핀테크 서비스의 보안 취약점과 대응방안

Countermeasure and Security Vulnerability of Fintech Services

박정국 (금융결제원), 김인재 (동국대학교 경영학부)

목차

요약

금융과 IT의 융합을 의미하는 핀테크(Fintech) 열풍이 전세계적으로 뜨겁게 불고 있다. 핀테크를 통해 신기술들이 금융 산업 전반에 융합되면서 새로운 형태의 금융서비스가 등장하고 기존의 금융 시스템들이 가져왔던 문제점들을 개선하는데 기여할 것으로 보인다. 하지만 핀테크 산업 활성화를 위한 지속적 규제 완화와 이용자 편의성을 위한 각종 절차의 간소화 그리고 채널·서비스·기술간의 융복합이 일어나는 환경에서 제공되는 핀테크 서비스의 안전성에 대해 우려가 있다. 핀테크 시대에 정보보안은 성장의 인프라이며 금융상품을 선택하는 중요한 기준이 될 것이므로 보안리스크의 정량화와 단계별 통제 방안을 수립하고 사용자 인증, 결제정보 보안, API(Application Programming Interface) 보안 등 필요한 보안요소를 사업모델에 맞게 적용함으로써 편리성과 보안성을 함께 확보할 수 있어야 한다. 본 연구에서는 정보보안 관점에서 핀테크의 서비스의 특징과 보안 취약점을 분석하고 관련 위험을 줄이기 위한 대응방안을 모색해 보았다.

키워드: 핀테크, 보안 취약점, 이용 편의성, 거래 신뢰성

1. 연구배경 및 현황

1.1 연구배경

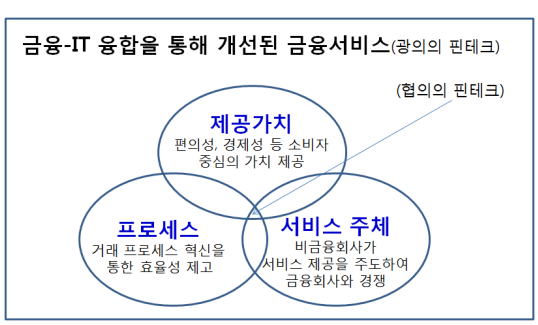
전 세계적으로 금융과 IT의 융합을 의미하는 핀테크(Fintech) 열풍이 뜨겁다. 국내에서도 핀테크 산업 활성화를 위해 핀테크 산업의 사전규제 최소화, 오프라인 위주의 금융제도 개편, 전자금융업 진입장벽 완화, 창업기업을 위한 테스트베드(Test-bed) 제공 등 지원을 펼치고 있다(금융위원회, 2015).

일련의 규제 완화가 정보보호에 부정적 영향을 미칠 수 있다는 시선과 소비자 편의성을 중시하고 채널·서비스·기술 간에 융복합이 일어나

는 환경에서 제공되는 핀테크 서비스는 상대적으로 보안성이 취약하기 때문에 이를 겨냥한 공격이나 사고 발생 가능성에 대한 우려가 있다. 핀테크 산업 활성화의 핵심은 사용자 인증, 고객정보 보호 등 보안적 요소를 비즈니스 모델 안에 어떻게 재구성해서 안전함과 편리함을 유도해 내느냐가 관건이 될 것이다. 이에 본 연구에서는 정보보안 관점에서 핀테크 서비스의 특징과 잠재적 보안 취약점을 분석하고 이와 관련한 위험을 줄이기 위한 대응방안을 제시하고자 한다.

