https://doi.org/10.33778/kcsa.2024.24.2.047

인공지능의 학습 특성을 고려한 개인정보 라이프 사이클 모델

장 재 영*, 김 종 민**

요 약

현행 개인정보 라이프 사이클 모델은 전통적인 시스템에 맞추어져 있어서 인공지능의 개인정보 흐름 파악과 효율적인 보호 대책 수립에 적합하지 않은 문제점이 있다. 따라서 본 논문은 인공지능에 적합한 개인정보 라이프 사이클 모델을 제시하는 것을 목적으로 한다. 본 논문은 수집-보유-학습-이용-파기·정지 단계와 파기·정지를 위한 재학습 프로세스가 포함된 인공지능의 학습 특성을 고려한 개인정보 라이프 사이클 모델을 제시했다. 이후 기존 모델(개인정보 영향평가와 ISMS-P 모델)과 본 논문에서 새로 제시한 모델의 성능을 평가했다. 이를 통해 새로 제안한 모델이 기존 모델보다 인공지능의 개인정보 라이프 사이클의 설명에 우수한 특성을 가지고 있음을 증명했다.

Personal Information life Cycle Model Considering the Learning Characteristics of Artificial Intelligence

Jaeyoung Jang*, Jong-Min Kim**

ABSTRACT

The traditional personal information life cycle model, primarily tailored to conventional systems, is inherently unsuitable for comprehending the nuances of personal information flow within artificial intelligence frameworks and for formulating effective protective measures. Therefore, this study endeavors to introduce a personal information life cycle model specifically designed for artificial intelligence (AI). This paper presents a personal information life cycle model suitable for artificial intelligence, which includes the stages of collection, retention, learning, use, and destruction/suspension, along with the re-learning process for destruction/suspension. Subsequently, we compare the performance of these existing models (such as personal information impact assessment and the ISMS-P model) with the newly proposed model. This underscores the superiority of our proposed model in comprehensively understanding the personal information flow in AI and establishing robust protective measures.

Key words : 개인정보, 인공지능, 생명 주기, 라이프 사이클, Personal Information, Privacy, Artificial intelligence, Life cycle

접수일(2024년 04월 24일), 게재확정일(2024년 04월 25일)

* 한국인터넷진흥원(주저자, 교신저자)
** 동신대학교/정보보안학과(공동저자)

1. 서 론

최근 컴퓨팅 파워 증대와 알고리즘의 발전으로 대규모 데이터 처리가 필요한 인공지능 기술이 급격히 발전하고 있다. 김도원 등에 따르면 OpenAI 사가 최근에 출시한 GPT-4는 미국 변호사 시험에 상위 10%로 합격할 정도로 성능이 향상됐다고 한다[1]. 인공지능은 이제 발전의 초기 단계라는 측면에서 향후 우리 사회에 더욱 커다란 영향을 끼칠 것으로 보인다[2].

이러한 인공지능은 데이터 처리 방식에서 기존 시스템과 차이가 있다. 기존 시스템은 사전에 작성한 명시적 규칙에 따라 데이터를 처리(processing) 하지만, 인공지능은 패턴을 학습(learning)하는 방식이다. 인공지능의 이러한 패턴 학습 방식은 기존의 시스템 보다 유연하고 정확한 의사 결정을 가능하게 한다[3]. 인공지능의 기술적 발전은 우리 사회의 다양한 부분을 발전시킬 것으로 예상되지만 대규모 데이터 처리로 인한 새로운 유형의 개인정보 침해(privacy invasion)와 같은 부작용 발생 가능성도 제기되고 있다[4].

많은 영역에서 개인정보는 침해 방지를 위해 라이프 사이클 모델을 만들어 보호하고 있다. 그러나 기존의 개인정보 라이프 사이클 모델은 전통적인 정보 처리 시스템에 기반하고 있어서 새로운 기술인 인공지능의 개인정보 흐름 파악 및 효율적인 보호 대책 수립에는 적합하지 않은 문제점이 제기되고 있다[5].

