情報保護學會論文誌
第20卷 第6號, 2010. 12

스마트폰 전자금융거래 보호를 위한 법제적 문제점 분석
- 전자금융거래법(안)을 중심으로 -

최 승 현,† 김 강 석, 설 희 경, 양 대 욱, 이 동 훈‡
고려대학교 정보경영공학전문대학원

A Study on Problem and Improvement of Legal and Policy Framework for Smartphone Electronic Finance Transaction
- Focused on Electronic Financial Transaction Act -

Seung-hyeon Choi,† Kang-seok Kim, Hee-kyung Seol, Dae-wook Yang, Dong-hoon Lee‡
Graduate School for Information Management and Security, Korea University

요 약

최근 스마트폰의 보급이 늘어남에 따라 스마트폰을 이용한 자금 이체 및 증권 거래를 하는 스마트폰 전자금융거래가 빠르게 확산되고 있다. 은행, 증권사, 신용카드사 등 대부분의 금융회사가 스마트폰을 통한 전자금융거래서비스를 제공할 것으로 전망된다. 또한 언제 어디서나 이용 가능한 스마트폰의 특성으로 인해 스마트폰 전자금융거래서비스의 이용은 더욱 급증할 것으로 예상된다. 하지만, 우리나라의 전자금융거래 법제도는 대부분 일반 PC에 국한되는 기준을 적용하고 있기 때문에 스마트폰의 특성을 제대로 반영하지 못하고 있다. 따라서 본 연구에서는 스마트폰의 특성과 보안위협을 고려하여 현행의 법제도를 공인인증서의 사용 제약, 전자금융거래의 안전성 확보 및 이용자 보호를 위한 보안 프로그램 설치, 전자금융 사고 책임 주체에 대한 문제점을 중심으로 분석했으며 이에 대한 개선방안을 제시하였다.

ABSTRACT

As wide propagation of smartphones, e-commerce with smartphones increases rapidly. Such as transfer or stock trade systems. It has prospect that most of financial companies going to offer e-commerce systems via smartphones. And e-commerce via smartphones will be increased, hence the nature of smartphone that can be used whenever, wherever. However, legislation of e-commerce in Korea does not reflect these characteristics of smartphones, because it has set standards in regular PC. So that this study is security threat and feature of smartphones considering that the current legal system will use Certificate constraints, ensuring the safety of e-commerce and install security programs for protection of users, e-commerce responsible for the accident analysis has focused on the issues presented for this improvement.

Keywords: Smartphone, e-commerce, Electronic Financial Transaction Act

접수일(2010년 7월 15일), 게재확정일(2010년 9월 28일)
† 주저자, baneve@korea.ac.kr
‡ 교신저자, donghlee@korea.ac.kr

I. 서 론

최근 3세대 이동통신 기술의 발전과 더불어 스마트폰 시장이 급속도로 확산되었다. 음성통신 및 데이터 통신을 모두 빠른 속도로 할 수 있는 3세대 이동통신 기술은 스마트폰의 가치를 높여 주었다. 이전에 등장한 PDA폰도 기본적으로 스마트폰이 할 수 있는 기능을 모두 제공하지만 3G에서 빨라진 데이터 통신은 외부에서 인터넷 웹서핑과 e메일 확인을 더 유용하게 해주고 있다 [1]. 또한 언제 어디서나 빠르게 사용 가능하다는 특성을 이용하여 금융회사들은 스마트폰용 전자금융거래서비스를 출시하고 있다.

다양한 기능과 편리함을 제공하는 스마트폰의 보급이 크게 확대됨에 따라 스마트폰 전자금융거래 시장도 크게 활성화 되고 있다. 2010년 3월말 기준 스마트폰을 이용한 뱅킹 및 증권거래 서비스 가입자는 10만 9천명이며, 2009년 12월 스마트폰 전자금융서비스가 시작된 이후 4개월 동안 거래규모는 37만 4천건, 총 4,232억 원에 달하는 것으로 조사되었다 [2]. 주로 일반 유선 컴퓨터(이하 PC, Personal Computer)를 통해 제공되었던 전자금융거래서비스가 스마트폰이 등장하면서 무선에 기초한 모바일 인터넷 서비스로 전환되고 있음을 보여준다. 또한 다양한 형태의 모바일 인터넷 거래 어플리케이션이 자유롭게 개발되고, 제공되면서 금융 채널의 혁신과 다양화가 가속화 될 것으로 보인다.

스마트폰 전자금융거래 시장의 활성화와 더불어 다양한 잠재적 보안위협이 제기됨에 따라 스마트폰에 관한 여러 가지 안전대책들이 마련되고 있다. 하지만 스마트폰 이용자 증가에 비해 보안 개발 속도는 상대적으로 지체되어 있으며, 금융 감독 체계를 벗어난 기관들 간의 전자결제가 활발해지면서 결제 시스템 위험 노출 가능성이 증가되고 있다 [3]. 또한 현행의 전자금융거래 법제도가 PC에 국한되는 기준을 적용하고 있기 때문에 스마트폰이라는 새로운 전자금융 거래 매체에 대해서 현행의 법제도를 그대로 적용시키기에는 여러 가지 문제점이 있을 것이라 예상한다. PC와는 다른 특성을 지닌 스마트폰이라는 새로운 전자금융거래 매체에 대해서 현행의 전자금융거래 법제도를 그대로 적용시키려 한다면 사회적으로 많은 논란을 발생시킬 것이다. 따라서 기존 전자금융거래의 연장선이 아닌 보다 근본적인 스마트폰 전자금융거래 보안 대책이 요구되고 있다. 이를 위해서 스마트폰의 특성을 제대로 이해하고, 전자금융거래 법제도를 적절하게 개선해야 할 필요성이 부각되고 있다.

본 논문은 전자금융거래 법제도 중 중추적인 역할을 하고 있는 전자금융거래법과 하위법령인 전자금융감독규정을 중심으로 현행의 법제도가 스마트폰 전자금융거래 환경에서 실효성이 있는지를 판단하고, 문제점과 개선방안을 제시한다. 2장에서는 스마트폰의 이해를 위해 스마트폰의 특성과 보안위협 등을 소개하고, 스마트폰의 보안위협이 전자금융거래에 미치는 영향에 대해 기술한다. 3장에서는 현행 전자금융거래 법제도 중 전자금융거래법과 전자금융감독규정을 중심으로 문제점을 제시하고, 개선방안을 제시한다. 마지막으로 4장에서는 본 논문의 결론을 내린다.

II. 스마트폰 전자금융거래 보안위협

2.1 스마트폰 전자금융거래의 개념 및 현황

전자금융서비스는 은행·증권·보험 등의 금융거래에서 IT 기술을 금융업에 접목시켜 자금 이체, 송금 등 대금결제업무를 자동화하고, 금융서비스의 네트워크화를 구현하여 제공하는 서비스를 의미한다 [3]. 전자금융거래는 금융기관과 전자금융업자가 CD/ATM, 컴퓨터, 전화, 휴대폰, 카드 단말기 등의 전자적 장치를 이용하여 [표 1]과 같이 다양한 유형으로 전자 지급·채권·증권·보험 거래 등을 제공하고, 이용자는 자동화된 방식(비대면, 비서면)으로 전자금융서비스를 이용함으로써 전자금융거래가 이루어진다.

[표 1] 전자금융거래서비스 유형 [4]

은 행 서비스	· PC : 인터넷 뱅킹 · 모바일뱅킹 : WAP 뱅킹, VM뱅킹, PDA&스마트폰 뱅킹 · 금융 IC칩 & USIM 뱅킹 · IPTV 뱅킹
증 권 서비스	· PC : HTS(Home Trading System) · 모바일 HTS : WAP 서비스, VM 서비스, PDA, 스마트폰, 전용 단말기
신 용 카 드	· PC : Web/응용프로그램 · 모바일 신용카드(USIM, IC카드)
기 타	· 교통카드, ATM 지급결제, SMS 서비스 · 모바일 공인인증서 · 모바일 안심결제

스마트폰 전자금융거래는 기존의 전자금융거래 방식과 동일하며, 단지 전자금융거래에 이용되는 전자적 장치로써 스마트폰 단말기가 이용되는 것이다. 스마트폰 전자금융거래 서비스 제공 방식은 전용 어플리케이

션 방식과 브라우저 방식이 있지만, SEED 암호 알고리즘과 전자서명을 위한 공인인증서를 사용해야 하는 우리나라의 전자금융거래 환경에서는 브라우저 방식을 사용하는데 어려움이 존재한다. 현재의 스마트폰 전자금융거래에서는 각 스마트폰 플랫폼에서만 사용 가능한 별도의 전용 어플리케이션들을 통해 스마트폰 전자금융거래 서비스를 제공하고 있다.

스마트폰 전자금융거래는 2009년 말 스마트폰이 본격적으로 출시되면서 짧은 기간 동안 큰 성장세를 보이고 있다. 2010년 3월 말 기준 스마트폰 전자금융거래서비스는 3개 은행, 6개 증권회사 등 9개 금융회사가 제공하고 있으며, 뱅킹 서비스의 경우 서비스 개시(2009년 12월 초) 이후 약 4개월간 306천 건, 2,701억 원의 자금이체가 이루어졌다. 또한 증권 거래의 경우 개시(2010년 2월) 이후 2개월간 68천 건, 1,531억 원의 증권매매가 스마트폰을 통해 거래 되었다 [2].

