핀테크(Fintech)가 정보보호산업에 미치는 영향에 대한 고찰

장상수*

금융과 ICT 기술이 융합된 핀테크(Fintech) 시대에 금융서비스 혁신과 함께 보안 패러다임이 새로운 변화에 직면하고 있다. ICT 기술 발전과 함께 글로벌 핀테크 시장은 빠른 성장을 지속하고 있으며 IT 강국이라 자부하던 우리나라도 최근에야 모바일 지급결제 서비스 중심으로 핀테크 열풍이 거세게 불고 있다. 그러나 핀테크에 대한 관심과 기대감이 크게 증가하고 있으나, 본질적인 카드사 정보유출 사고 및 해킹 등으로 ICT 기술을 활용한 금융서비스의 안전성 확보에 있어서는 아직 우려의 목소리가 높다. 핀테크 산업의 발전과 진화는 정보보호와 동반 성장하지 않고는 불가능하다. 규제 완화와 보안 강화의 최적의 룰을 만들어야 한다. 핀테크 기업들의 불안전한 서비스로 대형 보안사고가 발생할 경우 핀테크 산업 발전에 악영향 뿐만 아니라, 금융서비스의 근간인 신뢰가 무너지고 만다. 핀테크에서의 보안은 금융서비스와 기업의 생존을 결정하는 핵심 가치이다. 이에 따라 본고에서는 핀테크의 핵심 성공 요인인 핀테크 보안과 핀테크가 국내 정보보호 산업에 미치는 영향을 살펴보고자 한다.

* 한국인터넷진흥원 정책연구단 미래전략TF 수석연구위원(정보보호 박사), (ssjang@kisa.or.kr)

Ⅰ. 서론

최근 전세계적으로 클라우드, 사물인터넷, 빅데이터 시대가 꽃피우기도 전에 핀테크(Fintech)[1]라는 또 다른 새로운 패러다임이 IT · 금융 산업을 강타하고 있다. 국내에서도 반응이 신속하고도 뜨겁다. 이러한 글로벌 IT · 금융 융합 트랜드는 ICT 기술을 통해 금융시장에 파괴적 혁신과 부가 가치를 창출하며 급격하게 성장하고 있다. 금융서비스가 오프라인 중심에서 온라인 · 모바일 기반으로 확대되고 애플 · 구글 · 페이팔 등 글로벌 ICT 사업자가 금융관련 인 · 허가를 획득하며, ICT 기술을 활용한 금융서비스 제공 범위를 지속 확대하고 있다. 특히, 중국 등 신흥국의 경우 비교적 낮은 금융 발전도, 부족한 지급결제 인프라를 대신하여 ICT 회사의 금융서비스 제공이 활발하게 이루어지고 있다. 핀테크가 향후 5년이내에 글로벌 경제와 금융시장의 판도를 바꾸어 놓을 혁신적인 트랜드로 주목을 받을 것이다.

그렇게 하기 위해서는 금융회사는 과거의 보수적 관행에서 벗어나 금융서비스를 혁신하여 금융 소비자들에게 편리하고 안전한 핵심 가치를 제공해야 한다. 핀테크의 핵심은 사용자들이 좀 더 편리하게 금융 서비스에 접근하여 안전하게 결제하고 송금하고 거래하는 서비스를 원한다. 다양한 인증방법, 보안기술, FDS(Fraud Detection System),[2] 빅 데이터(big data)[3] 분석능력 등 기술 발전을 발판으로 과거에 없던 새로운 방법으로 고객 편의성을 증진시키고 가치를 만드는 다양한 서비스를 제공해야 한다. 그러나 편리하고 안전한 금융 서비스를 제공해야하는 입장에서는 그만큼 더 많은 ICT 기술들이 접목되면서 해킹 등 보안위협의 지속적인 증가로 더 많은 어려움에 직면하게 됐다.

특히 우리나라는 2013년 카드 3사 개인정보유출사고, POS시스템 해킹 등 전자적 침해사고 등으로 ICT 기술을 활용한 금융서비스의 안전성에 대한 우려의 목소리가 높다. 금융 거래는 편리함, 간편함, 간소화도 중요하지만 보안이 핵심이다. 고객의 신뢰를 잃게 되면 금융 산

1 핀테크(Fintech)는 금융을 뜻하는 '파이낸셜(Financial)'과 '기술(Technique)'의 합성어다. IT 기술 기반 금융서비스 또는 혁신적 비 금융기업이 신기술을 활용하여 금융서비스를 직접 제공하는 현상을 지칭(금융위원회)

2 FDS(Fraud Detection System) : 전자금융거래 접속정보, 거래내역 등을 종합적으로 분석하여 이상금융거래를 탐지 및 차단하는 시스템으로, 간편결제 활성화, 전자금융사기 등을 예방함으로써 금융소비자 보호 및 금융회사 리스크 관리 등을 목적으로 구축 운영(금융위원회)

3 빅 데이터(big data)란 기존 데이터베이스 관리도구로 데이터를 수집, 저장, 관리, 분석할 수 있는 역량을 넘어서는 대량의 정형 또는 비정형 데이터 집합 및 이러한 데이터로부터 가치를 추출하고 결과를 분석하는 기술을 의미한다(위키백과).

업과 핀테크의 존립자체를 위협하기 때문이다. 핀테크 산업의 발전과 진화는 정보보호와 동반 성장하지 않고는 불가능하다. 정보보호 산업이 주도하는 핀테크 산업[4]이 되야 한다는 것이다. 핀테크가 금융서비스에 단순한 ICT 기술 도입에 그치는 것이 아니라 새로운 부가가치를 창출하고 금융산업의 경쟁력 제고로 이어지기 위해서는 핀테크에 대한 국가적 보안체계를 갖추는 일도 중요해졌다. 핀테크 산업 활성화와 함께 불편하고 위험한 상태를 유지할 것인가 아니면 편리하고 안전한 금융혁신을 할 것인가 선택을 할 시점이다.

핀테크 관련 규제 완화 이슈와는 별개의 문제로 원칙을 무시한 핀테크 기업들의 불안전한 서비스로 대형 보안사고가 발생할 경우 핀테크 산업 자체가 무의미 하게 되고 만다. 이에 따라 본고에서는 핀테크의 핵심 성공 요인인 정보보호 이슈와 선진 핀테크 기업들의 정보보호 전략, 핀테크가 국내 정보보호산업에 미치는 영향을 살펴보고자 한다.

Ⅱ. 국내외 핀테크 산업 현황

1. 핀테크 산업 분류

핀테크는 전통적인 금융권 기업이 제공하는 서비스에서 IT 서비스를 제공하는 비 금융권 기업이 금융서비스를 제공하는 시대로 바뀌고 있다. 전통적인 금융 기업이 아닌 ICT 기업, 플랫폼 기업, 보안업체 등이 금융서비스 진출 및 확장이 지금 유행하고 있는 핀테크의 모습이라고 할 수 있다. 핀테크에 대한 산업 분류는 아직까지는 핀테크를 해석하는 관점이나 이해당사자의 입장에 따라 다양한 정의나 분류를 하고 있다. 아직 핀테크 기업에 대한 개념이 명확하게 정의되지 않았기 때문에 이에 대한 추가적인 논의가 필요하나 본고에서는 온라인 중심의 혁신적 금융서비스와 이를 뒷받침하고 있는 ICT 인프라와 기술들로 크게 구분하고 이에 따른 각사의 핀테크 산업을 분류하면 〈표 1〉과 같다.

4 핀테크 산업은 ICT기술을 기반으로 금융서비스를 제공하는 것으로 디지털 채널을 통한 결제·송금·자산관리·투자, 정보보호 등 금융과 ICT가 융합된 산업을 의미한다.

〈표 1〉 각사의 핀테크 산업 분류 예시

구분	금융위원회	여신금융 연구소	Accenture	신한금융 투자	UK Trade & Investment	israelfintech.com
금융 서비스	결제	결제	지급결제	결제	지급결제	Mobile Payments
	인터넷 전문은행	자산관리	자산관리	자산관리		
	전자지급수단	송금	송금	송금		Transaction
	크라우드 펀딩	투자	대출중개	대출	플랫폼	Trading
ICT 기술	보안 및 빅 데이터 (FDS, PCI-DSS, ISMS, Risk Management)	보안 및 데이터 분석		인터넷 전문은행	금융 S/W	Cyber Security, Risk Management, Management Tools, File Management
					금융데이터 분석	Cyber Security, Risk Management, Management Tools, File Management

※ 출처 : 각사 발표자료 재구성

또한 핀테크 관련 사업은 금융서비스 유형, IT · 금융 융합, ICT 기술 발전에 따라 다양한 산업이 나올 수 있으나 〈표 1〉의 내용을 분석하여 재분류하면 〈표 2〉와 같이 송금, 결제, 자산 관리, 투자, 보안 및 데이터분석 서비스 등으로 구분할 수 있다.

〈표 2〉 핀테크 산업 분류

구분		종류	특징
금융 서비스	송금	모바일 및 이메일 송금	• 온라인으로 거래 가능한 가상화폐 • 이메일과 모바일을 통해서 개인과 기업간 송금
	결제	전자결제서비스	• 상품 및 서비스 결제 편의성 향상 • 가상계좌, 신용카드, 실물계좌로 결제가능
	자산관리	온라인 펀드, 인터넷은행 · 보험 · 증권	• 온라인으로 다양한 펀드를 살 수 있는 슈퍼마켓의 역할 • 인터넷은행, 온라인 전용으로 여수신 기능을 제공 • 인터넷만을 통해 가입하는 보험 • 온라인 전용으로 주식, 채권, 선물 투자 플랫폼 제공
	투자	금융투자플랫폼 (소셜트레이딩, 크라우드 펀딩)	• 대출, 창업자금 지원 등 투자 관련 금융을 서비스하는 온라인 플랫폼 • 스마트폰 등을 이용하여 투자 정보교류를 통한 가치판단 및 투자활동에 영향 • 개인 간 자금조달을 중개해 주는 서비스 제공
ICT 기술	보안 및 데이터 분석	정보보안	• 새로운 금융서비스를 보다 편리하게 사용하기 위해서는 보다 고도화된 금융보안기술이 필요
		금융 빅 데이터분석 및 금융 S/W	• 빅 데이터 분석으로 소비패턴의 인식을 통한 소비활동 증진 • 대규모 데이터를 활용한 보다 정교한 대출금리 산정

※ 출처 : 여신금융연구소, "핀테크의 가치창출 요건 및 시사점", 2015.1, 재구성

미국 벤처캐피탈 전문조사기관인 CB Insights 자료에 따르면 2008년 투자의 70%가 지급결제 영역에 집중되었던 반면 2013년에는 금융소프트웨어와 금융데이터분석 부문에 투자가 58%로 집중되며 보안 및 데이터 분석 영역으로 글로벌 핀테크 산업의 발전이 진행되고 있다.

