논문접수 2022.11.19 | ISSN 1738-6144 | Journal of The Korea Association of Defense Industry Studies Vol. 29, No. 3(2022)
논문확정 2022.12.19 | http://journal.kadis.or.kr/ | 한국방위산업학회지 제29권 제3호 | http://doi.org/10.52798/KADIS.2022.29.3.4

미국 CMMC 제도 대응을 위한 통합실태조사 제도 개선 연구

A study on the improvement of the integrated real state investigation system for coping with the US CMMC system

김동선*, 류연승**
Dong-Sun Kim*, Yeon-Seung Ryu**

ABSTRACT

Recently, thanks to the rapidly growing K-defense industry, Korea's defense industry is rising as one of the world's top 10 powerhouses, and insider information leakage and cyber hacking attacks targeting core defense industry technologies are continuously increasing. The need for defense technology protection is increasing. In response, the government enacted the Defense Industrial Technology Protection Act and conducted annual integrated fact-finding surveys on defense companies to check their cyber security systems. Meanwhile, the US government, which holds the leadership in the defense industry market, is threatening the growth of the domestic defense industry by implementing the CMMC (Cyber Security Maturity Model Certification) system and planning to require CMMC certification from companies in other countries. In this paper, an integrated fact-finding survey improvement model was designed through the analysis of the integrated fact-finding survey checklist and CMMC control items that investigate the cyber security reality of the defense industry, and a solution was proposed for elements not included in CMMC, and the CMMC system was implemented in Korea. Suggested countermeasures for a soft landing. The government and academia are reviewing various policy measures to respond to the US CMMC, such as preparing the K-CMMC certification system. Therefore, this study is expected to help settle the K-CMMC system in the future.

초 록

최근 급속도로 성장하는 K-방산에 힘입어 우리나라 방위산업이 세계 10위권 내 강국으로 도약하는 등 위상이 날로 높아가고 있는 시점에 방위산업 핵심기술을 노리는 내부자 정보유출 및 사이버 해킹 공격이 지속 증가하고 있어 방산기술보호의 필요성이 증대하고 있다. 이에 정부에서는 방위산업기술보호법을 제정하는 한편 방산업체를 대상으로 매년 통합실태조사를 시행하며 사이버보안 체계를 점검하고 있다. 한편, 방산시장의 주도권을 쥐고 있는 미국 정부에서는 CMMC(사이버보안 성숙도 모델 인증) 제도를 시행하고 다른 국가 기업에도 CMMC 인증을 요구할 예정으로 국내 방위산업 성장에 큰 위협으로 다가오고 있다. 본 논문에서는 방위산업의 사이버보안 실태를 조사하고 있는 통합실태조사 점검항목과 CMMC 통제항목 분석을 통해 통합실태조사 개선 모델을 설계하고 CMMC에 미포함하는 요소에 대한 해결 방안을 제시하였으며 CMMC 제도가 우리나라에 연착륙할 수 있도록 대응방안을 제안하였다. 정부와 학계에서는 K-CMMC 인증제도 마련 등 미국 CMMC에 대응하기 위한 정책 방안을 다각적으로 검토중에 있다. 따라서, 본 연구는 미래 K-CMMC 제도 정착에 도움을 줄 것으로 기대한다.

Key Words : Defense company(방산업체), Integrated fact-finding survey(통합실태조사), CMMC(사이버보안 성숙도 모델 인증), Defense industry technology protection(방위산업기술보호), K-CMMC(한국형 사이버보안 성숙도 모델 인증)

* 김동선, 명지대학교 대학원 방산안보학과 박사과정(주저자)
** 류연승, 명지대학교 대학원 방산안보학과 교수(교신저자, E-mail: ysryu@mju.ac.kr)

Ⅰ. 서론

우리나라는 무기 수입국에서 세계 10위권 내 방산 수출국에 진입하는 등 방위산업이 크게 발전하고 있다. 국방기술진흥연구소가 발간한 「2021 국가별 국방과학기술 수준조사서」에 따르면 우리나라 국방과학기술은 세계 9위로 평가되고 화포, 지휘통제, 유도무기 기술은 선진국 수준에 이르고 있다. 선진국 수준의 국방기술이 해외로 유출되지 않도록 정부는2015년에 방위산업기술보호법을 제정하고 2018년에 8대 분야 45개 분류 123개 기술을 보호해야 할 방위산업기술로 지정·고시하였다. 또한, 방위산업기술보호지침을 제정하고 방위산업기술보호법상의 실태조사와 방위산업보안업무훈령상의 보안감사 업무를 통합하여 2019년부터 통합실태조사를 시행하게 되었다. 최근에는 사이버 취약점 진단사업, 긴급·수시 실태조사 등 지속적인 보호대책을 강구하고 있다.

한편, 세계 최고의 방산수출국이며 기술 주도권을 쥐고 있는 미국에서는 무기 등 전략물자를 미국 국방부에 납품시 CMMC(CyberSecurity Maturity Model Certification) 제도를 모든 국가에 적용할 예정으로 방산수출에 날개를 펴고 있는 현시점에서 자칫 보안관리 신뢰성 하락으로 수출에 차질이 생길까 우려되고 있다. [1, 2]에서는 「방산사이버보안 인증제도(가칭 K-CMMC)」를 구축하고 선제적으로 미국의 CMMC와 상호인정 협정을 추진해야 방산 사이버안보 주권을 지킬 수 있다고 하며 이와 같은 계획이 추진되려면 관련 국내 법령·제도 개정 및 방산업체의 K-CMMC 인증 구축을 지원하기 위한 조직과 예산도 확보해야 한다고 해법을 제시하고 있다.[1][2]

본 연구에서는 향후 우리나라가 수용해야 할 미국 CMMC 제도에 적합하도록 통합실태조사를 개선하는데 목적을 두고 있다. 이에 CMMC 버전2.0 2등급 110개 통제항목과 현재 시행중인 통합실태조사 237개 점검항목을 상세하게 분석하여 앞으로 다가올 CMMC에 대응하기 위한 통합실태조사 개선 방안을 제시하고자 한다. 먼저 정보보안 프레임워크에 입각해 통합실태조사 6개 분야의 점검항목을 관리적·물리적·기술적 측면의 정보보안 구성요소로 분류해서 분석하고 다음으로 CMMC 14개 영역의 통제항목을 같은 방식으로 분류해서 분석하고자 한다. 이러한 분석결과를 토대로 통합실태조사 개선 모델을 개발하여 미국 CMMC에 충족하는 통합실태조사가 되도록 하고 K-CMMC가 방산업체에 조기 정착되도록 통합실태조사 시행간 지원하는 방안을 제시하고자 한다.

