Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.6, Dec. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.6.1271

안전한 오픈뱅킹 구축을 위한 정책 및 B2B2C 모델에 관한 연구

최 대 현,† 김 인 석‡
고려대학교 정보보호대학원

A Study on the Policy Proposal and Model B2B2C for Safe Open Banking

Dae-Hyun Choi,† In-Seok Kim‡
Graduate School of Information Security, Korea University

요 약

4차 산업혁명과 디지털 전환(digital transformation)은 국내 금융 생태계에도 큰 변화를 가져오고 있다. 이미 해외 글로벌 금융회사들은 금융시장을 개방하고 핀테크 기업들과 상생의 방안을 모색하여 새로운 금융 비즈니스를 발굴하고 있다. 하지만 국내 금융환경은 독점적이고 폐쇄적인 구조로 이러한 변화에 대응하지 못했던 것도 사실이다. 이에 정부는 2019년 12월 금융결제 시스템의 전면 개방을 목표로 오픈뱅킹의 도입을 추진하기 시작했다. 하지만 기존 단순한 금융거래 구조와 달리 오픈뱅킹은 금융회사, 핀테크 기업, 고객 등 거래의 연계 구조가 복잡하여 금융사고 발생 시 이해 당사자 간 책임 관계가 불명확하여 해소되지 못한 부분이 아직도 존재하고 있다. 본 연구는 오픈뱅킹의 보안위협을 심도 있게 분석하였다. 이를 통해 국내 오픈뱅킹의 안전성을 높이고 금융소비자 보호를 위해 정부와 금융회사가 개선해야 할 정책 제안과 기존 모델의 취약한 부분을 개선한 새로운 금융모델을 제시하고자 한다.

ABSTRACT

The fourth industrial revolution and digital transformation are also bringing major changes to the financial ecosystem in Korea. Already, global financial firms overseas are opening their financial markets and exploring new financial businesses by seeking ways to co-prosperity with fintech firms. However, it is also true that the domestic financial environment has failed to respond to the changes due to its monopolistic and closed structure. In response, the government began pushing for the introduction of open banking in December 2019 with the aim of fully opening the financial settlement system. However, unlike the existing simple financial transaction structure, open banking still has an unresolved part due to the unclear relationship of responsibilities between interested parties in the event of financial accidents due to the complex linkage structure of transactions such as financial firms, fintech firms and customers. This study analyzed the security threat of open banking in depth. By doing so, the government and financial firms want to present policy proposals that need to be improved to enhance the safety of open banking in korea and protect financial consumers, as well as new financial models that have improved the vulnerable parts of existing models.

Keywords: B2B2C, Open Banking, Open API, OAuth

I. 서 론

최근 금융권에서의 최대 화두는 핀테크(fintech) 기술의 활성화로 비롯된 디지털 전환(digital transformation)으로 꼽을 수 있을 것이다. 디지털 전환은 디지털 기술을 사회 전반에 적용하여 전통적인

Received(10. 08. 2019), Modified(11. 12. 2019), Accepted(11. 12. 2019)

† 주저자, fradcom@korea.ac.kr
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

사회 구조를 혁신시키는 것이다. 금융권에서의 디지털 전환도 크게 다르지 않으며 금융 서비스인 수신, 여신, 외환, 지급결제 등 금융업 본연의 기능을 전통적인 방식에서 벗어나 새로운 혁신적 방법을 통해 고객이 원하는 다양한 금융서비스를 경쟁사보다 빠르게 시장에 제공하는 것이다. 디지털 전환을 앞당기기 위해서는 금융회사가 여러 기업과 협업하는 개방성의 확대가 중요하며 이에 따라 오픈뱅킹(open banking) 역시 빠른 속도로 주목받고 있다. 국내 금융권도 금융당국의 규제 완화와 기술의 발전을 통해 오픈뱅킹 도입에 적극적이다. 이러한 변화는 금융회사와 외부 기관과의 협업을 가속 시킬 것으로 예상할 수 있으며 개방형 혁신 체제로의 전환과 다양한 형태의 영업 전략 등의 계기가 될 것으로 보인다. 다만 고객 정보의 관리 소홀, API 인증 우회 등 새로운 보안위협과 금융범죄 등의 부작용도 커질 것으로 우려된다.

본 연구에서는 국내외 금융회사의 오픈뱅킹 적용 현황과 서비스 및 연결모델을 살펴보고 인증에 대한 기반 기술을 분석하였다. 이 분석 결과를 바탕으로 금융회사, 핀테크 기업, 그리고 고객이라는 주체들의 관계에 적용할 수 있는 OAuth 2.0 기반 B2B2(금융회사-핀테크 기업-고객) 오픈뱅킹을 구축하는데 요구되는 정책 및 모델을 제시하고자 한다.

II. 국내외 오픈뱅킹 동향

2.1 오픈 API 개요

오픈 API는 오픈뱅킹을 구현하는 핵심 기술로 인터넷상의 서비스, 데이터를 외부의 사용자 또는 개발자가 사용할 수 있도록 개방해 놓은 공개된 API이다. 오픈 API는 다양한 개발자들이 사용 가능한 형태로 배포되며, 네트워크 부하가 낮고, HTTP 프로토콜 상위에서 동작하기 때문에 플랫폼에 독립적인 특징을 지닌다. 오픈 API는 개별적으로 매우 단일 기능을 수행하지만 여러 오픈 API를 조합하면 다양한 매쉬업[1] 서비스의 제공이 가능해진다. 그 예로 국내를 포함하여 미국, EU, 뉴질랜드 등 많은 국가에서 행정, 재난, 교육 등 다양한 분야의 공공 데이터를 간단한 오픈 API로 제공하고 오픈 API의 조합을 통해 복잡한 서비스를 손쉬운 방법으로 개발하도록 장려하고 있다. 글로벌 기업인 Google, Yahoo, Amazon, Facebook 등에서도 다양한 기능을 수행하는 오픈 API를 배포하여 새로운 서비스 개발을 독려하고 있다[2]. 구체적인 사례로 오픈 API는 현재 우리 실생활에도 다양한 분야에 활용되고 있는데, 인터넷 업체가 보유하고 있는 지도 정보, 정부의 버스 위치 정보, 금융회사의 환율 정보 등이 이미 핀테크 기업에서 쉽게 활용할 수 있도록 API가 공개되어 핀테크 기업에서 다양한 방법으로 활용하고 있다. 다만, 외부 공개가 가능한 인터넷 서비스에 이용되는 오픈 API와 달리 민감한 정보와 금전을 다루는 금융회사에서는 오픈 API를 통해 금융과 신용정보에 접근하거나 고객 대신 핀테크 기업 등이 금융회사에 거래를 요청할 수 있으므로 API 접근 권한과 관련한 이용자 인증 등 기존 전자금융과는 다른 보안관리의 필요성이 대두되면서 안전한 오픈 API의 제공과 이용이 매우 중요한 과제로 떠오르고 있다. 보안위협이 발생 된다면 금융회사 자체의 신뢰성 하락과 고객 이탈은 물론 오픈 API 기술 활성화에도 크나큰 저해 요소가 될 것이다.

가트너 보고서는 오픈 API가 응용 프로그램을 서로 연계하여 많은 편의성을 제공하며 새로운 디지털 비즈니스 서비스를 제공하고 있지만, 데이터 유출 등의 API 보안사고가 발생하는 등 많은 취약점을 가지고 있다고 진단하였다. 또한, API 보안과 관련된 고객 문의가 전년 대비 30% 증가하였고 보안위협도 2019년 40%에서 2021년에는 90%까지 높아질 것으로 전망하였다. 'API 사용 및 디지털 플랫폼 성장에서의 역할'에 대한 설문조사(2018년 3월) 결과, 응답자의 50% 이상이 API 보안을 오픈 API 전략을 세우는데 매우 주요 과제 중 하나로 꼽았다[3].

