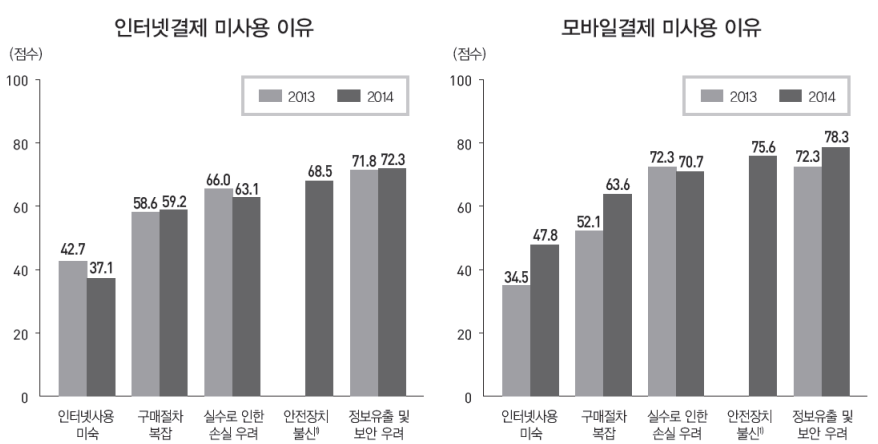
핀테크 서비스 활성화를 고려한 보안대책 제공방안 검토*

김영진·서영준 ((주)드림시큐리티), 박원주 (한국전자통신연구원)

목차

1. 서 론

통계청 조사에 따르면 온라인 결제 이용자들은 정보유출 및 보안에 대한 우려가 가장 큰 것으로 조사되고 있기 때문에 핀테크 등 신규 금융서비스 접근채널을 확대하기 위해서는 최우선적으로 핀테크 산업의 성장을 가능하게 해주는 성장 동력으로서의 핀테크 보안 개발에 중점을 두고 추진해야만 한다.[1,2]



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

(그림 1) 인터넷 및 모바일 결제 미사용 이유

* 이 논문은 2014년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No. R0101-14-308, 인메모리 클라우드기반 실시간 스마트폰 금융사기 대응 기술)

이를 위해 여기에서는 우선, 핀테크 및 보안관련 주요 동향을 살펴보고 이로부터 시사점을 도출할 뿐만 아니라, 핀테크 서비스 및 보안 활성화를 고려한 보안 제공방안을 검토 및 제시한다.

2. 핀테크 및 보안관련 주요 동향

2.1 핀테크 출현 배경

핀테크의 출현은 무엇보다도 스마트폰의 대량 보급과 모바일 전자 금융의 대중화에 기인하고 있다. 국내 스마트폰 가입자 수는 2013년 10월 기준 총 3,632만 명에 도달, 보급률이 67.6%로 세계 1위를 기록, 세계 스마트폰 보급률 14.8%와 비교하여도 4.6배 이상(미국 스트래티직 어낼러시스, 2013.10) 많으며, 2013년 1/4분기 전체 모바일 뱅킹 고객 수는 4,113만 명이고 스마트폰 기반 모바일 뱅킹 등록고객 수는 2,808만명(가입자 중복 허용)으로 모바일 소액 결제 서비스의 경우 이용자 수는 연 1,200만명, 거래액은 연3조원에 육박할 정도로 활성화된 상태이다. 이러한 추세로 인해 2018년경에는 2014년 대비 약6배의 트래픽 증가가 예상되며, 모바일 결제 시장의 경우에도 2017년에는 2011년 대비 약7배의 성장을 예상할 수 있다.

이와 더불어 이러한 ICT 환경의 변화가 사람들 간 대면접촉을 통한 오프라인 중심의 특징을 보인 금융산업을 고객 중성심이나 단골 관계가 아닌 디지털 기술 기반의 산업 형태로 변화하게 만들고 있다.[3]

2.2 핀테크 정의 및 분류

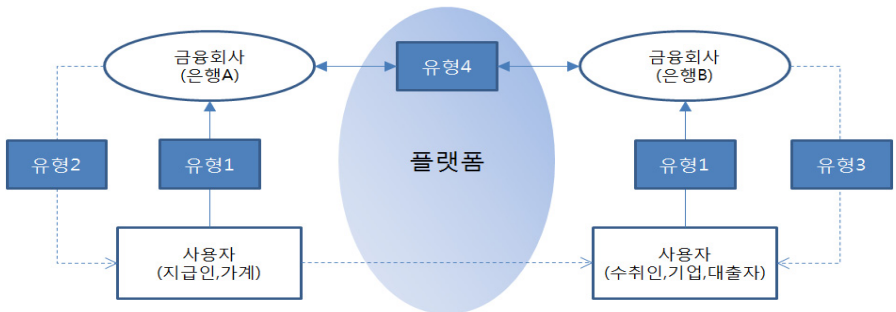
핀테크 기업들은 독창적인 금융 비즈니스 아이디어와 첨단 IT기술을 결합하여 기존의 금융거래 방식을 뛰어넘는 새로운 형태의 다양한 금융사업 모델을 제시

〈표 1〉 핀테크 등장배경

서비스 분류	내용
소비환경의 변화	– 굳이 오프라인 시장에 가거나 PC앞에 앉아 있지 않더라도 손안의 모바일만 이용하면 24시간 동안 언제 어디서나 물품을 구매할 수 있는 환경이 도래하여 모바일 소비시장이 폭발적으로 성장 – 이에 따라 모바일 지급결제, 송금 등 핀테크의 잠재력에 세간의 이목 집중됨
IT 기술혁신	– 모바일 기술 발달과 더불어 대량의 정형, 비정형데이터를 수집 분석할 수 있는 빅데이터 기술의 발전으로 핀테크의 영역은 지급결제를 넘어서 신용분석, 대출, 자산운용에 이르기까지 대폭 확대
금융시장의 성장 한계	– 서브프라임 모기지(비우량 주택 담보대출) 부실 대출과 재정위기 경험, 저금리에 따른 대출 수익 감소 등으로 기존 수익모델에서 눈을 돌려 혁신적인 금융기법을 활용한 수익 모델 창출에 대한 대안으로 핀테크 관심
글로벌 IT기업의 치열한 경쟁	– 글로벌 IT기업들의 치열한 경쟁 때문에 IT와 금융이 결합된 모바일 금융시장이 계속 확장됨 – 글로벌 모바일 금융 시장은 지난 10년간 연15% 이상의 성장세를 보임 – 특히, 중국은 2009~2014년간 불과 5년만에 모바일 전자상거래가 2600억위안에서 2조7,900억위안으로 10배이상 늘어남

