정 보 보 호 학 회 지
제28권 제6호, 2018. 12

각 軍의 방위산업기술보호 인식 및 역량 제고를 위한 교육 방안

손 창 근*, 류 연 승**

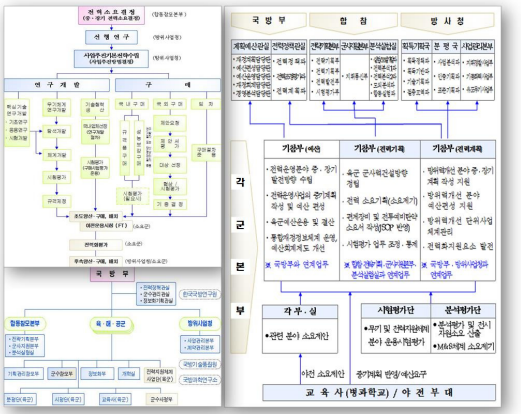
요 약

방위산업기술보호법의 대상기관인 각 軍은 방위산업기술보호 인식 및 역량 제고를 위한 방위산업기술보호 교육이 필요하다. 방위산업기술 즉 기밀기술정보, 비기밀통제기술정보, 핵심기능(CPI)에 대한 보호조치 등 軍 방위력개선사업 실무절차와 관련된 특징을 고려하여 전력소요제기~운용시험평가~후속양상·구매·배치에 이르는 全 단계에 방위산업기술 보호 지침에 따라 보안조치가 이루어져야 한다. 이러한 보안조치는 교육을 통해 효과가 극대화 된다. 따라서 본 연구는 각 軍의 방위산업기술 보호에 관한 교육의 발전방안을 제시하는데 주안을 두었다.

Ⅰ. 서 론

각 軍의 군사력 건설은 국가의 사활이 걸려있는 매우 중요한 사항이다. 군사력 건설은 막대한 국가재원이 사용되고, 소요제기로부터 전력화까지 장기간이 소요되며 절차적 투명성이 요구된다. 특히, 과학기술의 발전 속도가 매우 빠른 최근의 무기체계는 복잡성과 다양성이 증대되고 상호운용성이 더욱 요구되어 관련 부서 간 협업의 중요성이 날로 커지고 있다. 그러나 최근 군사기밀에 준하는 방위산업기술 자료의 대외유출 사고들이 보도되면서 국민의 신뢰 저하와 관련 근무자들의 사기가 저하되고있다. 이러한 어려운 여건을 극복하고 '싸워 이길 수 있는 군사력 건설'을 위해서는 방위력개선업무를 수행하는 실무자들이 관련 법규와 기획관리체계 전반에 대한 이해, 부대편성·교리를 포함한 전력화지원요소, 무기체계의 공학적 지식, 중기계획·예산편성 등 무기체계 획득절차와 전장환경, 작전계획 등을 이해하고 있어야 한다[1]. 또한 방위산업기술보호와 관련해서도 획득 全 단계에 방산기술보호 지침이 프로세스로 반영되어야 한다[2].

[그림 1]와 같이 방위력개선사업과 관련된 각 軍 본부의 역할은 기획관리참모부에서 예산, 전력기획, 전력계획을 담당하고 각 부·실에서는 교육사(병과학교) 및



〔그림 1〕 방위력개선사업 시 각 軍의 역할

야전부대에서 야전 소요제안을 검토하여 관련분야의 소요제안을 기획관리참모부로 제기한다. 무기체계 및 전력지원체계 분야의 운용시험평가는 시험평가단에서 분석평가 및 전시 지원소요 산출과 M&S체계 소요제기는 분석평가단에서 하고 있다.

