AI 기반 품목의 전략물자 통제 기준 및 방향 분석

2025. 11

과학기술정보통신부
KOSA KOREA AI-SOFTWARE INDUSTRY ASSOCIATION 한국인공지능·소프트웨어산업협회
성균관대학교 SUNG KYUN KWAN UNIVERSITY(SKKU)

제 출 문

한국인공지능·소프트웨어산업협회 회장 귀하

본 보고서를 「AI 기반 품목의 전략물자 통제 기준 및 방향 분석」의 최종보고서로 제출합니다.

2025년 11월

연구기관 : 성균관대학교

연구책임자 : 성균관대학교 교 수 이 태 진

목 차

표 목차

그림 목차

국문 요약

최근 AI 관련 하드웨어, 소프트웨어 기술이 고도화되고 성능이 개선되면서 다양한 민간용 및 군용 영역으로의 확산이 가속화되고 있으며 국제 무역 및 국가 안보 등에 미치는 영향력도 증대되고 있다. AI 관련 품목(하드웨어, 소프트웨어, 기술 등)의 수출통제 및 관리 필요성 역시 높아지고 있으며 미국을 비롯한 유럽, 일본 등은 AI 기술을 기반으로 한 전략물자에 대한 통제 대상과 범위를 점차 강화하고 있는 추세이다. 본 연구에서는 AI SW 품목에 대한 국내외 전략물자 수출통제 체제 및 통제 기준, 품목 사례 등을 파악하여 AI SW 관련 전략물자 통제 제도와 통제 대상을 이해하도록 한다. 또한 AI SW 품목의 기능 및 특성에 따른 분류를 기반으로 품목의 통제 가능성을 효과적으로 파악하도록 한다. 또한 수출통제 관련 정책적 대응 방안과 기업의 대응 방안을 제시하고, 품목 판정 가이드라인을 제공함으로써 AI 기반 품목의 산업 발전 및 기술 개발 선도와 함께 글로벌 컴플라이언스 확보에 도움이 되도록 한다.

영문 요약

Recent advancements and performance enhancements in AI-related hardware, software, and associated technologies have accelerated their diffusion into a broad spectrum of civilian and military applications. As a result, the influence of these technologies on international trade, national security, and strategic stability continues to grow. In parallel, the need for strengthened export controls and systematic management of AI-related items —including hardware, software, and technical data—has become increasingly pronounced. The United States, the European Union, Japan, and other major jurisdictions are progressively expanding and tightening the scope of controls applied to strategic items incorporating AI capabilities.

This report examines the export-control regimes and classification criteria applicable to AI software under domestic and international export control frameworks. It surveys relevant control lists, regulatory structures, and representative item classifications in order to establish a comprehensive understanding of the current control landscape governing AI-enabled items. Furthermore, the report develops a functional and technical categorization of AI software to support the effective identification and assessment of potential controlled features.

In addition, the report outlines policy-level considerations as well as compliance requirements and operational guidance for industry stakeholders. It provides item-classification guidelines intended to assist exporters in undertaking accurate and timely control determinations. Through these analyses and recommendations, the report seeks to support national efforts to foster the development of AI-based industries, promote technological leadership, and ensure adherence to global export-control compliance.

Ⅰ 서론

제1장 서론

1.1. 연구 배경

❍ 인공지능

- 인공지능(AI, Artificial intelligence)은 인간의 학습, 추론, 인식, 판단 기능 등을 모방하도록 인공 신경망((ANN, Artificial Neural Network)을 기반으로 설계된 기술로, 대량 데이터를 인공신경망에 입력하여 학습시킴으로써 자율적으로 문제를 분석, 해결하거나 결정을 내릴 수 있도록 하는 시스템임

- 최근 인공지능은 자연어 처리, 음성/영상 인식 및 분석/생성, 자율 주행, 추천 시스템, 전략 예측 분석, 드론 및 로봇 제어 등 다양한 응용 분야에 걸쳐 확산되고 있으며, 특히 대규모 학습 데이터와 고성능 컴퓨팅 연산 자원에 기반한 대규모 생성형 AI 기술(LLM(Large Language Model), LVM(Large Vision Model))이 핵심 인공지능 기술로 대두되고 있음

❍ AI 시스템의 구성 및 작동 원리

- AI 시스템은 일반적으로 다음 세 가지 요소로 구성됨

  ① 인공신경망 모델

  ② 학습용 데이터셋

  ③ 연산 자원(HW 플랫폼)

- 딥러닝 기반 AI 시스템은 수천 ~ 수조 개의 매개변수(가중치)를 갖는 인공신경망 모델로 구성되며, 대량의 학습용 데이터셋을 이용해 매개변수(가중치)를 최적화하는 방식으로 모델을 학습함[1]

- 이 과정에서 다수의 고속 병렬 연산을 필요로 하므로, 일반적으로 수천 ~ 수십만 개 이상의 GPU(Graphics Processing Unit), TPU(Tensor Processing Unit) 등의 고성능 HW(Hardware) 연산 자원을 사용함.

- AI 시스템의 일반적인 처리 구조 및 개발 단계는 다음과 같음[2]

표 1 AI 시스템의 일반적인 처리 구조 및 개발 단계

단계	주요 내용
(1) 데이터 수집	텍스트, 음성, 영상 등 다양한 형태의 데이터 확보
(2) 데이터 전처리	정제, 라벨링, 보강 등 AI 학습 전 처리 과정 수행
(3) AI 모델 설계	CNN(Convolutional Neural Network), RNN(Recurrent Neural Network), Transformer 등 기반 AI 모델 아키텍처 설계
(4) AI 모델 학습	GPU, TPU 등 이용 AI 모델의 대규모 학습 연산 수행
(5) 검증 및 테스트	AI 모델의 정확도 분석 및 조정 과정
(6) 배포 및 추론	API(Application Programming Interface), SaaS(Software as a Service) 등 형태로 제공 및 서비스

❍ AI 시스템의 개발 및 운영 단계

(1) AI 데이터 수집 및 전처리

- AI 모델의 학습을 위해서는 대량의 데이터셋이 필요하며, AI 시스템 모델의 서비스 종류에 따라 데이터 유형은 텍스트, 음성, 이미지, 동영상 등으로 다양함
- 데이터셋은 공공 데이터 이용, 웹 크롤링, 센서 정보 수집, 고객 로그 활용 등 다양한 형태로 확보되며, 수집된 데이터는 정제, 라벨링, 보강 등을 거쳐 AI 시스템 모델의 학습에 적합한 형태로 전처리됨

(2) 모델 설계 및 학습

- 설계된 AI 시스템 모델(예: CNN, RNN, Transformer 등 기반)은 GPU, NPU 등 고성능 컴퓨팅 자원 및 HBM(High Bandwidth Memory) 등 대용량 메모리 자원, 클라우드 플랫폼 등을 이용하여 학습됨
- 이 학습 과정에서 대규모 벡터/행렬 연산, 활성화(activation) 함수 연산, 역전파(back propagation) 알고리즘 수행 등이 반복되며 AI 모델의 매개변수가 최적으로 학습됨

(3) 추론 및 응용

- 학습이 완료된 AI 시스템은 추론(inference) 과정을 통해 실제 인공지능 서비스로 제공되며, API, SaaS 등의 서비스 형태로 AI 시스템이 활용됨
- AI 시스템은 언어 번역, 정보 요약, 정보 분석/통합/예측, 음성/영상 인식/생성, 생체 인식, 자율 제어, 전략 결정 등 다양한 민간용, 군사용 분야에 활용됨

❍ AI 모델

- AI 모델은 인간의 신경망을 모방한 인공 신경망에 대량의 데이터를 입력하여 특정 목적에 맞게 학습한 것으로, 학습 데이터 이외의 새로운 입력 데이터에 대해 예측이나 판단을 수행하거나 새로운 출력 데이터를 생성하는 추론 기능을 제공함
- 최근에는 언어, 음성, 이미지 등 단일 영역을 넘어 다양한 멀티모달(multi-modal) 데이터를 처리할 수 있는 대규모 생성형 모델(예: LLM·LVM) 등이 등장하고 있으며, 분석/예측, 번역, 대화, 코드 작성 및 수정, 이미지 생성, 비디오 생성 등 다양한 산업·서비스 분야에서 활용되고 있음

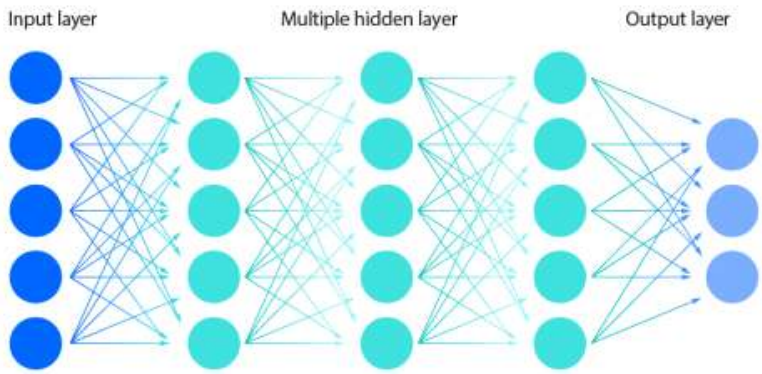


그림 1 인공신경망의 예(자료: IBM)

❍ AI 인프라/클라우드

- AI 인프라/클라우드는 대규모 AI 모델의 학습과 추론을 지원하기 위한 다수의 고성능 컴퓨팅 자원, 데이터 저장·처리 시스템, 네트워크, 개발 환경 등을 통합적으로 제공하는 기반 환경을 의미함
- 주요 클라우드 사업자(Google Cloud, AWS, Azure 등)는 GPU/TPU·스토리지·분산

학습 프레임워크를 포함한 AI 전용 플랫폼을 서비스 형태로 제공하고 있으며[3][4][5], 이를 통해 기업이나 연구기관이 고성능 AI 자원을 직접 도입하거나 설치하지 않고 초기 투자 없이 API 등을 이용해 활용하는 것이 가능해짐

그림 2 xAI 클라우드 플랫폼(자료: Grok, Oracle)

❍ AI 컴퓨팅

- AI 컴퓨팅은 AI 모델이나 알고리즘의 학습 및 추론을 위한 고성능 연산 수행 체계로, CPU 대비 대규모 병렬 연산에 최적화된 GPU, AI 전용 ASIC/TPU/NPU, FPGA 등 특수 목적의 고성능 컴퓨팅 하드웨어를 중심으로 발전하고 있음

- 최근에는 초거대 AI 모델의 학습을 위해 수천~수십만 개의 연산 장치를 연결한 슈퍼컴퓨팅 인프라가 활용되며[6][7], GPU 등의 클러스터 관리 소프트웨어, 분산 통신 라이브러리 등과 결합하여 AI 학습 및 추론 성능을 극대화하는 방향으로 발전하고 있음[8][9][10]

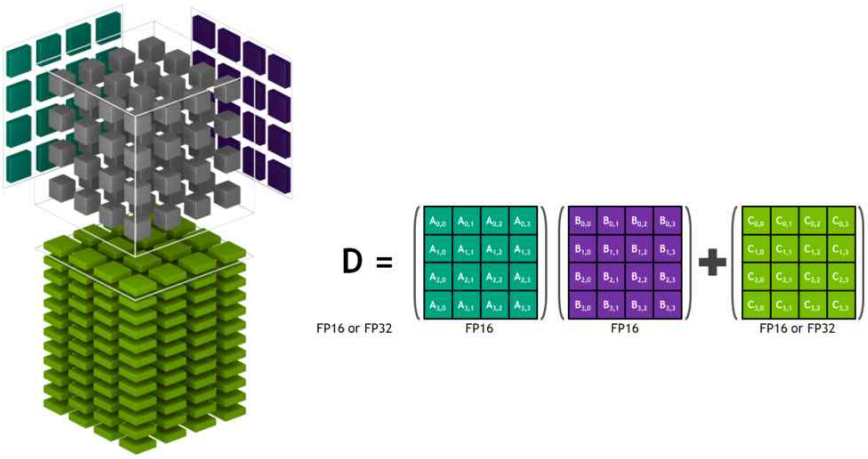


그림 3 AI 컴퓨팅을 위한 고성능 병렬 연산(자료: NVIDIA)

❍ AI 반도체 칩

- 인공지능 시스템에서는 다수의 연결/연산 요소를 갖는 인공신경망을 구성하여 대량의 데이터를 인공신경망의 입력으로 받아 학습/훈련하고, 학습/훈련된 인공신경망을 통해 출력 데이터를 추론함
- 이 과정에서 다량의 연산을 HBM 같은 고사양 메모리와 GPU, TPU와 같은 고성능/고속 연산 칩을 통해 병렬로 처리할 필요가 있음
- 인공지능 연산을 위한 고성능 반도체 칩으로는 다음과 같은 다양한 형태가 있음

  GPU(Graphical Processing Unit), TPU(Tensor Processing Unit)

  In-memory Processor, Vision Processor, Text Processor
  Coprocessor, Accelerator, Adaptive Processor

  FPLD(Field-Programmable Logic Device)

  ASIC(Application-Specific Integrated Circuit

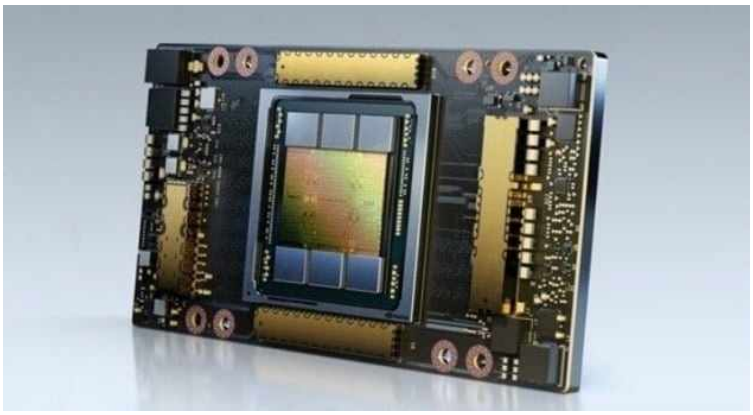


그림 4 NVIDIA H100 GPU(자료: NVIDIA)

❍ AI SW

- AI 소프트웨어는 데이터 학습, 추론, 최적화 과정 등을 구현하는 프로그램이나 프레임워크로, AI 모델의 개발, 운영, 배포를 지원하는 핵심 요소임

- 대표적으로 TensorFlow, PyTorch, JAX, Hugging Face Transformers 등 오픈소스 프레임워크가 활용되고 있으며[11][12][13][14], 분산 학습·모델 최적화·추론 가속을 위한 라이브러리(NCCL, Horovod 등)도 포함되며 최근에는 프라이버시 보존 학습(Federated Learning)과 암호화 기반 AI SW도 주목받고 있음[15][16][17][18]

❍ AI 서비스

- AI 서비스는 AI 모델을 응용하여 다양한 산업·사회 전반에 활용되는 제공되는 기능적 솔루션으로, SaaS(API 형태), 클라우드 기반 AI 서비스, 온디바이스 AI 등 다양한 형태로 제공됨

- 대표적으로 대화형 AI(챗봇), 생성형 AI(텍스트·이미지·음성 생성), 추천 시스템, 의료 영상 분석, 금융 리스크 평가, 자율주행 지원 서비스 등이 있으며, 최근에는 대규모 언어모델(LLM)과 멀티모달 모델 기반 생성형 서비스가 주요 서비스 형태로 확산되고 있음

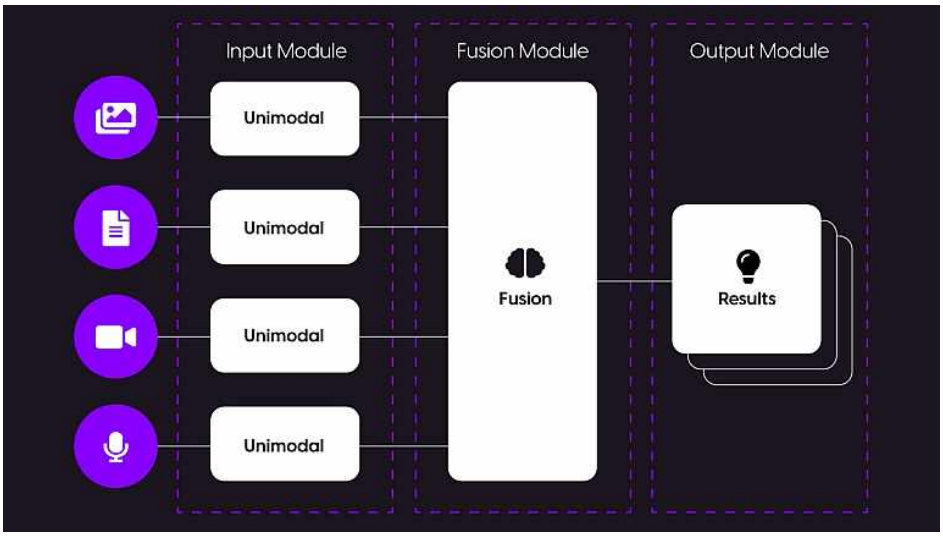


그림 5 멀티모달 생성형 AI 시스템(자료: https://sightcall.com/blog/multimodal-generative-ai-how-its-changing-service-forever/)

❍ AI 기반 품목 관련 수출통제

- AI 기반 품목은 AI 기술이 적용된 하드웨어(HW)·소프트웨어(SW)·서비스를 포함하며, 국가안보, 군사, WMD(Weapon of Mass Destruction, 대량살상무기) 관련 활용 가능성 및 우려로 전략물자 통제의 주요 대상이 되고 있음

- 미국 수출 관리 규정(EAR, Export Administration Regulations)[19][20] 및 바세나르 협정(WA, Wassenaar Arrangement) 통제 리스트[21][22]에서는 고성능 연산 반도체 칩/컴퓨터, AI 반도체, 고성능 AI 서버, AI 학습 SW, 암호화 SW/HW, 센서 관련 SW/기술 등을 수출통제 대상으로 규정함

  - 대규모 AI 모델의 가중치(파라미터)는 2023년 통제 대상으로 신설 후 2024년 삭제되었으나, Part 744 캐치올(catch-all) 규정을 통해 군사·정보 목적 사용 시 여전히 규제됨[23][24]

- 따라서 AI 관련 HW, SW, 기술 등의 품목은 통제 성능 기준, 암호화 기능 포함 여부, 군사 전용 가능성 등 여부에 따라 수출통제가 이루어지며, 기업·연구기관은 AI 기술의 수출 및 이전 시 관련 규정을 충분히 검토할 필요가 있음

1.2. 연구 필요성

- 고성능 반도체, 고속 컴퓨팅 등을 기반으로 하는 AI 기술은 정보 분석, 영상 분석, 자율 이동 시스템(자동차, 드론, 로봇), 생명공학, 사이버 보안, 전략/전술 통제 시스템, 자율 무기 체계 등 다양한 산업용 및 군용 기술에 활용되어 빠르게 확산되고 있음
- 최근 AI 관련 HW, SW 기술이 고도화되고 성능이 개선되면서 다양한 민간용 및 군용 영역으로의 확산이 가속화되고 있으며 국제 무역 및 국가 안보 등에 미치는 파급력도 증대되고 있음
- 따라서, AI 관련 품목(HW, SW, 기술 등)의 선도적 산업 발전 필요성과 더불어 기술 안보 측면에서 수출통제 필요성 역시 높아지고 있음. 미국을 비롯한 유럽, 일본, 중국 등은 AI 기술을 기반으로 한 전략물자에 대한 통제 대상과 범위를 점차 강화하고 있는 추세임
- 국내에서는 전통적인 군용/민간용 이중용도 품목인 전략물자에 대한 관리 및 통제에 대한 필요성 인식하에 국제 수출통제 제도인 바세나르 협정(WA) 기반 수출통제 제도를 운영해오고 있음
- 그러나, AI 시스템용 반도체, AI 기반 소프트웨어, AI 학습/추론 모델, 클라우드 컴퓨팅 기반 AI 관련 기술 등 다양한 최신 AI 관련 품목의 전략 물자 통제에 대한 인식과 통제 대상 분석 등은 미흡한 수준으로 이에 대한 연구가 필요한 실정임

1.3. 연구 목적

- 본 연구에서는 다양한 AI 기반 품목에 대한 국내외 전략물자 통제 및 판정 사례 등을 분석하여 통제 기준을 정립하고, 개선 방안을 제시하고자 함
- 본 연구를 통해 정부와 기업 등 관련 기관이 AI 관련 기술 및 HW, SW 품목의 연구 개발 및 생산, 사용 및 수출 과정에서 전략물자 통제 제도를 효과적으로 적용하고, 적절히 대응할 수 있도록 하기 위한 기초분석 자료를 제공하는 데 목적이 있음
- 또한, 이를 통해 AI 관련 기업들이 설계, 개발, 생산, 판매하는 품목들이 전략 물

자 통제 대상에 해당되는지, 혹은 향후 통제 대상에 해당될 가능성이 있는지 등을 파악하고 대비할 수 있도록 하는 가이드라인의 기능을 제공하고자 함

1.4. 연구 범위

(1) AI 기반 품목 및 수출통제 기준 분석

- AI 기술 관련 수출통제
- AI 기반 HW, SW 품목 및 기술
- AI 기반 품목의 WA 국제 수출통제 기준 소개 및 분석
- AI 기반 품목의 국가별 독자 수출통제 기준 및 분석

(2) 국내외 AI SW 품목 사례 및 전략 물자 가능성 분석

- 해외 AI SW 품목 사례 분석
- 해외 AI SW 품목의 전략 물자 가능성
- 국내 AI SW 품목 사례 분석
- 국내 AI SW 품목의 전략 물자 가능성

(3) 국내 AI SW 관련 기업 대상 설문조사 및 인터뷰 분석

(4) AI SW 품목 수출통제 대응 방향 및 판정 가이드라인 도출

II AI 기술 수출통제 체제 및 동향

제2장 AI 기술 수출통제 체제 및 동향

- 본 장에서는 AI 기술의 수출통제 관련 특성과 WA 및 미국, 유럽, 일본 등 국가와 국내의 AI 기술 관련 수출통제 체제 및 동향을 살펴보고, 향후 예상되는 AI 기술 수출통제 관련 전망을 제시해보고자 함

2.1. AI 기술의 수출통제 특성

- 최근 AI 관련 HW, SW 기술이 고도화되고 성능이 개선되면서 다양한 민간용 및 군용 영역(자율 이동 및 무기 체계, 정보/영상 자동 분석, 사이버 보안, 전략/전술 통제 시스템 등)으로의 확산이 가속화되고 있으며 국가 안보 및 국제 무역 등에 미치는 파급력도 증대되고 있음

- AI 관련 기술 및 품목(HW, SW)의 산업 혁신 및 발전의 필요성과 더불어 기술 안보 측면에서 수출통제 필요성 역시 중요해지고 있음. 미국을 비롯한 유럽, 일본, 중국 등은 AI 기술을 기반으로 한 전략물자 및 전략기술에 대한 통제 대상과 범위를 점차 강화하고 있는 추세임

2.1.1. HW 중심 수출통제

- AI 시스템은 일반적으로 방대한 시스템 인공 신경망 모델과 복잡한 연결 구조로 구현되는데 그 특성과 성능은 학습 및 추론을 위한 연산 능력, 데이터 처리량과 속도 등에 많이 좌우됨

- 연산 능력과 데이터 처리 성능은 1초당 조단위 이상의 연산을 수행하고(Tera FLOPS(Floating Point Operations Per Second, 1조번 부동소수점 연산/초) 데이터를 처리하는 고성능 AI 반도체 칩과 메모리, 컴퓨터 등 HW에 많은 영향을 받음

- AI 관련 기술의 전략 물자 통제는 주로 고성능 AI 반도체 칩과 메모리, 컴퓨터 등 HW 위주로 이루어져 왔는데 그 이유는 다음과 같은 특성에 기인함

(1) HW, 특히 AI 연산용 고성능 반도체 칩과 메모리는 연산 성능과 데이터 처리 성능 등을 객관적 수치로 정량할 수 있다는 점에서 통제 사양 기준을 설정하기가 용이함

- 주요 성능 지표로는 다음과 같은 것이 있음

FLOPS(초당 부동소수점 연산 횟수): AI 학습·추론 연산 성능 지표

메모리 대역폭(GB/s): AI 학습·추론을 위한 메모리 데이터 처리 성능 지표

성능밀도(TeraFLOPS/mm²): 면적 대비 연산 성능 지표

(2) HW는 제조 시점 기준으로 성능 사양이 정해지며, 일반적으로 동일 HW라면 동일한 성능을 가지게 되므로 통제 사양 기준의 일관된 적용이 가능함

(3) 첨단 AI 반도체 칩과 메모리의 제조 및 공급망은 소수의 주요 글로벌 제조사에 집중되어 있으므로[25] 관련 품목의 수출통제 및 관리가 상대적으로 용이함

주요 제조사: NVIDIA, AMD, 인텔, Google 등

주요 파운드리사: TSMC, 삼성전자 등

(4) 첨단 AI 반도체 칩과 메모리는 대규모 주문·계약을 거쳐 제한된 물류망을 통해 유통되므로 유통 경로가 비교적 단순하고, 선적이나 통관 시 HS(Harmonized System) 코드, ECCN(Export Control Classification Number) 코드 등으로 식별이 가능함

(5) 고성능 AI 반도체 칩과 메모리, 컴퓨터는 군사용 전략전술 및 정보 분야에 필요한 고성능 AI 시스템과 직접적으로 관련되어 활용될 수 있음

주요 군사 응용 분야:

무기 체계: 미사일 등 무기 체계의 탄도, 항로, 충격파 등 분석

암호 시스템: 정보 암호화 시스템의 암호화 특성 분석

자율 이동 시스템: 무인 차량, 무인 선박/잠수정, 무인 항공기/드론 등의 실시간 제어 및 의사결정

위성·정찰 영상 시스템: 대규모 이미지 인식 및 분석, 지속적 목표 추적

- 미국을 비롯한 주요국은 AI 기술을 군사·안보 측면의 핵심 기술 및 잠재적 위협으로 보고, AI 기술 발전 단계에 맞게 수출통제 및 관리가 비교적 용이하고 효과적인 HW를 주요 통제 대상으로 함

2.1.2. 제한적 SW 수출통제

- AI 시스템의 기본적인 모델과 구조, 정보 분석 및 예측 등의 주요 기능은 SW로 구현되는 경우가 많아 AI 시스템에서 SW도 AI 시스템의 특성과 기능에 핵심적인 역할을 수행함

- 하지만 AI SW는 HW에 비해 상대적으로 수출통제 대상 품목의 통제 사양 정의를 명확하게 정의하기 어려운 점 등 다음과 같은 특성 때문에 수출통제가 상대적으로 제한적임

  (1) SW는 HW와 달리 물리적 형태가 없는 디지털 정보로 이루어진 무형 품목으로 전통적인 수출입 단계에서 통관이나 실물 확인 등이 상대적으로 어려움

  (2) SW는 프로그램(코드) 형태이므로, 복사, 이메일, 클라우드 업로드 등 인터넷을 통한 전송을 통해 지역이나 국경을 초월한 전파가 가능함

  - 2019년 EAR 0Y521 시리즈에 포함된 영상인식 AI SW의 경우, 제재 대상국으로 이전 뒤 P2P 파일 공유 네트워크와 미러 사이트를 통해 확산됨[26][27]

  - AI 모델 파일(예: PyTorch .pt 파일, TensorFlow .pb 파일) 등은 이메일, 메신저, 클라우드 등 다양한 경로를 통해 이전이 용이함

  - 글로벌 클라우드 플랫폼(GitHub, Hugging Face, Google Drive, Dropbox 등)을 통한 파일 공유가 용이함

  - 클라우드 플랫폼은 다국적 법인 형태로 운영되거나 서버의 위치가 지역적으로 광범위하므로 클라우드를 통한 SW의 이동을 적절히 통제하기 어려움

  (3) SW의 경우 HW와 달리 통제 사양을 명확히 정량적으로 정의하기가 용이하지 않을 수 있음

- SW 업그레이드나 SW 컴포넌트의 모듈화 등으로 기존 SW와 특성이나 사양이 달라질 경우 기본적으로 새로운 품목으로 간주됨
- 동일한 기능(예: 객체 인식, 음성/영상 분석)의 수학적 원리나 알고리즘, 최적화 방법, 프로그램 구현 방법 등이 다양함

(4) AI 서비스는 API 또는 SaaS 형태로 제공되는 경우가 많음

예: OpenAI GPT API, Stability AI API

- 통제 대상 국가가 AI 시스템 HW나 SW가 없더라도 다른 국가에 위치한 데이터센터의 AI 서비스 모델의 API를 사용하면 동일한 AI 시스템 이용 효과를 얻을 수 있음

예: 고성능 GPU(A100, H100 등) 포함 미국·유럽 데이터센터의 AI 서비스 API 이용

- 대량의 API 호출을 통해 AI 모델 전체를 간접적으로 사용하거나, 연속 호출을 통해 고급 기능의 지속적 사용이 가능함

(5) 오픈 소스 모델의 경우 통제 대상 SW의 핵심 알고리즘이나 모델 구조가 공개되면, 이를 변경하거나 재구현하는 것이 가능함

- 2022년 Stability AI가 이미지 생성 모델 Stable Diffusion의 오픈소스 공개 이후, 모델 가중치와 학습 프로그램의 다운로드 및 실행이 가능해짐[28]
- 일부 상용 SW는 오픈 소스 라이브러리를 기반으로 하며, 핵심 기능만 비공개로 하므로 어느 부분까지 통제 대상으로 할 것인지 경계가 모호함

2.2. AI 기술의 국가별 수출통제

- 전략물자 및 전략기술의 수출통제는 기본적으로 42개 국가가 참여하는 다자간 협의체인 바세나르 체제(WA) 회의에서 제안 통제 대상 안건에 대해 만장일치로 통과된 안건을 통제 대상으로 함
- 최근 일부 국가의 반대로 합의가 되지 않거나 지연되는 반도체, 양자 기술 등 첨

단 기술 관련 통제 대상 품목에 대해 미국, 유럽 등은 국가별로 독자적인 수출통제를 시행하는 경우가 늘어나고 있는 추세임

2.2.3. 바세나르 체제(WA) 수출통제

2.2.3.1. HW 분야

- 바세나르 체제(WA)는 재래식 무기 개발 등과 관련된 군용/민간용 이중용도 품목과 기술의 국제 수출통제를 위한 42개 국가의 다자간 협의체임
- WA에서는 AI 관련 품목 및 기술의 직접적인 통제 조항은 없으나, 정보의 암호화를 수행하는 HW/SW 품목과 고성능 컴퓨팅 관련 장비 등 기존 WA 통제 조항으로 AI 관련 품목을 간접적으로 통제함

2.2.3.2. SW 분야

- WA는 AI SW 전용 통제 조항 또는 이에 상응하는 별도의 통제 대상을 보유하지는 않으나, AI 관련 SW는 기존의 범용 SW 품목 내에서 간접적으로 통제되고 있음
- 특히 이미지·음성·데이터 분석 기능을 포함하는 SW가 일부 통제 대상 품목으로 편입되어 있음
- 2023년 WA 회의에서 일부 회원국이 대규모 AI 모델 및 생성형 AI의 확산 위험성을 제기하였으나, 대상 기술의 정의, 성능 기준, 검증 절차 등에 대한 회원국 간 합의가 이루어지지 않음[29][30]
- 통제 대상 품목

