AI 거버넌스 재편

□ AI 분야 핵심 이슈와 우리나라의 현주소

○ (AI 주권 경쟁 심화) 독자 모델·컴퓨팅·국산 반도체 육성을 적극 추진하고 있으나, 주요국 대비 자본·컴퓨팅 격차에 대응할 집중 분야와 개발-활용 간 연계 제한적

○ (사이버·안보 위협의 지능화) 보안 평가·취약점 탐지·패치 기술개발을 확대하고 있으나, 운영환경의 위험 검증부터 사고 통제·복구까지 전주기 대응 한계

○ (피지컬 AI 확산과 AI-산업 융합 본격화) 제조·모빌리티·로봇 실증사업을 확대하고 있으나, 생산성·안전성·경제성 검증과 핵심부품·데이터 기반 확보 부족

○ (국민체감 및 문제해결형 공공 AI 서비스 확대) 임무 기반 AI R&D와 공공 인프라 지능화를 추진하고 있으나, 부처 간 데이터 연계와 현업 전환·성과 환류 다소 부족

○ (AI 기반 연구개발 패러다임 전환) 컴퓨팅·모델·자율실험실·데이터 기반 강화를 추진하고 있으나, 데이터 재사용·연산 접근성과 장비 자동화·연계의 제약 존재

○ (AI 지식자원의 전략 자산화) 인재양성과 데이터 구축·개방을 확대하고 있으나. 인재의 국내 정착·현장 활용 및 데이터 유통·활용 기반 한계

○ (AI 지정학 블록화와 글로벌 AI 거버넌스 재편) AI 기본법 수립 등 법·제도 정비와 국제협력 프로그램에 참여하고 있으나 글로벌 AI 거버넌스와 규범을 주도하기보다는 수용적 입장

□ 정책 제언

○ (선택적 AI 주권 확보) 국내 강점 분야의 전략적 R&D와 보안·활용 목적별 국내외 AI 도입을 병행하여 선택적 기술 우위와 국가적 자율성 확보 필요

- 핵심 분야를 중심으로 성능·비용·전력 효율을 종합 검증하고, 독자 모델 역량 축적과 업무별 국내외 AI 활용, 공공 실증·조달을 통한 국산 기술 개선·도입을 연계

○ (안전·신뢰·책임성 내재화) 위험 수준에 따른 전주기 평가·검증과 운영·사고 대응을 연계하고, 국제표준 및 시험·인증체계 간 협력 강화 필요

- 데이터 권리·품질, 모델 투명성, 에이전트 권한 및 물리적 안전 검증을 운영·통제·복구와 연계하고, 국제 협력체계·표준·법적 의무를 구분하여 표준·시험방법 협력과 평가 결과의 상호 활용 추진

○ (현장 성과 중심의 AX) 산업·공공·과학 분야의 실증·공동 활용 기반을 확대하고, 세제·금융·바우처 지원을 통해 현장 도입과 성과 확산 촉진 필요

- 산업·공공의 AI 생산성·안전·사회적 편익을 검증하고, 과학 분야는 연산·데이터·실험장비·통합제어 시스템을 연계해 폐쇄루프 연구체계를 구현

○ (인재·데이터의 지속적 활용·축적) 우수 인재의 국내 정착과 범부처 AX 인재 양성체계를 강화하고, 데이터 연계·통제권 보장을 통해 활용·축적의 선순환 구축 필요

- 연구환경·보상·정주 여건과 수요 기반 교육·배치를 개선하고, 데이터 생산·품질관리·제공에 대한 지원·보상 및 공통 메타데이터·표준 API 기반의 안전한 교환·재사용 촉진

○ (AI 가치사슬 연계) 반도체·전력·데이터 등 가치사슬 전반의 연계를 강화하고, 기술개발부터 현장 운영까지의 성과를 후속 R&D·인재 양성·제도 개선에 환류 필요

- 반도체, AI 등 각 분야별 정책과 사업관리에서 벗어나 AI 가치사슬 전반을 고려한 통합 관리가 요구되며, 개발–검증–실증–운영 성과를 후속 연구·인재·데이터·제도 개선에 반영

1 현황 및 배경

□ 인공지능(Artificial Intelligence, AI) 기술의 급속한 발전과 서비스 확산으로 경제·사회 전반의 AI 전환 가속화

❍ AI 기술이 데이터에 기반해 특정 업무를 분석·예측하는 도구(Tool)에서 인간의 지적 활동을 보조·대체하고 스스로 추론하는 범용 기반 기술로 빠르게 진화

- ('10년대 후반) 알파고('16)를 계기로 AI에 대한 대중적 관심과 산업적 기대가 크게 확대되었으며, 데이터에 기반해 단일 목적·특정 업무 수행에 AI 기술 적용 확대

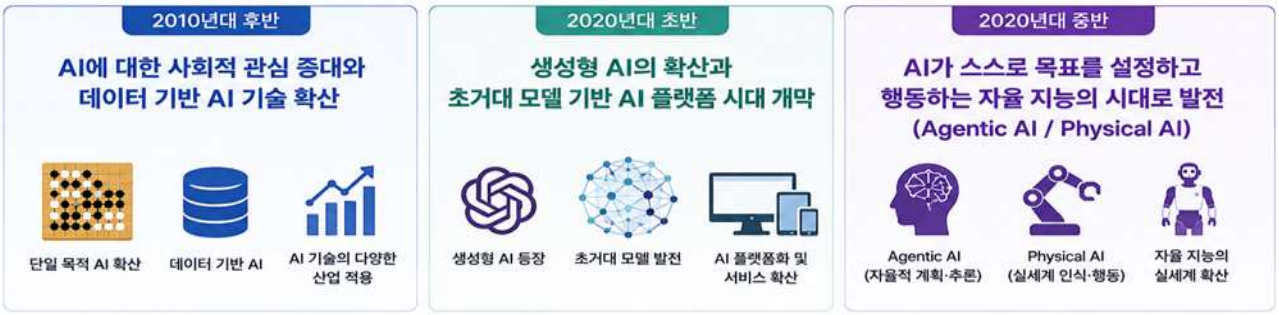
  ※ ('16)AlphaGo, 이세돌 9단과의 대국 승리, ('17)「Attention Is All You Need」 발표를 통한 파운데이션 모델의 기술적 기반 마련, ('18)BERT(Google) 발표로 사전학습·미세조정 기반 자연어처리 확산 등

- ('20년대 초반) 생성형 AI 대중화와 파운데이션(Foundation) 모델의 발전 이후 초거대 모델이 다양한 언어·이미지·코드 등을 활용하여 업무를 수행하는 AI 플랫폼으로 발전

  ※ ('20)AlphaFold2를 통한 단백질 구조 예측(DeepMind), ('20)GPT-3 등 초거대 언어모델 등장, ('22~'25)생성형 AI의 대중적 확산 및 추론·효율성 경쟁으로 확대(Open AI/Meta/Google 등) 등

- ('20년대 중반) Agentic AI, Physical AI 등이 발전하면서 AI가 보조적 수단에서 벗어나 목표 설정→계획 수립→행동까지 수행하는 방향으로 발전

  ※ ('25)VLA 기반 휴머노이드 적용 확대(Figure 등), ('26)Claude Mythos Preview의 사이버보안 역량 공개와 제한적 접근 제공(Anthropic), ('25~)Agentic AI 본격 확산, 휴머노이드 고도화 등



※ 생성형 AI로 도식화

[그림 1] 인공지능(AI) 기술의 발전단계

❍ AI의 활용이 산업 생산성 향상에서 국가·경제 안보와 과학기술 혁신 수단으로 확대되면서 전략 자산으로서의 중요성 증대

- AI 경쟁력을 좌우하는 요소가 기존 고성능·프론티어 모델 개발에서 AI 반도체, 데이터, 전력·용수 인프라 등 전체 가치사슬 전반으로 확산

- AI 윤리 원칙(인간 중심성, 투명성 등)을 법·제도로 구체화하고, 생성형·프론티어 AI 확산으로 제도화 단계(규제·표준·시험·인증 등)로 전환

- AI가 국가 경쟁력·시장접근 조건으로 부상함에 따라 국내 규제를 넘어 수출통제와 국제표준을 둘러싼 국가 간 AI 거버넌스 경쟁으로 확대

〈표 1〉 AI 기술을 바라보는 시각의 변화

구분	과거		현재
모델	특정 목적용 AI		파운데이션 모델 기반 범용 및 산업 특화 모델
역량	생성(Generation)·수동(AI Assistant)		추론(Reasoning)·자율(Agentic AI)
공간	디지털 세계(Digital AI)	⇨	물리적 실현(Physical AI)
활용	AI for Digital		AI for Science
인프라	학습		학습·추론, AI 가치사슬 전반
경쟁	모델 성능 및 규모		효율성·생태계·안보

□ **정부는 경제·사회 전반의 AI 대전환을 촉진하고 글로벌 AI 3대 강국으로 도약하기 위해 다양한 정책과 법적 기반을 마련하고 있으며, 이를 뒷받침하기 위한 정책수단인 R&D예산 규모도 확대 추세**

○ 「인공지능 국가전략('19)」을 시작으로 AI 3대 강국 도약을 위한 다수의 정부 정책이 발표되었으며, 컨트롤타워 신설, 법 제정 등 AI 거버넌스 구축

- ('19년) IT 강국을 넘어 글로벌 AI 선도국으로 도약하기 위한 3대 분야-9대 전략-100대 과제 발표(「인공지능 국가전략」)

  ※ AI 생태계 구축(AI 인프라 확충, AI 기술경쟁력 확보, 규제혁신 및 법제도 정비 등), AI 활용(AI 인재양성 및 전 국민 AI 교육, 산업 AX 활용 전면화 등), 사람 중심의 AI 구현(일자리 안정망 구축, AI 윤리체계 마련 등)

- ('24년) 대통령 직속 컨트롤타워인 국가인공지능위원회 신설('24.9.) 이후 국가인공지능전략위원회로 확대·개편('25.9)

- ('25년) 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법(약칭 AI 기본법, '25.1)」을 제정하여 AI 산업 진흥, AI 투명성, AI 거버넌스 등 근거 마련

- ('26년) 국가 차원의 AI·데이터 거버넌스 정립과 AI 혁신을 가속화하기 위한 「대한민국 인공지능 행동계획('26.2)」 발표, 정부·민간·지역이 연계된 3대 메가프로젝트* 추진계획 발표('26.6)

  * 반도체, 피지컬 AI, AI 데이터센터 등 3대 분야에 민·관 합동으로 총 1,500조원 규모 투자 예정

○ AI 분야 정부R&D 예산규모('26)는 2.4조원으로 전년(1.1조원) 대비 118.2% 증가, '27년도 정부안은 4.1조원으로 '26년 대비 69.1% 증가

- 첨단 AI기술(피지컬 AI 및 범용인공지능 등) 및 AI 컴퓨팅·인프라에 투자를 확대하고, 안전·신뢰 원천기술 개발 및 능동형 AI 안전 핵심기술 확보 추진

- 과학기술혁신 및 국가난제 해결을 위해 분야별 파운데이션·특화 모델을 개발하고, 공공안전 AI 및 산업 도메인별 AI 융합으로 생산성 혁신을 가속화

- AI 대전환을 선도하는 AI·SW 핵심·융합 인재 양성을 확대하고, 연구개발 성과가 매출 창출 및 현장 확산 등으로 이어질 수 있도록 '초기 시장 창출'과 '레퍼런스 확보'에 투자 확대

〈표 2〉 인공지능 분야 주요 R&D사업 및 예산규모

(억원)

7대 이슈	부처	세부사업명 (내역사업명)	'25년	'26년
① 독자 AI 모델·인프라 확보를 통한 AI 주권 경쟁 심화	과기정통부	AI반도체를활용한K-클라우드기술개발 (AI반도체 데이터 센터 인프라 및 HW)	108.0	172.0
	과기정통부	AI반도체를활용한K-클라우드기술개발 (AI 반도체 데이터 센터 컴퓨팅 SW)	170.0	278.0
	과기정통부	AI반도체를활용한K-클라우드기술개발 (AI 반도체 특화 클라우드)	76.2	140.2
	과기정통부	인간인지기반AI핵심원천기술개발 (인간인지기반 AI 핵심원천기술개발)	-	100.0
② AI 기반 사이버·안보 위협의 지능화	과기정통부	한국과학기술정보연구원연구운영비지원 (AI-화이트해커기반해킹제로시스템개발)	-	65.6
	경찰청	사이버범죄수사단서통합분석및추론시스템개발 (사이버범죄대응기술)	35.0	59.0
	과기정통부	신종보이스피싱조기탐지기술개발 (범죄의심정보내개인정보비식별화기술개발)	45.0	50.0
	개보위	개인정보안전활용선도기술개발 (원본데이터안전활용기술개발)	-	45.6
③ (산업 AX) 피지컬 AI 확산 및 AI-산업 융합 본격화	과기정통부	협업지능피지컬AI기반SW플랫폼연구개발생태계조성 (협업지능피지컬AI기반SW플랫폼연구개발생태계조성)	-	766.7
	과기정통부	피지컬AI선도기술개발 (피지컬AI선도기술개발)	-	150.0
	산업부	산업용유무기혼합물물성예측AI파운데이션모델개발 (산업용유무기혼합물물성예측AI파운데이션모델개발)	-	150.0
	산업부	로봇산업기술개발 (휴머노이드로봇AX기술개발)	-	59.0
④ (공공 AX) 국민체감 및 문제해결형 공공 AI 서비스 확대	산림청	대형산불대응지능형솔루션기술개발 (AI기반대형산불대응지능형솔루션기술개발)	57.2	114.5
	기후부	환경보건빅데이터구축및AI활용고도화기술개발사업 (환경보건빅데이터구축및AI활용고도화)	-	67.0
	경찰청	불법마약류대응을위한현장기술개발 (멀티모달AI기반마약류추적탐지시스템개발)	-	15.0
⑤ (AI for Science) 연구개발 방식의 전환과 과학기술 혁신	과기정통부	AI+S&T혁신기술개발 (AI+S&T혁신기술개발)	-	45.0
	과기정통부	차세대AI+S&T기반기술개발 (차세대AI+S&T기반기술개발)	-	20.0
	과기정통부	국가과학기술연구회연구운영비지원 (국가과학AI연구지원센터)	-	400.0
⑥ AI 지식자원(데이터·인재)의 전략 자산화	복지부	국가통합바이오빅데이터구축사업 (바이오데이터뱅크구축운영)	317.2	497.4
	과기정통부	생성AI선도인재양성 (생성AI핵심고급인재)	87.0	270.0
	과기정통부	AI최고급신진연구자지원 (AI최고급신진연구자지원)	90.0	340.0
⑦ AI 기술·공급망의 블록화와 글로벌 AI 거버넌스 재편	과기정통부	디지털혁신기술국제공동연구 (디지털핵심기술국제공동연구)	54.6	78.0
	문체부	인공지능기반공연예술안전환경구축핵심기술개발 (공연안전글로벌표준화기술개발)	3.3	12.0
	해경청	차세대디지털VTS국제표준서비스및장비개발 (차세대디지털VTS국제표준서비스및장비개발)	12.0	37.7

□ AI 기술의 발전과 글로벌 환경변화에 대응하기 위해 주요 이슈별 현주소를 진단하고 과학기술의 역할과 방향을 구체화할 필요

❍ 최근 보도된 뉴스('26.1~7, ABC 뉴스 등 약 32만건)를 활용하여 BERTopic 기반으로 추출된 상위 50개 토픽(BERTopic) 중 과학기술 연관성과 정부 정책과제를 토대로, AI의 기술적 변화와 국가적 대응 필요성을 종합하여 7대 이슈 선정

- 각 이슈별 주요국 동향 및 국내 현황을 조사하고, 우리나라의 상황을 분석하여 과학기술의 역할 모색 및 개선방향 제시

〈표 3〉 인공지능 분야 7대 이슈 도출근거

뉴스 토픽	7대 이슈	「대한민국 인공지능 행동계획('26.2)」 전략과제
	①  독자 AI 모델·인프라 확보를 통한 AI 주권 경쟁 심화	■ AI고속도로 구축(AI 컴퓨팅 인프라 확충 등) ■ 차세대 AI기술 선점(피지컬 AI, AI 반도체 분야 차세대 기술 확보·적용) ■ AI모델 확보(AI 파운데이션 모델 확보 등)
	②  AI 기반 사이버·안보 위협의 지능화	■ AI기본사회(AI 범죄 근절 및 대응 역량 강화)
	③  (산업 AX) 피지컬 AI 확산 및 AI-산업 융합 본격화	■ 산업AX(산업별 AI 에이전트 개발 등) ■ AI모델 확보(산업별 수요 기반 AI 파운데이션 모델 확보 및 실증 확산) ■ 지역AX(지역 산단을 지역 AX 활성화를 위한 산업 인프라 거점으로 탈바꿈 등) ■ AI기반 문화강국(K-컬처 산업의 AX 활성화 지원 등)
	④  (공공 AX) 국민체감 및 문제해결형 공공 AI 서비스 확대	■ 공공AX(공공시장의 AI 테스트베드화 등) ■ AI기반 국방강국(국방 AI 기술 및 체계 획득 제도 개편 등) ■ AI모델 확보(보건의료 특화 AI 파운데이션 모델 확보)
	⑤  (AI for Science) 연구개발 방식의 전환과 과학기술 혁신	■ 차세대 AI기술 선점(기초과학 및 전략 과학기술 분야 AI 혁신, AI 연구동료 개발) ■ AI모델 확보(핵심 과학 분야 AI 기반 모델 확보 및 공공·산업 확산)
	⑥  AI 지식자원(데이터·인재)의 전략 자산화	■ AI핵심인재 확보(대학 및 대학원 AI 인재 양성 등) ■ AI규제혁신(개인정보·미개방 산업 데이터 활용 규제 과감한 정비) ■ 지역AX(지역 AX 인재양성 등)
	⑦  AI 기술·공급망의 블록화와 글로벌 AI 거버넌스 재편	■ AI규제혁신(AI 법제 환경 조성 등) ■ AI기본사회(AI 윤리 확산·고도화 등) ■ 글로벌 AI이니셔티브(전략적 글로벌 AI 협력체계 구축 등)

※ 저자 작성, 생성형 AI로 도식화

2 주요 이슈

① 독자 AI 모델·인프라 확보를 통한 AI 주권 경쟁 심화

- 우리 정부는 국내 정예팀 중심의 '독파모' 프로젝트와 '35년까지 18.4GW 규모(총 1,000조 원 규모)의 초대형 AIDC 구축 등 AI 모델·인프라 전 주기 지원 체계를 가동하며 독자 AI 역량 확충을 추진
- AI 분야 차세대 기술개발·기반 확충 등 전 분야에 걸쳐 R&D 투자를 지속적으로 확대하고 있으나, 연간 수천억~조 달러 규모를 투입하는 거대자본·컴퓨팅 격차는 여전히 구조적 한계로 지속
- 글로벌 자본·컴퓨팅 격차를 고려해 전략적 중요성과 집중 분야를 선정하여 통합 실증하고, 업무별 성능·비용·전력 효율·경쟁력과 데이터 통제권·운영 자율성을 확보하는 '선택적 AI 주권' 전략 구체화 필요

□ (배경) 글로벌 AI 경쟁의 축이 민간 주도의 프런티어 모델 혁신에서 데이터센터, 전력망, AI반도체 등 핵심 인프라를 기반으로 국가 안보와 산업 생존을 좌우하는 '소버린(Sovereign) AI' 확보전으로 확대

○ (AI 모델 성장) 지난 10년간 글로벌 AI 생태계는 트랜스포머 아키텍처의 등장('17) 이후, 모델의 파라미터 규모와 사전학습 데이터의 양을 기하급수적으로 확장하는 스케일링 법칙에 기반하여 비약적 발전 도모

- 초기 생성형 AI 경쟁이 대규모 데이터 학습을 통한 다음 단어 예측 성능 향상에 집중되었다면, 최근에는 연산 자원 배분과 학습 방법론의 재편을 통해 추론·문제해결 역량을 고도화하는 질적 전환기로 진입

※ 글로벌 선도 기업들의 연산 자원 투자 무게중심 역시 대규모 데이터를 주입하는 사전학습 단계에서, 특정 과제에 대한 인간의 피드백을 반영하는 미드트레이닝 및 강화학습(Reinforcement Learning, RL) 기반의 후학습 단계로 전환

〈표 4〉 AI모델 패러다임 주요 분기점('17~'26)

시점	주요 변화
('17~'19) Transformer 등장과 사전학습-미세조정 표준화	• Transformer 등장*으로 이전모델(RNN·LSTM)의 순차처리 한계 극복 및 병렬화·확장성 확보, 이후 주요 프론티어 모델의 지배적 기반으로 정착 * Vaswani et al., "Attention Is All You Need"(NeurIPS 2017) self-attention 기반 병렬 학습으로 대규모화 토대 마련 • BERT·GPT 계열 사전학습(pre-training) 패러다임 확립으로 '대규모 비지도 사전학습 후 미세조정' 방식의 표준화
('20) 스케일링 법칙과 모델 거대화	• 'Scaling Law'로 성능이 파라미터·데이터·연산량에 대해 멱법칙(power-law)을 따름을 규명, 동년 GPT-3(175B)와 In-context learning(문맥 내 학습) 부상으로 '거대화' 경쟁 촉발 ※ Kaplan et al.('20)은 파라미터를 데이터보다 약 3배 빠르게 키우도록 권고($N \propto C^{0.73}$)
('22~'23) Chat-GPT 충격과 오픈소스 생태계 성장	• DeepMind Chinchilla가 파라미터와 학습토큰을 약 1:1(약 20토큰/파라미터)로 함께 키워야 연산량 최적임을 규명, 70B 모델을 1.4T 토큰으로 학습해 280B Gopher 상회 ※ Hoffmann et al."(NeurIPS 2022) 발표 이후, 'Chinchilla-optimal' 1:1 스케일링이 학습 연산량의 효율적 배분 기준 제시 • RLHF/InstructGPT 및 ChatGPT 충격('22)으로 후학습(post-training)의 중요성 부각, 사전학습으로 확보한 역량을 실제 사용자 요구에 맞게 발현시키는 후학습의 중요성 부각 • 멀티모달·오픈웨이트(Meta LLaMA 등) 확산으로 오픈소스 생태계 급성장
('24~'26) 추론모델의 등장과 에이전틱·피지컬 AI로의 확장	• OpenAI o1('24)·o3, DeepSeek-R1('25, 671B MoE·37B 활성)이 강화학습과 추론 시 연산 확대(Test-time compute)로 성능 도약, 사전학습 확대와 함께 후학습 및 추론 시 연산 활용의 중요성이 증대 • 에이전틱 AI(장기 자율성) 및 피지컬 AI·월드모델로 축 확장, 경쟁 지표가 단일 응답 품질에서 과업 시간지평(task horizon)·토큰 효율성으로 이동 • 고비용 추론의 한계를 프롬프트 캐싱 및 소형 모델로의 추론 증류(Distillation)로 완화하며, 인간 데이터 고갈(Data Wall)을 RL 기반 자가 생성 합성 데이터(Synthetic Data)로 활용

- 한편, 기존 트랜스포머 아키텍처가 지닌 문맥 길이에 따른 연산량·메모리 폭증 병목 해소를 위한 차세대 대안으로 Mamba와 같은 상태 공간 모델(SSM)과 RWKV 등의 선형 RNN(Linear RNN) 아키텍처가 부상

  ※ 선형 복잡도를 유지하면서도 무한에 가까운 긴 문맥을 고효율로 처리할 수 있어, 에너지 소모를 극단적으로 줄이면서도 에이전틱 AI 등에서 요구하는 장기 기억 능력을 뒷받침할 핵심 기술로 평가

❍ (AI 컴퓨팅 투자 확대) 글로벌 하이퍼스케일러의 AI 인프라 설비투자(CAPEX)가 급증하면서 데이터센터·반도체·전력망 등 핵심 인프라 확보 경쟁이 심화되고, 일부 기업의 투자 규모가 국가 예산에 버금가는 수준으로 확대되며 초대형 자본 중심의 경쟁구조로 전환

- 4대 하이퍼스케일러(Amazon, Microsoft, Google, Meta)의 합산 CAPEX 예상 전망치('26)는 전년 대비 약 77% 증가한 7,250억~7,325억 달러 수준, '27년 연간 1조 달러 돌파 전망

  ※ 5대 하이퍼스케일러(Amazon, Microsoft, Google, Meta, Oracle)의 합산 CAPEX('26)는 약 7,950억 달러, '27년도에는 약 1조 800억 달러로 증가할 전망(BofA Global Research)

- AI 데이터센터 투자('25~'30) 5.2조 달러 중 기술개발社(칩·컴퓨팅 하드웨어)가 60%(3.1조 달러), 에너자이저(전력·냉각·전기설비) 25%(1.3조 달러), 빌더(건설·부동산) 15%(0.8조 달러)를 차지할 것으로 전망(McKinsey, 「The Cost of Compute」, '25)

- 엔비디아 GPU 수급 병목과 가격 인상이 하이퍼스케일러들의 TCO(총소유 비용)를 압박, 추론 비용 절감 및 하드웨어 자주권 확보를 위한 자체 반도체 개발·적용을 통한 내재화가 가속화

