Journal of the Korea Academia-Industrial cooperation Society
Vol. 25, No. 8 pp. 501-508, 2024

https://doi.org/10.5762/KAIS.2024.25.8.501
ISSN 1975-4701 / eISSN 2288-4688

# 방산기술환경맵 데이터 비식별 처리 방안 연구

**황도빈*, 권경숙, 김정원, 최지웅**
**국방기술품질원**

# A Study of Defense-Industry-Technology-Environment-Map Data De-Identification Method

Do-Bin Hwang*, Kyung-Sook Kwon, Jeong-Won Kim, Ji-Woong Choi
Defense Agency for Technology and Quality

**요 약** 국내 방위산업은 1970년 초 자주국방 추진을 시작으로 급격하게 성장하여 현재는 전 세계 무기 수출시장 점유율 2.4%를 차지하며 수출순위 9위를 기록했다. 특히, 최근 2년간 수출액이 역대 최대 규모인 평균 150억 달러를 달성하였으며, 수출대상국도 4개국에서 12개국으로 확대되어 질적 향상을 이루어냈다. 이에 따라 정부는 전 세계로부터 인정받은 우리나라 방산업체의 첨단 국방기술을 보호하기 위해 방위산업기술보호법을 제정하고 주기적인 통합 실태조사를 통해 기술 유출사고 예방에 만전을 기하고 있다. 통합 실태조사 시 국내 방산업체 및 방산기술의 현황을 조사하기 위해 방산업체로 하여금 방산기술환경맵(이하 '방산맵')을 작성하여 제출하도록 권고하고 있다. 방산맵은 대외에 공개되어있는 업체현황 뿐만아니라 일부 개인정보 및 민감 방산정보를 포함하고 있으므로 데이터로 활용 전 비식별 처리 및 보호조치가 필수적이다. 향후 방산포탈(가칭)의 구축 완료 후 방산맵 데이터를 기반자료로 활용할 가능성이 크므로 그 전에 방산맵 데이터의 비식별 처리 방안에 관한 연구가 필요하다. 이를 위해 본 논문에서는 현재 개인정보 및 가명정보 비식별 처리에 관한 국내외 동향과 향후 방산분야 데이터 분석 환경의 초석으로 활용될 방산맵 데이터의 비식별 처리 기술에 대해 제시한다.

**Abstract** The domestic defense industry has grown rapidly since the early 1970s with a push for independent national defense, and it currently ranks ninth in exports, accounting for 2.4% of the global arms export market. In particular, exports over the past two years reached an average of US$15 billion (the most ever), and the number of export destinations has expanded to 12 countries from only four, achieving qualitative improvement. Accordingly, the government enacted the Defense Technology Security Act to protect cutting-edge defense technology of Korean defense companies recognized around the world, and is making every effort to prevent technology leaks through a periodic Current Status Investigation. In order to investigate the current status of domestic defense industry companies and defense technology during an investigation, it is recommended that defense industry companies prepare and submit a defense technology environment map (hereinafter referred to as a Defense-map). Since the Defense-map contains not only publicly available company information but also personal information and sensitive defense information, de-identification and protection measures are essential before it is used as data. In future, after establishment of the tentatively named Defense Industry Portal, research is needed on methods for de-identifying the Defense Map data. This paper presents current domestic and international trends in the de-identification processing of personal information, pseudonymous information, and de-identification processing technology for defense map data that will be used as the cornerstone of the future defense industry data analysis environment.

**Keywords :** Defense Industry, De-identification, Masking Method, Privacy Protection, Defense Technology

*Corresponding Author : Do-Bin Hwang(Defense Agency for Technology and Quality)
email: dobin119@gmail.com
Received June 28, 2024 Revised July 29, 2024
Accepted August 2, 2024 Published August 31, 2024

## 1. 서론

4차 산업혁명 이후 세계 각국은 첨단 방위산업기술의 확보와 기술개발을 통해 국가의 평화와 국민의 안전을 지키기 위해 힘을 쏟고 있다. 국가 주도로 개발한 방위산업기술이나, 방산업체 자체개발을 통해 개발된 첨단 무기체계의 핵심기술 등은 국가 방위력 수준뿐만 아니라 기업 경쟁력의 척도가 되므로 각국은 방위산업기술의 보호를 위해 다각도의 노력을 기울이고 있다.