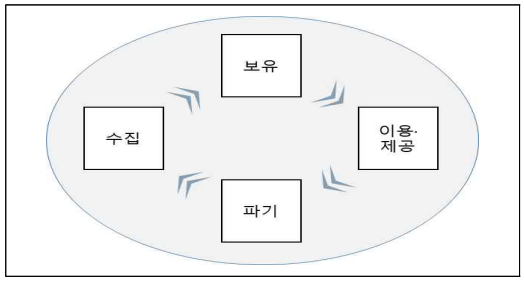
구체적으로 살펴보면 기존의 개인정보 라이프 사이클 모델은 개인정보의 생성이나 추론 등의 인공지능의 학습과 이로 인해 발생하는 개인정보 처리 및 보호 측면의 다양한 요구를 고려하는 데에 한계가 있다[6]. 특히 기존의 모델은 수집 단계를 동의 기반으로 하고 있다. 이러한 방식은 인공지능에서 사용하고 있는 공개된 개인정보의 수집을 수용하지 못하는 한계가 있다[7]. 또한 기존의 모델은 개인정보가 즉시 차단 및 삭제가 가능하다는 것을 전제하고 있다. 그러나 인공지능은 처리가 아닌 학습 방식이기 때문에 알고리즘에서 특정한 개인정보 만을 즉시 차단, 정지, 정정, 파기하는 것이 기술적으로 용이하지 않다. 이러한 기존 모델의 한계는 인공지능에 적합한 새로운 개인정보 라이프 사이클 모델의 개발을 요구하고 있다.

따라서 본 논문은 기존의 개인정보 라이프 사이클 모델과 차별화된 인공지능의 학습 특성을 고려한 새로운 개인정보 라이프 사이클 모델을 제안하고자 한다. 이를 위해 2장은 기존 개인정보 라이프 사이클 모델을 설명하고 이들 모델의 한계를 제시한다. 3장은 인공지능 라이프 사이클 마련을 위한 요구사항을 도출한다. 4장은 인공지능의 학습 특성을 고려한 새로운 모델을 제시한다. 5장은 기존 모델과 새로 제안한 모델을 비교한다. 6장은 본 연구의 결론을 제시한다.

2. 개인정보 라이프 사이클 모델

2.1 개념

개인정보 라이프 사이클이란 개인정보도 사람과 같은 생명 주기가 있다는 관점에서 출발한다. 사람에게는 생노병사(生老病死)가 있다면 개인정보에게는 수집에서 파기까지의 과정에서 일정한 단계가 존재한다고 간주한다[8]. (그림 1)에 개념과 항목을 기술했다.



(그림 1) 개인정보 라이프 사이클 모델 개념

본고에서는 개인정보 라이프 사이클이 대표적으로 사용되고 있는 개인정보 영향평가와 ISMS-P (Personal Information & Information Security Management System)을 중심으로 개인정보 보호 라이프 사이클 모델에 대해 살펴보고자 한다.

2.2 개인정보 영향평가 모델

개인정보 영향평가에서는 개인정보 라이프 사이클을 수집, 보유, 이용·제공, 파기의 4단계로 구분하고 있다[9]. 수집 단계는 정보주체의 개인정보를 취득하

는 단계로 회원 가입, 서면 신청, 민원 접수 등의 형태로 구성되어 있다. 보유 단계는 수집한 개인정보를 기술적·관리적 조치 등으로 안전하게 관리하는 단계이다. 정보주체의 개인정보 열람·정정권 등의 내용을 포함하고 있다. 이용·제공 단계는 개인정보를 목적에 따라 이용하거나 제3자에게 제공하는 단계이다. 파기 단계는 수집 및 이용 목적이 달성되면 개인정보를 파기하는 단계이다. <표 1>은 개인정보 영향평가의 개인정보 라이프 사이클의 주요항목을 정리한 것이다[10].