2. 해외 핀테크 추진 현황

1) 주요국의 핀테크 추진 현황

미국, 영국 등 주요국은 핀테크 추진에 있어서 자국의 금융 인프라, ICT 발전 등 환경을 충분히 고려하고 있으며 서비스 영역 또한 결제부터 여수신 업무, 정보보호 까지 광범위하게 적용하고 있다. 각 국가가 처한 특수성 때문에 금융 인프라 수준, 상거래 여건, 정부의 정책 방향 등의 차이에 따라 핀테크 산업의 발달 양상이 다르게 나타나고 있다. 우리나라는 신용카드, 인터넷뱅킹 등 실시간으로 송금 · 결제가 이루어지나 미국의 경우는 시간이 많이 소요되는 특성으로 페이팔 등 결제정보가 노출되지 않는 신속 · 간편한 결제서비스가 개발되어 활성화 되고 있다. 또한 중국은 신용카드 시스템, 지급결제 인프라 등이 미비하고 전자상거래 관련 사기가 빈번하여 결제대금 예치 방식(escrow)[5]의 충전식 전자지갑 서비스인 알리페이가 시장을 지배하고 있다. 특히 미국의 페이팔이나 중국의 알리페이는 시장지배력을 가진 유통사업자(이베이, 알리바바)의 독점적인 결제수단으로 사용되면서 크게 활성화 되었다. 주요국의 핀테크 현황은 살펴보면 〈표 3〉과 같다.

전세계 핀테크(Fintech) 산업은 금융산업이 발전되고 벤처창업이 활발한 미국과 영국이 주도하고 있으며, 최근 들어 이스라엘, 호주, 홍콩, 싱가포르 등도 글로벌 핀테크 산업 활성화에 노력중에 있다. 특히 영국과 미국 등의 주요 금융회사들은 모바일 등 신규 사업 분야의 경쟁력 확보를 위해 유망 핀테크 기업, 인터넷전문은행과 제휴하거나 인수를 추진하고 있다. 영국의 HSBC와 First Direct, Nationwide 등은 핀테크 기업인 Zapp와 제휴하여 비밀번호 입력만으로 간편하게 모바일 결제가 가능한 좀더 진화된 금융관련 서비스를 제공하고 있다.

5 에스크로(Escrow)란 구매자와 판매자 간 신용관계가 불확실할 때 제3자가 상거래가 원활히 이루어질 수 있도록 중계를 하는 매매 보호 서비스이다. 전자상거래의 경우에는 '결제대금 예치'를 의미하며, 거래대금을 제3자에게 맡긴 뒤 물품 배송을 확인하고 판매자에게 지불하는 제도로 사용되고 있다. 즉 소비자가 물건 값을 은행 등 공신력 있는 제3자에게 보관했다가, 배송이 정상적으로 완료되면 은행에서 판매자 계좌로 입금하는 것이다. 물품을 받지 못했거나 반품할 경우에는 금융기관이 즉시 환불해 주기 때문에 인터넷 쇼핑몰을 통한 사기 피해 등을 원천적으로 막을 수 있다.

〈표 3〉 주요국의 핀테크 현황

구분	미국	영국	중국
특징	• 기술혁신을 통한 세계 최대의 핀테크 시장 형성	• 핀테크에 대한 적극적인 정부 정책(Tech City)	• 온라인 소비정책 (모바일 시장 규모 2013년 39.8조 원 → 2016년 149.6조원)
주체	• 실리콘밸리, 뉴욕 등 중심 (전세계 글로벌 핀테크 투자의 83% 차지)	• 금융사(투자), 정부(컨트롤타워)	• 알리바바 등 대형 IT 업체
성공 요인	• 민간주도의 자생적 산업 환경 • 거대 금융센터, 기관, 회사들과 긴밀한 협조와 노하우 공유	• 민관협력(정부, 금융사) • 대형은행 중심으로 핀테크 주도 (금융인력 1백만명, 외국은행 251개, 외국금융사 588개사 주재)	• 거대한 모바일 시장으로 핀테크 수요 급증 (모바일 인터넷 이용자수 2013년 7억명 → 2016년 9억명 돌파전망)

미국의 금융그룹 캐피털 원(Capital One)은 네덜란드의 인터넷전문은행인 ING Direct를 인수하여 지점 없이 온라인으로만 영업을 추진하고 있다. 중국은 알리바바와 텐센트가 주도해 중국 최초로 설립한 5개 민영은행을 중심으로 핀테크 시장이 폭발적 성장을 하고 있다. 중국 모바일 결제 시장규모는 2011년 12조원, 2012년 24조원에서 2013년에는 320조원으로 급성장했다. 거대한 내수시장을 기반으로 2004년 출범한 알리페이는 자국시장 회원 3억명을 돌파했으며 모바일 결제 대행만 4,518만건에 달해 세계 1위로 등극했다. 또한 P2P 온라인 대출 거래 규모도 폭발적으로 성장하여 2009년 1억 5천만위안에서 2013년에는 약 680억위안으로 증가했다. 여기에 알리바바-알리페이-티몰-타오바오-알리윈으로 이어지는 모바일 결제 생태계가 구축되며 핀테크 시장의 발전을 끌어올렸다. 이 외에도 크라우드 펀딩을 제외한 빅데이터 금융서비스 플랫폼, 가상화폐, 인터넷은행 등은 아직 초보 단계에 있다.

2) 해외 주요 핀테크 기업 현황

해외 핀테크 기업들은 혁신적인 비즈니스 모델과 ICT 기업과의 제휴를 통해 글로벌 시장에 진출하고 있다. 이러한 기업들은 상이한 각국 통화나 결제시스템의 차이에 구애 받지 않고 전세계 개인고객과 기업들을 대상으로 편리한 지급결제 서비스를 제공하고 있다. 금융회사가 보유한 다양한 금융정보를 분석하여 초단시간에 고객의 신용도를 평가하거나 금융사고 여부를 정확하게 판단하는 보안기술을 보유하고 있다. 대표적인 기업으로는 결제(페이팔, 알리페이, 애플페이 등), 국제송금(Trasferwise 등), 온라인 대출중계(Ondeck 등), 보안자산관리(Billguard 등) 등이 있다.

〈표 4〉 해외 주요 핀테크 기업 현황

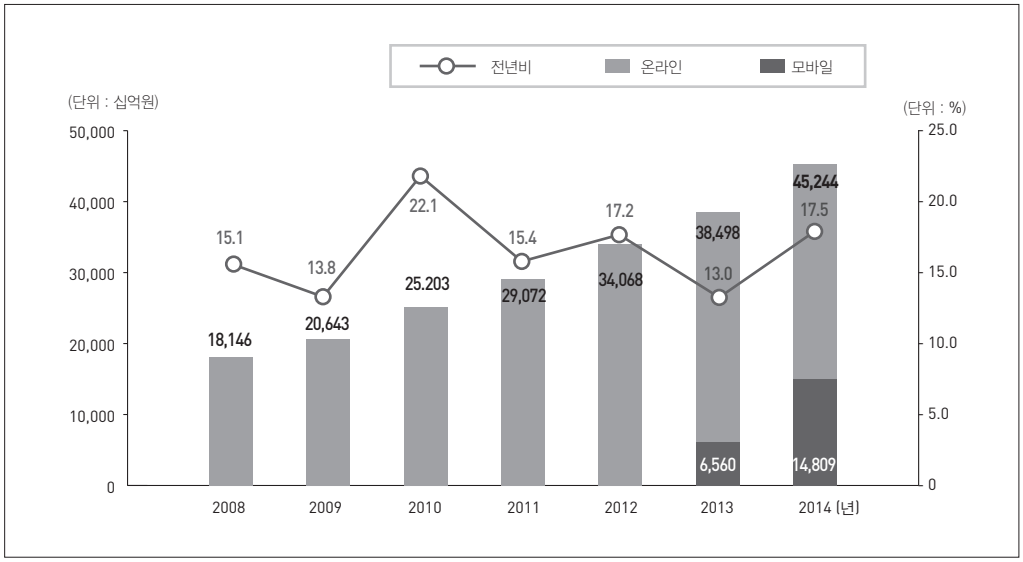
구분	종류	대표회사	특징	국가
송금	모바일 및 이메일 송금	사파리컴 (M-Pesa)	• 모바일 은행계좌처럼 이용하는 M-Pesa, 거래량이 케냐 GDP의 43% ('14. 1 기준)를 차지	케냐
		구글	• 구글월렛(전자지갑), 안드로이드 페이(결제 앱) • 소프트카드의 근접무선통신(NFC) 결제방식 구글이 인수	미국
		애플	• 패스북(전자지갑)	미국
		페이스북	• 전자화폐(아일랜드), 아지모와 제휴	미국
		텐센트	• 텐페이, MMF 리차이퉁	중국
		트랜스퍼와이즈	• 개인간 외환거래를 돕는 글로벌 인터넷 플랫폼 제공회사	영국
		PayPal	• 이베이의 자회사로 이메일 송금서비스를 제공	미국
		아마존	• '아마존페이컨트', 자사 사이트 내 결제서비스	미국
결제	전자결제시스템	Applepay	• 애플페이는 NFC 칩을 탑재한 아이폰6과 아이폰6 플러스, 아이워치에서 이용할 수 있는 서비스	미국
		Alipay	• 알리바바의 자회사로 타오바오 등에 결제서비스를 제공해주며 MMF 등 금융상품도 출시	중국
		Square	• 모바일 결제서비스 제공	미국
		PayPal	• 이베이의 자회사로 신용과 결제서비스를 제공	미국
		Stripe	• 전 세계 139개국 통화와 비트코인, 알리페이 등으로도 결제 가능	미국
		소프트카드	• AT&T와 버라이즌, T모바일 USA 등이 손잡고 공동 설립한 모바일 결제서비스 업체	미국
		AstroPay	• 중남미에서 가장 빠르게 성장하는 결제솔루션 회사	영국
자산관리	펀드, 인터넷은행, 보험, 증권	퍼스널캐피털	• 개인별 자산현황을 종합적으로 분석해 연금계획, 투자포트폴리오 및 소비행태 조정, 세금 및 금융비용 계산 등 다양한 자산관리서비스(빅데이터 기반, 20조원 관리)	미국
		중안온라인보험	• 알리바바, 텐센트, 형안보험이 투자한 인터넷 보험회사	중국
		파도르은행	• 2009년에 설립된 소셜미디어를 접목한 온라인 은행	독일
		etrade	• 온라인 전용증권사로 개인의 주식거래를 중개	미국
		Motif Investing	• 주식 또는 채권 최대 30종으로 이뤄진 테마별 투자 포트폴리오를 투자자들에게 제공하는 온라인 전용 위탁매매 서비스 업체. 사이버보안, 3D 프린팅, 석유가격, 금리 변동 등의 테마로 분류, 빅데이터를 활용해 종목을 선정	미국
투자	금융투자 플랫폼	엔젤리스트	• 초기 스타트업과 엔젤투자자를 연결 짓는 소셜네트워크 플랫폼 제공 업체	미국
		렌딩클럽	• 개인간 대출(Peer to Peer) 중개를 해주는 업체	미국
		Ondeck	• 자체개발한 신용평가 알고리즘이 대출 신청자의 금융기관 거래내용, 현금흐름, SNS상 평판 등을 고려해 몇 분만에 신용평가 및 대출여부 심사(플랫폼 제공업체)	미국
보안 및 데이터 분석	정보보안	사이버소스	• 비자카드의 자회사로 영국, 중국, 싱가포르, 일본 등 37개국에서 전자결제서비스를 제공, 전 세계 40여만 개의 기업들에게 온라인 지불 프로세스 및 부정거래 관리를 위한 지불보안 서비스 제공	미국
	데이터 분석	Affirm	• 공개 데이터를 통한 신용도 평가 후 할부수수료 책정, 자사 가입회원이 온라인 쇼핑몰에서 물건을 구매할 때 신용카드가 아닌 본인의 신용으로 할부 구매할 수 있는 결제 서비스 제공	미국
		Palantir Technologies	• 미국 CIA로부터 약 22억 원의 투자를 받아 시작되었으며, 페이팔 출신 Peter Thiel이 창업한 회사. 모든 구조화/비구조화된 정보의 통합 작업을 간소화해 사이버보안 담당자들이 보다 쉽고 신속하게 보안상의 경고를 조사하거나, 사이버범죄 및 사기와 관련한 주된 패턴을 찾을 수 있게 해줌	미국
		Splunk	• 기계 판독 데이터 검색을 수 초 안에 가능할 만큼 쉽고 빠르게 지원해 기업이 자사 데이터를 ≪구글과 유사한≫ 방식으로 찾을 수 있게 해줌. 조직 내 보안 위반사항이나 사기 이벤트 탐지가 가능	미국
	금융 S/W	Billguard	• 모바일 앱으로 회원의 신용카드와 은행 계좌를 통합 관리 가능, 모바일 앱을 통해 회원의 신용카드와 은행 금융정보를 통합한 개인자산관리서비스도 제공	미국