1.2 핀테크 현황

금융(Financial)과 기술(Technology)의 합성어인 핀테크(Fintech)는 IT기술을 이용하여 기존 금융기법과 차별화된 새로운 형태의 금융서비스 또는 금융 시스템과 서비스를 효율적으로 만드는 기술로 정의할 수 있으며(Ernst & Young, 2014), (그림 1)에서 보듯이 서비스 주체, 제공가치, 프로세스 맥락에서 의미를 찾을 수 있다(금융결제원, 2015). 간편한 결제, 송금서비스를 앞세운 페이팔, 알리페이, 애플페이 등이 글로벌 시장에서 성공을 거두었을 뿐만 아니라 점포 없이 운영되는 인터넷전문은행, 온라인 매체를 통해 자금을 모아 투자하는 크라우드펀딩(Crowd funding)등 다양한 금융분야에서 핀테크 서비스



(그림 1) 핀테크 개념

가 출현하고 있다.

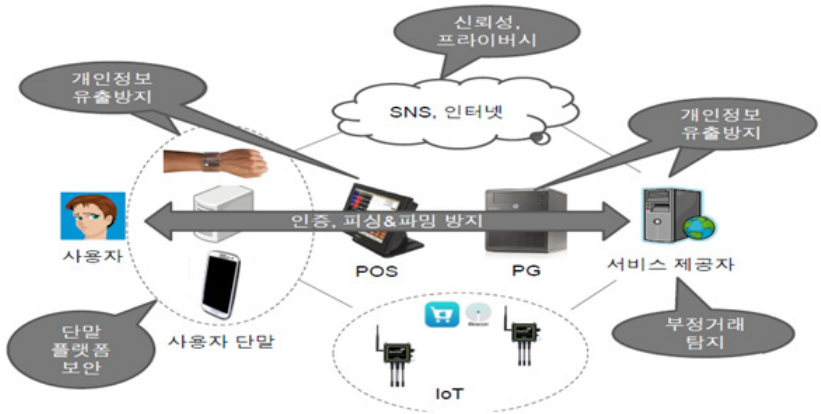
국내에서도 글로벌 전자결제시장의 성장에 맞춰 국내 인터넷 쇼핑몰의 불편한 결제시스템을 해외처럼 신속하고 간편하게 개선해야 한다는 요구가 높아지면서 핀테크 산업에 대한 관심도 높아지고 있는 가운데, 저성장·저금리로 날로 수익성이 악성되고 있는 금융회사는 이를 극복하기 위한 방안의 하나로 신규 핀테크 사업 모델 발굴에 나서고 있다. 또한, 테크기업과 창업기업도 핀테크를 새로운 먹거리 창출을 위한 새로운 시장으로 인식하고 다양한 서비스를 개발하고 있다.

2. 핀테크 서비스의 보안 취약점 및 대응방안

2.1 보안 취약점

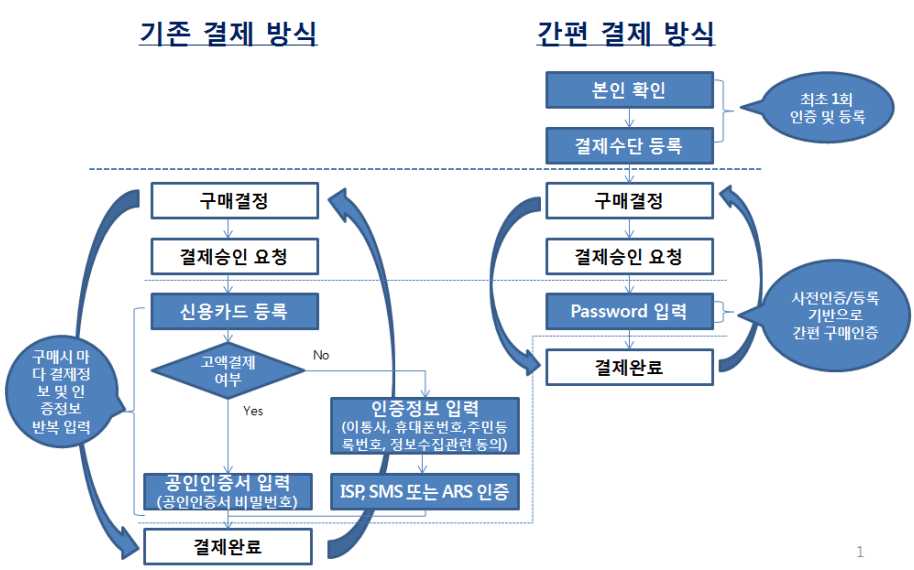
한국은행 조사(2015)에 따르면 모바일결제를 이용하지 않는 주된 이유가 개인정보 유출 우려(78.3%)와 안전장치에 대한 불신(75.6%)인 것으로 나타났다. 더욱이 서비스의 보안성 보다는 사용자의 편의성이 중시되는 핀테크를 통해 금융서비스에 대한 새로운 접근 채널이 확대됨에 따라 (그림 2)에서 보듯이 개인정보 유출방지, 거래 신뢰성 확보, 부정거래 탐지 등의 보안이슈와 보안 사고에 대한 우려는 더욱 커질 것으로 예상된다(최대선, 2015; 김인석, 2015).

