Headline

우주산업 발달에 따른 보안 위협 대응 방안

OT/ICS 컨설팅팀 김현주 팀장

■ 개요

2001년, 미국의 억만장자 기업가 데니스 티토는 국제우주정거장(ISS, International Space Station) 여행에 2억 달러(약 2,800억 원)를 지급하며 세계 최초로 자비 우주 여행을 한 인물이 됐다. 이를 시작으로, 아마존 창업자 제프 베이조스, SpaceX CEO 일론 머스크, 일본의 억만장자 기업가 마에자와 유사쿠 등이 막대한 돈을 내고 우주를 경험했다.

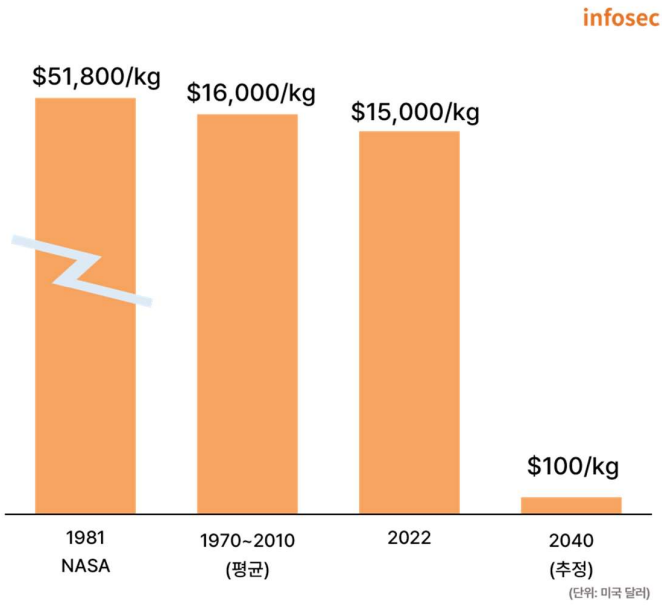
지금은 45만 달러(약 6억 원)만 있으면 누구나 우주관광을 할 수 있다. 러시아의 소유스(Союз) 우주선을 타고 달 궤도까지 돌고 오는 여행은 1억 달러(약 1,400억 원)면 가능하다. 세계 각국에서 민간이 우주여행을 주도하는 '뉴 스페이스' 시대가 본격적으로 시작된 것이다.

보안의 범위도 우주로 확장되고 있다. 이에 따라, '뉴 스페이스' 시대의 보안 동향과 우주 보안 위협 및 대응 방안에 관해 이야기해 보고자 한다.

■ 우주 산업의 성장

과거 우주산업은 국가 차원에서만 가능하다는 인식이 지배적이었다. 천문학적인 비용이 들어가기 때문에 민간 기업에서는 손댈 엄두조차 못 냈다. 하지만, 최근 저비용 발사체 및 위성 제조 기술이 발달하고, 우주 산업에 막대한 자본을 쏟아부을 수 있는 SpaceX, 블루오리진, 버진 갤럭틱 등 민간 기업이 등장했다. 이후 우주 산업은 고속 성장하기 시작했다.

세계 우주 산업 규모는 2016년 3,391억 달러(약 475조 원)에서 2021년 3,860억 달러(약 540조 원)로 성장했고, 2040년에는 1조 달러(약 1,400조 원)에 이를 전망이다. 이처럼 우주 산업이 팽창하는 이유 중 가장 두드러진 요인은 위성을 우주로 보내는 데 소요되는 비용이 급격히 감소했는 것이다. 재사용 로켓과 함께 민간 기업이 등장하며 발사 비용이 2022년에는 과거 대비 30배 이상 저렴한 kg당 1,500달러(약 210만 원)로 감소했으며, 2040년에는 kg당 100달러(약 14만 원)까지 감소할 전망이다.



