Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 8 pp. 616-622, 2024

https://doi.org/10.5762/KAIS.2024.25.8.616
ISSN 1975-4701 / eISSN 2288-4688

방산 공급망 보안 강화를 위한 제도 개선 방안 연구

류지선*, 최지웅, 김상빈, 황도빈
국방기술품질원

Improving the Regulation for Supply Chain Security in the Defense Industry

Jiseon Yu*, Jiung Choi, Sangbeen Kim, Dobin Hwang
Defense Agency for Technology and Quality

요 약 무기체계는 수 천, 수 만 개에 이르는 부품과 부체계가 모여 하나의 무기체계로 구성되어 수많은 이해관계자가 존재하기 때문에 공급망의 범위가 매우 넓다. 또한, 신기술의 빠른 성장과 함께 무기체계 첨단화가 진행되면서 방산 소프트웨어 공급망 확대를 야기하고 이러한 공급망은 사이버 공격의 대상이 될 수 있기 때문에 방산 공급망 보안의 중요성이 날로 증가하고 있다. 게다가 지금은 국내 무기체계 수출이 부흥기를 맞이하여 무기체계 수요가 전 세계로 확대되는 추세로 우리 무기체계의 방산 공급망 보안이 매우 중요한 시점이다. 따라서 본 논문에서는 현재 국방·방산 분야에서 공급망 보안을 위한 가장 유사한 활동으로 방위산업기술보호지침의 실태조사, 국방 사이버 안보 위험관리 지시의 국방 사이버 보안 위험 관리제도로 판단하였으며, 향후 미국 방산 관련 수출을 위한 전제 조건인 사이버 보안 성숙도 모델 인증 프레임워크의 국내 도입을 고려하여 이 프레임워크까지 포함한 세 제도의 유사성과 차이점을 분석하였다. 그 결과 방산 공급망 보안 강화를 위한 제도 개선 방안으로 산출물 테일러링의 필요성과 사이버 및 정보화 관련 규정의 전면 검토를 제안하였으며 이는 향후 실효성 있는 방산 공급망 보안 제도 정립에 기여할 수 있다.

Abstract Weapon systems are composed of various components and have numerous stakeholders, so the scope of the supply chain is vast. In addition, the advances in weapon systems may lead to an expansion of the defense industry software supply chain, making it a target of cyber attacks. These are why supply chain security is important in defense industry software. In this paper, the rules for supply chain security in the defense industry were determined to be fact-finding surveys on defense technology security guidelines, K-RMf on defense cyber security risk management, and the cybersecurity maturity model certification. The similarities and differences between them were analyzed. As a result, the need for tailoring existing outputs and an overall review of the regulations related to cyber and information were proposed. These regulations aim to strengthen the rules for supply chain security in the defense industry.

Keywords : Defense, Defense Industry, Supply Chain Management, Security, Supply Chain Security

1. 서론

최근 소프트웨어 보안 솔루션 기업인 시놉시스(Synopsys)와 포네몬 인스티튜트(Ponemon Institute)에서 공동으로 발표한 '소프트웨어 공급망 보안 위험 현황'보고서에 따르면 지난 1년간 전 세계 기업의 54%가 소프트웨어 공급망 공격을 경험하였다고 한다[1]. 공급망은 생산부터 배포까지 전 과정에 이르는 시스템 전부를 일컫는다. 이러한 전 과정에 속하는 모든 공급자를 관리하는 것이 공급망 관리이다.

*Corresponding Author : Jiseon Yu(DTaQ)
email: gsun2@dtaq.re.kr
Received July 9, 2024 Revised August 1, 2024
Accepted August 2, 2024 Published August 31, 2024

무기체계는 수 천, 수 만개에 이르는 부품과 부체계들이 모여 하나의 무기체계로 구성되는데 실제 체계 통합을 담당하는 체계업체부터 협력업체까지 수많은 이해관계자가 존재하기 때문에 공급망의 범위가 매우 넓다. 최근 무기체계 디지털 트윈 활용 지침이 제정되면서 무기체계의 네트워크 환경이 확대되어 방위산업 디지털 전환이 가속화되고 있는 상황은 소프트웨어 공급망의 확대의 원인이 되어 지속적으로 공격자들의 주요 공격 대상이 되고 있다[2]. 이와 같은 기술의 발전이 소프트웨어 공급망 확대에 가속 원인이 되고 있어 무기체계를 제조·개발하는 방산 공급망 역시 공급망 보안에 대한 문제에 직면한 상황이다.

