

무인항공기 운용 확대에 따른 항공보안 법규 개선 방안

UAV 활용 증가와 보안 체계 개선 필요성

202400634 구경민
202400635 기민경
202400643 신하람

목차

연구 배경 및 목적

- UAV 활용 증가
- 새로운 보안 접근 필요
- 기존 체계의 한계
- 위협 분석 및 개선 제시

무인항공기 운용 현황

- 한국 드론 시장 규모
- 기술 고도화 현황
- 다양한 분야 활용
- 보안 취약성 노출

현행 항공보안 법규

- ICAO Annex 17
- 국내 항공보안법
- 주요 규제 사항
- 현행 법규의 한계

보안 위협 유형 및 사례

- 항공기 운항 방해
- 테러 및 범죄 도구화
- 사이버 보안 위협
- 개인정보 침해 사례

법적·제도적 개선 방안

- 전담 법령 제정
- 위치 송신 의무화
- 통합 식별 시스템
- 국제 기준 정합성
- 탐지 기술 지원

결론

- UAV 운용의 양면성
- 보안 체계 개선 필요
- 위협 분석 및 대응책
- 유연한 법제도 구축
- 통합 대응 체계 시급



무인항공기(UAV) 활용 증가와 보안 문제

무인항공기의 활용이 급증하면서 항공 보안에 대한 새로운 접근이 요구되고 있다. 특히 드론의 다양한 활용은 공역 내 안전 및 보안 문제를 심각하게 부각시키고 있다.

기존 항공보안 체계의 한계와 연구 목적

- 유인항공기 중심의 보안 체계로는 대응 한계
- 드론의 소형성, 비가시성, 원격 조종 특성 고려 필요
- 새로운 항공보안 위협 분석 및 법규 개선 방향 제시
- 효과적인 UAV 보안 체계 구축을 위한 방안 모색



한국 드론 시장 현황

“

”

UAV 기술 발전 및 활용 분야 확대

- 2024년 기준 약 2,700억 원 규모
- 자율비행, 군집비행 기술 고도화
- AI 기반 자동조종 시스템 발전
- 물류, 재난대응, 국토 감시 등 활용
- 산업시설 점검 분야로 확대
- 군사용에서 민간 활용으로 급속 전환
- 다양한 산업 분야에서의 수요 증가



UAV 관련 주요 보안 위험

- 통신망 해킹: 불법적 원격 조종 가능성
- 비인가 지역 무단 비행: 제한구역 침범
- 불법 촬영: 개인정보 및 기밀정보 유출 위험



보안 취약성에 따른 잠재적 위험

- 항공 교통 혼잡 및 충돌 위험 증가
- 테러 도구로의 악용 가능성
- 사이버 공격을 통한 대규모 피해 우려
- 국가 주요 시설에 대한 보안 위협 증대



국제 및 국내 법규

- ICAO Annex 17: 국제 항공보안 기준 제시
- 국내 법규:
 - 항공보안법
 - 항공안전법
- 회원국: 자국 항공보안 프로그램 수립 의무