Ⅱ. 관련 연구

2.1. 방위산업기술보호와 통합실태조사

2.1.1. 방위산업기술보호 정책

방위산업기술보호 종합계획은 국내 및 해외 선진 방산기술보호체계의 현황 분석을 통해 방위산업기술 보호에 관한 기본목표와 추진방향 및 계획 등을 제시하는 중기계획 문서로써 방위산업기술보호법 제4조 및 同 시행령 제3조에 따라 매 5년마다 수립한다. 「2017~2021 방위산업기술보호 종합계획」이 종료됨에 따라 「2022 ~2026 방위산업기술보호 종합계획」을 수립하였다. 종합계획은 국방부장관 주재 방위산업기술보호 위원회의 심의를 거쳐 확정된다.

「2022~2026 방위산업기술보호 종합계획」은 2017~2021년의 이행성과 분석을 통해 핵심과제 선정 및 목표를 수립하고 정책 수요자 의견, 관련 기관과 협력, 연구용역 등을 통해 아래 〈표 1〉과 같이 방위산업기술보호 세부과제를 식별하고 실질적이고 실현가능한 과제를 도출한다.[3]

〈표 1〉 방위산업기술보호 4대 추진과제[3]

방 향	추 진 과 제
방위산업기술 보호기반 강화	① 사이버위협 대응역량 강화 ② 기술관리 체계 고도화 ③ 방산기술 수출 및 도입 시 보호 기반 구축 ④ 방위산업기술보호 정부 역량 강화
기술보호 대내외 협력 활성화	⑤ 기술보호 공조체계 내실화 ⑥ 기술보호 국제협력 활성화
기술보호인식제고 및 인력관리 강화	⑦ 기술보호교육 활성화 및 교육체계 고도화 ⑧ 국방연구개발 핵심 인력관리 강화 ⑨ 기술보호 인식 확산
자율적 보호체계 구축 유도 및 지원 확대	⑩ 기술보호체계 구축 지원 확대 ⑪ 방위산업기술보호 대상기관 책임성 강화 ⑫ 기술보호 지식 및 정보 공유 활성화

종합계획 수립이후 튼튼한 방위산업기술 보호체계 구축을 통한 국가안전보장 및 국익제고 기여에 대한 목표를 가지고 12가지 추진과제에 대해 관련기관에 공유하고 상호 협력을 통해 정책을 펼친다.

통합실태조사는 방위산업기술보호 4대 추진과제 중에서 방위산업기술보호기반 강화 분야의 방위산업기술보호 정부역량 강화 과제에 해당된다. 이는 방산기술보호법 제12조와 同 시행령 제17조 및 방위산업기술보호지침 제42조의 2에 근거하여 시행하고 있다.

2.1.2. 통합실태조사 점검분야 및 평가방법

2020년도 이전 방위사업청에서는 방위산업기술보호법을 근거로 국내 방위산업기술의 경쟁력 강화와 보호를 위해 방위산업기술보호 체계 구축·운영 실태를 점검·평가하기 위해 방산업체 실태조사를 실시하였고, 방첩사(구.안보사)에서는 군사기밀보호법 및 방위산업보안업무훈령을 근거로 군사기밀 보안관리 실태를 확인하기 위해 보안감사를 실시하였다. 그러던 중 2019년 국무총리 주관 국정현안점검조정회의에서 실태조사와 보안감사의 중복 수검에 따른 방산업체 부담을 경감시키기 위해 통합 시행하도록 결정되었다. 따라서 2020년부터는 방산기술보호 실태조사와 방산업체 보안감사를 통합하게 되었으며 방위사업청 주관으로 국정원, 방첩사 등 3개 기관이 수행하며 6개 점검분야에 대해 아래 〈표 2〉와 같이 역할분담을 하였다.[4]

방위사업청은 기술·인력·시설·연구개발(이하 기술관리) 분야에 대해, 국정원은 정보보호 분야에 대해, 방첩사는 군사기밀 분야에 대해 실태조사 업무를 수행하도록 방위산업기술보호지침에 명시하였다. 이에 따라 방위사업청에서 통합실태조사를 계획하고 조사 결과를 종합하여 방산업체 및 유관기관에 통보한다.[5]

정기적으로 실시하는 통합실태조사는 2022년 기준 85개 방산업체 및 국과연, 기품원 등 정부출연기관에 대해 국내 및 해외사무소를 포함하여 약 160여 개의 사업장을 매년 약 10개월간 실시하고 있다. 업체 규모나 기술보유 수준에 따라 A·B·C 그룹으로 수준별 분류하여 실태조사를 진행하고 있으며 조사기간은 사업장 당 3~5일 정도 소요되고 있다. 현재 조사관 인력부족으로 방산 협력업체까지는 통합실태조사 범위에 미치지 못해 민간에 위탁하여 실시하고 있는 실정이다.