  성능 지표: 처리 속도, 해상도, 데이터 처리량 등 정량화 가능한 통제 사양

  용도 기준: 군사·정보 수집·감시 목적에 활용될 경우 통제 적용 가능

  캐치올: 통제 조항에 명시되지 않은 SW라도, 군사적 전용 가능성이 확인되면 수출 허가를 요구하는 포괄 통제 방식

  예:

  군사 위성 영상 자동 분석 SW

초고속 암호 해독을 지원하는 AI 알고리즘

- WA 차원에서 AI SW는 '간접 통제'가 기본 틀이며, 기술의 빠른 발전 속도를 따라가기 위해 캐치올 방식 의존도가 높음
- 캐치올 방식은 사전 예측 가능성이 낮아 기업이 국제 거래 시 리스크를 완전히 제거하기가 어려우며, 회원국 간 해석 차이로 통제의 일관성이 저하될 수 있음

- WA 국제 체제에서는 기술 발전 및 변화를 반영하고, 회원국간의 논의를 통해 통제 대상 품목과 통제 대상을 매년 업데이트하고 있음
- 2023년 회의 결과, 수출통제 목록의 갱신 및 기술변화 반영 원칙을 재확인하고, 회원국의 각국 법령에 구현하도록 하여 이를 반영함
- AI 품목에 대한 구체적인 개별 통제 대상 신설보다는, 고성능 컴퓨팅, 전자, 센서 분야 통제 대상 품목의 통제 사양 조정 등이 이루어짐

2.2.4. 미국의 수출통제

2.2.4.1. 미국의 수출통제 체제

- 미국의 수출통제는 국가안보, 대외정책, 경제적인 측면을 보호하기 위해 마련된 제도로 민간·군사용 모두 가능한 이중용도(Dual-use) 품목 HW, SW, 기술을 상무부(DoC) 산하 산업안보국(BIS)이 수출관리규정(EAR), 수출관리개혁법(ECRA, 2018)에 따라 통제하고 있음
- ECRA(Export Control Reform Act of 2018)는 기존의 EAA(Export Administration Act)의 만료를 대체하는 항구적 법률로 1979년 제정되어 상무부(BIS)가 이중용도 품목 통제를 지속적으로 수행할 법적 근거를 마련함
- ECRA에 AI, 반도체, 양자기술, 생명공학 등을 포함하는 신흥기술(Emerging Technologies), 기반기술(Foundational Technologies) 통제 조항을 신설함
- ECRA를 근거로 한 행정명령 체계(EO, Executive Orders)가 BIS/OFAC/DoS의 제재 정책에 실질적 근거를 제공함

- 주요 EO로는 다음과 같은 것이 있음

  EO 13694 (2015): 사이버 공격 관련 제재 근거

  EO 13873 (2019): 외국산 ICT 공급망 위협 대응

  EO 13959 (2020): 중국 군산복합체 관련 투자 금지

  EO 14110 (2023): AI, 데이터, 생명공학 기술 관련 "국가안보 기반 신흥기술 통제" 강화

2.2.4.2. HW 분야

- 미국은 AI 관련 HW, SW 및 기술의 중요성을 인식하고 AI 반도체 칩과 AI 학습 인프라, AI SW 등을 중심으로 하는 수출통제 제도를 시행해 왔으며 점차 강화해 왔음
- 2022년 10월, 미국은 1차 대중국 AI 반도체 수출통제 정책을 발표함. ECCN 3A090, 4A090 등 고성능 AI 반도체 칩과 관련 SW의 대중국 수출을 제한하여, 엔비디아 A100, H100과 같이 특정 연산 성능 이상을 갖는 GPU, AI 가속기 등의 대중국 수출이 제한됨[31][32]
- 미국의 3A090, 4A090 규정은 AI 반도체 칩 자체뿐만 아니라 해당 칩을 탑재한 서버, AI 가속기 모듈, 고성능 워크스테이션 등까지 통제 대상을 확대하였음
- 이는 반도체 칩 단품의 수출 제한을 회피하기 위해 다른 형태나 서버 등으로 우회 수출하는 가능성을 차단하기 위한 것으로 일본, 네델란드 등도 유사 기준을 적용함
- 2023년 10월, 미국은 2차 대중국 AI 반도체 칩 수출통제 강화를 위해 기존 통제 성능 기준을 하향 조정하여 엔비디아 H800, A800 등으로 통제 대상이 확대되었음[33].
- 추가로 성능밀도(Memory Bandwidth Density)와 같은 정량적 수출통제 성능 기준을 도입하고, 클라우드 기반 AI 학습 서비스가 통제 대상에 포함되는 것에 대한 검토에 착수함
- 2024년 3월, 해외 클라우드 AI 서비스를 통해 AI 학습 및 추론을 수행하는

'우회 접근'을 차단하기 위해 클라우드 AI 서비스까지 수출통제 범위에 포함하는 방안을 검토하기 시작함[34]

- 2024년 12월, 미국은 고대역폭 메모리(HBM)와 첨단 반도체 장비에 대한 추가 통제를 시행하고 Entity Listdp 140여개의 기업 및 단체를 포함하여 등재함[70].

- 2025년 1월, AI 모델의 구조, 파라미터 등이 군사·안보 분야에서 직접 활용될 가능성을 고려하여, 기존의 AI 반도체 칩, AI 소프트웨어, 클라우드 AI 서비스뿐만 아니라 AI 모델 자체(파라미터)에 대한 통제 논의가 이루어지고 있음[35][73]

- 2025년 1월 상무부는 전세계 국가를 3개의 국가그룹으로 나누어 국가별 AI 반도체 칩 수출 한도를 제한하고, AI 칩을 활용해 훈련된 첨단 AI 모델을 수출통제 대상 기술로 추가하였음[71]

- 현재는 수출통제 기술인 ECCN 4E091의 통제 대상 적용 범위를 확장하여, 특정 규모 이상의 AI 모델 파라미터의 해외 이전을 제한하는 방안이 거론되고 있음[35]

2.2.4.3. SW 분야

- 미국은 AI 기술이 군사·안보적으로 중요한 핵심 기술이 될 것으로 보고, 기존의 HW 중심 수출통제 체계를 SW와 서비스 영역으로 확장하고 있음

- 2019년 1월, 미국 상무부 산업안보국(BIS)이 EAR에 AI 학습용 소프트웨어 규정을 신설함

- 2019년 1월, EAR § 734.8에 따라 AI 학습용 소프트웨어 중 위성 영상 인식용 지리정보 분석에 활용되는 AI 모델 훈련 코드를 0Y521 시리즈 품목으로 지정함[26][27]

- 해당 SW는 위성·항공 촬영 이미지에서 군사 시설·활동을 자동 식별·분석하는 기능을 포함하여 군사 감시·정찰 활동에 직접 활용이 가능함

- 2020년 1월, 해당 SW를 해외로 이전·수출·재수출하는 경우 BIS의 사전 허가 의무 부과 대상이 되고, 미국 내 클라우드 환경에서 외국인이 접근하는 경우에도 사실상 수출(deemed export) 규정이 적용, 사실상 원격 접근까지 통제

함

- 2024년 3월, SaaS 기반 AI 서비스를 통한 통제 우회 가능성이 지적됨에 따라, 원격 API 호출 및 대규모 AI 모델 학습 환경을 통제 대상으로 포함하는 방안을 논의함[36]

- 2024년 10월, License Exception AIA(Advanced Intelligent Applications)를 신설함. 미국과의 안보·경제 동맹국에 대해 일정 조건(접속 모니터링, 로그 유지, 기술 재이전 금지 등) 하에서 통제를 완화하고, 중국·러시아·북한·이란 등 국가에는 통제를 강화하여 우호국 개방과 경쟁국 차단 기조를 제도화함[37]

  - 미국은 수출 관리 규정(EAR)을 통해 AI 관련 SW를 통제하고 있으며 현재까지는 특정 군사·정보 목적과 직접적으로 연계될 수 있는 분야에 한하여 통제를 적용하고 있음

- 미국은 기본적으로 WA 국제 체제 변동을 반영하여 매년 이중용도 통제 리스트를 업데이트하고 있으나, WA 국제 체제에서 합의되지 않은 최신 기술을 전향적으로 독자 통제 리스트로 추가함

- AI 고성능 컴퓨팅 HW(예: 고성능 GPU)를 통제하기 위한 ECCN 4A090을 신설하고, 이와 연동해 해당 HW용 SW를 통제하기 위한 ECCN 4D090을 신설 도입함

- 이는 AI 고성능 컴퓨팅 HW의 개발·생산·사용을 위해 전용 설계(specially designed)된 SW를 통제함

2.2.5. 유럽 연합(EU)의 수출통제

2.2.5.1. 유럽의 수출통제 체제

- EU의 수출통제 체제는 재래식 무기와 이중용도 품목의 수출을 회원국 간 일관성 있게 관리하기 위해 구축되었으며, 미국처럼 국가 단위 통제가 아니라, EU 차원의 기본 규정(Regulation)과 회원국의 집행 시스템(National Authority)이 결합된 이중 구조임

- EU는 EU 집행위원회(EC)와 회원국 관할기관(Competent Authorities)이 2021

년 발효된 이중용도 품목 수출 통제에 관한 EU 규정(현재: Regulation (EU) 2021/821)에 따라 수출을 통제함[72]

2.2.5.2. HW 분야

- 유럽 연합(EU)은 이중용도 통제 체계의 CAT 3(전자부품), CAT 4(컴퓨터), CAT 5(정보보안)의 고성능 컴퓨팅과 암호화 품목 통제 리스트를 통해 AI 기술을 간접적으로 통제하고 있음

- 미국의 독자 통제 품목인 ECCN 3A090, 4A090 등에 직접적으로 대응하는 EU의 통제 규정은 아직까지 없으며 자체 규범인 'EU AI Act(2024)'를 병행 운영하고 있음[38]

- EU AI Act는 주로 AI의 안전성·윤리성·투명성을 규율하는 법률로, 수출통제 목적보다는 내부 시장 통제를 강화하는 성격이 강함

2.2.5.3. SW 분야

- EU는 이중용도 통제 체계를 기반으로 AI SW를 간접적으로 통제할 수 있는 기본적 통제 체계를 보유하고 있으나, AI 생성 모델 등 AI SW 자체를 명시적으로 통제하는 조항은 없음

- AI SW가 고성능 컴퓨터 운용, 암호 분석·정보 보안, 이미징·센서 데이터 분석 기능 등을 수행할 경우, EU의 이중용도 통제 규정(EU Regulation 2021/821)에 따라 수출 허가 대상이 될 수 있음[39]

- 미국 독자 통제 대상 EAR 3A090, 4A090, 4D090처럼 AI 칩 및 SW를 특정 성능 기준으로 직접 통제하는 규정은 없으나, 성능·기능 중심의 캐치올 조항을 통해 민감 용도의 AI SW를 통제하는 것이 가능함

- 2024년 제정된 EU AI Act는 내수 시장에서의 AI 안전·투명성 확보를 목표로 하며, 수출통제와는 별도로 운영되며 AI Act에서 정의하는 고위험 AI(high-risk AI) 카테고리가 향후 수출통제 리스트 개정에 영향을 줄 가능성이 있음

- EU는 EU 2021/821에 따라 WA 국제 체제 변동을 반영하여 매년 이중용도

통제 리스트 Annex I를 업데이트하고 있으며 2025년 9월 통제 리스트 최신화를 공지함

- AI SW 품목을 개별 통제 대상 AI SW 품목으로 직접 통제하기보다 기존 통제 대상 SW 품목으로 간접 통제함

2.2.6. 일본의 수출통제

- 2023년 5월, 일본은 외환·외국무역법(外為法)에 근거하여 고성능 반도체 칩 및 AI 서버의 중국 수출을 제한하는 조치를 발표하여 미국의 대중국 AI 반도체 수출통제에 동참함[40]
- 이 조치는 미국이 신설한 독자 통제 조항인 ECCN 3A090, 4A090을 자국의 수출통제 분류표에 매핑함으로써 사실상 미국과 유사한 통제 체계를 적용함
- 실제 통제 대상에는 NVIDIA A100, H100, AMD MI250/MI300 급의 GPU 등이 포함되었으며, 일본 기업이 제조하거나 해외에서 조립·판매하는 경우에도 통제 적용을 받도록 함
- 또한 고성능 컴퓨팅 서버 및 관련 소프트웨어 및 펌웨어(firmware)까지 포괄적으로 통제 목록에 포함시켜, 칩·서버·소프트웨어의 일괄 통제를 가능하도록 함
- 통제 대상은 AI 학습용 GPU, AI 서버(고성능 메모리·네트워크 포함), EUV/DUV 노광장비, 첨단 반도체 제조장비 등으로 미국 3A090, 4A090 기준에 준하는 성능 및 밀도 지표를 채택함
- 일본의 통제목록(일본 포괄허가 품목 코드)을 미국 ECCN 체계와 상호 매핑하고 수출 허가 심사 시 미국과 동일한 기준 적용이 가능함. 허가제 중심으로 운용하여 중국·홍콩·마카오 및 일부 중동·러시아 대상은 개별허가제, 기타 비동맹국 대상은 포괄허가(Permit Blanket License) 가능함

2.2.7. 네덜란드의 수출통제

- 2023년 6월 30일, 네덜란드 외무부·경제부가 공동으로 첨단 반도체 제조 장비(ASML의 DUV, EUV 노광장비), 고성능 AI 반도체 장비 및 시스템(미국 ECCN과 직접 호환)을 통제 대상으로 함[41]

- 미국과 공동집행 구조로 ASML 장비의 중국향 수출 시 미국 EAR 규정인 De Minimis Rule과 네덜란드 법령을 동시에 적용함. 미국 ECCN 3A090, 4A090을 참고하여 네덜란드 HS 코드 기반 통제 리스트를 개편함

- 중국 내 신규 AI 데이터센터 구축을 위한 장비나 부품의 수출 허가 불허 가능성이 높으며, 미국 GPU(예: A100, H100) 통합 서버의 네덜란드 조립품도 동일 통제 조항이 적용됨

2.2.8. 국내 수출통제

- 국내 수출 통제 체제는 대외무역법 제 26조 등에서 전략물자 수출입통제의 법적 근거를 두고 있으며, 전략물자 수출입고시(행정규칙)는 "국제평화 및 안전유지와 국가안보"에 기여하기 위해 전략물자의 수출입통제를 정하고 있음

- 제도적으로는 무역안보관리원에서 전략물자 및 전략기술을 판정하고, 수출허가·경유·환적 허가·중개 허가 등을 규정하며, 일정 기준을 갖춘 기업은 자율준수무역거래자로 지정되어 일부 관리를 자체적으로 할 수 있도록 함

- 국내 수출 통제 체제는 다자간 수출통제체제인 바세나르체제(WA, Wassenaar Arrangement), 미사일기술통제체제(MTCR, Missile Technology Control Regime), 핵공급국그룹(NSG, Nuclear Suppliers Group), 생화학무기 확산 방지를 위한 호주그룹(AG, Australia Group) 등과 연계되어 있음

- 과거에는 주로 군사·무기 관련 물자에 대한 수출통제가 중심이었으나, 최근에는 산업기술·민간기술까지 확장되는 경향이 있음

- 특히 최근에는 반도체·첨단소재·AI 기술 등 전략기술 분야에 대한 통제 강화 움직임이 나타나고 있으며, 2025년 2월 양자컴퓨터·AI반도체·3D프린팅 장비 및 기술 등을 전략물자로 추가 지정함

- 또한 한국이 다자간 수출통제 체제 및 미국, 유럽 등의 해외 독자 통제 체제와의 정렬(alignment)을 강화하고 있다는 분석이 있음[59]

- AI 품목이 군사·보안 응용 가능성, 고성능 연산 능력, 전용 고성능 하드웨어 연계성 등이 확인되면 전략물자로 판정될 가능성이 있음

- 기업은 전략물자 판정 및 수출허가 절차, 최종사용자 확인, 공급망 투명성 확보 등을 통해 수출 통제 체제 변화에 대응할 필요가 있음

- 국내 전략물자 및 전략기술 수출통제 고시는 WA 국제 체제 통제 규정을 반영하고 있음
- 미국, 유럽, 일본 등의 독자 통제 대상 및 통제 기준을 정합(align)하는 방향을 유지함
- AI SW 품목을 개별 통제 대상 AI SW 품목으로 직접 통제하기보다 기존 통제 대상 SW 품목으로 간접 통제하고 있으며, 사용 용도, 수출 국가, 최종 사용자 중심으로 통제함

2.3. AI 기술의 수출통제 전망

2.3.1. 수출통제 정책과 AI 기술의 특성

2.3.1.1. 지정학적 블록화

- 최근 미·중 간 기술 패권 경쟁이 반도체, AI, 양자컴퓨팅 등 첨단 분야 전반으로 확대되면서, 국제 공급망이 지역적으로 '블록화(Bloc-ization)'되는 양상이 있음
- 미국은 2022년 10월 대중국 AI 반도체 칩 수출통제를 시작으로, 첨단 반도체 제조장비, 부품, 소재, SW, 기술까지 통제 대상과 범위를 확장하고 있음
- 동맹국과의 기술 협력 및 공조가 중요한 역할을 하고 있으며, 미국·일본·네덜란드의 반도체 제조 장비 수출통제 공조, 미국, 유럽, 일본 등의 주요 첨단 기술 관련 전략 물자 및 기술의 국가별 독자 통제와 협력이 이루어짐
- 동맹국 및 우호국에는 통제 공조와 통제 완화를 적용해 첨단 기술 교류와 공동 R&D 등을 촉진함으로써, 기술 우위를 집단적으로 유지하고 강화하려는 움직임이 확산됨
- 수출통제 정책이 단순히 기술 보호와 안보 유지 목적에서 더 나아가 국가별 동맹 네트워크의 강화와 기술 우위 확보라는 전략적 협력의 성격을 띠게 됨

2.3.1.2. AI 기술의 범용성

- AI 기술은 군사 목적뿐 아니라 민간, 산업 분야에서의 활용 가능성 및 경제적·사회적 부가가치 창출 효과가 매우 크며, 첨단 산업, 제조업, 의료, 교육 등에서 사회적 혁신 기능을 제공할 수 있음

- 따라서 단순한 기술 보호 차원에서 수출통제를 강력하게 적용할 경우, 고부가가치 창출 및 활용성까지 제약을 받게 되어, 자국 산업 경쟁력 저하로 이어질 수 있음

- 특히, AI 연구개발은 데이터 및 인프라 접근성과 밀접하게 연계되기 때문에, 통제가 과도하면 혁신 생태계 전반에 '기술 장벽'이 형성될 우려가 있음

- 이에 따라, 각국은 군사적 전용 가능성이 낮은 AI 기술·서비스에 대해서는 통제를 완화하거나, 면제·조건부 허가 제도를 도입하는 방향으로 AI 기술의 범용성을 고려하고 있음

2.3.1.3. AI 기술의 혁신 속도

- AI 분야의 기술 발전 주기는 통상 6~12개월 이내로, 기존 하드웨어 중심의 전략 물자 통제 주기인 3~5년보다 매우 짧음[42][43][44]

- 예를 들어, 대규모 AI 모델(LLM)의 파라미터 수, 학습 데이터 규모, 연산 효율성은 매년 2~3배씩 향상되고 있으며, 신제품 출시 주기도 1년 미만으로 단축되고 있음[45][46]

- 이러한 상황에서 정적 통제(static control) 방식이 AI 기술 발전 속도를 따라가기 어렵고, 통제 발효 시점에는 이미 회피 설계 또는 차세대 기술이 등장해 통제가 무력화되는 경우가 많음

- 이에 따라, 통제 사양이나 대상을 기술 발전 추세나 수요, 공급 상황에 따라 동적으로 단기간에 통제 대상이나 사양을 가변하는 동적 통제(dynamic control) 및 조건부 완화 개념이 부상하고 있음[47][48]

  예: 특정 성능 이상은 원칙적으로 통제하되, 동맹국·공동연구 프로젝트·국제인증을 거친 기관에는 한시적으로 허용

- 통제 기준을 연산성능, 모델 크기, 학습 환경 등 다차원적으로 통합 설계해, 상황 변화에 따라 탄력적으로 조정함

- 따라서, 산업 발전을 고려한 진흥 중심의 통제 정책 전환은 단순한 통제 완화가 아니라, 기술 생태계와 안보 리스크 간 균형을 유지하면서 통제를 탄력적이면서 효과적으로 조정하는 것으로 볼 수 있음

2.3.2. AI 기술과 수출통제 패러다임

- 향후 AI 수출통제 정책은 단일한 수출통제 강화나 완화가 아니라, 산업 육성과 안보 확보를 동시에 고려하는 균형 전략으로 진화할 가능성이 있음
- 미국은 반도체 및 AI 핵심 기술 보호라는 통제 목표를 유지하면서도, 국내외 우호국 시장과 기업의 AI 역량 강화를 지원하는 방향으로 수출통제 프레임을 조정중임[49]
- 따라서, AI 기술의 산업적 활용과 발전을 촉진하는 동시에, 기술 보호와 군사적 안보 위협을 최소화하는 '투트랙' 정책을 제도화할 가능성이 높음
- 이를 위해 투자, 보조금 지원, 세제 혜택, 연구 인프라 지원 등 산업 진흥책과, 신규 통제 정책, 캐치올 방식 통제, 수출허가제 등 수출통제 정책을 병행하여 적용함
- 안보·경제 협력을 강화하는 동맹국에는 AI HW, SW, 클라우드 서비스 장벽을 완화하고, 경쟁국, 제재국에는 접근 제한을 적용하는 기조를 유지할 것으로 보임
- 이를 위해 ECCN 내 특정 품목에 대해 화이트리스트 국가 예외 조항을 추가하거나, 우호국 기업에 대한 사전 승인(Pre-Approval) 면제 제도를 도입할 가능성이 있음
- 또한 현재의 연산 성능(TOPS), 성능밀도(GB/s·mm²) 기준을 보다 세분화하고, 산업 발전 추세에 맞게 동적으로 기준을 변경하며, 비군사적 목적의 산업·학술 연구용 제품은 통제 제외하는 방향이 고려될 수 있음

  예: 고성능 GPU가 의료 영상 분석, 기후 예측 모델링 등 특정 용도 한정 사용 시 수출 허가 완화
- 미국, 일본, EU 등 주요국은 AI 기술의 범용성과 전략적 가치를 모두 고려해, 기존의 HW 중심 통제를 넘어 SW, 모델, 데이터, 서비스까지 아우르는 포괄

적 통제 체계를 고려하고 있음[50]

2.3.3. AI 기술의 수출통제 방법 진화

- 빠르게 발전하는 AI 기술을 동적이면서 효과적으로 통제하기 위해서는 통제 방법도 전통적인 통제 및 관리 방법을 개선한 진화된 통제 및 관리 방법의 도입이 필요함

- API 호출량·연산량 모니터링: AI 기능을 원격으로 제공하는 클라우드나 API 환경에 대해, 실시간 연산량 추적(TFLOP-hour), 데이터 입출력량, API 호출 패턴 등을 모니터링하는 기술의 적용 가능성

  - 이를 기반으로 사용자가 우회적인 방법으로 대규모 AI 모델 학습을 수행하거나, 군사 목적의 집약적 연산을 시도할 경우 탐지할 수 있도록 함

- 환경·모델 통합 통제: AI 모델 자체뿐 아니라 AI 학습 환경(컴퓨팅 자원, 데이터셋)에 대한 통제를 포함하여, AI 학습 및 추론 전 과정을 감시하는 통합 통제 체계의 도입 가능성이 고려될 수 있음

  예: 위험 국가 IP에서의 접속 시 자동 차단, 지정된 위험 성능 지표 기준 초과 시 연산 중단 등

- 위험국 접근 로그 공유: WA, G7 차원의 데이터 공유 체계를 통해, 특정 국가나 기관의 의심스러운 접속 이력, API 남용 패턴 등을 실시간으로 교환하여 공동으로 대응함[51]

2.3.4. AI 기술의 수출통제와 국제 협력

- 첨단 AI 기술의 수출통제는 개별 국가의 통제만으로는 효과를 담보하기 어려움. 따라서, 국제 협력과 표준화를 통한 조율은 기술 유출 방지와 동시에 과도한 통제로 인한 산업 발전 위축을 방지하는 핵심 수단으로 부상하고 있음

- WA 참여국들은 AI SW 및 대규모 AI 모델을 통제 대상으로 지정할 경우, 국가별 해석 차이로 인한 불필요한 통제 혼선을 최소화하기 위해 일관된 기능·성능 기준을 수립할 필요성을 인식함

- WA 차원에서 성능 지표(예: 초당 연산량, 처리 데이터 크기)와 사용 목적을 명확히 규정하면, 과도한 범용 SW 통제 문제를 완화할 수 있음

  예: 이미지 인식 AI SW를 통제할 때, 탐지 정확도·프레임 처리 속도를 기준화하여, 군사·감시 용도로만 통제하고 민간 연구·산업 활용은 보호함

- WA 차원에서 API 기반 AI 서비스에 대해 지리적 접근 제한(GEO-IP), 사용자 인증 수준, 모니터링 의무 등을 표준 방법으로 제시하는 방안 논의 가능성이 있음[52]

2.3.5. AI 기술의 수출통제 전망

2.3.5.1. 통제 대상 및 통제 사양 기준 확대

- 최근 AI 기술의 수출통제는 주로 고성능 반도체 칩 등 HW를 대상으로 하고 있으며, 연산 성능(TPP, Total Processing Performance) 및 성능 밀도(PD, Performance Density) 등의 통제 사양이 설정됨

- 기술 발전 추세에 따라 미국 독자 통제 대상인 ECCN 3A090, 4A090 등 고성능 AI 반도체 칩 및 컴퓨터 통제의 세부 성능 사양 기준이 확대될 가능성(메모리 대역폭, 병렬 연산 구조, 특수 연산 유닛(Tensor Core 등)이 있음[53]

2.3.5.2. AI 모델 크기·연산량 기준 통제

- 현재 HW 통제에서 적용 중인 TFLOPS, 성능밀도 개념을 AI SW에도 적용하는 방안이 논의되고 있음[54]

  예: 모델 파라미터 수가 1,000억(100B) 이상이거나, 학습에 소요된 누적 연산량이 10^{25} FLOPs를 초과하는 경우, 해당 모델 또는 학습 SW를 전략물자로 지정

- LLaMA 2, GPT-4, Claude 3, Gemini 1.5 등 초대형 AI 모델이 주요 통제 대상이 될 수 있음

2.3.5.3. 클라우드·API 제공 서비스 통제

- 고성능 AI 반도체 칩이나 메모리를 직접적으로 보유하지 않더라도 클라우드 기반 AI 학습·추론 시스템 및 서비스를 통해 AI 서비스가 원격으로 제공될 수 있다는 것이 통제 이슈로 부상함

- AWS, Microsoft Azure, Google Cloud, Oracle Cloud, Naver Cloud, Tencent Cloud 등 주요 CSP(Cloud Service Provider)가 H100·A100·MI300급 GPU 서버를 임대하여, 고객이 원격으로 대규모 학습을 수행할 수 있는 환경을 제공하고 있음

- 해당 클라우드 서비스 환경은 고성능 반도체 칩과 메모리 등 없이도 동일한 AI 서비스 환경을 제공하므로, 기존의 HW 중심 AI 기술 통제를 무력화할 가능성이 있음

- API 형태로 제공되는 LLM(예: ChatGPT API, Claude API 등)이나, 클라우드 AI 학습 플랫폼(Google Vertex AI, AWS SageMaker 등) 등을 통해 대규모 AI 서비스가 가능함

- 대규모 AI 모델 API 제공 시, 특정 연산량 이상 또는 특정 용도(예: 군사·사이버 작전) 요청을 차단하는 사용량, 사용 목적 기반 통제 도입 가능성이 있음[55]

- 미국은 이러한 원격 AI 서비스 제공을 '사실상 수출'로 간주하는 방안을 검토했으며, 국가/사용자별 IP 차단, 신원 인증 강화, 실시간 사용 모니터링 등을 통한 서비스 접근 차단을 대응 수단으로 논의함

- 특히 중국·러시아·이란·북한과 같이 미국 및 동맹국의 수출통제 대상국이 클라우드를 통해 우회 접근할 가능성이 제기되고 있음

2.3.5.4. SaaS/API 제공 지역 제한

- AI API를 통한 원격 모델 호출이 통제 대상국에 제공되지 않도록, 지리적 접근 제한(Geo-fencing)을 적용하는 방식 도입 가능성이 고려됨[56]

  예: OpenAI가 ChatGPT API를 중국·이란·러시아·북한 IP에서 차단, AWS와 Azure가 GPU 인스턴스 제공 국가를 화이트리스트 방식으로 제한

- 미국 EAR 개정 시, 클라우드 기반 AI 서비스도 '수출'로 간주하여, API 키 발급 자체를 허가제로 전환이 가능함

2.3.5.5. AI 모델 파라미터 통제

- GPT-4, LLaMA 3, Claude, Gemini와 같은 초거대 AI 모델이나 대규모 멀티 모달 AI 모델의 파라미터는 학습이 완료된 AI 시스템의 핵심 정보로 이를 통해 고성능 AI 시스템 구축이나 재현이 가능함
- 최근에는 완성된 대규모 언어모델(LLM)의 파라미터 자체를 전략물자에 준하는 통제 대상으로 지정하는 가능성이 논의되고 있음
- 이를 통해 군사 전략 분석, 전술 시뮬레이션, 자동 목표 식별, 암호 분석, 첨단 무기 제어, 사이버 공격 자동화, 생화학 무기 설계 등 고위험 분야에 활용 가능한 AI 모델의 확산을 방지하고자 함
- 신규 통제 리스트 코드 신설을 통해, 특정 파라미터 수 이상, 특정 성능 지표 이상인 AI 모델의 파라미터 이전을 수출 허가 대상으로 지정할 가능성이 있음[57]
- AI 모델의 API 접근뿐 아니라, AI 모델 파라미터의 전송, 다운로드, 클라우드 저장소 공유 등도 수출로 간주하고 관리를 강화함

2.3.5.6. AI 학습 데이터셋 및 환경 통합 통제

- AI 성능의 핵심 요소가 모델 구조 + 학습 데이터 + 학습 환경이라는 점에서, 세 가지를 패키지 형태로 통제하는 방식이 논의 중에 있음[58]
- AI 학습 데이터셋의 규모나 유형(민감 영상, 위성 영상, 군사기밀 포함 여부 등) 및 학습 환경 특성(총 연산량, 학습 시간 등)을 통합적으로 통제하는 'AI 개발 환경 총량 통제' 체계의 도입 가능성도 있음
- 통제 범위가 기존의 AI 반도체 칩 HW나 SW뿐 아니라 AI 모델 자체 및 학습 데이터·환경까지로 그 대상과 범위가 확대될 가능성이 있음

  통제 대상 후보 예:

완성된 LLM·멀티모달 모델의 파라미터

특정 규모 이상 파라미터 모델(예: 1,000억+ 파라미터)

대규모 학습 데이터셋(군사·핵·생물무기 관련 포함)

초대형 학습 환경(ExaFLOP급 연산 클러스터)

