http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.20, No.4, November 2015, pp.77-102
http://dx.doi.org/10.7838/jsebs.2015.20.4.077

핀테크 서비스의 개인정보보호 자가평가항목 개발에 관한 연구: 간편결제 서비스 중심

A Study of Self-Checklist for Personal Information Protection of FinTech Service: For the Simple Payment Service

강민수(Min Soo Kang)*, 백승조(Seung Jo Back)**, 임종인(Jong In Lim)***

초 록

핀테크 서비스 산업은 현재 전 세계적으로 ICT 기술을 기반으로 모바일 등 다양한 채널을 통해 금융 및 결제서비스의 혁신을 이끌며 빠르게 성장하고 있다. 국내에서도 간편결제 서비스를 중심으로 다양한 핀테크 서비스 산업이 형성되고 있다. 이러한 핀테크 서비스는 여러 가지 보안 위협들이 존재하며, 그 중 개인정보 및 금융정보를 수집・이용함에 따라 이에 대한 정보 유출이나 프라이버시 침해 사고 가능성도 증가할 것이다. 이에 본 논문에서는 핀테크 서비스 중 간편결제 서비스를 대상으로 자신의 개인정보보호에 대한 합리적인 선택을 하는 이용자들(Privacy Pragmatists)에 대해 해당 서비스를 이용 및 선택 시 개인정보보호에 대한 자가평가를 할 수 있도록 평가항목을 도출하며, 이를 통해 향후 핀테크 서비스의 개인정보보호를 위한 보안 정책을 제언하고자 한다.

ABSTRACT

FinTech service industry has been growing rapidly around the world. It has driven innovation in financial and payment service industry with different channels such as mobile based on Information and Communications Technology (ICT). However, FinTech service is vulnerable to different security threats due to use the valuable data such as personal information and financial information. It is undeniable that collection and use of those information may increase the possibility of identity theft or privacy breach. In this paper will develop a self-checklist for the Simple Payment service users (Privacy Pragmatists) who want to make a rational decision to protect their personal information. The checklist is going to let the users assess the personal information protection by performing the assessment themself when they use the service. The body of this paper is going to analyze the items of the checklist and through the analysis, will suggest a security policy for personal information protection of FinTech service.

키워드 : 핀테크, 개인정보보호, 간편결제 서비스
Fintech, Personal Information Security, Simple Payment Service

* First Author, Graduate School of Information Security, Korea University(kozinaru@korea.ac.kr)
** Co-Author, Graduate School of Information Security, Korea University(nomadvirus@korea.ac.kr)
*** Corresponding Author, Graduate School of Information Security, Korea University(jilim@korea.ac.kr)
Received: 2015-08-21, Review completed: 2015-09-17, Accepted: 2015-10-21

1. 서 론

현재 국내뿐만 아니라 전 세계적으로 핀테크(Fintech) 서비스 산업이 급부상하고 있다. 핀테크 서비스 산업은 ICT 기술을 통해 금융산업의 비즈니스 모델을 창출하고 다양한 모바일 채널 등을 활용하여 서비스를 급속하게 확대하고 있다. 이러한 핀테크 서비스 발달을 통해 간편결제 서비스, 송금, 크라우드 펀딩 등 다양한 서비스가 제공되고 있으며, 이용자들은 보다 편리하게 금융서비스를 이용할 수 있게 되었다.

하지만 이러한 핀테크 서비스는 편리하고 안전한 금융 서비스를 제공해야 하는 입장에서는 더 많은 ICT 기술들이 접목되면서 해킹 등 보안위협의 지속적인 증가로 더 많은 보안위협에 직면하게 되었다[6].

또한 '간편결제/송금', '인터넷 전문은행', '크라우드 펀딩', '금융 데이터 분석 등' 모든 분야의 핀테크 서비스는 금융소비자의 개인정보와 금융정보를 활용해야 하는데, 이러한 핀테크 서비스 제공을 위해 금융소비자의 개인정보, 금융정보 등을 보유하는 기업이 증가하면서 중요정보의 안전한 관리에 대한 문제가 대두되고 있다. 즉, 핀테크 기업마다 금융소비자의 금융정보 등을 보유하게 됨에 따라, 카드사와 은행에 요구되던 높은 수준의 정보보호 관리체계가 핀테크 기업에까지 요구된다[11].

기업에서는 자사의 보안기술력 및 개인정보보호 등에 대해 안내를 하고 있지만, 실제 이용자들이 자세한 사항을 확인하기에 제한적이거나, 어떠한 사항을 확인해야 하는지에 대해 정확히 모르는 경우가 많다. 실제로 대부분의 사람들이 매일 온라인에서 개인정보와 보안 관련 사항을 확인하고 결정하지만, 대부분은 이러한 중요한 결정을 하는데 있어 자신이 충분한 권한을 가지고 있지 않다고 느낀다고 한다[16].

이와 같이 이용자들이 핀테크 서비스를 이용 및 선택함에 있어, 해당 서비스가 개인정보보호 등에 취급 및 관리 등을 잘 하고 있는지에 대해 확인할 필요성이 있다. 이에 본 논문에서는 현재 국내 핀테크 서비스 중 주를 이루고 있는 간편결제 서비스를 대상으로 앨런 웨스턴(Alan Westin)이 제안한 개인정보보호에 대한 소비자 3가지 유형 중 '개인정보보호에 대한 합리적인 선택을 추구하는 이용자(Privacy Pragmatists)' 유형을 중심으로 이러한 사항을 확인하기 위한 개인정보보호 자가평가항목을 도출하고, 이를 통해 핀테크 서비스가 이용자들의 개인정보보호를 위해 필요한 정책적 방안을 마련하고자 한다.

본 논문의 구성은 제2장 연구배경에서 핀테크 서비스의 개요와 현황을 살펴보고, 핀테크 서비스에서 발생할 수 있는 정보유출 등의 보안이슈를 살펴본다. 또한, 핀테크 서비스 중 간편결제 서비스를 중심으로 개인정보보호 관련 현황을 살펴본다. 제3장에서는 개인정보보호법 등 현행법과 개인정보보호 관련 평가체계 등을 통하여 핀테크 서비스 이용자들이 해당 서비스를 선택 및 이용 시 개인정보보호 관련 사항을 확인할 수 있도록 개인정보보호 자가평가항목을 도출한다. 다음으로는, 도출한 자가평가항목을 이용자들의 설문을 통하여 평가항목의 필요성 등을 검증하고, 사례에 대한 실제 평가를 통하여 개인정보보호 수준을 진단하며, 향후 핀테크 서비스의 이용자의 개인정보보호를 위한 정책을 제언하는 것으로 논문을 마무리한다.

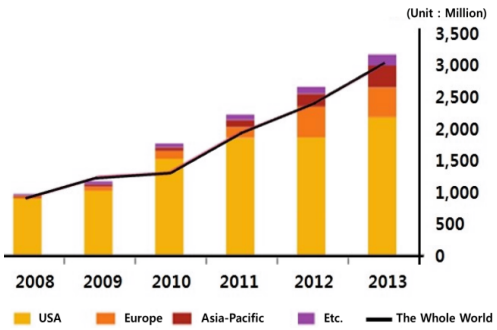
2. 연구배경

2.1 핀테크 개요 및 서비스 분류

핀테크(FinTech)는 Finance(금융)와 Technology(기술)의 합성어로, 금융과 IT의 융합을 통한 금융서비스 및 산업의 변화를 통칭한다[5].

현재 핀테크는 전 세계적으로 IT와 금융의 융합 트렌트가 확산되고 있으며, 온라인과 모바일을 통한 금융거래가 국가간의 경계를 넘어 이뤄지고 있다. 이러한 변화는 국내 소비자뿐만 아니라 현 산업의 거래습관과 환경에 변화를 촉발시키고 있다. 미국, 영국을 중심으로 핀테크 서비스에 대한 투자와 개발이 지속적으로 증가하고 있으며 각국 정부에서는 핀테크 산업을 발전시키기 위하여 적극적으로 정책 지원을 하고 있다[3].

<Figure 1>은 Accenture analysis od CB insights data의 연도별 전 세계 핀테크 투자규모 성장률 추이 그래프로 투자규모가 지속적으로 증가하고 있음을 확인할 수 있다.



* source: Accenture analysis od CB insights data.

〈Figure 1〉 Investment Scale of Fintech (The Whole World) [19]

전 세계적인 핀테크 열풍에 맞춰 국내에서도 핀테크 산업의 열풍이 불고 있다. 수익 위기에 빠진 금융사(은행, 카드사, PG사 등)는 위기를 극복하기 위해 신규 핀테크 사업모델 발굴에 나서고 있으며, IT기업과 인터넷 스타트업(start-up)도 핀테크를 새로운 블루오션(blue ocean)으로 인식하고 다양한 핀테크 서비스를 개발하고 있다. 글로벌 전자결제 시장의 성장에 맞춰 국내 인터넷 쇼핑몰의 불편한 결제시스템을 해외 쇼핑몰과 같이 간편하고 신속한 결제시스템으로 개선해야 한다는 요구가 높아지면서 핀테크 산업에 대한 관심도 높아지고 있다. 이에 정부는 핀테크 산업을 국가의 미래 신성장동력으로 인식하고, 핀테크 산업 활성화를 위한 단계별 전략을 세워 추진하며, 기업 지원 방안 마련에 적극 나서고 있다[11].