〈표 2〉 방산기술보호 점검분야별 점검지표[4]

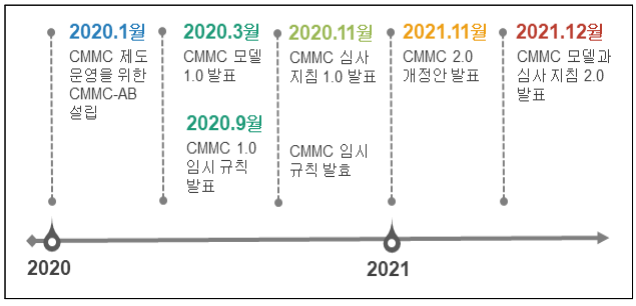
점검 분야 (6개)	방위산업기술보호법					방산보안 업무훈령
	기술의 식별·관리	인력통제	시설보호	연구개발 및 수출·기술이전 /협력업체	정보보호	군사기밀 관리
	방위사업청				국정원	방첩사
점검 지표	기술보호 내규	내규 (인원)	내규 (시설)	내규 (연구)	내규 (정보보호)	군사기밀 취급·관리
	연간계획/ 성과분석	신원조사	기술보호 구역	연구개발 보호정책 및관리	정보보호 시스템	군사기밀 보호구역
	기술보호 책임자	보직이동 및 퇴직시 대책	외부인·외국인 기술보호 구역통제	기술보호 활동이행	외부망 차단체계 구비	군사기밀 전산자료 관리
	기술보호 교육	상주·상시 출입 외 부인관리	정보통신 장비사용 통제	수출 및 국내 이전시 보호체계	정보시스템 및 저장 매체관리	암호장비/ 보안자재 관리
	심의회 구성·운영	상주·상시 출입 외국인 관리	보호구역 방문 외부인 ·외국인 통제	합작·제휴· 매매시 기술보호	자료별 접근 범위제한	군사기밀 송·수신
	기술유출 침해대응	기술취급 외부인· 외국인관리		협력업체 기술보호	보안관제 운용	군사기밀 보안사고
	자가진단	해외출장 자 관리			사이버 위협대응	
	실태조사 후속조치				긴급사태 대비	
	기술식별·등재					
	기술취급·관리					
	공개·제공시 절차준수					
(43개)	(11개 지표)	(7개 지표)	(5개 지표)	(6개 지표)	(8개 지표)	(6개 지표)
237개	15개 항목	11개 항목	10개 항목	21개 항목	118개 항목	62개 항목

조사에 앞서 매년 초 실태조사 실행 계획에 반영하여 점검항목 및 점검표를 작성하고 통합실태조사 가이드라인을 제작하게 된다. 또한, 수검 방산업체들 대상으로 사전 설명회를 갖고 점검표 배포 및 의견 수렴을 하게 된다. 평가는 최대한 객관적이고 공정하게 평가하기 위해서 항목별 평가기준을 정량·정성·이행여부로 구분하여 가이드라인에 따라 평가 점수를 부여한다. 평가 결과에 따라 실태조사 우수업체에 대해서는 무기체계제안서 평가시 가점 부여 및 표창 수여를 하고 미흡·미이행 사항 등에 대해서는 이행여부를 추적 확인하여 미이행시 방위사업청 심의위원회를 개최하여 개선권고, 시정명령, 과태료부과 등 행정조치를 실시한다. 결국, 통합실태조사는 현장에서 방위산업기술을 보호하는 일선 최전방 보루 역할을 하고 있다.

2.2. 사이버보안 성숙도 모델 인증(CMMC)

2.2.1. 미국 CMMC 제도의 발달

CMMC란 '미국 국방부의 계약업체가 보유한 민감한 정보를 사이버 위협으로 부터 보호하기 위해 개발한 사이버보안 성숙도 모델 인증 프레임워크'로 2014년에 백악관 지시하에 국토안보부(DHS) 에너지국(DOE)이 사이버보안 역량 강화에 필요한 지침 제공을 위해 4개 성숙도 등급과 10개 도메인으로 구성된 모델을 개발하였다. 이후 미국 국방부에서 2020년 3월에 5개 성숙도 등급과 17개 도메인, 171개 프랙티스(Practice)로 구성된 CMMC 모델 1.0을 발표하고 2020년 9월에 임시규칙을 발표하였으나, 미국 내 방산 계약업체들의 심한 반대로 인해 2021년 12월에 수준을 완화하여 3개 성숙도 등급과 14개 도메인, 110개 프랙티스로 구성된 CMMC 모델 2.0을 발표하였다. 그동안의 추진과정에 대한 타임라인은 다음 〈그림 1〉과 같다.[6]



〈그림 1〉 CMMC 타임라인

미국의 국가정보체계는 Top Secret, Secret, Confidential로 분류·관리하는 국가안보 관련 기밀정보(Classified Information)와 기밀은 아니지만 보호가 필요한 통제필요정보(Controlled Unclassified Information) 및 일반정보(Unclassified Information)로 구성되어 있다. 연방계약정보(FCI, Federal Contact Information)는 일반 공개용이 아닌 계약에 따라 정부에 의해 제공되거나 생성된 정보이고 통제필요정보(CUI)는 2009년 12월 발효된 국가보안정보분류 행정명령 13526에 따라 분류된 정보를 말한다. 여기서 계약업체의 CMMC 수준을 3개 등급으로 구분하여 인증을 부여하는데 연방계약정보만을 취급하는 경우에는 1등급 자체심사가 요구되며, 통제필요정보까지 취급하는 경우에는 2등급 또는 3등급 수준의 인증이 요구된다. CUI는 기초연구, 응용연구, 고급 기술개발, 조사분석 등 미국 국방부의 내부 및 외부 과학기술 사업으로 생산되는 문서, 데이터 세트를 국방기술정보센터(DTIC, Defense Technical Information Center)에 저장하고 공개범위를 제한하기 위해 배포등급을 부여하여 관리한다.[7]

2.2.2. CMMC 2.0의 특징

CMMC 2.0은 요구사항에 중점을 두어 기존 CMMC 1.0의 5개 등급에서 3개 등급으로 간소화하고 가장 널리 인정되는 국립표준기술연구소(NIST) 사이버보안표준을 사용하였으며, 1등급의 모든 기업과 2등급 대상 중 일부 기업은 자체 심사를 통해 규정 준수에 대한 입증이 가능하고 제 3자 심사원의 전문적이고 윤리적인 감독을 강화하여 신뢰할 수 있는 평가가 되도록 하였다. 또한, 특별한 상황에서 기업의 마일스톤에 따른 실행계획을 통해 제한적으로 인증 획득 가능토록 하고 CMMC 인증도 제한적인 면제를 허용하고 있으나, 2025년까지 미국뿐만 아니라 미국에 전략물자를 수출하는 모든 업체에 적용할 예정이다.

CMMC는 보호 요구 수준에 따라 다음 〈표 3〉과 같이 3등급으로 구분하고 등급별 프랙티스를 달리하고 있다.