2.3.5.7. 자동화 무기·사이버 공격용 AI SW 확산

- 드론 군집 제어, 실시간 영상 표적 식별, 자율 주행 차량, 해킹 툴 자동화 등 군사용으로 활용가능한 AI SW의 확산이 진행되고 있음
- 특히 사이버 공격 자동화 AI는 취약점 스캐닝, 공격 코드 생성, 익스플로잇 실행까지 전 과정을 자동화할 수 있어, 기존의 수동 해킹보다 훨씬 빠른 속도로 공격이 가능함
- 이로 인해 AI SW 자체가 무기에 준하는 것으로 간주될 가능성이 커지고 있어 통제 대상이 될 수 있음

III AI SW 품목의 WA 수출통제

제3장 AI SW 품목의 WA 수출통제

- 본 장에서는 AI 기술을 반도체 HW부터 운영 및 관리 SW까지 수직 계층적인 분류와 특성/기능 중심의 품목 분류를 통해 AI 기술을 분류하고, 이를 WA의 수출통제 대상 품목[60]과 연계하여 분석함

3.1. AI SW 품목의 분류

- AI 관련 기술을 반도체/칩셋 HW부터 응용 SW, 운영/관리 SW까지 수직 계층적으로 다음과 같이 구분해볼 수 있음

표 2 AI 관련 기술의 수직 계층적 분류

구분	세부 구분	설명
HW	반도체/칩셋	- 학습/추론 담당 핵심 연산 칩 - GPU, TPU, NPU, FPGA, ASIC 등 - 대규모 고속 병렬 연산 - 고대역폭 메모리(HBM), 저지연 인터커넥트(NVLink 등) 활용
	시스템 인프라	- 고성능 반도체/칩셋 포함 컴퓨터, 서버 및 슈퍼컴퓨터 - GPU 노드 클러스터/클라우드 - NVSwitch/InfiniBand 등 네트워크 연결
	스토리지/네트워크	- 학습 데이터 저장·전송 인프라 - HBM, DDR, NVMe SSD, 오브젝트 스토리지 - InfiniBand/Ethernet, CXL 기반 메모리 풀링
	엣지/IoT 디바이스	- 모바일·차량·IoT 환경에서 실시간 추론 수행 - 소형, 경량화 AI 장치 - 스마트폰, IoT 센서 등 - 로봇, 드론, 자율주행 차량/선박/항공기
SW	AI 프레임워크	- 고성능 HW 위에서 동작하는 학습/추론 툴킷 - 병렬 연산, 분산 학습, 혼합 정밀 연산 등 - TensorFlow, PyTorch, JAX 등
	모델/라이브러리	- LLM·LVM 등 영상·음성 모델 및 API - Hugging Face Transformers, OpenAI API - NVIDIA NeMo 플랫폼, LangChain 프레임워크 등

	응용 SW	- 사용자 서비스용 AI 응용 - 대화, 음성 인식/합성 - 이미지/영상 분석/생성 - 민간용, 산업용, 군용, 바이오/의료용
	운영/관리 SW	- AI 서비스의 개발·배포·운영 관리 - 모델 버전관리, MLOps, 모니터링, 드리프트 대응 기능 - Kubeflow, MLflow, Ray, Scale AI 등

- AI 기술 관련 품목을 수출통제 대상 품목과 연계하여 주요 특성과 기능을 중심으로 분석해보면 다음과 같이 구분할 수 있음(표 3 참조)

(1) 암호화

(2) AI 연산 인프라

(3) AI 모델 학습

(4) AI 응용

(4-1) 음성 인식·합성

(4-2) 영상 분석·생성

(4-3) 자연어 처리

(4-4) 추천·데이터 마이닝

(5) AI 자율 주행/로보틱스

(6) AI 네트워크 감시/분석/보안

(6-1) 네트워크 감시·분석

(6-2) 보안/침투

(7) 군사 감시/정찰 AI

(8) 바이오/의료 AI

표 3 AI 기술의 특성/기능별 분류

구분	주요 내용	관련 품목 예	관련 통제 조항
(1) 암호화	암호화 알고리즘, 모듈, 기능	보안 AI 프레임워크, 암호화 기술	5A002, 5D002, 5E002
(2) AI 연산 인프라	고성능 AI 컴퓨팅	LLM 학습용 GPU 서버, AI 슈퍼컴퓨터	4A003, 4A090, 4D001, 4D090, 4E001
(3) AI 모델 학습	AI 모델/프레임워크	PyTorch, TensorFlow, Horovod 등	4D0001, 4D090, 4E001
(4) AI 응용	AI 분석, 생성 응용 기술	영상·음성 인식, 생성형 AI 등	4A003, 4A090, 4D001, 4D090, 4E001, 6A001~6A008, 6D001~6D003, 6E001~6E003
(4-1) 음성 인식·합성	음성 데이터 분석, 생성	AI 음성 분석, 합성 시스템	4A003, 4A090, 4D001, 4D090, 4E001
(4-2) 영상 분석·생성	영상 처리, 인식, 생성	위성·드론 영상 분석 AI	4A003, 4A090, 4D001, 4E001, 6A001~6A008, 6D001~6D003, 6E001~6E003
(4-3) 자연어 처리	언어 처리, 분석, 생성	AI 언어 분석, 번역 시스템	4A003, 4A090, 4D001, 4E001
(4-4) 추천·데이터 마이닝	대규모 데이터 분석	AI 추천·행동패턴 분석 시스템	4A003, 4A090, 4D001, 4E001
(5) AI 자율주행/로보틱스	자율주행·로봇용 AI 제어·항법 기술	AI 차량 제어, 항법 알고리즘	6A001~6A008, 7A001~7A004, 8A001, 8A002, 9A001, 9A002, 9A007, 6D001~6D003, 7D001~7D004, 8D001~8D002, 9D001, 9D002, 9D004, 9D005, 6E0001~6E003, 7E0001~7E004, 8E001~8E003, 9E001~9E003

구분	주요 내용	관련 품목 예	관련 통제 조항
(6) AI 네트워크 감시/분석/보안	네트워크 감시, 분석, 보안	심층 패킷 분석 스스템, AI 보안 분석/공격 시스템	4A005, 5A001.j, 4D004, 5D001.c, 4E001, 5E001
(6-1) 네트워크 감시·분석	네트워크 트래픽 모니터링·패킷분석	AI 트래픽 감시 시스템	5A001.j, 5D001.c, 5E001
(6-2) 보안/침투	침입 탐지 및 공격 자동화	AI 침입 테스트·보안 평가 SW	4A005, 4D004, 4E001
(7) 군사 감시/정찰 AI	위성·드론 영상 기반 표적 탐지·식별 기술	SAR·IR 영상 인식, AI 표적추적	6A001~6A003, 6D001~6D003, 6E001~6E003
(8) 바이오/의료 AI	생체신호 분석, 질병 예측 등 의료용 AI	의료 영상 분석 시스템 군사 용도 활용 시 통제 검토 필요	6A001~6A003, 6D001~6D003, 6E001~6E003

3.2. WA의 AI SW 품목 통제 대상

- WA는 군사용과 민간용 이중용도로 사용이 가능한 수출통제 대상 품목을 품목의 종류별로 구분하여 CAT 0 ~ CAT 9 10개의 품목 구분(Category)으로 나눔

표 4 WA 통제 리스트 품목 구분

CAT	구분(영문)	구분(한글)	통제 품목 예
CAT 0	Nuclear Materials, Facilities and Equipment	원자력 소재, 시설 및 장비	핵연료, 원자로, 관련 장비
CAT 1	Special Materials and Related Equipment	특수 소재 및 관련 장비	고성능 합금, 복합재, 특수 세라믹, 내열재
CAT 2	Materials Processing	소재 가공	기계가공, 금속가공, 복합재 제조 장비
CAT 3	Electronics	전자	집적회로(IC), 반도체 장치, 전자 부품
CAT 4	Computers	컴퓨터	슈퍼컴퓨터, 고성능 서버
CAT 5 Part 1	Telecommunications	정보통신	위성통신, 광통신, 무선통신 장비
CAT 5 Part 2	Information Security	정보보안	암호화 장비/소프트웨어
CAT 6	Sensors and Lasers	센서 및 레이저	광학센서, 레이저, 이미징 장치
CAT 7	Navigation and Avionics	항법 및 항공전자	INS(관성항법), 항공기 전자 장치
CAT 8	Marine	해양	잠수함, 해양 장비, 해양 전자 장치
CAT 9	Aerospace and Propulsion	항공우주 및 추진체	로켓, 터보제트 엔진, 우주 발사체

- 각 카테고리 내에서 세부 품목 구분(Sub-category)은 A ~ E로 나누어 통제 대상 품목(예: 2A001, 4B002 등)이 정의됨

표 5 WA 통제 리스트 세부 품목 구분

코드	의미(영문)	의미(한글)	통제 품목 예
A	Systems, Equipment, Components	시스템, 장비, 구성품	4A001(고성능 컴퓨터 장비)
B	Test, Inspection and Production Equipment	시험, 검사 및 생산 장비	3B001(반도체 제조 장비)
C	Materials	소재, 물질	1C001(화학 물질)
D	Software	소프트웨어	5D002(암호화 소프트웨어)
E	Technology	기술	3E001(전자 기술)

- 특히 SW 품목은 세부 품목 구분 D에 해당하고, 기술은 세부 품목 구분 E에 해당됨(예: 5D002, 5E001 등)
- 통제 대상 HW, SW의 개발, 생산, 사용과 관련된 AI 모델 아키텍쳐, 구조, 학습 기법, 최적화 알고리즘 등의 '기술(Technology)'은 세부 품목 구분 E에 해당되어 통제가 가능함(예: 4E001, 5E001, 6E001 등)

- WA 이중 용도 수출통제 리스트 중 AI SW와 관련되는 통제 품목은 다음과 같음(특성/기능 중심의 AI SW 분류 대상 품목과 연계한 표 3 참조)

- 4D001: 고성능 컴퓨터(4A003 등)의 운영 및 관리용 소프트웨어로, 대규모 연산·분산 학습을 제어하는 클러스터 스케줄러, 운영체제 등이 포함됨
- 4D004: 침입 SW의 생성·제어에 특화된 전용 프로그램으로, 보안 테스트용 또는 AI 기반 공격·침투 자동화 시스템에도 적용될 수 있음
- 5D001.c: 통신 감시 및 패킷 분석용 소프트웨어로, 네트워크 트래픽의 수집·분

석·필터링을 수행하여 통신 흐름과 이상 행위를 식별하는 데 사용될 수 있으며, Deep Packet Inspection(DPI) 기반 네트워크 모니터링, AI 트래픽 분석, 보안 감시 시스템에도 적용될 수 있음

- 5D002: 대칭/비대칭 암호화 기능을 포함하는 보안용/일반 소프트웨어로, VPN, TLS 등 통신보안 SW와 더불어 보안 AI 모델/프레임워크 등도 통제 대상이 될 수 있음

- 6D001~6D003: 센서·광학 센서·레이더 등 감시·정찰용 장비의 제어 및 영상처리 SW로, SAR, IR 영상의 AI 분석, AI 위성·드론 영상 인식 등에 사용될 수 있음

- 7D001: 항공기·미사일·UAV의 항법·유도·자세제어를 수행하는 핵심 소프트웨어로, INS/GPS 융합, 관성항법 오차보정, 비행 안정화 알고리즘 등에 사용되며, AI 기반 자율비행·경로최적화·추락방지 시스템에도 적용될 수 있음

- 7D002: 항공기·미사일·UAV의 비행경로 산출, 속도·고도 최적화, 환경 변화 대응 시뮬레이션을 위한 소프트웨어로, AI 기반 비행경로 예측·충돌 회피·기상 대응 모델이 포함될 경우 통제될 수 있음

- 7D003: 정밀위치결정(PNT) 기능을 위한 GPS 보정, INS 추정 알고리즘, 센서 융합 필터링 등으로 구성되며, AI 기반 센서 융합 항법, 드론 정밀착륙, 자율주행 UAV의 오차 보정 기능을 포함할 경우 통제 대상이 될 수 있음

- 7D004: 무인기(UAV), 항공기, 미사일 등의 자세 안정화, 자동조종, 추력 제어를 수행하는 동적 제어 SW로, AI 기반 자율비행, 경로추종, 비행 효율 최적화·추력제어 알고리즘이 포함되면 통제 적용이 가능함

- 8D001: 잠수함, 수중 센서, 해양 음향 탐지 장비 등 8A, 8B 품목의 운용·제어 SW로 수중 음향 분석, 음향 신호 처리, UUV(무인잠수정) 움직임 제어, 수중 항법 연산, AI 기반 수중 표적 탐지·음향 패턴 분석 SW도 해당될 수 있음

- 8D002: 해양항법 및 제어 시스템용 소프트웨어로, 잠수정·무인수중운항체(UUV)의 경로제어 및 충돌회피 기능에 사용될 수 있으며, AI 기반 수중항법·센서 융합 제어 및 해양자율운항 기술에도 적용될 수 있음

- 8D008: 무인운항체(UUV/USV) 제어용 소프트웨어로, 자율운항선박 및 무인잠수정의 경로계획·항법통제 기능에 사용될 수 있으며, AI 자율운항 플랫폼의 실시간 제어·예측 알고리즘에도 사용될 수 있음

- 9D001: 항공기, 로켓, 재사용 우주 발사체 등 9A 관련 장비의 설계·모델링·시험용 SW로 비행제어 알고리즘 설계, 공력 특성 모델링, 추진·추력 시뮬레이션, AI 기반 비행 안정화, 공력 최적화 설계용 SW도 해당될 수 있음
- 9D002: 항공기·엔진·로켓 부품의 정밀 제조·가공·조립 과정 제어 NC/CNC 장비용 SW로 복합재 생산, 정밀 절삭·성형, 터빈 블레이드 제작 등 9B 설비 사용 SW, AI 기반 공정 최적화, 결함 예측·검사 자동화 SW도 포함될 수 있음
- 9D004: 항공기 및 로켓의 추진제어용 소프트웨어로, 비행제어, 엔진 추력분배, 항로안정화 시스템에 사용될 수 있으며, AI 기반 비행경로 최적화, 항공 추진 제어 알고리즘에도 적용될 수 있음
- 9D005: 추진체계의 설계 및 시뮬레이션용 소프트웨어로, 엔진시험·추력시뮬레이션·열역학 모델링 등에 사용될 수 있으며, AI 기반 추진성능 예측 및 비행 시뮬레이션 최적화 시스템에도 활용될 수 있음
- 전략 기술 통제 대상인 3E001, 4E001, 5E001, 5E002, 6E001~6E003, 7E001~7E004, 8E001~8E003, 9E001~9E003 등은 각각 대응하는 HW·SW의 개발·생산·사용 기술을 통제하며, AI 관련 기술 설계 및 최적화 알고리즘도 포함됨

표 6 WA 통제 번호 관련 AI SW 품목

품목	통제 품목 번호	통제 대상	주요 품목 예시	관련 AI 품목 (표 3 참조)	AI 관련 예시
HW	4A003	특정 성능 이상(FLOPS·연결성능 기준) 고성능 컴퓨터	슈퍼컴퓨터, 대형 서버	(2) AI 연산 인프라 (3) AI 모델 학습	LLM 학습용 GPU 서버, DGX SuperPOD
HW	4A005	침입 SW용 시스템, 장비, 구성품	침입 SW 시스템	(6-2) 보안/침투	AI 적용 침입 SW 시스템
HW	5A001.j	통신 감시·감청 장비	통신 감청·모니터링 장비	(6-1) 네트워크 감시·분석	AI 기반 트래픽 이상 탐지·행동 패턴 분석 시스템
HW	5A002	암호화 포함 HW	암호화 모듈, 보안 라우터	(1) 암호화	보안 컴퓨팅 지원 CPU/GPU, HSM
HW	6A001~6A008	영상/광학, 레이저, 레이더, 초음파, 광학/이미징, 항공기/우주/위성항법, 자기장, 위치 탐색 센서 등	위성·드론 영상 시스템	(4-2) 영상 분석·생성	위성·드론 AI 영상 시스템
HW	7A001~7A004	항법 장비, 관성 항법 장치(INS), 자이로스코프 등	항법 센서, 항공기 관성항법 시스템	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 기반 항법 융합제어, 자율주행 경로추적 장치
HW	8A001	잠수정, 원격무인수중체, 무인잠수정	군사용 또는 이중용도 자율운항 잠수정	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 자율수중항법, 지형기반 항법
HW	8A002	해양 시스템 및 장비	잠수정용 제어장치	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 기반 수중 항법 시스템, 자율잠수정 제어장치
HW	9A001	항공기 가스터빈 엔진	민·군용 항공기 엔진	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 기반 자동비행·경로최적화
HW	9A002	선박 가스터빈 엔진	선박 엔진	(5) AI 자율 주행/로보틱스	자율비행 드론·군사 감시 AI

				(7) 군사 감시/정찰 AI	
HW	9A007	로켓 추진 시스템	항공·우주 로켓 추진 장치	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 기반 비행제어 모듈
SW	4D001	고성능 컴퓨터 운영 SW, 클러스터 관리 SW	고성능 컴퓨팅 OS, 클러스터 스케줄러	(2) AI 연산 인프라 (3) AI 모델 학습	AI 분산 학습 관리 SW
SW	4D004	침입 SW용 전용 SW	침입 SW용 전용 SW	(6-2) 보안/침투	AI 적용 침입 SW용 전용 SW
SW	5D001.c	통신 감시·패킷 분석 SW	DPI, 네트워크 분석기	(6-1) 네트워크 감시·분석	AI 트래픽 분석 및 네트워크 감시 SW
SW	5D002	암호화 기능 포함 SW	보안 통신 SW, 암호화 API	(1) 암호화	보안 AI 모델·프레임워크, E2E 암호화 적용 AI 서비스
SW	6D001~6D003	특정 센서·광학·레이더·ATC 관련 SW	SAR 처리 SW, 고해상도 IR 영상 SW	(4-2) 영상 분석·생성	위성·드론 영상 AI 분석 SW, 군사 감시 AI
SW	7D001~7D004	항법·유도 시스템 제어 SW	항공기 INS 제어 SW, GPS 보정 SW	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	자율비행 제어 SW, AI 경로 제어 SW, AI 기반 융합 항법·추적 SW
SW	8D001	해양항법 및 제어 SW	잠수정 제어 SW	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 수중 항법 및 충돌회피 SW
SW	8D002	프로펠러 제어용 SW	프로펠러 소음 제어 SW	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 수중 소음 감소 SW
SW	9D001	항공기 엔진 추진제어 SW	항공기 엔진 제어 SW	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 비행 제어 SW
SW	9D002	선박 엔진 추진제어 SW	선박 엔진 제어 SW	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 엔진 제어 최적화 SW
SW	9D004	가스터빈 엔진 추진제어 SW	가스터진 엔진 제어 SW	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 가스터빈 엔진 제어 최적화 SW
SW	9D005	우주비행체 설계·시뮬레이션 SW	우주비행체 운용 SW	(5) AI 자율 주행/로보틱스	AI 우주비행체 시뮬레이션 SW

				(7) 군사 감시/정찰 AI	
기술	3E001	3A090 반도체 제조/설계 기술	첨단 반도체 공정 기술	(2) AI 연산 인프라 (3) AI 모델 학습	AI 전용 반도체(TPU 등) 설계 기술
기술	4E001	고성능 컴퓨터 개발·생산·사용, 침입 SW 개발 기술	슈퍼컴퓨터 설계/제작 기술, 침입 SW 기술	(2) AI 연산 인프라 (3) AI 모델 학습	AI 고성능 컴퓨팅 아키텍처, GPU·TPU 최적화 기술, AI 침입 SW 기술
기술	5E001	5A001, 5D001 관련 정보보안·통신 감시 기술	패킷 분석 알고리즘, 네트워크 감시 장비 제어 기술	(6-2) 보안/침투	AI 기반 DPI(Deep Packet Inspection) 분석 기술, 이상 트래픽 탐지 모델
기술	5E002	5D002 SW 개발·생산·사용 기술	암호화 SW 개발 기술	(1) 암호화	보안 AI 모델 개발 기술
기술	6E001~6E003	6A, 6D 개발, 생산 기술	센서·레이저 등 개발 설계 기술	(4-2) 영상 분석·생성	AI 기반 센서 설계 기술
기술	7E001~7E004	항법·유도 시스템 개발 기술	유도제어 알고리즘	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 자율 항법·정밀위치 기술
기술	8E001~8E003	수중항법, 자율운항 시스템 설계 기술	잠수정 항법 시스템 기술	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 수중 항법 및 제어 기술, AI 자율운항 알고리즘
기술	9E001~9E003	우주비행체 제어 기술	우주비행체 제어 기술	(5) AI 자율 주행/로보틱스 (7) 군사 감시/정찰 AI	AI 기반 비행 제어 및 항공 추진 최적화 기술

IV AI SW 품목의 국가별 수출통제

제4장 AI SW 품목의 국가별 수출통제

- 본 장에서는 WA 수출통제 대상과 비교하여 미국, 유럽, 일본, 한국의 국가별 수출통제 대상에 대해 살펴보고자 함
- 미국은 AI 전용 통제 대상 품목을 신설하여 유럽, 일본 등 다른 국가와 달리 AI 품목을 명시적으로 구분하여 직접 통제함
- 유럽은 기본적으로 WA 통제 체제를 기반으로 하며, AI 품목을 간접적으로 통제하고, 별도의 세부 운영 지침 등을 운영함
- 일본도 기본적으로 WA 통제 체제를 기반으로 하며, AI 품목을 간접적으로 통제하고, 별도의 성능 지표, 시험 장비 예외, 민수/연구 용도 예외 등 운용 지침을 세분화하여 운영함
- 한국도 기본적으로 WA 통제 체제를 기반으로 하면서 AI 품목을 간접적으로 통제하고, 별도의 통제 대상 판정 지침 등을 운영함

4.1. 미국 독자 통제 품목

- 미국의 전략물자 수출통제는 EAR(Export Administration Regulations)에 기반하며, ECCN(Export Control Classification Number) 체계로 관리됨[61][62]
- 국제 통제 체제(Wassenaar Arrangement, WA)는 회원국들의 합의를 통해 통제 대상 품목을 정하지만, 미국·EU·일본 등 주요국은 AI 기술의 민감성을 감안해 WA 통제 대상 품목 이외의 독자 통제 제도를 도입하고 있음
- 미국은 AI 전용 ECCN 3A090, 4A090, 4D090, 4E091 등을 신설하여 다른 국가와 달리 AI 품목을 명시적으로 구분하여 통제함
- 미국은 FDPR을 확장 적용하여 미국 기술, 장비 또는 SW를 사용한 제3국 생산품도 통제 대상이 되므로 주의할 필요가 있음
- 성능 기반 통제로 초당 부동 소수점 연산 횟수(FLOPS), 대역폭, 패키지 크기

등 정량적 임계치 기준을 제시함

- AI 학습·추론을 위한 플랫폼, 프레임워크도 4D090으로 관리함
- 중국·마카오·러시아 등 특정 지역은 전면 수출 금지 또는 사전허가제를 적용하여 통제함

- 미국은 EAR을 통해 AI 학습용 고성능 HW와 이를 지원하는 SW를 직접 통제함

  고성능 AI 컴퓨팅 반도체 칩, 컴퓨터 등 HW(3A090, 4A090)

  고성능 AI 컴퓨팅 SW(3D001, 4D090)

  고성능 AI 반도체 칩, 컴퓨터 등 설계 기술(3E001, 4E001, 4E091)

- 미국의 AI SW 품목 및 기술 관련 주요 통제 대상은 다음과 같이 구분할 수 있음

- 3D001(고성능 AI 칩 SW)

  고성능 AI 반도체 칩(3A090)의 개발·생산·사용을 위한 SW로, 설계자동화(EDA, Electronic Design Automation) 툴, 시뮬레이션 프로그램 등 AI 가속기 개발 핵심 SW 등이 포함됨

- 4D090(고성능 AI 컴퓨팅 SW)

  AI 학습·추론을 위한 고성능 컴퓨팅용 SW로, 딥러닝 학습 프레임워크(PyTorch DDP, Horovod 등) 및 모델 최적화·분산처리 SW 등이 통제 대상이 될 수 있음

- 3E001(고성능 AI 반도체 칩 설계 기술)

  3A090 반도체 개발·생산 기술로 첨단 반도체 공정 설계, AI 전용 칩 설계 기

술(EDA·설계문서 포함)을 포괄함

- 4E001(고성능 AI 컴퓨팅 설계 기술)

4A090·4D090 관련 고성능 컴퓨터 HW/SW 개발·생산·사용 기술로, 고성능 컴퓨팅·AI 시스템 아키텍처 설계, 학습 클러스터 최적화 기술을 포괄함

- 4E091(AI 모델 기술)

AI 모델 웨이트 및 기술 데이터 등 관련 기술로 학습 완료된 LLM 파라미터나 모델 웨이트 등, AI 모델 자체를 기술 데이터로 간주함

4E091은 2023년 신설되어 2024년에 삭제되었지만, WMD(대량살상무기)·군사정보용 등에 대해 Part 744 캐치올 규정(red flag) 하에 허가 대상이 됨

표 7 미국 독자 통제 대상 품목

품목	ECCN	통제 대상	주요 예시	비고	반영 시기
HW	**3A090**	고성능 AI 연산용 집적회로 (통제 기준: TPP, 성능·대역폭)	NVIDIA A100/H100, AMD MI250/MI300, Huawei Ascend 910C 등	2022 최신 EAR 신설 AI 가속기 통제 핵심	2022년 10월 7일 신설
HW	**4A090**	3A090 칩 탑재 서버/시스템	NVIDIA DGX 서버, AI 슈퍼컴퓨터 (SuperPOD 등)	3A090 확장 통제	2022년 10월 7일 신설 / 2023년 10월 보강
SW	**3D001**	3A090 개발·생산 SW	3A090 개발 생산 SW	2022 최신 EAR 신설 AI 가속기 통제 핵심	2022년 10월 7일 신설
SW	**4D090**	AI 학습·추론용 SW (3A090/4A090 관련)	딥러닝 학습 SW, 분산 학습 프레임워크(PyTorch DDP, Horovod), 모델 최적화 SW	2022 EAR 신설 AI 학습용 SW	2022년 10월 7일 신설
기술	**3E001**	3A090 반도체 칩 개발·생산 기술	첨단 반도체 공정 설계, AI 가속기 설계 기술	기술문서·매뉴얼·EDA 툴링 포함	기존 조항 (1998 제정 / 2022년 12월 갱신)
기술	**4E001**	4A090, 4D090 고성능 컴퓨터 HW/SW 개발·생산·사용 기술	고성능 컴퓨터 설계·생산 기술	고성능 컴퓨팅/AI 시스템 기술 문서	기존 조항 (1998 제정 / 2022년 개정)
기술	**4E091**	AI 모델 웨이트·기술 데이터	학습 완료 LLM 파라미터, 모델 가중치	2023 신설 → 2024 삭제(철회) (Part 744 캐치올 적용)	2023년 10월 25일 신설

4.2. 유럽(EU) 통제 품목

- EU는 WA 통제 리스트를 기본적으로 그대로 반영하면서, 최신 기술 발전에 따라 성능 기준·보안 기능·AI 응용 가능성 등을 중심으로 보완함[63][64]
- 특히 고성능 컴퓨팅, 암호화, 감시·정찰 센서 기술 등 AI 학습·추론·분석에 직접 활용 가능한 기술군을 중점 관리함
- 미국처럼 별도 EAR 코드(3A090, 4D090 등)를 신설하지 않고, 기존 WA 통제 대상(4A003, 4D001, 5D002 등) 내에서 AI 기술을 포괄 적용하는 방식을 사용함
- AI 기술을 별도 통제 조항으로 분리하지 않고, 기존 WA 품목 내에서 포괄 관리함
- APP(Adjusted Peak Performance) 지표 및 보안성능 기준 등을 개정 반영함
- 민수용·교육용 목적 예외 등(Mass Market, 연구 면제) 조항을 명시적으로 운용함
- AI 감시·정찰·암호화 기술에 대해서는 인권·안보 리스크 중심으로 심사를 강화함

- 이중 AI SW 관련 품목은 다음과 같은 것들이 있음

- 4D001(컴퓨터 SW)

  고성능 컴퓨터(4A003 등)의 운용 및 관리용 소프트웨어로, 대규모 연산·분산 학습을 제어하는 클러스터 스케줄러, 운영체제 등이 포함됨

- 4D004(침입 SW)

  침입 SW의 생성·제어에 특화된 전용 프로그램으로, 보안 테스트용 또는 AI

기반 공격·침투 자동화 시스템에도 적용될 수 있음

- 5D001.c (통신 감시·패킷 분석 SW)

DPI(Deep Packet Inspection) 등 네트워크 감시·패킷 분석용 소프트웨어를 포함하며, AI 기반 트래픽 분석 및 이상 탐지 SW가 감시·정보수집 목적으로 사용될 경우 통제 가능성이 있음

- 5D002(암호화 기능 SW)

대칭/비대칭 암호화 기능을 포함하는 보안용/일반 소프트웨어로, VPN, TLS 등 통신보안 SW와 더불어 보안 AI 모델/프레임워크 등도 통제 대상이 될 수 있음

- 6D001~6D003((센서·광학·레이더 SW)

센서·광학·레이더 등 감시·정찰용 장비의 제어 및 영상 처리 SW로, SAR, IR 영상의 AI 분석, AI 위성·드론 영상 인식 등에 사용될 수 있음

- 7D001~7D004 (항법·유도 제어 SW)

항법 및 INS, GPS 보정, 자율항법 알고리즘 SW를 포함하며, AI 자율비행 제어, 경로예측 SW 등 항법 알고리즘 포함이 가능함

- 8D001~8D002 (해양항법 및 자율운항체 제어 SW)

잠수정, 자율선박 등 해양 자율운항 시스템 제어 SW를 포함하며, AI 기반 항로 계획, 충돌 회피, 자율운항 SW 포함이 가능함

- 9D001 / 9D002 / 9D004 / 9D005 (항공기·로켓 추진·제어 SW)

비행제어, 추진제어, 시뮬레이션 SW 등을 포함하며, AI 기반 항공기 비행 제

어, 추진 체계 최적화 SW 포함이 가능함

- 전략 기술 통제 대상인 3E, 4E, 5E, 6E, 7E, 8E, 9E 등은 각각 대응하는 HW·SW의 개발·생산·사용 기술을 통제하며, AI 관련 기술 설계 및 최적화 알고리즘도 포함됨

- 3E001(전자부품 기술)

  3A001 등 전자 부품의 개발·생산·사용 기술로 고성능 집적회로/FPGA 설계 기술, 고속 ADC/DAC 설계 기술 등을 포함함

- 4E001(고성능 컴퓨팅 기술)

  4A00x(특히 4A003) 및 관련 고성능 컴퓨터용 SW(4D001)의 개발·생산·사용 기술로 고성능 컴퓨팅/AI 클러스터 아키텍처, 병렬화·스케줄링 최적화, 대규모 분산학습 운영 기술이 포함될 수 있음

- 5E001 / 5E002 (감시·암호화 SW 관련 기술)

  5A001, 5D001, 5D002 관련 기술로, DPI 분석·보안통신·암호화 알고리즘 기술 포함하며, AI DPI 분석·보안통신 암호화 기술 반영 가능함

- 6E001~6E003(센서 기술)

  6A/6B/6D 센서, 이미징 품목의 개발·생산·사용 기술로 IR/열영상, SAR 영상처리·보정·해석 알고리즘, AI 기반 표적 탐지 설계 등이 포함될 수 있음

- 7E001~7E004 (항법·유도 시스템 개발 기술)

