특집 06

국내 방산기술보호 통합실태조사와 미국CMMC 제도의 연계방안 연구

장항배(중앙대학교), 김선영(아주대학교)

목 차

1. 서 론

우리나라는 선택과 집중의 국방 R&D 투자를 통해 첨단 무기체계의 독자개발 능력을 확보해가고 있다. 국방기술진흥연구소는 국방분야 선진 16개국의 기술수준을 분석한 「2021 국가별 국방과학기술 수준 조사서」에서 우리 국방과학기술 수준을 세계 9위로 평가하였다. 2012년 10위권으로 진입한 이후 꾸준히 성장하고 있는 것이다. 이러한 국제경쟁력 확보를 통해 수출도 세계 10위권에 진입하는 등 꾸준한 성장세를 이어가고 있다.

이러한 기술 발전에 따른 보호 체계 구축과 대외적 신뢰도 제고를 위해 정부는 2015년 12월 「방위산업기술보호법」을 제정하고 이듬해 6월 동 법 「시행령」과 시행규칙을 제정하면서 기술보호체계를 구축하였다. 즉, 동 법의 제정으로 방산업체에 대한 실태조사, 기술유출자 처벌 및 방위산업기술 지정·고시 등 기술보호를 위한 근거를 마련한 것이다. 또한 방산업체를 대상으로 「방위산업기술보호법」의 실태조사와 「방위산업보안업무훈령」의 보안감사를 각각 실시하다가 기업의 부담 경감을 위해 2019년부터 통합하여 시행하고 있다. 또한 방위산업과 관련한 국방과학기술 중 국가안보 등을 위하여 특별히 보호되어야 하는 방위산업기술을 지정 고시하고 있는데 2023년 현재 센서·정보통신·탄약 등 8개 분야 128개 기술이 지정된 상태이다

그러나 2020년 대우조선해양 핵추진 잠수함 기술, 2021년 한국항공우주산업의 KF-21 전투기 기술 등 첨단 방산기술을 노리는 사이버 해킹 사고가 연이어 발생하는 등 사이버 보안 역량이 취약한 것으로 평가되었다. 이런 가운데 2020년 세계 최고의 방산수출국이며 기술 주도권을 쥐고 있는 미국이 자국 국방사업 참여 기업에게 강력한 사이버보안 체계인 CMMC(CyberSecurity Maturity Model Certification) 프레임워크를 구축할 것을 요구하고 있어 이에 대한 대비가 필요한 상황이다

본 연구에서는 미국 CMMC 시스템을 살펴보고 방위사업청 주도로 매년 실시하고 있는 통합실태조사와 연계함으로써 CMMC 도입에 따른 대응책을 제시하고자 한다

2. 방위산업기술보호 통합실태조사

2.1 방위산업기술보호 정책

방산기술보호 주무부처인 방사청은 「방위산업기술보호법」 제4조와 동 법 시행령 제3조를 근거로 2017년부터 5년 단위로 「방위산업기술보호 종합계획」을 수립하여 시행하고 있다 동 종합계획은 국내외 기술 보호 환경을 분석하여 추진과제를 선정하고 세부 추진계획을 제시하는 중기계획으로서 국방부장관 주재로 방위산업기술보호위원회 심의를 거쳐 확정된다. 현재 「2022-2026 방위산업기술보호 종합계획」이 시행되고 있다

「2022-2026 방위산업기술보호 종합계획」에서는 '방산업체 대상 사이버 위협이 증가하고 있으나 전문기관 부재 등 효과적 대응책이 부족한 실정이며, '기술유출 예방 차원에서 실태조사를 수행하고 있으나, 인력 부족으로 심층적 조사는 제한적임'을 문제점으로 지적하였다. 이에 대한 대책으로 향후 ①사이버위협 대응역량 강화 ②정부역량강화를 통해 방위산업기술 보호 기반을 강화할 것을 세부 과제로 선정하고 있다

