https://doi.org/10.33778/kcsa.2019.19.4.003

체계적인 방위산업기술보호를 위한 보호체계 우선순위 분석 연구

박 흥 순*, 김 세 용**, 김 용 환**

요 약

방위산업기술의 유출은 해당 기업의 영업 손실뿐만 아니라 국가안보 및 국익 차원에서도 심각한 피해를 야기할 수 있다. 최근 정부는 방위산업기술의 중요성을 인식하여 방위산업기술보호법을 제정하였고, 그에 따른 방위산업기술 보호지침을 마련하였다. 법규에 따르면 방위산업기술을 보유한 기관 및 업체는 방위산업기술 보호체계를 구축해야 하며, 정부는 이들의 기술보호 수준 향상을 위해 다양한 기술보호 정책을 수립하고 추진해야 한다. 본 연구에서는 기존의 기술보호지침에 대한 비교를 통해 시사점을 도출하고 방위산업기술 보호지침의 자가진단 항목을 대상으로 AHP 기법을 통해 보호체계 세부항목에 대한 우선순위 분석을 하였다. 이를 통해 대상기관에 대한 보호수준의 효율적 진단과 보호체계의 체계적인 구축을 위한 정책 지원이 가능할 것으로 기대된다.

Analysis of Security System Priority for the Systematic Defense Technology Security

Heungsoon Park*, Seyong Kim**, Yonghwan Kim**

ABSTRACT

The outflow of defense technology can cause serious damage not only in terms of business losses, but also in terms of national security and national interests. Recently, the government has enacted the Defense Technology Security Act, recognizing the importance of technology in the defense industry, and prepared guidelines for the defense technology security accordingly. According to the law, institutions and companies with defense technologies should establish a defense technology protection system, and the government should implement various technology protection policies to improve their level of technology protection. In this study, the implications were derived by comparing existing technology protection guidelines and priority analysis was performed on the protection system details through AHP for self-diagnosis items in the defense technology security guidelines. As a result, it is expected that it will enable efficient diagnosis of the level of protection and policy support for the systematic establishment of the protection system for the target institutions.

Keywords : 방산기술, 방산보안, 방산기술보호, 방산기술보호법, 방산기술보호지침, 사이버보안, Defense technology security

접수일(2019년 10월 1일), 게재확정일(2019년 10월 28일)

* 국방부 정보화기획관실 소프트웨어융합정책과(책임저자)
** 국방부 정보화기획관실 소프트웨어융합정책과

1. 서 론

방위산업기술(Defense Technology)은 국가안보적 측면뿐만 아니라 전략적 경제자원으로 인식되고 있어 국가 및 기업간 방위산업기술에 대한 중요성은 증대되고 있다. 4차 산업혁명 시대에 세계 각국은 방위산업에 대한 기술적 우위 확보 및 유지를 위해 치열하게 경쟁하고 있으며, 첨단 방위산업기술이 해외로 유출될 경우 국가 안전보장 및 국가경제 발전에 중대한 악영향을 끼칠 우려가 있어 유출방지대책을 강화하고 있다. 국내 방위산업의 경쟁력을 강화하고 국가안전보장 및 지속적인 방위산업 발전을 위해서는 국가차원의 체계적인 기술보호가 필요하다. 최근 정부는 그 중요성을 인식하여 2016년에 방위산업기술보호법(이하 방산기술보호법)을 시행하였고, 방위산업 관련 기업들로 하여금 기술보호체계를 구축·운영하도록 적극 유도하고 지원하는 정책을 추진하고 있다.

위와 같은 정책 추진에는 방위산업기술을 보유하고 있는 대상기관에 대한 기술보호 수준진단이 필수적이다. 이를 위해 방위사업청은 2019년 2월에 방위산업기술보호지침(이하 방산기술보호지침)을 마련하여 대상기관으로 하여금 자가진단을 통해 예방적 차원에서 보호수준을 진단하고 미흡부분을 개선토록 하고 있다. 하지만 방위산업기술을 보유하고 있는 대상기관의 규모나 역량에 따라서 보호체계를 구축하는데 한계가 있어, 우선순위를 정해 단계적으로 추진하는 전략이 필요하다.

따라서 본 연구는 방산기술보호지침의 자가진단 세부 평가항목에 대한 우선순위 분석을 통해 체계적인 방위산업기술 보호체계 구축 정책을 추진할 수 있도록 지원하고자 한다.

