Original Article

https://doi.org/10.12985/ksaa.2023.31.4.072
ISSN 1225-9705(print) ISSN 2466-1791(online)

운항승무원 전자비행정보장치(EFB) 사용에 따른 사이버보안 법률 및 정책 필요성 연구

강민호*, 전상훈**, 황호원***

A Study on the Necessity of Cybersecurity Legislation and Policies in Response to the Use of EFB by Flight Crew

Minho Kang*, Sanghoon Jeon**, Howon Hwang***

ABSTRACT

The use of EFB (Electronic Flight Bag) has expanded, providing convenience to flight crews by minimizing paper usage within aircraft and offering the latest information, operability, and convenience related to aircraft operations. EFBs provide flight-sensitive information such as aircraft performance calculations, airport diagrams, routes, and approach procedures. For these information, EFBs connect to the cyber environment through Wi-Fi or self-contained data communication, allowing access to cloud-based systems for information updates, with administrators uploading the latest information for retrieval. However, in contrast to the evolving aviation technology, there is currently no legislation or security policy in place to maintain the security of EFBs, leaving them exposed to potential cyber threats. Therefore, improvements such as revising relevant laws to address potential cyber threats targeting EFBs and establishing and implementing EFB management systems are necessary. This paper aims to present the necessity for amending laws related to EFB security in response to cyber threats and suggests methods for enhancement.

Key Words : Flight Crew(운항승무원), EFB(전자정보비행장치), Aviation Security(항공보안), Cyber Security(사이버보안), Policy(정책)

Ⅰ. 서 론

현대 사회는 정보통신기술의 발전과 더불어 전자장비도 빠르게 발전하고 있으며, 많은 양의 정보를 보관, 저장능력의 확장으로 정보 수용력도 향상됐다. 이를 토대로 더 빠르게 정보를 찾을 수 있고, 더불어 업무의 정확성과 처리 능력도 빨라졌다. 그로 인해 의존성은 시간이 지날수록 커지고 있음이 현실이다.

항공산업에서도 정보통신의 발전으로 지상과 항공기는 현재 수많은 통신정보를 교환하고 있으며, GNSS (Global Navigation Satellite System)를 이용한 위치 정보, 항공기 성능 검토, 운항과 정비에 사용되는 정보, 항공기 시스템 관리 정보 등이 항공기 내에서 공유되고 지상에도, 해당 정보들을 전송하고 있다. 또한,

Received: 13. Nov. 2023, Revised: 29. Nov. 2023, Accepted: 11. Dec. 2023
* 한국항공대학교 항공우주법학전공 석사과정
** 극동대학교 해킹보안학과 교수
*** 한국항공대학교 항공교통물류학부 교수
연락저자 E-mail : kangminho12@naver.com
연락저자 주소 : 경기도 고양시 덕양구 항공대학로 76

승객들에게 발전된 서비스를 제공하기 위한 유료 혹은 무료 무선 인터넷(WIFI) 서비스까지 제공하기에 이르렀다. 또한, 조종실에서도 운항승무원에서 태블릿 PC를 지급하여 매뉴얼과 운항 정보를 저장하고, 항공기의 이·착륙을 위한 성능 검토, 항공기 운항에 관한 정보를 제공함으로써 운항의 정밀성과 편리성을 높여 주었다. 이러한 태블릿 PC의 형태로 운항 정보를 제공하는 장치를 EFB(Electronic Flight Bag) 즉, 전자비행정보장치라고 한다.

전자비행정보장치의 정보 업데이트는 무선 인터넷 혹은 유·무선 통신을 통해 클라우드 서버, 중앙 컴퓨터 혹은 PMS(Patch Management System)에 접속하여 정보를 내려받는 형태로 이루어지고 있다. 그로 인해 지정된 장소나 지정된 통신망을 이용해서 업데이트하지 않고 보안 애플리케이션이 설치되어 있지 않으며, 무선 인터넷이나 블루투스 기능을 차단하지 않고 사용하여 보안 통제 조치가 제대로 이루어지고 있지 않아 사이버보안 관리체계와 지침이 필요하다.

국내에는 전자비행정보장치와 관련된 내용은 국토교통부의 「고정익 항공기를 위한 운항기술 기준」에 전자비행정보장치(EFB) 정의와 사용 승인 시 확인해야 할 내용 등의 개괄적인 내용만이 기술되어 있다. 세부적인 내용은 ICAO에 따른다고 되어 있으나, ICAO 부속서도 사이버보안에 관한 세부적인 지침은 미비한 상태이다. 그렇다고 해서 국내 자체적인 보안 관련 법률이나 관리정책 체계나 지침은 항공산업에 적용하기에 한계가 있는 상황이며, 항공보안법은 물리적 보안을 주로 명시하고 있어 사이버 위협을 대비하기에는 미비한 상황이다. 그러므로 전자비행정보장치 사이버보안을 위한 관련 법률의 개정과 관리정책 및 지침의 개선이 필요한 시점이다.

본 논문 2장에서는 사이버보안 위협과 국내외 사이버보안의 정의 및 규정, 국내외 EFB 관리현황을 살펴보고, 3장에서는 사이버보안을 위한 정책 및 법률 등과 ISO/IEC-27000 시리즈를 바탕으로 한 EFB 보안체계 구축의 개선 필요성을 제시한다. 그리고 4장에서는 개선방안을 제시하고 결론으로 마무리한다.

II. 본 론

2.1 사이버보안 위협

보안은 의도에 의한 불법행위로부터 국민의 생명과 자산을 보호하여 사회의 안녕과 질서를 유지하는 활동을 말하며, 현대 빈번히 발생하는 사이버 위협 유형은 Table 1과 같다.

