특집 07

국방 RMF 연구 사례 분석

조광수·김예준·안정근·김정현·곽지원·김해나·백근우·김승주 (고려대학교)

목 차

1. 서 론

소총, 기관총, 전차 및 야포 등의 다양한 무기체계들이 점차 네트워크로 연결되기 시작하였다. 이는 지휘관이 전장 상황을 빠르게 인지하고 신속하게 결심 및 지휘통제 할 수 있도록 만들기 위함이다. 하지만, 무기체계가 네트워크에 연결됨으로써 무기체계에 침투할 수 있는 공격 표면이 확대되었으며 확대된 공격 표면으로 인한 사이버 위협의 발생 가능성도 함께 증가하였다. 무기체계에 대한 사이버 위협이 늘어남에 따라 자연스럽게 공격자로부터 무기체계를 안전하게 보호하기 위한 무기체계 사이버보안의 중요성 또한 대두되고 있다[1]. 미 국방성은 증가하는 사이버 위협으로부터 무기체계를 안전하게 보호하기 위해 과거부터 평가 및 획득 체계를 개발하여 국방획득체계에 적용하였다. 통칭 Orange Book으로 불리던 TCSEC (Trusted Computer System Evaluation Criteria)부터 DITSCAP (Defense Information Technology Security Certification and. Accreditation Process), DIACAP (Department of Defense Information Assurance Certification and Accreditation Process)을 거쳐 가장 최신에 개발된 RMF A&A (Risk Management Framework Assessment & Authorization)까지 다양한 제도를 발전시키며 사용하고 있다[2]. 현재 사용되고 있는 RMF A&A의 가장 큰 특징은 잔존위험도를 기반으로 획득 여부를 결정한다는 것이다. RMF A&A 이전의 평가 수단은 체크리스트 형식으로 구성되어 전체 평가항목에 대해 통과하도록 요구되었다. RMF A&A의 경우 무기체계 개발에 필요한 막대한 비용 등을 고려하여 통과하지 못한 평가항목이 존재하더라도 임무 수행의 관점에서 위험도를 판단한 후 획득 여부를 결정하게 된다. 물론, 통과하지 못한 평가항목은 추후 보완 조치가 올바르게 취해질 수 있도록 요구된다[3].

미국의 경우, 국방 분야 대상으로 개발 및 활용되는 DoD (Department of Defense)의 RMF A&A, 연방정부 및 일반 산업 분야에서 활용할 수 있는 NIST (National Institute of Standards and Technology)의 NIST SP 800-37이 존재한다. 이 중 NIST SP 800-37은 전체 RMF 프로세스부

터 상세한 보안통제항목 Baseline까지 관련 문서가 모두 민간 영역에 공개되어 있기에 RMF를 적용하고자 하는 민간 업체에서 참조할 수 있는 충분한 자료를 획득할 수 있다. 반대로, 국방 분야에서 활용되는 RMF A&A의 경우 간단한 예시로 활용할 수 있는 극히 일부 자료만을 DoD 산하기관인 DCSA (Defense Counterintelligence and Security Agency) 등을 통해 공개하고 있다[4].

미 국방성은 RMF A&A를 개발하여 자국 내에서 적용하는 것뿐만이 아니라 외부 요인에 의해 미군의 중요 자원이 위협받지 않도록 2015년 국방 사이버 전략의 일부분으로 동맹국에 대한 사이버 보안 능력을 강화할 수 있도록 적극 지원할 것을 발표하였다[5]. 이러한 국방 사이버 전략 구현의 일환으로 우리나라를 포함한 동맹국들 중 미군의 무기체계와 직간접적으로 연동되는 무기체계 운용 국가에 대해 RMF 적용을 요구한 바 있다[6]. 이러한 요구에 대응하기 위해 우리나라에서도 국방부를 비롯한 유관기관에서 RMF 제도의 적용 및 대응하기 위한 연구와 시범 적용 사업을 수행하고 있다. 미국과 우리나라는 국방 획득체계의 제도적 기반과 요구되는 보안 수준이 상이하기 때문에 기존 미국의 RMF A&A를 그대로 도입할 수 없다[7]. 이에 우리나라에서는 미국의 RMF A&A와 NIST SP 800-37을 벤치마킹하여, 국방 사이버보안위험관리제도인 K-RMF (Korea-RMF)를 개발하고 있다. 하지만, 현재까지는 해당 K-RMF 제도와 관련하여 공개된 공식 문서는 존재하지 않으며 2026년 전면 적용될 예정에[8] 따라 추후 관련 자료들이 발표될 것으로 보여진다. 본 연구에서는 국내외에서 RMF와 관련하여 어떠한 연구들이 수행되었는지 조사한다. 이를 통해 추후 K-RMF 제도 개발 및 관련 연구를 수행함에 있어서 인사이트를 제공하고자 한다.

