韓國IT서비스學會誌
第20卷 第6號
2021年 12月, pp.63-81

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2021.20.6.063

정보보호 관점에서의 오픈뱅킹 수용도에 대한 영향요인

고정현* · 이원부**

Factors to Affect Acceptance of Open Banking from Information Security Perspectives

Jeunghyeun Go* · Woonboo Lee**

■ Abstract ■

Joint financial network of Korea Financial Telecommunications and Clearings Institute, which is an essential facility with a natural monopoly, maintained its closedness as monopoly/public utility model, but it has evolved in the form of open banking in order to obtain domestic fintech competitiveness in the rapidly changing digital financial ecosystem such as the acceleration of Big Blur. In accordance with digital transformation strategy of financial institutions, various ICT companies are actively participating in the financial industries, which has been exclusive to banks, through the link technology called Open API. For this reason, there has been a significant change in the financial service supply chain in which ICT companies participate as users. The level of security in the financial service supply chain is determined based on the weakest part of the individual components according to the law of minimum. In addition, there is a perceived risk of personal information and financial information leakage among the main factors that affect users' intention to accept services, and appropriate protective measures against perceived security risks can be a catalyst, which increases the acceptance of open banking. Therefore, this is a study on factors affecting the introduction of open banking to achieve financial innovation by developing an open banking security control model for financial institutions, as a protective measures to user organizations, from the perspectives of cyber financial security and customer information protection, respectively, and surveying financial security experts. It is expected, from this study, that effective information protection measures will be derived to protect the rights and interests of financial customers and will help promote open banking.

Keyword : Open Banking, Security Risks, Cyber Financial Security, Customer Information Protection, Security Control Model

Submitted : November 15, 2021 1st Revision : December 10, 2021 Accepted : December 10, 2021

* 동국대학교 핀테크블록체인학과 박사과정 재학 중
** 동국대학교 핀테크블록체인학과 교수, 교신저자

1. 서 론

자연 독점적 성격을 지닌 필수설비인 금융공동망은 독점/공익기업형 모델로 폐쇄성 유지하였으나 빅블러(BigBlur)의 가속화 등 급변하는 디지털 금융 생태계 속에서 국내 핀테크 경쟁력 확보를 위해 오픈뱅킹이라는 모습으로 개방되고 있다. 또한 금융사의 디지털 트랜스포메이션 전략 추구에 따라 오픈API라는 연계기술을 통해 다양한 ICT기업과의 합종연횡이 본격화 되고 있다. 이러한 이유로 핀테크 등의 ICT기업이 이용기관으로서 참여하는 금융 서비스 공급망 측면의 대변화가 발생 하였다. 금융 서비스 공급망 보안 수준은 최소량의 법칙에 따라 개별 구성요소 중 가장 취약한 부분을 기준으로 결정된다. 따라서 금융사는 제공기관으로 금융 서비스 보호를 위해 이용기관에 대한 다양한 측면의 평가를 포함한 보호대책의 마련이 필요하다.

이에 오픈뱅킹 서비스에 대한 보안위험과 이를 보완 할 수 있는 보호대책을 도출하고 이러한 보호대책이 오픈뱅킹 신뢰도 향상을 통해 서비스 수용도에 미치는 영향을 파악하고자 한다. 오픈뱅킹 서비스 수용도에 영향을 미치는 보호대책을 규명함으로써 금융 소비자의 수용도를 높이고 안전한 활용을 확대할 수 있는 금융회사별 전략 개발에 유용한 시사점을 제공한다는 점에서 그 기여점을 찾을 수 있다.

본 연구의 목적은 첫째, 오픈뱅킹 정보보호 위협별 도출된 대응 방안과 오픈뱅킹 서비스 수용의도에 관한 영향도를 파악하고, 둘째, 오픈뱅킹 수용도에 영향을 미치는 조절효과를 확인하며, 마지막으로, 금융기관 등 오픈뱅킹 서비스 제공자 측면에서 관련 서비스 확대를 위해 어떠한 정보보호 대책에 집중할 필요가 있는지 탐색하는 것이다.

개방형 디지털 금융 인프라의 시작인 오픈뱅킹서비스에 대한 정보보호대책 수립으로 오픈뱅킹 도입에 따른 금융서비스 제공 구조 및 기능적 역할의 변화로 발생되는 정보보호 리스크를 분석하고 리스크 요인별 제거방안을 도출하여 종합적 금융보안 보호대책을 수립하고자 한다.

이를 위해 오픈뱅킹 도입에 따른 금융 서비스 변화 요인과 이로 인한 정보보호 및 정보보안 리스크, 이를 위한 금융보안 보호대책과 적정성 평가방법을 대상으로 전략을 도출한다. 이후 관련 분야인 정보보호 전문가를 대상으로 설문을 실시하여 제안 전략 중 중요성을 선별 검증토록 한다.

2. 이론적 배경

2.1 오픈뱅킹에 대한 선행 연구

오픈뱅킹은 고객의 사전 동의下 고객 금융데이터를 은행 제3자에게 접근 허용하는 것을 통칭하며, 금융결제망을 폐쇄형에서 개방형으로 단계적 전환하는 계기가 되었다(금융위원회, 2019b). 기술적으로 핀테크 기업 및 은행들이 표준 방식(API)으로 모든 은행의 자금이체·조회 기능을 자체 제공할 수 있는 시스템을 의미한다.

국내의 경우 좁은 의미의 오픈뱅킹은 지급결제 중심의 공동 Open API 시스템 확대를 의미하며 향후, 오픈뱅킹 참여기관이 다양화되고 데이터 활용까지 포함될 경우 마이페이먼트와 마이데이터 연계로 오픈뱅킹의 역할이 확대 가능하다. 데이터 제공 부문에 있어서 오픈뱅킹에 새로 참여하는 기관는 일정 수준의 데이터를 제공하며, 핀테크 기업도 오픈뱅킹 망 운영비용을 일부 분담하며, 오픈뱅킹 서비스의 안전성 확보 측면에서 이상거래탐지시스템(FDS)를 고도화하며 참여기관을 대상으로 외부기관을 통한 사전 보안점검을 의무화하고 사고이력 등에 따라 사후 보안관리를 주기적으로 실시한다. 또한 이용기관 보증보험 가입을 통해 금융사고 발생시 신속하게 소비자 피해를 보상하는 체계를 구축하였다.

해외 주요 선진국들은 핀테크 활성화 및 금융혁신의 중요성을 인식하고 결제 및 데이터 인프라의 개방화를 추진하였다. EU의 경우 PSD2(Payment Service Directive 2) 도입을 통해 PISP와 AISP 등이 결제시스템과 계좌정보 등에 접근할 수 있도록 오픈API제공을 의무화 하였다. 영국은 지난해 초 고

객 동의하에 은행이 계좌정보를 API를 통해 제3자에게 제공하도록 하는 오픈뱅킹 제도를 도입해 금융권의 경쟁 및 혁신을 촉진하였다. 호주의 경쟁소비자위원회는 은행정보에 관한 소비자정보권 및 서비스 경쟁 활성화를 위해 오픈뱅킹을 추진하였다. 일본은 은행법 개정을 통해 '전자결제 등 대행업'을 도입하여 대행업자(AISP, PISP) 등록을 의무화하고, 금융회사에게 공개 API를 통한 정보제공 노력 의무를 부과하여 90여개 은행이 오픈 API를 구축하였다.

2.2 오픈뱅킹 정보보호 위협 및 대응방안

오픈뱅킹은 서비스 구조상 금융기관과 고객 간 정보이동에 제3자인 핀테크 업체 등의 이용기관이 추가되어 정보보호 측면의 여러 위협이 예상되며 이에 대한 대응이 필요하다.

오픈뱅킹 주요 정보보호 위협은 이용자 단말기의 악성코드 감염, 변조 애플리케이션 유통, 서비스 애플리케이션 취약점을 통한 악의적 행위시도, 공격자의 이메일 피싱, 가짜 사이트, 가짜 애플리케이션 개발 및 배포를 통해 이용기관으로 가장하는 등의 이용자영역 위협과 공격자의 계좌 소유주 사칭을 통한 이용기관 등록, 오픈API 관련 정보처리시스템의 악성코드 감염, API 데이터를 제3자에게 제공하는 이용기관에 대한 관리 미흡, 이용기관 시스템의 침해로 오픈API 접근키 대규모 도난 발생, 오픈API 이용 애플리케이션 침해 및 오류로 비정상적 API를 요청하는 등의 이용기관영역 위협으로 구분된다.

