Original Article

https://doi.org/10.12985/ksaa.2025.33.1.031
ISSN 1225-9705(print) ISSN 2466-1791(online)

# 항공분야 AI 기술 동향과 법적 대응 연구

김민정*

# Research on AI Technology Trends in the Aviation Sector and Legal Responses

Minjung Kim*

## ABSTRACT

Artificial intelligence (AI) is rapidly advancing in the aviation industry, enhancing efficiency, improving safety, and optimizing operational decision-making. However, its integration also raises new legal and cybersecurity challenges. This study analyzes the latest trends in AI applications within aviation, including air traffic control, aircraft operations, and airport management. It also examines international regulatory frameworks, such as the EU AI Act, EASA AI Roadmap 2.0, and ICAO cybersecurity guidelines, to assess legal responses. Additionally, it evaluates Korea's legislative developments and the need for regulatory adaptation to mitigate AI-related risks. Based on a comparative analysis of global AI regulations and aviation cybersecurity policies, this study provides policy recommendations to strengthen legal frameworks and enhance aviation security against AI-driven threats.

**Key Words** : AI Trustworthy(AI 신뢰성), Artificial Intelligence(인공지능), Aviation Security Law (항공보안법), EASA AI Roadmap(EASA AI 로드맵), ICAO Cyber-Security(항공 사이버 보안), ICAO TLP Protocol(항공 정보 데이터 분류 프로토콜)

## Ⅰ. 서 론

### 1.1 연구의 배경

유럽항공안전청(EASA)에서는 2030년을 시작으로 인공지능 기술이 적용된 항공기 개발과 항공관제 시스템의 변화, 지상에서 실시간으로 수신되는 항공기 정보를 활용한 안전 운항 체계를 구축하기 위해 2018년도부터 AI 기술 로드맵을 설계하여 사이버 보안에 관해 미국 연방항공청(FAA)와 공통으로 연구하고 있다.

유럽의회(EC)는 2023년 인공지능 기술에 관한 법안을 통과하면서 인공지능 기술을 적용하기 위한 규정과 윤리적 보안, 데이터 신뢰성 등의 기준을 제시할 수 있는 초석을 마련하였다.

IT 기술의 발전과 통신망과 네트워크 속도가 증가하고 기내에서 무선 인터넷 사용도 가능해진 세상에서 항공기의 시스템 안전성을 보호하고, 인공지능 기술을 활용한 항공기 관리 방안이 새롭게 제시되면서, 민간 항공산업의 사이버 보안 기술의 중요성도 강조되고 있다.

국제적으로 항공산업을 위한 사이버 보안에 관한 연구는 어떤 과정에 있고, EASA를 중심으로 한 AI 시스템을 도입한 항공기 설계 및 운영 방법을 연구하였으며, 이에 따른 사이버 위협을 예방할 수 있는 법률적 근거를

Received: 25. Feb. 2025, Revised: 03. Mar. 2025,
Accepted: 07. Mar. 2025
* 극동대학교 항공정비학과 교수
** 한국항공대학교 항공우주법 박사과정
연락저자 E-mail : beatriz121736@kdu.ac.kr
연락저자 주소 : 충북 음성군 감곡면 대학길 76-32, 연구실 A305-2호

ICAO의 지침과 국내외 입법 동향을 통해 살펴보았다.

또한, 국내 항공 사이버 보안 이행 지침을 마련하는 과정에서 AI 기술 관련 사항을 반영하기 위한 법률 개정 방안을 연구하였다.

### 1.2 연구의 목적

정보 기술의 발전으로 항공기 운항에 통신 시스템, 무선을 이용한 데이터 송수신 등 지상에서 실시간으로 항공기의 위치, 정보 등을 파악할 수 있다. 항공기를 이용한 테러가 증가하는데 원격 조정도 가능하고 사이버 시스템을 공격하여 통신망을 마비시키거나, 관제 레이더망 공격, 신호 교란 등의 사이버 보안 위협이 증가하고 있다.

항공기는 첨단 IT 기술을 접목하여 지상에서 원거리로 실시간 항공기 위치 정보를 전송하고, 기내에서 WiFi를 이용하여 승객 간 음성, 메시지 등의 데이터 송수신도 가능한 세상이며, 앞으로는 승객의 편의를 위한 인터넷 활용 서비스 품목이나 항공기 제어를 위한 최신 소프트웨어 등의 적용으로 항공기 안에서 활용되는 사이버 기술이 더욱 확대될 전망이다.

대표적인 기술이 적용된 분야는 공항 운영, 항공관제, 항공기 운항에 인공지능(artificial intelligence) 기술을 활용하여 인적 요소로 인한 오류를 감소하고, 신뢰도가 높은 시스템을 활용하여 항공기 안전 운항을 도모하기 위한 움직임이 EASA의 주도로 일어나고 있다.

유럽연합(EU)은 2021년도 인공지능 기술에 대한 법안을 발의하였고, 2024년 11월에 AI 기술을 4단계로 구분하여 규제하는 법안을 시행할 예정이다. 이러한 내용을 항공 분야에도 함께 적용하여 2019년부터 EASA에서는 AI 시스템을 적용한 로드맵을 공포하였고, FAA와 함께 AI 기술을 활용한 항공산업을 발전시키기 위해 관련 정책과 법안을 개발하고 있다.

최신 기술이 도입된 항공 운송 분야는 시스템의 안정적 운영을 위해 사이버 보안의 위협에도 함께 대응하기 위한 정책이 요구되고 있는데, ICAO에서는 2022년 Cyber Act를 발행하여 감항 당국이 이를 반영한 보안 정책을 수립하고 있다. 앞으로는 항공기간, 공항과 항공기, 공항과 공항 등의 상호의 데이터 정보 교환이 필수적일 것이며, 이러한 데이터를 보호하기 위한 보안프로그램의 운영도 필요성도 커질 것이다.

본 연구에서는 항공 분야의 AI 기술을 적용하기 위한 EASA AI Roadmap 2.0을 소개한다. 국내의 AI 관련 입법 동향과 ICAO Annex 17에서 사이버 보안에 관한 내용을 중심으로 항공 안전과 보안을 강화하기 위한 국제적인 노력의 현안을 연구하였다.

AI 기술 로드맵과 발전 현황을 살펴보면서 국내에도 항공기 안전 운항에 적용되는 AI 기술을 활용할 수 있는 정책이 마련되고 규정이 제정되는 데 도움이 되고자 연구를 진행하였다.

## Ⅱ. 본 론

### 2.1 인공지능(AI)의 정의

인공지능 기술의 아버지라 불리는 마빈 민스키는 인간의 사고체계를 형식화하는 방법을 고민하던 중 인간의 생각이 진행되는 과정과 추상화하여 어떠한 개념을 만들어내는 과정에서 외부 세계의 정보를 뇌의 한 부분에서 받아들이고 정보를 습득하면서 다른 부분으로 정보를 전달하는 '생각의 순방향'을 기반으로, 방향성을 통해 추상적 개념을 만들어가는 순방향 신경망을 통해 개념을 구체화한다고 하였다(Lee, 2023).

인공지능 기술은 이러한 정보의 추상적 개념을 연결하는 인공 신경망을 통해 인간의 사고 과정을 형식화한다고 정의하였다(Park and Kim, 2017).

