IDAP INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2022, Vol. 5, No. 2, 73-106.

https://doi.org/10.37944/jams.v5i2.151

The first step toward the success of the Korean risk management framework (KRMF): System Classification Orientation Study

Kim, Jaewook* · Jeong, Sukjae**

ABSTRACT

The risk management framework (RMF) applied by the United States combines the concepts of information security and risk management in the product development process. This includes the systematic structure of equipment, parts, other construction systems, facilities, and personnel, as well as the related security of cyberspace. This concept has been a concept that has been systematically applied for the completion of information security from the requirement planning stage to the destruction of the weapon system. The RMF, which should be reflected in the project of power enhancement to ensure the perfect performance of the weapons system that our military will use in the future, is unfamiliar to Republic of Korea Army (ROK). RMF is a step-level field that has not yet been based on detailed research and measures in any ROK military, such as the Army, Navy, and Air Force. However, the USFK, which is stationed in the Republic of Korea during peacetime, and the United States' wartime reinforcement forces [Flexible Deterrence Option (FDO), Force Module Package (FMP), Time Phased Forces Deployment Data (TPFDD)], which are deployed at the request of the CFC Commander in the event of a crisis situation on the Korean peninsula and under the direction of the Joint Chiefs of Staff, are thoroughly prepared for cyber threats by applying the RMF procedure. Therefore, the military should also create and apply the corresponding procedures during combined and joint operations as soon as possible. This study aims to provide a direction for the development of a categorization system, which is the most basic and important step 1 system in the RMF process, and I hope that it will help in the implementation of the Korean Risk Management Framework (KRMF) that should be applied in the future.

Keywords : Risk Management Framework (RMF), information security, confidentiality, integrity, availability, system classification, information type identification, provisional impact level analysis

* (First Author) Kwangwoon University, Department of Defense Acquisition Program, Ph.D. Candidate and Joint Forces Military University The 1st Joint Education Agency, Air Force Colonel, afbmir@gmail.com, https://orcid.org/0000-0002-0019-8649

** (Corresponding Author) Kwangwoon University, Department of Business Administration, Professor, sjjeong@kw.ac.kr, https://orcid.org/0000-0001-8094-4674

Ⅰ. 서론

1.1 연구 배경 : 보안(保安)의 중요성 증대

21세기 4차 산업혁명 시대에 군(軍)이 운용하는 무기체계[1]는 실물 시스템과 최첨단 정보통신 기술 등이 융합되어 무기체계를 실제 운용하는 사용자에게 최적화된 성능이 발휘되도록 군(軍) 요구도(작전운용성능 등)가 점차 변화되고 있다. 특히, 대한민국은 적의 위협 상황에서 자국의 영토 수호를 위해 최적의 방어수단(전투기, 지대공미사일 등)을 현장에 투입할 때, AI, Big Data, IOT 등을 활용하여 자동화 및 지능화된 시스템에 의해 제어될 수 있도록 첨단 무기체계 전력증강사업(구매 및 연구개발)에 반영하고 있다. 하지만, 이러한 최신 무기체계는 적의 사이버 위협에 노출될 수 있어 이를 보호하기 위한 보안체계가 더욱 중요해지고 있다. 실제 코로나 19로 인해 축소해왔던 을지연습은 북한의 사이버 공격에 대한 위협이 현실화되면서 2022년에 을지 자유의 방패(UFS, Ulchi Freedom Shield)로 명칭을 변경하고 북한 미사일 발사 위협 및 사이버 공격 등에 대한 대비 훈련을 진행할 예정이다. 이는 첨단 무기체계 개발과 운영에서 정보통신기술에 대한 의존도 높아지고, 정보통신 기술발달로 지능적인 공격기술이 활용되고 있어 정보보안 강화의 필요성이 정책 실행 차원에서 강조되고 있다는 것을 의미한다.

정보보안은 “정보시스템 자원(하드웨어, 소프트웨어, 펌웨어, 정보 / 데이터, 통신 등)에 대한 기밀성(Confidentiality)과 무결성(Integrity), 가용성(Availability) 유지와 같은 목적 달성을 위해 자동화된 정보시스템에 적용되는 보호”[2]이다. 즉, 기밀성은 인가되지 않은 사용자가 특정 시스템에 들어와서 작성된 비밀문서를 열람하지 못하도록 문서의 비밀번호를 입력하는 등의 방법으로 노출로부터의 정보를 보호하는 것이고, 무결성은 정보와 프로그램 등이 관리자인 자신이 알지 못하는 사이에 불법적인 방법으로 변경되지 못하도록 보호하는 방법이다. 일상생활 속에서는 온라인 전자결제 과정에 필요한 휴대폰 본인인증 등을 예로 들 수 있다. 가용성은 인가된 사용자가 특정 정보시스템에 접속하여 원하는 시간에 원하는 자료를 막힘없이 방해받지 않고 이용할 수 있도록 파괴로부터 보호하는 것이다. 앞서 설명한 세 가지(기밀성, 무결성, 가용성)는 보안의 핵심요소로 정보보안을 유지하기 위해 반드시 준수되어야 하는 원칙이다.

지난 2014년 한국수력원자력이 북한 해커조직인 김수키(Kimsuky) 계열 악성코드와 구성・동작 방식이 유사한 이메일 공격에 의해 해킹을 당한 사건과 2016년 외부와 분리된 대한민국의 국방망에서 ‘한・미 연합 작전계획 5015’ 등 군사기밀이 대거 유출됐던 해킹 사건은 북한 정찰총국 산하

1) 무기체계 : 유도무기・항공기・함정 등 전장(戰場)에서 전투력을 발휘하기 위한 무기와 이를 운영하기 위해 필요한 장비・부품・시설・소프트웨어 등 제반요소를 포함한 것으로서 대통령령이 정한 것을 말한다. 방위사업법(제17165호, 2021), 제3조.

2) 박명환 등(2016). 사이버전 개론. 양서각, p.6.

110 연구소의 해킹 그룹인 '안다리엘(Andariel)'의 소행인 것으로 밝혀졌다. 이렇듯 북한의 사이버 위협은 우리 군(軍)에만 한정된 것이 아니라 대한민국 사회 여러 곳에 대해 광범위하게 퍼져 있다. 특히 최근 들어 더욱 증가하고 있는 북한의 사이버 위협에 대비하기 위해 무기체계의 수명주기 동안 적용하고 있는 미국의 RMF(Risk Management Framework, 위험관리체계)에 대한 연구가 필요하다. 특히, 우리 군의 입장에서 사이버 해킹 가능 대상국은 주요 대응 국가인 북한뿐만 아니라 주변 적성국 모두를 고려해야 한다. 예를 들어, 2007년 중국 공산당이 중국 해커를 활용하여 미국 록히드 마틴사의 전산망을 해킹하고, 미국의 첨단기술인 F-35 설계도를 불법 확보하여 자국의 FC-31 전투기(중국명 J-31) 제작에 도용했다는 공공연한 의심을 받았다. 실제 2014년 중국 주하이(珠海) 에어쇼에서 J-31 전투기 시제품을 본 미국 정부 관계자는 중국이 개발 중인 J-31의 외관이 쌍발 엔진 장착 외에 F-35와 매우 흡사하여 국가적인 전략자산 유출의 심각성을 인지하였다. 이런 사례를 통해 완벽한 보안 시스템도 점차 관련 사이버 해킹 기술이 고도화되면서 위협도가 증가하고 있어 이를 저지하고 방지하기 위한 지속적인 위험관리체계 개선과 운용이 중요하다고 볼 수 있다.

1.2 연구 목적 : 무기체계에 대한 사이버보안 필요성 확대

정보통신 분야의 빠른 발전으로 인해 미래 전장 환경 대비 군(軍) 무기체계에도 기존 개발한 군사기술에 새롭게 추가되는 다양한 정보통신기술을 융합하여 무기체계를 개발하고 있다. 신규 정보통신기술을 활용하게 되면 복잡한 전장상황 하에서 지휘관의 결심이나 임무 요원의 전투 수행능력 등을 기존보다 향상시킬 수 있지만, 한편으로 정보통신기술의 취약점을 이용하여 임무를 방해하려는 사이버 공격으로부터 쉽게 노출될 수 있다. 따라서, 최근 들어 신규 무기체계의 전력증강 시 정보통신기술 의존도가 증대되고 있기 때문에 개발된 신규 무기체계는 향후 사이버 공격에 대한 중요한 표적으로 될 것이다.

전투기의 경우, 1960년대 개발된 F-4 전투기는 소프트웨어로 구현되는 요구성능이 불과 8%에 지나지 않았으나 F-22 전투기의 경우에는 80%의 성능이 내장형 소프트웨어를 기반으로 구현되고 있다.[3] 이처럼 전투기의 소프트웨어 비중을 높이는 이유는 비행 유도, 사격 통제 시스템, 데이터 링크 시스템 등의 극한 상황에서 요구되는 안전 운용과 최대 성능을 구현하는 역할을 지원하여 전투 임무 성패를 좌우하기 때문이다(e.g., Kim & Kang, 2019). 또한, 최근 우리가 보유한 최신 전투기인 F-35에서는 소프트웨어의 비중이 약 90%까지 높아졌다. 연도별 전투기의 소프트웨어 비중은 Table 1과 같고, Bold 기종이 대한민국 보유 전투기이다.[4]

---

3) 김의순『국방 분야 IT 융합 현황과 발전 방안』(정보통신산업진흥원: 주간기술동향, 2011), pp.1-13. https://www.itfind.or.kr/WZIN/jugidong/1492/file60467-1492.pdf

4) 이성남『국방 무기체계 SW 발전방안』(소프트웨어 정책연구소, 2017) https://www.spri.kr/posts/view/21870?code=

<Table 1> Proportion status of embedded software in Fighter system by year

Year	1960	1964	1970	1975	1982	1990	2000	2007
Model	**F-4**	A-7	F-111	**F-15**	**F-16**	B-2	F-22	**F-35**
Portion	**8%**	10%	20%	**35%**	**45%**	65%	80%	**90%**

최신 무기체계의 체계 구성과 개발 시에 소프트웨어가 전체에서 점유하는 비중이 급속도로 증가하고 있으며, 이러한 현상은 향후 무기체계의 발전 방향의 무인화, 지능화 등을 통한 상호운용성 등이 강화되면서 더욱 가속화될 것으로 보여진다. 최신 무기체계의 전력화로 인해 이루어지는 다양한 장점도 있지만, 만약 적의 사이버 공격으로 인해 장비의 중단 및 오작동을 일으키고 민감한 정보유출 등이 발생될 경우 전투력 손실로 인해 국가안보에도 심각한 악영향을 줄 수 있다. 사이버 공격에 의한 적아의 피해 사례는 Table 2와 같다.

<Table 2> Cyber-attack cases

Target	Contents	Presumptive causes
US RQ-170[5]	The U.S. stealth unmanned reconnaissance aircraft RQ-170 (Sentinel) captured Iranian forces during a reconnaissance of Iranian territory in December 2011	Cyber Attacks (Hacking) → Iranian side claims
North Korea Musudan IRBM(intermediate-range ballistic missiles)[6]	In 2016, North Korea launched the first test launch of a Musudan medium-range ballistic missile (IRBM) in the direction of Wonsan to East Sea, during an aerial explosion during a few seconds of flight in the ascending phase. * North Korea's Musudan IRBM failed 7 out of 8 test launches due to the U.S. Cyber Warfare of the missile called the "Left of Launch"	Cyber Warfare or energy and electronic attacks

따라서 미국 등을 포함한 선진국에서는 무기체계 개발 시 초기부터 불순 세력으로부터 사이버 위협에 적극적으로 대비하고 최적화된 시스템을 통한 보안의 최신화가 지속 구현되기 위해 요구되는 보안목표와 보안수준에 따라 보안통제항목을 세밀하게 개발하도록 제작사에 요구하고 있다(e.g., Kim, & Kang, Shin, 2021). 미국은 2014년도부터 미국 내 정부의 모든 시스템에 신규 보안시스템을 적용하도록 하는 획기적인 패러다임의 변화가 일어났으며, F-35 전투기 개발이 대표적인 사례이다. 미국은 첨단 무기체계인 F-35 전투기 개발 시 사이버 위협으로부터 보안을 확보하기 위해

&study_type=&board_type=

5) 윤상용(2020). RQ-170 센티널 다목적 무인항공기. 조선일보, 유용원의 군사세계. https://bemil.chosun.com/site/data/html_dir/2020/05/11/2020051102659.html

6) 유용원(2022), 북 핵미사일 무력화시킬 작전명 '발사의 왼편'. 주간조선 : 유용원의 밀리터리 리포트. http://weekly.chosun.com/news/articleView.html?idxno=18963

RMF(Risk Management Framework, 위험관리체계)를 만들어 적용하였다. 즉, 제품 개발 프로세스에 정보보안과 위험관리(Risk Management)의 개념을 서로 결합하여 기존에 적용하고 있던 장비와 부품 등 구성 체계 및 시설, 인원 등의 관련된 보안과 더불어 사이버공간이 포함된 보안 항목을 소요기획 단계에서부터 체계적으로 적용하여 무기체계 폐기 시까지 정보보안의 완전성을 달성되도록 노력하는 개념이다.[7] 한국공군도 2018년부터 F-35A 도입을 계기로 첨단 무기체계의 사이버 보안에 대한 중요성을 깊이 인식하게 되었다. 특히, 한미 연합공군의 핵심 전력인 전투기 등의 최첨단 무기체계에 대한 안정적인 사이버보안을 확보하는 것(Kim & Kang, 2019)은 적(사이버 공격 등)으로부터 한미 전력에 대해 무위의 전투력 손실을 방지하고 전투수행능력 극대화를 보장하기 위해 필수적이고 가장 기본적인 요건일 것이다.

