IDAP INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2021, Vol. 4, No. 3, 191-208. https://doi.org/10.37944/jams.v4i3.122

A study on the application of RMF for weapon systems in Korea: weapons and security system integration

Seungmok Lee*

ABSTRACT

With the advent of the Fourth Revolution, military weapon systems are also being advanced. In particular, as the proportion of software embedded in these weapon systems increases, the cyber vulnerabilities of advanced weapon systems also gradually increase. If cutting-edge weapons stop abruptly or malfunction owing to software defects or cyberattacks, they will adversely affect defense security as well as combat power and economic losses. The U.S. DoD is implementing the risk management framework (RMF) to cope with cyber vulnerabilities and threats. RMF is a risk management (RM)-based framework that classifies the cyber vulnerabilities of weapon systems based on data and evaluates them according to confidentiality, integrity, and availability. The application of RMF to the Korean military's weapon-system acquisition procedure is still in its infancy. In this study, we studied the application of the RMF to weapon acquisition processors in the U.S. DoD and suggested that measures of availability, reliability, and safety that can affect weapon performance should be managed with security, and that security systems should be applied to reliability, availability, and maintenance (RAM).

Keywords : acquisition system, cyber risk, risk-management framework (RMF), reliability, availability, maintenance (RAM), safety

* (First Author) Defense Security Support Command, The head of the department of information, lsm000lsm@naver.com, https://orcid.org/0000-0001-6944-541X

Ⅰ. 서론

1.1 상황 인식

최근 인터넷, 통신기술 등의 발달에 따라 네트워크로 사람, 데이터, 사물 등 모든 것이 연결되는 초연결사회(Hyper-Connected Society)[1]가 되었다. 전 세계 인구의 절반이 넘는 40억 명 이상이 인터넷을 사용하고 있다. 지난 2015년 발표한 미 DoD CYBER STRATEGY[2]에서도 "지난 10년 동안 인터넷 사용자들이 20억 명 이상 증가하였다."라고 밝혔다. 초연결사회에 접어들면서 악의적인 침해행위 또한 증가하고 있다. 국정원 국회 정보위 국정감사 업무보고서에도 "올해 국가 공공분야에 대한 사이버 공격 시도가 하루 평균 162만 건이며, 하루 기준 사이버 위협이 2016년의 41만 건과 비교해 약 4배 급증했다"고 밝혔다.[3] 초연결사회에 접어들면서 이런 사이버 위험(Cyber Risk)은 더욱 증가하고 있다(So & Cheung, 2021; Jin, Kim, & Han, 2021).

보안 측면에서 볼 때도 과거 물리적 보안(Physical Security)으로부터 정보 보안(Information Security)의 시대에만 해도 보안이 예측 가능하고(predictable), 통제 가능(controllable)하였다. 그러나 인터넷을 중심으로 초연결사회에서는 예측 불가능(unpredictable)하고 통제 불가능(out of control)한 상황이 되었다. 예측과 통제가 어렵다는 것은 보안에 큰 위협이 된다. 보안의 패러다임을 바꿔야 한다. 사이버상에서 모든 데이터를 보호할 수 없기 때문에 '등급에 맞게 분류하고 보호' 하는 데이터 중심의 보안으로 바뀌어야 한다. 사이버상에 존재하는 수많은 위험을 완벽히 예측하고 통제하는 것은 불가능하다. 따라서 데이터를 등급별로 분류하고 중요성을 고려한 보호의 방향으로 바뀌어야 한다는 것이다. 데이터 침해에 대해 예측・분석・평가를 통해 관리하는 위험관리(RM : Risk Management)의 중요성이 점차 현실로 다가오고 있다(Kumi, Lim, & Lee, 2020; Yoo, 2021).

1.2 위험관리(RM) 관련 이론적 배경

위험관리는 "위험도를 분석, 평가, 통제하는 업무에 대해 관리정책, 절차, 지침 등을 체계적으로 적용하여 보호하는 관리를 말하며, 위험에 대처할 수 있는 적절한 방법이 강구되어야 한다.[4]" "정보 시스템 자산에 피해를 끼칠 수 있는 위협의 영향을 확인, 통제, 제거, 최소화하는 전체압력 과정이며 위험 분석, 위험의 처리에 대한 결정, 보호 대책의 선정 및 구현, 잔여 위험 분석 등을 포함하

1) 일상생활에 정보기술이 깊숙이 들어오면서 모든 사물들이 거미줄처럼 인간과 연결되어 있는 사회(네이버 IT용어사전)
2) DoD. (April 2015). THE DEPARTMENT OF DEFENSE CYBER STRATEGY p. 1
3) 연합뉴스(2020.11.3.) "공공분야 사이버공격 시도 하루 162만 건…2016년의 4배" https://m.yonhapnewstv.co.kr/news/MYH20201104003700038
4) 최상복(2004). 산업안전대사전. 골드기술사.

는 순환적 과정으로 이루어진다" 라고 정의하고 있다.[5] 위험의 대응전략으로는 통상 '회피, 전가, 수용, 완화, 감시, 공유, 활용' 등의 방법이 있으며, 위험요소는 저(Low), 보통(Moderate), 고(High) 또는 5등급 척도로 평가한다. 우리 주위에는 항상 위험이 존재한다. 위험이 우리에게 어떠한 영향을 미치는지 분석하고 평가하여 적절한 방법으로 관리할 때 비로소 상승효과를 기대할 수 있다.

육군군수사령부에서 발간한 종합군수지원 개발 실무서[6]에서는 현재 우리 군이 보유하거나 획득하려는 무기체계 역시 첨단 과학기술의 발달과 함께 고성능화되어 가고 있으며 다음의 특성을 보인다. 첫째, 과거에는 고유한 임무 하나만을 수행하도록 개발되었으나, 현대전에서는 전장 환경의 변화에 부응하여 무기의 기능과 역할이 다양화되고 있다. 둘째, 무기의 사거리, 정확도, 파괴력 등 성능이 획기적으로 향상되고 복잡화되고 있다. 셋째, 고성능 무기체계의 전력화로 획득비용, 운용유지비, 훈련비용 등이 급속히 증대되고 있다. 넷째, 과학기술의 발전 속도와 상반되는 현상으로 무기체계에 사용되는 전자부품들의 단종이 빠르게 진행되고 있다. 다섯째, 무기체계의 획득 및 운용유지 비용이 증가함에 따라 획득하는 무기체계에 대하여 높은 신뢰성이 요구되고 있다. 무기체계에 대한 사이버 위협을 포함하여 다양화, 복잡화, 고성능화, 빠른 단종, 유지비용 증가 등 많은 위험요소가 상존하고 있다(e.g., Choi & Kook, 2014; Jung, Jung, & Kang, 2019).