<표 1> 개인정보 영향평가 라이프 사이클 주요항목

단계	주요 항목
수집	개인정보 수집의 적합성, 동의 받는 방법의 적절성
보유	보유기간 산정
이용·제공	개인정보 제공의 적합성, 목적 외 이용·제공 제한, 제공시 안전성 확보, 위탁 사실 공개, 위탁 계약, 수탁사 관리·감독
파기	파기 계획 수립, 분리보관 계획 수립, 파기대장 작성

2.3 ISMS-P

ISMS-P는 정보보호 및 개인정보보호 관리체계로 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 ISMS-P 인증 기준에 적합한지를 검증하는 제도이다. 이 인증 기준에는 개인정보 라이프 사이클을 수집, 보유·이용, 제공, 파기, 권리보호 단계로 구분하고 있다. 개인정보 영향평가 모델은 보유, 이용·제공으로 구분하고 있으나 ISMS-P는 보유·이용을 하나의 단계로 하고 있고, 제공을 독립된 단계로 구분하고 있다. 또한 개념상으로는 라이프 사이클과는 관계가 약하나 권리보호를 개인정보 처리 단계에 포함하고 있다. <표 2>는 ISMS-P의 개인정보 라이프 사이클의 주요 내용을 정리한 것이다[11].

<표 2> ISMS-P 라이프 사이클 주요항목

단계	주요 항목
수집	개인정보 수집·이용, 개인정보 수집 제한, 주민등록번호 처리 제한, 민감정보 및 고유식별정보의 처리 제한, 개인정보 간접수집, 영상정보처리기기 설치·운영, 마케팅 목적의 개인정보 수집·이용
보유·이용	개인정보 현황관리, 개인정보 품질보장 이용자 단말기 접근 보호, 개인정보 목적 외 이용 및 제공, 가명정보 처리
제공	개인정보 제3자 제공, 개인정보 처리 업무 위탁, 영업의 양도 등에 따른 개인정보 이전, 개인정보 국외이전
파기	개인정보 파기, 처리목적 달성 후 보유 시 조치
권리보호	개인정보 처리방침 공개, 정보주체 권리보장, 정보주체에 대한 통지

2.4 개인정보 라이프 사이클의 문제점

개인정보 영향평가나 ISMS-P와 같은 개인정보 라이프 사이클은 기존의 정보처리 시스템의 특성에 맞추어 개발되었다. 따라서 학습 기반의 생성과 추론을 주목적으로 하는 인공지능의 개인정보 보호에는 몇 가지 문제점이 있다.

첫째, 기존의 수집 단계는 공개정보의 수집을 고려하지 않았다. 따라서 공개 정보도 라이프 사이클에 반영할 필요가 있다. 둘째, 기존 모델은 추론을 통한 새로운 개인정보의 생성을 고려하지 않았다. 개인정보 영향평가 등에서는 '생성'을 설명하고 있지만 이는 서비스 제공 과정에서 수집한 정보라고 보는 것이 타당하다. 셋째, 보유 단계에서는 인공지능의 학습 알고리즘의 블랙박스와 적대적 학습(adversarial learning)과 같은 인공지능 공격에 대한 대책이 고려되지 않았다. 마지막으로 목적 달성 시 또는 이용자가 원하는 경우 개인정보를 파기, 삭제, 정정해야 하나 인공지능은 알고리즘에 개인정보가 학습되어 있는 방식이므로 특정한 개인정보를 즉시 파기, 삭제, 정정하는 것이 기술적으로 용이하지 않다.

이렇듯 인공지능 시스템은 학습 특성으로 인해 제한 사항이 다수 존재한다. 따라서 개인정보 주체의 자기결정권의 보호 및 정보처리자의 정확한 개인정보 처리를 위해 인공지능에 적합한 개인정보 라이프 사이클 모델을 만들 필요가 있다[12].

3. 인공지능의 개인정보 라이프 사이클 모델 요구 사항

3.1. 기술적 측면의 요구 사항 도출

인공지능은 입력 데이터와 출력 값으로 둘의 관계를 추론하는 방식이다. 따라서 인공지능의 학습은 개인정보가 온전히 데이터베이스에 저장되는 것이 아니라 인간의 학습 과정과 같이 인공지능 알고리즘의 특정 공간에 수치화되어 있다. 이러한 인공지능의 학습 특성이 라이프 사이클 단계에 반영되어야 한다.

