http://dx.doi.org/10.15813/kmr.2015.16.4.003

# 금융혁신을 위한 핀테크 서비스의 보안 리스크 대응방안 연구 *

## A Study of Countermeasure against Security Risk of Fintech Services for Financial Innovation

**박정국 (Jeong-Kuk Park)****

금융결제원 금융결제연구소, arspark@kftc.or.kr

**김인재 (Injai Kim)*****

동국대학교 경영학부, ijkim@dongguk.edu

**ABSTRACT**

Fintech, which means the convergence of finance and information technology, becomes a hot topic in the financial sector. Through innovative activities on financial services, ICT(Information and Communication Technology) is integrated into the overall financial industry, and a new form of financial services could be expected to improve the existing financial system.

On the other hand, fintech services are relatively vulnerable to security issues. Due to the process simplication and the channel fusion, the leakage of personal and financial informations, authentication bypass,phishing, and pharming are getting more concerned.

In this study we investigated the security risk of fintech services in the viewpoints of service provider, technology adoption, and security policy. The possible countermeasures to reduce those risks are suggested because security is an important criterion for selecting financial services.

This study basically offers quantification of the potential security risks and step-by-step control measures about business processes in the fintech services. The suggested security model includes user authentication, terminal security, payment information protection, API(Application Programming Interface) security, and abnormal transaction monitoring. This study might contribute to an understanding of the security risks and some possible measures for mitigating those risks on the practical perspective.

*Keywords: Fintech, Security Risk, Financial Service Innovation, Reliability, Financial Transaction*

* 논문접수일:2015년 9월 11일; 1차 수정: 2015년 11월 6일; 2차 수정: 2015년 11월 20일; 게재확정:2015년 12월 5일

** 주저자

*** 교신저자

# I. 서론

벤처 전문 조사회사(Venture Scanner 2015)[1]에 따르면 알리바바, 애플 등과 같은 글로벌 IT사업자를 비롯하여 2015년 11월 현재, 전세계 54개국에서 1,362개 핀테크 기업이 지급결제, 대출, 개인자산관리, 소액투자, 해외송금 등 금융업 전 영역에서 활동하고 있으며 2014년 핀테크에 투자된 자금은 122.1억 달러로 2013년 40.5억 달러에 비해 3배 이상 증가한 것으로 나타났다. 핀테크는 금융서비스에 대한 혁신 활동의 일환으로 이해할 수 있으며 이를 통해 기존의 금융 관련 업무들이 더 효율화되고, 금융거래과정이 좀 더 편리해질 것이며 나아가 새로운 상품과 서비스를 통한 신규 시장의 창출까지도 기대되고 있다(금융위원회 2015;이남희 외 2012; 허용석 외 2013).

한편, 소비자의 편의성을 중시하며 채널·서비스·기술 간에 융복합이 일어나는 환경에서 제공되는 핀테크 서비스는 상대적으로 보안성이 취약하기 때문에 이를 겨냥한 공격 발생 가능성이 높아질 것이다. 한국은행 조사(2015)에 따르면 모바일결제를 이용하지 않는 주된 이유가 개인정보 유출 우려(78.3%)와 안전장치에 대한 불신(75.6%)인 것으로 나타났다. 더욱이 핀테크를 통해 금융서비스에 대한 새로운 접근 채널이 확대됨에 따라 개인정보 유출, 해킹 등 보안 사고에 대한 우려는 더욱 커질 것으로 예상된다.

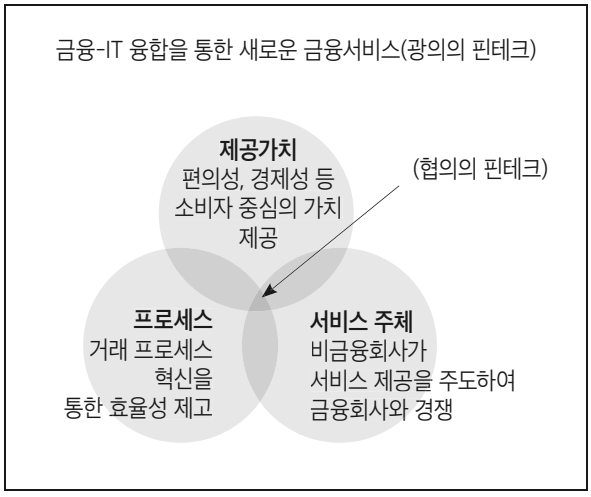
핀테크 서비스의 활성화 여부는 사용자 인증, 고객정보 보호, 이상거래탐지 등 이러한 보안적 요소를 비즈니스 모델 안에 어떻게 재구성해서 안전함과 편리함을 유도해 내느냐가 관건이 될 것이다. 이에 본 연구에서는 정보보안 관점에서 핀테크 서비스의 보안리스크를 분석하고 이러한 보안리스크를 줄이기 위한 대응방안을 제시하고자 한다.