본격적인 스마트폰 전자금융거래 환경이 조성되면서 대부분의 은행이 스마트폰 뱅킹 서비스를 제공할 예정이며, 증권회사, 신용카드사들도 신규 스마트폰 전자금융 서비스를 제공할 계획이다. 이에 따라 금융결제원에서는 스마트폰 모바일뱅킹 공동 서비스를 구축 중에 있으며, 금융감독원에서는 스마트폰 이용자 증가에 따른 금융거래 활성화에 앞서 스마트폰뱅킹서비스에 대한 보안수준을 강화하는 '스마트폰 전자금융서비스 주요 안전대책'을 발표하는 등 스마트폰 전자금융거래에 대한 관심이 급속도로 증가하고 있다.

2.2 스마트폰의 특성 및 전자금융거래 보안위협

스마트폰의 기본 운영체제로는 노키아의 심비안, 리서치 인 모션의 RIM, 애플의 아이폰 OS, 마이크로소프트의 윈도우모바일, 구글의 안드로이드 등 다양한 종류의 플랫폼이 존재한다. 전 세계 스마트폰 시장에서 가장 높은 점유율을 차지하고 있는 것은 노키아의 심비안이다. 우리나라에서는 마이크로소프트의 윈도우 모바일이 가장 대중적으로 자리 잡고 있지만, 애플의 아이폰 OS, 구글의 안드로이드 점유율이 점차 증가되는 추세이다. 결과적으로 앞으로 우리나라의 스마트폰 시장은 앞서 설명한 3사의 플랫폼(윈도우 모바일, 아이폰 OS, 안드로이드)이 장악하게 될 가능성이 매우 높다. 그러나 현재 대부분의 전자금융거래가 마이크로소프트의 윈도우즈(Internet Explorer 지원)에서만 발생되며 특히, 공인인증서와 보안 프로그램 사용을 위해 액티브엑스(ActiveX)[1] 기술을 이용하고 있다. 액티브엑스 기술은 타 플랫폼과의 호환성에서 여러 가지 문제가 발생되고 있다. 호환성 문제와 더불어 각 플랫폼마다의 특성으로 인해 개별적인 스마트폰 전자금융거래 어플리케이션을 개발해야하는 문제점도 지니고 있다.

다양한 종류의 스마트폰 플랫폼이 소개되면서 윈도우즈 기반의 전자금융거래 환경에 큰 변화가 예상된다. 특정 OS 환경에서만 전자금융거래가 가능하던 기존의 입장에서 스마트폰 전자금융거래의 대중화에 힘입어 그 동안 대처하지 못했던 다양한 OS 환경에서의 전자금융거래에 대한 고려가 필요하게 되었다. 동시에 전자금융거래 법제도의 수정·보완의 필요성도 부각되게 되었다. 그러나 이에 앞서 스마트폰의 특성과 보안위협들을 이해해야할 필요가 있다. 스마트폰의 특성과 보안위협을 제대로 이해하고 나서야 비로소 PC 뿐만 아니라 스마트폰 전자금융거래에도 함께 적용 가능한 합리적인 법제도의 개선방안이 도출될 수 있다.

2.2.1 스마트폰의 특성

현재 PC 기반의 전자금융거래에서는 안전한 거래환경 조성을 위해 E2E 암호화, 안티바이러스와 개인방화벽, 키보드 보안 프로그램, 메모리 해킹 방지도구, 공인 인증서와 같은 다양한 금융정보 보호기술을 이용하고 있다. 이에 반해 모바일 기반의 전자금융거래에 서는 신용카드나 현금카드 기능을 금융 IC 칩이나 USIM 칩에 탑재하여 사용하고, 가상 키보드와 휴대폰 소유자 인증을 위한 Call Back SMS 방식의 인증 방법을 사용함으로써 전자금융거래의 안전성을 강화하고 있지만 PC 기반의 전자금융거래 환경에 비해 많이 미흡한 편이다. PC와 모바일의 특성을 모두 지니고 있는 스마트폰의 경우 다단계 가입자 확인, 로그인시 이용자 인증 강화, E2E 암호화, 금융 정보 스마트폰 저장 금지와 같은 스마트폰 전자금융거래 서비스 안전 대책 지시사항 존재 할 뿐, 금융정보 보호와 관련된 보안 기술 규제는 현재까지 존재하고 있지 않다. 이는 PC와 유사하면서도 독특한 성질을 지니고 있는 스마트폰에 대한 특성 때문이다. 스마트폰과 PC의 특성을 [표 2]와 같이 비교할 수 있다.

1) 마이크로소프트사의 IE(Internet Explorer)에서만 동작되는 프로그램으로 이용자가 웹 서비스를 이용하는데 필요한 응용 프로그램(보안 프로그램 등)을 PC에 자동 설치할 수 있도록 해주는 기술이다 [5].

〔표 2〕 스마트폰과 일반 컴퓨터 특성 비교 〔6〕

구분	스마트폰(Smartphone)	일반 컴퓨터(Personal Computer)
운영체제	· 개방형 플랫폼(Open Platform) - Window Mobile, IPhone OS, Android, Symbian 등 · *다수의 OS가 다양하게 이용됨*	· 개방형 플랫폼(Open Platform) - Windows, Linux, Unix 등 · *특정 OS가 독점적으로 이용됨* - Windows 90% 이상 이용
서드파티 어플리케이션 지원	· AppStore와 같은 오픈마켓 시장(OMP) 또는 인터넷상에서 자유롭게 다운로드 가능 · 누구나 제작/배포/설치 가능 · 사용자 커스터마이징 가능	· 다양한 어플리케이션의 다운로드/설치 가능 · 누구나 제작/배포/설치 가능 · 사용자 커스터마이징 가능
인터넷 접속환경	· *3G and Wireless Network* - WCDMA, HSDPA, WiFi, Bluetooth, PC Sync	· *Fixed/Wireless Network*
저장 데이터	· 주소록, 일정관리, 오피스 문서, 금융정보 등의 중요한 개인정보	· 개인 문서 위주의 데이터 · 주소록, 일정 관리, 오피스 문서 등의 중요한 개인정보 · 평문 저장
사용시간	· *24시간 365일 항상 Power on* · *사용자의 시선에서 벗어날 수 있음*	· 인터넷 또는 문서작업 등의 *필요한 시간에만 사용 후 Power off* · *사용자의 시선에서 벗어나는 시간이 짧음*

스마트폰은 PC와 달리 365일 24시간 항상 켜놓기 때문에 언제든지 웜·바이러스에 감염될 수 있고, 오픈 플랫폼과 블루투스, PC 싱크(PC Sync) 등 다양한 인터페이스를 채택하고 있어 유선 환경에서보다 보안 위협이 더욱 커질 것으로 예상된다. 또한 3G(3Generation), 와이브로(WIBRO), 와이파이(WiFi) 등과 같은 초고속 무선 데이터 통신이 제공됨에 따라 음성 통신에서 데이터 통신으로 변화되면서 보안위협의 가능성이 증가되고 있다. 스마트폰에서의 보안위협은 스마트폰 전자금융거래 환경에서 다양하게 악의적인 목적으로 이용될 수 있다.

스마트폰의 특성을 설명하기 위해 피처폰(Feature phone)[2]과 비교할 수 있다. 피처폰에서 뱅킹 서비스를 이용하기 위해서는 VM 모바일 뱅킹이라는 별도의 응용프로그램을 설치해야만 이용가능하며, 이용자 인증을 위해서 PIN번호를 추가적으로 사용한다. 피처폰은 운영체제, 개발환경 등이 폐쇄적이기 때문에 현재까지 이용되면서 특별한 보안 이슈가 없었고, 시장규모도 작은 편에 속하여 공격을 통한 이득이 없었다. 그러나 스마트폰은 피처폰과 반대로 개방된 시장과 개발환경이 제공됨에 따라 다양한 어플리케이션이 개발될 수 있고, 개인정보의 집중화에 따라 PIMS(Personal Information Management System)의 역할을 수행한다. 이러한 특성은 다양한 형태의 공격 가능성이 존재하게 된다. 개방형 개발환경으로 공격자는 보다 많은 기술 습득이 가능하며, 시장 규모의 증가로 악의적 공격을 통한 상업적 이득이 높아진다. 또한 개인정보 수집은 프라이버시 침해와 더불어 제 2, 3의 공격에 활용될 수 있다.

〔표 3〕 스마트폰 플랫폼 특징 비교 〔4〕

	주요 특징
윈도우 모바일 (Windows Mobile)	· 전자금융서비스를 가장 많이 지원 · 웹 브라우저, 응용프로그램으로 서비스 · PC와 동일한 수준의 보안 위협이 존재 · 약 600여 종의 악성코드 존재 추정
안드로이드 (Android)	· 응용프로그램의 코드 서명, Sandbox 도입 · 응용프로그램의 권한 정보를 확인 후 사용자가 설치
아이폰 OS (iPhone OS)	· 코드서명 적용, 멀티태스킹 지원 안함 (iOS 4.0에서 지원) · App Store를 통해 어플리케이션 설치 (Apple의 프로그램 검증 수행) · 탈옥(Jail-break)를 통해 멀티태스킹 가능, 코드서명 우회

스마트폰의 또 다른 특성은 다양한 형태의 플랫폼에 있다. PC 기반의 전자금융거래는 여러 가지 운영체제(Wiondws, Linux, MacOSX 등)를 모두 고려하지 않고, 인터넷뱅킹이 시작되던 2000년대 초 우리나라 PC 시장에서 윈도우즈의 OS 점유율이 99%에 육박할 정도였기 때문에 윈도우즈 환경에서만 활성

2) 피처폰은 스마트폰이나 PDA폰이 아닌 모바일폰을 의미한다.