미 DoD 'CYBER STRATEGY(April 2015)[7]'에서는 '무기체계 사이버보안의 개선과 평가, 조달해야 하는 무기체계의 구체적인 사이버보안 기준 마련, 획득 및 조달정책과 관련 무기체계의 수명주기 전반에 걸친 효과적인 사이버보안"을 강조하면서 '사이버 위협(Cyber Threats)'과 '사이버 위험(Cyber Risk)'에 대한 데이터 보호(SECURE DoD Data), 완화(Mitigation), 억제(Deterrence), 대응(Response) 등의 단어가 자주 인용된다. 이는 첨단화된 미국의 국방 무기체계도 사이버 위협으로부터 완전한 보장(제거)을 받지 못하고 있음을 의미하며, 위험관리(RM)를 통해 체계를 보호해야 함을 보여주는 단적인 예이다.

1.3 위험관리프레임워크(RMF) 개념(선행연구)

RMF는 원래 미 연방에서 공통된 정보보호 프레임워크를 구성하기 위해 만들어졌으며, 정보보호 능력을 향상시키고 위험관리 프로세스를 강화하며 부처 간 상호 호환성을 높이기 위해 만들어졌다. 미 DoD도 이러한 흐름에 맞추어 이전에 사용하던 DIACAP(Defense Information Assurance Certification & Accreditation Process)에서 2008년부터 RMF로 전환하였다. RMF는 국방부지침(Department of Defense Instruction) 8510.01에 따라 체계개발 시부터 의무화하도록 명문화하고 있으며, 이는 시스템 개발수명주기 초기부터 사이버보안 설계 및 통합을 할 수 있도록 하기 위함이다.

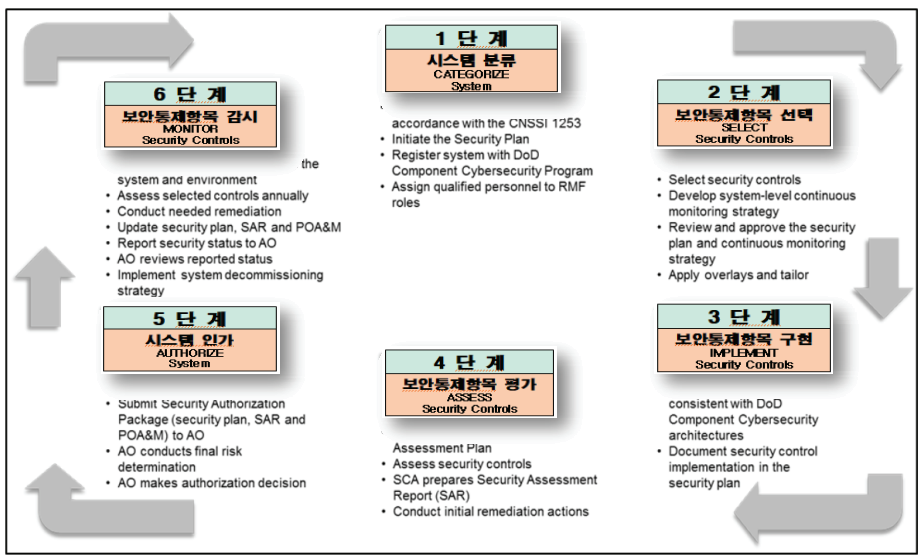
---

5) TTA 정보통신용어사전. 위험 관리.https://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=054578-1

6) 육군군수사령부, 종합군수지원 개발 실무지침서, 2018.1.24. 8쪽

7) DoD. (April 2015). THE DEPARTMENT OF DEFENSE CYBER STRATEGY

RMF는 <Figure 1> 같은 단계로 이루어져 있다.[8)]



<Figure 1> Risk Management Framework (RMF)[9)]

1단계는 시스템 분류(Categorize System) 단계이다. 각 보안 목표별로 영향 값(저, 중, 고)이 할당된 3개의 보안 목표(기밀성, 무결성, 가용성)를 사용하여 분류한다. 이 단계는 아군 무기체계에 영향을 미치는 연동되는 정보의 영향도를 평가하여 중요도에 따라 시스템을 분류하는 단계이다. 2단계 보안통제 항목 선택(Select Security Controls)은 1단계에서 분류한 데이터들에 대해 사이버보안 요구사항을 보안통제 항목으로 변환하는 단계이다. 이 단계에서는 조직이 자기 역할과 업무요구사항, 운용환경에 따라 보안통제 기준을 선택적으로 적용할 수 있도록 가이드라인을 제공한다. 3단계 보안통제구현(Implement Security Controls)은 보안통제 항목을 시스템의 기능관점으로 할당하여 구현한다. 사업관리자는 보안통제항목을 지식서비스에 저장된 구현지침을 참고하여 구현하는 단계이다.

4단계 보안통제 항목 평가(Assess Security Controls)는 앞 단계에서 선정, 구현된 보안통제 항목이 의도대로 올바르게 동작하는지 확인하는 단계이다. 5단계 시스템 인가(Authorize System)에서는 보안통제 항목 평가 이후 보완사항을 확인하여 시스템의 위험을 판단한다. AO는 시스템의 위험이 용납되는 수준이라고 판단되면, DATO(Denial of Authorization to Test)로 승인결정을 내린

8) 차성용(2019). 첨단 무기체계 획득 및 운용 시 사이버보안 강화방안 연구. 고려대학교 박사학위논문, p. 11

9) DoD. (December 29, 2020). Department of Defense INSTRUCTION 8510.01 “SUBJECT: Risk Management Framework(RMF) for DoD Information Technology(IT)”

다. 6단계는 모니터링(Monitor Security Controls)이다. 시스템 인가 후 양산, 유지보수 목적으로 대상 체계의 상황을 지속적으로 확인하는 단계이다. 조직이 보안모니터링 절차를 통해 지속해서 발생하는 보안문제를 최대한 빨리 식별하고 대응할 수 있도록 종합적인 가이드를 제공하는 최종 단계이다.

위험관리프레임워크(RMF)의 목적은 정보보안의 요구사항이 시스템 성능명세에 올바르게 반영되고 반영된 사항이 올바르게 작동되었는지 확인하는 것으로 보안과 관련된 계획을 사이버보안 시험평가(개발시험평가 및 운용시험평가)에 통합하고 운용 시 환경변화에 대해 대응을 하는 것이다.

Ⅱ. 무기체계에 RMF 적용을 위한 현상 진단

2.1 RMF 중요 프로세서 : 데이터의 식별·분류 과정

RMF 1단계(시스템 분류, Categorize System)에서 가장 중요한 과정은 '데이터 분류'라 할 수 있다. 데이터 분류(data classification)[10]는 "정보·통신 데이터 객체의 분류 급수와 사용자의 해제 급수를 비교하여 사용자의 연산 수행 가능 여부를 가리는 방법, 보안 유지를 위하여 사용한다."라고 정의하고 있다. 즉, 등급별로 데이터의 형태(Type)를 분류하고 등급에 맞는 사용자만이 이용해야 한다는 것을 의미한다. RMF를 수행하면서 왜 데이터에 관심을 두고 분류하려 하는지를 파악해 보아야 한다. 왜 우리는 데이터 분류에 관심을 두는가? 그것은 이렇게 해석될 수 있다. 무기체계나 시스템 운용 시 기하급수적으로 많은 데이터가 소통된다. 이 많은 데이터를 전부 보호하겠다고 해보자. 가능한 일인가? 전체 데이터를 보호하겠다는 것은 결국 가장 중요한 데이터를 잃을 수도 있다는 것이다. 따라서 위험관리(RM)의 입장에서 중요한 데이터를 등급화하여 분류하여 최적의 보호를 선택해야 한다는 것이다.

