情報保護學會論文誌
第 21 卷 第 6 號, 2011. 12

금융시장 건전성을 해치는 모바일단말 위협에 대한 대응방안(금융투자회사를 중심으로)*

유 길 상,† 박 태 형‡ , 임 종 인
고려대학교 정보보호대학원

Countermeasures and Mobile Terminal Threats to harm the Financial Market Soundness(focusing on the Financial Investment Companies)*

Kil-sang Yoo,† Tae-hyoung Park‡ , Jong-in Lim
Graduate School of Information Security, Korea University

요 약

스마트폰과 같은 모바일단말은 '모바일 빅뱅'이라 불릴 만큼 일상생활과 기업경영에 거스를 수 없는 커다란 변화를 가져왔다. 시간과 장소에 제한 없이 모바일뱅킹, MTS(모바일트레이딩시스템)을 이용할 수 있고, 회사 외부에서도 직원 간 의사소통이 간편해졌고 모바일오피스를 통해 업무까지 처리할 수 있다. 모바일단말은 금융회사에게 생산성 향상과 경쟁력 확보를 위한 '스마트모바일 이노베이션'으로 다가오고 있지만, 금융업을 영위함에 있어 직무관련 미공개정보와 모바일단말을 이용하여 '불건전 영업행위' 또는 '불공정거래'에 악용할 소지가 상당히 크며 고객정보를 유출할 위협 역시 증가하고 있다.

따라서 금융시장의 건전성을 확보하고 고객정보를 보호하기 위해 모바일단말로 인해 발생가능한 문제점을 분석하고 대책을 마련하는 등 선제적 대응이 필요하다. 본 논문에서는 '자본시장과 금융투자업에 관한 법률'에 의한 금융투자회사를 중심으로 금융회사에서 모바일단말 이용과 관련하여 발생할 수 있는 모바일단말의 위협을 문제점으로 분석하고 이에 대한 대응방안을 제시하고자 한다.

ABSTRACT

Mobile devices such as smart phones have brought big changes to be called as 'mobile big bang' against which we can't go. Mobile banking service and MTS(Mobile Trading System) are freely available at any time, anywhere and we are able to activate communications between financial company staffs out of the office and take care of business works even remotely by using mobile devices. Mobile devices are approaching as 'smart mobile innovation' to improve an enterprise productivity and competitiveness, but threats which engaged in unfair trading behaviors or unwholesome business works in finance companies are increasing and the customer's information can be leaked out by using the nonpublic official information and mobile devices.

Therefore, we have to analyze the potential problems and take the necessary countermeasures with preemptive steps to protect the customer's information and improve the financial trading soundness and fairness. In this paper, we would like to suggest countermeasures and threats against using the financial company's mobile devices focusing on the financial investment companies by 'Capital Market and Financial Investment Business Act'

Keywords: Mobile Terminal, Internal Control, Financial Information Security, Unfair Trading Behaviors, MTS

접수일(2011년 7월 14일), 수정일(2011년 8월 25일), 게재확정일(2011년 10월 28일)
* 본 연구는 지식경제부 :최고정보보안전문가과정" 지원사업(과제번호: NIPA-2011-C7050-1101-0001) 연구결과로 수행되었습니다.
† 주저자, rks912@naver.com
‡ 교신저자, mosto2004@korea.ac.kr

I. 서 론

금융회사는 금융업을 영위하면서 수많은 정보를 주고받으며 지속적으로 정보를 생성, 저장, 활용··유통, 폐기하는 등 '정보의 라이프사이클'에 따라 정보를 취급한다[1]. 이 과정에서 정보가 부당하게 이용되기도 하며 고객정보와 같은 중요정보가 유출되어 금융회사에 큰 손실을 입히기도 한다. 따라서 금융회사는 건전하고 공정하게 영업을 하면서 이익을 극대화(손실을 최소화)하기 위하여 지속적으로 정보를 보호하고 정보의 흐름을 적절히 통제할 필요가 있다.

금융회사 내·외부간의 정보의 유통은 '전산장비'(PC·노트북 등, 보조기억매체 포함) 및 '정보통신수단'(이메일·메신저 등)을 통해 이뤄지고 있음에도 금융회사는 이에 대한 내부통제수단이 미흡했었다. 금융감독원은 이를 감안하여 '금융회사의 정보통신수단 등 전산장비 이용관련 내부통제 모범규준'(이하 '전산장비 모범규준')을 마련하여 2011.4월에 시행하였다. 업무용 이메일이나 메신저를 지정하여 사용토록 하고 사용내용 등 로그 기록의 보관·관리를 의무화하였다[2].

하지만, 금융회사의 전산장비가 '모바일단말'로 다양해지고, '모바일오피스' 도입으로 업무의 활용범위도 비약적으로 확대되고 있다. 또한 금융회사 임직원 대부분이 모바일단말을 사용하고 있다. 따라서 금융회사 임직원은 업무시간에 모바일단말을 통해 이메일·메신저, '카카오톡'(모바일메시징서비스) 및 '페이스북'과 같은 'SNS'(소설네트워크서비스) 등을 사용하여 외부인과 통신할 수 있으며, MTS(모바일트레이딩시스템) 등 다양한 모바일 애플리케이션을 이용할 수 있다. 또한 모바일단말은 대용량의 저장장치를 갖고 있어 금융회사의 고객정보 등 중요 내부정보를 저장하는 매체로도 사용될 수 있다.

결국 모바일단말을 이용하면 금융회사가 그동안 구축해 놓은 유선망 중심의 내부통제수단과 전산장비 모범규준에서 제시한 내부통제수단을 모두 우회하거나 회피할 수 있다는 문제점이 발생할 수 있다. 특히 시장성상품의 거래를 담당하는 금융회사 임직원이 모바일단말을 업무용으로 사용하면 거래내역의 기록이 누락되며, 금융회사 임직원이 직무상 알게 된 정보로서 외부에 공개되지 아니한 정보('직무관련 미공개정보')를 이용하여 불건전 영업행위나 불공정거래 행위를 하게 될 위협이 증가할 수 있다. 따라서 금융시장의 건전성 확보와 공정한 금융질서의 확립을 위해 모바일단말에서 발생 가능한 문제점을 분석하고 대책을 마련하는 등 선제적인 대응이 필요한 시점이다.

본 논문은 스마트폰의 이용확대 등 최근 모바일단말의 환경변화와 금융시장 건전성을 확보하기 위한 금융거래관련 내부통제 현황을 살펴보고 금융회사에서 모바일단말의 사용과 관련하여 기존의 내부통제시스템을 약화시킬 수 있는 모바일단말의 위협을 문제점으로 분석한 후 마지막으로 이에 대한 대응방안을 제시하고자 한다.

II. 최근 모바일단말의 환경변화

2.1 모바일단말의 대중화

대표적인 모바일단말은 '스마트폰'과 '스마트패드'이다. 스마트폰은 전화 및 무선 인터넷 접속은 물론 다양한 애플리케이션을 실행할 수 있는 소형 컴퓨터의 기능을 갖춘 멀티 통신기기이다. 스마트패드는 스마트폰, PC, 넷북 등의 장점을 갖춘 멀티미디어 기기로서 '태블릿PC'로 호칭하기도 한다. 모바일단말의 사용증가로 인터넷은 유선 중심에서 무선 또는 FMC(유·무선통합) 환경으로 이동하고 있으며, 모바일단말을 활용한 모바일오피스, 스마트워크 및 모바일 클라우딩 등의 등장으로 스마트라이프(smart life)는 더욱 가속화 될 것으로 기대된다.

국내 스마트폰 가입자 수는 2009년말 80만명에서 2010년말 722만명으로 10배 가까이 증가하였으며, 2015년에는 4,000만명을 넘어설 것으로 예상된다. 스마트패드 이용자는 디지털 멀티미디어의 활용 증가로 인해 2015년에 1,000만명에 근접할 것으로 전망된다[3]. 이러한 전망은 2011.3.23일, 스마트폰 가입자수가 1,000만명을 넘어서면서 현실화 되었고 2011년말에는 기존 예상보다 많은 2,000만명을 돌파할 것으로 전망되는 등 본격적인 스마트폰 대중화 시대에 진입하였다[4].