방위산업기술보호 목표 및 추진방향

방 향	추 진 과 제
방위산업기술 보호기반 강화	① 사이버위협 대응역량 강화 ② 기술관리 체계 고도화 ③ 방산기술 수출 및 도입 시 보호기반 구축 ④ 방위산업기술보호 정부역량 강화
기술보호 대내외 협력 활성화	⑤ 기술보호 공조체계 내실화 ⑥ 기술보호 국제협력 활성화
기술보호 인식 제고 및 인력 관리 강화	⑦ 기술보호 교육 활성화 및 교육체계 고도화 ⑧ 국방연구개발 핵심인력 관리 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

(그림 1) 방위산업기술보호 목표 및 추진방향(2022-2026 방위산업기술보호 종합계획, 방사청)

(그림 1) 방위산업기술보호 기반강화 중 '①사이버위협 대응역량 강화 ④방위산업기술보호 정부역량강화' 가 통합실태조사와 관련된 추진과제라고 하겠다

2.2 방위사업기술보호 통합실태조사

통합실태조사는 「방산기술보호법」제12조(방위산업기술보호를 위한 실태조사)와 동 법 시행령 제17조에 근거하여 매년 방사청·국정원·방첩사 등 3개 기관 합동으로 방산업체를 대상으로 전수조사를 실시한다. 조사결과는 종합분석되어 해당 방산업체 및 유관기관에 통보되며 향후 기술보호 정책 뿐 아니라 해당 기업의 정부 무기체계 사업 참여 여부에도 영향을 미친다

실태조사는 2020년도 이전에는 방위사업청이 「방산기술보호법」을 근거로 하는 실태조사와 방첩사에서 「군사기밀보호법」과 「방위산업보안업무훈령」을 근거로 하는 보안감사가 별도로 실시되었다. 그러나 업체 입장에서 유사한 내용의 점검을 이중으로 받는다는 불만이 표출되자 업체 부담을 경감시키기 위해 2020년부터 방위사업청 주관으로 3개 기관이 합동으로 실시하게 된 것이다. 매년 3월 초 경부터 사업장의 규모 또는 중요도에 따라 3~5일간씩 점검하고 있다

통합실태의 핵심인 조사항목은 비공개이므로 방산기술보호지침으로 배포되어 사용하는 자가진단표를 통해 점검항목을 살펴보겠다. 2023년 자가진단표는 기술의 식별·관리, 인원통제, 시설보호, 정보보호, 연구개발 등 5개 분야로 구성되어 있다.

이중 CMMC와 직접 관련되는 정보보호 분야 점검항목은 <표 1>에서 보듯이 9개분야 38개항목이며 세부적으로 분류하면 79개 항목으로 증가한다. 정보보호 분야 점검은 점검관은 물론 피점검관까지 관련 분야에 대한 특별한 전문성을 요구하고 있다. 통합실태조사에서 정보보호 점검은 국정

