Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Study on the Improvement of FDS Effectiveness over the Case Analysis on E-commerce Credit-card Fraud-to-sales

Seung-Hyun Kim[1], Huy Kang Kim[*2], Eunjin Kim[3]

[1]*Department of Financial Security, School of Information Security, Korea University*
[2]*School of Information Security, Korea University*
[3]*Department of International Industrial Information, Kyonggi University*

ABSTRACT

As the advancement of information and communications technology (ICT) and the rapid growth of Fintech (Finance Technology) industry, the proportion of online e-commerce increases sharply in the credit-card payment market recently. Also, various payment services such as mobile card and the easy payment system have emerged in the e-commerce area, and electronic finance frauds and accidents using credit cards have also become more sophisticated and diversifiable accordingly. Thus, establishing FDS (Fraud Detection System) that considered differentiated e-commerce environmental features from the offline based current FDS system is needed to advance the prevention and detection of credit card frauds and accidents in e-commerce. In this paper, we compare the operating environment of the offline credit-card transaction and online e-commerce. Then we propose improvement method of credit-card e-commerce FDS detection that specialized online e-commerce. This method is considered the feature of the online credit-card transaction and the pattern of fraud usage in addition to operating offline transaction based FDS currently. And we verify the propriety and efficiency of the proposed method by applying it to the FDS system currently managed by a financial company.

KEYWORDS: Frauds, Fraud detection system, Credit cards, Online transaction, E-commerce

ARTICLE INFO: Received 11 November 2015, Revised 11 December 2015, Accepted 11 December 2015.

1. 서 론

정보통신기술의 발전과 무선 네트워크의 발전은 전자상거래 규모를 지속적으로 성장시켰다. 최근에

[*]Corresponding author is with the Graduate School of Information Security, Korea University, 145 Anam-ro SeongBuk-gu Seoul, 02841, KOREA.
E-mail address: cenda@korea.ac.kr

는 모바일 디바이스의 발전과 모바일 단말 사용자 수의 증가로 인해 언제 어디서나 모바일 단말을 이용할 수 있는 환경이 구축되었다. 또한 핀테크 산업의 활성화에 따라 다양한 온라인 지불결제 수단이 등장하고 있다. 이로 인해 신용카드 지불결제 시장에서 전자상거래의 비중은 급속하게 증가하고 있다. 한국은행 보도자료에 따르면 2014년도 4/4 분기 전자지급결제대행 중 카드 이용 건수는 20,3782(천건)으로 전체 건 수 중 67.5%, 이용금액은 104,766(억원)으로 전체 금액의 70%를 차지하고 있으며, 신용카드 전자상거래 거래 규모 또한 2013년 7.5%(40.9조원), 2014년 8.6%(49.8조원)로 급격히 증가하는 등 전자상거래를 위한 신용카드 사용은 지속적으로 증가하고 있다. 또한 스마트폰 사용이 보편화되고 앱(app) 방식의 카드발급이 확산되면서 2014년 말 모바일카드 발급장수는 1,588만장으로 2013년 말(450만장)에 비해 3.5배 증가하였고, 모바일 카드를 이용한 결제금액도 2014년 일평균 191억원으로 전년대비(26억원) 7.3배 증가하였다[1]. 이렇듯 고객들은 시간과 장소에 구애 받지 않고 온라인 상에서 신용카드를 이용한 전자상거래를 편리하게 이용할 수 있게 되었지만, 고객정보가 전자화되고 이에 접근할 수 있는 IT 기기들이 늘어남에 따라 전자상거래의 신뢰성을 위협하는 요인 또한 증가하게 되었다. 카드 사용 건수가 갈수록 증가함에 따라 카드 부정사용 또한 지속적으로 증가하며 발생하고 있는데, Visa Korea 분석에 따르면 전 세계적으로 비대면 신용카드 거래의 부정사용규모는 연간 7천억원 규모로 카드 부정사용 중 가장 큰 비중을 차지하고 있으며 2008년 40%에서 13년 57%로 점점 증가하고 있는 추세이다[2].

현재 국내에서 2014. 09 미래부 「인터넷 이용환경 개선 발표」를 시작으로 변화하는 금융 환경에 대한 가이드라인과 방향을 제시하기 위해 금융위에서 2015. 01 「IT금융융합지원방안 및 핀테크 지원방안」, 2015. 03「전자금융감독규정 개정」, 2015. 07 「전자상거래 결제 간편화 방안」등을 발표하였다. 이에 따라 ActiveX 퇴출이 진행되고 있으며, 공인인증서 의무사용의 폐지와 함께 핀테크 산업이 전면적으로 대두되면서 금융결제 패러다임이 크게 변화하고 있다. 핀테크 활성화로 인한 금융서비스의 변화는 이용자의 편의성과 시장 확대에 초점을 두고 있기 때문에 금융서비스의 절차가 간편해지고 범위가 확대되는 만큼 보안적인 측면에서 체계적인 대응책을 마련할 필요가 있다.

미래부는 2015년 올해부터 핀테크 서비스 이용자를 파밍, 피싱 또는 사기거래로부터 보호하기 위해 개인용 FDS (Fraud Detection System) 기술개발을 추진하겠다고 밝혔다. 또한 핀테크 보안기술 확산을 위해 FDS를 실시간 신용도 분석, 이상거래탐지 등 핀테크 보안 시스템에 적용하겠다는 방침을 내 놓았으며 금융감독원, 금융보안연구원, 주요 은행 및 증권사로 구성된 '이상금융거래탐지시스템(FDS) 협의체'를 구성하며 FDS 구축을 장려하고 있다. 2015년 현재 국내 모든 카드사들이 FDS 구축을 완료하였고 은행권 17개사 중 10개사가 구축을 완료한 상황이며, 아직 구축되지 않은 금융회사들도 올해 안에 FDS의 구축을 완료할 예정이다. 그리고 앞으로 전자상거래 상에서 발생하는 사기거래의 예방대책으로써 FDS 의 역할은 더욱 중요해지고 있다.

