

과학기술&ICT 정책·기술 동향

Science, ICT Policy and Technology Trends



CONTENTS

Ⅰ 이슈 분석	1	2. ICT	49
AI 심장, 데이터센터 : 정책·산업·기술 동향과 우리의 과제		AI 클래스, 차세대 사용자 인터페이스 경쟁 본격화	49
		Black Hat USA 2026, AI 공격의 가속과 방어체계 전환	62
		미국, 중국산 오픈웨이트 AI 모델 규제 범위와 대체 비용 논쟁 확산	75
		中, 대미 드론 수출통제·인증 협력 중단 등 대응 조치 발표	79
Ⅱ 주요 동향	23	Ⅲ 단신 동향	83
1. 과학기술	23	1. 해외	83
CSIS, RAM 공급난이 미국에 미치는 영향을 검토한 보고서를 발표	23	2. 국내	91
미국 CFI, 'AI 모델 탈취 방지 법안(DAAMTA)' 개선 의견 제안	26		
일본 CRDS, 미션지향형 과학기술혁신(STI) 정책 강화 방안 제안	29		
중국, '지식재산권 보호·활용 제15차 5개년 계획' 발표	32		
CSIS, 중국의 상업우주 발전이 미국에 미치는 영향을 분석한 보고서 발표	36		
CSIS, 미국 주정부·EU·산업계의 AI 규제 프레임워크 분석 보고서 발표	41		
JETRO, AI 시대 반도체 산업의 구조 변화 분석	44		
일본 PwC, 제조업의 'AI-Ready' 전환 전략 보고서 발표	47		



- 과학기술&ICT 정책 · 기술 동향 보고서는 한국과학기술기획평가원 기관고유사업의 일환으로 추진되고 있으며, 과학기술정보통신부의 지원 및 정보통신기획평가원(IITP)의 협조를 통해 발간되고 있습니다.
- 관련 자료는 <https://www.kistep.re.kr/gps/>를 통해서도 서비스를 이용할 수 있으며, 보고서 내용에 대한 문의는 아래와 같이 주시기 바랍니다.

과학기술
동향



KISTEP 한국과학기술기획평가원
Korea Institute of S&T Evaluation and Planning
TEL: 043-750-2670
E-mail: bchun@kistep.re.kr

ICT 동향



IITP 정보통신기획평가원
Institute of Information & Communications
Technology Planning & Evaluation
TEL: 042-612-8240
E-mail: now2@iitp.kr



AI 심장, 데이터센터 : 정책·산업·기술 동향과 우리의 과제¹⁾

1 AI 시대, 데이터센터가 국가 핵심 인프라로 부상

가. 생성형 AI 확산과 컴퓨팅 수요의 폭증

➔ 데이터 폭발과 연산 수요의 패러다임 전환

- 초거대 언어모델(LLM)과 생성형 AI의 발전으로 글로벌 컴퓨팅 연산 수요가 기하급수적으로 폭증하고 있음
 - 과거의 연산이 정형 데이터의 단순 처리와 저장에 집중되었다면, 현재는 수천억 개의 파라미터를 갖춘 모델의 학습(Training)과 실시간 추론(Inference)을 위한 대규모 병렬 연산을 요구함

➔ 컴퓨팅 자원의 희소성 심화

- 대규모 언어모델이 컨텍스트 길이와 동시 사용자 수를 확장함에 따라, 그래픽 처리장치(GPU) 및 고대역폭메모리(HBM) 수요가 공급을 압도하고 있음
 - 이는 단순한 칩 확보 경쟁을 넘어 칩을 가동할 전력, 냉각, 통신망이 집적된 ‘물리적 인프라’의 공급 병목 현상으로 이어짐

나. 전통 데이터센터에서 AI 데이터센터로의 전환

➔ 아키텍처의 근본적 변화

- 기존 클라우드 데이터센터가 중앙처리장치(CPU) 중심의 범용 워크로드를 위해 설계되었다면, AI 데이터센터는 GPU, 신경망처리장치(NPU) 등 고밀도·고전력 연산에 특화된 가속기 기반 구조로 진화함

➔ 전력 밀도와 물리적 스트레스 급증

- 전통적 데이터센터의 랙(Rack)당 전력 밀도는 평균 3~10kW 수준이었으나, AI 데이터센터는 40kW에서 120kW 이상의 초고밀도 전력을 요구함
 - 이러한 부하 패턴은 전력망에 극심한 과도 상태(Transient) 스트레스를 유발하며, 인프라의 전면적인 재설계가 불가피함²⁾

1) 정보통신기획평가원 디지털인프라단 디지털인프라전략팀 백선경 팀장(sunkyoung100@iitp.kr)
본 고는 저자의 개인적인 견해이며 과학기술정보통신부와 KISTEP의 공식적인 의견이 아닙니다.

다. AI 데이터센터를 둘러싼 글로벌 투자 경쟁

⇒ 하이퍼스케일러 및 자본의 대규모 유입

- 하이퍼스케일러 기업들은 글로벌 AI 주도권을 확보하기 위해 연간 수천억 달러를 AI 인프라에 투자하고 있으며, 투자 규모는 지속 확대 중
 - ※ '25년 대비 '26년 투자 규모(달러): (마이크로소프트) 800억 → 1900억, (아마존) 1,000억 → 2,000억, (구글) 750억 → 1,850억 수준
- 전 세계 AI 데이터센터 인프라 투자 규모는 '30년까지 약 5조 5천억 달러 (약 8,030조 원)에 이를 것으로 전망됨³⁾
- 미국·EU·UAE 등 주요국은 국가 주도로 대규모 AI 인프라에 투자 중임

〈 주요국 AI 인프라 투자 현황 〉

미국	EU	UAE	싱가폴	대만	사우디
스타게이트(Stargate) 프로젝트	AI대륙 액션플랜(AI Continent Action Plan)	국부펀드 전용 투자사 MGX	친환경 데이터센터 로드맵 (Green DC Roadmap)	TSMC 중심 반도체 및 AI 파운드리 인프라 구축	트랜센더스 프로젝트 & 국부펀드
최대 5,000억 달러 (약 730조원)	총 2,000억 유로 (약 310조원)	최대 1,000억 달러 (약 146조원)	기존 1.4GW + 추가 300MW~1.5GW 전력 공급 목표	연간 600억 달러 ↑ (약 88조원)	최대 1,000억 달러 (약 146조원)

출처 : 저자 작성

⇒ '전력-부지-냉각' 선점 전쟁

- 최신 AI 데이터센터 경쟁의 핵심은 칩 구매력이 아니라 '전력 및 수자원'의 안정적 확보로 이동함
- 이에 따라 대형 원자력 발전 및 소형모듈원전(SMR)과 결합된 오프그리드 (Off-grid) 데이터센터 투자가 폭발적으로 증가하고 있음

라. AI 데이터센터의 국가 전략적 의미

⇒ AI 주권(Sovereign AI)과 컴퓨팅 주권

- 자체적인 기초 모델과 이를 구동할 컴퓨팅 인프라를 보유하지 못한 국가는 기술적·경제적·문화적 종속을 피할 수 없음
- AI 데이터센터는 민간 상업 시설을 넘어 국가의 '디지털 영토'를 결정짓는 핵심 안보 자산으로 격상됨

⇒ 산업 경쟁력과 AI 생태계

- 대규모 컴퓨팅 자원 접근성은 자국 스타트업, 학계, 연구기관의 혁신 속도를 좌우함

2) 다우 IDC(<https://blog.daoudc.com/>), AI 데이터센터란 무엇인가?(25.11)

3) JP모건, Barron's·Dow Jones·Investor's Business Daily(26.6)

- 고성능 인프라가 구축된 국가와 지역으로 인재와 자본이 집중되는 ‘클러스터 효과’가 극대화되고 있음

⇒ 반도체·전력·통신·클라우드 산업과의 연계

- AI 데이터센터는 첨단 반도체(초고속 메모리, NPU), 차세대 전력망, 초저지연 통신 패브릭, 액체 냉각 설비 등 가치사슬 전반의 기술이 융합된 최종 집결지로, 인프라 구축 경쟁력이 곧 유관 산업의 글로벌 패권으로 직결됨

2 AI 데이터센터의 개념과 산업 생태계

가. AI 데이터센터의 정의와 특징

⇒ (정의) 방대한 비정형 데이터의 고속 처리 및 초저대 AI 모델의 분산 학습·추론 워크로드에 최적화되도록 설계된 특수 목적의 컴퓨팅 인프라

⇒ (특징) ▲수천~수만 개의 AI 가속기(GPU/NPU/TPU/DPU 등) 병렬 연결, ▲초저지연 고대역폭 네트워크(InfiniBand, Ultra Ethernet 등) 적용, ▲랙당 40~120kW 이상의 초고전력 밀도, ▲고발열·고열밀도 문제를 해소하기 위한 액체 냉각(Liquid Cooling) 기반의 열 관리 시스템이 필수적임

〈 기존 클라우드 데이터센터와 AI 데이터센터의 차이 〉

구분	기존 클라우드 데이터센터	AI 데이터센터
주요 워크로드	트랜잭션, 웹 서비스, 범용 IT (비동기적 처리)	AI 모델 학습(Training) 및 대규모 추론 (동기화된 집단 연산)
핵심 프로세서	CPU 기반	GPU, NPU 등 AI 가속기 기반
랙당 전력 밀도	평균 3 ~ 10kW	40 ~ 120kW 이상 (초고밀도)
네트워크 구조	이더넷(Ethernet) 중심, 트래픽 지연 내성 존재	InfiniBand, NVLink, Ultra Ethernet 등 초저지연 무손실 패브릭 필수
주요 냉각 방식	공랭식 (CRAC/CRAH)	직접액체냉각(D2C), 액침냉각(Immersion)
인프라 부하 특성	무작위 분포(Random Distribution) 형태의 부하	칩들이 동시에 연산하는 동기화된 집단행동(High di/dt) 발생

출처 : 저자 작성

나. AI 데이터센터의 주요 유형

〈 AI 데이터센터 유형별 특징 〉

유형	특징
AI 학습(Training) 중심	• 수만 개의 GPU를 거대한 단일 클러스터로 묶어 파운데이션 모델을 훈련하는 시설 - 지연시간보다 무조건 대규모 전력 공급이 중요하여 부지와 전기료가 저렴한 외곽 지역에 하이퍼스케일 규모로 구축됨
AI 추론(Inference) 중심	• 완성된 모델을 바탕으로 사용자 질의에 실시간 응답하는 시설 - 낮은 지연시간(Latency) 확보가 필수적이므로 사용자 밀집 지역이나 도심 근교에 엣지(Edge) 형태로 구축되는 경향이 큼
Hyperscale / Colocation / Sovereign AI	• 대형 테크 기업의 자가 사용형(하이퍼스케일), 공간 및 설비를 임대하는 상업용(코로케이션), 국가 데이터 주권 보호를 위해 정부 주도로 구축하는 폐쇄형 인프라(소버린 AI)로 구분됨
Neocloud (네오클라우드)	• AI 연산에만 100% 특화하여 GPU를 서비스형(GPUaaS)으로 제공하는 신흥 클라우드 - 범용 클라우드의 가상화 오버헤드를 제거한 베어메탈 인프라를 제공하며, 기존 하이퍼스케일러 대비 동급 인프라 사용료를 약 65% 절감하는 압도적 비용 경쟁력으로 급성장 중임⁴⁾ - 코어위브(CoreWeave), 람다랩스(Lambda Labs), 크루소(Crusoe), 네비우스(Nebius) 등이 대표적임

출처 : 저자 작성

다. AI 데이터센터 산업의 가치사슬

〈 AI 데이터센터 산업 가치사슬 〉

분류	기업 형태
AI 반도체	• AI 가속기*, 데이터 프로세싱 유닛(DPU)**, 고대역폭메모리(HBM)*** 등 반도체 설계 및 제조 기업 * 대규모 AI 학습·추론 연산을 수행하는 GPU·NPU·TPU 등 ** 데이터 이동·네트워크·스토리지 처리를 가속하여 연산 효율을 높이는 장치 *** AI 가속기의 메모리 병목을 완화하는 메모리 장치
AI 반도체 솔루션	• CPU·가속기·메모리 간 고속 연결 및 메모리 확장·공유를 지원하는 CXL(Compute Express Link) 기반 컨트롤러·스위치 및 메모리 솔루션 등을 설계·제조하는 반도체 및 관련 솔루션 기업
서버	• GPU·NPU·TPU 등 고성능 AI 가속기와 CPU, HBM 및 고속 인터커넥트를 집적한 고밀도 AI 서버·랙 시스템을 설계·통합하는 서버 제조사 및 시스템 통합 업체
스토리지	• AI 학습·추론 과정에서 발생하는 대규모 데이터셋과 모델 파라미터를 신속하게 공급·저장하기 위한 NVMe SSD, NVMe-oF, 병렬 파일시스템 및 분산 스토리지 기반의 고성능·대용량 스토리지 시스템 공급 업체
네트워크	• 수천~수만 개의 AI 가속기 및 서버 노드를 하나의 대규모 클러스터로 연결하고, 분산 학습 과정에서 발생하는 대용량 데이터 교환과 집단통신(Collective Communication)의 병목을 최소화하기 위한 초저지연·고대역폭 네트워크 인프라 공급 업체
전력·냉각	• 랙당 수십~100kW 이상으로 증가하는 AI 데이터센터의 초고전력 밀도와 이에 따른 고발열·고열밀도 문제를 안정적으로 처리하기 위한 전력 공급·분배 및 열관리 인프라 공급 업체

4) 디지털서비스(<https://www.digitalmarket.kr/>), 네오클라우드- AI 시대의 새로운 인프라 패러다임(26.1)



분류	기업 형태
데이터센터 설계·건설	AI 서버의 초고중량·고전력·고발열 특성을 반영해 데이터센터의 부지 선정부터 전력 인입, 건축, 기계·전기·배관(MEP), 냉각 및 네트워크 인프라까지 통합 설계·시공하는 엔지니어링·EPC(Engineering-Procurement -Construction)·건설업체
클라우드·AI 플랫폼	- 대규모 GPU·AI 가속기 인프라를 구축하고 이를 기업·개발자에게 서비스 형태로 제공하는 하이퍼스케일러 - 클라우드 서비스 사업자(CSP) - GPU 클라우드 및 전문 AI 인프라 서비스 사업자
운영·관리 소프트웨어	AI 데이터센터 내 서버·네트워크·전력·냉각 설비를 실시간으로 모니터링하고 자원 활용률과 에너지 효율을 최적화하는 DCIM*, BMS**, EMS** 및 AI 기반 운영 소프트웨어 공급 업체 * Data Center Infrastructure Management ** Building Management System *** Energy Management System

출처 : 저자 작성

라. 주요 사업자 및 산업구조 변화

⇒ 기존 클라우드 인프라는 AWS, MS, Google 등 소수 하이퍼스케일러가 지배했으나, AI 특화 네오클라우드(코어위브, 람다 등)가 엔비디아의 전략적 투자와 최신 칩 우선 할당 지원을 받으며 새로운 강력한 축으로 부상함

- H100, GB200 NVL72, Vera Rubin NVL72 등 최신 GPU 플랫폼을 대형 클라우드 사업자와 동등하거나 일부 세대에서는 더 빠르게 도입·상용화하며 시장 영향력을 확대

⇒ 빅테크 기업들 역시 엔비디아 의존도를 낮추기 위해 자체 맞춤형 AI 반도체(Custom Silicon) 개발을 강화하는 한편, 전력·냉각 설비부터 네트워크 인프라까지 데이터센터 아키텍처 전반을 내재화(수직계열화)하려는 시도를 가속화하고 있음

- Google, AWS, Microsoft, Meta 등 글로벌 빅테크 기업들은 TPU, Trainium, Maia, MTIA 등 자체 맞춤형 AI 반도체(Custom Silicon) 개발을 확대
- 나아가 자체 칩 간 인터커넥트와 AI 클러스터 네트워크, 서버·랙 시스템, 전력·액체 냉각 설비 및 소프트웨어 스택까지 공동 설계(Co-design)하는 추세임

3 AI 데이터센터 핵심 기술 동향

가. AI 컴퓨팅 기술

⇒ 대규모 모델 분산 처리 및 3D 병렬화(3D Parallelism) 고도화

- 최신 가속기들은 단일 칩 내 연산 능력의 극대화를 넘어, 거대한 모델을 여러 GPU로 쪼개어 연산하는 텐서 병렬화 파이프라인 기술을 필수적으로 적용함

- 데이터, 텐서, 파이프라인을 결합한 3D 병렬화(DeepSpeed, Megatron-LLM 등)를 통해 수만 개 규모의 GPU 클러스터 컴퓨팅 효율을 극대화할 수 있음⁵⁾

⇒ 초고성능 가속기 고도화

- 대규모 AI 연산에 특화된 범용 GPU 및 커스텀 ASIC/NPU 도입이 가속화됨
※ NVIDIA Blackwell/Rubin, Google TPU, AWS Trainium/Inferentia 등
- 저정밀도 연산 포맷(FP8, FP4, MXFPFP/Microscaling formats) 표준화로 컴퓨팅 성능 극대화 및 메모리 사용량 절감의 이점이 있음

⇒ 초고대역폭 메모리 및 3D 패키징

- HBM3E 상용화 및 HBM4(2048-bit 인터페이스, 로직 다이 통합) 전환으로 가속기 메모리 대역폭 한계를 돌파함
- CoWoS(Chip-on-Wafer-on-Substrate) 및 2.5D/3D 이종 집적 패키징 기술을 통한 칩렛(Chiplet) 구조의 컴퓨팅 밀도를 향상시킴

⇒ CXL(Compute Express Link) 기반 메모리 확장 및 풀링

- CXL 2.0/3.0 인터페이스를 활용한 메모리 확장 및 풀링 기술로 AI 서버 내 메모리 단편화 해소 및 동적 리소스 할당을 구현함
※ CXL 4.0 규격은 PCIe 7.0을 기반으로 128GT/s 전송 속도를 내며, 여러 물리 포트를 묶어 1.5TB/s 대역폭을 제공하는 ‘번들 포트’를 도입함⁶⁾

나. AI 서버 및 시스템 아키텍처

⇒ 초고밀도 랙 스케일 아키텍처(Rack-Scale Architecture)로의 진화

- 개별 서버 단위 설계에서 탈피하여, 엔비디아의 NVL 72, OCP Open Rack v3 등과 같이 랙 전체를 하나의 거대한 단일 컴퓨팅 노드로 통합하는 추세임
 - 초거대 AI 모델을 랙 내부에서 단일 시스템처럼 처리하여 지연을 최소화하고, 랙당 100kW~130kW 이상의 초고밀도 전력 및 냉각을 통합 관리하는 구조를 채택하고 있음

⇒ 서버 내 이종 프로세서 간 호환성 및 개방형 폼팩터 표준화

- 이종 프로세서 간의 메모리 공유 및 캐시 일관성 확보를 위해 CXL 및 PCIe 6.0/7.0 기반의 범용 인터커넥트 기술 도입이 가속화됨
- OCP 주도의 OAM(OCP Accelerator Module) 규격 및 UCIe(Universal Chiplet Interconnect Express) 칩렛 표준을 통해 이종 가속기를 동일 메인보드나 패키지 내에서 혼용 및 교체할 수 있는 상호운용성이 강화됨⁷⁾

5) NVIDIA, Megatron-LM & 3D Parallelism, Blackwell Architecture Technical Brief(‘24)

6) Introl Blog(<https://introl.com/>), CXL 4.0 인프라 계획 가이드: AI 스케일을 위한 메모리 풀링(‘26.3)

➔ 시스템 확장성(Scalability) 이슈 극복 아키텍처 도입

- 스케일업/아웃의 물리적 한계를 극복하기 위해 연산, 메모리, 스토리지를 물리적으로 분리한 뒤, 고속 패브릭망을 통해 워크로드 요구량에 맞춰 동적으로 자원을 할당 및 조합하는 기술을 적용함

다. 초고속 네트워크 기술

➔ 초고속 가속기 간(Scale-up) 인터커넥트: NVLink 및 UALink

- NVIDIA 독자 규격인 고대역폭 NVLink 기반 랙 단위 통합 기술에 대항하는 개방형 가속기 연결 표준인 UALink 도입 경쟁이 가속화됨

➔ 대규모 분산 클러스터(Scale-Out) 백본망 및 UEC(Ultra Ethernet Consortium) 이더넷

- 대규모 통신에 독보적인 Infiniband(Quantum-X800 등) 환경에서, AI 워크로드 처리에 특화된 UEC기반 차세대 이더넷(RoCE: RDMA over Converged Ethernet) 기술 등장으로 주도권 경쟁 중

➔ 광 인터커넥트(Optical Interconnect) 및 CPO(Co-Packaged Optics) 기술 적용

- 고대역폭·초저지연 백본망의 800Gbps 도입 확산 및 1.6Tbps 스위치/트랜시버 전환 가속화 추세에 따라 구리선의 신호 감쇄와 전력 소모 한계 극복이 필요함
- 이를 극복하기 위해 스위치 칩(ASIC) 패키지 내부에 광학 소자를 직접 통합하는 CPO 및 LPO(Linear-drive) 기술 도입을 시작함

➔ AI 최적화 패브릭 아키텍처

- 다대다(All-to-All) 통신 병목 해소를 위한 레일 최적화 Leaf-Spine, 초거대 AI 클러스터의 Dragonfly+, Leaf-Spine 다계층 스위칭 구조인 Non-blocking Fat-Tree 토폴로지 등을 채택하여 설계 중임

라. 스토리지 및 데이터 인프라 기술

➔ 초고속 병렬 파일 시스템 및 AI 전용 스토리지

- 수만 개 GPU에 데이터 공급이 지연되지 않도록 분산 병렬 파일 시스템(General Parallel File System) 필수화되는 추세임
- 텍스트, 이미지 등 페타바이트급 비정형 데이터를 AI 노드에 병목 없이 공급하기 위한 NVMe 기반의 올-플래시 스토리지 기술이 적용됨

7) OCP, OCP Open Rack v3(ORV3) Specification/UCI Consortium, Universal Chiplet Interconnect Express Specification

➔ GPU Direct Storage(GDS) 아키텍처

- CPU 메모리를 거치지 않고 NVMe 스토리지와 GPU 메모리 간 직접 DMA (Direct Memory Access) 전송을 통해 I/O 지연 시간 단축 및 CPU 부하 경감 효과를 극대화할 수 있는 구조임

마. 전력 인프라 기술⁸⁾

➔ 고전압 직류(HVDC) 및 랙 레벨 배전 효율화

- 교류-직류(AC-DC) 변환 단계를 최소화하여 전력 손실을 방지하고, 배전 설비가 차지하는 물리적 공간을 절감하여 컴퓨팅 인프라 밀집도 최적화를 위한 기존 48V DC 및 400V DC 버스바 랙 직결 구조 기술이 확산되고 있음

➔ 에너지 저장 시스템(BESS) 및 고효율 UPS(Uninterruptible Power Supply)

- BESS 결합과 수십 MW급 대용량 모듈러 UPS 수요가 증가함
 - 대규모 연산에 따른 순간적인 전력 스파이크 발생 시 즉각적으로 부하를 흡수하여 핵심 자원의 무중단 운영 및 설비 생존성 보장이 목적

➔ 전력망 병목 해소를 위한 온사이트 전력 생산

- AI 데이터센터는 지속적이고 안정적인 기저 부하를 요구하므로, 외부 전력망에 의존하지 않는 자체 마이크로그리드 시스템이 대두됨
- 대규모 전력 인입 지연 대응을 위해 SMR(소형 모듈 원자로), 천연가스 터빈, 수소 연료전지 기반 자가발전 연계 검토가 증가하는 추세임

바. 냉각 기술

➔ 액체 냉각(Liquid Cooling)의 필수화⁹⁾

- 공랭(Air Cooling)의 한계에 따라 D2C(Direct-to-Chip/Cold Plate) 냉각이 주류로 정착하고 있음
 - 발열이 심한 CPU 및 GPU 표면에 쿨드플레이트를 부착해 직접 냉각수를 순환시킴
 - ※ 공랭식 대비 전력 소비를 50% 이상 절감하며, 랙당 100kW 이상의 열 부하를 처리할 수 있어 최신 엔비디아 GB200 서버 등의 주력 냉각 방식으로 채택됨

8) Uptime Institute, Global Data Center Survey “Power and Resiliency Trends”/OCP, Open Rack v3 Power/DC Busbar Specification

9) ASHRAE TC 9.9, Liquid Cooling Guidelines for Datacom Equipment Centers

➔ 액침 냉각(Immersion Cooling)

- 서버 전체를 비전도성 절연 냉각액에 담가 열을 원천적으로 흡수하는 기술로 단상 및 2상 액침 냉각 방식이 있음
 - 팬이 필요 없어 소음이 없고, 냉각에 소모되는 전력을 90% 이상 획기적으로 줄여 데이터센터 전력사용효율(PUE)을 이론적 한계인 1.05 수준까지 낮출 수 있는 차세대 게임 체인저로 평가¹⁰⁾

➔ CDU(Cooling Distribution Unit) 다중화 및 폐열 회수

- 시스템 장애 시에도 냉각수가 지속 공급되도록 배관 및 펌프를 다중화(N+1)하고, 정밀 유량·온도 제어가 가능한 차세대 CDU 기술이 부상하고 있음
- 데이터센터 발생 온수(폐열)를 인근 지역난방/스마트팜으로 공급하는 열 회수 시스템 연계로 폐열의 재활용 기술도 등장함

사. 친환경·에너지 기술

➔ 핵심 지속가능성 지표 관리

- 막대한 수자원 낭비를 줄이기 위해 외부 보충수 공급이 필요 없는 ‘폐쇄형 순환 무수 냉각(Closed-loop Zero Water Cooling)’ 시스템 전환이 시도되고 있음
 - PUE(전력효율지수) 1.1 이하 목표, WUE(물사용효율) 0에 수렴하는 무수 냉각 시스템 및 CUE(탄소사용효율) 등 관리를 강화하고 있음¹¹⁾

➔ 24/7 무탄소 에너지(CFE, Carbon-Free Energy)

- 기존 RE100의 한계를 탈피하여, 시간 단위로 재생에너지와 전력 소비를 일치시키는 차세대 조달 표준 24/7 CFE 전력구매계약(PPA)으로 차별화를 추진 중¹²⁾

아. AI 데이터센터 운영·최적화 기술

➔ 디지털 트윈 및 지능형 DCIM

- AI 데이터센터와 동일한 가상 환경에서 AI 컴퓨팅 자율 운영, 열유체 및 전력 부하를 사전 예측, 대규모 장비 교체 시 물리적 위험 요소 사전 방지가 가능한 기술 도입
 - 센서 데이터를 기반으로 인프라의 디지털 트윈을 구축하고, AI 알고리즘을 통해 핫스팟(발열 집중 구간)을 사전에 감지하여 유량을 조절하는 예측 냉각 기술이 도입되어 물리적 장애를 예방함

10) OCP, Cooling Environments Project: Immersion Cooling and Cold Plate Requirements

11) The Green Grid, PUE, WUE, CUE Metrics and Guidelines

12) UN Sustainable Energy for All(<https://www.seforall.org/>), 24/7 Carbon-Free Energy Compact

⇒ AI 기반 전력·냉각 자동화 제어

- 시설 외부 환경 변수와 데이터 트래픽 폭증 양상을 실시간 학습하여, 개입 없이 최적의 냉각 인프라 가동률을 스스로 산출하는 자율형 제어가 가능함

⇒ 지능형 워크로드 오케스트레이션

- 개별 노드의 상태를 초 단위로 감시하여 연산 자원의 병목을 해소하고, 유휴 자원을 중요 임무에 즉각 재할당 처리를 위한 소프트웨어(Kubernetes/Slurm 등) 기반 분산 오케스트레이션 고도화는 필수적임

자. 보안 및 신뢰성 기술

⇒ 기밀 컴퓨팅(Confidential Computing) 및 RoT(Root of Trust)

- 하드웨어 기반 신뢰 실행 환경을 GPU 메모리로 확장하여 데이터 학습·추론 중 민감 데이터 유출 전면 통제 가능한 보호 기술
- 칩 부팅의 가장 첫 단계부터 하드웨어(RoT 칩)적으로 펌웨어를 검증하여, 외부로부터의 악의적인 백도어 삽입 및 변조 시도를 원천 봉쇄함

⇒ 네트워크 실시간 암호화(MACsec) 및 양자 내성 암호(PQC) 도입

- AI 데이터센터 간 트래픽 전송 시 하드웨어 가속을 통해 지연 없는 실시간 암호화를 수행하고, 미래 양자 컴퓨터의 해킹 위협까지 방어 가능한 최상위 보안망 구축을 지원함

⇒ 장애 예측 및 자율 복구

- 하드웨어 파손 전 발생하는 미세한 이상 징후를 선제 감지하여, GPU 통신 오류 발생 시 정상 노드로 워크로드를 자동 이관하는 무중단 방어 체계 확립 고려도 필수적임

4 글로벌 AI 데이터센터 산업 및 정책 동향

가. 글로벌 시장 및 산업 동향

⇒ 하이퍼스케일러 설비투자(CAPEX*) 폭발적 증가¹³⁾

* Capital Expenditures: 기업이 공장, 기계장치, 건물, IT 인프라, 소프트웨어 등 고정자산을 구매하거나 업그레이드하기 위한 지출

13) Synergy Research Group, Hyperscale Spending Spree ('25.12) / CBRE Investment Management, Data Centers: Ain't No Mountain High Enough ('26.2)

- 클라우드 선도 4사(Amazon, Microsoft, Google, Meta)를 중심으로 대규모 언어 모델(LLM) 학습 및 추론 인프라 확보 경쟁이 심화되고 있음
 - 글로벌 하이퍼스케일러들의 분기별 설비투자 규모가 2025년 1,400억 달러를 돌파하며 역대 최대치 경신
- 기존 일반 클라우드 워크로드용 데이터센터 비중은 축소되고, AI 전용 초고밀도 인프라(서버, 네트워크, 공간)를 선점하기 위한 10년 이상의 장기 임대 계약 및 포트폴리오 전환이 글로벌 시장 성장을 주도하고 있음

➔ GPUaaS(GPU-as-a-Service) 신흥 강자 부상 및 인프라 공급망 양극화

- 대규모 자본을 바탕으로 NVIDIA 최신 가속기(Blackwell 등)를 선제 확보하여 클라우드 형태로 전용 임대하는 코어위브, 람다 등 AI 특화 GPUaaS 기업들의 시장 점유율이 급속히 확대되고 있음
- 빅테크 기업들은 범용 GPU 확보 경쟁과 더불어, 엔비디아 의존도 탈피 및 인프라 구축 비용 절감을 위해 자체 설계한 맞춤형 AI 반도체 중심의 전용 인프라 확충을 병행하며 공급망을 재편 중임

➔ 전력망 제약 심화에 따른 입지 분산 및 신흥 거점 부상¹⁴⁾

- 북미 노던 버지니아(공실률 0.3%), 유럽 프랑크푸르트 등 기존 글로벌 Tier-1 데이터센터 허브의 극심한 송전망 포화로 인해, 신규 입지 선정 시 ‘네트워크 지연’보다 ‘전력 확보’가 최우선 기준으로 격상됨
- 부지 확보 후 전력을 끌어오던 방식에서 탈피하여, 풍부한 전력(원전, 재생에너지 등)과 확장 가능한 부지를 갖춘 중남미(케레타로 등), 아태지역(조호르, 바탐) 및 북미 외곽 지역(텍사스 서부 등)으로 대규모 자본이 선제 이동하며 신흥 허브를 형성 중임

➔ 인프라 후방 산업(전력 및 냉각 설비)의 메가 사이클 도래

- 랙당 전력 밀도의 급증(고집적화)으로 인해 글로벌 데이터센터 물리적 인프라(DCPI) 시장은 2030년까지 1,200억 달러 규모로 성장 전망(연평균 22% 성장)¹⁵⁾
- 단일 서버 단위를 넘어선 기반 인프라 수요 폭증으로 열 관리 부문이 가장 빠르게 성장 중이며, 액체 냉각 기술이 선택적 옵션을 넘어 신규 AI 인프라 구축의 필수 전제조건으로 자리매김

14) CBRE Research, Global Data Center Trends 2026('26.6)

15) Dell'Oro Group, Data Center Physical Infrastructure Forecast('26.8)

➔ 사모펀드(PE) 및 대체 자본의 AI 데이터센터 메가 펀드 투자 집중¹⁶⁾

- AI 인프라가 국가 필수 인프라이자 장기 수익이 보장되는 최우량 상업용 부동산 자산으로 부상하면서, 글로벌 사모펀드(Blackstone, KKR 등) 및 국부펀드 주도의 메가 펀드 조성을 통한 설비 직접 투자가 가속화되고 있음
- 전통적 부동산 자본의 AI 전력/공간 인프라 포트폴리오 재배치가 본격화 중임
※ 세계 최대 독립 데이터센터 운영사 QTS를 100억 달러에 인수한 Blackstone 社가 펜실베이니아 지역 데이터센터 및 전력망에 250억 달러를 투입

