J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

상호운용성을 고려한 RMF 기반의 위험관리체계 적용 방향

The direction of application of the RMF-based risk management system considering interoperability

권 혁 진[1] 김 성 태[2*] 주 예 나[3]
Hyuk-Jin Kwon Sung-Tae Kim Ye-na Joo

요 약

RMF(사이버보안 위험관리 프레임워크)는 지금 현재 국방영역을 넘어 미 연방정부 전체에 통용되는 보다 강화된 미 국방 사이버보안 프레임워크이다. 최근 십여년 간 미국이 접한 비정규전에 있어 사이버전이 차지하는 비율, 특히 중국과 북한으로부터 유발된 사이버공격 비중은 점점 더 증대되고 있다. 결국 미국은 범정부 차원의 보다 강화된 사이버보안 정책을 마련하고자 RMF체계를 새롭게 구축중이며, 미 국방부는 연방정부차원을 넘어 동맹국 간에도 미 국방 RMF평가 정책을 확대해 나가고자 한다. 이미 한국군도 F-35A 획득 시 RMF 적용방침을 통보한 미측 요구로 RMF를 적용한 바 있다. 한국군의 RMF적용은 더 이상 피할 수 없는 대세이다. 이제 우리 군은 성공적인 한국형 RMF체계 조기 구축을 위해 무엇을 준비해야 하는지 진지하게 고민해야 할 시점이다.

☞ 주제어 : 사이버보안, 시스템공학, Fuzzy, Secure SDLC, RMF

ABSTRACT

The RMF (Cyber Security Risk Management Framework) is a more strengthened U.S. defense cybersecurity framework that is currently used throughout the U.S. federal government beyond the defense sector. In the past decade, the proportion of cyber warfare in non-regular warfare encountered by the United States, especially cyberattacks caused by China and North Korea, has been increasing. In the end, the U.S. is newly establishing an RMF system to prepare a more strengthened cybersecurity policy at the pan-government level, and the U.S. Department of Defense aims to expand the U.S. defense RMF evaluation policy beyond the federal government level. The South Korean military has already applied RMF at the request of the U.S. that notified the policy to apply RMF when obtaining F-35A. The application of RMF by the Korean military is no longer inevitable. Now is the time for the Korean military to seriously think about what to prepare for the early establishment of a successful Korean RMF system.

☞ keyword : CyberSecurity System engineering, Fuzzy, Secure SDLC, RMF

1. 서 론

4차 산업 이후 전산화가 가속화되어 가며 사이버공간에 대한 의존도는 높아지고 있다. 따라서 향후 전쟁은 군사시설에 대한 직접적인 타격보다는 군사통신, 금융망에 대한 사이버 테러 양상을 나타낼 가능성이 크다.[1]

이에 사이버공간에 대한 우위를 확보하기 위해 미국, 중국, 이스라엘 등 사이버 강국으로 일컬어지는 국가들은 사이버전 역량 확보를 목적으로 공격적인 투자를 이어가고 있는 가운데[2] 탄생한 RMF(Risk Management Framework)는 미 국방부가 2007년부터 적용해오던 DIACAP을 대체하기 위한 차세대 사이버보안프레임워크이다. 2008년 미 국방부 CIO가 발표한 'NetOps Strategic Vision'에는 "네트워크중심전의 첫번째 목표인 전세계적 상황인식 공유를 위해 정보보증활동이 반드시 필요하다." 라고 명시되어 있다. 정보보증이라는 용어는 원래 1998년 발간된 미 정보작전 합동교리(Joint Pub 3-13)에서 최초로 사용되었는데, 민간에서 흔히 사용되어온 IT정보보호 개념과 달리 정보보증은 정보작전(Information Operations)이라는 작전술의 관점, 특히 '사이버전 전투준비태세 확립' 관점에서 접근하였다.

미 국방부는 2007년 연방정보보호관리법(Federal Information

1 Defense Protection and Safety Engineering Department, Seoul National University of Science & Technology, Seoul, 01811, Korea
2 Management Information Systems at School of Business, Seoul National University; Center for Military Analysis and Planning, Korea Institute for Defense Analyses, Seoul, 08826, Korea
3 Graduate School Of Information, Yonsei University, Seoul, 03722, Korea
* Corresponding author (withtea@kida.re.kr)
[Received 10 October 2021, Reviewed 20 October 2021(R2 2 November 2021), Accepted 8 November 2021]

Security Management Act, 이하 FISMA)를 충족하기 위해 DIACAP(DoD Information Assurance Certification and Accreditation Process)을 만들었다. 그 이유로 미 정부에 납품되는 모든 소프트웨어는 FISMA를 준수하도록 되어 있었기 때문에 미 국방부도 예외가 아니었다.