『방위산업기술보호법』이 2015년 12월에 제정되어 3년이 지났으나 각 軍은 대상기관임에도 불구하고 방산기술보호 관련 시행계획 조차도 없으며 보호대상 기술의 식별·관리와 기술보호 인식 및 역량이 매우 부족한 실태이다. 『방위산업기술보호법 시행령』제21조 (방위

* 명지대학교 대학원 보안경영공학과 박사과정, 육군 제1군단 정보참모처 보안과 (soncg2209@naver.com)
** 명지대학교 대학원 보안경영공학과 교수 (ysryu@mju.ac.kr)

산업기술 보호에 관한 교육) ② 대상기관의 장은 법 제16조 제2항에 따라 소속 임직원을 대상으로 제1항 각 호의 내용을 포함한 방위산업기술 보호에 관한 교육을 매년 하여야 하며, 그 결과를 교육 후 30일 이내에 방위사업청장에게 제출하여야 한다[3]. 하지만 군에서는 방위력개선사업의 주무부서인 기획관리참모부 또는 시험평가단, 분석평가단, 전력지원체계사업단에서 조차도 방위사업청 방위산업기술보호 교육과정에 참여하는 인원이 전무한 실정이고 자체 실무위탁교육 또는 초빙교육 조차도 없는 실태이다. 따라서 본 연구에서는 이러한 현실을 보완하기 위해 먼저 美 국방부 국방보안국 보안개발센터(DSS CDSE: Defense Security Service, Center for Development of Security Excellence)[4]의 국방 기밀 및 통제기술 보호 관련 교육현황을 조사하여 시사점을 도출하였다. 국내는 방위사업청이 제시한「2017~2021 방위산업기술보호 종합발전계획」[5]의 4대 추진방향 중 '기술보호 인식 및 역량제고'에 따라 추진하고 있는 방위사업청 방위산업기술보호 교육 실태를 2017~2018년 추진계획[6]에 주안을 두고 살펴봄으로 각 軍 방위산업기술보호 교육에 대한 발전방안을 도출하고자 하였다.

Ⅱ. 美 DSS CDSE 방위산업기술보호교육

2.1. DSS 보안교육 인증 항목

美 국방보안국(DSS)의 조직은 크게 국가산업보안, 인원보안, 대정보, 보안교육개발센터로 구성되어 국방보안 지원에 대해 주관하고 있다. 특히 軍 보안 교육은 국방보안국 보안개발센터에서 주관하며, 美 국방부 및 정부 기관, 방산업체 보안 관계자를 대상으로 보안교육·훈련 프로그램을 진행하고 있다.

사용자는 CDSE Web 사이트에 등록하여 웹 기반 교육·훈련을 진행하는데 프로그램은 ① 교육(Education), ② 훈련(Training), ③ 출처·교안으로 구성되어 있다. 이러한 프로그램은 소집교육, 사이버 강사, E-러닝, 동영상, CBT, 교안 등의 다양한 수단으로 이루어지고, 교육은 美 의회에서 인증된 수준 높은 보안교육(ACE Credit : American Council Education Credit)을 실시하여 교육 인증자격을 부여하고 있다. [표 1]과 같이 교육 인증은 5개의 과정으로 구분되어 세부 프로그램 교육 및 평가를 진행하며, 프로그램별 소규모(20명), 분기 단위 장기간(4개월) 교육을 실시 중이다[4].

〔표 1〕 美 국방보안국(DSS) 보안교육 인증 항목

Classification	Content
Education Certificate	① The CDSE Certificate in Risk Management ② The CDSE Certificate in Security Leadership ③ The CDSE Certificate in Security Management ④ The CDSE Certificate in Security(Generalist) ⑤ The CDSE Certificate in Systems and Operations
U.S Congress Certificate Education Programs (ACE Credit)	① Writing and Communication Skills for Security Professionals ② Security as an Integral Part of DoD Programs ③ Organizational Considerations In Applying Security within Federal and DoD Bureaucracy ④ Constitutional Law and Its Application to DoD Security ⑤ Understanding Adversaries and Threats to the United States and the DoD ⑥ Budgeting and Financial Management for Security Programs ⑦ Human Resource Management for DoD Security ⑧ Research Methods, Data Analysis, and Reporting to Support DoD Security Programs ⑨ Assessment and Evaluation of DoD Security Programs ⑩ The Future of Security Systems and Cybersecurity ⑪ Leadership in DoD Security ⑫ Effective Communication in DoD Security ⑬ Security in the DoD Acquisition Process ⑭ Cybersecurity and Oversight of Information System Security ⑮ Statutory, Legal, and Regulatory Basis of DoD Security Programs ⑯ Risk Management Project and Advanced Studies

2.2. DSS 보안훈련 항목 및 방법

[표 2]와 같이 훈련은 기본적인 SETA 프로그램 정책을 통해 실무 능력을 배양하는데 목적이 있으며, 대정보, 사이버 보안, 산업보안 등 12가지의 과정으로 구분되어 실용적인 세부 프로그램을 제공하고 있다[4].

