소프트웨어 / 모델 가중치 / 반도체 하드웨어 / 인류의 진보

수출 통제가 오픈소스 AI의 미래에 미치는 영향

Vikrant Rathore

코드와 가중치를 넘어 칩·메모리·초대형 클러스터 하드웨어까지 파고든 수출 통제가 오픈소스 AI와 인류의 미래를 어떻게 바꾸는가.



23

AI·반도체 관문

05

바이오의약

12

태양광 장비

일러스트 에디션 • 2026년 11월 2일

MOFCOM 48 / US EAR

수출 통제가 오픈소스 *AI*의 미래에 미치는 영향

Vikrant Rathore / CC BY-SA 4.0 Third-party materials retain their own copyrights and licenses. See NOTICE.

Jennifer Yuan, Vicky Ni, Ronak Rathore, Kanak Rathore
버전 2026-11-02
© 2026, Vikrant Rathore; original work CC BY-SA 4.0
2026-11-02
이 책은 GuideDog의 도움과 Jennifer Yuan, Vicky Ni, Ronak Rathore, Kanak Rathore의 조력으로 제작되었습니다.

차 례

01. 지식에 세관 부스가 세워진 날 9
어느 금요일 오후, 전혀 다른 두 개의 시계 9
나무 상자 하나 꾸리지 않고 국경을 넘는다는 것 10
모든 것을 바꾸는 네 가지 규제 용어 11
두 팀에 주는 의미 11

02. 마흔 개 통제 기술의 전체 지도 13
정부는 어떻게 하나의 아이디어를 자로 재는가 13
인계철선에 걸려 넘어지지 않고 조문을 읽는 세 가지 습관 14
인공지능, 반도체 칩 및 슈퍼클러스터 (23개 통제 지점) 14
바이오의약 및 유전자 플랫폼 (5개 통제 지점) 16
태양광 실리콘, 웨이퍼 및 공장 핵심 설비 (12개 통제 지점) 16
두 팀에 주는 의미 17

03. 지성과 실리콘: 모델과 칩, 클러스터를 지키는 관문 19
천연 발효종, 베이커리 창구, 그리고 무쇠 오븐 19
프런티어 모델을 가르는 세 개의 인계철선 (`266504X`) 20
데이터 레드라인(`266501J` 및 `266504X(1)`)과 자율 에이전트(`266505X` 및 `266502J`) 20
중국 AI 목록 속 하드웨어 계층: 반도체 칩, 메모리, 그리고 1만 장급 클러스터 21
두 팀에 주는 의미 21

04. 공개 모델: 공개와 비공개 이전 23
개방 라이선스는 공개의 일부 23
실제 파일에서 시작하기 23
중국: 현재 등록과 목록 초안 구분 24
미국: 별도 관할 검사 24
공개 모델에 가능한 영향 24
독립 검토와 한계 24
실용적인 공개 기록 25
두 팀에 주는 의미 25

05. 살아 있는 코드: 유전자 플랫폼과 공유되는 치료제 27
인쇄기는 지키되 그곳에서 찍어 낸 책은 세계와 나누다 27
미공개 생물학적 신규 표적과 생물안보의 성벽 28
두 팀에 주는 의미 28

06. 기계 속에 가둔 태양빛 29
태양광 패널은 실어 보낼 수 있어도 비밀 주방까지 내어 줄 수는 없다 29
주석 4: 물리적 기계 설비 그 자체 가 레시피일 때 30
두 팀에 주는 의미 30

07. 워싱턴의 문지기들: 실리콘 칩과 모델 가중치 31
전 지구적 연산의 물리적 엔진을 통제하다 31
2026년 1월 반도체 규정 개정: 문을 두드려 볼 자격을 준 것일 뿐 활짝 열린 문이 아니다 31
미국 AI 모델 가중치 규정(`4E091`)의 기묘한 법적 운명 32
워싱턴의 이웃한 두 관문: 벤처 투자 자금과 대량 민감 데이터 32
두 팀에 주는 의미 32

08. 두 개의 국경 체제와 공식 승인 획득 절차 33

하나의 프로젝트 안에서 마주치는 두 가지 통제 철학 33
단계별 실무 가이드: 공식 등록 및 승인 신청 방법 34
중국: 소관 정부 부처, 법정 처리 기한 및 검증된 연락처 35
미국: 소관 연방 기관, SNAP-R 업무 절차 및 검증된 연락처 36
두 팀에 주는 의미 37

09. 일상의 질문들: 독자를 위한 실전 현장 가이드 39
내 하드웨어에 딥시크(DeepSeek), 큐웬(Qwen) 등 오픈 모델을 계속 내려받아 써도 될까? 39
소프트웨어 라이선스가 MIT나 Apache 2.0이어도 하드웨어가 오픈소스 AI에 영향을 미치는가? 39
해외 사용자가 우리 AI 앱과 대화하거나 API를 호출하면 그것도 모델 수출인가? 39
연구소는 중국에 그대로 있는데 해외 투자자가 지배권을 인수한다면 등록해야 하는가? 39
공개 버튼을 누르기 전 두 장짜리 '릴리스 여권'에는 무엇을 기록해 두어야 할까? 40
여섯 가지 실전 시나리오 40

10. 1차 사료, 검증 방법론, 그리고 쉬운 용어 사전 43
이 책의 모든 사실은 어떻게 검증되었는가 43
일반 독자를 위한 쉬운 용어 사전 43
검증된 26개 1차 사료 전체 등록부 44
이번 검토에 추가한 연구·역사 자료 45
저자·협력자와 재사용 45
선택: 게임 예제 계산 확인 46
선택: 독립 검토는 안전을 보장하지 않는다 46

아이디어는 나누어도 소모되지 않습니다. Jefferson은 1813년 내 불로 촛불을 켜는 이는 나를 어둡게 하지 않고 빛을 얻는다 고 표현했습니다. 다른 팀의 지식을 빼앗지 않고 배울 수 있습니다. JEFFERSON



그림 1 두 연구팀이 협력하려 하지만 국경 장벽이 컴퓨터 부품과 기술 도면의 이동을 막습니다.

공개 가중치는 작은 조직에 통제권을 줄 수 있습니다. 병원·언어 사업·대학의 로컬 적응은 설명용 가능성이며 실제 임상 사례나 안전 증명이 아닙니다. 가중치 공개와 완전한 공개 AI 정의도 구별합니다. OSI R1 QWEN
모델 공유는 시작일 뿐입니다. 공유 지식을 유용한 도구로 만들려면 컴퓨터와 다른 팀에서 계속 배우는 길도 필요합니다.

소프트웨어와 가중치만이 아니다: 열린 지성을 떠받치는 하드웨어

모델은 코드와 학습된 숫자로 이동할 수 있습니다. 학습하고 실행하는 컴퓨터는 물리적 기계입니다. 공개 라이선스와 기계에 대한 접근은 문제의 다른 부분을 해결합니다.
모델에는 물리 컴퓨터가 필요합니다. 큰 학습은 첨단 칩·메모리·망을, 작은 모델은 보통 장비를 쓸 수 있습니다. 모두 최신 공정·만 장이 필요한 것은 아니지만 희소 장비 통제는 참여자를 바꿀 수 있습니다.

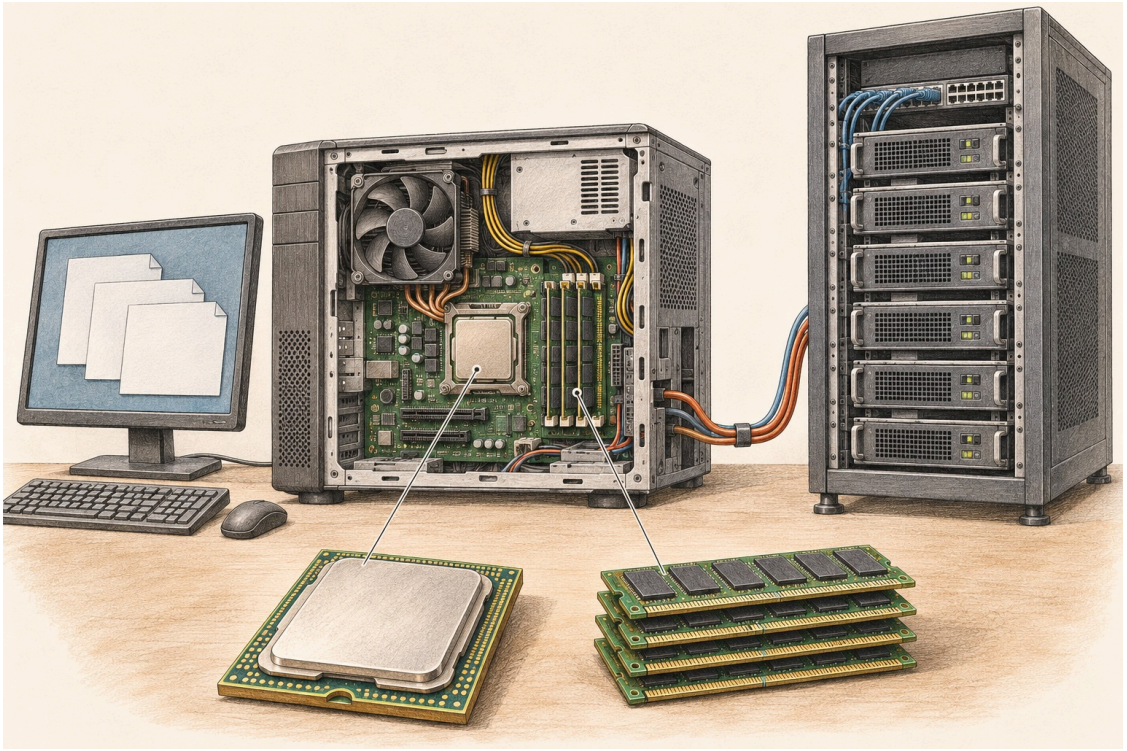


그림 2 공개 모델은 칩·메모리·계산 기반에 의존합니다. 일부 제한은 전체 접근에 영향을 줄 수 있습니다.

- **장비와 설계:** 미국은 조건부 특정 물품, 중국 제안은 특정 설계와 **1만 장 초과** 기술을 다룹니다. 지식·완성 칩·클러스터는 다른 대상입니다. US26 EAR734 EAR742 CN-A1
- **모델·데이터:** 중국 등록은 **2026년 10월 16일** 시작됐습니다. 계산·매개변수·적격 상위 평가는 대체 조건이며 제안·현재 등록·미국 규정은 별개입니다. CN48 CN-A1 US25 GAO26

> **중요**
> 공개 모델 사용 허가가 있어도 적절한 컴퓨터를 구하기 어려울 수 있습니다. 그래서 공유되는 지식과 이를 쓰는 하드웨어를 함께 살펴봅니다.

요새의 함정: 양쪽이 함께 잃는 구조

하드웨어 문제는 정책 문제로 이어집니다. 유용한 공개 모델은 여러 팀의 기여에 의존하지만 정부는 자국의 역량도 보호하려 합니다. 국익을 위한 선택이 어떻게 양쪽을 늦출 수 있을까요? 가상의 공동 작업대에서 따라가 봅니다.

두 팀, 같은 출발점

A국과 B국에 연구팀이 하나씩 있다고 가정합니다. 같은 공개 AI 모델을 일상적인 현지 언어 업무에 맞게 개선하려 합니다. A는 메모리를 덜 쓰는 방법을 찾고 B는 오류를 찾는 테스트를 개발하고 수정을 돕습니다. 실제 배포 사례가 아닌 가상의 팀과 기여입니다.

다음 개선을 교환하면 서로의 성과를 활용합니다. A는 더 나은 테스트를, B는 자원을 덜 쓰는 모델을 얻습니다. 양쪽 모두 컴퓨터, 인력과 시간이 필요합니다. 지식 공유는 자원 활용을 돕지만 하드웨어를 무료로 만들지는 않습니다.



그림 3 두 팀이 부품과 지식을 공유하면 컴퓨터를 완성하지만 벽으로 나뉘면 어려워집니다. 가정한 게임의 예시이며 실측 결과가 아닙니다.

각 정부의 두 가지 선택

정부가 다음 연구 단계의 정책을 정합니다. 자국의 유용한 발전을 원하지만 대가 없이 상대에게만 이익을 줄까 걱정합니다. 선택을 두 가지로 단순화합니다.

- **공유:** 팀의 일반적인 연구 개선을 교환하도록 허용합니다.
- **장벽:** 자국의 새로운 기여가 상대에게 전달되는 것을 광범위하게 제한합니다.

장벽은 미래의 기여를 다룹니다. 이미 공개된 모델 사본을 없앨 수는 없습니다. 시작 파일은 남지만 다음 개선은 서로에게 닿지 않을 수 있습니다. 실제 통제에는 특정한 제한과 허가 등 더 많은 선택이 있습니다. 먼저 이를 잠시 제외하고 유인 문제를 살펴봅니다.

네 가지 결말과 네 가지 점수

결과에 가상의 선호 점수를 붙입니다. 높을수록 이야기 속 정부가 선호하는 결과입니다. 유용한 발전, 보호와 상대적 우위에 대한 가정된 관심을 합친 것입니다. AI 시험 점수, 백분율이나 실측 국익이 아닙니다. 공고에 이 숫자가 제시된 것도 아닙니다.

양쪽 공유: 각각 17점. A의 메모리 개선이 B에, B의 테스트와 수정이 A에 전달됩니다. 모든 발견을 따로 반복하지 않고 발전합니다. 상호 협력의 좋은 결과를 각 17점으로 나타냅니다.

A 공유, B 장벽: A는 3점, B는 20점. B는 A의 새 공개 개선을 이용하면서 자기 기여는 보류합니다. B가 이 일방적 우위를 가장 선호한다고 가정하여 20점을 줍니다. A 정부는 상대가 보호하는 동안 혼자 공유하는 것을 가장 싫어한다고 가정하여 3점입니다. A 팀도 여전히 유용한 일을 합니다.3점은 이 예에서 정부가 가장 선호하지 않는 결과입니다.

A 장벽, B 공유: A는 20점, B는 3점. 역할이 바뀝니다. A가 일방적 우위를 얻고 B만 공유합니다. 현재 미국이나 중국을 어느 쪽에 대입하지 않고 전략 문제를 보기 위해 양국에 같은 가정의 우선순위를 줍니다.

양쪽 장벽: 각각 5점. 서로의 다음 기여를 받지 못합니다. 공개된 출발점에서 계속 일하지만 더 많이 반복하거나 유용한 개선을 포기합니다. 혼자 공유하기보다 자국 기여 보호를 선호한다고 가정하므로 5가 3보다 높습니다. 상호 고립보다 상호 협력을 선호하므로 17은 5보다 높습니다.

핵심 가정은 **20을 17보다 선호한다** 는 것입니다. 이번 단계에서 정부가 공동 발전보다 일방적 우위를 더 중시하며 제한의 유혹이 생깁니다. 공동 발전을 가장 중시하면 이 함정은 생기지 않을 수 있습니다. 숫자는 가정한 순서일 뿐 실제 정부의 선호를 증명하지 않습니다. GAME

게임 그림 읽기

A의 선택이 행을, B의 선택이 열을 정합니다. 만나는 칸에서 A 옆에는 A의 점수, B 옆에는 B의 점수가 있습니다. 오른쪽 위는 A 공유, B 장벽으로 A가 3, B가 20입니다. 초록은 상호 공유, 빨강은 상호 제한입니다.

가정한 선호 / 높을수록 선호

양쪽이 함께 잃는 구조



양쪽 모두 상호 장벽보다 공유를 선호합니다.

이 가정 아래에서만 장벽이 각자의 최적 대응입니다.

점수는 이야기의 선호이며 실측 효과가 아닙니다.

그림 4 두 팀의 네 결말입니다. 가상의 선호 점수이며 이 예에서는 높을수록 선호합니다.

장벽이 더 안전해 보이는 이유

A 정부는 B의 행동을 예상합니다. **B가 공유하면** A는 공유의 17점과 자기 기여 보류의 20점을 비교합니다. 가정에 따르면 일방적 우위를 위해 장벽을 선택합니다. 그림 왼쪽 열의 두 칸을 비교하는 것입니다.

B가 장벽을 세우면 A는 혼자 공유하는 3점과 자신도 제한하는 5점을 비교합니다. 이번에는 혼자 공유하지 않기 위해 다시 장벽을 고릅니다. 오른쪽 열의 두 칸을 비교합니다.