〈표 3〉 CMMC 등급별 프랙티스[7]

등급	프랙티스	심사
3등급 (전문)	110+개 프랙티스 * NIST SP 800-171,172 기반	3년주기 정부주도 심사
2등급 (고급)	110개 프랙티스 * NIST SP 800-171과 연계	3년주기 제 3자 심사
1등급 (기본)	17개 프랙티스	연단위 자체 심사

CMMC 1등급은 연방계약정보 보호에 중점을 두고 연방조달규정 조항에 명시된 기본적 보호 요구사항에 해당하는 프랙티스로 구성이 되고, 2등급은 통제필요정보 보호에 중점을 두고 국립표준기술연구소의 특별간행물 800-171에 지정된 110개의 요구사항으로 구성된다. 3등급은 국립표준기술연구소의 특별간행물 800-172 요구사항의 일부에 기반하는데 아직 발표가 안되었다. CMMC는 14개 영역으로 구성되어 있으며 2등급의 경우 다음 〈표 4〉와 같이 전체 110개의 프랙티스를 가지고 있다.

〈표 4〉 CMMC 14개 영역별 프랙티스 갯수

영역	약어	개수	영역	약어	개수
접근통제	AC	22	미디어 보호	MP	9
인식 및 교육훈련	AT	3	인원보안	PS	2
감사 및 책임추적	AU	9	물리적 보안	PE	6
구성관리	CM	9	위험평가	RA	3
신원확인 및 인증	IA	11	보안평가	CA	4
사고대응	IR	3	시스템 및 통신보호	SC	16
유지관리	MA	6	시스템 및 정보 무결성	SI	7

2.2.3. 통합실태조사와의 차이점

아래 〈표 5〉와 같이 CMMC는 계약정보와 통제필요정보에 대해 보안관리 수준을 인증기관 CMMC-AB(CYBER AB로 명칭 변경)에 의해 110개 항목을 인증하는 반면 통합실태조사는 방위산업기술과 군사기밀 보호를 위해 237개 항목에 대해 인증기관 없이 3개 기관에서 합동으로 직접 실태조사를 실시하고 있으며 방산기술보호 및 보안수준 역량 강화를 위한 관리적인 성격이 상대적으로 강하다고 볼 수 있다.

〈표 5〉 CMMC와 통합실태조사의 비교

구 분	CMMC	통합실태조사('22년 기준)
목 적	· 계약정보(FCI), 통제필요 정보(CUI)의 보호	· 방위산업기술, 군사기밀의 보호
법 령	· 행정명령 13556 · FAR clause 52.204-21 · DFARS clause 252.204-7012	· 방위산업기술보호법 및 지침 · 군사기밀보호법 · 방위산업보안업무훈령
조 직	· 정책기관 : 미국 국방부 · 인증기관 : CMMC-AB · 삼사기관 : 등급에 따라 상이	· 정책기관 : 국방부, 방위사업청 · 조사기관 : 방위사업청, 국정원, 안보지원사
대 상	· 미국 국방부 사업 참여 기업	· 방산업체 및 정부출연기관
점 검 함 목	· 14개 영역, 110개 프랙티스	· 6개 영역, 43개 지표, 237항목 · 방위산업기술보호 : 175개 · 군사기밀관리 : 62개
등 급	· 1등급(FCI) : 17개 · 2등급(CUI) : 110개 · 3등급(CUI 외) : 110+	· 등급 없음
유 효 기 간	· 3년	· 1년(제안서 평가점수에 반영)

CMMC는 유효기간이 3년인데 반해 통합실태조사는 1년 단위로 실시하고 있으며 입찰 시 통합실태조사 평가 점수가 무기체계 제안서 평가에 반영되고 실태조사를 받은 업체는 3년마다 받아야 하는 보안측정이 면제되고 있어 방산업체에서는 적극적인 자세로 실태조사에 응하고 있다.

Ⅲ. 통합실태조사와 CMMC 분석

3.1. 통합실태조사 현황 분석

3.1.1. 통합실태조사 정보보안 프레임워크

정보보안 프레임워크는 기업업무의 연속성을 위한 네트워크, 시스템 등의 주요 인프라에 대한 위협요인을 사전에 분석하여 예방하고 위협요인 발생시 적절히 대응하기 위한 정책, 프로세스, 기술적 요인을 말하는 것으로 대부분의 보안대책은 정보보안의 구성요소인 관리적, 물리적, 기술적인 3가지 관점에서 점검되고 있다.[8][9] 정보보안 관리의 핵심은 기업의 실정에 맞는 정보보안 프레임워크를 수립하고, 수립된 정보보안 프레임워크를 바탕으로 보안에 관한 운영을 어떻게 하느냐 하는 문제로 귀결된다.

정보보안 프레임워크 절차는 먼저 진단을 통해 도출된 요구사항으로부터 정보보안 목표를 설정하고 이를 구현하기 위한 기본 틀(Matrix)을 설계하여 표준 절차를 기술한다. 다음으로 정의된 서비스를 지원하기 위한 보안 표준 프로파일을 세부적으로 작성한다. 끝으로 정보보안체계 전반을 운용·통제하기 위해 필요한 핵심요소를 설계한다.[10]

〈표 6〉 웹 서비스 사용자 인증 보안 프로파일의 예

구 분	관리적 보안	물리적 보안	기술적 보안
보안 서비스	안전한 패스워드 관리	웹서버의 물리적 보관	사용자 인증 및 데이터 암호화
보안항목	패스워드의 주기적 갱신 강제화	서버실의 출입 통제	ID/패스워드의 인증 알고리즘 보안성
절차/방법	패스워드의 주기적 갱신 의무 통지	서버실의 출입기록 보관	시스템 도입시 해킹방지 S/W 도입

이중에서 정보보안 업무의 가장 핵심을 이루는 구성요소는 위 〈표 6〉의 웹 서비스에서의 사용자 인증 사례와 같은

표준 프로파일로 실태조사 점검에서도 중요한 역할을 하고 있다. 특히, 우리가 매일 직면하는 디지털 위협은 매우 다양하기 때문에 때로는 물리적 보호 방법을 간과하는 경우가 많다.정보보호 담당은 물리적 보안을 담당하는 부서와 적극적으로 협력해 현재의 위협과 취약점에 관한 피드백 제공을 수행해야 한다.[11]

정부기관에서 실시하는 통합실태조사도 방산기술보호지침과 방산보안업무훈령에 기반을 두고 실시하고 있는데, 점검항목이 정보보안 프레임워크의 구성요소를 모두 포함하고 있다. 특히, 방산기술보호지침은 기술보호 관점이 강해 기술관리 및 인원·시설에 대한 관리적인 점검 요소와 정보보호 관련 기술적인 점검 요소에 많은 비중을 차지하고 있으며, 방산보안업무훈령은 군사기밀 및 보안관리 관점이 강해 전통적인 문서·인원·시설 등의 융합적인 보안과 정보통신 보안을 포함하고 있다.