1) http://insights.venturescanner.com/category/financial-technology/

# II. 핀테크 이해

## 2.1 개념

핀테크(Fintech)는 주지하는 바와 같이 금융(Financial)과 기술(Technology)의 합성어로 IT기술을 이용하여 기존 금융기법과 차별화된 새로운 형태의 금융서비스 또는 금융 시스템과 서비스를 효율적으로 만드는 기술로 정의할 수 있다(금융위원회 2015;Ernst & Young 2014). 사실 핀테크가 주목받기 전부터 금융권에서는 IT기술을 도입해 활용해 왔으나 최근의 핀테크가 과거와 다른 점은 종전에는 금융회사들이 필요에 따라 IT기술을 주도적으로 채택해 활용해온 반면, 금융분야에서 기술의 중요성이 증가함에 따라 고도의 IT 역량을 보유한 비금융회사들이 금융 관련 영역으로 진출하여 영향력을 확대하고 있다는 사실이다. 또한 핀테크 트렌드의 핵심은 서비스 주체 외에도 제공가치, 프로세스 맥락에서도 찾을 수 있다(<그림1>참조, 박정국,김인재 2015).




<그림 1> 핀테크 개념

## 2.2 등장 배경

핀테크 등장배경은 기술 발전과 금융기관의 경쟁력 관점에서 살펴 볼 수 있다. 첫째, 전례 없는 빠른 속도

로 보급된 스마트폰을 기반으로 하는 디지털 혁신 환경은 핀테크가 전세계적으로 부상하게 된 핵심배경이자 성장의 주요 동력이다. 스마트폰을 중심으로한 모바일 기술 혁명은 상호간 정보 공유를 확대시키고, 오프라인 시장에 가거나 PC앞에 앉지 않더라도 손안의 모바일만 이용하면 언제 어디서든 구매할 수 있는 편재적 소비를 확대시켰으며, 나아가 금융서비스에 대한 세분화된 니즈를 증가시켰기 때문에 IT 경쟁력을 갖는 기민한 기업의 등장을 불러왔다. 둘째, 금융업은 전통적으로 규제, 규모의 경제, 신뢰도가 경쟁력의 근간을 이루어왔으나 최근 국내 전자지급결제대행사업자(Payment Gateway)에게 카드정보 저장 허용 그리고 미국의 스타트업 양성 및 크라우드펀딩 법적 허용 등과 같은 규제 완화, 지점의 저 수익화에 따른 규모의 경제 우위 축소, 그리고 금융업의 신뢰도 저하에 따른 탈중개화(Disintermediation) 현상 등으로 경쟁우위가 희석되면서 위기에 봉착한 금융기관들은 혁신적인 금융기법을 이용하여 새로운 수익모델을 발굴하기 위해 노력하는 과정에서 이에 대한 대안의 하나로 핀테크가 등장하였다(김남훈 2015a,b).

### 2.3 핀테크 현황

핀테크 사업분야는 광범위한 금융업을 모두 포괄하며 IT 기술 적용이 용이하고 고객의 이용 빈도가 높으며 플랫폼 사업 성격이 강한 지급결제 서비스가 초기 핀테크 시장을 주도하였다. 핀테크형 사업모델은 기존 금융의 비효율성 제거를 위한 거래비용 절감, 거래효율성 제고, 틈새시장 포용 유형과 파괴적 혁신을 추구하는 신시장형으로 분류할 수 있다(<표1>참조, 한국은행 2015).

세계 여러나라에서 핀테크 열풍이 불고 있으나 미국, 영국이 핀테크 시장을 선도하고 있는 가운데 중국, 일본 역시 IT기업의 금융업 진출을 장려하는 등 핀테크 산업 활성화를 위한 정책을 추진하고 있다(Accenture 2015). 국내 핀테크 산업은 투자규모, 사업자 수, 서비스 다양성 등에서 전반적으로 뒤쳐져 있다는 평가를 받고 있으나 정부의 핀테크 육성 정책 등에 힘입어 활성화 될 것으로 예상된다.

<표1> 핀테크 사업모델 및 사례

| 구 분 | 분 야 | 서비스 사례 |
|---|---|---|
| 거래비용 절감 | 지급결제 | Venmo, 2012년 미국에서 시작한 모바일 송금결제 서비스 |
| | 송금 | TransWise, 2010년 영국에서 설립된 온라인 국제 송금 서비스 업체 |
| | 증권거래 | ROBINHOOD, 2013년 미국에서 설립된 온라인 주식거래 서비스 업체 |
| | 뱅킹 | SIMPLE, 2012년부터 각종수수료 면제, 독특한 자산관리기능(PFM)으로 고객유치(2014년 BBVA Compass에 인수) |
| 거래효율성 제고 | P2P대출 | LendingClub, 2006년 미국에서 설립된 P2P대출중개 플랫폼 |
| | 자산관리 | Wealthfront, 소액투자자 대상 1위 미국 온라인 자산운용사 |
| 틈새시장 포용 | 지급결제 | M-PESA, 케냐 최대이통사 Safaricom이 영국 Vodafone과 제휴하여 2006년에 출시한 개인간 모바일결제 및 송금서비스 |
| | 소액대출 | Lenddo, 2011년 소셜네트워크 상에서 구축한 평판정보를 활용하여 개인신용도를 측정하고 대출서비스를 제공 |
| 파괴적 신시장형 | IoT | PROGRESSIVE, IoT와 빅데이터 분석을 활용한 손해보험상품 출시 |
| | 머신러닝 | Zestfinance, 2009년 미국에서 설리된 빅데이터 기반 신용분석 |

