정보관리기술사 데일리 다이제스트

2026-11-06 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	DS SE LAW 디지털서비스	**금융보안원 CSP 안전성 대표평가 개편, 2027 전면 적용** CSP 취약점의 금융권 연쇄 전파 차단 · dailysecu.com/news/articleView.html?idxno=209319	CSP 대표평가 · 집중위험 · 연쇄사고 · 증적 평가
국제	OS SE 운영체제	**OpenSSH musl 환경 장문 비밀번호 인증우회** 패스워드 비활성 계정 인증 우회 구조 · theregister.com/security/2026/11/05/get-root-on-a-musl-linux-system-by-slamming-it-with-an-overly-long-password/5307910	OpenSSH · musl libc · 인증우회 · Alpine Linux
공공·정책	LAW AI SE 법·규제	**에이전트·피지컬 AI 시대 개인정보 보호 기술 해법** **근거** 「개인정보 보호법」 · AI 에이전트 개인정보 처리 통제 논점 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttId=12617	개인정보 보호기술 · 에이전트 AI · 피지컬 AI · PETs

2. 오늘의 토픽 — 클라우드 집중위험(Cloud Concentration Risk)과 CSP 안전성 평가

DS SE LAW IM | 출제 예상: **2교시**

2-1. 개념 및 정의

소수 CSP 의존으로 단일 취약점·장애가 다수 기관에 연쇄 전파되는 위험 구조. CSP 평가 강화와 다중 클라우드 설계를 통한 연쇄 사고 억제.

2-2. 등장 배경

금융권 클라우드 활용 확대에 따른 CSP 취약점의 다수 금융사 동시 파급 우려. 서면·증적 중심 평가의 실효성 한계와 검증 중심 평가 전환 요구.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
위험 식별	의존도 분석, 공통 장애점, 대체 가능성	CSP 의존 구조의 단일 장애점 도출
통제 체계	CSP 대표평가, 증적 검증, 지속 점검	다수 금융사 공통 평가의 중복 부담 해소
복원 설계	다중 클라우드, 이탈 전략, 격리 아키텍처	CSP 장애 시 서비스 연속성 확보

2-4. 시험·실무 관점

- [SE 연계] 공급망 보안 관점의 CSP 공동책임모델 재정의
- [LAW 연계] 금융 클라우드 규제와 제3자 위험관리 체계
- [IM 연계] 벤더 종속 최소화 클라우드 거버넌스 전략

답안 필수 키워드 — 집중위험 / CSP 대표평가 / 공동책임모델 / 다중 클라우드 / 제3자 위험관리