디지털산업정보학회 논문지 제18권 제1호-2022년 3월
http://dx.doi.org/10.17662/ksdim.2022.18.1.037

마이데이터 모델을 활용한 개인정보 이용내역 통지 방안 연구

김 태 경*·정 성 민**

A Study on Notification Method of Personal Information Usage History using MyData Model

Kim Taekyung·Jung Sungmin

〈Abstract〉

With the development of the 4th industry, big data using AI is being used in many areas of our lives, and the importance of data is increasing accordingly. In particular, as various services using personal information appear and hacking attacks that exploit them appear in various ways, the importance of personal information management is increasing. Personal information must be managed safely even when collecting, retaining, using, providing, and destroying personal information, and the rights of information subjects must be protected. In this paper, an analysis was performed on the notification of usage history during the protection of the rights of information subjects using the MyData model. According to the Personal Information Protection Act, users must be periodically notified of the use of personal information, so we notify each individual of the use of personal information through e-mail or SNS once a year. It is difficult to understand and manage which company use my personal information. Therefore, in this paper, a personal information usage history notification system model was proposed, and as a result of performance analysis, it is possible to provide the controllability, availability, integrity, source authentication, and personal information self-determination rights.

Key Words : MyData Model, Privacy Information, Usage history, Notification

Ⅰ. 서론

개인정보의 중요성이 더욱 증대됨에 따라 개인정보를 안전하게 관리하고 사용하기 위한 다양한 제도와 법률들이 실행되고 있으며, 또한 이러한 개인정보들을 활용한 다양한 서비스들이 개발되고 있다. 특히 4차 산업혁명에 필요한 새로운 서비스의 개발을 위해 중복 규제를 없애고 개인과 기업이 정보를 활용할 수 있는 폭을 넓히기 위해 2020년 1월 개인정보보호법, 정보통신망법, 신용정보법 등 데이터 3법 개정안[1]이 통과됨에 따라 개인정보에 관한 개인정보 자기결정권을 강화하면서 개인정보를 활용할 수 있는 방안이 생기게 되었다[2].

* 명지전문대학 인터넷보안공학과 교수(제1저자)
** 명지전문대학 인터넷보안공학과 교수(교신저자)

기존에는 개인정보를 활용하기 위하여 개인을 식별할 수 없도록 가명 처리하는 개념이 도입되었으나 가명처리의 수준을 높이면 데이터의 활용 가치가 낮아지게 되고, 가명처리 수준을 낮추면 개인이 식별 가능성이 증가하여 개인정보를 활용하는 데 한계가 존재하였다. 그러나 최근에는 정보 주체의 요청으로 데이터를 수집하고 활용하는 마이데이터 서비스가 도입되었다. 마이데이터는 정보 주체 동의를 받기 때문에 규제 이슈에서 자유롭고, 원본 데이터를 그대로 사용할 수 있어 활용 가치도 높은 장점이 있으며, 본인에 대한 데이터는 본인이 주인이며, 본인이 관리한다는 인식 확산과 함께, 스마트폰 대중화 등의 마이데이터 서비스가 빠르게 발전할 수 있는 여건이 조성되었다[3]. 여기서, 마이데이터란 정보 주체가 본인 정보를 적극 관리·통제하고 이를 신용, 자산, 건강관리 등에 주도적으로 활용하는 것으로, 자료전송 요구권 즉 정보 주체가 정보제공자로 하여금 본인이 원하는 서비스를 제공받기 위하여 데이터의 전송을 요구하는 권리가 핵심 개념이라고 할 수 있다[3, 4].

마이데이터의 도입으로 다양한 마이데이터 서비스가 도입되고 있는데, 특히 금융 분야에서 마이데이터 서비스가 활발하게 도입되고 있다. 하나의 앱에서 고객의 데이터를 수집하고, 자산 및 소비 패턴을 분석하여 최적의 금융상품을 추천하는 방식이다. 그러나 이러한 마이데이터 서비스를 이용하기 위해서는 금융사의 고객 정보를 이용해야 하므로 개인정보 유출 우려도 있으나, 마이데이터 서비스는 보안환경을 안정적으로 구축하여 운영하고 있다. 데이터의 전송 시 API 방식으로 안전하게 개인신용정보를 전송하며, 강력한 본인인증 방식으로 개인신용정보를 보호하고 있다. 또한, 24시간 보안관제를 통해 실시간 모니터링을 통해 침해위협 조기대응 체제를 구축하고, 신용정보관리·보호인을 통한 개인신용정보 보호 계획 수립 및 시행을 하며, 물리적 보안설비를 구축하고 기술적 보안 사항을 수립하여 안전하게 운용하고 있어 은행, 카드, 보험, 증권, 통신 등에 흩어져 있는 개인의 금융정보를 일괄 수집하여 고객이 알기 쉽게 통합하여 제공하는 서비스의 활성화가 예상된다.

