정보관리기술사 데일리 다이제스트

2026-11-03 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE LAW DS 정보보안	**더존비즈온 백업서버 침해, 고객사 연쇄 유출** **근거** 「개인정보 보호법」 업무위탁 수탁자 관리·감독 · 수탁사 침해의 고객사 전이 사례 · dailysecu.com/news/articleView.html?idxno=209275	수탁자 관리 · 백업서버 · SaaS 위험 · 연쇄 유출
국제	AI DS SE 인공지능	**Uber, MCP 게이트웨이로 AI 도구 접근 통제** **근거** Model Context Protocol (MCP) 사양 · 에이전트 도구 호출 중앙 거버넌스 · infoq.com/news/2026/11/uber-mcp-gateway-ai-agents/	MCP · 게이트웨이 · 도구 레지스트리 · 에이전트 거버넌스
공공·정책	*해당 축 없음 — SPRi 월드 모델은 2026-09-25 기채택 토픽으로 중복이며, 개인정보위 인사발령은 기술사 논제 부적합*		

2. 오늘의 토픽 — MCP 게이트웨이(Model Context Protocol Gateway)

AI SE DS | 출제 예상: **1교시** | 근거: **Model Context Protocol (MCP) 사양, OWASP Top 10 for LLM Applications**

2-1. 개념 및 정의

AI 에이전트의 MCP 서버·도구 탐색과 호출을 단일 경로로 중개하는 프록시 계층. 인증·인가·감사를 중앙화하여 도구 남용과 접근 권한 난립을 통제하는 목적.

2-2. 등장 배경

에이전트 도입 확산에 따른 MCP 서버·도구 수 폭증과 개별 연동 방식의 권한·감사 사각지대 발생. 도구 레지스트리와 호출 경로의 분리를 통한 통제 일원화 요구 증대.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
탐색 계층	도구 레지스트리, 메타데이터 카탈로그	에이전트용 도구 등록과 검색 표준화
통제 계층	인증·인가, 정책 엔진, 레이트 리밋	에이전트·도구 단위 최소권한 호출 통제
관측 계층	호출 로그, 감사 추적, 비용 계측	도구 호출 이력 추적과 이상행위 탐지

2-4. 시험·실무 관점

- [SE 연계] 에이전트를 비신뢰 실행주체로 보는 제로트러스트 적용
- [DS 연계] API 게이트웨이 패턴의 에이전트 도구 계층 확장
- [AI 연계] 도구 포이즈닝·프롬프트 인젝션 대응 지점으로서의 게이트웨이

답안 필수 키워드 — MCP / 도구 레지스트리 / 최소권한 / 감사 추적 / 에이전트 거버넌스