정보 자산과 기술 유출 방지를 위해 무기체계 개발 과정에서 생산되는 일부 기술들은 방위산업기술로 지정되어 '방위사업기술보호법'에 따라 관련 제반 자료를 보호하고 '방위산업기술보호지침'에 따라 관리 현황에 대해 매년 실태조사를 수행한다. 최근에는 사이버 보안 강화를 위해 국내 무기체계 획득과정에서 보안 내재화를 구현하는 국방 사이버 보안 위험 관리 제도(K-RMF: Korea Risk Management Framework)가 발표 되었고 미국 국방부의 계약업체가 보유한 민감 정보를 사이버 위협으로부터 보호하기 위해 개발한 사이버 보안 성숙도 모델 인증 프레임워크(CMMC: Cybersecurity Maturity Model Certification, 이하 CMMC)의 도입을 앞두고 있는 상황이다. 이전까지는 능력성숙도모델(CMMI)이 소프트웨어 시장에서 사실상의 표준으로 활용되어 소프트웨어 개발 과정의 안전과 신뢰성을 평가하였으나 이제는 보안성이 새로운 과제로 자리잡으면서 RMF나 CMMC라는 제도가 점증적으로 자리를 잡아가는 추세이다. 이에 따라 기존에는 개발 완료 시점에 단순 체계에 대한 보안 기능에 집중해 왔다면 이제는 하드웨어, 소프트웨어를 포함한 해당 체계 자체의 개발 목적이나 성능, 시험 일정 등 관련된 정보를 다루는 사람까지 보안을 확보해야 하는 대상으로 판단하는 등 공급망을 지속적으로 관리하는 것이 필수이다. 따라서 무기체계를 개발하거나 수출하려는 공급망인 방산업체에서는 새로운 제도를 빠르게 파악하고 사내 파급력, 체계 영향성 분석이나 비용 분석 등 충분한 대비가 필요한 상황이다. 새로운 제도가 도입되면서 어쩔 수 없는 행정 소요가 발생하게 되고 일부는 이미 수행중인 보안 활동과 같거나 유사하나, 관리 감독 기관이 상이하거나 보안을 확인하는 시점의 차이로 인해 업체에서는 늘어난 행정 소요에 대해 피로감을 느낄 수 밖에 없는 상황이다.

본 논문에서는 방산 공급망 보안과 관련된 현재 규정 및 도입 예정인 규정에 대해 현재 공개된 표준 등을 이용하여 이론적인 분석을 통해 유사성과 차이점을 식별하고 향후 방산 공급망 보안 강화를 위한 제도의 개선 방안을 제안한다.

2. 공급망 보안 관련 연구

2.1 민간 공급망 보안

현재 정보 기술의 발달로 정보 유통 채널이 다양해지고 있기 때문에 국가 사이버안보의 기초가 되는 '국가사이버안보전략' 또는 '국가 정보보안 기본지침'과 같은 관련 규정들의 실효성 있는 개정이 필요한 시점이다. 지난 5월 '소프트웨어 공급망 보안 가이드'가 배포되었으나 이전까지는 공급망 보안 국내 소프트웨어 공급망 보안을 위해 '국가사이버안보전략'과 '국가사이버안보 기본계획'에 공급망 보안 관리 체계 구축을 명시하고 있는 반면 실제 이를 실현하기 위한 구체적인 공급망 표준 제도가 공개되지 않아 주요국들에 비해 많은 발전이 필요한 상황이었다. 따라서 우리나라에서도 미국의 '사이버보안강화법'과 '연방정보보안현대화법'에 기반한 미국 공급망 관리체계를 다룬 SP 800-161를 바탕으로 국내 소프트웨어 공급망 보안을 위한 연구가 수행되었다[3]. 또한, 미 SP 800-161 분석을 통해 '국가 정보보안 기본지침'과 매핑하여 개선 방안을 도출하는 연구 등 국내 공급망 보안 제도 개선을 위한 다양한 연구가 진행되었다[4].

