

방위산업 기술보호를 위한 통합 정보분류 체계 연구

A Study on the Integrated Information Classification System for the Protection of Defense Industry Technologies

황문경*, 김동선**, 박영욱***, 류연승****

Moon-Kyung Hwang*, Dong-Sun Kim**, Yeong-wook Park***, Yeon-Seung Ryu****

ABSTRACT

Defense companies handle various types of sensitive government information, but they face difficulties in systematically protecting and managing it due to the lack of a unified government classification system. In addition, malicious threats are increasing due to the rapid development of defense industry technologies, and the security paradigm is shifting to a data-centric approach, making it urgent to improve the information classification system.

Therefore, this study proposed a method for classifying the information held by defense companies according to the national classification system as a whole. This study is practical by proposing a method of utilizing the existing system instead of introducing foreign systems or designing new classification systems, which can lead to side effects and administrative waste. In addition, considering that defense companies are subject to legal and administrative controls regarding information protection and management, the classification level of each piece of information held by defense companies was determined through an in-depth analysis of relevant laws and regulations, and the need to distinguish between national network data classification and information in the private and defense industries was also considered.

However, this study has limitations in that it only proposes a method for classifying information held by defense companies into a single system. Future research is needed to develop policy proposals and a 'Guide to Information Classification and Protection.'

초 록

그간 우리 방산업체는 정부의 기밀분류체계가 통일되지 않은 가운데, 다양한 종류의 민감한 정부 정보를 보유 및 취급함에 따라 체계적인 정보 보호 및 관리에 어려움을 겪어 왔다. 더욱이 최근에는 방위산업 기술의 가파른 성장으로 악의적 위협이 증가하고, 데이터 중심의 보안 패러다임 변화도 심화되고 있어 정보분류체계 개선이 시급한 실정이다.

이에 본 연구에서는 방산업체 보유 정보 전반을 '국가기밀 분류체계'라는 기존 제도를 활용하여 통합 분류할 수 있는 방안을 제안했다. 해외 제도를 도입하거나 분류체계를 신규 설계하여 부작용 및 행정 낭비를 유발하기보다 기존 제도를 활용하는 방안을 제시함으로써 실용성을 확보했다. 또한, 방법론적으로는 방산업체의 정보 보호 및 관리에는 법적·행정적 통제가 적용됨을 고려하여 관련 법령 및 규정 등을 심도 있게 분석하여 이를 근거로 방산업체 보유 정보 각각이 해당하는 '국가기밀 분류체계' 등급 수준을 규명하는 방식을 주로 활용하였으며, 최근 국정원에서 발표한 '국가 망 보안체계 가이드라인' 상 데이터 분류와 민수 및 방산 부문 정보의 구분 필요성도 고려했다.

다만, 본 연구는 방산업체 보유·취급 정보를 하나의 체계로 분류하는 방안을 제시하는 데 그친 한계가 있다. 향후에는 정책 제안 및 '정보 분류 및 보호 가이드' 개발을 위한 연구로 발전시킬 필요가 있을 것이다.

Key Words : Defense company(방산업체), Defense industry technology protection(방위산업기술보호), Information classification(정보 분류), Classified Information protection(기밀 보호), Integrated classification system(통합된 분류 체계), Relative Importance(상대적 중요도)

* 황문경, 명지대학교 대학원 방산안보학과 석박사통합과정

** 김동선, 명지대학교 대학원 방산안보학과 박사

*** 박영욱, 명지대학교 대학원 방산안보학과 교수

**** 류연승, 명지대학교 대학원 방산안보학과 교수(교신저자 E-mail : ysrju@mju.ac.kr)

I. 서 론

미국, 중국 등 해외 국가에서는 통합된 국가기밀분류체계를 갖추고 있으나, 우리나라 경우는 관할 기관의 업무 성격에 따라 「형법」, 「군형법」, 「국가보안법」, 「군사기밀보호법」, 「산업기술의 유출방지 및 보호에 관한 법률」(이하 ‘산업기술보호법’), 「방위산업기술보호법」(이하 ‘방산기술보호법’) 등 여러 법률로 분산하여 ‘기밀정보’를 규정하고 있으며, 기밀의 종류도 국가기밀, 군사기밀, 군사상 기밀, 외교상 기밀, 산업기술, 방위산업기술(이하 ‘방산기술’) 등 다양하게 존재한다. 이에 따라 법정 절차에 따라 등급화되어 지정되는 국가기밀(I·II·III급 비밀)과 군사기밀(군사I·II·III급 비밀) 외에 기밀 분류와 우선순위마저도 불명확한 실정이다.

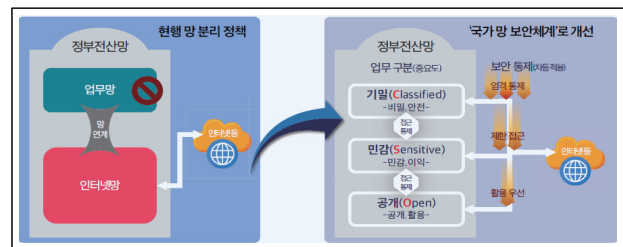
특히, 방산업체는 민간업체임에도 불구하고, 전략물자 연구개발 및 제조 등 국방획득사업 계약에 의해 국방 전략, 무기체계 역량 및 기능, 국방과학기술, 국방계약 사항 등 민감한 정부 주요 정보를 보유 및 취급하고 있다. 이러한 특성으로 인해 방산업체에는 국가기밀, 군사기밀, 영업비밀, 산업기술, 방산기술 등 다양한 종류의 기밀들이 혼재하여 존재할 수 밖에 없고, 이에 따라 방산업체가 보유하고 있는 정보에는 관리 주체가 다른 정부 기밀분류체계가 동시 적용되고 있다.[1]

이러한 환경 속에서 방산업체에서는 같은 시설·시스템 내에 존재하는 하나의 문건이 여러 종류의 기밀로 분류되기도 하고, 기밀 간 우선순위가 명확하지 않아 체계적인 보호 관리에 어려움을 겪고 있는 실정이다. 또한, 보유·취급하는 정보의 상대적 중요도를 반영하여 기업 스스로 전략적·효율적인 보안 투자가 필요하겠으나, 현실적 제한으로 국방부, 방사청 등 다수의 기밀 관할 기관으로부터 보안통제를 받을 수 밖에 없어 부담이 가중 되고 있는 실정이다.

또한, 2024년 우리 국방과학기술은 중국과 함께 2021년 대비 가장 많은 분야에서 기술 수준이 상승하였으며, 미국 대비 82%(세계 8위) 수준에 이르렀다.[2] 이에 따라, 방위사업청에서 2020년 3월부터 운영하고 있는 ‘방산기술 유출·침해사고 신고센터’로 접수된 방산기술 유출 사례가 2020년 3월부터 연말까지는 6건, 2021년 8건, 2022년 3건,

2023년 5건 등으로 매년 10건을 넘지 않던 것이 2024년 초부터 8월말 사이에 15건이 발생하는 등 우리 방산기술을 노리는 인터넷 해킹, 내부자 기술유출 등 악의적 위협 또한 지속 증가하고 있는 실정이다.[3] 더욱이 기존 망분리 정책으로 인해 AI, 빅데이터, 클라우드 등 신기술 적용에 어려움이 있고 다양화된 다층보안체계(MLS : Multi Level Security)와 연계가 필요한 상황이기도 하다.[1, 4]

따라서, 시대적으로 보안체계에 대한 패러다임 전환이 필요하다. 이러한 상황에서 최근 국정원에서는 다음 <그림 1>과 같이 ‘국가망 보안체계 보안 가이드라인’을 발표(2025. 1.24.) 하였다. 그 핵심 내용은 국가 망 데이터를 중요도에 따라 C(Classified, 기밀), S(Sensitive, 민감), O(Open, 공개)의 3개 등급으로 나누고 이에 맞춰 보안 강도를 차등 적용하는 것으로, 적용을 위한 선결과제는 통합된 정보분류체계이다.[5]



〈그림 1〉 국가망 보안체계 비교[5]

이러한 변화 속에서 정보분류체계 개선이 미뤄진다면, 방산업체의 혼란은 더욱 가중될 수 밖에 없으며 방산기밀에 대한 효과적 보호도 요원해질 것이다. 또한, RMF, CMMC 등 정보 중심의 글로벌 정보보안 거버넌스 대응에도 어려움이 있을 것으로 예측된다.

따라서, 본 연구에서는 방산업체가 보유·취급하고 있는 정보를 통합된 체계로 분류할 수 있는 방안을 제시하는 데 목적을 두고 있다. 이를 위해 먼저 방산업체에 현재 적용되고 있는 기밀분류체계에 대해 살펴보고, 이와 대비되는 미국과 중국의 국가기밀분류체계를 분석하여 이를 통해 발전 방안에 대한 시사점을 도출하였다. 다음으로 방산업체 보유 정보의 종류를 파악하고 이들의 상대적 중요도를 분석하였다. 끝으로 이들 정보들을 통합 분류할 수 있는 체계에 대해 제시하였다.

II. 관련 연구

2.1 국내 국가정보 분류체계(방산업체 보유·취급 정보를 중심으로)

국내 국가정보 분류체계 중 방산업체가 보유·취급하고 있는 정보와 관련된 기밀분류체계에 대해 살펴보고자 한다.

이를 위해서는 다음 <그림 2>와 같이 기밀 분류와 보안 체계 관련 국가정보 법률 체계에 대한 구조적 이해가 필요하다.



<그림 2> 국가정보 법률 체계

방산업체가 보유하고 있는 기밀에 대해서는 크게 국가기밀, 군사기밀, 방산기술, 산업기술의 4가지 분류체계가 적용되고 있다.

