방산안보연구
Journal of Defense Industrial Security

방산안보연구, 1권 1호, 2025년 3월, 71-86면.
Journal of Defense Industrial Security, Volume 1, Issue 1, March 2025, Pages 71-86.
https://doi.org/10.?????/jdis.2025.1.1.5

Print ISSN 3091-5546
Online ISSN 3091-5554

원저

국내 위성 사이버보안 가이드라인 발전 방안 연구

이용원[1], 손창근[2], 이규호[3]

[1]국방정보본부 전문군무경력관(가군)
[2]명지대학교 융합보안안보학과 겸임교수, 보안경영학박사
[3]LIG넥스원 사이버전자전개발단 수석연구원

교신저자: 이용원 (rongyuan007@naver.com)

요약

전세계는 우주 공간을 활용하여 우리의 일상에 필요한 정보를 제공하고 있으며, 국가안보를 위해서도 많은 우주시스템을 개발하여 운용있고, 우주시스템에 대한 침해가 발생된다면 우리의 모든 일상의 시스템이 비정상적으로 동작하여 큰 피해가 발생될 것이며, 이로 인해, 국가안보에 심각한 위협이 발생될 것이다. 최근 우리나라도 우주시스템에 대한 양적·질적 발전이 이루어지고 있는 상황에서 우리의 우주시스템을 보호하기 위한 가이드라인의 제정 및 적용이 시급한 상황이라고 할 수 있다. 따라서 본 논문에서는 해외 주요국가들의 우주시스템에 대한 사이버보안 가이드라인을 살펴보고 국내 위성 사이버보안 가이드라인의 수립을 위한 고려요소 및 목차구성(안) 등 정책적 발전 방향을 제시하고자 한다.

핵심어

우주안보, 위성보안, 위성사이버보안, 위성사이버보안 가이드라인

차례

1. 서론
2. 위성 사이버보안 배경 및 국내 활동
  2.1. 위성 사이버보안 배경
  2.2. 위성 사이버보안 국내 활동
3. 해외 위성 사이버보안 정책 사례 연구
  3.1. 美 NIST, 위성 사이버보안 관련지침
  3.2. 유럽, 저궤도 위성통신 사이버보안 평가
  3.3. 일본, 상업용 우주시스템 사이버보안 가이드라인
  3.4. 해외 위성 사이버보안 가이드라인 비교 연구 결과
4. 국내 위성 사이버보안 가이드라인 수립방향 제안
  4.1. 국내 위성 사이버보안 가이드라인 주요 고려 요소 도출
  4.2. 국내 위성 사이버보안 가이드라인 목차 구성 방안 제시
5. 결론

Open Access

접수일: 2024년 11월 14일
수정일: 2025년 03월 17일
게재승인일: 2025년 03월 17일
출판일: 2025년 03월 31일

Original Article

Study to develop Domestic Satellite Cybersecurity Guidelines

Yongwon Lee[1], Chang Gun Son[2], Kyuho Lee[3]

[1]Korea Defence Intelligence Agency, Specialist(A), Republic of Korea
[2]Adjunct Professor, Department of Convergence Security, Myongji University; Ph.D. in Security Management Engineering, Republic of Korea
[3]LIG Nex1 Corp, Cyber Electronic Warfare Center, Chief Research Engineer, Republic of Korea

Corresponding Author: Yongwon Lee (rongyuan007@naver.com)

ABSTRACT

The world utilizes outer space to provide information necessary for our daily lives, and many space systems have been developed and operated for national security. Any infringement on these space systems will cause a lot of damage due to abnormal behavior of all systems in our daily lives, and a very serious situation will occur in terms of national security. Korea is also making quantitative and qualitative advances in space systems, so it is urgent to establish and apply guidelines to protect our space systems. Therefore, this paper examines the cybersecurity guidelines for space systems of major foreign countries and suggests policy development directions such as consideration factors and table of contents for the establishment of domestic satellite cybersecurity guidelines.

KEYWORDS

Space Security, Space(Satellite) Cybersecurity, Space(Satellite) Cybersecurity Framework

1. 서론

사이버안보는 북한 등 위협행위자들이 자행하는 국가안보와 국익에 반하는 사이버 활동을 확인·견제·차단하고, 그에 필요한 대응 조치를 강구·이행함으로써 국가와 국민의 안전 그리고 국익을 보호하는 것을 말한다.[1]

최근 전 세계 거의 모든 국가들이 우주를 안보영역으로 확대, 포함하여 우주의 영역이 세계안보와 국가별 안보에 있어서 매우 중요한 대상으로 판단하고 지구관측, 통신 및 네트워크 유지, 항법 등 우주를 활용한 다양한 자산들을 개발 및 운용하고 있다.

이러한 상황에서 각 국가들은 사이버안보 및 사이버보안의 개념속에서 우주를 활용한 각종 자산들을 개발 및 운용하기 위한 기술과 자산에 대한 보호의 중요성을 생각하게 되었으며, 운용, 폐기 등 전체 수명주기에 걸쳐서 위협에 대응 및 보호하기 위한 방법을 강구하게 되었다.

우리나라에서도 2024년에 들어서 국가정보원 등을 중심으로 '위성사이버보안'의 중요성과 그에 대한 필요성을 인식하고 국가 전체의 관계기관들과 함께 위성 사이버보안 강화를 위한 협의체 구성 및 위성 사이버보안 가이드라인 제정 등의 활동을 적극적으로 시작하고 있다.[2]

이에 본 논문은 국내 위성 사이버보안 가이드라인 정책 발전 방안을 제시하고자 한다. 논문의 구성은 2장에서는 위성 사이버보안의 주요 침해 사례와 국내 활동을 분석하여 문제 제기를 통해 연구 방법론에 대해 서술하였으며, 3장에서 우리나라보다 우주 사이버보안을 먼저 시작한 선진국의 사례를 통해 우주와 위성에 대한 사이버보안 제도와 규정에 대한 방향을 분석한다. 또한 미국과 유럽, 일본 3개 국가에 대한 가이드라인 비교 분석을 통해 4장에서 우리나라의 위성 개발 및 운용 특성과 현실에 맞는 '국내 위성 사이버보안 가이드라인'의 주요 구성요소와 목차구성(안)을 제안한다.

2. 위성 사이버보안 배경 및 국내 활동

2.1. 위성 사이버보안 배경

2.1.1. 위성 사이버보안 정의

우주 사이버보안은 우주 자산의 기밀성, 무결성, 가용성을 보장하기 위해 사이버 위협으로부터 우주 운영을 보호하는 기술적 및 관리적 대책을 의미한다. 이는 위성체계의 주요 구성요소인 위성체, 지상체, 그리고 위성으로부터 수집된 데이터를 활용하는 사용자를 포함한다.

