Journal of the KNST

2025; Vol.8, No.1; pp.70-80

ISSN: 2635-4926 https://doi.org/10.31818/JKNST.2025.3.8.1.70

Received: 2025/02/25
Revised: 2025/03/07
Accepted: 2025/03/25
Published: 2025/03/31

*Corresponding Author:
Tae Shik Shon
Tel: +82-31-219-3321
E-mail: tsshon@ajou.ac.kr

K-RMF 조기정착을 위한 방위사업제도 발전방향

Development Directions for Defense Acquisition System to Facilitate Early Adoption of K-RMF

이진구[1], 손태식[2*]

[1]해군 대령/아주대학교 사이버보안학과 석사과정
[2]아주대학교 사이버보안학과 교수

Jin Goo Lee[1], Tae Shik Shon[2*]

[1]CAPT, ROK Navy/Graduate, Dept. of Cyber Security, Ajou University
[2]Professor, Dept. of Cyber Security, Ajou University

Abstract

한국 국방부는 2020년 K-RMF를 개발하였고, 시범적용과정을 거쳐 2023년 7월부터는 일부 연합체계 및 전장관리정보체계에 정식적용하였다. 그동안 한국군은 K-RMF 자체에 대한 완성도 향상과 함께 K-RMF 제도 정비에도 노력해왔으나, '국방사이버보안위험관리지시' 및 기존 방위사업과 관련된 훈령과의 상호 유기적 연결성이 미흡하고, K-RMF를 수행해야 하는 기관들의 이해가 부족한 실정이다. 본 연구는 미국과 한국의 RMF 지침에 대한 이해를 바탕으로 K-RMF 시행을 위해 추진했던 법령에 대한 제도적 보완, 기존 제도와의 중복성 최소화 등 K-RMF의 조기정착을 위한 방위사업제도 발전방향을 제시하였다.

The ROK Ministry of National Defense developed K-RMF in 2020, went through a pilot application process, and officially applied it to several combined systems and battlefield management information systems from July 2023. In the meantime, the ROK military has worked on improving the completeness of K-RMF itself and institutional reforms, but there is insufficient interconnection between the Instruction for RMF and existing directives related to defense projects, and there is a lack of understanding K-RMF. This study suggests directions for the development of defense acquisition systems for the early settlement of K-RMF, such as institutional supplementation of laws and regulations promoted for K-RMF implementation based on an understanding of RMF guidelines in the United States and the Repubic of Korea, and minimization of redundancy with existing systems.

Keywords

위험관리프레임워크(Risk Management Framework),
사이버보안(Cybersecurity),
방위사업(Defense Acquisition),
상호운용성(Interoperability),
시험평가(Test & Evaluation)

1. 서론

2022년 발발한 러시아-우크라이나 전쟁과 2023년에 발생한 이스라엘과 하마스 간 분쟁은 현대전에서 사이버전이 어떻게 자리매김하고 있는지를 여실히 보여주고 있다. 전통적인 물리적 공격에 앞서 전초전 양상으로 수행되던 이전의 사이버전과 달리, 개전 이전은 물론 개전 이후에도 국가 주도의 사이버전이 지속 수행되고 있으며, 이념과 종교 등이 대립하는 핵티비스트(hacktivist)들의 참전은 시·공간의 경계가 없고 페르소나 계층의 익명성이 두드러지는 사이버영역의 특성을 잘 나타내고 있다. 특히 대규모 DDoS 공격을 통한 정부·군·주요 기반시설 접속 차단, ViaSat에 대한 AcidRain 공격을 통한 위성 네트워크 교란, 전투관리시스템인 'Delta'에 대한 악성코드 유포 시도 등 러시아가 우크라이나에 감행한 사이버공격은 사회전반 및 군 무기체계에 대한 정보보호 안전성과 회복탄력성을 더욱 요구하고 있다.

미군은 1990년대 후반부터 군 정보시스템에 대해 보안성 관리/평가체계를 적용해 왔으며, 2014년부터 미국 정부표준을 기반으로 국방분야에 RMF(risk management framework)를 도입하였다. 또한, 2019년에는 자국 군사체계의 정보보호 안전성을 확보하기 위해 미군 시스템과 연동하는 동맹국 무기체계와 정보체계에도 RMF를 적용하도록 하는 정책을 결정하고, 한·미 연동체계에 RMF를 적용한 보안체계를 요구하였다. 이에 따라 대한민국 국방부는 2020년 1월 방첩사령부를 중심으로 K-RMF를 개발하였고, 2021년

에는 기존에 운용 중인 연합체계 및 각 군의 전장관리 정보체계를 선정하여 시범적용을 하였으며, 2023년 7월부터는 해당 체계에 대해 K-RMF를 정식적용하고 있다. 그러나 시범적용에 선정된 체계들은 애초에 RMF의 전 수명주기 개념에서 개발된 체계가 아니었기 때문에 접근통제, 장치식별 및 인증, 암호보호 등에서 보안통제항목이 부분적으로 구현되었거나 미구현된 항목이 일부 식별되고, 보안계획서 작성이 미흡하거나 보안계획서와 실제 현황이 불일치하는 등 K-RMF를 수행하는 데 많은 시행착오를 겪고 있다.

또한, 2024년 4월 한국군 RMF 시행을 위한 '국방 사이버보안 위험관리 지시'가 제정되었음에도 불구하고, 실제 방위사업을 추진해야 하는 소요군, 방사청 등에서는 여전히 무엇을 어떻게 해야 하는지에 대한 이해와 공감대 형성이 부족하고, 기존 '국방전력발전업무훈령'을 지원하는 국방상호운용성 평가와 사이버보안 평가의 내용과 절차가 일부 중복되어 개선이 필요하다.

본 연구에서는 2장에서 RMF에 대한 국내 연구 동향 및 관련 법령, 한국군의 K-RMF에 대한 인식을 확인하고, 3장에서는 한·미 RMF 제도의 특성과 수행절차, K-RMF 시범적용의 성과와 한계를 분석하고, 방위사업에서의 두 가지 사이버보안 평가 절차에 대한 통합가능성을 검증하였으며, 4장에서는 K-RMF 조기정착을 위한 발전방향을 제안하였다.