나. 주요국 정책 동향

➔ 미국

- (전력망 접속 규제 대폭 철폐) 미 연방에너지규제위원회(FERC)는 수년씩 걸리던 심사 절차를 최대 60~90일 이내로 단축하는 강력한 행정 조치를 단행¹⁷⁾
※ AI 팩토리의 전력망 연계 지연을 해소하기 위해 6대 권역 전력망 운영기관에 연방전력법 206조 기반 ‘소명 명령(Show Cause Order)’을 발동
- (세계 최대 원전 확장과 빅테크 동맹) 도널드 트럼프 정부의 원전 활성화 정책 (행정명령)과 맞물려, 빅테크와 원전 산업 간 대규모 자본 제휴가 본격화¹⁸⁾
 - 마이크로소프트는 스리마일 아일랜드 원전 1호기 재가동에 16억 달러를 투자해 20년 전력구매계약(PPA)을 체결함
 - 아마존(AWS)은 도미니언 에너지 인근 및 X-에너지 SMR에 5억 달러 이상을 투입하는 등 데이터센터의 민간 자체 전력 조달 생태계가 정립됨

➔ EU¹⁹⁾

- (AI Continent Plan 가동) 미국·중국 주도의 AI 패권에 대응하기 위해 2,000억 유로 규모의 단일 시장 최대 기술 프로젝트를 추진함
- (AI 팩토리 구축) 슈퍼컴퓨팅(EuroHPC) 인프라에 2만 개 이상의 GPU를 결합한 ‘AI 팩토리’를 역내 13개 지역에 거점화함
 - 이탈리아의 ‘IT4LIA’ 등이 대표적이며, 역내 스타트업과 연구기관에 컴퓨팅 자원과 데이터를 개방하여 유럽만의 독자적인 ‘소버린 AI’ 기반을 육성함

16) Blackstone Press Release, Digital and Energy Infrastructure Investment(‘25.7) / PitchBook, Private Equity Infrastructure Investment Report(‘26)

17) 임팩트온(<http://www.impacton.net/news/>), 美 FERC, AI 데이터센터 전력망 대란에 정책 전환(‘26.6)

18) 한국데이터경제신문(<https://www.dataeconomy.co.kr/news/>), AI 데이터센터 환경 오염 논란(‘26.5)

19) AI-BOOST meets AI factories(<https://aiboost-project.eu/>), The engine behind Europe’s AI-Continent strategy(‘25.8)

→ 영국²⁰⁾

- **(국가 중요 인프라(CNI) 격상)** 2024년부터 데이터센터를 전력·수도 등과 동일한 CNI로 지정하여 사이버 공격, 테러, 기후 재난으로부터 국가 차원의 보호망을 가동함
- **(AI Growth Zones 지정)** 데이터센터 신규 유치를 위해 간결한 인허가 패스트 트랙과 친환경 전력 우선 접속 혜택을 제공하는 ‘AI 성장 구역’을 신설하고, 국가 AI 연구 자원(AIRR) 용량을 ’30년까지 20배 이상 대폭 확장함

→ 중국²¹⁾

- **(동수서산(东数西算) 대규모 국책 사업)** 베이징, 상하이 등 동부 지역의 폭증하는 데이터를 에너지 리소스가 풍부하고 서늘한 서부 지역(구이저우, 닝샤, 간쑤, 네이멍구 등)으로 전송해 처리하는 인프라 분산 프로젝트를 가동함
 - 10개의 국가급 빅데이터 클러스터를 구축하여 전력 수급 불균형과 지연 문제를 동시 타개함
- **(자립형 칩 생태계와 컴퓨팅 바우처)** 미국의 첨단 칩 수출 통제에 맞서, 화웨이(Huawei), 캄브리콘 등 자국산 AI 반도체의 공공 조달을 의무화함
 - 또한 ‘컴퓨팅 바우처(算力券)’ 제도를 통해 기업의 자국 인프라 수요를 촉발시키며 폐쇄형 자체 생태계 고도화에 총력을 기울임

→ 일본²²⁾

- **(지방 분산 및 복원력 강화)** 도쿄·오사카 등 대도시에 집중된 인프라를 지진 등 자연재해 리스크로부터 분산시키기 위해 홋카이도 및 규슈 지역 거점화를 국가 차원에서 지원함
- **(소프트뱅크의 초거대 프로젝트)** 소프트뱅크는 최대 300억 엔의 정부 보조금을 바탕으로 홋카이도 도마코마이시에 내년 50MW를 시작으로 향후 최대 1GW까지 확장되는 일본 최대 규모의 자체 LLM 구동용 AI 데이터센터를 착공함

→ 싱가포르·중동 등 신흥 AI 데이터센터 허브

- 싱가포르는 협소한 국토와 전력난에도 불구하고, 2024년 예산에서 10억 달러(\$\$) 이상을 AI 컴퓨팅 지원에 투입²³⁾
 - 안정적인 규제 환경과 금융 허브 지위를 활용해 AWS(90억 달러), 구글(50억 달러) 등 빅테크로부터 수백억 달러 규모의 데이터센터 투자를 유치하며 아시아 최고 허브 지위를 공고히 함

20) 국회도서관 포털, Data centres : planning policy, sustainability, and resilience(‘25.8)

21) 한국통신학회 추계종합학술발표회, 중국 AI 반도체 발전요인과 정책적 시사점(IITP 이현재, ’25.11)

22) 요코하마 한국기업인 연합회(<https://yokokoba.org/>), 소프트뱅크, 홋카이도에 일본 최대 데이터센터 착공(‘25.8)

23) Introl Blog(<https://introl.com/>), 싱가포르의 270억 달러 AI 혁명이 2025년 동남아시아를 견인한다(‘25.8)

- UAE·사우디아라비아 등 중동 국가들은 풍부한 오일머니와 저렴한 전력을 무기로 데이터센터 및 AI 칩 구매에 약 3,000억 달러 규모의 투자를 기획함²⁴⁾
- 그러나 최근 이스라엘-이란 분쟁 등 중동 지역의 지정학적 무력 충돌로 데이터센터가 피격(바레인, UAE 등) 대상이 되면서 인프라 안보 리스크가 부각됨

〈 주요국 정책의 공통점과 차이점 〉

국가/지역	핵심 정책 및 전략 방향	주요 차별점
미국	민간 주도 확장, 전력망 규제 타파, SMR-데이터센터 융합	인프라 규제를 연방 차원에서 제거하며 시장 논리와 에너지 자본(원전)을 결합
EU	AI Continent Plan, 소버린 AI, 공공 'AI 팩토리' 구축	대규모 공공 자금 투입을 통한 역내 스타트업 보호 및 빅테크 종속 탈피 (하향식+상향식)
중국	'동수서산', 자립형 AI 반도체 생태계 강제 육성	철저한 국가 통제 및 지역(동/서) 분산 정책, 미국 제재 우회를 위한 강제 국산화
일본	재난 복원력(Resilience) 중심의 핫카이드/규슈 분산	정부 보조금 지급을 통한 지정학적 리스크 회피 및 로컬 LLM 생태계 구축 집중

출처 : 저자 작성

5 국내 AI 데이터센터 산업 및 정책 동향

가. 국내 데이터센터 산업 현황과 AI 전환

➡ 국내 데이터센터 폭발적 성장 및 상업용 시장 확대

- 국내 데이터센터는 '00년 52개소에서 '25년 182개소로 약 3.5배 급증하였으며, 현재 신규 구축이 구체적으로 추진 중인 부지만 72곳에 달함²⁵⁾
- 국내 상업용 민간 데이터센터 매출은 '24년 기준 6조 2,200억 원 규모이며, 대규모 AI 데이터센터 클러스터 사업이 본격화됨에 따라 '29년까지 연평균 12.4%의 고성장이 전망됨

➡ 초고밀도 AI 데이터센터 패러다임 전환 및 IT 전력 부하량 급증

- 기존 일반 클라우드 중심에서 대규모 언어 모델(LLM) 학습 및 추론에 특화된 하이퍼스케일 AI 전용 데이터센터로 수요가 급속히 재편됨
- 전체 IT 부하 용량은 '30년 6,320MW 규모로 폭증할 것으로 예측되며, 랙당 전력 요구량 역시 기존 10kW 이하에서 40~100kW 이상으로 고집적화되는 추세임

24) 매일경제(<https://www.mk.co.kr/news/>), "AI 허브의 꿈 날아갔다"…400조 투입 계획, 전쟁 포화에 묻힌 중동(26.3)

25) 한국데이터센터연합회(KDCC), KOREA DATA CENTER MARKET 2026~2029(26.8)



➔ 민간 AI 데이터센터의 수도권 극단적 편중 및 전력 수급 한계

- 네트워크 지연시간 최소화, 고객사 및 IT 인력 수급의 용이성 등으로 인해 현재 민간 데이터센터의 74.8%가 수도권에 밀집되어 있음
- 한국전력 송전망 포화로 수도권 신규 전력 연계가 대거 보류되면서, 전력망 쪼टा운 위험 해소 및 지방 분산이 업계 최대 화두로 대두됨

➔ 국내 IT장비·SW·솔루션의 외산 대비 큰 기술 격차와 낮은 국산화율

- 데이터센터의 두뇌인 IT 코어 부문의 평균 기술 수준은 2.0~2.5점(5점 만점)에 불과하며, 독자 제조 메인보드가 개발되어도 코어 칩셋 등 라이선스를 외산에 대부분 의존하고 있음²⁶⁾
 - 랙을 제외한 서버, 스토리지, 네트워크 장비의 국산화율은 1%~11.1%, DCIM/EMS·클러스터 SW·솔루션 등은 10~25% 수준임

나. 국가 AI 컴퓨팅 인프라 확충 정책

➔ 'AI G3' 글로벌 중추국가 도약 비전

- 대통령 주재 '국가인공지능위원회'를 중심으로 대한민국 AI 혁신 청사진인 「국가 AI전략 정책방향」을 수립함

➔ 범국가적 4대 AI 플래그십 프로젝트의 일환으로 국가 AI 컴퓨팅 인프라 대폭 확충

- AI 경쟁력의 근간이 되는 대규모 국가 AI 컴퓨팅 센터 구축, 민관 합작 투자를 통한 고성능 컴퓨팅 자원 대형화 및 집적화 지원을 제시함
- '27년까지 민간 부문 AI 투자 대폭 확대 유도를 위한 정부의 투자 활성화 환경 조성 및 산업계 전반의 자발적 AI 기술 및 인프라 투자 촉진 방안을 제시함

다. 국가 AI 컴퓨팅센터 추진 현황

➔ 민관 합작 운영 법인 '코아크(KOAK)' 설립 후 해남 솔라시도 인프라 착공²⁷⁾

- 공공 마중물과 민간 자본을 결합해 과기정통부, 국민성장펀드, 삼성SDS 컨소시엄 출자로 특수목적법인 출범
- 총사업비 약 2조 5천억 원이 투입되며, '28년까지 엔비디아 GPU 등 15,000장 규모를 집적해 1엑사플롭스(1EF) 이상의 연산 능력 확보를 목표로 함

26) 정보통신기획평가원(IITP), 국내 데이터센터 장비·SW 기술 경쟁력 분석('26.7)

27) 대한민국 정책브리핑, '국가 AI 컴퓨팅센터' 첫 삽...1만 5000장 규모·2028년 완공('26.08)

➔ 국산 반도체 생태계 조성

- 초기에는 첨단 글로벌 GPU 중심으로 서비스하되, 국산 AI 반도체의 개발·검증 과정을 거쳐 '30년까지 국산 칩 비중을 50% 수준으로 확대하여 자생적인 AI 반도체 생태계를 조성하고자 함

라. 대한민국 대도약, 메가프로젝트 'AI 데이터센터'

➔ 1,500조 원 규모의 초대형 메가프로젝트 및 AI 데이터센터 집중 육성²⁸⁾

- '26년 6월 정부는 '반도체, 퍼지컬 AI, AI 데이터센터'를 3대 축으로 하는 국가 전략 산업화를 위한 초대형 메가프로젝트를 발표
- 10년간 민간 투자 및 정부 인프라(전력·용수·인허가) 지원을 결합하여, AI 데이터센터 분야에만 550조 원의 대규모 자본을 집중할 계획임
 - SK, GS, 네이버 등 민간 3개 기업이 1단계 8.4GW, 장기적으로 '35년까지 총 18.4GW의 전례 없는 초대형 AI 데이터센터 클러스터를 권역별로 구축함

➔ 국내 AI 데이터센터 인프라 자체를 수출로 산업화

- 국내 기업의 고효율 냉각 기술, 전력 관리 솔루션, 국산 NPU 등 IT 장비 솔루션까지 모두 패키지화하여 글로벌 시장에 'AI 솔루션 및 데이터센터' 자체를 수출 동력으로 육성하는 청사진을 제시함

마. 국내 기업의 AI 데이터센터 투자 동향

➔ 통신사(SK, KT, LGU+ 등)와 IT 플랫폼(네이버, 카카오 등) 국내 기업들은 GPUaaS (서비스형 GPU) 확보 및 맞춤형 AI 모델 훈련을 위한 수천억 규모의 선제 투자를 집행

- (네이버) 글로벌 대체 투자사 Brookfield 등과 손잡고 약 10조 원 이상의 초대형 글로벌 AI 데이터센터 프로젝트 추진을 구상함²⁹⁾
- (SK에코플랜트 및 SKT) 엔비디아 등과 협력하여 전력 소모가 극심한 AI 워크로드를 감당할 대규모 AI 데이터센터 확장 및 울산 AI 데이터센터 프로젝트 등 인프라 고도화 추진³⁰⁾
- (삼성SDS) 엔트로픽과 기업용 AI 사업 협력을 확대하며, 국가 AI 컴퓨팅센터 구축 및 운영 역량 내재화를 추진 중

28) 삼일PwC, Q&A로 보는 '3대 메가프로젝트': AI, 기술을 넘어 국가성장 전략으로('26.7)

29) 연합뉴스, AI 데이터센터 판 키운다...네이버 14조·SKT 2GW 추진('26.7)

30) SK ecoplant Newsroom, AI 데이터센터 특별법 통과... AI 인프라 경쟁 본격화('26.5)

바. 지역별 AI 데이터센터 구축 및 입지 변화

→ 수도권 전력 포화에 따른 탈수도권 가속화

- 수도권의 송전망 부족으로 인해 신규 AI 데이터센터의 핵심 입지 기준이 '통신 지연시간'에서 '전력 수급 및 냉각 용수 확보'로 변모

→ 에너지 거점 중심의 신흥 AI 데이터센터 허브로 비수도권 지역의 부상

- 풍부한 재생에너지와 대규모 부지를 갖춘 서남권, 수열 에너지 활용 가능 및 기저 발전원 여유가 있는 강원권 등 에너지 접근성이 높은 비수도권으로 입지가 재편되고 있음

사. 전력·통신·에너지 정책과의 연계

→ 「인공지능 데이터센터 산업 진흥에 관한 특별법」 제정(2026.5)

- '27년 1분기 시행을 앞둔 AI 데이터센터 특별법은 AI 인프라를 국가 전략 자산으로 공식 인정하고 전력·입지 규제를 대폭 완화하는 내용을 포괄하고 있음

→ 비수도권 전력계통 영향평가 면제 특례

- 기존 「분산에너지 활성화 특별법」에 따라 대규모 전기사용시설(10MW 이상)에 의무화되어 1년 이상 지연을 초래하던 '전력계통 영향평가'를 비수도권 AI 데이터센터 신축·확장 시 전면 면제하여 지방 분산을 촉진함

→ 인허가 타임아웃제 및 일괄 처리 도입

- 과기정통부 장관으로 인허가 창구를 일원화하고, 관계기관이 일정 기간(40~150일) 내에 거부 통지하지 않으면 자동으로 인허가가 완료된 것으로 간주하는 '타임아웃제'를 신설함

→ 재생에너지 직접 전력구매계약(PPA) 특례 및 특구 지정

- 막대한 전력을 24시간 소모하는 AI 데이터센터의 특성을 고려하여, 한국전력을 거치지 않고 재생에너지로 생산한 전기를 사업자가 직접 공급받을 수 있는 PPA 제도 활성화의 법적 근거를 마련함
- 국가인공지능전략위원회의 심의를 거쳐 비수도권에 'AI 데이터센터 특구'를 지정하고, 기반시설(전력·용수·신재생설비)을 국가가 우선 지원할 수 있도록 제도화함

6 AI 데이터센터 확산을 둘러싼 주요 쟁점

가. 전력 확보와 전력망 병목(Grid Bottleneck)

⇒ 대규모 AI 데이터센터는 수십~수백 MW 이상의 상시 기저 전력을 요구하나, 지역 이기주의(NIMBY), 지중화 요구 등으로 인해 초고압 송배전망 건설의 극심한 지연이 계속될 수 있음³¹⁾

- 전기를 생산해도 송전 제약으로 전송하지 못하는 병목 현상은 AI 인프라 확충의 가장 치명적인 약점으로 작용함

나. 데이터센터 수도권 집중과 지역 분산의 한계

⇒ 분산에너지법 시행 이후 수도권 전력 계통 허가율이 2.1%에 불과한 상황에서, 규제(10MW)를 회피하기 위해 9.8MW 이하로 쪼개기 수전을 신청하는 등 제도적 사각지대와 편법이 등장하며 정책 실효성을 저해할 수 있음

⇒ 분산을 유도하여 비수도권 지역에 입지하더라도 해당 지역의 송전망이 부실하여 생산된 전력을 정상적으로 공급받지 못하거나, 핵심 IT 인력의 지방 근무 기피 현상이 겹쳐 실수요자들의 불만이 고조될 수 있음

다. 전기요금 및 계통비용 분담

⇒ 특정 지역에 초대형 부하가 신설됨에 따라 발생하는 막대한 송전선로 및 변전소 신설 비용(계통 보강 비용)을 원인 제공자인 데이터센터 사업자가 부담할 것인지, 아니면 한국전력과 일반 소비자가 분담할 것인지에 대한 사회적 비용 분담 갈등이 발생할 수 있음³²⁾

라. 용수·냉각·환경 문제

⇒ AI 데이터센터가 냉각탑을 통해 직접 증발시키는 물보다 해당 데이터센터의 전력을 생산하기 위해 발전소에서 소모하는 '간접 물 사용량'의 문제가 부각되고 있음³³⁾

⇒ SMR 1기(680MW) 가동에 매일 5,680만 리터(약 2만 3천 명의 일일 생활용수)의 물이 소모되는 등 수자원 고갈 및 농업 용수에 대한 갈등이 전망됨¹⁸⁾

31) 한국경제(<https://www.hankyung.com/>), AI 인프라 데이터센터, 수도권에 짓기 더 어려워진다('26.6)

32) 산업통상자원부, 데이터센터 수도권 집중 완화 방안('23.9)

33) 파이낸셜뉴스(<https://www.fnnews.com/news/>), AI 데이터센터, 수자원 고갈시키나('26.7)

- 세계적 기후변화로 식수가 고갈되는 가운데 데이터센터의 기하급수적 용수 소비는 향후 지역 농업 및 생활용수 배분 갈등의 뇌관으로 작용할 전망이다

마. 탄소중립과 AI 컴퓨팅 확대의 딜레마

- ⇒ 국내 기업의 RE100 달성 및 글로벌 ESG 규제 준수 목표가 연중무휴 전력을 소비하는 AI 인프라 확산과 정면으로 충돌하고 있음
- 간헐적인 태양광/풍력만으로는 데이터센터 가동이 불가능하므로 원전 기반의 무탄소 에너지(CFE) 도입 비중을 둘러싼 사회적 합의가 지연되고 있음

바. GPU 등 핵심 부품 공급망 병목 및 해외 기술·플랫폼 의존도

- ⇒ 엔비디아 GPU 및 고대역폭메모리(HBM) 등 필수 인프라 장비를 소수의 글로벌 독점 벤더에 의존하고 있어 비상 상황* 발생 시 국가 AI 연산망 전체가 마비될 수 있는 공급망 리스크를 안고 있음
- * 제품 조달 지연, 천문학적인 구축 단가 급등, 지정학적 무역 제재 발동 등
- ⇒ 하드웨어뿐 아니라 CUDA 플랫폼, 인피니밴드 네트워크 등 소프트웨어와 통신 프로토콜 전반이 해외 생태계에 종속되어 있어 국내 기업이 글로벌 경쟁에 주도권을 갖기 힘든 진입 장벽으로 작용하고 있음
- ⇒ 군사, 금융, 공공 데이터 등 민감 정보를 다루는 파운데이션 모델을 훈련할 때 외산 인프라에 의존할 경우 데이터 유출 및 주권 침해 소지가 존재함
- 폐쇄된 국경 내에서 구동되는 완벽한 ‘소버린 AI 인프라’ 확보 역량이 안보와 직결되어 있음

아. 투자 과열 및 사업성 문제

- ⇒ 천문학적 설비투자(CAPEX) 대비 수익화 지연 및 수요 격차
- 글로벌 빅테크의 AI 인프라 투자 규모가 수천억 달러로 폭증했으나, 실제 AI 서비스로 회수되는 누적 매출은 투자액의 일부에 불과하여 ‘수요-수익 격차’가 심화될 수 있음
- 차세대 AI 주도권 경쟁에서 도태될 것을 우려한 기업 간 ‘죄수의 딜레마’ 식 방어적 과잉 투자가 지속됨에 따라, 단기 투자 대비 수익률(ROI)에 대한 회의론이 확산되고 있음³⁴⁾

34) International Banker, AI's Capital-Spending Boom: Sustainable Investment or Emerging Bubble?(26.8)

➔ **초고가 GPU의 짧은 수명주기 및 감가상각에 따른 재무 리스크**

- 데이터센터는 통상 7~15년의 장기 투자 회수 기간을 전제로 대규모 부채 (Private Credit 등)를 조달하나, 핵심 자산인 AI 가속기(GPU/NPU)의 유효 경제 수명은 1~2년에 불과함
- 차세대 칩셋의 빠른 출시로 기존 하드웨어의 자산 가치가 급격히 하락(기술적 진부화)함에 따라, 담보 가치 하락 및 금융 연계 리스크로 전이될 우려가 있음³⁵⁾

➔ **전력·냉각 중심의 막대한 운영비(OPEX) 부담 및 좌초 자산(Stranded Asset) 위험**

- 초고밀도 전력 소모와 특수 냉각(액체/액침 냉각) 설비 도입으로 인해 초기 건축비뿐만 아니라 지속적인 유지·운영비가 기하급수적으로 증가함
- 장기 입주사나 전력구매계약(PPA)을 사전에 확정 짓지 않은 ‘투기적 데이터 센터’의 경우, 향후 투자 열기 둔화 시 전력망만 잠식하는 적자 자산으로 전락할 위험이 있음³⁶⁾

7 결론 및 정책적 시사점

가. AI 데이터센터, AI 인프라 생태계 경쟁으로의 전환

➔ **컴퓨팅 주권 및 ‘클러스터(집적) 효과’의 핵심 기반 시설**

- AI 데이터센터는 우수 인재와 자본, 혁신 기업을 집중시키는 구심점 역할을 하는 핵심 안보 자산이자, 국가의 디지털 영토를 결정짓는 중추 시설임

➔ **범정부 차원의 거시적 접근 필요**

- 주요국의 대규모 AI 인프라 투자에 대응하여, 단순 물리적 설비 확충을 넘어 전력·통신·데이터 안보를 포괄하는 인프라 생태계 전반의 경쟁력 확보가 필수적임

나. 반도체-IT장비-전력/냉각-AI를 망라한 통합 국가 전략 추진

➔ **첨단 기술 융합의 집결지**

- 국산 NPU, 고대역폭메모리(HBM), DPU, 초저지연 네트워크 인프라, 고효율 전력·액체 냉각 설비 등 가치사슬 전반의 융합 경쟁력을 선점해야 함

35) Man Group Insights, The AI Bubble: Hidden Risks and Opportunities('26.2)

36) KKR Global Macro & Asset Allocation, Beyond the Bubble: Why AI Infrastructure Will Compound('25.11)/Digital Infrastructure, Data centre infrastructure investment - AI bubble, boom or bust?('26)

➔ 통합 컨트롤타워 및 기술 실증 지원

- 현재 외산 의존도가 높은 국내 IT 장비 및 운영 소프트웨어(DCIM 등)의 자립도를 높이기 위해, 부처 간 협력 체계 구축이 필요
- 메가프로젝트의 대한민국 AI 데이터센터가 인프라 기술의 성능 검증과 레퍼런스 구축 사이트로 적극 활용되어야 함

다. 국내 AI 데이터센터 산업 생태계 육성 및 수출 산업화

➔ 국내 기술력 기반의 칩·장비 생태계 조성

- AI 데이터센터 필수 인프라 장비의 소수 글로벌 벤더 독점에 따른 공급망 리스크(조달 지연, 단가 급등 등) 완화를 위해, 국가 컴퓨팅 시설 내 국산 AI 칩 및 솔루션 도입 비중을 점진적으로 확대해야 함

➔ “AI 데이터센터 코리아 패키지” 수출 동력화

- 국내 우위 기술인 첨단 메모리, 고효율 냉각 기술, 전력 관리 솔루션에 NPU, DPU, CXL 등의 국산 기술력을 접목한 IT 장비·SW 솔루션까지 풀 패키지화 하여 신흥 글로벌 거점을 겨냥한 신규 수출 모델로 육성할 필요가 있음

라. 전력망 제약 극복을 위한 지역 분산형 인프라 구축

➔ 수도권 전력 포화 대응 및 입지 분산

- 민간 데이터센터의 70% 이상이 수도권에 편중된 바, 전력계통 영향평가 면제 등 특별법의 제도적 특례를 활용해 재생에너지 및 기저 발전 여유가 있는 비수도권으로 입지를 신속히 재편해야 함

➔ 지역 특화 AI 클러스터 연계 및 인센티브 강화

- 단순한 시설 이전을 넘어 지역 핵심 산업과 연계된 특화 거점을 조성하고, 입주 기업 및 필수 IT 인재의 자발적 이전을 유도할 수 있는 실효적 혜택(세제, 정주 여건 등)을 병행해야 함

마. 지속가능한 AI 데이터센터 정책 이행 방안 마련

➔ 친환경·고효율 에너지 체계 확립

- 막대한 수자원 고갈 우려를 불식시키기 위해 폐쇄형 무수 냉각 시스템 전환을 독려하고, 무탄소 에너지(CFE) 중심의 전력 공급 체계 연계를 강화해야 함

➔ 지역 상생 모델 및 인프라 비용 분담

- 데이터센터 발생 폐열의 지역사회(스마트팜, 난방 등) 재활용을 장려하여 주민 수용성을 높이고, 대규모 송배전망 신설에 따른 계통 보강 비용의 합리적 분담 기준을 확립하여 사회적 갈등을 최소화해야 함

마. 데이터 주권 보호 및 과잉 투자 리스크 선제 관리

➔ 소버린 AI(Sovereign AI) 인프라 확보

- 공공·민감 데이터의 해외 플랫폼 종속 및 외부 유출 리스크를 차단하기 위해, 독자적인 데이터 주권을 보장하는 폐쇄형 인프라 환경 조성이 선결되어야 함

➔ 재무적 지속가능성 검증 (좌초 자산 방지)

- 초고가 GPU의 짧은 교체 주기(1~2년)와 인프라 장기 회수 기간(7~15년) 간의 괴리로 인한 재무 리스크를 방지하고자, 철저한 수요 예측과 유연한 인프라 확장 모델을 채택하여 투기성 적자 자산으로의 전락을 방지해야 함



주요 동향(1) : 과학기술

1 CSIS, RAM 공급난이 미국에 미치는 영향을 검토한 보고서를 발표

➔ 미국 전략국제연구센터(CSIS)는 메모리(RAM) 공급난의 원인과 영향을 분석하고, 미국 경제와 AI 경쟁력에 미치는 함의를 고찰해 제시*('26.7)

* The United States' Accelerating Memory Chip Crunch: Implications for Tech and AI Leadership

※ 본 고는 CSIS 내부 연구부서 소속인 로린 윌리엄스(Laurnyn Williams)의 견해를 CISI가 인터뷰 형식으로 정리해 공개한 자료를 바탕으로 작성

- (개요) RAM 공급 부족 사태인 '램마겟돈*'의 원인과 기술 생태계의 영향, 잠재적 해결 방안에 대한 여러 논의들, 미국 경제와 AI 리더십에 미칠 함의 등을 정리

* RAMageddon: 데이터센터 등 AI 인프라 확대로 RAM 수요가 폭발적으로 급증하면서 발생하는 심각한 RAM 부족 사태를 대재앙을 뜻하는 '아마겟돈'에 빗대어 이르는 신조어

- (RAM 부족 현상) HBM 수요 증가로 인해 일반 소비자용 DRAM 공급이 크게 감소하고 있으나 단기간에 메모리 생산능력을 확대하는 것은 불가능

- (원인) 미국 내 AI 데이터센터 건설 붐으로 AI 연산에 필요한 HBM 수요가 급증하고, 메모리 제조업체들이 수익성이 높은 HBM 생산을 우선시하면서 범용 메모리인 DRAM의 공급 부족과 가격 상승이 가속화

※ 일각에서는 '26년 전체 생산 메모리의 50~70%가 데이터센터에서 소비될 것으로 추산

〈 메모리 유형 분류 〉

구분	주요 내용
DRAM (Dynamic Random Access Memory)	• 노트북, PC, 스마트폰 등 소비자 전자제품에 널리 사용되는 범용 메모리 • DRAM 가격은 역사적으로 하락세였으나 최근 공급 부족으로 가격이 상승
HBM (High Bandwidth Memory)	• 여러 DRAM 칩을 수직으로 적층해 높은 대역폭 및 에너지 효율을 구현 • AI 데이터센터와 고성능 컴퓨팅에 주로 사용
NAND flash memory	• 전원 없이도 데이터를 유지하는 비휘발성 메모리 • 스마트폰 저장장치, 솔리드 스테이트 드라이브(SSD) 등에 활용

- (제품 가격 압박) 기업들이 증가한 메모리 비용을 제품 가격에 반영하면서 소비자용 메모리 시장의 위기를 의미하는 '램마겟돈'이 이슈로 부상
- RAM 가격 상승으로 높은 수익을 기대할 수 있는 메모리 제조업체나, AI 인프라에 막대한 투자를 유지하면서 HBM에 대한 우선적인 접근권을 확보한 하이퍼스케일러들은 '램마겟돈' 속에서 유리한 입지를 확보

※ 구글, 아마존, 마이크로소프트, 메타와 같은 하이퍼스케일러들은 각각 1,000억 달러 이상을 AI 인프라에 투자하고 있는 것으로 알려짐

- 반면, PC·스마트폰 등 소비자 제품 제조업체들은 제품 원가의 최대 30%를 차지하는 DRAM 가격 상승으로 인해 잇따라 최종 제품 가격 인상을 발표
 - 통신장비·자동차·의료기기 산업도 생산 비용 증가에 직면
 - ※ 델(Dell)은 '25년 12월부터 개인용 컴퓨터 가격을 15~20% 인상하기 시작했고, 레노버(Lenovo)는 노트북 가격 인상을 예고했으며, '26년 6월 애플(Apple)은 메모리 대란으로 인해 아이폰 가격 인상이 불가피하다고 발표
 - **(단기 해결 어려움)** 미국은 메모리 생산을 한국의 삼성전자와 SK하이닉스, 미국 마이크론 등 3개 회사에 의존하고 있으나 이들 모두 당장 생산능력을 확대하기는 어려워 공급 부족을 완화하기까지는 수년의 시간이 필요할 전망
 - ※ 마이크론이 미국 아이다호에 건설 중인 2개의 생산시설은 '27년 이후에 가동될 전망이며, SK하이닉스와 삼성전자도 한국에 대규모 신규 생산시설 건설을 추진하고는 있으나 실제 가동까지는 오랜 시간이 걸릴 것으로 예상
 - **(공급난 영향)** 메모리 가격 상승은 전자제품 가격 상승을 견인할 뿐만 아니라 공급망 붕괴와 PC·노트북 수요 감소 등으로 이어질 가능성이 존재
 - 미국 전자제품 분야 9개 협단체는 “메모리 칩 시장의 불균형으로 인해 가격이 급상승하고 핵심 공급망이 붕괴될 수 있다”고 경고
 - ※ The Internet & Television Association, America's Communications Association, The Rural Broadband Association 등 9개 단체가 스콧 베센트(Scott Bessent) 재무장관과 하워드 러트닉(Howard Lutnick) 상무장관에 서한을 전달
 - 이들 단체는 이미 다양한 소비자 제품 및 IT 제품 가격 상승, 인터넷 및 통신 비용 증가, 자동차·의료기기 제조 지연 등 여러 문제가 발생하고 있다고 주장
 - 버니 모레노(Bernie Moreno) 오하이오주 상원의원도 러트닉 상무장관에 서한을 보내 트럼프 행정부가 마이크론, SK하이닉스, 삼성전자와의 협상에서 미국 내 RAM 수요 충족을 우선시해야 한다고 강조
 - 한편, 메모리 부족으로 인한 가격 상승의 영향으로 '27년까지 AI PC 보급이 지연되고 장기적으로 전자제품 교체 수요가 위축될 것으로 전망
 - **(잠재적 해결 방안)** 산업계는 메모리 공급난을 해결하기 위해 연방정부 차원의 개입과 중국산 메모리를 제한적으로 허용해줄 것을 촉구
 - 9개 협단체는 재무부·상무부에 ▲미국·동맹국 메모리 생산능력 확대 ▲무역 협정을 통한 공급망 안정화 ▲소비자 전자제품에 메모리 물량 우선 배분 ▲반도체법* 자금 지원 구조 개편·활용 ▲글로벌 공급 규제 장벽 완화 등을 촉구
- * CHIPS Act: 미국의 반도체 산업 지원법으로, 미국 내 반도체 제조시설 건설을 촉진하기 위해 직접 보조금을 지원하고 세액 공제 등 혜택을 제공하는 것이 골자



- 또한 애플 등 일부 기업들은 민감도가 낮은 소비자용 제품에 한하여 중국산 메모리를 제한적으로 사용할 수 있도록 허용해 줄 것을 제안
 - ※ 중국을 대표하는 DRAM 기업인 창신메모리(CXMT)와 NAND 플래시 기업인 양쯔메모리(YMTC)는 미국의 대(對)중국 수출통제 및 국가 안보 관련 제재 대상으로 지정된 상태
- 메모리 부족 문제를 해결하면서도 미국의 국가 안보 및 공급망 우려를 완화할 방법으로 중국산 메모리를 탑재한 제품은 중국에서만 판매되도록 제한하는 방안도 제안된 상황
- 다만 전문가들은 이러한 제안이 미국의 경제·안보에 미칠 장단점과 영향을 완전히 이해하기 위해서는 상당한 추가 비용 편익 분석이 필요하다고 지적
- **(AI 경쟁력에 미치는 함의)** 메모리 부족 사태는 미국의 AI 리더십과 중국과의 기술 경쟁에 관한 광범위한 전략적 과제를 강조
 - 미국은 AI 칩 설계와 클라우드 컴퓨팅 분야에 강점을 보유하고 있으나, 메모리 생산능력은 제한적
 - ※ 미국 내 유일한 주요 메모리 칩 제조사 마이크론의 미국 내 생산 비중은 전체의 2% 미만
 - 한국 SK하이닉스와 삼성전자는 신뢰할 수 있는 메모리 공급원이지만, 메모리 공급이 소수 기업과 특정 지역에 집중돼 있다는 점에서 공급망 취약성이 존재
 - 결국 메모리 부족 사태는 미국의 AI 리더십이 지정학적 약점이 많은 글로벌 공급망에 얼마나 크게 의존하고 있는지를 드러내는 계기로 작용
 - 또한 메모리 부족은 미국이 중국과의 AI 경쟁에서 필요한 컴퓨팅 능력을 확보하는 데 차질을 초래하고 미국의 우위를 약화시키는 요인이 될 것이라는 전망
 - 다만 이러한 영향이 가시화되기 전에 미국 경제가 우선적으로 타격을 입을 것으로 전망되며, 대기업을 제외한 경제 전반에서 AI 기술 발전에 대한 공평한 접근권이 저해될 것으로 예상

출처 : 미국 전략국제연구센터(CSIS) (2026.7.31.)