2.2 방산 공급망 보안

방산분야에서는 정보의 유통에 긴밀한 주의가 필요한 비밀 자료나 비밀로 취급하지 않으나 주의가 필요한 일반군사자료가 있고, 정보가 새어나갈 경우 국가 안보와 밀접한 관련이 있기 때문에 '국방보안업무훈령'이나 '국방사이버안보훈령', '방산기술보호법' 등으로 국방 및 방산에 유통되는 정보가 유출되지 않도록 규정함으로써 끊임없이 노력해왔다. 그러나 최근 신기술을 적용한 무기체계의 고도화가 전 세계적으로 빠르게 진행되고 단순 정보만을 지키는 것이 아닌 유통 경로 모두를 지켜야 하는 공급망 보안으로 범위가 확장하고 있기 때문에 무기체계와 무기체계 제조사, 무기체계 소프트웨어 개발사까지 관리가 필요하다. 게다가 국내 무기체계 수출이 부흥기를 맞이하여 우리 무기체계 수요가 전 세계로 확대되는 추세로 국내 방산 공급망 보안이 매우 중요한 시점이다.

현재 국내 방산 공급망 보안과 가장 밀접한 활동은 '방위산업기술보호지침'에서 방산기술을 소유한 업체나 기관의 기술보호구역에 대한 관리 실태를 점검하는 실태조사이다[5]. 이에 따라 실태조사 및 공급망 보안 관련 연구가 일부 수행되었고 그 중 향후 미국에서 국방 공급망 사이버 보안을 구현하기 위한 통합 표준으로 CMMC 인증 제도 도입을 위해 현재 수행중인 실태조사의 항목 확대를 통해 연계하는 방안을 제안한 연구가 수행되었다[6]. 아직 국내 국내 도입을 위한 구체적 방안이 논의되고 있는 시점으로 방산 공급망 보안을 위한 다방면의 연구가 필요한 상황이다.

3. 방산 공급망 보안 관련 규정

국방 및 방산분야에서는 사이버보안, 사이버안보, 정보화 등 다양한 이름을 가진 규정들이 존재한다. 각각의 목적에 맞게 국방부 또는 방위사업청에서 관련 규정을 제·개정하고 있고 규정의 범위 내에 있는 각급 부대나 기관, 업체에서는 이를 준수하여 업무를 수행한다. 본 장에서는 국방부와 방위사업청 규정 중에서 방산 공급망 보안과 가장 관련이 있는 규정을 식별 및 분석하고 향후 도입될 규정과의 유사점과 차이점을 식별 및 분석한다.

3.1 국방사이버안보훈령

본 훈령은 안전한 사이버공간 창출, 유지, 보호를 위한 지침과 절차를 규정하고 적용 범위 내 대상 기관은 국방정보시스템 도입 시 보호대책(보안대책)을 수립하는데 이때 도입의 적절성과 충분성을 검토하기 위한 보호기준과 보호요구사항이 규정되어 있다[7]. 규정의 내용은 도입되는 정보시스템의 보안기능과 적절한 위치에 도입되었는지 확인할 수 있는 보호요구사항으로 구성되어 정보시스템 도입 시 신뢰할 수 있는 공급망에 대한 보안요구사항은 다루지 않는다. 이에 따라 방산 공급망 보안 비관련 규정으로 판단하고 대외 비공개 규정임을 고려하여 본 논문에서는 더 이상 다루지 않는다.