국내에서 시행 예정인 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」[1] 제2조에서는 인공지능(artificial intelligence, AI)이란 학습, 추론, 지각, 판단, 언어의 이해 등 인간이 가진 지적 능력을 전자적 방법으로 구현한 것을 말하며, 인공지능을 구현하는 데 필요한 하드웨어·소프트웨어 기술 또는 그 활용 기술을 인공지능기술로 정의한다.

초기의 AI 시스템은 엔지니어가 설계한 규칙과 논리에 의존하였고, 복잡하고 유동적인 현실 세계의 문제를 다루는데 한계가 있었다. 이런 문제를 극복하고자 AI가 데이터로부터 스스로 학습하고 규칙을 도출하는 머신러닝(machine learning) 기술이 개발되었다. 머신 러닝은 인공지능의 핵심 동력이며, 인간 두뇌의 신경망을 모방한 심층 신경망을 활용하는 딥러닝의 등장으로 자율주행 분야에서 큰 주목을 받고 있다(NIA, 2024).

머신 러닝의 속도가 빠르면 이미지 인식, 음성 인식, 번역 등의 분야에서 활용할 수 있고, 데이터베이스의 규모가 커지면 연결되는 정보의 폭이 확장됨에 따라

1) 2026.01.22. 시행 예정.

Table 1. Status proposed AI bill of the 21st national assembly

| 법률명<br>(대표발의 의원, 발의일) | 주요 내용 |
|---|---|
| 인공지능 책임 및 규제법안<br>(안철수 의원 대표 발의, 2023.8.8.) | '금지된 인공지능', '고위험 인공지능', '저위험 인공지능' 의 세 가지 유형으로 구분하여 정의하였으며, 각각 유형에 대한 의무사항을 차등화하여 규정함 |
| 인공지능책임법안<br>(황희 의원 대표 발의, 2023.2.28.) | 고위험 인공지능에 관한 기본계획 수립, 인공지능 분야에 전문성을 갖춘 위원회 설치 및 운영, 인공지능분쟁위원회 운영 |
| 인공지능산업 육성 및 신뢰 확보에 관한 법률안<br>(윤두현 의원 대표 발의, 2022.12.7.) | 인공지능에 관련된 산업 진흥에 필요한 조치 규정과 사업자가 신뢰성 확보를 위한 노력을 하도록 의무를 부과 |
| 알고리즘 및 인공지능에 관한 법률안<br>(윤영찬 의원 대표 발의, 2021.11.24.) | 알고리즘 및 인공지능의 부작용을 최소화 하면서 관련 산업 육성에 필요한 내용을 규정함 (고위험 인공지능을 포함한 기술, 서비스에 대한 설명요구권, 이의제기권, 거부권, 손해배상 청구권 등) |
| 인공지능에 관한 법률안<br>(이용빈 의원 대표 발의, 2021.7.19.) | 인공지능 산업의 진흥과 경쟁력 강화를 위한 정부 및 지방자치단체의 필요 조치에 대한 규정 |
| 인공지능 육성 및 신뢰기반 조성등에 관한 법률안<br>(정필모 의원 대표 발의, 2021.7.1.) | 인공지능 관련 윤리기준, 기술표준 등을 마련하고, 특수활용 인공지능 개발, 제조, 유통 시 신고하도록 함<br>(특수활용에 대한 정의와 규정은 없음) |
| 인공지능 기술 기본 법안<br>(민형배 의원 대표 발의, 2020.10.29.) | 인공지능 산업 진흥 및 육성을 위한 지원에 관한 내용 규정 |
| 인공지능산업 육성에 관한 법률안<br>(양향자 의원 대표 발의, 2020.10.29.) | 인공지능 산업의 진흥 및 육성에 필요한 내용 규정 |
| 인공지능 연구개발 및 산업 진흥, 윤리적 책임 등에 관한 법률안<br>(이상민 의원 대표 발의, 2020.7.13.) | 인공지능 산업의 진흥 및 육성에 관한 내용 규정<br>(윤리적 책임은 국가, 지방자치단체, 사업자 등에게서 산업의 이용자 보호를 위한 윤리원칙을 정하는 책무 규정만 두고 있음) |

새로운 인공지능 기술이 발전될 수 있는 상황이다.

인공지능기술은 복잡한 수식을 빠르게 처리하는 분야에 효율적이지만, 인간의 감각기관 작용, 운동, 의사소통 등을 수행하는 데는 아직 한계가 있다.

AI 기술이 지닌 가장 부정적인 영향은 허위 정보가 대규모로 확산하여 사회의 혼란을 제공할 수 있다는 점이다. AI가 생성한 허위 이미지와 허위 뉴스가 경제지수에도 영향을 줄 수 있고, 인터넷에서 제공되는 정보의 신뢰도도 하락할 수 있어 AI 기술에 대한 규제의 필요성이 제기되고 있다.

## 2.2 AI 기술 관련 입법 동향

### 2.2.1 국내

정부의 인공지능 정책에 관한 동향을 살펴보면 2019년 인공지능 강국을 비전으로 '인공지능 국가전략'을 수립하였고, 글로벌 동향을 고려하여 인공지능 산업 진흥과 활용 기반을 강화하고 역기능을 방지하기 위한 「인공지능 법·제도·규제 정비 로드맵」을 마련하였다(MIST, 2020).

사람 중심의 인공지능 시대 실현을 위해 데이터 경제 활성화 기반을 조성하고, 알고리즘의 투명성과 공정성을 확보하는 과제를 추진하는 내용을 담았다.

각종 법안을 적용하기 위해 먼저 정의되어야 할 인공지능의 법인격 부여를 검토하고, 인공지능 기술의 책임 체계와 윤리 기준을 마련하는 것을 목표로 한다. MOLEG(2024)의 인공지능 기술과 관련하여 발의된 법령은 Table 1과 같이 2024년 6월 기준으로 50개인데, 실질적으로 인공지능의 정의를 규율하고 있는 법령은 23개이다.[2)]

이후 정부 부처 간의 합동으로 「새로운 디지털 질서 정립 추진계획」을 발표하였다. 「디지털 권리장전」의 철학과 자유, 공정, 안전, 혁신, 연대 등의 5대 원칙을 토대로 국민의 관심사가 높거나, 시급성이 큰 정책과제 8개를 핵심과제로 선정하여 집중적으로 관리한다.

2) 각 부처의 조직과 직무 범위에 관하여 규정하고 있는 직제 성격의 규정을 제외한 숫자이다.

AI 혁신과 안전·신뢰(이용자 보호 등)의 균형을 위한 법제 제정을 연내 마무리하여 AI 규범 체계를 선도적으로 정립하고, AI 안전성을 검증·연구하는 전담 조직도 설치하여 아태지역의 AI 안전 허브로 육성할 예정이다.

AI 관련 법안은 21대 국회에서 논의가 시작되어 회기 만료로 폐기되었다가 22대 국회에서도 관련 법안들이 제시되어 AI 기본법이 마련되었다.[3)]

AI G3 도약을 위한 국가역량 결집을 위해 대통령이 직접 주재하고, 민간 최고 전문가들이 참여하는 『국가인공지능위원회』를 구성하였고 2024년도 9월에 위원회가 출범하였다.

