API 보안 및 데이터 보안 표준

나재훈 ITU-T SG17 WP4 의장, 한국전자통신연구원 전문위원

1. 머리말

개인데이터의 활용을 위한 마이데이터 사업은 유럽연합(EU)에서 2018년 시행한 GDPR(General Data Protection Regulation)의 공표로부터 시작되었다. GDPR은 데이터의 주체가 자신의 데이터의 제공과 이용을 스스로 결정할 수 있게 하는 권리를 말하며, 마이데이터는 네트워크를 통하여 곳곳에 흩어져 있는 데이터를 데이터 주체를 중심으로 구성하고 데이터에 대한 권리를 주장할 수 있도록 정보의 결정권을 강화하는 제도를 일컫는다. 이러한 추세와 관련하여 마이데이터 서비스를 제공하는 오픈 플랫폼 구조, 오픈 API(Application Programming Interface)의 보안적 측면과 오픈 API를 통하여 제공되는 데이터의 보안 관련 국제표준들에 대하여 ITU-T SG17과 ISO/IEC JTC 1/SC27을 중심으로 살펴본다.

2. 오픈 API의 보안 표준[1]

2.1 오픈 플랫폼

오픈 플랫폼은 오픈 표준에 근거하여 표준 문서가 제정(게재)되고, 문서화된 외부 응용 프로그램 인터페이스(API, Application Program Interfaces)를 제공하는 소프트웨어 시스템을 의미한다. API는 원래 프로그램의 의도하지 않은 다른 기능으로도 소프트웨어를 이용할 수 있도록, 소스 코드를 수정하지 않고서도 쓸 수 있도록 허용하고 있다. 이러한 인터페이스를 이용하여 제삼자는 기능을 추가하여 플랫폼에 통합할 수 있다.

오픈 플랫폼이란 벤더가 다양한 기능을 부가할 수 있도록 허용하고 지원하는 플랫폼을 의미한다. 따라서 오픈 플랫폼을 이용할 때 플랫폼의 벤더가 아직 완료하지 못한, 또는 생각지도 못한 기능을 개발자가 추가할 수 있다. 다수의 개발자가 플랫폼을 이용할 수 있어야 하므로 오픈 플랫폼은 규격이 공공에 개방된 오픈 표준으로 공급되고, 개발자들이 현재의 기능을 변경할 수 있도록 허용한다.

소프트웨어 플랫폼이 오픈 플랫폼이려면 다음 과 같은 특징을 적어도 하나 이상 지녀야 한다.

- 오픈 API: 공개된 API가 문서화되어 모든 개발자들이 사용할 수 있어야 한다.
- 확장성(Extensibility): 본래 계획되지 않은 목적으로 플랫폼을 이용하려고 할 때 다양한 기능들(Capabilities)을 참조 할 수 있어야 한다.
- 오픈소스: 누구에게나, 그리고 어떤 목적으로든 소프트웨어 연구 개발과 변경, 배포를 위

해 프로그래밍언어의 프로그램 부분의 소스 코드를 이용할 수 있도록 저작권자가 라이선스를 통해 권리를 이양해야 한다.

- 수용성(Adoptability): 특정한 사업 목적에 따라 오픈플랫폼을 다른 사람이 이용할 수 있게 한 경우, 라이선스 조건 하에 비차별적으로 제공할 수 있어야 한다. 이는 오픈플랫폼의 모든 서비스가 반드시 무료 로열티(Royalty-free)를 고수할 필요는 없다는 뜻이다.
- 적응성(Adaptability): 규격을 공개적으로 이용할 수 있어서 플랫폼의 기존 기능을 변경할 수 있어야 한다. 이는 새로운 기능을 추가하는 것과는 다른 경우다.

2.2 오픈 플랫폼의 구조

최근 핀테크(FinTech)가 세계적인 트렌드로 자리잡으면서 영국, 미국 등을 중심으로 금융회사와 핀테크 기업 간 연대가 활발히 이루어지고 있다. 이에 따라 금융회사 내부 시스템과 핀테크 기업을 연결하는 도구로서 금융회사에서는 오픈 API에 대한 논의가 활발하다.

