항공우주산업기술동향 21권 2호 (2023) pp. 141~149
기술동향
https://www.kari.re.kr/library/ 에서 보실 수 있습니다.

국외 우주보안 관리체계 및 기술 동향

이명신*, 박재형*, 이보영*, 현대환*, 양형모*, 정옥철**, 정대원***

The Trends in Managemet Systems and Technology for Space Security Overseas

Lee Myeongshin*, Park Jaehyung*, Lee Boyoung*, Hyun Daehwan*, Yang Hyungmo*, Jung Okchul**, Chung Daewon***

ABSTRACT

As the use of space systems continues to increase in government, commercial, military, and civil sectors, interest in space security is also increasing. The traditional concept of security is to physically or logically protect systems, data, information, and assets from internal and external threats and keep them safe. Therefore, space security can be defined as protecting the space system, ground system, and space-ground communication system that constitutes space missions from threats and keeping them safe. In Korea, major infrastructures related to space mission operations are designated as critical infrastructure under the leadership of the government and security management activities are being conducted. This paper describes trends in establishing security management system platforms and implementing security technologies in foreign standard organizations and space operation organizations.

초 록

정부, 상업, 군 및 민간 영역에서 우주시스템의 활용은 지속적으로 증가하면서 우주보안의 관심도 증가하고 있다. 보안의 전통적인 개념은 시스템, 데이터, 정보, 자산 등을 물리적 또는 논리적으로 내·외부 위협으로부터 보호하고 안전하게 유지하는 것이다. 따라서, 우주보안은 우주임무를 구성하는 우주시스템, 지상시스템 및 우주-지상 통신시스템을 위협으로부터 보호하고 안전하게 유지하는 것으로 정의할 수 있다. 국내에서는 우주임무운영 관련 주요 시설을 정부 주도하에 주요정보통신기반시설로 지정하여 보안관리점검을 수행하고 있다. 본 논문에서는 국외 표준기관 및 우주운영기관의 보안관리체계 플랫폼 구축 및 보안기술 구현 동향에 대하여 기술하고 있다.

Key Words : Space Security(우주보안), Space Mission(우주임무), Ground Station(지상국)

* 이명신, 박재형, 이보영, 현대환, 양형모, 한국항공우주연구원, 국가위성정보활용지원센터 위성운영부
mslee@kari.re.kr, jhpark90@kari.re.kr, boyounglee@kari.re.kr, dhhyun@kari.re.kr , yhm@kari.re.kr
** 정옥철, 한국항공우주연구원, 국가위성정보활용지원센터 SSA연구실
ocjung@kari.re.kr
*** 정대원, 한국항공우주연구원, 국가위성정보활용지원센터
dwchung@kari.re.kr

1. 서 론

보안(Security)은 시스템, 데이터, 정보, 자산 등을 물리적 또는 논리적으로 내·외부 위협으로부터 보호하고 안전하게 유지하는 것이다[1]. 보안의 영역은 크게 IT 영역, 물리영역으로 나누게 될 수 잇을 것이며, IT영역은 통신보안, 컴퓨터 보안, 네트워크 보안, 인터넷 보안 및 정보보안 등이 있다. 물리영역으로는 항공보안, 가정보안(Home security) 등이 있을 것이며, 이외 인적보안 등이 포함된다[2]. 우주보안(Space Security)은 최초 군영역에서 만들어 졌으나[3], 최근 뉴스페이스 시대의 도래, 우주시스템(발사체, 위성 등)이용의 지속적 증가 등 우주산업이 성장하면서 우주보안이 보안영역에서 큰 관심영역 되고 있다.

우주시스템 표준기구인 CCSDS[4]에서 정의한 우주보안에서의 보안관리 대상은 지상시스템, 우주시스템 및 통신시스템이 있다. 보안관리에 있어서, 위협과 위험의 정의가 중요할 수 있다. CCSDS에서는 위험(Risk)을 특정 위협(Threat)이 특정 취약성을 악용하여 정보 시스템에 부정적인 영향을 미칠 가능성 으로 정의하고 있다[5]. 위협은 시스템 및 조직에 해를 끼칠 수 있는 사고의 잠재적 원인으로 정의하고 있다[5].