〈표 2〉 핀테크 서비스 분류 및 특징

서비스 분류	특징
지급결제	– 이용이 간편하면서도 수수료가 저렴한 지급결제서비스를 제공함으로써 지급결제시장의 진입장벽을 완화 – 대표 서비스 : 페이팔(PayPal), 알리페이(Alipay), 구글월렛(Google Wallet), 애플페이(ApplePay)
금융데이터분석	– 개인과 기업고객이 관련된 다양한 데이터를 수집하여 분석함으로써 새로운 부가가치를 창출 – 대표 서비스 : 어펌(Affirm), 민트닷컴(Mint.com)
송금/전자화폐	– 국제지급결제서비스를 활용한 해외송금, 해외송금서비스 전문업체와 SNS결합을 통한 해외송금, 이동통신사와 금융기관과의 제휴를 통한 해외송금 및 전자화폐 발행을 통한 해외송금 등 실시 – 대표 서비스 : 비트코인(Bitcoin), M-Pesa, 트랜스퍼와이즈(TransferWise)
플랫폼	– 전세계 기업과 고객들이 금융기관의 개입없이 자유롭게 금융거래를 할 수 있는 다양한 거래기반을 제공 – 대표 서비스 : 엔젤리스트(AngelList), 렌딩클럽(LendingClub), 온덱(Ondeck)



(그림 2) 핀테크 업무 영역에 따른 서비스 유형

하고 있다. 핀테크 서비스는 크게 지급결제, 금융데이터 분석, 송금/전자화폐 및 플랫폼으로 구분할 수 있다.[4,5]

핀테크 기술 개발 초창기에는 지급결제 분야에 투자가 집중되어 왔지만, 2008년 이후 지급결제보다는 금융데이터분석 부문에 대한 투자가 늘고 있으며, 앞으로는 기존 은행들의 고유 업무 분야인 금융데이터와 플랫폼 부분의 중요성이 더욱 부각될 것으로 예상된다.[5]

궁극적으로 핀테크 기술 활용을 통해서 제공하고자 하는 서비스 유형은 모든 기능이 융합된 플랫폼 서비스 형태로 활용될 것으로 보이며, 이미 보편화된 서비스로서 유형1의 서비스와 더불어 사용자에게 정보 제공 및 기업들에게 소비 패턴 분석에 따른 맞춤형 서비스 제공을 고려한 유형2와 유형 3의 핀테크 서비스에 덧붙여서 기존 금융기관의 역할에 있어 자동화된 플랫폼이 관여함으로써 온라인지급결제, 자금송금, 자산관리 외의 대출까지도 가능하게 하는 유형 4의 핀테크 서비스로 발달하고 있다.[6]

2.3 핀테크 및 보안 기술 동향

국내의 경우 내부 및 외주직원에 의한 정보복제 등 정보유출 사고가 주를 이루고 있지만, 더불어 최근에는 외부 악성 공격에 의한 신종 전자금융 보안사고도 급증하고 있다. 외부 악성공격의 경우, 악성코드 기술을 활용하여 정보를 탈취하는 방법이 큐싱, 파밍, 스미싱, 메모리해킹 등의 치밀한 악성공격으로 변모하고 있는 추세로 초기의 무작위적 피싱 형태에서 개인정보를 수집하여 보다 정교화된 형태의 공격이 이뤄지고 있어 맞춤형으로 바뀌고 있다 하겠다.

국내의 경우 이러한 공격 양상에 대응하기 위해 이상거래탐지시스템(FDS; Fraud Detection System) 등 서버 단 정보보호대책을 마련하고 있다. 그렇지만, 이러한 이상거래탐지시스템(FDS)은 신용카드사 중심으로 기 도입하여 운용 중이었으며, 은행권과 증권사의 경우 2013년 이후에 구축함으로써 아직까지는 전반적인 활용 수준이 낮다고 할 수 있다. 그러므로, 현재 구축 중인 은행권 및 증권사의 경우에는 안정화 단계까지는 다소 시일이 소요될 것으로 판단된다.

그러나, 해외의 경우에는 사용자의 행위 패턴을 분석하는 방식인 이상거래탐지시스템(FDS)을 활용함으로써 국내의 인증절차(공인인증서, ARS인증, SMS인증 등)보다 인증 절차를 간편하게 해 주면서도 간편한 인증절차의 부족한 부분을 보완하는 형태로 운용하고 있다. 특히, 미국의 경우, 룰 기반의 비정상적 금융거래 행위 탐지모델 도입과 더불어 위치정보와 디바이스 정보까지 활용하는 크로스 채널 탐지를 실시하고 있다.

2.4 핀테크 및 보안 시장 동향

해외에서는 금융기관과 핀테크 기업 간에 상생적 협력 관계를 추구하고 있다. 금융기관은 IT·금융 융합 과정에서 핀테크 기업과 협쟁 관계가 불가피하다. 하지만, 전체 금융산업을 발전시키는 측면에서 건전한 경쟁관계 조성에는 금융기관의 역할이 중요하다. 현재는 소액과 관련한 지급결제, 대출, 송금, 수신 등의 영역은 플랫폼을 보유한 다양한 IT기업과 혁신적인 핀테

〈표 3〉 한국과 핀테크 선진국의 규제 환경 차이

구분	한국	핀테크 선진국
규제원칙	Positive 원칙 – 규제를 일일이 나열, 사전 승인을 받지 않으면 사업 불가	Negative 원칙 – 명시된 규제만 적용, 문제 발생 시 사후 규제
사업등록요건	전자금융업자 등록 시 필요 자본금 10억원~50억원(전자금융거래법)	월 자금 거래 300만 달러 이하면 자본금없이 전자금융업자로 등록
보안인증	– 공인인증서 필요(정부 외에 KISA 등 5개 기관에서 관리->효율성↓ – 금융사고 발생 시 책임주체가 불명확(소비자 책임)	– 핀테크 회사가 모든 책임을 지고 자율적으로 보안 모니터링, 소비자는 별도 보안 프로그램 설치하지 않음 – 금융사고 발생 시 일정기간 동안 회사 전액 보상
금산분리	산업자본의 금융자본 소유 한도 최대 4%	미국 25%, 이탈리아 15%, 일본 20% 등 산업자본의 은행 소유 제한 완화

크 사업자들이 시장을 가져가고 있다.

