Journal of the KNST

2023; Vol.6, No.1; pp. 001-008

ISSN: 2635-4926 https://doi.org/10.31818/JKNST.2023.03.6.1.1

Check for updates

Received: 2023/01/11
Revised: 2023/01/25
Accepted: 2023/02/24
Published: 2023/03/31

*Corresponding Author:

Jin-Hwan Koh

Department of Electronic Engineering, Gyeongsang National University, Jinju-si, Jinjudae-ro 501 Gyeongsangnam-do, 52828, Korea

Tel: +82-55-772-1726

E-mail: jikoh@gnu.ac.kr

Abstract

현재 주요 선진국들은 적성국가 및 단체의 사이버 공격에 대비하기 위해 역량을 집중하고 있다. 특히, 항공기는 사이버공격으로 추락 및 인명피해를 비롯한 심각한 문제가 발생할 수 있으므로 철저한 대비가 필요하다. 따라서 본 논문에서는 항공기 사이버보안 선진국인 미 해군의 사례를 알아보고 우리 해군 및 군용항공기에 적용할 수 있는 사이버보안 제도에 대한 연구 및 향후 발전방향을 제시하였다.

Currently, major developed countries are concentrating their capabilities to prepare for cyber attacks by enemy countries and organizations. In particular, aircraft need to be thoroughly prepared because cyber attacks can cause serious problems, including falls and casualties. Therefore, in this paper, we investigated the cases of the U.S. Navy, an advanced aircraft cybersecurity country, and presented research on cyber security systems that can be applied to Korean Navy and military aircraft and future development directions.

Keywords

사이버보안(Cyber Security),
미 해군성 항공체계사령부(NAVAIR),
MIL-HDBK-516C,
미 해군성 항공체계사령부 감항당국(AIR-4.0P)

군용항공기 사이버보안에 대한 연구 및 발전방향

Research and Development Direction of Military Aircraft Cyber Security

고기성[1], 장영현[1], 박인수[2], 고진환[3*]

[1]해군 전력분석시험평가단 감항인증실 전문군무경력관
[2]공군 52시험평가전대 감항인증실 전문군무경력관
[3]경상국립대학교 공과대학 전자공학과 교수

Gi-Sung Ko[1], Yong-Hyun Jang[1], In-Soo Park[2], Jin-Hwan Koh[3*]

[1]Senior Manager, Office of Airworthiness, Force Analysis Test & Evaluation Group, ROK Navy
[2]Senior Manager, Office of Airworthiness, The 52nd Test & Evaluation Group, ROK Air Force
[3]Professor, Dept. of Electronic Engineering, Gyeongsang National University

1. 서론

전 세계적으로 빅데이터, IoT, 클라우드, 인공지능 등 새로운 ICT 환경이 빠르게 진전되면서, 새로운 ICT 환경에서의 사이버 위협이 지속적으로 증가하고 있으며, 점점 고도화·정교화되는 사이버위협은 사회 경제적 피해 규모를 지속적으로 증가시킴은 물론, 국가안보와 경제안정에도 중대한 위협이 된다[1].

더불어, 디지털 기술과 인공지능 기술의 비약적인 발전으로 항공기 시스템도 빠르게 디지털화되고 있다. 항공전자 시스템은 물론 전기, 유압, 랜딩 기어 등 컴퓨터에 의해 제어되는 시스템이 보편화되고 있으며, 이 중심에는 소프트웨어가 있다. 소프트웨어에 의한 시스템의 디지털화는 제어의 정확성을 높이고 사람이 수행하는 부분을 자동화함으로써 오류를 줄여 좀 더 안전하게 항공기를 운용할 수 있는 장점이 있지만, 외부에서 불법 또는 악의적인 목적으로 컴퓨터에 접근하는 해킹을 당한다면 해당 시스템에 위험한 결과를 초래할 수 있는 단점이 존재한다.

이미 인터넷으로 보편화된 네트워크 사회에서 컴퓨터 바이러스에 의한 정보의 탈취 및 시스템 손상은 사회적 문제로 대두될 정도로 피해가 증가하고 있으며, 외부와 단절되어 비교적 안전한 영역으로 인식되었던 항공기 시스템도 인터넷과 직/간접적으로 연결이 필요하게 되면서 사이버 분야에서 더 이상 안전한 영역이 아니게 되었다. 즉, 컴퓨터로 제

어되는 시스템이라면 그 컴퓨터는 어떠한 방법을 통해 외부로부터 해킹될 수 있으며, 외부와 유/무선의 형태로 정보가 소통되도록 연결되어 있는 경우, 이를 통해 해당 시스템이 침해당할 취약성이 존재한다.

Fig. 1과 같이 현대의 첨단 항공기는 전자기술의 발달로 항법, 비행제어, 무장운용과 같은 임무수행 등에 필요한 전자 장비 및 통신장비와 작전의 효율성을 높이기 위한 데이터링크 장비들이 꾸준히 증가하는 추세이며, 이로 인해 적성국가 및 테러리스트들이 악의적인 목적을 가지고 사이버공격을 가했을 경우 항공기와 탑승객들의 안전에 치명적인 결과를 가져올 수 있다.

