JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 20, No. 3, pp. 569-576, Mar. 2019

자금세탁 의심거래 탐지 방안 연구 – 소셜 네트워크 분석 기법을 중심으로

서 정 원, 김 형 중*
고려대학교 정보보호대학원 빅데이터 응용 및 보안학과

A Study on Detection Methods of Suspicious Transaction by Money Laundering - Focusing on Social Network Analysis

Jeong-Won Seo, Hyoung-Joong Kim*
Department of Big Data Applications and Security, Korea University, Seoul 02841, Korea

[요 약]

본 연구에서는 소셜 네트워크 분석 기법에 기반하여 전자금융 환경에서 발생한 자금세탁 의심거래 정보를 거래 유형별로 살펴보았다. 특히 연결중심성과 매개중심성 등 중심성 지표와 소시오그램을 통한 네트워크 구조를 분석함으로써, 자금세탁 의심거래를 탐지할 수 있는 효과적인 방안을 제안하였다. 본 연구에서 활용한 소셜 네트워크 분석 기법은 '자금세탁 행위자'를 중심으로 하는 연결관계를 기준으로 해당 판단을 수행한다는 점에서, 기존 룰 기반 추출 모델과 달리 금융거래의 종류 또는 특정 패턴에 한정적이지 않다는 장점이 있다. 또한 네트워크 노드의 수와 중심성 지표가 비례하는 특성상, 거래의 복잡도가 높을수록 자금세탁 거래의 특징을 더 잘 추출할 수 있다는 장점도 있다. 따라서 복잡한 전자금융 환경에서 자금세탁 거래를 식별하기 위한 효과적인 방법의 하나로 고려할 가치가 있다고 판단된다.

[Abstract]

In this study, it examined money laundering transactions occurred in the electronic banking environment by transaction patterns based on social network analysis. Then, analyzing the centrality indicators such as degree centrality and betweenness centrality and sociogram through the network structures, it tried to suggest effective ways to be able to detect suspicious money laundering transactions. The social network analysis technique applied to this study has the advantage that is unlimited to the types or particular patterns of financial transactions in the point of performing the decision based on the connections of 'money laundering actors.' Furthermore, there is another advantage that it can better-extract the characteristics of the transactions with 'money laundering actors' as the complexity of transactions is higher, under that the number of the network nodes is proportional to the centrality indicators. Therefore, it is worth considering as one of the effective ways to distinguish money laundering transactions in the complex electronic financial environment.

색인어 : 자금세탁, 소셜네트워크분석, 의심거래, 이상거래탐지, 거래모니터링

Key word : Money laundering, Social network analysis, Suspicious transaction, Fraud detection, Transaction monitoring

http://dx.doi.org/10.9728/dcs.2019.20.3.569

Received 15 February 2019; **Revised** 28 February 2019
Accepted 20 March 2019

***Corresponding Author; Hyoung-Joong Kim**

Tel: +82-2-3390-4895
E-mail: khj-@korea.ac.kr

Ⅰ. 서 론

2000년대 들어 인터넷 뱅킹을 비롯한 다양한 전자금융 기술이 본격적으로 발전하면서 돈의 흐름을 비교적 쉽게 추적할 수 있게 되었다. 하지만 동시에 자금세탁의 유형 및 기법은 보다 복잡화, 지능화되고 있다[1]. 자금세탁(ML; money laundering)이란 일반적으로 '자금의 위법한 출처를 숨겨 적법한 자산인 것처럼 위장하는 과정'을 의미한다. 범죄집단은 범죄를 통해 막대한 금전적 이윤과 부를 생성하고, 이러한 범죄 수익을 자금세탁을 통해 상업, 금융업을 비롯한 사회의 모든 계층에 침투하여 부패를 조장한다.

이에 따라 각국은 자금세탁 방지 제도를 확립하여 국내·국제적으로 이루어지는 불법자금의 세탁을 적발하고 예방하기 위한 법적·제도적 장치를 운영하고 있다[2]. 특히 전자금융에서 이루어지는 비대면 거래는 자금세탁을 쉽게 하는 부정적인 측면이 있다. 예를 들어 최근 부상하고 있는 암호화폐는 가상 자산 및 관련 금융 서비스로서 금융 혁신 및 효율성을 촉진하고 금융포용(financial inclusion)을 개선할 잠재력을 지니고 있는 동시에 범죄자 및 테러리스트가 수익금을 세탁하거나 불법행위에 자금을 조달할 수 있는 새로운 통로가 되고 있다[3].

대표적인 자금세탁 방지 제도로 의심거래보고제도(STR; suspicious transaction report)를 들 수 있다. 이 제도는 금융거래와 관련하여 불법재산 또는 자금세탁 행위를 하고 있다고 의심되면 금융정보분석원(KoFIU; korea financial intelligence unit)에 보고하는 제도이다. KoFIU는 금융기관으로부터 취합된 의심거래 보고 건에 대하여 외환전산망 자료와 신용정보 등 자체적으로 수집한 관련 자료를 종합 분석한 뒤, 불법거래로 판단되면 해당 자료를 법 집행기관에 제공하는 기능을 담당한다[4].

