J. Inf. Technol. Appl. Manag. 30(6): 17~29, December 2023
https://doi.org/10.21219/jitam.2023.30.6.017

ISSN 1598-6284 (Print)
ISSN 2508-1209 (Online)

UAM 항공교통관리 인프라의 사이버보안 고려사항 및 대응방안

김 경 욱*

Cyber Security Considerations and Countermeasures for UAM Air Traffic Management Infrastructure

Kyungwook Kim*

Abstract

In this paper, we aim to propose cyber security considerations and countermeasures for infrastructure and services in the UAM(Urban Air Mobility) Air Traffic Management field, which is one of the key elements of the UAM market that has not yet bloomed.

Air traffic management is an important factor for safe navigation and social acceptance of UAM. In order to realize air traffic management, infrastructure and services based on solid network connectivity must be established. And for industries where connectivity is the core component, it can become an infiltration route for cyber threats. Therefore, cyber security is essential for the infrastructure and services.

In detail, we will look into the definition of the existing air traffic management field and the cyber threats. In addition, we intend to identify cyber security threat scenarios that may occur in the newly designed UAM air traffic management infrastructure. Moreover, in order to study the cyber security countermeasures of the UAM air traffic management infrastructure, there will be analysis of the UAM operation concept. As a result, countermeasures applicable to the infrastructure and service fields will be suggested by referring to the cyber security frameworks.

Keywords : Air Traffic Management, UAM, Cyber Security, Infrastructure, Network, Service

Received : 2023. 11. 21. Revised : 2023. 12. 08. Final Acceptance : 2023. 12. 18.

※ This research was supported by "Development of CNSi Acquisition and Utilization System Reliability Verification Technology for Low-density Urban Air Mobility(UAM) Traffic Management(RS-2022-00141758)" from Korea Agency for Infrastructure Technology Advancement(KAIA).

* MS. Graduate, Sungkyunkwan University(SKKU), Hanwha Systems Co., Ltd. 188 Pangyoyeok-ro, Bundang-gu, Seongnam-Si, Gyeonggi-Do, 13524, Korea, Tel : +82-31-8091-7358, e-mail : kevinkim86@hanwha.com

1. 서 론

1.1 연구 배경 및 목적

본 연구는 아직 개화되지 않은 UAM(도심항공교통, Urban Air Mobility) 시장을 사전에 파악하고 사이버보안 관점에서 고려되어야 할 사항과 대응방안을 제안하고자 한다. UAM은 도시인구 증가와 도로교통의 혼잡, 각종 환경문제를 해결하기 위해서 등장한 새로운 개념의 이동 수단이다. 근본적으로 항공기와 같이 승객이 탑승하는 이동 수단이기 때문에 국제적인 감항 기준과 안정성 검증이 필요하며, 이와 함께 사이버보안도 동시에 고려되어야 할 사항이다.

해당 산업은 크게 제조와 서비스로 구분할 수 있으며, 제조는 UAM 기체에 대한 설계부터 조립까지 자동차 제조사와 같은 역할을 하게 된다. 서비스는 크게 지상 인프라, 관제 및 항행안전, 운항, 버티포트 등 각종 사업자로 구분되어 역할을 담당하게 된다. 기체 제작에 있어서는 미국은 Joby Aviation이 가장 선두에 있으며, 국내에서는 한국항공우주연구원이 OPPAV(미래형 유무인 겸용 개인항공기, Optionally Piloted Personal Air Vehicle)를 개발하여, 2023년 11월에 고흥항공센터에서 공개 비행을 국내 최초로 진행하였다.

서비스 분야에 있어서는 국가별로 연구과제 및 실증을 추진하고 있으며, 국내에서도 정부 주도하에 UAM 국책과제 및 실증사업을 활발하게 진행하고 있다. 최근에는 국토교통부에서 발행한 'K-UAM 로드맵'을 기반으로 한국항공우주연구원, 현대자동차, SKT, 한화시스템을 비롯하여 여러 연구기관과 민간기업이 컨소시엄을 구축해 UAM 산업을 발전시키기 위한 전략과 기술개발을 추진하고 있다.

제조와 서비스 분야를 포함한 전체 글로벌 UAM 시장은 2040년 1.5조 달러 규모로, 2021~2040년 중 연평균 30%씩 성장할 것으로 전망되며, 해당 기간 전기차 시장의 연평균 성장률 18.9%보다 더 빠른 속도의 성장세가 예측된다[Morgan Stanley Research, 2019].

새로운 산업이 등장하고 새로운 인프라와 서비스가 제공될 때마다 항상 사이버 공격에 대한 위협은 존재했다. 각종 이해관계자 간의 데이터 통신, 기체와 지상 간의 데이터 통신, 탑승 승객에 대한 정보보호 등 많은 시나리오가 있을 수 있다. 또한, 사이버 공격으로 인한 변조된 데이터 송수신이나 서비스 불가 상태가 되었을 경우, UAM의 항행 안전에 심각한 상황을 초래 할 수 있다. 이처럼 연결성이 중심에 있는 산업에서는 사이버 공격의 침투 경로가 될 수 있으며, 공격을 받을 확률도 높아지게 된다. 예를 들어 기내 무선인터넷 사용 증가, 기체 탑재 장비 및 지상 시스템 상비 증가, PC나 모바일을 통한 온라인 체크인, 정비시스템과 기체 간 연결 등 기존 항공업만 해도 다양한 사이버 공격 침투 경로가 존재한다.

국제민간항공기구 ICAO(International Civil Aviation Organization)에서 항공 사이버보안 전략을 2019년에 발표하였으며, 기존 항공업을 기반으로 제시된 전략이지만 UAM도 항공기로 분류되기 때문에 동일하게 적용받을 수 있다. 세부적으로는 국제협력, 거버넌스, 법률 및 규정, 사이버보안 정책 수립, 정보공유, 침해사고 관리 및 비상 계획, 그리고 역량 강화, 교육 및 사이버보안 문화 형성이 있다[ICAO, 2019]. 해당 전략은 9.11 테러 이후 민간항공기 자체의 무기화, 민간항공기에 대한 공격 그리고 민간항공기를 이용한 무기의 불법 운송 행위가 국제법상 범죄로 규정되었으며, 향후 민간 항공 안전의 확보 및 테러 행위 억제를 하기 위해서 진행되었다. 이를 비롯하여 국제적으로 많은 기관에서 사이버보안 영역을 연구하고 있으며, 항공 사이버보안의 중요성은 지속해서 커지는 상황이다. UAM 항행 안전에서도 사이버보안 영역은 앞으로 중요성이 커질 것으로 보인다.

