방산안보연구
Journal of Defense Industrial Security

방산안보연구, 1권 2호, 2025년 9월, 21-39면.
Journal of Defense Industrial Security, Volume 1, Issue 2, September 2025, Pages 21-39.
https://doi.org/10.64227/jdis.2025.1.2.2

Print ISSN 3091-5546
Online ISSN 3091-5554

원저

美 CMMC 동향에 대응한 정책방안 연구

백운일[1], 류연승[2], 석호영[3]

[1]명지대학교 대학원 방산안보학과 박사과정
[2]명지대학교 대학원 방산안보학과 교수
[3]명지대학교 법무행정학과 교수

교신저자: 백운일 (roti99@mju.ac.kr)

요약

美 국방부의 새로운 사이버보안 인증 체계인 CMMC는 국방산업기반(DIB)의 사이버보안 수준을 강화하고, 연방 계약정보(FCI)와 통제필요 정보(CUI)를 보호하기 위해 개발한 프레임워크이며, 계약을 준비하는 기업과 협력업체에 2025년부터 단계적으로 적용할 예정이다. 이에 본 논문에서는 AHP 분석 결과에 기반하여, 사이버 위협에 대응하면서도 수출 기업의 CMMC 평가 부담을 줄일 수 있도록 '한국형 CMMC를 독자 개발'하는 방안과 '美 CMMC 평가 방식을 직접 도입'하는 두 가지 방식을 절충한 2-Track 정책 방안을 제안하고, 이를 위한 ① 민간 주도 평가 생태계 조성 ② 방산 계약과의 연계 ③ 통합실태조사 일부 면제 등 3가지 시행 방안을 제시하고자 한다.

핵심어

CMMC, 방산기술보호, 방산안보, 사이버보안

차례

Open Access

접수일: 2025년 7월 26일
수정일: 2025년 8월 16일
게재승인일: 2025년 9월 16일
출판일: 2025년 9월 30일

Original Article

Research on Policy Measures in Response to CMMC Trends in the United States

Woonil Baek[1], Yeonseung Ryu[2], Hoyoung Seok[3]

[1]Ph.D. Candidate in Defense Industrial Security, Myongji University, Republic of Korea
[2]Professor, Department of Defense Industrial Security, Myongji University, Republic of Korea
[3]Professor, Department of Judicial Affairs Administration, Myongji University, Republic of Korea

Corresponding Author: Unil Baek (roti99@mju.ac.kr)

ABSTRACT

The U.S. Department of Defense's new cybersecurity certification framework, CMMC, is a framework developed to strengthen the cybersecurity level of the defense industrial base and protect federal contract information(FCI) and controlled unclassified information(CUI). It plans to gradually apply CMMC to all companies and contractors preparing for contracts. In this paper, based on survey analysis, we propose a 2-track policy approach that balances the need to respond to cyber threats while reducing the CMMC burden on exporting companies. This approach combines two options: Korean-style CMMC and directly adopting the CMMC method. To implement this policy, three implementation measures are proposed: ① Establishing a private-sector-led evaluation ecosystem, ② Linking the CMMC with defense contracts, and ③ Partially exempting certain aspects of the integrated status survey

KEYWORDS

CMMC, defense technology protection, defense security, cybersecurity

1. 서론

1.1. 연구 목적

美 국방부의 새로운 사이버보안 인증 체계인 CMMC는 국방산업기반(DIB)의 사이버보안 수준을 강화하고 연방계약정보(FCI)와 통제필요정보(CUI)를 보호하기 위해 개발한 프레임워크이다. 계약을 준비하는 모든 기업과 협력업체에 CMMC를 단계적으로 적용할 예정이어서, 평가를 준비해야 하는 국내 수출 기업에게는 상당한 부담으로 작용하고 있다.

또한, 국가가 지원하는 해킹 조직의 방산기업에 대한 해킹이 지속 증가하고 있는 상황에서 방산기술 보호 조치를 강화할 필요성도 커지고 있다. 현재 우리나라는 통합실태조사를 통해 방산업체의 보안 기준 준수 여부를 점검하고 있으나, 평가 인력 부족 문제로 인해 협력업체에 대한 직접 점검이 곤란하다는 점 등 여러 가지 문제점을 가지고 있다.

이에, 본 연구에서는 사이버 위협으로부터 방산기술을 보호하는 동시에, 美 CMMC 시행에도 대비할 수 있는 방안을 도출하는 데 중점을 두었다.

1.2. 연구 방법

美 국방부는 2024년 12월 그 간의 CMMC 추진 동향과 이해관계자들의 의견에 대한 입장 및 향후 단계별 시행 계획이 담긴 Federal Register(Vol. 89, No.199, Rules and Regulations)를 공식 발표하였다. 본 연구는 美 CMMC 최근 동향을 분석하기 위해, 이러한 美 국방부의 발표 자료와 함께 美 현지 보안업체들의 CMMC 분석 자료를 탐구하였다.

또한, CMMC 관련 선행 논문 분석을 통해 국내 통합실태조사 제도 개선 등 여러 대응 방안을 고찰하였으며, 일본 방위장비청의 「방위 산업 사이버 보안 기준」 등 해외 사례에 대해서도 살펴보았다. 이와 함께, 우리 정부의 정책 방향성에 대해 알아보기 위해 방사청이 수립한 「2017~2021 방위산업기술보호 종합계획」 및 「2025년도 방위산업기술보호 시행계획」을 참고하였다.

아울러, 美 CMMC 시행에 대비할 수 있는 합리적 방안 도출을 위해 이해관계자들의 의견에 대한 AHP 분석을 실시하였다. 설문은 1次와 2次로 나누어 실시하였으며, 1次에서는 CMMC 도입 시 고려해야 할 기준 5개에 대한 적정성 조사를, 2次에서는 5개 기준과 3가지 대안에 대한 쌍대 비교를 실시하였다.

1.3. 연구 구성

본 연구의 구성은 총 5장으로 이루어진다. 1장에서는 연구의 목적과 방법 및 구성을 설명하며, 2장에서는 CMMC 개요에 대해 살펴본다. 3장에서는 최근 개정 내용을 반영한 CMMC 세부내용에 대해 설명하고, 4장에서는 AHP 분석 결과와 함께 우리 정부의 정책 방향과 3가지 시행방안을 제시한다. 마지막으로, 5장에서는 연구 결과를 종합하여 결론을 도출하고 앞으로의 발전을 위한 제언을 제시한다.

2. CMMC 개요

2.1. 기본 개념

사이버보안 성숙도 모델 인증(Cybersecurity Maturity Model Certification, CMMC)은 美

국방부가 자국의 방위산업기반(Defense Industrial Base, DIB)에 소속된 기업들의 사이버보안 수준을 일관되게 평가하고 인증하기 위해 설계한 사이버보안 통합 인증 체계이다.

기존에는 방산 기업들이 NIST SP 800-171 준수를 '자체평가' 방식으로 증명해왔으나, CMMC는 이를 보완하여 보안 수준을 체계적으로 분류(Level 1~3)하고, 공식적인 제3자 인증 방식을 도입하였다.

CMMC는 미국 연방조달규정(FAR 52.204-21) 및 국방연방조달보충규정(DFARS 252.204-7012 등)의 보안 요구사항을 기반으로 하며, 연방계약정보(Federal Contract Information, FCI)와 통제필요정보(Controlled Unclassified Information, CUI)의 보호를 주요 목표로 하고 있으며, 계약 수행 기간 동안 해당 수준 및 평가 유형을 유지하고 있음을 확인하는 데 사용될 예정이다.

최신 개정판인 CMMC 2.0은 2024년 10월 15일 최종 규칙(Final Rule)으로 공표되었으며, 기존 5단계 체계를 3단계로 간소화하면서도 실효성을 강화하였다.

2.2. 도입 목적

CMMC는 단순한 보안 프레임워크를 넘어 국가 안보 관점에서 공급망 전체의 사이버보안 탄력성 강화를 목표로 한다. 美 국방부는 방위산업 공급망 전반에서 반복적으로 발생하고 있는 정보 유출, 해킹 사고, 내부통제 실패 등을 심각한 문제로 인식하였으며, 이에 따라 구체적인 목적을 갖고 CMMC를 도입을 추진하였다. 도입 목적은 다음과 같다.

첫째, 공급망 전반의 사이버보안 수준을 제고하는 것이다. CMMC는 주계약 방산업체뿐만 아니라, 하청 협력업체까지 보안 수준을 정량적으로 요구함으로써, 공급망 전체의 보안 일관성을 확보한다.

