https://doi.org/10.33778/kcsa.2023.23.1.109

과학기술 중심 국방혁신을 위한 데이터 가치 기반 보안정책 발전 방향

박 흥 순*

요 약

미래 국방은 세계 안보정세의 불확실성 가속화, 국내 사회·경제적 여건 제한 등 다양하고 도전적인 환경에 직면하고 있다. 이에 우리 국방부는 인공지능, 드론, 로봇 등 과학기술 기반의 국방혁신으로 당면한 문제점과 위협요인에 대응하려 하고 있다. 인공지능 기반의 첨단과학기술 도입을 위해서는 클라우드, 5G와 같은 IT기반 환경 위에 데이터를 융합하고 활용하는 것이 필수적이다. 하지만 기존의 전통적인 보안 정책은 주로 시스템 중심의 보안으로 일률적인 보안 통제수단을 적용하는 등 데이터 공유 및 활용에 어려움이 있다. 본 연구는 데이터 가치 평가 및 데이터 수명주기 관리에 대한 이론적 배경을 바탕으로 데이터 가치 기반의 국방 보안정책으로 패러다임 전환을 제안한다. 이를 통해 데이터 기반의 업무 활성화 및 AI기반 과학기술중심의 국방혁신 구현에 도움이 될 것으로 기대한다.

Improving the Security Policy Based on Data Value for Defense Innovation with Science and Technology

Heungsoon Park*

ABSTRACT

The future outlook for defense faces various and challenging environments such as the acceleration of uncertainty in the global security landscape and limitations in domestic social and economic conditions. In response, the Ministry of National Defense seeks to address the problems and threats through defense innovation based on scientific and technological advancements such as artificial intelligence, drones, and robots. To introduce advanced AI-based technology, it is essential to integrate and utilize data on IT environments such as cloud and 5G. However, existing traditional security policies face difficulties in data sharing and utilization due to mainly system-oriented security policies and uniform security measures. This study proposes a paradigm shift to a data value-based security policy based on theoretical background on data valuation and life-cycle management. Through this, it is expected to facilitate the implementation of scientific and technological innovations for national defense based on data-based task activation and new technology introduction.

Key words : Defense Innovation 4.0, Defense Security, Security Policy, Data Security, Data Life-cycle, Data Valuation, Zero Trust

접수일(2022년 09월 30일), 수정일(2022년 10월 24일), 게재확정일(2023년 03월 12일)

* 국방부 국방개혁실 국방혁신기술담당관실

1. 서 론

최근의 러시아-우크라이나 전쟁에서 볼 수 있듯이 국가 간 안보 환경의 불확실성은 가중되고 있으며, 첨단 무기체계의 발전에 따른 위협은 더욱 고도화되고 다변화되고 있다. 이에 국방부는 인공지능(Artificial Intelligence, 이하 AI)기반의 드론, 로봇과 같은 과학기술 기반의 첨단전력 도입으로 다양한 불안 요소를 극복하려고 하고 있으며, 이를 위해서는 기본적으로 국방데이터 활용이 중점적으로 고려되어야 한다.

하지만, 기존의 전통적인 보안은 영역중심, 경계중심의 시스템 보호정책으로 사물인터넷 기기 증가에 따른 무선 인프라 확산, 클라우드 중심 환경에는 충분한 대책이 되지 못하고 있다. 또한 정부의 데이터 공유 및 활성화 정책도 추진되고 있어 데이터 활용성이 증대될 수 있도록 보안정책 개선이 시급하다.

데이터 활용 중심의 보안정책은 시스템 별로 획일적인 보호수준을 적용하는 것이 아니라, 데이터의 속성에 따른 가치를 판단하여 맞춤형 보호대책을 수립하는 것으로 정의될 수 있다. 이는 기관에서 보유하고 있는 데이터의 가치를 판단하여 정보의 보호수준을 비밀데이터용, 비공개데이터용, 공개데이터용 등으로 차등하여 구분하고 데이터의 수명주기 전 단계에 걸쳐 주기적으로 보호수준을 재설정하는 등의 방법으로 구현할 수 있다.

