情 報 保 護 學 會 誌
第20卷 第6號, 2010. 12

스마트폰뱅킹 도입에 따른 국내은행의 고객정보보호에 관한 연구
- 스마트폰뱅킹의 법률적 고찰 및 규제환경 변화를 중심으로 -

김 경 민*

요 약

2009년 11월 KT의 애플사의 스마트폰인 아이폰(i-phone)의 국내 도입과 함께 촉발된 국내 스마트폰시장의 확산은 2010년 구글을 중심으로 삼성전자,SKT등 기존 대기업들의 갤럭시폰을 비롯한 안드로이드 OS기반의 스마트폰을 선보이면서 스마트폰 가입자가 2010년 말까지 약 600만명에 이를 것으로 전망된다. 이러한 스마트폰의 확대와 함께 2009년말 기업,하나은행 등 일부 은행들이 처음 스마트폰뱅킹을 시작한 이래 2010년 상반기, 이미 국내 대부분의 시중은행들이 아이폰용 iOS를 비롯한 주요 스마트폰의 OS 플랫폼을 기반으로 한 스마트폰뱅킹 서비스를 제공하고 있다. 그러나 금융산업의 특성상, 금융거래의 신뢰성과 안정성 측면에서의 개인정보보호 및 금융정보보안과 관련한 법규가 채 정비되지 않은 가운데 국내 은행들은 스마트폰뱅킹 출시경쟁에 치중한 나머지 보안 및 개인정보보호에 대한 대책수립은 미흡하며 정부당국의 정보보호관련 지침에 의존, 고객의 자발적인 주의에 호소하고 있는 실정이다. 이처럼 스마트폰뱅킹의 도입이 활발히 진행되면서 금융 서비스 혁신 등 기술적 편의성외에도 개인정보보호를 위한 보안 및 법적 안정성의 중요성이 높아지고 있다. 본 논문은 국내 은행의 스마트폰뱅킹 현황과 고객정보보호 및 관리에 대한 법률적 고찰과 규제환경 변화를 중심으로 국내 은행의 스마트폰뱅킹 도입에 따른 고객정보보호 방안을 제시하고자 한다.

Ⅰ. 서 론

1.1 연구배경 및 목적

1.1.1 연구배경

2009년 11월, KT의 애플사 스마트폰인 아이폰(i-phone)의 국내 도입과 함께 촉발된 국내 스마트폰시장의 확산은 2010년 구글을 중심으로 삼성전자, SKT 등 기존 대기업들의 갤럭시폰을 비롯한 안드로이드 OS 기반의 스마트폰을 선보이면서 스마트폰 가입자가 2010년 말까지 약 600만명에 이를 것으로 전망된다.

이러한 스마트폰의 확대와 함께 2009년말 하나은행과 기업은행이 아이폰 기반의 스마트폰뱅킹을 시작한 이래 2010년 7월말 현재 일부 특수은행을 제외한 16개 금융기관이 스마트폰 뱅킹 서비스를 제공하고 있으며 이중 6개은행[1]은 아이폰(iOS)을 비롯한 안드로이드, 윈도우모바일 등 3대 스마트폰 OS기반의 스마트폰 뱅킹 서비스를 제공하고 있다.

그러나 스마트폰뱅킹 도입 초기 금융감독 당국은 스마트폰 기반 전자금융서비스에 대해 기존 인터넷뱅킹과 유사한 보안수준을 요구하였고 이는 방송통신위원회를 비롯한 정보통신 관련 당국 및 업계와의 쟁점으로 부각되어 논의를 거듭하다 2010년 3월, 30만원 이하의 소액결제시 공인인증서의 사용을 폐지한데 이어 2010년 6월, 금융위원회는「전자금융감독규정」[2]개정을 통해 공인인증서외 이와 동등한 수준의 안정성이 인정되는 인증방법을 사용할 수 있도록 의결 하였다. 한편, 마이크로소프트사의 MS 윈도우기반 OS가 주류인 인터넷뱅킹과 달리 스마트폰의 경우 애플사가 주도하는 아이

1) 국민은행, 신한은행, 우리은행, 하나은행, 외환은행 및 농협 등 6개 은행

2) 제7조(공인인증서의 사용기준), "모든 전자금융거래에 있어「전자서명법」에 의한 공인인증서를 사용하여야 한다."

* 하나은행 신사업추진부 과장 (kyoungminkim@hanabank.com)

폰 기반의 OS가 초기 시장을 주도하면서 기존 온라인 뱅킹시 「전자금융감독규정시행세칙」 제29조에 의거, 의무적으로 적용했던 '보안 4종 셋트'[3]의 적용이 새로운 시스템에 일괄 적용하기 어려웠고 최근 해킹 등에 의한 개인정보 유출의 위험성 등 국내외의 스마트폰 보안성 취약문제가 지속적으로 제기되고 있으나 대부분의 국내 은행들은 스마트폰뱅킹 출시경쟁에 치중한 나머지 보안 및 개인정보보호에 대한 대책수립은 미흡하며 정부당국의 정보보호관련 지침[4]에 의존, 고객의 자발적인 주의에 호소하고 있는 실정이다. 이처럼 스마트폰 뱅킹의 도입이 활발히 진행되면서 금융 서비스 혁신 등 기술적 편의성외에도 개인정보보호를 위한 보안 및 법적 안정성의 중요성이 높아지고 있다.

1.1.2. 연구목적

스마트폰뱅킹 도입초기, 각 은행들은 선점효과를 위해 기존 인터넷뱅킹을 VM방식의 모바일뱅킹으로 구현하던 것을 단순히 화면작업만을 거쳐 서비스 중 일부를 스마트폰의 앱(APP)으로 구현하는 형태가 많아 부가서비스 기능이 미흡했었으나 최근 일부 은행을 중심으로 증강현실, 범프(Bump), QR코드, LBS 등과 같은 스마트폰의 다양한 기술과 다양한 앱을 활용한 결제서비스 개발 등 기술적인 측면에 초점을 맞추어 스마트폰 뱅킹 활성화를 추진하고 있다. 그러나 타 산업과 달리 기술진보성 및 창의성 등 마케팅적 요소와 함께 신뢰성과 안정성 등 리스크관리의 중요도가 높은 금융산업의 특성상 기술적 측면과 함께 엄격한 고객정보보호 및 관리가 필요한 만큼 관련 법규에 대한 사전검토는 물론 도입초기인 스마트폰의 확산에 따른 관련 법규의 개정추이[5] 등에 대한 지속적인 모니터링이 필요하다. 본 논문은 국내 은행의 스마트폰뱅킹 현황과 고객정보보호 및 관리에 대한 법률적 고찰과 규제환경 변화를 중심으로 국내 은행의 스마트폰뱅킹 도입에 따른 고객정보보호 방안을 제시하고자 한다.

1.2 연구방법 및 구성

1.2.1 연구범위 및 방법

본 논문은 '스마트폰뱅킹 도입에 따른 국내 은행의 고객정보보호 연구'를 주제로 국내 은행의 스마트폰 뱅킹 및 관련 법규 현황 및 법규 환경 변화를 중심으로 공간 및 내용범위를 문헌연구를 통해 분석하고자 한다. 또한, 국내 스마트폰뱅킹의 도입시점[6]에 맞추어 2009년 12월부터 2010년 7월까지의 통계자료를 활용하여 해석하고자 한다. 이는 국내 은행의 스마트폰뱅킹 서비스가 초기단계이고 이와 관련한 논문, 보고서 및 언론 등 대외적으로 노출된 사례가 적기 때문이다. 연구방법으로는 기초자료로서 국내외 참고서적, 관련 논문 및 정부간행물, 통계자료 등을 정리 분석하는 사례분석적 연구방법을 사용하고자 한다.