호주 스마트샛 CRC 2022에 의하면 위성 사이버보안은 사이버 공격으로 인한 외부 간섭, 손상 또는 파괴 없이 지구 대기권 밖에 위성을 배치하고 운영할 수 있는 능력이라고 정의하고 있다.[3]

특히, 그림 1과 같이, "위성 사이버보안"이란 위성의 "개발(설계, 제작) → 발사/운용 → 임무종료/폐기" 등 생애 전(全) 주기(life cycle)에서의 사이버 위협으로부터 위성체계를 보호하기 위한 기술적, 관리적 제반 대책이라고 할 수 있다.

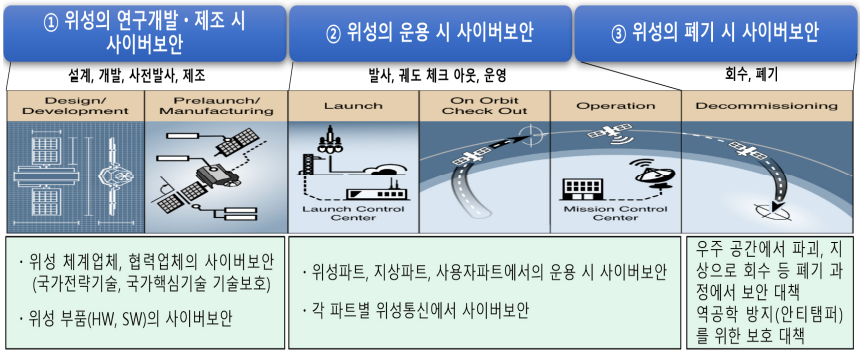

그림 1. 위성 생애주기(life cycle) 사이버보안

2.1.2. 위성 사이버보안 주요 침해 사례

최근 전세계적으로 위성 시스템의 개발과 운용이 활발한 가운데 위성 사이버보안 관련 주요 침해사례 중에서 주요한 몇가지를 아래에서 살펴보겠다.

2.1.2.1. 독일 ROSAT 위성 해킹

1998년 독일의 ROSAT 인공위성이 해커들에게 노출되어 위성 궤도가 임의로 변경된 사례가 있으며, 이로 인해 위성에 심각한 타격이 발생하였다.[4]

2.1.2.2. 美 공군연구소 'Hack-A-Sat' 대회에서 실제 운용중인 위성 해킹

2023년 8월 미국 공군 연구소가 개최한 해킹 대회에서 실제 지구 궤도를 도는 위성이 해킹되었으며, 이 사건으로 위성 보안의 취약성이 확인되어 우주항공 분야 사이버보안의 중요성이 강조되었다.[5]

2.1.2.3. 한국 국가위성운영센터 해킹

2024년 5월 출범한 우주항공청의 소속기관으로 편입된 제주 국가위성운영센터는 2022년 과학기술정보통신부와 국가정보원이 설립하여 다목적 실용위성 아리랑 3호와 3A호의 관제, 위성 영상 수신·관리 등을 맡고 있으며, 이 센터는 오는 2030년까지 다목적 실용위성과 차세대중형위성, 소형위성 등 저궤도위성 70기에 대한 운영을 담당하는 우주항공 분야 핵심 연구 시설이다.

이러한 국가위성운영센터가 2023년 12월 해킹 공격에 보안이 뚫린 것으로 확인되어 위성 관제권과 데이터 탈취 위험에 노출되었으며, 이 사건은 북한의 소행으로 추정되어 국가정보원이 조사를 실시했다.[6]

2.2. 위성 사이버보안 관련 국내 활동

2.2.1. 우주 사이버보안 관련 법제

우리나라의 우주 사이버보안 관련 법제는 국가정보원의 「우주안보 업무규정」과 우주항공청의 「우주개발사업 보안관리 규정」 그리고 「위성정보 보안관리 규정」이 있다.

하지만, 위성 사이버보안의 일차적 근거는 있으나, 위성의 "개발(설계, 제작) → 발사 및 운용 → 임무종료 및 폐기" 등 생애 전(全) 주기(life cycle)에서의 사이버 위협으로부터 위성체계를 보호하

기 위한 기술적, 관리적 제반 대책을 제시하고 적용할 수 있는 구체적인 법제 · 지침은 없는 상태이다.

2.2.2. 위성 사이버보안 거버넌스

우리나라의 위성 사이버보안 관련 거버넌스로는 2024년 6월 4일에 국가정보원의 국가사이버안보센터와 국가우주안보센터를 중심으로 국방부, 외교부, 우주항공청, 과학기술정보통신부 등 관계된 정부부처와 한국항공우주연구원, KAIST, 국가보안기술연구소 등 국책연구기관들이 참여하에 '위성 사이버보안 강화를 위한 관계기관 협의체'를 출범시켰다.[2]

이 협의체에서는 2024년 연말까지 '위성 임무 및 운영별 사이버 보안대책의 수립', '위성 사이버보안 가이드라인'을 제정하고, 우주 사이버위협에 대한 통합대응 방안이 담긴 중장기 로드맵도 마련할 계획이다.[2]

하지만, 우리나라 위성 사이버보안 거버넌스는 국가정보원, 국방과학연구소, 한국항공우주연구원, KAIST 등의 일부를 제외하고는 위성의 개발과 운용에 대한 지식과 경험이 부족하여, 위성 사이버보안의 실제 적용이 가능한 현실적인 정책적 방향을 연구하고 제시하는데 한계가 있다고 하겠다.

2.2.3. 국내 위성 사이버보안 가이드라인 제정 필요

앞에서 기술한 바와 같이 2024년 6월 4일에 국방부, 외교부, 우주항공청, 한국항공우주연구원, KAIST 등 20여개의 유관기관과 함께 '위성 사이버보안 강화를 위한 보안협의체'(이하, 협의체)를 발족하고, 위성의 '설계-운용-폐기' 등 생애 전(全) 단계를 보호하기 위한 위성 사이버보안 대책을 마련하기로 했다.

우리나라는 위성 개발 능력 자립화 및 핵심기술 확보를 중점적으로 추진해왔고, 우주개발진흥 기본계획 및 국방 우주력발전전략 등과 연계된 위성개발 계획에 맞춰 위성별 전용 보안시스템[1]을 개발하여 운용을 추진하고 있다.

협의체는 올해 안으로 위성임무 및 운영별 사이버 보안대책 수립, 위성 사이버보안 가이드라인 제정, 위성의 "개발(설계, 제작) → 발사/운용 → 임무종료/폐기" 등 생애 전(全) 주기(life cycle)에서의 사이버 위협으로부터 위성시스템을 보호하기 위한 기술적, 관리적 제반 대책으로 '위성 사이버보안 가이드라인'의 제정과 중장기 로드맵 수립이 필요하다.