화되어 왔다. 그러나 스마트폰에서는 특정 플랫폼의 점유율이 압도적이지 않고, 이용자의 개성에 따라 다양한 플랫폼이 선택되어 사용되기 때문에 기존의 전자금융거래환경과는 분명 다른 차이가 발생한다. [표 3]은 다양한 스마트폰 플랫폼 중 우리나라에서 가장 많이 사용되고 있고, 앞으로도 계속 유지될 것으로 예상되는 3가지 플랫폼에 대하여 특징을 비교한 것이다.

윈도우 모바일의 경우 PMP, MP4 Player 등의 운영체제로 많이 사용되어 왔던 Windows Embedded CE 버전에서 기능을 특화한 버전으로 PDA의 운영체제로 많이 이용되어 왔기 때문에 우리나라 이용자들에게 가장 친숙한 플랫폼이다. PDA 도입 시부터 이용되어 왔던 윈도우 모바일은 다른 스마트폰 플랫폼에 비하여 전자금융서비스를 가장 많이 지원하는 플랫폼이다. 그러나 그만큼 많은 취약점이 소개 되었으며, 알려진 악성코드의 종류도 많다. 안드로이드와 아이폰 OS의 경우 스마트폰 도입과 함께 알려진 플랫폼으로 윈도우모바일에 비해 알려진 취약점은 많지 않으나 속속 취약점이 발견되고 있다. 안드로이드와 아이폰 OS의 경우 코드 서명을 통해 응용 프로그램을 검증하여 응용프로그램으로 인한 보안 위협을 차단하려는 노력을 하고 있지만, 아이폰 OS 3.x 버전의 경우 멀티태스킹 기능을 지원하지 않아 우리나라 전자금융거래 환경을 이용하는데 어려움이 따르고 있다. 또한 불법적인 방법을 이용하여 관리자 권한을 획득할 수 있는 방법들이 소개되어, 비정상적인 상황에서의 보안위협이 증가 될 수 있다.

2.2.2 스마트폰의 보안위협

스마트폰은 다양한 무선 접속 환경의 개방성, 휴대성, 저성능 등으로 PC 환경의 보안 위협과 더불어 새로운 보안 위협에 노출되어 있다. 이러한 스마트폰의 사용 환경에 대한 보안위협은 다음과 같이 정의 할 수 있다 [7].

- 개방성 : 스마트폰은 피처폰과 다르게 무선 인터넷 및 외부 인터페이스를 개방하여 제공하고 있다. 이러한 다양한 외부 인터페이스 제공은 악성코드 전파 경로의 다양성을 제공하고, 내부 인터페이스는 악의적 개발자에 의해 악성코드가 은닉된 스마트폰 어플리케이션 제작을 용이하게 만드는 취약점을 가지고 있다.
- 휴대성 : 스마트폰의 휴대 편의성으로 인해 발생하는 분실/도난 사고는 월 평균 20만 대에 이르고 있다. 스마트폰 분실/도난에 따른 직접적인 경제적 피해와 더불어 스마트폰에 저장된 개인 정보, 금융정보 및 모바일 오피스를 지원하는 스마트폰의 특성으로 인한 기업 중요 기밀 정보의 유출은 심각한 사회문제를 야기 시킬 수 있다.
- 저성능 : 스마트폰은 PC에 비해 저전력, 저성능 기기이다. 따라서 PC 환경에서 제공하는 보안 소프트웨어를 스마트폰에 적용하기에는 무리가 있다. PC 환경에서는 다양한 보안 위협에 대응하기 위해서 지속적인 모니터링을 통해 악성코드를 탐지해야 하지만 스마트폰은 전력 및 성능적 제약으로 인해 백신을 비롯한 보안 소프트웨어의 적용에 어려움이 있다.

스마트폰 기반의 전자금융거래 환경에서 보안 위협은 공격 유형에 따라 다양하게 분류할 수 있다. 위협이 발생되는 위치에 따라 정의하면 [표 4]와 같이 크게 어플리케이션(Application), 플랫폼(Platform) 및 디바이스(Device)로 분류 가능하다.

[표 4] 스마트폰의 보안위협 분류 [6]

분 류	정 의	보안 위협
어플리케이션 (Application)	스마트폰에서 실행되는 다양한 어플리케이션의 취약성을 이용한 공격	· 데이터 변조 및 유출 · 스팸(SPAM) 프로그램 설치 · 악성코드(웜바이러스/유해트래픽) 등
플랫폼 (Platform)	스마트폰에서 사용되는 운영체제 및 플랫폼 상의 취약점을 이용한 공격	· 바이러스 및 악성코드 · 브라우징 취약점 이용 공격 · 플랫폼 위/변조, SMS 후킹 · 메모리 해킹 등
디바이스 (Device)	스마트폰에 탑재된 파일 시스템 접근, 개인정보 추출 및 변조 등 디바이스 불법 접근에 의한 공격	· 분실, 도난 시 데이터 재사용 · 불법적 위치추적 · 디바이스 부하로 인한 배터리 방전 · 개인정보 추출 등

스마트폰의 보안위협은 공격 방법과 목적이 다양하지만 대체적으로 스마트폰의 기능을 마비시키거나 정보 유출 및 금전적 이득을 목적으로 이뤄지고 있다. 각 영역에서 발생할 수 있는 데이터의 유출은 스마트폰 전자금융거래 환경에서 중요한 보안위협이다. 스마트폰에는 중요한 개인정보 및 금융정보를 저장하고 있

기 때문에 어플리케이션의 취약점이나 악성코드, 파일 시스템 불법 접근 등을 통하여 외부로 유출하려는 시도가 증가될 것이라 예상된다. 또한 3G, 와이파이(WiFi), 블루투스 등 해킹 침입 경로의 다양성으로 스마트폰의 보안 위협은 더욱 다양해질 것이다. 이러한 보안위협들로 인해 유출된 중요 정보들은 전자금융사고로 이어질 가능성이 크기 때문에 주의가 필요한 부분이다.

스마트폰의 플랫폼에 따라 서로 다른 보안 위협이 존재한다. 윈도우 모바일의 경우 파일 접근제어를 제공하지 않아 ActiveSync 연결시 스마트폰 단말의 모든 파일에 접근(읽기/쓰기)이 가능하며 서드파티 툴을 이용하여 레지스트리 편집이 가능하다. 또한 리소스 권한 관리 기능의 부재로 전화, 메시지, 메일, 연락처 등의 리소스에 대한 접근이 자유롭고, 윈도우의 취약점을 그대로 계승받아 키보드 해킹, 메모리 덤프 등의 취약점이 그대로 나타날 가능성이 매우 높다.

아이폰 OS의 경우 정식 버전에서는 애플의 폐쇄적인 정책에 의해 알려진 보안 위협이 거의 존재 하지 않는다. 다만 정식 아이폰으로 부터의 Jail Break[3]가 가능하고, 다양한 커스텀 펌웨어 제작 툴이 존재한다. 아이폰은 윈도우 모바일에 비해 높은 보안을 제공하지만, Jail Break에 의해 윈도우모바일과 마찬가지로 모든 파일 시스템 접근이 가능해진다. 또한 Jail Break로 인해 애플의 공식 어플리케이션 온라인 마켓인 앱 스토어를 통하지 않은 비공식 경로를 이용한 불법 어플리케이션의 다운로드 및 설치가 가능하다. 이는 바이러스 및 악성코드 유포의 중요 수단으로 이용 될 수 있다. 2009년 11월에 발견된 아이키(ikee) 웜은 아이폰의 바탕화면 이미지를 변조하고 전파하는 기능만 가져 큰 위협이 없었지만, 시만텍에 보고된 아이키웜의 변종(iPhoneOS.Ikee.B)은 여러 IP 범위를 스캔해 SSH 루트 암호를 변경한다고 전해지고 있다. 그리고 이러한 웜의 작동은 과도한 배터리의 소모를 부추기고, 사용자의 정보를 수집해 특정 서버에 전송하는 등 다양한 위협으로 나타나고 있다.

