The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 6, pp.255-264, Dec. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2016.16.6.255
JIIBC 2016-6-33

전자금융 이상거래 분석 및 탐지의 법제도적 한계와 개선방향 연구

A Study on the Institutional Limitations and Improvements for Electronic Financial Fraud Detection

전금연*, 김인석**

Geum-Yeon Jeon*, In-Seok Kim**

요 약 정보통신기술의 급속한 발전으로 경제활동 분야에서 큰 변화를 가져오고 있으며 혁신적으로 변화하고 있는 것은 전자상거래라고 할 수 있다. 더불어 전자금융사기의 방법도 나날이 진화하면서 피해사례도 함께 늘어나고 있다. 이에 따라 전자금융 이상거래에 대한 분석 및 탐지가 되고 있으나 여전히 피해가 발생되고 있는 상황이다. 본 연구에서는 금융환경, 금융 IT 환경, 금융 IT보안 환경과 법제도적인 변화의 특성을 분석하고 현재 금융기관에서 운영되는 이상금융거래 탐지시스템의 한계점을 보완하기 위하여 효과적인 전자금융 이상거래 분석 및 탐지 관리 체계와 외부기관과의 정보공유 및 개인정보 수집 및 활용에 대한 고려사항을 제안하고자 한다.

Abstract Due to the development of information and communication technology, the great change on economics has grown and the biggest change is the e-commerce. With the methods of electronic financial frauds becoming advanced, reported phishing incidents have greatly increased. The Fraud Detection System(hereafter FDS) has taken effect to prevent electronic financial frauds, but economic losses still occurring. This Paper aims to analyze the financial environment, financial information technology environment, financial information technology security environment and some features of the institutional changes. In order to supplement the defect of FDS, it gives some recommendations for the improvement of the effective FDS Management System and information sharing on frauds with some public institution and a major consideration for collection or utilization of personal information.

Key Words : Electronic Banking, Financial Frauds, Fraud Detection System

Ⅰ. 서 론

인터넷뱅킹, 폰뱅킹, 스마트뱅킹 등 전자금융이 활성화되고 간편 결제 서비스의 거래비중이 빠르게 증가함에 따라 전자금융사기도 증가하여 왔다. 보이스피싱, 파밍, 스미싱, 메모리해킹 등 전자금융사기는 계속해서 진화하여 수법은 더욱 지능화되고 있다. 이에 대응하기 위하여 정부는 전자금융사고 시 접근매체의 위조나 변조로 사고가 발생했을 때 고객과실을 입증하지 못하면 금융회사가 책임을 지도록 전자금융거래법을 개정하였다.[1] 그리고 2013년 7월 금융전산 사고를 계기로 금융전산 보안강화 종합대책을 통해 이용자 보호 강화를 위해 금융전산

*정회원, 고려대학교 정보보호대학원 금융보안학과
**정회원, 고려대학교 정보보호대학원 (교신저자)
접수일자 : 2016년 10월 16일, 수정완료 2016년 11월 16일
게재확정일자 : 2016년 12월 9일

Received: 16 October. 2016 / Revised: 16 November, 2016
Accepted: 9 December, 2016
**Corresponding Author: iskim11@korea.ac.kr
Dept. of Information Security, Korea University, Korea

내부통제 강화, 망분리 의무화 등을 권고하였다.[2] 2013년 12월 신·변종 전기통신 금융사기 피해방지 종합대책을 통해 더욱 적극적으로 전자 금융 사기에 대응하려 하였다.[3] 그러나 이러한 대책 이후에도 각종 금융사기로 인한 피해가 지속되어 거래보안수단 만으로는 신·변종 사기행위를 막기에는 어려운 상황이다. 이에 전자금융 이상거래 분석 및 탐지를 통해 사기 예방의 필요성을 부각시키고 있다. 이에 금융위원회에서 금융전산 보안강화 종합대책으로 이미 카드사에서 운영 중인 이상금융거래 탐지시스템(Fraud Detection System, FDS)을 국내 은행들에게도 구축 및 확대를 독려하였다.

이러한 상황에서 안전한 금융거래 환경을 실현하여 소비자를 보호하기 위하여 금융환경, 금융 IT 환경, 금융 IT보안 환경에 대해 살펴보고, 법제도적인 변화의 특성을 면밀히 분석하고 현재까지 운영되어온 이상금융거래 분석 및 탐지에 대한 한계점을 도출하고자 한다. 이러한 한계점을 보완하기 위해 고민할 필요성이 제기된다.
본 연구의 구성은 총 6장으로 구성되었다. 2장에서는 전자금융사고의 유형분석과 피해현황 및 대응현황을 살펴보고 3장에서는 전자금융 거래환경 및 법·제도적 분석, 4장에서는 이상금융거래 탐지시스템 개념 및 프로세스, 한계점에 대해 살펴보고 5장에서 개선방향을 제시하고 6장에서 본 논문에 대한 결론으로 마무리하고자 한다.

II. 관련 연구 및 현황

1. 전자금융사고의 발생

가. 전자금융사고의 유형분석 및 피해현황[4][5]

최근 전자금융사기 수법이 전통적인 보이스피싱 피해는 감소한 반면, 메모리해킹, 스미싱 등 인터넷 및 스마트폰 기반의 고도화된 기법 등을 활용한 신 · 변종 금융사기 및 개인정보 유출이 증가하고 있다.