그런데 최근 들어 STR 제도의 운영 과정에서 다음과 같은 문제점이 노출되고 있다. 각 금융기관에 자금세탁 방지 시스템이 구축된 이후 의심거래 보고 건수는 양적인 측면에서 급속히 증가하였지만, 보고되는 거래행위의 품질은 높아지지 않은 탓에 비용 면에서 효율적이지 못하다는 점을 들 수 있다. 또한 증가한 STR 수 대비 인적 자원이 한정되어 있다 보니 조사분석 프로세스에 병목 현상이 발생하는 문제도 있다[5]. 따라서 금융당국과 관련 기관들은 자금세탁 의심거래를 효과적으로 탐지할 수 있는 새로운 방안을 모색할 필요가 있다. 금융업계는 거래 모니터링을 위한 방법으로 룰(rule) 기반 모델을 오랫동안 채택해왔다. 거래 모니터링에서의 룰 기반 모델이란 탐지 대상 금융거래의 유형과 패턴, 임계치에 대한 규칙을 사전에 설정하고, 이후 비정상적인 거래가 발생하였을 경우 이를 추출해내는 시스템을 의미한다. 현재 대다수의 금융기관이 STR 모니터링을 위해 업권별 특성에 따른 룰 기반 모델을 채택하여 운영 중에 있다. 하지만 룰 기반 모델은 과거에 발생했던 금융거래 기반으로 의심거래 탐지 규칙을 생성하기 때문에, 과거 발생하지 않았거나 룰로 정의되지 않은 새로운 거래에 대해서는 탐지가 불가능하다는 한계가 있다.

이에 본 연구에서는 자금세탁 거래 정보를 대상으로 기존의 룰 기반 모델과는 다른 새로운 거래 모니터링 기술의 가능성을 검토하는 데 목적을 두었다. 특히 소셜 네트워크 분석 기법을 적용하여 자금세탁 의심거래를 효과적으로 탐지하는 방안을 모색하고자 하였다.

본 연구는 자금세탁 거래를 대상으로 소셜 네트워크 분석 기법을 적용함으로써, '자금세탁 행위자'를 중심으로 하는 네트워크의 유의성을 확인하는 데 의의가 있다. 이러한 소셜 네트워크의 특징을 활용하면 금융거래의 종류 또는 특정 패턴에 한정적이지 않으며, 거래의 복잡도와 무관하게 효과적으로 자금세탁 의심거래를 식별할 수 있기 때문이다. 이를 위해 자금세탁방지금융대책기구(FATF; financial action task force on money laundering)에서 공개한 내용 중 전자금융 환경에서 새로운 지불방법을 악용한 자금세탁 범죄 사례를 유형별로 구분하였다. 그런 다음 범죄 유형별로 소셜 네트워크 분석에 필요한 중요한 지표인 연결중심성과 매개중심성을 분석하는 동시에, 소시오그램을 통한 네트워크 특징을 도출하였다. 그 결과를 토대로 궁극적으로는 전자금융 환경에서 자금세탁 의심거래를 탐지할 수 있는 효과적인 방안을 마련하고자 하였다.

Ⅱ. 이론적 배경

2-1 자금세탁 방지 제도

1) 자금세탁 방지 제도의 개관

자금세탁은 범죄수익 및 불법수익의 은닉 및 가장 행위, 조세탈루의 목적으로 재산을 은닉하거나 재산취득 또는 처분 사실을 가장하는 행위를 의미한다. 국내에서는 2001년부터 자금세탁 방지 제도가 도입됨에 따라 이를 담당하는 중앙 행정기구인 금융정보분석원, 즉 KoFIU가 출범하여 운영되고 있다[2]. 특정금융거래보고법에 따른 자금세탁방지제도의 핵심은 의심거래보고제도 STR, 고액현금거래보고제도(currency transaction reporting system) CTR, 고객확인제도(customer due diligence) CDD로 요약된다. 이중 의심거래보고제도는 자금세탁 의심거래 탐지 방안을 모색하는 본 연구 주제와 밀접한 관련이 있다.

2) 의심거래보고제도

의심거래보고제도는 특정금융거래보고법에 근거하며 다음과 같은 단계로 실행된다. 즉 어떤 금융거래가 자금세탁에 이용되고 있다고 의심되는 경우 금융기관이 해당 거래를 KoFIU에 보고하면, KoFIU에서 이를 심사 · 분석하여 검찰 등 법 집행기관에 제공하게 된다. 금융당국에서 금융기관에 배포한 주요 의심거래 유형[6]은 다음의 표 1 과 같다. 현재 금융기관은 이러한 7가지 유형을 기반으로 각 회사의 실정에 적합한 룰을 정의하여 의심거래 모니터링 모델을 운영하고 있다.

표 1. 주요 의심거래 유형
Table 1. Major types of suspicious transactions

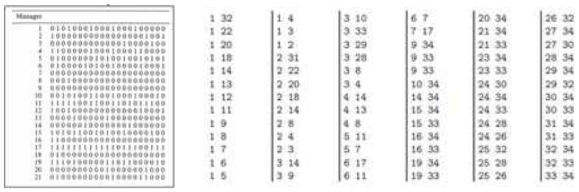
Type	Description
Cash transaction	Most of the money is withdrawn as cash
Distributed transaction	A transaction involving multiple individuals
Foreign currency Transaction	A transaction in which money laundering concerns are determined by a customer who has no overseas remittance
Transaction amount	A transaction in which the customer's financial transaction amount per day or the financial transaction amount accumulated for 7 days are determined based on the customer's confirmation
Frequency of transaction	A transaction in which the customer's financial transaction number per day or the total number of transactions for 7 days is determined based on the customer's confirmation
Split transaction (Dividing transaction)	If the customer has reasonable reasons to suspect that he / she is engaged in a financial transaction by dividing the amount for the purpose of avoiding the above amount and frequency of financial transactions
Subject of the transaction	A transaction in which a corporation or an organization is suspected of money laundering concern among financial customers

2-2 소셜 네트워크 분석

1) 소셜 네트워크

소셜 네트워크란 액터(actor)와 관계(relation)로 정의되는 구조(structure)를, 그리고 소셜 네트워크 분석은 이를 측정하고 분석하는 방법론을 가리킨다. 소셜 네트워크 분석은 구성원 간 관계의 관점에서 다양한 사회적 현상을 설명하려는 시도인데, 개별 구성원에 초점을 맞춘 기존 데이터 분석의 관점과는 다른 새로운 방법이라 할 수 있다. 소셜 네트워크 분석의 기본 단위는 노드(node)와 라인(line)으로 구성된다. 노드가 인간, 사물, 사건 등과 같은 행위자 즉 액터를 나타낸다면 라인은 행위자들 간 관계를 의미한다[7].