그러나, 현재 각각의 서비스에서 사용되고 있는 내 개인정보들이 어떠한 회사에서 어떤 정보들이 활용되고 있는지에 대한 파악 및 관리는 어려운 실정에 있다. 개인정보 보호법 제39조의 8(개인정보 이용내역의 통지)에 의하면 정보통신서비스 제공자 등으로서 대통령령으로 정하는 기준에 해당하는 자는 제23조, 제39조의 3에 따라 수집한 이용자의 개인정보의 이용내역을 주기적으로 이용자에게 통지하여야 한다고 되어 있다. 이에 따라 개인정보를 수집하는 기업에서는 수집한 개인정보의 이용내역에 대해 주로 이메일이나 SNS를 통해 각 개인에게 매년 전달하는데, 개인의 입장에서는 제공되는 정보를 파악하고 관리하는 것이 현실적으로 어려운 문제점이 있다.

따라서 본 논문에서는 마이데이터 모델을 활용하여 각 개인이 개인정보 이용내역 통지에 대한 확인 및 관리할 수 있는 방안에 대한 연구를 수행하였다. 2장에서는 마이데이터 모델에 대한 분석을 수행하였으며, 3장에서는 개인정보 이용내역 통지 모델을 제안하고, 제안한 모델에 대한 효용성을 제시하였다. 마지막으로 4장에서는 본 연구의 결론으로 구성하였다.

Ⅱ. 마이데이터 모델

2.1 마이데이터 수집 및 저장기술

데이터를 수집하는 방법으로 크게 두 가지 방식이 존재하며, 그 방법으로는 스크래핑 방식과 API 방식이 있다. 스크래핑은 인터넷 화면에 보이는 내용 중 필요한 내용을 추출 및 저장하는 방식으로, 해당 방식은 홈페이지마다 틀을 만들어야 해서 표준성이 떨어지는 문제가 있다. 이 방식은 개별 정보 보관 기관

이 제공하는 웹 서비스의 현재 버전에 맞추어 스크래핑 프로그램을 제작하고 유지, 보수해야 하기 때문에 프로그램 코드의 재사용성이 낮고, 스크래핑의 대상이 되는 웹사이트 등의 구조가 변경되거나 서비스를 중지하는 등의 상황이 벌어졌을 때 즉시 대처할 수 없어 데이터의 정확성과 연속성을 확보하기가 쉽지 않다. 또한, 스크래핑 주기나 범위를 데이터를 요청하는 클라이언트의 편의에 맞추게 되면 스크래핑 프로그램의 목표인 각 기관의 웹 서버에 불필요한 부하를 가하여 의도치 않은 피해를 입힐 가능성도 존재한다. 스크래핑 방식의 불안정성도 문제지만 더 큰 위험은 고객 인증정보 저장에 의한 보안의 취약성이다. 고객 인증정보가 서비스 제공 사업자 또는 개인정보를 탈취한 제3자가 악용한다면 고객의 프라이버시가 침해될 수 있고, 금융산업 분야인 만큼 고객이 심각한 금전적 손실을 입을 가능성도 있다[5].

스크린 스크래핑 방식의 한계를 극복하고 개인신용정보 전송요구권의 원활한 행사를 지원하기 위해서 보다 안정적이고 표준화된 데이터 전송 방식으로 API(Application Programming Interface) 방식이 사용되고 있다. 이 방식은 특정 프로그램의 기능이나 데이터를 다른 프로그램이 접근할 수 있도록 미리 정한 통신 규칙으로, 데이터 소유 주체가 웹 개발자나 사용자를 위해 정보 및 데이터를 정해진 방식으로 공개하는 기술이다. API를 통해 데이터를 송수신하면 데이터 통신을 위한 아키텍처가 플러그 앤 플레이 방식으로 단순화되고, 데이터를 송신하는 쪽과 수신하는 쪽이 모두 어떤 데이터가 어떻게 전달되는지 투명하게 확인할 수 있다. 데이터를 송신하는 쪽은 수신하는 쪽의 신원과 수신 요청 명세를 검토한 후 데이터를 송신할 수 있고, 데이터를 수신하는 쪽은 올바른 인증정보와 규격에 맞는 전송 요청을 보내면 원하는 정보를 사전에 정의된 형태로 수신될 것이라 기대할 수 있다. 여기에 마이데이터 사업자의 서비스에 가입한 개별 고객의 개인적인 인증정보는 필요하지 않다는 점 또한 API 전송방식의 강점이라고 할 수 있다[5, 6].

