Journal of the Korea Academia-Industrial cooperation Society
Vol. 20, No. 12 pp. 265-270, 2019

https://doi.org/10.5762/KAIS.2019.20.12.265
ISSN 1975-4701 / eISSN 2288-4688

국가 안보와 연계한 방위산업 보안 개념 정립

고희재[1], 이용준[2*]
[1]중앙대학교 융합보안학과, [2]국방보안연구소

Conceptualization of Defense Industrial Security in Relation to National Security

Hee-Jae Go[1], Yong-Joon Lee[2*]
[1]Department of Security Convergence, Chung-Ang University, [2]Defense Security Institute

요 약 한국의 방위산업기술은 세계적인 수준으로 발전하고 있으며, 방위산업 보안은 1945년 이후로 오랜 역사를 가지고 있다. 그러나, 지금까지 방위산업 보안이라는 용어의 개념을 설정하는 데는 관심이 부족했으며, 관련 법률에 의해 방위산업기술 보호에 대한 논의가 활성화 되었음에도 방위산업 보안의 개념 정립은 여전히 미흡한 실정이다. 정부는 방위산업기술 보호를 위해 2015년에 방위산업기술보호법을 제정하여 방위산업 보안에 대한 필요성을 강화하였다. 새로운 법이 제정됨으로써 방위산업 보안의 대상 및 보호 자산 다양화 등 패러다임이 변화됨에 따라 방위산업 보안 개념에 대한 연구가 필요해 졌다. 방위산업은 국가 안보 관점에서 보안 상의 이유로 정보 공개가 제한되어 학술적 연구가 많이 이루어지지 않았으나, 방위산업기술보호법 제정으로 보안 영역 확장 등 환경의 변화로 방위산업 보안 개념을 재정립 할 필요성이 증대되고 있다. 따라서, 본 연구에서는 기존 논문을 통해 다양한 방위산업에 대한 개념과 최근 변화된 방위산업 환경을 분석하여 국가 안보적 차원에서 방위산업 보안 개념을 정립하는데 그 목적이 있다. 연구 결과는 학문적 연구가 부족하고 폐쇄적인 방위산업 환경 속에서 상세 규격에 따른 방법론을 사용하여 방위산업 보안 개념을 학술적으로 정립한데 의의가 있다.

Abstract In order to protect the advancement of defense technology that has a tremendous e?ect on both the national security and the economy, the Republic of Korea established the Defense Technology Security Act in 2015. As the new enactment brought changes to the landscape of the defense industry and defense industrial security, a new examination of the concept of the defense industrial security has now become necessary. Even after taking into consideration the undisclosed nature of defense industrial security research, and the fact that only the limited number of firms participates in the subject matter, scientific studies related to the topic have not been active. However, with the new enactment of the Defense Technology Security Act, it is necessary to expand the scope of security and to redefine the concept of defense industrial security. In this paper, we analyzed the research works on related technology protection policies and our environment of the defense industry in order to conceptualize defense industrial security. The established concepts are expected to provide a systematic way to protect the confidential and defense technology.

Keywords : Defense Industrial Security, Defense Technology, Defense Industry, Defense Acquisition Program, National Security, National Interest

*Corresponding Author : Young-Joon Lee(DSI)
email: yjlee4279@gmail.com
Received October 22, 2019 Revised November 19, 2019
Accepted December 6, 2019 Published December 31, 2019

1. 서론

우리나라의 방위산업 수출은 2005년 2.62억불에서 점차 증가하여 2017년도에는 31.22억불을 달성하였으며, 주요 수출 품목도 탄약 부품 등 구성품에서 잠수함, 고등훈련기, 자주포 등과 같은 첨단 제품으로 다양화되는 등 이제는 세계적인 무기체계를 직접 개발할 수 있는 수준까지 발전하고 있다. 또한, 방산수출은 북미와 중동뿐만 아니라 남미, 아시아까지 확대되고 있으며, 방위산업 기술력은 미국의 80%, 세계 9위 수준으로 발전하는 한편, 방위산업 40주년이 되는 시점에서 항공기, 잠수함 등 고부가가치 기술제품을 수출함으로써 새로운 전기를 맞이하고 있다[1,2].

