Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.615

전자금융거래의 이상징후 탐지 규칙 개선을 통한 효과성 향상에 관한 연구

최 의 순,† 이 경 호‡
고려대학교 정보보호대학원

A Study on Improvement of Effectiveness Using Anomaly Analysis rule modification in Electronic Finance Trading

Eui-soon Choi,† Kyung-ho Lee‡
Graduate School of Information Security, Korea University

요 약

본 논문은 금융 사용자의 거래 행태를 반영한 이상거래 탐지 규칙 개선방안을 제시하고, 실제 적용된 사례를 분석하여 효과성을 검증하였다. 이상거래를 정상거래로 판단한 미탐분석은 전자금융사고 사례를 분석하여 사고유형과 거래행위를 파악하였고, 반대로 정상거래를 이상거래로 판단한 오탐 분석은 특정 기간 추가 인증 또는 차단 후 아웃바운드 안내 전화 실시 내역 전수 조사를 통해 수행하였다. 또한, 이상거래와 정상거래 행태 간 분류 기준을 정교화하기 위해 추가적인 탐지 규칙을 도출하였다. 특히, 아웃바운드 안내 전화 과정 중 탐지 규칙 정교화를 위한 추가 질의를 실시하여 금융 사용자의 거래 행태에 대한 다양한 통찰을 획득하였고, 이를 기반으로 기존 탐지규칙을 개선하였다. 그 결과 정상거래를 이상거래로 오탐하여 추가 인증 또는 차단하는 비율과 이상거래를 정상거래로 분류하여 실제 사고가 발생한 비율이 동시에 감소하였다. 본 논문에서 제안한 거래 행태에 기반한 이상거래 탐지 규칙 개선 방법은 이상거래 탐지의 효과성을 향상시키고 지속적인 탐지규칙 개선 방법론을 제공할 것으로 기대한다.

ABSTRACT

This paper proposes new methods and examples for improving fraud detection rules based on banking customer's transaction behaviors focused on anomaly detection method. This study investigates real example that FDS(Fraud Detection System) regards fraudulent transaction as legitimate transaction and figures out fraudulent types and transaction patterns. To understanding the cases that FDS regard legitimate transaction as fraudulent transaction, it investigates all transactions that requied additional authentications or outbound call. We infered additional facts to refine detection rules in progress of outbound calling and applied to existing detection rules to improve. The main results of this study is the following: (a) Type I error is decreased (b) Type II errors are also decreased. The major contribution of this paper is the improvement of effectiveness in detecting fraudulent transaction using transaction behaviors and providing a continuous method that elevate fraud detection rules.

Keywords: Fraud Detection System, Transaction Behavior, Outbound call

I. 서 론

금융 산업은 고객과의 신뢰를 기반으로 지속가능한 고객관계를 유지해야만 영속기업(going concern)의 본질을 유지할 수 있다. 안전한 금융거래환경을 만들어 금융소비자를 보호하는 것은 고객과의 신뢰를 형성

접수일(2015년 4월 16일), 수정일(2015년 6월 2일), 게재확정일(2015년 6월 3일)

† 주저자, mises99@gmail.com
‡ 교신저자, lee@hankook.re.kr(Corresponding author)

하는 첫 단추이다. 하지만, 인터넷뱅킹, 폰뱅킹 등 전자금융이 활성화 되고 및 핀테크 열풍으로 비대면채널 거래비중이 빠르게 증가함에 따라 전자금융사기도 동반 증가하여 왔다. 그간 금융감독원을 비롯한 감독기관과 금융회사들은 전자금융 활성화와 전자금융시스템 가용성 제고를 위해 많은 노력을 기울여왔다. 그러나, 보이스피싱·파밍·스미싱·메모리해킹 등 전자금융사기가 계속 진화하여 최근에는 사기수법이 더욱 교묘해지고 금융소비자들의 피해가 지속적으로 발생하고 있다. 특히, 지난 몇 차례 개인정보유출은 전자금융사기를 더욱 치밀하고 지능적으로 진화시켰다. 이에 대응하기 위하여, 정부는 관계부처 합동으로 전자금융사기 대응을 위한 범부처 협의체인 「전기통신금융사기방지대책협의회」를 발족하여 '14.8월 「신·변종 전기통신금융사기 피해방지 보완대책」을 수립하고, 같은 해 12월 금융소비자 보호를 위한 「전기통신금융사기방지대책」을 발표하였다. 금융회사 입장에서 「전기통신금융사기 방지대책」 내용 중 주목할 것은 금융회사의 사회적 책임에 부합하는 자율적 보안강화를 통해 금융소비자 피해방지 노력 확대를 주문했다는 점이다. 그 중 하나가 금융회사의 이상거래탐지시스템(Fraud Detection System, FDS) 구축·운영을 통한 금융소비자 보호 및 전자금융거래 사고 예방활동 강화이다. 금융감독원은 금융감독원, 금융보안연구원, 주요 은행 및 증권사의 FDS 담당자로 구성된 '이상금융거래탐지시스템(FDS) 협의체'를 운영하며 FDS 구축을 독려하고 있다. 이미 카드사는 8개 업체 전부 FDS 구축을 완료하여 운영중이고, 은행권은 18개 중 10개 회사가 구축 완료하였고 나머지 회사도 연내 구축을 완료하여 운영 예정이다. 하지만, FDS를 효과적으로 운영하기 위해서는 내부 지식을 활용한 분석역량이 절대적으로 요구되나, 국내 은행들의 경우 아직 운영 경험이 적고 이상거래 탐지에 필요한 데이터 축적도 미미한 수준이다. 결과적으로 오탐율이 높아 고객의 불편과 불만으로 민원발생 빈도가 높고, 오탐에 따른 추가인증 또는 아웃바운드 콜 등 고객확인 절차에 수반되는 마찰적비용도 동반 증가한다.