안드로이드에서는 개발자 확인 과정이나 어플리케이션의 보안성 검증 절차가 없어 악의적인 어플리케이션의 등록이 쉽고, 어플리케이션을 설치할 때 사용자가 접근 권한을 제어할 수 있는 확인 과정(퍼미션) 역시 악성 코드의 판단과 설치 후의 책임을 사용자 몫으로 넘기는 보안 위협이 존재한다. 특히 어플리케이션의 설치 시 권한 정보를 보여주고 사용자에게 해당 어플리케이션을 설치할 것인지의 여부를 확인하게 되는데, 일반 사용자의 입장에서 권한을 전부 살펴보고 설치하기 어렵다는 점에서 큰 위협으로 나타나고 있다. InformationWeek의 보도자료에 따르면 Trustwave에서 커널레벨에서 작동하는 안드로이드 rootkit를 개발했다. 이 rootkit는 Linux 기반의 안드로이드 스마트폰에서 작동하며, 공격자는 데이터베이스의 참조 무결성을 유지하는데 도움을 주는 트리거(trigger)를 이용하여 TCP를 통해 안드로이드 스마트폰의 root 계정에 접근한다. Trustwave 관계자에 따르면 실제로 해당 rootkit이 안드로이드 스마트폰에서 실행된다면 공격자는 SMS 메시지를 읽고 GPS를 실행시키는 등의 공격이 가능하게 된다. 또한 스마트폰에서 rootkit을 중단 시킬 수 있는 소프트웨어가 존재하지 않아 더 많은 취약점이 존재한다고 언급했다 [8]. 이러한 보안 위협을 이용하여 각종 악성코드가 유포되면 주소록, SMS, 휴대폰 정보 등의 탈취, 조작, 삭제 등이 가능하게 되어, 사용자의 전자 금융정보의 유출을 피할 수 없게 된다.

특히 스마트폰의 종류와 플랫폼에 상관없이 다양한 형태의 악성코드가 발생할 것으로 예상되며, 이미 스마트폰에서의 개인정보를 탈취하는 악성코드가 보고된 바 있다. 2010년 상반기에 스마트폰 상의 스파이웨어 등의 악성코드 프로그램이 두 배 이상 증가하였으며, 일부 악성코드는 스마트폰 상에서만 작동하는 것으로 나타났다. 이는 무료 스마트폰 보안프로그램 이용자들을 대상으로 조사하였으며, 2010년 5월 100대의 스마트폰 중 9대의 스마트폰이 악성소프트웨어에 감염되어 2009년 11월에 비해 두 배 이상 증가했다. 가장 일반적인 악성코드 프로그램은 스파이웨어로 Blackberry, Windows Mobile, Android 폰을 대상으로 공격을 시도하였으며, 이용자의 통화내용 도청, SMS 유출, GPS를 통한 위치정보를 알아내는 공격이 가능한 것으로 보고된 바 있다. Lookout 관계자는 일반 PC에 비해 스마트폰은 악성코드의 감염속도가 빠르며, GPS 정보, SMS, e-mail 등 개인 상세 정보가 포함되어 있어 이용자들의 주의를 강조했다 [9]. 스마트폰을 대상으로 한 악성코드는 통화 기록이나 전화번호, 아이디, 패스워드 등의 개인 정보를 탈취할 뿐 아니라, 비정상적 트래픽을 유발해 비정상적인 과금을 유도할 가능성도 있다.

이러한 스마트폰의 다양한 보안 위협에 대응하기

3) Jail Break라 부르는 일명 "탈옥"은 애플사에서 설정해 둔 잠금장치를 풀고 허용 범위 밖의 기능이나 다른 어플리케이션을 실행할 수 있도록 만드는 것이다.

위해 스마트폰 보안 기술이 계속적으로 등장하고 있지만 단말기와 더불어 네트워킹 서비스의 활성화에 따라 스마트폰의 보안 위협은 계속적으로 증가하고 있다[10]. 이에 따라 스마트폰 보안위협에 대응하기 위한 법적·제도적 장치의 필요성이 부각되고 있다. 그러나 현재의 전자금융거래 관련 법제도를 스마트폰 기반의 전자금융거래 환경에 적용시키기에는 무리가 있다. 또한 스마트폰 전자금융거래 보안대책이나 전자금융 사고에 대비한 적합한 규율이나 보완장치가 미비하기 때문에, 안전하고 신뢰성 있는 스마트폰 전자금융거래 환경을 위한 법적·제도적 장치가 마련되거나 현재의 법제도를 개선해야 필요가 있다.

III. 법제적 문제점 분석

3.1 스마트폰 보안위협이 전자금융거래에 미치는 영향

스마트폰 보안위협이 전자금융거래에 미치는 영향은 크게 전자금융 거래단계와 전자금융 사고발생단계로 분류하여 논의할 수 있다. 거래단계는 금융회사와 이용자 사이에 거래 행위 이루어짐에 있어, 스마트폰 전자금융거래의 안전성과 편리성에 중점을 두고 고려해야 하며, 사고발생단계에서는 전자금융사고 발생 시 책임 부담의 주체를 중점으로 고려해야 한다.

스마트폰의 보안위협은 전자금융거래 환경의 거래단계에서 위험을 증가 시킨다. 악성코드나 키보드 후킹을 이용한 금융정보 탈취, SMS 후킹을 통한 불법결제, 불법적 디바이스 접근을 통한 금융정보 탈취 등의 공격 방법으로 금전적 이득을 취하려는 전자금융사고의 발생이 점차 증가할 것으로 예상된다. PC를 이용한 인터넷뱅킹에서 발생되었던 파일변조, 프로세스 메모리 덤프 등의 위협이 스마트폰에서도 동일하게 발생될 가능성이 있기 때문에 이에 대한 대비책도 마련되어야 한다. 하지만 스마트폰 전자금융거래에 현재의 PC기반 전자금융거래 보안대책을 적용할 경우 소비자들의 활용도가 떨어지는 것은 물론 오히려 보안 위험성을 초래할 수 있다. 이러한 이유로 금융감독원에서 발표한 스마트폰 전자금융서비스 안전대책에는 각 금융회사가 입력정보 보호 대책과 악성코드 예방대책을 적용하라고 했을 뿐 구체적 기술을 명시하고 있지 않다[11].

스마트폰 보안위협에 대처하기 위해 강력한 보안장치를 마련한다면 이용자들의 편리성이 침해될 것이고, 이용자들의 편리성을 위해 보안위협에 미흡하게 대처한다면 이용자들의 안전성이 보장되지 않을 것이다. 결국 스마트폰 전자금융거래에서 핵심적인 고려사항은 이용자들의 편리성과 안전성을 모두 보장할 수 있는 합리적인 조치가 있어야 한다는 것이다.

다음으로 다양한 스마트폰 보안위협으로 인한 전자금융사고가 발생했을 시, 금융회사와 이용자 간의 책임 관계 문제이다. 전자금융거래법에서는 접근매체의 위·변조, 해킹 등으로 전자금융사고 발생 시 금융기관 등이 원칙적으로 무과실 책임을 부담하게 하고 금융기관 등이 이용자의 고의·중과실을 입증한 경우에만 면책이 되도록 하고 있다. 현재 스마트폰 전자금융거래에 대한 보안 장치 마련에 관련된 규제가 마련되어 있지 않고, 적절한 보안 장치가 제공되지 않은 시점에서 금융회사가 현행의 법제도처럼 모든 책임을 부담하는 것은 논란의 여지가 있다. 그렇다고 이용자에게 모든 책임을 전가 시키는 것 또한 부당할 수 있기 때문에 적절한 조율이 필요하다. 예를 들어 아이폰 OS의 경우 Jail Break된 운영체제에서는 스마트폰 뱅킹의 사용이 불가능하도록 개발되었지만, 정상적인 운영체제임을 확인하는 코드를 우회함으로써 Jail Break된 운영체제에서도 뱅킹 서비스를 이용할 수 있다. 이러한 경우에 있어 전자금융 사고 발생 시 책임 주체의 문제와 금융기관의 입증 능력이 고려되어야 한다. 이와 같이 스마트폰 전자금융사고는 PC기반의 전자금융사고와는 다른 형태로 발생할 가능성이 존재하기 때문에 스마트폰 전자금융사고에서도 현행의 책임부담과 관련된 내용을 그대로 적용시킬지 말지에 대한 논의가 절실하게 필요하다.

3.2 전자금융거래법 문제점 분석

우리나라의 전자금융거래 관련 법제도에는 전자거래기본법, 전자서명법, 정보통신 이용촉진 및 정보보호 등에 관한 법률, 전자상거래 등에서의 소비자보호에 관한 법률, 전자어음의 발행 및 유통에 관한 법률 등이 존재하지만, 이러한 법령들은 전자금융에 대한 규율을 위해 제정된 법률이 아님에 따라 전자금융거래에 직접 적용하기 어렵고 규율사항도 산재해 있어 효과적 대응이 어려운 문제점이 있다.

비록 [표 5]와 같이 전자거래기본법과 전자서명법이 전자금융거래의 전자적 특성을 보완하기 위해 제정되었다고 하지만 전자금융거래와 관련된 업무수행과 관련된 규제·감독이 미비한 상황이다. 이에 따라 전자금융거래에 대한 규율의 일관성 확보 및 법적용의

불확실성을 제거할 필요성이 높아져 정부는 전자금융거래법 제정을 통하여 전자 금융 사고 시 책임범위, 이용자의 금융거래정보 보호 등 전자금융거래의 안전성 확보장치를 보강하고, 법률관계를 명확히 하고자 했다.

〔표 5〕 전자금융거래 관련 법률 〔12〕

법 명	제정일자	제정 취지
전자거래 기본법	1999년 2월8일	전자문서의 효력, 전자거래계약 및 분쟁 처리와 관련된 법률관계를 명확히 하고 전자거래 활성화를 위한 기반 조성
전자서명법	1999년 2월8일	전자문서의 안전성과 신뢰성을 확보하기 위해 전자서명, 공인인증기관, 인증서의 효력 등에 대해 규율

본 논문에서는 전자금융거래 관련 법제도 중 핵심적인 역할을 하고 있는 전자금융거래법과 시행령, 그리고 하위법령인 전자금융감독규정을 중심으로 스마트폰 전자금융거래 환경에서의 전자금융거래법의 실효성과 문제점, 개선방안에 대해 설명하기로 한다.

