

정보관리기술사 데일리 다이제스트

2026-09-17 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE LAW 정보보안	카카오게임즈 해킹, 개인정보 140명 유출 근거 「개인정보 보호법」 (유출 통지·신고 의무) · 시스템 취약점 악용 실제 침해사례 · etnews.com/20260917000276	침해사고 · 개인정보유출 · 취약점공격 · 보안사고대응
국제	SE SW 정보보안	자바 27, 포스트 양자암호 표준 탑재 근거 NIST FIPS 203/204/205 (PQC 표준) · 양자시대 암호 전환 실증 사례 · infoq.com/news/2026/09/java27-released/	PQC · ML-KEM · ML-DSA · JDK27
공공·정책	LAW SE 법·규제	ISMS-P 인증심사 개편, 현장검증 강화 근거 「개인정보 보호법 시행령」 개정안 (ISMS-P 인증기준) · 인증제도 실효성 강화 정책 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&ntId=12500	ISMS-P · 개인정보보호법 · 시행령개정 · 인증심사

2. 오늘의 토픽 — 포스트 양자 암호(PQC, Post-Quantum Cryptography)

SE SW CA LAW | 출제 예상: 1교시 | 근거: NIST FIPS 203/204/205 (PQC 표준)

2-1. 개념 및 정의

양자컴퓨터의 쇼어 알고리즘 공격에도 안전한 차세대 공개키 암호체계. RSA-ECC 등 기존 암호를 대체해 양자시대 데이터 기밀성과 장기보안성 확보가 목적.

2-2. 등장 배경

NIST ML-KEM·ML-DSA 등 PQC 표준 확정에 따른 산업계 암호전환 가속. 자바27의 표준 API 탑재로 상용 소프트웨어 PQC 적용이 본격 확산.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
핵심 알고리즘	ML-KEM, ML-DSA, SLH-DSA	격자·해시 기반 양자내성 암호명 알고리즘
적용 계층	TLS 1.3, JDK 27, HSM	통신·플랫폼·키관리 계층별 PQC 통합 적용
전환 전략	하이브리드 암호, Crypto-Agility, 키 롤오버	기존·PQC 병행운용으로 점진적 마이그레이션

2-4. 시험·실무 관점

- [SE 연계] HNDL 공격 대비 선제적 암호 전환 필요성
- [CA 연계] 양자컴퓨터 상용화 시점과 암호 전환 골든타임 간 경쟁 구도
- [LAW 연계] KCMVP 등 국가 암호정책과의 정합성

답안 필수 키워드 — PQC / ML-KEM / ML-DSA / HNDL공격 / 크립토어질리티