이러한 정보보호 위협 대응방안으로 이용자 단말기 악성코드 감염 방지대응, 이용자 단말기 내 오픈API를 통해 수집한 개인신용정보 유출 및 도용 방지, 변조 애플리케이션 유통 및 피싱사이트 방지 등이 권고되며, 이는 보안성심의, 이상금융거래탐지, 데이터보안관리, 개발보안관리, 위수탁보안관리, 접근통제관리 등으로 분류할 수 있다. 이용기관의 이러한 정보보호 대책 수립 적합성은 제휴업체 적정성 평가(제휴 허용 업종, 재무건전성, 리스크 관리 등), 핀테크 어플리케이션(앱/웹) 취약점 점검, 이용기관 관리, 물리, 기술 영역의 보안점검과 개발·테스트 단계의 보안성심의, 운영 단계의 정기적 보안 실태 점검을 통해 검증한다. 오픈뱅킹 이상금융거래탐지는 핀테크 등 이용기관에서 오픈뱅킹 API(금융결제원)를 이용해 자금 이체 요청을 하는 경우와 금융결제원 FDS에서 주민등록번호 등 고객번호를 기반으로 특정 시간동안 금액 및 건수가 많은 경우에 대해 은행 등 제공기관에 전달하는 방식으로 구분된다. 오픈뱅킹의 이상금융거래를 효과적으로 탐지, 대응할 수 있는 방법으로 금융결제원 이상금융거래탐지 강화, 이용기관 이상금융거래탐지 강화, 제공기관 이상금융거래탐지 강화 등이 제시된다.

〈표 1〉 오픈뱅킹 정보보호 위협 대응

구분	항목
보안성 심의	• 이용기관 사용자 대상 사회공학적 공격에 대책 마련 • 악의적 행위자(이용기관 내부직원 또는 외부자) 오픈API 관련 정보자산 접근, 변조, 유출 등 방지 • 이용기관 정보보호 관리체계 수립 검증
이상금융거래탐지	• 이용자의 사기 피해 예방, 탐지, 대응 • 중요정보 유출 예방, 탐지, 대응 • 이상거래 등 보안사고에 대한 대응
데이터 보안관리	• 오픈API를 통해 수집한 개인·신용정보 유출 및 도용 방지 • 오픈API 관련 정보자산에 대한 보호
개발 보안관리	• 이용자 단말기 악성코드 감염 방지 • 변조 앱 유통 및 피싱사이트 차단 • 오픈API 이용 앱 취약점 방지 위한 시큐어 코딩 실시
위수탁 보안관리	• 오픈API를 통해 수집한 개인신용정보 제3자 제공, 위탁 관련 보호 대책 마련
접근통제 관리	• 오픈API 접근키 및 이용자 보호 대책 • 도용한 개인정보 악용 비인가 서비스 이용 방지 • 비정상적 오픈API 접근 방지

2.3 보호동기이론(PMT)

Rogers(1975)는 보호동기이론(Protection Motivation Theory)을 "공포를 유발하는 요인(Fear Appeal)에 대한 개인의 태도와 행동의 변화를 설명하기 위한 이론이라 하였으며 위협의 발생 가능성에 대한 믿음인

지각된 취약성(Perceived Vulnerability)과 해당 위협의 피해 크기를 나타내는 지각된 심각성(Perceived Severity), 위협 대응 행동의 효과성에 관한 믿음인 반응 효능감(Response Effectiveness)이 개인의 보호의도에 영향을 미치는 요인으로 확인하였다.

Bandura(1977)는 초기 보호동기이론에 자산의 위협 대응 능력에 대한 믿음인 자기효능감(Self-efficacy)과 대응 행동을 방해하는 요인인 반응비용(Response Cost)을 추가한 수정된 보호동기이론을 제시하였다. 수정된 보호동기이론은 지각된 취약성과 지각된 심각성으로 구성된 위협평가(Threat Appraisal)와 반응 효능감과 자기 효능감, 반응비용으로 구성된 대처평가(Coping Appraisal)를 통해 발생한 보호 동기가 보호 행동으로 이어진다고 하였다

보호동기이론을 통해 정보기술과 정보보호분야에서 위협에 대한 보호 행동을 설명하기 위한 연구가 진행되었으며, Chenoweth et al.(2007)은 보호동기이론의 위협평가와 대처평가는 안티스파이웨어 등의 보안 제품 채택 여부 결정에 영향을 주는 중요 요인이라 했으며, 기업 정보보호 담당자는 위협평가와 대처평가 결과를 기준으로 보안대책 적용 여부를 결정한다고 하였다. Woon et al.(2005)은 지각된 심각성, 반응 효능감, 반응비용이 안티스파이웨어 등의 보안 제품 사용의도에 유의미한 영향을 미친다고 하였다. Johnston et al.(2010)은 공포요인(Fear Appeal)은 이용자가 요구되는 보안 행위를 준수하도록 하는데 영향을 미치지만, 반응 효능감과 자기 효능감, 위협에 대한 지각된 심각성 등은 개인별 차이가 있다고 하였다. 김상훈 외(2015)은 정보보안기술 사용에 대한 규범수준, 기술의 유용성 인식수준, 자기 효능감이 정보보안기술 사용 의지에 유의한 영향을 미치며 보안위협의 발생가능성, 즉 지각된 취약성의 수준이 높을수록 정보보안기술에 대한 인식도가 향상된다고 하였다.

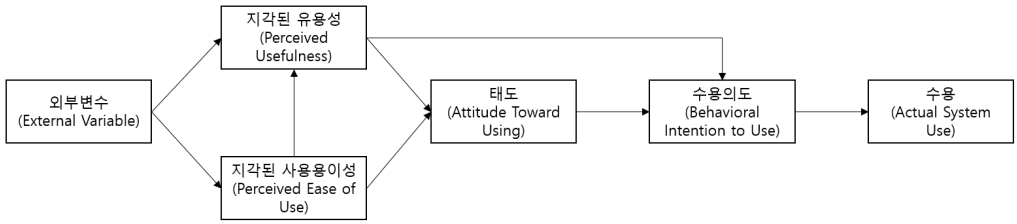
2.4 기술수용모델(TAM)

Davis(1989)는 기술수용모델(Technology Acceptance Model)은 “조직에서 업무 성과향상 등을 위한 정보기술의 수용에 영향을 미치는 요인을 연구하기 위한 연구모델”이라 하였으며, 정보기술 이용도 영향요인으로 정보기술을 사용함으로써 자신의 업무성과가 개선될 것이라는 주관적 신념의 정도인 지각된 유용성(Perceived Usefulness)과 특정 정보시스템을 신체적 혹은 정신적으로 큰 노력 없이 이용할 수 있다고 믿는 신념의 정도인 지각된 사용용이성(Perceived Ease of Use)을 합리적 행동이론(Theory of Reasoned Action)의 관점에서 설명하였다. 합리적 행동은 인간의 태도에 영향을 미치는 요인들을 ‘신념’과 ‘평가’라는 추상적인 개념을 사용한 것과 외부요인에 대한 고려가 없다는 점이 이론적 단점으로 지적되었다.

〈표 2〉 보호동기이론(PMT) 관련 연구 요약

관련 연구	연구 내용
김상훈 외 (2015)	규범 수준, 기술의 유용성 인식수준이 높고, 정보보안 기술 사용에 대한 자기 효능감이 클수록 정보보안기술 사용 의지가 강해짐
Chenoweth et al.(2007)	보호동기이론의 위협평가와 대처평가는 안티스파이웨어 등의 보안 제품 채택 여부 결정에 영향을 주는 중요 요인임
Johnston et al. (2010)	공포요인(Fear Appeal)은 이용자가 요구되는 보안 행위를 준수하도록 하는데 영향을 미치지만, 반응 효능감과 자기 효능감, 위협에 대한 지각된 심각성 등은 개인별 차이가 있음
Woon et al. (2005)	지각된 심각성, 반응 효능감, 반응비용이 안티스파이웨어 등의 보안 제품 사용의도에 유의미한 영향을 미침

기술수용모델에서는 외부 변수가 지각된 사용용이성과 지각된 유용성에 영향을 미치고, 지각된 사용용이성과 지각된 유용성으로 형성된 태도가 새로운 정보기술에 대한 사용자의 태도에 영향을 미쳐, 수용의도를 매개하여 실제 수용에 영향을 주는 것으로 설명하고 있다. TAM은 지각된 유용성, 지각된 사용용이성, 수용의도와 실제 사용만을 모델에 반영하고, 실제 외부요인들을 구체화하지 않음에 따라, 이후의 연구들에서는 모델을 수정하거나 다양한 변



[그림 1] 기술수용모델(TAM)

인들을 추가 확장한 다양한 연구가 진행되었으며, Venkatesh et al.(2000)은 Davis(1989)가 제안했던 초기 TAM 모델에 주관적 규범을 추가한 기술수용모델(TAM2)을 제안하였다.

