

	<h1>보 도 자 료</h1>	과학기술정보통신부 정보보호산업과 과 장 정은수(044-202-6450) 사무관 최보훈(044-202-6457)
 관계부처 합동	<p style="color: red;">2020년 12월 2일 조간</p> <p style="color: red;">(12. 1. 12:00 이후)부터</p> 보도하여 주시기 바랍니다.	국토교통부 첨단항공과 과 장 문석준(044-201-4307) 사무관 홍일산(044-201-4253)

## 과기정통부-국토부, 안전한 융합서비스 구현을 위한 드론 사이버보안 가이드 발표

- 산·학·연 전문가와 함께 드론 사이버보안 가이드 개발 -

□ 과학기술정보통신부(장관 최기영, 이하 '과기정통부'), 국토교통부(장관 김현미, 이하 '국토부')는 한국인터넷진흥원(원장 김석환)을 통해 드론 분야의 사이버안전 확보를 위한 '민간 분야 드론 사이버보안 가이드'를 발표하였다.

○ 과기정통부는 사물인터넷 제품·서비스의 보안 내재화를 위하여 'IoT 공통 보안 가이드'('16년)를 마련하고, 이를 주요 사물인터넷 산업 분야의 보안특성에 맞게 분석·특화하여 분야별 보안 가이드\* 개발을 지원해 왔다.

\* 홈·가전, 공장('17년), 교통, 의료('18년), 환경·재난, 에너지('19년) 등

□ 드론은 과거 군수용으로 시작하여 여가·취미용으로 대중화되었고, 기상관측, 시설점검, 재난·교통감시, 물류, 국토·해양관측, 농업 등 다양한 산업 분야에서 활용되고 있으며, 국내 시장 규모도 최근 4년여 만에 6배 이상 성장한 4차 산업혁명시대 신성장동력 이다.

\* (국내 드론시장 규모) '16.12월 704억 원 → '20.6월 4,595억 원

동 기간 기체신고 규모 6배, 활용업체 수 3배, 조종자격 취득자 25배 증가

- 하지만, 드론 확산과 함께 사이버 침해위협도 증가하여 해킹에 의한 데이터(기록 사진·동영상, 비행경로 등) 유출, 드론 탈취에 의한 폭탄 테러 위협 등으로 미 의회는 ‘드론 보안법(the American Security Drone Act of 2019)’을 발의하였고, 미군은 중국산 드론의 사용을 금지하는 등 드론 사이버 보안의 중요성은 날로 증가하고 있다.
- 이에 양 부처는 안전한 드론 서비스 환경 구축·운영을 위하여 드론 제품·서비스 개발·운용 업체, 정보보안 담당자 등이 참고할 수 있는 안내서인 동 가이드를 개발하였고, 향후 가이드를 기반으로 드론 안전 인증에 적용될 수 있는 보안 기준을 마련할 계획이다.
- 동 가이드는 드론 서비스를 구성하는 드론(구동부, 제어부, 페이로드, 통신부 등)과 주요 시스템(드론, 지상제어장치, 정보제공장치 등)에 예상되는 보안 위협 시나리오와 보안 요구사항을 제시하였다.
- 과기정통부 손승현 정보보호네트워크정책관은 “정보통신기술(ICT)이 산업 전반에 적용되어 다양한 융합 서비스로 확산됨에 따라 일상 생활 속 사이버 안전의 중요성이 더욱 강조되고 있다.”라고 말하며,
  - “산업 분야별로 마련한 보안 가이드가 다양한 정보통신기술(ICT) 융합 제품과 서비스에 적용되어 국민과 기업에게 안전한 ICT 융합 환경을 조성하도록 관계 부처와 협력을 강화할 것이다.”라고 밝혔다.
- 국토부 정용식 항공정책관은 “드론산업의 다양한 육성정책이 논의됨에 따라 안전한 드론 활용산업 육성 및 공공서비스 질 제고를 위한 사이버 보안은 필수적이다.”라며,
  - “이번 가이드를 바탕으로 사이버보안 인증 기준이 마련될 경우, 기체 안전성 인증 등 드론 관련 인증제도와 함께 유기적으로 연계될 수 있도록 과기정통부와 협력을 지속해 나갈 것”이라고 밝혔다.

