11차시. 핀테크와 사이버 보안

01. 핀테크의 이해

4차 산업혁명은 다보스포럼(2016)에서 이슈로 제기된 것처럼 통상 인공지능, 로봇기술, 생명과학 등이 주도하는 혁신적 변화에 기인한다. 산업·기술 간의 포괄적 융합, 네트워크 확장, 인공지능(AI) 발전에 따라서 우리의 생활과 산업 전반에서 지능적 자동화 등의 특징으로 현실화 될 것으로 전망한다. 즉 인공지능, 사물인터넷, 빅데이터 등의 활용을 통해 생산, 유통, 소비 각 분야에 신속 하게 맞춤형 상품과 서비스를 제공할 수 있는 단계가 도래하는 것이다.

금융분야는 4차 산업혁명 논의가 본격화되기 이전부터 ICT·금융간 융합인 핀테크 산업이 전 세계적으로 부상하고 있었다.

핀테크(Fintech)의 개념과 서비스 현황

- **핀테크 개념**

핀테크는 금융(Financial)과 기술(Technology)의 합성어로 IT 기술을 이용하여 기존 금융기법과 차별화된 새로운 형태의 금융서비스 또는 금융 시스템과 서비스를 효율적으로 만드는 기술로 정의된다.

사실 핀테크가 주목받기 전부터 금융권에서는 인터넷 뱅킹이나 온라인 주식거래와 같이 이미 IT기술을 도입해 활용해 왔으나 최근 이슈가가 되고 있는 핀테크가 갖는 차이점은 다음과 같다.

- 서비스 제공 주체: 예전에는 금융회사들이 필요에 따라 IT기술을 주도적으로 채택해 활용해온 반면, 금융분야에서 IT 기술의 중요성이 빠르게 증가함에 따라 고도의 IT 역량을 보유한 비금융회사들이 금융 관련 영역으로 진출하여 영향력을 확대하면 금융 서비스제공주체가 금융회사가 아닌 비금융 IT 회사가 등장하고 있는 점

-제공하는 가치: 핀테크 서비스에 대한 가치 판단은 기존 서비스와 비교하여 단순한 편의성을 넘어 어떠한 부가가치를 새롭게 제공하고 있는지, 특히 편의성과 결합된 경제성 등 소비자 중심의 가치를 구현하고 있는지 여부

- 프로세스: 이러한 제공가치를 구현하기 위해서는 저비용-고효율의 서비스 제공구조가 필요하다는 점에서 IT 기술을 기반으로 하는 프로세스 혁신을 촉진하는 것도 주요한 차이점

다음 표는 서비스 제공주체, 제공하는 가치 및 프로세스 혁신의 관점에서 최근 국내에서도 새롭게 등장한 인터넷전문은행과 기존 은행과의 차이점을 비교한 것이다.

기존 IT기술과 핀테크의 차이점

분야	기존 은행	인터넷 전문은행
인터넷 금융거래	인터넷을 보조적 영업채널로 간주, 조회 및 이체거래 중심	인터넷을 주채널로 영업, 모든 거래가 인터넷을 통해 이루어짐
영업 기반지역	지역 점포를 중심으로 해당지역적 기반을 두고 있는 고객 중심	해당국가 또는 전 세계
영업시간	인터넷뱅킹 조회, 이체를 제외하고 영업시간 제한(09시~16시)	24시간 영업체계를 통한 고객의 시·공간적 접근성 향상
업무범위	금융과 관련한 대부분 업무를 모두 취급	지급결제, 소액대출, 신용카드, 전자화폐 등 업무의 특화 가능

핀테크 개념

핀테크 서비스를 이야기하면 많은 이들이 모바일 기반 지급결제를 떠올리지만, 핀테크 서비스 제공분야는 광범위한 금융업을 모두 포괄하여 현재는 지급결제는 물론 대출, 개인자산관리, 소액투자 등 다양한 분야에서 다수 사업자가 진출해 있다. 특히 IT 기술 적용이 용이하고 고객의 이용 빈도가 높으며 플랫폼사업 성격이 강한 지급결제 분야는 핀테크시장의 활성화를 주도하고 있다.