국가인공지능위원회는 인공지능 산업을 진흥하고 신뢰할 수 있는 인공지능 이용환경을 조성함으로써 국가 경쟁력 강화, 국익 보호 및 국민의 삶의 질 향상을 목표로 인공지능 관련 주요 정책, 인공지능 분야의 연구개발 전략 수립, 인공지능 관련 투자 전략 수립과 인공지능 분야의 경쟁력 강화를 위한 민·관 협력 및 산업 발전에 관한 사항을 제정할 계획이다.

### 2.2.2 유럽연합(EU)의 AI Act

유럽 연합(EU)은 2024년 5월 21일 세계 최초로 인공지능을 포괄적으로 규제하는 법률을 최종적으로 확정하였는데, 이는 2021년 EU 집행위원회가 최초로 법안을 제안한 이후 3년 만이다.

EU 인공지능법은 AI 시스템 개발, 시장 출시, 서비스 개시 및 사용을 위한 통일된 법적 체계를 마련하여 인간 중심적으로 신뢰할 수 있는 인공지능(AI)의 활용을 촉진하는 동시에 EU 내 AI 시스템의 해로운 영향으로부터 기본권을 높은 수준으로 보고하고, 혁신을 지원하기 위해 제정되었다(EU, 2024).

AI 시스템의 핵심 특징은 추론 능력으로 정의하였다. 이 추론 능력은 물리적 및 가상 환경에 영향을 미칠 수 있는 예측, 콘텐츠, 추천 또는 결정과 같은 출력을 얻는 과정과 입력이나 데이터로부터 모델이나 알고리즘을 도출하는 AI 시스템의 기능이며, 데이터로부터 학습하는 머신 러닝 접근법, 추론과 논리 기반 접근법을 포함하며, 기계 기반(machine-based) 즉, AI 시스템은 기계에서 작동하는 사실임을 규정하였다(EU, 2024).

AI가 신뢰할 수 있고 윤리적으로 건전하다는 것을 보장하기 위해 7가지 구속력 없는 AI 윤리 원칙을 개발하였다. 인간의 대리 또는 감독, 기술적 견고성 및 안전성, 프라이버시 및 데이터 거버넌스, 투명성, 다양성, 차별 금지 및 공정성, 사회 및 환경적 복지 및 책임이 포함된다(EU, 2024).

인공지능 기술을 활용하여 여러 가지 편익도 얻을 수 있지만 기술이 오남용될 수 있으므로, 금지되는 인공지능 관행(prohibited AI practices)을 명시하고 있다. 각 영역에서 인간의 존엄성, 자유와 평등, 민주주의, 법규, 차별 금지, 아동 권리 등 기본권에 중대한 침해가 우려되는 AI 시스템에 대해 출시·이용 자체를 금지하면서, 피해자나 실종자 수색, 자연인에 대한 예측 가능한 테러 공격의 위험 감지, 형벌 집행을 목적으로 사람의 소재 파악을 하는 등의 일부 영역에서는 제한적으로 예외를 인정하고 있다(EU, 2024).

제5조에 따른 AI 관행의 금지 미준수에 대해 최대 35,000,000유로 이하의 과태료를 부과하며, 위반자가 사업체면 전 세계 연간 매출액의 최대 7% 중 높은 금액의 과태료를 부과한다. 제5조에서 규정되지 않은 사항을 AI 시스템이 준수하지 않으면 최대 15,000,000유로 또는 위반자가 사업체면 연간 매출액의 3% 중 더 높은 금액을 과태료로 부과하는 벌칙을 제정하였다(EU, 2024).

### 2.2.3 미국의 국가인공지능 이니셔티브법

미국 정부는 2020년도에 국가 인공지능 이니셔티브법(National Artificial Intelligence Initiative Act, 2020)을 제정하여 2021년 1월부터 시행하였고, 미국 상무부(DOC)는 인공지능(AI)과 관련된 다양한 문제에 대해 자문 등을 실시하기 위해 '국가인공지능자문위원회(National Artificial Intelligence Advisory ComMittee, NAIAC)'를 발족하였다.[4)]

NAIAC의 발족을 통해 AI 기술의 개발부터 사용에 이르기까지 모든 범위의 문제에 대한 통찰력을 제공하고자 학계, 산업계, 비영리 단체, 시민 사회 및 연방 연구소 등 광범위한 AI 관련 분야의 전문가로 구성하여 AI 관련 과학기술 연구, 개발, 윤리, 표준, 교육, 공정

3) 정보통신방송법안심사소위원회는 안철수 의원이 대표 발의한 「인공지능 산업 육성 및 신뢰 확보에 관한 법률안」 등 19개 법률안을 병합하여 심사한 결과, 이를 통합 조정하여 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법(이하 'AI 기본법')을 EU에 이어 세계에서 두 번째로 AI 기본법을 제정하였다.

4) 법 시행 이후 2021년 9월 8일에 국가인공지능자문위원회를 출범하였다.

성, 기술이전, 상업적 활용, 보안, 경제 경쟁력 등에 대한 자문과 정보를 제공한다. 국가 AI 이니셔티브의 목적은 다음과 같다.

첫째, 미국의 지속적인 AI 연구 개발 주도권 확보
둘째, 공공 및 민간 부문에서의 신뢰할 수 있는 AI 개발 및 활용
셋째, 경제 및 사회 전 분야에 걸친 AI 시스템 통합을 위한 현재 및 미래의 인력 양성
넷째, 민간 기관, 국방부 및 관련 단체 간의 진행 중인 AI 연구 및 개발, 시연 등의 활동을 조정하고 공유

2020년도 이후 미국 연방정부에서 AI 훈련법(Artificial Intelligence Training for the Acquisition Workforce Act) 내지 2023년 국방수권법(National Defense Authorization Act for Fiscal Year, 2023) 등이 입법된 바 있으며, 그 외에도 연방의회 차원에서는 「알고리즘 책임법(안)」, 「미국 데이터 개인정보 보호법(안)」이 각 제안되기도 하였다.

이 같은 AI 정책은 대체로 AI 규제에 대한 방향성을 제시하는 동시에, AI의 편향(bias) 때문에 발생할 수 있는 잠재적인 차별 위협 등을 완화하고, 공공영역에서도 AI를 도입하는 등 AI 이용의 규제와 진흥 정책을 모두 포함하고 있음을 알 수 있다(Yoon and Yang LLC, 2023).

## 2.3 EASA AI Roadmap 2.0

### 2.3.1 개요

항공산업의 기술적인 변화는 제트 엔진 도입과 Fly-By-Wire 시스템의 도입을 통해 발전해 왔다. 2020년대에는 가장 영향력이 큰 새로운 기술이 도입될 것이며, 인공지능 기술을 이용한 항공산업은 자율비행과 예방 정비, 항공기 관제 운용의 최적화를 가능하게 할 것으로 예측한다. 그러나, AI 기술의 도입으로 항공산업에는 새로운 도전과 과제를 맞이하게 되었다. 유럽항공안전청(EASA)에서는 안전, 보안, 환경 보호 부분에서 높은 수준의 AI 기술의 이점을 산업현장에 적용하고자 한다. 첫 번째로 고려했던 AI의 개념은 AI 시스템과 안전에 관한 내용이었고, 두 번째로는 최종 사용자인 조종사, 관제, 공항 운영자 등이었다.[5)]

EASA의 AI 로드맵 2.0에서는 항공 분야에서 AI 기술에 관한 내용을 업데이트하여 항공 운송 분야의 이해관계자들과 활발한 논의를 할 수 있는 기초 자료로 활용하고자 한다.

