인터넷활성화에 따른 전자금융위험에 대한 대응방안과 정책 연구

송경석†

A Study on the Risk Management of e-Finance by Active Internet

Keyong-Seog Song†

ABSTRACT

Although e-Finance has become more and more prevalent in everyday life, with the development of information technology, further development of e-Finance and commercial transactions has been limited. Therefore it is important for financial institutions to be aware of the significance of e0Finance risk and take appropriate actions. And an effective risk management function relies on a well-defined organization structure to eliminate gaps and minimize overlaps in risk management duties, responsibilities, and authorities. It defines and assigns risk management responsibilities, authorities, and accountabilities to appropriate personnel. The adequate organization of the risk management function is very important in the success of risk management.

Key Words : e-Finance, Risk management, Risk management structure, Information technology

1. 서 론

1.1 연구 필요성과 목적

금융업은 오래 동안 실물의 지점에 기초하여 발달하여 왔다. 그러나 최근의 정보통신기술의 발달은 금융기관이 지리적 장벽과 같은 여러 가지 장벽

† 호서대학교 디지털비즈니스학부 교수(교신저자)
* 본 논문은 호서대학교에서 시행한 2009년도 교내학술연구과제의 연구결과 보고임
논문접수 : 2010년 5월 15일, 1차 수정을 거쳐,
심사완료 : 2010년 6월 16일

을 극복할 수 있고 금융기관이 취급하는 재화와 서비스를 영의 한계비용에서 제공할 수 있게 까지 변화시켰다.

오늘날 금융기관들은 ATM과 인터넷뱅킹으로부터 모바일뱅킹에 이르기까지 소위 '전자금융'으로 불리는 다양한 전달경로를 가지고 있다. 그러나 이러한 변화는 금융기관에 대해 여러 가지 다양한 이익을 제공하기도 하지만 여러 가지 위험도 발생키시고 있다[1]. 금융서비스의 이런 특성의 변화에 따라 전통적인 위험을 인식하고 관리할 위험관리시스템 뿐만 아니라 금융기관이 위험의 변화에 대응할 수 있는 운영시스템을 효과적으로 구축하는 것도 더욱 중요해졌다.

금융업에 대한 위험관리가 새로운 개념은 아니다. 전통적으로 금융기관이 위험을 경감하기 위한 여러 가지 수단을 가지고 있지만 초점은 신용위험, 시장위험, 이자율위험, 유동성위험 등과 같은 일반적인 금융위험관리에 맞추어져 있다. 비즈니스측면에서 전자금융활동이 증가함에 따라 나타난 정보통신기술인프라에 대한 수요증가는 금융기관 경영측면에서도 위험관리를 고려해야 할 필요성을 제기시켰다[2]. 또한 위험관리측면에서 전자금융 고유의 위험을 분석해야 할 필요성이 제기된다.

더욱이 인터넷의 활성화로 인해 새로운 전자금융의 위험이 나타나고 있으나 이에 대한 대응방안과 정책에 관한 연구는 미미한 실정이다. 따라서 본고에서는 인터넷활성화에 따라 새롭게 제기되는 전자금융 위험관리를 위한 전자금융고유의 위험관리구조를 모색해 보고, 안정적인 금융환경을 조성하기 위한 대응방안을 찾아보고자 한다.

1.2 연구방법

본 연구에서는 기존의 전자금융 및 위험관리, 그리고 전자금융 위험관리와 관련된 문헌조사 및 연구를 위주로 전자금융의 위험관리에 대해 연구하고자 한다. 특히 인터넷이 활성화됨에 따라 제기되는 새로운 전자금융위험의 경우 명확하게 정형화되어 있지 않은 관계로 전문가 인터뷰 및 전자금융기관들의 신규보완책 및 대책을 중심으로 인터넷 전자금융위험 및 대책을 모색해보고자 한다.

따라서 먼저 기존연구에 대한 선행연구에 대한 분석을 통하여 전통적인 전자금융위험관리에 대한 분석을 시도한 이후 인터넷의 활성화에 따라 제기되는 새로운 전자금융의 위험과 그에 대한 대응방안 및 전략을 모색하고자 한다.

2. 선행연구

2.1 선행연구의 범주

본 연구에서는 인터넷이 활성화됨에 따라 변화되는 인터넷고유의 전자금융위험을 분석하고 그에 대해 요구되는 대응방안과 정책적 대책을 모색해보고자 한다. 이를 위해 먼저 본 연구에서 기존의 전자금융에 대한 위험과 그에 대한 관리방안에 대한 선행연구를 살펴 볼 필요가 있다. 기존의 연구를 보면 ATM기기 등 전통적인 전자금융과정에서 제기되는 위험에 대한 관리방안 및 대책 마련 등을 중심으로 연구가 이루어지고 있으며 최근의 인터넷활성화에 따른 전자금융위험의 변화 등에 대한 연구는 거의 이루어지지 않고 있다.

최근 전자금융이 활성화됨에 따라 전자금융의 위험을 관리하고 대응책을 마련해야 할 필요성이 크게 제기됨에 따라 BIS[21],[22] 등의 국제기구에 의한 대응책이 모색되고 있으나 국내에서 전자금융의 위험관리방안과 대책마련을 모색하는 선행연구는 많지 않으며, 최근의 인터넷의 활성화에 따른 인터넷 전자금융에서 제기되는 위험에 대한 분석이나 대응책마련은 연구가 필요한 상황이다.

전자금융의 위험관리에 대한 선행연구들을 살펴보면 심영[8]은 은행의 인터넷뱅킹을 중심으로 제기될 수 있는 전통적인 전자금융의 위험을 관리하기 위해 금융감독 측면에서의 전자금융규제방안을

1) 전통적으로 금융위험은 전략적 운영위험, 법률위험, 명망위험 등 금융기관의 활동과 관련된 위험으로 분류된다.

2) 바젤금융기관감독 위원회는 오래전부터 이런 측면에 초점을 맞추어 2003년 'Risk Management Principle for Electronic Banking'이라는 보고서를 발간하였는데, 이 보고서는 전자금융위험을 별도의 플랫폼으로 다룰 필요가 있음을 지적하고 있다 BIS[21].

모색하며, 전자금융거래법의 제정을 대응책으로 제시하고 있다.

이강식[9]의 연구를 보면 전자금융거래에서 제기되는 위험을 전통적인 위험분류절차를 따라 전략적, 운영적, 법률적, 명망적 위험에서 제기되는 위험으로 분류하고 이에 대한 위험관리방안으로 BIS협약에 따른 위험관리방안과 전자금융거래법제정을 통한 위험관리방안을 모색하고 있다.