- 동 가이드는 12월 2일부터 인터넷진흥원(www.kisa.or.kr), 항공안전기술원(www.kiast.or.kr) 홈페이지를 통해 누구나 무료로 내려 받아 볼 수 있다.

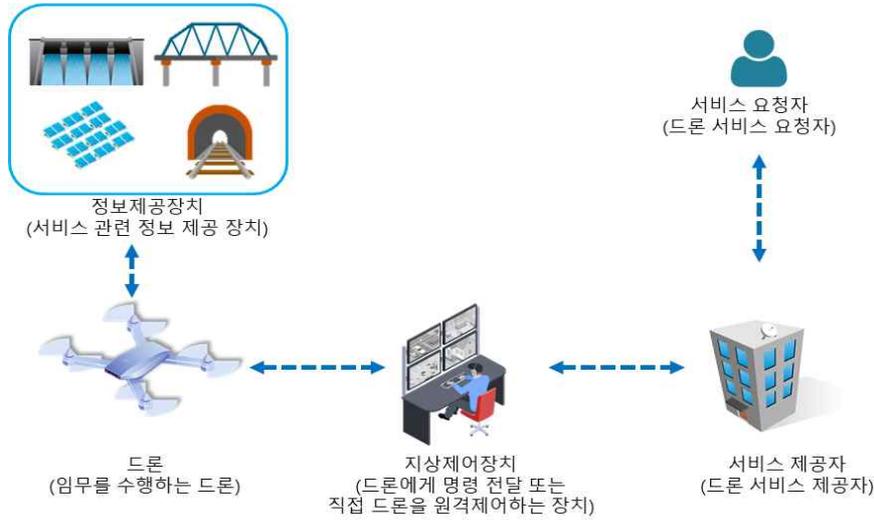
붙임 : 드론 사이버보안 가이드 주요내용



이 자료에 대하여 더욱 자세한 내용을 원하시면  
과기정통부 최보훈 사무관(☎ 044-202-6457), 국토부 첨단항공과 홍일산 사무관(☎ 044-201-4253), 인터넷진흥원 서영진 팀장(☎ 02-405-5195)에게 연락주시기 바랍니다.