소셜 네트워크를 분석하기 위해서는 해당 데이터 포맷으로 가공하는 일이 필요하다. 소셜 네트워크 데이터를 표현하는 형식은 크게 소시오매트릭스와 엣지리스트로 구분된다. 우선 소시오매트릭스(sociomatix)는 노드 간의 관계 또는 방향성을 숫자 행렬을 사용하여 작성하는 방식으로, 그림 1의 a와 같이 표현된다. 소시오매트릭스의 각 행과 열은 동일하며, 각 노드가 맺은 관계의 수가 매트릭스에 기입된다. 엣지리스트(edgelist)는 각 노드가 맺은 관계에 대한 정보를 나열하는 방식으로, 그림 1의 b와 같이 표현된다. 이 방식은 데이터 입력 및 저장에 효율적이며 비교적 쉽게 데이터를 입력할 수 있다는 장점이 있는 반면 노드의 관계 구조가 직관적으로 드러나지 않을 뿐만 아니라, 관계가 없는 노드는 표현되지 않는다는 단점도 존재한다.



a. Sociomatrix b. Edgelist

그림 1. 소시오메트릭스와 엣지리스트[8]
Fig. 1. Sociomatrix & Edgelist[8]

2) 중심성

중심성(centrality)은 소셜 네트워크 분석에 필요한 가장 중요한 지표 중 하나이다. 통계학에서 평균이나 중앙값, 최빈값과 같이 데이터에서 대표성을 가지는 값들과 유사한 성격을 지닌다. 즉, 중심성 분석은 네트워크에서 연결의 핵심적 위치에 있는 특성을 수치값으로 표현하는 기법을 의미한다. 액터의 구조적 위치에 따른 중심성은 아래 세 가지 관점으로 측정된다.

연결중심성(degree centrality)은 가장 기본적인 네트워크 측정방법이다. 이는 한 액터가 다른 액터와 어느 정도 연결되어 있는지를 양적으로 측정하는 것을 말한다. 노드의 연결 정도는 그 노드가 나타내는 액터의 활동성(activity)를 나타낸다는 점에서, 액터의 중심성을 나타내는 중요한 지표 중 하나가 될 수 있다. 본 연구에서 연결중심성을 분석할 경우 자금세탁 의심거래에서 어떠한 거래방식이 중심을 이루고 있는지 파악할 수 있다.

$$C_D(N_i) = \sum_{j=1}^{g} x_{ij}, \ (i \neq j) \tag{1}$$

- $C_D(N_i)$: 액터 i의 액터 연결중심성
- g : 액터의 개수
- $\sum_{j=1}^{g} x_{ij}, \ (i \neq j)$: 액터 i가 (g-1)개의 다른 액터와 갖는 연결관계의 개수, x_{ij}= 0 또는 1

근접중심성(closeness centrality)은 네트워크 내에서 특정 노드가 다른 노드들과 얼마나 가까이 있는지에 대한 거리를 측정하는 것을 말한다. 다만 본 연구에서는 근접중심성은 분석하지 않는다. 자금세탁을 목적으로 하는 일련의 거래를 다루는 본 연구의 특성상, 개별 노드 간의 거리는 자금세탁 거래의 특징을 나타내는 지표가 될 수 없다고 봤기 때문이다.

$$C_c(N_i) = \frac{1}{\sum_{j=1}^{g} d(N_i, N_j)}, \ (i \neq j) \tag{2}$$

- $C_c(N_i)$: 액터 i의 액터 근접중심성
- g : 액터의 개수
- $\sum_{j=1}^{g} d(N_i, N_j)$: 액터 i와 액터 j간의 최단경로거리의 합

매개중심성(betweenness centrality)은 네트워크 내의 정보교환 또는 자원흐름을 중개하는 경로상 위치하는 정도를 측정하는 지표이다. 어느 한 점이 다른 두 개의 점 사이의 최단 경로에 놓이게 되는 비율을 합하여 측정한다. 본 연구에서 매개중심성을 분석할 경우 자금세탁 의심거래가 어떠한 경로로 이루어지고 있는지 파악할 수 있다.

$$C_B(N_i) = \sum_{j<k} \frac{g_{jk}(N_i)}{g_{jk}}, \ (i \neq j \neq k) \tag{3}$$

- $C_B(N_i)$: 액터 i의 액터 근접중심성
- g_{jk} : 두 액터 j와 k 간의 최단경로의 개수
- $g_{jk}(N_i)$: 액터 j와 k간의 최단경로 가운데 액터 i를 포함하고 있는 경로의 개수

3) 소시오그램

소셜 네트워크에서는 노드를 이용하여 액터를 표현하고 라인을 이용하여 관계를 나타낸다. 이러한 노드와 라인으로 이루어진 그래프를 소시오그램(sociogram)이라고 부른다[9]. 소시오그램은 소셜 네트워크 구조의 중요한 특징을 시각적으로 쉽게 확인할 수 있는 장점이 있다. 그 유형은 그림 2와 같다.