한편 이종세[10]는 금융회사들이 정보통신기술을 도입함에 따라 제기되는 신규위험과 기존위험의 변화에 따른 위험을 관리할 수 있는 방안을 모색하고 있다. 이종세는 전자금융의 위험을 금융업무별로 구분하여 업무별로 제기되는 정보통신기술도입에 따른 위험관리방안을 모색하고 있다.

김태호 외[6]는 국내에 인터넷전문은행이 설립될 경우 제기될 것으로 예상되는 전자금융위험을 연구하고 있다. 특히 전자금융거래법의 제정에 따라 강화된 금융기관의 입증책임에 따라 금융기관의 전자금융위험이 상대적으로 증가할 것으로 보고 이에 따른 위험관리방안과 대책을 모색하고 있다.

대부분의 전자금융의 위험관리에 대한 연구를 보면 금융업무의 처리과정에서 전자금융의 이용이 활성화됨에 따라 변화되는 전통적인 금융위험프로파일을 분석하고, 이에 대한 대응책을 제시하고 있으며, 정책적인 대응방안으로는 전자금융에 대한 법률적 규범적 규제방안을 모색하고 있다.

2.2 선행연구의 내용

2.2.1 전통적인 전자금융위험

기존 연구결과를 보면 대부분이 전통적 전자금융 위험의 변화와 이에 대한 대응방안을 모색하고 있는데, 이들 연구를 종합하여 전통적인 전자금융위험 프로파일의 변화를 살펴보았다. 금융업무의 전통적인 여러 가지 특성은 전자금융의 도입에 의해 여러 가지 다양하게 변화하고 있다[3]. 특히 전자금융의 충격은 금융업무의 전통적인 위험요인들[4] 인 전략적, 운영적, 법률적, 명망위험에서 더 근본적인 변화를 일으키는 경향이 있으며, 이에 따라 온.오프라인 겸영은행의 경우에는 전반적인 위험프로파일이 영향을 받게 된다. 또한 인터넷을 이용한 전자금융의 경우에도 인터넷이라는 특성에 의해 발생되는 특수한 전자금융위험이 발생될 가능성이 높아진다.

1) 전략적 위험

전략적 위험은 주로 경영의사결정과 결합된 것이다. 전자금융의 측면에서 보면 기술관련 재화와 서비스, 그리고 프로세스, 운송채널 등과 관련된 기술의 성과를 경영과정에서 적절히 운영하고 모니터하기 위한 계획을 수립하지 못할 때 전략적 위험이 발생된다.

전략적 위험은 전략적 비즈니스 계획수립에 대한 기술관련 계획과 의사결정을 재정비함으로써 극소화될 수 있다. 그리고 효율적인 정보통신기술 관리[5] 는 경쟁우위, 고객만족, 비용효율성, 그리고 성장 및 혁신 능력 등을 개선시키게 된다. 이 과정에서 지속적인 기술업그레이드와 신기술에 대한 주기적 평가가 중요하다.

2) 운영위험

바젤위원회는 운영위험을 부적절하거나 실패한 과정이나 사람, 그리고 시스템이나 외부의 사건으로부터 결과되는 손실위험으로 정의하고 있다. 이 정의에 따르면 법률적인 위험은 운영위험에 포함되지만 전략적위험이나 명망위험은 배제된다. 혹자는 이를 거래위험, 보안위험 또는 정보통신기술 위험으로도 부른다.

이러한 운영위험은 제품과 서비스를 취급하고 있는 금융기관의 위험에 영향을 미치며, 고객서비스에도 직접적인 영향을 미친다. 이는 실질적인 금융손실을 초래

3) 바젤위원회는 금융기관과 결합된 주요위험을 여덟가지 주요 범주로 나누었다 BIS[20][21].

4) 조하연, 이승국[12]

5) 효율적인 정보통신기술 관리과정은 정보통신기술 전략의 수립, 가치전달을 위한 정보통신기술 과정의 경영, 성과평가, 그리고 정보통신기술 관련 위험의 관리 등의 측면에서 금융기관에 유익할 것이다.

하며 또한 금융기관의 전략적, 명망, 시장 그리고 신용위험에도 영향을 미친다.

3) 적합성 위험

적합성 위험은 전자금융과정에서 법이나 규칙, 또는 규제, 관습, 도덕적 기준 등의 위반이나 불일치에서 발생되는 위험을 말한다. 이 위험은 금융거래와 관련한 당사자의 법률적 권한이나 의무가 잘 정립되어 있지 않을 때 발생된다. 금융기관은 규제요건의 변화를 충족시키기 위해 기술을 변화시킬 경우 적합성위험이 높아지게 된다.

따라서 부적합성이 발생될 경우 금융기관의 신용등급 하락, 규제강요와 금전적인 과태료(Monetary fines), 운영정지, 명망손상, 그리고 극단적인 경우에 운영당국의 금융기관 지정철회 등을 포함한 여러 가지 심각한 결과가 초래될 수 있다.

4) 명망위험

고객관계를 설정하는 금융기관의 능력이 유의하게 손상된 경우 전반적인 금융기관운영에 대해 지속적으로 부정적인 대중이미지를 형성하는 위험을 명망위험이라 한다.

명망위험이 증가하게 되면 다른 범주의 위험들, 특히 운영위험이 높아지는 직접적인 계기가 될 수 있다. 그리고 이는 비용이 소요되는 법률적 문제를 발생시키거나 추가적인 수입이나 자본을 손상시키게 될 것이다. 극단적인 환경에서는 금융기관 명망위험이 금융시스템전체를 붕괴시킬 수도 있다.

2.2.2 전통적 전자금융위험 관리방안

기존의 선행연구에서 제시하고 있는 대표적인 전통적인 전자금융위험에 대한 관리방안은 대부분 국제결제은행(BIS: Bank for International Settlement)에서 제시한 전자금융위험관리준칙을 들고 있는데, BIS에서는 14개 항목의 전자금융위험관리준칙 가운데 평판위험에 대한 적극적인 관리가 무엇보다 필요하다고 보고 있다. 이는 전자금융의 특성상 전자금융회사의 평판과 관련된 정보가 일단 파급되어 자금인출 등의 사태가 발생하면 오프라인 금융기관에 비하여 통제가 용이하지 않기 때문이다.