본 논문에서는 먼저 우주보안 및 보안관리체계의 표준 플랫폼을 살펴보고자 한다. 우주보안 표준 플랫폼은 CCSDS의 우주보안 관리체계를 인용하였다. 이후 CCSDS 우주보안 체계에서도 참고하고 있는 NIST의 보안관리체계를 기술하였다. 우주시스템의 보안에 있어서, 우주파편과 재밍 등을 제외하면 대부분의 보안관리는 기존의 정보보안관리체계를 적용함으로써 보안 목표를 달성할 수 있다. 그리고, 국외 우주운영기관의 보안관리체계 및 보안기술 구현 동향에 대해서 기술한다. 또한, 우주보안에서의 주요 항목중의 하나로써 우주물체 보호를 위한 우주상황인식 동향에 대해서도 기술한다.

2. 우주보안 및 보안 플랫폼 동향

2.1 CCSDS 우주보안

CCSDS의 우주보안관련해서는 계획과 평가, 설계, 구현 단계로 이루어져 있다[6]. 우선 계획과 평가단계에서는 우주임무에 대한 보안 위협분석, 시스템에 대한 보안연결 가이드, 임무계획자에 대한 보안 가이드에 대한 정보를 제공한다.

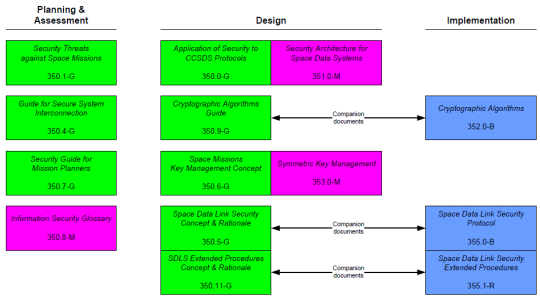

그림 1. CCSDS Security Document Tree

우주 임무에서의 보안위협을 살펴보면 다음과 간다. 우주임무에 영향을 주는 위협의 요소는 다음과 같이 제시하고 있다.

- 적대적 요소 : 테러리스트, 해외정보기관, 해커 등
- 내부 요소 : 부적절 유지보수 인원 및 시스템 인원, 불만을 품은 직원, 직원의 부주의한 행동 등
- 환경적 요소 : 자연/인적 재해, 팬데믹, 우주기상, 우주파편, 정전 등
- 구조적 요소 : 소프트웨어 및 하드웨어 실패

위에서 주목해야할 점은 환경적 요소의 팬데믹과 우주파편 등이다. 2020년 발발한 COVID-19로 인하여 그 이전까지 우주산업이 성장추세이었으나 COVID-19로 인하여 성장에 어려움을 겪은 적이 있다[7]. 우주물체에 있어서도 최근 CelesTrak[8]의 자료에 따르면 '23년 6월 현재 우주상공에 10cm이상의 우주물체는 약 21,369개이며, 이중 우주파편은 53.3%, 운영중인 우주물체는 41.8%, 로켓 몸체는 4.5%로 추산되고 있다. 특히 500km 상공에는 스타링크

위성이 2,500여개 운영되고 있다. 이러한 측면에서 우주물체보호는 우주보안 측면에서도 중요한 부분을 차지하고 있다.

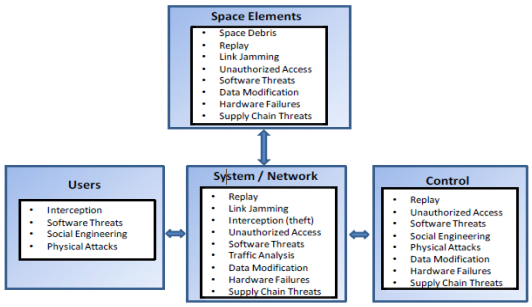

그림 2. CCSDS 우주 임무의 잠재적 위협

CCSDS에서는 <그림 2>와 같이 각 우주시스템 임무의 잠재적 위협을 정의하고 있다[9]. 우주부분, 사용자 부분, 제어부분 및 시스템/네트워크에 대한 위협을 정의하고 있다. 또한 위성의 임무별로 <표 1>과 같이 위협에 대한 잠재적 영향, 가능성 및 보안메커니즘을 제공하고 있다.

