파이토치
한국 사용자 모임

오픈소스 AI와 AI 테크맵

AI 시대, 변화하는 오픈소스 기준 및 활용 방안 제안

박정환 파이토치 한국 사용자 모임 (PyTorchKR)

9bow@pytorch.kr

파이토치
한국 사용자 모임

시작하며

Introduction

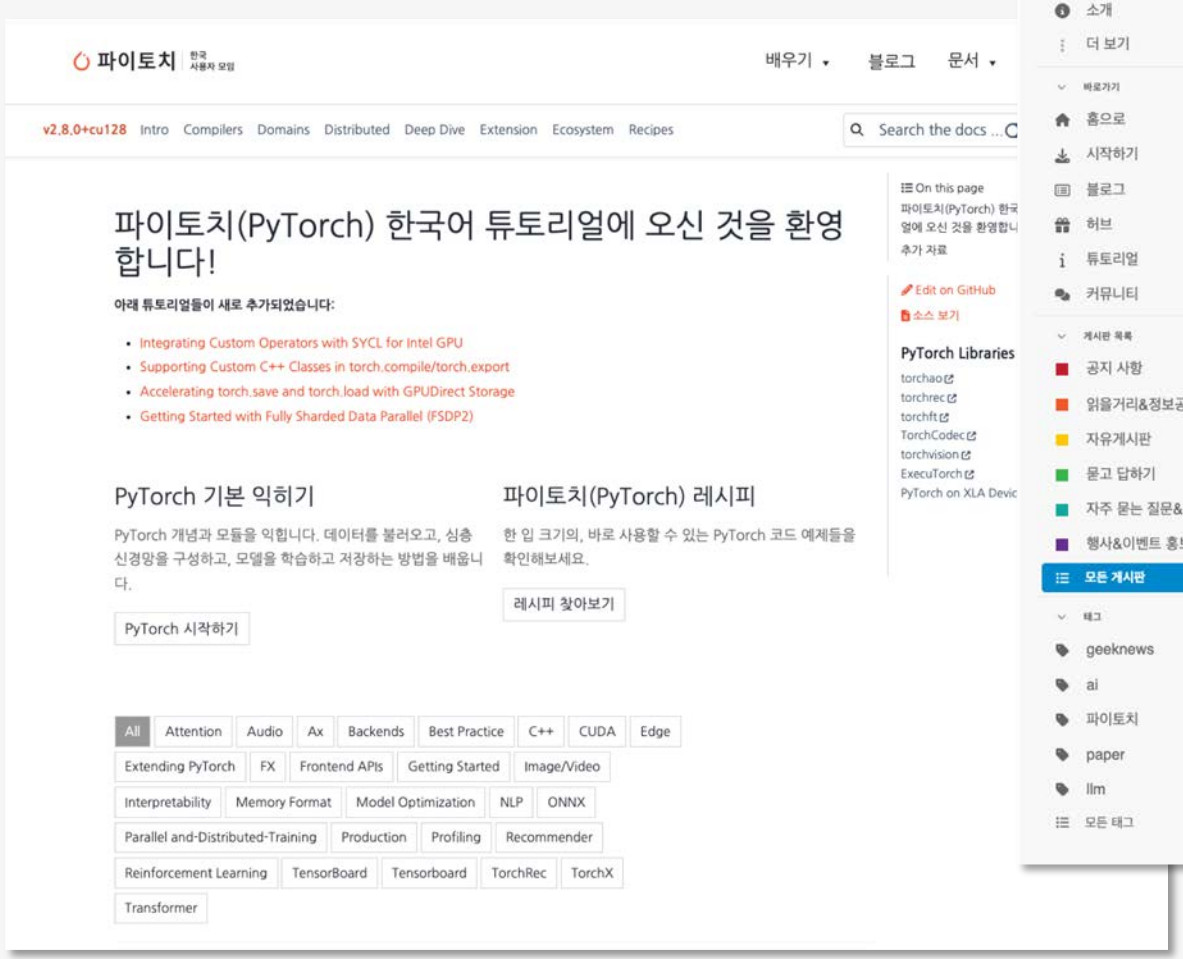
발표자 소개

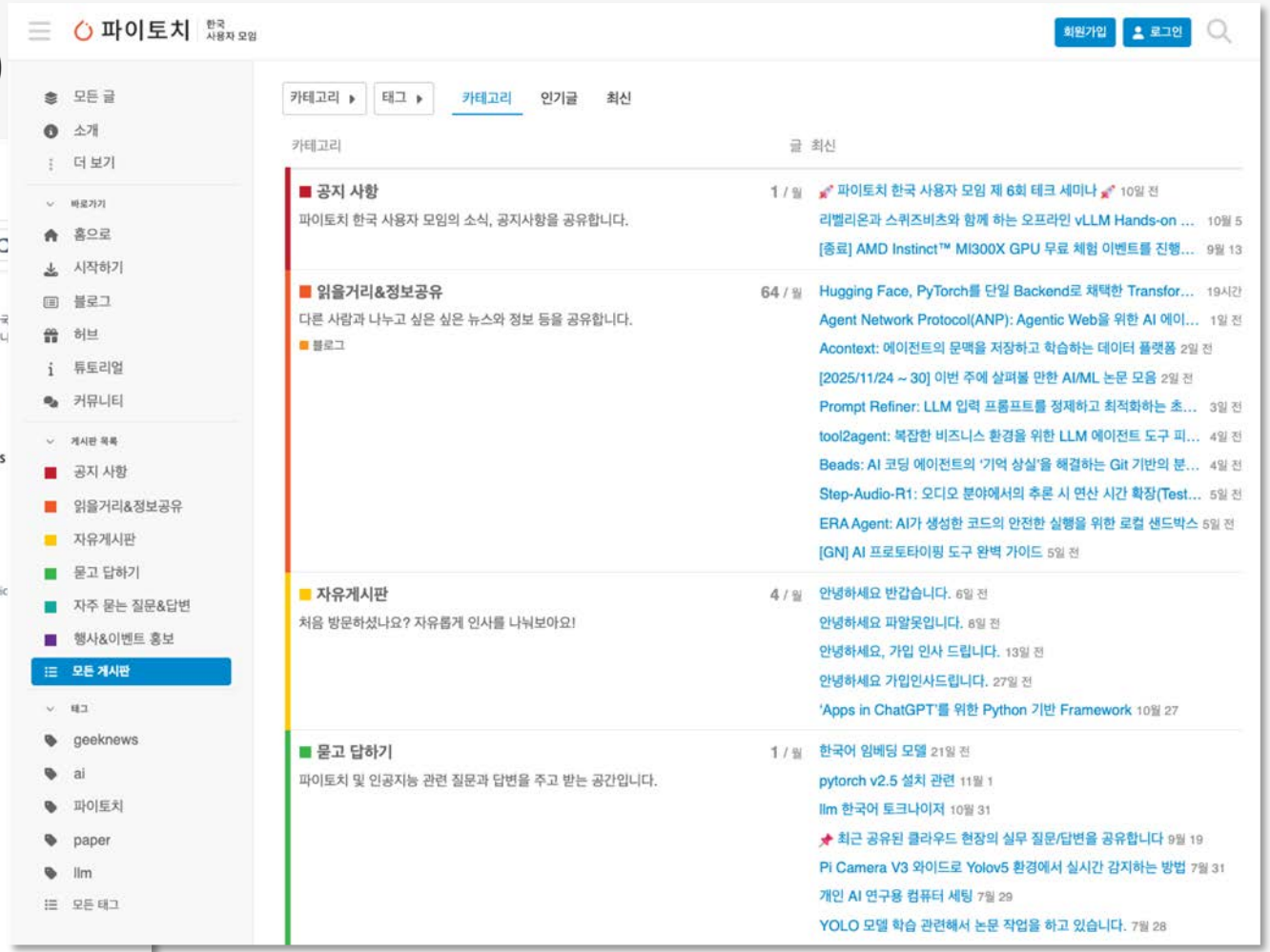
박 정 환 (9bow)

- ✓ 파이토치 한국 사용자 모임, 운영자
- ✓ PyTorch Ambassador, 2025/09 ~
- ✓ PyTorch Community Award, 2023/10
- ✓ Microsoft MVP Awards, 2007 ~ 2011
- ✓ 오픈소스, 커뮤니티, 멀티모달 및 시계열 예측