첫 번째로, 국가기밀 분류체계에서는 정보를 「보안업무규정」 및 「국가정보 보안기본지침」 등에 따라 ① 비밀(I·II·III급 / 보안업무규정 제4조에 따라 분류된 비밀), ② 대외비(비공개 대상 정보 중 직무 수행상 특별히 보호가 필요한 사항 / 보안업무규정 시행규칙 제16조 제3항에 따라 분류된 대외비), ③ 비공개 업무자료(공공기관의 정보공개

에 관한 법률 제9조 제1항에 따른 비공개 대상 정보), ④ 공개 업무자료(공공데이터의 제공 및 이용 활성화에 관한 법률 제19조에 따라 공표된 공공데이터를 포함한 비밀 및 대외비와 비공개 업무자료를 제외한 모든 자료 또는 정보)로 분류하고 있다.[6]

두 번째로, 군사기밀 분류체계에서는 국방보안이 적용되는 정보인지, 방산보안이 적용되는 정보인지에 따라 두 가지 다른 분류가 적용된다. 국방보안이 적용되는 정보는 「국방보안업무훈령」 등에 따라 ① 비밀(군사 I·II·III급 / 군사기밀보호법 제3조 및 시행령 제3조, 국방보안업무훈령 제16조), ② 비공개 업무자료(일반 군사자료 중 공공기관의 정보공개에 관한 법률 제9조 제1항 각호 요건을 갖춘 자료), ③ 일반 군사자료(군사비밀이 포함되지 않은 자료)로, 방산보안이 적용되는 정보는 「방산보안업무훈령」 등에 따라 ① 비밀(군사 I·II·III급 / 군사기밀보호법 제3조 및 시행령 제3조, 방산보안업무훈령 제5조), ② 방산관련 주요자료(대외 누설 및 유출 시 방산보안에 유해하거나, 방위산업에 미치는 영향을 고려할 때 관리가 필요한 자료 / 방산보안업무훈령 제149조), ③ 방산관련 일반자료(비밀, 방산기술자료, 방산관련 주요자료를 제외한 군 및 방산관련 자료 일체)로 분류하고 있다.[7, 8]

세 번째로, 방산기술에 대해서는 「방위산업기술보호법」 및 「방위산업기술 보호지침」 등에 따라 ① 판정기술(방산업체 등에서 보유하고 있는 기술이 방산기술에 해당함을 방위사업청으로부터 판정받은 기술 / 방위산업기술보호법 제7조 및 방위산업기술보호법 시행령 제13조), ② 식별기술(방위산업기술에 해당하거나 해당 가능성이 있는 기술을 방산업체 등에서 심의회를 거쳐 식별한 기술로, 관리대상 기술 대장에 기록하고 관리)로 분류하고 있다.[9]

네 번째로, 산업기술에 대해서는 「산업기술보호법」 및 「산업기술보호지침」 등에 따라 ① 국가핵심기술(해외로 유출될 경우에 국가의 안전보장 및 국민경제의 발전에 중대한 악영향을 줄 우려가 있는 기술로 지정 및 고시된 것 / 산업기술보호법 제9조 및 산업기술보호지침 제2조) ② 산업기술(기술상의 정보 중 행정기관의 장이 산업경쟁력 제고나 유출방지 등을 위하여 지정·고시·공고·인증하는 기술 / 산업기술보호법 제2조)로 분류하고 있다.[10]

문제는 방산업체에 이와 같이 다수의 상이한 기밀분류체계가 적용되고 있으며, 해당 분류체계의 각 등급이 다른

체계에서는 어느 등급 수준에 해당하는지를 설명하거나 규정하고 있는 법규가 존재하지 않는다는 점이다. 게다가 이러한 상황에서 기밀을 규정하고 있는 각각의 법규들은 해당 기밀에 대한 보호 및 관리는 물론이고 보호 절차를 위반하거나 기밀이 유출되었을 때의 벌칙까지 규정하고 있다.

〈표 1〉 방산업체에 적용되는 대표적 기밀분류체계

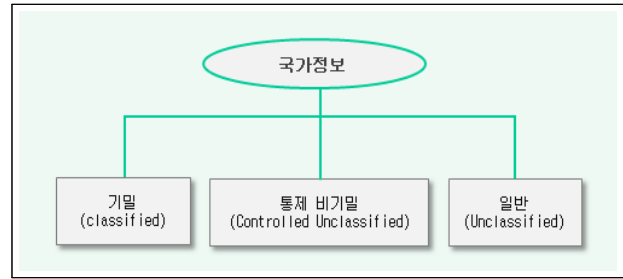
구분	국가기밀	군사기밀	방산기술	산업기술
관련 법규	보안업무규정, 국가정보보안 기본지침	국방보안업무훈령, 방산보안 업무훈령	방산기술보호법, 방산기술보호지침	산업기술보호법, 산업기술보호지침
관련 기관	국정원	국방부	방사청	산자부
등급 분류	4개 등급	3개 등급	2개 등급	2개 등급
등급 명칭	비밀, 대외비, 비공개 업무자료, 공개 업무자료	비밀, 비공개 업무자료, 일반 군사자료	판정기술, 식별기술	국가핵심기술, 산업기술

이에 따라 방산업체는 혼란스러울 수 밖에 없다. 이윤 창출을 목적으로 하는 기업 특성상 성과 없이 비용만 소모 되는 보안업무에 대해 인적·물적 투자를 충분히 할 수 없는 상황에서 정부기관에서 제시하는 기준 및 통제조차도 일관성과 체계성이 결여되어 있기 때문이다. 즉, 방산업체 입장에서는 보유·취급하는 정보의 상대적 중요도를 반영하여 기업 스스로 전략적·효율적인 보안 투자가 절실한 실정이다.

2.2 해외 국가정보 분류체계 검토

2.2.1 미국의 분류체계

미국은 정부기관이 취급하는 국가정보를 ① 기밀 정보(Classified Information), ② 통제 비기밀 정보(CUI: Controlled Unclassified Information), ③ 일반 정보(비기밀 정보: Unclassified Information)의 3가지 유형으로 다음 〈그림 3〉과 같이 분류한다.[11]



〈그림 3〉 미국의 국가정보 분류체계[11]

미국의 기밀 정보는 「대통령 행정명령(Executive Order) 13526, Classified National Security Information」에서 규정하고, 기밀은 아니지만 보호가 필요한 통제 비기밀(CUI)의 관리는 「대통령 행정명령 13556, Controlled Unclassified Information」에서 규정하고 있다. 미국 「대통령 행정명령 13526」에 대응하는 우리나라 법령은 대통령령인 「보안업무규정」이 있으나, 「대통령 행정명령 13556」에 대응하는 우리나라 법령은 없다.[11]

미국은 「대통령 행정명령(E.O) 13526」이행을 위해 「국가비밀에 관한 연방규정(Title 32 of the code of Federal Regulation)」을 제정·운영하고 있으며, 각급 기관은 행정명령과 연방규정에 근거하여 지침과 편람을 제작하여 활용하고 있다.[12]

특히, 국가기밀에 관한 연방규정은 사용 예시까지 포함되어 있을 정도로 구체적이며, 교육자료로 활용할 수 있도록 공개하며, 누구든지 인용할 수 있도록 허용하고 있다. 기밀 분류와 그에 따른 보호 절차에 대해서 전 정부 부처는 물론, 민간 부문과 국민들에게도 공유하여 일치된 인식을 갖도록 하고 있는 것이다.[12]

〈표 2〉 미국 기밀정보의 범주(E.O 13526)

- ① 군사계획, 무기체계 또는 군사작전
- ② 외국 정부 정보
- ③ 정보활동, 정보원이나 방법, 암호
- ④ 기밀정보원을 포함한 미국의 대외관계 또는 대외활동
- ⑤ 국가안보와 관련된 과학적, 기술적 또는 경제적 사항
- ⑥ 핵 물질 또는 핵 시설 보호를 위한 미 정부 프로그램
- ⑦ 국가안보와 관련된 시스템, 시설, 인프라, 프로젝트, 계획, 또는 방호 서비스의 취약성 또는 기능
- ⑧ 대량살상무기(WMD)의 개발, 생산, 또는 사용

이러한 법규에 따라 미국은 관할 부처에 관계 없이 8가지 범주에 해당하는 모든 정보를 통합되고 통일된 체계로 앞의 <표 2>와 같이 기밀정보를 분류한다.

미국 국방부(DoD)에서도 대통령 행정명령에 따라 과학기술 정보(STI: Scientific and Technical Information) 중에서 기밀은 아니지만 보호할 정보를 CUI로 분류하고 있다. DoDI 3200.12에 의하면 미국 국방부(DoD)에서도 다음 <표 3>과 같이 국가정보를 3개 등급으로 분류한다.[11]

<표 3> 미국 국가정보 분류

1. 기밀정보(Classified Information)
• TS(Top Secret, 1급 비밀)
• S(Secret, 2급 비밀)
• C(Confidential, 3급 비밀)
2. CUI(Controlled Unclassified Information, 통제 비기밀 정보)
3. U(Unclassified Information, 비기밀)

위와 같이 미국은 9.11. 테러 이후 대통령 행정명령(E.O 13526 및 E.O 13556)을 중심으로 모든 기관 간에 통일되고 통합된 기밀 보호체계를 운영하고 있으며, 전 정부 부처는 물론 민간 부문 및 국민들에게도 관련 정보를 공유하여 일치된 인식을 갖도록 돕고 있다.[12] 이러한 환경에서는 중요한 정부 정보가 방산업체 등 비정부 부문에서 보유 및 취급되더라도 혼란과 보안 위험을 최소화하면서 관리될 수 있다.

2.2.2 중국의 분류체계

최근 G2 국가로 등장한 중국에서도 기밀의 범주가 「국가기밀보호법」 및 「반간첩법」에 의해 하나의 체계로 통합하여 관리되고 있다.

중국의 위 법률 체계에 의하면, 국가사무·국방(군사)·외교·경제(산업)·과학기술·범죄 등 그 분야를 막론하고 누설 시 국가안보 또는 이익에 해를 끼칠 수 있는 모든 중요한 사안들을 하나의 ‘기밀체계’에 포함하여 ‘① 국가기밀(3개 등급: 絶密, 機密, 秘密三級), ② 국가정보, ③ 국가 안보와 이익에 관한 문건·데이터·자료·물품’으로 분류하여 보호하고 있다.[13, 14]

중국 국가기밀보호법에 의하면 기밀의 범주는 다음 <표 2-4>와 같다.