## III. 핀테크 서비스의 보안리스크 분석

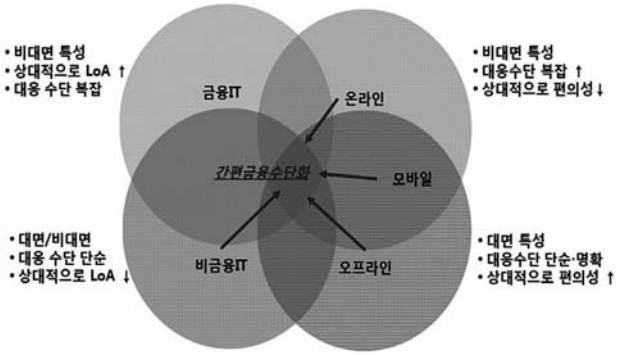
핀테크 열풍을 이끈 페이팔(Paypal)에서 계정이 탈취되는 보안사고가 발생하였듯이 서비스의 안전성 보다는 사용자의 편의성이 중시되는 핀테크 서비스는 개인정보 유출, 해킹 등에 의한 보안리스크 증가가 예상된다.

### 3.1 서비스 주체 변경에 따른 보안리스크

ICT 부문의 경쟁력을 가지고 금융업에 참여하는 비금융회사들은 민감한 정보를 처리하고 보호하는데 있어 금융회사와 같은 경험을 가지고 있지 못하며, 이 문제는 금융정보 뿐만 아니라 개인정보를 가지고 있는 모바일 기기를 이용한 거래의 증가와 금융과 기술 간의 융합 현상으로 인해 증폭될 수 있다(Brown 2013). 금융서비스가 비금융회사와 제휴 또는 외주의 형태로 제공될 경우 금융회사가 직접(in-house) 서비스를 제공하는 것에 비해 고객과의 접점에 있는 비금융회사에서 발생하는 모든 장애 상황을 점검•관리하기 어려워 진다. 또한, 비금융회사가 금융회사 고객의 금융정보를 보유하고 이용함에 따라 개인정보 유출이 확대될 가능성이 있다. 해킹, 사기, 정보유출 등의 사고 발생시 은행과 비금융회사간 책임소재 및 소비자 보호 등과 관련한 리스크가 발생할 수 있다.

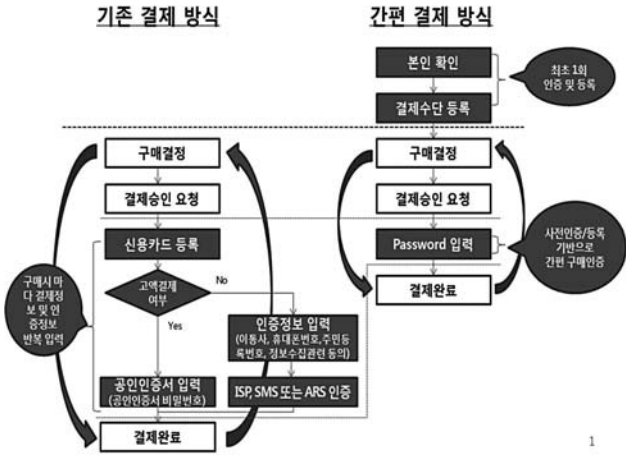
### 3.2 기술 변화에 따른 보안리스크

첫째, 채널·서비스·기술 간의 다양한 융복합 현상이 발생한다(<그림2>참조). 핀테크를 통해 다양한 성격의 비금융회사가 금융업에 진출하여 소비자의 편익을 증가시킬 것으로 예상되지만, 금융IT와 비 금융IT, 온라인과 오프라인, 모바일기술 간의 융복합이 일어나기 때문에 접점을 증가시키고 새로운 취약점을 발생시키는 원인을 제공할 수 있다(금융보안연구원 2015). 이러한 융복합 발생시 온라인 서비스의 경우 기술적 대




<그림2> 채널, 서비스, 기술간 융·복합>

응수단의 복잡도가 증가하고 편의성이 떨어지는 현상이, 오프라인 서비스의 경우 편의성이 향상되는 측면이 있으나 핀테크 서비스가 간편한 금융수단화라는 목표를 달성해 가는 과정에서 전체적 보안수준(LoA : Level of Assurance)이 높은 쪽에서 낮은 쪽으로 내려가는 현상 발생에 대한 대한 우려를 낳고 있다.




