031 모델 컨텍스트 프로토콜 / MCP

Model Context Protocol

AI 모델과 외부 도구·데이터를 표준 방식으로 연결하는 개방형 프로토콜

- AI 모델이 다양한 정보원과 안전하게 통신하도록 돕는 프로토콜
- 복잡한 연동 없이 외부 맥락을 확장해 활용할 수 있게 하는 연결 구조

모델 컨텍스트 프로토콜의 개념

MCP는 AI 모델이 파일, 데이터베이스, 내부 시스템, 외부 API 등 다양한 자원에 접근할 때 발생하는 통합 문제를 해결하기 위해 Anthrophic이 제안한 개방형 통신 규약입니다. 기존 방식은 각 서비스마다 별도의 연결 코드가 필요해 개발 비용과 유지 부담이 컸고, 시스템 간 호환성도 떨어졌습니다. MCP는 이런 문제를 개선하기 위해 모델과 외부 도구를 하나의 공통 규격으로 연결하는 구조를 제공합니다. 이를 통해 AI 모델은 고정된 학습 데이터에만 의존하지 않고, 실행 환경의 최신 정보나 사용자 맥락을 실시간으로 받아 활용할 수 있습니다. AI를 단순 대화 도구가 아닌 실제 작업 수행 도구로 확장하는 기반이라는 점에서 주목받고 있으며, 다양한 개발 환경과 플랫폼에서 표준처럼 쓰이기 시작한 기술입니다.

모델 컨텍스트 프로토콜의 구조

MCP는 호스트, 클라이언트, 서버가 서로 역할을 나누어 작동하는 구조로 설계되어 있습니다. 호스트는 AI 모델이 실행되는 환경으로, 사용자 인터페이스와 모델의 작업 공간을 제공하는 핵심 실행 단위입니다. 클라이언트는 이 호스트 내에서 AI 모델과 외부 도구를 이어주는 중간 매개체로, 모델이 요청한 작업을 표준 형식으로 서버에 전달합니다. 서버는 클라이언트 요청을 실제로 처리하는 구성 요소로, 파일 열기, 데이터 조회, 내부 시스템 호출, 외부 API 연동 등 구체적인 작업을 수행해 결과를 다시 클라이언트와 호스트로 반환합니다. 이 세 요소가 규칙화된 방식으로 연동되면서, AI 모델은 복잡한 맞춤형 개발 없이 다양한 도구를 일관된 방식으로 사용할 수 있게 됩니다.

모델 컨텍스트 프로토콜의 이점과 과제

MCP의 가장 큰 이점은 확장성과 재사용성입니다. 하나의 규격만 구현하면 여러 도구와 서비스에 쉽게 연결할 수 있어 개발 부담이 줄고, 모델이 실제 업무 환경 정보에 접근하면서 대화형을 넘어 작업 수행형 AI로 발전할 수 있습니다. 또한 구조가 단순해 도구 추가·관리 측면에서도 효율적입니다. 그러나 해결해야 할 과제도 존재합니다. 외부 도구와 직접 연결되는 만큼 보안과 권한 관리가 중요하며, 인증이 미흡하면 데이터 유출이나 도구 악용 위험이 발생할 수 있습니다. 구현 수준의 차이로 인해 성능과 호환성에 편차가 생길 수 있다는 점도 초기 생태계의 한계입니다. 그럼에도 MCP는 AI가 실제 시스템과 안정적으로 연결되는 기반 기술로 자리 잡아가고 있으며, 앞으로 AI 활용 범위를 크게 확장할 인프라로 평가됩니다.