Fig. 1. 군용항공기 사이버 전장 환경의 무기체계 구성품 및 네트워크

마찬가지로 군용항공기도 사이버공격으로 피해를 입었을 경우 항공전력 운용 및 작전 수행에 많은 영향을 받게 되어 결국 전쟁의 승패를 좌우하는 결과를 초래할 수 있다. 미국 등의 사이버보안 선진국에서는 일찍이 사이버보안의 중요성을 인지하고 관련 제도의 마련과 조직을 구성함으로써 이와 같은 문제를 해결하고자 노력하고 있으며, 관련 연구들도 활발하게 이루어지고 있다. 하지만, 국내에서는 아직 항공기 시스템에 대한 사이버보안 제도 및 조직이 전무한 실정이다.

따라서, 본 연구에서는 사이버보안 선진국인 미국 해군의 제도 및 관련 조직 사례 조사를 통해 국내에 적용할 수 있는 방안을 모색하였으며, 우리 해군 및 해병대에서 운용하는 항공기를 비롯하여 공군 및 육군에서 운용하는 모든 군용항공기에도 적용할 수 있는 사이버보안 제도에 대한 기틀을 마련하고자 한다.

2. 본론

2.1. 사이버보안(cyber security)의 정의/관련 훈령 및 표준

사이버보안에 앞서 사이버공간과 정보보안의 개념을 먼저 짚고 넘어갈 필요가 있다. 우선, 정보보안이란 정보의 수집, 가공, 저장, 검색, 송/수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적 방법과 기술적 방법을 의미한다.

미국의 표준기술연구소(NIST: National Institute of Standard and Technology)에서 발행한 컴퓨터 보안 핸드북[NIST 95]에는 정보보안에 대해 기밀성(confidentiality), 무결성(integrity), 가용성(availability) 3개 요소가 Fig. 2와 같이 유기적으로 연결되어 있으며 정보 데이터는 기밀성, 무결성, 가용성 모두를 만족해야 하는 것으로 기술하고 있다[2].

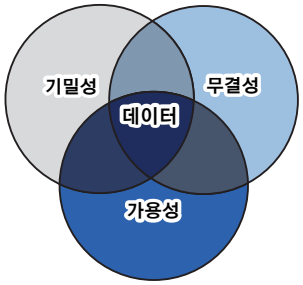

Fig. 2. 보안의 3요소

사이버공간은 '컴퓨터에 의해 제어되는'이라는 뜻을 지닌 단어 'cyber'와 '공간, 장소 혹은 시간'을 의미하는 단어 'space'가 결합된 것으로, 미국에서는 사이버전을 위한 사이버 공간의 전(全) 영역으로 정의하였다[3].

사이버보안은 컴퓨터, 전자통신 시스템, 전자통신서비스, 유선통신, 전자통신과 그 안에 담긴 정보에 대해 피해를 예방, 보호, 복원하여 기밀성, 무결성, 가용성, 인증, 부인방지를 보장하는 것을 의미한다[4].

국내에서는 대통령 훈령인 국가사이버안전관리규정 제2조 제3항에 명시된 바와 같이 "사이버안전이라 함은 사이버공격으로부터 국가정보 통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다"라고 정의하고 있다[5].

항공기 보안에 대한 설계, 평가, 환경 및 운용에 관한 사항은 Table 1과 같이 NextGen(Next Generation Air Transportation System)과 SESAR(Single European Sky ATM Research)에서 보안 관련 문서들을 다루고 있다[6].

항공기 시스템의 사이버보안은 시스템 개발 및 설계 단계에서 강력한 보안 개념이 포함되어야 한다. 소프트웨어 개발, 분배, 디지털 데이터의 기능, 리소스 관리 및 운용을 위한 항공기 내/외부 접근제어에 대한 보안 개념

을 수립하여야 한다[7]. 미 국방부에서는 Table 2와 같이 사이버보안 관련 규정과 지침이 수록된 국방정책 및 기술표준을 발간하여 사이버보안 개념 수립에 적극 활용하고 있다.

Table 1. 항공기 사이버보안 관련 절차 및 규정

구분	제목
ICAO Annex 17	Security
RTCA DO-178	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-254	Design Assurance Guidance for Airborne Electronic Hardware
RTCA DO-236	Security Assurance and Assessment Processes for Safety-related Aircraft Systems

Table 2. 미 국방부 사이버보안 관련 국방정책 및 기술표준

구분	제목
DoD Instruction 5000.02	Operation of the Adaptive Acquisition Framework
DoD 8500.01	Cyber Security
DoD 8510.01	Risk Management Framework(RMF)
SECNAVINST 5239.3c	Cyber Security Policy
SECNAVINST 5239.22	Cyber Security Safety Program
SECNAVINST 5239.20	Cyberspace IT and Workforce
NAVAIR	Airworthiness and Cybersafe Process Manual
JROCM	System Survivability
VCNO Joint Memo	Cybersecurity in systems engineering
IATA 2015-2016	Cybersecurity Standards

국내의 항공기 보안에 대한 현행 법률은 국토교통부 '항공보안법' 제5장 항공보안장비 등 제27조(항공보안장비 성능 인증 등) 및 국가정보원 '사이버 안보 업무 규정'이 있다.