2.2.4. 국내 위성 사이버보안 가이드라인 작성 및 고려요소 검토 필요

우리나라의 위성 개발과 운용 기술은 대부분 미국과 유럽에서 상당 부분 배워와서 현재 국내 위성 개발 및 운용 기술을 확보하게 된 것이다.

현재 국내에는 위성보안 가이드라인이 없는 상태이므로 국내 위성 사이버보안 가이드라인 작성을 위해 미국의 위성보안 관련 지침과 유럽의 '저고도 위성 사이버보안 평가', 일본의 '상업용 위성 사이버보안 가이드라인'의 포함요소를 살펴보고, 비교 분석하여 우리나라의 국내 위성 사이버보안 가이드라인 제정시 포함되어야 할 고려요소 및 목차의 도출이 필요하다.

1) 국방부훈령 제2935호(2024.6.11.)「국방보안업무훈령」별표#1.'용어의 정의'(제3조 관련)
보안시스템이란, 정보통신 수단으로 생산, 처리, 저장, 송 · 수신되는 정보를 유출, 변조, 훼손 등으로부터 보호하기 위한 암호장비, 보안자재, 암호논리 등을 말한다.

3. 해외 주요국가 위성 사이버보안 정책 사례 연구

한국인터넷진흥원(KISA)에서 발행한「해외 주요국가 위성 사이버보안 정책 동향 분석」에서 미국, 유럽연합(EU), 일본, 독일, 중국의 우주 공간 사이버 위협에 대응하기 위한 정책적 노력과 우주분야 사이버보안 전략의 통합적인 운영과 파트너십을 강조하는 등 정책 및 가이드라인을 소개하고 있다.[7]

미국은『국가안보전략('17.12)』,『국가사이버전략('18.9)』을 만들고,『우주 정책 지침(SPD)』 등의 법·제도를 수립하는 등 우주 자산과 우주시스템의 연결성 등 안전성이 우주 안보와 국방에서 중요한 우선순위임을 강조하고 있다.

유럽연합은『안보와 방위를 위한 EU 우주전략('17.12)』,『저궤도 위성통신에 대한 사이버보안 평가 보고서('24.2)』를 만들고,『EU 우주법』의 제정을 추진하고 있다.

일본은 우주활동의 자주성 확보와 우주 사이버 위협에 대한 대응을 주요한 국가 과제로 인식하고,『2023 우주정책 기본계획('23.6)』,『민간 우주시스템 사이버보안 대책 가이드라인('23.3)』을 만들었으며,『우주 기본법('08)』을 제정하는 등 우주 시스템과 관련된 보안상의 위험, 우주시스템 관련 이해관계자가 검토해야 할 기본적인 보안대책과 대책을 검토할 때 참고할 참고문헌과 기본적인 대책 등을 제시하고 있다.

본 장에서는 위에서 간략하게 언급한 미국, 유럽연합, 일본에 대한 우주분야 사이버보안에 대한 정책 및 가이드라인에 대해서 자세하게 알아보고 국가별 정책 방향을 비교 및 분석하겠다.

3.1. 美 NIST[2], 위성 사이버보안 관련지침

미국의 국립표준기술연구소(NIST)에서는 2021년 이후부터 위성 관련 사이버보안 관련 지침을 작성 및 배포하여 위성 개발과 운용에 대한 보안 지침을 제시하고 있다.

미국의 위성 관련 사이버보안 관련 지침은 상업용 위성 운영 분야, 위성 관제를 위한 위성의 지상시스템 분야와 하이브리드 위성 통신분야 및 항법 서비스 사용 등에 대해서 지침을 제공하고 있다.

각 사이버보안 관련 지침에서는 목적과 범위와 대상을 포함하고 해당 지침별 아키텍처를 도식화하여 제시하고 있으며, 미국의 위성 관련 사이버보안과 관련된 각각의 지침에 대해서는 아래에서 살펴보겠다.

3.1.1. NIST IR 8270 (상업용 위성 운영을 위한 사이버보안 소개)

NIST IR 8270 "상업용 위성 운영을 위한 사이버 보안"은 2023년 7월 제정되었으며[8], '섹션 1'에서는 상업용 우주기업에 대해 사이버보안 프레임워크(이하, CSF[3])를 소개하는 목적을 밝히고 있으며, 사이버보안 프레임워크를 적용하기 위한 특정한 방법에 대한 설명과 예상되는 위협을 기반으로 해서 목표로 하는 보안 결과에 대한 사이버보안 프레임워크의 예시 생성과 사이버보안 결과와 요구 사항 및 사이버보안 통제에 대한 추상적인 구조를 설명하고 있다.

'섹션 2'에서는 상업용 위성 운영에 대한 개념적이고 높은 수준의 아키텍처를 제시하고 있으며, '우주 공간 아키텍처 세그먼트'와 '위성 수명주기 단계별 아키텍처'로 구분하여 방향을 제시하고 있다. 그림 2에서와 같이 위성이 수행하는 감지(수집), 정보처리, 데이터 수집 및 통신의 운용단계와 설계 - 제작 - 발사 - 궤도운용 - 폐기 전(全)과정에 대한 사이버보안 아키텍처를 제시하고 있

2) NIST : National Institute of Standards and Technology, 국가표준기술연구소
3) CSF : Cybersecurity Framework, 사이버보안 프레임워크

다.

‘섹션 3’에서는 사이버보안 프레임워크(CSF)의 단계를 설명하고 있으며, ‘섹션 4’에서는 위성 관련 조직이 사이버보안 프레임워크 단계를 우주 비행체에 적용할 수 있는 방법에 대한 개념적인 예를 제공하고 있고, 이를 위해 사이버보안 프레임워크를 사용하여 프로파일을 개발하는 방향과 사례 연구 결과를 제시하고 있다.

