Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 10 pp. 268-274, 2023

https://doi.org/10.5762/KAIS.2023.24.10.268
ISSN 1975-4701 / eISSN 2288-4688

국내 무기체계 소프트웨어 산출물의 RMF 적용 방안 연구

최은진
국방기술품질원

A Study on the Application of RMF to Domestic Weapon System Software Products

Eun-Jin Choi
Defense Agency for Technology and Quality

요 약 최근 사이버 위협이 고도화되면서 국방 무기체계에 보안을 강화할 수 있는 정책 및 제도에 관한 연구가 중요해지고 있다. 이에 따라, 현재 美 RMF(Risk Management Framework) 제도에 한국군 환경을 고려한 한국형 보안위험관리 프레임워크(K-RMF) 제도가 개발되고 있다. K-RMF는 국방 무기체계 시스템 수명주기에 보안을 내재화할 수 있는 한국형 위험관리 제도로, 위험관리 개념을 적용하여 미구현된 보안통제항목의 보안 요구사항에 대한 위협 완화 방안을 마련할 수 있다. 시스템 수명주기 동안 보안위험을 관리할 수 있다는 장점이 있지만, 현 무기체계 개발단계에 K-RMF를 적용하기 위해서는 한국군 환경에 최적화되어있는 기존 문서를 최대한 활용할 수 있어야 한다. 본 논문에서는 개발 초기 단계에서 발생하는 현행 소프트웨어 산출물을 K-RMF 보안 평가 시 첨부 자료로 활용하는 방안을 제안하였다. 제안한 방법은 시스템 통신 관련 보안통제항목을 산출물 내 명시하는 방안이며, 향후 제안 방법을 활용하여 보안통제항목 평가 절차를 간소화시킬 수 있다.

Abstract Research on strengthening security in the defense weapon system is becoming increasingly important as cyber threats have increased. As a result, a K-RMF has emerged that considers the Korean military in the U.S. RMF. K-RMF is a Korean-style Risk Management Framework that can internalize security in the SDLC (System Development Life Cycle) of the defense weapon system and can be applied to mitigate the threat to the security requirements of not-satisfied security controls. Although it can manage cyber threats through SDLC, it is necessary to make the most of software documents optimized for the current Korean military to apply K-RMF to weapon systems. This paper proposes a method to perform K-RMF Assessments using current software documents occurring early in the SDLC. The proposed method aims to specify security controls related to system communication in software documents. In the future, the proposed method can be used to simplify the assessment process in the K-RMF procedure.

Keywords : Risk Management Framework, System Development Life Cycle, Security Controls, Cyber Security, K-RMF, Risk Assessment

1. 서론

최근 4차 산업혁명 기술의 발달에 따라 정보기술(IT)을 활용하는 각종 산업 분야에서 제공하는 서비스에도 변화가 생기고 있다. 4차 산업혁명 핵심 기술인 사물 인터넷(IoT) 기술을 활용하여 자료수집 및 분석이 쉬워졌

*Corresponding Author : Eun-Jin Choi(Defense Agency for Technology and Quality)
email: ejchoi@dtaq.re.kr
Received August 2, 2023 Revised September 1, 2023
Accepted October 6, 2023 Published October 31, 2023

으며, 네트워크망의 확장으로 연동 시스템 간 데이터를 주고받을 수 있게 되었다[1]. 하지만 정보기술의 의존도가 높은 산업 분야를 대상으로 잇따른 데이터 노출 사고가 발생하게 됨에 따라 사이버 위협으로부터 데이터를 보호하기 위한 대책을 개발하는 일이 중요해지고 있다[2,3].

사이버 위협을 실시간으로 식별하고 대응하기 어려운 이유는 다음과 같다. 첫째로, 보안 특성상 공격자를 추정하기 어렵기 때문이다. 최근 사이버 위협은 해킹 지식이 없어도 공격할 수 있으며, 공격 직후 원인을 특정하기까지 오랜 시간이 소요되기 때문에 악의를 가진 사람이라면 누구나 공격자가 될 수 있다. 둘째로, 취약점을 완벽하게 탐지하기 어렵기 때문이다. 과거에 파급력이 낮았던 취약점도 재발견되었을 때는 영향력이 급증하였으며, 과거에 파급력이 높았던 취약점 또한 현재까지도 높은 영향력을 보유하고 있다.

