방위산업기술보호 체계 구축 및 관리 방안 연구

강태우*, 남용석*
*국방기술품질원 감사실
e-mail:twkang12@dtaq.re.kr

A study on the Operational and Management method for Establishing a Defense Industry Technology Protection System

Tae-Woo Kang*, Yong-Seog Nam*
*Quality planning department, Defense Agency for Technology and Quality

요 약

오늘날 방위산업은 국가안보와 경제성장을 동시에 견인하는 핵심 분야로, 최근 K-방산의 글로벌 경쟁력 강화에 따라 기술유출 위협이 급증하고 있다. 특히 내부자에 의한 유출 사례가 전체의 절반이상을 차지하며, 외부로는 사이버 공격의 정교화로 인한 취약점 노출이 심각한 문제로 대두되고 있으며 계속해서 해킹 시도가 이어지고 있는 현실이다. 본 연구는 국방사업의 정부품질보증 업무를 수행하고 있는 본 기관의 기술식별·관리 체계를 강화하고 인적·물리적·사이버보안을 통합한 종합적 보호방안을 적용하여 현장 적용성을 확보하고자 한다.

1. 서론

2015년 방위산업기술보호법(약칭 : 기술보호법)이[1] 제정되고 다음해에 시행 된 이후 지금까지 방위산업기술의 가치와 효용이 저하되는 것을 막고 부적절한 방법으로 유출 또는 더 악용되어 수출되는 현상을 막아주는 장치로서 역할을 해오고 있다. 물론 기술보호법이 제정되기 전에도 방위사업법, 군사기밀보호법, 산업기술유출방지법 등 민·군 산업 전반에 제도적 안정장치가 있었지만 다양한 법률과 법망을 회피하는 문제로 인해 적절하게 대응하기 어렵다는 한계점이 있었다.

하지만 기술보호법의 시행으로 기술을 보유하고 있는 업체가 자율적으로 보호체계를 구축하면서 강화된 처벌 규정을 통해 불법적인 유출에 대한 한계점을 해결할 수 있는 제도가 마련되었다. 이에 따라 정부뿐 아니라 국방 무기체계 품질보증을 담당하는 본 기관도 해당 법의 적용을 받아 업체가 가지고 있는 기술을 보호하고 기술이 유출되지 않도록 할 의무가 있다. 방위산업기술보호법에서 제시된 주요 내용은 동법・동시행령에 따라 매 5년마다 수립된 종합계획을 바탕으로 각 출연기관 및 방산업체는 매년 세부계획을 수립하여 방산기술을 보호할 수 있는 체계를 구축하여 운영하여야 한다. 현재 「22-26 방위산업기술보호 종합계획」 의 주요 목표 및 방향은 국가안보 및 경쟁력 유지수단, 국제사회의 요구, 지능화되는 유출위협에 선제적 대응, 방위산업기술 보호체계 기반조성을 고려하여 튼튼한 방위산업기술 보호체계 구축을 통한 국가안전 보장 및 국익 제고이다[2], 기품원은 종합목표 달성을 위해 국방 보안분야와의 유사분야를 통합하여 효율성 및 효과성을 최적화 하려고 노력하였으며 그에 따라 부서장 중심 자율보안체계 구축과 사이버 대응체계 유지의 목표를 설정할 수 있었다 [표 1].

목표	리더 중심 자율보안체계 확립, 사이버위협 대응체계 유지
추진 방향	중점 사항
1 보안생활화 정착 및 현장 중심 보안활동 강화	① 보안생활화 공감대 형성 및 관련 절차 제공 ② 본원・지역센터 불시 보안점검을 통한 실행여부 확인 ③ 리더 중심 자율점검 및 본원 주관 현장점검 지원
2 사이버위협 선제적 예방 활동 강화	① 내・외부 취약 요소 및 보안 위규행위 점검 강화 ② 사이버공격 차단을 위한 관제 체계 강화
3 보안·기술보호 분야 직무 전문성 강화	① 직무 분야별 전문 교육 수강 및 자격 취득 ② 지역센터별 보안업무 담당자 직무 전문성 강화 ③ 전직원 보안 및 기술보호 중요성 인식 제고
4 고객만족을 위한 업무 추진	① 업무 수행 절차 사전고지, 신속한 업무수행

[표 1] 보안활동 주요 계획

2. 방위산업기술보호 체계 구축 및 운영

방위산업기술보호법을 근거로 방위사업청은 방산기술보호지침 훈령을 제정하였고, 기품원 또한 상위 규정을 근거로 관련 지침을 제정하였다. 관련 내용을 살펴보면 방위산업기술보호 체계 구축을 위해 기술의 식별・관리, 인원통제, 시설보호, 정보보호와 기술보호 체계 구축을 위해 운영해야 할 방안 등이 제시되어 있다.[3] 다만 이러한 내용 들은 국방보안업무 훈령상의 내용과 중복되는 부분이 많은 관계로 효율적인 적용을 통해 효과적인 업무수행을 할 필요가 있다.