DIACAP의 뒤를 이은 RMF는 현재 미 국방표준을 넘어선 미국의 정부표준으로 이는 미 국방부가 평가 후 인가한 결과가 연방정부 전 영역에 걸쳐 인정됨으로써 상호운용성이 보장됨을 의미한다. 이미 한국군도 F-35A 스텔스 전투기 구매/도입 시, 미측 요구로 RMF를 적용한 바 있으며, RMF는 한국군에게는 매우 생소한 보안체계로 적용과정에 있어 매우 많아 어려움이 있었다고 관련 부대 고위 관계자로부터 직접 전해 들은 바 있다.

하지만 국내 RMF 관련 연구사례는 거의 없으며 대부분 미연방정부 RMF(NIST-800계열지침)에 근거한 일반적인 위험관리프레임워크 소개에 초점을 두고 있다.[3][4]

이에 본 연구는 미국방 RMF만의 차별화된 요소(1단계에서 정보 레벨로 심화된 사이버보안 통제 구현, 4단계에서 능력기반소요기획 (Joint Capabilities Integration and Development System 이하 JCIDS)제도 하 능력평가(Capabilities Based Assessment 이하 CBA)활용한 신뢰할 수 있는 시스템 및 TSN(Trusted Systems and Networks analysis 이하 TSN)에 초점을 두고 기술하였다.

2. RMF기반 위험관리체계

2.1 RMF와 기존 사이버보안 관리기법 간의 차이점

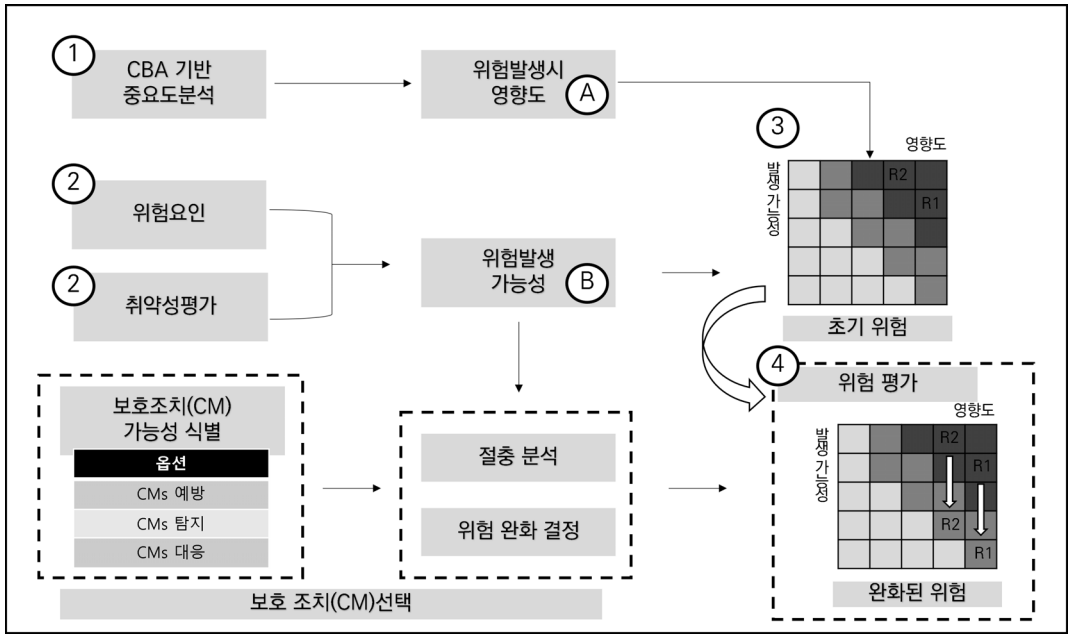
현시점에서는 아직 한국형 RMF 제도가 확립되지 않아 구체적인 한미 국방 사이버위험관리제도에 대한 상호비교 및 분석이 어렵다고 사료된 바 RMF와 기존 사이버보안 관리기법 간의 차이점을 분석함으로써 RMF 기반의 위험관리 체계를 살펴보고자 한다.

