정 보 보 호 학 회 지
제 30 권 제4호, 2020. 8

개방형 핀테크 플랫폼의 정보보호 지침

나 재 훈*

요 약

인터넷과 모바일 기기의 발달로 사용자는 언제, 어디서나 온라인 쇼핑 및 인터넷 뱅킹 등을 스마트폰 앱으로 결제를 하는 시대가 되었으나, 모바일 뱅킹 앱 경우에도 다수의 앱을 탑재하는 불편이 발생하여 이를 개선 하고자 하는 필요성이 대두되고 있다. 그리고 정부는 핀테크 산업을 국가의 미래 신성장 동력으로 인식하고 핀테크 산업 활성화 및 핀테크 기업 지원방안 마련에 적극 나서고 있다. 그러므로 핀테크 기업이 각 금융회사와 개별적으로 협약을 맺어 금융 데이터 및 서비스에 접근 하여야 하는 앱 기반 위주의 프레임워크는 상호운용 및 유지보수에 문제점이 점점 가중되고 있으며, 이를 해소하기 위하여 표준화된 개방형(Open) 플랫폼이 기술적 방안으로 권고되고 있고, 국내 ICT 기업들의 핀테크 비즈니스에 참여를 독려하기 위하여 개방형 핀테크 플랫폼의 정보보호 지침이 마련되었으며, 이를 기반으로 국제표준이 ITU-T SG17에서 승인되었다.

Ⅰ. 서 론

2008년 글로벌 금융위기 이후 런던, 뉴욕, 실리콘밸리를 중심으로 핀테크 시장이 태동 되었으며, 초기 핀테크 시장 형성은 페이팔, 알리페이등 온라인 결제업체를 기반으로 성장하였다.

핀테크 시장은 크게 3가지 영역으로 나눌 수 있으며, 첫 번째 영역인 전자화폐는 비트코인이 각광 받으며 글로벌 이슈가 되었다. 인터넷상에서 개인대개인(P2P) 간에 이용할 목적으로 암호체계를 기초해 설계되었다. 해킹 등 보안사고 및 금융사고 논란이 있지만, 독일에서는 비트코인 거래가 합법이며, 암호화폐를 포함한 전자화폐의 법정화, 국유화하는 방안들에 대하여 연구가 진행되고 있다.

핀테크 두 번째 시장은 전자지급결제 서비스이다. IT 기술 발달과 스마트폰 확산에 따라 전자지급결제 규모도 빠르게 성장하고 있다. PG(Payment Gateway), P2P 등 신기술 결제 서비스가 주목을 받고 있다. PG는 온라인 결제 중계 업체이다. 페이팔, 알리페이가 대표적이다. 신용카드, 은행계좌 등을 가상계좌와 연동하여 다양한 금융서비스를 제공하고 있다.

셋째는 인터넷 금융회사이다. 소셜 플랫폼을 바탕으로 개인들의 대출 수요와 자금 운용을 중개하는 비즈니스 모델을 구축했다. P2P 수요자(채무자)는 시중보다 낮은 금리로 대출을 받는다. 투자자(채권자)는 대출 이자, 상환 수수료, 연체 수수료 등을 통해 마진을 취득한다. 랜딩클럽과 같은 새로운 인터넷 금융회사의 출현은 은행, 증권, 보험 등의 기존 제도권 금융회사에 위협을 주고 있다.

본 논문에서 핀테크 개방형 플랫폼의 진화와 개방형 플랫폼을 중심으로 안전한 핀테크 서비스 제공을 위한 정보보호 지침에 대한 국제표준의 내용을 살펴 본다.

Ⅱ. 핀테크 서비스와 개방형 플랫폼

2.1. 개방형 플랫폼

개방형 플랫폼은 개방형 표준에 근거하여 표준문서가 제정(게재)되고, 문서화된 응용 프로프램 인터페이스(API: Application Program Interfaces)를 제공하는, 소프트웨어 시스템을 의미한다. 개방형 API는 개발 당시 의도하였던 원래 프로그램의 소스코드의 수정을 하지 않고서도, 또 다른 기능으로 소프트웨어를 이용할 수 있는 구조를 갖고 있다. 이러한 인터페이스를 이용하여 제삼자는 기능을 추가하여 손쉽게 소프트웨어를 이용하고, 자신의 소프트웨어를 융합하여 플랫폼에 탑재 할 수

* 한국전자통신연구원 정보보호연구본부 (전문위원/책임연구원, jhnah@etri.re.kr)

있다. 개방형 플랫폼을 이용한다는 것은, 플랫폼 벤더가 아직 완료하지 못한 또는 기존에 생각하지 못한 기능을 개발자가 추가할 수 있는 부작용 (Side effect)인 것이다[1,2].

