논문 20-45-12-17 The Journal of Korean Institute of Communications and Information Sciences '20-12 Vol.45 No.12
https://doi.org/10.7840/kics.2020.45.12.2132

한국군에 RMF 적용방안 연구

이 용 석◆, 최 정 민°

Research for Application the RMF to the Korean Military

Yongseok Lee◆, Jeong Min Choi°

요 약

연합작전의 기본은 상황 공유이고 이를 위해서는 시스템의 연동과 안전이 보장되어야 한다. 미 국방부는 자국의 정보기술을 보호하기 위하여 사이버보안정책을 수립하고, RMF를 실행하여 안전한 보안체계를 유지하고자 한다. 또한 미군은 연합작전을 수행해야 하는 나라에게 안전한 체계통합을 요구하게 되었고 그 안전성의 기준을 RMF를 통해 검증·확보하고자 한다. 이에 한국도 RMF를 도입 시, 미국에 적용된 RMF를 국내 상황에 맞게 적용하는 것을 고려해야한다. 본 연구는 미국의 RMF 절차와 임무수행 책임자들에 대해 살펴본 후, 이를 바탕으로 한국군의 RMF 적용을 위한 조직과 필요사항들을 구축하기 위한 방안을 제시하였다.

키워드: RMF(위험 관리 프레임워크), RMF 거버넌스, 사이버보안정책, 정보유통체계, 무기체계
Key Words : RMF(Risk Management Framework), RMF Governance, Cyber Security Policy, Information distribution system, Weapon System

ABSTRACT

The basis of the combined operation is situation sharing, and for this, interlocking and safety of the system must be guaranteed. The U.S. Department of Defense intends to establish a cyber security policy to protect its information technology and implement an RMF to maintain a secure security system. Also, the US military has demanded safe system integration from countries that must perform combined operations, and intends to verify and secure the standards of safety through the RMF. Therefore, when introducing RMF, Korea should also consider applying the RMF applied to the United States to suit the domestic situation. This study looked at the RMF procedures and mission officers in the United States, and based on this, suggested a method to build the organization and needs for the RMF application of the ROK military.

Ⅰ. 서 론

미국은 무기체계의 보안 보증을 위해 2010년 RMF(Risk Management Framework)를 개발하였다. RMF는 정보기술을 수반하는 모든 체계의 수명주기(제품 개발, 평가 및 유지관리) 동안 보안위험을 관리하는 미 국방부의 통합보안 관리제도이다. 미 국방부는 국방부지침(DoDI; Department of Defense Instruction) 8510.01에 의해 RMF를 준수하도록 하고 있다.

2019년 전반기 연례 한-미 국방부 지휘통제 상호운용성위원회(CCIB; Command & Control Interoperability Board)에서 RMF를 적용하기 위한 MOU를 체결하고 RMF를 공동으로 작성하였다. 미국

◆ First Author : Ministry of National Defence, lyskms@korea.ac.kr 정회원
° Corresponding Author : Sogang University Graduate School of Public Policy, mingg11@gmail.com, 겸임교수, 정회원
논문번호 : 202008-204-C-RE.R1, Received August 20, 2020; Revised September 28, 2020 Accepted October 6, 2020

은 이에 따라 사이버보안 검증을 수행할 것을 우리나라에 명시적으로 요청하였다. 이러한 요구는 다음과 같은 위협인식에서 출발한 것이다.

현재 운용되는 무기체계의 SW 의존도는 급격히 증가하고 있다. 1960년대 개발된 F-4의 경우 전체의 8%가 SW로 구성되어 있었으나, 2007년에 개발된 F-35의 경우에는 전체의 90%가 SW로 구성되어 있다[1]. 이는 첨단·정밀 기술이 사용되고 있다는 긍정적인 평가와 함께 해킹에 취약하다는 불안 요소를 동시에 내포하고 있다. 그럼에도 불구하고 많은 나라가 연합작전으로 국방을 수행하는 현 상황에서는 국가 간 원활한 작전수행을 지원하기 위해서 정보유통체계를 연동할 수밖에 없다는 것이 현장의 요구이다.

그러나 국가마다 IT 및 보안수준이 동일하지 않고 체계 안전성에 대한 인식도 같지 않다. 그 결과 안전한 자국의 체계와 연동되는 타국 체계의 미흡한 사이버 안전성으로 인하여 자국 체계에 보안취약점이 생길 수도 있다는 우려가 발생하였다.