그러나 IT기술의 급속한 발전과 다양한 전자지불결제 수단의 등장에 따라 공격자의 공격 및 사기 수법 또한 점점 고도화되고 있으며, 이로 인하여 기 구축된 FDS의 탐지 기능으로는 지속적으로 증가하고 있는 전자금융사기에 대응하는데 한계를 보이고 있으므로, 전자상거래 카드 사기사고 예방을 위한 FDS의 기능 개선이 필요한 시점이다.

따라서 본 논문에서는 개선된 전자금융 사기사고 예방대책의 마련을 위해 현재 신용카드사에서

운영 중인 FDS의 운영현황을 검토하고, 전자상거래의 환경 및 전자금융 사기사고 발생 패턴 등을 분석하여 전자상거래 FDS의 탐지 기능 개선방안을 제안하고자 한다. 이를 위해 먼저 실제 A금융회사에서 현재 운영 중인 기존 FDS의 시스템 구성현황 및 탐지 방법 등을 분석한다. 그 후 신용카드 오프라인 거래와 전자상거래의 거래발생 환경을 비교 분석하고 최근 발생한 전자상거래 부정사용 발생 패턴과 결합하여 분석함으로써 의심 거래 및 부정사용 탐지에 활용할 수 있는 전자상거래 FDS의 탐지 패턴을 제안한다. 또한 제안하는 방법을 A금융회사의 전자상거래 FDS 시스템에 적용하여 실험을 진행함으로써 제안 방법의 적절성과 효율성을 입증하였다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 통해 FDS와 관련된 선행 연구와 국내 및 해외의 전자금융 사고 및 대응 동향을 살펴보고, 3장에서는 FDS의 오프라인 거래와 온라인 전자상거래의 운영 환경을 비교하고, A금융회사에서 현재 운영 중인 오프라인기반 FDS의 한계점을 분석한 후 의심 거래 및 부정사용 탐지에 활용할 수 있는 새로운 탐지룰을 제안한다. 4장에서는 이를 이용하여 e-FDS 고도화를 위한 추가 탐지 방법을 제안한 후 이를 A 금융사에 실제 적용한 실험 결과를 분석하고, 5장에서 결론을 맺는다.

2. 관련 연구

<그림 1>에서 보는바와 같이 2011년 4분기 이후 신용카드 전체 매출액 대비 부정사용률(Fraud-to-sales ratios)은 하향추세였으나, 최근 온라인 비대면거래를 통한 부정사용은 증가추세인 것으로 나타났다[2].

이는 IT 기술의 급속한 발전 및 국내외 전자금융결제환경이 급격한 변화가 원인으로 판단된다. 이에 국내외 신용카드회사들은 사고 방지를 위해 기 운영 중이던 오프라인 기반의 FDS를 일부 개선하여 전자상거래 이용자의 이상금융거래 시도를

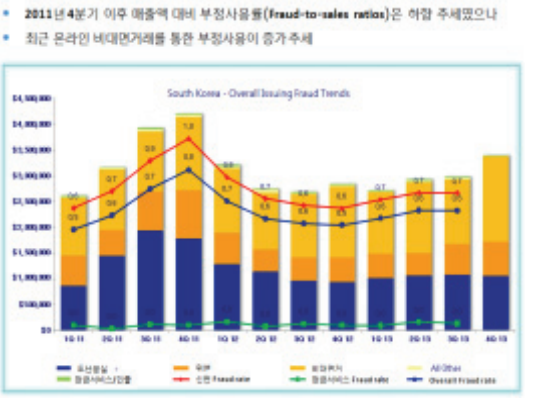

그림 1. 국내 부정사용 유형 별 동향
Figure 1. Trends of domestic fraud-to-sales

탐지하여 차단하는 시스템을 개발, 운영하여 왔으나, 오프라인 거래와 온라인 거래의 차별성 및 전자상거래 환경의 특성 등으로 인하여 기존의 FDS로 전자상거래 상의 부정사용을 탐지하는 것에 한계가 드러나 전자상거래의 특성을 고려한 e-FDS의 구축 필요성이 대두 되었다.

2.1 해외 연구동향

미국에서는 2003년에 제정된 공정 정확 신용거래법(FACTA)에 따라 2008년부터 금융기관에 이상금융거래 탐지 시스템(Fraud Detection System)을 필수적으로 적용하는 방안을 시행하고 있다. US BANK와 NetBank는 룰 기반의 비정상적 금융거래 행위를 찾아내는 탐지모델을 도입하여, 이상금융거래 탐지에 위치정보 뿐만 아니라 디바이스 정보 및 거래승인내역까지 활용하고 있다[3]. 반면 국내에서는 이상금융거래 대응 지침이 거래 시점부터의 정보를 이용한 사고 방지에 집중되어 있고, 이

에 대한 대응 방안들이 주로 사용자 단말 자체의 보안에 집중되어 있었기 때문에 FDS의 활용 비율은 국외에 비해 현저히 낮은 수준에 머무르고 있다. 국외에서는 해킹과 같은 시스템 외부로부터의 공격으로 인한 사고 발생 및 피해가 빈번한 반면, 국내에서는 회사 내·외부 직원으로 인한 개인정보 유출 사고가 큰 비중을 차지하였기 때문에 FDS와 관련된 연구는 국내보다 국외에서 좀더 활발하게 진행되었다.

