「정보시스템연구」 제26권 제3호
한국정보시스템학회
2017년 9월, pp. 313~337

http://dx.doi.org/10.5859/KAIS.2017.26.3.313

핀테크(FinTech) 서비스의 정보보안 위협요인과 개인정보보호행위와의 구조적 관계에 관한 연구: 기술위협회피와 건강행동이론 관점에서

배 재 권*

〈목 차〉

Ⅰ. 서 론

국내외 금융 산업은 2008년 글로벌 금융위기(global financial crisis) 이후 지속된 저금리 기조 및 투자 심리 위축으로 인한 수익성 악화와 강력한 금융규제로 어려움을 겪는 시점에서 정보기술(Information Technology, IT) 분야와의 융합을 통해 새로운 금융수익모델 개발과 혁신 서비스 제공으로 위기를 극복하고 있다. 혁신 서비스 중에서 대표적인 핀테크(FinTech)는 금융(Finance)과 기술(Technology)이 융합된 것으로 IT기반 금융서비스를 보다 낮은 비용과 향상된 보안성 및 편의성으로 금융소비자들에게 제공하고 있다. 핀테크 주요 서비스인 지급결제(payments)는 과거의 인터넷뱅킹과 모바일뱅킹의 결제서비스에서 현재는 인터넷전문은행과 앱카드(app card)를 활용한 간편결제 서비

* 계명대학교 경영대학 경영정보학전공 조교수, jkbae99@kmu.ac.kr

스로 이동하고 있다.

글로벌 컨설팅 전문기업인 액센츄어(accenture)의 '2015년 글로벌 핀테크 투자동향 보고서'에서는 전 세계 핀테크 시장규모는 2011년에 124조원에서 2015년에는 500조원, 2017년에는 845조원 수준으로 성장할 것으로 전망하였다. 또한 글로벌 시장조사기관인 리서치앤마켓(Reserch & Markets)의 '2016년 글로벌 핀테크 산업전망 보고서'에서는 전 세계 핀테크 투자 시장은 2016년부터 2020년까지 연평균 54.83%의 성장을 기록할 것이라고 예측하는 등 핀테크 분야가 금융 및 결제서비스 혁신을 만들어내면서 벤처캐피털(venture capital) 분야에서 가장 빠르게 성장하고 있다. 글로벌 핀테크 시장 선도국가인 미국은 지급결제 시장에서 매년 40%의 거래성장률을 나타내고 있으며, 현재는 지급결제 뿐만 아니라 IT를 활용한 대출, 개인자산관리, 보험 등 전통적인 금융업의 고유영역까지 서비스를 확대하고 있다. 미국과 함께 핀테크 산업을 주도하고 있는 영국은 유럽 최대의 핀테크 클러스터인 '테크 시티(Tech City)'를 기반으로 핀테크 사업을 추진하고 있으며, 2015년 기준 약 200억 파운드(약 29조원)의 시장규모를 갖추게 되었다. 이처럼 다가오는 '제4차 산업혁명(4th Industrial Revolution)' 시대를 맞아 주요 선진국들은 핀테크 서비에 대한 투자를 지속적으로 늘리고 있으며, 핀테크 기술개발을 위한 네거티브(negative) 규제와 전폭적인 정부지원을 통해 경쟁력 있는 핀테크 스타트업(start-up) 기업을 배출하고 있다.

그러나 국내 핀테크 산업은 각종 법적 규제와 해킹 위협으로 주요 선진국에 비해 경쟁력이 떨어지는 것이 현실이며 핀테크 전문 인력도 부족한 실정이다. 경직된 금융관련 규제 법안과 강력한 보안심의제도로 인해 핀테크 관련 지원 및 투자가 활발하지 못한 것이 그 이유이다. 국내 금융보안 산업 발전을 저해하던 공인인증서 의무 규정 및 액티브엑스(ActiveX) 보안 모듈 폐지와 핀테크 스타트업의 보안성 심의 완화로 인해 핀테크 서비스 시장은 이제 확산 초기 단계에 있으며 핀테크 산업의 기본적인 비즈니스 모델인 지급결제 서비스를 IT기업 주도하에 제공하고 있다. 향후에는 기존 은행들의 고유 분야인 금융빅데이터 분석과 대출, 자산운용 등의 플랫폼 분야에서 성장이 기대되고 있다.

최근의 핀테크 서비스 시장은 다양한 모바일 디바이스 확산으로 인한 모바일 금융거래 증가, 인공지능기법을 활용한 금융거래 분석, 결제소프트웨어의 지능화 등으로 인해 지능형 핀테크 서비스(Intelligent FinTech)로 진화하면서 핀테크 서비스 이용자 수가 급증하고 있다. 그러나 그 이면에는 개인정보유출과 프라이버시(privacy) 침해 가능성으로 인해 정보보호에 대한 우려도 급증하고 있다. 핀테크 서비스는 안정성 보다는 편의성 개선을 더 중요하게 고려하므로 결제처리, 인증방식 등의 간소화와 네트워크로 연결되어 있는 개방적 구조로 인해 이전의 결제 환경보다 심각한 보안위험에 노출되어 있다. 핀테크 산업은 다양화, 지능화되고 있는 보안 위협으로의 불안, 개인정보유출 우려, 정보프라이버시 침해 문제 등으로 핀테크 이용에 대한 저항요인이 발생하여 시장 활성화가 지연될 여지가 있다. 핀테크 서비스 이용의 초기 저항이 극복된다면 핀테크 서비스의 지속적

인 이용과 확산이 가능하게 될 것이다. 이를 위해서는 무엇보다 정보보호와 프라이버시 이슈를 해결해야만 한다.

핀테크 서비스의 보안 위험으로부터 개인 및 조직을 보호하기 위해 중앙정부, 금융당국, 핀테크 관련 기업 및 연구소들은 다양한 법적, 제도적 장치를 마련하고 있다. 핀테크 보안위협 대응을 위한 보안도구 개발과 같은 기술적 측면의 연구수행과 정보보호에 관한 법률 제정, 보안활동 지침과 정보보호정책 개발, 그리고 위협대응방안 등과 같은 정보보안 방법론을 개발하고 있다. 그러나 현재 핀테크 이용자들은 보안도구를 적극적으로 이용하지 않으며, 정보 프라이버시 침해를 최소화하기 위한 대책이나 정보보안 지침을 준수하지 않는 경우가 많다. 이는 PC보안(인터넷결제)에 비해 모바일보안(핀테크 결제)의 취약점과 위험의 심각성을 인지하지 못하기 때문이다. 정보보호 및 보안행동은 법적, 제도적 장치 마련과 기술적인 노력만으로는 해결될 수 없으며, 핀테크 서비스 이용자들은 결제환경에서 개인정보의 중요성을 인식하고 스스로 위험관리 노력과 정보보호 정책을 준수하는 노력을 기울여야 한다. 즉, 정보보호 및 보안행동은 스스로 개인정보를 보호하려는 행동 또는 정보유출 위협으로부터 예방하려는 부정적 관점과 이용자의 인지적 관점에서 접근해야 한다.

따라서 본 연구의 목적은 시장 확산 초기 단계에 있는 국내 핀테크 서비스 활성화를 위해 정보보안 기술적 관점이 아닌 이용자의 인지적 관점과 예방적 관점에서 핀테크 이용자들에게 개인정보 및 프라이버시 보호에 대한 중요성을 인식시키고, 스스로 프라이버시 보호 및 정보보호 행동을 취할 수 있도록 함이다. 핀테크 서비스 이용자들이 개인정보 유출과 정보 프라이버시 침해 등의 정보보호행위의 중요성을 인지하고 있는지 그리고 핀테크 이용자들이 정보보호행위를 하는 원인은 무엇인지 실증적으로 검증하기 위해 전통적으로 예방 의료행위와 건강행동을 설명하는 다양한 건강행동이론(Theories of Health Protective Behaviors)들과 기술위협회피이론(Technology Threat Avoidance Theory)을 적용하여 핀테크 서비스 이용자의 개인정보보호 행동에 미치는 영향을 살펴보고자 한다.

Ⅱ. 이론적 배경

2.1. 핀테크 서비스 관련 연구

최근까지 진행된 핀테크 서비스 관련 연구들은 핀테크 시장 동향 분석, 핀테크 비즈니스 모델 탐색에 관한 연구, 글로벌 핀테크 기업의 정보보호 기술 및 정책 분석, 핀테크 보안위협 분석 및 보안대책에 관한 연구, 핀테크 보안위협 대응을 위한 보안도구 개발 연구, 핀테크 산업 발전을 위한 법적 과제에 관한 연구, 핀테크 산업 생태계에 적합한 법 제정(규제특례제도)에 관한 연구 등의 주로 기술적인 연구와 법제적인 성격의 연구가 수행되었다.

최창열과 함형범(2015)은 국내외 핀테크 기업의 현황 및 비즈니스 모델 분석에 관한 연구에서 핀테크 서비스의 성격과 유형을 전통적(traditional) 핀테크와 신흥(emergent) 핀테크 서비스로 분류하였다. 전통적 핀테크는 금융회사 업무 지원을 위한 정보기술 솔루션과 금융

소프트웨어를 의미하고, 신흥 핀테크 서비스는 크라우드 펀딩(crowd funding), 인터넷전문은행, P2P(Peer-to-Peer)대출 등의 새로운 금융서비스를 의미한다.