B도 똑같이 생각합니다. 상대가 무엇을 해도 자기 장벽이 합리적이라 여깁니다. 협력의 17점을 모두 선호하면서도 장벽을 선택해 각각 5점이 됩니다. 더 나쁜 공동 결과를 아무도 원하지 않아도 그런 결과가 생길 수 있습니다.
이것이 **죄수의 딜레마** 입니다. 결말은 **내시 균형** 이기도 합니다. 상대 장벽이 남으면 혼자 선택을 바꿔도 점수가 오르지 않습니다. A가 혼자 열면 5에서 3으로 내려갑니다. 공유하려면 양쪽이 바뀌거나 협력의 유인이 바뀌어야 합니다. GAME

수출 통제를 이해하는 데 주는 의미

이야기는 다음 장의 기술 항목 뒤에 있는 정책 질문을 제시합니다. 정부는 넓은 제한에서 보호나 협상력을 볼 수 있습니다. 그러나 양국 전체에서는 상호 보완적 개선을 끊고 일을 중복시키며 작은 팀의 연구를 어렵게 할 수 있습니다. 이는 조사할 작동 방식이며 가상 점수로 측정한 비용이 아닙니다.
실제 미중 통제는 대칭적인 양자택일 게임이 아닙니다. 역량과 법적 도구가 다릅니다. 신고, 금지, 일반 허가, 공개 정보 예외와 간소화 배포는 협력에 서로 다른 영향을 줍니다. 다음 장들에서 구분합니다. 모든 신고를 장벽이라거나 모든 예외를 완전한 이전 자유라 부르지 않습니다.
심각한 피해를 막는 특정 통제는 선호 순서를 바꿀 수도 있습니다. 공개 모델에는 이익과 악용 위험이 있습니다. 전면 공개나 광범위한 폐쇄를 자동 해답으로 삼지 않고 막는 구체적 위험과 잃는 협력을 확인해야 합니다. NTIA OPENRISK

팀들이 계속 협력할 수 있을까

작업대로 돌아갑니다. 팀들은 다음 달에도 그다음에도 개선할 계획입니다. 오늘의 단기 우위는 정부가 소중히 여기는 미래 협력을 잃게 할 수 있습니다. 믿을 만한 지속적 합의는 선택을 바꿀 수 있습니다. 관찰 가능한 행동, 미래 교환의 가치와 실수 가능성이 중요하며 약속만으로 해결되지 않습니다.
책 전체에 한 질문을 가져갑니다. **어떤 규칙이 구체적 위험을 다루면서 다음 유용한 기여의 실행 가능한 길을 남길까?** 모델 파일, 하드웨어, 의료 플랫폼과 태양광 설비에서 공유 대상은 바뀌어도 잃는 협력의 질문은 남습니다. 선택 계산은 선택: 게임 예제 계산 확인 에 있습니다. 수식 없이도 이야기는 이해할 수 있습니다.

핵심 사실의 발견: 완전히 봉쇄된 성벽이 아니라 반쯤 열린 문

가상의 장벽은 실제 규칙의 중요한 차이를 감춥니다. 기술은 이미 공개되었는가, 새 이전은 금지인가 제한인가 간소화 경로 대상인가?48호 공고와 미국 규칙은 서로 다른 질문에 답합니다. 이제 가상의 작업대에서 원문으로 넘어갑니다.

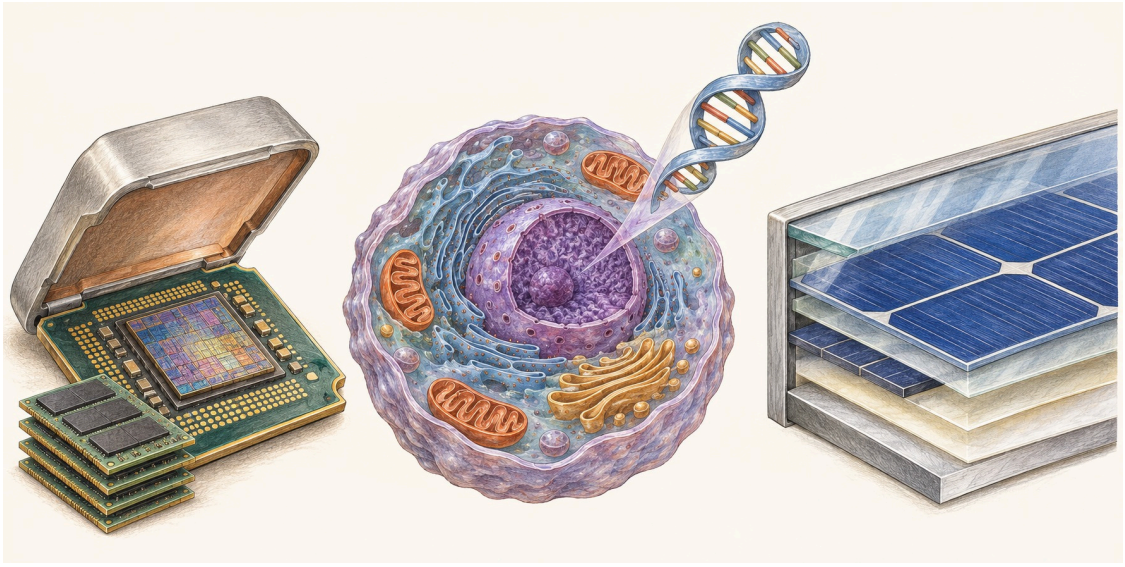


그림 5 프로세서, 세포, 태양광 패널의 층으로 컴퓨팅, 바이오의약과 태양광 제조를 보여줍니다.

표 1 제안된 기술40개 항목

분야	금지 제안	제한 제안
AI 및 컴퓨팅 하드웨어	6	17
바이오의약	3	2
태양광 제조	5	7

- **기존 공개와 최초 공개는 다릅니다.** 중국 제외와 미국 규칙은 범위가 다르고 논문이 사적 가중치를 공개하지는 않습니다. 파생판과 다른 법도 따로 봅니다. CN-A1, note 1 EAR734 EAR774
- **신규 오픈소스 AI와 칩 테이프아웃에는 전용 급행 차선이 열린다.** 중국 초안의 주석 2는 제한 등급 AI의 개방형 공개를 금지하는 대신, 오픈소스 수출, 해외 파운드리에서의 칩 테이프아웃(芯片流片), 그리고 중국 기업이 자체 구축·운영하는 해외 연산 클라우드에 대해 **자동 허가 및 간소화 조치** (상무부 공식 설명에 따르면 "신청 즉시 처리")를 제안한다 CN-A1, note 2 CNQA.
- **등록은 현재, 새 금지는 제안입니다.** 대상 소유·허락·지배 변화는 현재 문제입니다. 핵심 데이터 새 금지 항목은 초안이지 확정 시행이 아닙니다. CN48 CN-A1

이 책을 읽는 법

우리는 검증된 1차 사료에 뿌리를 둔 생생하고 명쾌한 이해를 원하는 평범하고 호기심 많은 독자들(개발자, 연구자, 의사, 창업자, 학생, 언론인, 그리고 시민들)을 위해 이 책을 썼다:

- 01. 지식에 세관 부스가 세워진 날 및 02. 마흔 개 통제 기술의 전체 지도에서는 베이징의 제48호 공고와 두 개의 서로 다른 시계, 그리고 **40개 통제 대상 기술** 전체를 하나씩 풀어낸다.
- 03. 지성과 실리콘: 모델과 칩, 클러스터를 지키는 관문에서는 소프트웨어 레시피와 실리콘 하드웨어 스택(`266504X`, `266506X`, `266507X`)의 내부로 깊이 들어간다.
- 04. 공개 모델: 공개와 비공개 이전 에서 공개 배포와 비공개 이전, 현재 의무와 제안된 경로를 구분합니다.
- 05. 살아 있는 코드: 유전자 플랫폼과 공유되는 치료제 및 06. 기계 속에 가둔 태양빛에서는 살아 있는 유전자 플랫폼과, 제조 노하우가 물리적 설비 안에 담겨 이동하는 태양광 장비를 탐구한다.

- 07. 워싱턴의 문지기들: 실리콘 칩과 모델 가중치에서는 2026년 5월 미 연방회계감사원(GAO) 결정을 둘러싼 충돌을 포함해 워싱턴의 반도체 칩(`3A090`) 및 모델 가중치(`4E091`) 규정을 명쾌하게 해설한다 USNE GAO26.
- 08. 두 개의 국경 체제와 공식 승인 획득 절차에서는 양국 체제를 나란히 비교하고, 공식 승인을 받기 위한 **담당 정부 부처, 온라인 포털, 정확한 법정 처리 기한, 검증된 전화번호·팩스·이메일·도로명 주소** 총람을 제공한다.
- 09. 일상의 질문들: 독자를 위한 실전 현장 가이드 및 10. 1차 사료, 검증 방법론, 그리고 쉬운 용어 사전에서는 여섯 가지 일상적 실전 시나리오와 쉬운 용어 해설, 그리고 **2026년 11월 2일** 기준 검증을 마친 **26개 1차 사료** 전체로 대단원을 맺는다.

> **참고**
> **공식 첨부파일 안내:** 중국 상무부는 부속서 1과 부속서 2를 WPS 형식으로 공표했으며, 10. 1차 사료, 검증 방법론, 그리고 쉬운 용어 사전에는 열람용 PDF 변환본과 함께 일체의 수정을 가하지 않은 원본 파일이 그대로 보존되어 있다. 이전에 로컬에 `china_export_control.pdf`라는 이름으로 저장되어 있던 무관한 오가노이드 연구 발표 자료는 본서의 근거 사료에서 제외했다.

01. 지식에 세관 부스가 세워진 날

어느 금요일 오후, 전혀 다른 두 개의 시계

어느 금요일 오후, 시청이 다가오는 겨울부터 고속도로 마흔 개 구간의 제한 속도를 낮출 계획이라며 시민들에게 30일 동안 의견을 보내 달라고 공고했다고 상상해 보자. 그런데 공고문의 후반부를 읽어 내려가다 보면 놀라운 문장이 나온다. 바로 그 금요일 오후부터 고속도로 위에 이미 실제 검문소가 문을 열어 대상 화물차의 통과 기록을 남기고 있으며, 심지어 어제 물류창고를 출발해 아직 다리를 다 건너지 못한 트럭까지 모두 기록 대상이라는 것이다.

2026년 제48호 공고 가 작동하는 방식이 문자 그대로 이와 같다. **2026년 10월 16일** , 중국 상무부(MOFCOM, 실무 총괄은 산업안보수출입통제국)와 과학기술부(MOST)가 중국 《대외무역법》 및 《기술수출입관리조례》에 근거해 공동 발표한 이 문서는 서로 다른 두 개의 시계를 동시에 째깍거리게 만들었다 CN48, sections I and III CNTIER:



그림 6 2026년 10월 16일 두 갈래 병행 궤도로 나뉜 제48호 공고: 40개 신설 기술 항목안에 대한 30일간의 의견 수렴과 ecomp.mofcom.gov.cn 포털에서의 즉시 수출 전 정보 등록 의무.

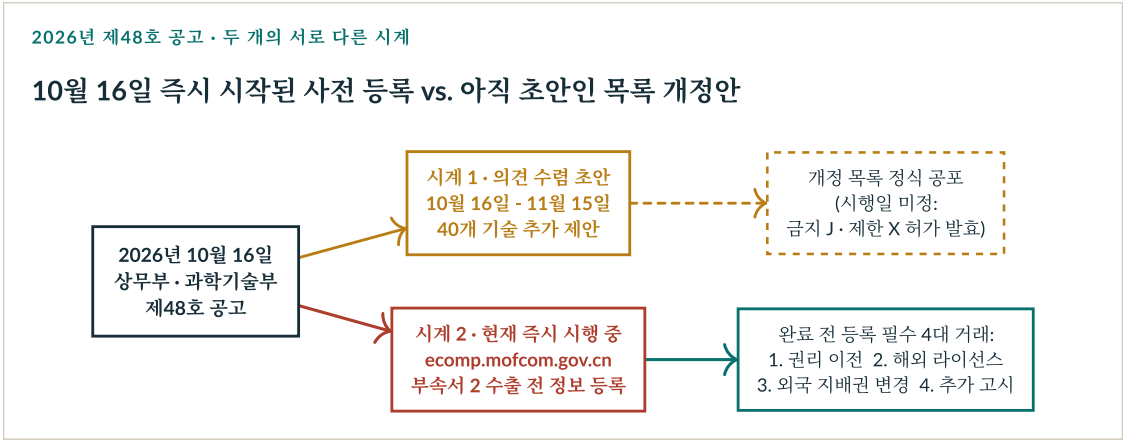


그림 7 2026년 10월 16일 두 갈래 병행 궤도로 나뉜 제48호 공고: 40개 신설 기술 항목안에 대한 30일간의 의견 수렴과 ecomp.mofcom.gov.cn 포털에서의 즉시 수출 전 정보 등록 의무.

1. **의견 수렴의 시계 (2026년 10월 16일 ~ 11월 15일):** 베이징은 인공지능 및 반도체(23개), 바이오의약(5개), 태양광 에너지(12개) 분야에 걸쳐 수출 금지 14개와 수출 제한 26개로 이루어진 **40개 기술 항목** 을 《수출금지·수출제한 기술 목록》에 추가하자고 제안한다. 공개 의견 수렴 기간이 끝나고 최종 개정 목록이 정식으로 공포될 때까지, 이 새로운 수출 금지 및 허가 규정은 어디까지나 **확정된 금지가 아닌 초안(제안)** 상태에 머문다 CN48, sections I and II.
2. **사전 등록의 시계 (지금 이 순간 작동 중):** 제48호 공고가 발표된 2026년 10월 16일 당일부터 향후 최종 개정 목록이 정식 발효되는 날(베이징은 이 날짜를 의도적으로 확정하지 않았다)까지, 부속서 1에 열거된 기술을 수출하려는 모든 주체는 상무부 업무시스템 통합 플랫폼(`https://ecomp.mofcom.gov.cn`)을 통해 온라인으로 **수출 전 정보 등록** 을 완료해야 한다 CN48, section III(1) CNPLAT.

이 두 개의 시계를 혼동하는 것이야말로 중국의 새 규정을 이야기할 때 사람들이 가장 흔히 저지르는 실수다. 등록 제도는 오늘 당장 시행 중이지만, 이는 신고 관문일 뿐 수출 금지가 아니다. 반대로 11월 중순 의견 수렴이 끝날 때까지 손을 놓고 있다가는, 지금 당장 해외 라이선스 계약을 체결하거나 대상 장비를 선적하거나 외국계 투자 라운드를 마무리하고 있는 스타트업과 대학 연구실이 예상치 못한 법적 허점에 걸려들 수 있다 CN48 CNQA.

나무 상자 하나 꾸리지 않고 국경을 넘는다는 것

우리 조부모 세대가 수출 이라는 단어를 들었을 때 떠올린 풍경은 상하이나 로테르담 항구에서 거대한 크레인이 화물선 위로 강철 컨테이너를 들어 올리는 모습이었다. 하지만 현대의 기술 규제 당국이 수출 을 말할 때는 나무 상자 하나도 부두에 닿을 필요가 없다.
제48호 공고 제3조 제2항에 따르면, 다음 네 가지 유형의 거래는 완료 전에 의무적으로 수출 전 정보 등록을 마쳐야 한다, **10월 16일 이전에 이미 시작되었으나 아직 완료되지 않은 이전 거래까지 포함해서** 말이다 CN48, section III(2):

- **핵심 자산을 해외에 매각하는 행위:** 특허권을 양도하거나 독자적인 모델·칩 지식재산권(IP)을 매각하는 등 국내 기술의 소유권을 해외 매수인에게 이전하는 경우.
- **해외 사용 라이선스를 부여하는 행위:** 소유권은 중국 내에 그대로 두되, 해외 파트너나 고객사, 해외 자회사가 국외에서 대상 국내 기술을 사용할 수 있도록 라이선스를 허여하는 경우.
- **운전대를 쥔 주체가 바뀌는 행위:** 기업 인수합병, 지배구조 개편, 지분 변동 등을 통해 국내 기술의 소유자 또는 실질적 지배자(실제 통제인)가 해외 법인·주체로 변경되는 경우. 모든 엔지니어와 서버가 항저우나 베이징에 그대로 머물러 있더라도 궁극적인 기업 지배권이 국경을 넘어가면 규정이 즉시 작동한다.
- **상무부가 별도로 고시하는 기타 상황:** 새로운 형태의 기술 이전 구조가 등장할 때 상무부가 공식 통지를 통해 대응할 수 있도록 열어 둔 포괄적 보충 조항.

수출자가 `ecomp.mofcom.gov.cn` 안의 기술무역 관리정보 애플리케이션에 로그인하여 **부속서 2**(《기술수출 정보등록표》)를 제출할 때, 포털은 감사 가능한 구체적 사실관계를 요구한다. 수출자의 법인 정보와 공식 법인 직인(公章), 기술 소유권자, 해외 인수자의 중문·영문 명칭과 국가·주소 및 수출자와의 지배구조 관계, 정확한 7자리 목록 코드와 핵심 기술 지표, 최종 사용자 및 최종 용도, 자체 개발 지식재산권 여부, 그리고 미화(USD)로 환산한 계약 금액 등이다 CN-A2. 단일 거래에서 동일한 해외 파트너에게 여러 기술을 함께 이전할 때는 한 장의 양식에 묶어 신고할 수 있으나, 거래 상대방이 다르면 각각 별도로 신고해야 한다 CN48, section III(3).

모든 것을 바꾸는 네 가지 규제 용어

법률 기술 목록이 처음 보기에 위압적으로 느껴지는 까닭은 일반 독자들이 모든 줄을 '전면 금지'로 읽곤 하기 때문이다. 그러나 실제 현장에서 네 가지 규제 범주가 인류의 진보에 갖는 의미는 하늘과 땅 차이만큼 다르다 CN-A1, notes 1 to 4 CNQA CNTIER:

수출 금지 (禁止出口, J로 끝나는 코드)
: 단단한 붉은 성벽이다. 목록이 최종 확정되면 명시된 범위 안의 대상 기술은 법적으로 일절 수출할 수 없다 CNTIER, Art. 32.

수출 제한 (限制出口, X로 끝나는 코드)
: 자물쇠와 열쇠가 달린 검문 관문이다. 기술을 이전하기 전에 정부의 공식 허가를 받기만 하면 적법하게 수출할 수 있다 CNTIER, Art. 33.

자동 허가 (自动许可)
: 특정 제한 수출의 신속 편의 제안입니다. 제외나 확정 절차·승인 시간 보장은 아닙니다. CN-A1, notes 2 and 3 CNQA

관리 대상 제외 (不纳入管理范围)
: 이 기술 목록의 바깥 영역이다. 이미 공개된 오픈소스 AI와 발표된 학술 논문이 주석 1에 따라 여기에 속하며, 데이터 보안법이나 저작권법 같은 일반 법률만 평소처럼 적용된다 CN-A1, note 1.