표 1. 지구관측위성 위협 분석

위협	영향	가능성 (1=낮음, 5=높음)	보안메카니즘
데이터 변조	·정보변조 ·시스템 손상	4	·데이터 무결성 스킴
지상시설 물리적 공격	·명령어, 제어 및 데이터의 손실	2	·가드, 게이트, 접근통제,백업사이트 등
차단 (Interception)	·민감데이터 손실	3(LEO) 3(GEO)	·암호화
재밍 (Jamming)	·관제데이터 손실	3(LEO) 2(GEO)	·다중 송수신경로 ·스프레드 스펙트럼
서비스 거부	·접근 불능	3	·방화벽, IPS ·암호화/권한부터
위장 (Masquerade)	·잠재적 송수신 장애	2	·높은수준 인증 ·접근통제
재전송 (Replay)	·시스템 손상	1	·인증된 명령어 카운터 시간
소프트웨어 위협	·비의도 이벤트 ·시스템손상	2	·인수시험 ·IV&V ·코드분석 등
비인증 접금	·데이터 탈취 ·운영 장애 ·시스템 손상	3	·암호화 ·명령어 인증/승인 ·접근 통제
하드웨어 오염	·시스템 불안정 ·시스템 손상 ·비의도 시스템 영향	3	·신뢰 공급망 ·하드웨어 인증 ·검증된 하드웨어 공급업체
공급 체인	·공급 장애 ·위조 부품/소프트웨어	4	·신뢰 공급망 ·검증/인증된 소스

2.2 NIST 정보보호 관리체계

정보보호 관리체계로써 미국 연방정부에서 활용되고 있는 NIST의 정보보호관리체계에 대하여 살펴본다. 2002년 제정된 전자정부법률에서는 미국의 경제적 국가적 보안 관심에 대한 정보보안의 중요성을 인식하였다. FISMA (Federal Information Security Management Act)라고 명명된 이 법률에서는 NIST에서 표준, 가이드라인 등을 만들도록 책임을 주었다[10].

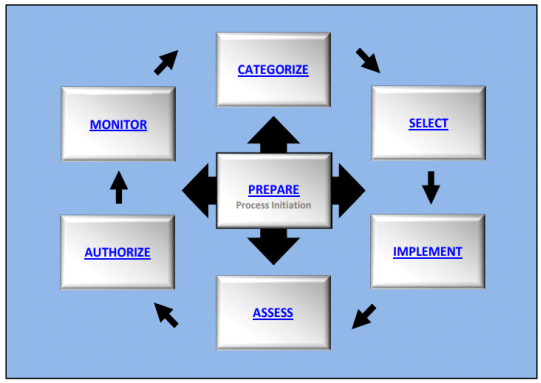

그림 3. NIST 위험관리 프레임워크

<그림 3>과 같이 위험관리 프레임워크(RMF, Risk Management Framework)에서 7단계를 제안하고 있다[11].

- Prepare : 조직이 보안 및 개인 정보 보호 위험을 관리할 수 있도록 준비하는 필수 활동
- Categorize : 영향 분석을 기반으로 처리, 저장, 전송되는 시스템 및 정보를 분류
- Select : 위험 평가를 기반으로 시스템을 보호하기 위해 NIST SP 800-53 제어 세트를 선택
- Implement : 컨트롤을 구현하고 컨트롤 배포 방법을 문서화
- Assess : 통제가 제대로 이루어지고, 의도한 대로 작동하며, 원하는 결과를 생성하는지 평가
- Authorize : 관리자가 위험 기반 결정을 내려 시스템 승인(운영)
- Monitor : 제어 구현 및 시스템에 대한 위험을 지속적으로 모니터링

표 2. 위험관리프레임워크를 위한 NIST 문서 목록

No	Subject
FIPS199	Standards for Security Categorization Federal information and Information System
FIPS200	Minimum Security requirements for federal information and Information System
SP 800-37	Guide applying the Risk Management Framework to Federal Information Systems
SP 800-53	Recommended Sedurity Controls for Federal Information Systems
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories

SP 800-37[11]에서는 총 18개의 보안통제 구성요소를 제공하고 있다. 보안통제의 구성요소는 운영(Operational), 기술(Technical), 관리(Management)로 구성이 되어 있다. 운영 클래스에는 총 9개의 패밀리로 구성되며 총 83개의 항목, 확장항목수는 총 216개의 항목을 포함한다. 확장항목이란 보안요구사항이 높은 기관에서 추가적 및 선택적으로 구현할 수 있는 항목을 의미한다. 기술 클래스는 4개의 패밀리로 구성되며, 총 34개의 항목 및 총 153개의 확장항목으로 구성되어 있다. 관리 클래스는 5개의 패밀리로 구성되고, 총 40개의 항목과 44개의 확장항목으로 구성되어 있다. <표 3>은 운영클래스의 예를 보여주고 있다.