2.2 금융회사의 모바일오피스 확산

모바일단말의 대중화는 '모바일오피스' 부문에 커다란 변화를 일으키고 있다. 모바일오피스 구축에 가장 노력하는 금융권은 증권업계이다. 증권회사는 MTS를 서비스하고 있는데 이는 증권회사 입장에서 모바일오피스 환경을 촉진시키는 동기부여가 되고 있다. 고객에 대한 실시간 자산관리서비스 등 모바일단말을 통해 제공할 수 있는 여러 기능을 구현하기 위해서는 모

바일오피스 구축이 필수적이기 때문이다. 삼성증권은 임직원에게 스마트폰을 지급하면서 FMC기반의 모바일오피스를 구축하여 스마트폰을 사내전화로 이용하면서 오피스 업무를 자유롭게 볼 수 있도록 하였다〔5〕. 은행권에서는 신한은행이 은행권 최초로 임직원에게 스마트폰을 지급하고 모바일오피스를 구축하였으며〔6〕, 외환은행은 SK텔레콤과 스마트오피스 협력을 위한 전략적 제휴를 통해 스마트 지점 구축 등을 추진하기로 하였다〔5〕.

금융권의 모바일오피스 추진은 보안문제로 당초 예상보다 지지부진하였으나 최근 보안업체 및 이동통신사들의 발 빠른 대응으로 기업용 '모바일 보안 통합솔루션'이 출시되고 있고〔7〕, 금융회사들이 모바일오피스 2단계 사업의 추진 움직임을 보이고 있어 금융회사의 모바일오피스 적용범위는 점차 확대될 것으로 예상된다.

2.3 전자금융거래에 모바일단말의 이용 증가

모바일단말은 '모바일 금융'의 도구로서 모바일뱅킹, MTS 및 모바일단말 결제 등 전자금융거래 부문에도 혁신적인 변화를 가져오고 있다. 2010년말 모바일뱅킹 등록고객수는 1,575만명으로 2009년말(1,117만명) 대비 41.0% 증가하였으며, 스마트폰 기반 모바일뱅킹 등록고객수는 2009.12월 이후 스마트폰 기반의 모바일뱅킹서비스가 도입·확산되면서 1년여 만에 261만명을 기록하였다. 2010년중 모바일뱅킹 이용건수 및 금액은 각각 65.4%, 53.5% 증가한 285만건, 4,087억원을 기록하여 전년에 이어 큰 폭의 증가세를 이어갔다. 스마트폰 기반의 모바일뱅킹 서비스의 이용건수 및 금액은 각각 95만건 및 468억원을 기록하는 등 스마트폰 기반의 모바일뱅킹에 대한 관심과 이용이 전반적으로 증대되는 추세이다〔8〕.

2010.1월 유가증권 전체 거래에 있어 MTS를 통한 비중은 2.46%에 불과했다. 당시 HTS(홈트레이딩시스템)을 통해 주문하는 비중은 74.49%였다. 그러나 2011.9월 MTS 거래비중은 9.91%로 4배이상 증가했고, 일반 HTS는 68.31%로 6%p가량 하락했다.〔9〕 이제는 직장상사 눈치를 보며 HTS를 통해 주식 거래를 하던 직장인들은 MTS를 사용함으로써 직장상사의 눈을 피해 주식투자를 할 수 있는 시대가 되었다.

서비스를 가장 늦게 시작한 모바일단말 결제는 아직 활성화되지 않았지만 통신사와 신용카드사의 제휴 및 NFC(근거리무선통신) 기술의 발달로 모바일 지갑의 현실화 등으로 앞으로 모바일단말 결제시장이 급성장할 것으로 전망된다〔10〕. 일부에서는 NFC 모듈이 탑재된 모바일단말 보급이 확산되면서 모바일단말 결제시장이 급성장하여 향후 신용카드 시장을 대체한다는 주장을 제기하기도 한다.

2.4 모바일단말의 이용 실태

2011.2월 기준 일반인의 스마트폰 가입자 비중은 이동전화 가입자의 18.1%이지만, 금융회사의 경우 모바일오피스를 추진하면서 모바일단말을 임직원에게 지급하는 등의 이유로 임직원 대부분(85%내외)이 스마트폰을 사용한다. 신한금융투자증권 직원의 설문조사에 의하면 가장 많이 사용하는 스마트폰의 기능은 '포털검색' 등 인터넷 이용이었으며, 남성은 금융거래를, 여성은 메신저를 주로 사용하는 것으로 나타났다. 금융거래로는 주로 시세조회(64%), 잔고확인(51%), 증권거래(41%) 순으로 사용 빈도가 높았다. 즉, 증권회사 직원의 10명중 4명은 스마트폰을 통해 증권거래를 하는 것으로 나타난 것이다.

일반인의 경우 2010.11월 기준 스마트폰 이용자는 일평균 1.9시간동안 스마트폰을 이용하고, 92.5%가 스마트폰을 통해 일평균 58.2분 동안 인터넷을 이용한다. 인터넷 이용은 '정보검색'을 위한 것으로 금융회사 직원과 일반인의 이용실태는 크게 다르지 않음을 알 수 있다. 이용 장소로는 이동 중인 교통수단(79.2%)이 가장 많았고, 가정(73.4%), 길거리·공원 등 실외장소(52.6%) 그리고 직장(50.8%) 순이었다. 즉 스마트폰 이용자의 2명중에 1명은 직장에서 스마트폰을 이용한다는 것이다〔11〕.

금융회사 임직원도 스마트폰과 같은 모바일단말을 회사에서 별다른 통제 없이 자유롭게 사용한다. 개인적인 용도로 지인들과 통화하고 메시지를 주고받으며 모바일 커뮤니티를 형성하고 있으며, 업무용으로 고객들과 통화하고 업무관련자들과 정보를 교환하면서 모바일오피스도 사용하고 있다. 문제는 금융회사내 시장성상품의 거래나 직무관련 미공개정보를 취급하는 부서에서 유선전화나 유선망의 전산장비 및 정보통신수단에 대하여는 내부통제를 실시하고 있음에도 모바일단말에 대한 내부통제가 없어 기존 내부통제시스템 및 보안의 홀(hole)이 되고 있다는 것이다.

III. 금융시장 건전성과 금융거래관련 내부통제 현황

3.1 금융시장 건전성과 내부통제의 연관성

금융시장 건전성이란 금융시장을 구성하는 모든 요소가 탈이 없이 튼튼한 상태로서 금융회사의 재무건전성과 함께 금융거래의 안정성과 공정성을 포함하는 개념으로 정의할 수 있다. 파생금융상품에 대한 내부통제 부재로 1995년 파산한 영국 '베어링' 사건과 금융회사의 한 직원이 내부통제 보안시스템을 뚫고 저지른 부정거래로 6조8천억원(49억유로)에 달하는 세계최대규모의 금융사고로 기록된 2008년 프랑스 '소시에테 제네럴(SG)' 사건 등을 계기로 금융시장의 건전성을 유지하기 위하여 내부통제시스템을 지속적으로 강화해 왔다. 우리나라도 내부통제관련 법·규정을 마련하였고 협회차원에서 자율 규제로서 내부통제시스템을 발전시켜 왔다. 최근에는 금융회사 임직원이 직무를 수행하면서 법·규정대로 적절하게 수행하고 있는지 감시하고 모니터링하는 준법감시활동을 보다 효율적으로 수행하기 위해 IT 인프라로 구현하는 IT 컴플라이언스(compliance)가 강조되고 있다. 이는 금융거래 등 금융관련 업무가 IT를 활용함에 따라 준법감시활동도 IT를 이용하여 철저히 대응하기 위함이다.