<https://www.csis.org/analysis/united-states-accelerating-memory-chip-crunch-implications-tech-and-ai-leadership>

2 미국 CFDI, 'AI 모델 탈취 방지 법안(DAAMTA)' 개선 의견 제안

➔ 미국 데이터혁신센터(CFDI)는 폐쇄형(closed-source) AI 모델 도용을 막기 위해 발의된 'AI 모델 탈취 방지 법안(DAAMTA*)'에 대한 개선 의견을 제안**('26.5)

* Detering American AI Model Theft Act of 2026

** How to Fix the AI Model Theft Bill Before It Becomes Law

- (DAAMTA 개요) DAAMTA는 적대국들이 미국의 최첨단 폐쇄형 AI 모델을 불법 추출·탈취하는 행위를 막기 위한 법안으로, '26년 4월 하원에서 발의
- (배경) 최근 오픈AI, 구글, 앤트로픽 등 미국의 주요 AI 기업들은 중국 정부의 지원을 받는 기업들로부터 일명 '적대적 증류(Adversarial AI Distillation)*' 공격에 노출되었다고 보고
- * 첨단 AI 모델에서 모델 가중치, 아키텍처, 기타 기술적 특성과 같은 핵심 데이터를 체계적으로 추출·탈취하여 저렴하게 자체 모델을 학습시키는 행위
- (목적) 중국, 러시아와 같은 적대국들이 미국의 첨단 AI 모델을 무단 추출하거나 학습하는 행위를 국가 안보 및 미국 기업의 경제적 경쟁력에 대한 위협으로 간주하고 이에 대응하기 위해 발의
- (주요 내용) 미국 AI 모델에 대한 추출 공격 평가를 의무화하고, 공격을 수행했거나 그러한 행위와 관련된 실체를 식별해 목록으로 관리하는 것이 골자

〈 DAAMTA 주요 내용 〉

구분	주요 내용
AI 모델 추출 공격 (model extraction attack)의 정의	• AI 모델을 복제·개발·훈련·개선하기 위해 폐쇄형 AI 모델(소유자가 복제·재현에 필요한 기본 정보를 공개하지 않는 모델)의 기능을 무단으로 추출하는 행위로 정의하고, 그 예시로 다음을 제시 - 모델 소유자가 구현한 ▲기술적·계약적 제약 및 기타 접근제어 ▲신원확인 요건 ▲지리적 접근 제한 등을 우회하거나, - 사기, 허위진술, 무단 접근을 통해 질의를 수행하거나, - 소유자·제공자가 정한 약관·조건·제한을 위반하는 경우 등
AI 모델 추출 공격 및 사기성 계정 네트워크 제공업체에 대한 평가 의무	• 미국 행정부에 동 법이 제정된 날로부터 180일 이내에 미국의 첨단 AI 모델을 대상으로 정보 추출 공격을 수행했거나 현재 공격을 수행 중인 '우려 기관*'과 '사기 계정 네트워크 제공자**'를 식별·파악할 것을 의무화 * Entity of Concern: 우려 대상 국가에서 활동하거나 본사가 위치하거나, 최종 모회사의 본사가 우려 대상 국가에 있거나, 우려 대상 국가에 본사를 두고 있는 법인의 지사·통제 하에 운영되거나, 미국인 소유의 폐쇄형 AI 모델에 대해 추출 공격을 시도·수행하는 실체(기관이나 개인) ** Fraudulent Account Network Provider: 미국의 폐쇄형 AI 모델에 접근할 수 있는 계정을 고의적·의도적으로 생성·획득·유지·판매·중개 또는 기타 방식으로 제공하는 모든 외국 법인 - 특히, 'AI 모델 추출 공격자 목록' 작성·관리 의무를 도입

구분	주요 내용
	- 평가 활동에 다음 사항들이 포함되도록 규정 - 공격 행위자들의 국적 식별 결과 - 해당 국가 정부의 물질적 지원 내용 - 주요 공격 기법과 사기성 계정 네트워크 제공자의 역할·위치 - 공격 탐지를 위한 다양한 접근방식의 장단점 검토 내용 - 공격의 경제·안보 상의 영향 - 미국 정부가 모델 소유자에게 제공하는 지원 - 공격 탐지·예방을 위해 동맹국·파트너를 활용하는 외교 전략 등
공격 예방·대응을 위한 모범사례 개발 및 정보 공유 메커니즘 구축 의무	- AI 모델 추출 공격의 표적이 되거나 피해를 입은 폐쇄형 AI 모델 소유자(자발적 참여 기반), 기타 기업, 학계 전문가, 산업 포럼 및 단체 등과 협의해 ▲공격 행동 패턴 및 방법 식별 ▲모델 추출 공격 방어를 위한 모범사례 개발 ▲사기 계정 네트워크 제공자의 활동을 식별할 수 있는 모범사례 개발 등을 수행할 것을 요구 - 동 법이 제정된 날로부터 210일 이내에 모델 추출 공격을 탐지·예방·대응하기 위한 모범사례 보고서 발표 의무를 명시 - 폐쇄형 AI 모델 소유자가 모델 추출 공격 및 사기 계정 네트워크 제공자에 대한 정보를 연방정부와 자발적이고 신속하게 기밀로 공유할 수 있도록 정보 공유 메커니즘을 구축할 것을 요구
제재	우려 기관에 대해 미국 내 재산 및 재산상 이익에 관련된 모든 거래를 차단·금지할 수 있음을 명시

● (개선 의견) 미셸 말도나도(Michelle Maldonado) CFDI AI 정책부장은 DAAMTA 제정을 지지하면서도, 실효성을 위해 개선이 필요하다고 제언

- 컴퓨터 사기 및 남용 방지법(CFAA*), 영업비밀 방어법(DTSA**) 등 기존의 법률에는 한계가 있어, DAAMTA가 좋은 입법적 수단이 될 수 있다고 평가

* Computer Fraud and Abuse Act: 권한 없이 컴퓨터 시스템에 접근하거나 정보를 탈취·파괴하는 행위를 처벌하고 민사상 손해배상을 청구할 수 있도록 규정한 미국 연방법

** Defend Trade Secrets Act: 영업비밀 절도 행위에 대해 금전적 손해배상 등을 위한 민사 소송을 제기할 수 있도록 규정한 미국 연방법

- 다만 ▲‘모델 추출’에 대한 광범위한 정의 문제 해결 ▲공격자 식별에 관한 증거 기반 확충 ▲오픈소스 AI 개발 및 보안 연구에 대한 보호 추가 ▲조화로운 법적 기반 마련 등을 통해 DAAMTA의 허점을 보완해야 한다고 권고

〈 DAAMTA 개선 방향에 대한 제언 〉

구분	주요 내용
‘모델 추출’ 정의와 관련된 문제 해결	- DAAMTA는 모델 추출 공격 행위를 ‘AI 모델 소유자·제공자의 서비스 약관 위반’을 포함해 지나치게 광범위하게 정의 - 약관은 기업과 사용자 간 사적 계약으로 공법이 아니므로, 정부 제재가 기업의 서비스 약관 위반 여부에 좌우되는 것은 바람직하지 않음 - 따라서 고의적인 계정 사기와 체계적인 모델 기능 추출 시도를 결합한 행위를 겨냥하도록 정의를 수정하는 것이 바람직

구분	주요 내용
AI 모델 추출 공격자 목록 작성과 관련해 공격자 식별 증거 확충	• DAAMTA는 AI 모델 추출에 참여한 기관을 식별해 목록을 공개하도록 규정하고 있는데, 이처럼 공개적인 지정이 AI 기업의 신고에만 의존하게 될 가능성이 높음 • 불투명한 증거를 기반으로 한 지정은 절차상 적법성 문제, 오류로 인한 기업 피해 가능성, 국제 분쟁 등을 초래할 수 있으므로 각 지정에 대한 증거 요건을 강화할 수 있는 방안을 검토
오픈소스 AI 개발과 보안 연구에 대한 보호 장치 추가	• DAAMTA는 ‘폐쇄형 AI 모델’을 주요 대상으로 주요 위험을 적절히 겨냥하고 있으나, 향후 정치적 압력 등으로 인해 규제 범위가 오픈소스 AI 및 연구 활동으로 확대될 위험이 존재 • 오픈소스 AI 개발, 학술연구, 합법적인 보안 테스트 활동을 보호할 수 있는 명확한 법적 안전장치를 추가하는 것이 바람직
정부의 자체 AI 개발 관행에 부합하는 조화로운 법적 기반 마련	• 정부가 적법하게 구매한 모델을 활용해 자체 모델을 개발하는 것은 사기 계정을 만들고 접근통제를 우회해 모델을 추출하는 행위와 본질적으로 다르지만, 이러한 구분을 법률에 명확히 반영해야 할 필요성이 존재

- 또한 다음과 같은 보다 광범위한 노력을 통해 AI 보안을 강화할 것을 촉구

〈 AI 보안 강화 조치에 대한 제언 〉

구분	주요 내용
DAAMTA 보완	• 개선 의견을 반영해 DAAMTA를 발전시킴으로써 법적 실효성을 강화
강력한 기술적 방어 체계에 대한 투자	• 미국 국립표준기술연구소(NIST)와 산하 기관인 인공지능 표준혁신센터(CAISI)를 통해 모델 추출 행위 탐지, 악용가능한 API 사용 제한, 포렌식 분석 등을 지원하는 표준 개발을 추진
동맹국과 협력해 AI 모델 탈취에 대한 공동 규범 수립	• 동맹국들과 협력해 중국 등 특정 국가가 지원하는 AI 모델 탈취 행위에 대한 공동 규범을 확립 • 영국, 일본, 캐나다, 프랑스 등 AI 산업 선도국들과 공동 대응을 추진해 미국의 정책적 영향력을 확대하고 모델 도용에 대한 제재 효과를 확대
기술 자체에 대한 규제 지양	• 유해 행위를 규제하는 데 초점을 맞추되, AI 기술 자체를 규제하지 않도록 주의함으로써 미국의 안보와 혁신을 보호

출처 : 미국 데이터혁신센터(CFDI) (2026.7.28.)

<https://datainnovation.org/2026/07/how-to-fix-the-ai-model-theft-bill-before-it>
<https://www.justsecurity.org/137498/diagnosis-deterrence-us-response-distillation/>

3 일본 CRDS, 미션지향형 과학기술혁신(STI) 정책 강화 방안 제언

⇒ 일본과학기술진흥기구(JST) 산하 연구개발전략센터(CRDS)는 일본에서 미션지향형 과학기술혁신(STI) 정책 실행을 강화할 수 있는 방안을 제안하는 보고서*를 공개(‘26.6)

* 日本におけるミッション志向型STI政策の実装強化 - 中核機能と地域ミッション -

- (개요) 미션지향형 STI 정책의 개념을 설명하고, 국제적 경험을 기반으로 관련 과제를 검토한 후, 일본에서 그 실행을 강화할 수 있는 방안들을 권고
 - 법적 구속력을 갖는 정책 문서는 아니지만, 향후 일본의 STI 정책 설계 및 집행에 영향을 줄 수 있는 전략 제안 문서
 - 미션지향형 STI 정책 실행을 강화하기 위한 방안으로 새로운 미션을 다수 설정하기보다는 이미 추진 중인 장기 STI 전략과 연구개발 사업이 사회변혁으로 이어질 수 있도록 지원·관리 체계를 구축할 것을 강조
 - CRDS는 이러한 조치를 통해 사회적 과제를 신속히 해결할 뿐만 아니라 전 세계에 일본의 정책 모델을 혁신 사례로 제시할 수 있을 것으로 기대
- (개념) 미션지향형 STI 정책은 사회적 난제 해결을 위해 명확하고 측정 가능한 목표(미션)를 설정하고, 이에 맞춰 연구개발, 규제, 재정 지원, 사회적 구현을 위한 시책을 종합적으로 동원하는 정책 접근법을 의미
 - ‘탄소중립 달성’, ‘지속가능한 사회 전환’ 등 단일한 기술혁신이나 연구개발 투자만으로는 해결이 어려운, 복잡하고 광범위하며 장기적 대처가 필요한 거대한 사회적 과제를 해결하기 위한 방안으로 대두
 - ’00년대 후반부터 STI 정책이 점차 사회적 과제를 직접 해결하는 방향으로 전환되면서 국제적으로 미션지향형 STI 정책이 주목받기 시작

〈 OECD 국가들의 미션지향형 STI 정책 사례 〉

구분	미션지향형 STI 정책 이니셔티브
EU	• EU Missions
오스트리아	• Austrian European Union missions • BMK Missions
벨기에	• Smart Specialisation Strategy Wallonia • Circular Economy Flanders
체코	• Smart Specialisation Strategy missions
덴마크	• Innomissions
핀란드	• Business Finland missions • The Research Council of Finland's Flagship Programmes

구분	미션지향형 STI 정책 이니셔티브
프랑스	• National Acceleration Strategies
독일	• Future Research and Innovation Strategy's Missions
아일랜드	• Research Ireland's National Challenge Fund
리투아니아	• Instrument for Mission-based Science and Innovation
네덜란드	• Mission Driven Top-Sector Policy
노르웨이	• Norway National Missions • Pilot-E
스페인 카탈루냐	• Smart Specialisation Strategy in Catalonia 2030 (RIS3CAT)
스웨덴	• Impact Innovation
영국	• Camden Council Missions • UKRI Challenge Fund • UK Quantum Missions
캐나다	• National Research Council Canada Challenge Programs
미국	• Energy Earthshots
브라질	• FNDCT Structuring and Mobilizing Programs
호주	• Commonwealth Scientific and Industrial Research Organisation (CSIRO) missions
한국	• The Alchemist program • National Strategic Technology Policy • Comprehensive Plan to Solve Social Problems Based on Science and Technology
일본	• Strategic Innovation Promotion Program(SIP)

- **(한계·과제)** 세계 각지에서 다양한 미션지향형 STI 정책이 시행되어왔으나, OECD의 분석에 따르면 미션지향형 STI 정책에는 ‘3가지 함정’이 존재
 - ※ OECD는 세계 각국의 넷제로 미션 관련 대처 사례 101건을 분석하고, 그 결과를 정리한 보고서(Mission-Oriented Innovation Policies for Net Zero, '24.11.22. 발표)에서 미션지향형 STI 정책의 함정을 3가지로 구분해 설명
 - **(STI 중시 함정(STI only trap))** 기술혁신만 강조함으로써 정책이 기존의 STI 정책 틀에서만 머물고 산업·환경·교통·복지 등 분야별 정책이나 실제 현장과는 연결되지 않는 문제를 의미
 - **(방향 설정 중시 함정(Orientation only trap))** 미션이 설정되어도 구체적인 실행계획이 미비해 실제 대처가 이뤄지지 않는 문제와 관련
 - **(정책 중시 함정(Policy only trap))** 정부가 관련 사업을 주도하고 있으나 민간 부문에서 폭넓은 참여와 자원을 이끌어내지 못하는 한계를 의미
- **(방안)** CRDS는 일본에서 미션지향형 STI 정책 실행을 강화하기 위한 방안으로
 - ▲중핵 기능* 구축 ▲지역 미션 구체화의 2가지 조치를 제안
 - * 중핵 기능이란 특정 기관이라기보다는 여러 주체가 같은 목표를 향해 움직일 수 있도록 정보를 제공하고, 조정하며, 전문 역량을 축적하는 지원 체계를 의미



1. 중핵 기능 구축

- 먼저, 미션 설정이나 이를 근거로 한 국가·지역 수준에서의 정책 입안·실천에 병목 현상이 나타나지 않도록 국가 및 지역적 노력을 촉진·지원하는 중핵 기능을 구축할 것을 권고
- 중핵 기능은 다음 3가지 세부 기능으로 구성:
 - (정보 및 기술 지원 기능) 미션 설정 및 로드맵 개발을 지원
 - (정보 수집 및 분석 기능) STI 동향과 정책·사업 진행 상황을 모니터링·분석
 - (역량 강화 기능) 장기적 정책 추진에 필요한 인력·데이터·평가도구·네트워크를 지속적으로 축적
- CRDS는 이러한 기능들을 통해 정책 설계에서부터 연구개발, 테스트, 사회적 적용까지 일련의 과정이 이어질 수 있도록 지원하고, 국가·지역·부문별 조치를 연계·조정할 수 있다고 설명
- 그러나 단일 조직에서 모든 기능을 수행하기는 어려우므로 대학, 공공 연구 기관, 연구비 지원기관 등이 참여하는 컨소시엄형 체계가 현실적이라고 제안

2. 지역 미션 구체화

- 두 번째로는 국가 수준의 미션을 각 지역의 산업 구조, 자연환경, 인구구성, 행정역량 등에 맞게 재해석해 지역 미션으로 구체화할 것을 제안
- 특히 지역 미션 설정 시 ▲기존 정책 검토·재구성 ▲지역 이해관계자들이 적극 참여하는 지역 혁신 생태계 조성 ▲연구개발·실증 등 지역 프로젝트 실시 등과 같은 수단을 활용해 실효성을 높일 수 있음을 강조
- 이와 더불어 지역 미션을 글로벌 과제 해결만이 아닌 지역 혁신 동력을 창출하는 기회로 인식하고, 지역 차원의 성과를 국가 전체로 확대할 수 있는 메커니즘을 병행해 설계할 것을 권고

출처 : 일본 연구개발전략센터(CRDS) (2026.6.)

<https://www.jst.go.jp/crds/pdf/2026/SP/CRDS-FY2026-SP-03.pdf>

4 중국, '지식재산권 보호·활용 제15차 5개년 계획' 발표

➔ 중국 국무원은 지식재산 강국 건설을 위해 '30년까지 추진할 지식재산권 정책·과업의 목표와 주요 사업들을 정리한 5개년 계획*'을 발표('26.7)

* 知识产权保护和运用“十五五”规划

- (개요) '30년까지 지식재산권 종합 역량과 국제경쟁력을 강화하고 지식재산 강국 건설에서 결정적인 진전을 이루겠다는 목표를 담은 전략 문서
 - 상위 문서인 '경제·사회 발전 제15차 5개년 계획*'에 따른 부문별 후속 실행 계획에 해당
 - * '제15차 5개년 계획'으로 불리는 중국의 종합 국가발전계획으로 '26년 3월 '中华人民共和国国民经济和社会发展第十五个五年规划纲要'이라는 제목으로 발표
 - 지식재산권을 산업 혁신, 국가 경쟁력, 경제 발전을 위한 전략적 자산으로 간주하고, '30년까지 중국 정부가 추진할 지식재산권 관련 정책의 목표·방향 및 세부 과업 등을 구체적으로 명시
 - 단순히 특허 보유량을 늘리는 데에 그치지 않고 지식재산권의 보호, 산업적 활용, 글로벌 규범 수립을 아우르는 포괄적 조치를 추진할 계획임을 강조
- (목표) '30년까지 달성해야 할 지식재산권 발전 목표를 설정

〈 지식재산권 목표 〉

'30년까지 달성할 지식재산권 역량 향상 목표

- 인구 1만 명당 고부가가치 발명특허 보유량: '25년 16건 → '30년 22건 초과
- 국내총생산 중 지식재산권(특허) 집약형 산업의 부가가치 비중: '24년 13.38% → '30년 14.60%
- 국내총생산 중 저작권 산업의 부가가치 비중: '24년 7.46% → '30년 7.53%
- 지식재산권 사용료 총 수출입액(5개년 누적 기준): '25년 1,960억 위안 → '30년 2,000억 위안
- 지리적 표시 제품 직접 생산액: '24년 9,960억 위안 → '30년 1조 1,000억 위안
- 지식재산권 보호 사회 만족도: '25년 82.81점 → '30년 83.90점

- (핵심 과제) 목표 달성을 위해 추진할 정책 방향 및 과제를 지식재산권의 ▲보호 환경 ▲활용 효율성 ▲포괄적 관리 시스템 ▲국제협력 측면에서 제시
 - AI 및 데이터에 관한 지식재산권 보호 규정 정비 계획이 가장 팔목할만한 부분으로, 중국은 이를 통해 알고리즘, AI 생성물, 데이터, 오픈소스 기술을 포괄하는 새로운 지식재산권 보호체계 구축 방침을 표명
 - 기존의 특허·상표·저작권 보호에서 한 걸음 더 나아가 새로운 디지털 창작물과 기술 거래를 제도화한다는 구상도 제시

- 그밖에 특허 이전 방식 개선, 지식재산권 관련 금융 발전 추진, 전략적 신흥 산업 보호, AI·지식재산권의 상호 활용, ‘일대일로(一帶一路)’ 협력 강화 등을 위한 과업들도 제시

〈 4가지 핵심 과제 〉

구분	주요 내용
지식재산권 보호 환경 최적화	① 지식재산권 법률 시스템 개선 • 지식재산권 법률·규정 개선 - 지식재산권에 대한 기초 법률 연구 강화 - 지식재산권의 보호 및 이용 제도 개선 - 특허 관련 법률 제도 지속 개선 - 상표법 및 시행령의 전면 개정을 추진하고 상표 보호 범위 확대 검토 - 저작권법 관련 시행령·규칙을 개정하고 저작권 공동 관리 제도 개선 - 중의학 지식 보호에 관한 규정 제정 • AI 등 신흥 분야에서 지식재산권 보호 시스템 및 규정 개선 - 알고리즘, AI 기반 제품, 플랫폼 경제 발전과 관련된 지식재산권 보호 규정 강화 - 데이터 지식재산권 보호 규정 등 체계 구축 방안 모색 - 오픈소스 지식재산권 계약 규정 관련 연구를 강화하고 국내 오픈소스 커뮤니티 육성 지원 - 온라인 출판물·영상·문학·예술 분야 지식재산권 보호 시스템 및 거래 규정 개선 - 생물유전 자원의 지속가능한 이용과 이익 공유를 촉진하고 중요 생물유전 자원의 손실 위험 평가 강화
	② 지식재산권 보호 시스템 개선 • 지식재산권에 대한 사법적 보호 강화 - 지식재산권 사건에 대한 심리 절차를 개선 - 사건의 전문화, 관할권 집중, 절차 간소화 등을 특징으로 하는 재판 시스템 구축 촉진 - 지식재산권 침해에 대한 징벌적 손해배상 제도를 지속 개선하고, 중대 지식재산권 침해는 법에 따라 엄중 처벌 • 지식재산권에 대한 행정적 보호 강화 - 핵심 제품, 핵심 산업, 핵심 시장 및 핵심 연결 고리에 집중하여 지식재산권 침해 및 위조품 근절을 위한 다양한 특별 캠페인을 지속 추진 - 독점 금지 집행을 강화하고, 지식재산권을 남용해 경쟁을 배제하거나 제한하는 행위를 법에 따라 조사·처벌 - 지식재산권 평가기관 육성·관리를 강화하고, 평가 업무의 표준화 및 전문화 촉진 • 지식재산권 보호 협력 강화 - 지식재산권 분쟁 해결 채널을 확대하고, 지역·부처 간 협력 강화 - 지식재산권에 대한 행정적 보호와 사법적 보호 연계 메커니즘 개선 - 주요 산업 분야에서 지식재산권 자율규제 협약 제정을 장려해 기업이 법규를 준수하고 공정하게 경쟁하도록 유도
	③ 국제 지식재산권 보호 강화 • 국제 지식재산권 분쟁 처리 개선 - 국제 지식재산권 보호 시스템을 구축하고, 국제적인 분쟁에 대응 - 모든 유형의 사업자에 대한 동등한 대우를 법적으로 보장 • 해외 지식재산권 보호 지침 및 국제 분쟁 대응을 위한 체계 개선 - 상공회의소, 산업협회, 글로벌 전자상거래 플랫폼 등이 외국 기업의 지적재산권 보호를 지원하는 플랫폼을 구축하도록 장려 - 보험기관들이 시장 원칙에 따라 지적재산권 관련 보험 사업을 수행할 수 있도록 지원

구분	주요 내용
지식재산권 이용 효율성 향상	④ 지식재산권 이전·활용 능력 강화 • 지식재산권 이전·활용을 위한 생태계 조성 - 지식재산 요소 시장의 육성 및 발전을 가속화 - 국가 지식재산 운영 플랫폼 시스템 개선 - 금융, 교육, 과학기술, 산업 등 다양한 플랫폼·매개체와의 시너지 강화 - 대학 내 기술이전센터 등을 활용해 대학 특허 및 기타 과학기술 성과와 기업 수요 연계 강화 - 위험도가 높거나 전환이 어려운 특허 기술에 대해 ‘선사용 후지불’ 및 ‘선전환 후투자’와 같은 특허 이전 모델을 적극 추진 • 지식재산권 수익 배분 개혁 - 과학기술 성과에 대한 권한을 강화하고, 동등한 권리와 의무를 기반으로 지식재산권 수익 배분 메커니즘 개선 • 지식재산권 금융 발전 추진 - 지식재산권 금융 생태계를 위한 포괄적인 시범 사업 추진 - 지식재산권 담보 대출, 증권화, 보험, 펀드 등 금융 상품을 혁신하고, 금융 데이터와 지식재산권 데이터 공유 강화 - 지식재산권 금융 서비스에서 위험 분담 및 보상 체계 개발 - 지식재산권 담보 대출에 대한 선지급 모델 장려
지식재산권 이용 효율성 향상	⑤ 지식재산권 공급 확대 • 핵심 기술 개발 지원 - 핵심 기술과 관련한 고부가가치 특허 및 특허 포트폴리오 발굴·육성 • 산업 혁신 및 발전 가속화 - 특허 집약적 산업을 육성하고 특허 집약적 제품의 개발·보급 강화 - 블록체인, 빅데이터, 클라우드 컴퓨팅, AI 등 신기술 및 산업 발전을 촉진하기 위해 저작권 서비스 및 보호 강화 - 신산업, 새로운 비즈니스 모델, 새로운 형식에 따른 상표 등록 수요 변화에 맞춰 상품 분류 체계 개선 - 디지털 및 녹색 기술 특허의 산업적 활용을 강화하고 핵심 디지털 경제 산업 및 녹색·저탄소 기술 분야의 유효 발명 특허 건수 증가 지원 • 지식재산권 기반 경제 육성·강화 - 국제적으로 영향력 있는 상표 및 브랜드와 국내 브랜드를 육성 - 지식재산권과 상업·관광·문화·스포츠·건강을 융합한 혁신 시나리오를 개발하고 ‘지식재산권+소비’ 발전을 촉진
지식재산권 이용 효율성 향상	⑥ 지식재산권 서비스 산업 발전 촉진 • 지식재산권 서비스 역량 강화 - 지식재산권 서비스 산업 클러스터의 최적화 및 고도화 촉진 - 지식재산권 서비스 기관들을 지원하고, 해외 유명 지식재산권 서비스 기관들의 중국 내 서비스 제공을 장려 • 지식재산권 서비스 산업 감독 강화 및 지식재산권 대행사에 대한 규제 시스템 개선 - 특허 대행 업계에 대한 진입을 통제하고, 상표 대행사 등록 관리 강화 - 저가 경쟁을 규제해 지식재산권 서비스 산업 내 무분별한 경쟁 근절
포괄적인 지식재산권 관리 시스템 지속 개선·발전	⑦ 지식재산권 관리 수준 향상 • 지식재산권 업무에서 협업 효율을 개선하고 효율적인 종합 지식재산권 관리 시스템 구축 - 부처 간 합동회의의 시스템 개선, 지역적 협력 강화 등 추진 • 지식재산권 심사·관리 수준 향상 - 관련 심사기관 구축을 가속화하고, 특허·상표 심사 정책·관리 시스템을 개선하며, 심사 협력 메커니즘을 최적화 - 국가 수준의 종합적인 저작권 등록 정보 서비스 플랫폼 연구

구분	주요 내용
지식재산권 분야에서 새로운 국제협력 모델 구축	⑧ 지식재산권 공공 서비스 강화 • 공공 서비스 역량 강화 - 부처 간, 중앙-지방정부 간, 지역 간 협력 강화 - 각 성(省) 내 지식재산권 서비스 기관의 전반적 관리를 강화하고, 일정 자격을 갖춘 시·군이 전문 공공 서비스 팀을 구축할 수 있도록 지원 • 공공 서비스의 질과 효율성 개선 - 공공 지식재산권 서비스에 대한 국가 표준 발표 및 시행 - 온라인·오프라인을 접수를 지원하고, 지식재산권 업무 처리 표준화 촉진
	⑨ 지식재산권에 대한 사회적 공동 관리 강화 • 지식재산권 분야에서 신용 시스템 구축 지속 추진 • 지식재산권 분야 인재 양성 강화 - 높은 전문성을 갖춘 실무 중심 인재 풀(pool) 육성 및 자격평가 강화 - 국제 지식재산권 아카데미 구축 및 지식재산권 싱크탱크 육성 추진 • 지식재산권 문화 조성 - 지식재산권 관련 인식증진 캠페인 실시 및 교육 강화
지식재산권 분야에서 새로운 국제협력 모델 구축	⑩ 글로벌 지식재산권 관리 참여 • 다자 협력 체제 발전 촉진 - 유엔(UN), 세계무역기구(WTO) 등 국제적 틀과 다자 메커니즘 내에서 지식재산권 관련 협력 강화 - 양자·다자 간 지식재산권 협상에 적극 참여 - 세계지식재산기구(WIPO)의 다자적 활동에 건설적으로 참여해 글로벌 지식재산권 서비스 시스템의 개선 도모 - 지식재산권 중재·조정과 분야에서 국제협력을 강화해 국제 분쟁 해결 역량 향상
	⑪ 국제 교류와 협력 심화 • ‘일대일로’ 구상 하에서 지식재산권 협력 증진 - 주요 국가·지역에서 양자·다자 간 협력을 강화하고, 이들 지역에서의 지식재산권 역량 강화 지원 - 특허 심사 하이웨이(Patent Prosecution Highway)* 등 국제 협력 네트워크 확대 및 강화 추진 * 국가 간 협약에 따라 어느 한 국가에서 특허 가능 결정을 받으면, 다른 국가에서도 이를 활용해 신속하게 심사와 특허를 받을 수 있는 제도 - 더 많은 중국의 상표, 브랜드, 지리적 표시 제품이 국제 시장에 진출할 수 있도록 지원