표 1. 「NIST IR 8270」 목차구성

1. 소개
- 목적과 범위 - 보고서의 구조
2. 위성 운영의 개념적 고급 아키텍처
2.1 Space 아키텍처 세그먼트
- 공간 세그먼트 - 주요 고려 사항 및 커뮤니케이션
- 다른 Space Architecture 세그먼트
2.2 우주선 차량 수명 주기 단계
- 운영 단계 - 다른 단계
3. 사이버보안 프레임워크 소개
4. 우주 운영을 위한 사이버보안 프로그램 생성
4.1 사이버보안 프레임워크를 사용하여 프로파일 개발
4.2 사례 연구 예시 4.3 결론

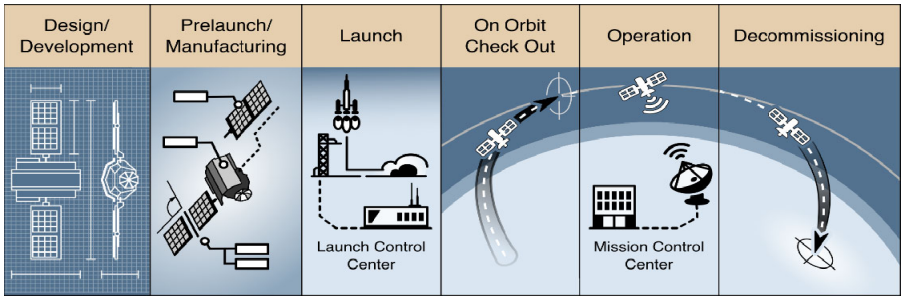

그림 2. 위성 수명주기 단계

3.1.2. NIST IR 8401 (위성 지상부문 적용 사이버보안 프레임워크)

NIST IR 8401 “위성의 지상 세그먼트 사이버보안”은 2022년 12월에 제정되어, 상업용 위성의 지상 부문의 운영 단계를 사이버보안 프레임워크에 따라 프로파일을 작성하여 상업용 위성의 지상 부문 운영자가 시스템에 사이버보안을 적용할 수 있도록 우주 관련 기업체에 사이버보안 프레임워크를 제시하고 있다.[9]

‘섹션 1’에서는 본 가이드라인의 제정 목적이 사이버보안 프레임워크를 적용하여 우주 지상 부문에 대한 프로파일을 생성하는 것이라고 밝히고 있다.

또한 이 문서의 범위는 상업용 우주 ‘지상 부문의 운영 단계’에서 사이버보안 프레임워크에 따라 프로파일을 개발하여, 상업용 우주 ‘지상 부문의 운영자’가 시스템에 사이버보안을 적용할 수 있도록 지원하는 것이다.

프로파일의 범위에는 쿼리, 명령, 제어 및 상태 또는 명령 및 제어를 위해 위성 본체 또는 탑재체와 상호 작용하는 모든 시스템과 네트워크 또는 기능이 포함된다.

‘섹션 4’에서는 식별 – 보호 – 감지 – 대응 – 복구 단계별 보호기능의 목적 및 예시를 제시하고 있

으며, 원격명령(Telecommand) 대해서는 필요한 보증수단으로 명령을 형식화하고 전송하는 시스템을 보호하고, 원격측정(Telemetry)에 대해서는 위성으로부터 데이터를 수신하고 처리하는 시스템을 보호하도록 목적을 제시하고 있다.

또한, 위협이 실현될 경우에는 검증된 대응 및 복구 계획을 세워 충분한 수준의 운영을 유지하도록 하고 우주부문에 대한 악영향을 방지하기 위해 지상 부문을 보호하도록 하고 있다.

3.1.3. NIST IR 8441 (하이브리드 위성 네트워크 사이버보안)

NIST IR 8441의 '섹션 1'에서 하이브리드 위성 네트워크 프로파일은 조직의 위험 허용범위와 일치하는 방식으로 위성 본체 또는 탑재체의 설계, 획득 및 운영에 종사하는 조직 및 이해관계자를 위한 실용적인 지침이라고 밝히고 있다.[10]

'섹션 2'에서 영상, 관측, 방송, 통신 또는 기타 우주 기반 아키텍처에 기여하는 여러 이해관계자가 활용하도록 '하이브리드 위성 네트워크 프로파일'의 사용목적을 제시하고 있다.

하이브리드 위성 네트워크 프로파일의 범위와 아키텍처는 예를들어 하나의 위성체에 다른 목적의 3개의 탑재체를 탑재하여, 일반적인 위성 탑재체와 지상체간 통신경로를 이용하는 형태와 3개의 탑재체가 독립적으로 운용되는 형태의 예시를 제시하고 있다.

'섹션 4'는 하이브리드 위성 네트워크 사이버보안 프레임워크 프로파일을 식별 – 보호 – 감지 – 대응 – 복구의 단계로 구분하여 제시하고 있으며, '식별'은 하이브리드 위성 네트워크와 관련된 시스템, 자산, 데이터 및 위험을 식별하는 단계이고, '보호'는 자체평가를 수행하고 사이버보안 원칙을 준수하여 하이브리드 위성 네트워크 서비스를 보호하는 단계이며, '감지'는 사이버보안 관련 장애 또는 하이브리드 위성 네트워크 서비스 및 데이터 손상을 감지하는 단계이고, '대응'은 하이브리드 위성 네트워크 서비스 또는 데이터 이상 징후 발생시 적시에 효과적이며 탄력적인 방식으로 대응하는 것이며, '복구'는 사이버보안 사고 이후 하이브리드 위성 네트워크를 적절한 작동순서로 복구하는 단계로 구분하여 프로파일을 제시하고 있다.

3.1.4. NIST IR 8323 (PNT[4] 서비스 사용 관련 사이버보안)

NIST IR 8323 "PNT 서비스 사이버보안"은 2021년 2월에 제정되었으며, PNT 프로파일의 범위에는 PNT 서비스를 사용하는 시스템이 포함되며, PNT 서비스는 "경도, 위도, 고도 또는 시간 또는 빈도 데이터의 전송을 계산하거나 보강하기 위한 참조를 제공하는 모든 시스템, 네트워크 또는 기능"으로 정의되는 다른 조직 단위에서 사용하기 위해 PNT 데이터를 사용한 다음 재송출하는 시스템을 포함하고 있다.[11]

PNT 서비스 공급자에는 GPS(Global Positioning Systems), 공용 NTP(Network Time Protocol) 서버, 상용 서비스 및 내부 시스템과 같은 정부 시스템이 포함되고, PNT 프로파일의 범위에는 소스 PNT 신호 발생기 및 공급자(예: 그림 3과 같이 GNSS(Global Navigation Satellite System) 제어 세그먼트 또는 우주 세그먼트)가 포함되지 않는다.

4) PNT : Positioning, Navigation, and Timing, (위치, 항법, 시간을 서비스하는 위성시스템)

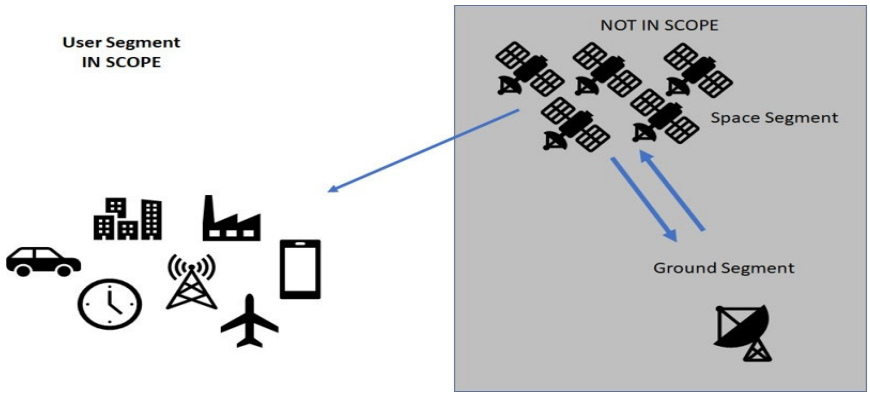

그림 3. PNT 프로파일 사이버보안 포함 범위

'섹션 4'는 PNT 서비스 프로파일'에서는 행정명령 구현 지침을 사이버보안 프레임워크 프로파일에 접목하여 제시하고 있다.