이 시점에서 방위산업기술보호법 제정은 방위산업 분야에 새로운 변화를 주었으며 관련 업계에서도 변화를 체감하고 있지만 다음과 같은 문제점이 있다. 현재의 방위산업 보안은 정부가 지정한 방산업체에 국한되어 있어 적용 범위가 제한되며 군사비밀 위주의 보호 정책에서 방위산업기술 보호 등 관련 정보로의 확장이 필요하다. 또한, 방위산업 보안과 방위산업기술 보호라는 두 개의 각기 다른 정책으로는 정부 지원이나 관련 연구에서 시너지 효과를 달성하기 어렵다.

최근 방위산업은 국가 안보와 국가 경제에 영향을 줄 만큼 고도로 기술이 성숙되어 방산업체 스스로 보안업무를 수행해야 한다[3]. 이런 관점에서 연구와 정책 수립 이전에 방위산업 보안에 대한 개념을 학술적으로 명확하게 정의 할 필요가 있다. 따라서, 본 연구의 목적은 기존의 논문을 분석하고 방위산업 환경에 입각하여 방위산업 보안의 개념을 정립하는데 있다.

2. 관련 연구

2.1 방위산업 보안의 역사

방위산업 보안은 자주국방의 역사와 맥락을 같이한다. 1945년 일제 해방 이후 미국의 군사원조에 의존해 오다가 1968년 김신조 청와대 습격사건, 1969년 닉슨독트린, 그리고 1970년대 초 미군 철수가 가시화 되면서 자주 국방의 필요성이 증대되었다. 한편, 방위산업 보안 업무는 1977년 국방부 훈령으로 군사비밀, 무기생산 시설 등을 보호하기 위해 방위산업보안업무시행규칙(現 방위산업보안업무훈령)이 제정되어 방위산업 보안 업무가 시작되었다[17].

2.2 방위사업과 연계한 방위산업

방위산업 보안에 대해서 알아보기 위해서는 용어에 대한 분석이 필요하다. 방위산업 보안은 방위산업과 보안의 합성어이며 방위산업은 협의적 관점과 광의적 관점으로 해석할 수 있다. 협의적인 관점에서는 방위사업법상 용어로 '정부가 지정한 방산물자 생산과 연구개발 관련 산업'이라고 정의 할 수 있으며[10], 광의적인 관점에서는 국가 방위를 위한 군사적으로 요구되는 물자의 생산과 개발에 기여하는 모든 산업으로 확대 해석할 수 있다[15]. 보안 연구는 대상이 되고 있는 방위산업에 대한 명확한 개념을 가져야 하지만 최근의 연구에서는 방위산업에 대한 정의가 명확하지 않다[6-8]. Woo. K[4, 5]만이 협의적인 관점에서 방위산업을 적용했다.

방위산업 선진국인 미국의 경우에는, 이 용어를 군의 시스템을 제공하는 주요 계약 업체, 하청 업체 및 부품 공급 업체로 정의했다[20]. 유럽에서 방위산업이라는 용어는 군수품의 연구, 개발, 생산, 분석, 유지 보수 등에 참여하는 모든 기업과 기관을 의미한다. 위에서 보는 바와 같이, 방위산업 선진국들은 방위산업이란 용어를 협의적 관점이 아닌 광의적 관점으로 사용하고 있다[9].

방위산업은 방위사업과 연계하여 그 개념을 알아 볼 수도 있다. Fig. 1과 같이 무기체계를 획득하는 주체는 방위사업청이고 무기체계를 개발하고 제조하는 당사자는 방산업체 즉, 기업들이다. 결국, 방위산업의 개념은 방위사업의 파생물이며, 방위산업관련 기업에는 방산업체, 일반기업, 군수품 공급 업체 등과 같은 다양한 대상이 있다[10].