이와 같은 협업을 위해 금융기관은 API를 공개함으로써 다양한 솔루션 사업자들의 참여를 독려하고 이를 통해 플랫폼화를 추구하는 전략을 추진하고 있으며, 이미 글로벌 금융사들은 스타트업 인수, 경진대회(Hackathons) 등 개방형 협업을 통해 아이디어 확보 및 앱 개발을 추진하고 있다.[7]

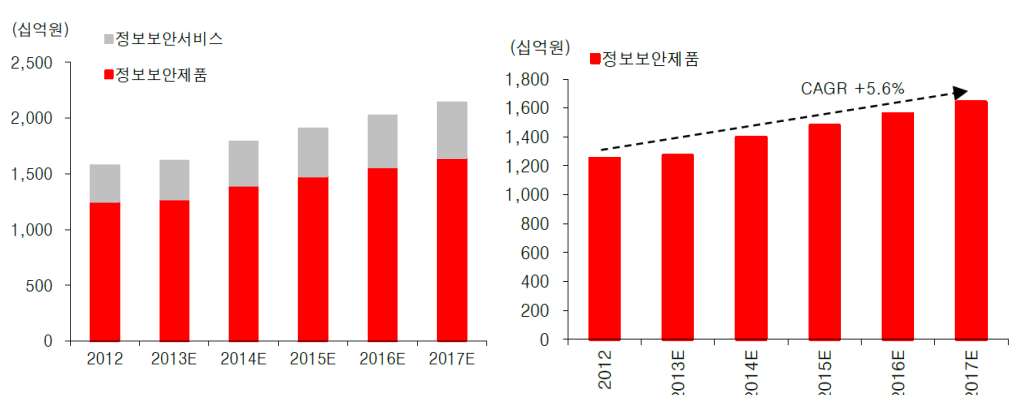
또한, 이에 따른 각 지역별 핀테크 성장률 및 투자 규모는 다음과 같다. 특히, 영국의 경우 핀테크 스타트업의 중심지로 부상 중이며 관련 투자와 인력 및 기술력 있는 업체가 몰리면서 발전속도 측면에서 세계 최고 수준을 유지하고 있다.

국내의 경우에는 불명확하고 포괄적인 규제 및 지나치게 세부적인 기술 지침 등으로 인해 혁신 기술을 활용한 서비스 제공과 핀테크 시장의 진출이 어려운 상황이지만, 핀테크의 진입 장벽을 낮추는 형태로 정책 변화가 진행 중에 있다.

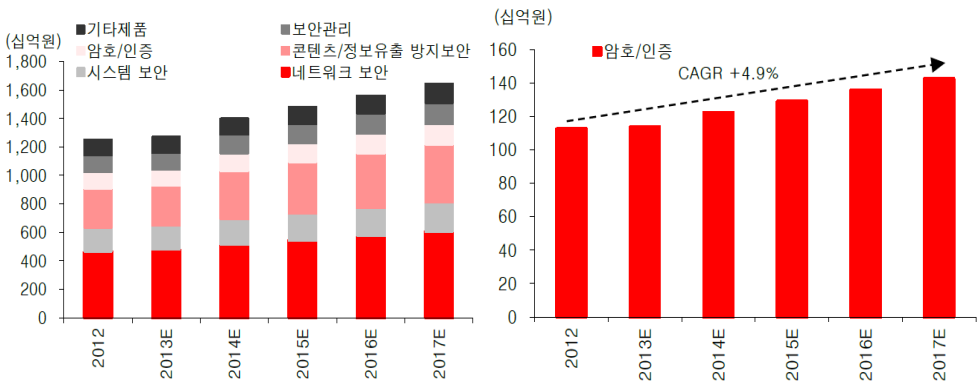
이와 더불어 국내 정보보안산업은 핀테크관련 사업 확대로 시장 확대가 예상되고 있다. 핀테크의 대두로 정보보안산업의 중요성이 커지고 있으며, 최근 핀테크와 관련된 간편결제서비스 확대 등을 중심으로 점차 시장이 확대될 것으로 예상되고 향후에도 이 분야의 지속적인 성장이 전망된다.

정보보안제품 부문 중에서도 개인정보보호 사고 발생 등에 따라 컨텐츠/정보유출 방지 보안제품, 네트워크 보안제품의 수요가 증가한 것으로 분석된다. 또한, 간편결제서비스 등 핀테크 시장 확대로 암호화 및 토큰화 분야의 시장이 확대될 수 있을 것으로 예상되고 있으며, 특히 암호/인증 분야가 예상보다 큰 폭의 성장을 가져갈 수 있을 것으로 보인다.

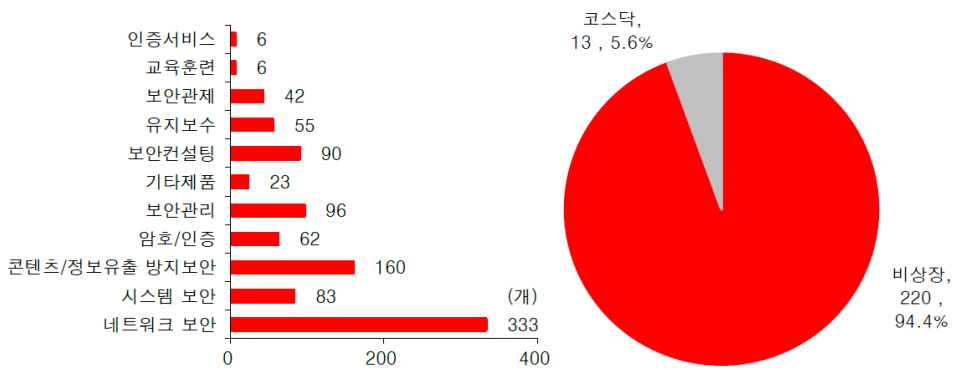
하지만, 시장 확대와 더불어 국내 정보보호산업관련 기업은 점차 증가하고 있으나 대부분 영세한 수준으로 코스닥 및 거래소 상장 기업은 그리 많지 않아, 자금 조달 및 인력 수급에 어려움을 겪고 있는 실정이다.[8]



(그림 3) 국내 정보보안제품 시장규모 및 성장률



(그림 4) 국내 정보보안제품별 시장규모 및 성장률



(그림 5) 국내 정보보안산업 업체 현황

3. 핀테크 및 보안관련 동향 시사점

3.1 핀테크 보안 기술개발 중요성

해외 핀테크 기업이 국내 금융시장에 진출하게 되면 이와 관련한 금융산업의 위축은 충분히 예상할 수 있다고 판단된다. 이러한 해외 핀테크 기업들이 국내 시장 진입이 단기간에 이뤄지기는 어려울 수 있겠지만, 만약 현실화될 경우 국내 금융시장에 상당한 영향을 미칠 것이기 때문이다.