Table 1. Statistics on incidents of breaches by type in the year 2022

구분	내용	비율
악성코드	1. 악성코드를 통한 공격 꾸준히 발생. 2. 서비스형 랜섬웨어(RaaS)의 대중화로 인해 사이버 공격에 대한 진입장벽이 낮아짐. 3. 대표적인 RaaS 랜섬웨어는 LockBit, Conti, Blackcat 등.	39.2%
중요정보 유출	1. 취약점을 이용한 정보탈취 후 다크웹, 블랙마켓 판매. 2. 최근 텔레그램, 디스코드와 같은 암호화 채널을 활용하여 거래하는 추세. 3. 해킹 그룹 랩서스의 국내외 대기업 기밀정보 탈취.	32.3%
피싱/스팸	1. 피싱을 통한 탈취 시도 증가. 2. 대상의 권한을 획득하거나, 가상자산을 탈취.	15.7%
시스템 장악	시스템 장악을 통한 금전 및 서비스망 마비.	11.8%
공급망 공격		1.0%

Table 1과 같이 악성코드를 이용한 공격이 39.2%로 가장 빈도가 높음을 확인할 수 있다. 즉, 악성코드를 이용한 사이버 공격이 가장 일반적이다. 악성코드는 이메일, 링크, 웹사이트 등을 통해 배포하고, 사용자가 접속할 시 사용자 시스템에 설치되어 악의적인 목적으로 사용된다. 현재까지 사례는 없으나 이러한 유형들은 전자비행정보장치에도 발생될 수 있으며, 메일을 통해 혹은 중앙 서버를 통해 악성코드를 배포하여 전자비행정보장치를 사용 불가능하게 만들거나, 전자비행정보장치를 통해 중앙 서버 또는 PMS와 같은 배포 서버에 접속하여 잘못된 정보를 내려받게 하는 등의 방법으로 항공기 안전운항에 치명적인 결과를 초래할 수 있다.

2.2 국외 사이버보안 기준과 법률

국제민간항공기구(ICAO)는 Table 2와 같이 사이버보안 관련 지침을 제공하고 있다.

Annex 17 Security의 내용 중 불법방해행위는 항공기를 불법으로 멈추는 행위, 항공기 서비스의 방해 등의 내용을 말하며, 사이버 위협과 관련된 조치 중 표준 내용을 보면 체약국은 각 국가의 민간항공 보안 프로그램에서 운영자 또는 주요한 정보 및 정보통신기술

Table 2. ICAO documents on cybersecurity

	내용
Annex 17 - Security	국제 민간항공에 대한 불법 간섭 행위로부터 보호에 대한 부속서
Doc 10049 - ICAO Cybersecurity Strategy	민간항공의 사이버보안 문제를 해결하기 위한 ICAO의 전략적 접근 방식에 대한 개요
Doc 10048 - ICAO Cybersecurity Guidance Material	사이버보안 조치를 강화하는 데 도움이 되는 지침 및 활용법 제공
Doc 8973 – ICAO Aviation Security Manual	Restricted 문건으로 안전, 보안 등의 규제 절차들을 다양한 측면으로 다루고 있다.
GASeP - ICAO Global Aviation Security Plan	사이버 위협에 관한 내용을 포함한 모든 항공보안에 대한 위협 해결을 위한 접근 방식 제공
ICAO Cyber security Toolkit	항공 분야 사이버보안 조치를 개발하고 구현하기 위한 툴킷 제공

시스템과 데이터를 식별하고, 위험 평가에 따라 불법 방해행위로부터 보호하려는 조치를 적절하게 개발 및 이행되도록 보장해야 한다고 서술되어 있다. 권고사항으로는 체약국은 식별된 중요 시스템 및 데이터의 기밀성, 무결성 및 가용성을 적절하게 보호되도록 하고, 특히 당국이 수행한 위험 평가에 따라 설계, 공급망 보안, 네트워크 분리, 원격접근 통제 및 보호 조치 포함을 권고하고 있으며(ICAO, 2022), ICAO는 현재 전 세계적 조화와 일관성을 위해 사이버보안 정책 지침을 개발하려고 하고 있다(ICAO, 2022).

미국은 국무부 주도하에 2015년 사이버보안을 개선하기 위해 정부와 민간 기관 간의 사이버 위협 정보를 공유하고, 이에 따른 유인책을 제공하는 CISA(The Cyber security information sharing act)를 제정하였다. 이는, 민간 부문 사이버보안 정보 공유를 촉진하는 명령으로 정부와 민간 간의 사이버 위협 정보 공유를 장려를 목적으로 한다. 이후 2019년에 국토안보부를 중심으로 관련 기업과 기관을 관리, 감독하여 기반시설을 보호를 확립하고, 책임과 의무 개선, 국가위험 식별에 따른 우선순위 결정, 사이버보안 투자증진, 연구 및 개발투자 우선순위 결정, 운송・해상・우주 공간의 사이버보안을 위한 국가 사이버안보 전략을 발표하였다(박상돈과 김인중, 2012).

CISA와 더불어 미국의 ATSA(Aviation and Transportation Security Act)는 항공교통보안법으로 보안 문제 발생 시 대응방법을 위주로 구성된 법안이다. ATSA를 통해 미국은 FAA에서 항공보안까지 전담하는 것에 한계가 있다고 판단하여 ATSA를 근거로 교통보안청을 설립하였다. 또한, 위협 검토를 통해 민간 항공기의 파괴, 징발 또는 민간 항공기의 무기화의 내용이 명시되어 있으며, 이후 사이버 공격을 포함한 민간항공 서비스의 방해를 추가하였다(정원희, 2020). 이를 바탕으로 미국에서는 현대 항공기의 통신, 내비게이션과 기타 시스템들이 네트워크를 통해 쌍방향 통신을 하고 있으며, 이 때문에 항공기 네트워크에 잠재적 사이버 위협이 발생할 수 있다고 판단하여 보안을 위한 프로그램인 AC 119-1 ANSP(Airworthiness and Operational Authorization of Aircraft Network Security Program)을 제정하였다(박상돈과 김인중, 2012).