〈표 1〉 BIS 전자금융위험관리준칙

분야	주요내용
이사회 및 경영진의 감시	- 이사회와 경영진에 의한 전자금융업무와 관련된 위험에 대한 실효성 있는 감시체제의 확립, 명확한 책임부여 - 이사회와 경영진의 은행보안통제절차중 중요사안에 대한 검토승인 - 이사회와 경영진의 전자금융을 지원하는 제3자에 대한 의존도 및 아웃소싱관계를 관리할 수 있는 포괄적이고 지속적인 심사 및 감독절차의 마련
보안통제	- 인터넷거래 고객의 신분 및 권한부여사항을 확인할 수 있는 적절한 조치 강구 - 금융기관은 거래부인방지 및 전자금융거래에 대한 책임을 명확히 할 수 있도록 거래에 대한 정당성확인수단을 사용 - 금융기관은 전자금융시스템, 데이터베이스, 응용프로그램하에 직무책임이 명확히 분리될 수 있는 적절한 대책 강구 - 금융기관은 전자금융시스템, 데이터베이스 및 응용프로그램에 대해 적절한 승인통제 및 접근권한을 마련 - 금융기관은 전자금융거래, 기록, 정보에 대한 데이터의 무결성을 보호할 수 있도록 적절한 대응책을 마련 - 금융기관은 모든 전자금융거래에 대해 명확한 감사증적을 남겨야 함 - 금융기관은 핵심적인 전자금융정보에 대한 비밀이 유지될 수 있도록 적절한 조치를 위해야 함
법률위험 및 평판위험 관리	- 금융기관은 자신의 웹사이트에 충분한 정보를 제공하여 잠재고객이 전자금융거래를 시작하기 전에 금융기관의 정체성과 규제상태를 알 수 있게 해야 함 - 금융기관은 전자금융상품 및 서비스를 제공하는 나라에서 제공되는 고객의 프라이버시 보호요건을 충실히 준수할 수 있도록 적절한 대책을 강구해야 함 - 금융기관은 전자금융시스템 및 서비스의 가용성을 보장할 수 있도록 거래처리용량, 업무의 연속성 및 비상계획 등에 대한 효과적인 계획수립절차를 확립 - 금융기관은 내외부로부터의 보안침해 등 전자금융시스템 및 서비스를 방해할 수 있는 사건에 대한 문제를 관리, 억제, 최소화할 수 있는 장애대비계획을 수립

자료:BIS[20][21]

3. 인터넷 전자금융 위험의 대두

인터넷이 사회적으로 광범위하게 확산되고 이용이 활발하게 이루어짐에 따라 금융기관에서도 전자금융운영시스템을 인터넷 중심으로 바꾸고 있다. 이 과정에서 온

오프라인 겸영은행의 전자금융이나 인터넷전문은행의 전자금융의 경우 인터넷이 지니고 있는 고유한 특성으로 인해 새로운 전자금융리스크가 제기될 수 있다.

3.1 계좌개설 및 공인인증서 위험

인터넷을 통한 금융업무를 처리하는 경우 외국의 경우 주요국에서 계좌개설시 대면확인을 하도록 강제하는 법률은 없으나, 신규로 개좌를 개설하는 경우 즉시 개설해주지 않고 리스크관리차원에서 실질적인 심사를 거쳐 신청인 본인여부를 확인하는 등 내부통제절차를 마련하여 운영하고 있다.

그러나 우리나라는 계좌개설시 반드시 실명확인을 해야 한다는 "금융실명거래 및 비밀보장에 관한 법률"[6]로 인해 인터넷을 통한 계좌개설에 문제가 제기되고 있다. 특히 인터넷전문은행이 전국을 영업대상으로 해서 영업을 할 경우 실명확인방법의 해결이 중요한 과제의 하나로 대두된다. 현행법을 엄격히 적용한다면 인터넷전문은행은 본점을 제외하고는 실명확인을 할 수 있는 방법이 없으므로 다른 금융기관을 통해 수수료를 지급하고 실명확인 대행을 해야 한다.

결국 인터넷을 통한 계좌개설의 경우나 인터넷전문은행의 활성화를 도모하고 소액 금융소비자의 편익을 도모하려면 온라인상에서 실명확인이 가능하도록 제도적인 뒷받침을 해야 할 것이다. 또한 그 방법의 하나로 현행 공인인증서를 실명확인수단으로 사용할 수 있도록 하여 본인확인이 가능하도록 하는 법제도의 개정 등이 고려되어야 할 것이다.

그러나 현행 공인인증서의 이용은 인증서 자체의 보안 취약점 보다는 보관 또는 관리상의 취약점으로 인해 복제와 도용 등 전자금융사고가 발생되고 있으며[7], 더욱이 해킹기술의 발달로 대형화 지능화 되고 있는 추세이다. 현재의 공인인증서는 무한히 복제가 가능한 정보에 불과한 것으로 진정한 디지털시대의 전자인감으로서 역할을 하려면 대면확인을 충분히 대체할 수 있는 안전한 기술이 뒷받침되어야 할 것으로 보인다.

3.2 인터넷에 대한 업무의존에 따른 위험

전자금융이 활성화되고 인터넷전문금융기관이 등장함에 따라 인터넷을 통해 대부분의 업무를 처리하고 24시간 영업 체제를 유지하는 등 IT부문에 대한 사업의존도가 절대적이 되고 있으며, 전통적인 은행보다 높은 차원의 서비스를 제공하기 위해 인넷 및 온라인서비스개발에 더욱 더 집중할 것으로 예상된다. 특히 인터넷전문은행은 새로운 비즈니스모델로서 예기치 못한 위험에 직면할 수 있다. 또한 미국, 유럽 일본 등 해외의 사례[8]를 벤치마킹해 지급결제, 소액대출, 신용카드, 전자화폐 등 인터넷전문은행마다 다양한 특화된 전략에 따른 고객서비스로 시장점유율을 높이려 할 것이다.

기존은행은 온오프라인의 여러 채널을 보유하고 있어서 온라인채널의 장애에도 지점이나 서면기록 등을 통해 영업을 영위할 수 있으나, 인터넷 전문은행은 모든 업무가 인터넷을 통해 전자적으로 처리되므로 웹서버 또는 인터넷뱅킹 서버 장애, 인터넷망 장애 등 일부 시스템의 장애나 외부장애요인의 발생에도 전체업무가 마비되어 업무지속이 어려운 리스크가 발생된다. 따라서 인터넷전문은행은 시스템장애에 대비하여 기존은행보다 철저한 대비와 노력이 필요하다. 이처럼 인터넷전문은행은 서비스채널이 인터넷에 집중됨에 따라 전통적인 온오프라인 겸영은행과 차별되는 추가적인 리스크에 노출될 위험성이 크다.