따라서 방산업체 통합실태조사는 내부보안뿐만 아니라 방산기술보호와 군사기밀보호라는 특수한 영역이 있어 일반적인 기업환경에서 실시하는 보안 관리에 비해 상대적으로 관리적인 요소가 많고 포괄적이라 할 수 있다.

3.1.2. 통합실태조사 점검항목 분석

실태조사나 기관 인증평가를 함에 있어 한 개의 점검항목을 정보보안 구성요소 중 한 개의 항목으로만 판단하기에는 어려움이 있어 평가항목을 세분화 하던가 때에 따라 종합적인 차원에서 평가할 필요가 있다. 통합실태조사도 6개 분야 237개 점검 항목으로 구성되어 있으나, 관리적, 물리적, 기술적인 측면으로 분할하여 세부 분류하였을 때 전체 248개로 9개의 추가 요소가 파악된다. 분류하는 근거 및 기준은 다음 [사례 1]과 같다.

- [사례 1] : 점검항목 6-①-⑧(군사기밀 보관기준 준수)

해당 항목은 방산보안업무훈령 제39조(보관기준)과 제40조(보관용기)에 적용을 받고 있어, 同 조항을 근거로 보안대책과 준수사항이 보안 내규에 반영되어야 하고 또한 보관용기 상태, 이중 잠금장치, 열쇠 관리 등 물리적인 기준에 충족하는 장치를 구비하여야 한다. 따라서 관리적 보안과 물리적 보안 2가지 점검이 필요하다.

통합실태조사 전체 항목을 분석한 결과는 아래 〈표 7〉에서와 같이 관리적 보안이 60.4%, 물리적 보안이 6.9%, 기술적 보안이 32.7% 로 분포해 있으며 인력통제와 시설보호는 군사기밀 관리 분야의 인원·시설 보안과 일부 겹치고 그리고 정보보호는 군사기밀 관리 분야의 정보통신 보안과 일부 겹치는 항목이 있으나, 점검 영역을 달리하고 있어 중복이라고 볼 수 없다.

〈표 7〉 분야별 통합실태조사 항목 분포

분 야		계	관리적 보안	물리적 보안	기술적 보안
계	개수	248	150	17	81
	비중	(100%)	(60.4%)	(6.9%)	(32.7%)
1 기술의 식별·관리	(15)	15	15		
2 인력통제	(11)	11	11		
3 시설보호	(10)	11	3	8	
4 연구개발 및 수출 기술이전/협력업체	(21)	23	20		3
5 정보보호	(118)	120	52		68
6 군사기밀 관리	(62)	68	49	9	10

3.2. CMMC 현황 분석

3.2.1. CMMC 통제항목 분석

CMMC 2.0의 2등급은 통제필요정보에 대한 보안요구 사항이 14개 영역 110개로 구성되어 있어 통합실태조사 항목 237개의 절반에도 못 미치고 있다. 하지만, 통제항목이 상대적으로 적지만 정보보안 구성요소로 분할 시 통제항목이 110개에서 136개로 26개 항목이 추가된다. 예를 들면 다음 [사례 2]와 같다.

- [사례 2] : 통제항목 AC.L1-3.1.1(인가된 접근통제)

해당 항목은 인가된 사용자와 인가된 사용자를 대신하는 프로세스 또는 장치(다른 정보시스템 포함)만이 정보시스템에 접근 할 수 있도록 제한하도록 하는 항목으로 관리적인 측면에서 기술보호 내규 및 보안 내규에 반영, 담당별 접근·출입 권한 설정 등을 점검해야 하고 물리적 측면에서는 스피드게이트 검색, 기술보호·통제구역 출입카드 인증 및 모니터링 등이 있으며, 기술적인 측면에서는 PLM 등 기술관

리시스템, 정보통신·정보보호 등 시스템에 대한 로그인(log-in)에 대한 점검을 하게 된다. 따라서 사례의 접근통제 관련해서는 관리적 보안, 물리적 보안, 기술적 보안의 3가지 점검이 모두 필요하고 볼 수 있다.

통합실태조사 항목 중에서는 접근통제 관련해서 인원 통제 분야(②-③-①), 시설보호 분야(③-④-①, ③-⑤-①), 정보보호 분야(④-④-④, ④-④-⑥, ④-⑤-②), 군사기밀관리 분야(⑥-②-①)가 同 항목을 충족하고 있다.

CMMC는 다음 〈표 8〉에서와 같이 관리적 보안이 33.8%, 물리적 보안이 8.1%, 기술적 보안이 58.1%로 분포해 있으며, 통합실태조사의 관리적 보안의 높은 비중에 비해 기술적인 보안요구사항 비중이 상대적으로 크다고 할 수 있다.

〈표 8〉 분야별 CMMC 항목 분포

도 메 인		계	관리적 보안		물리적 보안		기술적 보안	
	충족 여부		충족	미포함	충족	미포함	충족	미포함
계	개수	138	41	6	11	0	65	15
	비중	(100%)	(33.8%)		(8.1%)		(58.1%)	
① AC	(22)	30	7	1	4		12	6
② AT	(3)	3	3					
③ AU	(9)	12	3				7	2
④ CM	(9)	11	2	1			7	1
⑤ IA	(11)	12		1			9	2
⑥ IR	(3)	3	3					
⑦ MA	(6)	8	3	2			3	
⑧ MP	(9)	18	9		3		6	
⑨ PS	(2)	2	2					
⑩ PE	(6)	6	1		4		1	
⑪ RA	(3)	4	3				1	
⑫ CA	(4)	5	4				1	
⑬ SC	(16)	17	1	1			11	4
⑭ SI	(7)	7					7	

또한, 관리적, 물리적, 기술적 정보보안 분야로 세부 분류 시 전체 138개 항목으로 늘어나는 것을 감안했을 때 통합실태조사 항목에 비해 통제항목 하나에 많은 보안요소를 포함하고 있음을 알 수 있다. 반면에 통합실태조사에서는 CMMC 통제항목 110개 중 중복성을 배제하고 순수항목 19개(17.3%)를 충족하지 못하고 있다.