또한 인공지능은 학습 특성 외에 인공지능을 보호하기 위한 각종 보호 요소가 필요하다. 특히 현재까지 알려진 인공지능에 대한 공격 방식인 표적 공격(target)과 비표적 공격(non-target)과 모델 학습 공격 기법인 회피 공격(evasion), 백도어(back door), 중독 공격(poisoning), 전도공격(model inversion), 추론공격(model extraction), 모델 정보 보유 정도에 따른 화이트 박스(white box)와 블랙 박스(black box) 공격으로부터 인공지능을 보호할 요소들이 고려되어야 한다[13].

인공지능은 개인정보를 파기, 정정·삭제, 정지할 경우에도 학습을 통해 파기 등을 해야 한다. 그러나 현행 기술로는 이용자가 삭제 등을 요구할 경우 모델에서 해당 데이터를 즉시 삭제하기가 용이하지 않다. 따라서 인공지능의 학습 특성으로 인한 기술적 한계를 극복할 수 있는 라이프 사이클 모델을 마련해야 한다.

인공지능은 수집한 개인정보를 서비스 제공자가 운영하는 개인정보 처리 시스템에 보관 및 관리한다. 이 경우 개인정보의 안전한 보유를 위해 암호화나 접근통제와 같은 기술적 조치나 보유 기간의 산정, 접근권한 관리와 같은 관리적 방안을 고려해야 한다.

<표 3>은 인공지능을 위한 개인정보 라이프 사이클 모델의 기술적 요구 사항을 제시한 것이다. 인공지능은 학습 특성과 블랙박스 문제, 인공지능에 대한 적대적 학습(adversarial learning) 문제가 있다. 따라서 이러한 문제를 고려한 모델이 마련되어야 한다.

<표 3> 기술적 측면의 요구 사항

대분류	소분류	요구 사항
수집·이용·제공 단계		학습 특성 고려
보유 단계	기술적	▪ 암호화, 접근통제 적용 ▪ 공격자 목표 방어 - 표적 공격(target) - 비표적 공격(non-target) ▪ 모델 학습 방어 - 회피 공격(evasion) - 백도어(back door) - 중독 공격(poisoning) - 전도공격(model inversion) - 추론공격(model extraction) ▪ 모델 정보 보호 방안 마련 - 화이트 박스(white box) - 블랙 박스(black box)
	관리적	보호기간 산정, 접근 권한 관리

3.2 서비스 측면의 요구 사항 도출

인공지능의 핵심은 데이터와 학습이다. 따라서 최대한 많은 데이터를 수집해 학습에 이용해야 한다. 이러한 이유로 인해 인공지능은 기존 서비스에서 주로 활용했던 정보주체의 정보(ID/PW, 식별정보, 연락처, 주소 등)와 서비스 제공 과정에서 수집한 정보(IP 정보, 쿠키, 기기 정보, 서비스 이용 로그 기록, 위치정보) 외에 온·오프라인에 공개된 문자, 음성, 화상, 영상 정보 등을 인공지능 학습에 적극 활용하고 있다[14].

또한 인공지능은 학습을 통해 생성 또는 예측한 데이터를 이용·제공한다. 이러한 정보는 처리 또는 학습하지 않은 단순한 제공이 아닌 생성 또는 추론한 데이터의 제공이다. 따라서 생성·추론을 라이프 사이클 단계에 고려해야 한다.

아울러 현행 라이프 사이클에서는 학습된 개인정보의 파기를 위해서는 알고리즘 자체를 삭제해야 한다. 그러나 특정한 이용자를 위해 서비스 전체를 삭제하는 것은 현실적이지 못하다. 이러한 문제점은 정보주체의 요구에 따른 개인정보의 정정·삭제, 정지, 수정의 경우에도 모두 공통적으로 나타나는 현상이다. 따라서 새로운 라이프 사이클 모델은 서비스의 편의성과 유용성을 저해하지 않으면서 이용자의 권리를 보호하는 방법을 마련해야 한다. <표 4>은 서비스 측면의 요구 항목들을 정리한 것이다.

