정 보 보 호 학 회 지
제28권 제4호, 2018. 8

안전한 핀테크 서비스를 위한 오픈플랫폼 표준화 동향

나 재 훈*, 나 중 찬*

요 약

핀테크는 국제적으로 매우 각광을 받고 있는 산업이다. 이러한 동향에 편승하여 국제표준화에서도 많은 관심을 보이고 있다. 기술 개발을 통하여 핀테크로 구축된 정보를 공개적으로 사용이 가능하며, 이를 기반으로 새로운 산업 창출이 가능하기 때문이다. 간편결제와 같이 사용자의 편의성을 제공하는 전위적(Front-end)인 역할도 있지만, 서버의 정보를 폐쇄적으로 관리 하던 것을 핀테크 기술을 이용하여 공개되고, 사용자 및 스타트업들이 공개된 정보를 통하여 새로운 융합정보, 나아가 융합 서비스를 창출하는 후위적 역할도 있다. 핀테크 산업의 기반기술이 공개소프트웨어로 제공되고 있으며, 이를 이용하여 빠른 발전을 하고 있으나, 공개성으로 인하여 취약점 마저도 공개되어 정보보안의 위협으로 작용되므로 오픈 플랫폼의 정보보안을 중심으로 핀테크 정보보안 기술동향과 표준의 방향을 살펴본다.

Ⅰ. 서 론

최근에 핀테크(Fintech) 기술에 대한 관심이 IT뿐만 아니라 금융시장에서도 뜨겁다. 핀테크는 금융을 뜻하는 Finance와 기술을 뜻하는 Technology의 합성어로 IT기술을 접목시킨 금융사업을 의미한다[1]. 지급결제, 송금/전자화폐, 펀딩, 자산관리 등 여러 분야에서 서비스를 제공한다.

국제 핀테크 시장이 커짐에 따라, 국내에서도 국내 핀테크 기술을 개발 및 출시하기 집중되고 있다. 핀테크 기술을 개발하여 사용자에게 좋은 서비스를 제공하는 것도 좋지만, 핀테크 기술을 안전하게 사용하기 위한 보안기술도 간과되어서는 안된다.

본 논문에서 핀테크 서비스를 살펴보고, 안전한 핀테크 서비스를 위한 플랫폼 기술 동향 및 표준 동향에 대하여 살펴본다.

Ⅱ. 핀테크 서비스와 오픈 플랫폼

2.1. 핀테크 서비스

2008년 글로벌 금융위기 이후 런던, 뉴욕, 실리콘밸리를 중심으로 시장이 태동되었다. 초기 핀테크 시장 형성은 결제 업체가 주도했다. 페이팔, 알리페이등 글로벌 결제 업체들은 온라인 결제 서비스를 통해 성장했다.

이들은 지급 결제뿐만 아니라 송금 등 새로운 서비스를 제공하기 시작했다. 본격적인 산업의 성장은 알리바바, 구글, 페이스북 등 글로벌 플랫폼 업체들의 관련 비즈니스 진출 이후다. 이들은 결제업체, 은행 등을 인수/투자하며 핀테크 시장에 진출했다. 최근에는 신규 벤처기업들이 예금, 대출, 투자자문 서비스도 제공하는 등 핀테크 영역을 확대 시키고 있다.

핀테크 시장은 크게 3가지 영역으로 나눌 수 있다. 첫째 전자 화폐이다. 전자 화폐는 이전 가능한 금전적 가치가 전자적 방법으로 저장되어 발행된 증표 또는 정보다. 우리가 실생활에서 흔히 사용하는 교통카드, 도토리(싸이월드), 일본의 나나코(세븐일레븐) 등도 전자화폐의 일종이다.

전자화폐는 비트코인이 각광받으며 글로벌 이슈가 됐다. 인터넷상에서 개인대개인(P2P) 간에 이용할 목적으로 암호체계에 기초해 설계됐다. 해킹 등 보안사고 및 금융사고 논란이 있지만 독일에서는 비트코인 거래가 합법이다. ECB(유럽중안은행)에서도 일부에서 제기한 폰지사기 가능성이 낮다고 언급했다.

