최근 항공 사이버 보안 사례와 시사점

– B737 정비접속부 물리 삽입 공격 연구와 델타항공 비인가 기내 Wi-Fi 사례 –

발행일 2026. 8. 18. | 제2026-3호

항공 사이버보안은 전산 부서만의 업무가 아니라 출입통제·내부자 관리·정비보안·객실서비스가 연결된 항공보안의 새로운 과제

□ 최근 사례

가. Boeing 737 물리 삽입 공격 연구

o UC San Diego·Oberlin College 연구진은 B737 NG·MAX의 전자·장비실(E&E Bay)에 약 60초 접근해 정비 접속부에 소형 장치를 삽입하는 시나리오 검증

o 신호를 임의로 조작하는 방법으로, B737 시험 설비에서 비행계획과 중량·균형 자료 조작 가능성 확인

o 이는 실제 운항 항공기 침해 사건이 아닌 물리적 접근 전제의 통제 환경 下 연구이며, 연구진은 임박한 위협으로 평가하지는 않음

나. Delta Air Lines 591편 비인가 기내 Wi-Fi 사건

o 2026. 8. 10. 라스베이거스發 애틀랜타行 591편에서 'Delta Wifi Fast'라는 비인가 무선망 식별, 승무원이 기내 Wi-Fi를 중단하고 지상·기업 보안부서에 통보

o Delta는 自社 제공·운영망이 아니며, 自社 시스템과 기내 Wi-Fi의 해킹 및 항공기 운항시스템 영향은 없었다고 발표

□ 평가 및 진단

가. 시스템 분리를 넘어선 통합적 운영 관리 필요

o B737 연구는 물리적 접근을 통해 심각한 영향을 초래할 수 있는 고위협 사건이며, Delta 사례는 객실 서비스 영역에서 발생한 저강도 보안사건

o 위험수준은 다르지만 '시스템 분리'만으로 충분하지 않으며, 지상 접근·정비 작업·객실 서비스·승객 보호를 연결하는 운영통제가 필요

나. 사이버보안의 출발점은 물리적 접근통제

o 정비접속부와 객실 무선망은 권한·기록·현장확인이 느슨하면 보안 사각지대로 전환

o 따라서 출입증 보유 여부 확인보다, 작업 목적·시간·사용 장비·완료 결과를 연계 확인하는 '업무 단위 검증'이 핵심

□ 항공보안 측면의 시사점

가. 항공 사이버보안 보호대상 확대

o 항공기 주요 정비접속부, 정비 노트북·시험장비·저장장치와 MRO·지상조업사 접근권한을 기존 항공보안 위험평가에 포함

o 기내 Wi-Fi·승객 포털은 운항계통과 분리돼 있어도 개인정보 보호와 항공사 신뢰 차원에서 관리 필요

나. 사건 분류와 초동조치의 표준화

o 비계획 정비 시 작업지시서·작업자·접근시간·반입장비를 기존 기록체계에서 대조하고 중요 접속부는 위험도에 따라 훼손확인 봉인·2인 확인 적용

o 정비 완료 후 비인가 장치 잔류 여부를 기존 복구점검 항목에 포함

다. 객실 Wi-Fi는 과잉 차단보다 단계적 대응

o 공식 SSID·접속 도메인을 앱·기내화면·안내문에 표시하고, 승무원 1쪽 조치카드에 발견시각·SSID 기록, 통보, 로그보존 절차 명시

o 모든 미확인 SSID를 해킹으로 간주하지 않고 항공사 명칭 도용·피싱 화면·접속방해 등 추가 징후에 따라 서비스 격리 결정

라. 신규 규제보다 기존 점검·훈련의 보완

o 항공사·MRO 보안점검과 비상대응훈련에 '정비접속부 비인가 장치'와 '객실 비인가 무선망' 시나리오를 추가

o 탐지 → 운항영향 판단 → 서비스 격리 → 증거보존·통보 → 무결성 확인 → 정상화를 공통 흐름으로 적용

□ 결론

- o 항공 사이버보안은 전산보안만의 문제가 아니며, 출입통제·내부자 관리·정비보안·객실서비스가 연결된 항공보안 과제
- o 대규모 신규 시스템보다 작업기록 교차확인, 핵심 접속부 점검, 공식 SSID 고지와 승무원 초동조치 표준화를 우선할 필요

※ 참고자료

- o USENIX Security '26 발표·논문
- o Delta Air Lines 공식 기내 Wi-Fi 안내
- o Delta 591편 사건 및 Delta·FAA·FBI 입장
- o ICAO Aviation Cybersecurity Strategy