출처 : 중국 국무원 (2026.7.31.)

https://www.gov.cn/zhengce/zhengceku/202607/content_7077200.htmhttps://paper.people.com.cn/rmrb/pc/content/202608/01/content_30172552.html<https://research.hktdc.com/sc/article/MjM5NzY3OTYzNQ>

5 CSIS, 중국의 상업우주 발전이 미국에 미치는 영향을 분석한 보고서 발표

➔ 미국 전략국제연구센터(CSIS)는 중국의 상업우주 산업 발전 현황을 분석하고, 미국의 경제·안보에 대한 전략적 함의를 고찰한 보고서*를 발표('26.7)

* Blurred Orbits: Inside China's Commercial Space Expansion

- (개요) 중국의 상업우주* 발전을 우주 산업에 대한 전략적 접근법, 기업, 지원 및 투자, 제조 동향 측면에서 분석하고, 미국 경제와 안보에 미칠 영향을 전망
 - * 완전한 정부 소유·운영 기업이 아니고, 민간 또는 혼합 자본을 유치해 국내외에서 제품이나 서비스를 제공하는 기업을 의미
- 중국의 상업우주 및 제조 기반이 매우 놀라운 규모와 속도로 발전하고 있다고 진단하면서 이를 증명하는 다양한 지표 및 데이터를 제시
- 또한 중국 정부의 산업 정책과 긴밀히 연계된 중국의 상업우주 발전 모델에 대해 설명하고, 미국과는 다른 역학 관계 속에서 발전하고 있음을 강조
- 마지막으로 중국의 상업우주 산업 생태계 발전이 미국의 경제적 우위와 국가 안보에 도전이 될 수 있다고 경고하면서 미국 정책 입안자들에게 중국의 상업 우주 발전 현황을 파악해 범국가적 대응책을 마련해야 한다는 메시지를 전달
- (전략적 접근법) 중국은 우주 기술을 장기적인 경제 발전 및 국가 안보의 핵심 동력으로 삼아 세계 최고 우주 강국이 되기 위한 노력을 전개
 - 중국의 우주 전략은 단순한 기술 개발을 넘어 ▲경제 성장 및 공공 서비스 제공 ▲최첨단 군사력 구축 ▲중국 공산당의 역량과 위신 과시 ▲우주 기술 개발에 대한 중국 내 관심 고취를 동시에 추구

〈 중국의 상업우주 관련 발전 목표 〉

구분	주요 내용
경제 성장과 공공 서비스 전달	• ‘우주’를 신질생산력(新质生产力)*의 핵심 축의 하나로 설정 * '23년 시진핑 주석이 최초로 소개한 개념으로 노동·자본 같은 전통적 투입 요소에 의존하는 대신 지속적이고 혁신 주도적인 성장을 창출할 수 있는 산업을 의미 • 중국 기업 및 정부 기관들은 정부 정책 기조에 적극적으로 대응했고, 그 결과 지난 7년간 중국 내 우주 관련 기술 특허 출원 건수가 급증 - 우주 발사 분야에서 상위 10개 특허 출원 기업들은 '10년 이후 약 2,340건의 특허를 출원 - 위성통신(SATCOM) 분야에서 상위 10개 특허 출원 기업들은 '10년 이후 약 1,280건의 특허를 출원 • 중국 정부는 상업우주 비행을 새로운 성장 동력이자, 위성인터넷·우주 관광·첨단농업·우주제조 등 ‘저궤도(LEO) 경제’를 위한 기반으로 간주

구분	주요 내용
최첨단 군사력 구축	- 우주를 현대전에서 정보 우위와 정밀타격, 작전 주도권을 가능하게 하는 '군사 경쟁의 새로운 전략적 고지'로 인식 - 특히 AI·빅데이터 등이 결합된 지능화 전쟁 비전의 핵심으로 간주 - 군민융합(Military-Civil Fusion) 전략에 따라 군사적 변혁을 주도하는 동시에 항공우주 발전을 추진 - 미국 군부와 스페이스X의 협력 모델을 모방해, 군민 겸용 자체 저궤도 광대역 네트워크 구축과 이중용도 생태계 육성을 강조
국가적 위신	- 중국 공산당의 역량·자신감·현대성을 드러낼 수 있는 수단으로써 우주 분야에서의 가시적인 성과 창출을 강조 '24년 달 뒷면에 착륙해 2kg의 달 샘플을 수집해 지구로 귀환한 창어 6호(嫦娥六號)의 성과는 중국이 우주 분야에서 미국과 대등한 경쟁자라는 이미지를 강화한 사례로 평가
우주 기술에 대한 관심 고취	'우주의 날' 지정, 로켓 명소 조성, 우주과학 영화 제작, 우주 관광 및 우주 테마파크 등을 통해 우주를 교육·문화·관광·지역 브랜드와 결합

● (기업 현황 및 모델) '14년 우주 산업의 일부를 민간 투자자본에 개방한 이후* 중국의 상업우주 생태계 확장으로 기업 수 대폭 증가(12개→600개)

- * 중국 국무원은 핵심 분야 투자·융자 메커니즘 혁신 및 민간 자본 투자 장려에 관한 지침 (Guiding Opinions on Innovating Investment and Financing Mechanisms in Key Areas and Encouraging Social Investment)을 발표하며 민간 투자 개방 조치를 단행
- 이들 기업은 우주 발사, 위성통신(SATCOM), 원격탐사, 항법, 기상 관측은 물론 우주 내 서비스(in-space servicing) 및 상업용 유인 우주 비행 등 신흥 분야에 걸쳐 다양하게 활동
 - 민간 발사체 기업들은 재사용 로켓 개발 등에 주력하고 있으며, 저궤도 통신망 확보를 목표로 한 초대형 위성군(Mega-constellation) 구축도 진행 중
 - 그러나 이러한 기업 중 다수가 국가적 우선순위와 긴밀히 연계된 중국 특유의 모델로 운영되고 있다는 점에서 중국의 상업우주 발전은 서구와 같은 민간 모델이 아닌, 국가의 전략적·관료적 구조에 통합된 '혼합형 모델'에 해당

〈 부문별 발전 현황 〉

구분	주요 내용
우주 발사	'14년 민간에 우주 산업을 일부 개방한 뒤 다수의 상업 발사기업을 육성 - 대표 기업은 LandSpace, Space Pioneer, Galactic Energy, iSpace 등 - 이들 기업 중 다수는 스페이스X 모델을 추종해 저비용 발사, 대량 생산, 1단 추진체 재사용 등과 같은 목표를 추진 - 중국의 궤도 발사 횟수는 '15년 이후 거의 5배 증가하여 '25년 92 회로 사상 최고치를 기록 - 민간 기업이 발사 횟수 증가에 기여하고 있지만, '25년 대부분의 발사는 국영기업(SOE)들이 주도

구분	주요 내용
위성통신	• 스페이스X의 스타링크에 대항하기 위해 추진 중인 국가 주도형 저궤도 (LEO) 위성 인터넷망 구축 프로젝트인 ‘귀왕(Guowang)’과 ‘천 개의 돛 (Thousand Sails)’으로 각각 1만 기가 넘는 저궤도 위성 배치를 추진 • 이는 단순한 브로드밴드 위성망을 넘어 중국이 세계적인 정보·통신 인프라를 구축하고 국제적 영향력을 확대할 수 있는 수단이 될 전망 • 대표 기업은 Shanghai Spacecom Satellite Technology, Geespace 등
원격탐사	• 원격탐사는 위성통신과 함께 빠르게 성장 중 • 대표 기업은 China Siwei, Chang Guang Satellite Technology 등 • 기업들은 고해상도 전자광학(EO) 영상 위성, 합성 개구 레이더 위성(SAR), 비디오 위성 등을 활용한 대규모 상업용 위성군을 구축하고, 지도 제작, 토지이용, 국방·정보 분야 등에서 영상·데이터·분석 서비스를 제공
기타 분야	• 발사·위성통신·원격탐사 외에도 글로벌 위상 항법 시스템(GNSS), 기상 관측, 우주에서의 제조·생산·조립(ISAM), 유인 우주비행 및 우주 관광 등 다양한 우주 서비스 영역으로 확장을 추진

- (지원·투자) 중국 중앙 정부와 지방 정부는 상업우주를 발전 계획에 포함시켜 전국에 걸쳐 항공우주 도시, 기술 허브, 연구 센터, 제조 시설 확대 등을 지원

〈 중국의 상업우주 관련 정책 접근법 변화 〉

구분	상업우주 관련 핵심 메시지
중국 우주활동백서('00년)	• 국가 우주 정책에 따라 과학연구기관, 산업체, 민간 기업 및 대학이 각자 강점을 활용해 우주 활동에 적극적으로 참여하도록 장려 → 국가의 지도 하에 기업과 대학이 우주 분야에 참여할 수 있도록 허용
중국 우주활동백서('06년)	• 위성 통신·방송의 상용화를 적극적으로 추진하고, 통신·방송 위성 및 응용 분야의 산업 규모를 확대
중국 우주활동백서('11년)	• 위성 통신 상용화를 더욱 가속화하고 통신·방송 위성 응용 분야의 산업 규모를 확대
중국 우주활동백서('16년)	• 비정부 자본 및 기타 사회 부문이 과학연구 및 생산, 우주 인프라, 우주 정보 제품·서비스, 위성 활용 등 우주 관련 활동에 참여하도록 장려하여 우주 산업의 상업화 수준을 향상 → 상업화 전환 목표 명시
‘중국의 우주 프로그램: '21년의 관점’ 보고서	• 상업우주 부문에 주요 과학연구 시설·장비 개방 및 공유 촉진 • 상업우주 기업의 주요 우주 프로젝트 참여 지원 • 우주 활동에 관한 네거티브 리스트(Negative List)* 시스템 구축 * 특별히 금지하거나 제한하는 항목을 만들고, 나머지는 모두 원칙적으로 허용하는 제도를 의미 → 공정 경쟁 촉진, 규제 투명성을 위한 메커니즘 구축 강조

- 중국의 우주 산업 정책은 중앙 정부와 지방 정부가 서로 다른 역할을 수행하면서 서로 상호 보완적인 구조를 이루는 단계적 거버넌스 시스템을 통해 시행
- 국가 차원의 정책은 우주 분야에서 국가적 목표에 대한 청사진을 제공하고, ‘기술 자립’, ‘민간-군사 역량 통합’, ‘세계적으로 경쟁력 있는 항공우주 기업 육성’과 같은 전략적 우선순위를 정의



- 지방 정부는 ▲우주도시·산업단지 조성 ▲발사체·위성통신·원격탐사·위성제조 등 분야별 전문화 추진 ▲산업 클러스터 형성 ▲보조금 및 세제 혜택 지원 등에 대대적으로 투자하며 산업 정책을 구체적으로 실행하는 역할을 담당
- 또한 중국은 ‘민군 융합(Military-Civil Fusion)’ 전략을 통해 민간 기업의 첨단 기술과 위성 데이터, 제조 역량을 직·간접적 군사력 강화로 잇는 구조를 구축

〈 주요 지역별 발전 현황 및 목표 〉

구분	발전 현황 및 목표
베이징	• 중국 최대 우주 산업 클러스터 형성 - 300개 이상의 상업우주 기업과 상업우주 유니콘 기업의 절반 이상이 베이징에 집중 • ‘남쪽 로켓, 북쪽 위성’이라는 공간적 분업을 통해 다싱구(남부)에는 로켓 연구개발 및 발사 서비스를 위한 ‘로켓 스트리트(火箭大街)’를, 하이톈구(북부)에는 실리콘밸리 스타일의 위성 혁신 허브 ‘스타 밸리(星谷)’를 조성
상하이	• 당초 ‘25년까지 ‘연간 상업용 로켓 50기와 위성 600기’ 생산 역량 확보 목표를 제시했으나, 이후 달성 시한을 ‘27년으로 연장하면서 생산 역량 목표를 ‘연간 로켓 100기, 위성 1,000기’로 상향
광둥성	• ‘26년까지 상업 항공우주 경제 및 관련 산업 규모를 3,000억 위안으로 확대하고, ‘28년까지 위성·로켓 연구개발을 발전시키기 위한 프로 세스를 구축하는 것을 목표로 한 정책을 추진 • ‘25년 92억 위안 규모의 양장 우주 발사센터 건설 계획을 발표하는 등 우주 발사 및 로켓 기술에 집중 투자
장쑤성	• 성 차원에서는 ‘25년까지 항공우주산업 생산 규모를 1,500억 위안으로 확대한다는 목표를 설정 - 대체로 항공 분야 중심이지만 상업우주 개발 활동도 포함 • 시 차원에서는 장쑤성 남부의 우시(无锡) 시가 ‘27년 말까지 항공우주 산업 발전을 촉진한다는 계획을 발표 - 로켓·위성 분야 신생 기업에 지원금 제공, 인재 양성 촉진 등에 초점
후베이성	• 로켓, 위성, 데이터, 서비스라는 ‘4대 사슬’을 중심으로 한 발전 구상과 완전한 ‘로켓-위성-네트워크-단말기’ 생태계 구축을 추진 • ‘28년까지 연간 발사체 60기, 상업 위성 500기 생산능력, 관련 산업 규모 1,000억 위안 이상을 달성한다는 목표를 제시
기타	• 우한 국가항공우주산업기지, 하이난 원창 국제항공우주도시, 산둥성 하이양 동방우주항 등은 지방정부의 대표적인 우수 산업 클러스터·도시 사례

- (제조 역량) 중국은 위성 대량 생산이 가능한 ‘기가 팩토리’ 및 ‘스마트 팩토리’를 포함해 우주 산업 발전을 뒷받침하는 데 필요한 제조 기반을 구축 중
 - 중국 하이난성 원창 위성 기가팩토리 등 17개 주요 생산시설은 연간 약 4,100~5,000기의 위성을 생산할 수 있는 능력을 갖추고 있는 것으로 추정
- (미국 경제·안보 상의 함의) 상업우주 산업에서 중국의 빠른 발전과 규모 확대는 미국의 경제와 국가 안보상의 이익을 위협할 수 있을 전망

① 중국의 기술 주도권 장악 가능성

- 중국은 과거에도 국가 주도의 산업 정책을 통해 조선, 5G 통신, 핵심 광물, 친환경 제조와 같은 전략적으로 중요한 산업 분야에서 미국이 미처 효과적인 대응책을 마련하기도 전에 지배적 지위를 확보
- 중국 정부는 장기적 전략 목표 달성에 도움이 된다면 투자 중복과 같은 비효율, 중복 생산, 과잉 생산 등과 같은 부작용을 기꺼이 감수했고, 이러한 산업 발전 모델을 현재 상업우주 산업에도 동일하게 적용 중인 것으로 분석
- 미국은 여전히 상업우주 분야에서 혁신을 주도하고 있으나, 중국의 빠른 추격 추세는 미국의 장기적인 우위 유지 가능성에 의문을 제기
- 미국의 우주 산업이 빠른 혁신, 생산 확대, 충분한 장기 자본 동원력을 바탕으로 중국의 추격에 대응할 수 있을지가 미래 경쟁력을 결정지을 전망

② 글로벌 정보 인프라 구축·확장 가능성

- 중국은 상업우주 발전을 발판 삼아 전 세계 디지털 인프라와 영향력을 재편할 수 있는 글로벌 정보통신 아키텍처를 구축 중
- ‘귀왕’, ‘천 개의 돛’ 등 브로드밴드 위성군 프로젝트는 스페이스X 스타링크와의 경쟁뿐만 아니라, 서구의 표준 및 거버넌스 체계에서 벗어나 대안적인 통신 생태계를 구축하는 것을 염두에 두고 추진
- 이 가운데 중국 기업들은 일대일로(一帶一路), 우주 실크로드(Space Silk Road) 전략 등을 통해 아프리카, 라틴 아메리카, 동남아시아 등 개발도상국에 통신, 항법, 원격탐사, 디지털 인프라 서비스를 통합 패키지 형태로 수출
- 중국 정부의 보조금 및 재정 지원 속에서 이러한 수출은 더욱 가속화되고 있으며 중국의 기술 표준, 규제, 데이터 거버넌스 모델에 의존하는 국가들은 점점 더 증가할 전망
- 아직까지 중국 상업우주 산업은 수익성, 발사 역량, 국제적 신뢰 측면에서 여러 제약에 직면해 있지만, 우주 강국으로 발돋움하려는 중국 정부의 노력은 장기적으로 중국의 경제적·지정학적 영향력 확대에 이어질 가능성이 농후

출처 : 미국 전략국제연구센터(CSIS) (2026.7.29.)

https://csis-website-prod.s3.amazonaws.com/s3fs-public/2026-07/260728_Bingen_Blurred_Orbits.pdf?VersionId=B92oz6ebW4Fl8wZul4iqPuaJBikfQM9A

6 CSIS, 미국 주정부·EU·산업계의 AI 규제 프레임워크 분석 보고서 발표

➔ 미국 전략국제연구센터(CSIS)는 미국 주정부들의 AI 규제 법안과 EU AI법(AI Act), 산업계의 자발적 AI 안전 프레임워크를 비교·분석한 보고서*를 발표('26.8)

* Toward a Federal Framework: Lessons from State and International Frontier AI Regulation

- (개요) 주정부 차원에서 추진되는 프론티어 AI 규제 법안들과 EU 및 산업계의 AI 규제 프레임워크를 비교해 미국 연방 차원의 AI 규제 입법을 위한 제언을 제시
 - 9가지 프레임워크들이 AI 모델 규제 방법론에 있어 여러 공통 요소를 가지고 있다고 분석하고, 이러한 공통 기반이 글로벌 기준선이 되어가고 있다고 설명
 - 다만 규제 대상·범위·강도 등에서 여전히 상당한 불일치도 존재한다고 지적
 - 현재 미국 연방 차원의 AI 규제 프레임워크가 부재한 가운데, 주정부들의 AI 규제 실험을 '규제 파편화'나 '통일된 프레임워크를 가로막는 방해물'로 간주하기보다 연방정부의 AI 입법 설계에 활용할 것을 제언

〈 CSIS가 분석한 9가지 AI 규제 프레임워크 개요 〉

구분	주요 내용
캘리포니아주 S.B. 1047	• 대규모 AI 모델 개발사뿐만 아니라 컴퓨팅 클러스터 운영자 및 제3자 감사인까지 규제 대상에 포함시키는 등 매우 강력한 AI 규제 법안 • 보안 조치, 위험 평가, 사고 보고, 고객확인(KYC) 요건은 물론 일정 수준 이상의 위험 발생 시 모델 작동을 강제 종료하는 '킬 스위치' 조항도 포함 • 주지사의 거부권 행사로 폐기('24년 9월)
캘리포니아주 S.B. 53	• S.B. 1047보다 훨씬 완화된 개발자 중심 AI 모델 규제법 • AI 개발사에 안전 및 보안 프로토콜(SSP*) 공개 및 중대 사고에 대한 신고 등을 의무화 * safety and security protocol: 기업의 거버넌스 및 규정 준수 전략을 설명하는 문서로, 대개 위험 평가, 위험 완화·보안 조치 등을 포함 • '25년 제정되어 '26년 1월부터 시행 중
뉴욕주 RAISE 법 (Responsible AI Safety and Education Act)	• 대형 프론티어 AI 모델 개발사에 SSP 공개와 사고 보고 의무를 부과 • '25년 12월 주지사 서명을 통해 법률로 제정
일리노이주 S.B. 315	• 대형 프론티어 AI 개발사에 대해 독립된 제3자를 통한 연례 안전 감사를 의무화 • '26년 7월 주지사 서명을 통해 법률로 제정
미시간주 H.B. 4668	• AI 모델에 대한 안전·보안 요건, 위험 평가, 투명성 의무 등을 규정 • '25년 6월 발의되었으며 현재 의회 계류 중
매사추세츠주 S. 2630	• AI 모델에 대해 안전·보안 조치, 위험 평가·완화, 사고 보고, 내부 고발자 보호 등을 요구 • '25년 10월 발의되었으며 현재 의회 계류 중

구분	주요 내용
EU AI법	• 세계 최초의 포괄적인 AI 규제법 • AI가 미치는 위험 수준에 따라 차등적인 규제 적용 • 동 법에 명시된 범용 AI(GPAI) 모델 관련 의무 이행을 지원하기 위해 EU가 채택한 ‘범용AI 실천강령’(‘25.8.1.) 역시 법적 구속력을 보유 • ‘25년 7월 공표된 후 범용AI 실천강령 적용이 시작(‘25.8.2.~)되었고, 시스템적 위험을 가진 범용AI 관련 집행·제재도 본격 시행(‘26.8.2.~)
서울 프론티어 AI 안전 서약	• ‘24년 5월 AI 서울 정상회의에서 발표된 AI 기업 간 자발적 안전 서약 • AI 기업들은 프론티어 AI 모델의 위험 식별·평가, 위험 완화 조치 및 SSP 마련, 일정한 위험 임계치에 도달 시 책임 있는 조치 등을 약속
엔트로픽의 프론티어 모델 투명성 프레임워크	• ‘25년 7월 엔트로픽이 제안한 자발적 AI 안전 관리 프레임워크 • 초대형 모델과 개발사에 한정해 안전 관행 및 위험관리의 투명성을 높이는 비교적 가벼운 안전 프레임워크

- (공통 특징) CSIS가 분석한 9개 AI 규제 프레임워크는 ▲안전 프레임워크 ▲투명성 ▲위험 평가 ▲위험 완화라는 4가지 조치들을 공통적으로 포함

〈 9가지 AI 규제 프레임워크 비교·분석 결과 - 공통 요소 〉

구분	주요 내용
안전 프레임워크	• 안전 및 보안 프로토콜(SSP) 또는 이와 유사하게 일련의 심각한 위해에 대한 리스크 완화 전략, 보안 조치 등을 명시하는 프레임워크를 구현하고 정기적으로 업데이트하도록 의무 부여
투명성	• SSP를 일반에 공개해야 하는 의무 부여(필요시에는 상업적으로 민감한 일부 내용을 삭제해 공개)
위험 평가	• 잠재적으로 위험한 AI 모델의 기능을 식별·평가하도록 요구
위험 완화	• 재앙적인 결과를 예방하거나 줄이기 위한 조치를 마련하도록 요구

- 전 세계는 아직 프론티어 AI 규제 모델에 합의하지 못했으나 이러한 공통 조치는 AI를 책임 있게 감독하는 것에 대한 최소의 공통 기반을 형성
- 또한 CSIS가 분석한 프레임워크들은 엔트로픽을 제외하면 모두 모델 가중치·시스템에 대한 무단 액세스 방지와 같은 보안 조치를 요구
- 내부 고발자 보호를 위한 조치 역시 RAISE와 서울 서약을 제외한 대부분의 프레임워크에 포함
- ‘사고 보고 요건’도 다수의 프레임워크에 포함되었는데*, 보고 시한은 ‘72시간 이내’부터(RAISE에 해당) 사고의 심각성에 따라 보고 시한을 단계별로 적용하는 방법(캘리포니아 S.B. 53 및 EU의 범용 AI 실천 강령)까지 다양

* 서울 서약과 엔트로픽의 프레임워크에는 사고 보고 요건이 부재

- **(차이점)** 9개 AI 규제 프레임워크는 ▲규제 대상(가치사슬) 범위 ▲규제 모델 규모 ▲다루는 위험의 범주 ▲‘재앙적 위험’의 정의 측면에서 차이가 존재
 - 전반적으로 EU의 AI 규제는 현재 미국의 그 어떤 주 법안보다 더 많은 모델, 더 많은 위험, 더욱 광범위한 피해를 포괄

〈 9가지 AI 규제 프레임워크 비교·분석 - 차이점 〉

구분	주요 내용
규제 대상(가치사슬 내 행위자) 범위	• 프레임워크별로 의무를 이행해야 하는 AI 운영자(각 가치사슬 단계 및 관련 행위자)의 유형은 다양 • 캘리포니아주 S.B. 1047(현재는 폐기됨)은 AI 개발사는 물론이고 컴퓨팅 제공업체와 제3자 감사인에도 특정 의무와 규제를 부과
규제 대상 모델의 규모	• 미국 주정부 법안들은 바이든 행정부의 대통령 행정명령 14110호에서 영감을 받아 마련되어, AI 모델의 성능을 FLOP* 단위에서 구분해 높은 훈련 임계값과 규제 대상 기업을 정의하는 경우가 다수 * Floating Point Operations Per Second: 1초당 처리 가능한 부동 소수점 연산 횟수를 의미 • 반면 EU는 더 낮은 임계값을 설정하고 있으며, 소규모 모델을 시스템적 위험을 초래하는 모델로 직접 지정할 수 있도록 허용
위험의 범주	• 미국 주정부 법안들은 모두 화학·생물학·방사능·핵(CBRN) 위험, 인간의 통제가 거의 불가능한 심각한 범죄, 사이버 공격을 다루고 있으며, 대부분 AI에 대한 통제 상실도 위험의 범주에 추가 • EU는 여기서 더 나아가 대규모 조작이나 인권침해와 같은 사회적 위험도 위험의 범주에 추가
재앙적 위험에 대한 정의	• 미국 주정부 법안들은 모두 높은 인명 피해(사망자 50~100명 이상) 또는 경제적 손실(피해액 10억 달러 초과)을 기준으로 재앙적 위험을 정의 • 반면 EU는 인프라 붕괴, 인권침해, 환경적 피해까지 포함해 재앙적 위험을 정의하는 광범위한 접근방식을 채택

- **(연방 AI 정책에 대한 영향)** 연방정부는 주정부의 입법 실험을 억누르기보다 그 성과와 한계를 참고해 혁신을 과도하게 저해하지 않으면서도 통일된 연방 AI 규제 프레임워크를 마련하는 노력이 필요
 - 지난 수년 동안 미국의 각 주는 수백 건의 AI 관련 법안을 발의하면서 AI 규제에서 중요한 시험대 역할을 수행해왔음
 - 이러한 경험은 연방정부 차원의 AI 규제 접근방식 마련을 위한 유익한 정보로 활용 가능
 - 따라서 주정부의 AI 입법 시도는 연방정부가 규제 파편화를 막고 기업의 규제 부담을 줄이는 연방 차원의 AI 입법을 가속화하는 데 중요한 청사진을 제공

출처 : 미국 과학기술정책실(OSTP) (2026.8.3.)

<https://www.csis.org/analysis/toward-federal-framework-lessons-state-and-international-frontier-ai-regulation>

7 JETRO, AI 시대 반도체 산업의 구조 변화 분석

➔ 일본무역진흥기구(JETRO)는 데이터센터용 반도체 수요 증가로 인한 반도체 산업 구조 변화를 분석하고, 국가별 제조·투자 동향과 AI의 실생활 도입이 미칠 영향을 정리*(’26.8)

* AI向け半導体の「主役」に迫る(世界), AIの社会実装で活躍広がる半導体(世界)

※ 본 고는 ’26년 8월 JETRO가 발표한 ‘AI 시대 반도체 산업’ 분석 기사 2건을 종합해 작성

● (수요 변화) 생성형 AI의 급속한 보급으로 인해 AI 데이터센터용 반도체인 GPU 및 HBM 수요가 급증하며 **반도체 산업 수요에 구조적 변화를 초래**

- 기존 반도체 시장은 스마트폰이나 PC가 주도했지만, 생성형 AI가 확산하면서 현재는 AI 데이터센터를 위한 반도체 투자가 활발
- 기존 데이터센터용 반도체는 CPU 중심이었으나 대규모 언어모델 학습에는 방대한 병렬 연산 능력이 필요해 GPU가 AI 데이터센터의 핵심 연산장치로 부상
- 또한 AI의 학습·추론을 위한 방대한 데이터의 전송 속도가 느리면 GPU의 성능을 충분히 활용할 수 없으므로 고속·대용량 처리를 지원하는 HBM 수요가 급증
- 한편, GPU와 HBM 사이에서 대량의 데이터를 저전력으로 신속히 전송하기 위해 여러 개의 반도체 다이(die)*와 메모리를 하나의 패키지로 연결하는 첨단 패키징 기술이 각광

* 웨이퍼 위에 만들어진 수많은 집적 회로들이 개별적으로 분리된 작은 조각으로, 각 다이는 특정 기능을 수행하는 수많은 트랜지스터와 회로로 구성

※ 첨단 패키징 기술의 대표 사례는 TSMC의 CoWoS(Chip on Wafer on Substrate)

- 이는 AI 연산을 빠르게 수행하기 위해 만들어진 ‘AI 가속기’의 대표 사례로, GPU 기반 제품이 주류를 형성
- 현재 AI 반도체 공급은 TSMC의 첨단 로직·패키징 역량*과 SK하이닉스·삼성전자·마이크론의 HBM 생산능력**에 크게 의존하고 있는 실정
- * GPU 설계는 엔비디아·AMD가, 생산은 파운드리 업체인 TSMC가 담당하는데 TSMC는 GPU 다이 생산과 첨단 패키징 기술까지 갖춰 AI 반도체 공급망에서 핵심적 위치를 차지
- ** HBM 생산은 한국의 SK하이닉스, 삼성전자와 미국의 마이크론이 주도 중으로, ’26년 1분기 HBM 시장 점유율은 각각 58%, 21%, 21% 수준
- 소수 기업에 대한 AI 공급능력 집중 현상은 AI 시장 전체의 병목 요인이 될 수 있으며, 이에 관련 기업들을 세계 각지에서 생산능력을 확대 중



- **(데이터센터용 반도체)** AI 데이터센터에서 반도체의 ‘주역’은 GPU와 HBM을 주축으로 하는 AI 가속기이지만, 이외에도 AI 서버에는 **통신, 전력 공급, 냉각, 저장, 보안과 관리** 기능이 함께 필요

※ 미국 반도체산업협회(Semiconductor Industry Association)와 딜로이트의 보고서에 따르면, AI 가속기가 서버 반도체 가치의 약 74%를 차지

〈 AI 서버랙 1대를 구성하고 있는 전체 반도체 가치에서 각 부품별 비중 〉

구성요소	주요 기능	AI 서버랙 1대에서 차지하는 반도체 가치 비중
AI 가속기	AI 학습·추론을 위한 대규모 행렬연산	74%
CPU	서버 전체 제어 및 작업관리	8%
휘발성 메모리	CPU·DPU용 주기억장치	5%
통신/연결 부품	서버 및 AI 가속기 간 고속통신	5%
전력/냉각 부품	전력 공급, 열관리	3%
데이터 처리 유닛(DPU)	네트워크 통신, 스토리지 액세스, 보안 처리	2%
비휘발성 메모리	학습 데이터 및 AI 모델의 장기 저장	1%
시스템 통합/관리	서버 모니터링, 관리, 보안	1% 미만

출처 : Powering AI: The Semiconductor Ecosystem at the Foundation of Data Centers

- AI 반도체 산업의 경쟁력은 특정한 한 종류의 첨단 칩만으로 확보되는 것이 아니라, 다양한 반도체가 서로 보완하는 전체 시스템 역량에 의해 결정
- 더욱이 AI가 현실 세계의 다양한 기기 및 산업에 적용되면 수요나 중요성이 높은 반도체의 종류가 변화할 가능성도 존재
- **(국가별 제조 역량)** 로직 반도체와 메모리 제조는 **동아시아에 편중**돼 있으나 다른 반도체들은 각지에 제조 능력이 분산된 형태인 **국제 분업 체제**를 유지

〈 반도체 유형별 국가·지역의 제조 역량 〉

구분	주요 내용
로직 반도체·메모리	• '25년 4분기 기준 웨이퍼 생산능력을 살펴보면, 로직 반도체는 중국·대만·한국·일본 4개국에 77.8%, 메모리는 이들 지역에 93.9%가 집중 • 그중 로직 반도체는 대만, 메모리는 한국이 각각 40%의 생산능력을 점유
이산 반도체	• 중국이 절반을 차지하지만 일본과 유럽·중동도 각각 15%의 점유율 보유
아날로그 반도체	• 전 세계적으로 제조 역량이 폭넓게 분산
광전자 반도체	• 중국과 일본이 약 70%를 차지
미세전자기계 시스템(MEMS)	• 미주(30.5%)와 일본(23.9%)이 절반 이상을 차지

- **(국가별 투자 동향)** '25~'27년 전 세계 반도체 설비투자에서 **로직 반도체와 메모리의 비중은 77.8%로 전망**되며, 특히 **대만과 한국**에서는 이 두 분야의 설비투자가 전체 투자액의 95%를 초과할 전망

〈 대만·한국 외 국가·지역별 주요 반도체 투자 분야 〉

구분	주요 투자 분야
중국	·아날로그 반도체(22.3%), 이산 반도체(8.9%), 광전자 반도체(5.7%) 등
일본	·로직 반도체·메모리 중심 ·이산 반도체(11.0%)와 광전자 반도체(10.5%) 투자도 증가
유럽·중동 및 아태 지역	·아날로그 반도체 투자가 30~40%를 차지 ·독일과 싱가포르의 아날로그·혼합 신호(Analog/Mixed-Signal)에 투자
미주	·로직 반도체 투자가 60%를 차지 ·미국은 향후 SiC 전력 반도체 등 더 다양한 분야로 투자를 확대할 전망

- (엣지 AI*로 인한 산업 변화) AI 기반의 제품·서비스가 증가하고 엣지 AI가 더욱 확산하면, 반도체 수요에도 변화가 예상
 - * 스마트폰, PC, 자동차, 로봇 등 데이터가 생성되는 로컬 장치에서 AI를 직접 실행하는 방식
 - 엣지 AI에서는 단순히 대규모 모델을 학습하는 능력보다, 스마트폰, 자동차, 로봇 등의 단말·기기상에서 추론 처리를 계속해서 실행하는 능력이 중요하므로, 저전력·저비용·저지연과 같은 기능이 필요
 - 대규모 학습과 추론을 지원하는 GPU의 수요 증가세는 계속되겠지만, 단말 기반 추론에서는 특정 목적에 맞춘 ASIC*형 AI 가속기와 전원·센싱 관련 반도체 수요가 확대될 가능성이 높음
 - * Application-Specific Integrated Circuit: 특정 가전제품이나 AI 연산 등 오직 한 가지 특정 목적만을 수행하도록 설계 및 맞춤 제작된 주문형 반도체
- (피지컬 AI*로 인한 산업 변화) 향후 현실 세계에 폭넓게 적용될 것으로 예상되는 피지컬 AI도 반도체 산업에 영향을 줄 수 있을 전망
 - * 로봇·자율주행차처럼 물리적 환경과 상호작용하며 작동하는 AI
 - 피지컬 AI는 단순히 정보를 분석하거나 답변하는 데 그치지 않고, 물리적 공간을 자율적으로 인식해 행동해야 하므로 ‘보고’, ‘느끼고’, ‘움직이는’ 기능이 중요
 - 따라서 이러한 기능을 지원하는 화상 센서, LiDAR, 모터 제어용 전력 반도체 등의 중요성이 커질 전망

출처 : 일본무역진흥기구(JETRO) (2026.8.6.)