Siddhartha 등의 연구[4]에서는 국제 신용카드에서 거래되었던 실제 데이터에 Support Vector Machines, Logistic regression , Random forests 의 데이터마이닝 기법을 이용하는 신용카드 사기 탐지모델을 제안하였다. Jon T.S.Quah 등은 고객의 행동분석을 판독하기 위해 고객의 자기 조직맵을 만들어 실시간 사기탐지에 초점을 맞추고, 잠재적인 사기의 경우를 소비 패턴을 통해 판독하는 기법을 제안하였다[5]. 또한 D.Sanchez 등은 칠레의 유명한 소매회사의 신용카드 도용에 관한 데이터를 기반으로 연관 법칙 룰 등을 적용하여 정보를 추출함으로써, 사기 방지 및 탐지의 의사 결정에 활용 가능한 정보를 제공할 수 있는 온라인 솔루션의 마련이 가능함을 보였다[6].

2.2 국내 연구동향

정대용 등의 연구에서는 2013년 전자금융사기 피해사례 분석을 중심으로 전자금융사기 예방서비스의 한계를 분석하였고 전화(ARS)방식 및 거래연동 OTP 기술과 이상금융거래탐지시스템과의 연계를 제한함으로 개선방안을 도출하였다[7]. 최의순 등은 전자금융사고 사례에서 사고유형과 거래행위 파악을 통한 미탐 분석과 특정 기간 추가 인증 및 아웃바운드 전화 내역 전사조사를 통한 오탐 분석을 기반으로 거래 행태에 기반한 이상거래 탐지 규칙 개선 방법을 제안하였다[8]. 박은영 등은 현 금융회사에 구축되어 운영 중인 이상 금융거래 탐지 및 차단시스템을 분석을 통한 사고예방의 효과성과 보안대책에 대한 개선방안을 제안하였다[9].

국내 FDS는 주로 카드사에서 카드 도난과 부정사용에 대응하기 위한 방안으로 도입하여 운영하고 있는 중이다. 그러나 이러한 FDS는 앞서 이야기한 것처럼 거래 시점에서의 거래 내역 정보를 이용한 의심거래 탐지에 그 기능이 집중되어 있기 때문에, 점차 다양화·고도화되는 침해행위 및 부정사용 공격에 대응하기 위해서는 FDS의 개선 및 보완이 반드시 필요하다. 국내에서도 이러한 사회적 기술적 요구와 함께 사용자 편의성 위주로 결제 시스템 및 금융 환경이 변화하는 트렌드에 힘입어, 카드사뿐만 아니라 은행 및 증권사 등 전반적인 금융사들을 중심으로 금융거래 상에서의 이상거래 탐지 고도화를 위한 다양한 연구가 진행되고 있다.

한국정보통신기술협회에서는 전자금융거래를 위협하는 공격 방식이 정교화 및 기능화 됨에 따라 2012년 '이상 금융거래 탐지 및 대응 프레임워크'를 발간하면서 이상금융거래의 탐지를 위한 요구사항과 탐지 방법, 대응방법을 기술하고, 이상금융거래 탐지 및 대응 프레임워크를 제안하고 대응을 위한 메커니즘을 기술하고 있다. 이는 이상금융거래 탐지 및 대응 시스템을 개발하고자 하는 개발자와 도입 및 운영하고자하는 이들에게 표준으로 활용되고 있다.

금융보안연구원에서는 2014년 '이상 금융거래 탐지시스템 기술가이드'[10]를 발간하면서 이상금융거래 탐지의 효과성 향상을 위한 금융회사에서 알맞은 고유기능별 선택, 도입할 수 있는 대표적인 기능을 소개하고, 이상금융거래를 효과적으로 탐지할 수 있도록 참고할 수 있는 가이드를 제시하고 있다. 이는 전자금융거래의 수집된 정보를 종합적

으로 분석하여 이상 금융거래 유무를 판별하는 기능을 크게 4가지 기능(정보수집, 분석 및 탐지, 대응, 모니터링 및 감사)을 이루어 복합적인 시스템으로 판별해야 된다고 정의하고 있다.

3. 제안된 이상거래 탐지 시스템

현재 A금융사의 이상거래 탐지 시스템 운영방법인 Score 방식 및 Rule방식 기반 탐지모형을 살펴보고 기존 FDS의 한계점을 분석하여 전자상거래 환경에 적합한 탐지 정책을 제안하고자 한다.

3.1 Score방식과 Rule 방식 기반 이상거래 탐지 시스템

현재 금융사에서 적용되어 있는 이상 금융거래 탐지 시스템은 기 발생한 부정사용 매출 내역에 대한 통계 분석을 통해 부정사용을 적발할 수 있는 변수를 활용한 Score방식과 Rule방식에 기반을 두어 부정사용거래 여부를 판단한다. Score방식과 Rule방식 기반 부정사용거래 선정방식은 <표 1>의