본 논문에서는 실제 사고 내역과 FDS를 통한 사고경보를 비교·분석하여 False Negative와 False Positive를 동시에 감소시키는 방안으로 금융사용자 거래 행위에 기반한 사용자 프로파일 구성, 탐지규칙 도출, 유연한 허용 한도 적용 등을 통해 이상거래탐지 효과를 개선하는 방안을 제안하고자 한다. 본 논문에서 제시된 방안은 국내 A 금융회사의 FDS 적용 전·후, FDS 탐지 규칙 개선에 따른 금융사고율 감소를 실증함으로써 본 제안의 효과성을 입증하였다.

논문의 구성은 총 5장으로 구성되었다. 2장에서 본 연구에 앞서 선행된 기존연구 소개와 주요 특징을 해외와 국내 동향으로 구분하여 살펴보고, 본 연구의 차별성을 밝힌다. 다음으로, 3장에서는 A금융회사의 FDS 구성 현황· 업무 프로세스· 운영 조직 등을 소개한다. 다음으로, 4장에서는 FDS탐지규칙 개선을 위한 현황 및 문제점을 분석하였고, 이를 토대로 탐지규칙을 어떻게 개선했는지 기술하고 실제 데이터를 사용하여 검증하였다. 마지막으로, 5장에서는 본 연구에 대한 결론을 맺고, 향후 연구에 대한 방향을 제시하고자 한다.

II. 연구배경

국내와 해외의 전자금융 보안환경은 최근까지 상이하게 발전해왔다. 국내는 금융당국 주도로 보안성을 강조하면서 전자금융서비스가 사용자 편의성 보다 사고 방지에 초점을 두고 시행되었다. 특히, 금융사고 방지를 위한 보안솔루션이 사용자 단말 구간에 집중되었다. 반면, 해외의 경우 전자금융서비스가 사용자 편의성이 강조된 계정기반 간편서비스 위주로 발전되어 왔다. 그 결과 국내 전자보안 연구는 주로 금융사고 예방기법 중심으로 수행되었고 해외는 금융사고 예방기법과 더불어 이상거래 탐지 기법이 광범위하게 연구되었다. 하지만, 최근 금융권 중심으로 이상거래탐지가 강조되면서 국내도 이상거래탐지와 관련된 연구가 증가하고 있다.

2.1 해외연구동향

해외의 경우 90년대 후반부터 신용카드거래, 보험청구, 자금세탁, 탈세 등의 분야에서 이상금융거래탐지 연구가 폭넓게 진행되었다. 해외 이상금융거래탐지에 대한 연구는 크게 통계적 분석 기반 탐지기법과 인공지능을 이용한 탐지기법으로 분류할 수 있다. Richard J. Bolton과 David J. Hand[1]는 이상거래탐지규칙에서 사용되는 통계적 기법을 신용카드, 자금세탁, 침입탐지, 의료 및 과학 등 다양한 분야의 특성에 따라 각각 다른 적용기법을 제안하였다. 통계적 분석 기반 탐지기법은 대용량 데이터베이스 환경에서 데이터 처리기법[2], Hidden Markov alignment, Smoothing techniques 등 다양한 통계적 파라미

터 산출·비교 기법[3] 등으로 세분화 할 수 있다.

인공지능을 활용한 탐지기법은 데이터마이닝, 패턴인식 및 머신러닝 등을 이용한 기법으로 세분화 할 수 있다. 데이터마이닝을 활용한 탐지기법은 데이터를 분류하거나 군집화하여 이상거래와 정상거래를 자동으로 구분하는 기법이다[4]. 패턴인식과 머신러닝을 활용한 기법은 거래정보를 바탕으로 정상거래와 이상거래의 특성을 파악하여 이상거래를 판별하는 기법이다. 인공신경망을 활용한 기법, 베이지안 모델링을 활용한 기법 등이 대표적으로 연구되고 있다[5].

2.2 국내연구동향

공인인증서로 대별되는 국내 금융 환경의 특수성으로 인해 카드사를 제외한 다른 금융부문에서 최근까지 이상거래탐지시스템은 거의 활성화되지 않았다. 박래정의 연구[6, 7]는 신용카드 사기거래 검출을 위한 신경망 분류기 연구를 통해 신용카드 사기거래에 특화된 진화연산기법을 제안하였다. 해당 연구는 사기거래 검출 분류기의 특정 영역 성능을 선택적이고 직접적인 방법으로 제어할 수 있음을 보여준다. 또한, 사기검출기의 분류 비용 최소화를 위해 최적화 평가함수를 정의한 후 진화연산 기법을 이용하여 희망 동작 구간에서 최적의 분류 비용을 갖는 분류기를 제안하였다.

신용카드 부문을 제외한 금융 부문에서 이상거래탐지시스템의 연구는 한국정보통신기술협회에서 이상금융거래에 대한 정의, 탐지 요구사항, 탐지 대응정책과 방법, 이상거래탐지시스템 구성 및 동작 메커니즘에 대한 표준안을 기술한 '이상금융거래 탐지 및 대응 프레임워크'를 발표한 이후 본격적으로 연구되기 시작했다[8]. 이후 금융보안연구원에서 2014년 8월 이상금융거래탐지의 효과성 개선을 위해 '이상금융거래탐지시스템 기술가이드[9]'를 발표하였다. 위 가이드는 이상금융거래탐지시스템 구성 및 기능, 도입 시 고려사항에 대하여 기술하고 있다. 위 두 발표 자료는 이상금융거래시스템에 대한 표준 권고안 성격으로 실제 이상금융거래탐지시스템 구축 시 효과성을 높이기 위해 많은 노력과 시행착오를 겪어야 하는 부분은 개별 금융회사의 몫으로 남겨두었다. 이후 핀테크 열풍과 금융당국의 FDS 구축에 대한 권고가 계속되면서 은행권을 중심으로 FDS가 구축이 되기 시작하였고 관련 연구도 다수 발표되었다. 김정원의 연구[10]에서는 피싱 사기거래 방지를 위해 금융회사 홈페이지에서 전자금융거래 이용자의 접속행위, 공인인증서 사용 행위, 온라인 송금 행위 등을 분석하여 전자금융사고 혐의 이상 징후에 대한 탐지방법을 제안하였다. 박은영의 연구[11]에서는 기존 블랙리스트 기반 탐지기법이 갖고 있는 단점을 보완하기 위해 상태전이 기법을 적용하여 매체 환경과 거래 정보가 일치할 경우 이상거래 유무를 판별하는 모델을 제시하였다. 박재훈의 연구[12]에서는 빠르고 효과적인 이상거래 탐지를 위해 고객의 사고사례 패턴을 중심으로 탐지규칙을 설정한 후 의사결정 나무에 의한 정규화를 통해 시스템 효율성 향상과 유지비용을 감소시키는 방안을 제시하였다.