2.2. 핀테크과 정보보호

디지털화는 금융산업을 경쟁이 치열한 시장으로 바꾸고 있다. 전통적인 고가의 장비를 구축한 금융회사는 공격적으로 시장에 진출하여, 제공자 중심의 비즈니스 모델을 사용자 중심의 비즈니스 모델로의 전환을 민첩하기 위해 디지털 전환 프로젝트를 수행하고 있다. 전통적인 금융회사는 제한된 인적 자원과 기술 자원으로 사용자의 다양한 요구와 개인에게 맞춤형 서비스를 개발하는 데에 어려움을 겪고 있으므로, 핀테크 회사가 제공하는 혁신적인 핀테크 서비스에 의존할 수 밖에 없다. 스타트업 핀테크 회사는 훨씬 적은 인력으로도 실용 서비스에 접근 할 수 있는 우수한 서비스를 제공하기 위해 실제로 기존의 충분한 데이터를 기반으로 초기 제품을 검증하여 여러 금융회사와의 상호 연결 문제를 극복해야 했다. 따라서 기존 금융회사의 데이터와 서비스를 교환하고 통합하여 핀테크 제품을 개발 및 테스트 할 수 있는 무정지 개방형 플랫폼이 필요하였다.

금융 및 핀테크 회사의 개발자는 개방형 API를 사용하여 기술 (대부분 앱, 플랫폼 및 시스템)을 연결하여 디지털 금융 혁신을 이루었다. API는 플랫폼 간에 개방형 연결을 제공한다. 그러나 만약 이러한 연결을 보호하지 못한다면, 해커는 도난 당하거나 유효하지 않은 크리덴셜을 이용하여 API 서비스를 공격 할 수 있다. 금융서비스는 개방형 플랫폼 환경, 특히 API 보안에서 금융서비스를 만드는 것과 관련하여 보안 위험을 같이 고려하여야 한다.

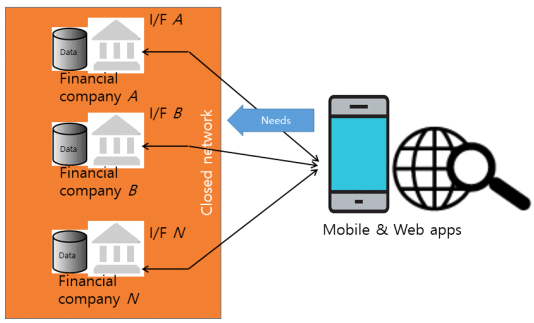
2.3. 핀테크 서비스를 위한 참조 구조

개방형 API는 기업이 보유하고 있는 서비스, 데이터를 쉽게 활용할 수 있도록 공개하여 웹서비스 및 애플리케이션 개발을 지원하는 개방 지향적인 성격을 갖는다. 사용자는 웹 검색 결과나 사용자 인터페이스(UI) 등을 제공 받을 수 있으며, 또한 직접 응용프로그램과 서비스를 개발할 수 있어 사용자 참여를 유도하는 사용자 중심의 비즈니스 모델이다[3].