〔표 2〕 美 국방보안국(DSS) 보안훈련 항목 및 방법

Type	Content	
Traning Type	① Counterintelligenc ② Cybersecurity ③ General Security ④ Industrial Security ⑤ Information Security ⑥ International Security	⑦ Operations security ⑧ Personnel Security ⑨ Physical Security ⑩ Special Access Programs ⑪ Sensitive Compartmented Information
Traning Method	① Intructor led ② e-learning ③ Curricula	④ Shorts ⑤ Webinars ⑥ Virtual Instructor-led

2.3. 美 국방보안국 SPED 인증제

美 SPED(Security Professional Education Development, 보안 전문 교육 개발) 보안 인증제는 보안실무자의 보안업무 능력 및 전문성 향상을 위해 제작된 미국 국방보안국 보안 인증 프로그램이다[4, 7, 8]. 美 SPED 보안 인증제 목적은 다양한 보안 분야에서 상호운용성을 향상시키고, 전문적인 능력 개발 및 훈련을 촉진하며 인증된 보안전문가 능력을 개발하는 것이다. 대상은 군인·군무원 등 미 국방부 보안 관련 직위자와 산업보안 전문가 실무자 등이다. 美 SPED 인증제 평가는 국방보안국 산하 프로그램 관리소(DSS CDSE PMO)에서 주관하며, 평가시간은 2시간 이내로 일자 및 장소는 사용자 신청에 따라 편의가 고려되어 선정된다. 신청절차로 인터넷 STEPP 웹 계정에 등록하여 신청하게 되며, 평가 장소 도착 시 필기구, Test용 컴퓨터가 지정 장소에 구비되어 있다. 인터넷 STEPP 사이트 계정이며, 사이트 평가 인증 단계는 Eligible에서 Certificant의 4단계로 나뉘어진다. 재갱신 주기는 인사 이동을 고려하여 2년이며 2년 이후 미갱신 시 사이트 계정에서 인증만료로 전시되고, 평가 이전 CDSE 교육 웹사이트에서 E-러닝, CPT, 시험 준비절차, 시험 출처 등 시험 준비가 가능하다. 美 SPED 보안 인증제는 크게 3개의 인증제로 나뉘어진다. ① 첫 번째 보안 실무 이해를 위한 SFPC, ② 보안 실무 응용을 위한 SAPPC, ③ 위험평가와 보안 프로그램 관리를 이해·응용하는 SPIPC로 구성된다.

구 분	① SFPC	② SAPPC	③ SPIPC
명 칭	Security Fundamentals Professional Certification	Security Asset Protection Professional Certification	Security Program Integration Professional Certification
내 용	보안 개념, 원칙, 관습 이해	보안 개념, 원칙, 관습 응용	위험 평가 및 보안 프로그램 관리 이해 및 응용
인증 카드	SPēD SFPC	SPēD SAPPC	SPēD SPIPC
시험자격	① 국방부 소속 직위자 ② PMO 계정 승인	① SFPC 인증 취득자 ② 국방부 소속 직위자 ③ PMO 계정 승인	① SFPC 인증 취득자 ② 국방부 소속 직위자 ③ PMO 계정 승인
합격조건	인증제 평가에서 자격점수 취득		
유지조건	· 2년 단위 전문적인 개발 및 노력 지속 / STEPP 계정 최신화 및 활동 유지		
재시험 환경	· 평가 인증제, 사용자 인증제 現 유지와 관계 없이 구시대적으로 판단 시(DSTC/국방보안훈련부) · 2년 인증 기간 內 인증제 유지조건 미충족 시		

〔그림 2〕 美 DSS SPED 보안 인증제 구분

2.4. SPED 방위산업기술보호 문제 구성

SFPC 인증제는 정보보호 25 %, 인원보안 25 %, 시설보안 25 %, 산업보안 13% 등으로 출제되고, 실무자 이해를 중점으로 내용이 구성되어 있다. SAPPC 인증제는 정보보호 28%, 인원보안 31%, 일반보안 18%, 산업보안 13% 등으로 출제되고, 실무자의 응용을 중점으로 내용이 구성되어 있다. SPIPC 인증제는 위험평가 41%, 위험관리 35%, 프로그램 및 임무 보장 16% 등으로 출제되며, 관리자로서 관리 이해 및 응용을 중점으로 구성되어 있다.