현재 ICAO에서는 사이버보안을 위한 개괄적 기준과 지침만을 제시하고 있고, 미국은 항공 사이버보안을 위해 법률의 제・개정을 하고 있으며, 정책 개발에는 노력하고 있다. 하지만 정책과 대응방안에 대한 세부적인 내용 제공에는 한계를 갖고 있다.

2.3 국내 사이버보안 법률 및 지침

국내 민간항공사의 IT 인프라는 「정보통신기반보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「개인정보보호법」 등의 법적 근거를 통해 사이버 위협에 대응하고 있다. 정보통신기반 보호법 제2조 정의에서 정보통신기반시설이란 국가안전 보장・행정・국방・치안・금융・통신・운송・에너지 등의 업무와 관련된 전자적 제어・관리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제1호에 따른 정보통신망을 말한다고 명시하고 있다. 정보통신기반시설에 운송이 포함되어 있으며, 운송업무와 관련된 전자적 제어관리시스템이라고 정의하고 있으며, 정보통신기반시설을 공격하는 행위를 전자적 침해행위라고 한다.

전자적 침해행위에는 해킹, 컴퓨터바이러스, 논리・메일 폭탄, 서비스거부 또는 고출력 전자기파 등의 방법이 있으며, 추가로 정상적인 보호・인증 절차를 우회하여 정보통신기반시설에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신기반시설에 설치하는 방법을 말한다. 이후 전자적 침해행위로 발생한 사태를 침해행위라고 한다. 전자적 침해가 발생한 경우, 제12조 주요 정보 통신기반 시설 침해행위 등의 금지에 따라 제28조 벌칙에 의거 10년 이하의 징역 또는 1억 원 이하의 벌금을 매긴다. 또한, 미수범도 처벌한

다(정보통신기반 보호법, 2022). 제6조에 관계 중앙행정기관의 장은 관리기관에 제출받은 주요 정보 통신기반 시설의 보호 대책을 종합·조정하여 소관 분야에 대한 주요 정보 통신기반시설에 관한 보호 계획을 수립·시행해야 한다. 국내도 국토교통 사이버안전센터가 운영 중이다. 이는 국토교통부의 정보보호 업무 담당 부서에서 운영하며, 정보통신기반시설에 대한 보호 대책 수립과 지도·감독, 사이버 공격에 대한 대응 그리고 기술개발을 하는 역할을 한다.

그러나 사이버보안에 관한 국내법률들은 항공에까지 적용하는 것은 내용적 한계가 있으며, 「항공보안법」, 「항공안전법」 이하 시행령, 시행규칙과 운항기술기준에 사이버보안의 내용과 정보통신시스템의 전자적 침해행위 등의 사이버 위협에 대응하는 법률과 정책이 미비하다는 문제점이 남아 있다(Jeon, 2023).

2.4 사이버보안을 위한 국제표준화기구의 관리 정책

국제표준화기구(ISO)는 정보와 데이터 보안을 위한 관리정책으로 정보보호 및 개인정보 보호 관리체계인 ISMS(Information Security Management System)를 제시하고 있다. 조직의 중요한 데이터를 체계적으로 관리하기 위한 정책과 절차로 위험을 최소화하고, 비즈니스의 연속성을 보장, 정보 및 기술과 더불어 직원의 행동까지 정보보안을 위해 지켜야 할 시스템을 제시하고 있다. 국가기관과 기업은 ISMS 인증을 받음으로써 사이버보안을 위해 노력하고 있다는 것이며, ISMS 구축을 위해 국제표준화기구는 ISO/IEC-27000 시리즈를 국제표준 사이버보안 관리정책으로 제시하고 있다. 이는 정보보안 관리 지침, 조직의 ISMS 구축, 유지 및 개선을 목적으로 한다(ISO/IEC, 2018). 주요 내용은 다각화된 위협으로부터 민감한 정보와 데이터 보호를 위해 ISMS를 구축하고, 위기관리 및 위험성 평가를 통해 의사 결정을 할 수 있게 한다. 그리고 정보 보안과 관련된 관련 법률, 규정 및 계약상 의무를 준수할 수 있게 한다. 전자비행정보장치 보안 관리에 적용할 수 있는 ISO/IEC-27000 시리즈는 Table 3과 같다.

ISO/IEC 27000 시리즈 중 ISO/IEC-27001은 조직의 ISMS를 구축, 유지 및 개선을 위한 요구사항을 제시하며, 기밀성, 무결성 및 가용성 보장으로 민감한 정보 관리를 위한 체계적이고 구조화된 접근방식을 제공한다(ISO/IEC, 2022). ISO/IEC-27002는 ISO/IEC-27001 부속서 A에 명시되어 있는 ISMS를 구축하기 위한 자세한 기준과 활용법을 제공하며, 위험 평가를 통해 확인된 위험을 제어하는 기준 제공을 통해 27001을 보완하는 역할을 한다(ISO/IEC, 2013). ISO/IEC-27004와 같은 경우, ISMS 구축 후 효과를 측정하기 위한 지침서로 관리체계 모니터링, 검토, 분석과 평가를 통해 보안 정책의 유지 및 개선을 위한 지침을 제공한다. 그리고 ISO/IEC-27005는 정보보안 위험관리에 중점을 둔 표준서로 조직의 정보보안 요구에 맞는 효과적인 위험 관리 프로세스를 수립할 수 있도록 기준과 활용법을 제시한다. 잠재적 사이버 위협 발생 시 대응방안이 될 수 있는 지침서이다(ISO/IEC, 2022). ISMS를 구축한다는 것은 정보의 기밀성, 무결성 및 가용성을 유지하기 위한 노력을 보여주어 조직의 신뢰성을 확보하고 국제적으로 인정을 받은 것이고, ICAO에서도 2022년 Cybersecurity Action Plan 문서 6.1에 ICAO에서는 전체성을 보장하는 항공 사이버보안을 위해 내부 거버넌스 구조를 구축해야 한다고 하였다. 따라서 국가는 민간항공 사이버보안을 위한 거