오픈 API는 API의 개념을 웹으로 확장한 것으로 개방 지향적이다. 즉, 기업이 보유한 서비스나 정보를 쉽게 활용할 수 있게 허용하여 웹 서비스 및 애플리케이션 개발을 지원한다. 또한 사용자는 일방적인 웹 검색 결과나 사용자 인터페이스(UI)를 제공받는 데 그치지 않고 직접 응용프로그램과 서비스를 개발할 수 있어서 사용자 참여를 유도한다. 이러한 특성은 오픈 API를 활용한 비즈니스가 사용자 중심의 모델임을 보여준다.

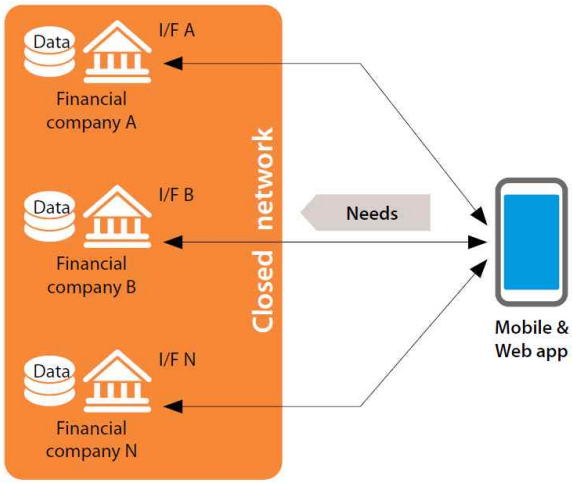
최근 모바일 생태계가 외부 개발자를 참여시키는 개방형 플랫폼으로 변화하면서 오픈 API를 제공하거나 도입을 추진하는 금융회사가 늘어나는 추세이다. 금융회사의 오픈 API는 핀테크 기업이 새로운 금융서비스를 손쉽게 개발할 수 있도록 금융정보를 요청하는 방법을 정의하며, 이를 통해 다양한 기업이 금융 관련 서비스를 제공할 수 있다.

금융기업이 오픈 API에 비상한 관심을 두는 이유는 이들이 제한된 인적, 기술적 리소스만으로 고객들의 다양한 요구와 개인화된 서비스들을 감당하기는 어렵기 때문이다. 반대로 핀테크 기업은 수요에 대응해 다양한 기능을 개발하는 역량은 갖췄지만, 다양한 금융기업의 정보에 일일이 서로 다른 방법으로 접근하는 데 어려움을 겪는다. 게다가 개발한 제품을 실질적이고 충분한 데이터를 배경으로 검증할 수 있는 테스트 환경을 구축하기도 어렵다. 따라서 오픈 플랫폼은 금융기업의 데이터와 핀테크 기업의 서비스를 종합하는 윈윈전략이라고 할 수 있다.

핀테크는 최근 수년 동안 가장 두각을 나타내는 기술 토픽으로, 가히 혁명이라고 할만한 변화를 이끌어내고 있다. 핀테크가 보편화되면서 금융계에 고착되어 있던 과거의 불편한 요소들이 개선되고 고객이 금융제품 및 서비스에 접근하는 방식에 혁신이 일어났다. 이러한 흐름에 따라 핀테크 스타트업은 그 숫자가 늘어나고 전문성도 강화되는 한편, 전통적인 서비스 제공자와 새로운 관계를 형성하고 견고하게 유지한다.