SPED 시험 내용은 미공개이나, CDSE 사이트에서 시험준비도구(CPT)를 이용하여 시험 출제 유형·내용에 대해 대비할 수 있다. CPT는 인터넷 웹사이트를 이용하여 SPED 시험준비를 소개하고 샘플 내용으로 모의 시험 평가가 가능하다. CPT는 개인 평가 및 이해 경험치 수준을 측정하는 Experience Checklist, 각 주제 영역에 대한 질문으로 사용자의 주관식 상세 답변 설명이 요구되어 추가 학습기회를 부여하는 Knowledge Test, 시나리오 기반 실질적인 예시형 문제를 제공하여 객관식 선다형, 진위형 등으로 답을 할 수 있는 Practice Test로 구성되어 있다.

앞에서 살펴본 美 DSS CDSE 방위산업기술보호교육이 시사하는 바는 군인·군무원 등 美 국방부 보안 관련 직위자와 방산보안 전문가 실무자를 대상으로 다양한 보안 분야에서 상호운용성을 향상시키고, 전문적

〔표 3〕 美 SPED 방위산업기술보호 출제비율 및 내용

Classification		%	Main Areas of Expertise
SFPC Industrial Security		13	1. Contracts and Contract Administration 2. Industrial Security Concepts 3. Personnel and Factility Securiy Clearance Under NISP 4. Visits and Meetings
SAPPC Industrial Security		13	1. Centracts and Contract Administration 2. Industrial Security Concepts 3. Personnel and Facility Security Clearance Under NISP 4. Foreign Ownership, Control, or Influence (FOCI) 5. Visits and Meetings
SPIPC	① Risk Assessment	41	1. Risk Management Benefits & Costs 2. Risk Assessment Concepts & Principles 3. Sources of Threat & Vulnerability Information
	② Risk Management	35	1. Strategies for Controlling and / or Managing Risks
	③ Program and Mission Assurance	16	1. Essential Functions of a Security Program 2. Approaches & Criteria for Evaluating Effectiveness of Security Policies, Plan, & Program Activities
	④ (Planning, Programming, Budgeting and Execution)	8	1. PPB&E Process, Concepts & Principles

인 능력 개발 및 훈련을 촉진하며 인증된 보안전문가 능력을 개발하는 것이다. 그 중에 하나에 방산기술보호 전문가를 교육하고 인증하여 자격을 부여하고 있다는 것이다. 따라서 국방부에서 추진하고자하는 국방보안자격인증제 [9]와 2019년 시행되는 국방보안관리사 [10, 11] 시험항목에 방위산업기술보호도 평가의 한 부분으로 반영되어야 함을 알 수 있다.

Ⅲ. 국내 방위산업기술보호 교육 현황

3.1. 방위사업청의 교육 과정

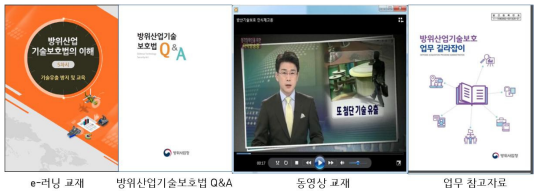
방위사업청은 방위산업기술보호 교육과정을 외부에 위탁하여 운영하고 있다. 방위산업기술보호법의 시행 이후인 2016~2017년은 방위산업진흥회에 위탁하다가 2018년에 전략물자관리원에 위탁하였다[12]. [표 4]는 방위사업청 주관 방위산업기술보호 교육 참석인원 및 과정을 보이고 있다. 2017년은 2012년에 비해 약 5.5배(3,000명) 증가한 인원에 대해 교육하여 양적으로 크게 증가하였다. 2017년 산・학・연 및 유관기관의 기술보호 전문강사 인력풀은 8개 분야 약 40여명을 확보하고 있다[6].