3.2. 유럽, 저궤도 위성통신 사이버보안 평가

유럽의 저궤도 위성통신 사이버보안 평가는 위성통신 시스템의 보안을 강화하기 위한 연구로 해킹, 신호 방해, 데이터 도청 등의 위협에 대해 분석하고 있다.[12]

암호화 및 인증 프로토콜을 개발하여 데이터의 기밀성과 무결성을 보장하며, 위성과 지상국 간의 통신 경로를 보호한다. 이외에도 사이버 공격에 대비한 위기 대응 계획을 수립하며, 규제와 표준화를 통해 일관된 보안 수준을 유지한다. 이러한 노력은 위성통신의 신뢰성을 높이고 안전한 통신 환경을 조성하는 데 기여하는 것으로 볼 수 있다.

표 2. 「유럽, 저궤도 위성통신 사이버보안 평가」 목차구성[21]

1. 소개(배경, 범위 및 목표, 대상, 구성)
2. 저궤도 통신위성(LEO SATCOM)[5] 개요 2.1 서비스 목록 2.2 저궤도 군집위성의 재정적 차원 2.3 정지궤도 위성 통신 시스템과의 비교
3. 저궤도 통신위성 자산 및 인프라 3.1 시스템 아키텍처 3.2 우주 프로젝트 조직 3.3 기술 및 공급망
4. 저궤도 통신위성 시스템 및 서비스를 위한 보안 과제 4.1 기술적 위험 4.2 재정 및 상업적 위험 4.3 악의적 위협 4.4 비(非)악의적 위협 4.5 사이버보안 사고사례
5. 통신위성 사이버보안 관련 표준 및 권고 5.1 우주 표준화를 위한 유럽 협력 5.2 우주 데이터 시스템 자문위원회 5.3 유럽 통신 표준 협회 5.4 미국 국립표준기술연구소(NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY) 5.5 유럽우주국 및 항공우주 위협 프레임워크 5.6 기타 활동 5.7 향후 활동 계획
6. COMPARIS 지상파 네트워크에서 SATCOM의 사이버보안 강점 및 약점
7. 결론

5) 저궤도 통신위성(Low Earth Orbit Satellites of Communication)

해당 문서는 통신 보안을 담당하는 국가기관을 대상으로 하였으며, 유럽연합 집행위원회의 정책 전문가, 사이버보안 기관, 통신 또는 위성 통신 부문에서 일하는 전문가, 산업 협회 및 표준화 및 통신 보안 분야에서 역할을 하는 기관에 유용하게 활용하도록 작성되었다.

'섹션 2'에서는 통신 서비스를 위한 저궤도 위성의 목적, 즉 저궤도 위성이 제공하는 서비스와 알려진 현재 및 향후 시스템에 대해 제시하고 있으며, '섹션 3'은 저궤도 시스템 설계 방법과 주요 공학적 개념에 대해 작성되었다. '섹션 4'는 저궤도 통신이 노출되는 위협의 목록을 제공하고 오픈 소스를 사용하여 이러한 시스템에 영향을 미치는 과거 사이버보안 사고를 식별하였으며, '섹션 5'는 우주 시스템 보안 분야에서 발표된 현재 표준화 및 권장사항에 대해 설명하고 있으며, '섹션 6'은 그림 4와 같이 사이버 보안의 관점에서 위협 노출 및 영향 심각도를 기준으로 우주 시스템과 지상 시스템간의 대응을 제시하였다.

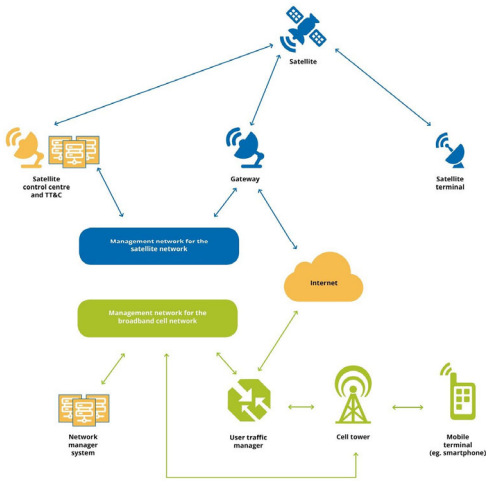

그림 4. LEO 및 셀룰러 네트워크의 아키텍처 구성

3.3. 일본, 상업용 우주시스템 사이버보안 가이드라인

일본의 경제산업성 제조산업국 우주산업실[6]에서는 2023년에「상업용 우주시스템을 위한 사이버보안 가이드라인(지침)」Ver 1.1을 배포하였다.[13] 이 지침서의 개발 배경은 "우주 정책 기본계획 이행 계획"(2022.12.15)에서 모든 우주 시스템의 기능 보장 강화의 일환으로 우주시스템의 사이버보안 대책에 대한 민간 기업의 가이드라인을 개발하는 것이다.

이 지침서에서는 표 3과 같이 목적과 범위, 대상을 포함하고 우주시스템의 사이버보안 상황과 상업용 우주 시스템을 위한 사이버 보안조치의 핵심사항을 제시하고 있으며 아래에서 내용을 살펴보겠다.

6) Space Industry Office, Manufacturing Industries Bureau, Ministry of Economy, Trade and Industry (METI)

표 3. 「일본, 상업용 우주시스템 사이버보안 가이드라인」 목차 구성

1. 소개
- 가이드라인 개발 배경과 목적 - 범위 - 대상

2. 우주 시스템의 사이버보안 상황
2.1 보안사고 사례 연구
2.2 상업용 우주 시스템의 사이버보안 위험 개념

3. 상업용 우주 시스템을 위한 사이버 보안 조치의 핵심사항
3.1 일반적인 조치
1) 조직의 사이버 보안 위험관리
2) 클라우드 보안 대책
3) 원격근무 대책
4) 내부 부정행위에 대한 대책 5) 외부기관에 보안사건 보고
3.2 우주 시스템에 대한 구체적인 조치
1) 법령에 근거한 조치
2) 위성 장치
3) 위성 운영 시설
4) 위성 데이터 활용 시설 5) 개발 및 제조 시설

부록 용어의 정의, 약어

지상시스템의 작동 및 유지 관리 단계에 중점을 두고 시스템 설계에서 폐기에 이르기까지 각 단계에서 주목해야 할 중요한 사항을 설명하고 있다.