마이데이터 표준 API에는 인증 API, 정보제공 API, 지원 API 등이 있으며, 인증 API는 고객이 개인신용정보 전송요구 및 본인인증을 수행하는 데 필요한 API로, 개별인증과 통합인증으로 구분된다. 정보제공 API는 고객의 개인신용정보(은행, 보험, 카드, 금융투자, 전자금융 등) 전송요구에 의거, 정보제공자가 마이데이터사업자에게 개인신용정보를 전송하는 데 필요한 API이다. 지원 API는 크게 두 가지 방식이 존재하며, 첫 번째로 종합포털이 마이데이터 산업을 지원하는 데 필요한 API는 마이데이터 참여기관이 종합포털에게 요청하는 API로 접근토큰 발급, 기관정보 조회, 서비스 정보 조회, 통계자료 전송, 통합인증 API 호출용 자격증명 조회, 정보수신자용 자격증명조회가 있으며, 두 번째로 종합포털이 마이데이터 참여기관에 요청하는 API는 정보제공자 상태 조회, 정보주체별 전송요구 내역 조회, 통계자료 재전송요청, 접근토큰 발급 등이 있다[7].

2.2 마이데이터 기술적 보안 사항

마이데이터의 보안환경은 API 방식으로 안전하게 개인신용정보 전송하며, 강력한 본인인증 방식으로 개인신용정보를 보호하고 있다. 또한, 24시간 보안관제로 실시간 모니터링을 통한 침해위협에 대한 조기대응이 가능하며, 신용정보관리 보호인을 통한 개인신용정보 보호 계획 수립 및 시행을 하고, 물리적 보안설비의 구축 및 기술적 보안 사항을 수립하여 안전하게 운용하고 있다.

마이데이터의 기술적 보안사항의 특징으로는 고유식별정보, 비밀번호, 바이오 정보 등을 포함한 개인신용정보는 암호화하여 저장하며, 업무용 단말기 및 모바일 기기에 개인신용정보를 저장할 때도 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암

호화하고 있다. 또한, 전용회선 등을 통해 개인신용정보 등을 전송할 시에는 TLS1.3 버전 이상의 인증서를 적용하여 인터넷 기반으로 개인신용정보를 암호화하여 송·수신하고 있다.

이외에도 망분리를 수행하고 있는데, 내부통신망과 연결된 내부 업무용 시스템 등은 외부통신망과 분리 차단할 수 있도록 망분리를 수행해야 하며, 전산실 내 위치한 정보처리시스템과 해당 정보처리시스템에 직접 접속하는 단말기에 대해서 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 한다. 보안시스템으로는 개인신용정보처리시스템에 침입차단시스템과 침입탐지시스템을 설치하고 운영하여야 하며, 이상거래 시도를 포함한 보안사고 등을 모니터링 및 기록 (IP주소, 인증 실패 횟수, 부정한 API 요구 등)하고 지원기관에 공유해야 한다. 그리고 개인신용정보처리시스템 등 정보처리기기에 컴퓨터 바이러스, 스파이웨어 등 악성 프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신 소프트웨어를 설치하도록 하고 있다. 이외에도 보안 설계, 테스트데이터 활용, 취약점 점검 및 개인신용정보취급자의 개인신용정보 출력·복사 시 보호조치를 위한 내부시스템의 구축과 외부 전송 시 사전 승인 등의 기술적 보안 조치를 취하도록 하고 있다[8].