핀테크 서비스 종류를 살펴보면, 첫 번째로 인터넷이나 모바일 등에서 제품 및 서비스 구매 시 사용자가 미리 등록한 카드나 계좌 정보를 활용하여 간편하게 결제가 가능하도록 한 간편결제 서비스가 있다. 대표적인 사례로 페이팔(Paypal), 알리페이(Alipay), 카카오페이(Kakaopay) 등이 있다.

두 번째로 사용자가 온라인으로 거래 가능한 가상화폐 및 이메일과 모바일을 통해서 개인과 기업간 송금이 가능한 송금서비스로 구글월렛(GoogleWallet), 페이팔(Paypal), 토스(toss), 뱅크월렛카카오 등이 있다.

세 번째로 소셜네트워크 서비스를 이용해 소규모 후원이나 투자 등의 목적으로 인터넷과 같은 플랫폼을 통해 다수의 개인들로부터 자금을 모으는 크라우드 펀딩이나, 개인 간 자금조달을 중개해 주는 서비스 등의 투자서비스가 있으며, 인터넷전문은행, 빅데이터를 활용한 서비스 등이 있다.

〈Table 1〉 Classification of Fintech service

Classification	Contents
Simple Payment	• Payment services • Improved ease of payment of products and services • Payment available using virtual bank accounts, credit cards, and real accounts
Remittance	• Virtual currency available for online trading • Remittances between individuals and businesses through e-mails and mobile devices
Asset Management	• Plays a role of supermarkets to buy a variety of roles funds online • Exclusive to internet banking, online use, providing credit and reception features
Investment	• Online platform crowdfunding, etc. of investment related services such as loans, start-up financing, investment banking, • Offers services that mediate financing between individuals
Data Analysis	• Promoting consumption through the recognition of the consumption patterns using the big data analysis • Calculate more sophisticated lending rate using large-scale data

이와 같은 핀테크 서비스별 유형은 정리하면 <Table 1>과 같이 분류할 수 있다.

2.2 핀테크 보안 이슈

2010년 이후 발생한 개인정보 유출의 경우는 영향을 미치는 개인정보의 수가 크게 증가하고 집단 소송으로까지 연결되는 등 사회적으로 큰 관심을 끌 사례가 더욱 많아진 정황을 고려하였을 때[9], 국내뿐만 아니라 전 세계적으로 성장하고 있는 핀테크 서비스의 경우도 다양한 보안 이슈에 대해 민감할 수 밖에 없다. 핀테크는 궁극적으로 금융과 IT가 융합된 서비스라고 볼 수 있어서 IT에 관련된 보안이슈에 그대로 노출될 수 밖에 없으며, 특히 결제, 송금, 자산관리, 크라우드 펀딩 등의 다양한 서비스에 관련되어 있기 때문에 보안이 취약하다면 예상하지 못할 규모의 경제 손실이 발생할 수 있다[3].

공인인증서와 키보드 보안 등 이용자단 인증 강화에 중점을 뒀던 기존 금융보안 체계로는 핀테크 서비스에 따른 다양한 새로운 보안 위협들을 막아내기 역부족 하다는 것이 전문가들의 지적이다. 갈수록 손쉬운 금융 거래를 요구하는 소비자들의 요구에 대응해야 하고, 혁신적인 금융서비스 제공을 위해서라면 IT기업과 보다 빈번하게 금융 정보를 공유할 수 밖에 없다. 다각도로 보안 허점들이 생길 수 밖에 없는 구조이다. 핀테크 열풍을 이끈 페이팔(Paypal)에서 원클릭으로 계정이 탈취되는 크로스사이트 요청위조(CSRF) 취약점이 발견되는 등 핀테크 서비스에 대한 보안위협이 지속적으로 발견되고 있다[18].

해외에서는 최근 들어 꾸준히 대량 정보유출 사례가 발생하고 있으며, 피해 사업자는 유통 업체부터 신용카드 결제서비스사업까지 다양하게 퍼지고 있다.

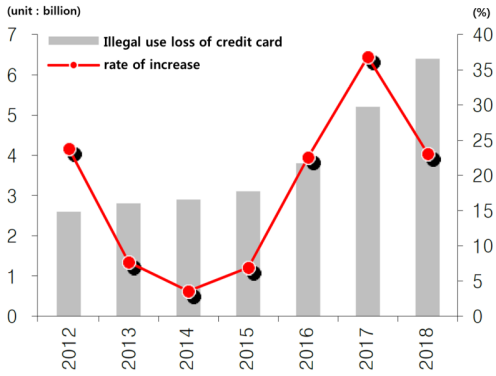
유출 사례를 살펴보면 대부분 해킹을 통한 정보유출이 많은 것으로 보이고 있으며, 2014년 이베이(ebay)가 해커들의 공격을 받아 이

베이(ebay) 계정과 연동된 페이팔(paypal) 계정이 외부로 유출되었다. 페이팔(paypal) 가입자 정보유출은 국내 '직구족'이 늘어나고 있는 것을 감안하면 매우 심각한 위협으로 평가된다.

유출된 정보의 내용으로는 단순 개인정보에 대한 것과 신용카드 정보까지 다양하다. 이렇게 유출된 신용카드 정보(카드번호, 유효기간, CVC 코드 등) 및 개인정보(사회보장번호, ID/PW)를 이용한 카드 부정사용 가능성도 있어 점차 피해는 확산될 것으로 예상된다. 또한 보안업체 RSA에 따르면 핀테크 선진국인 미국의 2014년 신용카드 부정사용 금액은 29억 달러, 약 3조 2천억 원으로 추산되고 2018년엔 64억 달러, 약 7조 5백억 원으로 증가할 것으로 전망하였다[3].

<Figure 2>는 2014년 RSA에서 발표한 미국 신용카드 부정사용 손실액 추이 그래프로, 향후 2018년까지 높은 증가세를 보일 것으로 예상하고 있다.

이러한 피해사례를 살펴보았을 때 국내 핀테크 서비스가 성장함에 따라 해외와 같은 금융정보 유출 및 개인정보 유출이 발생할 가능성이 있다.



*source: RSA(2014).

〈Figure 2〉 Illegal Use Loss of Credit Card(USA) [3]

2.3 핀테크 서비스 별 개인정보취급 현황

간편결제, 송금, 크라우드 펀딩 등 핀테크 서비스를 이용하기 위해서는 중요 정보(개인정보 및 금융정보)를 보관·사용해야 한다. 각 서비스별로 수집·보관 되어지는 정보를 정리하면 <Table 2>와 같이 정리할 수 있다.

〈Table 2〉 Handling Personal Information of Fintech Service Types

Classification	Types	
Simple Payment	Credit and Financial Information	Credit Card Information, Account Information
	Personal Identifiable Information	E-Mail Address, Phone Number
	Authentication Information	Password
Remittance	Credit and Financial Information	Credit Card Information, Account Information
	Personal Identifiable Information	User Name
	Authentication Information	Password
Funding	Credit and Financial Information	Credit Card Information, Account Information
	Personal Identifiable Information	User Name, Phone Number, E-Mail Address, Etc.
	Authentication Information	Password

2.4 간편결제 서비스 개인정보보호 관련 현황 분석

핀테크 서비스 중 국내에서는 간편결제 서비스가 주를 이루며, 다양한 기능 제공 등을 통해 높은 이용률 보이고 있다. 반면, 송금, 대출 등은 성장단계로 가입자는 꾸준히 증가하고 있으나, 시장 영향력은 아직 크지 않은 상황이다[4]. 이에 본 논문에서는 국내에서 가장 많이 이용되고 있는 간편결제 서비스를 대상으로 개인정보 및 금융정보 등에 대한 취급 및 관리에 대한 현황을 확인하고자 한다.

간편결제 서비스란 본인 명의로 된 신용카드, 계좌이체, 휴대폰 결제 정보를 스마트폰 어플리케이션을 이용해 최초 등록한 이후에 모바일 쇼핑 결제가 필요할 때마다 추가 정보를 입력할 필요 없이 아이디와 비밀번호 또는 비밀번호만으로 사용자를 인증하여 안전하게 결제할 수 있게끔 해주는 결제 서비스이다. 결제를 위해 사용자가 등록한 신용카드번호 등의 결제 정보들은 전자지급결제대행(Payment Gateway, PG)사에 암호화 되어 저장되며 결제 시에 해당 정보를 불러온다. 이런 프로세스는 서비스 마다 조금씩 차이는 있지만 공통적으로 기존 온라인 쇼핑에서 결제를 하기 위해 엑티브 엑스(Active-X)를 설치하지 않고 결제 정보는 PG사에 저장하고 있으며 결제 수단의 전용 비밀번호만을 통한 인증으로 결제하는 것이 특징이다.