핀테크 서비스는 다음과 같은 몇가지 특징을 가지고 있으며 이러한 특징은 동시에 잠재적 보안 취약점이 된다. 첫째, 결제단계, 입력되는 정보 그리고 인증방식 등의 간소화를 추구한다. 과거에는 이용 과정의 불편보다는 안전성을 중시해 카드정보, 공인인증서, 일회용비밀번호, 각종 보안프로그램을 사용하고 거래 시 마다 결제정

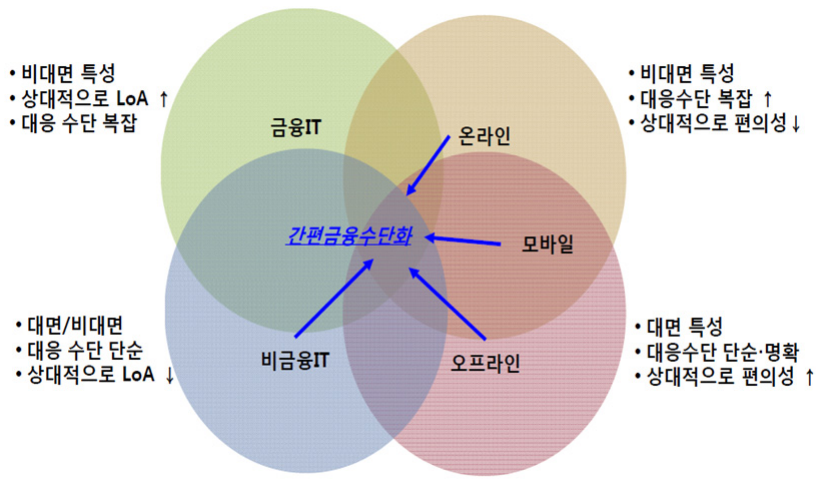


(그림 2) 핀테크 보안이슈

보 및 인증정보를 입력하도록 하여 사고를 예방해 왔다(조규민, 2015). (그림 3)에서 보듯이 결제 편의를 위해 온라인 상거래 구매자가 신용카드 정보(카드번호, 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). 지문, 정맥을 이용하는 생체인증, IC카드 등을 이용하는 소지매체를 활용한 신규 인증기법이 활성화되고 있으나 개방형 모바일 플랫폼 환경에서 사용되는