우리나라 또한 방위산업기술을 체계적으로 보호하고 관리하기 위해 2017년 방위산업기술 보호법을 제정하여 국가의 안전을 보장하고 기술보호 국제조약 등의 의무를 이행하여 국가신뢰도를 제고하고 있으며, 상기 법을 방위사업청, 국방과학연구소뿐만 아니라 방위산업기술을 개발하고 취급하는 방산업체에 적용하고 있다[1].

방위산업과 관련한 국방과학기술 중 국가안보 등을 위하여 보호되어야 하는 기술인 방위산업기술은 방위사업청장이 지정·고시하는 기술에 해당하는 것으로서 국방과학연구소에서 개발하는 무기체계의 핵심기술이나, 방위산업업체에서 개발하는 무기체계의 핵심기술 등을 말한다.

최근 우리나라는 K-2전차, K-9자주포, 레드백 등 지상 무기체계와 향후 개발이 완료될 KF-21 차세대 전투기까지 다양한 국내의 첨단 무기체계를 세계로부터 인정받아 많은 국가로 수출하여 위상을 드높이고 있다. 특히 우리나라의 방산 수출액은 23년 130억 달러를 넘어섰으며, 방산 수출대상국 또한 4개국에서 12개국으로 확대되어 질적 성장을 이뤄냈다[2].

하지만 동시에 우리나라의 첨단 방산기술이 개발되고 성장함과 동시에 기술 탈취를 위한 산업스파이의 시도나 적국의 사이버침해 시도가 급격하게 증가하고 있으며 다양한 방법을 통해 방위산업기술을 탈취하기 위한 시도를 지속하고 있다. 실제로 최근 한 방산업체에서는 7년 전부터 지속적으로 방산기술이 유출된 것으로 확인되어 수사를 진행중에 있고, 북한의 해킹조직 라자루스, 안다리엘, 킴수키가 합동으로 국내 방산업체를 해킹하여 방산기술의 탈취를 목적으로 공격하고 있다[3].

우리나라는 이러한 유출사고를 정부차원에서 예방하기 위해 통합 실태조사, 보안측정을 시행하고 있으며, 향후 한국형 RMF(K-RMF, Korea-Risk Manage -ment Framework), K-CMMC의 도입을 준비하고 있다. 특히 통합 실태조사는 방위산업기술 또는 관리대상기술을 보유하고있는 모든 방산업체의 기술보호수준을 점검하고 미흡사항을 식별하여 기술유출의 가능성을 최소화하고 있다.

방산기술환경맵(이하 '방산맵')은 방산업체에서 통합 실태조사 수검을 위해 업체 위치, 인원 수, 매출액 등의 현황자료와 관리대상기술 목록, 기술보호구역, 정보보호체계 현황, 출입자 현황자료 등 기술보호환경과 관련된 내용을 작성한 데이터로, 방위사업청 주관으로 수집하는 데이터이다. 업체의 관리와 지원을 위해 내부적으로 활용되어 외부에는 공개되지 않으나, 업체정보와 개인정보가 다수 포함되어있어 향후 방산맵데이터의 활용 전 비식별 조치가 필요하다.

본 논문에서는 향후 방산맵 데이터의 활용에 대비하여 방산맵 데이터 내에 포함된 개인정보 및 민감정보에 대한 범위와 적용할 비식별 처리 기술에 대한 방안을 제시하고자 한다.