본 연구의 구성은 다음과 같다. 2장에서는 관련 배경으로 국방혁신 4.0 추진 배경과 보안정책 변화의 필요성 등을 살펴보고, 3장에서는 국방 데이터 활용을 위한 보안정책 요인으로 국방데이터와 수명주기 모델을 분석하고 시간 경과에 따른 데이터 가치 변화를 살펴본다. 4장에서는 데이터 가치 기반의 보호수준 판단과 업무수행 방안을 제안하고 마지막 장에서 결론을 맺는다.

2. 이론적 배경

2.1 국방혁신 4.0

미래 국방은 외부적인 안보위협의 증가와 국내 병역자원 감소, 감염병 확산 등 비군사적, 초국가적 문제 등 다양한 환경에 직면하고 있다. 이에 국방부는 4차 산업혁명 과학기술 도입을 통한 국방 전 분야의 혁신을 구현하고자 2019년도에 '스마트 국방혁신 추진단'을 출범시켰다[1]. 과학기술기반의 국방혁신은 장기적 관점에서 '국방혁신 4.0'으로 발전하여 'AI 과학기술강군 육성'이라는 목표로 추진되고 있으며, AI 유·무인복합전투체계와 같은 첨단전력 확보가 핵심이다[2].

국방혁신 4.0의 목표에서 중심 기반이 되는 기술이 AI 인데, AI를 제대로 활용하기 위해서는 5G와 같은 무선 인프라 환경과 클라우드 컴퓨팅 환경, 그리고 국방데이터의 활용이 필수적이다. 하지만 국방 분야는 안보관련 중요성 등으로 보안정책이 보수적으로 적용되는 경향이 강해 신기술이 적용된 정보시스템 도입은 기존 체계와 융합되는데 적지 않은 시간이 소요되며, 데이터 공유 및 활용도 어려운 실정이다[3, 4, 5, 6].

2.2 보안 패러다임의 변화 필요성

정보시스템 보안은 통상 시스템이나 네트워크 장치에 정보보호제품(백신 소프트웨어나 방화벽 등)을 도입하여 조직 내부의 데이터를 외부의 위협으로부터 보호하거나 유출을 방지하는 개념으로, 국방 정보시스템의 보안정책은 일반적으로 시스템 도입 시에 ①대상시스템을 중요도에 따라 분류하고, ②보안수준에 따른 통제항목을 선정한 뒤, ③보안 통제항목에 따른 수단을 해당 시스템에 설치하는 순서로 적용된다[7, 8]. 즉 정보시스템 구축 시 시스템의 중요도에 따라서 보안수준이 결정되고 그에 따른 보안목표와 수준에 부합된 보안통제항목이 결정되는 방식이다. 이와 같은 시스템 중심 또는 네트워크 경계 중심의 보안은 보안담당자로 하여금 획일적·일률적인 보안정책을 적용하게 하여 관리를 용이하게 할 수는 있지만, 과도한 통제항목 적용으로 시스템 성능 발휘가 어렵거나 데이터 활용을 제한할 수 있다. 또한 활용도가 낮은 시스템(또는 보호할 데이터가 없는 시스템)에도 보안제품을 설치하여 예산이 낭비되는 등의 부작용이 발생할 수도 있다.

최근 제로 트러스트(Zero Trust)같은 보안 개념의 등장은 데이터 중심 보안정책 필요성을 부각시켜주고 있다. '아무것도 신뢰하지 않음'을 의미하는 제로 트러스트는 조직 내·외부의 모든 단말과 기기, 네트워크

등을 모두 신뢰할 수 없는 객체로 가정하고 자격이 증명된 단말만 허용된 데이터에 접근할 수 있도록 하는 개념으로 데이터 중심의 전사적 아키텍처를 바탕으로 구현된다[9].

스마트폰 등 모바일 기기의 보급으로 데이터 활용 중심 업무 문화가 확산됨에 따라 데이터의 공유가 활성화 되면서 정보보안에서의 보호대상과 영역도 점점 확장되고 있다[10]. 이에 대응하기 위해서는 일률적인 보안정책 적용에서 탈피하여 상대적이고 유연한 보안정책을 마련해야한다. 시스템 보호 중심의 보안에서 데이터 활용 중심의 보안정책으로 패러다임 변화가 필요한 시점이다.