둘째, 인증 기반 보안 검증 체계를 마련하는 것이다. 기존의 자체평가 기반 체계는 검증의 한계와 현실과의 괴리가 크다는 비판이 제기되었으며, 제3자 평가기관(C3PAO)의 공식 인증을 통해 객관성과 신뢰성을 확보한다.

셋째, 민간 기업의 보안 투자를 촉진하는 것이다. 美 국방부는 CMMC를 통해 기업들이 사이버보안을 경쟁력 요소로 인식하고 자발적인 투자를 유도하고자 한다. CMMC 인증은 계약 수주에 필수 요소가 되므로, 기업은 보안을 단순한 비용이 아닌 사업의 기반 인프라로 인식하게 된다.

넷째, 국가 안보 자산의 보호를 위한 것이다. 최종적으로, CMMC는 美 국방부의 미션과 연관된 시스템, 무기, 작전, 기술 정보를 적대적 사이버 위협으로부터 보호하는 것을 목표로 하며, 이는 국가 안보 차원의 보안 정책으로 기능한다.

3. CMMC 세부내용

3.1. 인증 체계

표 1. CMMC 단계별 평가[1)]

구 분	보호 대상	보안 요구사항	평가주체	POA&M (미비점 보완)	유효기간
Level 1	FCI	FAR 52.204-21(15개)	자체	불가	1년(연 1회 확인서 제출)
Level 2	CUI	NIST SP 800-171(110개)	자체 또는 C3PAO	허용(180일 내)	3년(연 1회 확인서 제출)
Level 3	CUI	NIST SP 800-171(110개) NIST SP 800-172(24개)	DIBCAC (국방부)	허용(180일 내)	3년(연 1회 확인서 제출)

3.1.1. Level 1 – 기본 사이버보안

CMMC Levle 1은 연방계약정보(FCI)를 보호하기 위한 기본 보안 요구사항을 다루며, FAR 52.204-21에 명시된 15개 보안 통제 항목을 포함한다.

이 수준은 美 국방부 계약의 기초 수준 공급망 참여자를 대상으로 하며, 자체평가(Self-Assessment) 방식으로 점검을 실시하고, 결과는 SPRS(Supplier Performance Risk System)에 제출한다. Level 1에서는 미비점 보완계획(POA&M)이 허용되지 않으며, 모든 항목은 즉각적이고도 완전한 충족이 요구된다.

3.1.2. Level 2 – 고급 사이버보안

Level 2는 통제필요정보(CUI)의 보호를 목적으로 하며, NIST SP 800-171 Revision 2에서 정의한 110개의 보안 통제 항목을 전체적으로 적용한다. Level 2는 다음 두 가지 형태로 구분된다.

첫째, Level 2(Self)는 비교적 낮은 민감도의 CUI를 다루는 기업에게 적용되며, 3년 주기로 자체평가를 수행한다.

둘째, Level 2(C3PAO)는 민감한 CUI를 다루는 기업에게 적용되며, 공인된 제3자 평가기관(CMMC Third-Party Assessment Organization, C3PAO)에 의해 공식 평가가 이루어진다.

3.1.3. Level 3 – 전문가 수준 사이버보안

가장 높은 보안 수준인 Level 3(DIBCAC)은 국가 안보에 직결되는 핵심 정보시스템을 보호하기 위한 수준으로, 적선 국가 APT 공격에 대한 보호를 위해 NIST SP 800-172(2021년 2월판) 중 24개의 보안 통제 항목을 Level 2의 110개 항목에 더해 추가 적용한다.

3.2. 인증 절차

3.2.1. 단계별 인증 절차

CMMC 인증은 조직의 보안 통제가 특정 수준의 요구사항을 얼마나 충족하는지를 공식적으로 평가하고 인증하는 절차이다. 이 절차는 자체평가를 제외하면 CMMC 인증 생태계에 속한 제3자 평가 기관인 C3PAO와 국방부 소속 DIBCAC에 의해 수행되며, CAP(CMMC Assessment

1) DOD Office of the Secretary. Federal Register Vol 89, No. 199 내용을 요약하여 작성.

Process) 문서를 통해 평가 기준과 운영 절차가 표준화되어 있다.

평가 절차는 다음과 같은 4단계로 구성되어 있다. 첫째, 조직은 인증 준비 단계에서 시스템 보안 계획(SSP)을 수립하고, 평가의 범위를 정의(Scoping)하며, 평가 기관과 계약을 체결한다. 둘째, 평가 기관은 증거 수집, 시스템 실사, 인터뷰 등을 통해 보안 요구사항 충족 여부를 검토하고 점수를 산정한다. 셋째, 평가가 완료되면 결과 보고서를 작성하여 eMASS에 등록한다. 마지막으로, 일부 미충족 항목이 있는 경우 정해진 조건에 맞는 경우에 한에 POA&M을 제출하고 정해진 기한(180일) 내에 수정 보완 후 최종 인증을 받게 된다.

3.2.2. 평가범위 지정(Scoping)

평가범위 지정은 조직內 어떤 자산이 평가 대상이 되는지를 결정하는 절차로, 평가의 효율성과 객관성을 확보하기 위한 필수 절차이다. 평가 대상 조직은 소유 정보 자산을 평가 유형(Level)에 따라 분류해야 하며, 유형에 따라 평가 대상이 달라지게 된다.

3.2.2.1. Level 1 평가범위

Level 1에서는 자산을 평가범위內 자산(Assets in Scope)과 평가범위外 자산(Asset Not in Scope)으로 분류한다.

평가범위內 자산은 FCI를 처리, 저장 또는 전송하는 정보 시스템인 FCI 자산으로, 해당 보안 요구사항 전체에 대해 평가되어야 한다. 평가 대상 조직은 FCI를 처리, 저장 또는 전송하는 환경內의 사람, 기술, 시설 및 외부 서비스 제공자(ESP)를 고려하여 Level 1 자체평가 범위를 지정해야 한다.

평가범위外 자산은 FCI를 처리, 저장 또는 전송하지 않은 조직 정보시스템으로, 평가범위에서 제외 된다. 특히, VDI(Virtual Desktop Infrastructure) 클라이언트를 호스팅하는 앤드 포인트 중, 키보드/비디오/마우스 입력 외에 FCI를 허용하지 않도록 구성한 경우, 평가범위外로 간주된다. 또한, FCI를 처리, 저장 또는 전송할 수 있지만, 완전히 보호하기 어려운 IoT 장치와 같은 특수 자산(specialized Assets)은 평가범위에 포함되지 않는다.

3.2.2.2. Level 2 평가범위

Level 2는 통제필요정보(CUI)를 보호하는 데 중점을 둔다. 평가범위內 자산은 첫째, CUI 자산(CUI Assets)이다. CUI를 처리, 저장 또는 전송하는 자산으로 NIST SP 800-171 R2에 명시된 110가지 보안 요구사항에 대해 평가를 받도록 준비하여야 한다. 나머지 범위內 자산들은 평가를 받지는 않지만 자산 목록, 시스템 보안계획(SSP), 네트워크 다이어그램에 문서화되어야 한다. ① 보안 보호 자산(Securtiy Protection Assets, SPA, CMMC 평가범위內에서 보안 기능을 제공하는 자산) ②계약자 위험 관리 자산(Contractor Risk Managed Assets, CRMA, 보안정책·절차·관행으로 인해 CUI를 처리·저장·전송할 수 있지만 이러한 행위를 의도적으로 하지 않는 자산) ③ 특수 자산(Specialized Assets)이 여기에 해당한다.

평가범위外 자산에는 CUI를 처리, 저장 또는 전송할 수 없으며, CUI 자산에 보안 보호 기능을 제공하지 않는 자산(Out-of-Scope Assets)과 VDI 클라이언트가 포함된다.

외부 서비스 제공자(External Service Provider, ESP) 범위 지정 요건은, 클라우드 서비스 제공자인 경우에는 48 CFR 252.204-7012에 명시된 FedRAMP Moderate 수준에 상응하는 보안 요구사항을 충족해야 하고, 클라우드 서비스 제공자가 아닌 ESP는 평가 대상 기관의 일부로 평가

되어야 한다. 다만, CUI를 처리하지 않는 서비스 제공자는 평가에서 제외된다. ESP를 사용하는 경우, ESP 사용과 관련된 내용이 ESP 서비스 설명 및 고객 책임 매트릭스(CRM)에 설명되어야 한다.