  항법·유도 알고리즘, GPS/INS 융합 시스템 설계 기술 포함하며, AI 자율항법·정밀위치 기술 등 적용이 가능함

- 8E002~8E004 (해양항법·자율운항 시스템 기술)

  잠수정, 자율운항체 시스템 설계 기술이 포함하며, AI 자율운항 알고리즘, 충돌회피 기술이 포함될 수 있음

- 9E001~9E003 (항공기 추진제어 기술)

  항공기·로켓·우주비행체 추진·비행 제어 관련 기술을 포함하며, AI 기반 추진 제어·비행 최적화 기술 반영이 가능함

표 8 EU 통제 대상 품목

구분	항목 번호	품목	EU Annex I (2021/821, 2025-09-08 반영)	차이점 및 비교
HW	3A001	고성능 IC, A/D-D/A 변환기, 마이크로프로세서 등	WA 와 동일 번호	성능·주파수·분해능 등 수치 주기적 개선
HW	4A003	고성능 컴퓨터 및 고성능 컴퓨팅 조립체	WA 와 동일 번호	APP 기준 동일 / AI 학습용 서버 포함 가능성
HW	4A005	침입 SW 용 시스템·장비·구성품	WA 와 동일 번호	사이버보안·침투 테스트 장비 명시 강화
HW	5A002	암호화 기능 포함 HW	WA 와 동일 번호	Mass-Market 조항 예외 규정 강화
HW	6A001~6A008	광학·레이저·레이더 등 센서류 전체	WA 와 동일 번호	민수 감시/항법 목적 비적용 명시
HW	7A001~7A004	항법·유도·자이로/관성항법 시스템	WA 와 동일 번호	AI 항법·유도 시스템 활용 가능성 논의 중 (EU 권고 유지)
HW	8A001 / 8A002	해양·무인수중항법 및 로봇 플랫폼	WA 와 동일 번호	AI 자율 운항체 통제 필요성 검토 (EU 기술위원회)
HW	9A001	항공기 가스터빈 엔진	WA 와 동일 번호	AI 기반 자동비행·경로최적화
HW	9A002	선박 가스터빈 엔진	WA 와 동일 번호	자율비행 드론·군사 감시 AI
HW	9A007	로켓 추진 시스템	WA 와 동일 번호	AI 기반 비행제어 모듈
SW	4D001	고성능 컴퓨팅 운용·클러스터 관리 SW	WA 와 동일 번호	고성능 컴퓨팅·AI 병렬 학습 프레임워크 적용
SW	4D004	침입 SW 용 전용 SW	WA 와 동일 번호	AI 자동화 침투 SW 포함 가능성 명시
SW	5D001.c	통신 감시·패킷 분석 SW	WA 와 동일 번호	심층 패킷 분석(DPI), AI 트래픽 분석 SW 포함 가능성 (감시 목적 시 적용)
SW	5D002	암호화 기능 포함 SW	WA 와 동일 번호	Mass-Market 예외 조항 유지
SW	6D001~6D003	센서·광학·레이더 관련 SW	WA 와 동일 번호	민수 감시/정찰 목적 예외 주석 추가
SW	7D001~7D004	항법·유도 제어 SW	WA 와 동일 번호	AI 자율비행·경로 예측 SW 포함 가능성
SW	8D001 / 8D002	해양 항법 및 자율 운항체 제어 SW	WA 와 동일 번호	AI 자율선박 제어 SW 적용 가능성
SW	9D001 / 9D002 / 9D004 /	항공기·로켓·우주비행체 추진 및 제어 SW	WA 와 동일 번호	AI 비행 제어·추진 최적화 SW 포함

구분	항목 번호	품목	EU Annex I (2021/821, 2025-09-08 반영)	차이점 및 비교
	9D005			가능성
기술	3E001	반도체 설계·제조 기술	WA 와 동일 번호	AI 가속기 기술 포함 가능성
기술	4E001	고성능 컴퓨팅 및 침입 SW 개발 기술	WA 와 동일 번호	AI 병렬처리·GPU 최적화 기술 반영
기술	5E001 / 5E002	감시·암호화 SW 관련 기술	WA 와 동일 번호	AI 심층 패킷 분석(DPI) 분석·보안 통신 암호화 기술 포함
기술	6E001~6E003	센서·레이더 기술	WA 와 동일 번호	AI 센서 융합 분석 기술 반영
기술	7E001~7E004	항법·유도 시스템 개발 기술	WA 와 동일 번호	AI 자율 항법·융합 항법 기술 적용 가능성
기술	8E001~8E003	해양 항법·자율운항 시스템 기술	WA 와 동일 번호	AI 자율운항 알고리즘 포함
기술	9E001~9E003	항공기 추진제어 기술	WA 와 동일 번호	AI 기반 추진제어·비행 제어 기술 반영

4.3. 일본 통제 품목

- 일본은 외국환 및 외국무역법(外為法)과 「수출무역관리령」에 따라 WA 품목 체계와 번호를 거의 동일하게 채택함[65][66]
- 다만 성능 지표, 시험 장비 예외, 민수/연구 용도 예외 등 운용 지침을 세분화함
- 미국처럼 3A090, 4D090 같은 독자 통제 코드 신설은 하지 않고, 고성능 컴퓨팅, 암호, 감시 센서 등 기존 WA 품목(4A003, 4D001, 5D002 등) 내에서 AI 관련 품목의 적용을 포괄함
- 성능 기준을 세분화 운용하여 APP/연결성/주파수, 분해능 같은 통제 사양 수치를 업데이트하여 반영함
- 연구 및 테스트용 예외를 명시하여 침입 테스트 장비/환경, 보안 평가 SW 등 한해 목적이나 범위를 밝힌 예외 사항을 운영함
- Mass Market 품목의 예외를 적용하고, 오픈소스 SW 예외를 가이드로 구체화함
- 영상, 정찰 분야를 별도로 지정하여 위성/드론 영상처리 SW를 데이터 처리 SW로 정하고 군사용, 민수용을 구분 심사함(민수용 감시/안전 목적 예외 주석 조항을 운영함)
- 기술이전 심사를 강화하여 특정 지역이나 기관으로의 기술이전은 별도 심사하고 허가하여 관리함

- AI SW 품목 관련 주요 통제 대상은 다음과 같이 구분할 수 있음

- 4D001(컴퓨터 SW)

  4A003 등 고성능 컴퓨터 운용/클러스터 관리 SW로 OS, 스케줄러 등을 포함하며, TensorFlow, PyTorch 등도 분산 학습 관리 기능 포함 시 4D001을 포괄 적용함

- 4D004(침입 SW)

  침입 SW의 생성, 제어 전용 SW로 보안 평가·테스트용 SW의 범위를 명확히 정의하고 오용 가능성이 있는 경우 통제함

- 5D001.c (통신 감시/패킷 분석 SW)

  DPI·네트워크 분석 SW. 위성·드론 영상처리 SW와 별도로 '데이터처리 SW'를 심사대상으로 지정(민수/군사 용도 수요 구분)

- 5D002(암호화 기능 SW)

  암호화 알고리즘이나 기능을 포함하는 SW로 VPN, TLS 암호 프로토콜 등이 해당되며, Mass Market 품목 예외, 공개 SW 예외를 운영함

- 6D001~6D003((센서·광학·레이더 SW)

  위성·드론 영상처리 SW를 포함하며 민수용 감시/안전 목적에 대한 예외를 적용하며, 군사, 정찰 전용 의심 시에는 심사를 통해 통제 대상으로 관리함

- 7D001~7D004 (항법·유도 SW)

  항공기 항법, 관성항법 제어, GPS 보정/융합 SW로 AI 자율비행·경로 제어 알고리즘 등의 포함이 가능함

- 8D001 / 8D002 (해양항법/자율운항 SW)

  잠수정 제어, 자율선박 항법·충돌 회피 SW로 AI 항로 계획·자율 운항 제어 포함이 가능함

- 9D001/ 9D002 / 9D004 / 9D005 (항공/로켓 추진·제어 SW)

비행 제어·추진 시뮬레이션 SW 등으로 AI 비행 최적화, 추력 제어 등을 포함하는 것이 가능함

- AI 관련 주요 전략 기술 통제 대상은 다음과 같이 구분할 수 있음

- 3E001(전자부품 기술)

3A001 반도체 설계, 공정 기술로 포토리소그래피, EUV 기술 이전 시 별도 허가(장비/기술 세트 심사)

- 4E001(컴퓨터 기술)

고성능 컴퓨터 및 고성능 AI 컴퓨터 설계 기술이 해당될 수 있으며, AI 모델 학습 등 고성능 컴퓨팅 설계 기술도 적용 대상이 될 수 있음

- 5E001 / 5E002 (감시·암호화 SW 관련 기술)

5A001, 5A002, 5D001, 5D002 관련 기술로, 심층 패킷 분석(DPI), 보안 통신, 암호화 알고리즘 기술 등을 포함하며, AI 심층 패킷 분석, 암호화 기술 등의 포함이 가능하며, 양자암호 등 신기술을 포함하도록 갱신함

- 6E001~6E003(센서 기술)

센서, 레이더, 이미징 설계 및 분석, 운용 기술 등이 해당되며 AI 기반 영상분석, 고사양 센서 융합 알고리즘도 포함될 가능성이 있음

- 7E001~7E004 (항법·유도 기술)

유도 제어·GPS/INS 융합 설계 기술로 AI 자율 항법·정밀 위치 산출 기술 등을 포함하는 것이 가능함

- 8E001~8E003 (해양·자율운항·추진 기술)

  잠수정·무인 잠수정 등의 설계, 자율운항 알고리즘, 해양 추진·제어 기술로 AI 자율 운항·충돌 회피·추진 제어 등을 포함하는 것이 가능함

- 9E001~9E003 (항공 추진제어 기술)

  항공기/로켓/우주비행체 등의 추진 및 비행 제어 기술로 AI 기반 추진 제어·비행 최적화 기술 등을 포함하는 것이 가능함

표 9 일본 통제 대상 품목

구분	항목 번호	품목	일본 수출무역관리령 (別表第 1, 2025 반영)	주요 차이점 및 비고
HW	3A001	고성능 IC, A/D·D/A, 고속 마이크로프로세서, FPGA 등	제 13 호 (1)항 (a)~(e)	WA 와 동일 기준, 성능·주파수·분해능 세분화
HW	4A003	성능·연결성 기준의 고성능 컴퓨터/조립체(고성능 컴퓨팅, 슈퍼컴퓨터)	제 14 호 (3)항	WA 와 APP 기준 동일, 통신 링크 수 항목별 명시, 클러스터 수출 시 보류·허가 필요 가이드
HW	4A005	침입 SW 용 시스템·장비·구성품	제 14 호 (4)항 (a)	보안 시험 장비(침입테스트 등) 예외 운영, 오남용 우려 시 심사 강화
HW	5A001.j	통신 감청·패킷 분석(모니터링) 장비(DPI 등)	제 15 호 (12)항 (c)	심층 패킷 분석(DPI) 장비 인권·감시 용도 심사 강화, 공개 SW/학술 목적 예외 제한적
HW	5A002	암호화 기능 포함 HW	제 15 호 (2)항	Mass-Market 예외 운영
HW	6A001~6A008	광학·레이저·항법 등 센서류 전체	제 16 호 (1)~(14)항	민수 감시/안전 목적 예외, ATC/군 정찰 목적은 심사 강화
HW	7A001~7A004	항법·유도·자이로/관성항법	제 17 호 (1)~(6)항	자이로·가속도계 정밀도 기준, 군수 적용, 무인 항법 연계 시 주의
HW	8A001 / 8A002	해양용 항법·탑재 장비	제 18 호 (1)항 / (2)항	군용/수중 정찰·음향 탐지 연계 시 강화
HW	9A001	항공기 가스터빈 엔진	제 19 호 (1)항	AI 최적화 제어 등과 연계 시 9D/9E 기술 검토
HW	9A002	선박 가스터빈 엔진	제 19 호 (2)항	AI 최적화 제어 등과 연계 시 9D/9E 기술 검토
HW	9A007	로켓 추진 시스템	제 19 호 (7)항	AI 최적화 제어 등과 연계 시 9D/9E 기술 검토
SW	4D001	고성능 컴퓨팅 운용·클러스터 관리 SW	제 14 호 (9)항	OS, 스케줄러, 클러스터 관리, 분산학습 프레임워크(TensorFlow/PyTorch 등) 등 적용 검토
SW	4D004	침입 SW 전용 SW	제 14 호 (10)항	침입 생성·제어 전용, 보안 평가·테스트 SW 범위 명시, 오용 우려 시 통제

AI 기반 품목의 전략물자 통제 기준 및 방향 분석 60

구분	항목 번호	품목	일본 수출무역관리령 (別表第 1, 2025 반영)	주요 차이점 및 비고
SW	5D001.c	통신 감시·패킷 분석 SW	제 15 호 (12)항 (c)	심층 패킷 분석(DPI), 네트워크 분석/시각화 SW, 감시·도청 목적 의심 시 심사 강화
SW	5D002	암호화 기능 포함 SW	제 15 호 (5)항	Mass-Market, 공개 SW 예외 규정 운영
SW	6D001~6D003	센서·레이더·IR/SAR 처리 SW	제 16 호 (9)~(11)항	위성·드론 영상 처리 포함, 민수 안전 목적 예외, 군정찰 용도 의심 시 통제
SW	7D001~7D004	항법·유도 시스템 제어 SW	제 17 호 (7)~(10)항	관성 항법 제어, 자율비행 경로 제어 포함 가능
SW	8D001 / 8D002	해양항법 및 제어 SW	제 18 호 (3)항 / (4)항	잠수정 제어, 장애물 회피, 자율 항법 포함 가능
SW	9D001 / 9D002 / 9D004 / 9D005	항공기 비행 제어/추진 연계 SW	제 19 호 (3)항 / (4)항 / (6)항 / (8)항	비행 제어, 추진 제어 알고리즘 포함 가능
기술	3E001	3A001 반도체 설계·제조 기술	제 13 호 (2)항	포토리소그래피, EUV 공정 이전 시 장비, 기술 세트 별도 허가 필요
기술	4E001	4A003 개발·생산·사용 기술(고성능 컴퓨팅/AI)	제 14 호 (11)항	고성능 컴퓨팅 설계·스케줄링 최적화 포함 가능
기술	5E002	5D002 관련 암호 기술	제 15 호 (5)항	종단간(E2E) 키관리·암호모듈, 양자암호 등 신기술 반영
기술	6E001~6E003	센서·레이더·이미징 설계/운용 기술	제 16 호 (12)~(14)항	AI 기반 영상 분석·센서 융합 알고리즘 포함 가능
기술	7E001~7E004	항법·유도 시스템 개발 기술	제 17 호 (11)~(14)항	유도제어·INS 정밀 보정 설계
기술	8E001~8E003	수중/해양 항법 시스템 설계 기술	제 18 호 (5)~(7)항	잠수정 항법·음향 항법 설계
기술	9E001~9E003	항공기·로켓 추진/비행제어 기술	제 19 호 (9)~(11)항	AI 기반 비행 제어·추진 최적화 포함 가능

4.4. 국내 통제 품목

- 한국은 「전략물자 수출입고시」(산업통상자원부 고시)를 통해 바세나르 체제(WA) 품목을 기반으로 관리하고 있음[67][68][69]
- WA 품목 통제 번호(3A001, 4A003 등)를 거의 동일하게 채택하되, 세부 규정과 판정 기준은 국내 환경에 맞게 일부 단서 조항을 추가함
- 미국과 달리 3A090, 4D090 등 AI 관련 독자 통제 품목은 운용하지 않으며, 기존 WA 품목 내에서 AI 관련 품목을 포괄적으로 관리함
- 품목 판정 시 통제 사양 성능지표(FLOPS, APP, 처리속도, 암호화 강도 등)를 고려하며, 연구용·민수용 목적은 예외 또는 캐치올 심사 제외 대상으로 구분함
- AI 관련 기술은 고성능 컴퓨팅, 암호화, 감시·정찰, 자율주행, 네트워크 감시, 데이터 분석 분야 등 WA 통제 대상 품목 기준과 유사하게 관리하고 있음

- 4D001(고성능 컴퓨터 SW)

  4A003 등 고성능 컴퓨터의 운용·클러스터 관리용 SW로, 고성능 컴퓨팅 OS, 스케줄러, 클러스터 관리 프레임워크가 해당되며, 대규모 분산 학습 기능이 포함된 SW는 4D001 범위에 포함될 수 있음

- 4D004(침입 SW)

  침입 탐지·제어 전용 SW로, 모의해킹·침입테스트·보안검증용 프로그램이 해당되며 목적이 보안 평가임을 명시한 경우 예외 가능하지만, 공격 자동화나 침투 모듈 생성 기능이 있는 경우 통제 가능성이 있음

- 5D001.c (통신 감시/패킷 분석 SW)

  심층 패팃 분석(DPI), 네트워크 트래픽 분석·시각화용 SW가 포함되며 군·정보

기관의 감시·도청 목적으로 활용될 경우 통제 대상이며, 민수 네트워크 품질 관리용은 예외로 판단함

- 5D002(암호화 기능 SW)

대칭·비대칭 암호화 기능을 포함한 보안 SW로 VPN, TLS, 암호화 API 등이 해당되며 공개 SW와 Mass Market 품목은 예외 조항에 따라 통제에서 제외되나, 군사보안 용도 등으로 설계된 경우 통제 가능성이 있음

- 6D001~6D003(센서·광학·레이더 SW)

IR, SAR 등 영상·센서 데이터 처리 SW로, 위성·드론 영상 분석용 AI SW가 포함되며 민수 안전 감시 목적은 예외로 인정되지만, 군사 정찰·표적 추적용 등은 통제 가능성이 있음

- 7D001~7D004 (항법·유도 SW)

항공기·무인기 INS 제어, GPS 보정·융합 SW가 해당되며 자율비행 제어, 경로 계획, 항법 보정 알고리즘 등 AI 기술이 포함된 경우 통제 가능성이 있음

- 8D001 / 8D002 (해양항법/자율운항 SW)

잠수정·수상 선박용 제어 SW로, 자율 항법·충돌회피 기능이 있는 SW가 포함되며 AI 기반 해양 경로 최적화·자율운항 시스템 SW는 군사용 전용 가능성이 있는 경우 통제 가능성이 있음

- 9D001 / 9D002 / 9D004 / 9D005 (항공/로켓 추진·제어 SW)

항공기·로켓 추진 및 제어 시스템 SW로, 비행 제어·추력 시뮬레이션 SW가 해당되며 AI 기반 비행 최적화, 추진제어 알고리즘 등 포함 시 통제 가능성이 있음

표 10 한국 통제 대상 품목

구분	항목 번호	WA	한국 전략물자 수출입고시 별표 2	차이점 및 비교
HW	3A001	고성능 IC, A/D·D/A 변환기, 마이크로프로세서, FPGA 등	WA 와 동일 번호	성능·주파수·분해능 등 세부 지표 세분화 운용, AI 용 GPU 도 동일 기준 적용
HW	4A003	고성능 컴퓨터 및 고성능 컴퓨팅 조립체	WA 와 동일 번호	APP 기준 동일, 클러스터 단위(통신 링크 수·노드 수) 심사
HW	4A005	침입 SW 용 시스템·장비·구성품	WA 와 동일 번호	보안 평가용 예외 인정, 공격 자동화 SW 포함 시 통제 가능성
HW	5A001.j	통신 감시·패킷 분석 장비(DPI 등)	WA 와 동일 번호	심층 패킷 분석(DPI), 감시 장비 등 통제 가능성
HW	5A002	암호화 기능 포함 HW	WA 와 동일 번호	Mass-Market 예외 유지
HW	6A001~6A008	광학·레이더·항법 등 센서류 전체	WA 와 동일 번호	민수 감시·안전 목적 예외 유지, 군 정찰·표적 탐지용 통제 가능성
HW	7A001~7A004	항법·유도·INS 시스템	WA 와 동일 번호	자율 주행·유도 시스템 포함 가능성
HW	8A001 / 8A002	해양·무인 수송·항법 플랫폼	WA 와 동일 번호	AI 자율 운항체 통제 검토, 민수·군수 용도 심사
HW	9A001	항공기 가스터빈 엔진	WA 와 동일 번호	AI 최적화 제어 등과 연계 시 9D/9E 기술 검토
HW	9A002	선박 가스터빈 엔진	WA 와 동일 번호	AI 최적화 제어 등과 연계 시 9D/9E 기술 검토
HW	9A007	로켓 추진 시스템	WA 와 동일 번호	AI 최적화 제어 등과 연계 시 9D/9E 기술 검토
SW	4D001	고성능 컴퓨팅 운용·클러스터 관리 SW	WA 와 동일 번호	고성능 컴퓨팅·AI 학습 프레임워크 포함 가능성
SW	4D004	침입 SW 전용 SW	WA 와 동일 번호	AI 자동화 침투·공격 SW 포함 가능성

AI 기반 품목의 전략물자 통제 기준 및 방향 분석 64

구분	항목 번호	WA	한국 전략물자 수출입고시 별표 2	차이점 및 비교
SW	5D001.c	통신 감시·패킷 분석 SW	WA 와 동일 번호	심층 패킷 분석(DPI), 트래픽 분석 SW, 감시·정보수집 목적 시 통제 가능성
SW	5D002	암호화 기능 포함 SW	WA 와 동일 번호	Mass-Market 예외 유지
SW	6D001~6D003	센서·광학·레이더 관련 SW	WA 와 동일 번호	민수 감시 목적 예외 유지, 군 정찰·AI 표적 추적 SW 통제 가능성
SW	7D001~7D004	항법·유도 제어 SW	WA 와 동일 번호	AI 자율 항법·비행 제어 SW 포함 가능, 정밀도 기준 강화
SW	8D001 / 8D002	해양항법 및 자율운항 제어 SW	WA 와 동일 번호	자율 항로 계획·충돌 회피 SW 포함 가능
SW	9D001 / 9D002 / 9D004 / 9D005	항공·로켓 추진 및 제어 SW	WA 와 동일 번호	AI 비행 제어·추진 최적화 SW 포함 가능
기술	3E001	반도체 설계·제조 기술	WA 와 동일 번호	AI 전용 반도체 설계 기술 반영 가능
기술	4E001	고성능 컴퓨팅 및 침입 SW 개발·생산 기술	WA 와 동일 번호	AI 병렬 처리·GPU 최적화 기술 반영, 대규모 학습 클러스터 설계 포함
기술	5E001 / 5E002	감시·암호화 SW 관련 기술	WA 와 동일 번호	AI 심층 패킷 분석·암호화 기술 포함
기술	6E001~6E003	센서·레이더·이미징 기술	WA 와 동일 번호	AI 센서 융합·표적 탐지 기술 반영, 영상분석 알고리즘 포함 가능
기술	7E001~7E004	항법·유도 시스템 개발 기술	WA 와 동일 번호	AI 자율 항법·융합 항법 기술 적용 가능
기술	8E001~8E003	해양항법·자율운항 시스템 기술	WA 와 동일 번호	AI 자율운항 알고리즘 포함, 충돌 회피·항로 계획 기술 포함 가능
기술	9E001~9E003	항공기 추진제어 기술	WA 와 동일 번호	AI 기반 추진 제어·비행 제어 기술 포함 가능

V AI SW 품목의 수출 통제 가능성 분석

제5장 AI SW 품목의 수출통제 가능성 분석

- 본 장에서는 다양한 AI SW 품목의 특성/기능별 구분 품목들의 WA, 미국, 유럽, 일본 등 수출통제 대상 가능성에 대해 분석하고자 함

5.1. 주요 AI SW 품목의 수출통제 가능성

- WA 수출통제 대상 검토 가능성이 있는 AI 기술 관련 주요 품목을 다음과 같이 구분해볼 수 있음

(1) 암호화

(2) AI 연산 인프라

(3) AI 모델 학습

(4) AI 응용

(4-1) 음성 인식·합성

(4-2) 영상 분석·생성

(4-3) 자연어 처리

(4-4) 추천·데이터 마이닝

(5) AI 자율 주행/로보틱스

(6) AI 네트워크 감시/분석/보안

(6-1) 네트워크 감시·분석

(6-2) 보안/침투

(7) 군사 감시/정찰 AI

(8) 바이오/의료 AI

5.1.1. 암호화 (CAT 5 Part 2)

- 데이터 보호, 접근 제어, 통신 보안 등을 위한 암호화 알고리즘, 암호화 기능을 포함하는 HW, SW에 해당함
- VPN, TLS 등 암호화 프로토콜, AES, PKI 등 대칭/비대칭 암호화 알고리즘 등과 관련되며 정보 보안 통제 대상 품목(5A002, 5D002)과 직접 연관됨

표 11 암호화 품목 예

구분	통제번호	품목 예시	설명
HW	5A002.a.1 / a.2	HW 보안 모듈(HSM, Hardware Security Module)	대규모 데이터센터의 키 관리 및 암호화 연산 가속
HW	5A002.a.3	암호화 지원 CPU/SoC	반도체 칩 레벨 데이터 암호화 지원
SW	5D002.c.1	종단간(End-to-End) 암호화 SW	군/정부/기업용 보안 통신 프로토콜
SW	5D002.c.1	API 호출 암호화 SaaS 플랫폼	AI 모델의 응답 처리 및 API 호출 구간 종단간 암호화

5.1.2. AI 연산 인프라 (CAT 4)

- AI 학습·추론을 위한 고성능 컴퓨팅 자원(고성능 컴퓨터, GPU 서버 등) 및 이를 제어하는 클러스터 관리 SW에 해당함
- 고성능 컴퓨터·모듈(4A003), 고성능 AI 컴퓨터 모듈(DGX 서버, AI 슈퍼컴퓨터, 데이터센터용 클러스터 포함)(4A090) 및 운용·관리 SW(4D001)와 직접적으로 연결되며, AI 학습용 HW/SW 인프라 통제의 핵심 영역임

표 12 AI 고성능 연산 인프라 품목 예

구분	통제번호	품목 예시	설명
HW	4A003 / 4A090	슈퍼컴퓨터, AI 용 컴퓨팅 노드	고성능 컴퓨팅 및 AI 모델 학습용 HW
HW	4A003 / 4A090	GPU 클러스터	AI/과학 계산용 고속 병렬 연산
SW	4D001	슈퍼컴퓨터 프로그래밍 플랫폼	분산 고성능 컴퓨팅 프레임워크
SW	4D090	GPU 클러스터 제어·최적화 SW	초거대 AI 모델 학습/추론용 GPU 클러스터 제어·최적화

5.1.3. AI 모델 학습 (CAT 4)

- 대규모 데이터 학습, 분산 처리, 모델 최적화 등을 수행하는 SW 및 알고리즘에 해당함
- 대규모 모델(LLM·LVM·멀티모달 등) 학습용 고성능 연산 시스템의 FLOPS, 메모리 대역폭, 연결성 기준이 WA 기준(4A003) 또는 미국 EAR 신설(4A090)을 초과할 경우 통제 가능성이 있음
- 분산 학습, 병렬 학습, 모델 최적화 SW는 AI 학습·추론용 SW나 클러스터 관리 기능 등이 포함 시 4D001 해당 가능성이 있음

표 13 AI 모델 학습 품목 예

구분	통제번호	품목 예시	설명
HW	4A090	AI 학습용 GPU 서버	10^8~10^{11}개 이상의 파라미터를 갖는 대규모 언어모델(LLM)·멀티모달 모델 학습용 고성능 GPU 서버
HW	4A090	TPU/NPU 클러스터	대규모 AI 모델 학습 전용 HW
SW	4D090 / 4D001	딥러닝/고속 컴퓨팅 프레임워크	대규모 분산 학습·모델 병렬처리용 SW
SW	4D090 / 4D001	모델 학습 최적화 라이브러리	대규모 AI 모델 학습의 파이프라인 병렬화·메모리 최적화·통신 효율화 SW

5.1.4. AI 응용

- AI 모델을 활용하여 특정 목적의 기능(예: 인식, 분류, 분석, 생성 등)을 수행하는 응용 SW 및 시스템에 해당함
- 민수용, 군사용 목적에 따라 통제 여부가 달라지며, 감시·정찰(6A003~6D003)이나 보안(5D002) 관련 기능이 있을 경우 통제 가능성이 있음

5.1.4.1. 음성 인식·합성 (CAT 4)

- 음성 데이터를 분석하여 음성을 인식하거나 텍스트 정보를 이용하여 음성을 합성하는 기능을 수행하는 AI 기술에 해당함
- 대규모 음성 데이터 기반 음성 인식·합성 모델(ASR, TTS) 학습에 사용되는 고성능 GPU 서버의 성능(FLOPS·연결성능) 기준 초과 시 4A003 또는 4A090 해당 가능성이 있음
- 실시간 다중 음성 인식 고성능 AI 학습·추론 SW(4D090) 해당 가능성이 있음

표 14 음성 인식·합성 품목 예

구분	통제번호	품목 예시	설명
HW	4A090	엣지용 TPU, AI 전용 ASIC	경량화 엣지 디바이스용 음성 AI 연산 모듈
HW	4A090	AI GPU/NPU 엔진	모바일·임베디드용 음성 AI 가속 프로세서
SW	4D090 / 4D001	음성 인식 모델 SW	대형 음성 인식 모델
SW	4D090 / 4D001	음성 합성 SW	텍스트 기반 고성능 음성 변환/합성 AI SW

5.1.4.2. 영상 분석·생성 (CAT 4, 6, 7)

- 영상·이미지를 인식, 분석, 생성하는 기술로, 객체 탐지·추적·합성 기능 등을 포함함
- 영상 생성형 모델 학습에 사용되는 고성능 GPU 서버의 성능(FLOPS·연결성능) 기준 초과 시 4A003, AI 전용 가속기는 4A090 해당 가능성이 있음
- 영상 수집·탐지용 센서 장비. 군사 감시, 위성·드론 영상 수집 용도 시

6A003~6A008, 영상 감시·정찰용 영상 처리 SW, 감시·표적 탐지 등 목적일 경우 6D003 적용 가능성이 있음

- 고성능 AI 학습·추론용 SW(4D090) 또는 고성능 컴퓨팅용 SW(4D001)에 해당 가성이 있음

표 15 영상 분석 및 생성 품목 예

구분	통제번호	품목 예시	설명
HW	4A090 / 6A003 / 6A008	위성·항공 영상 분석용 GPU 서버	EO/IR(Electro-Optical/Infrared) 영상 기반 AI 모델 실행용 고성능 GPU 서버
HW	6A002 / 6A008 / 7A003	고해상도 EO/IR 센서/레이더	군용·경찰용 드론 및 항공기 장착 영상 수집·표적 탐지 활용 고정밀 센서/레이더
SW	4D090 / 6D003	AI 영상 분석 SW	얼굴·객체 탐지, 행동 인식 등 대규모 영상 데이터 분석용 SW
SW	4D090 / 6D003	AI 얼굴 인식·식별 SW	국가 보안·경찰·국경관리 목적 얼굴 인식 시스템

5.1.4.3. 자연어 처리 (CAT 4)

- 텍스트 분석, 번역, 요약, 질의응답 등을 수행하는 언어 기반 AI 응용 기술에 해당함

- LLM 학습·추론에 활용되는 고성능 연산 장비로 FLOPS·연결성능(4A003) 또는 AI 가속기 성능(4A090) 초과 시 해당 가능성이 있음

