정보관리기술사 데일리 다이제스트

2026-10-21 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	LAW IM SE 법·규제	**정보보호 공시 의무, 2027년 전체 상장사 확대** **근거** 「정보보호산업의 진흥에 관한 법률」 정보보호 공시 제도 · 기업 보안투자 투명성의 제도화 · dailysecu.com/news/articleView.html?idxno=208963	정보보호 공시 · 투자·인력 공개 · 보안 거버넌스 · 공시 대상 확대
국제	SE NW SW 정보보안	**eMudhra 중간CA 개인키 8건 유출, 브라우저 긴급 차단** **근거** RFC 5280 (X.509 PKI 인증서·CRL 프로파일) · PKI 신뢰사슬 붕괴 사례 · thehackernews.com/2026/10/eight-emudhra-ca-keys-compromised.html	중간 CA · 신뢰저장소 · 인증서 폐지 · PKI 신뢰사슬
공공·정책	LAW IM 법·규제	**개인정보 유출·침해사고 조사 절차 신속·공정·투명화** **근거** 「개인정보 보호법」 개인정보 유출·침해사고 조사 절차 · 개인정보 사고조사 제도 개선 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttId=12555	침해사고 조사 · 개인정보위 · 조사 투명성 · 사고 대응

2. 오늘의 토픽 — 중간 CA 개인키 유출과 PKI 신뢰사슬 긴급 차단

SE NW SW LAW | 출제 예상: **1교시** | 근거: **RFC 5280 (X.509 PKI 인증서·CRL 프로파일)**

2-1. 개념 및 정의

중간 CA 개인키 유출로 임의 서버 인증서 위조가 가능해지는 PKI 신뢰사슬 침해. 신뢰저장소 차단과 인증서 폐지로 위조 인증서 수용을 막는 사고 대응 체계.

2-2. 등장 배경

eMudhra 중간 CA 개인키 8건 유출에 따른 브라우저·Go 런타임 긴급 차단. 신뢰 앵커 하위 CA 한 곳의 침해가 전 인터넷 TLS 신뢰로 전이되는 구조적 위험의 현실화.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
예방	HSM 키 보관, 이름 제약, CA 키 의식	개인키 유출 방지와 발급 범위 제한
탐지	인증서 투명성 로그, CT 모니터링	위조 인증서 발급 공개 검증과 조기 탐지
대응	신뢰저장소 제거, CRL·OCSP, 클라이언트 긴급 패치	침해 CA 신뢰 철회와 검증기 차단

2-4. 시험·실무 관점

- [NW 연계] TLS 핸드셰이크 인증서 체인 검증과 폐지 확인 한계
- [SW 연계] 런타임·브라우저 신뢰저장소 갱신과 긴급 배포 체계
- [LAW 연계] 공인인증기관 사고 대응 책임과 신뢰 서비스 규제

답안 필수 키워드 — PKI / 중간 CA / 인증서 투명성 / 신뢰저장소 / CRL·OCSP