※ 출처 : 여신금융연구소, "핀테크의 가치창출 요건 및 시사점", 2015.1. 참고 재구성

3. 국내 핀테크 산업 현황

1) 전자금융거래 현황

통계청의 온라인 쇼핑동향 자료에 따르면 최근 국내 스마트폰 가입자 수가 4,000만명을 넘어서고 국민 80% 이상이 모바일 기기를 가지고 있다. 지난해 국내 모바일 쇼핑 거래액이 14조 8천 90억원을 기록해 1년 사이 2배 이상으로 급증한 것으로 나타났다. 2014년 전체 온라인 쇼핑 거래액은 45조 2천 440억원으로, 이중 모바일 쇼핑이 32.7%(14조 8천 90억원)를 차지했다.



[그림 1] 온라인쇼핑 거래액 동향(통계청)[6]

한국은행에 따르면 인터넷 뱅킹 서비스(모바일 뱅킹 포함) 등록 고객수는 1억 110만명으로(2014년 9월말 기준) 전분기말 대비 1.6% 증가하면서 1999년 인터넷 뱅킹 서비스 개시 이래 최초로 1억명을 돌파하였으며, 2014년 3/4분기중 인터넷 뱅킹(모바일 뱅킹 포함) 이용건수(일평균)는 6,645만건, 이용금액(일평균)은 36조 7,131억원으로 전분기 대비 각각 2.8%, 2.5% 증가하였다. 또한 스마트폰 뱅킹 이용건수 및 금액은 3,161만건, 1조 8,232억원으로

6 통계청, "2014년 4/4분기 및 연간 온라인쇼핑동향" 2015.1.29.

전분기 대비 각각 7.6%씩 증가하였다. 금융서비스 전달 채널별 업무처리 비중에서도 〈표 5〉와 같이 비대면거래가 88.7%로 대면거래 11.3%보다 계속 증가세를 보이고 있다.

〈표 5〉 금융서비스 전달 채널별 업무처리비중(%)[7]

기간	대면거래 (창구거래)	비 대 면 거 래				합 계
		소계	CD/ATM	텔레뱅킹	인터넷뱅킹	
2012. 9월중	12.2	87.8	42.7	14.8	30.3	100.0
2012.12월중	13.0	87.0	39.8	13.4	33.9	100.0
2013. 3월중	12.3	87.7	42.3	14.0	31.4	100.0
2013. 6월중	11.6	88.4	42.2	13.7	32.5	100.0
2013. 9월중	11.6	88.4	41.2	13.3	33.9	100.0
2013. 12월중	12.2	87.8	40.6	13.1	34.1	100.0
2014. 3월중	11.3	88.7	41.2	13.0	34.5	100.0
2014. 6월중	11.2	88.8	41.0	13.3	34.5	100.0
2014. 9월중	11.3	88.7	40.7	12.9	35.0	100.0

국내 전자결제 규모와 비교하여 중국의 경우 중국 인민은행의 '2014년 지불시스템 현황'에 따르면 지난해 중국에서 이뤄진 전자결제 총액은 1천 404조 6천 500억위안(약 25경원)으로 전년보다 30.7% 증가했다. 전자결제 총액 가운데 모바일 결제액은 22조 5천900억위안으로 전년보다 134.3%나 늘었다. 또한, 인터넷 결제액은 1천 376조 200억위안으로 29.7%, 전화를 이용한 결제액은 6조 400억위안으로 27.4% 각각 늘었다. 이렇게 엄청난 중국내 거대 시장이 중국의 핀테크 산업이 급 성장하는 배경으로 보인다.

2) 국내 핀테크 기업 현황

국내는 신용카드사, 오픈 마켓, PG사가 각각 공인인증서가 적용되지 않는 소액결제에 대해 최근 간편결제 서비스를 제공해 왔으며, 금융당국의 공인인증서 사용 의무화 폐지와 간편결제 도입을 위한 규제 완화 이후 카드사와 신용정보 보관이 가능해진 PG업체의 서비스 확대가 추진되고 있다. 핀테크에 대한 추진 방향, 사업 영역, 분류, 서비스 내역 등에 대한 해석이 이해관계 주체에 따라 다양하며 시장을 바라보는 시각도 다른 것 같다. 국내 금융환경의 특수성도 있지만 금융 기반의 핀테크냐 기술기반의 테크핀이냐 보안 기반의 핀테크냐 등

7 한국은행, "2014년 3/4분기 국내 인터넷뱅킹서비스 이용현황", 2014.11.19.

〈표 6〉 국내 주요 핀테크 기업 현황

구분	종류	회사	서비스명칭
송금	플랫폼	다음카카오	뱅크월렛카카오(모바일지갑), 카카오페이(간편결제), 증권 플러스 for kakao
		네이버	라인페이, 네이버페이
	IT업체	비바 리퍼블리카	토스(송금, 계좌이체)
결제	모바일기기	삼성전자, LG전자	삼성월렛(전자지갑), 삼성페이, 앱카드
	통신사	KT	모카월렛(전자지갑), 모카페이(간편결제), 페오온 플러스, 탭사인, olleh touch, 올래앱 안심인증
		LG U+	Paynow+(간편결제), u+스마트월렛, 페이나우 플러스
		SKT	BLE 페이먼트
	PG업체	LG CNS	Mpay
		KG 이니시스	INIpay, Kpay
		페이게이트	MCP, AA(간편결제)
		KG 모빌리언스	엠틱, MCASH
		한국사이버결제(KCP)	페이코(퀵페이), 페이온(NFC 결제)
		브이피	일반결제(ISP), BC PayALL(간편결제), ISPay(휴대폰 결제)
	오픈 마켓	이베이, G 마켓, 옥션	Smilepay(간편결제)
		인터파크	Yellowpay
		티몬	티몬페이
	기타	SK 플래닛	페이핀(간편결제), 시럽(전자지갑)
		다날	바통(직불결제)
		한국 NFC	모바일 NFC 간편결제
자산관리	개인 온라인자산관리	에셋다이어리, 리더스리치, 키움에셋플래너 등	자산관리, 재무설계
투자	크라우드 펀딩	팝펀딩	굿펀딩(P2P 대출모집)
정보보호 및 데이터분석	모바일 보안	현재 지급결제 분야 이외에 국내 정보보호 업체 대다수가 핀테크 보안 분야에 포함되거나 진출 중으로 구체적 회사 명칭 및 서비스명은 생략	
	보안솔루션개발 (FDS, 안증 등)		
	인터넷 정보보호		
	개인, 기업 보안		

※ 출처 : 여신금융연구소, "핀테크의 가치창출 요건 및 시사점", 2015.1 참고 재구성

정의도 각기 다르다. 핀테크 기업이 접근하기에는 각종 규제, 보수적인 금융 환경, 금융기관별로 적용하는 핀테크 기술 등이 다르기 때문에 접점을 찾기가 어렵다는 문제도 있다. 공인인증서와 ActiveX 문제, 인증기술인 일회용비밀번호생성기(OTP, One Time Password)[8]

8 OTP(일회용 패스워드, One Time Password)는 무작위로 생성되는 난수의 일회용 패스워드를 이용하는 사용자 인증 방식이

등 일부 접근매체에 집중되 있다 보니 단순 간편결제 분야 위주로 발전하고 있다.

우리나라는 금융분야에 대한 높은 규제장벽으로 금융과 IT와의 융합이 느리게 진행되어 왔으나 최근 들어 IT업체의 금융업 진출에 위협을 느낀 국내 은행들이 ICT업체와 제휴를 본격화하는 양상을 보이고 있다. 또한 최근 해외 주요국에서 인터넷전문은행(Internet Primary Bank)이 꾸준하게 성장하고 있어 국내에서도 인터넷전문은행 설립에 대한 논의가 본격화될 전망이다. 그러나 금산분리 원칙이나 지분율 제한 등 규제 문제와 보안 문제는 여전히 풀어야 할 숙제이다. 인터넷전문은행은 지점망 없이 운영되는 저비용 구조로, 기존 은행에 비해서 각종 수수료를 최소화 하면서도 수익을 낼 수 있는 구조로 은행 이용자에게 보다 높은 예금금리, 낮은 대출금리, 저렴한 수수료 제공이 가능하다는 장점이 있다.