3.2.2.3. Levle 3 평가범위

평가범위內 자산인 CUI 자산, 보안 보호 자산, 계약자 위험관리 자산, 특수자산 모두에 대해 평가를 실시한다. 평가범위外 자산과 외부 서비스 제공자의 범위 지정 요건은 Level 2와 동일하다. Level 3 평가범위는 Level 2 CMMC 평가범위와 동일하거나 그 하위 집합이어야 한다. Level 2 인증은 Level 3 평가전에 최종 완료되어야 한다. DIBCAC는 평가범위內 모든 자산에 대해 Level 2 보안 요구 사항을 확인할 수 있으며, Level 2 보안 요구 사항이 충족되지 않는다고 판단되면 Level 3 평가 프로세스를 일시 중지, 보류 또는 즉시 종료할 수 있다.

3.2.3. SSP와 증거문서

SSP(System Security Plan)는 조직이 각 보안 요구사항을 어떻게 충족하고 있는지를 설명하는 핵심 문서로, 보안 요구사항을 개괄적으로 설명하고, 이러한 요구사항을 충족하기 위해 구현된 또는 계획된 보안 제어(Controls)를 상세히 기술하는 공식 문서이며, CMMC 평가의 출발점이 된다. SSP는 CUI를 취급하는 시스템 개요 및 보호 계획, 보안 통제 구현 상세내용, 시스템 경계 및 환경 설명, 정책 및 절차 등으로 구성된다.

Level 1 자체평가에는 SSP가 필수 요구사항은 아니지만, 모범 사례로서 권장된다. Level 2와 Level 3 평가에는 평가범위內 CUI 자산을 포함한 모든 자산에 대한 SSP가 필수적이다. SSP는 특정 형식에 강제되지 않으며, 각 조직이 자체적으로 가장 적합한 형식을 결정할 수 있다. SSP는 요구사항 충족을 설명하는 것뿐 아니라, 평가자가 다른 요구사항을 생각할 수 있는 근거를 제공하기 때문에, 평가의 난이도와 범위에 큰 영향을 미친다. SSP가 구체적이지 않거나 문서화가 미흡하면 평가자는 해당 요구사항에 대해 별도의 실사 또는 인터뷰를 요구하게 된다.

한편, 증거문서는 CMMC 평가 과정에서 보안 요구사항의 구현을 입증하기 위해 검토되거나 생성되는 자료를 의미한다. 이들은 조직의 사이버 보안 준수 상태에 대한 실질적인 증거로 제공된다. 평가 대상 조직은 평가를 지원하는 모든 증거 문서를 보유하고 해싱 하여야 한다. 해싱 된 값은 평가자에게 제공되어 eMASS에 제출된다. 이는 문서가 위조되거나 변조되지 않았음을 보장하기 위함이며, 증거문서는 최소 6년 동안 보존되어야 한다.

3.3. 정부 및 인증 생태계의 역할과 책임

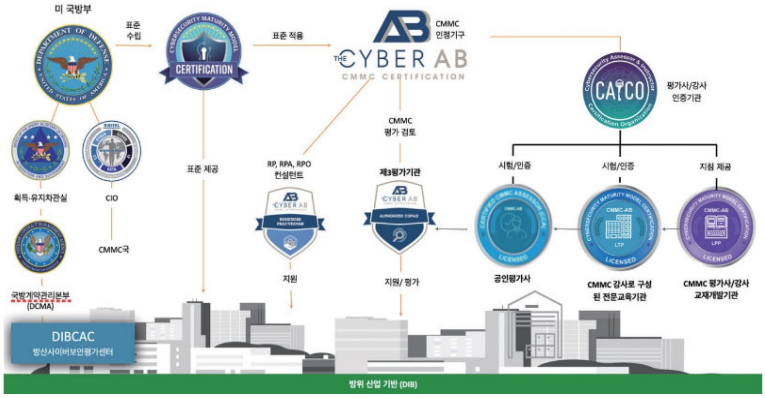


그림 1. 美 CMMC 생태계[2)]

3.3.1. DoD CIO와 CMMC PMO(Program Management Office)

美 국방부 최고정보책임자(CIO)는 CMMC 제도의 정책, 전략, 기술 기준을 총괄하는 핵심 기관으로, ①인증 수준별 요구사항 정의 ②보안 모델의 구조 수립 ③규정 개정 등을 총괄한다.

CIO 산하의 CMMC 프로그램 관리실(PMO)이 실무부서로 CMMC 프로그램에 대한 감독을 담당하며, CMMC 프로그램 정책과 구현 지침 개발 등을 책임지고 있다. 또한, CMMC AB(Accreditation Body)의 역할 수행을 모니터링하고 효과적인 수행과 관련된 문제를 해결하기 위해 필요한 조치를 취할 책임이 있다. PMO는 CMMC AB의 객관성에 영향을 미칠 수 있는 이해상충을 평가하고, 유효한 CMMC 상태에 의문이 제기될 경우 조사 및 조치를 취할 수 있다. 만약 DCMA DIBCAC 평가 결과, 준수 사항이 충족되지 않거나 유지되지 않았음이 드러나면, 이 결과는 기존 CMMC 상태보다 우선한다.

3.3.2. DIBCAC(Defense Industrial Base Cybersecurity Assessment Center)

DIBCAC는 국방부 획득 및 유지 담당 차관실(Office of the Under Security of Defense for Acquisition and Sustainment, OUSD(A&S)) 산하 기관인 국방계약관리청(Defense Contact Manatement Agency, DCMA) 소속으로 방위산업 기반(DIB) 계약자 및 하청업체가 국방부와의 계약상 요구되는 사이버보안 기준을 충족하고 있는지를 검증하는 역할을 담당하고 있다.

DIBCAC는 CMMC Level 3 인증 평가를 수행하고, 평가 결과를 eMASS에 업로드하며, Level 3 상태 증명서를 발급한다. 또한 CMMC AB와 C3PAO 정보시스템에 대한 Level 2 인증 평가도 수행한다. 평가 결과에 이의가 있으면 21일 이내에 서면으로 항소할 수 있다.

CMMC가 정식으로 시행되기 이전 DIBCAC로부터 고위 평가(High Assessment)로 인정받은 기관은 CMMC Level 2 최종 상태로 인정된다. 이는 중복 노력을 피하고 산업 및 국방부의 비용을 줄이기 위함이다.

3.3.3. CMMC AB(Accrediation Body)

CMMC AB는 국방부가 계약하는 민간 조직으로, 특정 시점에 단 하나의 업체만 인정된다. ISO/IEC 17020:2012 및 기타 관련 요구사항에 따라 평가 기관인 C3PAO를 승인하고 인증할 권한이 부여된다. 또한, C3PAO 승인 요구사항과 인증 체계를 수립하여 CMMC PMO의 승인을 받아야 한다.

CMMC AB는 미국에 기반을 두어야 하며, ISO/IEC 17020:2012 및 ISO/IEC 17024:2012 범위에서 ISO/IEC 상호 인정 협정(MRA) 서명 기관으로, ILAC(International Laboratory Accreditation Cooperation) 회원 및 IAAC(Inter-American Accreditation Cooperation)의 우수 회원 자격이 있어야 한다. 또한, FOCI(Foreign Ownership, Control, of Influence) 규정을 준수해야 하며, DIBCAC로 부터 Level 2 인증 평가를 받아야 한다.

아울러, CMMC AB는 ISO/IEC 17011:2017 및 국방부 요구사항에 부합하는 이해충돌(Conflict of Interest), 전문가 행동 강령(Code of Professional Conduct), 윤리정책(Ethics Policies)을 개발하고 유지해야 한다. 이 정책은 CMMC 생태계內 모든 개인, 단체 및 그룹에 적용된다. 또한, CMMC AB는 CAICO[3]가 ISO/IEC 17024:2012를 준수하고 모든 교육 제품, 지침 및 시험 자료의 고품질 상태를 유지하는지 확인하는 역할을 수행해야 한다.

---

2) 류화. CMMC 미국 방산 시장 진출을 위한 사이버 보안. 국방과 기술 제532호, 94. 2023.
3) CMMC Assessor and Instructor Certification Organization(CMMC 평가자 및 강사 인증 기관).

3.3.4. C3PAOs(CMMC Third-Party Assessment Organizations)

C3PAO는 CMMC AB에 의해 승인 또는 인증된 조직으로, Level 2 인증 평가를 수행하고 인증 대상기관(OSC, Organization Seeking Certification)에 CMMC 상태 증명서(Certificates of CMMC Status)를 발급할 권한을 가진다.

C3PAO는 ISO/IEC 17020:2012를 준수해야 하며, FOCI 위험 평가를 받아야 한다. 평가팀은 최소 선임 CCA와 한 명의 다른 CCA로 구성되어야 한다. CAP(CMMC Assessment Process) 문서에 기반하여 표준화된 평가를 수행하여야 하며, 평가 중립성과 기술적 역량 확보가 필수 요건이 된다.