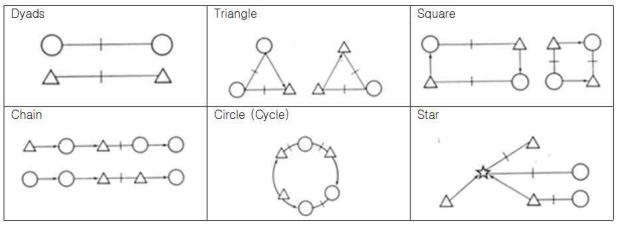


그림 2. 소시오그램의 구조[10]
Fig. 2. Construction of Sociogram[10]

2-3 선행 연구

소셜 네트워크 분석은 과거에는 사회현상 분석에 주로 사용되었으나 최근에는 다양한 거래 데이터로 그 대상이 확장되고 있다. 이에 따라 이러한 분석 기법을 이상징후 탐지에 적용하는 연구가 지속적으로 이루어지고 있다. 지금까지 자금세탁 의심거래 탐지를 위해 소셜 네트워크 분석을 적용할 필요성 및 효과성을 제시한 연구가 다수 진행되어왔다. 하지만 이들 연구는 실제 범죄 사례를 매개로 하여 분석을 수행하지 않았다는 한계가 있다. 반면 본 연구는 실제 발생한 자금세탁 범죄 사례에 대하여 소셜 네트워크 분석 과정을 제시하면서, 중심성과 구조적 특징을 도출하였다는 차별성을 지니고 있다.

선행연구를 살펴보면, Wi Choong Ki(2012)는 소셜 네트워크 분석기법을 금융사기에 적용함으로써, 대출 차주들 간의 연관성 분석을 통해 불법혐의 대출을 사전에 탐지할 수 있는 기법을 연구하였다. 불법대출이 대부분 제삼자 명의의 차명계좌를 이용하는 점에 착안하여, 대출 차주들 간의 연결고리 역할을 하는 연관성계수(특수 관계회사, 지급보증, 주요주주 등)를 추출하여 네트워크 분석을 수행하였다. 그 결과 중심성 지표를 통한 네트워크 분석의 효과성을 도출하였다[10].

Savage와 David(2016)는 네트워크 분석으로 금융거래의 패턴을 추출한 뒤 감독학습을 통해 자금세탁 의심거래를 사전에 식별할 수 있는 시스템을 설계하였다. 소셜 네트워크를 분석한 결과 호주거래보고센터(AUSTRAC; australian transaction reports and analysis centre)에 보고된 거래 데이터에서 커뮤니티 패턴을 추출할 수 있었다. 그런 다음 랜덤 포레스트와 SVM(support vector machine) 모델을 통한 감독학습을 수행하여 네트워크 분석의 효과성을 실증적으로 검증하였다[11].

Colladon 등(2017)은 팩토링 회사의 거래 데이터를 추출하여 네트워크 분석을 수행함으로써, 자금세탁을 방지할 수 있는 방안을 연구하였다. 이 연구에서는 많은 문헌이 자금세탁 문제를 다루고 있으나 불법거래에 사회적 행위자 간의 상호작용이 필요하다는 사실을 간과하는 문제를 제기하였다. 이에 따라 자금세탁 행위자의 개인적인 공헌에만 초점을 맞추기보다는 관계망을 고려한 네트워크 분석이 필요하다고 주장하였다. 연구 결과, 의심스러운 재무 운영이나 잠재적인 범죄자를 찾을 때 네트워크 분석 접근법이 효과적이라는 결론을 도출하였다[12].

Shaikh과 Abdul(2018)은 금융거래에서 자금세탁 의심거래를 사전에 식별하기 위한 접근법과 시스템 아키텍처, 작업 프로세스를 제시하였다. 이를 통해 의심스러운 특정 고객과 다른 고객 간의 네트워크 관계 분석(relational analysis)를 수행하기 위한 관계 규칙을 정의하였다. 하지만 실제 금융기관의 데이터를 통한 모델의 효과성 검증은 이루어지지 않았다[13].

Bodaghi 등(2018)은 자동차보험 전문사기를 식별하기 위하여 자동차 사고에 연루된 주체와 관련된 주변 개체(entity) 간의 관계를 분석한 뒤 네트워크 패턴을 추출하여 모델링하였다. 그 결과 노드가 3 이상($3 \geq n$)인 경우, 네트워크 관계 형태가 사이클(cycle)을 형성할 때 보험사기의 가능성이 높은 것으로 확인되었다[14].

Ⅲ. 연구 방법

3-1 연구 대상

FATF는 자금세탁의 경향 및 수법을 소개하는 보고서를 발간하여 웹사이트를 통해 민간에 공개하고 있다. 본 연구에서는 FATF에서 지금까지 공개한 내용 중 전자금융 환경에서 새로운 지불방식을 악용한 자금세탁 범죄를 유형별로 구분하여 검토하였다. 자금세탁 거래의 수법 및 패턴은 지불유형에 따라 달라지는 특징이 있다. 따라서 네트워크 분석을 수행할 경우, 다양한 지불유형에 따라 자금이 이동하는 경로를 알 수 있을 뿐만 아니라 결국엔 자금세탁 행위자에게 회귀한다는 점을 명확히 파악할 수 있다. 이러한 이유로 본 연구에서는 전신송금, 선불카드, 인터넷 결제, 전자화폐 등 네 가지 지불유형에 대한 자금세탁 범죄 사례를 연구 대상으로 선정하였다. 이 네 가지 지불유형은 전자금융 환경에서 가장 빈번하게 발생하는 대표적인 거래방식이다. 따라서 이를 제대로 파악할 경우 자금세탁 의심거래 방식의 대부분을 포괄할 수 있을 것으로 판단된다. 범죄 사례를 유형별로 제시해보면 표 2 와 같다.

3-2 연구 도구

소셜 네트워크 분석을 위한 전문 프로그램으로는 UCINET, Pajek, NetMiner, Social metrics, NodeXL 등을 들 수 있으며, 일반적으로 연구의 목적과 데이터 특징에 따라 적합한 프로그램을 선택하여 사용한다. 이중 UCINET는 현재까지 발전된 대부분의 소셜 네트워크 분석 이론에 대한 기능을 포함하고 있어서, 학술 연구에 많이 활용되는 장점이 있기에 본 연구에서는 UCINET을 이용하여 네트워크 분석을 수행하였다.