2. RMF 개념 및 단계

NIST에서 관리하고 공개하는 용어집인 NIST Glossary[9]에 따르면 RMF는 “A structured approach used to oversee and manage risk for an enterprise.”로 정의된다[10]. 즉, 어떠한 조직의 비즈니스 목표 달성 또는 주어진 임무 수행에 있어서 발생 될 수 있는 잠재적 위험을 미리 식별하고 완화 시키기 위해 수행해야 하는 일련의 활동들과 관련 바탕 자료들을 모아둔 하나의 방법론이다. 현재 공개되어있는 연방정부 및 일반 산업 분야 대상의 RMF인 NIST SP 800-37에 따르면 RMF 프로세스는 크게 총 7가지 단계로 구성되어 있으며, 점차 발전하고 정교해지는 공격 기법에 대응하고 이전에 미처 발견하지 못한 위험 요소를 지속적으로 추적 감시 할 수 있도록 7단계를 반복 수행하도록 만들어져있다. NIST SP 800-37 문서를 중심으로 RMF 각 단계에 대한 활동을 뒷받침할 수 있는 다양한 문서들이 존재한다. 대표적으로, 조직이 보안 목표를 달성하기 위해 필요한 보안 요구사항인 전체 보안통제항목을 NIST SP 800-53 문서로 작성하여 배포하고 있다. 다음 2.1 ~ 2.7절에서는 RMF 프로세스를 구성하는 각 단계에 대해 간략히 설명한다.

2.1 준비(Prepare) 단계

준비 단계는 RMF를 적용하고자 하는 조직이 체계 개발 프로젝트를 시작하기에 앞서서 이후 RMF 단계들을 원활히 진행하는데 필요한 사전 활동을 수행하는 단계이다. 준비 단계 활동을 통해 조직 구성원들의 RMF에 대한 이해도를 높이고, 보안 통제항목 baseline 및 공통 통제항목 등 추후 체계 보안 분류 단계 ~ 모니터링 단계에서 활용할 자원을 확보한다. NIST SP 800-37에 따르면 준비 단계는 다음 <표 1>과 같은 18개 활동으

〈표 1〉 준비 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
조직 수준의 준비 활동	
P-1 위험관리 역할 식별	- RMF에 따라 체계를 개발 및 획득하기 위한 중요 역할들이 식별되고 조직 구성원 개인에게 할당되어야 함
P-2 위험관리 전략 수립	- 조직이 감내(수용)할 수 있는 위험 수준에 관한 결정 및 표현을 포함하는 위험관리 전략이 수립되어야 함
P-3 위험평가 - 조직	- 조직 전체적인 관점에서 위험평가가 수행되고, 기존의 위험평가 결과가 최신화되어야 함
P-4 통제항목 baseline 구축 (Optional)	- 활용가능한 통제항목 baseline 및 사이버보안 프레임워크 프로필 구축
P-5 공통 통제항목 식별	- 개발 또는 획득하고자 하는 체계가 상속할 수 있는 공통 통제항목의 식별 및 문서화, 배포
P-6 영향도 우선순위 선정 (Optional)	- 조직의 임무 및 비즈니스 목표에 대해 동일한 영향 수준을 지니는 체계에 대한 우선순위 선정
P-7 지속 모니터링 전략 수립 - 조직	- 조직 전체적으로 구현된 통제항목의 효과를 모니터링 하기 위해 필요한 통제항목 모니터링 전략을 개발 및 구현
체계 수준의 준비 활동	
P-8 임무 및 비즈니스 식별	- 개발 및 획득하고자 하는 체계가 지원해야 하는 조직의 임무, 비즈니스 기능, 및 프로세스를 식별해야 함
P-9 체계 이해관계자 식별	- 개발 및 획득하고자 하는 체계와 관련된 이해관계자를 모두 식별하고 목록화해야 함
P-10 자산 식별	- P-9에서 식별된 이해관계자들의 중요 자산 목록을 식별해야 함
P-11 인가 범위 식별	- 개발 및 획득하고자 하는 인가 범위(체계)를 식별해야 함
P-12 정보 유형 식별	- 개발 및 획득하고자 하는 체계에 의해서 처리, 저장, 및 전송되는 정보 유형을 모두 식별해야 함
P-13 정보 수명주기 이해	- P-12에서 식별된 정보 유형들에 대한 체계 내 수명주기(즉, 언제 생성되어 어떠한 과정을 거쳐 언제 소멸되는지)를 식별하고 이해해야 함
P-14 위험평가 - 체계	- 개발 및 획득하고자 하는 체계에 대한 위험평가가 수행되고, 기존의 위험평가 결과가 최신화되어야 함
P-15 요구사항 정의	- 보안 및 개인정보보호 요구사항이 정의되고 각 요구사항 간 우선순위가 선정되어야 함
P-16 조직 아키텍처 결정	- 개발 및 획득하고자 하는 체계가 조직 내 어느 위치에 설치되고 조직에 기존에 존재하는 타 체계와 어떻게 연동되는지 그 아키텍처가 결정되어야 함
P-17 요구사항 할당	- P-15에서 정의된 요구사항을 체계 또는 체계의 운영 환경에 적절히 배치해야 함
P-18 체계 등록	- 관리, 유지보수 및 모니터링 목적으로 조직 내 관리 체계(형상 관리 서버 등)에 개발 및 획득하고자 하는 체계가 등록되어야 함

로 구성되며, 7개의 “조직 수준”활동과 11개의 “체계 수준”활동으로 구분된다.