3.3 의사소통채널부재에 따른 위험

미국 통화감독청에서는 점포없이 가상점포만으

6) 실명에 의한 금융거래를 실시하고 그 비밀을 보장하여 금융거래의 정상화를 기함으로써 경제정의를 실현하고 국민경제의 건전한 발전을 도모하기 위해 제정한 법(1997.12.31, 법률 제5493호).

7) 중국 해커로 추정되는 해커들이 국내 특정 웹사이트를 해킹하여 동 사이트에 접속한 고객의 PC에 저장된 5,000여명의 공인인증서 절취(2007.1)하는 등 사고가 발생하고 있다.

8) 미국의 Netbank는 담보대출, ING Direct는 인터넷 및 전화위주의 저축, 투자상품, 영국의 Eggbank는 소비자금융 특화로 신용카드, 일본의 Seven bank는 예금지급 등으로 전략적으로 특화하여 서비스를 제공하였음.

로 운영되는 인터넷전문은행이라 할지라도 고객과의 원활한 의사소통을 위해 최소한 한 개 이상의 물리적 실체(Physical)의 점포를 유지하도록 의무화하고 있다. 일본의 경우에도 금융감독청은 인가시 무점포영업이라 할지라도 고객보호와 관련하여 고객의 고충 및 상담과 시스템다운 등에 수반되는 고객대응, 법령에 근거한 고객에 대한 설명의무의 이행, 공시의 이행 등의 관점에서 대응태세가 적절한지를 철저하게 감독하고 있다.

3.4 아웃소싱 리스크

인터넷전문은행은 초기부터 다수 고객을 신속하게 확보하기위해 공격적 마케팅과 전략적 제휴, 철저한 아웃소싱을 통해 비용절감을 추구하는 모습을 보이고 있다. 미국의 NetBank가 대표적인 경우인데 본사는 기획과 콜센터만을 직접 관장하고 데이터관리, 네트워크관리, 대출심사 등 대부분의 업무를 아웃소싱하여 비용최소화전략을 추구하고 있다[9]. 아웃소싱의 활용이 일반화되는 추세로 국내 인터넷전문은행의 전략도 이와는 크게 다르지 않을 것으로 보인다. 비용절감을 통해 고객에게 높은 금리제공과 저렴한 수수료를 제공하기 위한 인터넷전문은행의 아웃소싱의 선택은 불가피하지만 핵심업무기능을 외부에 맡김에 따라 외부업체에 대한 의존도가 상대적으로 커지고 개인정보 및 금융거래정보의 유출가능성과 IT 부문에 대한 통제력이 약화될 위험성도 높아진다. 또한 제휴업체의 서비스중단우려와 기술종속성심화 등 잠재적인 리스크도 크게 증가할 것으로 예상된다.

4. 인터넷 전자금융위험의 대응전략

이상과 같은 인터넷 기반의 전자금융시스템 활성화에 따른 위험요인이 새롭게 대두되고 있는 바, 이에 대한 대응전략과 정책을 분석 정리하면 다음과 같다.

4.1 전자금융 위험관리의 체계화

정보통신기술의 발달은 여러 가지 예상치 못했던 금융위험을 야기하기도 하지만, 기술혁신으로 전자금융의 위험을 감소시킬 수 있는 여러 가지 방법을 모색할 수 있게도 한다. 이에 따라 전자금융에 대한 위험관리방법과 절차가 급격하게 변화되고 있다. 전반적인 위험관리프로세스의 발달은 데이터를 수집하고 전환하는 능력을 제고시키고 비용을 낮출 뿐 아니라 위험을 측정하고 관리하는 기술을 개선시켜 수량화를 보다 용이하게 한다.

금융위험에 대한 관리는 시장투명성의 제고, 금융공학의 발달 등으로 수년 동안 훨씬 더 발달하였다. 특히 기업의 재무기능의 발달로 인한 금융거래 및 위험의 복잡화는 금융기관이 가격, 이자율, 유동성, 외환 등에 대한 위험을 주기적으로 평가하고 관리하는 모형을 적극적으로 개발하고 사용해야 할 필요성을 유발시키고 있다. 또한 신용위험의 증대는 신용위험을 평가하는데 훨씬 더 강한 프레임워크의 개발을 필요로 한다.

비금융위험에 대한 관리는 훨씬 더 혁신적인 과정을 필요로 한다. 이들은 금융관리수단을 사용하거나 노출한계를 설정하는 방식으로 헤지할 수는 없으므로 이들 위험을 경감하기 위해서는 다른 전략을 개발해야한다. 기술집약적이며 혁신적이고 발전적인 전자금융환경의 위험은 보다 새로운 형태의 관리방안을 필요로 한다는 것이다.

상당수의 전통적인 위험관리모형은 다음과 같은 전자금융과정과 환경에서도 이용할 수 있다.

- 전자금융관련 정보통신기술의 정교화에 따라 나타나는 직접적인 운영과정을 반영하는 정책과 과정
- 전통적인 금융위험과 별개로 분리되어 있는 독자적인 전자금융위험에 대한 위험관리과정
- 개인에 의해 관리되고 조절되는 내부통제 및 감독

만약 금융기관의 전반적인 비즈니스 프로파일가운데서 전자금융 비즈니스의 규모와 전략적 중요성

9) NetBank는 여신기능도 외부회사인 first Mortgage Network에 맡기고 있다. 모든 여신기능을 외부에 맡겨 다른 인터넷 전문은행이나 인터넷 겸업은행보다 빨리 이익을 실현하는 것으로 해석되고 있다.

을 정당화할 수 있으려면, 전자금융 고유의 위험을 관리할 수 있어야한다. 전자금융위험은 전자금융 관리과정에서 분리될 수 있으며 프레임워크 설정단계에서 전통적인 금융위험의 경영구조와 통합될 수 있다. 이를 통하여 주요한 비금융 전자금융위험을 적절히 관리할 수 있으며, 이를 전자금융위험과 통합하여 총체적인 관리가 이루어질 수 있을 것이다.

규모가 큰 대형 금융기관의 경우에는 전자금융 위험을 명확하게 구분할 수 있는 중요한 위험 카테고리에 대한 별개의 프레임워크설정, 즉 정보보안, 운영위험, 아웃소싱, 사업연속성, 그리고 일치성 등에 대해 별개의 프레임워크를 설정하는 것이 보다 효율적인 접근법일 것이다. 물론 이들 역시 금융기관의 전반적인 위험관리구조하에서 통합되고 관리되어야 한다. 규모가 작은 소형 금융기관의 경우에는 통합모형이 적합할 수도 있다. 이 경우 금융위험 완화에 초점을 맞추기 위해 다른 전자금융위험으로부터 운영위험요소를 구분하는 방법을 모색할 필요성도 있다.