이러한 이유로 최근 사이버 위협의 대응책으로는 취약점을 완벽하게 탐지하고 대응하기보다 침해 영향을 최소화하고 원인을 분석하여 빠르게 회복하는 데 중점을 두고 있다. 특히 국방 분야에서는 사이버 위협으로부터 신속하게 대응할 수 있도록 지속해서 위험을 관리할 수 있는 제도를 개발하고 있다.

현재 美 국방부(Department of Defense, 이하 DoD)는 2014년부터 정보기술을 수반하는 모든 국방 무기체계를 대상으로 시스템 수명주기(Life Cycle) 동안 보안위험을 관리하는 위험관리 프레임워크(Risk Management Framework, 이하 RMF) 제도를 의무적으로 적용하고 있다. 한국 군에서도 2019년 4월부터 韓-美 연동체계를 대상으로 RMF를 적용하기 위하여 한국형 보안위험관리 프레임워크(K-RMF) 제도를 개발하고, 관련 연구를 진행하고 있다[4]. 다만 美 RMF를 제도를 한국에 도입하기 위해서는 기존 보안 정책과의 연계성을 우선하여 한국군 환경에 최적화된 K-RMF 제도를 개발할 수 있어야 한다.

본 논문은 기존 보안제도 산출물을 활용하여 K-RMF 보안 평가를 수행하는 방안을 제안하였다. 제안하는 보안 평가 방안은 기존 무기체계 소프트웨어 산출물에 보안 요구사항을 명시하는 평가 방안이며, 작성 사례로 美 RMF SC(System and Communication Protection) 패밀리 보안 요구사항을 참고하였다. 보안 요구사항이 명시된 문서는 평가 단계에서 보안 요구사항의 구현 여부를 판단하는 데 활용할 수 있으며, 추후 K-RMF 평가 절차를 단축하는 방안으로도 활용될 수 있다.

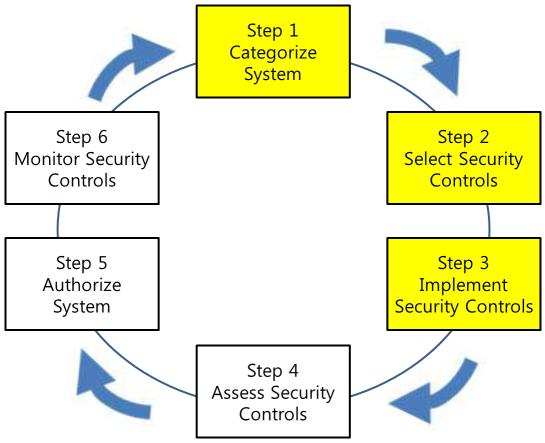

Fig. 1. RMF Process[5]

2. 관련 연구

2.1 美 RMF

2.1.1 도입 배경

미국은 1997년 도입한 DITSCAP(DoD Information Technology Security Certification and Accreditation Process) 제도에서 무기체계 시스템 수명주기 단계 내 인증 및 인가 단계를 포함시켰다[6]. 이후 2007년 도입한 DIACAP(DoD Information Assurance Certification and Accreditation Process) 제도에서 연방정보보호관리법(Federal Information Security Management Act. 이하 FISMA)을 충족할 수 있는 제도로 발전하였다[7].

RMF는 미국 표준기술연구소(National Institute of Standard and Technology, 이하 NIST)에서 개발한 시스템 수명주기 기반의 위험관리 프레임워크로, 기존 DIACAP에서 위험관리 및 모니터링 업무가 강화된 형태이다. RMF는 소프트웨어를 내장한 모든 국방체계를 대상으로 수행되며, 단계별 절차는 NIST SP 800-37 문서에서 확인할 수 있다.

2.1.2 진행 절차

RMF는 총 6단계로 구성되어 있으며, 진행 순서는 Fig. 1과 같다. 단계별 작성되는 산출물은 매 단계 종료 시점에서 확인 가능하며, 주기적으로 보완해야 한다.