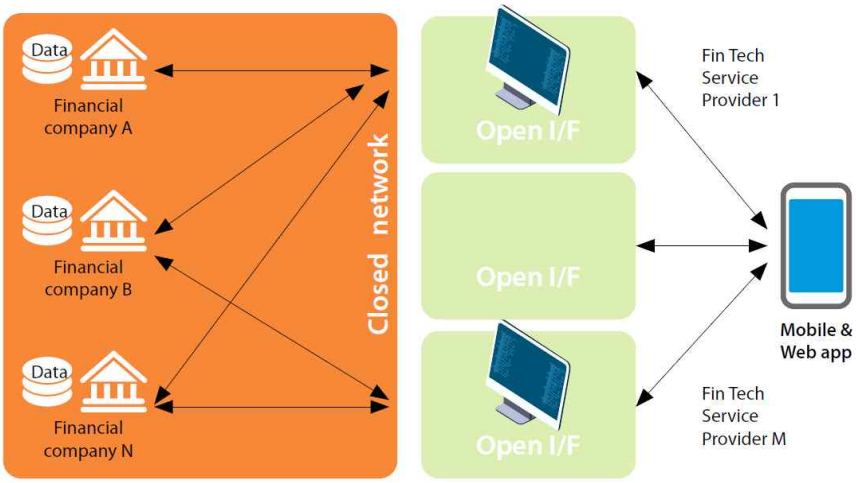
다만 개인정보가 오가는 시스템 간 인터페이스는 사이버 공격의 취약점이 될 위험성이 있다. 핀테크 기업은 플랫폼의 안전을 유지할 의무를 진다. 이는 '설계에 의한 정보보호(Security by design)'의 원칙을 요하며, 서비스와 앱을 설계하거나 구현하기에 앞서 처음 기획 단계부터 정보보호 방안을 구축해야 한다는 뜻이다.

[그림 1]의 금융 서비스의 구조는 금융 서비스 제공자가 일방적으로 서비스를 구축하여 사용자들에 제공하는 형태이다. 각 금융사가 자신의 데이터와 서비스를 자신들의 방식으로 사용자들에게 제공하는 형태로, 금융서비스를 이용하려면 금융사마다 별도의 앱을 이용하여 접속해야 한다. 자연히 금융사마다 서비스의 수준이 다를 수밖에 없는데, 사용자 입장에서는 이처럼 상이한서비스에 대해 불만이 쌓일 수밖에 없다. 게다가 앱이나 서비스가 금융사에 종속되어 있어 사용자 입장에서는 자유롭게 편리한 앱을 선택하기도 어렵다. 결국 금융사가 제공해야 하는 서비스가 모두 비슷한데도 유사한 기능을 개별 금융사가 일일이 개발해야 하고, 서비스 개선이나 유지보수 또한 금융사가 전적인 책임을 져야 해서 기업 경쟁력에 부적합한 모습을 보인다.



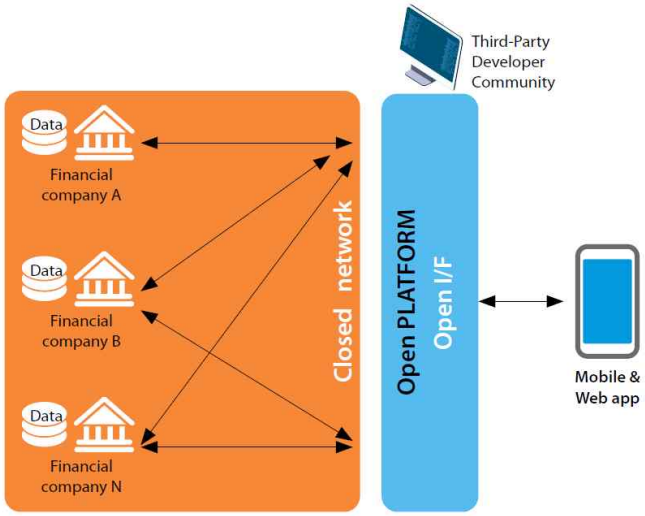
[그림 1] 디지털금융 서비스의 기능구조

[그림 2]의 핀테크 서비스 구조는 이러한 문제점을 개선하고 사용자의 요구사항을 적극적으로 수용한 결과다. 금융사 내부 인력으로 개발하기보다 외부의 핀테크 기업을 활용하여 서비스를 제공하는 형태다. 이 구조는 별도의 전문 기업이 소프트웨어를 개발하고 오픈 인터페이스를 사용자들에게 제공함으로써 전반적인 효율성을 향상시킨다. 그러나 개발사만 핀테크 기업일 뿐, 금융서비스에 사용하는 앱은 여전히 금융사마다 다르므로 여전히 사용자가 금융사마다 다른 앱을 설치해야 한다.