Table 3. List of ISO/IEC 27000 series for security management of electronic flight bag (EFB)

구분	제목
ISO/IEC-27000	Overview and vocabulary
ISO/IEC-27001	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
ISO/IEC-27002	Information security, cybersecurity and privacy protection — Information security controls
ISO/IEC-27003	Information security management system implementation guidance
ISO/IEC-27004	Information security management — Monitoring, measurement, analysis and evaluation
ISO/IEC-27005	Guidance on managing information security risks
ISO/IEC-27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC-27007	Guidelines for information security management systems auditing
ISO/IEC-27017	Code of practice for information security controls based on ISO/IEC 27002 for cloud services

버넌스 및 책임 구조를 정의하고 이행해야 하며, 국가 및 국제 사이버보안 및 사이버 복원력 요구사항의 개발 및 이행을 보장해야 한다고 하였다. 거버넌스 구축 방안 중 하나로 ISMS를 언급하였고, ICAO는 ISMS가 사이버보안을 관리하는 효과적인 도구가 될 수 있으며, 국가 또는 조직 차원에서 구현될 수 있다고 하였다(ICAO, 2022).

2.5 국외 전자비행정보장치(EFB)에 관한 기준과 정책

ICAO는 항공기 운항 또는 지원을 위해 전자비행정보장치에 정보를 저장, 업데이트, 표시 및 처리하는 전자 정보 시스템으로 전자비행정보장치를 정의하고 있다(ICAO, 2018). 또한, 전자비행정보장치 장착 장치, 전원공급, 장비의 형태, 신뢰성 등에 관한 내용과 더불어 전자기기인 전자비행정보장치에 미칠 수 있는 악영향에 대한 기본적인 내용이 서술되어 있다.

전자비행정보장치에 미칠 수 있는 악영향은 배터리 누출, 안정성, 과열로 인한 위험과 전자비행정보장치와 인적요소(Human Factor)와 같은 물리적인 내용만 명시하였다. 그리고 물리적 예방책으로 전자비행정보장치 시스템 설계, 전자비행정보장치 전용 전원 및 백업 전원. 애플리케이션의 이중 설치를 통한 백업 사용과 예비 목적으로 종이 문서휴대. 조종실 내 종이 문서를 보관 등의 제시하고 있다(ICAO, 2018).

미국연방항공국(FAA)은 조종석 또는 객실내 사용을 목적으로 하며, 전자 디스플레이 시스템이라 전자비행정보장치를 정의하고 있으며, 항공데이터 및 계산 수행 장치로, 애플리케이션 및 데이터베이스 등의 기능과 범위를 아래와 같이 구분하고 있다.

- Class 1(휴대용): 승인 필요 없이 설계, 생산 또는 승인되는 휴대용 전자 장치로 간주하여 사용되는 휴대용컴퓨터로 항공기에 장착하거나 항공기 시스템에 연결하거나 전용 항공기 전원공급 장치에 연결되지 않는 장치(FAA, 2007).
- Class 2(장착형/부착형): 설계, 생산 또는 설치 승인이 필요 없는 휴대용 전자 장치이나 항공기 장착 장치에 장착할 수 있는 장비를 말한다. 다만 탈부착이 쉬워야 하며, 항공기 전원공급 장치에 연결할 수 있는 장치(FAA, 2007).
- Class 3(항공기 장착형): 항공기 감항 규정을 따른 장치(AC 20-173)(FAA, 2011).

FAA에서는 전자비행정보장치에 설치되는 소프트웨어도 Type A/B/C로 분류한다(FAA, 2017).

- Type A는 종이 문서 대체용으로 비행 중에 필요한 문서들이 아닌 FOM, SOP, FCOM 등을 포함하는 애플리케이션(FAA, 2017).
- Type B는 비행에 필요한 정보들을 제공해주는 애플리케이션(FAA, 2017).
- Type C는 RTCA/DO-178B 준수나 다른 허용 가능한 수단으로 FAA가 승인한 소프트웨어(FAA, 2017).

ICAO와 FAA 모두 사이버보안의 필요성을 인지하고, 기준, 법률, 정책, 체계를 만들려고 하고 있으나, 전자비행정보장치에 대해서는 정의와 사용에 따른 분류와 물리적인 보안에 대해서만 언급하고 있을 뿐이다. 사용이 확대되고 있음에 따라 사이버 위협에 노출이 더 쉬운 전자비행정보장의 내용에 사이버보안의 내용은 ICAO, FAA 모두 미비하다.

2.6 국내 전자비행정보장치에 관한 기준과 정책

국내 전자비행정보장치는 「고정익 항공기를 위한 운항기술 기준」에서 운항승무원의 항공기 운항 및 비행 근무를 지원하기 위해 사용되는 전자비행정보장치이며, 저장, 갱신, 시현, 처리 기능을 할 수 있는 장치 및 소프트웨어로 구성된 전자정보시스템이라 정의하고 있으며, 전자비행장치의 장비, 기능, 운영승인에 대한 세부적인 사항은 ICAO 부속서인 DOC 10020, 위험평가에 대한 세부사항은 9859를 따르도록 하고 있다(국토교통부고시, 2023).

그러나 DOC 10020은 물리적인 전자비행정보장치의 내용만을 다루고 있고, SMM(Safety Management Manual)인 DOC 9859도 마찬가지로 물리적 안전과 보안에 관한 내용만을 기술하고 있다. 사이버보안 운영 및 보안 관리가 취약하며, 국내 항공안전법 및 항공보안법 등에는 전자비행정보장치 운영과 관련한 지침이 미비한 것이 현실이다(Jeon, 2023). 그리고 현재 일관된 기준 없이, 각 항공사의 개별적인 전자비행정보장치 운영 지침을 통해 최소한의 수준으로 운영하고 있어, 안전운항을 위해 적합한 지침이 필요하다.

