https://doi.org/10.33778/kcsa.2020.20.2.037

국내 오픈뱅킹 안정성 강화 및 이용자 보호를 위한 규제 개선 방안

권 남 훈*, 김 인 석**

요 약

최근 우리나라를 비롯한 EU, 영국 등은 금융구조 개혁 및 금융소비자의 편의성 제고를 위하여 금융회사가 보유하고 있는 금융정보를 핀테크기업에게 개방하는 오픈뱅킹을 적극 추진하고 있다. 향후 오픈뱅킹이 점차 활성화될수록 오픈뱅킹 제공기관의 안정성 확보 및 이용자 보호의 중요성은 더욱 커질 것이다. 특히 우리나라는 전자금융거래의 안정성과 신뢰성 확보를 위하여 2007년부터 시행해 온 전자금융거래법이 있지만, 오픈뱅킹 제공기관에게 적용하기 어려운 한계가 있어 오픈뱅킹에 대한 보안사고 예방 및 이용자 보호가 취약해질 위험성이 있다. 따라서 본 논문에서는 오픈뱅킹에 관한 외국의 규제를 살펴보고, 국내 오픈뱅킹의 안정성 강화 및 이용자 보호를 위한 규제 개선 방안을 제시해 본다.

Improvement of regulations to strengthen the safety and protect users of domestic Open Banking

Nam Hoon Kwon*, In Seok Kim*

ABSTRACT

The EU, the United Kingdom and South Korea are actively pursuing open banking to open financial information to fintech companies for financial structure reform and convenience of financial consumers. As open banking is gradually activated, the importance of stability and protecting users of open banking will increase. In particular, Korea has an electronic financial transaction law that has been in effect since 2007 to secure the stability and reliability of electronic financial transactions, but it is difficult to apply to participating organizations in open banking, so there is a risk of preventing security accidents and weakening user protection in open banking. Therefore, this paper examines the foreign legal system of open banking and analyzes the structure and characteristics of domestic open banking and suggests the ways to improve regulations necessary to strengthen open banking stability and user protection.

Key words : Open Banking, Security, Electronic Financial Transactions Act.

접수일(2020년 5월 12일), 게재확정일(2020년 5월 24일)

* 고려대학교/금융보안학과(주저자)

** 고려대학교/금융보안학과(교신저자)

1. 서 론

1.1 연구의 배경

오픈뱅킹이란 은행이 폐쇄적으로 관리하던 지급결제망을 타은행과 핀테크기업 등 제3자에게 개방하는 것을 의미한다. 즉, 과거에는 금융결제망에 직접 참가할 수 없었던 핀테크기업은 금융결제망을 이용하기 위하여 고비용의 수수료를 내면서도 은행과 제휴할 수밖에 없었다. 또한 고객은 자신이 거래하는 여러 은행의 모바일앱을 각각 설치해야하는 불편이 있었다. 이에 EU를 중심으로 오픈뱅킹이 시작되었고 우리나라는 금융위원회와 기획재정부 등 관계부처가 합동으로 2019년 2월 26일 「금융결제 인프라 혁신 방안」을 발표하고, 약 10개월간의 준비기간 및 2개월간의 시범운영을 거쳐 2019년 12월 18일 오픈뱅킹 서비스를 본격 가동하였다[1]. 오픈뱅킹이 시행됨에 따라 고객은 하나의 은행앱으로 본인이 가입한 여러 은행의 계좌를 조회할 수 있게 되었고, 자금이체 및 계좌관리를 더욱 편리하게 할 수 있게 되었다. 또한 핀테크기업들은 다수의 은행들과 개별적으로 계약할 필요없이 오픈뱅킹 참여만으로 모든 은행과 연결된 결제망에 접근할 수 있게 되었고 결제망 이용수수료도 약 1/10정도 수준으로 낮출 수 있게 되었다. 오픈뱅킹이 활성화 되면 금융회사의 금융상품별 또는 서비스별로 비교가능성이 증대되어 금융회사의 경쟁이 더욱 촉진되고 최신 IT기술을 보유한 핀테크기업이 참여함으로써 혁신적인 금융상품 또는 서비스가 제공될 수 있을 것으로 예상된다.

그러나 금융정보의 개방 및 핀테크기업의 참여로 인하여 금융혁신이라는 긍정적인 측면과 함께 새로운 유형의 전자금융 리스크가 발생하는 부정적인 측면도 함께 부각되었다. 오픈뱅킹에 참여하는 모든 은행의 금융데이터가 개방됨에 따라 오픈뱅킹 서비스를 제공하는 사업자 중 한 곳이라도 해킹공격이나 악의적인 내부자에 의하여 뚫리게 되면 개방된 모든 금융정보가 유출되거나 불법적인 전자자금이체 사고가 발생될 수 있다. 오픈뱅킹을 먼저 시작한 EU 등에서는 법제화된 오픈뱅킹 시행 근거를 마련함과 동시에 오픈뱅킹 사업자에 대해 자기자본금 확보, 강화된 인증방법 사용, 손해배상책임 등의 규제방안도 함께 마련한 후 오픈뱅킹을 시행하였다. 그러나 우리나라는 오픈뱅킹이 시행된지 몇 개월이 지났지만 여전히 오픈뱅킹에 관한 법제화를 준비중인 상황이다.

우리나라는 전자금융거래의 안정성과 신뢰성을 확보하기 위하여 2007년 1월부터 시행된 전자금융거래법이 있음에도 불구하고 전자금융서비스를 제공하는 일부 오픈뱅킹 참가기관에 대해서는 전자금융거래법을 적용하기 어려운 규제 사각지대가 발생하게 되었다. 즉, 오픈뱅킹에 참여하고 있는 일부 핀테크기업과 오픈뱅킹의 중계시스템을 운영하고 있는 금융결제원은 전자금융거래법상 금융회사 또는 전자금융업자 등에 해당되지 않으므로 법에서 규정하고 있는 전자금융거래의 안전성 확보 및 이용자 보호를 위한 기준, 전자금융사고로 인한 이용자 손해배상책임 등을 적용할 수 없다. 그러나 오픈뱅킹으로 새롭게 등장한 중소형 핀테크기업에게 기존 금융회사와 동일한 규제를 적용할 경우에는 핀테크기업의 활발한 참여와 혁신적인 금융서비스 개발이 어려워질 수 있으므로, 오픈뱅킹 활성화와 전자금융서비스의 안정성을 모두 만족하는 적정한 수준의 규제가 필요하며 이를 위한 지속적이고 폭넓은 토론과 연구가 필요한 시점이다.

한편 최근 신용정보의 이용 및 보호에 관한 법률(이하 '신용정보법') 개정안이 통과(2020년 1월 9일)됨에 따라 마이데이터 및 마이페이먼트와 같은 새로운 금융서비스가 출현할 수 있는 기반이 마련되었고, 이러한 서비스와 이미 시행중인 오픈뱅킹 서비스간의 차이점 또는 경계에 관한 법률적 문제점도 제기되고 있으나[2], 본 연구에서는 오픈뱅킹 서비스의 안전성과 소비자 보호로 한정하여 전자금융거래법 개정을 통한 규제 개선 방안을 제시하고자 한다.

1.2 선행 연구

오픈뱅킹에 관한 기존 연구는 외국의 오픈뱅킹 추진배경과 금융산업 변화에 따른 대응전략, 오픈뱅킹의 보안취약점 및 보안강화 방안을 제안하는 내용이 대부분이었다. 삼정KPMG의 2019년 3월 발표한 보고서에 따르면 EU, 영국 등은 금융데이터의 활용도를 높이고 금융산업 혁신 및 은행간 또는 은행과 핀테크기업간에 공정한 경쟁을 촉진하기 위하여 은행에서 보유하고 있는 금융계좌정보 및 지급결제망을 핀테크