〈표 7〉 기존 은행과 인터넷전문은행 비교

분야	기존 은행	인터넷전문은행
인터넷 금융거래	인터넷을 보조적 영업채널로 간주 조회 및 이체거래 중심	인터넷을 주 채널로 영업하며, 모든 거래가 인터넷을 통해 이루어짐
영업 기반지역	지역 점포를 중심으로 해당 지역적 기반을 두고 있는 고객 중심	해당국가 또는 전 세계
영업시간	인터넷뱅킹의 조회, 이체를 제외하고는 영업시간 제한(09시~16시)	24시간 영업 체계를 통한 고객의 시 · 공간적 접근성 향상
업무범위	금융과 관련한 대부분 업무를 모두 취급	지급결제, 소액대출, 신용카드, 전자화폐 등 업무의 특화(Niche Marketing) 가능

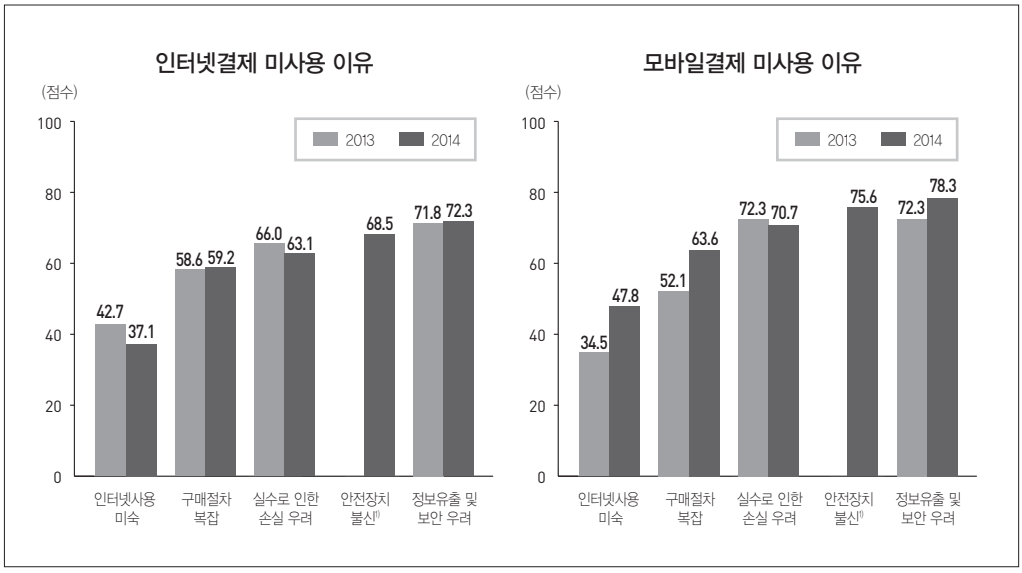
문제는 ICT 기반의 인터넷은행은 대부분 온라인으로 이루어지기 때문에 비대면에 따른 보안상 문제점을 어떻게 풀어내느냐가 관건이다. 금융위원회에 따르면 국내 인터넷전문은행 설립을 위한 중요한 요건으로 네트워크, 백업체계 및 차별화된 보안체계를 요구하고 있다. 인터넷전문은행의 성공 여부는 모든 업무가 인터넷으로 이루어지기 때문에 강력한 사이버 보안기술과 정책이 필수적으로 수반되어야 하며 튼튼한 고객 기반과 고객의 니즈, ICT 기반 기술에서 경쟁력에 좌우될 것이다.

다. 보안을 강화하기 위하여 도입한 시스템으로, 로그인 할 때마다 일회성 패스워드를 생성하여 동일한 패스워드가 반복해서 사용됨으로 발생하는 보안상의 취약점을 극복하기 위해 도입되었다.

Ⅲ. 핀테크 보안 전략

1. 핀테크 보안 중요성

지난해 우리나라는 카드 3사 개인정보 유출사고, POS시스템 해킹, 텔레뱅킹을 통한 1억 2천만 원 인출사고 등 크고 작은 금융사고가 지속적으로 발생하고 있다. 통계청 조사에 따르면 2014년도 온라인 결제 이용자들의 '인터넷결제 및 모바일 결제 미사용 이유'로 '정보유출 및 보안우려(72.3%, 78.3%)'를 가장 중요시 하고 있다. 금융서비스에 대한 새로운 접근채널이 확대됨에 따라 해킹 등 보안 및 개인정보에 따른 손실 우려가 커지고 있다는 것이다.



※ 출처 : 통계청, 2014년 지급수단 이용행태 조사결과 및 시사점

[그림 2] 인터넷 결제 및 모바일 결재 미사용 이유

해외의 경우 2007년 대형 글로벌 패션업체인 TJX에서 약 1억건의 신용정보와 개인정보가 유출되어 신원도용, 계좌 부정인출, 카드 부정사용 등 2차 범죄로 피해가 발생한 바 있다. 2009년에는 미국 신용카드 결제 업체인 Heartland Payment Systems가 해킹으로 금융정보(카드번호, 유효기간 등) 1억 3천만 건이 유출됐으며, 대형 할인 매장인 Target도 고객정보, 금융정보 등이 해킹으로(2013년) 7천만 건이 유출되었으며 작년에 인터넷 경매 사이트인

eBay가 해킹으로 개인정보가 유출되는 대형 사고를 당한바 있다. 또한 최근 가상화폐인 비트코인의 거래소인 비트스팸프가 1만 9000비트코인(약 55억원)을 해킹을 당해 거래가 일시 중단되는 사태가 발생했으며, 전 세계에 걸쳐 이용자가 1억명이 넘는 페이팔도 모회사인 이베이가 해커들의 공격을 받아 이베이 계정과 연동된 페이팔 계정이 외부로 유출됐다. 해외 핀테크 기업의 정보유출 사고는 국내'직구족'이 늘어나고 있는 것을 감안하면 매우 심각한 수준이다.[9]

핀테크는 보안이 선결되어야지 가능한 서비스이다. 보안이 뒷받침 되지 않으면 핀테크 시대에서는 어떠한 보안 위협이 발생할지 모르기 때문이다. 사용자의 접근성은 간편하게, 사용자의 안전성은 강화되야 하는 양날의 칼과 같다. 그래서 편의성과 보안의 조화가 필요하다. 또한, 피해를 최소화할 수 있도록 법적 책임을 명확하게 하되 이해당사가간 이해와 합의가 필요하다. 이렇게 핀테크 산업이 바람직하게 발전하고 금융 혁신을 이루기 위해서는 무엇보다도 핀테크의 보안성 강화가 절실한 상황이다. 미국의 애플페이, 중국의 알리페이와 같이 금융서비스를 이용하는 사람들에게 지금보다 간편하고, 편리한 서비스를 낮은 비용으로 안전하게 제공하는 것이 핀테크의 성공여부를 판가름 할 것이다.

2. 해외 주요 핀테크 기업 보안 체계

1) 미국, 영국 등 핀테크 선진국 보안 체계

미국, 영국 등 핀테크가 활성화된 국가의 핀테크 보안기술은 고객의 편의를 위해 금융거래를 할 때는 절차상의 보안은 완화하는 대신 사후에 부정 · 사기 거래를 찾아내고 문제를 걸러내는 사후 보안 강화 방식을 쓰고 있다. 이 같은 효율적인 보안 수준은 정부가 획일적으로 규제하지 않고 선별적 · 선택적 규제로 민간에서 자율로 정립했기 때문에 가능하다. 또한 사고 당사자에 대한 무거운 처벌과 보안사고의 책임 분산, 핀테크 기업들의 풍부한 보안 인력과 기술이 핀테크 산업 혁신을 이룰 수 있었던 원동력이 되었다고 본다. 주요국의 핀테크 보안 체계를 살펴보면 〈표 8〉과 같다.

9 아시아경제, "800조 핀테크 세계전… 금융·IT 스타트업, "2015.2.11.

〈표 8〉 미국, 영국 등 핀테크 선진국 보안 체계의 특징

구분	특징
'사전 규제'보다 '사후 보안' 강화	소비자의 편의를 위해 금융거래를 할 때는 보안 절차를 완화하는 대신 사후에 부정 · 사기 거래를 찾아내고 문제를 걸러내는 방식
선별적 · 선택적 규제	획일적으로 똑같은 보안수준을 강요하지 않고 거래 규모나 고객의 신용도에 따라 보안 강도를 차별적으로 집행. 소비자에게 보안 수위에 대한 선택권도 부여
사고 당사자에 대한 무거운 처벌	중대한 보안 사고를 저지른 기업에 대해서는 천문학적인 과징금을 매기는 등 가중처벌
민간 자율 규제 체계	민간이 자율적으로 보안 체계를 갖춤(PCI-DSS 등)
보안사고의 책임 분산	전자결제 업체나 IT기업, 금융소비자에게도 책임을 묻는 방식
핀테크 기업들의 풍부한 인력과 기술	검증된 첨단 FDS, 빅데이터 분석기술, 인증기술 등 확보, 풍부한 보안 관련 인력

※ 출처 : 동아일보, "금액-신용도따라 보안수준 차별화···금융거래 효율성 높여" , 2015.02.12., 참고 재구성

2) 주요 핀테크 기업의 보안 체계[10 · 11]

(1) 페이팔(PAYPAL)

페이팔 가입자는 물품 구매시 추가적 S/W 설치 가 불필요하며 페이팔 ID/PW만 입력하면 카드정보 입력이나 본인인증 절차 없이 결제가 가능하다. 일부 국가에서는 휴대폰 단문문자메세지(SMS) 또는 OTP(One Time Password)를 통한 추가 인증 절차가 필요하다.

가. 보안 체계

- 페이팔이 진출한 20개국에 500여 명의 정보유출방지 전담 인력 배치, 보안과 리스크 관리 등 인력을 합치면 전 세계 17개 센터 직원 7,000명이 보안 업무 수행
- PCI-DSS[12] 보안표준을 준수하는 동시에 전자금융사기를 방지하기 위해 보안업체를 인수하고(Fraud Science) 새로운 보안기술을 도입하여 금융사고 발생을 예방
- 웹 표준(SSL)[13] 활용, 휴대전화 등록 시 추가 인증(SMS) 가능

10 금융보안연구원, "전자지급결제서비스 동향 및 시사점", 2014.10.

11 여신금융협회, "간편결제서비스 확대에 따른 환경변화 요인 점검", 2014.9.

12 PCI-DSS(Payment Card Industry Data Security Standard) : PCI SSC(Security Standards Council)에서 발표하는 소비자의 신용카드 정보 보호, 신원 도용 및 사기방지, 글로벌 결제시스템을 위한 데이터 보안 강화를 목적으로 하는 가장 포괄적이며 국제적으로 인정받는 '데이터 보안 표준'이다. PCI SSC는 비자, 마스터, 아메리칸익스프레스, JCB, 유니온페이 등 글로벌 신용카드사에서 정보 유출을 막기 위해 설립한 신용카드협회 보안표준위원회다.

13 SSL(Secure Socket Layer)이란 웹서버와 PC간 이동하는 데이터를 암호화하는 글로벌 표준 암호화 알고리즘

– FDS(Fraud Detection System)[14]를 이용하여 부정거래 행위를 24시간 모니터링
– 송금, 결제 정보가 이메일로 구매자에게 전달되므로 피싱(Phishing) 사기 방지를 위해 피싱사이트 필터링 시스템을 운영

나. 사고배상책임

– PCI-DSS를 준수하지 않은 상태에서 정보유출 발생시 카드 브랜드사는 벌금부과 및 카드결제 승인 거부 등의 수단으로 해당 회사를 제재
– PCI-DSS를 준수했을 경우 민사소송에서는 면책되지 않지만 공공부문 소송에서는 면책이 가능
– CVC 없이 결제가 이루어진 이후 발생한 사고에 대해서는 PCI-DSS가 준수되었는지 확인후 보상여부를 결정

(2) 알리페이(ALIPAY)

알리페이는 신용카드 · 은행계좌 등을 가상계좌와 연동하여 입 · 출금, 결제, 송금, 담보거래, 요금납부, 펀드, 보험 등 다양한 금융서비스를 제공하고 있다.