Ⅱ. 국내 은행의 스마트폰뱅킹 현황

2.1 국내은행의 스마트폰뱅킹 현황

2009년 12월, 기업은행과 하나은행이 국내 최초로 아이폰용 OS(iOS)기반의 스마트폰뱅킹 서비스를 출시한데 이어 각 은행들의 다양한 스마트폰뱅킹 서비스 출시가 활발히 진행되면서 2010년 7월말 현재 일부 특수은행을 제외한 16개 은행이 스마트폰뱅킹 서비스를 제공하고 있으며 국민,신한,우리,하나,외환은행과 농협 등 6곳은 스마트폰의 3대 OS기반인 아이폰,윈도우모바일,안드로이드플랫폼을 모두 제공하고 있다. 이외 수협,기업,SC제일,한국씨티은행스마트폰 전자금융서비스는 3개 은행, 6개 증권사 등 9개 금융회사가 제공하고 있으며 스마트폰과 주요 지방은행 등 10곳은 아이폰 및 윈도우모바일OS 기반 서비스를 제공하고 있고 8월~10월중 안드로이드OS기반 서비스를 실시할 예정으로 2010년말 국내의 대부분의 국내 은행이 3대 스마트폰 OS기반 뱅킹서비스를 제공하게 된다. [표 1] 스마트폰뱅킹 서비스를 통한 일평균 이용건수는 2010년 1/4분기 31천건, 2/4분기 224천건, 이용금액은 2010년 1/4분기 27

3) 온라인 금융거래시 적용되는 보안 4종 셋트는 액티브 X기반으로 한 1. 통신 내용 암호화 프로그램 2. 공인인증서 사용을 위한 플러그인, 3. 키보드 해킹 방지 프로그램, 4. 개인방화벽을 말하며 애플의 맥킨토시 등 인터넷익스플로어(IE) 이외의 브라우저로는 인터넷뱅킹을 지원하지 못함.

4) 방송통신위원회, 「이용자 10대 안전수칙」 및 금융감독원, 「스마트폰 전자금융서비스 안전대책」 등.

5) 「전자감독규정」, 「위치정보의 보호 및 이용 등에 관한 법률」 등의 개정 동향

6) 하나은행의 iOS기반 아이폰용 스마트폰뱅킹 출시시점인 2009년 12월

억원, 2/4분기 121억원으로 스마트폰뱅킹이 도입된 2009년 4/4분기 19천건, 6억원에 비해 큰 폭으로 증가하고 있다. 한편, 스마트폰뱅킹 등록고객수는 2010년 1/4분기 93천명, 2/4분기 54만명으로 2009년 4/4분기 13천명에 비해 50배 이상 비약적으로 증가하였다.[7] 2010년 상반기 주요 시중은행의 스마트폰 뱅킹 가입자는 2010년 4월에 서비스를 시작한 우리은행이 17만 9천명으로 가장 많고 2010년 5월에 서비스를 시작한 국민은행이 17만 4천명, 2010년 3월에 서비스를 시작한 신한은행이 12만 5천명의 가입자를 보유하고 있으나 2009년 12월 가장 먼저 서비스를 출시한 하나은행은 7만 5천명으로 스마트폰뱅킹의 선점을 통한 타행 고객유치 효과를 누리지 못한 것으로 분석된다.

2.2 국내 주요 은행의 스마트폰뱅킹 서비스 현황

2009년 12월, 하나은행이 모바일금융협의회를 통한 은행권 스마트폰뱅킹 공동개발[8]이 아닌 독자적 아이폰용 뱅킹 어플리케이션을 출시하면서 각 은행들도 서비스개통을 서두르면서 기존 인터넷뱅킹의 VM방식의 모바일뱅킹 구현형태를 단순하게 화면작업만 거쳐 일부의 서비스만을 스마트폰으로 다시 옮겨 제공하는 형태가 많았고 이에 따른 부가서비스의 부실은 물론 개인정보

〔표 1〕 주요 운영체제별 국내 은행의 스마트폰뱅킹 서비스 현황 (2010.07.현재)

구분	iOS (iPhone)	Android	Window mobile
국민은행	서비스 제공	서비스 제공	서비스 제공
신한은행	서비스 제공	서비스 제공	서비스 제공
우리은행	서비스 제공	서비스 제공	서비스 제공
하나은행	서비스 제공	서비스 제공	서비스 제공
기업은행	서비스 제공	8월 중 출시예정	서비스 제공
SC제일은행	서비스 제공	8월 중 출시예정	서비스 제공
외환은행	서비스 제공	서비스 제공	서비스 제공
한국씨티은행	서비스 제공	8월 중 출시예정	서비스 제공
농협	서비스 제공	서비스 제공	서비스 제공
수협	서비스 제공	8월 중 출시예정	서비스 제공
부산은행	서비스 제공	8월 중 출시예정	서비스 제공
대구은행	서비스 제공	8월 중 출시예정	서비스 제공
광주은행	서비스 제공	10월 중 출시예정	서비스 제공
전북은행	서비스 제공	8월~9월 중 출시예정	서비스 제공
경남은행	서비스 제공	8월 중 출시예정	서비스 제공
제주은행	서비스 제공	8월 중 출시예정	서비스 제공

보호 등의 보안측면에 대한 대응은 미흡했다. 2010년 하반기에는 각 은행들의 안드로이드OS 플랫폼 출시까지 주요 OS별 서비스 제공이 완료됨에 따라 증강현실, LBS(위치정보서비스) 등 다양한 어플리케이션기술을 활용한 서비스 차별화 및 부가서비스의 다양화를 추진하는 어플리케이션 개발과 각 OS별 개발 및 운영에 따른 비용 등의 비효율성을 극복하기 위한 스마트폰에서 운영되는 플랫폼통합(모바일 클라우드)개발의 방향으로 진행되고 있다. 국내 은행 최초로 아이폰용 스마트폰뱅킹을 출시한 하나은행은 기존 인터넷뱅킹의 가계부서비스를 강화한 '하나N뱅크'에 이어 '하나N머니'라는 무료 어플리케이션을 통해 하나SK카드의 카드상품 판매와 인터넷뱅킹 내 'e-플러스클럽'의 쿠폰마케팅을 시행하고 있으며 온라인 마케팅 채널인 '하나N플라자'를 의사전문 커뮤니티인 메디게이트의 어플리케이션 내 컨텐츠 중 일부로 반영, 직접 스마트폰을 통해 대출 및 PB서비스 등 고객의 상품상담신청을 받아 신청영업점에 연계하는 형태의 서비스를 제공하고 있다. 또한 상반기 삼성전자와의 전략적 제휴를 통해 갤럭시-S 출시시 기본 가계부용 어플리케이션으로 '하나N머니'의 탑재와 간접광고 등을 추진하고 있다.

2010년 1월에 서비스를 시작한 기업은행의 'IBK아이폰뱅킹'의 장점은 순수 어플리케이션으로 속도가 빠르고 공인인증서 없이 어플리케이션의 다운로드만으로도 환율조회,이벤트,영업점 조회,상품 등 동영상 확인 서비스를 제공, 편의성과 간편함을 보완하였으며 데이터의 사용량이 적어 비교적 경제적이라는 점과 직관적 사용자 환경(UI)를 제공해 이용이 편리하다.