<그림3> 결제 처리절차 비교

둘째, 결제단계, 입력되는 정보 그리고 인증방식 등의 간소화를 추구한다(<그림3>참조). 과거에는 이용과정의 불편보다는 안전성을 중시해 공인인증서, 일회용비밀번호, 각종 보안프로그램을 사용하고 거래 시마다 결제정보 및 인증정보를 입력하도록 하여 사고를 예방해 왔다(조규민 2015). 간편결제 방식을 살펴보면 온라인 상거래 구매자가 신용카드 정보(카드번

호, 유효기간 등), 계좌정보 등의 결제정보를 최초 1회 또는 최소한의 횟수로 입력하고 결제 시에는 패스워드 등의 인증만으로 결제가 완료된다. 이러한 인증 및 결제과정의 간소화는 소비자의 결제 편의성을 향상시킨다는 점에서 긍정적으로 평가되나, 카드정보 유출사고 발생 시 부정사용 리스크 증대 등

보안성 약화에 대한 우려가 있다(김종현 2015).

셋째, 핀테크 서비스의 네트워크는 금융회사, 기술벤처기업 등 간의 협력이 필요하고 다양한 매체와 메쉬(Mesh) 구조의 복잡한 네트워크로 연결되어 있어서 한 부분이 뚫리면 금융시스템 전체로 확산될 위험성이 있다. 특히 인터넷 기반의 네트워크 연결이 증가함으로써 서비스 거부공격(DOS), 세션 하이재킹(Session hijacking)[2]등의 보안위협에 노출될 가능성이 높다. 인증기술은 기존에는 사용자단(User-end)에서 카드정보, 단말 플랫폼 보안 그리고 추가 인증수단을 사용하였으나 결제 편의를 위해 초기 인증이 단순화, 비 설치화 하는 형태로 변화하고 있으며, 지문, 정맥을 이용하는 생체인증, IC카드기반 인증 등의 신규 인증기법이 활성화되고 있다. 이러한 신규 인증기법은 보안성이 강화되었음에도 주로 개방형 모바일 플랫폼 환경에서 사용되기 때문에 여전히 ID 도용, 추가인증 우회 그리고 피싱 및 파밍 공격 등 위협이 존재한다.

넷째, 사용자기기의 활용범위가 확대된다. 금융서비스와 IT기술간 결합정도가 심화됨에 따라 시스템(Back-end) 중심에서 네트워크(Middle-end)를 거쳐 사용자(User-end)로 접속기기의 활용범위가 점차 확대되고 있다. 특히 핀테크를 통해 사물과 금융서비스의 접목이 더욱 확산될 것이므로 과거 대형서버를 해킹한 금융정보 탈취가 주를 이루었다면 앞으로는 사물인터넷(IoT)의 취약점을 악용한 보안위협 및 금융사고가 급속히 확산될 수 있다.

### 3.3 보안정책 변화에 따른 보안리스크

해외 주요 국가에서는 소비자가 금융 또는 결제 서비스 채널에 편리하게 접근하고 이용할 수 있는 환경을 마련하는데 정책의 포인트를  맞추고 있기 때문에 편의성을 크게 해치지 않는 범위에서 사업자의 자율성을 보장하고, 기술 중립적 사후적 규제와 거래금액이나 신용도에 따라 보안수준을 차등 적용함으로써 금융거래의 효율성을 높이고 있다. 한편, 국내의 경우 금융 또는 결제 서비스 채널 자체를 보호하는데 초점을 맞추고 온라인 거래에 대해 오프라인 거래 수준의 보안성을 확보하기 위해 사전적 일률적 규제를 적용하였다. 국내 소비자들은 결제 시에 보안 프로그램을 매번 설치해야 했고, 반복적으로 정보를 입력하는 수고

2) 사용자와 컴퓨터 또는 두 컴퓨터간에 활성화된 연결(세션)을 공격하는 기법

<표2> 국내외 금융보안 체계의 특징

| 구 분 | 해외(미국, 영국) | 국 내 |
|---|---|---|
| 보안 규제방식 | 사후 책임(부정사기거래 피해에 대한 무거운 책임부여 ) | 사전 규제 |
| 금융보안의 수행자 | 금융회사가 자율적으로 보안인증체계 (PCI-DSS) 구축 | 당국이 금융보안 직접 지시 |
| 보안수준 차별성 | 거래규모 및 고객의 신용도 등에 따라 필요 보안수준을 차등 적용,  소비자에게 보안수준에 대한 선택권 부여 | 획일적인 보안수준을 요구, 소비자에게 선택권을 부여하지 않음 |
| 보안사고의 책임 | 금융회사 뿐 아니라 전자결제업체, IT기업, 금융소비자에게도 책임 부여 | 금융회사가 선책임, 금융소비자는 판결 후책임 |
| 보안인력 및 기술 | 보안인력이 풍부하고 검증된 FDS,  빅데이 터 분석기술, 다양한 인증기술 등 확보 | 보안인력이 부족하고 FDS, 빅데이터 분석 등 기술 수준 낮음 |

※ 자료 : 동아일보 기사(2015.2.12) 등

를 경험해야 했다. 이 방식은 인증 프로세스가 복잡하고 특정기술에 의존하여 호환성 및 이용편의성이 떨어지며 서비스간 차별성과 기술혁신이 부족한 단점을 가지고 있으나 비교적 낮은 사고발생율과 실시간 처리 등의 장점을 가지고 있다.