박서기(2015)는 핀테크 산업동향을 분석하고 핀테크 비즈니스 모델을 탐색하였다. 핀테크 스타트업을 지급결제, 자금이체, 자산관리, 전자지갑, 크라우드 펀딩, 금융분석 솔루션의 6가지 서비스 유형으로 분류하였다. 핀테크 비즈니스 모델의 특징으로는 수수료 절감, 서비스 이용용이성 증대, 빠르고 간편한 서비스 등을 언급하였다.

박혜영(2016)은 핀테크 전문가를 대상으로 비대면 조사를 실시하여 핀테크 산업 현황을 조사하고 국내 핀테크 시장의 경쟁력을 글로벌 시장과 비교 분석하였다. 핀테크 산업 영역 중 송금과 결제 분야는 국내 경쟁력이 높다고 평가하였으나 금융데이터 분석 분야는 사업화를 위한 데이터 분석 기술 역량 강화가 필요하다고 주장하였다. 빅데이터, 인공지능, 기계학습 기술력과 산업 여건, 인력 등 원천 기술 개발 인프라가 주요 선진국에 비해 취약하다고 주장하였다.

정준호와 김정숙(2015)은 국내외 핀테크 시장 동향 분석과 보안이슈에 관한 연구를 수행하였다. 이들은 액티브엑스와 같은 보안 모듈의 추가 설치 없는 사용자 인증과 사전에 입력한 카드 및 계좌정보에 대한 암호화 및 무결성에 대한 지원을 보안이슈로 제기하였다.

문병순(2015)은 국내외 핀테크 산업동향을 분석하고, 한국과 미국의 핀테크 산업 규제 이슈를 검토하였다. 국내 핀테크 산업에서 자산관리 영역은 개인정보보호 규제로 영업이 쉽지 않은 실정이고, P2P 대출과 인터넷전문은행의 경우 영업은 가능하나 개인정보보호 규제로 경쟁력을 갖추기 힘들다고 언급하면서 비식별화된 개인정보활용 방안을 포함한 네거티브 방식의 규제 개선 필요성을 주장하였다.

유재필과 허세경(2015)은 해외 주요 핀테크 서비스 기업의 정보보호기술 및 정책을 분석하고, 국내 핀테크 산업의 보안 추진방향을 제시하였다. 이들은 애플페이(Apple Pay)의 보안인증 기술과 페이팔(PayPal)의 부정거래탐지시스템(Fraud Detection System) 및 리스크통합관리시스템(Risk Integrated Management System)을 소개하면서, 국내 핀테크 산업은 이용자 편의를 우선적으로 고려해야 하고, 모든 보안 기술은 글로벌 표준을 지향해야 한다고 주장하였다.

박정국(2015)은 핀테크 서비스 특성과 보안위협을 분석하고 핀테크 보안대책을 제시하였다. 핀테크 서비스 제공자는 보안대책을 수립함에 있어 정부의 핀테크 보안정책에 대한 명확한 이해를 바탕으로 안전성 확보방안을 수립해야 하며, 핀테크 이용자는 보안인식을 강화할 필요가 있다고 주장하였다.

이우석과 홍보경(2015)은 핀테크 현황과 법적 과제 분석에 관한 연구에서 핀테크 산업 발전을 위한 법적 과제를 제시하였다. 이들은 진입장벽이 높은 전자금융거래법과 여신전문금융업법의 검토 필요, 사전규제 최소화와 규제 예측성 제고, 금융권 자율보안체계 구축, 정보보호 및 금융보안 입법 노력 강화, 오프라인 위주의 금융제도 개편 등을 주장하였다.

곽관훈(2016)은 지급결제의 전자금융거래법, 송금・환전에 관한 은행법과 금융실명법, 투자

중개의 자본시장법 등을 분석하고, 핀테크 산업의 생태계에 적합한 법 제정(규제특례제도)의 필요성을 주장하였다. 또한 핀테크와 같은 혁신 기술 서비스의 경우 규제를 일일이 나열하고 사전승인을 받는 구체적인 규제는 기술발전을 저해하는 원인이라고 지적하였다.

강영모 등(2016)은 글로벌 핀테크 기업의 정보보안체계에 관한 연구에서 페이팔(PayPal), 알리페이(Alipay), 구글월렛(Google Wallet)의 핀테크 정보보안체계와 사고배상책임 제도를 분석하였다. 이들은 국내 핀테크 기업이 정보보안 통합관리시스템(Information Security Integrated Management System)을 구축해야 하며, 정부차원에서는 정보보안 산업육성 전략을 마련해야 한다고 주장하였다.

정보보호에 대한 기술적, 법적 논의 외에도 이용자 스스로 개인정보의 중요성을 인지하고 피해를 예방하는 행동에 관한 논의는 상대적으로 부족한 실정이다. 따라서 본 연구는 보안도구 개발과 같은 기술적 측면과 정보보안 방법론적 연구가 아닌 핀테크 이용자의 인지적 관점에서의 행동학적 접근방법을 통한 연구를 수행하고자 한다.

2.2 건강행동이론(Theories of Health Protective Behaviors)과 기술위협회피이론(Technology Threat Avoidance Theory)

핀테크 서비스는 보안위협으로부터 개인정보보호 및 정보보안행위가 매우 중요하며 이들 행위는 중대한 병이나 질병을 예방하기 위해 수행하는 예방적 건강행위와 유사한 특징을 지닌다(Ng et al., 2009). 따라서 건강행동과 관련

<표 1> 건강신념 및 건강행동(보호행동)에 적용된 이론과 모형

연구자	이론 및 모형	주요 선행요인	결과 변인
Rosenstock (1974)	Health Belief Model (HBM)	지각된 개연성, 지각된 심각성, 지각된 유익성, 지각된 장애성	예방행동 (건강행동)
Fishbein & Ajzen(1975)	Theory of Reasoned Action (TRA)	행동에 대한 태도, 주관적 규범	행동(건강행동)
Ajzen(1991)	Theory of Planned Behavior (TPB)	행동에 대한 태도, 주관적 규범, 지각된 행동 통제	행동(건강행동)
Weinstein (2000)	Precaution Adoption Process Model (PAPM)	지각된 심각성, 지각된 취약성, 신념단계	예방행동 (보호행동)
Rogers(1983)	Protection Motivation Theory (PMT)	지각된 개연성, 지각된 심각성, 반응효능감, 자기효능감	질병예방행동
Liang & Xue(2009)	Technology Threat Avoidance Theory (TTAT)	위협판단, 대처판단	위협회피행동

된 이론이나 모형 등을 적용하여 개인정보보호 및 정보보안행위를 설명할 수 있다.

의료 및 보건 분야에서 널리 알려진 건강행동이론(Theories of Health Protective Behaviors, THPB)은 건강을 보호하거나 추구하려는 행동을 예측하고 이를 설명하기 위한 이론과 모형을 말한다. <표 1>과 같이 개인이 건강을 추구하는 행동을 할 것인지 예측하거나 또는 건강예방행위를 설명하기 위해서 건강신념모형(Health Belief Model), 합리적 행위이론(Theory of Reasoned Action), 계획된 행동이론(Theory of Planned Behavior), 예방채택과정모형(Precaution Adoption Process Model), 보호동기이론(Protection Motivation Theory), 기술위협회피이론(Technology Threat Avoidance Theory) 등이 적용되었다.

건강행동이론 중 가장 대표적인 모형은 Rosenstock(1974)이 제안한 건강신념모형(Health Belief Model, HBM)이다. 사회인지이론(Social Cognitive Theory)을 이론적 기반으로 삼고 있는 HBM은 질병을 예방하기 위한 건강행동에는 신념(belief)이 가장 중요한 역할을 하며 사람들이 건강을 추구하는 예방행동(건강행동)을 할 것인지 예측하고 설명할 수 있는 4가지 신념변인을 제시하였다. 첫 번째로, 질병 위협(threats)에 대한 지각된 개연성(Perceived Susceptibility)과 지각된 심각성(Perceived Severity)을 제시하였다. 지각된 개연성은 질병에 걸릴 가능성이나 질병에 노출된 정도에 대해 개인이 주관적으로 인지하는 정도이며, 지각된 심각성은 질병으로 초래할 수 있는 부정적 결과(장애의 심각성)에 대해 개인이 지각하는 것이다. 다음으로 신념은 행위에 대한 기대(expectation)로 나타나며 행위에 대한 지각된 유익성(Perceived Benefits)과 지각된 장애성(Perceived Barriers)을 제시하였다. 지각된 유익성은 건강증진 행동이 이득이 됨을 지각하는 것(위험요인의 제거나 감소를 지각)이고, 지각된 장애성은 건강행동에서 발생 가능한 부정적인 결과와 더불어 건강증진 행동에 장애가 되는 것(예: 경제적 비용)을 지각하는 것을 말한다(Becker & Rosenstock, 1984, Rosenstock et al. 1994). 지각된 개연성, 지각된 심각성, 지각된 유익성, 지각된 장애성에 대한 신념이 크거나 작을수록 건강을 보호하거나 추구하려는 행동을 적극적으로 수행한다. 지각된 개연성과 지각된 심각성에 의해 위협감이 형성되어 행동 가치가 부여되고, 지각된 유익성과 지각된 장애성에 의해 그 가치가 평가(행동평가)되어 바람직한 건강행위 이행으로 나타나게 된다. 최근에는 HBM의 주요 변수를 기반으로 HBM의 설명력을 높이고자 다양한 분야에서 확장된 HBM과 다른 건강행동이론과의 통합모형이 제시된 바 있다.