군용항공기 감항인증 분야에서 사이버보안에 대해 다루고 있는 부분은 방위사업청장이 고시한 표준감항인증기준(Part I) 15장 "컴퓨터자원과 소프트웨어" 분야에 기술된 1개 기준이 있으며 내용은 아래와 같다[8].

15.2.8 보안기술 (Security techniques)

기준(Criterion) : 사용된 보안기술이 안전하게 구현됨을 검증한다.

표준(Standard) : 안전 필수기능(SCF)을 보호하기 위한 보안 요구도가 처리 아키텍처에 적용된다. 식별된 보안 취약성에 대해, 보안 기술들이 안전필수기능(SCF)의 저하효과를 가져오지 않도록 설계되어 구현되었음을 보장한다. 육군과 해군의 경우 시스템 처리 아키텍처(SPA)는 항공기 또는 항공기 시스템의 다른 구성품의 손실을 가져 올 수 있는 시스템에 승인되지 않은 통제 또는 접근(예 : 데이터, 제한사항, 정보의 변경 또는 추가)을 방지하기 위한 기능을 포함한다.

2.2. 항공기 및 군사 관련 사이버보안 침해사례

군사용으로 사용하는 항공기의 경우 현재까지는 무인항공기 관련 사이버보안 침해사례들이 주로 나타나고 있다. 무인항공기는 항공기에 물리적으로 조종사가 탑승하고 있지 않고 지상의 무인항공기 조종사와 항공기 간의 연결을 주로 C2-Link(command and control)로 이루어지기 때문에 이러한 취약점을 이용해 적성 국가 및 테러리스트 단체에서 활동하는 해커들의 표적이 되어 정보를 탈취하거나 항공기 작전을 무력화시키는 사고가 발생하고 있다[9].

무인항공기가 사이버공격을 받는 대표적인 형태는 Table 3와 같다.

Table 3. 무인항공기의 대표적인 사이버공격 형태

구분	내용
Jamming	적의 전자장비 사용을 방해할 목적으로 잡음이나 잡음과 유사한 전자신호를 계획적으로 방사, 재방사 또는 방사해 수신 내용을 교환하는 방법
Hijacking	소프트웨어 업데이트, 외부 인터페이스 연결 등과 같은 과정에서 악성코드 감염 등
Spoofing	Fake data를 보내 공격 대상 무인기를 해커가 의도한 곳으로 이동하거나 착륙하도록 유도하는 방법

2011년 12월 미국의 중앙정보국(CIA)이 사용하는 스텔스 정찰용 무인항공기 RQ-170(센티넬)이 아프카니스탄과 가까운 국경 지역에서 이란의 해킹에 의해 포획되었다. 이란은 Fig. 3와 같이 spoofing 방식을 이용하여 그들이 원하는 지점으로 무인항공기를 유인하여 착륙시켰다. 탈취한 무인항공기는 역설계하여, 2014년 11월 복제한 무인항공기의 비행 시험이 성공했다.

Fig. 3. 무인정찰기 RQ-170 해킹 방법[16]

버지니아주에서 열린 사이버샛(CyberSat) 컨퍼런스에서 미 국토안보국의 한 관계자는 200명 가량의 승객을 태울 수 있는 보잉 757기 여객기를 대상으로 무선주파수 통신을 통해서 항공기의 비행 통제시스템에 접근할 수 있다는 것을 시연을 통해 밝혔다[10].

상기와 같은 사례들은 항공기 및 군용항공기 운용을 위한 필수 시스템인 통신수단을 이용하여 해킹이 가능하다는 것을 여실히 보여주고 있다.

또한, 최근 국내에서 발생한 GPS 재밍 공격은 위치기반의 모든 시스템을 무용지물로 만들었고, DDOS 공격과 랜섬웨어와 같은 형태의 사이버공격 또한 급증하고 있는 추세이다[11].

이를 대비하고자 국내 항공업계에서도 사이버공격에 대한 노력을 기울이고 있다. 최근 한국항공우주산업㈜은 한국인터넷진흥원과의 협약을 통해 우주, 항공, 방산 등 국가전략기술 분야의 중요성에 따라 항공우주분야의 사이버 위협에 선제적으로 대응하기로 하였다. 이를 통해, 스마트공장, 도심항공교통(UAM) 등에도 협력을 강화하기로 하였다.