[그림 2] 핀테크 서비스의 구조

[그림 3]의 오픈 플랫폼은 표준화된 공개 인터페이스를 제공하여 여러 금융사가 함께 사용한다. 따라서 사용자는 하나의 앱으로 여러 금융사의 데이터와 서비스를 접할 수 있다. 핀테크 기업 입장에서도 단일화된 인터페이스로 인하여 개발 및 유지보수 요소가 최소화되기에 생산성이 높아진다. 또한 공개된 데이터와 서비스를 기반으로 새로운 종류의 서비스 발굴이 가능하여 금융서비스로부터 파생된 부가가치를 창출하기에 용이하다. 이러한 구조는 일반적인 개방형 플랫폼과 동일하다.

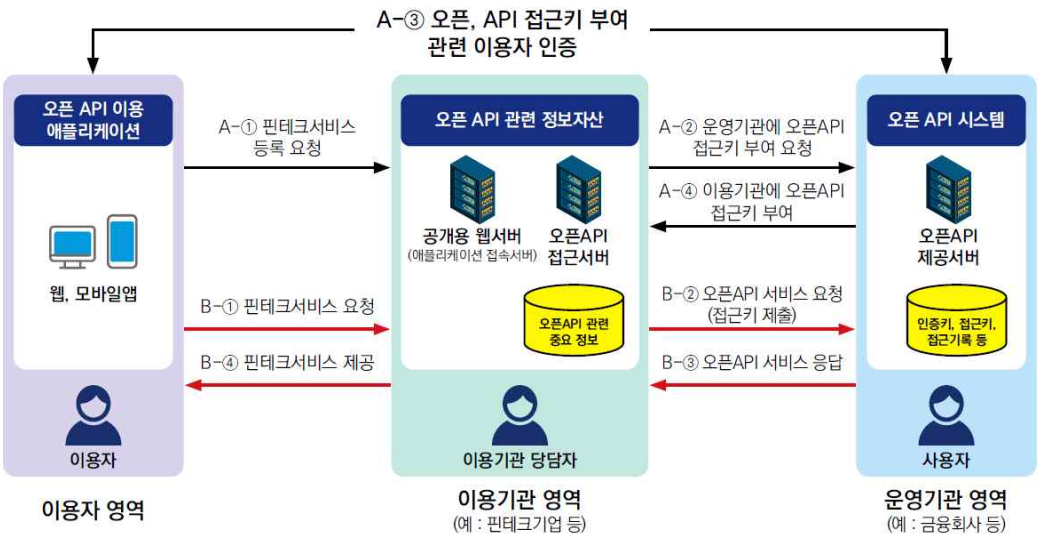


[그림 3] 오픈 플랫폼 구조

2.3 오픈 인증 구조 및 절차

[그림 4]는 일반적인 개방형 플랫폼 구조에서 핀테크 서비스를 위하여 핀테크 기업이 중개를 하는 절차를 보여준다. 금융권의 운영기관은 핀테크 기업인 이용기관에게 새로운 개방형 API를 개발할 수 있는 구조와 권한을 부여하고, 이용자는 이용기관을 통하여 다양하고 풍성한 개방형 서비스를 제공받는다. 또한 운영기관과 이용자 사이에서 중간에 핀테크 기업이 포털(플랫폼)을 공개하고, 그 포털을 통해 개방형 API를 공개하여 이용자들에게 서비스를 제공한다.

개방형 API를 사용하려면 [그림 4]와 같은 절차를 따른다



[그림 4] 마이데이터 서비스를 위한 오픈 인증 플랫폼 구조 및 절차

◆ 등록 단계 (A)

① 이용자는 이용기관에 오픈 API를 이용한 핀테크 서비스(예: 계좌잔액조회, 거래내역 조회 등) 등록을 요청한다.