3.2 금융회사의 금융거래관련 내부통제 현황

본 논문은 모바일단말을 이용하여 금융시장 건전성을 해치는 불건전 영업행위 등에 대한 내부통제 대책과 정보유출 위협에 대한 대응방안을 제시하기 위하여 금융거래(trading) 업무를 영위하는 '자본시장과 금융투자업에 관한 법률'(이하 '자본시장법')에 의한 '금융투자업자'(이하 '금융투자회사')를 중심으로 금융거래관련 내부통제현황과 전산장비 모범규준에 의한 내부통제현황을 파악하고 분석하였다.

3.2.1 시장성상품의 거래에 관한 내부통제

금융회사는 주식, 채권, 파생상품 및 외환 등 시장가격이 계속 변하는 '시장성상품'을 직접 매매하거나 중개한다. 시장성상품의 거래 방법은 상품종류, 거래방법, 거래자, 국내인지 해외인지 또는 장내인지 장외인지 등에 따라 금융권역별로 다양하지만 대부분은 〔그림 1〕과 같이 매수자와 매도자가 중개인(브로커)

〔그림 1〕 PC·메신저·전화를 이용한 시장성상품의 거래방법

을 통해 매수·도 주문을 하고 호가가 맞을 경우 주문이 체결되는 구조이다. 시장성상품은 한국거래소가 개설한 유가증권시장과 파생상품시장 내에서 거래되기도 하지만, 주식이외의 시장성상품 대부분은 장외에서 거래된다. 이런 과정에서 거래 참여자간 호가접수, 주문체결 등 거래관련 정보를 교환하기 위해 전화나 메신저 등의 정보통신수단을 사용한다.

금융회사는 자본시장법 제60조 및 외국환거래법 시행령 제16조에 의거하여 시장성상품의 거래관련 자료를 기록·유지해야 한다. 따라서 금융회사는 시장성상품의 거래에 이용되는 전화의 통화내용을 녹취하고, 이메일·메신저에 대하여는 송·수신 내용을 로깅(logging)하며, 전자금융거래의 경우에도 전자금융거래법 제22조에 의거하여 금융회사는 거래기록을 생성·보관한다.

3.2.2 불건전 영업행위 및 불공정거래 내부통제

금융투자회사 임직원은 자본시장법 제54조에 의거하여 직무관련 미공개정보를 정당한 사유 없이 자기 또는 제삼자의 이익을 위해 이용하면 아니 된다. 직무관련 미공개정보에는 금융투자상품의 주문이나 매매정보, 투자재산의 운용정보, 투자분석보고서, 기업금융정보 등이 있으며, 이러한 정보를 취급하는 임직원은 투자운용인력(딜러, 펀드매니저), 중개인(브로커, 투자상담사), 조사분석인력(애널리스트), 인수업무담당자(IB인력) 등이 있다. 관련부서로는 딜링(트레이딩)센터, 자산운용본부, 법인영업본부, 리서치센터, IB사업부 등이 있을 수 있다.

'불건전 영업행위'는 자본시장법 제71조 등에서 금융투자업 종류별로 규제하고 있는데, 금융투자상품의 주문이나 매매정보 등 직무관련 미공개정보를 이용하여 부당한 이익을 취하거나 손실을 회피할 목적으로 먼저 매수 또는 매도하는 '선행매매'(front running) 행위와 '조사분석자료'를 공표함에 있어 공개되지 아니한 기간 중(공표후 24시간이 경과하기전)에 조사분석대상이 된 금융투자상품을 매매하는 부정행위 등을 의미한다.

'불공정거래'는 '미공개정보이용', '시세조종' 및 '부정거래'로 구분된다. 자본시장법 제174조에서 상장법인의 미공개정보를 이용한 내부자거래를 금지하고 있다. 예를 들어 금융투자회사 임직원이 기업금융이나 법인영업을 하면서 상장법인 내부자로부터 미공개중요정보를 전달받은 경우에도 '미공개중요정보 이용행위 금지'의 대상자가 될 수 있다. 제176조는 상장증권이나 장내파생상품의 매매가 성황인 것으로 오인하게 하는 위장거래, 매수·도를 서로 짠 후 거래하는 통정거래, 권리이전을 목적으로 하지 않는 가장매매 등 시세조종(일명 '작전') 행위를 금지하고 있다. 제178조는 금융투자상품의 거래와 관련하여 부정한 수단, 계획 또는 기교를 사용하는 행위 및 허위나 오해유발(misleading) 행위인 '부정거래'를 금지하고 있다. 특히 거래나 시세의 변동을 도모할 목적으로 풍문의 유포, 위계(僞計)의 사용, 폭행 또는 협박을 하지 아니하도록 규정하고 있다.

금융투자회사는 자본시장법, 금융투자업규정 및 금융투자협회의 '영업 및 업무에 관한 규정'과 '표준내부통제기준'에 의거하여 자체 내부통제기준을 마련하고 준법감시인의 컴플라이언스 활동으로 내부통제를 하고 있다.

자본시장법 제63조에 의하면 금융투자회사 임직원은 금융투자상품을 매매할 경우 자기의 명의로 하나의 증권회사를 선택하여 하나의 계좌를 통해 거래해야 함을 원칙으로 하고 있다. 이에 증권회사는 사내에서 다른 증권회사의 HTS에 접속할 수 없도록 하고 있으며, 자사 HTS에 접속하더라도 임직원 본인 명의의 계좌에만 접속 가능하도록 내부통제시스템을 구축·운영하고 있다. 또한 금융투자회사 임직원은 금융투자상품 매매결과를 분기별(직무관련 미공개 정보를 취급하는 임직원은 매월) 준법감시인에게 통지해야 한다. 일부 증권회사에서는 직무관련 미공개정보를 취급하는 부서에 대해 HTS 접속을 근본적으로 차단하는 경우도 있다.

3.2.3 전산장비 모범규준에 의한 내부통제

금융거래관련 내부통제는 전산장비 모범규준의 시행에 따라 한층 강화되었다. 전산장비 모범규준은 '전산장비' 및 '정보통신수단'의 사용·관리 및 기록·유지에 대한 기준과 보안유지를 위한 내부통제절차 등을 정함으로써 불법적인 자료유출 및 루머확산을 방지하고 건전한 영업질서를 확립함을 목적으로 하고 있다.

〔표 1〕 전산장비 및 정보통신수단에 대한 내부통제 요구사항

구 분		내부통제 요구사항	기술적 수단 (솔루션)
전산장비	전자문서 (파일)	· 전자문서 암호화 · 복호화 로그기록 3년 이상 유지	· 문서DRM
	모니터 (화면)	· 화면 캡처(capture) 및 출력(print) 금지	
	출력물 (인쇄)	· 워터마킹(watermarking) 등 출력물 제어	
	CD, USB 등	· 승인받지 않은 보조기억 매체에 대한 '쓰기' 기능 불가	· 문서DRM · 보안USB
정보통신수단 (이메일·메신저 등)		· 업무용은 별도로 지정, 나머지는 차단 또는 발신 금지 · 송·수신 내용이 담긴 로그 기록은 3년 이상 보관	· 방화벽, IDS, IPS 차단 · 로그 아카이빙

전산장비 모범규준은 〔표 1〕과 같이 내부통제 요구사항을 구체적으로 명시하고 있다. 아울러 영업비밀이나 고객정보의 유출, 시장루머의 유포 등 금융회사 임직원이 해서는 아니 되는 행위에 대한 규제를 포함하고 있다. 특히 업무용으로 지정되지 않은 정보통신수단은 수신 이외의 목적으로 사용하면 아니 되도록 하고 있다. 금융회사는 전산장비 모범규준의 시행에 따라 문서DRM(디지털저작권관리), 보안USB, 로그아카이빙(log archiving) 시스템 등 기술적 수단을 구축해야만 한다. 시스템 구축과 관련된 사항은 6개월간의 준비기간을 거쳐 2011.10월부터 시행하였다〔2〕.