RMF는 그림 1과 같이 사이버 위험을 보다 체계적으로 관리 할 수 있는 7단계 프로세스로 기존의 피해가 발생하면 복구를 하는데 중점을 두고 있는 기존의 사이버방어체계[4]와 차별화되는 새로운 관리방법론들을 추가로 접목시켰다.[5]

(그림 1) RMF의 7단계 프로세스
(Figure 1) RMF's 7-Step Process

정보유형	초기 영향수준(보안요구수준) 검토			정보담당자
	기밀성	무결성	가용성	
군사정보	H 높음	H	M	정보공동체
날씨	L 낮음	M	M	기상청
군수	M 보통	H	H	군수조직
인력	L	M	M	인력조직
항공작전명령	H	H	H	임무담당자
…				
시스템 정보	H	H	H	시스템담당자
시스템 분류	**H**	**H**	**H**	…

(그림 2) 정보유형별 보안통제 요소식별 및 영향 수준평가(예시)
(Figure 2) Identification of security control elements by type of information and evaluation of impact level(example)



(그림 3) 잠재된 미래 사이버 위협식별 및 우선순위도출을 위한 TSN 분석절차
(Figure 3) TSN analysis procedure for identifying potential future cyber threats and deriving priorities

RMF란 용어 중 RM이란 두 글자가 '위험관리(Risk Management)'인 것처럼 일반적인 IT사이버보안 관리기법과 달리 RMF는 '위험'이란 용어를 강조하고 있어 무엇보다 '위험'의 개념에 대해 우선 고찰해볼 필요가 있다. 위험관리에 대한 원칙 및 지침을 제공하고 있는 국제표준인 ISO 31000에서 언급된 '위험'의 개념은 '불확실성에 따른 영향(effect of uncertainty)' 이라고 정의되어 있다.

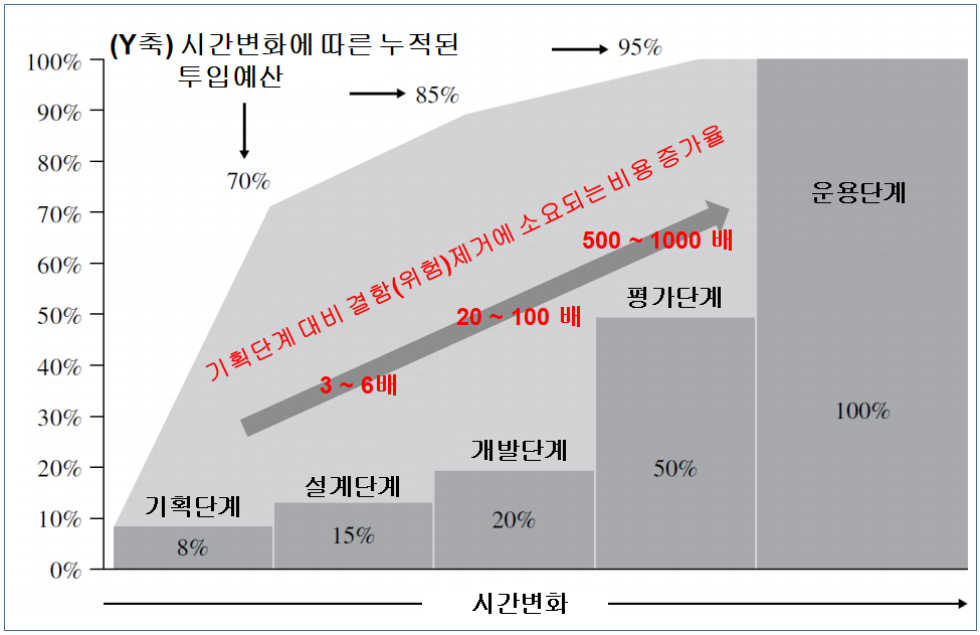
위험의 영향은 긍정적 또는 부정적 영향 모두를 야기할 수 있기 때문에 '위험(Risk) = 유해한 것(Hazard)'으로 간주하는 것은 부적절하다. 따라서 사이버 위험관리는 부정적 리스크의 발생 확률 및 영향을 감소시키거나 긍정적 리스크의 발생 확률 및 영향을 증가시키는 '불확실성의 영향을 체계적으로 관리하는 방안 마련'에 초점을 둘 필요가 있다.