다음은 데이터 분류는 누가 하며, 누구에게 책임이 있느냐는 것이다. 첨단화된 무기체계에 유통(설계)할 데이터를 분류하고 데이터 객체(object)의 중요성에 따라 보안도를 설정하는 것은 IPT팀장, 사업관리자(PM), 보안전문가, 소요군(또는 운용 요원) 등 어느 한 사람의 몫은 아니다. 포병 자주포의 예를 들어 사업 참여(관계)자의 수준을 파악해 보겠다. 자주포에 유통되는 데이터(적 위치, 진지 위치, 방열 제원, 장약, 탄약 제원, 관측소 위치, 기상 등)가 있다고 가정해 보자. 이 데이터에 대해 가장 잘 알고 식별할 수 있는 인원은 소요군(포병 운용요원)일 것이다. 반면, 사업관리자, 보안관계자 등은 데이터의 식별과 중요성 인지면에서는 소요군에 비해 부족하다. 한편, 사업관리자와 보안관계자, 소요군 간에는 데이터 분류에 대해 다른 생각을 가질 것이다. 보안관계자는 데이터 보호에 관심을 둘 것이지만 소요군은 데이터 보호보다는 운용 편의성에 우선할 것이며, 사업관리자는

10) 컴퓨터인터넷 IT용어대사전. https://terms.naver.com

데이터가 무기체계 성능에 어떤 영향을 미치는가에 우선할 것이다.

‘국내 무기체계에 대한 RMF 적용 사례 연구’(Cho, Cha, & Kim, 2019)에서도 “RMF 1단계에서 가장 중요한 것이 무기체계를 구성하는 데이터, 즉 모든 유형의 정보를 파악하는 것이며 그래야 무기체계를 구성하는 모든 정보에 대한 보안 요구사항이 확인되었음을 보장한다.”라고 밝히고 있다. 각 정보의 유형에 대한 임시 영향 값을 부여하고 이해관계자와 전문가의 검토과정을 통해 각 정보 유형의 영향 값을 확정 짓고 최종 무기체계의 보안 분류를 High, Moderate, Low 중 선택한다. 여기서 임시 영향 값이란 식별된 정보가 무기체계를 운용할 때 기밀성, 무결성 및 가용성을 고려하여 영향을 측정한 값이다. 사업관리 측면에서 볼 때 IPT팀장(또는 PM)은 이해관계자(Stakeholder)[11] 간에 이해충돌이 생기지 않도록 지속해서 의사소통하고 이슈 발생 시 적극적으로 해결하는 등 참여자들을 적절히 관리해야 한다. 데이터 분류에 참여하는 사람들은 모두 ‘이해관계자’들이다. 사업관리자와 보안관계자, 소요군 간에는 앞에서 설명했듯이 데이터 분류에 대해 다른 생각을 가진다. 이렇듯 RMF의 첫 단계인 데이터 분류는 사업에 참여하는 모든 ‘이해관계자’들의 합의를 도출해야 하는 매우 중요한 단계라 할 수 있다.

2.2 무기체계 획득절차와 RMF의 관계

한국형 RMF를 연구하기 위해서는 우선 미국의 획득시스템에 RMF가 어떻게 적용되고 있는지를 파악해야 한다. <Figure 2>는 ‘Alignment of RMF and Acquisition System Activities(RMF와 획득시스템 활동의 설정)’을 보여주는 세부 도표이다. 세부 수행절차는 아래와 같다.[12]

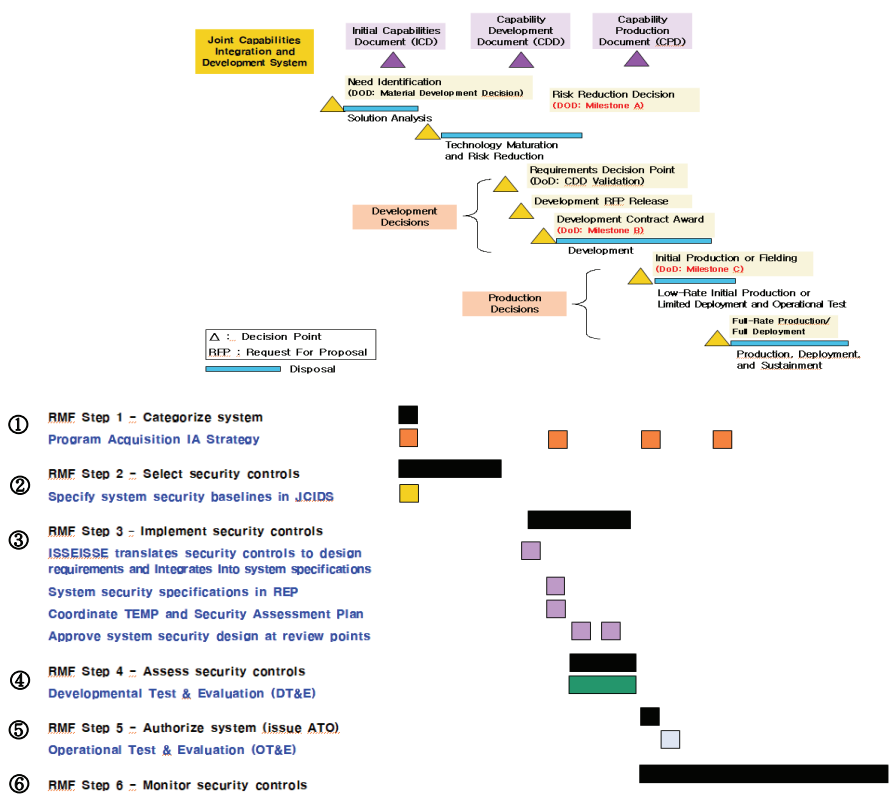
①	ICD(Initial Capabilities Document, 초기능력문서) 즉, 운용요구사항과 능력의 개념을 구체화하여 개발을 결정하는 단계(한국군의 획득체계로 판단해 볼 때 ROC, ORD, 선행연구단계)에 RMF 1단계(시스템 분류, Categorize System)를 시행하며 데이터(정보)를 분류하고 식별한다.
②	마일스톤[13] A에서 마일스톤 B의 사이로써 기술성숙과 위험을 감소시키는 기술개발 단계(한국군의 탐색개발 단계)에 RMF 2단계(보안통제항목 선택, Select Security Controls)를 시행하며, JCIDS(합동능력 통합개발 시스템) 내에서 보안시스템의 기준선(Baselines)을 확인한다.
③	마일스톤 B에서 마일스톤 C의 사이로써 무기체계 개발이 결정된 후 CDD(Capability Development Document, 능력개발문서)와 CPD(Capability Production Document, 능력생산문서)가 만들어 져 개발이 시행되는 단계(한국군의 체계개발 단계)에 RMF 3단계(보안통제 항목 구현, Implement Security Controls)를 시행하며, 보안통제 항목을 디자인하고 시스템 사양에 맞게 통합하며 TEMP(시험평가기본계획)와 보안 평가계획을 조화시킨다.
④	DT&E(Development Test & Evaluation, 개발시험평가) 단계(한국군 동일)에 RMF 4단계(보

11) 기업・행정・NPO 등과 관련하여 직접・간접적으로 이해관계를 가지는 사람(위키 백과사전) 오늘날에는 “영향을 받는 사람”이라는 뜻으로 사용되고 프로젝트의 내용에 따라 여러 Stakeholder가 존재한다 (https://happymemoryies.tistory.com/18).