3.3 소결론

금융회사는 시장성상품 거래 자료의 기록, 불건전 영업행위 등에 대한 내부통제 및 전산장비 모범규준에 의한 내부통제시스템을 갖추고 있지만 이들은 유선망 중심으로 이뤄지고 있다. 따라서 금융회사 임직원이 무선매체인 모바일단말을 자유롭게 사용할 경우 현행 내부통제시스템을 우회하거나 회피함으로써 시장성상품 거래 자료의 기록이 누락될 수 있고, 불건전 영업행위나 불공정거래가 발생하거나 내부정보가 유출될 가능성이 상존한다. 즉 모바일단말에 대한 적절한 내부통제와 보안대책을 적용하지 않는다면 금융회사의 현행 내부통제시스템을 무너뜨릴 수 있는 커다란 위협이 될 수 있다.

IV. 금융회사 내부통제를 약화시키는 모바일 단말 위협

4.1 시장성상품 거래관련 자료의 기록 누락

금융회사는 시장성상품을 거래함에 있어 〔표 2〕와 같이 유선전화 녹취, 유선망의 이메일·메신저에 대해 로깅 등의 방법으로 내부통제하고 있으나 휴대전화에 대하여는 한국씨티은행 등 일부 외국계은행만이 사용을 금지하고 있을 뿐 대부분 금융회사는 휴대전화는 물론 스마트폰과 같은 모바일단말에 대한 내부통제는 전혀 이뤄지지 않고 있다.

따라서 딜링(트레이딩)센터와 같은 부서에서 시장성상품 거래시 휴대전화나 모바일단말을 이용하게 될 가능성이 커지고 있다. 만약 시장성상품을 거래할 경우 모바일단말을 사용하면 녹취나 로깅이 되지 않아 거래관련 자료의 기록이 누락된다. 이는 법·규정을 위반하는 행위로 금융거래에 착오나 오류가 발생할 경우 거래당사자간 분쟁을 해결할 수 있는 근거자료가 남지 않아 금융거래의 건전성을 훼손하게 된다. 또한 금융회사 임직원이 거래기록을 남기지 않을 목적으로 휴대전화나 모바일단말을 사용할 경우 불건전 거래의 위험이 증가하여 금융거래의 공정성을 훼손할 우려도 있다.

4.2 불건전 영업행위 및 불공정거래의 증가

금융회사의 불건전 영업행위는 일반인에게 잘 드러나지 않지만 금융당국의 검사과정에서 종종 적발된다. 펀드 운용회사인 자산운용사 직원이 기업인수 정보를 미리 알고 해당 주식을 선취매한 후 매도하여 2배의 시세차익(2억6천만원)을 챙기거나, 증권회사 직원이 합병관련 미공개정보를 이용하여 지인으로부터 해당 주식의 매매주문을 수탁(230회, 17억원) 받는 사례 등이 있었다.

2010.11.11일 발생한 '도이치 옵션쇼크' 사건으로 옵션 만기일인 당일, 장 막판 2조4천억원 가량의 매도 주문이 쏟아졌고 코스피 주가지수는 전일대비 53.12p(2.30%) 급락하는 일이 발생하였다. 이 사건은 한국 도이치증권, 도이치뱅크 홍콩지점 등이 관여하여 자본시장법상 현물과 선물을 연계하여 증권시장을 교란시킨 불공정거래 행위이다. 이들은 스마트폰 메신저를 통해 범행을 모의하는 등 사전에 철저하게 준비한 것으로 보인다. 또한 이 사건 과정에서 한국 도이치증권 임원은 도이치뱅크 홍콩지점의 대규모 현물 매도 정보를 이용해 한국 도이치증권 법인자금으로 풋옵션을 매매한 것으로 나타났는데 이는 고객 주문정보를 이용한 선행매매로 간주될 수 있는 부분이다〔12〕.

2011.6.27일 감사원은 대한지방행정공제회 등 금융공기업의 임직원들이 근무시간 중 개인적으로 주식거래를 한 사실을 대거 적발했다고 밝혔다. 대한지방행정공제회의 주식운용부서 직원은 공제회 투자정보를 이용해 차명계좌로 2,087회에 걸쳐 주식을 거래해 1억1838만원의 부당이득을 챙긴 것으로 밝혀졌다. 대한지방행정공제회가 매수 예정인 종목(투자재산의 운용정보)을 미리 산 뒤 주가가 오르면 파는 선행매매를 한 것이다〔13〕.

모바일단말에 대한 내부통제의 부재로 금융회사 임직원은 타인명의로 MTS를 이용해 직접 주식거래를 할 수 있는 만큼 금융회사 임직원이 직무관련 미공개정보를 이용하여 선행매매 등 불건전영업행위를 하게 될 가능성은 더욱 증가하게 되었다.

2011년 1/4분기 금융감독원의 불공정거래 사건의 처리현황은 〔표 3〕과 같다. 부정거래행위, 시세조종 및 미공개정보이용 사건은 36건으로 전체 처리사건의 61.0%나 차지한다. 특이점은 부정거래행위 사건이 14건으로 전년 동기(2건) 대비 12건(600.0%) 증가하였다는 것이다〔14〕. 이는 모바일단말과 같은 통제되지 않는 정보통신수단이나 SNS와 같은 모바일 커

〔표 2〕 금융회사별 정보통신수단 통제현황

구 분	은 행	증 권	보 험
유선전화	○	○	○
이메일·메신저	○	○	○
휴대전화	△	×	×
모바일단말	×	×	×

〔표 3〕 혐의유형별 금융감독원의 불공정거래 조사처리현황

혐의유형	'09년	'10년	'10.1/4 분기	'11.1/4 분기
미공개정보이용	49	53	15	13 (22.0)
시세조종	45	49	22	9 (15.3)
부정거래행위	21	21	2	14 (23.7)
대량·소유주식보고	57	44	13	13 (22.0)
단기매매차익취득 등	4	11	3	1 (1.7)
무혐의	23	3	1	9 (15.3)
계(단위 : 건, %)	199	201	56	59 (100.0)

뮤니티를 악용하여 증권시장에 시세의 변동을 도모할 목적으로 악성루머를 유포하는 등 허위나 오해유발 행위가 증가했기 때문인 것으로 풀이된다[15].

2011.3.15일에는 일본 원전 폭발로 인한 방사능이 한국에도 상륙할 것이라는 루머가 증권시장에 퍼지면서 코스피 주가지수가 장중 한때 전일대비 72.45p(3.7%)까지 폭락하는 사건이 발생했다. 금융당국은 투기세력이 풋옵션을 매입한 후 의도적으로 루머를 퍼뜨렸다는 의혹을 제기했었는데 이 사건은 허위사실을 유포하여 증권시장을 교란한 대표적인 사례이다[16].

금융회사 임직원이 직무관련 미공개정보를 외부인과 공유·결탁하여 불공정거래를 저지르거나 연루되는 경우가 종종 발생하는데 2008년부터 2010년까지 3년간 불공정거래 조치자 중 금융회사 임직원은 100명 중 4명 수준이었다. 이는 공정한 금융거래가 되도록 관리해야 할 자가 불공정거래에 직접 가담해서 금융거래의 신뢰를 저하시킨다는 점에서 결코 무시해서는 아니 된다. 모바일단말의 보급이 급속히 확대되고 있어 금융회사 임직원은 내부통제가 이뤄지지 않는 모바일단말을 이용하여 불공정거래에 관여할 위협이 점차 고조되고 있다. 또한 모바일단말이 불공정거래에 이용되더라도 기록이 남지 않아 범행 근거가 은폐될 수 있는 문제점도 함께 발생한다.

4.3 금융회사의 내부정보 유출

금융회사는 고객의 개인정보(성명, 주민등록번호 및 영상 등을 통해 개인을 알아 볼 수 있는 정보), 금융정보(금융자산, 신용등급 및 금융거래의 내용에 대한 정보 또는 자료, 대출정보, 보증정보 등[17]) 및 직무관련 미공개정보 등의 내부정보를 보유·관리하고 있다. 이들 내부정보는 모바일단말을 통해 내부로부터 외부로 유출될 수 있으며, 또한 모바일오피스 환경의 취약점을 해킹하는 등 모바일단말의 외부요인에 의해 유출될 수 있다.