2.2 체계 보안 분류(Categorize) 단계

체계 보안 분류 단계는 RMF의 첫 번째 주요 단계로, 조직이 개발 및 획득하고자 하는 체계의 임무 영향도를 판단하는 단계이다. 이때, 임무 영향도란 위험도와 유사한 의미를 가지며, 조직에게 주어진 임무 또는 비즈니스 목표를 달성하는데 있어서 해당 체계 또는 정보 유형이 얼마나 큰 영향을 미치는지 수치화 한 것을 의미한다. NIST SP 800-37에 의하면 RMF에서는 이러한 임무 영향도를 분석하는 기준으로 CIA(C: Confidentiality – 기밀성, I: Integrity – 무결성, A: Availability – 가용성)의 3가지를 활용한다. 본 체계 보안 분류

〈표 2〉 체계 보안 분류 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
C-1 체계 설명	- 조직이 개발 및 획득하고자 하는 체계의 특징이 모두 설명되고 문서화되어야 함
C-2 보안 분류 선정	- 체계 내에서 처리, 저장, 전송되는 정보를 포함하여 조직이 개발 및 획득하고자 하는 체계의 보안 분류가 선정되어야 함 - 체계 보안 분류의 결과가 보안 계획, 개인정보보호 계획, 공급망 위험관리 계획에 문서화 되어야 함 - 체계 보안 분류의 결과가 조직의 임무, 비즈니스 기능, 임무 및 비즈니스 프로세스를 보호하기 위한 조직의 아키텍처 및 활동 목적과 일치하도록 조정해야 함 - 체계 보안 분류의 결과가 조직의 위험관리 전략을 충분히 반영하여야 함
C-3 체계 보안 분류 검토 및 승인	- 체계 보안 분류의 결과가 조직의 임원들에 의해 충분히 검토되고 최종적으로 승인되어야 함

단계에서 결정된 임무 영향도를 바탕으로 조직은 체계 개발 및 획득의 기준(즉, 보안 통제항목)을 선정하고 평가하게 된다. NIST SP 800-37에 따르면 체계 보안 분류 단계는 다음 <표 2>와 같은 3개 활동으로 구성된다.

2.3 보안통제항목 선정(Select) 단계

보안통제항목 선정 단계는 RMF의 두 번째 주요 단계로, 체계 보안 분류 단계에서 결정된 임무 영향도 및 체계 보안 분류에 따라 조직 및 체계를 보호하는데 필요한 보안통제항목을 선택, 교정, 할당하는 단계이다. NIST SP 800-37에 따르면 이전 단계에서 결정된 보안 분류에 따라 체계에 구현되어야 하는 보안통제항목의 기본 목록이 결정되며, 이를 보안통제항목 baseline이라고 칭한다. NIST에서는 본 단계에서 활용할 수 있는 전체 보안통제항목을 NIST SP 800-53 문서로 공개하고 있으며, 임무 영향도별 구현되어야 하는 보안통제항목 baseline을 NIST SP 800-53B 문서로 공개하고 있다. 하지만 미 국방성에서 활용 중인 군용 RMF A&A의 경우 별도로 보안통제항목 baseline을 공개하고 있지 않다. NIST SP 800-37에 따르면 보안통제항목 선정 단계는 다음 <표 3>과 같은 6개 활동으로 구성된다.

〈표 3〉 보안통제항목 선정 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
S-1 통제항목 선택	- 결정된 위험도(체계 보안 분류)에 상응하여 체계 및 조직을 보호하는데 필요한 보안통제항목 baseline을 선택해야 함
S-2 통제항목 교정	- 체계의 특성 및 조직 내 보안 정책에 따라 보안통제항목이 교정되어야 함
S-3 통제항목 할당	- 각 보안통제항목이 체계특정, 하이브리드, 또는 공통통제항목 중 한가지로 지정되어야 함 * *하이브리드 보안통제항목: 하나의 보안통제항목 내 세부 항목이 부분적으로 체계특정적, 공통적 특징을 모두 갖는 것* - 각 보안통제항목이 체계 내 적절한 위치에 할당되어야 함
S-4 통제항목 구현 계획 문서화	- 선택되고 교정된 보안통제항목이 보안 계획 문서, 개인정보보호 계획 문서 또는 이에 상응하는 문서에 기술되어야 함
S-5 지속적 모니터링 전략 수립 - 체계	- 준비 단계에서 수립된 조직적 모니터링 전략과 선택 및 할당된 보안통제항목을 반영하는 상세 체계 모니터링 전략이 수립되어야 함
S-6 계획 검토 및 승인	- 위험도(체계 보안 분류)를 충분히 고려하여 선택 및 교정된 보안통제항목이 체계와 조직을 충분히 보호할 수 있는지 인가 담당자(authorization official)에 의해 검토되고 승인되어야 함

〈표 4〉 보안통제항목 구현 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
I-1 통제항목 구현	- 보안 계획 및 개인정보보호 계획에 명시된 보안통제항목은 실제로 구현되어야 함 - 체계 보안 계획 및 개인정보보호 계획 내 통제항목을 구현하는데 체계 보안 및 개인정보보호 공학 방법론이 사용되어야 함
I-2 통제항목 구현 정보 갱신	- 통제항목의 계획된 구현에 대한 변화는 문서화 되어야 함 - 실제 구현 과정 중 발견된 정보 및 변경된 계획을 포함할 수 있도록 보안 및 개인정보보호 계획은 갱신되어야 함

2.4 보안통제항목 구현(Implement) 단계

보안통제항목 구현 단계는 RMF의 세 번째 주요 단계로, 보안통제항목 선택 단계에서 승인된 보안 계획 및 개인정보보호 계획에 따라 보안통제항목을 실제로 체계 또는 체계 운영 환경에 구현하는 단계이다. 본 단계에서는 보안통제항목을 구현하는데 필요한 소프트웨어를 개발하는 것뿐만 아니라 개발된 체계 소프트웨어 및 하드웨어를 실제 운영 환경에서 올바르게 설정 및 구현하고 잠재적 보안 위협이 존재하는지 확인 및 수정할 수 있는 상세 방법을 문서화하여야 한다. 이러한 구현 단계에서 작성되는 문서 일체를 STIGs(Security Technical Implementation Guides)라고 칭한다. NIST SP 800-37에 따르면 보안통제항목 구현 단계는 다음 <표 4>와 같은 2개 활동으로 구성된다.

