사이버보안 위협 대응을 위한 법률 개정안

항공보안학과
홍제준 김조엘 이서진

목차

9만 명 개인 정보 유출
2차 범죄 위험 ↑

핵심 인프라 마비
운영 차질
사회 혼란 및 경제 손실

금전 요구 및 거부 시
데이터 공개 협박

2024년 8월 시애틀 항만청
랜섬웨어 공격으로 약 9만 명
개인 정보 유출, 공항 운영 차질 발생

450만 명 대규모
개인 정보 유출
2차 피해 우려

정보 유출 인지
해킹 3개월 후 인지
초기대응 미흡

SITA 서비스를 이용하는
다른 항공사 고객 정보
유출 가능성

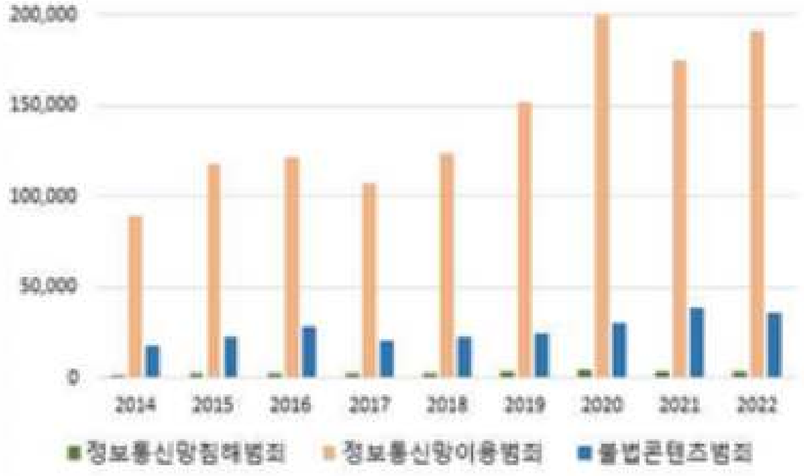
2021년 5월 에어 인디아
SITA의 시스템 해킹으로
약 450만 명 개인 정보 유출

데이터 보안 취약성 심화 → 사이버 공격 시 대형 보안 사고 직결 우려

〈그림 1〉 사이버 범죄 발생·검거 현황

자료: 경찰청, 경찰통계자료

〈그림 2〉 사이버 범죄 세부 유형별 발생 건수



자료: 경찰청, 경찰통계자료

동기 및 문제의식

서비스 거부 공격

비인가 접근 공격

개인정보 유출

범죄 계획

검색 시스템 우회 성공

사건 발생

종결

직접적 피해:

심리적 영향:

운송 차질: 항공편 대량 결항/지연, 공항 폐쇄로 국내외 여객 수송 중단

국제적 제재: ICAO 등 공항 보안 등급 하향, 국제선 취항 제한, 환승 거부 등

경제적 파급:

장기적 손실:

책임 소재 논란:

사회적 불신 심화:

2차 사회적 혼란:

- 실제로는 사이버 공격이 항공보안에 직접적인 위협이 되고 있음.

- 법제적 대응 부족:

- 국가 간 협력 미흡:

- 공급망 보안 취약:

항공 사이버 보안 법률 강화

기존 법률

ICAO

1 ICAO Annex 17에서는 사이버 위협을 **보조 위험요소**로 기술

2 Doc 10108는 기술적·조직적 대응 중심이며, 사고 발생 시 **법적 책임 불분명**

3 공급망 보안 취약: 민간·외주 업체 보안 체계 미비

도입될 필요가 있는 법률

1 사이버테러를 침입, 화물 위해물 등과 동등한 **독립 위협 범주**로 격상

2 항공기·공항·지상 인프라에 대한 사이버공격 발생 시, 관계자들의 **책임 분배** 원칙을 명시

3 디지털 침해 범죄에 대한 수사 공조 및 처벌 체계 정비

1. 사이버공격 대응의 책임 명확화
→ 신속한 복구 및 피해 최소화

- 명확한 책임 분배 덕분에 사고 발생 시 책임공방 없이 즉시 조치 가능.
- 조사·보상·시스템 복구 과정이 투명하고 빠르게 진행, 여론 신뢰 회복에 기여.

2. 항공 보안 시스템의 전반적 회복력 강화

- AI 보안검색, 무인탑승, 디지털 통신 등 모든 시스템에서 사이버방어 설계가 기본요건이 됨.
- 모의 침투 테스트, 보안 업데이트 체계화 등으로 보안 수준 상향 평준화.