* 출처 :씨티그룹(2022.05)"space the dawn of the new age"

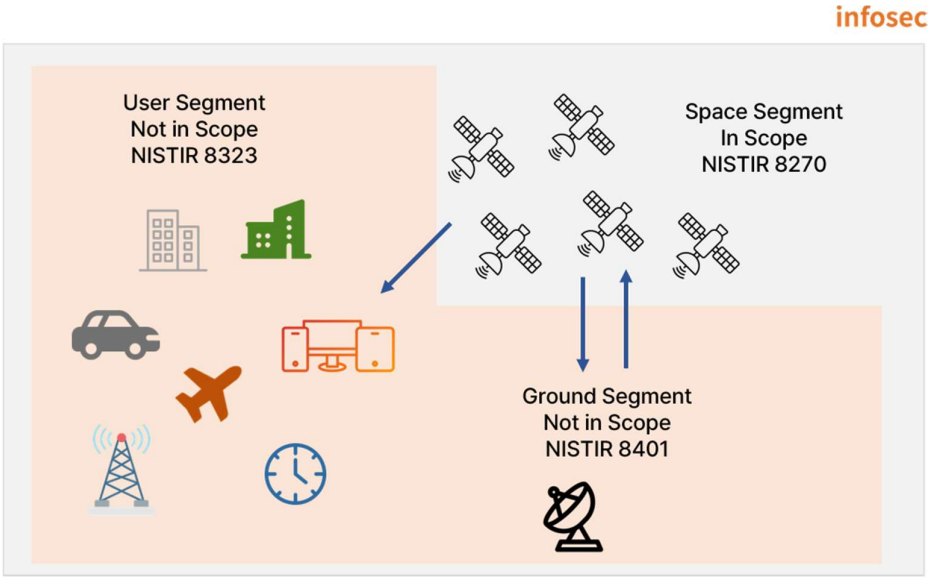
그림1. 우주 발사체 발사 비용 추이

우주 산업 최강국이라 불리는 미국은 우주 내 서비스, 조립 및 생산에 대한 국가 전략을 마련하여 글로벌 우주 시장의 주도권을 지속 확보하고자 노력하고 있다. 일본 역시 우주 산업 전략 기금을 운용하며 우주 관련 스타트업 육성에 적극 투자하고 있다. 스페이스X 등 글로벌 우주 기업들은 저궤도 소형위성 기반의 글로벌 위성 통신망을 구축하여 다양한 서비스를 준비하는 등 우주 서비스 주도 경쟁 역시 심화하고 있다.

국내에서도 글로벌 흐름에 발맞춰 정부 차원의 민간 주도 우주산업 생태계 조성을 위한 지원 강화 계획을 마련, 민간 우주기업 생태계 조성을 위해 노력하고 있다. 정부는 민관 협업 시장 스케일업 및 대체 불가 원천기술 확보를 위해 우주항공을 12대 국가전략 기술 중 하나로 선정했다. 2023년, 우주 예산을 8,392억 원으로 배정, 2027년까지 1조 5,000억 원으로 확대하고, 우주전문인력 양성을 위해 다양한 프로그램을 운영할 계획이다.

■ 우주 구성요소

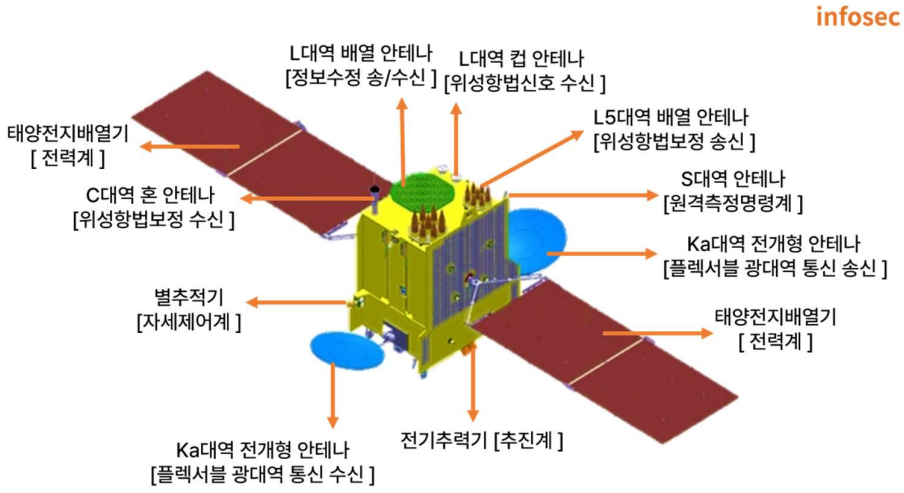
미국 국립표준기술연구소(NIST, National Institute of Standards and Technology) 기관 간 보고서 NIST IR(Interagency Report) 8270(상업용 위성 운영을 위한 사이버 보안, Introduction to Cybersecurity for Commercial Satellite Operations)에서는 우주 운영 아키텍처를 우주 영역, 지상국 영역, 사용자 영역으로 나누고 있다.