<https://www.jetro.go.jp/biz/areareports/special/2026/0801/1aee4b7856c0c87c.html>

<https://www.jetro.go.jp/biz/areareports/special/2026/0801/adf38a7c21c7f8ea.html>

8 일본 PwC, 제조업의 'AI-Ready' 전환 전략 보고서 발표

➔ 일본 PwC는 제조업 부문의 'AI 레디(AI-Ready)' 전환을 위한 조건과 과제를 정리하고, 구현을 위한 전략적 접근방법을 제시하는 보고서를 발표('26.8)

* 製造業が目指すべきAI-Ready

- (개요) 보고서는 제조업에서 AI 활용 기회, 'AI 레디'의 개념, 데이터 아키텍처·플랫폼·거버넌스를 설명하고, 이를 위한 접근방법을 제시
 - (제조업에서 AI 활용 기회) 생성형 AI와 피지컬 AI는 일본 제조업의 노동력 부족 및 공급망 불확실성을 완화하고 운영 효율을 재고할 수 있는 핵심 수단
 - 더욱이 일본은 제조업 현장에서 축적한 풍부한 데이터를 보유하고 있어 AI를 통해 산업 경쟁력을 강화할 수 있는 역량을 보유
 - 그러나 일본 기업들은 생성형 AI 활용·검토 비율이 높은 것에 비해 실제로 가치를 창출하는 비율은 낮는데, AI 활용을 위한 조직체계, 업무 프로세스, 데이터 관리 및 거버넌스가 갖춰지지 않은 것이 원인으로 지목
- ※ 일본 PwC의 '생성형 AI에 대한 실태조사 '26년 봄 6개국 비교' 보고서에 따르면, 일본 기업의 70%는 생성형 AI를 활용 중이고, 활용을 계획·검토 중인 기업을 포함하면 그 비율은 90%에 달하지만, 생성형 AI 활용을 통해 가치를 창출하고 있다는 기업 비율에서는 조사 대상 6개국 중 최하위를 기록
- (개념과 요건) 'AI 레디'란, 데이터가 단순히 디지털화되었거나 정리된 상태가 아니라 AI가 데이터의 의미와 맥락을 이해하고, 안전하고 지속적으로 업무에 활용할 수 있는 상태를 의미

〈 'AI 레디'의 구성요소 〉

구분	주요 내용
데이터	• AI가 접근할 수 있는 고품질 데이터가 갖춰진 상태
플랫폼	• AI를 실행할 수 있는 확장성·연계성을 갖춘 서비스·기능이 갖춰진 상태
거버넌스	• AI 운용에 관한 권한, 책임, 데이터 주권, 제약 조건 등이 구조화된 상태
운영 및 프로세스	• AI의 품질·위험·비용을 지속적으로 개선하는 프로세스가 갖춰진 상태
조직	• AI 관련 책임 범위와 의사결정 체계가 명확한 상태

- 그간 데이터 품질은 정확성·완전성·일관성·가용성·최신성을 기준으로 평가되어 왔음
- 하지만, 생성형 AI 활용 환경에서는 이용자의 데이터 이해가능성, 출처 등의 신뢰성, 데이터 이력에 대한 추적가능성, 관점·정보의 다양성 등이 중요

- 생성형 AI를 위한 데이터 품질을 확보하기 위해서는 제조업 부문에 존재하는 전문용어, 약어, 도면 등 다양한 데이터를 AI에 명확히 설명해야 함
- 이를 위해서는 메타데이터*와 온톨로지/지식그래프** 등 시맨틱(의미) 정보가 필요
 - * 메타데이터는 데이터를 설명하는 데이터로, AI의 신뢰성과 설명 가능성을 확보할 수 있는 핵심 기반으로 작용
 - ** 온톨로지와 지식그래프는 데이터 간 구조와 인과관계, 다음 행동을 구조화한 체계를 의미
- (데이터 아키텍처·플랫폼·거버넌스) 데이터 품질과 의미 정보를 관리·공유하는 방법으로 메쉬 아키텍처에 대한 관심이 고조
 - 메쉬 아키텍처는 데이터 품질 책임을 중앙 조직과 개별 사업 부문(도메인)에 분산시키는 것으로*, 기존 중앙집중형 데이터 관리의 한계를 극복하면서도 완전한 분산관리의 위험을 완화하는 중간 모델의 성격을 보유
 - * 데이터에 가장 가까운 사업 부문, 즉 도메인이 데이터에 대한 소유권과 품질 책임을 갖고, 중앙 조직은 공통 플랫폼·보안·접근통제·표준·모니터링을 지원하는 구조
 - 생성형 AI를 위한 데이터 플랫폼은 취급 데이터(정형 → 정형·비정형 포괄*), 데이터 품질(의미 중심), 데이터에 액세스하는 주체(인간 → 인간, AI)의 변화를 반영해 확장·재정의가 필요
 - * 제조업 데이터에는 업무 체계에서 미리 정의한 구조에 따라 표 형식 등으로 축적하는 구조화된 정형 데이터와 더불어 현장 메모, 영상, 설비 센서와 장비 로그 등과 같은 비정형(비구조화) 데이터가 모두 존재하며, 비정형 데이터를 어떻게 활용하는지가 생성형 AI 활용에 매우 중요
 - 마찬가지로 생성형 AI를 위한 지식 거버넌스 역시 시맨틱 정보, AI 모델, AI 모델이 생성한 결과와 판단 등을 포괄하도록 확대되어야 할 필요성이 존재
- (접근방법) 일본 제조업의 ‘AI 레디’ 전환을 위해서는 ‘도메인 주도의 거버넌스 운영’과 ‘자동화 및 구조화로 AI 활용의 복잡성을 해소’하는 접근방법이 필요

〈 ‘AI 레디’ 전환을 위한 접근방법 〉

구분	주요 내용
각 사업 부문(도메인)이 주도하는 거버넌스 운영	• 각 도메인이 기존의 업무 프로세스를 전면 검토해 생성형 AI를 어디에 적용할지 결정하고, 기대효과 및 활용 사례, 필요한 데이터, 품질 기준, 이용 규칙, 책임 체계 등을 주도적으로 설계 • 일본 제조업의 강점인 ‘현장력’을 AI와 결합하는 것이 핵심
자동화·구조화로 AI 활용의 복잡성 해소	• 중앙 조직이 각 도메인에서의 이니셔티브로는 해결이 어려운 보안·안전·인프라·비용 문제를 지원 • 구체적으로 중앙 조직은 전사 AI 정책·규칙 수립, 부문별 AI 활용 수준·품질 모니터링, 안전한 개발 플랫폼 제공 등을 통해 도메인을 지원 가능 - 특히 모니터링과 개발 플랫폼은 자동화·구조화하여 연속성을 담보

출처 : 일본 PwC (2026.8.4.)

<https://www.pwc.com/jp/ja/knowledge/thoughtleadership/ai-ready-manufacturing.html>



주요 동향(2) : ICT

1 AI 글래스, 차세대 사용자 인터페이스 경쟁 본격화

➔ 몰입형 XR 헤드셋에서 일상형 AI 글래스로 경쟁축 이동

- 상황을 먼저 읽는 AI가 안경형 인터페이스 경쟁을 촉발
 - 지난 십수 년간 디지털 서비스와 AI 이용의 중심은 스마트폰이었으나, 최근에는 착용한 상태에서 AI를 곧바로 이용하는 AI 글래스가 차세대 인터페이스 후보로 거론되는 국면
 - 이러한 변화의 배경에는 AI가 명령에 응답하는 단계를 넘어 주변 상황을 스스로 판단하는 방향으로 발전하면서, AI를 이용하는 기기의 형태가 사용자 경험의 차이를 만들기 시작한 점이 자리하고 있음
 - 실제로 주요 사업자들이 몰입형 XR 헤드셋에 집중했던 개발 자원을 일상 착용이 가능한 경량 AI 글래스로 옮기면서, 시장의 무게중심도 함께 이동
 - 이러한 흐름과 함께 AI 글래스 출하량은 '25년 870만 대로 전년 대비 322% 증가했으며, 신규 사업자의 시장 진입이 이어지면서 '26년에는 1,500만 대를 넘어설 전망 (Omdia, '26.3.)
 - 특히 '26년 2분기 주요 빅테크의 신제품 발표가 집중된 데 이어 3분기 출시도 잇따라 예고되면서, 복수의 대형 사업자가 처음으로 같은 시기에 제품 경쟁을 벌이는 국면에 진입
- 1세대와 달라진 기술적 전제, 대중화 조건은 여전히 미충족
 - 10여 년 전 등장한 1세대 스마트 글래스는 일상적으로 착용하기 어려운 외형과 부족한 콘텐츠, 제한적인 기능이 복합적으로 작용해 대중 시장에 정착하지 못한 것으로 평가
 - 반면 현재는 부품 소형화로 무게와 외형이 일반 안경 수준에 근접하고, 생성형 AI가 실시간 통역과 사물·장소 인식 등 체감 가능한 기능을 제공하면서 과거와 다른 기술적 여건이 형성
 - 다만 기술 여건의 성숙이 곧 대중화를 보증하는 것은 아니므로, 매일 착용할 만큼의 효용을 확보할 수 있는지가 차세대 인터페이스로 정착하는 핵심 변수

➔ (상호작용 변화) 입력 중심에서 상황 인식 중심으로 이동하는 AI 이용 방식

- 상황을 기기가 파악해 검색어 입력과 화면 조작 단계를 축소
 - 스마트폰에서 AI를 이용하려면 기기를 꺼내 앱을 실행하고 눈앞의 상황을 검색어나 사진으로 변환해 입력해야 하므로, AI 이용이 늘어날수록 반복적인 조작 부담도 함께 증가
 - 반면 AI 글래스는 착용자가 바라보는 장면과 음성, 위치, 시간 정보를 카메라·마이크로 곧바로 수집하므로, 사용자가 처한 상황을 일일이 설명하거나 직접 입력해야 하는 부담이 감소
 - 이에 따라 번역, 길 안내, 사물 인식도 촬영 후 질문을 입력하는 방식에서 대상을 바라보며 즉시 질문하고 답변을 받는 방식으로 바뀌고, 필요한 정보를 확인하는 데 걸리는 시간도 단축
 - 결국 AI 글래스의 핵심 가치는 화면을 작게 만드는 데 있지 않고, 이용자가 현재 상황을 검색어나 사진 등 AI가 인식할 수 있는 형태로 변환해 입력하던 과정을 기기가 대신 처리하는 데 있음
- AI가 에이전트로 진화하며 시야·음성 확보가 새로운 실행 조건으로 대두
 - AI 비서가 여러 기기와 앱을 넘나들며 작업을 수행하려면 이용자의 상황과 진행 중인 과업을 연속적으로 파악해야 하지만, 현재는 이용 환경이 기기와 앱별로 나뉘어 작업을 그대로 이어 가기 어려운 상황
 - 이러한 한계를 배경으로 AI는 질문에 답하는 기능 위에 주변 상황을 스스로 판단해 필요한 작업까지 처리하는 에이전트 역량을 더해 가는 방향으로 발전하는 상황
 - 에이전트가 이용자의 의도를 파악해 다음 행동까지 미리 준비하려면 시야와 행동, 주변 환경을 끊임 없이 읽어야 하므로, 상시적인 맥락 확보가 기능 작동을 위한 필수 전제 조건에 해당
 - 이에 맞춰 제조사들도 카메라·마이크가 수집한 정보에 개인의 일정과 위치, 선호 데이터를 결합해 다음 행동을 미리 제안하는 방향으로 제품을 설계하는 추세
 - 이러한 구조가 자리 잡으면 AI 비서가 여러 앱과 서비스를 연계해 과업을 처리하고 이용자는 주요 단계만 확인하게 되면서, 기기를 고르는 기준도 상시적인 맥락 확보 역량으로 이동할 전망
- 출하량 급증에도 이용은 단순 기능에 집중, AI 글래스만의 효용 입증은 아직 미흡
 - 다만 이러한 이용 방식의 전환은 아직 기업의 제품 구상과 전망에 가까우며, 실제 이용 행태와 반복 사용으로 이어지는지는 별도의 시장 검증이 필요한 단계

- 실제로 화면 없이 음성으로 답하는 음성형 AI 글래스는 '26년 1분기 출하량이 전년 동기 대비 167% 늘었으나, 이용은 착용자 시점 촬영과 음악·통화에 집중 (IDC, '26.6.)
- AI 글래스는 번역·길 안내에 필요한 정보를 신속하게 제공할 수 있으나, 상대방과 번역 결과를 주고받는 양방향 대화나 복잡한 내용을 입력할 때는 화면을 갖춘 스마트폰이 여전히 편리하다는 평가
- 여기에 음성 비서나 번역 등 유사 기능이 이어폰, 스마트워치, 스마트폰에서도 제공되는 만큼, AI 글래스는 다른 기기로 대체하기 어려운 안경만의 효용을 별도로 입증해야 하는 과제에 직면
- 결국 관건은 기능의 많고 적음이 아니라 안경을 쓴 상태에서의 이용이 매일 반복할 만큼 자연스러운 습관으로 정착하는지에 있으며, '왜 반드시 안경인가'에 대한 답은 아직 미흡

➔ (기기 차별화) 현실 활동을 이어가며 AI 지원을 제공하는 상시 착용형 기기

- 시야를 가리지 않고 필요한 순간에만 개입하는 AI 기기
 - AI 글래스의 차별성은 연산 성능이나 화면 품질이 아니라, 사용자의 시야와 행동을 가로막지 않으면서 상황에 맞는 정보를 필요한 순간에만 제공하는 이용 방식에서 출발
 - 스마트폰은 화면을 직접 조작해야 하고 XR 헤드셋은 시야를 가려 장시간 착용이 어렵지만, AI 글래스는 주변 환경을 계속 바라보며 현실 활동과 AI 이용을 병행할 수 있음
 - 이러한 이용 방식의 이점은 주요 빅테크가 몰입형 기기보다 경량 제품에 개발 자원을 우선 배정하는 배경이며, 일상에서 장시간 착용할 수 있는지가 제품 개발의 핵심 판단 기준으로 작용
- 기존 스마트 글래스와 달리 시청각 정보를 AI가 이해하고 대응
 - 다만 현실 활동과의 병행은 음악·통화 중심의 기존 스마트 글래스도 갖춘 장점이므로, 같은 안경 형태 안에서 AI 글래스를 구분하려면 상시 착용 외에 별도의 기준이 필요
 - 기존 스마트 글래스가 음악 재생, 통화, 알림 확인처럼 미리 정해진 기능만 실행하는 반면, AI 글래스는 시야에 들어온 사물·문자·대화의 의미를 멀티모달 AI로 이해하고 응답을 생성

- 이러한 해석 능력을 바탕으로 번역·검색·요약 등 개별 기능이 하나의 대화 흐름으로 통합되고, 기기의 역할도 정해진 기능의 실행에서 사용자의 상황을 이해하고 지원하는 방향으로 확장
- 따라서 AI 글래스를 구분하는 핵심 기준은 착용자가 보고 듣는 정보를 이해해 다음 행동으로 연결하는 멀티모달 AI의 탑재 여부이며, 디스플레이는 결과를 전달하는 선택 사양에 해당
- 정보 제공 방식에 따라 음성형, 표시형, 공간 XR형으로 분화
 - 멀티모달 AI가 시청각 정보를 해석하는 공통 기반으로 자리 잡으면서, AI 글래스는 정보를 전달하는 방식에 따라 음성형, 표시형, 공간 XR형의 세 유형으로 구분
 - (음성형) 화면 없이 카메라, 마이크, 스피커만으로 인식 결과를 음성으로 전달해 가장 가볍고 저렴하지만 지도나 문서 등 복잡한 시각 정보를 직관적으로 확인하는 데 한계
 - (표시형) 렌즈에 번역, 방향, 알림을 표시해 음성 안내의 한계를 보완하지만, 광학 부품과 배터리가 추가되면서 무게와 가격이 늘고 사용 시간은 단축
 - (공간 XR형) 양안 디스플레이와 위치 추적으로 정보를 현실 공간에 고정할 수 있어 작업, 교육, 엔터테인먼트에 유리하지만, 높은 가격과 무게로 장시간 착용에는 제약
 - 세 유형은 순차적으로 대체되는 제품 세대가 아니라 착용 시간과 필요한 정보량에 따라 용도가 구분되며, 사용 환경별로 요구되는 기능과 설계 수준도 달라짐
- 스마트폰을 대체하기보다 감지와 응답을 맡는 보완 기기로 발전
 - AI 글래스는 유형과 관계없이 안경 형태에 따른 연산 성능과 배터리 용량의 한계를 지니므로, 스마트폰과 성능을 겨루기보다 기능을 분담하는 보완 관계로 발전
 - 구체적으로 AI 글래스는 시선, 음성, 장면을 수집하고 결과를 즉시 전달하는 감지·응답을 맡고, 고부하 연산과 기존 앱·서비스의 실행은 스마트폰이 담당하는 역할 분담이 표준 설계로 정착하는 추세
 - 이러한 역할 분담은 AI 글래스의 배터리·발열 부담을 낮추는 동시에, 스마트폰에 축적된 데이터와 서비스를 별도 설정 없이 연속적으로 이용할 수 있게 해 이용자의 초기 도입 부담도 완화
 - 결국 단기적으로 AI 글래스는 스마트폰의 대체재보다 현실을 감지하고 AI를 즉시 호출하는 보완 기기에 가까우며, 스마트폰 및 기존 서비스와의 연계 완성도가 실제 사용 경험을 좌우할 전망

➔ (확산 조건) 기술적 제약과 사회적 수용, 수익 구조가 함께 걸린 대중화 과제

● (배터리) 제한된 용량과 상시 작동 기능이 사용 시간을 제약

- AI 글래스는 장시간 착용할수록 활용 가치가 커지지만, 연산을 스마트폰에 맡기더라도 주변을 지속적으로 감지하고 필요한 순간 즉시 응답하는 기본 동작만으로 상당한 전력을 소모
- 안경다리를 얇고 가볍게 만들수록 탑재할 수 있는 배터리 용량은 줄어드는 반면, 카메라, AI, 통신, 디스플레이가 함께 작동하면서 기능이 늘어날수록 실제 사용 시간은 더욱 단축
- 화면 탑재 제품은 음악 감상 등 가벼운 용도로는 수 시간 작동하지만, 번역, 길 안내, 영상 촬영을 연속 실행하면 사용 시간이 한두 시간 안팎으로 줄어 종일 착용 기준에 미달
- 배터리 용량을 키우거나 보조 전원을 연결하면 사용 시간은 연장할 수 있지만, 무게와 연결선이 추가되어 일반 안경처럼 부담 없이 착용할 수 있다는 본연의 장점이 약화
- 따라서 해법은 단순한 배터리 용량 확대가 아니라 작업 특성에 따라 기기, 스마트폰, 클라우드로 연산을 배분하고 상시 감지 및 대기 전력을 줄이는 저전력 설계에 있음

● (착용감) 무게 배분, 발열, 개인별 피팅이 종일 착용을 좌우

- 사용 시간을 늘리기 위해 배터리 용량을 확대하면 제품 무게도 증가하며, 안경다리에 탑재된 배터리와 칩의 하중이 코와 귀에 집중돼 장시간 착용을 제약
- 업계에서는 일반 안경처럼 종일 착용하려면 40g 안팎이 한계 무게로 거론되지만, 자체 연산 장치와 양안 디스플레이를 갖춘 제품은 이 기준을 초과하기 쉬운 상황
- 제품의 총 무게가 같더라도 배터리와 칩의 배치에 따라 좌우 균형과 압력이 집중되는 부위가 달라지므로, 실제 착용 피로도에는 무게 자체보다 배분 설계에 크게 좌우
- 고성능 칩에서 발생한 열도 안경다리를 통해 얼굴에 직접 전달되며, 방열 부품을 추가하면 무게와 부피가 다시 늘어나므로 연산 부하와 열원을 분산해 발열 자체를 낮추는 설계가 필요
- 아울러 착용감은 얼굴형, 코 높이, 시력 교정 여부에 따라 개인차가 크기 때문에, 도수 렌즈 제작과 안경테 조정을 담당하는 안경원·아이웨어 업계와의 협력이 제품 완성도를 좌우하는 요소로 부상

- 결국 무게 배분과 발열은 설계·소재의 문제이고 피팅은 유통 현장의 문제이므로, 전자기기 제조사만으로 해결하기 어렵다는 점이 착용감 과제의 특징
- **(광학 효율)** 렌즈의 빛 손실이 전력 소모와 제품 무게를 가중
 - 표시형 AI 글래스는 화면 구동에 별도 전력이 필요한 데다 렌즈 광학계의 빛 손실까지 보완해야 하므로, 음성정보보다 더 큰 배터리가 필요하고 제품 무게 부담도 커지는 구조
 - 소형 표시장치에서 생성된 빛은 렌즈 내부 광학계를 거쳐 눈에 도달하는 과정에서 상당 부분 손실되며, 특히 야외에서는 화면 식별이 가능하도록 밝기를 높여야 해 전력 소모가 더욱 증가
 - 이러한 부담을 완화하는 핵심은 광학계의 빛 전달 효율로, 효율을 높이면 동일한 밝기를 더 적은 전력으로 구현할 수 있어 배터리 크기와 무게, 발열을 줄이는 동시에 사용 시간도 연장 가능
 - 따라서 표시형 AI 글래스의 완성도는 최대 밝기나 해상도 같은 단순 사양뿐 아니라, 빛 전달 효율과 시야각, 사용자의 얼굴형에 따른 화면 정렬 허용 범위까지 종합해 판단할 필요
- **(프라이버시)** 촬영에 대한 불안과 불명확한 데이터 처리 책임이 일상 수용을 제약
 - 배터리, 착용감, 광학 성능이 부품 기술의 발전으로 개선 가능한 공학적 과제라면, 카메라를 탑재한 안경을 마주하는 주변인의 불안은 사양 개선만으로 해소하기 어려운 사회적 장벽
 - 일반 안경과 유사한 외형은 착용자에게는 장점이지만, 주변인은 카메라와 마이크의 작동 여부를 확인할 수 없어 자신도 모르게 촬영될 수 있다는 불안을 유발
 - 촬영 사실을 알리는 표시등도 밝은 야외에서는 식별하기 어렵고 물리적으로 가릴 수 있어, 주변인에게 촬영 여부를 알리는 보호 수단으로는 한계
 - 더 근본적으로 기기가 주변을 상시 인식하면 행인의 얼굴과 대화가 기업 서버로 전송될 수 있으나, 기기 사용자 동의 중심의 기존 개인정보 보호 체계로는 주변인 보호에 한계
 - 따라서 규제 정비 이전이라도 기기 내 처리, 자동 삭제·저장 제한, 작동 상태의 명확한 표시 등 주변인이 확인하고 신뢰할 수 있는 보호 장치를 제품 설계 단계에 반영하는 것이 대중화의 선결 과제
- **(수익모델)** 반복 이용과 판매 후 수익 확보가 시장 지속의 관건
 - 기기 설계와 사회적 수용성 문제가 해소되고 가격까지 낮아지더라도, AI 글래스를 매일 사용할 이유와 이를 수익으로 연결할 기반이 없다면 시장 확대는 일회성 구매에 그칠 가능성



- 음성형 AI 글래스의 평균 가격은 '26년 376달러에서 '30년 229달러로 약 40% 하락해, 소비자의 초기 구매 장벽도 빠르게 완화될 전망 (IDC, '26.6.)
- 그러나 활용 범위가 촬영이나 음악 감상 등 단순 기능에 머물면 반복 사용의 필요성이 낮아지고, 구독료나 서비스 이용료를 추가로 지불할 유인도 형성되기 어려운 상황
- 더욱이 가격 하락은 판매량 확대에 기여하는 반면 기기당 이익을 축소하므로, 하드웨어 사양만으로 경쟁하는 기업은 수익성 압박을 피하기 어려움
- 결국 판매 이후에도 수익을 확보하려면 앱 거래와 구독, 서비스 수수료 등의 수익원이 필요하며, 이는 반복 사용을 유도하는 기능과 개발자 수익을 함께 지원하는 생태계 구축의 문제로 귀결

➔ (플랫폼 경쟁) 단말부터 연산체계까지 연결하는 5계층 주도권 경쟁

- 경쟁 기준이 개별 단말 성능에서 생태계 결합 역량으로 이동
- 배터리, 착용감, 프라이버시, 수익모델 등 확산 제약 요인은 개별 제품의 사양 개선만으로 해결하기 어려워, 경쟁 범위도 단말 판매에서 기기와 서비스를 통합하는 생태계 구축으로 확대
- 본 고에서는 AI 글래스 생태계를 △단말 △운영체제(OS) △AI 비서 △앱·서비스 △칩·연산체계의 다섯 계층으로 구분, 각 계층이 유기적으로 연결될 때 일관된 이용 경험과 지속적인 수익 구조가 성립
- 단말은 착용 시간과 감지 데이터의 범위를, OS는 개인정보 접근 권한과 기기 연동 조건을, AI 비서는 상황 해석 수준과 외부 서비스 호출 방식을 각각 결정
- 앱·서비스 계층은 반복 이용과 과금 구조를 만들고, 칩·연산체계는 무게, 배터리, 원가의 한계를 규정해 다른 계층이 구현할 수 있는 기능의 범위를 결정
- 다섯 계층을 모두 자체적으로 확보한 기업은 없어, 초기 경쟁은 부족한 계층을 협력으로 보완하고 그 조합에서 이용자가 체감할 강점을 만드는 방향으로 전개

1. (메타) 아이웨어 유통망과 소셜 기반을 결합해 초기 시장 선점

- 메타는 아이웨어 전문기업과의 협력을 통해 다른 진영보다 먼저 제품을 출시하고 초기 이용자 규모를 확보하는 데 주력하며, 출하량 기준으로 시장 선두를 유지
- 특히 전자제품 매장이 아닌 안경원에서 도수 렌즈와 함께 판매하는 경로를 마련해, 자체 소매망이 없는 경쟁 진영이 단기간에 구축하기 어려운 유통 우위를 확보

- 여기에 30억 명 이상의 소셜 관계망, 광고 수익을 활용한 단말 가격 보조, 2년 이상 축적한 실사용 데이터가 더해지며 기기 사양만으로는 설명하기 어려운 시장 경쟁 우위를 형성
- AI 비서 계층에서도 외부 모델을 조달하는 진영과 달리 자체 멀티모달 모델을 적용해, 응답 속도와 지원 기능의 범위를 직접 조정 가능
- 다만 외부 개발자와 앱 계층은 아직 충분히 형성되지 않았고 새로운 기능을 이용자에게 노출·추천하는 경로도 자사 소셜·광고 플랫폼에 의존해 제3자가 이용 경험을 확장하기 어려운 상황
- 이에 더해 상시 감지 기능 시험 등을 둘러싼 프라이버시 논란도 지속되고 있어, 판매 규모가 확대될수록 이용자와 주변인의 신뢰 확보가 주요 과제로 부상 (FT, '26.7.)

2. (애플) 아이폰 이용 기반 위에 칩·OS·AI를 직접 연결하는 수직 통합 전략

- 메타가 빠른 출시를 통해 규모를 확보했다면, 애플은 칩, 기기, 소프트웨어를 직접 설계하는 수직 통합 방식을 유지하며 출시 시점보다 제품 완성도에 무게를 두는 전략
- 하드웨어 측면에서는 자체 저전력 전용 칩과 아이폰 연계 구조를 통해 안경 내부의 연산·배터리 부담을 낮추면서, 핵심 서비스와 데이터를 자사 기기 생태계 안에서 처리·관리하는 구조
- 아이웨어 부문에서도 외부 브랜드와 공동 제품을 개발하는 다른 진영과 달리 프레임을 자체 설계하는 방향으로 알려져, 부품 조달부터 외형까지 통제하는 수직 통합 기조가 유지될 전망
- 아울러 기기 내 데이터 처리 확대, 얼굴 인식·상시 녹음 배제, 촬영 없이 상황만 파악하는 감지 전용 카메라 검토 등 프라이버시 보호를 설계 단계부터 반영해 선두 진영과 차별화
- 다만 안경 소매망과 전용 앱, 실제 착용 데이터는 아직 갖추지 못했으며, 경쟁사가 시장 데이터를 축적하는 동안 출시가 늦어지는 부담도 존재

3. (구글) OS와 AI 비서를 중심으로 제조사·개발자 연합 확대

- 애플이 주요 계층을 직접 설계하는 방식이라면, 구글은 기기를 직접 생산하지 않고 OS와 AI 비서를 여러 제조사에 개방해 연합의 규모로 경쟁하는 플랫폼 방식을 채택
- 이를 위해 전용 OS를 협력 기업과 공동으로 운영하고 타사 스마트폰과의 연동도 허용해, 참여 제조사와 제품이 늘어날수록 플랫폼의 적용 범위가 확대 되는 구조를 구축



- AI 비서 계층에서는 자사의 검색, 지도, 메일, 일정 서비스에 축적된 이용 정보를 활용할 수 있어, 개인화 기반을 처음부터 마련해야 하는 단말 중심 진영보다 유리한 출발점을 확보
- 앱 계층에서도 별도의 생태계를 처음부터 구축하기보다 스마트폰용 앱을 음성형·표시형 안경에 맞게 전환·확장하도록 지원해, 신규 플랫폼의 최대 약점인 콘텐츠 공백을 기존 자산으로 보완
- 다만 출시 시점과 품질 및 가격에 대한 결정권이 협력사에 분산돼 있어, 제품별 이용 경험과 프라이버시 기준을 연합 전체에서 일관되게 유지해야 하는 과제가 병존

4. (삼성) 개방형 호환과 갤럭시 기기군을 결합한 연합 참여형 이원 전략

- 구글이 개방형 연합을 주도하는 플랫폼 사업자라면, 삼성은 연합의 대표 단말 사업자로서 호환 범위를 넓히는 동시에 자사 기기군의 연계 경험으로 차별화 하는 이원 전략을 추진
- 연내 출시 예정 제품을 갤럭시뿐 아니라 타사 안드로이드폰과 아이폰에도 연동할 수 있도록 설계해, 이용 대상을 자사 기기 보유자로 한정하는 폐쇄형 연동 진영보다 진입 장벽을 낮춤
- 글로벌 아이웨어 브랜드 젠틀몬스터·워비파커와 협업해 일반 안경과 유사한 디자인을 구현, 배터리는 1회 충전으로 최대 9시간 사용이 가능하며 충전 케이스를 이용하면 최대 7회 추가 충전 가능
- 갤럭시 워치로 통화와 음악을 제어하거나 버즈 터치로 AI 비서를 호출하는 전용 기능을 지원해, 개방형 호환을 유지하면서도 갤럭시 기기를 함께 사용할 때의 편의성을 강화
- 한편, 하드웨어 측면에서는 초슬림 힌지와 티타늄 등 경량 소재, 좌우 무게 배분과 방열 구조를 적용해 종일 사용할 수 있는 착용성을 주요 차별화 요소로 제시
- 다만 OS와 AI 비서를 구글에 의존해 플랫폼 운영과 AI 기능을 독자적으로 결정하기 어렵고, 가격과 출시 지역도 미정이어서 연합 참여가 실제 수익으로 이어질지는 아직 검증이 필요

5. (스냅) 제품 출시 전 AR 운영체제와 개발자 생태계를 선점

- 스냅은 완제품보다 개발 환경을 먼저 갖추는 전략을 선택하고 제품 출시에 앞서 안경 전용 OS와 개발 도구, 앱을 자체적으로 구축해 생태계 기반을 선점
- 출시 전 1년 반 동안 전용 OS를 열 차례 갱신하며 기능과 연동 규격을 40종 이상 확충했고, 첫 소비자용 제품이 나오기 전에 이미 수백 개의 전용 앱을 확보 (Snap, '26.6.)