## 2. 이론적 배경 및 선행연구

### 2.1 국제 데이터 비식별화 정책 동향

비식별화를 NIST(National Institute of Standards and Techno –logy)에서는 "수집, 활용, 저장, 공유하는 데이터 셋에서 개인을 식별할 수 있는 정보를 제거하는 것"으로 정의하고 있으며 개인의 영역은 조직을 포함하는 개념으로 적용하고 있다[4]. 또한 "제거하는 것"의 의미는 단순히 개인이나 조직을 식별하는 부분을 삭제하는 것을 말하는 것이 아니라 개인을 식별할 수 있는 연계성을 삭제하는 것이므로 비식별화와 익명화는 차별되는 개념으로 생각할 수 있다. 익명화는 비식별화를 수행하는 여러 방법 중 하나로 원본 데이터로 되돌릴 수 없도록 비식별화 하는 방법을 말한다.

국외에서 비식별 처리와 관련된 지침은 아래와 같다. 미국은 각 정부부처에서 생산되는 다양한 데이터셋을 대중에게 공개하여 활용하도록 하고 있으며 NIST에서는 "De-Identifying Government Datasets"을 발간하여 정부 데이터셋 내의 개인정보를 비식별화 방안과 절차를 설명하고 있다. 미국은 시민들이 정부에 개인정보 데이터를 제공하는 경우 정보에 대한 기밀을 보장하고 있으며, 공식 통계자료를 위해서만 활용되어야 하고 국민에게 공개되는 정보에는 개인정보가 반드시 비식별화를 하도록 규제하고 있다.

호주는 2017년 "The De-Identification Decision-

Masking Framework"를 발간하여 개인정보 비식별화 가이드라인을 제시하고 있다. 호주의 개인정보법에서는 비식별화가 완료된 개인정보는 개인을 더 이상 식별할 수 없어야 한다. 하지만 명확한 기준을 제시하지 않고 있으며 다양한 정보를 조합하여 개인을 식별할 수 있는지 등을 고려하여 비식별화가 완료되었는지 판단한다.

캐나다는 '23년 1월 "Privacy Implementation Notice : De-Identification"을 공표하여 비식별화 방법과 대상 등에 대해 설명하고 있다. 캐나다는 비식별화가 완료된 데이터셋은 개인정보를 포함하지 않으므로 개인 프라이버시가 침해되지 않는 것으로 판단하여 공개가 가능하다고 명시하고 있다.

위 세 국가의 가이드라인 또는 정부 시행문에 따르면 비식별화의 절차와 방법, 대상에 대한 법률이 체계적으로 제정이 되어있고 비식별화를 수행하지 않으면 공개할 수 없음을 명시하고 있다.

## 2.2 국내 비식별화 관련 정책 동향

국내에서는 2016년 "비식별 조치 가이드라인"을 발표하여 개인정보를 포함한 자료를 활용하는 경우에 적용하는 비식별화 절차와 방법들을 설명하였다.

2018년 데이터 3법(개인정보 보호법, 정보통신망 이용 촉진 및 정보 보호 등에 관한 법률, 신용 정보의 이용 및 보호에 관한 법률) 개정안이 발의되어 데이터 산업의 발전에 대비하였다. 데이터 3법에서는 개인의 동의없이 연구 목적으로 개인정보를 활용할 경우 비식별화 조치를 반드시 해야하도록 규제하고 있다. 하지만 비식별화의 기술적 어려움과 절차, 규제로 인해 데이터 활용에 어려움을 겪고 있으며, 법제화된 것이 아닌 가이드라인으로 제정되어 구체적인 법령이 필요했다[5].

2024년 2월 "비식별 조치 가이드라인"이 "가명정보 처리 가이드라인"으로 개정되어 빅데이터, AI 데이터 활용 급증에 대비하여 가명정보 활용에 필요한 절차, 방법, 안전조치에 관한 사항을 안내하고 안전한 데이터 활용 환경을 마련하였다.

## 2.3 비식별 처리 절차

기존의 개인정보 비식별 처리 가이드라인(2016)은 사전검토, 비식별 조치, 적정성 평가, 사후 관리의 4단계를 거쳐 비식별화 처리를 수행한다.