12) DoD. (December 29, 2020). Department of Defense INSTRUCTION 8510.01 “SUBJECT: Risk Management Framework (RMF) for DoD Information Technology(IT)”

	안통제 항목 평가, Assess Security Controls)를 시행하며, 무기체계의 시험평가와 병행하여 설계된 보안통제 항목도 함께 평가한다.
⑤	마일스톤 C 이후 무기가 저율(Low-Rate) 초도생산(Initial Production)이 되고 제한된 개발 및 운용시험평가 단계(한국군 생산 및 배치 단계/야전시험평가)에 RMF 5단계(시스템 인가, Authorize System)를 시행하여 보안시스템을 최종 검증한다.
⑥	Low-Rate Initial Production(저율생산)에서 야전 배치 후 운용유지, 폐기 단계(한국군의 배치 후 운용유지단계 동일) 시 RMF 6단계(모니터링, Monitor Security Controls)를 시행한다.

<Figure 2>와 같이 미국의 획득단계별 RMF에 적용하는 활동을 분석해 보았다. 현재 한국군은 RMF에 대해 시작하는 단계이다. 우리 군에서는 보안시스템이 무기체계에 통합되는 과정에서 관계자들의 이해관계 설정, 통합과 협업에 대한 구체적인 프레임이 부족하다. 미국 RMF에 대한 심화 연구를 통해 한국군만의 특화된 RMF 구현이 필요한 시점이다.



<Figure 2> Alignment of RMF and Acquisition System Activities

13) 획득절차에서 결정(심)이 이뤄지는 중요한 단계로 이정표 또는 분기점을 의미. 한국군의 획득시스템에서 마일스톤 A는 선행연구에서 탐색개발로 전환되는 단계, 마일스톤 B는 탐색개발에서 체계개발로 전환되는 단계, 마일스톤 C는 체계개발에서 전력화되는 단계로 보면 된다.

2.3 보안시스템이 무기체계 성능에 미치는 영향

획득할 무기체계에 보안시스템을 장착하는 경우 운용자와 다수의 사업 참여자 간에 많은 이해충돌이 생긴다. 무기체계의 가용성, 신뢰성, 안전성이 확보되면서 안정적인 보안시스템을 유지하기는 어렵다. 따라서 안정적인 보안시스템이 장착된 신뢰할 수 있는 무기체계(Trustworthy System)를 만들어 내기 위해서는 모든 사업 참여자들의 완벽한 조화가 요구된다. 여기서 잠시 'Trustworthy System'에 대해서 알아보겠다. 미국표준기술연구소(NIST, 2001)에서는 'Trustworthy System'에 대해 "Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures."이다. 즉, "(1) 침입과 오남용으로부터 합리적으로 보호하고 (2) 가용성, 신뢰성 및 올바른 작동을 합리적으로 제공하고 (3) 의도한 기능을 수행하는 데 합리적으로 적합하며 (4) 허용되는 보안 절차를 준수한다."라고 정의한다.[14] 신뢰할 수 있는 첨단화된 무기체계를 획득하기 위해서는 보안성(Security), 가용성(availability),[15] 신뢰성(Reliability),[16] 안전성(Safety)[17]이 적절히 조화를 이뤄야 한다. 첨단화되고 고도화된 무기체계를 위해서는 당연히 보안의 문제가 중요한 요소이다. 그러나 과도한 보안으로 인해 의도하지 않게 무기체계 성능이 저하된다면 많은 예산을 들여 획득한 무기체계가 성능 발휘도 못 한 채 무용지물이 될 것이다. 따라서, 무기체계의 성능을 보장하면서도 목표하는 수준의 보안을 충족하기 위한 이해관계자들의 합리적이고 올바른 위험관리(RM) 평가 및 토의과정이 필요하다.

예를 들어, 저자의 관련 경험(OO과장 근무)을 토대로 '문서중앙화 사업'을 시행하면서 신뢰할 수 있는 시스템 구현을 위해 위험관리(RM) 적용한 사례는 다음과 같다.

당시 OOO에서 최초 적용하는 '문서중앙화'에 대해 사업에 참여한 많은 관계자들은 시도해 보지 않은 길에 대한 걱정과 시스템 구현 전・중・후 발생할 수 있는 버그(bug)에 대한 두려움이 있었다. 그중 가장 이슈가 되었던 것은 사용자(User)가 '중앙화 접속 실패 시?' 어떻게 할 것이냐는 문제였다. 접속이 안 되어도 즉각 임무 수행이 되도록 '가상 드라이브(Z Drive)'를 구축하자는 결론을 내렸다. 가상의 드라이브를 만들어 줄 경우 자료의 중앙화에서 벗어나는 예외 조건이 생겨 보안능력[18]이 떨어질 수 있었고 떨어진 보안능력을 높여주기 위해 로그 계정의 방법을 새롭게 변경하였다. 즉, 이해관계자들의 지속적인 협의 과정을 통해 'Trustworthy System'을 구현할 수 있었다.

---

14) NIST(2001) SP 800-32 under Trustworthy System

15) the probability of an item to perform a required function under stated conditions for a specified period of time.(명시된 조건 하에서 일정한 기간 동안 필요한 기능을 수행할 수 있는 항목의 확률), DOD GUIDE(AUGUST 3, 2005)

16) a measure of the degree to which an item is in an operable state and can be committed at the start of a mission when the mission is called for at an unknown (random) point in time (랜덤 시점에서 임무가 호출될 때 임무 시작 시 수행될 수 있는 항목의 작동 가능한 정도를 측정하는 것), DOD GUIDE(AUGUST 3, 2005).