〈표 3〉 기술수용모델(TAM) 관련 연구 요약

관련 연구	연구 내용
김성덕(2015)	기업의 업무성과 개선을 위해 도입하는 IT기술 수용의도 연구에서 보안성은 인지된 유용성과 인지된 용이성에 유의한 영향을 미치는 것을 확인
김병곤(2019)	모바일 앱 서비스 특성이 사용자 만족 및 지속적 사용 의도에 미치는 영향 연구에서 보안성이 지각된 유용성과 용이성에 영향을 미침을 확인
서광규(2013)	클라우드 채택의도 영향요인 연구에서 보안은 신뢰와 더불어 가장 중요하게 고려되는 변수임을 확인
Luo et al.(2010)	기업용 메신저 시스템 도입의 영향 관계에 관한 실증연구에서 보안성이 기업용 메신저 사용의도에 영향을 미침을 검증

Venkatesh et al.(2008)는 TAM2에서 지각된 사용용이성에 영향을 주는 요인으로 조건 변인인 컴퓨터 자기효능감, 외부 지원에 대한 인식, 컴퓨터에 대한 불안감과 유희성, 조절 변인으로 인지된 즐거움, 객관적인 사용용이성 등을 추가한 TAM3를 제안하였으며, 기존의 기술수용 모델과는 다르게 경험이라는 조절효과에 대해 강조하였다.

2.5 오픈뱅킹 수용도 영향요인 고찰

은행의 경우 해당 은행 고객 外 금융 인프라 개방에 따라 전 국민을 대상으로 결제 및 다양한 금융서비스를 제공할 수 있는 변화가 발생하며 다양한 채널을 통한 고객 획득, 유지, 신상품 개발 및 유통 등 전반적인 경쟁력 제고 전략이 필요하다.

핀테크 기업의 경우 은행권 의존 없이 저렴한 비용으로 서비스 제공이 가능해짐에 따라 활발한 시장 진입이 예상된다.

금융소비자의 경우 하나의 은행 또는 핀테크 앱으로 본인의 모든 은행계좌를 등록하여 편리한 금융서비스를 이용할 수 있다. 소비자의 금융서비스 선택권 및 본인정보 통제권 강화로 금융노마드 출현 등 금융생활의 획기적 변화가 예상되나 반대 급부적으로 기존 신뢰성이 담보된 금융권 외 핀테크 등 다양한 채널에 정보와 자산이 통합관리 됨에 따라 보이스피싱 등 금융사기를 통한 피해가 확대될 것으로 보인다. 이는 오픈뱅킹의 초기 안정화 및 서비스 확대를 위해 정보보호의 중요성이 매우 높음을 의미한다. 이러한 정보보호의 중요성은 비단 오픈뱅킹 서비스만이 아니라 새롭게 출시되는 다양한 IT 서비스에 대해서 보안성의 서비스 수용의도에 미치는 영향 연구의 확대를 이끌어 왔다.

Luo et al.(2010)은 기업용 메신저 시스템 도입의 영향 관계에 관한 실증연구에서 보안성이 기업용 메신저 사용의도에 영향을 미침을 검증하였다. 서광규(2013)는 클라우드 채택의도 영향요인 연구에서 보안은 신뢰와 더불어 가장 중요하게 고려되는 변수임을 확인하였다. 김성덕(2015)은 기업의 업무성과 개선을 위해 도입하는 IT기술 수용의도 연구에서 보안성은 인지된 유용성과 인지된 용이성에 유의한 영향을 미치는 것을 확인하였다. 김병곤(2019) 등은 모바일 앱 서비스 특성이 사용자 만족 및 지속적 사

용 의도에 미치는 영향 연구에서 보안성이 지각된 유용성과 용이성에 영향을 미침을 확인하였다.

이러한 연구를 통해 확인된 기술 및 서비스 수용도에 유의미한 영향을 주는 인지된 보안성은 이용자의 서비스에 대한 지각된 취약성과 지각된 심각성으로 구성된 위협평가와 반응 효능감과 자기 효능감, 반응비용으로 구성된 대처평가를 통해 도출될 수 있다. 함상열(2017)은 서비스 이용시 노출될 수 있는 위험에 대한 위험인지정도를 촉진조건으로 삼아 인지된 보안이 수용의도에 영향을 미치는 것으로 발표하였다. 또한 정태기(2017)는 사용자가 모바일 뱅킹 서비스에 대해 금융거래로서 안전성을 매우 중시하고 있으며, 개인정보 보안을 주요 요인으로 고려하고 있다고 하였다. Chenoweth et al.(2007) 등은 정보보호 측면에서 보안위협 평가와 대처 평가에 따른 보안 대책의 우선순위화를 통해 최종 적용 여부를 결정한다고 하였다. 금융보안원(2019)은 오픈뱅킹 관련 보안점검 주요내용을 통해 보안성심의, 이상금융거래탐지, 데이터보안, 제휴사 보안관리 등이 필요하다고 하였다.

선행연구를 통해 확인된 오픈뱅킹 위협 및 대응방안을 고려하여 서비스 수용 선택을 위한 위협 및 대처평가 수행 항목으로 보안성심의 적용, 이상금융거래탐지, 데이터보안관리, 개발보안관리, 위수탁보안관리, 접근통제관리을 정의하였다.

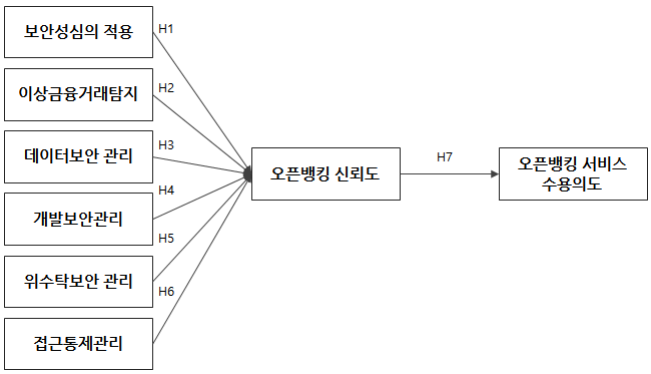
오픈뱅킹 정보보호 위협 대응 방안의 선택과 수용도 간의 영향도를 분석함으로써 각 금융사들은 오픈뱅킹 서비스 확산을 위해 적용할 수 있는 보안성 강화 방안을 확인하여 경쟁력을 확보할 수 있을 것이다.

3. 연구모형

3.1 연구모형

선행연구 고찰을 통해 보호동기이론과 기술수용모델 기반하여 오픈뱅킹 정보보호위협 대응방안과 서비스 수용도간의 영향도를 파악하는 연구 모델을 설계하였다. 오픈뱅킹 서비스 수용 의도에 영향을 미치는 요인 중 독립변수로 지각된 보안성심의 적용, 이상금융거래탐지, 데이터보안관리, 위수탁보안관리, 접근통제관리, 개발 보안관리를 선정하였다. 또한 Pavlou(2001)가 전자상거래의 신뢰도와 기술수용도 모델의 통합연구에서 제시한 정보보호 인식과 서비스 신뢰도가 궁극적으로 전자상거래서비스 거래의도에 미치는 영향을 기반으로 오픈뱅킹 신뢰도를 매개변수로 하여 독립변수가 오픈뱅킹 서비스 수용의도에 영향을 미치는지 확인하였다.

정보보안기술 사용에 대한 규범수준, 인식수준, 기술의 유용성 인식수준, 자기 효능감이 정보보안기술 사용 의지에 유의한 영향을 미치며 보안위협의 발생가능성, 즉 지각된 취약성의 수준이 높을수록 정보보안기술에 대한 인식도가 향상되므로 IT 이해도 등을 포함한 요소들의 조절효과를 파악하였다. 이를 정리한 연구 모델은 [그림 2]와 같다.



[그림 2] 오픈뱅킹 서비스 수용의도 연구 모형

3.2 연구가설

서비스 이용자는 이용기관의 오픈API 관련 정보처리시스템에 대한 악성코드 감염으로 이용자 본인의 거래정보 등 개인신용정보가 탈취될 수 있음을 위협으로 보고 이에 대한 이용기관 보안관리체계 수준 평가 등의 보안성심의에 대해서 위협평가 및 대처평가를 수행하여 서비스 신뢰도를 정하고 이를 통해 서비스 수용도를 결정할 수 있다. 이를 확인하기 위하여 다음의 가설을 설정하였다.

H1: 보안성심의 적용은 오픈뱅킹 신뢰도에 정(+)의 영향을 미칠 것이다.

