정보관리기술사 데일리 다이제스트

2026-10-30 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE SW LAW 정보보안	**회원정보 조회 API 공격에 의한 항공사 개인정보 유출** 근거 OWASP API Security Top 10 · API 인가·접근통제 실패 사례 · dailysecu.com/news/articleView.html?idxno=209172	API 보안 · 객체 수준 인가 · 속도 제한 · 이상행위 탐지
국제	SE SW NW 정보보안	**구글 OAuth 2.0 DPoP 도입, 토큰 탈취·재전송 차단** 근거 RFC 9449 (OAuth 2.0 Demonstrating Proof of Possession) · Bearer 토큰 한계 보완 표준 적용 · infoq.com/news/2026/10/google-dpop-oauth2/	DPoP · 발신자 제약 토큰 · 재전송 공격 · Bearer 토큰
공공·정책	LAW SE 법·규제	**고객센터 개인정보 조회 최소화·접근통제 강화** 근거 「개인정보 보호법」 안전조치 의무 · 상담 화면 개인정보 통제 기준 제시 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttId=12601	마스킹 · 최소 조회 · 접근통제 · 오남용 방지

2. 오늘의 토픽 — DPoP(Demonstrating Proof of Possession)

SE SW AI NW | 출제 예상: **1교시** | 근거: **RFC 9449 (OAuth 2.0 Demonstrating Proof of Possession)**

2-1. 개념 및 정의

클라이언트 개인키 서명 증명을 요청마다 첨부해 토큰을 해당 키 소유자에게 결속시키는 OAuth 2.0 발신자 제약 기법. 탈취된 액세스 토큰의 재전송 악용 차단 목적.

2-2. 등장 배경

Bearer 토큰은 소지만으로 사용 가능해 탈취 시 즉시 악용 가능. 구글 OAuth 플랫폼의 DPoP 지원으로 애플리케이션 계층 토큰 결속 방식 확산.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
키 결속	클라이언트 키쌍, DPoP 증명 JWT, 공개키 지문	공개키 지문을 토큰에 결속시키는 구조
요청 검증	htm·htu 클레임, jti, iat	메서드·URL·시각 일치로 재전송 차단
서버 보강	서버 nonce, ath 클레임, 토큰 해시	사전 생성 증명 방지와 토큰 연결 검증

2-4. 시험·실무 관점

- [SE 연계] Bearer 대비 mTLS·DPoP 발신자 제약 비교
- [SW 연계] API 게이트웨이 증명 검증과 jti 중복 저장소 설계
- [AI 연계] 에이전트 토큰 탈취 대응 수단으로서의 키 결속

답안 필수 키워드 — DPoP / 발신자 제약 토큰 / Bearer 토큰 / 재전송 공격 / mTLS