2010년 3월에 서비스를 시작한 신한은행은 'S뱅크'를 통해 조회이체 등 기본적 업무외에 신한카드,지로납부,외환,펀드 등의 부가서비스를 제공하고 있으며 기존 VM고객도 이용하기 쉬운 직관적이고 편리한 UI를 장점으로 메뉴이동 기능, 메인 메뉴 내 불켜짐 기능 등 재미요소를 가미했다. 또한 2010년 7월부터 증강현실(AR:Augmented Reality) 및 위치기반 (LBS:Location Based Service)의 모바일 쿠폰서비스(신한 S 쿠폰서비스)와 아파트시세 및 대출한도조회 서비스(신한 S 집시

7) 기타자료 〔18〕

8) 2010년 4월부터 국민,신한,하나은행을 제외한 우리,외환,기업,농협,대구,부산,전북,광주,경남은행 등 9개 시중은행이 공동서버구축을 통한 옴니아폰을 통한 스마트폰뱅킹 서비스를 공동으로 개시함.

세(ZipSise)서비스) 등 차별화된 스마트폰 특화서비스를 제공하고 있으며 8월 부터는 전 영업점에 KT 와이파이존(Wi-Fi)을 구축하였다.

외환은행은 2009년 4월 윈도우모바일 기반의 'M뱅크'를 출시하였고 7월 안드로이도 기반 스마트폰뱅킹 서비스를 통해 조회, 이체, 송금 등 기본 뱅킹거래 외에도 스마트 사이버 환전, 모바일 신용카드 서비스의 부가서비스 및 증강현실을 통해 영업점 및 자동화기기 정보를 제공하고 있다. 또한 SKT와의 전략적 제휴를 통해 SKT ICT기술을 활용, 소규모 은행 창구역할을 강화하는 스마트 브랜치 구축, 외환은행 임직원 대상 모바일 오피스 도입, 안드로이드 기반의 스마트폰 뱅킹 개발 및 보급 협력, 스마트 페이먼트(T Smart Pay) 도입협력 등을 단계별로 추진하고 있다.

2009년 4월 서비스를 시작한 우리은행은 통합 플랫폼 구축을 완료하였고 '우리 스마트 뱅킹'을 통해 웹과 앱(어플리케이션)을 적절히 혼용한 하이브리드 뱅킹서비스를 채택, 기존 인터넷뱅킹의 다양한 정보와 업무처리속도가 빠른 스마트폰 앱의 장점을 통해 실제 계좌이체 및 상품가입을 강화하는데 초점을 두고 있으며 금융권에서 처음으로 스마트폰을 통해서만 가입이 가능한 '우리스마트정기예금'을 출시하였고 향후 대출상품 및 PB등 다양한 상품구성을 통해 2010년 30만명, 2011년 120만명의 신규고객 유치를 목표로 하고 있다.

2010년 5월 'KB스타뱅킹'을 시작한 국민은행은 2010년 8월 스마트폰 기반의 생활 밀착형 금융서비스인 'KB스타플러스 서비스'를 출시하여 기존 KB시세정보를 바탕으로 아파트 시세,가계부(포켓북),KB카드 스타샵 및 영업점과 자동화기기 찾기,KB스타뱅킹,KB투자증권으로 구성되어 있으며 무료로 제공되고 있다. 또한 증강현실을 이용하여 스마트폰 카메라로 비쳐지는 화면에서 아파트 시세 또는 매물정보 등 부동산 정보를 상세조회 및 대출가능금액 조회에서 상담서비스까지 제공하고 있다.

Ⅲ. 스마트폰뱅킹의 고객정보보호 관련 법률 현황

3.1 국내 은행의 고객정보보호 관련 법률현황

스마트폰뱅킹과 관련하여 국내 은행에 적용되는 고객정보보호 관련 법률로는 개인정보보호 관련 법률과 금융정보보안 관련 법률로 구분할 수 있다. 먼저 개인정보보호 관련 법률로는 1. 신용정보의 이용 및 보호에 관한 법률 2. 금융실명거래 및 비밀보장에 관한 법률, 3. 특정금융거래정보의 보고 및 이용 등에 관한 법률, 4. 공공기관의 개인정보보호에 관한 법률, 5. 전자상거래 등에서의 소비자 보호에 관한 법률이 있으며 금융정보보안과 관련한 법률로는 1. 전자금융거래법, 2. 전자서명법 및 3. 전자거래기본법, 4. 정보통신망 이용촉진 및 정보보호에 관한 법률 등이 있으며 각 법률에 따른 시행령, 시행규칙, 감독규정, 지침, 관리규약 등으로 법체계를 이루고 있으며 각 개별 금융기관은 관련 법규에 근거한 내부지침 및 관리규정을 수립하여 금융거래에 적용하고 있다. 한편, 스마트폰의 증강현실 및 LBS 기술을 활용하여 각 은행들의 스마트폰뱅킹용 어플리케이션을 통한 영업점 및 자동화기기에 대한 위치정보를 비롯 제휴사 등의 위치정보 제공 서비스가 활성화되면서 각 은행들은 「위치정보의 보호 및 이용 등에 관한 법률」 9)상의 위치정보사업자로서 방송통신위원회를 허가를 받아야 한다. [표 2]

〔표 2〕 국내 은행의 스마트폰뱅킹 관련 고객정보보호 법률 현황

구분	관련 법률
개인정보 보호관련 법률	신용정보의 이용 및 보호에 관한 법률
	금융실명거래 및 비밀보장에 관한 법률
	특정금융거래정보의 보고 및 이용 등에 관한 법률
	공공기관의 개인정보보호에 관한 법률
	전자상거래 등에서의 소비자 보호에 관한 법률
	위치정보의 보호 및 이용 등에 관한 법률
금융정보 보안관련 법률	전자금융거래법
	전자서명법
	전자거래기본법
	정보통신망 이용촉진 및 정보보호에 관한 법률

3.2 개인정보보호관련 법률

3.2.1 신용정보의 이용 및 보호에 관한 법률

「신용정보 이용 및 보호에 관한 법률」은 개인 신용정보의 오,남용으로부터 사생활을 보호하기 위해 제정

9) 동법 제1조,"이 법은 위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하여 위치정보의 이용을 활성화함으로써 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다."