2.3. 미 해군의 사이버보안 관련 제도 및 조직

미 해군성에서는 사이버보안을 하드웨어 및 소프트웨어적 그리고 절차적 해결법을 활용하여 임무 수행능력에 영향을 끼치지 않고, 사이버공격을 저지, 감지, 분석, 보고 및 반응하고 회복함으로써 사이버 전장 환경에서 전투 요소들의 생존성(survivability)과 회복력(resiliency)을 최대한 보장하는 것이라고 정의하고 있다.

사이버보안과 관련된 감항관련 기술표준으로는 감항인증 요구조건을 명시한 DO-256A/ED-203A(Airworthiness Security Methods and Considerations)와 MIL-HDBK-516C(Airworthiness Certification Criteria)가 있으며, 감항인증 절차인 DO-202A(Airworthiness Security Process Specification), 유지감항 지침인 DO-355/ED-204(Information Security Guidance for Continuing Airworthiness)가 있다.

미 해군의 항공체계사령부(NAVAIR)의 AIR-4.0P에서는 사이버보안에 관련하여 감항인증 업무를 담당한다. AIR-4.0P는 사이버보안 프로그램의 담당 부서로 지정되어 있으며, 미 해군·해병대 전(全) 부대(서)/전투부대 및 무기체계에 사이버보안을 적용하는 NAVAIR M-13034.1(NAVAIR Airworthiness and Cybersafe Process Manual)를 준용한다.

미 해군 및 국방부의 사이버보안 획득 관련 절차는 Fig. 4와 같다.

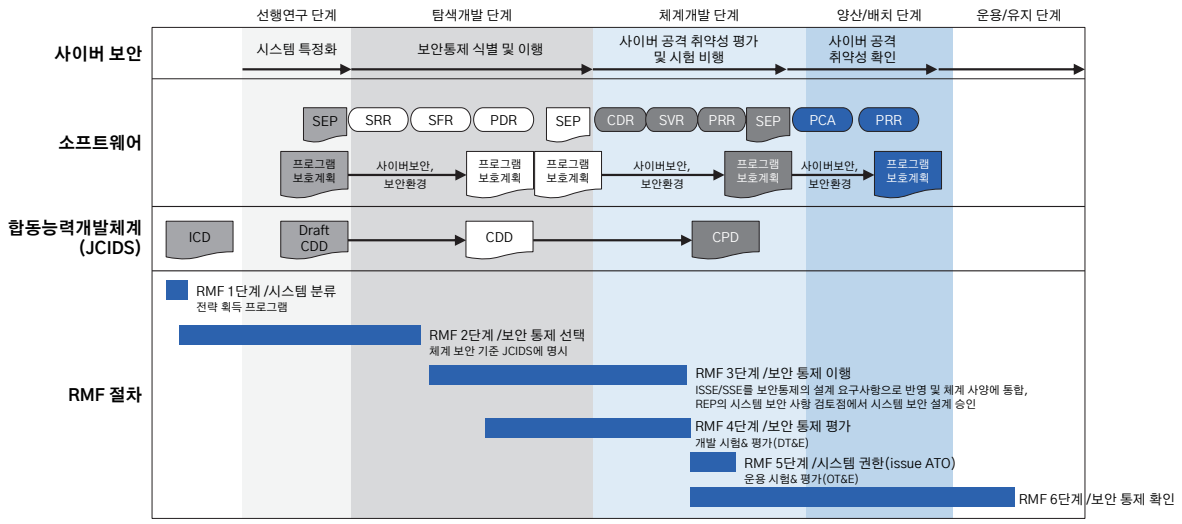

Fig. 4. 미 해군 및 국방부 획득(사이버보안) 절차

사이버보안 인증의 산출물로는, 사이버보안 요구조건 점검표(CyberSafe chop sheet), 사이버보안 인증(CyberSafe certification), 운용자 교범(NATOPS/NATIP) 변경, 무장학교 교육자료(임무 수행시 취약성 및 완화책)이 있다.

NAVAIR AIR-4.0P 사이버보안 전문가 그룹 및 업무 분장은 Table 4와 같다.

Table 4. 사이버보안 전문가 그룹 및 업무 분장

직책	역할
수석 엔지니어	사이버보안 기술 보증 권한
사업관리자	사이버 위험 관리 및 위험 완화
감항당국	사이버보안 인증(발행)
전문기술 엔지니어	각 분야별 요구조건·시험·양산품 기술 검토·확인
사이버전 담당	사이버 위험 평가
이해관계자	미 해군성·해병대 관련부대(서) 등 관련 부대(서) 참여

사이버보안 구축을 위한 단계별 활동은 크게 운용단계, 설계·검토단계, 계획단계, 솔루션 적용 단계까지 총 4단계로 구성되어 활동하고 있다. 우선, 운영단계는 훈련단계에서 사이버공격이 임무수행에 미치는 영향을 파악하고, 잠재 위협 식별 및 사이버 위협 평가에 반영하여 아래와 같이 3단계로 위협을 분류한다.