<표 4> 서비스 측면의 요구 사항

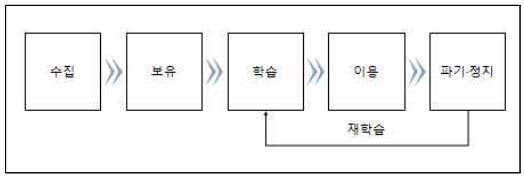
분류	요구 항목
수집 단계	정보주체, 서비스, 공개정보 수집 체계 구현
보유 단계	-

이용 단계	생성, 추론 프로세스 구현
파기 단계	파기, 정정·삭제, 정지 프로세스 구현

4. 인공지능에 적합한 개인정보 라이프 사이클 모델

4.1 새로운 라이프 사이클 모델

본 장에서는 인공지능의 학습 특성을 고려한 새로운 개인정보 라이프 사이클 모델을 제시하고자 한다. 본고에서 제시하는 새로운 모델은 3장의 요구 사항을 고려해 수집-보유-학습-이용-파기·정지 단계로 구성했다. 또한 현행 인공지능 기술 상 파기 등을 위해서는 해당 개인정보가 모델에 학습되지 않도록 재학습할 필요가 있으므로 재학습을 피드백(feedback) 방식으로 모델에 포함시켰다. 모델의 구성 및 단계는 (그림 2)와 같다.



(그림 2) 인공지능의 학습 특성을 고려한 개인정보 라이프 사이클 모델

4.2 라이프 사이클 단계별 구성 요소

4.2.1 수집 단계

수집 단계는 학습을 위한 데이터 수집 과정이다. 이 단계에서 수집하는 정보는 ①정보주체, ②서비스 이용 과정 외에, ③ 공개정보의 수집도 포함한다. 공개된 정보는 인터넷은 물론 Drone과 CCTV(closed circuit television)와 같은 영상 기기에서 수집한 정보도 포함한다. 개인정보의 종류에는 개인 식별정보, 개인관련 정보, 고유 식별정보, 신용 및 금융정보, 위치정보는 물론 생체인식정보나 건강정보와 같은 민감정보 등도 포함한다. 가명 또는 익명화된 정보도 포함한다[6].

4.2.2 보유 단계

보유는 수집한 데이터가 파기되기까지의 전 과정을 포함한다. 다만 프로세스 상으로 수집 다음 단계에 포함시키는 것이 개인정보의 안전한 이용을 위한 기술적·관리적 방안 적용에 효율적이라 판단된다. 보유 단계에서는 알고리즘의 안전성 확보를 위한 접근 통제나 암호화 등을 수행한다. 인공지능의 경우 target/no on-target attack, adversarial learning attack, white/black attack에 취약하므로 이러한 취약점과 공격에 대응하는 것도 보유 단계의 역할이다[15].

4.2.3 학습 단계

학습 단계는 수집한 데이터로 알고리즘을 학습시키는 단계이다. 학습 단계에는 개인정보 자체가 학습에 사용될 수 있다. 해당 정보가 가명 또는 익명 처리된 후 학습될 수 있다. 개인정보 또는 개인관련 정보가 아닌 것으로 판단했으나 학습을 통해 다른 데이터들과 연계·결합하여 개인정보 또는 개인관련 정보가 될 수 있다. 학습 과정에는 학습의 안전성과 학습 결과의 검증 작업이 포함된다. 학습의 안전성은 가명정보의 식별 또는 재식별 위험성 검토 과정 등이 해당한다. 학습 결과 검증은 테스트 데이터를 활용한 검증 작업이 대표적이다.