2.3 데이터의 가치 평가

시스템 중심의 보안이 시스템을 중요도에 따라 분류하듯이 데이터 중심의 보안은 데이터의 가치를 평가하여 선별적으로 데이터를 보호할 필요가 있다. 조직에서 보호해야할 핵심이 되는 데이터는 보안을 위해 데이터관리시스템으로 전사적이고 체계적으로 관리되어야 한다[11].

조직에서 보유하고 있는 데이터를 자산으로 여기고 그것에 대한 가치를 측정하고 평가하는 다양한 연구가 진행되고 있다[12, 13, 14]. 데이터가 높은 가치의 평가를 받기 위해서는 데이터가 유용해야 하는데, 일반적으로 데이터의 유용성에 영향을 미치는 주요 요인은 <표 1>과 같은 고려요소에 의해 결정된다[14, 15]. 각 요소는 데이터를 활용하는 조직의 특성에 따라서 고려되는 비중이 달라진다. 예를 들면, 적시성(Timeliness)은 데이터가 최신 정보일수록 높은 가치로 평가하기 때문에 과거의 자료를 수집하는 조직보다 주식시장 동향과 같은 최신 정보를 분석하여 예측하는 조직에게 더 비중 있는 요소로 작용될 것이다.

<표 1> 데이터 가치를 높이는 주요 요인

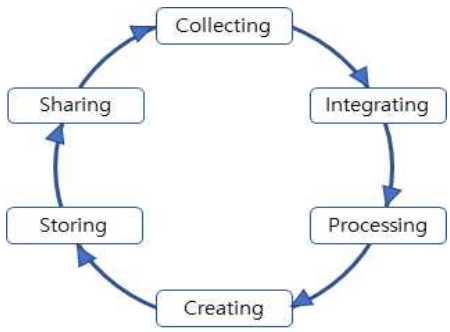
구 분	설 명
Completeness(완전성)	데이터세트는 편향되지 않아야 한다.
Consistency(일관성)	데이터는 미리 정의된 구분과 형식을 준수해야한다.
Accuracy(정확성)	데이터는 실 상황을 정확하게 묘사해야 한다.
Timeliness(적시성)	데이터가 최신 정보일수록 통상적으로 가치가 높을 수 있다.
Exclusivity(배타성)	데이터셋이 고유할수록 가치가 높아진다.
Liability and Risks (법적책임과 위험)	공유데이터와 관련된 잠재적 책임과 위험은 데이터 가치를 떨어뜨릴수 있다.
Accessibility(접근성)	사용자가 접근하기 용이한 데이터셋이 가치가 높다.

2.4 정보 수명주기 관리

정보는 업무를 수행하는 모든 단계에서 생성되며 특정한 단계화를 거쳐 데이터베이스에 저장된다. 정보수명주기 관리(Information Life-cycle Management, 이하 ILM)는 생명 순환주기 개념을 데이터 관리에 적용한 것으로 데이터도 '생성→활용→저장→폐기' 등 일련의 수명주기가 존재한다고 가정한다[16].

ILM 플랫폼은 통상 계층형 스토리지로 구성되며 장기간에 걸쳐 대량의 참조 데이터를 관리하여 조직 업무의 목표와 규정 준수 등 요구사항을 충족시킨다. 주어진 데이터가 시스템에서 어떻게 활용될 것인가 하는 최적화 결정은 스토리지 시스템이 적절한 시점에 올바른 정책을 적용할 수 있도록 어떤 데이터가 중요한지 가치를 평가함으로써 결정된다[17, 18].

ILM은 데이터에 시간 의존적인 값을 부여하여 정보의 가치에 따라서 데이터를 쉽게 저장하고 적절한 시점에 폐기하는 것을 원칙으로 한다. 하지만 본 논문에서는 데이터의 공유 및 활용 측면에서 (그림 1)과 같이 공유된 데이터가 폐기되지 않고 다른 시스템에서 다시 수집되어 활용되는 형태의 순환형 수명주기를 고려한다.