PyTorchKR 소개

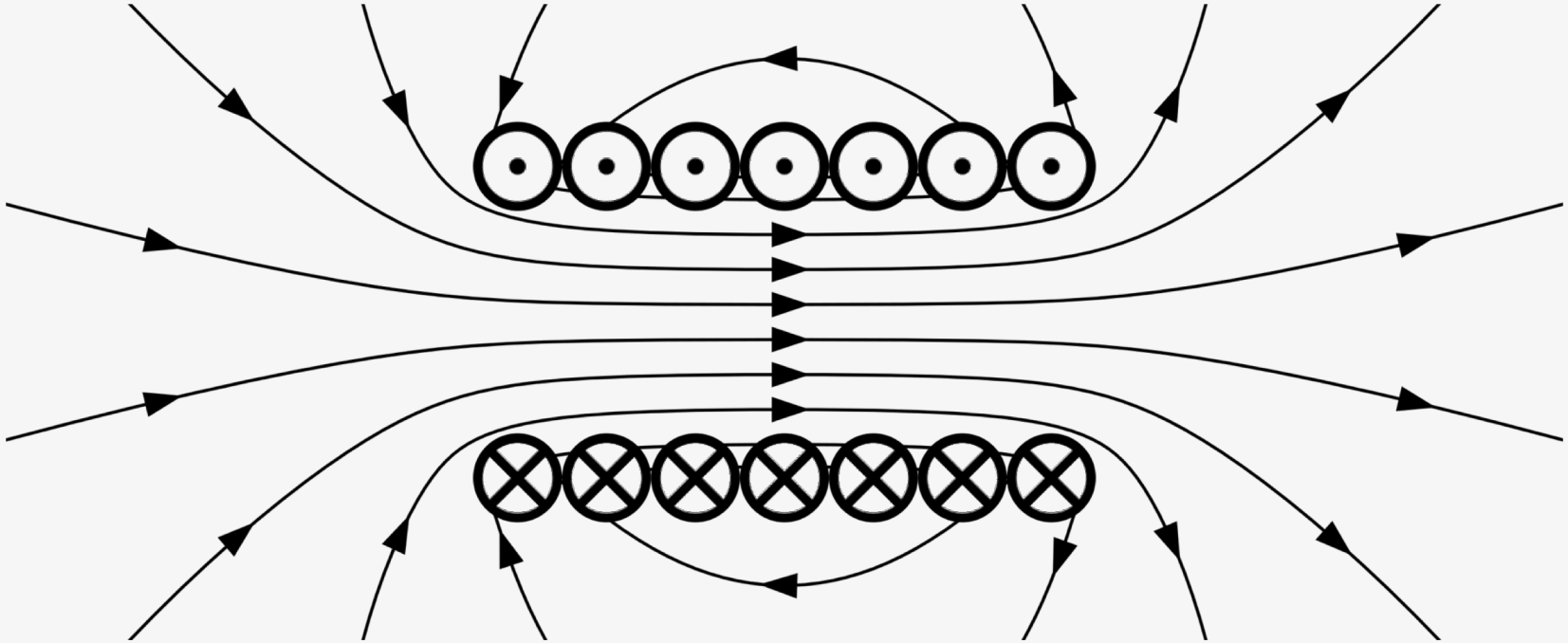
파이토치 한국어 튜토리얼 (tutorials.pytorch.kr)





파이토치 한국어 커뮤니티 (discuss.pytorch.kr)

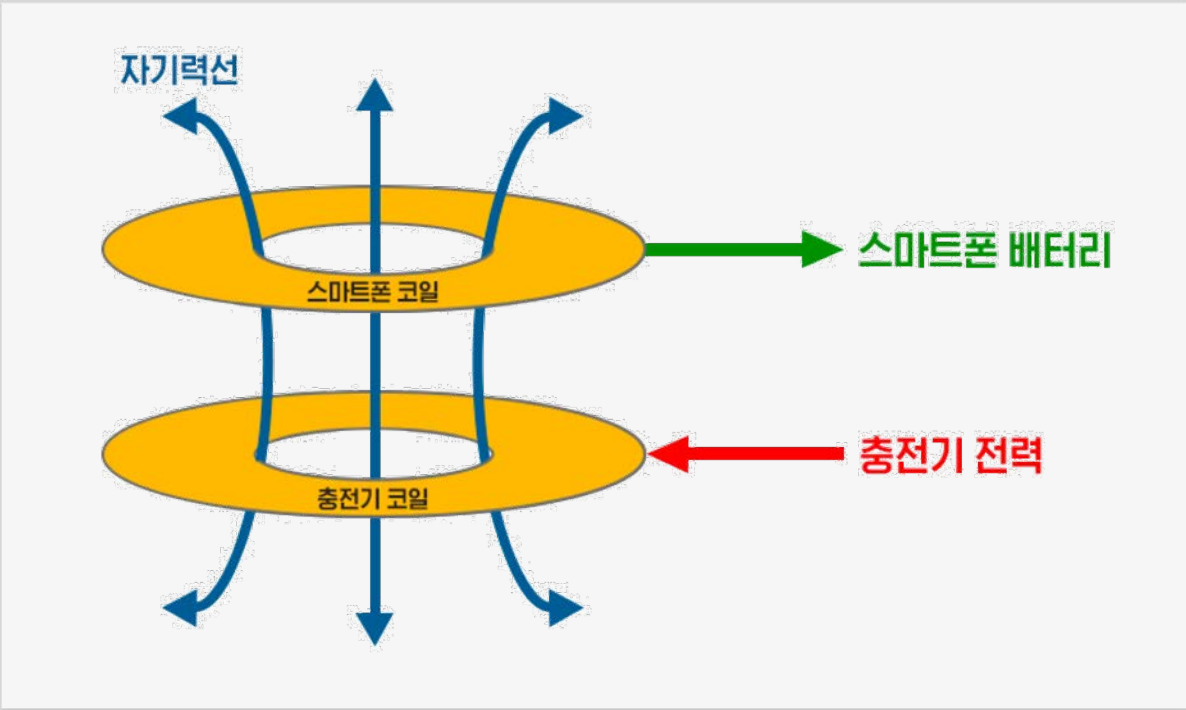
발표 소개



$$\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$$

출처: Wikipedia, '전자기 유도'

발표 소개



출처: 삼성디스플레이 뉴스룸

발표 소개

Consider the time-derivative of magnetic flux through a closed boundary (loop) that can move or be deformed. The area bounded by the loop is denoted as $\Sigma(t)$), then the time-derivative can be expressed as

$$\frac{\mathrm{d}\Phi_B}{\mathrm{d}t} = \frac{\mathrm{d}}{\mathrm{d}t}\int_{\Sigma(t)} \mathbf{B}(t)\cdot\mathrm{d}\mathbf{A}$$

The integral can change over time for two reasons: The integrand can change, or the integration region can change. These add linearly, therefore:

$$\left.\frac{\mathrm{d}\Phi_B}{\mathrm{d}t}\right|_{t=t_0} = \left(\int_{\Sigma(t_0)} \left.\frac{\partial \mathbf{B}}{\partial t}\right|_{t=t_0}\cdot\mathrm{d}\mathbf{A}\right) + \left(\frac{\mathrm{d}}{\mathrm{d}t}\int_{\Sigma(t)} \mathbf{B}(t_0)\cdot\mathrm{d}\mathbf{A}\right)$$

where t_0 is any given fixed time. We will show that the first term on the right-hand side corresponds to transformer emf, the second to motional emf (from the magnetic Lorentz force on charge carriers due to the motion or deformation of the conducting loop in the magnetic field). The first term on the right-hand side can be rewritten using the integral form of the Maxwell–Faraday equation:

$$\int_{\Sigma(t_0)} \left.\frac{\partial \mathbf{B}}{\partial t}\right|_{t=t_0}\cdot\mathrm{d}\mathbf{A} = -\oint_{\partial\Sigma(t_0)} \mathbf{E}(t_0)\cdot\mathrm{d}\mathbf{l}$$

Next, we analyze the second term on the right-hand side:

$$\frac{\mathrm{d}}{\mathrm{d}t}\int_{\Sigma(t)} \mathbf{B}(t_0)\cdot\mathrm{d}\mathbf{A}$$

The proof of this is a little more difficult than the first term; more details and alternate approaches for the proof can be found in the references.[27][28][29] As the loop moves and/or deforms, it sweeps out a surface (see the right figure). As a small part of the loop $\mathrm{d}\mathbf{l}$ moves with velocity $\mathbf{v}_\mathbf{l}$ over a short time $\mathrm{d}t$, it sweeps out an area whose vector is $\mathrm{d}\mathbf{A}_{\text{sweep}} = \mathbf{v}_\mathbf{l}\,\mathrm{d}t \times \mathrm{d}\mathbf{l}$ (note that this vector is toward out from the display in the right figure). Therefore, the change of the magnetic flux through the loop due to the deformation or movement of the loop over the time $\mathrm{d}t$ is

$$\mathrm{d}\Phi_B = \int \mathbf{B}\cdot\mathrm{d}\mathbf{A}_{\text{sweep}} = \int \mathbf{B}\cdot(\mathbf{v}_\mathbf{l}\mathrm{d}t\times\mathrm{d}\mathbf{l}) = -\int \mathrm{d}t\,\mathrm{d}\mathbf{l}\cdot(\mathbf{v}_\mathbf{l}\times\mathbf{B})$$

The area swept out by a vector element $\mathrm{d}\mathbf{l}$ of a loop $\partial\boldsymbol{\Sigma}$ in time $\mathrm{d}t$ when it has moved with velocity $\mathbf{v}_\mathbf{l}$.

Here, identities of triple scalar products are used. Therefore,

$$\frac{\mathrm{d}}{\mathrm{d}t}\int_{\Sigma(t)} \mathbf{B}(t_0)\cdot\mathrm{d}\mathbf{A} = -\oint_{\partial\Sigma(t_0)} (\mathbf{v}_\mathbf{l}(t_0)\times\mathbf{B}(t_0))\cdot\mathrm{d}\mathbf{l}$$

where $\mathbf{v}_\mathbf{l}$ is the velocity of a part of the loop $\partial\boldsymbol{\Sigma}$.