첫째, 피싱 사기란 기망행위로 타인의 재산을 편취하는 사기범죄의 하나로 전기통신수단을 이용한 비대면거래를 통해 금융 분야에서 발생하는 일종의 특수사기범죄이다. 일반적으로 형법상 '사기죄'가 적용되며, 사례에 따라 '컴퓨터 등 사기이용죄' 또는 '공갈죄' 등이 적용 가능하다.[6]

기존에는 대포통장을 이용해서 피해자를 기망 · 공갈하여 자금을 대포통장계좌로 송금 · 이체시킨 후 현금인출기를 통해 인출하거나 경찰청 또는 국가기관을 사칭하여 개인정보나 금융정보 등을 요구하였으나, 신·변종 보이스피싱은 정상계좌를 이용해 피해자 몰래 피해자계좌에서 귀금속 등 물품 판매자의 정상계좌로 이체하여 물품을 인도 받은 후 현금화하거나, 통신사를 사칭해서 통신사 전화번호로 발신번호 변작 후 통신요금 체납, 핸드폰 교체 이벤트 등을 가장하여 개인정보나 금융정보 등을 요구한다. 최근 금융감독원에 따르면 보이스피싱 사기수법은 서민들의 절박한 심리를 악용하여 신용도가 낮아도 저금리 대출을 받을 수 있다고 속이면서 보증서 발급비, 대출상환 자금을 편취하는 대출빙자형이 2016년의 경우 전체의 68.9%를 차지한다.

둘째, 파밍의 경우 기존에는 정상적인 인터넷뱅킹 사이트에 접속해도 가짜 인터넷뱅킹 사이트로 유도하여 보안카드 번호 등을 탈취하였으나 신·변종 파밍의 경우 정상적인 포털 사이트에 접속해도 가짜 포털 사이트로 유도하여 보안카드번호 전체를 탈취하는 유형이다. 최근 보이스피싱 사기범이 '팀뷰어'라는 원격지원 프로그램을 악용, 피해자의 컴퓨터에 접속하여 직접 자금을 이체하는 신종 파밍 수법이 발생하였다. 이는 정부기관 사칭형 보이스피싱과 결합하여 한층 더 진화한 형태로 기승을 부리고 있다. 금융감독원은 2016년 6월에서 7월 파밍 피해금액은 13억원이었으나, 진화된 수법으로 8월에서 9월 피해금액이 30억원으로 두 배 이상 증가되었다고 발표했다. 이는 사기범이 피해자가 평소 사용하던 컴퓨터를 통하여 자금 이체함으로써 금융회사의 의심거래 모니터링을 회피한 경우다.

셋째, 메모리해킹의 경우 기존에는 인터넷뱅킹 과정에서 악성코드를 이용하여 가짜 팝업창을 띄워 보안카드번호 앞 · 뒤 2자리 숫자를 탈취 후 자금을 편취하였으나, 신·변종 메모리해킹의 경우 인터넷뱅킹 과정에서 악성코드를 이용하여 입금계좌 정보와 이체금액을 변조하여 사기범 계좌로 직접 이체하는 유형이다.

넷째, 스미싱의 경우 기존에는 무료쿠폰, 결제내역 등의 문자 메시지를 누르면 악성앱을 설치하여 소액결제용 SMS 인증번호를 탈취하여 휴대폰 소액결제 피해가 발생하였으나, 신·변종 스미싱의 경우 청첩장, 돌잔치 문자메시지를 누르면 악성앱을 설치하여 개인정보를 탈취하고, 핸드폰에 저장된 모든 사람에게 동일한 가짜 청첩장, 돌잔치 문자메시지가 전송되는 유형이다.

전자금융사고의 유형은 거래 대상이 되는 매체에 따

표 1. 전자금융사기 피해현황(단위:건/백만원)
Table 1. Number of Electronic Financial Fraud by Damage cost

년도	보이스 피싱		파밍		스미싱		메모리 해킹		총계	
	건수	피해 금액	건수	피해 금액	건수	피해 금액	건수	피해 금액	건수	피해 금액
2009	6,720	62,100	-	-	-	-	-	-	6,720	62,100
2010	5,455	55,400	-	-	-	-	-	-	5,455	55,400
2011	8,244	101,900	-	-	-	-	-	-	8,244	101,900
2012	5,709	59,500	-	-	-	-	-	-	5,709	59,500
2013	4,749	55,300	3,218	19,424	76,356	4,807	463	2,762	84,786	79,293
2014.6	2,851	36,900	1,628	6,842	4,459	276	97	522	9,035	44,540
합계	33,728	371,100	4,846	26,266	80,815	5,083	560	3,284	119,949	402,733

라 인터넷뱅킹, 스마트폰뱅킹, 텔레뱅킹, CD/ATM 등으로 구분할 수 있다.

대체로 인터넷 뱅킹 및 스마트폰 뱅킹은 외부자의 해킹, 내부자의 정보유출, 이용자의 파밍에 의한 피싱사이트 피해사례 등으로 구분할 수 있으며 텔레뱅킹 및 CD/ATM은 보이스피싱에 의한 개인정보 절취가 주를 이루고 있다. 표 1에서 보는 바와 같이 보이스피싱은 2009년 이후 꾸준히 발생하는 추세를 보이고 있으며, 파밍과 스미싱, 메모리해킹은 2013년 이후 급증하는 추세를 보이고 있다. 특히 2013년을 기점으로 감독기관의 강력한 정책으로 증가추세가 둔화되고 있지만 사기범들의 신종 사기 수법은 대형화 되고 있다.[7]

나. 전자금융사고의 대응

감독당국과 업계에서는 전자금융사고가 가장 빈번하게 발생하는 클라이언트 구간, 데이터 전송을 하는 네트워크 구간과 해당 데이터가 저장, 활용되는 시스템 구간으로 나누어 사전적 대응을 하고 있다.[8]