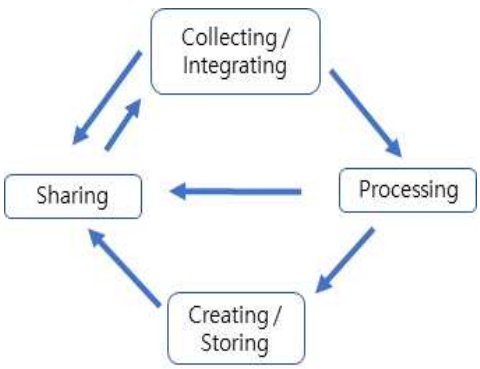
(그림 1) 데이터 수명주기 체인

3. 국방 환경의 데이터 활용 중심 보안 정책 요인분석

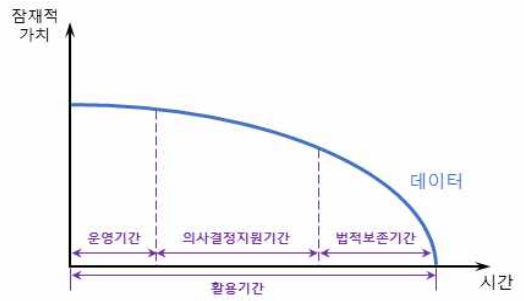
3.1 국방데이터와 수명주기 상태모델 분석

‘국방데이터’란 데이터베이스, 전자화된 파일 등 국방 기관 및 부대에서 생성 또는 취득하여 관리하고 있는 광 또는 전자적 방식으로 처리된 자료 또는 정보를 말한다[19]. 본 연구에서 데이터의 범위는 기존의 문서나 파일 위주의 데이터뿐만아니라 데이터베이스의 레코드 등 데이터에 대한 속성 값을 메타데이터로 관리할 수 있는 수준의 단위까지 포함하였다. 구체적으로는 각종 무기체계나 군용 장비에 탑재되어 수집되는 센서 데이터, 국방정보시스템(전장관리, 자원관리, M&S체계)의 데이터, 전자행정시스템의 문서파일 등으로 정형화된 데이터와 비정형 데이터를 통칭한다.

국방 AI 확산을 위해서는 다종ㆍ다량의 데이터가 공유되고 활용되어야 하는데 앞서 살펴본 순환형 수명주기 모델은 데이터가 저장된 후 공유되는 형태라서 적합한 모델로 볼 수 없다. 예를 들면 드론에서 수집된 비정형 데이터가 바로 공유되거나, 통합 및 처리 후 일정한 형식으로 구조화되어 데이터베이스에 저장되거나 공유될 수 있다. 이런 복합적인 형태를 수명주기 상태 모델로 구조화하면 (그림 2)와 같이 표현 될 수 있는데, 매 단계마다 데이터 상태 정보가 메타데이터로 작성되어 데이터관리정보시스템으로 관리되어야 하며[19], 가치가 없는 데이터는 식별하여 폐기해야 한다.



(그림 2) 국방데이터의 수명주기 상태 모델(안)



(그림 3) 시간 경과에 따른 데이터의 가치 변화

3.2 시간 경과에 따른 국방데이터 가치변화 분석

앞서 문헌 분석을 통해 데이터 가치에 영향을 주는 다양한 요인이 있음을 알 수 있었다. 그 중 ‘적시성’은 데이터에 시간 속성 값을 부여해 시스템으로 측정 가능한 주요 요인으로, 안보 상황을 다루는 국방에서도 정보의 가치 판단요소로 중요하게 작용될 수 있다.

시간 경과에 따라 데이터의 가치가 하락하는 경향을 문헌 및 사례분석을 통해 (그림 3)으로 제안한다. 여기서 데이터 가치를 정량적으로 측정하는 방법은 데이터의 활용도를 파악함으로써 나타낼 수 있으며, 사용자에 의한 조회수나 사용횟수 등으로 표현될 수 있다. (그림 3)에서 시간 축은 데이터가 활용되는 전체 ‘활용기간’으로 볼 수 있는데, 데이터의 본래 업무용도로 활용도가 가장 높은 ‘운영기간’, AI 등 데이터 분석을 위해 보다 장기간 사용되는 ‘의사결정지원기간’, 정해진 업무관련 법규나 제도에 따라 보관 및 백업이 필요한 ‘법적보존기간’ 등 세 구간으로 구분할 수 있다. 데이터의 유형이나 속성에 따라서 가치 하락 정도는 다를 수 있지만, 통상 앞의 ‘운영기간’과 ‘의사결정지원기간’이 경과하면 ‘법적보존기간’ 구간에서 데이터의 가치는 급락할 것으로 예상된다.