2.5 평가(Assess) 단계

평가 단계는 RMF의 네 번째 주요 단계로, 보안통제항목 구현 단계에서 개발되고 문서화된 보안통제항목이 최종적으로 제출된 보안 계획 및 개인정보보호 계획과 일치하는지, 잔존 위험도는 얼마나 존재하는지 검토하는 단계이다. 본 단계에서

〈표 5〉 평가 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
A-1 평가자 선택	- 보안통제항목 평가를 위한 평가자 또는 평가팀을 구성해야 함 - 구성된 평가자 또는 평가팀이 적절한 평가활동을 수행할 수 있도록 적절한 수준의 독립성이 보장되어야 함
A-2 평가 계획 수립	- 평가활동에 필요한 각종 문서 및 양식이 평가자 또는 평가팀에게 제공되어야 함 - 보안 및 개인정보보호 평가 계획이 개발되고 문서화되어야 함 - 보안 및 개인정보보호 평가 계획은 보안통제항목 평가 결과에 대한 기대치와 필요한 노력 수준을 설정하기 위해 검토 및 승인되어야 함
A-3 통제항목 평가	- 보안통제항목 평가는 보안 및 개인정보보호 평가 계획에 따라 수행되어야 함 - 비용 효율적으로 위험관리를 수행할 수 있도록 이전 평가 결과의 재사용 여부를 충분히 고려해야 함 - 가능한 경우 자동화 도구를 사용하여 보안통제항목 평가를 수행하여 평가의 속도, 효과 및 효율성을 향상시킬 수 있음
A-4 평가 보고서 작성	- 평가 결과와 수정 권장 사항을 제공하는 보안 및 개인정보보호 평가 보고서가 작성되어야 함
A-5 완화 활동 수행	- 구현된 보안통제항목의 결함을 해결하기 위해 즉각 수행할 수 있는 개선 조치를 취해야 함 - 평가 및 후속 개선 조치에 따라 변경된 보안통제항목 구현 변경 사항을 보안 및 개인정보보호 계획은 반영할 수 있도록 갱신하여야 함
A-6 보완 계획(PoA&M, Plan of Action & Milestone) 수립	- 보안 및 개인정보보호 평가 보고서에 기술된 허용 불가능 위험에 대하여 상세한 개선 계획을 문서화해야 함

〈표 6〉 인가 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
R-1 인가패키지 개발	- 인가패키지는 인가 담당자에게 제출하기 위해 개발되어야 함
R-2 위험 분석 및 결정	- 위험 분석 결과와 허용 가능한 위험도를 포함하는 위험관리 전략에 따른 인가 담당자의 위험 결정
R-3 위험 대응	- 결정된 위험에 대한 위험 대응이 제공되어야 함
R-4 인가 결정	- 공통 통제항목 또는 체계의 인가 결과가 승인 또는 거절로 결정되어야 함
R-5 인가 보고	- 인가 담당자는 인가 결정, 중대 취약점 및 위험 요소를 조직의 임원에게 보고해야 함

평가가 수행된 이후 미흡 항목이 발견되면 해당 미흡 항목에 대해 즉시 수정이 가능할 경우 수정 후 재검토를 받게 되며, 즉시 수정이 불가능할 경우 추후 보완 계획 수립과 함께 미흡 항목에 대한 잔존위험도를 측정한다. NIST SP 800-37에 따르면 평가 단계는 다음 <표 5>와 같은 6개 활동으로 구성된다.

2.6 인가(Authorize) 단계

인가 단계는 RMF의 다섯 번째 주요 단계로, 평가 단계 결과로 도출된 평가 결과를 바탕으로 인가 패키지를 개발하고 최종적으로 체계를 인가(획득)할 것인지 결정하는 단계이다. 인가 결정의 근거인 인가 패키지는 체계 보안 분류 단계부터 평가 단계까지 도출된 결과인 보안 계획, 개인정보보호 계획, 보안 평가 결과, 개인정보보호 평가 결과 및 보완 계획을 포함하는 문서 일체이다. 인가 담당자는 이러한 문서 일체를 바탕으로 잔존위험도를 감내하고 체계를 인가할 것인지 판단한다. NIST SP 800-37에 따르면 인가 단계는 다음 <표 6>과 같은 5개 활동으로 구성된다.

2.7 감시(Monitor) 단계

감시 단계는 RMF의 여섯 번째 주요 단계로, 인가한 체계에 추가적인 위협 또는 발견되지 않은 위험이 운영 중 발생되었는지 지속적으로 관찰하는 단계이다. 감시 결과에 따라 발생된 모든 변경사항은 보안 계획 및 개인정보보호 계획에 지속적으로 반영될 수 있도록 해당 문서를 갱신해야 한다. NIST SP 800-37에 따르면 감시 단계는 다음 <표 7>과 같은 7개 활동으로 구성된다.