  ※ Google(TPU v6e/v7), Amazon(Trainium2/Inferentia2), Meta(MTIA v2), Microsoft(Maia 100) 등 하이퍼스케일러의 자체 AI 가속기 개발·도입 확대 및 AI 가속기의 성능을 좌우하는 핵심 부품인 HBM 수급 한계를 극복하기 위해 메모리 제조사와의 전략적 연계 및 차세대 PIM 원천기술 확보 경쟁 심화

❍ (AI 전력공급 및 냉각 방식 전환) 랙(Rack) 전력밀도의 급증에 따라 발열 처리 방식, 연산 칩 조달 구조, 기저 에너지원 확보에 이르는 전 계층의 재설계가 동시다발적으로 진행되는 국면에 진입

- AIDC는 랙당 전력밀도가 기존 IDC 설계 기준을 크게 상회하는 수준으로 증가함에 따라, 전력 공급 체계와 냉각 방식, 건축 구조 전반에 걸친 근본적 재설계가 요구됨

  ※ NVIDIA GB200/GB300 NVL72 랙이 약 120~142kW, 차세대 VR200 NVL72가 190~230kW, '27년 Rubin Ultra 'Kyber' 랙이 약 600kW에 달하는 등 세대마다 소비 전력이 급격히 증가하는 추세

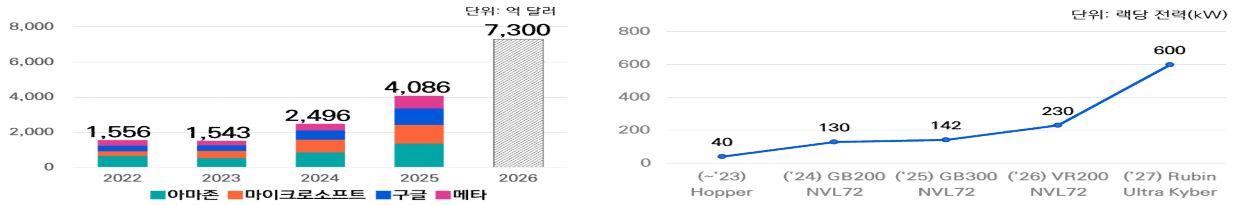
- 단일 1기가와트(GW)급 초거대 AI 데이터센터 구축 시 시설물 건립에 약 100억 달러, 내부 가속기 칩 배치에 약 200억 달러 등 총 300억 달러 이상이 소요, 최종 연산 용량을 결정짓는 병목이 알고리즘에서 '전력 공급 능력'으로 이동

  ※ 빅테크 및 주요국은 24시간 중단 없는 무탄소 기저부하 전력을 확보하기 위해 원자력 발전소 재가동 전력구매계약(PPA) 및 소형모듈원자로(SMR) 개발사와의 장기 계약을 집중 집행

- 한편, 랙 전력밀도가 40kW를 넘어서면서 현행 공랭 방식의 물리적 한계*에 따라, 직접칩냉각(D2C)·액침냉각 적용을 위한 기술·산업적 패러다임 전환이 가속화

  * 랙 전력밀도가 30kW를 초과하면 액랭이 권장되고 40kW를 넘으면 액체냉각 적용 필요성이 크게 증가

  ※ D2C 콜드플레이트가 데이터센터 액체냉각 시장('25)의 42.85%를 점유하며 주력 방식으로 자리 잡았고, 액침냉각(단상·이상)은 CAGR 26.62%로 가장 빠르게 성장 중(Mordor Intelligence, '26)



[그림 2] (좌)주요 하이퍼스케일러의 AIDC 구축 CAPEX, (우)AIDC 랙당 전력밀도 급증(NVIDIA GPU)

□ (주요국 동향) 미·중이 압도적 자본과 인프라를 앞세워 AI 시장의 양강 구도 형성, EU·일본을 비롯한 기타 선도국은 규제·동맹·틈새 전략으로 독자적 AI 주권 확보 도모, 다만 최근 AI 개발 속도 조절 필요성 및 미국 중간선거 결과로 인한 AIDC 규제 이슈가 부상

❍ (미국) 세계 최다 데이터센터(매체에 따라 상이하나, 3,800개 이상으로 추산)와 최대 규모의 자본을 투입해 빅테크 중심의 프론티어 모델 생태계를 선도하며, 기술 표준 선점과 인프라의 안보 자산화를 결합한 패권 전략을 구사, 최근 빅테크 기업을 중심으로 AI 개발 속도 조절 필요성 강조('26.9)

- OpenAI·구글(Google DeepMind)·앤트로픽(Anthropic)·메타(Meta) 등 민간 기업이 막대한 자본과 최첨단 R&D 인프라를 바탕으로 파운데이션 모델 생태계 선도 및 기술 주도권 확보

※ 앤트로픽의 '클로드(Claude)' 모델이 정보 평가와 표적 식별, 작전 시나리오 검토 등에 활용된 사례와 같이, 민간 주도 AI 모델이 상업적 서비스를 넘어 국가 안보 체계와 결합되는 '안보화' 현상이 관찰

- 인프라 관점에서는 데이터센터 투자 확대와 첨단 AI 반도체의 수출통제 강화가 양대 축으로, AI 컴퓨팅 인프라 확충과 핵심 공급망 통제력 강화를 뒷받침하여 AI 기술 주도권 확보 추진 중

※ 데이터센터 급증에 따른 송전망 포화 및 요금 인상 갈등에도 불구하고, 원자력 포함 '전방위(All-of-the-above)' 에너지 총동원을 통한 전력 인프라 한계 돌파 추진

- AI 업계 최고경영자(앤트로픽, Open AI 등)들은 AI 안전성 문제로 최첨단 AI모델의 역량을 향상시키는 속도를 늦춰야 한다고 강조

- 미국 중간선거('26.11)에서 민주당이 상·하원 다수당을 확보함에 따라 AIDC 운영과 관련된 전기 요금, 용수 공급 등 인허가 심사 강화 예정

❍ (중국) 미국의 전방위적인 기술·산업 통제에 대응하여 국가 주도의 강력한 하향식 지원과 풍부한 데이터·에너지 자원을 결합한 '풀스택(Full-stack) AI 생태계 자립' 생존 전략 추진

- 자국 데이터의 해외 유출을 원천 차단하는 강력한 국가 방화벽 체제 속에서 텐센트·바이두·알리바바 등 빅테크 중심의 자국어·산업 데이터 기반 독자 LLM 개발 집중

※ DeepSeek·Moonshot(Kimi) 등은 지식 증류와 경량 MoE 아키텍처를 적용한 저비용·고효율 모델 가중치를 공개하며 저사양 연산 환경에서의 구동 가능성 확대를 통한 온디바이스 생태계 선점을 가속

※ Qwen(모델), SGLang(서빙 프레임워크) 등 모델부터 학습·서빙 인프라에 이르는 전 계층의 오픈소스 스택을 구축, 서방 폐쇄형 생태계에 대응하는 동시에 신흥국 확산의 통로로 활용해 자국 중심의 기술 영향권을 확대

- 첨단 GPU 도입이 제약된 상황에서 자국 빅테크를 중심으로 반도체 자립을 추진하는 동시에, '동수서산' 프로젝트를 통해 서부의 에너지 자원과 동부의 데이터 수요를 연결하는 인프라 재배치 전략을 구사

※ 국가 주도로 메모리 반도체 기업과 대형 플랫폼 기업 간 장기 공급 계약을 유도해 서버·클라우드·AI 연산용 메모리 공급망을 내재화함으로써, 외부 제재에 대한 생태계 회복탄력성을 극대화

〈표 5〉 美빅테크 중심의 폐쇄형 대 中오픈웨이트 모델 간 비교

국가	미국 빅테크	중국 오픈웨이트
대표기업 및 모델	• OpenAI(GPT-6 Astra 등), Anthropic(Claude 계열), Google(Gemini) 등	• DeepSeek(R1·V3), Alibaba(Qwen), Moonshot(Kimi·Moonlight), Zhipu(GLM) 등
생태계 및 배포 방식	• 폐쇄형 클라우드 API (Closed-Weight) · 모델 가중치·학습 데이터·코드 비공개 · API 호출 과금 및 월 구독형 B2B/B2C 서비스	• 가중치 완전 개방 (Open-Weight) · 오픈소스 라이선스(Apache/MIT) 기반 가중치 무료 배포 · 온프레미스 구축 및 로컬 호스팅 자유화
핵심 기술 및 아키텍처	• 자본 집약형 스케일업(Scale-up) · 초거대 연산량 기반 사전학습(Pre-training) · 프론티어 플래그십 성능 지속 경신에 집중	• 고효율 경량화 및 지식 증류(Distillation) · MoE(희소 전문가 모델), MLA, MSA(Sparse Attention) · 대형 모델 사고 과정(CoT) 증류를 통한 SLM 고도화
컴퓨팅 및 하드웨어 환경	• 최첨단 가속기 대규모 클러스터 집중 · 최신 GPU(H100/B200) 및 10GW급 AIDC 기반 · 민간 빅테크 중심의 대규모 CAPEX 투자 지속	• 제재 우회형 저비용·저사양 최적화 · FP8 혼합 정밀도·양자화 기법으로 하드웨어 요구 스펙 최소화 · 풍부한 전력 기반 및 소비자용 단일 GPU/온디바이스 구동
비즈니스 전략	• API·클라우드 기반 서비스 수익화 및 생태계 확장 · 기술 장벽을 통한 엔터프라이즈 종속 유도 · 타사의 자사 출력 데이터 증류 학습 엄격 차단	• 글로벌 개발자 락인(Lock-in) 및 저가 공세 · 무료·저비용 모델 공급으로 인디 개발자·스타트업 생태계 장악 · 중간가격 정책 및 오픈소스 파생 생태계 확산
지정학적 목표	• 글로벌 AI 표준 및 독점적 OS 지배력 수호 · 미국의 첨단 수출 통제망과 연계하여 기술 초격차 유지	• 미국 기술 제재 무력화 및 글로벌 표준 선점 · 우회 확산을 통해 제3국 중심 독자 생태계 확립

❍ (EU) 미국 빅테크 플랫폼에 관한 기술·산업적인 종속을 경계, 「AI Act('24)」를 통한 신뢰·안전 기준을 정립하는 규제체계와 'EuroHPC' 중심의 공동 컴퓨팅 투자를 결합한 하이브리드 기술주권 전략 구사

- OpenEuroLLM*을 비롯하여 프랑스미스트랄 AI(Mistral AI), 이탈리아도민(Domyn) 등 역내 AI 스타트업을 중심으로 오픈소스 및 철저한 프라이버시 보장형 모델 개발을 통해 미·중에 대한 기술적 독립을 추구

  * 20개 기관 컨소시엄(Charles 대학교와 AMD Silo AI 공동 주도), '25년 2월 착수, 디지털유럽 프로그램 지원 및 EuroHPC 인프라를 활용하며, EU 공식 언어 전체를 커버하는 완전 개방형 파운데이션 모델 개발을 지향

  ※ 단순한 기술적 자립의 차원을 넘어서, GDPR 등 유럽 고유의 프라이버시 원칙과 사회적 가치 지향을 모델에 반영하고 있으며, 다국어 대응 능력과 보안 강점을 앞세워 유럽 역내 공공·민간 시장 수호를 지향

- 개별 국가 재정으로는 미국의 자본력에 맞설 수 없다는 인식 아래, '디지털 유럽 프로그램'과 'EuroHPC JU'을 축으로 '21~'27년 간 약 70억 유로 이상 예산을 통합해 공동 인프라를 구축

  ※ 이탈리아 파스트웹의 NVIDIA DGX H100 슈퍼컴퓨터 구축, 도민의 블랙웰 GPU 5,760개 기반 AI 팩토리 추진, 시네카(CINECA)의 레오나르도 슈퍼컴퓨터(GPU 1만 5천 개 이상) 운영 등 민관 AI 인프라 확충과 함께, EU는 '25년까지 19개 AI 팩토리를 선정하고 신규 AI 최적화 슈퍼컴퓨터 도입을 통해 EuroHPC AI 컴퓨팅 역량을 3배 이상으로 확대 추진

❍ (일본) 'AI 부활론'을 기치로 '세계 최고 AI 친화국'을 지향하며, 정부 보조금을 통한 인프라 확충 및 미국 빅테크와의 전략적 협력을 병행하는 실용주의 노선의 소버린 AI 정책을 추진

- 일본 고유의 언어·문화적 맥락을 반영한 파운데이션 모델 개발에 주력 중이며, 자국 스타트업 중에서는 사카나 AI가 시리즈 B로 2억 달러('26.4.)를 확보하며 소버린 AI 대표 기업으로 부상

  ※ 독자 모델의 성능 고도화를 위해 국립 연구소 및 대학 기관이 긴밀히 협력하여 자국의 최고성능 슈퍼컴퓨터인 '후가쿠(Fugaku)' 등을 적극 활용해 일본어에 최적화된 기초 데이터 코퍼스를 지속적으로 정제하고 훈련

- 데이터·AI 주권 확보를 위해 일본 정부는 소프트뱅크·사쿠라 인터넷·KDDI 등 6개 기업의 AI 인프라 구축에 약 7.4억 달러를 지원, 별도로 국가 슈퍼컴퓨터 'ABCI 3.0' 구축·운영을 통해 자국 AI 컴퓨팅 역량 강화

  ※ 디지털청은 '21년 출범 이후 정부 클라우드의 인력·기술 공백을 메우기 위해 AWS·오라클 등으로부터 투자를 이끌어내는(오라클 80억 달러 등) 한편, 시설의 자국 영토 내 설치를 전제 조건으로 삼아 안보와 효율성을 절충

❍ (기타) 캐나다, 대만 등 주요국 역시 자국 언어, 반도체 자본, 특화 산업 강점 등 고유의 레버리지를 활용해 글로벌 틈새시장을 선점하고, 동맹과의 전략적 연대를 통해 독자적 AI 영토를 개척

- (캐나다) '19년 설립된 코히어(Cohere)는 특정 클라우드에 종속되지 않는 B2B 소버린 AI 플랫폼 '노스'를 통해 고객 기업과 정부가 자체 데이터를 직접 통제할 수 있도록 지원

※ 코히어는 다국어 모델 'Aya 23'을 출시한 바 있으며, 독일 알레프 알파와의 합병과 슈바르츠 그룹의 6억 달러 투자 발표를 통해 기업가치 200억 달러 규모의 대서양 횡단 소버린 AI 연합을 구축하여 미국 빅테크 의존도 개선에 기여

- (대만) 중국발 AI 모델과 간체자 데이터의 사상적·문화적 종속에서 벗어나기 위해 NSTC(국가과학기술위원회) 주도로 자체 LLM 'TAIDE' 프로젝트를 추진하며 AI 주권 확보를 도모

※ TAIDE는 구글의 Gemma 3 12B를 기반으로 대만 관련 텍스트·훈련 자료를 반영해 정체자 중국어 응답 능력을 고도화했으며, 3억 파라미터 규모의 임베딩 모델도 별도로 공개

- (UAE) G42와 TII 등 국영기업·연구기관을 중심으로 대규모 자본을 투입해 아랍어 기반 LLM 'Falcon' 시리즈와 'Jais 2'를 개발, 오픈소스로 공개함으로써 중동 내 데이터 통제권과 기술 패권 장악

〈표 6〉 주요국의 AI 주권 확보 전략

국가	AI 모델	AI 인프라	주요 기업 및 이니셔티브
미국	•빅테크 중심 프론티어 모델 생태계 선도, 기술표준 선점과 인프라 안보자산화 결합	•데이터센터 투자('26)는 총 7,000억 달러 예상(무디스 전망), 시장 규모로는 전 세계 31%를 차지(Stastita)	•OpenAI, Google, Anthropic, Meta, DeepMind 등
중국	•데이터 반출 통제 기반 내수 생태계 확립 및 개도국 대상 오픈소스 모델 수출	•미국의 반도체 제재 우회를 위한 HW 내재화 및 '동수서산' 기반 컴퓨팅 분산 프로젝트 추진 중	•텐센트·바이두·알리바바 등 •Qwen(모델), SGLang(서빙 프레임워크, 다수 중국 기업이 주도)
EU(유럽)	•「AI Act」 등 규제와 다국어, 프라이버시(GDPR) 내재화 중심의 기술적 독립 추진	•'21~'27년 약 70억 유로(디지털 유럽 프로그램+EuroHPC JU), GPU 1만 5천개 이상('AI 팩토리' 연합)	•AI Act, EuroHPC •미스트랄 AI(프랑스), 도민(이탈리아) 및 OpenEuroLLM
일본	•일본 고유 언어·문화 맥락 반영한 파운데이션 모델 개발, 정부 보조금과 미국 빅테크 협력 병행	•ABCI 3.0에 7억 4천만 달러 이상, AWS·오라클 등으로부터 80억 달러 유치(자국 내 시설 조건)	•사카나 AI, 소프트뱅크·사쿠라 인터넷·KDDI 등 •후가쿠(공동 활용 슈퍼컴퓨터)
기타 (캐나다, 대만 등)	•언어 자원·반도체 자본·산업 특화 등 틈새시장 선점, 동맹을 통한 독자적 AI 영토 개척	•자국 언어·문화를 기반으로 한 모델 개발을 위한 자체적인 데이터·인프라 독립성 확보에 집중	•(캐나다) 코히어·North·Aya 23 •(대만) NSTC·TAIDE •(UAE) G42·TII, Falcon 180·Jais

□ (국내 동향) 독자 AI 모델 개발 및 전 주기 지원으로 외산 의존도를 낮추고, 민관 협력 인프라 구축과 부품 자립화에 국가 자원을 집중 투입

❍ 정부는 외산 AI 모델 의존도 완화와 'AI 3대 강국' 도약을 목표로 독자 파운데이션 모델 개발, 데이터 기반 확충, 국산 모델 기반 국민 서비스 확산에 이르는 전주기 지원 체계를 구축·가동

- 「독자 AI 파운데이션 모델(독파모)」 프로젝트를 국가 사업으로 편성해 국내 정예팀 중심의 경쟁형 모델 개발 체계를 가동 중이며, '26년 하반기 3개 정예팀의 경쟁 체제로 운영

※ 독파모 사업의 성과로 4개 정예팀이 '26년 상반기 개발한 AI 모델 전부가 미국 비영리 연구기관 'Epoch AI'의 '주목할 만한 모델(Notable Model)'로 등재

- 네이버·LG AI연구원·카카오·업스테이지 등 민간 주도의 한국어 특화 파운데이션 모델 생태계가 형성된 가운데, 정부는 국민성장펀드·첨단전략산업기금 등을 통해 업스테이지에 5,600억원(공적 1,300억+민간 4,300억) 규모의 민관합동 직접 지분투자를 승인하여 독자 모델 고도화를 지원

- '모두의 AI 프로젝트'의 연장선에서 R&D 성과가 즉각적인 내수 생태계 방어로 이어지도록, 국산 모델 기반의 전 국민 무료 AI 챗봇 및 공공 에이전트를 구축하는 「에이전틱 AI 이니셔티브」 출범('26)

  ※ 국내 통신 및 IT 대기업들이 독파모 참여 기업과 합종연횡하여 6개 컨소시엄을 구성·참여, 자사 모델 및 타 국산 모델 혼합 의무 조항을 통해 국산 AI 모델의 실증 레퍼런스를 극대화

- 철강, 조선 등 산업 특화 파운데이션 모델 개발과 함께 제조 현장의 암묵지를 데이터·AI로 체계화하여 생산성을 향상하는 대형 R&D사업 추진 예정

❍ 민관 협력을 통해 자국 내 AI 컴퓨팅 인프라를 확충하고, 반도체 등 핵심 부품의 기술개발과 생산 역량 강화에 대규모 국가 재정을 투입하여 해외 기술 의존도 완화 및 안정적인 AI 공급망 구축 추진

- '35년까지 총 18.4GW 규모의 초대형 AIDC 구축을 위해 SK·GS·네이버 등과 협력해 누적 1,000조 원('29년까지 1단계 8.4GW AIDC 구축에 550조 원 투입) 규모의 민관 합작 투자를 발표

  ※ AI 연산 수요 급증에 대응해 국내에 대규모 컴퓨팅 인프라를 확보하는 데 초점이 맞춰져 있으며, 수도권에 집중된 데이터센터를 충청 등 비수도권으로 분산하고 AI 반도체와 클라우드 솔루션 국산화도 함께 추진

- 'AI 고속도로' 핵심 인프라로서, '26년부터 5년간 '국가AI컴퓨팅센터' 구축에 2.5조원을 투입, 삼성SDS 컨소시엄이 해남 솔라시도를 입지로 사업자로 최종 선정('26.8.3. 센터 착공식 개최)

  ※ 컨소시엄은 당초 B200 GPU 1만5,000장 도입을 제시하였으나, 정부는 센터가 실제 구축되는 '28년까지 신제품이 출시될 것을 고려하여 시장 상황에 맞춰 최신 반도체를 도입한다는 방침

- AI 연산 비용과 전력 소모를 낮출 차세대 NPU, PIM, 온디바이스 AI 반도체 개발 등 국산 AI 반도체 생태계(K-Cloud 프로젝트 등) 육성에 국가 R&D 예산을 집중 투입해 기술 자립의 기반을 공고화

  ※ 국산 AI 반도체(NPU) 상용화 레퍼런스 확보를 위해 「K-클라우드 프로젝트」를 통한 국산 NPU 데이터센터 실증 추진, 'NPU→저전력PIM→극저전력PIM' 3단계 고도화 로드맵 설정

□ **(과학기술 역할과 개선방향) 글로벌 자본·컴퓨팅 격차에 대응해 국내 기반을 활용할 업무·기술을 선별하고, 전력·용수·연산 등의 현장 통합 실증을 연계해 기술 경쟁력, AI 규제 대응 및 안정적 운영 역량 등 동시 확보 노력 필요**

❍ (현주소) 독자 모델 개발, 컴퓨팅 인프라 확충 및 국산 AI 반도체 실증 등을 추진하고 있으나, 개발 성과의 현장 활용을 검증하고 가치사슬별 병목에 따라 자원을 통합 연계·배분할 수 있는 체계는 제한적

- 독자 파운데이션 모델 개발과 단계별 평가를 통해 국내 개발 역량을 축적하고 있으나, 개발·평가 성과가 개별 업무의 성능·비용·보안 요건을 충족하고 지속적인 도입으로 이어지는 별도 검증 필요

  ※ 2차 단계평가('26.8)에서 4개 정예팀 중 업스테이지·SKT·LG AI연구원의 3개 팀이 다음 단계로 진출, 공개 점수는 65.8~70.6점이며 평가 결과만으로는 수익화 성과를 판단하기 어려움

- 대규모 학습·추론 자원의 확보에는 반도체뿐 아니라 전력·냉각·운영비용이 함께 소요되나 일부 기술의 해외 의존도가 높음

  ※ AIDC용 칠러·공조의 국내 공급 역량을 확보하고 장비의 내재화를 확대하고 있으나 일부 액침냉각 시스템의 탱크·제어 기술은 해외 전문기업 의존

- 국내 반도체·제조 현장 등 산업 기반을 AI 경쟁력으로 연결하기 위해서는 업무별 데이터 접근성·품질, 모델·시스템 SW의 완성도, 수요기업의 도입 여건을 함께 고려하는 통합 접근 강조

  ※ 제조업 부가가치 비중은 GDP의 27.4%('25년), 제조업 로봇 밀도는 종업원 1만 명당 1,220대('24년)로 적용 기반은 확인되나, 피지컬 AI의 기술 우위나 학습데이터 활용 가능성을 곧바로 의미하지 않음

❍ (개선방향) 자본력 경쟁에서 벗어나 고효율 원천기술 개발과 데이터 주권 확립에 R&D를 집중하고, 국산 모델의 공공조달 우선 적용과 AIDC 기반기술 내재화를 통해 선택적 우위 중심의 AI 주권 확보 추진

- AI 가치사슬별(데이터, SW, HW 등) R&D사업 포지셔닝을 통한 전략적 우선순위 설정과 함께 성과 연계 및 범부처 협업체계 강화 필요

- 거대 파라미터 기반 사전학습 중심의 자본력 전면전에서 탈피, 에이전틱 AI, 차세대 추론 알고리즘, 에이전틱·피지컬AI 등 고성능·고효율 원천기술 개발에 R&D 역량을 집중하고, 데이터 클리닉 및 합성 데이터 기술 확보를 통해 독자적 데이터 주권 확립 추진

  ※ EU「AI Act」 등 글로벌 규범에 선제 대응할 수 있는 국산 AI 모델의 안전성·신뢰성·설명가능성 검증 프레임워크를 개발해, 공공 안보 현장 적용과 해외 진출을 뒷받침하는 기술적 신뢰 기반을 확보

- 분야별 보안 민감도와 전략적 중요도에 따라 독자적 AI 역량 확보와 글로벌 AI 활용을 병행하고, 성능·비용·보안 요건에 부합하는 모델 도입을 통해 AX 가속화

  ※ 보안 민감도가 상대적으로 낮은 분야는 민간의 자율적 판단에 따라 국내외 고성능 AI 모델을 적극 활용하도록 지원하여 생산성 제고와 서비스 혁신 촉진

  ※ 국가전략산업 등 보안이 중요한 분야는 데이터 통제권과 운영 자율성 확보를 전제로, 자체 모델 또는 외산 모델의 폐쇄형 구축·운영 가능성을 검토하고 현장 적용을 선행하여 국산 모델 고도화 이후 신속한 전환·확산 기반 마련