이렇듯 오픈 API는 디지털 전환의 핵심 기술로써 국내 금융 활성화를 위해 적극적 도입이 추진되고 있지만 이와 함께 고객 정보의 관리, 새로운 보안위협, 컴플라이언스에 대한 리스크도 점점 대두되고 있다.

2.2 국내외 은행의 오픈뱅킹 동향

2.2.1 해외은행의 오픈뱅킹

해외 오픈뱅킹은 영국을 중심으로 시작되었으나 이미 전 세계적인 추세로 자리를 잡고 있다. 2017년 영국의 경쟁 및 시장 당국인 CMA(Competition and Markets Authority)가 실시한 소매금융시장에 대한 평가를 토대로 영국 금융행위감독청(FCA)이 2018년 1월부터 시행한 정책에서 그 뿌리를 찾을 수 있는데 같은 시기 유럽연합(EU)이 시행한 PSD2(Revised Payment Services Directive,

개정 지급 서비스지침)와도 유사점이 많다[4].

영국의 오픈뱅킹은 PSD2 시행에 맞추어 자국 실정에 맞게 설계한 정책이지만 적용 범위, API 표준화 여부 등에서는 다소 차이를 보인다. 이후 오픈뱅킹 정책은 호주, 싱가포르, 홍콩, 일본 등 많은 나라로 확산되었으며 국제적인 추세로 자리 잡아 가고 있다. 그러나 각국의 오픈뱅킹 정책들이 모두 같은 내용을 담고 있는 것은 아니다. 영국의 경우는 대형 은행들이 과점적 구조를 형성하고 있는 소매금융시장에서 경쟁을 촉진하려는 목적이 강했기 때문에 타 은행 및 제3자 서비스 제공자들에게 결제계좌 정보를 개방하는 데 초점이 맞추어 있다.

호주도 출발점은 비슷했다. 소매금융(주택구입 대출, 개인수신, 신용카드 발행) 각 분야에서 4대 은행들의 합산 시장점유율이 모두 75%를 초과하기 때문에 이들이 보유한 고객 정보를 공개하도록 하는 것으로 오픈뱅킹 정책이 설계되었다. 다만 호주의 경우 공개 대상 정보의 범위가 매우 넓어서 사실상 은행이 보유하고 있는 모든 계좌 정보라 해도 무방해 보인다. 한편 일본은 2017년 은행법 개정을 통해 은행에 오픈 API 구축에 노력할 의무('노력의무')를 부여하여 2020년까지 110개 이상의 은행이 완료할 것으로 예상하고 있다[5].

- 스페인은행 BBVA는 2017년 5월 API Market에 8종의 API(사용자 정보, 계좌, 카드, 지급, 대출 등)를 시장에 공개해 현재 스페인, 미국, 멕시코 3개국에 서비스 중이다.
- Fidor Bank는 2009년 독일에서 설립된 인터넷 전문은행으로 API 자체 플랫폼 fidorOS를 설계하고 전체 프로세스를 통합하였다.
- 씨티그룹은 2016년 11월 Citi Developer Portal을 개설하여 계좌관리, 지급, 송금, 인증 등의 기능을 제공하고 있다.
- 2004년에 설립된 인도의 Yes Bank는 온라인 여행사 Akbar의 ERP와 연계하여 거래내역 추적, 자동인증 등의 기능을 제공하고 있다.
- 일본의 대형 금융회사인 미즈호그룹의 Mizuho Bank는 2018년 5월 IBM API와 연계한 IoT 결제 서비스를 구현 테스트 중에 있다[5].

2.2.2 국내은행의 오픈뱅킹

최근 국내 금융회사도 오픈 API 구축 및 활용에 관한 관심이 증대되고 있다. 2016년 금융결제원에 구축한 '은행권 공동 API'가 오픈뱅킹의 틀을 갖추는 역할을 해왔다면 2019년 2월 금융위원회에서 발표한 '금융결제 인프라 혁신 방안'[6]은 국내 오픈뱅킹의 발전과 오픈뱅킹 도입의 본격적인 계기가 될 것으로 예상한다.

금융위원회는 오픈뱅킹을 개별은행과 제휴 없이도 표준화된 방식으로 은행의 자금 이체기능을 이용할 수 있게 해주는 시스템으로 정의한 바 있다. 지금까지 핀테크 기업들은 은행 간 자금 이체를 위해서는 은행과 개별적으로 펌뱅킹 계약을 맺어야 했으나 오픈뱅킹 시스템을 이용해 앞으로는 은행과 개별계약 없이 이체기능을 편리하게 수행할 수 있도록 유도하겠다는 것이 정부의 정책 방향이다.

또한, 금융위원회는 핀테크 기업들이 오픈뱅킹을 손쉽게 이용할 수 있는 법적 기반을 마련하기 위해 전자금융거래법과 신용정보법 개정을 추진하고 있으며 금융회사, 핀테크 기업 등 민간에서도 API 통한 정보공개의 범위와 기술 표준을 마련하고 있다[6].

- 2016년 6월 금융결제원과 16개 은행, 15개 증권사, 9개 핀테크 기업이 참여해 표준 API를 구축하여 잔액조회, 이체 등의 API를 제공하고 있다.
- NH농협은행은 2016년 4월 국내 최초 오픈 API를 출시하였으며 가상계좌 API, 신용카드 결제 API 등을 제공하고 있다.
- KEB하나은행은 2018년 2월 오픈 플랫폼을 구축해 60여 개 API를 공개하고 서비스 패키지를 제공하고 있다. 패키지는 특정 서비스 구현을 위하여 다양한 API를 패키지화한 API 그룹을 말한다.
- 신한금융그룹은 2018년 7월 신한금융그룹 Open API Market을 오픈해 그룹 내부 관계사 간 상호 API를 제공하고 있다[7].

이렇듯 국내 금융회사들은 오픈뱅킹 도입해 새로운 금융 생태계 조성과 금융혁신을 통해 새로운 먹거리 창출을 기대하고 있다. 또한, 다양한 외부 핀테크 기업과 유연한 관계를 유지함으로써 은행의 상품과 서비스에 대한 다양한 판매 채널로 활용할 수 있기를 기대하고 있다.

III. 국내은행의 오픈뱅킹 운영환경 분석

3.1 국내은행의 오픈뱅킹 운영환경

앞에서 살펴본 오픈뱅킹을 도입한 국내 주요 은행들은 금융그룹 내 관계사 간을 상호 연계하는 방식과 은행과 사전 계약을 체결한 핀테크 기업과 연계하는 방식, 또는 금융결제원에 구축된 은행권 공동 API를 통해 핀테크 기업이나 금융결제원 회원사가 API를 이용하는 방식을 주로 채택하고 있다. 기존에는 혁신적인 아이디어와 기술을 보유한 핀테크 기업도 금융비즈니스 모델을 구현하기 위해 금융회사와의 연계에 어려움이 있었으나, 향후 일정한 자격조건을 갖춘 핀테크 기업이 금융회사의 개별 API를 받거나 금융결제원 은행권 공동 API를 제공 받아 은행 등 금융회사의 금융결제망에 직접 연결해 핀테크 서비스와 연계한 이체 등 독자적인 금융서비스를 제공할 수 있게 된다.

또는 핀테크 기업이 제공하는 애플리케이션 이용자도 자신의 은행 계좌 정보를 핀테크 애플리케이션에 사전 등록하여 지급결제 등 금융거래가 가능해진다. 참고로, 금융결제원에서 핀테크 기업을 대상으로 상담한 결과 81.3%에 달하는 대부분의 핀테크 기업들이 금융서비스를 위해 은행의 계좌가 필요하다고 응답하였다.