3.2.2. 통합실태조사 항목에서 CMMC에 미포함 요소 분석

CMMC에 미포함 항목은 접근통제, 감사와 책임, 신원확인 및 인증, 유지관리, 시스템 및 통신보호 등의 도메인(Domain)에 고루 분포되어 있으며, 접근통제 도메인에 가장 많은 미포함 요소의 분포가 확인되었다.

접근통제(AC) 도메인 중에 로그온(AC.L2-3.1.8)과 개인정보보호(AC.L2-3.1.9)에 해당하는 점검항목이 없으며, 화면보호기 설정과 같은 정보통신 보안 항목은 있으나 세션통제(AC.L2-3.1.10, AC.L2-3.1.11)와 같은 점검항목은 없다. 무선 LAN 보안(AC.L2 -3.1.16, AC.L2-3.1.17)은 훈령 제94조와 훈령 별표16의 자가진단 항목 항목에 명시되어 있으나 점검항목에는 누락되어 있으며, 훈령 제98조에 노트북, PDA 등 휴대형 컴퓨터와 스마트폰을 이용한 통제필요정보(방산기술 등) 취급시 암호화를 요구하고 있으나, 규정상 취급을 인정하지 않고 있어 점검항목에도 없는 실정이다.

또한, 감사와 책임(AU) 도메인 중 감사로그(Audit log) 실패 시 경고(AU.L2-3.3.4) 및 표준시간으로 시스템 동기화(AU.L2-3.3.7)하는 요소를 점검하지 않고 있고, 구성관리(CM) 중 훈령 97조에 보안에 취약한 프로그램 사용을 제한하고 있으나 명확한 점검항목이 없다. 신원확인 및 인증(IA) 도메인 중 훈령 별표 9에 ID와 비밀번호관리·운용 지침이 있으나, ID 재사용 금지 및 비밀번호 재사용 금지하는 점검항목은 없다. 유지관리(MA) 도메인에서도 정비업체를 통해 유지관리가 이루어지고 있지만, 유지관리 수행과 통제(MA.L2-3.7.1, MA.L2-3.7.2)하는 항목이 없다.

끝으로 시스템 및 통신 보호(SC) 도메인 중에 대기업 데이터센터에 있을 만한 보안공학적 설계(SC.L2-3.13.2), 휴대폰 모바일 코드의 사용 통제 (SC.L2-3.13.13), 통신 진본성(SC.L2-3.13.15) 등 고도의 보안을 요구하고 있고, 인터넷 전화 사용에 대한 모니터링을 요구하고 있지만, 현재 통합실태조사 점검항목에는 없는 미포함 요소들이다. 다음 〈표 9〉은 통합실태조사에서 CMMC에 미포함하는 19개 항목을 나열하였다. 다만, 아직까지는 CMMC 통제항목에 대한 평가 가이드라인이 정립되지 않고 경험 사례가 없어 정확한 판정에는 제한이 따른다.

〈표 9〉 CMMC 미포함 항목

통제항목	프랙티스	비고
AC.L2-3.1.8	· 로그온 시도 실패	기술
AC.L2-3.1.9	· 개인정보보호 및 보안사항 안내	관리
AC.L2-3.1.10	· 세션 잠금	기술
AC.L2-3.1.11	· 세션 종료	기술
AC.L2-3.1.16	· 무선 접근 인가	기술
AC.L2-3.1.17	· 무선 접근 보호	기술
AC.L2-3.1.19	· 모바일의 통제필요정보 암호화	기술
AU.L2-3.3.4	· 감사 실패 경고	기술
AU.L2-3.3.7	· 신뢰된 시간 출처	기술
CM.L2-3.4.9	· 사용자 설치 소프트웨어	관리·기술
IA.L2-3.5.5	· ID 재사용	관리·기술
IA.L2-3.5.8	· 비밀번호 재사용	기술
MA.L2-3.7.1	· 유지관리 수행	관리
MA.L2-3.7.2	· 시스템 유지관리 통제	관리
SC.L2-3.13.2	· 보안 공학	관리
SC.L2-3.13.9	· 연결 종료	기술
SC.L2-3.13.13	· 모바일 코드	기술
SC.L2-3.13.14	· 인터넷 전화	기술
SC.L2-3.13.15	· 통신 진본성	기술

이러한 항목들의 누락사항에 대해서는 방산기술보호지침 및 방산보안업무훈령의 일부를 개정하고 통합실태조사 시행계획상 점검항목을 추가함으로써 CMMC 보안요구사항을 충족할 수 있다.

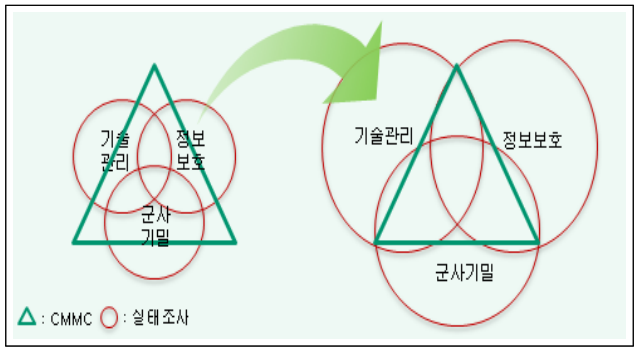
Ⅳ. 통합실태조사 개선 방안

CMMC 2.0 통제항목과 통합실태조사 점검항목에 대한 분석결과를 토대로 통합실태조사 개선 모델을 제시함으로써 CMMC에 미포함하는 점검항목을 추가하고 방산업체를 대상으로 지속적인 컨설팅 지원 방안을 제시하여 다가올 미국 CMMC 제도에 선제적으로 대응토록 한다.