국내의 간편결제 서비스는 다양한 형태로 구분된다. 우선 여러 카드사와 계좌이체, 휴대폰 결제 등의 다양한 결제방법을 지원하며 여러 쇼핑몰에서 범용적으로 사용할 수 있는 간편결제와 특정 쇼핑몰에서만 사용 가능한 간편결제가 있다[14].

이러한 국내 간편결제 서비스를 정리하면 <Table 3>과 같다.

간편결제 서비스에 대한 이용자의 보안인식을 살펴보면, 모바일 기기 이용자의 97.9%가 모바일 간편결제를 인지하고 있으며, 그 중 72%가 간편결제를 이용한 경험이 있는 것으로 조사되었다. 대다수의 이용자들이 이용의 편리성 때문에 간편결제 서비스를 이용하고 있지만, 반면에 가장 큰 불안요소로 개인정보 보호와 보안을 꼽았다[2].

〈Table 3〉 Classification of Domestic Simple Payment Services

Classification	Contents
INIpay (KGinicis)	Provides services over large open markets, etc.
Smile pay (Ebay)	Offers to its open markets (G Market, Auction) members
Paypin (SKplanet)	Offers to its affiliate members, etc. of subsidiaries such as 11 Avenue, social commerce
Yelopay	Offers to large open-market members, including INTERPARK
Ubpay	To register on a variety of payment methods and offline merchants Payment using the password in on and offline merchants by registering a variety of payment methods
Kakaopay	Payment via password by registering personal cards (credit/checks) in KakaoTalk
Paynow	Payment via the authorization number and the number of virtual payment by pre-registering with a smartphone app. for payment in an online shopping mall

이와 같이 간편결제 서비스의 불안요소인 개인정보보호에 대해 현재 간편결제 서비스를 제공하고 있는 기업의 현황을 살펴보고자 한다.

우선 각 핀테크 서비스 기업들은 각 자사의 홈페이지 및 모바일 앱 등을 통해 개인정보 취급방침 등 개인정보보호 관련 사항을 게시하고 있다. 해당 개인정보 취급방침을 통해 수집하는 개인정보 항목, 목적, 제 3자 제공 등에 대한 안내를 하고 있으며, 추가적으로 보안에 대한 기술적 보호조치방법을 별도의 페이지에 게시하고 있다.

먼저 개인정보 취급방침을 각 핀테크 서비스 기업별로 확인을 하였을 때, '정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법) 제27조의 2 개인정보 취급방침의 공개' 및 '개인정보보호법 제30조 개인정보 처리방침의 수립 및 공개' 등에서 정하고 있는 항목을 게시하고 있다.

하지만 해당 개인정보 취급방침을 비교하였을 때, 법에서 제시하고 있는 기준 항목에 대한 고지의 설명 부분이 일정한 형식 없이 상이하며, 내용 또한 일관성을 갖추고 있지 않음을 확인할 수 있다. 또한 실제 이용자들이 개인정보 취급방침 등의 각 핀테스 서비스 기업에서 게시하고 있는 개인정보보호 관련 사항을 확인할 때, 어떤 항목을 확인해야 하는지에 대한 가이드라인이나 평가항목 기준 안내 등이 없어 게시를 하고 있더라도 명확히 인지하고 확인하기는 어려움이 있다.

2.5 간편결제 서비스의 이용자 대상 선정

본 논문에서는 간편결제 서비스를 이용하는 이용자 중 일반적인 모든 이용자가 대상이 아닌 개인정보보호에 대한 합리적인 소비를 선택을 추구하는 이용자(Privacy Pragmatists)를 대상으로 하고자 한다. 개인정보보호에 대한 합리적인 선택을 추구하는 소비자란, 앨런 웨스턴(Alan Westin)이 개인정보보호에 대한 이용자의 의식 수준 등을 기준으로 분류 한 3가지 유형 중 하나로, 첫 번째 유형은 '개인정보보호 근본주의자(Privacy Fundamentalists)'로 자신의 개인정보에 대한 제공을 거부하는 분류로 대상자의 약 25%에 해당한다.

두 번째는 '개인정보보호 실용주의자(Privacy Pragmatists)'로 개인정보보호에 대한 노력의 타당성이나 보안에 대한 잠재적 위험을 능동적으로 알고 싶어 하며, 이에 대한 확인을 통해 합리적인 선택을 하는 분류로 대상자의 약 50%에 해당한다. 국내 이용자 중에서도 '2012년 정보보호 실태조사(한국인터넷진흥원)'에 의하면, 사용자의 41.1%가 개인정보보호를 위한 조치를 하고 있으며, 개인정보 취급방침 공개 사실을 인지하고 있는 인터넷 이용자 중 34.4%가 개인정보 취급방침을 직접 확인하는 등 능동적으로 자신의 개인정보보호에 대한 조치를 취하는 사용자들이 있으며, 해당 이용자들을 개인정보보호 실용주의자의 분류로 간주 할 수 있다[7].

세 번째는 '개인정보보호 무관심자(Privacy Unconcerned)'로 개인정보보호에 대한 취급 및 관리 등에 큰 관심을 두지 않으며, 대상자의 약 20%에 해당한다[1].

앨런 웨스턴의 조사에 따르면 1990년대부터 2000년대까지 '개인정보보호 무관심자'의 비율은 줄어들며, '개인정보보호 실용주의자'의 비율은 증가함을 확인할 수 있다. 이에 대해 앨런 웨스턴은 이용자들이 실제 개인정보보호에 대

한 기술과 그 의미들에 대해 더 많이 알아가기 때문이라고 설명하였다. 즉, 개인정보보호 실용주의자와 같이 개인정보보호에 대한 중요성이 높아짐에 따라 관심을 가지는 이용자들도 증가함을 확인할 수 있다[17].

위의 3가지 분류 중 '개인정보보호 실용주의자'를 선택한 이유는 이들은 실제적으로 자신의 개인정보보호에 대한 능동적인 확인을 원하는 대상으로, 본 논문에서 도출하고자 하는 개인정보보호 자가평가항목을 자신의 개인정보보호를 위해 활용할 수 있는 대상으로 적합하기 때문이다. 이에 본 논문에서는 개인정보보호 실용주의자를 이용자로 한정하고 연구대상으로 활용한다.

3. 핀테크 서비스 개인정보보호 자가평가 항목 도출

본 장에서는 이용자관점에서 간편결제 서비스가 개인정보보호에 대한 취급・보호 등을 안전하게 관리하는지를 확인 할 수 있도록 자가평가항목을 도출하고자 한다.

3.1 국내 개인정보보호 진단평가 방법

국내 개인정보보호 수준을 평가하는 방법으로는 공공기간을 대상으로 평가하는 개인정보 영향평가제도와 민간기업을 대상으로 하는 개인정보보호 관리체계제도(PIMS)가 있으며, 이외에도 기업에서 활용할 수 있는 기업 개인정보 영향평가, 한국인터넷진흥원에서 제공하는 개인정보 자가진단 체크리스트 등의 진단평가 방법이 있다.

공공기관을 대상으로 시행되고 있는 개인정보 영향평가(PIA: Privacy Impact Assessment)를 살펴보면, 개인정보파일을 운용하는 새로운 정보시스템의 도입이나 기존에 운영중인 개인정보 처리시스템의 중대한 변경 시 또는 시스템의 구축・운영・변경 등이 개인정보에 미치는 영향(impact)을 사전에 조사・예측・검토하여 개선방안을 도출하는 체계적인 절차이다. 평가항목으로는 대상기관의 개인정보보호 관리체계, 대상시스템의 개인정보보호 관리체계, 개인정보 처리단계별 보호, 특정 IT 기술 활용 시 개인정보보호 등의 총 4가지 영역에 114개의 평가항목으로 구성되어있다[12].

개인정보보호 관리체계(PIMS)는 기업을 대상으로 개인정보 보호 활동을 체계적・지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하여 일정 수준 이상의 기업에 인증을 부여하는 제도로, 평가항목은 개인정보 관리과정, 보호대책, 생명주기 3개 분야의 124개 통제항목, 310개의 세부점검 사항으로 구성되어 있다[8].

이러한 주요 개인정보보호 수준평가를 위한 제도들이나 평가항목들은 공공 및 기업에서 개인정보 처리가 수반되는 사업을 추진 시 해당 사업이 개인정보에 미치는 영향을 사전에 분석하고 이에 대한 개선방안을 수립하여 본 사업 수행 시 개인정보 침해사고를 사전에 예방하거나, 자율적인 점검을 통하여 개인정보보호 수준을 진단하고 개선할 수 있도록 한다.

