025 머신러닝 운영 / MLOps

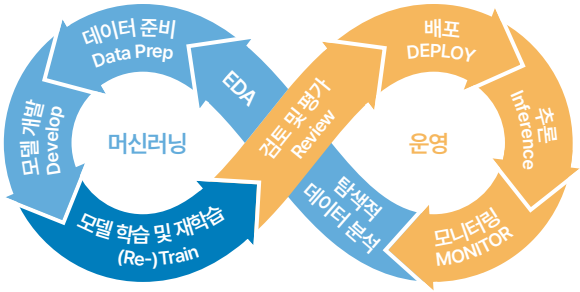
Machine Learning Operations

AI 모델의 개발·배포·운영을 자동화하고 관리하는 통합 관리 체계

- ML 모델의 학습·평가·배포 과정을 효율적으로 연결, 안정적 AI 서비스 운영을 가능하게 하는 체계
- 데이터 과학과 소프트웨어 엔지니어링을 통합해 모델의 품질·재현성·확장성을 확보

MLOps란?

MLOps는 머신러닝과 DevOps(개발·운영)의 합성어로, 데이터 수집부터 모델 개발, 실험 관리, 배포, 모니터링, 재학습까지 AI 모델의 전생애주기를 자동화하고 표준화하는 운영·엔지니어링 체계입니다. DevOps가 소프트웨어 배포와 운영 자동화를 다루는 반면, MLOps는 여기에 데이터·모델의 버전관리, 품질관리, 모델 드리프트 감지, 재학습 자동화를 포함하여 AI 서비스를 안정적으로 운영하기 위한 확장된 개념입니다. 과거 머신러닝 개발은 데이터 준비, 모델 학습, 평가가 연구자 중심으로 이루어졌지만, 실무에서는 모델을 주기적으로 업데이트하고 성능을 유지하는 과정이 복잡했습니다. MLOps는 이를 해결하기 위해 머신러닝 운영 전 과정을 자동화하고 표준화합니다. 즉, 모델 개발의 실험 중심 접근을 지속 가능한 서비스 운영 체계로 전환하는 역할을 합니다.



머신러닝 운영(MLOps)의 과정

출처 : Databricks

MLOps 관리

MLOps는 크게 데이터 파이프라인 관리, 모델 라이프사이클 관리, 지속적 모니터링 체계의 세 축으로 구성됩니다. 데이터 파이프라인은 원천 데이터를 자동으로 수집·정제·검증하여 모델 학습에 적합한 형태로 제공합니다. 모델 라이프사이클 관리 단계에서는 실험 관리, 하이퍼파라미터 최적화, 버전 관리 등을 수행하며, 모델이 서비스 환경으로 배포되면 성능 저하나 편향 발생 여부를 지속적으로 점검합니다. 이러한 체계를 통해 MLOps는 AI 모델의 품질과 신뢰성을 보장하면서 운영 비용과 시간을 절감합니다.