지금까지 진행된 진보된 기술 중 AI 기술은 가장 파괴적일 것으로 예상하는데, EASA에서는 다음의 질문사항에 답을 구하기 위한 선도적 역할을 진행하고 있다.

첫째, AI 기반 시스템에 대한 대중의 신뢰를 구축하는 방법은 무엇인가?
둘째, 안전 인증 프로세스에서 AI의 윤리적 차원(투명성, 차별 금지, 공정성 등)을 통합하는 방법은 무엇인가?
셋째, AI 시스템 인증은 어떻게 준비해야 하는가?
넷째, AI가 현재 항공 운송의 안전 수준을 더욱 향상하려면 어떤 표준, 프로토콜, 방법을 개발해야 하는가?

AI 로드맵 2.0에서는 AI의 신뢰성이라는 개념을 도입하여 프로그램 신뢰성의 목표를 설정하였다. 또한, AI에 관한 EU의 전략과 이니셔티브에 기여할 정책들이 마련되는 데 도움이 되는 내용을 포함하였다(EASA, 2023).

### 2.3.2 항공산업의 AI 영향

AI 기술에 대해서 머신러닝(ML)의 발전, 특히 딥러닝(DL)의 혁신은 항공산업에 커다란 변화를 가져올 가능성을 갖고 있다고 예측하였다(EASA, 2023).

AI와 디지털화는 항공산업의 생산성과 운영 효율성을 크게 향상하며, 특히 유지보수, 항공 교통 관리, 승객 서비스 등 다양한 분야에서 필수적인 역할을 하게 될 것으로 예측하였는데, 다음은 분야별 EASA의 AI 기술 전략을 소개하고자 한다.

#### 2.3.2.1 항공기 설계와 운영

AI 기술의 머신러닝 분야는 과거에는 불가능했던 애플리케이션 개발을 가능하게 하는 잠재력이 있다. 항공분야에 도움이 될 수 있는 기술 발전으로서는 첫 번째로 컴퓨터 비전 자연어 처리(NLP)와 같은 주요 분야는 항공산업에서 중요한 과제를 해결하는 데 이바지할 것으로 예측한다.

5) EASA AI roadmap 1.0 (2020)에서는 AI 기술의 항공 분야에 대한 주요 기술 소개와 조직, 절차, 규정에 미칠 영향을 논의하였고 「머신 러닝 적용 level 1 가이드」가 2021년 12월에 배포되었다. roadmap 1.0은 3년의 유효기간으로 적용되었는데, AI 기술개발 추진과 항공산업의 업데이트 관점이 포함된 내용이 AI roadmap 2.0으로 발간되었다.

1) 컴퓨터 비전
- 고해상도 카메라를 활용한 교통 탐지로 상황 인식을 향상
- 유인 및 무인 항공기를 위한 향상된 장애물 탐지 및 회피 시스템
- 활주로 상태를 정밀하게 관찰하여 악천후에서도 안전한 착륙 지원

- 2) 자연어 처리(NLP)[6]
  조종사의 가상 비서를 개발하여 반복적인 업무를 관리하고 명령에 응답하며, 항공 교통 관제(ATC) 지침을 해석
- 글로벌 항공 환경에서 의사소통을 간소화하기 위한 실시간 번역 시스템

3) 자율 비행

자율 비행은 머신러닝 기술의 가장 주목받는 응용 분야로서, 드론 시장이 이미 자율 비행의 기반을 마련했으며, 도시 항공 모빌리티 수요에 대응하기 위한 항공 택시 시스템 개발을 목표로 한 새로운 비즈니스 모델들이 등장하고 있다. 자율 항공기는 안전한 비행과 착륙을 보장하거나, 현재의 항공 교통 관리(ATM) 관행보다 짧은 거리로 항공기 간의 분리를 관리하는 등 복잡한 결정을 내려야 하는데, AI는 이러한 완전한 자율성을 실현하기 위한 핵심 기술로서, 내장된 센서와 기계 간 통신에서 생성되는 방대한 데이터를 처리할 수 있는 강력한 알고리즘이 필요로 하게 된다.

AI와 ML의 항공 분야 통합은 자율 비행을 넘어 조종사와 시스템 간의 상호작용을 재정의하며, 새로운 가능성을 제공할 수 있다. AI는 반복적이거나 일상적인 작업을 처리하여 조종사가 고부가가치 활동인 비행 안전과 관련된 작업에 집중할 수 있도록 지원한다. 모니터링은 AI가 관리하고, 이를 기반으로 의사결정은 조종사가 하게 되는데, 지금 도입된 auto flight 시스템보다 한 단계 높은 정도의 시스템 운영으로 이해할 수 있다.

AI 시스템으로 조종사가 고된 업무 환경(예: 복행(go-around)이나 우회(diversion))에서도 신속하고 정확한 결정을 내릴 수 있도록 지원하며 조종사의 건강 상태(예: 스트레스, 건강 등)와 운항 상황을 분석하여 잠재적인 위험을 사전에 식별하고 방지하는 데 도움을 줄 수 있다.

기존의 LRU(line replace unit) 간의 결과값을 조종석에서 확인하고 의사결정을 진행했다면 AI 기술은 수학적 최적화 문제를 포함하는 거의 모든 응용 분야에서 사용될 수 있어서, 모든 관련 변수의 조합과 논리적 조건을 분석할 필요 없이 효율적인 솔루션을 제공하게 된다.

예를 들어 비행 제어법, 센서 보정, 연료 탱크의 잔여량 계산, 결빙 탐지 등 센서를 이용한 자료 수집보다 빠른 속도로 조종사에게 정보를 제공할 수 있는 혁신적인 기술 도입이 가능하게 된다.

2.3.2.2 항공기 생산과 정비

AI 기술 도입과 디지털화는 항공 분야의 생산 및 유지보수(구성요소 물류 포함) 프로세스와 비즈니스 모델에 큰 영향을 미칠 것으로 예상하는데, 디지털화가 진행됨에 따라 생산 및 유지보수 조직이 처리해야 하는 데이터량이 꾸준히 증가하고 있으며, 이를 처리하기 위해 AI를 활용해야 할 필요성이 점점 커지고 있다. 대표적인 AI 기술 응용 분야로는 항공기 고장을 예방하기 위한 예지 정비(predictive maintenance)에서 항공기 기단별로 데이터를 활용하여 고장 예측과 예방적 조치를 가능하게 한다.

Airbus의 Aircraft Maintenance Analysis (Airman)'은 100개 이상의 고객이 사용하는 솔루션으로 항공기 상태를 지속해서 모니터링하고, 문제 메시지와 해결 우선순위 정보를 지상 통제소에 전달하고, 이러한 예지 정비를 통해 항공기 가용성을 최대 35% 증가시킬 수 있다.