2.1 기술의 식별・관리 방안

방위산업기술보호법의 적용을 받는 대상기관은 방위산업기술을 보호하기 위해 관련 지침을 기반으로 기술보호위원회를 구성해야 하며 보호대상 기술을 식별 해야한다. 현재 지정 고시된 방위산업 기술은 센서, 정보통신 등 8대분야, 45개 분류 128개의 기술로 지정되어 있다[4]. 이러한 방위산업기술을 보호하기 위해 위원회를 구성하여 식별・관리 활동을 지속적으로 이행하여야 한다. 기품원은 해당 업무를 수행하기 위해 총괄 책임자를 임명 후 조직특성, 규모를 반영하여 지역에 추가 관리 책임자들을 분포하였다. 식별된 관리대상은 1차 실무심의회 그리고 2차 본심의회를 거쳐서 운영될 수 있도록 지침을 마련하였다. 또한 매달 변동 여부를 확인하고 반기마다 점검을 통해 부서별 관리대상기술 현황을 파악할 수 있는 체계를 구축・보고 방안을 마련하였다.

2.2 현장 중심 보안활동 강화

언론 기사에 따르면 기술유출의 60% 이상은 내부인원에 의해 발생된다고 한다. 이에 인원통제 체계를 구축하는 것이 중요하며 그에 따른 방법중 하나로 현장 중심의 보안강화 활동을 계획하였다. 보안 생활화 실천방법, 관계 제도 설명 등 교육을 통한 공감대 형성 및 점검을 위해 분기별로 전국의 각 부서를 대상으로 현장 점검을 이행하였다. 6주 간의 일정 동안 총 600여명의 직원 교육을 시행하였고 현장에 참석하지 못한 직원들을 위해 영상강의를 작성・배포하여 전 직원의 교육 참여율을 높이는데 기여를 하였다. 또한, 이러한 교육 후 보안 생활화를 위한 점검을 시행하여 교육 효과를 조금 더 강화할 수가 있었다 [그림 1].

[그림 1] 현장 중심 보안활동 프로그램

2.3 시설보호 강화 방안

국방사업에 종사하는 기관이나 업체는 시설강화 방안에 대해 많은 고민을 했을 거라 판단된다. 왜냐하면 이 문제는 “기술보호구역”과 관계가 있기 때문이다. 기술보호구역 이란 관리대상기술을 보유하고 있는 건물 또는 장소를 지칭하는데 기술과 관련된 정보는(도면, 개발 보고서 등) 한곳에 있지 않고 대부분 관련 업무를 하는 곳에 산포 되어 있을 가능성이 크기 때문이다. 물론 시간과 예산이 충분하여 해당 되는 자료를 한 건물로 옮겨 관리하면 좋겠지만 사실상 불가능 하기 때문에 다른 방안을 찾는 노력을 해야 한다. 구조를 바꾸거나, 위치를 지정하여 기술보호구역을 한정적으로 만드는 방법이 가장 효과적이라 판단하여 1차적으로는 내외부를 명확히 구분 짓기 위해 본원을 시범사업으로 보안검색대를 설치하였다[그림 2]. 그리고 업무관련성을 기준으로 하여 기술보호구역을 더욱 명확하게 구분하였다.

< 보안검색대 구성 >

X-Ray 수하물 검색대 안면인식 리더기 스피드게이트

[그림 2] 보안검색대 구성 및 적용사례

2.4 정보통신(사이버보안 포함) 강화 방안

4차 산업혁명과 디지털 전환의 가속화로 인해 방위산업은 디지털 트윈, 빅데이터, 인공지능(AI) 등 첨단 기술을 적극 도입하고 있다. 이러한 기술의 융합은 무기체계의 효율성과 정밀도를 향상시키는 동시에, 사이버 위협의 공격 표면을 확장시켜 새로운 보안 취약점을 초래하고 있다. 최근 5년간 방위사업청 등 방위산업 관련 기관에 대한 해킹 시도가 약 30,000여 건 이상 달했으며, 이 중 일부는 기술정보 유출로 이어졌고, 이러한 공격은 지능형 지속 위협 형태로 이루어지며, 내부자에 의한 정보유출도 빈번하게 발생되고 있다.[5] 뿐만 특히 국가 안보와 직결되는 방위산업기술의 유출은 군사력 약화뿐만 아니라 국제적 신뢰도 저하로 이어질 수 있기 때문에 이에 대한 체계적인 보호와 대응이 시급한 과제로 부상하고 있다. 해당 기관에서는 내・외부 보안위협 차단을 위한 조치로 정보통신 보안 강화(사이버보안 포함)와 관리방안을 지속적으로 시행・운영 하였다.