표 3. NIST 보안 통제 구성요소(Operatinal Class)

Family	항목수	확장 항목수
Awareness and Training(AT)	5	35
Configuration Management(CM)	9	33
Contingency Planning(CP)	9	36
Indident Response(IR)	8	10
Maintenance(MA)	6	17
Media Protection(MP)	6	13
Physical Enviromental Protection(PE)	19	27
Personnel Security(PS)	8	4
System and Information Integrity(SI)	13	41
	83	216

3. 우주보안 및 관리체계 구현 동향

3.1 시스템 위협 평가

국가 주요 자산인 위성을 안전하게 보호하고, 우주 임무를 안정적으로 운영하기 위해서는 다중임무관제를 수행하는 지상국과 위성-지상국 간의 통신 링크를 외부의 위협으로부터 보호해야 한다. 지상국은 크게 네트워크, 안테나 시스템, 다중임무를 수행하기 위한 소프트웨어 등으로 구성되어 있다. 이러한 지상국 기반 시설을 보호하기 위한 보안 기술은 지상국 시스템에 대한 보안 위협을 분석 및 평가하고 이를 바탕으로 보안 프로토콜을 설계하는 절차를 반복적으로 수행하면서 개발 및 개선되고 있다[12]. 우주 임무를 수행하는 지상국 시스템에 특화된 위협 평가 및 분석 기법을 제시하기 위한 여러 연구가 수행되었다. NASA(National Aeronautics and Space Administration) 산하기관인 JPL(Jet Propulsion Laboratory)에서 위성 교신 계획 관리, 통신 자원 관리, 명령 생성 및 전송 등을 포함하는 임무 운영 전주기 과정에서 취약점 분석을 수행할 수 있는 임무운영시스템 특화 위협 평가 기술을 제안하였다[13]. 또한, 여러 지상국이 정보를 공유할 수 있는 플랫폼도 제시하고 공유된 데이터를 이용하여 실시간 보안 탐지 및 대응하기 위한 자동 데이터 처리시스템도 개발되었다[14]. ESA(European Space Agency)에서는 지상국 인프라 보호를 위한 정보보안관리시스템을 구현하였다. 해당 시스템의 위협 평가 기법은 네트워크 자원, 데이터, 컴퓨터 시스템 등의 주요 자산에 대한 가치 설정, 해당 자산에 대한 위협 및 취약점 정의, 평가, 대처의 과정을 포함하고 있다. ESA는 해당 내용을 표준화하여 국제표준인 ISO27001에 인증을 획득하고 지속해서 관리 및 개선하고 있다[15]. 또한, 우주 임무 유형의 특성을 고려하여 임무 특화 보안 평가 방법론도 제시함으로써 지상국의 보안 수준을 개선하였다[16].

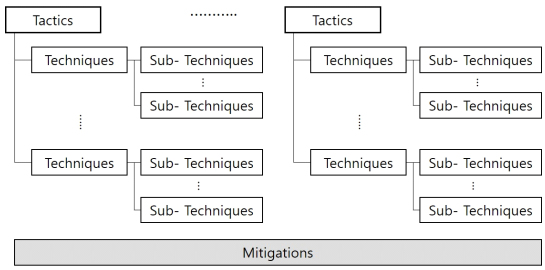

그림 4. SPACE-SHIELD 위협 모델 및 완화방안

또한 ESA에서는 MITRE ATT&CK®[17] 기반의 우주시스템 보안관리체계를 제공하고 있다. MIRTE에서는 보안관련 모든 잠재적 위협을 제시하고 이에 대한 저감방안(Mitigation)을 제공하고 있다. ESA에서는 이를 기반으로 우주시스템에 적용가능한 프레임워크를 제공하고 있고, 이를 SPACE-SHIELD (Space Attacks and Countermeasures Engineering Shield)라고 명명하고 있다[18]. 이 프레임워크에서 정의하고 있는 위협은 최상위 레벨에서 전술(Tactics)로 정의하고 각 전술마다는 기술(Techniques)과 상세 하위 기술(Sub-techniques)을 기술하고 있다. 우주시스템에 영향을 줄수 있는 모든 잠재적 위협을 기술하였다. 모든 위협에 대하여는 조치가능한 저감방안(Mitigation)을 제시하였다.