3.2.1 전자금융거래법의 의미와 특징

전자금융거래법은 총 7장, 51개조 및 부칙 4개조로 구성되어 있으며, 시행령 및 전자금융감독규정을 하위법령으로 두고 있다(감독규정이 시행규칙을 대체). 전자금융거래법은 전자금융거래의 안전성과 신뢰성을 확보하여 전자금융거래를 활성화하고 전자금융업의 건전한 발전을 지원함으로써 국민의 금융편의를 도모하고 국민경제의 발전에 이바지함을 목적으로 하고 있다(전자금융거래법 제 1조).

기본적으로 전자금융거래법은 오프라인 금융거래와 전달채널만 다를 뿐 본질적으로 동일한 금융거래이므로 기존의 오프라인 거래에 대한 법적 제도와 일관성을 유지할 수 있도록 별도 규율이 꼭 필요한 사항만을 규정하고 있다. 또한 전자적 장치를 통해 이루어지는 모든 금융거래에 전자금융거래법이 적용되지만 일반 이용자에게는 영향을 끼치지 않으며 기술 발전에 따라 탄력적인 대응이 가능하도록 거래 상대방간 계약(협약)으로 기본적인 규율을 정하여 적용하도록 하는 특징을 가지고 있다 〔13〕. 이러한 전자금융거래법은의 주요한 내용을 정리하면 〔표 6〕과 같다.

전자금융거래법과 더불어 금융위원회에 위임한 사항과 그 시행에 필요한 사항 및 다른 법령에 따라 금

〔표 6〕 전자금융거래법의 주요내용 〔12〕

법조항	주요내용
금융기관의 무과실 책임	전자금융사고 시 이용자의 고의·중과실을 입증하지 못하면 금융기관이 원칙적으로 손해배상 책임
보조업자 과실시 금융기관이 일단 책임 부담	IT 외부업체 등의 고의·과실로 인한 손해 발생 시 금융기관이 우선 책임을 부담하고 사후적으로 구상(求償)
전자금융거래 기본틀 법제화	전자지급 수단별로 효력발생과 철회 가능 시기 명확히 규정
비금융사업자도 건전성 감독	통신업체 등 비금융사업자가 전자 금융업을 하려면 금융감독위원회 허가·등록을 받아야 하고 건전성도 검사

융감독원의 검사를 받는 기관의 정보기술부문 안전성 확보 등을 위하여 필요한 사항을 규정한 전자금융감독규정이 존재한다(전자금융감독규정 제 1조). 전자금융감독규정에서는 인터넷 뱅킹이나 텔레뱅킹 등 지속적으로 증가하는 전자금융거래와 관련하여 금융기관들의 안전성 확보 및 이용자 보호에 관한 사항, 전자화폐 및 선불전자지급수단 발행업 등 전자금융업의 허가와 등록 및 영업에 관한 사항 등 전자금융거래와 전자금융업의 감독에 관한 제반 사항을 규정하였다.

전자금융거래법과 하위법령인 전자금융감독규정에서 전자금융거래에 정의하고 있는 전자적 장치는 전자금융거래정보를 전자적 방법으로 전송, 처리하는데 이용되는 장치로써, CD/ATM, 컴퓨터, 전화, 휴대폰, 카드단말기 등으로 분류하고 있다. 관련 법률과 규정은 대부분 이러한 전자적 장치에 기반을 두어 제정되었다. 하지만 스마트폰이라는 새로운 전자적 장치의 출현으로 전자금융거래 시장은 새로운 국면을 맞이하게 되었고 현재의 전자금융거래 법제도가 새로운 전자장치에 대해 동일한 기준을 적용시킬 수 있는가에 대한 논의가 필요하게 되었다.

3.2.2 전자금융거래법의 문제점 분석

1) 공인 인증서

공인인증서는 전자금융 거래를 할 때 신원을 확인하고, 문서의 위조와 변조, 거래 사실의 부인방지 등을 목적으로 공인인증기관(CA)이 발행하는 전자적 정보로서, 일종의 사이버 거래용 인감증명서이다. 다시 말해, 전자서명을 하는데 이용된 정보가 서명을 한 가입자에게 유일하게 속한다는 사실 등을 확인하고, 이를 증명하는 전자정보를 말한다.

스마트폰 전자금융거래에서 공인인증서의 논란은

스마트폰에서 공인인증서를 어떻게 지원할 것인가에 대한 논의에서 시작됐다. 현재 국내 대부분의 웹 사이트에서는 공인인증서를 통한 전자서명을 지원하기 위해 쉽게 구현하여 사용할 수 있는 액티브엑스 기술을 이용하여 전자서명을 제공하고 있다. 이 기능은 웹 브라우저의 플러그인 형태로 동작하게 된다. 그러나 이러한 방식은 국내 전자거래 환경이 MS의 기술에 종속되는 결과를 가져왔다는 논란을 야기하였다. 스마트폰이 확산됨에 따라 오픈웹 등에서는 전자결제를 위한 보안 기술로 기존의 공인인증서를 이용한 전자서명 기술뿐만 아니라, SSL과 OTP를 이용하는 기술도 사용할 수 있도록 해줄 것을 요구하고 있다 [7]. 2007년 1월에 오픈웹이 금융결제원을 상대로 '마이크로소프트 인터넷 익스플로러 외 환경에서도 인터넷뱅킹을 이용할 수 있도록 지원하라'며 제기한 민사소송에서 패소했지만, 다양한 공인인증서 관련 문제를 제기함으로써 전자금융서비스 이용자들의 관심과 동조를 얻고 있다.

실제로 스마트폰에서는 웹브라우저를 이용해 PC처럼 인터넷뱅킹을 이용할 수 없다. 스마트폰 웹브라우저에서는 액티브엑스를 지원하지 않아 공인인증서를 이용할 수 없기 때문이다. 이에 따라 금융기관에서는 독자적 혹은 공동으로 스마트폰용 공인인증서를 개발하고 스마트폰용 전용 인터넷뱅킹 어플리케이션을 개발하여 제공하고 있다. 정부 당국은 스마트폰 전자금융거래에서 공인인증서 사용의 한계를 인식하고, 2010년 5월 31일 방송통신위원회는 '전자금융거래 인증방법의 안전성 가이드라인'을 발표했다. 이에 따라 금융기관 또는 전자금융업자는 공인인증서를 사용하지 않고도 이용자 인증, 서버 인증 및 통신채널 암호화 요건을 갖춘 경우에 인증방법평가위원회의 안전성 평가를 거쳐 다양한 전자금융 서비스를 제공할 수 있게 되었다 [14]. 스마트폰 보안 위협의 증가, 스마트폰 전자금융거래에서 공인인증서 사용의 한계성, 급속히 증가되고 있는 스마트폰 전자금융 이용자 수 등의 현실적 상황을 통합적으로 고려하여 이전 전자금융거래 관련 법제도의 한계를 인식하고 정부당국이 발빠르게 대응한 것이다.

전자금융감독규정 제 7조(공인인증서 사용기준)에서는 모든 전자금융거래에 있어 '전자서명법'에 의한 공인인증서를 사용해야 한다는 규정을 볼 수 있다. 그리고 예외사항에 대하여는 전자금융감독규정과 전자금융감독규정시행세칙 제 31조 (전자금융거래에 있어서 공인인증서 사용 예외) 9항에 의하여 금융감독원이 정하는 기준에 의해 적용 가능하다고 명시하고 있다.

> 전자금융감독규정 제 7조(공인인증서 사용기준)
> 제7조(공인인증서 사용기준) 모든 전자금융거래에 있어 「전자서명법」에 의한 공인인증서를 사용하여야 한다. 다만 기술적·제도적으로 공인인증서 적용이 곤란한 전자금융거래로 감독원장이 정하는 경우에는 그러하지 아니하다.

'전자금융거래 인증방법의 안전성 가이드라인'은 본 조항에서 공인인증서 사용기준에 대한 예외 사항으로 스마트폰 전자금융거래에서 공인인증서의 사용제한 완화 조치라 볼 수 있다. 그러나 스마트폰 전자금융거래에서 공인인증서 사용제한이 완화되었다고 하지만 몇 가지 발생 가능한 문제점이 존재한다. 공인인증서 사용제한 완화를 위해 개정 준비 중인 전자금융감독규정을 미리 살펴보면, 제 7조 2항의 인증방법평가위원회가 기술적 요건들을 고려하여 인증방법의 안전성을 평가하여 공인인증서와 동등한 수준의 안전성을 보장하고자 한다.