- LLM 학습·튜닝·추론용 SW로, 대규모 병렬 학습 및 모델 최적화 기능 포함 시 4D090(AI 학습용 SW)로 분류 가능하며, 일반 운용 SW는 4D001 검토가 필요함

표 16 자연어 처리 품목 예

구분	통제번호	품목 예시	설명
HW	4A090 / 4A003	학습용 고성능 GPU 서버	대규모 언어모델(LLM) 학습용 GPU 서버 및 슈퍼컴퓨터
HW	4A090 / 4A003	AI 전용 클러스터	대형 AI 모델용 GPU/TPU 클러스터
SW	4D090 / 4D001	멀티모달 AI 학습·추론 라이브러리	사전학습 AI 언어모델 및 멀티모달 AI 학습용 프레임워크
SW	4D090 /	대규모 언어모델(LLM)	초대규모 생성형 언어모델 및 LLM 기반 API

구분	통제번호	품목 예시	설명
	4D001	및 API 서비스	

5.1.4.4. 추천·데이터 마이닝 (CAT 4)

- 사용자 행태·패턴 분석을 기반으로 추천, 이상 탐지, 예측을 수행하는 AI 기술에 해당함

- 대규모 데이터 마이닝 및 추천 모델 학습에 활용되는 고성능 컴퓨팅 장비. FLOPS·연결성능 기준(4A003) 또는 AI 가속기 기준(4A090)을 초과할 경우 해당 가능성이 있음

- 대규모 추천·분류·군집화·행동 패턴 분석용 SW, 분산 학습, 파이프라인 최적화 등 고성능 컴퓨팅 자원 제어 기능 포함 시 4D090 또는 4D001 해당 가능성이 있음

- 대규모 데이터 감시나 사용자 추적 용도로 사용되고 6A003 영상 장비를 통한 데이터의 정보 수집·감시용 데이터 마이닝 시스템과 통합되어 운용될 경우 해당 가능성이 있음

표 17 추천·데이터 마이닝 품목 예

구분	통제번호	품목 예시	설명
HW	4A003 / 4A090	AI 학습용 슈퍼클러스터	대규모 추천·데이터 마이닝 모델 학습용 고성능 연산 클러스터
HW	4A090 / 4A003	추천 시스템용 그래프 연산용 서버	추천 시스템, 지식 그래프 연산 특화 AI 가속기
SW	4D090 / 4D001	AI 추천 시스템 SW	추천 알고리즘·라이브러리 포함 학습·추론 SW
SW	4D090 / 4D001	머신러닝·데이터 마이닝 플랫폼	분산 학습·데이터 분석용 머신러닝 프레임워크

5.1.5. AI 자율 주행/로보틱스 (CAT 6, 7, 8, 9, 일부 4)

- 센서 융합, 주행 경로 인식, 의사결정 알고리즘 등을 통한 로봇 등 자율 이동체의 제어 기술에 해당함

- 자율주행 차량·로봇의 주요 구성품인 IR 카메라, 레이더 센서 등을 포함하고 고해상도 또는 군용 사양의 감지 센서를 적용한 경우(6A003), 통제 가능성이

있음

- 자율주행용 센서 데이터 처리·융합 SW가 6A003 장비(영상·레이더)와 연계될 경우 통제 가능성이 있음
- AI 자율 드론·UAV 시스템은 9A004 직접 통제 대상이 될 수 있으며 관련 AI 제어 알고리즘, 경로 계획 SW 등도 통제 가능성이 있음
- 민수용 자율주행 로봇이나 SW도 감시·정찰 등 군사용 전용 가능성이 있을 경우 상황허가 대상 가능성이 있음

표 18 AI 자율주행, 로보틱스 품목 예

구분	통제번호	품목 예시	설명
HW	4A090 / 7A003 / 7A004	자율주행용 AI 컴퓨팅 모듈	자율주행용 고성능 AI 연산 모듈
HW	6A003 / 8A002 / 8A007	AI 로봇 플랫폼 (센서 융합형)	레이더·IR 센서·광학 시스템 센서 등 포함 자율 로봇·드론·무인 선박 플랫폼
SW	7D003 / 8D002 / 4D090	로봇 제어 시스템 SW	로봇 제어용 미들웨어, 제어 커널, 항법 및 경로 계획 SW
SW	4D090 / 9D004 / 9D005	자율주행 SW	객체 인식·센서 융합, 경로 계획, 추론, 강화학습 기능 포함 자율주행용 AI SW
기술	4E001 / 7E004 / 9E003	자율주행·로봇 제어 기술	AI 제어 아키텍처, 자율 경로 탐색 알고리즘, 센서 융합·딥러닝 기반 제어 로직 등 설계·개발·운용 기술

5.1.6. AI 네트워크 감시/분석/보안

- 패킷 분석, 트래픽 모니터링 등을 수행하는 AI 기반 네트워크 분석 기술과 시스템, 네트워크 침입, 취약점 탐지·공격 자동화 등 침입, 탐지 AI 기술에 해당함

5.1.6.1. 네트워크 감시·분석 (CAT 5 Part 1)

- 패킷 분석, 트래픽 모니터링, 네트워크 이상 탐지 등을 수행하는 AI 기반 네트워크 분석 기술에 해당함
- 대규모 네트워크 모니터링, 메타 데이터 수집, 암호화된 트래픽 감시, 패킷 복

호화 기능 SW는 5D001(감시 SW), 5A004(감시 장비)에 해당 가능성이 있음

- AI 기반 IDS/IPS, 공격 탐지·분석·차단 SW는 4A005/4D004 통제 가능성이 있음(WA와 EU는 연구용·보안 테스트용 예외 조항이 있지만, 상용화나 감시·침투 기능 포함 시 통제 가능성 있음
- VPN, TLS, SSL 통신 암호화 처리 SW 또는 이를 분석하는 AI 네트워크 보안 SW는 5D002 통제 가능성이 있음

표 19 네트워크 감시·분석 품목 예

구분	통제번호	품목 예시	설명
HW	5A001.j	Deep Packet Inspection (DPI) 장비	패킷 레벨 트래픽 분석 네트워크 모니터링 장비
HW	5A001.j	통신 감청 장비	전화·메시지·데이터 트래픽 감시 및 메타데이터 수집 장비(통신 감청·위치 추적 등)
SW	5D001.c	네트워크 분석 SW	대규모 네트워크 트래픽 데이터 분석 SW
SW	5D001.c	네트워크 트래픽 감시 SW	네트워크 트래픽 감시 및 메타데이터 수집 SW

5.1.6.2. 보안/침투 (CAT 4)

- 시스템, 네트워크 침입, 취약점 탐지·공격 자동화 등 침입, 탐지 AI 기술에 해당함
- AI가 공격 벡터를 자동 탐색·생성하는 SW, 또는 침입 실행을 자동화하는 시스템은 4D004 통제 가능성이 있음
- AI 침투 시스템이 암호화 해제·우회 기능을 포함하거나 VPN, TLS 복호화 기능을 내장할 경우 정보보안(암호화) 품목으로 통제 가능성이 있음

표 20 보안/침투 품목 예

구분	통제번호	품목 예시	설명
HW	4A005	침입 SW 생성 장비	AI 기반 침입 SW 생성용 장비
HW	4A005	침입 SW 제어	AI 기반 침입 SW 제어용 장비

구분	통제번호	품목 예시	설명
		장비	
SW	4D004	침입 SW 생성 SW	AI 기반 침입 SW 생성용 SW
SW	4D004	침입 SW 제어 SW	AI 기반 침입 SW 제어용 SW

5.1.7. 군사 감시/정찰 AI (CAT 4, 6, 7 관련)

- 위성, 드론, SAR, IR 영상 등 군사 감시·표적 탐지용 AI 시스템에 해당함
- 열영상 해상도, 프레임, 스펙트럼 대역 등 통제 성능 기준 충족하거나 AI 표적 탐지·추적·식별 기능 포함 시 해당 가능성이 있음
- 6A 계열 센서, 광학 장비의 작동/시험/사용을 위한 SW나 AI로 표적 탐지·분류·변화탐지 수행 시 군 감시·정찰 용도로 사용 가능하므로 6D003 해당 가능성이 있음

표 21 군사 감시/정찰 AI 품목 예

구분	통제번호	품목 예시	설명
HW	6A008 / 6A003 / 4A090	SAR 위성 탑재체	SAR(Synthetic Aperture Radar) 기반 고해상 영상 레이더
HW	6A002 / 7A003 / 6A003	군용 UAV 탑재 EO/IR 장비	고해상도 광학·열 영상 획득 장비(장거리 감시·정찰용)
SW	6D003 / 7D003	지리정보 분석 SW	위성·항공·지상 감시 데이터 융합·분석 SW
SW	6D003 / 7D003	위성·드론 영상 분석 SW	AI 기반 위성·드론 영상 분석, 객체 인식, 이동경로 추적 SW

5.1.8. 바이오/의료 AI (CAT 4, 6)

- 의료 영상 분석, 유전자 데이터 처리, 신약 개발 등 생명과학 분야 AI 기술에 해당함
- AI 기반 영상 향상·자동 진단 기능이 군사 감시나 생체 인식 응용으로 전용될 가능성이 있으면 추가 검토가 필요함
- AI 영상 분석 SW가 6A003/6A006 장비의 작동·분석용이면 6D003 해당 가능성이 있음

- 대규모 AI 학습용 SW(딥러닝·모델 학습용)는 4D090(AI 학습용 SW) 적용 가능성 검토가 필요함

표 22 바이오/의료 AI 품목 예

구분	통제번호	품목 예시	설명
HW	4A003 / 4A090	DNA·유전체 분석 장비	AI 기반 유전체·단백질 구조 분석용 고성능 연산장치
HW	4A090 / 6A003	의료 영상 분석용 플랫폼	고해상도 의료 영상(MRI, CT, X-ray 등) 분석 GPU 클러스터·서버
SW	4D090 / 4D001	단백질 구조 예측 플랫폼	AI 기반 단백질 구조·기능 예측, 신약 후보 물질 설계용 SW
SW	4D090 / 6D003	의료 영상 분석 SW	AI 활용 의료 영상 진단·분류·탐지 SW

VI 해외/국내 AI SW 수출통제 품목 사례 분석

제6장 국내외 AI SW 수출통제 품목 사례 및 설문조사 분석

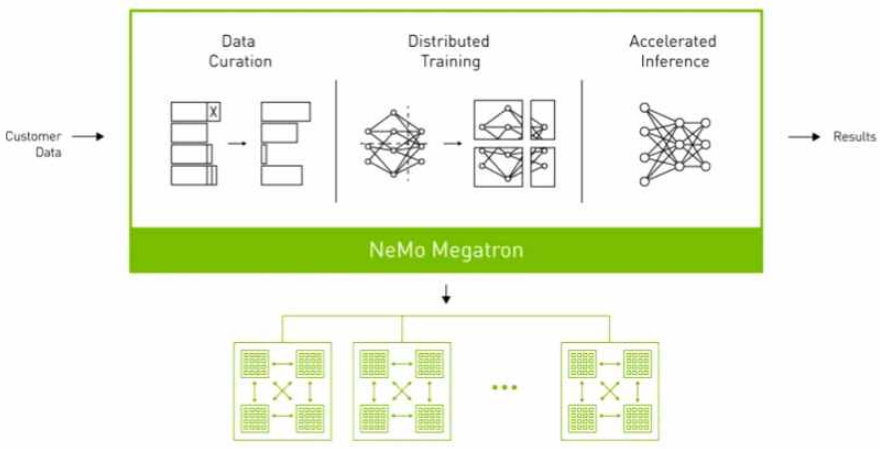
- 본 장에서는 미국, 유럽, 일본 등 해외와 국내의 수출통제 가능성이 있는 주요 AI SW 품목들의 사례를 해당 품목의 품목명, AI 기술 분류, 통제 번호(WA, 미국, 유럽, 일본), 품목 해설, 관련 기업 등으로 구분해 통제 가능성 있는 품목을 분석하고자 함

6.1. 해외 AI SW 통제 품목 사례 분석

6.1.1. 미국 AI SW 통제 품목 사례

<table>
<tr><th colspan="11">품목</th></tr>
<tr><td colspan="11">LLM 학습 배포 프레임워크</td></tr>
<tr><td>암호화</td><td>AI 인프라</td><td>모델 학습</td><td>음성</td><td>영상</td><td>언어 처리</td><td>데이터</td><td>지율 주행/로봇</td><td>네트워크 감시</td><td>보안</td><td>군사</td><td>바이오 의료</td></tr>
<tr><td colspan="11">▸초대규모 언어 모델(LLM)을 효율적으로 학습·배포하기 위한 프레임워크
▸모델 병렬화(tensor/pipeline parallelism) 기술을 통해 수백억~수천억 매개변수 모델 확장 가능</td></tr>
<tr><th colspan="11">통제 번호</th></tr>
<tr><td>WA</td><td colspan="2">미국</td><td colspan="2">유럽</td><td colspan="2">일본</td><td colspan="3">한국</td></tr>
<tr><td>-</td><td colspan="2">4D090</td><td colspan="2">캐치올 가능</td><td colspan="2">-</td><td colspan="3">상황허가 가능</td></tr>
<tr><th colspan="11">품목 해설</th></tr>
<tr><td colspan="11">▸NVIDIA GPU, NVLink, InfiniBand 등 고성능 하드웨어와 통합되어, 대규모 데이터 병렬 학습과 혼합 정밀도(FP16/BF16) 최적화

▸단순한 ML 라이브러리가 아닌 고성능 컴퓨팅급 분산 학습 제어 기능을 갖춘 경우 고성능 병렬처리 SW 범주 포함 가능

▸NVIDIA A100/H100 등 3A090, 4A090 기준을 초과하는 GPU 환경에서 동작 시 4D090 적용 가능
 
</td></tr>
<tr><th colspan="11">관련 기업</th></tr>
<tr><td colspan="11">미국: NVIDIA</td></tr>
</table>

품목

LLM API

암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율 주행/ 로봇	네트워크 감시	보안	군사	바이오 의료

- 대규모 언어 모델(LLM)을 API 형태로 기업 환경에 제공하여 안전하고 통제된 AI 활용 가능 클라우드 기반 서비스
- Enterprise-grade 보안, 데이터 격리, 관리 콘솔 기능을 통해 조직 단위의 대화형 AI 시스템 구축 가능

통제 번호

WA	미국	유럽	일본	한국
5D002	5D002 / 4D090	5D002	5D002	5D002

품목 해설

- OpenAI API 인프라(Azure, Microsoft Cloud 등) 기반, 독립된 데이터 격리 및 암호화 통신 제공
- 대규모 언어 모델(LLM) 추론용 SW로서, 질의응답·요약·분석 등 자연어 처리 기능을 API 형태로 제공
- 분산 환경에서 LLM 서비스 최적화 및 모델 파인튜닝(Enterprise Fine-tuning) 기능 제공
- 미국 EAR 기준상 5D002(암호화) 또는 4D090(고성능 AI SW) 적용 가능

관련 기업

미국: OpenAI

품목											
AI 얼굴인식 SW											
암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율주행/로봇	네트워크 감시	보안	군사	바이오 의료

▸ 인터넷·SNS 등 공개 이미지 데이터를 기반으로 얼굴 특징을 추출·매칭하는 AI 얼굴인식 시스템

▸ 수십억 장의 이미지 데이터베이스를 활용해 신원 식별 및 추적이 가능한 딥러닝 기반 생체인식 소프트웨어

통제 번호

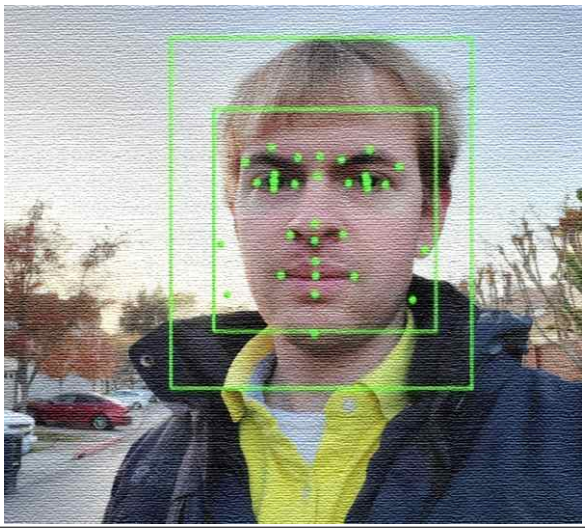
WA	미국	유럽	일본	한국
-	4D090	캐치올 가능	-	상황허가 가능

품목 해설

▸ 딥러닝 기반 얼굴 인식 모델 사용 얼굴 특징 벡터 추출, 대규모 이미지 데이터베이스와 매칭 신원 식별 및 검증 수행

▸ 고성능 컴퓨팅·GPU 기반 영상 처리 SW 해당, 병렬 이미지 분석 및 생체정보 추론 기능이 포함 시 고성능 병렬처리 SW 적용 가능

▸ AI 기반 신원 식별, 군·경찰 감시 및 보안 분야 적용 가능성 높아 4D090 (AI 응용 SW) 및 Catch-all 검토 대상 해당



관련 기업

미국: Clearview AI

품목

TPU 학습 프레임워크

암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율주행/로봇	네트워크 감시	보안	군사	바이오 의료

- Google이 개발한 TPU(Tensor Processing Unit) 하드웨어에서 최적화된 대규모 딥러닝 학습 프레임워크
- TensorFlow, JAX, XLA 등과 연동되어 모델 병렬화·자동미분·컴파일러 기반 최적화 수행

통제 번호

WA	미국	유럽	일본	한국
-	4D090	캐치올 가능	-	상황허가 가능

품목 해설

- TPU 하드웨어(3A090/4A090)와 연동되는 학습용 SW로, 대규모 행렬 연산 및 병렬처리 수행
- XLA(Accelerated Linear Algebra) 컴파일러를 통해 모델 그래프를 TPU 코어에 직접 매핑, 연산 효율과 메모리 사용 최적화
- 데이터 병렬·모델 병렬 학습 지원, 대규모 LLM·Vision 모델 학습 시 GPU 대비 효율적 전력/성능비 달성
- 병렬처리 및 AI 모델 학습 기능을 포함, 고성능 병렬처리 SW, 고성능 AI 학습 목적 시 4D090 적용 가능

관련 기업

미국: Google

품목											
클라우드 기반 AI 통합 플랫폼											
암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율 주행/로봇	네트워크 감시	보안	군사	바이오 의료

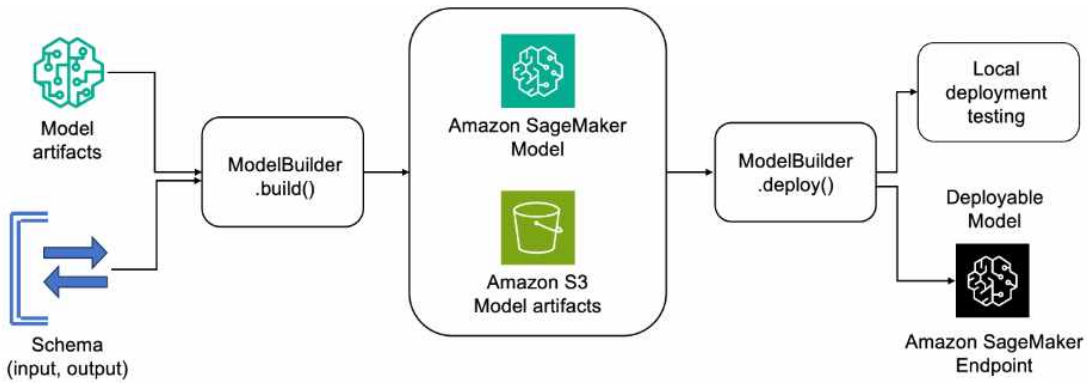
- Amazon Web Services(AWS)가 제공하는 클라우드 기반 통합 머신러닝(ML) 플랫폼
- 데이터 준비, 모델 학습, 배포, 모니터링을 엔드투엔드(End-to-End) 로 자동화하여 대규모 AI 서비스 개발에 활용 가능

통제 번호

WA	미국	유럽	일본	한국
-	4D090	캐치올 가능	-	상황허가 가능

품목 해설

- 클라우드 환경에서 AI 모델 학습·배포하는 통합 SW 프레임워크(Jupyter 기반 IDE, 데이터 파이프라인, AutoML, 모델 서빙 기능 포함)
- GPU·TPU·EC2 클러스터 등 고성능 컴퓨팅 인프라 위에서 동작, 분산 학습 기능 제공
- AI 모델 학습용 병렬처리 SW로 고성능 병렬처리 SW 기준에 포함 가능
- LLM, Computer Vision 등 고성능 AI 모델 학습·추론 수행 시 4D090(고성능 AI 응용 SW) 적용 가능



관련 기업

미국: Amazon

6.1.2. 유럽 AI SW 통제 품목 사례

<table>
<tr><th colspan="11">품목</th></tr>
<tr><td colspan="11">생명정보 분석 플랫폼</td></tr>
<tr><td>암호화</td><td>AI 인프라</td><td>모델 학습</td><td>음성</td><td>영상</td><td>언어 처리</td><td>데이터</td><td>지율 주행/ 로봇</td><td>네트워크 감시</td><td>보안</td><td>군사</td><td>바이오 의료</td></tr>
<tr><td colspan="11">▸ 단백질 구조 예측을 위한 딥러닝 기반 생명정보 분석 플랫폼
▸ 생체분자 데이터 처리 및 AI 모델 학습을 통해 신약개발·단백질 설계에 활용 가능</td></tr>
<tr><th colspan="11">통제 번호</th></tr>
<tr><td>WA</td><td colspan="2">미국</td><td colspan="2">유럽</td><td colspan="2">일본</td><td colspan="3">한국</td></tr>
<tr><td>5D002</td><td colspan="2">5D002 / 4D090</td><td colspan="2">5D002</td><td colspan="2">5D002</td><td colspan="3">5D002</td></tr>
<tr><th colspan="11">품목 해설</th></tr>
<tr><td colspan="11">▸ 고성능 연산용 GPU·TPU에서 동작하며, 병렬 학습 및 모델 파라미터 연산량이 고성능 컴퓨팅 수준임
▸ 암호화된 의료 데이터 처리 기능 포함 시 5D002(암호화 SW) 적용 가능
▸ 생체정보 분석 AI로서 센서·영상 SW, AI 기반 데이터 마이닝 SW로도 검토 가능
  </td></tr>
<tr><td colspan="11">관련 기업</td></tr>
<tr><td colspan="11">영국: DeepMind</td></tr>
</table>

품목											
영상 생성 플랫폼											
암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율 주행/로봇	네트워크 감시	보안	군사	바이오 의료

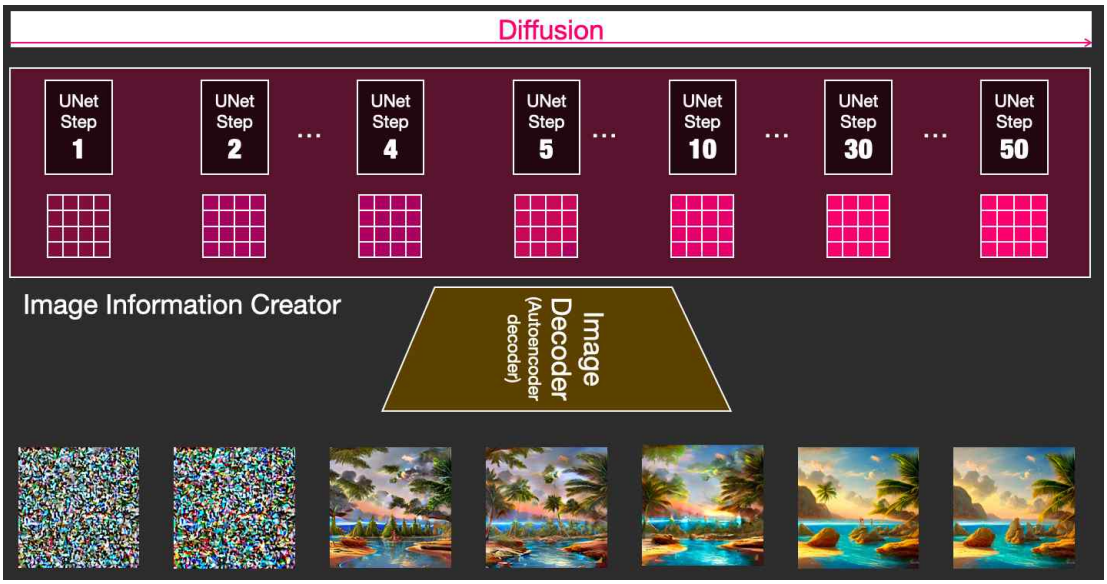
▸ 오픈소스 기반 이미지 생성형 AI 플랫폼
▸ 대규모 텍스트-이미지 데이터셋을 학습, 이미지 합성 및 분석에 활용 가능

통제 번호

WA	미국	유럽	일본	한국
-	4D090	캐치올 가능	-	상황허가 가능

품목 해설

▸ 모델 학습 및 확산 생성 과정에서 고성능 컴퓨팅 수준 병렬 연산(4D090) 수행
▸ 생성 이미지의 변조·오용 가능성(가짜뉴스·심리전 등)으로 EU Dual-use Regulation 821/2021에서 모니터링 권고 대상임
▸ 민간 공개 SW지만 군·정찰 목적 이미지 합성 응용 시 통제 검토 가능



관련 기업

영국: Stability AI

품목											
AI 기반 빅데이터 분석 SW											
암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율 주행/ 로봇	네트워크 감시	보안	군사	바이오 의료

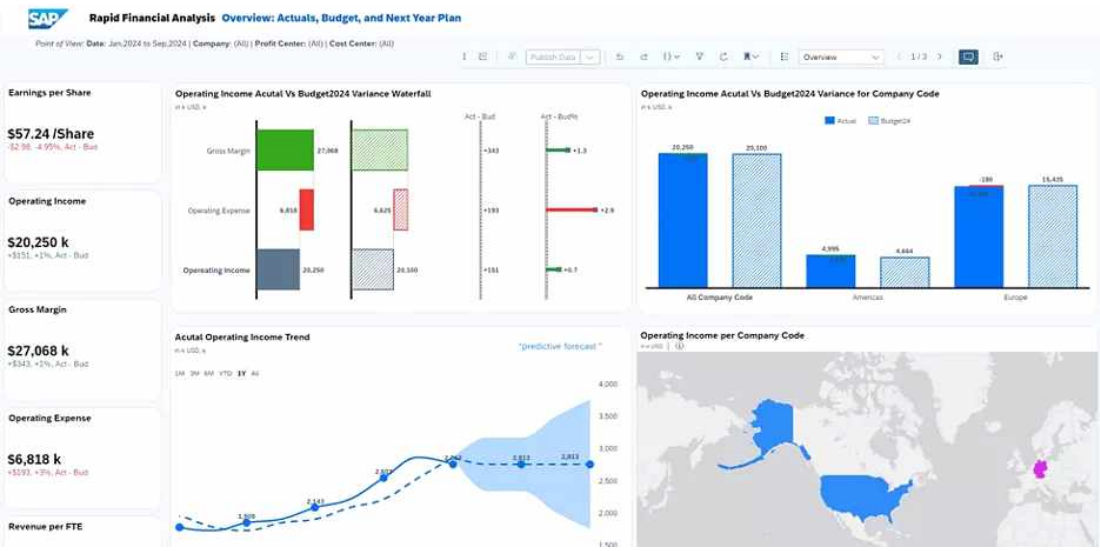
▸AI 기반 ERP·데이터 분석 클라우드
▸기업의 공급망, 금융, 국방 분석 등에 활용 가능

통제 번호

WA	미국	유럽	일본	한국
5D002	5D002 / 4D090	5D002	5D002	5D002

품목 해설

▸EU 규정상 데이터 처리·암호화 기능을 동시에 수행하는 AI 분석 SW로 분류됨
▸AI 기반 빅데이터 분석 SW로 고성능 컴퓨팅 병렬처리(4D090) 및 5D002(암호화) 조항에 해당
▸유럽 내 군수 물류·안보 데이터 분석 기능 포함 시 통제 대상 가능성 높음



관련 기업

독일: SAP

6.1.3. 일본 AI SW 통제 품목 사례

<table>
<tr><th colspan="11">품목</th></tr>
<tr><td colspan="11">고성능 컴퓨팅 기반 AI 학습용 SW 프레임워크</td></tr>
<tr><td>암호화</td><td>AI 인프라</td><td>모델 학습</td><td>음성</td><td>영상</td><td>언어 처리</td><td>데이터</td><td>지율 주행/로봇</td><td>네트워크 감시</td><td>보안</td><td>군사</td><td>바이오 의료</td></tr>
<tr><td colspan="11">▸ 고성능 컴퓨팅 기반 AI 학습용 SW 프레임워크
▸ 대규모 모델 병렬 학습 및 연구기관용 클러스터 관리 기능 포함</td></tr>
<tr><th colspan="11">통제 번호</th></tr>
<tr><td colspan="2">WA</td><td colspan="3">미국</td><td colspan="3">유럽</td><td colspan="2">일본</td><td>한국</td></tr>
<tr><td colspan="2">-</td><td colspan="3">4D090</td><td colspan="3">캐치올 가능</td><td colspan="2">-</td><td>상황허가 가능</td></tr>
<tr><th colspan="11">품목 해설</th></tr>
<tr><td colspan="11">▸ 일본 내각부 공고(별표 제1의 4호)에 따라 고성능 컴퓨팅 관련 SW로 명시
▸ 민간 연구용이지만 군수 전용 가능성 존재 시 별도 허가 대상
▸ AI 학습용 클러스터 관리 SW로, 고성능 컴퓨터 운용 SW/기술과 연계 평가 가능함
  </td></tr>
<tr><th colspan="11">관련 기업</th></tr>
<tr><td colspan="11">일본: Fujitsu, RIKEN</td></tr>
</table>

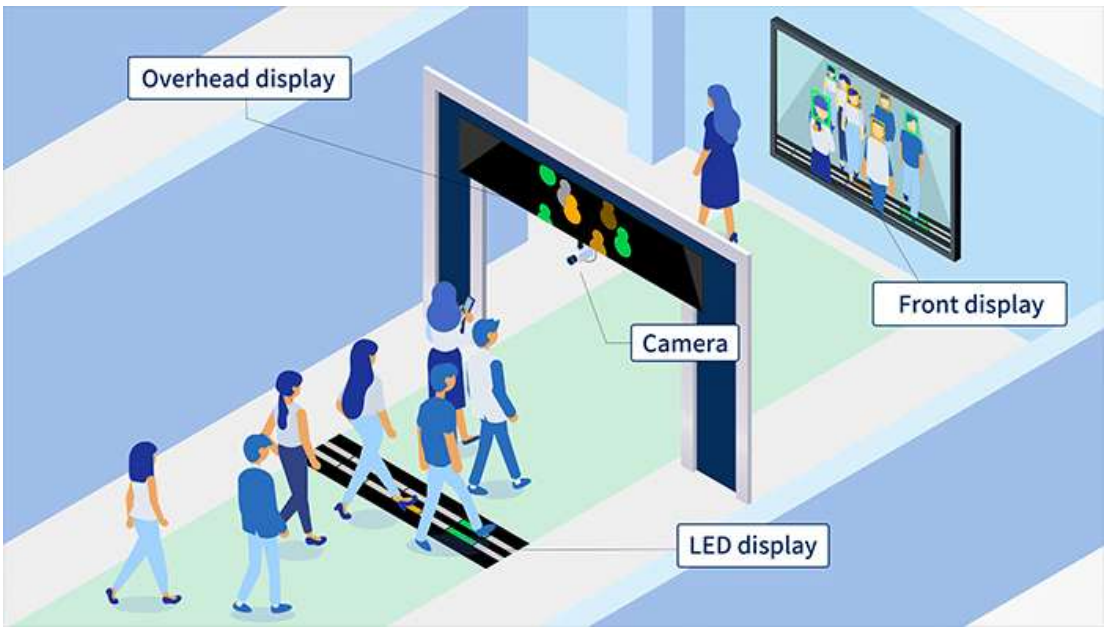
품목											
얼굴 인식 플랫폼											
암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율 주행/로봇	네트워크 감시	보안	군사	바이오 의료