다만, 은행의 계좌 정보를 등록해 이용할 때 해당 계좌거래가 정당한지 계좌 비밀번호의 검증은 필수 절차이다. 은행의 대부분 거래는 계좌번호와 계좌 비밀번호의 검증을 통해 이루어지는 만큼 계좌번호, 계좌 비밀번호 등 금융정보에 대한 보안관리가 무엇보다 중요해졌다.

3.2 OAuth 2.0 기술의 적용

오픈뱅킹은 기반 기술로 OAuth 2.0 기술을 채택하고 있다. OAuth 2.0은 기존 1.0의 기능을 보완해 다양한 애플리케이션 지원과 보안 개선으로 2012년 10월에 IETF 표준으로 등록되었다[8]. OAuth 2.0은 서비스를 제공하는 핀테크 기업의 애플리케이션(client)과 사용자의 정보를 포함하고 있는 리소스 서버(resource server) 간 사용자 자격증명의 직접적인 공유 없이 리소스 서버의 자원에 대한 접근 권한을 얻기 위해 고안되었다[9]. 접근 권한을 얻기 위해 다양한 위임방식을 제공하고도 있는데, 구체적인 사례로는 쇼핑몰 등과 같은 인터넷 사이트는 SNS 서비스와 위임방법에 따라 접근토큰 발급 절차를 미리 정의한 상태에서 사용자가 쇼핑몰을 접속하고자 할 때 Facebook, Google, Twitter 등 SNS 계정을 통해서도 인증하는 경우이다[10].

현재 대부분의 국내 금융회사의 개별 오픈뱅킹과 금융결제원 은행권 공동 오픈뱅킹의 인증방식은 OAuth 2.0의 Authorization Code Grant Type 방식을 주로 채택하고 있으며 은행 인터넷 뱅킹 고객은 인터넷뱅킹 아이디/비밀번호 등 인증정보를 입력하지 않고 접근토큰(access token) 기반으로 핀테크 애플리케이션 인증을 통해 은행 인터넷 뱅킹에 접속할 수 있다.

3.3 오픈뱅킹 구조 및 보안위협

3.3.1 B2B 연결모델

2019년 2월 정부는 금융결제망을 핀테크 기업과 은행 간에 전면적으로 개방하는 내용을 담은 '금융결제 인프라 혁신 방안'[6]을 발표하였다. 현재 국내 오픈뱅킹은 OAuth 2.0 기반의 오픈 API를 제공하는 운영기관(금융회사 등)과 오픈 API를 이용하여 금융서비스를 개발 및 제공하는 이용기관(핀테크 기업 등) 그리고 이용기관의 모바일 애플리케이션을 통해 오픈 API 이용 서비스를 이용하는 이용자(고객)로 구분될 수 있다[11]. 사실 국내 오픈 API는 2016년 8월 금융결제원 주관으로 이미 운영 중이었으나 이용기관 등이 매우 한정되고 높은 이용료 등으로 활성화에는 한계가 있었다. 정부는 이용기관을 모든 핀테크 기업 등으로 확대하고 합리적 비용으로 편리하게 금융결제망을 이용할 수 있도록 공동 결제시스템(오픈뱅킹)을 재구축해 2019년 12월 중 전면 시행을 목표로 추진하고 있다. 현재 A은행 계좌조회 등 금융거래는 A은행의 애플리케이션만을 이용해야 했지만, 오픈뱅킹이 도입되면 B은행이나 핀테크 기업의 모바일 애플리케이션에서도 다른 은행의 계좌조회가 쉽게 가능해지는 등 은행이나 핀테크 기업들의 애플리케이션을 통해 본인이 소유한 모든 은행의 계좌조회가 가능하고 자금의 출금이체도 가능해진다. 그간 개별은행 위주의 폐쇄적으로 운용되었던 금융결제망이 전면 개방되는 금융산업에서의 큰 전환점이다.

현재의 국내 오픈뱅킹은 이용자와 이용기관(핀테크 기업 등)은 핀테크 기업의 애플리케이션을 통해

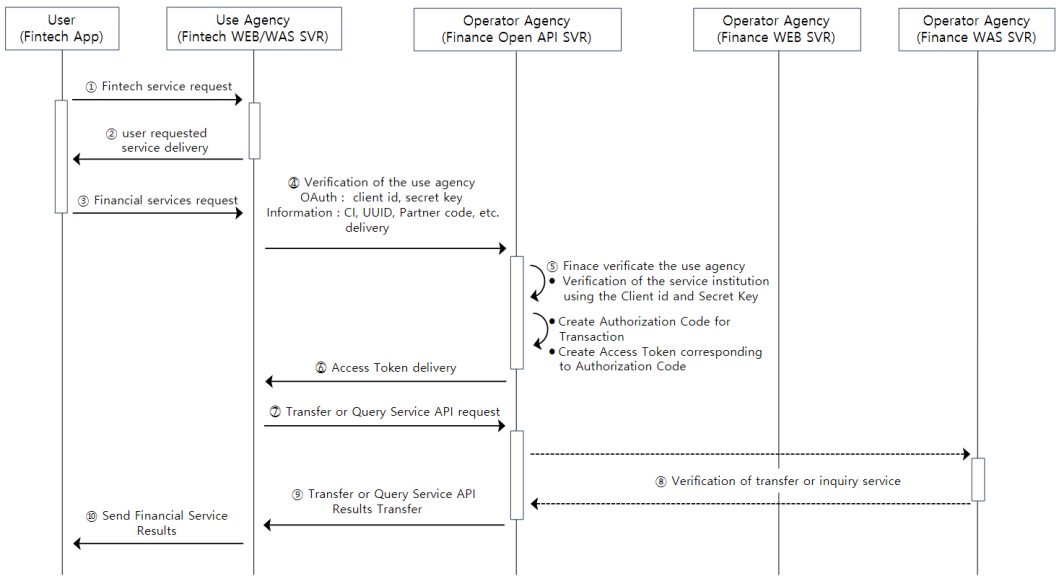

Fig. 1. Open Banking B2B Model Authentication Flow

기존 제공되는 방식인 일반전문 통신으로 연결되고, 이용기관과 운영기관은 새로운 방식인 오픈 API를 통해 연결된다. 즉 오픈 API 연결구간은 API를 제공하는 운영기관과 그 API를 제공 받은 이용기관 간 연결구간뿐이다. 이러한 연결방식은 금융결제원의 은행권 공동 오픈뱅킹을 비롯해 국내 금융회사가 오픈뱅킹을 연결하는데 널리 이용되는 방식으로 본 논문에서는 이를 B2B 연결모델이라 하겠다.

B2B(Business to Business)는 기업 대 기업 사이의 거래를 의미하는 경제용어로 오픈뱅킹에서는 이용자가 배제된 운영기관과 이용기관 간의 오픈 API 연결을 의미한다. B2B 연결모델의 장점은 우선 이용기관의 개발과 적용이 간편하다는 것이다. 운영기관으로부터 제공 받은 표준 API를 이용기관의 시스템에만 적용하고 이용자의 애플리케이션은 기존과 변경이 없으므로 개발비용이 적고, 적용이 간단해 오픈뱅킹 활성화에 적합한 모델로 인식되어왔다. 다만 이용자의 인증을 이용기관에 위임한 구조인 관계로 이용기관의 인증 등 보안관리, 이용기관 내 서버 자체의 보안관리 문제 등의 보안위협을 그대로 가지고 운영될 수밖에 없어 운영기관인 금융회사 입장에서는 이용기관의 의존성이 과도하다는 단점 있다.

Fig.1.에서 보이는 B2B 연결모델의 구체적인 금융거래 인증절차는 다음과 같다.