2. 관련 연구

2.1 기술보호관련 기존 연구

세계 각국은 다른 국가나 기업의 첨단 산업기술을 획득하기 위해 각종 보안시스템을 뚫고 유출하려는 시도를 해마다 증가시키고 있으며 이로 인해 예상되는 피해는 단순한 기업차원을 넘어 국가차원까지 그 경제적 파장이 급증되고 있다. 그렇다보니 기술선진국들은 기술혁신 경쟁이 가속화됨에 따라 기술보호를 위한 각종 정책을 추진하고 있으며 우리나라도 반도체 등 첨단산업 관련 기술 수준이 높아짐에 따라 다양한 기술보호 제도를 시행하고 있다[1]. 과거의 부정경쟁방지 및 영업비밀보호에 관한 법률(이하 부정경쟁방지법)은 민간기업의 영업비밀 누설에 초점을 두고 기술유출을 관리하였으나, 근래에는 정부에서 기술경쟁력을 강화하고 국가경제 발전에 이바지하기 위해 보호해야할 산업기술을 지정하여 관리토록 하고 있다. 산업기술의 유출방지 및 보호에 관한 법률(이하 산업기술보호법), 중소기업기술 보호 지원에 관한 법률(이하 중소기업기술보호법) 등과 같은 제도 정비로 다양한 기업의 기술유출 방지체계 구축에 대한 노력을 강화하고 있으며, 이에 따라 산업기술보호나 중소기업기술보호 분야에서는 기술 보유 대상 업체의 역량 수준을 높이기 위한 다양한 연구가 진행되었다. 채정우 등[2]은 산업보안 관리요소에 대한 상대적 중요도와 우선순위를 결정하는 등 계량적인 평가틀을 마련했으며, 장항배[3]는 중소기업기술 유출 방지를 위한 정보보호 관리체계를 설계했고, 홍준석 등[4]은 통계분석방법을 통해 중소기업기술보호에 대한 다양한 요인을 분석하여 제시하였다. 배제민 등[5]은 정보보호, 산업보안, 연구보안 등 각 분야별 보안관리체계의 통제항목을 분석하여 산업의 특성을 고려한 산업 중심의 보안수준 평가모형을 설계하였다.

2.2 방위산업기술의 특징

일반적인 산업기술이라 함은 산업 활동에 필요한 기술 가운데 국가가 법률로 정한 것이라고 할 수 있다. 산업기술보호법에서는 국가핵심기술을 포함하고 산업발전법 등 다양한 법률에서 지정된 기술을 산업기술(Industry Technology)로 정의한다. 여기서의 국가핵심기술은 기술적, 경제적 가치가 높아 해외로 유출될 경우 국가안전보장 및 국민경제발전에 중대한 악영향을 줄 우려가 있는 기술이다. 중소기업기술보호법에서의 중소기업기술은 중소기업자가 생산에 필요한 경제적 가치를 가지는 기술로써 기술의 주체가 중소기업자라는 것 외에는 산업기술과 큰 차별점이 보이지 않는다.

방산기술보호법은 방위산업기술을 체계적으로 보호하고 관련 기관을 지원함으로써 국가 안전 보장과 국제조약 등의 의무를 이행하여 국가신뢰도를 제고하는 것을 목적으로 하고 있다. 법률에서 보호대상으로 정의하고 있는 방위산업기술은 방위산업과 관련한 국방과학기술 중에서 국가안보 등을 위하여 보호되어야 하는 기술로서 방위사업청장이 지정하고 고시한다. 여기서의 국방과학기술은 국방에 필요한 무기체계와 자동화체계에 관한 기술적 조사, 연구, 개발 및 시험 등을 하는 엔지니어링 기술로 정의되어 있는데[6], 각 기술 간의 관계를 보면 (그림 1)과 같다. 방위산업기술은 일반적인 산업기술과는 다른 몇 가지 특징을 가지고 있다. 첫째, 방위산업기술은 다양한 첨단기술의 결합으로 이루어진다. 역사적으로도 최신의 기술들은 무기체계의 발달과 함께 진보되어 왔으며, 전장에서의 승리와 결부되어 왔다. 둘째, 연구개발 초기단계부터 보안대책 적용이 필수적이다. 무기체계는 일반적인 제품 개발보다 오랜 시간이 걸리며 방위산업기술의 적대국가로의 유출이 국가안보와 직결되기 때문이다. 셋째, 고부가가치 기술로써 국가 경제에 기여한다. 무기체계의 수출은 타 산업으로의 파급효과도 크고 고용창출에도 기여한다.

(그림 1) 방위산업기술의 범주

2.3 방산보안 환경 분석

방산기술보호법 시행 이전 초기의 방산보안은 군에 필요한 방산물자를 생산하고 공급하는 방산업체가 보유한 군사기밀을 보호하고, 적시에 물자가 공급될 수 있도록 지원하는 것이 주된 활동이었다. 이는 군사기밀보호법에 근거한 방위산업보안업무훈령(이하 방산보안업무훈령)으로 발전되어 현재까지 이르고 있다. 방위사업법에서도 방산물자를 생산하기 위한 방산업체 지정요건에 보안요건을 갖추도록 규정하고 있다. 방위사업법 시행령 제44조와 그 위임규정인 방위산업물자 및 방위산업체 지정 규정 제19조에는 방산업체 보안요건에 대한 세부항목을 명시하고 있는데, 군사기밀보호 위주의 방산보안업무훈령과 궤를 같이하고 있다.