- 반드시 시험필요
- 필요시 분석
- 재위험 · 경미

설계 및 검토단계는 무장체계의 세부 구성품 별 사이버공격 루트를 설계하고 공격이 예상되는 핵심 구성품, 기능 및 공격 진입 지점을 식별한 후 공격 진입 지점에서 목표까지의 가중치가 부여된 공격 루트를 설계한다.

계획단계는 보안에 취약한 시스템의 분류와 각 시스템 별 보안 통제(security control) 솔루션을 선정하고 실행 및 평가하며, 해당 시스템의 사용 인증 및 모니터링을 수행하는 단계이다.

솔루션 적용 단계에서는 모든 보안 통제 중 해당 항공무기체계에 맞는 솔루션을 식별하고, 그에 따라 견고한 사이버보안 솔루션을 설계에 적용한다.

미 해군 항공체계사령부(NAVAIR)의 사이버보안 인증체계를 간략히 도식화하면 Fig. 5와 같다.

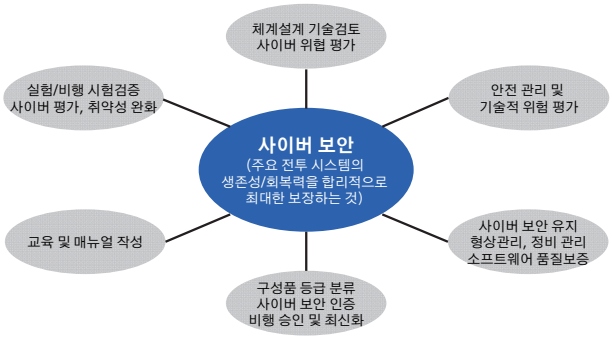

Fig. 5. 미 항공체계사령부 사이버보안 인증체계

2.4. 美 해군의 사이버보안 프로그램

사이버보안은 전통적으로 시스템과 네트워크에 대한 보호(protect)에 집중되어 왔다. 그러나 미 해군의 사이버보안은 보호를 능가하는 사이버 리질리언스(cyber resilience)를 통한 사이버전 대응 작전을 강조하고 있다.

사이버 리질리언스란 적의 사이버공격에도 불구하고 원하는 결과를 지속적으로 제공받을 수 있는 대비, 대응 및 복구 능력을 가진 엔티티(entity)이다. 사이버 리질리언스의 개념은 Fig. 6와 같다.

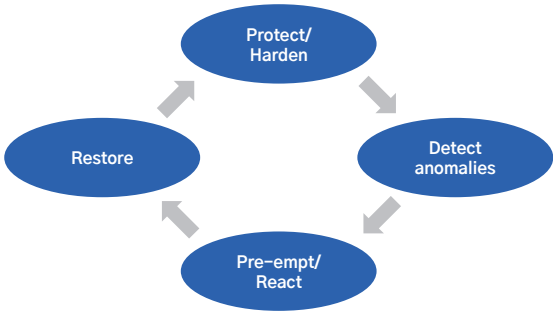

Fig. 6. 미 해군 임무보장을 위한 사이버 리질리언스[12]

보호(protect), 탐지(detect), 대응(preempt/react), 복구(restore)의 유기적인 결합을 통해 사이버 복원력이 완성된다.

보호(protect)는 적의 공격 대부분을 방지하는 역할을 하며, 위협으로부터 시스템을 보호하고 강화한다. 탐지(detect)는 적대 행위를 식별 및 평가한다. 대응은 선제적 공격을 통해 식별 및 평가된 적대 행위에 반응적 대응을 한다. 복구(restore)는 정상상태와 작전상태로 자산을 복원한다.

Fig. 7은 미 해군 사이버 레질리언스 전략의 상세 내용이며, 아래와 같이 사이버 시스템을 0~4단계로 구분하였다.

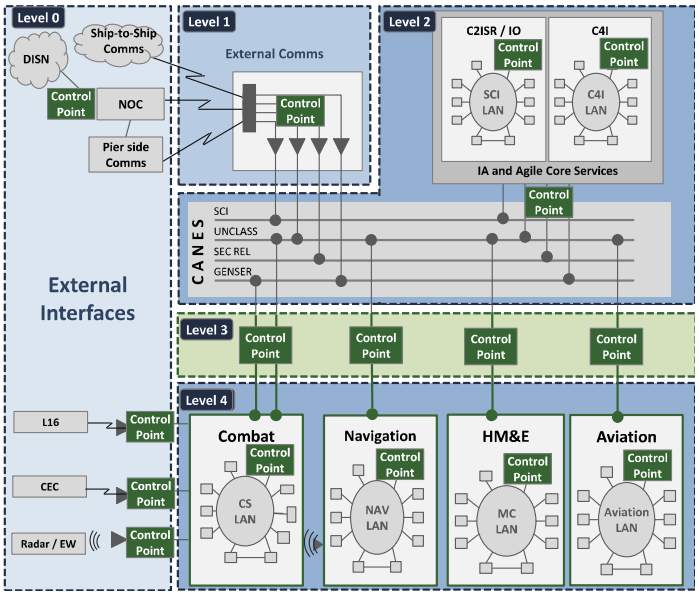

Fig. 7. 미 해군 사이버 리질리언스 전략[12]