<표 4> 중국의 기밀 범주(국가기밀보호법 제13조)

- ① 국정에 관한 주요 의사결정에 관한 사항
- ② 국방 건설 및 군대 활동에 관한 사항
- ③ 외교·대외 활동 및 외부 기밀 유지 의무가 적용되는 사항
- ④ 국가 경제 및 사회 발전에 관한 사항
- ⑤ 과학 및 기술 분야에 관한 사항
- ⑥ 국가 안보 활동 및 범죄 수사에 관한 사항
- ⑦ 국가기밀관리 부서에서 결정한 기타 사항

‘국가기밀’은 다음 <표 5>와 같이 법적 절차에 따라 3개의 비밀 등급(絶密, 機密, 秘密三級)으로 확정되고 일정 기간 동안 일정 범위의 인원만 알게 되는 정보를 말한다.[14]

<표 5> 중국 국가정보 분류

1. 국가 기밀(國家機密)
• 絶密(절밀, 1급 비밀)
• 機密(기밀, 2급 비밀)
• 秘密三級(비밀3급, 3급 비밀)
2. 국가정보(國家情報, 대외비)
3. 국가 안보와 이익에 관한 문건·데이터·자료·물품(비공개 정보)
4. 비기밀

‘국가정보’는 최고인민법원 ‘역외를 위한 국가비밀/정보의 절취/정탐/불법 매수/불법 제공 사건에 관한 구체적 법률 적용에 관한 약간의 문제에 관한 해석’ 제1조에 따라 ‘국가안보와 이익에 관련되나 아직 공개되지 않았거나 관련 규정에 따라 공개하면 아니되는 사항’으로 규정되며, 법적 절차에 의한 국가 비밀로 확정되지는 않았지만 국가 안보 및 이익과 관련되는 정보로서 대중에게 비공개되어야 할 정보이다. [14, 15] 또한, ‘국가 안보와 이익에 관한 문건·데이터·자료·물품’은 국가 비밀로 지정되거나 국가정보로 관리되지 않는 일반 정보이나, 누설 시 국가 안보나 이익에 해를 끼칠 수 있어 유출을 경계할 필요가 있는 정보를 말한다. [13, 16]

이처럼 중국에서도 그 분야나 관할 부처와 관계없이 국가 안보나 이익과 관련된 중요한 사안들을 통합되고 통일된 체계로 분류하고 있음을 알 수 있다.

이를 통해서 각종 정보가 어떤 내용이든, 어떤 부처의 업무에 속하든 관계없이 그 상대적 중요도를 알 수 있으며, 각각 어떻게 관리해야 하는지를 알 수 있어 효율적이고 체계적인 보호가 가능하다. 또한, 다수 부처의 정보가

존재하거나, 정보가 인수인계 또는 이동되더라도 해당 정보의 기밀 등급을 명확하게 알 수 있어 수평적 보호가 보장됨에 따라 보안 누수의 취약점도 예방할 수 있다.

2.2.3 시사점

방산업체가 정보 관리에 혼란을 겪고 있고, 방산업체가 보유하거나 취급하는 민감한 정부 정보들에 대한 효과적인 보호가 제한되는 실정인 만큼 해당 정보들을 통합되고 일치된 기준으로 분류할 필요가 있을 것이다. 그리고 좀 더 확장하여 국가적 관점에서 봤을 때도, 군사기밀이든, 군사상 기밀이든, 외교상 기밀이든, 산업기술이든, 방산기술이든 국가 안보와 국익을 위해 보호하고자 하는 모든 중요한 정보들은 업무 소관 부처가 다를 뿐, 결국 ‘국가기밀’에 속한다고 볼 수 있을 것이다.

사실 우리나라도 그 법규나 체계 면에서는 이미 미국이나 중국과 같은 기반을 갖추고 있기 때문에 통일된 ‘국가기밀 분류체계’를 마련하는 것이 다음과 같은 이유로 인해 요원한 일만은 아닐 것이라 판단된다.

(1) 법규 체계면에서는 우리나라에도 통합된 국가기밀 분류체계가 시행될 수 있는 기반이 이미 마련되어 있다.

우리나라는 「국가정보원법」(법률), 「보안업무규정」(대통령령), 「보안업무규정 시행규칙」(훈령) 및 부처별 행정규칙(「국방보안업무훈령」, 「방산보안업무훈령」등)의 체계로 국가기밀 분류를 하고 있으며, 이는 미국의 법규 체계와 크게 다르지 않다.

〈표 6〉 국가기밀보호 관련 법령체계 비교

우리나라	미 국	중 국
국가정보원법 (법률)	국가비밀보호령 (대통령 행정명령)	국가기밀보호법
보안업무규정 (대통령령)	국가비밀보호규정 (연방규정)	보안규정 (각 기관 행정법규)
보안업무훈령 (각 기관 행정규칙)	정보보안지침 (각 기관 규정)	

심지어 중국의 경우는 법규 면에서 오히려 우리나라보

다 그 체계성이 떨어진다. 국가별 기밀보호 법령체계는 앞의 〈표 6〉과 같다.

다만, 미국 연방 규정 대비 우리나라 「보안업무규정」의 구체성이 떨어지고, 기밀을 규정하고 있는 각종 특별법 및 각 기관 행정규칙이 다수 존재함에도 해당 법규 조항에 「보안업무규정」과의 연계성을 규정짓고 있지 않음에 따라 실제로는 부처별로 상이한 기밀 분류가 적용되고 있는 실정이다.

그러나, 특별법을 제외한 「국방보안업무훈령」이나 「방산보안업무훈령」은 현재 법규 체계를 고려하여도 국가 기밀체계의 분류를 따르지 않을 이유가 없는 만큼 적어도 국방기밀 분류체계와 방산기밀 분류체계 만큼은 국가기밀 분류체계를 그대로 인용하여 일치시킬 필요가 있을 것이다.

(2) 내용 면에서도 미국과 중국의 기밀 범주에 비추어 보면, 우리나라의 기밀들도 하나의 분류체계로 통합하지 못할 이유가 없다.

우리나라에서는 수 개의 법으로 분산하여 규정하고 있는, 국가기밀, 군사기밀, 군사상 기밀, 외교상 기밀, 산업기술 및 방산기술 중 어떤 것도 국가 안보와 국가 이익이라는 목적에 벗어나는 것은 없으며, 이에 따라 미국의 8개 기밀 범주나 중국의 7개 기밀 범주에서 벗어나는 내용은 없다.

결국 내용 면에서도 미국이나 중국과 같이 국가기밀 분류체계라는 하나의 분류체계로 각종 기밀들을 통합하지 못할 이유가 없는 것이다.

(3) 기밀 등급 분류 면에서도 국가기밀 보호체계의 등급 분류가 다른 기밀들을 수용하지 못할 이유가 없다.

우리 국가기밀 분류체계에서 기밀을 ‘비밀(I·II·III급), 대외비, 비공개 업무자료, 공개 업무자료’의 등급으로 분류하고 있는 것은 미국 및 중국의 기밀 등급 분류와 크게 다르지 않으며, 부처별로 분산된 기밀 분류 등급을 포괄하는 데도 무리가 없다.

군사기밀·방산기밀·방산기술·산업기술로 보호되는 정보들 중 ‘비밀’, ‘비밀은 아니지만 일반에 공개할 수 없고 특별한 보호가 필요한 정보’, ‘일반에 공개할 수 없는 정보’,

‘일반에 공개할 수 있는 정보’라는 4가지 분류의 카테고리를 벗어나는 정보가 존재하지는 어렵기 때문이다.

또한, 기밀 각각의 상대적 중요도를 규정하거나 설명하는 정보분류 가이드가 존재하지는 않지만, 그동안 행정 실무 및 형량 판단 시에 기밀 각각의 상대적 중요도를 내재적으로 판단해 왔기 때문에 이러한 행정적·법적 관념을 활용하면 등급 분류를 일치화하는 것이 어려운 문제만은 아닐 것이다.

〈표 7〉 국가기밀 분류체계 비교

구분	우리나라	미국	중국
법규체계	3단 체계	3단 체계	2단 체계
내용범주	• 국가 안보 및 국익과 관련한 사안에 대해 미범주화	8개 범주화	7개 범주화
등급분류	4개 등급	3개 등급	4개 등급

이에 따라 각 부처의 행정규칙을 국가기밀 보호체계에 적합하도록 정비하거나, 특별법 상 「보안업무규정」과의 연계성을 규정짓는 조항을 추가한다면, 낯선 외국 제도를 도입하거나 신규로 통합 분류체계를 설계하는 소요 없이 기존의 ‘국가기밀 분류체계’를 활용하여 우리나라 기밀도 통합되고 일치된 분류로 체계화할 수 있을 것이다. 이렇게 된다면, 방산업체에 산재하는 다양한 종류의 기밀정보들도 상대적 중요도가 명확해지고, 등급에 따른 합리적인 보호 및 관리가 가능할 것이다.

2.3 기존 연구 검토

방산업체가 보유하고 있는 다양한 정보를 체계적으로 분류하려고 시도한 기존 연구는 많지 않으나, 일부 존재한다.

허아라(2018)는 우리나라와 미국의 국방과학기술 정보 분류체계를 비교하고, 관련 법령 및 예규를 검토하여 국방과학기술 정보를 미국의 국가정보 분류체계를 기준으로 ‘비밀정보(I·II·III급 비밀), 통제기술정보(방산업체 및 국방기관 외부에 공개되면 안되는 정보), 일반정보’의 3개 등급으로 분류할 것을 제안하였다.[11]

이상열(2025)은 방산업체 기술보호 관계관 36명을 대상으로 몰 인터셉트 면접법(mall intercept interview)을 활용하여 방산업체 데이터 보유 현황을 확인하고, 데이터별 중요도에 따라 점수를 부여해 한 후 평균값을 산출하여

상대적 우선순위를 판단하였으며, ‘방산관련 비밀’을 우선 보호해야 한다는 결론을 도출하였다.[1]

기존 연구는 방산업체 보유 정보 분류를 위해 선진국의 분류체계를 도입하는 방안을 제시하거나 방산업체가 보유한 다양한 정보 간의 상대적 중요도를 판단하였으며, 그 방법론으로는 관련 법령 및 예규를 검토하는 방법과 방산업체 관계관의 의견을 수집하여 통계 분석하는 방법을 활용하였다.

다만, 기존 연구는 방산업체가 취급 및 보유하고 있는 정보 전반에 대한 위계 및 체계를 개관하지 못하고, 방산업체가 보유한 각각의 정보를 실무에서 실제 분류하는 데 활용하기에는 구체성이 부족한 측면이 있다.

2.4 연구 방향 및 방법

본 연구의 목적은 방산업체가 보유·취급하고 있는 정보를 통합된 체계로 분류할 수 있는 방안을 제시하는 데 있다. 이를 위해 선행적으로 국내 및 해외 국가정보 분류체계와 기존 연구를 검토했으며, 이를 기초로 연구 방향 및 방법을 설정했다.