최근 정책당국은 IT·금융 융합을 지원함에 있어서 그간의 사전적이고 지나치게 세세한 규율(<표2>참조)에서 벗어나 자율과 책임, 사후관리와 점검을 강화하는 방향으로 보안규제 방식의 전환을 추진하고 있다. 이러한 정책 기조하에서 공인인증서 사용 의무화 폐지(2014.5), PG사 카드정보 저장 허용(2014.7), 보안성 심의제도 폐지 계획발표(2015.1), 3종 Activ-X보안프로그램 의무설치 폐지(2015.3) 등 보안 관련 규제 완화를 추진하고 있다. 보안규제 완화 조치는 관련 다양한 기술의 등장을 촉진하고 소비자의 편의를 향상시키는 효과가 기대되는한편 금융서비스의 안전성을 약화시켜 해킹 등 금융사고 발생 가능성을 높일 것으로 예측된다.

## Ⅳ. 핀테크 서비스의 보안 리스크 대응방안

### 4.1 기본방향

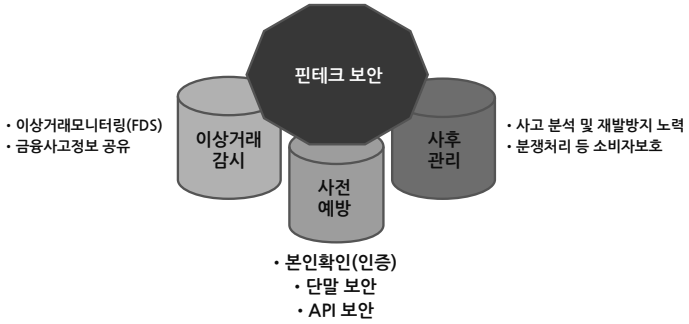
정보보안 관점에서 핀테크는 보안을 방어적 개념에서 사업의 요소로 전진배치하는 과정이며 본인확인, 중요정보 보호 등 보안 요소를 비즈니스 모델  안에 어떻게 재구성해서 안전함과 편리함을 유도해 내느냐가 관건이 될 것이다.

핀테크 보안의 추진방향은 첫째, 금융거래의 신뢰성을 훼손하지 않으면서 이용자의 편의성을 확보할 수 있어야 한다. 이를 위해 사용자단에서 서버단으로 보안 프레임워크를 이동시키는 이상거래탐지시스템(FDS)과 같은 서버단 모니터링 시스템을 강화하고 키보드보안 등 전자금융거래에 사용되어온 보안 S/W를 중기적으로 HTML5와 같은 비 설치형으로 전환을 검토할 필요가 있다. 둘째, 보안기술은 국제 표준을 준수해야 한다. 액티브 엑스와 같은 비표준 기술의 사용을 지양하고 핀테크 서비스는 종국에 금융업무의 온라인 플랫폼화 형태로 발전될 것이므로 국제 표준기술을 적용하여야 한다. 셋째, 비즈니스와 사회적 관점에서 정보보안을 접근해야 한다. 해킹기법이 날로 지능화·고도화되는 상황에서 기술적 시각을 넘어 보안투자 대비 효과, 사회적 영향 등을 고려한 위험 최소화 방안을 고민해야 한다.

### 4.2 보안 프로세스별 대책

핀테크 서비스의 보안리스크 최소화를 위한 대응방안을 예방, 탐지, 대응의 보안프로세스 측면에서  제시하고자 한다

(<그림4> 참조).




<그림4> 보안프로세스별 보안요소

#### 가. 본인확인(인증)

모바일 서비스의 차별성은 사용자 인증 과정의 편리성 여부에서 확인되기 때문에 인증방식은 서비스의 성공 여부에 커다란 영향을 미치는 요소이다(김수형 외 2015) . 핀테크와 사물인터넷 환경은 보안상 취약한 접점이 증가하여 고객이 실수로 악성코드를 받게 될 가능성과 원격접속을 통해 공격을 받을 위험성도 더욱 커지게 된다. 이러한 상황에서 본인 확인을 위한

인증 강화는 해킹사고 예방 측면에서 중요하다. 최근 금융·결제분야에서 FIDO(Fast IDentity Online)가 기존 패스워드 기반 인증을 대체할 수 있는 기술로서 많은 관심을 받고 있다. 이 기술은 사용자가 소지하고 있는 기기가 제공하는 인증수단을 통해 사용자 로컬 인증을 수행하고 사용자 기기는 인증된 사용자를 대신하여 FIDO 표준 기반의 원격 인증을 수행한다. 사용자의 고유특성을 사용자가 소지한 기기에서만 확인하고 이용해 프라이버시 위험없이 안전하고 편리하게 인증할 수 있는 표준화된 플랫폼을 제공하기 때문에 단기적으로는 스마트폰에 탑재된 지문인식 기술을 중심으로 확대 적용될 것으로 보이며, 향후에는 PC기반 금융 서비스에서도 다양한 인증 수단이 결합된 FIDO 기술을 활용할 수 있을 것으로 예상된다.