된 법률로 은행을 비롯한 신용정보 관련 기관을 규제한다. 동 법 제15조[10]는 개인신용정보의 적절한 유통을 통해 개인은 본인의 신용도에 맞는 금융거래를 하고 금융기관은 거래 상대방에 대한 신용평가에 따른 적정한 여신이 이루어지는 신용사회를 지향함을 목적으로 한다. 다만, 개인신용정보의 경우 동법 제19조[11] 및 동법에 대한 시행령 제16조[12]에 의해 금융기관 및 신용정보회사 등이 고객의 신용정보보호를 위해 신용정보 전산시스템의 기술적,물리적,관리적 보안대책을 의무적으로 마련하도록 명시하여 안전하게 관리하도록 규정하고 있다.[13]

3.2.2 금융실명거래 및 비밀보장에 관한 법률

「금융실명거래 및 비밀보장에 관한 법률」은 실지명의에 의한 금융거래를 위해 제정된 법률로 국내 은행을 규제하며 동 법 제3조[14] 및 제4조[15] 등에 의해 개인 등의 실명거래 수단에 대해 규정하고 있으며, 금융거래의 비밀보장을 위한 조치사항 등을 명시하고 있다. 또한 총리령 제3조는 동 법, 제3조 3항에 의거 실명거래의 확인방법 및 절차 기타 필요한 사항을 규정하고 있는데, 은행의 실무상, 주민등록증을 원칙으로 하되, 국가기관 또는 지방자치단체,유아교육법,초중등교육법 및 고등교육법에 의한 학교의 장이 발급한 것으로서 성명,주민등록번호가 기재되어 있고 부착된 사진에 의하여 본인임을 확인할 수 있는 증표를 인정[16]하고 있다. 법인의 경우 사업자등록증,고유번호증,사업자등록증명원을 인정하고 있으며 동일 은행 내부에서 원본을 대조,확인(확인영업점 및 확인자 표기)한 사업자등록증(고유번호증 등)사본도 가능[17]하며 임의단체의 경우 납세번호 또는 고유번호가 있는 경우는 납세번호증 또는 고유번호증을 인정하며 납세번호 또는 고유번호가 없는 경우에는 대표자 개인의 실명확인증표를 사용할 수 있다. 한편, 실명확인 생략이 가능한 거래로는 실명이 확인된 계좌에 의한 계속거래[18], 각종 공과금 등의 수납, 100만원이하의 원화 송금(무통장입금 포함)과 100만원이하에 상당하는 외국통화 매입,매각, 다음 각 호[19]의 채권으로서 1997년 12월 31일부터 1998년 12월 31일 사이에 재정경제부장관이 정하는 발행기간, 이자율 및 만기 등의 발행조건으로 발행된 채권의 거래와 보험,공제거래 및 여신거래는 실명거래대상에서 제외한다.[20]

3.2.3 전자상거래 등에서의 소비자보호에 관한 법률

10) 제15조(수집조사의 원칙),"신용정보회사,신용정보집중기관 및 신용정보제공,이용자(이하, "신용정보회사 등"이라 한다)는 신용정보를 수집,조사하는 경우에는 이 법 또는 정관으로 정한 업무 범위에서 수집,조사의 목적을 명확하게 하고 그 목적 달성에 필요한 범위에서 합리적이고 공정한 수단을 사용해야 한다."

11) 제19조(신용정보전산시스템의 안전보호) 제1항,"신용정보회사등은 신용정보전산시스템(제25조 제6항에 따른 신용정보 공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경,훼손 및 파괴, 그 밖에 위험에 대하여 대통령령으로 정하는 바에 따라 기술적,물리적,관리적 보안대책을 세워야 한다."

12) 제16조(기술적,물리적,관리적 보안대책의 수립) 제1항,"법 제19조 제1항에 따라 신용정보회사 등은 신용정보전산시스템의 안전보호를 위하여 다음 각 호의 사항이 포함된 기술적,물리적,관리적 보안대책을 세워야 한다." 1호, "신용정보에 제3자가 불법적으로 접근하는 것을 차단하기 위한 침입차단시스템을 접근통제장치의 설치,운영에 관한 사항, 2호, "신용정보전산시스템에 입력된 정보의 변경,훼손 및 파괴를 방지하기 위한 사항, 3호, "신용정보 취급,조회 권한을 직급별,업무별로 차등 부여하는 데에 관한 사항 및 신용정보조회기록의 주기적인 점검에 관한 사항, 4호, "그 밖에 신용정보의 안정성 확보를 위하여 필요한 사항, 동조 제2항 "금융위원회는 제1항 각 호에 따른 사항의 구체적인 내용을 정하여 고시할 수 있다.

13) 금융보안연구원,2009.11.pp 27.[1]

14) 제3조(금융실명거래) 제1항,"금융기관은 거래자의 실지명의(이하 "실명"이라 한다)에 의하여 금융거래를 하여야 한다.

15) 제4조(금융거래의 비밀보장) 제1항,"금융기관에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 "거래정보등"이라 한다)를 타인에게 제공하거나 누설하여서는 아니되며,누구든지 금융기관에 종사하는 자에게 거래정보등의, 제공을 요구하여서는 아니된다.

16) 단, 실명확인증표의 사본, 유효기간이 지난 실명확인증표, 사원증과 주민등록(등)초본의 경우 실명확인증표로 사용할 수 없다.

17) 단, 개인사업자는 법인이 아니므로 개인의 실명확인증표로 실명확인하여야 하며 사업자등록증을 실명확인증표로 사용 할 수 없다.

18) 실명이 확인된 계좌에 의한 계속거래라 함은 실명확인된 계좌에 의하여 통장,거래카드(현금,직불카드 포함),전자적 수단 등으로 거래하는 경우를 말함.

19) 1. 고용안정과 근로자의 직업능력향상 및 생활안정 등을 위하여 발행되는 대통령령이 정하는 채권, 2. 외국환거래법 제13조의 규정에 의한 외국환평형기금 채권으로서 외국통화로 표시된 채권, 3. 중소기업의 구조조정지원 등을 위하여 발행되는 대통령령이 정하는 채권, 4. 구 증권거래법 제160조의 규정에 의한 증권금융채권

20) 금융보안연구원,2009.11.pp 28.[1]
전국은행연합회,2008.10.pp 7-9.[3]

스마트폰뱅킹에 의한 지급거래는 전자거래기본법 제2조 5호의 규정에 의한 전자거래의 방법으로 상행위를 하는 것이므로 전자상거래에 포함되어 「전자상거래 등에서의 소비자보호에 관한 법률」이 적용된다. 동 법률은 전자상거래 및 통신판매에서 소비자의 권익을 보호하기 위해 제정된 법률로 통신판매업자 및 중계업자 등을 규제하고 있으며 제5조에 의거 전자상거래에 의해 이용되는 전자문서에 대해 「전자거래기본법」과 「전자서명법」을 준용하도록 명시하고 있으며 동법 제6조 및 시행령 제6조에 의거 사이버몰 및 전자결제업자 등이 소비자 권익을 위해 정보보안 유지에 필요한 사항 조치 및 거래기록의 보존을 규정하고 있으며, 대금지급 시점에서 소비자의 의사표시가 있었는지 확인하도록 명시하고 있다.[21] 특히 제8조에 의거,전자적 수단에 의한 거래대금의 지급방법을 이용하는 경우에 관해 동법은 소비자가 입력한 정보가 소비자의 진정 의사표시에 의한 것인지를 확인할 주의의무,거래에 관한 사실통지의무,관련자료 제공의무 등에 관한 특별 규정을 두고 있어 이들 규정이 동법의 목적 범위내에서는 적용된다. 다만, 동법 제4조에는 다른 법률과의 관계에 관해 전자상거래 또는 통신판매에서의 소비자보호에 관하여 이 법과 다른 법률의 규정이 경합하는 경우에는 이 법을 우선 적용하되 다른 법률을 적용하는 것이 소비자에게 유리한 경우에는 그 법을 적용한다는 규정을 두고 있다.[22]