기업에게 차별없이 오픈하는 정책을 도입하였으며, 이로 인하여 은행에서 핀테크기업으로 금융산업의 축이 이동되는 한편, 금융업의 분업화와 재결합이 촉진되면서 새로운 금융서비스가 출현하는 등 금융산업의 구조가 크게 변화될 것으로 전망하였다[3]. 한국금융연구원의 서정호 선임연구원은 “오픈API의 활성화를 통한 국내 은행산업의 혁신전략”에서 오픈뱅킹의 성공은 비즈니스 모델에 의해 결정되기 때문에 참신한 아이디어를 지속적으로 제시할 수 있는 여건 조성이 필요하며 개방형 혁신(Open Innovation)이 촉진되기 위해서는 오픈뱅킹 운영과정에서 보안사고가 발생할 경우 정부 또는 감독기관의 제재를 받을 수 있다는 우려가 없어야 하며, 금융회사에서 보안시스템을 강화할 책임은 있으나 감독당국의 재재나 처벌이 추가적으로 수반될 경우 새로운 혁신에 대해 시도가 줄어들 수 있다고 주장하였다[4]. 또한 오픈뱅킹시스템에 대한 접근성을 높이기 위하여 은행과 핀테크기업이 공동으로 사용하는 금융결제원 공동업무시스템의 이용 수수료 체계를 최대한 수익자 부담 원칙에 따라 개편하고, 핀테크기업의 파산 또는 결제불이행 우려를 방지할 수 있도록 핀테크기업에 대한 진입규제 강화 등 오픈뱅킹의 안정성 제고가 필요하다고 하였다[5]. 최대현의 “안전한 오픈뱅킹 구축을 위한 정책 및 B2B2C 모델에 관한 연구”에서는 오픈뱅킹의 구조와 보안위협 등에 대하여 연구하였는데, 오픈뱅킹 이용기관의 시스템 관리자에 의한 정보유출 위협을 방지하기 위해서는 오픈뱅킹 중계기관을 거치지 않는 고객과 금융회사간에 직접 인증하는 방안을 제안하였다[6]. 송미정의 “유럽 PSD2 시행에 따른 금융분야 마이데이터 정책의 개인정보보호 강화 방안 연구”에서는 PSD2시행으로 오픈뱅킹 및 마이데이터 정책이 시작되었으며, 금융정보가 핀테크기업으로 이동함에 따라 개인정보 유출 리스크가 증가되었고 이러한 위험에 대응하기 위하여 개인정보 생명주기별 기술적 대응방안을 제시하였다[7].

이와 같이 기존 오픈뱅킹에 관한 연구에서는 외국의 오픈뱅킹 규제에 대한 비교분석 및 우리나라 전자금융거래법을 통한 규제개선에 대한 연구는 없었으므로 본 연구의 가치가 있다고 평가할 수 있다.

2. 외국의 오픈뱅킹 규제 현황

2.1 EU의 오픈뱅킹 관련 규제

EU의 EBA(European Banking Authority, 유럽은행감독청)는 유로화 도입 이후 SEPA(Single Euro Payment Area, 단일유로지급지역) 내에 지급서비스의 효율성 및 안전성 확보를 위하여 지급서비스지침(Payment Services Directive1, PSD1)을 2009년 시행하였다[8]. 이후 모바일 결제 등 새로운 유형의 지급서비스 및 핀테크업체가 출현함에 따라 PSD를 개정하여 지급서비스지침2(Payment Services Directive2, PSD2)를 2015년 12월 공식 발표하고, 2년여의 준비기간을 거친 뒤 2018년 1월 13일 PSD2를 시행하였다[5]. PSD에서는 지급서비스(payment service)와 지급기관(payment institution)을 정의하고 은행외에 핀테크기업과 같은 비은행 기관도 지급서비스에 참여할 수 있도록 허용하였다[3]. 특히 PSD2(Article 66, Article 67)에서는 새로운 2종의 지급서비스로 지급결제지시서비스(Payment Initiation Services, 이하 ‘PIS’)와 계좌정보서비스(Account Information Services, 이하 ‘AIS’)를 추가함으로써 오픈뱅킹 서비스에 대한 법적근거를 마련하였다.

이어서 PSD2에서는 지급개시서비스를 제공하는 자(Payment Initiation Services Providers, PISP)와 계좌정보서비스를 제공하는 자(Account Information Services Providers, AISP)를 정의하고, 고객이 동의하는 경우 고객정보를 제공할 의무를 부과하였다. 그리고 이들 지급기관에게 초기자본금 요건(Article 7) 및 금융감독당국의 허가 또는 등록 요건(Article 5)을 부과하였다[9](표1 참고). 그 외에도 PSD2에서는 허가 또는 등록시에 보안사고 및 이용자 불만에 대한 보고의무, 지급결제정보에 대한 접근통제, 핵심업무에 대한 비상계획 수립 등의 요건을 함께 명시하였으며 금융감독당국은 지급기관의 설립 인허가 이후 12개월 동안 영업활동을 하지 않거나, 인허가 요건을 유지하지 못하는 경우에는 허가 또는 인가를 취소(Article 13)할 수 있도록 하였다. 아울러 PISP와 AISP에 대하여 연 1회 이상 위험평가를 실시하고 그 결과를 금융당국에 보고(Article 95)하도록 의무화하였다[5][10].

<표 1> PSD2에서 지급기관 진입규제

구분	PISP	AISP
초기자본	EUR 50,000	해당 사항 없음
자기자본	없음	없음
허가 또는 등록	허가	등록

또한 PSD2에서는 오픈뱅킹 이용자 보호를 위하여 지급지시 오류(unauthorised payment transaction)가 발생할 경우 은행이 우선 보상하고 PISP에게 청구하도록 하였다(Article 73). 다만, 고객이 지급수단을 분실하거나 도난당하여 승인하지 않은 거래가 발생했을 경우에는 고객의 책임한도를 50유로로 정하되, 고객의 사기나 고의성을 PISP가 입증하게 되면 해당 사고금액을 고객이 전액 부담하도록 하고 있다(Article 74)[11].

EU는 지급서비스의 안전성 확보를 위하여 기술규제 표준(Regulatory Technical Standards on Strong Customer Authentication and Secure Open Standards of Communication, 이하 'RTS')을 2018년 3월에 확정하고 18개월 이후인 2019년 9월 시행하였다. RTS에서는 API에 대한 세부표준을 제시하지 않고 은행들이 자율적으로 결정하도록 하였다. 다만 안전성이 낮고 고객의 명시적 동의없이 정보수집이 일어날 수 있는 스크린스크래핑은 불허하였고, 전자지급거래를 지시하는 경우 지식기반 인증과 속성기반의 인증방법 두가지 인증방식을 조합한 인증 방식을 적용하도록 의무화 하였다[5].

2.2 영국의 오픈뱅킹 관련 규제

영국의 경쟁시장당국(Competition & Markets Authority, CMA)은 EU의 PSD2의 주요 요건을 반영하여 Bank of Ireland, Barclays 등 9개 주요은행에 대하여 공통API프레임워크(Common API framework)를 의무적으로 채택하고 고객의 동의가 있는 경우 API를 통해 계좌정보를 제3자에게 제공하도록 의무화 하는 지침(Retail Banking Market Investigation Order 2017, 이하 'CMA order')을 2017년 10월에 발표하였다. CMA에 의하여 설립된 OBIE(Open Banking Implementation Entity)는 PSD2와 RTS의 기준을 충족하기 위해서 2018년 9월 오픈뱅킹의 API표준요건을 담은 'Open Banking Standard 3.0'을 발표하고 데이터, API, 보안 등에 관한 표준을 정의하였다[5][11].

영국 금융행위감독청(Financial Conduct Authority, FCA)은 PSR 2017(The Payment Services Regulations 2017)을 제정하고 비은행 지급기관(Non-bank Payment Service Providers)은 FCA로부터 지급기관(Payment Institution) 승인을 받도록 하였다(PSR PART 2 Registration 6. Conditions for authorisation as a payment institution).

또한 영국의 FCA는 PISP에게 초기 자본금으로 50,000유로를 보유할 것을 의무화하고 AISP에게는 초기 자본금 요건은 면제함으로써 지급서비스 종류에 따라 진입규제 요건을 차별화하였다. 또한 고객의 자금을 안전하게 관리하도록 하기 위하여 PISP에게 고객의 자금을 지급기관의 운영자금과 분리하도록 하였다. 아울러 PISP에 대하여 지배구조 협약, 고객자금에 대한 안전장치, 금융범죄 통제기능 등을 모니터링하고, 규제를 준수하지 않는 지급기관에게 벌칙을 부과하는 등 지급기관에 대한 관리감독을 실시하고 있다(PSR PART 9 The Financial Conduct Authority)[5][12].

2.3 일본의 오픈뱅킹 관련 규제

일본은 2009년 6월 17일 자금결제법(資金決濟に關する法律, Payment Services Act)을 제정하여 새로운 결제서비스 도입환경을 마련하고 결제서비스의 안정성 확보 및 이용자 보호를 위한 규제도 함께 시행하였다. 자금결제법에 따라 은행 이외의 사업자도 자금이동(자금이체)업을 수행할 수 있도록 허용(자금결제법 제37조)하되, 금융사고에 대비하여 자금이동의 한도를 100만엔/회 이하(총액제한은 없음)로 제한하였다[13].