따라서 본 연구를 통해 기존 항공교통관리에 있어서 사이버보안 위협 사례를 알아보고 UAM 산업으로 확장되었을 때 어떠한 사이버보안 위협 시나리오가 발생할지 알아보고자 한다. 이를 통한 UAM 항공교통관리 인프라의 사이버보안 고려사항 및 대응방안을 제시하는 것이 본 연구의 목표다.

1.2 연구 범위

전체적인 UAM 인프라는 기체, 인프라, 서비스로 구성되어 있으며, TCP/IP 기반의 네트워크망을 비롯하여, 항행 안전을 위한 센서로 구성되어 있다. 여기에 도심형 항공기인 UAM을 운영하기 위해서는 공중

LTE, 5G 통신을 비롯하여, 저궤도위성까지 연동하게 된다. 다만, 아직 개화되지 않은 UAM 시장에서 기존의 전통적인 방식의 항공 통신망을 모두 대입할 수는 없으며, 항공교통관리 인프라 전반의 사이버보안을 선행적으로 다루려고 한다.

UAM 기체에 대한 사이버보안도 중요한 요소 중 하나지만, 현재 기체 내 들어가는 각종 항전 시스템의 임베디드 단에서부터 보안성이 고려되고 있다. 따라서 본 연구에서는 UAM 인프라와 서비스를 중심적으로 항공교통관리 측면에서 발생할 수 있는 사이버보안 위협과 이에 대한 대응방안을 연구하고자 한다.

2. 항공교통관리 사이버보안 위협 유형과 사례

2.1 항공교통관리의 정의

항공교통관리의 시작은 과거로부터 항공기 운항에 있어서 안정성 확보 및 경제적 손실을 예방하기 위해서 도입되었다. 특히 매년 증가하는 항공 교통량으로 인하여 체계화된 교통관리 시스템이 갖추어져 있어야 하며, 항공에서의 사고 발생은 대규모 인명피해로 이어질 수 있으므로 항공분야에 있어서 가장 중요한 부분이라고 볼 수 있다. 또한, 기계적인 결함 혹은 시스템상의 문제 발생으로 인한 안전사고를 비롯하여, 관제사, 조종사 및 각종 이해관계자의 인적 오류, 납치 및 테러의 위험까지 발생할 수 있다. 따라서 기계, 시스템적인 내부적 요인과 인적 오류, 테러리즘과 같은 외부적 요인으로 인하여 고려해야 할 부분이 상당히 많고 광범위하다.

본격적인 항공교통관리는 1950년대 미국연방항공국 FAA(Federal Aviation Administration)의 NAS[1]가 등장하면서 시작되었다. NAS의 주요 구성요소는 항행시설, 항전장비 및 서비스, 공항 및 착륙지점, 항공 차트와 정보 서비스를 비롯하여, 각종 항공규칙, 법규, 절차가 반영되어 있는 항공교통관리 프레임워크다. 이처럼 레이다와 각종 항전장비들의 기술 발전과 비례하여 NAS가 항공교통관리에 있어서 표준으로 자리 잡게 되었다.

1980년대 이후 항공기 교통량의 증가로 공역의 혼잡도가 높아지게 되면서 각종 사고와 연착 이슈가 발생하게 되면서 안전과 경제적 손실을 보게 되었다. 비슷한 시기에 인터넷(TCP/IP)과 위성통신이 등장하면서 연결성을 극대화하려는 방안 마련으로 CNS/ATM[2]이 등장하게 되었다. CNS/ATM은 NextGen[3]으로도 불리며, 기존 NAS의 디지털 전환을 통한 연결성을 극대화하고 아키텍처를 간소화시키게 되었다. 이를 통한 항공 인프라의 안정성과 효율성을 극대화하고 예측 개념까지 도입하면서 전통적인 방식인 NAS 체계를 현대화해 나갔다.

국제민간항공기구 ICAO(International Civil Aviation Organization) 기준으로 항공교통관리를 항공교통 서비스, 공역 관리, 항공교통 흐름 관리를 통합적인 관리하고 이와 관련된 모든 이해관계자와 협력하여 안전하고 경제적이며 효율적으로 서비스를 제공해야 한다고 정의한다[ICAO, 2001]. 이를 바탕으로 항공교통관리의 유형을 분류해 보면 〈Table 1〉과 같이 항공교통서비스(ATS), 공역관리(ASM), 항공교통흐름관리(ATFM)로 분류해 볼 수 있다.

항공교통서비스(ATS)는 항공기 간 충돌 또는 항공기와 지상 장애물과의 충돌을 방지하고 항공교통의 질서 있는 흐름을 촉진하고 유지하기 위함이다. 보편적으로 항공교통관제, 비행정보업무, 경보업무 등의 서비스를 제공하게 된다.

공역관리(ASM)는 여객기, 경비행기, 헬리콥터 등 다양한 비행체가 운항할 수 있는 실질적인 공간인 공역을 스케줄링하여 관리하기 위한 목적을 가진다. 공역을 최대한 효율적으로 활용하기 위한 항공로의 설정, 공역으로의 지역항법 경로 등의 설정을 통해 차질 없이 항공관제가 될 수 있도록 하기 위함이다.

항공교통흐름관리(ATFM)는 공항 및 공역에서 운항하는 항공기의 수(수요량)를 관제기관이 관제할 수 있는 항공교통량(수용량)을 초과하지 않도록 조정하여 불필요한 운항을 줄이고, 승객 불편을 최소화하기 위함이다. 세부적으로 항공교통흐름관리 업무는 총 4가지 단계인 전략적 단계, 전전술적 단계, 전술적 단계, 사후

1) NAS(National Air Space): 항법시설, 공항, 정보, 시스템을 포함하는 미국의 영공 시스템.

2) CNS/ATM(Communication Navigation Surveillance/Air Traffic Management): 국제표준의 차세대 항행시스템.

3) NextGen(Next Generation Air Transportation System): 친환경, 효율, 안전을 표방한 차세대 항공운송시스템을 구축하려는 미국의 국가항공 장기계획(2006~2025년).

〈Table 1〉 Composition of Navigation Services

ANS (Air Navigation Service)	ATM (Air Traffic Management)	ATS (Air Traffic Service)	ATC (Air Traffic Control)	Local Control Approach Control Aerodrome Control
			FIS (Flight Information Service)	
			Alerting Services	
		ASM (Air Space Management)		
		ATFM (Air Traffic Flow Management)		

분석 단계로 구성되어 있다.

2.2 항공교통관리에 대한 위협

항공교통관리에 대한 위협은 다양하며, 이를 분류하는 방식 또한 각 연구기관 마다 차이가 있다. 대표적으로 NEASCOG(NATO/EUROCONTROL ATM Security Coordinating Group)의 경우 비행 중인 상태(Airborne)에 대한 위협과 인프라(Infrastructure)에 대한 위협으로 구분하였다[NEASCOG, 2013].