- 다른 개발 환경에서 제작한 결과물을 이전하는 도구와 기존 코드를 활용하는 개발 키트를 제공해 외부 개발자의 진입 부담을 낮추고, 출시와 동시에 앱 구매·구독을 지원해 수익 창출 기반도 마련
- 다만 지도, 결제, 일정 등 일상 서비스를 연결하는 범용 AI 비서가 없어 반복 사용을 유도하기 어렵고, 2,195달러의 높은 가격도 초기 이용자 확대를 제약
- 결국 스냅은 콘텐츠와 개발자 생태계를 다른 진영보다 먼저 확보했으나, 이를 이용자 확대와 매출로 연결할 수 있을지는 불확실한 상황

6. (알리바바) 원가 경쟁력과 내수 서비스망을 활용해 반복 이용 기반 확보

- 스냅·구글이 외부 개발자를 통해 안경용 앱을 확대하는 방식이라면, 알리바바는 이미 보유한 생활 서비스망을 안경에 직접 연결해 자체 서비스만으로 반복 사용을 유도하는 구조를 구축
- 이러한 전략은 중국의 부품 제조 기반과 세계 2위 규모의 내수 시장을 토대로 추진되며, 정부의 소비 보조금도 자국 기업의 초기 수요 확대를 뒷받침
- 배달 주문, 여행 계획, 예매 등 자사 앱의 주요 기능을 안경에서 바로 실행하도록 지원해 일상적 사용 유인을 높였으며, 중국 내 온라인 누적 판매 점유율 53%를 기록하며 초기 시장성을 확인
- 여기에 시간, 위치, 이용 습관을 분석해 사용자의 요청에 앞서 필요한 정보를 제시하는 선제형 AI 비서를 적용함으로써, 질문에 답하는 데 머무는 기존 제품과 이용 방식에서 차별화
- 다만 자사 생활 서비스가 제공되지 않는 해외에서는 중국과 같은 이용 경험을 구현하기 어렵고, 현지 서비스 확대와 개인정보 보호에 대한 신뢰 확보가 과제로 남는 상황

7. (화웨이) 자체 운영체제(OS) 기반 기기 연동으로 화면·전력 제약을 보완

- 화웨이는 안경을 독립 기기가 아니라 자체 운영체제로 묶인 기기군의 한 축으로 두고, 일부 기능을 다른 기기에 분산해 안경의 무게와 전력 소모를 줄이는 전략을 채택
- 구체적으로 복잡한 연산은 스마트폰이 처리하고 촬영 화면은 위치에 표시하는 방식으로, 안경에 고성능 칩과 디스플레이를 모두 탑재하지 않고도 주요 기능을 구현
- 이를 통해 안경에 탑재되는 부품과 배터리를 줄여 중국 내 음성형 AI 글래스 중 가장 가벼운 수준을 구현하고, 장시간 착용에 유리한 조건을 확보
- 판매 과정에서도 검안과 도수 렌즈 장착을 광학 전문업체에 위탁해, 전자기기 제조사가 관련 설비를 직접 갖추는 부담을 완화 (Omdia, '26.4.)



- 다만 이러한 기능 분산의 장점은 자사 고급형 스마트폰·워치와 연동할 때 온전히 구현되므로, 제품의 강점이 자사 프리미엄 기기 보유자에게만 집중되는 한계가 존재
- 또한 외부 OS 이용자는 연동 대상에서 제외되고 개발자 참여 기반도 제한적 이어서, 화웨이 생태계 밖으로 이용자와 앱을 확장하기 어려움

8. (로키드) 복수 AI 모델 지원으로 지역 제약과 특정 생태계 종속 완화

- 자체 생태계를 중심으로 서비스를 제공하는 다른 진영과 달리, 로키드는 AI 비서를 직접 개발하지 않고 복수의 외부 AI 모델을 지원하는 개방형 구조를 채택
- 이용자가 국가와 용도에 따라 AI 모델을 선택할 수 있어 특정 지역에서 기능이 제한되는 제품과 달리 국가별 서비스 격차가 작으며, 실시간 번역도 89개 언어를 지원
- 앱 계층 역시 외부 개발자에게 개방해 3,000건 이상의 개발 제안 가운데 400건 이상을 승인 및 공개했으며, 자체 개발 부담을 낮추면서 기능 범위를 확대
- 이러한 개방 전략은 해외 시장 성과로 이어져, '26년 1분기 해외 매출이 전년 동기 대비 300% 증가하고 일본 클라우드펀딩에서도 역대 최대 실적을 기록 (DigiTimes, '26.6.)
- 다만 AI 경험의 핵심을 외부 모델에 의존하는 만큼 공급사의 정책이나 요금 변경에 따라 제품 기능이 달라질 수 있으며, 이용 데이터와 거래 수익이 자체 생태계에 축적되기 어렵다는 한계도 존재

→ (국내 산업 기회) 단말 경쟁력을 플랫폼 공동 설계 역량으로 확장

- 광학·디자인·완제품 경쟁력은 확보했으나 OS·AI 비서 주도권은 제한적
- 국내 기업은 글로벌 AI 클래스 경쟁에서 광학 부품과 프레임 디자인, 완제품 통합 등 단말 계층을 중심으로 입지를 넓히며 주요 글로벌 협력망의 공급 주체로 진입
- **(광학 부품)** 레티널은 표시형 제품의 핵심 부품인 광학 모듈을 독자 방식으로 개발하고, 일본 NTT·다이나북 등에 양산 제품을 공급한 실적을 바탕으로 해외 소수 기업이 주도하던 시장에 진입
- **(프레임 디자인)** 젠틀몬스터는 구글·삼성 인텔리전트 아이웨어의 첫 프레임 디자인 파트너로 선정되어, 개방형 연합이 선보일 초기 제품의 외형과 착용 기준을 구체화하는 역할을 담당

- **(보급형 완제품)** 시어스랩은 카메라 없이 30g 안팎 무게의 20만 원대 보급형 AI 글래스를 패션 플랫폼에 단독 출시하며 가격과 유통 접근성을 앞세워 대중 수요를 공략
- **(연합 참여)** 삼성은 완제품 설계와 글로벌 플랫폼 연합 참여를 병행해, 부품 공급 중심의 타 기업과 달리 기기 기획 단계부터 글로벌 생태계에 참여할 수 있는 위치를 확보
- 다만 OS와 AI 비서, 앱 유통 규칙은 글로벌 플랫폼 기업이 주도하고 있어, 부품 공급과 완제품 조립을 넘어 제품의 초기 설계와 기능 결정 과정까지 국내 기업의 역할을 확대하는 것이 과제
- 참조 설계 참여와 현장 실증을 통한 플랫폼 협업 기반 확보
 - 이를 위한 현실적인 대응은 독자 플랫폼을 새로 구축하기보다 해외 참조 설계 참여와 국내 산업 현장 실증을 병행해 기술·데이터·사업 실적을 축적하는 접근이 필요
 - 해외에서는 퀄컴이 칩·광학·제조 기업을 연결하는 참조 설계 프로그램을 운영하고 있어, 국내 기업도 제품 개발 초기부터 자사의 광학 기술과 피팅 기준을 설계안에 반영할 수 있는 통로를 마련
 - 국내에서는 정부가 AX-스프린트를 통해 숙련 작업자의 노하우를 작업 지침으로 구현하는 스마트안경 과제를 지원하며, 기업의 초기 개발과 현장 실증 부담을 낮출 수 있는 기반을 조성



출처: Forbes 외(2026.6.)

<https://www.forbes.com/sites/tiriasresearch/2026/06/03/how-ai-is-driving-wearable-tech-as-the-future-of-personal-computing/>

<https://www.frontiersin.org/journals/human-dynamics/articles/10.3389/fhumd.2026.1695869/full>

<https://omdia.tech.informa.com/blogs/2026/may/beyond-the-screen-architecting-user-centric-intelligence>

<https://home.cib.natixis.com/articles/smart-glasses-back-in-focus>

<https://www.ft.com/content/934c7699-30f7-4fb5-be53-d526eab22138>

<https://blog.google/products-and-platforms/platforms/android/android-xr-io-2026/>

<https://newsroom.snap.com/introducing-specs-augmented-reality-glasses>

<https://newsroom.snap.com/snap-launches-new-tools-for-specs-developers>

<https://www.reuters.com/technology/snap-bets-life-beyond-smartphones-with-2195-specs-augmented-reality-glasses-2026-06-16/>

<https://about.fb.com/news/2026/04/introducing-muse-spark-meta-superintelligence-labs/>

<https://about.fb.com/news/2026/06/meta-essilorluxottica-partner-launch-meta-glasses/>

<https://www.ft.com/content/ac282450-91a8-4597-8f60-9e6ef416865a>

<https://www.qualcomm.com/news/releases/2026/06/qualcomm-launches-snapdragon-start-to-enable-the-next-phase-of-p>

<https://techcrunch.com/2026/05/18/south-koreas-letinar-is-building-the-optics-behind-ai-glasses/>

<https://www.venturesquare.net/en/1092835/>

<https://www.themiilk.com/articles/aeba3f463?u=9a5578ca&t=ad011ef75&from=>

<https://www.themiilk.com/articles/aa96bde1e?u=9a5578ca&t=a5065f570&from=>

2 Black Hat USA 2026, AI 공격의 가속과 방어체계 전환

→ AI의 실제 침해 사례가 드러난 에이전트 실행환경과 신뢰 경계의 취약성

- (행사 개요) 공격기법 시연부터 방어·정책 논의까지 연결한 실증 중심 행사
 - Black Hat USA 2026은 '26.8.1.~6. 미국 라스베이거스에서 개최되었으며, 실습 교육과 주제별 전문 회의, 연구 발표를 순차 배치해 최신 공격기법 재현부터 대응 방안 논의까지 함께 진행
 - 올해는 동료 심사를 거친 연구 발표 100여 건과 교육과정 100여 개, 도구 시연 80여 건을 통해 새로 확인된 취약점의 작동 조건을 검증하고 실제 방어 체계에 반영할 대응 방안을 제시
 - 특히 공식 의제를 네 개의 주제 축으로 구분하고 사이버전 포럼을 신설하면서, AI 에이전트의 행동부터 하드웨어와 신원 체계의 취약성, 국가 차원의 대응까지 논의 범위를 확대
- (핵심 메시지) AI가 공격 단계를 연속화하면서 방어 검증 범위도 모델 밖으로 확대
 - '26년 7월 OpenAI는 내부 사이버 역량 평가 중 연구용 AI 모델이 격리된 평가환경과 외부 저장소를 연결하던 Artifactory에서 제로데이를 찾아 외부 인터넷 연결을 확보한 사고를 공개
 - 해당 모델은 평가 환경 내부에서 관리자 권한을 확보하고 인터넷에 연결된 다른 시스템으로 이동한 뒤, 탈취한 자격 증명과 추가 취약점을 연계해 Hugging Face의 운영 DB에 저장된 비밀 정보에 접근
 - 이 사례는 단순한 사고를 넘어 AI가 격리 환경에서 인터넷 접근을 획득해, 탈취한 자격 증명과 취약점을 이용해 외부 운영 시스템으로의 이동을 실제 환경에서 수행한 사례라는 점에서 주목
 - 또한 Black Hat USA 2026에서도 AI가 취약점 탐색과 권한 확보, 후속 시스템 접근을 연이어 수행하는 공격 양상의 변화가 두드러지며, 이에 따른 각 신뢰 경계의 취약성이 주요 쟁점으로 부상
 - 이러한 변화는 행사 공식 의제에서도 △AI 기반 자율형 위협 △시스템 안전성과 격리 한계 △신원·신뢰·통제 △사이버 충돌과 실전 대응의 네 가지 주제 축으로 구체화

➔ Black Hat 2026이 보여준 AI 시대 공격 양상의 변화와 대응 범위의 확대

1. (AI 기반 자율형 위협) AI가 연결하는 공격 준비와 판단 조작

- 공격 준비의 자동화 : 탐색·시험·수정을 하나의 반복 과정으로 연결
 - 기존 사이버 공격은 전문가가 취약점을 찾고 악용 가능성을 판단한 뒤 공격 코드를 작성·실행하는 순서로 진행돼, 방어자가 중간 과정에서 공격을 발견하고 차단할 여지 존재
 - 그러나 Black Hat USA 2026에서는 AI가 공격 가설을 세우고 시험한 뒤 실패 원인을 반영해 다음 행동을 다시 선택하면서, 사람의 직접 개입 없이 여러 공격 단계를 연속 수행하는 흐름이 부각
 - 이러한 자동화는 완전히 새로운 공격 원리를 만드는 것보다, 기존 취약점과 공격기법을 더 많은 대상에 짧은 시간 동안 반복 적용하는 효과에 집중
- 에이전트 판단의 조작 : 오염된 기억과 계획이 후속 행동에 영향
 - AI 에이전트가 이전 입력과 작업 결과를 기억하고 이를 다음 행동의 근거로 활용하면서, 실제 도구를 실행하기 전의 기억·계획·행동 선택 과정도 새로운 공격 대상으로 부상
 - 악성 입력이 판단 근거에 남으면 에이전트는 허용된 권한 안에서도 공격자의 목적에 부합하는 행동을 정상적인 업무로 선택할 가능성
 - 따라서 AI 기반 위협은 공격 실행 여부뿐 아니라, 에이전트가 어떤 정보와 작업 상태를 근거로 후속 행동을 선택하는지도 함께 검증할 필요

(1) (공격 준비) 취약점 탐색에서 공격코드 검증까지 하나의 반복 과정으로 연결

- 전문가가 반복하던 탐색과 시행착오를 AI가 연속적으로 수행
 - 공격 준비 자동화의 핵심은 모든 판단을 AI에 맡기는 것이 아니라, 코드 분석과 가설 시험처럼 결과를 비교·검증할 수 있는 반복 작업을 AI가 연속적으로 수행하도록 하는 데 있음
 - 이에 AI는 가능한 코드 경로와 공격 가설을 폭넓게 시험하고, 공격자는 공격 목표와 시험 조건을 정해 복잡한 결과의 유효성을 판단하는 방향으로 역할이 변화
 - 그 결과 공격 준비 역량을 좌우하는 요인도 공격자의 작업 시간과 인력 규모에서 AI에 투입되는 연산 자원과 수행 가능한 시험 횟수로 일부 이동
 - 다만 새로운 공격 원리를 해석하거나 복잡한 공격 경로의 유효성을 판별하는 작업에는 여전히 전문가의 판단이 필요해, 반복 작업의 자동화와 공격 준비 전반의 자율화를 구분할 필요

① (취약점 탐색) 취약점 후보 탐색과 검증 자동화로 연구 범위 확대

- 이러한 자동화는 사람이 분석할 프로젝트와 코드 경로를 직접 선별해야 했던 취약점 탐색 단계에서 우선 적용되어, 한정된 인력으로 검토할 수 있는 대상을 확대
- Unit 42가 개발한 NOVA는 여러 AI 모델과 전문 보안 도구를 결합해, 오픈소스 코드를 분석하고 취약점 후보 탐색부터 공격 코드 작성과 재현까지 연속 수행하는 연구 시스템
- Unit 42 발표에 따르면 NOVA는 두 달 동안 GitHub 등 오픈소스 저장소의 3,915개 프로젝트를 분석해 취약점 1만 4,090건을 확인했으며, 이 가운데 92%를 논리·설계 결함으로 분류
- 특히 기존 퍼징으로 찾기 어려운 신규 결함과 고위험 취약점이 다수 발견돼, 자동화된 분석이 기존 취약점의 재탐지에 그치지 않고 미보고 결함까지 찾아낼 수 있음을 확인

② (공격 실행) 취약점 발견 이후 권한 획득·외부 침해까지 연속 수행

- NOVA가 다수 프로젝트에서 취약점 후보를 찾아내는 탐색 범위를 넓혔다면, Prompt2Own은 발견된 결함을 재현하고 실제로 작동하는 공격 코드로 발전시키는 과정에 AI를 적용
- UC Riverside 연구진의 「Prompt2Own」은 실제 리눅스 커널 취약점을 대상으로 AI가 관련 코드를 분석하고, 결함 재현과 공격 경로 탐색을 거쳐 공격 코드를 작성할 수 있는지 검증
- 연구진 발표에 따르면 AI는 기존 공격 코드가 없던 신규 취약점에서도 LLM을 활용해 실제로 작동하는 악용 경로를 탐색해 공격 코드를 개발할 수 있음을 시연
- 이는 취약점 발견과 실제 공격 사이에서 숙련된 공격자가 담당하던 분석·시험 과정의 일부를 AI가 수행하면서, 공격 코드 개발에 필요한 시간과 비용이 줄어들 가능성을 시사

(2) (판단 조작) 악성 입력이 에이전트의 판단 근거에 남아 후속 행동까지 변경

- 도구 실행을 막더라도 오염된 기억과 계획이 정상 권한 안에서 행동 선택에 영향
 - AI 에이전트의 작동은 목표와 정보를 바탕으로 다음 작업을 선택하는 판단 단계와, 선택한 작업을 도구와 권한을 이용해 수행하는 실행 단계로 구성
 - 기존 방어는 에이전트가 사용할 도구와 권한을 제한하고 중요한 실행 전에 사람의 승인을 받도록 해, 실행 단계에서 발생할 수 있는 직접적인 피해를 줄이는 데 집중



- 그러나 악성 입력이 기억과 계획 등 판단 근거에 포함되면 에이전트는 허용된 권한을 벗어나지 않고도, 공격자의 목적에 부합하는 행동을 정상적인 작업으로 선택할 가능성
- 이 경우 개별 명령이나 실행 결과만으로는 정상 업무와 공격을 구분하기 어려워, 에이전트가 어떤 정보와 작업 상태를 바탕으로 행동을 선택했는지도 검증할 필요

① (기억·계획) 악성 지시가 기억에 남아 이후 행동 선택에 영향

- 판단 상태의 오염은 악성 지시가 현재 작업에만 영향을 미치는 데 그치지 않고, 기억에 저장된 뒤 이후 대화나 다른 에이전트의 판단 근거로 재사용될 때 장기간 지속될 가능성
- Check Point 연구진의 「No Tools Required」는 별도의 도구 실행 권한이 없더라도 에이전트 내부의 정보 전달과 작업 상태 관리 구조가 공격에 이용될 수 있다는 문제를 제기
- 연구진은 악성 지시가 에이전트의 내부 상태에 남은 뒤 이후 요청을 처리하는 과정에서 다시 사용되면서, 도구를 직접 조작하지 않고도 행동 선택에 영향을 줄 수 있음을 확인

② (업무 흐름) 오염된 판단이 후속 작업으로 전달돼 실제 실행으로 연결

- 에이전트 내부에 남은 악성 지시와 오염된 판단이 다른 세션이나 자동화 작업의 입력으로 전달되면, 현재 작업에서 끝나지 않고 실제 코드 변경이나 외부 작업으로 이어질 가능성
- Novee의 「Trusted Enough to Run」 실험은 Claude Code, Gemini CLI와 OpenAI Codex의 자동화 절차에서 이전 단계의 입력과 판단 결과가 후속 작업으로 전달되는 과정을 분석
- 연구진은 공격자가 조작한 작업 상태와 파일을 후속 실행 단계가 다시 검증하지 않고 신뢰할 경우, 악성 지시가 더 높은 권한을 가진 자동화 작업으로 전달될 수 있음을 확인
- 이는 단계마다 별도의 승인 절차가 있더라도 앞 단계의 정보를 그대로 신뢰하면, 오염된 판단이 정상적인 실행 절차를 거쳐 실제 코드 변경이나 외부 작업으로 연결될 수 있음을 시사

2. (시스템 안전성과 격리 한계) 공유 자원을 통한 보안 경계 우회

● 저장소·서비스·GPU에서 확인된 새로운 공격 경로

- 기존 AI 보안은 작업별로 별도의 샌드박스를 만들고, 파일·권한·인터넷 접근을 제한해 하나의 작업에서 발생한 침해가 다른 시스템으로 확산되지 않도록 설계
- 그러나 Black Hat USA 2026에서는 개별 실행 공간을 분리하더라도 여러 환경이 함께 사용하는 저장소와 서비스, 하드웨어의 연결이 격리 우회 경로로 작용할 수 있다는 문제가 부각
- 이에 공격 방식도 개별 격리 장치를 직접 무너뜨리는 데서 벗어나, 경계 밖에 남은 공용 자원과 연결을 이용해 다른 실행환경과 외부 시스템으로 접근 범위를 확대
- 따라서 격리 검증도 개별 실행 공간의 설정만 확인하는 방식에서 벗어나, 여러 환경이 공유하는 저장소·서비스·하드웨어의 권한과 전체 연결 관계까지 점검할 필요

① (공용 저장소) 패키지 반입 통로의 취약점을 이용해 외부 인터넷에 접근

- 기존에는 AI 작업에 직접적인 인터넷 접근을 허용하지 않고, 필요한 소프트웨어만 내부 공용 저장소가 외부에서 대신 받아 제공하는 방식으로 해킹과 정보 유출을 차단
- 앞서 언급한 OpenAI 사고에서 각 AI 모델은 별도의 샌드박스에서 작동했으나, 평가 환경 전체가 공통으로 이용하던 Artifactory 저장소가 실행 환경 간 분리를 우회하는 지점으로 작용
- 공용 저장소는 여러 실행 환경에 동시에 연결되고 외부 패키지 반입을 위한 제한적 인터넷 접근도 갖고 있어, 한 환경에서 확보한 권한이 측면 이동을 거쳐 외부로 이어지는 경로를 제공
- 해당 사례는 샌드박스를 개별적으로 분리하더라도 공용 저장소가 가진 권한과 외부 연결을 통해 한 실행 환경의 침해가 공통 시스템을 거쳐 외부 운영 인프라까지 확산될 수 있음을 보여줌판단과 책임은 사람이 유지하는 방식으로 이해

② (샌드박스) 서비스의 응답 차이를 신호로 이용해 내부 정보 전달

- 공용 저장소의 권한과 외부 연결이 접근 범위를 넓히는 통로로 이용된 데 이어, 외부에서 관찰할 수 있는 공유 서비스의 상태 변화도 격리 환경의 정보를 전달하는 우회 경로로 부상
- 「A Billion-User Blast Radius」 연구는 ChatGPT의 격리된 코드 실행 환경에서 발생한 상태 변화를 외부에서 관찰하고, 이를 조합해 간접적인 정보 전달 경로를 만들 수 있는지 검증



- 연구진은 파일을 직접 보내지 않고, 로그인 실패와 요청 제한처럼 외부에서 관찰할 수 있는 서비스의 응답 차이를 정보 전달에 이용
- 이는 네트워크 차단으로 파일이나 메시지의 직접 전송을 막더라도, 여러 실행 환경이 공유하는 서비스의 상태와 응답 차이를 이용하면 정보를 간접적으로 전달할 수 있음을 보여줌

③ (GPU 메모리) 메모리 오류를 이용해 다른 AI 작업과 서버 침해

- 기존 GPU 보안은 여러 AI 작업이 하나의 GPU를 함께 사용하더라도 작업별 메모리 주소와 접근 권한을 분리해, 다른 작업의 데이터에 접근하지 못하도록 차단
- GPUBreach는 NVIDIA GPU의 GDDR6 메모리에 로우해머 공격을 적용해 비트 오류를 일으키고, 메모리 위치와 접근 권한을 관리하는 GPU 페이지 테이블을 변조
- 연구진은 변조된 페이지 테이블을 이용해 다른 GPU 프로세스의 메모리를 읽고 쓰는 권한을 확보한 뒤, 암호키를 유출하거나 GPU에서 실행되는 AI 모델 코드를 변경
- 특히 GPU의 서버 메모리 접근을 제한하는 하드웨어 보호 기능이 작동하는 상태에서도 호스트의 최고 관리자 권한을 확보해 기존 보호조치가 차단하지 못한 공격 경로를 확인
- 이는 동일한 GPU에서도 프로그램별 실행 공간을 논리적으로 분리하는 것만으로는 충분하지 않으며, 물리 메모리 오류가 다른 작업과 호스트 시스템 침해로 확산될 수 있음을 보여줌

3. (신원·신뢰·통제) 검증된 코드와 계정도 사용 과정에서 악용

- 코드 변환·보안 검사·로그인 이후 단계에서 새롭게 확인된 공격 경로
 - 기존 보안관리는 소스코드와 도구, 사용자 계정이 최초 검사나 인증을 통과하면 확인된 동작과 권한이 이후 사용 과정에서도 그대로 유지된다는 전제를 바탕으로 운영
 - 그러나 Black Hat USA 2026에서는 정상적으로 검증된 코드·도구·계정도 변환·실행·재사용 과정에서 처음과 다르게 작동하거나 공격에 악용될 수 있음이 확인
 - 공격자는 새로운 악성코드나 가짜 계정을 만들지 않고, 정상 프로그램이 코드를 변환·검사하는 과정과 로그인 후 남은 인증 정보, 자동화 계정의 관리 권한을 재사용해 내부 시스템에 접근

- 그 결과 최초 검사와 로그인 통과 여부뿐 아니라, 실제 실행 단계의 동작과 인증 결과의 재사용 여부, 관리 권한의 사용 범위까지 지속적으로 확인할 필요

(1) (코드·도구) 안전을 확인하는 과정이 새로운 공격 경로로 전환

- 검사를 통과한 코드와 보안 도구도 변환·실행 과정에서 예상과 다르게 작동
 - 기존에는 검토를 마친 소스코드가 컴파일 이후에도 같은 방식으로 작동하고, 승인된 보안 스캐너도 별도의 위험 없이 정해진 검사 기능과 권한의 범위 안에서만 작동한다고 전제
 - 그러나 컴파일러는 명령의 실행 순서를 재구성하고, 보안 스캐너는 외부 입력을 내부 시스템의 높은 권한으로 처리하기 때문에 두 절차 모두 실제 코드 동작과 권한 사용에 직접적인 영향
 - 그 결과 소스코드에서 확인한 안전장치가 컴파일 뒤 다르게 작동하거나, 보안 스캐너의 높은 권한이 외부 코드 실행에 이용되면서 최초 검증 이후 새로운 공격 경로가 형성될 가능성

① (컴파일러) 코드 변환 과정에서 안전 검사와 시리제 사용 순서 변경

- 기존에는 개발자가 소스코드에 안전 검사를 넣고 검토를 마치면, 컴파일을 거친 실행파일에서도 검사 순서와 프로그램 동작이 그대로 유지된다고 전제
- 「C and Its Consequences」 연구에서는 컴파일러가 코드의 처리 순서를 바꾸면서, 안전 검사를 받은 값과 프로그램이 실제로 사용하는 값이 달라질 수 있음을 확인
- 이는 컴파일러가 검사할 때 읽은 데이터를 실제 작업 단계에서 다시 불러오도록 코드를 바꾸면, 검사 후 변경된 값이 별도의 안전 확인 없이 사용될 수 있음을 보여주는 사례
- 이는 소스코드에서 안전성을 확인했더라도 최종 실행파일에서는 처리 순서가 달라질 수 있어, 배포 전 실제 실행파일의 동작까지 다시 검증해야 함을 보여줌

② (보안 스캐너) 외부 코드 검사 권한이 내부 시스템 침해에 악용

- 기존에는 보안 스캐너가 외부에서 받은 코드를 검사해 위험 요소를 찾아내므로, 코드가 내부 시스템에서 실행되기 전에 공격을 차단하는 안전장치로 인식
- ZeroPath는 「Scanning the Scanners」를 통해 공격자가 조작한 코드 저장소를 보안 스캐너에 제출해, 검사 과정에서 악성코드를 실행하도록 만드는 공격 가능성을 확인



- 실험 결과 일부 스캐너는 저장소에 삽입된 코드를 실제로 실행했으며, 이 과정에서 운영 데이터베이스와 클라우드 접속 정보, OAuth 토큰 등이 노출될 가능성을 확인
- 이는 위험을 찾아야 할 보안 도구가 외부 코드와 내부 운영환경을 연결하는 통로가 될 수 있어, 스캐너의 코드 실행 방식과 접근 권한을 제어해야 함을 보여줌

(2) (신원·권한) 정상 인증 결과와 관리 권한이 다른 접근에 재사용

- 로그인과 권한 부여가 정상이어도 인증 이후 남은 정보와 권한이 공격 수단으로 전환
 - 기존 신원 보안은 사용자가 정상적으로 인증됐는지와 자동화 계정에 필요한 관리 권한이 적절하게 부여됐는지를 최초 로그인과 권한 설정 시점에 확인하는데 집중
 - 그러나 로그인 후 시스템에 남은 인증 결과와 자동화 계정에 계속 유지되는 관리 권한은, 처음 허용된 사용자·시점·업무에서 분리돼 독립적인 접근 수단으로 재사용될 가능성
 - 공격자는 새로운 신원을 위조하거나 권한을 생성하지 않고도 기존 인증 결과와 관리 기능을 재사용할 수 있으며, 시스템에는 이러한 행위가 정상적인 권한 행사로 기록될 가능성

① (패스키 인증) 로그인 결과를 재사용해 고(高)권한 사용자로 인증

- 패스키는 비밀번호 대신 이용자의 기기에 저장된 암호키로 신원을 확인하며, 비밀번호를 탈취하는 피싱 공격을 차단하는 안전한 인증 방식으로 활용
- SpecterOps의 「Pass-the-Passkey」 연구는 Windows 시스템 로그에 남은 패스키 인증 결과를 가져와, 다른 로그인 요청에 반복 제출하는 방식으로 인증을 우회
- Microsoft Entra ID가 이미 사용된 인증 결과의 재제출을 차단하지 못하면서, 공격자는 암호키를 훔치거나 해독하지 않고도 고권한 사용자로 인증
- 이는 패스키의 암호 기술이 무력화된 것이 아니라, 로그인 후 남은 인증 결과가 재사용된 사례로, 인증 정보의 저장과 유효기간·재사용 여부까지 관리해야 함을 보여줌

② (자동화 계정) 한 고객의 접근이 다른 고객의 관리 권한으로 확대

- 클라우드 자동화 계정은 반복적인 운영 작업을 수행하도록 필요한 관리 권한만 부여하고, 고객별 계정과 자원을 분리해 다른 고객의 시스템 접근을 차단