3.2 방위산업기술보호지침

본 지침은 방위산업기술보호법과 방위산업기술보호법 시행령에 따라 방산기술보호에 필요한 방법과 절차 등이 규정되어 있으며 방산기술보호법 제12조 방위산업기술보호를 위한 실태조사에 필요한 사항을 정하고 있다[5]. 이 때 실태조사는 방위산업기술로 식별된 관리대상기술을 보호 대상으로 하고 이 기술을 체계적으로 보호하기 위해 일정한 범위를 기술보호구역으로 설정하는데, 본 지침에 따라 자체 보안 내규를 제정하고 보안대책을 강구하는 등의 보호 활동을 요구한다. 실태조사의 범위는 기술식별·관리, 인원통제, 시설보호, 정보보호, 연구개발 및 수출·국내이전 시 기술보호/방산협력업체 기술보호, 군사기밀 관리 등으로 구성되어 있고 대분류 기준 총 226개의 항목으로 구성되어 있으며 필요시 국정원, 국군방첩사령부 등과 함께 보안감사와 통합하여 통합실태조사를 실시함을 규정하고 있다[5].

본 지침에서 방산관련자는 방위사업법에서 방산업체의 방산관련 분야에 종사하는 자로 정의함과 동시에 방위사업법과 국방과학기술혁신 촉진법에 따라 방위력개선사업 또는 군수품 획득과 관련된 업무에 종사하는 자로 정의하고 있기 때문에 본 지침을 공급망 보안과 가장 밀접한 규정으로 판단하였다[8].

3.3 국방 사이버보안 위험관리 제도

최근 국방부에서는 무기체계의 사이버보안 능력을 강화하고 유무인 복합체계 등 첨단 무기체계의 안전한 운용을 위한 기반을 마련하기 위해 '국방 사이버보안 위험관리 지시'를 발표하며 '국방 사이버보안 위험관리 제도(이하 K-RMF)'를 공고히 하였다[9]. 이는 무기체계를 획득하는 소요부터 폐기까지 전 과정에서 사이버보안 요구사항을 조기에 식별하고 지속적으로 검토함으로써 시험·평가 단계나 운용 유지 단계에서 뒤늦게 발생할 수 있는 보안 문제를 사전에 식별하여 사이버 보안에 비교적 안전한 무기체계 전력화에 기여할 수 있다. 지시에 따르면 K-RMF는 소요부터 개발, 운용, 폐기까지 전 생명주기에 보안을 관리하는 제도이다. 각 단계를 거치며 보안계획서라는 산출물이 완성되고 이를 토대로 보안평가를 수행하면서 무기체계가 무형에서 유형으로 다시 무형으로 돌아가기까지 전 과정에서의 보안을 해당 무기체계와 관련된 모든 관계기관, 업체에서 보안 계획서를 통해 각 단계마다 발전시켜 완성하고 관리하는 구조이다. 예를 들면 소요단계에서는 합참에서 보안계획서를 작성하고 관리한다면 체계개발 단계에서는 방위사업청(방사청)에서 관리하여 한 무기체계와 관련된 모든 조직이 보안 내재화를 수행하는 것이다. 그러나 지시가 발표된 시점 당시에는 K-RMF의 전반적인 구조와 각 기관의 역할, 획득 단계에서 K-RMF를 위한 업무 프로세스가 포함되어 있으나 개발업체에서 준수해야 하는 보안통제항목에 대해서는 공개되지 않았으나 지난 6

Table 1. Supply Chain Management in SP 800-53

Security Control	
SR-1	Policy and Procedures
SR-2	Supply Chain Risk Management Plan
SR-3	Supply Chain Controls and Processes
SR-4	Provenance
SR-5	Acquisition Strategies, Tools, and Methods
SR-6	Supplier Assessments and Reviews
SR-7	Supply Chain Operations Security
SR-8	Notification Agreements
SR-9	Tamper Resistance and Detection
SR-10	Inspection of systems or Components
SR-11	Component Authenticity
SR-12	Component Disposal

월, 방첩사령부에서 보안통제항목 목록서를 대외 공개하였다. 본 연구는 목록이 공개되기 전에 수행되어 국내에서 국방 RMF 연구에 인용된 SP 800-53의 공급망 위험관리 보안통제항목을 참고하였다[10,11].