대한민국도 보안통제항목이 구분되어 있지만, 미국처럼 소요기획 단계부터 국방획득체계 전반에 각종 사이버 위협으로부터 사이버보안이 보장되는 선순환적 환류 구조로 정립되어 있지 않고 있다. 그러므로 우리보다 선진화된 보안체계를 2014년부터 개발하였고 현존하는 최고의 무기체계인 F-35에 직접 적용하고 있는 미국의 RMF(Risk Management Framework, 위험관리체계)에 대한 벤치마킹이 우리도 필요한 실정이다. 미국이 운영하고 있는 RMF의 여러 단계(총 7단계) 중 1단계(시스템 분류)가 매우 중요한 이유는 선순환적 환류 구조인 RMF의 첫 번째 단계임과 동시에 시스템에서 처리, 저장 및 전송되는 정보의 손실이 발생하게 된다면 시스템 자체의 기밀성, 무결성, 가용성이 저하되기 때문이다.

따라서, 본 연구는 한국형 위험관리체계(KRMF)의 성공적인 개발을 위한 첫걸음인 1단계(시스템 분류) 방향에 대해 중점적으로 제시하고자 하며, 논문의 구성은 다음과 같다. 2장에서는 미국의 RMF 분석을 위해 미국의 사이버보안 인증평가 제도의 변천사와 현재 미국이 적용하고 있는 RMF 7단계 및 시스템 분류(1단계)에 대해 설명하였다. 3장에서는 미국의 RMF 대비 한국의 사이버 보안제도 한계점 분석을 위해 미국과 한국의 사이버 보안제도를 비교하고, RMF를 한국에 도입하기 위해 연구한 문헌의 고찰 및 KRMF(한국형 위험관리체계)의 성공을 위한 조건을 살펴보았다. 4장에서는 최적의 KRMF 구축을 위한 중요한 시스템 분류 적용방안을 위해 1단계(시스템 분류) 정보유형 분류(대분류 → 중분류 → 소분류)와 1단계(시스템 분류)의 잠정 영향 수준 분석 방안을 고민하여 적용해 보았다. 마지막으로 5장에서는 결론 및 후속 연구방향에 대해 설명하였다. 향후 우리 군에서 운용될 무기체계에서도 최첨단 정보통신 기술이 적용될 것으로 예상되기 때문에 무기체계에 대한 사이버보안 확립이 필수적으로 요구되고 있다.

---

7) NIST Special Publication 800-37 Revision 2(Risk Management for Information Systems and Organizations, 2018.12), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.Spp.800-37r2.pdf

Ⅱ. 미국의 RMF 분석

2.1 미국의 사이버보안 인증평가 제도의 변천사

미국은 현재 보안목표의 기준이 되는 기밀성, 무결성, 가용성 중 기밀성에 초점을 두고 미국 국방부가 컴퓨터 보안제품을 평가하기 위해 표준규격 문서인 컴퓨터 보안 평가지침서(TCSEC, Trusted Computer System Evaluation Criteria)를 만들었다. 이를 위해 1960년부터 시작하여 1972년 지침이 발표되었고 1983년 초안으로 제정된 컴퓨터 보안 평가지침서는 국가안보기관(NSA, National Security Agency) 산하의 미국 국립컴퓨터보안센터(NCSC, National Computer Security Center)에서 규정한 컴퓨터 보안 평가의 하나로 1985년 미 국방부 표준(DoD 5200.28-STD)으로 채택되었다. 이 책의 표지가 오렌지색이었기 때문에 오렌지북이라고 불리었는데 오렌지북에서 미국 국방부가 완성된 컴퓨터 보안제품을 평가하는 기준으로 컴퓨터의 보안 레벨을 7단계(A1・B3・B2・B1・C2・C1・D)로 분류하였다(Yang, 2018). 여기서 A(Verified Design)는 보안 레벨이 가장 높으며, D(Minimal Protection)가 보안 레벨이 가장 낮음으로 정의하였다. 제품 평가에는 보안정책・보안등급・신원확인・감사 / 기록・시스템의 지속적인 보호 등이 포함되어 있다. 그러나 TCSEC은 운영시스템에만 중점을 두었고 무결성과 가용성에 대해서는 다루지 않고 있어서 단순한 분류만으로 다양한 보안 측면을 평가하기 어렵다는 단점이 존재하였다. 그래서 이를 보완하기 위해 1997년에 DISA(Defense Information System Agency)의 CISS(Center for Information Systems Security)에서 미국 국방부 정보기술 보안 인증(Certification, 정보시스템의 보안 요건이 충족되는지 확인) 및 인가(Accreditation, 시스템 운용 시 보안 위험에 대한 대책이 수립되어 있는지 확인) 절차(DITSCAP, Department of Defense Information Technology Security Certification and Accreditation Process)를 만들었다. DITSCAP은 시스템의 수명주기(시스템의 개발 / 통합에서부터 전력화가 이루어진 후 운영 시까지)에서 발생하는 보안문제를 해결하는 역할을 하였다. DITSCAP은 수명주기에 대해 4단계(1단계 Definition → 2단계 Verification → 3단계 Validation → 4단계 Post Accreditation) 방식을 적용하여 보안 관리를 진행하였다(Eller & Stauffer, 2000). DITSCAP의 적용으로 인해 TCSEC의 단점을 어느 정도 보완하였지만, 표준화/목록화된 보안통제항목이 부재하여 개발되는 모든 무기체계마다 보안통제항목을 새롭게 작성해야 하는 번거로움이 발생하였다. 이러한 DITSCAP의 단점을 보완하고 미 연방정보보안관리법안(FISMA, Federal Information Security Management Act)을 충족시키기 위해 2007년에 미국 국방부 정보보안 인증 및 인가 프로세스인 DIACAP(Department of Defense Information Assurance Certification and Accreditation Process) 제도를 만들게 되었다. 미 정부에 납품되는 모든 소프트웨어는 FISMA를 준수하도록 되어 있기 때문에 미국 국방부의 무기체계도 예외사항은 아니었다(Cho, Cha, & Kim, 2019). DIACAP 제도의 초기 의도는 좋았으나 다른 정부기관과 통합된 정보보증(Certification & Accreditation) 절차를 운

영하지 않고 별개의 정보보증 절차를 운영하였기 때문에 평가의 중복요소가 발생하여 시간과 비용이 많이 발생한다는 단점이 생겼다. DIACAP은 총 5단계(정보보증 인증 및 인가에 대한 착수와 계획 → 정보보증 통제항목 구현 및 검증 → 인증 및 인가 결정 → 운용 승인 및 검토 유지 → 폐기) 절차로 이루어진다(Kang, Choi, & Lee, 2019). 현재 미국이 적용하고 있는 RMF(Risk Management Framework) 7단계는 앞서 운용했던 DIACAP 제도의 단점인 비용대비 효과 개선과 시스템 개발 수명주기의 통합성 등을 보완하고 프로세스를 보다 명확하게 구현하기 위하여 인증 및 인가(Certification and Accreditation) 프로세스가 평가 및 승인(Assessment and Authorization)으로 변경되었다. 또한, DIACAP에서 적용했던 3년의 인증 및 인가 주기를 없애고, 운영을 위한 인가인 ATO(Authorization to Operate)가 부여되면 전체 보안태세를 유지하기 위해 보안 조치를 지속 평가해야 하는 개념으로 적용되고 있다. RMF는 미 국방부지침인 DoDI(Department of Defense Instruction) 8500.01 Risk Management Framework for DoD IT(Information Technology)에 반영되어 있기 때문에 관련 사이버보안 정책수립을 위한 지침을 제공하고 있으며 반드시 준수하도록 명시하고 있다. 미국의 사이버보안 인증평가 제도 관련 변천사를 종합해 보면 Figure 1에서 보는 바와 같다.

Category	TCSEC (1985)		DITSCAP (1997)		DIACAP (2007)		RMF (2014)
Feature	First Cybersecurity Certification Assessment	⇒	Applying assessments according to the life cycle	⇒	Transition to the concept of Certification & Accreditation (C & A)	⇒	Interconnection with the U.S. Government Certification Assessment System
To be evaluated	Evaluate the finished product		Independent System Unit Assessment		Assessing networked systems		Applying security controls from the initial stage of system development

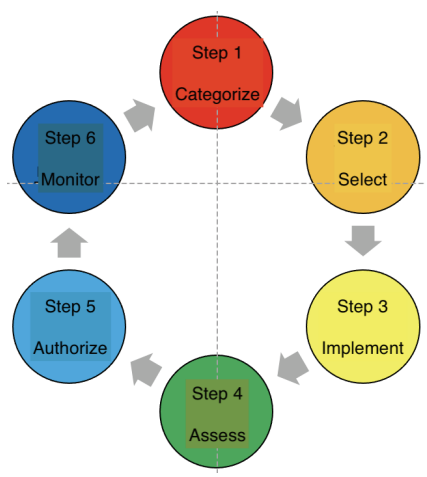
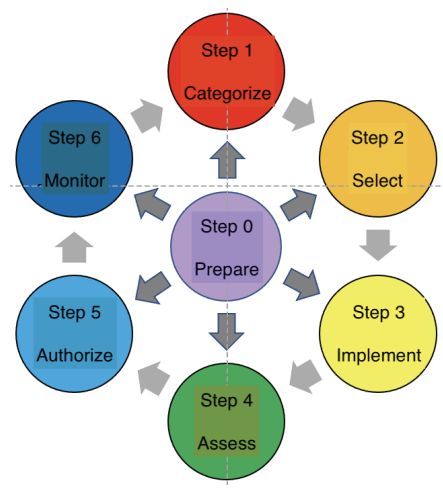
<Figure 1> Improving U.S. cybersecurity system

2.2 미국의 RMF 7단계 고찰

미국의 RMF는 지속적인 업데이트를 통해 발전되고 있다. 2018년 12월 NIST(미 표준기술연구소, National Institute of Standards and Technology) SP(Special Publication) 800-37(Risk Management Framework) Rev 2로 개정[8]되기 이전에는 RMF 6단계(1단계 시스템 분류 → 2단계

8) NIST Special Publication 800-37 Revision 2(Risk Management for Information Systems and Organizations, 2018.12),

보안통제항목 선택 → 3단계 보안통제항목 구현 → 4단계 보안통제항목 평가 → 5단계 시스템 인가 → 6단계 보안통제항목 모니터)로 구성된 NIST SP 800-37 Rev 1을 준수하여 연방 정보시스템에 대한 RMF를 적용하기 위한 지침을 따랐다. Figure 2는 RMF 6단계(NIST SP 800-37 Rev 1)와 RMF 7단계(NIST SP 800-37 Rev 2)의 주요 변경내용을 비교하였다.

Category	RMF Step 6 (NIST SP 800-37 Rev 1)	RMF Step 7 (NIST SP 800-37 Rev 2)
Major Changes (add new Step 0)		
Cybersecurity Focus	Primarily focused on processes against external threats	Efforts to improve external threats and privacy risk management processes

<Figure 2> The step change of Risk Management Framework (RMF)

현재 미국의 RMF는 7단계로 구성되어 있으며, 미국 국방부만 단독으로 적용할 수 있는 RMF 체계를 구축하는 것이 미국의 최종 목표가 아니기 때문에 미 표준기술연구소(NIST)에서 발간된 여러 가지 문서들뿐만 아니라 미 국가보안시스템위원회(CNSS, Committee on National Security Systems)의 정책 등을 함께 활용하여 작성한다. 이렇게 작성된 RMF 프로세스는 범국가 차원에서 사이버보안에 대한 동일한 기준을 적용할 수 있게 되었고, 평가 시 결과물을 함께 공유할 수 있게 되었다. 따라서 RMF를 연방 정보시스템 및 조직에 적용하기 위한 지침인 NIST SP 800-37을 통해 RMF 7단계 프로세스의 각각의 단계별 중점사항과 목적이 무엇인지 분석해보면 다음과 같다.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.Spp.800-37r2.pdf

2.2.1 0단계 : 준비(Prepare)

신규 추가된 0단계 준비의 목적은 RMF 1단계(시스템 분류)부터 6단계(보안통제항목 모니터)까지 주요 단계를 실행할 준비가 되어있는지 여부를 확인하기 위한 단계이다. 이를 위해 보안 및 개인의 정보보호에 대한 위험을 효율적으로 관리할 수 있도록 조직 수준(Organization Level)과 시스템 수준(System Level)으로 분리하여 세부 항목별 과업과 주요 담당자 및 협조자로 구분하여 꼼꼼하게 점검한다.

