

## 방위산업체 보안 평가 개선방안에 관한 연구

이상열, 유연승\*  
명지대학교 보안경영공학과

### A Study on the Improvement of Security Evaluation of Defense Industry Companies

Sang Yeol Lee, Yeon Seung Ryu\*  
Department of Security Management Engineering, Myungji University

**요약** 우리나라의 방위산업은 1972년 자주국방 추진을 시작으로 급속하게 성장하여 현재는 전 세계 무기 수출 규모의 2.1%를 차지하고 있으며 기술력은 9위권으로 평가받고 있다. 이러한 기술 관련 자료들을 탈취하기 위해 국내·외 방위산업체 간의 정보탐지뿐만 아니라 산업스파이의 활동과 컴퓨터 범죄가 점점 증가하고 있으며, 평생직장이라는 고정 관념이 깨지면서 전·현직 임직원에 의한 유출 사고도 증가하고 있다. 유출 사고를 미연에 방지하고자 관련 기관에서는 보안측정, 통합 실태조사를 시행하고 있으며, 한국형 RMF를 준비 중에 있다. 보안측정은 5개 분야 79개 항목, 통합 실태조사는 6개 분야 237개 항목, 한국형 RMF는 17개 분야 761개 항목으로 구성되어 있다. 그러나 이러한 평가제도의 주무 기관이 상이하여 평가 항목들이 중복하여 시행됨에 따라 방산업체들은 부담감과 함께 불필요한 행정력이 소모되고 있는 문제점이 있다. 이러한 문제점을 해소하고자 각각의 보안 평가에서 점검 분야별 중복점검 항목을 도출하였고 상관관계를 분석하였다. 분석 결과를 토대로 중복되는 점검 항목을 통합 실태조사 평가 결과로 대체하는 보안 평가 개선방안을 제안하였으며, 동일한 사항에 대해 중복하여 점검하고 있는 현 상황에서 본 연구의 결과는 이러한 문제점을 해소 하는데 활용될 것으로 기대된다.

**Abstract** The South Korean defense industry has grown rapidly since the promotion of self-defense in 1972, accounting for 2.1% of the worldwide arms exports by this industry. In addition, the technology of this industry is considered the ninth-largest in the world. Correspondingly, information detection between South Korean and foreign defense companies, activities of industrial spies, and computer crimes to steal the technology-related data of the South Korean defense industry are increasing. Moreover, there are also increasing information leakage accidents by former and current executives and employees of these companies. Hence, the companies are conducting security evaluations and integrated surveys to prevent information leakage accidents and are preparing for a Korea-RMF(risk management framework). The security evaluation consists of 79 inspection items in five inspection fields and 237 inspection items in six inspection areas for the integrated survey, and 761 inspection items in 17 inspection areas for the Korea-RMF. However, as the competent institutions of the system for this security evaluation are different, and the inspection items are repeatedly implemented in the evaluation, defense companies have a problem consuming additional administrative manpower and face an increased burden of the evaluation unnecessarily. Hence, this study derived duplicate inspection items by inspection field from each security evaluation and analyzed the correlation between the duplicate inspection items. The analysis was then used to propose the security evaluation improvement plan to replace the overlapping inspection items with the results of the integrated survey. In essence, this study is expected to be used to solve the above-mentioned problem in the security evaluation conducted by defense companies.

**Keywords** : Measurement of Security, Integrated Security Survey, Korea-Risk Management Framework, Duplication Inspection, Correlation

\*Corresponding Author : Yeon Seung Ryu(Myungji Univ.)

email: ysryu@mju.ac.kr

Received April 15, 2022

Accepted July 7, 2022

Revised May 24, 2022

Published July 31, 2022

## 1. 서론

정보화 사회를 맞아 첨단기술 확보가 국력의 척도로 작용하고 있으며 어느 나라가 얼마나 더 많은 첨단기술을 개발해 보유하느냐에 따라 그 나라 경쟁력의 우열이 판가름 나기 때문에 세계 각국은 치열한 기술전쟁을 벌이고 있다. 첨단기술이 집약된 무기체계의 기술력은 기업과 국가 경쟁력의 원천이 되는 관계로 각국은 방위산업기술보호법을 제정하여 그 기술의 개발 못지 않게 보호에도 혼신의 힘을 쏟고 있다. 우리나라도 2015년 방위산업기술보호법을 제정하여 대상기관들로 하여금 기술보호체계를 구축하도록 하고 있다[1].