- (①/②/③,이용자↔이용기관)핀테크 앱에서 운영기관(은행 등)의 이체 거래 등 금융서비스를 선택한다.(Confidential Client 방식으로 이용기관의 Web/WAS 서버로 요청)
- (④,이용기관→운영기관)이용기관의 Web/WAS 서버에서 운영기관의 API 이용을 위한 이용기관 인증 및 Access Token 발급을 요청한다.(전송해야 할 필수 정보는 Client ID, Secret Key, API Type(Client Grant Type), 선택 정보는 CI, UUID, 이용기관 코드 등)
- (⑤,운영기관)이용기관으로부터 전달받은 API 접근키 등의 유효성 검증한다.(이용기관은 API 접근키를 통해 검증, 이용자 인증은 핀테크 기업의 앱 가입 시 등록된 CI, UUID, 이용기관 코드 등을 비교 검증
- (⑥,운영기관→이용기관)유효성 검증 완료 후 Access Token을 발급하고 이용기관에 Access Token을 전달한다.(Access Token은 Client ID, TimeStamp, Hash값, Secrete Key와 기타 정보로 구성)
- (⑦,이용기관→운영기관)이체 또는 조회 등 실제 금융서비스 요청을 위한 API 수행을 요청한다.(이용기관은 Access Token을 통해 API를 호출하며, 운영기관은 Access Token으로 API 권한 제어를 수행, 실시간 검증을 위해

RESTful Body 전체를 일방향 암호화 (SHA-512) Hash 생성 후 인코딩)

- (⑧,운영기관)요청받은 금융서비스를 처리한다.
- (⑨/⑩,운영기관→이용기관→이용자)API 수행결과를 전송한다.

B2B 연결모델은 이용기관과 운영기관에만 적용되는 인증 연결모델인 관계로 금융서비스 이용에 대한 이용자 인증을 운영기관인 금융회사가 직접 하지 않고 이용기관인 핀테크 기업 등에 위임하는 구조로 이용자와 이용기관(B2C) 구간에서의 보안위협이 발생될 가능성이 있다.

3.3.2 B2B 연결모델의 보안위협

금융회사인 운영기관 입장에서 오픈뱅킹의 보안위협은 B2C 구간인 (i) 이용기관(핀테크 기업) 영역, (ii) 통신구간, 그리고 (iii) 이용자(핀테크 기업의 애플리케이션) 영역으로 구분[11]될 수 있으며 분석결과는 다음과 같다.

첫째, 이용기관은 금융결제원 은행권 공동 오픈뱅킹의 이용기관 승인 기준에 따라 사업자 중 금융위원회 분류기준의 핀테크 기업과 전자금융거래법상 전자금융업자 또는 전자금융보조업자 그리고 오픈뱅킹 운영기관인 금융결제원에서 인정한 기업이다. 이용기관은 운영기관의 적합성 심사 및 승인 절차를 통해 지정된다. 운영기관의 심사단계에서는 이용기관에 대한 보안수준을 점검하게 되어 이용기관의 보안상태를 확인하게 되지만 이용기관은 오픈 API 인증키와 접근키를 보관하고 있어 이용기관의 서버와 애플리케이션에 접근 가능한 최고권한의 시스템 관리자가 악의적 행위를 했을 때 이를 알기란 쉽지 않고 금융회사인 운영기관에서도 사전에 통제할 수 없다. 핀테크 기업의 시스템 관리자가 오픈 API 접근키와 인증키를 악의적으로 재사용하거나 핀테크 애플리케이션 이용자가 사전 등록한 은행의 계좌 정보 등을 무단으로 이용하는 경우 금융거래의 변조와 정보유출 가능성을 배제할 수 없다.

둘째, 통신 구간은 이용자와 이용기관, 이용기관과 운영기관 간 데이터를 전송하는 구간으로 이미 검증된 방식인 TLS 등의 암호화 통신과 데이터 암호화를 통해 충분한 보안체계가 유지된다고 볼 수 있다.

마지막으로 이용자 영역은 로그인 화면, 인증, 보안 등 핀테크 애플리케이션에서 제공하는 기능을 통해 핀테크 서비스를 이용한다. 핀테크 애플리케이션 보안이 잘 적용되어 있고 주기적으로 보안 점검을 시행한다 하더라도 웹 또는 모바일 등 디바이스에 대한 지속된 공격 시도로 안전을 보장할 수는 없는 상태이다.

앞서 분석한 보안위협 중 모든 금융거래가 중계되어 금융거래를 변조할 수 있고 정보를 중간에 가로챌 수 있는 오픈뱅킹 구조에서 가장 취약한 부분인 이용기관 영역에서 예상 가능한 해킹 시나리오를 상세 분석함으로써 오픈뱅킹의 개선점 도출에 참고자료로 이용하고자 한다. 첫 번째, 오픈뱅킹 불법 금융거래 시나리오다.

이용기관 서버 및 애플리케이션 관리자 또는 이용기관의 서버를 장악한 해커가 오픈뱅킹 금융거래를 실시간 모니터링 후 이용자의 정상 금융거래를 일시 중지시키고 수취인 입금 계좌번호를 외부의 악의적 계좌(일명 대포통장)로 임의 변조해 거래 전문을 운영기관에 요청한다면 B2B 연결모델에서의 운영기관은 이용기관만을 검증하므로 해당 변조된 거래가 실행된다. 기존 인터넷 뱅킹 또는 모바일 뱅킹 등 전자금융 거래의 메모리 해킹과 유사한 수법이다. 또 다른 방법은 악의적 관리자/해커가 출금 계좌번호와 계좌 비밀번호 그리고 수취인 입금 계좌번호를 사전에 수집한 후 일정 시간이 지나 입금 계좌번호만 악의적

Table 1. Open Banking security threat

Item	Retention information	Security threat
(i) Fintech	Authorization Code, Access Token, Financial information	Information leakage, Server vulnerabilities, Administrative vulnerabilities, Financial forgery
(ii) Connection section	N/A	Authentication detour, Financial forgery, Information leakage
(iii) User (Application)	Access Token (temporary)	Authentication detour, Financial forgery, Information leakage, Device vulnerabilities

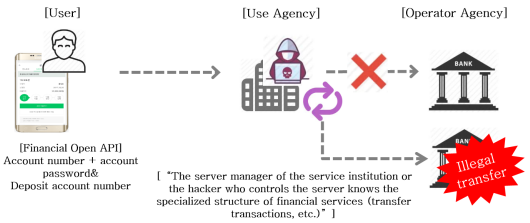

Fig. 2. Scenario of Open Banking Illegal Financial Transactions(expected)

계좌로 변조한 거래 전문을 생성해 운영기관에 새로운 거래로 요청하는 릴레이공격(relay attack)과 유사한 수법이 가능하다.

두 번째, 시나리오는 정보유출 사고 시나리오로 Fig. 3.와 같이 이용기관 서버 및 애플리케이션 관리자/해커가 금융거래를 위해 이용자가 입력한 은행의 아이디/비밀번호 등의 인증정보, 출금 계좌번호, 계좌 비밀번호, 수취인 입금 계좌번호 등 모든 금융정보와 기타 이용자의 개인정보를 수집할 수 있다. 수집한 다수 이용자의 모든 정보를 금융정보 불법 유통 브로커에게 직접 판매하거나 그 브로커가 중국 보이스 피싱 조직이나 불법 사금융 조직, 해커 등에 재판매하게 되다면 정보 유출로 인한 이용자의 피해뿐만 아니라 이용자 본인이 인지하지 못한 불법 대출, 차명 휴대전화 개통 등의 2차 피해도 우려되는 상황이 발생할 것이다.