(그림 3) 결제 처리절차 비교



(그림 4) 채널, 서비스, 기술간 융·복합

신규 인증기법의 취약점을 이용한 ID 도용, 추가 인증 우회, 피싱 및 파밍 공격 등 위협이 존재한다

둘째, 채널·서비스·기술 간의 다양한 융복합 현상이 발생한다. 이는 기술적으로 대응수단을 복잡하게 할 뿐 아니라 현실에서 금융 서비스와 온라인 서비스(SNS, 포털 등)간에 결합이 발생될 때 전체적 보안수준(LoA)이 높은 쪽에서 낮은 쪽으로 내려가는 현상 발생에 대한 우려를 낳고 있다. (그림 4)에서 보듯이 핀테크를 통해 다양한 성격의 비금융회사가 금융업에 진출하여 소비자의 편익을 증가시킬 것으로 예상되지만, 금융IT와 비 금융IT, 온라인과 오프라인, 모바일 기술 간의 융복합이 일어나기 때문에 접점을 증가시키고 새로운 취약점을 발생시키는 원인을 제공할 수 있다(금융보안연구원, 2015). 다양한 매체와 메쉬(Mesh) 구조의 복잡한 네트워크 연결 구조를 갖게 됨으로 한 부분이 뚫리면 금융시스템 전체로 확산될 위험성이 있으며, 특히 인터넷 기반의 네트워크 연결이 증가함으로써 서비스 거부공격(DOS), 세션 하이재킹(Session hijacking)[1] 등의 보안위협에 노출될 가능성이 높다.

셋째, 거래과정에서 데이터 공유가 광범위하게 이루어진다. 다양한 핀테크 서비스를 제공하기 위해 고객으로부터 관련 정보의 수집이 확대되고 사업자간의 정보 공유도 증가할 것이므로 모바일기기 등에 저장된 고객정보 유출, 비금융회사에 저장된 정보의 유출, 빅데이터 분석과 관련한 프라이버시 침해 사고 가능성도 역시 증가할 것이다. 최근 들어서 대량 정보유출 사태가 꾸준히 발생하고 있으며 유출된 정보의 내용은 단순 개인정보에서 부터 금융정보까지 다양하며 이러한 정보의 유출은 일차적 피해 뿐만 아니라 유출된 정보를 이용한 카드 부정사용 가능성도 있어 피해는 확산될 것으로 예상된다. 특히, 비금융회사들은 민감한 정보를 처리하고 보호함에 있어 금융회사와 같은 경험을 가지고 있지 못하는데 이 문제는 금융정보, 표적화된 대규모 공격을 받을 수 있는 많은 양의 개인정보 그리고 상용 데이터를 가지고 있는 모바일 기기를 이용한

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

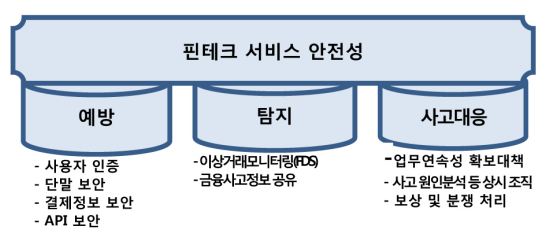
거래의 증가와 금융과 기술 간의 융합 현상으로 인해 증폭될 수 있다고 했다(IAN C. Wildgoose Brown, 2013).

넷째, 금융IT 규제 패러다임이 전환된다. 핀테크 활성화를 지원하기 위해 정보보호 정책이 규제중심에서 원칙중심으로, 사전규제에서 사후관리 및 금융회사 책임을 강화하는 추세로 전환하는 등 정보보호 규제 패러다임의 변화가 일어나고 있다. 이러한 변화에 따라 정책당국은 공인인증서 사용 의무화 폐지(2014.5), PG사 카드정보 저장 허용(2014.7), 보안프로그램 설치의무 폐지(2015.2), 보안성 심의제도 폐지(2015.6) 등 관련 규제를 완화하였다. 이러한 핀테크 산업 활성화를 위한 규제완화가 금융사고 발생 가능성을 높여 IT보안이나 정보보호에 부정적인 영향을 미칠 수 있다는 우려가 있다. 핀테크 서비스는 기본적으로 개인정보와 금융정보 등을 활용하고 있으므로 해킹 등 금융사고 발생시 개인의 재산 피해뿐만 아니라 사회적,경제적으로 혼란을 야기시킬 수 있기 때문이다.