- Level 0는 외부 인터페이스로부터 나오는 함대함 교신, 군사 전술자료 교환 네트워크, 고성능 상황 인식 및 통합 사격통제기능을 가능하게 하는 실시간 센서 네팅 시스템인 합동교전체계, 국방 정보시스템 네트워크, 레이더, 전자전 정보 등이 있다.
- Level 1은 함대함 통신, 정박 통신, 국방정보시스템 네트워크에서 교환되는 정보가 외부통신으로 분류된다.
- Level 2는 외부통신과 전술지휘자동화 체계(C4I)와 지휘통제 정보감시 및 정찰정보(C2ISR)가 특수정보, 대외비, 공개비밀, 일반정보로 분류된다.
- Level 3는 각 단계별 정보를 관리하는 컨트롤 포인트이다. 컨트롤 포인트의 역할은 크게 4가지(엔클레이브[enclave]의 경계 방호, 사건 발생 시 격리, 복구 작전, 애자일[agile] 기술 투입)로 나누어진다.
- Level 4는 전투, 항행, 선체, 기계 및 전기, 항공 통신망에 대해 각 분야별 컨트롤 포인트를 통해 통제된다. 함정, 항모, 잠수함, 항공기 등 모든 전력의 통신 정보를 등급에 따라 컨트롤 포인트를 통해 감시하고, 감지된 정보를 컨트롤 타워에서 전략적으로 사이버 상황을 통제한다.

이를 통해 아키텍처 프레임워크, 전략, 사이버 리질리언스 대책개발, 커뮤니케이션 사이버보안, 훈련, 사이버 안전, 표준서 제정, 지침개발 및 매뉴얼 작성과 같은 8가지의 작업 전반에서 공동으로 조율이 이루어진다.

Fig. 8은 미 해군 사이버보안 플랫폼에서 이뤄지고 있는 네트워크 관리와 모니터링, 각각의 시스템의 액세스 포인트에 지정하여 운용하고 있는 5개의 등급에 관하여 나타내고 있다.

미 해군 인트라넷이나 C4I, 자동 디지털 네트워킹 시스템(ADNS) 등은 네트워크 관리 대상으로 엔클레이브 영역으로 항상 모니터된다.

자동 디지털 네트워킹 시스템(ADNS)은 항모, 함정, 잠수함, 항공기 등과 특수정보(SCI)를 비롯한 전술과 비(非)전술 정보를 소통하는 도구로 미 해군 인터넷 프로토콜(IP) 네트워크 운영을 위한 전술적 광역 네트워크(WAN) 역할을 수행하는 핵심이며, 이 또한 내부 경계 액세스를 거쳐 정보가 전달되어 컨트롤 시스템과 연결된다.

외부 인터넷은 원천적으로 분리되어 있으며, 국방 정보시스템 네트워크(DISN), 해군 및 해병대 인트라넷(NMCI)은 내/외부 경계 액세스 포인트와 네트워크 관리 콘솔을 통해 액세스된다.

미 해군 사이버보안은 지속감지, 시스템, 네트워크 및 플랫폼의 보호와 전승을 보장하는 사이버 복원력 중심으로 크게 다음 3가지 주요 상호 관련된 측면으로 구성된다[12].

- 첫째, 사이버 시스템 수준(1~4단계)에서 시스템 유형에 대한 플랫폼 영역의 기본 세분화를 실시하여, 설계를 목적으로 플랫폼 아키텍처를 분류한다.