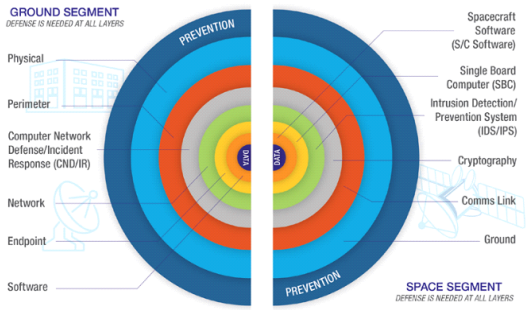

그림 5. 우주시스템의 종심방어 모델

SPARTA(Space Attack Research & Tactic Analysis)[19]에서는 우주시스템을 위한 종심방어(Depth-in-Defense, DiD) 모델을 제공하고 있다. DiD는 계층(Layered)보안으로도 불려지고 있으며, <그림 5>와 같이 맨 바깥에는 예방(Prevention)계층이 정의되고 있다. 예방계층의 서브계층으로는 인적 보안인식, 내부위협, 보안평가, 위협분석, 훈련, 공급 체인 등이 있다. 이와 같이 여러 계층의 보안위협을 정의하고 이를 방어하는 개념이다.

3.2 보안 프로토콜 설계

우주 임무를 수행하기 위한 주요 자산인 위성, 지상국 기반 시설 등을 보호할 수 있는 보안 기술이 사이버 공격 기술의 진보에 따라 더욱 중요해지고 있다[20]. ESA에서 위성과 지상국 통신 링크를 보호하기 위한 보안 프로토콜을 정의하였으며[21], 세계의 임무운영기관들이 보안시스템을 효율적으로 설계할 수 있도록 요구사항 분석, 설계, 구현, 검증 등의 기능들을 모듈화 및 표준화하였다[22]. 또한, ESA는 소프트웨어 공학 관점에서 응용 프로그램 계층 보안을 고려한 시스템을 여러 기관이 효율적으로 개발할 수 있는 GASF(Generic Application Security Framework)을 제안하였다.

우주 관련 기술의 향상에 따라 국제적 우주임무 수행을 위한 국제 협력도 증가하고 있다. 이에 따라 국제 협력을 위한 데이터 표준에 관한 여러 연구도 수행되고 있다. CAS (Chinese Academy Sciences)에서는 우주 임무 데이터에 대한 인증, 출처 등의 정보를 보존할 수 있는 프로토콜을 제안함으로써 안전한 국제적 임무를 수행할 수 있는 기틀을 마련하였다[23]. 미국 존스홉킨스대학교 응용물리학연구소에서도 다수 기관이 국제 협력을 안전하게 수행할 수 있도록 개별통신망 또는 각 계층에서만 특화된 기존 보안 프로토콜의 한계를 극복하는 종단간 보안 프로토콜을 설계하였다[24]. 또한, 지상국에서 운용되는 암호 체계를 암호 알고리즘의 계산 복잡성, 암호키 관리 정책, 암호 생성 방식 관점에서 질적 수준을 평가하는 방법론이 제시되었으며[25], NASA에서는 지상국 데이터

시스템에 대한 접근 제어를 위한 프로그램을 만들어 배포하였다[26]. 이러한 보안 프로토콜을 활용하여 우주 자산을 외부 위협으로부터 보호할 수 있다.

위성과 지상국을 보호하기 위한 보안 기술들이 많이 연구개발 되었지만, 새로운 우주 환경에 대응하기 위한 보안 기술 연구는 지속해서 수행되어야 한다. 새로운 우주 환경은 위성과 지상국의 수가 급격히 늘어나는 것만 고려할 것만 아니라 위성을 활용하는 차세대 통신 기술을 위한 지상 네트워크 복잡도 증가, 해양 네트워크 활용, UAV(Unmanned Aerial Vehicle) 네트워크 활용 등의 주제도 고려되어야 한다. 기존 보안 기술은 위성 통신 네트워크, 공중 네트워크, 지상 네트워크, 해양 통신 네트워크 등의 개별 네트워크를 보호하는 데 집중하였다. 그러나, 여러 계층의 네트워크 활용하는 기술 및 교차 계층을 고려한 사이버 공격 기술에 대한 연구개발이 활발히 진행되고 있으므로 교차 계층 공격에 대한 보안 대책이 필요하다[27].