따라서 B2B 연결모델에서 이용기관과 이용자 영역의 취약점을 통해 금융거래가 변조되거나 정보가 유출된다면 바로 금융사고로 이어지게 된다. 이러한 두 개의 시나리오를 통해 설명한 바와 같이 오픈뱅킹의 보안위협은 금융회사와 핀테크 기업의 신뢰도 저하뿐만 아니라 오픈뱅킹 생태계 자체에도 그 파장과 영향이 클 것으로 예상된다. 또한, 오픈뱅킹 보안위

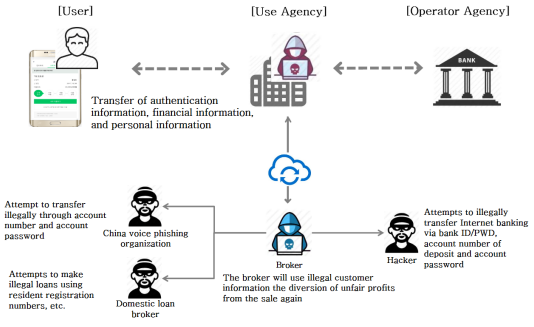

Fig. 3. Open Banking Financial Information Leak Scenario(expected)

협이 미치는 영향 등을 고려할 때 금융회사의 금전이 수반되는 금융거래에서는 보안위협에 대응하기 위해 더 강한 보안체계와 각별한 주의가 필요하다.

IV. B2B2C 오픈뱅킹 제안

4.1 오픈뱅킹의 개선 필요성

국내 오픈뱅킹은 금융결제원이 운영기관으로써 오픈 API를 제공하고 은행들이 이용기관으로 참여한 지급결제 위주의 금융서비스로 2019년 10월 시범 시행되고 핀테크 기업이 이용기관으로 확대 참여한 전면 시행은 2019년 12월로 예정되어 있다. 현재 오픈뱅킹의 유형은 2가지로 분류될 수 있다. 첫째, 금융결제원이 운영기관, 금융회사(은행)는 금융서비스를 제공하는 제공기관으로 구성되는 공동 API 방식과 둘째, 핀테크 기업이 이용기관, 금융회사는 오픈 API를 제공하는 운영기관이면서 동시에 금융서비스를 제공하는 제공기관으로 구성되는 개별 API 방식이다. 참고로, 개별 API는 외환, 여신, 방카 등 금융회사의 특화된 서비스를 제공하기 위해 금융회사가 자체 오픈 API를 제공하는 것으로 오픈 API의 인증 등 운영 전반을 관리하고 통제하는 주체가 금융회사이다.

공동 API와 개별 API는 금융거래에 대한 인증을 이용기관에 의존한다는 공통점이 있어 전형인 B2B 연결모델을 기반으로 운영되고 있다. A은행의 고객인 이용자가 A은행 애플리케이션 또는 핀테크 애플리케이션을 통해 B은행의 계좌조회나 입금, 출금이체 거래가 가능하다. 다만 B은행의 금융거래를 위한 인증이 이용기관인 A은행 또는 핀테크 기업에 이용자가

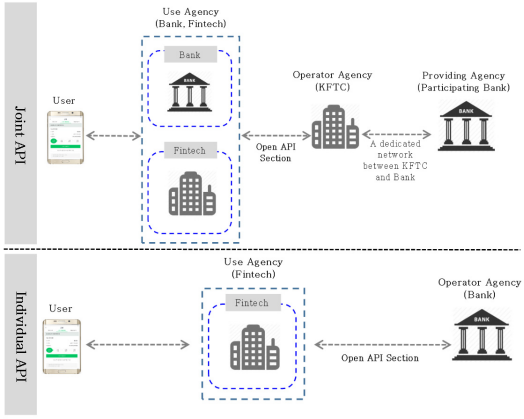

Fig. 4. Open Banking Type

사전 등록한 간편번호나 A은행의 기존 인증방식인 계좌 비밀번호 입력, OTP, 공인인증서 인증 등을 통해 처리된다. 이처럼 인증처리가 이용기관 방식을 따르게 되면 앞서 살펴본 바와 같이 B2B 모델상 이용기관의 관리 소홀이나 취약점을 통해 오픈뱅킹의 금융사고가 발생되었을 때 이용기관이 사고의 과실을 부인하는 경우 운영기관이 이를 입증하기가 어렵다. 현재 법적 근거와 법률적 정비가 부족한 상태에서의 오픈뱅킹 금융사고는 이용기관(핀테크 기업)과 운영기관(금융회사) 간 책임소재가 불명확해 분쟁이 예상되는 상황으로 금융소비자의 피해가 예상되는 등 예기치 못한 혼란이 야기될 수 있다. 따라서 오픈뱅킹에 대한 법률적 정비가 필요한 상황이다.

이러한 국내의 오픈뱅킹 상황과 달리 유럽을 중심으로 해외의 오픈뱅킹은 이미 정착기에 이르렀는데 이러한 정착기에 이르기까지 오픈뱅킹 도입을 위해 법규를 개정하고 새로운 기술규격을 제정하는 등 오픈뱅킹에 맞는 규정과 기술규격을 마련해 왔다. 예를 들어 2007년 제정된 유럽연합(EU) 내 지급결제서비스에 관한 지침인 PSD1(Payment Service Directive Ⅰ)을 디지털 금융환경에 맞게 개정한 PSD2를 2018년 1월부터 시행하고 있다. PSD2로의 개정의 주된 요인으로는 법적 불확실성으로부터 금융소비자를 보호하는 것과 디지털 금융환경에서의 안전성을 확보하는 것이다. PSD2 시행에 따라 새로운 유형의 지급결제서비스 제공업자(Payment Service Provider), 계좌정보서비스(Account Information Service), 지급개시서비스(Payment Initiation Service) 그리고 계좌접근권(Right of Access to Account) 등의 새로운 개념들이 정립되어 현재의 오픈뱅킹 기반이 마련되었다. 추가적으로 PSD2의 후속 조치로서 고객인증, 데이터 전송방식 등 지급결제서비스에 대한 보안 요구사항을 새로 규정한 규제기술표준(RTS, Regulatory Technical Standards)을 2019년 9월 발효해 시행하였다. 이 규제기술표준은 금융거래를 위해 계좌에 접근할 경우 강화된 고객인증 요건에 따라 추가적인 고객확인절차를 진행토록 규정하고 있다[12]. 이처럼 해외에서는 오픈뱅킹의 법률 정비뿐만 아니라 안전성을 위해 새로운 보안규제까지 마련하여 편리성과 보안성의 균형을 맞추었다는 점에서 시행 초기인 국내 오픈뱅킹에 시사하는 바가 크다 할 것이다.

따라서 국내 오픈뱅킹도 B2B 연결모델의 불명확한 책임소재를 보완해 책임소재가 명확할 수 있게 국내 관련 법률의 개정 정비와 B2B 모델의 보안위협 해소 및 해외 보안권고 사항인 PSD2-RTS의 보안규제 등을 만족할 수 있는 안전한 연결모델의 발굴이 필요하다.

4.2 안전한 오픈뱅킹 구축을 위한 정책 제안

정부는 오픈뱅킹의 법적 안정성 마련을 위해 2020년 내 전자금융거래법과 신용정보법의 이용 및 보호에 관한 법률(이하 '신용정보법')의 개정을 계획하고 있다. 그러나 개정 방향이 오픈뱅킹의 활성화에 주안점을 두고 있어 오픈뱅킹 B2B 연결모델에서의 금융사고 발생 시 책임소재 명확화와 금융소비자 피해 구제방안에 관한 내용은 담고 있지 않다. 이에 본장의 정책 제안을 통해 오픈뱅킹 금융사고 발생 시 당사자 간의 책임소재 명확화 방안과 소비자 보호를 위해 필요한 사항을 제시하고자 한다.