우리나라는 한미연합방위체제로 한반도를 방위한다. 연합작전을 위해 미국의 무기체계와 연동하려면 우리나라 무기체계의 안전성을 확보하고 검증해야 한다. 그러나 자국의 체계는 자국의 제도를 적용한다는 원칙하에 동등한 상호협의를 통해 검증방안을 도출해야 하는 문제도 발생한다. 이를 위해서는 우리나라가 수행하고 있는 기존의 무기체계 획득절차에 보안평가 제도를 RMF 수준으로 보완하며 양국 간 상호호혜적인 보안검증방안을 모색해야 한다.

기존 연구로는 미국과 국내 무기체계의 사이버보안 시험평가 현황 비교 연구[2]와 RMF 단계를 국내 무기체계에 적용한 사례 연구[3] 정도만 있을 뿐, RMF 국내 적용을 위한 거버넌스 체계와 방안을 모색한 연구는 거의 없다. 따라서 본 연구에서는 안전한 정보유통체계 연동을 위한 미군의 RMF의 발전경과, 대상 체계, 거버넌스, 수행책임과 절차를 살펴보고 한국군에 RMF를 적용하기 위한 방안을 제시하고자 하며, 이를 통해 향후 한국군의 사이버 보안 안전성 확립에 기여하고자 한다.

Ⅱ. RMF 발전경과

1985년 미군은 자국의 정보유통체계에 대한 사이버보안 인증평가 기준인 TCSEC(Trusted Computer System Evaluation Criteria)를 발표하였다. TCSEC는 기밀성, 무결성, 가용성 중 기밀성에 중점을 두고 정보유통체계를 평가했다. 이후 1997년에는 DITSCAP (DoD Information Technology Security Certification and Accreditation Process)로 발전되었다. 그러나 DITSCAP는 제품의 전 수명주기를 평가하기는 하였지만 아직 정보보증이라는 용어는 사용되지 않았다.

2007년에는 DITSCAP의 단점을 보완하여 DIACAP (Defense Information Assurance Certification and Accreditation Process)로 발전되었다. DIACAP는 독립 체계가 아니라 네트워크와 엔터프라이즈를 중심으로 평가하였으며, DoDI 8500.02 표준보안통제항목을 기반으로 하였다[2].

DIACAP의 정보보증 개념을 발전시킨 것이 RMF이다. 현재는 미 국립표준기술원(NIST)에서 국가급 RMF를 총괄하고 있고, 2010년부터 RMF는 미국 행정부에 개념화되기 시작하였다[3]. NIST는 체계연동을 위한 국가적 통제체계가 필요하다는 인식하에 국가급 표준지침을 만들었고, 각 정부기관에 각자의 상황에 맞는 세부지침을 수립하도록 지시하였다.

NIST의 지침에 따라 미 국방부는 2014년 RMF 초안을 작성하여 국방부 각 기관의 의견을 종합하였고, 2017년 7월 28일에 국방부 훈령(DoD Number 8510.01)으로 제시하였다. 해당 훈령은 미 국방 정보기술을 사용하는 모든 정보유통체계에 대하여 전수명주기 동안 사이버보안 위험을 관리하기 위한 통합보안 프레임워크로 기존의 정보보증 인증절차를 대체하기 위하여 작성된 것이다.

Ⅲ. 미군의 RMF

3.1 RMF 대상 체계

미 국방부 ICT의 형태는 개별 HW 및 SW 제품에서부터 독립망, 대규모 컴퓨팅환경, 네트워크에 이르기까지 크기와 복잡성에서 다양성을 내포하고 있다. 미 국방부의 기준에 따라 정보기술제품, 서비스, 플랫폼 정보기술(PIT)은 적용 가능한 국방부 정책과 보안통제를 통해 안전하게 구성되어야 하며, 보안 기능의 결함에 대해서는 특별평가를 받는다. 또한 정보시스템 보안관리자(ISSM : Information System Security Manager)는 미 국방부 기준에 따라 정보체계나 플랫폼 정보기술에 통합되거나 연결되기 전에 모든 제품, 서비스, 플랫폼 정보기술이 적절한 평가와 구성 절차를 완료했는지 확인해야 할 책임이 있다. 구체적으로 평가를 받아야 하는 대상 체계는 다음과 같다.