2. 관련연구

2.1 RMF와 관련된 국내 연구동향

RMF와 관련된 국내 연구는 2020년경부터 활발하게 이루어졌다. 그러나 미국의 RMF 제도는 미국표준기술연구소(NIST, National Institute of Standards and Technology)와 미 국방부 지침 등 공개된 자료를 통해 일부 연구가 가능하였으나, K-RMF는 공개된 자료가 거의 없어 실질적 연구가 제한되었다. 한국군의 비교연구 자료가 부족한 관계로 비교적 최근 발표된 연구논문들도 대부분 미군의 RMF 제도를 한국군에 적용하기 위한 방향성 제시에 그치고 있다.

안정근, 조광수, 정한진, 정지훈, 김승주는 K-RMF에 적용할 위협분석을 통해 보안요구사항을 식별하고, 개발하려는 시스템에 보안요구사항을 적용하기 위한 보안통제항목 도출방법을 제시하였으며, 향후 무기체계별 다양한 위협분석과 무기체계 개발 과정에서 방산업체와의 협업 필요성을 강조하였다[1].

이용석, 최정민은 한국군에 RMF를 적용하기 위하여 합참 내 RMF에 대한 기술적·정책적 수행 조직을 구성하고, 국방 RMF MKS(military knowledge service)를 구축하여 RMF 정책과 관련 법령 및 기준문서, 보안통제지침 등을 제공해야 하며, RMF 전문가 양성 및 확보, 한·미 간 RMF 실무협의체, 워킹그룹 구성 등 협력을 강화해야 한다고 제안하였다[2].

권혁진, 김성태, 주예나는 시스템공학에 기초한 위험관리 개념 도입을 통해 사이버보안 위험요소의 체계적 관리 시스템을 마련할 수 있도록 관련 법·제도를 정비하고, 방첩사 내 RMF 전담 조직 신설 및 전문인력 확충, RMF 기반 사이버보안 위험관리 자동화 체계 도입, 합참 및 각 군 본부, 국방부 직할기관 등에서의 RMF 전문가 양성 등을 제안하였다[3].

살펴본 연구 이외에도 위험우선순위 식별 방법론, 보안통제항목 선정 방법론 등과 같은 연구가 이루어지고 있으나, 앞서 언급한 바와 같이 대부분 RMF 특정 단계에서의 연구에 그치고 있으며, 관련 법령 및 현장 준비상태 등 우리나라 방위사업 환경에 적합한 K-RMF 시행 여건에 대한 연구는 부족한 실정이다.

2.2 K-RMF 관련 국내 법령

K-RMF를 위한 국방부 소관 법령은 '국방 사이버보안 위험관리 지시'와 '국방전력발전업무훈령', '국방사이버안보훈령'을 들 수 있다. K-RMF가 소요기획 단계에서 설계, 구현, 시험평가, 운용 및 폐기에 이르기까지 시스템 전 수명주기 동안 무기체계의 사이버보안 관리 및 평가를 위한 제도[4]라는 점에서 이들 법령은 상호 유기적으로 연결되어 있어야만 한다.

하지만 '국방전력발전업무훈령'이 '국방 사이버보안 위험관리 지시'보다 9개월 늦은 2015년 1월에 개정되었음에도 불구하고 '국방전력발전업무훈령'에는 무기체계 및 전력지원체계의 사이버보안 위험을 수명주기 관점에서 관리해야 한다는 K-RMF 개념이 충분히 반영되어 있지 않다. '국방사이버안보훈령'은 방위사업업무에 종사하는 모든 인원이 아닌 사이버 업무에 종사하는 인원이 수행해야 할 업무에 대한 기준과 지침만을 제공[5]하고 있다. 이를 종합하면 '국방

전력발전업무훈령’에 RMF 개념이 충분히 반영되었다거나, ‘국방사이버안보훈령’ 및 ‘국방 사이버보안 위험관리 지시’와 상호 유기적으로 연결되어 있다고 평가하기 어렵다.

‘국방전력발전업무훈령’이 무기체계와 전력지원체계의 소요·획득·운영유지를 포함하는 전력증강과 관련된 업무의 기본절차를 규정하고 지침을 제공[6]한다는 측면에서 K-RMF가 조기에 정착되기 위해서는 K-RMF가 사이버보안 업무에 종사하는 한정된 인원만이 수행하는 업무가 아니라 방위사업업무에 종사하는 모든 인원이 기본적으로 갖추어야 할 마인드가 될 수 있도록 ‘국방전력발전업무훈령’에 K-RMF 개념이 충분히 반영되도록 보완이 필요하다.

2.3 한국군의 K-RMF 인식 설문조사 결과

한국군의 K-RMF 인식에 대한 설문조사는 2024년 11월 8일부터 26일까지 육·해·공군본부, 해병대사령부 및 방위사업청에 근무하는 장교 및 부사관, 군무원, 공무원 등 총 165명의 간부들을 대상으로 실시하였다. 이 설문조사의 목적은 우리군이 이미 K-RMF를 정식적용하고 있으며, 향후 무기체계와 전력지원체계를 대상으로 점진적으로 확대 시행해야 하는 상황에서 방위사업 추진 간 소요제기기관과 사업관리기관 임무를 수행해야 하는 각 군 본부 및 해병대사령부, 방위사업청에서 근무 중인 간부들이 K-RMF에 대해 얼마나 이해하고 있는지를 확인하고, K-RMF의 조기정착을 위해 필요로 하는 사항은 무엇인지 현장의 의견을 청취하는 것이었으며, 설문조사 결과는 Table 1과 같다.