4.1.1 위험관리 정책과 절차의 수립

위험관리정책은 효과적인 위험관리를 강조하는 광범위한 지침을 제공하는 것인 반면 위험관리 절차는 위험관리정책의 요건을 충족시키는 과정을 설명하는 것이다.

전자금융 위험관리 정책과 절차는 전자금융과정을 어떻게 통제하고 운영할 것인가에 대한 기본적인 개념을 설정하는 것이다. 효율적인 위험관리 정책과 절차가 없다면 성과를 비교하고 운영상의 안전을 확보할 수 있는 방법이 없다. 전자금융 위험관리 정책과 절차는 전자금융 비즈니스와 결합된 모든 물리적 위험을 커버할 수 있어야 한다. 책임은 명확히 기술되어 있어야 하고 각 사업 활동과 성과에 대한 당국의 지침 역시 명확하게 정의되어 있어야 한다.

전자금융 위험관리와 관련하여 중요한 정책으로는 다음을 들 수 있다.

.정보보안정책
.아웃소싱정책
.사업연속성정책
.일치성정책
.고객정책과 관련된 프라이버시 보호정책

이들 위험관리 정책의 깊이와 포괄범위는 금융기관의 규모와 복잡성에 따라 아주 다양하다. 소규모 금융기관은 정보보안정책과 같은 단일집중지도안(one central guiding document)을 만드는 경우가 자주 있으며 이 경우 다른 정책요인들은 보안정책에 끼워 넣는다. 규모가 보다 큰 기관은 비즈니스 라인이나 다른 운영부서로부터 정책관리부서를 분리하는 경우가 많다.

또한 전자금융 위험관리 정책과 절차는 변화하는 환경에 보조를 맞추어야 하며 주기적으로 규제적 관점에서 이들 정책과 절차의 적절성을 검토해야 한다.

4.1.2 위험관리절차

위험관리의 첫 단계는 금융업무의 역할과 책임을 잘 이해하고 전자금융환경에서의 위험관리목표를 명확하게 설정하는 것이다. 그리고 위험관리 목표설정은 금융기관이 노출되어 있는 여러 가지 상이한 전자금융 위험유형에 대한 정의에 상당 부분 의존한다.

이때 이들 위험이 실질적으로 무엇을 의미하는지를 명확하게 정의하고 이들 주요 위험의 유형이 어떻게 관리되어야 하는지를 규명하는 것이 이사회와 고위경영자의 책임이다. 또한 금융기관이 금융조직간 일관된 개념의 사용을 돕기 위한 내부의사소통의 목적으로 상이한 업무 및 조직 카테고리에 대한 명확한 정의를 하는 것도 중요하다.

4.1.3 위험인식과 평가

위험에 대한 정확한 인식이 금융기관의 위험관리 계획을 수립하는 첫 단계이다. 위험을 정확히 정의하고 규명하는 과정은 이들 위험을 정확하게 이해하고 반응할 수 있는 능력을 갖고자 하는 시도이다.

규명된 여러 가지 위험에 대해서는 그러한 위험이 발생될 가능성과 그럴 경우의 영향에 대한 평가

도 이루어져야 한다. 규명단계에서 위험이 보다 명확하게 정의될수록, 위험에 따른 영향도 정확하게 평가될 수 있다. 금융위험은 전략위험이나 평판위험과 같은 전자금융환경에서 명시된 비금융위험보다 처리하기가 더 쉽다. 경쟁자의 과거 사건이나 경험은 이들 위험을 평가하는 유익한 자료를 제공할 것이다.

위험에 대한 규명과 평가는 주관적인 것이 아니다. 물론 많은 것이 분석가의 경험과 지식에 의존할 수밖에 없지만, 필요한 것에 대한 규명을 통하여 경험있는 사람과 경쟁할 수 있도록 여러 가지 객관적인 기준을 부과하는 것이 보다 더 현명하다.

위험에 대한 규명과 평가는 다음과 같은 것을 포함하여 여러 단계를 거쳐 보다 세밀하게 분석되고 배분된다.

.전자금융 환경의 위협과 취약점 분석

.전자금융제품과 서비스의 정보보안과 관련된 위험평가

.아웃소싱의 위험과 오프쇼어링에서의 국가 위험

.사업연속성에 대한 사업충격분석

.법률적 상태와 규제적 가이드라인에 대한 응낙요건

4.1.4 운영위험관리

운영위험관리는 금융기관이 사기를 막고, 내적통제를 강화하고 거래과정의 오류를 줄이는 등의 노력을 하는데 있어서 중요한 것이므로 새로운 것이라 할 수는 없다. 다만 과거에는 금융기관이 운영위험 관리를 위해 감독기능을 통한 비즈니스라인 내에 있는 내적통제 메커니즘에 거의 배타적으로 의존했다.

전자금융의 운영위험으로는 두가지 구성요소를 들 수 있다. 첫째는 금융기관 내부의 사람과 조직인 내부과정의 부적합이나 실패로 인해 결과되는 손실위험이다. 이는 내적자원을 명확히 함으로 조절할 수 있으며 전통적으로 전략적 계획수립, 인적 기술적이슈의 강조, 효율적인 내적 통제시스템 등을 통해 조절된다. 이를 통하여 정보체제의 부족, 사기, 인적자원오류, 기술측면의 붕괴 등과 같은 사고의 위험을 줄일 수 있다.

두 번째는 자연재해, 테러공격, 강탈, 아웃소스된 기능의 취약성 등과 같은 것에서 명백하게 나타나는 외부적 사건에서 초래되는 손실위험과 관련되어 있다. 이들 위험의 관리는 2단계 접근방식을 통해 관리할 수 있다; 보험을 통한 위험의 이전, 그리고 사건반응과 사업연속성계획수립을 통한 이들 위험의 흡수 등이다.[10]

4.1.5 지배 및 내적통제

성공적인 전자금융 위험관리를 위해서는 효율적인 내적통제구조를 통한 강력한 지배구조에 기초해야 한다. 위험관리와 기업지배, 내적통제 세가지는 공통의 원소를 갖는다.

전자금융의 범주에서 건전한 금융기관지배의 주요한 요소는 비즈니스라인, 내적 외적 감시기능을 포함한 적절한 내적 통제시스템, 그리고 필요한 체크와 잔고유지를 갖는 기능적 과정, 강력한 위험관리 함수 등을 들 수 있다.