: 국제공항을 떠올리면 이해가 쉽다. 수출 금지 품목은 비행기에 실을 수 없고, 수출 제한 품목은 정식 수출 허가증이 있어야 하며, 자동 허가 는 자동출입국 패스트트랙 게이트이고, 관리 대상 제외 품목은 세관에 멈춰 서지 않고 배낭에 넣은 채 그대로 통과하는 물건이다.

두 팀에 주는 의미

두 팀에게 대상 이전 전에 정보를 등록하는 것과 이전이 금지되는 것은 서로 다른 장애물입니다. 이야기는 각 규칙 아래 어떤 협력이 남는지 묻습니다. 영향을 판단하기 전에 현재 시행되는 의무와 제안 단계의 목록 변경을 구분합니다.
두 팀의 출발점은 요새의 함정: 양쪽이 함께 잃는 구조 에 있습니다.

02. 마흔 개 통제 기술의 전체 지도

정부는 어떻게 하나의 아이디어를 자로 재는가

대학생의 주말 코딩 프로젝트와 국가 전략 자산을 구분하는 법률 조문은 과연 어떻게 써야 할까? 만약 법전에 '첨단 AI 및 하드웨어를 통제한다'고 막연히 적어 놓는다면 세상의 모든 계산기 앱과 회로 기판이 서류 더미에 파묻히고 말 것이다. 반대로 특정 기업이나 모델 브랜드 이름을 콕 집어 적어 놓는다면 내일 아침 이름표만 바꾼 새 버전이 유유히 검문소를 빠져나갈 것이다. 규제 당국은 이 난제를 **수치화된 성능 인계철선과 목적 범위** 를 긋는 방식으로 해결한다. 제48호 공고 부속서 1에서 베이징은 7자리 목록 코드 안에 **40개의 개별 기술 통제 지점** 을 정밀하게 배치했다. **인공지능 및 AI 하드웨어 분야 23개** (수출 금지안 6개, 수출 제한안 17개), **바이오의약 분야 5개** (금지안 3개, 제한안 2개), **태양광 제조 분야 12개** (금지안 5개, 제한안 7개)로 구성되어 공식 집계인 **수출 금지 14개** 와 **수출 제한 26개** 기술 합계와 정확히 일치한다 CN48 CN-A1 CNQA.

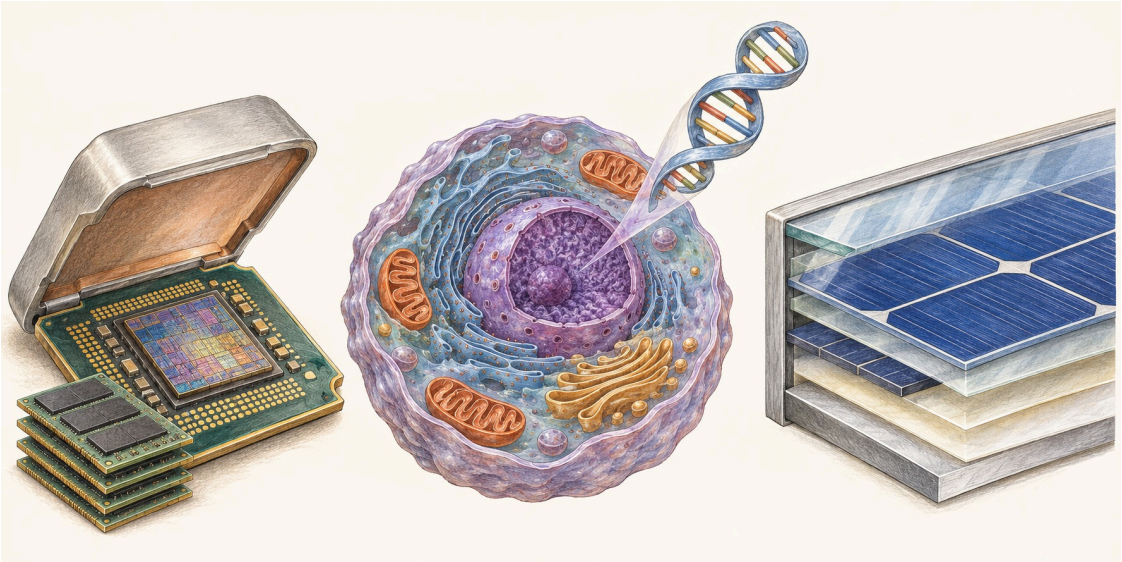


그림 8 프로세서, 세포, 태양광 패널의 층으로 컴퓨팅, 바이오의약과 태양광 제조를 보여줍니다.

266504X 주2항,266505X4항,266506X **주2항** ,266507X4항입니다. 원코드를 보존해40점으로 편집했으며 법적 목록 대체가 아닙니다. CN-A1

인계철선에 걸려 넘어지지 않고 조문을 읽는 세 가지 습관

이 기술 지도를 탐색할 때는 다음 세 가지 실전 독해 습관을 염두에 두자:

1. **'어느 하나(OR)' 조건과 '모두 충족(AND)' 조건을 구별하라.** `266504X` 제2호(프런티어 거대 모델)는 세 가지 기준 중 단 하나라도 충족되면 작동한다, 연산량 $\geq 10^{26}$ FLOPs, 또는 ≥ 2조 파라미터, 또는 수출 시점 글로벌 Top 10 벤치마크 순위다. 반대로 `266505X` 제1호(계획 수립 에이전트)는 과업을 ≥ 20단계로 분해하고, 동시에 분해 정확도 $\geq 80\%$를 달성하며, 동시에 하위 과업 평균 완수율 $\geq 90\%$에 도달하는 세 조건이 모두 결합될 때만 작동한다 CN-A1.
2. **개발 목적이 울타리의 절반을 결정한다.** 언뜻 매우 엄혹해 보이는 여러 항목, 예컨대 정확도 $\geq 95\%$ 이상의 딥페이크 탐지(`266401J`)나 고성능 민감 영역 에이전트(`266502J`)은 국가 국경 간 데이터 안보 방어, 핵심 기반시설, 군사, 또는 핵심 정부 업무를 전용 혹은 주된 목적 으로 제작된 경우에만 적용된다. 일반적인 콘텐츠 스튜디오 도구나 소비자용 비서 앱은 그 목적 범위 바깥에 있다 CN-A1.
3. **소프트웨어 목록 안에 숨은 하드웨어를 읽어 내라.** 아래 18번째부터 23번째 항목(`266506X` 및 `266507X`)은 챗봇과는 거리가 멀다, 이들은 **프로세서 칩 아키텍처, 3D NAND 및 DRAM 메모리 설계, 1만 장 초과 슈퍼클러스터 인터커넥트** 를 다루며, 나아가 주석 4는 **열거된의 물리적 태양광 제조 설비** 를 직접 수출 통제 안으로 끌어들이고 있다 CN-A1.

인공지능, 반도체 칩 및 슈퍼클러스터 (23개 통제 지점)

266401J · Point 1: 국경 간 데이터 안보용 딥페이크 탐지 *(수출 금지안)*
중국의 국경 간 네트워크 데이터 안보 수호를 주된 목적으로 구축되어 딥페이크 영상·음성·이미지·멀티모달 콘텐츠 전반에서 정확도(accuracy) 95% 이상과 재현율(recall) 95% 이상을 동시에 달성하는 고성능 탐지 시스템 및 장비 제조 기술. 이러한 국가 안보 목적 바깥의 일반 소비자용 미디어 판별 도구는 대상이 아니다.

266402J · Point 1: 자율형 악성코드 생성 및 변이 기술 *(수출 금지안)*
핵심 기반시설, 국방 시스템, 핵심 정부 전산망을 타격할 수 있는 악성코드를 자율적으로 작성·변이시키며 명시된 공격 성공률(다중 엔진 스캐너 상대 60% 이상, 주류 백신 상대 85% 이상, 머신러닝 탐지기 상대 90% 이상)에 도달하는 AI 기술. 일상적인 코딩 보조 도구는 포함되지 않는다.

266402J · Point 2: 자기적응형 사이버 탐지 회피 AI *(수출 금지안)*
국가 안보 민감 표적을 겨냥해 제작된 공격형 AI로서, 샌드박스·디버거·에뮬레이터 분석 환경을 스스로 감지해 탈출하거나 핵심 공격 페이로드를 유지한 채 매 실행 시 코드 구조나 제어 흐름의 50% 이상을 자동으로 재작성하는 기술.

266402J · Point 3: 탐지 회피 변종 악성코드 대량 자동 생성·배포 *(수출 금지안)*
민감 사이버 작전을 위해 회피형 변종 악성코드를 대규모로 생성·배포하는 기술. 구조가 뚜렷이 다른 변종 20개 이상 동시 생성(또는 전 과정 80% 이상 자동화), 구문 트리 차이 30% 이상의 일일 10개 이상 변종 생성, 또는 샌드박스 내 90% 이상의 행동 일관성 유지 기준이 적용된다.

266501J · Point 1: 중국 법정 '핵심 데이터' 기반 학습 거대 모델 *(수출 금지안)*
중국《데이터보안법》상 최고 국가 안보 등급인 법정 핵심 데이터*(Core Data)*를 사용해 학습되고 서비스 형태로 제공되는 거대 AI 모델. 이 레드라인을 작동시키는 기준은 학습 데이터의 법적 등급이지 특정 기업의 브랜드명이 아니다.

266502J · Point 1: 핵심 인프라·국방 전용 고성능 AI 에이전트 *(수출 금지안)*
핵심 기반시설, 국방, 또는 핵심 정부 업무를 전용·주된 목적으로 제작되면서 동시에 `266505X` 항목에 정의된 고성능 지표를 충족하는 AI 에이전트. 범용 업무 생산성 도구나 일반 코딩 에이전트는 여기에 해당하지 않는다.

266402X · Point 8: 초고정밀 딥페이크 탐지 시스템 (정확도·재현율 98% 이상) *(수출 제한안)*
국경 간 데이터 안보 방어 목적 여부와 관계없이 영상·음성·이미지·멀티모달 콘텐츠 전반에서 정확도와 재현율 모두 98% 이상을 달성하는 딥페이크 탐지 시스템 및 관련 장비 제조 기술.

266402X · Point 9: 비가시성 초정밀 영상·이미지 스테가노그래피 *(수출 제한안)*

이미지나 영상 속에 기밀 데이터를 은닉·추출하는 기술로, 세 가지 지표가 모두 동시에 충족될 때만 해당된다. 왜곡 환경에서의 높은 복원력(비트 오류율 <=0.5% 또는 재현율 >=99.9%), 오탐률 <=0.1%, 그리고 육안으로 식별 불가능한 비가시성(SSIM >=0.999, PSNR >=41 dB, 또는 LPIPS <=0.005)이다.

266404X · Point 6: AI 기반 제로데이 취약점 및 익스플로잇 자동 발굴 *(수출 제한안)*
여섯 가지 고난도 기준 중 어느 하나를 충족하는 사이버보안 AI: 주요 익스플로잇 벤치마크 >=75% 달성, 전체 공격 체인 자동 구축(주요 OS·브라우저 대상 >=50% 또는 임의 코드 실행 >=40%), 시니어 인간 연구원 대비 10배 속도, 중·저위험 버그 2개 이상을 결합한 실작동 개념증명(PoC) 공격 생성, 단일 분석으로 주요 OS나 오픈소스 프로젝트에서 치명적 취약점 5개 이상 또는 신규 버그 50개 이상 발견, 또는 주류 취약점 평가 척도 최상위 등급 도달.

266501X · Point 19: 고속·위변조 방지 및 방언 특화 성문(화자) 식별 *(수출 제한안)*
네 가지 기준 중 어느 하나에 도달하는 화자 식별 알고리즘 및 시스템: 단문 음성에서 오인식률 <=0.01% 조건 하 정인식률 >=99.1%, 초당 100건 이상 요청 시 지연시간 <=300 ms, 녹음 재생 및 합성 음성에 대한 위변조 탐지율 >=98%(또는 타인수락률 <=1%), 또는 중국 소수민족 언어·지역 방언 특화 정확도 >=90%.

266501X · Point 20: 중국어 및 소수민족 언어 고품질 기계번역 *(수출 제한안)*
중국어 및 중국 내 소수민족 언어를 주된 대상으로 구축된 기계번역 기술로서, 인간 품질 평가 점수(MOS) 4.8 이상을 기록하거나 의미 충실도 >=95%와 함께 일반 텍스트 BLEU >=35(전문 분야는 BLEU >=30) 이상을 달성하는 기술.

266504X · Point 1: 중국 법정 '중요 데이터' 기반 학습 거대 모델 *(수출 제한안)*
법정 중요 데이터*(Important Data)* 로 학습되어 서비스로 제공되는 거대 모델. 다만 항목 주석 1은 해당 데이터가 특정 분야 핵심 연구개발 역량을 높이지도 않고 모델 출력물에 재현되지도 않도록 정제된 극미량 사용(<=0.1%)과, 공개 채널에서 적법하게 취득 가능한 데이터를 명확히 통제 대상에서 제외한다.

266504X · Point 2: 프런티어 거대 모델 핵심 기술 *(수출 제한안)*
AI 모델 규정의 심장부다. 학습 연산량 >=10^26 FLOPs, >=2조 파라미터, 또는 수출 시점 기준 글로벌 Top 10 공개 벤치마크 순위 중 어느 하나라도 충족할 경우 가중치, 핵심 체크포인트, 기반 소스 코드, 아키텍처, 학습 최적화 및 추론 가속 기술 전반을 포괄한다. 오픈소스 공개는 주석 2의 자동 허가 패스트트랙 대상이 된다.

266505X · Point 1: 장기 호흡 자율 과업 계획 에이전트 *(수출 제한안)*
자연어 지시를 20단계 이상의 실행 가능한 하위 과업 사슬로 분해하면서 동시에 분해 정확도 80% 이상과 하위 과업 평균 완수율 90% 이상을 달성하는 과업 계획 기술. 세 가지 수치 기준이 모두 함께 충족되어야 한다.

266505X · Point 2: 60개 이상 다중 에이전트 협업 오케스트레이션 *(수출 제한안)*
60개 이상의 AI 에이전트를 동시에 구동하면서 동등 품질 기준 가장 빠른 단일 에이전트 소요 시간의 2배 이내에 작업을 마치고, 정답(ground-truth)과의 일치율 >=85%를 달성하는 다중 에이전트 조율 프레임워크.

266505X · Point 3: 200개 이상 외부 도구를 운용하는 에이전트 *(수출 제한안)*
200개 이상의 외부 서드파티 도구를 통합 지원하면서 90% 이상의 정확도로 적합한 도구를 선택하고, 서로 다른 도구 3개 이상을 연쇄 호출하는 복합 과업에서 종단 간(end-to-end) 성공률 90% 이상을 기록하는 도구 활용·시스템 조작 기술.

266505X · Point 4: 실시간 전략 게임 및 고속 의사결정 에이전트 *(수출 제한안)*
세 가지 요건을 동시에 충족하는 전략 의사결정 AI: >=20단계 계획 수립(또는 >=10개 동시 에이전트), 동적 환경에서 >=10개 제어 단위에 걸친 200 ms 미만의 적응형 의사결정, 그리고 표준 전략 벤치마크에서 인간 참여자 상위 90%를 능가하는 성능.

266506X · Point 1: AI 프로세서 아키텍처, 명령어 집합 및 IP 코어 *(수출 제한안)*
<=14 nm 공정 요구, 부동소수점·정수 연산 역량, 2.5D/3D 칩렛 패키징, 고속 인터커넥트, 비폰노이만·인메모리 컴퓨팅 설계, 또는 비전·음성·자율주행 등 명시된 용도 특성 중 어느 하나에 해당

하는 맞춤형 아키텍처, 명령어 집합, 연산 IP 코어 및 기반 소프트웨어 스택 설계 기술. 주석 2에 따라 해외 파운드리 테이프아웃에는 자동 허가 간소화가 제공된다.

266506X · Point 2: 첨단 3D NAND 플래시 및 적층형 DRAM / HBM 칩 설계 *(수출 제한안)*
기록 밀도 >=8 Gb/mm2, 입출력 속도 >=1.5 Gbps, 또는 웨이퍼 본딩을 구현한 3D NAND 플래시 메모리 설계 기술; 또는 <=18 nm 노광 공정, 수직 채널 트랜지스터, 본딩, 다층 HBM 방식의 웨이퍼·다이 적층을 채택한 DRAM 메모리 설계 기술.

266507X · Point 1: 1만 장 초과 GPU 클러스터용 초고속 인터커넥트 *(수출 제한안)*
가속기 카드 1만 장을 초과하는 초대형 AI 연산 클러스터 내부에서 양방향 대역폭 800 GB/s 이상을 제공하는 칩 간(chip-to-chip) 또는 노드 간(node-to-node) 고속 상호연결 기술.

266507X · Point 2: 1만 장급 클러스터 분산 학습 고속 장애 복구 *(수출 제한안)*
1만 장 초과 클러스터에서 다음 기준 중 어느 하나를 만족하는 분산 학습 회복탄력성 기술: 체크포인트 장애 복구 시간(MTTR) <=120초, 체감 중단 <=30초 이내의 무중단 과업 이관, 또는 네트워크 장애로 인한 유효 GPU 연산 손실률 <=5%.

266507X · Point 3: 마이크로초급 클러스터 집합 통신 스케줄링 *(수출 제한안)*
1만 장 초과 AI 클러스터에서 선형 확장 효율 >=98%, 종단 간 지연시간 <=1마이크로초의 동적 토폴로지 인지 라우팅, 또는 연산 과정 뒤에 통신 시간을 숨기는 연산-통신 중첩률 >=90% 중 어느 하나를 달성하는 통신 스케줄링 기술.