▸ 실시간 얼굴 인식·신원확인 시스템
▸ 대규모 감시 데이터 분석 기능 포함, 공항·경찰·국가보안기관 사용

통제 번호				
WA	미국	유럽	일본	한국
-	4D090	캐치올 가능	-	상황허가 가능

품목 해설

▸ 민수 감시용은 예외지만, 치안·국가정보 시스템 적용 시 통제 대상
▸ 얼굴 인식 알고리즘이 센서·영상 처리 SW 및 4D090(고성능 병렬처리 SW) 범위에 해당될 수 있어, 통제 가능성 있음



관련 기업

일본: NEC Corporation

품목											
드론·자율주행용 비전 AI SW											
암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율 주행/ 로봇	네트워크 감시	보안	군사	바이오 의료

▸ 드론·자율주행용 비전 AI SW
▸ 객체 탐지·추적·경로계획 기능 포함 군사 감시용으로 전용 가능성 존재

통제 번호

WA	미국	유럽	일본	한국
6D001~6D003	6D001~6D003 / 7D003/7D004	6D001~6D003 / 7D003/7D004	6D001~6D003 / 7D003/7D004	6D001~6D003 / 7D003/7D004

품목 해설

▸ 일본 경제산업성 해석상 비전·항법 AI SW는 군사적 응용 가능성 존재 시 심사 대상
▸ 자율비행·표적 인식 등 포함 시 별표 제1의 7호(항법 관련 SW)에 해당함
▸ 자율주행용 센서 융합·영상 인식 기능이 6D001~6D003(센서·광학 SW) 및 7D003/7D004(항법·유도 SW) 범위에 해당되어, 통제 가능성 있음

관련 기업

일본: NEC Corporation

6.2. 국내 AI SW 통제 품목 사례 분석

<table>
<tr><th colspan="11">품목</th></tr>
<tr><td colspan="11">보안관제 AI</td></tr>
<tr><td>암호화</td><td>AI 인프라</td><td>모델 학습</td><td>음성</td><td>영상</td><td>언어 처리</td><td>데이터</td><td>지율 주행/ 로봇</td><td>네트워크 감시</td><td>보안</td><td>군사</td><td>바이오 의료</td></tr>
<tr><td colspan="11">▸AI 기반 사이버위협 탐지·분석 플랫폼(AICC: AI Cyber Command Center)
▸로그·트래픽 데이터를 실시간 분석하여 이상행위 탐지 및 침투 예측 수행</td></tr>
<tr><th colspan="11">통제 번호</th></tr>
<tr><td>WA</td><td colspan="2">미국</td><td colspan="2">유럽</td><td colspan="2">일본</td><td colspan="3">한국</td></tr>
<tr><td>5D002</td><td colspan="2">4D090 / 5D002</td><td colspan="2">5D002</td><td colspan="2">5D002</td><td colspan="3">5D002</td></tr>
<tr><th colspan="11">품목 해설</th></tr>
<tr><td colspan="11">▸네트워크 이상행위 탐지 AI 프레임워크, 대규모 로그 분석·병렬 학습 SW
▸보안 데이터 암호화 및 AI 기반 이상 탐지 기능 통합
▸고성능 병렬처리 SW 해당 가능, 위협 예측/보안자동화 수행 시 4D090 적용 가능, 암호화(5D002) 적용 가능
  </td></tr>
<tr><th colspan="11">관련 기업</th></tr>
<tr><td colspan="11">한국: SK쉴더스</td></tr>
</table>

<table>
<tr><th colspan="11">품목</th></tr>
<tr><td colspan="11">LLM</td></tr>
<tr><td>암호화</td><td>AI 인프라</td><td>모델 학습</td><td>음성</td><td>영상</td><td>언어 처리</td><td>데이터</td><td>지율 주행/ 로봇</td><td>네트워크 감시</td><td>보안</td><td>군사</td><td>바이오 의료</td></tr>
<tr><td colspan="11">▸LLM을 효율적으로 학습하기 위해 모델 병렬화(Tensor Parallelism), 파이프라인 병렬화(Pipeline Parallelism), 데이터 병렬화(Data Parallelism) 결합 구조 채택
▸NAVER Cloud 슈퍼컴퓨터 (HyperScale AI Platform) 상에서 멀티노드·멀티GPU 간 통신 최적화를 수행, NVIDIA NVLink / Infiniband 기반 고속 인터커넥트 활용</td></tr>
<tr><th colspan="11">통제 번호</th></tr>
<tr><td>WA</td><td colspan="2">미국</td><td colspan="2">유럽</td><td colspan="2">일본</td><td colspan="3">한국</td></tr>
<tr><td>-</td><td colspan="2">4D090</td><td colspan="2">캐치올 가능</td><td colspan="2">-</td><td colspan="3">상황허가 가능</td></tr>
<tr><th colspan="11">품목 해설</th></tr>
<tr><td colspan="11">▸한국어 및 멀티모달(텍스트·이미지·음성) 데이터셋으로 사전학습된 모델을 API 및 클라우드 서비스 형태로 외부 제공
▸LLM Fine-tuning·Prompt Engineering·지식검색형 생성 모델 등 다양한 산업군에서 활용 가능
▸4D001(병렬처리 SW) 기준에 적용 가능, 초거대 모델(수백억~수천억 매개변수) 운용 시 4D090(고성능 AI 응용 SW) 기준 적용 가능
  </td></tr>
<tr><th colspan="11">관련 기업</th></tr>
<tr><td colspan="11">한국: 네이버</td></tr>
</table>

품목

영상 변환 플랫폼

암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율주행/로봇	네트워크 감시	보안	군사	바이오 의료

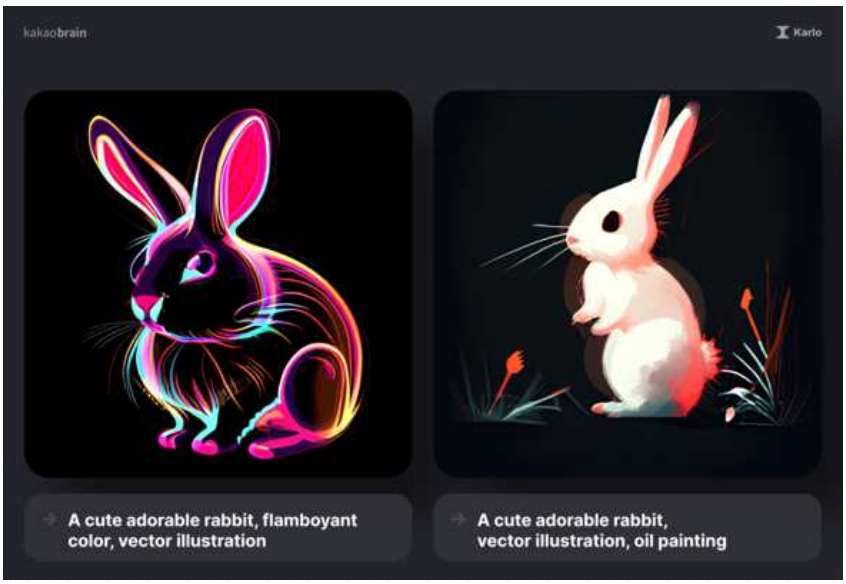
- 텍스트 입력을 이미지로 변환하는 Diffusion 기반 생성형 모델, 내부적으로 수억 건의 이미지·문장 페어 데이터를 병렬 처리하여 학습
- KoGPT 언어모델과 통합된 크로스모달 파이프라인을 통해 텍스트 의미 벡터를 시각적 잠재공간(latent space)으로 투영

통제 번호

WA	미국	유럽	일본	한국
-	4D090	캐치올 가능	-	상황허가 가능

품목 해설

- 학습 인프라는 다수의 GPU 노드가 연결된 분산 환경, 데이터·모델 병렬화를 통해 Stable Diffusion 구조를 대규모 확장
- 창작물 생성 자동화, 광고·디자인용 이미지 합성 등 산업 적용 가능
- 대규모 병렬 학습 구조를 갖는 생성형 AI로 4D001(병렬처리 SW) 범주에 포함
- 고해상도 이미지 합성·콘텐츠 제작 등 고성능 생성 응용에 해당, 4D090(고성능 AI 응용 SW) 적용 가능



관련 기업

한국: 카카오

품목											
자율주행 AI 플랫폼											
암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율 주행/ 로봇	네트워크 감시	보안	군사	바이오 의료

▸ 차량 주변 센서(LiDAR, 카메라, RADAR) 수집 대용량 데이터의 병렬처리 기반 실시간 인식·판단 엔진 분석

▸ 인식, 판단, 제어 단계 포함 End-to-End 딥러닝 자율주행 SW 스택

통제 번호

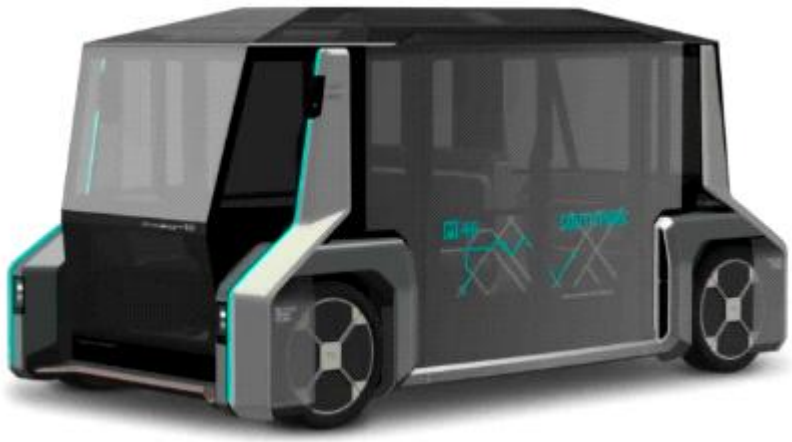
WA	미국	유럽	일본	한국
4A003	4A003 / 4A090 / 4D090	4A003,	4A003	4A003

품목 해설

▸ CNN·Transformer 기반 객체 검출 모델과, 강화학습 기반 주행 경로 결정 모델 통합

▸ 센서 융합(Fusion) 기반 분산 인지 시스템으로 고성능 컴퓨팅(4A003) 및 병렬 신경망 처리 SW에 해당

▸ 고성능 병렬처리 SW 분류 가능, 실제 주행 상황에서 실시간 의사결정 수행 AI 제어 응용 SW로 4A090 / 4D090 적용 가능



관련 기업

한국: 현대모비스

품목											
의료영상 진단 AI											
암호화	AI 인프라	모델 학습	음성	영상	언어 처리	데이터	지율주행/로봇	네트워크 감시	보안	군사	바이오 의료

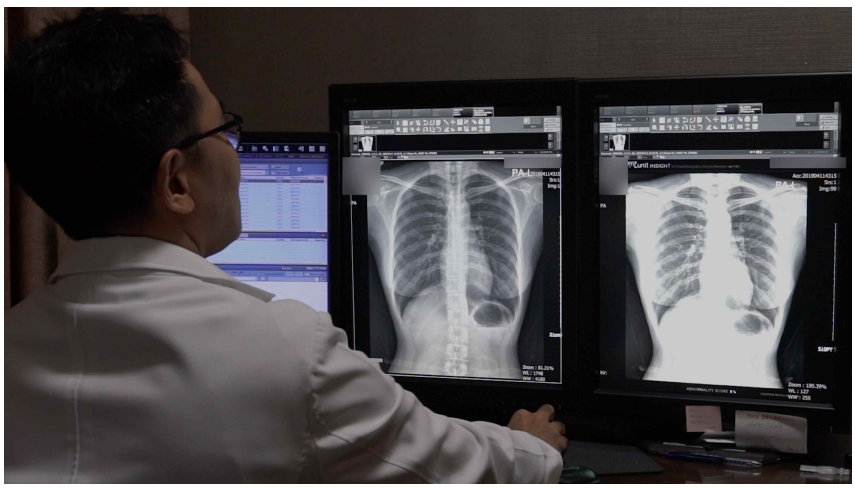
▸ 흉부 X-ray, 유방촬영, 병리 이미지 등 대규모 의료영상 데이터셋의 GPU 병렬 학습 구조에서 학습, 병변 위치 탐지 및 악성 확률 산출 모델 생성
▸ CNN 및 Vision Transformer 구조 혼합 의료 특화 네트워크 아키텍처 사용

통제 번호

WA	미국	유럽	일본	한국
-	-	-	-	-

품목 해설

▸ 분산 학습(Distributed Training) 통해 의료 영상의 다기관 데이터셋을 병렬로 처리
▸ 딥러닝 영상 분석 SW로 병렬처리 SW(4D001) 적용 가능성, AI 진단 및 영상 판독 기능 SW로 4D090(고성능 AI 응용 SW) 적용 가능성 있음
▸ 고성능 병렬처리 컴퓨터(4D001) 개발, 생산 SW가 아닌 응용 SW로 4D001에 해당한다고 보기 어려움
▸ 4A090((고성능 AI HW)용 전용 설계된 SW가 아닌 응용 SW로 4D090에 해당한다고 보기 어려움



관련 기업

한국: Lunit

6.3. 기업 대상 설문조사 분석

- 전체 AI SW 관련 참여 기업의 수는 355개로 SW 개발, 데이터 분석, 시스템 개발/통합 등 다양한 분야의 기업이 참여함
- 참여 AI SW 관련 기업에 대해 다음과 같은 수출통제 제도/판정 관련 항목에 대한 설문 조사를 시행함

(1) 참여 기업의 주요 업종

(2) 참여 기업의 주력 제품 및 서비스

(3) 참여 기업의 보유 AI 기술

(4) 참여 기업의 전략물자 제도(전략물자 판정, 수출통제제도 등) 인식

(5) 참여 기업의 AI 관련 제품/기술에 대한 전략물자 자가판정 또는 전문판정 진행 경험

(6) 참여 기업의 AI 관련 제품/기술에 대한 향후 전략물자 자가판정 또는 전문판정 진행 계획

(7) 참여 기업의 AI 관련 품목의 전략물자 판정 제도 인식

(8) AI 관련 품목의 전략물자 판정 및 관리 제도 건의 사항

6.3.1. 기업의 업종 분류

- 참여 기업의 업종 기준 분류 결과는 다음과 같음

(1) SW 개발 (64%)

(2) 데이터 분석 (19%)

(3) 시스템 개발/통합 (12%)

(4) HW 개발 (2%)

- 참여 기업을 업종을 기준으로 분류한 결과 SW 개발과 데이터 분석이 전체의 약 83%를 차지함
- 참여 기업의 업종을 5장의 AI SW 구분 분석에 따라 구분하면 AI 기술 중 "(4) AI 응용" SW와 관련이 많은 것으로 보임
- 시스템 개발/통합은 5장의 AI SW 구분 분석에 의하면 "(2) AI 연산 인프라"나 "(3) AI 모델 학습"과 관련이 있는 것으로 보임

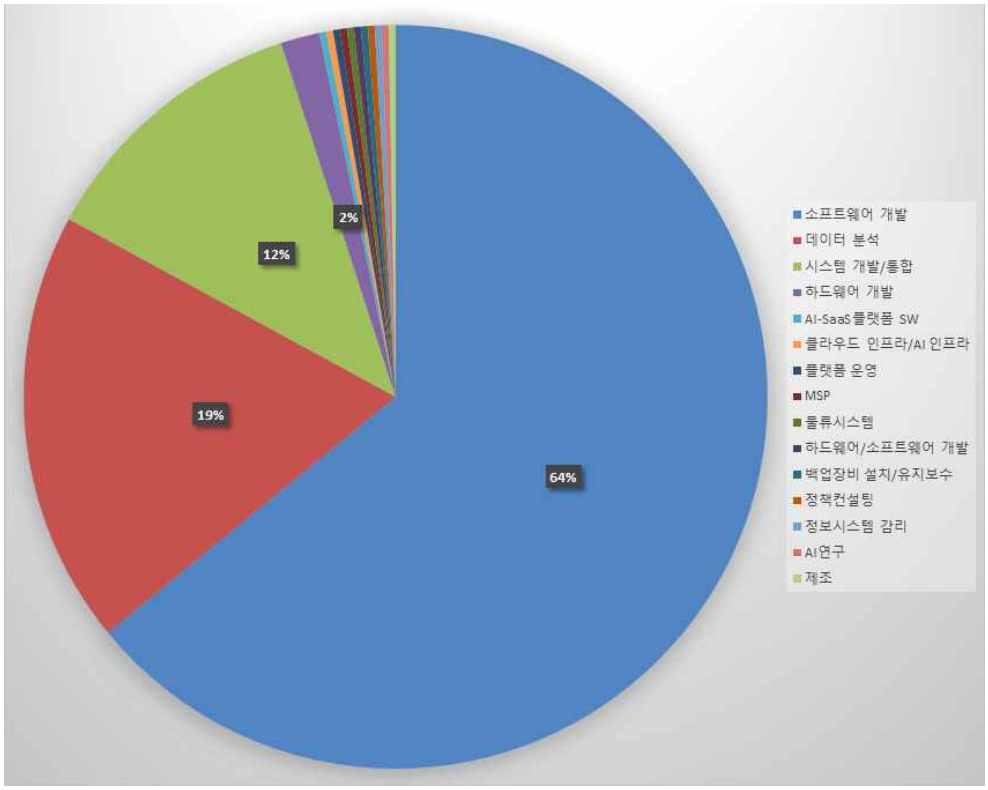


그림 6 참여 기업의 업종 분류

6.3.2. 기업의 주력 제품 및 서비스

- 참여 기업을 주력 제품 및 서비스를 기준으로 분류한 결과는 다음과 같음

(1) AI 기반 SW (40%)

5장 AI 기술 구분: "(2) AI 연산 인프라", "(3) AI 모델 학습", "(4) AI 응용"

(2) AI API/SaaS 등 (15%)

5장 AI 기술 구분: "(2) AI 연산 인프라", "(3) AI 모델 학습"

(3) AI 응용 시스템 (14%)

5장 AI 기술 구분: "(4) AI 응용"

(4) 클라우드 플랫폼 (11%)

5장 AI 기술 구분: "(2) AI 연산 인프라", "(3) AI 모델 학습"

(5) AI 모델(LLM, LVM 등) (8%)

5장 AI 기술 구분: "(2) AI 연산 인프라", "(3) AI 모델 학습"

- AI 기반 SW, AI API/SaaS, AI 응용 시스템 등이 전체의 약 69%를 차지함
- 기업의 주력 제품 및 서비스가 5장 AI 기술 구분에 따르면 "(2) AI 연산 인프라", "(3) AI 모델 학습", "(4) AI 응용" 등과 주로 관련이 있는 것으로 보임

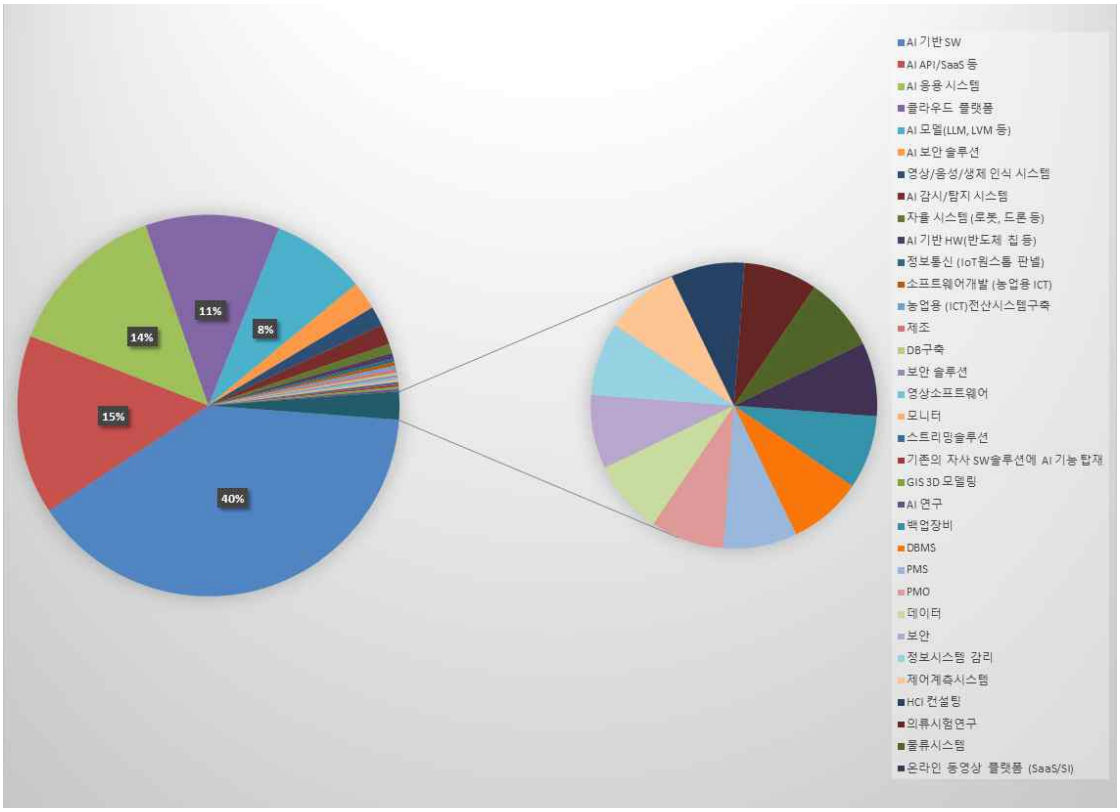


그림 7 참여 기업의 주력 제품 및 서비스

6.3.3. 기업의 보유 AI 기술

- AI 기술을 보유한 기업의 주요 AI 기술은 다음과 같음

(1) AI SW 기술 (42%)

(2) 클라우드/SaaS/IaaS/PaaS 기술 (26%)

(3) AI 모델 기술 (12%)

(4) AI 모델 기반 응용 기술 (10%)

(5) 영상/음성/생체 인식 기술 (4%)

(6) AI 보안 기술 (2%)

(7) AI 감시/탐지 기술 (2%)

(8) 자율 시스템 기술 (1%)

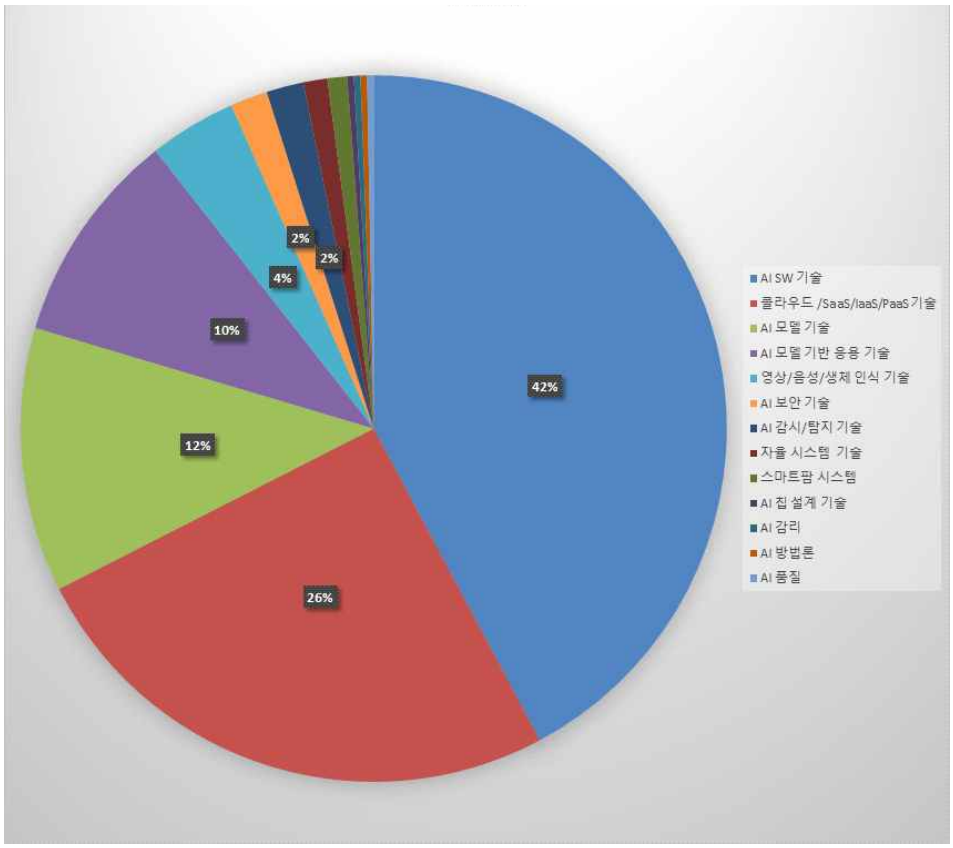


그림 8 참여 기업의 보유 AI 기술

- 전체 참여 기업 중 72.96% 기업이 다양한 형태의 AI 기술을 보유한 것으로 응답함
- AI SW 기술, 클라우드/SaaS/IaaS/PaaS 기술, AI 모델 기술이 전체의 약 80%를 차지함
- 다수 기업의 보유 AI 기술이 5장 AI 기술 구분의 "(2) AI 연산 인프라", "(3) AI 모델 학습", "(4) AI 응용" 등과 관련이 있을 것으로 보여 이들에 대한 수출통제 대상 여부 분석과 사례 제시가 중요할 것으로 보임
- 그 외 일부 기업이 AI 모델 기반 응용 기술, 영상/음성/생체 인식 기술, AI 보안 기술, AI 감시/탐지 기술, 자율 시스템 기술 등을 보유하고 있는 것으로 나타남

- 이는 5장 AI 기술 구분의 "(4-1) 음성 인식·합성", "(4-2) 영상 분석·생성", "(1) 암호화", "(6-1) 네트워크 감시·분석", "(5) AI 자율 주행/로보틱스" 등과 주로 관련이 있는 것으로 보임

6.3.4. 기업의 전략물자 제도 인식

- 참여 기업의 전략물자 제도(전략물자 판정, 수출통제제도 등)에 대한 인식 조사 결과는 다음과 같음

(1) 매우 잘 알고 있다 (11%)

(2) 어느 정도 알고 있다 (46%)

(3) 들어본 적은 있다 (32%)

(4) 전혀 모른다 (11%)

- 참여 기업의 약 57%가 전략물자 제도에 대해 매우 잘 알고 있거나 어느 정도 알고 있는 것으로 응답함
- 일반적인 전략물자 제도에 대한 기본 인식은 일정 수준을 보유하고 있는 것으로 보임

6.3.5. 기업의 AI 품목 전략물자 판정 경험

- 참여 기업의 AI 관련 제품/기술에 대한 전략물자 자가판정 또는 전문판정 진행 경험 관련 참여 기업의 약 98.59%가 AI 관련 제품/기술에 대한 전략물자 자가판정 또는 전문판정 진행 경험이 없는 것으로 응답함
- AI 관련 제품/기술에 대한 판정 경험이 있는 기업의 판정 관련 품목의 종류는 다음과 같음

(1) AI 기반 SW

(2) AI 보안 솔루션

(3) AI 모델(LLM, LVM 등)

(4) AI API/SaaS 등

(5) AI 응용 시스템

(6) AI 감시/탐지 시스템

(7) AI 기반 GIS

(8) 백업관련 장비

(9) 영상/음성 생체 인식 시스템

(10) 자율 시스템(로봇, 드론 등)

(11) 클라우드 플랫폼

- 아직까지 AI 관련 제품/기술의 직접적 수출 대상 및 확대가 많이 이루어지고 있지는 않은 것으로 판단됨
- 일부 판정 경험이 있는 품목들은 5장 AI 기술 구분에 따른 다양한 품목과 관련이 있는 것으로 보임

6.3.6. 기업의 AI 품목 전략물자 판정 계획

- 참여 기업의 AI 관련 제품/기술에 대한 향후 전략물자 자가판정 또는 전문판정 진행 계획 관련 참여 기업의 약 20.85%가 AI 관련 제품/기술에 대한 전략물자 자가판정 또는 전문판정 진행 계획이 있는 것으로 응답함
- 판정 계획이 있는 기업의 해당 판정 계획 품목의 종류는 다음과 같음

표 23 향후 판정 계획이 있는 기업의 판정 대상 품목

품목 종류	비율(%)
AI 기반 SW	34.1
AI 모델(LLM, LVM 등)	17.5
AI API/SaaS 등	11.9
AI 응용 시스템	12.7
AI 보안 솔루션	6.3
클라우드 플랫폼	3.2
AI 기반 HW(반도체 칩 등)	3.2
AI 감시/탐지 시스템	3.2
영상/음성 생체 인식 시스템	3.2
자율 시스템 (로봇/드론 등)	2.4

- 기존에 AI 관련 제품/기술에 대한 판정 경험이 있는 기업들(1.41%)에 비해서 많은 기업들(20.85%)이 향후 AI 관련 제품/기술에 대한 전략물자 판정 진행 계획이 있는 것으로 나타남

- 앞으로 많은 기업들이 AI SW 품목 관련 수출이나 전략물자 판정 계획을 가지고 있는 것으로 나타나 관련 통제 대상 품목에 대한 인식 제고가 필요한 것으로 보임

- 판정 진행 계획이 있는 기업의 주요 품목은 AI 기반 SW, AI 모델(LLM, LVM 등), AI API/SaaS 등, AI 응용 시스템, AI 보안 솔루션 등으로 약 82.5%를 차지함

- 판정 예상 AI SW 품목은 5장 AI 기술 구분의 "(2) AI 연산 인프라", "(3) AI 모델 학습", "(4) AI 응용", "(1) 암호화" 등과 관련이 있는 것으로 보여 이들에 대한 수출통제 대상 여부 분석과 사례 제시가 중요한 것으로 보임