가. 보안 체계

– 알리페이는 PCI-DSS 보안표준을 준수하고 있으며, 인증서에 의한 서버인증(VeriSign), 웹표준(128bit SSL)을 활용하여 거래 및 인증데이터 암호화
–'05년부터 실시간 모니터링을 통한 전자금융결제 사고 방지를 위해 FDS 도입 · 운영
– 데이터 암호화 기술을 활용한 SSL인증서와 자체 앱(app)을 기반으로 한 OTP서비스를 제공
– 다양한 보안 S/W, H/W를 사용자의 선택에 따라 설치 및 사용 가능

14 페이팔의 FDS 도입 배경 :'01년 국제해커가 페이팔계정에 침투하여 다수의 계정으로부터 소액을 이체, 국제 사기로 판단, 미연방수사국(FBI)에 협조를 요청하였으나 한달에 10억꼴로 손실이 지속 되고 해결도 잘 안되던 상황, 이에 페이팔은 결제사기를 법에 기대기 보다는 자사의 위험관리(risk management) 차원으로 받아들이고 독자적인 이상징후 탐지시스템을 구축

나. 사고배상책임

- 결제사고 발생시 회원에게 피해금액의 한도 내에서 손해 배상을 하며, 회원이나 제3자에게 책임이 있는 경우는 제외
- 배상조건에 부합할 경우 고객 증빙자료를 바탕으로 배상여부를 결정
- 회원의 ID/PW, 검증번호, 신분정보 유출, 연계 은행의 시스템 문제, 천재지변 등 불가항력 발생으로 인한 사고는 배상 책임에서 제외

(3) 구글 월렛(GOOGLE WALLET)

구글 월렛은 전자지갑 서비스로 온라인 오프라인(상점) 결제를 모두 지원하며, 지메일, 구글플러스 등 자사 서비스와 연계한 결제 부가서비스 제공하고 있다.

가. 보안 체계

- 웹 표준 기술사용, PIN 번호, 실시간 트랜잭션 통지 등의 대책 마련
- 통신 시 SSL 암호화 프로토콜 사용, 결제 데이터 저장 시 최소 2,048 bits 암호화
- PIN번호 설정을 통해 구글월렛 앱 접근, ATM인출 등에 사용가능
- 앱을 통한 실시간 거래 내역을 통지

나. 사고배상책임

- 거래일로부터 120일 이내에 보고된 비 인가된 거래에 대해서 100% 보상프로그램 마련(미국 내)
- 분실폰 관리를 위해 온라인(wallet.google.com)에서 원격으로 구글 월렛 앱 또는 카드 중지 가능

(4) 아마존 페이먼츠(AMAZON PAYMENT)

아마존 페이먼츠는 아마존 계정에 결제정보(은행계좌, 신용카드)와 배송정보를 연결, ID PW만 입력하면 원클릭으로 결제 및 배송 가능하다. 또한 AWS[15] 등을 이용한 초기사업자에

15 AWS(Amazon Web Service) : 인터넷을 통해 서버 및 네트워크의 자원을 임대하여 사용하는 일종의 클라우드 컴퓨팅 서비스

게는 일정 매출 발생 시까지 결제 서비스 수수료가 무료이다.

가. 보안 체계

- 추가 비용 없이 아마존의 검증된 FDS를 통하여 결제 서비스 보호
- SSL 등 표준기술 활용, 추가 S/W의 설치가 없으며 추가인증 필요시 질문/답변 방식 활용
- 모든 정보는 아마존 클라우드 서버에 저장하며, 어떠한 결제정보도 제3자에게 전달하거나 공유하지 않음

Ⅳ. 핀테크 보안기술의 패러다임 전환

핀테크는 기존 보수적인 금융업계의 관념을 깨고 IT와 금융의 경계를 무너트리는 혁신적인 변화이다. 핀테크는 단순한 트랜드가 아니다. 규제의 틀 안에서 그들만의 리그를 펼치던 시대는 지났다. 핀테크라는 IT · 금융 융합 패러다임에 금융회사에게만 맡겨두면 안 되겠다는 의미이다. 해외 사례처럼 핀테크 산업의 성공적인 비즈니스 모델은 은행이 하지 못하는 일을 대부분 ICT 기업, 플랫폼이나 보안업체가 주도했다. 더욱이 금융서비스 뿐만 아니라 정보보호 기술에 있어 새로운 패러다임 전환을 의미하고 또 그렇게 바꿀 것이다. 간편하고 편리하고 안전한 금융서비스를 제공하기 위해서는 결국 '보안'을 간과해서는 안 된다. 우리가 추구하는 핀테크의 가치인 간편하고 편리하고 안전한 금융서비스의 미래는 사람중심의 '보안' 문제에 달려있다. 핀테크의 방향에 따라 보안기술도 어떤 기술이 등장할지 예측하기는 어려우나 핀테크 보안 기술이 금융시장에서 최고의 경쟁력이 될 것임은 틀림없다. 따라서 핀테크 시대에는 기존 보안 제품이나 서비스를 뛰어 넘는 혁신적이고 창의적인 새로운 글로벌한 보안기술과 보안사고시 어떻게 접근해야 하는지 사고의 패러다임 전환이 필요하다. 핀테크 보안기술에 대한 패러다임 전환에 대해 살펴보고자 한다.

1) 공인인증서[16] 등 대체 인증 기반 기술

공인인증서는 부인방지 등 높은 보안수준으로 인해 국내 금융거래 시 기본 보안수단으로 지난 15년간 사용되어 왔으나, ActiveX 등 非표준기술로 구현되어 금융거래 편의성을 저해하고 안전한 관리가 어렵다는 지적을 받아왔다. 공인인증서에 기반한 생태계가 무너지고 다양한 인증 기술의 도입과 더불어 전자금융과 모바일 결제서비스 등 금융시장의 지각 변동이 예고되고 있다. 최근 전자서명 키 위임방지 기술,[17] HTML5 기반,[18] 스마트 카드 기반[19] 등 다양한 공인인증서 기반 기술이 시장에 등장하고 있다. 결제분야는 간편 인증(ARS, SMS)으로 대체 중이며 뱅킹 증권 분야는 서명 기능과 편의성이 더해진 非설치형 공인인증기법이 본격 활용될 것이다. 공인증서를 대체하는 것만이 능사가 아니지만 공인인증서의 벽을 넘으면 다양한 인증 수단을 활용한 새로운 금융상품 개발이 가능하다. 금융회사와 ICT 기업들이 공인인증서에 대한 절대적인 의존에서 벗어나 보안성과 편리성을 갖춘 혁신적인 금융서비스를 개발해야 글로벌 경쟁에서 뒤처지지 않는다.

2) 빅 데이터 분석 기술 개발 및 활용 기반 마련

국내 금융환경에 적합한 '빅데이터 분석 솔루션' 및 '빅데이터 플랫폼' 등 빅데이터 기술개발을 서둘러야 한다. 또한 활용 측면에서는 개인정보 보호를 전제로 빅 데이터 분석을 통해 비 식별화된 빅 데이터를 바탕으로 新 금융상품 개발, 부가서비스 제공, 마케팅 활용, 금융관련 부정행위 방지, 신용평가, 리스크 관리 등 금융 빅 데이터 분석기술 개발이 필요하다. 또한 금융거래(결제 · 여신 · 자산운용 기록 등) 정보의 분석 · 활용 능력을 갖춘 금융 빅 데이터 전문인력 양성도 필요하며, 결제 정보에 관한 빅 데이터 분석을 통해 선호 업종 지역 등 소비 패턴을 고려한 맞춤형 서비스를 개발해야 한다. 개인정보 및 금융정보 등 보호를 위한 내부통제 정책에 있어서도 내부 위협을 감지하고 차단하는 빅 데이터 분석기반 내부통제 시스템

---

16 공인인증서 : 국산암호화 기술인 SEED(웹브라우저 미지원)와 함께 사용. 당시 IE가 국내에서 지배적으로 사용되면서 ActiveX를 활용하여 구현됨. 결제·뱅킹 시 공인인증서가 의무화됨에 따라, ActiveX가 동작하는 IE에 대한 의존도가 더욱 심화되었으며, 이후 ActiveX에 대한 보안취약성 대두, OS 및 브라우저 환경변화에 따라 서비스가 불가능하게 되는 등 사용자 편의를 저해하는 상황발생

17 전사서명 키 위임방지 기술 : 전자서명값을 제3의 신뢰기관이 보유, 고객 서명 시 인증(OTP 등)을 통해 서명요구를 밝히면 신뢰기관은 고객을 대신하여 서명

18 HTML5 기반 : 웹 브라우저가 관리, 통제하는 영역에 공인인증서를 저장

19 스마트 카드 기반 : 신용카드 IC칩내에 공인인증서를 저장, 스마트폰을 매개체로 하여 인증 및 전자서명 수행

도 구축이 필요하다. 또한 빅데이터의 적극적인 활용을 통한 핀테크 산업의 혁신 및 발전을 위해서는 개인정보보호 이슈와 조화로운 추진 방향을 모색해야 한다.

3) 간편결제 수단 개발

그동안 안전한 보안기술로 평가 받던 공인인증서가 작년에 규제의 대표적인 예로 지목되면서 다양한 인증 기술, 간편결제 등 지급결제서비스 시장의 판도를 바꾸고 말았다. 핀테크의 상징을 의미하는 간편결제[20] 방식은 주로 온라인 구매시 지급결제에 필요한 개인정보와 신용정보를 전달하는 과정을 단순화하여 거래의 편의성을 향상시키는 서비스를 의미한다. 개인정보와 신용정보를 특정 서버에 등록하고 거래 발생시 설정된 인증수단으로 본인인증을 완료하는 서버형 결제방법을 주로 사용한다. 서버형 결제에는 웹(web) 표준기술이 적용되므로 PC, 스마트폰, 태블릿PC 등 다양한 접근매체를 통해 사용이 가능하다. 전세계적 대표적인 대형 PG(payment gateway)[21]업체인 미국의 페이팔과 중국의 알리페이가 이러한 방식의 'One-Click 결제서비스'를 제공해오고 있다.

