

전자금융거래 이상징후 분석을 통한 사고예방 효과성에 관한 연구

A Study of Accident Prevention Effect through Anomaly Analysis in E-Banking

박은영(Eun Young Park)*, 윤지원(Ji Won Yoon)**

초 록

금융회사는 인터넷뱅킹, 스마트폰뱅킹 등 비대면 서비스를 위해 다양한 사용자 단말 환경을 통해 전자금융거래 서비스를 제공하고 있다. 그러나, 이러한 서비스는 기본적으로 사용자의 보안인식 및 기술적 대응의 한계로 인한 금전사고가 빈번하게 발생하고 있어 금융 감독 당국으로부터 보다 근본적인 보호대책이 요구되고 있다. 이에 따라, 금융권에서는 전자금융거래에서 발생하는 금전사고를 예방하기 위해 사용자의 전자정보, 접속정보, 거래내용 등을 종합적으로 분석하고 탐지하여 이상 금융거래를 차단하는 금융보안연구원에서 제시한 “이상 금융거래 탐지시스템 구축 가이드”에 따른 시스템을 구축하거나 계획하고 있다. 본 논문에서는 금융회사에 구축되어 운영 중인 이상 금융거래 탐지 및 차단시스템의 구축사례와 운영현황을 살펴보고, 좀 더 개선된 방식의 시스템을 구성하여 분석을 통한 사고예방의 효과성과 이후 보안대책에 대한 개선방안을 제안하고자 한다.

ABSTRACT

Financial companies are providing electronic financial transactions through a variety of user terminals for non-face-to-face services such as Internet banking, smart phone banking, or etc. However, in these services users' security awareness and the limitations of technical responses has frequently caused the financial loss so that fundamental protection measures are required from financial authorities. Accordingly, financial industry is planning and establishing systems that block unusual financial transactions by comprehensively analyzing and detecting user's electronic information, access information, transaction information, and so on in accordance with "Guide for building Unusual financial transactions detection system" to prevent the financial loss that happens in electronic financial transactions. In this paper, we analyze case studies of unusual financial transactions detection and prevention system that is built and operated in financial companies and current operating status and propose effects of the accident prevention and security measures later.

키워드 : 전자금융, 사고예방, 이상징후

Electronic Banking, Accident Prevention, Anomalies

* Co-Author, Graduate School of Information Security, Korea University(sara7499@korea.ac.kr)

** Corresponding Author, Graduate School of Information Security, Korea University(jiwon_yoon@korea.ac.kr)
2014년 10월 30일 접수, 2014년 11월 06일 심사완료 후 2014년 11월 07일 게재확정.

1. 서 론

인터넷의 보급은 PC와 스마트 폰 뿐 만 아니라 스마트 위치와 같은 다양한 사물 인터넷(IoT, Internet of Things)제품의 확산에도 영향을 미쳤다. 사람들은 시간과 장소의 제약을 받지 않고 다양한 서비스를 즐길 수 있게 되었으며, 이에 맞춰 금융 회사들 또한 다양한 전자금융 서비스를 제공하기 시작했다. 2013년 조사에 따르면, 모바일 뱅킹을 포함한 인터넷 뱅킹의 가입 고객 수만 약 9,549만 명이며, 이 수는 전년 말의 8,643만 명에서 꾸준히 증가했음을 나타낸다. 증가하는 고객의 수와 함께 월 평균 거래금액 또한 약 33조를 돌파하며 그 성장세를 보여주었다[1]. 하지만 전자 금융거래가 확산되어 감에 따라 이를 노리고 사용자들의 금융거래 정보나 현금을 탈취하는 사고 또한 증가하였다. 한국인터넷진흥원에서 발표하는 인터넷 침해사고 정기 보고서 및 통계에 따르면 악성코드 감염 탐지는 총 5만여 건, 해킹사고 접수 처리 현황은 매월 거의 1000건, 국내 피싱 사이트 대응 현황 800여건, 악성코드 은닉사이트 탐지조치 현황은 매월 3000여건에 이르며, 매달 증가추세를 보이고 있다[2].

최초의 인터넷 뱅킹 사고는 지난 2005년에 악성 프로그램을 이용한 것이었으며 2008년, 2009년에는 공인 인증서나 자금을 노리는 여러 해킹 사고가 발생했다. 이에 대한 대응으로 2005년부터 전자 금융 정보 보안 종합 대책이 세워졌으며, 2007년에는 OTP센터를 구축했다. 이러한 대응에도 불구하고 전자 금융 사고의 유형은 보안 스피싱과 함께 대출사기, 인터넷 피싱, 파밍, 메모리해킹 등의 신종 전자금융

사기행위가 2012년 이후 전 금융권을 대상으로 대폭 증가하였으며 또한 고도화와 함께 그 종류도 다양해졌다. 이에 따라 정부의 대응책 또한 끊임없이 변화하고 있는 상황이다[9, 10].

이러한 정부의 전자금융사고 발생 이후 이루어진 지속적인 대응 변화는 일면 긍정적 효과를 보여 왔다. 하지만, 이러한 대응책들은 공격자가 공격의 방식을 조금만 바꾸면 쉽게 우회해 가능하기에 최근에는 여러 가지 우회가 가능한 고도화 과정을 거친 사기 수법들이 등장하고 있다. 그로 인해 등장한 것이 일시적인 대응책이 아닌, 사용자의 패턴을 분석하여 공격자의 공격을 구분해 낼 수 있는 이상 금융 거래 분석 기법이다. 본 논문에서는 현재 금융 회사에 구축되어 있는 이상 금융거래 탐지 및 차단 시스템의 운영 현황 중 블랙리스트 기반 이상거래 탐지 시스템을 살펴보고, 효과적인 사고 예방을 위한 고객 거래 패턴을 이용한 새로운 이상 금융거래 방안을 제시한다.