Putting these together results in,

$$\left.\frac{\mathrm{d}\Phi_B}{\mathrm{d}t}\right|_{t=t_0} = \left(-\oint_{\partial\Sigma(t_0)} \mathbf{E}(t_0)\cdot\mathrm{d}\mathbf{l}\right) + \left(-\oint_{\partial\Sigma(t_0)} (\mathbf{v}_\mathbf{l}(t_0)\times\mathbf{B}(t_0))\cdot\mathrm{d}\mathbf{l}\right)$$

$$\left.\frac{\mathrm{d}\Phi_B}{\mathrm{d}t}\right|_{t=t_0} = -\oint_{\partial\Sigma(t_0)} (\mathbf{E}(t_0)+\mathbf{v}_\mathbf{l}(t_0)\times\mathbf{B}(t_0))\cdot\mathrm{d}\mathbf{l}.$$

출처: Wikipedia, ‘Faraday's law of induction’

발표 소개

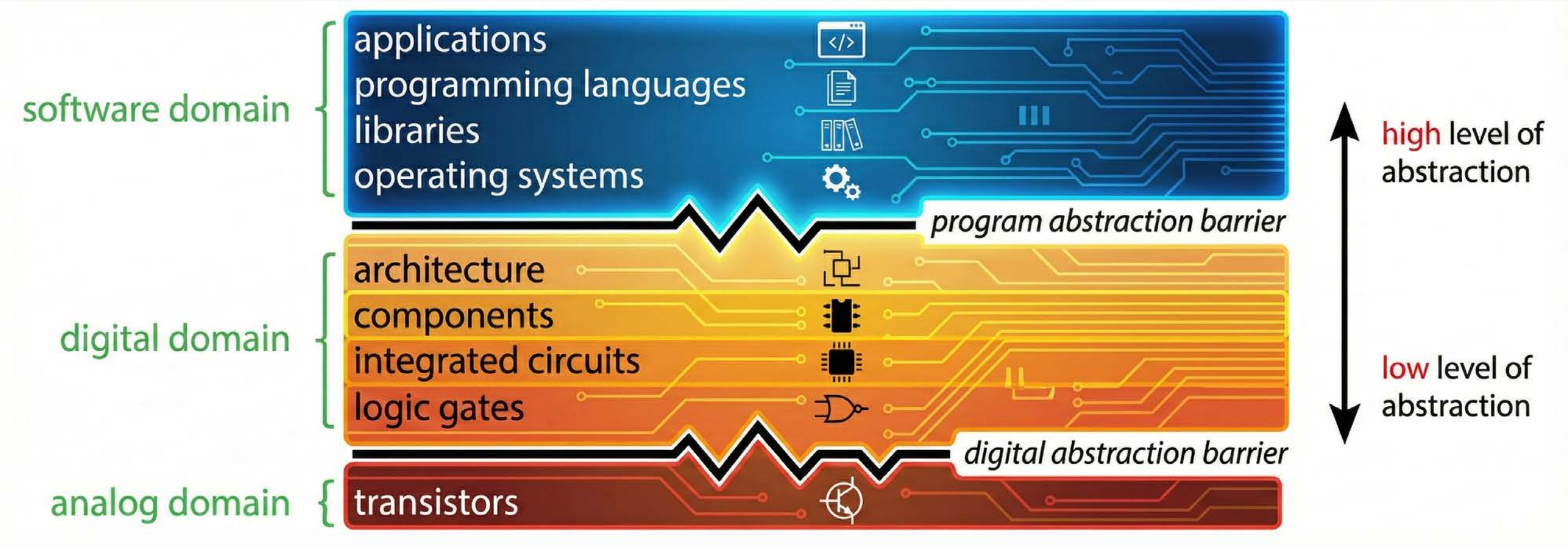


Image created by Gemini (Nano Banana Pro)

파이토치

한국 사용자 모임

오픈소스 AI

Open Source AI

오픈소스 (소프트웨어)

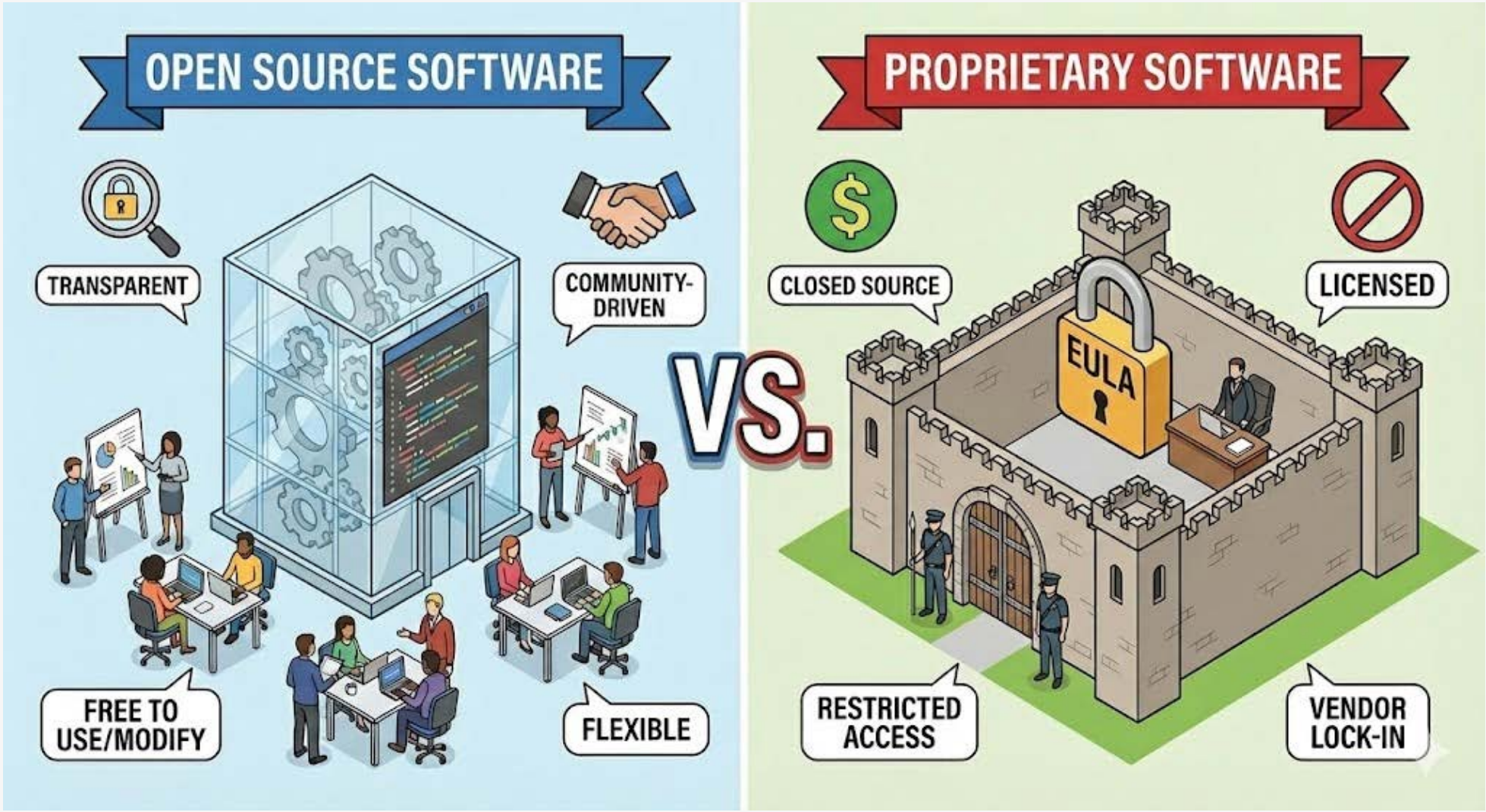


Image created by Gemini (Nano Banana Pro)

오픈소스... AI?

