

A DAILY PERSPECTIVE ON AI

AP News

AI를 연결하는 다섯 가지 기준

출력 형식, 도구 검색, 모델 분담, 실행 주체와 네트워크 경로. 지난주 미수록 공식 자료에서 AI를 업무 시스템에 연결할 때 구분해야 할 기준을 살펴봅니다.



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

THE DAILY BRIEF · 5 STORIES

2026년 10월 26일 편집 · 전달 · 최근 72시간 신규 자료가 부족해 최근 7일로 확대 · 10월 19~21일 AWS 공식 자료 5건 · 지난주 미수록 기능 · 구현 안내 · AI 작성 및 원문 확인



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

01 · AI DATA

Bedrock, Claude의 구조화된 JSON 출력 지원 안내

AWS 공식 AI 블로그 · 발표 2026-10-19

출력 형식을 고정하면 연결이 쉬워지지만 내용의 사실성은 별도로 확인해야 합니다.

AWS는 Bedrock의 Claude 모델에서 JSON Schema 기반 구조화된 출력과 엄격한 도구 호출을 안내했습니다. 모델이 제공되는 곳의 bedrock-runtime·bedrock-mantle 엔드포인트를 대상으로 하며 지원하는 스키마 문법에는 제한이 있습니다. 숫자 범위와 문자열 길이 같은 일부 제약은 지원하지 않으므로 형식 일치에 값의 정확성이나 업무 규칙까지 보장하지는 않습니다.

AP의 관점 · AP뉴스의 기사 JSON과 커머스 조사 데이터를 자동 생성할 때 필드 누락을 줄이는 데 활용할 수 있습니다. 발표일·금액·원문 링크와 발행 여부는 원본 대조와 별도 업무 검증을 거쳐야 합니다.

오늘 해볼 일 · 자동 생성 데이터 한 건의 필수 필드와 별도 검증할 날짜·금액·출처 규칙을 나눠 정리하십시오.

공식 원문 읽기 ↗



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

02 · AI AGENTS

AWS, 실행 시 필요한 도구를 찾는 연결 패턴 공개

AWS 공식 AI 블로그 · 발표 2026-10-20

도구 목록을 모두 넣는 대신 승인된 목록에서 필요한 기능을 검색하는 방식입니다.

AWS는 Agent Registry에서 MCP 서버·에이전트 정보를 검색하고 클라이언트를 만든 뒤 실행하는 구현 예제를 소개했습니다. 설정된 승인 절차를 마친 검색 가능 기록을 이용하며 검색 결과는 호출 자격 증명을 제공하지 않습니다. 연결 정보 발견과 인증은 분리되고, 등록된 기능을 찾았다고 자동으로 실행 권한을 얻는 것은 아닙니다.

AP의 관점 · AP의 뉴스·문의·커머스 자동화가 늘어날 때 기능별 설명과 입력·출력 조건을 관리하면 필요한 도구를 구분하기 쉬워집니다. 검색된 도구에도 최소 권한과 게시·발송 같은 외부 행동의 실행 조건을 적용해야 합니다.

오늘 해볼 일 · 자동화 도구 한 개의 목적·입출력·관리자·실행 권한·실패 시 동작을 명세로 기록하십시오.

[공식 원문 읽기](#) ↗



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

03 · HYBRID AI

AWS, 로컬 소형 모델과 클라우드 모델의 역할 분담 소개

AWS 공식 AI 블로그 · 발표 2026-10-21

요청 난도에 따라 처리 위치와 모델을 나누는 설계 예제입니다.

AWS는 Strands Agents·Ollama·Bedrock으로 일상적인 처리를 로컬 소형 모델에, 복잡한 분석을 클라우드 모델에 보내는 AAIF 예제를 공개했습니다. IoT 모니터링을 참고하며 실습의 장치 데이터는 모의 데이터입니다. 실제 비용 절감률이 나 모든 장비의 오프라인 처리·개인정보 보호가 검증된 완제품 발표는 아닙니다.

AP의 관점 · AP의 콘텐츠 분류·문의 정리에서도 단순 작업과 근거 검토가 필요한 작업을 나눠 모델과 처리 방식을 선택할 수 있습니다. 분기 오류와 클라우드로 전송되는 데이터 범위를 확인해야 하며 로컬 처리라는 이유만으로 안전성을 단정해서는 안 됩니다.

오늘 해볼 일 · 반복 업무 한 건을 단순 분류·복합 판단으로 나누고 각 단계의 오류 기준과 외부 전송 정보를 기록하십시오.

