# 048 오픈소스 AI

Open-Source AI

**AI 모델과 코드를 공개해 누구나 수정·활용할 수 있도록 한 구조**

- AI의 알고리즘, 학습 데이터, 모델 매개변수, 코드 등을 공개해 누구나 접근·수정·배포할 수 있게 하는 개방형 AI 개발 방식
- 기술 협력과 투명성을 높이는 동시에, 보안·윤리 위험도 함께 존재

## 오픈소스 AI의 개념

오픈소스 AI는 AI의 핵심 구성 요소인 모델, 학습 코드, 데이터, 알고리즘 등을 공개해 누구나 자유롭게 사용·수정·재배포할 수 있도록 하는 개방형 개발 체계를 의미합니다. 기존의 상용 AI가 기업 내부에서 폐쇄적으로 관리되는 것과 달리, 오픈소스 AI는 연구자·기업·개발자가 공동으로 모델을 발전시키는 협력 기반 생태계를 지향합니다. Meta의 LLaMA, Stability AI의 Stable Diffusion 등이 대표적 예로, 이러한 개방적 구조는 기술 발전 속도를 높이고 특정 기업 중심의 기술 집중을 완화합니다.

## 오픈소스 AI의 확산

오픈소스 AI는 주로 코드 저장소(예, GitHub)나 모델 공유 플랫폼(예, Hugging Face)을 통해 배포됩니다. 개발자는 공개된 모델을 다운로드해 새로운 데이터로 재학습하거나 알고리즘을 수정해 자신만의 응용 모델을 만들 수 있으며, 다시 커뮤니티에 공유함으로써 순환적 발전 구조가 형성됩니다. 이런 방식은 AI 모델을 단일 제품이 아닌 공동 지식 자산으로 만들며, 오픈소스 생태계 특유의 피드백 문화가 지속적인 품질 개선을 이끕니다. 확산의 배경에는 대형 AI 기업이 독점하는 폐쇄형 생태계에 대한 견제와, AI 기술의 민주화 흐름이 있습니다. 클라우드 인프라와 GPU 자원의 확산, 학습 비용 절감, 정부의 데이터 개방 정책도 오픈소스 AI 성장의 기반이 되었습니다. 그 결과, 대학·스타트업·공공기관까지 참여할 수 있는 개방형 AI 혁신 구조가 전 세계적으로 빠르게 확산되고 있습니다.

## 오픈소스 AI의 위험

오픈소스 AI의 개방성은 기술 확산을 가속하지만 동시에 보안·윤리·법적 위험을 수반합니다. 모델의 가중치와 학습 데이터가 공개되면 악의적인 사용자가 이를 조작하거나 부적절한 콘텐츠를 생성할 수 있으며, 허위 정보·딥페이크·사이버 공격용 코드 등이 확산될 가능성도 있습니다. 또한 학습 데이터에 포함된 개인정보, 저작권 문제, 국가별 규제 차이 등으로 인해 법적 분쟁이 발생할 위험이 큽니다. 오픈소스 모델을 충분히 검증하지 않고 상용 서비스에 적용할 경우, 편향된 결과나 사회적 차별이 강화될 수 있습니다. 따라서 오픈소스 AI의 발전은 개방성과 책임성의 균형을 전제로 해야 하며, 신뢰 가능한 사용 지침과 글로벌 거버넌스 마련이 필수적입니다.