3.3.5. CAICO(CMMC Assessor and Instructor Certification Organization)

CAICO는 CMMC 평가자(assessors), 강사(instructors) 및 관련 전문가(professionals)를 훈련, 시험, 승인, 인증, 재인증 권한이 있으며, 특정 시점에 단 한 개의 CAICO만 인정된다.

CAICO는 ISO/IEC 17024:2012를 준수해야 하며, CMMC AB의 이해충돌, 전문가 행동 강령, 윤리정책을 따라야 한다.

3.3.6. CCAs(CMMC Certified Assessors)

CCA는 Level 2 인증 평가를 담당한다. CCP 여야 하며, 최소 3년의 사이버보안 분야 경험과 1년의 평가 또는 감사 경험이 필요하다. 또한, Tier 3 신원조사나 이에 준하는 자격을 갖추어야 한다. 선임 CCA(Lead CCA)는 최소 5년의 사이버보안 분야 경험, 5년의 관리 경험, 3년의 평가 또는 감사 경험 등을 갖추어야 한다.

3.3.7. CCPs(CMMC Certified Professionals)

CCP는 CMMC 및 평가 프로세스에 대한 엄격한 교육을 이수하며, OSA(Orranization Seeking Assessment) 고객에게 조언, 컨설팅 및 권고를 제공할 수 있다. 이들은 CCA 감독하에 Level 2 인증 평가에 참여할 수 있으나, 최종 결정은 CCA의 고유 권한이다.

3.3.8. CCIs(CMMC Certified Instructiors) 및 PIs(Provisional Instructors)

CMMC 임시 강사(PI)는 2024년 12월 6일 이후 18개월 동안의 전환 기간 동안 CCA 및 CCP 후보자를 교육한다. CMMC 인증 강사(CCI)는 CCP, CCA 및 CCI 후보자를 교육하며 CMMC 교육 업무를 수행한다.

CCI는 CCP 또는 CCA 인증을 취득 및 유지하여야 해당 교육을 제공할 수 있으며, 이들은 CMMC 교육 활동 중 얻거나 생성된 모든 정보를 기밀로 유지해야 하고, 특정 이해 충돌 활동(자격 시험 개발 또는 감독 등)에는 참여할 수 없다.

3.4. CMMC 프로그램 주요 개정사항

美 국방부는 계약자가 연방 계약 정보(FCI) 및 통제필요정보(CUI)를 보호하는 데 필요한 보호 조치를 구현했는지 확인하기 위해 CMMC 프로그램을 개정하였다. 새 규정은 2024년 12월 16일부터 효력이 발생하였다.

美 CMMC 프로그램은 2019년 국방부가 '자체인증' 보안 모델에서 벗어나, 진화하는 사이버보

안 위협으로부터 국방산업기지(DIB)를 보호하기 위해 개발되었다. 2020년 9월 초기 프로그램을 구현하는 48 CFR CMMC 임시 규칙을 발표하였으며, 이는 5년 동안의 단계적 이행 기간을 설정하였다. 이 임시 규칙에 대한 약 750건의 공개 의견을 검토하여 개정 사항에 반영하였다.

최근 개정 동향과 주요 내용은 다음과 같다.

3.4.1. 프로그램 구조 및 이행

초기 이행 1단계가 6개월 연장되었으며, 새로운 분류 체계가 도입되었다. 예를 들어 평가 레벨은 Level 1(self), Level 2(self), Level 2(C3PAO), Level 3(DIBCAC)로 나누고, 그 결과는 Final Level 1, Conditional Level 2 등의 CMMC 상태로 나타낸다. 계약자는 계약 체결 전에 필수 CMMC 상태를 충족하여야 한다.

3.4.2. 평가 및 인증 프로세스

초기 모델에서는 허용되지 않았던 조건부 인증을 위한 POA&M이 허용된다. 조건부 CMMC 상태 일로부터 180일 이내에 종료되어야 한다.

Level 1은 POA&M이 허용되지 않으며, Level 2는 자체평가 또는 C3PAO를 통한 인증 평가로 충족될 수 있다. Level 3는 DIBCAC에서 수행하며, 무료로 제공된다.

Level 1 및 2 자체평가에 대한 산출물 보관 요구사항이 추가되었으며, 표준 수준을 충족한 조직의 CMMC 상태는 SPRS(Supplier Performance Risk System)에 자동으로 업데이트된다. 한편, DIBCAC의 후속 평가 결과는 기존 자체평가 또는 최종 인증 평가보다 우선하며, 규정 미준수 상태로 이어질 수 있다.

3.4.3. 역할 및 책임

조직의 지속적인 규정 준수 확인(Affirmation)을 책임자의 명칭이 기존 'Senior Official'에서 'Affirming Official'로 변경되었다. CMMC AB의 기준이 강화되었으며, 이해충돌 냉각기간이 6개월에서 1년으로 연장되었고, 컨설팅과 평가 사이의 냉각기간도 3년으로 제한되었다.

전환 기간 동안 CCP 및 CCA 후보자를 교육하기 위한 PI 역할이 추가되었으며, CCI는 자신이 교육하는 클래스의 수준과 같거나 더 높은 수준의 인증을 받아야 하고, CCA와 CCP는 Tier 3 신원조사를 완료하여야 한다.

또한, 개별 평가자는 C3PAO가 제공하는 IT, 클라우드, 사이버보안 서비스 및 엔드 포인트 장치만 사용하여야 하고 개인 소유의 IT 사용은 금지된다.

3.4.4. 정보유형 및 범위

CUI를 처리, 저장 또는 전송하지 않는 ESP는 평가에서 제외하였으며, CSP의 정의는 NIST SP 800-145를 기반하는 것으로 범위를 제한하였다. SPA(Security Protection Assets)와 SPD(Security Protection Data)에 대한 평가 요구사항을 완화하였으며, SPD에 대한 정의가 추가되었다.

COTS(Commercially Available Off-the-Shelf) 품목의 독점적인 조달을 위해 계약 및 하도급 계약은 평가가 면제되지만, 계약자의 정보시스템內에서 CUI를 처리, 저장 또는 전송하는 데 사용되는 COTS는 면제되지 않는다.

또한, 특정 구성의 VDI 클라이언트를 호스팅 하는 엔드 포인트는 평가범위에서 제외될 수 있음을 명확히 하였다.

3.4.5. 표준 및 지침

Level 2는 NIST SP 800-171 R2 전체 보안 요구사항을, Level 3은 NIST SP 800-172 Feb2021에서 선택된 요구사항을 기반으로 하였다. NIST 문서 버전을 명시하여 일관성을 확보하였으며, 추후 버전 개정 사항은 별도의 규칙 제정을 통해 적용할 예정이다.

3.5. 최근 CMMC 추진 동향

美 국방부는 CMMC 프로그램의 새로운 규정을 2024년 12월 16일부터 시행하였다. 이 프로그램은 연방계약정보(FCI)와 통제필요정보(CUI)를 보호하기 위해 계약자가 필요한 보호 조치를 구현했는지를 확인하는 것을 목표로 하며, 단계별 이행 계획을 통해 계약요청(Solicitation)과 계약 문서에 CMMC 요건을 포함할 예정이다.[1]

美 국방부의 CMMC 요건 구현 시작 목표 시점은 2025년 회계연도이다. 전체 이행 기간은 4단계로 구성되어 있으며, 이는 CMMC 평가에 따른 문제점을 해결하고, 필요한 평가자들을 훈련 시키며, 기업들이 CMMC 요건을 이해하고 구현할 시간을 제공하기 위한 것이다. 美 국방부는 모든 국방 계약업체가 CMMC 준수를 달성하는 데 약 7년이 소요될 것으로 예상하고 CMMC 프로그램을 설계하였으며, 단계별 이행 계획이 계약 유형이나 회사 규모 등에 기반하지 않고 CMMC 평가 수준 및 유형에 기반을 둠으로써, 모든 잠재적 이해관계자들에게 공정한 접근 방식이 될 것이라고 판단하고 있다.[1]

3.5.1. 1단계(Phase 1)

1단계는 CMMC 32 CFR part 170 CMMC 프로그램 규칙 또는 48 CFR part 204 CMMC 획득 규칙 중 나중에 발효되는 날부터 시작한다. 기존 6개월에서 1년간으로 연장되었다.