2.3 마이데이터 서비스 가입정보 제공

마이데이터산업은 고객의 전송요구권 행사에 따라 분산되어 있는 개인신용정보를 제공받아 해당 고객에게 통합조회 서비스를 제공하는 산업이다. 따라서 고객의 개인정보 자기결정권을 행사하는 것을 실질적으로 보장해야 하며, 고객의 개인정보 자기결정권 행사를 최대한 보장함을 원칙으로 모든 절차를 진행하여야 한다. 다음의 <그림 1>은 마이데이터 종합포털 서비스 가입정보 제공화면의 예시이다[8].

고객이 마이데이터 앱을 통해 개인신용정보전송요

<그림 1> 마이데이터 서비스 가입정보 제공화면

구권을 행사하면, 마이데이터사업자의 앱(App)을 통해 금융회사가 필요한 정보 항목을 마이데이터사업자에 제공할 것을 요구하게 되며, 금융회사는 표준화된 전산처리방식(API)을 통해 고객의 정보를 마이데이터사업자로 전달하는데, 고객의 인증정보는 암호화하여 안전하게 전달되며, 고객은 마이데이터사업자를 통해 본인 정보를 통합조회 할 수 있게 되는 것이다.

특히, 중요한 사항으로는 개인정보 자기결정권을 보장하기 위해서 정보제공자, 전송요구내용 등이 명확하게 제시되기 때문에 사용자가 어떠한 기관에서 어떠한 정보들이 제공되는지를 명확히 파악할 수 있다.

반면에, 사용자들이 다양한 서비스를 제공받기 위하여 동의를 받은 개인정보들에 대해서는 1년에 한 번 사용자들에게 수집하는 개인정보의 항목 및 수집방법, 개인정보의 처리 위탁, 개인정보의 제3자 제공, 개인정보처리방침 등에 대해서 통지를 하고 있지만, 각 회사별로 SNS나 이메일을 통하여 전달하고 있으므로 전체적으로 어떠한 내용들이 어떻게 제공되고 있는지도 파악하기 어렵고, 수집된 개인정보 중 일부 정보의 삭제를 요청하는 것도 별도의 지정된 방법으

로 각 회사에 요구해야 하므로 체계적인 관리가 어려우므로 이에 대한 대책이 필요할 실정이며, 3장에서 이를 효율적으로 관리할 수 있는 개인정보 이용내역 통지 모델을 제안하였다.

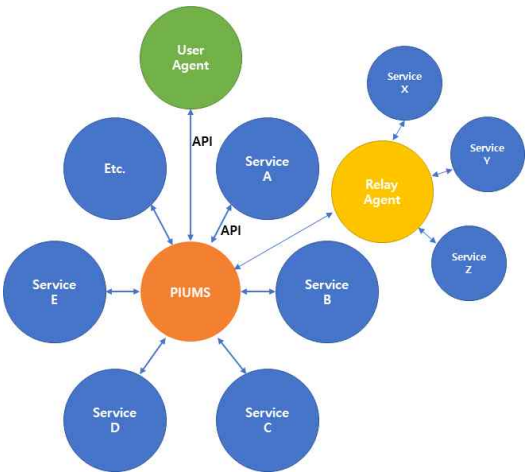
Ⅲ. 개인정보 이용내역 통지 모델

3.1 제안 모델

개인정보 이용내역 통지는 법적 의무 대상자에 해당하는 경우 개인정보 이용내역을 주기적으로 정보주체(이용자)에게 통지하고 그 기록을 유지해야 하는데, 여기서 법적 의무 대상자는 전년도 말 기준 직전 3개월간 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자가 이에 해당한다.

통지 주기는 연 1회 이상이며, 통지 방법은 전자우편, 서면, 모사전송, 전화 또는 이와 유사한 방법 중 하나의 방법을 이용해야 하며, 통지 예외로는 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우이다. 또한, 개인정보 이용내역 통지항목으로는 법적 요구항목을 모두 포함해야 하는데, 그 항목으로는 개인정보의 수집, 이용 목적 및 수집한 개인정보의 항목과 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목 그리고 개인정보 처리위탁을 받은 자 및 그 처리위탁을 하는 업무의 내용을 통지해야 한다. 또한, 이러한 통지받은 개인정보들은 정보주체 또는 그 대리인이 개인정보에 대한 열람, 정정, 삭제, 처리정지, 이의제기, 동의 철회 요구를 개인정보 수집방법 및 절차보다 쉽게 할 수 있도록 권리 행사 방법 및 절차를 마련해야 한다[9].