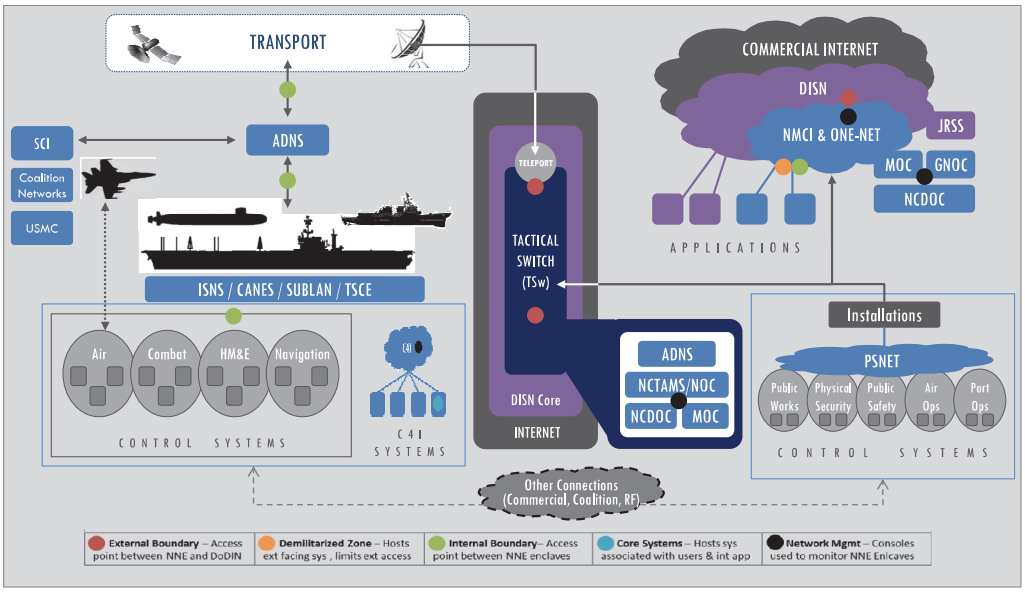

Fig. 8. 미 해군 사이버보안 플랫폼[12]

- 둘째, 사이버 안전등급(A, B, C)을 나누어 할당된 하드웨어 및 소프트웨어의 획득 단계에서부터 취급 및 유지관리 단계까지 제어함으로써 엄격하게 적의 위협으로부터 보호한다.
- 셋째, 장비와 시스템의 네트워크 접근에 대한 통제를 3단계(fully netted, semi-netted, no net)로 나누어 관리하여, 사이버보안 침입 또는 비정상적인 조건에 대응하기 위해 플랫폼 특성을 조정하는데 사용되는 운영 및 대응 절차를 결정한다.

사이버안전 프로그램의 시스템 수준과 단계에 따라 적의 위협으로부터 자산을 보호하고, 적의 행동을 탐지하여 식별 및 평가한다. 이는 선제적 또는 사후 대응을 통해 정상 상태로 유지하고 복원하는 프로세서가 규칙적으로 원활하게 작동될 때 요구하는 수준의 사이버보안을 유지하며, 사이버전에서의 우위를 달성하는데 그 목적을 둔다.

2.5. 우리 해군 및 해병대의 사이버보안 제안

현재 우리나라 해군 및 각 군에서는 항공기 사이버보안을 전담하는 부서 및 인력이 전무한 실정이다. 항공기 및 함정, 지상장비를 포함한 모든 무기체계에 대한 시스템과 네트워크 및 플랫폼을 보호하는 것 이상의 유기적이고, 지속발전이 가능한 학습형 전투적 사이버보안이 필요하다고 할 수 있다.

항공기 및 함정에 탑재장비에 적용되는 소프트웨어는 운용요구서(ROC)를 시작으로 개발 초기부터 사이버보안에 대한 요구사항을 적용하여 각 설계 단계마다 평가를 통해 취약점을 보완해야 한다. 이에 선행되어야 할 과제는 사이버보안 안전프로그램을 개발, 관리 및 구현할 수 있는 정책을 수립하고, 책임을 할당하는 것이다.

미국 카네기멜론대학(CMU) 소프트웨어 공학연구소의 보고서에 따르면 일반적인 IT 분야 소프트웨어 보안 취약점의 70 %가 설계과정의 오류로부터 발생하며, 마이크로소프트 사(社)는 개발단계에서 SDL(security development lifecycle)적용 시 보안 취약성이 50 % 감소한다고 보고하고 있다[13][14].

소프트웨어의 생명주기별 사이버보안 활동의 지침은 미국국립표준기술연구소에서 발표한 SP800 Series에서 제시하고 있다.

Fig. 9은 NIST SP 800-64(Rev.2) “Security Considerations in the Development Life Cycle”에서 제시하고 있는 소프트웨어 생명주기를 도식화한 것이다[15].

우리 해군도 미국의 사례를 벤치마킹하여 국내 실정에 맞는 조직과 절차를 수립하는 것이 급선무이다.

우선, 단기적으로는 미 해군의 사례를 바탕으로 사이버보안 인증 및 요구 조건과 관련 절차를 습득해야 할 것이다. 또한, 방위사업청 및 미 정부기관의 유기적인 협력을 통해 사이버보안 관련 표준과 책자 등을 확보하여야 할 것이다.

항공기 사이버보안 전문가를 확보하고 양성하기 위

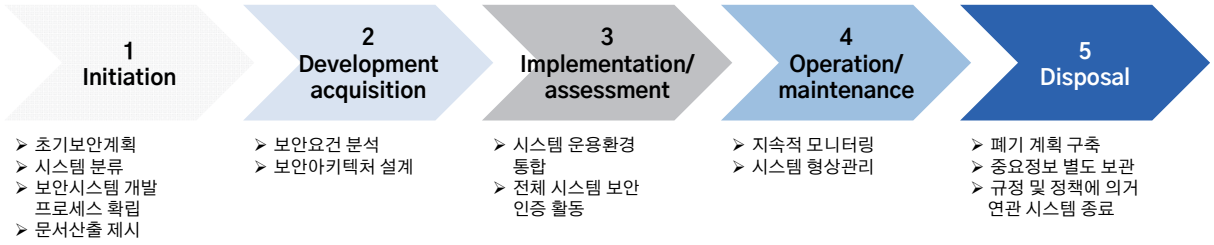

Fig. 9. NIST SP 800-64 소프트웨어 개발 생명주기

한 조직을 만들기 위해 중/장기 계획을 통해 편제에 반영하여 조속히 조직 구성이 필요하다.