(1) 분류(Categorize)

분류 단계에서는 보호 대상 시스템별 임무 특성을 기

반으로 정보 유형을 분류하고, 요구되는 보안목표 및 수준을 결정한다. 보안 등급은 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)의 손상 정도(Low, Moderate, High)로 표기되며, 정보 유형별 보안 등급 매핑 가이드에 해당하는 NIST SP 800-60 Appendix C, D에서 확인할 수 있다. 최종 결정된 보안 등급은 보안계획서(System Security Plan) 내 작성한다.

(2) 선정 (Select)

선정 단계에서는 요구되는 보안목표 및 수준을 달성하기 위한 보안통제항목을 선정한다. 시스템 보안 등급에 부합하는 보안통제항목을 식별 후, 시스템 특성 및 운용 환경 등을 고려하여 보안통제항목 기준선을 조정한다. 보안통제항목 선정 시에는 NIST SP 800-53 문서 내에 정의된 기준선과 CNSSI 1253 문서 내 [국가보안시스템(National Security Systems, 이하 NSS)을 위한 보안 분류 가이드]를 참고하며, 최종 선정된 보안통제항목 목록을 보안계획서에 명시한다.

(3) 구현 (Implement)

구현 단계에서는 최종 선정된 보안통제항목의 요구사항을 충족할 수 있는 구현 계획을 세워 이를 개발하는 과정이다. 구현 계획은 DoD 및 연방정부 정책에 기반하며, 사전에 실무자 간 회의 및 예상되는 위협 분석을 토대로 개발되어야 한다.

(4) 평가 (Assess)

평가 단계에서는 보안통제항목이 정보 및 정보시스템의 보안 요구사항에 맞게 구현되었는지를 평가한다. 보안 요구사항을 토대로 보안 평가계획서(Security Assessment Plan)를 작성하면 평가 절차에 따라 보안통제항목의 구현 여부를 평가하게 된다. 평가 방법에는 관련 문서 검토, 담당자와의 인터뷰, 평가 도구(Tool) 활용 등이 해당되고 평가 종료 후 보안평가 결과서(Security Assessment Result)를 제출하게 된다. 평가 결과 구현되지 않은 보안통제항목은 개발을 통해 보완하거나 운용 단계에서 후속조치 계획(Plan of Action and Milestones, POA&M)을 참고하여 보완할 수 있다.

(5) 인가 (Authorize)

인증 단계에서는 미구현 보안통제항목을 대상으로 보완 사항을 확인하여 위험평가를 진행한다. 인가 책임자(AO, Authorizing Official)는 이전 단계까지 작성된 산출물을 검토하여 미구현된 보안통제항목에 대한 위험평가를 실시하며, 보안통제항목 위험 수준에 따라 인가 여부가 결정된다.

(6) 모니터링 (Monitor)

모니터링 단계에서는 시스템이 일정 수준의 보안수준을 유지할 수 있도록 보안 위험관리 활동을 지속한다. 시스템은 모니터링 단계를 통해 보안 위협을 빠르게 식별해내고 대응할 수 있으며, 이 단계는 시스템 폐기까지 진행된다.

2.1.3 보안통제항목 (Security Controls)

美 RMF에서 활용되는 보안통제항목은 NIST SP 800-53 revision 4 기준으로, Table 1과 같이 총 18개 패밀리 826개 항목으로 구성되어 있다. 보안통제항목은 정보체계 및 조직 정보의 기밀성, 무결성, 가용성을 보호하고 일련의 정의된 보안 요구사항을 충족하도록 설계된 보호조치 또는 대책으로, 주로 선정부터 평가까지 활용된다.