본 논문의 구성은 다음과 같다. 연구 배경에서는 금융보안 연구원의 이상 징후 탐지 시스템에 관한 가이드를 통해 기존의 이상 금융 거래 탐지 시스템의 정의와 탐지 방법 등을 살펴본다. 제 3장에서는 현재 금융회사에서 구축되어 운영 중인 블랙리스트 기반의 이상 금융거래 분석 시스템의 운영 현황을 살펴본다. 그와 더불어 사고 탐지 후 대응까지의 과정을 살펴본다. 다음으로는, 이렇게 살펴본 기존의 시스템에서 찾은 한계점을 바탕으로 고객의 프로파일링 기법을 도입한 개선 방안을 도출하고 개선된 시스템을 제안한다. 간단한 시나리오 대입을 통해 그 효과를 분석하고 결론을 도출하고 향후 연구 보안되어야할 개선점을 제안하는 것으로 논문을 마무리한다.

2. 연구 배경

본 장에서는 스마트 폰이나 인터넷을 통한 금융서비스를 제공함에 있어서 사기 수법의 진화 과정과 은행의 대응조치 및 결과를 살펴보고 새로운 사기수법 출현에 따른 즉각 대응할 수 있는 이상징후 탐지 시스템 마련의 필요성이 대두된 사회적 배경을 살펴본다.

2.1 전자금융거래의 사고 및 대처 현황

2.1.1 피싱 사이트 유도

‘피싱 사이트’로 접속을 유도하여 탈취한 고객정보로 자금을 이체하는 보이스 피싱이나 스미싱 등에 따른 전자금융사기 피해액이 최근 5년간 약 4000억 원에 달하는 것으로 나타났다. 이후 금융회사는 심야시간 해외 IP 접속 고객에 대한 인증서 발급 차단 및 인터넷 뱅킹을 통해 1일 300만 원 이상을 이체할 경우 본인확인 절차를 강화하는 것으로 2013년 9월 26일부터 모든 금융기관에서 전자금융사기 예방서비스를 시행하였고, 결과적으로 금융사고금액이 대체적으로 300만 원 미만으로 제한되는 결과를 보였다[3].

2.1.2 신종 파밍 수법

금융회사의 정상적인 은행 사이트에서 인터넷 뱅킹을 하는 사용자들의 보안카드 일부 번호만을 빼내 돈을 가로채는 신종 금융사기 피해 사례 발생하였다. 사용자가 보안카드 앞 뒤 2개 번호를 제대로 입력해도 ‘오류’가 나게 한 뒤 이 번호를 입수해 돈을 빼내는 방식의 수법이다[4]. 이후 금융회사의 대응조치는

보안카드 난수 재발행시 추가인증을 시행하도록 전자금융거래 프로세스를 변경하였다. 이후로는 신종 파밍 사고는 더 이상 증가하지 않았다.

2.1.3 피싱 사기 앱 수법

금융회사의 금융권 모바일 뱅킹 어플리케이션(앱)을 위장한 피싱 앱이 등장해 SMS피싱 및 업그레이드를 유도하는 방식으로 사기 앱을 설치하도록 하여 고객정보 및 SMS 인증번호를 모두 탈취하는 사고가 발생하였다. 이후 금융회사는 SMS 추가인증 수단 보안을 강화하고 ARS 음성 멘트를 개선하는 방향으로 SMS 탈취로 인한 사고 발생률을 줄일 수 있었다[5].

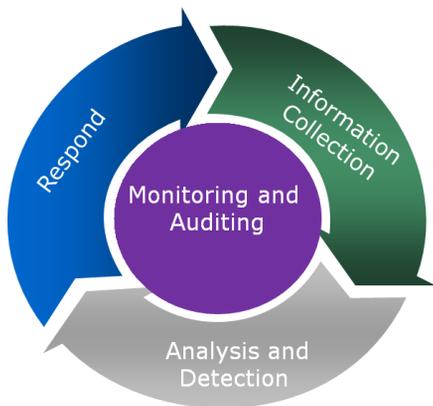
위와 같이 사기범들의 사기수법의 진화과정을 보면 향후 어떠한 사기수법이 등장하여 고객의 자산을 탈취할지 예상할 수 없는, 점점 고도화된 수법으로 진화해 왔음을 알 수 있다. 즉, 이러한 사기 수법들에 능동적으로 대응하고 사기를 예방하기 위해서 무엇보다도 선제적 대응이 필요하며 이를 위한 지속적인 관리 시스템이 필요한 상황이다.

2.2 이상 금융거래 탐지 시스템 기술가이드 및 운영 현황

금융회사들이 전자금융서비스를 제공함에 있어 서비스의 비약적인 발전과 함께 금융거래정보 탈취 및 변조 등 관련 보안위협이 급증하면서 안전한 보안 방안과 대응이 시급한 실정이다. 과거의 보안 사고에 대한 금융회사의 대응방안을 살펴보면, 각각의 특수 사건에 해당되는 조치 방법으로, 모든 금융 서비스에

일괄 적용하는 방식이었다. 향후 개선된 조치 방안이 필요며, 사기범 및 고객의 거래패턴 분석을 통한 차별적인 보안정책을 적용할 필요가 있다. 즉, 고객별 개인화된 보안정책 제공을 통한 선제적이고 지속적 전자금융 사고 예방의 필요성이 대두된 것이다.