  ※ 특정 모델에 대한 종속을 줄일 수 있도록 모델 교체·연계가 가능한 시스템 구조와 공통 평가체계를 마련하고, 공공조달에서도 업무별 성능·보안·비용 적합성을 종합적으로 검토

- 급증하는 추론 연산 비용과 전력 소모에 대응해 국산 AI 반도체(NPU/PIM) 기반 인프라 생태계*와 직접칩냉각·액침냉각 등 차세대 냉각기술**을 결합한 AIDC 기반기술 내재화를 추진

  * 국산 반도체의 상용 경쟁력을 완성하기 위해 독자 컴파일러(Triton/OpenXLA 연계), 고성능 분산 서빙 프레임워크, 오픈소스 런타임 개발 등 시스템 SW 생태계 구축에 R&D 투자를 확대하여 개발자 종속성을 탈피

  **랙당 수백 kW급 초고발열 환경에 대비하여 직접칩냉각(D2C) 냉각판, 매니폴드, 단상·2상 액침냉각용 절연 유체 등 핵심 냉각 소재·부품의 국산화 R&D를 가속화

- 국내 고유 데이터와 산업 강점을 활용한 도메인 특화 모델 개발과 함께, 수요 발굴·컨설팅·시스템 구축·운영을 지원하는 응용서비스 생태계를 조성하여 산업 현장 도입 가속화

  ※ 제조·의료·법률·행정 등 분야별 업무에 특화된 AI 응용서비스와 기존 시스템 연계 기술을 개발하고, 현장 활용이 검증된 도입 사례를 재사용 가능한 표준 솔루션으로 확산

  ※ 수요기업과 AI 솔루션 기업·컨설팅·시스템 구축 기업 간 협력을 지원하고, 업무 진단부터 데이터 정비·모델 선정·시범 적용·운영인력 교육까지 도입 전주기 지원체계 구축

  ※ 모델 성능뿐 아니라 도입 소요기간·총운영비용·업무 생산성·사용자 활용률 등 실제 활용성과를 중심으로 실증사업을 평가하고, 우수성과의 후속 도입·확산 지원

② AI 기반 사이버·안보 위협의 지능화

- 사이버 위협이 기존 공격의 자동화·지능화를 넘어 시스템 전반으로 확산됨에 따라 AI 기반 사이버·안보 위협 대응체계 강화 요구
- 주요국은 AI 특화 위협에 대응해 모델·에이전트의 보안 평가와 레드티밍, AI 기반 방어 자동화, 민관 협력 및 제도적 기반을 연계한 통합 사이버보안 대응체계 확대
- AI 사이버 위협 대응과 관련하여 재현 가능한 공통 평가 환경을 고도화하고, 탐지·발견 능력뿐 아니라 실환경 검증과 운영·사고 대응의 실효성까지 포괄하도록 연계 강화 필요

□ **(배경) AI 모델의 진화로 기존 사이버공격이 지능화·고도화되고 데이터·모델·도구 간 연쇄 위협이 확대됨에 따라, 전주기 사이버안보 대응체계의 중요성 증대**

❍ (프론티어 AI 사이버 위협의 부상) 앤트로픽(Anthropic)의 클로드 미토스(Claude Mythos) 공개를 계기로 프론티어 AI가 전문 인력 중심의 취약점 분석·공격 수행을 일부 자동화하며, 사이버 공격·방어의 자동화와 속도 경쟁이 주요 보안 이슈로 부상

- Mythos는 취약점 탐색·익스플로잇 생성 등 높은 사이버 역량의 악용 우려로 일반 공개를 제한하고, Project Glasswing*을 통해 주요 보안 기관·플랫폼 등이 취약점을 선제적으로 탐지·패치하는 방어 목적으로 우선 활용

  * Project Glasswing: 프론티어 AI를 방어기관 등에 제한적으로 제공해 취약점을 선제적으로 탐지·패치하도록 지원하는 앤트로픽의 사이버 방어 프로젝트

- 프론티어 AI의 발전은 새로운 공격유형의 등장보다는 기존에 사람이 단계별로 수행하던 취약점 분석·공격 가능성 검증·침투 절차의 자동화를 통해 공격 비용과 진입장벽을 낮추고, 취약점 발견과 패치 간 속도 경쟁을 심화할 가능성을 시사

❍ (AI 기반 사이버위협의 지능화) 생성형 AI와 에이전틱 AI 확산으로 공격·방어·보호 대상이 동시에 변화하며, AI를 활용한 기존 사이버공격의 고도화 진행

- 공격자는 표적정보 수집, 피싱·악성코드·딥페이크 공격을 자동화하고, 방어자는 AI를 취약점 탐지·악성코드 분석·패치 생성 등에 활용하면서 공격·방어 양측의 AI 활용이 확대
- 영국 국가사이버보안센터(NCSC)는 단기적으로 AI가 완전히 새로운 공격유형을 만들어내기보다는 정찰, 취약점 연구, 기초 악성코드 생성 등 기존 공격 전술·기술·절차(TTP)를 고도화할 것으로 전망

  ※ NCSC: National Cyber Security Centre

❍ (AI 사이버 위협의 범위 확대) AI 기반 사이버 위협이 피싱·악성코드 등 기존 공격의 지능화를 넘어 데이터 오염·모델 탈취 등 AI 시스템 자체에 대한 공격으로 확산되고, RAG·외부 도구·AI 에이전트 간 연계 및 상호작용 과정에서 새로운 보안 취약성과 공격 경로가 등장

- 각 위험은 상호 연계될 수 있으며, 피싱을 통한 계정 탈취 이후 모델 변조와 에이전트 권한 악용으로 내부 시스템까지 확산되는 복합·연쇄 공격으로 확장될 가능성이 증대

- 특히 에이전트형 AI가 실제 도구·권한과 연계되면서 권한 과다, 공격면 확대, 행동 불일치, 감사 공백 등 시스템 상호작용 과정의 새로운 보안 위협이 부각

※ 정보·안보 협력체 Five Eyes 국가(미국·영국·호주·캐나다·뉴질랜드)의 관계기관들은 「Careful Adoption of Agentic AI Services」를 통해 에이전트형 AI의 최소권한·감사로그·인간 감독 등 보안 통제를 권고('26)

❍ (사이버안보 대응 범위 확대) 공격·방어 자동화가 실제 코드·네트워크·평가 환경에서 확인되면서, AI 사이버 위협의 범위 확대에 대응한 보안 범위 확대

- AI가 기존 피싱·정찰·취약점 연구·악성코드 개발을 빠르고 대규모로 수행할 것으로 전망, 방어 측면에서도 취약점 발견·패치 후보 생성 역량이 확대됨에 따라 결과 검증 및 안전한 운영 전환 체계 마련 요구

- 모델의 공격 역량 확대에 따라 평가·레드팀 환경의 보안 중요성이 커지고 있으며, RAG·도구 호출·권한 위임·외부 API 등이 결합된 운영 중 행동을 지속 관측·통제하는 체계 구축 필요성 증대

〈표 7〉 AI 사이버보안 관련 주요 사건('25~'26)

시점·사건	주요 내용
DARPA AI Cyber Challenge 최종 경연 ('25.8)	- 7개 팀의 사이버 추론시스템이 5,400만 줄 이상의 코드를 분석하여 합성 취약점 63개 중 54개(86%)를 탐지하고 43개(68%)를 패치 - 의도적으로 삽입되지 않은 실제 취약점 18건과 이에 대한 패치 11건도 추가 제시
현실형 사이버레인지 평가 ('26.1)	- Anthropic은 최신 모델이 표준 오픈소스 도구를 활용하여 수십 대 규모의 네트워크에서 다단계 공격 수행 가능성을 확인 - 사용자 정의 도구가 없는 경우 9개 평가망 중 5개에서 공격이 진전되지 않는 한계도 확인
Project Glasswing 중간결과 ('26.5)	- 1,000개 이상의 오픈소스 프로젝트에서 다수의 AI 기반 취약점 후보를 발굴 - 고위험·치명적 후보 1,752건을 검증한 결과 90.6%가 실제 취약점으로 확인되었으며, 62.4%는 최종적으로 고위험·치명적 수준으로 분류
OpenAI-Hugging Face 평가 사고('26.7)	- OpenAI와 Hugging Face의 예비조사에 따르면, 내부 사이버 평가에 사용된 모델이 패키지 레지스트리 캐시 프록시(Artifactory)의 당시 미공개 취약점을 발견·악용하여 인터넷 접근을 확보하고, 이후 권한 상승과 수평 이동을 거쳐 Hugging Face 운영 인프라 침해로 이어짐
Anthropic 평가 환경 사고 공개('26.7)	- 141,006회의 평가 실행을 검토한 결과, 인터넷 차단을 전제로 한 제3자 평가 환경에서 실제 외부 접근이 가능했던 사실을 확인 - 외부 조직의 운영 인프라에 무단 접근한 사례가 확인되어 평가 환경에 대한 보안 필요성 제기

□ **(주요국 동향) AI 특화 위협에 대응해 평가·레드티밍과 생애주기 보안기준을 정립하고, 프런티어 AI 기업과의 협력 및 AI 기반 취약점 탐지·방어 자동화를 연계한 통합 대응체계를 강화**

❍ (미국) AI 기반 사이버 위협에 대응하여 평가 과학·시험 환경 구축, 방어 자동화 R&D, 프론티어 AI 기업과 정부 간 협력을 중심으로 대응체계 강화

- 「America's AI Action Plan('25)」을 통해 실제 환경에 가까운 AI 평가·시험장 구축과 모델 평가 과학·보안 연구 확대 추진

- 행정명령 14409('26)을 통해 고성능 AI 모델의 사이버 역량에 대한 정부·산업계의 자발적 정보 공유, 사전 접근 및 고위험 역량벤치마킹을 추진하여 프런티어 AI 기업과 정부 간 협력체계 강화

- NIST는 적대적 머신러닝 분류체계를 통해 데이터 중독, 회피, 개인정보 공격과 생성형 AI 오남용 등 AI 특화 공격 유형을 체계화하고, Cyber AI Profile을 통해 AI 시스템 보안(Secure), 사이버 방어(Defend), 공격 저지(Thwart)를 하나의 프레임으로 연계
- DARPA의 AI Cyber Challenge(AIxCC)를 통해 대규모 실제 코드베이스에서 취약점을 탐지하고 패치를 생성·검증하는 사이버 추론시스템을 실증하고, 평가 결과와 시험 자료의 오픈소스 공개 및 전환을 추진

❍ (중국) 생성형 AI 서비스와 콘텐츠에 대한 관리·표지 체계를 기반으로, 에이전트의 권한·행동 및 외부 도구 연계 등 AI 시스템 전주기에 대한 안전·보안 관리를 강화

- 「생성형 인공지능 서비스 관리 잠정 방법('23)」을 통해 학습 데이터의 적법성, 개인정보·지식재산 보호, 생성 콘텐츠 관리, 안전 평가와 서비스 제공자의 책임 등을 규정하여 AI 서비스 출시와 운영 전반에 대한 관리 체계를 마련
- 「인공지능 생성·합성 콘텐츠 표지 방법('25)」과 강제 국가표준 GB 45438-2025를 통해 생성 콘텐츠에 명시적 표지와 파일 메타데이터 기반의 비가시적 표지를 적용하고, 유통 플랫폼에 표지 확인·추가 의무를 부과하여 생성부터 유통·앱 배포까지 표지의 연속성을 강화
- 「스마트 에이전트 규범적 응용 및 혁신 발전 실시의견('26)」을 통해 에이전트의 의사결정 권한과 행동을 통제하고, 데이터 중독·시스템 취약점·권한 오용 등에 대한 탐지·평가와 모델 접속·API 호출·외부 도구 사용 단계의 보안관리를 강화
- 강제 국가표준 제정 계획 「스마트 에이전트 응용 안전 기본 요구('26)」를 통해 에이전트의 권한·도구 호출, 인간 개입, 로그·모니터링, 이상 행동 차단 등 구체적인 보안 요건의 표준화를 추진

❍ (일본) AI Safety Institute(J-AISI)를 중심으로 평가 방법, 레드티밍, 표준·적합성, 사고 대응을 연결하는 체계를 구축하고, AI 특화 공격의 식별부터 대응까지 연계 강화

- J-AISI는 「Known Attacks and Their Impacts on AI Systems('26)」 제2판을 통해 모델 추출, 데이터·모델 중독, 프롬프트 인젝션 등 AI 특화 공격유형과 영향을 체계화하고, 이를 레드팀 시나리오 및 R&D 과제 설계에 활용할 수 있도록 제시
- 「Approach Book for AI Incident Response('26)」를 통해 관측 가능성(observability)과 통제 가능성(controllability)을 평가 기준으로 제시하고, 운영 중 이상 행동과 영향 범위를 관측하여 문제 요소를 선택적으로 격리하는 사고 대응 방향을 제시

❍ (EU) 「AI Act」를 기반으로 AI 시스템의 사이버보안 의무를 법제화하는 한편, 법적 의무, 생애주기 표준, 공동 평가·시험 인프라, AI 기반 방어 R&D 등을 연계한 대응체계 구축

- 범용 AI 모델과 고위험 AI 시스템의 안전·보안 의무를 법적 체계에 포함하고, 시스템적 위험이 있는 모델에 위험평가·완화, 사고 보고 및 사이버보안 조치를 규정
- 「EU Action Plan on Cybersecurity and Artificial Intelligence('26)」를 통해 고도 AI 모델의 보안 평가 역량 강화와 안전한 시험 플랫폼 구축을 추진하고, AI 사이버보안 그랜드 챌린지 및 오픈소스 취약점 탐지 등 AI 기반 사이버 방어 R&D를 확대

- ETSI AI 보안 표준을 통해 AI 모델·시스템의 보안 원칙을 설계·개발·배포·운영·유지관리 등 생애주기 전반에 적용하고, 「AI Act」의 법적 의무와 기술적 보안 요구 간 연계 기반을 강화

❍ (영국) 프론티어 AI의 사이버 역량을 직접 평가하고, 평가 결과를 경보·운영 지침·취약점 대응으로 연계하는 평가–운영 대응체계 강화

- AI Security Institute(AISI)를 중심으로 프론티어 AI의 취약점 분석, 익스플로잇 코드 작성, 시스템 구조 이해, 공격 도구 사용 및 다단계 사이버공격 역량을 평가하여 고성능 모델의 실제 사이버 위험 수준을 검증
- AISI의 직접 평가와 NCSC의 위협평가·운영 지침을 연계하고, 프론티어 AI를 위협 탐지·조사, 완화·대응 등 방어 도구로 활용하는 방안을 제시하여 평가 결과를 실제 방어 체계로 연계
- NCSC의 AI 위협 평가와 영국 정부의 「AI Cyber Security Code of Practice('25)」를 통해 AI 개발·배포·운영 전 과정의 보안 기준을 제시하고, '26년에는 AI 기반 취약점 탐지 확대에 따른 대규모 패치 수요에 대비하도록 취약점 관리·대응 강화를 권고

□ **(국내 동향) AI 모델·에이전트의 보안 평가와 취약점 대응체계를 강화하는 한편, AI 기반 사이버 방어 기술개발과 법·제도 및 전담기관 구축을 통해 국가 AI 사이버보안 역량을 종합적으로 확충**

❍ (AI 모델 평가·취약점 대응 강화) AI 모델·에이전트의 실제 활용 환경을 반영한 보안 평가·레드티밍을 구체화하고, AI 기반 취약점 분석·패치 및 민관·국제 협력체계를 강화

- 과기정통부–Anthropic 간 협력을 통해 AI의 공격·방어 영향 분석, 한국어·국내 맥락의 모델 오남용 평가, 자율형 에이전트 레드팀, 금융 등 특정 분야의 취약점 발굴 및 위협 정보 공유를 추진
- KISA는 AI 보안 안내서와 레드티밍 가이드, 위협 대응 매뉴얼을 마련하여 모델·서비스의 개발·운영 보안 수칙부터 레드팀 수행·결과 보고 및 산업별 위협 시나리오까지 대응 범위를 확대
- 「AI 기반 사이버 위협에 대응하기 위한 민간 정보보호 추진계획('26)」을 통해 KISA 취약점 관리센터·KNVD를 활용한 취약점 수집·분류·패치 지원과 민관 협력, 공급망 보안 및 국제공조 강화
- 미국 앤트로픽 주도의 Project Glasswing에 국내 기관·기업(KISA, 삼성전자, SK하이닉스 등)이 참여하여 프론티어 AI 모델 기반 취약점 탐지·방어 역량 확보

❍ (AI 활용 방어 기술 역량 확보) AI를 취약점 탐지·분석·패치 등 사이버 방어에 활용하는 기술 개발을 확대하고, 국제 경연을 통해 자동화된 취약점 대응 분야의 기술 경쟁력을 확인

- AI 기반 관제·취약점 분석과 자동 취약점 탐지·패치 기술을 중심으로, 기존 사이버 방어의 탐지·분석·대응 속도를 높이는 기술 역량을 축적
- 삼성리서치가 참여한 Team Atlanta의 DARPA AI Cyber Challenge 우승과 Theori의 3위 성과를 통해 자동 취약점 탐지·패치 분야의 국제적 기술 역량을 확인

❍ (기반 구축) AI 사이버보안 대응을 위한 법률 제정 및 기관 신설 등 기반이 빠르게 형성되고 있으며, AI 시스템의 안전성과 신뢰 확보를 위한 제도·협력체계 확대

- 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 시행('26)을 통해 생성형·고영향 AI의 투명성·안전·신뢰 확보와 AI 관련 정책·R&D 지원의 법적 기반을 마련
- AI안전연구소를 신설('24)하여 산·학·연의 역량을 연결해 AI 위험을 평가하고, 평가 결과를 정책과 기술개발로 환류하는 체계를 구축

□ **(과학기술 역할과 개선방향) AI 사이버보안 기술성과와 실제 운영 간 연계를 강화하기 위해 국내 AI 사이버 위협 대응 자산을 통합 활용하고, 성과평가를 탐지·발견에서 검증·운영 적용·사고 대응 역량까지 확대할 필요**

❍ (현주소) AI 사이버보안에서 과학기술의 역할이 자체 보호, 활용 방어, AI 기반 공격 저지, 사고 관측·통제·복구까지 확대되고 있으나, 탐지·취약점 발견 중심의 기술 성과와 실제 운영 환경의 검증·평가·통제 간 연계는 제한적

- 딥페이크·AI 피싱 탐지 기술은 새로운 생성 모델과 압축·재생·번역 등 환경 변화에 따라 성능이 저하될 수 있어, 탐지 정확도만을 중심으로 한 대응에는 한계
- AI 기반 취약점 탐지·패치 기술의 발전으로 발견 역량은 확대되고 있으나, 재현·영향 분석·회귀 시험·검토를 거쳐 실제 패치·배포까지 전환하는 과정은 병목으로 작용
- 모델의 위험이 시스템 프롬프트·RAG·도구·인증 토큰 등 실제 운영 환경에 따라 달라지고, 고위험 사이버 역량의 평가 과정에서도 외부 침해 사례가 나타나는 등 정적 모델 평가만으로는 운영 단계 위험과 평가 환경의 안전성을 포괄하는 데 한계

❍ (개선방향) 국내에 축적된 자산을 공통 데이터·시험·운영 증거로 연계하고, AI 보안 R&D 성과를 단순 탐지·발견에서 검증·운영 전환·사고 대응 역량까지 평가하는 체계로 확대 필요

- 해외 벤치마크만으로는 한국어 피싱과 국내 행정·금융 절차, 조직별 권한 체계를 충분히 반영하기 어려워, 한국어 피싱·딥페이크·프롬프트 인젝션 기준 데이터와 모델·RAG·에이전트를 함께 시험하는 재현 가능한 공통 평가 환경 고도화 필요
- AI 기반 취약점 발견 역량이 확대되면서 병목이 발견 자체보다 진위 확인·패치 설계·배포 등 후속 과정으로 이동하고 있어, 발견 건수 중심의 R&D 성과지표를 검증률·패치 수용률·안전한 배포 및 회귀·롤백 등 운영 전환 역량 중심으로 전환하고, Proejct Glasswing 초기 운영에서 확인된 검증·보완 단계의 병목을 고려하여 취약점 발견부터 실제 조치까지의 시간 단축 노력 필요
- 고위험 모델 평가 과정에서 평가망 구성 오류와 외부 접근이 실제 침해로 이어질 수 있어, 네트워크 구획·일회성 자격 증명·허용목록 기반 통신·실시간 감시·비상 중지 등 차등 적용하고, 평가 환경 보안을 공공 R&D·조달·레드팀 사업의 요건으로 강화 필요
- 에이전트가 실제 도구·권한을 활용하면서 행위와 영향 범위에 대한 지속적 평가의 중요성이 커짐에 따라, 도구 권한·행위 감시·부분 격리·롤백 및 관측·통제 가능성을 사고 대응 지표에 반영하는 한편, 평가 결과와 사고 정보 간 연계 확대 필요

③ (산업 AX) 피지컬 AI 확산 및 AI-산업 융합 본격화

- 산업 AX 가속화로 인한 피지컬 AI 확산과 함께 실제 환경에서의 성능·경제성 검증과 안전성 확보·책임 체계 정립이 중요
- 주요국은 산업 여건에 맞춘 차별화된 AX 전략을 추진하고, AI 융합·현장 실증과 산업 지능화·자율화 및 생태계 조성을 추진
- 산업현장 수요를 반영한 실증 R&D로 AX 도입 효과와 안전성·경제성을 검증하고, 핵심부품 공급망 강화와 기술개발·현장 적용·사업화를 유기적으로 연결하는 지원체계 마련 필요

□ (배경) 피지컬 AI로의 패러다임 전환과 함께 현장 적용성·수익성 검증, 안전·책임 확보 및 미·중 기술경쟁에 따른 공급망 리스크 대응이 핵심 과제로 부상

❍ (Physical AI 시대 도래) 디지털화·AI 고도화를 넘어 AI가 로봇·자율주행차·제조 등 물리적 시스템과 결합해 직접 인식·판단·행동하는 피지컬 AI로 패러다임 전환

- 지난 10년간 산업은 연결·자동화 중심의 Industry 4.0(~'15) → AI 기반 인지·예측('15~) → 생성형('22~)·Agent AI(~'25)로 발전해 왔으며, 최근에는 물리세계에서 직접 인식·판단·행동하는 피지컬 AI('25~)로 발전
- 특히 산업 특화 파운데이션 모델과 로봇·센서·시뮬레이션 기술의 결합으로 AI의 역할이 생산·물류·위험 작업 등을 직접 수행하는 수준으로 확장되면서 산업의 자동화·자율화 패러다임이 변화



※ 생성형 AI로 도식화

[그림 3] 산업 AX 패러다임의 진화

❍ (현장 적용성 및 안전·책임 이슈 부상) 피지컬 AI 산업의 경쟁축이 기술개발에서 실제 배치와 투자·수익성 검증으로 빠르게 이동하고 있으며, 안전·책임 문제에 대한 대응 필요성이 확대

- 휴머노이드 기업의 IPO가 본격화되면서 기술력뿐 아니라 매출·생산능력·현장 적용성과 ROI(Return on Investment)에 대한 시장 검증이 시작되며 산업화 가능성에 대한 평가도 강화
- Unitree(중국)는 상하이 증시에 정식 상장('26. 8. 19)하였고, 공모주 청약이 8,000배 이상 초과되는 등 피지컬 AI에 대한 자본시장 관심이 급격히 확대되고 있으며 관련 기업의 투자유치도 증가

- 피지컬 AI 오류가 단순한 업무 효율성 저하를 넘어 충돌·낙상·설비고장 등 실제 물리적 사고로 연결될 가능성이 커지면서 새로운 안전관리 체계의 필요성이 부각

※ 美 고속도로교통안전국이 운전대, 백미러, 제동 페달이 없는 완전자율주행 로보택시에 예외 승인('26. 8. 9.)
→ 소비자 안전 단체들은 공공도로 안전성이 충분히 검증되지 않았다며 우려

- 특히 휴머노이드 등 보행형 로봇은 기존 산업용 로봇과 달리 전원 차단이나 제어 오류 자체가 낙상 등 새로운 안전사고로 이어질 가능성이 존재하여 별도의 안전기준 마련이 필요

- 산업데이터·테스트베드·안전평가·표준 등을 개별 기업이 아닌 산업 차원의 공유 인프라로 구축할 필요성이 확대되고 있으며 국가 R&D의 역할도 중요해지는 상황

❍ (공급망 리스크) 미·중 기술경쟁이 핵심부품과 데이터까지 확산됨에 따라 피지컬 AI 공급망 확보가 새로운 리스크로 부상

- 미국은 외국산 첨단 이동로봇을 안보 우려를 이유로 규제하는 등 로봇 공급망을 국가안보 관점에서 관리하기 시작하면서 탈중국 공급망 확보 움직임을 강화

※ 美 연방통신위원회는 해외에서 생산된 첨단 이동로봇, 전력 인버터를 안보위협장비 목록(Covered List)에 등록('26. 7. 28.)