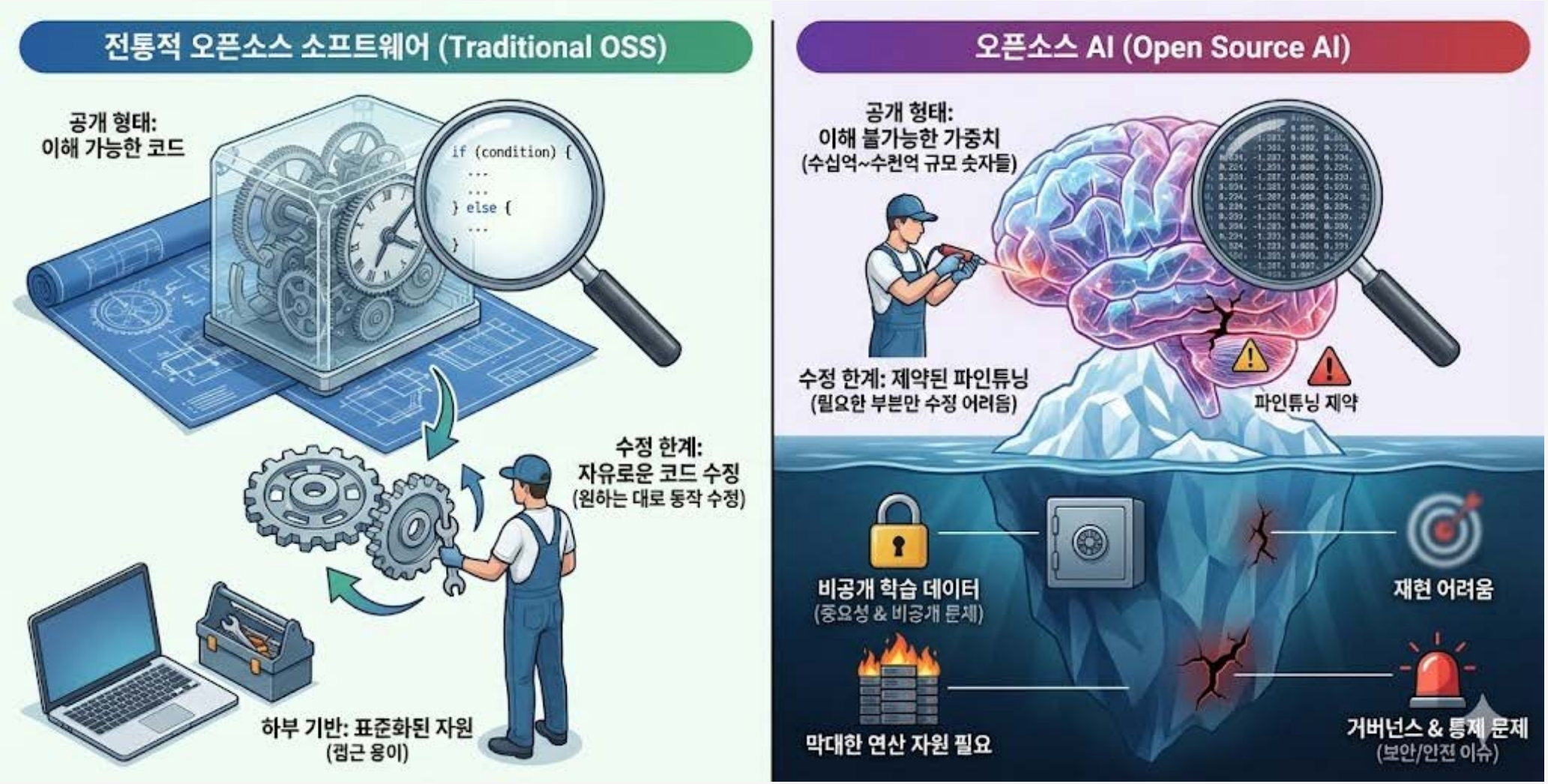


Image created by Gemini (Nano Banana Pro)

오픈소스 AI

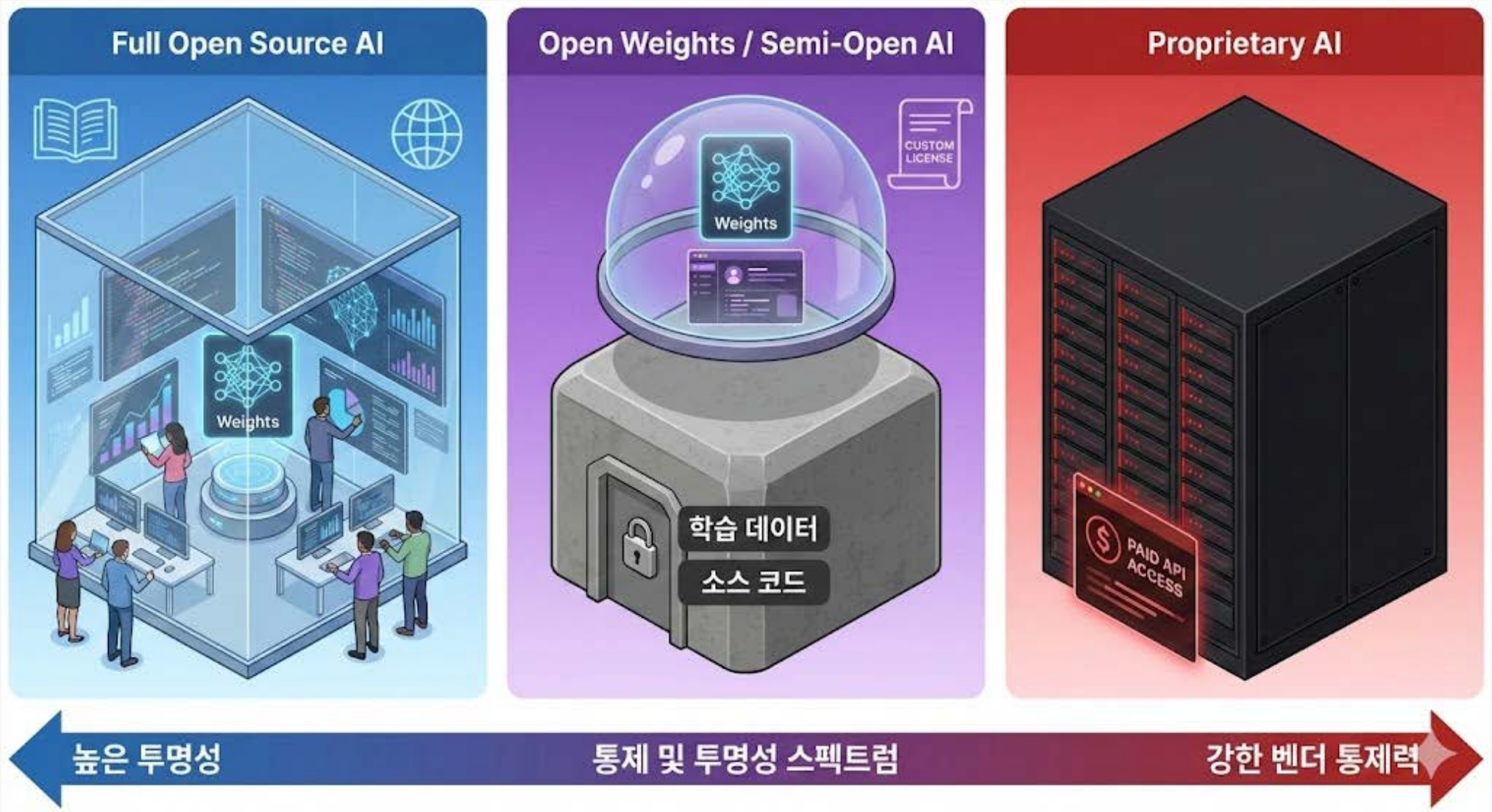
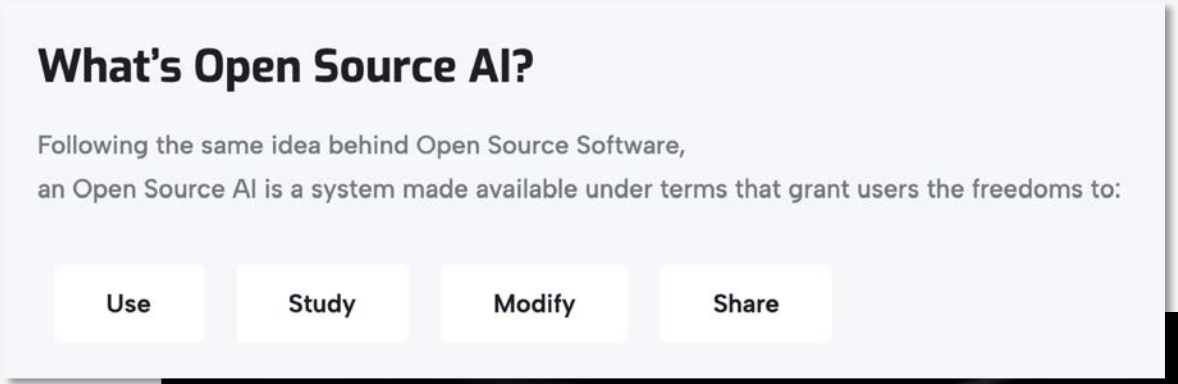


Image created by Gemini (Nano Banana Pro)

OSI의 오픈소스 AI 정의(OSAID)

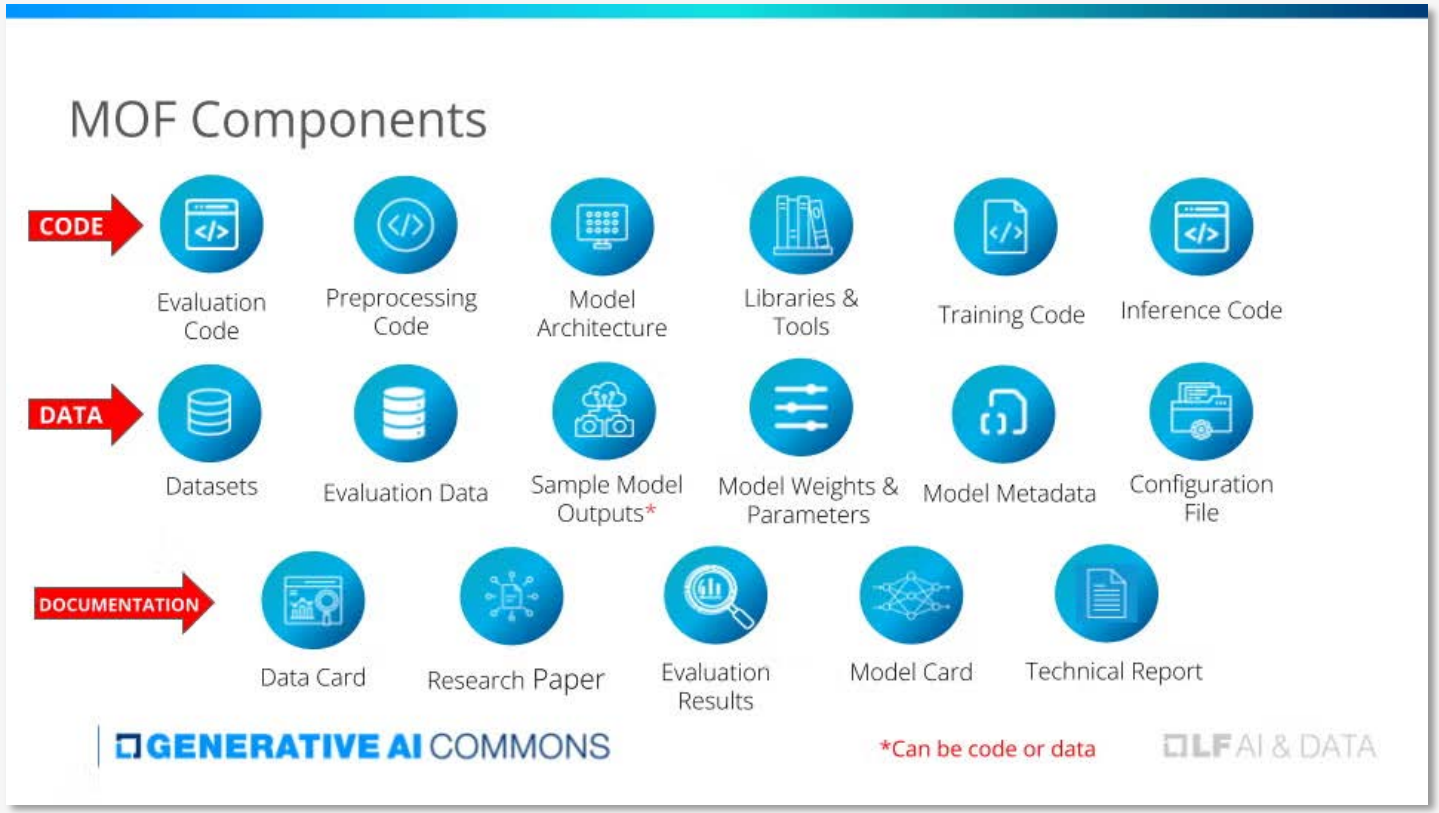
- OSI(Open Source Initiative)가 제안한 오픈소스 AI 정의 (Open Source AI Definition)
- 사용(Use), 연구(Study), 변경(Modify), 공유(Share)의 자유가 보장된 AI 시스템
- **사용**: 목적에 관계없이, 허가 없이 AI 시스템을 사용
- **연구**: AI 시스템 및 구성 요소들의 검사 및 동작 연구
- **변경**: 사용 목적에 따른 (출력 포함) 시스템의 변경
- **공유**: 목적 및 변경 여부에 관계없이 타인에게 공유