첫째로, 방산업체 보유·취급 정보 전반에 대한 위계를 먼저 제시함으로써, 방산업체 보유·취급 정보를 파편적이기보다 개관적·통합적 시각으로 바라볼 수 있도록 하였다. 전반적 위계를 제시함에 있어서는 방산업체가 민간 기업이므로 정보보호에 있어 경제성을 고려하지 않을 수 없다는 점과 데이터 중심으로 보안 패러다임이 변화하고 있는 현실을 반영하여, 서승우(2008)가 보안의 경제성을 고려하여 제시한 기업정보 분류 기준과 국정원(2025)이 국가 망 데이터 보호 및 관리를 위해 제시한 C/S/O 구분을 활용하였다.

둘째로, 기존 ‘국가기밀 분류체계’를 기준으로 방산업체 보유·취급 정보를 통합 분류하는 방안을 제시했다. 국내 및 해외 국가정보 분류체계 검토를 통해 우리나라에는 이미 ‘국가기밀 분류체계’라는 방산업체 보유·취급 정보에 적용되는 다수 기밀분류체계를 수용할 수 있는 기준이 존재하며, 이 기준이 통합을 위한 법규 및 등급 체계를 갖추고 있다는 점을 파악했다. 이에 따라 본 연구에서는 해외 제도를 도입하거나 통합 분류체계를 신규로 설계하여 부작용 및 행정 낭비를 유발하기보다 상이한 기밀분류체계의 각 등급이 ‘국가기밀 분류체계’에서는 어느 등급 수준에 해

당하는지 규명하여 기존 ‘국가기밀 분류체계’를 기준으로 방산업체 보유·취급 정보를 통합 분류할 수 있는 방안을 제시했다.

셋째로, 연구 방법으로는 관련 법령 및 규정 등을 심도 있게 분석하여 방산업체 보유·취급 정보 각각의 상대적 중요도가 어떠하며, ‘국가기밀 분류체계’에 있어서는 어느 등급 수준에 해당하는지를 논리적 근거를 가지고 제시하는 방법을 주로 활용하였다. 방산업체가 보유·취급하고 있는 정보의 보호 및 관리에 대해서는 법적·행정적 통제가 적용되고 있으며, 보호 절차를 위반하거나 기밀이 유출되었을 때의 벌칙도 규정되어 있다. 이러한 상황에서 방산업체 실무에 활용할 수 있는 실용적인 분류 방안을 제시하기 위해서는 그 분류의 근거를 법령 및 규정에 둘 필요가 있다. 그 래야만 방산업체에서 연구 결과를 활용하여 전략적·효율적 보안 관리를 하더라도 민감한 정부 정보를 법규에 어긋나 지 않게 보호할 수 있는 안전성이 제공되기 때문이다.

Ⅲ. 정보 위계 및 통합 분류 방안

3.1 방산업체 보유 정보의 위계

3.1.1 방산업체에서 보호해야 할 정보

서승우(2008)는 기업의 정보는 정보의 가치나 공개 가능 여부에 따라 분류할 수 있으며, 이 두 가지 기준을 동시에 적용하여 업체 스스로 보호해야 하는 정보를 가릴 수 있다고 하였다.[17]

다음 <표 8>의 정보특성에 따른 기업정보 분류에서와 같이 1·2·3 영역에 해당하는 정보는 정보의 가치에 관계 없이 반드시 공개되어야 하고, 1·4·7 영역에 해당하는 정보는 공개 여부와 관계없이 정보 가치가 낮아 보호할 필요가 없고, 5·6·8·9 영역에 해당하는 정보는 적절한 대책을 세워 기업에 이익이 되는 방향으로 보호해야 한다.[17]

<표 8> 정보특성에 따른 기업정보 분류[17]

정보가치 공개가능	정보가치		
	낮은수준	중간수준	높은수준
공개된 정보	1	2	3
공개 가능한 정보 (공개 여부 판단 후)	4	5	6
공개 가능하지 않은 정보	7	8	9

이와 같은 기준은 방산업체에서 보유하고 있는 정보에 대해서도 적용할 수 있다. 방산업체가 보유하고 있는 정보에는 다음 <표 9>와 같이 민수 관련 일반자료, 방산 관련 일반자료, 민수 관련 주요자료, 방산 관련 주요자료, 영업비밀, 산업기술(국가핵심기술 미포함), 방산기술, 방산 관련 기밀(비밀, 대외비) 등이 있다.

방산업체가 보유한 정보의 가치를 판단하자면, 공익적 가치를 지니지 않는 영업비밀보다 공익적 가치와 기업 사적 가치를 모두 지니는 산업기술, 방산기술, 방산관련 기밀의 가치를 더 높게 볼 수 있다. 또한, 공개 가능성 면에서는 방산기술 및 산업기술은 관련 법규에 따라 보안성 검토를 거쳐 공개할 수 있지만, 방산 관련 기밀은 관련 법규상 기밀에서 해제되지 않는 한 공개할 수 없다는 점에서 공개 가능성 수준이 다르다.[18, 19, 20, 21]

결론적으로 방산업체의 입장에서 보호할 필요가 있는 정보는 방산 관련 주요자료, 민수 관련 주요자료, 영업비밀, 산업기술, 방산기술, 방산 관련 기밀로 볼 수 있다. 역으로 민수 관련 일반자료와 방산 관련 일반자료는 방산업체 입장에서 보호할 필요가 없는 정보로 판단할 수 있다.

<표 9> 정보특성에 따른 방산업체 보유 정보 분류

정보가치 공개가능	정보가치		
	낮은수준	중간수준	높은수준
공개된 정보	• 민수 관련 일반자료		
공개 가능한 정보 (공개 여부 판단 후)	• 방산 관련 일반자료	• 방산 관련 주요자료	• 산업기술(국가핵심기술 미포함)
		• 민수 관련 주요자료	• 방산기술
공개 가능하지 않은 정보	• 영업 비밀 • 방산 관련 기밀 (비밀, 대외비)		

3.1.2 국가가 보호를 강제해야 할 정보

방산업체는 비정부 부문에 해당하나, 연구개발 및 제조 등 국방획득사업 계약에 의해 국방 전략, 무기체계 역량 및 기능, 국방과학기술, 국방계약 사항 등 민감한 정부 정보도 보유 및 취급하게 된다. 또한, 방산업체의 88%는 방산과 민수 양쪽 부문 사업을 모두 시행하고 있으며, 방산업체가 아닌 협력업체들과 하도급 관계를 맺고 방산 사업을 함께 추진하고 있다.[22]

이러한 특성들에 의해 민감한 정부 정보들이 아래와 같은 이유로 위험한 상황에 노출될 수 있다.

첫째, 이윤 창출을 목적으로 하는 방산업체가 본인 소유도 아닌 정보를 보호하기 위해 막대한 비용을 감당하면서 군이나 정부 수준의 보안체계를 갖추기는 어렵고, 둘째, 민간 부문의 정보와 혼합되어 관리될 수 있는데 이 경우 정보 유출 가능성이 현저히 높아질 수 있으며, 셋째, 하도급 계약에 의해 기본적 보안 수준도 검증되지 않은 협력업체로 민감한 정부 정보가 유입될 수 있다.

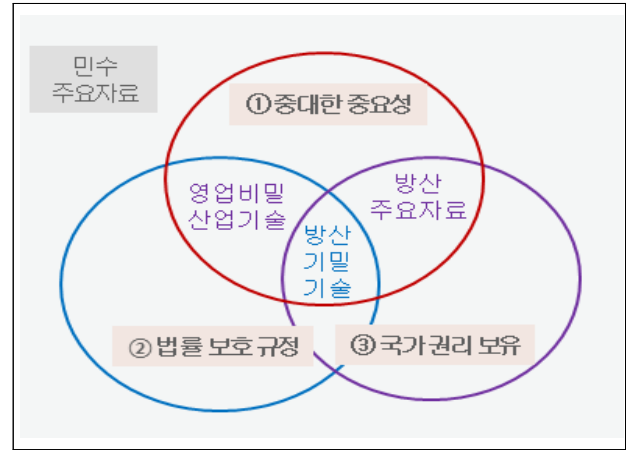
이러한 위험성 때문에 국가는 방산업체에 대해 정보 보호를 강제할 수 밖에 없다. 반면, 방산업체가 계약에 의해 특수한 관계 놓여 있기는 하지만 엄연히 비정부 부문에 속하고, ‘국가가 정보 보호를 강제한다는 것’은 국가가 방산업체의 정보관리에 개입하고 보호 대상 정보를 보호하지 못했을 때는 형벌 또는 행정벌 등 벌칙을 부과한다는 것을 내포하고 있기 때문에 민간 법인에 대한 기본권 제한에 해당한다.

이에 따라 정부가 방산업체를 대상으로 보호를 강제해야 하는 정보의 범위는 엄격하게 제한하여 최소한으로 판단해야 할 것이다.

우리 헌법에서는 기본권 제한 요건에 대해 ‘국가안전 보장, 질서 유지 또는 공공복리를 위해 필요한 경우에 한하여 법률로써 제한할 수 있으며, 제한하는 경우에도 자유와 권리의 본질적인 내용을 침해할 수 없다.’고 규정하고 있다.[23]

이에 따라 국가가 보호를 강제할 수 있는 정보는 ① 정보유출 시 국가안전 보장·질서 유지·공공복리에 악영향을 미치는 중대한 중요성이 있어야 하고, ② 법률로써 보호가 규정된 정보여야 할 것이다. 또한, 계약 관계 관점에서는

③ 국가에 소유권이 있거나 국가가 원본 출처임에 따라 국가가 권리를 주장할 수 있는 정보여야 할 것이다.



〈그림 4〉 국가의 정보보호 강제가 가능한 조건

이러한 조건들을 벤다이어그램으로 정리한 내용은 앞의 〈그림 4〉와 같으며, 세 가지 조건을 모두 만족하는 정보는 방산 관련 기밀과 방산기술이라고 할 수 있다.

방산 관련 기밀은 ① 관련 법규에 의해 정보유출 시 국가 안전보장에 악영향을 미치는 중대한 중요성이 규정되어 있으며, ② 법률(국정원법 및 군사기밀보호법)로써 보호가 규정되어 있고, ③ 국가에서 생산한 것이거나 국가에서 생산한 원본의 내용 전체 또는 일부를 포함하여 방산업체에서 재생산한 것이기 때문에 국가에 권리가 있다고 할 수 있다.[24, 25, 26, 27, 28, 29, 30]

또한, 방산기술도 ① 관련 법규에 의해 국가안보 등을 위해 보호되어야 하는 것으로 규정되어 있으며, ② 법률(방위산업기술보호법)로써 보호가 규정되어 있고, ③ 「국방과학기술혁신촉진법」에 의해 원칙적으로 그 소유권이 국가에 있다.[31, 32]

반면, 방산업체에서 보호해야 할 정보 중에서도 방산 관련 기밀과 방산기술을 제외한 정보들은 국가가 정보보호 강제가 가능한 조건 전부 또는 일부를 만족하지 않는다.