최근 반도체를 비롯한 첨단 기술들은 세계적인 경쟁력을 확보하고 있어 경쟁국 산업스파이의 표적이 되고 있으며 방위산업분야의 경우 무기체계를 수입하던 국가에서 IT 분야의 첨단기술을 접목시켜 개발한 K2 전차, K9 자주포, KF-21 차세대 전투기 등 첨단무기체계를 수출하는 국가로 변화했다. 2020년 우리나라 방위산업 수출액은 1조8,150억원으로 방위산업 총 매출액 15조3,517억원의 11.8%에 달한다[2]. 방위산업 물자의 수출 증가에 따라 우리의 방위산업기술도 복제되거나 기술 이전이 되고 이로 인해 국가 안전보장과 국제평화에 저해요소로 작용될 가능성이 증대되고 있는 실정이다. 또한 우리나라 방위산업 분야 기술수준은 최고 선진국인 미국 대비 약 81% 수준, 세계 9위권이며, 특정 분야에 있어서는 세계 최고의 기술력을 보유하고 있고 네트워크 환경 변화, 적대국의 사이버공간 상의 침투, 산업스파이 등으로 인해 기술 유출 가능성이 항시 내재되어 있다[3]. 이러한 환경 하에서 보호해야 할 방위산업기술이 외부로 유출될 경우 막대한 경제적 손실과 함께 국가안보에도 치명적일 수 있다.

2020년 9월부터 2021년 8월까지 13개 국내 주요 방위산업체 대상 총 121만 8981건의 해킹 시도가 있었다[4]. 이는 오늘날 방위산업의 세계화 및 기술 수준이 높아지면서 국내·외 방위산업체 간의 경쟁이 치열해지고, 경쟁사 간의 정보활동도 보이지 않게 뜨거워지고 있다는 방증이다. 하지만 아무리 경쟁사의 중요 정보를 입수한다 하더라도 우리 기업의 중요한 기업 비밀이 경쟁사로 유출된다면 치열한 경쟁 전쟁에서 생존하기는 어렵게 된다. 2017년부터 2021년까지 방위산업체 대상으로 한 해킹이 총 14건 발생했으며, 첨단 무기 설계도 등 주요 방산관련 비밀이 다수 빠져나가 사이버 안보 위협이 심각한 수준인 것으로 조사됐다[5]. 그러나 우리의 현실은 주

요정보를 지키기 위한 노력보다는 기술개발을 위한 연구 투자와 재산보전에만 급급한 게 사실이다. 이에 2020년 8월 방위산업기술보호를 주무하는 중앙행정부처에서 기술유출 사고 발생 시 해당 업체에 최고 10억원의 과징금을 부과하고, 과태료를 5억 원까지 올리겠다고 발표한다[6].

오늘날 국내·외 방위산업체 간의 경제 전쟁에서 경쟁사의 정보탐지 뿐만아니라 산업스파이의 활동과 컴퓨터 범죄가 점점 증가하고 있으며, 평생 직장이라는 고정 관념이 깨지면서 전·현직 임직원에 의한 유출 사고도 증가하고 있다. 이러한 유출 사고를 미연에 방지하고자 관련기관에서는 보안측정, 통합 실태조사를 시행하고 있으며, '24년 전면 시행예정인 한국형 RMF를 준비 중에 있다. 그러나 이러한 평가제도의 점검항목들이 중복하여 시행됨에 따라 방산업체들은 부담감과 함께 불필요한 행정력이 소모되고 있는 문제점이 있다.

2019년 1월 3일 시행된 제63회 현안조정회의에서 실태조사와 보안감사의 중복점검에 대한 내실화를 국방부에 권고[7]하여 기술보호를 위한 실태조사와 방산관련 비밀 보호를 위한 보안감사가 통합되어 통합 실태조사를 실시하게된 배경과 같이 중복점검에 소모되는 방산업체의 행정력을 보호체계 보강에 투입하는 것에 대해 고려해 볼 필요가 있다.

따라서 본 연구에서는 방산업체 대상 보안 평가 중 보안측정, 통합 실태조사, 한국형 RMF(K-RMF, Korea-Risk Management Framework)에서 중복 적용되는 평가항목을 도출하여 보안 점검 개선방안을 제안하고자 한다.