3-3 연구 절차 및 방법

본 연구는 자금세탁 거래정보에 대한 소셜 네트워크 분석을 위하여 ① 자료 수집, ② 자료 정제, ③ 자료 변환, ④ 네트워크 분석, ⑤ 결과 고찰 등의 단계로 진행하였다.

자료 수집(collection) 단계에서 소셜 네트워크 분석을 위한 고객의 금융거래 원천 데이터 수집이 이루어진다. 자금의 흐름을 추적하기 위해서는 일련의 거래 데이터가 필요하지만, 현재 금융거래 취급기관 간 고객의 거래정보를 공유하는 통합 모니터링 체계는 마련되어 있지 않은 실정이다. 따라서 본 연구에서는 이미 공개된 자금세탁 사례를 대상으로 자료를 수집하였다.

원천 데이터를 네트워크 데이터 형식으로 변환하기 위해 필요한 정보를 추출하고 데이터의 형식을 일치시키는 정제(cleansing) 작업을 수행하였다. 자금세탁은 단일한 행위가 아니라 배치, 반복, 통합 등의 3단계로 이루어진다[15]. 자금세탁 행위자는 자금의 출처나 소유자를 감추기 위해 각종 금융거래를 반복하여 추적을 어렵게 만들기 때문이다. 이러한 자금세탁 단계에 따라 거래행위를 표 2와 같이 구조화하였다.

표 2. 자금세탁 범죄사례 정제 결과
Table 2. Refinement results for cases of ML offenses

Cases	Steps	Contents
Case 1	Source of funds	Smuggling weapons and illegal sales through online (website)
	Placement	Receive Internet payment for three of his bank accounts
	Layering	Receive international telegraphic remittance or checks
	Integration	Cash Deposits and Capitalization
Case 2	Source of funds	Illegal proceeds from hacking crime
	Placement	Take out 61 card account information and transfer funds to the prepaid card
	Layering	Overdose tuition fees of university and claim refund
	Integration	Receiving a check back from the university
Case 3	Source of funds	Illegal proceeds from phishing
	Placement	Telegraphic remittance to agent account
	Layering	The agent withdraws the cash and buys the voucher online.
	Integration	Use voucher information for online payments and gambling
Case 4	Source of funds	Illegal proceeds from international crime
	Placement	Remittance to a member account through overseas telegraphic remittance
	Layering	The member purchases and sells the electronic money of the electronic money exchange and transfers it to the prepaid card account
	Integration	Offline payments and cash withdrawals using prepaid cards

자료 변환 단계에서는 행위자 간의 관계를 비교적 직관적으로 파악할 수 있는 소시오매트릭스 방식으로 데이터 변환(transform)을 수행하였으며 그 결과는 표 3~ 표 6과 같다.

표 3. Case1 사례에 대한 소시오매트릭스 구성
Table 3. Configure of source matrix for Case1 case

Money laundering activity	Out	W	D	D1	D2	D3	T	I	C
In	Node	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
Weapons trafficking revenue W	A_1	0	1	0	0	0	0	0	0
Defendant (Money laundering leader) D	A_2	0	0	1	1	1	0	0	0
Defendant account 1 D1	A_3	0	0	0	0	0	1	0	0
Defendant account 2 D2	A_4	0	0	0	0	0	1	0	0
Defendant account 3 D3	A_5	0	0	0	0	0	1	0	0
Telegraphic remittance T	A_6	0	1	0	0	0	0	0	0
Issuing checks I	A_7	0	1	0	0	0	0	0	0
Cash deposit C	A_8	0	1	0	0	0	0	0	0

표 4. Case2 사례에 대한 소시오매트릭스 구성
Table 4. Configure of source matrix for Case2 case

Money laundering activity	Out	I	D	P1	P2~ P60	P61	U	R	C
In	Node	B_1	B_2	B_3	B_4~ B_62	B_63	B_64	B_65	B_66
Illegal proceeds I	B_1	0	1	0	0	0	0	0	0
Defendant (Money laundering leader) D	B_2	0	0	1	1	1	0	0	0
Prepaid card account 1 P1	B_3	0	0	0	0	0	1	0	0
Prepaid card account 2~60 P2~60	B_4 ~B_62	0	0	0	0	0	1	0	0
Prepaid card account 61 P61	B_63	0	0	0	0	0	1	0	0
University tuition fee U	B_64	0	0	0	0	0	0	1	0
University tuition fee refund R	B_65	0	0	0	0	0	0	0	1
Issuing checks C	B_66	0	1	0	0	0	0	0	0

표 5. Case3 사례에 대한 소시오매트릭스 구성
Table 5. Configure of source matrix for Case3 case

Money laundering activity	Out	P	D	T	A	C	E	U
In	Node	C_1	C_2	C_3	C_4	C_5	C_6	C_7
Phishing revenues P	C_1	0	1	0	0	0	0	0
Defendant (Money laundering leader) D	C_2	0	0	1	0	0	0	0
Telegraphic remittance T	C_3	0	0	0	1	0	0	0
Agent account A	C_4	0	0	0	0	1	0	0
Cash withdrawal C	C_5	0	0	0	0	0	1	0
Electronic payment agency E	C_6	0	0	0	0	0	0	1
Use voucher U	C_7	0	1	0	0	0	0	0

표 6. Case4 사례에 대한 소시오매트릭스 구성
Table 6. Configure of source matrix for Case4 case

Money laundering activity	Out	C	D	T	O	E1	E2	P	U
In	Node	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8
Crime proceeds C	D_1	0	1	0	0	0	0	0	0
Defendant (Money laundering leader) D	D_2	0	0	1	0	0	0	0	0
Telegraphic remittance T	D_3	0	0	0	1	0	0	0	0
Overseas account O	D_4	0	0	0	0	1	0	0	0
E-money exchange E1	D_5	0	0	0	0	0	1	0	0
E-money transaction E2	D_6	0	0	0	0	0	0	1	0
Prepaid card charging P	D_7	0	0	0	0	0	0	0	1
Using prepaid cards and cashing U	D_8	0	1	0	0	0	0	0	0

Ⅳ. 연구 결과

4-1 분석 결과

1) 중심성 분석

본 연구에서는 연결중심성과 매개중심성의 관점에 의거하여 네트워크 분석을 수행하였다. 연결중심성을 통해서는 자금세탁 의심거래에서 어떠한 거래방식이 중심을 이루고 있는지 파악할 수 있다. 그리고 매개중심성을 통해서는 자금세탁 의심거래가 어떠한 경로로 이루어지고 있는지 파악할 수 있다.