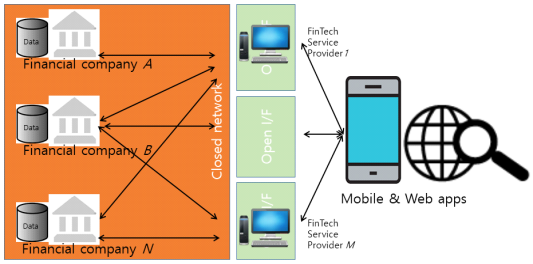
핀테크의 등장으로 금융회사와 핀테크 기업 간의 연대가 중요해지면서 국내외 금융 회사들은 개방형 API 기술에 주목하고 있다. 금융기업들은 제한된 리소스(인적 또는 기술적)를 가지고 고객들의 다양한 요구와 개인화된 서비스들을 개발하기에 어려움이 있다. 그리고 핀테크 기업들은 적은 인력으로 동일한 기능을 제공하기 위하여 여러 금융기업들에게 서로 다른 인터페이스/접근방법으로 개발하는 것은 매우 큰 어려움을 갖는 것이고, 그들이 개발한 제품을 실제적이고 충분한 데이터를 배경으로 검증할 수 있는 테스트 환경이 없다는 것 또한 큰 애로 사항이다. 그러므로 금융기업들로부터 데이터와 서비스를 제공 받고, 그리고 핀테크 회사가 개발한 제품을 시험하는 개방형 플랫폼에 대한 요구가 있는 것은 당연한 것이다.

[그림 1]은 디지털 금융 서비스를 위한 전통적인 기능적 구조를 보여준다. 이 구조에서 모든 금융 회사는 금융 서비스를 개발 및 운영하고 자체 앱을 제공하므로 사용자는 금융 회사에 직접 연결할 수 있으나, 동일하거나 유사한 종류의 서비스를 위하여 다른 금융 회사에 접속하는 경우에는 다른 앱을 사용하여야 한다. 이것은 새로운 서비스에 대하여 금융사가 개별적으로 개발을 하여야 하며, 유지보수 또한 금융사가 책임을 갖으며, 기업 경쟁력에 있어서, 매우 부적합 구조를 보이고 있다.

[그림 2]의 핀테크 서비스 구조는 정보통신기술(Information Communication Technology)이 빠르게 발전하여, 금융회사는 사용자에게 제공하는 자체 금융서비스를 개발하고 운영에 어려움을 해결한 구조이다. 핀테크 회사는 발전된 정보통신기술과 기능을 갖추고 있으므로 금융 회사는 이러한 핀테크 회사를 이용하여 자체적 개발에 의한 어려움을 극복하고 경쟁 업체보다



〔그림 1〕 전통적 디지털금융 서비스의 구조



〔그림 2〕 핀테크 서비스의 구조

더 나은 위치를 차지하기를 원한다.

[그림 2]는 기존 디지털 금융 서비스의 구조에 없는 핀테크 업체의 출현을 보여준다. 금융회사는 다른 핀테크 회사를 고용하여 다른 서비스 앱을 개발하고 각각의 API를 제공한다. 이 구조는 사용자가 각 금융회사별로 다른 앱으로 연결하여야 하는 불편함을 유발한다. 이 구조는 데이터 공유가 제한적이라는 특징이 있다. A라는 금융회사의 데이터는 핀테크 회사에 개방되어 핀테크 회사는 이 금융회사의 데이터에 액세스하기 위한 전용 권한을 갖지만, 핀테크 회사는 B 금융회사의 동일한 이용자의 데이터에 접근 권한이 없다. 사용자의 관점에서 볼 때 다른 핀테크 회사와의 인터페이스는 여전히 다르며 개방되어 있지 않다. 핀테크 회사는 각 금융 회사 및 사용자와 각 인터페이스를 보호하여야 하는 책임도 있다. 이용자들의 요구사항을 수용하기 위하여 나름 금융사가 투자를 한 결과 금융사의 내부 기술자가 아닌 외부 핀테크 기업을 활용하여 이용자들에 서비스를 제공하는 형태의 구조를 보이고 있다.

[그림 2]에서 보이는 것과 같이 금융 서비스를 제공하기 위한 유용성과 효율성은 이슈가 된다. 즉 핀테크 회사는 새로운 데이터와 서비스를 만들려면 이용자 중심으로 금융회사 전체에 대한 추가 권한이 필요하다. 반면에 핀테크와 서로 다른 금융회사와의 인터페이스는 여전히 다른 인터페이스를 갖고 있는 문제점을 보이고 있는 구조이다.