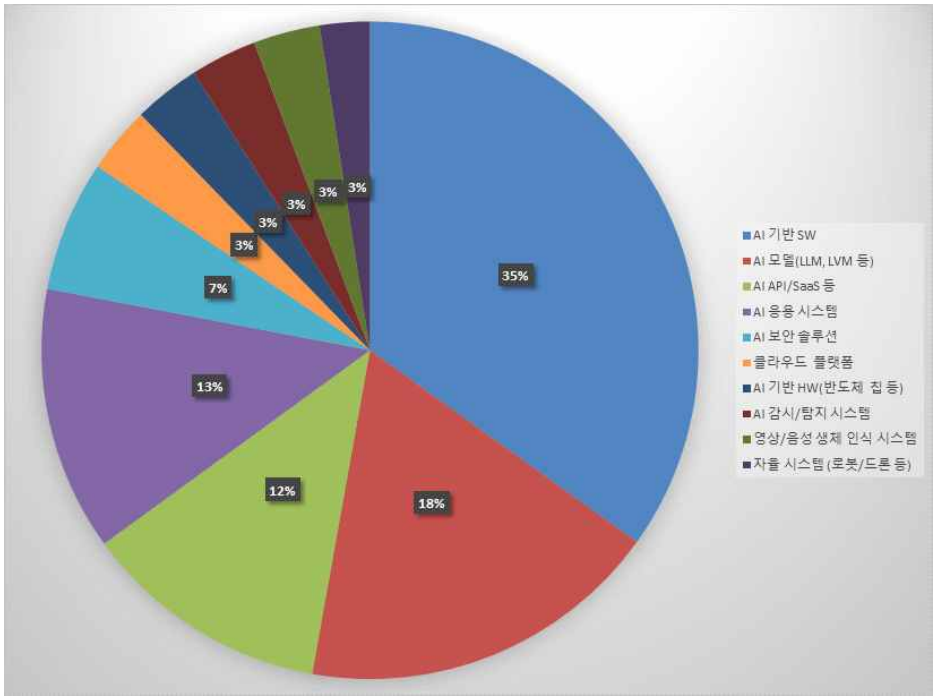


그림 9 판정 계획 기업의 판정 대상 품목

6.3.7. AI 관련 품목의 전략물자 판정 제도 인식

- 참여 기업의 AI 관련 품목의 전략물자 판정 제도 인식 조사 결과는 다음과 같음

(1) 불명확하다 (21.4%)

(2) 모호하다 (51.0%)

(3) 보통이다 (26.2%)

(4) 명확하다 (1.4%)

- 참여 기업들 중 AI 관련 품목의 전략물자 판정 제도가 모호하거나 불명확하다고 응답한 기업이 약 72.4%로 나타나 일반적인 전략물자 판정 제도에 대한 인식에 비해 AI 관련 품목의 전략물자 판정 제도에 대한 인식 제고가 필요해 보임

6.3.8. AI 관련 품목의 전략물자 판정/관리에 대한 의견

- 참여 기업들은 전반적으로 전략물자 수출통제 제도의 인식 확산을 위한 홍보, 교육 등이 필요하다고 응답하였으며, 판정 절차 간소화, 온라인/컨설팅 지원, AI 판정 기준 수립 및 명확화, 자율준수기업(CP) 확대, 기업에 대한 다양한 지원 등의 의견을 피력하였음
- 참여 기업이 응답한 AI 관련 품목의 전략물자 판정 및 관리 제도에 대한 주요 의견은 다음과 같음

(1) 홍보 및 교육

- 전략물자 수출통제 제도 전반에 대한 홍보와 교육
- 기업의 글로벌 진출에 필요한 수출통제 정보와 품목 기술 분류 및 관리, 수출입 절차, 내부 관리 체계 구축 등 관련 정보 전파와 교육
- 기업 대상 수출통제 제도 교육 프로그램 운영, 교육 컨텐츠 제공, 산업별 맞춤형 설명회 개최
- 전략물자 통제 및 관리 관련 최신 사례 공유
- 글로벌 수출통제 동향 정보공유

(2) 판정 절차 간소화 및 온라인/컨설팅 지원

- 판정 신청 서류, 제출 방식 등 간소화
- 판정 후 사후 점검 절차 단순화
- 판정 업무 처리 속도 개선을 위한 예산 지원 확대
- 판정 관련 비용 최소화로 기업 부담 경감
- 판정 관련 FAQ 등 관련 내용 업데이트 및 정보 제공
- 전략물자 수출통제 판정 기준 변경 시 사전 알림
- 판정 이력 관리 시스템 및 플랫폼 구축을 통한 기업 참고 정보 제공

- 판정 신청 전후 상담 및 컨설팅 지원
- 판정 관련 전문가 상담 창구의 확대
- 기업이 참고할 판정 사례, 판정 결과 활용 가이드 등 제작
- 판정 신청자에게 사전 안내 및 체크리스트 제공
- 기업 맞춤형 판정 관련 알림 서비스 제공
- 기업 내부 검토용 판정 모의 테스트 제공

(3) AI 품목 관련 판정 기준 수립

- AI 관련 품목들의 전략물자 판정 관련 통제 기준 및 가이드라인 제공
- AI 모델, AI 학습용 데이터셋 등 관련 통제 대상 등 정보 제공
- AI SaaS/클라우드 서비스, GPU 등 AI 반도체 관련 통제 기준 등 정보 제공

(4) 판정 기준 명확화

- 판정 대상 품목의 판정 기준 명확화
- 판정 대상 품목의 직관적 분류 고려
- 기술 발전 속도에 맞춘 판정 제도 및 판정 기준의 신속한 개정
- 기술개발 단계별 수출통제 영향도 안내 고려
- 암호화 기능 품목 등의 통제 기준 현실화
- 판정 결과 관련 판정 데이터 기반 분석 자료 제공
- 국제체제/국가별 상이한 통제 규정 비교 및 차이 설명
- 판정 기준 변경 시 기업 의견 수렴 과정을 통한 산업계 의견 반영

(5) 자율 준수 기업 확대

- 자율준수기업(CP) 인증 확대
- 기업 내부의 자율 준수 활동에 대한 인센티브 제도 도입/확대

(6) AI 산업 활성화

- AI 산업의 발전, 산업 경쟁력 확보 및 기술안보를 위한 산업 발전과 수출통제의 균형 유지
- 불필요한 중복 규제의 최소화

(7) 기업 지원

- 수출 기업 대상 지원팀 운영
- 신규 수출 기업을 위한 수출 및 전략물자 관련 컨설팅
- 대기업, 중견기업, 중소기업, 스타트업 기업별 맞춤형 컨설팅 제공
- 전략물자 판정 관련 법률 상담 지원
- 산업별 전문 컨설턴트 지원 프로그램 제공
- 글로벌 파트너 기업과의 협력을 위한 제반 지원

(8) 중소기업 지원

- 수출관리 전문 인력 부족에 대한 중소기업 지원
- 중소기업 전용 우대 및 판정 지원 제도 운영
- 중소기업 수출통제 관련 비용 지원 바우처 제공
- 스타트업 기업을 위한 맞춤형 가이드 제공

(9) 기타

- 관리 제도 적용 시 국내외 산업 영향 분석

- 수출통제 관련 장기적 로드맵 제시
- 산업별 데이터 기반 리포트 제공
- 판정 제도 개정 시 기업 의견 수렴
- 전략물자 관련 법규와 판정 지침 통합 제공

6.4. 기업 대상 인터뷰 분석

- AI 관련 기업의 전략물자 수출통제와 관련한 현황 파악과 의견 수렴을 위해 AI 반도체 칩 설계, AI 검색 플랫폼, AI 보안, AI 데이터 분석, AI 에이전트 등 주요 분야 관련 기업 5개사에 대해 2025.9.25~2025.10.31까지 현장/온라인 인터뷰를 진행함

6.4.1. 참여 기업

- 인터뷰에 참여한 기업은 반도체, 데이터 분석, 보안, 검색, 에이전트 등 AI 관련 5개 분야의 기업으로 다음과 같음

(1) A사

- 반도체 설계
- AI 추론 반도체 칩 설계

(2) B사

- 데이터 분석
- AI 데이터 분석/클라우드 서비스

(3) C사

- 보안
- AI 보안/클라우드 보안

(4) D사

- 검색 서비스
- AI 검색/서비스 플랫폼

(5) E사

- 에이전트 서비스

- AI 서비스/에이전트

6.4.2. 주요 제품군 및 수출 지역

(1) 주요 제품군

- AI 추론용 반도체 칩
- AI 보안 관리 도구
- 산업용/전문가용 AI 모델 및 에이전트
- 사내 비지니스 AI 시스템 및 AI 에이전트
- AI 멀티 에이전트

(2) 주요 수출 지역

- 미국, 북미
- 유럽
- 아시아: 일본, 대만, 동남아
- 중동
- 해외 법인

6.4.3. 주요 제품 형태

- AI 추론용 반도체 칩
- AI 시스템 인프라 및 서비스
- On-premise AI SW
- SaaS/클라우드 AI 서비스

6.4.4. 주요 의견

- 많은 기업이 전략물자 통제 체계 운영 및 관리권으로 편입되기를 희망하며, 전략물자 관리 체계의 운영 및 선제적 대응이 글로벌 경쟁력 확보에 도움이 됨을 인식하는 것이 중요하다는 의견을 제시함
- 수출통제 관리 절차가 개발, 양산, 계약, 허가, 수출, 관리 등 제품 사이클 전 단계에 포함되어 실행되도록 하는 절차가 필요할 것으로 보임
- 자율준수체계(CP) 인증 참여 유도 및 확대를 통한 수출통제 절차의 간소화 및 단축이 필요할 것으로 보임
- 인터뷰 참여 기업의 주요 의견 및 건의 사항은 다음과 같음

(1) 판정 기준 명확화

- AI 품목의 수출통제 판정 기준이 명확할 필요가 있음
- 암호화 관련 품목의 통제 조항 현실성 제고가 필요함

(2) 전략물자 제도 인식 제고

- CEO 등 기업 및 기관 책임자의 관심과 지원이 필요함
- 전략물자 관리 체계 운영 및 선제적 대응이 글로벌 경쟁력 확보에 도움이 됨
- 더 많은 기업이 전략물자 통제 체계 운영 및 제도권으로 편입되는 것이 바람직함
- 전략물자 수출통제 개념 정립 및 필요성 관련 인식 제고 및 내부 교육이 필요함
- 기업 부담감 해소 및 신속한 수출 환경 마련을 위해 제도의 명확·간소화, 인센티브 등이 필요함

(3) 기업의 전략물자 관리 절차 수립

- 수출통제 절차가 개발, 양산, 계약, 허가, 수출, 관리 등 전단계에 포함되어 실행되도록 하는 내부 절차가 필요함
- 수출통제 관리 문서 및 규정집의 온라인 배포 및 조회수 확인 등을 통한 관심 유도와 인식 확산이 필요함
- 국내 AI 기업들이 수출 가능성이 높은 품목을 보유하고 있음에도 전략물자 수출통제 관련 전담 조직 구성이 어려움

(4) 자율준수체계(CP) 인증 참여 및 확대

- CP 인증 참여 유도를 통한 수출통제 절차의 간소화 및 기간의 단축이 필요함
- 자율준수체계 등급 보유로 자가 판정 권한, 포괄허가 등 혜택 부여가 가능함을 인지할 필요가 있음
- AI 품목의 수출통제 관련 지원 시스템 운영 검토가 필요함

(5) 기타

- 수출통제 관련 민간 협의체 운영에 대해 고려해볼 필요가 있음
- 미국의 기술 보호 정책으로 대만 등 다른 국가의 규제 조치가 강화되고 있어 이에 대한 지원 및 협력이 필요함
- 중소기업의 경우 주요 수출국 대응과 함께 대만 등 다른 국가의 규제 조치 대응을 위한 제도 안내 및 전문 컨설팅 지원 검토가 필요함

VII AI SW 수출통제 대응 방향 및 가이드라인

제7장 AI SW 수출통제 대응 방향 및 가이드라인

- 본 장에서는 앞에서 살펴본 AI SW 품목의 WA, 미국, 유럽, 일본, 한국의 수출통제 체제 및 통제 대상과 통제 가능성이 있는 품목, 기업의 인터뷰와 설문 조사 결과를 바탕으로 필요한 정책적 대응 방향, 기업의 대응 방향 및 판정 관련 가이드라인을 제시하고자 함

7.1. AI SW 수출통제 대응 방향

- AI SW의 수출통제와 관련 기존의 전통적인 HW 위주 수출통제 패러다임을 넘어, 주요 기능 및 최종 사용 위험 등을 기준으로 새로운 수출통제 체계가 형성되고 있음
- 정책적으로 WA 등 국제 체제 간 통제 대상 품목이나 통제 사양의 정합화와 함께 산업 자율성의 균형을 추구하고, 기업은 제품 사이클 전단계에서의 품목 분류 및 수출통제 관리 역량을 주요 대응축으로 강화해 나갈 필요가 있음

7.1.1. 정책적 대응 방향

- 급속히 변하는 AI 기술의 특성과 AI 산업 발전의 중요성과 필요성을 기술안보 측면의 수출통제 관점에서 함께 이해하고 균형을 이루어 글로벌 경쟁력을 확보할 수 있도록 하는 차원에서 대응 방향을 수립하고 접근할 필요가 있음

(1) AI 품목 특화 분류체계 도입

- AI SW 품목을 특성 및 기능에 따라 적절히 구분하고 통제 대상 조항과의 매핑을 위해 AI SW 품목의 하위 분류 신설 검토

  예: 5장의 AI SW 품목의 특성/기능별 분류

  AI 연산 인프라 SW, AI 모델 학습 SW, 응용 SW 등

(2) 수출판정 제도 및 절차의 고도화

- AI SW의 세부 분류 품목의 통제대상 가능성 매핑
- AI 관련 품목의 HS 코드와 통제 대상 품목 간의 연계 가능성 검토
- HS 코드와 통제 대상 품목 간 자동 연계 시스템(HS 코드 + 통제 대상 매핑 AI) 검토

(3) 상황허가(캐치올) 운용의 고도화

- AI 기술 발전 속도 대비 통제 리스트 반영의 지연 문제 보완
- 엔드유즈 리스크 관리 중심의 AI SW 캐치올(군사 및 감시 용도) 관리 방향 설정
- 군용 또는 감시/보안 목적 전용 가능성 판단을 위한 지침 제공

(4) 국제공조 및 정보공유와 다자체제·동맹국 공조 강화

- 미국 BIS, EU DG TRADE 등과 정책 대화 채널 구축
- AI, 양자, 반도체 등 첨단 기술 분야 공동 정책 협의 기구나 워킹그룹 운영 고려

(5) 기업 및 산업계 품목 특성별 수출통제 관리 부담 완화

- 민수용 AI SW의 기본적인 통제 비해당 가능성 명확화
- 의료·교육·상업 용도 AI SW의 통제 비해당 가이드라인 제공

- AI SW 품목의 자가 판정 가이드라인(AI SW 체크리스트) 제공

(6) 수출통제 제도 관련 인식 제고 및 전문 인력 양성

- 수출통제 제도를 글로벌 스탠다드를 지향하는 관점에서 기본 컴플라이언스로 인식
- 수출통제 관련 기술과 법 체계를 통합하는 복합 전문가 교육
- AI 관련 품목의 수출통제 관리를 담당하는 AI 담당 컨설턴트의 운영 고려
- 산학연 공동 수출통제 교육 프로그램 운영

7.1.2. 기업의 대응 방향

- AI SW 관련 기업은 다양한 AI 품목의 수출통제 체계 및 프로세스 관리 역량 제고 관련 다음과 같은 방향을 고려할 필요가 있음
- 기본적으로 AI SW 관련 기업은 분류, 판정, 허가, 내부 관리, 데이터 보호 등 5단계 관리 체계로 AI SW 수출통제를 관리하는 것이 바람직할 것으로 보임

(1) 제품 분류 및 주요 정보 파악

- 기업 제품별로 5장의 AI 기술 분류표에서 해당되는 분류 대상의 매핑
- 연계된 분류 대상과 관련되는 주요 통제 대상 및 통제 사양 기준 등 검토
- AI 고성능 컴퓨팅 HW에 전용 설계(specially designed)된 SW인지 검토

  제품/패키지 등 관련 문서에 GPU등 특정 고성능 컴퓨팅 HW 전용성(전용 설계 여부), 주요 핵심 기능 등 기재
- AI SW 설계, 개발 단계에서 미국 FDPR 적용 여부 점검

  미국 장비, SW, 기술 사용 여부 및 포함 정도 분석
- 최종 용도 확인(EUC, End-use Certificate), 수출 대상 국가, 최종 사용자, 우

려 거래 대상자 정보 관리 및 사전 심사(캐치올 가능성)

- AI SW 라이선스 판매, API 이용계약 시 최종 사용자 관리 조항 고려
- 의료, 교육, 내부 업무용 등 비군사 민수용은 엔드유즈 진술서 작성

(2) 판정 및 허가

- 무역안보관리원(KOSTI)에 품목 전문판정 신청 및 해당/비해당 결과 확보
- 전략물자 비해당이라도 수출 대상 국가, 최종 사용자, 우려 거래 대상자, 사용 용도에 따른 상황허가 대상 여부 판정 신청
- 해당/비해당 판정 관련 문서 5년 이상 보관(대외무역법 시행령 제55조, 전략물자수출입고시 제57조)

해당/비해당 판정서, 판정 근거자료, 기술자료, 고객정보 등 보관

(3) 클라우드, SaaS 등 배포 관리

- 클라우드/SaaS 서비스 시 기본적으로 수출에 준하는 것으로 보고 수출허가 등 관리
- 클라우드 API 접속 국가/사용자 통제 및 권한 관리
- 해외 사용자 접속 관리(Geo-blocking) 고려
- Geo-IP/ASN(Autonomous System Numbers) 차단, KYC(Know Your Customer), API 스로틀링(Throttling) 등 Geo-Fencing 고려

(4) 모델 및 데이터 관리

- AI 모델, 학습 데이터, 모델 파리미터 등의 별도 관리 및 접근 통제
- 해외 전송 및 이동 시 암호화 및 접근 권한 관리
- AI 모델 및 모델 파라미터 등의 향후 통제 가능성에 대비

(5) 전략 기술 이전, 기술 협력 및 오픈소스 활용 관리

- 다양한 형태(노하우, 기술 문서, 세미나 등)의 전략 기술 이전 시 전략 물자 수출통제와 유사한 관리 고려
- 외국 협력사/파트너와의 공동연구/기술 협력 시 기술 이전 요건 검토
- 오픈소스 활용 SW 설계 및 개발 시 통제 대상, 라이선스 조건, 미국 FDPR 조건 등 확인

  예: 오픈소스 기반 LLM SW 개발(고성능 컴퓨팅 GPU/TPU 등과 연계)

  공개 모델 기반 대규모 얼굴 인식 SW 개발(감시/추적 기능)

  공개 AI 개발 프레임워크에 데이터 암호화 기능 등 추가 SW 개발

(6) 교육 및 관리 체제 수립

- 수출통제 제도 및 AI 관련 품목 수출통제 교육 제도화
- 수출통제 제도 인지, 내부 관리 및 점검 프로세스 운용

  개발, 생산, 계약, 판정, 허가, 수출, 배포, 사후 관리 등 제품 전 단계

  1) 관리자/담당자 지정: 수출통제 관리자/담당자 선임
  2) 관리 프로세스 수립: 각 단계별 관리 절차 수립

     제품 분류 → 판정 → 허가 → 수출 → 사후 관리
  3) 교육/점검: 연 1회 이상 교육 및 내부 관리
  4) 문서 관리: 판정서, 판정 근거자료, 기술자료, 고객정보 보관
  5) 신고/조사 대응: 관계기관 요청 시 자료 제출 준비 체계 수립
- 연간/수시 관리 체계 및 점검 개선 프로세스 수립

(8) 컴플라이언스 프로그램(CP) 운영 고려

- 자율준수기업(CP) 인증 추진/확대

  자가 판정, 포괄 허가 등 가능

  판정/허가 절차/시간 간소화

(9) 관련 정보 업데이트, 정부 협의 및 컨설팅 채널 확보

- 무역안보관리원 안내서, 정보 및 FAQ 참고

  무역안보24, 이슈 분석리포트, 해외연구동향 Report, 무역안보 Brief 등

- 미국 BIS FAQ, EU Catch-all 가이드 등 참고
- 정기/비정기 법률, 기술 자문 라인 구축
- 수출통제 판정 및 해외 수출통제 동향 모니터링

7.2. AI SW 품목의 수출통제 가이드라인

7.2.1. AI SW 수출통제 대상 여부 검토 시 주요 고려 사항

- AI SW 품목의 수출 통제 대상 여부를 결정하는데 필요한 주요 고려 사항(표 24 참조)은 다음과 같음

(1) 수출 대상 국가

- 국가별 해당 지역 등급 검토
- 별표6 전략물자 수출 지역 구분 기준으로 국가별 "가" "나" 지역 확인
- "가" 지역 이외 지역 수출 시 허가 대상 가능성 검토

(2) 최종 용도

- 군사·치안·전략 목적 전용 가능성 검토
- 대규모 감시·식별·추적 등 보안 기능 여부 검토
- 제품/서비스 설명서에 민수용/비군사용 등 사용 목적 문서화
- 기술 문서, 기능 설명서, 계약서 등에 보안·감시 기능 포함/비포함 명시
- 군/경찰/보안 기관과의 거래 시 상황허가(캐치올) 여부 검토

(3) 최종 사용자

- 엔드유즈 진술서(EUC) 확보 및 보관
- 우려 거래 대상자 검색 및 관리(무역안보관리원 홈페이지)
- 재수출 여부 및 조건 관리
- 계약서에 재수출 금지 및 용도 제한 조항 삽입 포함 여부 결정

(4) 미국 FDPR

- 미국 기술, 장비, SW 사용 설계/개발 품목 여부 검토

  미국 GPU(NVIDIA, AMD) 또는 SW(TensorRT 등) 사용 시 EAR §734.9 FDPR 적용 여부 검토
- 미국 오픈소스 기반 모델의 라이선스나 통제 대상 가능성 검토
- 미국 기술 포함 시 미국 재수출 허가 필요 가능성 검토

  예: 국내 기업이 미국 엔비디아 GPU 기반 클라우드에서 AI 학습·추론 API 제공 시 미국산 GPU 사용

(5) 클라우드/SaaS 서비스

- 사용 국가, 사용 지역, 사용자 국적 제한 여부 검토
- 최종 종단간(E2E) 데이터 암호화 적용 확인

- 서비스 약관에 국가별 접근 제한 조항 명시 여부 검토
- 클라우드 제공 형태(국외 호스팅 포함) 문서화

(6) AI SW 유형별 분류 및 매핑(표 25 참조)

- 제품별 특성/기능 분석서에 5장의 AI SW 특성/기능별 분류와 통제 대상 매핑 연계 관리
- 군사·보안 응용 포함 시 상황허가 신청 고려
- 의료용·민간용 SW 등의 군사·보안용 전용 제한 검토 및 명시

(7) AI SW 품목 분류 및 통제 대상 연계(표 25 참조)

- 품목의 AI SW 특성/기능별 분류
- 해당 분류 대상의 주요 점검 사항 확인
- 별표2에서 관련 통제 대상 및 통제 사양 확인

(8) 사후 관리

- 수출통제 관련 관리 프로세스의 상시 운영
- 주요 문서 등 일정 기간 관리 및 보관

  판정서, 판정 근거자료, 기술자료, 고객정보 등 문서 5년 보관
- 재수출·제3국 이전·국외 접근 로그 관리
- 정책 변경 시 재판정 또는 재허가 절차

(9) 통제 대상 관련 시나리오 예시 및 대응 전략

① 미국 기술/장비/SW 사용 AI 모델 SW의 중국, 러시아 등 수출

4D090 해당 가능성 (미국 FDPR 적용 여부 확인)

미국 수출허가 신청 및 EUC 관리

② 클라우드/SaaS API 형태의 AI 모델 서비스 제공

클라우드/SaaS도 기본적으로 SW 수출에 준하는 수출통제 관리

서비스 국가별 Geo-Fencing 및 접속 로그 보존 관리

③ AI 보안·감시 SW

군사·치안 용도 전용 가능한 경우 상황허가(캐치올) 심사 대상 검토

계약서에 비군사 용도 명시 및 최종 용도, 최종 사용자 확인

④ 의료용 AI SW

의료용 SW는 수출통제 비해당이나 감시·보안 기능 탑재 시 검토 필요

의료용 한정 표시 및 비군사 용도 증빙 첨부

⑤ 공동연구 중 AI 소스 코드 교환

기본적으로 기술 이전에 준하는 것으로 전략 기술 허가 가능성 검토

NDA 교환, 기술 이전 허가 등 검토

표 24 AI SW 품목의 수출통제 대상 판단 시 주요 고려 사항

구분	확인 대상	검토 내용	관련 근거	고려 사항
사용 용도	- 군사·보안·전략 목적 전용 가능성 - 대규모 식별·추적 기능 여부	- 최종 용도 증빙 서류 기반 수출 허가(상황허가) 심사	- 「전략물자수출입고시」 제 54 조(상황허가, 캐치올(catch-all) 규정) - 별표 2 의 2	- 군사·보안 목적 전용 가능성 AI SW 또는 감시 시스템은 전략물자 비해당이라도 상황허가 대상 가능성 - 제품 설계 단계에서 군사·감시 기능 없는 경우 문서화 - 계약서에 재수출 금지조항 및 용도 제한 조항 삽입
수출 대상 국가	- 수출 지역	- "가" 지역 국가(화이트리스트) 이외 국가 수출 시 허가 대상	- 「전략물자수출입고시」 별표 6 (전략물자 수출지역 구분) - 별표 2 의 2 - 산업부 통상안보정책관실 지침	- 우려 국가 거래 시 최종사용자·재수출 조건 등 검증 - 수출 대상 국가 리스크 평가 체계 구축 - 대중국 AI 가속기 및 AI SW 수출에 대한 사전허가 심사 강화 추세
최종 사용자	- 최종 사용자	- 최종 사용자 증빙 서류 기반 수출 허가 심사	- 「전략물자수출입고시」 제 7 조(최종사용자 확인)	- 고객 확인 및 최종 사용자 진술 필수 - EUC 및 재수출 조건 관리 - EUC 및 고객확인서 5 년 보관 - 우려 거래 대상자 조회 및 확인
미국 FDPR	- 개발/설계 시 미국 기술, 장비, SW 사용 여부	- 미국 기술, 장비, SW 사용 여부 및 정도 확인	- 미국 EAR — 15 CFR (Code of Federal Regulations) Part 734	- 미국 기술 포함 제품·SW 는 해외 제조 시에도 FDPR 적용 가능성 - 관련 품목의 제재 대상국 이전 시 최종 사용자·최종 용도·재수출 가능성 등 검증 필요 - 계약서상 미국 수출통제 조항(EAR/FDPR 준수) 명시 및 내부 컴플라이언스 문서 기록
기술이전		- AI 모델의 가중치,	- 「대외무역법」 제 24 조(기술의 수	- AI 모델의 가중치, 알고리즘 소스코드 등 해

구분	확인 대상	검토 내용	관련 근거	고려 사항
	- AI 모델 가중치, 알고리즘, 소스코드 등	소스코드 등이 전략 기술인지 여부 - 미국 FDPR 조항 해당 여부	출 허가) - 산업부 기술수출 심사 지침 (2023 개정)	외 이전 시 전략 기술 여부 검토 - 모델 가중치, 데이터 전송 시 암호화 및 접근 기록 보관
SW 품목의 서비스 형태	- 클라우드, SaaS	- 암호화 기능 포함 등 SW 통제 대상 해당 여부	- 별표 2	- 암호화 기능 포함 등 통제 대상 해당 시 클라우드/SaaS SW/서비스도 전략물자 해당 가능성

표 25 AI SW의 특성/기능별 분류 및 수출통제 대상과의 연관성

특성/기능 구분	주요 내용	관련 품목 예	주요 점검 사항	관련 통제 조항
(1) 암호화	암호화 알고리즘, 모듈, 기능	- 보안 AI 프레임워크 - 암호화 기능 포함 SW	- 고성능 대칭/비대칭 암호화 기능 포함 여부	5A002, 5D002, 5E002
(2) AI 연산 인프라	고성능 AI 컴퓨팅	- LLM 학습용 GPU 서버, AI 슈퍼컴퓨터 - AI HW 용 드라이버/런타임/파이프라인 SW	- 고성능 컴퓨팅 HW(4A003) 연계 SW 여부 - 고성능 AI 전용 컴퓨팅 HW(4A090) 관련/전용 설계 SW 여부	4A003, 4A090, 4D001, 4D090, 4E001
(3) AI 모델 학습	AI 모델/프레임워크	- AI HW 용 드라이버/컴파일러/오케스트레이션/프레임워크	- 고성능 컴퓨팅 HW(4A003) 연계 SW 여부 - 고성능 AI 전용 컴퓨팅 HW(4A090) 연계 여부 - 범용 SW 프레임워크의 전용 설계 여부	4D0001, 4D090, 4E001
(4) AI 응용	AI 분석, 생성 응용 기술	- 영상·음성 인식, 생성형 AI 등	- 고성능 컴퓨팅(4A003) 연계 SW 여부 - 고성능 AI 전용 컴퓨팅 HW(4A090) 의존 여부	4A003, 4A090, 4D001, 4D090, 4E001, 6A001~6A008, 6D001~6D003, 6E001~6E003
(4-1) 음성 인식·합성	음성 데이터 분석, 생성	- AI 음성 분석, 합성, 생성 시스템	- 고성능 컴퓨팅 연계 여부 - 고성능 AI 전용 컴퓨팅 HW(4A090) 의존 여부 - 국가/지역, 최종사용자, 사용용도 검토	4A003, 4A090, 4D001, 4D090, 4E001
(4-2) 영상 분석·생성	영상 처리, 인식, 생성	- 위성·드론 영상 분석 AI	- 고성능 컴퓨팅 연계 여부	4A003, 4A090, 4D001, 4E001,

특성/기능 구분	주요 내용	관련 품목 예	주요 점검 사항	관련 통제 조항
		- 얼굴 인식/감시 AI	- 고성능 AI 전용 컴퓨팅 HW(4A090) 의존 여부 - 국가/지역, 최종 사용자, 최종 용도 검토	6A001~6A008, 6D001~6D003, 6E001~6E003
(4-3) 자연어 처리	언어 처리, 분석, 생성	- AI 언어 번역, 분석, 생성 시스템	- 고성능 컴퓨팅 연계 여부 - 고성능 AI 전용 컴퓨팅 HW (4A090) 의존 여부 - 국가/지역, 최종 사용자, 최종 용도 검토	4A003, 4A090, 4D001, 4E001
(4-4) 추천·데이터 마이닝	대규모 데이터 분석	- AI 추천·행동패턴 분석 시스템	- 고성능 컴퓨팅 연계 여부 - 고성능 AI 전용 컴퓨팅 HW(4A090) 의존 여부 - 국가/지역, 최종 사용자, 최종 용도 검토	4A003, 4A090, 4D001, 4E001
(5) AI 자율주행/로보틱스	자율주행/로봇용 AI 제어 및 항법 기술	- AI 자율 주행 제어, 인지, 경로 결정, 항법, 추진 제어 기술	- 고성능 센서, 영상 장치 등 융합 여부 - 최종 사용 목적 검토 - 군사/보안용 캐치올·국가별 허가 가능성 검토	6A001~6A008, 7A001~7A004, 8A001, 8A002, 9A001, 9A002, 9A007, 6D001~6D003, 7D001~7D004, 8D001~8D002, 9D001, 9D002, 9D004, 9D005, 6E0001~6E003, 7E0001~7E004, 8E001~8E003, 9E001~9E003
(6) AI 네트워크 감시/분석/보안	네트워크 감시, 분석, 보안	- 심층 패킷 분석 기반 AI 보안 분석 시스템	- 네트워크 트래픽 심층 분석/침입용 여부	4A005, 5A001.j, 4D004, 5D001.c, 4E001, 5E001