합리적 행위 이론(Theory of Reasoned Action, TRA)은 사회심리학자인 Fishbein and Ajzen(1975)이 기대-가치이론(Expectance-Value Theory)을 확장하여 정립한 이론으로 사람들이 어떤 행동(행위)을 결정하기 전에 관련된 정보를 합리적이고 체계적으로 사용하며 행동의 결과에 대해 신중히 고려한 다음에 비로소 행동한다고 가정한다. 행동을 직접적으로 결정하는 것은 행위의도이며 행동에 대한 태도와 주관적 규범이 행위의도에 영향을 미치게 된다. Rogers(1983)를 비롯한 많은 연구자들은 TRA를 건강행동에 적용하여 건강행동에 대한 태도

와 주관적 규범이 상호작용하여 건강행동의도와 행동에 유의한 영향을 미친다고 주장하였다.

Ajzen(1991)은 TRA에 지각된 행동통제력 변인을 추가하여 행동의도와 행동을 예측하는 계획된 행동이론(Theory of Planned Behavior, TPB)을 제시하였다. TPB에서는 행동의도에 영향을 미치는 행동에 대한 태도와 주관적 규범 이외에 사회심리학의 자기효능감(Self-Efficacy)에서 비롯된 지각된 행동통제가 영향을 미치며 이 변인은 행동에도 직접적인 영향을 준다고 주장하였다. 지각된 행동통제력은 그 사람이 바라는 행동적 결과를 달성하는 것이 가능한가에 대한 신념으로 과거의 행동 경험과 장애물을 극복할 수 있는 자기 능력에 대한 지각을 나타낸다. 건강행동에 적용하면, 건강행동을 쉽게 통제하여 수행할 수 있다고 믿는 사람들이 그 행동의 수행에 대한 통제력이 거의 없다고 믿는 사람들에 비해 그 행동을 수행하려는 의도가 높다는 것이다.

예방채택과정모형(Precaution Adoption Process Model, PAPM)은 HBM, TRA, TPB 등의 건강행동이론이 질병 및 장애에 대한 사람들의 지각된 심각성이나 취약성에만 제한된 관심을 갖고 건강행동 준비가 단계에 따라 달라진다는 점을 간과하였다고 비판하였다(Weinstein, 2000). PAPM은 사람들이 자신의 건강을 보호하기 위해 새롭고 복잡한 예방 행동을 시작하는 시점에서 자신의 취약성에 관한 신념의 단계를 거친다고 주장하였고, 대처평가 요인인 자기효능감과 반응효능감의 필요성을 제기하였다.

보호동기이론(Protection Motivation Theory, PMT)은 Rogers(1983)가 사회심리학과 의료·보건 분야에서 개인이 지각된 위험에 대해 어떠한 태도변화와 행동을 보이는가를 설명하기 위해 HBM을 확장한 이론이다. PMT는 특정 건강행동 채택의향을 결정하는 요인으로 위협평가 과정(threat appraisal process)과 대응평가 과정(coping appraisal process)의 두 가지 인지과정을 제시하였고, 이들을 통해 보호동기가 유발된다고 주장하였다. 위협평가 과정은 위험의 심각성(severity)과 그 위험에 처하게 될 취약성(vulnerability)이라는 하위 개념으로 파악된다. 심각성은 문제가 되는 사안이 얼마나 심각하고 위협적인가를 말하고, 취약성은 그 위험에 자신이 연루될 가능성 정도를 말한다. 대응평가 과정은 반응효능감(response-efficacy)과 자기효능감(self-efficacy)으로 구성되는데, 반응효능감이란 위험에 대처하는 대안적 행동이 위험을 감소시키고 이로 인해 얻어지는 혜택에 대한 믿음을 말하고, 자기효능감은 그 행동을 수행할 수 있는 자신의 능력에 대한 확신의 정도를 말한다.

마지막으로 기술위협회피이론(Technology Threat Avoidance Theory, TTAT)은 이용자들의 IT위협과 회피행위를 설명하기 위해 사회심리학 분야의 접근-회피 동기이론(Approach-Avoidance Motivation Theory)을 기반으로 하고 있다(Elliot, 1999). 접근-회피 동기이론에서 인간은 환경에 대해 긍정적이고 바람직한 일이 발생할 가능성에 의해 유발되는 접근행동과 부정적이고 바람직하지 못한 일에 유발되는 회피행동이라는 두 가지 행동 양상을 보인다고 주장한다. 만약 조직구성원들이 특정 IT를 이용하면서 부정적인 반응이 유발된다면 회피동기를 가지게 되고, 이것이 위협 요소로 인지된다면

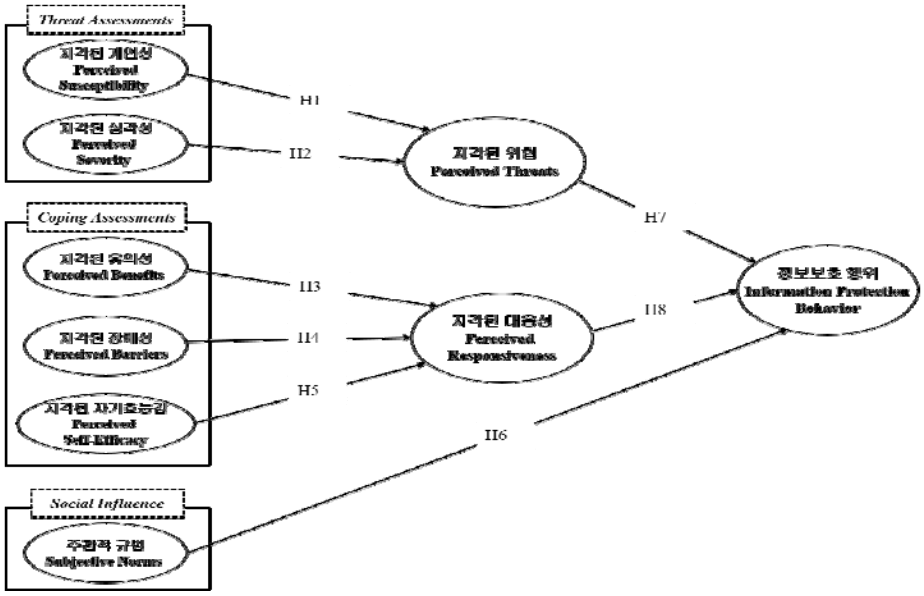
사용자들은 이에 대처하는 행동을 취하게 된다는 것이다. Liang and Xue(2009)는 지능형 지속위협, 바이러스의 피해, 개인정보유출, 지능화된 사이버 범죄와 같은 정보화의 역기능으로 개인의 정보기술 위협을 회피하려는 IT사용자의 행동을 설명하기 위해 기술위협회피이론(TTAT)을 제안하였다. TTAT는 사용자가 IT위협 판단과 IT위협에 대처하는 대처 판단이라는 두 개의 인식론적 프로세스를 거친다고 주장한다. 위협 판단은 대처 판단을 이끌 것이고 사용자들은 지각된 유익성, 지각된 비용, 자기효능감 등을 통해 IT위협이 회피될 수 있는 정도로 평가한다. 만약 IT위협을 회피될 수 있다고 판단되면 문제 중심적 대처를 취할 것이고, IT위협이 완전히 회피될 수 없다고 판단되면 감정 중심적 대처를 취하게 될 것이다.

이와 같이 건강행동 관련이론들은 주로 개인의 질병예방 활동과 식품의 안정성 평가와 관련된 분야에서 적용되었고, 최근에 IT분야에서 정보보호행위를 설명하기 위해 이들 이론을 적용한 연구가 수행되고 있으나 핀테크 서비스와 같은 혁신 IT서비스의 정보보호행위에 관한 연구는 부족한 실정이다.

Ⅲ. 연구 설계

3.1. 연구 모형

본 연구는 건강신념 및 건강예방행동에 관한 HBM, PMT 이론과 IT위협회피이론인 TTAT를 기반으로 핀테크 서비스 이용자의 정보보호행위에 미치는 영향요인을 알아보고자 한다. 구체적으로 핀테크 서비스 이용자의 정보보호행위 영향요인으로 건강신념변인, 보호동기요인, 그리고 사회적 영향변수를 제시하였다. 건강신념변인의 위협평가요인에는 지각된 개연성과 지각된 심각성을 제시하였고, 대응평가요인에



<그림 1> 연구모형

는 지각된 유익성, 지각된 장애성, 지각된 자기효능감, 그리고 사회적 영향변수로는 주관적 규범을 제시하였다. 지각된 위협과 지각된 대응성을 매개변수로 설정하였고, 종속변수는 개인정보보호행위이다. 본 연구모형은 <그림 1>과 같다.

3.2. 건강신념변인(위협평가요인)과 지각된 위협과의 가설

본 연구는 핀테크 서비스의 정보보호행위 영향요인 중 위협평가요인으로 지각된 개연성과 지각된 심각성을 제시하였다. 이들 영향요인이 지각된 위협에 미치는 영향에 관한 가설은 다음과 같다.