2014년 금융감독원에서 전자금융사고에 대한 대응 수준을 강화하기 위하여 이상금융거래 탐지시스템 구축을 독려한 이후에 대부분의 금융사에서는 FDS 도입 및 구축을 완료하였고, 고도화 2단계(FDS 확대, 2015년), 그리고 현재 3단계(금융권 공동대응, 2016년)를 준비 중에 있다. 대부분의 금융사들이 초기에 FDS를 구축하면서 신속한 구축을 위하여 이상거래 탐지에 초점을 두고 시스템을 구축하였으며, 구축된 FDS에서 사용하는 시나리오나 룰들은 기존에 사용하고 있는 유사 시스템인 IP 추적시스템이나 금융사기 예방시스템에서 사용하고 있는 패턴을 그대로 FDS에 적용하였고 이후, 담당자의 경험에 의한 신규 룰들이 추가되었다. 최근의 전자금융 환경은 인터넷, 모바일, 소셜미디어 등 다양한 채널을 통한 고객 맞춤형 서비스가 변화하고 있기에 더욱 다양한 탐지 및 분석 룰들이 필요하게 되었다.

Ⅲ. 전자금융 거래환경 및 법/제도적 분석

1. 전자금융 거래환경 분석

가. 국내 금융환경 변화

인터넷뱅킹 이용건수 및 금액은 일평균 기준으로 6,645만건, 36조8,550억원으로 전년대비 22.4% 9.5% 증가하였으며, 특히 스마트폰뱅킹 이용건수 및 금액이 3,099만건, 1조7,976억원으로 전년대비 각각 45.5%, 31.3% 증가하여 전체 증가세를 주도하고 있다. 표 2 2014년 12월 기준 한국은행 경제통계시스템에 따르면 영업점 창구에서의 대면거래 규모는 점차 감소하는 등 금융환경은 인터넷과 모바일을 중심으로 재편되고 있으며, 금융 IT기술에 기반하여 금융환경의 급격한 변화가 이루어지고 있다.[9]

표 2. 은행 채널별 거래처리 비중(단위:%)
Table 2. Ratio on Online Transaction of Channels

구분	대면 (창구) 거래	비대면거래			
		소계	CD/ ATM	텔레 뱅킹	인터넷 뱅킹
입출금 및 이체거래	11.6	88.4	39.9	13.1	35.4
조회거래	13.9	86.1	4.0	4.8	77.4

금융과 IT기술이 융합된 핀테크가 최근 모바일 간편결제 서비스를 시작으로 대출, 외환, 크라우드 펀딩 등 금융업무 전반으로 확산되고 있다. 금융사 뿐만 아니라 통신사, IT전문회사 및 유통사까지 가세하여 경쟁적으로

서비스를 출시하며 핀테크 시장이 과열 양상 조짐을 보이고 있다. 그러나 보안성에 대한 철저한 검토없이 시장 선점을 위한 시장 적시성(Time To Market)에만 치중하고 있어 보안에 대한 우려의 목소리가 커지고 있다. 따라서 진정한 핀테크 성공을 위한 전제 조건이 '보안'과 '신뢰'에 있음을 시장 참여자 모두 다시 한번 각인해야 할 시점이다.

나. 국내 금융IT 환경의 변화

국내 금융 IT 환경은 1999년 금융 역사의 획기적인 혁명이라 할 수 있는 PC기반 인터넷뱅킹이 등장하였으며, 2003년에는 그동안 사용상의 불편함 때문에 사용률이 저조했던 무선 애플리케이션 프로토콜(Wireless Application Protocol) 기반의 모바일 뱅킹을 대체하는 금융 IC칩 방식과 가상머신(VM)방식의 모바일뱅킹이 등장하였다. 2009년 애플사의 아이폰을 필두로 한 스마트폰의 열풍에 따라 모바일뱅킹은 스마트뱅킹으로 진화하게 되고, 스마트폰 대중화에 힘입어 스마트뱅킹의 이용자수도 증가하게 되었다. 지금까지 금융 IT는 금융 비즈니스를 지원하는 도구 수준의 물리적 결합수준에 머물렀으나, 현재는 금융 비즈니스와 IT기술이 화학적 융합을 통하여 시너지 극대화를 꾀하고 있다. 이러한 융합은 핀테크로 대변되는 새로운 금융 패러다임의 등장을 이미 예고하였으며, IT분야의 빅데이터 및 사물인터넷 기술의 발전은 이러한 핀테크의 고도화를 더욱 가속화시키고 있다.

금융 비즈니스의 예금, 증권 및 보험 등 전통적인 금융 비즈니스의 금융사별 경계를 허무는 융.복합 사례가 증가함에 따라 금융 비즈니스는 더욱 복잡해지고 있다. 또한 금융IT기술이 발전함에 따라 스마트폰과 웨어러블(Wearable)등 금융 채널은 더욱 다양해지고 있다.

다. 국내 금융IT 보안환경의 변화

금융보안은 규제 중심에서 자율과 책임 중심으로, 정부 주도의 보안에서 금융회사 중심으로 변화되고 있다. 또한 고객 중심의 사전대응에서, 금융회사가 다양한 대체인증 수단을 마련하는 등 보안을 강화하는 방식으로 변화했으며, 사전예방에서 사후점검과 복구와 회복에 중점을 두는 방향으로 변화하고 있다. 특히 보안이 비용보다는 투자라는 인식으로 변화하면서 CEO와 경영진뿐만 아니라, 전 직원이 참여해 주도하는 보안으로 변화하고 있다.