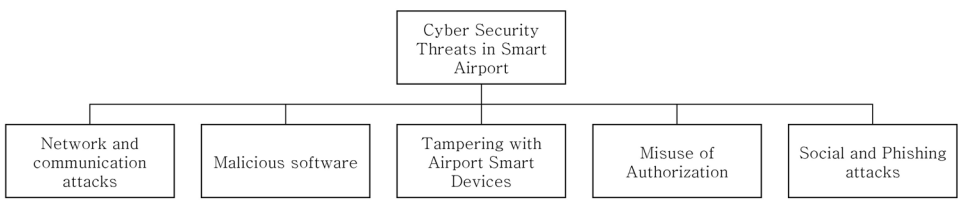
비행상태(Airborne)에 대한 위협은 크게 항공기 하이제킹, 폭발물 등 테러 행위와 항로 이탈을 통한 공역 위반 및 침범, 승객 난동 등 불법 행위로 구분할 수 있다. 인프라(Infrastructure)에 대한 위협으로는 공항, 터미널, CNS/ATM 시설물, 관제탑, 제어센터에 대한 사이버 공격을 뜻한다. 여기서 사이버 공격은 인프라 내 정보 시스템에 대한 공격을 의미하며, 세부적으로는 데이터 처리 시스템, 데이터베이스, 정보 관리 네트워크 등을 의미한다. 다시 말해서 사이버공격은 TCP/IP를 기반하고 있으며, 항공 인프라 전반에 구축된 인터넷 통신이 사이버 위협의 통로라고 할 수 있다.

또한, 항공기 시스템과 기내 혹은 지상의 네트워크 사이에서 불법 접속에 의한 사이버 침입은 일반적인 산업에서 나타나고 있는 사이버 테러나, 그 위협이 크게 다르지 않다고 하였다[Lim and Kang, 2017].

2.3 항공교통관리 사이버보안 위협 사례

항공교통관리 분야에 있어서 발생할 수 있는 사이버 보안 위협을 정의하고 대표적인 사례들을 정리하기 위해서 기존 항공시스템에 발생할 수 있는 사이버 위협을 먼저 분석하였다. 〈Figure 1〉과 같이 네트워크 연결성이 극대화되고 지능화된 스마트공항 인프라에서 발생할 수 있는 사이버 위협이 나열되어 있다.

악의적인 의도를 가진 공격자가 IT 자산을 훼손하거나 권한 상승 공격을 수행하기 위해 다양한 공격기법을 사용할 수 있으며, 기밀성, 무결성, 가용성을 위반하는 보안 사고로 이어질 수 있다. 이를 보호하기 위한 스마트공항 인프라의 안전과 서비스 연속성을 보장하기 위해 각 자산에 대한 공격 벡터를 평가할 때 (a) 네트워크 공격; (b) 악성 소프트웨어; (c) IoT 조작; (d) 승인 오용; (e) 소셜 및 피싱 공격과 같은 지표를 고려 해야한다[Lykou et al., 2018].



〈Figure 1〉 Cyber Security Threats in Smart Airport

(a) 네트워크 공격: 모든 사이버공격은 네트워크(통신)를 통해서 이루어진다. 근본적으로 통신이 발생하는 곳에 위협이 있다고 볼 수 있으며, 이를 크게 능동적 공격과 수동적 공격으로 나눌 수 있다. 능동적 공격은 스푸핑, 데이터 위변조, DDoS 등과 같이 공격자가 적극적으로 목표 시스템의 자원을 변경시키거나 시스템 작동에 영향을 미치는 공격 형태를 말한다. 반면 수동적 공격은 스캐닝, 스니핑, 트래픽 분석 등 공격자가 시스템으로부터 정보를 획득하거나 사용하려는 시도만 이루어지며, 시스템 자원 자체에 대한 영향은 주지 않는 공격 형태를 의미한다. 이와 같은 공격이 항공교통관리 인프라에서 발생한다면 네트워크 중단, 승객 탑승 지연, 항공편 취소 등 항공서비스 관점에서 심각한 영향을 미칠 수 있다. 이를 통한 항공서비스 신뢰도 상실, 평판 하락, 잠재적인 재정적 피해 등이 연쇄적으로 발생할 수 있다.

(b) 악성 소프트웨어: 네트워크를 통해서 정보수집이 이루어졌으면, 이를 바탕으로 정보 시스템을 감염시킬 수 있는 악성 소프트웨어 혹은 악성코드를 배포하게 된다. 그 대상은 항공교통관리 인프라의 PC, 서버 등이 되겠으며, 기장, 승무원, 공항 직원을 포함하여 승객의 휴대용 장치까지도 해당한다. 해당 악성코드를 통해서 인프라 전반의 정보 시스템에 대한 권한 오남용이 발생할 수 있으며, 대규모 사이버보안 위협으로 확대될 수 있으므로 주의가 필요하다. 이를 해소하기 위해서는 근본적으로 모든 정보 시스템이 최신 보안 패치가 적용된 상태여야 한다.

(c) IoT 조작: 스마트공항 시스템에는 체크인 기계, 여권 심사대, 안면인식기 등 다양한 IoT가 존재한다. 이처럼 외부로 노출되는 IoT를 포함하여, 이를 통제하기 위한 중앙 시스템, 서버, PC가 있다. 여기에는 공항 행정 전반, 그리고 승객의 개인정보까지 데이터 관리가 이루어진다. 따라서 공격자는 잠재적으로 시스템에 대한 제어권을 얻을 수 있으며, 공항 보안에 심각한 영향을 미치는 악의적인 행동을 초래할 수 있다.

(d) 승인 오용: 권한은 사용자와 시스템이 상호 작용하는 방식을 정의하는 보안 기능이다. 해당 기능의 취약점을 통해서 공격을 성공하게 되면 공격자가 해당 공격 성공 시 내부 시스템에 대한 권한을 획득하게 된다. 해당 공격은 내부자에 대한 사회공학 공격, 스피어피싱 등을 통해서 발생할 수 있다.

(e) 소셜 및 피싱 공격: 사회공학 기법을 통한 공격은 기술이 발전하여 지능화되고 시대가 변하여도 여전히 성공률이 높은 공격기법이다. 이는 사람의 심리를 이용하여 물리적 통제를 우회할 수 있다는 점에서 효과적이며, 보안 인식이 부족하고 절차를 무시하는 내부 직원에 의해서 발생할 수 있는 인적 장애로 볼 수 있다. 이를 막기 위해서는 이메일을 통한 피싱을 주의해야 하며, 계정, 신원 및 인증에 대한 접근 및 권한에 신경을 써야 한다.