표 1. FDS 탐지 패턴 생성 기준
Table 1. The criteria for generating FDS detection pattern

Score 방식	세부내용
고객 프로파일 정보 영역	고객이 사용한 승인금액, 시간대, 업종 등
가맹점 프로파일 정보 영역	카드가 사용된 가맹점에서 거래되는 매출 패턴 정보 - 평균 객단가 등
카드 프로파일 정보 영역	해당 카드의 거래 매출 패턴 정보 - 주사용 업종 등
On/Off-line 통합 사용 패턴정보	온라인 및 오프라인 거래를 통합한 카드 매출 패턴 정보
패턴 생성 방식	기 발생한 부정사용 매출발생에 대해 여러 통계기법을 이용하여 발생 유형 및 변수를 도출하여 Scoring Model을 개발
Rule 방식	**세부내용**
위치기반정보 반영	고객 최신 지역정보에 의한 위치정보를 반영하여 정확한 지역간 이동가능시간 분석
최신 사고 유형 학습	최근 많이 발생하고 있는 사고 유형 학습
패턴 생성 방식	사고 발생 다발 특정 국가나 업종, 가맹점 정보 등을 조합하고, 거래금액 및 거래횟수 등을 고려하여 검색 Rule 조건을 생성

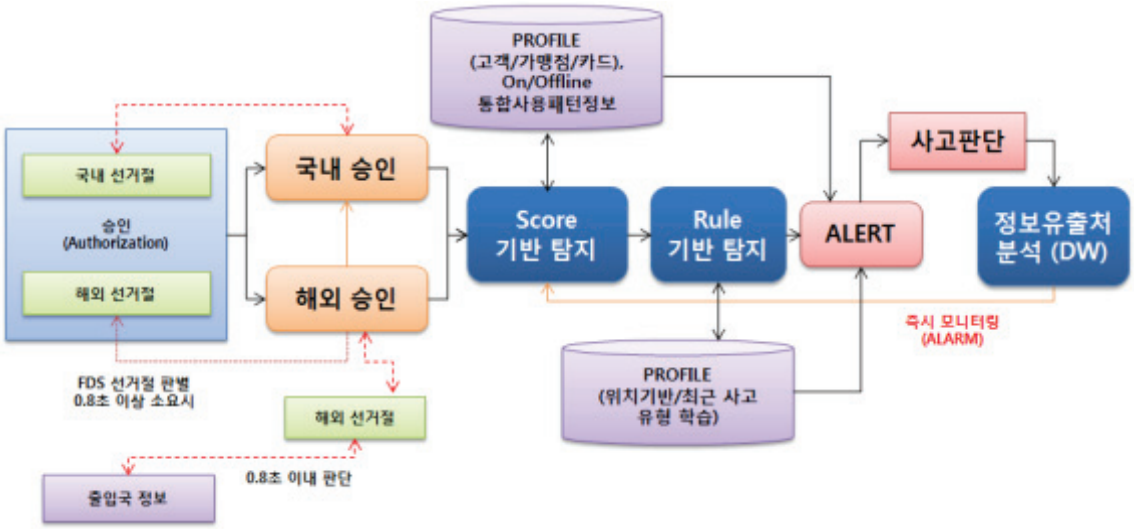

그림 2. FDS 모니터링 프로세스 모델
Figure 2. The model of FDS monitoring process

기준으로 선정한다.

이렇게 선정된 패턴을 기반으로 Score방식과 Rule방식을 병행하여 FDS 시스템에서 <표 2>의 방법으로 모니터링 대상을 선정하고 사고거래 의심건을 판단한다. FDS 모니터링 프로세스 모형은 다음 <그림 2>와 같다.

표 2. FDS 의심거래 선정 방법
Table 2. Methods to select suspicious transaction of FDS

방식	의심 거래 선정 방법
Score 방식	거래 발생 시 마다 동 Model에 의해 거래위험도를 산정하고 일정점수 이상 건에 대해 실시간 모니터링 관리
Rule 방식	거래 발생 시 마다 동 Rule 조건에 해당하는 건을 자동으로 선정하여 실시간 모니터링 관리

3.2 Score방식과 Rule방식 기반 이상거래 탐지 시스템의 한계점

서론에서 언급한 바와 같이 현재 국내 카드사들의 FDS 시스템은 과거 거래내역 및 거래발생 시점에 수집된 정보 기반의 패턴분석 결과에 따른 의심거래 탐지에 그 기능이 집중되어 있어 다양한 전자금융 사기 사고를 예방하는 데에는 한계가 있다.

표 3. 신용카드 온/오프라인 거래 환경
Table 3. On/Off-line trade environments of credit-card

구분	오프라인	온라인
거래방식	대면	비대면
카드소지 여부	실물카드 필요	실물카드 불필요
거래 매체	이용매체 제한적	PC 및 모바일 디바이스 등 다양한 매체 사용
본인 확인 절차	사용자 실물 확인	전자적 인증방법 사용
가맹점	다양한 가맹점에서 매출 발생	매출 발생 가맹점 제한적

표 4. 신용카드 온/오프라인 부정사용 사고 발생 유형
Table 4. Type of on/off-line fraud-to-sales risk by the credit-card

구분	오프라인	온라인
시고유형	실물카드 위변조	인증서 및 신용카드 정보 도용
사고발생 업종	제한 없음	환금성 업종
발생지역	위변조카드에 의한 해외 매출	국내 온라인 매출
사고 발생 가맹점 수	다수	동일 가맹점 집중
건당 금액	평균 30만원 이상	평균 30만원 미만
발생 건수	소수	짧은 시간 다량 발생

위의 <표 3>에서 보는 바와 같이 신용카드의 오프라인 거래는 실물카드 기반의 대면거래인 반면 전자상거래는 비실물카드 기반의 비대면거래로써 기본적인 거래환경이 확실하게 구분됨을 알 수가 있다. 이것은 기존 FDS 탐지 패턴의 중요한 항목 중의 하나인 위치정보가 전자상거래 상에서는 중요한 정보가 아니라는 것을 의미한다. 또한 오프라인 거래의 경우 가맹점에 설치된 단말기를 통하여서만 거래가 발생하므로 거래이용 매체가 제한적이지만 전자상거래의 경우 PC, 스마트폰 및 다양한 모바일 기기 등을 통하여 거래가 발생하므로 전자상거래에서는 매체정보가 중요한 의미를 갖는다. 그리고 전자상거래의 경우 주사용 가맹점이 제한적인 성향을 나타내므로 최근 거래 가맹점 정보도 중요한 변수로 활용이 가능하다.