SP 800-53은 미국 연방 정보보호 관리법(FISMA)에 규정된 법적 책임을 다하기 위해 국립표준기술연구소(NIST)에서 개발한 사이버 보안 위험 관리 프레임워크로서 연방 정부 및 중요 인프라의 사이버 보안에 대한 상세한 보안 통제항목과 개인정보보호 설정을 제공하는 정보보호 표준이다[11]. SP 800-53은 2020년에 Rev.5가 발표되었는데 기존에는 공급망 보안이 시스템 및 서비스 획득(system and services acquisition) 패밀리의 일부였다면 Rev.5에서는 이 보안통제항목이 공급망 위험관리(supply chain risk management)라는 하나의 패밀리가 되어 보안 관련 공급망 위험 관리 개념이 RMF에 통합되었음을 확인할 수 있었다. 해당 보안통제항목 목록은 Table 1과 같다.

3.4 방산 사이버보안 인증 제도

미 국방부는 국방부에서 발주하는 방위 사업에 참여하기 위해 관련 기관과 계약하기 위해서 반드시 획득해야 하는 사이버 보안 인증 제도로 CMMC를 발표하였다. 국내에서는 아직 도입 예정인 수준으로 방사청에서는 국내 방산 환경에 적합한 방산 사이버보안 인증 제도(가제)로 발전시키기 위해 관계기관과 협업 및 연구를 수행하고 있다. 특히, 방사청과 국방기술품질원에서는 방산업체의 원활한 CMMC 인증 획득을 위해 방산업체에 CMMC 컨설팅을 지원하고 있다. 따라서 본 논문에서는 CMMC 자체가 국방 공급망의 사이버 보안 수준 인증을 위한 제도로 판단하고 방산 사이버보안 인증 제도를 CMMC와 같은 의미로 사용하며 CMMC의 보호 대상인 연방계약정보(FCI: Federal Contract Information, 이하 FCI)와 통제필요정보(CUI: Controlled Unclassified Information, 이하 CUI) 모두를 점검하는 Level 2를 기준으로 소개하고 이를 분석한다.

Table 2. Supply Chain Risk Management in SP 800-171

Supply Chain Risk Management	
1	Supply Chain Risk Management Plan
2	Acquisition Strategies, Tools, and Methods
3	Supply Chain Requirements and Processes

Level 2는 NIST SP 800-171의 보안 요구 사항을 인증 수준으로 요구하고 있는데 최근 Rev.3이 발표되면서 일부 항목이 삭제되었고 기존 항목이 조정되며 공급망 보안(supply chain risk management) 패밀리가 새롭게 등장하였다. 패밀리가 추가되었으나 새롭게 추가된 항목이 아닌 기존 항목의 조정을 통해 공급망 관리 패밀리가 독립함을 미루어 보았을 때, 공급망을 관리하는 이해관계자들에 대한 자체적인 보안 계획 수립과 절차 관리 등을 수행하는 공급망 보안의 중요성이 더욱 커졌다고 볼 수 있다. 공급망 관리 항목들은 FCI, CUI를 생성하거나 저장, 유통하는 업체나 기관의 관리 수준을 확인할 수 있는 항목들로 구성되어 있으며 인증 항목은 Table 2와 같다[12].

4. 규정 분석 및 제도 개선 방안

무기체계 보안이나 방산 환경의 사이버 보안 강화를 위해 다양한 규정과 제도 속에서 무기체계 획득의 공급망 보안이 자연스럽게 요구되면서 그 중요성이 확대되고 있음을 확인하였다. 본 장에서는 앞서 소개한 규정 중 실제 공급망을 대상으로 점검을 수행하는 방위산업기술보호지침의 실태조사, 국방 사이버보안 위험관리 지시의 K-RMF, 향후 도입 예정인 CMMC를 중점으로 분석하고자 하며 본 장에서는 특히 각 제도에서 공급망 보안과 관련된 항목만을 비교 분석 범위로 정하였으며 이를 요약하면 Table 3과 같다. 또한, 이 세 제도는 무기체계 획득 단계 중 수행 시기에서 가장 큰 차이가 있는데 실태조사는 방산기술을 보유한 업체를 대상으로 수행하기 때문에 Fig. 1과 같이 획득 단계 중 어느 단계에나 해당 될 수 있으며, K-RMF는 전 생명주기에 관리하고, CMMC는 수출 계약 전에 수행되어야 하므로 운용 유지 단계로 볼 수 있다.