이를 위해, 해외 핀테크 기업들의 경우 다양한 방법으로 국내 진출을 꾀할 수 있을 것이다. 특히, 해외 핀테크 기업들의 경우 송금·결제시장 진출을 통해 고객 접점을 확보하고 이를 기반으로 점차 거래비중을 확대해 갈 것으로 예상되며, 그 후에는 서비스 제공 과정에서 확보된 거래정보를 활용하여 예금, 대출, 자산관리 등의 금융영역으로 사업을 손쉽게 확대할 것으로 예상한다.[5]

우리나라 핀테크 산업의 성장이 부진한 이유로는 법과 규정에 의한 사전 규제와 관련된 환경적 요인이 크다 할 것이다. 이에 반해, 해외에서는 미국 페이팔, 중국 알리페이 등과 같이 국가별 주도 사업자가 글로벌 경쟁에 나서고 있고, 국내는 초기 단계로 통신사, 인터넷 서비스 기업 등이 경쟁적으로 지급결제 서비스를 내놓고는 있으나 아직 뚜렷하게 시장을 주도하는 사업자가 없는 실정이다. 한편으로는 국내의 경우에 이러한 상황을 극복하기 위해서 스마트폰의 높은 보급률, LTE 기술의 확산 등 전 세계적으로도 수준이 높은 한국의 ICT 역량을 활용하여 핀테크 산업을 육성해 갈 필요성이 크다 하겠다.

국내 핀테크 산업의 경쟁력 강화를 대비하기 위해서는 무엇보다도 핀테크의 신뢰(보안)환경을 우선적으로 도입할 필요성이 크다고 판단된다. 신뢰와 안전이 중요한 금융업의 특성 상 '보안'이 중요한 경쟁력이 될 것으로 판단되며, 핀테크 기업들은 '편리함의 효용성'과 '보안성의 강화' 사이의 적절한 트레이드 오프(Trade-off) 관계를 고려해야 할 것이다. 이처럼 핀테크 서비스가 사용하는 데이터와 중요 정보에 대한 보호 및 상호간의 신뢰 확보를 통해 핀테크 서비스의 생태계 조성과 발전의 핵심으로 '보안'이 중요한 역할을 해야 할 것이다. 이와 더불어 다양한 핀테크 서비스를 지원할 수 있도록 핀테크 보안 플랫폼을 핀테크 트러스트 인프라로 활용을 확대한다면 핀테크 거래 시 발생하는 비용을 감소시킴으로서 핀테크 산업의 활성화 및 신뢰 기반의 생태계 조성을 가능하게 할 것이다.

해외에서의 금융과 핀테크 업체 간의 관계 및 발전 형태를 분석했을 때, 초기 핀테크 태동 단계에서 각각의 핀테크 업체들은 각자 보안체계를 구축하고 서비스하였지만, 핀테크 성장 단계를 거쳐 재편 단계에서는 보안체계를 공유하고 연계해가는 형태로 발전하였다.[9]

국내의 경우 이러한 핀테크 재편 단계에서의 금융 및 핀테크 업체 간 운용 모델을 고려하여 개인식별번호관리체계, 서비스 보안수준에 따른 사용자 인증체계 및 데이터 송수신 암복호를 위한 암호키관리체계를 구축하는 것을 목표로 기술 개발을 준비해가는 것이 필요할 것으로 판단된다.

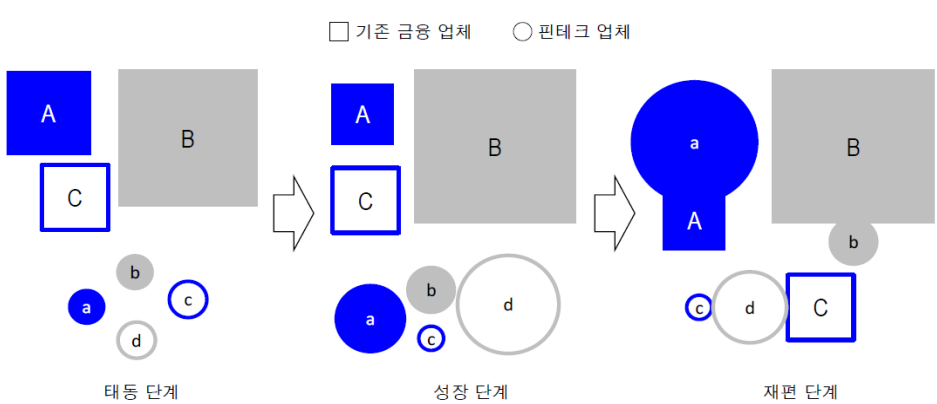
특히, 국내 보안정책에서는 "비밀번호 및 바이오정보를 일방향 암호기술로 암호화해 저장할 것", "주민등록번호 및 계좌정보 등 금융정보를 암호화해서 저장할 것"(이상 정보통신망 시행령), "개인정보처리자가 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 암호화 등 안전성 확보에 필요한 조치를 할 것"(이상 개인정보보호법) 등과 같이 규정하고 있기 때문에, 국내 법·제도에 부합하면서도 창의적인 방법으로 개인식별번호관리체계 및 비대면 거래 본인확인 방안을 제시하는 것이 요구될 것이다.

그리고, 인증수단도 금융거래 중요도(핀테크 서비스, 거래 규모 등)에 따라 사용할 수 있도록 하고, 개인정보관리를 강화함으로써 사용자 편의성 및 보안성을 향상 시킬 수 있도록 고려한 안전한 핀테크 서비스를 제공하도록 하는 것이 중요할 것이다.[10]

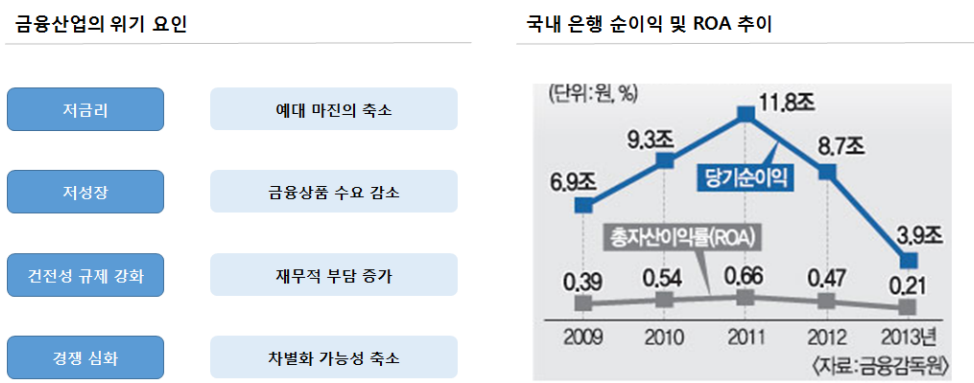
3.2 핀테크 보안 기술개발 파급효과

우선, 금융산업의 위기를 핀테크 활성화를 통해 개선 가능할 것으로 본다. 핀테크 영역에서 새로운 형태의 부가가치 창출을 통해 저금리, 저성장, 건전성 규제 강화 및 경쟁 심화로 침체되고 있는 금융산업의 위기(국내 은행 순이익 등 감소 등)를 극복할 수 있을 것이다.