4.1. 통합실태조사 개선 모델

본 연구는 현재 진행중인 통합실태조사의 신뢰성 및 인증능력을 논하기 이전에 CMMC 제도에 충족하도록 하는데 목적이 있다. 앞장에서 살펴보았듯이 CMMC 통제항목과 통합실태조사 점검항목 분석을 통해 관리적, 물리적, 기술적 측면에서 CMMC에 미포함하는 요소들을 확인하였다. 즉, 아래 〈그림 2〉와 같이 기술관리, 정보보호, 군사기밀에 대해 3개 기관에서 점검하는 통합실태조사 영역의 밖으로 왼쪽 삼각형 도형과 같이 CMMC 범위에서 벗어나 통제 사각지대가 발생한다.

따라서, 이를 해결하기 위한 방안으로 삼각형 도형 CMMC는 그대로 둔 채 통합실태조사 영역인 3개 분야의 원형을 확대해서 CMMC를 충족시키는 개선 방안을 제안한다.



〈그림 2〉 통합실태조사 개선 모델

결국, CMMC 충족을 위해서는 통합실태조사 영역이 더욱 확대되어 점검항목이 늘어날 수밖에 없는 상황으로 조사인력과 기간 연장이 제한됨에 따라 점검항목에 대한 테일러링(Tailoring)이 필요하다.

4.2. CMMC 미포함 항목 추가 반영

위의 개선 모델에 따라 CMMC에 미포함하는 19개 통제항목을 아래 〈표 10〉과 같이 서로 관련성있는 영역에 신규로 점검항목을 추가하고 CMMC에서 요구하는 평가내용이 통합실태조사 평가요소에 포함되도록 한다. 일부 점검항목을 제외하고 추가해야 할 대부분의 점검항목에 대해 평가근거가 없고 향후 평가에 대한 공정성 논란의 여지가 있어 지침이나 훈령 개정이 필요하다.

현재 결과로만 봤을 때 CMMC에 충족하기 위해서는 통합실태조사의 기술적 보안 영역인 정보보호 분야에 대한 확대와 세부적인 점검항목 추가가 필요하다.

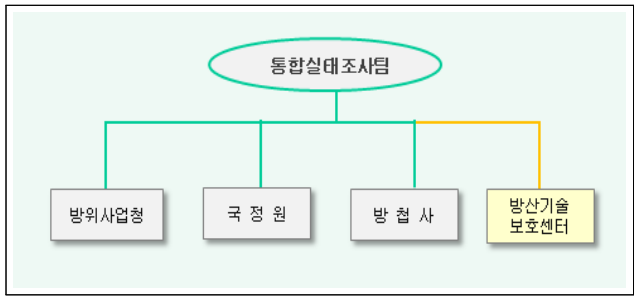
〈표 10〉 통합실태조사 점검항목 추가 분야

통제항목	통합실태조사 점검항목(추가)	근거
AC.L2-3.1.8	4-⑤-③ 접근통제 및 로그온	·
AC.L2-3.1.9	4-④-④ 개인정보보호 안내	·
AC.L2-3.1.10	4-④-④ 세션 잠금 및 종료	·
AC.L2-3.1.11		
AC.L2-3.1.16	4-③-① 무선 접근 인가 및 보호	훈령94조
AC.L2-3.1.17	4-④-② 모바일 기기의 암호화	훈령98조
AC.L2-3.1.19		
AU.L2-3.3.4	4-⑥-① 감사로그 실패시 경고	
AU.L2-3.3.7	4-⑤-③ 내부시스템 시간 동기화	·
CM.L2-3.4.9	4-④-② 사용자 설치 SW 통제	훈령97조
IA.L2-3.5.5	4-④-④ ID / 비밀번호 재사용 금지	·
IA.L2-3.5.8		
MA.L2-3.7.1	4-①-① 유지관리 수행	·
MA.L2-3.7.2	4-④-① 시스템 유지관리 통제	·
SC.L2-3.13.2	4-①-① 보안 공학 운칙 내규 반영	·
SC.L2-3.13.9	4-④-④ 네트워크 연결 종료	·
SC.L2-3.13.13	4-④-② 모바일 코드 사용 통제	·
SC.L2-3.13.14	4-④-⑥ 인터넷 전화 기술 통제	·
SC.L2-3.13.15	4-①-① 통신 진본성 보호	·

4.3. 통합실태조사팀 확대 및 K-CMMC 지원

최근 방위사업청은 K-CMMC 관련 조직체계, 인증심사, 교육체계, 법규개정 등 구체적인 추진방안을 연구하였으나, 현실적으로 당장 실행에 옮기기에는 조직구성, 지원제도 마련, 예산확보 등에 있어 많은 제약이 따르고 있다. 따라서, 현재 수행하고 있는 통합실태조사 제도와 연계하여 K-CMMC를 점진적으로 발전시키는 것이 바람직한 것으로 판단된다.

2022년 7월에 국방기술품질원 산하에 「방산기술보호센터」가 신설되었다. 이 기관은 방산분야 사이버 위협에 대한 보안관제, 사고대응 및 예방, 방산기술보호 및 관리 등 집행기능을 수행하는 임무로 현재 직무를 식별하며 조직체계를 정비하고 있다. 따라서 이 기관을 적극 활용할 필요가 있다. 현재 3개 기관 체계의 통합실태조사에서 다음 〈그림 3〉과 같이 방산기술보호센터를 포함한 4개 기관 체계로 재편하여 K-CMMC를 지원하는 방안을 제안한다.



〈그림 3〉 통합실태조사팀 편성

K-CMMC가 정착될 때까지 방산기술보호센터에서 2~3년간 한시적으로 예비 CMMC 심사원 역할을 하며 방산업체 및 실태조사관들과 피드백을 통해 방산업체가 K-CMMC 인증 심사를 받기 위한 역량이 어느 수준에 오를 때까지 컨설팅을 지원하여 방산업체의 자발적인 참여 유도를 이끌 필요가 있다.