첫 번째로, 민수 관련 주요 자료는 정보보호 강제가 가능한 조건 3가지 중 어느 하나도 만족하지 않는다. 헌법에 규정된 중대한 중요성을 가지지 않고, 이에 따라 법률로써 그 보호에 대해 규정하고 있지 않으며, 국가 업무와는 관계없는 순수 민간 정보이기 때문이다.

두 번째로, ‘영업비밀 및 산업기술’은 ‘③ 국가가 권리를 보유해야 한다’는 조건이 결여되어 있다. ‘영업비밀’은 국가의 관여 없이 생산되는 정보로, 해당 업체 외부에는 알려져 있지 않고 독립적인 경제적 가치를 지니는 정보이기 때문에 국가가 권리를 가지지 않는다.[33] 또한, ‘산업기술’은 「산업기술혁신촉진법」에 의해 원칙적으로 주관연구기관(방산업체)이 소유권을 가지기 때문에 방산업체가 그 소유권을 가진다.[34]

세 번째로, ‘방산관련 주요자료’는 그 정의 및 보호가 법률이 아닌 국방부 행정규칙(방산보안업무훈령)에 규정되어 있기 때문에 ‘② 법률로써 보호가 규정되어야 한다’는 조건을 결여하고 있다.[8]

따라서 국가가 방산업체 대상 보호를 강제할 수 있는 정보는 방산 관련 기밀과 방산 기술 2가지라고 할 수 있으며, 이러한 강제력은 형사처벌 및 행정처벌(과태료)의 형태로 발현되고 있다.[35, 36]

3.1.3 중간적 중요도를 지닌 정보

3.1.1 및 3.1.2를 통해 방산업체 보유 정보 중 보호할 필요가 없는 낮은 중요도를 가진 정보(민수 관련 일반자료, 방산 관련 일반자료)와 국가가 보호를 강제해야 할 정도로 특별히 높은 중요도를 가진 정보(방산 관련 기밀, 방산기술)를 파악했다.

반면, 방산업체가 보유하고 있는 정보의 위계를 파악하기 위해서는 그 외 방산업체에서 보호할 필요는 있지만, 국가가 보호를 강제할 필요는 없는 중간적 중요도를 지니는 정보(민수 관련 주요자료, 방산 관련 주요자료, 영업비밀, 산업기술)에 대한 우선순위 판단도 필요할 것이다.

첫째, ‘민수 관련 주요자료’는 중간적 중요도를 지니는 정보 중에서는 그 중요도가 가장 낮다. ‘민수 관련 주요자료’는 헌법에 규정된 중대한 중요성을 보유하지 않으며, 나머지 정보들은 공통적으로 이러한 중요성을 보유하고 있기 때문이다. 관련 법규에 따라 ‘영업비밀’은 ‘건전한 거래 질서’라는 질서 유지 및 공공복리 차원에서의 중요성을, 산업기술은 ‘국내산업의 경쟁력 강화, 국가의 안전보장, 국민경제의 발전’이라는 국가 안전보장 및 공공복리 차원에서의 중요성을, 방산 관련 주요자료는 ‘유출 시 방산 보안에 유

해하거나, 방위산업에 악영향을 미치는’ 국가 안전보장 및 공공복리 차원에서의 중요성을 보유하고 있다.[8, 33, 37]

둘째, ‘산업기술 및 영업비밀’과 ‘방산 관련 주요자료’ 중에서는 ‘산업기술 및 영업비밀’의 중요도가 더 높다. 국가는 중요도가 더 높은 정보에 더 강한 개입을 하기 마련인데, ‘산업기술 및 영업비밀’에 대한 국가 개입 수준이 더 높기 때문이다. ‘산업기술 및 영업비밀’에 대한 개입은 법률에 의해 형사 및 행정 처벌과 손해배상의 형태로 나타나고, ‘방산 관련 주요자료’에 대한 개입은 행정규칙에 의해 권고나 시정 요구의 형태로 나타난다.[38, 39, 40] 또한, ‘산업기술 및 영업비밀’에 대한 국가 개입은 그 권원이 ‘법률’에 있는 데 반해, ‘방산 관련 주요자료’는 ‘권리’에 있다는 점도 이를 뒷받침한다.

즉, ‘산업기술 및 영업비밀’은 방산업체가 권리를 가지고 있긴 하지만 중대한 중요성이 있기 때문에 법률이 국가로 하여금 개입을 통해 보호에 도움을 주도록 하고 있는 것이며, ‘방산 관련 주요자료’는 ‘산업기술 및 영업비밀’에 비해 중요도가 상대적으로 낮지만 국가가 ‘권리’를 가지고 있기 때문에 이를 근거로 관리에 개입하고 있는 것이다.

따라서 방산업체 보유 정보 중 중간적 중요도를 지니는 정보에 대해서는 ‘산업기술 및 영업비밀’ > 방산 관련 주요자료 > 민수 관련 주요자료’ 순으로 우선순위를 판단할 수 있다.

3.1.4 방산업체 보유정보 위계 판단(C/S/O)

국가정보원에서는 2025. 1.24. ‘국가망 보안체계 보안 가이드라인(이하 ‘가이드라인’)을 발표하였다. 이에 따르면 앞으로 국가·공공기관의 업무정보와 정보시스템 내 정보는 기밀(Classified), 민감(Sensitive), 공개(Open)의 3개 등급으로 분류해야 하며, 이러한 등급 분류는 「보안업무규정」등 관련 법령의 근거에 따라 이뤄져야 한다.[5]

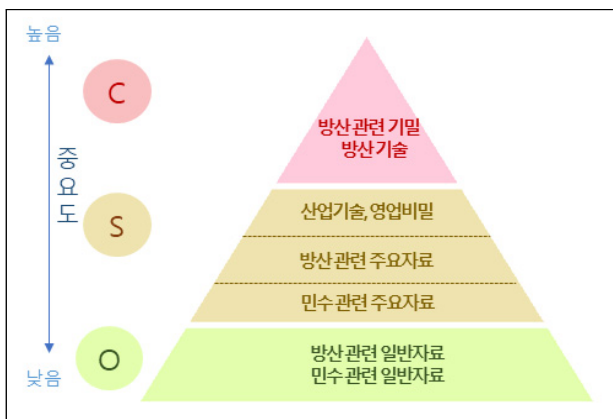
방산업체는 ‘국가·공공기관’에 해당하지는 않지만, ‘국가·공공기관’의 정보도 취급 및 보유하고 있기 때문에 국가 망 보안체계와 연관될 수 밖에 없다. 이에 따라 방산업체 보유정보의 위계를 판단함에 있어서 해당 가이드라인을 고려하지 않을 수 없는 것이다.

가이드라인에 따르면, 기밀정보(C)는 비밀, 안보·국방·

외교·수사 등의 기밀정보와 국민 생활·생명·안전과 직결된 정보로서 정보공개법 제9조 제1호부터 제4호까지를 포함한다. 민감정보(S)는 비공개 정보 등 개인·국가 이익 침해가 가능한 정보로서 정보공개법 제9조 제5호부터 제8호까지의 정보 및 로그, 임시백업 등의 기타 정보를 포함한다. 공개정보(O)는 기밀정보(C) 및 민감정보(S) 이외의 모든 정보를 포함하며, 관련 법령 등에서 규정하는 요건을 조치한 비공개 정보와 기간의 경과 등으로 비공개 필요성이 소멸된 정보를 포함한다.[5]

앞서 방산업체 보유정보 간 상대적 중요도를 판단함에 있어 관련 법령을 주로 그 근거로 해왔기 때문에 가이드라인의 취지에 부합하며, 가이드라인 상 기밀정보(C)에는 국가가 보호를 강제해야 할 정도로 특별히 높은 중요도를 가진 정보(방산 관련 기밀, 방산기술)가, 민감정보(S)에는 방산업체에서 보호할 필요는 있지만 국가가 보호를 강제할 필요는 없는 중간적 중요도를 지니는 정보(산업기술, 영업비밀, 방산 관련 주요자료, 민수 관련 주요자료)가, 공개정보(O)에는 보호할 필요가 없는 낮은 중요도를 가진 정보(방산 관련 일반자료, 민수 관련 일반자료)가 그 의미 면에서 잘 호응함을 알 수 있다.

이러한 개념으로 방산업체가 보유한 정보의 위계를 가이드라인 상 C/S/O 구분을 적용하여 표현하면, 다음 <그림 5>와 같다.



〈그림 5〉 방산업체 보유정보의 위계

이를 활용하면 향후 국가망 보안체계 개편에 대응할 수 있을 뿐 아니라, C에 대해서는 비밀망, S에 대해서는 보안

망, O에 대해서는 일반망을 적용하거나, C에 대해서는 물리적 망 분리, S에 대해서는 논리적 망 분리, O에 대해서는 망 분리를 미적용하는 등 데이터 관련 보안 통제를 차등화하는 데에도 활용할 수 있을 것이다.

3.2 국가기밀 보호체계 해당 등급 분석

앞서 C/S/O(데이터 분류) 관점에서 방산업체 보유 정보의 위계를 판단해 보았지만, 국가기밀 분류체계를 적용하여 방산업체 보유 정보를 분류하기 위해서는 다른 분류체계가 적용되고 있는 각각의 정보가 국가기밀 분류체계의 ‘비밀-대외비-비공개 업무자료-공개 업무자료’ 등급 중 어떤 등급에 해당하는지 따져 보아야 한다.

먼저, 방산업체 입장에서 보호할 필요가 없는 정보이며, C/S/O 위계에서 O(공개정보) 등급으로 판단된 방산 관련 일반자료와 민수 관련 일반자료는 공개 업무자료 등급으로 쉽게 판단할 수 있다. 또한, 일반에 공개할 수는 없지만, 법률로써 보호가 규정되어 있지 않은 방산 관련 주요자료와 민수 관련 주요자료는 비공개 업무자료 등급으로 판단할 수 있을 것이다.