## 2. 이론적 배경

### 2.1 방위산업의 정의

방위산업은 “방위산업물자를 생산하거나 연구개발하는 업”으로 정의 되어 있으며, 이는 안정적 조달원 확보와 엄격한 품질보증 등을 위하여 정부로부터 방위산업물자로 지정받은 이른바 지정 방위산업물자를 생산하거나 연구개발하는 산업을 말한다[8]. 광의의 개념으로는 정부가 지정한 방위산업물자를 포함한 무기체계 또는 비무기체계를 생산하거나 연구개발하는 산업을 포함한다. 방위산업은 1970년대 이전까지 미국의 군사원조에 의존하여 군사력을 유지하다가 1972년 자주국방 추진으로 새로운 전환점을 맞이하였으며, 급속한 성장을 이루었다. 2015~2019년, 우리나라는 수십 년 만에 처음으로 전 세

계 무기 수출 규모의 2.1%로 세계 10위권 내에 진입한 것으로 평가되고 있다[9].

국내 방위산업에 참여하는 업체를 방위산업체(방위산업물자를 생산하는 업체), 일반업체(방위산업과 관련된 업체로서 방산업체가 아닌 업체), 방위산업과 관련이 없는 일반업체(군수품을 납품하는 업체로서 방위산업체 또는 일반업체가 아닌 업체) 등으로 분류 된다[10]. 그 중 방위산업체는 2021년 9월말 기준 85개社로 주요 방위산업체는 65개社(76.5%), 일반 방위산업체는 20개社(23.5%)이다. 방위산업체는 해당 업체가 생산하는 방위산업물자(2021년 9월말 기준 1,493개의 완제품 및 구성품)에 따라 주요 방위산업체와 일반 방위산업체로 분류한다. 기업규모별 방위산업체 현황은 대기업 19개社(22.4%), 중견기업 18개社(21.2%), 중소기업 48개社(56.4%)로 절반 이상이 중소기업이다[11]. 방위산업체 구성의 절반 이상이 중소기업으로 중소기업은 대기업에 비해 예산 및 인력이 부족하여 법령에서 규정하고 있는 보안체계 구축이 미흡한 상태이다.

## 2.2 방위산업보안의 정의

사전적 의미에서 보안(Security)이라 함은 “안전을 유지하는 것”, “자산을 보호하기 위한 활동”이라고 할 수 있는데 여기에서의 “자산”이란 유형의 자산 뿐만 아니라 무형의 자산까지 포함할 수 있으며, 보안의 주체별로 개인보안, 기업보안, 국가보안 등으로 구분할 수 있다.

방위산업보안은 적(불순분자)으로부터 군이 필요로 하는 방위산업 물자를 생산 공급하는 방위산업체의 기밀을 보호하고 업체가 방위산업 물자를 적절한 시기에 생산 공급할 수 있도록 지원하여 군 전투력을 보장하기 위한 제반 활동을 말한다. 이 활동에는 적의 간첩행위나 테업 등으로부터 군을 보호하기 위한 “군사안보”와 방위산업체가 보유하고 있는 유·무형자산(기술, 인력, 장비, 정보 등)을 보호하고 손실을 방지하기 위한 “산업보안”이 공존하고 있다.

방위산업보안은 원래 군에 필요한 각종 장비 및 장병들의 의식주에 필요한 물품을 생산하는 업체가 파업이나 화재 등 각종 사고 시 군에 직접적 피해를 올 수 있어 이를 예방하기 위해 제도화 된 것으로 시대환경에 맞게 변화 발전하고 있다. 방위산업 분야는 군사비밀, 산업기술, 방위산업물자, 핵심기술인력, 국가보안목표시설 등 국가안보와 관련된 다양한 보안요소를 보유하고 있기 때문에 다른 산업보다 더 높은 수준의 보안이 요구된다. 이로 인해 방위산업체들은 보안 전담조직과 보안담당관을 임명

하여 전사적 차원에서 제반 보안요소를 보호하기 위한 종합적인 대책을 강구하고 있다. 또한, 방위산업보안업무훈령에 의거해서 보안대책 수립으로부터 시행과 조정 및 감독까지 전반적인 보안업무를 수행하고 있다.