〈표 1〉 정보보호분야 자가진단표 점검항목

구 분	점검 항목 (★) 핵심요소
❶ 정보보호시스템 설치 및 운용 (7개항목)	① UTM 또는 방화벽, IPS 설치 · 운영(★) ② 바이러스 백신 프로그램 설치 · 운영(★) ③ DRM 설치 운영(★) ④ 자료유출방지시스템(DLP 등) 설치 운영(★) ⑤ 네트워크 접근제어 인증시스템설치(★) ⑥ 보안정책이력 등 관련 로그 존안(★) ⑦ 보안취약점 분석 및 평가(★)
❷ 외부망 차단 (6개항목)	① 외부망 차단체계 구축 운영(★) ② 패치관리시스템 및 백신서버 분리 운용 ③ 네트워크 접근제어(NAC)를 설치하여 비인가 기기 접속 통제(★) ④ 관리대상기술 전산자료 반출시 망간 자료교환시스템 운용 ⑤ 망간자료교환시스템 이용시 압축파일 전송 불가토록 조치 ⑥ 분기별 취약점 분석 평가(★)
❸ 보안관제 (3개항목)	① 보안관제 시스템 설치·운용(★) ② 보안관제시스템 관리 ③ 관제결과 이상 발생시 유관기관 통보 및 이행조치
❹ 긴급사태 예방 및 복구대책 (2개항목)	① 긴급사태 발생에 대한 관리대상기술자료 백업 및 복구계획 수립(★) ② 긴급사태 발생시 유관기관 신고
❺ 정보통신망 원격 관리 및 외부업체 관리 (4개항목)	① 지정된 단말기에서만 원격관리(★) ② 외부업체의 정보통신망 유지보수 보안대책 수립(★) ③ 외부업체 정보통신망 접속 통제 ④ 외부업체 반입 정보통신기기 관리
❻ 정보통신기기 및 저장매체 관리 (6개항목)	① 지정된 정보통신기기 및 저장매체 도입 총괄(★) ② 정보통신기기 개별 등록 ③ 정보보호시스템 설치 후 정보통신망 연결 ④ 녹음,촬영 등 정보보호시스템이 통제할 수 없는 행위 통제 ⑤ 정보통신기기 및 저장매체 외부 반출시 포맷 등 보안대책 ⑥ 정보통신기기 및 저장매체 분실시 유관기관 신고
❼ 관리대상기술 접근범위 제한 (3개항목)	① 관리대상기술 자료별 접근범위 및 권한에 대한 정책수립(★) ② 기술자료 보관 주컴퓨터(서버) 접속기록 생성 유지(★) ③ 관리대상기술 관련 시스템 접근시 경고문구, 출력시 이력표시
❽ 관리대상기술 전산자료 반출 (3개항목)	① 외부 전자메일 발송시 해당 부서장 승인 전송(★) ② 파일 첨부메일 발신시 일시, 발신자, 수신자 및 파일내용 기록(★) ③ 저장매체를 활용한 전산자료 반출 통제
❾ 자료유출 관리 대응 (4개항목)	① 전자메일을 통한 무단자료반출 확인 및 추후조치(★) ② 이동식 저장매체 관리(★) ③ PC · 노트북 등 자산관리(★) ④ 인터넷 PC에서 업무자료 작성 및 저장금지(★)

출처 : 방위산업기술보호지침

원이 전담하다가 올해부터 중소·중견기업에 대해서는 방첩사도 참여하고 있다. 한편 방사청은 실태조사관의 전문성 제고를 위해 산하에 「방위산업기술보호센터」를 설립하고 실태조사 전문 인력(5명)을 투입하고 있다.

통합실태조사는 각 점검 항목별로 정성·정량·이행여부 등을 구분하여 확인한다. 조사결과에 따라 개선권고·시정명령 및 최고 3000만원의 과태료 부과 등 행정조치도 따른다. 또한 조사결과 우수한 점수를 획득한 기업은 무기체계 제안서에서

가점을 받는 등 인센티브도 주어지고 있다. 즉, 통합실태조사가 방산업체 규모나 참여사업 수준 등에 무관하게 동일한 보호수준을 요구하고 협력업체의 경우는 체계업체에서 자체적으로만 점검하는 등 문제점도 지적되고 있지만 통합실태조사는 방산업체가 기술보호를 위해 관심과 노력을 투자하도록 유도하는 결정적인 역할을 하고 있는 것이다

3. 미국의 사이버보안 성숙도모델 인증(CMMC) 제도

3.1 CMMC(CyberSecurity Maturity Model Certification) 도입 배경

미국 대통령 경제자문위원회CEA, Council of Economic Advicors)는 악의적인 사이버 활동이 2016년 미국 경제에 570억 달러에서 1,900억 달러의 손실을 입힌 것으로 추정한 가운데 2018년도에는 중국에 대한 무역적자가 4,192억 달러에 이르는 등 사상 최고치에 이르게 된다. 미국 정부는 막대한 무역적자의 원인 중에서 기술 및 지식재산권에 대한 중국의 불법적인 침해가 있다고 보고 이에 대한 대응으로 「수출통제개혁법(Export Control Reform Act: ECRA)」을 제정한다. 「수출통제개혁법」은 신흥기술과 기반기술을 새로이 수출통제 대상으로 포함시키고, 기술의 식별 및 통제 절차를 강화하는 법이다. 또한 미국 정부는 첨단산업 분야 중국 유학생의 비자 단축(5년→1년, '18) 중국 군부 관련 연구인력 입국금지(1,000명 비자취소, '20비자취소) 등 인적교류도 제한한다.