3.2 개인정보보호 자가평가 항목의 필요성

앞서 살펴본 국내 개인정보보호 수준 평가

제도나 평가항목들은 기술적, 관리적, 법적인 기준을 제시하여 평가항목을 구성하고 있지만, 이용자들 관점에서 이를 가지고 평가를 하기에는 적합하지 않다. 왜냐하면, 개인정보보호 수준 평가제도나 평가항목들은 실제 개인정보를 전문적으로 담당하는 기관(한국인터넷진흥원 등)이나 전문업체의 전문가들에 의해 대상이 되는 기관의 개인정보관련 시스템 및 정책 등을 종합하여 평가를 진행하게 되므로 이용자의 입장에서 해당 방법 등을 통해 개인정보 수준을 평가하기에는 전문적인 지식이나 실제 대상기관의 상세정보 등을 파악하기는 현실적으로 제한이 되기 때문이다. 그러므로 이용자들이 개인정보보호 취급 및 안전성 등의 수준을 확인할 수 있는 방법은 개인정보보호 평가제도의 인증사항이나, 개인정보 취급방침, 별도로 게시하고 있는 개인정보보호 관련 사항 외에는 구체적인 사항을 확인하기에는 무리가 있다.

간편결제 서비스를 제공하는 기업은 보안과 개인정보보호에 관한 조치를 다하고 있지만 실제 이용자들이 개인정보보호 수준을 진단하거나, 확인할 수 있는 방법 및 가이드라인 등이 마련되어 있지 않은 것이 현실이다. 이에 본 연구에서 이용자관점에서 간편결제 서비스의 개인정보보호 취급・보호 등에 대한 사항을 직접 평가할 수 있도록 기준과 평가항목을 제시하여, 이용자가 객관적으로 개인정보보호 수준을 확인할 수 있도록 하고자 한다.

3.3 개인정보보호 자가평가항목 분류 기준

평가항목을 도출하기 위하여 다음과 같이 평가항목 분류 기준을 정리하여 종합적인 평가항목을 도출하고자 한다.

첫 번째로, 이용자가 개인정보관련 관리 및 취급에 대한 사항을 확인할 수 있는 개인정보 취급방침 및 처리방침 항목을 기준으로 활용한다. 개인정보 취급방침은 '정보통신망법 제27조의2 개인정보 취급방침의 공개'에 따라 이용자에게 홈페이지 등을 통해 개인정보 취급에 관련 사항을 안내한다. 또한 '개인정보보호법 제30조 개인정보 처리방침의 수립 및 공개'를 통하여 사업자, 단체의 개인정보 처리기준 및 보호조치 등을 문서화하여 공개하고 있다. '정보통신망법 제27조의2'에 해당하는 경우에는 별도의 개인정보 처리방침을 수립 공개하지 않아도 되나, 본 연구에서는 두 가지 사항을 모두 활용하여 평가항목에 반영한다.

두 번째로 개인정보 라이프 사이클을 활용하여 평가항목 기준을 정한다. 개인정보 라이프 사이클(Life-Cycle)이란 개인정보를 취득하여 활용하는 단계로써 통상적으로 수집, 보유, 이용・제공, 파기의 4단계로 구분하며, 개인정보 영향평가에서 라이프 사이클로 개인정보 흐름을 분류하여 단계별로 처리되는 개인정보 현황 및 처리 내역 등을 식별할 수 있도록 평가에 활용한다[12].

세 번째로 간편결제 서비스 이용시의 개인정보의 보안위협에 대한 진단을 위해 기술적, 관리적, 물리적 항목을 분류하여 평가 기준으로 활용한다.

위의 3가지 기준으로 개인정보보호 자가평가항목 분류를 구성하면, '1. 개인정보의 수집', '2. 개인정보의 처리 및 보유', '3. 개인정보 이용 및 제공', '4. 개인정보의 파기', '5. 개인정보의 안전성 확보', '6. 유출신고 및 피해구제', '7. 기타' 항목으로 분류할 수 있다.

7가지 항목을 분류 시 개인정보 취급방침 및 처리방침의 항목을 모두 포함하며, 개인정보 라이프 사이클을 1~4항목으로 분류하여 정리할 수 있다. 간편결제 서비스의 개인정보의 보안위협은 '5. 개인정보의 안전성 확보 항목에 포함시켜, 개인정보 취급방침 및 처리방침 항목에 포함되도록 구성할 수 있다. '6. 유출신고 및 피해구제'의 항목은 개인정보보호법 제34조 및 정보통신망법 제27조의3 등에서 의무사항으로 정하고 있으며, 정보유출 대응 사항 중 통지와 관련된 부분은 유출 사고 시 정보주체 외 프라이버시를 보호하고 정보주체 및 기업의 피해확산 방지를 위한 주요 조치 사항으로 각별히 주의를 기울여야 하므로, 해당 항목을 평가항목으로 분류하였다[10].

'7. 기타' 항목에서는 개인정보 취급방침 및 처리방침의 항목 중 1~6 항목 외 '이용자 및 법정대리인의 권리와 그 행사방법' 등의 항목을 포함하도록 한다.

3.4 개인정보보호 자가평가항목 세부 도출 기준 및 요건

앞에서 분류한 기준에 따라 이용자관점에서 개인정보보호 수준을 진단하기 위한 세부 평가항목을 도출하며, 도출항목의 정확성과 신뢰성을 위하여 총 3가지 도출 기준 지표를 정한다.

첫 번째로 '개인정보보호법', '정보통신망법'과 '표준 개인정보 보호지침' 등의 현행법률 및 지침 등을 활용하여 필수적으로 고지되어야 하는 항목 등을 도출한다.

두 번째로 국내 개인정보보호 관련 평가항목 중 개인정보 영향평가항목(PIA), 기업 개인정보 영향평가항목, 개인정보보호 관리체계(PIMS), 개인정보보호 자가진단 체크리스트 등의 평가항목을 활용하여 이용자관점에서 진단하거나 확인할 수 있는 항목을 도출한다.

세 번째로 간편결제 서비스 안전성 및 보안 관련 항목을 도출하기 위한 지표로, '개인정보의 기술적·관리적 보호조치 기준', '개인정보의 안전성 확보조치 기준', '인터넷뱅킹 보안가이드Ⅳ 모바일 뱅킹', '스마트폰 전자금융서비스 보안 가이드' 등을 활용하였다. 해당 지표를 바탕으로 간편결제 서비스 이용 시나 기업에서 게시하고 있는 보안관련 항목들에 대해 평가할 수 있는 항목을 도출한다.

또한, 위의 3가지 지표를 활용하여 평가항목을 수립할 시 다음의 요건을 충족하도록 하였다.

첫째, 도출된 평가항목은 현행법 및 지침 등에서 고지하는 부분에 대한 사항을 확인할 수 있도록 하여, 법에서 제시하는 요건을 충족하며, 객관적이고 타당하도록 해야 한다.

둘째, 모든 평가항목은 이용자관점에서 진단이 이뤄질 수 있도록 분류 및 구성하며, 이해하기 쉽도록 작성되어야 한다.

셋째, 간편결제 서비스의 특성에 대한 안전성 항목을 확인할 수 있도록 하여, 이용자가 개인정보의 관리 외에 기술적 보안요소를 확인할 수 있도록 해야 한다.

3.4.1 현행법 및 지침 기준 점검 항목 도출

자가평가항목 분류기준에 따라 '개인정보보호법', '정보통신망법', '표준 개인정보 보호지침'에서 각 항목에 적용되는 조항을 분류하고, 평가항목으로 재구성하였다.

평가항목으로 재구성 시에는 실제 이용자가 확인할 수 있는 항목들을 정리하여 평가항목으로 활용하도록 하였다.

3.4.2 국내 개인정보 영향평가 등 기준 항목 도출

개인정보 영향평가, 기업 개인정보 영향평가, 개인정보보호 관리체계(PIMS) 등의 평가항목 중 이용자관점에서 진단이 가능한 항목과 현행법에 근거하여 필수적으로 확인해야 하는 항목들을 선정하였다. 해당 항목들 중 현행법 및 지침 기준에서 도출한 항목들과 중복되는 항목들은 다시 재구성하여 평가항목에 반영하였다.