다섯째, 사용자단(User-end) 접속기기의 활용범위가 점차 확대되고 있다. 금융서비스와 IT기술간 결합정도가 심화됨에 따라 시스템(Back-end) 중심에서 네트워크(Middle-end)를 거쳐 사용자단(User-end) 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. 온라인과 오프라인이 융합되며 사물의 인터넷접속이 기본 전제가 되는 환경이므로 종단간(end-to-end) 정보보안 프로세스를 구현해야 한다. 악성코드 공격 위협으로부터 보호가 중요하며 이를 위해 모바일 기기와 서비스 제공자는 PC수준의 보안을 확보할 필요가 있다.

2.2 대응방안

핀테크 보안은 정보보안의 요소를 비즈니스 모델 안에 어떻게 재구성해서 안전함과 편리함을 유도해 내느냐가 관건이며, (그림 5)에서 보듯이 핀테크 서비스의 안전성 확보를 위한 대응방안을 예방, 탐지, 사고대응의 보안프로세스 측면에서 제시하고자 한다.



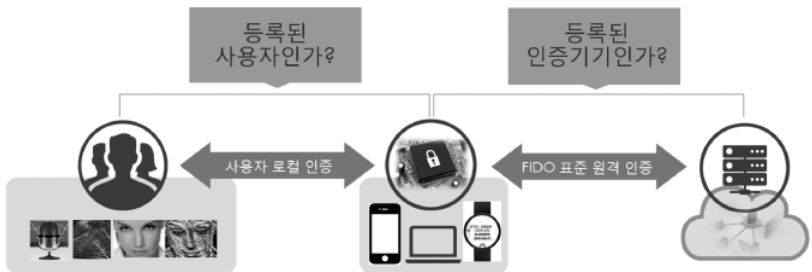
(그림 5) 보안프로세스과 핀테크 보안요소

2.2.1 사용자 인증

모바일 기반 핀테크 서비스의 차별성은 사용자 인증 과정의 편리성 여부에서 확인 되기 때문에 인증방식은 서비스의 성공 여부에 커다란 영향을 미치는 요소이다(김수형 외 2015). 핀테크와 IoT 서비스 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.

FIDO(Fast IDentity Online) 얼라이언스(Alliance)[2]

2) 온라인 환경에서 생체인식기술 등을 활용한 인증방식에 대한 기술표준을 정하기 위해 2012년 7월 설립된 협의회 이며, 삼성전자, 블랙베리, 크루셜텍, 구글, 레노보, 마스터카드, 마이크로소프트, 페이팔,

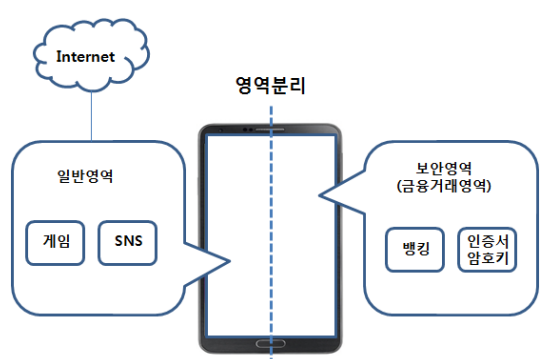


(그림 6) FIDO 인증 기술의 개념

는 기존 패스워드 기반 인증을 대체할 수 있는 기술 표준(FIDO 1.0 2014)을 발표하였으며 이는 최근 금융·결제분야에서 많은 관심을 받고 있다. (그림 6)에서 보듯이 사용자가 소지하고 있는 기기가 제공하는 인증수단을 통해 사용자 로컬 인증을 수행하고 사용자 기기는 인증된 사용자를 대신하여 FIDO 표준 기반의 원격 인증을 수행한다. 이 기술은 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 예상되며, 향후에는 PC기반 금융 서비스에서도 다양한 인증 수단이 결합된 FIDO 기술을 활용할 수 있을 것으로 예상된다.