설문조사 결과를 살펴보면, 방위사업업무 경험 및 국방전력발전업무훈령 숙지도는 대부분 양호(근무경험 6~10회 이상 40 %, 전력발전업무훈령 숙지도 중급 경험자 이상 50 %)한 반면, K-RMF에 대한 이해도(초급경험자 이하 82 %) 및 교육 이수 경험(32 %)은 상대적으로 부족한 것을 확인할 수 있었다. 이는 K-RMF

Table 1. The survey result on the perception of K-RMF in the Korean military refinement

Question	Answer		
Q1. Affiliation	A. Army/Navy/AF/Marine Corps HQs.(40 %) B. HQs. subordinate(42 %)	C. DAPA(18 %)	
Q2. Rank	A. Field officer(54 %) D. CME(22 %)	B. Company officer(9 %) E. Gov. employee(10 %)	C. NCO(5 %)
Q3. Experience in defense acquisition position	A. 10 times or above(3 %) D. 2 times or less(66 %)	B. 6-9 times(3 %)	C. 3-5 times(28 %)
Q4. Experience in defense acquisition	A. 20 times or above(10 %) D. 5 times or less(66 %)	B. 11-19 times(5 %)	C. 6-10 times(19 %)
Q5. Familiarization with directive for defense power development operation	A. Expert(3 %) D. Beginner(50 %)	B. Skilled(12 %)	C. Intermediate(35 %)
Q6. Familiarization with instruction for cybersecurity risk management framework	A. Expert(1 %) D. Beginner(82 %)	B. Skilled(5 %)	C. Intermediate(12 %)
Q7. K-RMF training completion records	A. 5 times or above(2 %) D. None(68 %)	B. 3-4 times(4 %)	C. 1-2 times(26 %)
Q8. K-RMF training providers	A. MND/JCS(7 %) D. Army/Navy/AF/Marine Corps HQs.(14 %)	B. DAPA(3 %)	C. DCC(8 %)
Q9. Key elements required for K-RMF	A. Guideline refinement(10 %) B. Expanding educational opportunities(30 %) C. Additional pilot implementation(11 %) D. Distribution of explanatory materials(21 %) E. K-RMF management system(24 %)		
Q10. Key departments responsible for K-RMF	A. All department(41 %) C. Information planning and management(36 %)	B. Cyber Operation Center(23 %)	

가 아직 시행 초기이고, 국방부와 방첩사가 K-RMF에 대한 저변의 이해도 증진 및 인식확산보다는 K-RMF의 제도적 완성도와 K-RMF 시행력 구축에 우선하고 있는데 기인한 것으로 보인다.

또한 K-RMF에 대한 교육 이수 경험이 매우 저조(없음, 68 %)하므로, 기관별로 교육 주관부서를 지정하고 전문 강사를 확보하는 등 교육 기회 확대와 K-RMF 인식 제고, 관련 규정 숙지도 향상을 위한 노력이 필요하겠다.

K-RMF의 조기정착을 위해 필요한 것은 K-RMF에 대한 교육 기회 확대(30 %), K-RMF 관리시스템 구축(24 %), K-RMF에 대한 설명자료 배포(21 %), 신규 방위사업에 대한 추가적인 시범적용(11 %) 순으로 응답하였는데, 향후 K-RMF 관리시스템 구축 시 제반 교육자료 및 참고자료 등이 충분히 제공되어야 할 것으로 보인다.

각 군 본부의 K-RMF 주관부서 지정에 대해서는 소요제기를 담당하는 전 참모부라고 응답한 비율이 41 %인데 비해, 정보화기획참모부, 사이버작전센터 등으로 응답한 비율도 59 %나 되었다. K-RMF와 사이버보안은 방위사업업무를 수행하는 모든 인원이 수행해야 하는 것임에도 불구하고, K-RMF의 수행범위를 여전히 IT 전문분야로 생각하는 인원이 많은 것으로 판단된다. 각 군 본부의 모든 소요제기 부서에서 해당 사업을 추진하면서 K-RMF를 적용하여 추진해야 하나, K-RMF 조기정착을 위해서는 한시적으로 각 군에 K-RMF 전담부서를 두고, 교육 및 컨설팅 등 업무지원을 하는 것도 방법 중 하나가 될 것이다.

3. 한·미 RMF 및 K-RMF 시행여건 분석

3.1 미군의 RMF

미군의 RMF는 미 연방정보보호관리법(FISMA, Federal Information Security Management Act)에 따라 미국표준기술연구소(NIST)에서 개발하였으며, 적의 사이버공격에 대비하여 안전한 무기체계를 개발하기 위해 소요 기획 단계에서 설계, 구현, 시험평가, 운용 및 폐기에 이르기까지 시스템 전 수명주기 관점에서 무기체계의 사이버보안 관리 및 평가를 위한 제도이다. RMF는 정보시스템에 대한 위험이 임무수행에 미치는 영향의 정도에 초점을 맞추어 시스템이 정상적으로 임무를 수행할 수 있도록 위험을 제거하거나 완화하는 것을 목표로 한다[7].

RMF의 프로세스를 구현하기 위한 기준문서는 미 국방부와 NIST, 연방정보처리표준(FIPS, Federal Information Processing Standards) 및 국가안보시스템위원회(CNSS, Committee on Natinal Security System)에서 제공하며 주요 내용은 Table 2와 같다.

Table 2. Publications for RMF

Publisher	Title	Major instruction
DoD	DoDI 5000.02	Defense acquisition system guidelines
	DoDI 8500.01	Cybersecurity guidelines
	DoDI 8510.01	RMF guidelines
NIST	SP 800-18	Identification, security control implementation, and assessment methods
	SP 800-30	Guidelines for risk assessment and mitigation of identified system risks
	SP 800-37	Guidelines for applying the RMF to federal information systems
	SP 800-53	Guidelines for security control identification and selection
	SP 800-53A	Security control assessment guidelines
	SP 800-60	Security classification guidelines
	SP 800-137	Monitoring guidelines
FIPS	FIPS 199	Security classification standard
	FIPS 200	Minimum security requirements regulations
CNSS	CNSSI 1253	Guidelines for mapping types of information and information systems to security categories

NIST에서 정의하는 RMF 단계는 NIST SP 800-37에 의거하여 (0) 준비, (1) 시스템 보안분류, (2) 보안통제항목 선정, (3) 보안통제항목 구현, (4) 보안통제항목 평가, (5) 시스템 인가, (6) 모니터링의 7단계로 구성되며, 각 단계별 주요 내용은 아래와 같다[8].

(0) 준비 단계: 조직의 정보시스템 수준에서 보안 위험관리 우선순위를 설정하여 조직 및 시스템

수준 관점에서 RMF를 준비한다. 조직의 자산 및 임무를 식별하고, 위험평가를 통해 위험관리 전략을 수립하며, 보안요구사항을 정의한다.