출처: Open Source AI by OSI

Linux Foundation의 모델 개방성 평가체계(MOF)

- Linux Foundation 및 GenAI Commons 등이 함께 공개한 모델 개방성 평가체계
- 17가지 구성 요소(코드, 데이터, 문서)의 공개 정도에 따라 3단계(Class 1~3)로 구분



출처: LF AI&Data 블로그

Linux Foundation의 모델 개방성 평가체계(MOF)

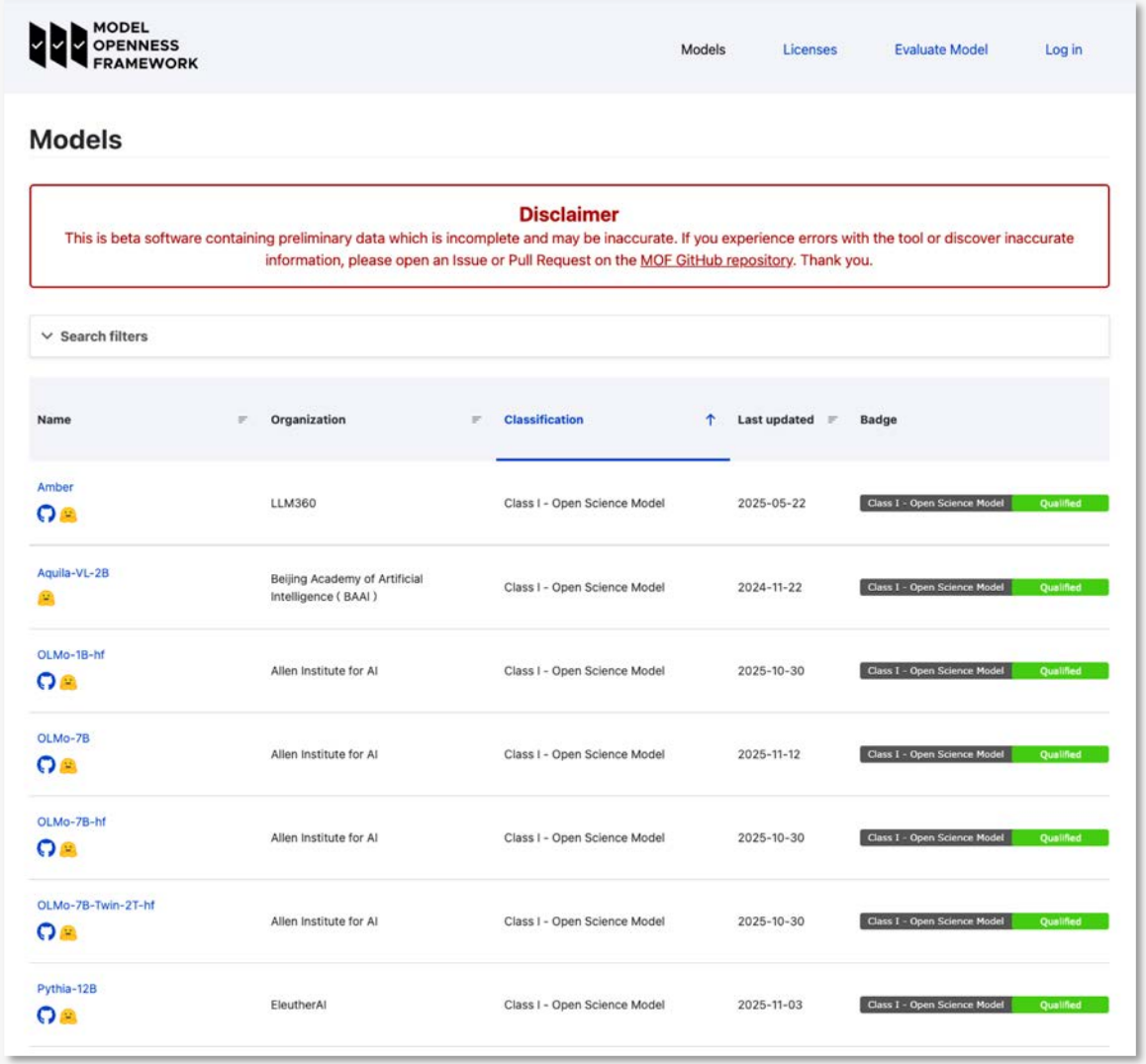
- 17가지 구성 요소(코드, 데이터, 문서)의 공개 정도에 따른 3단계 구분
- **Class 3. Open Model**
  - 가장 낮은 공개 등급으로, '사용'이 가능한 단계
  - 모델 가중치 및 기본 문서, 평가 결과만 공개
- **Class 2. Open Tooling**
  - 모델 검증 및 확장, '변경'이 가능한 단계
  - Class 3 + 학습 코드 및 주요 데이터셋 공개
- **Class 1. Open Science**
  - 가장 높은 공개 등급으로, '재현'이 가능한 단계
  - Class 2 + 학습 데이터 및 논문, 중간 결과물 등 공개

MOF Class	Components Included
Class III. Open Model	1. Model Architecture 2. Model Parameters (Final Checkpoints) 3. Technical Report or Research Paper 4. Evaluation Results 5. Model Card 6. Data Card 7. Sample Model Outputs (Optional)
Class II. Open Tooling	1. All Class III Components 2. Training, Validation, and Testing Code 3. Inference Code 4. Evaluation Code 5. Evaluation Data 6. Supporting Libraries & Tools
Class I. Open Science	1. All Class II Components 2. Research Paper 3. Datasets 4. Data Preprocessing Code 5. Model Parameters (Intermediate Checkpoints) 6. Model Metadata (Optional)

출처: arXiv:2403.13784

Linux Foundation의 모델 개방성 평가도구(MOT)