특히 미국 국방부는 악의적인 사이버 범죄자들이 지속적으로 방위산업계(DIB, Defence Industrial Base)와 국방부(DoD, Department of Defence)의 공급망을 표적으로 삼고 있다고 분석하고 미 국방사업에 참여하는 해외업체를 포함한 모든 업체에 일정 수준의 사이버 보안 체계 구축을 의무화하는 CMMC 제도를 도입키로 한다. 이를 위해 2020년 1월 사이버보안제도 운영을 위한 인증기관(CMMC-AB, Accreditation Body)을 설립하고 2020년 3월 CMMC 모델 1.0을 발표한다. CMMC 모델1.0은 5등급으로 구성되며 17개 도메인(Domain)과 171개 프랙티스(Practice)로 구성되었다. 그러나 미국 방산업체들이 CMMC 프레임워크 구축에 반발하자 이를 수용한 미국 국방부는 2021년 12월 3개 등급 14개 도메인 110개 프랙티스로 구성된 모델 2.0을 발표하였다. CyberAB에서는 CMMC 모델 2.0이 모델1.0에 비해 5개에서 3개로 등급이 간소화되었고 사이버보안 역량을 강화시키면서 중소기업이 구현할 수 있는 비용효율적이고 합리적으로 설계되었다고 강조하고 있다.

즉, CMMC는 점점 더 빈번하고 복잡해지는 사이버 공격으로 부터 미국 방위산업계(DIB)를 보호하기 위해 그동안 특별하게 기밀로 분류하지 않고 공유되었던 통제된 미분류정보(CUI, Controlled Unclassified Information) 및 연방계약정보(FCI, Federal Contract Information)의 보

(그림 2) CMMC 타임스케치

호를 강화하는 것을 목표로 미국 국방부(DoD)에서 구축한 프로그램인 것이다. 2026년부터 미국 국방사업에 참여하기 위해서는 CMMC 인증 요구 레벨을 RFP상에 포함시켜야 할 것으로 예상된다

- 연방계약정보(FCI, Federal Contract Information) : 제품 또는 서비스를 개발하거나 정부에 제공하기 위한 계약에 따라 정부가 제공하거나 정부를 위해 생성한 정보로서 공개할 목적이 아닌 정보를 의미. 정부가 공공 웹사이트 등에서 대중에게 제공하는 정보나 결제 처리에 필요한 단순 거래 정보는 포함하지 않는다(출처: 48 CFR§ 52.204-21, cyberab.org, CMMC 용어집 및 약어)
- 통제된 미분류정보(CUI, Controlled Unclassified Information) : 법률, 규정 및 정부 차원의 정책에 따라 보호 또는 배포 통제가 필요한 정보(2009년 12월 29일자 행정명령 13526호, 국가 기밀 보안 정보, 또는 그 이전 또는 후속 명령이나 개정된 1954년 원자력법에 따라 기밀로 분류되는 정보는 제외). (출처: NIST SP 800-171 Rev 2. cyberab.org, CMMC 용어집 및 약어)

3.2 CMMC(CyberSecurity Maturity Model Certification) 등급

CMMC는 가장 널리 인정되고 있는 미국 국립표준기술연구소(NIST) 사이버보안표준을 사용하고 있고 국방사업 참여 계약업체의 수준을 3개 등급으로 구분해서 인증을 요구하고 있다

업체가 정부에 의해 제공되거나 생산된 정보인 FCI(연방계약정보)만을 취급하면 가장 낮은 수준인 1등급 인증을 요구되며 연 단위로 자체 심사한다. 업체가 CUI(통제된 미분류정보) 까지 취급하게 되면 2등급 이상의 인증이 요구되며 국가 중요보안 정보에 대해서는 3년 주기로 제3자에 의해 심사를 받는다. 최고 전문등급인 3등급은 NIST SP 800-172에 기반하는데 아직 발표되지 않은 상태이다.

3.3 미국의 CMMC와 통합실태조사

CMMC 실행을 위해 미국 국방부가 승인한 유일한 인증기관은 CyberAB이다. CyberAB는 국방부로부터 자금지원을 받지 않는 비영리법인으로서 수익원은 시스템 내 참가자로 부터 자격 등록 및 갱신 수수료 등으로 유지된다.