〈표 7〉 감시 단계 세부 활동 목록

활동	활동 수행 결과 및 산출물
M-1 체계 및 환경 변화 감시	- 정보 체계와 운영 환경은 지속적인 감시 전략에 따라 감시되어야 함
M-2 지속적 평가 수행	- 지속적인 감지 전략에 따라 보안통제항목 효과에 대한 지속적인 평가를 수행해야 함
M-3 지속적 위험 대응	- 지속적인 감시 활동의 결과를 분석하여 발견된 위험에 적절하게 대응해야 함
M-4 인가패키지 갱신	- 인가패키지에 포함된 위험관리 문서 일체는 지속적인 감시 활동을 기반으로 갱신되어야 함
M-5 보안 및 개인정보보호 보고	- 조직별로 정해진 절차에 따라 현재의 보안 및 개인정보보호 상태를 인가 담당자 및 기타 고위 경영진과 임원에게 보고해야 함
M-6 지속적 인가 수행	- 인가 담당자는 지속적인 감시 활동의 결과를 사용하여 지속적인 인가 활동을 수행하고 위험 결정 및 인가 결정의 변경사항을 전달해야 함
M-7 체계 폐기	- 필요에 따라 체계 폐기 전략을 개발하고 실행해야 함

3. 국외 RMF 동향

미 정부는 1980년대 초부터 제품 개발 시 사이버보안의 중요성을 인식하여 군을 중심으로 이와 관련한 기반 기술을 마련함과 동시에 각종 기준 및 지침 등을 개발하였다. 미 국방부는 1985년 신뢰성 있는 컴퓨터 시스템 평가기준인 TCSEC을 시작으로 제품에 대한 보안성 평가를 수행하여 안전한 제품을 개발하기 시작하였다. 이후 유럽의 평가기준인 ITSEC(Information Technology Security Evaluation Criteria)과 통합하여 CC(Common Criteria)가 제정되었다. CC는 전체 시스템이 아닌 단일 제품만 평가한다는 측면에서 평가방법을 무기체계에 직접 적용하기 어려운 부분이 존재한다. 따라서 무기체계를 운용하는 군에서는 사용하기에 적합하지 않다. 이에 미 국방부는 1997년 군에서 사용되는 제품, 환경, 시스템에 대한 통합적 보안 평가 및 인증을 위해 정보 기술 보안 인증 및 인가 프로세스인 DITSCAP을 수립하였다. 하지만 DITSCAP의 경우 독립적인 체계에 한정하여 평가가 가능하고, 표준화된 보안통제 항목이 없기에 시스템별로 새롭게 정의한 보안통제항목을 사용한다는 문제점이 존재한다. 이러한 문제점을 해결하고자 미 국방부는 2007년에 DITSCAP을 DIACAP으로 대체하였다. DIACAP은 DoDI 8500.02의 표준 보안통제항목을 활용하는 것으로 DITSCAP의 문제점을 보완하였다. 이후 국방부는 타 정부기관과의 상호호환성을 높일 수 있는 인증 및 획득 제도를 구축하기 위해 NIST의 RMF를 바탕으로 RMF A&A 프로세스를 구축하였다. 이러한 흐름에 따라 2012년 미 국방부지침(DoDI) 8510.01 “Risk Management Framework(RMF) for DoD Information Technology(IT)”에서는 국방부 내의 RMF 사용을 의무화하고 있다[11]. DoDI 8510.01은 RMF를 이용하여 DoD IT의 수명주기 내 사이버 보안 위험을 관리하는 지침을 제공하고 있으며 무기체계 획득 시 관련기관이 개발·운용시험평가에 RMF 프로세스를 통합하도록 의무화하고 있다[12]. 또한 2015년 미 국방부는 ‘국방부 사이버 전략(The Department of Defense Cyber Strategy)’을 통해 군에서 사용하는 일반적인 전산 시스템뿐만 아니라 첨단 무기체계도 사이버보안을 개선해야 한다고 발표했다[13]. 이외에도 2019년 미 국방부는 ‘Risk Management Framework for Army Information Technology’을 통해 육군에 RMF를 적용하기 위한 지침을 제공하여 육군의 IT 개발자, 관리자 등이 해당 지침을 준수해야 한다고 명시하였다[14]. 이러한 흐름에 따라 현재 미 국방부는 첨단 무기체계의 소프트웨어 결함이나 사이버보안 위협에 대응하기 위해 무기체계에 RMF를 적용하고 있다. 이처럼 연방정부용 RMF는 관련 문서가 모두 민간 영역에 공개되어 있고, 특히 모든 보안 통제항목의 목록 및 세부 내용 또한 NIST SP 800-53 Rev.5에 상세히 기술되어 있다. 이 외에도 2023년 NIST에서는 AI 시스템을 설계, 개발, 배포, 사용하는 조직을 대상으로 RMF와 관련된 리소스를 제공하여 AI를 통해 발생될 수 있는 다양한 위험을 관리하는데 도움을 주고자 AI RMF에 대한 표준인 “Artificial Intelligence Risk Management Framework (AI RMF 1.0)”을 개발하였다[15]. AI RMF는 AI 기술이 지속적으로 발전함에 따라 이에 적응하고, AI를 통해 사회가 받을 수 있는 잠재적인 피해로부터 보호할 수 있도록 다양한 수준에 따라 조직 운영에서 사용될 수 있도록 개발되었다. 하지만, 무기체계를 개발 및 획득하는데 적용해야 하는 것은 NIST의 연방정부용 RMF가 아닌 DoD에서 관리하는 RMF A&A이다. DoD는 NIST와 달리 RMF A&A에 대한 문서 및 보안 통제항목 등을 민간 영역에 공개하지 않고 있다. DoD 산하기관인 DCSA에서 발행한 평가 및 인가 프로세스 메뉴얼(DAAPM,