2.3 연구의 차별성

선행 연구를 종합해 보면 해외의 경우 축적된 데이터를 기반으로 통계적 기법과 빅데이터 분석기법을 접목하여 이상탐지 기반 탐지규칙 정교화 및 고도화 연구를 중심으로 수행되었다. 국내의 경우 이와 유사하나 공인인증서, 개인정보 수집 금지 정책 등 국내 금융 환경을 반영하여 매체 정보 중심 탐지기법이 주로 연구되었다.

본 연구는 기존 연구에 비해 다음과 같은 차별성을 갖는다. 첫째, 은행권을 중심으로 이루어지는 전자금융사기 탐지규칙 정교화를 위해 고객의 금융거래 행태에 대한 탐색적 연구를 수행하여 그 결과를 탐지규칙에 반영하였다. 둘째, 탐지규칙의 효과성 증명을 위해 실제 데이터에 통한 실증분석을 수행하였다. 셋째, 탐지규칙 개선을 위해 이상거래탐지시스템 운영과 연관된 조직과 업무 절차 조사를 수행하여 이상거래탐지시스템 도입 초기에 발생할 수 있는 시행착오와 조직 갈등 요소를 최소화하고자 하였다.

이를 위해서, 작년 말 이상거래탐지시스템을 구축한 A금융회사의 사례를 중심으로 연구조사와 개선사항을 도출하였다.

III. A금융회사의 이상거래탐지시스템 구성 및 운영 형태

3.1 이상거래탐지시스템 구성

A금융회사의 이상거래탐지시스템은 Fig.1.과 같이 '데이터 수집 모듈', '분석 및 탐지 모듈', '모니터링 및 보고 모듈'로 구성되었다.

데이터 수집 모듈에서는 이용자의 매체(devices) 정보와 A사가 보유한 금융거래정보를 수집한다. 분석

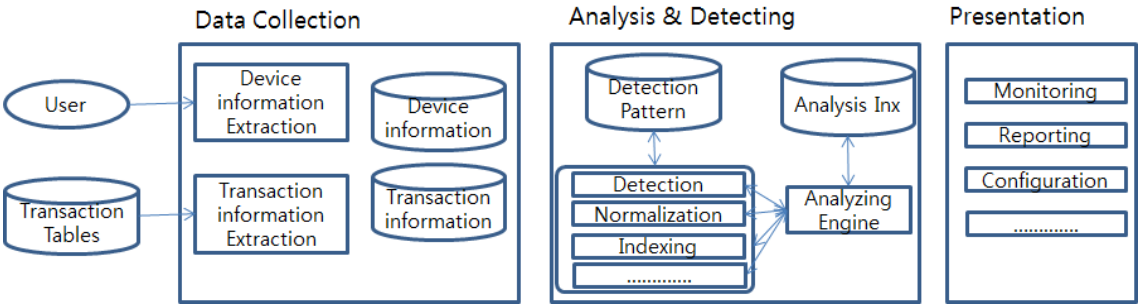

Fig. 1. The structure of fraud detection system

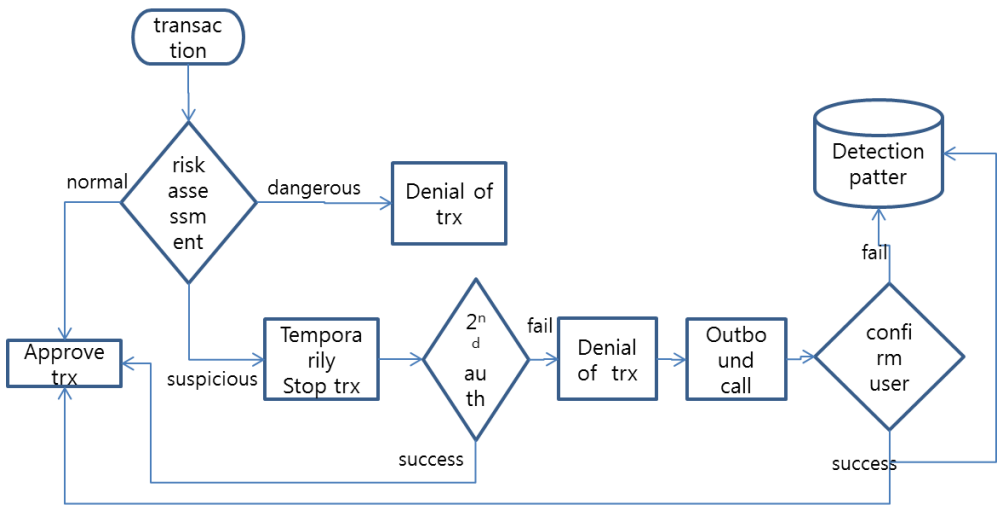

Fig. 2. The process flow of Fraud Detection

및 탐지모듈에서는 데이터분석 엔진과 탐지패턴 데이터베이스를 이용하여 이상금융거래를 식별하고 탐지패턴을 업데이트하는 기능을 담당한다. 모니터링 및 보고 모듈은 관리자에게 각종 통계 정보와 모니터링 결과를 리포팅하여 관리자가 탐지패턴을 개선할 수 있도록 지원하는 기능을 담당한다.