이어서 일본은 은행법(銀行法, Banking Act)을 개정(2017년 5월 26일)하고 시행일(2018년 6월 2일)로부터 2년 이내에 오픈API 도입을 위해 노력할 의무를 부과하였다(은행법 부칙 제11조 제1항). 개정된 은행법에서는 전자결제대행업자(電子決濟等代行業者)를 신설하고 금융청 등록요건과 최소자본금 요건(0엔 이상)을 부과하였다[15]. 일본의 전자결제대행업자

(Electronic Payment Intermediate Service Provider, EPIS Provider)는 PISP와 AISP를 결합한 형태의 서비스로 핀테크기업이 전자결제대행업자로서 오픈API를 적용하기 위해서는 다음의 조건을 충족하여야 한다[5].

- 전자결제대행업자로서 금융청에 등록
- 최소순자본금으로 0엔 이상을 유지
- 은행과 계약 체결

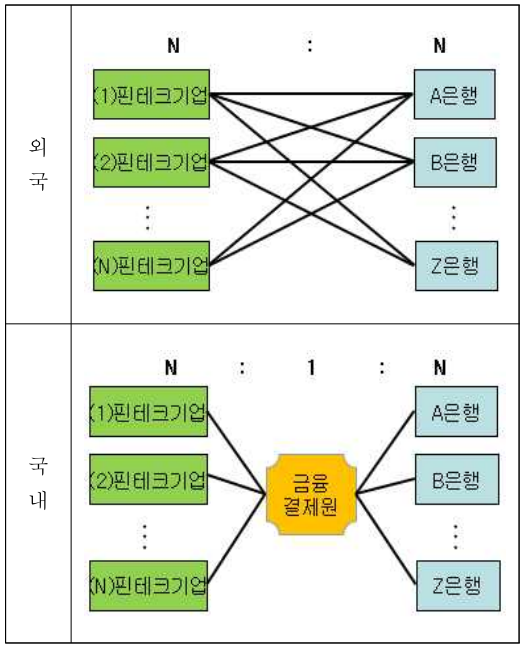
또한 일본은 전자지급서비스 이용고객에게 손실이 발생할 경우 전자결제대행업자가 우선 배상하고 필요시 은행에게 사후 구상요구를 할 수 있도록 하였다[14].

2.4 외국의 오픈뱅킹 규제를 통한 시사점

EU 등 외국의 오픈뱅킹의 규제를 살펴본 결과 국내 오픈뱅킹 환경과 구별되는 3가지 시사점이 있다. 첫 번째는 오픈뱅킹 법제화에 관한 사항으로 EU의 PSD2와 RTS, 영국의 CMA order, 일본의 개정된 은행법에서 알 수 있듯이 외국은 금융정보 개방(오픈뱅킹)에 관한 법적인 근거를 마련한 후 서비스가 시행된 반면, 우리나라는 금융정보 개방에 관한 법제화가 시행되기도 전에 은행과 금융결제원 및 금융결제원과 핀테크기업간에 체결한 약관을 근거로 서비스가 시행되었다. 오픈뱅킹 이용약관에는 안정적인 오픈뱅킹 서비스 유지를 위한 다양한 요건들이 명시되어 있지만, 오픈뱅킹에 참여하는 기관이 다수이고 구조가 복잡하여 사고 발생시 원인분석이 어렵고, 은행이 오픈뱅킹 계약을 해지하거나 서비스를 중단하는 경우 오픈뱅킹 사업자 및 이용자의 손실 또는 불편이 초래될 수 있는 문제점이 있다. 따라서 안정적인 오픈뱅킹 서비스 제공을 위한 법제화가 필요하다.

두 번째는 오픈뱅킹 구성에 관한 사항으로 외국의 오픈뱅킹 구성에는 은행과 핀테크기업을 연결하는 중계기관이 없다. 즉, 외국은 핀테크기업과 은행의 관계를 N : N으로 표현할 수 있다. 이에 반해 우리나라는 은행과 연결된 금융결제원에서 핀테크기업에게 금융정보를 제공하는 형태이므로 핀테크기업, 금융결제원, 은행의 관계를 N : 1 : N의 관계로 표현할 수 있다(그림1 참고). 이는 우리나라 오픈뱅킹은 금융결제원이라는 중계기관(오픈뱅킹 공동업무시스템)을 통해서 시스템이 운영되는 특징이 있으며, 오픈뱅킹의 표준 적용 및 관리통제가 용이한 장점이 있는 반면, 오픈뱅킹 중계기관의 장애 또는 해킹사고가 발생할 경우 오픈뱅킹 서비스 전체에 영향을 미치는 위험이 발생한다. 따라서 오픈뱅킹 중계기관에 대한 철저한 관리감독이 필요하다.

세 번째는 오픈뱅킹에 참여하는 핀테크기업에 대한 정부기관의 감독에 관한 사항으로 영국, 일본의 사례에서 제시한 바와 같이 EBA, FCA 등 금융감독기관이 오픈뱅킹에 참여하는 비금융회사(핀테크기업)에 대해 인허가 및 안전성 감독을 수행하고 있다. 그러나 국내는 금융감독기관이 아닌 금융결제원이 계약에 근거하여 핀테크기업에 대한 점검과 승인 등 관리를 수행하고 있다. 현재 우리나라는 전자금융거래법에 근거하여 금융감독당국이 금융회사의 전자금융서비스를 감독하고 있다. 따라서 오픈뱅킹에 참여하는 핀테크기업에 대해서도 유사한 감독체계가 적용될 필요가 있다.



(그림 1) 외국과 국내 오픈뱅킹 구성 비교

<표 2> 각국의 오픈뱅킹 관련 규제 비교

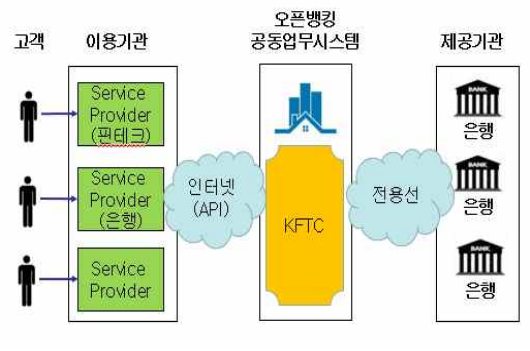
구분	한국	EU	영국	일본
오픈뱅킹 제공서비스	추심이체(direct debit)를 이용한 자금이체서비스, AIS(Account Information Services 계좌정보서비스)	PIS(Payment Initiation Services 지급지시서비스), AIS(Account Information Services 계좌정보서비스)	EU와 같음	EPIS(Electronic Payment Intermediate Service, 전자결제대행)
오픈뱅킹 운영근거	-금융결제원과 참여기관간 계약	- PSD2 - RTS (Regulatory Technical Standards)	- PSR(Payment Services Regulations) 2017 - Open Banking Standards 3.0	- 은행법, 자금결제법 - Open API 이용약관
오픈뱅킹 법제화 여부	없음 (준비중)	있음	있음	있음
오픈뱅킹 감독주체	없음	EBA(European Banking Authorities, 유럽은행감독청)	FCA(Fianacial Conduct Authority, 금융행위감독청)	FSA(Financial Services Agency, 금융청)
진입규제 및 건전성 확보 기준	- 진입규제 : 금융결제원 승인 - 최소자본금 요건 없음	- 진입규제 : PIS(허가), AIS(등록) - 최소 설립 자본금 : PIS(EUR 50,000), AIS(조건 없음)	EU와 같음	- 진입규제 EPIS(등록) - 최소 자본금 0엔(음수 불가) - 자금이동업자 이행보증금 공탁
안전성 확보 기준	- 금융보안원의 보안점검 통과(이용기관 점검 및 어플리케이션 보안점검)	- 보안점검 및 비상계획 수립 - 금융사고 발생시 금융감독당국 보고 - 온라인 접속, 또는 비대면 거래시 강화된 인증(SCA, Strong Customer Authentication) 사용 - Screen Scraping 사용불가	EU와 같음	- 적절한 보안수단 확보 및 불법적인 접근 차단 - 국제적인 API기준 준수 - 스크린스크래핑 대신 Open API 제공
이용자 보호 기준	- 일간 이체한도(최대 1천만원) 설정 - 일간 이체한도 금액의 200% 이내의 보증보험 가입 -이용기관은 고객민원 및 사고발생시 피해금액을 선지급	- 고객으로부터 받은 자금은 다른 목적의 자금과 분리 - 무권한 거래로 인한 고객손실은 은행이 우선 보상후 PISP에게 청구 - 고객의 지급수단 분실 및 무권한 거래에 대해 고객의 책임한도를 EUR50 한정 (고객의 고의 또는 중과실인 경우 제외)	EU와 같음	- 무권한 거래(unauthorised payment transaction)에 의한 고객 손실은 전자결제대행업자가 우선 배상 - 고객에서 은행서비스 오인 방지를 위한 설명의무

3. 국내 오픈뱅킹 현황

3.1 오픈뱅킹 참가기관 및 구성

국내 오픈뱅킹 구성을 보면 고객, 이용기관(핀테크 기업 등), 오픈뱅킹 공동업무시스템 운영기관(금융결제원), 제공기관(은행)으로 구분할 수 있다. 은행은 오픈뱅킹 이용기관이 요청하는 금융정보조회, 출금이체 등을 처리하고 그 결과를 오픈뱅킹 공동업무시스템을 통해 이용기관에게 제공한다. 금융결제원은 오픈뱅킹 공동업무시스템을 운영하고 이용기관에서 요청하는 서비스를 제공기관에 전달하고 그 처리결과를 다시 이용기관에게 전달하는 중계시스템을 운영하고 오픈뱅킹에 참가를 원하는 핀테크기업에 대한 보안점검 및 이용기관 등록, 수수료 정산 등 오픈뱅킹 업무 전반을 운영·관리한다. 오픈뱅킹 이용기관은 금융결제원과 오픈뱅킹업무에 관한 계약을 체결하고 오픈뱅킹 이용고객에게 은행계좌에 대한 거래내역 조회, 이체 등의 금융서비스를 제공한다. 현재 오픈뱅킹 이용기관으로는 은행, 전자금융업자 또는 핀테크기업이 참여하고 있다[15](그림2 참고).