NIST SP 800-53 문서에서는 보안통제항목 별 지침(Supplemental Guidance), 보안 요구사항(Control Enhancements) 등을 확인할 수 있다. 예를 들어, 무기체계 소프트웨어의 경우 실시간성 및 안정성 등을 관리하기 위하여 선정 단계에서 실시간 모니터링 (SI-4), 침해사고 대응 (IR-5) 항목 등이 선별될 것이며, 기관에서

Table 1. RMF Security Controls[8]

Identifier	Family
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authentication
IR	Incident Response
MA	MAintenance
MP	Media Protection
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisition
SC	System and Communications Protection
SI	System and Information Integrity
PM	Program Management

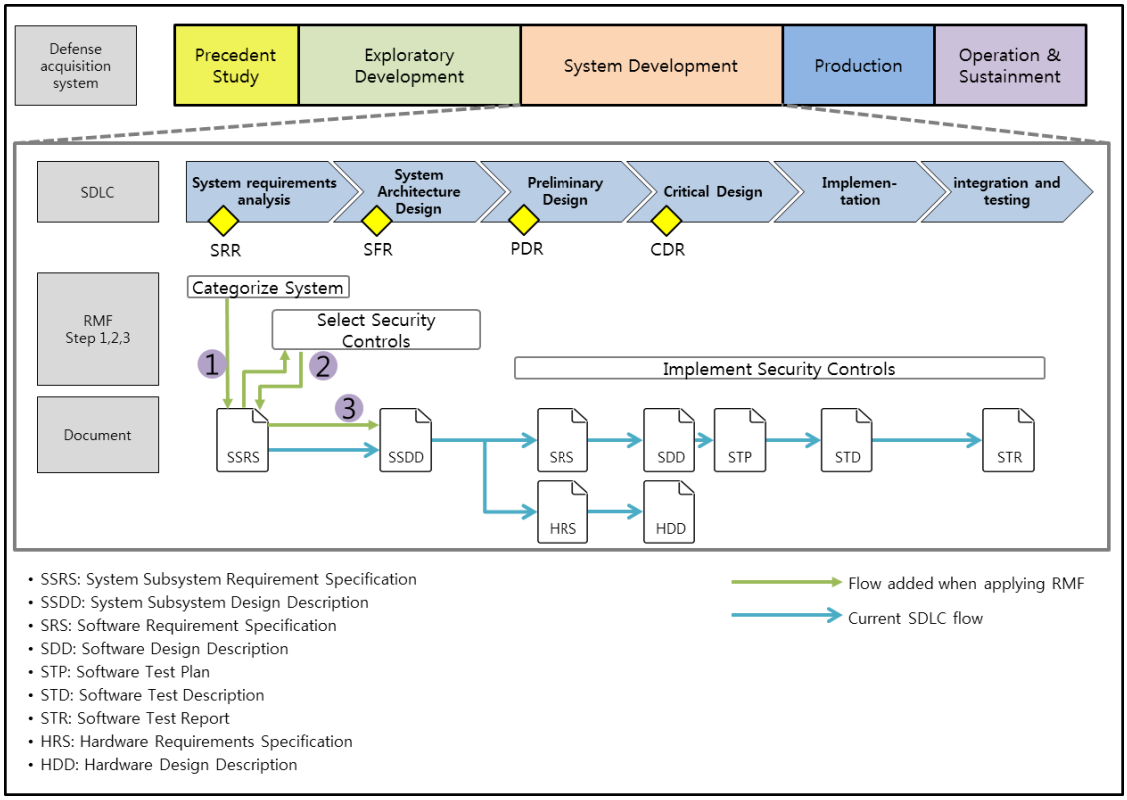

Fig. 2. Proposal of the relationship between documents and SDLC when applying RMF[9]

는 조직 혹은 시스템을 대상으로 보안 요구사항을 반영할 수 있도록 개발하고, 구현 여부를 평가받아야 한다.

2.2 K-RMF

2.2.1 연구 배경

K-RMF는 미국 군에서 동맹국에 RMF 제도를 도입할 것을 요구함에 따라 연구되기 시작한 제도이다. 미 군에서는 이미 2014년부터 RMF 제도를 군 내에 도입하여 사용하고 있었지만, F-35의 경우 데이터의 전송 범위가 F-35를 운용하는 다른 동맹국까지 확장되어 있다. 따라서 미국에서는 동맹국에도 RMF 제도를 도입하여 데이터의 안전성을 보장할 것을 요구하였고, 美 RMF 제도를 벤치마킹한 한국형 RMF 제도의 개발이 시작되었다[4].