UCINET 6 프로그램을 사용하여 연결중심성을 분석한 결과는 표 7과 같다.

표 7. 자금세탁 사례별 네트워크 연결중심성
Table 7. Network connection centrality by ML case

Cases	Node	Degree			Standardized		Network Centralization	
		Out Deg	In Deg	Total	Out Deg	In Deg	Out Deg	In Deg
Case 1	A_1	1.000	0.000	1.000	14.286	0.000	28.571%	44.898%
	A_2	3.000	4.000	7.000	42.857	57.143		
	A_3	1.000	1.000	2.000	14.286	14.286		
	A_4	1.000	1.000	2.000	14.286	14.286		
	A_5	1.000	1.000	2.000	14.286	14.286		
	A_6	1.000	3.000	4.000	14.286	42.857		
	A_7	1.000	0.000	1.000	14.286	0.000		
	A_8	1.000	0.000	1.000	14.286	0.000		
Case 2	B_1	1.000	0.000	1.000	1.538	0.000	92.308%	92.308%
	B_2	61.000	2.000	63.000	93.846	3.077		
	B_3	1.000	1.000	2.000	1.538	1.538		
	B_4~62	1.000	1.000	2.000	1.538	1.538		
	B_63	1.000	1.000	2.000	1.538	1.538		
	B_64	1.000	61.000	62.000	1.538	93.846		
	B_65	1.000	1.000	2.000	1.538	1.538		
	B_66	1.000	1.000	2.000	1.538	1.538		
Case 3	C_1	1.000	0.000	1.000	16.667	0.000	0.000%	19.444%
	C_2	1.000	2.000	3.000	16.667	33.333		
	C_3	1.000	1.000	2.000	16.667	16.667		
	C_4	1.000	1.000	2.000	16.667	16.667		
	C_5	1.000	1.000	2.000	16.667	16.667		
	C_6	1.000	1.000	2.000	16.667	16.667		
	C_7	1.000	1.000	2.000	16.667	16.667		
Case 4	D_1	1.000	0.000	1.000	14.286	0.000	0.000%	16.327%
	D_2	1.000	2.000	3.000	14.286	28.571		
	D_3	1.000	1.000	1.000	14.286	14.286		
	D_4	1.000	1.000	1.000	14.286	14.286		
	D_5	1.000	1.000	1.000	14.286	14.286		
	D_6	1.000	1.000	1.000	14.286	14.286		
	D_7	1.000	1.000	1.000	14.286	14.286		
	D_8	1.000	1.000	1.000	14.286	14.286		

Case1 분석 결과, 총 8개 노드 중 노드 A_2(Defendant)의 연결중심성이 가장 높게 나타났다. 총 연결 정도는 7로 가장 높았다. 표준화된 연결중심성은 외향연결 42.9, 내향연결 57.1로 가장 높았다. 반대로 연결중심성이 가장 낮은 노드는 '자금의 원천'에 해당하는 A_1(Weapons trafficking revenue)과 '자금세탁 통합 단계'에 해당하는 A_7(Issuing checks), A_8(Cash deposit)이었다. 각 노드의 총 연결 정도는 1이었으며 표준화된 연결중심성은 외향연결과 내향연결 모두 14.3으로 A_2의 지표값 대비 3배 가량 낮았다.

Case2 분석 결과, 총 66개 노드 중 노드 B_2(Defendant)의 연결중심성이 가장 높게 나타났다. 총 연결 정도는 63이었으며 표준화된 연결중심성은 외향연결 93.8, 내향연결 3.1로 외향연결이 압도적으로 높았다. 반대로 연결중심성이 가장 낮은 노드는 '자금의 원천'에 해당하는 B_1(Illegal proceeds)이었다. 총 연결 정도는 1이었으며 표준화된 연결중심성은 외향연결 1.54, 내향연결 0.0으로 B_2의 지표값 대비 60배 가량 낮았다.

Case3 분석 결과, 총 7개 노드 중 노드 C_2(Defendant)의 연결중심성이 가장 높게 나타났다. 총 연결 정도는 3이었으며 표준화된 연결중심성은 외향연결 16.7, 내향연결 33.3으로 외향연결이 압도적으로 높았다. 반대로 연결중심성이 가장 낮은 노드는 '자금의 원천'에 해당하는 C_1(Phishing revenues)이었다. 총 연결 정도는 1이었으며 표준화된 연결중심성은 외향연결 16.7, 내향연결 0.0으로 C_2의 지표값 대비 3배 가량 낮았다.

Case4 분석 결과, 총 8개 노드 중 노드 D_2(Defendant)의 연결중심성이 가장 높게 나타났다. 총 연결 정도는 3이었으며 표준화된 연결중심성은 외향연결 14.3, 내향연결 28.6으로 내향 연결이 압도적으로 높았다. 반대로 연결중심성이 가장 낮은 노드는 '자금의 원천'에 해당하는 D_1(Crime proceeds)이었다. 총 연결 정도는 1이었으며 표준화된 연결중심성은 외향연결 14.3, 내향연결 0.0으로 D_2의 지표값 대비 2배 가량 낮았다.

UCINET 6 프로그램을 사용하여 매개중심성을 분석한 결과는 표 8과 같다.