266507X · Point 4: 이종(다중 제조사) 및 권역 간 GPU 통합 오케스트레이션 *(수출 제한안)*
1만 장 초과 클러스터 안에서 서로 다른 2개 이상의 하드웨어 제조사 AI 칩을 하나로 통합 운용하며 고대역폭, 처리량 향상(+30%), 카드 가동률(+65%), 비용 절감(-20%), 가용성 99.9%, 또는 데이터센터 간 분산 학습 효율 >=80% 등 명시된 지표를 달성하는 소프트웨어 및 운영 기술.

바이오의약 및 유전자 플랫폼 (5개 통제 지점)

262704J · Point 1: 재사용형 세포·유전자 치료제(CGT) 기반 플랫폼 *(수출 금지안)*
다수의 세포·유전자 치료제를 반복 창출할 수 있는 중국 주체 소유의 원천 기반 플랫폼. 핵심은 플랫폼 소유권의 해외 매각만 금지된다는 점이다. 해외 라이선스 아웃, CRO/CDMO 위탁개발생산, 그리고 개별 의약품의 연구·임상·품목허가·상업화에 필요한 기술은 금지 범위 바깥에 남는다.

262705J · Point 1: 재사용형 siRNA 신약 개발 기반 플랫폼 *(수출 금지안)*
중국 주체가 소유한 원천 소간섭 RNA(siRNA) 기반 플랫폼으로, CGT와 정확히 동일한 경계가 적용된다. 재사용 엔진 자체의 소유권을 국외로 이전하는 행위는 금지되지만, 라이선스 계약과 위탁 연구개발·생산, 개별 신약 파트너십은 그대로 열려 있다.

267302J · Point 1: 병원체 기능 강화 및 유도 진화 기술 *(수출 금지안)*
병원체의 기능을 강화하거나 대규모 배양 시 독성을 유지시키고 진화 적응 속도를 높이는 인공 유전자 변형 및 통제 계대배양 기법을 차단하는 생물안보 레드라인. 일반적인 의료 진단과 백신 진료 활동에는 영향이 없다.

262705X · Point 1: 미공개 신규 세포·유전자 치료제 표적 발굴·검증 *(수출 제한안)*
전 세계 특허, 학술지, 공개 데이터베이스, 학술대회 어디에서도 이전에 공개된 적 없는 완전히 새로운 CGT 치료 표적을 발굴·검증하는 중국 보유 기술. 주석 3에 따라 해외 라이선스 아웃, 국제 공동연구, 공중보건 위기 대응에는 자동 허가 간소화가 적용된다.

262706X · Point 1: 미공개 신규 siRNA 신약 표적 발굴·확정 *(수출 제한안)*
전 세계적으로 미공개된 완전히 새로운 siRNA 신약 표적을 스크리닝·확정하는 중국 보유 기술이며, 국제 라이선스 협력과 공동연구, 인도주의적 보건 대응을 위한 주석 3의 패스트트랙 간소화가 동일하게 적용된다.

태양광 실리콘, 웨이퍼 및 공장 핵심 설비 (12개 통제 지점)

263003J · Point 1: 초대형 냉수소화 폴리실리콘 생산 공정 *(수출 금지안)*

단일 생산 라인당 연간 25만 톤 이상의 삼염화실란을 생산할 수 있는 냉수소화 유동층 반응 공정 레시피 및 핵심 장비 제조 노하우.

263003J · Point 2: 대용량 실란 유동층 폴리실리콘 공정 *(수출 금지안)*
단일 생산 라인 기준 연간 생산량 2만 톤 이상을 구현하는 실란 유동층 화학 공정 레시피 및 장비 제조 기술.

263004J · Point 1: 종이보다 얇은 70마이크로미터 이하 실리콘 웨이퍼 절단 *(수출 금지안)*
태양광 실리콘 웨이퍼를 두께 70마이크로미터(사람 머리카락 굵기 수준) 이하로 절단하는 공정 노하우 및 설비 제작 기술로서, 제어 소프트웨어, 핵심 알고리즘, 엔지니어링 설계 도면을 명시적으로 포함한다.

263801J · Point 1: 박형 대면적 태양전지 에지 패시베이션 공정 *(수출 금지안)*
두께 140마이크로미터 이하인 182~230 mm 규격 결정질 실리콘 웨이퍼에 적용되는 태양광 전용 에지 패시베이션(측면 부동태화) 공정 및 장비 제조 노하우.

263801J · Point 2: 효율 30% 이상 페로브스카이트 및 탠덤 태양전지 기술 *(수출 금지안)*
네 가지 기준에 걸친 차세대 태양전지 제조 기술: 효율 >=30% 양산형 실리콘-페로브스카이트 탠덤 셀(>=182 mm), 폭 >=1.1 m 대면적 슬롯다이 코팅, 효율 >=18% 단일접합 페로브스카이트 모듈(면적 >=1 m2), 또는 효율 >=28% 탠덤 모듈(면적 >=1 m2).

263004X · Point 1: 연산 3만 톤 이상 폴리실리콘 플랜트 엔지니어링 *(수출 제한안)*
단일 라인 기준 연간 3만 톤 이상을 생산하는 폴리실리콘 생산 라인의 종합 플랜트 엔지니어링 패키지, 공장 설계도 및 핵심 설비 설계 기술.

263004X · Point 2: 환원로 1기당 연산 800톤 이상 고수율 환원 공정 *(수출 제한안)*
환원로 1기당 연간 최소 800톤 이상의 폴리실리콘을 생산해 내는 고수율 환원로 공정 레시피 및 설비 제조 기술.

263005X · Point 1: 대형 챔버 단결정 실리콘 인상로 설계 *(수출 제한안)*
챔버 내경 >=1,600 mm, 핫존(열장) >=35인치, 인상 속도 >=1.2 mm/min, 또는 등직경 공정 소비전력 <=40 kW 중 어느 하나의 기준에 해당하는 태양광 단결정 잉곳 성장로 설계 기술.

263005X · Point 2: 720 mm 이상 장축 실리콘 잉곳 절단·연마 가공 *(수출 제한안)*
길이 720 mm 이상인 태양광 실리콘 잉곳의 반봉 절단·연마 공정 또는 정밀 기계가공 및 전용 설비 제작 노하우.

263005X · Point 3: 직사각형 웨이퍼 또는 130마이크로미터 박형 웨이퍼 절단 *(수출 제한안)*
<=28마이크로미터 극세 텅스텐 와이어 쏘 또는 고속 스핀들(>=6,500 rpm) 및 고밀도 가이드 롤러 구조를 이용한 직사각형 태양광 웨이퍼(어느 한 변 >=182 mm) 또는 박형 웨이퍼(두께 <=130 마이크로미터) 제조 기술.

263802X · Point 1: 고효율 TOPCon 및 후면전극형(XBC) 태양전지 공정 *(수출 제한안)*
셀 효율 >=25% 또는 모듈 효율 >=22.3% 구현을 위해 두께 <=140마이크로미터의 182~230 mm 웨이퍼 위에서 수행되는 6대 핵심 양산 공정군(LPCVD/PECVD 터널 산화막, 고속 ALD 패시베이션, 붕소 확산, 구리 도금, 미세결정질 증착, XBC 전극 도금).

263802X · Point 2: 고효율 이종접합(HJT) 태양전지 제조 공정 *(수출 제한안)*
저인듐(<=50%) 또는 초고속 투명전도성산화막(TCO) 코팅, 두께 <=110마이크로미터 웨이퍼 상의 결정질 실리콘 박막 증착, 저은(은 함량 <=30%) 은코팅 구리 페이스트, 구리 도금 HJT 전극 등 4대 HJT 핵심 제조 공정군.

두 팀에 주는 의미

색인은 제안된 기술 항목을 셉니다. 게임 점수는 가상 선호이며 기술 수가 아닙니다. 팀에게는 모든 AI가 한 장벽 뒤에 있는지보다 다음 기여에 어떤 정확한 항목과 조건이 적용되는지가 중요합니다.

두 팀의 출발점은 요새의 함정: 양쪽이 함께 잃는 구조 에 있습니다.

03. 지성과 실리콘: 모델과 칩, 클러스터를 지키는 관문

천연 발효종, 베이커리 창구, 그리고 무쇠 오븐

스마트폰에 질문을 입력하는 평범한 사용자에게 인공지능은 매끄럽게 이어진 하나의 마술처럼 느껴진다. 말을 걸면 대답을 돌려주는 작은 입력창 말이다. 그러나 엔지니어의 눈으로 보면, 그리고 이제 베이징과 워싱턴에서 수출 통제 조문을 작성하는 정책 입안자들의 눈으로 보더라도, 하나의 AI 시스템은 **세 개의 뚜렷한 물리적·디지털 계층** 으로 나뉜다:

1. **베이커리 판매 창구 (원격 API 및 앱 서비스):** 가게 창구 너머로 손님에게 따뜻한 빵 한 조각을 건네준다고 해서, 그 손님이 오븐 배선을 어떻게 깔아야 하는지나 내일 스스로 빵 1만 개를 어떻게 구워 낼 수 있는지를 알게 되는 것은 아니다.
2. **천연 발효종과 마스터 레시피 (가중치, 체크포인트 및 학습 코드):** 학습을 통해 조율된 수십억~수조 개의 수치 파라미터(模型权重), 학습 중간 단계의 스냅샷(关键检查点), 모델 아키텍처, 그리고 학습 최적화 및 추론 가속 코드(训练优化、推理加速)다. 이 파일들을 복사하는 순간 훈련된 지성 그 자체가 복제된다.
3. **무쇠 오븐과 발전소 (AI 칩, 메모리 스택 및 슈퍼클러스터):** 물리적인 실리콘 프로세서와 고대역폭 메모리, 칩 설계도, 그리고 광 클러스터 네트워크다. 이 기반이 없으면 모델을 새로 학습시키는 일도, 외부와 단절된 로컬 환경에서 직접 구동하는 일도 불가능하다.

상무부 설명은 API, 앱, 웹, SaaS, 경량 로컬 서비스와 초안의 제한 대형 모델 기술 이전을 구분합니다. 모든 기술 및 데이터 규칙의 면제는 아닙니다. 부속서1은 모델 기술(`266504X`), 프로세서와 메모리 설계(`266506X`), 가속 카드 10,000개 초과 클러스터의 특정 기술(`266507X`)을 별도로 열거합니다. CNQA CN-A1

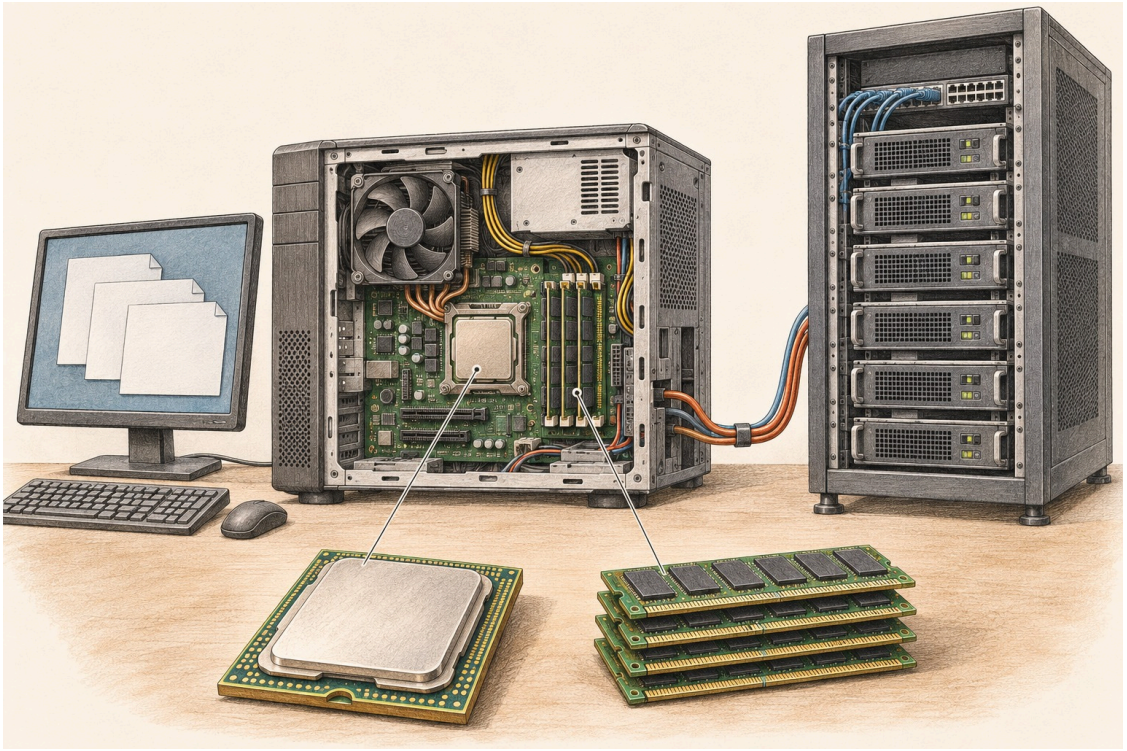


그림 9 공개 모델은 칩·메모리·계산 기반에 의존합니다. 일부 제한은 전체 접근에 영향을 줄 수 있습니다.

프런티어 모델을 가르는 세 개의 인계철선 (266504X)

대학 연구실이나 스타트업 차고에서 학습시킨 신경망이라고 해서 모두 수출 제한안인 **266504X 제2호** 의 망에 걸리는 것은 아니다. 모델의 핵심 기술(가중치, 핵심 체크포인트, 기반 소스 코드, 아키텍처, 학습 최적화, 추론 가속 기술)은 다음 세 가지 인계철선 중 **어느 하나라도** 넘어설 때 비로소 통제 범위에 들어온다 CN-A1, 266504X(2), note 3:

1. **연산 규모:** 총 학습 연산량이 최소 10^{26} **부동소수점 연산(FLOPs)** 에 도달하는 경우, 미국의 4E091 모델 가중치 규정에서도 동일하게 채택한 초대형 연산 임계치다 US25.
2. **파라미터 규모:** 전체 매개변수(파라미터) 수가 최소 **2조 개(2,000억 개의 10배)** 이상인 경우.
3. **수출 시점 기준 글로벌 상위 10위권 성능:** 아무리 날렵하고 작은 모델이라도 **수출이 이루어지는 바로 그 시점** 에 국내외 주류 벤치마크 기관이나 주요 산업 플랫폼의 공개 평가에서 종합 역량, 전문 비즈니스 과업, 글로벌 호출량, 안전 성능, 또는 학습 효율 부문 **글로벌 Top 10** 안에 이름을 올리고 있다면 대상에 해당한다 CN-A1, 266504X, note 3.

이 세 번째 인계철선은 살아 움직이는 유기체와 같다. 오픈소스 연구자들이 최첨단 추론 능력을 300억(30B)이나 700억(70B) 파라미터 크기로 증류해 내는 기발한 기법을 쉼 없이 발명하기 때문에, 작지만 영특한 신예 모델이 세계 6위로 데뷔한 주간에는 제한 범위 안으로 들어왔다가도 8개월 뒤 더 새로운 모델들에 추월당하면 다시 범위 바깥으로 걸어 나갈 수 있다. 즉 분류 여부는 특정 날짜의 특정 모델 버전에 귀속될 뿐, '딥시크(DeepSeek)'나 '큐웬(Qwen)' 같은 브랜드 이름에 영구히 낙인처럼 찍히지 않는다 CN-A1.

데이터 레드라인(266501J 및 266504X(1))과 자율 에이전트(266505X 및 266502J)

아무리 크기가 작은 모델이라도 국가 기밀을 먹고 자랐다면 단단한 벽에 가로막힌다. 중국 《데이터보안법》의 분류 체계를 차용한 부속서 1은 법정 **핵심 데이터(Core Data)** 로 학습된 모델을 원격 서비스 제공 형태까지 포함해 **수출 금지안** (266501J)의 붉은 성벽 뒤에 두는 한편, **중요**

데이터(Important Data) 로 학습된 모델은 **수출 제한 차선** (`266504X(1)`)에 배치한다. 다만 해당 중요 데이터가 **적법한 공개 경로** 에서 수집되었거나, 특정 분야의 연구개발 역량을 끌어올리지도 않고 출력물로 유출될 수도 없도록 정제된 **0.1% 이하의 극미량 비중** 에 불과한 경우에는 명시적인 예외를 인정한다 CN-A1.
기반 모델의 주변부에서는 **266505X** 안의 네 개 제한 항목이 고성능 **AI 에이전트** 를 다룬다. 과업 계획기(≥ 20단계 분해, 분해 정확도 ≥ 80% 및 하위 과업 완수율 ≥ 90%), 다중 에이전트 군집(≥ 60개 동시 실행 에이전트), 도구 호출 엔진(≥ 200개 외부 소프트웨어 도구 연동 및 다중 도구 정확도 ≥ 90%), 그리고 인간 운용자의 90% 이상을 능가하는 200밀리초 미만의 실시간 의사결정 시스템이 그 대상이다. 이러한 에이전트가 국방, 핵심 기반시설, 또는 핵심 정부 업무를 전용 혹은 주된 목적 으로 제작된 경우에만 수출 금지안(`266502J`)으로 넘어간다 CN-A1.

중국 AI 목록 속 하드웨어 계층: 반도체 칩, 메모리, 그리고 1만 장급 클러스터

AI 항목에는 프로세서 설계, 메모리 설계와 대형 클러스터 기술도 포함됩니다.