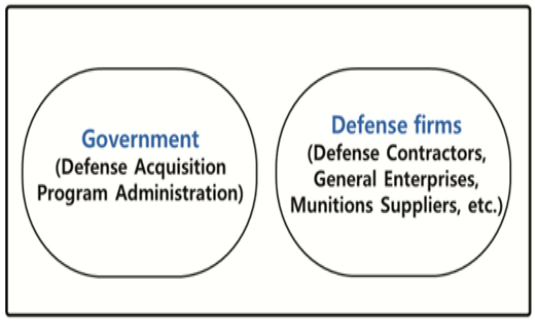

Fig. 1. Main body in the defense industry

2.3 보안의 개념

'보안'이라는 용어는 일반적으로 일상적인 언어로 사용되지만 명확하게 개념화하기 쉽지 않은 단어이다. 이것은 '국가 보안'과 같은 가장 높은 수준에서 '출입 보안'과

같은 낮은 수준까지 다양하고 광범위한 분야에서 사용된다. '보안'에 대한 의미를 살펴보면 미국 역사 사전과 웹스터 대학 사전은 '위험이나 위험으로 부터의 자유'라고 정의하고 있으며, 콜린스 영어 사전은 '안전한 상태'를, 국립 한국어 학당의 한글 사전에는 '안정성을 유지하며 평화와 사회 질서를 유지한다'라고 정의되어 있다.

'안보'라는 용어는 우리나라 역사에서 정치 권력을 유지하기 위해 정치 조직과 함께 했던 것처럼 부정적인 의미를 지니고 있다. 그러나 최근에는 산업보안, 사이버 보안, 정보보안 등을 포함하여 개인 정보와 자신을 보호하기 위해 '보안'이라는 용어가 널리 사용되고 있다.

위에서 보는 바와 같이 '보안'이라는 용어는 다르게 정의 되었으며, 보안의 정의 또는 개념에 관한 연구가 실시되었다. DavidA.Baldwin[13]은 보안의 개념화에 대한 다양한 접근 방식을 제시하고 LuciaZender[14]는 좋은 공공 서비스 또는 긍정적인 존재로써 의미를 비교 분석한다. 본 논문에서는 정책의 합리성에 대한 방위산업 보안을 분석하였다[13].

2.4 방위산업기술의 특성과 보호

매년 전 세계의 국가들은 다른 나라의 기업들로부터 첨단 기술을 습득하기 위해 보안 시스템에 침입하려고 노력하고 있다. 결과적으로 일어날 수 있는 경제적 피해는 기업뿐만 아니라, 국가적 차원으로도 확산되고 있다. 이에 따라 기술 선진국들은 기술혁신 경쟁이 가속화됨에 따라 자국의 기술을 보호하기 위한 다양한 보안 정책을 추진하고 있다.

우리나라의 방위산업기술은 세계 9위 수준으로 2015년 방위산업기술보호법을 제정해 141개의 방위산업기술을 지정·고시하여 보호하고 있다. 방위산업기술은 Fig. 2와 같이 방위산업과 관련된 '국방과학기술' 가운데 국가안보를 위해 보호되어야 할 기술이다[16]. 방위산업기술은 방위사업청에 의해 지정·고시된다.

방위산업기술은 일반적인 산업 기술과는 다른 특성을 가지고 있다. 첫째, 국방과학기술은 다양한 첨단 기술의 결합체이다. 역사상 최신 기술들은 전쟁이 일어났을 때 무기 개발에 적용되었고, 그것은 전쟁에서 승리로 이어질 수 있다. 둘째, 연구개발 초기부터 보안 조치를 취하는 것이 필요하다. 셋째, 고부가 가치의 기술로써 국가 경제에 기여할 뿐만 아니라 일자리 창출에도 기여하고 있다. 이러한 방위산업기술의 중요성을 인식하여 정부는 2015년 12월에 방위산업기술보호법을 제정하여 2016년 6월부터 시행하고 있다.

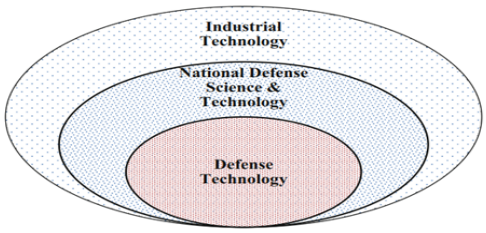

Fig. 2. Relationship between the defense technology and other technologies

방위산업기술보호법은 방위산업기술을 보유한 대상기관에 대해서는 기술의 식별 및 관리, 인원통제, 시설보호, 정보보호 등으로 구성된 '보호체계'를 구축하도록 통제하고 있다[16]. Table 1과 같이 기존의 방위산업 보안 정책과 비교해 보면 방위산업기술보호법은 방위산업기술 관리의 추가 기능과 강화된 정보보안 시스템을 특징으로 한다[17]. 정보보안 시스템은 사이버 위협을 예방하고 대응하기 위해 다양한 보안 솔루션을 포함하고 있다[11].

