美 GAO 항공통신 사이버보안 감사 결과와 항공보안 시사점

– 조종사가 주고받는 관제통신 메시지의 가로채기·사칭·전파방해 취약점 지적 –

발행일 2026. 9. 24. | 제2026-10호

미국 회계감사원(GAO)이 9. 21. 조종사가 지상과 문자로 주고받는 관제통신(ACARS : 항공사-항공기 업무 메시지, CPDLC : 관제사-조종사 지시 문자)이 가로채기·사칭·전파방해에 취약하다고 지적하고 FAA에 9개 권고를 제시

→통신보안의 핵심은 '통신이 잘되는가'가 아니라 '내용의 변조·왜곡 등 불법적 시도를 막는 것'

감사 개요

가. (감사기관) 미국 회계감사원(GAO) : 의회를 지원하는 독립 감사·평가기관

나. (감사대상) FAA의 항공기-지상 통신에 대한 사이버 위협 대응체계

다. (발표경위) 와이든 상원의원 요청, 2026. 9. 21. 보고서(GAO-26-108439) 공개

라. (감사결과) 실제 사고가 아닌 취약점·위험관리 미비를 지적, FAA에 9개 권고

* 와이든 의원 : "관제사와 항공기의 통신 기술은 매우 불안전하며 가로채기·사칭·방해가 가능하다"

감사 배경 : 잇따른 전파방해 사례

가. 유럽 전역의 GPS 방해 급증

- 2022년 우크라이나 전쟁 이후 발트해·흑해 등에서 **GPS 방해(재밍)·기만(스푸핑) 급증** — 러시아 소행으로 지목

  * 라트비아 위성신호 방해 건수 : 2022년 26건 → 2024년 820건

- 2024. 4. 핀에어는 GPS 방해로 착륙에 두 차례 실패한 뒤 **에스토니아 타르투 노선을 한때 중단**

나. 정부 요인 탑승기 피해

- 2025. 9. 로블레스 스페인 국방장관 탑승기(A330)가 칼리닌그라드 인근에서 GPS 방해를 받았고, 같은 달 **폰데어라이엔 EU 집행위원장 탑승기도 불가리아 착륙 중 방해**

  * 두 기체 모두 대체 항법으로 무사 착륙했으나, 위성항법에 의존하는 민간 운항의 취약성이 드러난 계기

- 이런 사례가 잇따르면서 미 의회가 항공통신 전반의 보안 점검을 요청, **이번 감사로 이어짐**

항공기와 지상 간 정보 교환 방법

가. 음성 무전과 문자 데이터통신의 병행

- 항공기와 지상은 음성 무전 외에 **문자 형태의 데이터통신**으로 운항정보와 관제지시를 교환 — 복잡한 지시를 화면에서 다시 확인해 **음성 전달의 오해를 줄이는 장점**

나. 조종사가 받는 문자통신 구분

구분	주요 기능 및 역할	활용
ACARS	항공기와 항공사·지상 간 **업무용 메시지 체계**	운항 관련 보고·요청·정보 교환
CPDLC	관제사와 조종사 사이의 **관제용 문자통신**	고도·항로·속도·주파수 변경 지시와 응답

다. 취약점 평가

- 두 시스템 모두 설계 당시 **발신자 인증과 암호화가 없어** 가로채기나 관제사를 사칭한 가짜 지시가 가능한 구조
  * 현재는 조종사가 절차에 따라 메시지를 검토·수락하는 과정이 사실상 **마지막 안전장치** 역할

감사 결과 및 대책

가. 네 영역의 지적과 권고

영역	확인된 지적	GAO 권고(대책)
위험평가	스푸핑·재밍 위협은 파악했으나 **위험평가·보안문서 미흡**	위험평가 완료, 보안문서 보완
실시간 감시	전파 위협을 **실시간 탐지하는 체계 없음** — 신고 후 조사 방식	실시간 감시·탐지 역량 확보
통신 보호	ACARS·CPDLC의 **인증·암호화 부재**	인증·데이터 보호 강화 계획 수립
기관 간 협력	협력체계는 있으나 **민간 관계자와의 정보공유 지침 부재**	정보공유·보고·조정 절차 문서화