17) 자재의 손상이나 손실, 인간의 사상과 관련되는 상태가 존재하지 않는 것.(네이버 컴퓨터인터넷IT용어대사전)

2.4 예측·통제 가능한 보안시스템 구현

2019년 국방과학연구소의 연구보고서에 의하면, 최근 도입된 공군의 F-35 소프트웨어 비중은 전체 80%를 차지한다. 이처럼 첨단무기체계의 개발 비용 중 소프트웨어가 차지하는 비중이 점점 증가하고 있다. 또한, 2017년 미 공군 수명주기 관리센터의 발표자료 '무장 시스템에서의 사이버보안 위험 관리'에서는 2006년 개발된 F-35 라이트닝Ⅱ의 작전 소프트웨어 소스코드 라인이 6,800 개로 2012년 개발된 동일 기체는 작전·지원 소프트웨어의 소스코드 라인이 2만4000개를 돌파했다고 명시했다. 즉 첨단무기체계도 자율주행 차량처럼 하나의 무장 디바이스(Weapon Device)로 생각할 수 있다. 이에 따라 해킹 같은 사이버 공격에 취약할 수 있다고 짐작할 수 있다. 고가의 최첨단 무기체계가 소프트웨어 결함이나 사이버 공격으로 인해 기능 중단·정지, 오작동 등이 발생한다면 전투력 저하뿐만 아니라 경제적 손실로 국방안보에 악영향을 줄 수 있다.[19]

현재의 첨단화되고 고도화된 무기체계일수록 소프트웨어의 비중이 커지면서 보안시스템의 복잡도도 증가하고 있다. 시스템이 복잡해진다는 것은 고장과 정비 소요가 증가하는 것을 의미한다. RMF를 무기체계에 적용할 경우 보안시스템의 복잡도는 결국 무기체계 'RAM'[20]에 많은 영향을 줄 것이다. RAM의 목푯값에 영향을 주는 변수가 대부분 고장(Failure), 정비(Maintenance), 수리(Repair) 등에 의해 결정된다. 따라서 복잡한 보안시스템으로 인해 고장과 정비소요가 발생한다면 무기체계는 결국 RAM의 목푯값이 저하되는 결과를 초래하게 된다. 반면, 소프트웨어(보안시스템)에 대한 신뢰도에 대해서는 아래와 같이 정의하고 있다. "대부분의 하드웨어 불량은 부품 또는 재료 불량의 결과로 시스템의 의도된 기능을 하지 못하는 것이다. 하드웨어 부품을 수리 또는 교체하는 것으로 시스템의 고장 이전 상태로 돌아가게 한다. 그러나 소프트웨어는 하드웨어가 고장 나는 방식으로 고장 나지 않는다. 대신, 소프트웨어 불량은 예측하지 못했던 소프트웨어 작동의 결과이다. 심지어 상대적으로 작은 소프트웨어 프로그램도 천문학적인 수의 입력 및 상태 조합이 가능하다. 소프트웨어를 초기 상태로 돌려놓아도 똑같은 입력과 상태를 만나면 똑같은 의도하지 않은 결과를 불러온다. 소프트웨어 신뢰성 공학은 이를 반드시 고려해야 한다."라고 말하고 있다.[21] 소프트웨어는 RAM의 중요한 변수인 MTBF(Mean Time Between Failure, 고장 간 평균시간) 등을 적용하기 어렵다는 것이다. 그러나 무기체계 일부로서 보안시스템(소프트웨어)은 당연시 예측할 수 있고 통제가 가능한 상태가 되어야 한다. 즉, RAM의 목푯값 설정에 종속되는 요소가 되어야 한다는

18) Security Capability, 정보의 침해로부터 시스템을 보호하기 위해 사용되는 각종 대책 및 솔루션

19) 국방일보(2020. 8.28.). SW 비중 높아진 첨단무기, 사이버 공격에 대비하라... 미 국방부 사이버 보안 시스템 적용. https://m.blog.naver.com/mc341/222078092809; https://bemil.chosun.com/nbrd/bbs/view.html?b_bbs_id=10002&num=13443

20) RAM은 신뢰도(Reliability), 가용도(Availability), 정비도(Maintainability)로 구성되며, 신뢰도는 주어진 조건하에서 고장 없이 수행할 확률, 가용도는 무기체계의 운용 준비태세 및 임무가 요구된 기간 동안 운용 가능 정도, 정비도란 주어진 조건 및 시간 동안에 군수품을 정비하여 그 성능을 규정된 상태로 원상복구 할 수 있는 확률이다.

21) 위키백과. 신뢰성 공학. https://ko.wikipedia.org/wiki/%EC%8B%A0%EB%A2%B0%EC%84%B1_%EA%B3%B5%ED%95%99

것이다. 그런 상태가 되지 않는다면 무기체계에 심대한 영향을 끼쳐 '신뢰할 수 없는 무기체계'가 될 수 있다. 반드시 예측과 통제를 할 수 있는 보안시스템의 설계가 전제되어야 한다.

Ⅲ. 무기체계 & 보안시스템 통합을 위한 제언

3.1 데이터 분류 방법 구체화 및 이해관계자들의 소통 강화

RMF 구현의 첫 번째 핵심적인 요소는 모든 사업 참여자들을 이해관계자(Stakeholder)로 설정하여 최적의 수준으로 데이터의 분류하는 과정을 거쳐야 한다. 데이터가 명확하고 적정한 등급으로 분류가 된다면 보안요구사항이 명확해지고 보안통제항목 구현을 통한 최상의 보안시스템이 갖춰질 것이다. 앞에서 제시한 포병 자주포 일부 데이터(기상제원, 적 위치)로 <Figure 3>과 같이 등급을 분류해 보았다. 각 이해관계자가 5점 척도에 의해 데이터에 임의값을 부여하고 제시한 임의값의 평균을 3단계(0~1.7:L, 1.7~3.4:M, 3.4~5:H)로 분류하였다.

Type		Confidentiality	Integrity	Availability
Weather information	Stakeholder 1	1 2 **3** 4 5	1 2 **3** 4 5	1 **2** 3 4 5
	Stakeholder 2	1 2 3 **4** 5	1 2 **3** 4 5	**1** 2 3 4 5
	Stakeholder 3	1 **2** 3 4 5	1 2 3 **4** 5	1 **2** 3 4 5
	Stakeholder 4	1 2 3 4 **5**	1 2 3 4 **5**	**1** 2 3 4 5
	Stakeholder 5	1 **2** 3 4 5	1 2 3 **4** 5	1 **2** 3 4 5
Average		3.2(M)	3.8(H)	1.6(L)

Type		Confidentiality	Integrity	Availability
The enemy's position	Stakeholder 1	1 2 3 4 **5**	1 2 3 **4** 5	1 2 3 4 **5**
	Stakeholder 2	1 2 3 **4** 5	1 2 3 **4** 5	1 2 3 **4** 5
	Stakeholder 3	1 2 3 **4** 5	1 2 3 **4** 5	1 2 3 4 **5**
	Stakeholder 4	1 2 3 4 **5**	1 2 3 4 **5**	1 2 3 **4** 5
	Stakeholder 5	1 2 3 4 **5**	1 2 3 **4** 5	1 2 3 4 **5**
Average		4.6(H)	4.2(H)	4.6(H)

<Figure 3> Method of assigning security ratings by classification of artillery self-propelled artillery data (Example)

RMF 1단계의 데이터를 식별하고 잠재적 영향도에 따라 보안등급을 분류하는 동안 사업에 참여한 이해관계자들은 수시 소통과 이해를 통해 각 정보 유형의 영향 값을 최종 확정 짓는다. <Figure 4>는 각 이해관계자의 합의를 통해 도출된 데이터별 영향 평가 결과이다. IPT팀장(또는 PM)은 각 이해관계자가 데이터의 영향 값을 부여할 때 절대 통제해서는 안 된다. 각 이해관계자의 임시 영향 값에 영향을 주지 않도록 주의해야 한다. 필요하다면 자유로운 소통과 이해 협력을 위한 '비상설 TF구성'도 필요하다고 판단된다.