금융보안연구원에서 제공된 「이상 금융거래 탐지시스템 기술가이드」에 따르면, 전자 금융거래의 다양한 채널과 매체를 통해 수집된 정보를 종합적으로 분석하여 이상 금융거래 유무를 판별하는 복합적인 시스템으로 FDS (Fraud Detection System)을 정의하고, 아래 <Figure 1>과 같이 이용자의 거래정보 및 행위에 대한 정보를 수집하는 ‘정보 수집’ 기능, 수집된 정보를 통해 거래 분석을 수행하고, 이상거래를 탐지하는 ‘분석 및 탐지 기능’, 분석 및 탐지된 거래 유형에 따른 ‘대응’ 기능을 가지고 있어야 하며, 이런 수집, 분석/탐지, 대응 단계의 상호 밀접한 관계를 유지하면서 효율적인 기능을 위해 보안 역할을 하는 ‘모니터링 및 감사’ 기능. 크게 4가지 기

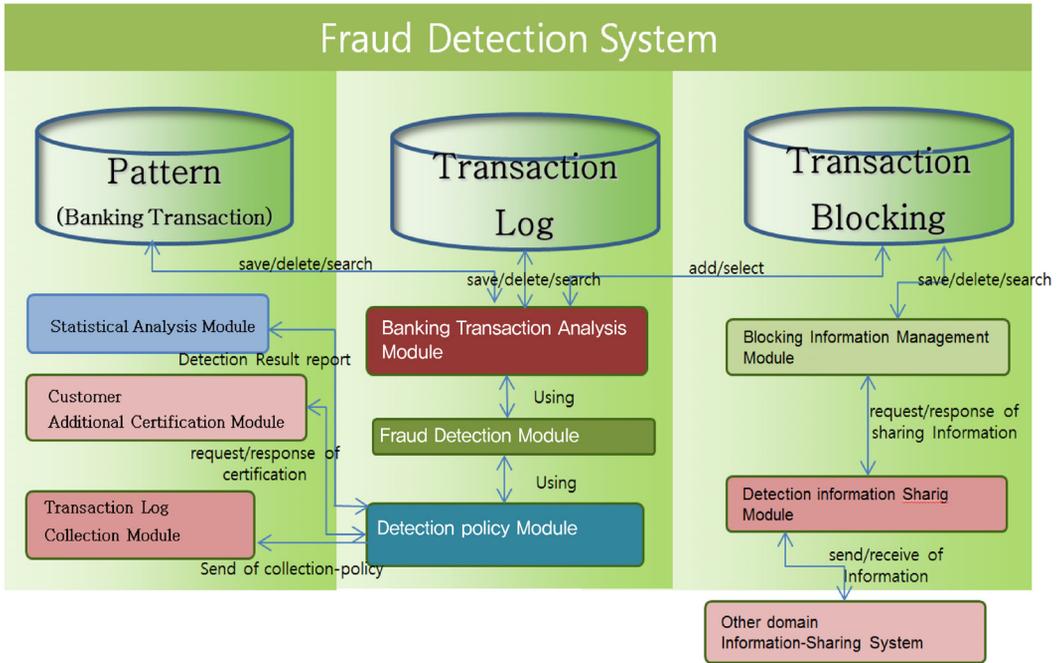


<Figure 1> Unusual Financial Transaction Detection System for Components

능으로 기본적 구성을 갖춰야 한다고 기술하고 있다[6].

금융 회사 중에서 FDS(Fraud Detection System)을 우선적으로 적용 및 모범 효과를 보고 있는 신용카드사와 보험회사의 시스템 및 대응 방법을 살펴 볼 필요도 있다. 금융 감독 당국과 카드업계는 보이스 피싱 피해방지 대책으로 다음과 같은 카드론 지연입금제도를 이미 2012년 5월 17일~21일부터 시행하였고, 카드 론을 최초 이용한 경우가 카드론 보이스 피싱 피해의 대부분(87%)을 차지하고 피해자의 72%가 2시간 이내에 피해 사실을 인지함에 따라 카드업계는 카드론 최초 이용자가 300만 원 이상 신청한 경우 승인 후 2시간 지연입금을 하였다. 은행 시스템에도 비슷한 ATM지연 입금서비스가 시행되고 있다[7].

한국정보통신기술협회에서는 이미 2012년부터 이상 금융거래 탐지 및 대응 프레임워크에 대한 표준가이드를 발표하였으며, 이 표준은 전자 금융 환경에서 금융거래의 보호를 위해 이상 금융거래의 탐지를 위한 요구사항과 시스템의 기능을 제시하고 있고, 아래 그림과 같은 이상 금융거래에 대한 거시적 관점에서의 탐지/대응 프레임워크를 제시함으로써 향후 각 금융사는 유사한 대응 체계의 개발과 시행을 위한 기본 지침으로 활용하고 있다[8]. 특히 주목할 내용으로는 아래 <Figure 2>와 같이 각 금융회사 및 관련 기관의 이상 금융거래 탐지 관련 정보를 교환하는 탐지정보 공유 모듈에 대한 가이드를 제공함으로써, 각 금융회사의 FDS 운영 및 탐지 정보의 공유 및 공동 대응의 필요성을 강조하고 있다.



<Figure 2> Detail Structure of FDS from Telecommunication Technology Association 20

3. 블랙리스트 기반 이상거래 탐지 시스템

현재 금융사의 이상거래 탐지 시스템의 하나로 블랙리스트 기반 시스템의 내용과 금융사의 사고에 대한 대응 및 조치 현황을 살펴본다.

3.1 블랙리스트 기반 이상거래 탐지 시스템

현재 금융회사에 적용되어 있는 이상 금융거래 탐지를 위한 시스템은 주로 과거 사고 발생 PC 정보만을 이용하여 추가 피해를 방지하는 용도로 주로 사용한다. 사고 발생

PC 정보만을 이용한 블랙리스트 기반의 탐지 방법은 전자금융거래에 이용된 매체의 정보는 <Table 1>의 해당 정보에 기반하여 수집한다. 이렇게 수집한 정보들의 목록은 각 운영체제별로 구분지어지며 <Table 2>는 윈도우 환경에서, <Table 3>은 mac 환경에서 수집되는 정보들을 나타낸다. 이렇게 수집된 매체환경 정보와 거래정보가 정확하게 일치하는 거래에 대해서만 이상 금융거래 유무를 판단하는 모델로 대부분의 금융회사에서 사용하고 있다. <Figure 3>은 현재 블랙리스트 기반의 이상 거래탐지를 위한 시스템 구성도로 이번 연구를 위해 같은 시스템을 이용하여 구성하고 추가로 분석 시스템을 이용하였다.