(1) 시스템 보안분류 단계: 시스템에 대한 기밀성, 무결성, 가용성의 잠재적 손실영향분석을 기반으로 시스템을 분류한다. 시스템이 처리하는 정보를 포함하여 보안분류를 수행하며, 준비 단계에서 수립된 위험관리 전략을 반영한다.

(2) 보안통제항목 선정 단계: 시스템 위험평가를 기반으로 위험을 수용 가능한 수준으로 완화하기 위한 보안통제항목을 선정한다. 위험에 따른 시스템 보호에 필요한 통제 기준을 선정하고 이에 따른 기준선을 설정하며, 지속적인 모니터링 전략을 수립한다.

(3) 보안통제항목 구현 단계: 시스템 및 해당 운영환경 내에서 보안통제항목이 적용되도록 구현한다.

(4) 보안통제항목 평가 단계: 보안통제항목이 올바르게 구현되고, 의도된 대로 작동하며, 정보보호 및 개인정보보호에 대한 요구사항을 충족하는지 평가하고, 보안통제항목의 미비점을 보완한다.

(5) 시스템 인가 단계: 시스템이 사이버공간에서의 작전적 요구사항이 충족되는지 검토하여 시스템의 사용을 승인한다. 위험관리전략이 반영된 수용 가능한 위험 등을 결정하며, 결정된 위험에 대한 대응 방안을 준비한다.

(6) 모니터링 단계: 보안통제항목의 유효성, 시스템 및 운영환경 변경사항 등을 지속적으로 모니터링한다. 모니터링 결과에 따라 지속적인 승인 또는 인가를 변경하고, 시스템 폐기전략을 개발하여 구현한다.

3.2 한국군의 K-RMF

K-RMF의 성공적 시행을 위한 국방부 관련 법령의 핵심은 기존의 '국방전력발전업무훈령', '국방사이버안보훈령'과 2024년 4월 제정된 '국방 사이버보안 위험관리 지시'이다.

'국방전력발전업무훈령'은 무기체계와 전력지원체계의 소요·획득·운영유지를 포함하는 전력증강과 관련된 업무의 기본절차를 규정하고 지침을 제공[6]한다. '국방사이버안보훈령'은 안전하며 효과적인 국방 사이버공간을 창출·유지·보호하고, 적대세력에 비해 사이버공간의 우위를 확보하는 것을 목표로 하는 제반 업무에 대해 지침과 절차를 규정[5]하며, '국방 사이버보안 위험관리 지시'는 무기체계 및 전력지원체계의 사이버보안 위험을 수명주기 관점에서 관리하기 위해 국방 사이버보안 위험관리의 추진, 운영, 관리 등에 필요한 사항을 규정[4]한다.

'국방 사이버보안 위험관리 지시'에 명시된 K-RMF 단계는 (1) 시스템 보안분류, (2) 보안통제항목 선정, (3) 보안통제항목 구현, (4) 보안평가, (5) 시스템 인가, (6) 보안통제항목 모니터링의 총 여섯 가지 절차로 운영되며, 각 단계별 주요 내용은 아래와 같다.

(1) 시스템 보안분류 단계: 시스템 및 해당 시스템이 생산, 유통하는 정보 유형에 따라 대상체계를 기밀성, 무결성, 가용성 수준 또는 기타 유형으로 분류한다.

(2) 보안통제항목 선정 단계: 시스템 보안분류 결과를 토대로 보안계획서 작성을 통해 대상체계에 구현해야 하는 보안통제항목을 선정하고, 구현계획을 수립 및 구체화한다.

(3) 보안통제항목 구현 단계: 작성한 보안계획서에 따라 선정된 보안통제항목에 대해 소프트웨어 개발, 장비구매, 운영절차 및 운용환경 마련 등의 방법으로 해당 대상체계에 대한 보안요구사항을 구현한다.

(4) 보안평가 단계: 보안통제항목이 보안계획서에 따라 구현되었는지를 평가한다.

(5) 시스템 인가 단계: 보안평가를 통해 도출한 결과에 따라 해당 대상 체계의 위험수준을 결정하고, 운용 가능 여부를 결정한다.

(6) 보안통제항목 모니터링 단계: 운용인가서, 보안계획서, 후속조치계획서 등에 따라 대상 체계의 폐기 전까지 위험을 지속 관리한다.

3.3 한·미 RMF 보안통제항목 패밀리 비교

미군의 RMF 보안통제항목은 SP 800-53에 보안통제강화항목을 포함한 모든 내용이 공개되어 있으나, K-RMF의 보안통제항목은 통제항목 수를 제외

하고 비공개되어 있어 미 RMF 보안통제항목과의 세부적인 비교는 제한된다. 다만, RMF 패밀리 구성을 통해 보안통제항목을 어떻게 구분하고 있는지 살펴볼 수 있는데 한·미 RMF 보안통제항목 패밀리를 비교한 결과[9,10]는 Table 3와 같다.

Table 3. Comparison of ROK and US RMF family

Family	US	ROK
AC	Access control	Same as US
AT	Awareness and training	
AU	Audit and accountability	
CA	Assessment, authorization, and monitoring	
CM	Configuration management	
CP	Contingency planning	
CR	–	Crypto management
IA	Identification and authentication	Same as US
IR	Incident response	
MA	Maintenance	
MP	Media protection	
PA	–	Planning and assessment
PE	Physical and environmental protection	Same as US
PL	Planning	–
PM	Program management	–
PS	Personnel security	Same as US
PT	PII processing and transparency	–
RA	Risk assessment	–
SA	System and services acquisition	Same as US
SC	System and communications protection	
SI	System and information integrity	
SR (SM)	Supply chain risk management	

한·미 RMF 보안통제항목 패밀리는 대부분 유사하나, 일부 패밀리의 구분이 상이함을 알 수 있다. 미군에는 없는 한국군의 PA(보안계획/평가)는 한국군에는 패밀리로 구분되지 않은 미군의 PL(계획수립), RA(위험평가)를 통합한 것과 유사한 내용이며, 한국군의 CR(암호관리)의 경우 미군은 별도 패밀리로 구성하고 있지는 않지만 CM(형상관리), SC(시스템/통신보호) 패밀리에 암호관리, 암호보호, 암호키 생성 및 관리 등의 보안통제항목으로 포함되어 있다. 반면 미군의 PT(개인정보처리/투명성)는 한국군의 MP(매체보호)와 AC(접근통제)에 일부 보안통제항목이 포함되어 있다는 것을 확인할 수 있었다. 미군의 PM(사업관리)에는 관련 연방법, 행정명령, 지침, 정책, 규정 등을 용이하게 준수하도록 하는 보안통제항목이 수록되어 있으나, 한국군 RMF에는 관련 항목이 반영되어 있지 않다.