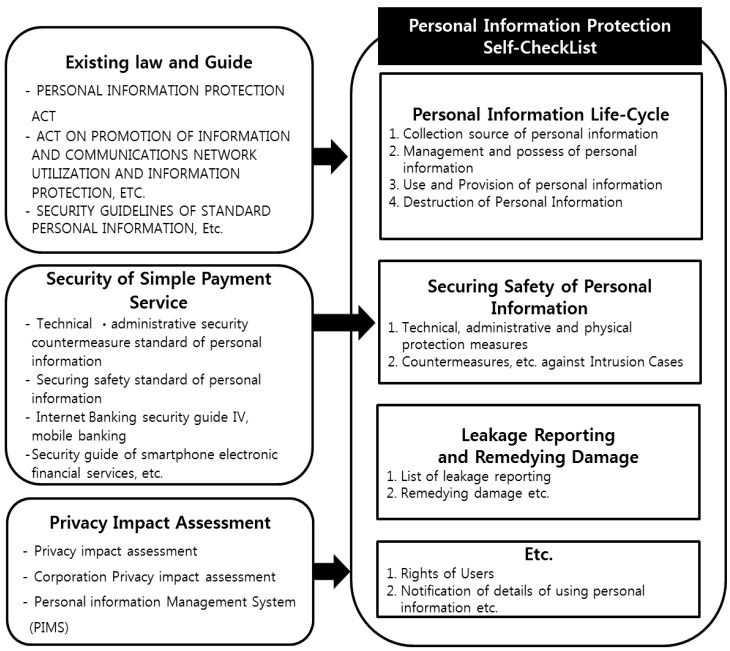
3.4.3 간편결제 서비스 보안 항목 도출

'개인정보보호법 제29조' 및 '정보통신망법 제28조' 등에서 개인정보의 안전성 확보에 대한 필요한 보호조치를 취하도록 고지하도록 하고 있으나, 간편결제 서비스 이용 시에 확인이 필요한 세부적인 평가항목을 추가 도출하여 평가항목 '5. 개인정보의 안전성 확보'에 활용하였다.

3.5 개인정보보호 자가평가항목

개인정보보호 자가평가항목은 '1. 개인정보의 수집', '2. 개인정보의 처리 및 보유,' '3. 개인정보 이용 및 제공', '4. 개인정보의 파기', '5. 개인정보의 안전성 확보', '6. 유출신고 및 피해구제', '7. 기타' 등으로 '총 7개 항목', '19개 중분류', '42개의 평가항목과 필수 항목'으로 구성되며, <Table 4>와 같이 도출할 수 있다. 또한 각 평가항목별 관련 산출 근거는 <Table 5>와 같이 정리할 수 있다.

<Figure 3>은 현행법, 간편결제 서비스 보안, 개인정보 영향평가 등의 항목을 기준으로 개인정보보호 자가평가항목을 도출한 방법론을 도식화하였다.



〈Figure 3〉 Deduction Methodology of Personal Information Protection Self-Checklist

〈Table 4〉 Personal Information Protection Self-Check List of Fintech Service

Personal Information Protection Self-Check List of Fintech Service(Simple Payment)				
Classification		Check List		Prerequisite item
1. Collecting of Personal information	Check the personal information consent item	(1)	Do you separate consent items for the collection of personal information as below and receive consent from each? ① Purpose of collecting and using ② Items of Personal information to be collected ③ Period for which personal information is held and used ④ Fact that a subject of information has a right to has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent	○
		(2)	Do you separate the consent items on providing the personal information by a third person as below and can you check the consent items? ① A recipient of personal information ② Purposes for which a recipient of personal information uses such information ③ Items of personal information to provide ④ Period for which a recipient of personal information holds and uses such information ⑤ The fact that a subject of information has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent	○
		(3)	Can I confirm the items consent of the legal representative for the collection and processing of the personal information of a child under the age of 14 years?	○
		(4)	Are there any items requiring a separate agreement if using the personal information for other purposes than the purpose of receiving personal information?	○
		(5)	Can you distinguish the personal information items that can be processed without the consent from the one requiring the personal information items?	○
		(6)	Can I check a veto for the collection if collecting personal information is not necessarily?	
		(7)	Are there the procedure items required to be noticed individually and to receive · consent if different from the purpose of the existing collection and use when collecting individual information additionally to the traditional Personal Information?	

Personal Information Protection Self-Check List of Fintech Service(Simple Payment)				
Classification		Check List		Prerequisite item
	Check the collecting and using purpose item of personal information	(8)	Can I see the purpose of collecting personal information?	○
		(9)	Can I check the items that provide the guidance and legal basis of the facts of collecting personal information?	○
		(10)	Can I check the items personal information that you collect?	○
		(11)	Can I definitely check the items for the financial information required for payments and remittances?	○
		(12)	Can I check the details on how to collect personal information?	○
		(13)	Do you distinguish between mandatory collecting items and optional collecting items?	○
		(14)	Do you collect social security numbers even when there is legislation based?	○
		(15)	Do you notice the details on a minimum of personal information collected?	
		(16)	Do you use alternate means (i-pin) for collecting social security numbers during sign-up	○
2. Management and possess of personal information	Check the period item for which personal information is held and used	(17)	Can I see clearly the reason for holding the privacy	○
		(18)	Can I check the use and preservation period according to the personal information items that you have?	○
		(19)	Do you clearly explain about the legal basis, purpose, and scope for you use that for the purpose of using the personal information held by others	○
3. Use and Provision of personal information	Check the entrusted handling item of personal information	(20)	Can I check the following matters on the entrusted handling of personal information via a third party? ① The person to whom the handling of personal information is to be entrusted ② Purpose, details and scope of the business affairs subject to the entrusted handling of personal information ③ Matters concerning restrictions on re-entrust ④ Restriction to access to personal information ⑤ Details regarding the check and supervision of personal information management during entrusted affairs ⑥ Check whether to exist information and referral service that the consignor's website ⑦ Protective measures necessary for securing safety of personal information, Etc.	○

Personal Information Protection Self-Check List of Fintech Service(Simple Payment)					
Classification			Check List		Prerequisite item
	Matters concerning providing a third person with personal information	Purposes and items when providing personal information to a third party	(21)	Can I check the following items (payment, remittance, Etc.) by service when providing services a third party? ① A recipient of personal information ② Purposes for which a recipient of personal information uses such information ③ Items of personal information to provide ④ Period for which a recipient of personal information holds and uses such information	○
			(22)	Can I check the contents of the penalty related services in accordance with the denial rights and denial of the consent on providing service to a third party?	○
		Items to check when the information to a third party other than the purpose	(23)	Do you have any content of making the following items known to the user if agreeing on providing personal information to a third party other than the purpose? ① A recipient of personal information ② Purposes for which a recipient of personal information uses such information ③ Items of personal information to provide ④ Period for which a recipient of personal information holds and uses such information ⑤ Securing safety of personal information ⑥ The fact that a subject of information has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent, Etc.	○
4. Destruction of Personal Information	Check the procedure and method item for destruction of the personal information		(24)	Can I check the following items with respect to personal information destruction? ① Destruction-related content - The principle is to be immediately destroyed. ② Destruction procedure ③ Destruction method - When they are in Electronic format: permanent and irrecoverable deletion - Destruction of burning if records, printed mater or writings other than	○
			(25)	Do you notify the matter to the data subject after destroying personal information?	○

Personal Information Protection Self-Check List of Fintech Service(Simple Payment)				
Classification		Check List		Prerequisite item
5. Securing safety of personal information	Check the securing safety item of personal information	(26)	Do you take the following precautions to ensure safety of personal information? 1) Technical measures ① Encryption of personal information - Whether to encrypt measure of personal information - Whether to save of one-way encrypted passwords - Reliable or not concerning additional authentication method (pattern authentication, etc.) to the password for payment ② Whether to network encryption communication ③ Securing safety of personal information processing system - Whether to use Vaccine Program - Restriction to access to Personal Information Management System - Whether to regular backup personal information and transaction information - Management of password. Etc. ④ Whether to run Personal Information Leakage System ⑤ Whether to run an antivirus program when executing mobile app runtime ⑥ Whether to apply anti-hacking technology of keyboard when inputting such sensitive information as device ID, password, account number, card number, etc. in a personal information processing terminal ⑦ Whether to check if the mobile app has been forged ⑧ Protection measures for personal information displayed limit - Whether to apply masking(*) when entering such personal information as sign-up: date of birth, phone number, Etc. 2) Administrative management ① Whether to establish and implement an internal control plan to protect personal information ② Whether personal information-related staff and employees have personal information education ③ Whether to minimize the number of staffs handling personal information ④ Whether to run a personal information - related team 3) Physical management ① Whether to take security measures, such as access control for personal information storage area 4) Whether to Information Security Certification ① Personal Information Management System certification (PIMS) ② Privacy impact assessment certification (PIA) ③ Information Security Management System certification (ISMS) Etc.	○

Personal Information Protection Self-Check List of Fintech Service(Simple Payment)				
Classification		Check List		Prerequisite item
	Check the safety item when entrusted to a third-party	(27)	Do you have items for the actions to ensure safety when entrusting personal information to a third party?	○
	Check the personal information handling and management policies item	(28)	Can you check the personal information handling and management policies when after signing up services at Homepage or Mobile App?	○
	Check the prevention of and response to an intrusion item	(29)	Did you establish procedures to respond to accidents of intrusion of personal information?, ① Countermeasures against intrusion plan ② Notification of the data subject for the infringement	○
	Check the designation of personal responsible for management of personal information	(30)	Are you designating the manager of protecting personal information?	○
		(31)	Are guiding the personnel in the role of the manager of the personal information protection?	○
6. Leakage reporting and remedying damage	Check the notification , on leakage of personal information item	(32)	Are you guiding the user in the below way on the report of the leak of personal information? ① Reporting Institution ② Reporting Method ③ Notification Contents - Items of leaked personal information - When and how personal information has leaked - Information on means, etc. available to a subject of information to minimize damage that could inflicted on by leakage - A person information manager's actions and damage remedy procedures - A department in charge of receiving reporting, etc. and contact if damage is inflicted on a subject of information	○
	Remedying damage item	(33)	Are you guiding the user in the way of remedies under the disclosure of personal information? - Personal information dispute mediation committee guide: Application, etc. for mediation - Class actions on personal information	○