2020년 1월 기준으로 193개 기업이 오픈뱅킹 이용기관으로 신청한 가운데 48개 기업이 오픈뱅킹에 참여중이며, 이중 기존 금융결제원의 오픈플랫폼 이용기관이었던 19개사는 전자금융거래법의 적용을 받지 않은 이용기관이다[16](표3 참고).



(그림 2) 오픈뱅킹 개념도[15]

<표 3> 오픈뱅킹 이용기관 구분(2020.1.10. 기준)

구분	이용기관 (회사수)		비고
은 행	은행	(17)	전자금융거래법 대상(29)
핀테크 사업자	전자금융업자	(7)	
기존 오픈플랫폼 이용기관	전자금융업자	(5)	
	일반	(19)	전자금융거래법 대상이 아님(19)
합 계		(48)	

3.2 오픈뱅킹 추진경과 및 서비스 종류

금융위원회는 관계부처와 합동으로 2019년 2월 「금융결제 인프라 혁신 방안」으로 3대 추진전략 및 9대 추진과제를 발표하고, 오픈뱅킹의 법제화 등을 세부 추진과제로 제시하였다[1](표4 참고). 다만 2단계 과제였던 오픈뱅킹 법제도화를 제외하고 오픈뱅킹 서비스는 계획대로 진행되었다.

현재 시행중인 오픈뱅킹 서비스는 조회서비스와 이체서비스 2가지로 구분할 수 있고, 조회서비스는 이용자가 보유하고 있는 은행계좌에 대한 잔액조회, 거래내역조회, 계좌실명조회, 송금인정보조회가 있고, 이체서비스는 출금이체와 입금이체로 2가지로 구성되어 있다(표5 참고). 2020.1월 기준으로 오픈뱅킹 서비스 이용건수는 일평균 374만건이며 잔액조회(58%), 출금이체(28%), 거래내역 조회(10%), 계좌실명조회(3%), 입금이체(1%) 순으로 이용하고 있다[16].

<표 4> 오픈뱅킹 추진 로드맵[1]

구분	추진계획	관련 규정
1단계 ('19년 시행)	공동결제시스템 (오픈뱅킹) 구축	금융결제원 규약 개정
2단계 ('19년 추진)	오픈뱅킹 법제도화	전금법 개정
3단계 (중장기 추진)	핀테크기업에 금융결제망 직접 개방	전금법 및 한은 규정 개정

<표 5> 오픈뱅킹 서비스 유형[17]

구분	세부 내용
조회	① 잔액조회 : 사용자 본인계좌의 잔액을 조회
	② 거래내역 조회 : 사용자 본인계좌에 대한 입출금내역을 조회
	③ 계좌실명조회 : 이용기관이 사용자 계좌의 유효성 및 예금주명을 조회
	④ 송금인정보조회 : 이용기관 수납계좌로 입금한 사용자명 및 송금계좌번호 조회
이체	⑤ 출금이체 : 사용자 계좌에서 자금을 인출하여 이용기관 수납계좌로 집금
	⑥ 입금이체 : 이용기관 지급계좌에서 자금을 인출하여 사용자 계좌로 입금

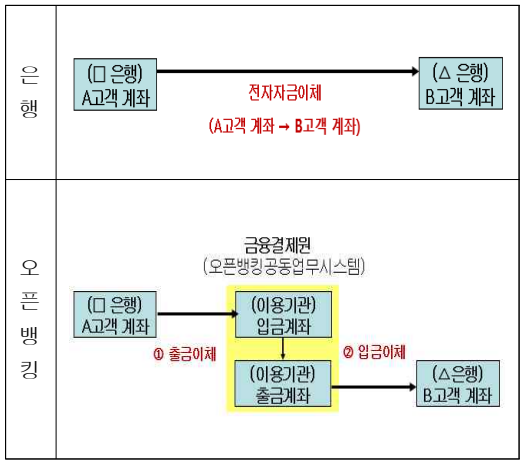
오픈뱅킹 이용기관은 고객에게 오픈뱅킹 앱 또는 웹어플리케이션을 통해 서비스를 제공한다. 이용기관으로 참여하는 은행은 주로 간편결제, 간편송금 등의 서비스를 제공하고, 이용기관으로 참여하는 핀테크기업은 간편송금 외에도 해외송금, 중개서비스, 자산관리 등 다양한 서비스를 제공하고 있다(표6 참고). 또한 은행의 오픈뱅킹 서비스 이용실적은 잔액조회가 84%인 반면, 핀테크기업의 이용실적은 출금이체가 81%로 은행과 핀테크기업의 오픈뱅킹 서비스 이용실적이 다른 특징이 있다[16].

<표 6> 오픈뱅킹 이용기관 신청 및 승인 현황[16]

구 분	신청	승인	전면시행 참여 기관	
			기관수	비고
은 행	18개	—	17개	분야 / 개수
핀테크 사업자	149개	103개	7개	간편송금 23개 / 해외송금 13개 / 중개서비스 6개 / 자산관리 5개 / 쇼핑몰 1개
기존 오픈플랫폼 이용기관	26개	—	24개	
합 계	193개	103개	48개	

3.3. 오픈뱅킹 자금이체의 특성

오픈뱅킹에서 이용고객이 오픈뱅킹을 통해 자금이체지시를 하면 오픈뱅킹 이용기관은 출금이체와 입금이체 서비스 조합하여 자금이체가 이루어지는 특징이 있다(그림3 참고).



(그림 3) 오픈뱅킹 자금이체 흐름도 비교

오픈뱅킹 이용고객의 지급지시(지급인 A계좌에서 수취인 B계좌로의 자금이체)가 있을 때, 이용기관은 ① 출금이체(지급인 A계좌에서 이용기관 수납계좌로 이체지시) ② 입금이체(이용기관의 지급계좌에서 수취인의 B계좌로 이체지시) 2단계로 정보를 처리함으로써 지급인계좌(A)에서 수취인계좌(B)로 자금이체를 실행하게 된다. 이때 출금이체 및 입금이체는 은행이 수수료를 받고 일반기업에게 제공해온 추심이체 서비스 또는 펌뱅킹 서비스와 동일한 방식이다.

전자금융거래법 제2조 제11호에서는 전자자금이체를 지급인과 수취인 사이에 자금을 지급할 목적으로 금융회사 또는 전자금융업자에 개설된 계좌에서 다른 계좌로 자금을 이체하는 방식이라고 정의하고 있다. 또한 동법 제28조 제2항에서는 전자자금이체업무를 행하고자 하는 자는 금융위원회에 등록을 하도록 명시하고 있다. 그러나 오픈뱅킹에서 제공하는 전자자금이체는 출금이체와 입금이체의 조합으로 구성되어 있어 전자금융거래법상의 전자자금이체와는 다르며, 오픈뱅킹 이용기관에게 전자자금이체업자로 등록하도록 요구하고 있지 않는 상황이므로, 이용기관 중 일부 금융회사 또는 전자금융업자에 해당하지 않는 핀테크기업 19개사는 전자금융거래법을 적용받지 않으며 전자금융거래법에서 규정하고 있는 관리적, 기술적, 물리적 보안기준을 적용할 의무가 없다.