물론 오늘날에는 지배, 위험관리, 내적통제에 대한 명확한 코드, 표준 등에 대한 명확한 지침을 가지고 있다. 그렇지만 이들을 통합하는 단일화된 코드는 없다. 그리고 이들 표준의 많은 부분이 전자금융활동에만 국한된 것도 아니다. 따라서 금융기관은 둘이상의 활용 가능한 표준을 조합하여 사용하는 것이 필요하며 금융기관의 특정요구를 충족하기 위한 전자금융환경에 대해 이들을 적용할 수 있다.[11]

4.2 기술적.물리적 대책

금융기관은 전자금융거래법의 제정으로 금융거

10) 2003년에 바젤금융기관감독위원회에 의해 발간된 레포트인 'Sound practices for the management and supervision of operational risk'가 효율적인 운영위험관리기능을 개발하기 위한 훌륭한 사례를 제시하고 있다 BIS[20].

11) 바젤금융감독위원회에 의해 2006년에 발간된 보고서 'Enhancing corporate governance for banking organization가 좋은 예를 제시하고 있다 BIS[22].

래에 있어서 무과실책임 등으로 위험을 적극적으로 관리해야 할 부담은 점점 커지고 있으나 전자금융 시스템은 다양한 종류의 네트워크와의 연동, 이용자중심의 여러 가지 서비스채널구축, 기능별.영역별 개별시스템들의 통합, 전산시스템의 구축과 운영의 아웃소싱, 안정적 전자금융시스템의 구축 등이 요구되고 있어 기술적 보안에 취약해질 가능성이 높아지고 있다.

따라서 금융기관이 전자금융에 따른 위험을 최소화하여 안정적으로 생존할 수 있으려면 무엇보다도 먼저 기술적 물리적 측면에서 위협요소별 보안대책을 마련하여 시행하고 지속적인 모니터링을 하는 것이 필요하다. 금융기관들은 이를 위해 해킹방지, 대고객보안, 내부보안, 보안조직 및 전문인력확보 등의 기술적.물리적대책을 강구하여 시행하고 있다.

4.2.1 해킹방지

현재 금융기관들이 인터넷뱅킹에 설치하는 국내 해킹방지프로그램들의 경우 보안프로그램에서 새롭게 발생하는 해킹프로그램의 대응에는 한계가 있고 애플리케이션영역에 대한 키보드보안프로그램의 경우도 미흡한 점이 많다. 이에 대해 정부에서도 다양한 대응책을 강구하고 있지만[11] 해킹방지기능 강화를 위해 PC용 보안프로그램의 설치의무화는 물론, 인터넷뱅킹 전과정에 대한 보안체계구축을 위하여 키보드입력으로부터 애플리케이션으로 넘어가는 부분까지 암호화를 추진하고 전자금융이용자 정보보호수칙을 마련하여 이용자가 인터넷뱅킹 등 전자금융사이트에 접속할 경우 팝업창의 형태로 반강제적으로 숙지하도록 하는 조치를 취하며, 금융부문 해킹대응에 대한 국가차원의 전담조직을 설립할 필요도 있다.

4.2.2 대고객보안

최근에는 위변조기술의 발달에 따라 주민등록증, 운전면허증 등의 위변조를 확인하기가 쉽지 금융기관에서 사용하고 있는 보안카드의 비밀번호의 경우도 경우의 수가 30-35개로 부족하고, 입력정보 특히 공인인증서의 온라인 재발급시 신원확인정보에 대한 해킹공격 및 도청에도 취약하며, 금융기관의 중요거래정보의 고객통지 및 정보관리도 미흡한 상태이다. 또한 전자상거래시 신용카드정보나 계좌정보 등에 대한 보호장치 및 인증시스템의 본인확인 절차도 취약하기 때문에 전자금융 위험부담을 경감하기 위해서는 전반적인 대고객보안시스템의 보완 및 개선이 필요하다.

1) 신분위변조에 대한 확인 강화

전자금융 신규가입업무를 담당하는 금융기관 창구직원에 대한 실명확인 증표의 식별방법[12]에 대한 교육을 강화한다. 또한 위험대비 비용을 감안해야 할 필요성은 있지만 가능하면 공적인 신분증 이외에 생체인식을 추가적으로 활용할 필요성도 있다.

2) 인터넷뱅킹 및 텔레뱅킹 보안대책

2005년 7월부터 시행되고 있는 이용자의 전자금융거래시 개인PC에 보안프로그램(키보드해킹방지, 개인방화벽)의 제공을 의무화한 조치를 실효성을 높이기 위해 감독당국의 해킹대응전담조직을 강화하여 지속적으로 해킹 등에 대한 정보를 제공하도록 해야 하며 일회용비밀번호생성기(OTP: One Time Password)를 활성화시킬 필요성도 있다. 또한 하나의 OTP생성기로 다수의 금융기관과 거래가 가능하도록 통합인증체제를 구축할 필요성도 있다.

또한 고액이 예치된 중요계좌의 경우 조회나 이체 등 모든 비대면전자금융거래를 허용하지 않는 보안계좌제도를 두거나 전자금융서비스별 선택항목란을 추가하여 고객의 서면동의를 강화하는 것도 고려할만하다.

4.2.3 내부보안

내부관련자의 정보유출이나 부정조작을 방지하

11) 정부에서는 한국정보보호진흥원으로 하여금 해킹프로그램의 수집분석체계를 구축하여 해킹프로그램을 인터넷뱅킹 등 전자금융거래에 적용테스트를 한 후 문제가 발생될 경우 보완조치를 취하도록 하고 있다 금감원[2].

12) 주민등록증의 경우 홀로그램, 사진, 성명 등의 수정확인 및 ARS1382 및 인터넷 진위확인 서비스 등을 통한 확인강화

기 위해서는 적절한 절차와 책임을 규정한 강력한 지침을 마련 엄격하게 시행하며 정기적인 교육을 통해 보안의식을 제고하는 것이 중요하다. 또한 주요자료는 DRM(Digital Rights Management) 및 워터마킹기술을 활용하여 복사방지나 유출문서의 추적이 가능하도록 하고, 전자거래기본법 및 전자금융거래법에 이해 전자금융의 경우에도 전자문서의 효력이 이용되므로 신규이용자가 전자금융가입시 제출한 신청원본은 스캐너 후 스캐너한 이용자정보만 컴퓨터에 저장한뒤 책임자만 열람할 수 있도록 전자자물쇠를 채워 보관하는 방법을 도입하는 것도 생각할 수 있다.