2.2.2 1단계 : 시스템 분류(Categorize System)

1단계 시스템 분류의 목적은 국가나 조직의 시스템에서 처리, 저장 및 전송되는 정보의 손실이 발생하면 시스템의 기밀성, 무결성, 가용성이 저하되기 때문에 정보의 손실이 발생하지 않도록 사전 예방 조치를 시행한다. 즉, 정보담당자가 각 정보유형을 식별하고 식별된 각 정보유형별 잠정 영향 수준(Low, Moderate, High)을 분석해 정보시스템의 보안 분류(보안목표 : 기밀성, 무결성, 가용성)를 결정하게 된다. 이때 각 정보유형별 잠정 영향 수준이 결정되면 이를 바탕으로 시스템에 가장 높은 수준으로 적용할 최종 영향 수준을 결정한다. 정보 및 정보시스템에 대한 3가지 영향 수준 분석은 FISMA(미 연방정보보안관리법안, Federal Information Security Management Act)에 정의되어 있다. 보안 분류의 위반이 발생될 경우 조직과 개인 관점에서 잠정 영향 수준 분석에 대한 FIPS(Federal Information Processing Standards) 199의 정의[9]는 Table 3에서 보는 바와 같다.

<Table 3> Latent impact in organization and individual level

Latent impact	FIPS 199 Definition
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

2.2.3 2단계 : 보안통제항목 선택(Select Security Controls)

NIST SP 800-37(Risk Management Framework)에서 2단계 보안통제항목 선택의 목적으로 국가나 조직의 시스템 등에 발생하는 다양한 위험에 상응하도록 정보시스템과 조직을 보호하는 것으

9) FIPS 199(Standards for Security Categorization of Federal Information and Information Systems 2004.02), pp. 2-3. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

로 언급하고 있다. 보안통제항목은 2020년 9월에 발간된 NIST SP 800-53 Rev 5[10]에 명시된 바와 같이 보안과 개인정보보호 선택 및 특정 프로세스에서 사용하기 쉽도록 식별자(ID)를 20개 패밀리(묶음)로 구성하고 있다. 각 통제항목은 2개의 알파벳 문자가 부여됨에 따라 식별이 용이[예를 들면 AC, Access Control(접근 통제)]하게 되어있다. 또한, 식별자 내 구체적인 평가항목(중분류 총 322개)이 수립되어 있어 시스템 및 조직에 대한 위험을 효율적인 방법으로 평가하기 쉽게 구성되어 있다.

2.2.4 3단계 : 보안통제항목 구현(Implement Security Controls)

3단계 보안통제항목 구현의 목적은 시스템 및 조직에 대한 보안과 개인정보보호 계획의 통제항목을 실현하는 것이다. 조직은 보안 및 개인정보보호 계획에 설명된 대로 통제항목을 구현하며 이를 위해 조직의 엔터프라이즈 아키텍처와 관련된 보안 및 개인정보보호 아키텍처가 일치하도록 한다. 하지만 계획대로 항상 통제항목을 구현할 수 있는 것은 아니므로 통제항목에 대한 지속적인 최신화를 통해 보안 및 개인정보보호 계획이 구현되도록 노력해야 한다.

2.2.5 4단계 : 보안통제항목 평가(Assess Security Controls)

4단계 보안통제항목 평가의 목적은 선택한 통제항목이 올바르게 구현되어 최초 의도한 대로 작동하고 있는지와 시스템과 조직에 대한 보안 및 개인정보보호 요구사항을 충족하고 있는지 등을 종합 판단하여 만족할만한 결과의 도출 여부를 결정하는 것이다.

2.2.6 5단계 : 시스템 인가(Authorize System)

5단계 시스템 인가의 목적은 보안 및 개인정보보호 위험이 조직 운영이나 시스템 운영 시 공통통제항목에 사용될 경우 고위 경영진(결정권자)이 시스템 인가를 결정함으로 조직에 대한 책임을 지도록 하는 것이다. 만약 통제항목을 재평가한다면 재평가 시 시스템과 조직의 보안 및 개인정보보호 요구사항을 충족하기 위해 수정된 통제항목이 올바르게 구현되고, 의도한 대로 작동하며, 원하는 결과를 생성하는지를 확인해야 한다.

2.2.7 6단계 : 보안통제항목 모니터(Monitor Security Controls)

6단계 보안통제항목 모니터의 목적은 시스템 운영 중 시스템 자체 및 외부환경 변화가 보안에 미치는 영향성을 판단하여 보안통제항목과 위험을 재평가하고 주요 사항에 대한 최신화를 수행하는 등 시스템이 폐기될 때까지 전(全) 수명주기 동안 설정된 보안목표 수준이 유지 및 관리될 수 있도록 노력하는 것이다. 즉 시스템 운영 간 변경 사항이나 추가 위험요소가 식별되면 1단계부터

10) NIST Special Publication 800-53 Revision 5(Scurity and Privacy Controls for Information Systems and Organizations, 2020.09), pp. 8-15. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.Spp.800-53r5.pdf

다시 RMF 절차를 반복하여 시스템 보안계획을 최신화하고 보안통제항목을 개선하는 환류 구조를 진행한다.

2.3 미국 RMF 시스템 분류(1단계) 연구

RMF에 적용되는 정보유형은 NIST SP 800-60 Ver2[11]에 정의되어 있고 임무기반 정보유형과 관리 및 지원 정보유형 2가지로 구분된다. 임무기반 정보유형은 임무지역과 정보유형 19개(세부 항목 76개) 및 서비스 제공구조와 정보유형 7개(세부 항목 24개)로 구분하고 있지만, 국방 및 국가안보에 대한 보안 분류(보안목표 : 기밀성, 무결성, 가용성) 관련 정보는 공개되어 있지 않고 있다. 공개된 임무기반 정보유형별 세부 사항은 Table 4와 같다.

<Table 4> Mission-based information types and security classification

Direct Service	Number of Items	Checking impact level of security classification
Mission Areas & Information Types	Subtotal : 76	
① Defense and National Security	3	X
② Homeland Security	4	○
③ Intelligence Operations	5	○
④ Disaster Management	4	○
⑤ International Affairs & Commerce	3	○
⑥ Natural Resource	4	○
⑦ Energy	4	○
⑧ Environmental Management	3	○
⑨ Economic Development	4	○
⑩ Community & Social Service	4	○
⑪ Transportation	4	○
⑫ Education	4	○
⑬ Workforce Management	3	○
⑭ Health	5	○
⑮ Income Security	5	○
⑯ Law Enforcement	8	○
⑰ Litigation & Judicial Activities	5	○
⑱ Federal Correctional Activities	2	○
⑲ General Science & Innovation	2	○

11) NIST Special Publication 800-60 Volume 1 Revision 1(Guide for Mapping Types of Information and Information Systems to Security Categories, 2008.8) pp. 15-18. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v1r1.pdf

Direct Service	Number of Items	Checking impact level of security classification
Service Delivery Mechanisms & Information Types	Subtotal : 24	
⑳ Knowledge Creation & Management	4	○
㉑ Regulatory Compliance & Enforcement	3	○
㉒ Public Goods Creation & Management	4	○
㉓ Federal Financial Assistance	4	○
㉔ Credit & Insurance	3	○
㉕ Transfers to State / Local Government	4	○
㉖ Direct Service for Citizens	2	○

관리 및 지원 정보유형은 서비스 전달지원 기능과 정보유형 8개(세부 항목 42개) 및 정부 자원관리 정보유형 5개(세부 항목 35개)로 구분되어 있다. 공개된 관리 및 지원 정보유형별 세부 사항은 Table 5와 같다.

<Table 5> Support delivery of services and management of resources

Direct Service	Number of Items	Checking impact level of security classification
Service Delivery Support Functions & Information Types	Subtotal : 42ea	
① Control & Oversight	3	○
② Regulatory Development	4	○
③ Planning & Budgeting	9	○
④ Internal Risk Management & Mitigation	3	○
⑤ Revenue Collection	3	○
⑥ Public Affairs	4	○
⑦ Legislative Relations	4	○
⑧ General Government	12	○
Government Resource Management Information	Subtotal : 35ea	
⑨ Administrative Management	5	○
⑩ Financial Management	7	○
⑪ Human Resource Management	10	○
⑫ Supply Chain Management	4	○
⑬ Information & Technology Management	9	○

RMF에 정의된 정보유형은 총 39개 정보유형과 177개 세부 항목으로 임무기반 정보유형과 관리 및 지원 정보유형으로 구분하여 보안분류(기밀성, 무결성, 가용성)에 대한 영향 수준을 제시하고 있다. NIST SP 800-37(Risk Management Framework)에는 1단계(Categorize System)에서 작업을

준비하기 위해 다음 과정(C-1～C-3)의 순서대로 세부 사항을 검토하게 되는데 각 과정의 주요 착안 사항은 Table 6과 같다.

<Table 6> Task categorization

Category	Description
TASK C-1 System Description	Documentation the characteristics of the system
TASK C-2 Security Categorization	Categorize the system and document the security categorization results.
TASK C-3 Security Categorization Review & Approval	Review and approve the security categorization results and decision.

1단계 시스템 분류(Categorize System)를 종합해 보면 각 정보유형을 식별하고 식별된 정보유형별 보안 분류(보안목표 : 기밀성, 무결성, 가용성)에 대해 잠정 영향 수준 분석(Low, Moderate, High)을 선정함으로 시스템 분류가 종료된다. 이때 각 정보유형별 잠정 영향 수준이 결정되면 이를 바탕으로 시스템에 가장 높은 수준으로 적용할 최종 영향 수준을 결정한다. 보안목표를 준수하고 보안에 문제가 발생하지 않도록 잠정 영향 수준은 상위 평준화가 된다. 예를 들어, 어떤 무기체계에 대한 시스템 영향 수준 평가를 하였다고 가정해 보자(Table 7). 무기체계의 많은 시스템 중의 한 가지인 A 시스템에 적용하기 위한 정보유형별 영향 수준을 종합한다면, A 시스템의 각각의 최종 영향 수준은 기밀성/무결성/가용성에서 가장 높은 수준으로 결정되기 때문에 기밀성은 Moderate, 무결성은 High, 가용성은 High가 된다.

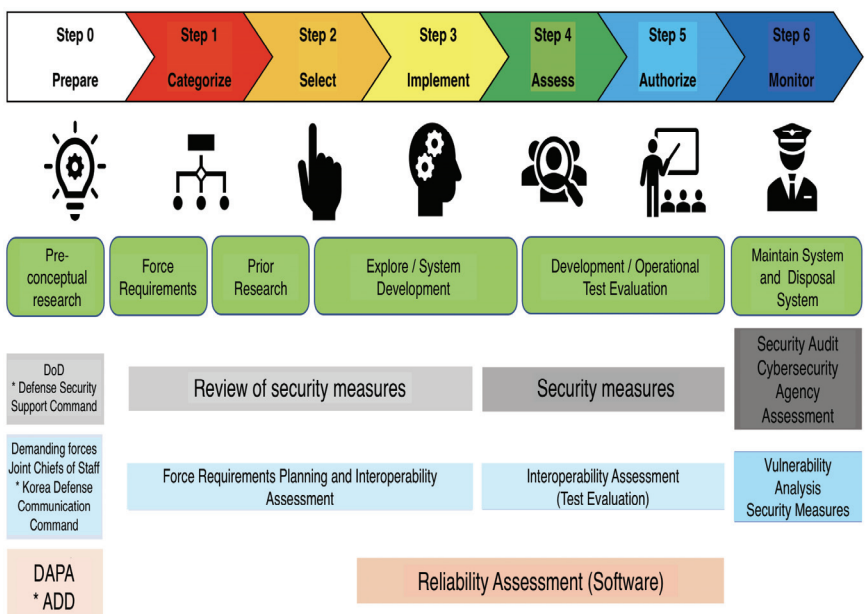
<Table 7> Assessing system impact level

Category		System Impact Level		
		Confidentiality	Integrity	Availability
Types of information	①	Low	Moderate	High
	②	Moderate	Low	Moderate
	③	Moderate	High	Low
	④	Moderate	High	High
System A Application		Moderate	High	High

Ⅲ. 미국 RMF 대비 한국 사이버 보안제도 한계점 분석

3.1 미국과 한국의 사이버 보안제도 비교

미국은 RMF 제도운영 시 국방부를 중심으로 기술적・관리적 보안을 통합할 수 있도록 합참・전투사・민간보안업체 등 무기체계 전력증강의 보안과 관련된 부서를 통제하고 종합적인 관점에서 사이버보안 취약점 관리가 가능토록 운영하고 있다. 미국의 RMF(0단계~6단계) 대비 한국 무기체계 사업의 수명주기별(소요제기, 선행연구, 탐색/체계개발, 개발/운용시험평가, 운영유지 및 폐기) 사이버보안 제도에 대한 분석(수명주기별 담당 기관, 주요 보안 활동 등)은 Figure 3에서 보는 바와 같다.