또한, 방위사업청은 [그림 3]과 같이 대상기관 및 방산관련업체가 임직원을 대상으로 자체 전산시스템을 활용하여 교육할 수 있는 e-러닝 콘텐츠 지원 및 방위산업기술보호법 Q&A를 작성・발간하여 2017년 4월부터 지원하고 있다. 또한 2017년 10월에는 방위산업기술보호 홍보・교육 동영상 제작 및 배포하여 지원하고 있다[6].

〔표 4〕 방사청 주관 방위산업기술보호 교육인원 및 과정

Year	2012	2013	2014	2015	2016	2017
People	548	1,174	1,368	1,869	2,170	3,000

Course	Time	Content
Defence Technology Security General	6H	Examples of Technology Leak, Etc 4 Subjects
Defense Industry Export Clearance	4H	Law and Institution, Etc 4 Subjects
Professional for Defense Technology Security	12H (1박 2일)	Main Policies, Etc 8 Subjects
R&D Personnel	4H	R&D Security Management, Etc 4 Subjects
Information System Personnel	4H	Information Security, Etc 4 Subjects
CEO Seminar for Defense Technology Security	2H	Examples of Technology Leak, Etc 2 Subjects



e-러닝 교재 방위산업기술보호법 Q&A 동영상 교재 업무 참고자료

〔그림 3〕 주요내용은 중요성, 법규 및 제도, 종합・시행계획, 보호체계 구축, 교육 실시. 실태조사, 유출・침해 금지 및 신고 등

또한, 협력기관으로 중소벤쳐기업부, 한국산업기술보호협회, 중소기업기술정보진흥원, 대중소기업 농어업협력재단으로 업무협약을 체결하여 방위산업기술 보호 및 지원을 위한 협력체계를 구축하고 있다.

방위사업청과는 별도로 한국방위산업진흥회 방위산업교육센터에서는 방산보안실무 과정을 개설하고 방위산업기술보호 등 5개 과목을 운영하고 있다[13].

3.2. 대학(원) 과정

방산기술보호를 포함한 방산보안에 특화된 대학(원)으로는 명지대 대학원 보안경영공학과/융합보안학과에서 방산보안협의회[1]와 협약을 맺고 방산보안 석박사 전공 트랙을 운영하고 있다. 주요 과목으로는 방산보안개론, 방산보안실무, 국방보안관리, 방위사업론, 무기체계론, 방산기술보호특론, 방산기술보호기법, 지식재산권보호, 정보보호체계, 연구개발보안, 위험관리론 등이 개설되어 있다.

3.3. 시사점

앞에서 살펴본 방위산업기술보호 교육 현황이 시사하는 바는 첫째, 軍은 방위사업청 및 대학 등 방산기술보호 전문 기관과 협력하여 방위산업기술보호 교육 체계를 구축하여야 한다. 둘째, 軍 특성에 부합된 방위력 개선 업무절차를 고려한 교육콘텐츠, 교육과정별 프로그램을 개발하고 이를 교육하기 이한 방위산업기술 보호 내규를 마련해야 한다. 그리고 시행여건을 보장하기 위해서는 예산 사업으로 방위산업기술보호 계획을 수립하는 것부터가 기술보호 인식 및 역량제고의 첫 걸음이 될 것이다.

1) 방산보안협의회는 방산업체 및 방산관련업체의 보안담당관의 조직으로 방산보안 발전을 위해 운영되고 있음

Ⅳ. 軍 방위산업기술보호교육 발전방안

4.1. 「軍 방위력개선 실무지침서」에 '방위산업기술 보호'의 반영

2017년 12월 육군본부 방위력개선업무 취급 및 관련 인원 100명 대상 현장실태조사 결과에 따르면, "방위산업기술보호 법규 및 제도를 알고 있는가?"에 답변한 사람은 15% 내외이었다. 15%의 인원을 대상으로 "군사비밀은 아니지만 방위력개선사업 관련 비기밀통제기술정보(기술자료 등) 관리는 어떻게 하는가 ?"에 대한 답변으로 "『공공기록물 관리에 관한 법률』에 의해 "비공개 문서(파일)로 관리하는 수준이다"라고 답변하였고 이에 대한 대책으로 방위력개선 실무지침서에 기술보호 대책 반영을 요구하였다[14].