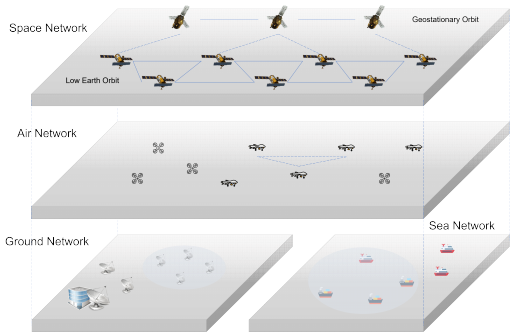

그림 6. 네트워크 계층조도

<그림 6>은 우주, 공중, 지상, 해상 네트워크를 모두 포함하는 네트워크 구조도를 보여준다. 향후, 위성 통신 기술을 활용하여 지구상의 수 없이 많은 자산이 연결될 것이기 때문에 이러한 자산 보호를 위해 교차 계층 사이버 공격에 대처할 수 있는 보안 기술에 대한 요구는 더욱 커질 것이다.

3.3 우주물체 보호

국제연합(UN)에서는 우주활동의 장기지속성 확보를 위한 LTS(Long-Term Sustainability) 가이드라인을 제정하여 정책 및 규제, 우주운영의 안전, 국제협력 및 역량강화, 과학기술 연구개발 분야로 각각 세분화하여 총 21개 지침을 마련하여 이행을 촉구하고 있다[28]. 한편, 대한민국을 포함한 13개국이 참여하고 있는 국제우주쓰레기조정위원회(IADC, Inter-Agency Space Debris Coordination Committee)에서는 우주물체를 보호하기 위한 방안 중의 하나로, 우주쓰레기 경감 가이드라인을 제정하여 계속해서 갱신하고 있다[29]. 또한, 국제표준을 다루는 ISO(International Organization for Standardization) 에서는 우주쓰레기 완화를 위한 요구사항을 ISO 24113을 발행하였는데 여기에는 우주공간에서 우주쓰레기 배출 제한, 궤도상 분열 방지, 임무종료 이후 우주시스템(인공위성 및 발사체 등) 폐기 등이 포함된다[30].

유럽에서 발표한 우주교통관제 기술 동향[31]에 따르면, 충돌 및 간섭위험을 줄여 궤도상 운영의 안정성 향상, 우주환경의 부정적 영향을 완화하여 우주활동의 장기적인 지속 가능성 보장, 우주활동의 세계화, 증대화, 다양화뿐만 아니라 혼잡한 우주환경 문제의 해결을 우주교통관제 목표로 제시하였다. 또한, 우주 공간에서의 물리적 충돌 및 분리 또는 간섭(주파수)과 같은 운영 위험요소를 해결하기 위해, 우주시스템의 수명주기(Life Cycle), 즉 설계-제작-발사-운영-폐기의 모든 단계에 적용해야 한다고 적용범위를 제안하였다. 우주환경보호를 위한 기술적 고려사항으로는 궤도자원 보호, 우주쓰레기 경감 및 제거, 우주 궤도 상에서의 충돌(Collision) 및 파손(Breakup) 방지 등을 포함하고 있다. 미국은 2018년 6월 우주 이물질의 생성 억제 및 우주물체 간의 충돌위험을 감소시키기 위해 우주활동의 안전성 및 안전의 지속가능성을 확보하기 위한 방안으로 우주정

책지침 3호(Space Policy Directive-3)를 발표하였는데, 여기에는 우주교통관제의 효율성을 높이기 위한 전략으로 데이터 공유의 필요성을 강조하고 있다[32]. 이를 근거로 우주상황인식의 기본적인 데이터와 우주교통관제 서비스를 무료로 제공하는 것을 목표로 하고 있으며, 상무부는 민간에 우주안전에 관한 데이터를 제공하기 위해, OADR(Open Architecture Data Repository)의 형태로 TraCss(Traffic Management System for Space)을 구축하고 있다[33].