4.3.1 내부로부터의 정보유출

금융회사 내부정보는 임직원의 실수, 개인정보 관리소홀, 임직원의 고의 등에 의해 유출될 수 있다. 실제로 금융투자상품 소개 자료를 보내야 하는데 그 상품에 가입된 고객명단을 이메일로 전송하거나, 고객정보가 저장된 엑셀파일을 USB에 복사하여 유출한 사례가 있다[18]. 또한 금융회사 직원이 해외고객의 주문내역(종목명, 매매구분, 수량, 가격)을 개인 노트북의 메신저로 반복적으로 전달한 행위가 금융당국의 검사과정에서 적발되기도 하였다.

그래도 다행스럽게 전산장비 모범규준의 시행에 따라 유선망에서의 내부정보의 유출경로가 상당부분 통제될 것이란 점이다. 그러나 모바일단말에 대한 내부통제는 미흡하기 때문에 모바일단말을 잘못 사용하거나 악용할 경우 금융회사 내부정보의 유출 가능성은 상당히 높다고 할 수 있다. 금융회사 전산장비와 모바일단말을 연결(동기화)한 후 모바일단말에 내부정보를 저장하여 유출할 수 있으며, 모바일단말을 무선 AP(access point)로 이용할 수 있는 테더링(tethering) 기술을 사용할 경우 금융회사 전산장비를 무선으로 인터넷에 연결하여 정보를 유출할 수 있다. 물론 모바일단말을 통해 직접 접근 가능한 내부정보는 곧바로 유출할 수 있다[19].

4.3.2 외부요인에 의한 정보유출

금융회사가 모바일오피스를 운용함에 있어 모바일단말은 다양한 무선접속환경의 개방성, 휴대성 및 저성능 등의 특성으로 기존 PC환경의 보안 위협에 더해 새로운 보안위협에 노출되어 있다[20]. 모바일오피스 접속이 가능한 모바일단말을 분실·도난당하거나, 악성코드가 내재된 애플리케이션을 설치했을 경우 해킹 등의 외부요인에 의해 내부정보가 유출될 수 있다는 것이다.[19]

외부요인에 의한 보안위협은 무선인터넷 서비스 구조에 따라 모바일단말, 애플리케이션 및 플랫폼, 네트워크 및 서버 구간으로 크게 구분할 수 있다. 모바일단말 보안은 단말의 도난·분실로 인하여 단말에 저장된 내부정보가 유출되거나 타인이 모바일오피스에 접속하여 내부정보를 유출하는 위협을 말하며, 애플리케이션 및 플랫폼 보안은 모바일단말이 악성코드에 감염되거나 해킹되어 내부정보가 유출될 위협을 말한다. 네트워크 및 서버 보안은 무선구간에서 패킷이 가로채기(packet sniffing)되어 내부정보가 유출되거나 단말을 경유하여 금융회사 서버시스템까지 위협받는 것을 말한다[6].

기존의 PC와 같은 유선망 중심의 내부통제수단이나 보안대책만으로는 대응하기 어렵기 때문에 모바일단말에 대한 내부통제와 보안에 대한 체계적인 연구를 통해 실행 가능한 대응방안을 마련할 필요가 있다.

V. 대응방안

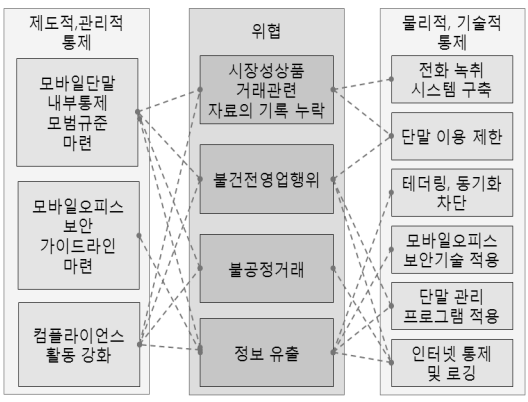
금융회사는 전산장비 모범규준에 따라 유선망의 전산장비 및 정보통신수단에 문서DRM, 보안USB, 이메일·메신저 로깅, 불필요한 인터넷 차단 등 내부통제 수단을 우선 적용하여 정착시켜야 한다. 아울러 모바일단말에 대한 내부통제수단 및 보안대책을 강구해야 할 것이다. 이를 위해 모바일단말 내부통제 모범규준과 모바일오피스 보안 가이드라인이 마련되어야 하고, 컴플라이언스 활동의 강화 등 제도적·관리적 통제가 이뤄져야 할 것이다. 또한 모바일단말로 발생하는 문제점을 해결하기 위해 휴대전화 녹취시스템 구축, 단말 이용 제한, 테더링·동기화 차단 등 물리적·기술적 통제방안도 함께 강구해야 할 것이다.

본 논문에서 문제점으로 제시한 모바일단말의 위협은 〔그림 2〕와 같이 여러 가지 대응방안과 상호 연관성을 갖는다. 따라서 기존의 내부통제수단은 물론 모바일단말의 위협에 대한 새로운 내부통제수단 및 보안기술 등을 효율적으로 접목시켜 적용할 필요가 있다.

5.1 제도적 · 관리적 통제

5.1.1 모바일단말 내부통제 모범규준 마련

모바일단말의 대중화로 금융회사는 그동안 갖춘 내부통제시스템이 약화되거나 한 번에 무너지게 될 심각한 위협에 처해 있음에도 불구하고 모바일단말 위협에 적극적으로 대처하지 않고 있다. 금융당국은 모바일단말 위협에 대한 내부통제의 필요성에 대하여는 인식을 하고 있으나 실행에는 옮기지 못하고 있다. 따라서 금융당국은 우선적으로 금융회사 임직원이 사용하는 모바일단말에 대한 내부통제 모범규준을 마련해야 할 것이다. 물론 회사소유의 전산장비와 회사의 정보통신망을 대상으로 전사적으로 적용하고 있는 전산장비 모범규준을 개정하거나 적용의 확대를 통해 시행할 수도 있으나 개인 모바일단말까지 내부통제를 하고 부서별로 통제 수준을 차등화 하는 등 모바일단말의 특성으로 고려할 경우 별도로 제정하는 것이 바람직해 보인다.



〔그림 2〕 모바일단말 위협과 대응방안의 연관성

그럼에도 모바일단말에 대한 내부통제 기본원칙은 모바일단말이 노트북과 같은 전산장비라는 인식에서부터 시작해야 할 것이다. 외부 전산장비에 대해 NAC(네트워크 접근통제)를 하는 것처럼 개인 모바일단말에 대해서도 금융회사 내부망에 연결을 차단하고, 업무시간 중에는 MTS는 물론 인터넷서비스 일체의 사용을 금지하며, 개인 모바일단말을 업무용으로 사용하지 못하도록 내부통제 규준을 마련해야 한다.

업무용 모바일단말에 대하여는 본래의 취지에 맞도록 금융회사 외부에서만 모바일단말을 사용하도록 하며 금융회사 내부에서는 개인 모바일단말에 준하여 내부통제를 하도록 한다. 시장성상품의 거래시 모바일단말을 사용하기 위해서는 반드시 휴대전화의 통화내용을 녹취할 수 있는 시스템을 구축하도록 하고, 모바일단말을 통한 이메일·메신저 등 정보통신수단에 대해서는 송·수신 내용을 로깅하도록 제도적 방안을 마련할 필요가 있다. 또한 MTS을 통해 주식거래를 할 수 없도록 해야 할 것이다.

모바일오피스의 적용범위가 확대되면 PC에서와 같이 모바일단말에도 내부통제수단을 임직원 개인마다 각각 다르게 적용할 수 있어야 할 것이다. 그래야만 PC에서와 같이 모바일단말을 활용하여 모든 업무를 처리할 수 있게 되어 진정한 FMC 환경을 구축할 수 있는 것이다.