<Table 1> The Collection of Information Related to PC Information Used as Media in the Electronic Financial Transaction is as Follows

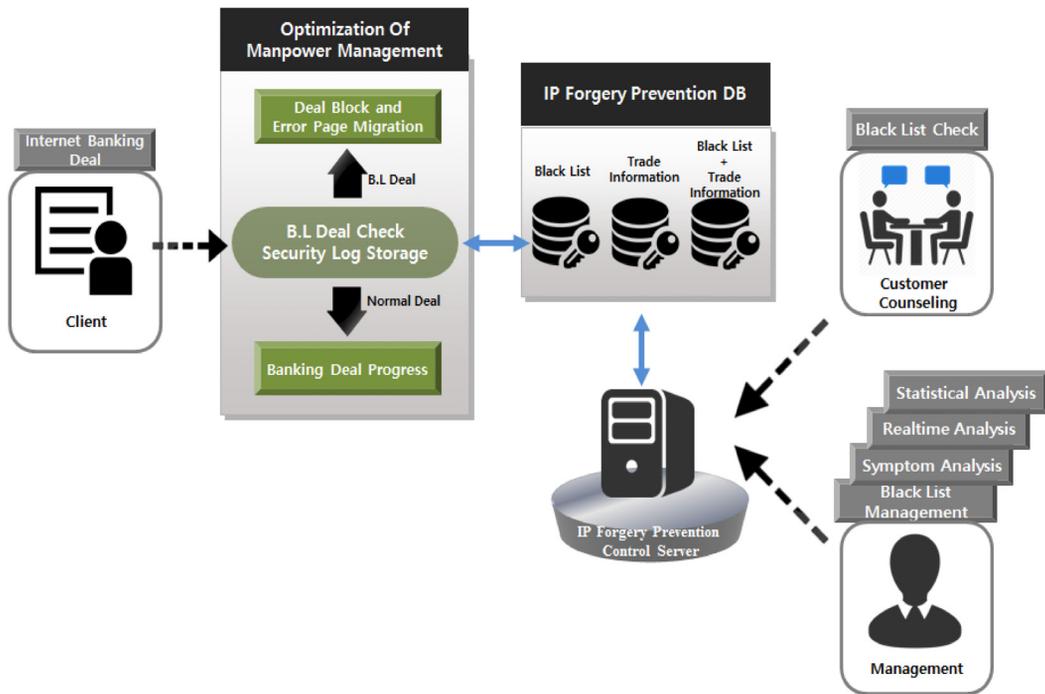
Major categories	Sub-categories	Explanation	Window		Mac	
			Manager	User	root	General
Hardware	CPU	CPU ID	0	0	X	X
		CPU Identification Number	0	0	X	X
		CPU Process Name	0	0	0	0
	HDD	HDD Model	0	0	0	0
		HDD Serial Number	0	0	0	0
		HDD Volume Name	0	0	X	X
	Mother Board	Main Board Manufacturer	0	0	X	X
		Main Board Product Name	0	0	X	X
		Main Board Serial Number	0	0	X	X
Network	Network	Gateway IP	0	0	0	0
		IP set up in the Local PC	0	0	0	0
		MAC Address	0	0	0	0
		NAT IP	0	0	0	0
		Proxy IP	0	0	0	0
		Proxy Server IP	0	0	0	0
		VPN IP	0	0	X	X
		VPN Local Settings IP(user PC)	0	0	X	X
		Connection IP for remote connection	0	0	X	X
Software	Browser	IE Detailed Version	0	0	X	X
		IE Product Number	0	0	X	X
		IE Version	0	0	X	X
	OS	Keyboard Type	0	0	0	0
		USB Serial	0	0	X	X
		OS Code	0	0	0	0
		OS Version	0	0	0	0
		OS Classification(New)	0	0	0	0
		OS 구분(Former)	0	0	0	0
		OS Main Version	0	0	0	0
		OS Low Version	0	0	0	0
		OS Detailed Version	0	0	0	0
		Whether to apply Window Security Patches	X	X	X	X
Window Service Pack	0	0	X	X		
OS Language Pack	0	0	0	0		
Security	Security Function	Whether to Use Proxy	0	0	0	0
		Whether to set Local PC Firewall	0	0	0	0
		Whether to allow remote access	0	0	X	X
		AOS Status	0	0	X	X
		Netizen Status	0	0	X	X
		King's Keyboard Security	0	0	X	X
		King's Hacking Breaker	0	0	X	X
		Soft Camp Keyboard Security	0	0	X	X
		Soft Forum Keyboard Security	0	0	X	X
		Inca Internet Keyboard Security	0	0	X	X
		Whether to use VPN	0	0	X	X
Whether to exist Certificate Folder in USB	0	0	X	X		

<Table 2> PC Specifications Used as a Medium for Electronic Financial Transactions : Windows

Internet Explorer	Installation Version	2000	XP	Vista	Win 7
	less than 6	Unsupported	Unsupported	No browser	No browser
	6	O	O	No browser	No browser
	7	No browser	O	O	No browser
	8	No browser	O	O	O
FireFox	Installation Version	2000	XP	Vista	Win 7
	3	O	O	O	O
	3.5	O	O	O	O
	3.6	O	O	O	O
	4	O	O	O	O
Opera	Installation Version	2000	XP	Vista	Win 7
	9	O	O	O	O
	10	O	O	O	O
	11	O	O	O	O
	11.1	O	O	O	O
Safari	Installation File	2000	XP	Vista	Win 7
	4	No Browser	O	O	O
	5	No Browser	O	O	O
	5.1	No Browser	O	O	O
	Chrome	Installation File	2000	XP	Vista
4		No Browser	O	O	O
6		No Browser	O	O	O
7		No Browser	O	O	O
8		No Browser	O	O	O
10		No Browser	O	O	O
11		No Browser	O	O	O
12	No Browser	O	O	O	