3.3 금융정보보안관련 법률

3.3.1 전자금융거래법 및 전자서명법

「전자금융거래법」은 전자금융거래를 금융기관 또는 전자금융업자가 전자적 장치를 통해 금융상품 및 서비스를 제공(전자금융업무)하고, 이용자가 금융기관 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다고 규정하고 있다.(제2조 1호)[23] 동법에서는 제3장 제21조 - 제27조를 통해 전자금융거래의 안전성확보 및 이용자 보호에 대해 규정하고 있으며 제21조 3호는 "금융위원회는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 「전자서명법」 제2조제8호의 공인인증서의 사용 등 인증방법에 대하여 필요한 기준을 정할 수 있다."라고 안전성 확보의무에 대해 명시하고 있다. 또한 제26조는 "전자금융거래와 관련한 업무를 수행함에 있어서 다음 각 호의 어느 하나에 해당하는 사항[24]을 알게 된 자는 이용자의 동의를 얻지 아니하고 이를 타인에게 제공·누설하거나 업무상 목적 외에 사용하여서는 아니된다."[25]라고 전자금융거래정보에 대한 제공과 관련하여 명시하고 있다.[26]

한편, 「전자서명법」은 전자문서 및 전자거래의 안정성과 신뢰성을 확보하기 위해 제정된 법률로 공인인증서 이용기관(전자서명법) 및 전자거래기관(전자거래기본법)을 규제한다. '전자금융거래법'[27]은 접근매체인 공인인증서 이용부분에 대해서 전자서명법[28]을 준용하도록 하였으며, 동법 제5조[29]는 전자문서 관련 부분은 전자거래 기본법[30]을 준용하도록 명시하고 있다.[31]

---

21) 금융보안연구원2009.11.pp 32.[1]
22) 정경영,2010.06.17.pp 12.[4]
23) 정경영,2010.06.17.pp 8.[4]
24) 1. 이용자의 인적 사항
2. 이용자의 계좌, 접근매체 및 전자금융거래의 내용과 실적에 관한 정보 또는 자료
25) 「금융실명거래 및 비밀보장에 관한 법률」 제4조제1항 단서의 규정에 따른 경우는 예외로함.
26) 정경영,2010.06.17.pp 8-9.[4]
27) 동법 제2조(정의) 제10항 나호," 「전자서명법」 제2조 제4호의 전자서명생성정보 및 같은 조 제7호의 인증서"
28) 동법 제2조(정의) 제4항,""전자서명생성정보"라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말한다." 동법 제2조 제7항,""인증서"라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다."
29) 동법 제5조(전자문서의 사용) 제1항,"전자금융거래를 위하여 사용되는 전자문서에 대하여는 「전자거래기본법」 제4조 내지 제7조,제9조 및 제10조의 규정을 적용한다."
30) 동법 제4조(전자문서의 효력) 제1항,"전자문서는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 전자적 형태로 되어 있다는 이유로 문서로서의 효력이 부인되지 아니한다.(이하 생략)동법 제7조(작성자가 송신한 것으로 보는 경우)
제1항,"작성자의 대리인 또는 자동으로 전자문서를 송신, 수신하도록 구성된 컴퓨터프로그램 그밖에 전자적 수단에 의하여 송신된 전자문서에 포함된 의사표시는 작성자가 송신한 것으로 본다." 동법 제9조(수신확인) 제1항,"작성자가 수신확인을 조건으로 하여 전자문서를 송신한 경우 작성자가 수신확인통지를 받기 전까지 그 전자문서는 송신되지 아니한 것으로 본다.(이하 행략)
동법 제10조(작성자와 수신자간 약정에 의한 변경), "작성자와 수신자는 다른 법령에 특별한 규정이 있는 경우를 제외하고는 제6조 내지 제9조의 규정과 다른 약정을 할 수 있다."

3.3.2 정보통신망 이용촉진 및 정보보호에 관한 법률

「정보통신망 이용촉진 및 정보보호에 관한 법률」은 정보통신망의 이용촉진 및 안전성 확보를 위해 제정된 법률로 정보통신서비스 기관을 규제한다. 동 법은 민간 침해사고의 대응,개인정보보호,정보보호안전진단,정보보호관리체계인증 등의 내용을 포함하며 동법 제48조[32] 및 제48조의 2[33]에 의거 민간 침해사고의 대응으로 정보통신망 침해행위 등의 금지,한국인터넷진흥원의 침해사고 대응 등을 규정한다. 또한, 동법 제23조[34] 및 제24조[35]는 개인정보보호를 위해 정보통신 서비스 기관의 개인정보 수집제한 및 제공범위 제한 등을 명시하여 OECD의 개인정보보호 가이드 준수 및 제30조는 정보통신서비스 제공자가 개인의 어떤 정보를 수집하였고 어디에 제공하였는지를 이용자 본인이 열람할 수 있는 권리를 명시하고 있다. 한편, 동법 제23조의 2(주민등록번호 외의 회원가입 방법)는 고객이 주민등록번호를 사용하지 않고도 회원으로 가입할 수 있는 방법을 제공해야 한다고 규정하고 있으며 동 법 시행령 제15조 제4항은 금융정보를 암호화하여 저장하도록 규정하고 있다. 동 법은 정보통신사업자의 '정보보호 안전진단'을 의무화하였으며 금융기관 등 일반기관의 '정보보호관리체계 인증(ISMS)' 수검을 권고하고 있다.

2007년 12월 21일 동법의 개정에 따라 그동안 전자금융보조업자로서 전자금융거래법의 규제를 받아오던 통신과금서비스업자들이 동 법의 규제를 받게되므로 규제기관이 금융위원회에서 행정안전부로 변경되었다.[36]

Ⅳ. 규제환경 변화에 따른 고객정보보호방안

4.1 전자서명법 개정

현재 2,200만명이 사용하고 있는 공인인증서가 스마트폰 환경에서 적용하기 어렵고 사용절차가 복잡해 국제적으로 통용되고 있는 다른 보안기술도 병행하여 사용할 수 있도록 허용해 달라는 관련업계의 요구에 따라 2010년 3월, 한나라당과 국무총리실,금융위원회,행정안전부,방송통신위원회,중소기업청 등 관련 부처간 당정협의에 따라 전자금융 거래시 공인인증서 이외의 인증방법을 금지[37]한 현행 규제를 풀기로 결정하였다. 이에 따라 스마트폰을 이용한 30만원 미만의 소액결제에 대해서는 새로운 보안방법의 도입과는 상관없이 공인인증서를 사용하지 않고도 결제가 가능하도록 금융감독원의 전자금융거래보안체계에 대한 보안성 심의를 탄력적으로 운영하기로 했다. 또한 동 조치로 온라인상거래의 97%를 차지하는 소액결제 활성화 및 중소 홈쇼핑몰 관련 업체의 다양한 전자금융거래 보안기술을 활용할 수 있게 되어 공인인증서용 앱(APP)을 개발해야하는 부담을 덜게 되었고 스마트폰 이용자도 간편한 결제방식을 이용하여 전자상거래를 할 수 있게 되었다.[38]

또한 행정안전부는 2010년 8월, 전자서명법 개정안을 입법예고 하였으며 그 주요내용은 1. 공인인증서의 종류 및 이용대상의 다양화[39] 2. 공인인증서 가입자의 신분확인 절차 강화 등 신뢰성 제고[40], 3. 공인인증업무

31) 금융보안연구원,2009.11.pp 20.[1]

32) 제48조(정보통신망 침해행위 등의 금지) 제1항,"누구든지 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망에 침입하여서는 아니 된다."
제48조 제2항,"누구든지 정당한 사유없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손,멸실,변경,위조하거나 그 운용을 방해할 수 있는 프로그램을 전달 또는 유포하여서는 아니된다."
제48조 3항,"누구든지 정보통신망의 안정적인 운영을 방해할 목적으로 대량의 신호 또는 데이터를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 정보통신망에 장애가 발생하게 해서는 아니된다."