3.4. 오픈뱅킹 이용기관 신청 및 승인

오픈뱅킹 이용기관으로 참여하고자 하는 기업은 금융결제원에 신청을 한 후 5단계 절차(① 오픈뱅킹 이용신청 ② 이용적합성 심사 ③ 서비스 개발 및 테스트 ④ 이용기관 보안점검 및 어플리케이션 취약점 점검 ⑤ 이용계약 체결)를 거치게 된다. 금융결제원은 신청기관에 대해 보안점검결과와 사업 모델의 적정성, 법률적 자격요건 등을 종합적으로 검토하여 이용기관으로 등록 여부를 결정한다. 4번째 단계의 보안점검은 현재 금융결제원으로부터 위탁받은 금융보안원에서 수행하고 있으며, 보안점검은 신청기관의 운영환경 전반에 대한 보안관리체계 점검 및 모바일앱 또는 웹어플리케이션에 대한 취약점 점검으로 구분하여 점검하고 있다. 금융결제원은 금융보안원의 보안점검결과를 통과한 신청기관과 최종적으로 수수료 책정 등 업무협상을 거친 뒤 계약을 체결하게 된다[17].

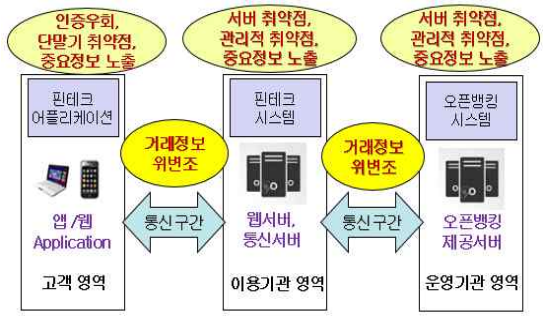
오픈뱅킹 이용기관이 금융결제원과 체결하는 이용계약에는 개인정보에 대한 관리의무, 출금이체와 입금이체에 대한 건당한도 및 일간한도 설정, 일간한도의 금액에 상응하는 보증보험 가입, 하위사업자에 대한 관리 및 추가시 금융결제원의 사전 승인, 자금세탁방지를 위한 보고, 금융사고 방지를 위한 대응체계 마련, 고객의 착오송금 등의 오류에 대한 자금 청구 반환 처리, 정보유출시 통지, 민원 및 사고발생시 피해금액 선지급 등 피해구제 방법 수립, 거래기록의 유지, 손해배상 책임, 분쟁발생시 금융결제원 처리기준으로 처리 등의 의무가 명시되어 있다[18].

4. 오픈뱅킹 문제점과 규제 개선 방안

4.1 문제점

4.1.1 이용기관의 기술적·관리적 보안리스크

오픈뱅킹의 보안위협 및 취약점으로는 사용자 인증우회, 거래정보 노출 및 위변조 등이 있다[6]. 오픈뱅킹에 참여하는 은행은 금융결제원과 연결된 전용선을 통해 거래에 관한 전문을 송수신한다. 은행과 금융결제원간의 연결방식은 오랜 기간 CD공동망, 전자금융공동망과 같이 운영해온 방식이므로 안정성이 검증되었다고 판단된다. 이에 반해 오픈뱅킹 이용기관으로 참여한 핀테크기업은 인터넷망을 통해 금융결제원과 처음 연동함에 따라 새로운 보안리스크가 발생하게 되었다(그림4 참고). 핀테크기업이 이용고객에게 제공하는 오픈뱅킹용 모바일앱 또는 모바일 단말기 자체에 보안취약점이 존재할 수 있으며 이러한 취약점을 이용하여 사용자 인증우회, 거래정보 노출 등의 사고가 발생할 수 있다. 또한 핀테크기업에서 운영중인 서버 또는 네트워크 등의 보안설정 또는 보안패치 미적용, 보안정책 미흡 등 기술적, 관리적 보안취약점을 이용하여 오픈뱅킹 시스템에 있는 금융거래정보가 노출되거나 변조되는 위험이 존재할 수 있다.



(그림 4) 오픈뱅킹 위협과 취약점[19]

이러한 오픈뱅킹의 보안리스크를 진단하기 위하여 오픈뱅킹 이용기관으로 참여하는 이용기관은 금융보안원이 수행하는 보안점검을 통과하여야 하며, 보안점검은 이용기관의 보안관리체계를 점검하는 보안점검과 이용기관이 고객에게 제공하는 모바일앱 또는 웹어플리케이션에 대한 보안취약점 점검으로 구분하여 진행된다. 첫 번째 이용기관 보안점검은 금융보안원이 개발한 3개영역 14개분야 30개의 점검항목으로 이루어져 있으며(표7 참고), 금융보안원 인력 3명 내지 5명이 서면점검과 현장점검으로 구분하여 약 4주간 실시한다. 단, 이용기관이 은행이거나 전자금융업자로 등록된 기관, 한국인터넷진흥원의 ISMS인증을 받은 경우에는 이용기관 자체점검으로 대체가 가능하다. 두 번째 이용기관이 개발한 모바일앱 또는 웹 어플리케이션에 대한 취약점 점검은 모바일앱의 경우 5개분야 17개항목으로 구성되어 있고, 웹어플리케이션의 경우는 4개분야 12개항목으로 이루어져 있다[20].

<표 7> 오픈뱅킹 이용기관 점검항목[20]

구분		점검분야(점검항목 수)
관리체계 보안점검	관리	보안정책(2), 인적보안(5), 위험관리(1), 침해사고 대응(2), 이용자 보호(3)
	물리	물리적보안(2)
	기술	개발보안(2), 암호통제(1), 접근통제(2), 시스템보안(6), 네트워크보안(4)
어플리케이션 취약점 점검	웹	중요정보 보호(6), 거래정보 위·변조(3), 서버보안(1), 인증(2)
	모바일	중요정보 보호(6), 거래정보 위·변조(3), 서버보안(1), 인증(2), 클라이언트 보안(5)

오픈뱅킹 이용기관은 이용고객의 계좌정보를 조회하고 이체정보를 처리하므로 신용정보법의 신용정보제공·이용자에 해당[신용정보의 이용 및 보호에 관한 법률 제2조 제7호]되며, 신용정보법에서 정하고 있는 기술적·물리적·관리적 보안대책[신정법 제19조]을 준수할 의무가 있다[21]. 그러나 신용정보법 제19조에 근거한 신용정보업감독규정 별표3의 '기술적·물리적·관리적 보안대책 마련기준'에 있는 항목을 전자금융거래법 제21조 및 전자금융감독규정 제3장의 '전자금융거래의 안전성 확보 및 이용자 보호'의 항목과 비교해 보면 크게 차이가 있음을 알 수 있다. 즉, 전자금융서비스를 제공하는 금융회사는 전자금융거래법규의 안정성 기준을 의무적으로 준수해야 하는데 반해, 오픈뱅킹에 이용기관으로 참가하는 핀테크기업은 전자금융거래법의 안전성 기준을 준수할 의무가 없다. 다만 신용정보이용기관에 해당되므로 신용정보법의 보안대책 기준을 준수할 의무가 있지만 전자금융거래법 수준에는 크게 미치지 못하는 문제가 있다. 오픈뱅킹 이용기관으로 참여하기 위해 통과해야 하는 금융보안원의 30개 보안점검 항목과 신용정보법 하위 신용정보업감독규정 별표3의 '기술적·물리적·관리적 보안대책 마련기준'을 모두 준수한다 하더라도 전자금융감독규정 제3장의 '전자금융거래의 안전성 확보 및 이용자 보호'의 항목과 비교해 보면, 전자금융감독규정의 13개 항목에 대해서는 여전히 충족하지 못하고 있다(표8 참고)[22].

<표 8> 전자금융거래 보안대책 기준 비교

전자금융감독규정	신용정보법 및 오픈뱅킹 보안점검 항목
인력 조직 및 예산(제8조), 전산실 등에 관한 사항(제11조), 단말기 보호대책(제12조), 전산자료 보호대책(제13조), 정보처리시스템 보호대책(제14조), 해킹 등 방지대책(제15조), 악성코드 감염 방지대책(제16조), 홈페이지 등 공개용 웹서버 관리대책(제17조), IP주소 관리대책(제18조), 정보기술부문 계획서 제출(제19조), 정보보호 교육계획의 수립 시행(제19조의 2), 비상대책 등의 수립·운용(제23조), 정보처리시스템의 성능관리(제25조), 전산원장 통제(제27조), 프로그램 통제(제29조), 암호프로그램 및 키관리 통제(제31조), 내부사용자 비밀번호 관리(제32조), 이용자 비밀번호 관리(제33조), 전자금융거래 시 준수사항(제34조), 전자금융기반시설의 취약점 분석·평가 주기, 내용 등(제37조의 2), 정보보호최고책임자의 업무(제37조의 5), 외부주문등에 대한 기준(제60조)	유사항목 존재 (22개)
정보보호위원회 운영(제8조의 2), 건물에 관한 사항(제9조), 전원, 공조 등 설비에 관한 사항(제10조), 클라우드컴퓨팅 이용절차 등(제14조의 2), 정보처리시스템 구축 및 전자금융거래 관련 사업 추진(제20조), 정보처리시스템 구축 및 전자금융거래 관련 계약(제21조), 비상대응훈련 실시(제24조), 직무의 분리(제26조), 거래통제 등(제28조), 일괄작업에 대한 통제(제30조), 이용자 유의사항 공지(제35조), 자체보안성심의(제36조), 인증방법 사용기준(제37조)	유사항목 없음 (13개)