- **AI 프로세서 설계도 (266506X 제1호 및 제2호):** 열거된 특성 중 어느 하나라도 충족하는 AI 프로세서 아키텍처, 맞춤형 명령어 집합, 연산 IP 코어, 기반 소프트웨어 스택 및 설계 도구의 수출을 제한하자고 제안한다, 여기에는 ≤ 14 nm 미세공정 설계, 2.5D/3D 칩렛 패키징, 신형 비(非)폰노이만·인메모리 컴퓨팅(CIM) 아키텍처뿐만 아니라 부동소수점·정수 연산 역량이나 스마트 음성·비전·자율주행 용도 같은 폭넓은 기능적 특성까지 포함된다 CN-A1, 266506X. 이 조항이 맞닿는 현장을 떠올려 보라. 오픈소스 하드웨어 프로젝트(예컨대 RISC-V 기반 AI 가속기), 맞춤형 NPU 스타트업, 다국적 칩 설계 엔지니어링 팀 모두가 영향권에 들어온다! 팹리스(fabless) 반도체 설계 팀은 물리적 실리콘을 찍어 내기 위해 완성된 회로 레이아웃을 해외 파운드리로 보내야만 하므로, **주석 2** 는 필수적인 안전밸브를 마련해야 했다. 바로 **해외 칩 테이프아웃을 위한 자동 허가 패스트트랙** (赴境外开展芯片流片制造)이다 CN-A1, note 2 CNQA.
- **메모리 설계(266506X 제2항):** 3D 플래시와 메모리 하위 항목이 다릅니다. 밀도·속도·접합 또는 18 nm 이하·수직 채널·적층 등은 대체 조건이며 모든 메모리의 공통 18 nm 기준이 아닙니다. CN-A1, 266506X(2)
- **슈퍼클러스터 배관망 (266507X 제1호~제4호): 1만 장을 훌쩍 넘는 가속기 카드** 위에서 프런티어 오픈 모델을 학습시키려면 클러스터가 매시간 멈춰 서지 않도록 지탱하는 고도의 산업적 마법이 필요하다. 네 개의 제한 항목은 ≥ 800 GB/s 노드 간 인터커넥트, ≤ 120 -second 자동 장애 복구, ≤ 1 -microsecond 집합 통신 라우팅, 그리고 **서로 다른 두 곳 이상의 하드웨어 제조사 칩을 하나의 학습 풀로 묶어 내는 이종(heterogeneous) 클러스터 소프트웨어** 를 통제한다 CN-A1, 266507X. 워싱턴이 엔비디아 GPU(`3A090`)를 조이고 베이징이 다중 제조사 클러스터 결합 기술(`266507X`)을 통제할 때, 오픈소스 분산 학습 프레임워크는 두 체제가 맞부딪치는 단층선 한복판에 놓이게 된다!

두 팀에 주는 의미

A의 메모리 개선과 B의 테스트는 교환 가능한 지식이며 컴퓨터는 별도의 의존 조건입니다. 공개 라이선스가 없는 칩을 공급하지 않으며 하드웨어 제한만으로 모든 모델 파일의 법적 지위가 정해지지 않습니다. 작업대의 두 부분을 함께 봅니다.
두 팀의 출발점은 요새의 함정: 양쪽이 함께 잃는 구조 에 있습니다.

04. 공개 모델: 공개와 비공개 이전

개방 라이선스는 공개의 일부

코드와 가중치를 공개하면 다른 연구자도 검토하고 수정하고 실행할 수 있습니다. 저작권 허가는 공개 조건의 일부입니다. 적용되는 수출, 데이터, 안전 규칙도 검토해야 합니다. DeepSeek-R1과 Qwen3의 공개는 모든 관련 활동의 면제를 뜻하지 않습니다. R1 QWEN



그림 10 파일과 지식을 받아 독립적으로 작업하는 것은 기본 모델을 다른 곳에 보관하는 서비스를 이용하는 것과 다릅니다.

실제 파일에서 시작하기

논문·다운로드 가중치·비공개 코드·후속 미세조정은 다릅니다. 공개 AI 정의는 자유·코드·매개변수·충분한 데이터 정보를 요구합니다. 일부만 제공할 수도 있으며 저작권 명칭이 수출 지위를 결정하지 않습니다. OSI

중국: 현재 등록과 목록 초안 구분

공고48은 미완료를 포함한 대상 이전 전에 등록을 요구합니다. 소유권·해외 허락·외국 지배·추가 공지가 포함됩니다. 목록 금지·허가와는 다른 단계입니다. 제안 금지만으로 새 현행 금지는 아니며 기존 법도 확인합니다. CN48 CN-A1

모든 공개에 필수 관문 네 개를 적용하기보다 전체 주석과 함께 읽습니다.

1. **이미 공개된 AI:** 주석1은 개방·논문으로 공개된 기술을 제외합니다. 무엇이 공개됐는지 확인합니다. 논문은 비공개 가중치를 공개하지 않으며 비공개 파생판은 모든 제외를 자동 승계하지 않습니다. CN-A1, note 1
2. **미공개 데이터 민감 기술:** 지정 핵심 데이터 모델은 금지, 중요 데이터는 제한 제안입니다. 미량 제외에는 0.1% 외 조건도 있습니다. 정확한 사실·해석이 필요합니다. CN-A1, 266501J and 266504X
3. **다른 비공개 대상 기술:** 대체 모델 기준과 함께 전달되는 에이전트·칩·클러스터를 확인합니다. 한 기준 미만이어도 다른 항목·기존 법·묶음 파일은 별개입니다. CN-A1
4. **편의 경로:** 주석2는 특정 공개 AI·해외 제조·자체 계산센터에 자동 허가 등을 제안합니다. 제외와 쉬운 허가는 다르고 최종 절차·조건이 중요합니다. CN-A1, note 2 CNQA

표 2 이전 전 별개의 세 가지 질문

질문	확인 사항
현재 중국 등록	아직 끝나지 않은 수출을 포함한 대상 기술과 이전.
중국 목록 초안	정확한 항목, 주석, 예외와 제안된 간소화 경로.
별도의 미국 규칙	대상이 EAR의 적용을 받는지 먼저 확인한 다음 분류와 적용 조건을 확인합니다.

미국: 별도 관할 검사

먼저 EAR 대상 여부를 봅니다. 공개 규정·4E091은 적격 공개 파일을 제외할 수 있습니다. 파생 모델에는 추가 학습 조건이 있어 사적 개선판은 원본과 자동으로 같지 않습니다. 불집행·GAO·규정 문구도 구분합니다. EAR734 EAR774, 4E091 notes GAO26

중국의 API·앱·웹·SaaS·경량 배포 설명은 제안된 제한 대형 모델에 관한 것입니다. 미국 보편 면제나 다른 중국 통제 승인이 아닙니다. 비공개 가중치 전달과 원격 서비스도 다릅니다. CNQA

공개 모델에 가능한 영향

공개 지속 은 편의와 일치합니다. **문서 증가·지연** , **공개 소형 모델과 비공개 서비스** , **학습 집중** 은 가능한 경로입니다. 조사할 문제이지 입증된 결과나 수치 예측은 아닙니다. CN-A1 CNQA NTIA 원인을 분리할 증거 없이 특정 효율 향상을 칩 통제 탓으로 단정하지 않습니다. 적은 매개변수가 제외를 보장하지 않으며 로컬 사용도 개인정보·안전·임상 신뢰성을 보장하지 않습니다.

독립 검토와 한계

공개하면 외부 팀도 모델을 검사하고 수정을 제안할 수 있습니다. 검토자가 늘어도 같은 사각지대나 테스트 자원 부족이 있을 수 있습니다. 결함 발견은 수정과 다릅니다. 선택: 독립 검토는 안전을 보장하지 않는다 의 선택 확률 예제가 한계를 설명합니다.

공개 가중치는 악용 수정·방호 제거도 돕습니다. NTIA는 2024년 이익·위험을 비교해 당시 모델 관찰을 권했습니다. 연구는 기존 대안 대비 추가 위험 비교를 요구합니다. 보편 안전 배수는 입증되지 않았습니다. NTIA OPENRISK

실용적인 공개 기록

버전·파일 해시·허락·공개/비공개 자료·데이터·측정·수령자·국가·이전 형태와 공개·절차 증거를 제안합니다. 새 의무나 공식 등록 양식 대체가 아닙니다. CN-A2

두 팀에 주는 의미

팀은 공개된 시작 모델을 유지합니다. 다음 기여는 논문, 새 코드, 비공개 가중치나 서비스일 수 있고 각각 평가가 필요합니다. 공개 정보 예외와 제안된 간소화 경로는 이야기의 넓은 장벽이 막을 특정 교환을 보존할 수 있어 중요합니다.
두 팀의 출발점은 요새의 함정: 양쪽이 함께 잃는 구조 에 있습니다.

05. 살아 있는 코드: 유전자 플랫폼과 공유되는 치료제

인쇄기는 지키되 그곳에서 찍어 낸 책은 세계와 나누다

인공지능이 부동소수점 숫자로 문장을 쓴다면, 현대 바이오의약은 네 글자로 이루어진 생명의 알파벳(`A, C, G, U/T`)으로 문장을 쓴다. 지난 10년 동안 중국의 바이오테크 연구진들은 특허가 만료된 복제약을 만들던 수준을 넘어, 해로운 단백질이 만들어지기 전에 질병 유발 유전자를 침묵시키는 반복 활용형 **세포·유전자 치료제(CGT)** 엔진과 **소간섭 RNA(siRNA)** 플랫폼을 독자 발명하는 단계로 도약했다.

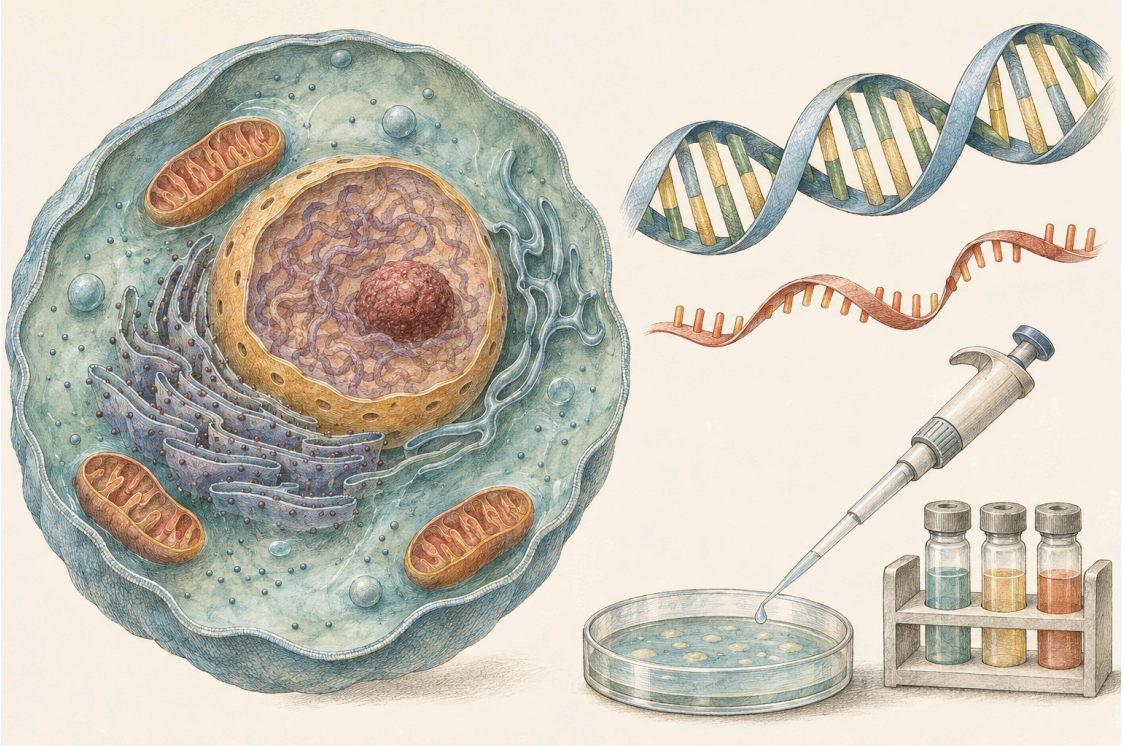


그림 11 세포, DNA, RNA와 실험 도구로 주제를 구체적으로 보여줍니다. 재사용 가능한 신약 개발 플랫폼은 개별 치료와 다릅니다.

초안은 재사용 가능한 신약 개발 플랫폼의 소유권과 개별 의약품 사업을 구분합니다. 대상 플랫폼의 소유권 이전을 제한하되 라이선스 등은 명시적으로 제외합니다. 이는 해당 항목의 예외이며 의약품과 임상시험에는 다른 규칙이 적용될 수 있습니다. CN-A1, 262704J and 262705J CNQA

기반이 되는 CGT나 siRNA 플랫폼을 10년에 걸쳐 완성한 맞춤형 **인쇄기** , 장차 스무 종의 신약을 찍어 낼 수 있는 전달 벡터와 화학적 안정화 레시피, 모듈형 설계 규칙의 집합체로 떠올려 보자. 그리고 특정 임상 신약 후보물질을 그 인쇄기에서 찍어 낸 **한 권의 책** 으로 그려 보자:

- **플랫폼 소유권 이전은 금지 제안(262704J·262705J)입니다.** 특정 재사용 플랫폼과 명시적 제외를 다룹니다. 공고48이 이미 확정 시행한 새 금지가 아닙니다. CN-A1
- **기술 수출(라이선스 아웃), 위탁개발생산, 개별 신약 파트너십은 그대로 열려 있다:** 두 항목 아래 달린 세 개의 명시적 주석은 해외 **라이선스 아웃** (对外授权许可), 소유권이 국내에 남는 조건의 **위탁 연구개발 및 위탁생산(CRO/CDMO)** , 그리고 글로벌 사업개발(BD) 거래에서 **특정 신약 후보물질의 비임상 연구, 임상시험, 제조, 품질관리, 인허가 승인 및 상업화** 에 필요한 일체의 파이프라인 데이터를 금지 범위에서 명확히 제외한다 CN-A1 CNQA. 오직 형식만 라이선스일 뿐 실질적으로 국내 소유권을 박탈하는 편법적 '영구 매절(buyout) 라이선스'만이 레드라인을 넘게 된다.

미공개 생물학적 신규 표적과 생물안보의 성벽

두 개의 **수출 제한안** 항목(`262705X` 및 `262706X`)은 CGT 및 siRNA 의약품 영역에서 **완전히 새로운 치료 표적** 을 발굴·검증하는 중국 보유 기술을 다룬다, 여기서 신규 표적이란 전 세계 특허, 학술지, 공개 데이터베이스, 산업 공시 자료, 학술대회 어디에서도 **이전에 단 한 번도 공개된 적이 없는** 분자 표적으로 엄격히 정의된다 CN-A1. 심지어 이 영역에서조차 **주석 3** 은 공중보건 위기 대응, 인도주의적 구호, 해외 자원을 활용한 국제 공동연구, 그리고 해외 라이선스 아웃에 대해 **자동 허가 간소화 혜택** 을 부여한다 CN-A1, note 3 CNQA.

다섯 번째 항목(`267302J`, 수출 금지안)은 병원체의 독성을 강화하거나 통제된 병원체의 진화 적응을 가속하는 인공 유전자 변형 및 유도 계대배양 기법을 차단하는 순수한 **생물안보 성벽** 이다 CN-A1, 267302J, 이는 미국 측의 카테고리 1 병원체 통제 및 `EAR 744.4` 규정과 정확히 궤를 같이 한다 EAR774 EAR744. *(한편 대량의 인간 유전체 데이터는 미국 법무부의 데이터 보안 프로그램 `DOJ <https://www.justice.gov/nsd/data-security>`_ 등 양국에서 별도의 데이터 보안 규제를 적용받는다.)*

두 팀에 주는 의미

의료의 공동 작업대는 플랫폼, 연구와 개별 치료를 다룹니다. 위 구분은 규칙이 어떤 협력을 다루고 무엇을 남기는지 묻게 합니다. AI 점수를 의료에 적용하거나 공개만으로 환자 안전을 입증한다고 가정하지 않습니다.

두 팀의 출발점은 요새의 함정: 양쪽이 함께 잃는 구조 에 있습니다.

06. 기계 속에 가둔 태양빛

태양광 패널은 실어 보낼 수 있어도 비밀 주방까지 내어 줄 수는 없다

공식 설명은 제조 기술과 제품을 구별합니다. 공고48은 완성 패널 전면 금지가 아니며 다른 통관 조치까지 판단하지는 않습니다. CNQA



그림 12 결정 성장로, 얇은 웨이퍼와 코팅 장비로 완성된 태양광 패널 뒤의 설비와 지식을 보여줍니다. 기계는 개략도입니다.

그렇다면 왜 **40개 기술 항목 중 무려 12개** (수출 금지안 5개, 수출 제한안 7개)가 태양광 제조 기술을 겨냥하고 있을까? 원석 상태의 석영을 초고순도 폴리실리콘으로 정제하고, 거대한 단결정 잉곳을 끌어 올리며, 복사용지보다 얇은 웨이퍼를 썰어 내고, 차세대 적층형(탠덤) 태양전지를 코팅하는 공정 전반에서 중국이 세계 최선두를 달리고 있기 때문이다. 각국 정부가 자국 내 태양광 공장을 세우기 위해 보조금을 풀고 수입 관세 장벽을 높이자, 베이징은 **산업 공정 레시피와 그 레시피를 몸체에 품은 물리적 공장 설비 모두** 에 국경선을 긋고 나섰다 CN-A1 CNQA:

1. **실리콘 고순도 정제 (263003J 및 263004X):** 수출 금지안은 초대형 냉수소화 유동층 공정(단일 라인 기준 삼염화실란 연간 생산량 $\geq 250,000$ tonnes/year)과 실란 유동층 공정(연간 $\geq 20,000$ tonnes/year)을 포괄하며, 수출 제한안은 연산 $\geq 30,000$ -tonne 규모의 폴리실리콘 플랜트 엔지니어링 패키지와 환원로 1기당 연산 ≥ 800 -tonne-per-furnace 이상의 환원 공정 레시피를 다룬다 CN-A1.