반면, 방산 관련 기밀과 방산기술, 산업기술과 영업비밀의 등급을 판단하는 것은 비교적 쉽지 않으며, 여러 법적·행정적 고려가 필요하다. 이에 따라 방산 관련 기밀과 방산기술 및 산업기술과 영업비밀이 어떤 등급에 해당하는지 관련 법령 및 규정 등을 세부적으로 검토하여 판단해 보고자 한다.

3.2.1 방산 관련 기밀과 방산기술의 등급

방산 관련 기밀은 관련 법령에 의해 ‘비밀(군사 및 국가 II·III급)·국가 대외비·군사 비공개 업무자료’를 포함하는 것으로 판단할 수 있으며, 이는 방산과 관련된다면 군사기밀 뿐 아니라 기타 정부 부문의 국가기밀도 포함함을 의미한다. [6, 7, 8]

이에 따라 방산 관련 기밀이 가지는 중요도를 판단함에 있어서는 군사기밀 분류체계에서는 대외비 등급이 폐지되었으나, 국가기밀 분류체계에는 대외비 등급이 여전히 남아 있다는 점을 고려해야 한다. 이러한 상황에서는 군사기

밀 분류체계에 있어서의 비공개 업무자료와 국가기밀 분류 체계에 있어서의 비공개 업무자료의 의미가 다를 수 밖에 없기 때문이다.

군사기밀 분류체계에 있어서 비공개 업무자료는 기존 ‘군사 대외비’를 대체하는 개념이고, 국가기밀 분류체계에 있어서의 비공개 업무 자료는 「국가정보보안기본지침」에 의해 비밀 및 대외비를 제외한 업무자료로 정의된다.[6, 7, 8]

군사 분야에서는 업무자료가 기본적으로 일반에 비공개 되고 이례적으로 공개되기 때문에 ‘공개 정보’라고 별도로 지정된 정보 외 모든 정보는 일반에 공개하면 안된다는 것을 소속원들이 기본적으로 인지하고 있고, ‘대외비’라고 표현하지 않고 ‘비공개 업무자료’라고만 별도로 지정하여도 일반에 비공개하는 것을 넘어 특별한 보호가 필요한 정보라고 인식할 수 있다. 이는 「국방보안업무훈령」에서 일반 군사자료도 ‘임의로 공개할 수 없으며 별도의 절차를 거쳐야 함’을 규정하고 있는 것으로써 설명된다.[41]

반면, 기타 정부 부문에서는 업무자료가 기본적으로 일반에 공개되고 이례적으로 비공개되기 때문에 ‘대외비’ 등급을 폐지하고 ‘비공개’의 취지만 표시할 경우 소속원들이 일반에 비공개하는 외 특별한 보호가 필요한 정보라고 인식하기 어렵다. 이러한 이유로 군사 분야에서는 ‘대외비’ 등급을 폐지할 수 있었고, 기타 정부 부문에서는 실행할 수 없었던 것으로 판단된다.

따라서, 방산업체에 존재하는 군사 비공개 업무자료는 국가기밀 분류체계의 ‘대외비’ 등급에 해당한다고 볼 수 있으며, 방산 관련 기밀의 국가기밀 분류체계를 기준으로 한 실제 중요도는 비밀과 대외비 등급에 해당한다고 볼 수 있다.

방산기술은 「방위산업기술보호법」 제2조 제1호에 따라 ‘방위산업과 관련한 국방과학기술 중 국가안보 등을 위하여 보호되어야 하는 기술로서 방위사업청장이 지정하고 고시한 것’으로 정의된다. 이를 통해 모든 방산기술은 국방과학기술에 속하고, 국방과학기술 중에서 상대적 중요도가 높은 정보를 별도로 분류한 것이라는 점을 알 수 있다. 이에 따라, 국방과학기술의 중요도를 알 수 있다면, 방산기술의 중요도도 판단할 수 있을 것이다.

방산기술의 상위 개념인 국방과학기술은 「국방과학기술 혁신촉진법」 제2조 제2호에 따라 ‘군사적 목적으로 활용하기 위한 군수품의 개발·제조·가동·개량·개조·시험·측정 등에 필요한 과학기술’로 정의되며, 국방과학기술의 기밀

성 수준에 대해 명시적으로 규정한 법규는 존재하지 않지만, 방위사업청 예규인 「국방과학기술 정보관리 업무지침」에 의해 그 중요도를 유추할 수 있다.

해당 지침은 비밀/대외비로 분류되지 않은 기술정보와 연구개발 보고서에 대한 보호·관리 등급 분류에 대해서 규정하고 있다. 여기서 주목할 점은 해당 지침이 국방과학기술 정보관리에 대해 규정하면서, ‘비밀/대외비로 분류되지 않은 정보’에 대해서만 등급을 분류하여 보호하겠다는 취지를 밝히고 있다는 점이다.[42]

이는 국방과학기술 중에도 비밀이나 대외비로 분류되는 것이 있으나, 이러한 정보는 기밀보호체계로 보호하고 나머지 정보에 대해서만 국방과학기술보호체계로 보호하겠다는 의미이며, 동시에 군사기밀 분류체계에서의 ‘비공개 업무자료’(국가기밀 분류체계의 대외비의 중요도 가집)에 해당하는 자료는 여전히 국방과학기술보호체계로 보호하겠다는 의미라고 볼 수 있다.

이에 따라 국방과학기술보호체계로 보호되는 순수한 국방과학기술은 국가기밀 분류체계를 기준으로 대외비(군사기밀 분류체계에서의 비공개 업무자료)·비공개 업무자료·공개 업무자료 등급에 해당한다고 볼 수 있다.

모든 방산기술은 국방과학기술에 속함에 따라 방산기술의 등급 후보군도 대외비(군사기밀 분류체계에서의 비공개 업무자료)·비공개 업무자료·공개 업무자료 등급으로 좁힐 수 있다. 이는 「국방보안업무훈령」 및 「방산보안업무훈령」에서의 보안성 검토는 비밀 내용이 없거나 제거된 정보에 한해서만 공개를 허용하는 개념인데 반해, 「방산기술보호지침」에서의 보안성 검토는 부서장 사전 검토, 기술보호 부서 확인 및 기술보호총괄책임자 승인으로 방산기술을 공개하는 개념으로 규정되어 있는 것으로써 뒷받침된다. [18, 19, 20] 이러한 규정은 방산기술이 비밀과 같이 공개가 금지된 정보는 아님을 의미하기 때문이다.

또한, 방산기술은 비밀은 아니지만, 국방과학기술 중에서 상대적으로 중요도가 높은 정보이며, 그 유출에 대해 형벌 및 행정벌을 규정하고 있음에 따라 일반에 공개되는 ‘공개 업무자료’ 등급은 그 후보군에서 제외되어야 함을 알 수 있다.[31, 36] 즉, 국가기밀 분류체계를 기준으로 한 방산기술의 중요도는 ‘대외비(군사기밀 분류체계에서의 비공개 정보) 및 비공개 업무자료’ 등급으로 다시 한번 좁힐 수 있는 것이다.

방산기술은 「방산기술보호법」에 의해 대상기관(방산업체)에서 자체 식별한 것과 식별 후 방사청에 의뢰하여 방산기술에 해당한다고 판정받은 것 즉, '식별기술'과 '판정기술'로 분류할 수 있다.[9] 이중 방산업체가 자체 식별한 '식별기술'에 대해서는 방산기술 고시 목록 외 정부 차원에서 제시한 별도의 공식적 식별 기준이 없고, 방산기술 해당 여부에 대한 판단을 전적으로 대상기관(방산업체)에 맡기고 있는 실정이므로 객관성을 확보하기 어렵다. 이에 따라 식별 기술이 일반에 공개하지 말아야 할 정보인 것은 맞지만, 특별한 보호가 필요한지 여부에 대해서는 확인하기 어렵다.

이에 반해 '판정기술'은 주무 통제기관인 방사청으로부터 '국가안보 등을 위하여 보호되어야 하는 기술'임을 확인 받은 정보로, 일반에 공개하지 않아야 함은 물론 특별한 보호가 필요한 정보임을 확신할 수 있다.[9]

따라서, 방산기술 중 '식별기술'의 중요도는 국가기밀 분류체계를 기준으로 일반에 비공개되어야 하는 '비공개 업무자료' 등급에, '판정 기술'은 일반에 비공개되어야 함은 물론, 특별한 보호가 필요한 '대외비' 등급에 해당한다고 판단할 수 있을 것이다.

앞서 살펴봤듯이 방산 관련 기밀의 국가기밀 분류체계를 기준으로 한 중요도는 비밀과 대외비 등급에 해당하고, 방산기술의 중요도는 대외비와 비공개 업무자료 등급에 해당하기 때문에 전체적으로는 방산 관련 기밀의 중요도가 방산기술의 중요도보다 높다고 볼 수 있다. 다만, 부분적으로는 방산 관련 기밀 중 대외비 및 군사 비공개 업무자료가 방산기술 중 판정기술과는 동등한 중요도를 지닐 수 있다.

3.2.2 산업기술과 영업비밀의 등급

산업기술과 영업비밀은 국가기밀 보호 관련 법령체계를 따르지 않고 특별법으로 보호되기 때문에 국가기밀 분류체계에 따른 등급 판단이 더욱 어렵다. 다만, 산업기술과 영업비밀 모두 그 유출에 대해 형벌 및 행정벌이 규정되어 있기 때문에 '공개 업무자료' 등급에 해당한다고 볼 수 없으며, 비밀 지정과 관리를 적용하지 않기 때문에 '비밀' 등급에 해당한다고 볼 수도 없다.[38, 39] 이에 따라 산업기술과 영업비밀의 국가기밀 분류체계를 기준으로 한 등급 후보군은 대외비 또는 비공개 업무자료 등급으로 좁힐 수 있다.