이렇게 금융보안 환경이 변화에 따라 금융위원회와 금융감독원은 2015년 6월 19일, 금융IT부문 자율보안체계 확립 방안으로 금융회사의 자율점검을 강화하기로 발표하였다. 즉, 금융회사가 자체감사로 IT보안의 부족한 부분을 보완하고, 금융감독원이 이행결과를 사후 관리한다는 것이다. 이는 금융회사의 IT보안상 취약점은 해당 금융회사가 가장 잘 파악할 수 있기 때문이다.

2. 전자금융 관련 법 · 제도적 분석

가. 전자금융거래법 및 전자금융 감독규정 분석

2012년 11월 이후 2013년 2월까지 금융 사고는 323건, 약 20.6억의 피해가 발생하였고, 이에 따라 정부는 소비자 보호 요구 강화를 위해 전자금융거래법을 금융소비자 위주로 다음과 같이 개편 강화하였다.

첫째는 접근매체의 위조나 변조, 계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고로 고객 손해 발생 시 금융회사가 손해를 배상한다. 둘째는 현행 전자금융 사고 이외에 해킹사고로 고객 손해 발생 시 금융회사에 손해 배상 책임을 부과한다. 전자금융거래법은 고객이 피싱, 스미싱, 메모리 해킹으로 고객 예금이 탈취될 경우 금융사에 책임을 부과하여함으로서 금융기관의 시스템 강화만이 금융사고에 의한 손해를 최소화 할 수 있다. 표 3과 같이 정부 및 금융당국은 2013년 7월 금융전산 사고(3.20)를 계기로 금융권 전산보안 전반에 대한 실태점검과 TF운영을 통해 종합 개선대책을 마련하였다. 금융전산 위기 대응 체계 강화, 전자금융 기반 시설 보안강화, 보안조직 인력 역량 강화, 금융이용자 보호 및 감독 강화, 금융회사의 자율적 보안 노력 지원 등이다. 그 중에 금융이용자 보호 및 감독 강화에는 이상금융거래 탐지시스템 구축 확대, 금융회사 사칭 불법사이트 접속 차단, 보안사고 예방교육 및 홍보 강화 대책이 마련되었다.

또한, 2014년 2월 시행된 전자금융감독규정의 주요 내용은 금융소비자 위주의 규정이 아닌 금융사 내부의 보안을 위한 내부 통제 규정이다. 즉, APT, DDoS와 같은 시스템의 마비사고, 내부 직원에 의한 정보 유출 사고 방지를 위한 규정이라 할 수 있다. 이후, 금융감독원은 증가하는 전자금융사고에 대한 대응 수준 강화를 위하여 이상금융거래 시스템 구축을 독려하였고, 고도화 로드맵을 제시하였고 관련 법/제도도 강화되었다.

표 3. 전자금융 관련 법 · 제도
Table 3. The Collection of Law of E-Banking

법·제도명	발표 시기	주요 내용
금융전산 보안강화 종합대책	'13.07	금융전사 위기 대응 체계 강화 금융회사의 전자금융 기반 시설 보안강화 금융회사의 보안조직 인력 역량 강화 금융이용자 보호 및 감독 강화 금융회사의 자율적 보안 노력 지원
전자금융 감독규정	'14.02	단말기, 네트워크 보호 전산자료 유출방지 정보처리시스템 보호 해킹, 바이러스 방지 공개용 웹서버 관리 대책 IP 주소 보호
개인정보 유출 재발방지 종합대책	'14.03	단계별 정보보호 강화 자기정보결정권 보장 금융회사 책임 강화 사이버 안전대책 강화 예방조치 강화

나. 제도적 분석

인터넷·모바일뱅킹의 이용확대로 인하여 비대면거래의 비중이 증가하면서 금융사고도 꾸준히 증가추세에 있다. 증가하는 금융사고에 대응하고자 금융권도 보안정책 및 기술 가이드를 꾸준히 제시하여 왔다.

첫째, 금융보안원은 금융결제원 및 코스콤의 정보공유분석센터(ISAC : information Sharing & Analysis Center)와 금융보안연구원의 기능을 통합하여 종합적인 금융보안 서비스를 제공하는 기관으로 2015년 4월 10일 설립하여 보안관제, 침해대응, 침해정보공유, 취약점 분석·평가, 금융보안 정책·기술 연구, 금융보안 교육, 금융IT·보안 인증 및 시험·평가 등 종합적인 금융보안 서비스 제공함으로써 금융권 전반의 보안수준 및 금융소비자 보호수준을 한층 강화할 수 있는 역할을 기대하고 있다.

둘째, 금융감독원은 이상거래탐지시스템 구축으로 수동적 사고예방에 머물던 관행에서 능동적 탐지를 통한 금융사고 예방체계 마련과 이상거래탐지시스템을 전자금융거래를 취급하는 은행, 증권 등으로 확대 권고하였다.

셋째, 금융보안연구원은 최근 강화된 전자금융거래 법규에 대한 금융회사의 자체 보안 컴플라이언스 활동을 지원하기 위하여 『금융IT 보안 컴플라이언스 가이드』를 개정하여 회원사에 배포하였다.[10] 가이드는 금융보안 관련 법규 및 국내외 컴플라이언스 사례를 조사·분석하였고, 표 4와 같이 3개 보안영역, 11개 도메인, 178개 통제항목 구성되어 있다.