K-RMF는 美 RMF 요구수준과 국제표준을 충족시키는 한국형 위험관리 프레임워크이다. K-RMF는 시스템 소요제기부터 전력화 및 폐기 단계까지 보안위험을 관리하기 위하여 美 RMF 6단계 프레임워크 구조와 동일한 단계로 진행된다. 다만 각 요구사항은 한국군 및 제도를 반영할 수 있도록 美 RMF 보안통제항목과 ISO 27001을 반영한 한국형 보안통제항목으로 개발되었다[6].

2.2.2 무기체계 개발단계 소프트웨어 산출물

K-RMF 제도를 도입하기 위해서는 사업의 다양성, 사업관리 측면 등이 종합적으로 고려되어야 하며, RMF 단계별로는 매 단계 종료 시점에서 발생하는 산출물의 작성 방안이 연구되어야 한다. 따라서 기존 산출되는 문서와 K-RMF 산출물과의 연계성을 검토하고, 현행 산출물과 과업을 최대한 활용해야 한다.

이와 관련하여 기존 무기체계 개발단계에서 산출되는 문서를 美 RMF 단계에 적용하는 방법을 제안한 연구 사례가 있다[9]. 제안 방법에서는 美 RMF 1단계 수행 결과를 체계요구사항명세서(System Subsystem Requirement Specification, 이하 SSRS) 3.8장 '보안 및 프라이버시 보호 요구사항'에, 2단계 수행 결과를 체계설계기술서(System Subsystem Design Description, 이하 SSDD) 4장 '체계 구조설계'에 반영하면 기본설계 이후부터 요구되는 기술문서는 SSDD까지 작성된 요구사항을 세분화하여 표기할 수 있다. 다만 제안 방법을 K-RMF 제도 도

입 시 활용하기 위해서는 기본설계(PDR) 단계 이후부터 요구되는 기술문서에도 보안통제항목 요구사항을 반영할 수 있어야 한다.

Table 2. Example of SC-7(5) Implement Plan in SDP

1. Scope
2. Referenced documents
3. Overview of required work … o Only necessary traffic should be allowed exceptionally by utilizing intrusion prevention systems, web firewalls, etc., and all traffic except this should be rejected. …
4. Plans for performing general software development activities
5. Plans for performing detailed software development activities
6. Schedules and activity network
7. Project organization and resources
8. Notes

현행 무기체계 연구개발단계 중 PDR 단계 이후부터 요구되는 문서는 하드웨어와 소프트웨어로 구분하여 작성된다. 이중 상세설계(CDR) 단계까지 작성되는 소프트웨어 산출물에는 소프트웨어 개발계획서(Software Development Plan, 이하 SDP), 소프트웨어 요구사항명세서(Software Requirement Specification, 이하 SRS), 소프트웨어 설계기술서(Software Design Description, 이하 SDD)가 있다. 해당 문서는 모든 개발 사업이 준수해야 하는 표준 문서로, 각 문서의 목차별 상세 작성 방법은 [무기체계 소프트웨어 개발 및 관리 매뉴얼]에 명시되어 있다[10].

Table 3. Example of SC-5 Implement Plan in SRS

1. Scope
2. Referenced documents
3. Requirements … o Availability: Servers and networks should be redundant to protect systems from denial-of-service (DoS) attacks …
4. Qualification provisions
5. Requirements traceability
6. Notes

3. K-RMF 보안 평가 방안 제안

본 논문에서 제안하는 보안 평가 방안은 개발 초기 단계에서 작성되는 소프트웨어 산출물에 보안통제항목 요구사항을 반영하는 방법이다. 활용 가능한 산출물로는 소프트웨어 개발계획서, 요구사항명세서, 설계기술서가 해당하며, 문서 내 명시된 보안 요구사항은 추후 평가 단계에서 검토 자료로 활용될 수 있다.