* 출처 : 미국 국립표준기술연구소 기관 간 보고서 NIST IR 8270

그림2. 우주 영역

우주 영역(Space Segment)은 우주선이나 위성 등이 위치하는 우주 공간, 지상국 영역(Ground Segment)은 위성을 운영 및 제어하는 영역이다. 사용자 영역(User Segment)은 스마트선박, 비행기, 자율자동차, 버스 등 위성을 활용하는 서비스 영역이다.



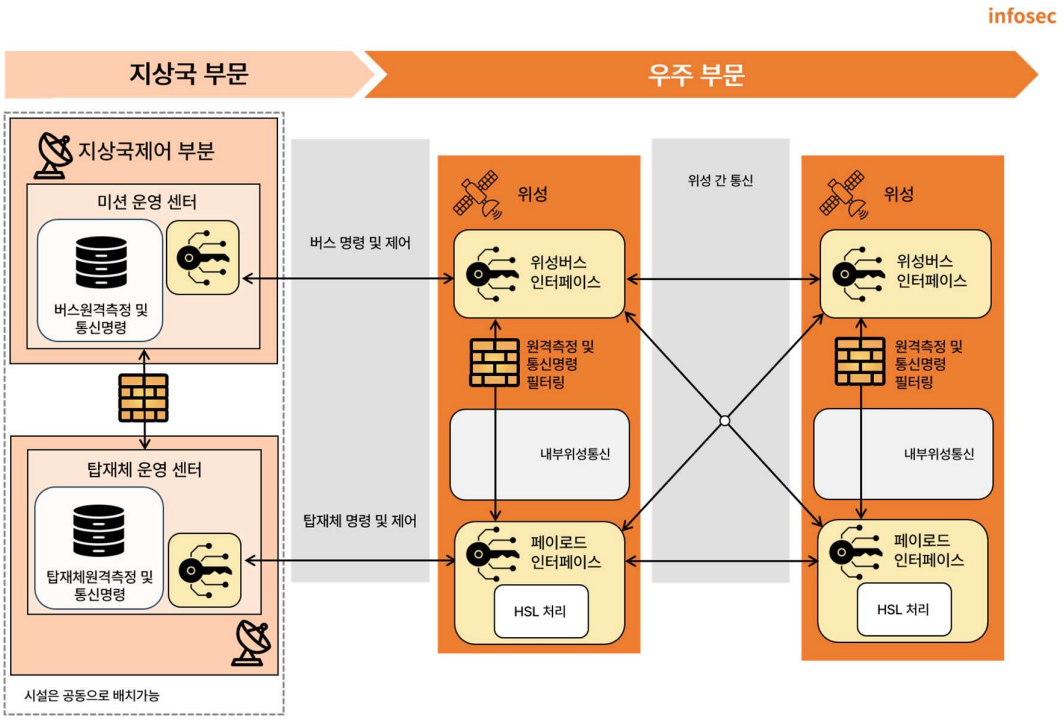
* 출처 :천리안 3호 위성체 형상도 [과학기술정보통신부]

그림3. 위성체 형상도

우주 영역인 위성은 위성을 구동하는 버스(Bus)와 통신, 관측, 탐사 등의 임무를 수행하는 탑재체(Payload)로 구성되어 있다. 위성은 기능에 따라 통신위성, 기상위성, 해양관측위성, 방송위성 등으로 나눠지고, 위성서비스를 담당하는 것이 탑재체, 탑재체를 탑재하고 기능을 수행할 수 있도록 하는 것은 버스다.

2027년 발사 예정인 재난/안전 대응 공공 통신위성 천리안3호의 경우 위 그림과 같이 여러 개의 안테나 및 서브시스템으로 구성되어 있다. 그림에서 보는 바와 같이 위성 본체인 버스는 여러 가지 서브 시스템으로 구성되어 있다. 뼈대가 되는 구조계, 전력원을 공급하는 전력계, 자세와 궤도를 제어하여 이탈하지 않도록 하는 자세제어계, 연료와 추력기 등 추진계, 지상국과 명령을 주고받는 원격측정 및 명령계, 위성을 적정 온도로 관리하는 열제어계 등이 있다. 탑재체(Payload) 구성에 따라 위성 종류(통신위성, 관측위성, 방송위성 등)가 결정되며, 구조 및 형상이 달라질 수 있다.