33) 제48조의 2(침해사고의 대응) 제1항,"방송통신위원회는 침해사고에 적절히 대응하기 위하여 다음 각호의 업무를 수행하고,필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다."

34) 제23조(개인정보의 수집 제한 등) 제1항,"정보통신서비스 제공자는 사상,신념,과거의 병력 등 개인의 권리,이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다."

35) 제24조(개인정보의 이용 제한),"정보통신서비스 제공자는 제22조 및 제23조 제1항 단서에 따라 수집한 개인정보를 이용자로부터 동의받은 목적이나 제22조 제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니된다."

36) 금융보안연구원,2009.11.pp 24-26.[1]

37) 기술적인 측면에서 행정안전부는 금융분쟁발생시 사용자 책임을 입증할 수 있는 '부인방지 기능(전자서명)이 없는 SSL(암호통신기술)과 OTP(일회용 비밀번호 생성기)만으로는 스마트폰뱅킹을 통한 지급결제가 어렵다는 입장임.

38) 기타자료 [5]

39) 기존 용도 및 보안수준에 관계없이 발급되던 단일 공인인증서를 본인확인용,전자결제용,보안용 등으로 다양화하여 국민들의 용도에 맞게 선택적으로 발급받을 수 있도록 법적인 근거를 마련,

40) 폐지사유에 대한 명확화(현재의 폐지사유 인지에서 폐지사유 발생시 즉시 폐기), 전자상거래업체 등 공인인증서 이용

관리의 효율성 확보[41], 4. 공인전자서명 외의 전자서명에 대한 효력 규정 명확화[42]이며 이와 함께 주무부처인 행정안전부는 공인인증서의 암호키 길이를

2,048비트로 확정하여 보안성을 강화하고 학교를 통한 학생용 공인인증서의 발급을 추진(본인확인용)[43]하고 재외공관을 통해 국외체류 재외국민 공인인증서 발급을 지원하는 등 공인인증서 이용자 확대를 지속 추진할 계획이다.

4.2 전자금융감독규정 개정 및 안전대책마련

금융위원회는 2010년 6월 제11차 금융위원회정례회의에서 스마트폰 뱅킹, 온라인 중소쇼핑몰 증가 등 최근의 전자금융거래 환경변화를 고려하여 공인인증서외 다양한 인증방법을 사용할 수 있도록 하는 내용을 골자로 한「전자금융감독규정」개정안을 의결하여 현행 모든 전자금융거래에 있어 공인인증서의 사용을 의무화한 내용을 모든 전자금융거래에 있어 공인인증서 또는 이와 동등한 수준의 안정성이 인증되는 인증방법을 사용해야 한다고 개정하였으며 공인인증서 이외의 인증방법의 안전성 평가를 위해 금융감독원에 '인증방법평가위원회'를 둘 수 있도록 하여 위원회의 구성,운영 등 세부사항은 금융감독원장이 정하도록 하였다.[44]

한편, 금융감독원은 2010년 1월, 스마트폰 보급 확대에 따른 다양한 잠재적 보안위협이 제기됨에 따라 '스마트폰 전자금융서비스 안전대책'을 마련하였다. 동 대책은 PC의 인터넷뱅킹과 유사한 보안수준을 적용하는 것을 기본방향으로 1. 전자금융거래부문, 2. 기술적 침해대응 부문, 3. 취약점 모니터링 부문으로 구분, 수립되었다. 전자금융거래 부문의 경우 스마트폰 뱅킹 등 전자금융서비스 가입시 다단계 가입절차 확인[45]을 거치도록 하고 로그인시 사용자 인증을 강화하는 등 서비스 이용단계에서의 이용자의 신원확인을 강화[46]하며 PC 인터넷뱅킹의 전자자금이체시 적용하는 거래인증방법과 보안등급별 자금이체한도를 적용함으로써 PC뱅킹과 유사한 보안수준을 적용하도록 하였다. 기술적 침해 대응부분은 금융거래의 기밀성 및 무결성을 확보하기 위해 "스마트폰 對 금융회사"의 全 통신구간에서 금융거래정보는 암호화(SSL)하여 송수신되도록 함으로써 정보유출에 대비하고 비밀번호 등 중요입력정보가 유출되거나 변조되지 않도록 입력정보 보호대책을 적용하며 비밀번호 등 중요정보를 스마트폰에 저장을 금지하였으며 바이러스 등 악성코드에 의한 보안위협으로부터 전자금융거래를 보호하기 위해 악성코드 예방대책을 적용하고, 전자서명을 의무화하여 고객이 거래사실을 부인하는 것을 방지하도록 하였다. 취약점 모니터링 부문은 서비스 제공 금융회사는 정보보호전문기관 등과 협력하여 스마트폰 관련 새로운 취약점을 신속히 인식하고 대응할 수 있는 모니터링 체제를 구축하도록 하였다.[47]

또한 방송통신위원회도 2010년 2월 스마트폰 이용자를 위한 「10대 안전수칙」[48]발표한데 이어 2010년 6월에는 '스마트폰 정보보호 민관합동 대응반', 및 '모바일 시큐리티 포럼' 등을 통해 스마트폰 정보보호 주체인 이동통신사,스마트폰 제조사,백신사,보안솔루션 및 정부 등의「스마트폰 정보보호 주체별 역할」을 발표, 각 주체별 상세역할을 정립한 바 있다.[49] [표 3]

기관(업체)의 공인인증기관으로부터 공인인증서의 정지,폐기 등 유효성의 실시간 검증 의무화.

41) 공인인증서의 갱신지정절차를 법으로 규정하고 공인인증서용 S/W외에 일반 업체의 S/W도 평가 대상에 포함.

42) 전자서명법상 공인전자서명 외의 전자서명의 제3자까지 효력이 있음을 명확히 규정 및 공인인증서 수수료 수익자 부담 원칙에 따라 전자거래업체 등 공인인증서비스 이용자와 공동부담할 수 있도록 법적근거 마련.

43) 금융거래상 대리인의 동의가 필요한 초,중,고교생 등 미성년자의 단순 본인확인용 공인인증서는 전자서명기능을 제외하여 발급, 높은 보안수준이 요구되는 보안용에는 지문 등을 추가할 수 있도록 근거마련.

44) 기타자료[4]

45) 1단계 확인(ID,비밀번호 등), 2단계 확인(일회용비밀번호 등), 3단계 확인(공인인증서 등)

46) 스마트폰 전자금융서비스 가입시 가입자 유의사항 안내 후 가입을 허용하고, 로그인시 공인인증서를 사용하거나 ID, 비밀번호 외에 일회용비밀번호(보안카드추가)를 추가로 적용, 이중요소 인증(two-factor authentication)하는 등 사용자 인증을 강화

47) 기타자료 [1]

48) 1. 의심스러운 애플리케이션 다운로드하지 않기, 2. 신뢰할 수 없는 사이트 방문하지 않기, 3. 발신이 불명확하거나 의심스러운 메시지 및 메일 삭제하기, 4. 비밀번호 설정 기능을 이용하고 정기적으로 비밀번호 변경하기, 5. 블루투스 기능 등 무선 인터페이스는 사용시에만 켜놓기, 6. 이상증상이 지속될 경우 악성코드 감염여부 확인하기, 7. 다운로드한 파일은 바이러스 유무를 검사한 후 사용하기, 8. PC에도 백신프로그램을 설치하고 정기적으로 바이러스 검사하기, 9. 스마트폰 플랫폼 구조를 임의로 변경하지 않기(탈옥:Jailbreak), 10. 운영체제 및 백신프로그램을 항상 최신 버전으로 업데이트하기.