2.2.2 단말 보안

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. (그림 7)에서 보듯이 스마트폰의 AP(Application Processor)를 일반영역과 보안영역으로 논리적으로 분리한 기술이며, 보안영역이 활성화 되면 모든 일반영역의 활동은 홀딩되어 보안영역으로 접근이 불가능하다. 또한 각 영역은 별도의 OS가 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.

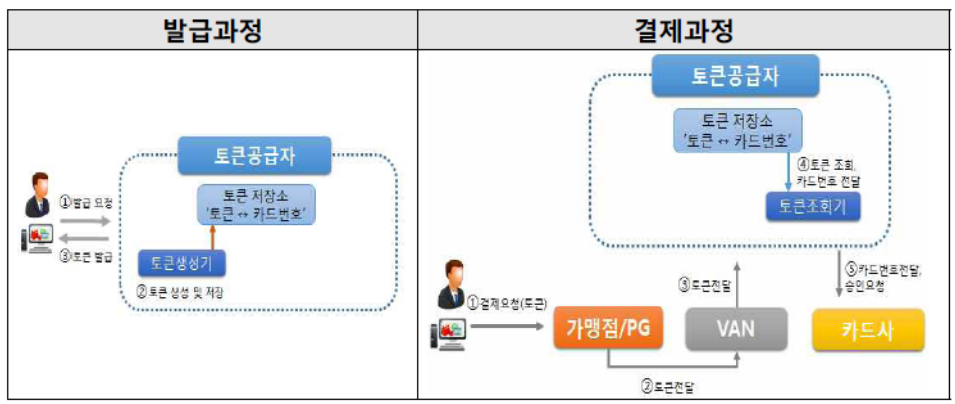


(그림 7) 신뢰된 실행환경(Trusted Execution Environment)

2.2.3 결제정보 보안

핀테크 확산으로 통신사, PG사, 플랫폼사, 스

LG전자 등이 회원사로 가입.

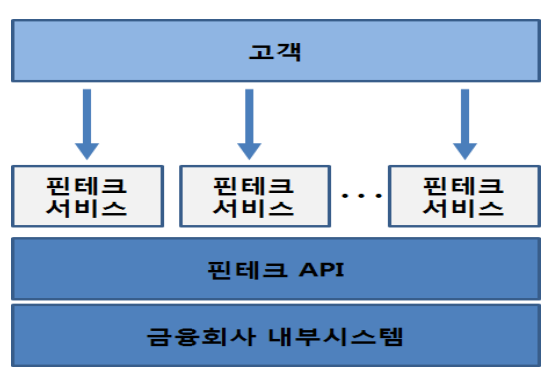


(그림 8) 토큰의 개념

마트폰 제조사 등 여러 외부 사업자에게 개방해야 하는 상황의 대두와 함께 결제사고에 대한 우려도 동시에 커짐에 따라 단순히 카드복제를 어렵게 하는 것에서 벗어나 카드정보처리 전 구간에서 유출을 방지하기 위한 토큰화(Tokenization) 기술이 등장하였다. (그림 8)에서 보듯이 결제토큰시스템은 이용자, 토큰공급자, 가맹점, VAN, 서비스공급자 등으로 구성되고 절차는 등록, 발급, 결제로 구분할 수 있다. 결제분야에 토큰 서비스가 성공적으로 안착되면, 향후 금융IT는 물론 IT 전분야로 확산될 것으로 보인다. 다만 토큰화 기술은 고정형태의 토큰카드번호도 노출 시 일반카드번호의 노출과 유사한 위협수준을 가지며, 특히 이를 검증하는 토큰검증값도 함께 유출되면 부정거래로 악용될 수 있는바 토큰검증값의 유노출 위협수준이 최소화되도록, 검증값 생성환경에 대한 보호 및 토큰 자체의 유효시간을 최소화 등 부정거래 사용을 방지하기 위해 노력이 지속되어야 할 것이다(금융보안원 2015).