<Figure 3> Analysis of the cybersecurity system of weapon systems in South Korea

대한민국은 국방부(안보지원사, 사이버사), 합참(통신사령부), 소요군, 방사청(ADD) 등 각각의 소관 기관별로 부여된 보안업무를 성실히 수행하기 위해 각 단계별 임무(보안대책 검토, 보안측정, 상호운용성 평가, 신뢰성 평가, 취약점 분석 등)를 분장하여 운영하고 있다. 그러나 대한민국은 미국과 달리 보안업무를 여러 기관에서 담당하고 있고, 통합되지 않은 보안업무 수행으로 인해 현재 각 단계별로 부여된 임무가 중복되거나 누락되기 때문에 무기체계 전력증강 시 수명주기 전(全) 과

정에 일원화된 사이버보안 취약점 관리가 어려운 실정이다. 즉, 국내의 사이버보안 제도는 미국의 RMF와 달리 선순환적인 환류 구조가 아니어서 소요기획~전력화 시까지 안보지원사・통신사령부・ADD 등에서 사이버보안 관련 평가한 결과가 전력화 이후의 운용단계에서 취약점 분석 등과 서로 연계되지 못하는 구조인 것이다.

무기체계 소요제기 시 각 기관별 임무를 살펴보면 다음과 같다. 소요군과 합참은 합동성 및 상호운용성의 정보보호를 위해 네트워크・서버 정보보호 대책을 제시하고 안보지원사는 탐색개발 및 체계개발 단계에서 정보시스템 및 내장형 SW별 각 체계의 보안등급별로 요구되는 정보보호 대책이 적절히 강구되었는지에 대한 보안대책을 검토한다. 무기체계 개발・운용시험평가 등 전력화 이전 단계에서는 국군통신사령부가 연동 체계 간 데이터의 원활한 유통이 보장되고 필요한 정보보호 항목이 구성되어 있는지에 대한 상호운용성의 시험평가를 담당하고 안보지원사는 보안측정을 담당한다. 이러한 보안대책 검토와 상호운용성 평가 시 미국처럼 국방부를 중심으로 업무가 이루어지는 개념이 아니라서 효율성이 다소 감소되는 상황이 발생하고 있다. 또한, 방사청(ADD)이 담당하고 있는 신뢰성 평가는 무기체계의 요구성능 보장을 위해 내장된 SW(Embedded Software)의 오류를 검증하고 소스코드의 보안 허점이 있는지를 평가하고 있다. 전력화 이후 운영유지 단계에서 소요군 등에서 실시하는 취약점 분석 시 해킹, 바이러스, DDoS 등 점점 고도화되고 있는 각종 사이버 위협에 대해 무기체계가 보유하고 있는 취약요소를 점검하여 신규 보완할 부분이 있는지를 점검하고 있다.

3.2 국내 RMF 관련 연구 문헌 고찰

국내에서 미국의 RMF를 도입하여 한국에 적용하려는 연구는 아직 활발하게 진행되고 있지 않다. 공개된 국내 RMF 관련 연구의 내용을 살펴보면 미국의 RMF 관련 소개는 많이 이루어지고 있으나, 미국의 RMF를 벤치마킹하여 한국형 RMF로 전환하기 위해 각 단계별 실질적인 구현 방법을 연구한 자료는 찾아보기 어렵다. 그 동안 대한민국 군(軍)과 관련된 주제로 연구한 논문은 '한국군에 RMF 적용방안 연구', '한국형 RMF 체계구축을 위한 위험우선순위 식별 방법론 제언', '국내 무기체계에 대한 RMF 적용 실 사례 연구' 등이 있다. '한국군에 RMF 적용방안 연구'에서는 미국의 RMF를 한국으로 도입 시 우리나라 상황에 적합하도록 만들기 위해 한국군의 RMF을 적용하기 위한 조직과 필요한 사항들을 구축하기 위해 방안을 제시하였다. 이를 위해 첫째, RMF 정책과 지침을 제공하는 등 각종 정보를 전달하고 접근 가능하도록 국방 RFM MKS(Military Knowledge Service) 체계 구축이 우선되어야 하고, 둘째, RMF 거버넌스 구성은 한미 전술지휘통제(C4I) 자동화 체계를 통합하는 주무 부서인 합참 사이버지휘통신부를 중심으로 설계되어야 한다. 셋째, RMF를 수행할 수 있는 무기체계와 보안 전문 지식을 습득한 인력이 양성되어야 하며, 넷째, 한미 간 원활한 RMF 활용을 위한 협력이 지속되어야 한다(Lee, S. M.,2021; Lee & Choi, 2020). '한국형

RMF 체계구축을 위한 위험우선순위 식별 방법론 제언’에서는 한국형 RMF 체계 구축 시 미군(軍)과 우리 군(軍)의 임무 수행 환경이 상이함을 언급하였다(Joo, Kim & Kwon, 2021). 따라서, 한국군(軍)에 부합하도록 RMF에 대한 개선작업이 필요하기 때문에 한국군 실정에 적합한 RMF 위험우선순위 식별 방안에 대해 위험우선순위(RPN, Risk Priority Number) 기법을 변형 / 활용하는 방안(RMF I형)과 새로운 인공지능 Fuzzy 기술을 활용하는 방안(RMF II형)을 제시하였다(Joo, Kim, & Kwon, 2021). ‘국내 무기체계에 대한 RMF 적용 실 사례 연구’ 에서는 RMF를 적용함으로 인해 기존 대비 무기체계의 보안 분류를 보다 객관적인 기준으로 분류할 수 있었고, 보안 관련 요구사항 반영 시 그동안 미반영되었던 사항에 대해서도 최소화할 수 있었다고 한다. 또한, RMF를 문서에 의거 수명주기 전반에 적용하기 위해 보안 전문가의 검토가 필요한 부분이지만, 현재 연구되고 있는 무기체계에 비해 보안분야 전문 인력이 상당히 부족하기 때문에 RMF를 도입한다 해도 모든 무기체계의 보안을 검토할 수 있는 전문 인력 확보가 선행되어야 할 것으로 제시하였다(Cho, Cha, & Kim, 2019).

살펴본 연구 이외에도 사이버보안 관련 ‘사이버보안 강화 측면의 미국 국방 기술 및 사업 보호 정책 변화’, ‘RMF를 활용한 정보보호 관리제도 발전방안’ 등이 있다. ‘사이버보안 강화 측면의 미국 국방 기술 및 사업 보호 정책 변화’에서는 미국의 정책(단순하게 사이버보안의 강화를 획득단계에서만 반영하는 것이 아니라 적합한 보안수준을 전(全) 수명주기를 통해 체계적으로 관리)을 정확히 이해하고 우리의 제도와 업무체계 등을 적시에 개선해야 함을 강조하였다.[12] 각종 정책 변화에 능동적으로 대처하기 위해 국방획득체계를 담당하고 있는 기관 및 조직 간에 유기적인 업무 협업을 통해 사이버보안 전문성을 강하하는 등 다각적인 노력과 한미 연합체계의 상호운용성을 반영한 표준화 작업이 필요하다고 제시하였다.[13] ‘RMF를 활용한 정보보호 관리제도 발전방안’에서는 완성도 높은 제도인 미국의 시스템 수명주기 접근 방식인 RMF를 우리나라도 벤치마킹하여 정보보호 관리제도를 발전시키기 위해 미국과 우리나라 정보보호 제도를 상호 비교 / 분석하였다. 국내 정보보호 관리제도 발전방안으로 첫째, 효율적인 정보보안을 유지하기 위해 현재 시스템 수명주기별 단계에 따라 구분하고 있는 정보보호 사전점검제도(사업계획~시험 단계)와 ISMS-P(정보보호 및 개인정보보호 관리체계 인증, Personel Information & Information Security Management System) 제도(운영~폐기 단계)를 통합할 필요가 있으며 둘째, 완벽한 보안관리를 위해 개발부터 폐기까지 전(全) 수명주기 단계 동안 통합 정보보호 관리를 위해 기존 제도의 대상을 포함한 의무대상 확대가 필요하고 셋째, 제도의 통합(정보통신망법), 의무인증대상 확대(정보통신기반조성법), 법률 개정 등 3가지 분야로 발전방안을 제시하였다(Na & Shon, 2022).

---

12) 이승배(2020). 사이버보안 강화 측면의 미국 국방 기술 및 사업 보호 정책 변화, 국방과 기술, pp. 104-111. hhttps://www-dbpia-co-kr.libproxy.kw.ac.kr/journal/articleDetail?nodeId=NODE10496905

13) 이승배(2020). 사이버보안 강화 측면의 미국 국방 기술 및 사업 보호 정책 변화, 국방과 기술, pp. 104-111. hhttps://www-dbpia-co-kr.libproxy.kw.ac.kr/journal/articleDetail?nodeId=NODE10496905

이렇듯 국내 RMF를 위한 연구와 함께 윤석열 정부도 120대 국정과제 중 하나(101번 과제)로 '국가 사이버안보 대응역량 강화'를 선정하였고, 범 정부차원의 협력체제 구축 및 관련 산업・기술 경쟁력 제고, 인재 육성 등을 통해 사이버안보 기반 공고화를 과제 목표로 産・學・硏・官 협력 하 기술 고도화 및 국제협력 강화, 사이버전문인력 양성 등[14]의 빠른 추진을 기대해 볼 수 있겠다.

3.3 KRMF(한국형 위험관리체계)의 성공을 위한 조건

나날이 발전하고 있는 사이버 위협에 적극적이고 능동적으로 대처하기 위해 RMF가 미 국방부 지침인 DoDI(Department of Defense Instruction) 8500.01 Risk Management Framework for DoD IT(Information Technology)에 반영되어 있는 것과 같이 대한민국도 국방부를 중심(Control Tower)으로의 사이버보안 관리구조 정립이 필요하다. 우리 군(軍)도 무기체계 전력증강 사업 시 사이버보안 강화를 위해 정보시스템의 소요기획, 시스템 개발, 개발 / 운용시험평가, 전력화 및 폐기에 이르는 수명주기 전(全) 단계를 수행하는 동안 반드시 진행되어야 하는 보안대책 검토, 상호운용성 평가, 소프트웨어 신뢰성 평가 및 취약성 점검 등 사이버 위협에 적극적으로 대응하기 위해 다양한 사이버보안 제도를 운영하고 있다. 그러나, 미국처럼 국방부(DoD, Department of Defense)를 중심으로 무기체계의 정보시스템에 대한 취약점을 보완하여 완벽한 성능을 보장하기 위한 핵심 조직이 부재하기 때문에 국방부 중심의 일원화된 보안업무 수행이 불가하고 각 기관(안보지원사, 국군통신사, 사이버사 등)에 부여된 보안업무를 수행하는 수준이어서 사이버보안 관련 업무수행의 기준이 다소 복잡하다. 즉 현(現) 사이버보안 제도를 적용함으로 인해 각 기관(안보지원사, 국군통신사, 사이버사 등)의 조직이 통합되어 있지 않고 분산되어 있으며 무기체계의 전(全) 수명주기에서의 사이버보안이 아닌 수명주기 단계별 각 기관에게 부여된 보안업무만 처리하는 구조라서 유기적이고 종합적인 사이버보안 평가와 관리가 이루어지기에 매우 제한적인 구조로 이루어져 있어 국방부 중심으로의 사이버보안 관리구조 정립이 필요하다.