Table 1. Comparison between the defense technology protection and existing defense industrial security

Spec.	Defense technology protection	Conventional defense industrial security
Law	Defense Technology Security Act	Defense Acquisition Program Act, Military Secret Protection Act
Target party	All organizations handling defense technology	Designated defense contractors
Assets to protect	Defense technologies designated by government	Military secrets (mainly)
Policy department	Defense Acquisition Program Administration	Defense Intelligence Agency

3. 방위산업 보안의 개념화

이 장에서는 이전의 관련 연구에 기초하여 방위산업 보안에 대한 체계적 개념을 확립할 것을 제안한다. 방위산업 보안을 학술적으로 유용하게 만들기 위해 몇 가지 규격을 만들어 분석 틀을 설계하고 다음으로, 현재의 방위산업 보안에 대한 환경을 진단하고 미래의 정책 수립을 위한 보안 목적을 제시한다.

3.1 분석 구성 요소

Wolfers에 따르면, “보안이라는 용어는 상세 규격없이 사용되는 경우에 모호한 개념이 될 수 있다.”라고 한다[18]. 방위산업 보안의 개념을 정의하는 것이 관련 보안 정책을 수립하기 위한 것 이라는 점을 고려할 때 타당한 견해이다. 먼저, Wolfers[18] 규격과 관련하여 보안 정책을 정의하기 위한 몇 가지 규격을 제시한다. 보안 정책은 다음과 같이 특징 측면에서 정의할 수 있다.

첫 번째 구성 요소는 보안 주체이다. 보안 주체는 개인, 그룹, 조직 또는 시스템 등이 될 수 있다. 선택은 특정 보안 영역의 특성에 따라 결정되어야 한다. 방위산업 보안을 위한 대상 조직은 방산업체와 방위사업청과 같은 관련 조직일 수 있다.

두 번째는 보호해야 할 자산이다. 보호해야 할 대상을 결정하는 것이 보안 정책의 시작이며, 자산의 가치와 유출이나 손실의 영향을 고려하여 보호해야 할 자산을 식별해야 한다. 세부 단계를 고려할 경우 자산의 유형에 대해 보호 조치를 취해야 하기 때문에 자산의 형식을 분류해야 한다. 기존의 방위산업 보안은 군사비밀로 지정된 자산을 보호하는 데 초점을 맞추고 있지만, 그 범위를 확대하는 것이 필요하다.

세 번째는 보안의 가치가 정의되어야 한다. 개인, 그룹, 조직 및 국가는 많은 가치를 지닌다. 개인의 수준에는 신체 안전, 심리적 안전성, 재정적 풍요, 복지 등이 포함될 수 있지만 국가 안보에는 정치적 독립성과 영토 보호가 포함된다. 방위산업 보안은 국가 안보와 경제적 가치를 포함할 수 있다.

네 번째는 보안의 정도이다. 전통적인 보안 정책 담당자들과 같은 일부 사람들은 보안 정도에 대해 비판적일 수 있다. 그 이유는 보안이 개량화 할 수 없는 조건이라고 주장하는데 이것은 안전하거나 안전하지 않은 둘 중 하나라는 극단적인 결과를 의미한다. 하지만 직관적으로 극단적 안전성의 상태는 도달할 수 없다. 그러면, 우리는 극단적이지 않은 보안 조건에 얼마나 많은 자원을 할당할 것인지 고민해야 한다.

다섯째, 보안 정책 담당자는 발생 가능한 모든 위협을 파악해야 한다. 그들은 보통 각각의 위협에 대해 구체적인 대응책을 강구한다. 또한, 이미 한번 설정된 보안 정책은 새로 식별된 위협에 따라 변경해야 한다. 예를 들어, 과거에 내부 보안시스템이 내・외부자 위협에 초점을 맞추었다면, 이제는 사이버 공격을 고려하게 될 것이며, ‘안전’을 고려하여 보안 개념에 화재, 지진 또는 정전과 같은 의도하지 않은 위협까지 확대해서 포함해야 한다.