## 2.3 방위산업체 보안 평가 종류

본 연구에서는 보안 평가를 “보안사고 예방 등을 위하여 보안 실상을 분석·파악하며, 취약점을 도출하여 현재의 보안 상태를 확인하는 행위”라고 정의 하였다. 그러나 적용하는 법령에 따라 사용하는 용어와 범위를 달리 하고 있어 점검을 받는 업체는 혼란스럽다. 방위산업체 대상 보안 평가의 종류에는 방위산업보안업무훈령에 따른 보안측정, 방위산업기술보호법에 따른 통합 실태조사, 국방보안(사이버보안)제도에 따른 한국형 RMF (K-RMF: Korea-Risk Management Framework)라고 칭한다. 물론 한국형 RMF는 2023년부터 무기 체계에 시범 적용 예정이고, 2024년 전면 시행 예정이다. 그러나 본 연구에서는 위 세 종류의 점검을 보안 평가로 통칭한다.

보안측정은 방위산업 보안의 대상인 시설, 장비 등을 테러나 파괴, 도청, 해킹 등 각종 위협요소로부터 보호하는 데 필요한 보안대책을 강구하기 위하여 보안업무 전반에 걸쳐 보안취약 요인을 종합적으로 진단하는 보안조사 활동이다[12].

통합 실태조사는 대상기관(방위산업기술을 보유하거나 연구개발 사업을 수행하는 기관)의 방위산업기술 보호체계의 구축·운영, 기술 보호에 필요한 대책 수립·시행 현황, 수출 및 국내이전 시 방위산업기술 보호에 필요한 대책 수립 현황을 진단하는 활동으로 대상기관이 방위산업기술을 보유하고 있는 동안 법령에서 규정한 기준에 따라 보호하고 있는지를 점검한다[13].

한국형 RMF는 국방 IT 전 수명주기에서의 사이버 보안 위험관리를 위한 프레임워크로 국방사이버공간에서 보안 취약점 분석·평가·조치를 통한 정보의 기밀성, 무결성, 가용성을 보장하기 위하여 취하는 물리적, 기술적, 관리적 활동이다[14].

## 3. 보안 평가 개선방안

### 3.1 보안 평가 유형별 분석

방위산업보안업무훈령은 보안측정 시기·절차를 설명하고, 방위산업기술 보호지침은 통합 실태조사의 가이드

를 제공하며, 국방사이버안보훈령은한국형 RMF의 사이버안 관리수준평가의 기반을 제공하고 있다. Table 1은 보안측정·통합 실태조사·한국형 RMF의 목적, 대상, 점검 시기, 주관기관을 비교한 것으로 다음과 같다. 보안측정은 방위사업 시작 전 방위사업과 관련된 자료를 보호할 수 있는 체계를 구축하고 있는지 확인하는 것을 목적으로 하며, 방위산업계(방산업체·방산관련업체·군무역대리점)를 측정 대상으로 한다. 점검 시기는 수시 점검으로 방산업체 지정, 정보통신망 신설·증설 등 측정 사유가 발생 시 시행하고, 유효 기간은 3년을 원칙으로 하며, 군사안보지원사령부가 관련 기관의 보안측정 요청을 받아 주관한다[12]. 통합실태조사는 방위산업기술 보

호 체계 운영·유지 관리 실태를 점검을 목적으로 하며, 방위산업기술을 보유하고 있거나 연구개발사업을 수행하고 있는 기관을 조사 대상으로 한다. 점검 시기는 매년 점검하는 정기와 유출사고 발생 시 점검하는 수시로 나뉘며, 주관 기관은 방위사업청으로 국가정보원, 군사안보지원사령부와 협조하여 3개 기관이 시행하고 있다[13]. 한국형 RMF는 방위사업 시작 전과 사업 간에 국방정보(방위사업 관련 정보 포함)를 보호할 수 있는 체계를 구축하여 운영하고 있는지를 확인하는 것을 목적으로 하며, 국방부 장관의 조정 통제를 받는 부대·기관 및 방위사업법에 따라 정부에서 지정한 방산업체를 점검 대상으로 한다. 점검 시기는 부정기적으로 취급하는 무기체계 보안 위험도의 높고·낮음에 따라 주기를 달리하며, 국방부에서 주관하고 있다[14].