이와 같이 오프라인 거래와 전자상거래는 이상거래 탐지를 위한 점검항목에 큰 차이를 보이고 있다. 또한 오프라인거래와 전자상거래 상에서 발생한 신용카드 부정사용 사고의 유형을 비교해보면 아래의 <표 4>와 같다.

<표 4>에서 볼 수 있듯이 온라인에서 발생하는 부정사용은 오프라인에서 발생하는 부정사용 유형과 비교하여 사고발생 업종, 지역 및 매출형태 등의 특성이 뚜렷한 차이를 나타내고 있다. 따라서

과거 오프라인 기반의 변수를 활용한 기존의 FDS로는 전자상거래 상에서 발생하는 이상거래탐지를 통한 부정사용 발생 예방에는 한계가 있음을 확인할 수 있다.

3.3 전자금융거래를 위한 이상거래 탐지 시스템의 개선 방안

다양한 단말환경 및 핀테크 산업의 발전으로 인한 비대면 거래의 증가에 따라 비대면 거래의 신용카드 부정사용은 갈수록 증가하고 있다. 그러나 앞서 수행된 분석과 같이, 기존 이상금융거래 탐지 시스템(FDS)의 Score 기반 및 Rule 기반의 변수들은 대부분 과거의 거래 환경을 토대로 구축되어 있어, 다양한 유형의 온라인상의 비대면 거래의 부정사용 거래 탐지에 효과적으로 대응하기 어려운 환경이다. 따라서 전자금융거래에서의 이상거래탐지시스템을 활용한 부정사용 사고 발생을 줄일 수 있는 방안을 전자금융거래 환경 및 특성 등을 반영하여 개선하고자 한다.

기존의 오프라인 환경 변수 중 온라인 환경에서도 활용 가능한 변수에 전자상거래 환경을 반영한 FDS Rule 변수를 결합하여 개선된 이상거래탐지 시스템 방법론을 제안하고자 한다. 기존 오프라인 환경 기반 FDS Rule방식에는 신용카드 단말기를 통한 대면인증 방식이었다. 그러나 온라인 전자금융거래에서는 다양한 디바이스를 통해 거래가 발생하므로 디바이스 정보 활용 검색 Rule이 필요하며, 비대면인증을 위한 전자적인 방식의 인증서를 활용하므로 인증서 관련 정보 또한 유용하게 활용이 가능하다.

또한 온라인거래 특성상 발생할 수 있는 거래유형의 다양성 및 다발사용가능성 등의 매출특성 Rule을 추가하였다.

오프라인거래에 비해 주로 온라인거래에서 이루어지는 게임, 파일공유, 포인트 충전, 상품권, 경매 등

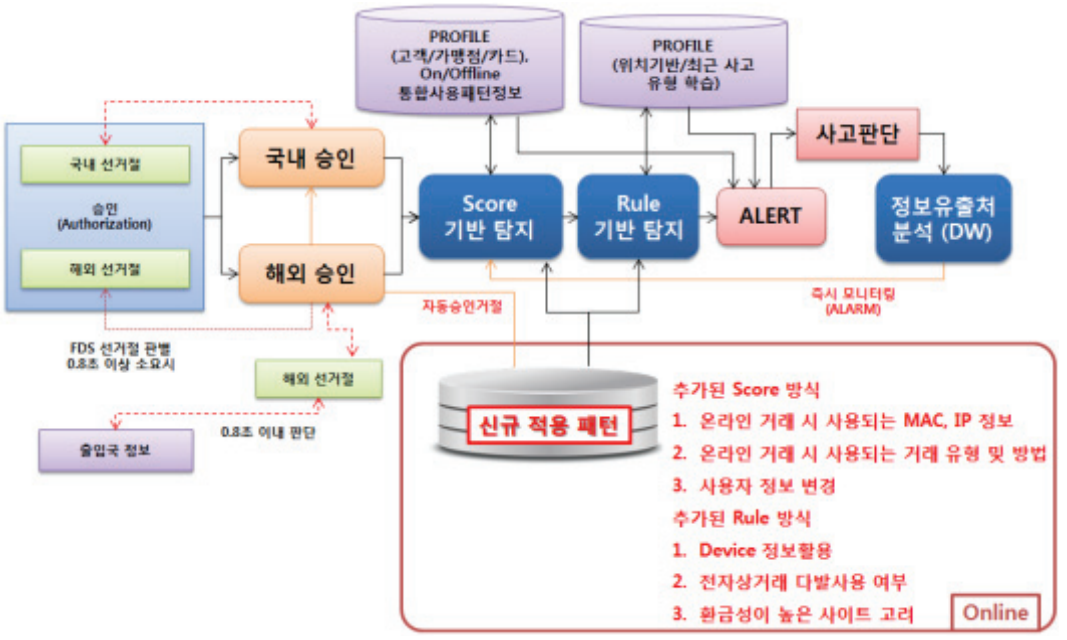

그림 3. 개선된 FDS 모니터링 프로세스 모델
Figure 3. The improved model of FDS monitoring process

환금성이 높은 사이트를 고려한 업종검색 Rule도 추가하였다. 기존 Score 방식과 Rule 방식 기반에서 추가된 방식은 <표 5>와 같다. <표 5>의 신규 탐지 패턴을 기존 방식에 추가하여 적용한 FDS 모니터링 프로세스 모형은 <그림 3>과 같다.