한·미 RMF 보안통제항목 간의 차이는 한국과 미국의 사이버보안 및 RMF와 관련된 법령, 정책, 지침 등이 상이한 것에서 기인한다고 할 수 있다. 사이버 위협이 고도화되고, 이에 따른 대응 기술, 정책의 발전에 따라 보안통제항목도 진화적으로 발전해야 한다. 따라서 RMF 보안통제항목은 각국의 RMF 시행 여건을 고려하여 자체적으로 개발·발전시켜 나가야 하므로 이 점에서 양국의 보안통제항목 간 차이가 발생하는 것으로 판단된다.

3.4 K-RMF 시범적용 분석

2021년부터 2023년까지 국방부는 K-RMF의 연착륙을 위하여 연합체계 및 각 군의 전장관리정보체계에 시범적용과 정식적용의 단계적 적용을 시행하였다. 기존 운용 중인 전장관리정보체계에 K-RMF 절차를 적용하려다 보니 K-RMF의 모든 단계를 적용하지 못하는 태생적 한계가 존재하는 제약사항은 있지만, 국방부는 적지 않은 성과를 거둘 수 있었으리라 평가된다.

방첩사와 각 군 본부는 우선 1단계(시스템보안 분류)부터 5단계(시스템 인가)까지 K-RMF 절차를 실제로 경험해 봄으로써 K-RMF에 대한 보다 나은 수준의 이해를 가지게 되었으며, 이후 6단계(보안통제항목 모니터링) 절차를 계속 수행하면서 부분 구현된 보안통제항목에 대한 위험완화 조치를 수행하고, 재

평가를 실시하는 등 전장관리정보체계에 대한 실질적인 보안수준을 강화할 수 있었다.

하지만 K-RMF 시범적용 기관에 방위사업청이 포함되지 않음으로써 K-RMF에 대한 방위사업청의 역할을 검증하고, 이해 수준을 높일 수 있는 기회를 가지지 못했다는 것은 아쉬움으로 남는다. '국방 사이버보안 위험관리 지시'에 따라 방위사업청은 사업관리기관으로서 사업관리 기간 동안의 위험관리 업무를 수행하고, 보안평가 결과에 따른 후속조치 방안을 조정해야 하며, 무기체계 탐색개발 시 보안통제항목을 선정하고, 체계개발 단계에서 보안계획서 작성을 총괄해야 한다. 또한, 무기체계 보안평가 기간 중 보안평가계획서를 작성하는 등 K-RMF 2단계(보안통제항목 선정)부터 4단계(보안통제항목 평가)까지 핵심역할을 수행해야 한다. 따라서, 시범적용 대상 체계가 기(旣) 운용 중인 체계라 할지라도 각 단계별 소관업무에 대해 각 군 및 방첩사와의 절차연습 등 방위사업청의 참여가 필요하였다.

또한, K-RMF가 모든 무기체계와 전력지원체계를 대상으로 하는 사이버보안 제도라는 점에서 전력지원체계에 대한 시범적용 절차 없이 2026년 이후 단계적으로 적용하는 것도 현 추진계획의 보완이 필요해 보인다. 전력지원체계의 경우 전반적으로 사업관리기관에서 대부분의 K-RMF 절차를 직접 수행해야 하는데 전력지원체계의 많은 사업관리기관은 앞서 설문결과에서 알 수 있듯이 K-RMF에 대한 이해가 상대적으로 부족하다. 따라서 정보화사업으로 획득되지 않는 다른 전력지원체계에 대해서도 시범적용 및 절차 숙달이 필요하다.

3.5 국방상호운용성 시험평가(사이버보안)와 K-RMF 보안평가 통합가능성 검증

K-RMF 제도의 도입 이전에도 한국군이 방위사업에 대해 사이버보안을 적용하지 않은 것은 아니다. '국방상호운용성 관리지시'는 '국방정보화업무훈령'에서 위임한 국방정보화 표준, 연동업무 관리 및 국방상호운용성 평가에 관련된 업무의 기본절차를 규정하고 지침을 제공한다[11]. 국방부는 무기체계와 전력지원체계의 소요 기획 및 획득, 운영유지 단계에 각각 사이버보안 요소를 적용하도록 하고, 국군지휘통신사령부 예하의 합동상호운용성기술센터 주관으로 시험평가를 통해 상호운용성을 갖추고 있는지를 확인하여 기준의 충족 여부를 평가한다.

소요 기획 단계에서 설계, 구현, 시험평가, 운용 및 폐기에 이르기까지 시스템 전 수명주기 동안에 무기체계의 사이버보안 관리 및 평가를 위한 제도라는 점에서 K-RMF는 국방상호운용성 평가와 유사성을 가지고 있으며, 방위사업 각 단계별 국방상호운용성 평가와 K-RMF를 비교[4,11]하면 Table 4와 같다.

Table 4. Comparison of interoperability assessment and RMF in the stages of defense acquisition

Stage	Interoperability assessment	RMF
Planning	Requirement assessment/ Select	Categorize/ Select
Exploratory development	Develop an implementation plan	Develop an implementation plan
System development	Implement	Implement
T&E	Assess/ Authorize	Assess/ Authorize
Operation & maintenance	O&M evaluation	Monitor/ Reevaluation

그러나, 국방상호운용성 평가와 K-RMF는 제도 도입의 취지를 볼 때 분명한 차이가 있다. 국방상호운용성 평가는 무기체계 획득에 방점을 두고 상호운용성 평가항목 선정 및 pass/fail 평가를 수행하는 반면, K-RMF는 전 수명주기 동안 무기체계의 사이버보안 관리 및 평가, 모니터링을 수행하기 위한 제도이므로 두 제도가 병립하더라도 서로 의미가 있다고 할 수 있다.