2.2.4 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. 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 (그림 9)의 핀테크API가 해킹 공격의 통로가 될



(그림 9) 핀테크 API 개념

수 있다는 경고가 나오고 있다. 많은 핀테크 기업과 다양한 핀테크 서비스가 API를 활용할 경우 각종 보안사고가 발생할 수 있으므로 검증된 소프트웨어의 사용을 통해 보안성을 확보하고 권한 있는 사용자가 편리하게 사용할 수 있도록 해야 할 것이다.

2.2.5 이상거래 탐지

사용자단의 보안 절차가 간소화되고 사용자의 PC나 모바일 단말기에 설치되어야 할 보안 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 이상거래 탐지시스템의 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.

2.2.6 사고대응

보안사고를 100% 막을 수 있는 보안기술은 존재하지 않으며 특히 핀테크 시대에는 해킹 등 금융사고 위험이 증가할 것으로 예상됨에 따라 이러한 사고로부터 대응하고 회복하는 스피드가 핀테크 기업의 보안 수준을 결정하게 될 것이다(한국인터넷진흥원, 2014). 기업은 사고가 발생했을 때 전전긍긍할 것이 아니라 그로 인한 피해를 최소화하고, 원인을 정확히 파악해서 기업의 운영을 본 상태로 돌리는 데 전력을 다해야 하는데 이를 위해 사고 발생 시 긴급 조치와 사고원인을 분석하여 재발방지 대책을 수립하는 상시 조직, 평소 관련 시스템 간 상호 연관성에 대한 충분한 숙지와 잘 준비된 침해사고 대응 시나리오 등을 포함하는 비즈니스연속성 계획(BCP : Business Continuity Plan)을 갖추는 것이 중요하다. 또한 간편 결제 및 송금 등 핀테크 서비스를 이용하는 금융 소비자 보호와 핀테크 기업의 위험 분산을 위해 고객 피해 보상액 증액 등 사고 관련 보험 강화, 보상체계 등을 포함한 분쟁조정 방안 마련 역시 중요할 것으로 생각된다.

3. 금융보안 특징 및 향후 방안

금융 선진국에서는 <표 1>에서 보듯이 소비자가 금융 또는 결제 서비스 채널에 편리하게 접근하고 이용할 수 있는 방법들을 주로 고민해 왔다. 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 지금까지 금융 또는 결제 서비스 채널 자체를 보호하는데 초점을 맞추고 온라인 거래에 대해 오프라인 거래 수준의 보안성

〈표 1〉 국내외 금융보안 체계의 특징

구 분	해외(미국, 영국)	국 내
보안 규제방식	사후책임(부정사기거래 피해에 대한 무거운 책임 부여)	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	전자결제업체, IT기업, 금융소비자에게도 책임 부여	금융당국 또는 금융회사에 집중
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

을 확보하기 위해 사전적 일률적 규제를 적용하였다. 국내 소비자들은 결제 시에 보안 프로그램을 매번 설치해야 했고, 반복적인 정보들을 입력하는 수고를 경험해야 했다. 이 방식은 비교적 낮은 사고발생율과 실시간 처리 등의 장점을 가지고 있으나 인증 프로세스가 복잡하고 특정기술에 의존하여 호환성 및 이용편의성이 떨어지며 서비스간 차별성과 기술혁신이 부족한 단점을 가지고 있다.

핀테크 시대를 맞아 정보보안은 성장의 인프라이며 금융상품을 선택하는 중요한 기준이 될 것이므로 시작부터 보안 원칙을 세워 실행해가야 한다. 그간의 타율 보안체계하에서 관련 법규정 준수라는 소극적 차원을 벗어나 자율보안이라는 변화된 정책에 맞추어 금융회사 및 핀테크 기업은 보안리스크의 정량화와 단계별 통제 방안을 수립하고 필요한 보안 요소를 사업모델에 맞게 적용함으로써 보안성과 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 한다.