특히, 대면(영업점 방문 등)을 통한 금융 거래의 패턴(2005년 27%에서 2014년 11.2%까지 하락)에서 CD/ATM 기기, 인터넷 뱅킹 및 텔레뱅킹을 통한 비대



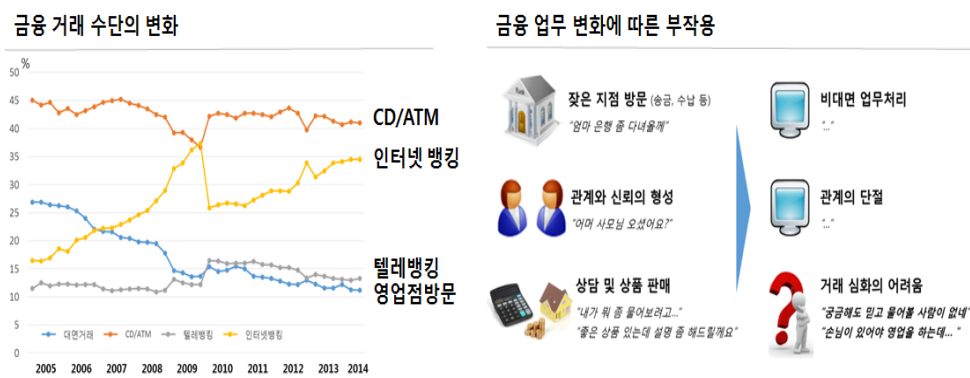
(그림 6) 금융 및 핀테크 업체 간 발전 형태



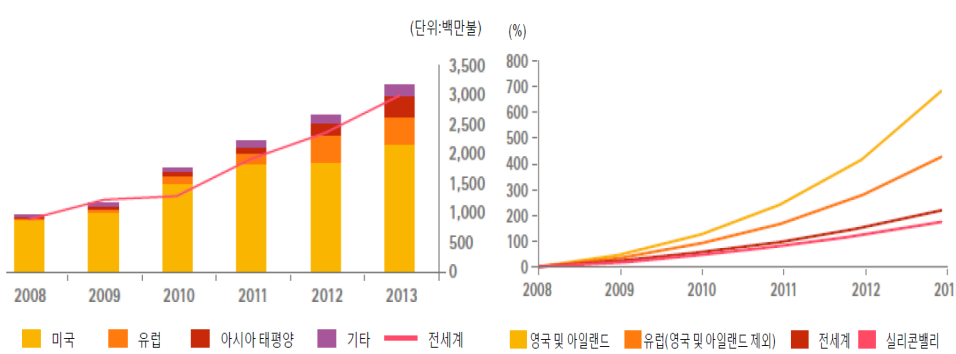
(그림 7) 금융산업의 위기 요인 및 순이익 현황

면을 통한 금융 거래 패턴으로 바뀌는 상황에서 핀테크 서비스를 통해 고객과의 관계를 형성하고 부가가치를 창출하는 활동을 가능하게 할 것이다.[11]

또한, 핀테크 보안에 따른 신뢰성 보장을 통해 서비스를 이용하게 될 수요자들의 안전한 이용환경을 제공할 뿐만 아니라 서비스를 제공하는 업체들 역시 보안에 대한 신뢰성을 확보할 수 있게 해줌으로써 새로운 사업(전 세계적으로 2013년까지 29.7억달러(약3.5조



(그림 8) 금융 거래 수단 변화에 따른 부작용



(그림 9) 전세계 핀테크 투자 규모 및 성장률

원) 규모 투자)을 추진할 수 있게 할 것이다.[12]

하지만, 해외 핀테크 기업들의 송금, 결제시장 진출뿐만 아니라 예금, 대출, 자산관리 등의 금융영역으로 사업을 확대하게 되면, 국내 핀테크 산업이 뒤처진 상황에서 국내 금융시장뿐만 아니라 정보보호산업에도 영향을 크게 미칠 가능성이 커질 수 있다. 왜냐하면, 우리나라는 인증기술, 금융데이터 분석, 이상거래탐지(FDS) 등 핀테크 보안의 핵심기술이 뒤처져 있는 상황이기 때문이다. 이를 극복하기 위한 방안으로 국내 핀테크 기술 개발과 더불어 핀테크 보안관련 핵심 기술 확보에 미리 앞장선다면 해외 핀테크 기업들에게 시장 잠식과 종속될 우려를 줄일 수 있을 것이다.

4. 핀테크 보안 제공방안 검토

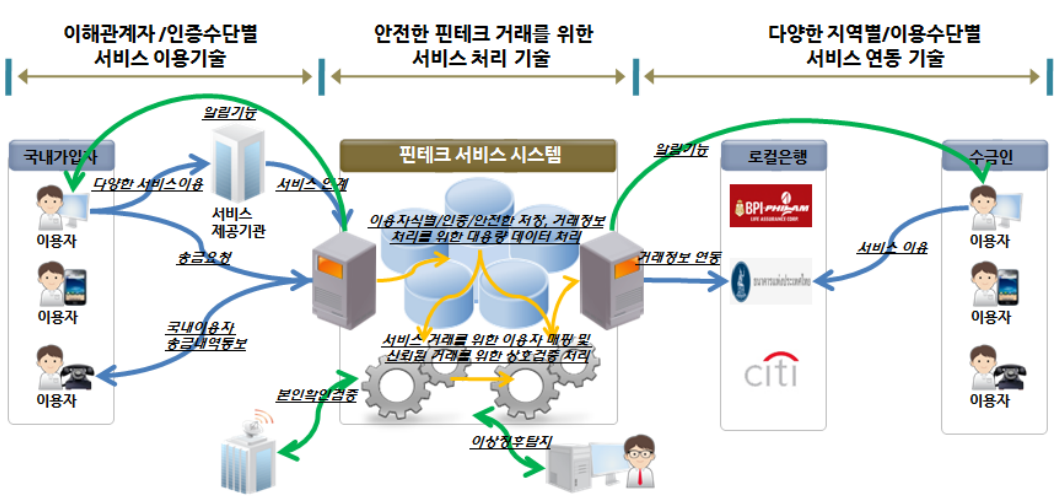
4.1 핀테크 보안 목표

핀테크 보안대책으로 검토해야 할 것은 많겠지만, 우선적으로 핀테크 서비스를 제공하는데 핵심적인 보안 기능이라고 할 수 있고 다양한 핀테크 서비스에서도 사용될 수 있는 공통적인 보안 요소라고 할 수 있는 부분으로 사용자 관리 또는 개인의 신원정보 관리를 검토하고 적용하는 것이 있을 것이다.