보안 요구사항을 명시하기 위해서는 [무기체계 소프트웨어 개발 및 관리 매뉴얼]에 보안 요구사항을 표기 가능한 목차를 지정해야 한다. 본 논문에서는 목차 지정과 더불어 美 RMF SC 패밀리 보안통제항목 일부를 사례로 작성해 보았다. SC 패밀리는 저장, 처리, 전송되는 정보의 기밀성과 무결성을 보장할 수 있는 정책 등을 요구하는 보안통제항목으로, 확장된 네트워크 공간에서 발생할 수 있는 각종 위협으로부터 데이터를 보호하기 위해 요구되는 보안 대책을 포함한다.

(1) 소프트웨어 개발계획서

소프트웨어 개발계획서는 사업 전반에 걸쳐 개발 전 결정이 필요한 구매 소프트웨어 등과 관련된 내용을 포함한다. 따라서 소프트웨어 개발계획서에 작성될 수 있는 보안 요구사항은 사업 전반에 걸쳐 요구되어야 한다. 예를 들어, SC-7(5) BOUNDARY PROTECTION | DENY BY DEFAULT / ALLOW BY EXCEPTION 항목의 경우, 네트워크 영역에 방화벽(Firewall), 침입방지시스템(IPS) 등을 활용하여 필요한 트래픽만 예외적으로 허용할 수 있는 환경을 계획할 수 있다.

(2) 소프트웨어 요구사항명세서

소프트웨어 요구사항명세서는 소프트웨어 요구사항분석 단계에서 작성되어야 하며, 연구개발 주관기관에서 보안 기능과 관련하여 요구해야 하는 보안 요구사항을 포함하게 된다.

SC 패밀리 보안통제항목 중 요구사항 단계에서 작성 가능한 항목에는 기밀성, 무결성을 보장하는 방안 등이 해당될 수 있다. 예를 들어, SC-5 Denial of Service Protection 항목에서는 DoS(Denial of Service) 공격에 대한 보호 방안을 구성할 것을 요구하는데, 해당 요구사항에 대한 구현 여부를 판단하기 위하여 소프트웨어 요구사항명세서 내 DoS 공격 발생 시 빠른 복구 방안을 포함하고, 이를 검토할 수 있다.

Table 4. Example of SC-8, SC-10 Implement Plan in SDD

1. Scope
2. Referenced documents
3. Requirements … o If the user does not perform any action for more than 10 minutes, the communication session should be automatically terminated. … o To maintain the integrity of the transmitted information, all data transmitted within the network segment must be encrypted during transmission. o To ensure the confidentiality of the transmitted information, the firewall must check and block untrusted ports in advance. …
4. Architectural Design
5. CSCI Detailed Design
6. Requirements Traceability
7. Notes
8. Acronyms and Abbreviations

(3) 소프트웨어 설계기술서

연구개발 주관기관은 소프트웨어 형상품목(CSCI)의 소프트웨어 구성품(CSC)과 기능을 식별하고 이들 간의 상관관계를 정의하여 소프트웨어 설계기술서에 표기해야 한다. 소프트웨어 형상항목(CSCI)의 설계 결정사항, 구성품이 식별 가능한 수준으로 명시되어야 하며 소프트웨어 구성품(CSC)는 운영/유지 실현 가능성을 확인하기 위하여 실행개념이 상세하게 기술되어 있는지 검토해야 한다.

소프트웨어 설계기술서에 작성될 수 있는 보안통제항목 요구사항은 상세한 매개변수 설정이 필요한 항목이다. 예를 들어 보안통제항목 SC-10 Network Disconnect의 경우, 보안 요구사항으로 일정 시간 사용하지 않는 시스템의 연결을 종료해야 한다는 요구사항이 뒤따르는데 이를 구현하기 위해서는 소프트웨어 설계기술서에 해당 요구사항이 요구되는 응용프로그램의 요구사항으로 관련 항목을 포함할 수 있다.