- 지급결제 (Payment): 상품대금결제, P2P 송금영역에서 기존 지급결제서비스와 차별화된 고객경험을 제공. 상품 및 서비스결제의 편의성 향상은 물론 가상계좌, 신용카드, 실물계좌로 결제 가능
  · 서비스 사례: 페이팔(PayPal), 스퀘어(Square), 알리페이(Alipay), 벤모(Venmore), 카카오페이, 뱅크월렛 카카오, 토스
- 대출(Lending): 개인간 또는 개인과 기업간 대출을 중개하거나 중소기업을 대상으로 대출을 제공하는 서비스
  · 서비스 사례: 랜딩클럽(Lendingclub), 캐비지(Kabbage), 온덱(Ondeck), 어펌(Affirm), 와디즈, 8퍼센트
- 개인자산관리(Personal Finance): 개인의 자금흐름을 통합관리하고 지출계획을 세워주는 서비스제공. 온라인으로 다양한 펀드를 살 수 있는 슈퍼마켓의 역할
  · 서비스 사례: 민트(Mint), 빌가드(Billguard)
- 투자(Investment): 대출, 창업자금 지원 등 투자 관련 금융을 서비스하는 온라인 플랫폼으로 스마트폰 등을 이용하여 투자 정보교류를 통한 가치판단 및 투자활동에 영향. 개인 간 자금조달을 중개해 주는 서비스 제공과 함께 소액투자자 대상의 재무설계, 투자자문 등 자산운용 서비스를 제공
  · 서비스 사례: 넛맥(Nutmeg), 시그피그(Sigfig)
- 뱅킹(Banking): 비금융회사가 인터넷전문은행과 같이 은행업에 진출
  · 케이뱅크(K-bank), 카카오 뱅크(KaKao-bank), 심플(Simple), 지분은행(Jibun bank), 라쿠텐 은행(Rakuten bank), 텐센트(Tencent)
- 해외송금(Remittances): 이메일과 모바일을 통해서 개인과 기업 간 송금을 제공. 기존 화폐는 물론 온라인으로 거래 가능한 가상화폐를 이용하여 낮은 수수료로 국제송금 서비스제공
  · 서비스 사례: 줌(XOOM), 아지모(azimo), 트랜스퍼와이즈(TransferWise)

- 뱅킹인프라(BankingInfra) : 은행의 데이터에 접근하기 위한 API(Application Program Interface)를 제공
  · 서비스 사례: 스탠다드 트레저리(StandardTreasury)

전체적인 트렌드를 보면 한국내에서는 신용카드, 인터넷뱅킹, 모바일뱅킹 등의 발달로 온라인 간편결제, 외환송금, 보안·인증 분야에 관심이 집중되어 있는 상황이지만, 글로벌 차원에서는 데이터 기반 분야에 대한 관심 점증되면서 핀테크 사업영역이 지급결제 영역에서 데이터 분석, 자산관리, 대출, 블록체인 등 고부가가치 영역으로 투자자들의 관심이 확산되고 있다.

주요국의 핀테크 서비스 제공현황

우리나라는 신용카드, 인터넷뱅킹 등 실시간으로 송금·결제가 이루어지고 있지만, 각 국가가 처한 특수성 때문에 즉, 금융 인프라 수준, 상거래 여건, 정부의 정책 방향 등의 차이에 따라 핀테크 산업의 발달 양상이 다르게 나타나고 있다.

미국, 영국 등 주요국은 핀테크 추진에 있어서 자국의 금융 인프라, ICT 발전 등의 환경을 충분히 고려하고 있으며 서비스 영역 또한 결제부터 여수신 업무, 정보보호까지 광범위하게 적용하고 있다. 즉, 전 세계의 핀테크(Fintech) 산업은 금융산업이 발전되고 벤처창업이 활발한 미국과 영국이 주도하고 있다. 최근 들어 이스라엘, 호주, 홍콩, 싱가포르 등도 글로벌 핀테크 산업 활성화에 노력 중에 있다.

특히 영국과 미국 등의 주요 금융회사들은 모바일 등 신규 사업 분야의 경쟁력 확보를 위해 유망 핀테크 기업, 인터넷전문은행과 제휴하거나 인수를 추진하고 있다. 미국의 경우는 시간이 많이 소요되는 특성으로 페이팔 등 결제정보가 노출되지 않는 신속·간편한 결제서비스가 개발되어 활성화 되고 있다. 특히 미국의 페이팔이나 중국의 알리페이는 시장지배력을 가진 유통사업자(이베이, 알리바바)의 독점적인 결제수단으로 사용되면서 크게 활성화 되었다. 미국의 금융그룹 캐피털 원(Capital One)은 네덜란드의 인터넷전문은행인 ING Direct를 인수하여 지점 없이 온라인으로만 영업을 추진하고 있다. 영국의 HSBC와 First Direct, Nationwide 등은 핀테크 기업인 Zapp와 제휴하여 비밀번호 입력만으로 간편하게 모바일 결제가 가능한 좀 더 진화된 금융관련 서비스를 제공하고 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 급성 장했다. 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.