- Microsoft의 「Handle With Care」 연구는 Azure Automation의 취약점을 연계해, 한 고객 환경의 접근 권한이 다른 고객의 자동화 계정과 클라우드 관리 권한 탈취로 이어질 수 있는지 검증
- 연구진은 외부에 공개되는 기본 설정을 통해 다른 고객의 자동화 서비스에 접근한 뒤, 코드 결함을 차례로 이용해 해당 자동화 계정의 클라우드 관리 권한을 확보
- 이를 통해 다른 고객의 관리형 ID 토큰을 확보하고, 해당 계정에 부여된 정상 관리 권한으로 클라우드 자원을 생성·변경·삭제 할 수 있음을 확인
- 이는 정상적으로 발급된 자동화 계정도 다른 고객이 관리 권한을 탈취하면, 본래 운영 편의를 위한 기능이 고객 간 경계를 넘어 클라우드 자원을 통제하는 수단으로 바뀔 수 있음을 보여줌

4. (실전 대응) 개별 조직의 방어에서 국가 차원의 서비스 복원력으로 전환

- 개별 기업의 기술적 예방을 넘어 침해 이후까지 포괄하는 국가 차원의 대응으로 확대
 - 기존 사이버 대응은 개별 기업이 취약점을 보완하고 침입을 차단하면 공격을 조직 내부에서 통제할 수 있다는 전제 아래, 시스템별 기술적 예방조치를 강화하는 데 중점
 - 그러나 공격이 짧은 시간 안에 민간기업, 클라우드, 공공기관의 시스템으로 이어지면서, 단일 조직이 보유한 정보와 권한만으로 전체 경로와 피해 범위를 파악하기 어려운 상황
 - 이에 개별 보안기술의 침입 차단 여부만으로 대응 성패를 판단하기 어려워졌으며, 여러 기관의 정보와 권한을 연계해 공격 중 피해를 통제하는 국가 차원의 운영 역량이 중요
 - 이에 Black Hat USA 2026에서도 국가 사이버 역량과 실제 작전 수행이 주요 의제로 부상하며, 개별 조직의 위험관리를 넘어 필수 서비스를 유지·복구하는 민관 대응체계에 주목
- (대응 주체) 기업 중심 대응에서 정부·민간·국제 공조로 확대
 - 국가 차원의 실전 대응에서는 민간이 확보한 취약점·공격 행동 정보와 정부가 보유한 수사·제재 권한을 같은 대응 과정에서 활용할 수 있도록 역할을 조정하는 것이 핵심
 - 기술기업은 취약점과 공격 행동에 관한 정보를 보유하지만, 수사·제재 권한이 없고, 정부는 대응 권한을 보유하더라도 민간 시스템에서 발생하는 침해 상황을 실시간으로 확인하기 어려운 구조



- 이에 Sean Cairncross 백악관 국가사이버국장은 Black Hat 개막 세션에서 이러한 역할 차이를 보완하기 위한 정부·산업 간 정보 공유와 공격·방어 활동의 조정을 주요 방향으로 제시
- Black Hat이 신설한 사이버전 포럼도 실제 사이버 충돌을 가정하고 상황 분비와 의사결정, 기관 간 조정, 필수 서비스 복구 단계에서 정부와 민간의 역할을 구체적으로 논의
- **(보호 목표)** 침해 예방에서 필수 서비스 유지와 신속한 복구로 전환
 - 국가·민간의 대응체계가 마련되더라도 중요 인프라의 노후 시스템과 인력·예산 부족이 겹치면, 공격이 진행되는 동안 모든 시스템을 동일한 수준으로 보호하기는 어려운 상황
 - 이에 Black Hat 2026의 정부 패널 「AI와 새로운 사이버 복원력 시대」에서는 모든 침해를 막는 것보다 공격 중에도 필수 서비스를 유지·복구하는 역량에 우선순위를 둘 필요성을 강조
 - 패널에서는 이러한 접근을 적용한 사례로 미국 사이버보안·인프라보안청(CISA)의 CI Fortify와 캐나다 사이버보안센터의 Minimum Viable Canada를 실제 정책 사례로 소개
 - 두 정책은 필수 서비스 운영에 필요한 시스템을 먼저 선별하고, 일부가 중단되더라도 서비스를 이어갈 대체 운영 절차와 시스템별 복구 순서를 사전에 정하는 데 초점
 - 이에 대응 성과도 침해 건수와 차단율뿐 아니라, 공격 중 유지한 필수 기능의 수준과 중단된 시스템을 목표한 시간 안에 정상 운영 상태로 복구했는지를 함께 측정할 필요
- **(대응 범위)** 피해 복구에서 공격조직의 재건과 공격 재개 억제로 확대
 - 필수 시스템과 서비스를 복구하더라도 공격조직의 서버와 계정, 자금세탁 수단과 제휴 관계가 그대로 유지되면 동일한 조직이 다른 인프라를 이용해 공격을 재개할 가능성 상존
 - 이에 대응 범위도 피해 시스템을 정상화하는 단계에서 벗어나, 공격조직의 기술 인프라와 운영 인력, 자금 흐름과 제휴자 간 신뢰를 함께 약화하는 방향으로 확대할 필요
 - Black Hat의 LockBit 브리핑에서는 미국 FBI와 영국 국가범죄청이 국제 랜섬웨어 조직 LockBit을 해체하기 위해 수행한 크로노스 작전(Operation Cronos)의 과정과 성과를 공개

- 수사기관은 LockBit의 서버와 관리 시스템, 소스코드를 장악하고 피해자·제휴자 관련 정보를 활용해, 조직의 기술적 운영 역량과 제휴자 간 신뢰를 동시에 약화
- LockBit 사례는 AI 특화 대응은 아니지만, 공격 속도가 빨라지는 환경에서 기술 인프라와 조직 운용 기반을 함께 약화한 국제 공조 모델이라는 점에서 의미

4. (종합) 연속 공격에 따른 방어 범위 확대와 대응 기준의 재정립

- 즉시 결과를 확인하는 공격과 맥락을 판별해야 하는 방어 간 속도 격차
 - AI는 공격과 방어 양쪽의 작업을 자동화할 수 있지만, 목표 달성 여부를 판단하는 방식과 처리해야 할 정보가 달라 실제 적용 효과와 속도에서는 차이가 발생
 - 실제로 Dreadnode가 구축한 기업 인증 체계 모의 환경 실험에서 공격 에이전트는 다양한 경로를 반복 시험해 6분 이내에 해당 환경의 관리 권한을 확보 (Dark Reading, '26.7.)
 - 반면 방어 에이전트는 대량의 기록을 처리하는 과정에서 분석 범위를 유지하지 못해, 최초 경보 이후 이어진 추가 활동과 시스템 간 측면 이동을 놓치는 한계를 노출
 - 이에 공격은 성공 여부를 즉시 확인해 다음 경로 선택과 재시험에 반영하는 반면, 방어는 분산된 기록을 연결해 행위의 목적과 진행 맥락을 판별해야 하는 속도 격차가 형성
- 여러 공격 단계의 연계로 심화되는 공격과 방어 간 검증 범위의 비대칭
 - 공격 시도의 속도 증가에 더해, 공격은 하나의 취약점 악용에 그치지 않고 행동 선택과 인프라 접근, 권한 확보와 후속 시스템 이용이 순차적으로 연결 되는 공격 사슬로 진행
 - 공격자는 각 단계에서 확보한 정상 권한과 신뢰된 연결을 다음 단계의 접근 수단으로 이용해, 서로 다른 취약점과 시스템을 하나의 침해경로로 결합
 - 반면 방어자는 개별 명령이나 격리 설정, 최초 승인만 확인해서는 공격을 판별하기 어려워 전체 실행 흐름과 인프라 연결, 권한 인계와 서비스 영향을 함께 점검할 필요
 - 결국 공격자가 확인해야 할 범위는 성공 가능한 하나의 경로로 수렴하지만, 방어 범위는 공격이 통과할 수 있는 모든 경계와 침해 이후의 영향까지 넓어지는 비대칭이 심화



- 실제 악용 가능성과 피해 확산 범위를 기준으로 대응 우선순위 설정
 - 모든 취약점을 같은 기준으로 처리하기보다 실제 공격에 이용될 가능성이 높고, 하나의 시스템 침해가 다른 사용자·서비스·인프라로 확산될 수 있는 취약점을 먼저 식별할 필요
 - 대응 우선순위는 외부 노출 여부와 공격에 필요한 사전 권한, 공격자가 확보할 수 있는 최대 권한, 연결된 후속 시스템과 예상 피해 범위를 종합해 결정
 - 특히 개별 심각도가 낮은 취약점도 여러 시스템과 권한으로 이어지는 경로의 교차 지점에 있으면, 단독으로 심각도가 높은 결함보다 넓은 피해로 연결될 가능성
 - 따라서 개별 취약점뿐 아니라 과도한 권한, 공유 상태의 관리 미흡, 정보 출처 미확인과 단계 간 재검증 누락처럼 여러 공격 경로가 공통으로 이용하는 취약 요인을 우선 개선할 필요
 - 여러 경로가 교차하는 지점을 먼저 차단하면 제한된 대응 자원으로 다수의 공격 경로를 동시에 끊고, 공격자의 재탐색을 유도해 후속 침해의 진행을 지연할 수 있음

출처 : Black Hat 외(2026.8.)

<https://blackhat.com/html/press/2026-06-02.html>

<https://blackhat.com/html/press/2026-07-16.html>

<https://startwithidentity.com/blog/black-hat-usa-2026-recap/>

<https://www.techrepublic.com/article/news-black-hat-ai4-2026-ai-security-takeaways/>

<https://www.cybersecuritydive.com/news/administration-securing-ai-stifling-tech-innovation/827088/>

<https://www.straiker.ai/blog/black-hat-usa-2026-ai-security-talks>

<https://securitypointbreak.com/2026/08/04/zero-trust-infinite-vibes-inside-black-hat-2026/>

<https://unit42.paloaltonetworks.com/frontier-ai-vulnerability-burst/>

<https://www.cybersecuritydive.com/news/openai-hugging-face-hack-ai-models-black-hat/827167/>

<https://www.wired.com/story/the-most-dangerous-ai-hacking-techniques-still-have-human-input/>

<https://www.darkreading.com/cyber-risk/ai-browsers-zero-click-agent-hijacking>

<https://www.darkreading.com/application-security/ai-harnesses-potential-exploit-ops>

<https://www.darkreading.com/application-security/finding-and-prioritizing-vulnerabilities-no-easy-task>

<https://www.darkreading.com/cloud-security/researcher-claims-control-chatgpt-secure-sandbox>

<https://www.axios.com/2026/08/06/openai-hugging-face-black-hat>

<https://www.darkreading.com/application-security/when-appsec-scanners-become-supply-chain-attack-vector>

<https://www.darkreading.com/identity-access-management-security/flaws-passkeys-implementation-old-attacks-work>

<https://www.darkreading.com/cloud-security/default-azure-automation-setting-cross-tenant-identity-takeover>

3 미국, 중국산 오픈웨이트 AI 모델 규제 범위와 대체 비용 논쟁 확산

➔ 중국산 오픈웨이트 모델 확산으로 미국 규제 논의 재점화

- 저비용 기반 중국산 모델 확산과 안보 우려 속 규제 논의 재개
 - 중국산 오픈웨이트 모델은 자체 서버 구동이 가능한 개방성과 미국 폐쇄형 모델 대비 낮은 이용 비용을 앞세워 미국 기업의 AI 개발·서비스 현장으로 빠르게 확산
 - 모델 중개 플랫폼 오픈라우터(OpenRouter) 내 미국 기업의 중국산 모델 토큰 이용 비중이 '26년 들어 46%까지 상승하면서, 논의의 초점도 비용 절감에서 중국 중심 AI 생태계 종속 우려로 확대
 - 여기에 중국 문샷AI 키미 K3를 둘러싼 미국 AI 모델 무단 지식증류 의혹과 정부·국방·핵심 인프라 적용 시 정보 유출 가능성이 더해지며, '25년 보류됐던 규제 논의가 '26년 7월 재개
- 규제 수위 미정 속 대체 비용 둘러싼 실익 논쟁 확산
 - 트럼프 행정부는 특정 기업 엔터티 리스트 지정, 고위험 분야 이용 제한 등 다양한 수위의 규제 방안을 검토 중이며, 민간 이용까지 제한하는 전면 금지도 거론되나 대상과 수위는 미확정
 - 조지아공대는 중국산 모델을 고가의 폐쇄형 모델로 대체할 경우 미국 기업에 연간 30억~120억 달러의 추가 비용이 발생할 것으로 추산했으나, 제한된 표본에 기반한 시나리오 분석으로 불확실성 상존
 - 이에 규제로 얻을 수 있는 안보·기술보호 편익이 미국 기업의 비용 증가와 AI 생태계 위축을 상쇄할 수 있는지가 쟁점으로 제기되며, 선별 제재·미국산 오픈웨이트 육성 등 대안적 접근도 병행 논의

➔ 규제 논의의 쟁점 : 안보·기술 보호 편익과 산업 비용의 충돌

(1) 규제 추진 논거: 생태계 종속과 기술 유출 우려

- 미국 기업의 이용 확산과 중국 생태계 종속 우려
 - 오픈라우터 내 미국 기업의 중국산 모델 토큰 이용 비중은 '25년 상반기 4.5%, 직전 12개월 평균 11% 수준에서 '26년 2월 이후 매주 30% 이상으로 상승하며 단기간에 큰 폭으로 확대

- 코인베이스(Coinbase)는 비용 절감을 위해 중국산 모델을 채택하고, 모질라(Mozilla) 최고기술책임자도 GLM-5.2와 키미 K3를 업무에 활용하는 등 중국 모델의 실무 적용 사례 확산
- 중국산 모델이 미국 기업의 제품·서비스 개발 기반으로 자리 잡으며, 생태계 종속과 고위험 분야 보안 위험이 규제 검토의 근거로 작용
- 키미 K3의 무단 증류 의혹과 미국 기술 보호
 - 문샷AI의 키미 K3가 일부 벤치마크에서 오픈AI·엔트로픽의 최상위 모델과 경쟁할 수 있는 성능 공개, 미국 정부는 이러한 성능 향상에 미국 모델의 무단 증류가 활용됐다는 의혹을 제기
 - 백악관은 문샷AI가 엔트로픽의 폐쇄형 모델을 증류해 키미 K3를 개발했다고 주장했으며, 미국 재무장관 스콧 베선트도 무단 증류가 확인될 경우 제재할 수 있다고 경고
 - 반면 지식증류는 미국 기업도 모델 경량화 및 성능 개선에 사용하는 일반적 학습 방식으로, 기법 자체보다 약관을 위반한 결과물 추출 여부를 기준으로 대응해야 한다는 의견도 병존
 - 해당 의혹은 사실 여부와 별개로 중국산 모델 성능 향상 경로에 대한 불신을 키우며 미국 기술 보호를 위한 규제 논의를 촉발하는 계기로 작용

(2) 규제 신증 논거: 대체 비용 부담과 산업 전반의 파급 우려

- 비용 추산의 산출 근거와 불확실성
 - 규제로 중국산 모델 이용이 제한되면 기업들은 단가가 높은 폐쇄형 모델로 전환해야 하며, 이때 발생할 추가 부담의 규모가 규제 실익 판단의 핵심 변수로 대두
 - 조지아공대 다니엘 유 교수는 오픈라우터 토큰 이용량과 모델별 가격 차이를 토대로, 중국산 모델을 대체 시 오픈라우터 이용자에게 연간 약 20억 달러의 추가 비용이 발생할 것으로 추산
 - 스타트업 등 소규모 기업일수록 AI 비용이 원가에서 차지하는 비중이 커, 저렴한 중국산 모델의 강제 배제가 수익성 악화로 직결되는 구조
 - 다만 토큰 비중은 실제 지출과 다른 층위이고 오픈라우터가 전체 추론 시장의 일부만 포착해, 추정 근거의 정밀도가 낮아 비용의 과대·과소 여부와 무관하게 규제 수위와 범위의 판단 자체가 흔들릴 소지



- (가격 경쟁) 중국산 모델 배제 시 폐쇄형 모델의 가격 인하 압력 약화
 - 중국산 오픈웨이트 모델은 낮은 가격으로 미국 최상위 모델보다 유사한 성능을 제공하며, 기업의 선택지를 넓히고 폐쇄형 모델 사업자 간 가격 경쟁을 촉진
 - 글로벌 LLM 평균 추론 단가는 '26년 6월 100만 토큰당 2.07달러에서 7월 1.67달러로 약 19% 하락했으며, 실리콘 데이터는 저비용 중국산 모델 확산이 하락의 배경 중 하나로 분석
 - 같은 기간 오픈AI도 경량 모델의 가격을 80%, 중간급 모델은 20% 인하해, 저비용 모델의 확산과 미국 사업자의 가격 조정이 함께 진행되는 양상
 - 중국산 모델 제한 시 경쟁 압력이 약화돼 미국 기업의 모델 선택권과 가격 협상력이 축소될 수 있다는 우려 제기
- (수요·인프라) 모델 교체보다 AI 이용 축소를 선택할 가능성
 - 규제 단행 시 기업이 고가의 폐쇄형 모델로 전환하기보다, 수익성이 낮은 AI 기능 및 업무를 축소, 중단할 소지
 - 파운데이션 캐피탈의 자야 굽타는 미국 주요 산업·시스템이 자체 환경에서 운영할 수 있는 오픈웨이트 모델에 의존해, 전면 금지 시 AI 수요의 상당 부분이 소멸할 수 있다고 주장
 - 특히 미래 AI 수요를 전제로 차입을 통해 건설된 데이터센터는 모델 이용량이 예상보다 감소 시 가동률과 투자 회수에 부담 발생 가능성 존재
 - 규제 영향이 이용료 증가를 넘어 기업의 AI 도입 위축, 추론 수요 감소, 클라우드·데이터센터 등 인프라 투자 축소로 이어지는 연쇄효과로 파급될 소지

(3) 정책 방향: 선별 규제와 자국 모델 육성으로 수렴 조짐

- 광범위한 금지 규제에는 정부·산업계 모두 신중론
 - 엔비디아·메타·마이크로소프트 등 270여 개 기업은 공개서한을 통해 오픈웨이트 모델에 대한 성급하고 광범위한 규제를 경계해야 한다는 입장을 표명
 - 백악관은 중국산 모델의 규제 강화를 검토하는 반면, 상무부 내부에서는 이미 공개된 모델의 유통과 자체 구동을 차단하기 어렵다는 이유로 광범위한 규제의 실행 가능성에 의문 제기
 - 규제가 자국 혁신을 저해할 수 있다는 우려로 일부 강경 규칙안은 내부 논의 단계에서 무산된 것으로 관측

● 선별 제재와 미국산 오픈웨이트 육성의 구체화 동향

- 중국산 모델을 전면 금지하기보다 무단 기술 추출이 확인된 기업을 제재하고, 정부·국방·핵심 인프라 등 고위험 분야를 중심으로 이용을 제한하는 방안도 선택지로 거론
- 하워드 러트닉 상무장관은 중국산 모델에 대응할 수 있도록 미국 주요 AI 연구소의 오픈웨이트 모델 개발에 인센티브를 제공하는 방안을 검토하고 관련 기업들과 협의를 진행
- 산업계는 스타트업과 연구자의 컴퓨팅 접근 확대, 공용 데이터·개발도구·평가체계 투자 등 미국산 모델 경쟁력 강화 방안을 제안

출처 : South China Morning Post, 외(2026.8.)

<https://www.scmp.com/tech/tech-trends/article/3362583/potential-us-ban-chinese-ai-models-could-cost-american-businesses-us12b-year-report>

<https://www.axios.com/2026/07/20/ai-us-china-open-source-kimi>

<https://techcrunch.com/2026/07/24/as-us-weighs-response-to-chinese-ai-industry-urges-against-broad-open-weight-restrictions/>

<https://www.cnn.com/2026/07/07/chinese-ai-models-costs-us-openai-anthropic.html>

<https://mitsloan.mit.edu/ideas-made-to-matter/ai-open-models-have-benefits-so-why-arent-they-more-widely-used>

<https://www.wired.com/story/the-white-house-is-trying-to-figure-out-what-to-do-about-chinese-ai/>

<https://www.microsoft.com/en-us/corporate-responsibility/topics/open-weight/>

<https://apnews.com/article/china-ai-model-us-kimi-deepseek-a00bf637866fcd4d81f4fde28c9862ce>

4 中, 대미 드론 수출통제·인증 협력 중단 등 대응 조치 발표

→ 中, 美 제재에 맞선 대응 조치 4건 동시 발표로 미중 기술 갈등 재점화

- 中 당국, 드론 수출통제부터 안보 조사까지 4건의 조치를 동시 공고
 - 中 당국은 드론 수출통제와 거래 금지, 인증 협력 중단, 안보조사 4개 영역의 조치를 동시에 공고하며 美 연방통신위원회(FCC)와 국토안보부의 연이은 규제 조치에 대응 ('26.8.5.)
 - 같은 날 中 상무부는 美 기업·단체 7곳과의 거래 금지와 사무기기 안보조사를, 국가시장감독관리총국 산하 국가인증인가감독관리위원회는 의무 인증 협력 중단을 각각 공고
 - 수출과 제재, 인증, 조사 권한이 하루 만에 동시 발동되면서, 중국의 대응 수단이 개별 품목 규제를 넘어 여러 층위에 걸쳐 작동하는 형태로 넓어졌음을 보여주는 사례
- 국가 안보와 비확산 의무를 명분으로 앞세우며 美에 조치 철회를 요구
 - 中 상무부는 대외제재 방지법 등을 근거로 삼고 국가 안보와 이익 수호, 비확산 의무 이행을 명분으로 내세우며 이번 조치가 자의적 보복이 아닌 규범에 근거한 대응임을 강조
 - 중국은 美 FCC가 통신 운영과 시험기관, 드론, 소비자용 라우터, 해저 광케이블을 규제한 데 이어 '26년 7월 첨단 로봇 장비와 전력 인버터까지 대상을 넓혀 왔다는 점을 근거로 제시
 - 미국의 잇단 규제 조치가 양국 정상 간 합의를 위반하고 중국의 정당한 권익을 훼손했다며, 관련 조치의 즉각 철회를 요구하는 입장을 공식 성명으로 표명
 - 미국의 추가 제한 조치 시 재차 대응에 나서겠다는 경고까지 더해지면서, '26년 9월 시진핑 주석의 방미를 앞두고 협상 준비와 규제 확대가 동시에 진행되는 국면 형성

→ 품목 규제를 넘어 수출·거래·인증·조사 4개 영역으로 확대된 대응 조치

(1) 드론 수출통제: 전면 금수가 아닌 건별 심사로 공급 속도를 조절

- 中, 드론 대미 수출에 건별 심사를 적용해 공급 속도를 늦추는 방식 채택
 - 中 상무부는 이중용도 수출통제 리스트에 오른 무인기와 부품·기술의 대미 수출을 건별로 엄격 심사하고, 기존 허가 편의 조치는 더 이상 적용하지 않겠다고 공고에 명시

- 수출을 일괄 금지하는 방식이 아니라 심사 절차를 강화하는 방식이어서, 이중용도 통제 규정이 적용되는 대미 선적 전반에서 통관 지연이 발생할 수 있는 구조
- 심사 강도를 조정하는 것만으로 규제 수위를 높이거나 낮출 수 있어, 별도 조치 없이도 대미 공급 속도를 상황에 맞춰 관리할 수 있는 여지를 남긴 점이 특징
- 美 FCC의 드론 수입금지에 중국이 같은 품목의 수출 심사 강화로 대응
 - 美 FCC는 '25년 12월 중국산 드론 신규 모델의 수입을 금지한 뒤 일부 모델에 한해 허용하도록 완화했고, 중국은 이번에 같은 품목을 대상으로 대미 수출 심사를 강화
 - 중국은 세계 최대 드론 생산국으로 완제품과 핵심 부품의 공급 비중이 커, 이번 심사 강화는 美 제조사의 조달 일정에 차질을 일으킬 수 있는 요인 (CNN, '26.8.5.)
 - 양측이 수입 차단과 수출 통제를 주고받으면서, 드론을 조달하는 기업이 조달선을 여러 국가로 다변화하고 부품 재고를 미리 확보해 두어야 하는 부담이 커지는 국면

(2) 美 기업·단체 7곳 거래 금지: 검증·감시 기능 수행 기관이 대상

- 신장 제재를 지원한 기업·단체 6곳을 지정해 中 내 거래와 협력을 금지
 - 앞서 美 국토안보부는 신장 원자재 조달과 강제 동원 관여를 이유로 中 기업 43곳을 위구르 강제노동 방지법 목록에 추가('26.7.31.), 중국은 이를 이번 지정의 직접적 사유로 명시
 - 中 상무부는 신장 관련 美 제재를 지원했다는 이유로 Applied DNA Sciences 등 美 기업·단체 6곳을 대응 목록에 올려 中 내 조직·개인과의 거래와 협력을 일괄 금지
 - 지정 대상에는 생명공학·자원 분석 기업이 포함되며, 상당수는 공급망 추적과 노동 위험 평가, 인권 옹호처럼 기업의 규제 준수를 검증하는 업무를 맡아온 주체
 - 제품을 공급하는 기업이 아니라 제재 이행을 실무에서 뒷받침하는 검증 기능을 대상으로 삼은 것으로, 검증 업무 자체가 국가 간 통상 갈등의 대상으로 올라선 사례
- FCC 조치를 지원한 시험·인증업체 1곳을 별도 사유로 추가 지정
 - 美 FCC는 '26년 7월 국가안보를 이유로 인간형·사족보행 로봇과 전력 인버터의 수입을 금지했고, 상당수가 중국에서 생산되는 만큼 신형 중국산 로봇의 美 내 판매와 기기 인증이 함께 차단
 - 中 상무부는 애리조나주에 본사를 둔 시험·인증업체 Compliance Testing을 신장 사안과 분리해 대응 목록에 올리고, FCC의 중국 관련 조치를 지원한 점을 별도의 지정 사유로 제시

- 中 당국은 해당 업체가 中 기업의 정당한 권익을 훼손하고 국가 주권과 안보를 해치는 데 협력했다고 설명했으나, 구체적으로 어떤 방식으로 관여했는지는 밝히지 않음
- 美 규제 집행을 도운 제3자까지 제재 대상에 포함되면서, 시험·인증 사업자의 협력 관계 선택 자체가 새로운 부담으로 작용할 수 있음을 보여주는 사례

(1) CCC 인증 협력 중단: 시장 진입에 필요한 검사 절차 자체를 지연

- 中, CCC 공장 검사 협력 중단으로 美 전기·통신장비의 중국 수출 절차가 지연
 - 中 국가시장감독관리총국 산하 국가인증인가감독관리위원회는 의무 인증(CCC) 지정기관이 美 현지 인증기관에 위탁해 수행해온 美 생산시설 공장 추적 검사를 '26.8.5.부터 전면 중단
 - CCC 인증은 전기·가전과 컴퓨터, 통신장비, 자동차를 중국에서 판매하려면 반드시 받아야 하는 인증이어서, 이번 중단으로 미국산 제품의 중국 수출 절차가 한층 까다로워질 전망
 - 인증이 필요한 美 전자제품 제조사는 미국 밖에 있는 심사기관이나 미국 이외 지정기관을 새로 구해야 하는 상황에 놓이면서, 심사 비용과 인증 기간이 함께 늘어나는 부담 발생
- 美 FCC도 시험소 인정 개편 추진, 시험·인증이 양국 모두의 규제 수단으로 활용
 - 美 FCC도 앞서 '26년 4월 상호주의 협정을 맺은 국가의 시험기관에서 시험한 기기에 신속 심사를 적용하고, 협정이 없는 국가의 시험·인증기관은 인정하지 않는 방안을 제안
 - 이 제안이 확정되면 중국에 자리한 시험소와 인증기관이 제조사의 美 판매용 기기 인증 취득을 지원하기 어려워져, 중국을 거쳐 美 인증을 취득하던 경로가 좁아질 전망
 - 양국이 서로 상대국 인증기관의 역할을 제한하면서, 국경을 넘어 통용돼 온 시험·인증 결과의 상호 인정 체계가 국가 단위로 나뉘는 흐름이 나타나고 있음

(4) 수입 사무기기 안보조사: 규제 대상 품목 확대

- 中, 외국 SW 탑재 프린터·복사기를 안보조사 대상으로 지정
 - 中 상무부는 외국 시스템 소프트웨어(SW)를 탑재한 수입 프린터·복사기 등 사무기기가 국가안보에 영향을 줄 수 있다며 별도 안보조사에 착수, 규제 대상을 새 품목으로 확대

- 상무부는 조사에서 특정국·기업을 지목하지 않았으나, 이번 조사를 美 조치에 대한 대응의 하나로 명시하고 수입 현황과 국내 의존도, 산업 영향을 함께 점검한다고 공고
- 조사 대상 범위를 넓게 열어 둔 방식이어서, 확정 규제로 이어지기 전에도 사무기기를 중국에 수출하는 기업의 조달·계약 판단에 영향을 줄 수 있는 사안
- 美, 데이터센터 부품 수입금지 초안을 검토하며 규제 범위를 AI 인프라로 확대
- 中 발표에 앞서 美 트럼프 행정부가 광 트랜시버를 포함한 중국산 데이터센터 부품 신규 모델의 美 수입을 막는 안보 조치 초안을 준비 중인 것으로 보도 (Reuters, '26.8.5.)
- 해당 조치는 아직 확정되지 않은 초안 단계이나, 로봇과 전력 인버터 규제에 이어 데이터센터 부품까지 미국의 규제 범위가 단계적으로 넓어지는 흐름을 보여주는 사례
- 본격적인 규제 시행 이전 단계에서 사무기기와 데이터센터 부품이 각각 조사와 검토 대상에 오르면서, 양국이 규제를 검토하는 품목의 범위가 함께 확대되는 양상

출처 : AP 외(2026.8.)

<https://apnews.com/article/china-us-sanctions-drone-forced-labor-ad0b637298e9608c5351bca84debeb25>

<https://www.hani.co.kr/arti/international/china/1271606.html>

<https://www.yna.co.kr/view/AKR20260805151800083>

<https://www.reuters.com/world/asia-pacific/china-targets-us-firms-drone-exports-after-fcc-xinjiang-actions-2026-08-05/>

<https://edition.cnn.com/2026/08/05/china/china-us-sanctions-intl-hnk>



단신 동향

1. 해외

※ 제목 클릭 시 원문 링크(URL)로 연결됩니다.