Personal Information Protection Self-Check List of Fintech Service(Simple Payment)				
Classification		Check List		Prerequisite item
7. Etc.	Methods and procedures of User and legal representative right, Notification of details of using personal information	(34)	Are you guiding the contents and methods concerning · reading · correcting · deleting and treatment-stopping of personal information?	○
		(35)	Are there certain restrictions on the relevant laws and regulations or contracts in that the user withdraws consent, un-subscription of membership withdrawal, and termination of service, etc.? If there are any restrictions, do you notify the facts to the user in advance or do you state the details in the terms of services?	○
		(36)	Do you offer an easier way of withdrawing the user's consent; reading and providing personal information; or requiring errors to be corrected?	○
		(37)	Are you guiding the user in a way to check the history of use of his/her personal information or provision of the same information to a third party?	○
	Notice when changing management and handling policies (notice obligations)	(38)	Can you confirm the changes or changed items if there are the following changes in personal information? ① Purpose of collecting and using ② Items of Personal information to be collected ③ Period for which personal information is held and used ④ The fact that a subject of information has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/her rejection to give consent ⑤ Personal information handling and management policies	○
	Matters concerning installation, operation, and denial of a device that collect personal information automatically, such as an information file for access to internet;	(39)	Can I check the following items for the information gathering personal information automatically? ① Personal information items automatically collected (cookies, etc.) ② The purpose and used contents of the personal information items that are automatically collected	○
		(40)	Are you guiding the user in a way of rejecting the personal information collected automatically?	○
	Method of personal information handling and management policies notification	(41)	Are you guiding how to notification of management/handling the personal information?	○
	Guidance to personal information-related inquiries	(42)	Are you guiding the user in the procedures and methods related to personal information matters?	○

〈Table 5〉 Legal Basis of Self-Check List

List	Legal Basis					
	Personal Information Protection Act	Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc	Standard Personal Information Security Guideline	Technical and Administrative Protection Standard of Personal Information	Securing Safety Standard of Personal Information	Etc.
(1)	Article 15 Article 22	Article 22	Article 13			
(2)	Article 17	Article 24-2				
(3)	Article 22	Article 31				
(4)	Article 18	Article 24-2				
(5)	Article 22					
(6)						Corporation PIA
(7)						
(8)	Article 15	Article 22				
(9)	Article 15	Article 22	Article 6			PIA
(10)	Article 15	Article 22				
(11)	Article 15	Article 22				
(12)		Article 27-2				
(13)	Article 16					Corporation PIA
(14)	Article 24-2					
(15)	Article 16	Article 23				
(16)	Article 24-2	Article 23-2	Article 17			PIA
(17)		Article 27-2	Article 12			
(18)	Article 15 Article 30	Article 22 Article 27-2	Article 56			
(19)	Article 18 Article 19		Article 9			PIA
(20)	Article 26 Article 30	Article 25 Article 27-2	Article 20			Corporation PIA
(21)	Article 17	Article 24-2	Article 8			
(22)	Article 17	Article 24-2				
(23)	Article 18		Article 9			
(24)	Article 21	Article 27-2 Article 29	Article 11			
(25)		Article 29				

Legal Basis						
List	Personal Information Protection Act	Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc	Standard Personal Information Security Guideline	Technical and Administrative Protection Standard of Personal Information	Securing Safety Standard of Personal Information	Etc.
(26)	Article 24 Article 29	Article 28 Article 45		Article 3 Article 6 Article 7 Article 9	Article 3 Article 4 Article 6 Article 8 Article 9	- Internet Banking Security Guide Ⅳ Mobile-Banking(KFTC) - Smart Phone Electronic Financial Service Security Guide(FSI)
(27)	Article 26					
(28)	Article 30	Article 27-2	Article 34			
(29)	Article 62	Article 48-3 Article 48-4				
(30)	Article 31	Article 27	Article 22 Article 23			
(31)	Article 31	Article 27	Article 22 Article 23			
(32)	Article 34	Article 27-3	Article 26 Article 27 Article 28 Article 29			
(33)	Article 43 Article 51					
(34)	Article 4 Article 35 Article 36 Article 37 Article 38 Article 39	Article 30	Article 20 Article 31 Article 32 Article 33			
(35)		Article 30				Corporation PIA
(36)		Article 30				
(37)		Article 30-2				
(38)	Article 30	Article 27-2	Article 35			
(39)		Article 27-2				
(40)		Article 27-2				
(41)	Article 30					
(42)		Article 27-2				

4. 핀테크 서비스 개인정보보호 자가평가항목 활용

4.1 개인정보 자가평가항목 설문조사 분석

개인정보보호 자가평가항목에 대한 설문조사는 간편결제 서비스의 개인정보보호에 대한 이용자의 인식 확인 및 평가항목에 대한 필요성을 검증하고자 하였다. 설문 대상자는 본 논문에서 한정한 이용자에 부합하도록 현재 핀테크 서비스를 이용하고 있으며, 개인정보 및 정보보호에 대한 인지도가 있고 개인정보보호에 대한 합리적인 선택이 가능한 정보보안에 관련된 직원 및 학생 등 67명을 대상으로 진행하였다. 조사항목은 총 18개 항목으로 간편결제 서비스와 자가평가항목에 대한 문의로 구성되며, 관련 사항을 중심으로 결과를 분석한다.

첫 번째로 간편결제 서비스의 개인정보보호에 대한 이용자들의 인식에 대한 설문 결과를 정리하면 응답자들이 핀테크 서비스를 선택하는 기준으로는 60%가 편의성을 선택했으며, 그 다음으로 보안성(25%), 광고 등에 의한 인지도(14%)를 선택하였다. 이는 간편결제 서비스에 대한 특성인 결제의 편의성을 선택에 중요한 기준으로 두는 것을 확인할 수 있다. 간편결제 서비스 이용 시 개인정보에 대한 안전성 여부가 서비스 선택 및 이용에 중요하다고 응답한 이용자는 90%(매우 중요하다 포함)이며, 응답자의 53%가 개인정보보호에 관한 사항을 확인하며, 그 중 75%가 개인정보 취급/처리방침을 통하여 확인하는 것으로 조사되었다. 또한 간편결제 서비스 이용 시 자신의 개인정보 등이 안전하게 취급 보호되고 있지 않다고 생각하는 응답자가 41%로 그 이유로 기업에서 제공하는 개인정보보호에 대한 사항을 신뢰할 수 없거나(53%), 개인정보보호 관련 조치 사항을 확인하기 힘들기(32%) 때문이라고 하였다. 이와 관련하여 개인정보보호에 관한 안내 사항을 확인 쉽다고 생각하는지에 대한 문의에 대해서는 94%가 어렵다고 응답하였으며, 그 이유로는 개인정보보호 관련 안내 사항이 많고 복잡해서(48%), 개인정보보호 관련 사항을 어떻게 확인해야 하는지 몰라서(43%)로 응답을 하였다.

위의 조사결과 확인하였을 때, 실제 응답자들은 간편결제 서비스 이용 시 개인정보보호에 대한 안전성이 중요하며, 관련 사항을 확인하고 있으나, 실제 개인정보보호가 안전하게 취급・보호되고 있지는 않다고 생각하며, 관련 사항을 실제 확인하기 쉽지 않은 것으로 정리할 수 있다.

두 번째로 개인정보보호 자가평가항목에 대한 설문 결과를 정리하면, 이용자들의 평가항목에 대한 중요도는 응답자의 87%가 중요하다 이상(매우 중요하다 포함)으로 응답하였으며, 그 중 개인정보의 안정성 확보 항목이 39%로 가장 중요하며, 그 다음으로 개인정보의 수집(22%)이 중요한 것으로 조사되었다. 또한, 평가항목 중 추가적으로 도출된 항목, 개인정보 안전성 확보 항목, 침해사고 대응 항목, 개인정보 유출 신고 및 피해구제 방법에 대한 필요성에 대한 조사는 필요하다 이상(매우 필요하다 포함)으로 89%가 응답하였다.

개인정보보호 자가평가항목과 같이 개인정보보호에 대한 사항을 확인할 수 있는 평가항목이 있으면 좋은지에 대한 설문에 대해서는 응답자 93%가 '있으면 좋겠다'라고 응답하였

으며, 해당 평가항목으로 실제 서비스 이용 및 선택 시 이용할 의향이 있냐는 설문에 84%가 의향이 있다고 조사되었다.