지상국은 미션운영센터와 탑재체 운영센터로 구성되어 있다. 미션운영센터는 위성에 명령을 내리고 원격 측정을 수신하는 역할을 한다. 탑재체 운영센터는 위성의 탑재체와 통신하여 위성서비스를 한다. NIST IR 8270(상업용 위성 운영을 위한 사이버 보안)에서는 지상국과 위성의 통신 링크를 포괄적으로 설명하고 있다.



* 출처 :NIST IR 8270(Introduction to Cybersecurity for Commercial Satellite Operations)

그림4. 우주 및 지상국 영역 아키텍처

우주 영역에서는 위성과 위성 간 레이저 통신을 하고, 지상국과 위성 간에는 커다란 안테나를 통해 전파를 주고받으며 통신한다. 지상국의 미션운영센터에서 버스에 원격 명령을 통해 위성을 운영 및 제어하며, 탑재체 운영센터에서 위성 탑재체 데이터를 수신 및 처리한다. 지상국 영역과 위성 간 통신은 목적 및 용도에 따라 주파수를 선택하여 사용하고 있다. 위성 통신에는 L밴드(1~2 GHz), S밴드(2~4 GHz), C밴드(4~8 GHz), X밴드(8~12 GHz), Ku밴드(12~18 GHz), Ka밴드(26~40 GHz) 등이 사용된다.

■ 우주 보안사고 사례

2022년 2월, 러시아가 우크라이나 침공 직전에 위성 인터넷 네트워크를 공격해 수만 대의 비아샛(Viasat) 모뎀을 무력화시킴으로써 우크라이나 군의 지휘와 명령 체계에 혼란을 준 것이 대표적인 우주 보안사고 사례다. 현재 우주산업이 고속 성장하고 있고, 위성 활용 서비스가 증가하며 우주 관련 보안사고는 증가할 것으로 예상한다.

발생 연도	우주 보안사고 사례	보안사고 영향
2008	NASA Terra 위성에 대한 재밍 공격으로 위성 제어 불능	위성 제어 불가
2014	미국 해양대기청(NOAA)의 기상관측 위성 네트워크에 인터넷 사이버 공격	위성 데이터 수신 불가
2015	실제 시판 안테나 등에서 이리듐 통신위성의 페이저 통신 데이터를 해석, 해독하고, 클리어 텍스트 정보(평문)로 변환 가능하다고 발표(국제회의 Chaos Communication Camp 2015)	통신 내용 노출
2018	직원이 무허가 설치한 Raspberry Pi 를 이용하여 나사(NASA) 제트추진연구소(JPL)의 네트워크에 불법 침투, 23 개 파일, 50MB 데이터 유출	미션 데이터 유출
2020	정지궤도 통신위성에 대해, 시판하는 안테나를 이용한 전파분석으로 통신 내용이 암호화되지 않음을 시연(국제회의 블랙햇(BlackHat)) - 위험물에 관한 정보, 풍력발전소의 관리자 권한 정보, 개인정보(여권 번호, 신용카드 데이터 등) 평문 확인	통신 도청
2022	Viasat 사의 통신위성 "KA-SAT" 서비스를 이용하는 특정 통신모뎀이 와이퍼(wiper) 악성코드 감염으로 위성 접속 불가	위성 접속 불가
2022	칠레에 있는 알마망원경의 계산기 시스템이 사이버공격을 받아 과학 관측과 칠레의 합동 알마 관측소 웹사이트 정지	위성 관측 불가

* 출처 :일본 '민간 우주시스템의 사이버 보안대책 가이드라인'

표1. 우주 보안사고 사례

■ 우주 보안위협

위성은 학문, 군사, 비즈니스 등의 목적으로 사용되고, 선박, 자동차, 비행기, 기업, 가정집 등 여러 사용자에게 광범위하고 다양한 서비스를 제공한다. 이를 위해, 위성에 탑재된 제어 소프트웨어, 위성과 지상국 간 통신 링크, 지상국 네트워크 및 시스템 등 모든 우주 관련 구성 요소들이 해커에게는 매우 매력적인 공격 목표가 될 수 있다.