핀테크(Fintech)의 개념과 서비스 현황

핀테크 등장배경

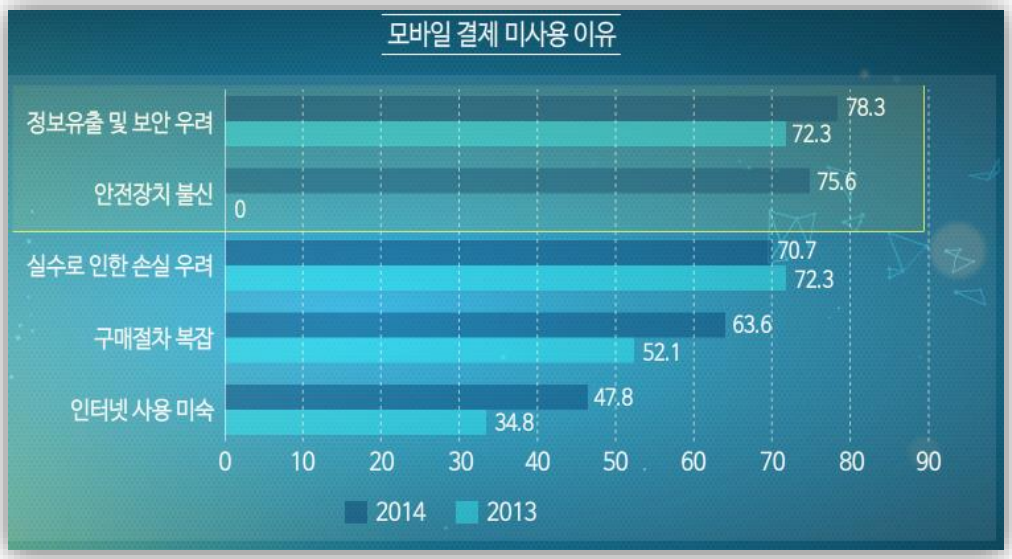
기술 발전과 금융기관의 경쟁력 관점에서 살펴보자.

첫째, 전례 없는 빠른 속도로 보급된 스마트폰을 기반으로 하는 디지털 혁신 환경은 핀테크가 전 세계적으로 부상하게 된 핵심배경이자 성장의 주요 동력이다. 스마트폰을 포함한 모바일 기술혁명은 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 기업(Fintech)의 등장을 불러왔다.

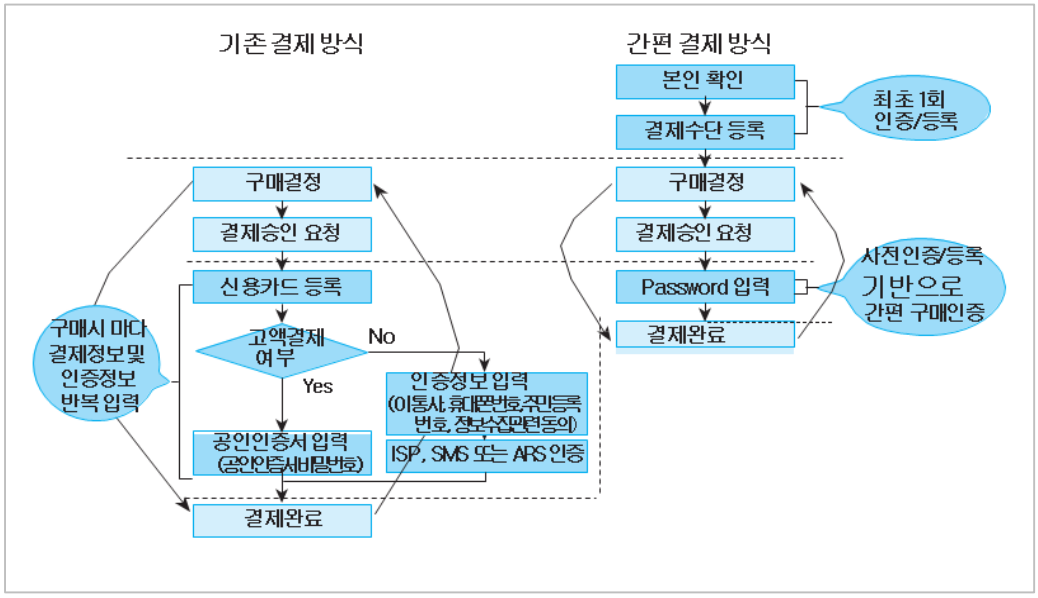
둘째, 금융업은 전통적으로 규제, 규모의 경제, 신뢰도가 경쟁력의 근간을 이루어왔으나 최근 국내 전자지급결제대행사업자(Payment Gateway)에게 카드정보 저장 허용 그리고 미국의 스타트업 양성 및 크라우드펀딩 법적 허용 등과 같은 규제 완화, 지점의 저수익화에 따른 규모의 경제우위 축소, 그리고 금융업의 신뢰도 저하에 따른 탈중개화(Disintermediation) 현상 등으로 경쟁 우위가 희석되면서 위기에 봉착한 금융기관들은 혁신적인 금융기법을 이용하여 새로운 수익모델을 발굴하기 위해 노력하는 과정에서 이에 대한 대안의 하나로 핀테크가 등장하게 되었다.