이러한 요구사항을 만족하기 위해서 개인정보 이용내역 통지 모델은 동의된 개인정보 현황을 용이하게 파악할 수 있어야 하는데, 개인은 자신의 정보가 활용되는 목적, 기관, 범위에 대해 쉽게 이해할 수 있는 형태로 파악할 수 있어야 한다. 또한, 개인은 개인 데이터 수집 및 이용(동의, 내려받기, 공유 등)에 관한 내역을 이해하기 쉬운 방식으로 실시간 확인할 수 있어야 하며, 서비스 이용 중 언제라도 쉽고 편한 방식으로 개인정보 제공에 대한 동의내역을 변경할 수 있어야 한다. 이러한 고려사항을 반영하여 제안하는 개인정보 이용내역 통지 시스템 모델은 다음의 <그림 2>와 같다.



<그림 2> 개인정보 이용내역 통지 시스템 모델

<그림 2>의 이용내역 통지 시스템 모델에서 User Agent는 개인정보 이용내역을 확인 및 수정 요청 그리고 결과를 확인하는 사용자의 시스템을 의미하며, PIUMS(Personal Information Usage history Management System)는 각 사용자에 대한 이용내역을 수집하여 사용자에게 제공하고, 수집된 개인정보에 대한 정정, 삭제, 처리정지, 이의제기, 동의 철회 요구를 처리하는 시스템이다. Relay Agent는 중계기관으로 개인정보를 처리하는 시스템의 용량이 많이 필요한 경우에는 각 산업군 혹은 지역별로 Relay Agent를 두어 효율적으로 데이터를 처리하도록 할 수 있다.

데이터를 교환하기 위한 API의 메시지 형식은

JSON(JavaScript Object Notation) 방식을 사용하며, 이 방식은 용량이 적은 메시지를 송수신하기 위해 데이터 객체를 속성·값(Key:Value) 형식으로 표현하는 개방형 표준 메시지 형식이다. 메시지 전송을 위한 인코딩 방식은 UTF-8을 사용하며, UTF-8는 ASCII 코드를 확장하여 전 세계의 모든 문자코드를 표현할 수 있는 표준 인코딩 방식이다. 데이터 통신은 네트워크 구간을 보호하기 위해 TLS(Transport Layer Security) 1.3 이상의 버전을 사용해야 하며, API 요청 및 응답(메시지) 교환방식은 REST 방식을 사용한다. 개인정보 이용내역 통지 절차는 다음의 <그림 3>과 같다.

<그림 3> 개인정보 이용내역 통지 절차

개인정보 이용내역 통지에 대한 주요 서비스의 절차는 다음과 같다.

(개인정보 이용내역 통지 요구) ① 개인은 자신의 개인정보가 이용된 내역을 확인하기 위하여 PIUMS를 이용하여, 본인의 개인정보를 이용하고 있는 서비스 제공자를 대상으로 API 규격에 따라 이용내역을 전송할 것을 요구한다.

(이용내역 통지 요구사항 전달) ② PIUMS는 개인의 이용내역 전송 요구사항을 서비스 제공자에게 전송한다.

(본인확인 및 개인정보 이용내역 전송) ③ 개인정보를 가지고 있는 서비스 제공자는 인증수단을 활용하여 개인이 정보의 소유주임을 확인하고, ④ API 규격에 따라 PIUMS에게 개인정보 이용내역을 전송한다.

(개인정보 이용내역 제공) ⑤ PIUMS는 하나 이상의 서비스 제공자로부터 수집된 개인정보 이용내역을 개인에게 제공한다.

서비스를 이용하기 위하여 동의한 개인정보 수집 항목에 대하여 변경 및 동의 철회를 요청하는 절차는 다음의 <그림 4>와 같다.

<그림 4> 개인정보 수집내역 변경 절차

① 개인은 자신의 개인정보가 수집된 내역을 확인한 후 개인정보 수집내역 변경을 위하여 PIUMS에게 서비스 제공자 및 변경 요구 정보를 전송한다. ② PIUMS는 개인의 개인정보 수집내역 변경 요구사항을 서비스 제공자에게 전송한다. ③ 개인정보를 가지고 있는 서비스 제공자는 인증수단을 활용하여 개인이 정보의 소유주임을 확인하고, ④ API 규격에 따라 PIUMS에게 개인정보 변경된 개인정보 수집내역을 전송한다. ⑤ PIUMS는 서비스 제공자로부터 수집된 변경된 개인정보 수집내역을 취합하여 정보의 소유주인 개인에게 제공한다.

