

정보관리기술사 데일리 다이제스트

2026-09-19 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE CA 정보보안	PQC 전환·암호자산 진단 협력 체결 근거 NIST FIPS 203/204/205 (PQC 표준) · 양자컴퓨팅 위협 대비 암호전환 착수 · dailysecu.com/news/articleView.html?idxno=208543	PQC 전환 · 암호자산진단 · 양자내성암호 · MOU
국제	SE AI 정보보안	Azure AI Foundry 치명적 권한상승 결함 근거 CVSS 3.1 (Common Vulnerability Scoring System) · 클라우드 AI 서비스 최고위험 취약점 · thehackernews.com/2026/09/microsoft-patches-cvss-100-azure-ai.html	CVSS 10.0 · 권한상승 · Azure AI · 클라우드보안
공공·정책	LAW SE 법·규제	ISMS-P 심사기준 개편 시행령 입법예고 근거 「개인정보 보호법 시행령」 개정안 (ISMS-P 인증심사기준) · ISMS-P 인증제도 개선 추진 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttlId=12500	ISMS-P · 시행령 개정 · 인증심사 · 개인정보위

2. 오늘의 토픽 — 양자내성암호(PQC) 전환

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

2-1. 개념 및 정의

양자컴퓨터의 쇼어 알고리즘 공격에도 안전성을 유지하는 암호 알고리즘 체계. RSA·ECC 등 기존 공개키 암호를 대체해 장기 데이터 기밀성을 확보하는 차세대 암호 기술.

2-2. 등장 배경

양자컴퓨터 실용화 임박에 따른 선수집 후복호화(HNDL) 공격 우려 확산. 국내 보안기업 간 PQC 전환 및 암호자산 진단(Crypto Discovery) 협력 확대.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
표준 알고리즘	ML-KEM, ML-DSA, SLH-DSA	NIST 표준화된 PQC 키교환·전자서명 알고리즘
전환 전략	하이브리드 암호, Crypto Agility	기존·PQC 병행 적용해 이행 리스크 최소화하는 전략
자산관리	Crypto Discovery, 암호자산 인벤토리	조직 내 암호 사용 현황 식별·진단 체계

2-4. 시험·실무 관점

- [SE 연계] 암호 알고리즘 전환 로드맵과 이행 리스크 관리방안
- [LAW 연계] 개인정보 암호화 규정과 PQC 적용 의무화 논의
- [CA 연계] 양자컴퓨터 큐비트 발전과 암호해독 위협 시점

답안 필수 키워드 — PQC / 양자내성암호 / 하이브리드 암호 / Crypto Agility / HNDL 공격