4. 이상거래탐지 시스템 분석 및 실험 결과

4.1 이상 금융거래 탐지 및 분석

기존의 오프라인 기반 Score 방식과 Rule 방식의 이상 금융거래 탐지패턴의 한계점을 개선하기 위해 기존의 A금융회사에서 현재 운영 되고 있는 FDS에 온라인 전자금융거래 환경을 반영한 신규 패턴을 추가로 적용하여, 제안하는 개선된 e-FDS 고도화 방안에 대한 실험을 진행하였다.

신규 패턴 추출을 위한 데이터 수집 기간은 2013년 01월 01일 ~ 2014년 12월 31일로, 총 24개월 동안 A금융회사의 FDS에서 발생하였던 온/오프라인 이상징후 탐지 모니터링 데이터 및 부정사용 사고 데이터를 기반으로 FDS 고도화를 위한 패턴 분석을 진행하였다.

도출된 신규 패턴을 적용한 FDS 의 실험은 최근 발생한 6개월분(2015년 05월 01일 ~ 2015년 10월 30일, 약 2천만건)의 신용카드 거래내역 데이터를 대상으로 진행하였다. 실험 과정은 다음과 같다.

첫 번째로, 기존의 오프라인 기반 FDS에서 2013년 01월 01일 ~ 2014년 12월 31일까지 총 24개월 동안 발생한 온/오프라인 부정사용 발생 건(34건)과 기존 탐지 패턴(약 90개) 및 전자상거래 환경 특성 등의 데이터를 분석하여, <표 5> 와 같이 FDS 개선을 위해 적용할 수 있는 신규 패턴을 도출하였다.

두 번째로, 도출된 패턴을 기존 FDS에 추가로 적용하여 탐지 기능을 개선시킨 e-FDS를 이용한 탐지 시뮬레이션을 실시하였다. 시뮬레이션 정보유출처분석(DW)으로 부터 모니터링 대상으로 들어간 유형들을 분석 하였고, 최근 6개월간의 거래내역(2천만 건)을 대상으로 추가된 신규 패턴에 의해 탐지된 모니터링 대상 부정사용 거래 내용 프로파일링을 추출하였다.

표 5. 신규 적용 패턴 종류
Table 5. The type of novel application pattern

Score 방식	세부내용
고객 프로파일 정보 영역	온라인 거래시 사용되는 MAC, IP 정보
거래 방법, 거래 유형	온라인 거래시 사용되는 거래 방법 및 유형
이용자 정보 변경	인증방법 및 전화번호 등 사용자 정보의 변경
업종 정보	온라인 부정사고 다발 업종 - 게임사이트, 상품권 업종 등
Rule 방식	**세부내용**
Device 정보활용 검색 Rule	인증결제 및 발급 과정 중 사용되는 기기정보를 활용
인증서 정보	전자적 인증 방식 별 인증 정보 검증
전자상거래 다발 사용	온라인 거래시 비정상적으로 많은 거래를 발생시키는 경우
환금성이 높은 사이트를 고려한 업종	기존과 다른 비정상적인 패턴 발생

세 번째로 시뮬레이션을 통해 추출된 부정사용 거래 데이터에 최근 6개월 동안 실제로 발생한 부정사용 사고 건의 포함 여부를 검증하였다.

<그림 4>는 FDS 모니터링 과정을 거친 결과 데이터를 분류하여 나타낸 것이다. A1은 기존 FDS 패턴으로 추출된 모니터링 대상 의심거래 데이터이고, A2는 신규 패턴을 추가 적용 후 추출된 모니터링 대상 의심거래 결과 데이터이다.

B1은 A1 모니터링 대상에 포함되지 않은 최근 6개월간 실제로 발생된 온라인 부정사고 전체 건을 나타내는 부분이고, B2는 A1에는 포함되지 않았었으나, A2의 모니터링 대상 데이터에는 포함된 최근 6개월간 발생된 온라인 부정사고 건(6건)이다.

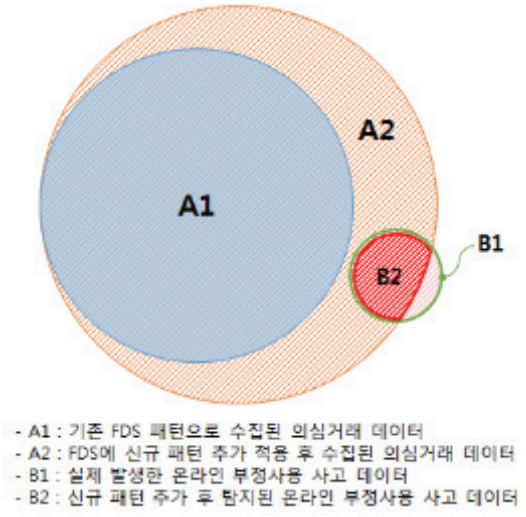

그림 4. FDS 모니터링 데이터 분류
Figure 4. The classification of FDS monitoring data

실험 결과, 제안하는 신규 패턴이 적용된 FDS 시스템의 경우 기존 FDS 시스템에서 모니터링 하지 못했던 데이터를 포함하여 더 많은 양의 의심 거래 데이터를 모니터링 하였다. 이러한 모니터링 데이터로부터 기존 FDS 시스템에서는 모니터링이 불가능했던 전체 온라인 부정사용사고 B1 부분 중 B2에 해당하는 금융사고 데이터를 개선된 FDS 시스템에서 모니터링이 가능했다. 이를 통해 제안하는 방법이 효과적으로 금융사고 데이터를 모니터링 할 수 있음을 확인할 수 있었다.