오픈뱅킹 참가기관에 대한 점검항목 30개를 전자금융감독규정의 관리적 기술적 보호대책에 관한 조항과 비교해 보면 13개 항목에 대해서는 유사하게 매칭되

는 항목이 없고, 전자금융감독규정 보다 세부적이지 않다. 따라서 오픈뱅킹 보안점검 항목만으로는 기술적 또는 관리적인 보안리스크가 발생될 수 있음을 알 수 있다. 구체적으로 예를 들어보면, 전산시스템이 위치한 건물 및 전산실의 전원 및 공조 시설, 출입통제 등 물리적 안전대책, 중요 정보보호에 관한 사항을 심의·의결하는 정보보호위원회 운영, 정보처리시스템 구축 시 설계단계부터 보안대책 마련, 정보처리시스템 구축 및 전자금융거래 계약시 정보보안 관련 사항 포함, 전산망 마비 등에 대비한 정기적인 비상대응훈련 실시, 정보처리시스템 운영의 내부통제 강화를 위한 직무분리 등의 항목이 미흡해질 위험이 존재한다.

전자금융감독규정의 기술적 관리적 보호대책의 세부항목까지 비교해보면 몇 가지 더 중요한 보안대책 기준이 오픈뱅킹 점검항목에는 누락되어 있음을 알 수 있다. 특히 금융회사에서는 의무적으로 적용되고 있는 내외부망 분리가 오픈뱅킹 이용기관에 대한 보안점검 항목에는 포함되어 있지 않다. 그 외에도 전산자료의 사고추적 등을 위한 정보처리시스템 접근기록 보존 의무, 5회 이상의 시스템 접속 오류시 사용제한, 전산자료의 백업 및 소산 등의 보안대책이 포함되어 있지 않다. 따라서 오픈뱅킹 이용기관은 금융보안원의 보안점검을 통과하더라도 전자금융거래법에 의해 금융감독당국의 감독을 받아온 금융회사의 보안수준에는 크게 미치지 못할 수 있는 문제점이 있다.

지금까지의 내용을 정리하면, 오픈뱅킹 점검항목은 전산시설 보안, 비상대응훈련 실시, 정보보호위원회 운영, 내부통신망와 업무망 분리, 정보시스템 접근기록 보관, 전산자료 백업 및 소산 등 관리적·기술적 보호기준이 누락되어 있거나 상세하지 못한 한계가 있고, 전자금융거래법규에 근거하여 금융감독당국의 정기적인 감독을 받는 금융회사에 대비하여 오픈뱅킹 이용기관은 법적 근거가 없으므로 보안수준을 보장하기 어려운 문제점이 있다.

4.1.2 오픈뱅킹 이용자보호 리스크

오픈뱅킹 이용기관은 오픈뱅킹에 관한 계약을 체결하면서 오픈뱅킹 사고에 대비하여 출금이체 일간한도를 사용자별 일간한도(1천만원)내로 설정하고, 일간한도의 200%를 보증보험에 가입하도록 하고 있다[18]. 그러나 오픈뱅킹 공동업무이용약관 제20조(보증보험증권 발급 및 관리)에서 보증보험증권의 피보험자를 금융결제원으로 설정하고 있으므로 이용기관의 보증보험은 이용기관의 횡령, 파산 등에 대비한 금융결제원 또는 오픈뱅킹 제공기관(은행)의 피해보상을 위한 보험으로 볼 수 있다. 즉, 오픈뱅킹 이용기관의 모바일앱 해킹으로 인한 정보유출 또는 금융사고로 인한 고객 피해에 대해서는 이용기관이 별도의 배상보험에 가입하거나 준비금을 마련해야 한다. 이에 반해 전자금융거래법 적용대상인 금융회사 또는 전자금융업자는 전자금융사고로 인한 이용자 손해배상을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하도록 의무화 하고 있다(전자금융거래법 제9조, 전자금융감독규정 제5조).

이용자 피해보상과 관련하여 오픈뱅킹 공동업무이용약관 제41조(사용자 보호)에 따라 이용기관은 민원 및 사고발생시 피해금액을 이용고객에게 선지급하는 등 우선적 피해구제 방법을 수립하도록 하고, 제45조(손해배상 및 면책)에서 이용기관이 전송한 내용이 착오·오용 및 위조·변조·기타의 사고에 의한 것이라도 금융결제원과 은행은 해당 처리결과에 대하여 책임을 지지 않고 이용기관이 책임을 지도록 되어 있다[18]. 그러나 오픈뱅킹에 참여하는 핀테크기업의 대부분은 중소형 회사이기 때문에 은행과 같은 전자금융사고 신고접수 및 보상처리를 담당할 인력과 시스템이 미흡할 가능성이 매우 높다. 아울러 오픈뱅킹 특성상 오픈뱅킹 이용고객은 이용기관(핀테크기업)과 제공기관(은행), 금융결제원간의 역할과 책임범위를 이해하기 어렵기 때문에 오픈뱅킹으로 인한 피해발생시 이용기관(핀테크기업) 보다는 은행으로 신고 및 피해보상을 요구할 가능성이 높지만, 은행은 오픈뱅킹 약관에 따라 이용기관에게 사고 책임 및 피해보상 처리를 전가할 수 있어 피해보상이 쉽지 않을 우려가 있다.

지금까지의 내용을 정리하면, 오픈뱅킹 이용기관은 해킹 등 전자금융사고 발생시 피해고객에 대한 보상을 위한 준비금 적립 또는 보험 가입의무가 없고, 전자금융사고 발생시 오픈뱅킹 피해고객에 대한 안내 및 대응체계가 미흡하여 신속한 피해보상이 제공되지 않을 문제점이 있다.

4.1.3 오픈뱅킹 공동업무시스템 보안리스크

금융결제원이 운영하는 오픈뱅킹 공동업무시스템이 전산오류, 디도스공격, 해킹 등으로 인하여 시스템 가동중단, 불법적인 자금이체 및 대량의 금융정보 유출과 같은 사고가 발생한다면 동 시스템에 연결된 금융회사와 수많은 고객에게 막대한 피해는 물론이고 국가신용도에도 커다란 손실을 초래할 수 있다. 그러나 현행 전자금융거래법에서는 금융결제원이 운영중인 오픈뱅킹 공동업무시스템에 대해서는 대부분의 규제가 제외되어 있다. 즉 인터넷뱅킹, 모바일뱅킹 등 전자금융서비스를 제공하는 금융회사에게 준수의무를 부과하고 있는 정보보호인력 및 최고정보보호책임자 지정, 정보보호 정책 수립 및 보안교육 등 관리적인 보호대책과 전자금융거래를 처리하는 단말기에 대한 접근통제, 전산자료의 기록보관·백업·소산, 해킹방지를 위한 정보보호시스템 설치·운영 및 패치적용, 정기적인 취약점 분석·평가 및 보고 등 기술적인 보호대책과 금융감독당국의 감독 및 검사에 이르기까지 폭넓고 세세하게 명시되어 있는 안전성 규제들이 오픈뱅킹 공동업무시스템에 대해서는 적용되지 않는다.

전자금융거래법상 금융결제원이 운영하는 오픈뱅킹 공동업무시스템은 결제중계시스템에 해당될 수 있으나(법 제2조 제5호), 시행령 제5조 제1항 제1호에서 결제중계시스템에 대해서는 전자금융거래법 적용을 예외하고 있다. 그러나 금융결제원의 결제중계시스템과 유사하게 금융권 공동의 시스템을 운영하고 있는 한국거래소나 한국예탁결제원은 금융회사에 포함(법 제2조 및 동법 시행령 제3조 제7호 및 제8호)되어 있으므로 전자금융거래법의 안전성 대책을 모두 준수하여야 한다.

지금까지의 내용을 정리하면, 금융결제원이 운영하고 있는 오픈뱅킹 공동업무시스템에 대해서는 전자금융거래법상의 기술적 관리적 보호대책 등 안전성 규제가 적용되지 않고, 금융감독당국의 감독을 받고 있지 않으므로 해당 시스템에 대한 보안수준을 보장하기 어렵다. 따라서 보안취약점을 이용한 해킹사고가 발생될 경우 대량의 고객정보 유출 및 전자금융사고가 발생될 수 있는 문제점이 있다.