② 이용기관은 운영기관에 해당 이용자에 대한 오픈 API 접근키 부여를 요청한다.

③ 운영기관은 오픈 API 접근키 부여에 앞서 이용자 인증을 수행한다.

④ 운영기관은 오픈 API 접근키를 이용기관에 부여한다.

◆ 이용 단계 (B)

① 이용자가 이용기관에 오픈 API를 이용한 핀테크서비스(예: 계좌잔액조회)를 요청한다.

② 이용기관은 등록 단계에서 부여받은 오픈 API 접근키를 운영기관에 제출하고 오픈 API 서비스(예: 이용자 계좌잔액정보 제공)를 요청(호출)한다.

③ 운영기관은 해당되는 오픈 API 서비스 응답을 이용기관에 제공한다.

④ 이용기관은 ③에서 수신된 이용자 정보를 활용하여 이용자에 서비스를 제공한다.

2.4 오픈 플랫폼 위협과 취약점

오픈 플랫폼과 오픈 API와 관련하여 분석된 위협은 세계적으로 오픈소스 비영리 재단인 OWASP(Open Web Application Security Project)을 중심으로 취합된 바 있다. OWASP가 정리한 취약점은 다음과 같다. 상세한 사항은 참고자료로 갈음한다.

위협 목록[2,3]

계정 수집(Accountaggregation), 계정 생성(Account creation), 광고 사기 (Ad fraud), 캡차 공격(CAPTCHA defeat), 카드 크래킹 (Card cracking), 카딩 (Carding), 캐싱아웃 (Cashing out), 크리덴셜 크래킹 (Credential cracking), 크리덴셜 스터핑 (Credential stuffing), 재고 거부 (Denial of Inventory), 서비스 거부 (Denial of Service), 신속처리 (Expediting), 핑거프린팅 (Fingerprinting), 풋프린팅 (Footprinting), 스캘핑(Scalping), 스크래핑 (Scraping), 스큐잉 (Skewing), 스니핑 (Sniping), 스패밍 (Spamming), 토큰 크래킹 (Token cracking), 취약점 스캐닝 (Vulnerability scanning), 비인가 접근 (Unauthorized access).

취약점 목록[4]

Glibc 취약점, 쿼드루터 (Quadrooter), 드로운 취약점 (DROWN), 제로데이 공격 (Zero-Day attack), DB 취약점 (Database vulnerability), OS커널 취약점 (Operating System Kernel vulnerability), OpenJDK 취약점 완전동형 암호 (FHE, Fully Homomorphic Encryption) 표준

2.5 오픈 API 보안 지침

오픈 API 이용구조의 주요 객체는 이용자, 마이데이터 사업자(이용기관), 데이터 제공기관(운영기관)등 세 가지다. 오픈 API 보안은 이들 중 마이데이터 사업자(이용기관) 측면과 데이터 제공

기관(운영기관: 은행, 투신사, 통신사 등) 측면에서 조사해야 한다. 두 개의 측면에서 상세한 보안의 언급은 ITU-T X.1149[1,5]를 참고하는 것을 권고하며, 각 측면에서 중요 API 보안 고려 사항을 간략히 요약하면 다음과 같다.