첫째, ICT 제품을 통해 호스팅 IS 및 PIT 시스템에 취약점이 도입되지 않도록 검증되어야 한다. 둘째, 내부 정보기술서비스를 사용하는 국방부 조직은 국방부

의 보안 요구인 기밀성, 무결성, 가용성에 적합한 서비스를 도입해야 하며, 훈령에 따라 서비스 수준계약서에 사이버 위험관리 분야를 명시적으로 포함하여야 한다. 셋째, 플랫폼 정보기술 도입 시에는 사이버보안 요구사항을 사안별로 평가하여 적절한 보안통제 수단과 절차를 적용하여야 한다.

3.2 RMF 거버넌스

미 국방부의 RMF 거버넌스 구조는 NIST SP 800-39[4]에 기술된 사이버보안 위험관리에 대한 3단계 접근법을 통해 구현된다. 이는 IT 수명주기의 모든 단계에서 RMF 활동을 동기화하고 통합하여 논리적이고 조직적인 실체로 나타난다.

[그림 1]에서 설명하는 바와 같이 RMF의 가장 기초를 이루는 것은 첫째, 3계층의 IS/PIT 시스템이다. 국방부 각 기관의 CIO(Chief Information Officer)와 SISO(Senior Information Security Officer)는 IS/PIT 시스템에 대한 사전교육을 받은 사람들이 수행하게 된다. 그 이유는 수행해야 하는 임무와 보안 문제를 균형 있게 조정하는 권한과 책임을 부여하기 위해서이다. 또 3계층에서 점검되는 사이버보안 프로그램은 시스템연동 수준에서 국방부의 정책, 절차, 활동으로 구체화되며 필요에 따라 1, 2계층의 정책과 지침을 강화하게 된다.

둘째, 2계층은 RMF 임무와 사업절차를 규정하는 단계이다. 국방부 각 기관의 CIO와 SISO는 국방부의 각 임무 영역(전쟁 임무지역, 비즈니스 임무지역, 기업정보환경 임무지역, 정보영역)에서 관리자로서 기능한다. 국방부 각 기관의 CIO는 훈령(8500.01)에 따라 사이버보안 프로그램 내에서 RMF를 관리할 책임을 진다. 특별히 각 기관 SISO는 보안통제평가를 수행할 권한과 책임이 있으며 각 기관 사이버보안 프로그램이 적용되는 정보기술에 대하여 조정된 보안평가 절차를 수립하고 관리한다.

셋째, RMF 거버넌스의 최상위 계층은 전략적 위험과 가장 근접한 계층이다. 이들은 국방부 수준에서 전략적 위험관리를 다룬다. 1계층의 핵심 관리요소는 국방부 정보기술의 사이버보안 위험을 관리·감독하는 것이다. 국방부의 선임정보보안책임자는 훈령(8500.01)에 따라 국방부를 대표하여 RMF의 수립 및 유지보수를 포함하는 국방부 사이버보안 프로그램을 지휘·통제한다. 국방부 사이버보안 아키텍처는 이 계층에서 통합되며 존속 가능한 정보엔터프라이즈를 달성하기 위해 개발된 전략, 표준, 계획으로 구성된다.

시험평가 국방차관보((DASD(DT&E): Deputy Assistant Secretary of Defense for Developmental Test and Evaluation))가 통제하는 RMF TAG(RMF Technical Advisory Group: 기술고문 그룹)는 국방부 각 기관의 사이버보안 프로그램, 국방부 사이버보안 워킹그룹(DSAWG)과의 상호작용을 통해 RMF를 어떻게 구현할 것인지에 대한 지침을 제공한다. 지침 제공은 온라인 지식기반인 KS(Knowledge Service)를 통해 이루어지며, KS는 RMF의 구체적인 구현, 계획, 실행을 지원하도록 작성되어 가장 신뢰할 수 있는 출처가 된다[6].

* WMA: Warfight Mission Area
* BMA: Business Mission Area
* EIEMA: Enterprise Information Environment Mission Area
* DIMA: DoD Portion of Intelligence Mission Area

그림 1. DoD RMF 거버넌스
Fig. 1. DoD RMF Governance[5]

3.3 RMF 시행 책임[5]

미 국방부에서 RMF에 대한 시행 책임은 다음과 같다. 국방부 정보화차관보(DoD CIO: DoD Chief Information Officer) → 국방부 정보체계국장(DISA: Defense Information Systems Agency) → 획득·기술·군수담당 차관(USD(AT&L): Under Secretary of Defense for Acquisition, Technology, and Logistics) → 시험평가국방차관보(DASD(DT&E): Deputy Assistant Secretary of Defense for Developmental Test and Evaluation) → 운용시험평가책임관(DOT&E: Operational Test and Evaluation) → NSA 사령관 겸 중앙안보국장(DIRNSA/CHCSS: Director, National Security Agency/Chief, Central Security Service) → 국방부 부서장 → 합동참모의장 → 미 전략사령관으로 이어진다. 이 업무계통은 정보체계를 연동하고 사이버보안에 대한 위험관리를 책임지는 부서

로 구성되어 있다. 즉 체계연동을 통해 발생할 수 있는 정보유통체계의 취약점을 조기에 식별하여 차단하고 안전한 네크워크를 구성하려는 것이다.