2. **잉곳 인상 및 종이보다 얇은 웨이퍼 절단 (263004J 및 263005X):** 두께 ≤ 70 micrometers 이하의 초박형 실리콘 웨이퍼 절단 기술은 제어 소프트웨어와 알고리즘, 기계 설계 도면을 포함해 **수출 금지안** (`263004J`)에 올랐다. 수출 제한안은 초대형 단결정 인상로(챔버 내경 $\geq 1,600$ mm 또는 등직경 소비전력 ≤ 40 kW), 길이 ≥ 720 mm 잉곳 정밀 가공, 직사각형 웨이퍼(≥ 182 mm), 그리고 ≤ 28 -micrometer 텅스텐 와이어 쏘를 이용한 ≤ 130 -micrometer 박형 웨이퍼 절단 기술을 포괄한다 CN-A1.
3. **탠덤 및 고효율 태양전지 (263801J 및 263802X):** 수출 금지안은 양산형 **페로브스카이트 및 실리콘-페로브스카이트 탠덤** 제조 기술(셀 효율 $\geq 30\%$, 폭 ≥ 1.1 -meter 슬롯다이 코터, 대형 탠덤 모듈 효율 $\geq 28\%$)과 박형 웨이퍼 에지 패시베이션(측면 부동태화) 공정을 지킨다. 수출 제한안은 고생산성 **TOPCon, 후면전극형(XBC), 이종접합(HJT)** 공정(셀 효율 $\geq 25\%$ 또는 모듈 효율 $\geq 22.3\%$)을 다룬다 CN-A1.

주석 4: 물리적 기계 설비 그 자체 가 레시피일 때

AI 소프트웨어를 AI 칩에서 떼어 놓을 수 없듯, 태양광 제조 노하우 또한 태양광 용광로에서 떼어 놓을 수 없다. 장비 공급사가 증착 반응기를 선적하고 내장 제어 코드를 설치한 뒤 해외 공장 현장에서 6개월 동안 현지 엔지니어들을 교육할 때, 하드웨어는 그 몸체 안에 지성을 고스란히 품고 바다를 건넌다.

초안 주4 는 해당 기술 기준을 구현한 반응기, 결정 성장로, 웨이퍼 절단기, 코팅 장비 등을 다룹니다. 대상 수출에는 현재 임시 사전 등록이 필요합니다. 채택된 최종 목록은 금지 기술과 허가가 필요한 제한 기술을 구분합니다. 허가는 금지된 이전을 허용하지 않으므로 최종 문구와 절차를 확인해야 합니다. CN-A1, note 4 CNQA CNMEAS

두 팀에 주는 의미

완성 패널, 제조 장비와 운용 지식은 다릅니다. 협력하는 공장 팀이 하나를 얻어도 나머지를 모두 얻지는 못합니다. 어떤 설비와 지식이 적용 규칙에 따라 함께 이동할 수 있는지가 질문입니다. 두 팀의 출발점은 요새의 함정: 양쪽이 함께 잃는 구조 에 있습니다.

07. 워싱턴의 문지기들: 실리콘 칩과 모델 가중치

전 지구적 연산의 물리적 엔진을 통제하다

태평양을 건너 워싱턴 D.C.로 가면 전 지구적 기술 국경 구조에서 더 오랜 역사를 지닌 하드웨어 중심의 나머지 절반과 마주하게 된다. 미국 상무부 산하 **산업안보국(BIS)** 이 **수출관리규정(EAR, 15 CFR Parts 730-774)** 에 따라 집행하는 미국 체제는 **최첨단 컴퓨팅 하드웨어, 반도체 설계 소프트웨어(EDA), 그리고 반도체 제조 장비** 에 대한 전 세계의 접근권을 규율한다 EAR734 EAR742 EAR774.

미국 수출 통제 체계와 맞닿는 모든 프로젝트는 순서대로 네 가지 질문 앞에 선다:

1. **EAR 대상인가:** 미국 소재·원산·지정 외국 물품에 조건·제외가 있습니다. 공개·연구·암호에는 세부 조건이 있습니다. 일부 미국 소프트웨어 이용만으로 모든 외국 칩이 대상은 아닙니다. EAR734
2. **수출통제분류번호(ECCN)는 무엇인가 (Part 774)?** 통제 대상 품목에는 상업통제목록(CCL) 상의 고유 코드가 부여되는데, 첨단 AI 가속기를 가리키는 **3A090** 과 특정 폐쇄형 프런티어 AI 모델 가중치를 가리키는 **4E091** 이 대표적이다 EAR774.
3. **목적지가 어디인가 (Part 742)?** 수출 허가 필요 여부는 목적지 국가군 분류에 따라 달라진다.
4. **최종 사용자와 최종 용도는 무엇인가 (Part 744)? 우려거래자 목록(Entity List, 744.11)** 등재 기관으로 향하거나 제한 대상 슈퍼컴퓨터, 첨단 공정 반도체, 혹은 대량살상무기 최종 용도(`744.23`, `744.4`)를 지원하는 거래는 평소라면 비통제 대상인 품목이더라도 별도의 수출 허가를 받아야 한다 EAR744.

2026년 1월 반도체 규정 개정: 문을 두드려 볼 자격을 준 것일 뿐 활짝 열린 문이 아니다

지난 3년 동안 중국으로 향하는 고성능 AI 데이터센터용 칩에는 원칙적 거부(presumptive denial) 방침이 적용되었다. 그러다 **2026년 1월 15일** , BIS는 정밀 조정된 하드웨어 규정(`91 FR 1684`, `15 CFR 742.6(b)(10)` 개정)을 발표했다. 칩의 성능이 **총연산성능(TPP) 21,000 미만** 및 **총 DRAM 대역폭 6,500 GB/s 미만** , 규정 본문에서 엔비디아 **H200** 과 AMD **MI325X** 가 대표 사례로 명시된 성능 구간에 해당할 경우, 미국에서 중국 또는 마카오 소재 최종 사용자에게 수출하는 적격 건에 한해 자동 거부 대신 **건별 허가 심사(case-by-case review)** 를 신청할 수 있도록 길을 연 것이다 US26 EAR742.

그러나 부속 조건을 꼼꼼히 읽어 보면 건별 심사는 신청서를 내 볼 자격을 뜻할 뿐 프리패스가 결코 아니다. 신청인은 미국 내 고객사가 공급 부족을 겪지 않는다는 점, 글로벌 파운드리 생산 물량이 미국 구매자 몫을 잠식하지 않는다는 점, 누적 출하량이 미국 내 공급량 대비 엄격한 비율 이내로 유지된다는 점, 철저한 물리적·사이버 보안 고객확인(KYC) 통제로 무단 원격 접속이

나 우려거래자 목록(Entity List) 대상자의 사용을 차단한다는 점, 그리고 수출 전에 **미국에 본사를 둔 독립 시험기관** 이 칩 성능을 직접 시험·검증했다는 점을 모두 입증해야 한다 US26, sections I and IV. 제3국을 통한 재수출에는 동일한 심사 경로가 자동으로 적용되지 않는다.

미국 AI 모델 가중치 규정(`4E091`)의 기묘한 법적 운명

워싱턴이 하드웨어 칩을 넘어 상위의 **AI 모델 가중치** 영역으로 통제를 확장하려 했을 때, 한 편의 흥미진진한 3막 법정 드라마가 펼쳐졌다:

- **제1막 (2025년 1월 15일):** BIS가 **인공지능 확산 프레임워크(AI 확산 규칙)** (`90 FR 4544`)를 공표하여 최소 10^{26} 연산량 이상으로 학습된 폐쇄형 모델 가중치의 수출에 허가제를 부과하는 ECCN **4E091** 을 신설하되, **공개적으로 이용 가능한 오픈 가중치 모델** (및 선도적 오픈 가중치 벤치마크 미만의 모델)은 **명시적으로 통제에서 제외** 했다 US25 EAR774, 4E091.
- **제2막 (2025년 5월 13일):** BIS가 공식 대체 입법이 이루어질 때까지 AI 확산 규칙을 **집행하지 말도록 단속 공무원들에게 지시했다** 고 보도자료를 통해 발표했다 USNE.
- **제3막(2026년5월12일):** GAO 결정 `B-337935` 는 비집행 정책을 의회심사법에 따라 제출해야 하는 규칙으로 판단했습니다. 폐지 절차가 시작되었지만 끝나지 않았다는 상무부 설명도 기록했습니다. 이는 의회 심사에 관한 결정이며 `4E091` 을 폐지하거나 집행하는 법원 판결이 아닙니다. 2026년11월2일 BIS의774부에 항목이 남아 있음을 별도로 확인했습니다. GAO26 EAR774

공개 가중치 조항은 중요하지만4E091에는 파생판 규칙이 있습니다. 장비·데이터·소프트웨어·문구·불집행은 별도 질문입니다. EAR734 EAR774 GAO26

워싱턴의 이웃한 두 관문: 벤처 투자 자금과 대량 민감 데이터

BIS 바로 옆에는 서로 다른 두 연방 문지기가 나란히 서 있다:

- **미 재무부 해외투자 안보 프로그램 (Outbound Investment Security Program): 2025년 1월 2일** 부터 중국의 반도체, 양자 기술, 특정 AI 시스템에 자금을 투자하는 미국인(US persons)은 투자 금지 또는 의무 신고 규정을 적용받는다. 이어 **2026년 10월 22일** , 재무부는 기술 임계치를 정교화하는 개정안에 대해(**2026년 12월 7일** 까지) 공개 의견 수렴을 개시했다 TREAS.
- **미 법무부 데이터 보안 프로그램 (Data Security Program):** 미국인의 민감 개인정보(유전체, 생체정보, 건강, 금융, 정밀 위치정보) 및 미국 정부 관련 데이터의 대량 국경 간 이전이나 접근을 엄격히 제한한다 DOJ.

두 팀에 주는 의미

게임의 A국과 B국은 가상입니다. 미중 통제는 범위, 기관과 컴퓨팅 공급망의 위치가 다릅니다. 이 장은 이를 설명하며 어느 실제 국가에도 3,5,17,20점을 매기지 않습니다.
두 팀의 출발점은 요새의 함정: 양쪽이 함께 잃는 구조 에 있습니다.

08. 두 개의 국경 체제와 공식 승인 획득 절차

하나의 프로젝트 안에서 마주치는 두 가지 통제 철학

중국의 제48호 공고를 미국의 수출관리규정(EAR) 옆에 나란히 펼쳐 놓으면, 두 초강대국이 똑같은 다리의 양 끝을 마주 보고 지키고 있는 풍경이 드러난다. 베이징은 **국내 독창 기술과 기업 소유권의 국외 유출** 을 지킨다, 중국에서 개발된 모델 핵심 기술, 반도체 설계도, 유전자 플랫폼, 태양광 제조 설비가 중국 밖으로 나가거나 외국 지배권 아래로 넘어가는지를 묻는 것이다. 반면 워싱턴은 **물리적 컴퓨팅 병목 자산에 대한 전 지구적 접근권과 우려 최종 사용자** 를 지킨다, 전 세계 어디에서든 칩과 제조 장비, 우려거래자 목록(Entity List) 등재 주체의 움직임을 추적하는 방식이다 CN48 EAR734 EAR742 EAR744.

표 3 중국 제48호 공고와 미국 BIS 수출관리규정(EAR) 통제 체제 핵심 비교

비교 항목	중국 (상무부·과학기술부 제48호 공고)	미국 (산업안보국 BIS 수출관리규정 EAR)
핵심 관할 기준	국내 기술 소유권의 국외 이전, 해외 사용 라이선스 부여, 또는 실질적 지배자(실제 통제인)의 해외 주체로의 변경 CN48 CNTIER.	미국산(US-origin) 품목, 미국 내 소재 품목, 그리고 해외직접생산품규칙(FDPR)에 따라 미국산 칩 소프트웨어·장비로 제조된 해외 생산 품목 EAR734.
하드웨어 및 실리콘	수출 제한안 `266506X` (14nm 이하 AI 칩, 칩렛, 18nm 이하 DRAM/HBM, 3D NAND), `266507X` (1만 장 초과 클러스터), 태양광 핵심 장비 열거된 CN-A1.	ECCN `3A090` AI 칩, 팹 장비 및 EDA 소프트웨어; 2026년 1월 `742.6(b)(10)` 개정에 따라 TPP <21,000 및 대역폭 <6,500 GB/s 이하 대(對)중국·마카오 칩 건별 심사 US26 EAR742.
프런티어 AI 가중치	제안266504X(2)는10^26회·2조 매개변수·적격 상위10위 중 하나입니다.266501J는 금지 제안이고 서비스 설명은 한정적입니다. CN-A1 CNQA	성문 법규 `4E091` (>=10^26 연산 폐쇄형 가중치); 2025년 5월 BIS 미집행 지시가 내려졌으나 2026년 5월 GAO 결정 `B-337935` 에서 법적 다툼 발생 US25 USNE GAO26.
오픈소스 AI	**주석 1** 로 이미 공개된 오픈소스 AI·논문 제외; **주석 2** 로 신규 오픈소스 공개 및 해외 칩 테이프아웃에 자동 허가 간소화("신청 즉시 처리") 부여 CN-A1.	**15 CFR 734.7** (공개 정보) 및 **4E091 주석** 에 따라 접근 제한 없이 공개된 오픈소스 코드와 오픈 모델 가중치는 수출 허가 제외 EAR734 EAR774.
온라인 신청 포털	`https://ecomp.mofcom.gov.cn` (상무부 업무시스템 통합 플랫폼, 기술무	`https://snapr.bis.gov` (SNAP-R 접수 포털) 및 `https://snapr.bis.gov/public/stela`

비교 항목	중국 (상무부·과학기술부 제48호 공고)	미국 (산업안보국 BIS 수출관리규정 EAR)
	역 관리정보 애플리케이션) CN48 CNPLAT.	(STELA 심사 현황 조회) EAR734 SNAPR.

중국·싱가포르의 가상 연구실이 대상 칩을 쓰고 사적 기술을 해외 허락합니다. 장비·용도는 미국, 이전은 중국 등록과 관계될 수 있습니다. 하나로 둘 다 충족하지는 않습니다. CN48 EAR734 EAR744

단계별 실무 가이드: 공식 등록 및 승인 신청 방법

수출 통제를 다룬 대부분의 글이 불길한 경고만 던진 채 멈추어 버리기 때문에, 일선의 창업자와 오픈소스 메인테이너, 대학 연구자, 장비 구매 담당자들은 지극히 현실적인 질문 앞에 홀로 남겨지곤 한다. "만약 우리의 모델 공개나 칩 테이프아웃, 기술 제휴가 실제로 이 규정 안에 들어온다면 도대체 어느 정부 부처가 담당하고, 어떤 온라인 포털을 열어야 하며, 승인까지 며칠(영업일)이 걸리고, 어디로 전화하거나 이메일을 보내야 하는가?"
그림 13 에서 신고에 필요한 문서를 소개합니다. 아래에 국가별 절차와 연락처를 설명합니다。 CN48 CN-A2 CNTIER CNMEAS CNPLAT EAR734 EAR742 SNAPR



그림 13 연구자가 기술 문서를 제출해 검토를 받습니다. 서류 작업의 소개이며 완전한 법적 절차나 승인 보장은 아닙니다.

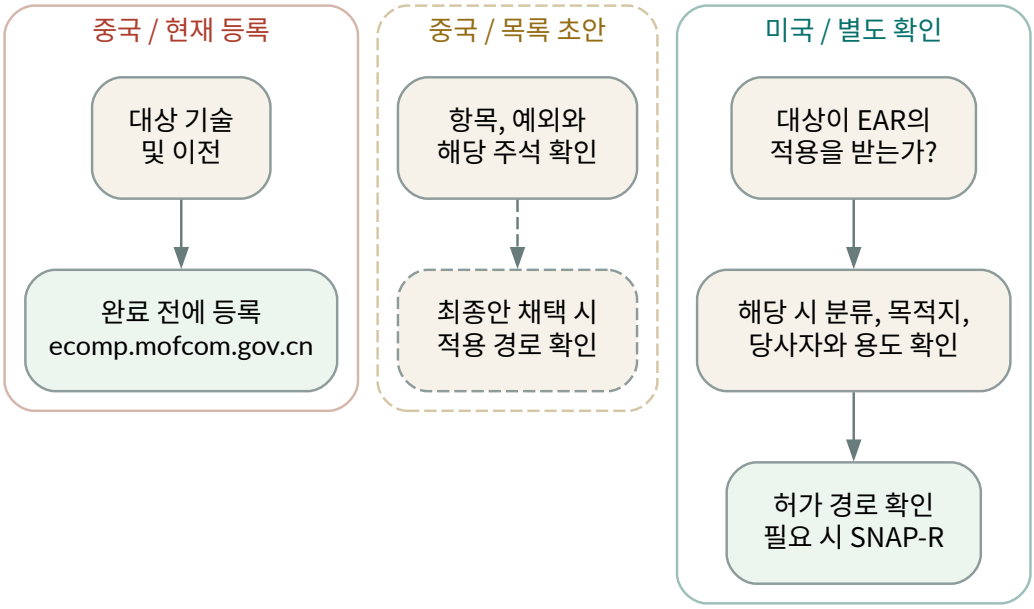


그림 14 중국의 현재 등록, 중국 목록 초안과 미국 관할은 별개의 확인입니다. 점선은 제안된 경로입니다.