2.5.1 마이데이터 사업자(이용기관) 측면 보안 고려사항

- 오픈 API를 이용한 서비스에서 정보보호 관리 대상이 되는 모든 정보자산을 식별할 수 있어야 한다. 정기적으로 식별된 정보자산에 대한 기밀성, 무결성, 가용성, 법적 요구사항 등을 고려하여 조직에 미치는 영향을 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다.
- 오픈 API 관련 정보처리시스템이 알려진 취약점에 노출되어 있는지 여부를 확인하기 위하여 정기적으로(연 1회 이상) 취약점 점검을 수행하여 위험을 관리하여야 한다.
- 오픈 API를 이용한 서비스에서 회원가입을 받거나 개인정보를 입력받는 경우, 개인정보 처리방침을 작성하여 이용자가 쉽게 확인할 수 있는 위치(예: 홈페이지 메인화면 등)에 공개하여야 한다.
- 수집하려는 개인정보 항목, 수집방법 및 이용목적, 보유 및 이용 기간, 동의 거부 권리 및 거부에 따른 불이익 내용 등 법적으로 요구되는 필수 사항이 기재되도록 작성하여야 한다.
  - 수집하려는 개인정보가 목적을 위한 최소한의 정보가 되도록 필수/선택을 적절히 구분하고 동의를 받아야 한다.
  - 마이데이터 서비스 개발 시 데이터 제공기관(운영기관)의 약관, API 개발 가이드 등을 준용하며, 오픈 API 인증키, 접근키 등 중요정보의 관리 지침을 따라 개발하여야 한다.
  - 마이데이터 서비스(이용기관)를 안전하게 제공하기 위하여 암호통제, 접근통제, 시스템 보안, 네크워크 보안 지침들을 준수하여야 한다.

2.5.2 데이터 제공기관(운용기관) 측면 보안 고려사항

- 이용자 및 마이데이터 사업자 인증 방법의 적정 보안수준을 유지해야 한다.
- 이용자 및 마이데이터 사업자의 API 접근 요청 처리 시 권한의 적정성을 검증해야 한다.
- 이용자 인증 우회방지와 안전한 인증을 위하여 인증키를 관리해야 한다.
- 이용자의 거래정보의 기밀성 및 무결성을 보장하고, 정보 유출, 이상금융거래방지 방안을 구축하여 운영해야 한다.
- 업무의 지속성을 위하여 시스템을 이중화하고, 백업 및 분산 관리해야 한다.

3. 데이터 보안 표준

마이데이터 서비스 환경에서 데이터 보안은 곧 개인정보 보호를 의미한다. 마이데이터 서비스 환경에서 개인정보 보호 기술로는 개인정보의 비식별화 처리가 있다. 이러한 기술에 대한 국제표준이 이미 제정됐으며, 나아가 데이터의 내용을 노출하지 않은 채로도 보안 처리를 원하는 대로 할 수 있는 차세대 암호 알고리즘의 국제표준화가 진행 중이다. 먼저 비식별화 관련 국제표준 현황을 살펴보고, 이어 완전동형암호의 국제표준화 현황을 살펴본다.

3.1 비식별 표준화

마이데이터 서비스 환경에서 공익적으로 데이터를 사용하려면 데이터에 있는 개인정보의 비식별(De-identif ication)화가 필요하다. ITU-T SG17에서 제정된 ITU-T 권고 X.1148(Framework of de-identification process for telecommunication service providers)은 한국에서 주도적으로 개발하였다. 데이터 생명 주기 모델을 기반으로 하는 비식별화 프로세스의 개요를 제공하는 한편, 비식별화 프로세스에서 이해 관계자의 역할 및 운영 단계, 비식별화 프로세스 프레임워크를 정의하였다.

위 권고의 후속으로 ITU-TX. rdda(Requirements for data de-identification assurance)이 개발 완료 단계에 있으며, 2023년 3월 회의에서 사전승인(Determination) 제안을 계획하고 있다. 익명화된 데이터는 개인을 재식별할 위험이 있다. 이러한 위험에 대한 수준을 평가하기 위하여 이 예비 권고는 데이터 비식별화 보증을 정의하며, 데이터 위험 평가, 데이터 사용 환경의 위험 평가, 비식별 데이터 사용 및 관리를 포함하여 데이터 비식별화 보증을 관리하는 데 필요한 일련의 요구사항을 제공한다.