표 8. 자금세탁 사례별 네트워크 매개중심성
Table 8. Network betweenness centrality by ML cases

Cases	Node	Betweenness	nBetweenness	Network Centralization
Case 1	A_1	0	0	45.58%
	A_2	21	50	
	A_3	1.333	3.175	
	A_4	1.333	3.175	
	A_5	1.333	3.175	
	A_6	9	21.429	
	A_7	0	0	
	A_8	0	0	
Case 2	B_1	0	0	89.72%
	B_2	3910	93.99	
	B_3~62	0.148	0.004	
	B_63	0.148	0.004	
	B_64	3848	92.5	
	B_65	3847	92.476	
	B_66	3846	92.452	
Case 3	C_1	0	0	16.67%
	C_2	15	50	
	C_3	14	46.667	
	C_4	13	43.333	
	C_5	12	40	
	C_6	11	36.667	
	C_7	10	33.333	
Case 4	D_1	0	0	14.29%
	D_2	21	50	
	D_3	20	47.619	
	D_4	19	45.238	
	D_5	18	42.857	
	D_6	17	40.476	
	D_7	16	38.095	
	D_8	15	35.714	

Case1 분석 결과, 노드 A_2(Defendant)의 매개중심성은 21, 표준화값은 50으로 가장 높게 나타났다. 반면 '자금 원천'에 해당하는 노드 A_1 (Weapons trafficking revenue)과 '자금세탁 통합 단계'에 해당하는 노드 A_7(Issuing checks), A_8(Cash deposit)의 매개중심성은 0이었다.

Case2 분석 결과, 노드 B_2(Defendant)의 매개중심성은 3910, 표준화값은 93.9으로 가장 높게 나타났다. 반면 '자금 원천'에 해당하는 노드 B_1(Illegal proceeds)의 매개중심성은 0이었다.

Case3의 분석 결과, 노드 C_2(Defendant)의 매개중심성은 15, 표준화값은 50으로 가장 높게 나타났다. 반면 '자금 원천'에 해당하는 노드 C_1(Phishing revenues)의 매개중심성은 0이었다.

Case4의 분석 결과, 노드 D_2(Defendant)의 매개중심성은 21, 표준화값은 50으로 가장 높게 나타났다. 반면 '자금 원천'에 해당하는 노드 D_1(Crime proceeds)의 매개중심성은 0이었다.

2) 소시오그램 분석

네트워크 시각화 도구인 Netdraw를 이용하여 소시오그램을 제작하여 네트워크 구조를 분석한 결과는 그림 3 과 같다.

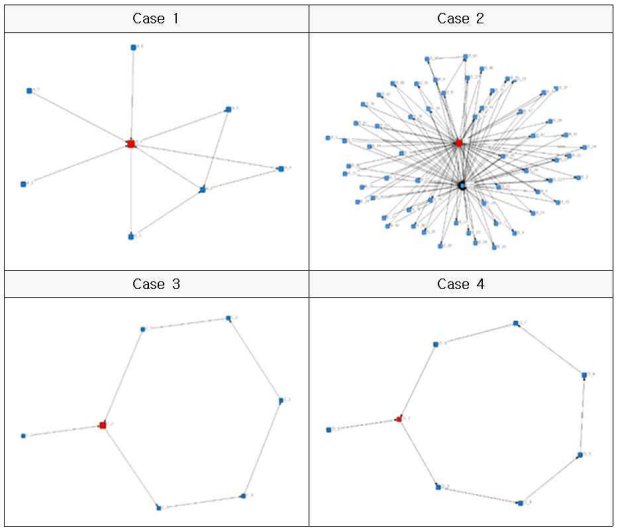


그림 3. 자금세탁 사례별 소시오그램
Fig. 3. Sociogram by ML case

Case 1의 경우, 노드 A_2(Defendant)가 가장 중심적 노드이며 빨간색으로 표현되어 있다. 노드 A_1, A_7, A_8의 링크는 노드 A_2를, 노드 A_2의 링크는 노드 A_3, A_4, A_5를 향하고 있다. 노드 A_3, A_4, A_5의 링크는 노드 A_6를 향하고 있으며, 노드 A_6의 링크는 A_2로 회귀하는 사이클(cycle)을 구성한다.

Case 2의 경우, 노드 B_2(Defendant)가 가장 중심적 노드이며 빨간색으로 표현되어 있다. 노드 B_3~63의 링크는 노드 B_64를 그리고 노드 B_64의 링크는 노드 B_65를 향하고 있다. 노드 B_65의 링크는 노드 B_66를 거쳐 노드 B_2로 회귀하는 사이클을 구성한다.

Case 3의 경우, 노드 C_2(Defendant)가 가장 중심적 노드이며 빨간색으로 표현되어 있다. 노드 C_2의 링크는 차례대로 C_3, C_4, C_5, C_6, C_7을 거쳐 C_2로 회귀하는 사이클을 구성한다.

Case 4의 경우, 노드 D_2(Defendant)가 가장 중심적 노드이며 빨간색으로 표현되어 있다. Case 4는 Case 3과 유사한 구조를 가진다. 즉 노드 D_2의 링크는 차례대로 D_3, D_4, D_5, D_6, D_7, D_8을 거쳐 D_2로 회귀하는 사이클을 구성한다.