DCSA Assessment and Authorization Process Manual)[16]에 극히 일부의 보안 통제항목 baseline만이 제시되어 있다.

Lockheed martin, BAE Systems, Boeing 등 세계 유수의 방위사업체에서는 방위사업 기술에 대한 사이버 공격에 대응하고 RMF를 준용할 수 있도록 위협 모델링 기반의 사이버보안 프레임워크를 독자적으로 개발하여 운영 및 서비스하고 있다. 대표적으로 Lockheed martin이 2020년 'An overview of the Lockheed martin Cyber Resiliency Level(CRL) framework for weapon, mission and training systems'문서를 통해 발표한 CRL Framework가 존재한다. 또한, 연방정부 산하의 비영리기관인 MITRE(The MITRE Corporation, 이하 MITRE)에서는 국방획득체계와 직접 연계될 수 있는 TARA(Threat Assessment and Remediation Analysis, 이하 TARA) 위협 모델링 방법론을 개발하였다[17]. 다음 <표 8>은 세계적인 방위사업체들로부터 개발된 사이버보안 프레임워크를 설명한다.

4. 국내 RMF 동향

K-RMF는 무기체계를 비롯하여 국방 정보체계에 대해 보다 높은 사이버보안 수준을 확보하기 위해서 새롭게 제정 및 시행될 국방 사이버보안 위험관리 제도이다. 2019년 미군에서는 CCIB(Command, Control and Interoperability Board, 지휘통제상호운용성위원회)에서 미군의 지휘통제체계인 CENTRIXS-K와 연동된 한국군의 지휘통제체계에 RMF를 적용할 것을 요구하였다[18]. 하지만 현재 미국과 우리나라는 제도적 기반과 기존 구축되어있는 보안수준이 서로 상이하기 때문에 미국의 DoD RMF A&A를 그대로 도입할 수 없다[19]. 이에 따라 우리나라에서도 국방부가 당시 군사안보지원사령부(현 국군방첩사령부)에 한국현 위험관리 제도 개발 TF를 창설하고 미국의 국방 RMF인 DoD RMF A&A, 연방정부용 RMF인 NIST RMF 등을 참고하여 2020년 K-RMF를 제정하였다. 이어 2021년부터는 일부 무기체계를 대상으로 K-RMF를 시범 적용하고 평가를 진행하며 그 타당성을 검증하고 있다. 또한 국내 방위사업청은 2021년 '방위산업기술보호 종합계획'을 발표하며 미국의 사이버보안 인증제도 바탕의 한국형 기술보호 인증제도를 국내에 도입하여 방산업체의 한국형 기술보호체계 구축과 K-RMF 연계 여부를 검토해야 한다고 명시하고 있다[20]. 이러한 시범 적용 및 평가가 완료되면 오는 2024년부터는 국방부 및 군에서 새롭게 도입하는 모든 무기체계 및 정보체계와 기존 운용중인 주요 지휘통제체계를 대상으로 K-RMF를 전면 적용할 예정이며, 2026년부터는 K-RMF에 대한 전면 적용을 목표로 하고 있다. 하지만 현재 K-RMF와 관련된 자료는 제한적이며, 미국의 국방용 RMF는 외부

〈표 8〉 해외 방위산업체에서 개발된 RMF 기반 사이버보안 프레임워크

방위산업체	설 명
Lockheed martin	- 위험을 식별하고 효과적으로 관리하기 위해 RMF를 기반으로 무기시스템의 사이버 복원력 성숙도를 측정하는 CRL(Cyber Resiliency Level) 프레임워크 개발
BAE Systems	- 무기체계에 대한 정보보호 및 RMF 기능을 수행하는 정보 관리 솔루션인 Epiphany를 개발
Boeing	- RMF를 기반으로 하는 보안 인프라 모니터링 시스템인 SMIS(Security Monitoring Infrastructure System)을 개발
Northrop Grumman	- 사이버 위험관리를 위해 개발 프로세스에 대한 보안성 평가를 수행하는 도구인 Cycape와 FAN을 개발

에 공개되지 않는 기밀자료에 속하는 등의 문제로 인하여 기존 국내에서 수행된 RMF 적용 연구를 실제 무기체계 개발에 적용하는데 한계가 있다. 이러한 한계점을 극복하고 K-RMF 제도를 구축할 수 있도록 국내 무기체계 대상의 RMF 적용 사례 연구를 바탕으로 한 한국형 국방 RMF 구축 방안 연구도 최근 수행되었다[6]. 이와 같이 국외 뿐만 아니라 국내에서도 무기체계에 RMF를 적용하기 위한 움직임을 보이고 있다.