한편 ISO/IEC JTC 1/SC 27/WG5에서 마이데이터 서비스와 연관된 표준들이 개발되고 있으며, 프라이버시 선호도 기반 사용자 친화형 개인정보 처리 프레임워크 (ISO/IEC 27556), 조직 프라이버시 리스크 관리(ISO/IEC 27557), 프라이버시 강화 데이터 비식별화 프레임워크(ISO/IEC 27559), 개인정보보호 관리체계의 인증 및 심사기관 요구사항 (ISO/IEC 27006-2), 동의 레코드 정보 구조 (ISO/IEC 27560, CD단계) 등 국제표준이 개발되었다[6].

3.2 완전동형암호(FHE, Fully Homomorphic Encryption) 표준

단순 사용자 인증에 해당하는 패스워드 사용을 1세대라고 한다면, 송수신 및 저장 데이터 암호를 2세대, 서명 및 키 공유에 활용하는 암호를 3세대라 구분할 수 있다. 3세대 암호가 네트워크상의 데이터 안전성을 충족하지 않는 상황이 발생하여 4세대 암호, 즉 암호화된 데이터를 복호화하지 않고 바로 처리하는 암호화가 필요하게 되었다고 볼 수 있다. 일반적으로 암호화는 데이터의 기밀성과 무결성을 제공한다. 그러나 동형암호는 데이터의 무결성을 보장하지 않는 반면, 가단성(Malleability)을 제공하고 데이터를 암호화된 채로 연산할 수 있다. 완전동형암호는 횟수 제한 없이 암호화된 데이터에 다양한 유형의 연산을 허용하는 암호를 말한다. 다만 성능 측면에서는 개선이 필요하다.

마이데이터 서비스 환경에서 개인정보 노출은 매우 민감한 사항이다. 정보가 개방적으로 유통, 활용되는 만큼 명시적 동의가 없는 상태에서 이용자 데이터에 무단 접근 및 처리(삭제 포함)가 일어난다면 마이데이터 서비스의 신뢰성이 훼손되기 때문이다. 완전동형암호는 암호화된 데이터의 내부 데이터를 모르더라도 데이터의 특정 위치에 제한적으로 접근해서 처리할 수 있는 방식으로, 마이데이터 서비스 환경에 적합한 것으로 평가받는다[7].

개인정보보호에 대한 규제가 엄격해지면서 전통적 암호 스킴(scheme)으로는 데이터를 저장하고 처리하기 어려워져서 현재 동형암호가 대안으로 대두되고 있다. 2009년 IBM이 제안한 이래 연구가 급진전된 동형암호는 산업계에서 자발적으로 표준화의 필요성을 인식하여 컨소시엄 형태의 표준화가 진행되고 있다.[8] 이를 글로벌 환경에 보급한다는 목표로 공적표준화 기구에서

도 표준화 작업을 2020년 시작했다. 관련 표준화 기구로 Homomorphic Encryption Standardization 컨소시엄, ITU-T, ISO/IEC JTC 1이 있으며, 주요 활동을 소개한다.

가. Homomorphic Encryption Standardization[8]

많은 기업과 개인이 클라우드 스토리지 및 컴퓨팅으로 전환함에 따라, 동형암호를 쉽게 적용할 수 있도록 기준을 조정하자는 요구가 있다. 현재 구현된 상태는 비전문가가 사용하기에 쉽지않아서 애플리케이션 개발자가 API를 원하는 대로 활용하기 어렵다. 이에 API를 균일화 및 단순화하기 위한 표준화가 필요하다는 공감대가 형성됐다. 산업계에서는 Microsoft, Samsung SDS, Intel, Duality Technologies, IBM, Google, SAP 등이, 기관으로는 NIH, NIST, NSF, UN/ITU 등, 학계는 서울대, Boston Univ., Columbia, EPFL, MIT, UCSD 등이 참여하고 있다.

본 컨소시엄에서는 동형암호 보안, API, 애플리케이션의 세 가지 백서를 기반으로 동형암호에 대한 표준을 개발 중이다. 현재 커뮤니티의 주요 구성원의 검토와 공개 의견 수렴이 마무리된 후, 두 번째 표준화 워크숍(March 15-16 2018, MIT, Cambridge MA, USA)에서 보안 백서를 공개적으로 승인하여 동형암호 표준의 첫 번째 버전을 제정하였다. 이 표준은 스킴 설명, 보안 속성에 대한 설명 및 보안 매개변수에 대한 표를 제공한다. 표준의 향후 버전에서는 동형암호를 위한 표준 API 및 프로그래밍 모델을 기술할 예정이다.