3.2 제안 방법론의 효용성

개인정보 이용내역 통지에 대해 제안한 모델과 기존의 통지 방법과의 차이점은 다음의 <표 1>과 같다.

<표 1> 기존 방법과의 기능 비교

항목	기존 방법	제안 방법
개인정보 이용내역 제어 가능성	X	O
개인정보 이용내역 정보의 가용성	X	O
개인정보 이용내역 무결성	X	O
개인정보 이용내역 출처인증	X	O
개인정보 자기결정권	X	O

기존 방법과 제안한 모델의 기능적인 차이의 첫 번째 항목으로는 개인정보 이용내역 제어 가능성이 있다. 개인정보 이용내역 통지는 법적 준거성 측면에서 매년 사용자에게 통보하고 있으나, 실제적으로 사용자들은 이메일이나 SNS를 통해 전송되는 각 정보에 관해 확인하기도 어렵지만, 여러 서비스 제공자에게서 오는 다양한 정보들을 통합적으로 분석하는 것도 힘들기 때문에 서비스 가입 시 혹은 서비스 이용 중에 수집에 동의한 개인정보들의 현황을 종합적으로 판단하여 그에 대한 적절한 조치를 수행하기 어렵다는 문제점이 있다. 따라서 제안한 모델을 통해 개인정보 이용내역의 통지된 정보를 전체적으로 분석하고 관리할 수 있다.

두 번째로는 개인정보 이용내역 정보의 가용성이다. 현재는 많은 서비스 제공자들이 연말 혹은 연초에 개인정보 이용내역에 대한 통지를 하고 있으나, 제안한 모델을 이용하면 개인정보의 소유주인 사용자가 언제든 본인의 정보가 어떻게 이용되고 있는지 확인하고 싶을 때 확인할 수 있다는 것이다.

세 번째로는 개인정보 이용내역에 대한 무결성을 제공할 수 있다. 기존에는 개인정보 이용내역이 1년에 한 번씩 제공되므로 이용내역에 대한 무결성을 확보하기 위해서는 매년 제공되는 메일이나 SNS를 확인해야 하지만, 제안한 모델에서는 주기적으로 개인정보 이용내역에 대한 확인 및 정보가 취합되는 PIUMS를 통해 개인정보 이용내역에 대한 변경 사항 및 그에 대한 사용자의 승인 여부들에 관해 확인할 수 있다.

네 번째로는 출처인증 기능을 수행할 수 있다. 현재는 이메일이나 SNS로 전송되는 정보들에 대해서 이메일의 송신자나 SNS 계정 정보로 개인정보 이용내역을 통지한 서비스 제공자를 판별할 수 있으나, 이러한 정보들은 위변조에 취약한 특성이 있다. 그러나 제안한 모델에서는 개인과 서비스 제공자가 상호인증을 통해 서로의 신원을 인증하게 되므로 사용자는 출저인증을 할 수 있으며, 서비스 제공자는 정보의 소유주에게 안정적으로 개인정보 이용내역을 통보할 수 있다.

마지막으로 개인정보 자기결정권을 제공할 수 있다. 현재의 시스템은 수동적으로 내가 동의한 개인정보 내역과 이용된 내역들을 단순하게 비교하고, 잘못된 정보가 있는 경우에는 서비스 제공자에게 이메일이나 전화 등을 통해 확인 및 변경 등의 절차를 수행해야 하지만, 제안한 모델의 경우에서는 능동적으로 개인정보 이용내역에 대한 확인 및 이에 대한 변경 및 동의 철회 등을 수행할 수 있다는 장점을 가지고 있다.

Ⅳ. 결론

4차산업의 발전에 따라 AI 등을 활용한 빅데이터가 우리 생활의 많은 부분에서 활용되고 있으며, 이에 따라 데이터의 중요성도 더욱 증가하고 있다. 특히 개인정보를 활용한 다양한 서비스의 등장 및 이를 악용한 해킹 공격들이 다양하게 등장함에 따라 개인정보 관리의 중요성이 더욱 증대되고 있다.