또한 금융거래와 전산시스템의 특성을 감안하여 금융거래를 위한 임시거래소 설치, Packet Switch Node에 독립적인 통신인프라의 구축, 물리적 보안 및 접속제한의 강화, 기반시설보안평가를 위해 정부와 금융기관간 및 금융기관 상호간 공동전선의 구축, 정부와 금융기관의 정보교환을 위한 공동커뮤티케이션 채널구성 등이 필요하다.

4.3 인터넷 전자금융위험 대응방안

4.3.1 보안토큰기반 공인인증서의 사용

온라인계좌개설과 관련하여 공인인증서를 이용하여 온라인상에서 안전하게 계좌개설에 사용할 수 있다면 기존 금융기관에서도 실명확인 업무처리에 소요되는 직접적인 비용절감 효과만 아니라 창구거래의 온라인화를 촉진하여 금융기관의 상당한 수익제고를 기대할 수 있다.

이러한 효과를 얻기 위한 기술적 해결방안으로는 보안토큰 기반의 공인인증서[13] 사용을 들 수 있다. 현재의 공인인증서의 보관 및 관리상의 취약점을 보완하고 사용자본인을 인증하기 위하여 하드웨어 매체를 이용하는 것이다. 보안토큰기반의 공인인증서는 국내에서 표준화 및 적합성 인증이 이미 이루어져 있어 쉽게 적용이 가능하며 사용편의성이 높으며 보안토큰발행에 소요되는 비용도 현행 실명확인 대행 위탁수수료보다 적은 비용으로 발급이 가능하다.[14]

물론 계좌개설을 위해 본인확인을 하는 온라인 인증체계가 보안토큰기반의 공인인증서로만 제한할 필요는 없다. 이 뿐만 아니라 기발급된 OTP를 통한 본인확인, 핸드폰 소유주 명의 확인방법 등 다채널 다각도의 인증과정을 거친다면 훨씬 효율적일 것이다.

다만 이런 기술정책이 전자금융시장에서의 자유로운 경쟁환경을 저해하지 않도록 투명성과 일관성을 유지할 수 있어야 한다.

4.3.2 보안시스템에 대한 적극적인 투자

인터넷을 이용한 전자금융이 활발하게 이루어지고 있는 상황에서는 인터넷으로 금융서비스가 집중되게 되므로 이에 따른 위험을 줄이고 다양한 온라인채널에 대한 보다 안전한 금융서비스를 제공하기 위해서는 보안시스템에 보다 많은 자원의 투자가 이루어져야 한다.

또한 이러한 자원의 투자가 효율적으로 이루어지고 IT기술변화에 따른 위험을 최소화하기 위해서는 기술전문임원의 영입, 전문인력의 확보 등 조직운영상의 대책을 수립할 필요가 있으며 인터넷전문은행 자체적으로도 해당 위험에 대한 적절한 관리방안을 수립할 필요가 있다.

또한 장애나 재해 등 비상시에 대비하여 업무 연속성 및 안정성을 유지하기 위해서는 비상영업계획, 백업센터 구축을 포함한 재해복구계획을 철저하게 마련할 필요가 있다. 정부는 인가 심사시 이런 리스크에 대한 대응이 가능한 실질적인 대책이 수립되었는지 여부를 점검, 관리, 감독할 필요가 있다.

또한 기술적으로는 기존은행과 유사하게 시스템의 다중화를 통한 안정성도 확보해야 하지만, 외부

13) HSM(Hardware Security Module) 전자서명 알고리즘 생성키 등 비밀정보를 안전하게 저장하고 보관하기 위해 키 생성과 전자서명 생성 등을 기기내부에서 처리되도록 구현한 하드웨어기기로서 물리적 보안 및 암호연산기능을 내장해 키보드해킹이나 피싱으로부터 공인인증서의 유출을 방지하는 장치

14) 2007년 11월 KISA(한국정보보호진흥원)에서 보안토큰기반의 공인인증서 이용규격(V1.7-표준화)을 발표하였고, '구현적합성 검증평가 인증'을 실시하여 2008년 4월 현재 3개업체의 제품이 인증을 획득하였다.

장애요인에 대한 업무마비의 문제가 발생하지 않도록 장애시 전환하여 수용이 가능한 추가적인 온라인 금융거래채널을 확보하는 방안도 고려해야 한다. 예를 들면 인터넷뱅킹 금융거래 장애시 폰뱅킹을 통한 금융거래로 전환할 수 있도록 비상시 서비스제공기관(회선제공업자)으로부터 충분한 시스템을 확보하는 방안 등을 마련할 필요도 있다.

4.3.3 다양한 의사소통채널의 확보

인터넷 전자금융을 이용하는 소액금융소비자의 불편이나 문의사항 등 고객의 고충에 대한 원활한 해소를 위해서는 콜센터 등 다양한 의사소통채널을 충분히 유지하도록 해야 한다.

또한 비상시 금융소비자가 이용할 수 있는 서비스채널을 사전에 충분히 확보해야 한다. 이처럼 소비자보호를 위한 충분한 시설과 인력을 갖추어야 소비자의 합리적인 선택을 유도할 수 있고 궁극적인 수익성의 향상에 기여할 것이다.

4.3.4 체계적인 아웃소싱위험관리기준의 마련

전자금융기관이 비용절감을 위해 추구하는 아웃소싱의 경우 전자금융기관 특히 인터넷을 위주로 한 전자금융기관의 경우 불가피한 측면으로 보인다. 미국의 경우에는 외부 아웃소싱업체를 선정하는 경우 금융기관의 영업전략과 부합하는 계약서를 작성하도록 하며 아웃소싱업체는 감독당국의 검사에 협조한다는 내용을 계약서에 명시하도록 하는 등 구체적인 위험관리준칙을 제시하고 있다.

물론 국내의 경우에도 금융기관에 대해 아웃소싱에 따른 IT위험에 대한 가이드를 마련하도록 하고 있으나 아직 체계적이고 일관된 감독기준 제시는 미흡한 편이다. 국제적인 기준에 부합하는 체계적인 아웃소싱 위험관리기준을 마련할 필요가 있다.

5. 결 론

전자금융시대에 금융기관은 더 이상 수동적으로 금융상품을 판매하는 문지기Gate Keepers)가 아니다. 그보다는 금융기관들은 적극적으로 금융상품 판매를 유인하는 게이트웨이(Gateway)역할을 담당해야 한다. 과거 금융기관은 자신이 제공할 수 있는 범위내로 고객의 선택을 제한하는 금융중개 역할만을 수행했다. 그러나 전자금융의 시대에 금융기관들은 전통적인 금융상품 및 서비스를 전통적 접속경로로 고객에게 전달하는데 그치지 말고, 보다 다양한 금융상품과 서비스를 보다 다양한 접속경로로 고객에게 전달할 수 있어야 한다. 결국 금융기관은 자신과 제 삼자간의 신뢰관계를 바탕으로 게이트웨이 역할을 수행함으로 고객이 전세계 어느 곳에서도 부가가치 서비스제공자와 접속할 수 있는 환경을 제공해야 한다.