위에서 설명한 스마트공항에 대한 사이버보안 위협은 항공교통관리 인프라에 있어서 공항 및 터미널에 대한 보안 위협이다. 하지만 CNS/ATM 시설물, 관제탑, 제어센터에 대한 위협을 설명하기 위해서는 추가적인 연구가 필요하다. 최근 항공 서비스는 수많은 장치와 시스템이 디지털화되고 무선으로 연결되어 있으며, 해당 분야에서 사이버보안을 보장하는 것이 점점 더 중요해지고 있다. 특히 무선통신을 통한 사이버보안 위협이 가장 큰 비중을 차지할 것으로 예상된다[Tamasi and Demichela, 2011].

EUROCONTROL EATM-CERT(European Air Traffic Management Computer Emergency Response Team)에 의하면 항공의 사이버보안 위협 중에서는 승객에 대한 사이버 공격이 대세를 이룰 것이라고 발표하였다. 이는 승객의 데이터를 다루는 운항사를 시작으로 항공기 기체 제조사, 공항 순으로 공격이 많았다. 각종 해킹 공격 기법 기준으로는 데이터 탈취(36%), 웹사이트 위변조(35%), 피싱(16%), 랜섬웨어(5%), 악성코드(5%), 그리고 기타(3%)로 나타났다[EUROCONTROL, 2021].

대표적인 항공 인프라에 대한 사이버 위협으로 2016년에 발생한 베트남항공 사이버 공격이 있었다. 해당 공격으로 약 41만 명의 승객 개인정보를 탈취하고 비행정보시스템까지 마비시키게 되었으며, 정상적인 공항 서비스가 불가하게 만들어 금전적인 피해와 안전사고 이슈를 발생시켰다. 배후로는 중국 1937CN 해커 그룹이 지목되었으며, 해당 해커 그룹은 과거에도 1,000개 이상의 베트남 웹사이트를 마비시킨 전적이 존재한다. 이는 동베트남 해에 대한 중국의 클레임을 무시하는 UN 재판소의 결정에 반발하는 정치적 의도가 숨어있는 것으로 분석된다.

또 다른 항공 인프라에 대한 사이버 위협으로는

2019년에 발생한 미국 클리블랜드 홉킨스 공항 랜섬웨어 공격이 있다. 공항 내부 정보시스템이 랜섬웨어에 감염됨에 따라 개인과 기업 데이터가 모두 암호화되어 사용할 수 없게 되었고, 이를 인질로 삼아 비트코인을 요구하게 되었다.

이외에도 많은 사이버 위협 피해가 발생했으며, 국제적으로 심각한 문제를 초래하고 있다. 이 중에는 외부로 노출되지 않은 이슈들도 상당하며, 내부적으로 처리하여 언론까지 확대되지 않는 이슈들도 존재한다. 이와 같은 사이버 위협은 전 세계적으로 지속해서 생겨나고 있다.

3. UAM 항공교통관리 인프라의 사이버보안 위협 시나리오

3.1 UAM 생태계 및 인프라 구조

UAM은 기체 제작, 버티포트 건설, 서비스 등 다양한 분야가 연계된 생태계로 고부가치 창출이 매우 큰 신사업이다. 전 세계 UAM 시장 규모는 초기 상용화 시점인 2025년 109억 달러(약 14조 원)에서 2030년 615억 달러(약 80조 원)로 성장하며, 2040년 6,090억 달러(약 793조 원)에 이를 것으로 전망했다[Ministry of Land, Infrastructure and Transport, 2023]. 이에 따라 신시장 개척을 위해서 국내외로 UAM 관련 활동들이 활발히 이루어지고 있다.

K-UAM 운영개념 1.0은 2021년에 등장하게 되었으며, 현재 해당 운영개념을 바탕으로 다양한 업종의 기업과 기관에서 참여하여, 한국형 UAM 생태계를 구축하고 있다. 해당 운영개념은 FAA와 NASA를 비롯하여, 국제민간항공기구인 ICAO 등 다양한 항공관련 국제기관의 가이드라인을 참고하여 제작되었다. 2023년 기준 현재까지도 가시화된 생태계의 모습은 없으며, 전 세계적으로 운영 개념과 컨셉이 대부분인 상황이다.

K-UAM 운영개념 1.0에는 각 이해관계자의 주요 역할과 책임이 명시되어 있으며, 정보의 흐름을 나타냄으로써 초기 K-UAM 교통체계의 구조라고 볼 수 있다. 초기 K-UAM 교통체계에는 크게 교통관리 전반을 담당하는 PSU[4], UAMO[5], VPO[6], SDSP[7], 그리고 공공 업무를 담당하는 기타 이해관계자 등으로 구성되어 있으며, 각 이해관계자별로 데이터 흐름이 발생하게 된다.

UAMO는 PSU, SDSP 및 VPO로부터 운항정보[8]와 운항안전정보[9]를 확보하여 비행계획 수립에 적용한다. PSU는 이미 승인된 타 비행계획과 운항지원정보의 종합분석을 통해 UAMO가 신규 제출한 비행계획의 안전성을 확인하여 이를 승인하거나 UAMO와의 협력을 통해 비행계획을 조정한다.

PSU는 UAM 감시 정보, UAM 항공기의 실시간 운항정보와 기타 국가공역시스템 사용자 정보를 종합하여 실시간 교통관리 서비스를 수행하고 필요시 이해 관계자들과 정보를 공유한다. 여기에 하나의 PSU만 있는 것이 아니기 때문에 각 지역 혹은 권역에 대한 항공교통관리를 진행하는 다수 PSU간 네트워크를 별도로 구성한다. 이를 통해 관련 정보를 공유함으로써 서로 다른 UAM 교통관리서비스를 제공받는 UAM 항공기들 사이에서 안전한 분리가 이루어질 수 있도록 실시간으로 UAM 교통을 관리하게 된다.

VPO는 버티포트 가용성, UAM 항공기 운용상태, 실시간 수용량 변화, 버티포트 권역 감시현황 등의 정보를 PSU와 UAMO에게 제공한다. 이 정보는 UAMO의 비행계획 수립, PSU의 비행계획 승인, 이착륙 관리와 분리 서비스 제공에 이용된다. PSU는 버티포트의 실시간 수용량 변화 정보를 수요량과 수용량 관리에 적용함으로써 보다 효율적인 교통관리 서비스를 제공할 수 있다. VPO는 UAMO와 PSU로부터 비행계획이나 실시간 비행 정보(예상 도착시간 등)를 제공받아 효율적인 버티포트 운영에 활용할 수 있다. VPO는 안전하고 효율적인 UAM 운용을 위해 버티포트 권역 내에서 (이착륙 과정 포함) PIC[10]와 직접 통신할 수 있다.