핀테크 두 번째 시장은 전자지급결제서비스이다. IT기술 발달과 스마트폰 확산에 따라 전자지급결제 규모

본 논문은 2018년도 과학기술정보통신부의 재원으로 정보통신방송표준개발지원사업의 일환으로 수행되었음.[2017-0-00472, 안전한 웹기반 개방형 핀테크 플랫폼 표준 개발]
* 한국전자통신연구원 시스템보안연구부(jhnah@etri.re.kr, njc@etri.re.kr)

도 빠르게 성장하고 있다. PG(Payment Gateway), 금융 OTT(Over The Top), 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. 금융 OTT는 IT 플랫폼 회사의 통신(플랫폼) 기반 결제 서비스이다. 구글 월렛, 아마존 페이먼트, 카카오 페이가 해당된다. NFC, 소셜 네트워크를 기반으로 개인간 송금 및 온/오프라인 결재를 제공한다. Venmo, GEO Payment 등 소셜, 위치기반 등 혁신적 IT 기술을 바탕으로 새롭게 등장한 전자결제 서비스도 각광을 받고 있다. 새로운 결제수단의 등장으로 단일 결제수단이 아닌 다양한 채널이 융합된 결제서비스 제공도 예상된다.

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 위협으로 작용 할 수 있다.

2.2. 오픈 플랫폼

오픈 플랫폼은 오픈 표준에 근거하여 표준문서가 제정(게재)되고, 완전하게 문서화된 외부 응용 프로프램 인터페이스(API: Application Program Interfaces)를 제공하는, 소프트웨어 시스템을 의미한다. API는 원래 프로그램의 의도하지 않은 다른 기능으로 소프트웨어를 이용할 수 있도록, 소스코드의 수정을 하지 않고서도 허용을 하고 있다. 이러한 인터페이스를 이용하여 제삼자는 기능을 추가하기 위하여 플랫폼에 통합을 할 수 있다.

오픈 플랫폼이란 벤더가 기능을 허용하고, 지원하는 것을 의미한다. 오픈 플랫폼을 이용한다는 것은, 플랫폼 벤더가 아직 완료하지 못한 또는 생각지도 못한 기능을 개발자가 추가할 수 있는 것이다. 오픈 플랫폼은 규격이 공적으로 오픈 표준으로 공급이 되고 개발자들로 현재의 기능을 변경하도록 허용한다[3].

또한 소프트웨어 플랫폼이 오픈이라고 호칭할 수 있으려면 아래와 같은 특징을 하나 이상 갖는 것을 전제로 한다:

- 오픈API: 공개하는 API에 대하여 문서화되어 있으며 모든 응용개발자들이 사용이 가능하게 제공되는 경우
- 확장성 (Extensibility): 본래 계획되지 않은 목적으로 플랫폼을 이용하려고 할 때에 기능들(Capabilities)을 참조하는 경우
- 오픈소스: 아무에게나 또 어느 목적으로 소프트웨어를 연구와 변경 그리고 배포를 위하여 저작권자가 권리를 이양한 라이선스를 갖고 있는 프로그래밍언어의 프로그램 부분의 소스 코드를 이용 가능한 경우
- 수용성 (Adoptability): 특정 비즈니스 협상을 우회하여 오픈플랫폼을 다른 사람들이 이용 가능하게 한 경우-무료 로열티(Royalty-free)만을 의미하지는 않음, 라이선스 조건하에 비차별적 제공
- 적응성(Adaptability): 규격이 공개적으로 이용할 수 있음을 전제로 하고, 플랫폼의 기존 기능을 변경할 수 있는 경우 - 새로운 기능을 추가 하는 것과는 다른 경우

Ⅲ. 오픈 플랫폼의 진화

최근 핀테크가 세계적인 트렌드로 자리함에 따라 영국, 미국 등을 중심으로 금융회사와 핀테크 기업 간에 연대가 활발히 이루어지고 있다. 이에 따라 금융회사 내부 시스템과 핀테크 기업을 연결하는 도구로서 금융회사에서는 오픈 API에 대한 논의가 지속되고 있다.