**나. 단말플랫폼 보안**

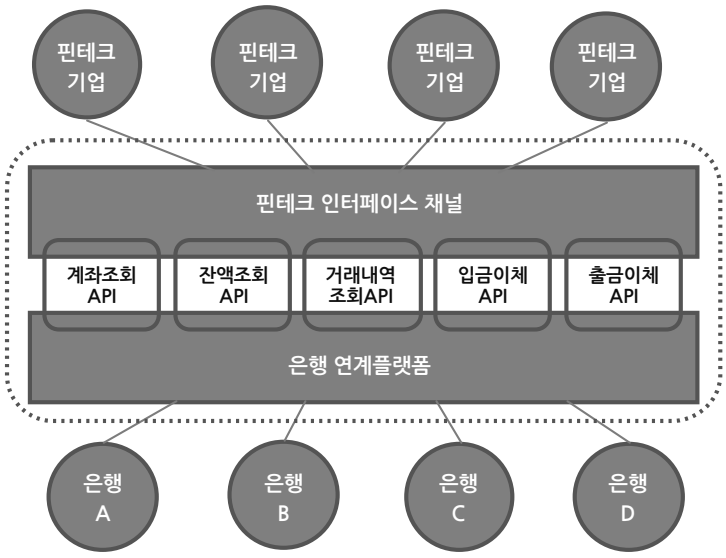
악성코드 공격 위협으로부터 보호가 중요하며 이를 위해 모바일 기기와 서비스 제공자는 PC수준의 보안을 확보할 필요가 있다. 모바일 단말 보안은 지금까지 주로 악성코드 등에 의한 앱의 위·변조방지와 악성 앱 설치 차단이 주요한 대책이었으나 이는 소프트웨어 방식으로 한계를 노출시켜왔다. 스마트폰에 대한 공격이 주로 소프트웨어 취약점을 악용하고 있기 때문에 하드웨어 기반의 신뢰된 실행환경(TEE: Trusted Execution Environments)기술의 적용을 고려해 볼 수 있다. 이 기술은 스마트폰의 AP(Application Processor)를 일반영역과 보안영역으로 논리적으로 분리한 기술이며, 보안영역이 활성화 되면 모든 일반영역의 활동은 홀딩되어 보안영역으로 접근이 불가능하다. 또한 각 영역은 별도의 운영체제가 구동되고 보안영역이 항상 먼저 부팅되어 일반영역으로부터 격리되는 특징을 가진다. 스마트폰에서 입출력되는 화면과 좌표값을 보호할 수 있기 때문에 안전한 모바일 금융거래 환경 구현이라는 목표에 부합되는 기술로 생각된다.

**다. 결제정보 보안**

온라인과 오프라인이 융합되며 사물의 인터넷접속이 기본 전제가 되는 환경이므로 종단간(end-to-end)의 보안 프로세스 구현이 중요해진다. 핀테크 확산으로 통신사, PG사, 플랫폼사, 스마트폰 제조사 등 여러 외부 사업자에게 문호를 열어야 하는 상황에서 안전성에 대한 관리를 하면서 다양한 외부 서비스에 개방을 위한 기술로써 토큰화(Tokenization) 기술이 등장하였다. 날로 강화되는 컴플라이언스와 빅데이터 환경에서의 보안 강화를 위해 결제 데이터를 토큰(Token)으로 치환하여 원본데이터 대신 토큰을 사용하는 토큰화 기술을 적용할 필요가 있다. 사용자가 카드를 등록할 때 마다 카드사에서 생성된 이 토큰(가상카드 번호)이 온라인 결제서비스 또는 오프라인 모바일 지갑 사업자에게 전달되어 사용자의 아이디 등 식별정보에 매핑되어 저장된다. 이후 결제 시 토큰이 카드사에 전달되어 연결되어 있는 실제 카드로 승인이 처리되게 되는 방식이다(성기윤 2015).

**라. API 보안**

API(Application Programming Interface)란 소프트웨어 간에 상호작용 및 데이터 교환이 가능하게 하는 인터페이스이며, 비즈니스 관점에선 내부 자산을 외부에 공개해 새로운 서비스를 개발하고 사업 기회를 찾을 수 있도록 하는 방법으로 널리 활용되고 있다(<그림5>참조). 특히, 핀테크 시대를 맞아 금융인프라 개방을 통한 상생의 핀테크 생태계 조성의 일환으로 핀테크기업 등이 제공하고자 하는 서비스와 연관된 금융회사 시스템  또는 정보에 접근할 수 있도록 하는 통로의 개념으로 부상하고 있다(Open Data Institute and Fingleton Associates 2014). 외부 서비스와 사내 시스템을 연동시키거나 협력사와 협업을 위해 내부와 외부를 연결하는 사례가 많아질 핀테크 환경에서 핀테크API가 해킹 공격의 통로가 될 수 있다는 경고 가 나오고 있다.