4.2.1 오픈뱅킹 금융사고 공동책임

전자금융거래법에서는 전자금융거래에서 발생한 사고로 인해 고객에게 손해가 발생한 경우에는 그 손해의 배상 책임이 금융회사에 있다고 규정하고 있다. 2007년 법 시행 이후 금융회사는 전자금융거래 사고에 대한 입증책임과 평소 금융사고 방지를 위해 충분한 주의의무를 다 했는지를 소명할 의무를 진다. 또한, 고객의 피해 구제를 위해 금융회사는 손해배상 보험 가입 또는 준비금 적립 등의 피해 고객의 금전적 보상에 필요한 조치가 의무화되었다[13]. 즉 금융소비자 보호를 위한 법의 취지로 고객과 금융회사 간 직접적인 관계인 기존 전자금융거래에서는 거래의 연계구조가 단순해 사고 발생 시 금융회사가 사고를 입증할 수 있는지 없는지에 따라 금융회사의 책임 여부가 명확히 구별되었다.

이러한 환경에서는 책임소재에 대한 분쟁의 소지가 적어 이용자에게 금전적 피해를 신속히 보상될 수 있지만, 오픈뱅킹은 금융회사, 핀테크 기업, 고객 등 거래의 관계자가 다수이고, 연계 구조가 복잡하여 금융사고 발생 시 금융회사의 입증 범위와 책임이 불명확하다. 다른 측면에서는 금융회사와 핀테크 기업 간 과실 책임이 명확하지 않을 경우 책임소재에 대한 분쟁이 장시간 소요됨으로 인해 고객에 대한 배상이 지연될 수 있다.

따라서 사고에 대한 책임 소재가 구조적으로 불명확한 B2B 모델에서는 금융소비자 보호를 위한 법률적 개선이 우선적으로 필요하다. 즉 오픈뱅킹 금융사

고에 대한 입증책임과 손해배상 책임을 금융회사와 핀테크 기업이 공동으로 책임지게 하고 현재 금융회사에만 주어진 손해배상 보험 가입 의무를 핀테크 기업까지 확대해 사고가 신속히 처리될 수 있도록 전자금융거래법의 개정이 필요할 것이다.

4.2.2 동의 받는 주체에 대한 금융사고 책임 명확화

오픈뱅킹은 이용기관인 핀테크 기업이 금융거래를 제공하기 위해서는 운영기관인 금융회사로부터 계좌번호, 잔액, 거래내역 등의 금융정보를 제공 받아야 한다. 구체적으로 핀테크 기업은 고객의 동의하에 금융회사의 개인신용정보를 받고, 제공 받은 정보는 제공목적 범위 내에서만 이용할 수 있다. 그런데 현행 개인정보보호법과 신용정보법에서는 금융회사가 고객으로부터 동의를 받아 해당 고객의 개인신용정보를 핀테크 기업에 제공하여야 한다[14][15].

금융결제원이 운영기관인 공동 API는 금융실명제법[16]에 따라 금융결제원과 금융회사 간에 별도의 동의 없이 금융정보를 주고받을 수 있지만, 개별 API는 공동 API와 달리 이용기관인 핀테크 기업이 운영기관인 금융회사로부터 금융정보를 제공 받기 전 반드시 고객의 금융정보 제공에 관한 동의를 받아야 한다. 이 경우 원칙적으로는 정보를 제공하는 금융회사가 고객의 동의를 받아야 하나, 오픈뱅킹 B2B 연결모델의 구조적 특성상 고객의 동의를 금융회사가 받지 않고 핀테크 기업이 받게 된다. 합법적인 관계하에서는 핀테크 기업이 금융회사를 대신하여 일명 대리 동의방식으로 고객의 금융정보 제공 동의를 받게 되는 것이다. 대리 동의는 두 주체가 상호합의한 경우에만 가능하므로 고객의 동의를 받을 수 없는 경우나 공공의 이익 등 매우 제한적으로 허용되고 있는 것이 현실이다.

향후 많은 핀테크 기업들이 대리 동의방식을 통해 금융정보를 제공 받고자 할 경우 대리 동의를 허용해 준 법의 취지와 다르게 대리 동의가 과도하게 허용되는 측면이 생긴다. 또한, 이용기관인 핀테크 기업이 악의적으로 고객의 동의를 받지 않은 상태에서 동의를 받은 것처럼 금융회사에 정보제공을 요청하더라도 금융회사는 동의 여부를 알 수 없어 고객의 금융정보를 그대로 제공할 수밖에 없다. 이때 정보제공에 동의하지 않은 고객이 금융회사에 정보제공에 대해 민원 등 문제를 제기하거나 핀테크 기업이 제공 받은 고객의 금융정보를 이용해 금융거래를 변조하거나 정보가 유출되는 금융사고가 발생한다면 금융회사와 핀테크 기업 간 책임소재가 불명확해진다. 즉 제3자 정보제공에서는 금융정보의 관리·감독책임과 손해배상 책임이 정보를 제공 받은 이용기관인 핀테크 기업에 있다는 것이 법률적 해석이지만 핀테크 기업이 의도적으로 과실책임을 부인한다면 정보주체인 고객으로부터 명시적으로 동의를 받지 않은 상태에서 제3자에게 정보를 제공한 금융회사도 책임에서 벗어나지 못할 것이다.

따라서 고객의 금융정보 제공에 대한 책임을 명확히 하기 위하여 금융회사는 대리 동의를 통해 핀테크 기업에 금융정보를 제공할 때 핀테크 기업이 고객으로부터 금융정보 제공에 관한 명시적인 동의가 있었는지를 명확히 확인한 후 금융정보를 제공해야 한다. 확인하는 방법으로는 첫째, 핀테크 기업이 금융회사에 정보제공을 요청하는 API 전문에 고객의 동의 여부를 알 수 있게 API 전문항목을 추가하여 확인하거나 둘째, 핀테크 기업과 사전에 계약 또는 약정체결을 통해 핀테크 기업에서 정보제공 요청 시 고객 동의를 받은 것으로 간주하고 그에 따른 모든 책임을 핀테크 기업에 있다는 조건을 명문화하는 방법을 생각해 볼 수 있을 것이다. 마지막으로는 금융회사가 핀테크 기업에 고객의 금융정보를 제공할 때 금융회사가 고객으로부터 직접 제공에 관한 동의를 받을 수 있는 연결모델을 채택하는 것도 고려해 볼 수 있을 것이다. 참고로, 정부는 신용정보법 개정을 통해 이러한 문제를 해결하고자 하고 있다.

4.2.3 보안심사 및 서비스 차등

전자금융 서비스를 운영하는 금융회사의 전자금융거래에 대한 기술적 보호조치 기준은 전자금융감독규정과 감독당국의 권고 사항에 따른다. 규정에는 금융회사의 정보처리시스템과 정보보호시스템에 대한 보호 대책, 외부 해킹 방지, 전자금융거래 시 준수사항, 취약점 분석·평가 등 금융회사의 안전성 확보를 위한 전반적인 사항이 규정되어 있다[17]. 대부분 금융회사는 감독규정을 이행하고 있으며 감독당국의 주기적 검사를 통해 지속해서 평가를 받고 있어 높은 보안수준을 유지하고 있다.

오픈뱅킹 이용기관인 핀테크 기업은 전자금융감독규정 준수의무를 가지는 전자금융업자도 일부 있으나 대부분 전자금융보조업자로서 전자금융감독규정의 직접 준수의무가 없다. 즉 금융회사와 같이 지속해서 보안상태를 평가받거나 규제받지 않아 핀테크 기업의 보안수준은 금융회사나 전자금융업자와 비교해 상대적

으로 낮을 수밖에 없다. 이에 공동 API를 주관하는 금융위원회는 오픈뱅킹 참여를 신청한 핀테크 기업을 대상으로 금융보안 전담기관을 통한 보안 점검을 실시할 계획이며 그 보안 점검에 통과한 기업만이 오픈뱅킹에 참여할 수 있다고 밝혔다.