Type of information	Temporary impact value		
	Confidentiality	Integrity	Availability
Weather information	M	H	L
The enemy's position	H	H	H
⋮	⋮	⋮	⋮

<Figure 4> RMF Step 1 Evaluation of the Impact of Classified Data

3.2 신뢰할 수 있는 무기체계를 위해 요소들의 최적화

2016년부터 전력화되는 사단급 UAV에 암호장비가 미부착된 것과 관련 일부 언론매체에서 지적한 바 있다.[22] 처음부터 암호장비 부착을 염두에 두지 않고 개발했다는 것이다. 이 경우에서와같이 전력화 이후 암호장비를 장착할 경우 많은 문제가 발생할 수 있다. UAV에 암호장비를 설치할 공간 부족, 암호장비의 무게로 인해 비행거리 및 시간 감소, 안전성 미검증 등 많은 제약이 수반된다. 암호장비를 무기체계에 장착한다는 것은 단순한 것이 아니다. 암호장비로 인해 무기체계의 가용성, 신뢰성, 안정성에 문제가 생기게 되는 것이다. 언론에서 언급했듯이 보안장치 설치공간 부족, UAV 무게 증가 등의 영향을 받아 암호장비가 아닌 소프트웨어로 보안문제를 해결해야 하는 상황이 된 것이다.

무기체계에 보안시스템을 통합(장착)하는 과정에서 사업 참여자들은 모두가 충족할 만한 결과물을 도출하기 위해 전 단계에 걸쳐 RMF 1단계 때 보다 더 많은 소통과 이해 노력이 요구된다. IPT 팀장(또는 PM)은 이해충돌이 생기지 않도록 보안성(Security), 가용성(Availability), 신뢰성

22) 이데일리(2015.11.11.). 軍, 암호장비 없는 사단급 무인정찰기 내년부터 전력화. https://www.edaily.co.kr/news/read?newsId=03739206609564736&mediaCodeNo=257

(Reliability), 안전성(Safety) 척도가 균형감 있게 척도별 가중치를 부여하고 끊임없는 협의가 이뤄져야 한다. 보안성, 가용성, 신뢰성, 안정성은 각자 독립적인 요소가 아닌 상호 의존적인 관계이다. 보안을 중요시하다 보면 가용성, 신뢰성, 안전성이 저하될 가능성이 크다. 보안시스템의 장착으로 무기체계가 정상 작동되지 않는다면 무용지물이 될 것이다. 따라서 사업에 참여한 모두가 위험관리(RM)의 책임자라는 인식을 하고 신뢰할 수 있는 시스템(Trustworthy System)을 설계해 내는 숙고의 협의를 지속 시행하여야 한다. 무기체계를 개발하는 동안 보안능력에 따른 타 척도(가용성, 신뢰성, 안전성)와의 영향을 수시 모니터링하고 필요에 따라 AOA(Analysis of Alternatives, 대체방안분석)[23]를 통해 성능개선을 시켜야 한다. 일정 수준의 보안을 유지하면서도 가용성, 신뢰성, 안전성을 유지할 수 있는 대체 기술을 반영하여 최적의 무기를 만들어야 한다.

3.3 무기체계 RAM에 적용받는 보안시스템 설계

사업관리자는 보안시스템이 무기체계에 통합(장착)시 반드시 RAM에 영향을 받도록 설계하여야 한다. 보안시스템이 무기체계의 중요한 요소로써 운용이 되려면 반드시 선행되어야 하는 문제이다. 앞에서 언급했듯이 보안시스템이 예측할 수 있고 통제 가능한 상태가 되기 위해서는 보안 내재화(Security by design)[24] 또는 임베디드 시스템(embedded system)[25]이 되어야 한다. 외부 침해로부터 보호를 받고 신뢰할 수 있는 보안시스템 구축을 위해서는 무기체계의 한 부분(Units)으로 운용되면서 예측과 통제가 되는 최상의 상태가 지속 유지되어야 한다.

예측과 통제가 된다는 것은 보안시스템의 고장이 발견되어도 즉시 정비를 통한 복원이 가능하고, 고장이 나지 않더라도 고장 전 예측 정비가 가능하다는 것이다. 즉, 상태기반정비(CBM: Condition Based Maintenance) 체계가 가능하다는 것이다. 국방전력업무훈령에서는 “무기체계에 내장된 각종 센서 또는 계측장비를 통해 얻은 데이터를 활용하여 실시간 상대평가를 통해 필요에 근거한 정비를 수행하며, 데이터와 프로세서, 기술 및 지식기반 능력의 통합적 적용을 통해 결함을 사전 진단하고 예측하여 최적의 정비 시점을 결정하는 정비절차 또는 능력:을 의미한다.[26] 이처럼 무기체계 내 부품의 고장을 예측하고 사전 정비를 통해 최상의 상태를 유지할 수 있다. 그러나 보안시스템이 예측할 수 없고 통제할 수 없다면 최상의 능력을 갖춘 무기체계 유지가 어렵게 되는 것이다.

---

23) 초기 능력 문서(ICD)에서 식별해야 하는 확립된 능력을 충족하는 대안 재료 솔루션의 운영 효과, 적합성 및 라이프사이클 비용을 분석적으로 비교하는 것(https://acqnotes.com/acqnote/acquisitions/analysis-of-alternatives)