특정 서비스를 제공함에 있어서 사용자에 대한 식별 및 인증을 수행하고 그 결과로써 서비스 접근을 허용한다고 하면, 사용자 식별을 위한 고유번호와 패스워드 기반의 사용자 인증 메커니즘을 수행하는 네트워크 시스템 환경에서는 스니퍼 프로그램 등을 이용하여 송수신 데이터를 불법 도청함으로써 쉽게 사용자의 패스워드를 알아낼 수 있기 때문에 이에 따른 보안 대책을 강구하는 것이 필요해지는 것이다.

또한, 핀테크 운용 환경에서 개인의 신원정보를 안전하게 유지 및 관리할 수 있도록 해야지만, 자신의 신분을 증명하고 서비스를 받을 수 있도록 통제가 가능하기 때문에 개인 신원정보 보호를 가능하게 해주는 보안 대책 등도 강구되어야 한다. 특히, 개인의 신원정보를 안전하게 관리하게 해주면서 해당 신원정보를 바탕으로 송수신 데이터 등에 대한 기밀성 및 무결성 제공 대책이 마련된다고 한다면 궁극적인 상호 신뢰형성을 가능하게 할 것이다.

그러므로, 여기에서는 핀테크 보안을 제공하는 방안으로 사용자 프라이버시가 강조되어야 할 대국민 핀테크 서비스 분야에서 개인정보보호 기반의 안전한 서비스 제공이 가능하도록 이용자 고유식별번호 생성, 이용자 연계기능, 개인정보 동의/활용 접근정책 관리 기능 등의 핵심기술들을 묶어서 핀테크 보안 플랫폼으로 특화시켜 제공하는 방안을 제시하고자 한다.



(그림 10) 핀테크 서비스 시스템 기술 개념도

〈표 4〉 핀테크 서비스 처리 단계별 제공 기능

구분	기능 제공 내역
이해관계자/인증수단별 서비스 이용기술	· 이용자 ID기반 처리 기능 · 다양한 인증수단별 연동기능 · 인증수단별 본인확인기관간 연동기능 · 서비스 제공업체와 서비스 제휴를 위한 연동기능
안전한 핀테크 거래를 위한 서비스 처리 기술	· 이용자 고유식별번호 생성, 연계기능 · 이용자ID 기반 관리 기능 · 서비스 토큰 저장 및 운용 기능 · 이용자 사용패턴을 통한 빅데이터 분석/처리 기능 · 이용자 사용패턴을 통한 이상징후 탐지 기능 · 네트워크 분산 클러스터링 DB처리 기능 · 개인정보 동의/활용 접근 정책 관리 기능 · 서비스 거래를 위한 이용자 매핑 기능 · 서비스 거래를 위한 상호검증 기능 · 이용자의 여권을 자동인식하는 기능 · 이용기관별 OPEN API이용을 위한 라이선스 제공 및 검증기능
다양한 지역별/이용수단별 서비스 연동기술	· 로컬은행과 서비스 거래를 위한 데이터 연동 기능

4.2 핀테크 보안 주요 기능

국내의 경우 금융실명거래법 및 개인정보보호법에 의거하여 금융권에서도 주민등록번호 외에 고객관리번호를 기반으로 금융거래처리 실시하고 있으므로 핀테크 서비스 플랫폼에서도 마찬가지로 별도의 고객관리번호로 은행 간 연계 등을 실시할 수 있도록 고려해야 하고, 해당 고객관리번호가 노출되더라도 서비스 접근통제 및 개인신원정보 보호에 문제가 없도록 운용해야 할 것이다. 이러한 보안 대책 제공을 위해 일반적으로 ID관리시스템에 개인식별정보 운용 및 구축방안에 따른 고려사항을 기반으로 시스템 기능 개발 및 제공을 실시해야 한다.

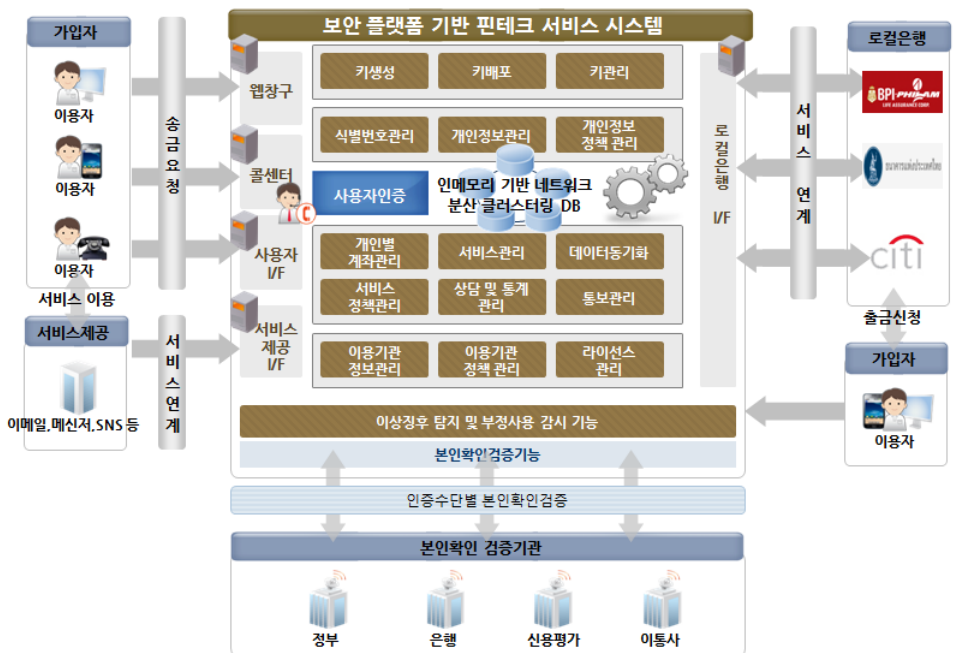
특히, ID관리 및 개인정보보호 기술은 사용자의 편의성과 안전성, 개인정보보호 수준을 높이고 사업자의 관리비용 감소와 시스템 보호 및 조직 간 서비스 연계 등을 지원하는 기술로 핀테크 서비스 플랫폼을 적절히 운용하기 위해 필수적으로 기능이 개발되어야 하는 기술에 해당된다.

이러한 ID관리 및 개인정보보호 기능을 보안 플랫폼화 하고, 이를 기반으로 핀테크 서비스 시스템을 구축할 경우를 고려한 시스템 아키텍처는 다음과 같이 설계할 수 있을 것이다. 여기에서는 한국형 핀테크에 적합한 개인정보 통합관리 기반의 핀테크 서비스 거래 시 보안이 요구되는 이용자 기반의 인증/식별/연계 등 개인정보의 안전한 생성, 저장, 추출, 매핑, 처리 기술 구현 및 검증 등이 제공되도록 하고, 개인정보 통합관리와 연동된 핀테크 서비스 처리 요소기술이 구현되도록 개발한다.