또한, 우리 군(軍)은 각 기관별로 분리되어있는 사이버보안 활동에 대해 미국의 RMF처럼 소요기획 단계부터 국방획득체계 전반에 사이버보안이 보장되는 선순환적 환류 구조로 정립되어 있지 않다. 현재 우리 군(軍)에 적용되고 있는 체계는 국방획득체계 각 단계에 따라 사이버보안 관리 기능이 분산되어 운영되고 있다. 그러므로 무기체계 전력증강 사업의 전력화가 이루어진 후 사이버보안 관련 추가 소요 발생 시 후속 조치를 수행하기 위해 최초 계획보다 비용의 상승이 발생하거나 원하는 성능이 나오지 않는 경우도 발생하게 된다. 따라서 사이버보안의 효율성 증대와 비용의 중복투자를 제거하고 체계적인 관리가 가능하도록 최적화된 시스템(KRMF, 한국형 위험관리체계)의 적용이 필요하다. 또한, 한미 연합작전을 수행해야 하는 우리 군은 미군과의 시스템 연동 시 안정성을 확보하기 위해 KRMF도 미국의 RMF(0단계~6단계)와 마찬가지로 유사하게 구성되어야 하며,

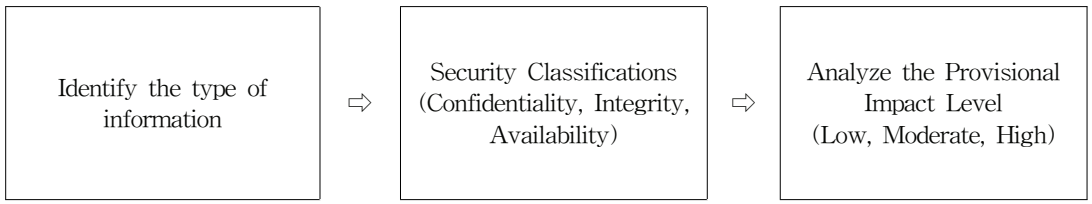
14) 국무조정실 국무총리비서실, p.168. https://www.opm.go.kr/_res/opm/etc/kukjungfile2022.pdf

각 단계에 대해 개념을 설명하면 다음과 같다. 0단계는 RMF 1단계(시스템 분류)부터 6단계(보안통제항목 감시)까지 주요 단계에 대해 실행할 준비가 되어있는지를 확인해야 한다. 1단계 시스템 분류(Categorize System)는 최적화된 KRMF(Korean Risk Management Framework)를 수립하기 위하여 가장 중요하다. 왜냐하면, 1단계(시스템 분류)는 정보시스템에 유통되는 정보유형을 선정하고 정보유형별 담당자를 지정한 후, 정보유형별 각각의 보안 분류(보안목표 : 기밀성, 무결성, 가용성)에 대해 잠정 영향 수준 분석(Low, Moderate, High)을 설정하여 보안계획에 반영하는 최초 시발점이기 때문이다. 즉 시스템에 영향을 주는 각종 정보에 대한 영향 수준을 분석하여 반영하는 가장 중요한 단계인 것이다. 1단계 시스템 분류 후, 다음 단계인 2단계 보안통제항목 선택 단계는 1단계에서 선정된 정보유형과 조직의 보안목표 수준을 시스템에 적용하기 위해 보안통제항목으로 변환해야 한다. 3단계 보안통제항목 구현에서는 시스템 및 조직에 대한 보안과 개인정보보호 계획의 통제항목을 구체적으로 나타나도록 해야 한다. 4단계 보안통제항목 평가에서는 선택한 통제항목이 올바르게 구현되어 최초 의도한 대로 작동하고 있는지와 시스템과 조직에 대한 보안 및 개인정보보호 요구사항을 충족하고 있는지 등을 종합 판단하여 만족할만한 결과가 시현되는지 확인해야 한다. 5단계 시스템 인가에서는 보안통제항목에 대한 평가 후 미비점의 보완 등을 점검하고, 시스템 운영 시 문제가 발생하지 않는지를 확인하여 인가해야 한다. 6단계 보안통제항목 모니터를 통해 시스템 운영 간 변경 사항이나 추가 위험요소가 식별되면 1단계부터 다시 RMF 절차를 반복하여 시스템 보안계획을 최신화하고 보안통제항목을 개선하는 선순환적 환류 구조로 진행해야 한다.

Ⅳ. 최적의 KRMF를 위한 시스템 분류 적용방안

RMF 7단계 중 가장 중요한 단계는 보안통제항목을 도출해내는 최초 시발점인 1단계 시스템 분류(Categorize System)일 것이다. 현재 우리 군(軍)에 적용하고 있는 보안통제항목은 미국의 RMF에서 적용하고 있는 보안통제항목에 비해 정보유형과 세부 항목 수 등에서 부족한 것은 사실이다. 따라서 우리 군(軍)도 빠르게 기술이 변화하고 있는 사이버 환경을 고려하고 사이버 위협에 대한 보안 활동을 강화하기 위해 새로운 보안통제항목의 개발이 절실하게 필요하다.

우선 1단계 시스템 분류(Categorize System)를 수행하기 위해 정보유형을 식별하고 식별된 정보유형별 보안 분류(보안목표 : 기밀성, 무결성, 가용성)에 대해 잠정 영향 수준 분석(Low, Moderate, High)을 선정함으로 시스템 분류가 종료된다. 이를 도식화하면 Figure 4와 같다.



<Figure 4> Classification procedure of Step 1 system

그러나 대한민국은 이러한 정보유형별 보안 분류를 처음 시도하는 것이기 때문에 그동안 운영해 온 미국의 정보유형 분류에 비해 걸음마 수준이다. 미국의 정보유형은 크게 임무기반 정보유형(중분류 26개, 소분류 100개)과 관리 및 지원 정보유형(중분류 13개, 소분류 77개)으로 분류되어 있다. 임무 기반 정보유형은 임무지역과 정보유형 19개(세부 항목 76개), 서비스 제공구조와 정보유형 7개(세부 항목 24개)로 자세하게 구분되어 있고, 관리 및 지원 정보유형은 서비스 배달지원 기능 및 정보유형 8개(세부 항목 42개), 정부 자원관리 정보유형 5개(세부 항목 35개)로 세분화되어 있다.

다만 미국과 다른 여건(국력, 문화, 환경 등)을 보유하고 있는 대한민국에 미국과 동일한 정보유형을 적용할 수 없기 때문에 “대한민국은 정보유형별 보안 분류를 위해 어떤 기준을 적용해야 할 것인가?”에 대한 고려가 필요하다. 궁극적으로 대한민국도 미국과 같이 무기체계 전력증강 사업에 사이버보안 관련 보안목표(기밀성, 무결성, 가용성)를 달성하기 위해 대한민국 국방부 주도로 정부의 각 부처를 이끌어가야 한다. 그러나 미국과 같은 제도로 정착되어 대한민국 국방부가 주도권을 갖기 위해서는 법적 근거 마련과 타 정부 부처와 협의 등을 위해 많은 시간이 필요할 것으로 예상되는 바, 가장 현실적으로 적용할 수 있는 방안을 모색해 본다면 국방부가 구현하고자 하는 목표와 미국의 정보유형 분류(임무기반 정보유형, 관리 및 지원 정보유형 등)를 참고하여 적정 수준의 시스템으로 분류를 우선 시행하고 추후 이를 보완하고 발전시켜 완전성을 기하는 방법이 현실적인 적용방안일 것이다.

Figure 5와 같이 정보유형을 식별하기 위해 20년 이상 군 근무 경력이 있는 전문가와 토의를 하였지만, 과학적 의사결정방법(델파이, AHP 등)을 적용하여 식별한 것은 아니다. 비록 과학적인 의사결정방법을 적용하지는 못하였으나, 객관적인 정보유형 식별을 위해 국방백서에 언급된 정부의 방침과 대한민국의 안보 현안 등을 다각적으로 연구하여 작성하였다. 향후 후속 연구 진행 시에는 과학적 의사결정방법을 적용하는 것이 필요하다.

4.1 KRMF 1단계 정보유형 분류(대분류(Section), 중분류(Division))

일반적으로 군사전략은 대한민국이 추구하고자 하는 국가안보전략과 국방정책을 군사적 차원에서 구현하기 위해 군사전략 목표를 설정하고 이를 달성하기 위한 군사력 운용개념과 군사력건설

방향을 구체화한 것이다.[15] 군사전략 목표는 아군의 장점을 최대한 살려 적의 취약점을 공격하고 만약 아군의 취약점이 발생하면 이를 보완하기 위해 물리적 또는 비물리적 수단을 마련하는 것이다. 일반적으로 국가안보 위협 요인에 대비하고 국익과 군사전략 목표를 달성하는 효과적인 방안은 군사력인 무기체계 전력증강(전투기, 미사일 등 타격 수단)을 통해 직접 위협을 감소시키거나 제거하는 것이다.

2020년 국방부에서 발간한 국방백서에서도 군사전략의 목표를 안보환경의 급격한 변화를 고려하여 북한의 위협과 잠재적 위협 그리고 비군사적 위협에 동시에 대비하며 외부의 도발과 침략을 억제하고 억제 실패 시 '최단시간 내 최소피해'로 전쟁에서 조기에 승리를 달성하는 것[16]으로 명시하고 있다. 따라서 전방위 안보위협에 유연하게 대응하고 군사전략의 목표를 달성하기 위해 여러 가지 변수를 다각적으로 고려해야 한다. 우선 위협에 대한 정의를 명확하게 설정해야 하고 그 위협에 대한 수준이 어느 정도인가를 판단할 수 있는 능력을 보유해야 하며 그 위협에 대해 실질적으로 대비하기 위해 군사력건설 방향(지휘구조, 부대구조, 병력구조, 전력구조 등)을 설정해야 할 것이다. 또한, 대한민국은 한미동맹을 기반으로 시행하는 실질적인 연합・합동 연습 및 훈련, 자연재해 등 비군사적 위협에 대해서는 국내・외 국민 보호를 위한 대비와 효율적인 정보공유 및 공동 대응 체계의 구성을 위해 관련 기관과 공고한 협조체계를 구축하는 한편 상황 발생 시에는 신속한 대응이 가능하도록 정보유형별 분류에 이 사항들도 반영되어야 한다. 미국이 개발한 정보유형별 보안 분류를 살펴보면, 너무 상세한 수준까지 개발하지 않았다는 것은 정보담당자로 하여금 정보유형별 보안 분류를 실질적으로 적용해 융통성을 부여하고 혼돈을 방지하기 위함으로 판단된다.

KRMF(한국형 위험관리체계) 1단계 시스템 분류(Categorize System)는 국방백서의 내용 등과 전문가들의 의견, 연구자의 근무경험 등을 바탕으로 작성하였다. 정보유형별 분류는 크게 대분류 10개(안보위협 등), 중분류 37개(직접 위협 등)으로 구분할 수 있다. 대분류는 군사전략 목표를 달성하기 위한 주요 임무에 따른 구분이며, 중분류는 대분류의 임무를 달성하기 위해 수행해야 하는 주요 항목을 나타낸다(Table 7). 보안 분류(기밀성, 무결성, 가용성) 영향 수준에 대한 판단이 필요한 사유는 정보를 다양한 위협으로부터 보호하기 위함이다. 즉 인가되지 않은 누군가로부터 정보의 훼손, 변조, 유출 등을 방지[17]하기 위해 정보보안의 3대 요소인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)에 대한 검토가 반드시 필요하다.

---

15) 『2020 국방백서』(국방부 정책기획관실, 2020), p.41. https://www.mnd.go.kr/cop/pblictn/selectPublicationUser.do?siteId=mnd&componentId=14&categoryId=15&publicationSeq=897&pageIndex=1&id=mnd_040501000000

16) 『2020 국방백서』(국방부 정책기획관실, 2020), p.41. https://www.mnd.go.kr/cop/pblictn/selectPublicationUser.do?siteId=mnd&componentId=14&categoryId=15&publicationSeq=897&pageIndex=1&id=mnd_040501000000

17) 사이버작전사령부, 『알기 쉬운 도해식 사이버전 용어사전』(출판사 : 국군인쇄창, 2019), p.245.

<Table 8> Classification of Step 1 system at KRMF

Section (10ea)		Division (37ea)	Security Classifications (Confidentiality, Integrity, Availability)
①	Security Threats	Direct threats, Potential threats, Non-military threats (3ea)	○
②	Military Forces Construction	Defense Budget, Command Structure, Troop Structure, Military Personnel Structure, Military Power Structure (5ea)	○
③	Acquire military power	Ground (Army), Maritime (Navy), Air (Air Force), Cyber, Space (5ea)	○
④	Military Forces Operations	Command and Control, Military Operations, Military Power Protection, Practice/Training (4ea)	○
⑤	Maintain power operation	Integrated system support, Combat development support (2ea)	○
⑥	Intelligence Operations	Information Collection, Data Processing, Information Analysis, Information Production (4ea)	○
⑦	Military Support・Cyber	Command and Communications, Military Security, Cybersecurity, Personnel Management (4ea)	○
⑧	Military Strength Development	Defense Space Force, Defense Science and Technology, Combat Development (3ea)	○
⑨	Disaster Management	Disaster Monitoring, Disaster Preparedness, Disaster Recovery, Emergency Response (4ea)	○
⑩	External Cooperation	Public Relations/Public Affairs, Civil-Military Cooperation, Cooperation of Departments of the Whole Government (3ea)	○

KRMF(한국형 위험관리체계) 1단계 시스템 분류(Categorize System)를 수행하기 위한 정보유형별 분류의 대분류와 중분류를 연구자가 선정한 사유는 다음과 같다.

---

① 동북아지역에서 대한민국은 책임국방을 실현하고 강한 국가안보를 달성하기 위해 직접 위협, 잠재 위협, 비군사 위협 등에 대해 항상 대비해야 한다. 특히 한반도는 주변국 이해관계가 상충되는 전략적 요충지이므로 군사적 위협에 대응하기 위해 적극적인 방어 체계구축과 비군사적 위협(국내・외 테러 등)에 신속하고 능동적으로 대응하기 위해 군 대테러특공대 및 유형별 대테러 작전부대를 추가로 지정하고 민・관・군・경의 효율적인 통합방위체계를 구성하여 철저한 대비태세를 확립하여야 한다.

② 군사력 건설은 급변하는 안보환경에 능동적으로 대처하고 전방위 안보위협에 유연하게 대응하기 위해 투입되는 국방예산과 우리 군(軍)의 지휘구조, 부대구조, 병력구조, 전력구조 등에 대해 체질을 강화하고 미래전장 환경에 적극적으로 대비해야 한다.