대표적인 건강신념변인인 지각된 개연성과 지각된 심각성은 PMT에서 언급된 위협평가 과정에 속한다. 위협평가 과정은 두려움과 위협에 반응하는 행위를 설명하는데 매우 유용하다(Workman et al., 2009). Rosenstock et al.(1994)은 사람들이 위협평가 과정을 통해 위협을 인식하다고 주장하면서 지각된 개연성과 지각된 심각성 변인의 중요성을 강조하였다. 지각된 개연성은 자신을 포함한 주변인들이 핀테크 보안위험에 노출되기 쉽다고 인지하는 정도를 말하며, 지각된 개연성이 높을수록 정보보호행동을 취할 가능성이 높다고 판단할 수 있다. 또한 지각된 심각성은 핀테크 보안위협으로 초래할 수 있는 경제적, 심리적, 사회적으로 부정적인 결과에 대한 지각이나 문제의 심각성, 해결의 필요성, 피해정도의 심화가능성으로 측정할 수 있다. 지각된 위협은 개인정보유출이 위협적이라고 개인이 지각하는 정도를 말한다(Liang & Xue, 2009, 2010). Rogers(1983)는 PMT에서 지각된 개연성과 지각된 심각성이 지각된 위협에 유의한 영향을 미친다고 언급하였다. Liang and Xue(2010)는 개인용 컴퓨터 사용자의 IT위협-회피 행동에 관한 연구에서 지각된 개연성과 지각된 심각성이 지각된 위협에 유의한 영향을 주고, 이들이 IT위협-회피 행동에도 유의한 영향을 준다고 언급한 바 있다. Prati et al.(2011)은 인플루엔자(influenza) 바이러스 위험인식과 예방보호행동에 관한 연구에서 지각된 개연성과 지각된 취약성이 지각된 공포(위협)에 유의한 영향을 미친다고 언급하였다. 지범석 등(2011)은 HBM 기반의 정보품질을 위한 정보보호행위에 관한 연구에서 개인정보유출에 관한 지각된 심각성과 지각된 개연성이 지각된 위협에 유의한 영향을 미친다고 주장하였다. 김상희와 김종기(2016)는 프라이버시 계산모델(Privacy Calculus Theory)을 기반으로 온라인 환경에서의 프라이버시 의사결정 영향요인으로 지각된 개연성, 지각된 심각성, 반응효능감, 자기효능감을 제시하였다. 이들 영향요인 중 지각된 개연성과 지각된 심각성이 프라이버시 위협에 유의한 영향을 미친다고 주장하였다. 마지막으로 장유진과 김영욱(2016)의 일본 원전사고 이후 식품의 위험인식 및 행동의도에 관한 연구에서도 지각된 개연성과 지각된 심각성이 지각된 위협에 유의한 영향을 미치는 것으로 나타났다. 이상의 이론적 배경을 토대로 핀테크 서비스의 정보보호행위 영향요인 중 위협평가 요인이 지각된 위협에 영향을 미칠 것이라는 다음과 같은 가설을 제시한다.

[가설 1] 핀테크 서비스에서 보안위험에 노출되기 쉽다고 인지하는 지각된 개연성은 지각된 위협에 정(+)의 영향을 미칠 것이다.

[가설 2] 핀테크 서비스에서 개인정보가 유출됨으로 발생할 수 있는 지각된 심각성은 지각된 위협에 정(+)의 영향을 미칠 것이다.

3.3. 건강신념변인(대응평가요인)과 지각된 대응성과의 가설

본 연구는 핀테크 서비스의 정보보호행위 영향요인 중 대응평가요인으로 지각된 유익성, 지각된 장애성, 지각된 자기효능감을 제시하고자 한다. 이들 영향요인이 지각된 대응성에 미치는 영향에 관한 가설은 다음과 같다.

지각된 유익성은 핀테크 보안정책을 준수하고 정보보호행동 등의 위협을 감소시키는 행동의 효과에 대한 개인의 믿음이나 주관적 기대정도를 말한다. 핀테크 정보보호정책을 수행함으로써 받게 되는 혜택을 인지한다면 불편함에도 정보보호행동을 수행할 것이다. 지각된 장애성은 핀테크 보안정책을 준수하는 행위와 정보보호행동 및 프라이버시 보호행위의 결과가 부정적인 것이라고 지각하거나 또는 경제적 비용으로 인해 핀테크 정보보호행위에 장애가 발생하는 것을 말한다.

매개변수로 제시한 대응성(Responsiveness)의 사전적 의미는 어떤 발생 사태에 맞추어 적절하고 호의적으로 반응하는 것을 말한다. 건강행동이론에서는 지각된 대응성(perceived responsiveness)을 질병으로부터 위협을 감소시킬 수 있는 행위에 대한 상대적인 효과성이라고 정의한다(Rosenstock et al., 1994; Jones et al., 2015). 지각된 대응성은 다양한 기호를 포함한 패스워드 지정 및 패스워드의 주기적 변경, 바이러스 및 악성코드 방지 프로그램 설치 등과 같은 보호대응과 보호대책이 개인정보유출 방지와 정보보호가 가능한지에 대한 개인의 평가를 말한다(Liang & Xue, 2009).

Rosenstock(1974)과 Rogers(1975)는 건강예방행동을 설명하기 위해 HBM을 적용하여 지각된 유익성, 지각된 장애성이 지각된 대응성에 유의한 영향을 미칠 것이라고 주장하였다. Stillman(1977)은 여성 건강신념과 유방암 예방행동에 관한 연구에서 지각된 유익성, 지각된 장애성이 지각된 대응성에 유의한 영향을 미친다고 언급하였다. Volk and Koopman(2001)은 케냐(Kenya)인의 에이즈(AIDS) 예방행동에 관한 연구에서 건강신념변인 중 지각된 유익성과 지각된 장애성이 지각된 대응성(콘돔사용)에 유의한 영향을 미치는 것으로 나타났다. 또한 Liang and Xue(2010)는 지각된 효과성(지각된 유익성)과 자기효능감이 지각된 대응성에 유의한 영향을 미친다고 언급한 바 있다. 국내 연구로 지범석 등(2011)은 정보품질을 위한 정보보호행위 요인인 지각된 유익성(반응효능감)과 자기효능감이 지각된 대응성에 유의한 영향을 미친다고 주장하였다. 장국현 등(2016)은 환경경영에서 HBM을 이용한 병원환경이 건강예방행동에 미치는 영향요인으로 지각된 개연성, 지각된 심각성, 지각된 유익성, 지각된 장애성을 제시하였다. 이들 요인 중에서 지각된 유익성과 지각된 장애성이 지각된 대응성에 유의한 영향을 미친다고 언급하였다.

대응평가요인으로 제시한 지각된 자기효능감은 핀테크 서비스에서 보안위협을 막기 위해 보안도구를 실행하거나 보안정책을 준수할 수 있다는 자신의 능력에 대한 믿음을 의미한다. Ifinedo(2012)는 정보시스템 보안정책 준수에

관한 연구에서 PMT와 TPB을 통합한 연구모형을 제시하였다. 정보시스템 보안정책 준수의 영향요인으로 지각된 심각성, 지각된 취약성, 자기효능감, 반응효능감, 주관적 규범 등을 제시하면서 자기효능감 변인의 중요성을 강조하였다. 배재권(2014)은 개인용 클라우드(personal cloud) 서비스의 개인정보보호행위에 관한 연구에서 지각된 자기효능감이 지각된 대응성에 유의한 영향을 미치고, 지각된 대응성은 정보보호행위에 유의한 영향을 미친다고 주장하였다. 또한 김정은 등(2016)과 신세미 등(2016)은 소셜네트워크서비스(Social Network Services, SNS) 환경에서의 정보보호행위에 관한 연구에서 지각된 자기효능감이 지각된 대응성에 유의한 영향을 미친다고 언급한 바 있다. 이상의 이론적 배경을 토대로 핀테크 서비스 이용자의 정보보호행위 영향요인 중 대응평가요인은 지각된 대응성에 영향을 미칠 것이라는 가설을 제시한다.

[가설 3] 핀테크 서비스 환경에서의 지각된 유익성은 지각된 대응성에 정(+)의 영향을 미칠 것이다.

[가설 4] 핀테크 서비스 환경에서의 지각된 장애성은 지각된 대응성에 정(+)의 영향을 미칠 것이다.

[가설 5] 핀테크 서비스 환경에서의 지각된 자기효능감은 지각된 대응성에 정(+)의 영향을 미칠 것이다.

3.4. 주관적 규범, 지각된 위협, 지각된 대응성과 개인정보보호행위와의 가설

사회적 영향(social influence)은 주변에 있는 중요한 사람들이나 집단의 규범에 의한 영향력을 의미한다. 이용자들이 새로운 기술을 수용할 경우 준거집단의 규범, 사회적 영향, 그리고 태도에 영향을 받는다. Fulk et al.(1987)은 사회적 영향정도란 동료 및 주변 사람들이 특정 제품과 서비스를 이용하는 분위기나 평가(피드백) 정보에 영향을 받는 정도라고 주장하면서 사회적 영향모델(social influence model of technology use)을 제시하였다. Liang and Xue(2009)는 사회적 영향변수의 중요성을 언급하면서, 혁신기술 이용자의 IT위협-회피 행동에도 영향력 있는 변수라고 주장하였다. 주관적 규범(Subjective Norms)은 행위자가 속한 준거집단들이 예방행위에 대해 가지고 있는 태도 및 평가를 말하는 것으로 대표적인 사회적 영향변수이다(Fishbein & Ajzen, 1975). 주관적 규범은 대인 간 상호작용과 관련된 변인으로 정보보호행위에 직접적인 영향을 미치는 요인이다. 핀테크 환경에서 정보보호행위는 위험에 대처하기 위한 개인 스스로의 위험 인식과 연관성이 있으며, 준거집단의 태도가 개인의 위험인식에 영향을 미친다. 따라서 주관적 규범은 핀테크 서비스의 보안위협에 대한 인식과 정보보호행위의도에 영향을 미칠 가능성이 크다. 최근 소셜미디어(social media) 영역의 발전으로 IT분야에서 집단 구성원 간 상호작용의 영향력이 크게 나타나므로 사회적 영향변수의 중요성은 날로 커질 것이다.