49) 기타자료 [9]

〔표 3〕 방송통신위원회, 스마트폰 정보보호 주체별 역할

구분	주체별 역할
이동통신사의 역할	1. 모바일 악성코드 대응방안 수립 및 이행 2. 스마트폰 정보보호 침해사고 접수 및 처리 절차 수립 3. 악성코드 조기경보 서비스 제공 4. 중요 S/W 패치 및 업데이트 서비스 지원 5. 스마트폰 원격 제어 서비스 제공 6. 단말기 보안설정 정보 제공
스마트폰 제조사의 역할	1. 단말기 잠금 기능 강화 2. 데이트암호화 기능 탑재 3. 데이터 및 시스템 백업,복구 기능 탑재 4. 데이터 및 시스템 접근제어 기능 제공 5. 단말기 악전성 검사 강화 6. 단말기 보안설정 매뉴얼 제공 7. 악성코드 샘플 확보 협력 등
모바일 백신사 및 보안솔루션사의 역할	1. 신속한 악성코드 샘플확보 체계 마련 2. 모바일 환경을 고려한 백신 개발 3. 신속한 백신 업데이트 제공 4. 악성코드 정보의 제공 5. 다양한 보안 솔루션 연구,개발 추진 등
방통위/KISA의 역할	1. 민관 협의체 구성 및 지원 2. 이용자 보안인식 제고 3. 모바일 위협정보 수집 및 분석기술 개발 4. 발생 가능한 침해사고에 대한 예측 및 대응방안 연구 5. 모바일 시큐리티 전문인력 양성 및 교육강화 6. 모바일 서비스용 웹사이트 침해예방 및 대응체계 구축 등 스마트폰 정보보호 침해사고 예방 및 대응활동 강화

그러나 스마트폰 도입초기 주요 이슈였던 금융거래시 공인인증제도 완화 등의 주 대상이었던 금융관련 당국 및 시중 은행등 금융기관에 대한 내용은 언급되지 않아 앞으로 이점에 대한 추가 보완이 필요하다.

4.3 위치정보의 보호 및 이용 등에 관한 법률 개정

2010년 7월, 방송통신위원회의 「위치정보의 보호 및 이용 등에 관한 법률」 개정안에 따르면 1. 위치정보 시장 활성화 및 중소사업자 보호를 위한 위치정보중개 사업 도입의 법적근거 마련[50], 2. 위치기반서비스사업의 양수 및 합병에 대한 신고의무 및 기한 명확화[51], 3. 개인위치정보를 취급하지 않는 사업자를 허가, 신고 등의 대상에서 제외하고 개인위치정보가 아닌 위치정보 수집, 이용, 제공사실 확인자료에 대한 기록, 보존 의무면제[52], 4. 개인위치정보주체의 자발적인 본인 위치정보 제공에 대해 즉시 통보의무를 면제하고, 개인위치정보주체가 매회 즉시통보를 원하지 않을 경우,8세 이하 아동등의 안전보장을 위한 서비스를 이용하는 경우 등에 있어 즉시 통보방법을 조정할 수 있도록 규정하여 위치정보사업자등의 즉시 통보 규정 완화[53], 5. 누구든지 긴급구조 외의 목적으로 긴급구조 요청을 할 수 없도록 법조문 정비[54] 6. 공정한 경쟁 환경 조성 및 위치정보의 동등제공 관련 규정 신설[55]7. 법을 위반한 위치정보사업자 등에 대해 방송통신위원회가 시정조치를 마련하거나 관련 자료를 제출하게 할 수 있도록 법적 근거 마련[56]을 주요골자로 하여 동 법의 규제완화를 추진하고 있다.[57]

최근 국내 은행들의 스마트폰 뱅킹을 통한 증강현실,LBS를 활용한 영업점 안내 뿐만아니라 금융이업종과의 제휴를 통해 은행 스마트폰뱅킹용 앱(APP)에서직접 제휴사의 쿠폰 및 가맹점정보를 보여주는 서비스를 제공하고 있다.[58] 이러한 스마트폰뱅킹을 통한 비금융서비스에 대한 부대서비스 제공과 관련하여 기존 은행법상의 겸영업무나 부수업무 규정은 물론 금융위원회의 「은행업무 중 부수업무의 범위에 관한 지침」 상에 적용내용이 불분명하며 은행관련 금융법 외에도 방송통신위원회의 위치정보의 보호 및 이용 등에 관한 법률 상에 위치정보사업자로 허가를 별도 득하여야 한다. 최근 구글의 스트리트뷰를 통한 위치정보서비스 제공과 관련하여 Wi-Fi를 이용한 개인정보의 무단 수집에 대한 구글을 비롯한 협력사에 대한 경찰 등의 압수색이 시행되고 있는 가운데 국내 은행도 은행이 직접 수집한 고객정보나 가맹점 정보외에도 서비스 제휴사를 통한 간접정보제공에 대해서도 관련 법규동향을 지속적으로 모니터링 하는 것이 필요하다.

Ⅵ. 결 론

5.1 연구의 요약 및 제언

본 연구는 '스마트폰뱅킹 도입에 따른 국내 은행의

50) 안 제2조 제7호
51) 안 제10조 제1항
52) 안 제12조의 2 및 안 제19조의 2 신설
53) 안 제19조 제3항 단서 실설 및 제4항
54) 안 제29조 제1항 단서
55) 안 제53조의 2 및 제35조의 3 신설
56) 안 제37조의 2 및 제37조의 3 신설
57) 기타자료 [10]
58) 김경민, 2010.06.p32.[2]

고객정보보호에 관한 연구'를 주제로 국내 은행의 스마트폰뱅킹 현황과 고객정보보호 및 관리에 대한 법률적 고찰과 규제환경 변화를 중심으로 국내 은행의 스마트폰뱅킹 도입에 따른 고객정보보호 방안을 연구하고자 하였다.

2009년 후반, 국내 아이폰 도입에 따른 스마트폰의 급속한 확산은 국내 은행들의 비대면채널 활성화를 위한 스마트폰 뱅킹 출시 경쟁으로 이어져 불과 출시 일년이 채 되지 않은 짧은 기간 동안 국내 대부분의 시중은행이 주요 스마트폰용 OS 플랫폼을 지원하는 스마트폰뱅킹 서비스를 제공하고 있다. 그러나 스마트폰 뱅킹의 경우 대면채널은 물론 PC를 통한 인터넷뱅킹이나 VM뱅킹과는 달리 안정성과 신뢰성을 중시하는 법규 및 감독규정을 우선하기 보다는 오히려 방송통신위원회 및 관련 통신업계가 우선시 하는 기술혁신 및 서비스 진보성과 마케팅 차별화에 치우친 나머지 금융관련 법제가 채 정비되기 전 출시를 함에 따라 지급결제에 따른 고객정보보호 및 보안에 대한 각 은행들의 충분한 검토와 대응이 미흡하였다.