금융회사는 시장성상품을 거래하는 부서에 들어갈 경우 모바일단말을 휴대하지 않도록 물리적인 대응수단은 퀵윈(quick win)전략으로서 즉시 적용할 수 있으며, 직무관련 미공개정보를 취급하는 부서에 대하여는 일반부서보다 내부통제수준을 높게 적용하는 등 금융회사 조직과 사람에 따라 내부통제를 차등화하는 전략을 구사해야 한다. 따라서 금융당국은 모바일단말의 활용성과 내부통제의 목적성을 모두 고려하여 금융회사가 자율적으로 내부통제수단을 강구할 수 있도록 금융회사의 의견을 수렴하여 모바일단말 내부통제 모범규준을 조속히 마련하여 시행해야 할 것이다.

5.1.2 모바일오피스 보안 가이드라인 마련

모바일오피스의 적용범위는 점차 확대될 것이고 모바일오피스를 안정적으로 이용하기 위해서는 강력한 보안정책을 적용해야 한다. 왜냐하면 모바일오피스에 대한 해킹의 증가와 악성코드의 확산으로 모바일환경에서의 보안사고 위협이 심각한 문제로 제기되고 있기 때문이다. 모바일오피스 보안위협은 금융회사의 보안위협과 직결되며 보안사고가 발생할 경우 금융회사에게 커다란 피해를 주게 된다. 그러나 모바일오피스에 대한 보안 가이드라인은 아직까지 마련되지 않았다.

모바일환경은 PC에 비해 훨씬 다양하여 유선망에서 고안된 많은 보안지침들만으로는 대처할 수 없다. 따라서 금융회사가 모바일오피스를 추진하는데 있어 〔표 4〕와 같이 모바일단말, 애플리케이션 및 플랫폼, 네트워크 및 서버 등 영역별로 보안 취약점 및 대응방법을 포함한 모바일오피스 보안 가이드라인을 조속히 마련하여 시행할 필요가 있다.

〔표 4〕 모바일오피스 보안 가이드라인〔6〕〔21〕

구 분	취약점	대 응 방 법
단말 보안	도난, 분실, 악성 앱	· 원격 잠금 기능 및 원격 파일삭제 기능 등 물리적 보안책 마련 · ID/PW, 단말인증, 공인인증, OTP 등 복합인증방식 적용 · 업무와 인터넷을 별로 플랫폼 기반으로 실행하는 단말 가상화 솔루션 채택 · 업무 등 중요자료는 모바일단말에 저장 금지 · 외부출력·화면캡처 금지 · 문서DRM 적용 · PC나 서버에서 모바일단말 사이의 데이터 전송 통제(동기화 제한) · 테더링 및 카메라 기능 제한 등
애플리케이션 및 플랫폼 보안	악성 앱, 피싱, 바이러스, 악성코드, 시스템 잠금해제, 키보드 해킹	· 안전한 S/W 유통체계 환경조성을 위한 개발·판매·사용 단계에서의 정보보호체계 확립 · 악성코드에 대비한 안티 바이러스 솔루션 도입 · 악성 애플리케이션에 대한 정보 공유 및 응용프로그램 검증강화로 안전한 유통환경 조성 · 응용프로그램의 정기적 원격 패치 및 패치관리(PMS) 솔루션 제공 · 플랫폼에 대한 보안 취약점 및 업데이트 공지 · 취약점 연구 및 침해사고대응센터 운영 · 안전한 사용 방법 등에 대하여 이용자 인식 제고 등(교육)
네트워크 및 서버 보안	도청, 변조, DDoS 공격, 네트워크 무단접속, 서버 해킹	· 모바일 플랫폼은 상용 인터넷망을 경유하지 않고 이동통신망에서 전용회선으로 직접 연결 · 종단간(E2E) 데이터 및 음성에 대해 암호화 기능 및 VPN(가상사설망) 적용 · 침입차단, 침입탐지, 유해트래픽 탐지 등 보안장비를 구축·운영 · 침해사고대응센터 운영 · 모바일단말에서 내부 업무서버로의 직접 연결은 차단 · 외부망과 내부망을 분리할 수 있는 릴레이 연계서버 구축 · 릴레이 연계서버는 외부 연동서버와 내부 연동서버를 물리적으로 구분

5.1.3 컴플라이언스 활동 강화

5.1.3.1 금융회사의 자체 컴플라이언스 활동 강화

모바일단말 위협에 대하여 금융회사가 스스로 임직원의 모바일단말 이용관련 컴플라이언스 활동을 강화해야 한다. 내부통제를 효율적으로 하기 위해서 내부통제 전산시스템을 개발하여 IT 컴플라이언스를 갖출 필요가 있다. 임직원의 윤리의식에 의존하는 선언적 내부통제기준은 사문화되기 쉽기 때문이다. IT를 활용한 내부통제활동은 임직원의 의식을 전환시켜 내부통제기준을 직장 문화로 흡수·정착시킬 수 있는 장점이 있다. 다만, 시스템 구축비용이 소요되므로 위협이 큰 부서부터 적용하는 방법 등으로 선택과 집중이 필요하며, IT 컴플라이언스 구현을 위하여 금융회사간 협의를 통해 세부기술 및 업무 프로세스 등을 표준화할 필요가 있다〔22〕.

아울러 내부통제 및 보안의 중심은 사람이므로 금융회사 임직원을 대상으로 하는 윤리교육과 보안교육을 내실 있게 실시해야 한다. 불건전 영업행위나 내부정보 유출 행위는 임직원의 윤리의식의 부족으로부터 시작하기 때문이다. 모바일단말은 보안사고 예방관점에서 사용자의 주의와 관리가 절실히 요구되므로 IT 조직과 협력하여 모바일단말의 올바른 사용방법에 대한 교육을 실시한다. 또한 금융감독원이 2011.2월에 마련한 '스마트폰 금융거래 10계명'과 같은 모바일단말에 대한 보안 가이드북 등 최신 보안관련 자료를 임직원에게 수시로 제공하여 모바일단말을 보다 안전하게 사용할 수 있도록 한다.

5.1.3.2 금융당국의 검사 강화

금융당국은 금융회사가 모바일단말에 대한 내부통제기준을 적정하게 마련하고 있는지, 불건전 영업행위

및 불공정거래 방지를 위한 내부통제 운영실태 및 윤리·보안 교육 실시현황 등에 대한 검사를 강화해야 한다. 특히 금융회사에서 마련한 내부통제 대책들이 실제로 적정하게 운용되고 있는지 중점적으로 살펴봐야 할 것이다.

모바일단말에 대한 내부통제 활동이 미흡한 경우 경영실태평가 등급산정에 불이익을 주는 등 금융회사 경영실태평가시 모바일단말에 대한 내부통제 점검결과를 반영하도록 한다. 또한 모바일단말에 대한 내부통제 모범사례를 발굴하여 다른 금융회사와 공유할 수 있도록 한다. 특히 제2금융권 금융회사의 경우 제1금융권 금융회사에 비해 상대적으로 취약하므로 은행이나 증권회사에 잘 갖춰진 내부통제시스템을 제2금융권과 공유하고 현실에 맞도록 최적화하여 적용할 수 있도록 컨설팅할 필요가 있다.

5.2 물리적 · 기술적 통제

5.2.1 휴대전화의 통화내용 녹취시스템 구축

영국 FSA(금융감독청)은 주가조작 등 시장교란 행위를 막기 위해 은행과 헤지펀드 종사자들 및 증권거래인들을 대상으로 휴대전화 통화내역을 녹음·보관하도록 의무화하여 2011.11월부터 시행한다. 이는 금융거래관련 유선전화 통화내역 녹취 의무를 명시한 기존의 규정을 무선전화로까지 확대한 것이다[23]. FSA는 단순히 휴대전화를 업무용으로 사용할 수 없도록 사용 제한하는 것만으로는 컴플라이언스를 위해 충분한 조치가 아니라고 거론함에 따라 영국 금융회사들은 휴대전화에 대한 녹취 시스템을 도입해야 할 것이다[24].