공식 원문 읽기 ↗



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

04 · AGENT IDENTITY

AWS, 에이전트 신원과 위임 권한을 분리하는 구조 소개

AWS 공식 AI 블로그 · 발표 2026-10-20

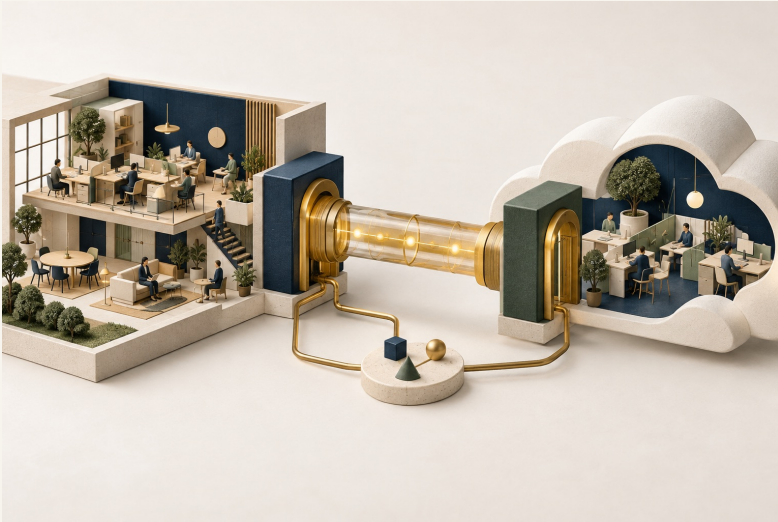
누가 어떤 사용자를 대신해 어느 도구를 호출했는지 증명하는 설계입니다.

AWS와 Keyfactor는 X.509 인증서 기반 신원, 서명된 요청, 사용자 위임 증명과 대상별 토큰을 조합한 참고 구조를 소개했습니다. 인증서 폐기 상태 확인과 호출 기록도 다룹니다. EJBCA Enterprise·Keycloak 등 별도 구성과 운영이 필요한 예제이며 인증서를 사용하기만 하면 AI의 응답 정확성이나 모든 공격 방어가 보장되는 것은 아닙니다.

AP의 관점 · AP의 구독 발송 · 관리자 기능에서도 로그인한 사람의 권한과 자동화가 받은 권한을 구분해야 합니다. 작업 주체·수행 목적·허용 범위·철회 방법이 기록되어야 오류 발생 후 원인을 추적할 수 있습니다.

오늘 해볼 일 · 자동화 한 경로의 요청 사용자·실행 주체·허용 작업·권한 철회 방법·감사 기록을 확인하십시오.

[공식 원문 읽기](#) ↗



AI 제작 · 편집 일러스트 · 실제 제품 화면 아님

05 · PRIVATE AI ACCESS

AWS, 사내망과 Amazon Quick의 비공개 연결 방법 안내

AWS 공식 AI 블로그 · 발표 2026-10-21

사용자의 접속 경로와 AI가 데이터를 가져오는 경로를 따로 설계합니다.

AWS는 Direct Connect 또는 Site-to-Site VPN이 있는 환경에서 Quick의 사용자·API 접속용 VPC 엔드포인트와 데이터 조회용 VPC 연결을 구성하는 방법을 설명했습니다. VPC 연결에는 Enterprise 구독 등이 필요하며 SharePoint·Google Drive 등 모든 지식 소스가 같은 연결을 지원하는 것은 아닙니다. 사설 경로 설정이 데이터별 권한이나 전체 보안을 대신하지는 않습니다.

AP의 관점 · AP가 업무 자료를 AI에 연결할 때도 사용자가 어디로 접속하는지와 외부 서비스가 어느 데이터에 접근하는지 따로 파악해야 합니다. 구독·문의 데이터의 실제 전달 경로와 계정 권한을 함께 확인하는 것이 중요합니다.

오늘 해볼 일 · 업무 자료 연결 한 건의 사용자 접속·데이터 조회 경로를 나누고 지원 소스·요금제·계정 권한을 대조하십시오.

공식 원문 읽기 ↗

ONE THING TO TAKE AWAY

오늘, 하나만 해본다면.

AI 연결은 한 번의 설정으로 끝나지 않습니다. 데이터 형식과 내용, 도구 발견과 실행 권한, 사용자 접속과 데이터 조회를 구분해 실제 업무 흐름을 검증하십시오.