표 4. 금융 IT보안 통제항목
Table 4. The Control Items in the Financial IT Security

구분	주요내용
3개 보안영역	관리적, 기술적, 물리적 측면의 보안영역
11개 도메인	정보보호정책, 정보보호조직, 인적보안, 물리적·환경적 보안, 운영관리, 접근통제, IT도입·개발·유지보수 관리, 업무연속성관리, 금융정보·거래 보안, 외주주문보안, 보안사고대응
178개 통제항목	'전자금융거래법 및 시행령', '전자금융감독규정 및 시행세칙' 등을 분석하여 도출

Ⅳ. 이상금융거래 탐지시스템

1. 개념 및 탐지프로세스

금융보안원 기술가이드에 따르면 이상금융거래 탐지시스템의 주요기능은 이용자의 정보 및 행위에 대한 정보 수집으로 이용자 매체환경 정보와 사고 유형 정보를 수집한다.[11] 수집된 정보를 통해 이상 행위에 대한 분석으로 이용자 유형별, 거래 유형별 다양한 상관관계 분석 및 패턴을 검사해 이상행위를 탐지한다. 그리고 이상행위로 판단되었을 때 거래를 차단하거나 추가 기능을 요구하여 부당 거래를 방지한다. 또한 정보수집, 분석 및 탐지, 대응 등의 모든 종합적인 절차를 통합 관리하고 탐지시스템을 침해하는 다양한 유형에 대한 감사를 실시한다.

그림 1은 금융거래절차와 FDS간 상호연동 예를 도식적으로 나타낸다. 첫 번째, 이용자인증 단계에서는 이용자를 인증한 후 이용자의 매체환경 정보를 금융회사의 수집시스템으로 전달한다. 두 번째, 거래지시 단계에서는 매 거래시 수집된 정보와 금융회사에서 자체 보유하고 있는 다양한 접속 및 금융거래 정보 등을 분석시스템으로 전달하여 이상금융거래 유무를 분석한다. 세 번째, 거래확정 단계에서는 앞서 분석된 결과를 바탕으로 거래승인 또는 취소여부를 결정한다. 사용자의 평소 거래 패턴을 분석하여 패턴에 위배되는 액션이 취해지게 되면 이상 행위로 판단하기 때문에 패턴분석이 FDS의 핵심 엔진이다.

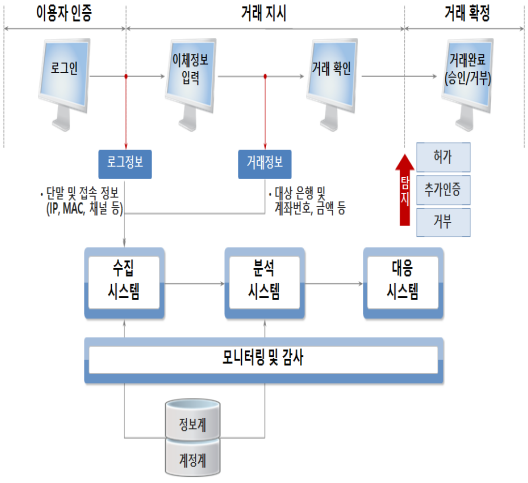

그림 1. 이상금융거래 탐지시스템과 금융거래절차 간 상호연동 예

Fig. 1. The example of Interface between FDS and Financial Transaction Process

2. 탐지모델분석

FDS에서 “분석 및 탐지 기능”은 수집 시스템에서 전달받은 수집 정보를 활용하여 이상 탐지 여부를 판단하는 기능으로 탐지방법은 탐지 모델별로 상이하며, 데이터베이스에 탐지패턴을 저장하여 관리한다. 탐지모델은 서비스 유형에 따라 단일 또는 복합적으로 이용되며 크게 오용탐지모델(Misuse Detection Model)과 이상탐지모델(Anomaly Detection Model)기법이 있다.

가. 오용탐지모델

과거의 부정행위패턴을 기반으로 현재 알려진 패턴과 일치하는지 검사하여 부정행위를 탐지하는 것으로 시그니처 기반 탐지 혹은 지식기반 탐지로 칭하며, 해당 탐지모델은 과거정보(사고정보 등)에 의존하기 때문에, 비교적 과거정보가 많으면 많을수록 탐지의 오탐률이 낮아지는 특징이 있다.

주로 과거 발생된 사고정보만을 이용하여 탐지패턴을 생성하고, 해당 패턴에 정확하게 일치하는 거래에 대해서만 이상금융거래 유무를 판단하는 패턴탐지모델(Pattern Based Model)과 정상적인 거래절차 및 유형을 벗어나는 행위를 패턴화하여 이상금융거래 유무를 판단하는 상태전이모델(State Transition Model)로 나눌수 있다.

나. 이상탐지모델

정상 금융거래 행위(데이터)를 기준으로 상대적으로 급격한 변화를 일으키거나 확률상 낮은 행위가 발생할 경우를 탐지하는 것이 기본 개념으로, 알려지지 않은 부정거래행위에 대한 사전 탐지가 가능하지만, 정상 행위를 예측하기 어렵고 오탐률이 높으며 수집된 다양한 정보를 분석하는데 많은 학습시간이 필요하다.

과거에 이용했던 접속환경 또는 정상적인 금융거래 유형 정보를 바탕으로 이용자 프로파일을 생성하고, 매 거래시 생성된 프로파일을 비교하여 이상금융거래 유무를 판단하는 통계모델(Statistical Approaches Model)과 정형화되지 않은 대량의 데이터를 분석하고 규칙을 발견하기 위해서 탐색하고 분석하는 데이터 마이닝 모델(Data Mining Model)로 나눌 수 있다.

3. 탐지정책분석 및 수립방안

이상 금융 거래의 탐지 정책 및 방법은 이용 환경, 거래 패턴, 거래 사전 행위에 의해 종합적으로 결정이 되어야 하며, 각각의 허용 범위에 따라 이상 금융거래 여부를 판별한다. 새로운 사고유형 발생이나 관련기관의 지침이나 권고사항 등으로 새로운 룰을 생성하여 적용하기 전에 시뮬레이션 기능을 통해 실시간 데이터로 검증한다.