핀테크 서비스 특징

핀테크가 금융 시장의 혁신을 가져오게 된 배경에는 스마트폰의 보급과 모바일 기술의 발전을 손꼽을 수 있지만, 이를 이용하는 금융소비자는 비대면 금융거래의 안전성에 대해 상당한 우려를 가지고 있다. 한국은행 조사에 따르면 모바일결제를 이용하지 않는 주된 이유가 개인정보 유출 우려(78.3%)와 안전장치에 대한 불신(75.6%)인 것으로 나타났다(아래 그림 참조). 더욱이 핀테크를 통해 금융서비스에 대한 새로운 접근 채널이 확대됨에 따라 개인정보 유출, 해킹 등 보안 사고에 대한 우려는 더욱 커질 것으로 예상된다.



핀테크를 정보보안 관점에서 살펴보면 다음과 같은 특징이 있다.
- 이용자 편의성 제고: 결제단계, 입력되는 정보 그리고 인증방식 등의 간소화를 통해 이용자 편의성 제고를 추구한다. 과거에는 이용 과정의 불편보다는 안전성을 중시해 공인인증서, 일회용 비밀번호, 각종 보안프로그램을 사용하고 거래 시 마다 결제정보 및 인증정보를 입력하도록 하여 사고를 예방해 왔다. 핀테크 서비스의 하나인 간편결제 방식을 살펴보면 온라인 상거래 구매자가 신용카드 정보(카드번호, 유효기간 등), 계좌정보 등의 결제정보를 최초 1회 또는 최소한의 횟수로 입력하고 결제 시에는 패스워드 등의 인증만으로 결제가 완료된다(아래 그림 참조). 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.



기존 결제방식과 간편겨제방식의 비교

(출처: 김종현, "금융권 핀테크 전략과 정보보안 방안", 동아 인포섹 2015-정보보호 콘퍼런스, 2015.2)

- 채널·서비스·기술 간의 다양한 융복합 현상이 발생: 핀테크를 통해 다양한 유형의 비금융기업이 금융업에 진출하여 소비자의 편익을 증가시킬 것으로 예상된다. 하지만, 금융IT와 비 금융IT 기업, 온라인과 오프라인 기업, 모바일기업 간의 융복합이 일어나기 때문에 접점을 증가시키고 새로운 취약점을 발생시키는 원인을 제공할 수 있다. 이는 현실에서 기술적 대응수단을 복잡하게 할 뿐 아니라 전체적 보안수준이 하향하는 현상이 발생하리라는 우려를 낳고 있다.

- 거래과정에서 데이터 공유가 광범위하게 진행: 다양한 핀테크 서비스 제공을 위해서는 고객으로부터 관련 정보의 수집이 확대되고 사업자간의 정보 공유도 증가할 것이므로 고객 정보유출이나 프라이버시 침해사고 가능성도 증가할 것이다. 물론 오래전부터 정보유출이 있었으나 최근 들어서 꾸준히 대량 정보유출 사태가 발생하고 있고, 유출된 정보의 내용으로는 단순 개인정보에 대한 것과 신용카드 정보까지 다양하다. 이러한 개인정보와 신용카드 정보유출은 개인의 정보유출 피해뿐만 아니라 유출된 정보를 이용한 카드 부정사용 가능성 등의 2차 피해는 점차 확산될 것으로 예상된다. 뱅킹분야에서 빅데이터 분석 방법을 사용할 때에는 언제, 어디서, 누구의 개인정보가 수집, 처리, 저장, 이용되는지가 투명해야 하고, 정보주체의 개인정보 노출, 이용 그리고 폐기 여부를 정보주체인 고객이 스스로 결정할 수 있도록 기회를 제공하는 것이 중요하다.