국가	제목 (발간처 / 발간일)	주요내용
미국 	백악관, 수입 드론에 최대 100% 차등 관세 부과로 국가안보·자국 드론 산업 기반 강화 (Axios / 2026.08.14)	○ 트럼프 대통령이 국가안보 보호를 명분으로 수입 드론에 최대 100%의 관세를 부과하는 계획을 발표하면서 자국 드론 제조 기반 육성 본격화 - 러시아-우크라이나 전쟁으로 드론의 군사적 중요성이 부각된 가운데, 중국 등 해외 생산 의존으로 유사시 국방 수요에 대응하기 어려울 수 있다는 우려 지속 - 이에 열화상 등 안보 민감 기능을 갖춘 대형 드론에 100%, 부품·소형 드론에 25%, EU 등 주요 동맹국산에 15%, 영국산에 10%의 차등 관세 부과 방침 - 백악관은 관세가 국가안보와 방산 연관 산업 기반을 보호 하고 일자리 창출에 기여할 것으로 기대했으며, 무기 부품 공급망을 둘러싼 미·중 경쟁은 심화될 전망
	에너지부, 미국의 과학, 에너지 및 국가 안보 임무 강화를 위해 에너지부 산하 국립연구소 운영 지침 현대화 (에너지부 / 2026.08.13)	○ 미 에너지부는 세금 재원의 효율적 집행을 강화하고 국립 연구소 운영의 불필요한 행정 장벽을 제거해 연구진의 임무 집중도를 높이기 위한 국립연구소 운영 지침 개정안을 발표 - 에너지부는 국가 연구소 운영 요건을 전면 개정함으로써 세계적 수준의 과학 인력이 복잡하고 급변하는 안보 임무와 과학기술 개발에 전념할 수 있도록 지원하고자 함 - 이번 개혁안은 근로자와 대중의 안전, 핵 안보 기업의 통제 수준은 철저히 유지하되, 의회와 정부책임처(GAO) 및 국립과학원이 중복성과 무용성을 지적해 온 복잡한 지침 프레임워크를 대폭 간소화 - 이를 통해 에너지부 산하 국립연구소들이 기술 개발, 미국 에너지 안보 강화, 미국 혁신 주도, 그리고 과학 기술 분야에서 미국의 리더십 유지에 더욱 집중할 수 있도록 지원
	백악관, 민간기업에 공격적 사이버 작전 권한 부여... 정부 전유 사이버 대응의 민간 개방	○ 트럼프 대통령이 민간기업의 초국가 범죄조직 대상 공격적 사이버 작전을 정부 지휘·통제 아래 허용하는 대통령 메모에 서명하면서, 정부가 주도해 온 사이버 작전에 민간 참여 확대 - 강력한 AI 모델의 확산으로 사이버 공격 우려가 커지는 가운데, 올해 미국에서는 수처리 시설 등 핵심 인프라 해킹과 해외 범죄조직의 랜섬웨어·금융사기 위협 지속

국가	제목 (발간처 / 발간일)	주요내용
미국 	(The Guardian / 2026.08.13)	- 이에 국토안보부(DHS)와 법무부가 공동 감독 프로그램을 신설하고, 검증된 참여기업에 지정 표적 대상 사이버 감시·공격을 허용하되 100만 달러(약 14억 원) 이상의 보증금 유지 의무 부과 - 다만 민간기업의 국제 사이버 분쟁 개입에 따른 확전 위험과 법적 책임 범위를 두고 법률 전문가들의 문제 제기 지속
	백악관, 신규 AI 모델 출시 전 안전성 검증 프레임워크 확정... 기준 비공개로 투명성 논란 (The Guardian / 2026.08.07)	○ 백악관이 신규 AI 모델의 안전성과 사이버보안 위험을 출시 전 검증하는 체계를 확정했으나, 세부 기준을 공개하지 않으면서 투명성 논란 확산 - Anthropic의 Mythos 모델 공개 보류를 계기로, 백악관은 6월 행정명령을 통해 신규 모델을 출시 최대 30일 전 정부에 자발적으로 제출하는 검토 체계 마련 - OpenAI, Anthropic, 메타, 구글 등과 비공개 협의를 거쳐 자발적 검증 절차를 확정했으나, 검증 기준은 일부 기업에만 공유하고 오픈소스 모델은 대상에서 제외 - 검증 수준과 안전 기준이 공개되지 않아 AI 활용 기업과 외국 정부의 불확실성이 커지고, 외부 연구자와 보안 전문가도 정부 평가를 확인하기 어렵다는 우려 제기
	에너지부, 핵심 광물 인력 육성 및 국내 공급망 강화를 위한 1억 달러 규모 이니셔티브 출범 (에너지부 / 2026.08.07)	○ 미 에너지부는 에너지 자립 및 핵심 광물 공급망 안보 강화를 목적으로, 총 1억 달러 규모의 차세대 전문 인력 양성 이니셔티브인 'PROSPECT' 계획의 공식 출범을 발표 - 미국은 국방 및 첨단 제조업에 필수적인 핵심 광물 공급망 전반의 구인난을 해소해야 하며, 특히 향후 10년간 광업 분야에서만 약 6,000명의 신규 엔지니어가 추가로 필요한 심각한 공급 격차에 직면 - 이에 대응하는 'PROSPECT' 이니셔티브는 핵심 광물의 국내 생산, 가공, 회수 및 재활용 전문 인력을 확충하기 위해 관련 분야 학위를 가진 대학 졸업자 수를 향후 2년 안에 2배로 증대시키는 것을 단기 목표로 추진 - 이를 달성하기 위해 정부는 대학 장학금 지원 및 학자금 보조를 확대하고 혁신적인 맞춤형 교과과정과 교수 도구를 도입해 차세대 공학 전공자와 전문 기술 인력을 대대적으로 육성할 방침

국가	제목 (발간처 / 발간일)	주요내용
일본 	방위백서 채택... AI·드론 등 신전쟁 방식 대응과 자국산 전투 드론 개발 우선 추진 (AP / 2026.08.18)	○ 일본 정부가 우크라이나·중동에서 부각된 AI·드론 중심의 새로운 전쟁 양상에 대한 대응과 방위산업 강화를 담은 연례 방위백서를 각의에서 채택하며, 중국을 최대 전략적 도전으로 재확인 - 백서는 태평양 내 중국 군함 활동 확대와 중·러 연합 폭격기·함정 작전, 북한의 극초음속미사일 개발 등을 중대한 안보 우려로 지목하고 남서부 도서 전력 증강과 장거리 순항미사일 배치를 병행 - 이와 함께 인구 감소에 따른 병력 부족을 무인장비로 보완하기 위해 국산 연안 방어용 전투드론 개발을 우선 추진하고, 방위장비청은 4개 제조사를 선정해 8월 초 해상자위대 시험에 착수 - 아울러 살상무기 수출금지 폐지 이후 호주 호위함 11척 공동개발 등 방산 수출로 산업 기반 확충을 추진하지만, 상용드론 시장을 중국산이 장악하고 있어 완전한 국산화에는 난항 전망
	「과학기술지표 2026」 발표 (과학기술·학술정책연구소 / 2026.08.07)	○ 일본 과학기술·학술정책연구소(NISTEP)는 「과학기술지표 2026」을 발간 - 과학기술지표는 과학기술 활동을 객관적·정량적 데이터를 바탕으로 체계적으로 파악하기 위한 기초 자료로, 약 160개의 지표를 통해 일본 및 주요 국가의 현황을 나타내고 있는 자료 - 산학관을 합친 연구개발비와 연구자 수는 주요국 중 중국과 미국에 이어 3위를, 총 논문 수는 5위를 유지했으나, 주목도가 높은 논문의 수는 4년 연속 13위를 기록 - 일본은 '20년대에 접어들면서 기업 부문 및 대학 부문 등의 연구개발비는 증가 추세이며, 박사과정 입학자 수가 3년 연속 증가하는 등 변화 조짐이 나타난 반면, 중·고기술 산업 무역수지 비율에서는 중국에 추월당해 2위를 기록 - 주요국의 순위 변동에서는 기업 부문의 연구개발비 및 산·학·관을 합한 총연구개발비에서 중국이 미국을 근소하게 앞지르며 1위를 기록

국가	제목 (발간처 / 발간일)	주요내용
일본 	‘AI for Science’ 관련 당면 정책의 방향성(안) (문부과학성 / 2026.08.04)	○ 일본 문부과학성은 제32회 인문학·사회과학 특별위원회를 개최하여 「인문학·사회과학의 추가 발전을 위한 ‘AI for Science’ 관련 당면 정책의 방향성(안)」에 대해 논의 - 인문학·사회과학을 포함한 일본의 과학기술·학술은 AI의 급속한 진전으로 역사적인 전환점을 맞이하고 있음 - 올해 3월 책정된 「제7기 과학기술·혁신기본계획」 및 「AI for Science 추진을 위한 기본전략 방침」에서는 AI가 모든 분야의 연구활동을 근본적으로 바꿀 수 있다고 밝히고 있음 - 본 방향성은 인문학·사회과학을 둘러싼 이러한 상황을 감안하여, 인문학·사회과학특별위원회에서 전문가 청취를 포함한 논의를 거쳐 인문학·사회과학 분야에서의 AI 활용의 의의 및 과제 등을 정리한 내용 - 향후 정책 방향은 ▲데이터, 지역, 분야, 연구자 간 연계가 가능한 네트워크 구축 ▲AI 활용을 전제로 한 데이터 구축 ▲시민, 지역에 묻혀 있는 자료의 활용 촉진 ▲선진 사례의 축적과 공유 ▲사회와의 연계 유지
중국 	엔비디아 H200 반입 제한 완화… 국산 칩 육성과 첨단 AI 모델 경쟁력 확보 병행 (Financial Times / 2026.08.19)	○ 중국 정부가 바이트댄스·텐센트 등 자국 AI 선도기업에 엔비디아 H200 칩의 본토 소량 반입을 허용하면서, 국산 칩 육성과 첨단 모델 개발 경쟁력 보완을 병행 - 화웨이 중심의 국산 반도체 육성을 위해 미국 승인 물량(기업당 최대 10만 개)의 대부분을 본토 밖에 두도록 통제해 왔으나, 최첨단 제조장비 부족으로 급증하는 수요 대응에 한계 - 이 같은 한계를 보완하기 위해 최근 바이트댄스와 텐센트가 각각 1만 개를 반입하고 홍콩 내 사용도 허용했으며, 구매에는 국가발전개혁위원회(NDRC)의 별도 승인 필요 - 이에 중국 기업들은 추론에 국산 칩, 훈련에 엔비디아 칩을 병행 활용하고 있으며, Moonshot K3 등 중국 모델과 미국 선도 모델 간 성능 격차도 좁혀지는 양상
	「2026년 중국 수소에너지 발전 보고서」 발표 (에너지국 / 2026.08.11)	○ 중국 국가에너지국은 「2026년 중국 수소에너지 발전 보고서」를 발표 - 보고서에 따르면, 중국의 재생에너지 기반 수소 생산 능력이 전 세계의 53%를 차지하며 수소 산업이 시범 탐색에서 규모화 발전 단계로 전환되고 있으며, 2026년 상반기 수소 분야 투자가 전년 동기 대비 160% 이상 성장 - 2025년 말 기준 중국의 수소 생산능력은 연간 5,100만 톤 초과(전년 대비 1.4% 증가), 연간 생산량은 3,900만

국가	제목 (발간처 / 발간일)	주요내용
중국 		톤 초과(7.3% 증가)를 기록했으며, 신재생에너지 수소 건설·운영 규모는 연 100만 톤을 초과 - 현재 저장·운송 인프라 미비, 수요 창출 지연, 핵심 소재 및 원천기술의 해외 의존도(현상 유지 또는 추종 단계) 등 초기 단계의 도전 과제에 직면해 있어 중국 정부는 제15차 5개년 발전 목표를 수립하고 정책·관리 체계 완성, 기술 혁신 심화를 통해 신형 에너지 시스템 구축을 가속화할 방침
영국 	글로벌 인재 비자(GTV) 적용 대상을 약 100개 혁신기업으로 확대 (연구혁신청 / 2026.08.07)	○ 영국 연구혁신청은 글로벌 우수 R&D 인재 영입을 통한 자국 혁신 산업의 성장을 목적으로, '글로벌 인재 비자(GTV)' 신속 보증 적용 대상을 7월 말까지 핵심 성장 분야의 약 100개 연구개발(R&D) 집약 기업으로 확대 지정하는 공식 조치를 발표 - UKRI는 보증 자금 지원 경로를 통해 지금까지 총 130개국 이상의 국가에서 온 12,500명 이상의 글로벌 우수 인재들이 영국에서 연구 경력을 계속 쌓을 수 있도록 지원해 왔음 - 이번 비자 제도 확대에 아스트라제네카, 재규어 랜드로버 등 영국 내 100여 개 연구 집약 기업이 공식 호스팅 기관으로 등록되었으며, 의학과 AI를 포함한 영국 정부 현대 산업 전략의 8대 핵심 고성장 분야에서 글로벌 인재를 직접 채용할 수 있게 되었음 - 이번 조치는 정부의 비자 자문위원회 및 주요 산업 협회들과의 긴밀한 민관 협업으로 실현되었으며, 글로벌 인재의 신속한 영국 유입을 도와 영국의 과학적 지식 진보와 혁신 경제의 성장을 가속할 것으로 기대
독일 	중소기업·스타트업 지원 강화를 위해 2027년 ERP 지원 규모를 120억 유로로 확대 (연방정부언론정보국 / 2026.08.12)	○ 독일 연방정부는 자본 조달에 어려움을 겪는 중소기업과 스타트업의 혁신 역량을 높이고 경제 자생력을 강화하기 위해 2027년 유럽부흥계획(ERP) 특별기금의 지원 규모를 약 120억 유로로 확대하기로 의결 - ERP 특별기금은 일반적인 정부 예산사업이나 민간은행이 아니라, 독일 경제정책을 지원하기 위한 장기저리 정책 금융 자산 - 독일재건은행(KfW)을 통해 저금리 용자, 긴 만기, 초기 상환 유예 조건의 창업 대출 및 지분 투자 자본을 제공 - 지원 규모는 총 120억 유로에 달하며, 신규 사업 추진과 초기 설비 투자 비용 지원에 활용되고 중소기업 및 스타트업의 제품·생산 공정·프로세스 디지털화와 핵심 기술 분야의 혁신 프로젝트를 지원

국가	제목 (발간처 / 발간일)	주요내용
독일 	연방 내각, 정보기관법 개정안 의결 (연방정부언론정보국 / 2026.08.12)	- ERP 특별기금은 지정학적 위기 속에서 독일 경제 기반인 중소기업과 스타트업의 성장 동력을 확보하고 기술 혁신을 촉진하고자 추진되었으며, 연방경제에너지부(BMW)가 관리하며, 창업 초기 기업의 자금 부담을 줄여 자율적인 연구개발과 시장 진출을 지원 ○ 독일 연방 내각은 하이브리드 위협 및 사이버 공격에 대응하기 위해 연방정보국과 연방헌법수호청의 기술적 수집 권한 및 AI 데이터 분석 역량을 대폭 강화하는 정보기관 법률 개정안을 의결 - 정보기관법 개정안은 사보타주, 스파이 행위, 사이버 공격 등 현대적 안보 위협에 능동적이고 기술적으로 대응하고 유럽 파트너 국가들과의 공조를 높이기 위해 추진 - 적대적 해커 그룹, 드론 공장, 화학무기 연구소의 IT 시스템 침입 및 서버 무력화 등 능동적 사이버 방어 권한이 부여되며, 사물인터넷부터 개인용 모바일 기기에 이르기까지 정보 기술 시스템에 대한 차등적 접근 및 침입 권한이 법적으로 신설 - BND의 전략적 수집 데이터를 사전 검토 없이 최대 12개월 까지 보관할 수 있어 위기 발생 시 즉각 활용 가능하며, 생체 인식 영상 대조 도구 사용, AI 활용, 연구개발 목적의 데이터 재처리 및 연방군 등 타 기관으로의 정보 공유 절차가 간소화됨
프랑스 	정부, 공공 사이버보안에 미스트랄 등 자국 AI 활용 방침 발표 (Reuters / 2026.08.18)	○ 프랑스 정부가 세무청 해킹으로 납세자 약 70만 명의 정보가 유출되자, 정부 서비스의 사이버 취약점 점검에 미스트랄 등 자국 AI를 활용하겠다는 방침 발표 - 재무부에 따르면 세무청 사이버 공격으로 납세자 약 70만 명의 데이터가 탈취됐으며, 월요일 추가 침해가 감지돼 피해 규모 파악 진행 - 이에 아미엘 예산장관은 정부 서비스의 취약점을 찾는 데 AI 도구를 도입하되, 계약 대상을 미스트랄 등 자국 사업자로 한정하고 OpenAI는 명시적으로 배제 - 잇단 해킹 사고를 계기로 공공 보안 분야의 자국 AI 조달을 공식화하면서 주권 AI 활용 기조 강화
EU 	IRIS ² 위성 네트워크 본격 배치를 위한 이행 협약 체결 (EU집행위원회 / 2026.08.07)	○ EU 집행위원회와 SpaceRISE 컨소시엄은 EU의 차세대 독자 위성 군집망인 IRIS²의 본격적 배치를 위한 이행 협약을 체결 - IRIS²는 ‘위성을 통한 회복탄력성, 상호연결성, 보안 인프라 (Infrastructure for Resilience, Interconnectivity and Security by Satellite)’를 의미

국가	제목 (발간처 / 발간일)	주요내용
EU 		- EU가 추진하는 안전한 위성통신·광대역 연결망 구축 사업으로, 유럽의 디지털 주권과 통신망의 안정성을 강화하는 것을 목표로 함 - 이행 협약에 따라 저궤도 위성 66기가 추가되어 전체 위성군은 총 348기(저궤도 위성 330기, 중궤도 위성 18기)로 확대되며, 이를 통해 EU 내 정부용 보안 통신 용량은 60%, 전 세계적으로는 54% 향상될 전망 - 사업 재원은 2028~2034년 EU 예산과 민간 투자, 회원국 및 제3국의 추가 출자로 충당될 예정 - 위성 통신 및 우주 과학기술 분야의 자립성을 극대화하고 2029년 첫 발사를 목표로 신속하게 추진하고, 유럽 우주국(ESA)과 에어버스 디펜스 앤드 스페이스(Airbus Defence and Space), 탈레스 알레니아 스페이스(Thales Alenia Space) 등 우주 항공 산업체들이 참여하는 민관 협력을 강화할 예정
	50억 유로 규모 '스케일업 유럽 펀드' 투입 본격 착수 (EU집행위원회 / 2026.08.04)	○ EU 집행위원회가 유럽 스케일업 기업의 글로벌 경쟁력 강화를 위한 50억 유로 규모의 '스케일업 유럽 펀드' 설립의 법적 절차를 완료하고 본격적인 투자 집행에 착수 - 이 펀드는 유럽의 뛰어난 과학기술 역량에도 불구하고 대규모 자금 부족으로 유망 기업들이 해외로 이탈하는 현상을 방지하고자 유럽혁신위원회(EIC) 펀드의 일환으로 마련됐으며, 공개 경쟁을 통해 선정된 사모펀드 EQT가 독립적 투자 관리자로 참여 - AI, 양자 기술, 바이오테크, 청정기술 등 핵심 과학기술 영역의 유망 스케일업 기업을 중점 지원할 예정이며, 세계 최대 연구 프로그램인 '호라이즌 유럽(Horizon Europe)'의 재정 지원을 바탕으로, 공공 및 민간 합작을 통해 목표액인 50억 유로 유치를 지속적으로 추진할 계획 - 노보 홀딩스(Novo Holdings), 알리안츠(Allianz), 발렌 베리 인베스트먼트(Wallenberg Investments) 등 강력한 민관 연합 펀딩을 기반으로 수 주 내 첫 투자를 집행할 예정이며, 역내 과학기술 성과물의 유출을 막고 글로벌 시장 선도 기업으로 육성할 방침
인도 	재무부, 전자제조 설비공급 외국기업 면세 2041년까지 연장... 對중국 대체 생산기지 육성 가속	○ 인도 정부가 폭스콘 등 위탁제조사에 장비를 공급하는 외국기업의 세금 면제 기간을 10년 연장해 2041년까지 적용하는 법안을 제출하면서, 중국 대체 제조기지 육성 가속 - '메이크 인 인디아' 정책에 따라 올해 도입한 면세 기간이 대규모 장기투자의 회수 기간보다 짧다는 업계 의견을

국가	제목 (발간처 / 발간일)	주요내용
인도 	(Financial Times / 2026.08.04)	반영해, 기업 활동 편의와 세제 예측 가능성을 높이기 위한 긴급 개정 추진 - 이번 개정안은 휴대폰·태블릿·노트북·서버·웨어러블 등 전자제품 제조에 적용되며, 수일 안에 의회를 통과할 전망 - 이 같은 지원 속 애플의 인도 생산 비중이 2022년 6%에서 2026년 26%로 확대될 것으로 전망되는 등 ‘차이나 플러스 원’ 공급망 다변화가 더욱 빨라지는 양상
튀르키예 	정부, 사이버보안법 시행으로 인터넷·소셜미디어 통제 권한 대통령실 집중... 디지털 검열 확대 논란 (Financial Times / 2026.08.09)	○ 튀르키예가 7월 말 발효된 사이버보안법을 통해 인터넷 서비스·게임 플랫폼·소셜미디어 감독 권한을 대통령실 산하 사이버보안청에 집중하면서 디지털 검열 우려 확산 - 자국 언론의 약 90%가 정부 통제 아래 있어 X·유튜브 등이 비판적 보도의 제한된 통로로 기능하는 가운데, 대역폭 제한과 계정 차단 등 접속 통제 관행 지속 - 신법은 사이버 공간을 국방에 준하는 영역으로 규정하고, 사이버보안청이 긴급조치를 명령하면 통신사·플랫폼이 2시간 안에 이행한 뒤 법원의 사후 심사를 받도록 함 - 여기에 15세 미만의 소셜미디어 계정 금지와 전자정부 포털 연계 연령 확인도 검토되면서, 이용자 신원과 계정 이력이 국가에 노출될 수 있다는 ‘디지털 판옵티콘’ 우려가 부상

2. 국내

※ 제목 클릭 시 원문 링크(URL)로 연결됩니다.

분류	제목 (발간처 / 발간일)	주요내용
과 학 기 술 정 보 통 신 부	과기정통부·행안부, 재난안전통신망 연동 스마트워치 및 AI 무전요약 시스템 개발로 재난현장 대응 역량 강화 추진 (과학기술정보통신부 / 2026.08.17)	○ 과기정통부와 행안부가 ‘국민생활안전 긴급대응연구’ 신규 과제로 재난안전통신망 연동 스마트워치와 AI 기반 무전 요약·알림 시스템 개발을 추진하면서, 재난현장 대응 역량 강화 - 경찰·소방 등 재난현장 대응인력은 재난안전통신망 단말기·무전기·휴대전화를 동시에 휴대·조작해야 하며, 상황 발생 시 교신이 집중되면서 핵심 지시와 정보를 신속하게 파악하기 어려운 문제 지속 - 이에 AI가 교신 내용을 분석·요약해 주요 정보를 제공하고 심박·피부온도·위치 등을 확인할 수 있는 스마트워치를 개발하며, 9월 7일까지 연구기관을 공모해 2년간 9억 원 내외의 연구개발비 지원 - 개발 기술을 현장에 적용하면 장비 휴대 부담을 줄이고 상황과 임무를 실시간으로 파악하는 데 도움이 될 것으로 예상되며, 이를 통해 재난 대응 역량과 인명·재산 피해 예방 효과 제고 기대
	과기정통부, 주파수 재할당 대가 산정 제도 개선 연구반 발족 (과학기술정보통신부 / 2026.08.13)	○ 과기정통부가 법률·경제경영·기술 등 분야별 전문가가 참여하는 연구반을 발족하고, 주파수 재할당 대가 산정 제도 개선에 본격 착수 - AI 시대에 주파수가 데이터 전송을 뒷받침하고 국가 경쟁력에도 영향을 미치는 핵심 인프라로 중요성이 커지면서, 효율적 이용을 유도하고 경제적 가치를 합리적으로 반영하는 대가 산정체계의 필요성 증대 - 그간 주파수 이용기간이 끝나면 이용자 보호와 서비스 연속성을 고려해 재할당을 추진하고, 전파법령에 따라 희소자원인 주파수의 경제적 가치를 반영해 재할당 대가를 산정·부과 - 연구반을 통해 주파수의 경제적 가치와 시장·정책 환경 변화, 해외 제도 동향 등을 종합적으로 검토해 주파수 재할당 대가 산정 제도 개선방안을 마련할 계획
	국가연구개발혁신법 시행령 개정으로 ‘민감 과제’ 신설 등 연구 보안 체계 강화 (과학기술정보통신부 / 2026.08.11)	○ 민감과제 분류 기준과 보안대책 수립기관 확대를 담은 「국가연구개발혁신법 시행령」 개정안이 국무회의를 통과하면서, 기술 패권 시대 국가 R&D 성과의 해외 유출 방지 체계 강화 - 보안과제의 일률적 확대가 연구현장에 부담이 될 수 있다는 점을 고려해 보안·일반과제의 중간 등급인 ‘민감과제’를

분류	제목 (발간처 / 발간일)	주요내용
과 학 기 술 정 보 통 신 부		신설하고, 국제협력은 제한하지 않되 핵심기술 정보의 해외 유출을 막기 위한 추가 보안절차 적용 - 보안대책 수립 의무를 보안·민감과제 수행기관, 출연연·국립연구소, 연간 300억 원 이상 정부 연구비를 지원받는 대학까지 확대하고, 성과 누설·유출 등 연구보안 부정행위에 참여 제한·제재부가금 등 제재 적용 - 8~9월 현장설명회 개최에 이어 10월까지 범부처 공통 「국가연구개발사업 보안지침」 고시를 제정하고 등급 분류 가이드라인을 발간하는 등 후속조치 추진 계획
	과기정통부, 국내 첫 자율실험실 산·학·연 협의체 출범으로 K-문샷 기반 연구 혁신 가속화 (과학기술정보통신부 / 2026.08.11)	○ 과기정통부가 80여 개 기관이 참여하는 국내 첫 자율실험실 (Self-Driving Lab) 산·학·연 협의체를 출범시키면서 AI 기반 과학기술 혁신과 K-문샷 프로젝트 지원에 본격 착수 - 자율실험실은 장비·로봇·AI를 연계해 24시간 실험을 자동으로 수행함으로써 연구기간을 수년에서 수개월로 단축할 수 있으나, 국내는 기관별 장비·데이터·운영 기준이 달라 개별 실험실 간 연계가 어려운 한계 존재 - 협의체는 서울대 정유성 교수를 위원장으로 기술·플랫폼 개발과 표준 정립, 표준형 자율실험실 구축, 수요기업 실증·민간 확산을 추진하며, 삼성종합기술원·SK하이닉스 등 기업 50개사와 30여 개 대학·연구기관 참여 - AI가 생성한 가설을 실험으로 검증하고 그 결과를 다시 학습하는 순환형 체계를 구축해 소재·바이오 등 첨단분야의 연구 속도와 재현성을 높이고 참여기관도 지속 확대할 계획
	국산 AI 반도체 실증·확산에 600억 원 투입, 퍼지컬 AI 등 22개 신규 과제 착수 (과학기술정보통신부 / 2026.08.06)	○ 과기정통부가 국산 AI 반도체 기반 3대 실증사업 합동 착수보고회를 개최하고, 올해 600억 원 이상을 투입해 22개 신규 과제에 착수하며 일상·산업 현장의 AI 융합 확산을 본격 추진 - AX 디바이스 개발·실증, AI 응용제품 신속 상용화, 온디바이스 AI 서비스 실증·확산 등 3개 사업을 통해 2027년 말까지 국산 AI 반도체를 활용한 제품·서비스 개발 추진 - 특히 물류·협동로봇, 소방진압용 사족보행로봇, 드론 기반 구조 지원 등 실제 환경을 스스로 인식·판단하고 움직이는 퍼지컬 AI 실증과제 7건에 신규 착수해 생활·안전 분야의 선도 사례 창출 계획 - AI 기반 통합보안 플랫폼, 교정 데이터 통합분석 플랫폼(법무부 협업), 도시 안전망 실증(천안시) 등을 통해 산업 생산성을 높이고 해외 진출에 활용할 실증 사례를 확보할 방침

분류	제목 (발간처 / 발간일)	주요내용
산업 통 상 부	테라파워-SK이노베이션 SMR 협력 합의로 한국 원전기업 수출 공급망 진입 확대 (산업통상부 / 2026.08.14)	○ 산업부 장관과 빌 게이츠 테라파워 이사회 의장의 면담을 계기로 테라파워-SK이노베이션이 글로벌 공동사업 추진 조건 합의를 체결하면서, 한국 원전기업의 해외 SMR 공급망 진입 확대 - AI 인프라·데이터센터 확대로 빅테크의 SMR 수요가 늘고 전 세계에서 100여 개 SMR이 개발 중인 가운데, 테라파워는 미국 와이오밍주에서 소듐냉각 방식 Natrium SMR(모듈당 345MWe)의 건설허가를 취득하고 2031년 상업운전을 목표로 건설 추진 - 한국 측은 SMR의 표준화·보급 확대를 위해 테라파워의 표준설계와 한국의 대량생산 공급망을 결합할 필요가 있다며, 50여 년간 구축한 원전 제조·건설 생태계와 중소·중견기업 중심의 제조 역량을 강점으로 제시 - 이번 합의로 SK이노베이션이 미국 및 해외 SMR 사업 개발에 참여할 기회를 확보했으며, 공급망 형성 초기 단계에서 대기업과 원전 중소·중견기업의 해외 SMR 공급망 진출도 확대될 것으로 기대
	산업부·육군·현대차 그룹, 국방 로봇·피지컬 AI 활용 확대 MOU 체결로 민·관·군 실증 협력 본격화 (산업통상부 / 2026.08.14)	○ 산업부가 육군·현대차그룹과 국방 분야 로봇·피지컬 AI 및 첨단기술 활용 확대를 위한 MOU를 체결하고, 3대 메가프로젝트인 피지컬 AI의 국방 적용과 국방 로봇 도입 확대 추진 - 민간의 첨단 피지컬 AI 기술을 군에서 신속히 실증하고 실제 전력화로 연계할 수 있는 협력체계가 필요한 가운데, 장병의 위험·반복 업무 부담을 줄일 수 있는 적용 분야 발굴 추진 - 산업부는 기술개발·실증 지원과 로봇기업-국방 수요 연계를, 현대차그룹은 인력·기술 지원과 장비 피드백을 반영한 성능 개선을, 육군은 테스트베드 제공을 담당하는 역할 분담에 합의 - 경제·경찰·지속지원·물류 분야의 로봇 도입을 확대하고 실증 결과를 제품 구매와 군 전력화로 연계해, 국방 등 공공 수요를 기반으로 국내 로봇의 양산 확대를 추진할 전망
	정부, 미래성장동력 ‘7대 SEED’ 프로젝트로 SMR·양자·우주 등 첨단기술 장기 육성 착수 (산업통상부 / 2026.08.12)	○ 정부가 관계부처 합동으로 미래성장동력 「7대 SEED」 보고회를 개최하고, 미래 청정에너지·차세대 프론티어·첨단 공급망 등 3대 분야의 첨단기술을 국가 차원에서 장기 육성하는 프로젝트 추진 - AI 확산에 따른 전력 수요 급증과 탄소중립 과제에 대응해 경수형 SMR의 '35년 상용화, 한국형 혁신 핵융합로 기반 '30년대 전력 생산, 페로브스카이트 탠덤셀·초대형 풍력터빈 등 재생에너지 기술 경쟁력 확보 추진

분류	제목 (발간처 / 발간일)	주요내용
산업 통 상 부		- 양자 분야에서 '29년 오류정정 100큐비트 QPU 확보와 K-퀀텀 파운드리 구축을 추진하고, '30년 민간 주도 달 착륙, '35년 저궤도 위성통신망 구축·BCI 제품 상용화 등 차세대 프론티어 분야별 목표 제시 - 핵심광물 재자원화율 20% 확대와 향후 5년간 10조 원 규모의 소부장 R&D 투자 등 첨단 공급망 역량을 강화하고, 민·관 합동 미래개척추진단 구성과 투자형 R&D 도입을 통해 범정부 지원체계 마련 방침
중 소 벤처 기업 부	「제2차 모두의 창업 프로젝트 추진계획」 발표 (중소벤처기업부 / 2026.08.13)	○ 중소벤처기업부는 비상경제본부 회의 겸 경제관계장관회의 겸 민생물가 특별관리 관계장관 TF 겸 국가창업시대 전략회의에서 관계부처 합동으로 「제2차 모두의 창업 프로젝트 추진 계획」을 발표 - 지난 3월 '1차 모두의 창업 프로젝트' 모집 결과, 정부 창업·아이디어 공모전 역대 최대 규모인 6만 3천여 명의 도전자를 기록했으며, 청년층(39세 이하) 도전자가 전체 신청자의 68%, 지역에서의 도전자가 53.4%를 차지하면서 전국적인 창업 열기를 입증 - '2차 모두의 창업 프로젝트'에서는 '모두의 창업'이 단발성 행사를 넘어 창업생태계에 진입하는 첫 시작점으로 안착하는 것을 목표로 5대 핵심과제를 추진 - 5대 핵심과제는 ①지원규모 확대 및 보육기관·멘토 확충, ②다양한 분야의 도전을 위한 특화 리그 운영, ③심사체계 공정성 강화 및 지원체계 고도화, ④창업의 일상화를 위한 전국 창업 문화 확산, ⑤플랫폼 보안성 강화 및 운영 거버넌스 구축
국 토 교 통 부	「제4차 공간정보산업진흥 기본계획 (2026~2030)」 수립 (국토교통부 / 2026.08.03)	○ 국토교통부는 「공간정보산업 진흥법」에 따라 「제4차 공간 정보산업진흥 기본계획('26~'30)」을 국가공간정보위원회 심의를 거쳐 확정 - 국토부는 디지털트윈·자율주행·로봇배송·스마트물류·AI 시티 등 신산업의 핵심 데이터 인프라로서 중요성이 커지고 있는 공간정보산업 경쟁력 강화를 추진 - AI가 읽고 분석할 수 있는 고정밀 3차원 공간정보를 구축하여 국토·도시·교통 등 다양한 분야와 쉽고 빠르게 융·복합 활용될 수 있는 기반을 조성하고, 강소기업 육성, 해외진출 지원 및 인재 양성을 추진해 공간정보 산업을 확장하여 신성장 동력을 창출할 계획 - 3대 추진전략은 전략 ① GeoAI 핵심 공간정보 구축, 전략 ② 공간정보 유통·활용 활성화, 전략 ③ 공간정보 산업 경쟁력 강화



과학기술 & ICT 정책·기술 동향

과학기술	ICT
■ 과학기술정보통신부 과학기술전략과 Tel : (044) 202-6735 E-mail : jms6551@korea.kr ■ 한국과학기술기획평가원 혁신전략기획센터 Tel : (043) 750-2670 E-mail : bchun@kistep.re.kr	■ 과학기술정보통신부 정보통신산업정책과 Tel : (044) 202-6223 E-mail : hara614@korea.kr ■ 정보통신기획평가원 동향분석팀 Tel : (042) 612-8240 E-mail : now2@iitp.kr