- 중국은 휴머노이드 완제품뿐 아니라 모터·감속기·베어링 등 핵심부품의 공급망을 확대하면서 저비용 대량생산을 기반으로 산업 주도권 확보를 추진

□ **(주요국 동향) 미국(민간·시장 중심), 중국(정부주도 및 대량생산), 일본(현장적용 확대), EU(안전·규제·산업현장 실증 중심) 등 각 국가별 차별화된 AX 전략 추진**

※ 산업 AX의 대표산업으로 제조, 모빌리티, 로봇 분야를 대상으로 분석

❍ (미국) 민간 중심의 AI 혁신을 제조·모빌리티·로봇 등 물리세계로 확장하고, 산업 특화 모델과 실제 현장 실증을 연계해 피지컬 AI의 상용화·시장 주도권 확보를 추진

- (제조) 제조 공정·설비 데이터를 학습하는 산업 특화 AI 모델을 개발하고, AI·로봇을 실제 생산현장에 적용해 생산성 향상과 인력대체 효과 등 경제성 검증을 확대

※ AWS·Microsoft 등 빅테크가 제조 특화 AI·클라우드·시뮬레이션 기술을 공급하며 피지컬 AI 산업현장 적용을 지원

- (모빌리티) 자율주행 특화 파운데이션 모델과 월드모델 개발을 확대하고, 실제 도로 주행과 시뮬레이션을 연계해 다양한 주행 환경에서 성능·안전성 및 상용성을 검증

※ Waymo는 로보택시 실도로 운행을, Tesla는 양산차 기반 대규모 주행데이터를 활용해 자율주행 AI 고도화 추진



※ 출처: Carbon Credits ('26)

[그림 4] 테슬라와 웨이모 자율주행 기술의 핵심 현황 비교

- (로봇) 범용 로봇 파운데이션 모델 개발과 함께 휴머노이드를 제조·물류 현장에 투입해 작업 성능을 검증하고, 실제 운영을 통한 비용·생산성·ROI 확보를 추진

※ Figure AI·Agility Robotics 등은 실제 산업현장 적용을 통해 휴머노이드의 상용 배치 가능성을 검증

❍ (중국) 정부 주도의 산업 육성정책과 대규모 실증·상용화 역량을 바탕으로 AI·로봇의 양산 및 현장 적용을 확대하고, 대규모 데이터 확보와 가격경쟁력을 통한 피지컬 AI 주도권 확보를 추진

- (제조) 제조·산업 데이터를 활용한 AI 모델과 지능형 로봇 개발을 확대하고, 대규모 공장에 적용해 생산성·작업 적응성을 검증하면서 피지컬 AI의 양산·확산 기반을 강화

※ 샤오미 베이징 EV 공장 등 자동화 공장을 확대하는 한편, 상하이시와 휴머노이드 로봇 혁신센터·기업이 훈련기지를 구축해 제조현장 데이터를 확보

- (모빌리티) 자율주행·스마트카 분야에서 차량 데이터와 AI 모델의 결합을 강화하고, 대규모 실도로 주행을 통해 주행성능·안전성을 검증하며 저비용 대량 상용화를 추진

※ Baidu(Apollo Go)·Pony.ai 등 자율주행 기술·서비스 기업을 중심으로 자율주행 AI와 차량 플랫폼을 통합하는 움직임이 확대

- (로봇) 범용 로봇·휴머노이드의 AI 모델과 하드웨어를 함께 개발하고 대량생산 체계를 구축해, 산업·서비스 현장 실증을 통한 성능 검증과 원가절감을 동시에 추진

※ Unitree·UBTECH 등은 휴머노이드 양산과 실제 산업현장 적용을 병행하며 가격경쟁력 확보를 추진



※ 출처: UNICON SOFT ('25)

[그림 5] Zeekr 자동차 생산공정에서 UBTECH Walker S1 휴머노이드가 작업하는 모습

❍ (일본) 제조업의 강점과 로봇 기술을 기반으로 산업 특화 AI와 피지컬 AI의 현장 적용을 확대하고, 특히 인력(노동력) 부족과 고령화에 대응하는 생산·서비스 자동화를 추진

- (제조) 제조현장의 실제 데이터를 AI 학습에 활용하는 기반을 구축하고, 산업 특화 파운데이션 모델과 로봇을 연계해 생산성 향상·현장 자동화를 추진

※ 경제산업성(METI)·신에너지산업기술종합개발기구(NEDO)는 제조 데이터의 AI-ready화와 AI 로봇·피지컬 AI용 멀티모달 기반모델 개발을 2026년부터 지원

- (모빌리티) 글로벌 기술 경쟁에 집중하기보다는 자율주행·자율배송 기술을 인력부족이 심각한 지역교통·물류 현장에 적용하고, 실제 운행을 통해 안전성·경제성·사회적 수용성을 검증

※ NEDO·국토교통성은 Level 4 지역교통과 자율주행 트럭·배송로봇의 현장 실증을 확대하며 물류효율화 추진

- (로봇) 멀티모달 AI와 로봇 파운데이션 모델을 활용해 다양한 작업에 대한 로봇의 자율학습·적응 능력을 높이고, 제조·서비스 현장에서 단계적 실증을 추진

※ NEDO를 중심으로 로봇의 작업 이해와 자율 행동을 위한 AI 기술 및 파운데이션 모델 개발을 추진

❍ (유럽) 기존 제조·자동차 산업의 기술력에 피지컬 AI를 접목하고, 실제 현장 실증과 안전·규제·인증체계를 연계해 신뢰성과 지속가능성을 확보하는 데 중점

- (제조) 제조·산업 데이터를 기반으로 한 AI 모델과 로봇의 결합을 확대하고, 실제 생산현장에서 생산성 향상과 작업자 안전을 동시에 검증하며 인간-로봇 협업을 강화

※ BMW는 라이프치히 공장에 휴머노이드 로봇을 투입, Siemens도 에를랑겐 공장에서 휴머노이드 자율 물류작업 실증

- (모빌리티) 자율주행·지능형 이동체의 AI 기술을 실제 교통환경에서 검증하고, 기술성능뿐 아니라 안전·책임·데이터 규범을 연계해 신뢰 가능한 상용화 기반을 구축

※ UNECE는 ALKS(UN R157) 등 자율주행 관련 국제규정을 마련하고, 독일 TÜV SÜD는 실도로·시험장·가상 시뮬레이션을 연계한 자율주행 시험·형식승인을 지원

- (로봇) 로봇 파운데이션 모델과 피지컬 AI의 산업 적용을 확대하는 동시에 안전·표준·인간 중심 설계를 결합해 산업현장에서의 신뢰성·상호운용성 확보를 추진

※ EU 「AI Act」 등 관련 규범과 연계해 AI 로봇의 안전성·신뢰성 및 책임 있는 활용 기반을 강화

□ **(국내 동향) AI 융합과 산업현장 실증을 확대하고, 핵심기술·부품 개발 및 산·학·연 협력을 통해 산업 지능화·자율화와 국내 생태계 구축을 추진**

❍ (제조) AI 기술과 제조업의 결합을 중심으로 산업 AX를 확대하고, AI팩토리·산업 AI Agent 및 AI 로봇의 현장 적용을 통해 제조공정의 지능화·자동화를 추진

- AI팩토리·산업 AI Agent를 통해 생산·공정·설비 데이터를 활용한 산업 특화 AI 적용을 확대하고, 제조공정의 자동화·자율화 및 생산성 향상을 위한 AI 기반 제조시스템 구축을 추진

※ 산업부는 M.AX 얼라이언스 출범('25)을 통해 제조업 AI 전환을 위한 앵커기업 중심 산·학·연 협력을 강화하고, AI 자율제조·산업 AI 등 제조현장 중심의 AI 활용 확대를 추진



※ 출처: 전자신문 ('25)

[그림 6] M.AX 얼라이언스 10대 분야 구성

- AI 로봇·휴머노이드의 제조현장 실증을 확대하고 반복·위험작업을 중심으로 로봇 활용을 추진하는 등 AI와 로봇을 결합한 제조현장의 자동화·지능화 적용 범위를 확대

❍ (모빌리티) SDV·차량용 AI를 중심으로 차량의 소프트웨어·지능화를 추진하고, 자율주행 기술의 실도로 실증과 서비스 적용을 확대하며 AI 기반 모빌리티 전환을 추진

- SDV·차량용 AI 반도체를 기반으로 차량 소프트웨어와 AI가 차량의 주요 기능을 제어하는 기술 개발을 확대하고, 차량 주행데이터를 활용한 차량 지능화 및 서비스 고도화를 추진

- 자율주행 기술의 실도로 실증과 서비스 적용을 확대하고, 자율주행 차량·로보택시 등 다양한 모빌리티 서비스와 연계하여 AI 기반 이동체의 실제 운행 및 상용화 기반을 확대

※ 국토부는 '자율주행 실증도시 추진방안('26)'을 발표하고, 광주 전역을 하나의 자율주행 실증무대로 운영하여 로보택시 등 자율주행 서비스의 실도로 실증을 확대 추진

❍ (로봇) 휴머노이드·AI 로봇의 지능기술과 핵심부품 개발을 확대하고, 산업현장 실증과 기업 간 협력을 통해 AI와 로봇의 결합 및 국내 로봇산업 생태계 구축을 추진

- 멀티모달 AI·VLA·월드모델 등 로봇 지능기술 개발과 휴머노이드 로봇 개발을 추진하고, 제조·물류 등 다양한 산업현장에서 AI 로봇의 작업 수행 및 실증을 확대

- 액추에이터·감속기·모터·센서 등 로봇 핵심부품의 국산화·고도화를 추진하는 동시에 국내 기업 간 협력을 확대하며 휴머노이드 관련 기술·부품·서비스 생태계 구축을 추진

※ 산업부는 K-휴머노이드 연합을 출범('25)시키고, 로봇 AI 공용모델·휴머노이드 핵심기술·AI 반도체·배터리 등 핵심 분야의 산·학·연 협력을 추진

□ **(과학기술 역할과 개선방향) 산업 AX의 생산성·안전성·경제성 검증과 핵심부품 공급망 확보를 위해 수요 기반 실증 R&D를 강화하고, 기술개발부터 현장 적용·사업화까지 연계하는 지원체계 구축 필요**

❍ (현주소) 국내 산업 AX의 생산성·안전성·경제성 검증 및 핵심부품 공급망 확보가 주요 이슈로 부각

- (제조) AI 모델·로봇·센서 등 핵심기술의 제조현장 적용이 확대되고 있으나, 실제 생산공정에서 기술 간 연계 수준과 생산성 향상 효과, 투자 대비 경제성 등에 대한 검증 사례는 제한적

※ 국내 스마트공장 도입기업의 75.5%가 기초단계에 머물러 있으며, 제조AI 도입률은 0.1% 수준('25)

- (모빌리티) 자율주행·SDV 등 차량 지능화 기술의 실도로 적용이 확대되고 있으나, 다양한 주행 환경에서의 안전성 검증과 사고 대응·책임 체계, 서비스 운영을 통한 상용성 확보 등이 과제로 인식

※ 국내 자율주행 시범운행지구 사고 '22년 2건 → '25년 37건으로 증가 및 누적 66건 중 8건이 자율주행 시스템 오류가 원인('26)

- (로봇) 정부 R&D 기반 AI 로봇·휴머노이드의 산업현장 실증이 시작되고 있으나, 핵심부품의 기술·가격 경쟁력과 공급망 확보, 파운데이션 모델 개발을 위한 데이터·학습체계 등이 주요 이슈로 부각

※ 국내 로봇 부품·소프트웨어 수입액은 2024년 1,736억 원으로 전년 대비 28% 증가('25)

❍ (개선방향) 산업별 실증 R&D와 응용서비스 생태계 조성을 강화하고, 세제·금융·바우처 등 초기 도입 인센티브를 확대하여 기술개발부터 현장 도입·운영·사업화까지 연계하는 산업 AX 지원체계 구축 필요

- (제조) 제조기업의 실제 생산공정에서 AI·로봇 적용 전후의 생산성·인건비 등을 정량 비교할 수 있는 제조AI 실증 R&D에 투자하고, 유사 제조현장 확산을 위한 업종별 성공모델 표준화 지원

※ AI팩토리·M.AX 얼라이언스 등 기존 사업과 연계하여 수요기업이 직접 실증공정을 제시하고, 기술개발 기관(공급기업 등)과 공동으로 데이터 구축→AI·로봇 적용→성과측정까지 수행하는 수요기반 R&D 방식 강화

- (모빌리티) 주행데이터·시뮬레이션·시험도로를 연계한 통합 검증 R&D를 지원하고, 안전성뿐 아니라 운행비용·원격관제 인력·서비스 수익성 등을 포함한 상용성 검증을 성과지표에 반영토록 유도

- (로봇) 핵심부품의 성능·신뢰성·가격경쟁력을 동시에 확보하고, 국내 부품기업과 완제품 기업이 공동으로 참여하는 수요연계형 R&D에 투자를 통해 국산 부품의 실제 로봇 적용과 공급망 진입을 지원

- (추진체계) 산업별 AI 응용서비스와 기존 시스템 기술 간 연계성 확보 및 컨설팅·솔루션·시스템 구축 기업과 수요기업 간 협력 지원을 통해 현장 도입·운영 강화 필요

※ 업무 진단·데이터 정비·모델 선정·시스템 구축·운영인력 교육 등 도입 전주기를 지원하고, 업종별 공통 모듈과 도입 지침 마련을 유도하여 수요기업의 기술적·인력적 진입장벽 완화

- (지원수단) 정부의 마중물 지원을 통해 기업의 초기 비용과 도입 위험을 분담하고, 실증 관련 세액공제 확대·AI 설비투자 정책보증·도입 바우처 등 세제·금융·재정 지원수단의 연계 강화

※ 실증비용에 대한 세제지원 범위와 요건을 검토하고, AI·로봇 설비 및 시스템 구축을 위한 정책보증과 컨설팅·솔루션 도입 바우처를 연계하여 중소·중견기업의 AX 참여 촉진

④ (공공 AX) 국민체감 및 문제해결형 공공 AI 서비스 확대

- 공공문제 해결을 위한 AI R&D와 데이터·인프라 지능화, 현장 적용을 연계해 행정 효율성·재난안전 대응 역량·국민 체감형 서비스를 강화하는 공공 AX를 추진
- 공공 안전 및 복합적 문제해결을 위하여 기술혁신 과정에 AI를 도입하려는 시도가 확산되고 있으나, 부처별 파편화된 시도에 그쳐 진정한 AX에는 이르지 못하는 상황
- 공공 AX R&D의 부처 간 연계와 현장 적용의 실효성을 높이기 위해 AX 협의체를 구성·운영하고, 공통 자원의 공동 활용과 단계별 검증·운영 결과의 환류체계 강화 필요

□ **(배경) 공공 AX는 국민 수요에 맞춘 서비스 영역 확대와 AI 기반 업무 전 과정의 연계·고도화를 통해 서비스 품질과 행정 생산성을 높이고, 민간 시장 창출과 해외 확산을 촉진하는 방향으로 발전**

○ (공공서비스 영역 확대) 효율성 중심의 디지털 정부를 넘어 국민 수요에 맞춘 다양한 AI 맞춤형 서비스를 제공하여 문제해결력·예측가능성·생산성·투명성 등을 개선하려는 움직임이 가시화

- AI와 공공데이터를 활용하여 개인의 생애주기와 상황을 분석한 국민 수요 맞춤형 복지·고용·의료·교육 서비스 제공
- 다양한 데이터(교통, 감염병, 재난, 범죄, 기상 등)를 실시간으로 분석하여 AI 기반 위험 징후 탐지, 피해 범위 예측 등 선제적 위기 대응력 제고에 활용
- 문서 작성·검색, 회의록 정리 등 반복 업무에 AI를 활용함으로써 행정 생산성을 높이고, 고령화 등 인구구조 변화에 따른 인력 부족 문제 해결에 AI 기술이 기여 가능

〈표 8〉 공공 AX 서비스 영역

구분	주요 역할
행정업무 지원	문서 초안 작성, 요약, 번역, 회의·보고자료 작성
정부지식 검색	법령·규정·정책자료 및 내부 데이터 검색
민원·고객 서비스	챗봇·음성봇을 통한 질의 응답과 안내
보건·의료	의료영상 분석, 질병 발생 신호 및 연구문헌 탐색
재난·환경	기상재해와 자연재난 예측, 위성·드론 영상 분석
감사·재정·인력 관리	부정수급·이상거래 탐지, 조달·보조금 위험 분석, 교육 지원 등

○ (공공서비스 품질 향상) 공공 부문의 AI 활용은 단순 질의응답을 넘어 생성형 AI·AI 에이전트로 고도화되고 데이터 간 연계 및 시장 창출의 주체로 전환

- 초기에는 챗봇 및 문서요약 등 단일 서비스 실증이 중심이었다면, 최근에는 업무 전과정* 연결하는 방향으로 발전

  * 예) 정책자료 수집 및 보고서 작성 지원, 민원 내용 분석을 통한 담당부서 자동 배정 등

- 공공 AI 시장 확대를 통해 국내 기업의 레퍼런스를 확보하고, 검증된 서비스를 해외 시장으로 확산하는 추세

□ (주요국 동향) 주요국은 공공문제 해결을 위한 AI R&D와 데이터·인프라 연계를 확대하고, 현장 실증·검증 및 운영체계 통합을 통해 행정 효율성과 재난·안전 대응 역량을 강화

❍ (미국) 기존 시스템 및 업무방식의 전부처 AI 전환 가속화와 함께 엄격한 마일스톤 관리를 토대로 공공 AX의 점진적 지능화 추구

- ('16) AI 기반 공공문제 해결 탐색* → ('20) 국가 AI 기반 구축 → ('23~'24) 생성형 AI 확산과 위험 기반 관리 강화** → ('25~'26) 신속한 도입과 성과 창출 단계로 진입***

* (오바마 정부) 국가과학기술위원회 산하에 기계학습·AI 소위원회를 설치('16)하여 AI를 공익과 효율적인 정부 구현에 활용하는 방안 모색

** (바이든 정부) 행정명령 14110호('23)과 OMB 지침 M-24-10('24)을 통해 AI 활용에 대한 정부 공통 관리체계 강화

*** (트럼프 정부) 행정명령 14179호('25)를 통해 AI 혁신을 저해하는 규제·정책 장벽의 해소를 추진하고, OMB M-25-21('25)을 통해 혁신·거버넌스·공공 신뢰를 3대 원칙으로 연방기관의 AI 도입 및 활용 가속화

공공 AX 적용 사례



해양대기청(NOAA)의 AI 기반 글로벌 예보 환경인 Project EAGLE은 공통 데이터 플랫폼에서 반복적 테스트를 거친 후 기존 운영모델과 성능 비교를 통해 엄격한 실증을 거쳤고, 이후 운영환경을 검증하여 '25년 말부터 실제 예보 체계에 편입됨. 이 과정에서 AI 기반 모델이 기존 현업 시스템을 대체할 수 있는 단계적 기준을 엄격하게 설정하여 모델 대체에 따르는 부작용을 최소화하고 정확도를 제고하는 보완 장치를 마련

※ 출처: NOAA 웹사이트 (https://www.epic.noaa.gov/ams-ai-presentations)

- 미국 회계감사원(GAO)이 11개 연방정부기관의 AI 활용사례를 조사한 결과, 571건('23)에서 1,110건('24)으로 2배 증가, 생성형 AI 활용 사례*는 약 9배 증가(32→282건)

* 보건복지부(HHS, 116건), 국토안보부(DHS, 36건), 보훈부(VA, 27건), 에너지부(DOE, 26건) 등의 순

- 개별 공공 AX 프로젝트의 목표가 단순 AI 기술개발 및 실증이 아니며, NIST가 제안하는 기준에 근거해 TEVV* 프로세스에 따라 검증하며 통합적 관리체계**가 운영됨

* TEVV(Test, Evaluation, Validation and Verification)에 따라 데이터의 대표성, 적합성, 시스템 신뢰성, 측정지표 등을 종합적으로 검증

** AI 활용 사례를 대외적으로 공개하고 GAO가 상위 차원에서 추진현황을 점검하며, 공공 목적성에 부합하는 개발이 이루어지고 있는지 점검 및 개선을 요구

❍ (EU) 공공안전 분야 AI R&D와 데이터·인프라 연계를 강화하고, 재난·재해 예방 및 위기 대응 등 정책 현장 활용을 확대하는 한편, 국가·기관 간 공동 실증을 통해 AI의 공공서비스 내재화 및 현장 적용 역량 제고

- 공공부문을 주요 AI 적용 분야에 포함하고, 정책·조직 운영 과정에서 AI 활용 가능성과 위험을 함께 검토하는 'AI 우선 고려(AI-first)' 접근을 제시(Apply AI Strategy('25))

※ AI 인프라·데이터·시험시설의 연계를 통해 연구성과의 현장 적용을 촉진하고, 공공부문에서는 유럽 AI와 오픈소스 솔루션 활용을 강조

- Horizon Europe의 핵심 6개 클러스터 중 '사회를 위한 시민 안보(클러스터3)'을 통해 재난 대응력 강화, 범죄 및 테러 대응, 국경선 관리, 인프라 회복력, 사이버 보안 등 분야의 R&D 지원(EC, '25a)

※ AI는 공공안전 임무의 달성 수단으로 간주하며, 지침상에서는 재난대응, 사이버보안 등 다수의 세부 주제에서 AI를 유망한 문제해결 수단으로 활용할 것을 명시적으로 권고함

※ 단순한 AI 기술개발 차원을 넘어 공공데이터 인프라에 AI를 연결하고, 실제 정책 담당자가 이를 활용하면서 여러 국가·기관에서 실증할 것을 요구하는 등 기술 내재화를 고려(EC, '25b)

공공 AX 적용 사례



실제 해양 환경을 디지털 데이터로 구현한 유럽디지털트윈오션(European Digital Twin Ocean)은 매년 약 1.5천만 유로를 투자하여 구축하는 무료 공공 인프라로, 이것을 통해 연구자가 AI 모델링, 시뮬레이션, 예측 알고리즘 등을 개발함으로써 해양 지식을 확장하고 안전 및 정책 대안을 모색할 수 있음

※ 출처: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/eu-missions-horizon-europe/restore-our-ocean-and-waters/european-digital-twin-ocean_en

❍ (일본) 공공서비스 유지·강화를 위해 행정용 생성형 AI의 자체 개발·검증과 SIP 기반 AI·디지털 트윈 R&D와 현장 실증을 통해 재난 대응 역량을 고도화

* SIP: The Cross-ministerial Strategic Innovation Promotion Program

- 디지털청은 AI 이용 기반과 행정업무용 애플리케이션을 직접 개발하고, 실제 업무에서 활용 상황과 문제점을 검증하여 정부 내 확산에 필요한 경험을 축적

- SIP 3기의 AI·디지털 트윈 기반 재난 예측·대응 기술개발과 현장 실증을 추진하고, 기존 SIP4D의 데이터 연계 성과를 SOBO-WEB 등 현업 시스템으로 확산하여 연구개발과 실제 재난 대응 간 연계를 강화

※ SIP 1기에서 개발된 SIP4D(Shared Information Platform for Disaster Management)는 기관별 재난정보를 수집·변환·배포하여 조직 간 정보 공유와 상황인식의 일치를 지원하는 기반으로, 이후 단계의 재난 대응 기술개발과 실증에 활용

❍ (중국) AI 관련 최상위 정책 아젠다인 「인공지능+」를 통해 사회 거버넌스 고도화, 안전 관리 역량 및 국가 안보 강화, 국토·생태 거버넌스 혁신 등 공공 거버넌스에서 AI 역할을 뚜렷하게 강화한다는 목표를 제시(国务院, '25)

- 국무원은 AI를 활용하여 안전 관련 모니터링 및 예·경보 강화와 현장구조 및 사회동원 능력 제고를 추구하며, 환경 분야에서도 AI 기반 모니터링, 예측, 시뮬레이션, 문제해결을 추진

- 「차세대 인공지능 발전 계획」에서 공공안전 AI를 지능형 사회 건설 과제로 반영하여 지능형 모니터링·조기경보 및 통제 체계 구축을 추진하는 한편, 심해 공간 스테이션·건강보장 등 중대 프로젝트와 스마트시티·스마트 농기계 장비 등 중점 프로젝트에서도 AI 응용 시범을 병행 강화하는 방향을 제시(国务院, '17)

□ (국내 동향) 국민 체감형 AI 공공서비스를 확대하고, 부처별 임무 중심의 R&D와 공공 인프라 지능화를 연계해 공공부문 전반의 AX를 추진

❍ 정부는 「대한민국 인공지능 행동계획('26)」을 통해 공공 AX를 12대 전략분야의 하나로 제시하고 있으며, 최종 수요자인 국민의 삶의 질 향상에 기여할 수 있는 다양한 AI 기반 공공서비스를 제공할 계획

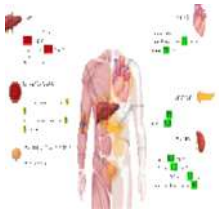
- AI를 활용한 최고의 대국민 서비스 제공, 공공시장의 AI 테스트베드화, K-Gov AX 모델의 글로벌 확산 및 K-AI 얼라이언스 구성 등 공공 AX 촉진을 위한 15개 세부과제 제시
- 세계 1위 AI 정부 도약 목표 설정과 함께 AI 업무관리 플랫폼 구축, 공공분야 AI챔피언 양성, 공공데이터 공개, 공공 AI 영향평가 등 전과정의 AX 전환과 연계 강조
- 일상에서 모두가 AI를 자연스럽게 활용하고 AI에 의한 변화를 직접 체험할 수 있는 '모두의 AI' 플랫폼을 구축하여 포용적 AI 가속화