불확실성의 영향을 체계적으로 관리하는 것에 초점을 둔 RMF의 주요 방법론적 특징으로 그림 1의 7단계 프로세스 절차 중 2단계에서 정보 레벨로 심화된 사이버보안 통제 구현, 5단계에서 JCIDS 제도 하 CBA를 활용한 신뢰할 수 있는 시스템 및 TSN 분석방법 적용이 대표적이다.

첫째, 정보 레벨로 심화된 사이버보안 통제 구현은 그림 2와 같이 ①'정보' 단위별로 ②'영향수준을 평가'함으로써 ③'시스템을 분류(대상 시스템의 보안 등급을 산출)'할 수 있다. 구체적인 예로 무인폭격기(UABS)라는 대상 시스템의 보안 등급은 기밀성, 무결성, 가용성이라는 3가지 요소에 대한 영향수준을 평가(각 요소별로 모든 정보유형의 평균값을 도출)함으로 결정된다. 단순히 대상 시스템의 기능 중심에서 보안통제항목을 도출하는 기존방식에 비해 RMF는 대상 시스템의 정보가 유통되는 환경적 측면을 종합적으로 고려함으로써 보다 세분화된 사이버보안 통제를 구현할 수 있다.[3] 실제로, 국내에서 개발중인 잠수함 무기체계를 대상으로 RMF시범과제를 수행한 고려대 김승주교수 연구팀은 "기존 잠수함 무기체계의 보안통제항목은 27개 였으나, RMF방법론을 적용 시 도출된 보안통제항목은 총 171개로 기존에 미반영된 144개의 보안통제항목을 추가로 확보할 수 있었다." 라고 기술하고 있다. 즉, 대상 시스템의 기능만 보고 보안통제항목을 선정하는 것보다 RMF를 적용하여 환경적 측면까지 종합적으로 검토하면 보다 더 세분화된 사이버보안 통제 수준을 구현할 수 있음을 의미한다.

둘째, RMF는 체계적인 사이버위험 우선순위 식별방안으로 TSN 분석기법을 새롭게 채택하고 있다.[7]

RMF에서 TSN 분석기법 활용 관련 주요내용은 주로



(그림 4) 프로젝트 수행단계별 결함(위험)제거에 소요되는 비용
(Figure 4) The cost of eliminating defects(risks) by project execution stage

RMF가이드북 내 '부록 C'파트에 기술되어 있으나, RMF 가이드북은 TSN 분석기법 자체를 자세히 설명하고 있지 않다. RMF가이드북에서는 미획득대학(DAU)에서 발간한 국방획득가이드북(Defense Acquisition Guidebook)을 참고하라고 기술되어 있다. 따라서 TSN 분석기법 자체에 대한 보다 상세한 정보는 국방획득가이드북 외 2014년 미국방부 시스템공학 부차관보실에서 발간한 'Trusted Systems and Networks (TSN) Analysis' 문서에서 확인할 수 있다.

TSN은 원래 미국방 획득가이드북에 수록된 시스템보안공학에 기초한 범용적인 위험분석기법으로 TSN 위험분석절차는 그림 3과 같다.

구체적으로 TSN 분석기법에서는 우선 불활실한 미래를 예측/관리하기 위한 도구로 미군이 새롭게 개발한 CBA방법론에 기초한 중요도분석(①)을 통해 위험 발생 시 영향도(Ⓐ)를 평가한다. 그 다음 위협요인 식별 및 취약점분석(②)을 통해 위험발생 가능성(Ⓑ)을 도출한다.

다음으로 위험발생 가능성(Ⓑ)과 위험발생 시 영향도(Ⓐ)간의 상관관계를 분석하여 기 식별된 위험(R1, R2..) 요소들의 예상 위험수준(초기위험)을 예측(③)한다.

마지막으로 잠재된 위험, 발생된 위험 등 기 식별된 위험요소들의 특성을 고려, 예방, 탐지, 대응 등 보호 조치방안을 도출, 향후 보호 조치방안 적용 시 기존 식별된 위험요소들의 '완화된 위험' 수준을 재산출(④)해 낸다.