Jones et al.(2006)은 건강 예방행동의도 및 위험인식 연구에서 주관적 규범이 행동의도에 유의한 영향을 미친다고 주장하였다. 장유진과 김영욱(2016)은 지각된 취약성, 지각된 심각성, 주관적 규범 등의 요인을 식품의 예방행동의도

요인으로 제시하였고, 주관적 규범은 예방행동 의도에 유의한 영향을 미친다고 주장하였다.

Rosenstock(1974)이 제안한 HBM에서는 지각된 위협 요인이 보호행동에 영향을 미치는 주요 요인으로 언급하였다. Rosenstock(1974)을 비롯한 많은 연구자들은 HBM과 PMT에서

<표 2> 연구가설과 관련된 건강행동 및 IT관련 이론

연구주제	이론 및 모형주)	독립변수	매개변수 및 종속변수	참고문헌
여성건강신념과 유방암 예방행동	HBM, PMT	개연성, 심각성, 유익성, 장애성	지각된 대응성(매개), 예방행동	Stillman(1977)
에이즈(AIDS) 예방행동	HBM	개연성, 심각성, 유익성, 장애성	지각된 대응성(매개), 예방행동	Volk & Koopman (2001)
PC사용자의 정보기술 위협회피행동	TTAT	개연성, 심각성, 효과성, 비용 자기효능감	지각된 위협(매개), 지각된 회피성(매개), IT위협회피행동	Liang & Xue (2009, 2010)
정보시스템 보안행동	HBM, PMT	개연성, 심각성, 반응효능감	정보시스템 보안행동	Workman et al.(2009)
바이러스 위험 인식과 예방보호행동	SCM, PMT	사회상황요인, 개연성, 심각성, 반응효능감	예방보호행동	Prati et al. (2011)
정보시스템 보안 정책 준수	TPB, PMT	개연성, 심각성, 반응효능감, 자기효능감, 주관적규범	정보시스템 보안 정책 준수 의도	Ifinedo(2012)
빅데이터 환경에서의 정보보호행위	HPT, PMT, TPB	개연성, 심각성, 반응효능감, 자기효능감, 주관적규범	정보보호행위의도	Bae(2016)
온라인 환경에서 프라이버시 의사결정요인	PMT, PCT	개연성, 심각성, 반응효능감, 자기효능감	지각된 위협(매개) 정보제공의도	김상희, 김종기(2016)
식품 위험인식 및 행동의도	HBM, TPB, EPPM	주관적 규범 미디어노출	지각된 개연성(매개), 지각된 심각성(매개), 지각된 위협(매개), 예방행동의도	장유진, 김영욱(2016)
병원환경의 대응성과 예방행동	HBM, PMT	개연성, 심각성, 유익성, 장애성	지각된 대응성(매개), 건강가치성(매개), 예방행동	장국현 등 (2016)

주) HBM: Health Belief Model, PMT: Protection Motivation Theory
TTAT: Technology Threat Avoidance Theory, SCM: Social Cognitive Model
TPB: Theory of Planned Behavior, HPT: Health Psychology Theory
PCT: Privacy Calculus Theory, EPPM: Extended Parallel Process Model.

지각된 개연성과 심각성으로 인한 지각된 위협이 보호행동 및 예방행동에 유의한 영향을 미친다고 주장하였다(Rosenstock et al., 1994; Rogers, 1975, 1983). Jones et al.(2015)은 인플루엔자(influenza) 바이러스에 대한 보호행동에 관한 연구에서 지각된 위협이 바이러스 예방행동에 유의한 영향을 미친다고 주장하였다.

PMT에서는 지각된 대응성 또한 건강보호행동에 유의한 영향을 미친다고 주장하였다. Volk and Koopman(2001)은 지각된 대응성이 에이즈(AIDS) 예방행동에 유의한 영향을 미친다고 언급한 바 있다. 배재권(2014)은 지각된 대응성이 개인용 클라우드 정보보호행위에 유의한 영향을 미친다고 주장하였고, 김정은 등(2016)과 장국현 등(2016)에서도 지각된 대응성이 건강예방행동에 유의한 영향을 미친다고 주장하였다. 핀테크 환경에서 핀테크 보안위협을 인지하고 대응성의 요소들을 파악하여 예방행동 매뉴얼과 정보보호 정책을 수립하고 이를 활용하기 위한 정기적 교육과 캠페인 활동 등을 통해 정보보호활동을 성공적으로 수행하는 것이 무엇보다 중요하다. 이상의 이론적 배경을 토대로 주관적 규범, 지각된 위협, 지각된 대응성과 개인정보보호행위 간의 가설은 다음과 같다.

[가설 6] 핀테크 서비스 환경에서 주관적 규범은 정보보호행위에 정(+)의 영향을 미칠 것이다.

[가설 7] 핀테크 서비스 환경에서 지각된 위협은 정보보호행위에 정(+)의 영향을 미칠 것이다.

[가설 8] 핀테크 서비스 환경에서 지각된 대응성은 정보보호행위에 정(+)의 영향을 미칠 것이다.

이상으로 핀테크 서비스의 정보보호행위 영향요인과 지각된 위협, 지각된 대응성, 그리고 개인정보보호행위 간에 관련된 8가지 가설을 제시하였다. 이들 가설의 인과관계에 관한 이론적 근거를 <표 2>에 요약하였다.

Ⅳ. 연구 방법: 조작적 정의 및 표본 선정

본 연구는 HBM과 PMT의 문헌연구를 기반으로 핀테크 서비스 이용자의 정보보호행위에 관한 개념적 정의와 설문문항을 도출하고 TTAT을 토대로 IT분야의 설문문항을 정보보호행위에 맞게 수정하였다. <표 3>은 연구변수의 조작적 정의와 관련 연구를 정리한 것이다.

설문조사 실시 전, 핀테크 서비스 운영자, 금융정책기관 및 금융기관 실무자, 핀테크 비즈니스 사업가, 단말솔루션업체 등의 실무자와 관련 연구자를 중심으로 설문항목의 적정성 및 내용검토 등의 사전조사(pre-test)를 실시하였다. 설문지 사전조사는 2017년 2월 13일부터 24일까지 실시하여 설문문항의 내용 타당성 및 가독성을 확보하였다.

국내 핀테크 서비스는 주로 모바일 송금 및 결제 등의 지급결제 서비스 이용이 주를 이루고 있어 모바일에서의 핀테크 서비스 이용자를 설문조사 대상자로 선정하였다. 스마트폰 이용자 중 핀테크 서비스를 이용한 경험이 있는 수도권 지역의 이용자를 대상으로 2017년 3월 6일부터 23일까지 18일간 설문조사를 실시하였으며, 설문지는 전문설문조사업체와 연구자가

직접 방문하거나 또는 이메일을 이용해 배포, 회수하였다. 이 기간에 총 325부의 설문이 회수되었으며, 이중 불성실한 답변이 포함된 53부를 제외한 272부의 설문지가 자료 분석에 사용되었다.

마지막으로 회수된 설문지를 바탕으로 통계분석을 시행하였다. 측정모형 검정을 위해 연구변수들의 측정도구에 대한 신뢰성 및 타당성을 분석하고, 구조모형 검정을 위해서는 연구모형의 경로계수와 유의성을 검정하였다.

<표 3> 연구변수의 조작적 정의 및 선행연구

연구 변수	조작적 정의	관련 연구
지각된 개연성 (SUS)	자신을 포함한 주변인들이 핀테크 보안위협에 노출되기 쉽다고 인지하는 정도	Rosenstock(1974); Rogers(1983)
지각된 심각성 (SEV)	핀테크 보안위협으로 초래할 수 있는 경제적, 심리적, 사회적으로 부정적인 결과에 대한 지각이나 문제의 심각성, 해결의 필요성, 피해정도의 심화가능성	Rosenstock(1974); Rogers(1983)
지각된 유익성 (BEN)	핀테크 보안정책을 준수하거나 정보보호행동이 이득이 됨을 지각하는 것	Becker & Rosenstock(1984); Rosenstock et al. (1994)
지각된 장애성 (BAR)	핀테크 보안정책 준수 행위와 정보보호행동의 결과가 부정적인 것이라고 지각하거나 또는 경제적 비용으로 인해 정보보호행위에 장애가 되는 것을 지각하는 것	Becker & Rosenstock(1984); Rosenstock et al. (1994)
지각된 자기효능감 (SEF)	핀테크 서비스에서 보안위협을 막기 위해 보안도구를 실행하거나 보안정책을 준수할 수 있다는 자신의 능력에 대한 믿음	Bandura(1997); Ifinedo(2012)
주관적 규범 (SUB)	행위자가 속한 준거집단들이 정보보호행위에 대해 가지고 있는 태도 및 평가, 정보보호행위에 대한 지각된 사회적 압력	Fishbein & Ajzen (1975); Ifinedo(2012)
지각된 위협 (THR)	핀테크 보안위협(개인정보유출과 프라이버시 침해) 가능성으로 인한 정보보호에 대한 염려 수준	Rogers(1983); Jones et al.(2015)
지각된 대응성 (RES)	효과적인 패스워드 사용 및 패스워드의 주기적 변경 등과 같은 보호대응과 보호대책이 정보유출방지와 정보보호가 가능한지에 대한 개인의 평가	Liang & Xue (2009, 2010); Volk & Koopman (2001)
정보보호행위 (IPB)	핀테크 서비스 환경에서 개인정보를 보호하기 위한 지속적인 행동과 정보보호정책을 준수하려는 적극적인 노력	Workman et al. (2009); Jones et al.(2015)