상업용 우주시스템의 사이버보안 위험 개념은 “사이버/물리적 보안 프레임워크(Cyber/Physical Security Framework, 이하 CPSF) Ver.1.0”(2019년 2월, 경제산업성)을 활용하여 상업용 우주시스템에서의 보안 위험을 제시하고 있다.[14] 이 프레임워크는 계열사 및 비즈니스 파트너를 포함한 전체 공급망의 보안 조치에 대해 다중의 이해관계자가 접근하는 것으로 CPSF 접근 방식은 공급망이 위성 개발자, 위성 운영자, 지상국 운영자 및 위성 데이터 플랫폼 운영자와 같은 다양한 이해관계자로 구성되기 때문에 우주시스템에도 효과적일 것으로 평가하고 있다.

‘섹션 2’에서는 보안사고 사례 연구를 통해 상업용 우주 시스템의 사이버 보안 위험 개념에 대해 작성되었다.

‘섹션 3’은 조직 사이버보안 위험관리와 클라우드 보안대책을 중심으로 법령에 근거한 우주 시스템에 대한 구체적인 조치사항을 제시하였으며, 그림 5와 같이 상업용 시스템을 위한 사이버보안 조치의 핵심사항을 정리하였다.

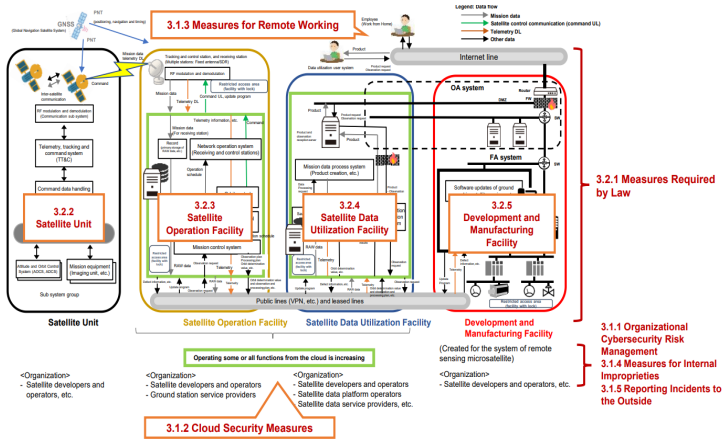

그림 5. 우주 시스템을 위한 사이버 보안 조치 핵심 사항

3.4. 해외 위성 사이버보안 가이드라인 비교 연구 결과

3.4.1. 미국

미국은 유럽과 일본보다 빠르게 2021년에 PNT 서비스에 대한 사이버보안 가이드라인 제정을 시작으로 2023년까지 '위성 지상 세그먼트 사이버보안', '하이브리드 위성 네트워크 사이버보안', '상업용 위성 운영을 위한 사이버보안'을 마련하는 등 우주(위성)분야 사이버보안 가이드라인 제정을 선도하고 있다.

미국의 우주(위성)분야 사이버보안 가이드라인의 중요한 특징은 설계 – 운용 - 폐기 등 우주(위성)체계의 생애 전(全) 단계에 대한 보안대책을 포함하고 있다는 것과 우주(위성)체계의 주요 구성분야인 위성체, 지상체, 데이터사용자, 네트워크, 위성통신 등 분야별 사이버보안 프레임워크를 구분하여 적용하고 있다는 것이다.

이러한 미국의 우주(위성)분야 사이버보안 가이드라인은 2023년 이후 유럽과 일본의 우주(위성)분야 사이버보안 가이드라인 제정에 영향을 준 것으로 보인다.

3.4.2. 유럽

유럽에서는 저궤도 통신위성에 대한 사이버보안 가이드라인을 발표했다. 저궤도 통신위성은 지리적 제약을 뛰어넘어 전 세계를 연결할 수 있는 능력을 지니고 있다. 위성통신은 첨단 기술을 활용하여 운영되며 이는 보안기술의 지속적인 발전과 적용이 요구되는 고도의 기술을 요구하고 있다. 또한, 위성통신은 국가안보와 경제에 중요한 역할을 하므로 보안의 중요성이 특히 강조된다고 할 수 있다.

유럽 위성통신 사이버보안의 장점으로는 먼저, 암호화 및 인증 기술을 통해 데이터의 기밀성과 무결성을 보장하여 정보유출 및 변조를 방지할 수 있다는 점이 있다. 또한, 실시간 보안 모니터링과 신속한 대응체계를 통해 사이버위협을 효과적으로 탐지하고 대응할 수 있는 능력을 갖추고 있으며, 위성통신 시스템의 사이버보안을 강화하고, 시스템의 안정성과 신뢰성을 높이는 데 기여한다고 할 수 있겠다.

3.4.3. 일 본

일본의 우주시스템에 대한 사이버보안 가이드라인의 특징으로는 상업용 우주 시스템의 CPSF[14]의 3층 구조(조직, 사이버/물리 관계, 사이버)를 활용하면서 지구관측용 초소형 위성을 분석 대상으로 하여 상업용 우주시스템의 전체적인 이미지와 이해관계자의 관계를 정리하여 분석 대상을 명확히 하기 위한 표준 모델을 제시하고 있다는 것이다. 또한, 관련 사고 사례 및 사이버보안 위험 시나리오의 예시를 제시하는 실제 활용 측면에서 체크리스트를 제공하는 장점을 가지고 있다는 것이다.

3.4.4. 비교연구 결과

아래 표 4와 같이, 미국과 유럽연합, 일본의 위성 사이버보안 가이드라인을 비교 연구한 결과를 정리해 보면, 미국은 PNT 서비스, 위성 지상 세그먼트, 하이브리드 위성서비스, 상업용 위성 운영 등에 관한 사이버보안 프레임워크(CSF)의 프로파일 문서를 작성하는 방향을 구체적으로 제시하였으며, 유럽연합은 저궤도 통신위성의 개발부터 운영단계에서의 위협을 자세하게 평가하였다. 일본은 미국과 유럽의 가이드라인의 형태가 모두 집합된 형태이며 특히, 위성 수명주기 단계에서 예상되는 보안 위협별 조치대상과 조치방법을 사이버/물리적보안 프레임워크(CPSF) 개념의 제시를

통해 이해관계자 그룹별 실행계획 수준으로 매우 세분화하여 구체적으로 작성하여 지침을 제시하고 있다는 특징을 보여주고 있다.