탐지정책 수립시 룰은 룰템플릿(Rule-Template), 탐지 룰(Detection-Rule), 시나리오 룰(Scenario-Rule)로 구성되고, 룰템플릿은 패턴유형과 프로파일유형으로 구성되며, 탐지 룰은 단일 룰과 프로파일 룰로 구성된다.

룰템플릿은 탐지하고자 하는 업무의 가장 기본적인 단위 업무를 룰엘리먼트로 정의한 것으로 패턴유형과 프로파일 유형으로 구성된다. 예로 블랙리스트로 등록된 IP 접근패턴이나 일정기간 동안 휴면계좌의 반복적인 자금이체 행위 유형이 해당된다.

탐지 룰은 엘리먼트로 정의된 룰템플릿을 실제 탐지를 위한 탐지설정을 하는 단위로 1개 또는 2개 이상으로 구성된다. 시나리오룰은 사건의 선후관계를 대조하여 발생된 이벤트의 이상거래를 탐지하는 정책으로 실시간 이벤트 연관분석이 가능한 정책을 설정할 수 있다. 예로 대포통장으로 거래 시 계좌생성일, 입·출금 거래 1회 확인 후 다수의 입금거래 발생유형이 여기에 해당된다. 정의된 Rule Templates를 기반으로 탐지 정책의 기준을 반영한 실제 탐지 규칙을 설정한다.

다양한 데이터 유형과 서비스 형태에 따라 유연하게

대응할 수 있도록 패턴과 프로파일링 룰을 이용하여 상황에 따른 룰셋 정의 및 이상거래 연관 분석에 따른 룰 시나리오를 구성한다. 그리고 모니터링과 유효탐지분석, 변수조정을 통해서 탐지룰에 대한 최적화가 이루어다.

시나리오는 패턴과 패턴, 패턴과 프로파일, 프로파일과 프로파일로 조합한다. 탐지시나리오 구성방안은 첫째, 데이터의 특정 항목을 패턴 매칭하여 이벤트를 도출하는 것으로 블랙리스트 IP, MAC, 계좌번호, 계정 대조 유형이 있다. 둘째, 주기 별로 과거 행위 프로파일 생성 후, 실시간으로 프로파일과 대조하여 이벤트를 도출하는 것으로 3개월 휴면 계정에서 로그인 또는 6개월 동안 접속하지 않던 국가에서 접속 유형이 있다. 셋째, 사건의 연계 사건의 선후 관계를 대조하여 이벤트를 도출하는 경우로 로그인 후 5분 이내 이체한도 조회, 인증서 재발급 후 자동이체 신청, 개인정보 변경 후 계좌이체 시도 유형이 있다.

4. 이상금융거래 탐지시스템의 한계점

첫째, FDS는 다양한 수집정보를 분석/탐지하여 운영정책에 의해 연계·구축되어야 하는 복합적인 시스템이다. 따라서 전사차원에서 부서 간 협조에 의해 상호 연동되도록 구축 및 운영되어야 하지만 R&R에 대한 정의가 부족하여 조직체계가 미흡하거나 IT운영 시스템과 FDS 정책관리 프로세스에도 정비가 필요하다.

금융기관에서 운영하는 IT운영 시스템에는 이상금융거래 탐지시스템과 세부적으로는 다르지만 거시적인 관점에서 전자금융사기 예방을 목적으로 구축되어 대응하는 시스템들이 많다. 하지만 이러한 전자금융사기 예방을 위한 서비스와 제도들은 연계나 통합이 원활하게 이루어지지 않고 있다. 따라서 효과적인 채널 간 연계 범죄 탐지가 어려울 것으로 분석된다.

둘째, 개인정보의 개념 및 범위는 사회 환경, 기술 발전 등에 따라 지속적으로 확대되면서 생체인식정보, 위치정보, 네트워크정보, 전자우편주소, 신용카드 비밀번호, CCTV에 의해 수집된 영상정보 등과 같은 새로운 유형이 지속적으로 출현하고 있다. FDS에서 수집 정보는 금융거래유형 정보, 사고유형 정보와 표4와 같이 이용자가 사용하는 PC나 스마트폰에서 수집하는 정보가 있다. 이러한 정보들은 정확한 사기 탐지를 위해 FDS에서는 중요한 정보이다. 그러나 머신러닝을 활용 시 빅데이터 활용에서처럼 개인정보를 모두 비식별화 처리를 할 수 없는 문제가 존재한다.

표 4. 이용자 매체환경 수집정보
Table 4. The Collection of Information Related to Used Media

구분	수집정보	
	PC 계열	스마트폰 계열
하드웨어 정보	· 물리적 MAC정보 · HDD 정보(S/N 모델등) · CPU 정보(코어수 등 · 메인보드 정보 (제조사, Product Name, Product S/N 등) 등	· UUID 정보 · 디바이스 모델명 등
OS 및 애플리케이션 정보	· 가상화 SW사용정보 · 브라우저 정보	· OS 버전정보 · 제조사 정보
네트워크 정보	· IP정보 (공인/사설, 국가, 지역 등) · Proxy IP 정보 (설정여부, 국가 등) · VPN 정보 (설정여부, 국가 등)	· 연결된 네트워크 정보 등