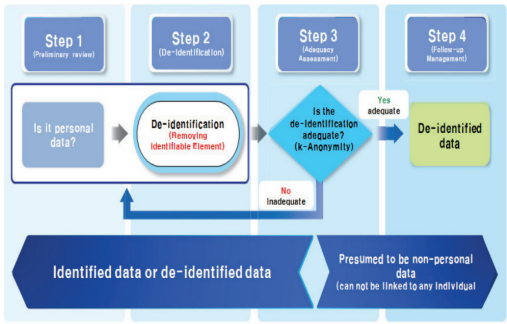


Fig. 1. Personal Information De-Identification Procedure[6]

2024년 2월 새롭게 개정된 가명정보 처리 가이드라인의 비식별화 조치 절차는 사전준비, 위험성 검토, 가명처리, 적정성 검토, 안전한 관리의 5단계로, 기존의 가이드라인과 크게 달라진 점은 없으나 위험성 검토 단계가 추가 되었다.


Fig. 2. Procedure for pseudonymizing personal information[7]

가명정보 비식별 처리는 1단계, 사전준비 단계에서 가명정보의 처리 목적을 명확히하고 어떠한 개인정보와 가명정보를 비식별화 처리할 것인지 식별한다. 2단계인 위험성 검토 단계는 주어진 정보 외의 정보와 결합하여 개인이나 조직을 식별할 수 있는지 고려하는 단계이다. 3단계인 가명처리 단계는 비식별화 방법을 선정하고 항목별 가명처리 계획을 설정한다. 4단계인 적정성 검토 단계에서는 비식별화 처리된 정보가 적절하게 비식별화 처리 되었는지를 최종 검토하는 단계이다. 5단계인 안전한 관리 단계는 생산된 비식별화 처리의 마지막 단계로, 비식별 처리를 완료한 데이터를 법에 따라 기술적, 관리적, 물리적 안전조치를 시행하고 사후관리 계획을 수립하는 단계이다. 비식별 처리를 완료한 데이터는 지속적으로 모니터링하여 재식별 방지를 위한 조치를 수행해야 한다.

## 2.4 가명처리 단계 기술 정의

가명정보 처리 가이드라인에서 정의한 비식별 처리 단계 중 실질적인 비식별화가 처리되는 단계는 3단계인 가명처리 단계이다. 가명처리 단계에 활용이 가능한 비식별 처리 기술은 삭제(Suppression), 마스킹(Masking),

라운딩(Rounding), 범위방법(Data Range) 등 29개 기술을 정의하고 있으며, 상황과 데이터의 형태를 고려하여 적절한 비식별 처리 기술을 적용할 수 있다.

Table 1. De-Identification Method[5]

| Method | Techniques | |
|---|---|---|
| Delete personal information | Deletion | Suppression |
| | | Partial suppression |
| | | Record suppression |
| | | Local suppression |
| Replace some or all personal information | Deletion | Masking |
| | Statistical Tools | Aggregation |
| | | Micro aggregation |
| | Generalization | Rounding |
| | | Random rounding |
| | | Controlled rounding |
| | | Top and bottom coding |
| | | Local generalization |
| | | Data range |
| | | categorization of character data |
| | Encryption | Two-way encryption |
| | | One-way encryption-Cryptographic hash function |
| | | Order-preserving encryption |
| | | Format-preservering encryption |
| | | Homomorphic encryption |
| | | Polymorphic encryption |
| | Randomization | Noise addition |
| | | Permutation |
| | | Tokenization |
| | | Random Number Generator |
| Others | | Sampling |
| | | Anatomization |
| | | Synthetic data |
| | | Homomorpic secret sharing |
| | | Differential privacy |

가명정보 처리 가이드라인과 국제 표준으로 정의된 ISO/IEC 20889을 비교하면 암호화, 총계처리, 부분총계, 라운딩, 재배열, 감추기, 랜덤라운딩, 범위 방법, 임의잡음 추가, 공백 처리 등 대부분의 기술이 상호 적용이 가능한 것으로 파악되며, 일부 분야에 있어서는 국내 가이드라인이 더욱 세부적인 비식별 처리 기술을 설명하고 있다[8].