CMMC 제도에서는 제 3자에 의한 인증 방법으로 3가지 절차를 거치는데 먼저 요구되는 이행과제에 대한 감사증적 등 문서를 검토하고 다음으로는 심사 대상 조직의 구성원이 이행과제를 어떻게 수행하는지 파악을 위한 담당자 면접을 실시하고 마지막으로 요구되는 이행과제가 실제로 수행되었지 입증을 위한 현장 확인의 방법을 거친다.[12] 현재 통합실태조사도 CMMC 인증 심사와 동일한 방법으로 진행하고 있어 통합실태조사를 진행하며, CMMC 인증 심사 준비를 지원하는데 무리가 없다.

4.4. CMMC 인증 참여 보상제도 부여

통합실태조사에서는 평가 결과 점수를 무기체계 제안서 평가시 반영하고 있어 자발적인 실태조사 참여를 유도하고 있으나 입찰과 무관한 중소 방산업체나 협력업체들에게 별다른 실익이 없어 보인다. 현재 85개 방산업체 중 중소업체 비중이 48개(56.4%)를 차지하고 있으며[13], 중소 협력업체까지 포함하면 훨씬 많은 비중을 차지하고 있다. 국내 방산업체의 전반적인 방산기술보호 수준을 끌어 올리기 위해서는 체계업체 및 중견업체와 동반 성장이 필요한다. CMMC 인증을 받기 위해서는 관리적 측면에서 인력 증원과 물리적·기술적 측면에서 정보보안 강화를 위한 추가적인 비용이 필요하다. 인력 및 자금 여력이 부족한 중소업체들 상대로 평가점수로 CMMC 인증 획득을 유도하는 것은 전혀 동기

부여가 되지 않는다.

따라서, K-CMMC가 국내 방산업체에 조기 정착되기 위해서는 정부차원의 강력한 지원과 체계업체에서의 협력업체 관리가 필요하다. 즉, 정부 차원에서는 인증 참여 업체에 대해 일정 금액 지원이나 매출의 일정비율을 원가로 보전해주고, 체계업체에서는 협력업체를 대상으로 보안 장비 및 기술을 지원하는 방안을 제안한다. 특히, 체계업체에 먼저 적용으로 성공사례를 활용하여 인력·자금이 부족한 중견·중소업체에는 점진적으로 적용하는 방안이 필요하다.

V. 결론

통합실태조사는 기술(기밀)보호 및 정보보호 측면에, CMMC는 사이버보안 측면에 초점이 맞춰져 있어 관점의 차이로 서로 지향하는 바가 조금은 차이가 있다. 통합실태조사에서는 인력통제·시설통제·정보보호 분야 뿐만 아니라 기술식별·연구개발·군사기밀 등 광범위하게 세분화되어 있어 CMMC를 포함하고 있는 반면 CMMC는 항목수는 적으나 정보보안 영역을 깊이 있게 다루고 있어 서로 미흡·부족함을 비교하는 것은 무의미하다고 본다. 하지만, 우리나라가 방산수출과 기술적 우위를 점하고 있는 미국을 상대하기 위해서 CMMC 제도를 따라야 하는 것은 자명한 사실이다. 이에 정부와 학계에서는 K-CMMC 제도 도입 방안을 연구하고 미국 CMMC와 상호인정 협정 추진 등 다각적인 방안을 모색하고 있다.

본 논문에서는 통합실태조사에 CMMC의 요구조건을 반영함으로써 우리나라에 K-CMMC 제도가 연착륙할 수 있도록 방안을 제시하였다. 먼저 통합실태조사 점검항목과 CMMC 통제항목을 정보보안 3가지 측면에서 빈도분석을 하여 두 제도의 정보보안 구성요소의 비중 차이와 CMMC에 미포함하는 19개 요소를 파악하였다. 이를 통해 CMMC 통제항목을 통합실태조사 점검항목에 추가하여 미포함 요소를 해소하였다. 또한, K-CMMC 제도가 조기 정착할 수 있도록 통합실태조사팀 확대 편성 방안과 여건이 불비한 중소 방산업체에 대한 지원 방안을 제안하였다.

향후 과제로는 아직 발표가 안된 CMMC 3등급에 대한 요구사항이 발표되면 통합실태조사에 반영하기 위한 추가적인 연구가 필요하다.

참고문헌

1) 뉴스투데이(www.news2day.co.kr), “[에디터 인터뷰] 류연승 명지대 방산안보학과 주임교수 미국 방산수출에 필요한 사이버 보안 인증(CMMC) 해법 제시” (검색일 : 2022. 10. 7.)
2) 시큐리티월드(www.boannews.com), “[이슈칼럼] 방위산업 사이버안보 주권을 지키자” (검색일 : 2022. 10. 8.)
3) 대한민국 정책브리핑(www.korea.kr), 2022~2026 방위산업 기술보호 종합계획, Dec, 2021. p13-15 (검색일 : 2022. 10. 7.)
4) 대한민국 정책브리핑(www.korea.kr), [방위사업청 보도자료] “방산기술보호 통합실태조사, 무엇이든 물어보세요!”, Jan, 2020. p3-5 (검색일 : 2022. 10. 7.)
5) 이상열, 류연승, 방산업체 보안평가 개선방안에 관한 연구, 한국산학기술학회논문지 제23권 제7호 2022. p250-254.
6) 한국산업기술보호협회, 2022년 통합실태조사관 직무역량 강화 교육, Aug, 2022. p280-290.
7) 류연승, 미국 CMMC 동향 및 우리의 대응, 국방보안컨퍼런스, Sep, 2022.
8) 정보보호 및 개인정보보호 관리체계(ISMS-P), 강혁, Jan, 2020.
9) 케듀아이, ISE 국가공인 산업보안관리사, 산업보안실무위원회, Feb, 2021.
10) 서울대출판부, 보안경제학(CEO를 위한 정보보안 투자 가이드), 서승우, 2008. p213-218.
11) 에이콘, Defensive Security Handbook, 리브라더스톤·아만다 베를린, 2018. p123-132.
12) 류연승, 미국 CMMC 소개 및 인증 취득방안, DX-KOREA CMMC 세미나, Sep, 2022.
13) 한국방위산업진흥회, 방산업체 경영분석, 2021.