> 전자금융감독규정 제 7조 2항(기술적 요건)
> ① (이용자 인증) 금융기관 또는 전자금융업자는 전자금융거래 제공시 정당한 이용자 여부를 식별 및 인증할 수 있어야 함
> ② (서버 인증) 금융기관 또는 전자금융업자는 이용자가 서버(정보처리시스템)에 접속한 경우 정당한 금융기관 등의 여부를 이용자가 식별 및 인증할 수 있도록 하여야 함
> ③ (통신채널의 암호화) 금융기관 또는 전자금융업자는 이용자와 서버간의 전자금융거래내역 등 중요정보가 유출되지 않도록 암호화를 통한 비밀성·무결성을 제공하여야 함
> ④ (거래내역의 무결성) 금융기관 또는 전자금융업자는 해당 전자금융거래내역의 위조·변조 여부를 확인할 수 있어야 함
> ⑤ (거래내역의 부인방지) 금융기관 또는 전자금융업자는 정당한 전자금융거래 사실을 이용자 및 금융기관이 부인할 수 없는 수단을 제공할 수 있음
> 〈2010년 6월 준비 중인 개정안〉

개정안에 따르면 전문가로 구성된 인증방법평가위원회를 설치하여 기본적으로 이용자 인증, 서버 인증, 통신채널의 암호화를 갖춘 경우 차별적으로 전자금융거래를 할 수 있으며, 거래내역의 무결성, 거래내역의 부인방지의 기술적 요건이 추가적으로 제공되어 공인인증서와 동등한 수준으로 인정되는 경우에 한하여 공인인증서를 대체하여 사용 가능하다고 명시하고 있다.

본 개정안에 따라 금융기관에서 공인인증서를 사용하지 않고, 현재와 같은 수준의 전자금융거래 서비스

를 제공하기 위해서는 1차적으로 5가지 기술요건을 모두 만족하는 대체 보안 수단을 강구해야 하며, 2차적으로 인증방법평가위원회의 검증 과정을 통과해야만 한다는 결론을 도출할 수 있다. 즉, 금융기관에서 공인인증서를 사용하지 않는 전자금융거래 서비스를 제공하기 위해서는 추가적인 비용과 시간의 대가를 지불해야 한다는 의미이다. 공인인증서에 상응하는 안정성을 갖춘 보안 수단을 마련하기 위해 기술적 연구와 개발에 대한 비용이 소요되며, 이를 평가받고 상용화하기까지의 많은 시간이 소요될 가능성이 존재하게 된다.

2) 전자금융거래의 안전성 확보 및 이용자 보호

전자금융거래의 안전성은 거래의 신뢰성을 확보하는 기초이다. 전자거래기본법은 전자거래의 안전성 확보를 위하여 개인정보보호, 영업비밀보호, 암호제품의 사용, 전자거래사업자에 대한 인증 등을 규정하고 있다(電法 제 12조~제 14조, 제 18조). 나아가 전자금융거래법은 전자금융거래의 안전성 확보를 위하여 안전성의 확보의무, 전자금융거래 기록의 생성 및 보전, 전자지급수단의 발행과 이용한도 등을 규정하고 있다(제 21조~제 23조).

금융위원회는 전자금융거래법이 제정되기 이전에 '금융기관전자금융감독규정'(2000. 12. 29, 금융위원회공고 제 2000-117호)과 '금융기관전자금융업무감독규정 시행세칙'(2001. 3. 30)을 제정하여 전자금융업무 감독의 지침으로 사용해왔다 [15].

스마트폰 전자금융거래에서의 안전성 확보와 이용자 보호가 기존의 법제도 틀 안에서 유연성 있게 적용가능하다면 이상적이겠지만, 스마트폰이 2장에서 기술한바와 같이 기존의 전자적 단말과는 차별된 특성을 지니고 있어 그대로 반영하는 것이 쉽지 않다. 전자금융감독규정시행세칙 제 29조(전자금융거래 시 준수사항) ②항에는 전자금융거래에서의 안전성 확보와 이용자 보호를 위해 보안 프로그램 설치를 강제하는 규정이 존재한다.

전자금융감독규정시행세칙 제 29조
(전자금융거래 시 준수사항) ②항
3. 이용자PC에서의 정보유출을 방지하기 위해 이용자의 접속 시 우선적으로 이용자PC에 개인용 침입차단시스템, 키보드해킹방지 프로그램 등의 보안프로그램을 설치할 것(다만, 고객의 책임으로 본인이 동의하는 경우에는 보안프로그램 해제 가능)

금융감독원에서 발행한 전자금융감독규정 해설(2007. 12)에 의하면 본 규정은 전자 금융 이용자가 전자적 장치(PC, 노트북)를 이용하여 금융기관 또는 전자금융업자의 전자금융 서비스에 접속하는 경우 우선적으로 이용자의 전자적 장치에 키보드해킹 방지 프로그램 등의 보안 프로그램을 제공해야 한다고 기술되어있다. 즉, 보안 프로그램의 제공으로 이용자의 금융정보 유출을 방지하기 위한 목적으로 제정된 것이다.

하지만 본 조항을 스마트폰 전자금융거래에 적용시에 크게 두 가지 문제점이 발생한다. 첫 번째는 용어 해석상의 문제점이다. 본 조항에서는 이용자PC라는 직접적인 대상을 제시하였을 뿐, 그 외의 어떠한 장치에 대한 언급도 없다. 일반적으로 보았을 때 이용자PC는 개인이 사용하는 PC와 노트북 정도로 간주할 수 있다. 그렇다면 스마트폰을 과연 PC와 동일선상에서 바라 볼 것인가에 대한 해석론적 문제점이 발생한다. 스마트폰을 PC로 분류한다면 보안프로그램 설치 의무를 이행해야 하지만, PC와 별개의 장치로 분류한다면 보안프로그램을 설치해야 하는 의무가 사라진다고 해석할 수 있다. 즉, 이용자PC에 대한 해석의 차이가 보안 프로그램 설치 규정을 피해갈 수도 있다는 의미가 된다.

두 번째는 적용 범위에 대한 문제점이다. 스마트폰을 이용자PC로 간주한다면, 보안 프로그램 설치의 적용 범위를 PC와 동일하게 적용할 것인가에 대한 문제이다. 하드웨어적으로 PC와 크게 차이가 없다고 할지라도 스마트폰은 항상 휴대하고 다니는 모바일 단말기라는 특성을 고려해볼 때, PC와 동일한 기준을 적용하는데 무리가 따른다. 구글의 CEO인 Eirc Schmidt는 백신이나 키보드 해킹 방지 프로그램 등을 스마트폰에 설치할 경우, 백그라운드에서 실행되기 때문에 스마트폰 배터리의 빠른 소모를 발생시킨다고 지적한 바 있다. 이는 안전한 전자금융거래를 위해 스마트폰에 보안 프로그램의 설치를 PC와 동일한 기준으로 강제할 경우 스마트폰의 특성을 침해하는 행위가 된다는 뜻이다.

또한 스마트폰 단말의 종류에 따라서도 적용 기준이 달라질 수 있음을 인지해야 한다. 아이폰 OS의 경우 3.0 버전에서 멀티태스킹을 지원하지 않고, iOS 4.0에서는 멀티태스킹을 지원하되 백그라운드 실행은 제한된다. 이는 아이폰 OS에서 전자금융거래 시점과 동일한 시점에서 키보드 해킹 방지 프로그램이나 백신 등의 보안 프로그램을 실행할 수 없다는 것이다. 때문에 스마트폰 단말 자체에서 기술 지원이 되지 않아 보안 프로그램을 설치할 수 없는 경우에 대비한 대책마

련도 함께 마련되어야 한다.

3) 전자금융 사고 책임 주체

전자금융거래법은 금융기관 또는 전자금융사업자의 책임에 관하여 접근매체의 위조·변조나 거래 처리 과정에서 발생한 사고에 대하여 원칙적으로 이용자의 고의·과실과 상관없이 손해를 배상할 책임을 지우고 있다. 다만, 이용자의 고의나 중대한 과실이 있는 경우로서 이용자와 사전약정을 체결한 경우나 기업 간 거래의 경우에는 예외가 인정된다.

전자금융거래법 제 9조
(금융기관 또는 전자금융업자의 책임)

① 금융기관 또는 전자금융업자는 접근매체의 위조나 변조로 발생한 사고, 계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고로 인하여 이용자에게 손해가 발생한 경우에는 그 손해를 배상할 책임을 진다.

② 제1항의 규정에 불구하고 금융기관 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 경우에는 그 책임의 전부 또는 일부를 이용자가 부담하게 할 수 있다.

1. 사고 발생에 있어서 이용자의 고의나 중대한 과실이 있는 경우로서 그 책임의 전부 또는 일부를 이용자의 부담으로 할 수 있다는 취지의 약정을 미리 이용자와 체결한 경우
2. 법인(「중소기업기본법」 제 2조 제 2항에 의한 소기업을 제외한다)인 이용자에게 손해가 발생한 경우로 금융기관 또는 전자금융업자가 사고를 방지하기 위하여 보안절차를 수립하고 이를 철저히 준수하는 등 합리적으로 요구되는 충분한 주의의무를 다한 경우

③ 제 2항 제 1호의 규정에 따른 이용자의 고의나 중대한 과실은 대통령령이 정하는 범위 안에서 전자금융거래에 관한 약관(이하 "약관"이라 한다)에 기재된 것에 한한다.