4) PSU(Provider of Services for UAM): UAM 교통관리서비스 제공자.
5) UAMO(UAM Operator): UAM 운항자 혹은 운항사.
6) VPO(Vertiport Operator): 버티포트 혹은 공항 운영자.
7) SDSP(Supplemental Data Service Providers): 운항지원정보 제공자.
8) 운항정보: 회랑가용성, 출도착지 버티포트 가용성 등 운항에 필요한 기본 정보.
9) 운항안전정보: 기상, 제한공역 정보 등 운항안전에 필수적인 부가정보.
10) PIC(Pilot In Command): UAM 조종사.

3.2 발생 가능한 사이버보안 위협 시나리오

UAM 시장은 아직 개화되지 않은 상황으로 UAM 항공교통관리라는 것이 존재하지 않는다. 다만, UAM 관련 인프라가 구축되기 이전에 사이버보안에 대한 고려사항과 대응방안은 마련이 되어 있어야 안전하고 서비스 연속성을 보장할 수 있을 것이다. UAM 인프라 시스템 내 아직 식별되지 않은 기계적 오류로 인한 위협을 포함하여, 사이버 위협까지 발생하게 되면 인명피해로 커질 수 있다.

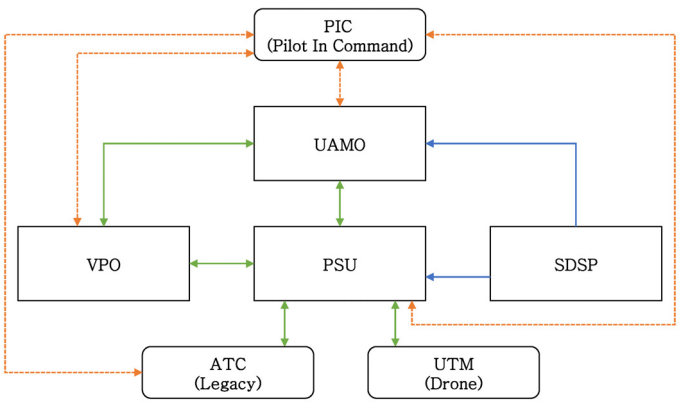
수십 년 동안 운항한 항공기의 경우 단순하고 가벼운 통신 프로토콜을 사용하여, 항행 안전성 및 안정성을 극대화했다. 반면 UAM은 기존의 전통적인 항공기와 다르게 연결성이 극대화된 IoT 디바이스에 가깝다. 이는 기존 내연기관의 자동차에서 환경문제로 인한 전기차로의 전환됨에 따라 자율주행 기술이 적용되어 발전하게 된 배경과 유사하다. 기체의 크기를 떠나서 동력원이 기존에 연료를 소모하는 내연기관 방식에서 전통 모터로 변경된 것이 UAM의 기본적인 기체 형식이다. 궁극적으로 나아가 자율주행, 무인운항, 즉각적인 이용을 목표로 하므로 기존 항공기와 차이점이 존재한다. 따라서 UAM 생태계는 항공분야의 한 가지 축에 속하지만, 사업의 특성에 따라서 새로운 모빌리티 생태계로 구성될 것이다.

2장에서 설명한 항공교통관리에 대한 위협과 사이버보안 위협 사례를 바탕으로 포괄적인 배경 설명이 진행되었다. 이를 바탕으로 UAM 항공교통관리 인프라에 대한 사이버보안 위협 시나리오를 재구성해 볼 수 있다. 그전에 〈Figure 2〉와 같이 초기 K-UAM 교통체계의 구조를 간소화했으며, PSU를 비롯하여 주요 이해관계자들만 구성하여 데이터 통신의 방향성을 표현했다. 이를 바탕으로 각 이해관계자 간의 주요 데이터 통신 경로를 이해할 수 있으며, 크게 유무선 양방향 통신과 정보제공 및 수집을 위한 단방향 통신으로 구분할 수 있다. 여기에 각종 항공 시스템과 서버/PC 등 각종 IT 자산을 포함하여, 센서 및 IoT 장비가 구축될 수 있다. 이를 바탕으로 UAM 인프라에 있어서 공격의 대상 및 경로를 파악할 수 있으며, 간접적으로 영향을 받을 시스템을 식별할 수 있게 된다.

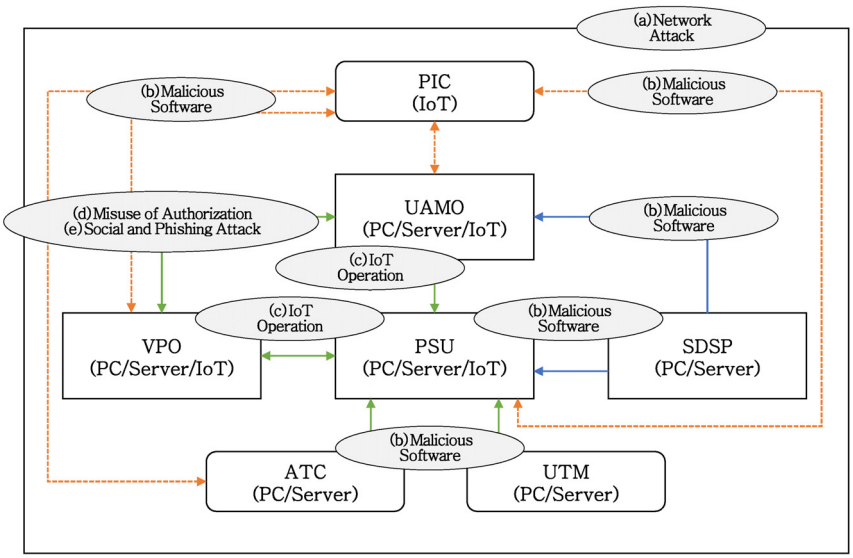
초기 K-UAM 교통체계의 구조를 기반하여 발생할 수 있는 사이버보안 위협 시나리오를 구성해 보면 〈Figure 3〉과 같이 대입해 볼 수 있다.

(a) 네트워크 공격은 UAM 인프라 전반이 공격 대상이며, 연결성이 존재하는 모든 구간이 공격에 대한 경로가 될 수 있다. 능동적 공격과 수동적 공격 모두 가능하며, DDoS와 같이 가용성에 침해를 주는 공격 외에도 간접적으로 해당 인프라에 대한 정보를 획득하기 위한 스캐닝 공격이 주로 발생할 가능성이 크다. 공격 대상에 대한 환경을 먼저 분석하기 위해서 해당 구간에 대한 대응방안을 수립해야 한다.