- 모델 개방성 평가체계에 따른 평가 도구 (베타 공개 단계)
- Amber, Aquila-VL, OLMo, Pythia 등 Class 1

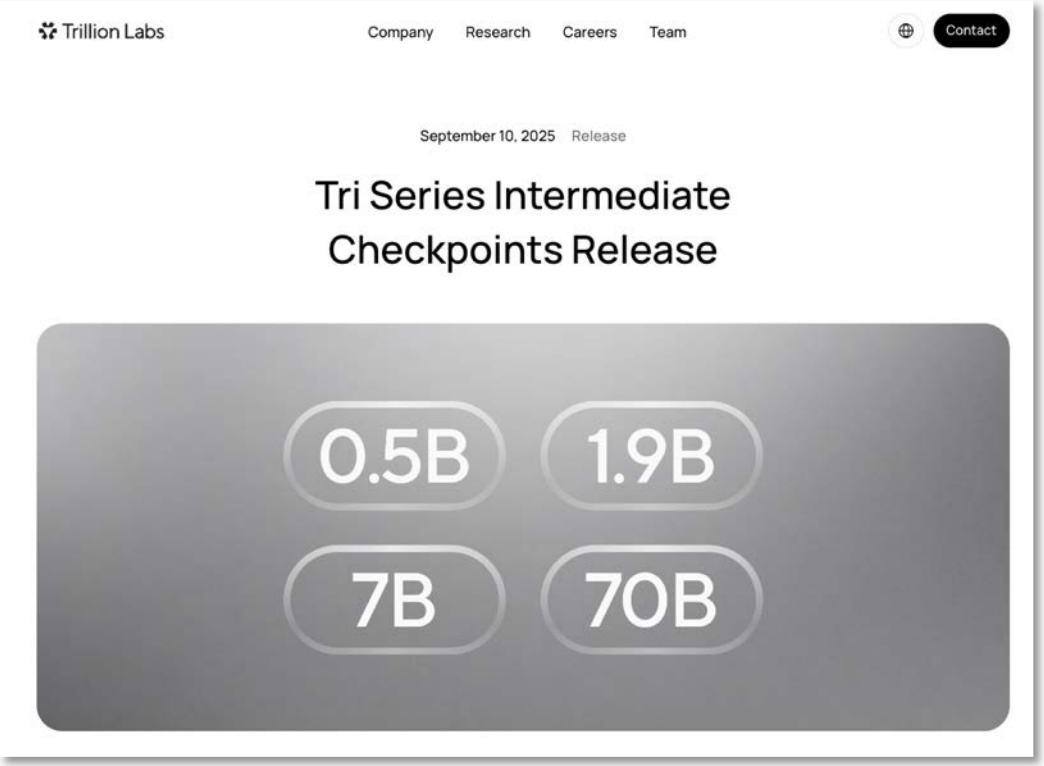


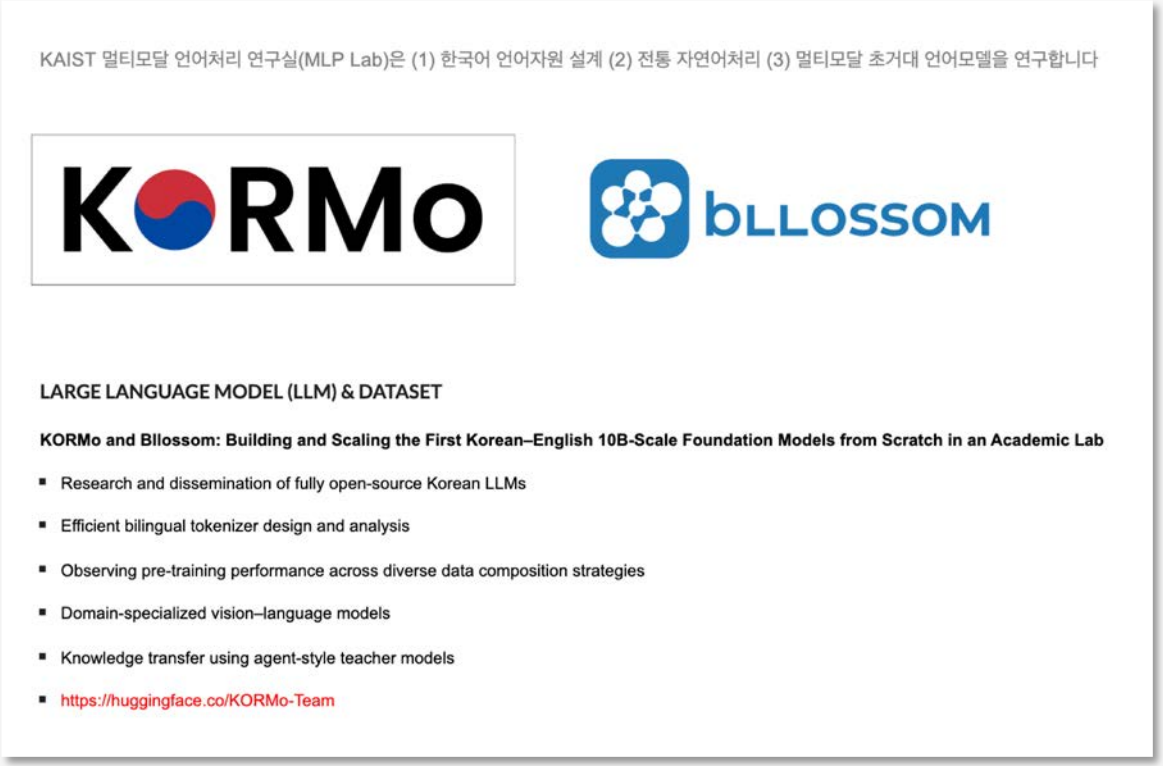
- Website: https://mot.isitopen.ai/
- GitHub: lfai/model_openness_tool

출처: arXiv:2403.13784

오픈소스 AI

- 단순 사용(Use)이나 변경(Modify)을 넘어, 재현(Reproduction)이 가능해야
- 한국에서는 Trillion Labs의 Tri Series, KASIT MLP Lab의 KORMo 등이 공개 중





출처: Trillion Labs Blog 및 MLP Lab 홈페이지

파이토치

한국 사용자 모임

AI 테크맵

AI Techmap

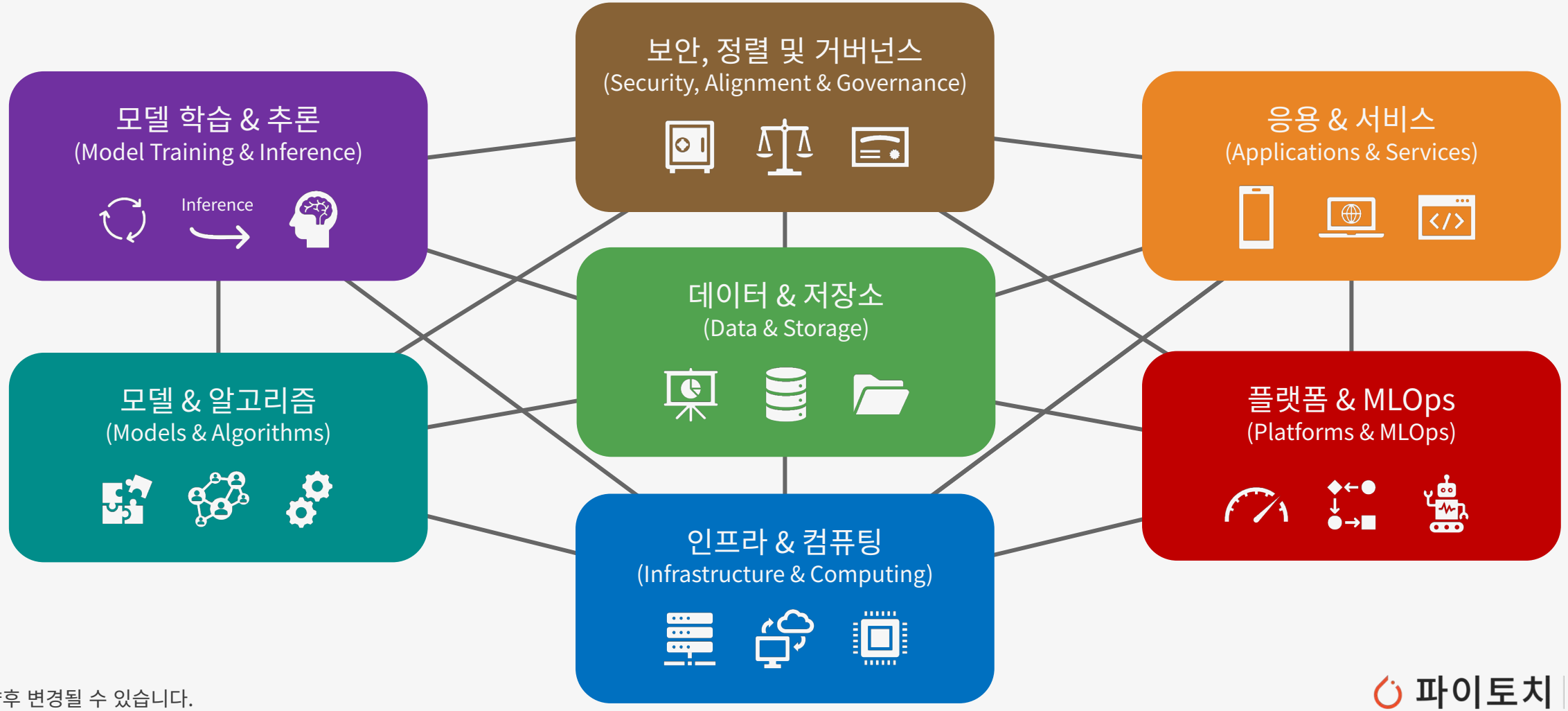
제안 배경

- 지도: ‘어디’에 ‘무엇’이 있는지 확인하고, 원하는 곳을 ‘어떻게’ 찾아갈지 돕는 도구
- AI 테크맵: AI 서비스 개발 시 ‘보유하지 않은 기술’과 ‘대체 가능한 오픈소스’ 탐색을 돕는 도구

Image created by Gemini (Nano Banana Pro)

AI 테크맵 제안

- 어떠한 기술 및 도구가 필요한지 식별하기 위해 AI 기술 스택을 7가지 분류로 정리



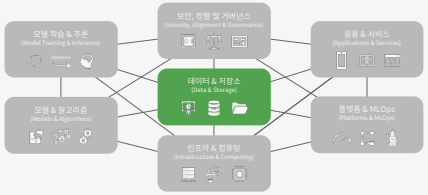
⚠ WIP, 향후 변경될 수 있습니다.