TSN분석기법의 가장 핵심은 바로 능력에 기초한 총수명주기 관리체계인 JCIDS체계 하 미래 부족능력 소요도출을 위한 방법론인 CBA이다. 미국방 RMF의 일련의 사이버위험관리 절차는 TSN분석으로부터 시작되며, TSN 분석의 첫 시작은 그림 3에서처럼 CBA분석에 기초한 중요도 분석이다.

사이버보안전문가에 의해 수행되는 위험발생 가능성(Ⓑ) 분석과정과 달리 위험발생 시 영향도(Ⓐ)평가과정에 있어서는 도메인전문가들의 폭넓은 의견수렴이 필요하다. 따라서 특정 임무영역 내에서 사이버보안 위험 종합분석업무를 제대로 수행하기 위해서는 반드시 사이버보안 전문지식 외 해당 임무도메인에 대한 숙련된 전문지식이 함께 뒷받침되어야 하며, 이를 위해 정보통신, 항공, 함정 등 각 임무영역별 RMF전문가 확보가 전제되어야 한다.

2.2 RMF기반 위험관리체계 도입 필요성

미군의 국방 사이버보안체계는 불확실성의 영향을 체계적으로 관리하는 것에 초점을 두고 진화하였다고 볼 수 있는데, 미군은 시스템공학에 기초한 위험관리 개념 도입을 통해 불확실성의 체계적 관리체계를 마련하였다. 이러한 미군의 변화과정은 향후 한국군의 사이버보안체계 미래발전방향과도 부합된다.

미 국방부가 사이버보안분야에 기존 무기체계 획득분야에서 주로 사용되어 온 총수명주기 개념에 기초한 사전예방중심 위험관리 개념을 도입한 근본 배경에는 "최초 소요기획단계 때부터 사이버보안 요구능력을 조기에 식별/통합관리하지 않으면, 초기 설계에 포함되지 못한 사이버보안 요구능력을 구비하기 위해 수명주기 후반에는 훨씬 더 많은 비용을 지불해야 할지도 모른다."는 우려로부터 비롯되었다.

미 국방부에서 발간한 RMF가이드북 '부록 A'에는 "사이버보안은 수명주기 후반에 구축하는 것보다는 최초 설계에 미리 통합하는 것이 보다 비용 효과적이다."라고 기술하고 있다. 또한 '부록 C'에서는 "보안 요구사항이 조기에 통합되지 않으면 수명주기 후반에 상당한 비용이 초래될지도 모른다."라고 기술하고 있다.

미국 등 선진국들은 사이버보안분야에서의 총수명주기(Secure System Development Life-Cycle, 이하 Secure SDLC)개념을 이미 오래전부터 도입하였다. 1983년 미 국방부가 일명 오렌지북이라 불리는 TCSEC(Trusted Computer System Evaluation Criteria)를 통해 Secure SDLC 개념을 도입한 이후로 미국과 다른 강대국들은 수십년간 자국만의 Secure SDLC를 개념을 발전시켜 왔다.

체계적인 SDLC 관리개념은 원래 시스템공학으로부터 출발한다. 사실 시스템공학에 기초한 국방획득관리분야에 있어 최초 소요기획단계 때부터 위험관리의 필요성에 대한 관련 연구는 매우 오래전부터 진행되어온 주제이다.

그림 4와 같이 "최초 소요 기획단계에서 제거되지 못한 결함(위험)이 이후 설계, 개발, 시험평가, 운용단계로 갈수록 결함(위험)을 제거하는 비용이 기하급수적으로 증가한다."는 사실은 이미 오래전부터 알려져 왔기 때문에 크게 놀랄만한 일은 아니다. 그림 4와 같이 프로젝트가 진행됨에 따라 결함(위험)을 제거하는 비용이 기하급수적으로 증가한다는 사실은 1993년 국방획득가이드북에 수록된 이래 계속해서 회자되어져 왔다[8]

이러한 이유로 RMF는 기존 사이버보안개념에 SE(System Engineering)기반한 불확실성의 체계적 위험관리 기법을 접목시킨 사이버보안공학 개념을 채택하고 있다.[9]