Ⅲ. 전자비행정보장치 사이버보안 관련 법 및 정책 개선의 필요성

3.1 전자비행정보장치 사이버보안 관련 법률 및 정책 개선의 필요성

국내 항공산업 보호를 목적으로 하는 「항공보안법」, 「항공안전법」 이하 시행령, 시행규칙 및 고시 등에는 전자비행정보장치에 대한 사이버보안 내용이 미비하다. 이 때문에 명확한 사이버 보안・관리 기준 없이 항공사에서는 운항기술 기준에 명시되어 있는 최소한의 내용을 토대로 전자비행정보장치를 사용하고 있으며, 그 내용은 물리적 보안과 물리적 기기 관리만을 기술하고 있어 보안상 문제점이 남아 있다.

「항공보안법」 제1조 목적에 따라 국제민간항공협약 등 국제협약에 따라 항공기 내 불법행위를 방지하고, 민간항공의 보안을 확보하기 위한 기준, 절차 및 의무사항 등을 규정함을 목적으로 한다. 하지만 「항공보안법」 제2조 정의에서 제8호 불법 방해행위 내용은 ICAO에서 말하는 불법방해행위보다 범위가 좁게 명시되어 있어, 사이버 공격으로 인한 항공기 멈춤은 현행법상 불법방행행위로 간주하기 어렵고 「정보통신기반보호법」이 항공 IT 인프라에 적용되더라도 모든 항공사이버보안을 포함하는 데 한계가 있으므로 관련 내용이 항공보안법에 포함되어야 한다.

추가적으로 「항공보안법」 제23조 승객의 협조의무 제5호를 보면, 「항공안전법」 제73조 전자기기의 사용제한을 위반하여 전자기기 사용 행위는 항공기 내에 있는 승객이 항공기와 다른 승객의 안전한 운항과 여행을 위해 하면 안 되는 행위로 되어 있다. 「항공안전법」 제73조는 운항 중인 항공기의 항행 및 통신장비에 대한 전자파 간섭 등의 영향을 방지하기 위해 사용을 제한할 수 있다. 단, 「항공안전법 시행규칙」 제214조 전자기기의 사용제한에 따라 휴대용 음성 녹음기, 보청기, 심장박동기, 전기면도기, 그 밖에 항공기 제작회사의 권고 등에 따라 해당 항공기에 전자파 영향을 주지 아니한다고 인정한 휴대용 전자기기는 사용할 수 있다(항공보안법, 2022; 항공안전법, 2023). 하지만 실제로 기내에서는 비행기모드로 변경을 요청하지만, 관리 감독할 방법이 없어 말로 요청만 하며, 일부 승객들은 계속해서 스마트 폰을 사용하고 있다. 또한, 운항 중 노트북, 태블릿, 스마트 폰을 사용하고 있는 승객들이 어떤 용도로 사용하고 있는지의 규정이 없어 관리 감독할 수 없으며, 보안규정이 따라오지 못하는 상황에서 항공산업은 기내 무선 인터넷 서비스 제공과 같은 승객 편의 서비스는 계속 발전하고 있다. 이는 전자비행정보장치에도 마찬가지이며, 운항 중에도 승객들은 자신의 전자기기로 해킹, 고출력 전자기파 발생 등과 같은 사이버 공격이 가능하며, 전자비행정보장치도 사이버 위협에 노출되어 있다.

항공산업은 항공테러, 탐지, 검색, 경계 등과 같은 물리적 보안규정은 지속적 개정과 제정으로 비교적 체계를 잘 갖추고 있지만, 항공 사이버 위협에 대한 경각심이 낮아 빠르게 발전하고 있는 항공산업과 ICT 기술 융합에 대한 보안을 관련 법이 반영하고 있지 못한 문제점이 있다. 전자비행정보장치도 마찬가지로 사이버 침해행위, 위해행위 등의 규정・관련 법률과 정책이 필요한 시점이다.

3.2 전자비행정보장치 사이버보안 관리 정책 구축의 필요성

「항공안전법」제93조 제1항 및 제2항에 따라 FOM(운항일반교범), MEL, POM(조종사 일반교범), FCOM 등을 제작하여 행정당국에 인가 또는 신고해야 하며, 「항공안전법」 제93조 제7항에 항공기의 운항 또는 정비에 관한 업무를 수행하는 종사자는 운항규정 및 정비규정을 준수하여야 한다는 강행규정을 두고 있으며, 이를 위반하는 경우 법 제43조 제1항 제30호에 의거 처분을 받는다(Kim, 2023). 이에 따라 전자비행정보장치에 해당 정보를 저장하고 있다. 또한, 업데이트된 정보, 필요한 정보 갱신과 애플리케이션 업데이트를 위해 아무 지역에서 혹은 공공장소에서 유・무선 인터넷을 접속하여 무분별하게 PMS에 접속을 허용하고 있어, 의도적으로 시스템을 위・변조하거나 운영 방해, 무단접근, 서비스거부 등의 사이버 위협에 노출되어 있다. 그리고 장비 고장이나 오류 등이 발생할 경우를 대비한 지침이 없다. 그러므로 문제 발생 시 운항이 지연, 결항 될 수 있다.

하지만 국내외 항공보안 지침 및 부속서는 사이버보안을 개괄적으로만 제공하고 있어, 사이버보안 침투시험 및 평가 등과 같은 위협 예방 활동 및 세부지침과 같은 내용은 포함하고 있지 않다. 또한, 전자비행정보장치 장비, 애플리케이션의 기밀성, 무결성, 가용성 등의 소프트웨어 검증 프로세스와 취약점 및 보안 운영 시험, 감항성 평가 등의 세부지침을 제공하지 않고 있다(Jeon, 2023).