나. ITU-T SG17[9]

ITU-T SG17에서는 동형암호를 산업에 적용할 수 있는 분야 중 하나로 기계학습 분야를 정하고 동형암호의 이해와 데이터 분석 중 개인정보보호를 위한 처리구조, 절차와 특성들에 대한 지침을 개발 중이다. 삼성SDS, 서울대, ETRI가 에디터로 참여하여 활동하고 있으며, 2020년 3월 신규아이템(TR.sgfdm, FHE-based data collaboration in machine learning) 채택이 승인되어 개발에 착수하였다.

완전동형암호 기술을 사용하여 기계학습의 보안 추론 서비스 및 데이터 집계에 대한 보안 지침을 제공하며, 데이터 소유자가 기계학습 모델 공급자의 추론 서비스를 사용하되 각 당사자는 자신의 데이터를 공개하지 않는 구조와 절차를 제공하는 것이 주요 내용이다.

다. ISO/IEC JTC 1/SC27[10]

ISO/IEC JTC 1/SC27 WG2에서는 기존 IS 18033-6, Encryption algorithms — Part 6: Homomorphic encryption 표준이 존재하며, 2019년 개정판을 제정하였다. 이 표준은 부분동형암호를 위한 지수 ElGamal 암호와 Paillier 암호의 두 가지 메커니즘으로 구성되어 있다. 부분동형암호는 하나의 유형 연산만(예: 덧셈 Paillier 암호) 또는 곱하기(예: 지수 ElGamal 암호)를 지원하는 스킴을 기술한다.

완전동형암호(FHE)와 관련해서는 임의 작업을 지원하고 암호화 데이터에 대한 임의 계산을 허용하는 동형암호 스킴 표준을 위한 작업이 2021년 9월 신규 표준아이템(AWI 18033-8 Fully Homomorphic Encryption)이 승인을 받아 현재 WD 작업 중이다.

4. 결론

마이데이터는 규제가 필수적인 민감한 개인정보를 산업에 활용할 수 있도록 개인정보 자기결정권을 제공함으로써 개인정보 보호와 활용을 조화시키는 사업이라고 할 수 있다. 개인정보에 대한 산업적 요구가 빠르게 변화하고 있으며, 이를 처리하는 메커니즘도 지속적으로 개발되고 있다.

개인정보 처리의 핵심 분야가 보안이다. 데이터의 특정 부분에는 필요에 따라 접근할 수 있으면서도 개인식별정보를 완전하게 보호하는 프라이버시 보전형 암호가 필요하며, 완전동형암호가 이 역할을 잘 감당할 것으로 기대된다. 금융권이나 기계학습 등과 같은 분야에서 완전동형암호에 대한 관심이 국제적으로 고조되는 상황에서 한국(서울대)이 그 핵심 기술 개발에 선두주자로 활동하고 있다는 것은 매우 반가운 소식이다.

향후 완전동향암호 메커니즘 기반의 오픈 API 서비스 플랫폼을 고려해야 한다. 꼭 동형암호뿐만 아니다. 정보보호 암호학계에서도 양자 컴퓨터의 위협에 대응하고자 부지런히 양자내성암호 등 차세대 암호 연구에 박차를 가하고 있다. 필요는 발명의 어머니라는 말과 같이, 한국은 이러한 환경변화와 니즈에 대해 융통성 있게 대응해야 할 것이다.

완전동형암호 이론이 산업에 효과적으로 사용되려면 표준화가 필수다. 현재 기술과 표준 개발을 병행하여 추진 중이므로, 학계와 산업계, 정책적인 부분에서 경쟁과 조율이 필요하다.

※ 출처: TTA 저널 제204호