예를 들어 RAG 시스템에서는 문서 색인 시 각 문서에 접근 가능한 사용자나 역할을 지정하고, 사용자가 쿼리할 때 현재 사용자에게 허용된 문서만 검색되도록 필터링한다.

이를 통해 관리자는 전체 문서에 대한 조회 권한을 가질 수 있고, 일반 사용자는 미리 정의된 역할 범위 내의 문서만 이용하도록 제어할 수 있다.

DO 솔루션의 시큐리티 에이전트(DO-SA) 모듈은 이같은 인증/권한 설정과 실시간 모니터링을 제공하여 보안 정책을 관리한다.

RBAC (Role-Based Access Control)
RBAC는 권한을 **직접 사용자에게 주는 방식이 아닌**, **역할(Role)을 통해 간접적으로 부여**하는 방식입니다.
즉,

- **권한(Permissions)** → 기능 수행 권한 (예: 읽기, 쓰기)
- **역할(Role)** → 여러 권한의 묶음 (예: 관리자, 편집자, 뷰어)
- **사용자(User)** → 하나 이상의 역할을 가짐

이렇게 **권한** → **역할** → **사용자** 순서로 계층이 구성되어 관리가 단순하고, 확장성이 좋습니다.

4. 오케스트레이션 프레임워크가 무엇인가?

오케스트레이션 프레임워크는 LLM, 검색기, 도구(API) 등 AI 애플리케이션의 구성 요소들을 연계하고 제어해주는 통합 도구다.

즉, 복잡한 프롬프트 체인, 외부 데이터 검색, 상태관리 등을 하나의 워크플로로 통합하여 LLM 기반 앱의 개발과 운영을 간소화한다.

대표 예로 LangChain 같은 프레임워크가 있는데, 이는 LLM 호출, 프롬프트 템플릿, 검색기, 메모리 등 다양한 컴포넌트를 모듈화하여 손쉽게 연결할 수 있도록 지원한다.

5. 로컬 데이터 활용이 AI 활용 시 문제점으로 꼽히는 이유는?

사내·로컬 데이터만 사용하면 여러 위험이 발생할 수 있다. 먼저 보안·프라이버시 측면에서, 내부 데이터를 적절히 격리·암호화하지 않으면 외부 모델로 전송 시 유출 위험이 있다.

실제로 기업 데이터 통합 과정에서 데이터 프라이버시 및 보안 우려가 문제로 지적된 바 있다.

또한 로컬 데이터만으로 AI를 구동할 경우 지식 범위가 제한되고 최신 정보가 반영되지 않아 모델의 부정확한 결과(할루시네이션) 가능성이 커진다.

예를 들어 RAG 기법은 외부 신뢰 문서로 모델의 할루시네이션을 줄이는 데 사용되는데, 로컬 데이터가 부족하면 모델이 자체적으로 부정확한 답변을 생성할 위험이 높아진다.

6. 할루시네이션 문제란 무엇인가?