이 단계에서는 Level 1(자체평가) 또는 Level 2(자체평가) 상태 요건을 계약 체결 조건으로 포함할 예정이다. 다만, 美 국방부 재량에 따라 제도 유효일 이전에 체결된 계약의 경우에도 옵션 기간 행사 조건으로 Level 1(자체평가) 또는 Level 2(자체평가) 상태 요건을 포함할 수 있으며, Level 2(자체평가) 대신 Level 2(C3PAO) 상태 요건을 계약에 포함할 수 있다.

3.5.2. 2단계(Phase 2)

2단계는 1단계 시작일로부터 1년 후에 시작된다. 1단계 요구사항에 더해, 적용 가능한 계약 요청과 계약 문서에 계약 체결 조건으로 Level 2(C3PAO) 상태 요건을 포함한다. 다만, 美 국방부 재량에 따라 Level 2(C3PAO) 상태 요건의 포함을 계약 체결 조건 대신 옵션 기간으로 연기할 수 있으며, Level 3(DIBCAC) 상태 요건을 계약요청과 계약 문서에 포함할 수도 있다.

3.5.3. 3단계(Phase 3)

2단계 시작일로부터 1년 후에 시작된다. 1단계와 2단계 요구사항에 더해, 모든 적용 가능한 계약요청과 계약 문서에 계약 체결 조건으로 Level 2(C3PAO) 상태 요건을 포함할 예정이며, 유효일 이후 체결된 계약의 옵션 기간 행사 조건으로도 포함할 예정이다. 또한, 모든 적용 가능한 계약

에 계약 체결 조건으로 Level 3(DIBCAC) 상태 요건을 포함할 예정이다. 다만, 美 국방부 재량에 따라 Level 3(DIBCAC) 상태 요건의 포함을 계약 체결 조건 대신 옵션 기간으로 연기할 수 있다.

3.5.4. 4단계(Full Implementation)

3단계 시작일로부터 1년 후에 시작된다. 이 단계부터 4단계 시작일 이후에 체결된 계약의 옵션 기간을 포함하여 모든 적용 가능한 계약요청과 계약 문서에 CMMC 프로그램 요구사항을 포함할 것이다. 다만, 이 단계에서도 적절한 경우에는 자체평가가 허용된다.

4. CMMC 대응 정책방안

4.1. 해외 대응 사례

일본 정부는 CMMC 제도 시행에 대응하기 위해 방위산업체 중심의 포괄적인 사이버 보안 정책을 수립하고 있다. 특히, 일본 경제산업성는 2024년 4월 5단계 사이버 보안 등급 제도를 발표하였으며, 2025년 회계연도부터 본격 시행할 예정이다. CMMC의 등급체계와 유사한 구조를 가지고 있으며, 평가 기준도 미국 NIST SP 800-171/172에 기반을 두고 있다.

또한, 일본 방위장비청은 2025년 6월, NIST SP 800-171에 부합하는 '장비 등 서비스 조달의 정보 보안 기준'을 정비하였다. 이는 방위산업 공급망을 통해 사실상의 CMMC 준비 단계로 평가할 수 있으며, 미국과의 상호 인정을 고려한 정책이라 하겠다.

이스라엘은 NIST SP 800-171을 전면 채택하고 이스라엘 자체적으로 평가사를 육성하기 위한 계획을 추진하고 있으며, 영국은 미국과 사이버보안 준수에 관한 접근 방식을 통일하기로 하고 서로의 평가 방식을 참관하며 협력하고 있다.[2]

4.2. 국내 관련 제도와 한계점

우리나라의 경우 방위산업 관련 기밀 및 방위산업기술 보호를 위해 '방산보안측정' 제도와 '통합실태조사' 제도를 운용중에 있다.[3]

이들 제도와 CMMC는 방산 기술 관련 중요 정보의 보호를 위해 운영한다는 공통점을 가지고 있지만, 주요한 차이점은 다음과 같다. 첫째, CMMC는 사이버 위협에 대응한 계약업체의 정보시스템 보호가 주요 목적이며 일부 시설과 인원 보안 내용을 포함하고 있지만, 보호 대상은 통제필요정보(CUI)를 다루는 계약업체의 정보시스템으로 한정되어 있는 반면, 국내 2개 제도는 문서, 시설, 인원, 정보통신 등 대상기관 자산 전반에 대한 보호를 목적으로 하고 있다.

둘째, CMMC는 프로그램에 대한 정책 수립은 美 국방부가 주도하지만 실제 현장 행위자들은 Level 3(DIBCAC) 평가 등 일부 기능을 제외하고는 대부분 민간 주도로 이루어지는 반면, 우리의 경우에는 정책에서부터 현장 평가에 이르기까지 정부 기관이 주관하고 있다.

셋째, CMMC와 통합실태조사는 정보통신 분야 평가항목에 차이가 있으며, CMMC 통제항목 110개 중 중복성을 배제하면 순수 항목 19개(17.3%)를 충족하지 못하고 있다.[4]

국내 제도의 한계점은 다음과 같다. 첫째, 협력업체를 통한 보안 사각지대 발생 우려이다. 정기적으로 실시하는 통합실태조사는 2022년 기준 85개 방산업체 및 국과연, 기품원 등 정부출연기관에 대해 국내 및 해외사무소를 포함한 약 160여 개의 사업장을 매년 약 10개월간 실시하고 있으나, 현재 조사관 인력 부족으로 협력업체까지는 직접 점검을 못하고 있는 실정이다.[4] 반면, CMMC는 主 계약업체뿐만 아니라 계약과 관련된 협력업체의 보안 평가를 기본으로 하고 있으며,

보안 위협은 협력업체라고 해서 달라지지 않는다는 원칙을 고수하고 있다. 이러한 원칙은 핵심 임무와 기능을 성공적으로 수행하는 국방부의 능력에 직접적인 영향을 미칠 수 있다는 판단에 근거하고 있다. 실례로, 국가 지원 해커와 사이버 범죄조직은 방산업체와 그 협력업체를 집중적으로 공격하고 있으며, 최근에도 Blue Yonder(공급망, 2025년)과 ENGlobal(방산 협력업체, 2024년 12월) 랜섬웨어 공격이 미국에서 큰 이슈가 되었다.[5]

둘째, 미국 수출 방산업체의 이중 평가 부담이다. 현재 국내에는 80여 개의 방산업체뿐만 아니라 2,000개 이상의 하청업체들이 있는 것으로 추정되며,[6] 이들 중 미국 수출 계약에 관련된 업체들은 CMMC 인증을 받아야 한다. 이는 통합실태조사와 CMMC를 동시에 준비해야 하는 부담으로 작용하게 될 것이다.

셋째, CMMC의 평가 인증이 민간 주도로 시행되는 반면, 국내 제도들은 아직도 정부기관이 직접 수행하는 방식을 채택하고 있다. 민간 주도의 시행은 시행 초기에 국내 전문 기관과 인력을 확충해야 하는 등 준비가 필요하지만, 장기적으로는 우수 보안 인력과 기업을 양성하는 기회와 함께 관련 산업을 활성화하는 촉매제가 될 것이다.

4.3. 대응방안 3가지 모델

美 국방부는 CMMC를 본격 시행하고, 단계적으로 평가 수준을 올릴 예정이다. 이에 따라 미국 수출을 준비하는 국내 방산업체는 CMMC를 준비해야 하는 어려움과 함께 국내 제도에 따라 시행하는 통합실태조사에도 대응해야 하는 이중고에 직면하고 있다.

본 논문에서는 CMMC에 대응하는 우리 정부의 정책방안에 대해 3가지 모델을 제시하고, 이에 대한 이해관계자들의 의견을 조사하였다. 대안 모델은 다음과 같다.

첫째, 美 CMMC 제도를 전면 도입하는 방안이다. 미국 제도를 그대로 수용하여 국내 방산 계약에도 美 CMMC 인증을 요구하는 대신, 통합실태조사에서 정보통신 보안 항목은 면제해 주는 방식이다. 사이버 위협은 국경의 범위를 넘어서는 글로벌 공동 위협이며, 이에 대한 대응에 국가별 차이는 중요한 요소가 아닐 수 있다. 전체적인 방산기업들의 사이버 보안 수준의 향상을 기대할 수 있으며, 수출 기업 입장에서는 이중 평가의 부담을 피할 수 있는 장점이 있으나, 非 수출 기업의 경우에도 CMMC를 준비해야 하는 부담이 발생할 수 있다.

둘째, 美 CMMC 제도를 부분 도입하는 방안이다. 첫째 방안을 대기업 또는 수출 기업에 우선 적용하고 단계적으로 확대하는 방식이다. 중소업체의 부담을 줄여주는 장점은 있으나, 보안 사각지대가 발생할 가능성이 존재한다.