미 국방부 훈령과 지침에 명시된 체계연동 관련 책임자와 임무는 다음과 같다. 첫째, DoD CIO는 각 부서의 RMF가 국방부 지침대로 예하 기관에서 이행되는지 관장하며 미 국방부 IT 사이버 위험관리를 총괄한다. 둘째, DISA는 국방부의 RMF 업무를 총괄하여 통제하는 기관으로서 임무를 수행한다. 또 국방부 각 기관을 업무적으로 지원하기 위하여 교육 자료를 개발, 지원하고 RMF 관리 도구를 개발한다. 셋째, USD(AT&L)는 RMF 절차를 국방획득체계에 통합한다. 넷째, DASD(DT&E)는 국방부 CIO와 USD(AT&L)의 감독 통제 하에 개발시험평가 활동을 통합하고 RMF TAG를 통제한다. 국방부 수준의 RMF TAG는 실무차원에서 RMF 업무를 수행한다. 다섯째, D OT&E는 감독대상인 모든 국방부 ICT의 사이버보안 평가를 위한 운영시험 계획, 실행, 결과를 검토한다. 여섯째, DIRNSA/CHCSS는 승인 결정지원을 위한 위험모델 및 평가도구를 지원한다.

이에 따라 실제 RMF를 수행해야 하는 국방부 각 부서장들의 임무와 역할은 다음과 같다.

① 각 부서의 RMF 관련 항목의 분류가 국방부 IS 및 PIT시스템의 지침에 따라 분류되었는지 확인한다.
② 모든 IS 및 PIT시스템에 프로그램관리자(PM) 또는 시스템관리자(SM)를 임명한다.
③ 훈련을 받고 자격을 갖춘 AO를 서면으로 임명한다.
④ 각 부서의 운영환경 요구를 반영하여 PIT시스템에 대한 지침을 개발한다.
⑤ 해당 부서의 RMF 준수 여부를 확인한다.
⑥ 현재 작동권한(ATO) 또는 임시승인(IATT)된 IS 및 PIT시스템만 운영한다.
⑦ 운영허가 거부(DATO : Denial of Authorization to Operate)와 승인종료일(ATD : Authorization Termination Date)을 시행한다.
⑧ RMF 요원의 훈련과 전문자격증 보유 여부를 확인한다.
⑨ IS 책임자(ISO : Information System Owner)는 IS 및 PIT시스템 사용자대표(UR : User Representative)를 지정한다.
⑩ 해당 부서 CIO(Chief of Information Officer)의 지침 구현 여부를 감독한다.
⑪ RMF TAG에 참여한다.
⑫ 체계연동계약서에 이 지침의 특정 요구사항이 포함되었는지를 확인한다.

3.4 RMF 수행절차

NIST SP 800-37은 RMF 6단계를 설명하고, 사이버보안 상호성 분야에서 국방부의 정책적용과 시행지침에 대한 가이드를 제공한다[7]. [표 1]은 국방부 훈령(8500.01)의 RMF 6단계 절차별로 수행업무를 정리한 것이다. 1단계는 시스템 분류단계(Categorize System)이다. 이 단계는 사이버보안 요구사항을 도출하기 위

표 1. RMF 6단계
Table 1. RMF for IS & PIT System[8]

Step	Contents
Step 1 - Categorize System	- System classification according to CNSSI1253 - Beginning a security plan - Registration system using cyber security program of each agency of the Ministry of National Defense - Assign qualified persons to RMF missions
Step 2 - Select Security Controls	- Common control identification - Select Security Control - Develop a system-level continuous monitoring strategy - Review and approve security plan and continuous monitoring strategy - Overlay and Taylor applied
Step 3 - Implement Security Controls	- Implementation control solution consistent with each agency's cybersecurity architecture - Implementation of security control of solution security plan document
Step 4 - Assess Security Controls	- Evaluation development and security evaluation plan - Security control evaluation - SCA Security Evaluation Report Preparation - Perform initial treatment
Step 5 - Authorize System	- Preparation of POA & M - Submit security approval package (security plan, SAR, POA & M) to AO - AO makes final risk decision - AO Certification Decision
Step 6 - Monitor Security Controls & Feedback	- Determining the impact on system and environmental changes - Evaluation control selected annually - Treatment requiring command - Security plan, SAR, POA & M - Report security status to AO - AO review status report - Implementation system dismantling strategy