나. 이행 현황 : 미 교통부는 9개 권고에 모두 동의

- FAA : “항공기와 운항이 더 연결될수록 사이버·전자기 취약점의 위험이 커진다”며 **권고 이행 입장**

평가 및 진단

가. 통신보안에서 확인해야 할 핵심 질문

- 메시지가 화면에 정상 표시되더라도 그 사실만으로 **발신자와 내용의 신뢰성이 입증되는 것은 아님**

확인할 질문	보안 개념	일상적인 비유
정말 권한 있는 사람이 보냈는가	**인증**	발신자를 사칭한 가짜 문자 구분
전달 중 내용이 바뀌지 않았는가	**무결성**	원본과 받은 문서의 내용 대조
허용된 사람만 읽을 수 있는가	**기밀성**	업무정보를 외부인이 읽지 못하게 보호
필요할 때 정상 사용할 수 있는가	**가용성**	중요한 순간에도 통신 유지

나. 외부 위협과 내부 위협 진단

- GPS 방해처럼 외부에서 전파로 가해지는 위협은 기술 부서의 영역이나, **통신·정보시설에 접근할 수 있는 사람이 정보를 바꾸거나 권한을 넘겨주는 경로는 물리적 보안의 영역**
- 인증과 암호화가 없는 통신체계에서는 **시설 출입·장비 접근·작업기록 관리가 곧 정보 보호의 첫 번째 방어선**

항공보안 측면의 시사점

가. 물리적 출입관리와 정보보호의 연결

- 통신·정보시설 보호는 장비만이 아니라 **접근하는 사람, 유지보수 작업, 권한 변경과 작업기록**을 함께 관리해야 가능

  → 출입이 허용된 사람이라도 승인된 업무범위를 벗어난 행위는 별도 확인

나. 이상징후를 정확히 보고하는 역량

- 현장 근무자가 원인을 규명할 필요는 없음 — **발생시각·장소·현상·영향을 기록해 담당자에게 전달**하는 역량이 핵심

  * “해킹당했다”는 추정보다 “어떤 정보가 어떻게 달랐는지”를 보고하는 방식이 조사와 대응에 유용

다. 기술 부서와 보안 부서의 역할 구분

- 기술 원인 분석은 전문부서, 현장 보안조직은 **시설보호·출입관리·상황보고·기록 보전**에 집중하도록 역할 정리

라. 내부자 위협 교육과의 연계

- 이번 감사가 드러낸 ‘인증 없는 정보’ 문제는 최근 항공보안의 핵심 이슈인 **내부자 위협과 맞닿아 있음** — 정당한 출입권한을 가진 사람이 정보·시설에 접근해 변조·유출·사칭의 통로가 될 수 있음

  → 협회는 항공보안 요원 교육 프로그램에 이번 사례를 반영해, 출입증관리·보안문화·내부자 위협 교육에서 ‘정보의 출처와 정확성 확인’을 함께 다룰 예정

결론

- 공항보안 교육은 사람·물품 확인 역량에 더해 **업무에 쓰는 정보의 출처와 정확성을 확인하는 역량**을 강화할 필요
- 통신·관제 전문부서의 역할은 존중하되, 공항 근무자가 할 수 있는 **이상징후 인지·정확한 보고·공식 경로 확인·기록 보존**을 교육에 반영
- 협회는 GAO 권고 이행 경과를 계속 모니터링하고, **통신보안(정보 신뢰성 확인) 교육 모듈 개발** 방침

※ 참고자료

- Aviation Cybersecurity: Threats to Aircraft Communications (GAO-26-108439, 2026. 9. 21.)
- FAA Must Better Address Threats to Aircraft Communication (Reuters, 2026. 9. 21.)
- Aircraft Communications with FAA ‘Incredibly Insecure’ (Insurance Journal, 2026. 9. 22.)
- Spanish minister’s plane hit by GPS jamming near Kaliningrad (AeroTime, 2025. 9. 24.)
- Data Communications (Data Comm) (FAA, 항공 데이터통신 프로그램)