Ⅴ. 가설 검정

5.1. 표본의 기술적 특성

<표 4>는 총 272개 표본의 성별 및 연령 분포, 직업, 최종학력, 월평균 소득, 핀테크 서비스 이용기간을 포함하는 인구통계학적 특성을 보여준다. 표본의 성별 분포는 남자가 150명(55.15%), 여자가 122명(44.85%)이며, 연령 분포는 30~39세가 110명(40.44%)으로 가장 많았다. 직업은 사무직이 87명(31.99%)으로 가장 많았고, 다음으로 학생이 60명(22.06%), 교육

<표 4> 표본의 인구통계학적 특성

구 분	항 목	응답 수	비 율(%)
성 별	남 성	150	55.15%
	여 성	122	44.85%
연 령	19세 이하	11	4.04%
	20~29세	70	25.74%
	30~39세	110	40.44%
	40~49세	56	20.59%
	50세 이상	25	9.19%
직업	학생	60	22.06%
	사무직	87	31.99%
	공무원	16	5.88%
	교육, 연구직	32	11.76%
	기술직, 기능직	14	5.15%
	판매, 서비스직	28	10.29%
	자영업	20	7.35%
	기타	15	5.51%
최종 학력	고등학교 졸업	18	6.62%
	대학교 재학 (전문대 포함)	48	17.65%
	대학교 졸업	175	64.34%
	대학원 재학	17	6.25%
	대학원 졸업	14	5.15%
월평균 소득	150만원 미만	56	20.59%
	150만원 ~ 250만원 미만	94	34.56%
	250만원 ~ 350만원 미만	62	22.79%
	350만원 ~ 450만원 미만	31	11.40%
	450만원 ~ 550만원 미만	18	6.62%
	550만 원 이상	11	4.04%
핀테크 서비스 이용기간	6개월 미만	19	6.99%
	7~12개월	35	12.87%
	1년~2년	91	33.46%
	2년~3년	74	27.21%
	3년 이상	53	19.49%
합 계		272	100%

· 연구직이 32명(11.76%)으로 나타났다. 최종 학력은 대학교 졸업이 175명(64.34%)으로 가장 높은 비율을 차지하였고, 가구별 월평균 소득은 150~250만원 미만(94명, 34.56%)이 가장 많은 것으로 나타났다. 핀테크 서비스 이용기간으로는 1년~2년이 91명(33.46%)으로 가장 많았고, 그 다음으로 2년~3년이 74명(27.21%)으로 나타나 전체 표본의 약 80.1%가 핀테크 서비스를 1년 이상 이용한 것으로 나타났다.

5.2. 측정모형 검정

회수된 설문지를 바탕으로 측정모형 및 구조모형 검정을 위해 확증적 요인 분석 도구인 *SmartPLS 3.0*을 사용하였다. 측정모형 검정을 위해 연구변수들의 측정도구에 대한 신뢰성 및 타당성을 분석하고, 구조모형 검정을 위해서는 연구모형의 경로계수와 유의성을 검정하였다. 신뢰성 검정을 위해 종합요인 신뢰성 지수(Composite Scale Reliability Index, CSRI)값을 산출하였으며, <표 5>와 같이 모든 연구변수의

<표 5> 연구변수의 내적 일관성 및 수렴 타당성 검정

연구변수	구성개념	요인 값	CSRI	AVE
지각된 개연성 (SUS)	SUS1	0.849	0.823	0.719
	SUS2	0.703		
	SUS3	0.747		
지각된 심각성 (SEV)	SEV1	0.742	0.834	0.634
	SEV2	0.718		
	SEV3	0.985		
지각된 유익성 (BEN)	BEN1	0.826	0.936	0.831
	BEN2	0.955		
	BEN3	0.947		
지각된 장애성 (BAR)	BAR1	0.843	0.927	0.808
	BAR2	0.891		
	BAR3	0.960		
지각된 자기효능감 (SEF)	SEF1	0.763	0.927	0.812
	SEF2	0.942		
	SEF3	0.982		
주관적 규범 (SUB)	SUB1	0.899	0.802	0.602
	SUB2	0.924		
	SUB3	0.779		
지각된 위협 (THR)	THR1	0.940	0.966	0.904
	THR2	0.955		
	THR3	0.957		
지각된 대응성 (RES)	RES1	0.810	0.896	0.742
	RES2	0.858		
	RES3	0.913		
정보보호행위 (IPB)	IPB1	0.930	0.962	0.895
	IPB2	0.962		
	IPB3	0.945		

CSRI값이 0.802에서 0.966사이로 나타나 연구변수의 측정항목은 신뢰성이 있다고 판단된다. 다음으로 측정항목에 대한 수렴타당성과 판별타당성 검증을 위해 확인적 요인분석(Confirmatory Factor Analysis: CFA)을 수행하였다. CFA를 통한 수렴타당성 검증 결과, 모든 연구변수의 요인 값이 기준치 값보다 높은 0.7 이상으로 나타나 수렴타당성이 확보되었다. 마지막으로, 연구변수의 판별타당성 측정을 위해 평균분산추출(Average Variance Extracted, AVE)값을 이용하였다(Fornell & Larcker, 1981). <표 6>과 같이 모든 연구변수들의 AVE 제곱근 값이 0.7보다 크고, 나머지 변수와의 상관계수가 AVE 제곱근 값보다 작게 나타나 판별타당성도 있는 것으로 조사되었다(Chin, 1998).

5.3. 구조모형 검정

구조모형 검정을 위해 *PLS*의 부트스트랩핑(Bootstrapping) 방법을 500회 실시하여 연구모형의 경로계수와 유의성을 검정하였다. 핀테크 서비스 이용자의 정보보호행위에 미치는 영향요인이 지각된 위협과 지각된 대응성, 그리고 개인정보보호행위에 미치는 영향에 관한 가설검정 결과는 <표 7>과 같다. 건강신념변인의 위협평가 요인인 지각된 개연성과 지각된 심각성은 지각된 위협과 모두 유의수준 1%에서 채택되었다(H1, H2). 대응평가 요인인 지각된 유익성과 지각된 자기효능감도 지각된 대응성과

<표 6> 연구변수의 AVE(평균분산추출)값을 통한 판별 타당성 검정

	SUS	SEV	BEN	BAR	SEF	SUB	THR	RES	IPB
SUS	0.848*								
SEV	0.212	0.796*							
BEN	-0.088	-0.055	0.912*						
BAR	0.041	0.086	0.024	0.899*					
SEF	0.009	-0.042	0.054	0.066	0.901*				
SUB	-0.013	-0.037	-0.062	-0.060	-0.022	0.776*			
THR	0.145	0.050	0.020	-0.118	-0.457	0.040	0.951*		
RES	0.055	0.260	-0.109	0.052	0.031	0.036	-0.054	0.861*	
IPB	0.047	0.007	-0.024	-0.427	-0.035	0.133	0.006	-0.114	0.946*

주) *AVE 제곱근 값(Square Root of the AVE).
SUS: 지각된 개연성, SEV: 지각된 심각성, BEN: 지각된 유익성, BAR: 지각된 장애성, SEF: 지각된 자기효능감
SUB: 주관적 규범, THR: 지각된 위협, RES: 지각된 대응성, IPB: 정보보호행위.

<표 7> 경로분석 결과와 가설채택 여부

가설	인과관계	경로계수	T값	P값	검정
H1	지각된 개연성 → 지각된 위협	0.440	6.388	0.000	채택
H2	지각된 심각성 → 지각된 위협	0.271	4.611	0.000	채택
H3	지각된 유익성 → 지각된 대응성	0.313	5.107	0.000	채택
H4	지각된 장애성 → 지각된 대응성	0.052	1.006	0.315	기각
H5	지각된 자기효능감 → 지각된 대응성	0.230	3.789	0.000	채택
H6	주관적 규범 → 정보보호행위	0.638	11.050	0.000	채택
H7	지각된 위협 → 정보보호행위	0.406	6.114	0.000	채택
H8	지각된 대응성 → 정보보호행위	0.519	8.254	0.000	채택

유의수준 1%에서 채택되었다(H3, H5). 그러나 지각된 장애성과 지각된 대응성과의 가설(H4)은 기각되었다. 사회적 영향변수인 주관적 규범과 정보보호행위와의 가설(H6)은 유의수준 1%에서 채택되었고, 지각된 위협, 지각된 대응성과 정보보호행위와의 가설(H7, H8)도 모두 유의수준 1%에서 채택되었다.

Ⅵ. 결론 및 시사점

6.1. 연구결과 요약

혁신적인 아이디어와 첨단기술을 보유하고 있는 비(非)금융 분야의 기업들이 주도하여 IT 기반 금융서비스를 제공하는 핀테크 서비스는 기존의 금융거래 방식과는 차별화된 형태의 비즈니스 모델과 부가가치를 창출하고 있다(이경전 외, 2016). 주요 선진국은 핀테크 기업 육성을 위한 법 규제 완화와 보안기술 공동 개발 등의 전략을 추진하고 있으나 국내 핀테크 사업은 개인정보 유출과 프라이버시 침해 우려 등의 핀테크 활성화 저항요인으로 시장 확산 초기 단계에 머물러 있다. 핀테크 시장의 활성화 속도를 높이기 위해서는 정보보호인식 증대 및 정보보호행위에 관한 대책이 시급하며 이를 위해 이용자 스스로 정보보호행위를 수행하려는 인지적 관점과 정보유출 위협으로부터 예방하려는 부정적 관점에서 접근해야 한다.