여섯째는 위협에 직접적으로 연관된 수단이다. 보안 정책은 매우 다양한 수단을 포함하고 있으며, 위협에 대응하여 수단을 계속 업데이트해야 한다. 위의 예에서, 보안 시스템은 물리적 위협에 대응하기 위해 카메라와 경비원을 배치하고 해킹에 대한 정보보안 시스템을 구축할 것이다[12].

일곱째, 비용은 언제나 중요하다. 집단이나 국가 같은 보안 주체는 자원이 제한된 상태에서 조직 전체의 목표를 달성하기 위해 자원을 효율적으로 분배하려고 한다. 보안 정책을 실행하기 위해서는 재정적 지원이 필요하다. 따라서, 의사 결정권자는 불필요한 비용 지출을 최소화하기 위해 보안의 정도를 ‘절대적’ 조건으로 보지 않는다.

마지막은 기간이다. 정책의 효과를 예상하기 위한 기간의 관점으로 단기적이고 장기적인 방법들이 있다. 보안의 경우 단기 정책은 장기적인 방법과 다를 수 있다. 단기적으로 위협 요소를 제거하는 직접적인 접근 방식에 초점을 맞추며, 위협 요소는 적용하기 쉽고, 눈에 띄며, 가격이 저렴하다. 하지만, 장기적인 정책은 적용이 상대적으로 어려울 수 있고, 많은 재정적 지원을 받으며 시스템 개선을 요구한다.

지금까지 보안 개념에 대한 구성 요소를 검토하였다. 그러나 위에서 언급된 구성 요소는 보안 정책 수립에 꼭 적합한 것은 아니다. 모든 구성 요소가 항상 설명되어야 하는 것도 아니며, 각 항목은 광범위하고 협의의 관점에서 설명될 수 있다.

3.2 문제점 분석

방위산업 보안 연구는 폐쇄적인 특징으로 인해 오랜 역사를 가지고 있음에도 불구하고 학술적 연구가 거의 없었다. 그러므로 이 장에서는 기존의 방위산업보안에 관한 연구의 문제가 아닌 방위산업 환경의 변화와 관련 정책의 결과로 인한 문제 분석을 하려고 한다.

기존의 방위산업 보안은 지정된 방산업체와 함께 정부에 의해 통제되었다. 이에 따라 방산업체와 협력하는 기업(일반 기업, 군수품 공급 업체 등)들은 정부의 보안 정책을 적용 받지 않아서 중요 정보가 유출되는 피해가 발생하기 쉽다. 반면, 미국에서는 국가 산업보안 매뉴얼이 포함된 산업보안 정책이 모든 대상에 대해 적용되어 전체 계약 프로세스 동안 기밀정보의 유출을 방지할 수 있다[19].

보호가 필요한 자산을 살펴보면, 기존의 보안 정책은 주로 군사비밀 보호에 초점을 맞추어 왔다. 그럼에도 불구하고 그것들에 적용할 수 없는 일부 방산관련 정보는

보호되기 어렵다.

심지어 이원화된 정책 부서도 문제다. 기존의 방위산업 보안은 국방부가 주관이 되어 수행해 왔지만, 방위산업기술 보호는 방위산업기술보호법과 함께 방위사업청의 정책에 의해 보호를 받는다. 방산업체의 관점에서는 같은 보안 수단을 적용하지만, 이원화된 정책은 방산업체로 하여금 중복된 노력을 기울이게 할 수 있다. 따라서, 일원화된 정책 부서와 함께 방위산업 보안에 대한 통합 개념을 설정할 필요가 있다.

3.3 방위산업 보안 개념화 정립

보안의 가치 측면에서 방위산업은 국가 안보를 유지하는데 결정적으로 중요하다. 방위산업기술이 더욱 발전함에 따라 방위산업은 더 정교한 첨단 기술의 무기체계를 만들어 내기 위해 노력하고 있다. 오늘 날의 방위산업기술은 국가 안보의 영역을 넘어서 국가 산업과 경제에 부가가치를 창출하는 원천으로 인식되고 있다. 특히, 북한과 IS 등 테러 조직에 유출된 방위산업기술은 세계 경제에 큰 피해를 주면서 국제 안보 차원에서도 큰 위협이 되고 있다. 결론적으로 보안의 가치에는 국가 안보, 국력, 국가 신인도 제고 들이 포함된다.