Table 3. Difference in the regulations

	Fact-finding Survey	SP 800-53	SP 800-171
Stakeholder	Defense Industry Company	Systems, Company	Contractor, Sub-contractor
Target	Security Area	Systems	FCI, CUI
Items	226	12	3
Period	1 year	All life cycle	1 year

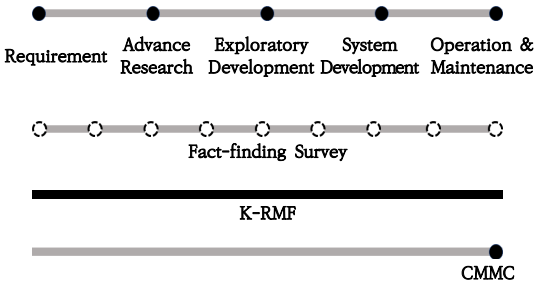

Fig. 1. Differences in check points

실태조사와 CMMC의 유사점과 차이점을 살펴보면, 앞선 연구에서는 실태조사와 CMMC의 차이점을 평가 항목 개수의 차이와 목적으로 판단하여 실태조사는 관리적인 보안에 중점을 두고 CMMC는 기술적인 보안에 중점을 둔 차이가 있음을 보였다[3]. 이러한 차이로 인해 실태조사를 테일러링하여 CMMC 인증 항목 확인에 한계가 있기 때문에 실태조사의 항목을 추가하여 영역을 확대하는 개선 모델을 제안하였다[3]. 본 연구에서도 실태조사와 CMMC는 일부 유사한 부분이 있지만 기술보호구역에 대한 관리 현황을 점검하는 실태조사와 수출 계약 관련 정보인 FCI와 CUI의 저장, 유통에 대한 관리 현황을 인증하는 CMMC는 범위와 자료 요구 수준이 다르다는 한계로 서로의 자료를 테일러링하기에 어려움이 따른다고 판단하였다. 특히 실태조사는 국가 차원에서 업체에서 보유한 방위산업기술을 보호하기 위한 지정된 영역에서의 관리 현황을 파악하고 지속 관리하기 위함이고 CMMC는 체계나 부품 등을 수출하기 위한 민간 평가자에 의한 업체 주도의 인증 획득이며 실태조사는 점수로 결과를 확인 가능하지만 CMMC는 한 항목이라도 충족하지 못할 시 인증 획득이 불가하다는 차이가 있다. 실태조사는 결과 점수가 향후 각종 사업에 제안서 평가 요소로 반영되는 CMMC는 수출 계약에 반드시 필요하기 때문에 시기나 필요에 따라서 업체의 업무 우선순위가 달라질 수 있다.

K-RMF에서 참조한 조직 보안과 개인 프라이버시 강화를 위한 SP 800-53과 CMMC Level 2에서 참조하는 SP 800-171의 공급망 보안 관련 항목은 공급망 보안을 다룬 SP 800-161을 공통적으로 참조하고 있다는 점에서 상당한 유사성을 확인할 수 있었다. 그러나 이를 K-RMF와 CMMC에 빗대어 비교하면 전 획득 주기에서 보안 내재화를 점검하는 K-RMF에서 공급망은 업체부터 부대, 품질인증기관, 시험평가기관 등 상당히 넓은 범위를 갖지만 CMMC는 이미 개발이 완료된 체계나 부품에 대해 수출을 준비하는 것이기 때문에 체계개발업체나 협력업체가 공급망의 범위가 된다. 그렇기 때문에 두 제도의 공급망 보안 항목 자체가 유사하더라도 다른 결과가 나올 수 밖에 없는 것이다. 그래도 방산업체라는 동일 범위가 있다는 점은 향후 제도를 정립하고 발전하면서 제도 간 산출물을 테일러링 할 여지가 있으므로 이를 활용할 수 있도록 공통 산출물 양식 등에 대한 추가 연구가 필요하다. K-RMF는 기존 국방사이버안보훈령과 국방보안업무훈령의 보안대책 및 보안측정과 유사하다는 한계가 있었으나 이번 지시가 발표되면서 지시에 따라 보안계획서 검토 및 보안평가를 받은 경우 보안대책 검토와 보안측정을 받은 것으로 한다는 특례가 적용되었다. 이로써 현재는 보안대책과 보안측정이 새로운 제도인 K-RMF로 전환되는 과정에 있음을 확인할 수 있었다. 이와 같이 완벽하게 같은 활동은 아니지만 획득 전 과정에서 보안내재화를 수행하기 위해 K-RMF를 수행하면서 많은 이해관계자들이 노력해야 하는 방향으로 발전되면서 제도가 정착하게 될 것이다. CMMC와 실태조사 역시 관련연구를 통해 비슷한 방향으로 발전하고자 하는 것으로 보여진다[6]. 그러나 실효성 있는 제도로 발전하고 정착하기 위해서 두 제도 간 범위와 증빙자료 수준이 다른 한계를 극복하고 하나의 제도로 통합할 수 있는 연구와 완전히 독립적인 제도로 발전하는 관점의 연구 역시 병행되어야 하며 이를 위해 두 제도의 차이를 명확히 구분하는 것이 선제 되어야 할 것이다. 또한 향후 통합실태조사와 CMMC가 국내 실정에 적합한 한국형 제도인 방산 사이버보안 인증 제도가 되기 위해서는 K-RMF와 같이 미국에서 상호 인정이 가능하도록 국가 차원의 노력이 필요하다.