- (드론 서비스 구성) 국내에서 운용하는 드론 기반의 대표적인 서비스를 분석하여 드론 서비스와 관련된 일반적인 구성요소 분류·분석

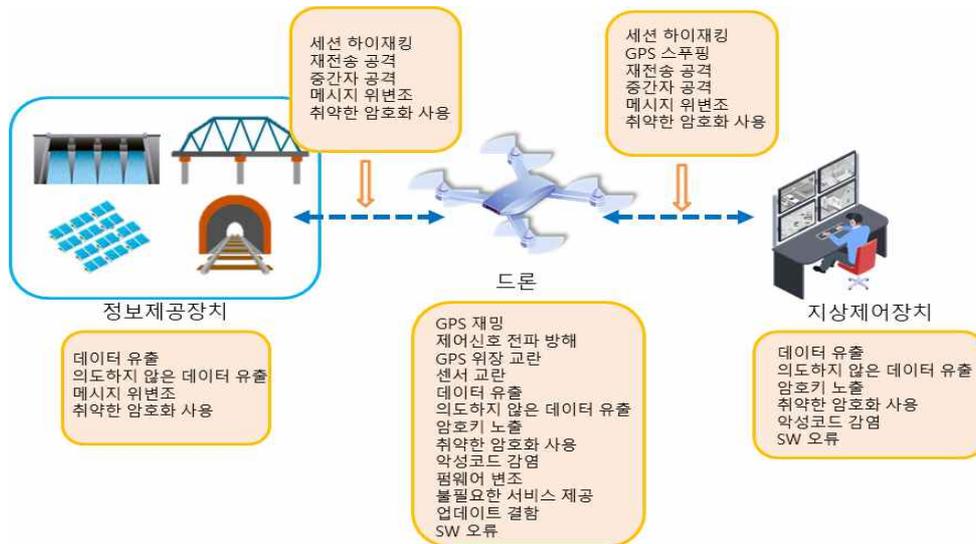
< 드론 서비스 구성도 >



- (보안위협 및 위협 시나리오) 드론 시스템에서 발생할 수 있는 주요 17가지 보안위협 및 6가지 위협 시나리오를 도출

※ 서비스 제공자 및 서비스 요청자는 일반 ICT 보안위협과 동일하므로 동 가이드에 포함하지 않음

< 드론 시스템 주요 보안위협 >



□ (보안 대응방안) 보안위협 및 위협 시나리오에 대한 **보안항목** 및 대응방안을 제시

보안항목	대응방안
HW 및 SW의 안전성	<p>(<b>안전한 업데이트</b>) 펌웨어 및 SW를 업데이트할 경우 안전하게 수행해야하며, 보안기능이 적용된 운영체제를 선택해야함</p> <p>(<b>변조 대응</b>) 펌웨어, 업데이트 소스 및 패치 관리 기능에 대해 무결성을 보장해야함</p> <p>(<b>악성코드 대응</b>) 악의적인 메시지 및 행위를 탐지 및 차단해야함</p> <p>(<b>안전한 3rd Party 라이브러리</b>) 설치된 3rd Party 코드는 사전에 검토되어야함</p> <p>(<b>시큐어코딩</b>) SW 개발 생명주기를 고려하여 구현되어야함</p>
인증	<p>(<b>드론 식별</b>) 드론의 고유 식별번호를 보유해야함</p> <p>(<b>사용자 인증</b>) 민감 정보에 접근할 경우 사용자인증을 수행해야 함</p> <p>(<b>상호 인증</b>) 중요정보 전송 및 서비스 접근 시 상호 인증을 선행해야함</p>
안전한 통신	<p>(<b>무선신호 보호 기능</b>) 무선신호에 Nounce와 시간 정보 등을 함께 전송하여 통신 보호 기능을 적용해야함</p> <p>(<b>통신 채널 확보/재밍 대응</b>) 방해 재밍 신호를 탐지하고 우회 통신 채널 등을 확보해야함</p> <p>(<b>전송 데이터 보호</b>) 중요정보가 전송될 경우 국제표준 암호 알고리즘을 통해 데이터 암호화하여 전송해야함</p> <p>(<b>메시지 감지</b>) 비정상 메시지를 감지하고 대응해야함</p>
안전한 비행	<p>(<b>자율비행</b>) 정상적인 명령에 따른 임무 수행 기능이 수행되어야함</p> <p>(<b>위치추적 대체수단 제공</b>) GPS 위성 접근이 어려울 경우 대체 절차가 구현되어야 하며, 드론 긴급 추락에 대비해야함</p> <p>(<b>특정지역 접근 방지</b>) 비행 금지구역 및 접근불가 지역 등의 접근방지 기능이 필요함</p> <p>(<b>자동충돌 회피</b>) 장애물 등의 위험요소를 탐지하고 충돌 회피 및 자동 착륙 기능을 적용해야함</p> <p>(<b>자동 회귀</b>) 제어통제권 상실 시 지정된 지점의 자동회귀 기능이 필요함</p>
암호	<p>(<b>안전한 암호키 관리</b>) 안전성이 검증된 방법으로 암호키를 생성해야하며, 노출되지 않게 안전하게 저장해야함</p> <p>(<b>안전한 암호 알고리즘 사용</b>) 통신 구간에 적합한 암호 알고리즘을 사용해야함</p> <p>(<b>안전한 난수 생성</b>) 안전한 암호키 생성 및 보호를 위한 안전한 난수 생성기를 사용해야함</p> <p>(<b>안전한 암호모듈 사용</b>) 안전성이 검증된 암호모듈을 사용해야함</p>
중요 데이터 보호	<p>(<b>저장 데이터 보호</b>) 데이터의 기밀성과 무결성을 보장해야함</p> <p>(<b>운영 데이터 보호</b>) 드론의 경로 이탈 방지 등을 위해 내비게이션 데이터베이스의 무결성을 보장해야함</p> <p>(<b>접근통제</b>) 저장 데이터의 접근권한에 대한 인증이 이뤄져야함</p> <p>(<b>개인정보 보호</b>) 개인정보 수집, 이용 등의 개인정보는 국내 법령 및 지침에 따라 처리되어야함</p>
보안감사	<p>(<b>감사기록</b>) 감사기록 생성 기능이 구현되어야함</p> <p>(<b>모니터링</b>) 드론 시스템 모니터링을 통해 비이상적인 행동을 탐지해야함</p>