CMMC의 시스템내에는 인증기관인 CyberAB를 중심으로 심사기관 C3PAO(CMMC 3rd Party Assessor Organization), 컨설팅 기관 RPO(Registered Provider Organization), 교육훈련기관 LTP(Licensed Training Provider), 교육커리큘럼 개발기관 LPP(Licensed Publishing Partner) 등이 주요 구성기관이다

특히 CMMC 등급 취득의 핵심인 심사기관 C3PAO 로 승인받기 위해서는 미국의 신용조사 전문회사인 Dun & Bradstreet 로 부터 배경 조사

〈표 2〉 CMMC 2.0 등급별 프랙티스 및 심사

등 급	프랙티스 / 모델	심 사
3등급 (전문, Expert)	• 110+개 프랙티스 • NIST SP 800-172에 기반	• 3년주기 정부 주도심사
2등급 (고급, Advanced)	• 110개 프랙티스 • NIST SP 800-171(r2)에 연계	• 국가중요보안정보는 3년주기 제3자 심사 • 일부 프로그램은 연 단위 자체심사
1등급 (기본, Foundational)	• 17개 프랙티스 • 48 CFR 52.204-21에 명시된 기본적인 이행과제	• 연 단위 자체 심사

〈표 3〉 CMMC의 14개 도메인과 2등급 110개 프랙티스 요약 (NIST SP 800-171)

도메인	프랙티스	
❶ 접근통제 (AC)	• 시스템 접근 요구사항 설정 • 원격 시스템 접근통제	• 내부 시스템 접근통제 • 무선, 모바일 장치, 휴대용 저장장치 통제
❷ 인식및교육훈련 (AT)	• 역할 기반 위험인식, 교육훈련	• 내부자 위협 인식
❸ 감사및책임추적 (AU)	• 감사 요구사항 정의 • 감사정보 식별 및 보호	• 감사 수행 • 감사로그 검토 및 관리
❹ 구성관리 (CM)	• 구성 기준 설정 • 최소 기능만 구성	• 구성 및 변경관리 수행 • 사용자 설치 통제
❺ 신원확인및인증 (IA)	• 신원 확인 • 비밀번호 관리	• 인증, 다단계 인증, 재생방지 인증
❻ 사고대응 (IR)	• 사고대응 계획 • 사고대응 테스트	• 이벤트 감지 및 보고
❼ 유지관리 (MA)	• 유지보수 관리 • 원격 유지관리 통제	• 장비 소거 및 미디어검사
❽ 미디어보호 (MP)	• 미디어 식별 및 표시 • 미디어 처리 • 백업 보호	• 미디어 보호 및 통제 • 운송 중, 미디어 보호
❾ 인원보안 (PS)	• 신원조사	• 인사조치 중 통제필요정보 보호
❿ 물리적보안 (PE)	• 물리적 접근 제한 • 시설 모니터링	• 방문자 에스코트 • 대체 작업장 보안
⓫ 위험평가 (RA)	• 위험 식별 및 평가 • 취약점 보완	• 취약점 진단
⓬ 보안평가 (CA)	• 시스템보안 계획수립 및 관리 • 보안통제 모니터링	• 보안통제 평가
⓭ 시스템 및 통신 보호 (SC)	• 시스템 및 통신에 대한 보안 요구사항 정의 • 시스템 경계에서 통신 통제	• 암호키 관리
⓮ 시스템 및 정보 무결성 (SI)	• 정보시스템 결함 식별 및 관리 • 비인가 사용 식별	• 악성코드 보안 • 통신 모니터링

를 받은 후 비즈니스 고유 식별 코드이며 이미 미국 정부와의 계약 프로세스에서 중요한 역할을 하고 있는 DUNS 번호를 받아야 한다. 그리고 무엇보다도 100% 미국 시민권자 소유의 기업이어야만 한다. 또한 CMMC 인증심사원(CCA)도 미국 시민권자이어야 취득할 수 있도록 제한되어 있다. 우리 정부와 방산업체 입장에서는 CMMC 진입 장벽이 너무 높을 뿐 아니라 기술 보호를 위한 인증심사 과정에서 우리 기업 내부 중요 정보가 외국 기업에게 노출될 우려가 있는 것이다.