표준화된 형식의 개방형 API를 갖춘 개방형 플랫폼은 개방형 API를 사용하기 위한 효율적인 인터페이스를 제공하며, 금융회사간에 사용자 데이터를 사용하여 부가가치 데이터 및 서비스를 생성하고 공유 할 수 있는 공용 공간을 제공한다. [그림 3]의 개방형 플랫폼은 표준화된 공개 인터페이스를 제공하기에 이용자는 하나의 앱을 통하여 여러 금융사의 데이터와 서비스를 접할 수 있으며, 더욱이 핀테크 기업은 단일화된 인터페이스로 인하여 동일한 기능에 대하여 단일한 소프트웨어를 개발하므로 생산성에 있어서 매우 큰 이점을 갖으며 향후 유지보수 또한 용이 하다. 공개된 데이터와 서비스로 스타트업의 출현과 새로운 서비스 발굴로 최종 금융사의 기업의 가치가 창출될 수 있는 구조를 보이고 있다.

Ⅲ. 안전한 개방형 플랫폼의 정보보안

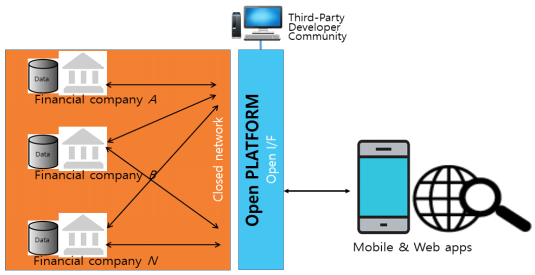
[그림 3]의 개방형 플랫폼 구조로 핀테크 서비스가 제공되면 생산성과 효율성 및 기업의 가치에 긍정적인 영향을 주므로 국내 금융권에서는 개방형 플랫폼 구축을 하였다. 그러나 중요한 데이터와 서비스를 안전하게 관리하고 처리하는 것에 대한 고려가 부족하였으며, 또 개방형 온라인 인터넷 상에서 서비스의 중단 없이 추가하고 변경하는 것이 원활하게 수행할 수 있어야 하는 것이 핵심 요구사항이다.

[그림 4]는 일반적인 개방형 플랫폼 구조에서 핀테크 서비스를 위하여 핀테크 기업이중개를 하는 형태의 구조를 보이고 있다. 즉 금융권의 운영기관은 핀테크 기업인 이용기관에게 새로운 개방형 API를 개발할 수 있는 구조와 권한을 부여하고, 이용자는 이용기관을 통하여 다양하고 풍성한 개방형 서비스를 제공 받을 수 있는 구조이다. 중간에 핀테크 기업이 포털(플랫폼)을 공개하고, 그 포털을 통하여 개방형 API를 공개하여 이용자들에게 서비스를 제공한다.

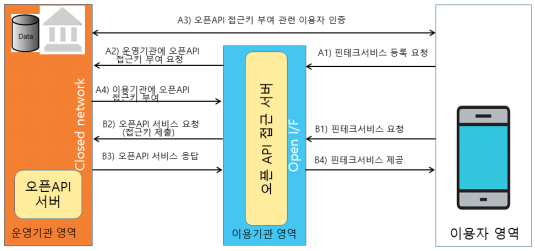
개방형 API를 사용하기 위해서는 [그림 4]의 절차를 따르며 아래에 간략한 설명을 한다.

◆ **등록 단계 (A)**

① 이용자는 이용기관에 오픈API 이용 핀테크서비스(예: 계좌잔액조회, 거래내역 조회 등) 등록을



〔그림 3〕 핀테크 서비스를 위한 개방형 플랫폼 구조



〔그림 4〕 핀테크 서비스를 위한 개방형 플랫폼 구조 및 절차

요청한다.

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

③ 운영기관은 오픈API 접근키 부여에 앞서 이용자 인증을 수행한다.

④ 운영기관은 오픈API 접근키를 이용기관에 부여한다.

◆ 이용 단계 (B)

① 이용자가 이용기관에 오픈API 이용 핀테크 서비스(예: 계좌잔액조회)를 요청한다.

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

③ 운영기관은 해당되는 오픈API 서비스 응답을 이용기관에 제공한다.