(b) 악성 소프트웨어는 UAMO, PSU, VPO 시스템 내 PC, 서버, 그리고 IoT 장비를 통해서 악성코드 감염이 이루어질 수 있다. 또한, 해당 자산에서 감염이 이루어지고 끝나는 것이 아니라 네트워크 접점을 통해서 수평 이동이 가능하며, 각 이해관계자의 자산까지 침해할 수 있기에 주의가 필요하다.



〈Figure 2〉 Simplified Structure of K-UAM Transportation System



〈Figure 3〉 Cyber Security Threats for UAM Infrastructure

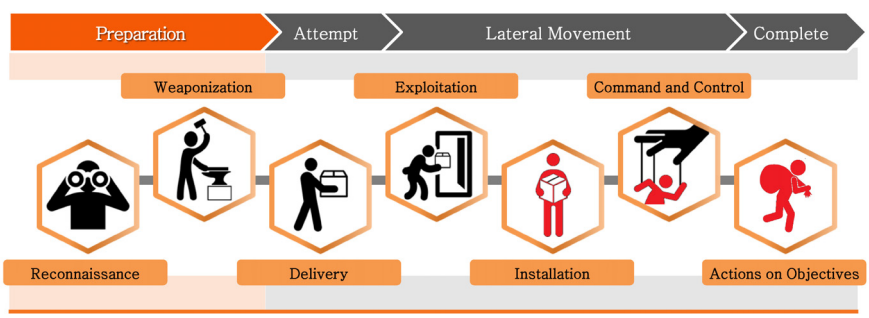
(c) IoT 조작은 UAM 인프라의 이해관계자 중에서 특히나 IoT를 많이 다루는 곳에서 위협이 발생할 가능성이 크다. UAMO를 비롯하여, 특히 버티포트 운영 및 승객의 물리적인 보안까지 신경을 써야 하는 VPO가 신경을 써야 하는 분야라고 볼 수 있다.

(d) 승인 오용과 (e) 소셜 및 피싱 공격은 (a) 네트워크 공격과 마찬가지로 공격의 초기 단계에서 실행되는 공격기법이다. 내부 시스템의 환경구성을 이해해야 악성코드를 배포할 수 있을 것이며, 획득된 정보를 바탕으로 조작 및 파괴를 진행하게 된다. 이와 같은 부분을 고려하여 전반적인 UAM 교통체계 구조 내 시스템과 IT 자산에 대한 사이버보안 조치 및 대응방안을 수립해야 한다.

4. UAM 항공교통관리 인프라의 사이버보안 대응방안

4.1 적용 가능한 사이버보안 프레임워크

3장에서 제시된 UAM 생태계 및 인프라 내에서 발생할 수 있는 사이버보안 위협에 대응하기 위한 프레임워크를 분석하였다. 세계적으로 표준화된 프레임워크는 2011년에 미국의 대표적인 방위산업체인 Lockheed Martin의 Cyber Kill Chain(이하 CKC)이 있다. CKC는 사이버 공격에 대해서 일련의 단계를 제공하여 다음 단계 혹은 최종적인 공격자의 목표에 도달하기 전에 방어하는 메커니즘으로 구성되어 있다. 〈Figure 4〉와

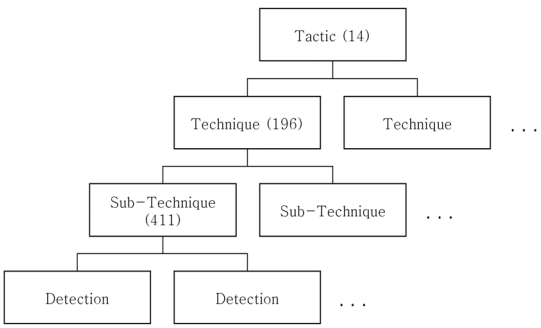


〈Figure 4〉 Lockheed Martin's Cyber Kill Chain Framework

같이 해당 프레임워크는 관찰, 제작, 배달, 침투, 설치, 원격조정, 해킹과 같이 총 7단계로 구성되며, 공격자의 행위 및 침해시도 상태를 관리하기 위해서 개발되었다.

관찰과 제작 단계의 경우 해킹 준비 단계로 공격자의 영역으로 구성된다. 공격자는 목표로 하는 대상에 대해서 정보분석을 진행하며, 이를 바탕으로 공격의 범위, IP 대역, 이메일 주소, 취약점 분석 등을 수행한다. 수집된 데이터를 바탕으로 공격자는 악성코드를 제작하게 되며, 해킹 시도를 준비하게 된다. 이후 공격자는 해킹 메일, 악성 봇, 스피어 피싱 공격 등을 실시하여, 제작된 악성코드 배달을 시도하며, 보안장비를 우회하거나 시스템 취약점을 활용하여 침투를 시도하게 된다. 성공적으로 악성코드가 설치되면 이를 바탕으로 내부 확산을 시도하게 되며, 이때부터 공격자는 내부 시스템에 대한 접근 권한을 획득하게 된다. 마지막으로 내부 시스템에 대한 기밀자료 유출, 시스템 파괴 등 악의적인 행위를 실시하여, 임무를 완료하는 형태로 진행된다.

이와 같이 CKC는 사이버보안 대응방안으로 개념과 큰 틀을 제공한 것은 분명하다. 다만 CKC의 각 단계에 따른 공격자의 행위를 시간의 흐름에 따라 구분했을 뿐, 단계별로 어떤 기술들이 사용되고 관련된 공격 도구나 해킹그룹 등에 대한 정보를 제공하지는 않는다. 이러한 한계점을 극복하기 위해서 등장한 것이 MITRE ATT&CK 프레임워크라고 볼 수 있으며, 공격자의 실질적인 행위를 기반하여 전술적인 공격 목표와 각 행위의 연관성을 전달하기에 적합하다[Naik et al., 2022].



〈Figure 5〉 MITRE ATT&CK Structure

특히 내부자의 공격에 대한 사이버보안 대응방안을 제공했다는 점에서 의의가 크다. 또한, MITRE ATT&CK은 공격자의 전술(Tactics), 기술(Techniques), 절차(Procedures)를 분석하여 다양한 해킹 그룹의 공격기법들을 데이터로 관리하고 체계화 시켜 나가고 있다[Naik et al., 2022].

2023년 4월 기준 MITRE ATT&CK에는 14개의 전술, 196개의 기술, 그리고 411개의 하위 기술로 구성되어 있다.

기존 CKC와 가장 큰 차이점은 개념적인 프레임워크에서 끝나지 않고 실제 사이버 공격의 actor를 정의하고 분류할 수 있는 도구로 활용된다는 것이다[Choi et al., 2022]. 또한, 기존의 시그니처 기반 공격자 그룹을 식별 혹은 분류 기술이 가지고 있던 단점을 극복하기 위해서 MITRE ATT&CK 프레임워크를 활용한 연구가 활발히 진행되고 있다.