저장된 정보 외에 수신 간 정보를 보호하기 위한 보안 요구사항을 다루는 SC-8 Transmission에서는 데이터의 기밀성과 무결성을 보호하는 것을 요구하는데, 이와 관련해서는 기밀성과 무결성을 보호하는 방안을 각각 작성할 수 있다. 무결성을 보호하기 위하여 SHA-256과 같은 해시함수를 이용하여 데이터가 최초 원본 상태와 다른 것인지 확인할 수 있으며 기밀성을 보호하기 위해서는 불필요한 포트를 차단하고 유입되는 유해 트래픽을 침입방지시스템에서 차단하여 안정적인 서비스를 제공한다는 내용이 포함될 수 있다.

4. 결론

본 논문에서는 개발 초기 단계에서 작성된 소프트웨어 산출물 내 美 RMF 시스템 및 통신 관련 보안 요구사항을 작성하는 방안에 관하여 기술하였다. 개발 초기 단계에서 작성되는 산출물인 소프트웨어 개발계획서, 요구사항명세서, 설계기술서 내 보안 요구사항을 명시할 수 있는 목차를 확인하였으며, 시스템 통신 관련 보안 요구사항을 산출물 내에 작성할 수 있는 사례를 제시하였다.

K-RMF 제도가 성공적으로 정착되기 위해서는 평가 단계뿐 아니라 타 단계에서도 사업 영향성 및 비용을 최소화하면서 K-RMF 제도를 도입할 방법을 고려해야 한다. 시스템 분류 단계에서는 무기체계별 상황, 운영환경 등을 종합적으로 반영할 수 있는 기준이 마련되어야 하며, 구현 단계에서는 한국군 환경 및 훈령을 포함할 수 있는 구현 계획이 작성되어야 할 것이다. 제시한 무기체계 소프트웨어 산출물 기반 평가방법은 K-RMF 단계별 산출물에 대한 이해를 높이는 데 참고 가능하며, 향후 K-RMF 제도 도입 시 일부 보안통제항목을 대상으로 보안평가 절차를 간소화하는 데 활용할 수 있다.

References

[1] Y. Jeong, S. Kim and H. Park, "Development Trends of Defense Science and Technology based on the 4th Industrial Revolution," Electronics and Telecommunications Trends, vol. 35, no. 6, pp. 56-67, Dec, 2020. DOI: https://doi.org/10.22648/ETRI.2020.J.350606

[2] http://www.boannews.com/media/view.asp?idx=1156_10

[3] https://www.boannews.com/media/view.asp?idx=1103_01

[4] https://www.dailysecu.com/news/articleView.html?idxno=71186

[5] "Guide for Applying the Risk Management Framework to Federal Information Systems," NIST SP 800-37 Rev.1, Feb. 2010.

[6] W. Yang, S. Cha, J. Yoon, H. Kwon, and J. Yoo, "Korean Security Risk Management Framework for the Application of Defense Acquisition System," Journal of the Korea Institute of Information Security & Cryptology, vol. 32, no. 6, pp. 1183-1192, Dec. 2022.

DOI: https://doi.org/10.13089/JKIISC.2022.32.6.1100

[7] J. Kim, S. Jeong., "The first step toward the success of the Korean risk management framework (KRMF): System Classification Orientation Study," Journal of Advances in Military Studies, vol. 5, no. 2, pp. 73-106, 2022. DOI: https://doi.org/10.37944/jams.v5i2.151

[8] "Security & Privacy Controls for Federal Information Systems and Organizations", NIST SP 800-53 Rev.4, 2013.

[9] H. Cho, S. Cha, and S. Kim, "A Case Study on the Application of RMF to Domestic Weapon System," Journal of the Korea Institute of Information Security & Cryptology, vol. 29, no. 6, pp. 1463?1475, Dec. 2019. DOI: https://doi.org/10.13089/JKIISC.2019.29.6.1463

[10] "Weapon System Development and Management Manual," DAPA(Defense Acquisition Program Administration, Nov. 2018.

최 은 진(Eun-Jin Choi) [정회원]

- 2019년 2월 : 한국기술교육대학교 컴퓨터공학부 (공학사)
- 2021년 2월 : 성균관대학교 전자전기컴퓨터공학과 (공학석사)
- 2022년 7월 ~ 현재 : 국방기술품질원(DTaQ) 연구원

〈관심분야〉
국방품질경영, 사이버보안, K-RMF