다만, 소요제기 기관과 사업관리 기관은 방위사업의 운용시험 단계에서 사이버보안이라는 평가항목에 대해 '국방상호운용성 관리지시'에 따른 상호운용성 시험평가(사이버보안)와 '국방 사이버보안 위험관리 지시'에 따른 K-RMF 보안평가라는 두 가지 평가 절차를 수행해야만 하는 절차의 중복성을 갖는다. 절차의 중복성을 제거하기 위하여 사이버운용성 시험평가(사이버보안)와 K-RMF 보안평가를 통합하여 수행하되, 사이버보안평가를 수행하는 국군지휘통신사령부(합동상호운용성기술센터)와 방첩사령부

두 기관이 만족할 만한 산출물을 획득할 수 있다면 효율적인 사업관리는 물론 인력이나 불필요한 국방예산 사용을 절감하는 데에도 기여할 것이다.

평가 주체가 상이한 상호운용성 시험평가(사이버보안)와 K-RMF 보안평가를 통합하기 위한 조건들을 상정하고, 이 조건들의 충족 여부에 대해 검증이 가능하다면, 제도의 일부 보완을 통해 두 평가를 통합할 수 있을 것이다.

두 가지 보안평가를 통합하기 위해서는 두 평가의 평가범위와 세부평가항목에 대한 비교가 요구되며, 통합가능성을 검증하기 위한 조건을 아래와 같이 상정하였다.

(1) 범위: 두 평가에서 요구하는 사이버보안 평가범위가 서로 일치하거나, 하나의 평가가 다른 하나의 평가범위를 모두 만족

(2) 세부평가항목 : (1)항이 충족한다면, 두 평가에서 구현하고자 하는 세부평가항목이 서로 일치하거나, (1)항의 평가에서 다른 하나의 평가범위를 만족했던 평가의 세부평가항목이 다른 평가의 세부평가항목을 모두 만족

통합가능성 검증조건 (1)항(평가범위)의 만족 여부를 확인하기 위해서는 우선 두 평가에서 요구하는 사이버보안 평가범위에 대한 확인이 필요하다.

'국방상호운용성 관리지시'에 명시된 상호운용성 시험평가(사이버보안)의 평가범위는 네트워크 정보보호, 관제체계 구축, 키 관리체계 구축, 응용체계 정보보호, 서버 정보보호, 단말기 정보보호, 암호장비 적용, 신분위장 위협 대응능력, 데이터 변조 위협 대응능력, 공격행위부인 위협 대응능력, 정보유출 위협 대응능력, 서비스 거부(DoS) 위협 대응능력, 권한 상승 위협 대응능력, 시큐어 코딩 규칙 적용 적절성, 오픈소스 취약점 제거 적절성 등 총 15개 분야[11]이다.

K-RMF 보안평가의 통제항목은 AC(접근통제) 등 17개 항목과 모의침투항목인 모의침투, 취약점 제거 등 총 19개 분야이다[10].

두 평가의 평가범위 간 상관관계를 도식화한 결과는 Fig. 1과 같다. 상호운용성 시험평가(사이버보안)는 AT(보안인식 교육·훈련), MA(유지보수), SM(공급망 관리) 등 K-RMF 보안평가의 평가범위를 모두 충족하지 못하지만, K-RMF 보안 평가는 상호운용성 시험평가(사이버보안)의 평가범위를 모두 충족함을 알 수 있다.

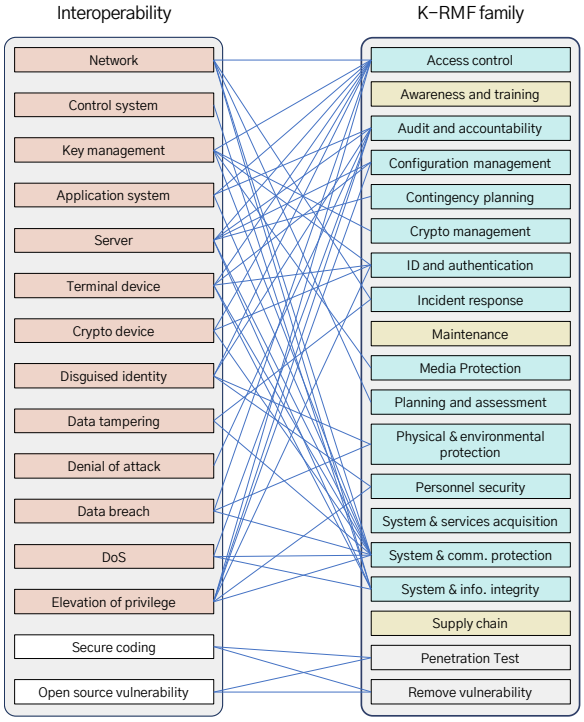

Fig. 1. Assess areas of interoperability T&E and K-RMF

통합가능성 검증조건 (2)항(세부평가항목)의 충족 여부를 확인하기 위해서는 소요 기획 단계에서부터 상호운용성 평가와 K-RMF 절차를 모두 수행한 무기체계나 전력지원체계가 필요하나, 불행히 한국군에 (2)항을 온전히 검증하기 위한 무기체계나 전력지원체계는 존재하지 않는다. 따라서 제한적이지만 해군전술 C4I 체계인 KNCCS에 대해 2019년 실시한 상호운용성 시험평가(사이버보안) 결과와 2023년 K-RMF 시범적용 시 적용했던 보안평가 사례를 바탕으로 두 평가 간 세부평가항목의 충족 여부를 확인하였다.

2019년 실시한 KNCCS 성능개량사업에 대한 상호운용성 시험평가(사이버보안) 항목은 네트워크 정보보호 등 총 8개 분야 20여 개 항목이었으나, 본 연구에서는 연구목적 상 평가를 미실시한 7개 항목을 포함하여 총 13개 분야 30여 개 항목을 진행하였다.

KNCCS 성능개량사업에 대해 K-RMF 시범적용 간 보안평가 시 적용했던 보안통제항목은 AC(접근통제) 등 19개 분야 460여 개 항목을 적용하였다.

두 평가의 평가범위 간 상관관계를 도식화한 결과는 Table 5와 같으며, K-RMF 보안평가의 보안통제 항목은 상호운용성 시험평가(사이버보안)의 세부평가항목을 모두 충족하였다.