<그림5> 핀테크 API

많은 핀테크 기업과 다양한 핀테크 서비스가 API를 활용할 경우 각종 보안사고가 발생할 수 있 으므로 검증된 소프트웨어의 사용을 통해 보안성을 확보 하고 권한 있는 사용자가 편리하게 사용할 수 있도록 해야 할 것이다.

**마. 이상거래 탐지**

사용자단의 보안 절차가 간소화되고 사용자의 PC나 모바일 단말기에 설치되어야 할 모듈들이 줄어들거나 없게 되는 핀테크 서비스 환경에서 기존 보안시스템은 더욱 한계를 갖게 될 것이므로 사용자 구간에 집중된 사실상 단일 계층 보안체계를 다계층 방어로 전환해야 한다. 유출된 개인정보 등을 이용한 인증 후에 발생하는 위협과 악성코드 등에 의한 인증절차를 우회한 부정 거래 시도를 탐지, 차단하는 것이 중요하므로 사용자 정보, 거래정보 등을 분석하여 서버단에서 이상거래를 탐지·차단하는 시스템(Fraud Detection System) 구축 및 고도화가 필요하다(금융보안연구원 2014). 오탐(False positives)에 의한 피해 발생 최소화를 위해 현장과의 커뮤니케이션과 이상거래를 탐지·분석하고 차단하는 과정에서 수반될 수 있는 거래지연 현상을 대비한 업무 약관 등 제도적 보완과 같은 이상거래탐지시스템의 실효성을 높이기 위한 노력이 필요하다. 또한, 유관기관과의 원활한 정보 공유를 위해 필요하다면 현재의 관련 법규(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보의 이용 및 보호에 관한 법률 등)의 개정을 통해 전자금융사고 예방을 위한 일련의 활동에 법적 근거를 부여하는 방안도 검토할 필요가 있다.

**바. 사고대응**

보안사고를 100% 막을 수 있는 보안기술은 존재하지 않으며 특히 핀테크 시대에는 어떤 기술 및 공격이 등장할지 정확히 알 수 없으나 사고 발생 가능성은 높아질 것이다(한국인터넷진흥원 2014). 사고로부터 대응하고 회복하는 스피드가 보안 수준을 결정하게 되므로 기업은 사고가 발생했을 때 전전긍긍할 것이 아니라 그로 인한 피해를 최소화하고, 원인을 정확히 파악해서 기업의 운영을 본 상태로 돌리는 데 전력해야 한다. 침해사고 등에 효과적으로 대응하기 위해 관련 시스템 간 상호 연관성에 대한 충분한 이해와 잘 준비된 침해사고 대응 시나리오 등을 포함하는 비즈니스연속성 대책(BCP : Business Continuity Plan)을 갖추어야 하고, 사고 발생 시 긴급 조치와 사고원인을 분석하여 재발방지 대책 등을 수립하는 상시적 조직이 필요하다. 특히 간편 결제 및 송금 등 핀테크 서비스를 이용하는 금융 소비자 보호와 핀테크 기업의 위험 분산을 위해 전자금융사고 관련 보험 대책, 보상체계 등을 포함한 분쟁조정 방안 마련 역시 중요할 것으로 생각된다.

## V. 결론

모바일, 소셜, 클라우드, 빅데이터 기술은 물론이고,

서서히 현실화되고 있는 IoT(사물인터넷), VR(가상 현실) 등 다양한 IT 신기술과 금융이 결합한 핀테크는 새로운 지평을 여는 다양한 가능성과 함께 우리에게 큰 짐을 안겨줄 수 있다(김형중 2015). 특히, 높은 IT 의존성과 서비스의 혁신성을 중시하는 핀테크의 기본 철학, 채널·서비스·기술 간의 융복합, 거래과정에서 광범위한 데이터의 공유 등으로 인해 금융거래의 신뢰성에 대한 우려를 갖게한다.

핀테크 시대에는 보안이 성장의 인프라이며 금융상품을 선택하는 중요한 기준이 될 것이므로 서비스의 주체, 적용기술 및 보안정책의 변화에 따른 보안리스크를 분석하고 이를 줄이기 위한 노력이 참여자 모두에게 필요하다. 잠재적 보안리스크에 대한 정량화와 단계별 통제 방안을 수립하고, 사용자 인증, 단말 보안, 결제정보 보안, API보안, 이상거래모니터링 등 보안요소를 비즈니스 모델에 맞도록 유연하게 적용하여 서비스의 보안성과 이용자의 편리성을 함께 확보할 수 있어야 한다. 특히 산재되어 있는 개인정보 및 금융정보에 대한 유출 공격, 지능화되는 인증우회·피싱·파밍 공격, 금융·IT 연계 취약성을 노린 공격 등 핀테크 서비스 환경에서 강조되는 보안위협 요인에 대한 철저한 대비가 이루어져야 할 것이다.

마지막으로 금융정책당국, 금융회사, ICT기업 그리고 소비자간의 정보보안에 대한 책임 및 역할에 대한 공유와 명확화를 출발점으로 하여 정보보안 투자 확대를 통해 보안 강화와 소비자 신뢰를 제고하고 나아가 핀테크 서비스 활성화와 참여기업의 수익증대를 달성함으로써 다시 보안투자 확대로 연결되는 금융보안과 핀테크 간의 선순환 체계가 작동되길 기대해 본다.