셋째, 美 CMMC와 유사한 국내 제도(이하 K-CMMC)를 별도로 개발하는 방안이다. 평가는 NIST SP 800-171에 근거하여 자체 제도를 개발하고, 미국과의 상호인증협약(MRA)을 체결을 추진하는 방식이다. 이는 사이버안보 주권을 확보할 수 있으며, 국내 관련 산업을 육성하고 전문 인력을 양성할 수 있음을 물론, 업체의 평가 비용도 절감할 수 있는 등 장점을 가지고 있으나, 미국과의 상호인증협약이 난제로 남을 수 있다.

4.4. 설문결과 분석

4.4.1. AHP 설문 설계

CMMC 시행에 대한 최적의 대응 방안을 선정하기 위해 AHP 방식을 채택하였다. 목표는 '美 CMMC 시행에 따른 대응 방안'으로 정하고, 대안으로는 (A1) 美 CMMC 제도 전면 도입, (A2) 美 CMMC 제도 부분 도입, (A3) 국내 제도(K-CMMC) 개발 3가지를 선정하였다. 대안을 선정하는

기준으로는 (C1) 사이버 보안 강화, (C2) 경제적 효율성, (C3) 국내 적합성, (C4) 국제협력, (C5) 조직 및 인적 자원으로 정하였다. 이들 기준은 학계와 산업계 CMMC 전문가들의 의견을 반영하여 AHP 분석에 적합하게 선정하였으며, 1次 설문을 통해 적정성을 검증하였다.

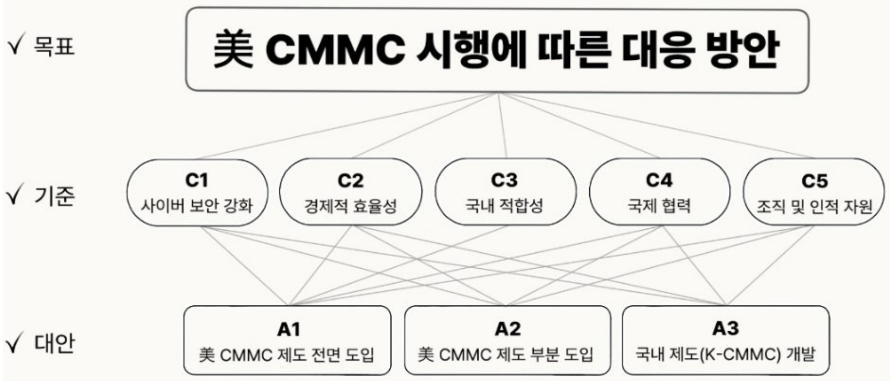


그림 2. AHP 분석 체계도[4)]

4.4.2. 결과 분석

설문은 1次와 2次로 구분하여 실시하였다. 1次에서는 기준 5개에 대한 적정성에 대하여 전문가 28명에 대해 조사를 실시하였으며, 24명(85.7%)이 적절하다는 의견을 주었다.

2次 설문은 AHP 분석을 위한 쌍대 비교 설문으로 실시하였으며, 참여한 총 29명 중 일관성 검증을 통과한 23명에 대한 결과는 다음과 같다.[5)]

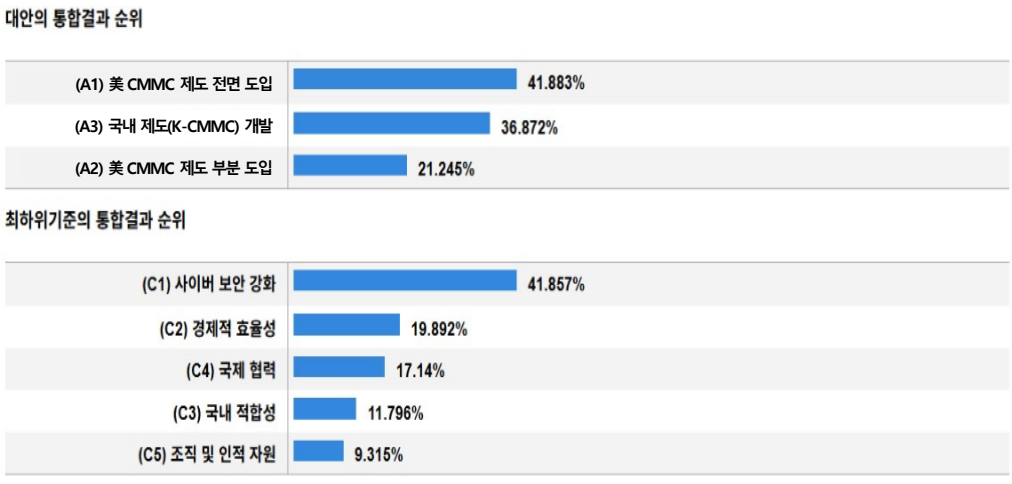


그림 3. AHP 분석 결과[6)]

설문 응답자들은 CMMC 제도를 국내에 도입할 때 고려하는 5개 기준 중 '(C1) 사이버 보안 강화'를 가장 중요한 기준(41.9%)으로 의견을 주었다. 2번째 순위인 '(C2) 경제적 효율성(19.9%)'에

4) 김병욱의 의사결정계층(AHP) 분석방법(킴스정보전략연구소, 2015)을 참고하여 작성.
5) 2次 설문 응답자 수 23명은 정책 연구에 활용될 수 있는 표본 크기이지만, 다소 제한적인 숫자로 결과의 일반화에 한계가 있을 수 있으므로 해석에 주의가 필요함.
6) 디시전 사이언스(社) 'MAKE IT' AHP 분석 도구를 활용한, Ideal Mode(이상적 모드) 분석 결과.

비해서도 큰 차이를 보이고 있다. 다음으로 '(C4) 국제협력(17.1%)', '(C3) 국내 적합성(11.8%)', '(C5) 조직 및 인적 자원(9.3%)' 순으로 기준의 중요도를 판단하였다.

이는 최적 대안 선정 결과에 영향을 미쳐, '(A1) 美 CMMC 제도 전면 도입(41.9%)', '(A3) 국내 제도(K-CMMC) 개발(36.9%)', '(A2) 美 CMMC 제도 전면 도입(21.2%)'의 순으로 결과가 나왔다.

상위 두 개의 대안을 기준별로 분석해 보면, '(A1) 美 CMMC 제도 전면 도입' 방안이 '(A3) 국내 제도(K-CMMC) 개발' 방안에 비해 '(C1) 사이버 보안 강화' 기준에 대해서 1~9 크기 중 2.583 정도의 크기로 더 많이 충족한 다는 결과를 보였다. 또한, '(C4) 국제협력' 기준에서도 '(A1) 美 CMMC 제도 전면 도입' 방안이 '(A3) 국내 제도(K-CMMC) 개발' 방안에 비해 6.890로 크게 앞서는 결과가 나왔다.

한편, '(C3) 국내 적합성' 기준에서는 '(A3) 국내 제도(K-CMMC) 개발' 방안이 '(A1) 美 CMMC 제도 전면 도입' 방안에 비해 5.158 정도의 크기로 앞서는 결과가 나왔으며, '(C2) 경제적 효율성'과 '(C5) 조직 및 인적 자원' 기준에서도 '(A3) 국내 제도(KCMMC) 개발' 방안이 '(A1) 美 CMMC 제도 전면 도입' 방안에 비해 각각 3.256과 4.671로 앞섰다.

5개 기준 모두를 다른 대안에 비해 우월하게 충족시키는 하나의 대안은 없다는 점과, 어느 하나의 방안으로 추진하는 방식이 비교적 명확한 장단점을 가진다는 점을 고려 시, '(A1) 美 CMMC 제도 전면 도입'과 '(A3) 국내 제도(K-CMMC) 개발' 두 방안을 절충하는 방식으로 추진하는 것이 바람직하다는 결론을 도출할 수 있다.

4.5. 2-Track 정책방안 제안

설문 분석 결과에서 보듯이, '美 CMMC를 직접 도입하는 방식'과 '국내 제도(K-CMMC)를 개발'하는 방안은 어느 하나의 방안으로만 추진하기에는 서로 간에 장단점을 내포하고 있다.

첫째, CMMC를 직접 도입하는 방식은 미국의 선진 평가 제도를 그대로 도입할 수 있는 장점이 있다. 오랜 준비 기간을 거쳐 만든 합리적인 제도를 적은 비용으로 적용할 수 있으며, 특히, 국가 간의 대응에 차별성이 크지 않은 사이버 보안 분야에서는 선진 제도를 그대로 도입하는 것에 대한 부작용도 크지 않을 것으로 생각된다. 다만, "미국의 제도와 평가 기관에 의존하게 되어 우리의 사이버안보 주권이 위협받게 된다."는 우려가 있는 것도 사실이다.