그 밖에도 다양한 핀테크 서비스를 지원하기 위해

〈표 5〉 개인식별정보 운용 방안 및 구축 고려사항

구분	내용
운용 방안	– 개인식별관리체계를 주민등록번호 기반에서 고객관리번호 기반으로 개선 – 계층(Layer)화된 개인식별관리체계로 개인정보 연계 최소화 – 고객관리번호 노출 등 사고 발생 시 고객관리번호 등 교체 실시 – 고객관리번호 기반 개인식별관리체계 운용을 위한 관리번호 역할 구분 (구분 예, 고객고유번호, 고객관리번호 등) – 고객관리번호 생성 및 처리를 위한 고객관리번호생성시스템 등 운용
구축 고려사항	– 고객관리번호 변경에 따른 서비스 운용 영향도 최소화 고려 – 각 이용기관의 외부연계(주민등록번호, 연계관리번호 등) 방안 검토 – 고객관리번호 등 개인정보 유·노출 사고를 대비한 체계 마련 필요



(그림 11) 핀테크 보안 플랫폼 기반의 핀테크 서비스 시스템 아키텍처

ID관리 및 사용자 인증과 관련하여 핀테크 보안 플랫폼이 제공해야 할 기능으로는 다음과 같은 기능들을 제공하는 것으로 설계하는 것이 요구될 것이다.

1)본인확인 기능

- 공인인증서, 아이핀/마이핀, 휴대폰본인인증, 은행 거래계좌인증, 신용카드 인증 등 다양한 인증수단별 연동기술 개발
- 공인인증서, 아이핀/마이핀, 휴대폰본인인증, 은행 거래계좌인증, 신용카드 인증 등 인증수단별 본인확인용 검증 모듈 개발

2)고유식별번호 생성, 연계, 관리 기능

- 서비스 제공을 위한 키생성, 교환, 배포, 이력관리시스템 구축
- 서비스 토큰 통한 다양한 이해관계자간 서비스 운용을 위한 기술 개발
- 대용량 DB를 실시간 처리하기 위한 인메모리 기반 네트워크 분산 클러스터링 DB 구축
- 이용자의 개인정보 공개범위 설정에 따른 동의/활용 접근정책 관리 기술 개발
- 서비스 제공업체, 로컬은행 등의 이용기관 정보 및 정책, 라이선스 관리 기능 개발

3) 서비스 송수신 데이터보호기능

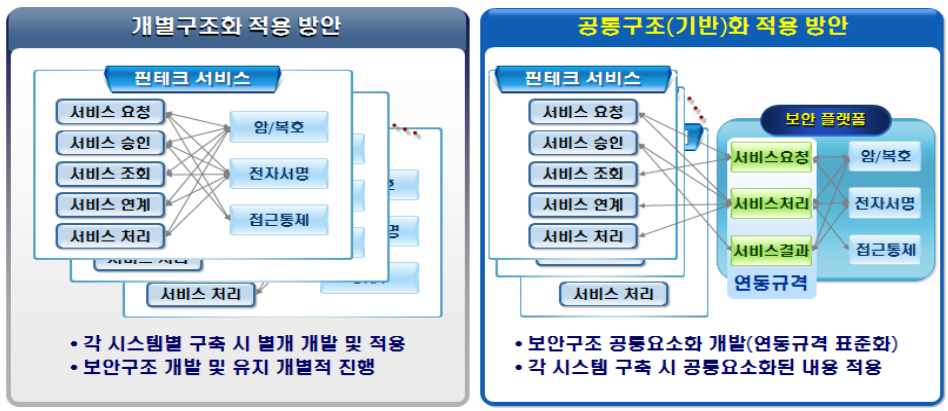
- 서비스 활성화를 위한 서비스제공업체와 서비스 제휴를 위한 연계 모듈 개발 시 서비스 제공업체별 이용자 정보 생성 처리 및 전송구간에 대한 안전한 채널 개발
- 신뢰된 로컬은행과 데이터 동기화를 위한 서비스 연계 모듈 개발시 이용자 정보 생성, 처리 및 전송구간에 대한 안전한 채널 개발
- 이용자정보의 유효성 확인을 위한 인증수단별 본인확인기관과 연동을 위한 유효성 검증기능 개발

3) 이상징후탐지 기능

- 이용자의 사용패턴분석을 빅데이터화 기술 개발
- 이용자 이상징후 발생 시 탐지 및 차단 기술 개발

4.3 핀테크 보안 제공방안

다양한 형태의 핀테크 서비스를 고려했을 때 핀테



(그림 12) 핀테크 서비스 보안 기능 적용 방안

크 서비스 보안 기능을 공통 구조로 만들어 사용할 수 있도록 핀테크 보안 플랫폼 형태로 개발하는 것이 타당할 것이다. 이러한 보안 플랫폼 제공 방안에서는 인증, 암복호, 전자서명 등 공통적인 기능 요소가 각기 다른 핀테크 서비스가 개발될 때마다 서비스별로 반복해서 기능 개발 및 적용하는 것이 아니라 공통 구조화된 보안 플랫폼을 먼저 잘 구성하여 개발한 뒤에 보안 플랫폼 인터페이스, 즉 연동규격을 통해 핀테크 서비스와 핀테크 보안이 연계하도록 구축해 가는 것이 바람직하다 할 것이다.

이를 통해서 핀테크 서비스에 대한 개발과 별개로 보안관련 기능이 각각 개발되고 연동규격을 통해 정합이 이루어짐으로써 개발업체간 협업을 통해 원활하게 핀테크 서비스와 핀테크 보안이 연계되는 효과를 가질 수 있게 할 수 있다.

특히, 핀테크 서비스 개발업체 등이 스타트 업인 업체의 경우, 사용자 규모가 작고 시스템 운용이 쉽지 않다고 하더라도 핀테크 보안 플랫폼을 표준화 또는 규격화된 형태로 관련 업체들에게 클라우드 서비스 방법으로 제공한다면 서비스 개발 및 보안 적용에 따른 비용 부담도 줄일 수 있으면서도 보안 플랫폼 자체의 품질과 성능은 높일 수 있는 형태로 보안 전문업체에 의해 관련 보안기능이 개발되고 융합이 이뤄질 수 있는 기반이 될 수 있을 것이다.