- 정보보안 관련 규제 완화: 핀테크 산업 성장 부진의 원인으로 법과 규정에 의한 사전규제가 지목되는 현 상황에서 산업의 활성화를 추진하는 정부 당국과 지금을 금융업에 진출하는 기회로 인식하는 IT기업들의 요구에 따라 보안성 심의제도 등 정보보안 규제가 완화 또는 폐지되고 있다. 이는 해킹 등 금융사고 발생 가능성을 높여 사업자의 고객 피해 배상액을 증가시키고 사업자별 배상책임 원칙 마련의 필요성을 높이는 역할을 할 것이다.

최근 국내 금융보안 규제 완화 주요 사례

년도	내용	비고
2014.5	공인인증서 사용 의무화 폐지	금융위
2014.7	PG사 카드정보 저장 허용 등 전자상거래 결제 간편화 방안	관계부처합동
2015.1	보안성심의 제도 폐지 등 IT·금융융합 지원방안	금융위
2015.4	실물카드 없는 모바일카드 단독 발급 허용	금융위
2015.5	계좌 개설 시 비대면 실명확인 방식 허용	금융위
2015.6	인터넷 전문은행 도입 방안	금융위

02. 핀테크 보안

핀테크 보안의 이해

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.

핀테크 선진국 보안 체계

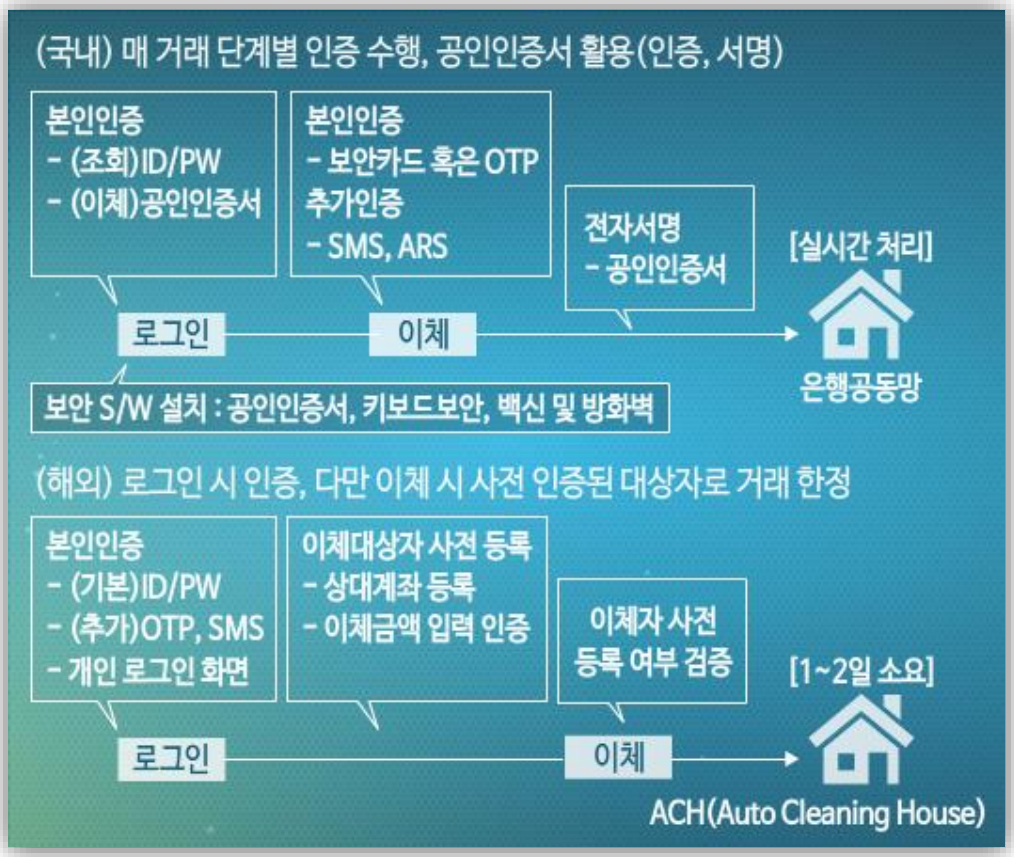
미국, 영국 등 핀테크가 활성화된 국가의 핀테크 보안기술은 고객의 편의를 위해 금융거래를 할 때는 절차상의 보안은 완화하는 대신 사후에 부정·사기 거래를 찾아내고 문제를 걸러내는 사후보안 강화 방식을 쓰고 있다. 이 같은 효율적인 보안수준은 정부가 획일적으로 규제하지 않고 선별적 및 선택적 규제로 민간에서 자율로 정립했기 때문에 가능하였다. 또한 사고 당사자에 대한 무거운 처벌과 보안사고의 책임 분산, 핀테크 기업들의 풍부한 보안 인력과 기술 들이 핀테크 산업 혁신을 이룰 수 있었던 원동력이 되었다고 본다. 주요국의 핀테크 보안 체계를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