③ 미래전을 대비하기 위한 첨단 과학기술 기반의 군사력 획득으로 전장 구조가 전통적인 지상・해상・공중의 3차원에서 우주와 사이버공간이 추가된 5차원으로 변화될 것이므로 우리 군(軍)의 정예화를

통해 지상(육군), 해상(해군), 공중(공군), 사이버, 우주 공간에 대비할 수 있도록 철저히 준비할 필요가 있다.

④ 군사력 운용은 주변국 및 북한의 핵・미사일 위협을 효과적으로 억제하고 대응하며 한반도의 항구적 평화체제를 정착시키기 위해 완벽한 지휘통제, 치밀한 군사작전, 동맹의 포괄적 핵・미사일 대응 전략[4D(탐지 Detect → 방어 Defense → 와해 Destruct → 파괴 Destroying) 작전개념 적용 등]에 기반한 전력방호, 발전된 무기체계와 작전 운용체계를 최대로 활용하여 주기적인 연습 / 훈련 등을 지속 보완 발전시켜야 한다.

⑤ 전력 운영유지는 군이 보유하고 있는 무기체계의 효과적이고 경제적인 운영유지와 수명주기 동안 가동율 향상, 수리부속의 단종 등으로부터 후속군수지원의 제한을 극복하기 위한 통합체계지원 및 원활한 장비의 운영을 위한 전투발전지원 등을 확보해야 한다.

⑥ 주변국 위협(군사 활동 포함)에 대비한 조기경보 태세와 전・평시 북한의 도발에 즉각 대응할 수 있는 군사대비태세를 유지하기 위해 정보작전은 정보수집, 정보처리, 정보분석, 정보생산 등을 보장할 수 있도록 능력을 확보해야 한다.

⑦ 최첨단 정보통신기술과 발달된 인프라 구축에 따라 이에 비례하여 증가하고 있는 사이버 위협 대비 우리 군(軍)도 국방 사이버공간에서 우위를 확보하기 위해 상응하는 군사지원・사이버 대책을 마련해야 된다. 즉 지휘관의 신속한 의사결정이 가능하도록 완벽한 지휘통신 구축, 철저한 군사보안 대비태세 유지, 사이버 환경에 걸맞는 사이버안보 체계구축, 타 전장보다 사이버 인력의 전문성에 의해 작전역량이 크게 좌우되므로 사이버 전문인력지원 등 종합적인 인사관리 정책을 보완 발전시켜야 한다.

⑧ 우리 군(軍)도 변화하는 우주 안보환경에 능동적으로 대처하기 위하여 지난 2019년에 국방부 차원의 「국방우주력 발전 기본계획서」를 개정하였다. 또한, 한미 미사일 사거리 지침 종료에 따라 우주발사체 핵심기술과 부품에 대한 의존과 종속에서 벗어나고 자주성을 확보할 수 있도록 군사력 발전을 추진해야 한다. 이를 위해 국방우주력(우주전력 확충 등), 국방과학기술(핵심기술 연구개발 등), 전투발전(전투실험 등)에 대해 발전시켜야 할 것이다.

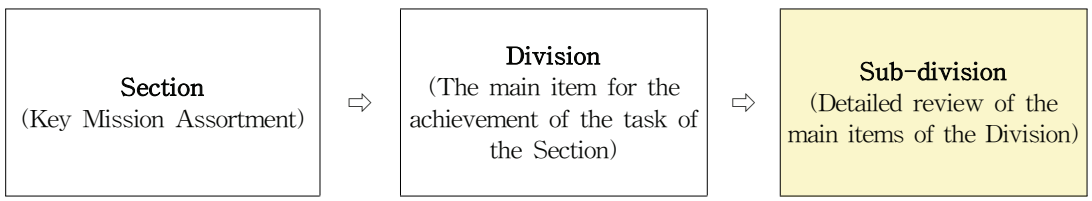
⑨ 재해관리는 세계적인 유행에 따른 감염병(코로나 19, 아프리카돼지열병 등)과 비정상 자연현상(태풍・호우・대설・홍수・해일・지진 등) 및 그 밖의 재해 원인(화재・폭발, 방사성물질 방출, 선박 침몰, 항공기의 조난 등)으로 인해 국민의 생명과 재산 등의 심각한 위협을 초래하는 새로운 안보위협에 대해 국방부를 포함한 범정부 차원에서 재난감시, 재난대비, 재난복구, 비상대응을 고려해야 한다.

⑩ 대외협력은 고효율・신뢰성・개방성을 기반으로 선진화되고 효율적인 국방운영을 달성하기 위해 홍보 / 공보(국민의 눈높이에 맞는 병영문화 개선 등), 민군협력(국제수준의 경쟁력 확보를 위한 방위사업 개선 등), 범정부 협력 등에 대해 고려해야 한다.

4.2 KRMF 1단계의 소분류 절차

앞서 설명한 대분류는 군사전략 목표를 달성하기 위한 주요 임무에 따른 구분이며, 중분류는 대분류의 임무를 달성하기 위해 수행해야 하는 주요 항목으로 정의했다. 그렇다면 중분류는 어떤 세

부 검토사항들로 구성되어야 할까? 중분류의 주요 항목 달성 여부를 판단하는 기준이 되는 것이 소분류인데, 소분류는 중분류의 주요 항목에 대한 세부 검토사항으로 구성하였다. 소분류의 세부 검토 시 기밀성 / 무결성 / 가용성에 대해 각각의 영향 수준 평가를 활용하여 중분류의 주요 항목 달성 여부를 판단하는 방식을 적용하였다. 이를 도식화하면 Figure 5에서 보는 바와 같다.



<Figure 5> Identification procedure of information type for classification of Step 1 system

앞서 KRMF(한국형 위험관리체계) 1단계 시스템 분류(Categorize System)를 수행하기 위한 정보유형별 분류의 대분류(10개, 임무 구분), 중분류(37개, 주요 항목)을 선정하였고, 소분류(108개, 세부 검토사항)를 정리하였다(Table 9). 연구의 이해도를 높이기 위해 다음과 같이 설명하고자 한다. 예를 들면 첫 번째 숫자가 대분류(주요 임무 구분)를 의미하며 두 번째 숫자는 중분류(대분류의 임무달성을 위한 주요 항목)에 해당함을 의미한다. 따라서 ①(안보위협)-ⓐ(직접 위협), ②(군사력 건설)-ⓐ(국방예산) 이하의 내용은 ①-ⓐ, ②-ⓐ 등으로 표현하였으며 관련 소분류를 연구자가 선정한 사유에 대해 설명하면 아래와 같다.

<Table 9> Classification of information type in Step 1 system at KRMF

Section (10ea)		Division (37ea)	Sub-division (108ea)
①	**Security Threats** (sub-division: 10ea)	ⓐ Direct threats	Nuclear weapons, Weapons of Mass Destruction, Theater ballistic missiles, Local provocation
		ⓑ Potential threats	Arms races, Territorial issues, Exclusive economic zones, Disputes over air defense identification zones
		ⓒ Non-military threats	Counterterrorism, Cyber Attacks
②	**Military Forces Construction** (sub-division:15ea)	ⓐ Defense Budget	Defense Improvement Costs, Power Operation Costs
		ⓑ Command Structure	Development of the future command structure, Revision of the National Army Organization Law
		ⓒ Troop Structure	Command Corps, Combat Units, Combat Support Units, Military Support Units
		ⓓ Military Personel Structure	Reinforcement of combat unit leaders, Expansion of civilian personnel in non-combat sectors, Maintenance of reduced adequate forces
		ⓔ Military Power Structure	Strategic target strikes, South Korean missile defense system, Overwhelming response, 4D power upgrade

Section (10ea)		Division (37ea)	Sub-division (108ea)
③	**Military Power Acquisition** (sub-division:5ea)	ⓐ Ground (Army)	Securing Ground Advantage
		ⓑ Maritime (Navy)	Securing Maritime Dominance
		ⓒ Air (Air Force)	Securing Air Superiority
		ⓓ Cyber	Securing Cyber Advantage
		ⓔ Space	Securing Space Advantage
④	**Military Forces Operations** (sub-division: 12ea)	ⓐ Command and Control	Command Guidelines, Real-Time Battlefield Information Sharing, Decision System Enhancement
		ⓑ Military Operations	Operation Plan, Joint Operations Warfare, Ground, Maritime and Air Operations
		ⓒ Military Power Protection	Nuclear and missile defense, Weapons of Mass Destruction defense, protection of key infrastructure
		ⓓ Practice /Training	Coalition and Joint Planning, Coalition and Joint Implementation, Coalition and Joint Evaluation
⑤	**Force Operation and Support** (sub-division: 16ea)	ⓐ Integrated system support	System Support Management, Research and Design Reflection, Maintenance, Maintenance Planning and Management, Support Equipment, Supply Support, Manpower Operation, Technical Teaching and Technical Data, Education & Training and Support, Packaging, Handling, Storage and Transportation, Facilities, Support Information System
		ⓑ Combat development support	Military doctrine, Troop formation, Facilities, Hardware and Software necessary for interoperation
⑥	**Intelligence Operations** (sub-division: 12ea)	ⓐ Information Collection	Objects to be collected, ability to collect assets, and utilization of collected information
		ⓑ Information Data Processing	Information processing system, Proficiency of information processing personnel, Utilization of multi-source collected information
		ⓒ Information Analysis	Logic of analysis, Appropriate analysis tools, Command and determination support
		ⓓ Information Production	Scope of uses of information, customer requirements, information diffusion effect
⑦	**Military Support · Cyber** (sub-division: 12ea)	ⓐ Command & Communications	Battlefield network, Battlefield management system, Battlefield system interlocking
		ⓑ Military Security	Personnel, Document, and Facility Security
		ⓒ Cyber security	Cyber Policy, Cybersecurity, Cyber Operations
		ⓓ Personnel Management	Workforce planning, Personnel operations, Education and Training
⑧	**Military Strength Development** (sub-division: 9ea)	ⓐ Defense Space Force	Building a policy base, Developing an operating system, Expanding space power
		ⓑ Defense Science and Technology	R & D of key technologies, Technology transfer, Protection of intellectual property rights, Combat development support
		ⓒ Combat Development	Combat Experiments, Warfare Analysis, Defense M & S

Section (10ea)		Division (37ea)	Sub-division (108ea)
⑨	**Disaster Management** (sub-division: 8ea)	ⓐ Disaster Monitoring	Natural disasters (typhoons, earthquakes, etc.), social disasters (infectious diseases, etc.)
		ⓑ Disaster Preparedness	
		ⓒ Disaster Recovery	
		ⓓ Emergency Response	
⑩	**External Cooperation** (sub-division: 9ea)	ⓐ Public Relations / Public Affairs	Policy Promotion, Media Response, Defense Media Operation
		ⓑ Civil-Military Cooperation	Defense R&D Spin-Up, Localization of Key Technologies and Components, Promotion of Defense Exports
		ⓒ Cooperation of Departments of the Whole Government	Establish an integrated crisis management system, Strengthen integrated defense capabilities, Integrated Protection of Overseas People

---

・①-ⓐ : 국가가 추구하는 궁극적인 목적은 국가의 생존과 번영에 있다.[18] 국가안보는 국가가 수행하는 가장 기본적인 기능 중 하나이며 국가 내외의 각종 위협으로부터 국민, 영토, 주권에 대한 보호를 해야한다. 우리의 생존과 번영에 반해 안보를 직접 위협하는 핵무기, 대량살상무기, 전구탄도탄, 국지도발 등에 대해 세부 검토사항을 고려해야 한다.

・①-ⓑ : 잠재 위협은 현재 또는 가까운 미래에 예상되는 위협으로 향후 특정 요인 또는 정치, 외교적인 역학관계의 변화에 따라 발생할 수 있다. 대한민국을 둘러싸고 있는 잠재 위협에 효과적으로 대응하기 위한 주변국에 의한 군비경쟁, 영토문제, 배타적 경제수역 및 방공식별구역 분쟁 등[19]에 대한 세부 검토사항을 고려해야 한다.

・①-ⓒ : 비군사 위협은 국가 및 비국가 행위자의 군사력 이외 수단 또는 자연적인 요인에 의해 발생하며, 국가안보를 위태롭게 하는 요소이나 초국가적 위협요인인 국제테러와 전(全) 세계적으로 발생하는 사이버 공격은 비군사적 위협이면서 동시에 군사적 위협[20]이 되고 있다. 특히 테러는 어떤 특정한 이념을 가진 조직이 일반인을 대상으로 폭력적인 수단을 통해 대중의 공포를 조장함으로써 자신들의 정치적 목적을 달성하려는 행동을 의미한다. 점점 정교해지고 복잡해지는 테러에 대한 대응을 위해 국내 발생, 국외 발생, 국내외 동시 발생 등 테러의 발생 지점 등을 기준으로 다각적인 검토가 필요하다.

・②-ⓐ : 국방예산은 우리 군(軍)을 편성하고 유지하는데 소요되는 예산으로 군사력 건설에 투입되는 방위력개선비와 군사력 운영에 소요되는 전력운영비 2가지로 구분되어 있다. 효율적인 국방예산의 집행을 통해 튼튼한 국방태세 확립을 지속 유지해야 한다.