먼저, 국가핵심기술을 제외한 산업기술에 대해서는 법률

상 정의에 '산업경쟁력 제고나 유출 방지 등을 위하여' 정도로만 규정되어 그 중요도가 대외비 요건에 해당한다고 보기에 부족한 측면이 있으며, 「산업기술보호법」이 「영업비밀보호법」으로 제한되는 보호의 범위를 확대하고자 제정되었기 때문에 비공지성, 비밀유지성, 경제적 유용성을 요건으로 하지 않는 등 성립 요건이 완화되어 있어 실질적으로는 행정기관의 장에 의해 등록만 되면 산업기술에 해당할 수 있다는 점에서 비공개 정보인 것은 맞지만, 특별한 보호가 필요한 것으로 보기에는 적절하지 않다.[37, 43, 44]

이에 비해, 국가핵심기술의 경우는 그 법률 상 정의에 '국가의 안전보장 및 국민경제 발전에 중대한 악영향을 줄 우려가 있는 기술'로 중대한 중요성을 명확히 제시하고 있으며, 해당 기술의 한계 범위도 고시를 통해 세부 규격으로 엄격하게 제한하고 있기 때문에 일반에 공개하지 않아야 함은 물론 특별한 보호가 필요한 정보라고 볼 수 있다.[37, 45] 이에 따라 방산업체에서 주로 보유하고 있는 국가핵심기술을 제외한 산업기술은 국가기밀 분류체계의 비공개 업무자료 등급에 해당한다고 볼 수 있으며, 국가핵심기술은 대외비 등급에 해당한다고 판단할 수 있다.

다음으로, 영업비밀은 국가의 관여 없이 생산되는 정보로, 해당 업체 외부에는 알려져 있지 않고 독립적인 경제적 가치를 지니는 정보이기 때문에 기업의 사익을 보호하기 위한 것일 뿐 공익을 위해 생산된 것이 아니다.[33] 또한, '국가망 보안체계 보안 가이드라인'에 따르면 공공기관의 정보공개에 관한 법률 제9조 제1호 내지 제4호에 해당하는 사항만 C(기밀 정보)로 구분하고, 5호 내지 8호에 해당하는 사항은 S(민감 정보)로 구분하고 있는데, 영업비밀은 제7호에 해당하여 비공개하는 것을 넘어 특별한 보호가 필요한 정보라고 판단하기 어렵다.[5, 46]

따라서 영업비밀은 국가기밀 분류체계를 기준으로 한 '대외비' 등급에 해당한다고 보기는 어려우며, '비공개 업무자료' 등급에 해당한다고 보는 것이 적절할 것이다.

이는 국가에서 영업비밀보다 산업기술 유출 범죄에 대한 양형을 더 높이 판단하고 있음에 의해 간접적으로 뒷받침된다. 대법원 양형위원회는 2024. 3.25.에 열린 제130차 전체회의에서 지식재산·기술침해범죄 등에 대하여 수정된 양형기준을 최종 의결한 바 있다.[47]

이에 따르면 영업비밀 침해 범죄에 대해서는 국내 침해는 10월~3년(감경 6월~1년 6월 / 가중 2년~5년), 국외

침해에 대해서는 1년 6월~5년(감경 10월~3년 / 가중 3년~8년)을 권고하고, 산업기술 침해 범죄에 대해서는 국내 침해는 1년~4년(감경 8월~2년 / 가중 2년 6월~6년), 국외 침해에 대해서는 2년~6년(감경 1년~3년 6월/가중 4년~10년)을 권고하였다.[47]

앞서 살펴봤듯이, 방산업체에서 주로 보유하고 있는 국가핵심기술을 제외한 산업기술 및 영업비밀은 ‘비공개 업무자료’ 등급에, 국가핵심기술은 ‘대외비’ 등급에 해당한다고 판단할 수 있다.

3.3 방산업체 보유정보 통합 분류 방안

3.3.1 국가기밀 분류체계를 적용한 방산업체 보유정보 분류 방안

3.1 및 3.2를 통해 분석한 내용을 종합하여 ‘국가기밀 분류체계’를 기준으로 방산업체 보유·취급 정보를 통합 분류하였다.

먼저, 3.1 및 3.2를 통해 파악한 방산업체 보유·취급 정보 종류 각각이 ‘국가기밀 분류체계’에서 어느 등급에 해당하는지를 매칭하여 <표 10>과 같이 정리했다.

<표 10> 방산업체 보유 정보별 해당 등급

등급	의미	해당되는 방산업체 보유 정보
비밀	법정 절차로 비밀 지정/관리	• 군사 비밀(군사 I·II·III급), 국가 비밀(I·II·III급)
대외비	일반 비공개 + 특별한 보호	• 국가 대외비, 군사 비공개 업무자료, 방산기술(판정), 국가핵심기술
비공개 업무자료	일반 비공개	• 방산기술(식별), 산업기술, 영업비밀, 방산 주요자료, 민수 주요자료
공개 업무자료	일반 공개	• 방산 일반자료, 민수 일반자료

3.1 및 3.2 분석 내용을 정리하면, ‘국가기밀 분류체계’를 기준으로 ‘비밀’ 등급에 해당하는 정보에는 군사 비밀과 국가 비밀이 있으며, ‘대외비’ 등급에 해당하는 정보에는 국가 대외비, 군사 비공개 업무자료, 방산기술 중 판정기술, 국가핵심기술이 있다. 또한, ‘비공개 업무자료’ 등급에 해당하는 정보에는 방산기술 중 식별기술, 산업기술(국가핵심기술 제외), 영업비밀, 방산 관련 주요자료, 민수 관련 주

요자료가 있으며, ‘공개 업무자료’ 등급에는 방산 관련 일반자료와 민수 관련 일반자료가 있다.

두 번째로, C/S/O 구분과 국가기밀 분류체계 등급 간의 관계를 파악하여 함께 제시함으로써 통합 분류를 데이터 관리에도 활용할 수 있게 했다.

국가망 보안체계 보안 가이드라인에 의하면, C(기밀)은 비밀, 안보·국방·외교·수사 등의 기밀정보와 국민 생활·생명·안전과 직결된 정보로서 정보공개법 제9조 제1호부터 제4호까지 포함하는 것으로 정의되므로 법정 절차로 지정 및 관리되는 ‘비밀’ 등급은 물론, 비공개와 특별한 보호가 모두 필요한 ‘대외비’ 등급도 이에 해당한다고 볼 수 있다.[5] S(민감)은 비공개 정보 등 개인·국가 이익 침해가 가능한 정보로서 정보공개법 제9조 제5호부터 제8호까지의 정보를 포함하는 것으로 정의되므로 일반에 비공개되어야 하는 ‘비공개 업무자료’ 등급이 이에 해당한다.[5] O(공개)는 C(기밀) 및 S(민감) 이외의 모든 정보를 포함하는 것으로 정의되므로, 일반에 공개가 가능한 ‘공개 업무자료’ 등급이 해당된다.[5]

마지막으로, 민수 부문과 방산 부문 정보가 혼합 관리되는 것은 정보유출 방지 차원에서 바람직하지 않기 때문에 민수와 방산 부문 정보를 구분하여 제시하였다.

이러한 과정을 통해 ‘국가기밀 분류체계’를 기준으로 방산업체 보유·취급 정보를 통합 분류할 수 있는 방안을 <표 11>과 같이 제시하였다.

<표 11> 방산업체 정보에 대한 국가기밀 등급

구분	분류 등급	방산부문	민수부문
C	비밀	• 군사 비밀 • 국가 비밀	
	대외비	• 국가 대외비 • 군사 비공개 업무자료 • 방산기술(판정)	• (국가핵심기술)
S	비공개 업무자료	• 방산기술(식별) • 방산 주요자료	• 산업 기술 • 영업 비밀 • 민수 주요자료
O	공개 업무자료	• 방산 일반자료	• 민수 일반자료

방산업체 보유·취급 정보 종류 각각이 어느 등급 수준에 해당하는지 판단하는 근거를 현행 법령 및 규정에 두었기 때문에 방산업체 현장 실무에 당장 적용하더라도 법규

에 어긋나지 않게 정보를 관리할 수 있다. 또한, 다수 부처 소관의 정보가 혼재하는 상황에 있더라도 각 정보 종류의 기밀 등급을 명확히 알 수 있어 관련 법규를 준수한 가운데 방산업체 스스로 기준을 가지고 불필요한 보안 투자는 제거하고 중요한 정보 보호에 집중하는 전략적·효율적 보안 관리를 수행할 수 있게 된다.

3.3.2 정책적 보완 방안

반면, 이를 국가 차원에서 공식화하기 위해서는 법규 정비 등 정책적인 보완이 여전히 필요하다.

먼저, 「국방보안업무훈령」 및 「방산보안업무훈령」을 「보안업무규정」과 통일된 기밀분류체계로 개정할 필요가 있다. 군사 분야에서는 대외비가 폐지되었지만, 기타 정부 부문은 폐지가 어려운 환경에 놓여 있는 만큼 군사 분야에 대외비 등급을 부활시키는 것이 필요하며, 군사 분야에서도 정보를 '비밀(Ⅰ·Ⅱ·Ⅲ급) - 대외비 - 비공개 업무자료 - 공개 업무자료'의 등급으로 분류함으로써 국가기밀 보호 관련 법령체계의 완결성을 꾀할 필요가 있다.

두 번째로, 「방산기술보호법」 및 「영업비밀보호법」 등 특별법이나 하위 법령(규칙)을 개정하여, 특별법 상 보호 대상 정보가 국가기밀 분류체계에 있어 어떤 등급에 준하여 보호 및 관리되어야 하는지를 제시해 줄 필요가 있다. 더 나아가 「국정원법」에 국가기밀의 범주를 제시하고, 그러한 범주에 해당하는 정보를 보호하기 위해 특별법을 제정할 때는 해당 법률이나 하위 법령(규칙) 상 해당 보호 대상 정보가 국가기밀 분류체계에 있어 어떤 등급에 준하여 보호 및 관리되어야 하는지 명시하도록 규정할 필요가 있다.

세 번째로, 「국방보안업무훈령」 및 「방산보안업무훈령」 등 각 기관 행정규칙에 비공개 업무자료에 대한 분류 기준을 제시할 필요가 있다. 방산업체에서 보유하는 비밀이나 대외비는 국가에서 생산한 것을 접수하거나, 국가에서 생산한 원본의 전체 또는 일부를 포함하여 재생산한 것이며, 원본에 대해서는 관련 법령에 따라 국가 기관에서 보호 등급을 명시하여 배포하고 있다.[48, 49, 50, 51] 이에 따라 방산업체가 비밀이나 대외비를 분류하는 데 있어서는 큰 어려움이 없다.

반면, 방산 관련 비공개 업무자료를 분류하는 데는 어려

움이 있다. 방산 관련 비공개 업무자료는 방산업체에서 생산하는 경우가 많고, 원본에 대해서도 국가 기관에서 보호 등급을 명시하여 배포하지 않으며, 분류 시 「공공기관의 정보공개에 관한 법률」 제9조 제2호를 참고할 수 있겠으나, 「국가안전보장·국방·통일·외교관계 등에 관한 사항으로서 공개될 경우 국가의 중대한 이익을 현저히 해칠 우려가 있다고 인정되는 정보」로만 개괄적으로 제시되어 있어 비정부 부문인 방산업체가 자체적으로 판단하기에는 부족한 기준이기 때문이다.