Table 5. Comparison of interoperability assessment and RMF in the stages of defense acquisition

Category	Evaluation criteria in interoperability T&E	K-RMF Family (Number of Controls)
Network	Firewall, IPS, NAC, UTM, etc.	SC(17), SI(7), AC(5), AU(5), CM(2), IA(1)
Control system	EMS, ESM, etc.	SI(4), AU(3), SC(2)
Key management	User authentication, etc.	SC(5), IA(5), AC(3), CR(1), AU(1)
Application system	PW management, etc.	AC(12), AU(11), IA(4), CM(1)
Server	Server security, etc.	AU(7), SC(5), SI(4), AC(1), CM(1)
Terminal device	Access control, etc.	SI(5), SC(4), IA(3), AC(2), CM(2)
Cryptographic device	Data confidentiality, etc.	SC(4), AC(1), CR(1)
Cyberwarfare	Disguised identity	AC(9), IA(3)
	Date tempering	SC(6), SI(1)
	Denial of attack	AU(11)
	Data breach	SC(3), SI(3), AC(2)
	DoS	SC(3)

상호운용성 시험평가(사이버보안)와 K-RMF 보안평가의 통합가능성을 검증하기 위해 상정하였던 두 가지 조건을 검증한 결과 K-RMF 보안평가는 (1) 평가범위와 (2) 세부평가항목에 있어서 상호운용성 시험평가(사이버보안)의 평가범위와 세부평가항목을 모두 충족하는 것을 확인하였다. 즉, 소요제기기관과 사업관리기관은 운용시험 단계에서 사이버보안 평가 시 상호운용성 시험평가(사이버보안)와 K-RMF 보안평가를 모두 수행하지 않고, K-RMF 보안평가만 수행하여도 사이버보안 평가를 수행하는 국군지휘통신사령부(합동상호운용성기술센터)와 K-RMF 보안평가를 수행하는 방첩사령부 두 기관이 만족할 만한 산출물을 획득할 수 있다.

4. K-RMF 조기정착을 위한 방위사업제도 발전방향

4.1 국내 K-RMF 관련 법령 보완

K-RMF는 사이버업무에 종사하는 특정 집단의 업무가 아니며, 방위사업에 종사하는 모든 인원이 정확히 관련 내용을 숙지하고 수행해야 하는 업무임을 명확히 하여야 한다.

따라서 K-RMF가 조기에 한국군에 정착되기 위해서는 방위사업과 관련된 한국군의 최상위 훈령인 '국방전력발전업무훈령'에 K-RMF 개념을 반영해야 한다. 이를 위한 방안으로 현재 훈령의 제1장 총칙 제4조에 총수명주기관리 업무가 포함[5]되어 있는 것처럼 '사이버보안 프레임워크' 업무를 별도의 조항으로 추가함으로써 무기체계와 전력지원체계 획득 업무를 수행하는 관계자들이 방위사업에서 K-RMF가 가장 기본바탕이 되어야 한다는 인식을 가지도록 해야 할 것이다.

또한, '국방전력발전업무훈령'을 지원하는 '국방정보화업무훈령', '국방사이버안보훈령'에도 RMF 개념이 상세하게 반영되도록 보완함으로써 이들 3개의 훈령이 유기적으로 연결되고, 상호 지원할 수 있어야 한다.

4.2 방위사업 간 사이버보안 평가의 통합 시행

K-RMF 보안평가는 평가범위와 세부평가항목에 있어서 상호운용성 시험평가(사이버보안)의 평가범위와 세부평가항목을 모두 충족한다는 것이 검증되었다. 이는 이들 두 가지 평가를 통합하여 시행할 수 있음을 의미한다.

그러나 두 가지 평가를 그대로 통합하여 시행할 수 있는 것은 아니다. 상호운용성 시험평가(사이버보안)와 K-RMF 보안평가의 평가항목들은 방위사업의 절차에 따라 소요 기획 단계, 탐색 및 체계 개발 단계를 진행하면서 구체화되는 산출물이므로, 두 평가를 통합하기 위해서는 방위사업의 소요 기획 단계에서부터 상호운용성 시험평가(사이버보안)의 평가항목들이 K-RMF 보안평가 통제항목에 반영될 수 있도록 해야 한다.

K-RMF 보안평가 결과는 우선 국군지휘통신사령

부(합동상호운용성기술센터)에서 상호운용성 기준의 충족 및 미달 여부를 우선 평가하고, 소요군(소요제기기관)은 상호운용성 기준을 충족한 무기체계와 전력지원체계에 한해 K-RMF 시스템 인가 절차를 진행한다면 방위사업에 대해 한 번의 사이버보안 평가 절차를 통해서도 두 가지 평가 목표를 모두 달성할 수 있을 것이다. 이는 방위사업의 운용시험 단계에서 사이버보안이라는 평가항목에 대해 두 가지 평가 절차를 수행해야만 했던 소요제기기관과 사업관리기관의 부담을 최소화하면서도 사업관리의 효율성을 증대시켜 인력 및 국방예산의 절감도 기대할 수 있을 것이다.

4.3 추가적인 K-RMF 시범적용 기회 마련

K-RMF가 한국군 무기체계 및 전력지원체계 획득에 조기에 정착하기 위해서는 국방부와 합참, 방첩사 및 각 군의 역할을 제대로 수행하는 것이 매우 중요하다. 특히, 방위사업청은 무기체계 사업관리기관으로서 사이버보안 위험관리 업무 전반에 대한 임무를 수행해야 하므로 신규 획득되는 무기체계 중 K-RMF를 적용하는 체계가 선정되기 이전에 자체 역량을 구비해야 한다. 이를 위해서는 현재 진행되고 있는 무기체계 도입사업 중 K-RMF를 적용할 수 있는 사업을 선정하고 방첩사, 각 군과 협업하여 K-RMF 각 단계별 방사청의 임무와 역할에 대해 숙달할 수 있는 시범적용 기회를 마련해야 한다.

또한 K-RMF의 효과적인 적용을 위해 방사청 외에도 '국방 사이버보안 위험관리 지시' 제12조(공통임무)에 명시된 K-RMF 업무를 수행해야 하는 국방부 예하 기관 중 K-RMF 시범적용 기간에 참여하지 않았던 국군지휘통신사령부, 국방전산정보원, 국방과학연구소, 국방기술품질원 등도 해당 기관의 임무와 역할에 대해 숙달할 수 있는 기회를 가져야 한다.