4.2 규제 개선 방안

4.2.1 오픈뱅킹 이용기관 규제

전자금융거래법 제2조(정의)에 따르면 오픈뱅킹 서비스는 전자금융거래에 해당된다. 그러나 오픈뱅킹 이용기관으로 참여하는 핀테크기업은 사용자 동의를 거쳐 금융거래 내역조회 및 전자자금이체와 같은 전자금융서비스를 제공함에도 전자금융거래법의 규제대상에 해당되지 않는다. 그 이유는 3장의 오픈뱅킹 구성에 대해 살펴보았듯이 이용기관은 고객과의 관계에서는 전자금융서비스 제공자로 볼 수 있지만, 은행(오픈뱅킹 제공기관)과의 관계에서는 은행이 제공하는 전자금융서비스 이용자이며 전자자금이체업자로 등록하고 있지 않기 때문이다. 그러나 중소형 핀테크기업을 금융회사 또는 전자금융업자와 동일한 수준의 규제를 적용하게 되면 당장에는 오픈뱅킹 활성화가 저해될 수 있고, 오픈뱅킹 이용기관의 역할(은행이 제공한 전자금융서비스를 고객에게 제공)에 비해 과도한 규제가 될 수 있으므로, 금융회사를 통해 간접적인 관리감독이 가능한 전자금융보조업자로 포함시키는 방안이 적절할 것으로 판단된다.

전자금융거래법상 전자금융보조업자란 금융회사 또는 전자금융업자를 위하여 전자금융거래를 보조하거나 그 일부를 대행하는 업무를 행하는 자(법 제2조 제5호)를 말하며, 금융회사 또는 전자금융업자는 전자금융보조업자에 대하여 연 1회 이상 취약점 분석·평가를 실시(법 제21조의3 제1항 제4호, 시행령 제11조의4 제1호)하고, 주기적인 보안점검 및 연 1회 이상 재무건전성 평가 및 서비스 품질수준 평가를 진행하여 그 결과를 금융감독원장에게 보고(전자금융감독규정 제60조)하여야 한다. 또한 전자금융거래와 관련하여 전자금융보조업자의 고의나 과실은 금융회사의 고의나 과실로 보며, 전자금융보조업자의 과실로 인하여 발생한 손해에 대하여 이용자에게 그 손해를 배상한 경우에는 전자금융보조업자에게 구상할 수 있도록 하고 있다(법 제11조). 오랜 기간 전자금융서비스를 제공해온 은행에 비하여 중소형 핀테크기업은 피해고객에 대한 안내 및 손해배상 등의 처리가 원활하지 않을 수 있으므로, EU의 규제사례와 같이 오픈뱅킹 사고 발생시 은행에서 피해고객 상담 및 배상 등을 우선 처리하고 핀테크기업에게 사후 구상을 요구하는 것이 오픈뱅킹 이용고객 보호를 위한 방안이다. 따라서 오픈뱅킹 이

용기관에 대한 안전성 점검 및 이용자 보호수준을 강화하기 위하여 전자금융감독규정 제3조(전자금융보조업자의 범위)를 다음과 같이 개정하여 오픈뱅킹 이용기관으로 참여하는 핀테크기업을 전자금융보조업자로 포함시키는 방안을 제시한다.

> 제3조(전자금융보조업자의 범위)
> 1. 정보처리시스템을 통하여 「여신전문금융업법」상 신용카드업자의 신용카드 승인 및 결제 그 밖의 자금정산에 관한 업무를 지원하는 사업자
> 2.부터 4.까지 (생략)
> 5. (신설) 금융회사등에서 제공하는 고객정보 및 지급결제 서비스를 이용하여 이용자에게 전자금융서비스를 제공하는 사업자

오픈뱅킹 이용기관을 전자금융보조업자로 포함시키는 경우 금융회사는 오픈뱅킹 이용기관에 대한 취약성 분석·평가를 실시할 때, 4.1.1에서 명시한 오픈뱅킹 점검항목에서 누락된 안전성 확보대책 13개 항목을 포함할 수 있도록 전자금융감독규정시행세칙 또는 관련 가이드라인 등에 반영할 필요가 있다. 또한 다수의 금융회사들은 CD-VAN 등 부가통신사업자와 같은 전자금융보조업자에 대한 점검을 금융보안원에 위탁하여 수행하고 있다. 따라서 이러한 금융회사 공동의 전자금융보조업자에 대한 점검을 금융회사별로 각각 수행하지 않고 하나의 외부평가기관에게 위탁하고 평가방법 및 보고절차 등을 명문화함으로써 전자금융보조업자에 대한 보안점검 수준을 강화하고 업무의 효율성을 높여나갈 필요가 있다.

4.2.2 오픈뱅킹 공동업무시스템 규제

오픈뱅킹 제공기관(은행)의 장애는 한 은행의 업무처리에만 영향을 주지만 금융결제원에서 운영하는 오픈뱅킹 공동업무시스템의 장애 또는 사고는 오픈뱅킹 서비스 전체가 중단될 수 있는 큰 위험요소이다. 그럼에도 불구하고 현재의 전자금융거래법 체계에서는 금융결제원에 대하여 어떠한 전자금융거래의 안전성 대책 및 관리감독에 관한 규제가 없는 상황이므로 이에 대한 개선이 필요하다. 또한 오픈뱅킹 공동업무시스템의 중요도를 고려했을때 금융회사와 동일한 수준의 기술적 관리적 보호대책 준수의무가 부과되고 금융감독당국의 정기적인 감독·검사를 받을 필요가 있다. 따라서 다음과 같이 전자금융거래법 시행령 제2조에 금융결제원을 추가하는 항목을 신설하고, 전자금융거래법 적용 예외 조항인 시행령 제5조 제1호를 삭제함으로써 오픈뱅킹 공동업무시스템을 운영하는 금융결제원을 전자금융거래법 규제에 포함시켜 오픈뱅킹의 안전성을 확보 유지할 필요가 있다.

> 제2조(금융회사의 범위) 「전자금융거래법」(이하 "법"이라 한다) 제2조제3호마목에서 "대통령령이 정하는 자"라 함은 다음 각 호의 어느 하나에 해당하는 자를 말한다.
> 1.부터 18.까지(생략)
> 19. (신설) 사단법인 금융결제원
>
> 제5조(적용범위의 예외) ①법 제3조제1항 단서에서 "대통령령이 정하는 경우"라 함은 다음 각 호의 어느 하나에 해당하는 경우를 말한다. <개정 2013. 11. 22.>
> 1. (삭제) 법 제2조제6호에 따른 결제중계시스템을 이용하는 전자금융거래

4.2.3 오픈뱅킹 규제 개선의 기대효과

오픈뱅킹 이용기관으로 참여하는 핀테크기업은 전자금융거래법상 전자금융보조업자로 포함됨에 따라 은행이 매년 1회 이상 전자금융기반시설에 대한 취약점 분석·평가시 오픈뱅킹 이용기관의 정보처리시스템에 대해서도 점검을 실시하여야 한다. 이는 은행이 전자금융기반시설 취약점 분석·평가시 정보기술부문과 연계된 전자금융보조업자의 정보처리시스템 등에 관한 사항을 포함(법 제21조의3 및 시행령 제11조의4)하여야 하기 때문이다. 또한 취약점 분석·평가시 정보기술부문의 조직, 시설 및 내부통제에 관한 사항, 정보기술부문의 전자적 장치 및 접근매체에 관한 사항, 전자금융거래의 유지를 위한 침해사고 대응조치에 관한 사항 등 안정성 확보에 대한 사항이 폭넓게 적용된다. 아울러 전자금융감독규정시행세칙 별표3에서도 전자금융기반시설의 취약점 분석·평가시 관리적 보안(정보보호정책, 정보보호조직 및 인력, 내부통제, 사고관

리 등), 물리적 보안(전산설비 보안, 전산센터 보안), 기술적 보안(인터넷 전자금융 보안, 접근통제, 전산자료 보안, 서버보안, 데이터베이스 보안, 웹서비스 보안, 단말기 보안, 네트워크 보안, 정보보호시스템 보안)으로 구분된 상세한 항목이 명시되어 있어 오픈뱅킹 보안점검 항목에서 누락된 부분을 모두 충족시켜 줄 수 있다. 그 밖에도 핀테크기업은 전자금융보조업자에게 부과되어 있는 안전성 확보 의무(법 제21조), 전자금융거래기록 생성·보존 및 파기(법 제22조), 금융회사와 연결시 전용회선 또는 전용회선과 동등한 보안수준을 갖춘 가상회선 사용, 금융회사를 통한 연 1회 이상 재무건전성 및 서비스 품질 평가(규정 제60조), 금융감독원에 자료제출 의무(규정 제61조) 등을 준수하여야 한다.