3.2 운영 조직 및 대응 프로세스

FDS 운영 조직은 크게 Table 1.과 같이 '데이터분석 및 정책결정 부서', '시스템 구축 및 운영부서', '민원대응 부서'로 구성되었다. '데이터분석 및 정책결정 부서'는 이상금융거래 탐지 규칙 및 정책결정, 데이터 분석 등의 업무를 수행한다. '시스템 구축 및 운영부서'는 FDS 구축 및 유지보수를 수행한다. '민원대응 부서'는 FDS를 통해 거래가 차단된 고객에게 전화를 걸어 본인 확인을 실시하고, 고객으로부터 걸려온 민원전화에 대한 대고객 응대를 담당한다.

FDS는 전자금융거래가 기존 탐지규칙에 위반되지 않으면 정상거래로 간주하여 이후 거래 프로세스를 진행한다. 거래위험판정 결과 의심(suspicious) 등급과 고위험(dangerous) 등급 거래는 각각 Fig.2.와 같이 추가 인증 또는 차단을 통해 거래의 안전성을 확보하게 된다. 의심 등급 거래는 ARS나 SMS를 통한 추가 인증을 실시한 후 본인확인이 정상적으로 된 경우에 한하여 이후 거래를 진행하고 추가 인증에 실패하게 되면 차단 후 민원담당 부서로 해당 내역을 실시간으로 전송하여 해당 고객에게 본인거래 확인 전화를 하게 된다. 이 결과, 본인 확인이 정상적으로 종료되면 차단을 해제하고 일정시간동안 이상거래탐지 예외 승인을 통해 고객이 해당 금융 거래를 수행할 수 있도록 한다. 고위험 등급으로 판정되면 즉시 거래를 차단하고 민원대응 부서에서 아웃바운드 콜을 실시한다. 고객의 신원과 본인 거래 여부 확인을 통해 차단 해제

Table 1. The FDS organization

Department	Role
Policy Management	Fraud detection modeling, data analysis, fraud detection policy management
IT Management	FDS implementation, FDS Maintenance
Complaint Management	Inbound/outbound call, operating call center

여부를 결정하고 고객 전화가 부재중이거나 착신전환일 경우 SMS를 전송한 후 거래 차단을 유지한다. 블랙리스트에 등록된 매체정보 또는 대포통장인 경우 고위험 등급과 동일한 절차를 거치게 된다.

IV. 탐지규칙 개선 절차 및 방법

4.1 개요

본 논문에서 수행한 탐지규칙 개선 절차는 Fig. 3. 같이 총 7단계로 수행되었다. 첫 번째 단계에서는 FDS 가동 전과 후에 대한 사고 사례를 비교·분석 한다. 두 번째 단계에서는 FDS 운영 프로세스 관찰과

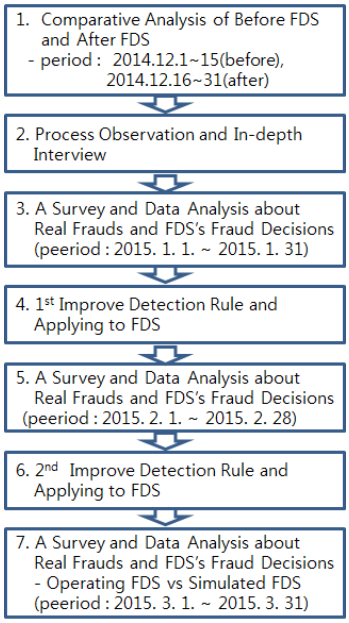

Fig. 3. The overall process of improving detection rules

각 부서 담당자에게 FDS 운영과 관련된 주요 이슈에 관한 개별 심층 면접을 실시한다. 세 번째 단계에서는 1월 한 달간 실제 발생한 전자금융 사기와 FDS에서 사기 의심으로 판정하여 차단한 내역을 상호 비교·분석하여 FDS의 도입 효과를 분석한다. 네 번째 단계에서는 세 번째 단계에서 파악한 문제점을 개선할 수 있는 방안을 마련한 후, FDS에 전산 반영한다. 다섯 번째 단계는 세 번째 단계에서와 마찬가지로 2월 한 달간 실제 발생한 전자금융 사기와 FDS에서 사기 의심으로 판정하여 차단한 내역을 상호 비교·분석하여 네 번째 단계에서 적용한 탐지 규칙의 효과성을 분석한다. 여섯 번째 단계는 다섯 번째 단계에서 발견된 추가 고려사항을 파악하여 탐지 규칙 개선사항을 도출한 후 시뮬레이션 시스템에 반영한다. 일곱 번째 단계에서는 3월 중 실제 거래 내역과 개선된 탐지 규칙이 반영된 시뮬레이션 시스템 간 비교·분석을 통해 탐지 규칙 개선안에 대한 효과성을 최종적으로 검증하였다.

4.2 1단계 : FDS 가동 이전·이후 비교 분석

A사는 2014년 12월 16일 이상거래탐지시스템을 가동하였다. 이상탐지방법(Anomaly Detection Method)에 기반한 탐지 규칙을 Table 2.에 정리하였다. 특정 금액 이상 특정 계좌로 반복 이체, 타행 계

Table 2. Detection Rule sets

No.	Formula
1	$\sum AMT_{rt\rightarrow rc} > DL_{rt\rightarrow rc}$ $(where\ rt \neq rc, AMT > H)$
2	$N(AMT_{rt\rightarrow rc}) > N(DL_{rt\rightarrow rc})$ $(where\ rt \neq rc)$
3	$\sum(AMT_{rt\rightarrow rc}) > AVG(AMT_{rt\rightarrow rc}) \times K$ $(where\ rt \neq rc)$
4	$N(User\ Account) > H(User\ Account)$ $(User\ Account_i \neq User\ Account_j$ $during\ H(T))$
5	$N(Mode(AMT_{rt\rightarrow rc}) \neq 0) > H(N)$

AMT : Transfer Amount
rt : remittance bank
rc : receiving bank
DL : Daily Limitation of Transfer Amount
N : Number of occurrence
K : the multiplier
H : Hurdle(Tolerance Level)
Mode : Modular Operation

좌로 반복 이체, 평소 이체 금액 대비 높은 금액 이체, 매체에 여러 로그온 사용자가 일정 기준 이상 존재하는 경우, 997원, 999원 등 원단위 이체를 하는 경우 등이 있다.