중국: 소관 정부 부처, 법정 처리 기한 및 검증된 연락처

중국의 기술 수출 행정은 《중화인민공화국 기술수출입관리조례》(中华人民共和国技术进出口管理条例, 제30~39조)와 《수출금지·수출제한 기술 관리방법》(禁止出口限制出口技术管理办法, 2009년 상무부·과학기술부령 제2호, 제4~18조)에 따라 **중앙과 성(省)급 지방 당국의 협력 체계** 로 운영된다. 베이징의 **상무부(MOFCOM)** 와 **과학기술부(MOST)** 가 국가 기준을 제정하고 통합 온라인 포털을 운영하며, 수출 제한 기술에 대한 정식 허가 심사와 발급은 수출자가 등록된 소재지의 **성급 상무 주관부서** 와 **성급 과학기술 행정부서** 가 담당한다 CN48 CNTIER CNMEAS.

> **중요**
> **기간 범위:** 30·15근무일은 기존 표준 절차입니다. 총45일 보장이나 임시 등록·미래 자동 허가 기한이 아닙니다. 협상·서류·추가 심사가 더 걸릴 수 있으며 연락처도 현재 정보를 확인합니다.

중국에서의 세 가지 공식 신고·신청 경로

1. **경로 A: 의무적 수출 전 정보 등록 (2026년 10월 16일부터 현재 즉시 시행 중):**
   - **신청 시점:** 부속서 1의 40개 항목 중 어느 하나에 대해 국내 기술 소유권을 국외로 이전하거나, 해외 사용 라이선스를 부여하거나, 국내 기술 소유자·실질적 지배자를 해외 주체로 변경하기 전(10월 16일 이전 시작되어 아직 완료되지 않은 진행 중 거래 포함) CN48, section III.
   - **신청 방법: 상무부 업무시스템 통합 플랫폼** (`https://ecomp.mofcom.gov.cn`)에 접속해 **기술무역 관리정보 애플리케이션** (技术贸易管理信息应用)을 선택한 뒤 **부속서 2** (《기술수출 정보등록표》: 공식 법인 직인 公章, 기술 소유권자 정보, 해외 인수자의 명칭·국가·주소·관계, 7자리 목록 코드, 기술 지표, 최종 용도, 미화 환산 계약 금액 기재)를 제출한다 CN48 CN-A2 CNPLAT.
2. **경로 B: 오픈소스, 칩 테이프아웃 및 자체 클라우드 패스트트랙 (주석 2 및 3의 "자동 허가" 제안):**

- **적용 대상:** 개정 목록이 정식 발효된 이후 제한 등급 AI 기술을 오픈소스로 공개하거나, **중국 기업이 자체 구축·운영하는 해외 연산 센터** 에 모델을 배포하거나, **파운드리 테이프아웃** (芯片流片)을 위해 반도체 설계도를 해외로 전송하거나, 국제 공동 연구개발 및 표준화 활동을 수행하거나, 라이선스 아웃·인도주의 구호를 목적으로 제한 등급 바이오의약 표적 기술을 수출하는 경우 CN-A1, notes 2 and 3.
- **제안 내용:** 자동 허가 등 편의이지 완전한 최종 절차나 시간 보장은 아닙니다. 담당 기관에 확인합니다. CN-A1 CNQA

3. **경로 C: 표준 2단계 수출 제한 기술 수출 허가증 (技术出口许可证):**
   - **1단계: 실질적 협상 개시 또는 계약 체결 전 (최대 30영업일):** 소재지 **성급 상무 주관부서** (省、自治区、直辖市商务主管部门)에 《중국 수출제한 기술 신청서》(中国限制出口技术申请书)를 제출한다 CNMEAS, Arts. 4-5. 성급 상무청은 **5영업일** 이내에 기술 자료를 **성급 과학기술 행정부서** (省、自治区、直辖市科技行政主管部门)로 이첩하며, 과학기술청은 전문가를 소집해 **15영업일** 이내에 기술 심사를 마친다 CNMEAS, Art. 7. 접수일로부터 **총 30영업일** 이내에 당국이 승인 여부를 결정하며, 승인 시 **최대 3년** 동안 유효한 **기술수출 허가의향서** (中华人民共和国技术出口许可意向书)를 발급한다 CNTIER, Arts. 35-36 CNMEAS, Arts. 6, 10. *(법정 의무 규정: 이 허가의향서를 취득하지 않은 상태에서는 그 어떤 기관이나 개인도 실질적인 수출 협상을 진행하거나 법적 구속력이 있는 약정을 맺을 수 없다 `CNMEAS, Art. 11 <https://www.mofcom.gov.cn/dl/file/20211203230621.pdf>`_.)*
   - **2단계: 계약 체결 후 본허가 (최대 15영업일):** 계약을 체결한 뒤 온라인 시스템에 계약 정보를 등록하고, 성급 상무청에 **(i)** 기술수출 허가의향서, **(ii)** 서명된 계약서 사본, **(iii)** 기술자료 수출 목록(技术资料出口清单), **(iv)** 계약 양 당사자의 법적 지위 증명 서류를 제출한다 CNTIER, Art. 37 CNMEAS, Arts. 13, 16. 성급 상무청은 계약의 진위 여부를 심사하여 **15영업일** 이내에 결정하고 정식 **기술수출허가증** (中华人民共和国技术出口许可证)을 발급한다 CNTIER, Arts. 37-38 CNMEAS, Art. 14. **핵심 법정 원칙:** 수출 제한 기술의 수출 계약은 기술수출허가증이 발급된 날로부터 비로소 법적 효력이 발생 하며, 수출자는 이 허가증을 제시해야만 **세관 통관, 외환, 은행 결제 및 세무** 절차를 처리할 수 있다 CNTIER, Art. 38 CNMEAS, Arts. 15, 18 CNQA.

검증된 중국 정부 공식 연락처 편람

- **중앙 주관 부처 (목록 정책, 적용 범위 및 공개 의견 수렴):** 중화인민공화국 상무부 산업안보수출입통제국(中华人民共和国商务部安全与管制局) 및 과학기술부(科学技术部) 합동 CN48.
- **우편 주소:** 중국 베이징시 둥창안제 2호 상무부 산업안보수출입통제국, 우편번호 100731: No. 2 Dongchang'an Avenue, Beijing 100731, China (北京市东长安街2号商务部安全与管制局，邮编：100731) CN48.
- **공식 의견 수렴 및 정책 문의 이메일:** `jinxianmulu@mofcom.gov.cn` *(2026년 11월 15일까지 진행되는 공개 의견 제출 시 제목에* 《中国禁止出口限制出口技术目录》公开征求意见 *을 명기하고, 기관·법인 명의로 제출할 경우 연락처와 함께 법인 직인을 날인하여 첨부)* CN48.
- **공식 팩스:** `+86-10-6519-7565` (`010-65197565`) CN48.
- **통합 온라인 사전 등록 및 허가 포털:** `https://ecomp.mofcom.gov.cn`, 기술무역 관리정보 애플리케이션 (商务部业务系统统一平台 - 技术贸易管理信息应用, 기존 `jsjckqy.fwmys.mofcom.gov.cn` 통합) CN48 CNMEAS, Art. 16 CNPLAT.
- **통합 플랫폼 기술지원 전화:** `+86-10-6787-0108` (`86-10-67870108`) CNPLAT.
- **지방 수출 허가 심사 당국:** 수출자 등록 소재지의 성·자치구·직할시 상무 주관부서 및 과학기술 행정부서 (所在地省、自治区、直辖市商务主管部门会同科技行政主管部门) CNMEAS, Art. 4.

미국: 소관 연방 기관, SNAP-R 업무 절차 및 검증된 연락처

미국에서는 이중용도 하드웨어, 소프트웨어 및 기술 수출 허가를 연방 차원에서 **미국 상무부 (U.S. Department of Commerce)** 산하 **산업안보국(BIS)** 이 일원화해 관장하며, 전자 신청에 대한 정부 접수 수수료는 무료다 EAR734 EAR742 SNAPR.

미국 수출 통제 분류 판정 및 허가 승인을 위한 4단계 절차

1. **관할·공개부터:** 734.3·734.7·734.8·4E091을 확인합니다. 공개로 EAR 밖인 것과 한 목적지에 허가 불필요는 다릅니다.744는 주로 대상 물품, 다른 제재·미국인 규칙은 따로 봅니다. EAR734 EAR744 EAR774
2. **2단계: SNAP-R 포털에서 기업식별번호(CIN) 발급:** 통제 대상 하드웨어(`3A090`), 반도체 장비, 또는 비공개 통제 기술을 수출하는 당사자는 BIS의 **간소화 네트워크 신청 프로세스(SNAP-R)** 포털(`https://snapr.bis.gov`)에서 온라인으로 CIN을 등록한다(미국 내 소재 주체는 수출 허가를 신청하며, 해외 소재 주체도 재수출 허가나 품목 분류 판정을 직접 신청할 수 있다) EAR734 SNAPR.
3. **3단계: 분류가 불확실할 때 품목 분류(CCATS) 또는 정책 질의 접수:** `snapr.bis.gov` 포털에서 품목 분류 작업 항목(Commodity Classification Work Item)으로 기술 사양서를 제출해 공식 ECCN 판정(`ACN` 추적 번호 부여)을 받거나, BIS 규제정책과(Regulatory Policy Division)에 규정 유권해석을 문의한다 EAR734 SNAPR.
4. **4단계: 수출 허가 신청서 제출 및 STELA 진행 상황 추적:** 증빙 문서 PDF, 최종 사용자 진술서, 기술 사양서를 업로드한다(`742.6(b)(10)` 조항에 따른 2026년 1월 대(對)중국·마카오 반도체 심사의 경우 `TPP < 21,000`, `DRAM bandwidth < 6,500 GB/s`, 미국 내 공급 충분성, KYC 보안 통제, 미국 소재 독립 시험기관 검증 인증서를 함께 첨부) US26 EAR742 SNAPR. 이후 **STELA** 시스템(`https://snapr.bis.gov/public/stela`)에서 심사 진행 현황을 실시간으로 조회한다 EAR734.

검증된 미국 연방 정부 공식 연락처 편람

- **전자 허가 접수 및 심사 조회 포털:** SNAP-R 접수 포털: `https://snapr.bis.gov` | STELA 심사 현황 조회: `https://snapr.bis.gov/public/stela` EAR734 SNAPR.
- **SNAP-R 헬프데스크 및 계정 지원:** 기술 지원 헬프데스크: `snapr@bis.doc.gov` | 계정 복구 및 수권임원(Empowered Official) 서한 접수: `ECDOEXS@bis.doc.gov` SNAPR.
- **BIS 대외협력·교육서비스과 (워싱턴 D.C. 본부):** U.S. Department of Commerce, 14th and Pennsylvania Avenue, NW., Room H1099D, Washington, DC 20230 | 전화: `+1 (202) 482-4811` | 팩스: `+1 (202) 482-2927` EAR734.
- **BIS 서부 지역사무소 (남부 캘리포니아):** 2302 Martin St., Suite 330, Irvine, CA 92612 | 전화: `+1 (949) 660-0144` | 팩스: `+1 (949) 660-9347` EAR734.
- **BIS 북부 캘리포니아 지부 (실리콘밸리):** 160 W. Santa Clara Street, Suite 725, San Jose, CA 95113 | 전화: `+1 (408) 998-8806` | 팩스: `+1 (408) 998-8677` EAR734.
- **BIS 규제정책과 (Regulatory Policy Division):** Room 2099B, U.S. Department of Commerce, Washington, DC 20230 | 전화: `+1 (202) 482-2440` | 이메일: `RPD2@bis.doc.gov` US25 US26 EAR742.
- **BIS 분야별 기술 담당관 (반도체 및 AI):** 카테고리 3 반도체(`3A090`): Carlos Monroy, `+1 (202) 482-3246`, `Carlos.Monroy@bis.doc.gov` US25 US26 | 카테고리 4 컴퓨터 및 AI 모델 가중치(`4E091`): Aaron Amundson, `+1 (202) 482-0707`, `Aaron.Amundson@bis.doc.gov` US25.
- **미 재무부, 해외투자 안보 프로그램 (Outbound Investment Security Program):** `https://home.treasury.gov/policy-issues/international/outbound-investment-program` | 일반 문의: `Outbound@treasury.gov` | 법규 문의: `OIS.Outbound.Regulations@treasury.gov` | IT 기술지원: `Outbound.ITSupport@treasury.gov` TREAS.
- **미 법무부, 데이터 보안 프로그램 (국가안보국 산하):** `https://www.justice.gov/nsd/data-security` | 컴플라이언스 문의: `NSD.FIRS.datasecurity@usdoj.gov` | 대외 공보: `nsd.public@usdoj.gov` DOJ.

두 팀에 주는 의미

작업대 이야기는 실제 질문이 됩니다. 무엇을 이전하고 어떤 체계가 다루며 어느 경로가 남는가? 명확한 예외, 이용 가능한 절차와 신뢰할 지속 협력이 유인을 바꿀 수 있습니다. 효과에는 근거가 필요하며 서류 작성만으로 협력 개선을 알 수 없습니다.

두 팀의 출발점은 요새의 함정: 양쪽이 함께 잃는 구조 에 있습니다.

09. 일상의 질문들: 독자를 위한 실전 현장 가이드

내 하드웨어에 딥시크(DeepSeek), 큐웬(Qwen) 등 오픈 모델을 계속 내려받아 써도 될까?

공고는 공개 다운로드를 전면 금지하지 않습니다. 비공개 조정·데이터·재이전은 별도이며 원본 다운로드가 모든 파생·용도를 승인하지 않습니다. CN-A1, note 1 EAR734 EAR774

소프트웨어 라이선스가 MIT나 Apache 2.0이어도 하드웨어가 오픈소스 AI에 영향을 미치는가?

결정적인 영향을 미친다. MIT 라이선스가 모델을 실행할 법적 권리 를 부여한다면, 물리적 GPU와 고대역폭 메모리, 클러스터 인터커넥트는 모델을 학습시키거나 구동할 물리적 능력 을 부여하기 때문이다. 미국 규정(`3A090`, `742.6(b)(10)`)은 누가 첨단 AI 가속기를 구매할 수 있는지를 통제하고, 중국이 제안한 `266506X` 및 `266507X` 항목은 AI 프로세서 아키텍처, 3D NAND·DRAM 메모리 설계, 1만 장 초과 클러스터 엔지니어링의 국경 간 이전을 통제한다(다만 주석 2가 해외 파운드리 테이프아웃을 간소화해 준다) CN-A1 US26 EAR742. 따라서 언제나 소프트웨어 파일뿐만 아니라 그와 함께 움직이는 맞춤형 실리콘 설계나 클러스터 스택까지 함께 점검해야 한다.

해외 사용자가 우리 AI 앱과 대화하거나 API를 호출하면 그것도 모델 수출인가?

공식 답변은 제안 이후 제한 대형 모델 서비스를 구분합니다. API 등은 핵심 데이터·다른 물품·데이터 법·현재 등록의 보편 면제가 아닙니다. CNQA

연구소는 중국에 그대로 있는데 해외 투자자가 지배권을 인수한다면 등록해야 하는가?

즉시 점검해야 한다. 제48호 공고 제3조 제2항은 모든 서버와 엔지니어가 중국 내에 그대로 남더라도 **대상 국내 기술의 소유자 또는 실질적 지배자(실제 통제인)가 해외 주체로 변경** 될 때마다 수출 전 정보 등록을 마치도록 요구한다 CN48, section III(2). 만약 미국계 투자자가 거래에 참여한다면 미 재무부의 해외투자 안보 규정(`Outbound@treasury.gov`)도 별도로 확인해야 한다 TREAS.

공개 버튼을 누르기 전 두 장짜리 '릴리스 여권'에는 무엇을 기록해 두어야 할까?

주요 오픈 가중치 모델 공개, 해외 파운드리 칩 테이프아웃, 또는 국경 간 라이선스 계약을 실행하기 전에는 깔끔한 내부 관리 폴더 하나를 만들어 여섯 가지를 기록해 두는 것이 좋다. **(1)** 정확한 버전명과 SHA-256 해시값, **(2)** 대조 점검한 목록 코드(`266504X`, `266506X`, `266507X`, `3A090`, `4E091`), **(3)** 실측 학습 FLOPs와 파라미터 수 및 공개 당일 기준 공개 벤치마크 순위, **(4)** 핵심 데이터 무사용 확인 및 공개·극미량 중요 데이터 내역을 담은 학습 데이터 감사서, **(5)** 기존 공개 이력 증빙 또는 최초 공개 여부, 그리고 **(6)** `ecomp.mofcom.gov.cn` 등록 사본이나 `snapr.bis.gov` ACN 접수 사본이다 CN-A1 CN-A2 SNAPR.

여섯 가지 실전 시나리오

> **참고**
> **실전 예시 안내:** 아래 여섯 가지 사례는 검증된 규정들이 실제 현장에서 어떻게 작동하는지 보여 주기 위한 예시이므로, 실제 의사결정 전에는 반드시 개별 프로젝트의 구체적 사실관계와 정부 공식 원문을 대조해야 한다.