세부적인 시스템 접근 및 정보보안 운영・관리・보안 지침의 미비로 인한 예로 그리고 전자비행정보장치 내 보안 애플리케이션 미설치, 정보 업데이트 후, 접속차단 등의 애플리케이션 보안 정책은 이행되고 있지

않으며, 항공사와 운항승무원의 전자비행정보장치에 대한 사이버보안 인식 부족은 사이버 위협요소를 증가시키고 있다. 그러므로 개인과 단체는 전자비행정보장치 관리 정책과 지침을 만들고, 사이버 위협에 대비하기 위한 보안체계와 사이버 위협 발생 시 대응방안에 대한 관리체계를 구축해야 한다. 항공기는 고도의 안전성 확보가 요구되는바, 사이버 위협에 선제 대응을 위해서는 상시 위협을 감시하고, 사이버 침해행위, 위해행위에 실시간 대응이 가능한 관리체계를 구축하여 항공 부분의 안전성을 확보해야 한다.

국내뿐만 아니라 전 세계적으로 항공 사이버보안 관리 정책과 지침은 부족하지만, FAA에서는 최소한의 지침으로 운항승무원에 대한 전자비행정보장치 관리 정책으로 조종실 내 타 시스템과 전자비행정보장치가 제공한 정보가 일치하지 않을 때 정보의 우선순위와 운항승무원 상호 간 전자비행정보장치 응용프로그램의 업데이트 번호 및 날짜 등의 정보를 확인하는 절차를 수행하도록 하고 있다. 또한, 운항승무원에게 보안의식 확립을 위해 전자비행정보장치 하드웨어 작동 및 제어와 소프트웨어 사용 및 오류에 대한 설명, 보안 관련 절차, 시스템의 비행 전 점검, 승무원 자원 관리(CRM) 등의 교육을 진행한다. 또한, 항공사 자체적으로 운영자가 전자비행정보장치 운영하는 데 보안 수준을 유지하기 위한 프로세스와 절차를 마련하고, 전자비행정보장치와 해당 프로그램의 보안이 적절하게 유지되기 위한 절차도 수립하도록 하고 있다(FAA, 2017).

EASA에서도 마찬가지로 운항승무원에게 하여금 전자비행정보장치가 제공하는 정보가 상이할 경우, 취해야 할 조치에 대한 절차, 전자비행정보장치 응용프로그램의 개정 번호 및 날짜 등 업데이트 정보를 확인 절차를 제시한다. 또한, 전자비행정보장치 운용 전 운항승무원에게 운용 관련 절차 교육을 진행하며, 운항승무원에게 전자비행정보장치 시스템 구조, 시스템의 비행 전 점검절차, 시스템 제한사항, 소프트웨어 사용 및 사용불가능 및 오류발생 시 조치방법 및 절차, 승무원 자원관리(CRM) 및 인적 요인 등을 교육한다. 항공사 자체적으로는 비행 전 전자비행정보장치 운영 소프트웨어가 정상적으로 작동하고 데이터가 완전하고 정확하다고 보장될 수 있도록 전자비행정보장치 시스템 보안절차를 수립하고 관찰하며, 전자비행정보장치 시스템의 정기적인 유지보수와 전자비행정보장치 시스템의 무결성을 보장하기 위해 고장 처리 방법에 대한 절차도 수립해야 한다(EASA, 2019). 이처럼 FAA와 EASA는 전자비행정보장치 관리를 위한 최소한의 정책을 수립·발전시키고 있다.

ICAO에서도 시스템 및 데이터의 기밀성, 무결성 및 가용성을 적절하게 보호하고, 공급망 보안, 네트워크 분리, 원격접근 기능 보호 및 제한하는 내용을 포함하여 위험 평가를 각 국가기관에서 수행하도록 권고하고 있으며, ICAO에서 제공하고 있는 부속서에는 사이버보안의 개괄적 지침을 제공하고 있지만, 사이버보안 침투시험 및 평가 등과 같은 위협 대응방법, 예방 활동, 보호 조치 등의 세부지침은 포함하고 있지 않으며, 사이버 위협에 대한 기밀성, 무결성, 가용성 등의 소프트웨어 검증 프로세스와 취약점 및 보안 운영 시험, 그리고 감항성 평가시험 등의 세부지침을 제공하고 있지 않은 한계를 갖고 있다. 그러므로 ICAO에서도 언급한 ISMS를 구축하여 전자비행정보장치를 포함한 정보보안 및 관리정책 마련이 필요하다(Jeon, 2023; ICAO, 2022).

Ⅳ. 개선방안

4.1 전자비행정보장치 보안·관리를 위한 관련 법률 개정

현재 전자비행정보장치에 관련하여 「항공보안법」에 어떠한 법률적 내용이 없고, 「고정익을 위한 운항기술기준」에 개괄적인 내용과 ICAO 기준에 따른다고만 나와 있다. 또한, 현행법에 명시되어 있는 불법방해행위에는 사이버보안으로 인한 방해행위는 포함되어 있지 않다. 따라서 「항공보안법」제2조 정의의 불법방해행위에 ICAO의 Unlawful interference 중 하나인 'Unlawful seizure of aircraft'을 추가하거나 정의 항목에 '항공전자장비'라고 하여 장비 항목 중 하나로 전자비행정보장치를 「전기통신 기본법」 제2조 2호 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제로 간주하여 포함시키고, '항공 전자적 침해'의 내용으로 해킹·컴퓨터바이러스·논리 폭탄·메일 폭탄·서비스 방해 등으로 항공기·공항시설 및 시스템 등의 정보통신망에 불법 침입·교란·마비·파괴하거나 정보를 절취·훼손하는 공격행위 등의 내용을 포함하는 것이다. 이와 더불어 제3장 공항·항공기 등의 보안에 '항공 정보통신체제 및 장비 보안'이라고 법률을 추가하는 등의 개정이 요구된다. 항공 사이버보안 내용일 추가하여 법

적 보호 수단을 마련해야 한다. 이러한 법률 개정을 통해 법적 보호 수단을 마련해야 한다.