과거의 방위산업은 무기체계의 전력화시기를 고려하여 주로 해외 직구매를 우선시 하였으나, 최근에는 자체 연구개발에 의한 국내 방위산업기술을 확보하고자 노력하고 있다. 국방과학기술 수준이 높아지고 최첨단 기술을 유출하기 위한 시도가 증가하자 방위사업청에서는 방산기술보호법을 제정하여 보호해야하는 국방과학기술을 방위산업기술로 지정하고 보호체계 구축을 지원하고 있다. 방산기술보호법 시행으로 기존의 방산보안은 군사기밀보호 위주의 보안정책에서 방위산업기술 유출 방지를 위한 보안정책도 포함하며, 대상기관도 정부에서 지정된 방산업체 외에 방위산업기술을 다루는 일반업체・연구소 등 관련기관으로 보안정책의 확장이 필요한 실정이다[7].

방위산업기술 유출 실태를 살펴보면, 외부 침입에 의한 유출보다는 전・현직 종사자에 의한 내부 기술유출이 약 80%로 대다수를 차지하며, 최근에는 해킹에 의한 기술유출이 의심되는 악성코드 유포 등 사이버위협이 방위산업 관련 업체 대상으로 증가하고 있어[8], 사이버 위협관련 정보공유에 대한 필요성도 커지고 있다[9]. 방위산업 관련 업체 구성은 무기체계를 통합하는 체계종합업체와 구성품을 생산하는 다수의 협력업체로 이루어져 있는데, 업체의 약 70% 정도를 중소기업이 차지하고 있어 상대적으로 기술보호 역량이 부족한 실정이다. (그림 2)는 중소벤처기업부에서 실시한 중소기업과 대기업간 기술보호 역량수준을 평가한 결과로써 대기업에 비해 약 70% 정도 수준을 유지한다[10].

2.4 기술보호지침별 보호수준 평가

앞서 언급했듯이 국내 기술보호 관련 법규는 부정경쟁방지법, 산업기술보호법, 중소기업기술보호법, 그리고 2016년에 시행된 방산기술보호법 등이 있다. 각

(그림 2) 기업규모에 따른 기술보호 역량수준

각의 법규에서는 기술보호활동을 적극 지원하고 있는데, 특히 산업통상자원부, 중소벤처기업부, 방위사업청에서는 기술보호지침을 통해 관련기관으로 하여금 기술보호체계를 갖추도록 하고 있으며, 기술보호 역량을 강화하기 위해 대상기관별로 보호수준을 객관적인 지표로 판단하도록 자가진단표를 마련하고 있다[11,12,13]. 일단 기술이 유출되면 복구가 쉽지 않은 만큼, 각 기관은 자신이 보유하고 있는 기술의 보호수준 진단을 통해 취약점을 보완하여 기술 유출을 사전에 예방하는 것이 상당히 중요하다.

각 기술보호지침 및 자가진단 항목을 살펴보면 <표 1>과 같다. 산업기술보호지침의 자가진단은 운영, 자산, IT, 외부, 사고 대응 등 총 5개 영역으로 구성되어 있으며, 대상기관의 장이 매년 1회 이상을 실시하도록 되어있다. 각 문항별 우수(10), 양호(8), 보통(6), 미흡(4), 위험(2)으로 구분하여 점수를 부여하게 되어있으며, 자가진단표(총 400점)와 세부적 자가진단 리스트(총 1000점)를 통해 보호수준을 평가한다[11].

중소기업기술보호에서의 자가진단은 기술보호정책, 주요 자산관리, 영업비밀 관리, 인적자원 관리, 기업 시설관리, 정보시스템 관리 등 6개 영역으로 되어있으며, 각 분야의 문항별로 점수를 부여하여 결과를 합산한다. 부여점수는 진단결과에 따라 0점·1점·2점을 차등하여 부여하며, 총 50문항으로 100점 만점으로 구성된다. 진단결과 총점을 5개 점수 구간별로 나누어 기술보호 수준을 평가하며, 70점 이상(우수・양호)의 점수를 취득하고, 각 분야별 득점이 50% 이상이 되도록 권고하고 있다[12].

