정보관리기술사 데일리 다이제스트

2026-10-15 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE DS 정보보안	**정상 원격제어 기능 악용 냉장설비 마비 사이버공격** OT·IoT 정상기능 악용 공격 사례 · dailysecu.com/news/articleView.html?idxno=208868	OT 보안 · 원격제어 악용 · 구형 제어장치 · 인터넷 노출
국제	SE CA AI NW 정보보안	**AI 글래스 대상 컨피덴셜 컴퓨팅 기반 프라이빗 프로세싱 확장** **근거** IETF RFC 9334 (RATS 아키텍처) · TEE·원격증명 결합 프라이버시 구조 · infoq.com/news/2026/10/meta-private-process-ai-glasses/	TEE · 원격증명 · 익명 자격증명 · OHTTP
공공·정책	IM AI 경영전략	**글로벌 AI 벤처투자 집중구조와 국내 시사점** AI 투자 쏠림의 산업정책 시사점 · spri.kr/posts/view/24028?code=data_all	AI 벤처투자 · 투자 쏠림 · 산업정책

2. 오늘의 토픽 — 컨피덴셜 컴퓨팅(Confidential Computing)과 원격증명

SE CA AI NW | 출제 예상: **1교시** | 근거: **IETF RFC 9334 (RATS 아키텍처)**

2-1. 개념 및 정의

하드웨어 기반 TEE로 사용 중 데이터까지 암호화 보호하는 기술. 원격증명으로 실행환경 무결성을 검증해 클라우드 운영자까지 비신뢰 처리하는 효과.

2-2. 등장 배경

AI 글래스 등 웨어러블 AI의 상시 수집 데이터 클라우드 처리 확대. 운영자도 열람 불가한 처리 구조의 프라이버시 요구 증대.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
격리 실행	컨피덴셜 VM, TEE	메모리 암호화 기반 운영자 접근 차단
신뢰 검증	원격증명, 익명 자격증명	실행환경 무결성 증명과 사용자 비식별 인증
전송 경로	OHTTP 라우팅, TEE 내부 처리	요청자 IP 분리와 종단 간 처리 보호

2-4. 시험·실무 관점

- [CA 연계] CPU·GPU 메모리 암호화 엔진 기반 TEE 하드웨어 신뢰루트
- [AI 연계] 추론 데이터 보호를 위한 AI TRiSM 프라이버시 계층
- [NW 연계] OHTTP 결합 요청자-내용 분리 통신 구조

답안 필수 키워드 — TEE / 원격증명 / 컨피덴셜 VM / 익명 자격증명 / 사용 중 데이터 보호