Table 1. Comparison Table by Security Assessment Type

Division		Specifics
Measurement of security	Definition	Security investigation activities that comprehensively diagnose security vulnerabilities throughout security operations
	Purpose	Ready for protection
	Inspection Object	Defense Industry Companies
	Inspection Cycle	Nonscheduled (security environment changes, etc)
	Authorities Concerned	Defense Security Support Command
Integrated security survey	Definition	Establishment and Operation Inspection of Defense Industrial Technology Protection System
	Purpose	Operational status for protection
	Inspection Object	Agency with Defense Industry Technology
	Inspection cycle	Every year
	Authorities Concerned	Defense Acquisition Program Administration
Korea-Risk Management Framework	Definition	Physical, technical and administrative activities to ensure confidentiality, integrity and availability of information in cyberspace
	Purpose	Ready-Operational status for protection
	Inspection Object	Units and Agencies coordinated and controlled by the Minister of Defense
	Inspection cycle	Nonscheduled (The inspection cycle varies depending on the high and low security risk)
	Authorities Concerned	Ministry of National Defense

### 3.2 보안 평가 중복 점검항목 도출

앞에서 살펴보았듯이 보안측정은 측정 사유가 발생 시 수시로 실시하며, 유효기간은 기본 3년이지만 매년 통합 실태조사를 받을 경우 유효기간이 갱신되는 형태이다. 통합 실태조사는 매년 보안 수준 평가를 하며, 평가 시 3개 기관(방위사업청, 국가정보원, 군사안보지원사령부)이 평가하고, 기술의 식별·관리, 인원 통제, 시설보호, 연구개발 및 수출/기술이전, 방산협력업체 기술보호 분야는 방위사업청이 평가한다. 정보보호 분야는 국가정보원이 평가하고, 군사기밀보호 분야는 군사안보지원사령부가 평가를 한다.

Table 2는 보안 평가 유형별 점검 항목을 비교한 것이다. 보안측정은 Table 2 Measurement of security에서 처럼 문서보안, 인원보안, 시설보안, 정보통신보안, 기업보안, 5개 분야 79개 점검 항목으로 구성되어 있고[12], 통합 실태조사는 Table 2 Integrated security survey에서 처럼 기술의 식별·관리, 인원통제, 시설보호, 정보보호, 연구개발 및 수출·국내이전 시 기술보호·방산협력업체 기술보호, 군사기밀보호, 6개 분야 237개 항목으로 구성되어 있으며[13], 한국형 RMF는 Table 2 Korea-Risk Management Framework과 같이 접근통제, 보안교육·훈련, 감사·책임, 형상관리, 비상계획, 암호관리, 식별·인증, 사고대응, 유지보수, 매체보호, 보안계획·평가, 시설·운용환경 보호, 인원보안, 시스템·서비스 획득, 시스템·통신 보호, 시스템·정보 무결성, 공급망 관리, 17개 분야 761개 항목으로 구성되어 있다[14].

Table 2. Comparison of Security Inspection Categories in the Defense Industry Companies

Division	Inspection Categories	Amount
Measurement of security	Total	79
	Document Security	4
	Personnel Security	9
	Facility Security	22
	Information and Communications Security	41
	Enterprise Security	3
Integrated security survey	Total	237
	Identification and Management of Technology	15
	Personnel Security	11
	Facility Protection	10
	Information Protection	118
	R&D and Export · Technology Transfer / Technology Protection for Defense partners	21
	Military Secret Management	62
Korea-Risk Management Framework	Total	761
	Access Control	111
	Awareness and Training	9
	Audit and Accountability	56
	Configuration Management	48
	Contingency Planning	43
	Cryptography Management	6
	Identification and Authentication	44
	Incident Response	33
	Maintenance	25
	Media Protection	18
	Security Planning and Assessment	35
	Physical and Environmental Protection	47
	Personnel security	14
	System and Service Acquisition	59
	System and Communications Protection	110
	System and Information Integrity	82
	Supply Chain Management	21

Fig. 1은 각각의 점검 항목을 분야별로 매칭을 한 결과이다. 보안측정 점검 항목 79개를 통합 실태조사 점검 항목에 매칭을 하였다. 매칭 결과 보안측정 평가 항목 모두 통합 실태조사 항목에 포함되었다. 다시 통합 실태조사 점검 항목을 한국형 RMF 항목과 매칭을 하였다. 기술의 식별·관리 분야에서는 한국형 RMF와 중복되는 항목은 없었으며, 인원통제 11개 항목, 시설보호 10개 항목, 정보보호 118개 항목, 군사기밀보호 45개 항목, 총

184개 항목이 중복되었다. 이는 통합 실태조사 237개 평가 항목을 기준으로 77.63%, 한국형 RMF 761개 평가 항목을 기준으로 24.17%에 해당한다.