4.2 효과성 분석 및 개선 방안

2013년 01월 01일 부터 2014년 12월 31일 까지 총 24개월 동안 발생하였던 온/오프라인 이상 징후 탐지 모니터링 데이터 및 부정사용 사고 데이터를 기반으로 분석하여 신규 적용 패턴을 <표 5> 로 도출하였다. 제안한 신규 패턴을 기존 FDS에 추가로 적용하여 최근 6개월 동안(2015년 05월 01일 ~ 2015년 10월 30일, 약 2천만 건) 발생하였던 신용카드 거래내역을 대상으로 이상 징후 탐지를 실험해본 결과 신규 패턴 적용으로 기존에는 탐지하지 못했던 온라인에서 발생하는 부정거래 의심 모니터링 데이터를 얻을 수 있었다. <표 6>과 같이 일평균 모니터링 된 데이터들을 본 논문에서 제안한 신규 패턴으로 분류할 수 있었다.

FDS 일평균 모니터링 건수는 <표 7>과 같이 신규 패턴 적용 후 기존에 비해 약 10배 가량 탐지 데이터가 증가하는 결과가 나타났다. 또한 <그림 4>와 같이 FDS에 신규 패턴을 적용시킨 결과, 개선된 e-FDS는 최근 6개월 동안 실제 발생하였던 온라인 부정사용 사고 데이터(B1) 중에 82% 해당되는 데이터(B2)를 탐지해 낼 수 있었다.

표 6. 추가 신규 패턴 적용 후 의심 부정사용 거래 건수
Table 6. Suspicious fraud-to-sales transaction count following additional novel pattern application

	적용한 추가 신규 패턴	모니터링 된 의심 부정 사용 거래 건수
Score 방식	고객 프로파일 정보 영역	77건
	거래 방법, 거래유형	102건
	이용자 정보 변경	14건
	업종 정보	73건
Rule 방식	Device 정보 활용 검색 Rule	220건
	인증서 정보	32건
	전자상거래 다발사용	63건
	환금성이 높은 사이트를 고려한 업종	189건

표 7. 부정사용 거래 내용 프로파일링
Table 7. Profiling of fraud-to-sales transaction contents

	기존 FDS	신규패턴 적용 후 개선된 e-FDS
일평균 모니터링 건수	70건	770건

비록 FDS 정보유출처분석(DW)으로 부터 모니터링 결과로 추출된 데이터 중 실제 부정사용 사고로 발생하는 건이 큰 비율을 차지하지는 않지만 즉시성과 가용성, 거래에 대한 신뢰성을 바탕으로 운영되는 금융회사에게는 적은 수의 사고 건수도 잠재적으로 큰 위협이 될 수 있다.

따라서 본 논문에서 제안하는 신규 패턴을 적용한 개선된 e-FDS를 활용함으로써 온라인 거래가 급격하게 증가하고 있는 전자금융거래 환경에서 부정사용 거래의 탐지율 향상을 기대할 수 있으며, 향후 변화하는 환경에 따른 패턴을 추가로 수집·분석하여 FDS에 적용함으로써 부정사용 거래에 대한 탐지율을 개선시킬 수 있음을 확인하였다.

5. 결 론

본 논문에서는 현재 카드사에서 운영 중인 FDS의 운영환경 및 전자금융 사기사고 탐지방법 등을 분석하여 그 한계점을 지적하였으며, 기존 FDS의 기능을 개선하기 위하여 신용카드 오프라인 거래와 전자상거래의 거래발생 환경을 비교 분석하고 최근 발생한 전자상거래 부정사용 발생 패턴과 결합하여 분석함으로써 전자상거래에서 발생할 수 있는 의심 거래 및 부정사용 탐지에 활용할 수 있는 e-FDS의 탐지 패턴을 제안하였다. 또한 제안하는 방법을 A금융회사의 전자상거래 FDS 테스트시스템에 적용하여 실제 거래데이터를 대상으로 실험을 진행함으로써 제안 방법의 적절성과 효율성을 입증하였다.

이는 기존의 FDS 관련 타 연구에서는 제시된 적이 없는 실질데이터를 이용하여 실험하였기 때문에 본 제안이 현재 FDS를 구축·운영 중이거나 곧 도입하려는 신용카드사 및 타 금융회사가 향후 전자금융거래 FDS 의 기능 개선 추진 시 많은 도움이 될 것으로 기대한다.

본 논문을 통해서 제시된 탐지 패턴은 기존 FDS의 탐지 패턴에 전자상거래의 환경적 특성 및 기 발생했던 온라인 부정사용 사례를 분석하여 도출된 디바이스 정보 및 인증 관련 정보 등의 변수들을 반영하여 전자상거래 이상거래탐지에 특화된 탐지 패턴들을 선정하여 적용하였으며, 그 결과 기존 FDS에 탐지하지 못했던 온라인 의심거래 건에 대한 탐지 기능을 개선함으로써 전자상거래 부정사용사고 발생 예방에 큰 효과가 있음을 입증하였다.

앞으로 이번 논문에서 제시된 Rule 패턴 이외에도 웹 및 모바일 전자상거래 환경에서 발생할 수 있는 새로운 위협에 대응 가능한 다양한 내용의 Rule 패턴 업그레이드를 위한 지속적인 연구가 필요할 것으로 판단되며, 또한 패턴 기반의 이상거래탐지 시스템의 한계를 극복하고 부정사용 사고 발생을 사전에 효율적으로 예방하기 위해서는 다양한 사전 정보 분석을 통한 사전 행위기반 이상거래탐지 모델에 대한 연구도 병행되어야 할 것이다.