오픈 API는 API의 개념을 웹으로 확장한 것으로 기업이 보유한 서비스, 정보등을 쉽게 활용할 수 있도록 하여 웹서비스 및 애플리케이션 개발을 지원하는 개방지향적인 성격을 갖는다. 또한 이용자는 일방적인 웹 검색 결과나 사용자 인터페이스(UI) 등을 제공받는데 그치지 않고 직접 응용프로그램과 서비스를 개발할 수 있어 사용자 참여를 유도하는 사용자 중심의 비즈니스 모델이다[2].

핀테크의 등장으로 금융회사와 핀테크 기업 간의 연대가 중요해지면서 국내외 금융 회사들은 이를 위한 수단의 하나로 오픈 API 기술에 주목하고 있다. 금융회사의 오픈 API는 핀테크 기업이 새로운 금융서비스를 손쉽게 개발할 수 있도록 금융정보 요청 방법을 정의한다. 최근 모바일 생태계가 외부 개발자를 참여시키는 개방형 플랫폼으로 변화하면서 오픈 API를 제공하거나 도입을 추진하는 금융회사가 늘어나는 추세이다.

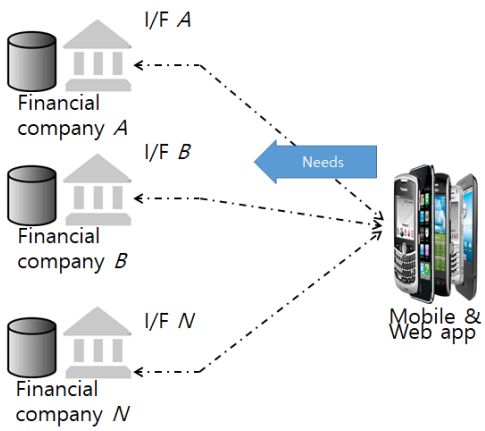
금융기업들은 제한된 리소스(인적 그리고 기술적)를 가지고 고객들의 다양한 니즈와 개인화된 서비스들을 감당하기에 어려움이 있다. 그리고 핀테크(FinTech) 기업들은 적은 인력으로 동일한 기능을 제공하기 위하여 여러 금융기업들에게 서로 다른 접근방법으로 개발하는 것은 어려움을 갖는 것이고, 또한 그들이 개발한 제품을 실제적이고 충분한 데이터를 배경으로 검증할 수 있는 테스트 환경이 없다. 그러므로 금융기업들로부터 데이터와 서비스를 교환하고 종합하는 그리고 핀테크 제품을 시험하는 오픈 플랫폼에 대한 요구가 있는 것은 당연한 것이다.

핀테크 혁명은 최근 수년 동안에 가장 두각을 나타내는 기술 토픽이다. 이것은 현재의 상황과 현대의 구습의 기관들을 파괴하고, 고객이 금융제품과 서비스에 접근하는 방편을 변화시키고 있다.

핀테크 스타트업들은 그 수에 있어서 또 그 전문성에 있어서도 성장하고 있으며, 전통적인 서비스 제공자들과 관계를 만들고 유지 하려고 할 것이다. 그리고 시스템간의 인터페이스는 구 시스템 설계자들에 의하여 만들어진 조화롭지 못한 규칙에 의하여 발생하는 사이버 취약점의 공동 원천이 될 수 있다.

핀테크 기업들은 그들의 플랫폼의 안전을 위하여 모든 노력을 해야 할 의무를 갖고 있다. 이것은 “설계에 의한 정보보호(Security by design)”의 원칙을 취하는 것을 요구하며, 설계나 또는 구현중에 그리고 그 이후에 정보보호를 적용할 것이 아니고 처음부터 정보보호를 플랫폼에 바로 구축을 하는 것을 요구하는 것이다.