AI 테크맵 구성: 인프라 & 컴퓨팅

- AI 시스템 구동에 필요한 H/W, S/W 및 이에 기반한 컴퓨팅 인프라/관리 도구 일체
- **온-디바이스 AI 반도체**
  - IoT 기기 등에서 AI 추론을 직접 수행하는 저전력 AI 반도체
- **AI 가속기(GPU/NPU 등)**
  - AI 모델 학습에 필요한 고성능 병렬 처리용 하드웨어 및 런타임 - 예. OpenCL, ROCm, Vulkan 등
- **대규모/분산 컴퓨팅 인프라**
  - AI 모델 학습/배포에 필요한 인프라 자원 및 플랫폼(IaaS 등) - 예. OpenStack, CloudStack 등
- **컨테이너/오케스트레이션**
  - 대규모 컴퓨팅 인프라 자원 관리 및 최적화 기술 및 도구 - 예. Docker, Kubernetes 등

⚠ WIP, 향후 변경될 수 있습니다.

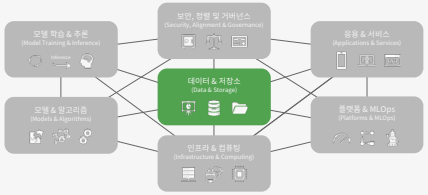
AI 테크맵 구성: 데이터 & 저장소



- 모델 학습, 추론 및 평가에 필요한 데이터 및 데이터 수집 - 저장 - 전처리 - 관리 도구
- **ETL & Workflow**: 다양한 데이터 원천으로부터 ETL(Extract/Transform/Load) 수행 및 관리 도구
- **카탈로그 및 버전/계보**: 메타데이터 수집/정제 및 데이터 버전/계보(Lineage) 관리 도구
- **데이터셋 및 관련 도구**: 모델 학습에 필요한 데이터셋 및 저장소/도구 등
- **합성 데이터 생성 / 관리 도구**: 프라이버시 보호 및 데이터 보완을 위해 실제와 유사한 데이터 생성/관리
- **데이터 라벨링**: 모델 학습에 필요한 데이터 라벨 생성/관리 및 협업/검수/자동화 도구
- **데이터 품질 관리/보증**: 데이터 정제 및 스키마 검증, 이상치 탐지, 정합성 확인 등 품질 관리
- **벡터 데이터베이스**: 임베딩 벡터 등을 저장/조회/검색하여 유사도 기반 검색 및 RAG 등에 활용

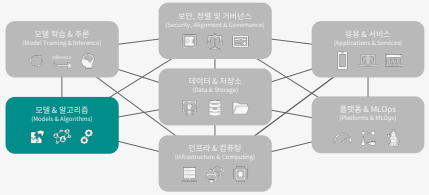
⚠ WIP, 향후 변경될 수 있습니다.

AI 테크맵 구성: 데이터 & 저장소



- 모델 학습, 추론 및 평가에 필요한 데이터 및 데이터 수집 - 저장 - 전처리 - 관리 도구
- **ETL & Workflow** 도구 예. Apache Airflow, Apache Oozie, Dagster, ...
- **카탈로그 및 버전/계보** 도구 예. DataHub, OpenMetaData, OpenLineage, Amundsen, ...
- **데이터셋 및 관련 도구** 예. LAION, Common Crawl, Hugging Face Datasets, ...
- **합성 데이터 생성 / 관리 도구** 예. Faker, SDV, Synthea, Syth, YData Synthetic, ...
- **데이터 라벨링** 도구 예. CVAT, Label Studio, ...
- **데이터 품질 관리/보증** 도구 예. OpenRefine, elementary, GreatExpectations, Soda Core, ...
- **벡터 데이터베이스** 예. Milvus, Qdrant, Chroma, FAISS, Weaviate, ...

⚠ WIP, 향후 변경될 수 있습니다.

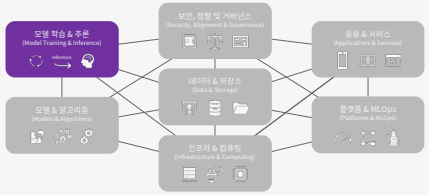


AI 테크맵 구성: 모델 & 알고리즘

- LLM 외, 전통적인 Deep Learning / Machine Learning 모델 포함
- 벤치마크 및 리더보드 등을 통해 활용 사례에 맞는 모델 검색 및 탐색 지원

⚠ WIP, 향후 변경될 수 있습니다. Image created by Gemini (Nano Banana Pro)

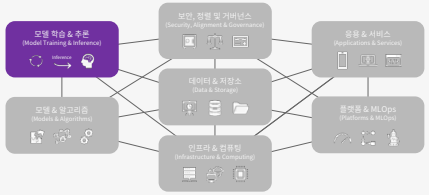
AI 테크맵 구성: 모델 학습 & 추론



- 모델 개발 및 학습/추론을 위한 도구, 라이브러리 및 프레임워크
- **딥러닝 프레임워크**: 모델 정의 및 학습, 추론의 토대가 되는 범용 프레임워크
- **강화학습 라이브러리**: 에이전트 학습 및 문장/이미지 생성 등에 사용하는 강화학습 라이브러리
- **분산학습 프레임워크**: 여러 서버/노드를 활용하여 병렬화된 학습을 통해 학습 속도 및 확장성 강화
- **연합학습 프레임워크**: 여러 엣지 단말 등에서 데이터 이동 없이 중앙 서버를 통해 학습하는 프레임워크
- **AutoML/HPO**: 모델/파이프라인 생성, Hyper Parameter 최적화 등 모델 개발 과정 자동화 도구
- **파인튜닝/PEFT**: 학습된 모델을 추가적으로 미세조정(파인튜닝)하기 위한 도구
- **모델 경량화**: Quantization, Pruning, Knowledge Distillation 등, 추론 시 메모리 및 연산량 감소
- ...

⚠ WIP, 향후 변경될 수 있습니다.

AI 테크맵 구성: 모델 학습 & 추론



- 모델 개발 및 학습/추론을 위한 도구, 라이브러리 및 프레임워크
- **딥러닝 프레임워크** 예. PyTorch, JAX, Tensorflow, Keras, ...
- **강화학습 라이브러리** 예. veRL, torchRL, Hugging Face TRL, Catalyst, Ray Rllib, ...
- **분산학습 프레임워크** 예. Horovod, DeepSpeed, ColossalAI, Determined, Ray Train, ...
- **연합학습 프레임워크** 예. FedML, Flower, FATE, PySyft, Tensorflow Federated, ...
- **AutoML/HPO** 예. Auto ScikitLearn, AutoGluon, Optuna, TPOT, Hyperopt, ...
- **파인튜닝/PEFT** 예. Hugging Face PEFT, LitGPT, Adapters, Ray Tune, Transformer Lab, ...
- **모델 경량화** 예. Optimum, bitsandbytes, GPTQModel, Neural Compressor, ...
- **...**

⚠ WIP, 향후 변경될 수 있습니다.

AI 테크맵 구성: 플랫폼 & MLOps

- 학습한 모델의 활용 및 운영을 위한 플랫폼 및 도구
- **모델 서빙 및 추론 엔진**: 실시간 모델 서비스를 위한 고성능 서빙 및 추론 엔진
- **온디바이스 런타임**: 특정 하드웨어(PC, 모바일 등)에 최적화한 모델 서빙 및 추론 런타임
- **프롬프트 관리 및 실험**: 프롬프트/컨텍스트 엔지니어링 및 성능 평가, 버전 관리 등을 위한 도구
- **RAG 및 GraphRAG**: 모델에 외부 지식을 주입하고 최종 결과를 생성하는 RAG 파이프라인 프레임워크
- **메모리 및 지식 그래프**: LLM 및 에이전트의 대화 기억, 지식 관리 등을 위한 장/단기 메모리 시스템
- **에이전트 개발 프레임워크**: 에이전트 정의, 도구/상태/메모리 관리 등, 에이전트 개발 프레임워크
- **테스트 및 성능 평가**: AI 시스템 전체(E2E) 또는 모듈별 기능 / 비기능 성능 테스트 및 평가 프레임워크
- ...

⚠ WIP, 향후 변경될 수 있습니다.

AI 테크맵 구성: 플랫폼 & MLOps

- 학습한 모델의 활용 및 운영을 위한 플랫폼 및 도구
- **모델 서빙 및 추론 엔진** 예. vLLM, SGLang, Ray Serve, NVIDIA Triton Inference Server, ...
- **온디바이스 런타임** 예. ollama, llama.cpp, MLC LLM, MNN, ncnn, ...
- **프롬프트 관리 및 실험** 도구 예. promptfoo, DSPy, PromptTools, OpenPrompt, ...
- **RAG 및 GraphRAG** 프레임워크 예. GraphRAG, Haystack, RAGFlow, ...
- **메모리 및 지식 그래프** 시스템 예. Mem0, cognee, Memary, memonto, txtai, ...
- **에이전트 개발 프레임워크** 예. LangChain, CrewAI, AutoGen, LlamaIndex, SuperAGI, ...
- **테스트 및 성능 평가** 도구 예. RAGAS, TruLens, DeepEval, ...
- **...**

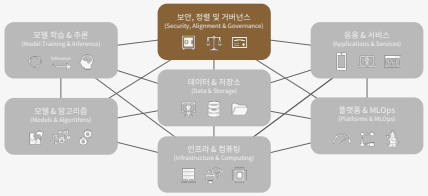
⚠ WIP, 향후 변경될 수 있습니다.

AI 테크맵 구성: 응용 & 서비스

- 기업 및 소비자에게 직접적으로 제공되거나 사용하는 제품 및 솔루션
- **자율형 에이전트 서비스**
  - LLM/VLM 기반, 자율적으로 복합 작업을 생성 및 수행하는 에이전트 서비스
- **산업별 AI 솔루션**
  - 의료 영상 분석, 금융 사기 탐지 등, 제조 / 의료 / 금융 등 산업 도메인 특화된 AI 솔루션
- **추천 시스템 및 검색 엔진**
  - 사용자 행동 또는 아이템 기반 콘텐츠, 제품 추천 및 정보 검색 서비스 솔루션
- **대화 기반 어시스턴트**
  - 대화 기반으로 사용자에게 정보를 전달하거나 업무 수행을 돕는 Chatbot 등 솔루션

⚠ WIP, 향후 변경될 수 있습니다.