우리나라도 시장성상품의 거래 등 직무관련 미공개정보를 취급하는 부서에서 휴대전화를 업무용으로 사용할 때 통화내용을 녹취하도록 의무화하여 금융회사가 휴대전화에 대한 전화녹취 시스템을 구축하도록 해야 할 것이다. 동시에 개인 휴대전화나 모바일단말과 같이 녹취되지 않는 휴대전화가 업무용으로 사용되지 않도록 모바일단말에 대한 통제가 함께 이뤄져야 한다.

5.2.2 주요부서 모바일단말 이용 제한

모바일단말은 휴대전화 기능 외 MTS 및 인터넷 서비스를 이용할 수 있다. 때문에 선행매매와 같은 불건전 영업행위 및 내부정보의 유출을 방지하기 위하여 직무관련 미공개정보를 취급하는 부서에서 모바일단말을 자유롭게 사용하는 것을 제한할 필요가 있다.

금융회사 출근시 또는 부서에 출입할 때 모바일단말을 반납토록 하여 내부에서 모바일단말을 사용하지 못하게 반출·입 통제를 할 수 있다. 그러나 이러한 물리적인 방법보다는 업무시간에는 자동으로 모바일단말이 작동되지 않도록 제어하는 기술적인 접근이 바람직하다. 따라서 모바일단말관련 보안기술을 적용하여 개인별 또는 부서 그룹별로 차등화된 보안수준을 적용할 수 있도록 해야 하겠다.

5.2.3 모바일단말 테더링 및 동기화 차단

금융회사가 모바일단말에 대한 기술적 보안대책을 적용함에 있어 모바일단말의 테더링과 동기화를 가장 우선적으로 차단해야 할 것이다. 모바일단말 테더링은 내부망을 거치지 않고 외부 인터넷에 직접 접속함으로써 내부 보안정책을 우회하게 된다. 따라서 모바일단말의 테더링을 전사적으로 차단하고 내부 전산장비에 테더링 프로그램의 설치를 막아야 한다. 또한 유선케이블 또는 블루투스와 같은 무선으로 내부 전산장비와 모바일단말을 동기화하면 내부 전산장비에 있는 정보가 모바일단말에 저장되어 유출될 수 있기 때문에 내부 전산장비와 모바일단말의 동기화를 함께 차단하도록 해야 한다.

5.2.4 모바일오피스 환경의 보안기술 적용

금융회사 일부부서에서는 모바일단말의 이용을 제한할 필요가 있지만 외부에서는 모바일오피스를 통해 수행하길 원하기 때문에 모바일오피스의 적용범위가 중요 정보를 다루는 영역까지 점차 확대되고 있다. 따라서 모바일오피스 환경의 보안위협을 방어하기 위한 기술적인 보안이 강조되고 있다.

모바일오피스 환경의 정보보호 아키텍처를 구성함에 있어 보호대상을 모바일단말, 응용프로그램과 플랫폼, 네트워크 및 서버 등 4개로 구분하고, 보안기능은 사용자인증, 정보유출방지(기밀성), 접근통제(무결성), 침해사고 예방(가용성), 모니터링 등 5개로 구분하여 적용 가능한 보안기술을 〔표 5〕와 같이 조사·분류 하였다. 금융회사는 각 영역별 보안기술을 선택·적용하여 회사에 적합하면서 효과적인 정보보호 아키텍처를 구축해야 할 것이다.

〔표 5〕 모바일오피스 환경의 보안기술 적용 예시〔18〕

구분	모바일단말	응용 프로그램 및 플랫폼	네트워크	서버
사용자 인증	비밀번호, 패턴 및 지문 인식	계정 및 비밀번호, PKI, OTP	장치(MAC 주소) 인증	계정 및 비밀번호
정보 유출 방지 (기밀성)	중요파일 저장금지, 스트리밍 뷰어 적용, 파일암호화, DRM, 테더링·카메라 차단	데이터 암호화 , 메일·메시지 암호화, 데이터 발송 제한	VPN, SSL 암호화, 메일·메신저 차단, 유해트래픽 통제	DRM, 백업 및 복구, DB 암호화
접근 통제 (무결성)	단말잠금 (원격잠금), 원격데이터 삭제, 동기화차단	앱 방화벽, 앱 암호 설정, 위변조 및 피싱방지	침입차단, NAC	DB 권한관리, 액티브 디렉토리 (AD)
침해 사고 예방 (가용성)	백신/ 악성코드 방지, 주기적백업, 피싱 유의	공인된 마켓 이용, 검증된 앱만 설치, 침해사고 공동대응	IDS, IPS, Anti-DDoS, 무선침입 방지 (WIPS)	릴레이 연동서버의 내부·외부 분리 구축, 취약점 점검
모니터링	보안정책 적용 실태, API 적용 상태, 전화 녹취	업무용 앱 자동 설치, 설치된 앱 상태, 메일·메신저 로깅	N/W접근 로그 분석, 기업보안 관리 (ESM)	서버·DB 로그분석, 서버 인사이트 매니저 (SIM)

한편 모바일단말의 특성상 분실·도난, 악성코드, 비인가 AP 접속, 비인가 사용자에 의한 권한 도용, 내부 인트라넷 접속 등 여러 가지 보안위협이 발생하는데 보안기술을 각각 적용하다보면 효율성이 저하될 수 있으므로 이들 위협에 최적화한 통합보안 솔루션을 적용하는 것도 대안이 될 수 있을 것이다.

5.2.5 모바일단말 관리 프로그램의 적용

금융회사에서 모바일단말의 무분별한 사용은 금융거래관련 내부통제시스템을 약화시킬 수 있으므로 모바일단말의 기능을 제어하거나 모바일단말의 상태를 점검하여 모니터링할 수 있어야 한다. 네트워크나 서버 영역보다 모바일단말이나 애플리케이션 영역에서 보안사고가 발생할 가능성이 높으므로 모바일단말의 내부통제와 보안을 강화해야 한다. 최근에는 회사 건물에 들어서면 카메라를 차단하거나 테더링 등 모바일단말의 기능을 제어할 수 있는 MDM(모바일단말 관리) 프로그램이 등장하고 있는데 주요 기능은 〔그림 3〕과 같다.

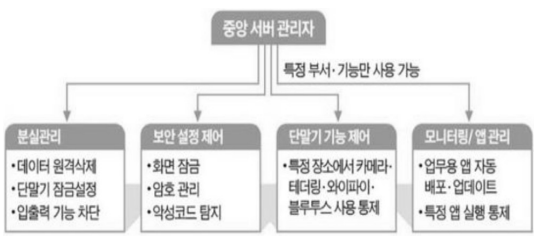
이동통신사는 현재 착신전환이나 인터넷차단 서비스를 하고 있으며, MDM를 통해 모바일단말의 기능을 제어할 수 있으므로 금융회사는 모바일단말을 출결카드와 연계하여 회사에 근무하고 있는 경우에는 휴대전화를 유선전화로 착신전환하고, 인터넷, 테더링, 블루투스 및 카메라 기능 등을 차단하도록 모바일단말 내부통제시스템을 구현할 수 있을 것이다.

5.2.6 모바일단말 인터넷서비스 통제 및 로그 기록

금융거래관련 내부통제를 위해 모바일단말의 이용제한이나 단말기 기능제어와 같은 기술적인 수단을 강구하는 것만으로 현재에는 충분하다 할 수 있을 것이나 향후 모바일오피스 환경에서 시장성상품의 거래를 하거나 직무관련 미공개정보를 다루는 일을 하게 된다면 모바일단말에서 휴대전화 녹취는 물론 이메일·메신저 등 정보통신수단을 차단하거나 발신을 제한할 수 있어야 하며, 컴플라이언스 목적으로 모바일단말을 이용한 정보통신수단의 사용내역 등을 로깅할 수 있어야 할 것이다.