보호해야 할 자산의 경우 군사비밀 및 지정된 방위산업기술 뿐만 아니라 방위사업의 전체 프로세스와 관련된 모든 형태의 정보가 보호해야 할 대상이다. 따라서 방산업체, 일반기업, 군수품 공급업체, 연구소, 공공기관 등 방위사업 정보를 보유한 모든 조직으로 활동 영역을 확대해야 할 필요가 있다.

재래식 보안에 있어서 위협은 주로 절도, 스파이, 테러리스트, 적국, 내부자 등 방산업체에 대한 정보 유출 측면에서 의도된 위협을 포함하고 있었는데 앞으로는 가용성 상실의 측면에서 화재, 홍수, 지진 및 정전과 같은 자연현상을 포함하는 것이 필요하다.

또한, 위협은 예측하기 어렵기 때문에 다양한 보호 방법을 적용하고 있다. 일반적으로 보안 조치는 위협에 대처하기 위해 인원, 시설, 정보 보안 등과 같은 부 문 기반 솔루션이다. 하지만 부문기반 솔루션을 구축하게 되면 예측할 수 없는 위협에 대응하기에는 한계가 있다. 따라서 섹터 기반 솔루션과 관련 조직과의 파트너 공유 솔루션을 통합하는 보안 융합이 필요하다. 정부는 이 위협을 막기 위해 다른 나라, 방산업체와 협력하여 상황을 설정하고 정보를 공유해야 한다. 미국의 DIB ISAC은 위협에 공동으로 대응하는 좋은 사례이다.

보안의 수준에 관해서 전통적인 보안담당자는 보안이 얼마나 엄격한 기준을 갖출 수 있는지에 대해 비판해 왔다. 일반적으로 정부 주도의 보안 정책은 모든 조직에 절대적인 방식을 적용하여 가장 높은 수준의 보안을 추구하기 위한 것이기도 하다. 하지만 어느 정도의 보안 수준이 적절한가?라는 질문에 그 누구도 정확하게 답할 수 없을 것이다. 민간 부문의 관점에서 보안 조치는 회사의 시스템 환경과 작업 흐름을 고려하여 보안 수준을 결정해야 한다. 궁극적으로 최적화된 사용자 중심의 보안 정책은 제한된 리소스로 비용 효율성을 달성하기 위해 요구된다.

비용 면에서 보안의 개념은 보안의 수준과 크게 연관되어 있다. 우리나라의 방위산업 환경에서는 대부분의 자산이 개인적인 것이기 때문에 방산업체들이 프로젝트 초기에 회사 예산으로 보안에 소요되는 비용을 투자한다. 따라서 보안에 대한 인식이 낮은 회사들은 상대적으로 투자를 적게하는 경향이 있다. 하지만 방위산업은 공공재에 대한 강한 특성을 가지고 있기 때문에 정부의 재정적 지원과 기업의 공동 노력이 필요하다.

기간 면에서는 단기 및 솔루션을 기반으로 한 보안 정책은 급속하게 변화하는 보안 환경에 따른 위협에 대해 적합하지 않으므로 장기적인 정책 추진이 필요하다.

결론적으로 방위산업 보안 개념은 Table 2와 같이 요약할 수 있다.

Table 2. Summary of the conceptualization for defense industrial security by specifications

Spec.	As-Is	To-Be
Values concerned	National security	National security, National interest, National credibility
Assets to protect	Military confidential, Designated defense technologies, Relevant facilities	All the information for the defense acquisition program, Relevant facilities
Actors	Designated defense firms, Public organizations	All organizations that handle the information related to defense acquisition program
Threats	Theft, Espionage, Competitors, Insiders, Cyber terrorists, etc.	All threats, including natural disasters
Means	Sector-based solutions, (personnel, facilities, IT system, etc.)	Security convergence, Partnership with other agencies
Degree of security	Absolute	Optimum
Costs	Company's own budget	Government financial support needed
Time period	Solution-driven, short-run policies	Additional long-term policies required to improve awareness