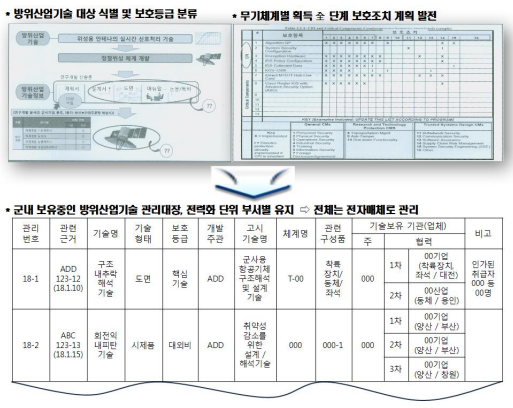
육군은 매년 1월에 방위력개선사업관련 변경지침 등을 고려하여 육군「방위력개선 실무지침서」를 발간하여 자체 교육을 실시하고 있다[1]. 그러나, 육군의「방위력개선 실무지침서」내용에는 방위산업기술보호 관련 내용이 전혀 없고 각 軍의 보안정책에도 방위산업기술보호 분야가 없는 것은 방위산업기술보호 대상기관인 각 軍의 기술보호에 대한 인식이 전무한 것으로 평가된다.

방위사업청은 용역연구[15] 등을 통해 '방위산업기술보호지침'을 작성하였고 2019년 1월부로 배부할 예정이다[16]. 따라서 대상기관인 각 軍 본부 기획관리참모부에서는 2019년 실무지침서 발간 시 별지에 방위산업기술 보호지침을 반영해야 한다. 보호지침의 반영이란 "무엇을 교육할 것인가?"를 의미한다. 이를 위해서는 첫째, 각 軍별로 방위산업기술 보호내규를 작성해야 한다. 둘째, 방위산업기술보호 연간 계획을 수립해야 한다. 셋째, 군에서 보호하고 있는 보호대상 기술을 식별해야 한다. 넷째는 보호대상 기술의 취급~자료관리~관리대장(자료관리 카드) 관리지침을 부여해야 한다.

취약사례를 살펴보면 먼저 무기체계 및 전력지원체계별 ① 기밀기술정보 ② 비기밀통제기술정보 ③ 핵심기능정보(CPI) 분류와 보호조치의 구분이 없다. 또한 합참의 경우 연간 70여건 이상의 무기체계 소요를 결정중이며, 2016년 경우에는 도약적 우위확보 전력 소요 창출, 소요 최적화 등 소요결정 건수가 66건에서 129건으로 증가 하였다. 이러한 Top-down식 소요기획 업무는 더욱 증가될 것으로 예상된다. 특히, 합동전략실무회의-합동전략회의-합동참모회의가 통상 1주일 간격으로 이루어지고 있어 월 평균 5회 정도의 회의록을 생산하여 약 30여개 부대(서)에 배부하고 있다. 특히, 전자적 수단을 활용하여 배부하는 것이 효율적이나 회의록 분량의 방대함·검토시간의 제한으로 회의 1주 前 인편으로 비밀을 배부하는 등의 행위는 업무 효율성이 매우 떨어진다. 이를 위한 취약점 해소대책으로 합참 內 부서에서는 '보안나라'(비밀유통시스템)로 합참 外 부서는 DTIMS T-시스템으로 배부하는 방안도 검토되어야 한다.

넷째, 각 軍의「방위력개선 실무지침서」에 '방위산업기술 보호지침'의 반영을 위하여 각 軍의 업무 프로세스를 면밀히 분석하여 이를 SOP(Standard Operating Procedure)화 해야 한다. [그림 4]는 각 軍에서 방위산업기술보호 대상을 식별하고, 식별된 보호대상(산출물별) 보호등급을 지정·분류하고, 획득 全 단계별로 보호조치 계획을 수립하여 시행하는 방안을 예시로 제시한 것이다. 그 과정에 산출물은 전력화 단위 부서별로 '방위산업기술 관리대장'을 유지하는 절차를 예시하였다. 이러한 내용이 면밀히 검토되어 보호지침으로 반영되어야 한다.