해 아군체계에 영향을 미치는 연동되는 정보의 영향도를 평가하여 중요도에 따라 시스템을 분류하는 단계이다. 2단계 보안통제 수단설정(Select Security Controls)은 사이버보안 요구사항을 보안통제항목으로 변환하는 단계이다. 이 단계에서는 조직이 자기 역할과 업무요구사항, 운용환경에 따라 보안통제기준을 선택적으로 적용할 수 있도록 가이드라인을 제공한다. 3단계 보안통제구현(Implement Security Control)은 보안통제항목을 시스템의 기능관점으로 할당하여 구현한다. 사업관리자는 보안통제항목을 지식서비스에 저장된 구현지침을 참고하여 구현하는 단계이다.

4단계 보안통제항목 평가(Assess Security Controls)는 앞 단계에서 선정, 구현된 보안통제항목이 의도대로 올바르게 동작하는지 확인하는 단계이다. 연방기관 정보체계에 보안통제평가 지침을 제공하기 위해 포괄적인 절차와 보안평가 계획의 수립을 위한 기본적인 절차를 명시한다. 5단계 시스템 인가(Authorize System)에서는 보안통제항목 평가 이후 보완사항을 확인하여 시스템의 위험을 판단한다. AO는 시스템의 위험이 용납되는 수준이라고 판단되면, DATO(Denial of Authorization to Test)로 승인결정을 내린다. 6단계는 모니터링(Monitor Security Controls)이다. 시스템인가 후 양산, 유지보수 목적으로 대상체계의 상황을 지속적으로 확인하는 단계이다. 조직이 보안모니터링 절차를 통해 지속적으로 발생하는 보안문제를 최대한 빨리 식별하고 대응할 수 있도록 종합적인 가이드를 제공하는 최종 단계이다.

Ⅳ. 한국군에 RMF 적용 방안

한국 국방부는 우리의 보안수준 향상과 한미 연동체계 전반에 대한 RMF 적용요구에 대비하여 대응계획을 수립하고 있다. 미 전투사령부는 작전능력 향상을 위해 파트너 국가와 함께 상호 연결된 네트워크의 보안을 보장하고 미 국방부는 연결을 승인한다. 우리나라 국방 사이버공간은 악의적 사이버 위협에 대해 더욱 강력한 조치가 필요한 시점으로 파트너 국가와의 연동정책 전반에 대한 평가 및 안전성을 담보할 수 있는가에 대한 평가가 불가피한 상황이다.

현재 한국군과 미군에서 적용되는 국방획득체계 프로세스는 매우 유사하다. 이는 한국이 국방획득체계 프로세스를 구축할 시 미군의 체계를 표준으로 삼아 도입하였기 때문이다. 미군의 RMF는 기존의 국방획득체계 프로세스를 크게 변경하지 않고 RMF 세부 활동을 추가하여 구축한 것으로 평가된다. 그러므로 한국에서 RMF를 적용할 때도 미국 국방획득체계에 적용된 RMF를 우리나라 상황에 맞게 적용하는 것을 고려해 볼 수 있을 것이다[9]. 이를 위해서는 다음과 같은 사항들이 필요하다.

4.1 국방 RMF MKS 체계 구축

한국군이 미군의 RMF를 효율적으로 수행하기 위해서는 모든 RMF 수행자에게 동일한 관점과 지식, 절차를 공유하도록 해주어야 한다. 이를 위해서는 우선적으로 국방 RMF MKS (Military Knowledge Service) 체계를 구축해야 한다. 국방 RMF MKS는 국방부의 RMF 정책과 지침을 제공하기 위한 각종 지식을 전달하는 수단이다. 이는 국방부의 ICT를 보호하기 위한 가장 적절한 방법, 표준, 절차를 제시하고 지금까지 관행적으로 적용되고 있던 절차에 대한 효과성을 확립하고 체계화시키는데 기여할 것이다.

국방 RMF MKS의 구현지침은 진화하는 보안목적 및 위험조건에 관한 가장 최신의 국방부 의도를 반영해야 한다. 국방 RMF MKS가 설치되면 다음과 같은 이점을 제공할 것이다.