이상거래시스템 도입초기 효과성을 분석하기 위해 2014년 중 12월 실제 전자금융 사고 발생 현황과 이상거래탐지시스템에서 금융 사기로 판정하여 차단 후 아웃바운드 콜을 실시한 현황을 전수 조사하여 비교하였다. 실시 결과는 Table 3.과 같이 이상거래탐지시스템 가동 전과 비교하여 가동 후에 전자금융 사기에 대한 유의미한 감소효과는 발견되지 않았고, 오히려 파밍 공격에 의한 피해 발생 건수 및 피해 금액이 증가하였다. 이는 이상거래탐지시스템 가동 초기로 안정화가 필요한 시점이고 연말정산 등을 사칭한 스미싱·파밍 공격 증가가 주요 요인으로 파악되었다.

4.3 2단계 : 프로세스 관찰 및 담당자 심층 인터뷰

FDS 초기 가동 후 안정화 작업이 수행되었던 시기여서 IT 부서와 민원대응 부서의 업무 부하가 많이 관찰되었다. FDS 관련 부서 각 담당자들과 심층면접을 실시한 결과 Fig.4와 같은 부서 간 이해상충 문제가 발견되었다. '데이터분석 및 정책결정 부서'의 최우선 과제는 실제 전자금융 사기 사건이 발생하지 않도록 하는 것이다. 이에 따라, 효과성이 조금이라도 있다고 판단되면 탐지규칙 즉각 반영을 원한다. 하지만, IT 부서와 민원담당 부서의 입장이 서로 다르다. IT 부서는 탐지 규칙 추가에 따른 시스템 사용률 급증 등으로 인한 시스템 불안정성을 예측할 수 없고, 민원담당 부서는 FDS의 도입 초기 오탐율이 증가하여 FDS가 거래를 차단할 때마다, 고객에게 본인거래유무를 확인을 해야 하므로 업무량이 폭증된다. 그러나, 본 연구에서는 고객민원 대응 과정이 고객의 거래 의도와 거래 행태 등을 파악할 수 있다는 점에서 매우 효과적인 탐지 규칙을 생성할 수 있다는 것을 발견하였다.

Table 3. Number and Damage Amount of Fraud

	Before FDS		After FDS	
	Num	AMT (100M)	Num	AMT (100M)
Pharming	33	1.8	36	2.5
Phising	1	0.4	1	0.1
Unknown	12	0.2	18	0.6
Total	46	2.4	55	3.2

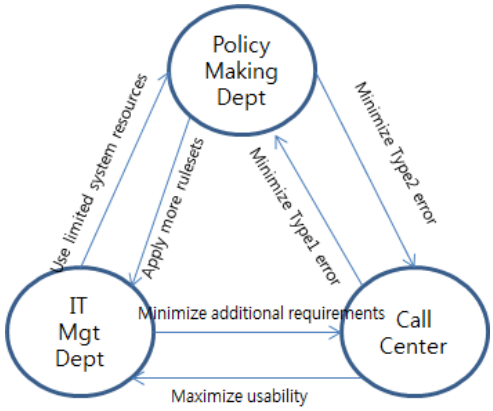

Fig. 4. The Relation Diagram of FDS operating parties. A→B means A wants B to 【 】. EX) Policy Making Dept wants IT Mgt Dept 【to apply more rulesets】

4.4 3단계 : 1월 중 실제 발생한 전자금융 사기 현황과 FDS 사기 판정 현황 분석

분석에 앞서 FDS의 사기 판정이 정탐(True Positive)인지 또는 오탐(False Negative)인지 여부를 판정하기 위해 아래와 같은 기준을 설정하였다.

〈정탐 판정기준〉
- 추가 인증 실패 후 24시간 내 inbound call이 없는 경우
- 차단 후 outbound call 실시 결과 본인 거래가 아닌 경우
- 차단 후 outbound call 실시 결과 부재중이고 24시간 내 inbound call 없이 차단이 유지된 경우

〈오탐 판정기준〉
- 추가 인증 성공 후 정상 거래 종료된 경우
- outbound call 결과 본인 거래가 확인된 경우
- outbound call 결과 부재중이었으나 24시간 내 inbound call로 본인확인 후 차단이 해제된 경우

Table 4.는 1월 중 발생한 전자금융 사기를 매체별, 이체 거래에 사용하는 추가 인증 수단 별로 분류된 내역이다. 1월 중 발생한 전자금융 사기는 총 108건으로 OTP 이용 중 발생 건수는 9건, 보안카드 이용 중 발생 건수는 99건으로 보안카드 이용자의 피해

Table 4. Number of Occurrence by Device and Authentication Method (2015.1.1. ~ 2015.1.31).

	OTP	Grid OTP	Total
Mobile	3	34	37
Internet	6	64	70
Telephony		1	1
Total	9	99	108

가 압도적으로 많았다.

시간대로 분석을 한 결과 Fig.5.와 같이 18시 이후부터 자정까지에 발생 빈도가 그 외 시간대 발생빈도보다 크다.