IT(Information Technology)/OT(Operational Technology) 관점에서 위성과 지상국의 구성요소들은 보안 취약점이 내포된 시스템으로 구성되어 있고, 암호화되지 않은 상태로 전송되는 경우가 많아 다양한 IT/OT 보안 위협에 노출되어 있다. 우주 시스템을 공격하는 해커의 동기도 IT/OT 시스템을 공격할 때 의도(금전적, 사회적, 정치적)와 다르지 않다. 2023년 6월, 미국 공군에서 시험용 위성을 발사한 뒤 '위성 해킹 대회'를 개최한 바 있는데, 이는 우주항공 분야의 보안 수준이 미흡하다고 봤기 때문이다. 우주항공 분야는 위성통신 네트워크, 지상국 제어 인프라, 항법 시스템 등 정보통신망 의존도가 매우 높아 해킹에 취약하다고 판단된다.

NIST IR 8270(상업용 위성 운영을 위한 사이버 보안)에서는 우주 사이버보안 잠재적 위협을 여덟 가지로 분류하고 있다. 위성과 지상국 간 통신 링크의 재밍, 스푸핑, 하이재킹 등의 보안 위협이나 위성 제어에 영향을 줄 수 있는 시스템 손상, 서비스 거부 공격, 악성코드 삽입 등의 보안위협을 제시하고 있다.

A. 센서 데이터의 의도적인 재밍 및 스푸핑
B. 센서 데이터 가로채기 및 도청
C. 센서 시스템의 고의적 손상
D. 센터에 대한 서비스 거부 공격
E. 의도적인 재밍 및 가이던스 제어 스푸핑
F. 가이던스 제어에 대한 하이재킹 및 무단 명령
G. 악성코드 삽입
H. 가이던스에 대한 서비스 거부 공격

또한, 일본 '민간 우주시스템의 사이버 보안대책 가이드라인('23.03)'에서는 우주 시스템에 심각한 피해를 미칠 수 있는 위험 시나리오 7가지 사례를 제시했다.

순서	우주 위험 시나리오(사례)	
1	표적형 메일 공격을 통한 위성 궤도 제어의 상실	① 직원 단말이 메일을 통해 멀웨어에 감염 ② 해커가 인터넷을 경유하여 부정 접속 ③ 업링크 데이터를 탈취하여 자세 제어 정보와 미션 기기제어 정보 등을 조작하여 위성에 보냄 ④ 일시적 위성 제어 상실
2	개발제조용 단말의 멀웨어 감염으로 인한 위성·미션 기기 제어의 상실	① 메일을 통해 위성 본체 소프트웨어 업데이트에 사용되는 개발/제조용 단말이 멀웨어에 감염 ② 해커가 인터넷을 경유하여 부정 접속(멀웨어에 감염된 업데이트 프로그램에 백도우가 삽입됨) ③ 업데이트 프로그램의 백도우를 사용하여 지상국(위성 운용 설비)에서 위성으로 원격 조작 ④ 위성의 제어 불능
3	위성 데이터 이용설비 사이버공격을 통한 위성 제어의 상실	① 지상국(위성데이터 이용 설비)에 무허가 단말 설치 ② 해커가 인터넷을 경유하여 부정 접속 ③ 미분리된 네트워크망을 오가며 다수 서버에 부정 접속 ④ 지상국(위성 운용 설비)의 각종 서버 다운, 위성 제어 상실
4	관측 접수 서버 부정 접속을 통한 서비스 제공 불능	① 관측 접수 서버에 해커가 인터넷을 경유하여 부정 접속, 랜섬웨어 감염 ② 클라우드로 구축된 지상국(위성데이터 이용 설비)의 보안 설정 미흡으로 지상국(위성데이터 이용 설비)내 모든 서버 및 단말이 랜섬웨어에 감염 ③ 위성데이터 제공 서버 등의 시스템 데이터(부팅 파일 등)가 삭제되어 리부팅 불가, 서비스 제공 불가
5	원격근무 환경에서 메일 공격을 통한 기업 기밀 유출	① 원격업무 중 동료로 가장한 메일에 의해 멀웨어 감염 ② 해커가 인터넷을 경유하여 부정 접속 ③ 위성 제조 기업 기밀정보 유출
6	무허가 USB 메모리 이용으로 인한 조업 정지	① 해커가 멀웨어에 감염된 USB 제작, 컨트롤러의 설정용 USB 인 것처럼 속여 제조설비 담당자에게 전달 ② 제조설비 담당자가 컨트롤러 설정 변경 시 해커가 제공한 USB 를 사용하여 멀웨어에 감염 ③ 컨트롤러의 설정 및 제조 프로그램이 변조되어 설비 제어 이상 및 제조 업무 정지
7	불법적인 위성 탑재 기기의 도입으로 인한 군집 위성의 붕괴 위기	① 해커가 자세궤도 제어 컨트롤러에 사용되는 기판에 논리폭탄을 설치, 수십 대 규모의 군집위성을 계획 중인 위성 개발 사업자에게 저렴하게 제공 ② 제조 담당자의 인수 검사 및 시스템 검사를 통과하고 양산 위성에 탑재 ③ 발사 후 특정 조건이 성립되어 논리폭탄이 실행 ④ 위성 제어 불능, 군집위성 붕괴 위기 직면

