정보관리기술사 데일리 다이제스트

2026-11-11 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	LAW AI SE 법·규제	**조달청 평가위원 사진 외부 생성형 AI 유출** 근거 「개인정보 보호법」(안전조치의무) · AI 개발·시험 단계 개인정보 외부 전송 사례 · dailysecu.com/news/articleView.html?idxno=209442	섀도 AI · 개인정보 유출 · 안전조치의무 · 생성형 AI
국제	SE NW CA 정보보안	**Cloudflare 머클트리 인증서 기반 PQC 웹PKI** 근거 NIST FIPS 204 (ML-DSA) · PQC 전환 대역폭 부담 해소 구조 · infoq.com/news/2026/11/cloudflare-merkle-certificates/	MTC · 양자내성암호 · 웹 PKI · 핸드셰이크
공공·정책	IM AI 경영전략	**에이전틱 AI 시대 AX 인재 진단과 정책 과제** AI 전환 인력 확보 정책 논점 · spri.kr/posts/view/24024?code=data_all	AX 인재 · 에이전틱 AI · 인력 정책 · AI 전환

2. 오늘의 토픽 — 머클트리 인증서(Merkle Tree Certificates, MTC)

SE NW CA | 출제 예상: **1교시** | 근거: **NIST FIPS 204 (ML-DSA), RFC 6962 (Certificate Transparency)**

2-1. 개념 및 정의

다수 인증서를 머클트리로 묶어 루트 서명 하나로 검증하는 인증서 구조. PQC 서명 크기로 인한 TLS 핸드셰이크 대역폭 증가 완화.

2-2. 등장 배경

PQC 서명·공개키의 수 KB 규모화에 따른 TLS 핸드셰이크 비대화. Cloudflare·Chrome 공개 CA 실험을 통한 실용성 검증 진행.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
발급 구조	머클트리, 루트 서명, 배치 발급	다수 인증서 일괄 서명으로 서명 횟수 절감
검증 방식	포함 증명, 감사 경로, 신뢰 앵커	해시 경로 검증으로 전송 데이터 축소
투명성 연계	로그, 공개 CA, 모니터링	발급 이력 공개 검증으로 오발급 탐지

2-4. 시험·실무 관점

- [SE 연계] PQC 전환 로드맵과 하이브리드 인증서 병행 전략
- [NW 연계] TLS 핸드셰이크 패킷 증가와 초기 혼잡윈도우 영향
- [CA 연계] 해시 기반 검증의 연산 부하와 하드웨어 가속

답안 필수 키워드 — 머클트리 / PQC / 웹 PKI / 인증서 투명성 / TLS 핸드셰이크