2.3.2.3 환경

AI 기술의 다양한 적용 분야 중에서는 탄소배출을 줄이는데 이점이 있을 것으로 보인다. 항공 분야에서 환경 평가 요소인 항공기 소음, 비행 중 엔진의 탄소 배출량 등은 오랜 시간 동안 산출되어 비행기록장치(FDR)이나 비행경로 분석을 할 수 있는 (ADS-B) 등의 자료로 컴퓨터에 저장이 되면 누적된 데이터를 활용하여 분석할 수 있다. 머신러닝 알고리즘이 비행 중의 연료 소모량을 계산하여 반영하는 방법을 감항 당국에서 환경 평가 항목으로 반영하면 시스템 개선을 하기 위

6) 자연어(NLP)는 컴퓨터 과학, 인공지능 및 언어학을 종합하여 컴퓨터가 사람의 언어를 의미 있고 맥락과 관련해 이해, 해석, 생성, 응답 등을 하게 하는 것이다. 사용자에게 더 쉽고 직관적인 AI를 만드는데 중요한 요소이다.

한 논의들이 진행될 수 있을 것이다.

2.3.2.4 항공 교통 관제 시스템

항공 교통관리 시스템에 AI 기술을 접목하는 것은 아직 초기 단계로 볼 수 있는데, AI 응용 프로그램을 통해서 빅데이터 처리를 기반으로 복잡한 항공 교통량 패턴과 관제사 지침을 이해하고 해결하는 데 이바지할 수 있다.

날씨 패턴, 항공 교통 혼잡도 및 기여 요인에 대한 데이터를 분석해서 비행경로 최적화를 지원하면 비행시간, 연료 소비, 비용 등을 절감할 수 있는데, 이를 통해 항공 교통 관제 시스템을 효율적으로 운영하여 항공편 지연을 줄이고, 여행량을 증가시킬 수 있다.

머신러닝 모델은 항공교통관제사에서 실시간 지침을 제공하는 의사결정 지원 도구로서 반복적인 항공 교통 관제사(ATCO) 작업의 자동화에 초점을 맞추며, 안전 중심 업무에 더 집중할 수 있도록 지원할 수 있다.

2.3.2.5 비행장

공항 터미널과 비행장에 AI 기술과 머신러닝 기술을 적용할 수 있는데, 비행장에서는 항공기 안전 운항을 위해 다음의 요소들이 고려될 수 있다.

1) 활주로상의 FOD 감지

비행장 운영의 주요 목적은 항공기 운항에 방해가 되는 이물질을 제거하는 것이다. 머신러닝을 통한 FOD 감지 방식은 운영시스템의 신뢰도를 높이게 한다.

2) 조류 탐지 레이더[7)]

공항에서 조류 충돌을 방지하기 위해 Avian Radar를 이용하여 조류 떼의 비행경로를 감지한다. 머신러닝을 적용하여 조류의 규모, 속도, 방향, 비행경로 등의 상황을 파악할 수 있다.

3) UAS 감시 시스템

비행장을 주변으로 불법적으로 비행하는 무인 비행체나 항공기의 이착륙을 위협하는 요소에 적용할 수 있다. 최근에 사용하는 방식은 여러 개의 센서를 기반으로 감지하게 되는데, 머신 러닝을 통한 논리적 접근 방식이 가능하다.

4) 공항 터미널

AI 기술을 통해 승객들이 이용하는 공항 터미널에서는 공항 보안 검색이나 승객의 안전과 보안을 향상하기 위한 공항 운영자를 대상으로 다양하게 적용될 수 있다. 입국 심사나 검색대에서 안면인식을 통한 검색 방법도 가능하며, 공항 테러나 폭발의 위협을 감지하고, 위험하지 않은 열쇠나 벨트의 버클 등을 구분하여 검색의 효율성을 높일 수 있다.

2.3.2.6 사이버 보안

사이버 보안은 3개의 주요 요소로 구분될 수 있다.

첫째, 취약점이 있어 운항에 악용될 위험이 있는 시스템과 조직

둘째, 시스템과 조직의 취약점을 악용할 수 있는 위협(예:악성 프로그램)

셋째, 한 개 이상의 보안 위험을 완화하기 위해 도입한 보안 통제 프로그램 또는 대책

성급한 AI 기술 도입은 위의 3가지 요소에 영향을 끼칠 수 있다. AI를 통해 시스템의 효과가 향상될 수 있지만, 사이버 보안을 위협하는 새로운 형태의 취약점도 드러낼 수 있기 때문에 데이터 오염과 같은 사이버 보안의 위협 양상을 잘 이해하고, 기술적으로 또는 조직적으로 구체적인 보안 통제 요소를 정의해야 한다.

위협 측면에서 보면, 최근의 악성 소프트웨어는 실행 환경에 따라 동작을 조정하는 돌연변이 형태로 나타난다. 새로운 종류인 딥락커[8)]와 같은 AI 기반의 악성프로그램도 연구되었으며, 사이버공격에 AI를 사용하면 기존의 규칙을 기반으로 탐지하는 시스템을 우회하여 소프트웨어 자체가 적응하고, 자율적으로 위협 요소를 생성하는 방식도 가능하다.

AI 기술을 기반으로 하는 사이버공격에 대비하기 위한 대응책 마련이 필요하다.

방어적인 측면에서는 AI의 효과를 극대화하기 위해 보안 통제프로그램에 AI 기술을 적용할 수도 있다. 시스템의 취약점을 자동으로 감지하는 AI 기술을 통해 사이버공격을 예방하고, 행동 기반의 위협을 식별하는 탐지 기술에도 도움이 될 수 있을 것이다.

2.3.2.7 안전 위험 관리

데이터 사이언스는 통계, 수학, 지능형 데이터 확보

7) Avian Radar를 조류 탐지 레이더로 번역함.

8) Deeplocker : AI 기술을 통한 악성코드를 삽입하는 기술로 AI 기반의 영상을 통해 공격대상자를 선정하여 랜섬웨어 공격을 시행한다.

기술, 마이닝과 프로그래밍 등의 여러 분야가 결합하여 빅데이터를 분석하고, 패턴과 정보를 추출하는 전문 분야이다. 다양한 방법, 알고리즘, 복잡한 프로그래밍 기법을 통해 대용량의 데이터를 처리하고 예측하는 분석을 수행해야 하므로 고도의 기술이 필요한 분야인데, AI 사용으로 인해 데이터의 상관관계를 식별하고 분석하는 부분을 중점적으로 데이터 과학 기술의 영향이 많을 것으로 예상한다.

EASA에서 고려하는 AI 기술은 안전에 취약한 요소를 발견하는 능력을 키워서 위험 관리를 하는 데 도움이 될 수 있다. 안전 지능과 관리 분야에서 AI 기술은 위험을 감지하고 분류하여 포트폴리오를 구성할 수 있다. EASA의 데이터 관리 프로젝트 (EASA Data 4 Safety, D4S)에서 머신러닝을 이용한 솔루션을 제공하는 기술을 진행하고 있으며, 자료를 수집하고 분석하는 단계에서 비행 정보, 안전 장애 보고 사항, 날씨 정보 등의 방대한 데이터를 활용하여 분석을 단계별로 진행하고자 한다.