<Table 3> PC Specifications used as a Medium for Electronic Financial Transactions : Mac

Safari	Installation File	less than 10.5	10.5	10.6	10.7
	3.2.3	Unsupported	O	O	O
	5	Unsupported	O	O	O
	5.1	Unsupported	O	O	O
FireFox	Installation Version	less than 10.5	10.5	10.6	10.7
	3	Unsupported	O	O	O
	3.5	Unsupported	O	O	O
	3.6	Unsupported	O	O	O
	4	Unsupported	O	O	O
	5	Unsupported	O	O	O
	6	Unsupported	O	O	O
7	Unsupported	O	O	O	
Chrome	Installation File	less than 10.5	10.5	10.6	10.7
	10	Unsupported	O	O	O
	11	Unsupported	O	O	O
	12	Unsupported	O	O	O
	13	Unsupported	O	O	O

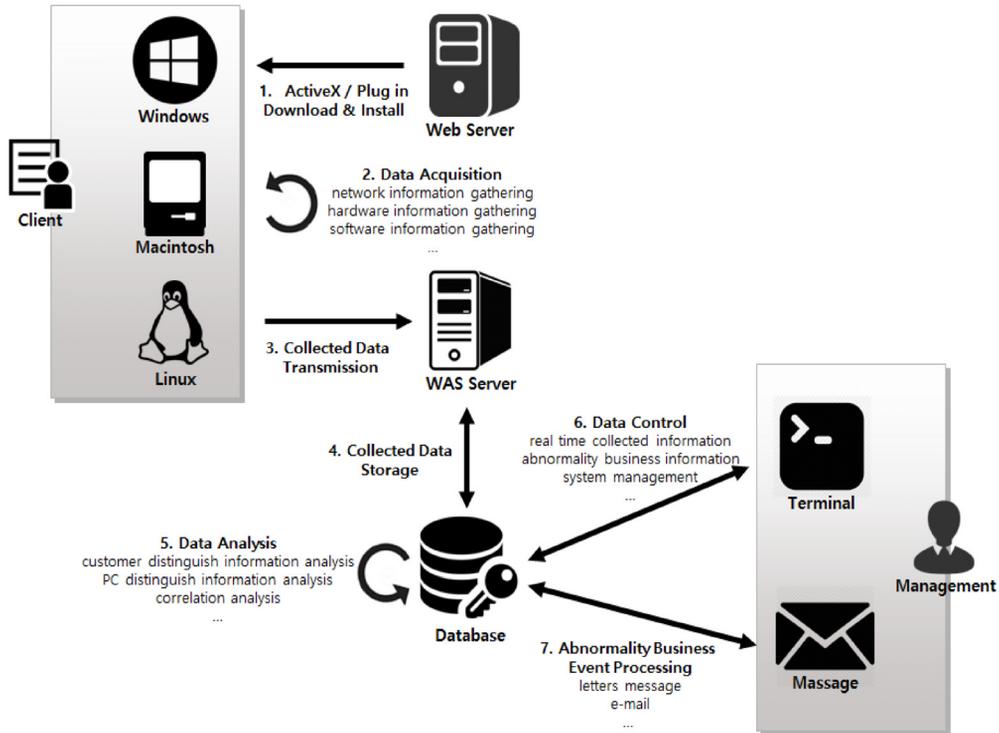


<Figure 3> Detail Structure of FDS from Telecommunication Technology Association 2011

3.2 블랙리스트 기반 이상거래 탐지 시스템의 한계점

현재 금융회사 적용되어 있는 이상 금융거래 탐지 및 분석을 위한 시스템들은 과거에 발생한 사건사고들에서 수집된 이용매체의 특정정보(MAC주소 등)를 차단 룰에 적용하여 동일 PC에서 추가 피해거래가 발생할 경우 차단하는 패턴탐지모델의 초보적인 수준인 블랙리스트 기반으로 구성하고 있다. 특히, 이러한 블랙리스트 기반의 이상 금융거래 탐지 시스템의 주요기능으로 실시간 분석, 이상거래 관리, 통계분석 기능으로 구성되어 있다. 실시간 분석기능은 전자금융거래를 할 때 실시간으로 수집되는 로그인, 이체, 공인

인증서 거래 내역을 조회하고 블랙리스트로 등록된 정보(PC정보 또는 ID)와 일치 할 경우거래를 차단하는 기능이다. 이러한 블랙리스트 기반 시스템 기능은 동일 PC에서 여러 개의 인터넷뱅킹 ID가 사용되거나, 여러 국가에서 동시 다발적으로 사용된 경우 등 매체인 PC정보를 중심으로 이상징후를 분석하는 기능이다. 본 기능은 이상 금융거래 사고 발생 매체 또는 금융회사 간 상호 공유가 되지 않은 블랙리스트 매체인 경우 사전적으로 이상 금융거래를 예방할 수 없는 단점이 있다. 그리고 PC의 수집정보를 기반으로 다양한 통계정보로 기간별, 일자별, 국가별 매체 이용현황을 통해 이상 금융거래 분석을 위한 기초자료로 활용이 된다.