국내 방위산업체인 한화시스템에서는 K-RMF에 대해 대비하기 위하여 “함정 전투체계에 대한 RMF 적용 방안 연구”과제를 통해 NIST RMF 및 DoD RMF A&A를 바탕으로 함정 전투체계를 대상으로 RMF 준비단계부터 구현단계까지에 대한 사례 연구를 진행하였으며, 현재 SRTOS(Secure Real-Time Operationg System)를 대상으로 K-RMF를 준용하기 위한 “보안 실시간 SW 플랫폼 RMF 기반 보안 표준 준용 방안 연구”과제를 수행하고 있다. 또한 국내의 또다른 방위산업체인 LIG Nex1에서도 “무기체계 K-RMF 적용 대응 방안 연구” 과제를 통해 개발되는 무기체계에 대한 위협 식별, 위험 분석, 보안통제항목 선정 등에 대한 기술을 연구하고 적용하는 연구를 수행하고 있다. 이와 같이 국내 방위산업체에서는 K-RMF 준용을 위한 연구를 활발히 수행하고 있으며, 학계에서도 K-RMF에 대비하기위한 연구가 지속적으로 수행되고 있다. 2019년, 조현석 외 2명은 “국내 무기체계에 대한 RMF 적용 실 사례 연구”라는 주제로 당시의 한국형 RMF 연구를 활용하여 최근 개발된 실제 무기체계에 적용하고 RMF를 우리나라 무기체계에 적용할 수 있도록 상세한 가이드라인을 제시한 바가 있다[21]. 2021년, 조광수 외 1명은 “무기체계 개발을 위한 RMF A&A의 실증에 관한 연구”라는 주제로 상세한 정보가 공개되지않아 실제 산업 환경에 적용이 어려운 RMF A&A를 분석하여, RMF A&A의 요구사항을 만족시킬 수 있는 증거자료 작성방안을 제시하였다. 또한 제시한 방안을 실제 드론 시스템에 적용하여 제안된 방안이 RMF A&A의 요구사항에 부합하는지에 대한 검증을 수행하였다[22]. 이후 K-RMF에 대한 전면 적용에 대비하기위해 2023년에 안정근 외 5명은 “무기체계 개발을 위한 한국형 국방 RMF 구축 방안 연구”라는 주제로 우리나라 국방용 RMF인 K-RMF를 예측하여 무기체계의 보안통제항목을 구축하기위한 방안과 이를 함정 전투체계에 적용하여 효용성을 입증하였다[6]. 이처럼 국내의 산업계 및 학계에서는 K-RMF 전면 적용에 대비하기 위해 K-RMF 제정의 기초가 된 RMF A&A와 NIST RMF 바탕의 K-RMF 연구가 활발히 수행되고 있다.

5. 결 론

기존에 독립적으로 운용되던 무기체계가 지휘관의 빠른 결심 및 실시간 전장 상황 공유 등의 목적을 위해 점차 네트워크로 연동되고 있다. 이러한 무기체계의 변화는 전장에서의 이점도 가져다줄 수 있지만, 동시에 사이버 위협에 노출될 가능성 또한 높이고 있다. 무기체계에 대한 사이버 보안 위협에 대응하기 위해 미국은 과거 TCSEC을 시작으로 현대에 이르러서 RMF라는 위험관리 및 평가 체계를 개발하고 적용하고 있다. 본 연구에서는 RMF에 대한 개념과 미 국방성의 RMF 적용 요구에 따른 국내외의 다양한 대응 노력에 대한 사례 조사를 진행하였다. 본 사례 조사를 바탕으로 추후 RMF와 관련한 연구가 더욱 심도있게 수행되고 우리나라의 K-RMF 제도 또한 올바르게 개발되고 안정적으로 정착되어 사이버 위협으로부터 안전한 무기체계를 개발할 수 있을 것으로 기대된다.

참 고 문 헌

[1] 이지섭, 차성용, 백승수, 김승주, “무기체계의 사이버보안 시험평가체계 구축방안 연구”, 한국정보보호학회논문지, 제28권, 제3호, pp.765-774, 2018.

[2] 차성용, “첨단 무기체계 획득 및 운용 시 사이버보안 강화방안 연구”, 고려대학교, 박사학위 논문, 2019.

[3] 권혁진, 김성태, 주예나, “상호운용성을 고려한 RMF 기반의 위험관리체계 적용 방향”, 제22권, 제6호, pp.83-89, 2021.

[4] “Defense counterintelligence and security agency assessment and authorization process manual”, Defense Counterintelligence and Security Agency, 2020.

[5] “The DoD cyber strategy”, Department of Defense, 2015.

[6] 안정근, 조광수, 정지훈, 정한진, 김승주, “무기체계 개발을 위한 한국형 국방 RMF 구축방안 연구”, 한국정보보호학회논문지, 제33권, 제5호, pp.827-846, 2023.

[7] 양우성, 차성용, 윤종성, 권혁주, 유재원, “국방획득체계 적용 한국형 보안위험관리 프레임워크”, 한국정보보호학회논문지, 제32권, 제6호, pp.1183-1192, 2022.