방산기술보호지침 내의 자가진단 평가영역은 방

<표 1> 기술보호지침 및 자가진단 항목 비교

구 분	산업기술보호	중소기업 기술보호	방위산업 기술보호
소관 부처	산업통상자원부	중소벤처기업부	방위사업청
자가 진단 평가 영역	운영, 자산, IT, 외부, 사고 대응 등 5개 영역	기술보호 정책, 주요 자산관리, 영업비밀 관리, 인적자원 관리, 기업 시설관리, 정보시스템 관리 등 6개 영역	기술관리, 인력관리, 시설보호, 정보보호, 연구개발시, 수출 및 국내이전시 등 6개 영역
구성	- 자가진단표 (40개 항목) - 세부적 자가 진단리스트 (100개 항목)	50개 항목	27개 항목 (123개 요소)
실시 주기	대상기관이 1년에 한번	명시되지 않음	대상기관이 1년에 한번
특징	- 자가진단표와 세부적 자가진단 리스트로 구성 - 문항별 10점 만점으로 점수화	- 진단결과를 5개 구간으로 나누어 평가 - 각 분야별 총점의 50% 이상의 수준을 유지하도록 권고	- 핵심요소를 두어 기본적으로 갖추어야할 보호수준을 제시

산기술보호법에서 규정하는 방위산업기술 보호체계 구축항목과 유사하다. 평가영역은 방위산업기술의 관리(기술관리), 방위산업기술 취급 인력관리(인력관리), 기술보호구역 인원통제 및 시설보호(시설보호), 방위산업기술 정보보호(정보보호), 연구개발시 방위산업기술보호, 방위산업기술의 수출 및 국내이전시 보호 등 6개 영역으로 구성되어있다. 다른 기술보호지침의 자가진단과 차별되는 점은 점검 항목을 평가함에 있어서 점수를 부여하기보다는 하위 세부 평가 요소를 제시하여 목표를 달성토록 하고 있으며, 특히 핵심요소를 통해 기본적으로 갖추어야 할 보호수준을 제시하고 있다[13].

3. 보호체계 우선순위 분석방법

3.1 AHP 개요

AHP(Analytic Hierarchy Process)는 1970년대

초에 Thomas L. Saaty가 고안한 기법으로 평가기준이 다수인 문제 상황에서 여러 가지 대안들의 상대적인 중요도를 체계적으로 점수화하는 다기준 의사결정(multi-criteria decision making)기법이다[14]. AHP기법은 몇 가지 단계로 구성되어 있는데, 의사결정 문제를 상호 관련된 의사결정 요인들의 계층으로 분류하는 계층구조화 단계, 각 요인들을 단순 비교하기 위해 전문가 설문을 통한 쌍대비교를 하고, 이를 토대로 가중치를 산출하는 단계, 일관성을 검증하는 단계 등으로 이루어진다.

3.2 보호체계에 대한 가중치 분석 설계

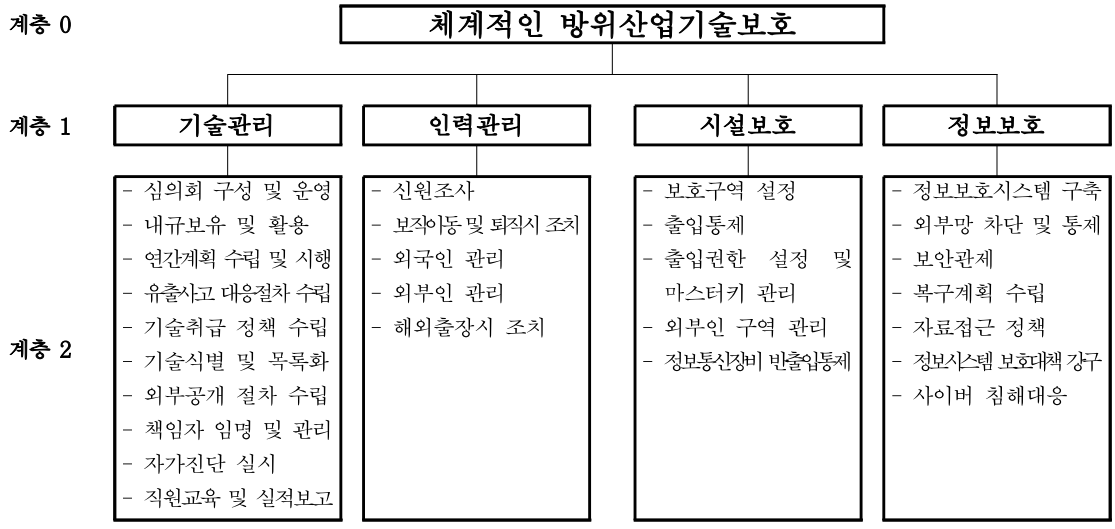
방산기술보호지침에서의 자가진단 항목은 방산기술보호법 13조(보호체계 구축・운영)과 8조(연구개발사업 시 보호), 9조(수출 및 국내이전 시 보호)를 구체화하여 반영하고 있다. 여기서 연구개발시 기술보호와 수출 및 국내이전시 기술보호 평가항목은 보호체계 구축・운영관련 자가진단 항목을 중복하여 평가하고 있고, 본 논문의 목적도 방위산업기술보호를 위한 보호체계를 체계적으로 구축하기 위한 우선순위 분석이므로 기술관리, 인력관리, 시설보호, 정보보호 등 4개 분야만을 분석 대상으로 선정하였다.