3. 국제 협력 강화 및 '사이버 테러' 억지 효과

- ICAO 차원의 국제 공조 프레임워크가 작동되면, 범국가적 수사·처벌 가능

→ 공격자에게 실질적 위협.

- 사이버공격의 비용은 올라가고 성공률은 낮아져, 조직범죄나 테러조직의 시도 자체를 줄이는 억지력 효과.

4. 항공산업과 국민의 신뢰 회복

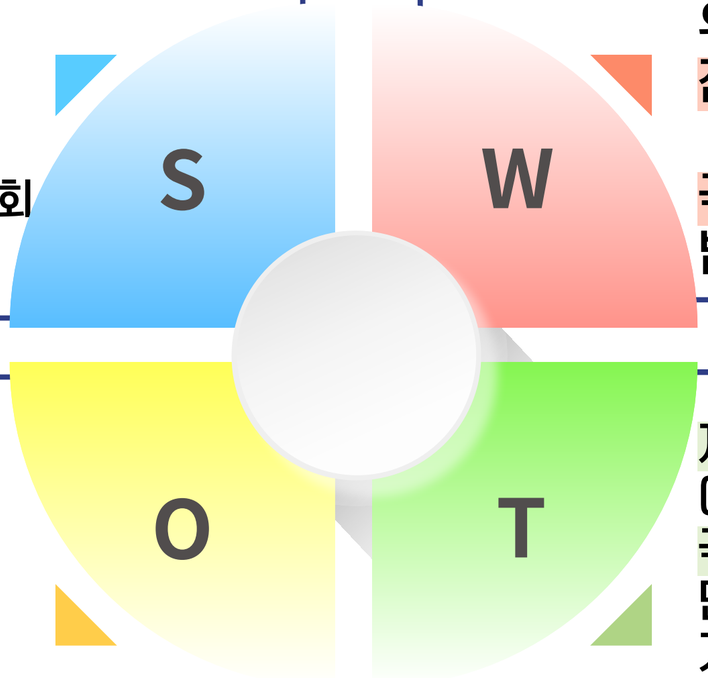
- 사이버보안을 공식 위협 범주로 다루는 정책적 선언은, 국민과 국제 사회에 "우리는 대비하고 있다"는 강력한 메시지.

→ 항공사·공항의 이미지 회복, 관광·물류 회복, 경제적 회손 최소화

SWOT 분석

STRENGTHS

보안 대응 속도 향상: 제도적 명확화로 신속 대응
책임 소재 명확화: 책임 주체 명시, 사고 후 공방 감소 및 피해 최소화
미래 보안 선제 대응: AI/자동화 중심 미래 항공 보안 대비
국제 리더십 확보: 국제사회 항공 안전 주도 기회



WEAKNESSES

협력 체계 구축 난항: 공항/항공사/위탁업체 간 시간·비용 소요
전문 인력/기술 부족: 사이버 보안 전문 인력 및 기술 역량 격차
국제 법규와의 충돌: ICAO 및 각국 법 체계와 정합성 문제 발생 가능

글로벌 협력 확대: 국제 항공사/보안업체와 협업 증진
기술 경쟁력 확보: AI 보안 기술 수출 시 차별성 확보
시장 선도 우위: 항공 보안 정책 선도국으로 경쟁 우위
국가 회복력 강화: 사이버 테러 억지로 국가 이미지/관광/물류 회복력 향상

OPPORTUNITIES

제도적 한계: 지능화/국제화되는 사이버 공격에 대한 제도만으로는 한계
국제 공조 지연: 수사 및 처벌 공백 발생 가능
민간 반발 및 예산 부담: 정책 도입 초기 기업 반발 및 비용 부담
정책 실패 시 역효과: AI/자동화 기술 불신 증폭

Threats

ICAO Annex 17 – Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference

ICAO Doc 10108 – Aviation Cybersecurity Strategy and Action Plan (Cybersecurity Guidance)

IATA (International Air Transport Association) – Aviation Cybersecurity Toolkit

EU Aviation Safety Agency (EASA) – Cybersecurity in Aviation

UNODC (United Nations Office on Drugs and Crime) – Guide on International Cooperation in Cybercrime Cases

네이버뉴스,구글 참조.