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

3.1. 개방형 핀테크 플랫폼의 정보보호 지침 [4,5]

본 절에서 금융보안연구원에서 작성하여 배포된 “금융권 오픈 API 이용기관과 운용기관의 자체 보안점검 가이드”를 참고하여 국제표준화를 추진하였음을 밝히며, 세부 사항은 문헌을 참고 할 것을 권고하며 ITU-T SG17에서 국제표준의 지침 항목을 제시한다.

〈〈이용기관의 보안점검 지침〉〉

3.1.1 정보보호 정책·조직
3.1.1.1 정보보호최고책임자 지정 및 실무조직
3.1.1.2 정보보호정책 수립 및 공표

3.1.2 외부자 관리
3.1.2.1 위탁업체 선정 및 관리

3.1.3 정보자산 관리
3.1.3.1 정보자산 식별 및 등급부여
3.1.3.2 정보자산별 책임자 지정

3.1.4 정보보호 교육
3.1.4.1 정보보호 교육계획 수립 및 이행
3.1.4.2 실무자 정보보호 교육 이수

3.1.5 인적 보안
3.1.5.1 비밀유지서약서
3.1.5.2 직무분리
3.1.5.3 퇴직 및 직무변경 관리

3.1.6 위험 관리
3.1.6.1 취약점 점검 정책 수립 및 점검 수행

3.1.7 침해사고 대응
3.1.7.1 침해사고 대응절차 마련 및 교육 시행
3.1.7.2 침해사고 대응 관련 로그 보존 및 모니터링

3.1.8 장애 대응
3.1.3.1.1 백업정책 수립 및 복구절차 마련

3.1.9 이용자 보호
3.1.9.1 개인정보 처리 관련 이용자 보호
3.1.9.2 개인·신용정보 접근 및 거래지시 권한 관련 안내
3.1.9.3 이용자 고충 처리방침 마련 및 공개
3.1.9.4 이용자 보안 주의사항 안내

3.1.10 물리적 보안
3.1.10.1 보호구역 지정 및 출입 통제
3.1.10.2 보호구역 반출입 관리
3.1.10.3 사무실 환경 보안 정책 수립 및 이행

3.1.11 개발 보안
3.1.11.1 설계 시 보안 요구사항 도출 및 반영
3.1.11.2 시큐어 코딩 적용 및 보안 취약점 점검·보완

3.1.11.3 테스트 시 이용자 개인·신용정보 사용 제한
3.1.11.4 소스 프로그램 및 전산원장 대상 접근·변경 통제

3.1.12 암호 통제
3.1.12.1 중요 정보 암호화 정책 수립 및 이행

3.1.13 접근 통제
3.1.13.1 중요 정보자산 계정 및 접근 권한 관리

3.1.14 시스템 보안
3.1.14.1 주요 시스템 등의 악성코드 감염 및 정보유출 방지
3.1.14.2 인터넷망을 통한 원격관리 통제
3.1.14.3 적 외 기능·프로그램·포트 등 제거
3.1.14.4 중요 서버 독립 운영 및 정보보호시스템 적용
3.1.14.5 공개용 웹서버 보호대책 마련
3.1.14.6 중요 보안패치 적용 지침 수립 및 이행

3.1.15 네트워크 보안
3.1.15.1 DMZ 구간 구성
3.1.15.2 내부망 사설IP 활용 및 주요 시스템 배치
3.1.15.3 무선 네트워크 이용 최소화 및 보안대책 수립·적용
3.1.15.4 대외기관과 통신 시 보안통신 적용

〈〈운영기관의 보안점검 지침〉〉

3.1.16 거래 당사자 인증
3.1.16.1 이용자 인증 방법의 적정성
3.1.16.2 이용기관 인증 방법의 적정성
3.1.16.3 고위험 전자금융거래 인증 방법의 적정성
3.1.16.4 API 접근 요청 처리 시 권한의 적정성 검증
3.1.16.5 운영기관 정보처리시스템 인증
3.1.16.6 이용자 인증 우회방지
3.1.16.7 접근키 등 유출 위험 완화 대책
3.1.16.8 이용기관 인증정보 추측방지
3.1.16.9 인증 및 거래 관련 기록관리
3.1.16.10 인증키 관리