주요국 핀테크 보안 체계

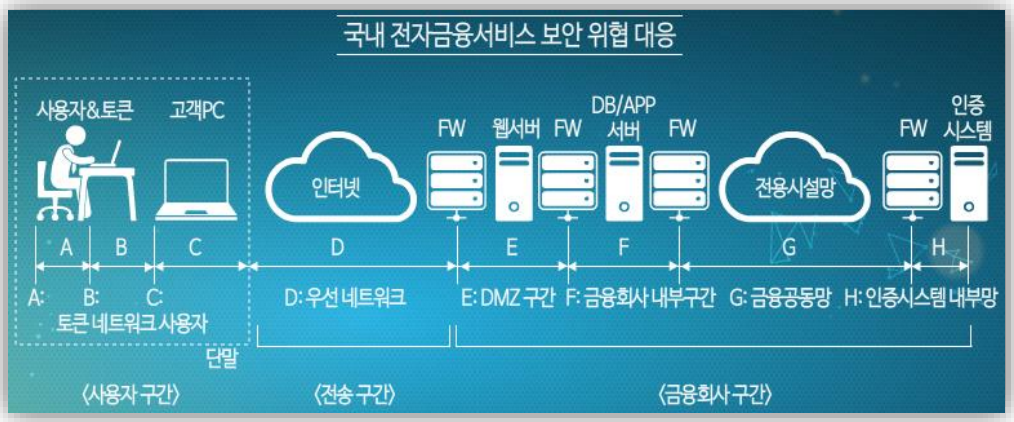
구분	특징
사전 규제 ➡ 사후 보안 강화	소비자 편의를 위해 금융거래 시 보안 절차 완화 대신에 사후에 부정 및 사기거래를 찾아 문제를 해결하는 방식
선별적·선택적 규제	거래 규모/고객 신용도에 따라 보안 강도 차별적 집행: 획일적 보안수준 요구 지양, 소비자에게 보안 수위에 대한 선택권도 부여
사고 당사자 : 무거운 처벌	중대한 보안 사고 기업에 대해서는 천문학적인 과징금을 매기는 등 가중 처벌
민간 자율 규제 체계	민간이 자율적으로 보안 체계를 갖춤 (PCI-DSS 등)
보안사고 책임 분산	전자결제 업체나 IT 기업, 금융소비자에게도 책임을 묻는 방식
핀테크 기업의 인력/기술 활용	검증된 첨단 FDS, 빅데이터 분석기술, 인증기술 등 확보, 풍부한 보안 관련 인력

국내의 보안 체계

국내는 온라인 거래에 대해 오프라인 거래 수준의 보안성 확보를 명분으로 사전적 일률적 규제를 적용하고 있는데, 이 방식은 비교적 낮은 사고발생율과 실시간 처리 등의 장점을 가지고 있으나 인증 프로세스가 복잡하고 특정기술에 의존하여 호환성 및 이용 편의성이 떨어지며 서비스 간 차별성과 기술혁신이 부족한 단점을 가지고 있다(아래 그림 참조).



이러한 국내 금융보안 정책은 결과적으로 아래의 그림과 같이 금융서비스를 보호하기 위한 보안 S/W 및 인증기술들을 사용자구간(A~C)에 집중시키는 결과를 가져왔다. 하지만 편리함 보다 안전함을 강조했던 국내의 경우 카드 부정사용률이 미국이나 영국 등 금융 선진국보다 매우 낮은 수치를 보이고 있지만 '불편한 안전'으로 국내 소비자들을 설득하기에는 한계에 도달한 것은 분명하다.