먼저 위협요인 및 취약점 분석을 통해 보호가 필요한 영역을 식별하고 위험을 분석하여 대책을 수립, 시스템 구축, 점검 및 개선하는 단계별 접근법을 수립하였다. [그림3]

[그림 3] 정보통신보안 보호 계획

최근 스마트폰 이용 보안사고 증가에 따른 비밀자료의 보호대책 강화가 필요하고 내부 기술유출의 대부분은 사용자 미인지 상태에서 해킹 또는 악성코드 감염에 의한 군사자료 유출(군사비밀 촬용, 회의 내용 녹음 등) 가능성이 크다고 판단하였기 때문에 정보통신장비의 일부 기능을 통제하기 위한 모바일 통제 시스템(MDM, Mobile device management)을 도입하였다 [그림 4].

[그림 4] 모바일 통제 시스템

또한 비밀정보관리시스템 및 방화벽 접근통제 권한 검증, 차단·로그생성 기능정상 작동 등 사이버보안시스템 실행상태를 주기적으로 점검하여 최상의 보안상태를 유지토록 관리·운영하였다. 이러한 전산 모니터링 점검 뿐 아니라 출력자료 통합 관리 시스템을 구축하여 근무시간 외 출력이나 갑작스런 기술자료 출력량 등가 등 특이점 발생에 대한 모니터링을 강화하기 위한 방안을 마련하기 위해 노력하였다 [그림 5].

[그림 5] 모바일 통제 시스템

이러한 물리적 보안강화 외에 내부 보안취약점을 점검하여 기술보호 유출을 막고 개선점을 찾기 위한 활동을 지속하였다 [표 2].

구분	점검내용
문서 출력	1) 네트워크 연결된 국방망 PC로 비밀 출력 여부 2) 승인된 자료 외 워터마크 해제 출력 여부
문서암호화 해제	1) 문서 암호화(DRM) 해제 시 승인절차 준수 여부
저장매체 사용	1) 비인가 저장매체 연결 여부 2) 국방망용 저장매체 오인삽입 여부
자료 반출	1) 상용메일(Naver, Daum, Gmail 등)로 메일 발송 여부 2) 인터넷 대용량(10MB) 메일 발송 여부
망혼용	1) 업무PC 망혼용 여부 점검

[표 2] 내부 보안취약점 점검 방안

3. 결론

방위산업기술보호 지침은 국가 방위력 강화를 위해 보호가 필요한 기술(핵심기술·보호기술)을 체계적으로 관리·보호하는 것을 목표로 한다. 이를 위해 기술 등급 분류, 접근통제, 암호화 저장, 보안점검, 외부 반출 및 이전 통제 절차를 마련하고 있다.

방위산업기술보호지침을 적용받는 대상기관인 기품원은 관리대상기술을 보호하기 위해 인원통제, 시설보호, 정보통신 보호 등 기술보호체계 구축을 이루었다. 하지만 아직까지 기술식별관리에 있어 핵심기술과 일반기술의 특성에 따른 보호방안을 현실적으로 수행하기 어렵기 때문에 이를 해결하기 위해 추가적 노력이 필요한 것도 사실이다.

[그림 6] 보안 성숙도 향상 로드맵

또한 증가하는 K-방산 수출의 활성화를 위해서는 향후 무기체계를 개발하는 방산업체들은 미국의 "국방 산업기반 사이버보안 기준(CMMC, Cybersecurity Maturity Model Certification)"과 같은 보안 인증이 필수적이기 때문에 도입, 운영, 그리고 평가하는 방법도 추가적으로 연구해야 할 사항이다

[6]. 뿐만아니라 관련 기관과 정부는 NATO의 "Protected Defense Information Sharing" 사례처럼 위협정보를 공유하는 유기적 체계를 구축해야 하고 신속 대응 체계 의 고도화를 통해 기술유출 사고 발생 시 핵심보호기술 등을 효과적으로 보호할 수 있는 방안을 도출된 로드맵을 고려하여 구축 ·운영 되어야 할 것으로 판단된다.

참고문헌

[1] 방위산업기술보호에 관한 법률, 법률 제13632호, 2016. 6. 30. 시행
[2] 방위사업청, 2022-2026 방위산업기술보호 종합계획, 2021. 12.
[3] 방위사업청, 훈령 867호 방위산업기술보호지침, 2024. 9.10.
[4] 방위사업청, 방위산업기술 지정 고시, 2023. 6.15.
[5] 류지선, 박정호. "방위산업 디지털 전환에 따른 보안위협 분석 및 대응방안." 한국산학기술학회논문지 (2023): 682-689.
[6] 이승배, "사이버보안 강화 측면의 미국 국방 기술 및 사업 보호 정책 변화.", 국방정책 (2021).