이러한 문제를 해소하기 위해 방사청은 매년 실시하고 있는 통합실태조사를 미국 CMMC 인증과 연계시키는 방안을 추진하고 있다. 즉 우리 정부가 주관하는 통합실태조사를 완료하면 미국 CMMC 1등급에 해당하고 2등급의 경우는 필요시 추가 인증하는 내용으로 2024년 중 미국과 상호인정(MRA) 체결할 계획이다.(참고 : 2023 전반기 방산기술보호 합동설명회, 방위사업청)

이를 위해 방사청은 통합실태조사와 CMMC 등급 취득을 연계하기 위해 통합실태조사를 분석하여 점검항목 보완 연구를 진행중이다. 즉 통합실태조사 점검항목 내용과 이행 점검을 CMMC 프랙티스와 매칭시킴으로서 CMMC가 요구하는 보안수준을 확보한 것으로 인정 받겠다는 계획이다.

〈표 4〉 CMMC 시스템 및 통신보호(SC)와 통합실태조사 자가진단표 대응분석

CMMC 시스템 및 통신보호 (이행과제 번호/내용)	실태조사 자가진단 항목 (점검번호/ 점검내용)	대응결과
SC.L1.3.13.1 경계 보호	4.1 정보보호 시스템 설치 및 운용	대응 가능
SC.L1.3.13.5 공개접근 시스템 분리	4.2.1 외부망차단체계 구축 운용	대응 가능
SC.L2-3.13.2 보안 공학적 원칙사용	아키텍쳐 설계, S/W기술 개발 및 시스템 공학 원칙 적용	대응 부족
SC.L2-3.13.3 역할 분리	4.6 정보통신기기 및 저장매체관리	대응 가능
SC.L2-3.13.4 공유 자원 통제	4.7 자료별 접근범위 제한	대응 가능
SC.L2-3.13.6 예외에 의한 네트워크 통신	4.1 정보보호 시스템 설치 및 운용	대응 거눙
SC.L2-3.13.7 분할 터널링	4.2 정보통신망 외부망과 차단 4.4 긴급사태 대비	대응 가능
SC.L2-3.13.8 전송 자료 보호	4.6 정보통신기기 및 저장매체관리	대응 가능
SC.L2-3.13.9 연결 종료	4.7 자료별 접근범위 제한	대응 가능
SC.L2-3.13.10 암호키 관리	4.1 정보보호 시스템 설치 및 운용	대응 가능
SC.L2-3.13.11통제필요정보 암호화	4.1 정보보호 시스템 설치 및 운용	대응 가능
SC.L2-3.13.12 협업 장치 통제	협업 컴퓨팅장치 원격활성화 금지 및 사용중지 표시	대응 부족
SC.L2-3.13.13 모바일 코드 통제	자바스크립트, 엑티브엑스 등 모바일코드 사용 통제 및 감시	대응 부족
SC.L2-3.13.14 인터넷전화기술통제	인터넷전화 기술의 시스템 위협 대비 통제 및 감시	대응 부족
SC.L2-3.13.15 통신 진본성 보호	4.1 정보보호 시스템 설치 및 운용 4.6 정보통신기기 및 저장매체관리	대응 가능
SC.L2-3.13.16 저장된 자료 보호	4.1 정보보호 시스템 설치 및 운용	대응 가능

그런데 통합실태조사의 자가진단표와 CMMC 프랙티스를 비교했을 때 가장 큰 차이가 나는 도메인은 CMMC의 「시스템 및 통신보호(SC)」이다. 아직 CMMC 프랙티스를 실제 적용한 사례와 정보가 제한적이라서 판정에는 제한이 따르지만 「시스템 및 통신보호(SC)」16개 프랙티스 중에서 '보안 공학적 원칙 사용' (SC.L2-3.13.2) "협업 장치 통제'(SC.L2-3.13.12) '모바일 코드 사용 통제와 감시'(SC.L2-3.13.13) '인터넷 전화 기술 사용 통제 및 감시' (SC.L2-3.13.14) 등은 자가진단표의 항목과 매칭하기 어렵다. 게다가 모두 고난도의 보안 수준을 요구하는 내용으로서 현장에서 일시에 반영하는 것은 부담이 큰 프랙티스이다. 다음 <표 4>는 CMMC '시스템 및 통신보호' 프랙티스와 자가진단표의 점검항목을 매칭시킨 후 대응 가능 여부를 판정한 내용이다