FDS에서 “개인정보 수집 및 활용”은 다른 법률과의 충돌문제가 존재한다. 즉, 이상금융거래 정보 중 개인정보 수집 및 활용은 『전자금융거래법』 제22조에서는 ‘전자금융기록 보관’에 근거하고 있다. 반면 『개인정보보호법』 제18조 제2항 제4호에 따르면 개인정보 주체의 개인정보자기결정권을 실질적으로 보장하기 위하여 개인정보처리자가 개인정보를 ‘익명화’하더라도 정보주체의 동의 없이는 해당 정보를 통계 목적이나 연구 목적 등으로 제공하는 경우 외에는 제공할 수 없다고 규정하고 있다. 하지만 금융기관은 개인정보가 포함된 빅데이터를 통해서 이상금융거래 분석 및 탐지 등의 목적으로 이를 이용하려고 한다는 점이며 그에 따른 비식별화를 위한 현실적인 주요 쟁점은 개인정보의 범위가 넓기 때문에 비식별화를 해야 하는 데이터의 범위도 불명확하다는 것이다. 또한『위치정보법』, 『정보통신망법』 등에서 개인정보 수집 및 활용을 제한하고 있는 실정이다. 금융권에서 이상금융거래 정보 수집 관련한 법률은 표 5와 같다.

표 5. 이상금융거래 정보수집 관련 법률
Table 5. The laws related to collecting information to FDS

법	조항
전자금융거래법	제22조(전자금융거래기록의 생성·보존 및 파기) 제1항
개인정보보호법	제15조(개인정보의 수집·이용)제1항 1호 제16조(개인정보의 수집 제한)제1항, 제2항
위치정보법	제12조(이용약관의 신고 등)제1항 제15조(위치정보의 수집 등의 금지)제1항 제18조(개인위치정보의 수집)제1항
정보통신망법	제22조(개인정보의 수집·이용 동의 등)제1항

셋째, 전화나 문자메시지를 통해 피해자를 속여 금융거래에 필요한 정보를 입력하거나 직접 물어보는 방식으로 탈취하는 수법은 피해자가 OTP 값과 보안카드 번호 등의 금융 정보뿐만 아니라 인증정보를 스스로 범죄자에게 제공할 가능성이 높다. 전자금융거래에 있어서 부정이용자에 의해 발생되는 거래의 이상 유무를 판단하여 거래차단 혹은 추가인증 등의 절차를 추가하여 사고를 예방 할 수는 있어도, 파밍(Pharming) 등을 통해 이용자 부주의로 입력된 금융정보의 유출을 막을 순 없다는 점이 한계점이다.

V. 제안하는 방법

본 논문에서는 금융환경, 금융IT환경과 전자금융거래법, 개인정보보호법 등 법제도적인 변화의 특성을 반영하여 이상금융거래 분석 및 탐지를 위해 다음과 같은 제안을 하고자 한다.

첫째, 효율적이고 효과적인 이상금융거래 탐지시스템 서비스 제공을 위하여 그림 2와 같이 전사 FDS 관리체계를 제안한다. FDS 관리체계에는 전사적 FDS 규범 체계, FDS 관리 조직/역할 체계, 관리 프로세스 체계, IT 운영 정책으로 구성되며, FDS 정책 체계로 구성한다. 전사적 FDS 규범 체계는 정보화 관련 법령 및 규정을 기반으로 절차서, 매뉴얼 등으로 구성된다. FDS 관리 조직/역할 체계는 현업부서와 IT부서, 정보보호부서 등이 참여하는 협의체가 구성되어 공식적인 의사소통 채널을 확보한다. 현업부서에서 개인고객 뿐만 아니라 법인 및 외국인 고객의 통장개설 시 관련 내부통제 강화를 유도하고 개설자가 직원이 아닌 경우 등 의심스러운 경우에는 모니터링계좌로 관리하도록 한다.

관리프로세스 체계는 정책을 정의, 설계, 변경, 현행화 등으로 구성되며, IT 운영 정책은 IT 인프라 정책, 운영정책 등으로 운영관리 항목으로 정의된 구성요소에 대한 운영 상태를 관리한다. 탐지한 내용을 분석하고 대응하기 위하여 전문적인 지식과 업무경험을 가진 모니터링 인력의 육성도 매우 중요하다. 그리고 국내 FDS 규제가 채널 보안 강화에 집중되어 있지만, 향후 자금세탁방지나 외환거래, 계정거래에서 사기 유형거래를 검출하는 형태로 확대를 고려한다면 이러한 업무 경험을 가진 모니터링 인력 확보가 금융소비자 보호에 효과적이다.

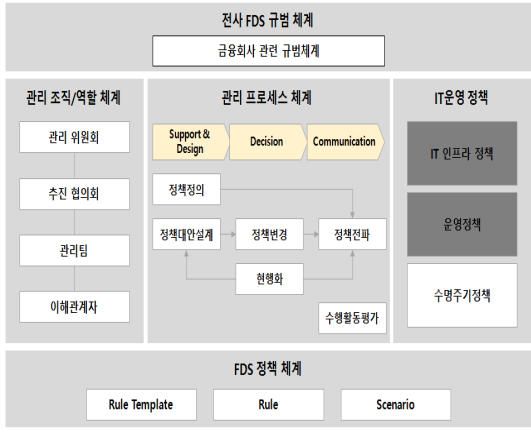

그림 2. FDS 관리체계
Fig. 2. The Management System of FDS

둘째, 정보가 결합하여 개인 식별 가능성을 가질지 알 수 없는 모든 정보들에 대해 사전에 모든 이용자들에게 동의를 구하는 것은 현실적으로 불가능하다. 따라서 완벽한 개인정보보호는 어렵지만 법적 허용 범위 안에서 비식별처리와 재식별 방지 및 지속적인 모니터링이 필요하다. 그리고 이상금융거래 정보 수집 관련 법적 이슈에 대해서는 금융회사 등이 의무를 이행할 수 있는 『전자금융거래법』 상에서 '개인정보 수집 및 활용' 관련 예외조항 추가 등 법령의 통일적인 개정 여부에 대해 지속적으로 검토 및 모니터링이 필요하다.