다섯째, 육군 방위산업기술보호 총괄 책임자 및 기술보호 부서 책임자를 육군의 특성에 맞게 내규·조직도·직제규정 등에 명시해야 한다. 여섯째, 방위산업기술보호 자가진단표를 제정하고 주기적으로 자가진단을 실시하여 취약점을 개선하여야 한다. 일곱째, 방위산업기술 취급 및 관련 인원 대상 교육계획을 수립하여 직책·수행하는 업무에 맞게 교육을 매년 1시간 이상 실



〔그림 4〕 방위산업기술 보호대상의 식별 및 보호조치와 전력화과정의 산출물관련 방위산업기술 관리대장 예규화

시해야 한다.

4.2. 군별 e-러닝 홈페이지 운영

육군본부는 e-보수·전문교육 스마트 포털을 운용 중에 있다. 방위산업기술 취급 및 관련 인원이 방위산업기술보호 업무 절차를 언제든지 참조할 수 있도록 군별 e-러닝 홈페이지에 방위산업기술보호 교육 콘텐츠를 탑재해야 한다.

美 MOOC(Massive Open Online Course) 프로그램은 '08년 미국 OER(Open Eucational Resources) 운동에서 시작되어 확산되었으며, 인터넷 기반 온라인 공개강의 프로그램을 신설하여 대중들을 대상으로 운영 중이다[17, 18]. 국방부에서도 2017년부터 합동군사대학교에 국방원격교육체계(M-MOOC)를 운용하고 있다. 따라서 필요시 방위력개선사업을 담당하는 기획관리참모부 및 시험평가단, 전력지원체계사업단 대상으로는 합동군사대학교에서 운용하는 M-MOOC 활용하여 '방위산업기술보호과정'을 신설하여 운용하는 방안도 고려해 보아야 한다. 이를 위해서 각 軍은 방위력개선사업 절차를 고려하여 軍 특성에 부합된「방위산업기술 보호지침」을 디지털 콘텐츠로 개발하여 탑재해야 한다. 이를 위해 방위사업청에서 제공하는 기술보호 동영상 등 교육용 콘텐츠를 벤치마킹한다.

4.3. 군별 실무위탁교육과정 운영

육군은 인사참모부 인재개발과 주관으로 소관업무의 전문성 향상 및 전문인력 양성을 위해 매년 평균 300여 개 실무위탁교육과정을 실시하고 있다. 하지만 방위산업기술보호 교육과 관련된 실무위탁교육 과정 및 예산은 없는 실태이다. 따라서 육군본부의 기획관리참모부 등 방위력개선사업 관련부서와 분석평가단, 시험평가단 등 주요부서의 경우에는 맞춤형으로 외부의 방위산업기술보호교육 전문기관에 위탁교육 과정을 반영해야 한다. 이러한 효과는 근거리에서 많은 인원이 참가가 가능하기 때문이다. 내용·장소 면에 있어서도 육군 특성에 부합되도록 (가칭) "방위력개선사업 기술보호 과정"을 신설하여 육군본부 내 강의장에서 운용하는 방안도 고려해야 한다. 이 경우는 육·해·공군본부 대상인원을 통합하여 시행함으로써 상호 시너지 효과를 높이는 교육방법도 검토되어야 한다.

4.4. 기반 및 여건 조성

軍의 특성 상 간부들의 병력순환 및 보직 교체율과 망각주기를 고려하면 주기적인 방위산업기술보호 전문가 초청 교육이 필요하다. 이를 위한 예산을 반영하고 체계성과 연속성을 유지하는 기반을 조성하여야 한다. 이는 전문성 향상 → 방위력개선사업의 효율성 향상 → 무기체계의 품질 향상으로 궁극적으로는 예산절감 및 위험 관리강화 등 경제적 효과로 이어질 것이다[19].

Ⅴ. 결 론

각 軍은 방위산업기술보호법의 대상기관이다. 방위산업기술 정보에 대한 보호조치 등 방위력개선사업 실무절차와 관련된 특징을 고려하여 전력소요제기~운용시험평가~후속양상, 구매, 배치에 이르는 全 단계에 방위산업기술 보호지침에 따라 보안조치가 이루어져야 한다. 이러한 보안조치는 교육이 없이는 시행이 불가능하다.