4.2.4 이용 단계

이용·생성·추론 단계는 학습을 완료한 알고리즘으로부터 개인정보를 서비스에 이용하는 단계이다. 인공지능에서도 단순한 이용이 있을 수 있다. 또한 학습 과정에서 개인정보는 아니었으나 수집에 사용되지 않은 개인정보가 생성되거나 추론될 가능성도 있다.

또한 학습 과정에서 과적합(overfitting)이 발생하거나 딥 뉴럴 네트워크(deep neural network)의 hidden layer가 다수인 경우 인공지능은 훈련 세트(training set)에 포함한 개인정보를 기억(memorized)할 수 있다[16]. 따라서 단순한 개인정보의 제공, 추론, 생성된 개인정보의 제공이 이 단계에 해당한다.

4.2.5 파기·정지 단계

본 단계는 크게 ①파기, ②정정·삭제, ③정지로 구분할 수 있다. 그러나 알고리즘에 학습된 개인정보는 즉시 삭제가 되지 않기 때문에 크게 두 단계로 나누어 구성할 필요가 있다. 첫째는 개인정보에 대한 특정한 처리가 필요한 경우 해당 개인정보가 생성되지 않도록 모델을 재학습 하는 단계이다. 파기, 정정·삭제가 이 단계에 해당한다. 둘째는 개인정보를 제공하지 말아야 할 경우 해당 데이터에 대한 필터링 처리를 하는 단계이다. 정지가 이 단계에 해당한다.

4.2.6 각 단계별 구성 요소

인공지능을 위한 새로운 개인정보 라이프 사이클 모델의 구성 요소는 <표 5>와 같다. 정정·파기 등의 단계에는 재학습 프로세스가 포함되어 있다.

<표 5> 각 단계별 구성 요소

분류	구성 요소
수집 단계	정보주체 제공 / 서비스 이용 과정 수집 / 공개정보 수집
보유 단계	저장 / 보유 / 안전조치
학습 단계	학습 / 검증
이용 단계	이용 / 생성 / 추론
파기·정지 단계	파기·정정·삭제(재학습) / 정지

5. 모델 성능 비교

3장의 인공지능 개인정보 라이프 사이클 모델 요구사항을 기존의 개인정보 영향평가 ISMS-P과 새로 제안한 모델과 비교했다. <표 6>은 각 모델의 성능을 비교한 결과이다. 3장의 요구 사항을 기준으로 했을 때 인공지능의 학습 특성을 고려한 개인정보 라이프 사이클 모델이 가장 많은 요구 사항을 충족하는 것을 알 수 있다.

<표 6> 모델간 성능 비교

측면	단계	내용	영향평가/ISMS-P	신규 모델
기술적	학습 특성		-	○
측면	기술적	암호화, 접근통제 적용	○	○
		인공지능 보안	-	○
	관리적		○	○
서비스 측면	수집 단계	정보주체	○	○
		서비스 제공	○	○
		공개정보 수집	-	○
	이용 단계	이용	○	○
		생성	-	○
		추론	-	○
	파기·정지 단계	파기	△	○
		정정·삭제	△	○
		정지	△	○

6. 결 론

이 논문은 인공지능에 적합한 개인정보 라이프 사이클 모델을 제시하는 것을 목적으로 한다. 이를 위해 본 논문은 기존의 개인정보 라이프 사이클 모델(영향평가 모델, ISMS-P 모델)을 살펴 본 후 이러한 모델이 인공지능 서비스에 적용했을 때 어떠한 문제점이 있는지 살펴보았다. 이후 인공지능에 적합한 개인정보 라이프 사이클 모델을 위한 기술 및 서비스 측면의 요구 사항을 도출했다. 이를 토대로 인공지능의 학습 특성을 고려한 개인정보 라이프 사이클 모델을 제시했다. 이후 요구 사항에 대해 기존 모델과 새로 제시한 모델의 충족 여부를 비교했다. 이를 통해 새로운 모델이 인공지능의 개인정보 라이프 사이클 설명에 보다 우수한 성능을 가지고 있음을 증명했다.