## 참고문헌


[1] 김남훈(2015a), “Fintech 트렌드와 금융업에 대한 시사점”, 2015 모바일 비즈니스 인사이트 세미나

[2] 김남훈(2015b), “지급결제 및 금융혁신 동향과 금융기관의 대응”, 2015년 한국은행 지급결제컨퍼런스

[3] 김수형 외(2015), “핀테크시대 : 새로운 인증 기술을 요구하다”, 정보과학회지, 제33권, 제5호, 17-22.

[4] 김인석(2015), “핀테크 환경변화에 따른 금융보안 및 금융권의 대응방안”, 월간 금융 Vol.732, 7-13.

[5] 김종현(2015), “금융권 핀테크 전략과 정보보안 방안”, 동아 인포섹 2015-정보보호 콘퍼런스 (2015.2)

[6] 김형중(2015), “핀테크 : 그 새로운 지평”, 정보처리학회지, 제22권, 제5호

[7] 금융결제원(2015), “핀테크에 대한 이해와 대응전략”

[8] 금융보안연구원(2014), “전자지급결제서비스 동향 및 시사점”

[9] 금융보안연구원(2014), “이상금융거래 탐지시스템 가이드 및 소개 자료”

[10] 금융위원회(2015), “IT·금융융합 지원방안”

[11] 동아일보(2015), “금액-신용도 따라 보안수준 차별화… 금융거래 효율성 높여”

[12] 박정국, 김인재(2015), “핀테크 서비스의 보안 취약점과 대응방안”, 정보처리학회지, 제22권, 제5호,36-45

[13] 성기윤(2015), “핀테크 결제의 편리성과 안전성 : 토큰화 관점”, 정보과학회지, 제33권, 제5호, 13-16

[14] 이남희, 정재은(2012), “서비스 혁신에 관한 문헌연구: 성공요인, 프로세스 및 성과를 중심으로”, 지식경영연구, 제13권, 제1호

[15] 조규민(2015), “핀테크와 정보보호”, 스마트금융&핀테크 비즈니스 콘퍼런스(2015.3)

[16] 최대선(2015), “핀테크와 보안”, SCON(Sopt Conference 10th) IT 콘퍼런스(2015.1)

[17] 한국은행(2015), “2014년 지급수단 이용행태 조사결과 및 시사점”, 지급결제조사자료(2015-1)

[18] 한국은행(2014), “국내외 비금융기업의 지급서비스 제공현황 및 정책과제”, 지급결제조사자료(2014-6)

[19] 한국인터넷진흥원(2014), “산업간 융합 관점에서 본 핀테크의 시사점”, INTERNET & SECURITY FOCUS

[20] 허용석, 강민형(2013), 조직 구성원들이 인식하는 자사의 외부 지식 네트워크 구축의 선행요인들이 제품 및 서비스 혁신에 미치는 영향에 관한 실증분석 : 개방형 혁신의 관점을 기반으로”, 지식경영연구, 제14권, 제3호

[21] Accenture(2015), “The Future of Fintech and Banking: Digitally disrupted or re imagined?

[22] Brown, I. W.(2013), “Data Security Considerations for FinTech Companies”, Bloomberg BNA Banking Report, 100 BBR 766.

[23] Deutsche Bank(2014), “Fintech-The digital (r) evolution in the financial sector”

[24] FIDO Alliance(2014), “Specification Overview “, https://fidoalliance.org/specifications/overview/

[25] Open Data Institute and Fingleton Associates(2014), “Data Sharing and Open Data for Banks”

[26] UK Trade & Investment(2014), “Landscaping UK Fintech”, Ernst & Young

[27] Venture Scanner(2015), “Fintech Landscape Update: 1,000 Companies!”

## 저 자 소 개

**박정국(Park, Jeong Kuk)**

한양대학교 경제학과를 졸업하고, 동국대학교에서 석사(정보보호학) 및 박사(경영정보학) 학위를 취득하였다. 공인인증기관(yessign)과 금융ISAC(Information Sharing and Analysis Center) 근무하였으며 금융결제원 연구소에서 수석연구원으로 재직중이다. 주요 관심사로는 금융보안, 정보보호관리체계, 전략적 IT응용 등이다.

**김인재(Kim, Injai)**

동국대학교 경영대학 경영학부 교수로 재직 중이다. 서울대학교 산업공학과 학사, KAIST 경영과학 석사, University of Nebraska-Lincoln 경영정보학 박사학위를 받았다. .LG전자(구 금성사) 중앙연구소 전산실 개발팀장으로 근무하였다. 국내외 주요 저널에 다수의 논문을 발표하였다. 주요 관심분야는 정보기술의 수용과 혁신, 정보보안, 소프트웨어 품질, 빅데이터와 소셜 네트워크 분석, 정보기술을 매체로 한 커뮤니케이션, 그리고 유헬스니스 등이다.