둘째, K-CMMC 제도를 독자 개발하는 방식은 일본을 비롯한 여러 국가에서 이미 추진하고 있는 방안으로, 국내에 자체적인 민간 생태계를 조성할 수 있는 기회가 된다. 그러나, 가장 큰 전제 조건인 '미국과의 CMMC 상호인정협약(MRA) 체결'을 성사시켜야 하며, 이를 위해서는 미국이 받아들일 수 있는 정도의 평가 기준과 절차를 마련해야 하는 선결 조건이 있다.

본 논문에서는 이 두 가지 방안을 함께 시행하되, 정부는 두 평가 제도 시행을 위한 국내 민간 생태계 조성을 지원하고, 기업은 두 가지 방안 중 하나를 선택하여 국내 방산 계약의 자격을 획득하는 2-Track 방식을 제안하고자 한다. 그 이유는 첫째, 위에서 살펴본 바와 같이 뚜렷한 장단점을 가진 정책 중 어느 하나만을 선정하여 시행하는 방안은, 정책 실행에 있어 위험 요소를 내재하고 있다. 우선 '美 CMMC를 직접 도입하는 방식'을 선정할 경우 우리의 사이버안보 주권이 위협받을 수 있으며, 국내 방산업체의 사이버 보안이 미국이라는 글로벌 패권국가 제도에 의존하게 된다는 비판에 직면할 수 있다. 한편, '국내 제도(K-CMMC)를 개발'하는 방안은 '미국과의 CMMC 상호인정협약(MRA) 체결'을 성사시켜야 하는 현실적인 어려움에 처할 수 있다. 만약 미국과의 협약이 지연되거나 불가할 경우 미국 수출을 준비하는 기업의 입장에서는 미국과 국내의 평가를 둘 다 준비해야 하는 이중 부담을 안게 된다.

둘째, 이 두 가지 방안은 서로 배타적으로 어느 하나만을 운용할 필요성이 없다는 점이다. 각 방안은 각기 독립적으로 운용될 수 있으며, 기업은 필요성과 경제성을 비교하여 두 개의 평가 제도 중 하나를 선택하여 인증을 받을 수 있다. 두 가지 방안 모두 방산업체 정보시스템의 보안 수준을 객관적으로 검증할 수 있으며, 기업 입장에서도 자신들에게 유리한 제도를 자율적으로 선택할 수 있는 유연한 선택권이 주어지게 된다. 이에 2-Track 방식을 제안하고, 이를 위해 우선적으로 시행해야 하는 정책 방향을 다음과 같이 제시한다.

4.5.1. 민간 주도 평가 생태계 조성

우선, K-CMMC 제도를 독자 개발하고 정착시키기 위해서는 무엇보다 국내 맞춤형 생태계 조성이 시급하다. 정부의 참여를 프로그램의 기획과 운영 기관에 대한 적절성 검증으로 범위를 한정하고, 민간에서 자율적으로 평가와 인증 업무를 수행할 수 있도록 생태계를 지원하는 방식의 정책을 시행하여야 한다.

이에 대한 이유는 첫째, 정부 기관이 방산업체와 협력업체 평가 업무를 전담하여 수행할 수 있는 충분한 자원을 가지고 있지 못하기 때문이다. 현재 통합실태조사에도 중소업체와 협력업체에 대한 정부 평가는 인원 등 자원 부족으로 제대로 수행하지 못하고 있다. 둘째, 이러한 민간 주도 생태계 조성을 통해 관련 산업 진흥과 보안 전문가 양성의 기반을 마련할 수 있다. 이를 통해 방산업체의 보안 수준 향상과 함께 국내 보안산업의 활성화도 기대할 수 있다.

이를 위해 美 CMMC AB와 유사한 조직을 선정, 전체 평가 인증 제도를 운용하면서 민간 평가기관에 대한 자격을 심사하는 기능 등을 부여하고, 이 기관을 통해 민간 자율 생태계가 운영될 수 있게 하여야 한다. 정부는 이러한 운영 기관과 평가 기관이 갖추어야 할 조건을 사전에 정의하고, 공정하고 합리적으로 제도가 운용될 수 있도록 하는 감독 역할에 집중하여야 한다.

다음으로, 美 CMMC 평가를 준비하는 기업에 대한 적극적인 지원이 필요하다. 관련 공공기관을 통해 CMMC 제도에 대한 충분한 컨설팅과 안내를 시행해야 한다. 또한 미국과의 협상을 통해 국내 보안업체가 C3PAO 자격을 취득하기 용이하게 하는 여건을 만들고, 국내 보안 전문가들이 CCA, CCP 자격증을 취득할 수 있도록 지원하는 제도와 환경 구축이 필요하며, 자금 여력이 없는 영세 협력업체들의 CMMC 평가를 지원하는 방안도 마련되어야 한다.

4.5.2. 방산 계약과의 연계

2024~2025년 사이 북한의 대표적인 해킹 조직이 국내 방산기술 탈취를 목표로 최소 1년 6개월 이상 전방위 공격을 감행한 사실이 수사로 확인되었다. 이 기간 동안 방산업체 10여 곳 이상이 해킹 피해를 입었으며 방산 협력업체와 IT 유지 보수 업체까지 공격 대상으로 확대되는 추세이다.[8]

이에, 국내 방산 계약 시 K-CMMC 또는 美 CMMC 인증을 받은 업체(협력업체 포함)에 한해 계약을 체결하는 제도가 필요하다. 이는 CMMC 프로그램의 핵심 내용이며, 공급망 공격을 포함한 사이버 위협으로부터 방산기술을 보호하기 위한 최소한의 조치이다.

현재 통합실태조사는 협력업체에 대해 직접적인 조사를 실시하지 못하고 있으며, 평가 우수업체에 대해서 무기체계 제안서 평가 시 가점 부여 및 표창 수여를 하고, 미흡 사항 등에 대해서는 이행 여부를 추적하여 시정명령 등 행정조치를 실시하고 있다.[4]

이러한 미온적인 조치로는 사이버 위협에 지속 노출될 가능성을 높이게 된다. 美 CMMC 프로그램과 같은 방식으로 제도를 개정하여, 협력업체를 포함하여 평가에서 인증받지 못한 기업은 계약에 참여하지 못하게 하거나 계약을 취소하는 강력한 조치가 필요하다.

4.5.3. 통합실태조사 일부 면제

K-CMMC나 美 CMMC 인증을 통과한 업체는 통합실태조사에서 일부 항목을 면제 시켜주는 제도가 필요하다. CMMC는 통제필요정보(CUI)를 다루는 계약 업체의 정보시스템의 보안상태가 안전하다는 것을 인증하는 제도로, 통합실태조사의 정보보호 항목 점검에 해당한다.

따라서 CMMC 평가를 통과한 업체는 정보보호 항목에 대한 점검을 면제해 주거나, 서류 조사만 실시하는 방식으로 개편되어야 한다. 이는 업체의 이중 평가 부담을 해소하고, 통합실태조사 기관의 인적 부담도 해결할 수 있다.

이와 함께, 통합실태조사의 정보보호 항목에 대한 전향적인 검토도 고려해 보아야 한다. 사이버라는 글로벌 공통 환경에서 자국의 특수성을 고집하기보다는, 유연한 자세로 합리적이고 객관적인 통제항목으로 수정할 필요성이 있다. 일본이 미국의 NIST 표준을 기반으로 평가 항목을 조정한 이유도 여기에 있다고 할 것이다.

5. 결론

본 논문에서는 美 국방부가 사이버 위협으로부터 방산업체 정보시스템을 보호하기 위해 시행 중인 CMMC 프로그램에 대응하기 위한 2-Track 정책 방안을 제안하였다. 국내에도 美 CMMC와 유사한 독자적인 평가 제도(K-CMMC)를 개발 시행하는 방안과, 美 CMMC 평가 제도를 직접 도입하는 방안을 절충하여 시행하는 방식이다.

이를 위해서는 독자적인 평가 제도 운용을 위한 민간 주도 평가 생태계를 빠른 시간에 조성하는 한편, 美 CMMC 평가를 준비하는 기업에 대한 적극적인 지원도 시행하여야 한다. 또한, 국내에서 독자 개발한 평가나, 美 CMMC 평가를 통과한 업체에 한하여 계약을 체결할 수 있도록 관련 제도를 강화하여야 하며, 평가를 통과한 업체에 대해서는 통합실태조사 일부 항목을 면제해 주는 인센티브도 필요하다.