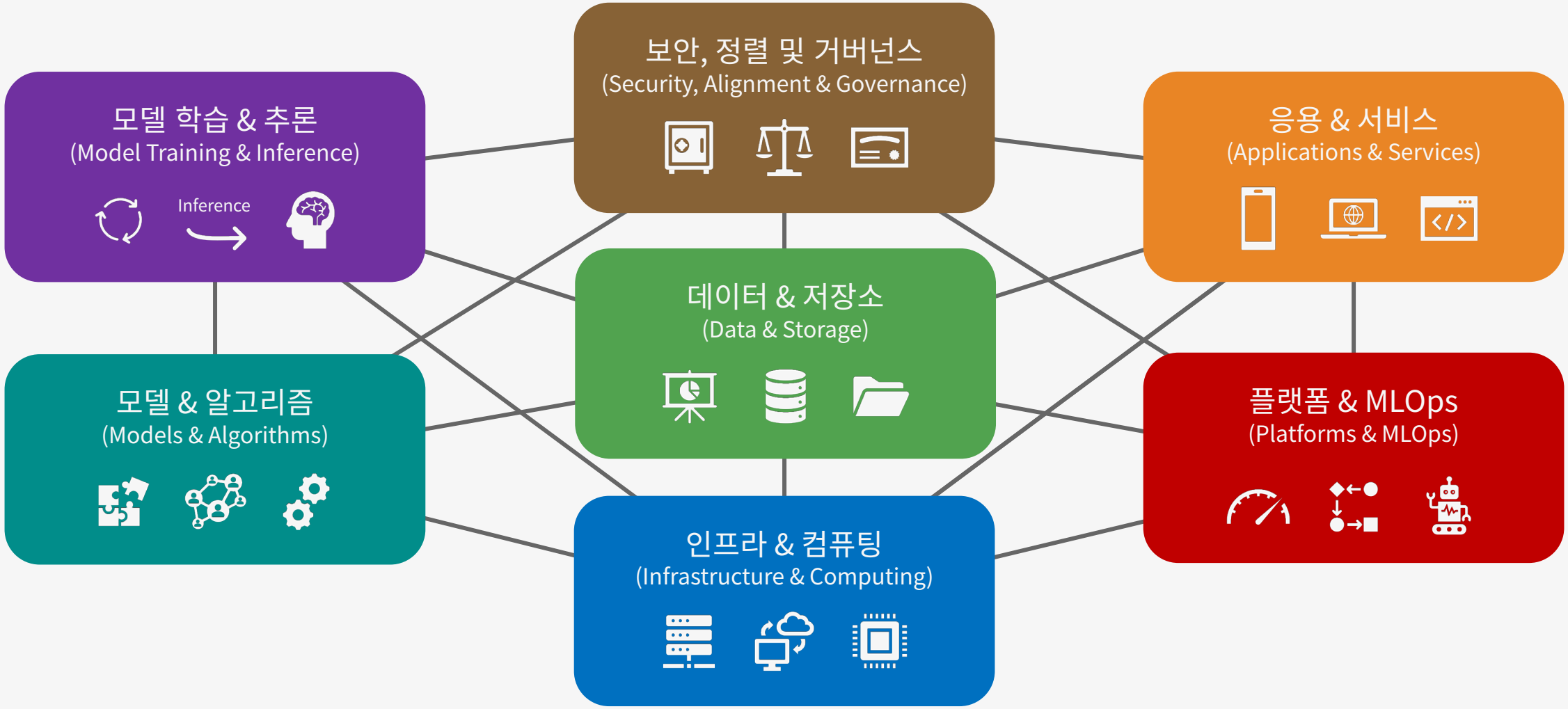
AI 테크맵 구성: 보안, 정렬 및 거버넌스



- AI 시스템의 유용성, 안전성 및 신뢰성 확보를 위한 정책 및 도구
- **AI 거버넌스**: AI 시스템의 윤리성, 규정/규제 준수 여부를 포함한 운영 체계 전반 검증 및 관리 체계
- **프라이버시 및 비식별화**: 개인식별정보(PII) 탐지 및 마스킹, 차등 프라이버시 적용 등 학습 데이터 보호
- **공정성 및 편향 탐지**: 특정 인종, 성별 또는 연령 등에 대한 데이터 및 모델의 편향 진단 및 공정성 확보
- **설명 가능한 AI(XAI)**: AI 모델의 의사 결정 과정을 설명하여 투명성 향상 및 의사 결정 과정 개입 등
- **가드레일 및 정책 엔진**: 답변 제한, 개인식별 정보 마스킹 등, 목적에 어긋난 대화를 하지 않도록 제한
- **보안 테스트 및 레드팀**: 탈옥, 악성 프롬프트 방어 등, AI 시스템 전반의 보안 검증 및 운영 체계 관리
- **AI 정렬(Alignment)**: 인간의 가치관/윤리관에 맞도록 AI 시스템의 유용성 / 안전성 / 신뢰성 확보
- ...

⚠ WIP, 향후 변경될 수 있습니다.

AI 테크맵 제안



⚠ WIP, 향후 변경될 수 있습니다.

AI 테크맵 활용 예시: 가상 시나리오

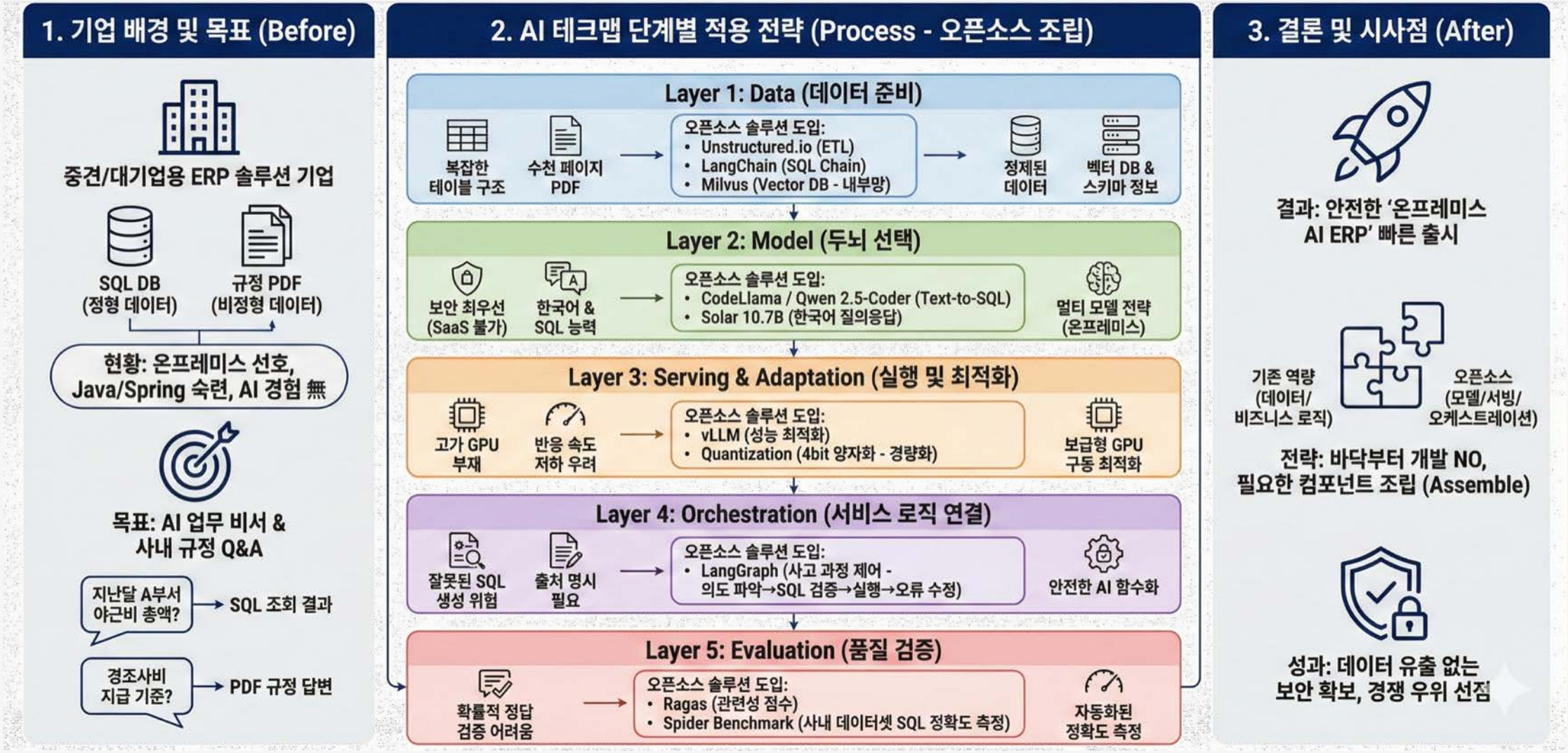


Image created by Gemini (Nano Banana Pro)

파이토치

한국 사용자 모임

감사합니다.

발표 관련 추가 질문 또는 AI 테크맵 관련 개선 의견이 있으시면
이메일(9bow@pytorch.kr)로 연락 부탁드립니다.