예를 들어 군부대 급식을 위해 식재료를 구매한다고 가정하자. 이 때 식재료에 대한 ‘구매 데이터’의 가치는 해당 식재료가 사용되는 날짜까지 단기간 가장 높을 것이며(운영기간), 이후에 급식담당자의 식단 및 예산배정을 위한 의사결정을 위해 데이터가 보관되어 일정기간 활용될 것이다(의사결정지원기간). 마지막으로 장시간이 경과하여 구매 데이터가 활용되지 않더라도 지출 증빙 등을 위해 관련 규정에 따라 일정기간 보존이 필요할 것이다(법적보존기간).

3.3 국방데이터 보호수준 분석

국방보안업무훈령이나 국방사이버안보훈령 등 정보시스템 및 데이터 관련 보안규정에서는 시스템의 중요도에 따라서 '가'급, '나'급, '다'급 수준으로 보호수준을 설정하고 있다. 이는 시스템이 중요 업무에 활용되는 정도와 작동 불가시 국방 업무수행에 미치는 영향도 등을 고려하여 설정된다[7, 8].

본 연구의 중점은 데이터 가치 기반의 보안정책 방향성 제시로써 각 보호수준에 따른 통제수단(데이터 암호화, 암호키 관리 등)을 별도로 제안하지는 않고 추후 연구로 남겨둔다. 따라서 기존 정책에서 제시하는 보호수준을 토대로 개념적으로 설정하였으며, 비밀데이터는 'A'급 보호수준, 평문 중 비공개 데이터는 'B'급 보호수준, 그 외 일반 자료는 'C'급 보호수준(또는 미보호)으로 정의한다.

4. 데이터 가치 기반 국방 보안정책 제안

데이터 가치 기반의 보안 정책(Data Value-based Security)은 데이터의 가치를 측정하여 보안 통제수단을 차등 적용함으로써 전체 데이터의 활용도를 높이는 것이다. 이를 위해 국방데이터의 가치 측정에 영향을 주는 요인을 알아보고, 데이터 가치기반의 보호수준 정립 및 업무수행 방안을 제안한다.

4.1 국방데이터 가치 측정에 영향을 주는 요인

국방데이터의 가치에 영향을 미치는 요인은 다양할 수 있지만, 본 연구는 보안정책에 대한 개념적인 방향 설정에 중점을 두어 데이터의 가치에 영향을 주는 요소를 <표 2>와 같이 단순화하였다.

첫째는 데이터의 시간 의존성이다. 일반적으로 시간 변화에 따라 데이터 값이 잘 변하지 않는 정적인(static) 속성의 데이터(부대위치, 군번 등)는 활용기간이 긴 반면, 값이 자주 변화하는 동적인(dynamic) 데이터(드론 위치정보 등)는 정적 데이터에 비해 수명이 짧다. 수명 주기가 짧은 데이터는 그 만큼 빈번한 가치 측정을 통해 보호수준을 낮춰 데이터 공유 및 활성화에 기여해야 한다. 둘째는 중요성으로 국방데이터는 크게 비밀과 평문 데이터로 나뉠 수 있으며, 대부분 최초 데이터 설계 단계에서 생성자에 의해 결정된다. 셋째는 공개성으로 공공기관의 정보공개에 관한 법률(정보공개법)에 근거한 비공개 대상의 정보를 포함할 경우 비공개 데이터로 분류하여 관리할 수 있으며, 비공개 사유가 종료될 경우 공개 데이터로 전환해야 한다. 마지막 보존기간은 개인정보보호법이나 기록물 보존기간 등 해당 소관 규정에 따라 정해지거나 특정 업무별로 목적에 맞게 설정될 수 있으며, 보존기간이 종료되는 데이터는 보호수준을 낮춰 공개하거나 폐기를 검토해야 한다.