또한, 비교연구한 주요국가 모두 최근 미국의 주도하에 사이버보안 분야에서 강조되고 실행되고 있는 '위험관리 프레임워크(이하, RMF)[7]'와 '사이버보안 성숙도모델 인증제도(이하, CMMC)[8]'의 우주(위성)분야 적용에 대해서는 일본 가이드라인에서 CMMC에 대한 소개로 필요성을 제시한 것 외에는 언급되어 있지 않았다.

표 4. 위성 사이버보안 가이드라인 국가별 반영내용 비교연구 결과

* 범례: ●반영, ◑부분 반영, ◌미 반영

고려요소	미국 NIST IR				유럽연합	일본
	8270 ('23.7월)	8401 ('22.12월)	8441 ('23.9월)	8323 ('21.2월)	LEO SATCOM ('24.2월)	Commercial Satellite ('23.3월)
목적/범위/대상	●	●	●	●	●	●
보호대상 아키텍처	●	●	●	◑	●	●
보호대상 세그먼트	●	●	●	●	●	●
수명주기관리	●	●	●	●	◌	●
위협평가	◑	●	●	●	●	●
보안대책	◑	●	●	●	◑	●
CSF 적용	●	●	●	●	◑	●
RMF 적용	●	●	●	●	●	●
CMMC 적용	◌	◌	◌	◌	◌	◑
위성공급망 보안	◑	●	●	●	●	●
안티탬퍼(Anti-Tamper)	◌	◌	◌	◌	◌	◌
용어정의/약어집	●	●	●	●	●	●

* 출처 : 저자가 각국 가이드라인을 비교 분석하여 재구성한 결과 도표임

4. 국내 위성 사이버보안 가이드라인 수립방향 제안

4.1. 국내 위성 사이버보안 가이드라인 주요 고려 요소 도출

앞에서 위성에 대한 주요 사이버보안 위협 및 침해사례를 알아보고, 미국, 유럽연합, 일본 등 해외 위성 사이버보안 정책 및 가이드라인의 주요 내용을 비교하여 연구해 보았다. 그 연구 결과에 따라 국내 위성 사이버보안 가이드라인을 제정하기 위한 주요 고려요소를 살펴보면 아래 표 5와 같이 제시해 볼 수 있겠다.

표 5. 위성 사이버보안 가이드라인 주요 고려요소

고려요소	내용
1. 목 적	위성 시스템의 개발부터 운용과 폐기 단계까지 각종 사이버보안 위협에 대응하기 위한 가이드라인을 제시
2. 범 위	위성 시스템을 개발(설계 및 제작) 단계부터 운용과 폐기 단계까지 위성 시스템의 전체 수명주기
3. 대 상	위성체, 지상체, 사용자 부문
4. 보호대상 아키텍처 제시	위성 사이버보안 가이드라인에서 보호해야 할 대상을 식별, 대상별 위협 식별을 위한 아키텍처를 도식화하여 제공 * 위성 사이버보안 위협 : 지상·위성·통신 위협

7) RMF(Risk Management Framework) : 위험 관리 프레임워크. 미국의 조직의 정보 시스템 및 관련 자산에 대한 위험을 체계적으로 관리하기 위한 프로세스와 가이드라인을 제공하는 프레임워크

8) CMMC(Cybersecurity Maturity Model Certification) : 미국 사이버보안 성숙도모델 인증제도

5. 보안대책	위성 수명주기 전(全) 단계인 설계 → 운용 → 폐기 단계에 대한 보안대책을 포함
6. 보호대상 세그먼트 구분	체계개발 및 운용 등 위성체계 특성을 고려하여 일반적으로 위성체-지상체-데이터활용 사용자로 세그먼트를 구분
7. 사이버보안 프레임워크 적용	사이버보안 프레임워크(CSF)를 적용, 식별-보호-감지-대응-복구에 이르는 위협을 식별, 보안조치 적용 대상별 보안조치(보안통제항목) 사항에 대한 구체화 * 위성 운용자, 사업자, 개발자, 서비스사용자 등
8. 보안요구사항 / 보안통제 항목 식별	위성시스템에 대한 심층방어 우선순위 고려 사이버보안 위협 및 취약성에 대한 NIST 위험관리 프레임워크(RMF) 보안통제항목을 도출 * RMF와 위성 수명주기 단계별 활동 매핑 → 핵심 보안조치 사항 도출
9. 기타	위성 부품 공급망 보안, Anti-Tamper, 위성 제작업체 CMMC 인증제도 반영 등

4.2. 국내 위성 사이버보안 가이드라인 목차 구성 방안 제시

위에서 살펴본 위성 사이버보안 가이드라인에 반영될 고려요소를 기초로 아래 표 6과 같이 국내 위성 사이버보안 가이드라인의 목차를 구성해 보았으며, 이는 향후 전문가 그룹 토의 및 추가 연구를 통해 발전시킬 필요가 있겠다.

표 6. 국내 위성 사이버보안 가이드라인 목차 구성(예시)

1. 개요
1.1 배경 및 목적
1.2 활용 범위 및 적용 대상

2. 위성 사이버보안 개념 및 보호대상
2.1 위성 사이버보안 개념
2.2 위성 사이버보안 보호대상

3. 위성 사이버보안 위협평가
3.1 지상 세그먼트 위협 개념 및 시나리오
3.2 위성 세그먼트 위협 개념 및 시나리오
3.3 통신 세그먼트 위협 개념 및 시나리오

4. 위성 사이버보안 대책(보안통제항목)
4.1 지상 위협 보안대책
4.1.1 상용제품의 위협 보안대책
4.1.2 허가되지 않은 접근 보안대책
4.1.3 데이터 조작 공격 보안대책
4.1.4 공급망 공격 보안대책
4.1.5 컴퓨터 네트워크 탈취 보안대책
4.1.6 클라우드 플랫폼 공격 보안대책
4.2 위성 위협 보안대책
4.2.1 상용제품의 위협 보안대책
4.2.2 유도항해 및 제어시스템 위협 보안대책
4.2.3 소프트웨어 정의 라디오의 위협 보안대책
4.2.4 전력시스템의 위협 보안대책
4.3 통신 위협 보안대책
4.1.1 재밍 보안대책
4.1.2 스푸핑 보안대책
4.1.3 지상국-위성 간 도청 보안대책
4.1.4 위성 무단제어 보안대책

5. 별지
#1 사이버보안 프레임워크 적용, 식별-보호-감사-대응-복구 조치사항
#2 위성 사이버보안 잠재적 위협 사이버보안 프레임워크 맵핑
#3 위성 수명주기와 RMF 및 사이버보안 프레임워크 맵핑

6. 부 록 : 용어의 정의, 약어집 등

위 표 6의 목차 구성 예시를 살펴보면, 1장 개요에서는 국내 위성 사이버보안 가이드라인 제정의 배경과 목적을 제시하고, 활용 범위 및 적용 대상을 구체화한다.