특성/기능 구분	주요 내용	관련 품목 예	주요 점검 사항	관련 통제 조항
(6-1) 네트워크 감시·분석	네트워크 트래픽 모니터링, 패킷분석	- AI 네트워크 트래픽 감시 시스템	- 네트워크 트래픽 심층 분석 여부	5A001.j, 5D001.c, 5E001
(6-2) 보안/침투	침입 탐지 및 공격 자동화	- AI 침입 테스트·보안 시스템	- 침입용 SW 관련 여부	4A005, 4D004, 4E001
(7) 군사 감시/정찰 AI	위성·드론 영상 기반 표적 탐지·식별 기술	- SAR·IR 등 영상 인식, AI 표적 추적	- 군사용/감시 정찰 여부	6A001~6A003, 6D001~6D003, 6E001~6E003
(8) 바이오/의료 AI	생체신호 분석, 의료용 AI	- 질병 예측, AI 영상 판독 등	- 통상 비해당 - 엔드유즈 중심 관리	6A001~6A003, 6D001~6D003, 6E001~6E003

7.2.2. AI SW 수출통제 품목 판정 가이드라인

- AI SW 관련 기업이 다양한 AI 품목의 수출통제 대상 여부 판단에 필요한 주요 체크 사항 및 판정 가이드라인을 다음과 같이 제시함(표 26, 부록 3. AI SW 수출 통제 가이드라인 참조)

(1) 품목의 최종 용도/수출 대상 국가/최종 사용자 검토

- 최종 용도
- 수출 대상 국가
- 최종 사용자

(2) 품목의 미국 FDPR 대상 여부 검토

(3) 품목 분류 및 통제 대상 해당/비해당 여부 검토

- 암호화 기능
- 고성능 컴퓨팅 HW 연동
- 네트워크 감시, 분석
- 침입 SW
- 고성능 센서/영상 장치 연계
- 자율주행/로보틱스
- 전략 기술 등

(4) 상황허가 대상 해당/비해당 여부 검토

표 26 AI SW 품목의 수출통제 대상 검토 체크 사항

구분	점검 항목	세부 검토 사항	예/아니오(☑)	비고 / 근거
① 사용 용도	군사·보안 전용 가능성 포함	SW가 군사·보안 목적(감시·정찰·사이버보안 등)에 사용될 가능성이 있는가?	□ 예 □ 아니오	End-Use 심사 대상
	대규모 식별·추적 기능 포함	SW가 얼굴·행동 식별 또는 추적 등 보안 감시 기능을 내장하고 있는가?	□ 예 □ 아니오	상황허가 - 캐치올(Catch-All) 적용 가능
② 수출 대상 국가	우려 국가 거래	"가" 지역 국가(화이트리스트) 이외 우려 국가와 직·간접 거래가 있는가?	□ 예 □ 아니오	수출 국가 통제 연동
	재수출 가능성 검토	품목이 다른 국가로 재수출·재이전될 가능성이 있는가?	□ 예 □ 아니오	최종사용자 진술서(EUC) 확보
③ 최종사용자	최종사용자 확인	최종사용자가 군·정보기관 또는 제재 리스트(우려거래 대상자)에 해당하는가?	□ 예 □ 아니오	OFAC·UN 리스트, 우려 거래 대상자 리스트 등 참조
	최종사용자 진술서(EUC) 보유	EUC 및 재수출 금지 조항이 계약에 포함되어 있는가?	□ 예 □ 아니오	계약 검토 대상
④ FDPR	FDPR 적용 여부	제품이 미국 기술, 장비, SW를 사용하여 개발, 설계되었는가?	□ 예 □ 아니오	미국 EAR 기준 적용
⑤ 암호화 기능	암호화 HW 특성 보유	SW가 암호화 기능을 포함하는 HW와 같은 암호화 특성을 갖는가?	□ 예 □ 아니오	5D002 가능성 검토
	암호화 SW 기능 수행	SW가 종단간(E2E) 암호화 등 암호화 기능을 수행하는가?	□ 예 □ 아니오	5D002 가능성 검토
⑥ 고성능 컴퓨팅 HW 연동	고성능 컴퓨팅 HW(4A003) 연동	SW가 슈퍼 컴퓨터/고성능 컴퓨터(4A003)와 연동되도록 설계되었는가?	□ 예 □ 아니오	4D001 가능성 검토
	고성능 AI 컴퓨팅 HW(4A090) 연동	SW가 고성능 AI 컴퓨터/가속기 전용으로 설계(specially designed) 되었는가?	□ 예 □ 아니오	미국 4D090 가능성 검토

	전용 설계 구성요소 확인	SW가 드라이버·컴파일러·클러스터·오케스트레이션 등 전용 설계 구성 요소인가?	□ 예 □ 아니오	전용 설계 검토 대상
	학습·추론 성능 향상 검토	SW에 모델 병렬화, 파이프라인 처리, TPP 향상 등 학습·추론 성능 향상 기술이 탑재되어 있는가?	□ 예 □ 아니오	고성능 컴퓨팅 연관 4D001/4D090 가능성 검토
⑦ 네트워크 감시, 분석	네트워크 분석/모니터링	심층 패킷 분석 등을 통해 네트워크 트래픽을 분석 및 모니터링하는가?	□ 예 □ 아니오	5A001.j/5D001.c 가능성 검토
	네트워크 감시/정보 취득	SW가 네트워크 트래픽을 감시해서 메타데이터 등 정보를 취득하는가?	□ 예 □ 아니오	5A001.j/5D001.c 가능성 검토
⑧ 침입 SW	침입 SW 탑재	공격·취약점 탐색 또는 침입 기능이 내장되어 있는가?	□ 예 □ 아니오	4A005/4D004 가능성 검토
	침입 도구 연계	외부 해킹 도구·취약점 테스트 모듈과 연계되어 있는가?	□ 예 □ 아니오	4A005/4D004 가능성 검토
⑨ 고성능 센서 연계	센서·레이더·광학 데이터 연동	SW가 고성능 센서·레이더·광학 장치의 센싱 데이터를 처리, 분석하는가?	□ 예 □ 아니오	6A/6D 가능성 검토
	군사 감시 응용	위성·드론 영상 분석, 표적 추적 기능 등이 포함되어 있는가?	□ 예 □ 아니오	상황허가 - 캐치올(Catch-All) 적용 가능
⑩ 자율주행/로보틱스	자율주행/로봇 제어/인지	자율주행(육상/해상/공중)이나 로봇의 제어나 인지 기능을 수행하는가?	□ 예 □ 아니오	6A~9A/6D~9D 가능성 검토
	자율주행/로봇 경로 결정/항법	자율주행(육상/해상/공중)이나 로봇의 경로 결정이나 항법 기능을 수행하는가?	□ 예 □ 아니오	6A~9A/6D~9D 가능성 검토
⑩ 전략기술	AI 모델 가중치(Weights) 등 이동	AI 모델 가중치·데이터셋 등을 이전하는가?	□ 예 □ 아니오	전략기술 가능성 검토
	전략기술(소스 코드 등) 제공	전략기술 관련 소스코드·알고리즘 등을 제공·공유하는가?	□ 예 □ 아니오	전략기술 가능성 검토

VIII 결론

제8장 결론

- 본 보고서에서는 WA 국제체제, 미국, 유럽, 일본 등 국가의 독자 통제 체제의 특징과 변화를 알아보고, 각국의 주요 통제 대상 품목과 통제 기준을 살펴보았음. 다양한 AI 기반 품목을 전략물자 통제 가능성 측면에서 8개로 분류하고, 관련되는 주요 국내외 전략물자 통제 대상 품목과 판정 사례 등을 분석하였음. 이를 통해 AI SW 품목의 WA 국제체제 및 각국의 독자 통제 체제하에서의 통제 기준과 방향을 고찰하였음.

- 그리고, 이러한 통제 기준 방향 설정을 기반으로 수출통제 관련 정책적 측면과 관련 기업 측면에서 필요한 대응 방향과 주요 고려 사항, 통제 대상 판정용 체크사항, 판정 가이드라인 등을 도출하였음. 정책적으로는 수출통제 제도 관련 인식 제고, AI 품목 특화 분류체계 도입, 수출판정 제도 및 절차의 고도화, 다자체제·동맹국 등 국제공조 강화 등의 대응을 고려할 수 있음. 기업 측면에서는 AI SW 품목의 효과적인 통제 대상/비대상 구분, 제품과 통제 대상간의 매핑, 제품 사이클 전단계(개발, 계약, 판정, 허가, 수출, 사후 관리 등)에서의 수출통제 관리 프로세스의 수립 및 운영 등의 대응을 고려할 수 있음.

- AI 기술은 정보 분석, 정보 생성 및 융합, 자율 이동, 전략 수립 등 다양한 기능을 수행하는 핵심 디지털 기반 기술로, 산업·사회·경제 전반에 걸쳐 파급력이 확대되고 있음. 특히 초거대 언어 모델, 자율주행 및 로보틱스, 영상·언어 기반 인텔리전스 기술은 국가 기간산업, 공급망 효율화, 신약 개발, 국방·보안 분야까지 활용 범위가 확장되고 있어 AI 기술 개발과 선도는 곧 국가 경쟁력 확보와 직결되고 있는 상황임.

- 이러한 기술적 확장성은 동시에 군사·보안적 민감성을 높여, 의도치 않은 군사적 오용 가능성, 감시·정찰 기능 전용 가능성을 내포하고 있어 WA 국제체제 및 각국 독자 통제체제에서는 AI 기반 품목의 민간용·군용 이중용도 특성에 주목하여 통제 기준의 고도화를 추진하고 있음. 따라서 AI 기술의 특성과 글로벌 규제 환경 변화에 대응하기 위해, AI 산업 육성과 기술안보 전략을 병행하는 균형 있는 접근이

필요할 것으로 보임.

- 국내 기업은 글로벌 시장 진출 과정에서 국내 수출통제 체제 뿐만 아니라 미국, 유럽, 일본 등 복수의 수출통제 체제를 고려하고 관리하는 것이 필요하며, 이를 기업 전략 및 기술 개발 등과 함께 전반적으로 관리하는 통합 관리 차원의 접근이 요구됨. 또한 기업은 제품 개발 초기 단계에서부터 통제 가능성이 있는 기능을 구조적으로 식별하고, 이를 위한 판정 및 관리 프로세스를 체계화함으로써 기술안보 리스크를 최소화하고 글로벌 컴플라이언스에 부합하면서, AI 산업 발전을 선도해 나갈수 있을 것으로 판단됨.

부록 1 기업 대상 인터뷰

부록 1. 기업 대상 인터뷰

2025 AI 기반 품목의 전략물자 통제 관련 인터뷰
한국인공지능·소프트웨어산업협회(KOSA)

안녕하십니까?
KOSA에서는 최근 인공지능(AI) 관련 HW, SW, 기술 등 다양한 품목의 확대 및 수출과 관련하여, 관련 품목이 전략물자에 해당할 가능성이 있는지를 선제적으로 파악하고, 필요한 제도 및 지원 방안 수립에 활용하고자 합니다. 본 인터뷰에서는 귀사에서 개발, 생산, 판매하는 HW, SW, 기술 등의 품목이 AI 기술과 관련이 있는지, 전략물자에 해당할 가능성이 있는지 등에 대해 문의드리고자 하니, 성심껏 답변해 주시면 감사하겠습니다.

1. 배경

○ 인공지능(AI) 기술의 산업용/군용 응용 확산 및 기술 고도화

- 정보 분석, 영상 분석, 자율 주행, 생명공학 등
- 전략/전술 통제 시스템, 자율 이동 및 무기 체계 등

○ AI 기술의 국제 무역 및 국가 안보 영향력 확대

○ AI 관련 품목(HW, SW, 기술)의 수출통제 및 관리 필요성 증대

○ 미국, 유럽, 일본, 중국 등의 AI 기술 독자 통제 대상과 범위 강화

○ AI 관련 품목의 전략물자 관련 인식 제고 및 통제 가능성 분석

2. 인터뷰 내용

2-1. 기술 및 제품 현황

[1] 귀사의 AI 관련 품목(HW, SW, 기술)은 무엇이며, 주로 어떤 용도로 활용되고 있습니까?

[2] AI 관련 품목이 수출되거나 해외에 이전/제공되는 경우가 있다면 주요 대상

국가나 지역은 어디입니까?

2-2. 전략물자 판정 경험

[3] AI 관련 품목에 대해 전략물자 판정 신청 후 해당/비해당 판정(사전판정 또는 자가판정)을 받은 경험이 있거나, 계획이 있으십니까?

[4] AI 관련 품목에 대해 자체적으로 전략물자 해당 여부를 검토하거나 외부 자문을 받은 적이 있거나, 계획이 있으십니까?

[5] AI 관련 품목의 전략물자 판정이나 수출통제 전체 과정에서 가장 어려웠던 점은 무엇이었습니까?

[6] AI 관련 품목의 전략물자 해당 여부 판정 기준이 명확하지 않다고 느꼈던 경험이 있으신가요?

[7] 위 [6]에 해당된다면 어떤 부분에서 그렇게 느끼셨습니까?

2-3. 제도 인식 및 대응

[8] WA(Wassenaar Arrangement), EAR(Export Administration Regulations) 등 해외 수출통제 제도에 대한 이해는 어느 정도라고 생각하십니까?

[9] 회사 내에 전략물자 판정 및 규제 대응을 위한 전담 부서, 인력 또는 프로세스가 갖추어져 있습니까?

2-4. 제도 관련 의견

[10] AI 관련 품목의 특성(소프트웨어, 모델, API, 클라우드, SaaS 등)을 고려하여 기존의 전략물자 판정/통제 제도와 다른 형태의 제도가 필요하다고 보십니까?

[11] AI 관련 품목의 전략물자 판정 제도나 기준과 관련해 바라는 점이 있다면 무엇입니까?

부록 2 기업 대상 설문조사

부록 2. 기업 대상 설문조사

2025 AI 기반 품목의 전략물자 통제 관련 인터뷰
한국인공지능·소프트웨어산업협회(KOSA)

안녕하십니까?
KOSA에서는 최근 인공지능(AI) 관련 HW, SW, 기술 등 다양한 품목의 확대 및 수출과 관련하여, 관련 품목이 전략물자에 해당할 가능성이 있는지를 선제적으로 파악하고, 필요한 제도 및 지원 방안 수립에 활용하고자 합니다. 본 설문에서는 귀사에서 개발, 생산, 판매하는 HW, SW, 기술 등의 품목이 AI 기술과 관련이 있는지, 전략물자 판정 경험이 있거나 판정 계획이 있는지 등에 대해 문의드리고자 하니, 성심껏 답변해주시면 감사하겠습니다.

1. 배경

○ 인공지능(AI) 기술의 산업용/군용 응용 확산 및 기술 고도화

- 정보 분석, 영상 분석, 자율 주행, 생명공학 등
- 전략/전술 통제 시스템, 자율 이동 및 무기 체계 등

○ AI 기술의 국제 무역 및 국가 안보 영향력 확대

○ AI 관련 품목(HW, SW, 기술)의 수출통제 및 관리 필요성 증대

○ 미국, 유럽, 일본, 중국 등의 AI 기술 독자 통제 대상과 범위 강화

○ AI 관련 품목의 전략물자 관련 인식 제고 및 통제 가능성 분석

2. 설문 조사 내용

2-1. 기본 정보

(1) 귀사의 업종 분류는 무엇입니까?
① 하드웨어 개발 ② 소프트웨어 개발 ③ 시스템 개발/통합
④ 데이터 분석 ⑤ 기타 ( )

(2) 귀사는 다음 중 어디에 해당합니까?
① 대기업 ② 중견기업 ③ 중소기업 ④ 스타트업

(3) 귀사의 주력 제품 또는 서비스 유형을 선택해 주십시오. (복수 선택 가능)
① AI 기반 HW(반도체 칩 등) ② AI 기반 SW
③ AI 모델(LLM, LVM 등) ④ AI API/SasS 등
⑤ AI 응용 시스템 ⑥ 클라우드 플랫폼
⑦ 자율 시스템(로봇, 드론 등) ⑧ 영상/음성/생체 인식 시스템
⑨ AI 보안 솔루션 ⑩ AI 감시/탐지 시스템
⑪ 기타 ( )

2-2. AI 기술 보유 여부

(4) 귀사는 AI 관련 기술을 보유하고 있습니까?
① 예 ② 아니오

(5) 보유하고 있다면, 다음 중 어떤 형태입니까? (복수 선택 가능)
① AI 칩 제조 기술 ② AI 칩 설계 기술
③ AI SW 기술 ④ AI 모델 기술
⑤ AI 모델 기반 응용 기술 ⑥ 클라우드/SaaS/IaaS/PaaS 기술
⑦ 자율 시스템 기술 ⑧ 영상/음성/생체 인식 기술
⑨ AI 보안 기술 ⑩ AI 감시/탐지 기술
⑪ 기타 ( )

2-3. 전략물자 인식 및 판정 경험

(6) 전략물자 제도(전략물자 판정, 수출통제 제도 등)에 대해 알고 계십니까?
① 매우 잘 알고 있다 ② 어느 정도 알고 있다
③ 들어본 적은 있다 ④ 전혀 모른다

(7) 귀사의 AI 관련 제품/기술에 대해 전략물자 사전판정 또는 자가판정을 진행한 **<u>경험이 있습니까</u>**?
① 예, 있다 ② 아니오, 없다 (→ 12번으로 건너뛰기)

(8) 어떤 품목(또는 기술)에 대해 판정을 **<u>요청하셨습니까</u>**? (복수 선택 가능)
① AI 기반 HW(반도체 칩 등) ② AI 기반 SW
③ AI 모델(LLM, LVM 등) ④ AI API/SasS 등

⑤ AI 응용 시스템 ⑥ 클라우드 플랫폼
⑦ 자율 시스템(로봇, 드론 등) ⑧ 영상/음성/생체 인식 시스템
⑨ AI 보안 솔루션 ⑩ AI 감시/탐지 시스템
⑪ 기타 ( )

(9) **해당 품목은** 암호화(대칭, 비대칭) 기능을 포함하고 있습니까?(예: AES, PKI 등)
① 예 ② 아니오 ③ 잘 모르겠음

(10) 판정 결과는 어떻게 **나왔습니까**?
① 전략물자/기술 해당 ② 전략물자/기술 비해당 ③ 기억나지 않음

(11) 해당일 경우 판정 번호는 어떻게 **나왔습니까**?(예: 5D002.c.1, 5E002.a 등)

(12) 향후 귀사의 AI 관련 제품/기술에 대해 전략물자 사전판정 또는 자가판정을 진행할 **계획이 있습니까**?
① 예, 있다 ② 아니오, 없다 (→ 17번으로 건너뛰기)

(13) 어떤 품목(또는 기술)에 대해 판정을 요청하실 **계획입니까**? (복수 선택 가능)
① AI 기반 HW(반도체 칩 등) ② AI 기반 SW
③ AI 모델(LLM, LVM 등) ④ AI API/SasS 등
⑤ AI 응용 시스템 ⑥ 클라우드 플랫폼
⑦ 자율 시스템(로봇, 드론 등) ⑧ 영상/음성/생체 인식 시스템
⑨ AI 보안 솔루션 ⑩ AI 감시/탐지 시스템
⑪ 기타 ( )

(14) **해당 향후 예상 품목은** 암호화(대칭, 비대칭) 기능을 포함하고 있습니까? (예: AES, PKI 등)
① 예 ② 아니오 ③ 잘 모르겠음

(15) 판정 결과는 어떻게 나올 것으로 **예상하십니까**?
① 전략물자/기술 해당 ② 전략물자/기술 비해당 ③ 잘 모르겠음

(16) 해당으로 예상하실 경우 판정 번호는 어떨 것으로 **예상하십니까**?(예: 5D002.c.1, 5E002.a 등)

2-4. 제도 관련 인식

(17) AI 관련 품목의 전략물자 판정 제도에 대해 다음 중 귀하의 생각에 가까운 항목을 골라주십시오.

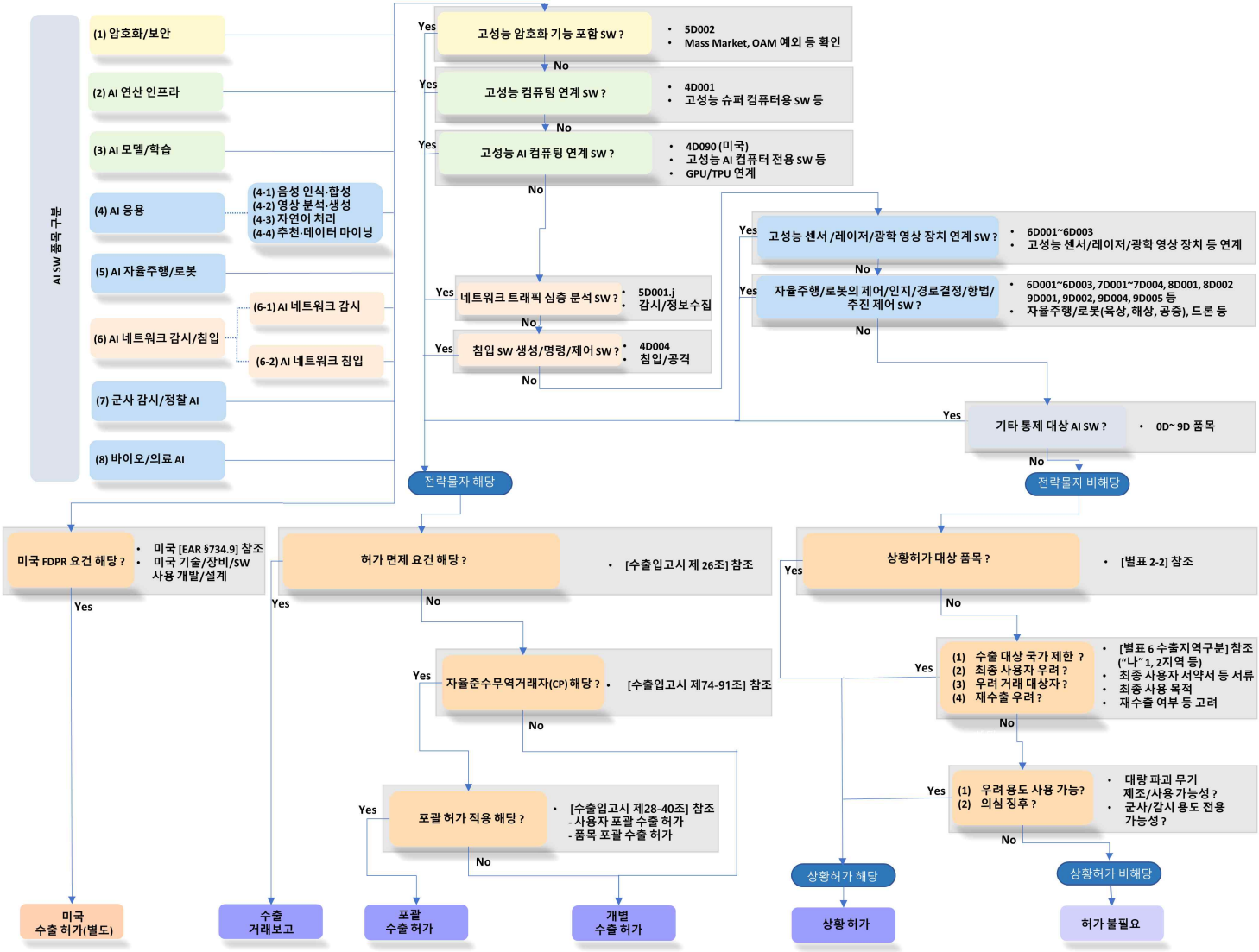
- AI 관련 품목의 전략물자 판정 기준이 명확하다:
  ① 그렇다 ② 보통이다 ③ 모호하다 ④ 불명확하다

2-5. 기타 의견

(18) AI 관련 품목의 전략물자 판정 및 관리 제도를 위해 바라는 점이 있다면 자유롭게 적어주십시오. (서술형)

부록 3 AI SW 수출통제 대상 판정 가이드라인

부록 3. AI SW 수출통제 대상 판정 가이드라인



참고문헌

[참고문헌]

[1] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, 2016.
[2] European Commission, Ethics Guidelines for Trustworthy AI, 2021.
[3] Google Cloud, "AI and Machine Learning Products." Available: https://cloud.google.com/ai
[4] Amazon Web Services, "Machine Learning on AWS." Available: https://aws.amazon.com/machine-learning/
[5] Microsoft Azure, "Azure AI Services." Available: https://azure.microsoft.com/en-us/products/ai-services/
[6] Y. You et al., "Large batch optimization for deep learning: Training BERT in 76 minutes," arXiv:1904.00962, 2019.
[7] R. Rajbhandari et al., "ZeRO-Infinity: Breaking the GPU memory wall for extreme scale deep learning," SC '21, 2021.
[8] SchedMD, Slurm Workload Manager Documentation, 2023. https://slurm.schedmd.com
[9] OpenMPI Project, Message Passing Interface (MPI) Standard, Version 4.0, 2021.
[10] NVIDIA, NVIDIA NCCL: Collective Communication Library, 2023. https://developer.nvidia.com/nccl
[11] M. Abadi et al., "TensorFlow: A system for large-scale machine learning," OSDI 2016, pp. 265–283.
[12] A. Paszke et al., "PyTorch: An imperative style, high-performance deep learning library," NeurIPS 2019.
[13] J. Bradbury et al., JAX: Composable transformations of Python+NumPy programs, 2018. https://github.com/google/jax
[14] T. Wolf et al., "Transformers: State-of-the-art natural language processing," EMNLP 2020: System Demonstrations, pp. 38–45.
[15] A. Sergeev and M. Del Balso, "Horovod: fast and easy distributed deep learning," arXiv:1802.05799, 2018.
[16] NVIDIA, CUDA C Programming Guide, 2023.
[17] K. Bonawitz et al., "Towards federated learning at scale: System design," MLSys, pp. 374–388, 2019.
[18] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," ACM CCS, pp. 1310–1321, 2015.
[19] Bureau of Industry and Security (BIS), Export Administration Regulations (EAR), Parts 730–774, 2023.

[20] BIS, Export Controls on Advanced Computing and Semiconductor Manufacturing Items to the PRC, Oct. 2022.
[21] Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List, 2023.
[22] Wassenaar Arrangement, Guidelines & Procedures Including the Initial Elements, 2023.
[23] BIS, Addition of ECCN 4E091, Federal Register, Oct. 2023.
[24] BIS, Removal of ECCN 4E091; Revisions to Controls on Advanced Computing, Federal Register, Oct. 2024.
[25] BIS, Export Controls on Advanced Computing and Semiconductor Manufacturing Items to PRC, Federal Register, Oct. 2022.
[26] BIS, "Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery," EAR 0Y521, Federal Register, Jan. 2019.
[27] Congressional Research Service, Export Controls: Key Challenges, 2020.
[28] The Verge, "AI art tool Stable Diffusion is now publicly available," Aug. 2022.
[29] Wassenaar Arrangement, Public Documents Vol. IV: Background and Plenary Statements, Dec. 2023.
[30] M. Beck, The Devolution of Export Controls: The Wassenaar Arrangement in Crisis, Strategic Trade Research Institute, 2023.
[31] BIS, Additional Export Controls: Advanced Computing and Semiconductor Items, Federal Register, Oct. 13, 2022.
[32] White House, Fact Sheet: Implementation of Export Controls on Advanced Computing to PRC, Oct. 7, 2022.
[33] BIS, Export Controls on Semiconductor Manufacturing Items, Federal Register, Oct. 17, 2023.
[34] The Wall Street Journal, "U.S. Weighs New Rules to Curb China's Access to Cloud Computing," Mar. 2024.
[35] Wilmer Hale, BIS Issues Long-Awaited Export Controls on AI, Feb. 2025.
[36] The Wall Street Journal, "Biden Administration Considers New Limits on U.S. Investment in Chinese AI Firms," Apr. 2024. ← 중복 교체
[37] Reuters, "US eases AI export rules for allies, tightens curbs on China and Russia," Oct. 2024.
[38] Bruegel, The EU AI Act: A landmark in digital regulation, 2024.
[39] European Commission, EU Dual-Use Export Controls — FAQs and Guidance Note, 2022.
[40] METI Japan, Export Control on Advanced Semiconductor Manufacturing

Equipment, May 2023.
[41] Government of the Netherlands, New Export Control Measures for Advanced Semiconductor Equipment, June 2023.
[42] McKinsey & Company, The State of AI in 2023, 2023.
[43] Stanford HAI, AI Index Report 2023, 2023.
[44] Wassenaar Arrangement, Statement of Understanding on Export Controls for Intrusion Software, 2022. ← 중복 교체
[45] OpenAI, GPT-4 Technical Report, arXiv:2303.08774, 2023.
[46] Stanford HAI, AI Index Report 2024, 2024.
[47] CSET, Export Controls in the Age of AI, 2022.
[48] BIS, Framework for AI Diffusion: Export Controls on Certain AI Model Weights, Federal Register, Jan. 2025.
[49] CSIS, Balancing National Security and Innovation: U.S. AI Export Control Policy, 2025.
[50] CSIS, The Future of AI Export Controls: Hardware to Models and Data, 2024.
[51] Carnegie Endowment, Toward Multilateral Cooperation on AI Export Controls, 2024.
[52] Carnegie Endowment, Toward Multilateral Cooperation on AI Export Controls, 2024.
[53] CSIS, Next-Generation Export Controls on AI Hardware, 2024.
[54] CSIS, AI Export Controls: From Hardware FLOPS to Software Efficiency Metrics, 2024.
[55] CSIS, Regulating AI Services: Usage-Based Export Controls, 2025.
[56] U.S. Department of Commerce, Request for Comments: Potential Controls on Cloud and AI Services, Mar. 2024.
[57] CSIS, Controlling AI Models: Parameters, Performance, and Export Policy, 2025.
[58] CSET, AI Export Controls in the Age of Generative Models, 2024.
[59] CSIS, Understanding U.S. Allies' Legal Authority for AI and Semiconductor Export Controls, 2025.
[60] Wassenaar Arrangement, Best Practices for Effective Export Control Enforcement, 2023.
[61] BIS, Commerce Control List (CCL), Supplement No.1 to EAR Part 774, 2024 Revision.
[62] BIS, Export Administration Regulations (EAR), Parts 730–774, 2024.
[63] European Commission, EU Dual-Use Regulation (2021/821), Annex I —

Dual-Use Items, Consolidated 2024.
[64] European Commission, Updates to Annex I — EU Dual-Use Control List, OJEU, 2023/2024.
[65] METI Japan, List Controls under the Foreign Exchange and Foreign Trade Act, 2024.
[66] METI Japan, Security Export Control Handbook, 2024.
[67] 산업통상자원부, 전략물자 수출입고시(별표2 전략물자 분류기준), 2024.
[68] 무역안보관리원, 전략물자 판정 및 자율준수프로그램(ICP) 가이드라인, 2024.
[69] 무역안보관리원, 전략물자 통제 제도 운영 매뉴얼, 2023/2024.
[70] 홍연서, 김주원, 김지혜, 미 상무부, HBM 및 반도체 장비 통제강화 발표, Issue Report, 2024.12.
[71] 김주현, 美, AI 글로벌 확산 통제 조치 발표, 2025.1.
[72] 무역안보관리원, EU, 2025년 이중용도 수출 통제 목록, 무역안보24, 2025.9.
[73] BIS, Framework for Artificial Intelligence Diffusion, Federal Register, Vol. 90, No. 9, January 15, 2025.

본 보고서는 『AI 기반 품목의 전략물자 통제 기준 및 방향 분석』의 최종보고서입니다.

과학기술정보통신부
KOSA KOREA AI·SOFTWARE INDUSTRY ASSOCIATION 한국인공지능·소프트웨어산업협회
성균관대학교 SUNG KYUN KWAN UNIVERSITY(SKKU)