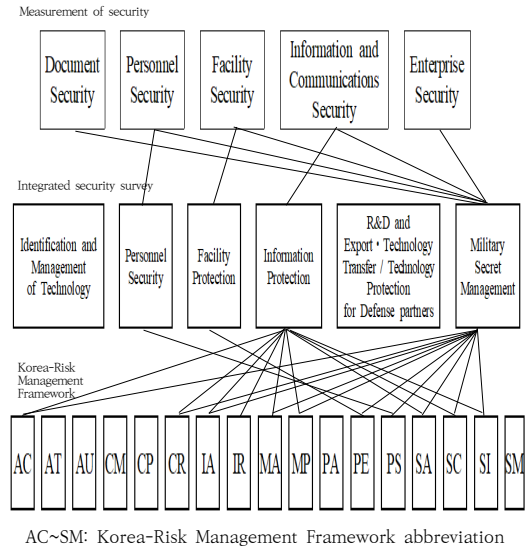


Fig. 1. Relationship by Field of Security Inspection

### 3.3 보안 평가 중복 점검항목 개선방안

3.2절에서 살펴보았듯이 방산업체의 보안 평가를 위한 점검에 있어서 적용 법령에 따라 보안측정, 통합 실태조사, 한국형 RMF를 시행하지만, 이 세 종류의 보안 평가의 점검항목들이 중복됨에 따라 한국형 RMF를 기준으로 통합 실태조사는 77.63%의 불필요한 행정력을 소모하고, 통합 실태조사를 기준으로 한국형 RMF는 24.17%의 행정력을 소모하고 있으며, 이는 고스란히 방산업체들은 부담감으로 남아 있는 문제점이 있다. 따라서 이러한 문제점에 대한 해소방안이 필요할 수 있다.

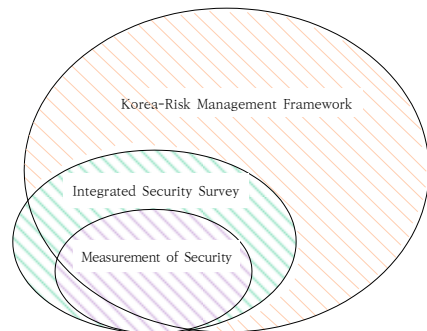


Fig. 2. Relationship between Integrated Security Survey and other Security Audit

Fig. 2는 세 종류의 보안 평가에서 중복하여 점검하고 있는 항목을 도출하여 집합화한 결과로 보안측정은 통합 실태조사의 부분집합이고, 통합 실태조사는 한국형 RMF와 교집합으로 표현될 수 있다.

그러므로 매년 정기적으로 점검하고 3개 기관이 함께 평가함으로써 객관성이 확보된 통합 실태조사의 점검항목을 기준으로 하여 보안측정 및 한국형 RMF 보안 평가 시 통합 실태조사와 중복되는 점검항목은 통합 실태조사 평가 결과로 대체하는 보안 평가 개선방안을 제안한다.

#### 4. 결론

방위산업체의 보안 평가를 위한 점검에 있어서 관계 법령에 따라 보안측정, 통합 실태조사, 한국형 RMF를 적용하고, 각각의 점검항목으로 평가하고 있다. 따라서 본 연구는 세 종류의 보안 평가에서 동일 사항에 대해 중복하여 점검하는 항목을 도출하였고, 이를 토대로 개선방안을 제안하고자 하였다.

보안 평가 점검 항목은 보안측정이 5개 분야 79개 점검 항목, 통합 실태조사가 6개 분야 237개 점검 항목, 한국형 RMF는 17개 분야 761개 항목으로 구성되어 있었다. 이에 보안측정과 통합 실태조사와 한국형 RMF를 분야별로 동일한 점검 항목을 찾기 위해 매칭을 시켰다. 매칭 결과 보안측정의 79개 점검 항목 모두가 통합 실태조사에 포함되었다. 또한, 통합 실태조사 측면에서는 인원 통제(11개), 시설보호(10개), 정보보호(118개), 군사기밀보호(45개) 분야에서 184개 항목이 한국형 RMF 점검 항목과 매칭되었다. 이는 통합 실태조사 점검 항목 237개 중 184개로 77.63%를 한국형 RMF 측면에서는 점검항목 761개 중 184개로 24.17%를 차지한다. 따라서 보안측정은 통합 실태조사의 부분집합이고, 보안측정과 통합 실태조사는 한국형 RMF와 교집합으로 표현될 수 있었다. 이러한 결과로 방위산업체 대상 보안 평가 항목들이 중복되어 있음을 알 수 있었지만, 적용 법령에 따라 평가 기관이 서로 상이하여 타 기관이 평가한 결과에 대한 수용의 문제가 있었다. 따라서 같은 기관이 평가하는 보안측정과 한국형 RMF는 평가 결과를 서로 수용하고 차후 타 기관이 평가한 결과를 수용하는 단계적 추진 방안을 고려해 볼 수 있다.