・②-ⓑ : 미래전에서 필요로 하는 합동성은 각 군별 이기주의에 기반한 조직의 통・폐합보다는 서로 다른

18) 합동참모본부『군사기본교리』(출판사 : 국군인쇄창, 2014), p.9.

19) 합동참모본부『군사기본교리』(출판사 : 국군인쇄창, 2014), p.6.

20) 합동참모본부『군사기본교리』(출판사 : 국군인쇄창, 2014), p.7.

군 조직들의 상호 협동 및 팀워크를 통해 시너지 효과가 최대로 발휘될 수 있도록 지휘구조를 개편해야 한다. 한편 전시작전통제권전환과 관련하여 너무 급하게 서두르면 한미동맹과 대한민국의 안보에 균열이 발생할 수 있으므로 신중한 결정이 필요하다. 이러한 점을 차근차근 고민하여 앞으로 지휘구조는 미래 지휘구조 발전, 국군조직법 개정 등까지 세부 검토사항을 고려해야 한다.

- ②-ⓒ : 부대구조는 국방부로부터 승인된 정원을 기초로 지휘부대, 전투부대, 전투지원부대, 군수지원부대 등으로 구분하여 전투력 발휘가 용이하도록 지휘 제대별로 형성된 체계에 대한 세부 검토사항을 고려해야 한다.
- ②-ⓓ : 병력구조는 대한민국 인구절벽 시대의 도래에 따른 병역자원 감소(Ko, 2020)를 반영할 수 밖에 없는 상황이 되었다. 이에 따른 전투부대 간부 보강, 비전투분야 민간인력 확대, 감축된 적정 병력 유지 등에 대해 세부 검토사항을 고려해야 한다.
- ②-ⓔ : 전력구조는 대한민국 주변의 위협을 고려한 전투력의 수단을 가장 효율적으로 적용하기 위해 전략표적 타격, 한국형 미사일 방어체계, 압도적 대응, 4D 전력 고도화 등에 대해 세부 검토사항을 고려해야 한다.

- ③-ⓐ : 지상(육군)은 대한민국 주변의 위협을 다각적으로 고려하여 전투 효용성을 극대화하기 위해 지상우세 확보 등에 대해 세부 검토사항을 고려해야 한다.
- ③-ⓑ : 해상(해군)은 대한민국 주변의 위협을 다각적으로 고려하여 전투 효용성을 극대화하기 위해 해상우세 확보 등에 대해 세부 검토사항을 고려해야 한다.
- ③-ⓒ : 공중(공군)은 대한민국 주변의 위협을 다각적으로 고려하여 전투 효용성을 극대화하기 위해 공중우세 확보 등에 대해 세부 검토사항을 고려해야 한다.
- ③-ⓓ : 사이버공간 상에서 보안목표(기밀성, 무결성, 가용성)가 보장되지 않는다면 군사작전의 완전성을 기대할 수 없고 최첨단 무기체계도 무용지물로 전락시킬 수 있으므로 사이버우세 확보 등에 대해 세부 검토사항을 고려해야 한다.
- ③-ⓔ : 우주에 대해 군이 적으로부터 방해받지 않고 자유롭게 적에 대해 우주 작전을 수행할 수 있도록 우주우세 확보 등에 대해 세부 검토사항을 고려해야 한다.

- ④-ⓐ : 지휘통제는 임무의 목표를 달성하기 위해 자원을 효과적으로 이용하여 군사력을 행사하는 기능인 지휘(指揮, command)와 작전 실행에 필요한 물자 등을 배분하고 지휘관의 의도를 달성하기 위해 감독하는 통제(統制, control)를 의미한다. 즉 지휘지침, 실시간 전장 정보공유, 의사결정체계 고도화 등이 지휘통제의 핵심이므로 이에 대한 세부 검토사항을 고려해야 한다.
- ④-ⓑ : 군사작전은 전・평시(각종 분쟁 포함)에 군사전략의 목적을 달성하기 위해 다양한 지역에서 군사적 수단을 사용하는 제반 군사행동으로 작전계획, 합동작전, 지・해・공 작전 등에 대해 세부 검토사항을 고려해야 한다.
- ④-ⓒ : 전력방호는 대한민국 주변의 위협으로부터 국민의 생명, 국가 핵심시설 및 전력 등을 방호하기 위해 전력을 구축하고 운용하는 것으로 핵・미사일 방어, 대량살상무기(WMD) 방어, 주요 기반시설 보호 등에 대해 세부 검토사항을 고려해야 한다.

・④-ⓓ : 연습 / 훈련은 전시 대비 한미 간의 연습/훈련만을 의미하지 않으며 범정부 차원에서의 테러 및 재해관리 등에 대한 다각적인 연습/훈련이 필요한 실정이다. 다만 현재 국방부 차원으로 한정하여 정보유형을 분류한 것이므로 연합・합동 계획, 연합・합동 실행, 연합・합동 평가 등에 대해 세부 검토사항을 고려해야 한다.

・⑤-ⓐ : 통합체계지원은 소요제기 단계부터 획득, 운용유지 및 처분 시까지 전 과정에 걸쳐 체계를 효과적이고 경제적으로 운영 유지하기 위해 소요를 식별, 설계반영, 확보, 관리하는 활동을 총칭한다. 이 활동들은 궁극적으로 체계의 가동률(운용가용도) 향상과 수명주기비용 감소에 기여[21]하며, 체계지원관리, 연구 및 설계반영, 유지관리, 정비계획 및 관리, 지원장비, 보급지원, 인력운용, 기술교범 및 기술자료, 교육훈련 및 지원, 포장・취급・저장・수송, 시설, 지원정보체계 등에 대해 세부 검토사항을 고려해야 한다.

・⑤-ⓑ : 전투발전지원은 무기체계 획득과 연계하여 개발・획득하여 지원하는 요소로서 군사교리, 부대편성, 교육훈련, 시설, 무기체계 상호운용에 필요한 하드웨어 및 소프트웨어(주파수 확보 포함)[22] 등에 대해 세부 검토사항을 고려해야 한다.

・⑥-ⓐ : 정보수집은 군사정보시스템을 활용하여 확보하기 위한 정보순환단계의 초기 단계이므로 수집대상, 수집자산 능력, 수집정보 활용성 등에 대해 세부 검토사항을 고려해야 한다.

・⑥-ⓑ : 정보처리는 정보순환단계 중 처리단계를 중심으로 지능정보기술을 적용하여 자동화와 지능화를 추진[23]하고 있으며 이는 정보처리체계, 정보처리요원 숙련도, 다출처 수집정보 활용 등을 종합하여 세부 검토사항을 고려해야 한다.

・⑥-ⓒ : 정보분석은 현재의 인력 중심에서 지능정보기술을 활용함으로써 효율적인 정보분석 및 능동적인 예측이 가능하도록 관련 능력에 대해 분석의 논리성, 적절한 분석툴, 지휘결심 지원 등에 대한 세부 검토사항을 고려해야 한다.

・⑥-ⓓ : 정보생산은 군사정보시스템을 활용하여 정보순환단계의 최종 단계에서 작성되는 것이며 정보의 활용범위, 수요자의 요구사항, 정보의 파급효과 등을 다각적으로 고려해야 한다.

・⑦-ⓐ : 지휘통신은 임무 수행에 필요한 우리 군(軍)의 지휘통제를 위한 유무선 통신망을 구축하고 운용하는 것을 의미하며 특히 전장네트워크, 전장관리체계, 전장체계연동 등에 대해 세부 검토사항을 고려해야 한다.

・⑦-ⓑ : 군사보안은 비인가자의 탐지행위로부터 국가의 안전보장에 영향을 미치는 인원, 군사자료, 시설(통제/제한/보호구역) 등을 보호하는 제반 활동으로 인원보안, 문서보안, 시설보안 등에 대해 세부 검토사항을 고려해야 한다.

・⑦-ⓒ : 사이버안보는 국가의 안전보장을 목표로 사이버공간에서 발생하는 적대세력들로부터 사이버 위

---

21) 국방부『국방전력발전업무훈령』(출판사 : 국군인쇄창, 2022), p.180.

22) 국방부『국방전력발전업무훈령』(출판사 : 국군인쇄창, 2022), p.176.

23) 조성림(2020). 지능형 군사정보 발전방안. KIDA Brief, pp. 1-4. https://kida.re.kr/cmm/viewBoardImageFile.do?idx=28186

협에 대해 아군의 사이버공간을 보호하기 위한 것이며 이를 위해 사이버정책, 사이버보안, 사이버작전 등에 대해 세부 검토사항을 고려해야 한다.

- ⑦-ⓓ : 사이버에서의 인사관리는 타 전장보다 사이버 인력의 전문성에 의해 작전역량이 크게 좌우되므로 사이버 전문인력지원 등을 대상으로 종합적인 인사관리 정책을 수립해야 하며 세부 검토사항으로 인력계획, 인력운영, 교육훈련 등이 있다.

- ⑧-ⓐ : 4차 산업혁명 시대의 빠른 변화에 적응하기 위한 첨단 과학기술의 발전과 함께 우주가 전통적인 지상, 해상, 공중에 이어 새로운 전장이 이루어지는 공간이 되는 미래 안보환경 변화를 고려하기 위해 국방우주력은 정책기반 구축, 운영체계 발전, 우주전력 확충 등에 대해 세부 검토사항을 반영해야 한다.
- ⑧-ⓑ : 국방과학기술은 국방에 필요한 무기체계와 자동화 체계 등에 대한 기술적 조사, 연구개발 및 시험 등을 하는 것으로 핵심기술 연구개발, 기술 이전, 지적재산권 보호 등에 대해 세부 검토사항을 고려해야 한다.
- ⑧-ⓒ : 군사력 발전에서의 전투발전은 적대세력과 싸워서 승리하기 위해 장차전에 대비하는 총체적인 연구발전 노력이며 미래의 작전 요구능력을 과학적이고 합리적으로 판단하기 위한 것으로 전투실험, 전훈분석, 국방M&S 등에 대해 세부 검토사항을 고려해야 한다.

- ⑨-ⓐ : 재난예방은 위험과 관련된 각종 재난에 대해 완화를 하는 것이며 대상으로 자연 재난(태풍, 지진 등), 사회 재난(감염병 등) 등에 대해 세부 검토사항을 고려한다.
- ⑨-ⓑ : 재난대비는 각종 재난으로부터 피해를 대비하기 위한 훈련들과 국민의 인식을 향상을 위한 활동들을 포함하는 것으로 자연 재난(태풍, 지진 등), 사회 재난(감염병 등) 등에 대해 세부 검토사항을 고려해야 한다.
- ⑨-ⓒ : 재난대응은 각종 응급상황이나 재난이 발생한 후의 단계로 수색, 구조, 의료서비스 지원 등과 같이 자연 재난(태풍, 지진 등), 사회 재난(감염병 등)에 대해 세부 검토사항을 고려해야 한다.
- ⑨-ⓓ : 재난복구는 각종 재난으로부터 발생한 피해를 감소시키기 위한 모든 활동을 수행하는 단계이며 자연 재난(태풍, 지진 등), 사회 재난(감염병 등) 등에 대해 세부 검토사항을 고려해야 한다.

- ⑩-ⓐ : 국방에 대한 국민 신뢰도 제고와 국민의 눈높이에 부합하기 위해 홍보 / 공보는 정책홍보, 언론대응, 국방미디어 운영 등에 대해 세부 검토사항을 고려해야 한다.
- ⑩-ⓑ : 민군협력은 국내 방위산업 활성화 여건 보장, 민간 역량의 강화를 위해 업체주관 연구개발 및 범정부 차원의 무기체계 우수성 홍보를 통해 국방 R&D Spin-Up, 핵심기술・부품 국산화, 방산수출 증진 등에 대해 세부 검토사항을 고려해야 한다.
- ⑩-ⓒ : 범정부부처 협력은 북한의 다양한 도발 위협에 효과적인 대응과 화생방 위협, 사고, 테러, 감염병 등에 대한 범정부 차원의 대응 등을 위해 통합 위기관리체계 구축, 통합 방위역량 강화, 통합 재외국민보호 등에 대해 세부 검토사항을 고려해야 한다.

4.3 KRMF 1단계 잠정 영향 수준 분석

미국의 RMF 시스템 분류(1단계) 연구에서 언급한 바와 같이 소분류(108개, 세부 검토사항)에 대한 각각의 보안 분류(기밀성, 무결성, 가용성)의 잠정 영향성 평가 결과(Low, Moderate, High)를 작성해야 하는데 미국은 정보담당자가 이 업무를 담당한다. 우리도 무기체계에 따라 요구되는 잠정 영향 수준이 다르기 때문에 본 연구에서 일률적으로 결론을 도출하기는 어렵다. 다만, 잠정 영향 수준 분석을 하는 방법에 대해 예시를 살펴보면 Table 10과 같다. 예를 들어, 대분류 ⑧ 군사력 발전에 대한 중분류 ① 국방우주력을 평가하기 위해 소분류에 해당하는 정책기반 구축, 운영체계 발전, 우주전력 확충의 영향 수준을 평가하게 된다. 소분류(세부 검토사항)의 영향 수준 평가를 위해 앞서 설명한 Table 3은 보안 분류의 위반이 발생될 경우 조직과 개인 관점에서 잠정 영향 수준 분석에 대한 FIPS(Federal Information Processing Standards) 199의 정의[24]를 준용하여 평가하였다. 그러나 우리도 미국과 같이 잠정 영향 수준 분석에 대한 우리 군(軍)에 최적화된 정의를 제정하여 영향 수준 평가에 적용할 수 있도록 준비해야 한다.