서비스 이용자는 피싱 등을 통해 노출된 이용자 본인의 정보를 악용하여 이용기관에 본인을 사칭, 서비스를 등록하여 불법적인 계좌이체 등을 수행할 수 있음을 위협으로 보고 이에 대한 예방, 탐지, 대응을 위한 이상금융거래탐지 등의 대응에 대해서 위협 및 대처 평가를 실시하여 오픈뱅킹 신뢰도 및 최종 서비스 수용여부를 결정할 수 있다. 이를 확인하기 위하여 다음의 가설을 설정하였다.

H2: 이상금융거래탐지는 오픈뱅킹 신뢰도에 정(+)의 영향을 미칠 것이다.

서비스 이용자는 이용기관시스템 침해로 오픈뱅킹 데이터와 서비스에 접근하는 핵심데이터인 오픈API 접근키가 대규모 유출되어 대규모 침해와 부정사용이 발생 할 수 있음을 위협으로 인지하고 이에 대해서 암호화 등을 통해 오픈API 관련 정보자산을 보호하는 데이터보안 관리에 대한 평가를 실시하여 오픈뱅킹 서비스 신뢰도 및 최종 사용도를 결정할 수 있다. 이를 확인하기 위하여 다음의 가설을 설정하였다.

H3: 데이터보안관리는 오픈뱅킹 신뢰도에 정(+)의 영향을 미칠 것이다.

서비스 이용자는 악의적으로 변조된 애플리케이션을 통해 이용자데이터 및 인증정보가 유출되는 침해행위를 위협으로 인지하고 이에 대해서 오픈API 이용 애플리케이션 개발시 시큐어 코딩 등을 적용하여 안전성을 확보토록 하는 개발보안관리에 대한 평가를 실시하여 오픈뱅킹 서비스의 신뢰도 및 서비스 수용 여부를 결정할 수 있다. 이를 확인하기 위하여 다음의 가설을 설정하였다.

H4: 개발보안관리는 오픈뱅킹 신뢰도에 정(+)의 영향을 미칠 것이다.

서비스 이용자는 금융기관에 제공한 정보가 취약하고 영세한 이용기관에게 제공될 경우 이용기관을 통해 개인신용정보가 유출될 수 있음을 위협으로 인지하고 이에 대해서 오픈API를 통해 수집한 개인신용정보의 제공, 위탁 관련하여 사전 제휴업체 적정성 등을 평가하는 위수탁 보안관리에 대해서 위협평가와 대처평가를 수행하여 서비스 신뢰도를 정할 수 있다. 이를 확인하기 위하여 다음의 가설을 설정하였다.

H5: 위수탁보안관리는 오픈뱅킹 신뢰도에 정(+)의 영향을 미칠 것이다.

서비스 이용자는 공격자가 이용기관 등을 통해 사칭한 이용자계좌에 접근하는 경우 이용자 데이터 침해가 침해될 수 있고 오픈API 이용 애플리케이션의 침해 또는 오류로 비정상적으로 오픈API에 접근되어 금전적 손실이 발생할 수 있음을 위협으로 인지하고 이용기관과 제공기간 간 연계 시 고객정보에 대한 불필요 접근 탐지 및 차단 등을 적용하는 접근통제관리에 대해서 위협평가와 대처평가를 실시하여 서비스 신뢰도를 정할 수 있다. 이를 확인하기 위하여 다음의 가설을 설정하였다.

H6: 접근통제관리는 오픈뱅킹 신뢰도에 정(+)의 영향을 미칠 것이다.

함상열(2017)은 인지된 보안이 수용의도에 영향을 미치며 정태기(2017)는 사용자가 금융거래의 안전성을 매우 중시하고 있으며, 개인정보보안을 주요 요인으로 고려하고 있다고 하였다. Pavlou(2001)의 전자상거래의 신뢰도와 기술수용도 모델의 통합연구를 통해 오픈뱅킹 서비스의 수용의도는 정보보호에 의한 오픈뱅킹 신뢰도가 관여한다고 판단할 수 있으며 이를 확인하기 위하여 다음의 가설을 설정하였다

H7: 오픈뱅킹 신뢰도는 오픈뱅킹 서비스 수용의도에 정(+)의 영향을 미칠 것이다.

3.3 변수의 조작적 정의

본 연구는 기술수용이론과 보호동기이론을 기반으로 독립변수는 보안안성심의적용, 이상금융거래탐지, 데이터보안관리, 위수탁보안관리, 접근통제관리, 개발보안관리를 선정하였다. 오픈뱅킹 신뢰도를 매개변수로 하여 독립변수가 종속변수인 오픈뱅킹 서비스 수용의도를 측정토록 구성하였다.

〈표 4〉 변수의 조작적 정의

변수		조작적 정의
독립변수	보안성심의 적용	오픈뱅킹 이용기관에 대한 보안관리체계 수준 평가 정도
	이상금융거래탐지	오픈뱅킹 이용기관 및 제공기관 간 전달되는 금융거래의 이상유무 판단, 사고예방 정도
	데이터보안관리	오픈뱅킹 사용자(금융소비자)의 개인신용정보 보호 수준
	개발보안 관리	제휴 이용기관의 연계시스템 개발 시 시큐어 코딩 등을 통한 위험 방지 방안 적용 정도
	위수탁 보안관리	은행 등 오픈뱅킹 제공기관이 핀테크 등 이용기관과 제휴시 해당 기관에 대한 위험 판단 정보
	접근통제 관리	이용기관과 제공기간 간 연계 시 고객정보에 대한 불필요 접근 탐지 및 차단 등 위험 통제 수준
매개변수	오픈뱅킹 신뢰도	오픈뱅킹 서비스시 사용시 사용자 개인신용정보의 안전한 처리 여부에 대한 믿음 정도
종속변수	오픈뱅킹 서비스 수용의도	오픈뱅킹 서비스를 수용하고자 하는 의향의 정도

4. 연구 검증 및 실증 분석

4.1 조사 대상의 인구통계학적 특성

오픈뱅킹 통제항목 중 중요 요소 선별을 위해 정보보호 및 사이버보안 업무를 담당하는 관리자, 실무자를 대상으로 전문가그룹을 구성하여 설문조사를 실시하였다. 조사 기간은 2021년 7월 1일부터 4일간 1차 파일럿 설문을 진행하였고, 2021년 7월 19일부터 3주간 2차 설문을 실시하여 총267부의 설문 응답을 회수하였다. 수집된 데이터 중 결측치 및 불성실한 응답을 제외한 207부의 설문을 최종 분석하였다.

수집 데이터의 탐색적 요인분석을 통한 타당성과 신뢰성 분석을 실시하였다. 연구 모형 검증을 위해 확인적 요인분석과 구조방정식 분석을 실시하였으며, 통계분석 프로그램은 IBM SPSS Statistics 28.0과 AMOS 26을 활용하였다. 응답자의 빈도분석을 통한 인구통계학적 특성은 <표 5>와 같다.

〈표 5〉 조사표본의 인구통계학적 특성

구분		빈도수 (명)	비율 (%)
성별	남성	174	84.1
	여성	33	15.9
연령	20대	12	5.8
	30대	48	23.2
	40대	93	44.9
	50대 이상	54	26.1
업무경력 (정보보호)	3년 미만	12	5.8
	3년~6년 미만	65	31.4
	6년~9년 미만	35	16.9
	9년 이상	95	45.9
근무조직	IT회사(핀테크 등)	42	20.3
	공공기관	10	4.8
	교육기관(대학교 등)	5	2.4
	금융사(은행 등)	150	72.5
오픈뱅킹 사용	사용	172	83.1
	미사용	35	16.9
오픈뱅킹 신뢰도	매우 신뢰함	35	16.9
	신뢰함	75	36.2
	보통	64	30.9
	신뢰하지 못함	16	7.7
	매우 신뢰하지 못함	17	8.2

응답자는 207명으로, 남성은 174명(84.1%), 여성은 33명(15.9%)이며 연령대는 40대가 93명(44.9%)으로 가장 많고, 50대 이상 54명(26.1%), 30대 48명(23.2%), 20대 12명(5.8%) 순으로 분포되었다. 정보보호 업무경력은 9년 이상이 95명(45.9%)으로 가장 높고 3년~6년 미만인 65명(31.4%)이 다음으로 높고 6년~9년 미만이 35명(16.9%), 3년 미만이 12명(5.8%)순으로 분포되었다. 근무조직은 금융사가 150명(72.5%)으로 가장 많고 핀테크 등 IT회사가 42명(20.3%), 금융보안원 10명(4.8%), 대학교 등 교육기관이 5명(2.4%) 순으로 분포되었다. 오픈뱅킹 사용유무의 경우 사용자는 172명(83.1%), 미사용자는 35명(16.9%)으로 분포되었다. 오픈뱅킹 신뢰도의 경우 매우 신뢰함은 35명(16.9%), 신뢰함은 75명(36.2%), 보통은 64명(30.9%), 신뢰하지 못함은 16명(7.7%), 매우 신뢰하지 못함은 17명(8.2%) 순으로 분포되어 있다.