평가 기관이 방위산업체 대상 보안 수준 평가 시 적용 법령에 따라 동일한 사항에 대해 중복하여 점검하고 있는 상황에서 본 연구는 이러한 문제점을 해소하는데 활용될 것으로 기대된다.

#### References

- [1] ROK Ministry of National Defense, "Defense Technology Security Act", Dec. 2020
- [2] Korea Defense Industry Association Statistical Team, "2021 Management Analysis of Defense Companies", Korea Defense Industry Association, Dec. 2021, pp.150-153
- [3] Defense Agency for Technology and Quality, "Defense Industry Technology Identification Study", Defense Acquisition Program Administration, Mar. 2015, p.11
- [4] KBS NEWS, "'1.21 Million Attempts to Hack Major Defense Companies in One Year'.... Defense Acquisition Program Administration 'Compositon of Ant-Hacking Pan-Governmental Organization'", Korea Google Suvey, [cited 2021 October 12], Available From: <https://news.kbs.co.kr/news/view.do?ncd=5298789> (accessed Mar. 20, 2022)
- [5] NEWSIS, "In the Past Five Years, 14 Cases of Hacking Damage to Defense Companies... 'KF-21 Schematic Diagram Leakage'", Korea Google Suvey, [cited 2021 October 6], Available From: [https://mobile.news1.com/view.html?ar\\_id=NISX20211006\\_0001604443](https://mobile.news1.com/view.html?ar_id=NISX20211006_0001604443) (accessed Mar. 20, 2022)
- [6] NWES1, "Defense Acquisition Program Administration 'A Fine of not more than 1 Billion Won on Defense Companies that Leak Technology such as Hacking'", Korea Google Suvey, [cited 2021 August 20], Available From: <https://www.news1.kr/articles/?4409286> (accessed Mar. 20, 2022)
- [7] Cabinet Office Press Release, "We will keep our country's main industrial technology even more firmly.", January. 2019, p.4-5
- [8] ROK Ministry of National Defense, "Defense Acquisition Program Act", Mar. 2021, p.1
- [9] Stockholm International Peace Research Institute, "SIPRI YEARBOOK 2020, Armament, Disarmament, International Security, Yearbook: Korean Summary", PEACEMOMO, 2020, p.13
- [10] ROK Ministry of National Defense, "Defense Acquisition Program Act", Mar. 2021, p.2
- [11] Korea Defense Industry Association Statistical Team, "2021 Management Analysis of Defense Companies", Korea Defense Industry Association, Dec. 2021, pp.42-49
- [12] ROK Ministry of National Defense, "Defense Industry Security Service Instruction", Feb. 2021
- [13] Defense Acquisition Program Administration, "Defense Industry Technology Protection Instruction", June. 2021
- [14] ROK Ministry of National Defense, "Korea-Risk Management Framework, ' 21 Year Educational Resources", Dec. 2021, pp.2-10

---

이 상 열(Sang Yeol Lee)

[정회원]



- 2005년 7월 ~ 2013년 11월 : 육군종합정비창 군수담당
- 2019년 2월 : 아주대학교 사이버 보안전공(석사)
- 2021년 8월 ~ 현재 : 명지대학교 보안경영공학 박사과정 재학

<관심분야>

사이버보안, 방위산업보안, 개인정보보호

---

유 연 승(Yeon Seung Ryu)

[정회원]



- 1990년 2월 : 서울대학교 계산통계학과(학사)
- 1992년 2월 : 서울대학교 계산통계학과 전산과학전공(석사)
- 1996년 8월 : 서울대학교 계산통계학과 전산과학전공(박사)
- 2003년 3월 ~ 현재 : 명지대학교 컴퓨터공학과 교수
- 2015년 3월 ~ 현재 : 명지대학교 대학원 보안경영공학과 교수
- 2022년 3월 ~ 현재 : 명지대학교 대학원 방산안보학과 교수

<관심분야>

보안경영, 방산안보, 사이버보안