최근 금융당국이 의무사용을 폐지한 Active-X 기반의 공인인증서와 이용자 단말 보안프로그램은 국내 전자금융거래 보안의 근간으로서 본인확인, 거래의 무결성 보장 및 부인방지, 이용자 단말보호라는 역할을 담당해 왔다. 이들에 대한 의무사용 폐지는 소비자의 편의성 향상과 인증수단을 다양화하는데 기여할 것으로 예상되지만 정보유출에 따른 도용카드 사용 위험을 증가시키고 본인확인 기능의 불명확성으로 인해 금융사고 시 책임소재 문제가 제기될 수 있으며 보안프로그램의 선택적 적용 시 악성 코드 감염, 메모리 해킹 위험성 등을 증가시킬 수 있다. 또한, 해외에서 나타난 공격이 국내 금융거래에서도 곧 바로 발생할 가능성도 현재보다 증가할 것으로 예상된다.

주요 핀테크 기업의 보안 체계

- **애플페이(Applepay)**
  애플페이는 신용카드정보를 스마트폰에 등록 후, 스마트폰만으로 오프라인 가맹점에서 결제를 처리하는 기술 및 시스템으로, 애플페이는 신용카드 수준의 결제편의를 제공하기 위하여 TouchID라는 지문인식 기술과 비접촉 통신 방식인 NFC 기술을 활용하였다.

- **페이팔(PAYPAL)**
  페이팔 가입자는 물품 구매시 추가적 S/W 설치가 불필요하며 페이팔 ID/PW만 입력하면 카드정보 입력이나 본인인증 절차 없이 결제가 가능하다. 즉, 페이팔은 카드번호, 계좌번호 등을 페이팔 ID로 대체하여 송금, 이체를 온라인상에서 처리해주는 서비스이다. 일부 국가에서는 휴대폰 단문문자 메세지(SMS) 또는 OTP(One Time Password)를 통한 추가 인증 절차가 필요하다. 페이팔은 사용자 접속단말에 비 설치형 표준보안기술을 적용하여 이른바 간편결제와 같은 이용편의를 제공하고 상금융거래탐지시스템(Fraud‥Detection‥System)을 통해 보안성을 확보하는 대표 사례라 할 수 있다.

- **알리페이(ALIPAY)**
  알리페이는 신용카드·은행계좌 등을 가상계좌와 연동하여 입·출금, 결제, 송금, 담보거래, 요금납부, 펀드, 보험 등 다양한 금융서비스를 제공하고 있다. 또한 중국이 신용카드 시스템, 지급결제 인프라 등이 미비하고 전자상거래 관련 사기가 빈번하여 결제대금 예치방식(escrow)의 충전식 전자지갑 서비스를 제공하여 중국의 시장을 지배하고 있다.

잠깐!

'에스크로(Escrow)'란?
구매자와 판매자간 신용관계가 불확실할 때 제3자가 상거래가 원활히 이루어질 수 있도록 중계를 하는 매매 보호 서비스이다. 전자상거래의 경우에는 '결제대금 예치'를 의미하며, 거래대금을 제3자에게 맡긴 뒤 물품배송을 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.

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

- **아마존 페이먼츠(AMAZON PAYMENT)**
  아마존 페이먼츠는 아마존 계정에 결제정보(은행계좌, 신용카드)와 배송정보를 연결, ID와 PW만 입력하면 원클릭으로 결제 및 배송 가능하다. 또한 AWS 등을 이용한 초기사업자에게는 일정 매출 발생 시까지 결제 서비스 수수료가 무료이다.

핀테크의 핵심 보안기술 이슈

핀테크는 기존 보수적인 금융업계의 관념을 깨고 IT와 금융의 경계를 무너트리는 혁신적인 변화이다. 핀테크라는 IT·금융 융합 패러다임의 변화는 금융회사가 하지 못하는 일을 대부분 ICT 기업, 플랫폼이나 보안업체의 주도에 의해 가능했다. 더욱이 금융서비스 뿐만 아니라 정보보호 기술에 있어 새로운 패러다임 전환을 의미하는 것이다. 간편하고 편리하고 안전한 금융서비스를 제공하기 위해서는 결국 '보안'을 간과해서는 안 되는 것이다. 즉 핀테크의 가치인 간편하고 편리하고 안전한 금융서비스의 미래는 사람중심의 '보안' 문제에 달려있는 것이다. 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 전환과 밀접한 기술 이슈에 대해 학습한다.