본 연구는 핀테크 서비스 이용자들이 개인정보 유출과 정보 프라이버시 침해 등의 정보보호행위의 중요성을 인지하고 있는지 그리고 핀테크 이용자들이 정보보호행위를 하는 원인은 무엇인지 실증적으로 검증하기 위해 건강신념 및 건강행동에 관한 HBM, PMT와 IT위협-회피 이론인 TTAT를 기반으로 핀테크 서비스의 정보보호행위에 미치는 요인들을 파악하고 이들 요인이 정보보호행위에 어떠한 영향을 미치는지 분석하였다. 대표적인 핀테크 비즈니스 모델인 모바일 지급결제 서비스 이용자를 대상으로 설문조사를 실시하였고, 구조방정식 방법론을 채택하여 측정모형과 구조모형을 검정하였다.

본 연구의 주요 연구결과는 다음과 같다.

첫째, 핀테크 서비스의 정보보호행위 영향요인 중 위협평가요인으로 제시한 지각된 개연성과 지각된 심각성은 지각된 위협에 모두 유의한 영향을 미치는 것으로 나타났다. Liang and Xue(2010)는 개인용 컴퓨터 사용자의 지각된 개연성과 지각된 심각성이 지각된 위협에 유의한 영향을 준다고 주장하였으며, Prati et al.(2011)의 연구에서도 지각된 개연성과 지각된 취약성이 지각된 위협에 유의한 영향을 미친다고 언급한 바 있다. 이처럼 지각된 개연성과 지각된 심각성에 의해 위협감이 형성되어 행동 가치가 부여된다는 것을 말한다.

둘째, 핀테크 서비스의 정보보호행위 영향요인 중 대응평가요인으로 제시한 지각된 유익성과 지각된 자기효능감은 지각된 대응성에 모두 유의한 영향을 미치는 것으로 나타났다. Stillman(1977)은 지각된 유익성이 지각된 대응성에 유의한 영향을 미친다고 주장하였으며, Volk and Koopman(2001)은 건강신념변인 중 지각된 유익성이 지각된 대응성에 유의한 영향을 미친다고 주장한 바 있다. Ifinedo(2012)는 정보시스템 보안정책 준수의 영향요인으로 자

기효능감 변인의 중요성을 강조하면서 지각된 자기효능감이 지각된 대응성에 유의한 영향을 미친다고 언급한 바 있다. 그러나 핀테크 서비스 환경에서의 지각된 장애성은 지각된 대응성에 영향을 미치지 않는 것으로 나타났다. 이병관 외(2014)의 HBM을 적용한 국내 연구들의 메타분석 연구에서도 지각된 장애성이 지각된 대응성과 행동의도에 유의한 영향을 미치지 않은 것으로 나타났다. 건강신념모형 관련 연구에서도 지각된 장애의 영향력이 건강신념 변수 중에서 가장 낮은 것으로 검증되었는데, 이는 예방행동에 관한 지각된 장애정도가 높을수록 그 행동을 회피하려는 성향이 높아진다는 것을 의미한다. 따라서 핀테크 환경에서 정보보호행위를 유도하기 위해서는 보호행동이나 정보보호정책 준수 행동으로 인한 잠재적 손해보다 이득이 더 크다는 점을 인지할 수 있는 정보보호 캠페인과 교육, 미디어 노출 및 홍보 등이 필요할 것이다.

셋째, 대표적인 사회적 영향변수인 주관적 규범은 정보보호행위에 유의한 영향을 미치는 것으로 나타났다. Jones et al.(2006)은 건강 예방행동의도 및 위험인식에 관한 연구에서 주관적 규범이 위험인식 및 행동의도에 유의한 영향을 미친다고 주장한 바 있다. 본 연구변수 중 주관적 규범이 핀테크 정보보호행위에 가장 큰 영향을 미치는 것으로 나타났는데 이는 핀테크와 같은 혁신 IT서비스의 경우 준거집단 내 상호작용의 영향을 많이 받는다는 것을 의미한다. 준거집단의 핀테크 서비스 사용 경험과 평가 의견들이 공유되고 전파되어 사회적 영향력으로 작용한다는 것이다. 국내 핀테크 서비스 시장은 초기 확산 단계에 있으므로 핀테크에 대한 긍정적인 사회적 여론 형성은 매우 중요하게 작용할 것이다. 핀테크 서비스에 대한 사회적 평판을 우호적으로 구축하는 것이 무엇보다 중요하겠다.

넷째, 핀테크 서비스 환경에서 지각된 위협과 지각된 대응성은 정보보호행위에 모두 유의한 영향을 미치는 것으로 나타났다. Jones et al.(2015)은 바이러스에 대한 보호행동에 관한 연구에서 지각된 위협이 바이러스 예방행동에 유의한 영향을 미친다고 주장한 바 있다. TTAT에서는 특정 IT를 이용하여 부정적인 반응이 유발된다면 회피동기를 가지게 되고, 이것이 위협 요소로 인지된다면 사용자들은 정보보호행위를 취하게 된다는 것이다. 이것은 지각된 개연성과 심각성으로 인한 지각된 위협이 보호행동 및 예방행동에 영향을 미치는 것을 말한다. PMT에서는 지각된 대응성 또한 건강보호행동에 유의한 영향을 미친다고 주장하였다. 핀테크 보안에서 개인정보 및 프라이버시 침해에 대한 불안감과 위협은 개인정보 및 프라이버시 정책을 적극적으로 준수하여 스스로 개인정보를 보호하려는 긍정적인 행동으로 이어질 수 있다는 것이다.

6.2. 시사점 및 향후 연구방향

본 연구는 다음과 같은 학문적, 실무적 시사점을 제시한다.

학문적 시사점으로는 핀테크 서비스의 정보보호행위에 영향을 주는 요인을 이용자의 인지적 관점과 예방적 관점에서 도출하여 실증적으로 검증하였다. 핀테크 정보보호 관련 행동학적 접근방법의 연구가 부족한 상황에서 보건의료

예방 및 의료행위를 설명하는 주요 변인들을 결합하여 핀테크 서비스 정황에 적용함으로써 정보보호행위에 관한 융합모델을 제시하는 등 이론적 발전에 기여하였다. 또한 본 연구결과는 핀테크 서비스 이용자의 정보보호행위에 대한 이해와 더불어 IT위협-회피 행동과 정보보안 위협의 부정적 인지에 대한 포괄적인 이해를 제공한다.

본 연구결과를 통해 핀테크 이용자의 보안인식 제고와 보안도구 활용의 필요성을 제시하였으나 1차적으로 핀테크 서비스 기업의 핀테크 보안대책과 정보보안체계가 매우 중요하다. 핀테크 서비스 운영자, 금융정책기관 및 금융기관 실무자, 핀테크 비즈니스 사업가, 그리고 단말 솔루션업체 등에게 핀테크 정보보호 서비스의 운영에 관한 고려사항과 핀테크 보안위협 관련 전략수립의 기본 지침을 제공하였다는 실무적 시사점을 제공한다.

본 연구결과를 통해 핀테크 서비스의 개인정보보호 전문가와 보안정책 전문가 양성을 위한 교육과정에도 큰 도움이 될 것이다. 핀테크 이용자 스스로 개인정보 및 프라이버시를 보호하려는 노력이 중요하다는 연구결과를 제시하여 정보보호 및 보안정책 수립에 있어서 이용자의 인지적 관점과 예방적 관점에서 바라볼 수 있는 시각과 이에 관한 교육과정 보완을 통해 핀테크 보안인재양성 수립방향에 기여할 수 있을 것이다.

마지막으로, 본 연구의 한계점과 향후 연구방향은 다음과 같다. 첫째, 표본 크기의 경우 구조방정식 방법론의 최소 표본 크기 조건을 충족하였으나 후속 연구에서는 표본의 수를 늘려 정확한 인과관계를 확인할 필요성이 있다. 또한 표본의 기술적 특성과 본 연구모형의 연관성을 검증하는 것도 필요할 것으로 보인다. 둘째, 핀테크의 경우 정부의 정책적인 영향을 많이 받는 산업으로 정책적 변수가 중요하게 작용될 것이다. 향후 연구에서는 정책적인 변수 및 핀테크 기업의 신뢰도 관련 변수를 적용할 필요성이 있다. 셋째, 본 연구가 수행된 시점은 핀테크 서비스 이용 초기 단계이므로 핀테크 서비스 이용이 본격화되는 시점에서의 연구와 핀테크 서비스 이용의 확산 단계에 따라 정보보호 행위가 달라지는지 연구할 필요성이 있겠다.

참고문헌

강영모, 이영근, 권현정, 한경석, 정현수, “핀테크 기업의 정보보안체계 관한 연구”, 중소기업정보기술융합학회 논문지, 제6권, 제2호, 2016, pp. 19-24.

곽관훈, “핀테크 관련 국내법제의 현황과 과제”, 강원법학, 제49권, 제1호, 2016, pp. 259-286.

김상희, 김종기, “온라인 환경에서 프라이버시 의사결정에 영향을 미치는 요인에 관한 연구: 이중계산모델을 중심으로”, 정보시스템연구, 제25권, 제3호, 2016, pp. 197-215.

김정은, 김성준, 권두순, “소셜 네트워크 서비스(SNS) 이용자들의 개인정보보호 행동에 관한 연구: 보호동기이론을 중심으로”, 정보시스템연구, 제25권, 제3호, 2016, pp. 1-30.

문병순, “핀테크의 동향과 과제 - 개인정보 보

호 문제를 중심으로", 은행법연구, 제8권, 제1호, 2015, pp. 29-53.