한편, 국제 간편결제 방식 표준화 동향은 ID/PW 방식과 국제 표준을 주도하는 FIDO[22] 방식으로 이원화 되는 양상을 보이고 있다. FIDO가 발표한 'FIDO 1.0'인증 표준은 사용자 인증의 새로운 규격으로 서버에서 인증하는 방식이 아니라 클라이언트에서 인증하는 방식이다. PW기반 인증과는 다르게 인증 정보를 서버에 보관이나 송신하지 않기 때문에 공격자에게 도난당하거나 유출될 위험성이 적다는 것이다. FIDO 표준은 두 가지 프로토콜을 제안하고 있다. 하나는 UAF(Universal Authentication Framework)로 사용자의 디바이스에서 제공하는 인증방법을 온라인 서비스와 연동하여 사용자를 인증하는 기술이고 두 번째는 U2F(Universal Second Factor) 로 기존 PW를 사용하는 온라인 서비스에서 두 번째 인증 요소로 강한 인증을 사용자 로그인 시에 추가할 수 있는 프로토콜이다.[23]

---

20 간편결제 : 복잡한 세부정보 입력이나 S/W 추가 설치 없이 ID·PW만으로 결제(사전에 설정해 둔 ID/PW + 사전 인증(공인인증서, SMS 등)

21 PG(payment gateway)사업자는 전자상거래 공급업체(온라인 가맹점 등)을 대표하면서 수요자와 공급자간의 온라인 대금결제를 중계하고 정산하는 통합전자결제시스템 사업자를 의미

22 FIDO(Fast Identification Online Alliance) : 국제 온라인 인증 컨소시엄으로 최근 증대되는 온라인 및 모바일 보안 위협에 대해 쉽고 안전한'글로벌 인증 기술 표준'을 개발하고 보급하기 위해 조직된 범세계적 연합체로 구글, 마이크로소프트(MS), 알리바바, 크루셜텍, 레노보, 삼성, LG, 마스터카드, 비자, 페이팔, 야후, 퀄컴, 등 IT, 금융, 전자상거래, 생체인식 업체를 망라한 전세계 153개 기업이 회원사로 활동 중이다.

23 한국전자통신연구원, "패스워드없는 인증기술-FIDO", 2014.8.

또한 최근 미국의 핀테크 기술 정책은 명의 도용을 방지하기 위한 국가 아이덴티티 기술을 개발해 적용하며, 온라인 결제 사기를 방지하기 위한 안전한 지불 결제 기술을 개발하고 적용하며, 이를 뒷받침할 법제도 개선을 추진하고 있다. ID/PW 기반 인증 체계도 "바이오인증 + 공개키기반구조 + IC 카드" 기반 다중요소 인증(multi-factor authentication)[24] 기술로 변경하기로 하고 American Express, 인텔, 마스터카드 등 기관이 다중 요소 인증 기술 도입을 추진하고 있다.[25]

4) FDS(Fraud Detection System, 이상거래탐지시스템) 기술 고도화

국내의 결제시스템은 사용자단에서 인증 작업 등의 보안절차가 진행되는 반면 해외에서는 대부분 사용자단 보다는 서버단에서 보안절차가 이뤄어진다. 이러한 서버단의 보안 강화를 위해 FDS 등 보다 강력한 보안체계가 적용되고 있다. 페이팔과 알리페이 등 주요 핀테크 기업들은 FDS를 통해 부정결제, 무단 계좌 이체 등 이상 징후를 미리 파악해 피해를 최소화 한다. 이렇게 해외에서는 FDS 운영을 통해 서버단에서 보안 위협에 적극적으로 대응을 하여왔으나 국내는 아직 도입단계에 있다. 이 시스템을 통해서 사용자의 평소 거래 패턴을 분석하여 범위를 정한 이후에 그 범위 이외의 액션이 취해지게 되면 이상 행위로 판단하여 제제를 가한다는 것이 FDS의 기본 개념이다. 이 모든 작업들은 사용자단이 아닌 거래가 이러난 이후 서버단에서 모두 진행된다.

FDS는 패턴 분석이 핵심이기 때문에 다양한 소스에서의 정보수집, 분석 및 탐지, 대응, 모니터링 및 감사 기능이 이뤄져야 한다. 정보수집은 이용자의 정보 및 행위에 대한 정보 수집으로 이용자 매체환경 정보와 사고 유형 정보의 수집 기능을 의미한다. 분석 및 탐지 기능은 수집된 정보를 통해 이상 행위에 대한 분석으로 이용자 유형별, 거래 유형별 다양한 상관관계 분석 및 패턴을 검사해 이상 행위를 탐지하는 기능이다. 대응 기능은 이상 행위로 판단되었을 때 거래를 차단하거나 추가 인증을 요구하여 부당 거래를 방지하는 등의 기능이다. 모니터링 및 감사 기능은 정보수집, 분석 및 탐지, 대응 등의 모든 종합적인 절차를 통합해

24 다중요소 인증(multi-factor authentication)란 2가지 이상의 인증요소로 인증하는 방식을 이용하여 사용자의 신원을 확인하는 과정을 의미하며 사용자 인증 방식에는 사용자가 특별한 정보를 알고 있는지를 확인하는 지식요소(지식기반), 사용자가 특별한 하드웨어를 가지고 있는 확인하는 소유요소(소유기반), 사용자가 생체적으로 특별한 특성을 보유하고 있는지를 확인하는 내재요소(생체기반) 등이 있다.

25 http://www.whitehouse.gov/the-press-office/2015/02/13/

관리하고 탐지시스템을 침해하는 다양한 유형에 대한 감사기능을 의미한다. 문제는 기존의 FDS는 사후결제와 오프라인 거래에 중점을 뒀다면 간편결제에서는 사전예방과 전자상거래까지 범위를 넓혀 부정거래를 추적할 수 있어야 한다. 오픈된 쇼핑몰의 경우 해당 고객의 DB정보가 없기 때문에 이용자 본인의 PC나 모바일 기기에 거래이력을 확인할 수 있는 아무런 보안솔루션도 깔지 않고도 거래 추적이 가능할 수 있는 기술이 필요하다. 따라서 최근 메모리해킹, 텔레뱅킹 사고 등 지능적 금융사기, 결제인증 간소화 등으로 인해 금융 데이터 분석기술과 함께 한국형 FDS 도입 확대 및 기술 고도화가 필요하다. FDS을 우회하거나 복제 단말 사용, 사용자 단말기 권할 탈취 등 FDS가 탐지하기 어려운 새로운 위협에 어떻게 대응할 것인가도 고민해야 한다. 핀테크 활성화를 위해서는 금융정보의 보안성과 시스템의 안정성을 확보할 수 있는 한국형 FDS 개발과 지속적인 보안기술에 대한 투자가 절실히 필요하다.

5) 초연결사회의 사물인터넷(IoT), 모바일 금융보안 위협 대응 기술 개발

다가오는 초연결시대는 PC 서버에서 모바일 사물인터넷으로 전환되고 핀테크로 인해 사물과 금융서비스의 접목이 더욱 활성화 되면서 사물인터넷(IoT), 모바일 금융 보안취약점을 이용한 보안위협이 급속 확산될 것으로 예상된다. 더불어 금융권의 사물인터넷, 모바일 보안기술 활성화를 위해선 보안 플랫폼, 금융보안기술 표준화, 획기적인 인증체계 마련, 생체인증 기술 개발 등이 필요하다.

6) 금융보안 거버넌스 체계 구축, 취약점 분석 · 평가 등 사전 예방 활동 강화

금융위원회의 발표에 의하면 보안규제의 방식을 선진형 규제 방식인 사전 규제 최소화와 사후점검 강화로 개선할 계획이다. 핀테크가 활성화 되도록 보안에 대해서 시장의 자율성을 높여주되, 대신 책임은 엄격하게 묻겠다는 뜻이다. 그간 보호대상으로 정보자산인 시스템, 네트워크, DB, 보안시스템 등 IT 분야로 한정돼 있었다면, 이제는 전사적, 서비스 전체가 대상으로 확대 되며, IT부서 직원, 보안담당자 등이 해야 하는 일에서 전부서 전직원의 필수 업무로 바뀌고 있다.

이제는 금융보안을 강화하기 위해 보안을 바라보는 패러다임의 전환이 필요하며, 이를 위해 전사 차원에서 “보안 전략”을 자율적으로 수립하고 촘촘하고 적극적인 실행이 필요하다. 이를 위해 금융보안 거버넌스 체계 구축, 사전 예방 차원의 위험평가 활동이 중요한 요소이

며 취약점 분석 · 평가 강화, 정보보호 관리체계(ISMS)[26] 구축, PCI-DSS 보안표준 준수 등 선제적 사전 예방 활동이 필요하다. 이를 위해서는 금융사, 제조사, 플랫폼사, 통신사, 개발업체 등 관련 구성 주체의 유기적 협력을 통해 보안거버넌스 체계를 구축해야 한다.

Ⅴ. 핀테크가 정보보호산업에 미치는 영향

앞에서 살펴본바와 같이 금융과 IT기술의 융합인 핀테크는 국내 정보보호산업에 미치는 영향은 상당할 것이 틀림없다. 금융권의 핀테크 전문 보안업체 인수가 가능하고 전자결제 시장에서 공인인증서의 아성이 무너지면서 이미 많은 간편결제 서비스가 출시되고 있다. 많은 핀테크 보안 업체들이 출현하면서 기존 공인인증시장은 점진적으로 축소될 것이다. 이제는 금융관련 보안기술 개발과 확보가 금융시장에서 글로벌 경쟁력을 확보하고 생존과도 마찬가지가 될 것이다. 더욱이 인터넷전문은행 출현은 핀테크 보안업체들의 치열한 경쟁 촉발로 다양한 보안제품 출시 등 금융보안서비스의 양적 · 질적으로 많은 성장을 하게 될 것이다. 그러나 정보보호 업체의 대형화, 글로벌 경쟁력 확보 등 정보보호산업 활성화의 절호의 기회이면서 해외 핀테크 보안 기업의 국내 진출로 인한 절박한 위기를 맞고 있다. 핀테크로 인한 국내 정보보호산업에 미치는 영향을 살펴보면 다음과 같은 것들이 나타날 것이다.

1) 보안 규제 방식 개선에 따른 정보보호 시장 활성화

지식정보보안산업협회(KISIA)가 관련 산업현황을 수집 · 분석한 '2013년 국내 정보보호산업 실태조사'에 따르면 국내 정보보호 관련 기업체는 비상장 기업이 577개(93.4%), 코스닥 기업이 35개(5.7%), 거래소 기업이 6개(1.0%)인 것으로 조사되었다. 2013년 정보보호산업의 매출은 총 7,145,444백만원으로 2012년 대비 14.5% 증가한 것으로 조사되었다. 이 중, 정보보안 매출은 2012년 1,577,587백만원에서 2013년 1,616,761백만원으로 2.5% 증가하였으며, 물리보안 매출은 2012년 4,662,041백만원에서 2013년 5,528,683백만원으로 18.6% 증가하였다.

26 정보보호 관리체계(ISMS, Information Security Management System) : 조직에서 비즈니스의 연속성 확보를 위하여 각종 위협으로부터 정보자산을 보호하기 위한 위험관리 기반의 체계적이고 지속적인 프로세스 개선 활동으로 국내는 "정보통신망법"의 ISMS 인증과 국제 표준인 ISO/IEC 27001 인증이 대표적이다.