장기적으로는 사이버 공간의 빠르고, 치열한 다변화적 사이버공격에서 인지 및 탐지 방법, 대응, 복원 방법에 대해 끊임없이 학습할 수 있는 빅데이터를 구축하여, 다변화적이고 불규칙적인 사이버공격에 신속한 복원능력을 가진 사이버 인공지능(AI) 대응 체계 및 공격 능력을 갖추어야 할 것이다.

3. 결론

본 논문에서는 사이버보안의 개념과 침해사례, 규정 등과 사이버보안 선진국인 미 해군의 NAVAIR 4.0-P 사례를 조사하였다.

항공기 및 군사 관련 사이버보안 침해사례를 비추어 볼 때 해킹으로 인한 유무인 항공기 탈취 위험과 정보 유출에 대한 위험이 지속적으로 증가하고 있다. 사이버보안은 포괄적인 사이버 안전의 중요한 구성 요소이다. 사이버보안의 목적은 중요 전투정보기술, 구성요소 및 프로세서의 생존 가능성과 복구능력을 보장하는 것이다. 항공기와 장비의 총 수명주기 전반에 걸쳐 중요 정보기술(IT)에 대한 강화된 보호능력과 복원력을 보유하고 임무에 영향을 주지 않으면서 보호, 방어, 복원에 필요한 적합한 구성 요소 및 프로세스, 재료 및 소프트웨어 솔루션을 제공함으로써 성공적 임무수행과 사이버보안 목표를 달성할 수 있다.

또한, 사이버보안의 성공 요소는 자격을 갖춘 사이버보안 전문가의 양성과 증명된 프로세스 그리고 효과적인 도구의 확보이다. 사이버보안은 단순한 컴퓨터 및 네트워크의 문제가 아닌, 전투임무를 달성할 수 있는가의 문제로 비행안전성 확보를 위해 사이버보안의 중요성을 인식하고 관련 제도 및 조직 마련에 힘을 쏟아야 할 것이다.

참고문헌

[1] "주요국가의 사이버보안 정보공유 및 협력체계," Monthly Issue of National Cyber Security, 제2020-05호, Vol. 99, p. 11.
[2] 오명호 외, "사이버전 개론 2nd Edition," 양서각, ISBN 978-89-5568-433-9, p. 6.
[3] Joint Publication(JP) 1-02, Department of Defence Dictionary of Military and Associated Terms
[4] Cybersecurity Policy, National Security Presidential Directive-54 / Homeland Security Presidential Directive 23, January 2008.
[5] Cybersecurity Test and Evaluation Guidebook, Department of Defense, 2015.
[6] CSFI, "CSFI ATC(Air traffic control) cyber security project," July 16, 2015.
[7] In-Kyu Lim, Ja-Young Kang, "Security Problems in Aircraft Digital Network System and Cybersecurity Strategies," JANT, Dec. 2017, p. 636.
[8] 방위사업청 고시 제2021-1호, 군용항공기 표준감항인증기준, p. 629.
[9] Geon-Hyeong Ko, Min-Su Park, Gi-Sung Ko, "A Study on the Institutional Development Plan of Unmannned Aircraft System Cyber Security," 2021 한국군사과학기술학회 종합학술대회 : 시험평가 부분.
[10] 홍병진, 항공무기체계 소프트웨어 사이버공격에 대한 작전영향성평가 방안, 2021.2, 아주대학교 박사학위논문.
[11] In-Kyu Lim, Ja-Young Kang, " Security Problems in Aircraft Digital Network System and Cybersecurity Strategies", JANT, Dec. 2017, p. 634.
[12] Mr.Troy Johnson, "Navy Cyber Resilience", 『USN Information warfare cybersecurity Division』, Feb. 2016.
[13] James W. Over, Team Software process for Secure Systems Development, CMU Software Engineering Institute, Mar. 2002.
[14] Microsoft Corporation, Microsoft Security Development Lifecycle(SDL), Version 5.2, Microsoft Corporation, P.167, May, 2012.
[15] NIST SP 800-64(Rev.2), "Security Considerations in the System Development Life Cycle," Oct. 2008.
[16] 백연상, 美무인기 포획 방법, 이란 엔지니어 주장 들어보니…, 2011.12.17., 동아일보. (https://www.donga.com/news/Inter/article/all/20111217/42677576/1)