Table 5.를 보면, 1월 중 FDS에서 이상거래로 판정을 한 건수는 9,653건이고 이 중 정탐은 331건, 오탐은 9,322건으로 오탐률이 96.6%로 오탐률이 매우 높다. 이는 사기거래와 정상거래 간 유사성이 높아 FDS 운용 초기 사기 거래와 정상 거래 구분을 위한

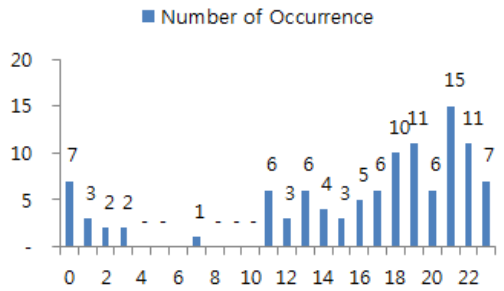

Fig. 5. The number of occurrence in time slots(2015.1.1. ~ 2015. 1.31)

Table 5. FDS Detection Results(2015.1.1.~2015.1.31)

	False Positive	True Positive	Total
Number	9,322	331	9,653
Percentage	96.6%	3.4%	100%

Table 6. Confusion Matrix of FDS(2015.1.1.~2015.1.31)

		Actual	
		Fraud	Legitimate
FDS	Fraud	331	9,322
	Legitimate	108	Approximately 224,750,000

결정경계를 설정이 매우 어려움을 보여준다.

Table 6.는 전체 거래 건수를 고려한 혼동행렬(Confusion matrix)을 보여주고 있으며, 사기 거래 수가 정상 거래 대비 매우 적기 때문에 단일 지표로 사기 거래 판별을 위한 효과적 탐지 규칙을 찾기가 쉽지 않다.

4.5 4단계 : 1차 개선

1차 개선의 목표는 사기 거래와 정상 거래 간 중첩(overlapping)된 부분을 찾아, 결정경계를 좀 더 명확하게 정하는데 도움이 되는 요소(factor)를 휴리스틱 접근방법(Heuristic Approach)을 사용하여 찾는 것이다. 시스템 도입 초기로 아직까지 안정적 운영 환경이 형성되지 않았기 때문에 시스템 가용성을 훼손하면서 통계분석에 필요한 데이터를 획득·처리에 애로가 많았다. False Positive 확인의 접점에 있는 민원대응부서(콜센터)를 2차례 방문하여 Table 2.에 기술된 탐색 규칙의 문제점을 파악하는데 많은 노력을 기울였다. 그 결과 다음과 같이 의미 있는 결론을 도출할 수 있었다.

- Rule #1, #2에 의한 False Positive은 대부분 자영업자 또는 기업고객이었다.
- Rule #3에 의한 False Positive는 물품 거래, 부동산 거래, 개인간 금전대차 거래였다.
- Rule #4에 의한 False Positive는 기업고객과 자영업자였다.

이를 바탕으로 기업고객, 자영업자, 개인고객 에 따라 최대 허용한도(Hurdle, Tolerance Level)를 차등 적용하였다. 가중치는 '기업고객 〉 자영업자 〉 개인고객' 순으로 하였고, 세부 수치는 일정 구간 내에서 공격자가 규칙성을 파악하기 어렵도록 일정시간 간격을 두고 무작위로 설정하여 적용하였다. 또한, IT 부서와 민원 부서의 협조를 얻어 콜센터 상담 애플리케이션에 상담 과정에서 수집한 정보를 구조화 할 수 있도록 탐지 규칙별 표준 질의사항 및 확인사항을 입력할 수 있도록 데이터베이스를 추가적으로 설계하였다. 애플리케이션 구현까지 시간이 소요되므로, 그 동안 비망계정(콜센터 어플리케이션내 일종의 메모장 기능)에 상담내용을 정확히 기술하도록 업무 매뉴얼 수정과 상담원 교육을 동시에 진행하였다. 18시 이후 이체 건에 대해서 허용수준(Tolerance Level)을 α만

큼 가중하였다. 2회 이상 차단된 고객은 본인이 동의하면 FDS 정책을 적용하는 것을 배제할 수 있도록 화이트리스트(White list)에 등록하여 중복 오탐을 제거하였다.

False Negative 감소를 위해 1월 중 발생한 전자금융 사기 거래 108건에 대해 상세 조사를 수행하였다. 그 결과 사고 유형 중 연속 3회 미만 이체가 85건으로 비중은 78.7%였다. 통합이체 서비스를 이용한 사고는 29건이 발생하였다. 또한, 한 가지 특이한 것은 연속 10건 이상 다량 이체서비스를 이용한 사고 거래도 존재했다는 것이다. 위 사항을 탐지 규칙에 반영하여 2월 1일 FDS에 적용하였다.

4.6 5단계 : 2월 중 실제 발생한 전자금융 사기 현황과 FDS 사기 판정 현황 분석

2월 중 전자금융 사기 발생 건수는 1월 대비 65.7% 감소한 37건이 발생하였다. Fig. 6.을 보면 시간대별 전자금융 사기 발생 건수는 1월 중 발생 빈도가 높았던 18~24시 사이 발생 건수가 현저하게 줄어들었음을 확인할 수 있다.

이는 16시 이후 이체 거래에 대해서 허용수준(Tolerance Level)을 α만큼 가중시킨 것이 주효했던 것으로 보인다. 그러나, Table 7.을 보면 허용 수준 강화로 인하여 1월 대비 FDS에 의한 차단 건수도 862건이 증가하여 Type Ⅰ에러 역시 증가했음을 알 수 있다.

Table 8.의 거래매체와 인증수단 간 전자금융 사고 건수를 분석한 결과 1월과 비교하여 사고 건수는 크게 감소했지만 디바이스별, 인증수단별 상대적 비중은 크게 변동되지 않았다.

Table 9.의 2월 중 FDS에 의한 탐지 건수는 총 11,131건으로 아웃바운드 콜에 의한 본인 거래 확인이 10,760건으로 전월과 비교하여 오탐률은 크게 개선되지 않았다.