[8] 김하늬, “K-RMF 구축으로, 국내 사이버보안 수준 높인다”, 공학저널, 2023.11.25. 접속,

[9] “NIST Glossary”, NIST, 2023.11.28. 접속, https://csrc.nist.gov/glossary

[10] “risk management framework (RMF)”, NIST Glossary, 2023.11.28. 접속, https://csrc.nist.gov/glossary/term/risk_management_framework

[11] DoD,“DoDI 8510.01 - Risk Management Framework (RMF) for DoD Information Technology (IT)”, 2016

[12] DoD, “DoD Program Manager’s Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle”, 2015

[13] DoD, “The Department of Defense Cyber Strategy”, 2015

[14] Department of the Army. “Risk Management Framework for Army Information Technology”, 2019

[15] Tabassi, Elham. "Artificial Intelligence Risk Management Framework (AI RMF 1.0)." (2023).

[16] DCSA, Defense counterintelligence and security agency assessment and authorization process manual, DCSA, Aug.2020

[17] MITRE,“Threat Assessment and Remediation Analysis(TARA) Overview”, MITRE Corporation, https://www.mitre.org/sites/default/files/2021-11/pr-11-4987-presentation-tara-overview.pdf, 2013

[18] 안병오, “KIDA Brief - 미국의 新(신) C4I 정책과 연계한 연합 C4I체계 발전 방안”, 군사발전연구센터(KIDA), 2021

[19] Woo-sung Yang, Sung-yong Cha, Jong-sung Yoon, Hyeok-joo Kwon and Jae-won Yoo, “Korean security risk management framework for the application of defense acquisition system,” Journal of the korea institute of information security & cryptology, 32(6), pp.1183-1192, Dec. 2022

[20] 방위사업청,“방위산업기술보호 종합계획”, 방위사업청, 2021

[21] 조현석, 차성용, and 김승주. "국내 무기체계에 대한 RMF 적용 실 사례 연구." 정보보호학회논문지 29.6 (2019): 1463-1475.

[22] 조광수, and 김승주. "무기체계 개발을 위한 RMF A&A 의 실증에 관한 연구." 정보보호학회논문지 31.4 (2021): 817-839.

저 자 약 력

조 광 수

이메일 : cks4386@korea.ac.kr

- 2019년 호서대학교 컴퓨터공학과 (학사)
- 2021년 고려대학교 정보보호대학원 정보보호학과 (석사)
- 2021년~현재 고려대학교 정보보호대학원 정보보호학과 (박사과정)
- 관심분야 : 보안공학, RMF, DevSecOps

김 예 준

이메일 : v3locy@korea.ac.kr

- 2019년 순천향대학교 정보보호학과 (학사)
- 2019년~현재 고려대학교 정보보호대학원 정보보호학과 (석박사통합과정)
- 관심분야 : 보안공학, 위협모델링, 보안성 평가/인증, 취약점 분석, 역공학

안 정 근

이메일 : stable_root@korea.ac.kr

- 2014년 육군사관학교 지역연구학과 (학사)
- 2019년~현재 국군방첩사령부
- 2023년~현재 고려대학교 정보보호대학원 정보보호학과 (석사과정)
- 관심분야 : 보안공학, 위험관리, 보안성평가/인증

김 정 현

이메일 : letter@korea.ac.kr

- 2018년 순천향대학교 정보보호학과 (학사)
- 2020년 순천향대학교 정보보호학과 (석사)
- 2020년~현재 고려대학교 정보보호대학원 정보보호학과 (박사과정)
- 관심분야 : 보안공학, 자동차보안, CSMS

곽 지 원

이메일 : jwkwak4031@korea.ac.kr

- 2017년 중앙대학교 전자전기공학부 (학사)
- 2019년 고려대학교 일반대학원 사이버국방학과 (석사)
- 2019년~현재 고려대학교 정보보호대학원 정보보호학과 (박사과정)
- 관심분야 : 보안성분석평가, 정형기법, 고신뢰시스템개발

김 해 나

이메일 : haena0114@korea.ac.kr

- 2021년 서울여자대학교 정보보호학과 (학사)
- 2021년~현재 고려대학교 정보보호대학원 정보보호학과 (석사과정)
- 관심분야 : 제로트러스트, 보안공학, 위협모델링, RMF

백 근 우

이메일 : sinse100@korea.ac.kr

- 2023년 한국항공대학교 소프트웨어학과 (학사)
- 2023년~현재 고려대학교 정보보호대학원 정보보호학과 (석사과정)
- 관심분야 : 블록체인, 보안공학

김 승 주

이메일 : skim71@korea.ac.kr

- 1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)
- 1998년~2004년 한국인터넷진흥원(KISA) 팀장
- 2004년~2011년 성균관대학교 정보통신공학부 부교수
- 2011년~현재 고려대학교 정보보호대학원 정교수
- 2004년~현재 한국정보보호학회 이사
- 2014년~2015년 육군사관학교 초빙교수
- 2016년~2018년 개인정보분쟁조정위원회 위원
- 2017년~현재 고려대학교 국방RMF연구센터(AR*C) 센터장
- 2018년~현재 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
- 2018년~2020년 대통령직속 4차산업혁명위원회 위원
- 2023년~현재 대통력직속 국방혁신위원회 위원
- 2023년~현재 고려대학교 디지털정보처 처장
- 2023년~현재 (사)한국국방혁신기술보안협회 협회장
- 관심분야 : 보안공학, 위협모델링, 보안성 평가/인증, DevSecOps, 암호학, 블록체인