4. 결론

한국의 방위산업기술은 세계적인 수준으로 발전하고 있으며, 방위산업 보안은 1945년 이후로 오랜 역사를 가지고 있다. 그러나, 지금까지 방위산업 보안이라는 용어의 개념을 정립하는 데는 관심이 부족했다. 관련 법에 의해 방위산업기술 보호에 대한 논의가 활성화 되었지만 보안의 개념 정립은 여전히 미흡하다. 학문적 연구의 부족과 폐쇄적인 방위산업 환경은 학술적 개념 정립을 어렵게 만들었다. 본 연구는 상세 규격에 따른 방법론을 사용하여 방위산업 보안을 개념화한 것에 의의가 있다.

References

[1] ROK Defense Acquisition Program Administration: Defense Acquisition Program Statistical Yearbook (2016)

[2] Jang, W.: The present status and development strategies of defense industry in South Korea.Sci. Technol. Policy 27(11), 38-45 (2017)

[3] ROK Ministry of National Defense: Military Secret Protection Act (2015)

[4] Kim, Y.: A study on the criminal laws of security in the defense industry of South Korea. Korean J. Ind. Secur. 2(2), 49-90 (2011)

[5] Woo, K.: Research trend and conceptualization of defense industry security from convergence security perspective. J. Inf. Secur. 15(6), 69-78 (2015)

[6] Cho, W.: Industrial policies enhancing the level of security of the defense industry. Master's thesis, The University of Suwon, South Korea (2015)

[7] Lee, J.: Legal restrictions on the industrial secret outfl ow: concentrated on the defense industry. Master's thesis, Seoul School of Integrated Sciences and Technologies (2013)

[8] Shin, H.: A study on the analysis and countermeasure of the real condition for defense industry secrecy-spillage. Master's thesis, Dongguk University, South Korea (2008)

[9] Dussauge, P., Cornu, C.: L' industrie Francaise de l'armement. Economica (1998). (in French)

[10] ROK Ministry of National Defense: Defense Acquisition Program Act (2017)

[11] Y. J. Lee, C. B. Lee, "An Fingerprint Authentication Model of ERM System using Private Key Escros Management Server", Journal of The Korea Academia Industrial cooperation Society, 20.6 (2019): 1-8. DOI:https://doi.org/10.5762/KAIS.2019.20.6.1

[12] Y. J. Lee, T. Y. Jeon, "A Malware Detection Method using Analysis of Malicious Script Patterns", Journal of The Korea Academia Industrial cooperation Society, 20.7 (2019): 613-621. DOI:https://doi.org/10.5762/KAIS.2019.20.7.613

[13] Baldwin, D.A.: The concept of security. Rev. Int. Stud. 23, 5-26 (1997)

[14] Zedner, L.: The concept of security: an agenda for comparative analysis. Leg. Stud. 23(1), 153-175 (2003)

[15] ROK Defense Agency for Technology and Quality: Dictionary of National Defense Science and Technology Terms (2017)

[16] ROK Ministry of National Defense: Defense Technol ogy Security Act (2017)

[17] ROK Ministry of National Defense: Directive, Defen se Industrial Security Service (2017)

[18] Wolfers, A.: "National Security" as an ambiguous symbol. Polit. Sci. Q. 67(4), 481-502 (1952)

[19] U.S. Department of Defense: (DoD) 5220.22-M, Nati onal Industrial Security Program Operating Manual (2006)

[20] Defense Industrial Base Information Sharing and An alysis Center. http://www.dibisac.net

고 희 재(Hee-Jae Go) [정회원]

- 1999년 3월 : 육군 3사관학교 전산정보처리학과 학사
- 2003년 8월 : 연세대학교 전산학과 석사
- 2019년 8월 : 중앙대학교 융합보안학과 박사과정 수료

〈관심분야〉
방위산업보안, 방위산업기술보호, 산업보안

이 용 준(Yong-Joon Lee) [종신회원]

- 2005년 2월 : 숭실대학교 컴퓨터학과 박사
- 2010년 2월 ~ 2016년 3월 : 한국인터넷진흥원 수석연구원
- 2016년 4월 ~ 현재 : 국방보안연구소 선임연구원

〈관심분야〉
산업보안, 사이버보안, 기밀유출차단