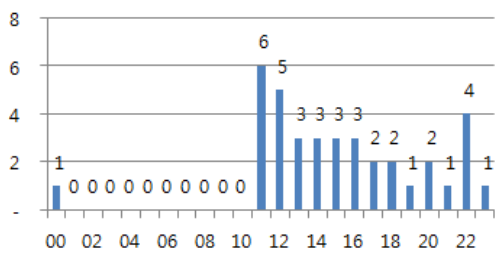

Fig. 6. The number of occurrence in time slots(2015.2.1. ~ 2015. 2.28)

Table 7. The Monthly Comparison for FDS detection by Time slots

Time slot	Jan(A)	Feb(B)	Difference (B-A)
16	937	1159	222
17	964	1090	126
18	754	948	194
19	499	615	116
20	489	540	51
21	407	481	74
22	349	374	25
23	248	302	54
Total	4,647	5,509	862

Table 10.의 전체 거래 건수를 고려한 Confusion matrix를 보면, False Negative는 크게 감소하였지만, False Positive는 크게 변동이 없었다.

일반적으로 False Negative와 False Positive는 역의 관계에 있다는 것을 고려하면, 1차 개선을 통해 실제 사고 감소 건수와 오탐 건수가 동시에 감소했다고 볼 수 있다.

Table 8. Number of Occurrence by Devices and Authentication Methods (2015.2.1. ~ 2015.2.28).

	OTP	Grid OTP	Total
Mobile	2	9	11
Internet	3	23	26
Total	5	32	37

Table 9. FDS Detection Results(2015.2.1.~ 2015.2.28)

	False Positive	True Positive	Total
Number	10,760	371	11,131
Percentage	96.7%	3.3%	100%

Table 10. Confusion Matrix of FDS(2015.2.1.~ 2015.2.28)

		Actual	
		Fraud	Legitimate
FDS	Fraud	371	10,760
	Legitimate	37	Approximately 203,372,000

4.7 6단계 : 2차 개선

1차 개선으로 실제 전자금융 사기 사건 발생 건수는 크게 감소하였지만, 2월 중 FDS에 의한 탐지 건수는 전월대비 1,478건이 증가한 11,131건이다. 이에 따라, 민원발생 증가로 민원담당 부서의 불만이 증가하여, 2차 개선은 오탐률을 낮추기 위해 탐지 규칙 정교화에 초점을 맞추어 진행하였다. 1차 개선 때 적용한 아웃바운드 콜 과정 중 입력된 상담내용을 세부적으로 분석하여 오탐 원인 파악과 사고의 주요 요인 분석을 중점적으로 진행하였다. 또한, 시스템 성능제약조건으로 과도한 탐지 규칙을 운영시스템에 바로 적용하는 것은 시스템 안정성 측면에서 부담스러운 상황이기 때문에 개선된 규칙은 시뮬레이션 시스템에 적용하여 운영시스템과 비교·분석하는 방향으로 진행하였다. 시뮬레이션 시스템에 적용한 탐지규칙 주요 개선사항은 다음과 같다.

- 이전 이체가 발생했던 계좌는 탐지 규칙 예외 적용
- 기업고객은 허용수준 2월 대비 축소
- OTP 사용 고객, 전자금융사기예방서비스 가입고객 등 사용자 거래 위험 성향에 따라 허용 수준 차등 적용
- 이전 거래 정보를 바탕으로 거래 패턴에 대한 통계 수치 사전 측정값을 통해 개별 거래에 대한 허용 수준 결정
- 블랙리스트, 화이트리스트를 통해 사전 선별
- 사용자 프로파일링을 디바이스 정보, 네트워크 접근 정보, 이전 거래 패턴 정보, 이전 거래 패턴을 기초로 생성한 통계 수치 정보, 추가 보안 수단 정보 등으로 세부 속성을 구성하고 허용 수준 결정에 활용
- 스마트 기기의 경우 단말기 내 공인이증서가 1개를 초과한 경우 즉시 차단
- 출금 계좌가 3~6개월 이상 장기 미사용인 계좌 (금액에 따라 차등 적용)
- 이전 거래와 본 거래의 지역이 다른 경우

Fig.7.은 사용자 프로파일링 정보를 이용하여 이체 거래에 대한 승인 프로세스를 도식적으로 나타낸다.

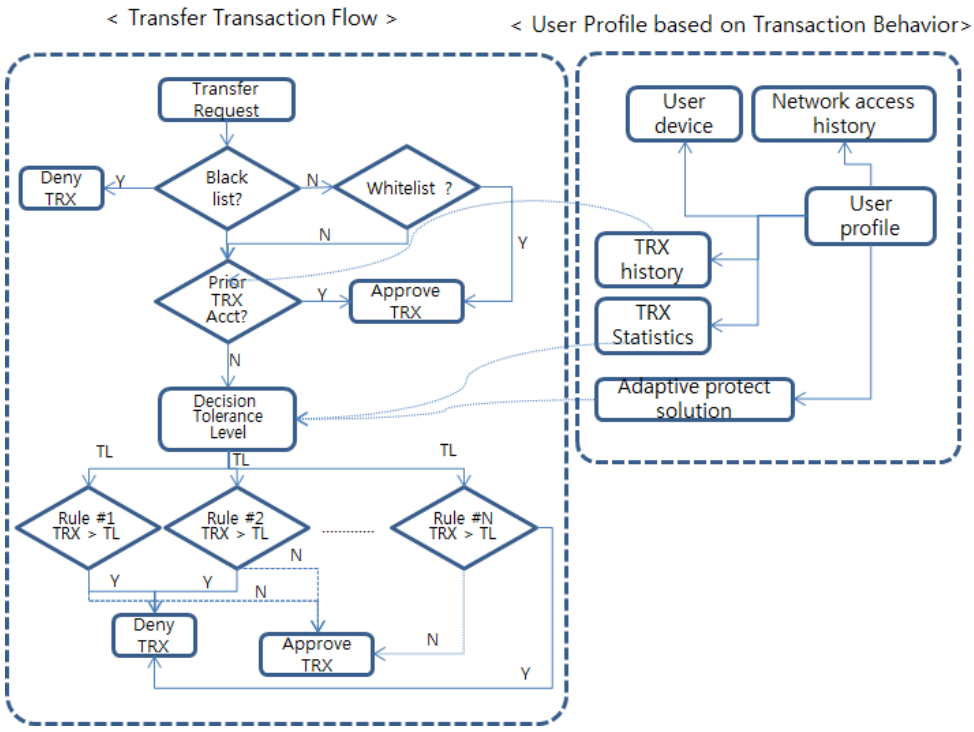

Fig. 7. The Transaction Flow Using User Profiling

4.8 7단계 : 2차 개선의 효과성 검증

2차 개선에 대한 효과성 테스트는 A사 시뮬레이션용 FDS를 통해 3월 1일부터 31일까지 발생한 실제 거래 건수 약 225백만 건을 가지고 수행하여, 동 기간 실제 가동중인 FDS로부터 나온 결과와 비교하는 방법으로 진행하였다.