더 나아가 독자적으로 보안 플랫폼 구축이 가능한 핀테크 서비스 업체의 경우에는 독자적으로 보안 플랫폼을 설치할 수 있을 뿐만 아니라, 핀테크 서비스 개발업체에게 API형태로 필요 보안기능만 별개로 공급할 수 있는 형태로도 운용이 가능해질 것이기 때문에 핀테크 서비스의 개발과 핀테크 보안의 개발을 전문화시키면서도 융합이 가능한 형태로 상호간 시너지 효과를 볼 수 있도록 활용이 가능할 것으로 판단한다.

5. 결 론

저금리, 저성장, 건전성 규제 강화 및 경쟁 심화로 침체되고 있는 금융산업의 위기(국내 은행 순이익 등 감소 등)를 극복하기 위해서는 핀테크 활성화를 통해 새로운 형태의 부가가치 창출이 필요한 상태이다. 또한, 대면(영업점 방문 등)을 통한 금융 거래의 패턴에서 비대면을 통한 금융 거래 패턴으로 바뀌는 상황에서 핀테크 서비스를 통해 고객과의 관계를 형성하고 부가가치를 창출하는 활동도 절실히 요구되는 상황이다. 이러한 상황과 더불어 핀테크 서비스에 대한 신뢰성을 보장하기 전에는 새로운 사업으로의 투자를 추진하지 못할 것이기 때문에 핀테크 산업의 성장을 가능하게 해주는 성장 동력으로서의 핀테크 보안 개발에 중점을 두고 추진해야 할 시기라 할 수 있다.

또한, 우리가 핀테크 보안에 대한 투자 및 개발에 힘써야 하는 이유에는 해외 핀테크 기업의 국내 진출로 발생할 수 있는 국내 정보보호산업의 위기 대응 대책이 되기 때문이다. 해외 핀테크 기업들이 국내의 송

금, 결제시장 진출뿐만 아니라 예금, 대출, 자산관리 등의 금융영역으로 사업을 확대하게 되면, 국내 핀테크 산업이 뒤처진 상황에서 국내 금융시장뿐만 아니라 정보보호산업에도 영향을 미칠 가능성이 커질 수 있다. 특히, 우리나라는 인증기술, 금융데이터 분석, 이상거래탐지기술 등 핀테크 보안의 핵심기술이 뒤처져 있는 상황이기 때문에 국내 핀테크 기술 개발과 더불어 핀테크 보안관련 핵심 기술 확보에 미리 앞장설 필요성이 크다 할 것이다. 이를 통해서만이 국내 핀테크 및 보안관련 시장의 종속을 방지할 수 있을 것이다.

그러므로, 핀테크 서비스 적용을 통해 정립된 핀테크 보안 플랫폼을 다양한 핀테크 서비스 제공 시에 활용하도록 뒷받침해주고, 이를 통해 확보한 기술을 바탕으로 IoT, 스마트의료분야, 전기, 수도, 가스등의 국가기반시설 관리 분야에서도 민감한 정보 유출 없이 이용자들의 편리한 삶을 영위 할 수 있는 보안 플랫폼으로서 기반이 되도록 함으로써 신뢰성 있고, 안전한 보안 플랫폼의 역할을 수행하도록 선도적으로 추진해야 할 것이다.

참 고 문 헌

[1] 장상수, “핀테크(Fintech)가 정보보호산업에 미치는 영향에 대한 고찰”, 한국정보보호진흥원, INTERNET & SECURITY FOCUS, 2015년 2월

[2] 황병선, 이순학, “플랫폼 관점에서 본 핀테크”, 한화투자증권, 2015년 2월

[3] 정유신, “핀테크 금융 혁명의 방아쇠 당기다”, 한국경제매거진, 2014년 11월

[4] 박대현, “산업간 융합관점에서 본 핀테크의 시사점”, 한국인터넷진흥원, 2014년 11월

[5] 김종현, “국내외 핀테크(Fintech) 산업의 현주소와 과제”, 우리금융연구소, 2014년 12월

[6] 김미애, “금융과 ICT기술 융합을 위한 무(無)규제 원칙”, 한국경제연구원, KERI Brief, 2015년 3월

[7] 김남훈, “부상하는 Fintech 동향과 IT 및 금융업에 대한 시사점”, 한국정보산업연합회, FKII Issue Report, 2015년 4월

[8] 박종선, 한병화, 윤혁진, “보안에서 본 핀테크, 결제에서 본 핀테크”, 유진투자증권, 2015년 4월

[9] 김지운, “핀테크 2) 해외사례 분석”, 신한금융투자, 신한생각, 2015년 1월

[10] 임석재, “핀테크 보안동향”, TTA Journal, 2015년 3월

[11] 이승건, 양주영, “TOSS 서비스 소개”, 비바리퍼블리카, 2014년 10월

[12] 박세열, “핀테크 해외사례를 통해 본 금융사의 대응과제”, 증권사 CIO 커뮤니티 세미나, 2015년 3월

[13] 고원택, “핀테크(Fintech)의 주요 서비스 및 주요국 동향”, 정보통신기술진흥센터, 주간기술동향, 2015년, 3월

[14] 김종현, “국내외 핀테크 산업의 주요 이슈 및 시사점”, 우리금융경영연구소, 디지에코 보고서, 2015년 2월

저 자 약 력

김 영 진

이메일: yjkim@dreamsecurity.com

- 1989년 중앙대학교 컴퓨터공학과 (공학사)
- 2000년 충남대학교 컴퓨터과학과 (이학석사)
- 2003년 충남대학교 컴퓨터과학과 (이학박사수료)
- 1990년~2000년 국방과학연구소 연구원
- 2000년~2001년 국가보안기술연구소 선임연구원
- 2004년~현재 드림시큐리티 이사
- 관심분야 : 인증프레임워크, 암호프로토콜, 전자서명, 보안토큰, 바이오인식

서 영 준

이메일: dumbman@dreamsecurity.com

- 1996년 동국대학교 경영학 (학사)
- 2000년~2003년 삼익악기(주) 정보전산부 계장
- 2004년~2005년 (주) 보그인터내셔날 전산실 대리
- 2005년~2010년 (주) 도원유비텍 기술연구소 1팀 팀장
- 2010년~현재 드림시큐리티 부장
- 자격사항 : CISSP, CISA, PMP
- 관심분야 : 인증프레임워크, 암호프로토콜, 전자서명, 보안토큰, 바이오인식

박 원 주

이메일: wjpark@etri.re.kr

- 1998년 충남대학교 정보통신공학과 (공학사)
- 2000년 충남대학교 정보통신공학과 (공학석사)
- 2005년 충남대학교 정보통신공학과 (공학박사수료)
- 2000년~현재 한국전자통신연구원 선임연구원
- 관심분야 : 모바일금융보안, 안드로이드악성코드분석, 스마트미디어