2019년에는 국방부 차원에서 대한민국 주변국의 우주 안보환경 변화를 감지하고 '국방우주력 발전 기본계획서'를 개정하였다. 개정된 중장기 국방우주력 발전 목표를 위해 정책기반 구축, 운영체계 발전, 우주전력 확충 등 중점분야와 분야별 추진과제를 제시하였다.[25] 연구자가 생각한 ⑧-ⓐ 국방우주력 중 우주전력 확충에 대한 영향 수준 평가는 다음과 같다. 정부가 추진하고 있는 4차 산업혁명 인프라(위치, 항법, 시각)로서 한국형 위성항법시스템(KPS, Korea Positioning System)이 2022년 착수를 목표로 진행 중에 있다. KPS는 다수의 인공위성으로 구성될 것이고 군(軍)에서 운영하는 핵심 정밀무기에 필요할 뿐만 아니라 민간의 경제・사회 전반에 걸쳐서 중요한 역할을 담당할 것이다(e.g., Hein, 2020). 이러한 우주전력 확충(KPS)에 대한 기밀성(Confidentiality)은 적으로부터 위성의 물리적 파괴를 거부하고 정당한 권한이 부여된 사용자만 접근하도록 하며 비인가자로부터 정보를 보호하는 것으로 노출 시 조직 또는 개인에 가혹(severe)하거나 치명적인(catastrophic) 악영향을 미치게 되기 때문에 High(잠재 영향 높음)로 평가하였다. KPS의 무결성(Integrity)은 관리자가 인지하지 못하는 사이에 정보의 내용이 불법적으로 생성, 변경, 삭제되지 않도록 보호해야 하며, 정보의 무결성을 보장하지 못하면 조직 또는 개인에 가혹하거나 치명적인 악영향을 미치게 되므로 High(잠재 영향 높음)로 평가하였다. 만약 무결성이 보장되지 않는다면, 군(軍)의 정밀무장 사용 시 재밍을 받게 되고 민간의 경제・사회 전반에 엄청난 혼란이 발생할 것이다. KPS의 가용성(Availability)은 인가된 사용자가 언제든지 원하는 자료를 사용할 수 있어야 하

24) FIPS 199(Standards for Security Categorization of Federal Information and Information Systems 2004.02), pp. 2-3. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

25) 2020 국방백서. 국방부 정책기획관실, p.79. https://www.mnd.go.kr/cop/pblictn/selectPublicationUser.do?siteId=mnd&componentId=14&categoryId=15&publicationSeq=897&pageIndex=1&id=mnd_040501000000

고, 자료 사용이 불가하다면 조직 또는 개인에 가혹하거나 치명적인 악영향을 미치게 되므로 High (잠재 영향 높음)로 평가하였다. 만약 가용성을 보장받지 못한다면, 작전 수행 시 위성의 신호를 수신하여 움직이는 첨단 전력(전투기, 함정 등)에 악영향을 끼칠 것이다.

<Table 10> Example of security classification of information type at KRMF

Section (Mission Assortment)		Division (Main Items)	Sub-division	Impact Level Assessment		
				Confidentiality	Integrity	Availability
⑧	**Military Strength Development**	ⓐ Defense Space Force	Building a policy base	Low	Low	Low
			Developing an operating system	Moderate	Low	Moderate
			Expanding space power	**High**	**High**	**High**
		ⓑ Defense Science and Technology	R&D of key technologies	High	Moderate	High
			Technology transfer	High	High	Moderate
			Protection of intellectual property rights	High	High	High
		ⓒ Combat Development	Combat Experiments	High	High	High
			Warfare Analysis	Low	Low	Low
			Defense M & S	High	Moderate	Low

V. 결론 및 논의

1960년대부터 컴퓨터 보안의 중요성 관련 연구를 시작한 군사 선진국인 미국이 아직도 RMF 체계가 발전하고 있는 단계라고 언급하고 있는 것에 비교하면 대한민국은 지금 RMF 중요성을 인지하고 첫걸음을 하고 있다. 본 연구를 통해 미국을 중심으로 사이버보안 강화를 위해 개발된 미국 RMF 제도와 대한민국의 보안제도의 차이점을 분석하여 우리의 사이버보안 관련 현 실태를 진단하였다. 그 결과, 최첨단으로 발전하고 있는 사이버 위협에 능동적으로 대처하기 위해 국방부를 중심(Control Tower)으로의 사이버보안 관리구조 정립이 필요함을 느낄 수 있었으며, 우리 군(軍)도 각 기관별로 분리되어있는 사이버보안 활동에 대해 미국의 RMF처럼 소요기획 단계부터 국방획득체계 전반에 사이버보안이 보장되는 선순환적 환류 구조 정립의 필요성을 제기한다. 또한, 진단된

현 실태를 기준으로 무기체계 전력증강 사업에 반영해야 하는 보안통제항목 선정을 위해 미국의 RMF 7단계 프로세스 중 가장 중요한 1단계 시스템 분류를 집중적으로 분석하였고 우리 군(軍)에 맞춤형으로 적용(KRMF, 한국형 위험관리체계)하기 위한 첫 걸음인 시스템 분류 방향에 대해 세부적으로 연구해 보았다. 그 결과 대분류(10개)인 임무를 구분하고 대분류의 임무달성을 위해 중분류(37개)인 주요 항목을 도출하였으며, 중분류의 주요 항목에 대해 소분류(108개)인 세부 검토사항을 작성하였다. 이렇게 작성된 각각의 세부 검토사항은 보안 분류(기밀성, 무결성, 가용성) 영향성 평가를 진행한 결과가 2단계 보안통제항목 식별에 반영하게 된다. 본 연구는 KRMF의 성공을 위한 가이드 라인을 제시하기 위한 탐색연구 결과를 제시하였다는 점에서 학술적인 가치가 높다고 볼 수 있다. 또한, 한국형 위험관리체계(KRMF) 관련 위험에 대한 인식 제고와 정책적 개선방안 등을 제시하였다는 점에서 실무적 가치가 있다.

다만, 본 연구는 최적의 항목(대분류, 중분류, 소분류)을 도출하기 위해 다기준 의사결정 방법(AHP 방법, 컨조인트 분석 등)의 체계적인 방안을 적용하지 못하였다는 한계점이 있으므로 향후 후속 연구를 진행 시에는 시스템 분류에 필요한 주요 항목들을 도출하기 위해 검증된 방법론인 과학적 의사결정방법을 적용하는 것이 필요하다. 이를 위해 후속연구는 시스템 분류 방법을 보완하여 구체화하고 2단계(보안통제항목 선택) 및 기타 단계 등도 실질적으로 도출해야 한다. 현재뿐만 아니라 미래의 무기체계 사이버보안의 영역은 지금까지 우리 군(軍)이 접하지 못했던 매우 생소하고 높은 기술 수준을 요구하는 분야이기 때문에 한국형 위험관리체계 구축과 운용을 위해 국방부와 관계 기관의 적극적인 관심과 도전적인 업무 추진이 필요한 시점일 것이다.

Acknowledgements

We would like to thank Editage (www.editage.co.kr) for English language editing.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Author contributions

Conceptualization: KJ and JS; Resources and Data curation: KJ and JS; Investigation: KJ and JS; Methodology: KG and JS; Writing (Original Draft): KJ and JS; Writing (Review and Editing): KJ; Project administration and Supervision: KJ and JS

Reference

Cho, H. S., Cha, S. Y. & Kim, S. J. (2019). A Practical Case Study of RMF Applicationto Domestic Weapons Systems. *The Journal of the Society for Information Security, 29*(6), 1463-1475. https://doi.org/10.13089/JKIISC.2019.29.6.1463

Hein, G. W. (2020). Status, perspectives and trends of satellite navigation. *Satellite Navigation, 1*(1), 1-12. https://doi.org/10.1186/s43020-020-00023-x

Joo, Y. N. Kim, B. S., & Kwon, H. J. (2021). Suggestion of Risk Priority Identification Methodology for the Establishment of the Korean RMF System. *The Quarterly Journal of Defense Policy Studies*, 37(2), 99-130. https://doi.org/10.22883/jdps.2021.37.2.004

Kang, J. W., Choi, H. J., & Lee, H. H., (2019). Parsing analysis the Concept of Information Assurance through Literature Research. *The Journal of Convergence Security, 19*(1), 31-40. https://www.dbpia.co.kr/Journal/articleDetail?nodeId=NODE10088596

Kim, H. J., & Kang, D. S. (2019). A Design of Risk-Based Security Threat Assessment Process for Fighter-Aircraft Airworthiness Security Certification. *KIPS Transactions on Software and Data Engineering, 8*(6), 223-234. https://doi.org/10.3745/KTSDE.2019.8.6.223

Kim, I. J., Kang, J. W., & Shin, D. K. (2021). A study on the application of mission-based weapon system cybersecurity test and evaluation. *Korean Society for Internet Information, 22*(6), 71-81. https://doi.org/10.7472/jksii.2021.22.6.71

Ko, S. S., (2020). A Study on the Development Direction of the Reorganization of the Korean Military Structure Following the Reduction of Military Service Resources in the Population Cliff Era. *The Journal of Korean Military, 8*, 185-211. https://doi.org/10.33528/kjma.2020.12.8.185

Lee, S. M. (2021). A study on the application of RMF for weapon systems in Korea: weapons and security system integration. *Journal of Advances in Military Studies, 4*(3), 191-208. https://doi.org/10.37944/jams.v4i3.122

Lee, Y. S. & Choi, J. M. (2020). Research for Application the RMF to the Korean Military, *The Journal of Korean Institute of Communications and Information Sciences, 45*(12), 2132-2138. https://doi.org/10.7840/kics.2020.45.12.2132

Na, S. H. Shon, T. S, (2022). A Study on the Development of Information Security Management System Using RMF, *Journal of Digital Contents Society, 23*(5), 977-983. https://doi.org/10.9728/dcs.2022.23.5.977

Yang, E. I. (2018). Introduction to Information Security, 251.

원 고 접 수 일 2022년 06월 23일
원 고 수 정 일 2022년 08월 23일
게 재 확 정 일 2022년 08월 26일

IDAP 광운대학교 방위사업연구소 INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2022, Vol. 5, No. 2, 73-106.

https://doi.org/10.37944/jams.v5i2.151

한국형 위험관리체계(KRMF)의 성공을 위한 첫걸음: 시스템 분류 방향 연구

김재욱* · 정석재**

국문초록

미국이 적용하고 있는 RMF(Risk Management Framework, 위험관리체계)는 제품 개발 프로세스에 정보보안과 위험관리(Risk Management)의 개념을 서로 결합하여 기존에 적용하고 있었던 장비, 부품 등의 구성 체계 및 시설, 인원 등의 관련된 보안과 더불어 사이버공간이 포함된 보안 항목을 소요기획 단계에서부터 체계적으로 적용하여 무기체계 폐기 시까지 정보보안의 완전성을 달성되도록 만든 개념이다. 향후 우리 군이 사용하게 될 무기체계의 완벽한 성능을 보장하기 위해 전력증강 사업에 반영해야 하는 RMF는 대한민국 군(軍)에 생소한 분야로 육군, 해군, 공군 등 어느 군에서도 아직까지 세부적인 연구와 방안 등 기반이 갖추어져 있지 않은 걸음마 수준의 분야이다. 그러나 대한민국에 평시 주둔하고 있는 주한미군과 한반도에 위기상황 발생 시 연합사령관이 요청하고 美 합참의 지시에 의해 전개되는 미국의 전시증원전력[신속억제방안(FDO), 전투력증강(FMP), 시차별부대전개제원(TPFDD)]은 RMF 절차를 적용하여 사이버 위협에 철저한 대비를 하고 있기 때문에 우리 군(軍)도 연합합동작전을 위해 이와 상응하는 절차를 만들어 신속히 적용해야 할 것이다. 이번 연구의 대상을 RMF 프로세스 중에 가장 기본이 되고 중요한 1단계 시스템 분류(Categorize System)에 대해 발전 방향을 제시하였고, 향후 적용해야 할 KRMF(한국형 위험관리체계) 시행에 도움이 되었으면 한다.

주제어 : RMF(위험관리체계), 정보보안, 기밀성 · 무결성 · 가용성, 시스템 분류, 정보유형 식별, 잠정 영향 수준 분석

* (제1저자) 광운대학교 박사과정(합동군사대학교 제1합동교육처 공군 대령), afbmir@gmail.com, https://orcid.org/0000-0002-0019-8649

** (교신저자) 광운대학교, 경영학부, 교수, jsjjeong@kw.ac.kr https://orcid.org/0000-0001-8094-4674