개인정보보호 자가평가항목에 대한 설문결과를 확인하였을 때, 도출한 평가항목에 대한 중요도는 높은 편이며, 개인정보보호 자가평가항목 활용에 대한 이용자의 필요성을 확인할 수 있었다.

설문 조사에 따른 내용을 종합 정리하면, 간편결제 서비스를 이용 및 선택함에 있어 개인정보보호 관련 사항들은 중요하지만, 실제 이용자들은 해당 사항을 확인하기 힘들며, 본 논문에서 도출한 개인정보보호 자가평가항목을 활용하여 이용자들이 개인정보보호 관련 사항을 확인하는데 필요성이 있음을 확인하였다.

4.2 개인정보보호 자가평가항목 사례 적용

도출된 개인정보보호 자가평가항목을 통해 실제 간편결제 서비스를 제공하는 두 개의 기업을 대상으로 개인정보보호 수준을 진단하여 현황 및 문제점 등을 확인하고, 앞서 조사한 설문 대상자 중 일부 대상자에게 자가평가항목을 통해 실제 간편결제 서비스 평가를 진행함으로써 그 실효성을 검증하고자 한다.

A 간편결제 서비스는 온라인 쇼핑몰에서 상품 구매 시 스마트폰으로 청구내역이 수신되고 이를 결제하는 기업으로써, 개인정보 자가평가항목의 총 42개 중 22개의 항목을 확인할 수 있었으며, 전반적으로 이용자가 개인정보보호 항목에 대한 사항을 확인하기 위한 분류 및 내용정리가 정형화 되어있지 않았다. 평가항목으로 결과를 정리하면, 개인정보 수집의 항목 중 필수・선택 수집 항목을 구분하고 있지 않으며, 결제 및 송금 시 필요한 금융정보 수집 항목에 대해 명확히 안내하고 있지 않았다. 개인정보 취급위탁에 관한 사항은 위탁하는 업무의 목적, 범위 및 내용에 관한 사항이 구분되어 설명되어 있지 않으며, 개인정보 안전성 확보 항목에서도 물리적 조치 등에 관한 사항은 고지하고 있지 않았다. 또한 인터넷 접속 정보파일 등 개인정보 자동 수집에 관한 사항에 대해서는 수집항목에 대한 정보를 간략히 설명하고 있어, 자세한 내용을 확인하기 어렵다.

B 간편결제 서비스는 간편결제, 송금 등의 서비스를 제공하며, 신용카드 정보를 등록하여 인터넷 쇼핑몰 등에서 비밀번호만으로 결제를 할 수 있도록 하는 기업이다.

개인정보 자가평가항목 중 28개의 항목을 확인할 수 있으며, 이용자가 확인하기 쉽도록 개인정보보호 항목을 분류하고, 전반적으로 내용 설명도 자세히 고지하고 있다. 개인정보 수집의 항목에 대해서는 수집하는 목적을 필수・선택 항목을 구분하고, 결제 및 송금 시 필요한 금융정보 항목을 분류하여 고지함으로써, 이용자가 간편결제 이용 시 어떤 정보가 이용되는지 알 수 있도록 하고 있다. 개인정보 제 3자 제공 및 취급위탁 항목의 경우 제공・위탁 받는자, 제공・위탁 업무의 목적・범위・내용, 위탁 시 개인정보의 관리 현황 점검 등에 관한 사항에 대해 이용자가 명확히 알 수 있도록 분류하여 고지하고 있다. 하지만 동의철회에 관한 사항 및 인터넷 접속 정보파일 등 개인정보 자동 수집에 관한 사항에 대해서는 앞의 사례와 같이 고지에 대한 내용이 간략히 설명되어 있어 이용자가 해당 내용을 명확히 확인하기 어렵게 되어 있다.

위의 두 사례를 종합하였을 때, 이용자의 입

장에서 개인정보보호 관련 사항을 확인 후 간편결제 서비스를 이용 및 선택 시 개인정보가 어떻게 취급・관리되고 있는지에 대한 정보를 보다 쉽고 자세하게 확인할 수 있으며, 자가평가항목에서 보다 많은 항목을 확인할 수 있는 'B 간편결제 서비스'를 이용하는 것이 더 합리적인 선택으로 볼 수 있다. 하지만 두 사례 모두 개인정보보호에 대한 개인정보 취급방침 등의 필수 항목들은 고지를 하고 있으나, 평가항목 중 개인정보를 목적 외로 보유・이용하거나, 위탁하는 경우 등의 확인이 필요한 사항 등은 고지되고 있지 않거나 확인이 어렵게 되어있다. 또한, 개인정보 취급방침의 형식 등이 정형화 되어 있지 않고 서술형식으로 적어놓아 이용자들이 해당 내용을 쉽게 확인하기 쉽지 않다.

즉, 필요 항목에 대해서는 고지는 되고 있으나, 추가적인 항목이나 세부항목에 대한 내용은 자세히 고지되어 있지 않아, 이용자가 확인할 수 있는 정보가 제한적이다. 또한 도출한 평가항목을 전부 고지 및 게시를 해야 하는 것은 아니지만, 항목에 대한 내용이 없어 실제 해당 사항이 없어 고지를 안 하는 건지, 고지가 자체가 누락이 된 건지를 확인하기가 어렵다.

각 사례에 대한 자가평가항목 적용 결과를 정리하면 <Table 6>과 같이 정리할 수 있으며, 각 항목별 전체 평가항목 수 대비 확인된 평가항목 수를 나타내었다.

설문 대상자를 통한 자가평가항목 실효성 검증 시 대상 참여자 총 23명 중 23명이 'B 간편결제 서비스'를 선택하였다. 'B 간편결제 서비스'의 선택의 이유로 해당 자가평가항목을 통한 평가 시 'A 간편결제 서비스'보다 개인정보보호에 관한 사항을 자세히 확인할 수 있으며, 자가평가항목 별로 내용이 보다 잘 정리되어있어 확인이 용이하다는 점을 들었다. 또한 각 간편결제 서비스에 대한 자가평가항목에 대한 비교를 통해 보다 많은 사항을 확인할 수 있는 'B 간편결제 서비스'를 선택의 이유로 들었다. 추가적으로 'A 간편결제 서비스'의 개인정보보호 관련 사항이 'B 간편결제 서비스'보다 간략하게 고지되어 있어 평가 시 내용 확인은 쉬웠으나, 종합적인 평가를 비교하였을 때 보다 많은 사항을 확인할 수 있었던 'B 간편결제 서비스'를 선택하였다는 의견도 있었다.

실제 이용자의 자가평가항목 진단을 통한 결과를 정리해보면, 각 간편결제 서비스를 자가평가항목을 통해 평가를 진행한 후 해당 평

〈Table 6〉 Result of Personal Information Protection Self-CheckList Case Application

Classification	A case	B case
Collecting	7 / 16	10 / 16
Management and Possess	2 / 3	2 / 3
Use and Provision	2 / 4	4 / 4
Destruction	1 / 2	1 / 2
Securing Safety	4 / 6	5 / 6
Leakage reporting and Remedying damage	1 / 2	1 / 2
Etc.	5 / 9	5 / 9
Total	22 / 42	28 / 42

가 결과를 비교할 수 있어 유용하며, 고지되는 항목 중 어떠한 부분이 부족하게 설명되어 있는지와 자신이 어떠한 항목을 확인해야 하는지 등을 알 수 있어 선택에 도움이 된다고 하였으나, 자가평가항목 수가 많아 평가 시간이 다소 많이 소요된다고 지적하였다.

실제 대상자를 통한 자가평가항목 사례 검증을 통해 평가항목의 이용자들에게 간편결제 서비스의 개인정보보호 항목에 대한 유용성을 확인함에 따라 그 실효성을 검증하였으나, 핀테크 서비스 기업에서 개인정보보호에 대한 고지부분을 이용자 입장에서 확인하기 용이하도록 필수적인 내용을 간략하게 정리할 필요성이 있으며, 평가항목 수에 대한 지적 사항은 가중치 부여에 따른 항목 정리 및 전문가 의견 수립을 통한 방법 등 향후 추가적인 연구를 통해 간소화 할 수 있도록 하는 개선점도 제시하였다.

4.3 핀테크 서비스 이용자 개인정보보호를 위한 정책 제언

본 연구의 개인정보보호 자가평가항목을 통하여 이용자들이 핀테크 서비스의 개인정보보호 관련 필수사항들을 확인하고, 어떠한 개인정보 항목들을 확인해야 하는지에 대해 확인할 수 있었다. 하지만 해당 평가항목을 통해 사례 검증 및 설문을 통하여 도출된 핀테크 서비스의 개인정보보호에 대한 문제점 및 향후 이용자 보호를 위하여 3가지 정책적 제언을 하고자 한다.