## 3. 본론

### 3.1 방산기술환경맵 정의

방산기술환경맵(이하 '방산맵')은 국내 83개 방산업체의 현황을 파악하고, 업체에서 보유하고 있는 방산기술을 사전에 관리하여 적의 사이버위협을 대비하기 위한 데이터이다. 방산맵은 방위산업기술 지정고시에 따라 식별한 방위산업기술 또는 관리대상기술을 취급, 관리, 저장하는 방산업체의 현황정보를 포함하고 있다[9]. 방산맵 데이터는 방산기술보호 통합 실태조사 시 대상업체에서 작성하여 방위사업청으로 제출하며, 업체의 현황을 파악하는 참고자료로 활용되어 정부차원의 관리와 적절한 지원을 가능케 한다.

### 3.2 방산기술환경맵 데이터 구조

방산맵은 엑셀파일 내 16개의 시트로 구성되어 있으며, 각 시트는 세부 데이터를 포함하고 있다. 방산맵 내 데이터는 기본정보인 업체의 소재지, 방산분야 매출액, 인원 현황 등 업체의 일반현황자료를 포함하고 있으며, 추가적으로 방위산업기술/관리대상기술, 기술보호구역, 외국인 출입대장, 자료교환체계 현황 등 개인정보 및 민감정보를 다수 포함하고 있다.

Table 2. Data Structure

| Sheet | Column |
|---|---|
| Location | Company Name, Location |
| Employee | Total number of employee, Number of defense industry employee, Ratio |
| Sales | Total sales, Sales of defense industry, Ratio |
| Manager | Position, General/Department manager, Name, Contact |
| Authorized Person | Position, Name |
| Main Production | Civil/Defense, Main production, Applicable Weapon |
| Defense Technology | Company name, Management no., Protection level, Name of technology, Description, Applicable Weapon, Owned company, note |
| Additional Technology | Company name, Management no., Protection level, Name of technology, Description, Applicable Weapon, Owned company, note |
| Protection Area | Number of Area, Description |

| | |
|---|---|
| R&D | Type of project, Name of project, Cost, Period, Applicable Weapon |
| Export | Project Name, Period, Cost |
| Foreigner | Nation, Company, Name, Period, Purpose, Place, Background check, Escort, Notes |
| Overseas | Location, Related weapon, notes |
| Data Exchange | System name, Methon, Solutions, notes |
| Military secret | (Not open to the public) |
| Teleworking | Implementation, Teleworking system |

또한 각 시트의 세부데이터는 정형, 비정형데이터로 분류가 가능하다. 기본정보 내의 소재지, 인원 수, 매출액 등 통계적 활용이 가능한 정형데이터와 업체의 방위산업/관리대상기술 설명 등 비정형데이터가 복합적으로 결합되어 정보를 이루고 있다.

### 3.3 비식별 대상 범위 및 적용 기술 선정

방산맵 내에는 업체 및 개인정보와 방산분야의 민감정보가 다수 포함되어 있으며, 향후 방산기술보호업무포탈(가칭) 구축 시 방산맵 데이터를 기반 데이터로 활용할 여지가 있으므로 비식별화 처리가 필요하다. 특히 관리대상기술 시트는 업체가 개발중 또는 개발이 완료된 기술에 대한 명세와 적용 무기체계명, 이 작성되어 있으므로 반드시 비식별화가 필요하다.

다만 업체의 인원 수, 매출액, 소재지 등 일반적인 업체 현황자료는 홈페이지나 웹 상에 공개되어 있어 비식별 처리가 불필요한 것으로 판단된다.

따라서 방산맵 데이터 중 비식별 처리가 필요한 대상 및 범위는 아래의 표와 같이 분류하였다.