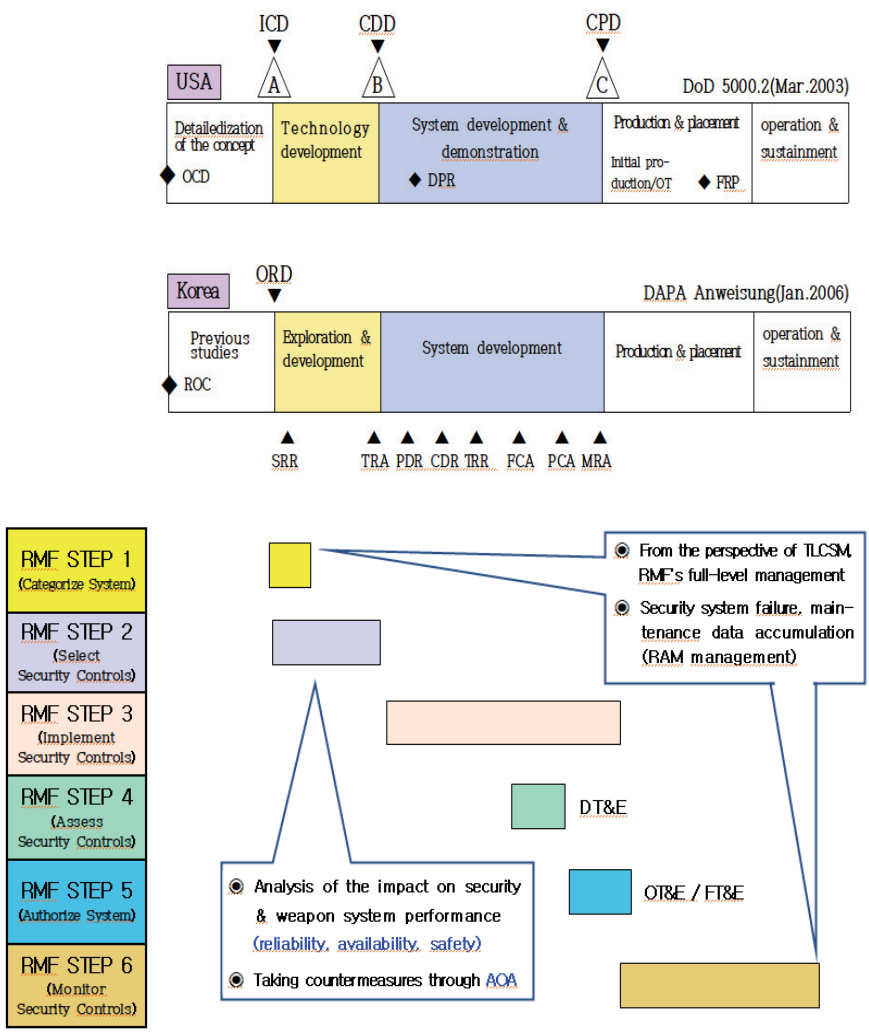
24) 처음부터 시스템에 내장되어 강력한 아키텍처 설계(Wikipedia, https://ko.wikipedia.org)

25) 기계 또는 전자 시스템 내에서 전용 기능을 가지고 있는 컴퓨터 시스템(Wikipedia)

26) 국방전력발전업무훈령(2021. 4. 6.) 별표 1 용어의 정의

Ⅳ. 국내 무기체계 획득절차에 한국형 RMF 적용방안

한국군과 미군의 무기체계 획득절차 비교[27]를 통해 한국형 RMF 단계별 적용 시점을 <Figure 5>와 같이 제시하였다. 앞서 제시했던 미군의 무기체계 획득절차의 RMF적용 방안을 참조하여 우리 실정에 맞게 구상해 보았다.



<Figure 5> Weapon system acquisition procedure & RMF application timing

27) 시스템체계공학원(주).(2011), 효율적인 무기체계 연구개발을 위한 운용요구서(ORD) 작성방안 연구, p. 36 그림 20 참조(한국/미국 획득절차 비교)

[RMF 1단계] 선행연구를 통해 획득방식이 결정되면 ORD(운용요구서)를 근거로 SRR(체계요구조건검토)를 통해 본격적으로 RMF 1단계를 시행한다. 무기체계 요구조건을 분석하여 소통할 데이터를 파악하고 분류하게 된다. 보안시스템에 대해서 수명주기관리계획(LCSP)[28]에 포함하여 개략적으로 정의한다.

[RMF 2단계] SRR(체계요구조건검토) 후 탐색개발 단계에 접어든다. 이때 RMF 2단계를 시행하며 분류한 데이터들을 어떻게 접근하고 통제시킬 것인가에 대한 보안시스템 기준선(Baselines)을 확인하고 보안통제항목(Security Controls)을 식별한다. 또한, 무기체계에 보안시스템을 통합하는 과정에서 성능에 미치는 영향 분석을 하고 IPT팀장(또는 PM)을 중심으로 보안관계자, 소요군 등 이해관계자들이 조율과 협의를 한다. TRA(기술성숙도평가) 시 보안시스템에 대한 평가도 병행 시행하여 RMF 3단계로 전환한다.

[RMF 3단계] TRL(기술성숙도) 6 이상이 결정되면 체계개발로 진입한다. 이때 보안통제항목을 구현하는 RMF 3단계가 시행되며 보안통제 설계를 검토한 후 무기체계 PDR(기본설계검토), CDR(상세설계검토) 시 보안통제항목을 설계한다. 보안시스템이 무기체계에 미치는 영향력을 지속 모니터링하면서 무기체계 TEMP(시험평가종합계획)에 보안평가계획을 포함한다.

[RMF 4단계] 보안시스템을 통합한 초기 시제품이 완성되면 개발시험평가를 한다. 이때 RMF 4단계를 시행한다. 보안시스템 통합과정에서 무기체계의 FCA(기능적 형상 확인, Functional Configuration Audit),[29] PCA(물리적 형상 확인 : Physical Configuration Audit)[30] 절차를 시행하는 동안 보안시스템도 기능적으로 구현이 제대로 되었는지, 계획된 설계대로 구현되었는지를 개발시험평가를 통해 확인해야 한다. 무기체계 시험평가를 하는 동안 설계한 보안시스템의 통제항목에 대한 평가도 동시에 이루어진다.

[RMF 5단계] 이후 무기체계의 운용(OT) 및 야전시험평가(FT) 시 RMF 5단계를 시행하여 보안시스템을 최종 검증하고 시스템 인가를 하게 된다.

[RMF 6단계] 개발시험평가가 이뤄지는 RMF 4단계 이후 6단계까지 보안시스템의 보안통제항목(Security Controls)이 제대로 구현되는지 지속 모니터링을 하면서 보안시스템의 고장과 정비에 대한 데이터를 축적하여 보안시스템이 RAM에 의해 통제되도록 총수명주기 관점에서 폐기단계까지 지속 관리・유지해야 한다.

---

28) LCSP(Life Cycle Sustainment Plan) : 체계의 총수명주기관리를 목적으로 통합체계지원 업무수행과 체계적인 관리를 위한 계획문서(총수명주기관리업무훈령 별표1 용어정의)

29) 형상품목의 실제 성능이 기능기준선 및 할당 기준선에 명시된 요구조건을 충족하는 지를 확인하는 절차

30) 형상이 설계문서와 일치하는지를 판단하고, 제품기준선을 확인하기 위한 절차

Ⅴ. 결론 및 논의

모든 것이 연결되고 보다 지능화된 사회, 4차 혁명의 시대가 도래되었다. 사이버 공간에 가까이 갈수록 사이버 위협도 더욱 우리에게 다가오고 있다. 보안의 미래 또한 모든 것이 사이버상에서 이뤄질 것이다. 하지만 사이버 위협과 예측이 어려워지고 있다. 보안의 패러다임이 변화할 수밖에 없다. 미래의 보안(활동)을 다음과 같이 정의해 보았다. '사이버 위협과 취약점에 대해 위험관리(RM)를 통해 최적의 상태로 복귀시키는 안정화 활동'인 것이다.