방위산업기술을 체계적이고 효율적으로 보호하기 위한 보호체계 구축마련을 목표로 영역 및 구성요소에 대한 계층 구조화를 실시하면 (그림 3)과 같다. 해당 항목은 자가진단의 세부항목 순서와 동일하다. 설문조사는 방산기술보호를 의사결정을 위한 평가기준이 다수이고 상호 독립적인 대안들을 체계적으로 평가할 수 있는 방법으로, 리커트 9점 평가척도를 사용하여 설문 문항을 구성하였다. 설문대상은 <표 2>와 같이 방산보안 전문가와 기술취급 전문직 49명을 대상으로 실시하였으며, 응답자의 판단 오차를 최소화하여 신뢰성을 높이기 위해 직접 방문하여 설문방법 및 절차에 대한 설명을 하고 설문을 진행하였고, Expert Choice 프로그램을 활용하였다. AHP 분석결과 전문가 49명의 답변 중 일관성(CI, CR)값이 유효하지 않은 4명을 제외한 45명의 평가결과를 활용하여 보간법을 적용하여 가중치를 산출하였다.

4. 연구결과

4.1 분야별 기술보호체계 평가영역 분석

방위산업기술보호를 위한 보호체계 우선순위(중요도) 분석 전에 보호체계 평가영역에 대한 기존 기술보호지침과의 관계성을 분석해보았다. 방위산업기술보호를 위한 보호체계 평가항목을 살펴보면 기존의 산



(그림 3) 방위산업기술 보호체계 우선순위 분석을 위한 계층화

<표 2> 설문 대상자의 인구 사회적 현황

구 분		인원(수)	백분율(%)
연령	계	49	100
	30대	29	59.2
	40대	15	30.6
	50대 이상	5	10.2
직업	계	49	100
	공공기관 보안실무자	13	26.5
	방산업체 보안담당	12	24.5
	방산기술 취급 연구원	12	24.5
	타 기술협회 실무자	12	24.5
직위	계	49	100
	팀장이하	39	79.6
	부서장급	8	16.3
	경영진 급이상	2	4.1
경력	계	49	100
	10년이하	27	55.1
	11 ~ 20년	21	42.9
	21 ~ 30년	1	2

업기술보호지침과 중소기업기술보호지침의 것과 유사하다. 방산보안과 방위산업기술보호가 선행연구의 방위산업기술범주나 방산보안의 역사를 살펴보았을 때 일반적인 기술보호나 산업보안정책과 따로 떨어져서 생각할 수 없기 때문이다. <표 3>은 방위산업기술보호지침 구조 관점(정책일반, 인원보안, 시설보안, IT보안)에서 세 분야의 기술보호지침 내 자가진단 평가영역 구조를 보여준다.

산업기술보호지침의 자가진단 평가항목은 세부 자가진단리스트를 기준으로 운영(지침, 조직), 자산(비밀, 인력, 시설), IT, 사고대응, 외부(계약, 해외진출) 등의 평가 분야로 나눠진다. 각 분야별 문항구성 비율을 살펴보면 보호체계 구축과 직접적으로 연관되지 않은 평가항목(외부)을 제외하면 운영 12.4%, 비밀·자재 16.8%, 인력 14.6%, 시설 16.8%, IT 25.8%, 사고대응 13.5%이다. 중소기업기술보호지침은 기술보호정책 20%, 자산관리 10%, 영업비밀 14%, 인력 22%, 시설 14%, 정보시스템 20%로 평가영역 구성을 보여주며, 방산기술보호지침은 연구개발과 수출·국내이전 관련 항목을 제외하면 기술관리 37%, 인력 18.5%, 시설 18.5%, 정보보호 26%이다.