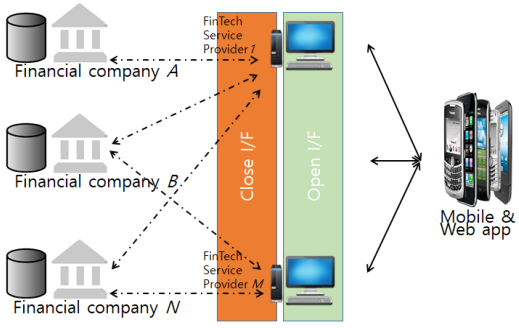
그림 1의 금융 서비스의 구조는 금융 서비스 제공자가 일방적으로 서비스를 구축하여 이용자들에 제공하는 형태를 보이고 있다. 이는 각 금융사가 자신의 데이터와 서비스를 자신들의 방식으로 이용자들에게 제공하는 것이다. 이는 각 금융사를 접속하기 위해서는 각기 다른 앱을 이용하여 접속을 하여야 한다는 것이다. 각 금융사별로 서로 다른 수준의 서비스에 대하여 이용자들은 불평을 하고, 금융사에게 동등한 수준의 서비스를 요구할 것이며, 더욱이 공개되지도 않을뿐더러, 개발되지도 않은 서비스로 인하여 금융사의 기업 가치를 판단할 수가 없어서 이용자들은 금융사를 선택할 수 있는 여지가 없는 형태의 구조를 갖고 있다. 이것은 새로운 서비스를 개발하기 위하여 유사한 기능에 대하여 금융사가 개별적으로 개발을 하여야 하며, 유지보수 또한 금융사가 책임을 갖는 구조를 가지고 있어서, 기업 경쟁력에 매우 부적합 구조를 보이고 있다.



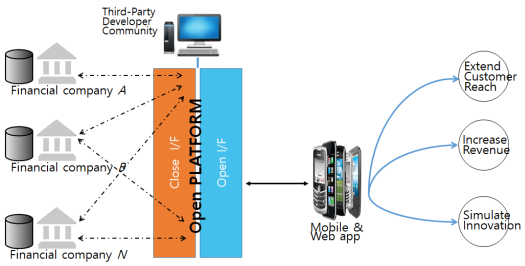
〔그림 1〕 디지털금융 서비스의 기능구조

그림 2의 핀테크 서비스 구조는 이용자들의 요구사항을 적극 수용하기 위하여 나름 금융사가 투자를 한 결과 금융사의 내부 기술자가 아닌 외부 핀테크 기업을 활용하여 이용자들에 서비스를 제공하는 형태의 구조를 보이고 있다. 이 구조는 핀테크 기업이 금융사를 위하여 서비스 구축을 위하여 소프트웨어를 개발하고 오픈 인터페이스를 이용자들에게 제공하여 주고 있다는 커다란 장점을 가지고 있다. 그러나 유사하거나 동일한 기능을 이용자들에게 각 금융사별로 다른 인터페이스로 서비스를 제공하기에 이용자는 각각의 앱을 설치하여 서비스를 처리하여야 한다.

그림 3의 오픈 플랫폼은 표준화된 공개 인터페이스를 제공하기에 이용자는 하나의 앱을 통하여 여러 금융사의 데이터와 서비스를 접할 수 있으며, 더욱이 핀테크 기업은 단일화된 인터페이스로 인하여 동일한 기능에



〔그림 2〕 핀테크 서비스의 구조



〔그림 3〕 핀테크 서비스를 위한 오픈 플랫폼 구조

대하여 단일한 소프트웨어를 개발하므로 생산성에 있어서 매우 큰 이점을 갖으며 향후 유지보수 또한 용이하게 되고, 공개된 데이터와 서비스로 스타트업의 출현과 새로운 서비스 발굴로 최종 금융사의 기업의 가치가 창출될 수 있는 구조를 보이고 있다.