운항기술기준에 기술되어 있는 전자비행정보장치의 내용도 ICAO의 부속서 모든 내용을 다루고 있지 않기 때문에 FAA와 EASA와 같이 최소한의 보안 및 관리체계가 필요하다. 필요시 국외의 체계를 따르되 ICAO에서도 언급하고 있듯이, 국가는 구가 차원에서 사이버보안 관리 프로세스의 효율성, 품질 및 일관성을 지속발전하기 위해 국내 실정에 맞게 있어야 한다(ICAO, 2022). 또한, 현행 운항기술 기준 나항 전자비행정보장치(EFB)의 기능에 항공기운영자에게 세부항목 없이 기능과 관련 위험 평가, 기능과 장비사용을 위한 절차 및 훈련기준을 수립과 문서화, 고장 시 운항승무원이 안전운항을 위한 충분한 정보를 즉시 이용할 수 있지 여부를 수행하라고 나와 있어 현재 각 항공사는 전자비행정보장치를 비용적인 문제 혹은 각자의 제반 사항에 의하여 관리 수행 여부가 각기 다르며 명확하지 않은 실정이다. 따라서 세부적인 내용의 예로 전자비행정보장치 관리, 필수 설치 애플리케이션 및 보안 애플리케이션 설치, 데이터 접속 지정, 장비 교체 주기와 관리부서의 설치 등에 관한 내용이 필요하다.

4.2 전자비행정보장치 보안 관리체계 수립 및 시행

전자비행정보장치는 현재 개인이 소지하여 클라우드나 메인 서버에 공중 무선 인터넷 접속이나 데이터 통신으로 VPN(Virtual Private Network)과 같은 별도의 보안장치 또는 애플리케이션 없이, 정보를 내려받고 있다. 또한, 하나의 전자비행정보장치를 소지하므로 분실, 고장 또는 문제 발생 시 예비 장비 등 대책 방안이 명확히 없어 가용성이 저하된다. 따라서, 전자비행정보장치 가용성 및 운용 신뢰성 확보를 위해 정보 및 데이터 기반의 항공보안 운영 및 관리체계가 수립・이행되어야 한다.

법률 개정을 통한 전자비행정보장치와 관련된 사이버보안을 바탕으로 국제 기준과 국내 실태에 맞게 사이버보안 관리 및 운영 정책 기준을 적시하고, 세부적인 전자비행정보장치 보안을 위한 관리 및 운영체계의 수립이 필요하다. 이를 위해 ICAO에서도 언급한 국제표준화기구(ISO)의 정보보안관리체계(ISMS)를 구축하는 것이다. ISMS를 토대로 전자비행정보장치 사이버보안체계를 만들어 관리・감독하고, 잠재적 사이버 위협을 대응하고 개선하는 것이다.

ISO/IEC-27000 시리즈는 정보보안 관리를 위한 일련의 국제적으로 공인된 표준 및 지침을 제공하므로, 이러한 표준은 위험 관리, 통제, 정책, 절차를 포함한 다양한 측면에서 이점이 된다. ISMS를 접목하면 전자비행정보장치의 특정 요구사항에 맞게 확립된 체계를 만들 수 있다. 각 항공사는 보안 팀에 전자비행정보장치를 관리할 수 있는 인원을 확보하고, 보안 관리체계를 구축하여 전자비행정보장치에 대한 모니터링을 하게 될 것이고, 정기적으로 보안 검사를 시행하여 시스템, 네트워크 및 애플리케이션에 대해 취약점 및 문제점을 보완하며 관리체계를 개선해 나아간다. 위험 관리와 위험 평가를 통해 전자비행정보장치의 잠재적인 취약성과 위협을 식별하고, 이를 완화하기 위한 적절한 제어를 구현할 수 있다. 그리고 ISO/IEC-27000 시리즈에서 제공하는 사이버보안 모범사례와 통합시켜 전반적인 보안 태세를 개선해 나가며, 전자비행정보장치 보안 상태를 정기적인 평가, 검토 및 업데이트를 통해 지속적인 개선으로 더욱 효과적이고 최신으로 사이버보안을 유지해 가는 것이다.

추가로 전자비행정보장치에 보안 기능을 설치 및 운영하며, 클라우드나 메인 서버에 접속 시 전자비행정보장치를 지정된 지점에서만 할 수 있게 하고, 지정된 장소 이 외에서는 항공기에 탑승한 후부터는 외부 통신과 차단되도록 해야 한다. 지정된 장소에서만 네트워크에 접속하게 하는 만큼 보안 팀에서는 침입 탐지 및 예방 시스템인 IDPS(Intrusion and Prevention System)을 구축하여 네트워크 통신량을 감시하고, 필요할 때 접속을 차단하는 등의 방법으로 실시간 위협 탐지 및 예방을 해야 한다. 기내 탑승 전후, 전자비행정보장치 반・출입을 관리하고, 상시 최신 업데이트된 전자비행정보장치 사용을 통해 최신성을 유지하고, 전자비행정보장치 보안 운영 및 관리를 강화해야 한다. 이를 통해 운항 지연을 방지하고, 외부 사이버 위협으로부터 보안성을 강화할 수 있는 대안이 된다.

그리고 개인적인 보안방법으로 운항승무원은 전자비행정보장치 사용 시 주기적으로 보안을 위해 비밀번호를 변경하고, 기타 장비에 설치된 보안방식인 지문인식, 얼굴 인식 등의 보안방법을 적극적으로 사용하도록 하여 추가적인 장치 인증을 강화해야 한다. 사이버보안은 개인의 역량으로만 가능한 것이 아니므로 전자비행정보장치와 관련된 모든 사람이 적극적으로 참여해야 한다. 특히 당사자인 운항승무원에게 전자비행정보장치 보안 관리 및 사이버 위협에 대한 보안 인식 교육을

통해 성숙한 보안 인식을 고취할 수 있다. 또한, 기타 사이버보안 모범사례를 교육하고, 상호 개선해 나갈 수 있게 문제점 및 개선사항이 있으면 작성하여 제출할 수 있도록 보안 문화를 구축시켜 나아간다.