2장에는 위성 사이버보안 개념 및 위성 사이버보안의 위협에 대한 보호대상을 구체화하여 제시한다.

3장에서는 위성 사이버보안을 적용하고 보호해야 할 대상을 지상-위성-통신 부문으로 구분하여 각각에 대한 위협의 개념과 시나리오를 작성한다.

4장에서는 위성 사이버보안 대책으로 지상 – 위성 - 통신 부문에서의 각각의 보안위협에 대한 보안통제항목을 제시한다. 먼저, 지상부문의 위협에 대한 보안대책에서는 '상용제품의 위협', '허가되지 않은 접근', '데이터 조작 공격', '공급망 공격', '컴퓨터 네트워크 탈취', '클라우드 플랫폼 공격'에 대한 보안대책을 제시한다. 두 번째로는 위성부문의 위협에 대한 보안대책으로 '상용제품의 위협', '유도항해 및 제어시스템의 위협', '소프트웨어에 대한 전파 위협', '전력시스템의 위협'에 대한 보안대책을 제시한다. 세 번째로는 통신부문의 위협에 대한 보안대책으로 '재밍', '스푸핑', '지상국-위성 간 도청', '위성 무단제어'에 대한 보안대책을 제시한다.

5장에서는 '사이버보안 프레임워크(CSF) 적용 및 식별 - 보호 - 감시 - 대응 - 복구 조치사항'과 '위성 사이버보안 잠재적 위협과 사이버보안 프레임워크 매핑'을 제시하고, 마지막으로 '위성 수명주기와 위험관리 프레임워크(RMF) 및 사이버보안 프레임워크의 매핑'을 제시한다.

CSF는 조직의 사이버보안 위험 관리 프레임워크로 산업에 보편적으로 적용 가능하며 유연성과 효율성을 강조하고 있고, RMF는 시스템의 생애 주기를 고려한 체계적인 보안 프레임워크로, 특히 정부 및 공공기관에서 유용하다고 하겠다.

현시점에서 국내에서는 위의 표 6의 국내 위성 사이버보안 가이드라인의 목차 구성 예시에서 밝힌 바와 같이 '국내 위성 사이버보안 가이드라인'을 먼저 제도화하고, 이후 국방 위성의 개발과 운용특성에 맞도록 "국방 위성 사이버보안 가이드라인"의 제정이 필요하다고 하겠다.

5. 결론

전세계는 우주에 많은 관심을 가지고 있으며, 우리의 일상 뿐만 아니라 안보분야에서도 우주(위성)에 대한 중요성은 날로 커져가고 있는 상황이다. 우주공간에서 운용중인 인공위성과 인공위성을 운용하는 지상 통제장비와 시설, 수집 및 생산된 많은 데이터의 활용체계 등 우주시스템에 대한 개발 및 운용 사례가 무수히 증가되고 있다.

미국, 유럽, 일본 등 우주시스템의 선도국가들은 날로 심각해지고 있는 우주시스템의 사이버보안 유지를 위해 가이드라인을 만들어 우주시스템의 구성 대상별, 우주시스템의 형상별 최초 설계부터 개발, 운용단계에 이르기 까지 사이버보안을 유지하기 위해 사이버보안 대책을 제시하고 있으며, 국가 차원에서 적극적으로 대응을 하기 시작했다.

본 논문에서는 국내 위성 사이버보안 가이드라인 수립의 필요성을 강조하는데 목적이 있었으며, 국내 및 국방분야 위성 사이버보안 가이드라인의 수립의 방향과 우주 사이버보안 분야 정책적 발전 방향을 제안하였다.

금번 연구를 통해 앞으로 국내 민간 및 국방 분야 위성 사이버보안 분야 발전을 위한 정책발전 방향으로 아래와 같이 강조하고자 한다.

첫 번째, 국내 위성 개발 및 운용 특성에 맞는 위성 사이버보안의 정책적 발전을 위한 유관기관 간의 협조체제 속에서 일관성 있고 범용성이 높은 국가차원의 거버넌스 조직과 긴밀한 협력체제의 유지가 필요하겠다.

두 번째, 국내에서도 증가되고 있는 위성 사이버보안 위험 및 위협에 대비하기 위한 가이드라인의 제정이 시급하겠다.

세 번째, 국내 산업계의 우주산업과 기술에 대한 보호와 해외협력 및 수출의 경쟁력 확보를 통한 우주기술의 주권화와 산업화를 가속화 하기 위해 우주(위성) 분야에 대한 '위험관리 프레임워크'(RMF)와 '사이버보안 성숙도모델 인증제도'(CMMC), '안티탬퍼'(Anti-Tamper) 등의 적용이 하루 빨리 추진되어야 할 것이다.

참고문헌

[1] 국가사이버안보센터. http://www.ncsc.go.kr (검색일 2024. 10. 26).

[2] 국가정보원 홈페이지. 위성 사이버보안 강화를 위한 관계기관 협의체 발족. http://www.nis.go.kr›CM (검색일 2024. 10. 1).

[3] 호주 SmartSat CRC. Satellite Cyber Resilience Whitepaper. 2022.

[4] 차세대융합기술연구원 블로그. 인공위성이 해킹을 당한다고? 우주 사이버보안 이야기. https://blog.naver.com/isaict/223141143675 (검색일 2024. 10. 1).

[5] 머니투데이. 인공위성까지 해킹하는 시대, 우주항공 사이버위협 대응 필요. https://news.mt.co.kr/mtview.php?no=2023103114023395265 (검색일 2024. 10. 1).

[6] 조선비즈, 한국 위성 운영의 심장 해킹에 뚫렸다. https://biz.chosun.com/science-chosun/science/2024/03/26/QH6X2YD5A5FLDJLDYJXJPMJA5M/ (검색일 2024. 10. 1).

[7] KISA Insight. 주요국 우주(Space) 사이버시큐리티 정책 동향 조사·분석. Vol. 4. 2024.

[8] NIST Interagency Report 8270. Introduction to Cybersecurity for Commercial Satellite Operations. 2023.

[9] NIST Interagency Report 8401. Satellite Ground Segment ; Applying the Cybersecurity Framework to Satellite Command and Control. 2022.

[10] NIST Interagency Report 8441. Cybersecurity Framework Profile for Hybrid Satellite Networks. 2023.

[11] NIST Interagency Report 8323. Foundational PNT Profile : Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing(PNT) Services. 2021.

[12] EUROPEAN UNION AGENCY FOR CYBERSECURITY. LEO Satcom Cybersecurity Assessment. 2024.

[13] Ministry of Economy, Trade and Industry. Cybersecurity Guidelines for Commercial Space Systems Version 1.1. 2023.

[14] Ministry of Economy, Trade and Industry. The Cyber/Physical Security Framework Version 1.0. 2019.