VI. 결 론

우리들의 일상생활에 깊숙이 파고든 모바일단말은 생산성 향상과 경쟁력 확보를 위한 '스마트모바일 이노베이션'임에는 틀림없다. 모바일단말은 전자금융에 활용되어 모바일뱅킹이 인터넷뱅킹을, MTS가 HTS를 각각 대체하고 있고 모바일오피스에 활용되어 업무의 효율성을 높이고 있다. 그러나 모바일단말의 위협에 대한 대비는 미흡한 편이다. 모바일단말은 금융업종사자가 불건전 영업행위 등에 연루될 가능성을 증가시켰으며, 금융회사에게 고객정보의 유출 등 새로운



〔그림 3〕 모바일단말 관리(MDM)의 주요 기능〔25〕

보안위협이 발생하고 있다. 따라서 금융회사는 불건전 영업행위 등에 대한 내부통제 문제와 모바일단말의 보안문제를 해결하면서 모바일단말의 업무 활용성을 점차 높여야 할 것이다.

모바일단말의 보안위협은 공격패턴이 점차 스마트해질 것이므로 정부와 산학 연계로 종합적이고 체계적으로 대응해 나가야 한다. 금융회사는 모바일 보안 솔루션을 지속적으로 업그레이드해야 하며, 모바일단말에 대한 컴플라이언스를 위한 내부통제장치를 마련해야 한다. 이를 위해 모바일단말에서 이용할 수 있는 서비스를 차단하거나 제한하고, 사용내역을 기록하는 등의 내부통제시스템의 개발도 이뤄져야 한다. 또한 금융회사 종사자 모두가 모바일단말 내부통제와 모바일보안에 대하여 인식을 같이 하고 보안대책을 준수할 수 있도록 보안사고 예방활동에 중점을 두어야 할 것이다.

본 논문은 금융투자회사를 중심으로 모바일단말 사용과 관련되는 예상 문제점을 파악하였고, 이에 따른 제도적·기술적인 대응방안을 모색하였다. 제도적 방안으로는 모바일단말 내부통제 모범규준 마련, 모바일오피스 보안가이드라인 마련 및 컴플라이언스 활동 강화 등을 제시하였다. 기술적 방안으로는 휴대전화 통화내용 녹취시스템 구축, 모바일단말 이용제한, 테더링과 동기화 차단, 모바일오피스 환경의 보안기술 적용, MDM 적용 및 모바일단말 인터넷서비스 통제 및 로그 기록 등 금융회사가 향후 적용해야 할 대응방안을 제시하였다.

금융업에 있어 모바일단말 위협과 대응방안을 제시함으로서 금융회사의 고객정보를 안전하게 보호하고 시장성상품 거래의 투명성을 제고하며, 금융업 종사자의 불건전 영업행위 및 불공정거래를 방지하여 신뢰성을 확보하고 증권시장에서 근거 없는 악성루머의 유포가 근절되어 증권시장의 공정성 확립에 기여할 것으로 기대한다. 앞으로도 모바일 금융업무의 발굴과 함께 모바일단말 위협에 대한 지속적인 연구로 모바일 금융산업의 혁신에 적극 대응할 수 있도록 계속 노력해야 할 것이다.

참고문헌

〔1〕 윤한성, 내부보안위협과 정보유출방지(내부자 정보유출의 기술적 대응방향), 한국학술정보, pp. 35-36, 2009년 4월.

〔2〕 금융감독원, "「금융회사의 정보통신수단 등 전산장비 이용관련 내부통제 모범규준」 마련 및 시행," 금융감독원 보도자료, pp. 1-3, 2011년 3월 10일.

〔3〕 방송통신위원회, "Smart Korea 강국 도약을 위한 스마트 모바일 시큐리티 종합계획," pp. 1-8, 2010년 12월.

〔4〕 방송통신위원회, "스마트폰 가입자 1,000만 돌파, 스마트 시대 본격 개막," 방송통신위원회 보도자료, pp. 1-2, 2011년 3월 24일.

〔5〕 데이코산업연구소, 스마트워크·모바일오피스 실태와 추진전략, 데이코, pp. 129-130, 2011년 1월.

〔6〕 한국정보화진흥원, "스마트폰과 모바일 오피스의 보안이슈 및 대응 전략," CIO Report Vol. 26, pp. 1-26, 2010년 10월.

〔7〕 함정선, "SKT '기업 스마트폰 보안 책임진다'..솔루션 출시," 이데일리, 2011년 5월 17일

〔8〕 한국은행, "지급결제 뉴스레터 제2011-2호," pp. 72-80, 2011년 2월.

〔9〕 방성훈, "급변하는 증시에 스마트폰 거래 급증", 아시아투데이, 2011년 9월 25일

〔10〕 민경락, "아시아 모바일 결제 선호…북미・유럽의 2배," 연합뉴스, 2011년 3월 1일

〔11〕 방송통신위원회, "스마트모바일강국실현 스마트폰이용실태조사(Ⅱ)," 방송통신위원회·한국인터넷진흥원, pp. 5-15, 2010년 12월.

〔12〕 남기현, "옵션쇼크 도이치증권 6개월 영업정지…사건의 재구성," 매일경제, 2011.2.23.

〔13〕 이철재·한애란, "'신의 직장' 금융공기업…근무 시간에 주식 투자," 중앙일보, 2011년 6월 28일

〔14〕 금융감독원, "2011년 1/4분기 자본시장 불공정거래 조사결과," 금융감독원 보도자료, 2011년4월 20일.

〔15〕 금융감독원, "2010년 자본시장 불공정거래 조사결과," 금융감독원 보도자료, 2011년 1월 26일.

〔16〕 신창용, "금융당국, '日방사능 韓상륙' 루머 조사(종합)," 연합뉴스, 2011년 3월 16일.

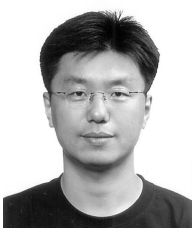
〔17〕 이중기, "금융정보보호의 법적 구조," 한림법학 FORUM 제7권, pp. 129-133, 1998년.

〔18〕 김인석·김태호·강형우·이정호·홍기석, "전자금융, 이러면 안전할까?," pp. 86-91, 150-169, 2010년 4월.

〔19〕 금융보안연구원, "정보유출 위협 및 대응방안 연구 보고서 - 무선 인터넷을 통한 정보유출 중심 -," pp. 8-9, 2010년 12월.

〔20〕 강동호외 6명, "스마트폰 보안위협 및 대응기술," 한국전자통신연구원, 전자통신동향분석 제25권 제3호, pp. 72-80, 2010년 6월.
〔21〕 김지숙, "스마트폰 이용 환경에서 국가기관 정보보호 관리방안," 정보보호학회논문지 제20권 제6호, pp. 89, 2010년 12월.
〔22〕 금융보안연구원, "금융부문의 IT 컴플라이언스 분석결과 보고서," pp. 15, 2009년 11월.
〔23〕 FSA(Financial Services Authority), "Taping of mobile phones," November 2010.
〔24〕 wendy.chothia, "FSA warns finance firms regarding compliance with new mobile phone recording rules," hedgeweek, 2011년 4월 13일.
〔25〕 이승우, "스마트폰 보안 진화…실내서 카메라 차단·분실 땐 자동 잠금," 한국경제, 2011년 6월 12일.

〈著者紹介〉



유 길 상 (Kil-sang Yoo) 학생회원
2010년 3월~현재: 고려대학교 정보보호학과 석사과정
〈관심분야〉 정보보호, 금융정보보호, 정보보호정책

박 태 형 (Tae-hyoung Park) 일반회원
2002년 2월: 고려대학교 서양사학과 학사
2004년 2월: 고려대학교 행정학과 석사
2004년 4월~2008년 4월: 한국행정연구원 연구원
2011년 2월: 고려대학교 정보보호대학원 박사
현재: 고려대학교 정보보호대학원 정보보호연구원 연구교수
〈관심분야〉 정보보호정책, 전자정부, 정보화, 성과관리, 성과평가

임 종 인 (Jong-in Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 원장
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 사이버전, 융합기술보안 등