대표적인 연구로는 공격 벡터 간의 코사인 유사도(Cosine similarity)를 이용하여 공격 그룹 유사도를 산출하고, 각 전술(Tactic)에 대한 영향도를 고려하여 합계를 구해서 사이버 공격 그룹을 분류하는 연구를 진행하였다[Shin et al., 2021].

따라서 국제적으로 표준화된 사이버보안 프레임워크인 CKC 혹은 MITRE ATT&CK을 바탕으로 3장에서 제시한 발생 가능한 사이버보안 위협 시나리오를 대입하여, UAM 인프라에 대한 사이버보안 대응방안을 수립해야 할 것이다.

4.2 사이버보안 대응방안

CKC 혹은 MITRE ATT&CK과 같이 전통적인 사이버보안 프레임워크를 2장에서 설명된 (a) 네트워크 공격; (b)악성 소프트웨어; (c) IoT 조작; (d) 승인 오용; (e) 소셜 및 피싱 공격에 대입하여 UAM을 위한 사이버보안 대응방안을 수립할 수 있다. 여기에 추가로 각종 사이버 위협에 대한 재발방지대책과 복원력 혹은 탄력성을 확보하려는 방안도 생각해 볼 수 있으며, 해당 위협을 해소하기 위한 완화 조치 방안까지 정리해 볼 수 있다. 그 결과, 〈Table 2〉와 같이 UAM 인프라 기준의 사이버보안 대응방안을 수립하였다.

해당 표는 UAM 교통체계 내에서 발생할 수 있는 사이버보안 위협 시나리오를 전반적으로 다루고 있다. 크게 5가지 공격 유형을 기반으로 공격 대상과 경로, 이를 바탕으로 영향을 받을 시스템, 그리고 해당 시스템의 보안성을 보장하고 강화하려는 조치 및 대응방안으로 구성했다.

〈Table 2〉 Cyber Security Countermeasures for UAM Infrastructure

Cyber Security Countermeasures for UAM Infrastructure			
Category	Target & Route	Affected System	Mitigation Actions
(a) Network Attack	• Web service • Network service • UATM communication • Wireless communication • ICS/SCADA system • VPO CCTV system • Baggage handling system • VPO systems and IT assets	• Overall UAM infrastructure • PSU systems and IT assets • VPO systems and IT assets • UAMO systems and IT assets • Baggage handling system	• Enhancing security solutions such as FW, IDS, IPS, etc. • Enhanced system security • Apply network separation • ISP multiplexing • Apply strong user authentication security • Change Admin default PW • Apply IoT equipment control system • Apply data encryption
(b) Malicious Software	• Network service • ICS/SCADA system • Crew IoT equipment • Passenger smartphones • Passenger electronic devices • PC/Server	• PSU systems and IT assets • VPO systems and IT assets • UAMO systems and IT assets • Passenger management system • Physical security equipment (Security gate, etc.)	• Enhancing security solutions such as FW, IDS, IPS, etc. • Vaccine engine update • Apply IoT equipment control system • ISP multiplexing • Grant minimal access rights • SW/HW firmware update • Apply application security system
(c) IoT Operation	• Passenger ticketing system • Baggage handling system • Passenger boarding system	• LAN • VPO systems and IT assets • Passenger management system	• Prohibit use of external IoT devices • Advancement of security solutions such as FW, IDS, IPS, etc. • Apply data encryption • Enhanced physical security and surveillance
(d) Misuse of Authorization	• Insider(pilot, flight attendant, vertiport ground staff, etc.) threat • ICS/SCADA system • UAM air traffic control system (UATM) • Facility management system • Access control and surveillance equipment • Various IT assets	• Facility Management System • Vertiport Manager • VPO systems and IT assets • UAMO systems and IT assets	• Change the default PW of IoT devices • Apply IoT equipment control system • SW/HW firmware update • Minimal authorization and data classification • Apply data encryption • Apply strong user authentication security • Apply user access control system
(e) Social and Phishing Attack	• Outsiders(passengers, general public, hackers, terrorists, etc.) threat • VPO systems and IT assets • Facility management system • ICS/SCADA system • Various IT assets	• Facility Management System • Vertiport Manager • VPO systems and IT assets • UAMO systems and IT assets	• Enhancing security solutions such as FW, IDS, IPS, etc. • SW/HW firmware update • Apply spoofing prevention system • Apply strong user authentication security • Apply application security

(a) 네트워크 공격은 UAM 인프라 전반으로 이해관계자 구분 없이 모든 시스템이 영향을 받을 수 있다. 이에 대응하기 위해 필수적인 방화벽을 비롯하여 탐지된 로그의 사후 분석을 위한 IDS(Intrusion Detection System)와 침해시도를 원천 차단 할 수 있는 IPS (Intrusion Prevention System)를 구축해야 한다. 또한, 다중회신을 이용하여 DDoS 공격에 대응해야 할 것이며, 네트워크상의 데이터는 암호화 통신을 이용하는 것이 바람직하다.

(b) 악성 소프트웨어의 공격 경로는 조종사 혹은 승객의 IoT 장비로부터 시작되는 경우가 많을 것이다. 또한, 이를 관리하기 위한 버티포트 내 PC와 서버들이 공격이 경로가 될 수 있을 것이며, 승객의 UAM 탑승을 방해하고 UAM 항행 업무를 마비시킬 위협이 존재한다. 이에 대응하기 위해서 내부 자산에 설치된 백신의 엔진을 최신버전으로 유지해야 할 것이며, 스마트폰과 전자기기를 사용하는 UAM 관계자는 최소한의 권한만 부여해야 한다. 추가로 SW와 HW에 대한 펌웨어 업데이트를 비롯하여, 애플리케이션 보안 체계를 구축해야 할 것이다.

(c) IoT 조작의 경우 승객 ticketing 시스템, 수하물 처리 시스템, 승객 탑승 시스템 등이 공격 경로가 될 수 있으며, PSU나 UAMO보다는 버티포트 운영을 담당하는 VPO 시스템과 IT 자산이 영향을 받을 수 있다. 따라서 VPO 직원의 경우 외부 IoT 장비 사용을 금지하고 데이터 암호화를 도입해야 한다. 추가로 사이버보안뿐만 아니라 버티포트 내 물리적 보안 및 감시에 대해서도 강력한 대응이 필수적이다.