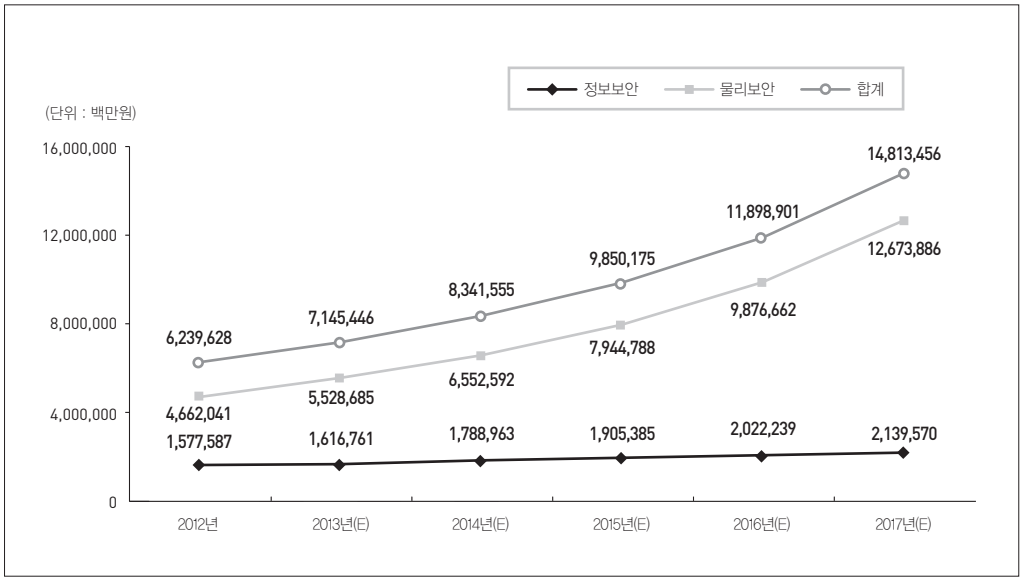
〈표 9〉 정보보호산업 매출 현황

(단위 : 100만원 / %)

구분	정보보안		물리보안		합계	
	2012	2013(E)	2012	2013(E)	2012	2013(E)
매출액	1,577,587	1,616,761	4,662,041	5,528,683	6,239,628	7,145,444
성장률	2.5		18.6		14.5	

※ 출처 : 지식정보보안산업협회, 2013 국내 정보보호산업 실태조사, 2013. 12

정보보호산업의 2017년까지 매출전망은, 2012년 매출 6,239,628백만원(정보보안 1,577,587백만원/물리보안 4,662,041백만원)에서 연평균 18.9%(정보보안 6.3%, 물리보안 22.1%)씩 성장하여 2017년도 매출전망은 14,813,456백만원(정보보안 2,139,570백만원, 물리보안 12,673,886백만원)까지 증가할 것으로 예상된다.



[그림 3] 정보보호산업 규모 전망

국내 정보보호산업 규모면에서 정보보안 성장률이 2.5% 수준으로 경기침체와 함께 저성장을 면치 못하고 있다. 2015년을 원년으로 핀테크 산업 활성화 정책과 핀테크 보안의 중요성에 따른 보안투자 확대로 국내 보안시장 매출이 큰 폭으로 증가 할 것으로 예상된다. 보안 전략에 있어서도 금융보안거버넌스 체계 구축, 금융분야 기반시설에 대한 정기적인 취약점 분석 · 평가, ISMS, PCI-DSS 등 선제적 예방 중심으로 패러다임도 변화할 것이다. 금융정

보나 개인정보 유출로 인한 금융보안 강화를 위해 보안시스템 구축뿐만 아니라 정보보호 전담조직 구성, 직원 대상 보안 교육 등의 중요성을 인식하여 정보보호 컨설팅 시장이 확대될 것이다. 이로 인해 보안관리체계의 대표적인 규격인 ISMS, ISO/IEC 27001,[27] PCI-DSS 등 보안 표준의 영향력 확대로 금융권의 관리적, 기술적, 물리적 보호조치 등 정보보호 체계 구축이 강화될 것이다. 다만, 이러한 보안 표준 준수가 최소한의 자발적 기준으로 표준을 준수 하였다고 다양한 보안 위협으로부터 안전을 담보하거나 완벽한 방어를 하는 것이 아님을 인식할 필요가 있다.

규제 완화 정책에 따라 핀테크 기업의 보안에 대한 자율권과 책임은 한층 더 커졌다. 정보유출에 대한 책임 강화로 금융권 스스로 보안체계를 구축하는 환경 조성이 필요하다. 핀테크 시대의 보안은 다양한 매체와 복잡한 연결 구조로 한 부분이 뚫리면 금융시스템 전체로 확산될 가능성이 높기 때문에 금융기관간 정보공유와 해킹기술에 대응할 수 있는 동적인 보안 체계를 갖출 필요가 있다. 금융 S/W 개발과 규제방식을 선진형 규제방식인 사후점검 체계로의 전환으로 지속적이고 동적인 위험평가 활동을 통해 대응력을 높일 수 있도록 금융과 보안을 겸비한 융합전문가인 금융보안전문가 육성 필요성에 대해 본격적으로 논의되어야 한다. 금융보안시스템이 아무리 잘 만들어진다 하더라도 실제 현장에서 금융시스템을 점검하고 보안사고시 철저한 조사를 할 수 있는 전문가가 있어야 효과적인 보안강화가 가능하기 때문이다.

2) 핀테크 보안기술 경쟁에 따른 보안서비스의 파괴적 혁신

기존의 일방적, 획일적으로 제공하던 과거의 보안서비스 행태에서 벗어나 고객이 직접 다양한 선택을 할 수 있도록 혁신적인 맞춤형 보안서비스 제공이 필요하다. 특히 간편결제 방식에 있어 패스워드 인증 방식은 보안 취약점으로 웹환경이나 모바일 환경에서 사용하기에는 한계가 있다. 인증기술의 패러다임은 다양한 모바일 디바이스들의 등장으로 간편하고 안전한 인증기술이 필요하다. 간편하고 보안강도가 높은 인증기술인 음성인식, 지문인식, USIM(Universal Subscriber Identity Module), NFC 기반의 디바이스 인증기술 등을 기반으로 하는 다양한 하드웨어기반 보안시스템이 출현할 것이다. 또한, 금융 · IT 융합으로 인한 편익과 부작용은 나타날 것이다. 비대면방식의 확대로 전자금융시에, 개인정보유출 등 방지

27 ISO/IEC 27001 : 정보보호 관리체계(ISMS)에 대한 국제 표준 규격으로 국내는 "정보통신망법"에 따른 ISMS 인증 제도(일정 규모 이상 정보통신서비스기업은 의무화)와 국제적 인증 규격인 ISO/IEC 27001 인증 제도로 이원화 되어 운영중에 있다.

를 위한 금융소비자보호 강화 방안을 마련할 필요가 있다. 핀테크 보안의 치열한 경쟁 촉발로 다양한 보안제품 출시 등 금융보안서비스의 양적 · 질적 업그레이드가 또한 기대된다.

3) 오프라인 및 인터넷에서 핀테크 보안으로 재편, 보안 플랫폼 기업 등장

스마트폰 보급과 ICT 기술의 발전으로 금융보안의 중심이 기존 오프라인 및 인터넷에서 모바일 금융보안으로 급속히 재편이 예상된다. 따라서 사물인터넷, 빅 데이터 및 데이터마이닝, FDS, 다중 요소 인증기술 등 신규 핀테크 보안기술이 출현할 것이다. 핀테크 보안 시스템이 제대로 작동되기 위해서는 핀테크에 참여하는 모든 기업들이 핀테크 보안 시스템을 이해하고 협력할 필요가 있다. 일부 참여 기업의 보안 취약점으로 모든 핀테크 시스템에 영향을 미치기 때문에 참여 기업 모두 핀테크 보안 시스템의 적용을 받아야 한다. 핀테크 시대에는 오프라인 및 인터넷에서 핀테크 보안으로 재편될 것이다.

또한 보안서비스를 비즈니스 플랫폼으로 하는 보안 또는 빅데이터 플랫폼 기업이 탄생할 것이다. 구글이나 애플 등 세계적 기업들의 공통점은 바로 플랫폼을 기반으로 성장한 기업들이다. 구글은 원래 검색 업체였지만 구글 안드로이드 기반으로 여러 휴대폰 제조 회사와 연합하고 이에 해당하는 여러 웹들을 사용자가 이용할 수 있게 하였다. 애플도 아이폰, 아이패드가 하나의 iOS로 구동되고 앱들은 모두 연결되어 애플 한 제품을 사면 결국 이에 연동된 앱과 기기에서 자유로울 수 없다. 이렇게 구글과 애플은 OS 플랫폼 공급자의 역할을 하고 있는 동시에 플랫폼 공급자와 이용자를 연결, 매개하는 광의의 플랫폼을 형성하고 있는 것이다.

핀테크는 다양하고 복잡한 연결 구조로 여러 보안 업체 기술들이 적용되기 때문에 단일화된 보안 플랫폼으로 융합된 기술이나 서비스가 필요하다. 즉 플랫폼이란 정거장은 특정한 장소로 가기 위해 반드시 이용자가 타고 내려야 할 운송 수단이 필요하다. 보안 플랫폼은 바로 이용자와 운송 수단이 만나는 접점 또는 통신사, PG사, 금융사, 기기 제조사, 보안업체 등 다양한 주체들이 만나는 매개 지점의 역할을 한다고 볼 수 있다. 이러한 플랫폼의 중요성이 날로 높아지기 때문에 핀테크 보안 업체는 생존 전략으로 핵심 역량과 가치를 높일 수 있는 보안 플랫폼 구축 전략에 집중해야 한다.

4) 금융권, ICT 업체, 정보보호 업체 등 합종연횡 촉발 및 투자 확대

핀테크 시장은 경쟁과 협력이 엇갈리는 복잡한 구조로 합종연횡이 촉발할 것이다. 최근 삼성전자의 루프페이 인수, 엘로모바일의 JTNet 인수, BBVA의 심플 인수, 캐피털 원의 IGN

다이렉트 인수와 핀테크 관련 제조사, 플랫폼사, 통신사, 보안업체간 MOU나 M&A 등 많은 기업들이 발 빠르게 움직이고 있다. 액센츄어 분석에 따르면 2020년에 오프라인 은행의 시장점유율은 35% 이상 축소되고 은행 간 인수합병도 2020년까지 북미 지역 은행의 15~25%에 해당하는 7,000여개 은행이 인수합병으로 사라질 것으로 내다봤다. 핀테크라는 새로운 먹거리를 창출하고 생존하기 위해서는 기술 우위의 핀테크 기업을 금융권이나 관련 기업이 인수 · 합병하게 될 것이다. 새로운 핀테크 생태계가 형성될 것이나 정보보호기업 측면에서는 위기이자 기회가 될 것이다. 또한 공인인증서 기반 업체들의 신규 보안 사업 진출 등 간편결제 시장의 재편이 필연적으로 일어나고 국내 정보보호 업체의 대형화, 글로벌화 진입을 목표로 혁신적인 아이디어와 기술력으로 무장한 핀테크 보안 스타트업 기업들의 대거 출현할 것이다.

국내 핀테크 산업 육성 방안에 따라 정보보호 스타트업도 정부뿐만 아니라 민간 금융기관, ICT 대기업의 직접적인 투자와 지원이 확대될 것이다. 정보보호 산업 육성차원에서라도 유망한 정보보호 스타트업을 창업단계부터 조기 발굴하여 육성하기 위한 투자와 지원이 필요하다. 핀테크 보안 기업의 초기 투자 단계부터 행정 · 법률자문, 외부 투자자 유치, 금융기관이나 ICT 대기업과의 제휴, 저작권 등의 서비스를 종합적으로 제공하는 프로그램이 필요하다.