Table 11.은 3월 1일부터 31일까지 실제 운영 중인 FDS에서 추출된 값과 시뮬레이션용 FDS 결과와 비교 사항을 기술하였다. 2차 개선이 적용된 시뮬레이션 FDS에서 오탐 건수는 운영 중인 FDS 대비 2,128건이 감소한 8,875건이다. 정탐 건수도 실제 운영 중인 FDS 대비 25건이 증가하였다. 즉, 오탐률과 정탐률이 동시 개선되었음을 확인할 수 있었다.

또한, 1차 개선 사항이 적용된 실제 운영 중인 FDS도 1차 개선 전과 비교하여 전자금융 사기 감소에 효과적임을 보여준다.

Table 11. The Comparison of Actual FDS and Simulated FDS (2015.3.1.~2015.3.31)

	False Positive	True Positive	Total
Actual FDS(A)	11,004 (96.3%)	427 (3.7%)	11,431 (100%)
Simulated FDS(B)	8,875 (95.2%)	452 (4.8%)	9,328 (100%)
Difference (C=B-A)	△2,128 (△1.1%)	25 (1.1%)	△2,103 (0%)

V. 결론 및 향후 연구방향

이상거래탐지시스템의 특성상 안정화와 고도화에 많은 노력과 시간이 소요된다. 본 논문에서는 그러한 노력의 강도와 시간을 단축할 수 있는 방법으로 FDS에서 차단 후, 본인 확인 절차를 위한 아웃바운드 콜 과정에서 입수된 정보를 토대로 2차례 탐지 규칙을 개선하고, 그 결과 False Positive와 False Negative를 동시에 감소시켰음을 실제 사례를 통해 확인할 수 있었다. 향후 연구 방향은 현재 진행 중인 아웃바운드 콜 과정에서 입수된 정보를 체계화를 목적으로 FDS 업그레이드 진행하여 오탐률을 더욱 감소시킬 수 있는 탐지 규칙 개선방법 정형화기법 도출이다. 이 과정에서 본 논문에서 적용한 휴리스틱 기법을 패턴인식과 데이터마이닝 기법을 접목하여 좀 더 발전시킬 수 있을 것으로 기대된다. 본 논문을 통해서 제시된 방법은 FDS를 구축·운영 중이거나 곧 도입하려는 금융회사에게 FDS 정상화 및 안정화에 소요되는 시간과 노력을 훨씬 감소시켜 줄 수 있다고 확신한다.

References

[1] Richard J. Bolton and David J. Hand, "Statistical Fraud Detection: A Review," Statistical Science, Vol. 17, No. 3. pp. 235-249. Aug, 2002,

[2] A Fast, L Friedland, M Maier, B Taylor, "Relational data pre-processing techniques for improved securities fraud detection," IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[3] Franz Josef Och¤ Hermann Ney, "A Systematic Comparison of Various Statistical Alignment Models," Computational Linguistics Volume 29 pp9-51, March. 2003.

[4] Chan, P.K et tl, "Distributed data mining in credit card fraud detection," Intelligent Systems and their Applications, IEEE (Volume:14 , Issue: 6), pp67 - 74, Aug 200.2

[5] Clifton Phua et tl. "A Comprehensive Survey of Data Mining-based Fraud Detection Research," Intelligent Computation Technology and Automation (ICICTA), pp50 - 53 Sep 2010.

[6] Lae-Joeng, Park, "Evolutionary Learning of Neural Networks Classifiers for Credit Card Fraud Detection," Korean institute of Intelligence Systems, pp 400 - 405, Oct 2001.

[7] Lae-Joeng, Park, "Cost Sensitive Learning for Credit Card Fraud Detection," Korean institute of Intelligence Systems, pp 544 - 551, Oct 2005.

[8] Telecommunications Technology Association. "Fraud Detection and

Response Framework Electronic Financial Transaction System,"Dec 2011.
〔9〕 Financial Security Researchers, "Fraud Detction System Technical Guide," Aug.2014.
〔10〕 J.S. Kim, "Trading for over phishing detection assay fraud prevention," Information Security Journal, 23(6), pp.41-48, Dec. 2013.
〔11〕 E.Y. Park, "A Study of Accident Prevention Effect through Anomaly Analysis in E-Banking," Society for e-Business Studies, pp 119-134, Nov 2014.
〔12〕 J.H, Park, "Effective Normalization Method for Fraud Detection Using a Decision Tree," Journal of The Korea Institute of Information Security & Cryptology, Vol 25, Feb. 2015.

〈저자소개〉

최 의 순 (Euisoon, Choi) 정회원
1999년 2월: 고려대학교 경영정보학과 학사
2012년 9월~현재: 고려대학교 정보보호대학원 석사과정
2000년 1월~2004년 3월: 한국오라클 ERP, BSC 컨설턴트
2004년 3월~2005년 3월: (주)넥서브 ERP 컨설턴트
2005년 3월~현재: 농협중앙회 상호금융리스크관리부 근무
〈관심분야〉 위험관리,금융보안, 핀테크, 금융리스크관리모델

이 경 호 (Kyung Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 위험관리. 정보보호컨설팅. 정보보호 및 개인정보보호정책