References

[1] The Bank of Korea, *Banking services usage statics throughout the year*, 2015.

[2] VISA Korea, *TC40 client fraud reporting and operating certificates submission.*

[3] KB, *Recent trends and prospects of information security in the domestic and international financial institutions*, KB vitamin of knowledge, Vol. 15-19, Mar. 2015.

[4] Siddhartha Bhattacharyya, Sanjeev Jha, Kurian Tharakunnel, and J. Christopher Westland, *Data mining for credit card fraud: A comparative study*, Decision Support Systems, Vol. 50, Issue 3, pp. 602-613, Feb. 2011.

[5] Jon T.S. Quah, and M. Sriganesh, *Real-time credit card fraud detection using computational intelligence*, Expert Systems with Applications, Vol. 35, Issue 4, pp. 1721 −1732, Nov. 2008.

[6] D. Sánchez, M.A. Vila, L. Cerda, and J.M. Serrano, *Association rules applied to credit card fraud detection*, Vol. 36, Issue 2, pp. 3630−3640, Mar. 2009.

[7] 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*, Journal of The Korea Institute of Information Security & Cryptology, Vol. 24, No. 6, pp. 1243-1261, Dec. 2014.

[8] Eui-soon Choi and Kyung-bok Lee, *A study on improvement of effectiveness using anomaly analysis rule modification in electronic finance trading*, Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, No. 3, pp. 615-625 Jun. 2015.

[9] Eun Young Park, and Ji Won Yoon, *A study of accident prevention effect through anomaly analysis in E-banking*, The Journal of Society for e-Business Studies, Vol. 19, No. 4, pp. 119-134, Nov. 2014.

[10] Financial Security Agnecy, *Technical guide of Fraud Detection System*, 2014.

[11] Seo Hojin, Eunjin Kim, and Huy Kang Kim. *A novel biometric identification based on a users input pattern analysis for intelligent mobile devices.* Internatational Journal of Advanced Robotic Systems, 2012.

[12] Jae Hoon Park, Huy Kang Kim, and Eunjin Kim, *Effective normalization method for fraud detection using a decision tree,* Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, No. 1, Feb. 2015.

전자상거래 신용카드 부정사용 사례분석을 통한 FDS 효과성 향상에 관한 연구

김승현[1], 김휘강[2], 김은진[3]

[1]*고려대학교 정보보호대학원 금융보안학과*
[2]*고려대학교 정보보호대학원*
[3]*경기대학교 국제산업정보학과*

요 약

최근 정보통신기술의 발달 및 핀테크 산업의 급속한 성장에 따라 신용카드 지불결제 시장에서 온라인 전자상거래의 비중이 급격하게 증가하고 있다. 이로 인해 모바일카드 및 간편결제 등 전자상거래에서 다양한 지불결제 서비스 가 등장 하였으며 이에 비례하여 신용카드를 이용한 전자금융사기 사고 또한 고도화 및 다양화 되고 있다. 금융 사고 방지를 위해 정부 및 금융당국은 FDS(Fraud Detection System, 이상거래 탐지시스템) 활성화를 추진하고 있지만, 현재 카드사에서 사용되고 있는 FDS는 오프라인 거래 내역 기반의 의심거래 탐지에 기능이 집중되어 있어 온라인 상의 전자상거래에 적용하기에는 그 한계점이 드러나고 있다. 따라서 전자상거래 신용카드 사기사고 예방 및 탐지의 고도화를 위해서는 오프라인 거래 기반의 현 FDS 시스템과 차별화된 전자상거래의 환경특성을 반영한 FDS의 구축이 반드시 필요하다. 본 논문에서는 신용카드 오프라인 거래와 온라인 전자상거래의 운영환경을 비교하고, 현재 운영중인 오프라인 거래 기반의 FDS에 온라인 신용카드 거래의 특성 및 부정사용의 발생패턴 등을 반영하여 온라인 전자상거래에 특화된 신용카드 전자상거래 FDS 탐지 기능 개선방안을 제안한다. 또한 제안하는 방법을 실제 금융사에서 운영하고 있는 FDS 시스템에 적용하여 제안 기법의 적절성과 효율성을 검증한다.

Seung Hyun Kim received his B.S. degree in Computer Engineering from Dongguk University, Seoul, Korea, in 1991. Currently, he is a M.S. student in Korea University Graduate School of Information Security, Seoul, Korea. In Dec. 1990, he joined the Division of Information Technology at BC Card, Seoul, Korea, and he is currently serving as a Team Leader. His current research information protection policy of finance, all the way to protection of private information security, fraude detection system of credit card.

E-mail address: kim2405@naver.com

Huy Kang Kim received the bachelor's degree in Industrial & Systems Engineering from KAIST in 1998. He received the MS degree in Industrial & Systems Engineering from KAIST in 2000. He worked as Technical Director at NC soft from 2004 to 2010. He received the Ph.D. degree in Industrial & Systems Engineering from KAIST in 2009. He is now an associate professor in School of Information Security at Korea University. His current research interests include Online game security, network security, network forensic, IDS, botnet detection.

E-mail address: cenda@korea.ac.kr

Eunjin Kim received the bachelor's degree in Industrial & Systems Engineering from KAIST in 1999. She received the MS degree and the Ph.D. degree in Industrial & Systems Engineering from KAIST in 2001 and 2007, respectively. She is now an associate professor in Department of International Industrial Information at Kyonggi University. Her current research interests include Management information systems, security economics.

E-mail address: ejkim777@kgu.ac.kr