1. 이미 공개된 기존 오픈 가중치 모델을 미세조정하는 경우
가상 병원팀이 공개 가중치를 적응합니다. 원본과 후속 비공개 임상판은 다르며 공개·데이터·재이전을 확인합니다. 저작권은 안전 증명이나 정부 승인이 아닙니다. CN-A1, note 1 EAR734 EAR774
2. 중국 연구소가 글로벌 Top 10급 신작 오픈소스 모델을 최초 공개하는 경우
중국의 한 AI 연구소가 새로 학습시킨 추론 모델을 전 세계에 최초로 오픈소스 업로드하려는데, 실시간 벤치마크 평가에서 세계 7위를 기록해 `266504X(2)` 기준을 넘어섰다. 우선 중국 핵심 데이터(`266501J`)가 전혀 쓰이지 않았음을 확인하고 중요 데이터 극미량 예외 기준을 점검한다. 2026년 10월 16일 이후의 전환 기간에는 `ecomp.mofcom.gov.cn` 포털에서의 수출 전 정보 등록 요건을 확인하고, 최종 개정 목록이 발효된 뒤에는 **주석 2의 자동 허가 패스트트랙** ("신청 즉시 처리")을 이용하면 된다 CN48 CN-A1, note 2 CNQA.
3. 비공개 프런티어 가중치나 맞춤형 반도체 IP를 해외 파트너에게 상업 라이선스하는 경우
베이징의 한 기술 기업이 비공개 상업 계약을 맺고 미공개 2.4조 파라미터 가중치(`266504X`)나 맞춤형 7nm NPU 명령어 집합 코어(`266506X`)를 해외 기업에 인도하려 한다. 이는 오픈소스 공개가 아닌 비공개 상업 이전이므로, 오늘 당장 `ecomp.mofcom.gov.cn` 포털에서 **부속서 2 수출 전 정보 등록** 을 완료하고, 목록 확정 이후에는 **성급 상무청 + 성급 과학기술청의 2단계 수출 허가** (허가의향서 30영업일 + 정식 기술수출허가증 15영업일) 절차를 밟을 준비를 해야 한다 CN48 CNTIER CNMEAS. *(참고: 오직 파운드리 웨이퍼 위탁 제조만을 위해 회로 레이아웃을 해외로 전송하는 테이프아웃은 주석 2의 간소화 특례 대상이 된다.)*
4. 전 세계 사용자를 대상으로 웹 채팅이나 종량제 API 서비스를 제공하는 경우
상하이의 한 스타트업이 중국 내 서버에 호스팅된 주력 프런티어 모델을 기반으로 웹 인터페이스와 HTTPS API를 통해 해외 고객에게 서비스를 제공한다. 상무부 공식 Q&A는 기반 가중치나 소스 코드를 넘기지 않는 원격 API 및 앱 서비스가 (수출 금지 대상인 핵심 데이터 `266501J` 로 학습된 모델이 아닌 한) **거대 모델 기술 수출 통제 대상 바깥** 에 있음을 명확히 확인하고 있다 CN-A1 CNQA.
5. 해외 벤처 자본 유치에 따른 지배구조 개편 또는 국경 간 인수합병
미공개 `266505X` 60개 에이전트 오케스트레이션 소프트웨어나 미공개 `262705X` 유전자 치료 신규 표적 발굴 엔진을 보유한 국내 스타트업이 역외 지주회사가 실질적 지배자가 되도록 지배구조를 개편한다. 설령 선전(深圳) 서버에서 단 한 개의 파일도 국외로 나가지 않더라도, 제48호 공고 제3조 제2항에 따라 **지배권 이전이 완료되기 전에 수출 전 정보 등록** 을 마쳐야 한다, 아울러

미국 자본이 참여하는 경우에는 미 재무부의 해외투자 안보 규정도 병행 검토해야 한다 CN48, section III(2) TREAS.

6. 태양광 웨이퍼 또는 페로브스카이트 턴키 생산 라인을 해외에 선적하는 경우

중국의 한 장비 제조사가 해외 신설 태양광 공장에 단결정 인상로와 PECVD 코팅 설비를 납품하면서 공정 레시피와 엔지니어 현장 시운전 교육을 함께 제공하는 계약을 맺었다. **주석 4** 에 따라 해당 물리적 기계 설비가 `263004X``~``263802X` 구간의 기술 지표를 구현하고 있다면 장비 자체가 수출 통제 대상이 된다(나아가 `<=70 micrometer` 초박형 웨이퍼 절단 `263004J` 또는 `>=30%` 탠덤 셀 레시피 `263801J` 는 수출 금지안에 해당한다). 따라서 이행 완료 전에 반드시 `ecomp.mofcom.gov.cn` 수출 전 정보 등록을 마쳐야 한다 CN48 CN-A1, note 4 CNQA.

10. 1차 사료, 검증 방법론, 그리고 쉬운 용어 사전

이 책의 모든 사실은 어떻게 검증되었는가

2026년 11월 2일 기준 26개 법률·기술·연구 자료와 대조했습니다. 새 연구는 협력·위험 분석을 돕지만 가정을 실측으로 만들지 않습니다. 연락처는 인용 기록의 내용으로 바뀔 수 있습니다. WPS 원본 파일의 바이트 데이터와 SHA-256 해시값은 일체의 변형 없이 그대로 보존되어 열람용 PDF 변환본과 함께 제공된다. GAO 서버가 자동화된 바이트 아카이빙을 차단한 경우(`HTTP 403`)에는 그 한계 또한 투명하게 명시했다. 본문 전체에 걸쳐 1차 법령 사실에는 대괄호 인용 표기를 달았으며, 게임이론 보수 행렬과 미래 시나리오는 특정 거래에 대한 법률 자문이 아닌 이론적 분석 모델임을 분명히 밝힌다.

무수정 공식 원문 사본 다운로드

- 제48호 공고 공식 웹페이지 (열람용 PDF 사본)
- 부속서 1: 40개 신설 제안 기술 목록 (원본 WPS) | 변환 PDF 열람본
- 부속서 2: 기술수출 정보등록표 양식 (원본 WPS) | 변환 PDF 열람본
- 2009년 상무부·과학기술부령 제2호: 수출금지·수출제한 기술 관리방법 (공식 PDF)
- 미국 BIS 2026년 1월 반도체 규정 91 FR 1684 (공식 PDF)
- 미국 BIS 2025년 1월 AI 확산 프레임워크 90 FR 4544 (공식 PDF)
- 미국 BIS 공식 SNAP-R 전자 신청 가이드 및 FAQ (공식 PDF)
- 기계 판독용 사료 출처 및 SHA-256 해시 매니페스트 (sources.json)

일반 독자를 위한 쉬운 용어 사전

모델 가중치 (파라미터)
: 모델 출력에 영향을 주는 학습한 수치입니다. 가중치만으로 재현 가능하고 안전한 시스템의 모든 요소가 갖춰지지는 않습니다.

체크포인트 (Checkpoint)
: 학습 도중이나 종료 시점에 저장해 둔 가중치 스냅샷 파일로, 학습을 이어서 진행하거나 소형 모델을 증류하거나 전문 과업용으로 미세조정할 때 쓰인다.

FLOPs (부동소수점 연산 횟수)
: 모델 학습 과정에서 수행되는 개별 수학 연산 횟수다. 10^{26} **FLOPs** (1 뒤에 0이 26개 붙는 수)는 중국이 제안한 `266504X`와 미국의 `4E091` 모두가 채택한 프런티어 연산 임계치다.

TPP 및 HBM (하드웨어 병목 지표)
: **총연산성능(TPP)** 은 AI 칩의 순수 연산 처리량을 재는 지표이고, **고대역폭 메모리(HBM / DRAM 대역폭)** 는 칩 안으로 데이터가 얼마나 빠르게 공급되는지를 재는 지표다(2026년 1

월 미국의 대중국 건별 심사 규정 `742.6(b)(10)` 에서는 각각 `TPP < 21,000` 및 `6,500 GB/s` 미만이 상한선이다).

칩 테이프아웃 (芯片流片)
반도체 설계 팀이 완성한 프로세서 회로 설계도를 물리적 실리콘 웨이퍼로 제조하기 위해 파운드리 공장으로 넘기는 최종 공정 단계다, 제48호 공고 주석 2에서 자동 허가 간소화 대상으로 명시되어 있다.

API / SaaS (베이커리 판매 창구)
기반 모델 가중치나 소스 코드, 반도체 설계도를 직접 넘겨주지 않고, 원격 사용자가 클라우드 서버로 질문을 보내 답변만 받아 가도록 하는 서비스 방식이다.

내시 균형
누구도 자기 선택만 바꿔 더 나아질 수 없는 조합입니다. 안전·공정·사회 최선일 필요는 없습니다. 상호 장벽은 이 예의 가정 아래에서만 균형입니다. GAME

소프트웨어 라이선스 vs. 기술수출 허가증
MIT 또는 *Apache 2.0* 라이선스는 창작자가 누구나 코드나 가중치를 재사용할 수 있도록 허용하는 사적 저작권 허락이다. 반면 기술수출허가증 (`技术出口许可证` 또는 미국 BIS 허가증)은 통제 대상 기술이나 하드웨어가 국경을 넘을 수 있도록 주권 국가 정부가 발급하는 공적 행정 허가다.

자동 허가 (自动许可)
제한 등급 AI의 오픈소스 공개, 자체 보유 해외 클라우드, 해외 칩 테이프아웃, 인도주의 바이오의약 협력을 위해 제48호 공고 주석에서 제안된 "신청 즉시 처리"(`即报即出`) 방식의 간소화된 정부 허가 경로다.

ECCN, CCATS 및 SNAP-R
미국 수출 통제 체제에서 **ECCN** (AI 칩은 `3A090`, 모델 가중치는 `4E091`)은 통제 품목 분류 번호를 뜻하며, **SNAP-R** (`snapr.bis.gov`)은 수출자가 수출 허가 신청서와 **CCATS** 공식 품목 분류 판정 요청서를 무료로 제출하는 전자 포털이다.

검증된 26개 1차 사료 전체 등록부

표 4 2026년 11월 2일 기준 검증을 완료한 1차 법령·규제·기술 문헌 목록

사료 코드	공식 문헌 명칭 및 검증 범위	일자	원문 URL 및 SHA-256 해시 앞자리
`CN48`	중국 상무부·과학기술부, 2026년 제48호 공고 (제1·2·3조 전문)	2026-10-16	mofcom.gov.cn (`a5261a74...`)
`CN-A1`	제48호 공고 부속서 1: 40개 신설 제안 기술 항목 및 4개 주석 (WPS 원본)	2026-10-16	원본 WPS (`213158bb...`)
`CN-A2`	제48호 공고 부속서 2: 기술수출 정보 등록표 양식 (WPS 원본)	2026-10-16	원본 WPS (`d65818c2...`)
`CNQA`	제48호 공고에 관한 중국 상무부 대변인 공식 기자 문답(Q&A)	2026-10-16	mofcom.gov.cn (`37fc685a...`)
`CNTIER`	중국 국무원, 《중화인민공화국 기술수출입관리조례》 (제30~39조)	2020-11-29	xzfg.moj.gov.cn (`39f4b9bb...`)
`CNMEAS`	2009년 상무부·과학기술부령 제2호, 《수출금지·수출제한 기술 관리방법》	2009-04-20	mofcom.gov.cn PDF (`d14e5230...`)
`CNPLAT`	상무부 업무시스템 통합 플랫폼 공지 및 기술지원 안내 (`+86-10-6787-0108`)	2026-11-02	mofcom.gov.cn (`5bc9740f...`)
`US26`	미국 BIS 반도체 수출 허가 심사 최종 규칙 (`91 FR 1684; 742.6(b)(10)`)	2026-01-15	govinfo.gov (`d3b27863...`)

사료 코드	공식 문헌 명칭 및 검증 범위	일자	원문 URL 및 SHA-256 해시 앞자리
US25	미국 BIS 인공지능 확산 프레임워크 (90 FR 4544; 4E091)	2025-01-15	govinfo.gov (6e202458...)
USNE	AI 확산 규칙 미집행 지시에 관한 미국 BIS 공식 보도자료	2025-05-13	bis.gov (14a05e6e...)
GAO26	AI 확산 규칙 및 의회검토법(CRA) 적용에 관한 미 연방회계감사원(GAO) 결정 B-337935	2026-05-12	gao.gov *(HTTP 403;* 웹 열람 검증*)*
EAR734	15 CFR Part 734: EAR 적용 범위, 공개 오픈소스 면제(734.7) 및 연락처	2026-11-01	bis.gov/ear/734 (eeb76281...)
EAR742	15 CFR Part 742: 상업통제목록(CCL) 기반 통제 정책 (742.6(b)(10))	2026-11-01	bis.gov/ear/742 (3eccf859...)
EAR744	15 CFR Part 744: 최종 사용자 및 최종 용도 기반 통제 (744.11, 744.23)	2026-11-01	bis.gov/ear/744 (ab19c823...)
EAR774	15 CFR Part 774: 상업통제목록(CCL) (ECCN 3A090 및 4E091)	2026-11-01	bis.gov/ear/774 (01d3beba...)
SNAPR	미국 BIS SNAP-R 전자 신청 FAQ 및 연락처 안내서 (snapr.bis.gov)	2026-11-02	snapr.bis.gov PDF (e0c3bdee...)
TREAS	미 재무부 해외투자 안보 프로그램 및 2026년 10월 규칙 개정안	2026-10-22	home.treasury.gov (75f52eee...)
DOJ	미 법무부 국가안보국(NSD), 데이터 보안 프로그램	2026-11-02	justice.gov/nsd (1bf01adb...)
OSI	오픈소스 이니셔티브(OSI), 오픈소스 AI 정의 1.0 (OSAID 1.0)	2024-10-28	opensource.org (a5442179...)
R1	DeepSeek-R1 공식 저장소 및 MIT 라이선스 기록	2025-01-20	github.com/deepseek-ai (875b282c...)
QWEN	Qwen3 공식 저장소 및 Apache 2.0 라이선스 기록	2025-04-29	github.com/QwenLM (2b7cdab9...)
GD	GuideDog 문서 및 도서 출판 엔진 (v1.0.0-beta.10)	2026-11-02	github.com/insanai/guidedog (6fe7704f...)

이번 검토에 추가한 연구·역사 자료

- NTIA: 2024년 7월 공개 가중치 보고서. 당시 모델의 이익·위험·관찰을 평가하며 모든 미래 모델의 증거는 아닙니다. Dual-Use Foundation Models with Widely Available Model Weights (July 2024)
- OPENRISK: 공개 기반 모델의 사회적 영향 연구입니다. 추가 위험 논의와 수출 통제의 인과적 측정을 구별합니다. On the Societal Impact of Open Foundation Models
- GAME: 네트워크·시장 교재 제1장으로 게임·최적 대응·균형을 정의합니다. 점수와 반복 계산은 책의 자체 예입니다. A Course in Networks and Markets, Chapter 1
- JEFFERSON: 1813년 8월 13일 Isaac McPherson에게 쓴 편지입니다. 촛불 인용의 원전이지 경제 효과 증명은 아닙니다. Thomas Jefferson to Isaac McPherson, 13 August 1813

저자·협력자와 재사용

저자 **Vikrant Rathore** , 도움 **Jennifer Yuan, Vicky Ni, Ronak Rathore, Kanak Rathore** .
원본 글·편집·새 삽화는 **CC BY-SA 4.0** 입니다. 출처 표시와 같은 조건의 2차 공유가 필요합니다. 공식 문서·인용·글꼴·소프트웨어·제3자 자료는 원래 권리와 라이선스를 유지합니다. LICENSE와 NOTICE를 참고합니다.

7개 판은 독립 법률·원어민 전문 검토를 받지 않은 편집 번역입니다. 원문 법률이 우선하며 사례·점수는 공식 분류나 실측 예측이 아닙니다.

선택: 게임 예제 계산 확인

도입 이야기는 계산 없이 이해할 수 있습니다. 확인하려는 독자를 위해 추가 가정을 명시합니다.

결말이 안정적인 이유

20 >17 >5 >3이라는 순서는 상대와 무관하게 제한할 이유를 줍니다. 양쪽 장벽 아래 혼자 공유하면 5에서 3이 됩니다. 상호 공유는 이 작은 게임에서 파레토 효율적입니다. 나열된 다른 결과로 어느 한쪽을 악화하지 않고 다른 쪽을 개선할 수 없습니다. 각자의 개인 최고 점수라는 뜻은 아닙니다. GAME

미래 협력이 중요해질 때

다음 계산은 가상 점수를 각 단계에서 비교 가능한 보수로 취급하는 가정을 추가합니다. 수치 기준은 선호 순서뿐 아니라 이 척도에 달려 있습니다.
국가는 반복 교류합니다. 둘 다 공유하면 협력하며 이탈은 한 번20, 그 뒤 영원히5라고 가정합니다. δ 는 다음 회차의 현재 대비 가치입니다. 협력이 적어도 유리한 조건은:

$$\frac{17}{1-\delta} \geq 20 + \frac{5\delta}{1-\delta} \quad \Longleftrightarrow \quad \delta \geq \frac{1}{5}$$

가정 게임의 계산이지 외교 예측이 아닙니다. 무기한 관계·관찰 가능한 행동·믿을 만한 대응을 전제합니다. 실수·숨은 행동·알려진 마지막 회차는 이를 깨뜨립니다. 지속 협력을 믿게 만드는 방법이 질문입니다. GAME

선택: 독립 검토는 안전을 보장하지 않는다

개방은 독립 검사·수리를 돕습니다. 결함 존재 확률이 p_0, 각 독립 팀의 탐지 확률이 q, 팀 수가 n 이면:

$$P(\text{flaw remains undetected}) = p_0(1-q)^n$$

존재하는 결함과 탐지 절반 가정에서 한 팀 누락50%, 네 팀6.25%, 열 팀 약0.098%입니다. 조건부 계산입니다. 실제 팀은 같은 맹점·자원 부족·미수리가 있을 수 있어 전체 사이버·생물·사회 위험 측정은 아닙니다.
공개 가중치는 악용 수정·방호 제거도 돕습니다. NTIA는 2024년 이익·위험을 비교해 당시 모델 관찰을 권했습니다. 연구는 기존 대안 대비 추가 위험 비교를 요구합니다. 보편 안전 배수는 입증되지 않았습니다. NTIA OPENRISK