Table 3. De-Identification Range, Target

| | Sheet | De-identification Required | |
|---|---|---|---|
| | | Structured | Unstructured |
| De-identification Required | Manager | Position, Name | - |
| | Authorized Person | Name | - |
| | Defense Technology | Company name, Management no., Protection level, Owned company | Name of technology, Description, Applicable Weapon |
| | Additional Technology | Company name, Management no., Protection level, Owned company | Name of technology, Description, Applicable Weapon |
| | Protection Area | Number of Area | Description |
| | R&D | Cost | Name of project, Applicable Weapon |
| | Foreigner | Nation, Company, Name, Period | Purpose, Place, Notes |
| | Military secret | (Not open to the public) | |
| De-identification Not Required | Location | Company Name, Location | |
| | Employee | Total number of employee, Number of defense industry employee, Ratio | |
| | Sales | Total sales, Sales of defense industry, Ratio | |
| | Main Production | Civil/Defense, Main production, Applicable Weapon | |
| | Export | Project Name, Period, Cost | |
| | Data Exchange | System name, Methon, Solutions, notes | |
| | Overseas | Location, Related weapon, notes | |
| | Teleworking | Implementation, Teleworking system | |

비식별 처리 대상 데이터 중 직책, 업체명, 보호등급, 국적, 소속, 성명, 출입장소, 출입목적 등의 정형데이터는 마스킹, 부분삭제 등의 삭제기술을 적용하거나 잡음추가 등의 무작위화 기술을 적용하여 비교적 간단하게 비식별 처리가 가능하다.

또한 외국인 출입기간, 기술보호구역의 구역 수는 범위로 변환시키는 일반화 기술을 적용하여 비식별 처리가 가능하다.

하지만 방위산업기술/관리대상기술의 기술명, 기술명세, 적용 무기체계명 등의 데이터는 비정형데이터로 저장되어있어 일괄적인 비식별 처리를 적용하는 것이 제한된다. 따라서 위의 비정형 데이터는 여러번의 비식별 처리를 수행하는 다중 비식별 처리 기술을 적용하여 비식별 처리가 가능하다.

### 3.4 비식별 처리 알고리즘 모델 정의

업체명, 보호등급, 국적, 소속 등 정형데이터는 단일 컬럼 내에 위치하여 컬럼의 위치를 사전에 정의하고 해당 컬럼을 즉각적으로 삭제하거나 의미가 없는 데이터로 변환하는 삭제기술, 무작위화 기술을 적용하였다.

외국인 출입기간, 기술보호구역 수 등 숫자로 표현이 가능한 정형데이터는 범위로 변환하는 방법인 범위방법을 적용하였다.

방위산업기술/관리대상기술의 기술명, 기술명세, 적용 무기체계명이나 외국인 출입 시트의 방문목적, 특이사항 등의 비정형데이터는 동일한 단어라도 표기하는 방법이 다양하여 추가적인 비식별 처리 규칙이 요구된다. 예를 들어 K-2전차를 표기하는 경우 K-2, K2, K2전차,

K-2전차 등 다양한 형태로 표기하고 있어 단일 치환기술로는 비식별화 적용이 불가능하다. 따라서 동일한 무기체계를 표기하는 다양한 용어을 사전에 정의한 후 다중 치환기술을 적용하였다.

Table 4. De-Identification Rules

| Target | Applied technique | Description |
|---|---|---|
| Protection Level | Data suppression | Delete the column data |
| Person name | | |
| Natioin | | |
| Company | | |
| Place | | |
| Purpose | | |
| Notes | | |
| Period | Data range | Convert value to range<br>ex) 2 area → 1~5 area,<br>7 area → 6~10 area |
| Number of protection area | | |
| Company name | categorization of character data(single) | Define the target in advance and replace it only once<br>ex) DTAQ → Defense Company |
| Technology name | categorization of character data(multiple) | Define the target in advance and replace it multiple times<br>ex1) Boramae, KF21, kf-21, Kf-21, kF-21, etc<br>→ Weapon system<br>ex2) K2, K-2, Black panther, etc<br>→ Weapon system |
| Description | | |
| Applicable weapon ex)KF-21, K-2 | | |
| ⋮ | ⋮ | ⋮ |

Table 4의 규칙에 따라 비식별 처리 중 명칭이 유사한 무기체계로 인해 오류가 발생하여, 이를 예외처리 하는 알고리즘을 추가 적용하였다.