박서기, "핀테크 산업 동향과 주요 비즈니스 모델에 대한 연구", 한국멀티미디어학회지, 제19권, 제1호, 2015, pp. 1-8.

박정국, "핀테크(Fintech)와 정보보안", 정보과학회지, 제1권, 특집호, 2015, pp. 23-32.

박혜영, "핀테크 사업 분야별 현황과 한국형 핀테크 산업 성장 방향 모색", 정보와 통신, 제33권, 제2호, 2016, pp. 73-78.

배재권, "개인용 클라우드 컴퓨팅 서비스의 정보보호 행위에 관한 연구", 로고스경영연구, 제12권, 제4호, 2014, pp, 77-92.

신세미, 김성준, 권두순, "건강신념모델을 이용한 소셜네트워크서비스에서의 개인정보 보호행위에 관한 연구", 정보보호학회논문지, 제26권, 제6호, 2016, pp. 1619-1637.

유재필, 허세경, "해외 사례를 통해 알아본 핀테크 보안 이슈 진단 및 보안 추진방향", 정보과학회지, 제1권, 특집호, 2015, pp. 33-36.

이경전, 허미리, 황보유정, 전정호, "핀테크의 이해", 정보시스템연구, 제25권, 제2호, 2016, pp. 173-189.

이병관, 손영곤, 이상록, 윤문영, 김민희, 김채린, "건강 관련 행동의 예측을 위한 사회인지이론의 유용성: 국내 건강신념모델 연구의 메타분석", 홍보학연구, 제18권, 제2호, 2014, pp. 163-206.

이우석, 홍보경, "핀테크의 현황과 법적 과제", 영산법률논총, 제12권, 제2호, 2015, pp. 219-256.

장국현, 황찬규, 송영우, "환경경영에서 건강신념모델을 이용한 병원환경이 대응성과 건강가치성을 통해 예방행동에 미치는 영향", 디지털산업정보학회논문지, 제12권, 제3호, 2016, pp. 231-257.

장유진, 김영욱, "행위단서, 공포 및 정부신뢰도가 위험인식 및 행동의도에 미치는 영향: 원전사고 이후 일본산 수산물 섭취 이슈 중심 분석", 광고학연구, 제27권, 제8호, 2016, pp. 7-32.

정준호, 김정숙, "핀테크(FinTech) 서비스의 발전과 주요 보안 이슈", 한국멀티미디어학회지, 제19권, 제1호, 2015, pp. 9-15.

지범석, 판류, 이상철, 서영호, "정보품질을 위한 개인정보 보호행위: 건강심리이론 관점을 중심으로", 품질경영학회지, 제39권, 제3호, 2011, pp. 432-443.

최창열, 함형범, "핀테크 기업의 비즈니스 모델에 대한 이론적 연구", e-비즈니스 연구, 제16권, 제4호, 2015, pp. 85-100.

Ajzen, I., "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, Vol. 50, 1991, pp. 179–211.

Bae, J., "An Empirical Study on the Effect of Leakage Threat of Personal Information on Protective Behavior Intention in Big Data Environment: Based on Health Psychology Theory and Protection Motivation Theory," *The e-Business Studies*, Vol. 17 No. 3, 2016, pp. 191-208.

Bandura, A., Self-efficacy: The exercise and

control, New York: W. H. Freeman, 1997.

Becker, M. H., and Rosenstock, I. M., Compliance with medical advice. In A. Steptoe & A. Mathews (Eds.), Health care and human behavior. London: Academic Press, 1984.

Chin, W. W., "Issues and Opinion on Structural Equation Modeling," *MIS Quarterly*, Vol. 22, No. 1, 1998, pp. 7-16.

Elliot, A. J., "Approach and Avoidance Motivation and Achievement Goal," *Education Psychology*, Vol. 34, No.1, 1999, pp. 169-189.

Fishbein and Ajzen, Belief, attitude, intention, and behavior: An introduction to theory and research. Reading, MA: Addison-Wesley, 1975.

Fornell, C. and Larcker, D. F., "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, Vol. 18, No. 1, 1981, pp. 39-50.

Fulk, J., Steinfield, C. W., Schmitz, J., and Power, J. G. (1987), A Social Information Processing Model of Media Use in Organizations, *Communication Research*, Vol. 14, No. 5, pp. 529-552.

Ifinedo, P., "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers & Security*, Vol. 31, No. 1, 2012, pp. 83–95.

Jones, C. L, Jensen, J. D., Scherr, C. L., Brown, N. R., Christy, K., and Weaver, J.. "The Health Belief Model as an Explanatory Framework in Communication Research: Exploring Parallel, Serial, and Moderated Mediation," *Health Commun*, Vol. 30, No. 6, 2015, pp. 566–576.

Jones, K. O., Denham, B. E., and Springston, J. K., "Effects of mass and interpersonal communication on breast cancer screening: Advancing agenda-setting theory in health contexts", *Journal of Applied Communication Research*, Vol. 34, No. 1, 2006, pp. 94-113.

Liang, H. and Xue, Y., "Avoidance of Information Technology Threats: A Theoretical Perspective," *MIS Quarterly*, Vol. 33, No. 1, 2009, pp. 71-90.

Liang, H. and Xue, Y., "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems*, Vol. 11, No. 7, 2010, pp. 393-413.

Ng, B. Y., Kankanhalli, A., and Xu, Y., "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems*, Vol. 46, No. 4, 2009, pp. 815-825.

Prati, G., Pietrantoni, L., and Zani, B., "A social-cognitive model of pandemic influenza H1N1 risk perception and

recommended behaviors in Italy," *Risk Analysis*, Vol. 31, No. 4, 2011, pp. 645-656.

Rogers, R. W., "A Protection Motivation Theory of Fear Appeals and Attitude Change," *The Journal of Psychology: Interdisciplinary and Applied*, Vol. 91, No. 1, 1975, pp. 93-114.

Rogers, R. W., Cognitive and Physiological Process in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation, in Social Psychophysiology: A Source Book, R. Petty (ed.), New York: Guilford Press, 1983, pp. 153-176.

Rosenstock, I. M., "Historical Origin of the Health Belief Model. In M. H. Becker(Ed.)," The Health Belief Model and personal health behavior, 1974, pp. 1-8.

Rosenstock, I. M., Strecher, V. J. and Becker, M. H., The Health Belief Model and HIV Risk Behavior Change, In Diclemente and Peterson, Preventing AIDS: Theories and Methods of Behavioral Interventions, New York: Plenum Press, 1994, pp. 5-24.

Stillman, M. J., "Women's health beliefs about breast cancer and breast self-examination," *Nursing Research*, Vol. 26, No. 2, 1977, pp. 121-127.

Volk, J. E., and Koopman, C., "Factors Associated with Condom use in Kenya: A Test of The Health Belief Model," *AIDS Education and Prevention*, Vol. 13, No. 6, 2001, pp. 495-508.

Weinstein, N. D., "Perceived Probability, Perceived Severity, and Health Protective Behavior," *Health Psychology*, Vol. 19, No. 1, 2000, pp. 65-74.

Workman, M., Bommer, W. H., and Straub, D., "The amplification effects of procedural justice on a threat control model of information systems security behaviours," *Behaviour & Information Technology*, Vol. 28, No. 6, 2009, pp. 563-575.

배 재 권 (Jae Kwon Bae)

계명대학교 경영정보학과 조교수로 재직 중이다. 서강대학교 MIS전공으로 경영학 박사학위(2009)를 취득하였다. 주요 관심분야는 비즈니스빅데이터분석, 신용평가, Data Mining, Neural-net Computing, Intelligent Systems 등이며, 국제저명학술지인 International Journal of Distributed Sensor Networks, International Journal of Multimedia and Ubiquitous Engineering, Expert Systems with Applications, Information Systems Frontiers 등에 논문을 게재하였다.

<Abstract>

The Structural Relationships among Information Security Threat Factors and Information Protection Behavior of the FinTech Services: Focus on Theoretical Perspectives of Technology Threat Avoidance and Health Protective Behaviors

Jae Kwon Bae

Purpose

Financial technology, also known as FinTech, is conceptually defined as a new type of financial service which is combined with information technology and other traditional financial services like payments, investments, financing, insurance, asset management and so on. Most of the studies on FinTech services have been conducted from the viewpoint of technical issues or legal and institutional studies, and few studies are conducted from the health belief perspectives and security behavior approaches. In this regard, this study suggest an extended information protection behavior model.

Design/Methodology/Approach

The Health Belief Model (HBM), the Protection Motivation Theory (PMT), and the Technology Threat Avoidance Theory (TTAT) were employed to identify constructs relevant to information protection behavior of FinTech services. A new extended information protection behavior model in which the influence factors of information protection behavior (i.e., perceived susceptibility, perceived severity, perceived benefits, perceived barriers, perceived self-efficacy, subjective norms) affect perceived threats and perceived responsiveness positively, leading to information protection behavior of FinTech users eventually. This study developed an extended information protection behavior model to explain the protection behavior intention in FinTech users and collected 272 survey responses from the mobile users who had experiences with such mobile payments and FinTech services.

Findings

The finding of this study suggests that the influence factors of information protection behavior affect perceived threats and perceived responsiveness positively, and information protection behavior of FinTech users as well.

Keywords: Fintech Services, Health Belief Model, Protection Motivation Theory, Technology Threat Avoidance Theory, Information Security Threat Factors, Information Protection Behavior

* 이 논문은 2017년 4월 21일 접수, 2017년 6월 15일 1차 심사, 2017년 8월 7일 게재 확정되었습니다.