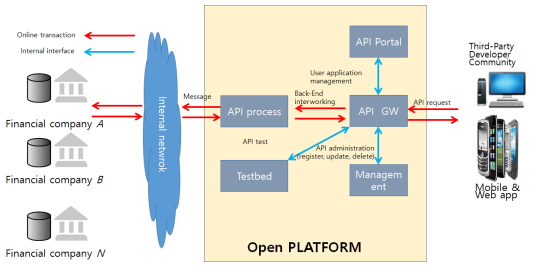
Ⅳ. 안전한 오픈 플랫폼 시스템 구조

Ⅲ장의 오픈 플랫폼 구조로 핀테크 서비스가 제공되면 생산성과 효율성 및 기업의 가치에 긍정적인 영향을 주므로 국내 금융권에서는 오픈 플랫폼 구축을 이미 진행하였다. 그러나 중요한 데이터와 서비스를 안전하게 관리하고 처리하는 것에 대한 고려가 부족하며, 오픈 온라인 인터넷 상에서 서비스의 중단 없이 추가하고 변경하는 것이 원활하게 수행할 수 있어야 하는 것이 핵심 요구사항이다.

안전한 핀테크 서비스를 위하여 먼저 고려하여야 할 사항은 기존에 제공되고 있는 API의 접근제어이다. 이것은 웹에서 추구하고 있었던 SOP(Single Origin Policy)를 파괴하는 것이다. 즉 매쉬업 구조의 서비스를 구축하여야 하며, 이를 위한 인증 및 권한관리 도메인간의 데이터의 이동 및 융합을 위한 정보보호 메커니즘이 제공되어야 한다. 우선 쿠키 기반의 인증이 토큰 기반의 인증방식으로 변경한 OAuth 2.0을 임의적으로 사용을 하고 있다. 임의적이라는 말은 금융권에서는 아직 OAuth 2.0이 핀테크 서비스를 위한 인증 방식인가에 대한 정확한 결정을 내리지 않은 상황이며 이를 심도 있게 검토를 하고 있는 중이다.

또한 웹은 이용자가 서버를 방문하지만, API 방식은 서비스와 데이터를 가져감으로 세션 개념이 없으며, 전달된 서비스나 데이터에 대한 통제권이 없는 상태에서 관리하며, API를 쉽게 변경하고, 호환성을 보장하며 자동화된 방식으로 유지/관리하는 구조가 필요하다.

그림 4는 오픈 API를 제공하면서, API를 변경, 그리고 추가를 함과 온라인 상에서 자유롭게 시험을 할 수 있는 오픈 플랫폼의 구조를 보이고 있다. 이용자가 직접 API를 접속하는 API GW(게이트웨이)가 있어서 이용자로부터 입력된 요청을 내부 네트워크를 통하여 해당 서버에 맞는 명령어로 전환하여 수행 처리하는 API업무처리가 있다. 이러한 API에 관한 인터넷 공지를 담당하는 포털이 있어서, API 사용법, 변경하기 위한 기초정보, 사용권한 등등을 문서화하여 이용자나 핀테크 개발자에게 공지를 하는 포털이 운영된다. 그리고 오픈 API를 수정 또는 추가 하려고 할 때에 사전에 오픈 플랫폼에 적합한지 그리고 안전한지를 검증하기 위한 테스트베드가 있으며, 검증을 마친 오픈 API를 등록, 수정, 삭제를 관리하는 관리센터가 있다. 이와 같은 구조에서 도메인을 넘나드는 이용자 인증 및 정보의 융합에 따른 안전성을 보장하는 오픈플랫폼 서비스의 정보보호와 오픈 플랫폼의 각 콤토넌트간의 연동을 통한 각 인터페이스에서 상호작용 가운데 서비스 및 데이터와 시스템의 안전성을 위한 정보보호 메커니즘이 폭넓게 고려되어야 한다.