더욱이 최근 국내외에서 안드로이드 OS 플랫폼 기반 스마트폰의 다양한 해킹에 대한 취약성과 iOS 플랫폼 기반의 아이폰용 스마트폰의 이용자에 의한 탈옥(Jailbreak)[59] 및 LBS기술을 활용한 구글의 스트리트뷰 등의 개인위치정보 무단 수집에 대한 문제 등 스마트폰 정보보안의 문제가 다양하게 제기되고 있어 전자금융거래 특히 스마트폰뱅킹서비스의 제공에 대한 금융시스템 적보안 뿐만아니라 고객정보보호에 대한 대책의 마련이 시급하다.

물론 행정안전부를 비롯하여 금융위원회와 금융감독원 등의 관련 정부기관 및 부처가 스마트폰뱅킹과 관련한 규제완화 및 보안대책을 수립하고 있으나 국내 은행은 서비스 차별화를 위해 금융시스템 외에도 다양한 어플리케이션을 활용한 컨텐츠 제공과 금융이업종과의 제휴를 통한 기존 관련 법규상 허용된 범위 외의 서비스 및 신규 사업분야의 진출을 활발히 추진하고 있어 스마트폰뱅킹을 사용하는 금융소비자에 대한 정보보호를 위한 관련 당국의 선제적 대응 및 관련 법규의 개정과 함께 전에도 서비스 제공 주체인 은행을 비롯한 금융기관에 대한 적절한 내부통제 및 가이드라인을 수립할 필요가 있다.

향후 급격한 정보통신기술의 발달과 금융서비스 제공 및 채널전략 다변화를 위한 국내 은행의 스마트폰뱅킹과 같이 신채널을 활용한 신금융서비스 및 증강현실이나 LBS 등 신기술을 활용한 위치정보사업자 등 신사업으로의 진출이 활발해 질 것으로 전망됨에 따라 국내 은행 또한 금융관련 법규외에 관련 업계의 규제환경에 대한 지속적인 관심과 대응을 통해 금융거래 및 고객정보와 관련한 정보보호에 대한 선행적 검토와 대책마련이 필요하다.

5.2 연구의 한계 및 연구과제

국내 스마트폰뱅킹의 도입이 2010년부터 본격 시작되었고 기존 인터넷뱅킹이나 VM뱅킹과는 달리 아직 어플리케이션을 활용한 금융 컨텐츠의 제공이나 조회서비스 제공에 치중하다보니 주요 법률적 쟁점인 지급결제와 관련한 실제 사례가 미비하여 어려움이 많았고 스마트폰뱅킹 도입기의 관련 법규 현황 및 규제환경 변화 동향에 초점을 맞추어 고찰하였다.

앞으로의 연구과제는 국내 은행의 스마트폰뱅킹이 활성화됨에 따라 발생되는 다양한 지급결제 사례를 통한 법규적용을 중심으로 고객정보보호 관리 현황과 대책을 연구하고자 한다.

참고문헌

[1] 금융보안연구원, "금융부문의 IT컴플라이언스 분석 결과 보고서," pp. 20-32. 2009년 11월.

[2] 김경민, "경품류 고시 개정에 따른 국내 은행의 마케팅 유형별 시사점," 전국은행연합회, 월간 금융 2010년 6월호, pp.32, 2010년 6월.

[3] 전국은행연합회, 금융실명제거래 업무해설, 전국은행연합회, pp.7-9. 2008년 10월.

[4] 정경영, "모바일 지급수단의 법률관계에 관한 소고," 금융결제원 2010년 지급결제 세미나 발표자

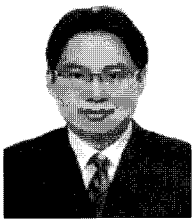
59) 지금까지 개방형 OS인 안드로이드 스마트폰에 비해 애플의 아이폰의 경우 애플의 앱스토어에서 판매되는 전용 어플리케이션만을 사용, 상대적인 보안성 측면에서 안전할 수 있었으나 2010년 7월, 미국연방통신위원회(FCC)의 1998년 관련 법령을 폐지하면서 스마트폰 플랫폼 구조를 변경하여 애플을 비롯한 타사의 스마트폰 제품을 해킹하여 해당사에서 지원하지 않은 앱(APP)을 다운로드 받아 설치하거나 핸드폰 통신사를 옮겨 사용하는 탈옥(Jailbreak)가 허용되어 이에 대한 취약성이 노출.

료, pp. 8-12. 2010년 6월
[5] 황성구, "국내 모바일뱅킹 서비스 현황 및 향후 발전방향," 금융결제원 2010년 지급결제 세미나 발표자료, pp. 16. 2010년 6월.

기타자료

[1] 금융감독원, 보도자료, "10.3월말 현재 스마트폰 전자금융서비스 현황 및 향후 제공계획," 2010년 4월 9일.
[2] 금융감독원, 보도자료, "스마트폰 전자금융서비스 안전대책," 2010년 1월 6일.
[4] 금융위원회, 보도자료, "공인인증서 사용규제 개선을 위한 전자금융감독규정 개정," 2010년 6월 23일.
[5] 국무총리실, 보도자료, "인터넷 금융거래시 '공인인증서 의무사용'규제 푼다," 2010년 3월 31일.
[6] 디지털타임즈, "은행 스마트폰 뱅킹 출시 '신경전'," 2009년 12월 28일.
[7] 디지털타임즈, "아파트시세,영업점,스타샵 '스마트폰'으로 조회하세요," 2010년 8월 9일.
[8] 민중의 소리, "경찰,구글코리아대표 소환조사, 협력업체로 수사확대," 2010년 8월 14일.
[9] 방송통신위원회, 보도자료, "스마트폰 보안위협,민관이 함께 적극 대응한다.," 2010년 6월 29일.
[10] 방송통신위원회, 보도자료, "위치정보의 보호 및 이용 등에 관한 법률 개정안 공청회 개최," 2010년 7월 29일.
[11] 서울파이낸스경제, "스마트폰 뱅킹'업그레이드 붐'," 2010년 6월 6일.
[12] 시사서울, "신한은행, 전 영업점에 와이파이존 구축," 2010년 8월 10일.
[13] 세계일보, "스마트폰 뱅킹시대 '활짝'," 2010년 7월 27일.
[14] 중앙일보, "스마트폰 공인인증서 규격화," 2010년 3월 22일.
[15] 중앙일보, "인터넷 뱅킹서비스 '이식',은행 합 '어플'개발이 숙제," 2010년 7월 30일.
[16] 파이낸셜뉴스, "국내 스마트폰 비약적 성장,", 2010년 8월 1일.
[17] 한국경제, "스마트폰 뱅킹,우리,국민銀 약진," 2010년 8월 9일.
[18] 한국은행 보도자료. "2010년 2/4분기 국내 인터넷 뱅킹서비스 이용현황," 2010년 7월 27일.
[19] 행정안전부 보도자료, "공인인증서 종류 3종으로 다양화한다.," 2010년 8월 10일.

〈著者紹介〉



김 경 민 (Kim Kyong Min)
정회원

2001년 8월 : 성균관대학교 경영/행정학부 졸업
2007년 8월 : 연세대학교 경제대학원 경제학 석사
20010년 9월 ~ 현재 : 성균관대학교 법학전문대학원 법학과 박사과정
관심분야 : 복합채널전략, 재휴마케팅, 정보보호, 금융규제