4.2 탐색적 요인 분석과 신뢰도 분석

타당성(validity)은 측정하려는 추상적인 개념이 측정 도구에 의해 얼마나 정확하게 측정되었는지를 판단하는 기준이며, 신뢰성(reliability)은 연구자가 설문 조사를 다시 반복한다고 가정할 때 그 결과가 얼마나 원래 측정치와 일치하는지를 나타내는 척도이다.

탐색적 요인 분석 시 요인추출 방법은 주성분 분석을 사용하였고, 요인회전 방식은 다중공선성 방지를 위해 베리맥스 직교 회전 방식을 적용 하였다. 요인들 가운데 고유값(Eigen Value)이 1.0 이상이면서 요인 적재량(Factor Loading Value)이 0.5 이상인 경우 유의한 것으로 판단할 수 있다. 요인분석의 결과 그룹화된 요인에 대한 신뢰도 분석시 크론바흐 알파 계수(Cronbach's α coefficient) 값을 기준으로 사용하며, 이 값이 0.7 이상이면 각 변수의 측정이 내적 일관성이 있다고 판단하고, 신뢰도가 낮은 경우 신뢰도를 확보하기 위해 항목을 삭제하기도 한다. 분석결과 개발보안관리의 1번째, 3번째, 5번째 항목은 기준 요인 적재량이 상이하게 적재되어 분석에서 제외하였다. 탐색적 요인분석 결과는 <표 6>, <표 7>과 같다. 각 요인들의 적재값, 고유 값(Eigen Value)같은 유의미하며, KMO는 0.923이고 Bartlett 구형성 검정 유의확률은 0.05 이상이며 신뢰도 분석 결과인 크론바흐 알파 계수의 값은 모두 0.7이상으로 내적 일관성 있는 항목으로 구성되었음을 확인하였다.

〈표 6〉 KMO 검정

KMO & Bartlett's Test		
Kaiser-Meyer-Olkin's Measure of Sampling Adequacy		.923
Bartlett's Test of Sphericity	Approx. Chi-Square	2680.298
	df	105
	Sig.	.000

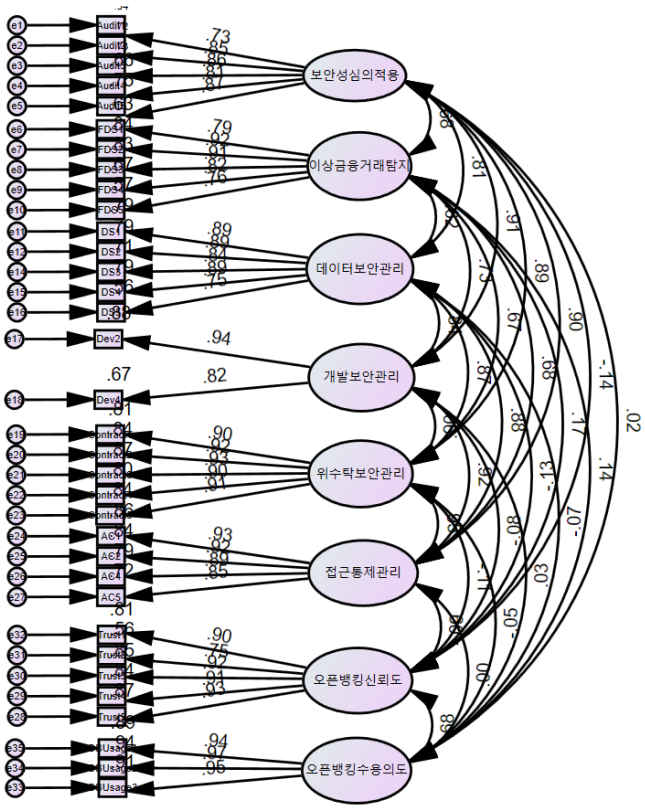
4.3 확인적 요인분석

측정모형 적합도 평가를 위해 수집된 자료와 연구모형의 부합되는 플랫폼 정보를 절대적으로 평가하는 CMIN(χ^2), CMIN(χ^2)/df, GFI(Goodness-of-Fit Index), RMR(RootMean Residual), RMSEA (Root Mean Square Error of Approximation)인 절대 적합도 지수(absolute fit index)와 PNFI(parsimony normed fir index), PGFI(parsimony goodness of fit index) 등 간명 적합도 지수(parsimonious fit index)를 이용하여 측정하는데, CMIN(χ^2)은 일반적으로 p>0.05가 적합하나 사례수에 민감하므로 다른 적합도 지수들을 우선적으로 고려하여 평가한다.

연구자의 구조방정식 모형과 변수 간 상관을 설정하지 않는 모형(영모형)과 비교하여 정확하게 측정되었는지를 확인하기 위해서는 NFI(Normed Fit Index), CFI(ComparativeFit Index) 및 TLI(Tucker and Lewis Index) 등 증분 적합도 지수(incremental fit index)를 이용하여 측정한다.

〈표 7〉 탐색적 요인 분석 및 신뢰도 분석

개념	항목	1	2	3	4	5	6	7	8	Cronbach's a
보안성심의 적용	3	.813								.944
	2	.770								
	4	.769								
	5	.731								
	1	.554								
이상금융거래탐지	2		.836							.945
	4		.831							
	3		.830							
	5		.796							
	1		.726							
데이터보안 관리	4			.827						.944
	3			.820						
	2			.776						
	5			.753						
	1			.750						
개발보안관리	4				.873					.972
	2				.619					
위수탁보안 관리	4					.804				.969
	2					.765				
	3					.739				
	1					.734				
	5					.709				
접근통제관리	5						.824			.970
	2						.708			
	1						.665			
	4						.633			
오픈뱅킹신뢰도	3							.885		.947
	5							.873		
	4							.864		
	1							.842		
	2							.775		
오픈뱅킹수용의도	2								.914	.968
	1								.913	
	3								.902	
Eigen Value		3.615	3.892	3.994	2.209	4.056	3.306	3.943	3.014	
% of Variance		24.100	25.948	26.629	20.086	36.872	30.053	49.283	37.676	



[그림 3] 측정모형(확인적 요인분석)

<표 8>에 제시된 최종 측정모형의 적합도를 살펴보면, CMIN(χ^2) = 947.240(df = 502, p < 0.001), CMIN(χ^2)/df = 1.887, RMSEA = 0.066, RMR = 0.028, NFI = 0.890, TLI = 0.938, CFI = 0.945, PNFI = 0.797, PCFI = 0.846, PGFI = 0.672 등으로 나타나 비교적 양호한 적합도를 보였다.

〈표 8〉 측정모형의 적합도

적합도 지수		임계치	측정값
절대 적합도 지수	CMN(x^2)	p > 0.05 (표본의 크기에 민감)	947.240(df = 502, P = 0.000)
	CMN(x^2)/df	≤3 or 4	1.887
	RIVSEA	≤0.05~0.08	0.066
	RIVR	≤0.08	0.028
증분 적합도 지수	NFI	≥ 0.08~0.9	0.890
	TLI	≥ 0.08~0.9	0.938
	CFI	≥ 0.08~0.9	0.945
간명 적합 도지수	PNFI	≥ 0.6	0.797
	PCFI	≥ 0.6	0.846
	PGFI	≥ 0.6	0.672

4.4 집중 타당성과 판별 타당성

보안성심의적용, 이상금융거래탐지, 데이터보안관리, 개발보안관리, 위수탁보안관리, 접근통제관리, 오프뱅킹신뢰도, 오픈뱅킹수용의도 등 잠재변수에 대한 모든 측정 변수의 비표준화 λ의 C.R.(Critical Ratio)은 $p < 0.05$ 기준에서 1.96 이상으로 모두 유의했다.

$$C.R. = \frac{\text{비표준화}\lambda}{S.E.(Standard\ Error)}$$

다음으로 연구변수들의 집중타당성 검증을 위해 표준화 λ, 평균분산추출 값(Average Variance Extracted), 개념신뢰도(Construct Reliability)를 확인하였다. 일반적으로 표준화 λ는 0.5 이상, 평균분산추출 값은 0.5 이상, 개념신뢰도는 0.7 이상이면 집중타당성이 있다고 본다. <표 9>에 제시된 바와 같이, 모든 잠재변수의 평균분산추출 값은 0.5 이상, 개념신뢰도는 0.7 이상으로 높게 나타나 집중타당성이 검증되었다.