개인정보는 개인정보의 수집, 보유 및 이용, 제공 그리고 파기 시에도 안전하게 관리를 수행해야 하며, 정보주체의 권리를 보호해야 한다. 최근에는 정보주체의 요청에 의해 데이터를 수집하고 활용하는 마이데이터 서비스가 도입되어 다양한 서비스가 제공되고 있으며, 다양한 보안방안을 도입하여 하나의 앱에

서 고객의 데이터를 수집하고, 자산 및 소비 패턴을 분석하여 최적의 금융상품을 추천하는 방식으로 운영하고 있다.

본 논문에서는 마이데이터 모델을 활용한 정보주체 권리보호 중 이용내역 통지 모델에 대한 분석을 수행하였다. 개인정보 보호법에 의해 개인정보 이용내역을 주기적으로 사용자에게 통지해야 하며, 일반적으로 1년에 한 번씩 주로 이메일이나 SNS를 통해 각 개인에게 이용내역을 통지하고 있지만, 서비스 사용자들의 개인정보들이 어느 회사에서 어떤 정보들이 활용되고 있는지에 대한 파악 및 관리는 어려운 실정에 있다. 따라서 본 논문에서는 개인정보 이용내역 통지 시스템 모델을 제안하였으며, 기능분석을 통한 효용성의 분석 결과 기존의 개인정보 이용내역 통지방안보다 제안한 모델이 개인정보 이용내역 제어 가능성, 가용성, 무결성, 출처인증, 개인정보 자기결정권 등을 제공할 수 있는 것으로 분석되었다.

향후 연구계획으로는 제안한 개인정보 이용내역 통지 시스템 모델에 대해 취약성 및 위협 분석을 통해 위험분석을 수행하고 안정적인 사용에 관한 추가적인 연구를 수행할 계획이다.

참고문헌

[1] 이양복, "데이터 3법의 분석과 향후과제," 한국비교사법학회, 비교사법, 제27권, 제2호, 2020, pp.423-463.

[2] 오현택·양진홍, "마이데이터 환경에서 개인의 전자 건강/의료 데이터 활용을 위한 데이터 거래모델," 한국정보전자통신기술학회 논문지, 제13권, 제3호, 2020, pp.250-261.

[3] 마이데이터 발전 종합정책, 대통령직속 4차산업혁명위원회, 관계부처 합동, 2021. https://www.4th-ir.go.kr/article/download/795

[4] 포스트 코로나 시대 핀테크와 마이데이터, 한국연구재단, 이슈리포트 2021-17호, 2021.

[5] 김혜빈·신원·신상욱, "마이데이터 개념을 활용한 탈중앙화 저작권 관리 모델," 멀티미디어학회 논문지, 제23권, 제2호, 2020, pp.262-273.

[6] 송미정·김인석, "유럽 PSD2 시행에 따른 금융분야 마이데이터 정책의 개인정보보호 강화 방안 연구," 정보보호학회 논문지, 제29권, 제5호, 2020, pp.1205-1219.

[7] 마이데이터 종합포털, https://www.mydatacenter.or.kr:3441/myd/mydapi/sub1.do

[8] 금융분야 마이데이터 서비스 가이드라인, 금융위원회·한국신용정보원, 2021. https://www.mydatacenter.or.kr:3441/myd/bbsctt/normal1/normal/62a478f6-2903-4107-9093-29072912e974/32/bbsctt.do

[9] ISMS-P 인증기준 안내서, 한국인터넷진흥원, 2019.

■ 저자소개 ■

김 태 경
Kim TaeKyung

2017년 9월~현재
명지전문대학 교수
2008년 3월~2017년 8월
서울신학대학교 교수
2006년 3월~2008년 2월
서일대학교 교수
2005년 8월 성균관대학교
전기전자및컴퓨터공학과 (공학박사)

관심분야 : 네트워크보안, IoT 보안, 개인정보보호
E-mail : tkkim@mjc.ac.kr

정 성 민
Jung Sungmin

2020년 9월~현재
명지전문대학 교수
2014년 3월~2020년 8월
한국원자력연구원 선임연구원
2014년 2월 성균관대학교
전기전자및컴퓨터공학과 (공학박사)

관심분야 : 산업시설보안, 제어시스템보안,
센서네트워크, 클라우드 컴퓨팅
E-mail : smjung@mjc.ac.kr

논문접수일 : 2022년 2월 23일
수 정 일 : 2022년 2월 28일
게재확정일 : 2022년 3월 10일