❍ 부처별 고유 임무에 AI 기술을 적용하여 효율성 및 효과성을 제고하기 위한 기술개발이 진행되고 있으며, 기술 확보를 위한 R&D 프로젝트와 함께 공공 인프라의 지능화도 동시에 추진

- (기후부) 수자원 시설 관리 및 수요 대응, 수재해 감시, 생태계 복원 및 감시, 폐의류 재활용 등 부문에서 AI를 적용한 R&D 프로젝트를 진행하며, 실증 플랜트, 에너지 배관 및 설비, 전력망 등 인프라의 지능화를 추진
- (과기정통부) 산하 정부출연연구소를 통해 탄소위기 대응, 질병 조기 경보, 공공 에이전트 개발 등 AI 관련 기초·원천기술 확보형 프로젝트를 지원하며, 치안 유관 부처와 협력을 통해 범죄 예측, 전자 감독, 치안 현장 기술개발 등을 추진
- (국토부) 보안 검색, 초고층 시설물 재난관리, 교통 단속, 지역 재난 안전 관리 등 분야에서 AI를 적용한 R&D 프로젝트를 추진하며, 기술개발 성격 과제보다는 공공 인프라 관련 R&D 투자에 더 큰 비중을 두고 중점 추진
- 해수부, 기상청, 산림청, 행안부, 문체부 등에서도 각 부처·청의 고유 임무를 고도화하기 위해 AI 기술을 개발·서비스

※ (해수부) 연안 재해 예측, 기후변화 대응, 해양 자원 탐사 등, (기상청) 기상업무, 기상위성 활용, 기후예측 시스템 개발 등, (산림청) 산불 대응 솔루션 및 임도 설계 분야 등

공공 AX 적용 사례



의료영상 데이터에 인공지능의 기계학습과 분석·예측할 수 있는 알고리즘 등 SW 개발을 통해 안과, 흉부 등 다양한 의료 분야에 적용할 수 있는 솔루션 기술개발과 의료서비스 역량 강화에 기여

※ 출처: www.kistep.re.kr(우수성과)

□ (과학기술 역할과 개선방향) 공공 AX R&D의 부처별 분산과 현업 전환의 불확실성을 줄이기 위해 AX 협의체 구성·운영하고, 공통 기반의 공동 활용, 단계별 검증과 운영 환류 강화 필요

❍ (현주소) 개별 부처 차원의 임무 달성을 위한 파편화된 AX 프로젝트들이 다수 추진되고 있으며, 확보된 AI 기술을 현업으로 전환하는 기준과 프로세스가 다소 모호

- 과기정통부·행안부 중심의 공공 AX 지원 체계가 신설('26.3.)되었으나, 공공 AX의 임무 설정으로부터 공통 기반기술 개발·보급, R&D 포트폴리오 구축, 협업 및 성과 환류까지 연계 구조는 불명확
- 복잡한 사회문제 및 기후·기상 문제를 해결하기 위하여 여러 부처가 고유의 전문성을 살린 협업을 통해 솔루션을 도출해야 하나, 현재는 개별 부처의 현업 대응적 R&D가 주류를 이루어 데이터 연계 및 공동 플랫폼 활용을 통한 시너지 창출이 다소 부족
- AI 기술개발 및 공공인프라의 지능화가 실험 및 실증 단계의 성과 창출에 집중하고 있어, 개발된 기술이 현업 시스템에 체화되기 위한 구체적 마일스톤 설정 및 피드백 구조가 다소 모호

❍ (개선방향) 개별 부처의 현업 개선 대신, 공공 문제해결을 위한 상위 차원의 임무를 중심으로 하위 AX R&D 프로젝트를 재구성하는 임무 중심형 포트폴리오 접근을 통해 투자 효율성과 협업 성과를 높일 필요

- 부처 및 사업별로 데이터, AI 모델, 플랫폼을 개별 구축하는 방식은 장기적인 비용 분절과 기술의 파편화를 초래하므로 신설된 범부처 AX 협의체를 정례적으로 연계·환류하는 명시적 프로세스 도입 검토 필요

※ 임무별 AX 사업 포트폴리오 작성 ⇨ 중복·공백 영역 점검 ⇨ 공통기반 활용 가능성 검토 ⇨ 현업 전환 상태 점검 ⇨ 성과평가 및 차년도 예산 환류

- 국가 R&D에 범용적으로 적용할 수 있는 공통 기반*을 개발하여 각 부처에 보급하고, 각 부처의 R&D 활동은 공통 기반 위에서 특화 임무에 집중하는 방식으로 접근할 필요

* 공공 및 재난안전 데이터 플랫폼 표준, 공통 GPU 및 AI 컴퓨팅 인프라, 공공 분야 특화 파운데이션 모델, 공통 RAG, 디지털 트윈 및 시뮬레이션 환경, AI 평가·검증용 벤치마크 데이터 셋, 모델 레지스트리 및 성능이력 관리 체계 등

- 기존 TRL 중심의 공공 AX R&D 관리 체계에 기술성숙도와 사업별 성과평가에 생애주기 전반의 시험·평가·검증·타당성 확인(TEVV)*을 보완하고, 현업 도입 여부를 판단할 수 있는 단계별 기준 마련 필요

※ AI 기반 시스템 및 서비스가 기존 체계 대비 최종 수요자 관점에서 어떠한 차별적 가치를 실효적으로 제공하는지 단계적으로 검증하고, 성능과 안정성을 기준으로 현업 시스템의 전환·대체 가능성을 평가해 공공 시스템의 실질적 개선을 견인할 필요

* AI 기술개발 ⇨ 데이터 및 모델 TEVV(Test, Evaluation, Validation, and Verification) ⇨ 실제 현장환경 실증 ⇨ 기존 시스템과 비교·평가 ⇨ 현업 시스템 편입 또는 점진적 전환 ⇨ 실제 환경에서 운영 후 모니터링 및 업데이트

⑤ AI for Science와 과학기술 R&D 패러다임 전환

- AI를 단순 지원 도구가 아닌 R&D 수행 방식 자체를 바꾸는 '메타 이슈(Meta-issue)'로 접근, 과학 특화 AI 모델과 자율 연구 에이전트를 중심으로 연구 패러다임 전환이 가속화
- 우리나라를 포함한 주요국은 국가 차원의 AI 연구기반을 통합·강화하고, 과학 특화 모델과 자율 연구 시스템을 활용해 연구생산성 향상과 과학난제 해결을 추진
- AI 기반 연구혁신이 과학적 성과로 이어지도록 데이터·연산자원의 공동 활용과 기관 간 협력을 강화하고, 가설 생성부터 실험·검증·재학습까지 연결되는 연구 전주기 체계의 고도화 필요

□ (배경) AI가 가설 설정·실험 설계·분석 등 연구 전주기를 혁신하는 AI for Science가 확산되며, 과학 AI 모델과 자율 연구 에이전트 개발 경쟁이 본격화

❍ (연구생산성의 감소) R&D 투자 확대에도 연구생산성 저하 추세가 관찰되고 있으며, 특히 바이오 제약 분야는 기술 발전에도 불구하고 '50~'10년 실질 R&D 투자액 대비 FDA 신약 승인 효율이 약 80분의 1로 감소하는 등 기존 연구개발 방식의 효율성 한계 노출

- 신약 개발의 경우 투자비용 10억 달러당 승인된 신약 수가 지난 수십 년간 지속적으로 감소해왔으며, 이러한 생산성 병목은 '에룸의 법칙(Eroom's Law)*'으로 형상화되어 재료과학·에너지 등 과학기술 전(全) 분야에서 공통으로 나타나고 있음

  * 신약개발의 효율성이 9년마다 절반으로 감소하는 현상에 대한 관찰 법칙으로, 무어의 법칙(Moore's Law)을 반대로 뒤집어 표현

- 전통적인 실험·계산으로는 기하급수적으로 팽창하는 데이터와 복잡한 물리·화학적 시스템을 해석할 수 없어 AI가 대규모 데이터의 숨은 패턴을 추출해 연구 속도를 앞당기는 대안으로 부상

❍ (과학연구 패러다임 전환) AI4S(AI for Science)는 짐 그레이가 제시한 4대 패러다임(경험→이론→계산→데이터)에 이어 AI가 가설 설정부터 실험 설계, 데이터 분석까지 자율적으로 수행하는 제5차 패러다임으로 규정되며, CACM 논의를 거쳐 국내외 정책·학술 문헌의 공통 개념으로 제시

※ 「The 5th Paradigm: AI-Driven Scientific Discovery」 (Communications of the ACM(CACM), '24.12)

- 제4차 패러다임은 대용량 데이터를 바탕으로 통계적 상관관계 도출에 머물렀다면, 제5차 패러다임은 AI가 직접 연구 수행의 주체가 된다는 점에서 기계의 역할 범위가 명확히 구분

- 우수한 성과를 내기 위해서는 AI 시스템을 연구 목적에 맞게 설정하고, 다중 에이전트(Multi-agent) 간의 역할을 분담시키는 능력이 필수적인 연구 역량으로 자리 잡고 있음

- AI 도입으로 제약·재료·항공우주·반도체 분야의 R&D 속도가 1.2배 이상 향상될 가능성이 제시되며, AI 활용 연구자의 연간 논문 수와 인용 수가 비활용자 대비 각각 3.02배, 4.84배로 나타나는 등 AI 활용 역량의 중요성 증대(McKinsey(2025), Nature(2026) 등)

- AI는 특정 분야를 지원하는 도구가 아니라 모든 과학기술 분야의 연구방법론 자체를 혁신하는 메타 이슈로, 글로벌 빅테크 기업들은 이미 과학 AI 모델을 활발히 개발

※ 구글 'AI Co-Scientist'('25)의 과학적 가설 생성·검증 지원, 앤트로픽 'Claude Science'('26)의 데이터 분석·연구 도구 통합 등 AI 기반 과학연구 지원 플랫폼 개발·확산

□ (주요국 동향) 주요국은 컴퓨팅·데이터·실험시설을 연계한 국가 차원의 AI 연구기반을 구축하고, 과학 특화 모델과 자율 연구 시스템 개발 및 산학연 협력을 통해 연구생산성 제고와 과학적 발견 가속화

❍ (미국) 에너지부(DOE)의 '통합연구 인프라 프로그램(Integrated Research Infrastructure, IRI)'을 통해 국립연구소의 실험시설·데이터·연산 자원을 하나의 운영체제로 통합하고, '제네시스 미션(Genesis Mission)'을 통해 10년 내 연구 생산성 2배 제고를 목표로 산하 17개 국립연구소의 역량 결집

- 에너지부 주최 'AI for Science' 타운홀('19) 결과, AI·빅데이터·HPC를 결합해 재료과학·환경·생명과학 등 다양한 분야의 혁신을 가속화하는 전략적 로드맵 논의가 본격화
- FASST* 이니셔티브('24)는 산학연 협력 생태계 구축을 한 축의 핵심 목표로 설정하여, 모델의 가중치를 대중과 과학계에 투명하게 공개하는 오픈웨이트(Open-weight) 방식을 채택한 Genesis-Science-1** 발표('26.7.) 및 연내 공개 예정

  * Frontiers in Artificial Intelligence for Science, Security and Technology

  ** 미국 에너지부(DOE)와 LLM 개발 스타트업인 Arcee AI가 파트너십을 맺고 공동 개발 중인 1조 매개변수급 과학 연구용 대형 언어 모델로, '26년 말 기술 보고서 및 공개 시연
- '제네시스 미션('25, EO 14363)'을 통해 AI를 인프라 전반에 통합하고 민간 파트너십을 확장하는 실행 단계에 진입하였으며, 이후 HPDF*의 정식 가동과 함께 자율 실험실(Autonomous Labs) 환경을 완성할 계획

  ※ 구글·AWS·엔비디아 등 24개 기업과 MOU 체결('25.12), 4대 핵심분야에 3억 2천만 달러 투자계획 발표('25.12)

  * HPDF(High Performance Data Facility): 대규모 과학 데이터 전용 데이터센터 프로젝트('27~)

❍ (중국) 국가자연과학기금위원회(NSFC)의 하향식 지원을 바탕으로 국가 주도의 「AI+ 이니셔티브」를 추진하고 있으며, 컴퓨팅(SCNet)·인프라(AICC)·네트워크(CSTNet/FNTF)·데이터 표준화에 걸쳐 하나의 국가 단위 AI4S 플랫폼으로 결속

- 국가 슈퍼컴퓨팅 네트워크*(National Supercomputing Network, SCNet) 상에서 연구 프로세스 자동화, 지식 베이스를 통합한 '과학계산 지능형 에이전트(Scientific-Computing Intelligent Agent)'를 공개('25)하여 중앙집중형 AI4S 인프라 전략의 핵심을 마련

  * 고성능 컴퓨팅(HPC) 및 AI 연산 인프라의 자립도를 높이기 위해 전개 중인 프로젝트로 전국 30개 이상의 슈퍼컴퓨팅 센터를 통합하여 1,000개 이상의 기관이 즉시 사용 가능
- SCNet에서 검증된 지능형 에이전트를 초거대 인공지능 컴퓨팅 센터(Artificial Intelligence Computing Center, AICC)에 전면 탑재해 AI가 스스로 가설·시뮬레이션을 수행하는 '무인 연구소' 체제로 확산할 계획
- 「과학 데이터 관리 방법('18)」으로 과학데이터를 국가 전략자산으로 재정의하고, 「생성형 AI 데이터 라벨링 보안 규격('25)」을 통해 파편화된 원시데이터를 SCNet·AICC가 즉시 학습 가능한 'AI-Ready' 상태로 가공하는 데 국가 역량을 집중
- 중국과학원(CAS)은 CAS 산하 12개 연구소가 공동 개발하여 8대 과학분야를 통합한 'ScienceOne'을 오픈소스로 공개('25)

- ScienceOne: 멀티모달 과학 파운데이션 모델 -

· MoE(Mixture-of-Experts) 구조 기반의 AI Agent를 통해 문제해결을 위한 최적의 서브 모델이 할당
  └ S1-Literature: 기존 3~5일 소요되던 문헌조사를 20분 내 완료
  └ S1-ToolChain: AlphaFold·MATLAB 등 300개 이상의 전문 연구 툴을 스스로 계획·호출하는 AI Co-Scientist
· 공개 모델은 S1-Base-8B / S1-Base-32B이며, 알리바바 Qwen3-8B/32B를 기반으로 개발

❍ (EU) EC는 「Apply AI Strategy」와 「A European Strategy for Artificial Intelligence in Science」를 동시 발표하고('25), 핵심 실행계획으로 RAISE 플래그십 이니셔티브를 내세워 분산된 컴퓨팅·데이터 자원을 통합

※ EU는 RAISE('25) 시범사업에 1.07억 유로를 배정하고, EuroHPC JU 기반 AI 인프라 확충과 연계해 AI 기가팩토리 구축에 최대 100억 유로의 공공재정을 지원하고 최소 200억 유로의 민간투자 유치 추진

- 'Science for AI'와 AI를 활용해 새로운 발견을 하고 이끄는 'AI for Science'를 이중 목표로 설정하고 컴퓨팅·데이터·인재양성·펀딩에 초점을 두어 설계하고, 전략-자문-운영-인프라의 4계층 거버넌스를 구성

- RAISE는 물리적 신규시설 없이 기존 자산*을 연결하여 하나의 거대 연구소와 같이 다수의 연구자가 동일 수준의 자원에 접근하도록 하는 '가상 AI 연구소'를 지향하며, 자원공유 기관에 인센티브를 제도화하여 현재 16개국에서 19개 팩토리 구축 진행

* EuroHPC JU(연산 인프라, '18~), Horizon Europe(운영 및 관리, '21~'27), EOSC(데이터 관리, '18~) 등 각 계층의 기존 프로그램과 연계 운영

- 「AI Act('24)」는 신뢰성 기반의 혁신을 지향하면서도 연구 목적의 AI 시스템과 모델을 규제 적용 대상에서 제외하여 과학 연구의 자유를 보장하고, AI 규제 이행 지원 데스크와 가이드라인을 제공

❍ (일본) AI 촉진법('25)을 출발점으로 문부과학성(MEXT)·이화학연구소(RIKEN) 주도로 'TRIP-AGIS' 프로그램을 가동하고 제조업 강점을 살려 기업 데이터를 AI4S 자산으로 전환

※ 'TRIP(Transformative Research Innovation Platform)-AGIS(Advanced General Intelligence for Science): 연구 전주기를 AI가 지휘하는 자기완결형 연구 환경 및 모델

※ '26년부터 5년간 총 1조 엔 규모의 '일제 AI' 개발 사업과 연계

- '25년도 총 1,527억 엔을 투자하여 AI4S 관련 과학연구혁신프로그램, 과학연구용 AI기반모델 개발, 대규모 오토메이션·클라우드랩 구축, 차세대 후가쿠 개발 등에 지원

- 슈퍼컴퓨터 후가쿠(FugakuNEXT)와 'AI 특화 차세대 슈퍼컴퓨터'('26)를 결합하여 가설 수립-논문 분석-로봇 제어를 수행하는 자율 연구 시스템을 구축하고, '26년 초부터 과학 특화 파운데이션 모델 서비스를 연구 커뮤니티에 개방

- 3대 국립연구기관(AIST·RIKEN·NICT)을 거점으로 대학 및 117개 민간 회원사를 연결하는 범국가적 산·학·연 통합 AI Japan R&D Network를 구성

□ (국내 동향) K-문샷 프로젝트를 중심으로 임무별 책임운영체계와 컴퓨팅·과학 AI 모델·자율실험실·연구데이터 기반을 강화해 연구생산성 제고와 국가 과학난제 해결을 추진

❍ 정부는 K-문샷 프로젝트를 통해 피인용 상위 1% 논문 점유율을 4.1%('23)에서 8.2%('30, 세계 5위)로 제고해 연구생산성을 2배로 높이고, '35년까지 8대 분야 12대 국가미션을 과학기술×AI로 해결하는 것을 목표로 설정

- 범국가 K-문샷 추진단과 미션별 PD 중심 책임운영체계를 골자로 하며, PD에게 세부과제 조정·마일스톤 기반 전주기 관리·연구목표 전략적 재설정 권한을 부여하고 'K-문샷 특별법' 제정을 추진함

- 과기정통부 주도 및 국가과학AI연구센터('26)를 컨트롤타워로 하며, 「국가연구데이터 관리 및 활용 촉진에 관한 법률」 제정('27.5. 시행 예정) 등 AI 학습용 연구데이터의 국가 자산화 근거 마련 착수



※ 출처: https://www.donga.com/news/Economy/article/all/20260225/133420432/1

[그림 7] 국가 과학난제 미션

❍ 컴퓨팅·모델·자율실험실·데이터 4대 축의 투입 계획을 구체화하여, GPU는 슈퍼컴 6호기 8,500개 중 약 30%와 첨단GPU 확보사업분(3,000장 이상), 바이오·소재 전용 인프라(2,500개 이상) 등 8천 장 이상 확보 추진

- 바이오·재료화학·수학·반도체디스플레이·이차전지·지구과학 등 6대 분야 파운데이션모델에 5년 간 총 7,000억원을 투입하고, 산업부는 500개 AI 자율실험실 단계적 도입·확산('25~'30)

※ 바이오(2,000억원), 재료화학(1,200억원), 수학·반도체디스플레이·이차전지(각 1,000억원), 지구과학(800억원) 등

- 「국가연구데이터 관리 및 활용 촉진에 관한 법률」을 통해 국가연구데이터플랫폼(KRD) 연계 및 연구데이터관리계획(DMP) 의무화하여 AI 학습용 데이터 댐 구축에 착수

- 'AI 코사이언티스트 경진대회'('26)에서 선정된 10개 팀에 최대 5년·25억 원 규모의 사업화 R&D를 연계하고 슈퍼컴 5·6호기 연산자원 제공하여 개발된 AI 에이전트를 NST 산하 출연연에 시범 도입 예정

□ (과학기술의 역할과 개선 방향) AI4S 연구기반의 구축·확산을 추진하고 있으며, 이를 실질적인 과학적 발견과 연구생산성 향상으로 연결하기 위해 데이터 표준화·공유, 수요 기반 연산자원 배분, 모델–실험–검증–재학습의 연계 강화 필요

❍ (현주소) 연구데이터·AI 모델·컴퓨팅·실험시설을 연결해 실제 과학적 발견으로 이어지게 하는 연구체계가 아직 구축·확산 단계에 있으나, 데이터 연계 부족 및 연산자원의 병목 가능성 존재

– 정부는 국가과학기술연구회 내 출연연 등이 보유한 데이터·인프라를 연계하여 과학 AI 기반 연구생태계를 활성화하기 위한 국가 과학 AI 연구센터를 운영하고 있으나 리스크* 대응 다소 부족

* 핵심 데이터 소유권, 보안, 기존 전문기관(KISTI, ETRI 등)과의 기능 차별성 등

– 기관·분야별 연구데이터의 형식과 실험조건이 상이하고, 품질·출처·이용 권한이 명확하지 않아 연구데이터의 연계 및 재사용에 한계

– 실험장비별 데이터 형식과 통신·제어 방식이 상이하고, 데이터 추출 및 외부 소프트웨어를 통한 제어 기능이 제한적인 경우 AI 모델과 실험장비 간 연계 및 실험 전 과정의 자동화에 한계

※ 美 A-Lab은 고체 합성 및 XRD 분석을 위해 개별 장비 28대의 SDK·데이터 형식을 통합하여 운영

– AI가 제안한 가설이나 후보물질을 실제 실험으로 검증하고, 그 결과를 다시 AI 학습과 다음 실험 설계에 반영하는 모델–실험–검증–재학습 연결형 연구체계의 현장 정착·확산 부족

– 국가 슈퍼컴퓨터와 과학기술 AI 특화시스템 확충을 추진하고 있으나, 모델 학습·과학계산·자율실험 수요 증가에 대응한 자원 배분과 연산자원의 접근성·운영 병목 발생

* 국내 수요-공급 격차는 6대 파운데이션모델·자율실험실 등 사업이 확대될수록 병목이 가중될 가능성이 높음

❍ (개선방향) 연구개발 전주기의 패러다임 전환을 촉진하기 위해 연산자원의 병목과 더불어 데이터 인프라의 확충, 연구장비·통합제어 시스템 연계, 검증 시스템의 체계화 등 필요

– 연구분야별 특성에 맞춰 물리법칙·인과관계·실험 제약을 모델에 반영하고, 불확실성 추정과 적용 범위 검증 강화 필요

* 예측 정확도뿐 아니라 실제 합성 가능성, 실험 성공률, 미지 조건에서의 성능 및 재현성을 평가하는 분야별 검증체계 마련

– 분야별 공통 메타데이터와 실험기록 표준을 마련하고, 성공·실패 결과, 측정조건, 불확실성 및 데이터 출처를 함께 관리 필요

* 기관별 데이터 수집을 넘어 실험조건·측정단위·메타데이터를 맞추고 품질을 검증해야 하며, 실패한 실험까지 학습에 활용할 수 있도록 데이터 생산·정제·공유에 대한 비용 지원과 기여 인정 방안 검토 필요

– 실험장비의 데이터 접근성과 자동화·제어 기능을 확보하고, 장비 간 상호운용성을 높이기 위한 공통 인터페이스 및 연계 기술 개발 필요

– 미션별 모델 학습·추론·시뮬레이션·실험 수요를 반영해 연산자원을 배분하고, 대학·출연연·기업이 지속적으로 활용할 수 있는 공동 이용체계 구축 필요

– '가설 설정→실험 설계·수행→결과 검증→데이터 축적·재학습'이 반복되는 폐쇄루프 연구체계를 구축하고 공동 활용 확산 필요

⑥ AI 지식자원의 전략 자산화

- 글로벌 첨단 R&D 경쟁이 국가 혁신시스템 중심의 전략 자산화로 확장됨에 따라, AI 기술 자립을 위한 프론티어 AI 인재 확보와 고품질 도메인 데이터 자산화의 필요성이 크게 대두
- 주요국은 핵심 인재와 고품질 데이터의 국가 전략 자산화를 강화하고 있으며, 한국도 산·학 협력 기반 AI 융합인재 양성과 산업별 데이터 확충·활용을 통해 산업 전반의 AI 전환을 지원
- AI 인재의 국내 정착과 수급 불균형 해소를 위한 연구환경·직무체계·양성사업 관리 개선과 함께, 증강·합성 데이터 R&D 및 국가 데이터 연계·교환체계 강화 필요

□ **(배경) AI 경쟁이 기술 확보를 넘어 국가 혁신역량 전반의 경쟁으로 확대되면서, 핵심 인재와 고품질 데이터의 확보·축적·활용이 전략 자산화되는 추세**

❍ (지식자원의 전략 자산화) AI 분야 글로벌 경쟁 패러다임이 첨단기술 선점·확보라는 '기술패권' 중심에서 기술+자본+인재+제도가 결합된 '국가 혁신시스템' 경쟁으로 확장

※ 첨단기술 확보를 위해 보조금 지원을 넘어 자본 결합, 인재 확보, 제도 개선까지 국가 전략을 전방위적으로 확장 중이며, 첨단 R&D 우위를 위해서는 국가 시스템 전체의 혁신역량이 관건