셋째, 이용자 부주의로 입력된 금융정보의 유출을 막기 위해 금융범죄의 숙주 중 하나인 대포폰에 대한 강력한 단속이 필요하다. 대포통장 이외에 보이스피싱 등 금융범죄의 핵심도구인 대포폰의 부정사용을 방지하기 위해 휴대폰의 양도 시 이동통신사의 사전 승낙을 의무화하고 부정 사용된 휴대폰의 계약자 본인확인 요청 거절 시 사용을 정지하는 것이다. 또한 여권만 소지한 외국인의 단기간 다수의 계좌 개설을 방지하기 위해 은행연합회에 여권번호를 등록하여 금융회사 간 공유한다.

금융보안원에서 FISS 정보공유시스템을 통해 각 금융회사에서 탐지된 이상행위정보 혹은 의심정보를 공유하고 있다. 그러나 한국인터넷진흥원 등 유관기관이나 관련 기업으로부터 사이버 위협 정보를 수집·공유하고, 은행연합회, 한국소비자보호원, 공정거래위원회, 경찰청, 출입국관리소 같은 외부 기관들과 유기적인 정보교환 통로의 구축이 FDS 시스템을 더 효율적으로 만들어 줄 수 있을 것이다.

Ⅵ. 결 론

본 연구에서는 금융환경, 금융 IT 환경, 금융 IT보안 환경과 법제도적인 변화의 특성을 분석하고 현재 운영되는 이상금융거래 탐지시스템의 한계점을 보완하기 위해 세 가지를 제안하고자 한다.

첫째, 금융기관의 효율적이고 효과적인 이상금융거래 탐지시스템 서비스 제공을 위하여 전사적 FDS 규범 체계, FDS 관리 조직/역할 체계, 관리 프로세스 체계, IT 운영 정책 , FDS 정책 체계로 구성되는 전사 FDS 관리 체계이다.

둘째, 수집정보가 결합하여 개인 식별 가능성을 가질지 알 수 없는 모든 정보들에 대해 사전에 모든 이용자들에게 동의를 구하는 것은 현실적으로 불가능하므로 완벽한 개인정보보호는 어렵지만 법적 허용 범위 안에서 비식별 처리와 재식별 방지 및 지속적인 모니터링이 필요하다.

셋째, 이용자 부주의로 발생하는 전자금융 사고를 막기 위해 유관기관이나 관련 기업으로부터 사이버 위협 정보를 수집·공유하고, 외부 기관들과 유기적인 정보교환 통로의 구축이 필요하다.

이상금융거래 탐지시스템은 잘 운영된다면 이상 금융거래를 적발해내고 방지하는데 큰 도움이 되는 시스템이다. 하지만 모든 시스템이 그러하듯이 이상금융거래 탐지시스템이 모든 이상 거래를 탐지해주고 사전에 방지해준다고 맹신해서는 안 된다. FDS 출발 자체가 결코 완전무결할 수 없는 보안 체계 및 시스템 모니터링을 통해서 지원하는 보완재의 성격이기 때문이다. 본 제안이 금융감독 당국과 금융회사의 사기 방지 대책 관련 연구에 도움이 되리라 예상된다.

References

[1] The Electronic Financial Transaction Act Article 9, May, 2013
[2] FSC(Financial Service Commission), "Financial Security Comprehensive Plan", Nov, 2013
[3] FSC, "Comprehensive Measures to Prevent the New and Variety Form Telecommunications Financial Fraud", Aug, 2014
[4] Dae Yong Jeong, Kyung-bok Lee and Tae Hyoung Park, "A Study on Improving the Electronic Financial Fraud Prevention Service : Focusing on an Analysis of Electronic Financial Fraud Cases in 2013", Dec, 2014
[5] Jae-Mo Seung, Su-Mi Lee, Seung-Ho Ahn, Bong-Nam Noh, "The End-to-End Encryption for Enhancing Safety of Electronic Financial Transactions," Journal of the Korea Academia-Industrial cooperation Society(JKAIS), Vol. 10, No. 8, pp. 1920-1925, 2009.
DOI : https://doi.org/10.5762/kais.2009.10.8.1920
[6] Kim, J. S., "Trading for over phishing detection assay fraud prevention", Dec, 2013
[7] Number of Electronic Financial Fraud by Damage Cost, Korean National Police Agency, 2014
[8] Han-Jun Lee, In-Seok Kim, "A Study on Improving Cyber Liability Insurance for Electronic Financial Incident in Easy Payment System," The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 16, No. 2, pp. 1-8, 2016.
DOI : https://doi.org/10.7236/jiibc.2016.16.2.1
[9] The Bank of Korea, "Economic Statistic System: ECOS", 2014
[10] Financial Security Agency, "Compliance guide of Financial IT Security : 2014", 2014
[11] Financial Security Agency, "Technical guide of Fraud Detection System", 2014

저자 소개

전 금 연(정회원)

- 1991년 : 숭실대학교 전자계산학과(학사)
- 2015년 3월~현재 : 고려대학교 정보보호대학원 금융보안학과 석사과정

<주관심분야 : 전자금융보안, 전자금융법규, 정보보호정책 등>

김 인 석(정회원)

- 2008년 : 고려대학교 정보경영공학과 박사
- 2009년 ~ 현재 : 고려대학교정보보호대학원 교수
- 현 FDS산업포럼 회장, 한국사이버정보전학회 운영위원 등

<주관심분야 : 전자금융보안, IT감사, 전자금융법규 등>