전자금융 사고 발생 시 이용자가 자신의 고의·과실이 없었음을 증명하는 것은 상당한 어려운 일이며, 이는 곧 전자 금융 사고 발생에 대한 모든 책임을 이용자에게 지우겠다는 것과 일맥상통한다. 때문에 본 조항에서 금융기관 또는 전자금융업자에게 기본적인 배상 책임을 지우는 취지는 약자인 이용자를 보호하기 위함이다. 하지만 스마트폰 전자금융거래에서는 PC 환경의 전자금융거래에서보다 높은 금융정보 유출 가능성과 보안 위협이 존재하므로, 사고 발생 시 책임 주체에 대해 다시 고려해 볼 필요가 있다. 제한된 공간에서 다중 인증 요소를 이용하여 전자금융거래가 이루어져왔던 PC환경에서는 대체로 전자금융사고의 발생 건수가 높지 않았다. 2010년 5월 10일 기준 금융감독원의 자료에 따르면 2009년 전자금융 관련 사고가 모두 24건 발생해 3억 8,400만원의 피해를 냈다고 보고된바 있다. 그리고 대부분의 금융사고 발생 원인이 해킹 등을 통해 유출된 개인정보를 이용한 인터넷 뱅킹 범죄라는 것에 주목해야 한다.

스마트폰 전자금융거래는 언제 어디서든지 이용 가능하고, 스마트폰의 특성상 금융 정보의 유출 가능성이 매우 높으며, 스마트폰 단말의 분실 가능성도 매우 높아진다. 또한 Jail Break 등을 통한 비 인가된 스마트폰 단말을 통하여 전자금융거래 서비스를 이용할 수 있는 방법들이 소개 되고 있어 스마트폰 전자금융거래의 위험성을 증가시키는 요인이 되고 있다. 이러한 사실을 종합해보면 PC환경에서보다 많은 전자금융사고가 발생할 가능성이 존재한다는 결론이다. 금융기관에서 본 조항에 따라 면책을 받기 위해서는 사고 발생 시마다 이용자의 고의 또는 중대한 과실을 입증해야 하지만, 과연 금융기관이 시간, 인력, 비용적 측면에서 이를 감당할 수 있는가가 문제점이 될 수 있다. 실제로 PC환경에서 발생한 전자금융거래 사고의 대응 사례를 살펴보면 금융기관은 스스로 이용자의 과실을 입증할 수 있는 능력이 되지 않거나 혹은 비용이 많이 들어 수사 기관에 의뢰하는 일이 빈번히 발생한다. 때문에 이용자는 사고가 발생하더라도 많은 시간을 기다려야만 보상을 받을 수도 혹은 과실이 입증되어 보상을 받지 못할 수도 있다.

이용자 과실 입증을 위해 막대한 시간과 인력, 비용이 소요된다면, 금융기관으로써는 이 모든 것을 원천 봉쇄하기 위해 강력한 보안 수단을 설치할 수밖에 없는 것이다. 이는 편리성이 중시되는 스마트폰 전자금융거래 환경에 악영향을 미치게 된다. 즉, 이용자 보호를 위해 만들어진 법 조항이 오히려 이용자의 편리성을 훼손하는 역기능으로 작용할 수 있다는 것이다.

3.3 전자금융거래 법제도 개선방안

스마트폰 전자금융거래 보호를 위한 법제적 문제점을 3.2절에서 제시하였다. 본 절에서는 앞서 분석한 문제점을 바탕으로 전자금융거래 법제도의 개선방안에 대해 제시한다.

3.3.1 개선방안

스마트폰 전자금융거래 관련 법제도의 문제점을 크게 공인인증서의 사용, 전자금융거래의 안전성 확보

및 이용자 보호, 전자금융 사고 책임 주체로 분류하여 제시하였다.

공인인증서 사용에 관한 전자금융거래법은 현재 개정을 앞둔 상황이라 발표 이전까지 정확한 개선방안을 제시하기는 어렵지만, 사전에 공개된 개정안을 바탕으로 개선방안을 제시한다. 우선적으로 스마트폰 전자금융거래의 최대 걸림돌이었던 공인인증서의 사용 제한이 완화된 측면에서는 정부의 대처가 긍정적으로 평가된다. 하지만 기술 변화에 따른 이번 조치가 성공적인 정책이었음을 입증하기 위해서는 인증방법평가위원회의 구성과 평가 기준, 평가 방법 등이 객관적이고 합리적으로 진행되어야 한다는 전제하에 진행되어야 한다는 점이다. 공인인증서를 대체할 보안 수단의 기술요건을 갖추고 서비스를 제공함에 있어 금융기관이 투자하는 시간과 비용이 합리적인 결과를 이끌어 낼 수 있도록 해야 한다. 만약 공인인증서 대체 기술의 개발에서부터 서비스 제공까지의 시간과 비용에 막대한 투자가 필요하다면 어떠한 금융기관도 공인인증서를 포기하고 새로운 기술을 개발하려 노력하지 않을 것은 분명한 사실이다. 이러한 상황이 발생한다면 본 조치는 표면적으로만 공인증서 사용에 대한 선택권을 부여한 것일 뿐, 속내는 공인인증서의 사용을 계속적으로 제한한다고 밖에 볼 수 없는 것이다.

개정안의 성공적인 정착을 위해서는 인증방법평가위원회는 보안강도, 신규 인증방법에 대한 보안 등급 등 세부 평가기준을 마련하고 공개하되, 관련 기관들이 모두 공감할 수 있어야 한다. 또한 단순 기술적 측면 뿐만 아니라 대체 기술의 개발 혹은 도입에 따른

〔표 7〕 스마트폰 전자금융거래 보호를 위한 법제도 개정(안) 예시

현행	개정(안)
전자금융감독규정[4)] 제 7조 2항(인증방법평가위원회 설치·운영) ○ 위원회는 금융기관 등이 평가를 요청한 인증방법에 대해 동 가이드라인의 준수 여부를 판단 ○ 위원회는 전자금융거래 유형별 보안강도, 신규 인증방법에 대한 보안등급 등 세부평가기준을 마련, 공개하여야 함	전자금융감독규정 제 7조 2항(인증방법평가위원회 설치·운영) 개정안과 동일 ※ 개정안 시행에 있어 심의 절차와 평가 방법 등이 합리적으로 이행되어야 함
전자금융감독규정시행세칙 제 29조(전자금융거래 시 준수사항) ②항 3. 이용자PC에서의 정보유출을 방지하기 위해 이용자의 접속 시 우선적으로 이용자PC에 개인용 침입차단시스템, 키보드해킹방지 프로그램 등의 보안프로그램을 설치할 것(다만, 고객의 책임으로 본인이 동의하는 경우에는 보안프로그램 해제 가능)	전자금융감독규정시행세칙 제 29조(전자금융거래 시 준수사항) ②항 3. 전자금융 거래에 이용되는 이용자의 전자적 장치(PC, 노트북, 스마트폰 등)에서의 정보유출을 방지하기 위해 이용자의 접속 시 우선적으로 이용자의 전자적 장치에 개인용 침입차단시스템, 키보드해킹방지 프로그램 등의 보안프로그램을 설치할 것(다만, 고객의 책임으로 본인이 동의하는 경우에는 보안프로그램 해제 가능) 다만 기술적·제도적으로 보안프로그램 적용이 곤란한 경우 인증방법평가위원회의 보안성 심의를 통과한 대체 보안 수단을 적용해야 한다.
전자금융거래법 제 9조(금융기관 또는 전자금융업자의 책임) ② 제1항의 규정에 불구하고 금융기관 또는 전자금융업자는 다음 각 호의 어느 하나에 해당하는 경우에는 그 책임의 전부 또는 일부를 이용자가 부담하게 할 수 있다. 1. 사고 발생에 있어서 이용자의 고의나 중대한 과실이 있는 경우로서 그 책임의 전부 또는 일부를 이용자의 부담으로 할 수 있다는 취지의 약정을 미리 이용자와 체결한 경우	전자금융거래법 제 9조(금융기관 또는 전자금융업자의 책임) ① 현행과 동일 ② 현행과 동일 1. 현행과 동일 2. 금융기관 또는 전자금융업자는 전자금융사고 발생 예방을 위해 적당한 조치를 취했을 경우 3. 전자금융거래에 이용된 이용자의 전자적 장치가 불법적으로 변경(개조)된 경우로서 그 책임의 전부 또는 일부를 이용자의 부담으로 할 수 있다는 취지의 약정을 미리 이용자와 체결한 경우

4) 2010년 6월 23일 제 11차 금융위원회 정례회의에서 전자금융감독규정 개정안이 의결되었으며, 관보게재 절차 등을 거쳐 고시한 날부터 시행할 계획임.

비용 대비 수익 등 타당성 있는 경제성 분석을 통하여 금융기관에 큰 부담을 지우지 않는 범위 내에서의 후속 조치가 이루어져야 한다.

전자금융거래의 안전성 확보 및 이용자 보호를 위해 제시되었던 해석상의 차이가 발생 가능한 용어의 사용과 보안 장치의 적용 범위에 대해 분명한 기준이 제시되어야 한다. 기존 법 조항에 명시되어 있는 이용자PC라는 용어 선택에 있어, 이용자PC에 스마트폰 단말을 포함할 것인지 판단해야 하는데 현재의 전자금융거래 서비스 현황을 보아서는 스마트폰단말을 포함시키는 것이 올바르다. 때문에 이용자PC라는 용어의 사용 보다는 전자금융감독규정 해설서에 기술되어 있는 전자금융 이용자가 이용하는 전자적 장치(PC, 노트북, 스마트폰)로 변경하는 것이 해석상의 차이를 줄이는 효과적인 방법이라 할 수 있다.