美 CMMC 프로그램은 금년부터 단계적으로 시행될 예정이며, 각 단계에 맞춘 발 빠른 정책방안 수립과 시행이 필요하다. 일본을 비롯한 여러 국가들은 우리보다 한발 앞서 준비하고 있으며, 우리 정부도 지속적인 관심과 함께 적시의 대책을 내놓아야 할 것이다.

현재 방사청에서도 CMMC에 관심을 가지고, 여러 가지 방안들을 마련하고자 하는 것으로 알고 있다.[9][10] 방사청의 '2025년도 방위산업기술보호 시행계획'에 따르면, 정부는 미국 사이버 보안 인증 제도(CMMC)의 단계적 시행에 맞추어 한국 방위산업기술 사이버 보안 인증 제도(가칭)를 도입하고, 이러한 인증 제도에 대해 미국과 상호인정협정을 추진하고자 한다.[9]

또한, 인증 제도 운용을 위해 국방부 및 방사청이 정책 추진 주체가 되고, 통합실태조사심의위원회를 두어 인증기관의 역할을 수행하며, 기품원과 방산기술보호센터를 심사기관으로 하는 방식으로 계획(안)이 작성되었다.[9]

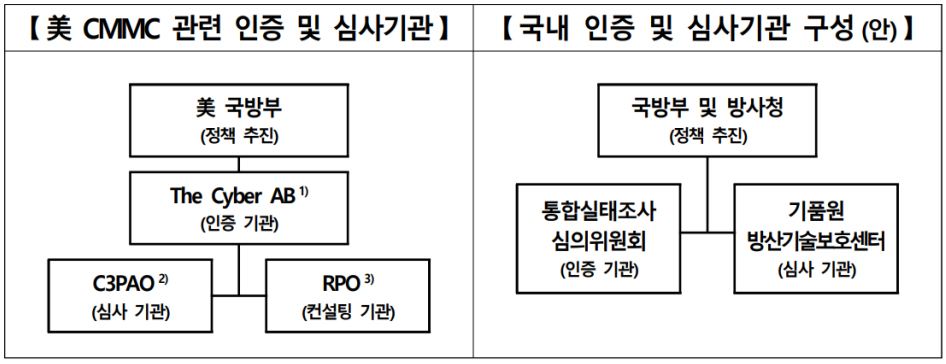
아직까지 구체적인 계획에 대한 확인은 어려우나, 시행계획에 나온 내용을 위주로 살펴보면 정부기관이 정책 추진부터 평가 및 인증까지 전체 과정을 주도하여 수행하는 방식이다. 이러한 방식은 현재 시행하고 있는 통합실태조사의 확장 버전으로 다음과 같은 문제점이 예상된다.

첫째, 지금도 부족한 평가 인원 문제가 해결되지 않고, 오히려 더 많은 공공기관 인원을 필요로 한다. 협력업체를 포함한 평가가 원활하게 진행할 수 있을 정도로 심사 기관으로 예정된 기품원과 방산기술보호센터 인원을 늘리는 것은 공공기관 비대화 등의 문제들을 발생시킬 수 있다. 또한, 통합실태조사 심의위원회의 성격도 모호하다. 계획안에 따르면 이 위원회가 인증기관으로 되어 있는데 이러한 인증기관으로서의 기능을 수행하기 위한 자격 요건과 구성원 그리고 권한에 대한 세부

정의가 필요하다고 하겠고, 이러한 인증기관을 운영하기 위해 추가적인 공공 인력이 필요한 것이 아닌지 하는 자연스러운 우려가 생길 수밖에 없다.

둘째, 이러한 방식으로는 미국과의 상호인증협약(MRA)이 이루어지기도 힘들 것으로 예상된다. 미국은 CMMC 평가 기관과 평가자에 대한 국제표준 준수, 시험 평가, 관련 경력, 교육 이수 등 엄격한 조건을 요구하고 있다. 단순히 공공기관을 평가 기관으로 지정하고 구성원들이 평가자가 되는 방식으로는 미국이 상호인증 대상으로 인정하기에 부족할 것이다. 美 CMMC 제도에 상응할 만큼 정교하고 객관적인 국내 제도 마련이 상호인증 협약을 위한 선결 조건으로 필요하다고 하겠다.

셋째, 국내 보안업체 육성과 전문가 양성을 위해 서는 정부 주도보다는 민간 자율 생태계 조성이 필요하다. 민간 주도의 평가 생태계가 조성되어야, 국내 보안산업을 활성화하고 국가 경제 발전에도 이바지할 수 있을 것이다. 정부는 민간 생태계의 운용 정책을 수립하고, 이 정책이 올바르게 운용될 수 있도록 감독 역할에 집중하는 것이 더 바람직하다는 의견이다.



1) The Cyber AB (Accreditation Body) 2) C3PAO (CMMC 3rd Party Assessment Organization)
3) RPO (Registered Provider Organization)

그림 4. 한국형 사이버 보안 인증제도(안)[7]

본 논문에서는 방산수출 세계 10위권에 진입하는 K-방산 중흥기에, 고도로 진화하고 있는 사이버 위협으로부터 우리 방산기술을 지켜내고, 해외에서 안전한 장비로 인정받으며, 수출과 국내 경제 발전에도 도움이 되었으면 하는 목적으로 몇 가지 정책 방안을 제시하였다.

설문조사 유효 응답 인원의 제한적인 숫자로 인한 일반화의 한계 등 아쉬운 부분이 있으나, 추가적인 후속 연구를 기대하며 본 논문을 마치고자 한다.

참고문헌

[1] DOD Office of the Secretary. Federal Register, Vol 89, No. 199 Rule and Regulations.

[2] 류화. CMMC 미국 방산 시장 진출을 위한 사이버 보안. 국방과기술, 제532호. 2023.

[3] 원동훈 등. 미 CMMC 제도와 한국 방산보안 대응방안. 국방과 보안, 제5권 제1호, pp. 68-93. 2023.

[4] 김동선, 류연승. 미국 CMMC 제도 대응을 위한 통합실태조사 제도 개선 연구. 한국방위산업학회지, 제29권 제3호, pp.52~57. 2022.

[5] Cyber Management. Major Cyber Attacks, Data Breachs, Ransomeware Attacks. https://www.cm-alliance.com/cybersecurity-blog/december-2024-major-cyber-attacks-data-breaches-ransomware-attacks/ (검색일 2025. 6. 7).

7) 방사청. 2025년도 방위산업기술보호 시행계획. 2024.

[6] Staista. Number of defense contractors in South Korea in 2025. https:// www.statista.com/statistics /1365407/south-korea-defense-contractors-by-sector/ (검색일 2025. 6. 21).
[7] 류연승. 방위산업 사이버안보 주권을 지키자. 보안뉴스 칼럼. https://www.boannews.com/media/view.asp?idx=106297 (검색일 2025. 7. 5).
[8] 디지털데일리. 작년 해킹 80%는 북한발, 방산의 ㅂ만 들어가면 다 턴다. https://m.ddaily.co.kr/page/view/20250418163821306 56/ (검색일 2025. 7. 5).
[9] 방사청. 2025년도 방위산업기술보호 시행계획. 2024.
[10] 방사청. 2017~2021 방위산업기술보호 종합계획(안). 2016.
[11] 김병욱. 의사결정계층(AHP) 분석방법. 킴스정보전략연구소. 2015.
[12] NIST. NIST SP 800-171r2. 2024.
[13] DOD CIO. CMMC Level 1 Self-Assessment Guide. 2024.
[14] DOD CIO. CMMC Level 2 Guide. 2024.
[15] DOD CIO. CMMC Level 3 Assessment Guide. 2024.
[16] DOD CIO. CMMC Model Overview. 2024.
[17] DOD CIO. CMMC Level 1 Scoping Guidance. 2024.
[18] DOD CIO. CMMC Level 2 Scoping Guidance. 2024.
[19] DOD CIO. CMMC Level 3 Scoping Guidance. 2024.
[20] DOD CIO. CMMC Alignment to NIST Standards. 2025.
[21] DOD CIO. Supplier Performance Risk System. 2025.
[22] DOD CIO. Introduction to the CMMC eMASS. 2025.
[23] DOD CIO. FedRAMP Authorization and Equivalency. 2025.
[24] DOD CIO. CMMC Level Determination. 2024.
[25] 32 C.F.R § 170(CMMC Program).
[26] 48 C.F.R § 204(CMMC Acquisition Rule).
[27] 日 방위장비청. 방위 산업 사이버 보안 기준. 2023.