미국 등 해외 선진국의 경우, 보다 체계적인 위험관리를 위해 새로운 ICT신기술을 활용, 자동화체계 구축을 통해 비용을 절감하고 새로운 환경변화에 보다 기민하게 대처할 수 있도록 진화해나가고 있는 추세이다. 시스템공학분야의 대표적인 위험관리기법인 위험예측 및 파급효과분석(Failure Mode and Effect Analysis 이하 FMEA)의 경우, 인공지능 Fuzzy기술을 이용한 위험우선순위식별 자동화방안 연구가 매우 폭넓고 다양하게 진행되어져 왔으며, 2016년 Springer에서는 신뢰할 수 있는 관련 연구사례들만을 모아 논문집이 발간되기도 하였다.[10]

이와 유사하게 체계적 위험관리를 위한 RMF 자동화체계 구축은 사이버보안 관련 비용절감 및 사이버보안 수준 향상에 기폭제가 될 수 있으며, RMF 자동화체계 구축은 단순 무기체계 획득 뿐 아니라 정보화된 국방업무 전반에 걸쳐 도입 및 확대가 필요하다.

사이버보안 분야만 유독 선진국에 비해 뒤처져 있을 뿐 한국군도 국방 자원관리 분야에서는 단순 무기체계 획득 뿐 아니라 군수 정비와 같은 운영유지업무에도 오래전부터 체계적인 공학적 관점의 위험관리 개념을 도입, 소요예측(사전예방) 관리체계를 발전시켜 왔다. 일례로 한국국방연구원은 2012년부터 VARI-METRIC이론을 토대로 소요예측을 통해 수리부속 재고수준을 효율적으로 관리하기 위해 다단계 재고모형(Multi-Echelon Inventory Model)을 개발, 발전시켜 오고 있다.[11]

3. 결론 및 정책제언

한국군에게 RMF는 더 이상 피할 수 없는 대세이며, 그와 동시에 한국군의 RMF도입은 한국군의 사이버보안 전투준비태세 수준을 획기적으로 향상시킬 수 있는 매우 좋은 기회이다. RMF는 무기체계 수명주기에 전 단계에 대한 통합적인 사이버보안 관리정책과 운영개념 변화요구에 맞추어 지속적으로 개정 및 보완될 것이 예상되므로.[4] 성공적인 한국형 RMF 조기 구축을 위해서는 다음과 같이 몇 가지 주요 전제조건들이 반드시 선결되어야 한다.

첫째, 한국형 RMF 조기 정착화를 위해서는 관련 법/제도 정비 등 제반여건을 조기에 정비하고 RMF활성화를 주도해나갈 선도기관으로 안보지원사 내 RMF수행 전담조직 신설 및 전문인력 확충이 필요하다.

둘째, RMF기반 사이버보안 위험관리 자동화관리체계

구축을 위해 이미 미군은 미 국방부 주관 eMASS(enterprise Mission Assurance Support Service)라는 RMF자동화지원체계를 구축, 운영중에 있으며, 피평가기관을 위한 다양한 RMF자동화지원 솔루션들을 민간에서 제작, 판매중이다. 체계적인 RMF운영을 위해서는 반드시 한국형 eMASS체계 개발이 필요한데, 이 역시 안보지원사에서 책임지고 한국형 eMASS체계를 조기개발, 운영업무를 주도해나가야 한다.

셋째, 한국형 RMF제도 정립 시, 단순 무기체계 획득뿐 아니라 국방업무 전반에 걸쳐 RMF를 의무적용하기 위한 관련 법/제도 정비가 필요하다. 특히 안보지원사가 주관하는 '방산분야 보안측정'은 RMF기반 보안평가체계로 조기에 전환해야 한다. 그 이유는 민간 방산업체는 군 내부 기관들에 비해 절대적으로 보안에 취약하기 때문이다.

보안취약점은 저수지의 구멍과 같다. 아무리 작은 구멍이라도 방치한다면 구멍은 점점 더 커져 어느 순간 저수지 제방을 무너뜨리게 된다. 비록 방산업체에서 초기 RMF도입 시에는 많은 노력과 수고가 요구되겠지만 장기적으로 미 국방 뿐 아니라 미 연방정부, 향후 동맹국 간에도 통용되는 RMF적용 시 해외 방산수출에 있어 경쟁력 강화에 큰 도움이 되리라 예상한다.