장기적인 관점에서는 AI가 실시간으로 자료를 수집하고, 실시간으로 위험 관리를 할 수 있는 솔루션을 제공할 수 있다고 예상한다.

#### 2.3.3 신뢰성·안전성 기준

인공 지능 기술의 신뢰도를 확보하고, 기계 학습의 단계적 접근을 통해 시스템의 안전성을 구축해 나가는 것이 EASA AI 로드맵의 정책이다. AI 신뢰성을 위한 체계를 만들고, 항공 분야에서 AI를 사용하기 위해 AI 신뢰성 분석, AI 보증 개념, AI를 위한 인적 요소 그리고 AI 안전성 위험도 완화 등의 4개의 요소가 EASA AI 로드맵의 핵심 내용이다.

Orian (2021)은 신뢰성 분석은 항공 분야에서 AI 기술이 전개되어 항공기 운항이 가능한지 불가능한지 판단하기 위한 도구로 활용될 수 있으며, 시스템 설계자를 비롯한 이해관계자들은 AI 기술의 발전을 고려할 때 규제와 AI 기술을 수용할 수 있는 문화를 형성해야 한다고 연구하였다.

EASA의 AI 로드맵에서는 AI를 위한 인적 요소 분야에는 AI를 소개하는 특정한 인적 요소의 필요성에 대해 제시하였다. AI 운항의 설명 가능성은 인간이 제공해야 하며, 이해할 수 있는 사용자가 있어서 실현할 수 있는데, 어떻게 AI와 머신러닝이 원하는 결과를 도출할 수 있는지 적절한 시기를 고려해야 한다. 이 분야에서는 인간과 AI가 팀으로 구성되어 AI 기반의 시스템과 인간이 협력하여 특정한 목적을 달성해야 한다 (EASA, 2023)(Table 2).

AI 로드맵에서 제시한 민간 항공 운송 부분의 ATM/UTM 영역에서 AI 기술의 타임 프레임을 Table 3과 같이 제시하였다. 공항 운영, 정비, 비행장 등의 AI 기술 적용 시점도 유사할 것으로 생각한다.

### 2.4 항공 분야의 사이버 보안 위협과 ICAO의 대응 전략

#### 2.4.1 항공 사이버 보안 위협 사례

기내에서는 항공기와 지상의 기지국 간의 위성을 이용한 통신, 기내 내부에서 무선 인터넷을 이용한 개인과 항공기와의 통신, 기존에 적용되는 항공기 간의 통신 방법 등 항공기를 하나의 통신 무선국으로 활용하여 쌍방향 통신이 가능한 시스템을 적용하고 있다.

Jeong (2019)의 연구에서 항공의 사이버 보안은 항공 사이버 보안과 항공기 사이버 보안으로 구분하며, 항공 사이버 보안은 공항 전산망을 포함한 광범위한 개념이고, 항공기 사이버 보안은 항공기간의 통신 또는

Table 2. EASA AI Roadmap 2.0 trustworthy AI building-blocks

| EASA trustworthy AI building-blocks | | |
|---|---|---|
| Input (EC, Ethical guidelines) | AI Trustworthiness analysis | Output |
| Accountability | | Learning assurance |
| Technical robustness and safety | | |
| Oversight | | |
| Privacy and data governance | | AI explainability |
| Non discriminaion and fairness | | |
| Transparency | | AI safety risk mitigation |
| Societal and environmental well being | | |

Table 3. EASA AI time framework

| First step (2023-2025+) | Second step (2025-2035+) | Third step (2035-2050+) |
|---|---|---|
| Human assistance/ augmentation | Human-AI teaming | Advanced automation and autonomous |

항공기와 지상 기지국 간의 위성통신과 관제 시스템을 포함한 개념으로 정의했다.

최근에 발생한 마이크로소프트사의 보안프로그램의 오류로 항공 사이버 보안에 영향을 미친 사례를 보면, AI 기술을 이용하여 머신 러닝으로 보안 요소를 원격으로 통제하는 새로운 센서에 업데이트 오류로 마이크로소프트 사의 윈도우 운영프로그램과 충돌하여(Crowdstrike, 2024) 전 세계의 공항에서 해당 프로그램을 사용하는 항공사의 발권이 불가하였다.[9]

외부에서의 위협이 아닌 AI 시스템의 신뢰성이 항공 사이버 보안 영역에서 중요함을 입증하게 되었다.

최근 나타나는 새로운 공격 중 일부는 머신러닝(ML)의 형태를 사용하고 있다. 인공지능(AI)과 머신러닝(ML) 활용으로 인해 자동화된 피싱 공격이 점점 더 정교해지고 있으며, 문자나 음성 메시지와 같은 채널을 사용하여 백신 개발에 관한 뉴스를 피싱 캠페인에 사용한다고 연구하였다(Chae, 2021).

ICAO의 부속서 17 Aviation Security는 민간 항공 분야에 승객, 승무원, 지상 직원과 공익의 안전을 위해 불법행위를 정의하고, 이에 대응할 수 있는 조직의 역할이 예방조치 등을 규정할 것을 권고하고 있다.

항공 안전에 관한 내용으로 민간 항공 분야의 안전을 위해하는 요소 중 사이버 위협으로부터 대비하기 위해 각 체약국은 국가 민항항공 안전 프로그램을 마련하고, 정보와 통신 시스템의 위험 요소를 분류하여 불법행위로 간주한 위험 요소를 평가하고, 대응 방안을 실행하고 발전시켜 나갈 것을 권고한다(ICAO, 2022).

또한 체약국은 위험 요소를 분류하여 피해가 식별된 중요 시스템 및/또는 데이터의 기밀성, 무결성 및 가용성 등을 확인하고 사이버 보안을 위협하는 대응 방안에는 특히 설계 보안, 공급망 보안, 네트워크 분리, 원격 액세스 보호 및/또는 제한이 포함될 것을 요구한다(ICAO, 2022).

ICAO에서는 사이버 보안을 공격, 손상, 무단 액세스, 사용 및/또는 착취로부터 시스템, 네트워크, 프로그램, 장치, 정보 및 데이터의 기밀성, 무결성, 가용성 및 전반적인 보호를 보장하도록 설계된 기술, 제어 및 조치, 프로세스 및 관행의 본체로(ICAO, 2022) 정의하였고, 2022년에는 Cybersecurity를 강조하며, 민간 항공 분야에서 사이버 보안에 관한 문화를 형성하고, 항공 안전을 위협하는 요소에 대한 보안 방안을 강화하는 내용의 권고 사항을 제시하였다(ICAO, 2022).

국내에는 항공에 관한 사이버 위협이나 사이버 보안에 관한 국제 지침을 이행할 수 있는 법률이 아직 마련되어 있지 않으며, 항공 보안법에서 정의한 불법행위의 개념에도 사이버 위협은 없고, 실제 물리적으로 손해를 입을 수 있는 행위들이 정의되어 있다.

ICAO의 체약국으로서 부속서 17의 권고안을 수행하기 위한 사이버 보안에 대한 정책 마련이 필요한 부분이다.