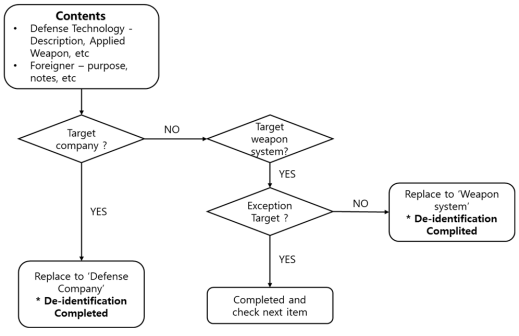


Fig. 3. De-Identification exception Flowchart

예를들어 “K-2”를 “무기체계”로 치환 하는 기술 적용 시 “K-2소총”이 “무기체계소총”으로 치환되는 경우가 발생하였으며, 이를 해결하기 위해 앞, 뒤 문자열을 고려하여 치환 기술이 적용되도록 개선하였다.

Table 5. De-Identification Exception Rules

| De-identification Target | Exception Rules |
|---|---|
| K-2 Black panther | Compare the before and after strings and handle exceptions if there is a predefined string<br>* If K-2 rifle, K2 rifle, K2 gun, etc. are identified, no replacement is made |
| ⋮ | ⋮ |

위의 기술을 파이썬을 활용하여 구현하였다. 우선 방산맵 데이터를 읽어들인 후 삭제기술을 적용할 시트와 데이터 컬럼을 식별하여 삭제를 수행한다. 그 후 외국인 출입 시트의 출입기간과 기술보호구역 시트의 구역 수의 경우 일반화(범위 방법)기술을 적용하여 비식별 처리를 적용한다. 다음으로 치환기법 적용을 위해 사전 정의된 업체명, 무기체계 목록과 입력된 데이터를 비교하여 해당하는 업체명, 무기체계가 있을 경우 변경되도록 알고리즘을 작성하였다. 사전정의된 치환대상을 식별한 경우 replace 함수를 활용 변경을 수행하였으며, 이때, 치환 오류를 줄이기 위해 예외처리 항목의 처리를 위한 조건문을 작성하여, 앞뒤의 단어를 고려하도록 구성하였다.

Table 6. Example of De-Identification results

| Sheet - Column | Contents |
|---|---|
| Defense/Additional technology - Description | Owned Company : DTAQ<br><br>Turbine blade shape design simulation and design technology for KF-21 and FA-50 air turbine starters |
| | K-2 rifle cooling optimization design technology |
| | ↓ (De-identification) |
| Defense/Additional technology - Description | Owned Company : Defense company<br><br>Turbine blade shape design simulation and design technology for weapon system and weapon system air turbine starters |
| | weapon system rifle cooling optimization design technology |

알고리즘 작성 후 방산맵 샘플데이터에 적용한 결과, 약 5분 후 비식별처리가 완료되었다. 기존에는 수작업으로 비식별 처리를 하여 83개 방산업체의 방산맵 데이터를 비식별 처리하는 경우 80시간의 시간이 소요되었으나, 알고리즘 적용 후 수 분내에 비식별 처리가 완료되어 월등한 수준의 비식별 처리 시간 단축 효과를 기대할 수 있을 것으로 판단된다.

## 4. 결론

빅데이터, AI 등이 전 산업군에 적용되어 데이터 이용 수요가 급증하는 가운데 데이터 활용의 근거가 되는 법적 근거가 마련되었다. 개인정보보호법, 정보통신망법, 신용정보법이 시행되어 통계작성, 과학적 연구, 공익적 기록보존을 목적으로 데이터를 비식별화(가명처리) 후 이용할 수 있는 기반이 마련되었다.