3.4 우주-지상 통신링크 보호

우주시스템 및 지상국간의 통신을 위한 주파수는 국제전기통신연합(ITU) 및 각국의 전파법 등에 의하여 ITU 등록 및 국내등록 등을 완료한 이후 주파수를 사용할 수 있다[34, 35]. 따라서, 등록된 주파수는 보호받고 간섭을 받지 않을 권한을 부여받게 된다. 이러한 관점 및 우주보안 측면에서 잠재적 위협으로 식별되는 "재밍(Jamming)"은 ITU 및 각국 전파법의 규제대상이 될 것이다. 악의적 재밍 위협에 대한 보안 조치 사항으로는 주파수 호핑, 스프레드 스펙트럼 및 다중경로 등을 제안하고 있다[9, 18]. 주파수 재밍에 대해서는 다양한 연구가 진행되고 있으며, 대부분 통신위성 신호 및 GNSS 신호에 대한 재밍연구가 수행되고 있다[12]. 또한, 주파수 재밍으로부터 안정적인 통신을 위한 RF 필터에 대한 연구가 국내외로 진행되고 있으며, 대역통과 필터의 주파수를 조정하여 재밍 신호로부터 회피하는 방법과 대역저지 필터를 이용하여 재밍신호를 억제하는 방법등이 연구되고 있다[39]. 통신/방송 신호 및 GNSS(GPS)신호등의 재밍은 분쟁지역에서 사례(중동, 우쿠라이나 등)가 보고되었다[36, 37]. GPS 신호 교란시의 회피 방안으로써는 fast orthogonal search, signals cross-correlation, turbo codes 등이 시뮬레이션 및 실험을 통하여 연구되었다[12]. 또한, HawkEye360과 같은 군집위성으로 GPS 신호를 수집하여 데이터 교란 여부 및 발생위치를 알려주는 서비스도 제공되고 있다[37]. 또한, GPS신호를 이용하는 위성지상국에서는 GNSS 방화벽 설치를 통하여 재밍신호에 대비하고 있다[38].

4. 고찰 및 결론

통신, 방송, 안보, 항법 및 지구관측 등의 일상생활에서 우주의 활용은 지속적으로 높아지고 있다. 또한, 저궤도 위성통신 및 지구관측 등의 서비스를 제공하기 위한 군집위성 및 소형위성의 증가 등으로 우주자산이 급격하게 증가하고 있다. 우주자산에 활용 및 관심도가 높아질수록 보안영역에서는 악의적 공격의 대상에 노출되는 사례가 증가할 수 있다. 이에 따라 CCSDS에서는 각종 우주임무관련 설계 및 구현을 위한 권고 및 표준화 방안을 제시하고 있으며, 우주임무에서 많은 부분을 차지하는 정보보안 영역에서 NIST의 정보보호 관리체계를 참고할 수 있도록 권고하고 있다. 이를 기반으로 국외 우주운영기관에서는 우주보안 관리체계 및 프로토콜 구현 등을 수행하고 있다. 또한 우주보안에서의 특징인 우주물체 보호 및 주파수 재밍에 있어서도 다양한 활동을 수행하고 있다. 국내에서도 우주운영을 포함한 주요 기반시설에 대해서는 년간 정보보호관리체계에 따라서 정보보호 감사를 수행하고 있다.

국가우주자산의 보호를 위하여 더욱더 체계적인 우주보안 정책 및 기술 구현과 운영이 필요한 시점으로 판단된다. 국내외의 우주보안 관련 풍부한 정보보호 관리체계 및 기술이 현장에서 구현·운영될 수 있도록 적절한 정보보호 조직 등의 구성이 선결되어야 하는 시점으로 사료된다.