표2. 우주 위험 시나리오 사례

위성은 스마트선박, 자율자동차, 도심항공모빌리티(UAM, Urban Airport Mobility), 스마트폰 등 다양한 분야에서 서비스를 제공하고 있다. 다만, 항법위성(GNSS, Global Navigation Satellite System)이 중단되거나 항법위성에서 제공하는 위치정보가 조작된다면 사회적으로 많은 혼란을 초래할 수 있다. 스마트선박이 항로를 이탈하거나 도심항공모빌리티가 주행 오류로 추락하는 등의 사례가 발생할 수 있다. 따라서, 우주 관련 보안위협을 더욱 면밀히 분석하고 보안 대책을 수립하는 것이 매우 중요하다.

■ 우주 보안 동향

우주 보안 위협에 대한 인식이 높아지며 각국에서는 우주 사이버보안에 대한 관심까지 고조되고 있다. 2020년 트럼프 행정부에서 우주 정책지침(SPD)-5를 통해 우주 사이버보안에 대한 원칙과 가이드라인을 준수할 것을 천명한 바 있다. 또한, 위성 등 우주 시스템이 사회경제 전반에 걸쳐 필수 서비스를 제공한다는 점을 고려해 우주를 17번째 기반 시설로 지정해야 한다는 논의가 수년째 이어지고 있다. 일본에서는 우주 시스템 보안 가이드라인을 발표하고 본격적인 사이버보안 강화 사업들을 전개하고 있다. 국내에서도 민간 항공우주 산업 보안 수준 제고를 위한 정보보호산업의 글로벌 경쟁력 확보 전략을 발표('23.9, 과기정통부)하고 우주 자산 사이버보안협의체를 출범했다. 이에 따라, 국정원, 국방부, 우주항공청 등과 위성 사이버 위협 통합 대응 로드맵 마련을 추진 중이다.

다음은 글로벌 주요국들의 우주 및 우주 보안 관련 정책 및 전략이다.

국가	주요 내용	
미국	정책 및 가이드라인	· 국가안보전략(17.12) · 국가사이버전략(18.9) · 우주 우선순위 프레임워크(21.12) · 하이브리드 위성 네트워크를 위한 사이버안보 프레임워크_NIST IR 8441(23.6)
	법·제도	· 우주정책지침(SPD 1~7) · 미 하원, 우주인프라 법안 발의(21.6) - 국토안보부에 의해 핵심 인프라로 분류된 16개 부문에 우주시스템 추가 추진 · 미 상원, 상업용 위성 사이버보안에 관한 법안 재발의(23.5) - CISA가 상업 위성 사업자를 보호하는 것을 의무화 - 국가사이버국장과 우주위원회가 위성 시스템의 사이버보안과 관련하여 연방정부 전반에 걸친 조정을 강화하기 위한 전략을 개발하도록 요구
유럽연합(EU)	정책 및 가이드라인	· 안보와 방위를 위한 EU 우주 전략(23.3) · 저궤도 위성통신(LEO SATCOM)에 대한 사이버보안 평가 보고서(24.2)
	법·제도	· EU 우주법(추진 예정)
일본	정책 및 가이드라인	· 2023 우주정책 기본계획(23.6, 개정) · 민간 우주시스템 사이버보안 대책 가이드라인(23.3)
	법·제도	· 우주 기본법(08)
독일	정책 및 가이드라인	· 국가 우주전략(23.9, 개정)
	기술개발/인프라	· 우주 인프라를 위한 IT 기본 보호 프로필(22.7)
	법·제도	· 우주기관설립법(98) · 원격탐사법(07) · 국가우주법(마련중)
중국	정책 및 가이드라인	· 과학기술혁신 2030 계획, '우주-지상 통합 정보 네트워크' 구축 사업 · 2021 우주백서 발간(5년 주기)
	기술개발/인프라	· 제로트러스트 시스템 기술 사양 발표(21)