오픈뱅킹 공동업무시스템을 운영하는 금융결제원이 금융회사로 포함되는 경우 전자금융거래법에서 정한 전자금융거래의 안전성과 신뢰성 확보에 필요한 관리적 기술적 보호조치를 모두 준수해야 하고, 금융당국의 정기적인 감독·검사를 받게 됨에 따라, 오픈뱅킹 시스템의 안정성이 지속적으로 향상되는 효과가 발생할 것이다.

- (오픈뱅킹 이용기관) 금융회사를 통해 연 1회 이상 정기적인 취약점 분석·평가를 받음
- (오픈뱅킹 이용기관) 취약점 분석·평가 항목 및 평가결과에 대하여 금융감독당국의 관리통제가 가능해짐
- (오픈뱅킹 이용기관) 전자금융거래의 내용을 추적·검색하기 위한 거래기록 생성 및 5년범위 안에서 보존의무가 부과됨
- (금융회사) 오픈뱅킹 이용기관의 고의나 과실로 인해 발생한 고객피해에 대하여 손해를 배상하고 이용기관에게 구상 가능
- (오픈뱅킹 이용고객) 사고신고 및 피해보상에 대한 절차를 거래하던 은행으로 일원화하고 은행의 전자금융사고 피해구제 절차를 적용 받음
- (오픈뱅킹 공동업무시스템) 금융회사 수준의 기술적 관리적 보호대책 준수의무가 부과되고 금융감독당국의 감독·검사를 받게 됨에 따라 보안성 및 안정성에 대한 신뢰성이 높아짐

5. 결론

정부는 금융혁신을 촉진하기 위하여 오픈뱅킹을 본격 시행하였고, 향후에도 오픈뱅킹 참가기관을 상호금융, 저축은행, 우체국 등으로 확대하고 제공서비스의 종류를 다양화 하는 등 오픈뱅킹 고도화를 지속적으로 추진해 나갈 예정이다[17]. 앞으로도 오픈뱅킹이 확대 및 발전해 나가기 위해서는 오픈뱅킹 시스템이 안정적으로 운영되어야 함은 물론, 사고 발생시에는 신속한 안내 및 피해보상체계가 마련되어야 할 것이다. 따라서 본 연구에서는 오픈뱅킹의 활성화를 저해하지 않으면서도 최소한의 안정성을 확보할 수 있는 규제 방안을 제시해 보고자 하였다.

우리나라 오픈뱅킹은 영국, 일본 등 외국과 달리 2016년도부터 금융결제원에서 운영해온 금융권 공동 API 방식의 오픈플랫폼을 활용하였기 때문에 보다 신속하게 오픈뱅킹을 시행할 수 있었다. 따라서 이용기관에 대한 이체한도 제한 및 보증보험 가입, 오픈 API 및 인증방식에 대해 시행착오를 거치면서 운영해온 경험이 있기 때문에 단기적으로는 큰 사고가 발생하지 않을 수 있다. 그러나 외국의 오픈뱅킹 규제 사례에서 알 수 있듯이 오픈뱅킹에 참여하는 핀테크 기업에 대하여 기존 전자금융법규에 근거하여 안전성 규제를 부과하고 정부 또는 금융감독당국의 승인 및 감독을 시행함으로써 금융회사와 동일한 수준의 오픈뱅킹 안전성을 갖추도록 하고 있으므로 국내에도 오픈뱅킹 참여기관에 대한 규제 개선이 필요하다. 따라서 본 연구에서는 오픈뱅킹에 참여하는 핀테크기업을 전자금융거래법상의 전자금융보조업자로 포함하여 은행의 관리감독 및 금융감독당국의 간접적인 통제가 가능하도록 하고, 오픈뱅킹의 핵심 인프라를 운영중인 금융결제원에 대해서는 그 중요도 및 규모를 고려하여 금융회사와 동일한 수준의 안전성 대책과 금융감독당국의 직접적인 감독·검사를 받을 수 있는 규제 방안을 제시하였다.

오픈뱅킹에 관한 규제 방안을 연구하면서 오픈뱅킹을 선도하고 있는 외국의 규제에 대해 자료를 수집하여 분석해 보았으나, 내용이 매우 방대하고 국가마다 금융업법 체계 및 환경이 달라서 안정성 규제를 비교하는데 어려움이 있었다. 향후 핀테크기업에게 은행

업을 허용하는 등 새로운 금융혁신을 추진중인 미국과 호주 등 다양한 국가의 전자금융 규제와 안전성 확보 대책에 대해서도 분석해본다면 더 의미있는 시사점과 오픈뱅킹 규제 방안을 제안해 볼 수 있을 것으로 예상한다.

참고문헌

[1] 금융위원회, '개방형 금융결제망 구축, 핀테크 성장을 촉진하고 생활금융을 혁신하겠습니다. - 핀테크 및 금융플랫폼 활성화를 위한 금융결제 인프라 혁신방안', 보도자료 2019.2.26.

[2] 이정민, 김세중, 박해리, '오픈뱅킹의 개념과 법적 쟁점', 서울대학교 금융법센터 BFL 제99호, pp. 16-27, 2020.1.

[3] 김규림, 조민주, 최연경, '오픈뱅킹, 금융산업 지형 변화의 서막', Issue Monitor 제108호, pp. 7, 2019.3.

[4] 서정호, '오픈API 활성화를 통한 국내 은행산업의 혁신전략', 한국금융연구원 KIF VIP 리포트 2018권 8호, pp. 53, 2018.12.

[5] 서정호, 김자봉, '최근 핀테크 지급결제시장 참여 확대와 시사점', KIF VIP리포트, pp. 71-75, 2019.3.

[6] 최대현, 김인석, "안전한 오픈뱅킹 구축을 위한 정책 및 B2B2C 모델에 관한 연구", 정보보호학회지, Vol. 29, No.6, pp 1271-1283, 2019.12.

[7] 송미정, 김인석, "유럽 PSD2 시행에 따른 금융분야 마이데이터 정책의 개인정보보호에 관한 방안 연구", 정보보호학회지, Vol. 29, No.5, pp. 1205-1219, 2019.10.

[8] European Central Bank, Single Euro Payments Area (SEPA), https://www.ecb.europa.eu/paym/integration/retail/sepa/html/index.en.htm

[9] European Commission, "Payment services (PSD 2) - Directive (EU) 2015/2366", https://eur-lex.europa.eu/eli/dir/2015/2366/oj

[10] 김현부, 김인석 "개정된 유럽연합 지급결제서비스지침의 보안위험에 대한 제도적인 대응과 관련 국내 전자금융 규제와의 비교 연구", 한국전자거래학회지, 24권 4호, pp. 79-107, 2020.1.

[11] Open Banking Implementation Entity, "Open Banking Standards 3.0", https://standards.openbanking.org.uk/

[12] Financial Conduct Authority, "Payment Services Regulations 2017", https://www.fca.org.uk/firms/payment-services-regulations-e-money-regulations

[13] 자금결제에 관한 법률(資金決済に關する法律, Payment Services Act), http://www.japaneselawtranslation. go.jp/law/detail/?id=2319&vm=&re=

[14] 은행법(銀行法, Banking Act), http://www.japaneselawtranslation.go.jp/law/detail/?vm=04&re=02&lvm=02&id=3435

[15] 금융결제원 오픈뱅킹 공동업무, http://open-platform.or.kr/main

[16] 금융위원회, '오픈뱅킹 전면시행 이후 동향', 보도자료 2020.1.10.

[17] 금융위원회, '은행과 핀테크 기업 모두가 참여하는 오픈뱅킹 서비스가 전면 시행됩니다.', 보도자료 2019.12.18.

[18] 금융결제원, '오픈뱅킹 공동업무이용약관', 2020.1.15.

[19] 금융보안원, '오픈뱅킹 관련 보안점검 주요내용', 2019.6.

[20] 금융위원회, '오픈뱅킹 진행 현황 및 향후 일정', 보도자료 2019.6.20.

[21] 금융위원회, '신용정보의 이용 및 보호에 관한 법률', 법제처 법령정보센터, 제16188호, 2018.12.31.

[22] 금융위원회, '전자금융거래법', 법제처 법령정보센터, 제14828호, 2017. 4. 18.

〔저자소개〕

권 남 훈 (Nam-hoon Kwon)
1999년 2월
고려대학교 정보공학과 학사
2018년 9월 ~ 현재
고려대학교 정보보호대학원 금융보안학과 석사과정
email : knh002@naver.com

김 인 동 (Gil-dong Hong)
1973년 2월
홍익대학교 전자계산학과 학사
2003년 2월
동국대학교 정보보호학과 석사
2008년 2월
고려대학교 정보경영공학과 박사
2009년 ~ 현재
고려대학교 정보보호대학원 교수
email : iskim11@korea.ac.kr