본 논문에서는 방위산업기술보호법 대상기관인 각 軍에 방위산업기술보호 교육을 시행하기 위한 방안을 제시하였다. 첫째, 「각 軍 방위력개선 실무지침서」에 '방위산업기술 보호지침'이 반영되어야 한다. 둘째, 군별 e-러닝 홈페이지에 방위사업청 지원 방위산업기술보호 콘텐츠를 탑재 활용해야 한다. 셋째, 군별 실무위탁교육과정에 '방위산업기술보호 과정'을 반영해야 한다. 넷째, 주기적인 공감대 형성 및 인식 확산 교육이 이루어지도록 기반 및 여건을 조성해야 한다. 궁극적으로 이러한 위험 관리 강화가 수명주기를 고려한 무기체계의 특성상 유지보수 비용의 절감에 기여하게 될 것이다.

참 고 문 헌

[1] 육군본부, "방위력개선 실무지침서", 2018.

[2] 류연승, "선진국 방산기술보호 사례 및 적용방안", 제15회 국방보안 컨퍼런스, Nov. 2017.

[3] 『방위산업기술 보호법 시행령』,대통령령 제29114호, 2018. 8. 21.

[4] DSS(Defense Security service) Center for Development of Security Excellence, http://www.cdse.edu/

[5] 방위사업청, “2017~2021 방위산업기술보호 종합계획”, 2016.
[6] 방위사업청, “2018년도 방위산업기술보호 시행계획”, 2017.
[7] DSS(Defense Security service), SPED Certification Program Candidate Handbook, http://www.cdse.edu/certification/sped_what, 2014.
[8] DSS CDSE, “Security Professional Education Development(SPED) Certification Program Implementation Plan,” 2014.
[9] 국방부 보안암호정책과, “보안자격인증제 정책 시행방안 및 실무토의”, (2016~2017)
[10] 한국직업능력개발원, “국방보안관리사 자격신설 연구”, 2017.
[11] 법제처, 국방부공고 제2018-186호 “군인사법 시행규칙 일부개정령(안) 국방보안관리사 입법예고”
[12] 한국전략물자관리원, https://www.kosti.or.kr
[13] 한국방위산업진흥회 방위산업교육센터, https://edu.kdia.or.kr
[14] 손창근, “육군 방위산업기술보호교육 발전방안 모색”, 국방부, 2017.
[15] 명지대학교 방산보안연구소, “방위산업기술 유출 및 침해 대응체계 구축 방안 연구”, 방위사업청 연구용역 보고서, Oct. 2017.
[16] 방위사업청 통제정책담당관실, “방위산업기술 보호지침(案)”, Jun. 2018.
[17] 배예나, 박선주, “교육・학습 분야의 新ICT 융합 전략”, 한국정보화진흥원 정보화 정책연구 제1호, 2014.
[18] Wikipedia, Massive open online course, http://en.wikipedia.org/wiki/Massive_open_online_course, 2015.
[19] 한국산업관계연구원, “방위산업 전문교육기관 설립 방안 연구”, pp.4, 2014.
[20] 17-2차 방위산업기술보호위원회 개최 결과, 2017. 11. 29

〈저자소개〉

손 창 근 (Chang-gun Son)
정회원

1993년 2월 : 단국대학교 체육학과 학사
1999년 8월 : 건국대학교 무역학과 국제통상 석사
2017년 7월~현재 : 명지대학교 대학원 보안경영공학과 박사과정
관심분야 : 국방보안정책, 국방보안관리, 방산보안

류 연 승 (Yeonseung Ryu)
종신회원

1990년 2월 : 서울대학교 계산통계학과 학사
1992년 2월 : 서울대학교 계산통계학과 전산과학 석사
1996년 8월 : 서울대학교 계산통계학과 전산과학 박사
2003년 3월~현재 : 명지대학교 컴퓨터공학과 교수
2014년 9월~현재 : 명지대학교 대학원 융합보안학과 교수
2015년 3월~현재 : 명지대학교 대학원 보안경영공학과 교수
관심분야 : 방산보안, 무기체계보안, 보안경영