(d) 승인 오용과 (e) 소셜 및 피싱 공격은 공통점이 많으며, 크게 공격자의 신분에 따라서 구분될 수 있다. 내부자와 외부자를 통한 위협으로 구분하고 있으며, 내부자의 경우 UAM 기장, 버티포트 지상 직원 등 UAM 인프라 내부에서 활동하는 직원을 얘기한다. 외부자의 경우 이와 무관한 승객, 일반인, 해커, 테러리스트 등으로 볼 수 있다. 이처럼 공격자의 신분에 따라서 대응방안이 달라질 수 있으며, 내부자 경우 IoT 장비를 통제하고 보안 인식 교육을 주기적으로 실시하는 것이 중요하다. 외부자의 경우 스푸핑을 방지하기 위한 체계를 구축하고, 악성 이메일 열람 금지 및 신고 절차를 교육해야 한다. 또한, 버티포트 내에서 신분을 확인하고 검증을 철저히 해야 할 것이다. 추가로 사용되는 자산들에 대한 보안 취약점 진단 및 테스트를 주기적으로 실시하여, 보안성을 강화해야 할 것이다.

5. 결 론

본 연구는 아직 개화되지 않은 UAM(도심항공교통, Urban Air Mobility) 시장의 핵심요소 중 하나인 항공교통관리 분야의 인프라와 서비스에 대한 사이버보안 고려사항 및 대응방안을 분석하였다.

UAM의 안전한 항행과 사회적 수용성을 위해서는 항공교통관리가 중요한 요소로 분석되었으며, 항공교통관리를 실현하기 위해서는 견고한 네트워크 연결성을 바탕으로 한 인프라와 서비스가 구축될 것이다. 이처럼 연결성이 중심에 있는 산업의 경우 사이버 공격의 침투 경로가 될 수 있으며, 이에 대한 사이버보안은 필수적이다.

세부적으로 기존의 항공교통관리 분야의 정의와 이에 대한 위협, 그리고 대표적으로 발생한 사이버보안 위협 사례에 대해서 분석했다. 또한, 새롭게 설계될 UAM 항공교통관리 인프라에 있어서 발생할 수 있는 사이버보안 위협 시나리오 식별하였으며, 이를 바탕으로 UAM 인프라와 서비스 분야에 있어서 적용할 수 있는 사이버보안 프레임워크를 수립하여 대응방안을 마련하고자 하였다.

결국 사이버보안은 통신이 완벽히 보장되어 있다는 전제하에 UAM 인프라가 운영되어야겠으나, 네트워크가 있는 곳에 완벽한 보안이라는 것은 실현되기 매우 어렵다. 또한, K-UAM 운영개념이 개정되고 있는 상황으로 구체적인 환경구성을 파악하기 위해서는 많은 이해관계자들간의 협력과 공감대 형성이 필수적이다. 따라서 UAM 인프라 상용화 단계에 돌입하기 이전에 각종 이해관계자의 접점으로부터 시작되는 사이버보안 위협을 사전에 파악하고 발생할 수 있는 시나리오를 설계해 보는 데 의의를 두었다.

추가로 사이버보안은 사고가 발생하기 이전에 피해를 최소화하는 데 중점을 둔다. 사고 발생 후에 조치하는 것은 향후 유사한 형태의 위협에는 대응할 수 있겠으나, 새로운 기법의 공격에 대해서는 대응이 불가하다. 따라서 본 연구를 통해 UAM 인프라가 수립되기 이전에 UAM 인프라 환경을 구성하여, 구간별로 어떠한 보안 솔루션을 도입하거나 대응 정책을 세워야 하는지 방향성을 제시하고자 했다.

또한, 본 연구를 바탕으로 국토교통과학기술진흥원의 "저밀도 도심항공모빌리티(UAM) 교통관리 CNSi[11] 획득 활용 체계 신뢰성 검증 기술 개발" 과제의 연구 항목 중 하나인 UAM 사이버보안 관리시스템 아키텍처 설계 시 내용을 반영하여, 향후 UAM 사이버보안 관련 연구에 기여하고자 한다.

향후에는 본 연구를 바탕으로 분석된 사이버보안 프레임워크를 준용하여 기존 국방과 민간분야의 UAM 사이버보안 관리체계를 구성할 예정이다. 구체적으로 보안성 향상 및 보안관리 효율성 증대를 위한 침입 감시, 침해사고 대응방안, 정책관리, 구성관리, 보안 솔루션 관리 등을 통합적으로 관리할 수 있는 사이버보안 통합체계를 구축하는 것을 목표로 한다.

References

〔1〕 Choi, C. H., Shin, C. H., and Shin, S. U., "Cyber Attack Group Classification Based on MITRE ATT&CK Model", Journal of Internet Computing and Services, Vol. 23, No. 6, 2022, pp. 1-13.

〔2〕 EUROCONTROL, "EUROCONTROL EATM-CERT Services Think Paper #12 - 5 July 2021", 2021.

〔3〕 ICAO, "Procedures for Air Navigation Services: Air Traffic Management (Doc 4444)", 2001.

〔4〕 ICAO, "Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy", 2019.

〔5〕 Lim, I. K. and Kang, J. Y., "Security Problems in Aircraft Digital Network System and Cybersecurity Strategies", Journal of Advanced Navigation Technology, Vol. 21, No. 6, 2017, pp. 633-637.

〔6〕 Lykou, G., Anagnostopoulou, A.. and Gritzalis, D., "Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls", Sensors, Vol. 19, No. 1, 2018, p. 19.

〔7〕 Ministry of Land, Infrastructure and Transport, "Korean Urban Air Transportation(K-UAM) Roadmap", 2020.

〔8〕 Morgan Stanley, "Flying Cars: Investment Implications of Autonomous UAM", 2019.

〔9〕 Naik, N., Jenkins, P., Grace, P., and Song, J., "Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model", 2022 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2022, pp. 1-7.

〔10〕 NEASCOG, "Manual for National ATM Security Oversight", 2013.

〔11〕 Shin, Y., Kim, K., Lee, J. J., and Lee, K., "ART: Automated Reclassification for Threat Actors based on ATT&CK Matrix Similarity", 2021 World Automation Congress (WAC), Taipei, Taiwan, 2021.

〔12〕 Tamasi, G. and Demichela, M., "Risk assessment techniques for civil aviation security" Reliability Engineering & System Safety, Vol. 96, 2011, pp. 892-899.

11) CNSi(Communication Navigation Surveillance and information): 통신・항법・감시・정보 시스템.

저자소개

김 경 욱

현재 한화시스템(주) UAM인프라 기술개발센터에서 전문연구원으로 재직 중이다. 성균관대학교 기술경영학 석사학위를 취득하였고, (주) 안랩 사이버 침해사고 대응분석가로 활동하였다. 주요 관심 분야는 사이버보안, 시스템 엔지니어링, 사업 개발, 전략 기획 등이다.