〈표 9〉 측정모형의 확인적 요인분석

구분		비표준화계수	S.E.	C.R.	표준화 계수	평균분산추출	개념신뢰도
보안성 심의적용	→ Audit1	1.000	-	-	.732	.773	.944
	→ Audit2	1.064	.086	12.377***	.849		
	→ Audit3	1.106	.089	12.478***	.856		
	→ Audit4	1.032	.088	11.765***	.810		
	→ Audit5	1.057	.084	12.642***	8.66		
이상 금융거래탐지	→ FDS1	1.000	-	-	.793	.811	.955
	→ FDS2	1.077	.057	18.895***	.916		
	→ FDS3	1.090	.059	18.593***	.909		
	→ FDS4	1.097	.072	15.142***	.816		
	→ FDS5	1.000	-	-	.756		
데이터 보안관리	→ DS1	1.000	-	-	.887	.841	.963
	→ DS2	.993	.050	19.978***	.887		
	→ DS3	.998	.056	17.621***	.841		
	→ DS4	1.074	.054	19.937***	.886		
	→ DS5	1.000	-	-	.745		
개발보안관리	→ Dev2	1.000	-	-	.937	.844	.915
	→ Dev4	.974	.057	17.093***	.821		
위수탁 보안관리	→ Contract1	1.000	-	-	.899	.897	.977
	→ Contract2	.937	.036	25.713***	.916		
	→ Contract3	.1.009	.037	27.452***	.931		
	→ Contract4	1.037	.044	23.684***	.896		
	→ Contract5	1.000	-	-	.914		
접근통제관리	→ AC1	1.000	-	-	.926	.880	.967
	→ AC2	1.021	.044	23.923***	.915		
	→ AC4	.980	.046	21.389***	.890		
	→ AC5	.994	.052	18.962***	.851		
오픈뱅킹 신뢰도	→ Trust1	1.000	-	-	.901	.746	.936
	→ Trust2	.689	.050	13.844***	.747		
	→ Trust3	.996	.046	21.592***	.920		
	→ Trust4	.940	.044	21.204***	.914		
	→ Trust5	1.052	.047	22.332***	.931		
오픈뱅킹 수용의도	→OBUsage1	1.000	-	-	.941	.876	.955
	→OBUsage2	1.108	.036	31.136***	.969		
	→OBUsage3	1.137	.039	29.192***	.954		

〈표 10〉 잠재변수들 간의 판별타당서 검증결과

구 분	보안성 심의적용	이상금융 거래탐지	데이터보안 관리	개발보안 관리	위수탁 보안관리	접근통제 관리	오픈뱅킹 신뢰도	오픈뱅킹 수용의도
보안성심의적용	**.773**							
이상금융거래탐지	.463	**.811**						
데이터보안관리	.656	.381	**.841**					
개발보안관리	.656	.540	.702	**.844**				
위수탁보안관리	.769	.448	.751	.806	**.897**			
접근통제관리	.641	.466	.770	.675	.724	**.880**		
오픈뱅킹신뢰도	.018	.029	.015	.656	.012	.007	**.746**	
오픈뱅킹수용의도	.001	.018	.435	.108	.280	.001	.462	**.955**

잠재변수간의 판별타당성은 두 잠재변수 각각의 평균분산추출 값이 두 잠재변수 상관계수의 제곱보다 크면 판별타당성이 있는 것으로 본다. 즉, 평균분산추출값(AVE)은 상관계수의 제곱(ρ^2)보다 커야 한다. <표 10>에 제시된 바와 같이, 모든 잠재변수의 평균분산추출 값은 상관계수 제곱보다 큰 것으로 확인되어 판별타당성이 검증되었다.

$$AVE = \frac{\sum 표준화\lambda^2}{\sum 표준화\lambda^2 + \sum 오차계수}$$

4.5 연구 가설 검증

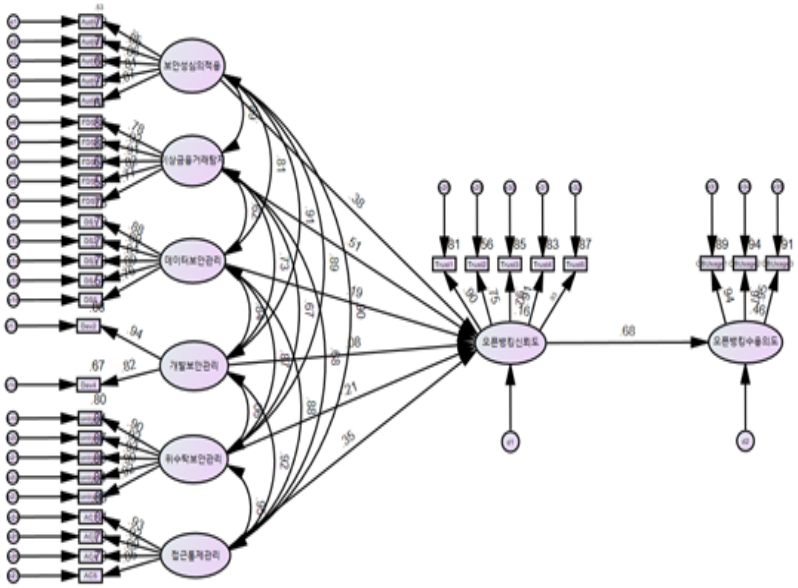
연구모형의 적합도는 <표 11>과 같이 CMIN(χ^2) = 959.041(df = 505, p < 0.001), CMIN(χ^2)/df = 1.899, RMSEA = 0.066, RMR = 0.033, NFI = 0.889, TLI = 0.938, CFI = 0.944, PNFI = 0.800, PCFI = 0.850, PGFI = 0.673 등으로 나타나 비교적 양호한 적합도를 보이며, 연구결과를 수용하는 데 무리가 없음을 확인하였다.

<표 12>의 가설 검증 결과를 보면 H1의 보안성심의는 오픈뱅킹 신뢰도에 유의미한 영향을 미치는 것으로 확인되었다(표준화계수 0.382, C.R. 1.960). 즉, 오픈뱅킹 이용기관에 대한 보안관리체계 유무, 고객 정보 유실에 대한 대응책 등에 대한 준비가 오픈뱅킹 신뢰도에 영향을 줄 수 있음을 의미한다.

또한 H2의 이상금융거래탐지시스템은 오픈뱅킹 신뢰도에 유의미한 영향을 미치는 것으로 확인되었다. 금결원 등을 중심으로 오픈뱅킹 거래 트랜잭션에 대한 모니터링과 이상금융거래 발생에 대한 포괄

〈표 11〉 연구모형 적합도

적합도 지수		임계치	측정값
절대 적합도 지수	CMIN(χ^2)	p>0.05 (표본의 크기에 민감)	959.041 (df = 505, P = 0.000)
	CMIN(χ^2)/df	≤3 or 4	1.899
	RMSEA	≤0.05~0.08	0.066
	RMR	≤0.08	0.033
증분 적합도 지수	NFI	≥ 0.08~0.9	0.889
	TLI	≥ 0.08~0.9	0.938
	CFI	≥0.08 ~0.9	0.944
간명 적합 도지수	PNFI	≥0.6	0.800
	PCFI	≥0.6	0.850
	PGFI	≥0.6	0.673



[그림 4] 연구모형 검증 결과

〈표 12〉 연구모형의 경로계수 및 가설 검증 결과

가설	경로	표준화계수	S.E.	C.R.	P	결과
H1	보안성심의 → 오픈뱅킹신뢰도	.382	.328	1.960	***	채택
H2	이상금융거래탐지 → 오픈뱅킹신뢰도	.506	.206	4.390	***	채택
H3	데이터보완관리 → 오픈뱅킹신뢰도	.191	.312	1.110	.267	기각
H4	개발보안관리 → 오픈뱅킹신뢰도	.075	.482	0.244	.807	기각
H5	위수탁보안관리 → 오픈뱅킹신뢰도	.213	.479	0.700	.484	기각
H6	접근통제관리 → 오픈뱅킹신뢰도	.353	.652	0.907	.365	기각
H7	오픈뱅킹신뢰도 → 오픈뱅킹신뢰도	.679	.060	11.198	***	채택

*p<0.05, **p<0.01, ***p<0.001.

적 대응이 중요함을 의미한다.

마지막으로 H7의 오픈뱅킹 신뢰도는 오픈뱅킹수용의도에 유의미한 영향을 미치는 것으로 확인 되었다. 오픈뱅킹이라는 신서비스에서 금융서비스라는 특징에 기인한 서비스 안정성과 보안성, 즉 신뢰성이 서비스 사용도에 영향을 미침을 확인하였다.