4. 결 론

미국 국방부는 미국의 국방사업을 지원하는 외국기업이 민감한 국가안보 정보를 보호할 수있도록 CMMC 프레임워크를 갖추도록 요구하고 있다. 이에 주무부처인 방위사업청도 국내방산업체들이 순조롭게 CMMC에 대비할 수 있도록 통합실태조사 완료가 미국 CMMC 등급 인증 취득으로 연계되도록 추진하고 있다. 이를 위해서는 CMMC를 충족할 수 있도록 통합실태조사 항목을 추가적으로 보완하는 작업이 선행되어야 할 것이다.

그리고 무엇보다도 미국 국적자 또는 미국 소유기업만 심사관 및 심사기관 자격이 부여되는 현재의 CMMC제도는 우리의 사이버안보 주권을 위협할 수 있다. 따라서 방위사업청은 미국과 CMMC 상호인정협약(MRA) 체결과 병행하여 CMMC 인증기준과 절차를 준수하되 CMMC 심사원에 한

국 국적자에 의한 인증심사가 가능하도록 해야 할 것이다. 또한 공정성과 객관성 확보를 위해 CyberAB와 같은 독립된 비영리법인으로 인증기관을 설립하는 등 관련 체계도 갖추어 나가야 할 것이다.

끝으로 방산업체들은 CMMC 도입으로 통합실태조사 과정에서 난이도가 가장 높은 정보보호 비중이 더욱 높아지는데 부담을 갖고 있다. 더구나 CMMC 제도 초기인 관계로 관련 전문가도 부족한데다 CMMC 프랙티스 구현에 대한 경험 사례도 없는 등 정보가 매우 제한적이다. 따라서 정부는 제도 개선과 더불어 방산업체을 대상으로 CMMC 인증제도와 등급별 프랙티스 등을 충분히 이해할 수 있는 다양한 교육·훈련 프로그램을 개설하여 방산업체들이 CMMC 도입에 대비할 수 있도록 지원해야 할 것이다.

참 고 문 헌

[1] 한국산업보안연구학회, “산업보안학” pp. 437-453, 박영사, 2019.

[2] 이민재 역, “CMMC의 이해”, pp.115-345, 2021

[3] 박언경,왕상한, “미국 수출통제개혁법 제정의 함의”, 법제연구제 61호, pp.300-304, 2021

[4] 김동선, 류연승, “미국 CMMC제도 대응을위한 통합실태조사 제도개선연구”,한국방위산업학회지, 제29권, 제3호, pp.54-57, 2022

[5] 방위사업청(www.dapa.go.kr) “2022-2026 방위산업기술보호 종합계획“ pp.6-13,

[6] 방위사업청, “2023 전반기 방산기술보호 합동설명회”, 방위사업청,국정원,방첩사

[7] 한국산업기술보호협회, 2023년 통합실태조사관 직무역량강화 교육, 2023.8,

[8] 한국산업기술보호협회, 2023년 방위산업기술보호 책임자교육, 2023.6

[9] 산업보안실무위원회, ”국가공인 산업보안관리사“, pp.60-61케듀아이, 2023

[10] 김혜정, ”기술보호에 관한 주요 국내법분석 및 시사점, 한국지식재산연구원, pp.4-13, 2022-29호

저 자 약 력

장 항 배

이메일 : hbchang@cau.ac.kr

- 2014년~현재 중앙대학교 산업보안학과 교수
- 현재 한국공학한림원 회원 (기술경영정책)
- 전 방위사업청 방위산업기술보호 실무위원회 위원
- 전 국가과학기술자문회의, ICT융합전문위원회 위원
- 관심분야 : 산업보안, 방산기술보호, 데이터보안

김 선 영

이메일 : syk4590@gmail.com

- 2019년~현재 아주대학교 지식정보공학과 교수
- 2023년 10월~현재 CMMC RP
- 현재 한국산업보안관리사협회 부회장
- 전 한국산업기술보호협회 센터장
- 관심분야 : 기술보호 실태조사, 방위산업보안, 보안지식경영