공통적으로 기술보호 관련 정책일반 분야와 IT보안 분야가 다른 두 영역(인원·시설보안) 보다 평가 항목 비중이 많았으며, 산업기술보호지침의 경우 IT자산 관리와 침해사고 대응 등 IT보안 항목이 다른 두 지침보다 상대적으로 비중이 높았다. 중소기업기술보호지침은 상대적으로 IT보안 보다는 정책일반과 인원보안이 다른 기술보호지침보다 비중이 높다. 중소기업의 기술보호 역량 수준이 대기업에 비해 낮기 때문에

<표 3> 분야별 기술보호지침 평가항목 점유비 비교

구분	산업기술보호지침				중소기업기술보호지침			방위산업기술보호지침		
	평가영역		항목수	점유비(%)	평가영역	항목수	점유비(%)	평가영역	항목수	점유비(%)
정책일반	운영		11	12.4	기술보호정책	10	20	기술관리	10	37
	자산	비밀·자재	15	16.8	자산관리	5	10			
					영업비밀	7	14			
인원보안		인력	13	14.6	인적자원	11	22	인력관리	5	18.5
시설보안		시설	15	16.8	기업시설	7	14	시설보호	5	18.5
IT보안	IT		23	25.8	정보시스템	10	20	정보보호	7	26
	사고대응		12	13.5						
기타	외부		11	제외				연구개발	1	제외
								수출·국내이전	2	

보호정책과 내부자에 의한 유출(이직 등)을 보완하기 위한 구성이라고 판단된다. 방위산업기술보호지침은 방위산업기술이 타 분야의 기술 중요도 대비 국가안보 측면이 부각되어 기술관리 구성이 높으며, 최근의 사이버 보안 인식이 반영되어 IT보안 비중이 높다.

4.2 방위산업기술 보호체계 평가항목별 우선순위 분석 결과

방위산업기술 보호체계 수준진단을 위해 평가영역에 대한 중요도를 살펴보자. <표 4>는 AHP기법을 활용한 방위산업기술 보호수준 평가항목에 대한 가중치 산출결과이다. 평가영역 가중치에서 기술관리 영역과 정보보호 영역이 다른 영역에 비해 상대적으로 높음을 알 수 있다. 방위산업기술의 경우 국가안보 측면에서 타 기술보다 중요성이 크기 때문에 방위사업청에서 지정하여 관리하고, 대상기관으로 하여금 철저하게 관리 감독하도록 방산기술보호법에서 규정하고 있어 기술관리 영역에 대한 중요도가 상대적으로 높은 것으로 분석된다. 정보보호 영역은 방산물자 생산에 필요한 자료들이 전자문서로 활용되고 있으며, 최근 방위산업기술의 사이버 해킹을 통한 유출이 증대되고 있는 환경을 반영한 것으로 보인다. 설문 대상자 측면에서 분석해보면 방산보안실무 및 기술보호업무를 직접적으로 다루고 있는 보안실무자들은 정보보호 영역에 대한 중요도를 높게 평가하고 있었으며, 보호대상인 기술을 취급하는 연구원 등은 기술관리 영역에 대한 우선순위가 더 높았다. 인력관리와 시설보호는 평가항목 및 세부요소 등의 항목 수가 거의 동일하였으나 설문대상자의 직군과 상관없이 공통적으로 인력관리 영역의 중요도가 시설관리 보다 더 우선순위가 높았다. 시설보호는 전통적인 보안관리 영역으로써 최근의 정보통신망을 통한 유출이나 내부자 유출과 같은 보안사고보다 직접적인 사고 발생 사례가 적어 상대적으로 중요도가 낮게 인식된 것으로 판단된다.

평가영역별로 살펴보면, 기술관리 영역은 다른 분야의 기술보호지침과는 달리 방위산업기술의 추적 및 관리를 위해서 대상기관에서 방위산업기술을 식별하도록 하고, 보유하고 있는 기술 목록을 유지하도록 하고 있다. 기술관리 영역에서 우선순위가 높은 세부 항

<표 4> 방위산업기술 보호수준 세부 평가항목별 가중치 분석 결과

영 역 (가중치)	기술관리 (40)	인력관리 (14)	시설보호 (10)	정보보호 (36)
세부 평가 항목	심의회 구성 및 운영 (3.5)	신원조사 (5.1)	보호구역설정 (2.6)	정보보호시스템 구축 (9.0)
	내규보유 및 활용 (7.4)	보직이동 및 퇴직시 조치 (3.7)	출입통제 (2.2)	외부망 차단 및 통제 (8.6)
	연간계획 수립 및 시행 (1.6)	외국인 관리 (1.8)	출입권한 설정 및 마스터키 관리 (2.8)	보안관제 (4.7)
	유출사고 대응절차 수립 (3.5)	외부인 관리 (1.6)	외부인 구역 관리 (1.0)	복구계획 수립 (2.2)
	기술취급 정책 수립 (7.0)	해외출장시 조치 (1.8)	정보통신장비 반출입 통제 (1.4)	자료접근 정책 (4.6)
	기술 식별 및 목록화 (4.8)			정보시스템 보호대책 강구 (4.0)
	외부공개 절차 수립 (2.6)			사이버 침해대응 (2.9)
	책임자 임명 및 관리 (6.2)			
	자가진단 실시 (1.6)			
	직원교육 및 실적보고 (1.8)			

목은 대상기관의 내규 보유 및 활용 여부와 방위산업기술의 취급에 대한 정책 등으로 분석되었다. 이는 관련 법규가 최근에 시행되어 설문에 참여한 전문가들이 대상기관의 내규 수립에 대한 중요성을 높게 인식하고 있음을 알 수 있으며, 보호대상인 방위산업기술의 식별과 현황관리가 기본적으로 선행되어야 다른 영역의 보호체계 구축 정책이 제대로 수립될 수 있기 때문에 우선순위가 높은 것으로 판단된다.