국방 및 방산분야에는 앞서 분석한 규정 및 제도뿐만 아니라 사이버보안, 사이버안보, 정보화 등 다양한 이름을 가진 유사해 보이는 규정이 존재한다. 정보화 환경이 급격하게 발전하면서 시대에 맞추어 각 목적에 맞는 규정이 제정되었으나 현재는 산재되어 있는 규정 속에서

AI와 같은 신기술을 반영하거나 보안과 같은 소프트웨어의 속성을 반영하기에 다소 혼란스러운 상황이다. K-RMF도 지시를 제정하여 제도를 빠르게 도입하고 특례로 보안대책과 보안측정을 대체하고 있으나 국방사이버안보훈령이나 국방보안업무규정의 보안대책과 보안측정이 K-RMF로 완전히 자리 잡을 수 있도록 관계 규정 파악을 통해 규정 전면 개정이 필요하기 때문이다. CMMC도 같다. 단순히 계약 필수 조건이 아닌 방산 공급망의 보안 강화를 위한 제도로 자리 잡기 위해서는 장기적인 제도 적용 계획을 세우고 관계 규정을 전체적으로 파악하는 것으로부터 시작하여 불필요한 행정 처리 절차를 사전에 제거함으로써 실효성 있는 제도를 만들고자 하는 모든 이해관계자들의 노력과 관심 속에서 제도 발전이 이루어져야 한다.

5. 결론

본 논문에서는 디지털 전환 및 무기체계 첨단화에 따른 방산 공급망 확대로 대두되는 방산 공급망 보안 강화라는 목적을 가지고 현재 제도와 향후 도입 예정인 제도를 현재 공개된 표준 등의 자료를 기준으로 이론적인 비교 분석을 수행하였다. 그 결과 기존 제도의 산출물을 테일러링하고 관련 제도 전면 검토를 통한 실효성 있는 제도 발전의 필요성을 보였다. 현재 민간에 공개된 자료는 지극히 제한적이기 때문에 제도의 상세한 절차와 산출물, 산출물의 내용 등에 대해 상세한 비교 분석에 어려움이 있었다. 그러나 논문에서 다룬 도입 예정인 제도가 곧 본격 시행되기 때문에 향후 실 데이터 수집이 가능할 것으로 보이며 이를 활용한지속적인 제도 발전 연구가 필요하다.

국방과 방산에는 각 군, 부대, 방산업체 등 다양한 공급망으로 구성되어 공급망 보안 제도가 발표되면 상당한 파급력이 예상된다. 그렇기 때문에 방산보안이라는 특수성으로 정보 수집이 어렵고 민간 기관과의 협업이 어려운 한계를 극복하고 관계기관 모두가 조직의 보안 강화에서 나아가 방산 공급망 보안 강화라는 공동의 목표 달성을 위해 국방부, 방사청 등 정부부처와 연구기관, 방산업체 모두의 의견을 적극적으로 반영할 수 있도록 꾸준히 소통하며 제도 발전을 위한 노력이 필요하다.