- 공항 주변 비행금지구역 지정
- 드론 등록제도 시행
- 조종자 자격 요건 설정
- 비행 허가 및 안전 기준 준수 요구

주요 규제 사항





유인항공기 중심 법규의 한계

- 기존 법규, 유인기 중심
- UAV 특성 고려 미흡
- 새로운 위협 대응 한계
- 법적 체계 개선 필요성



무인항공기 특성 미반영

- 소형성 고려 부족
- 비가시성 대응 미흡
- 원격 조종 특성 간과
- UAV 운용방식 미반영



제재 및 탐지 기술 기반 부족

- UAV 위반행위 제재 미흡
- 처벌 수위 불충분
- 탐지기술 법적근거 부재
- 대응체계 구축 지연



무인항공기 관련 보안 위협 유형



항공기 운항 방해

- 공항 주변 불법 비행
- 항공기 충돌 위험
- 비행 경로 간섭
- 이착륙 방해



테러 및 범죄 도구화

- 폭발물 운반
- 생화학 물질 살포
- 주요시설 공격
- 불법 물품 운송



사이버 보안 위협

- 통신 해킹 위험
- 원격 조종 탈취
- 데이터 유출
- GPS 스푸핑



사생활 침해

- 불법 촬영
- 개인정보 수집
- 사유지 침입
- 스토킹 도구화



사건 개요

- 2018년 영국 게트윅 공항
- 드론 불법 출몰 사건
- 36시간 공항 폐쇄
- 1,000여 편 항공기 운항 차질
- 14만 명 승객 영향



발생 원인

- 드론 탐지 시스템 부재
- 불법 비행 제재 미흡
- 공항 보안 체계 허점
- 드론 대응 매뉴얼 부재



대응 조치

- 군 병력 동원
- 드론 탐지 장비 긴급 도입
- 공항 주변 비행금지구역 확대
- 드론 등록제 강화



시사점

- UAV 위협 현실화 확인
- 공항 보안 체계 재검토 필요
- 드론 탐지·대응 기술 중요성
- 법규 및 제도 개선 시급성



보안 위협 사례 (2)

1

사건 개요

- 2025년 아일랜드 더블린
- 드론 이용 테러 시도
- 파이프 폭탄 장착 드론 추락

2

공격 방식

- 소형 드론에 폭발물 부착
- 원격 조종으로 목표물 접근
- GPS 기반 자동비행 추정

3

피해 상황

- 민가 지붕 추락, 폭발 미발생
- 인명피해 없음
- 주변 건물 일부 파손

4

대응 및 조치

- 현장 즉시 봉쇄 및 대피
- 폭발물 처리반 출동
- 드론 잔해 분석으로 조종자 추적
- 주변 CCTV 영상 분석

5

시사점 및 교훈

- 드론의 테러 도구화 현실화
- 소형 UAV 탐지·요격 기술 필요
- 드론 구매·운용 규제 강화 필요
- 대테러 대응체계에 UAV 고려 필수



무인항공기 관련 사이버 보안 위협



Wi-Fi 신호 해킹

- DJI 드론 해킹 사례 발생
- Wi-Fi 신호 취약점 이용
- 드론 제어권 탈취 가능성
- 개인정보 유출 위험 증가
- 드론 통신 보안 강화 필요



통신 취약점 악용

- 드론-조종기 간 통신 취약
- 데이터 암호화 미흡 문제
- GPS 스푸핑 공격 위험
- 펌웨어 업데이트 취약점
- 보안 프로토콜 개선 시급



원격 조종 위험

- 무단 원격 조종 가능성
- 테러 및 범죄 악용 우려
- 중요 시설 침입 위험
- 사생활 침해 문제 발생
- 인증 시스템 강화 필요



무인항공기 전담 법령 제정 필요성



현행법 한계

- 유인항공기 중심 법규
- UAV 특성 미반영
- 제재 수준 부족
- 탐지 기술 법적 기반 미흡

UAV 특성

- 소형성 고려
- 비가시성 대응
- 원격 조종 규제
- 다양한 용도 반영

보안 강화

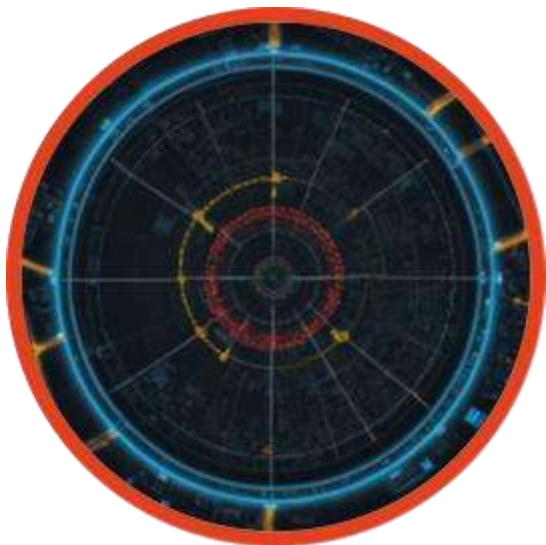
- 위치 추적 의무화
- 등록제 강화
- 조종자 자격 강화
- 비행 제한구역 확대