방산 관련 비공개 업무자료도 결국, 국가의 입장에서 방산업체가 보호하기를 바라는 정보이기 때문에 이에 대한 전향적 검토가 필요할 것이다.

IV. 결론

위와 같이 본 연구에서는 현행 「국가기밀 분류체계」를 적용하여 방산업체가 보유 및 취급하고 있는 정보를 통합된 체계로 분류할 수 있는 방안에 대해 제안하였다.

그간 우리 방산업체는 정부의 기밀분류체계가 통일되지 않은 가운데, 다양한 종류의 민감한 정부 정보를 보유 및 취급하고 있어 정보관리에 어려움을 겪어 왔다. 관리 주체가 다른 복수의 정부 기밀분류체계가 동시 적용됨은 물론, 기밀 각각의 상대적 중요도에 대한 법령 상 규정이나 정보 분류 가이드가 존재하지 않아 기밀 간 우선순위 마저도 명확하지 않기 때문이다.

반면, 우리나라는 기본적으로 「국가기밀 분류체계」로 통합할 수 있는 법령 및 등급 체계를 갖추고 있으며, 행정실무에서는 행정적·법적 관념을 활용하여 상대적 중요도를 내재적으로 판단해 왔기 때문에 이를 활용하면, 「국가기밀 분류체계」를 기준으로 기밀 각각의 등급 수준을 「비밀-대외비-비공개 업무자료-공개 업무자료」의 4개 등급으로 판단할 수 있다.

또한, 대다수 방산업체가 방산과 민수 양쪽 부문 사업을 모두 시행함에 따라 방산과 민수 정보가 혼재한다는 점을 고려하고, 최근 국정원에서 공공기관의 데이터 관리를 위해 발표한 가이드라인에 따라 향후 정부 데이터들이 C/S/O로 구분될 것이라는 점을 반영하여 <표 11>과 같이

방산업체가 보유 및 취급하고 있는 정보들에 대한 분류 방안을 제안하였다.

방산업체 현장실무에서는 이와 같은 분류를 활용하면, 민감한 정부 정보를 법규에 어긋나지 않게 보호하면서도 스스로 전략적·효율적 보안 투자 및 관리를 수행할 수 있게 될 것이다.

다만, 금번 제안이 미봉책으로 그치지 않고 근본적 해결 방안이 되기 위해서는 법규 정비 등을 통해 ‘국가기밀 분류체계’로의 통합이 공식화되어야 할 것이다. 군사 대외비 부활 등 군사기밀 분류체계를 국가기밀 분류체계와 통일해야 할 것이고, 정보 보호를 목적으로 하는 특별법에 해당 보호대상 정보가 국가기밀 분류체계의 어떤 등급에 준하여 보호되어야 하는지 명시되어야 할 것이며, 방산업체에서 분류에 어려움이 큰 ‘비공개 업무자료’ 등급에 대한 분류 기준을 정부에서 제시해 줄 필요가 있을 것이다.

다만, 본 연구는 방산업체가 취급 및 보유하고 있는 정보들 간의 상대적 중요도를 밝히고, 하나의 체계로 통합 분류하는 방안을 제시하는 데에 그친 한계가 있다.

향후에는 방산업체에 통합된 기밀분류체계를 도입하는 방안에 대해 관련기관 간 협의하고 정책화 및 제도화하기 위한 방안에 대한 연구가 필요하겠으며, 방산 부문 정보와 민수 부문 정보를 구분하는 기준, 정부와 방산업체의 책임 한계, 등급별 세부 분류 기준, 등급별로 차등화하여 적용할 보호 통제 등을 방산업체 입장에서 이해하고 적응하기 용이하도록 제시하는 ‘방산업체 정보 분류 및 보호 가이드’ 개발을 위한 연구가 필요할 것이다.

참고문헌

- 1) 이상열·유연승, 방산업체의 데이터 보유현황 분석에 관한 연구, 한국산학기술학회논문지 제26권 제1호, 2025, p404-410
- 2) 국방기술진흥연구소, 국가별 국방과학기술 수준 조사서, Dec, 2024
- 3) 김보리 기자, 방산기술 유출사례 올해 들어 급증 ...“북한 해커 자료 빼가”, 데일리한국, 2024.10.11. (검색일 : 2025. 4.11.)
- 4) 신삼범·류연승·장경준·손창근, 방산 통합클라우드 시스템 구축방안 연구, 국방과 기술 제542호, Apr, 2024, p110-121
- 5) 국가정보원·국가보안기술연구소, 국가 망 보안 체계 보안 가이드라인, 2025. 1.24. p12 및 p21
- 6) 국가 정보보안 기본지침 제2조, 국가정보원 지침, 2023. 1.31.
- 7) 국방보안업무훈령 제3조, 국방부훈령 제2935호, 2024. 6.11.
- 8) 방위산업보안업무훈령 제3조, 국방부훈령 제2742호, 2022.12. 8.
- 9) 방위산업기술보호지침 제2조 및 제12조, 방위사업청훈령 제867호, 2024. 9.10.
- 10) 산업기술보호지침 제2조, 산업통상자원부고시 제2023-151호, 2023. 7.26.
- 11) 허아라, 방위산업기술 분류체계에 관한 연구, 명지대학교 석사학위논문, Feb, 2018. p11-13
- 12) 장월수, 미국의 국가비밀분류체계 분석 및 시사점, KIDA 주간국방논단 제1638호, Sep, 2016, p1-8
- 13) 中和人民共和國反間諜法 제4조, 2023. 4.26.
- 14) 中和人民共和國保守國家機密法 제2조 및 제2장, 2024. 2.27.
- 15) 김정애, 중국 개정 반간첩법에 관한 소고, 한국 법학회 법학연구 제23권 제4호, Dec, 2023. p49-74
- 16) 손덕중, [중국] 개정 반간첩법 해설 및 컴플라이언스 이슈, 법무법인 지평, 2023. 8. 6.
(<https://www.jipyong.com/kr/board>) (검색일 : 2024. 2. 9.)
- 17) 서승우, 보안 경제학-CEO를 위한 정보보안 투자 가이드, 서울대학교출판문화원, May, 2008. p46-48
- 18) 국방보안업무훈령 제8장 제1절 및 제2절, 국방부훈령 제2935호, 2024. 6.11.
- 19) 방위산업보안업무훈령 제8장 제1절 및 제2절, 국방부훈령 제2742호, 2022.12. 8.
- 20) 방산기술보호지침 제16조, 방위사업청훈령 제867호, 2024. 9.10.
- 21) 산업기술보호지침 제19조 및 제25조, 산업통상자원부고시 제2023-151호, 2023. 7.26.
- 22) 한국방위산업진흥회, 2024 방산지정업체 경영분석, Dec, 2024. p135-137
- 23) 대한민국 헌법 제37조 제2항, 헌법 제10호, 1987.10.29.
- 24) 보안업무규정 제4조, 대통령령 제3154호, 2020.12.31.
- 25) 보안업무규정 시행규칙 제16조, 대통령령 제450호, 2022.11.28.
- 26) 군사기밀 보호법 시행령 제3조, 대통령령 제32968호, 2022.11. 1.
- 27) 국방보안업무훈령 제16조 및 제3조, 국방부훈령 제2945호, 2024. 6.11.
- 28) 방위산업보안업무훈령 제5조 및 제3조, 국방부 훈령 제2742호, 2022.12. 8.
- 29) 국방보안업무훈령 제3장, 국방부훈령 제2945호, 2024. 6.11.
- 30) 방위산업보안업무훈령 제2장, 국방부훈령 제2742호, 2022.12. 8.
- 31) 방위산업기술보호법 제2조, 법률 제20024호, 2024. 1.16.
- 32) 국방과학기술혁신촉진법 제10조, 법률 제19948호, 2024. 1. 9.
- 33) 부정경쟁방지 및 영업비밀보호에 관한 법률 제1조 및 제2조, 법률 제20321호, 2024. 2.20.
- 34) 산업기술혁신촉진법 제13조, 법률 제20695호, 2025. 1.21.
- 35) 군사기밀보호법 제10조 내지 제22조, 법률 제 19076호, 2022.12.13.
- 36) 방위산업기술보호법 제19조 내지 제22조, 법률 제20024호, 2024. 1.16.
- 37) 산업기술의 유출방지 및 보호에 관한 법률, 제1조 및 제2조, 법률 제20319호, 2024. 2.20.
- 38) 부정경쟁방지 및 영업비밀보호에 관한 법률 제11조 및 제19조 내지 제20조, 법률 제20321호, 2024. 2.20.
- 39) 산업기술의 유출방지 및 보호에 관한 법률 제22조의2 및 제6장, 법률 제20319호, 2024. 2.20.
- 40) 방위산업보안업무훈령 제7장 제3절, 국방부 훈령 제2742호, 2022.12. 8.
- 41) 국방보안업무훈령 제200조, 국방부훈령 제2935호, 2024.

6.11.

- 42) 국방과학기술 정보관리 업무지침 별표 5 및 별표 6, 방위사업청예규 제356호, 2017. 1.12.
- 43) 헌법재판소 2013. 7.25. 선고 2011헌바39 결정
- 44) 대법원 2013.12.12. 선고 2013도12266 판결
- 45) 국가핵심기술 지정 등에 관한 고시 별표, 산업통상자원부 고시 제2024-114호, 2024. 7. 5.
- 46) 공공기관의 정보공개에 관한 법률 제9조, 법률 제19408호, 2023. 5.16.
- 47) 법무법인 김앤장(www.kimchan.com), 영업비밀 및 산업기술 침해에 대한 처벌을 강화한 양형기준 시행 예정(검색일 : 2024.11.24.)
- 48) 보안업무규정 제16조, 대통령령 제3154호, 2020.12.31.
- 49) 보안업무규정 시행규칙 제16조, 대통령훈령 제450호, 2022.11.28.
- 50) 국방보안업무훈령 제24조 및 제63조, 국방부 훈령 제2945호, 2024. 6.11.
- 51) 방위산업보안업무훈령 제16조 및 제56조, 국방부 훈령 제2742호, 2022.12. 8.