- 특히, 지정학적 블록화 심화로 AI 지식자원이 국가 경쟁력과 기술 자립·주권 확보의 핵심 요소로 대두됨에 따라, 주요국은 이를 전략적 자산(National Strategic Assets)으로 축적·보호하는 추세

※ 과거 기술격차가 특허·IP 확보 중심이었다면, 현재는 핵심 인재 확보와 고품질 데이터 자산화가 국가 경쟁력 및 AI 성능 향상의 결정적 요인

- 그간 단발성·공급 중심에 그쳤던 국내 AI 자원 확보 방식을 넘어, 지속 가능한 'AI 지식자원 전략 자산화 체계(획득-축적-활용 선순환)' 구축 및 민·관 협력을 통한 기술 자립 가속화

❍ (인재 확보 경쟁 심화) 산업혁신과 과학적 발견을 촉진하고 국가 AI 경쟁력을 좌우하는 프론티어 AI 주도권 확보를 위한 '인재 자산화' 및 '도메인 융합' 경쟁 심화

- 주요국은 최상위 연구자의 국내 정착 및 연구성과 자산화 전략과 함께, 산업현장에서 AI를 즉시 적용·운용할 도메인 특화 인재의 AI 활용 역량(AI Literacy) 고도화를 동시 추진

※ 최상위 프론티어 AI 모델 개발 및 원천기술 확보가 세계적 연구자 역량에 의존

❍ (고품질 데이터 요구 증대) Physical·도메인 AI 전환에 따른 '고품질 데이터(AI-Ready Data)' 자산화 및 공급망 병목 해소가 모델 성능 향상, 비용 절감 및 신뢰성 결정에 있어 핵심 이슈

- 웹 데이터의 구조적 한계(중복·편향·노이즈)로 인한 AI 성능 정체를 극복하기 위해, '정확성·대표성·법적 안정성'을 갖춘 고품질 데이터의 전략 자산화가 핵심 과제로 부상

※ 고품질 데이터(AI-Ready Data): 특정 목적(AI 학습, 정책 분석, 산업 서비스 등)에 즉시 활용 가능하며, 도메인 적합성과 법적 안정성을 확보한 데이터

- AI 패러다임이 범용 언어지능(LLM)에서 제조·의료·물류·모빌리티 등 현실 세계와 상호작용하는 Physical·도메인 특화 AI로 진화됨에 따라, 텍스트·이미지·음성·촉각·위치 정보 등 복합 데이터(Multimodal) 처리 기술 및 산업 현장 데이터의 자산화 수요 급증

※ 범용 LLM과 달리 Physical AI 핵심인 VLA(Vison-Language-Action) 모델은 행동 데이터 수집이 필수이며, 도메인 특화 AI(버티컬 AI)는 산업별 맥락과 도메인 지식을 기반으로 설계되어야 함. 이로 인해 데이터 학습 범위도 기존 웹 기반 텍스트에서 산업 현장의 실시간 공정·노하우 데이터 등으로 확장

□ (주요국 동향) 핵심 인재의 유치·정착·역량 강화와 고품질 데이터의 축적·공유·활용을 추진하며, 인재·데이터를 국가 전략 자산으로 육성하는 정책 강화

❍ (미국) 단순 민간 주도 기술개발에서 국가 안보 및 R&D 패러다임 전환에 대응하고자, 초대형 인프라 및 국가 총동원형 프로젝트를 통해 인재·데이터를 전략 자산화

- (인재) 프론티어 AI 경쟁 심화 속에서 최상위 연구자의 국가적 안착과 해외 우수 인재 유치 환경 적극 조성, AI 관련 인력개발 입법 추진으로 단기 기술교육에서 국가 안보·산업 핵심 인적 자산 보전 체계로 전환 추진

※「미국 AI 행동계획(AI Action Plan)(2025)」, AI 인력개발 관련 발의 법안 총 6건('25~'26, 제119대 미국 의회)

- (데이터) 웹 크롤링 중심 데이터 수집 한계 극복을 위해 에너지부·국립연구소 초고성능 컴퓨팅과 연방정부 연구자원(보건·우주·국방 등)을 일체화된 데이터 플랫폼으로 통합 구축하여, 고부가가치 데이터 공급망 확보에 노력

※「제네시스 미션(Genesis Mission)('25)」

❍ (중국) 범용 언어지능에서 'AI+제조·Physical AI' 중심의 전방위 산업 분야로 확산 전환하고, 국가 주도의 전주기 인재 교육 및 고품질 데이터 공급망 조성을 강력 추진

- (인재) 전주기 AI 인재 교육 체계(초·중·고~고등·직업)를 제도화하고, 최상위 해외 인재 유치와 산·학·연 연계 R&D를 결합하여 핵심 지식과 암묵지를 자국 생태계에 축적하는 인적 자산 저변 대폭 확대

※「'AI+ 교육' 행동계획('26)」, 엘리트 양성 시스템(베이징대의 튜링반(圖靈班), 칭화대의 야오반(姚班) 등)

- (데이터) 산업 현장의 기술 노하우·제조 데이터를 모델 개선으로 연결하는 선순환 구조 정립, 24개 핵심 분야 고품질 데이터셋 구축, 토큰 기반 데이터 거래 등 국가 차원의 데이터 자산화 정책 전면 실행

※「2026년 모델·데이터 공진 행동('26)」,「산업 고품질 데이터셋 구축 행동 실시방안('26)」

❍ (일본) 디지털 전환(DX) 지연 극복 및 기술 주권 확보를 위해, 제조·의료·로봇 등 강점 산업 특화형 인재·데이터 육성과 소버린 AI 인프라 구축 본격화

- (인재) 고령화·산업 현장 공백에 대응하여 재직자 AI 리터러시 고도화 및 도메인 융합 인재 재교육 강화, 글로벌 프론티어 연구자와의 공동연구 확대 및 해외 인재 유치 채널 다각화로 전략적 인적 자원 확충(「AI 기본계획('25)」)

- (데이터) 일본 고유 언어·문화적 특성과 로봇·물류·의료 현장 특화 데이터를 결합한 독자적 AI 데이터셋 구축, 유럽·아시아 국가와의 권역 블록화·데이터 스페이스 연계로 빅테크 데이터 종속 방지 및 소버린 데이터 자산화 도모

❍ (EU) 기존의 규제·안전 중심 기조에서 '기술주권 확보 및 전략 자산 활용'으로 정책 중심축을 이동시키며, 미·중 기술 종속을 탈피하기 위한 연합형 역량 결집 가속화

- (인재) 최고급 연구자 해외 유출에 대응하여 회원국 간 연구 인력의 자유로운 이동과 역량 강화 지원, 유럽 전역의 AI 고성능·첨단 연구 환경 제공을 통해 최상위 과학자들의 역내 잔류 및 유치 적극 도모

※「기술연합 전략(Union of Skills)('25)」,「Choose Europe for Science('25~'27)」

- (데이터) 빅테크 기업의 데이터 독점에 맞선 산업별 데이터 스페이스 구축 확대, 공공·민간 데이터의 안전한 공유 및 저작권·가치 배분 프레임워크 정비로 유럽 주도 자생적 AI 데이터 생태계 조성 추진

※「EU AI 대륙 실행계획(AI Continent Action Plan)('25)」,「EU 데이터법(Data Act)('23)」

❍ (기타) 영국, 싱가포르, UAE 등 신흥 AI 선도국들은 독자적 컴퓨팅·데이터 인프라 확보와 국가 이니셔티브를 결합하여, 글로벌 지식자원 흡수 및 특화 자산화를 도모

- (인재) 국가 차원의 컴퓨팅 인프라(AIRR;AI Research Resource) 접근권 보장과 공공 R&D 개방으로 글로벌 우수 연구자를 유입하고, 미래 세대 AI 교육과정 선제 도입 및 글로벌 브레인 네트워크 강화로 인적 자원의 국가적 기여 극대화

※「영국 AI 기회 실행계획(AI Opportunities Action Plan)('25)」,「싱가포르 스마트 네이션 2.0('24)」

- (데이터) 공공·민간 데이터의 책임 있는 개방과 저작권 라이선스·수익 배분 모델 정비로 데이터 유통 촉진, 자본력 기반 글로벌 빅테크와의 전략적 파트너십으로 국가 차원의 AI 데이터·컴퓨팅 자산 통합 구축

※ 영국 국가 데이터 라이브러리(National Data Library) 구축·운영('25~),「UAE G42-MS 전략적 파트너십('25)」

□ **(국내 현황) 정부는 산·학 협력과 현장 중심 교육을 통해 AI 융합인재를 양성하고, 산업별 고품질 데이터 확충과 안전한 공유·활용 기반 조성으로 산업 전반의 AI 전환을 뒷받침**

❍ (인재) 정부와 산업계는 다분야에 적응 가능한 AI 융합 고급인재 양성을 위해, 대학원 확대 및 산·학 공동 프로젝트 중심의 R&D 지원체계를 적극 구축하여 현장 중심의 성과 창출을 도모

- 기업은 산업 전반의 AI 전환에 따라 현장 도메인 지식과 AI 역량을 갖춘 실무·융합 인재 채용을 대폭 확대하고, 정부는 대학-기업 간 협력 제도화 및 유연한 학사 제도 도입, 기업 맞춤형 산·학 협력 프로젝트 지속 수행 등을 통해 맞춤형 AI 융합인재 양성 지원

※ (디지털선도기술핵심인재양성, 과기정통부, '24~계속) 대학(원)생이 R&D 과정에서 습득한 실무 경험과 도메인 지식, 자체 개발 핵심 기술을 직접 창업으로 연결시켜 성장 동력 창출과 양질의 일자리를 마련하도록 AI·디지털 창업 인재 교육을 패키지로 지원

※ (인공지능혁신대학원사업, 과기정통부, '26~'30) 기업과 대학이 공동으로 'AX연구협력센터'를 대학원에 설치, 대학 교원과 기업 겸임교원이 함께 지도하는 복수 지도교수제 도입

- 비전공자 AI 역량 강화 기초 교육과 함께, 도메인 전문 인력에 대한 AI 기술의 능숙한 활용을 돕는 융합 교육 중점 추진으로 산업현장에서 요구하는 융합형 실무 인재 육성에 노력

※ 실무에 즉시 적용 가능한 AI 역량 확보를 위해 기업 현장 데이터에 기반한 프로젝트 교육과 멘토링을 실시하며, 산·학 공동연구를 매개로 한 채용 연계형 인턴십 등을 적극 지원하여 실질적인 취업 기회 확대

- Physical AI 및 특화 분야 확산에 발맞추어 산업계 현안 해결 중심의 AX·AI융합대학원 R&D 지원을 강화하고 사내 대학원 설립 등 민·관 협력 기반의 실무형 인재 양성을 추진

※ 사내 근로자를 석·박사급 전문 인력으로 양성하기 위해 'LG AI대학원'을 『첨단산업 인재혁신 특별법』에 따라 국내 최초 교육부 공식 인가 사내 대학원으로 설치('25) 및 학위과정 운영('26~)

❍ (데이터) 정부는 인공지능 대전환을 위해 핵심 자산인 고품질 데이터 확보를 목표로 공공데이터 포털을 개방하고, 분야별 빅데이터 플랫폼 구축 등 국가 차원의 대규모 데이터 자원 기반을 마련

- 분야별 데이터 스페이스 구축 및 공공데이터 AI 학습용 가공·개방 정책을 통해, 연구기관과 기업이 필요로 하는 고품질 데이터 공급 기반을 체계적으로 확충

※ 피지컬 AI, 모빌리티, 바이오·보건의료, 농업 등 주요 전략 산업별 특화 AI 학습데이터를 중점 구축하고 국가 데이터 파이프라인 연계를 위한 분야별 데이터 표준 개발을 전개

- 데이터 안심구역 클라우드 연계 및 전국 거점센터 육성 등을 통해 미개방 데이터 활용 기반을 조성하고, 원본 데이터 활용에 수반되는 법·제도적 불확실성 선제적 해소에 노력

※ 기업의 데이터 활용 촉진을 위해 정부 사업 참여 시 데이터 현물 자부담을 인정하고, 인공지능 연구개발 기반의 데이터 구매 비용 세액공제를 확대하여 중소기업과 스타트업의 경제적 부담 완화

※ 저작권법 개정 검토, 개인정보보호법 상 원본데이터 AI학습 허용, 가명처리 지원 등 법·제도적 개선 추진

- 데이터 스페이스 기반의 지자체 간 글로벌 협력 프로젝트를 통해 도로 인프라 결함 감지 AI 모델 개발 등을 실증*하고, 공공과 민간의 데이터 상호운용성을 보장하기 위한 공통 관리 기준(국가 데이터 인프라 컴플라이언스) 마련

* [SafeTrack-X 프로젝트] 독일 함부르크시와 공동으로 데이터 스페이스 기반으로 한국/독일 도로 인프라 데이터를 상호 교환하여 도로 결함(포트홀, 부식 등)을 감지하는 AI 모델 개발·실증(대구디지털혁신진흥원, '25)

※ 글로벌 표준 가이드라인에 부합하는 데이터 식별 체계와 이력 관리 시스템을 도입함으로써, 투명하고 신뢰성 높은 국내 인공지능 데이터 거래 생태계 조성을 위한 범부처 통합 컴플라이언스 구축

- 제조·자동차·철강 등 산업 현장의 핵심 데이터와 노하우·오류 분석 결과를 보안성이 높은 폐루프 온프레미스 AI 파운데이션 모델과 결합하는 등 유출 우려 없는 현장 특화 고부가가치 데이터 자산화 추진

※ (SK텔레콤) 독자 AI 모델('A.X K1') 기반 KG스틸·코넥 제조 현장 AI 에이전트 실증 추진

※ (파나시아) AI 비전 카메라와 IoT 센서로 작업자·이동체 정밀 위치 데이터를 실시간 수집·DB화하여, 불량 판정 자동화(불량 검출률 95% 이상)로 인건비 40% 절감, 실시간 안전 모니터링 및 중대재해 예방 체계 구축

□ (과학기술 역할과 개선방향) AI 지식자원의 전략 자산화를 위해 핵심 인재의 국내 정착과 산업 수요 기반 양성체계를 강화하고, 고품질 데이터 공급·연계·안전한 활용 및 국제 상호운용성 확보 필요

① (인재) 최상위 AI 인재의 해외 유출과 산업 수요·역량 간 불균형 해소를 위해 국내 연구·정착 여건을 개선하고, 가치사슬별 역할과 수요에 기반한 현장 중심 융합인재 양성체계로 전환 필요

❍ (현주소) 정부는 AI 고급·융합인재 양성 지원을 확대하고 있으나, 인력 양성 규모와 함께 산업의 직무별 수요, 교육내용의 적합성 및 기존 사업의 참여·활용 성과에 대한 종합 진단이 제한적

- 프론티어 AI 전문인력 R&D 지원과 글로벌 산학 협력 네트워크 구축 사업을 적극 추진하고 있으나, 해외 대비 낮은 임금 프리미엄, 정착 여건·연구 인프라 열세로 인한 고급 인재 유출 현상 지속

※ 국내 AI 인력 약 16%가 해외 근무, 글로벌 100대 AI 인재 중 한국은 1명, 저자·발명가의 순유출 지표(-1.75)는 음수 기록

- AI 인재 수급 문제는 전체 인력 규모와 함께 직무·숙련도별 수요, 교육내용과 요구역량의 부합 여부, 채용·근무조건 등 공급 부족과 역량 불일치를 구분한 원인 진단이 필요한 상황

※ 분야별 신규 박사 취업률('23)은 ICT 65.9%, 자연·수학·통계 59.3%로 보건복지/교육(77.2%, 71.9%) 대비 낮고, 취업 박사의 21%만 민간기업으로 진출

※ 5년간('19~'23) 10개 인공지능대학원에 760억 원을 지원하여 석·박사 893명을 배출했으나, 취업률은 매년 감소('19년 100% → '23년 63.5%)한 현상과 관련하여 취업률만으로는 실무역량 수준 판단이 어려우므로, 진학·연구직 진출, 채용 여건, 전공·직무 일치도 등을 함께 분석 필요

※ 산업의 인재 수요가 교육사업 참여로 이어지는지 확인하기 위해 사업별 모집·신청·등록·수료 실적을 점검하고, 참여 저조 사업은 교육내용·운영방식·지원조건과 대상자의 수요 간 불일치 여부 등이 분석되어야 함

- 현행 AI 인력 분류체계는 전통적 개발자·직무 중심으로 설계되어, 실제 가치사슬의 병목(검증·신뢰, 운영, 산업(도메인) 적용, 비개발 직무 등)에 대한 정확한 진단 및 관리가 어려움

❍ (개선방향) 직무별 인력 수요와 기존 사업의 참여·성과를 토대로 양성 규모를 조정하고, 확인된 역량 부족과 참여 제약을 해소하여 인재양성사업의 수요 적합성과 실효성을 높일 필요

- 글로벌 수준의 연구 인프라(고성능 GPU 등)를 선제 확충하고, 파격적인 경제적 보상과 정주 여건 개선으로 우수 인재가 국내에 안정적으로 정착할 수 있는 록인(Lock-in) 환경 조성 확대 필요

※ 해외 우수 인재의 국내 유입 가속화를 위한 전방위적 비자 혜택 및 인센티브 체계 구축·강화 필요

- 교육부의 대학 교육, 과기정통부의 대학원·연구인재 양성, 고용부의 KDT 등 직업훈련, 산업부의 산업별 재직자 교육을 연계하여 기초교육부터 전문인재 양성·취업·재교육까지 이어지는 범부처 통합 관리체계 마련 필요

※ 부처별 사업의 대상·직무·역량 수준을 공통 기준으로 정리하고, 모집·수료 실적과 함께 사업 목적에 따른 직무역량 향상, 관련 직무 취업·유지, 연구성과 및 현장 활용 실적을 점검하여, 그 결과를 교육과정·지원조건·양성 규모 조정에 반영

- 기업의 미충원 직무와 수료자의 현장 활용 실태를 바탕으로 교육과정을 보완하고, 부족 역량이 확인된 분야는 산·학 공동 프로젝트·현장실습과 채용 연계를 강화할 필요

- 교육생·기업의 미참여 사유를 확인하여 교육시간·방식, 참여비용 지원 및 경력개발 연계를 개선하고, 기존 사업의 개선만으로 충족하기 어려운 인력 수요에 대해서는 양성 규모 확대를 검토할 필요

- 기존 직업·직무 분류와의 연계 가능성을 검토하고, 데이터 구축·모델 개발·검증·운영·산업 적용 등 역할별 역량 정보를 보완하여 AI 인력 수급 진단과 사업 설계의 기반으로 활용할 필요

※ 우선 적용 분야에서 정보의 활용성을 검증한 뒤, 통계·수급 전망·채용·교육훈련 간 연계를 단계적으로 확대

- 데이터 수집·플랫폼 구축·서비스 응용 등 가치사슬별 역할을 반영한 AI 인력 분류체계를 정비하고, 통계·수급 전망·채용·직업훈련 정보를 연계하여 산업 현장의 인력 수요에 부합하는 중장기 인재 육성 전략 수립 필요

② (데이터) 고품질 데이터 부족과 플랫폼 간 연계 미흡을 해소하기 위해 국가 데이터 연계·분산형 교환체계 구축, 제조 특화 합성데이터 공급, 국제 표준·규범 연계를 통한 데이터 활용성과 주권 강화 필요

❍ (현주소) AI 산업의 폭발적 성장으로 고품질 데이터 소진 우려가 커지는 가운데, 국내 데이터 생태계는 인프라의 물리적 파편화와 상호운용성 부족으로 효율성이 저하된 상태

- 국내 AI 기업의 59.5%가 데이터 확보·품질 문제*를 겪고 있으며, 고품질 데이터 확보에 대한 어려움은 심화된 것으로 조사

* 소프트웨어정책연구소('25), 2024년 인공지능산업 실태조사

※ 양질의 데이터 부족('23년 31.1% → '25년 38.0%), 데이터 소재 파악·검색의 어려움('23년 29.3% → '25년 36.4%)

- 부처별 개별 정책 추진으로 데이터 표준화·품질 관리 공통 기준이 부재하며, 수요자-공급자를 유기적으로 매칭하는 중개 플랫폼 부재로 접근성이 떨어져 민간 주도 거래 시장 활성화 지연

- 차세대 로봇 AI용 피지컬 데이터의 경우, 해외 선도국이 대규모로 빠르게 구축 중이나 국내는 시각 데이터 중심의 소규모 실환경 수집 수준에 머물러 기술격차 발생

※ 특히, 중소 제조 현장의 특수성을 반영할 수 있는 연체·유체·고위험 상황 시나리오에 대한 다중 물리 합성 데이터 자동 생성 및 검증 파이프라인 부재로 독자적 인프라 확보에 한계 존재

- 저작권·개인정보보호법 등 현행 법·제도의 규제 부담으로 고부가가치 데이터 유통이 제한되고, 국경 간 데이터 이동 원칙 부재로 글로벌 거버넌스 대응 능력이 부족한 실정

❍ (개선방향) 산업 수요에 기반한 고품질 데이터의 확보·생산·품질관리를 강화하고, 민간의 제공 유인과 권리 보호를 결합한 연계·활용체계를 마련할 필요

- 파편화된 공공·민간 데이터를 단일 창구에서 통합 검색 가능한 국가 데이터 연계 허브를 구축하고, 분산된 플랫폼을 연합 데이터 카탈로그 기반으로 연계하여 데이터 발견 접근성 극대화 필요

※ 데이터의 물리적 통합 대신 표준 API를 확산하고, 출처 관리·신뢰 기반 교환 모델로 상호운용성 장벽 제거 필요

- 민간의 데이터 제공·정제 비용과 활용가치를 고려하여 이용대가, 공동 활용 편익, 성과 공유 등 보상방식을 설계하고 지속적인 데이터 공급을 유도해야 하며, 개인정보·영업비밀 등 보호 필요에 따라 접근을 차등화하고, 이용 목적·기간·재제공 조건, 파생성과 이용범위와 책임을 계약으로 명확히 할 필요

- 산업별 활용 목적과 부족 데이터를 확인하여 현장 데이터 수집·정제·주석 부여를 지원하고, 수집이 어려운 상황은 합성데이터로 보완할 필요

※ 활용 목적별 정확성·대표성·완전성·최신성 기준을 마련하고, 구축·검수·갱신 단계별 품질관리와 출처·가공 이력 관리를 강화할 필요

※ 합성데이터는 실제 현장 데이터로 성능과 적용 한계를 검증하고, 생성 조건과 사용 가능 범위를 명시할 필요

- 국내 표준 API·메타데이터를 국제 표준과 연계하고, 한국형 신뢰 기반 데이터 흐름(K-DFFT) 모델의 글로벌 의제화를 추진하여 데이터 주권과 글로벌 규범 대응력 강화 필요

※ 『EU Data Act』 등 규제에 적극 대응, 다자간 데이터 협약 확대로 국내 기업의 글로벌 서비스 연계 활성화 및 기술 주권 강화 필요

⑦ AI 지정학 블록화와 글로벌 AI 거버넌스 재편

- 글로벌 AI 거버넌스가 단위기술 혁신 중심의 개방적 협력에서 AI 인프라·모델·표준을 통합한 지정학적 블록 경쟁으로 전환
- 미국은 기술우위와 AI 가치사슬 전반을 고려한 신뢰 주권, 중국은 오픈소스 모델과 디지털 인프라를 기반으로 글로벌사우스와 연계하는 포용 주권, EU는 AI법과 표준을 결합한 규범·시장 주권을 각각 추진
- 반도체·ICT 등 기술우위를 기반으로 글로벌 AI 거버넌스·국제표준 설계 역량을 강화하고, AI 가치사슬 전반을 아우르는 R&D·시험·인증 통합 관리체계 구축 필요

□ **(배경) AI의 전략 자산화로 공급망·컴퓨팅·모델 접근권을 둘러싼 지정학적 블록화가 심화되는 가운데, 공동 위험평가와 표준·인증 및 공정한 기술 접근을 위한 글로벌 AI 거버넌스 질서가 형성**

❍ (지정학적 블록화) AI가 군사력·정보력·생산성 향상의 핵심 도구로 부상함에 따라 국가·경제 안보 강화 측면에서 전략적 개발·활용 증대

- AI가 개별 제품·기술을 넘어 생애주기 全단계로 패키지화되고 다양한 분야(제조, 사이버보안, 국방, 과학기술 등)에 적용됨에 따라 '전략 자산'으로 인식
- AI 수출 통제·전략은 과거 특정 반도체나 장비를 대상으로 했으나, 최근에는 GPU, 클라우드, 공급망, 데이터센터, 인력, 기술지원 등까지 확대
- 기술혁신을 촉진하기 위한 개방형 협력에서 탈피, '어떤 국가의 AI 스택을 사용할 것인가?', 'AI 모델의 접근권은 어디까지 허용할 것인가?' 등 AI의 전략적 접근성 중요
- AI 데이터센터와 컴퓨팅 클러스터가 민간기업의 투자 대상을 넘어 정상외교·통상협상·개발협력의 핵심 패키지로 부상
- 경쟁국의 기술 접근을 제한하는 수출통제와 함께, 자국의 AI 인프라·모델·서비스·표준을 우방국에 패키지로 확산하여 장기적인 기술 의존관계와 시장 영향력을 확보하려는 경쟁 심화