Ⅴ. 결 론

본 연구에서는 소셜 네트워크 분석 기법에 기반하여 전자금융 환경에서 발생한 자금세탁 의심거래 정보를 거래 유형별로 살펴보고 연결중심성과 매개중심성 등 중심성과 소시오그램을 통해 네트워크 구조를 분석하였으며, 분석 결과를 정리하면 다음과 같다. 첫째, 연결중심성의 분석 결과 '자금세탁 행위자'에 해당하는 노드의 연결중심성은 가장 높은 반면, '자금의 원천'에 해당하는 노드의 연결중심성은 가장 낮게 나타났다. 이러한 결과는 '자금세탁 행위자'를 중심으로 자금세탁 의심거래 행위가 이루어지고 있을 뿐만 아니라, '자금의 원천'이 거래행위 과정에서 큰 역할을 하지 못하고 있음을 나타낸다. 둘째, 매개중심성의 분석 결과 '자금세탁 행위자'에 해당하는 노드의 매개중심성은 가장 높은 반면, '자금의 원천'에 해당하는 노드의 매개중심성은 0으로 나타났다. 이러한 결과는 '자금세탁 행위자'가 자금세탁 의심거래 행위의 중심을 차지하고 있음을 의미한다. 셋째, 소시오그램의 분석 결과 '자금세탁 행위자'를 중심으로 하는 사이클이 형성되었다. 이는 세탁된 자금이 궁극적으로는 자금세탁 행위자에게로 수렴됨으로써, '자금세탁 행위자'가 자금의 실제 소유자라는 사실을 증명해준다. 결론적으로 자금세탁 거래 네트워크는 '자금세탁 행위자'를 중심으로 자금세탁 의심거래 행위가 이루어지며, 세탁된 자금은 거래반복 단계를 거쳐 '자금세탁 행위자'에게 최종 수렴되고 있다고 할 수 있다.

본 연구에서 활용한 소셜 네트워크 분석 기법은 자금세탁 행위자를 중심으로 하는 연결관계를 기준으로 해당 판단을 수행한다는 점에서, 금융거래의 종류 또는 특정 패턴에 한정적이지 않다는 장점이 있다. 특히 자금세탁 거래의 경우 복잡도가 높을수록 해당 거래를 탐지하기 어렵고 비용과 시간이 많이 소요되는 문제가 있지만 소셜 네트워크 분석의 경우 네트워크 노드의 수와 중심성 지표가 비례하기 때문에, 거래의 복잡도가 높을수록 자금세탁 행위자와 거래의 특징을 더 잘 추출할 수 있는 장점이 있다. 따라서 '자금세탁 행위자'를 중심으로 하는 네트워크의 유의성을 확인하였다는 데 본 연구의 의의가 있다고 할 수 있으며, 제안한 기법은 복잡한 전자금융 환경에서 자금세탁 거래를 식별하기 위한 효과적인 방법의 하나로 고려할 가치가 있다고 판단된다.

참고문헌

[1] I. H. Kang, C. H. Yoon, "A study on the incentive for money laundering prevention effort," *Journal of Economics and Business*, vol. 11, pp. 1-19, Dec. 2006.

[2] The Korea Financial Intelligence Unit (KoFIU)[Internet], Available: www.kofiu.go.kr

[3] FATF, The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Financial Action Task Force, 2018.

[4] H. J. Lee, "Suspicious transaction report and currency yransaction report as anti-money laundering systems,", *Administrative Law Journal*, vol. 16, pp. 23-53, Oct 2006.

[5] K. S. Shin, H. J. Kim, and H. S. Kim, "Development of the knowledge-based systems for anti-money laundering in the Korea Financial Intelligence Unit," *Journal of Intelligence and Information Systems*, vol. 14, no. 2, pp. 179-192, 2008.

[6] Financial Services Commission (FSC), Anti Money Laundering Guidelines for Virtual Currency, Seoul; Financial Services Commission, Jan. 2018.

[7] W. Zachary "An information flow model for conflict and fission in small groups," *Journal of Anthropological Research*, vol. 33, no. 4, pp. 452–473, 1977.

[8] Social Network Analysis[Internet].(2019, Jan 15) Available: http://www.mjdenny.com/workshops/SN_Theory_I.pdf

[9] C. Hollander, *An Introduction to Sociogram Construction*, Snow Lion Press, 1978.

[10] C. K. Wi, H. J. Kim, and S. J. Lee, "A study on detection technique of anomaly signal for financial loan fraud based on social network analysis," *Journal of the Korea Institute of Information Security*, vol. 22, no. 4, pp. 851-868, Aug. 2012.

[11] D. Savage, Q. Wang, P. Chou, X. Zhang, and X. Yu, "Detection of money laundering groups using supervised learning in networks," arXiv, Aug 2016.

[12] Colladon, Andrea Fronzetti, and Elisa Remondi, "Using social network analysis to prevent money laundering," *Expert Systems with Applications*, vol. 67, pp. 49-58, 2017.

[13] A. Shaikh and A. Nazir, "A model for identifying relationships of suspicious customers in money laundering using social network functions," *Proceedings of the World Congress on Engineering*, vol. 1, pp. 141-144, 2018.

[14] A. Bodaghi and B. Teimourpour, "The detection of professional fraud in automobile insurance using social network analysis," arXiv:1805.09741, 2018.

[15] KoFIU, The case study for authoritative interpretation of anti-money laundering system, KoFIU, pp. 11-12, 2018.

서정원(Jeong-Won Seo)

2011년: 인하대학교 공간정보공학 학사
2019년: 고려대학교 정보보호대학원 빅데이터응용 및 보안학과 (공학석사)

2011년～2011년: ㈜네이버 비즈니스 플랫폼
2012년～2014년: ㈜코스콤
2014년～현 재: 딜로이트 안진회계법인

※관심분야 : 빅데이터분석, 머신러닝, 리걸테크, IT감사 등

김형중(Hyung-Joong Kim)

1978년: 서울대학교 전기공학과 학사
1986년: 서울대학교 제어계측공학과 (공학석사)
1989년: 서울대학교 제어계측공학과 (공학박사)

1989년～2006년: 강원대학교 교수
2006년～현 재: 고려대학교 정보보호대학원 교수

※관심분야 : 컴퓨터보안, 패턴인식, 가역정보은닉, 머신러닝, 빅데이터분석 등