인력관리 영역에서 우선순위가 높은 항목은 신원조사와 관련된 항목이다. 방산기술보호지침에서는 방위산업기술을 취급하거나 관리하는 전 인원에 대해 신원조사를 실시하도록 하고 있으며, 신원조사결과를 토대로 해당업무에 적격자를 보직시켜야 한다. 이는 방위산업기술이 타 분야의 기술보호정책보다도 국가안보 측면에서 부각되는 항목이라고 할 수 있다. 다음으로 중요도가 높은 항목은 보직이동이나 퇴직시 조치항목으로 기술경쟁 국가나 기업으로의 스카우트에 의한 유출의 심각성을 보여주는 사항으로 분석된다.

시설보호 영역은 27개 세부 평가항목의 가중치 평균점수 3.7을 기준으로 보았을 때 전 항목이 평균이하의 중요도를 보여준다. 이것은 방위산업기술을 취급하는 방산업체나 연구소 등이 일반적으로 이미 군사시설과 같은 통제구역으로 설정되어 있어 상대적으로 설문응답자들이 우선순위를 낮게 인식하는 것으로 분석된다. 시설보호에서 중요도가 높은 항목은 보호구역·출입권한 설정 및 마스터키 관리로써 기존의 전통적인 물리보안에서의 접근통제 정책과 유사하다.

정보보호 영역은 기술관리 영역보다 우선순위가 낮은 것으로 분석되나, 세부 평가항목의 평균값은 기술관리 평균값보다 높게 나타났다. 특히 정보보호시스템 구축에 있어서는 전 영역의 세부 항목 중 가장 높은 가중치가 나왔다. 이는 정보통신망을 통한 기술유출에 대한 언론보도가 영향을 미쳤다고 할 수 있지만, 기본적으로 방위사업청의 방위산업물자 및 방위산업체 지정 규정 제19조(보안요건 측정 등)에 방산업체 보안대책으로 구축해야 할 정보보호시스템이 명시되어 있다[15]. 해당 정보보호시스템에는 외부망과 방산업무망에 대한 망분리시스템과 24시간 보안관제시스템이 포함되어 있어 설문 대상자들에게 중요하게 인식되어 있을 것으로 판단된다. 사이버 침해대응과 복구계획 수립 측면에서는 사후관리적인 인식이 강해 상대적으로 중요성이 적은 것으로 나타났지만, 향후 위협정보 공유를 통한 사이버 위협 공동 대응체계 구축도 중요할 것으로 판단된다.

전체 세부항목을 기준으로 상위 5위를 살펴보면, 정보보호시스템 구축(9.0) > 외부망 차단 및 통제(8.6) > 내규보유 및 활용(7.6) > 기술취급 정책 수립(7.0) > 책임자 임명 및 관리(6.2) 순으로 가장 덜 중요하게 생각하는 외부인 구역 관리(1.0) 보다 약 6~9배 정도의 차이를 보이고 있다. 중요도가 상대적으로 높게 인식되는 항목들 위주로 먼저 보호대책을 마련함으로써 기본적인 기술보호수준을 확보하는 전략을 마련해야 할 것이다.

4.3 추가 연구

방산기술보호지침의 자가진단표에는 핵심요소 항목이 포함되어있다. 이는 보호수준을 평가함에 있어서 방위산업기술보호 목표를 충족하기 위한 세부 평가요소 중 기본적이고 필수적인 요소이다. 이는 다른 기술보호지침이 점수를 부여하여 해당 항목에 대한 수준을 평가하는 것과 달리 핵심요소와 일반요소로 나누어 기본적으로 달성해야할 요소와 확산시켜 나가야할 요소를 명확하게 구분해 놓은 것이다. 본 연구결과와 함께 핵심요소를 기반으로 방위산업기술보호 성숙도 모델을 확립한다면, 방산기술보호수준을 한층 더 체계적으로 관리할 수 있을 것으로 기대한다.

5. 결 론

본 연구는 방위산업기술보호를 위한 보호체계를 구축함에 있어, 체계적으로 보호수준을 향상하기 위해 우선순위를 결정하고 분석을 하였다. 이를 뒷받침하기 위해 방산기술보호지침의 자가진단 세부 평가항목에 대한 가중치를 전문가 집단 설문 및 AHP기법을 통해서 검증하였다.