〈Figure 4〉 Detection of Unusual Financial Transactions and the Analysis Flows

3.3 블랙리스트 기반 이상거래 탐지 시스템의 현재 운영방법 및 대응 현황

블랙리스트 기반의 이상 금융거래 탐지 시스템은 이상 금융거래 발생 시 선 차단 후조치를 원칙으로 운영되나, 동일 PC에서 여러 개의 인터넷뱅킹 ID가 사용되거나, 여러 국가에서 동시 다발적으로 사용된 경우 등 매체인 PC정보를 중심으로 이상징후가 탐지된 경우 오탐 여부를 확인 할 필요가 있다. 「이상 금융거래 탐지시스템」의 대응 기능은 분석 및 탐지 기능으로부터 전달받은 결과에 따라 정상, 차단, 추가 인증 등을 수행하는 기능으로 운영한다. 이와 같이 블랙리스트 기반의 이상

거래 탐지 시스템은 기존에 이미 전자금융사고가 발생한 기기로 등록된 단말(PC, 스마트폰, 태블릿)에서 고객 ID로 접속 시도가 있을 경우 실시간으로 인증서 발급 및 이체거래가 차단되는 시스템으로 인터넷뱅킹 이용고객 중에 개인 및 기업 인터넷뱅킹 이용고객을 대상으로 하며, 대부분 블랙리스트 체크가 되는 시점은 해당 주요거래로, 공인인증서 (재)발급, 타행인증서 등록, 즉시이체, 다계좌이체, 적금이체, 예약이체, 예금해지, 펀드이체, 공과금 등의 거래로 제한되고, 고객의 화면에 출력되는 안내메시지는 다음과 같다. “고객님! 금융사기 등으로 인한 비인가자 불법거래 의심됩니다. 콜센터로 연락주시기 바랍니다.”

혹은, 경우에 따라서는 고객에게 정확한 차단 원인 및 조치사항을 안내하지 못하고, 콜센터로 2차 응대가 가능토록 금융사로 고객이 직접 연락하거나 블랙리스트 차단 고객을 대상으로 아웃바운드 안내 전화를 거는 방식으로 운영하고 있다. 블랙리스트 차단 고객의 상세 응대방법으로는 다음과 같은 순서의 절차를 따른다.

- ① 정보보호부 담당자를 통하여 대상 고객 인지 여부 확인
- ② 보안매체 분실등록 및 이용제한등록
- ③ 거래제한 사유 안내. 기존 전자금융사고가 발생한 기기로 등록된 단말(PC, 스마트폰, 태블릿)에서 고객 ID로 접속 시도
- ④ 반드시 PC 및 스마트 폰의 악성코드 감염에 대한 점검조치 후 공인인증서 재발급 및 인터넷뱅킹을 이용하여야 함을 안내
- ⑤ 보안매체 재발급, 계좌비밀번호 변경, 인터넷뱅킹 사용자암호 변경을 위한 영업점 내점안내
- ⑥ 위의 조치가 완료되신 고객님들의 경우 정보보호부 담당자에게 '블랙리스트' 해지 요청

4. 이상 금융거래 탐지 및 분석 실험 및 결과

4.1 이상 금융거래 탐지 및 분석

기존 블랙리스트 패턴기법의 사후분석기

법의 문제점을 개선하기 위해 탐지 및 분석 기법중 하나인 '상태전이기법'을 적용한 가칭 'New 이상 금융거래 탐지시스템'을 다음과 같이 구성하고 연구를 진행하였다.

분석 대상 및 기간은 2014. 10. 2~2014. 10. 25으로 총 4주간의 데이터를 분석하였다. 투입 자원 및 정보로는 HP 서버 3대(빅 데이터 분석용), 빅데이터 분석엔진 및 관련 S/W 다수, 거래내역 21개월분(2012. 1~2013. 9, 약 7억 7천만 건), PC 매체정보 로그 DB들이다. 또한 분석과정으로는 아래와 같은 과정을 거쳤다.

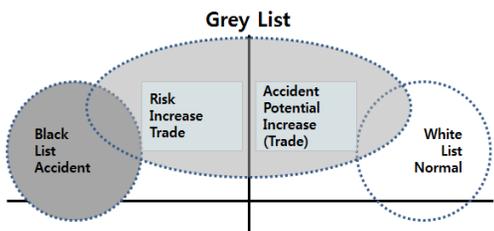
우선, 거래 성향분석 기준 및 이상거래 탐지조건 정의하고, 2012년 분석 대상기간 거래내역과 해당 거래의 PC매체정보 로그를 빅데이터 사전 성향분석을 실시하였고, 2013년 분석 대상 기간 동안 시간 순으로 모든 인터넷뱅킹 이체거래 1건씩 대입, 이상거래여부 탐지 확인(약 1,500만 건)을 진행하였고, 탐지된 이체거래로그를 별도 테이블 저장한 후, 2013년 분석 대상기간에 발생했던, 보이스피싱 및 해킹 피해거래와 일치여부를 확인하였다.

본 연구에서 사용한 분석방법은 첫째, 프로파일링 패턴 변수 추출하고, 2012년 1월부터 9월까지의 A-금융회사의 PC기반 전자금융거래 중 인터넷뱅킹 고객의 거래내역과 PC매체의 환경 및 거래정보 약 7억 7천만 건을 대상으로 이용자의 상시 정상적인 거래 절차 및 유형을 벗어나는 행위를 식별하였고, 매체 환경 정보와 거래유형에 대해 프로파일링을 <Table 4>와 같이 추출하였다.

<Table 4> Profiling Classification Table

	Contents
Profiling Variables	1. Domestic trading rate
	2. Security module operating rate (online vaccines, keyboard Security, etc.)
	3. concordance of using equipment (PC, SmartPhone, etc.)
	4. the maximum number of daily transaction
	5. the maximum amount of daily transaction
	6. relation with the Just before the transaction
	7. first transaction's deposit bank-account
	8. first transaction's deposit-amount

두 번째로, 프로파일링 패턴 변수를 통한 고객을 분류하였다. 인터넷뱅킹 로그인 계정(ID)별로 1년 치 거래를 매일 빅데이터 분석을 하고, 첫 번째 추출한 패턴변수를 기준으로 가중치를 부여하여 각 계정별로 최신 1년 프로파일링을 유지하고, 프로파일링을 기준으로 고객을 White/Gray/Black List 그룹으로 분류하였으며, 각 계정이 기존 추출된 프로파일링 그룹을 벗어날 경우 이상 금융거래로 탐지하였다.