마지막으로 합참 및 각군본부, 예하 각 하위기관별로 정보통신, 항공, 함정 등 임무영역별로 RMF전문가 양성이 필요하다. 앞서 설명한 바와 같이 TSN 분석 등 RMF기반 사이버위험관리는 임무영역에 대한 숙련된 전문지식이 뒷받침되어야 함에 따라 안보지원사 주도 혹은 사이버작전사령부의 추가 업무지원만으로 모든 국방 RMF업무를 전담하는 것은 사실상 불가능하기 때문이다.

참고문헌(Reference)

[1] Ho-Yeon Ryu, Young-Ho Nam, "An Attack Model Based on Software Cruise for Information Warfare", Journal of Internet Computing and Services, Vol. 5, No. 5, pp 49-59, 2004.
http://www.jics.or.kr/digital-library/260

[2] Uihyeon Song, Donghwa Kim, Myung Kil Ahn, "Layered Authoring of Cyber Warfare Training Scenario", Journal of Internet Computing and Services, Vol. 21 No. 1, pp191-pp199, 2020.
https://doi.org/10.7472/jksii.2020.21.1.191

[3] Seungbae Lee, "Implementation Considerations for Program Protection and Cybersecurity in Weapon Acquisition Systems from U.S.", Vol. 1, No. 2, pp 23-36, 2019.

[4] Hyunsuk Cho, Sungyong Cha, Seungjoo Kim, "A Case Study on the Application of RMF to Domestic Weapon System", Korea Institute of Information Security & Cryptology, Vol. 29, No. 6, pp.1463-1475, 2019.
https://doi.org/10.13089/JKIISC.2019.29.6.1463

[5] DoD, "NetOps Strategic Vision", 2018.

[6] Sung-Joong Kim et al, "A Study on the Operation Concept of Cyber Warfare Execution Procedures", Journal of Internet Computing and Services, Vol. 21 No. 2, pp. 73-80, 2020.
https://doi.org/10.7472/jksii.2020.21.2.73

[7] Korea University Security Analysis and Evaluation Laboratory, "Research on how to apply the RMF process of the defense acquisition system for cybersecurity test evaluation," Joint Chiefs of Staff's Test and Evaluation Department Service, 2017.

[8] Stephen Cook, Shaun Wilson, "The case for investment in Systems Engineering in the early stages of Projects and Programs", SETE conference, 2018.
https://www.shoalgroup.com/wp-content/uploads/2018/05/Cook-Wilson-2018-Case-for-early-stage-investment-in-SE-SETE-2018.pdf

[9] DoD, DoD Program Manager's Guiedbook for Integrating the Cybersecurity Risk Management Framework into the System Acquisition Lifecycle, September 2015.

[10] Hu-Chen Liu, FMEA Using Uncertainty Theories and MCDM Methods, Springer, 2016.
https://link.springer.com/book/10.1007/978-981-10-1466-6

[11] Craig C. Sherbrooke, "Vari-metric: Improved Approximations for Multi-indenture, Multi-echelon Availability Models", Operations Research, Vol.34, No.2, 1986.
https://doi.org/10.1287/opre.34.2.311

◐ 저 자 소 개 ◑

권 혁 진(Hyuk-Jin Kwon)
1989년 성균관대학교 산업공학과(공학사)
1991년 성균관대학교 산업공학과(공학석사)
2000년 성균관대학교 산업공학과(공학박사)
1991.3~2021.8 한국국방연구원 책임연구위원
2017.12~2020.12 국방부 정보화기획관
2021.8~현재 서울과학기술대학교 국방방호공학과 교수
관심분야 : 국방정보화 정책, 정보화평가, 사이버보안, 스마트국방, etc.
E-mail : kwonhj@seoultech.ac.kr

김 성 태(Sungtae-Tae Kim)
2003년 인하대학교 컴퓨터공학과(공학사)
2005년 서울대학교 컴퓨터공학과(공학석사)
2005년~현재 한국국방연구원 연구위원
2013년~현재 서울대학교 경영학과 박사과정
관심분야 : 정보화 평가, 성과평가, 데이터사이언스, 정보화전략 및 정책, etc.
E-mail : sungtae.kim@snu.ac.kr

주 예 나(Ye-na Joo)
2021년 전북대학교 정보보호학과(공학사)
2021년~현재 연세대학교 정보대학원 정보보호학과 석사과정
관심분야 : 사이버보안, 소프트웨어공학
E-mail : jooyean03@yonsei.ac.kr