<표 2> 국방데이터 가치 영향 요소

구 분	내 용	비 고
시간 의존성	정적/동적	부대주소 등(정적) 센서데이터 등(동적)
중요도	비밀/평문	국방보안업무훈령 등 근거
공개성	공개/비공개	정보공개법 근거
보존기간	1년, 3년, 5년 등	개인정보보호법, 기록물 보존기간 등에 근거

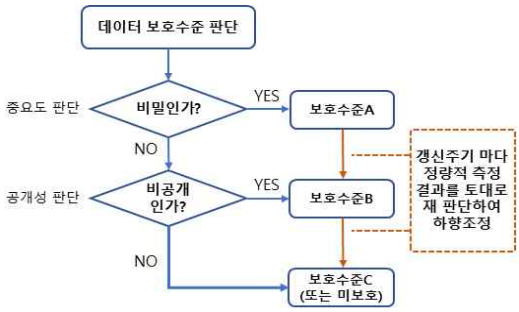
4.2 데이터 가치 기반의 보호수준 판단

데이터 가치를 기반으로 보호수준을 판단하기 위해서는 먼저 데이터관리정보시스템을 통해 조직 내에 어떤 데이터가 존재하는지, 어디에 위치하는지, 접근할 수는 있는지, 어떻게 사용하는지 등 데이터의 전반적인 현황을 알 수 있어야 한다.

데이터의 보호수준은 관리자에 의한 정성적 판단을 주된 기준으로 하되, 시스템 측정에 의한 정량적 방법을 종합적으로 고려한다. 정성적 방법은 데이터의 중요도와 공개성을 기반으로 데이터의 용도 및 활용 범위 등이 정해지는 준비 단계에서 관리자에 의해 판단된다. 보호수준은 A, B, C 등급으로 차등 구분하여 메타데이터로 관리하는데, 갱신 주기마다 데이터의 가치를 정량적으로 측정하여 보호수준을 재 판단한다. 갱신 주기 시점은 앞의 (그림 3) 데이터 활용기간에서 운영기간 종료시점과 의사결정지원기간 종료시점 등 데이터 가치 하락이 예상되는 시점으로 정할 수 있다.

정량적 측정 방법은 데이터정보관리시스템에 등록된 메타데이터를 통해 측정 대상 데이터의 활용기간 중 전체 사용량, 최근 사용빈도수, 데이터에 접근하는 사용자 수 등을 통해서 데이터의 가치를 추론할 수 있

다. 이는 과거의 사용기록을 통해 현재 데이터의 중요도를 추론할 수 있는데, 해당 데이터가 더 최근에 사용되거나 다른 데이터보다 더 많이 사용되는 경우 상대적으로 더 가치가 있다고 할 수 있다. 데이터 가치 기반의 보호수준 판단 방안을 도식화하면 (그림 4)와 같다.



(그림 4) 데이터 가치 기반의 보호수준 판단

4.3 데이터 가치 기반 보안 업무수행 방안

데이터 가치 기반의 보안정책 수행은 메타데이터를 통한 다양한 데이터 명세가 필요하다. 데이터 수집 전에 해당 데이터에 대한 속성을 정의하고, 데이터관리정보시스템을 통해 전체 수명주기 단계에서 현황이 관리되어야 한다.

또한, 데이터의 수집단계부터 데이터 가치를 정성적, 정량적 방법으로 종합 평가하여 보호수준을 결정하고, 갱신 시점마다 주기적인 재평가를 통해 보호수준을 재조정하여 불필요한 보안통제를 제거해야 한다. <표 3>은 데이터 가치 기반의 보안업무 수행을 위한 관련 업무 절차를 정리한 내용이다.

5. 결 론

본 연구에서는 국방혁신 4.0을 위한 인공지능 기반 첨단과학기술적용에 있어서 데이터 활용 중심의 보안을 위해 기존의 시스템 영역보안, 네트워크 경계 중심의 보안정책에서 벗어나 데이터 가치 기반의 보안정책으로의 전환을 제안하였다.

이를 위해 모든 데이터는 데이터관리정보시스템에 의해 중앙 관리되어야 하며, 중요도나 비공개성이 높은 데이터에 대해서는 높은 보호수준을 적용하고 반대로 군사적 활용도가 낮거나 비공개할 필요가 없는 데이터는 낮은 보호수준을 적용하여 다른 기관이나 민간에 공개하여 활용하거나 폐기를 고려해야 한다.