따라서 개별 API 운영하는 금융회사도 핀테크 기업의 API 신청단계에서 핀테크 기업의 재무적, 기술적 측면 등을 고려해 자격 적격성을 판단할 수 있는 심사기준을 마련하고 그 기준에 따라 API 이용 심사와 핀테크 기업의 보안수준을 판단할 수 있는 보안심사를 반드시 실시해야 한다. 보안심사절차에는 핀테크 기업 내 시스템 관리, 모바일 보호 대책 등의 기술적 점검과 개발자, 시스템 관리자 등 잠재적으로 보안위협이 될 수 있는 모든 분야에 대해 점검해야 한다.

또한, 금융회사는 보안심사 결과에 따른 핀테크 기업의 보안수준을 등급화하고 보안등급별 API 제공 서비스를 차등화하여야 한다. 보안등급이 낮은 핀테크 기업은 환율 정보, 영업점 위치 정보 등 공개가 가능한 API만 제공하고, 일정 보안수준을 갖춘 핀테크 기업에만 금융거래용 API가 제공되어야 한다.

4.3 안전한 B2B2C 연결모델 제안

오픈뱅킹은 편리한 금융서비스 제공과 금융소비자의 선택권 강화를 위한 새로운 금융혁신 모델로 기존 금융거래에서 발생할 수 있는 일반적인 보안위협뿐만 아니라 오픈뱅킹 고유의 보안위협이 발생될 수 있다. 따라서 정책 제안과 더불어 현재 금융권에서 채택하고 있는 B2B 연결모델이 갖는 구조적 약점을 보완하고 오픈뱅킹 고유의 위협에 대응할 수 있는 기술적, 정책적 새로운 보안 프로세스 마련이 필요하다. 특히 금융회사가 자체적으로 오픈 API를 운영하는 개별 API 방식에서는 API 운영 전반에 걸쳐 모든 책임이 금융회사에 있는 만큼 더욱 세분화된 안전한 장치가 필요로 하게 되었다. 해외 오픈뱅킹 우수 사례 등을 분석해 볼 때 금융 조회성 업무는 B2B 모델, 금융거래에 대한 인증처리는 금융회사가 직접 처리할 수 있는 B2B 모델의 확장 개념인 B2B2C 연결모델을 검토할 필요가 있다.

구체적인 절차는 Fig.5.에서 보인다.

- (①/②/③,이용자↔이용기관)핀테크 App에서 운영기관(은행 등)의 이체 거래 등 금융서비스를 선택한다. (Confidential Client 방식으로 이용기관의 Web/WAS 서버로 요청)
- (④,이용기관→운영기관)이용기관 Web/WAS서버에서 운영기관의 API 이용을 위한 이용기관 인증 및 Access Token 발급을 요청한다.(전송해야 할 필수 정보는 Client ID, Secret Key, API Type(Client Grant Type), 선택 정보

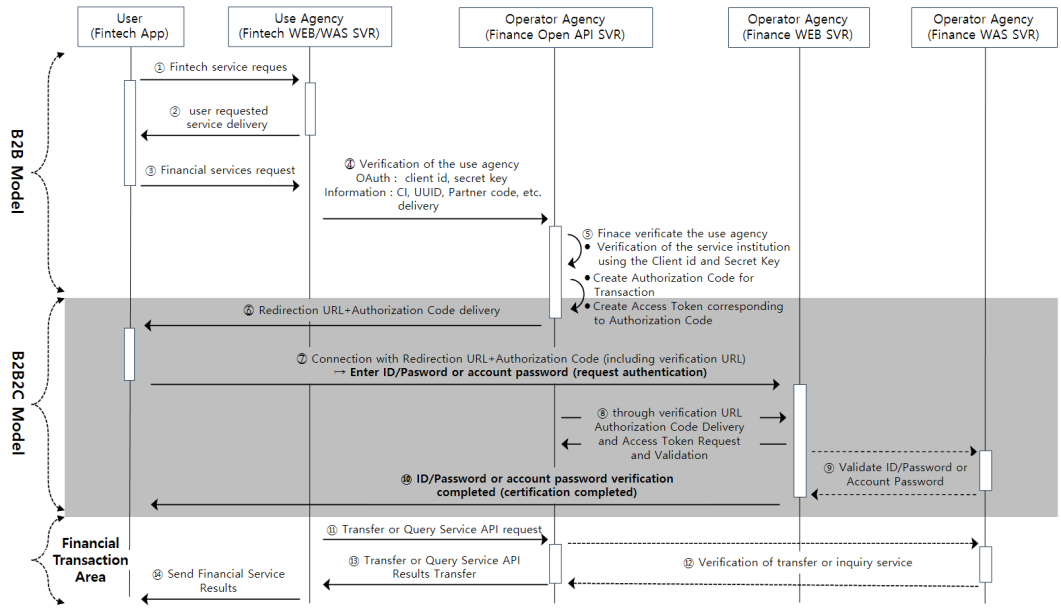

Fig. 5. Open Banking B2B2C Model Authentication Flow

는 CI, UUID, 이용기관 코드 등)

- (⑤,운영기관)이용기관으로부터 전달받은 API 접근키 등의 유효성 검증 및 이용자 인증을 위한 전처리를 수행한다.(이용기관은 API 접근키를 통해 검증, 1차 이용자 인증은 핀테크 App 가입 시 등록된 CI, UUID, 이용기관 코드 등을 비교 검증, 2차 이용자 인증을 위한 전처리는 Authorization code(일회성 인증코드) 생성 및 대응되는 Access Token 생성)
- (⑥,운영기관→이용기관→이용자)유효성 검증 완료 후 이용자 인증을 위해 이용기관과 사전에 약속된 운영기관의 인증 페이지를 전달한다.(Redirection URL, Authorization code, Access Token 요청 URI)
- (⑦/⑧,이용기관↔운영기관)Redirection URL을 통해 이용자는 운영기관의 인증 페이지를 호출하여 이용자 인증을 위한 ID/Password 또는 계좌 비밀번호를 입력한다.(정상적으로 호출되면 운영기관 서버는 Access Token 요청 URL을 통해 Auth- orization code 제출 및 Access Token을 수신)
- (⑨,운영기관)이용자가 입력한 인증정보를 운영기관의 인증원장과 비교하여 인증을 처리한다.
- (⑩,운영기관→이용기관→이용자)이용자 인증 결과 및 Access Token을 전달한다.
- (⑪,이용기관→운영기관)자금 이체 또는 조회 등 실제 금융거래 요청을 위한 API 수행을 요청한다.(이용기관은 Access Token을 통해 API를 호출하며 운영기관은 Access Token으로 API 권한 제어를 수행, 실시간 검증을 위해 RESTful Body 전체를 일방향 암호화(SHA-512) 해싱 후 인코딩)
- (⑫,운영기관)요청받은 금융서비스를 처리한다.
- (⑬/⑭,운영기관→이용기관→이용자)API 수행 결과를 전송한다.

따라서 국내 오픈뱅킹에 B2B2C 모델을 추가 적용함으로써 B2B 연결모델의 약점을 보완하고 금융사고에 대한 책임소재를 명확하여 금융사고 발생 시 고객정보 보호 및 금융소비자의 피해보상 등을 즉각적으로 조치해 오픈뱅킹의 편리성과 금융사고 예방 등 안전성 확보를 위한 유연한 절차가 가능하다. 금융회사는 필요할 경우 금융거래의 성격과 중요도에 기존 B2B 연결모델 또는 본 논문에서 제시된 B2B2C 연결모델을 선택적으로 적용할 수 있을 것이다.