참고문헌

1. https://terms.tta.or.kr
2. https://en.wikipedia.org/wiki/Security
3. “Handbook of Space Security”, pp 7-21
4. https://www.ccsds.org
5. “Information Security Glossary of Terms”, CCSDS, 350.8-M-2, March 2020
6. “Security Guide for Mission Planners”, CCSDS, 350.7-G-2, April 2019
7. “The impacts of COVID-19 on the space industry”, OECD Policy Response to COVID-19,
8. https://celestrak.org/
9. “Security Threat Against Space Missions”, CCSDS, 350.7-G-3, February 2022
10. “Standards for Security Categorization Federal information and Information System”, NIST, FIPS199,
11. “Guide applying the Risk Management Framework to Federal Information Systems”, NIST, SP 800-37,
12. Tedeschi, P., Sciancalepore, S., and Di Pietro, R., “Satellite-based Communications Security: A Survey of Threat, Solutions, and Research Challenges”, Computer Networks, Vol. 216, 2022, pp. 109246-109264.
13. Ko, A. T., Tan, K., Cilloniz-Bicchi, F., and Faris, G., “Cyber Threat Assessment of Uplink and Commanding System for Mission Operation”, 13th SpaceOps Conference, California, USA, 2014.
14. Vivero, J., and Marin, R., “Cyber Situational Awareness in Space Organizations Operations Centers”, 15th SpaceOps Conference, Marseille, France, 2018, pp.2481.
15. Melgarejo Diaz, N., Flentge, F., and Eggleston, J., “Security Risk Assessment and Management for ESOC’s Mission Operations Infrastructure Data Systems”, 13th SpaceOps Conference, California, USA, 2014. pp. 1766.
16. Vivero, J., and Del Monte, L., “Space Missions Cybersecurity”, 13th SpaceOps Conference, California, USA, 2014. pp. 1765.
17. https://attack.mitre.org/
18. https://spaceshield.esa.int/
19. https://attack.mitre.org/
20. Duo, W, Zhou, M., and Abusorrah, A., “A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advance and Challenges”, IEEE/CAA Journal of Automatica Sinica, Vol. 9, 2022, pp. 784-800.
21. Krimgen, M., Fischer, D., and Engel, T., “A Security Protocol for Space Link Communication”, 9th SpaceOps Conference, Heidelberg, Germany, 2008. pp. 3502.
22. Fischer, D., and Spada, M., “Ready for Secure Software: Secure Software Engineering for Space Missions”, 13th SpaceOps Conference, California, USA, 2014. pp. 1790.
23. Qu, Y., Wu, H., Liu, T., and Zhao, Y., “Space Mission Data Provenance Traceability”, 15th SpaceOps Conference, Marseille, France, 2018, pp.2482.
24. Birrane, E., Ramachandran, V., and Jacobs S., "Security Standards for Space-Terrestrial Internetworks – A Multi-Dimensional Approach to Securing Shared Circuits“, 13th SpaceOps Conference, California, USA, 2014. pp. 1829.

25. Garcia Chillon, M., and Rueckert, M., "Holistic Password Management for the Ground Segment", 13th SpaceOps Conference, California, USA, 2014. pp. 1788.

26. Pajevski, M. J., Tso, K. S., and Johnson, B., "Securing Ground Data System Applications for Space Operations", 13th SpaceOps Conference, California, USA, 2014. pp. 1789.

27. Guo, H., Li, J., Liu, J., Tian, N., and Kato, N., "A Survey on Space-Air-Ground-Sea Integrated Network Security in 6G", IEEE Communications Survey & Tutorials, Vol. 24, 2022, pp. 53-87.

28. P. Martinez, The UN COPUOS guidelines for the long-term sustainability of outer space activities, Journal of Space Safety Engineering, Volume 8, Issue 1, March 2021, Pages 98-107

29. IADC Space Debris Mitigation Guidelines, IADC-02-01, Rev. 3, June 2021, Issued by IADC Steering Group and Working Group 4

30. 00ISO 24113:2023, Space Systems-Space Debris Mitigation Requirements, May 2023

31. ESPI Report 71 - Towards a European Approach to Space Traffic Management, Jan 2020

32. Space Policy Directive(SPD)-3, National Space Traffic Management Policy, The White House, 2018

33. https://www.space.commerce.gov

34. ITU Radio Regulations, https://itu.int/pub/R-REG-RR

35. 대한민국 전파법

36. https://spacenews.com/eutelsat-says-satellite-jammers-within-iran-are-disrupting-foreign-channels/

37. https://spacenews.com/hawkeye-360-gps-ukr/

38. https://www.microchip.com/, GNSS Firewall

39. B. Lee, et al, "Bandwidth Tuning of Resonator Filter Using Reduced Number of Tuning Coupling Structures" IEEE Trans. Microw. Theory Techn., vol. 67, no. 4, pp. 1496–1503, Apr. 2019.