A. 한국군에게 RMF를 구현하고 실행하기 위한 지침과 도구를 제공한다.
B. 권위 있는 RMF 지침의 출처와 국방부 RMF정책의 출처 역할을 수행한다.
C. ICT 위험관리 책임이 있는 모든 사람에게 일관성 있는 정보를 제공한다.
D. 보안통제 기준, 개별 보안통제 및 보안통제 구현지침과 평가 절차에 대한 접근이 편리하다.
E. RMF의 자동 및 비자동 구현을 지원한다.

국방 RMF MKS는 도구, 도표, 절차도표, 문서 등의 라이브러리를 호스팅 하여 RMF의 실행을 지원해야 한다. 또한 RMF 사용자 커뮤니티는 습득한 교훈, 모범사례, 사이버보안 뉴스 및 이벤트, 기타 사이버보안 관련 정보 리소스를 개발, 공유 및 게시할 수 있는 공동작업 공간이 될 것이다.

향후 한국의 RMF 조직 내에도 구성될 RMF TAG는 국방 RMF MKS의 기능 구성 및 콘텐츠 관리를 담당하며 MKS 콘텐츠의 엔터프라이즈 부분에 대한 자세한 분석 및 제작을 지원하게 될 것이다.

4.2 조직 구성

앞에서 살펴보았듯 RMF는 무기체계 개발 후 안전을 담보하는 것이 아니다. 무기체계 개발 시부터 최초 요구사항 분석과 설계단계에서의 보안성을 고려하여

개발해야 한다. 또 보안수준은 체계가 수행해야 할 임무의 중요도에 의해서 결정되어야 한다. 따라서 RMF 관련 업무는 평시 작전을 지휘하고 연합작전을 지도하기 위해 한·미 전술지휘통제자동화(C4I)체계를 통합하는 주무부서인 '합참 사이버지휘통신부'가 담당하는 것이 타당하다.

합동참모본부에서 체계연동을 주 임무로 하는 '합참 사이버지휘통신부'가 주가 되어 정보본부, 전력기획부, 사이버작전사령부, 군사안보지원사령부의 체계통합 및 정보보호 업무를 담당하는 인원들로 조직을 구성해야 한다. [그림 2]는 한국군의 RMF를 위한 밑그림 구상과 행정적 지원을 위한 조직이다. 행정지원 조직과 함께 RMF는 절차에 따라 미국 측과 체계 안전성 검증과 통합을 위한 기술적 조치들을 수행할 능력을 확보한 조직으로 구성해야 한다.

해당 실행 조직에 요구되는 인적구성은 수준 높은 컴퓨터 기술 인력으로 미국 측과 연동해야 하기 때문에 언어능력을 갖추는 것이 유리할 것이다. 이러한 인력은 미국 측의 경우처럼 기술 요원으로서 기업과 군을 기술적으로 잘 융합시켜주는 Contractor를 채용하는 것이 바람직할 것이다.

합참 사이버지휘통신부는 미군처럼 합참을 대표하는 CIO이다. 그러므로 [그림 2]와 같이 우리나라 RMF 업무의 대표는 합참 사이버지휘통신부에서 수행하는 것이 바람직할 것이다. 실제로 미국과 체계통합을 위해서는 CCIB의 한국 측 대표자인 합참의 사이버지휘통신부가 미국 측의 카운터 파트가 되는 것이 적합할 것이다.

최고 책임자(Top Contractor)는 RMF 업무를 수행하기 위한 기술적·정책적 조언을 총괄하는 사람으로 장기간 고정적으로 보직되어 업무를 수행할 수 있는 사람으로 지정하는 것이 타당하다. 이 직책은 미 국방부 정보화차관보의 기능과 역할을 수행하도록 한다.

국방부를 대표하는 SISO로서 국방정보본부의 보안암호정책과(DIA CISO)가 참여하여 미 국방부의 NSA국장 겸 중앙안보국장이 수행하는 체계통합의 승인 결정지원과 위협모델 및 평가도구를 개발한다.

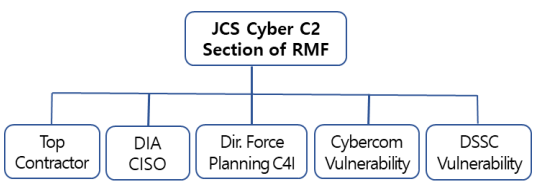


그림 2. 한국군 RMF 수행조직
Fig. 2. ROK RMF Governance

합참 전략본부 전력부 C4I과는 미 국방부의 획득·기술·군수차관이 수행하는 업무를 하며 RMF절차를 국방획득체계와 통합한다.