〔그림 4〕 안전한 핀테크 서비스를 위한 오픈 플랫폼 구조

Ⅴ. 오픈 API의 위협(Threat)

오픈 API는 금융기관의 시스템에서 다른 회사를 통행 새로운 통신 경로를 설정하여 사용자에게 새로운 서비스를 제공하는데, 이러한 통신 경로가 데이터 유출이나 변조 그리고 승인되지 않은 트랜잭션을 초래하는 위협이 있을 수 있다[4].

a. 제3 자의 로그인 ID 및 암호 누출은 권한 없이도 제3 자의 리소스에 접근 위협
b. 제3 자 시스템이 공격으로 서비스 기능이 중단되

고 대량의 데이터 유출, 위조 또는 데이터 손실 및 승인되지 않은 송금이 발생

c 권한 없이 접근 토큰과 허가 없이 토큰 발행하는 은행 API 시스템의 위협

d 토큰의 유출 또는 위조로 인해 은행에서 대규모로 데이터가 누출 될 위험이 있으며 위조 또는 정보 손실 및 승인되지 않은 송금이 발생

e. 라우터와 같은 통신 경로 해킹 및 무선 통신 차단으로 인해 정보 유출, 위조 또는 정보 유출 및 무단 송금 위험

f. 제3 자 프로그램의 부적함으로 인해 은행 시스템 오류 발생

g. 불필요하게 많은 양의 데이터가 은행 오픈 API 통신 경로를 통해 전송되므로 은행 시스템에 대한 부하가 증가하고 다른 은행 서비스에 영향을 줌

h. 내부 임원 및 직원이 사용자 정보를 무단으로 사용하는 위협 (재판매 및 개인사용 포함)

i. 계좌 잔액 정보를 얻거나 승인되지 않은 결제 지시를 보내기 위해 승인 없이 토큰을 사용하는 내부 임원 및 직원의 위험

Ⅵ. 결 론

오픈 플랫폼은 웹서비스 산업의 경쟁력을 제고 하고 있으며 고객의 선택의 폭을 넓히는 방법 중의 하나로 제시되고 있다. 금융기업이 제삼자에게 API를 공개할지라도, 그것이 표준으로 개발되지 않는다면 각자의 API에 따른 개발은 비생산적이고 비효율적인 것이다. 전체적이고 종합된 방법으로 핀테크 개발자들이 필요한 제어와 궁극적으로 고객을 위한 종대종 보호를 보증할 수 있도록 국제표준화가 선행되어야 한다고 미국, 영국 등의 의견이 있었으며, 2017년 9월 ITU-T SG17 제네바 회의에서 신규 표준아이템이 X.sfop: Security framework of open platform for FinTech services (Q.7/17, Secure application services) 한국의 제안으로 승인되었다. 이는 국내의 기술을 국제적 기술로 승화 시키며, 국제 경쟁력을 높이는 표준화로 평가되고 있다. 이 표준 아이템에 대하여 한중일간에 긍정적이고 적극적인 논의가 진행중에 있으며, 일본의 은행권에서 상용중인 오픈 API에 대한 경험을 이 표준에 반영하기를 의도하고 있으며, 중국은 알리바바의 표준전문가를 ITU-T SG17 회의에 참여하게 하여 표준화 협력에 대한 의사 표명을 하였다.

참 고 문 헌

[1] 금융위원회, “핀테크”, 금융용어사전, 2015, http://fsc.go.kr/know/wrd_list.jsp

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

[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

〈저 자 소 개〉

나 재 훈 (Jae Hoon Nah)
종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 정보공학 박사
1987년~현재 : 한국전자통신연구원 정보보호연구본부 전문위원/책임연구원
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, CPS보안, P2P보안, 웹메쉬업보안

나 중 찬 (Jung Chan Na)
종신회원

1986년 2월 : 충남대학교 계산통계학과 학사
1989년 2월 : 숭실대학교 전자계산학과 석사
2004년 2월 : 충남대학교 컴퓨터과학과 박사
1989년2월~현재: 정보보호연구본부 시스템보안연구그룹장/책임연구원
<관심분야> ITS보안, 제어시스템보안, 펌웨어 보안 취약성