<표 3> 데이터 가치기반 보안을 위한 업무수행 절차

단 계	업 무 내 용
0.사전 준비	- 데이터의 속성(형태, 종류, 규모 등) 정의 - 데이터관리정보시스템을 통해 메타데이터 현황 관리
1. 수집/통합	- 국방데이터 해당여부 확인 - 법규상 준수해야할 정보 포함여부 확인 (비밀, 개인정보 등 비공개 정보)
2. 처 리	- 부적합 데이터 선별, 민감정보 처리 등
3. 생 성	- 메타데이터 생산 및 데이터관리정보시스템에 등록, 현행화
4. 저 장	- (법적)보존기간을 확인하여 보관 및 백업
5. 공 유	- 국방데이터 제공 및 공유 여부 결정
6. 폐 기	- 유용성 측면에서 데이터 가치를 판단하여 폐기여부 결정

본 연구의 한계로 데이터 가치 기반의 보안 정책 방향성만 제시하고 정량화된 측정 척도 등 세부적인 내용은 제시하지 못했다. 추가 연구로 다양한 유형의 국방데이터를 분류하여 데이터 유형을 정의하고, 정량화할 수 있는 요소 및 기준을 구체화해야 한다. 또한 데이터관리정보시스템을 통해 국방에서 보유하고 있는 국방데이터의 소재 및 연관데이터 정보 현황을 파악하고 분석하는 연구가 선행되어야 할 것이다.

데이터 가치 기반 보안정책 전환으로 데이터 중심 업무가 활성화되고 나아가 국방혁신 4.0의 AI기반 과학기술 도입에 도움이 될 것으로 판단된다. 또한 비용적인 부분에서도 작게는 보안에 투입되는 비용을 절약할 수 있을 뿐만 아니라 민간 분야에도 필요한 데이터를 제공함으로써 데이터 산업발전에도 기여할 수 있을 것이다.

참고문헌

[1] K. J. Lee, “A Consideration about the Status and the Development Plans of MND Smart Defense Innovation,” Journal of Information Technology Services, vol. 20, no. 1, pp. 1-9, Feb. 2021.

[2] 박홍순, “국방 AI·무인체계 추진전략 및 발전방안 고찰,” 대한산업공학회 춘계공동학술대회 논문

집, pp. 2670-2670, Jun. 2022.
[3] 국방부, 국방 인공지능 추진전략, 2021. 5.
[4] 국방부, 국방 인공지능(AI) 전략, 2022. 4.
[5] 국방부, 국방 무인체계 발전계획, 2023. 2.
[6] 국방부, 국방혁신4.0 기본계획, 2023. 3.
[7] 국방부, 국방보안업무훈령, 2022. 12.
[8] 국방부, 국방사이버안보훈령, 2019. 12.
[9] S. Rose et al., "Zero Trust Architecture," NIST Special Publication(SP) 800-207, National Institute of Standards and Technology, 2020.
[10] 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, Jul. 2018.
[11] H. Park, et. al., "A Study on the Implementation of Defense Technology Master Data Management System for Defense Technology Security," Journal of the Korea Institute of Information Security & Cryptology, vol. 31, no. 1, pp. 111-122, Feb. 2021.
[12] D. Moody and P. Walsh, "Measuring the Value of Information: An Asset Valuation Approach," European Conference on Information Systems(ECIS'99), pp.496-512, 1999.
[13] O. Kim et al., "Data Asset Valuation Model Review," The Korea Journal of BigData, vol. 6, no. 1, pp.153-160, Aug. 2021.
[14] T. Sung et al., "Models of Database Assets Valuation and their Life-cycle Determination," The Journal of the Korea Contents Association, vol. 16, no. 3, pp. 676-693, Mar. 2016.
[15] IMDA and PDPC, "Guide to Data Valuation for Data Sharing," 2019.
[16] P. Tallon et al., "Information life cycle management," Communications of the ACM, vol. 50, no. 11, pp. 65-69, Nov. 2007.
[17] Y. Chen., "Information valuation for Information Lifecycle Management," Proceedings of the Second International Conference on Autonomic Computing(ICAC'05), IEEE. pp. 135-146, Jun. 2005.
[18] H. Kim and C. Youn, "A Case Study for the Application of Storage Tiering based on ILM through Data Value Analysis," Journal of Digital Convergence, vol. 10, no. 8, pp. 159-172, Sep. 2012.
[19] 국방부, 국방데이터 관리 및 활용 활성화 훈령, 2021. 12.

〔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 국방부 정보화기획관실 국방소프트웨어정책담당
2020년 11월~현재 국방부 국방개혁실 과학기술혁신담당
email : heungsoon.park@gmail.com