- **공인인증서 등 대체 인증 기반 기술**
  공인인증서는 부인방지 기능 등 우수한 보안 속성으로 인해 국내 금융거래 시 기본 보안수단으로 지난 15년간 사용되어 왔으나, ActiveX 등 비 표준기술로 구현되어 금융거래 편의성을 저해하고 안전한 관리가 어렵다는 지적을 받아 왔다. 공인인증서에 기반한 생태계가 무너지고 다양한 인증 기술의 도입과 더불어 전자금융과 모바일 결제서비스 등 금융시장의 지각 변동이 예고되고 있다. 최근 전자서명 키 위임방지 기술, HTML5 기반, 스마트 카드 기반 등 다양한 공인인증서 기반 기술이 시장에 등장하고 있다. 결제분야는 간편 인증(ARS, SMS)으로 대체 중이며 뱅킹 증권 분야는 서명 기능과 편의성이 더해진 비 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 않을 것이다.

- **빅 데이터 분석 기술 개발 및 활용 기반 마련**
  국내 금융환경에 적합한 '빅데이터 분석 솔루션' 및 '빅데이터 플랫폼' 등 빅데이터 기술개발을 서둘러야 한다. 데이터의 활용 관점으로 보면, 개인정보 보호를 전제로 빅 데이터 분석을 통해 비 식별화된 빅 데이터를 바탕으로 새로운 금융상품 개발, 부가서비스 제공, 마케팅 활용, 금융관련 부정행위 방지, 신용평가, 리스크 관리 등을 위해서는 금융 빅 데이터 분석기술 개발이 절실하다. 결제 정보에 관한 빅 데이터 분석을 통해 선호 업종 지역 등 소비 패턴을 고려한 맞춤형 서비스의 개발이 이용자에 새로운 가치를 제공하기 때문이다. 개인정보 및 금융정보 등 보호를 위한 내부 통제 정책에 있어서도 내부 위협을 감지하고 차단하는 빅 데이터 분석기반 내부통제 시스템도 구축이 필요하다. 또한 빅데이터의 적극적인 활용을 통한 핀테크 산업의 혁신 및 발전을 위해서는 개인정보보호 이슈와 조화로운 추진 방향을 모색해야 할 시점이다.

- **간편결제 수단 개발**
  그동안 안전한 보안기술로 평가 받던 공인인증서가 작년에 규제의 대표적인 예로 지목되면서 다양한 인증 기술, 간편결제 등 지급결제서비스 시장의 판도를 바꾸고 말았다. 핀테크 의 상징을 의미하는 간편결제 방식은 주로 온라인 구매 시 지급결제에 필요한 개인정보와 신용정보를 전달하는 과정을 단순화하여 거래의 편의성을 향상시키는 서비스를 의미한다. 개인정보와 신용정보를 특정 서버에 등록하고 거래 발생 시 설정된 인증수단으로 본인인증을 완료하는 서버형 결제방법을 주로 사용한다. 서버형 결제에는 웹(web) 표준기술이 적용되므로 PC, 스마트폰, 태블릿PC 등 다양한 접근매체를 통해 사용이 가능하다. 전 세계적 대표적인 대형 결제 대행업체(PG: payment gateway)인 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(Fast IDentification On-line) 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.

잠깐!

FIDO(Fast IDentification On-line)
아이디와 비밀번호 조합 대신 지문, 홍채, 얼굴 인식, 목소리, 정맥 등을 활용한 새로운 인증 시스템. 사용자가 잊을래야 잊을 수 없는 생체 정보를 활용. 기존 생체 인증에서 단점으로 지적된 안정성을 확보하기 위해 인증 프로토콜과 인증수단을 분리해 보안과 편리성을 챙겼다.

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) 기술로 변경하기로 하고 American Express, 인텔, 마스터카드 등 기관이 다중 요소 인증 기술 도입을 추진하고 있다.

- **이상거래탐지시스템(FDS: Fraud Detection System) 기술 고도화**

국내의 결제시스템은 사용자단에서 인증 작업 등의 보안절차가 진행되는 반면 해외에서는 대부분 사용자단보다는 서버단에서 보안절차가 이루어진다. 이러한 서버단의 보안 강화를 위해 이상거래 탐지시스템(FDS: Fraud Detection System) 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 일어난 이후 서버단에서 모두 진행된다.

기존의 FDS가 사후결제와 오프라인 거래에 중점을 뒀다면 핀테크의 시대에서의 FDS는 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.

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

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

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