〈표 10〉 글로벌 은행의 핀테크 기업 육성방안

국가	은행	육성방안
영국	HSBC	• 리테일뱅킹 부문 핀테크 기업에 투자하는 2억달러 규모의 펀드 조성('14.5)
	Barclays	• 유망 핀테크 기업에 대해 최고 5만달러 투자하고 창업지원서비스를 제공하는 핀테크 기업 육성 프로그램 'Barclays Accelerator' 운영 중('14.5)
미국	Wells Fargo	• 유망 핀테크 기업에 대해 최저 5만달러에서 최고 50만달러까지 투자하고 창업지원서비스를 제공하는 핀테크 기업 육성 프로그램을 운영 중('14.8)
	Citi	• 2014년 한해 동안 'Citi Ventures'를 통해 유망 핀테크 기업에 총 7천만달러 투자
스위스	UBS	• 유망 핀테크 기업을 선정하여 투자와 창업지원서비스를 제공하는 'Innovation Spaces'라는 Working Group 운영 중('14.5)
스페인	산텐데르	• 런던을 중심으로 핀테크 기업에 투자하는 1억달러 규모의 펀드 조성('14.7)
	BBVA	• 美, 실리콘밸리 중심으로 핀테크 기업에 투자하는 1억달러 규모의 펀드 조성('13.1)

※ 출처 : 우리금융연구소, "국내외 핀테크 산업의 주요 이슈 및 시사점", 2015. 2

5) 해외 핀테크 기업의 국내 진출로 인한 국내 정보보호산업의 위기

국내 핀테크 산업이 뒤처진 상황에서 해외 핀테크 기업이 국내에 진출할 경우 국내 핀테크 산업과 금융시장에 상당한 영향을 미칠 가능성이 많다. 단기적으로는 구글, 아마존, 알리페이, 애플페이 등 해외 핀테크 플랫폼 기업들은 직접적인 국내 시장진입 보다는 국내 PG사 또는 은행들과 제휴하여 국내 송금, 지급결제 시장 진출을 추진하고 있다. 그러나 향후 송금 · 결제시장 진출 뿐만아니라 예금, 대출, 자산관리 등의 금융영역으로 사업을 확대함으로써 국내 금융산업 전반에 상당한 영향을 미칠 가능성이 많다. 특히 우리나라는 인증기술, 금융데이터 분석, 금융소프트웨어, FDS, 보안기술 등 핀테크의 핵심기술이 뒤처져 있는 상황이다. 이러한 기술이 향상되지 않을 경우 결국 국내 핀테크 기업들의 경쟁력 약화로 이어져 시장에서 검증된 기술력과 경험이 많은 해외 핀테크 기업에게 시장 잠식과 종속될 우려가 있다.

최근 국내는 구매 비용, 수수료 등 문제로 해외 직접구매에 나서는 사람들이 많아지면서 페이팔과 같은 해외 원클릭 결제서비스를 선호하는 추세이다. 이러한 추세라면 국내 금융서비스가 개선되지 않을 경우 고객들의 이탈, 시장 점유율 하락, 국내 핀테크 기업의 경쟁력 약화, 해외 핀테크 기업의 국내 시장 잠식, 핀테크 산업 붕괴라는 가상의 시나리오가 발생해선 안 된다는 것이다.

우리나라의 높은 인터넷 이용율, 스마트폰 보급률, 인터넷 뱅킹, 신용카드 등 금융 인프라(ICT) 역량은 전세계적으로 최고 수준이다. 그러나 이러한 인프라를 가지고 경쟁력을 확보하지 못할 경우 해외 기업에게 시장을 내줘야 할 가능성도 있다. 따라서 국내 핀테크 산업을 효과적으로 육성하기 위해서는 규제 완화와 더불어 국내 핀테크 산업, 특히 정보보호산업의 경쟁력을 제고하는데 투자가 보다 확대되고, 핀테크 보안 기업의 자체 경쟁력도 강화되어야 한다. 국내 정보보호산업 측면에서는 그야말로 그동안 겪어보지 못한 최대 위기이자 기회이다.

Ⅵ. 시사점

미국, 유럽, 중국 등 국가들은 핀테크 산업이 이미 본격화 단계에 접어들었다. 이러한 글로벌 핀테크 산업 성장세와 달리 우리나라는 지급결제 영역에서 초기 단계가 진행되고 있을 뿐 송금, 예금, 대출, 투자자문, 정보보호 등 영역에서는 이제 걸음마 단계에 그치고 있는 상황이다. 핀테크가 정보보호산업 측면에서는 새로운 블루오션이다. 그러나 대기업부터 스타트

업까지 비교적 진입장벽이 낮은 모바일 결제 및 송금 분야로 몰리면서 자칫 과열경쟁양상마저 보이고 있다. 보안업체 입장에서는 생존경쟁에 내몰린셈이다. 국내 핀테크 보안 업체가 이러한 시장논리에 살아남기 위해서는 틈새시장을 찾아 철저한 시장분석과 연구개발에 집중하여 차별화된 제품 및 서비스개발이 중요하다. 또한 보안 업체들의 혁신적인 기술 개발과 함께 금융업체와의 협력관계를 통해 경쟁력 제고 노력도 선행되어야 한다.

결국 핀테크가 국내 정보보호산업 전반에 상당한 영향을 미칠 것은 분명하다. 핀테크 산업이 효과적이고 균형적으로 발전하기 위해서는 정보보호 기업에 대한 투자가 확대되야 한다. 외국의 사례처럼 핀테크 산업 육성의 원동력은 정부의 적극적인 투자와 지원방안이다. 특히 유망 핀테크 보안기업, 정보보호 스타트업을 선정해 투자하고 금융권 등과 제휴할 수 있도록 적극 지원을 해야 한다. 아울러 금융권이나 민간 대기업이 유망 보안 스타트업에 투자할 수 있도록 지원하고 규제 완화와 관련 업체간 협업을 촉진하여 경쟁력을 키우고 자생력을 갖출 수 있도록 환경을 조성해야 한다.

핀테크 산업이 성공하기 위해서는 각종 규제 개선은 두말할 필요가 없다. 핀테크 성공의 핵심은 본질적으로 각각의 디테일에서 보안문제와 규제완화에 있다. 그러나 글로벌 핀테크 산업을 빠르게 성장시키는 데만 집중한 나머지 금융 서비스의 가장 기본 원칙인 보안성이 훼손된 채로 서비스가 제공됐을 때 그로 인해 발생할 수 있는 피해는 핀테크 산업이 고도화할수록 그 규모도 커질 수밖에 없다. 금융서비스의 편의성과 보안은 불가분의 관계로 보안과 편리함의 균형을 잃어서는 안 된다. 따라서 규제 완화와 보안 강화와의 적절한 조합이 될 수 있도록 기술과 인간이 조화를 이루듯이 국민적 합의점을 찾아야 한다.

우리나라는 금융 인프라는 IT 위상에 걸맞게 세계적이다. 온라인 뱅킹 등으로 계좌이체가 실시간으로 되는 나라는 흔치 않다. 이렇게 잘 만든 금융 인프라는 핀테크 시장을 꽃피울 좋은 기반이 될 수 있다. 온라인 · 모바일 금융 거래가 전 세계적으로도 가장 활발하며 부가가치통신망(VAN)을 기반으로 한 실시간 금융 거래가 가능하다. 그러나 핀테크가 활성화한 선진국 사례를 그대로 적용할 수 없는 독특한 금융 환경을 가지고 있다. 그렇기 때문에 더욱더 핀테크 산업 발전 과정에서 절대 간과해선 안 되는 부분은 다름 아닌 '보안'이다. 편리하고 간편함을 추구하다가 오히려 금융의 가장 기본 원칙인 보안을 놓치면 핀테크 산업 자체가 무의미하다.

융합, 연결, 협업의 시대에 금융혁신과 함께 정보보호산업도 같이 발전해야 성공할 수 있다. 핀테크 기술의 특성상 완벽한 보안이란 있을 수 없다. 급변하는 ICT 환경과 함께 다양한

새로운 보안 위협들을 막아내는 것은 더더욱 어려울 수 있다. 향후 모든 기기가 인터넷으로 연결되어 상호 소통하는 초연결사회인 사물인터넷(IoT) 시대에 강력한 보안체계를 마련하기 위해서는 지금부터라도 정보보호산업 육성 전략과 국가적 핀테크 보안체계를 구축하려는 패러다임 전환이 필요하다.

참고문헌

금융결제원 금융결제연구소 (2013). "최신 글로벌 지급결제 트렌드 및 시사점"
금융위원회 (2015). "IT · 금융융합 지원방안"
금융위원회 (2014). '전자상거래 결제 간편화 및 Active-X 해결 방안'
금융보안연구원 (2014). "전자지급결제서비스 동향 및 시사점"
동아일보 (2015). '금액-신용도따라 보아수준 차별화… 금융거래 효율성 높여'
미래창조과학부 (2013). "정보보호산업 발전 종합대책"
아시아경제 (2015). '800조 핀테크 세계전… 금융 · IT 스타트업'
아이티투데이 (2015). '애플페이, 美 정부기관서도 사용 확대'
여신금융연구소 (2015). "핀테크의 가치창출 요건 및 시사점"
여신금융협회 (2014). "간편결제서비스 확대에 따른 환경변화 요인 점검"
여신금융협회 (2014). "미국 카드보안체계에 대한 분석과 시사점"
여신금융협회 (2014). "해외 정보유출 현황과 카드보안"
연합뉴스 (2015). "중국인 지갑은 휴대전화'…작년 모바일 결제 폭증"
우리금융경영연구소 (2014). "국내 핀테크(Fintech) 산업의 현주소와 과제"
우리금융연구소 (2015). "국내외 핀테크 산업의 주요 이슈 및 시사점"
지식정보보안산업협회 (2013). "2013 국내 정보보호산업 실태조사"
통계청 (2015). "2014년 4/4분기 및 연간 온라인쇼핑동향"
통계청 (2014). "2014년 지급수단 이용행태 조사결과 및 시사점"
한국전자통신연구원 (2014). "패스워드 없는 인증기술-FIDO"
한국은행 (2014). "2014년 3/4분기 국내 인터넷뱅킹서비스 이용현황"
한국인터넷진흥원 (2015). "2014년 정보보호 실태조사(기업편)"
KB금융지주경영연구소 (2014). "국내외 핀테크(fintech) 동향과 전망"
KDB산업은행 (2015). "ICT 업계의 금융업 진출에 따른 시장영향 분석"
http://www.israelfintech.com/imageBank/FinTech%20_catalog_26_6_14_1.pdf
http://www.whitehouse.gov/the-press-office/2015/02/13/
World Bank (2012). "Kenya's Mobile Revolution and the Promise of Mobile Savings"