국제 협력

- ICAO 기준 준수
- EU 규정 참조
- 국제 공조 체계
- 기술 표준화



위험지역 실시간 위치 송신 의무화



공항 주변

- 비행 금지구역 설정
- 실시간 위치 정보 전송
- 비인가 접근 시 경고



원자력 시설

- 보안구역 설정 확대
- 드론 탐지 시스템 구축
- 비상 대응 절차 마련



군사기지

- 군사보호구역 확장
- 드론 식별 체계 도입
- 무력화 시스템 배치



등록제 강화

- 모든 UAV 의무 등록
- 소유자 정보 데이터베이스
- 정기적 안전점검 실시



UAV 통합 식별 시스템 도입



1

국토교통부

- 드론 등록 관리
- 비행 허가 시스템
- 공역 관리 총괄
- 민간 드론 규제
- 사고 조사 주관
- 정책 수립 주도



2

경찰

- 불법 비행 단속
- 범죄 용의 추적
- 도심 감시 활용
- 수색 구조 지원
- 교통 관리 보조
- 증거 수집 활용



3

군

- 군사시설 보호
- 적 드론 식별
- 대공방어 통합
- 군사용 운용
- 국경 감시 활용
- 정찰 임무 수행



4

해양경찰

- 해상 불법 감시
- 해양 수색 구조
- 항만 보안 강화
- 해양오염 감시
- 어업 단속 보조
- 해상 경계 순찰



5

정보기관

- 대테러 정보 수집
- 주요 인사 경호
- 해외 정보 수집
- 사이버 보안 강화
- 첨단기술 보호
- 위협 평가 분석



국제 기준에 부합하는 규제 정비



ICAO 기준

- Annex 17 준수
- 보안 프로그램 수립
- 위험 평가 체계화



EU 규정

- 원격 조종사 자격증
- 운영자 등록 의무화
- 위험 기반 분류 체계



국제 협력

- 정보 공유 플랫폼
- 공동 대응 훈련
- 국제 회의 참여



기술 표준화

- 통신 프로토콜 통일
- 식별 시스템 호환
- 안전 기준 일원화



1



2



3



4



5

C-UAS 배치

- 공항 및 중요 시설에 C-UAS 배치
- 드론 탐지 및 대응 시스템 구축
- 실시간 모니터링 및 대응 체계 확립

예산 확보

- C-UAS 도입 및 운영을 위한 예산 확보
- 정부 지원 및 민간 투자 유치
- 장기적인 자원 조달 계획 수립

법적 근거 마련

- 드론 탐지 및 무력화 기술 관련 법규 제정
- C-UAS 운영에 대한 법적 권한 부여
- 개인정보 보호 등 관련 법규 정비

기술 개발 지원

- 국내 드론 탐지 및 무력화 기술 R&D 지원
- 산학연 협력 체계 구축
- 기술 표준화 및 인증 제도 마련

국제 협력 강화

- 국제 기구와의 기술 및 정보 공유
- 글로벌 C-UAS 표준 개발 참여
- 국가 간 공동 대응 체계 구축

결론

- 
- 무인항공기 운용 확대에 따른 편익과 위험 공존
 - 기존 유인항공기 중심 보안체계의 한계 노출
 - UAV 관련 다양한 보안 위협 분석 및 대응방안 제시
 - 무인항공기 특성에 맞는 별도 법령 제정 필요
 - 실시간 위치 송신, 통합 식별 시스템 등 기술적 대응 강화
 - 국제 기준에 부합하는 규제 정비로 글로벌 대응력 향상
 - C-UAS 등 첨단 기술 도입을 위한 제도적 지원 확대
 - 지속적인 기술 변화에 대응 가능한 유연한 법제도 필요

참고문헌



1. ICAO (International Civil Aviation Organization). Annex 17 to the Convention on International Civil Aviation - Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference. Retrieved from <https://www.icao.int/security/sfp/pages/annex17.aspx>

2. UAV Coach. Drone Laws in South Korea (Updated). Retrieved from <https://uavcoach.com/drone-laws-in-south-korea/>

3. DJI. 드론 비행 안전 가이드: 한국의 드론 규제 안내. Retrieved from <https://www.dji.com/flyingtips/kr>

4. Grand View Research. South Korea Drone Market Size Report, 2024-2030. Retrieved from <https://grandviewresearch.com/horizon/outlook/drone-market/south-korea>

5. The Times UK. (2025). Finglas drone attack: Pipe bomb drone crashes in Dublin. Retrieved from <https://www.thetimes.co.uk/article/finglas-drone-attack-guns-prisons-5zv8szm3t>

6. Airsight GmbH. Gatwick Airport Incident: How Drones Exposed Global Airport Vulnerabilities. Retrieved from <https://www.airsight.com/blog/airport-security-gatwick-shows-u-s.-airport-vulnerability-to-drones-threats>

7. ArXiv.org. (2023). DJI Drone WiFi Protocol Reverse Engineering and Remote Takeover. Retrieved from <https://arxiv.org/abs/2309.05913>