국제표준인 ISO/IEC-27000 시리즈 체계로 관리하므로 국내뿐만 아니라, 국외의 다양한 이해 관계자들의 의사소통이 원활하고 같은 체계로 운영하므로 혼동이 없으므로 사이버보안이 빠르게 발전할 수 있다. 더 나아가 ISO/IEC-27000 시리즈를 준수한다는 의미는 국제적으로 사이버보안과 관련된 요구사항 및 표준을 준수하고 있다는 증표가 되고, 국내 전자비행정보장치 시스템에 대한 신뢰와 국내 항공산업 신뢰를 높이는 데 이바지한다.

V. 결 론

과학 및 통신 기술의 발전에 힘입어 항공산업은 비약적으로 발전되었다. 하지만 그만큼 사이버 위협도 커지고 있다. 사이버 위협은 항공기의 운항을 보호해야 하는 안전영역을 위협하는 또 다른 잠재적 요인으로, 승인되지 않은 정보통신 간섭 및 방해로 항공기의 각종 컴퓨터를 해킹 및 오류 등으로 오작동, 오정보 제공으로 항공 운항의 정시성, 안전성, 쾌적성을 감소시킨다. 이러한 불법방해행위는 ICAO에서 말하는 'Unlawful seizure of aircraft'에 해당하게 된다(ICAO, 2022).

오늘날까지 항공기의 안전한 운항을 위해 탐지, 검색, 경계, 등과 같은 물리적 보안체계를 유지 및 지속 발전시켰으며, 이 밖에 항공테러 및 불법행위 등으로부터 성숙한 대응과 관리가 자리잡혀 있고 활발히 업데이트되고 있다. 그러나 정보통신 기술의 발전과 융합으로 새로운 위협으로 드러나고 있다. 정보통신 기술의 빠른 발전에 따른 체계적인 항공보안에 관한 법률, 정책 그리고 관리 지침 및 체계의 발전이 필요한 시점이다. 진보하고 있는 기술 그리고 새롭지 못한 항공보안 정책으로는 잠재적 위협으로부터 항공기 운항의 안전을 확보할 수 없다.

그러므로 본 논문에서 언급한 내용과 같이 전자비행정보장치 보안을 위해 관련 법률을 개정하고 각 법률이 뒷받침되고 있는 환경 속에서 ICAO에서도 사이버보안 관리로 권장하고 있는 ISO/IEC-27000 시리즈를 토대로 정책과 관리 지침을 확립시켜 사용자가 체계적으로 관리할 수 있도록 해야 한다. 이를 통해 전자비행정보장치 사용에 안정성과 보안성이 강화되어 사이버 위협에도 효율적으로 대응이 가능해질 것이다.

따라서 본 연구에서 제안하고 있는 전자비행정보장치 사용 확대에 따른 잠재적 사이버 위협으로부터 사이버보안에 관한 법률 및 보안 정책과 체계를 구축하여, 사이버 위협으로부터 대비하고 안전성을 확보하면 항공 안전에 이바지될 것으로 생각한다.

References

1. SK Shieldus, "Occurrence Statistics By Type of Infrigement Accident", Korea Fiscal Information Service, 2022.
2. ICAO, " Annex 17 to the Convention on International Civil Aviation", Aviation Security, Twelfth Edition — July 2022.
3. Jung, W. H. "Study on aviation cybersecurity in public law," M.S. Thesis, Chung-Ang University, Seoul, August 2020.8.
4. Park, S., and Kim, I. J., "Comparative study on legal system on cybersecurity stages on south korea and the unitesd states", Journal of Convergence Security, 44, 2012, pp.33-40.
5. Jeon, S., "A study on proactive responses to in-flight cyber threats - centered on comprehensive information security management system improvements-", Aviation Management Society of Korea, 21(5), 2023, pp. 66-78.
6. Cybersecurity Action Plan, ICAO, Second edition January 2022.
7. Kim, S. M., Ahn, H. B., Yeo, U. J., Hwang, and H. W., "A study on the judicial judgment of flight regulations under the aviation safety act", Journal of the Korean Society for Aviation and Aeronautics, 31(3), 2023, pp. 161-171.
8. International Standard, ISO/IEC 27001, "Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements", Third edition 2022-10.

9. International Standard, ISO/IEC 27002, Information Technology — Security Techniques — Code of Practice for Information Security Controls, Second edition 2013-10-01.
10. International Standard, ISO/IEC 27005, Information Security, CyberseCuRitYand Privacy Protection — Guidance Onmanaging Information Security Risks, Fourth edition 2022-10.
11. 49 USC 40101 Note, Aviatiob and Transportation Security Act, Public Law 107-71 107th Congress, 19/11/01.
12. AC 20-173, Installation of Electronic Flight Bag, 09/27/11.
13. AC 91-78, Use of Class 1 or Class 2 Electronic Flight Bag (EFB), 07/20/07.
14. AC 120-76B, Guidelines for the Certification, Airworthiness, and Operational Use of Electronic Flight Bags, 6/1/12.
15. AC 120-76D, Authorization for Use of Electronic Flight Bags, 10/27/17.
16. AC 119-1, Operational Authorization of Aircraft Network Security Program (ANSP), 9/30/15.
17. Flight Safety Regulations For Aeroplanes, 2022-572, 2022.10.5., Ministry of Land, Infrastructure and Transport.
18. Aviation Security Act, No 18354, 2022.1.28, Korea Ministry of Government Legislation.
19. Aviation Safety Act, No 18870, 2023.1.19, Korea Ministry of Government Legislation.
20. Information and Communication-Based Protection Act, No 18870, 2022.9.11, Korea Ministry of Government Legislation.
21. Promotion of Information and Communication Network Utilization and Information Protection Act, No 19154, 202.7.4, Korea Ministry of Government Legislation.
22. KIAST, “Study on the Improvement of the System in the Flight Standards”, Ministry of Land, Infrastructure and Transport, 2020.