V. 결 론

최근 금융산업은 전 세계적으로도 핀테크 중심의 혁신이 가장 활발히 이루어지고 또한 경쟁이 가장 치열하게 전개되고 있는 분야이다. 특히 글로벌 금융시장에서는 이미 핀테크 기업을 비롯해 여러 간편결제 사업자가 금융결제 시장에 진출해 시장을 빠른 속도로 선점하고 있다. 국내 핀테크 기업들도 간편결제, 금융플랫폼 구축 등 새로운 금융서비스를 속속 등장시키고 있으며 정부와 금융회사도 폐쇄적인 금융결제 시스템과 경직된 규제 체계에 대한 문제의식을 공감해 금융결제 시스템의 접근성, 개방성을 확대해 나가기 위해 노력하고 있다. 이에 2019년 12월 오픈뱅킹이 전면 시행될 예정으로 국내 모든 은행인 18곳과 100여 개가 넘는 핀테크 기업들의 참여가 예상된다. 오픈뱅킹이 도입되면 금융소비자는 앱 하나만 있으면 자신의 모든 은행 계좌를 편리하게 이용할 수 있고 은행 등 금융회사는 다양한 채널을 통해 고객 유치와 새로운 서비스 및 금융상품 개발, 유통 등 전반적인 경쟁력 강화가 예상된다. 이러한 금융규제 완화와 금융시장의 개방 분위기, 무엇보다 간편성을 지향하는 금융소비자 요구에 힘입어 오픈뱅킹은 향후 비약적으로 성장해 나갈 것으로 예상한다.

정부는 오픈뱅킹 전면 시행 이후 은행에서 상호금융, 저축은행, 우체국 등 제2금융권으로 참여를 확대하고 해외 간편 송금 등 외국환거래, 신용카드 거래 그리고 은행의 영업점 대면 거래까지 서비스 범위를 확대할 계획에 있다[18]. 앞으로 오픈뱅킹은 더 많은 핀테크 기업들에 금융결제 시스템이 개방될 것이다. 또한, 국내 오픈뱅킹 활성화는 글로벌 금융회사와 해외 핀테크 기업들과의 경쟁에서도 중요한 시장 변수가 될 것이다. 이러한 오픈뱅킹의 비약적인 성장이 예상됨에 따라 법률적 기반 마련과 함께 금융소비자 보호 및 금융사고 예방을 위해 금융거래에 대해서는 안전성과 유연성을 갖는 B2B2C 연결모델로 구현함으로써 공개 가능한 일반 정보와 구별 처리하는 방식이 구현된다면 오픈뱅킹의 유연성과 보안성을 동시에 만족시킬 수 있을 것으로 기대한다.

또한, 현재 국회 계류 중인 신용정보법이 개정되면 개인정보의 자기결정권과 개인신용정보 이동권이 도입되면서 국내 마이데이터산업이 본격적으로 시작될

것이다. 마이데이터는 고객의 동의하에 고객의 모든 정보가 핀테크 기업으로 이동되기 때문에 금융결제망 개방보다 파급력이 훨씬 클 것으로 예상된다. 즉 핀테크 기업은 금융회사와 동일한 또는 그 이상의 정보를 보유하게 되어 금융회사의 모든 거래가 가능해진다. 이에 따라 많은 양의 금융정보를 보유하게 되는 핀테크 기업의 보안관리 또한 그 중요성이 더욱 높아질 것이다. 하지만 핀테크 기업의 보안관리 소홀과 핀테크 기업 내 서버 관리자의 악의적 행위로 고객의 동의가 위조 또는 오용된다면 고객 정보 사고로 이어질 것이다. 핀테크 기업을 통한 고객 정보유출 사고는 유출의 주체와 경로가 핀테크 기업인지 금융회사인지 파악하기 어렵고 그 유출 책임에서도 소재가 불명확해 유출 사고로 인한 소비자의 금전적 피해배상의 지연과 기업 간의 장기간 분쟁 등 금융산업에 끼치는 유무형의 손실과 피해가 클 것으로 예상된다.

따라서 오픈뱅킹 환경에서의 마이데이터산업도 정보의 제공에 대한 결정책임을 명확히 하기 위해 고객 정보제공에 관한 동의절차, 분쟁처리 방법 등 법률적 이슈에 대해 충분한 재점검가 필요하다. 특히 정보제공 동의 등 중요한 거래는 금융회사에서 직접 처리하는 방안 등을 검토해 만일의 정보 유출 시 책임소재를 명확히 해야 한다.

References

[1] Da-Eun Lee, Seung Il Moon, and Choong Seon Hong, "Development of Single Sign-On Platform Based OAuth Mechanism for Mashup Services," Jonornal of The Korean Institute of information Scientists and Engineers, 854-856(3), pp. 854-855, Dec 2015.

[2] ty.kim, dwkwon, hwkim84 and juht, "State of Art Open API Development," KNOM Reivew '15-01, Vol.18, No.1, pp. 25-34, August 2015.

[3] Dionisio Zumerle, Jeremy D'Hoinne, and Mark O'Neill, "API Security:What You Need to Do to Protect Your APIs," Gartnet research, August 2019.

[4] Jung Ho Seo, "The Rise of the Open Banking Era and Future Challenges," KIF Brief 28(13), pp. 4, Jul 2019

[5] Se Kyung Oh, "A Study on the Development of Payment Market according to the Change of Digital Environment," Korea Institute of Finance KIF Working Paper 2019-01, pp. 38-45, Jan 2019.

[6] Financial Services Commission, "The Plan on the Innovation of Financial Payment," Financial Services Commission Release, Feb 2019.

[7] Jung Ho Seo, "Innovation Strategy of Korea's Banking Industry through the Activation of Open API," Korea Institute of Finance KIF VIP Report 2018-08, pp. 34-46, Dec 2018.

[8] D. Hardt, "The OAuth2.0 Authorization Framework," Internet Engineering Task Force(IETF), RFC 6749, Oct 2012,

[9] Jinouk Kim, "A Study on Vulnerability Prevention Mechanism Due to Logout Problem Using OAuth," Jonornal of The Korea Institute of information Security & Cryptology, 27(1), pp. 6-7, Feb 2017.

[10] Kyu-Won Jung, Hye-seong Shin, and Jong Hwan Park, "Integrated Authentication Protocol of Financial Sector that Modified OAuth2.0," Jonornal of The Korea Institute of information Security & Cryptology, 27(2), pp. 374-376, Apr 2017.

[11] Financial Secuirty Institute, "A Guide to Self-Security Inspection of Open API User Agencies in the Financial Secotr," Financial Services Institute Release, Dec 2018.

[12] Kyusun Choi and Jiyoung Lee. "The Effects of the European Union's Implementation of PSD2 on the Financial Sector," KFTC Institue for Financial Settlements research, pp. 3-4, Nov 2018.

〔13〕 Financial Services Commission, "Electronic Financial Transactions Act," Jul 2017.
〔14〕 Ministry of the Interior and Safety, "Personal Information Protecton Act," Jul 2017.
〔15〕 Financial Services Commission, "Credit Information Use and Protection Act," Sep 2016.
〔16〕 Financial Services Commission, "Act on Real Name Financial Transaction and Confidentiality," Dec 2016.
〔17〕 Financial Services Commission, "Electronic Financial Supervision Regulations," Jan 2019.
〔18〕 Financial Services Commission, "Open Banking status and future plans," Financial Services Commission Press Release, Oct 2019.

〈저자소개〉

최 대 현 (Dae-Hyun Choi) 정회원
2018년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 전자금융보안, 정보보호 컴플라이언스, 핀테크

김 인 석 (In-Seok Kim) 정회원
1973년 2월: 홍익대학교 전자계산학과 졸업(학사)
2003년 2월: 동국대학교 정보보호학과 졸업(석사)
2008년 2월: 고려대학교 정보경영공학과 졸업(박사)
2011년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, IT감사, 전자금융법규