보안 장치의 적용 범위에 대해서는 스마트폰의 특성을 고려하여 기본 법조항에 예외 조항을 마련하거나, 스마트폰 전자금융거래에 합당한 법조항을 제정해야 할 필요가 있다. 스마트폰의 단말기 종류마다 서로 다른 특성이 존재하므로 하나의 큰 테두리 안에서 같은 법제도적 규정을 마련하여 적용시키는 것은 다소 문제가 될 수 있다. 보안 프로그램의 설치를 스마트폰에도 강제하고자 한다면 스마트폰의 특성을 최대한 고려하여 PC환경과는 다른 보안 프로그램의 적용을 시도해야 할 것이며 예외 사항을 두어 기술적, 환경적으로 보안 프로그램의 적용이 어려운 단말에 대해서는 대체 수단을 강구하여 명시해야 한다. 법 조항의 명확화는 추후 전자금융 사고 발생 시 이용자와 금융기관 간의 책임 전가를 막을 수 있는 효과적인 방법이 된다.

전자금융 사고 책임의 주체에 대한 문제는 금융기관의 능력에 따라, 사고 예방에 대한 노력 등에 따라 등급별 책임 의무 부여가 필요하다. 스마트폰 전자금융거래에 대한 명확한 근거를 제시하고, 금융기관의 이행 여부와 이용자의 고의, 과실 등을 입증할 수 있는 능력 등을 전반적으로 고려하여 상세 등급으로 분류하여 책임을 지우는 것이 합리적이다. 또한 스마트폰 전자금융거래에서는 이용자의 고의나 과실(Jail Break 등을 통한 비 인가된 스마트폰을 이용한 전자금융거래 시도 등)의 가능성이 높아질 수 있음에 따라 이용자에 대한 책임도 일부 부여해야 한다. 이용자의 고의, 과실을 입증하기 위한 별도의 위원회를 구성할 수도 있다. 대부분의 금융기관이 전자금융 사고 원인에 대하여 입증하는 것에 대해 회의적인 반응을 보이고 있으며, 수사기관에 의뢰하는 것은 상당히 많은 시간이 소요되어 금융기관과 이용자 모두에게 좋지 않은 영향을 줄 수 있다고 판단된다. 이를 위해 금융 사고에 대한 원인 분석을 위한 별도의 위원회를 구성한다면 모두에게 바람직한 방향으로 나아갈 수 있는 방법을 제시할 수 있다.

3.3.2 개정(안) 예시

스마트폰 전자금융거래 보호를 위해 현행의 법제적 문제점을 분석하고 개선방안을 기술하였다. 이를 바탕으로 [표 7]과 같이 개정(안)을 제시한다.

IV. 결 론

스마트폰의 도입과 함께 급속히 증가되고 있는 스마트폰 전자금융거래에서 안전한 거래환경 조성을 위해 현행의 전자금융거래 관련 법제도를 분석하였다. 현행의 전자금융거래 법제도가 PC 환경에 맞게 제정되어 스마트폰이라는 새로운 특성을 지닌 전자적 장치의 출현으로 현행의 법제도를 그대로 적용하기에 다양한 문제가 발생하게 되었다.

본 연구에서는 전자금융거래법과 전자금융감독규정을 중심으로 스마트폰 전자금융거래에 적용 시 발생 가능한 문제점을 공인인증서의 사용 제약, 전자금융거래의 안전성 확보 및 이용자 보호를 위한 보안 프로그램 설치, 전자금융 사고 책임 주체로 분류하여 분석하였으며, 이에 대한 개선방안을 제시했다. 이러한 연구는 현행 법제도의 문제점을 지적한다기보다는 더욱 안전한 전자금융거래 환경을 조성할 수 있는 발판을 마련하기 위함이며, 전자금융거래 제공자와 이용자의 안전성과 편의성을 도모하기 위함이다. 급속한 기술의 발전과 환경 변화에 따른 법제도의 개정이 빠르고 적절하게 진행되어야만 전자금융거래에서의 다양한 위험으로부터 이용자를 보호하고 안전한 전자금융거래 환경을 조성할 수 있을 것이다.

참고문헌

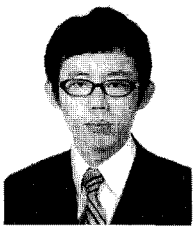
[1] 한국경제매거진, "스마트폰 시장이 열린다," 한경비즈니스, 11(676), 2008년.

[2] 금융감독원, "10.3월말 현재 스마트폰 전자금융서비스 현황 및 향후 제공계획," 금융감독원 보도자료, 2010년 4월.

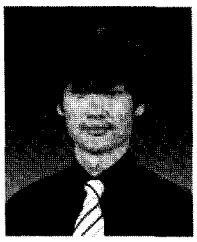
[3] 원종현, "스마트폰 발매가 전자금융서비스에 미칠

영향," 국회입법조사처 입법조사회답, 2010년.
〔4〕 장재환, "신기술 기반 금융보안 기술 및 동향," NETSEC-KR 2010, 2010년 4월.
〔5〕 공감코리아(korea.kr), "인터넷서비스 이용환경 개선 적극 추진", 공감코리아 정책정보 보도자료, 2010년 4월.
〔6〕 이기혁, "Mobile security(open marketplace security ecosystem)," SKTelecom 강연자료, 2010년 2월.
〔7〕 강동호 외 6, "스마트폰 보안 위협 및 대응 기술", 한국전자통신연구원 전자 통신 동향 분석, 25(3), 2010년 6월.
〔8〕 Mathew J. Schwartz, "Android malware's potential detailed," InformationWeek, June. 2010.
〔9〕 Kelly Jackson Higgins, "Smartphone malware multiplies," DarkReading, June. 2010.
〔10〕 김기영, 강동호, "개방형 모바일 환경에서 스마트폰 보안기술," 한국정보보호학회 정보보호학회지, 19(5), 2009년 10월.
〔11〕 조성훈, "스마트폰 금융보안 딜레마," 디지털타임즈, 2010년 1월.
〔12〕 이용수, "전자금융거래법 시행에 따른 전자금융의 과제," 정보통신정책연구원 우정정보, 67, 2006년 12월.
〔13〕 강준모, "전자금융거래 법적문제에 관한 연구(전자금융거래법(안)을 중심으로)," 한국국제조세협회 조세학술논집, 21(2), pp. 179-247, 2005년.
〔14〕 방송통신위원회, "전자금융거래 인증방법의 안전성 가이드라인," 방송통신위원회 보도자료, 2010년 5월.
〔15〕 손진화, 전자금융거래법, 제 2판, 법문사, 2008년 3월.
〔16〕 전자금융거래법, 법률 제 9325호, 2008년 12월.
〔17〕 전자금융거래법 시행령, 대통령령 제 21765호, 2009년 10월.
〔18〕 전자금융감독규정, 금융위원회 고시 제 2008 -21호, 2008년 7월.
〔19〕 전자금융감독규정시행세칙, 2009년 7월.
〔20〕 금융감독원, 전자금융감독규정 해설, 2007년 12월.

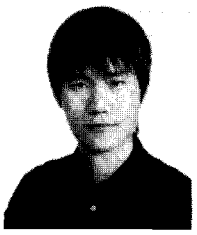
〈著者紹介〉



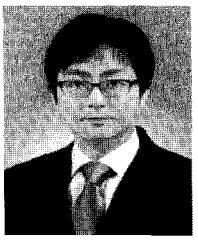
최 승 현 (Seung-hyeon Choi) 학생회원
2009년 2월: 강원대학교 산업공학과 학사 졸업
2009년 3월~현재: 고려대학교 정보경영공학전문대학원 금융보안학과 석사과정
〈관심분야〉 정보보호, 금융보안, 스마트폰 보안, 클라우드 컴퓨팅, P2P 보안



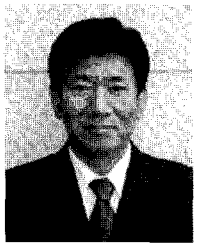
김 강 석 (Kang-seok Kim) 학생회원
2009년 2월: 숭실대학교 컴퓨터학부 학사 졸업
2009년 3월~현재: 고려대학교 정보경영공학전문대학원 금융보안학과 석사과정
〈관심분야〉 정보보호, 금융보안, 포렌식, 역공학



설 희 경 (Hee-kyung Seol) 학생회원
2009년 2월: 서울시립대학교 컴퓨터과학부 학사졸업
2009년 3월~현재: 고려대학교 정보경영공학전문대학원 금융보안학과 석사과정
〈관심분야〉 정보보호, 금융보안, IT컨설팅, ERP보안



양 대 욱 (Dae-wook Yang) 학생회원
2008년 2월: 중앙대학교 정보시스템학과 학사 졸업
2009년 3월~현재: 고려대학교 정보경영공학전문대학원 금융보안학과 석사과정
〈관심분야〉 정보보호, 금융보안, 네트워크 보안



이 동 훈 (Dong-hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학사 졸업
1987년 12월: Oklahoma University 전산학과 석사 졸업
1992년 5월: Oklahoma University 전산학과 박사 졸업
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 3월~현재: 고려대학교 정보경영공학전문대학원 교수
〈관심분야〉 암호프로토콜, 암호이론, 금융보안, 스마트폰 보안, USN이론, 키 교환