* 출처 :한국인터넷진흥원 '주요국 우주(Space) 사이버 시큐리티 정책 동향 조사·분석'

표3. 우주 및 우주 보안 글로벌 정책 및 전략

■ 우주 보안 대응방안

위성은 지상과 멀리 떨어진 우주에 위치하기 때문에 과거에는 안전한 것으로 여겨져 왔다. 하지만, 앞서 우주 보안사고 사례 및 보안위협에 관해 설명한 것처럼 위성은 더 이상 안전지대가 아니다. 우주 보안 강화를 위해 우주 제품의 개발/제조 단계, 운영 단계, 폐기 단계에 이르는 우주 시스템 라이프사이클에서 사이버보안을 내재화하고 적용하는 것이 필요하다. 이를 위해 다음과 같은 보안 대책이 요구된다.

1) 우주 제품 개발 보안 및 공급망 보안

우주 제품에 탑재되는 소프트웨어의 설계/개발 단계에서 보안을 고려하고, 부품의 제조 단계부터 보안 내재화를 하는 것이 최우선이다. 위성에 탑재되는 소프트웨어와 위성서비스를 위해 개발되는 애플리케이션은 설계/개발 단계에서 보안 요구사항을 정의하고 시큐어코딩을 적용해서 개발해야 한다. 또한, 오픈소스 취약점을 확인하는 등 공급망 보안 취약점 점검을 수행하고 테스트 단계에서 보안 적용 여부를 검토하는 보안성 검토 프로세스를 준수해야 한다.

2) 영역별 위험 분석 및 보안기술 적용

우주 영역(위성), 지상국 영역(위성 제어 설비, 탑재체 데이터 운영 설비), 위성 활용 서비스 영역(스마트선박, 자율주행차, 도심항공모빌리티 등)에서 발생할 수 있는 위험을 식별하고 대응하기 위한 보안 기술을 적용해야 한다.

A. 위성 : 탑재 소프트웨어 및 장치에 대한 보안성 검증, 취약점 조치

B. 위성과 지상국 간 통신 구간 : 통신 구간 터널링, 전송되는 데이터 암호화, 데이터 변조 대응을 위한 메시지 인증, 안티재밍 기술(주파수 호핑 등) 등 적용

C. 지상국 영역(위성 제어 설비, 탑재체 데이터 운영 설비) : 비인가자에 대한 네트워크 보안(침입 차단, 침입 방지, 네트워크 접근제어 등), 위성 제어 및 탑재체 데이터 보안(데이터 암호화, 정보 유출 방지), 인증 및 권한 제어(멀티 인증, 계정관리), 악성코드 대응(백신, 이상징후 탐지), 물리적 접근 제어(안테나, 중요 설비 출입 통제, 모니터링 등)

D. 위성활용서비스 영역 : 서비스별 위험을 식별하고 관리하기 위한 대책 마련

■ 맺음말

위와 같은 우주 보안 대책을 적용하기 위해서는 국가 차원의 우주 사이버 보안 가이드라인을 제정할 필요가 있다. 우주 관련 기업을 선도하고, 가속화되는 우주산업의 보안 적용을 위해 정부, 기업 모두가 끊임없는 관심을 가지는 것이 필요하다.

이와 같은 흐름에 따라, SK쉴더스는 우주산업 보안에 적합한 사이버 보안 서비스 및 컨설팅을 제공하고 있다.

지상국 운영 기업은 보안 강화를 위한 보안컨설팅, 진단/모의해킹, SI사업(암호화 솔루션, 네트워크 보안, 인증/접근제어 시스템 등), 물리보안 서비스를 제공받을 수 있다. 위성서비스 제공 애플리케이션은 주로 웹으로 구현하는 경우가 많아 소스코드 진단, 모의해킹, 공급망보안 진단(오픈소스 점검 등) 등이 필요하다.

위성은 일단 쏘아 올리면 S/W 업데이트 및 수정이 어렵기 때문에 발사하기 전 IoT보안 진단과 같이 위성에 탑재된 S/W에 대한 진단이 필요하고, 위성에 들어가는 부품을 제조하는 기업의 경우 OT/ICS보안 컨설팅 및 보안 솔루션 서비스를 제공받으면 더 안전한 관리가 가능하다.

자세한 내용은 SK쉴더스 홈페이지나 문의하기를 통해 확인할 수 있다.