<Figure 5> Classified Customers Based on Profiling

위 <Figure 5>의 프로파일링에 따른 고객 분류중에 White group은 사고가 한 번도 없는 정상거래만 존재하는 고객, Gray group 은 사고가능성 높아진 거래 혹은 Risk 증가되고 있는 거래로 분류되는 고객 집단, Black group 은 사고가 한번이라도 났었던 거래를 가진 고객집단으로 분류된다.

세 번째로 이상 금융거래 Rule 패턴 setting을 분석하여 과거 금융거래 사고 실 사례를 통해 7개의 Rule 패턴을 <Table 5>와 같이 설정하였다.

<Table 5> The Detail Concept of Rules

Rule Number	Detail Concept
#RULE01	Accidents transaction and new PC-transaction
#RULE02	Intensive interest terminals and new PC and
#RULE03	2 hours of transboundary logical/physical impossibility deal and new PC-transaction
#RULE04	change of profiling-group
#RULE05	Past suspicious transaction or PC
#RULE06	Foreign transaction and Just before the transaction inconsistency PC
#RULE07	Country-code is null and Just before the transaction is other country-code or different IP

<Table 5>의 Rule 패턴을 이용하고, 2012년 1월~9월의 data를 분석하여 <Table 6>과 같은 결과를 얻을 수 있었다. 평균 일 이체건 수 5만 건, 일 로그인 건수 50만 건 기준으로 월별 해당 룰에 탐지된 건수는 다음 <Table 6>과 같고, 룰은 사기기법의 변화에 따라 신규/변경/소멸 등 변화케이스를 가지고 룰 변경 및 검증이 필요할 것으로 생각된다.

<Table 6> The Number of Detection/Analysis/Block

Rule	Month								
	1	2	3	4	5	6	7	8	9
#RULE01 accident relation and newPC	94	87	160	118	228	231	242	252	187
#RULE02 interested object and newPC and just before trade within 1hour	1	2	2	1	1	2	0	0	26
#RULE03 within 2hour nation band change and newPC	108	130	85	111	234	192	26	250	180
#RULE04 profiling group change	10	6	11	9	6	10	4	8	6
#RULE05 interested object relation check	0	0	0	0	0	0	0	0	22
#RULE06 foreign country trade and just before PC discord	355	180	174	229	361	247	243	219	162
#RULE08 nation code=NULL and just before trade nation code and just before trade IP error	17	15	7	22	19	27	30	10	19

이번 연구에서는 총 7가지의 룰 패턴을 사용하였다. 향후 분석 요소에서 고객별 전자금융거래금액 및 통장 잔고, 거래시간, 이용매체, 입금 계좌, 거래위치, 연속 출금여부 및 추가인증 해킹 수법에 따른 다양한 룰 패턴을 적용하여 좀 더 정확도를 높일 수 있을 것이다.

네 번째는 이상거래 탐지를 위한 데이터 처리 프로세스 진행하였다. 위에서 설정한 고객의 프로파일링 변수, 고객 그룹 분류, Rule 패턴 정보를 이용하여, 2013년 1월 1일부터 9월 30일까지 거래 중, 1,500만 건의 의심거래를 우선 추출하였고, 이상거래 탐지하는 절차를 다음과 같은 프로세스 절차로 추출하였다.

<Figure 3>과 같이 추출된 거래 데이터의 거래가 과거 사고기록 혹은 사고연관이 있었는지 선 추출 후 룰 변수 및 패턴변수 분석하여 설정된 룰 변수와 패턴에 일치하는지 분류하여 데이터 분석 결과를 업데이트 후 통

계 데이터를 추출하고, 다시 룰 패턴분석 변경 및 정교화를 실시하고, 룰 탐지된 결과 값을 처리하는 방식으로 진행하였다.

4.2 사고예방 효과성 분석 및 개선 방안

2012년도 인터넷뱅킹 거래의 매체 환경 정보와 거래유형을 빅데이터 분석기법을 통해 추출한 프로파일링 정보와 2013년도 인터넷뱅킹 거래와 비교하여 이상 금융거래 여부를 사전 분석한 결과 약 1,500만 건의 의심거래를 탐지하여 도출하였고, 탐지된 이체 거래로 그를 별도 테이블 화 해서 실제 2013년 1월 1일부터 9월 30일까지 사고 신고된 인터넷뱅킹 보이스피싱 및 해킹피해 주장 거래와 일치여부를 확인한 결과 이미 알고 있는 블랙리스트 차단 거래를 제외한 블랙리스트 패턴으로 탐지하지 못한 사고거래 중 58%를 탐지하는 <Table 7>, <Table 8>과 같은 적중률을 보였다.

〈Table 7〉 Detailed Result of Anomaly Detection Analysis in E-Banking

Detect	Accident		Accident Type	Nation	Rule#	remarks
	Day	Time				
O	13.01.25	10:44	Phishing	China	2	
O	13.02.15	10:33	Phishing	unknown	7	
O	13.03.11	11:53	Phishing	Domestic	6	
	13.03.12	15:26	Phishing	Domestic		Faint Pattern
O	13.03.13	11:02	Phishing	China	6	
O	13.04.02	16:53	Phishing	China	6	
O	13.04.02	16:38	Phishing	China	6	
O	13.04.21	03:39	Fraud	China	6	
	13.05.08	17:36	Phishing	unknown		Faint Pattern
	13.06.12	10:41	Phishing	Domestic		Faint Pattern
O	13.07.25	02:49	Fraud	Domestic	2	
	13.07.26	15:39	Phishing	Domestic		Deposit/Saving Termination
O	13.08.25	13:09	Fraud	China	6	
O	13.08.26	17:11	Fraud	China	6	
	13.08.29	01:19	Fraud	Domestic		Faint Pattern
	13.08.30	21:27	Fraud	Domestic		Faint Pattern
	13.08.30	22:03	Fraud	Domestic		Faint Pattern
	13.09.26	16:31	Fraud	Domestic		Faint Pattern
O	13.09.26	00:52	Fraud	unkown	7	
Total					11건	

〈Table 8〉 Result of Anomaly Detection Analysis in E-Banking

Classification	Total Number of Transfer Detected	The Number of Unusual Transactions Detected	The number of Accident Detected	Hit Rate	Note
Number	13 million	24.6 thousand (0.19%)	11 of 19	58%	

따라서, 본 연구 결과 분석으로 전자금융 인터넷뱅킹을 통한 불법 이체사고 및 보이스 피싱과 관련한 이상 금융거래 사고는 수집정보의 유형에 따른 차이는 있을 수 있으나, 빅데이터 기술을 활용한 프로파일링 기

반의 사전분석에 의한 이상 금융거래 탐지의 효과성을 확인 할 수 있었으며, 향후, 전자금융거래 정보(예적금해지 등 다양한 전자금융거래)를 추가로 수집하여 분석 할 수 있다.