본 논문은 인공지능 학습과 개인정보 보호의 영역에서의 인공지능 서비스의 체계적 관리 가능성을 높였다는 측면에서 학문적 의의가 있다. 본 연구를 계기로 개인정보나 보안 분야에서 인공지능 학습에 대한 학문적 관심이 높아질 수 있기를 기대해 본다.

참고문헌

[1] 김도원, 김성훈, 이재광, 박정훈, 김병재, 정태인, 최은아, “ChatGPT(챗GPT) 보안 위협과 시사점,” KISA INSIGHT, Vol. 2023, No. 3, pp. 1-26, 2023.

[2] D. E. O'Leary, "Artificial intelligence and big data," IEEE intelligent systems, Vol. 28, No. 2, pp. 96-99, 2013
[3] I. H. Sarker, "Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions," SN Computer Science Vol. 2, No. 6, pp. 1-20. 2021.
[4] 개인정보보호위원회, "인공지능 시대 안전한 개인정보 활용 정책방향", pp. 1~23, 2023.
[5] 이아람. "개인정보 생명주기 (Lifecycle) 에 따른 인공지능 (AI) 개인정보보호," 한국통신학회지 (정보와통신), Vol. 39, No. 12, pp. 3-7, 2022.
[6] 개인정보보위원회, "인공지능 시대 안전한 개인정보 활용 정책방향," 2023.
[7] 김현경. " 공개된 개인정보의 법적 취급에 대한 검토—AI 학습용 데이터로서 활용방안을 중심으로—," 미국헌법연구, Vol. 34, No. 1, pp. 157-192. 2023.
[8] V. S. Bhamidipati, S. De, "A Risk Based Approach for Privacy Compliant Machine Learning Lifecycle," In 2022 2nd International Conference on Intelligent Technologies (CONIT) (pp. 1-6). IEEE. 2022.
[9] J. Y. Jang, T. H, Park, & B. S. Kim, "The life cycle model considering legal and technical characteristics of personal data," The Journal of Society for e-Business Studies, Vol. 17, No. 3, pp. 43-60, 2012.
[10] 개인정보보호위원회, 한국인터넷진흥원, "개인정보 영향평가 수행안내서," 2020.
[11] 과학기술정보통신부, 개인정보보호위원회, 한국인터넷진흥원, "정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 안내서," 2023
[12] J. Jung, J. Yang, "A Study on Data Compliance Measures of Digital Healthcare Service-Focusing on Personal Information Lifecycle." The Journal of Korea Institute of Information, Electronics, and Communication Technology, Vol. 15, No. 2, pp. 134-143, 2022.
[13] R. R. Wiyatno, A. Xu, O. Dia, & A. De Berker, "Adversarial examples in modern machine learning: A review," arXiv preprint arXiv:1911.05268., 2019
[14] 네이버, "네이버 개인정보 처리방침(ver.11.5)," https://policy.naver.com/policy/privacy.html
[15] N. Carlini, F. Nicholas, E. Wallace, M. Jagielski, A. Herbert-Voss, K. Lee, A. Roberts, T. Brown. "Extracting training data from large language models." 30th USENIX Security Symposium (USENIX Security 21). 2021.
[16] H. Hu, Z. Salcic, L. Sun, G. Dobbie, P. S. Yu, X. Zhang, "Membership inference attacks on machine learning: A survey," ACM Computing Surveys (CSUR), Vol. 54, No. 11s, pp. 1-37. 2022.

〔저 자 소 개〕

장 재 영 (Jaeyoung Jang)
2023년 8월 연세대학교 정보시스템학 박사(정보보호 전공)
2003년 8월 ~ 현재 한국인터넷진흥원
2023년 9월 ~ 현재 연세대학교 강사
2024년 3월 ~ 현재 고려대학교 겸임 교수

email : jyjang31@gmail.com

김 종 민 (Jong-Min Kim)
2015년 산업보안학박사
현 재 동신대학교 정보보안학과 교수

email : dyuo1004@dsu.ac.kr