3.1.17 거래정보의 기밀성 및 무결성
3.1.17.1 거래정보 등의 기밀성
3.1.17.2 거래정보 등의 무결성
3.1.17.3 안전한 암호 알고리즘 사용
3.1.17.4 안전한 키관리
3.1.17.5 안전한 암호 프로그램 관리

3.1.18 정보처리시스템 보호대책
3.1.18.1 관리자 및 책임자 지정·운영
3.1.18.2 중요 패치 수행
3.1.18.3 운영체제 계정 추가인증
3.1.18.4 서버접근 중요단말 보호
3.1.18.5 서버 해킹 방지
3.1.18.6 보안성 검증 및 취약점 점검
3.1.18.7 공개용 서버 설치 및 접근통제
3.1.18.8 이용기관 침해사고 대응

3.1.19 고객단말기 보호대책
3.1.19.1 입력정보보호
3.1.19.2 이용기관 고객단말기 보호대책
3.1.19.3 이용기관 서명 인증서 관리

3.1.20 정보유출 방지대책
3.1.20.1 접근계정 관리
3.1.20.2 정보시스템 로그 기록 및 분석
3.1.20.3 이용기관 정보유출 방지대책

3.1.21 이상금융거래 방지대책
3.1.21.1 이상금융거래 모니터링 및 탐지
3.1.21.2 이상금융거래 탐지 시 대응
3.1.21.3 중요거래 고객통지

3.1.22 시스템 가용성 확보 및 비상대책
3.1.22.1 업무지속성 확보방안 수립
3.1.22.2 주요 전산장비 이중화
3.1.22.3 백업·소산 관리

3.1.23 시스템 가용성 확보 및 비상대책
3.1.23.1 이용기관 물리적 접근통제

Ⅳ. 결 론

개방형 플랫폼 및 개방형 API은 이미 산업에서 필수적인 기술로 자리를 차지하였다. 이를 제도권에서 산업 육성을 위하여 개방형 플랫폼을 구축하고, 핀테크 업체들이 개발한 API를 시험할 수 있도록 테스트베드를 제공하고 있다. 또한 이와 병행하여 금융보안연구원은 2018년 12월 운용기관과 이용기관에서 개방형 플랫폼을 구축함에 있어서 지켜야 할 정보보호 지침을 발행하였으며, 이를 근거로, 즉 한국의 기술 경험을 바탕으로 국제표준화를 달성한 것으로 그 의가 크다고 사료된다 (ITU-T X.1149, Security framework for open platform of FinTech services). 미국, 영국, 일본의 관심과 알리페이 및 시만택 (브로드콤에 2019년 합병)의 협력하에 표준이 완성되었으며, 향후 이 지침에 근거하여 구체적인 정보보호 기술을 근거로 핀테크 정보보호 표준을 개발이 확대 되기를 기대 한다.

참 고 문 헌

[1] 해외 금융회사의 오픈 API 구축 동향 및 시사점, 2015.12. 지급결제와 정보기술 제62호, 금융결제원

[2] Report of Review Committee on Open APIs: Promoting Open Innovation https://www.zenginkyo.or.jp/fileadmin/res/news/news290713_3.pdf

[3] Open platform, https://en.wikipedia.org/wiki/Open_platform

[4] Report of Review Committee on Open APIs: Promoting Open Innovation. https://www.zenginkyo.or.jp/fileadmin/res/news/news290713_3.pdf

[5] 금융권 오픈API 이용기관 자체 보안점검 가이드, 금융보안연구원 https://www.fsec.or.kr/common/proc/fsec/bbs/147/fileDownLoad/1786.do

〈저자소개〉

나 재 훈 (Jae Hoon Nah)

종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 학사
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 정보공학 박사
1987년 ~ 현재 : 한국전자통신연구원 정보보호연구본부 전문위원/책임연구원
2019년~현재 : 글로벌ICT표준마에스트로
2009년 ~ 현재 : ITU-T SG17 WP4 부의장, Q7 라포처
2018년7월~현재 : TC307 대표전문위원
2011년~2012년 : 한국정보보호학회 학회지 편집위원장
2011년~현재 : 한국정보보호학회 학회지 정보보호 국제표준 특집호 책임 편집위원
<관심분야> 블록체인보안, 핀테크보안, 웹메쉬업보안, 스마트시티보안, 익명인증