5. 결론 및 향후 연구방향

본 논문에서는 과거 발생한 사고정보만을 이용하여 탐지하던 블랙리스트 기반의 탐지방법은 전자금융거래에 이용된 매체환경과 거래정보가 정확하게 일치하는 거래에 대해서만 이상 금융거래 유무를 판단하는 모델로 신규 매체에 의한 이상 금융거래 사고 발생 또는 금융회사 간 상호 공유가 되지 않은 블랙리스트 매체인 경우 사전적으로 이상 금융거래를 예방할 수 없음을 지적했다. 따라서, 기존 블랙리스트 기반의 단순 패턴분석의 문제점을 개선하기 위해 과거에 이용했던 접속 환경 또는 금융거래 정보를 바탕으로 Profile을 생성하고 이를 비교 분석하여 이상 금융거래 유무를 판단하는 사전적 사고 예방을 위한 효과적인 분석 방법을 제시하고, 과거 금융 사고를 탐지해냄으로써 사고 예방성을 입증하였다.

이상 금융거래 패턴 분석 시 수집 정보가 PC기반으로 제한된 경우 특정 유형을 정할 수 없는 경우 사고 발생 시 자주 이용되는 개인정보변경거래 또는 예적금해지 거래정보를 추가적인 거래정보로 확보하여 본 분석방법을 적용할 경우 효과성이 향상 될 수 있다.

또한 이번 논문에서 제시된 Rule 패턴 이외에도 새로운 위협에 대응 가능한 추가적 다양한 내용의 Rule 패턴 업그레이드, 개인별 거래 행태분석의 꾸준한 업데이트가, 로그수집이 안된 거래에 대한 정밀 분석 및 재 필터링 방법 연구가 필요하다. 예를 들면, 장애 발생 시, 해킹의심, 미 지원 OS환경 등에 대한 로그 수집 및 이에 대한 집중 분석이 필요하다. 고객이 인터넷뱅킹 로그인ID를 바꾼 경우, 기존 키 값의 연결 분석을 고려할 필요가 있으

며, 금융 ISAC 위협정보공유체제와 연동하여 타행 사고 데이터를 연동한 분석시스템 구성을 고려해야 함을 향후 연구 과제로 남겨두었다. 또한 이번 논문에서 연구 되지 않은 실시간 이상 징후 탐지에 따른 거래제한 방법, 실시간 모니터링의 시각화 방법, 빅데이터를 활용한 고객 거래패턴 분석을 위한 관제시스템 운영자의 역할에 대해서도 논의 필요성을 남겨두었다.

References

- [1] The Bank of Korea, "Banking services usage statics throughout the year 2013,"
- [2] KISA, "Internet incident response statistics," KISA, pp. 133-139, 2014.
- [3] Newspaper of Korean Economics, "Electronic Banking strengthen identity verification procedures carried out."
<http://www.wowtv.co.kr/newscenter/news/view.asp?bcode=T30001000&artid=A201305140181>, 2013.
- [4] News of Kukiew.com, "New Farming Techniques Accident."
<http://news.kukinews.com/article/view.asp?page=1&gCode=kmi&arcid=0007333110&cp=nv>.
- [5] News of Ajunews.com. "Accident of Phishing-App."
<http://www.ajunews.com/common/redirect.jsp?newsId=20130118000370>, 2013.
- [6] Financial Security Agency, "Technical guide

- of Fraud Detection System,” 2014.
- [7] Kim, J. S., “Trading for over phishing detection assay fraud prevention,” *Information Security Journal*, Vol. 23, No. 6, pp. 41-48, 2013.
- [8] Telecommunications Technology Association. ‘Fraud Detection and Response Framework in Electronic Financial Transaction System.’ TTA/KO-12.0178. 2011.
- [9] Han, C. H., Kim, M. K., and Lim, C. K., “A Study on the Effects and Value Analysis of the B2B e-Commerce Guarantee Service,” *The Journal of Society for e-Business Studies*, Vol. 15, No. 4, pp. 265-284, 2010.
- [10] Kim, D. H., Lee, J. H., and Park, Y., P., “A Study of Factors Affecting the Adoption of Cloud Computing,” *The Journal of Society for e-Business Studies*, Vol. 17, No. 1, pp. 111-136, 2012.

저 자 소 개



박은영 (E-mail : sara7499@korea.ac.kr)
1998년 이화여자대학교 화학과 졸업
2000년~현재 KB국민은행 전산정보본부
2013년~현재 고려대학교 정보보호대학원 (석사과정)
관심분야 금융정보보안, 보안개발방법론



윤지원 (E-mail : jiwon_yoon@korea.ac.kr)
2003년 성균관대학교 정보공학사 졸업
2005년 University of Edinburgh. 정보학과 (석사)
2008년 University of Cambridge 전자공학과 (박사)
2008년~2009년 University of Oxford. 로봇연구소 (박사)
2009년~2011년 University of Dublin 통계학과 연구원 및 강사
2011년~2012년 IBM 연구소 정규 연구원
2012년~현재 고려대학교 정보보호대학원 조교수
관심분야 신호정보처리, 응용통계, 빅데이터 분석 기술, 도감청 탐지기술