우선순위를 분석한 결과 평가 영역에서는 방위산업기술의 취급 및 관리를 위한 기술관리 정책과 정보보호 시스템 구축 정책이 중요함을 보여주었으며, 인력관리나 시설보호 측면에서의 정책은 상대적으로 우선

순위가 낮았다. 따라서, 방산업체의 규모나 역량 측면에서 모든 기술보호 요소를 동시에 구축하기 제한될 경우 대상기관의 상황에 따라 우선순위가 높은 요소부터 순차적으로 구축하고 점차 확대해 나가는 정책이 필요하다.

방위산업의 특성상 폐쇄적 환경이고 상대적으로 해당 분야의 전문가 인재풀도 제한적이어서 본 연구의 분석결과에 대한 일반화에 한계가 있지만, 앞으로 방위산업기술보호 수준 향상을 위한 모델 정립에 기초자료로써 활용될 수 있기를 기대해 본다.

참고문헌

[1] Jong-ho Kim, “The emerging technology protectionism and competition conolidating scheme on the knowledge property,” Law Review, vol. 50, pp. 55-94, Jun. 2013.

[2] Jeong-Woo Chae, Jin-Hong Jeong, “Study on decision making for the industrial security management factor’s priority,” Journal of Society Engineering, vol. 10, no. 2, pp. 123-140, Apr. 2013.

[3] Hangbae Chang, “The design of information security management system for SMEs industry technique leakage prevention,” Journal of Korea Multimedia Society, vol. 13, no. 1, pp. 111-121, Jan. 2010.

[4] Junsuk Hong et al., “Small business technological assets protection factors analysis using logistic regression analysis,” The Journal of Society for e-Business Studies, vol. 20, no. 3, pp. 1-10, Aug. 2015.

[5] Je-Min Bae et al., “A study on design direction of industry-centric security level evaluation model through analysis of security management system,” The Journal of Society for e-Business Studies, vol. 20, no. 4, pp. 177-191, Nov. 2015.

[6] 국방기술품질원, '국방과학기술용어사전', 2017.

[7] H. Park, et. al., "Conceptualization of Defense Industrial Security in Relation to Protecting Defense Technologies," in Proc. Computational Science and Its Applications – ICCSA 2018, pp. 158-169, July 2018.

[8] Hyungjin Lee, “A study on the meaning of the enactment of defense technology security act and awareness improvement,” Korean Journal of Industrial Security, vol. 6, no. 2, pp. 57-80, Dec. 2016

[9] 박홍순, "방위산업 사이버 보안을 위한 방산 정보 공유·분석센터(ISAC) 설립 방안," 정보보호학회지, 제28권, 제6호, pp. 56-62, 2018.

[10] 중소기업청, 대중소기업협력재단, '2016 중소기업 기술보호 수준 실태조사', 2017.

[11] 산업통상자원부, '산업기술보호지침 및 매뉴얼', 산업통상자원부, 2017.

[12] 중소벤처기업부, '중소기업기술 보호 지침', 대·중소기업·농어업협력재단, 2018.

[13] 방위사업청, '방위산업기술 보호지침', 2019

[14] Thomas L. Saaty, Decision Making for Leaders: The Analytic Hierarchy Process for Decisions in a Complex World, 3rd ed., RWS Publications, Sep. 2012.

[15] 방위사업청, '방위산업물자 및 방위산업체 지정 규정', 2018.

〔저자소개〕

박 흥 순 (Heungsoon Park)
2002년 3월 육군사관학교 전산학 학사
2007년 3월 미국 Air Force Institute of Technology 컴퓨터공학 석사
2016년 1월 국방대학교 컴퓨터공학 박사
2016년 8월 국방보안연구소 선임연구원
2018년 12월~현재 국방부 정보화기획관실 국방소프트웨어정책담당
2019년 10월~현재 국방보안관리사 국가자격검정 자문위원
email : heungsoon.park@gmail.com

김 세 용 (Seyong Kim)
2001년 3월 육군사관학교 핵화학학사
2009년 1월 국방대학교 운영분석 석사
2014년 12월 국방부 국방통계 담당
2019년 현재 충남대학교 경상대학 생산관리/MIS 박사 中
2019년 2월~현재 국방부 정보화기획관실 국방빅데이터/인공지능정책담당
email : seyong58@naver.com

김 용 환 (Yonghwan Kim)
2004년 3월 공군사관학교 산업공학 학사
2015년 2월 서울대학교 경영학 석사
2017년 3월 연세대학교 국방융합공학 박사 재학중
2016년 12월~현재 국방부 정보화기획관실 국방M&S정책담당
email : skyair4s@gmail.com