사이버작전사령부와 군사안보지원사령부의 취약성 평가팀은 미 개발시험평가부차관보가 수행하는 업무를 한다. 즉, 개발시험 단계에서 취약성을 평가하고 RMF에 통합하며 기술고문 그룹을 운용한다. 이와 같이 미국 측의 수행업무 조직과 대응할 수 있는 조직을 구성한 것이 위의 [그림 2]이다.

4.3 RMF 수행을 위한 전문가 양성 및 확보

RMF 6단계 중 시스템 분류, 보안통제 수단설정, 보안통제 구현과 같은 1~3단계가 전 절차에서 95% 정도의 시간과 노력이 소요되는 과정이다. 이를 원활히 수행하기 위해서는 체계와 보안에 대한 전문가가 필요하다.

해당 전문가는 체계개발의 요구사항 분석단계, Design 및 설계단계, 구현을 위한 SW의 Coding 단계, 운용단계까지를 체계개발 시점부터 판단 예측하여 위협요소를 사전에 제거할 수 있는 능력을 갖춰야 한다. 즉, 체계개발도 하면서 Secure Testing도 해낼 수 있는 고급 SW개발자가 필요한 것이다.

고급 SW개발자가 되기 위해서는 보안공학(Information Assurance), SDL(Secure Development Lifecycle), RM(Risk Management), CC(Common Criteria), ISMS(Information Security Management System) 등의 과목을 이수해야 할 필요가 있다. 이를 통해 체계 개발단계에서부터 운용단계까지의 Secure hole을 분석하여 제거하는 능력을 갖추어야 할 것이다. 향후 RMF의 원활한 수행을 위해서는 이상의 분야에 대한 지식을 습득하고 현장을 경험한 인원이 필수적으로 확보되어야 할 것이다.

4.4 RMF 수행을 위한 한미 협력

2019년 8월 미 합동참모본부는 한국 정보유통체계에 RMF를 어떻게 적용시킬 것인가에 대한 논의를 시작하였다. 이 때 주한미군사령부는 원활한 한미 RMF의 적용을 위하여 RMF 전문가를 별도로 고용하여 한국 측과 RMF를 적용하는 문제를 국방부 ICT 포럼, 한·미 C4I Summit, CCIB 등 다양한 채널을 통해 지속적으로 협의하고 있다.

그러나 아직까지 주한미군사령부는 RMF가 미국 측의 규정을 바탕으로 한 절차이므로 한국 측 체계에 동일하게 적용하는 것은 무리가 있다는 판단을 하고 있는 것으로 보여진다. 또한 한국군도 미국의 RMF를

그대로 수용하기보다는 현재까지 한국군이 발전시켜 온 연합체계 연동을 위한 보안성 확보방안을 보다 발전시켜 국가 vs 국가로서 대등한 위치에서 체계통합과 안전성 담보가 이루어져야 한다고 보고 있다. 따라서 현재 연동하고 있는 각종 체계들의 상황을 고려하여 적절한 수준에서 RMF를 적용하는 방안이 검토되어야 할 것이다. 이는 기존 체계와 향후 연동이 필요한 신규 체계들에 대한 동시적인 RMF 수행이 바람직하지만, 주한미군사령부도 RMF를 수행하기 위한 전담 인원이 부족하므로 현실적으로 무리가 따른다는 판단이 있기 때문인 것으로 보인다.

주한미군사령부는 빠른 시일 내에 미 인도태평양사령부에 RMF 적용의 우선순위를 포함한 적용계획을 보고할 것이다. 따라서 향후에도 한국과 미국은 한-미 RMF 실무협의체와 워킹그룹 등 다양한 기구를 통해 관련 정보와 조치사항을 지속적으로 식별해야 할 것이다. 또한 RMF에 관련된 각급 부대들과 협력하여 적극적인 대응방안을 모색해야 할 것이다.

V. 결 론

연합작전의 기본은 상황의 공유이고 이를 위해 시스템의 연동과 안전이 보장되어야 한다는 것은 자명한 사실이다. 이를 위해 한국군의 RMF 적용을 위한 철저한 준비가 필요하다. 따라서 본 연구는 미군의 세부적인 RMF 절차와 임무수행 그룹에 대해 살펴보았으며, 이를 바탕으로 한국군에 RMF 적용을 위해 필요한 조직과 시스템을 제시하였다.