이런 과정에서 전통적인 금융위험이 변화될 뿐 아니라 새로운 여러 가지 금융위험이 발생된다. 따라서 금융기관은 전자금융위험에 대해 적극적으로 대응할 수 있는 금융위험관리조직을 구성하여 대처해야 할 필요성이 있으며, 이를 통하여 전자금융위험의 발생 가능성에 대해서도 선제적으로 대응해야 할 필요성이 있다.

또한 금융기관이 건전성을 유지할 수 있으려면 전자금융에서 제기되는 위험의 중대성을 인식하고 이에 대한 적절한 보안대책을 마련해야 한다.

금융소비자가 금융기관을 선택하는 요인에는 편리성, 예금이자율, 안전성 등 여러 가지가 있으나 그중에서도 안전성이 가장 중요하다. 물론 모든 금융기관이 이러한 위험을 갖고 있기는 하지만 전자금융의 경우 그 위험도는 더 높다 할 수 있다. 따라서 전자금융업무의 경우 기본적인 신뢰성과 안전성 확보가 무엇보다 중요하다 할 것이다.

본 연구의 한계는 문헌조사를 위주로 인터넷의 활성화에 따른 새로운 전자금융위험의 제기와 그에 대한 대응책을 모색하고 있다는 것이다. 향후 보다 심도 깊은 연구를 위해서는 전문가 인터뷰 등을 통한 통계적 분석 및 검증을 모색해야 할 것으로 보인다.

참 고 문 헌

[1] 강임호(2003), 인터넷전문은행의 진입에 관한 연구, 한국금융연구원

[2] 금융감독원(2005), 전자금융거래 및 감독정책.

[3] 금융감독원(2005), 전자거래 안정성 강화 종합대책.

[4] 김자봉 (2006), 최근 전자금융의 발전과 주요이슈, 한국금융연구원.

[5] 김창호(2003), 인터넷전문은행의 설립전망 및 과제, 한국은행.

[6] 김태호 외(2008), 국내 인터넷전문은행 설립시 예상되는 전자금융리스크에 대한 대응방안 연구, 정보보호학회지, 정보보호학회.

[7] 김혜숙, 전자금융채널 도입 성과와 채널 도입-수용 요인 연구, 박사학위논문, 목원대학교.

[8] 심영(2000), 전자금융에 있어서의 위험과 감독적 규제 방안, 비교사법12, 한국비교사법학회

[9] 이강식(2006), 전자금융거래에 있어서 리스크관리방안에 관한 연구, 박사학위논문, 숭실대학교

[10] 이종세(2008), 금융회사 IT리스크의 효율적 관리방안, 금융위원회

[11] 정현철(2005), 전자금융거래 보안강화 방안, 한국정보보호진흥원.

[12] 조하현. 이승국(2002), 금융리스크 측정과 관리, 세경사

[13] 조용혁(2001), 전자지급결제의 법정책적 과제, 한국전산원.

[14] 최운열외 (2004), 전자금융의 발달과 통화정책, 한국은행.

[15] 한국은행 (2003), 전자화폐·전자상거래와 금융정책, 한국은행 금융결제국.

[16] 한국은행 (2004), 전자금융과 전자화폐의 발달이 경제에 미치는 영향, 한국은행 금융결제국.

[17] 日本銀行金融研究所 (2002), 電子貨幣·電子商取引と金融政策, 日本銀行.

[18] BIS(1998), Framework for internal control systems in banking organizations.

[19] BIS(2002), The Sarbanes Oxley Act.

[20] BIS(2003 a), Risk Management Principle for Electronic Banking.

[21] BIS(2003 b), Sound practices for the Management and Supervision of Operational Risk.

[22] BIS(2006), Enhancing corporate governance for banking organization.

[23] Green E.J. (1999), 'We Need to Think Straight about Electronic Payment', Journal of Mnoey, Credit and Banking, 31(3), Pt2, August, 668-70.

[24] IMF (2004), "Six Puzzles in Electronic Money and Banking", in http://www.imf.org/external/pubs/ft/wp/2004/wp0419.pdf

[25] Sato Setsuya, Hawkins John. (2001), "Electronic Finance: An Overview of the Issues", BIS Working Paper No. 7.

[26] Sato Setsuya, Hawkins John, and Berentsen Aleksander (2001), E-finance: Recent Developments and Policy Implications, Washington DC, Brookings Institution Press.

인터넷활성화에 따른 전자금융위험에 대한 대응방안과 정책 연구

송경석†

요 약

전통적으로 금융기관이 전자금융을 취급하는 과정에서 제기되는 여러 가지 위험을 경감하기 위한 다양한 수단을 가지고 있지만, 인터넷의 활성화로 인해 새로운 전자금융의 위험이 제기되고 있으나 이에 대한 대응방안과 정책수단에 대한 연구는 미미한 실정이다. 인터넷이 사회적으로 광범위하게 확산되고 이용이 활발해짐에 따라 금융기관에서도 전자금융운영시스템을 인터넷중심으로 바꾸고 있다. 이 과정에서 온오프라인 겸영은행의 전자금융이나 인터넷전문금융기관의 전자금융의 경우 인터넷이 지니고 있는 고유한 특성으로 계좌개설에서 제기되는 새로운 위험이나 아웃소싱과정에서 제기되는 위험 등 새로운 위험이 제기되고 있다. 이러한 위험에 대응하기 위해서는 전자금융위험관리방식을 체계화할 뿐 아니라, 해킹방지, 고객보안강화 등 기술적 물리적 대책도 필요하며 체계적인 아웃소싱위험관리기준의 마련 등 다양한 대응책의 마련이 요구된다.

키워드 : 전자금융, 위험관리, 해킹방지, 아웃소싱

† 호서대학교 디지털비즈니스학부 교수

송 경 석

1988 성균관대학교 무역학과 (경제학사)
1991 성균관대학교 무역학과 (경제학석사)
2001 성균관대학교 무역학과 (경제학박사)
1990-2001 한국산업은행 조사부 조사역
2008.08-2009.08 샌프란시스코주립대학 교환교수
2001-현재 호서대학교 디지털비즈니스학부 부교수
관심분야: 전자금융, 디지털정책
E-Mail: keyong@hoseeo.edu