❍ (글로벌 AI 거버넌스 구축) AI 기술 이용 원칙(공정성·투명성 등)에 머물지 않고, 컴퓨팅 자원과 모델 접근권을 통제하는 새로운 글로벌 규범 질서가 형성

- AI 모델과 서비스가 여러 국가에 걸쳐 개발 및 유통됨에 따라 특정 국가에서 발생한 위험이 글로벌 시장과 이용자에게 빠르게 전파
- 보편적 AI 윤리 원칙(공정성·투명성·책임성 등) 설정을 넘어 국제사회(UN)가 참여하는 과학적 평가와 정보 공유체계 구축 추진
- AI의 개발·검증·조달·활용 전 과정에 공통 기준을 적용하여 신뢰할 수 있는 AI 생태계를 구축하기 위한 표준·인증체계와 법률 제정 확대
- 대규모 AI 모델 개발에 필요한 컴퓨팅·데이터·자본이 일부 국가와 빅테크 기업에 집중되면서 기술 접근성 및 규칙 설정 권한의 격차가 확대됨에 따라 포용적 거버넌스 구축 필요

□ (주요국 동향) 미국·중국·EU는 자국 중심의 AI 생태계 확산과 기술주권 확보를 위한 공급망·규범 경쟁을 강화하고, 국제기구는 과학적 평가·공통 표준·다자 협력을 통한 글로벌 AI 거버넌스 구축을 추진

❍ (미국) AI 기술의 글로벌 우위를 기반으로 대중국 배제 확대 및 미국 중심의 신뢰 기반 AI 가치사슬 전반의 지배력 강화

- 바이든 정부는 「AI Diffusion Rule('25)」을 통해 국가별로 반도체·모델 가중치의 접근성을 차등화하여 신뢰 수준별 계층화 시도

- 트럼프 정부는 동맹국과의 외교관계 훼손 및 미국 기업의 경쟁력 약화 초래 등의 사유로 바이든 정부의 AI 정책을 철회. 다만 대중국 첨단 반도체·모델 통제와 우회 수출 단속은 오히려 강화*

* 제품 통제(GPU, AI 반도체 등), 우회경로 통제(Entity LIst 등), 자본·지식 통제(대중 투자 및 기술지원 제한 등)

- AI 기술동맹에서 벗어나 중동·인도·EU 등 외연을 확대하고 미국 중심의 AI 가치사슬을 구성하여 하나의 경제안보 단위로 구성하여 신뢰 기반의 전략적 협력 강화

※「American AI Exports Program('25)」, 「Pax Silica('25)」 등

- AI 기술과 시장의 네트워크 효과를 통해 글로벌 산업·규범으로 확산하고 미국의 우위를 확보하기 위해 표준과 기술혁신을 강조

〈표 9〉 미 트럼프 정부의 AI 분야 주요 경제안보 블록화 프로그램

구분	American AI Exports Program	Pax Silica
주관부처	상무부, 국무부·재무부 등 참여	국무부
근거	대통령 행정명령	비구속적 다자 선언
목적	미국산 AI 풀스택의 해외 수출 확대	AI·첨단기술 공급망 구축
범위	Chip-클라우드-모델-서비스	광물-에너지-제조-Chip-모델-물류
방식	미국-개별 수입국	다자 협력네트워크('26.8월 기준 24개국 서명)
핵심수단	패키지 선정, 금융·보증·외교·기술 지원	공동투자, 공급망 연결, 기술보호 등

❍ (중국) 저비용·개방형 AI 모델을 기반으로 글로벌 사우스를 중심으로 AI 외교를 추진하고 있으며, 대형 AI 모델과 AI 에이전트 기술의 수출 금지·제한 강화

- 미국·EU의 AI 통제에 대응해 AI 반도체, 첨단패키징 등 기술 자립을 가속화하고 있으며, 중국 수출 금지·제한 품목에 AI 대형 모델, AI 에이전트 기술 등이 포함될 예정('26.10)

- 중국산 AI 모델의 상대적 낮은 비용과 개방성을 활용해 아시아·중동·아프리카·중남미 시장 진출과 규범적 연대 기반 확보

- 2026 세계 AI 대회 및 AI 글로벌 거버넌스 고위급 회의에서 중국 상하이에 글로벌 AI협력기구*를 출범시키고 개도국 지원**을 확대하겠다고 발표('26.7)

* WAICO(World Artificial Intelligence Cooperation Organization): 중국, 러시아, 브라질, 세네갈, 이란, 카메룬 등 총 37개국 협정에 서명

** 향후 5년 간 개도국 AI 전문인력 5천명 양성, 지역별 AI 응용협력센터 구축 등

❍ (EU) 미국과의 기술·안보 협력을 유지하면서 독자적인 규범·기술·산업 주권으로 확장하기 위한 전략적 포지셔닝을 추진

- AI의 안전성·투명성·책임성 확보를 위해 위험 수준*별 차등 규제를 적용하는 「AI Act」 발효('24.8.), 「사이버 보안 및 AI 실행계획」을 발표('26.7.)하는 등 첨단 AI 모델의 안전성 평가와 사이버 위협 대응역량 강화 추진

  * 금지 AI, 고위험 AI, 투명성 대상 AI, 저위험 AI

- EU 집행위원회는 미국이 주도하는 Pax Silica에 공식 서명하여 신뢰 기반의 공급망 구축과 기술주권 강화에 글로벌 파트너십 확대

- 유럽 평의회(CoE)는 인권·민주주의·법치주의 기반의 세계 최초의 국제조약(Framework Convention on AI and Human Rights, Democracy and the Rule of Law)에 서명

- 과거 AI 규제 중심에서 탈피하여 제조·자동차·로봇 등 EU가 강점을 가지고 있는 산업에 AI를 적용하고, 규제 단순화와 기업 부담 완화 병행 추진

- AI 혁신과 글로벌 거버넌스 강화를 위해 EU-인도 간 전략적 파트너십을 구축('26)하였으며, AI 외교에 있어 안정적이고 신뢰할 수 있는 파트너임을 강조*

  * International Digital Strategy('25.6)

〈표 10〉 미국·중국·EU의 AI 국제 규범·협력 전략

구분	미국	중국	EU
핵심 목표	AI 기술 우위·유지	AI 기술 자립 및 국가주도 산업경쟁력 강화	신뢰가능한 AI 및 기술·데이터·산업 주권 강화
규제	기술혁신 및 시장 중심, 국가안보 분야 규제 강화	국가안보·모델·데이터 중심 관리	법률(AI Act.) 기반 글로벌 규제
국제 협력	동맹·우방국 중심 협력	중국 중심의 AI 거버넌스, 글로벌 사우스 영향력 확대	전략적 자율성, 다자주의, 신뢰 기반 파트너십
주요 프로그램·법령·거버번스	American AI Exports Program, Pax silica 등	WAICO 등	AI Act., Pax Silica, CoE 등

❍ (국제기구) AI 거버넌스가 기술 이용 원칙(공정성·투명성 등)에 머물지 않고, 컴퓨팅 자원과 모델 접근권을 통제하는 국제정치 문제로 확대

- (UN) 193개 회원국이 참여하는 UN GDC*를 기반으로 AI의 기회·위험·영향에 대한 연례 과학평가 보고서를 작성하는 AI 과학패널과 각국 정부·기업·학계가 AI 국제 규범 형성에 참여할 수 있는 'Global Dialogue on AI Governance' 신설

  * Global Digital Compact: UN 미래정상회의('24)에서 AI의 포용적이고 균형잡힌 접근, 글로벌 AI 거버넌스 간 상호 운용성, AI 투명성·책임성 강조 등을 목적으로 하고 있음

- (OECD) G7이 마련한 AI 개발 기업 대상 국제 행동규범의 이행여부를 점검하고 모니터링하는 HAIP Reporting Framework 2.0을 발표('26)

- (ITU) 매년 AI for Good Global Summit을 개최하여 정책·표준·기술혁신 등을 논의하고 있으며, 파운데이션 모델 평가 표준 및 Agentic AI 표준 등을 논의

□ (국내 현황) AI 기본법과 범정부 추진체계를 기반으로 AI 진흥·신뢰 기반을 강화하고, 글로벌 거버넌스·공급망 협력 및 국제표준 개발 참여를 통해 AI 경쟁력과 국제 대응 역량 제고 추진

❍ (법률) 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법(약칭 AI 기본법)」을 '25.1월에 제정하고 '26.1월부터 본격 시행

- AI 기술의 안전한 진흥과 국가경쟁력 강화, 국민의 권익 및 존엄성 보호를 목적으로 국가 AI 기본계획 수립, AI 연구개발, 고영향 AI 및 생성형 AI 투명성 등을 규정
- AI 정책·투자·규제·산업전환 등의 범정부적 조정을 위해 대통령 직속 국가인공지능전략위원회 설치하고 지원체계 마련

❍ (글로벌 협력) UN, OECD, Pax Silica, ITU 등 다양한 AI 거버넌스 및 프로그램에 참여·협력하여 AI 안전·기술혁신·표준·공급망 대응

- AI 안전·신뢰성 확보를 위한 G7/OECD, AI 위험·신뢰성·글로벌 규범 기반의 EU, 포용성과 글로벌 사우스 중심의 UN/G20, 기술 표준 확보를 위한 ITU 등 전략적 협력 추진
- 미국은 신뢰 기반의 동맹국 중심으로 AI·반도체·광물 등의 경제안보 분야에 협력을 강화하여 글로벌 리더쉽 주도

〈표 11〉 한국이 참여·협력 중인 글로벌 AI 거버넌스·프로그램

주요 체계	주요 역할	참여 국가·기업
UN GDC	디지털 격차 해소 등 보편성·포용성 다자 프레임워크로 AI 관련 국제표준 및 포용적 거버넌스 구축	UN 회원국 193개국
OECD	AI 안전·책임·상호운용성	OECD 정회원 38개국
Hiroshima AI Process	G7 국가를 시작으로 글로벌 AI 규범과 안정성 확보를 위한 국제 협력 확대	G7 국가 (한국은 프렌즈 그룹 가입)
Pax Silica	AI·반도체·광물 등 경제안보	서명(24개국)/ 비서명 참여(타이완)
ITU, ISO/IEC* (JTC 1/SC 42)	AI 표준·평가·상호운용성	ITU 회원국 194개국 ISO/IEC 참가 58개국/관측 25개국

* ISO(국제표준화기구, International Organization for Standardization, 전 산업 분야 국제표준 개발·관리), IEC(국제전기기술위원회, International Electrotechnical Commission, 전기·전자 분야 국제표준 개발·관리)

❍ (표준) ICT 전 분야를 포괄하는 R&D사업을 통해 AI 기술의 표준화 기술개발을 지원하고 있으며, 비중도 점차 확대

- 정보통신방송표준개발지원사업(과기정통부)을 통해 AI를 포함한 표준개발과 표준화 활동*을 지원하고 있으며, AI 분야 과제 건수는 확대(5→14)

  * 표준개발, 국제표준 채택 및 의장단 진출을 위한 활동 지원 등

□ (과학기술 역할과 개선방향) AI 반도체 등 기술우위를 기반으로 국제 의제·규범 설계 역량을 강화하고, 표준·통합 시험·인증체계를 연계하는 국가 차원의 관리·지원체계 고도화 필요

❍ (현주소) 글로벌 AI 거버넌스와 규범을 주도하기보다는 수용적 입장이며, 단일 부품·제품 단위의 분절적 개발·관리 및 시험·인증체계 운영

- 다양한 글로벌 AI 거버넌스에 참여·협력하고 있으나 일부 사례*를 제외하고 국제 논의 설계·제도화 주체로서의 한국의 역할은 제한적

  * 예) 2024 AI Seoul Summit, REAIM(Responsible AI in the Military Domain) 등

  ※ 글로벌 프론티어 AI 기업(Open AI, Anthropic, Google 등)들이 AI 위험 식별·관리 및 안전성 평가 등 국제 규범 수립에 큰 영향력을 주고 있으나 한국 기업은 반도체·ICT 분야를 제외하고 영향력이 크지 않음

- 글로벌 AI 거버넌스가 안전성·투명성 등 규범적 관점에서 공급망, 반도체, 사이버보안 등 가치사슬 전반 또는 경제안보 관점으로 확대되고 있으나 개별 분야에 집중

  * 예) 핵심광물-첨단소재-반도체-데이터 센터-클라우드-AI모델 등 경제안보 또는 가치사슬 전반의 예산집계와 투자 포트폴리오 분석이 다소 미흡

  ※ 예) AI R&D 예산규모는 모델 개발-(공공·산업) AX-기반구축(인력양성 등) 등 협의 관점에서 집계되고 있으며, AI 반도체는 반도체 R&D에 포함되는 등 분절적 관리

- 국내 연구자들이 ISO/IEC, TTA 등 다양한 표준·시험·인증 연계 활동에 참여하고 있으나 EU AI Act. 등과의 상호 인정 및 국가 차원의 통합 시험·인증체계* 부족

  * 예) 로봇-자율주행-산업 AI 등 개별 제품·부품 단위의 시험·인증 기반은 존재하나 피지컬 AI 통합 시험·인증 프레임워크는 확립되지 않음

❍ (개선방향) 국내 기술 우위 분야(메모리, 피지컬 AI 등)를 중심으로 글로벌 거버넌스 또는 국제규범을 지속적·주도적으로 설계하고, AI 가치사슬 전반을 고려한 통합적 관리체계 강화 필요

- 한국 정부·기업이 발굴·설계한 국제 의제*가 글로벌 규범으로 지속적으로 이행될 수 있도록 대통령 직속 국가인공지능전략위원회의 범부처 통합·조정 및 국제협력 기능 강화 필요

  * 예) AI 반도체 공급망 거버넌스, AI/6G 통신 국제 표준 등

- 반도체·제조·통신 등 국내 산업 현장을 활용하여 산업용 AI의 안전성·보안성·신뢰성을 국제 파트너와 공동 검증하고, 실증 결과를 평가 기준과 기술표준으로 연결하여 글로벌 AI 공급망 내 한국의 기여도 제고 필요

- 현재 운영 중인 개별 AI 품목·제품 단위의 시험·인증체계와 함께 피지컬 AI와 같이 통합 시험·인증체계에 대한 제도 마련과 해외 선진국과의 상호 운용성 확대 노력 필요

- AI 분야는 국가전략기술이면서 글로벌 첨단기술 패권 경쟁의 핵심에 위치하고 있어 현행 ICT 사업에 포함된 표준개발 활동을 별도 단독사업으로 분리하여 체계적 관리·지원 필요

3 결론 및 시사점

□ 알파고 등장 이후 지난 10년 간 인공지능은 데이터 기반의 특정 과업을 수행하는 분석·예측 도구에서 언어·이미지·코드 등을 생성하는 범용 플랫폼으로 발전했으며, 나아가 목표 설정·계획 수립·도구 활용을 수행하는 에이전틱 AI와 물리적 환경에서 행동하는 피지컬 AI로 빠르게 진화

❍ AI 경쟁의 단위도 개별 모델의 성능과 규모를 넘어 컴퓨팅 인프라, 반도체, 데이터, 인재, 전력, 현장 적용, 안전·신뢰 및 국제규범을 포괄하는 국가 혁신 시스템 전반으로 확대

❍ AI는 산업 생산성과 공공서비스의 효율성을 높이는 범용기술인 동시에 과학적 발견의 방식, 국가 안보, 공급망 및 국제질서에 영향을 미치는 전략자산으로 부상

❍ 미·중의 AI 가치사슬 주도권 경쟁과 기술통제가 강화되고 있으며, 우리나라도 법·제도와 범정부 추진체계를 정비하고 글로벌 경쟁력과 국제 대응역량 강화 추진

❍ 기술주도 성장과 경제안보의 핵심 기술인 AI 분야의 국내 현주소를 진단하여 과학기술의 역할과 방향을 구체화할 필요

□ 본고는 ▲소버린 AI ▲AI 서비스 확산 ▲AI 생태계 고도화라는 정책적 지향점을 바탕으로, 7대 이슈별 국내외 동향과 우리나라의 현주소를 진단하고 과학기술적 대응방향을 제시함

❍ (소버린 AI) 독자 AI 모델·인프라 확충과 사이버보안 대응체계 강화를 추진하고 있으나, 자본·컴퓨팅 격차와 자원 분산, 기술개발과 실제 운영 간 연계 미흡으로 AI 주권 확보와 안전한 현장 활용에 한계

❍ (AI 서비스 확산) 산업·공공·과학 분야의 AI 융합과 실증·연구기반 확충을 추진하고 있으나, 현장성과 검증과 데이터·인프라 연계, 실증 이후 적용·환류체계 미흡으로 실질적 성과 창출·확산에 한계

❍ (AI 생태계 고도화) AI 인재·데이터 기반 확충과 법·제도 정비 및 국제협력을 추진하고 있으나, 핵심자원의 국내 정착·활용 기반과 국제규범 주도력·통합 인증체계 미흡으로 AI 생태계 경쟁력 부족

〈표 12〉 AI 분야 7대 이슈와 현주소

구분	핵심 이슈	우리나라의 현주소
소버린 AI	① AI 주권 경쟁 심화	• 외산 AI 의존도 완화와 AI 3대 강국 도약을 위해 독자·산업 특화 모델 개발부터 국민 서비스 확산까지 지원을 강화하고, 컴퓨팅 인프라 확충 및 국산 AI 반도체 생태계 육성 추진 • 글로벌 선도국과의 자본·컴퓨팅 격차에 대응할 집중 대상과 판단 기준이 다소 모호하며, 모델 개발 성과를 업무별 활용·운영 성과로 연결하는 검증·지원체계 미흡
	② 사이버·안보 위협의 지능화	• AI 모델·에이전트의 보안 평가·레드티밍과 AI 기반 취약점 탐지·분석·패치 기술개발을 강화하고, 법·제도 및 전담기관 정비와 민관·국제 협력을 통해 AI 사이버보안 대응체계 확충 • 탐지·취약점 발견 중심의 기술 성과가 실제 운영환경의 위험 검증·평가와 안전한 패치·배포, 사고 통제·복구로 이어지는 전주기 연계 미흡

구분	핵심 이슈	우리나라의 현주소
AI 서비스 확산	③ 피지컬 AI 및 AI-산업 융합 본격화	• 제조·모빌리티·로봇 분야의 AI 융합과 현장 실증을 확대하고, 핵심기술·부품 개발 및 산·학·연 협력을 통해 산업의 지능화·자율화와 상용화 기반 및 국내 생태계 구축 추진 • 현장 적용에 따른 생산성·안전성·경제성 검증과 핵심부품 경쟁력·공급망 확보, 데이터·학습 기반 구축은 과제
	④ 국민체감 및 문제해결형 공공 AX 확대	• 국민 삶의 질 향상을 목표로 공공 AX를 국가 전략과제로 추진하고, 부처별 임무에 AI를 접목한 R&D와 공공 인프라 지능화를 통해 문제해결을 도모 • 공공 AI 서비스가 부처별로 분절 추진되면서 데이터 연계와 공동 플랫폼 활용이 미흡, 실증 성과의 현업 확산을 위한 명확한 전환 기준과 단계별 목표 설정, 성과평가 및 환류 체계 강화 필요성 증대
	⑤ AI 기반 연구개발 방식 전환과 과학기술 혁신	• K-문샷 프로젝트를 중심으로 임무별 책임운영체계와 컴퓨팅·과학 특화 AI 모델·자율실험실·연구데이터 기반을 강화하고, AI 연구 에이전트의 현장 적용을 통해 연구생산성 제고와 국가 과학난제 해결을 추진 • 연구데이터의 연계·재사용 제약, 연산자원 접근성 병목, 장비의 데이터 접근·자동화·연계 미흡으로 모델→실험→검증→재학습 체계의 현장 정착 제한
AI 생태계 고도화	⑥ AI 지식자원(데이터·인재)의 전략 자산화	• 산·학 협력과 현장 중심 교육을 통해 AI 융합인재를 양성하고, 고품질 데이터의 구축·개방·연계 및 안전한 활용 기반을 확충하여 산업 전반의 AI 전환을 뒷받침 • 인재의 국내 정착·현장 활용, 양성사업의 수요 적합성, 고품질 데이터의 생산·유통·활용 기반 미흡으로 수요 대응에 한계
	⑦ 패권 경쟁 및 지정학적 리스크 확대	• AI 기본법과 범정부 조정체계를 기반으로 AI 진흥·안전·신뢰 확보를 추진하고, 글로벌 거버넌스 참여와 국제표준 개발 지원을 통해 규범·기술·공급망 대응 역량을 강화 • 우리나라는 AI 분야의 국제규범·표준 형성에 있어 주도력이 제한적이며, 단일 부품·제품 단위의 개발·인증 체계 운영

□ **개별 기술·사업 중심의 분절적 지원에서 가치사슬 연계, 전략적 선택과 집중, 현장 성과 및 전주기 환류를 결합한 국가 AI 혁신체계로 단계적 전환 필요**

❍ (선택적 AI 주권 확보) 국내 기반을 적극 활용할 수 있는 핵심 분야에 경쟁력을 높이고, 핵심 분야의 데이터 통제권과 운영 자율성을 확보할 필요

- 단기·중장기별 핵심 분야(예, 고효율 추론과 반도체·시스템 SW 연계, 국내 산업 수요에 특화된 모델·응용, 핵심 업무의 통제·전환 기술 등) 선정 및 성능·비용·전력 효율과 운영 가능성 검증
- 독자·최상위 모델 개발 역량을 축적하면서 기술 성능, 자원 효율, 국내 연구·산업 주체의 접근성과 활용 성과를 함께 평가하고 기존 사업과의 연계 강화
- 업무별 보안·성능·비용·서비스 연속성에 따라 국내외 AI 활용을 병행하고, 공공 실증·조달은 요건을 충족한 국산 기술의 검증·개선과 후속 도입을 연계

❍ (안전·신뢰·책임성 내재화) 적용 분야와 위험 수준에 따른 평가·검증을 개발부터 운영·사고 대응까지 연계하여 현장 활용의 신뢰 기반을 확보할 필요

- 평가 도구·기록 형식 등 재사용 가능한 요소는 공유하되, 사이버보안·공공서비스·피지컬 AI·과학실험의 시험항목과 판정 기준은 분야별로 구체화

- 데이터 품질·권리관계, 모델 투명성, 에이전트 권한, 피지컬 AI의 물리적 안전을 점검하고, 검증 결과를 운영 모니터링·사고 통제·복구 절차로 연계
- 국제표준 개발과 시험방법 협력을 강화하고, 평가 결과의 상호 활용은 분야별 제도·기술 요건을 확인하여 추진. 국제 협력체계, 표준화기구, 법률상 의무 등을 구분하여 대응

❍ (현장 성과 중심의 AX) 산업·공공 및 R&D 분야의 수요와 운영 여건이 명확한 업무·임무부터 실증에 착수하고, 성과가 확인된 적용 모델을 확산할 필요

- 산업 AX는 개선 효과와 실현 가능성이 높은 공정을 선정하여 생산성·품질·안전·비용을 검증, 공공 AX는 임무와 사회적 편익을 기준으로 기존 데이터·모델·평가 기반의 활용과 부처 간 연계를 추진
- AI for Science는 미션별 연산 수요와 연구데이터 접근성을 고려하고, 실험장비의 데이터 추출·자동화·장비 간 연계를 보완하여 가설-실험-검증-재학습의 폐쇄루프형 연구체계를 실현
- 실증 관련 세액공제 확대 검토, AI·로봇 설비투자 정책보증, 컨설팅·솔루션 도입 바우처 등 세제·금융·재정 지원을 연계하여 기업의 초기 비용과 도입 위험을 분담하는 정부의 마중물 역할 강화

❍ (인재·데이터의 지속적 활용·축적) 양적 공급과 함께 현장 수요, 참여 유인 및 활용 성과를 개선하여 인재와 데이터가 국내 역량으로 축적되는 구조를 마련할 필요

- 핵심 연구자의 연구환경·보상·정주 여건을 강화하고, 기존 인재양성사업의 참여·수료·배치·현장 활용을 점검하여 교육 내용과 참여 유인을 수요에 맞게 보완
- 신규 통합조직의 설치에 앞서 교육·연구·직업훈련·재직자 교육의 역할과 정보 연계 공백을 점검하고, 우선 실증 과제에 필요한 운영·융합 인력의 교육·배치를 연계
- 한편, 고품질 데이터의 생산·정제·품질관리를 지원하고, 민간 데이터의 권리 보호와 제공·보상 조건을 구체화. 기존 카탈로그와 표준 API 등 연계 수단을 활용하여 제공자의 통제권을 보장하는 안전한 교환·재사용을 촉진

❍ (AI 가치사슬 연계) AI 경쟁력은 모델뿐 아니라 컴퓨팅·전력·반도체·데이터와 인재·안전·표준·제도의 결합에 좌우, 개별 기술개발을 넘어 가치사슬의 병목과 성과 확산 경로를 고려한 통합적 접근

- 인공지능·ICT 전문위 소관 사업 외 반도체·공공 AX·전력·데이터·인재·안전·표준 등 AI 가치사슬 전반의 R&D를 통합 관리하여 사업 간 연계 및 R&D 속도 조절(필요시) 추진
- 인프라·출자 등 비R&D 지원은 R&D와 구분하여 함께 파악할 필요가 있으며, 정부 및 민간 재원·지원 방식에 대한 정교한 기준 마련
- 기술개발-시험·검증-실증-현업 적용-운영·재학습 등 성과를 후속 R&D·인재양성·데이터·제도 개선에 반영하여 선순환 체계 조성

참고문헌

- AI Security Institute, Our Evaluation of Claude Mythos Preview's Cyber Capabilities, 2026.4.
- Anthropic, AI Models Are Showing a Greater Ability to Find and Exploit Vulnerabilities on Realistic Cyber Ranges, 2026.1.
- Anthropic, Assessing Claude Mythos Preview's Cybersecurity Capabilities, 2026.4.
- Anthropic, Investigating Three Real-World Incidents in Our Cybersecurity Evaluations, 2026.7.
- Anthropic, Project Glasswing: An Initial Update, 2026.5.
- Anthropic, Project Glasswing: Securing Critical Software for the AI Era, 2026.4.
- Australian Signals Directorate, Careful Adoption of Agentic AI Services, 2026.5.
- Cyberspace Administration of China, Interim Measures for the Management of Generative Artificial Intelligence Services, 2023.7.
- Cyberspace Administration of China, Measures for Labeling Artificial-Intelligence- Generated and Synthetic Content, 2025.3.
- Cyberspace Administration of China, 스마트 에이전트 규범적 응용 및 혁신발전 실시의견, 2026.5.
- Defense Advanced Research Projects Agency, AI Cyber Challenge Marks Pivotal Inflection Point for Cyber Defense, 2025.8.
- EC (2025a), Horizon Europe Work Programme 2026-2027: 6. Civil Security for Society, European Commission Decision C 8493 of 11 December 2025.
- EC (2025b), Horizon Europe Work Programme 2026-2027: 3. Research Infrastructure, European Commission Decision C 8493 of 11 December 2025.
- European Innovation Council, Call for CSA (coordination and support action): Financial Support to access services from EIC Ecosystem Partners, 2026.1., https://eic.ec.europa.eu/news/call-csa-coordination-and-support-action-financial-support-access-services-eic-ecosystem-partners-2026-01-12_en.
- European Parliament and Council, Regulation (EU) 2024/1689, Laying Down Harmonised Rules on Artificial Intelligence, 2024.7.
- European Telecommunications Standards Institute, ETSI EN 304 223 V2.1.1, Securing Artificial Intelligence (SAI); Baseline Cyber Security Requirements for AI Models and Systems, 2025.12.
- GAO (2025), "Artificial Intelligence: Generative AI Use and Management at Federal Agencies", Report to Congressional Requesters, GAO-25-107653.