4.6 조절효과 검증

연구 결과에 대해 집단 특성의 차이로 발생 가능한 조절 효과를 확인하고자 근무조직(금융권/비금융권), 오픈뱅킹 이용기관 수, 오픈뱅킹 보안책임(이용기관/제공·중계기관), 보안인식 수준 및 근무경력 등의 잠재변수 영향도를 검토하였다. 가설 경로의 동질성 제약을 둔 제약모델과 제약을 두지 않은 자유모델 간 비교를 실시하였다. 자유모델과 제약모델의 카이제곱(Chi-square)과 자유도(Degree of freedom) 간의 p값이 유의수준 범위(p<.05)에 들지 못할 경우 귀무가설인 “영향의 차이가 없다”를 기각할 수 없어 조절효과가 없는 것으로 판단한다.

근무조직, 오픈뱅킹 이용기관 수에 기인한 특성의 경우 제약모델에 대한 유의수준이 p<.05로 조절효

과가 있었으나, 보안인식수준, 근무경력 등은 유의하지 않아 기각하였다.

근무조직의 경우 금융권(105명/207명)과 비금융권(102명/207명)에 따라 조절효과가 있었다. 이는 금융권에 속하는 경우 오픈뱅킹 서비스의 보안성을 보장하기 위해서 이상금융거래탐지가 필요함을 인식한다고 판단할 수 있다(<표 13> 참고).

〈표 13〉 근무조직의 조절효과 검증결과

Model Comparison			
Model	DF	CMIN	P
제약모델	7	31.048	***

Path	측정항목	3개 미만	3개 이상
이상금융거래탐지 → 오픈뱅킹신뢰도	Estimate	1.174	1.089
	C.R.	4.157***	.203

*p<0.05, **p<0.01, ***p<0.001.

오픈뱅킹 이용기관 수의 경우 사용하는 오픈뱅킹 앱 수를 기준으로 3개 미만(109명 /207명), 3개 이상(98명/207명)으로 구분하여 3개 미만인 경우도 이상금융거래탐지에 대해 조절효과 있음으로 확인되었다(<표 14> 참고).

〈표 14〉 오픈뱅킹 이용기관 수의 조절효과 검증결과

Model Comparison			
Model	DF	CMIN	P
제약모델	7	22.120	**

Path	측정항목	3개 미만	3개 이상
이상금융거래탐지→ 오픈뱅킹신뢰도	Estimate	1.174	1.089
	C.R.	4.157***	.203

*p<0.05, **p<0.01, ***p<0.001.

5. 결 론

5.1 결과 요약 및 시사점

본 연구는 보호동기이론과 기술수용모델에 관한 선행연구를 기반으로 사용자의 서비스 수용의도에 서비스의 신뢰도가 영향을 미칠 것이며, 서비스 신뢰도는 해당 서비스의 위협 및 대응 방안에 대한 이용자의 평가를 기반으로 선택된 보호조치에 영향을 받음을 실증하였다.

오픈뱅킹 서비스 이용자는 오픈뱅킹 서비스 이용자 앱의 취약점을 악용하여 이용기관 오픈뱅킹 정보처리시스템을 침해하는 등의 오픈뱅킹 정보보호 위협과 보안성심의 적용, 이상금융거래탐지, 데이터보안관리, 개발보안관리, 위수탁보안관리, 접근통제관리라는 대응방안에 대해 비교 평가를 실시한다.

연구 결과 오픈뱅킹 서비스 수용도는 해당 서비스에 대한 이용자의 신뢰도에 영향을 받음을 확인하였다. 또한 보호동기이론에 따라 이용자의 신뢰도는 해당 서비스의 위협평가와 이에 대한 대처평가가 영향을 미치며, 보호조치 중 이상금융거래탐지(FDS)와 서비스 오픈전 사전 보안성 심의가 신뢰도에 유의미한 영향을 미치는 것을 확인하였다.

조절효과 검증을 통해 은행 등 금융권에 근무하며 오픈뱅킹 앱을 사용한 경험이 있는 경우 오픈뱅킹 서비스 수용도에 조절효과가 있음을 확인하였다.

또한 본 연구 응답자에게 오픈뱅킹 서비스의 이용자 신뢰 강화 방안을 파악하기 위해 “오픈뱅킹 이용기관 중 전자금융사고에 가장 취약할 것으로 예상되는 기관”, “오픈뱅킹 중계기관의 이상금융거래 탐지 신뢰도”, “오픈뱅킹 서비스 고객 신뢰 확보를 위한 필요 사항” 등을 문의하였다.

가장 취약할 것으로 예상되는 이용기관은 중소형 핀테크가 90%로 가장 높았다. 중계기관인 금융결제원의 이상금융거래탐지 시스템에 대한 응답자 신뢰도 평가 결과를 살펴보면 “안전하다”가 “49%(102명/207명)”, “미흡하다”가 “51%(105명/207명)”로 절반 이상이 부정적이었으며, 오픈뱅킹 서비스에 대한 고객 신뢰도 확보를 위한 방안으로 42%가 핀테크 등 이용기관의 이상금융거래탐지 강화를, 35%가 금융결제원 등 중계기관의 이상금융거래탐지의 신뢰도 강화를 요구하고 있다.

연구결과를 고려할 경우 다음과 같은 시사점을 제시할 수 있다.

〈표 15〉 오픈뱅킹 서비스 고객 신뢰 확보를 위해 필요한 사항

항목	분포
① 이용기관(핀테크 등) 이상금융거래탐지시스템(FDS)의 신뢰도	42%
② 중계기관(금융결제원) 이상금융거래탐지시스템(FDS)의 신뢰도	35%
③ 제공기관(은행 등) 이상금융거래탐지시스템(FDS)의 신뢰도	15%
④ 이용기관(핀테크 등) 보증보험가입 및 일일 출금 한도 제한 등	8%

첫째, 오픈뱅킹 서비스에 대한 수용의도 중 서비스 신뢰도는 매우 중요한 요인이다. 오픈뱅킹을 먼저 도입한 영국의 경우 오픈뱅킹에 대한 높은 기대에도 불구하고, 실제 인지도가 매우 낮은 상태이며, 이는 고객 데이터 보안에 대한 이용자들의 낮은 신뢰도 등에서 기인된 것으로 볼수 있다. 거래의 안전성과 신뢰성에서 발생되는 리스크는 고객의 금전적 손실과 연계되므로 특히 주의해야 할 부분이며 사이버보안에 대한 다중적 보안체계를 구축해야 할 필요가 있다. 이러한 측면에서 보안성심의가 오픈뱅킹 서비스 신뢰성에 유의미한 영향을 미치는 것은 보안관리체계 필요성과 중요성을 나타내는 또 다른 증거로 볼 수 있다. 변수의 조작적 정의를 통해 보안성심의는 오픈뱅킹 이용기관에 대한 보안관리체계 수준평가 정도를 의미토록 하였다. 또한 핀테크 등 오픈뱅킹 이용기관에 대한 보안성심의 시 정보보호관리체계 인증 취득여부와 고객금융자산 보호조치 유무를 포함한 보호조치의 필요성을 설문에 포함하여 조사하였다. 결과적으로 오픈뱅킹 서비스 조기 정착 및 확대를 위해 필요한 신뢰도 확보는 이용기관이 ISMS-P 또는 ISO27001 등과 같은 표준적 정보보호 관리체계를 유지하고 있어야 가능함을 의미한다. 오픈뱅킹 서비스 제공기관의 입장인 은행 등 금융기관은 전자금융거래법 및 전자금융감독규정 등 기존 금융 컴플라이언스 준수를 위해 이미 ISMS-P 또는 ISO27001과 같은 표준 정보보호관리체계를 유지하고 있다. 따라서 오픈뱅킹 서비스의 이용기관으로 신규 진입한 핀테크 기업 등에 표준 정보보호 관리체계 수립이 요구된다.