첫째, RMF 정책과 지침을 제공하는 등 각종 정보를 전달하고 접근 가능케 하는 국방 RFM MKS 체계 구축이 우선되어야 한다. 둘째, RMF 거버넌스 구성은 한미 전술지휘통제자동화(C4I)체계를 통합하는 주무부서인 합참 사이버지휘통신부를 중심으로 설계되어야 한다. 셋째, RMF를 수행할 수 있는 무기체계와 보안 전문 지식을 습득한 인력이 양성되어야 하며, 한미간 원활한 RMF 활용을 위한 협력이 지속되어야 할 것이다.

다만 RMF 적용을 위해서는 상대국의 제도, 관습, 그리고 법률의 차이를 인정하고 일방의 강요가 아닌 상호 호혜주의에 따른 협의가 필요할 것이다. 또한 RMF가 전작권 전환의 걸림돌이 되어서는 안 되며 부족한 것은 상호 협의와 협조를 통해 수정보완해 나간다면 국제적으로도 모범 사례를 남기게 될 것이다.

현재까지 식별된 한미 양국의 RMF에 대한 보안검증방안은 다음과 같이 평가된다. 우선 한측이 원하는 보안검증방안은 상대방의 평가결과를 인정하고 필수 검증절차와 범위, 항목을 협의하여 결정하고 이를 공동평가하는 것이다. 그러나 미측이 원하는 방안은 RMF를 적용하여 미측에서 평가 및 승인하고 한측의 평가결과를 미측에서 검증, 승인하는 것이다. 이는 앞선 사이버 능력을 가진 미측의 입장에서는 일견 당연하다고 할 것이다. 그러나 이는 무기체계 보안성검증에 대한 국가적 자존심의 문제이기도 하다.

한미 연합방위체제로 한반도를 방어하는 미국에게 있어서 한측과의 RMF 합의는 매우 중요한 의미를 갖는다. 이는 세계 곳곳에서 연합작전을 수행하는 미국에게도 좋은 경험요소가 될 것이며, 한미 연합작전의 공고화를 달성하는데도 기여할 것이다.

References

[1] S. N. Lee, "SW policy research institute forum, issues and challenges of defense SW for strong security and responsible defense," *Defense weapon system SW development plan*, Sep. 2017.

[2] J. S. Lee, S. Y. Cha, S. S. Baek, and S. J. Kim, "Research for construction cybersecurity test and evaluation of weapon system," *J. The KIISC*, vol. 28, no. 3, 2018.

[3] H. S. Cho, S. Y. Cha, and S. J. Kim, "A case study on the application of RMF to domestic weapon system," *J. The KIISC*, vol. 29, no. 6, 2019.

[4] National Institute of Standards and Technology special publication 800-39, *Managing information security risk: organization, mission, and information system view*, Mar. 2011.

[5] DoD Number 8510.01, DoD CIO, *Department of Defense INSTRUCTION*, Incorporating Change 2, p. 14, Jul. 28, 2017.

[6] https://www.dcsa.mil/About-Us/News/News-Display/Article/2171047/rmf-knowledge-service-site-accessibility-update/

[7] National Institute of Standards and Technology special publication 800-37, *Guide for applying the risk management framework to Federal information systems: A security life cycle approach*, Feb. 2010, as amended.

[8] DoD Instruction 8500.01, *Cybersecurity*, Mar. 14, 2014.

[9] S. J. Kim, *Cyber security test evaluation plan research*, Research result report, pp. 101-107, Dec. 14, 2017.

이 용 석 (Yongseok Lee)

2003년 8월 : 연세대학교 정치학석사

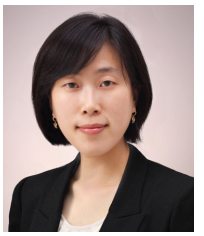
2019년 2월 : 고려대학교 정보보호대학원 공학박사

현재 : 국방부 서기관

<관심분야> 사이버국방/안보, 사이버무기체계, 정보보호, 암호체계 개발

[ORCID:0000-0002-4914-4756]

최 정 민 (Jeong Min Choi)



2000년 2월 : 한국외국어대학교 행정학 학사

2005년 2월 : 서울대학교 행정학 석사

2013년 2월 : 서울대학교 행정학 박사

현재 : 서강대학교 공공정책대학원 겸임교수

<관심분야> 조직, 정보보호, 전자정부, 사이버안보

[ORCID:0000-0002-9166-1829]