### 2.4.2 ICAO의 Cyber Security 정책

항공산업은 인공지능(AI) 기술의 통합으로 상당한 발전을 이루고 있다. 항공 분야에서 AI 기술은 빠른 체크인 프로세스와 고객 서비스에 점점 더 많이 사용되어 전반적인 여행 경험을 향상하고, 실시간 수요 및 공급 분석을 기반으로 항공권 가격을 최적화하여 항공편 운항에 혁신을 일으키고 있다. AI 기반 컴퓨터 비전은 감시 목적으로 활용되어 시스템 효율성과 공항 인프라를 관리하고 있다(Sarah, 2024).

항공기에서 통신 채널을 통해 접수된 정보를 공유할 수 있는 내용인지, 사이버 안전성에 위해를 주는 내용인지를 분류하여 정보의 위험도를 단계별로 구분하여 대응할 수 있도록 ICAO에서는 TLP(traffic light protocol)를 제시하고 있다(ICAO, 2021).

항공 분야에서 사이버 보안과 사이버 회복력을 다루는 핵심은 인적 요소이므로 안전하고 회복력 있는 부문을 지원하기 위해서는 모든 사람의 인식을 높이는 것이 필수적이다. 정보가 커뮤니케이션 채널을 통해 수신될 때, 어떤 정보가 다른 사람들과 공유 가능한지, 그리고 그 정보를 누구와 공유할지를 이해하는 것은 인식을 높이는 데 필요한 핵심 행동 중 하나이다(ICAO, 2021).

TLP는 민감한 정보를 아는데, 어떻게 공유할 수 있는

9) MS 사의 클라우드를 기반으로 운영하는 미국 내의 공항에서 4일간 1,000회 이상의 비행이 취소되고 9,000편의 항공기가 지연되었다.

지를 나타내는 간단하고 직관적인 개요를 제공하여 더 빈번하고 효과적인 협업을 촉진하고자 한다(ICAO, 2021).

다음은 정보의 위험도에 따른 대응 단계를 색깔별로 구분해서 분류해 놓은 권고안이다(Table 4).

ICAO 체약국과 이해관계자들은 TLP 사용 가이드가 이행될 수 있도록 독려해야 한다.

Lim and Kang(2017)은 사이버 보안은 과거의 방화벽이나 소프트웨어 제어 인증 (authentication)만으로는 충분하지 않다. 시스템을 관찰하여 비정상적인 상태를 검출하여 침입자를 확인하고 보호해야 하며, 주기적인 시스템 검사와 검증으로 무결성과 가용성을 확인해야 한다고 연구하여 선행연구도 ICAO의 정보 공유 프로토콜의 중요성을 입증한다.

한편, 민간 항공 분야에서도 사이버 위협에 대응하기 위해 위험 요소를 인지하고 분석하고 대응할 수 있는 사이버 보안 문화 정착을 권고하고 있다. 보안문화에 반드시 고려해야 하는 요소로서는 다음과 같다.

첫째, 사이버 보안 정책을 수립하고, 그 방안에 순응하기 위한 문화를 조성하는데 지도력을 제안한다.

둘째, 모든 조직의 다양한 사이버 위험과 취약점을 고려하여 도메인 간 링크를 공식적으로 설정해야 한다.

셋째, 소통의 중요성을 강조한다. 내부적으로나 외부적으로 의사소통은 핵심적인 역할을 담당하므로, 성공적인 사이버 보안 문화 구현을 위한 기대되는 인식 수준에 도달할 수 있는 주요 수단이 될 수 있다.

넷째, 인식, 훈련 및 교육은 강력한 사이버 보안 문화를 위해 활용되어야 하는 학습 과정의 핵심 영역으로서, 인식은 사람들에게 지식을 제공하고, 훈련은 기술을 가르치고, 교육은 이론적 틀 안에서 지식과 기술을 제공하여 인식과 훈련을 통합한다.

다섯째, 보고 시스템 구축을 제시한다. 사이버 보안 보고 시스템은 항공 안전 및 항공 보안 보고 시스템의 요소를 모두 수집한다. 첫 번째 영역은 조직 정보 보안 정책 및 프로세스와 일치하지 않는 자체 조치/오류 보고이고, 두 번째 영역은 다른 직원의 의심/오류 행동을 보고한다. 사이버 보안 보고 메커니즘을 개발할 때 조직은 항공 안전 및 항공 보안 보고 시스템을 개발하고 구현하는 데 있어 얻은 경험을 활용할 수 있다.

여섯 째, 사이버 보안문화를 형성하는 조직에서는 현재 시행 중인 조치가 사이버 보안 문화에 미치는 영향을 평가하고, 원하는 문화 결과와 실제 문화 결과 사이에 존재하는 차이를 파악할 수 있도록 설계된 성과 지표 체계를 개발해야 한다.

마지막으로 긍정적인 근무 환경이 조성되도록 노력해야 한다. 일반적인 긍정적인 업무 환경은 또한 사이버 보안 문화에 대한 직원들의 헌신에 큰 영향을 미치고, 사이버 보안 성과를 향상할 수 있다(ICAO, 2022).

Table 4. Traffic light protocol category

| TLP | 정보 사용과 접근 제한 |
|---|---|
| Red | 정보의 소스가 오용되면 당사자의 개인 정보 보호 평판이나 운영에 영향을 미칠 수 있을 때 |
| Amber | 정보를 효과적으로 처리하기 위한 지원이 필요한 경우<br>하지만, 관련 조직 외부에서 공유하는 경우 개인 정보 보호, 평한 또는 운영에 위험을 초래하는 경우 |
| Green | 정보가 광범위한 커뮤니티나 동료가 있는 모든 참여 기관의 인식에 유용할 때 |
| White | 정보가 오용될 위험이 거의 없거나 전혀 없을 때 공증에 공개할 수 있는 정보 |

## Ⅲ. 결 론

### 3.1 국제적 법률 정비 및 협력 방안

국제 지침인 ICAO의 항공 사이버 보안에 관한 행동지침을 국내 제도에 도입할 수 있도록 항공 당국, 항공사, 공항 등 이해관계자들의 협의체가 구성되어 연구가 진행되어야 한다.

운항과 항행 그리고 항공 안전 및 보안 부문의 정책이나 관련 법률 정비와 연구의 지원이 가장 시급한 분야로, 정보통신 기술과 항공 부문 기술 융합은 더욱 많은 영향을 미치게 될 것으로 생각하며, 사이버 위협에 대응할 수 있는 항공 보안 정책 및 관리 체계 개선이 요구된다(Jeon, 2023).

국내에서 사이버 보안에 대한 부처별 대응체계는 Fig. 1과 같이 분류한다(National Assembly Library, 2023).

국가정보원은 「국가정보원법」 제4조에 따라 2004년 2월 출범한 '국가사이버안보센터'를 중심으로 사이버 위협정보의 허브 구실을 하고 있으며, 국가사이버위기관리단을 설치하여 관련 부처, 전문기관 그리고 기업 등과 실시간 위협정보 공유 및 사이버 위기에 대비·대응하고

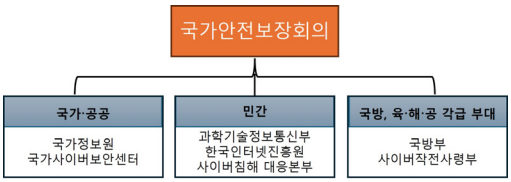


Fig. 1. Cyber security response system in Korea

있다(National Cybersecurity Center, 2025).