첫 번째로 개인정보보호 자가평가항목으로 확인한 결과에서 핀테크 서비스의 개인정보보호에 대한 수준을 이용자가 확인하기에는 정보가 부족하거나, 제한적이었다. 이에 핀테크 서비스 기업은 제시하고 있는 개인정보보호와 기술적 보안 항목들에 대한 사항과 이용자가 알 수 있는 정보에 대한 격차가 생기지 않도록 충분히 정보를 공유할 수 있도록 해야 한다. 즉, 보안 공시 제도나 개인정보 취급방침 등에 보다 자세한 보안관련 사항을 게시하여, 이를 통해 정보의 불균형이 생기지 않도록 하여, 이용자가 자신의 개인정보가 실제 안전하게 보호되고 관리되고 있는지를 확인할 수 있도록 해야 한다.

두 번째로 개인정보 취급방침에 대한 내용의 형식을 정형화 하여, 이용자가 해당 사항을 명확히 인지할 수 있도록 해야 한다. 앞에서 사례검증 등을 통해 살펴본 바와 같이 평가항목을 통해서 진단 시에도 각 서비스별로 취급방침의 형식이나 내용 기술 방법이 상이하여, 평가가 쉽지 않음을 확인할 수 있었다. 실제로 개인정보 취급방침을 확인하지 않는 이유 중 '내용이 많거나 어려워 이해하기 힘들다'는 조사결과가 있었다[13].

정형화된 개인정보 취급방침을 통하여, 이용자가 개인정보보호 항목을 쉽게 확인할 수 있도록 정비가 필요하다.

세 번째로, 실제 핀테크 서비스 기업이 공지하고 있는 개인정보 정책 및 안전성 등의 항목에 대해 직접적인 진위여부를 확인하기가 힘들다. 또한, 이용자들이 해당 사실에 대한 확인을 위한 기관 및 제도적 장치가 마련되어 있지 않다.

미국 연방거래위원회(FTC)에서는 웹사이트 운영자가 자사 웹사이트에 고지된 프라이버시 정책을 준수하지 않았거나 적용을 받는 일체의 자율규제 차원의 가이드라인을 이행하지

않는 경우에는 사기적 수단 중 하나인 허위사실의 공언(misrepresentation)에 해당되어 FTC의 제제를 받을 수 있다. 또한, 영국의 정보보호청은 자신의 개인정보의 처리로 인하여 직접 불이익한 영향을 받고 있거나 그렇게 믿고 있는 개인은 문제의 개인정보처리가 개인정보보호법의 규정을 준수하고 있는지 여부에 대한 감사(assessment)를 정보보호청에 요청할 수 있다[15].

이와 같이 국내에서도 이용자가 핀테크 서비스 이용 외에도 기업에서 공시하고 있는 개인정보보호 정책 등의 진위성을 확인할 수 있도록 제도적 장치나 개인정보관련 기관의 역할 추가가 필요하다. 이를 통해 이용자는 기업에서 고지하고 있는 개인정보보호 정책 등의 진위를 확인하여 실제로 고지에 대한 이행여부를 확인하고, 기업이 개인정보보호 정책을 허위로 고지하는 것을 방지하는 방안을 마련할 수 있을 것이다.

5. 결론 및 향후 연구방향

본 논문에서는 현재 핀테크 서비스 산업이 활성화됨에 따라 개인정보 유출 등의 보안 위협이 증가되고, 이에 핀테크 서비스 중 간편결제 서비스를 대상으로 이용자들이 해당 서비스를 선택 및 이용 시 개인정보보호에 대한 안전성 등을 확인할 수 있도록, 개인정보보호 자가평가항목을 도출하였다. 또한, 평가항목의 이용 시 필요성 및 실효성을 확인하기 위해 간편결제 서비스 이용자를 대상으로 설문을 진행하였다. 본 설문을 통해 이용자들이 간편결제 서비스를 이용 및 선택할 경우 개인정보보호 관련 사항을 확인하기 위해 해당 평가항목이 도움이 되며, 평가항목의 필요성과 실효성을 확인할 수 있었다. 그리고 평가항목을 실제 간편결제 서비스에 적용하여 사례검증을 하였으며, 본 연구를 바탕으로 향후 핀테크 서비스 이용자의 개인정보보호를 위한 정책을 제언하였다.

서비스를 제공하는 기업의 관점이 아닌 실제 서비스를 이용하는 이용자의 입장에서 확인해야 할 개인정보보호를 위한 평가항목을 도출하였고, 그 실효성을 입증했다는 점에서 의의가 있다. 하지만 이용자 선정을 일반 모든 이용자를 대상으로 적용하지 못하였으며, 해당 평가항목을 산술적인 평가지표로 활용하기에는 제한적으로 이용자들의 입장에서 개인정보보호 관련 항목을 확인할 수 있는 가이드 수준의 제시라는 점에서 본 논문의 한계로 지적할 수 있다.

향후 본 연구를 통해 도출한 평가항목을 개인정보 영향평가 등과 같은 평가지표로 활용하기 위해서는 연구가 더 필요하며, 실제 이용자 자가평가를 통해 제시되었던 자가평가항목 수에 대한 간소화 방안 마련과 간편결제 서비스뿐만 아니라, 핀테크 서비스 전반 및 그리고 개인정보를 이용하는 모든 서비스 등에 대해 실제 모든 일반적인 이용자의 입장에서 자신의 개인정보보호를 위한 범용적인 평가지표를 수립하는데 기여가 가능하도록 앞으로 연구가 진행되어야 할 것이다.

References

[1] Chris Jay Hoofnagle, “Alan Westin’s Pri-

vacy Homo Economicus," Berkeley Law Scholarship Repository, 2014.

[2] DMC Media, "Mobile Simple Payment Using State Survey," 2015.

[3] Eugene Investment and Securities, "Fintech Series 2nd," 2015.

[4] Financial Security Institute, "Fintech Status and Prospect," 2015.

[5] Financial Services Commission, Financial Dictionary, http://www.fsc.go.kr/.

[6] Jang, S. S., "Fintech on the information security industry impact study," Internet and Security Focus, Feb 2015.

[7] Korea Internet and Security Agency (KISA), "2012 Information Security Survey Report (Individual)," 2012.

[8] Korea Internet and Security Agency (KISA), "Introduce PIMS" Menu, http://isms.kisa.or.kr/kor/intro/pimsIntro01.jsp.

[9] Kim, J. Y., "Analyzing Effects on Firms' Market Value of Personal Information Security Breaches," The Journal of Society for e-Business Studies, Vol. 18, No. 1, pp. 1-12, 2013.

[10] Lee, C. H., "A Framework and Guidelines for Personal Data Breach Notification Act," Korea Institute of Information Security and Cryptology, Vol. 21, No. 5, pp. 169-179, 2011.

[11] Lim, S. J., "Fintech Security Trend," TTA Journal, 2015.

[12] Ministry of Government Administration and Home Affairs, "Privacy Impact Assessment Guidelines," 2015.

[13] Ministry of Science, ICT and Future Planning, Reason of do not check the personal information handling, http://kosis.kr/statHtml/statHtml.do?orgId=329&tblId=TX_342_2009_H2122&vw_cd=MT_ZTITLE&list_id=342_34205_002_001&conn_path=F0&path=, 2013.

[14] No, S. H., "A comparison study on Korea's Mobile environment simple payment services," The Korea Society of Management Information Systems, pp. 695-698, 2014.

[15] Personal Information Protection Commission, A study on Foreign Personal Information Security Execution System and Personal Information Security Trend Investigation, 2012.

[16] Pew Research Center, http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance, 2015.

[17] Ponnurangam Kumaraguru, Privacy Indexes: A Survey of Westin's Studies, Institute for Software Research International School of Computer Science Carnegie Mellon University, Dec. 2005.

[18] SFIS 2015 Smart Financial and Information Security Fair, http://www.mt.co.kr/view/mtview.php?type=1&no=2015022419214561437&outlink=1, 2015.

[19] Terms.naver.com, Financial Dictionary, http://terms.naver.com/entry.nhn?docId = 2717871&cid=55594&categoryId=55594.

저 자 소 개

강민수 (E-mail: kozinaru@korea.ac.kr)
2011년 고려대학교 산업시스템정보공학과 (학사)
2011년~현재 고려대학교 정보보호대학원 정보보호학과 (석사과정)
관심분야 개인정보보호, 핀테크, 정보보호정책

백승조 (E-mail: nomadvirus@korea.ac.kr)
2005년 세종사이버대학교 정보보호시스템공학과 (학사)
2007년 고려대학교 정보경영공학전문대학원 (석사)
2015년 고려대학교 정보경영공학전문대학원 (박사)
현재 고려대학교 정보보호대학원 연구교수
관심분야 정보보호정책, 사이버안보, 개인정보보호

임종인 (E-mail: jilim@korea.ac.kr)
1980년 고려대학교 수학과 (학사)
1982년 고려대학교 수학과 (석사)
1986년 고려대학교 수학과 (박사)
현재 고려대학교 정보보호대학원 교수, 고려대학교 사이버국방학과 교수
관심분야 정보보호정책, 사이버안보, 개인정보보호