둘째, 오픈뱅킹은 서비스 이용자 접점인 이용기관과 고객정보를 보유하며 금융서비스를 제공하는 제공기관, 그리고 이용기관과 제공기관의 연계를 담당하는 중계기관 등 다양한 서비스 요소들이 결합된 플랫폼 서비스이다. 연결도가 증가할 경우 결국 복잡성과 함께 불확실성이 확대되며, 여기서 파생되는 위협을 예방하기 위해서는 참여 기관들의 협업이 필요하다. 특히 신용정보의 송수신으로 처리되는 금융거래의 이상유무를 확인하는 이상금융거래탐지(FDS)의 역할은 매우 중요하다. 이러한 사실은 이상금융거래탐지가 오픈뱅킹 서비스 신뢰성에 유의미한 영향을 미침에서 확인할 수 있다. 오픈뱅킹 이용기관 및 제공기관 간 전달되는 금융거래의 이상유무 판단, 사고예방 정도를 나타내는 이상금융거래탐지는 이용기관의 취약점을 통해 불법적인 계좌이체가 수행되어 금전적 피해가 발생할 수 있다는 위협인지와 이러한 위협에 대한 예방, 탐지, 대응이 필요하다는 대처평가의 결과로 볼 수 있다. 오픈뱅킹 서비스 이전 금융기관 간 거래는 금융결제원의 전자금융거래 인프라를 통해 은행 상호 간 금융거래정보를 송수신하는 구조이며, 각 은행은 개별적 이상금융거래탐지 시스템을 구축하여 불법적인 거래를 탐지, 차단하는 예방체계를 구축하였다. 그러나 오픈뱅킹 서비스 시행 이후 이용기관의 등장은 기존 예방체계만으로는 안전한 금융거래를 보증하기에 부족한 부분이 있다. 이러한 이상금융의 탐지와 예방을 위해서는 많은 정보가 필요하며, 중계기관인 금융결제원을 중심으로 이상금융거래 탐지 강화를 위해 각 제공기관 및 이용기관이 개별적으로 운영하는 FDS의 통합 표준 관리 방안이 필요하다.

이러한 오픈뱅킹 서비스 신뢰도에 유의미한 영향을 주는 두 가지 정보보호 대응방안은 오픈뱅킹 서비스를 구성하는 핀테크 기업, 은행 등 금융기관, 그리고 금융결제원 등 모든 이해관계자에게 오픈뱅킹 서비스 조기 안정화 및 추가 확대를 위한 전략적 방향을 제시할 수 있다는데 시사점이 있다.

5.2 한계점 및 향후 연구방향

본 연구의 한계점은 오픈뱅킹의 신 기술적 특성에 기인해 기술수용이론과 보호동기이론이 효과적으로 적용될 수 있느냐이다. 즉, 기술적 요인보다는 정책적 요인에 기인한 부분이 있을 수 있다.

검증과정에서 탐색적 요인분석과 함께 확인적 요인분석을 실시하여 타당성과 신뢰성을 높였으나 결국, 연구의 신뢰성을 강화하기 위해서는 더 많은 측정변수의 수집과 분석, 필요시 변수제거 등의 효율화 과정이 필요해 보인다. 또한 조절효과 분석시 성별, 나이, 사용경험을 활용하여 분석하였으나 특별한 효과가 확인되지 않은바 후속 연구시 조절변수에 대한 검토와 확인이 필요한 것으로 생각된다.

추후 오픈뱅킹 서비스의 신뢰도 향상과 관계하여 주요 영향 변수인 이상금융거래탐지에 관해 오픈뱅킹 서비스와의 연계성을 고려한 특화 정책, 방향 등을 연구할 필요가 있다고 생각한다.

참고문헌

고제욱, 고형석, 남상완, 한경석, “블록체인 채택에 영향을 미치는 요인 관련 개선된 연구모델 제시를 위한 실증연구”, *한국디지털콘텐츠학회논문지*, 제20권, 제3호, 2019, 513-526.

권남훈, 김인석, “국내 오픈뱅킹 안전성 강화 및 이용자 보호를 위한 규제 개선 방안”, *한국융 합보안학회*, 제20권, 제2호, 2020, 37-52.

권홍진, “오픈뱅킹 도입성과와 발전방향”, *한국금융연구원 주간금융 브리프*, 제29권, 제17호, 2020, 3-12.

금융결제원, “오픈뱅킹 공동업무 추진현황”, 2019.

금융보안원, “금융권 오픈API 이용기관 자체 보안점검 가이드”, 2019.

금융보안원, “오픈뱅킹 관련 보안점검 주요내용”, 2019.

금융위원회, “글로벌핀테크 규제환경 분석과 개선방향”, 2019a.

금융위원회, “핀테크 및 금융플랫폼 활성화를 위한 금융결제 인프라 혁신방안”, 2019b.

금융위원회, “해외 유망 핀테크기업 비즈니스 모델”, 2019.

금융위원회, “제3차 디지털금융협의회, 오픈뱅킹 고도화 방안”, 2020.

김병곤, 김기원, 서홍일, “모바일 앱 서비스 특성이 사용자 만족과 지속적 사용의도에 영향을 미치는 요인”, *Journal of Information Technology Applications & Management*, 제26권, 제3호, 2020, 99-120.

김상훈, 이갑수, “정보보안기술 사용의 영향요인에 관한 실증적 연구”, *한국전자거래학회지*, 제20권, 제4호, 2015, 151-175.

배병렬, Amos21 구조방정식모델링-원리와 실제, 청람, 2011.

배재권, “빅데이터 환경에서 개인정보유출 위협이 정보보호행위에 미치는 영향에 관한 연구”, *e-비즈니스연구*, 제17권, 제3호, 2016, 191-208.

서광규, “TAM과 VAM을 적용한 기업의 클라우드 서비스 채택의도의 영향요인 분석”, *디지털융복합연구*, 제11권, 제12호, 2013, 155-160.

서정호, “오픈API 활성화를 통한 국내 은행산업의 혁신전략”, *한국금융연구원 VIP리포트*, 2018-08, 54-55.

송지준, SPSS/AMOS 통계분석방법, 21세기사, 2010.

우종필, 구조방정식 모델 개념과 이해, 한나래 출판사, 2012.

이홍제, 노은희, 한경석, “정보보호 투자의도에 영향을 미치는 요인에 대한 연구”, *한국디지털콘텐츠학회논문지*, 제19권, 제8호, 2018, 1515-1525.

Chenoweth, T., R. Minch, and S. Tabor, “Expanding views of technology acceptance: seeking factors explaining security control adoption”, *AMCIS 2007 Proceedings*, 2007, 321.

Davis, F.D., R.P. Bagozzi, and P.R. Warahaw, “User acceptance of computer technology:

A comparison of two theoretical models", *Management Science*, Vol. 35, No. 8, 1989, 982-1003.

Floyd, D.L., Prentice-Dunn, S., and Rogers, R. W., "A meta-analysis of research on protection motivation theory", *Journal of Applied Social Psychology*, Vol.30, No.2, 2000, 407-429.

Fornell, C. and D.F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol.18, No1, 1981.

Johnston, A.C. and M. Warkentin, "Fear appeals and information security behaviors: An empirical study", *MIS Quarterly*, Vol.34, No.1, 2010, 549-566.

Pavlou, P., "Integrating trust in electronic commerce with the technology acceptance model: Model development and validation", *AMCIS 2001 Proceedings*, 2001.

Rogers, R.W., "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol.91, No.1, 1975, 93-114.

Rogers, R.W., "Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation", *Social Psychophysiology: A Sourcebook*, 1983, 153-176.

Venkatesh, V. and F.D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies", *Management Science*, Vol.46, No.2, 2000, 186-204.

Venkatesh, V. and H. Bala, "Technology acceptance model 3 and a research agenda on interventions", *Decision Science*, Vol.39, No.2, 2008, 273-315.

Venkatesh, V., J.Y.L. Thong, and X. Xu, "Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology", *MIS Quarterly*, Vol 36, No 1. 2012, 157-178.

Woon, I., G.-W. Tan, and R. Low, "A protection motivation theory approach to home wireless security", *ICIS 2005 Proceedings*, 2005, 31.

About the Authors

고 정 현 (doctorgo@naver.com)

동국대학교 핀테크블록체인학과 박사과정 재학 중으로, 연세대학교 정보대학원에서 금융정보보호 석사학위를 취득하였고, 서울시 핀테크 자문위원, 금융보안포럼 부회장이며, 시중은행에서 디지털 담당 부장, 플랫폼사업부 본부장을 역임하고, 정보보호최고책임자(ciso)로 3년 이상 재직하였다 주요 관심 분야는 디지털 전환, 핀테크 비즈니스, 금융 정보보호 등이다.

이 원 부 (wblee@dongguk.edu)

미국 보스톤 대학교 및 신시내티대학교 경영대학원에서 경영학 석·박사 학위를 취득하였다. 미국 볼티모어대학교, 텍사스주립대학교 및 동국대학교 경영대학원에서 인공지능 및 정보관리론을 강의하였으며 현재 동국대학교 일반대학원 핀테크블록체인학과 교수로 재직 중이다. 주요 연구 관심분야는 디지털 전환, 핀테크 비즈니스, 블록체인기술 및 암호화폐 기반 DeFi 등이다.