교통 분야는 「자동차관리법」에 따라 주관 부처인 국토교통부가 상황을 보고하고 있으나, 항공 분야는 공공기관이나 국가기관 중 대응할 수 있는 근거 법령이 없다.

정부는 현재 부처별 소관 개별 법령에 따라 제각각 분리, 독립 대응하고 있는 국가 사이버 보안 체계를 대통령실 중심의 관리 체계로 구축하고, 국가 사이버안보 위협 상황 발생 때 범정부 차원의 종합적으로 대응하기 위해 「국가사이버안보 기본법」 입법을 예고하였다(MOLEG, 2022).

현재 공항의 사이버 위협에 대한 대응 활동은 항공기를 이용하는 승객과 공항에서의 항공기 안전 운항을 위해 인천국제공항에서 해킹이나 컴퓨터 바이러스 등에 의한 개인정보 유출 및 훼손을 막기 위하여 보안프로그램을 설치하고, 주기적인 갱신·점검을 하며, 외부로부터 접근이 통제된 구역에 시스템을 설치하고, 기술적/물리적으로 감시 및 차단하고 있다(IIAC, 2025).

공항 이용객은 디지털 서비스 이용을 위해 공항에 다양한 개인정보를 제공하고 있는데, 허가받지 않은 접근 예방을 위한 기술적, 제도적 장치를 마련하여 신뢰를 확보해야 한다(Lee et al., 2024).

사이버 보안을 위협하는 사례가 정보기술이 발전됨에 따라 다양한 양상으로 시도되고 있으나, 국내에는 이를 처벌할 수 있는 규정이 미비한 상황이며, ICAO에서는 항공 사이버 보안 위협을 단계별로 분류하여 대응할 수 있도록 기준을 제시하고 있는 만큼, 국내에서도 사이버 보안을 위협하는 불법행위에 대해 적극적으로 대응할 수 있는 법적 근거가 마련되어야 한다.

### 3.2 시사점

항공기는 고도의 안전성 확보가 요구되는바, 사이버 위협에 선제 대응을 위해서는 상시 위협을 감시하고, 사이버 침해행위, 위해행위에 실시간 대응이 가능한 관리 체계를 구축하여 항공 부분의 안전성을 확보해야 한다(Kang et al., 2023).

현재 한국에는 항공 AI 관련 법률이 없지만, 기존의 「항공안전법」·「항공보안법」 등을 개정하여 AI 기술을 적용하기 위한 법률 검토가 필요하다. 또한, 2026년 시행 예정인 「인공지능 기본법」을 「항공보안법」에서 국제 지침과 연계하여 AI 기반의 항공기 발전 동향을 적용한 정책도 함께 마련될 수 있다.

「국가사이버안보 기본법」에 따라 항공 분야도 공공기관 및 정부 기관이 대응할 수 있는 규정이 명문화 되어야 한다. 현재 대한민국에서는 항공 운항 분야에 적용될 인공지능(AI) 기술에 대한 구체적인 정책이나 규정이 명확하게 제정되어 있지 않으나, AI 기술의 중요성을 인식하고, 다양한 산업 분야에서의 활용을 촉진하기 위해 노력하고 있다.

국제 지침을 시행하면서 AI 기술을 적용하기 위한 근거법 마련과 함께 항공 안전을 위협하는 사이버 불법행위에 대해서도 규제할 수 있는 법률도 마련하여 새로운 패러다임으로 전환하는 항공산업에 대비해야 한다.

## References

1. Chae, J. B., "International political trends in cyber security and Korea's strategic plan", INSS, Seoul, 2021, pp.54-55.
2. Crowdstrike, "External Technical Root Cause Analysis-Channel File 291", Crowdstrike, Austin, 2024, pp.1.
3. Europe Union Artificial Intelligence Act, Regulation(EU) 2024/1689, 2024.
4. European Union Aviation Safety Agency, AI Roadmap 2.0, 2023.
5. Incheon International Airport Corporation, "privacy policy' article 8. measures to ensure the security of personal information", Available from : https://www.airport.kr/ap_en/1568/subview.do
6. International Civil Aviation Organization, Annex 17 Aviation security, 2022.
7. International Civil Aviation Organization, Cybersecurity action plan, 2022.
8. International Civil Aviation Organization,

Cybersecurity Culture in Civil Aviation, 2022.
9. International Civil Aviation Organization, Guidance on Traffic Light Protocol, 2021.
10. Jeon, S. H., "A study on proactive responses to in-flight cyber threats", Journal of the Aviation Management Society of Korea, 21(5), 2023, pp.67-78.
11. Jeong, D. Y., "Legal considerations on tortious interference in aircraft cyber security", Korean Society of Aviation Management Spring Conference Presentation Papers, Gwangju, 2019, pp.1-8.
12. Kang, M. H., Jeon, S. H., and Hwag, H. W., "A study on the necessity of cybersecurity legislation and policies in response to the use of EFB by flight crew", Journal Korean Society for Aviation and Aeronautics, 31(4), 2023, pp.72-81.
13. Lee, G. J., Park, J.W., and Lee, S. R., "Investigating the determinants of willingness to provide personal information based on privacy concerns of smart airport passengers", Journal Korean Society for Aviation and Aeronautics, 32(4), 2024, pp.73-84.
14. Lee, S. W., "How AI and the brain work", Sol-book, Goyangsi, 2022, pp.20.
15. Lim, I. K., and Kang, J. Y., "Security problems in aircraft digital network system and cybersecurity strategies", Journal of Advanced Navigation Technology, (6), 2021, pp.637.
16. Ministry of Goverment Legislation, "Legal trends related to artificial intelligence (AI)", July, Latest Legislative Trends, 2024.
17. Ministry of Goverment Legislation, Pre-Announcement of Legislation, 2022-5.
18. Ministry of Science and ICT, "Roadmap for Maintenance of Artificial Intelligence Laws, Systems, and Regulations", Sejong, 2020, pp.4-38.
19. National Assembly Library, "'Cybersecurity at a Glance", Factbook 2023-8, 108, pp.56.
20. National Cybersecurity Center, "Center introduction", Available from: https://www.ncs c.go.kr
21. National Information Society Agency, "The AI Report 2024-1", AI Policy Research Team, Daegu, 2024, pp.145-146.
22. Orian D. and Ivo E., "Flying high for AI? Perspective on EASA's roadmap for AI in aviation", Air and Space Law, (1), 2021, pp.5-6.
23. Park, J. B. and Kim, H. H., "Advancement of artificial intelligence technology and its legal countermeasure", Hanyang Law Review, 34(2), 2017, pp.39.
24. Sarah, "Artificial Intelligence (AI) In aviation market 2024-2028", Technavio, 2024, Available from: https://newsroom.technavio.org/artificial-intelligence-in-aviation-market-analysis
25. Yoon & Yang LLC, "AI trends and implications in the United States", The Law Times, 2023, Available from : https://www.lawtimes.co.kr/LawFirm-NewsLetter/187480