논문에서 제시하는 기술은 향후 방산기술보호 업무포탈(가칭) 등 방산업체 정보를 활용하여 데이터를 분석하는 체계를 구축한 후 기반 데이터 내 개인정보 및 방산분야 민감정보를 신속하게 비식별 처리할 수 있다. 또한, 기존에는 수작업으로 비식별 처리 작업을 수행하여 작업자의 휴먼에러로 인한 오류가 발생하였으나, 본 논문의 알고리즘 적용 시 오류 발생가능성이 희박해졌다. 그 결과 방산맵 비식별 처리 알고리즘을 적용하여 기존보다 신속하고 효율적인 방산분야 데이터 분석 기반을 제공할 것이다.

다만, 본 연구에서 적용한 비식별 처리 방안은 방산데이터의 1차적인 비식별 처리에 대한 연구로, 사전에 비식별 처리 대상을 정의해야하고, 방산맵 데이터를 사전/사후에 점검해야하는 한계가 있다. 또한 비식별처리된 방산맵 데이터의 프라이버시 보안이나 데이터 보안에 대한 부분은 추가적인 연구가 필요하다.

따라서 향후에는 본 연구에서 수행한 방산맵 내 정형화 및 비정형데이터 비식별 처리에만 적용하는 것이 아니라 다른 형태의 데이터 비식별처리를 수행하고, 프라이버시 및 데이터 보안에 대한 추가 연구를 수행하여 방산분야 데이터 분석의 기반 환경을 제공함으로써 다양한 연구자와 정부 및 군 관계자에게 효율적으로 방산 정보를 제공하고 동시에 비식별 처리를 통해 개인정보와 민감정보를 철저히 보호하여 방산분야 데이터를 안전하게 공유할 수 있는 체계적 기반을 조성할 수 있을 것이다.

## References


[1] ROK Ministry of National Defense, Defense Technology Security Act, Jun. 2021

[2] KBS NEWS, “This year's defense industry exports are expected to exceed $13 billion... Diversification of weapon systems and export countries”, Dec. 2023, https://news.kbs.co.kr/news/pc/view/view.do?ncd=7846583 (accessed Jul. 23, 2024)

[3] National Cybersecurity Strategy, Office of National Security, Feb. 2024

[4] Simson L. Garfinkel, De-Identification of Personal Information, NISTIR 8053, National Institute of Standards and Technology, U.S., p.1-2 DOI: http://dx.doi.org/10.6028/NIST.IR.8053

[5] Jimin Son, Minho Shin, Research on the current status of de-identification of personal information and supple -mentary guidelines for de-identification measures, Review of KIISC, 33(6), 2023, p.89-109.

[6] OGPC, MOIS, KCC, FSC, MSIFP, MOHW, Guidelines for actions against personal information de-identification, KISA, 2016, pp.3.

[7] Pseudonym information processing guidelines, PIPC (Personal Information Protection Commission), 2024. p.10., p.85-57.

[8] ISO/IEC 20889, Privacy enhancing data de-identification terminology and classification of techniques, 2018

[9] ROK Ministry of National Defense, “Defense Acquisi -tion Program Act”, Mar. 2021, p.1



황 도 빈(Do-Bin Hwang) [정회원]

- 2014년 2월 : 공군사관학교 시스템공학과 (학사)
- 2023년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
정보통신, 사이버보안, 개인정보보호, 인공지능

권 경 숙(Kyung-Sook Kwon) [정회원]

- 2009년 8월 : 이화여자대학교 통계학 전공 (석사)
- 2015년 9월 ~ 현재 : 국방기술품질원 선임연구원

〈관심분야〉
사이버보안 인증, 국방무기체계, 국방보안

김 정 원(Jeong-Won Kim) [정회원]

- 2022년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
사이버보안 인증, 국방SW, 항공무기체계

최 지 웅(Ji-Woong Choi) [정회원]

- 2014년 2월 : 금오공과대학교 컴퓨터공학부 (학사)
- 2023년 7월 ~ 현재 : 국방기술품질원 연구원

〈관심분야〉
국방무기체계, 국방무기SW, 인공지능, 빅데이터