본 연구를 통해 전 세계적으로 열풍을 일으키고 있는 핀테크의 의미를 살펴보고 핀테크 서비스의 주요 특징과 그에 따른 잠재적 보안 취약점을 연구하였다. 또한 핀테크 서비스의 안전성을 확보하기 위해 대응방안을 제시하였다. 이제 우리나라 핀테크 서비스가 발걸음을 내디는 단계이므로 향후 전개되는 나타날 구체적 양상은 불분명한 하다고 할 수 있다. 본 연구 역시 구체적 사건이나 현상에 대한 실증적 분석 없이 보안 취약점과 대응방안을 제시하였다 점에서 한계를 가지고 있다. 향후 연구에서는 구체적 사례에 대한 분석을 바탕으로 대응방안을 연구하고 제시함으로써 연구결과의 현장 활용도를 높일 수 있을 것으로 기대된다.

참 고 문 헌

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

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

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

[4] 금융결제원(2015), “핀테크 이해와 대응전략”
[5] 금융보안원(2015), “결제토큰 기술현황 및 적용 사례 분석”
[6] 금융보안연구원(2014), “이상금융거래 탐지시스템 가이드 및 소개 자료”
[7] 금융위원회(2015), “IT · 금융융합 지원방안”
[8] 동아일보(2015), “금액-신용도 따라 보안수준 차별화… 금융거래 효율성 높여”
[9] 조규민(2015), “핀테크와 정보보호”, 스마트금융&핀테크 비즈니스 콘퍼런스
[10] 최대선(2015), “핀테크와 보안”, SCON(Sopt Conference 10th) IT 콘퍼런스
[11] 한국은행(2015), “2014년 지급수단 이용행태 조사결과 및 시사점”, 지급결제조사자료 2015-1
[12] 한국은행(2014),“국내외 비금융기업의 지급서비스 제공현황 및 정책과제”, 지급결제조사자료 2014-6
[13] 한국인터넷진흥원(2014), “산업간 융합 관점에서 본 핀테크의 시사점”, INTERNET & SECURITY FOCUS
[14] Accenture(2015), “The Future of Fintech and Banking: Digitally disrupted or re imagined?
[15] Deutsche Bank(2014), “Fintech-The digital (r)evolution in the financial sector”
[16] FIDO Alliance(2014), “Specication Overview”, https://fidoalliance.org/specifications/overview/
[17] IAN C. Wildgoose Brown(2013), “Data Security Considerations for FinTech Companies”, BNA’s Banking Report
[18] Jonathan Cedarbaum, Robert Finkel, and Heather Zachary(2013),“CyberSecurity and Data Privacy”, Wilmerhale, FinTech Webinar Series
[19] Open Data Institute and Fingleton Associates(2014), “Data Sharing and Open Data for Banks”
[20] UK Trade & Investment(2014), “Landscaping UK Fintech”, Ernst & Young

저 자 약 력

박 정 국

이메일: arspark@kftc.co.kr

- 1991년 한양대학교 경제학 (학사)
- 2003년 동국대학교 정보보호학 (석사)
- 2015년 동국대학교 경영정보학 (박사)
- 2002년~2008년 금융ISAC/팀장
- 2009년~2011년 공인인증기관(yessign)/팀장
- 2014년~현재 금융결제원 연구소 수석연구역
- 관심분야 : 금융보안, 정보보호관리체계, 전략적 IT응용, 핀테크

김 인 재

이메일: ijkim@dongguk.edu

- 1983년 서울대학교 산업공학 (학사)
- 1985년 KAIST 경영과학 (석사)
- 1996년 The University of Nebraska-Lincoln 경영정보학(박사)
- 1985년~1991년 금성사(LG전자) 중앙연구소 전산실 개발팀장
- 1997년~1998년 한남대학교 경영대학 조교수
- 1998년~현재 동국대학교 경영대학 경영학부 교수
- 관심분야 : 기술수용, 빅 데이터, 소셜 네트워크 분석, IT커뮤니케이션, 유 웰니스, IT전략