4.4 K-RMF 전문성 교육 강화

K-RMF가 제대로 시행되기 위해서는 소요제기기관 및 소요결정기관, 이를 지원하는 국방부 직할부대에 이르기까지 국방획득 전 과정에서 K-RMF가 어떻게 적용되는지 명확히 이해하고 있어야 한다. 하지만 K-RMF 인식 관련 설문조사 결과에서 알 수 있듯이 현재 한국군의 K-RMF에 대한 이해도는 매우 낮은 상황이다.

따라서 방첩사는 물론, 합동참모본부, 각 군 본부, 방사청 등 각 기관별 책임하에 주기적으로 K-RMF 교육을 시행해야 하며, 국방대학교 직무연수부에서 시행하는 직무전문교육의 일환으로 K-RMF 과정을 신설하고, 방사청 방위사업교육원에서 시행 중인 사업관리 기본과정을 보완하거나 전력지원체계 사업관리과정 같은 별도의 전문과정을 신설하여 운영하는 것도 필요하다.

또한, K-RMF에 대한 접근성을 보장할 수 있도록 국방부 또는 방첩사가 주관하여 K-RMF 홈페이지를 개설하고, 관련 훈령과 규정, 교육 동영상 등을 누구나 쉽게 접할 수 있도록 시스템도 구축해야 한다.

5. 결론

K-RMF가 이미 시행되었음에도 불구하고, 한국군의 K-RMF에 대한 이해는 여전히 저조한 실정이다. K-RMF가 조기에 한국군에 정착되기 위해서는 방위사업업무에 종사하는 모든 인원이 무기체계와 전력지원체계의 소요부터 폐기까지 전 생애주기에 걸쳐 K-RMF가 적용되어야 한다는 것을 인식하고, 관련업무 수행 시 K-RMF 절차들이 적용되어야 한다. 따라서, 본 논문에서는 K-RMF의 조기정착을 위해 선결되어야 하는 다음 몇 가지 사항들을 제안하였다.

첫째, K-RMF 관련 법령의 보완이 필요하다. 국방부는 2024년 K-RMF의 시행근거로 '국방 사이버보안 위험관리 지시'를 마련하였으나, '국방전력발전업무훈령'과의 연계성은 아직 미흡하다. '국방전력발전업무훈령'의 총칙에 사이버보안 프레임워크 개념을 별도 조항으로 추가함으로써 방위사업 종사자들이 K-RMF를 반드시 염두에 두고 업무를 수행해야 한다는 인식을 가지도록 해야 하며, '국방전력발전업무훈령'을 지원하는 '국방정보화업무훈령', '국방사이버안보훈령'과의 유기적 연결성도 증대시켜야 한다.

둘째, 방위사업에 있어서 사이버보안 평가의 통합시행이 요구된다. 소요 기획 단계에서부터 각 방위사업 단계별로 상호운용성 시험평가(사이버보안)에서 요구되는 평가항목들이 K-RMF 보안평가 통제항목에 반영될 수 있도록 관련 법령과 지침의 보완이 필요하다. 또한, 운용시험 단계에서 사이버보안 평가를

K-RMF 보안평가에 통합하여 시행함으로써 사업관리의 효율성을 증대시켜 인력의 중복투입을 방지하고 사업기간 단축을 통해 국방예산을 절감할 수 있을 것이다.

셋째, 방위사업청과 국방부 예하 기관들의 K-RMF 역량 강화가 필요하다. 시범적용에 포함되지 않았던 방위사업청과 국군지휘통신사령부, 국방전산정보원, 국방과학연구소, 국방기술품질원 역시 K-RMF 단계별 역할을 숙달해야 한다.

넷째, K-RMF 이해도 증진을 위한 교육이 강화되어야 한다. 현 시점에서 방첩사 및 각 군의 일부 부서에서만 K-RMF 제도의 필요성과 업무절차에 대해 정확히 이해하고 있으며, 방위사업업무에 종사하는 다수의 인원들에게는 여전히 생소한 분야이다. K-RMF 수행 절차에 대한 기관별 특성에 맞는 전문교육프로그램을 마련하고, K-RMF 홈페이지 등을 통해 누구나 쉽게 접할 수 있도록 시스템 구축이 필요하다.

참고문헌

[1] Jung-keun Ahn, Kwang-soo Cho, Han-jin Jeong, Ji-hun Jeong, Seung-joo Kim, "A Study on Constructing a RMF Optimized for Korean National Defense for Weapon System Development," Journal of The Korea Institute of Information Security & Cryptology, Vol. 33, No. 5, pp. 827-846, Oct 2023, DOI: 10.13089/JKIISC. 2023.33.5.827
[2] Yong-seok Lee, Jeong-min Choi, "Research for Application the RMF to the Korean Military," The Journal of Korean Institute of Communications and Information Sciences, Vol. 45, No. 12, pp. 2132-2139, Oct 2020, DOI: 10.7840/Kics.2020.45.12.2132
[3] Hyuk-jin Kwon, Sung-tae Kim, Ye-na Joo, "The Direction of Application of the RMF-based Risk Management System Considering interoperability," Journal of Internet Computing and Services, Vol. 22, No. 6, pp. 83-89, Dec 2021. DOI: 10.7472/jksii.2021.22.6.83
[4] "National Defense Instruction for Cybersecurity Risk Management Framework," Ministry of National Defense, Apr 2024.
[5] "National Defense Directive for Cybersecurity," Ministry of National Defense, Dec 2023.
[6] "National Defense Directive for Defense Power Development Operation," Ministry of National Defense, May 2024.
[7] "DOD Instruction 8510.01: Risk Management Framework for DoD Systems," Office of the Department of Defense, Jul 2022.
[8] "NIST Special Publication 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations," National Institution of Standards and Technology, Dec 2018.
[9] "NIST Special Publication 800-53 Revision 5: Security and Privacy controls for Information Systems and Organizations," National Institution of Standards and Technology, Sep 2020.
[10] Sang-kwon Kim, "The Current State and Future Path of K-RMF," The 19th Defense Security Conference, Seoul, pp. 215-239, 2023.
[11] "National Defense Instruction for Interoperability Management," Ministry of National Defense, Jan 2023.