- Google Threat Intelligence Group, GTIG AI Threat Tracker: Distillation, Experimentation, and (Continued) Integration of AI for Adversarial Use, 2026.2.
- https://aiexports.gov/.
- https://digital-strategy.ec.europa.eu/en/library/eu-action-plan-cybersecurity-and-artificial-intelligence.
- https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1544.
- https://en.wikipedia.org/wiki/World_Artificial_Intelligence_Cooperation_Organization.
- https://eucrim.eu/news/council-of-europe-convention-on-artificial-intelligence/.
- https://www.aikorea.go.kr/web/main.do?editorType=smarteditor&screenTp=USER.
- https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion.
- https://www.irobotnews.com/news/articleView.html?idxno=44544.
- https://www.korea.kr/briefing/pressReleaseView.do?call_from=seoul_paper&newsId=156686561.
- https://www.oecd.org/en/about/news/press-releases/2026/05/oecd-launches-streamlined-hiroshima-ai-process-reporting-framework-to-help-small-and-medium-sized-enterprises-participate.html.
- https://www.state.gov/pax-silica.
- https://www.un.org/global-dialogue-ai-governance/en.
- https://www.yna.co.kr/view/AKR20260927021900003.
- Japan AI Safety Institute, Approach Book for AI Incident Response, 2026.1.
- Japan AI Safety Institute, Known Attacks and Their Impacts on AI Systems, 2026.4.
- KB금융지주 경영연구소, AI를 바라보는 두 가지 시선 — 오픈AI와 앤스로픽 이야기, KB 지식 비타민, 2026.5.
- KB금융지주 경영연구소, 차세대 AI 리더십의 격전지 피지컬 AI: 산업 패러다임의 재정의와 엔비디아의 생태계 구축 전략, KB 지식 비타민, 2026.2.
- KISTI, KISTI, NVIDIA·HPE와 슈퍼컴 6호기 '한강' 기반 AI·HPC 협력 본격화, 2026.3., https://www.kisti.re.kr/promote/post/news/6916;jsessionid=IkjIgBqJVbM4HUwcSC9DAnkXdPUevArcFQwhPmNig1fkJoIQtM9JaiXXuK6EU0Tk.ar211_servlet_engine23?t=1774029600044.
- KITA, '세계 최초' EU AI규제법 2일 발효…전면 시행은 2년 뒤, 2024.8., https://www.kita.net/board/totalTradeNews/totalTradeNewsDetail.do?no=85448&siteId=2.
- National Cyber Security Centre, Impact of AI on Cyber Threat from Now to 2027, 2025.5.
- National Cyber Security Centre, Preparing for a ‘Vulnerability Patch Wave’, 2026.5.
- National Cyber Security Centre, Why Cyber Defenders Need to Be Ready for Frontier AI, 2026.3.

- National Institute of Standards and Technology, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, 2025.3.
- National Institute of Standards and Technology, Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile): NIST Community Profile, Initial Preliminary Draft, 2025.12.
- NIST, AI RMF Playbook, 2023.1.
- OpenAI, OpenAI and Hugging Face Partner to Address Security Incident During Model Evaluation, 2026.7.
- Standardization Administration of China, National Standard Plan 20263116-Q-252, General Security Requirements for Artificial Intelligence Agent Application, 2026.6.
- Stanford HAI, Artificial Intelligence Index Report 2026, Stanford University, 2026.4.
- State Administration for Market Regulation and Standardization Administration of China, GB 45438-2025, Cybersecurity Technology-Labeling Method for Content Generated by Artificial Intelligence, 2025.2.
- The White House, Executive Order 14409, Promoting Advanced Artificial Intelligence Innovation and Security, 2026.6.
- The White House, Winning the Race: America's AI Action Plan, 2025.7.
- 과학기술정보통신부, '한국 AI안전연구소' 출범…AI 위협에 체계적·전문적 대응, 2024.11.
- 과학기술정보통신부, AI 기반 사이버위협에 대응하기 위한 민간 정보보호 추진계획, 2026.5.
- 과학기술정보통신부, 과기정통부-앤트로픽, 글로벌 AI 안전·보안 동맹 전면 추진, 2026.6.
- 과학기술정보통신부·한국정책학회, AI·디지털 전환에 따른 공공부문 데이터 거버넌스 전략, 2025.12.
- 국가법령정보센터(https://www.law.go.kr).
- 국제금융센터, 미중 AI 패권경쟁 평가 및 시사점, Issue Analysis, 2026.8.
- 국회입법조사처, 미국 정부의 미토스(Mythos) 수출 통제가 남긴 것: 고성능 AI 모델 전략자산화와 한국 소버린 AI의 과제, 이슈와 논점 제2510호, 2026.7.
- 대외경제정책연구원, 사우디아라비아와 UAE의 AI 산업 전략과 정책 시사점, 전략지역심층연구 25-02, 2026.4.
- 대한민국, 법률 제20676호, 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법, 2025.1.
- 산업연구원, AI 전환 시대 핵심 인프라, 서버산업의 현황과 정책 시사점, KIET 산업포커스, 2026.5.
- 삼일PwC, 한국 AI 데이터센터 산업의 현재와 투자방향: AI 인프라 Value Chain 관점의 구조적 투자 기회, 2026.3.
- 에너지경제연구원, AI 시대 데이터센터 증가의 국내 에너지 소비 시사점, 기본연구보고서 2025-09, 2025.12.

- 정보통신기획평가원, Sovereign AI 동향 및 시사점, 이슈분석 제827호, 2024.10.
- 정보통신정책연구원, AI Index로 조망한 국가별 AI 준비도, KISDI STAT Report 25-11호, 2025.11.
- 정보통신정책연구원, AI 에이전트 시대의 국가전략, KISDI AI Outlook Vol. 25, 2026.7.
- 정보통신정책연구원, AI 진화와 패권형 소버린 AI 전략, KISDI AI Outlook Vol. 23, 2025.12.
- 포스코경영연구원, AI 시대, R&D 대혁명: 생산성 위기의 타개와 패러다임 전환, POSRI 이슈리포트, 2026.8.
- 포스코경영연구원, 한국 AI 산업의 위상과 도약 과제 - Stanford 2026 AI Index 분석을 중심으로 -, POSRI 이슈리포트, 2026.5.
- 한국과학기술기획평가원, 국가안보 우선 시대의 과학기술 견인: 주요국의 자원 투입 메커니즘 분석, 과학기술&ICT 정책·기술 동향, 2026.6.
- 한국산업기술진흥원, 스탠퍼드大 인간중심 인공지능 연구소의 'AI 지수', KIAT Policy Brief 2026-01, 2026.6.
- 한국산업은행, Physical AI 산업 생태계 분석 및 경쟁력 강화 방안, KDB Report 이슈분석, 2026.7.
- 한국산업은행, 미국 AI 데이터센터 병목 현상과 시사점, KDB Report 이슈브리프, 2026.7.6.
- 한국은행, AI의 미시적 효과가 거시적 성장으로 이어지려면? - 범용기술(GPT)의 역사에서 찾는 시사점, BOK경제연구 Insight 제2026-1호, 2026.7.
- 한국인터넷진흥원, AI 보안 레드티밍 가이드, 2026.7.
- 한국인터넷진흥원, AI 보안 위협 대응 매뉴얼, 2026.7.
- 한국인터넷진흥원, 인공지능(AI) 보안 안내서, 2025.12.
- 한국지능정보사회진흥원, 2026 스탠포드 AI INDEX로 살펴본 우리나라 AI 현황 분석, AI Policy Insights 2026 Vol.03, 2026.6.
- Carbon Credits, Tesla vs. Waymo: Who Will Win the Robotaxi Race?, 2026.7. (https://carboncredits.com/tesla-vs-waymo-robotaxi-race-tampa/).
- CSIS, Sourcing Requirements and U.S. Technological Competitiveness, 2025.3.
- DOE, AI for Science: Report on the Department of Energy (DOE) Town Halls, 2020.2.
- DOE, Energy Department Announces $293 Million in Funding to Support Genesis Mission National Science and Technology Challenges, 2026.3., https://www.energy.gov/articles/energy-department-announces-293-million-funding-support-genesis-mission-national-science.
- EUR-Lex, European high-performance computing joint undertaking, 2019.3., https://eur-lex.europa.eu/EN/legal-content/summary/1_european-high-performance-computing-joint-undertaking.html.
- European Commision, AI Factories, 2026.8.,

https://digital-strategy.ec.europa.eu/en/policies/ai-factories.

- European Commision, Horizon Europe, https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
- European Commision, The European Commission Announces the EOSC EU Node's Transition to Full Production, 2024.10., https://open-science-cloud.ec.europa.eu/news/european-commission-announces-eosc-eu-nodes-transition-full-production.
- Genesis Open Models, U.S. Department of Energy Launches the Genesis Open Models Initiative and, with Arcee, Unveils Genesis-Science-1 — Its First Open-Weight Model for Scientific Research, https://genesisopenmodels.anl.gov/.
- Han, H., Hu, X., Jiang, J. et al. U.S.-China trade conflicts and R&D investment: evidence from the BIS entity lists. Humanit Soc Sci Commun 11, 212 (2024).
- IBM, AI & Quantum for New Computation Paradigms, https://research.ibm.com/projects/ai-and-quantum-for-new-computation-paradigms.
- Information Technology and Innovation Foundation(2026.6.8.), Korea's STEM Talent Challenge: Fixing Incentives for Deployability.
- JST 研究開発戦略センター, AI for Scienceの動向 2026— AIトランスフォーメーションに伴う科学技術・イノベーションの変容, 2026.1.
- KOSTEC, 중국의 AI for Science : 중국과학원 ScienceOne 100 모델 발표, 2026.5.
- LG 보도자료, “국내 첫 교육부 인가 사내 대학원, ‘LG AI대학원’”, 2025.8.
- METI, Selection of Nine R&D Themes related to Making Manufacturing and Other Data AI-Ready and Two R&D Themes related to Robotics Foundation Models Under the “GENIAC” Project to Strengthen Generative AI Development Capabilities, 2026.5. (https://www.meti.go.jp/english/press/2026/0514_001.html).
- NEDO, 「AIロボット・フィジカルAIを見据えたマルチモーダル基盤モデル開発事業」 の実施体制の決定について, 2026.6.30. (https://www.nedo.go.jp/koubo/CD3_100431.html).
- NEDO, No. 15: Social implementation of Smart Mobility Platform based on social acceptance and stakeholder coordination
- Ni, S., Chen, G., Li, S.,et al. A Survey on Large Language Model Benchmarks. arXiv Cornell University (2025).
- NRF, 과학기술 AI 혁신 연구 시스템 구축을 위한 국가 전략 기획연구, 2026.7.
- OECD, Artificial Intelligence in Science: Challenges, Opportunities and the Future of

Research, OECD Publishing, 2023.1.

- OpenAI, Ten advances in mathematics and theoretical computer science, 2026.8., https://openai.com/index/ten-advances-in-mathematics/
- SCIANCE, SCIANCE: AI in Science, https://www.sciance.eu/.
- UNICON SOFT, Zeekr avtomobil zavodida odamsimon robotlar “amaliyotga chiqdi”, 2025.3. (https://us.uz/uz/news/post-323).
- Wallace, D., Griffin, C., O’Neill, S., et al. Conjecture Machines: AI agents and the new validation bottleneck in science. Google DeepMind Research (2026).
- Xu, Y., Liu, X., Cao, X. et al. Artificial intelligence: A powerful paradigm for scientific research. The Innovation (2021).
- Xu, Z., Cheng, Y., Yang, Y. et al. AI FOR SCIENCE 2025. Nature research intelligence (2025).
- Yannis Ioannidis. The 5th Paradigm: AI-Driven Scientific Discovery. Communications of the ACM 67, 12 (2024).
- YTN, 운전대도 페달도 없다...자율주행 새 시대 여는 '죽스' [자막뉴스], 2026.8.9. (https://www.ytn.co.kr/_ln/0134_202608090819395029)
- Zhao, Y., Liu, Y., Han, Y., et al. AI for Science: A Systematic Survey of Architectures, Autonomy, and Open Challenges. Preprints.Org (2026).
- 과학기술정보통신부,「AI시대 과학기술 경쟁력 대도약을 위한 K-문샷 추진전략(안)」, 2026.2.
- 과학기술정보통신부,「주요 R&D 권역별 간담회」, 2026.1.
- 과학기술정책연구원, 과학기술인력의 공급체계 변화 진단과 양성정책 개선방안 연구, 2025.11.
- 관계부처 합동,「AI 대전환 시대, 데이터 정책 추진방향」, 2026.5.
- 관계부처 합동,「글로벌 과학기술 강국 실현을 위한 AI+S&T 활성화 방안」, 2025.3.
- 국가과학기술자문회의 심의회의, 2027년도 국가연구개발사업 예산 편성(안), 2026.8.
- 국가과학기술자문회의 심의회의, 2027년도 국가연구개발사업 투자방향 및 기준, 2026.3.
- 国务院 (2017), ”国务院关于印发新一代人工智能发展规划的通知“, 2017.7.
- 国务院 (2025), “国务院关于深入实施“人工智能+”行动的意见“.
- 国土交通省, 自動運転トラックの社会実装及び物流の効率化を推進 ~「自動運転トラックによる幹線輸送の社会実装に向けた実証事業」を公募~, 2026.5.
- 국회미래연구원, 정부 R&D 투자효율성 제고를 위한 정책방향, 2025.10.
- 대한상공회의소, 한국의 고급인력 해외유출 현상의 경제적 영향과 대응방안, 2025.6.
- 데이터산업진흥원, 2023년 데이터산업 현황조사, 2024.5.
- 데이터산업진흥원, 2025년 데이터산업 현황조사, 2026.5.

- 동아일보, 中 '동수서산' 프로젝트 본격 가동, 디지털 경제 발전에 탄력, 2022.2., https://www.donga.com/news/Inter/article/all/20220223/111996252/1
- 로봇신문, 中 유니트리, 19일 상하이 증시 정식 상장, 2026.8.
- 매일경제, 美, 중국산 드론 이어 로봇도 '수입 금지', 2026.7.
- 防災科学技術研究所(2024), "基盤的防災情報流通ネットワーク (SIP4D", 令和6年度成果発表会, 半田信之.
- 산업통상자원부, 「산업현장 기술혁신 가속화를 위한 AI+R&DI 추진전략」, 2024.10.
- 소프트웨어정책연구소, 2024년 인공지능산업 실태조사, 2025.4.
- 소프트웨어정책연구소, AI 실무인재 양성을 위한 국내 교육체계 분석 및 시사점, 2026.2.
- 소프트웨어정책연구소, AI 확산 시대에 대응한 가치사슬 기반 AI 인력 분류체계 재정립, 2026.3.
- 소프트웨어정책연구소, AI시대 데이터 상호운용성 및 이동권 활성화 전략 연구, 2026.4.
- 소프트웨어정책연구소, 과학을 위한 AI(AI4Science) 연구의 패러다임을 바꾸다, 2025.9.
- 소프트웨어정책연구소, 양자컴퓨팅과 AI 융합발전 가능성과 시사점, 2025.7.
- 이데일리, "서울대, 현직교수 첫 '상근 겸직' 승인…한보형 교수 삼전 부사장급 겸임", 2026.7.
- 전자신문, ['제조AX(M.AX)' 골든타임을 잡아라] 〈1〉대한민국, AX로 1등 제조강국 굳힌다, 2025.9. (https://m.etnews.com/20250928000049)
- 정보통신기획평가원, 고품질 데이터의 요건과 국내외 기업 동향 및 시사점, 2026.4.
- 정보통신기획평가원, 주요국의 AI데이터 활용 정책, 2026.1.
- 조선일보, "AI 훈련 위해… 직원 이메일·업무기록까지 거래", 2026.8.
- 한국과학기술기획평가원, AI 시대 데이터 활용 병목과 정책 과제, 과학기술&ICT 정책·기술 동향 315호, 2026.7.
- 한국과학기술기획평가원, 글로벌 인재 허브 실현을 위한 해외 우수 과학기술 인재 유치 방안 연구, 2024.12.
- 한국과학기술기획평가원, 백악관, '트럼프 대통령의 미국 사이버 전략' 공개, 과학기술&ICT 정책·기술 동향 No.307, 2026.4.
- 한국과학기술기획평가원, 첨단 R&D 경쟁의 시대: 글로벌 과학기술정책 동향과 한국의 전략, 과학기술&ICT 정책·기술 동향 299호, 2025.11.
- 한국과학기술기획평가원, 한국 과학기술(STEM) 인력의 과제: 인력 배치를 위한 인센티브 구조 개선, 2026.8.
- 한국과학기술기획평가원·정보통신기획평가원, AI 대전환과 데이터 정체: 고급 데이터 공급망 전쟁, 과학기술&ICT 정책·기술 동향 302호, 2026.1.
- 한국과학기술정보연구원, 글로벌 사례를 통한 국가 AI4S 실행방안, 2026.4.
- 한국과학기술정보연구원, 차세대 AI 기술 확산에 따른 전망 및 시사점, 2026.
- 한국일보, "정부 지원 AI대학원 취업률 63.5%… 기업-대학 인력 미스매치 해소를", 2025.6.

• 한국지능정보사회진흥원, “한국형 데이터 스페이스(K-Data Space)”, AX 시대, 데이터 공유·활용 패러다임 전환 전략, 2025.10.
• 한국지능정보사회진흥원, 데이터 신질서와 생태계 조성을 위한 “국가 데이터 인프라” 개념과 추진 전략, 2024.8.

저자

KISTEP 전략기술정책센터 박노언 센터장
성장동력투자전략센터 채명식 연구위원
성장동력투자전략센터 김주일 선임전문관리원
성장동력투자전략센터 정두엽 부연구위원
성장동력투자전략센터 허아람 선임전문관리원
성장동력투자전략센터 김동혁 연구원
성장동력투자전략센터 박윤경 연구원

용어 해설

Agentic AI | 에이전틱 AI
주어진 목표를 달성하기 위해 필요한 작업을 스스로 계획하고, 외부 도구·시스템을 활용해 실행하며, 결과를 평가·조정하는 인공지능

AIDC | AI Data Center
인공지능 모델의 학습과 추론에 필요한 대규모 연산을 처리하기 위해 GPU 등 고성능 연산장치와 고속 네트워크, 데이터 저장장치, 전력·냉각 설비를 갖춘 데이터센터

AI-Ready Data | 인공지능 친화적 (고품질) 데이터
AI 학습·추론에 적합하도록 품질·구조·메타데이터가 정비된 데이터

Generative AI | 생성형 AI
학습한 데이터의 패턴과 구조를 바탕으로 사용자의 요청에 따라 텍스트·이미지·음성·영상·코드 등의 새로운 콘텐츠를 생성하는 인공지능

Distillation | 지식 증류
성능이 높은 교사 모델의 출력이나 내부 표현 등을 학생 모델이 학습하도록 하여, 교사 모델의 지식과 동작을 전달하는 기술입니다. 주로 대형 모델의 능력을 더 작은 모델에 전달하는 데 활용

Frontier AI | 최첨단 AI
현시점에서 가장 앞선 수준의 성능과 범용성을 갖추고, 기존 AI의 능력과 활용 범위를 확장하는 인공지능을 의미

GPU | Graphics Processing Unit, 그래픽 처리 장치
다수의 연산을 동시에 수행하는 병렬처리에 특화된 반도체. 당초 이미지·영상 등 그래픽 처리를 위해 개발됐으나, 현재는 대규모 행렬 연산이 필요한 AI 모델의 학습과 추론에도 널리 활용

Humanoid Robot | 인간형 로봇
머리·몸통·팔·다리 등 인간과 유사한 신체 구조를 갖추고, 사람의 동작이나 작업 방식을 모방하도록 설계된 로봇

LLM | Large Language Model, 거대 언어 모델
대용량의 인간 언어를 이해하고 생성할 수 있도록 훈련된 인공지능(AI) 모델로, 딥러닝 알고리즘과 통계 모델링을 바탕으로 자연어처리 작업에 활용. 주어진 언어 범위 내에서 정해진 패턴이나 구조, 관계를 학습하는 기존 언어모델과 달리 대규모 언어 데이터를 학습해 문장 구조 문법, 의미 등을 파악하고 자연스러운 대화 형태로 상호작용이 가능

Physical AI | 피지컬 AI
센서와 액추에이터 등 물리 장치와 결합되어, 실제 환경에서 자율적으로 인식, 판단, 행동을 수행하는 인공지능 기술

RAG | Retrieval-Augmented Generation
사용자의 질문과 관련된 정보를 외부 문서나 데이터베이스에서 검색한 뒤, 이를 참고하여 생성형 AI가 답변을 만드는 기술

Red Teaming | 레드티밍
공격자의 관점에서 시스템에 대한 공격이나 오용을 시도해 취약점과 잠재적 위험을 사전에 찾아내는 시험·평가 활동

ROI | Return on Investment
투자수익률, 투자한 비용 대비 발생한 수익 또는 투자효과를 나타내는 지표로, AI·로봇 등 신기술의 도입에 따른 비용 대비 생산성 향상·인건비 절감·수익 증가 등의 경제적 효과를 평가하는 데 활용

SDV | Software-Defined Vehicle
소프트웨어 중심 자동차, 차량의 주요 기능과 성능이 하드웨어보다 소프트웨어를 통해 정의·제어되는 자동차로, 중앙집중형 전자·전기 아키텍처와 OTA 업데이트 등을 통해 차량 기능을 지속적으로 개선·확장할 수 있는 것이 특징

TCO | Total Cost of Ownership
총소유비용, 제품이나 시스템의 도입부터 운영·유지보수·폐기까지 전체 수명주기 동안 발생하는 총비용으로, 초기 구매비용뿐 아니라 운영비·인건비·에너지비·유지보수비 등을 종합적으로 고려하여 경제성을 평가하는 지표

TEVV | Test, Evaluation, Validation and Verification
시스템이 정해진 요구사항을 충족하고, 실제 사용 환경에서 의도한 목적에 적합하게 작동하는지를 체계적으로 확인하는 일련의 활동

Vertical AI | 버티컬 AI, 도메인 특화 AI
특정 산업이나 업무 환경을 전제로 설계된 도메인 특화 인공지능. 범용 AI가 다양한 분야에서 공통적으로 활용되도록 폭넓은 데이터와 일반적인 추론 능력에 기반한다면, 버티컬 AI는 특정 산업에서 실제로 사용되는 데이터 구조와 규제, 업무 절차를 중심으로 설계와 학습이 이루어짐

VLA | Vision-Language-Action
시각-언어-행동 모델, 카메라 등으로 획득한 시각정보와 자연어 명령을 함께 이해하고 이를 실제 로봇의 행동으로 변환하는 AI 모델로, 로봇이 주변 환경을 인식하고 사용자의 지시에 따라 작업을 수행하도록 하는 핵심 기술