우리 군의 무기체계도 사이버상 많은 위협에 직면하였다. 첨단화된 무기체계(또는 전력지원체계)의 사이버 취약점에 대해 위험관리(RM)를 중심으로 프레임워크(새로운 계획・설계・골격 등)를 설계하여 안정화해야 'RMF'인 것이다. 상기 연구를 통해 한국군의 무기체계 획득절차와 보안시스템의 통합에 대한 방향을 제시하였다. 보안시스템이 무기체계의 성능에 악영향을 주지 말아야 하며 무기체계 일부로서 예측과 통제를 할 수 있도록 설계되어야 한다(Lee & Choi, 2020; Lee, Cha, Baek, & Kim, 2018). 이것이 무기체계와 보안시스템 통합(장착)의 핵심 요소인 것이다.

미군 측에서 시행하고 있는 RMF에 대한 세부절차는 입수할 수 없는 실정이다. 이런 현실에서 국내 무기체계 획득절차별 RMF를 적용방안을 제시하였다는 점에서 실무적인 시사점이 크다고 볼 수 있다. 다만, 본 연구는 일반 무기체계 획득절차만을 제시하여 함정 및 전장관리정보체계 등 체계별 적용방안을 제시하지 못하였다는 한계점이 있다. 따라서. 후속 연구는 해외구매[31]에 대한 RMF 적용뿐만 아니라 국내 무기체계와 방위산업 발전을 위해 다양한 RMF 적용 방안을 도출하기 위한 연구를 활발히 진행할 필요성이 있다.

31) 무기를 해외구매 시 오퍼요청서 명시, 제안서 접수・평가 전에 연합암호장비와 RMF에 대한 구체적인 요구가 있어야 하는데, 고성능・첨단화된 무기를 해외구매할 경우 자국 기술 보호의 명목으로 무기체계 데이터 미제공 등 RMF 적용에 어려움이 발생할 수도 있다.

Reference

Cho, H. S., Cha, S. Y., & Kim, S. J. (2019). A Case Study on the Application of RMF to Domestic Weapon System. *Journal of The Korea Institute of Information Security and Cryptology, 29*(6), 1463-1475. https://doi.org/10.13089/JKIISC.2019.29.6.1463

Cho, H., Cha, S., & Kim, S. (2019). A Case Study on the Application of RMF to Domestic Weapon System. *Journal of the Korea Institute of Information Security & Cryptology*, *29*(6), 1463 - 1475. https://doi.org/10.13089/JKIISC.2019.29.6.1463

Choi, J. S., & Kook, K. H. (2014). Developing Warfare System SW Development Security Classification System Using KJ method. *Journal of Security Engineering, 11*(2), 165-176. https://doi.org/10.14257/jse.2014.04.03

Jin, J. H., Kim, B. J., & Han, K. H. (2021). A Study on Applications of Information Security in Implementing Cloud-Based Defense Information Systems. *The Journal of Korean Institute of Communications and Information Sciences, 46*(9), 1415-1425. https://doi.org/10.7840/kics.2021.46.9.1415

Jung, Y. T., Jung, H. S., & Kang, J. W. (2019). A Study on Enhancing Cybersecurity of Weapon Systems for Life-Cycle. *Journal of Convergence Security, 19*(4), 67-75. https://doi.org/10.33778/kcsa.2019.19.4.067

Kumi, S., Lim, C., & Lee, S. (2020). Cost-Effective, Real-Time Web Application Software Security Vulnerability Test Based on Risk Management. *Journal of the Korea Institute of Information Security & Cryptology, 30*(1), 59-74. https://doi.org/10.13089/JKIISC.2020.30.1.59

Lee, J. S., Cha, S. Y., Baek, S. S., & Kim, S. J. (2018). Research for Construction Cybersecurity Test and Evaluation of Weapon System. *Journal of The Korea Institute of information Security & Cryptology, 28*(3), 765-774. https://doi.org/10.13089/JKIISC.2018.28.3.765

Lee, Y. S., & Choi, J. M. (2020). Research for Application the RMF to the Korean Military. *The Journal of Korean Institute of Communications and Information Sciences, 45*(12), 2132-2139. https://doi.org/10.7840/kics.2020.45.12.2132

So, B. K., & Cheung, C. S. (2021). Cyber Risk Management of SMEs to Prevent Personal Information Leakage Accidents. *Journal of the Society of Disaster Information, 17*(2), 375-390. https://doi.org/10.15683/kosdi.2021.6.30.375

Yoo, J. (2021). A Study on the Application of Cybersecurity by Design of Critical Infrastructure.

The Journal of the Convergence on Culture Technology, 7(1), 674-681. https://doi.org/10.17703/JCCT.2021.7.1.674

Acknowledgements

We would like to thank Editage (www.editage.co.kr) for English language editing.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

원 고 접 수 일 2021년 10월 23일
원 고 수 정 일 2021년 12월 15일
게 재 확 정 일 2021년 12월 20일

IDAP 광운대학교 방위사업연구소 INSTITUTE OF DEFENSE ACQUISITION PROGRAM

JAMS JOURNAL OF ADVANCES IN MILITARY STUDIES

2021, Vol. 4, No. 3, 191-208.

https://doi.org/10.37944/jams.v4i3.122

국내 무기체계의 RMF 적용방안 연구: 무기체계 & 보안시스템 통합

이승목*

국문초록

4차 혁명이 도래하면서 군사 무기체계도 고도화・첨단화되고 있다. 특히 첨단화된 무기시스템은 소프트웨어 비중이 높아지면서 사이버상 취약점도 점차 증가하고 있다. 소프트웨어 결함이나 사이버 공격으로 최첨단 무기가 중단되거나 오작동할 경우 전투력, 경제적 손실뿐 아니라 국방안보 등에 악영향을 미칠 것이다. 미 DoD는 이러한 사이버 취약성 및 위협에 대처하기 위해 RMF(Risk Management Framework)를 시행하고 있다. RMF는 무기시스템의 사이버 취약성을 데이터 중심으로 분류하고 기밀성, 무결성, 가용성에 따라 평가하는 RM(Risk Management) 기반 프레임워크이다.

한국군의 무기체계 획득절차에 대한 RMF 적용은 아직 초기 단계다. 본 연구에서는 미 DoD에서 무기획득 프로세서에 RMF를 적용하는 방법을 연구, 우리 군에 적용하는 방안을 제시하면서 무기 성능에 영향을 미칠 수 있는 가용성, 신뢰성 및 안전성의 척도가 보안과 함께 관리되어야 하고, 보안시스템이 무기체계의 일부로 RAM(Reliability, Availability, Maintainability)에 적용을 받아 언제나 예측 가능하고 통제 가능한 장치(Units)가 되어야 함을 제시하였다.

주제어 : 획득체계, 사이버 위험, 위험관리프레임워크, 신뢰성・가용도・유지보수성, 안정성

* (제1저자) 군사안보지원사령부 정보학과장, lsm000lsm@naver.com, https://orcid.org/0000-0001-6944-541X