References

[1] GTT KOREA, The Serious Software Supply Chain Security, [cited 2024 May 19], Available From: https://www.gttkorea.com/news/articleView.html?idxno=10741 (accessed May. 31, 2024)

[2] Jiseon Yu, & Jeongho Park. "Analysis and Countermeasures of Security Threats to Digital Transformation in Defense Industry". *Journal of the Korea Academia-Industrial cooperation Society*, Vol.24, No.10. pp.682-689, Oct. 2023.
DOI: https://doi.org/10.5762/KAIS.2023.24.10.682

[3] Jinmin Kim, Seongseung Wee, Nacil Kim, Yongtae Shin. "A Study on Cyber Security Policy for S/W Supply Chain Security in Korea". *The Journal of Society for e-Business Studies*, Vol.28, No.1, pp.29-53, Feb.2023.
DOI: https://doi.org/10.7838/jsebs.2023.28.1.029

[4] Young-in You, Sunha Bae, So Jeong Kim, Dong Hee Kim. "A Study on the Supplementation of the Korea's National Information Security Manual from the Perspective of Cyber Supply Chain Security". *Journal of The Korea Institute of Information Security & Cryptology*, Vol.32, No.2, pp.309-327, Apr. 2022.
DOI: https://doi.org/10.13089/JKIISC.2022.32.2.309

[5] DAPA, "DEFENSE TECHNOLOGY SECURITY GUIDELINE", No.797, May. 2023

[6] Dong-Sun Kim, RYU YEON SEUNG. "A study on the improvement of the integrated real state investigation system for coping with the US CMMC system". *Journal of The Korea Association of Defense Industry Studies*, Vol.29, No.3, pp.51-61, Dec. 2022.
DOI: https://doi.org/10.52798/KADIS.2022.29.3.4

[7] Ministry of National Defense, "DEFENSE CYBER SECURITY DIRECTIVE".

[8] DAPA, "DEFENSE ACQUISITION PROGRAM ACT", No.20190, May.2024

[9] Ministry of National Defense, "DEFENSE CYBER SECURITY RISK MANAGEMENT DIRECTION".

[10] Jung keun Ahn, Kwangsoo Cho, Han-jin Jeong, Ji-hun Jeong, Seung-joo Kim. "A Study on Constructing a RMF Optimized for Korean National Defense for Weapon System Development". *Journal of The Korea Institute of Information Security & Cryptology*, Vol.33. No.5, Oct.2023.
DOI: https://doi.org/10.13089/JKIISC.2023.33.5.827

[11] NIST, "Security and Privacy Controls for Information Systems and Organizations" NIST SP 800-35 Rev.5, Sep.2020.
DOI: https://doi.org/10.6028/NIST.SP.800-53r5

[12] NIST, "Protecting Controlled Unclassified Infor-mation in Nonfederal Systems and Organizationss". NIST SP 800-171 Rev.3, May.2024.
DOI: https://doi.org/10.6028/NIST.SP.800-171r3

류 지 선(Jiseon Yu) [정회원]

- 2018년 8월 : 고려대학교 정보보호대학원 정보보호학과 (정보보호학석사)
- 2018년 12월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
무기체계 소프트웨어, 소프트웨어 보안

최 지 웅(Jiung Choi) [정회원]

- 2014년 2월 : 금오공과대학교 컴퓨터공학부 (공학학사)
- 2017년 2월 ~ 2023년 7월 : 국방과학연구소
- 2023년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방, 정보보안, 네트워크

김 상 빈(Sangbeen Kim) [정회원]

- 2023년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
사이버 보안, 소프트웨어 보안

황 도 빈(Dobin Hwang) [정회원]

- 2014년 2월 : 공군사관학교 시스템공학과(시스템공학학사)
- 2023년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방보안, 방위산업보안, 개인정보보호, 인공지능