Journal of the Korea Convergence Society
Vol. 8. No. 4, pp. 19-24, 2017
https://doi.org/10.15207/JKCS.2017.8.4.019

빅데이터 기술을 활용한 이상금융거래 탐지시스템 구축 연구

강재구[1], 이지연[2], 유연우[3*]
[1,2]한성대학교 일반대학원 스마트융합컨설팅학과 박사과정, [3]한성대학교 지식서비스&컨설팅학과 교수

A Study on Implementation of Fraud Detection System (FDS) Applying BigData Platform

Jae-Goo Kang[1], Ji-Yean Lee[2], Yen-Yoo You[3*]
[1,2]Candidate of Ph.D., Dept. of Smart Convergence Consulting, Hansung University
[3]Professor, Dept. of Knowledge Service & Consulting, Hansung University

요 약 본 연구는 최근 전자 금융거래의 증가와 동시에 금융거래 정보의 탈취 혹은 변조 등 보안위협 또한 급증하면서 안전한 보안 방안과 대응이 시급한 실정이다. 이에 종래에 사용된 사기방지시스템 혹은 이상금융거래 탐지시스템(FDS, Fraud Detection System, 이하 FDS)을 최근 주목 받고 있는 빅데이터 관련 기술(이상금융거래에 대한 다양한 형태의 정형/비정형 금융거래 이벤트 데이터를 실시간으로 수집/저장하고 과학적 연관 분석 기법을 활용하여 비정상 행위를 탐지 및 차단할 수 있는 기능)을 활용하여 국내 금융회사인 A사에 개선 모델을 구축 하였다. 구축결과 시나리오 고도화 분석을 통한 오검출을 최소화 하여 기존 시나리오 Detect탐지 대상의 감소 효과를 나타냈다. 아울러 FDS고도화에 대한 향후 발전방향을 제안하고자 한다.

• **주제어** : 이상금융거래 탐지시스템, 빅데이터, 전자금융, 금융IT 융합, 금융보안, FDS.

Abstract The growing number of electronic financial transactions (e-banking) has entailed the rapid increase in security threats such as extortion and falsification of financial transaction data. Against such background, rigid security and countermeasures to hedge against such problems have risen as urgent tasks. Thus, this study aims to implement an improved case model by applying the Fraud Detection System (hereinafter, FDS) in a financial corporation 'A' using big data technique (e.g. the function to collect/store various types of typical/atypical financial transaction event data in real time regarding the external intrusion, outflow of internal data, and fraud financial transactions). As a result, There was reduction effect in terms of previous scenario detection target by minimizing false alarm via advanced scenario analysis. And further suggest the future direction of the enhanced FDS.

• **Key Words** : FDS(Fraud Detection System), Bigdata, E-Banking, Financial IT Convergence, Financial Security.

*Corresponding Author : 유연우(threey0818@hansung.ac.kr)
Received February 16, 2017 Revised March 22, 2017
Accepted April 20, 2017 Published April 28, 2017

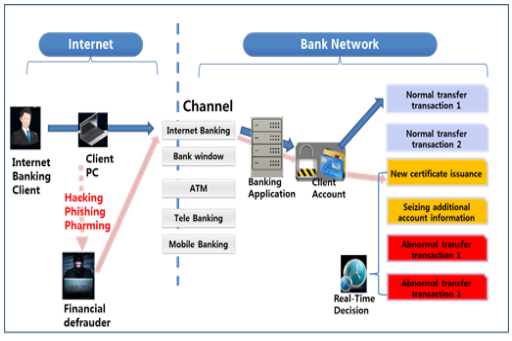
1. 서론

금융거래에 있어서 비정상적인 행위를 탐지하여 금융사고를 예방하고자 하는 기술적 접근이 이상금융거래 탐지시스템(FDS, Fraud Detection System)이라고 일컫는다. 이러한 FDS시스템은 실시간으로 단말기(PC, 모바일 등) 정보와 거래내용, 이용자 유형 등 이용자의 데이터 및 결제 데이터를 종합적으로 분석 후 평소 거래패턴 데이터와 다른 거래임을 탐지하여 이상 징후를 파악하고 금융기관과 이용자에게 탐지 사실을 알리고 더 나아가 임의로 거래를 중단시키는데 활용된다[1,2,3].

전 세계적으로 1990년대 중반부터 FDS시스템을 구축하기 시작 하였고 국내에서는 2000년대 초기부터 신용카드사들이 구축하기 시작하여 비대면 거래가 많은 은행, 보험사, 증권사 중심으로 FDS를 구축하고 있다[4].

최근에는 금융 산업과 정보기술의 발달에 따라 두 기술을 융합한 다양한 형태의 비대면 거래가 증가하고 있다[1.4].

이상과 같이 전자 금융거래가 확산되어 감에 따라서 이를 노리고 사용자들의 금융거래 정보나 현금을 탈취하는 등의 이상금융거래유형[Fig. 1]의 형성과 각종 금융보안 관련된 사고가 발생하였다[5].



[Fig. 1] Abnormal Financial transaction Flow Chart

이상금융거래의 유형 및 증가에 대해 살펴보면 2002년에 현금, 신용카드 위조 및 복제를 통한 현금인출 사고가 발생하고 2003년에 웜(Worm)에 의한 인터넷 네트워크 마비 및 전자금융서비스 중단 사고가 사회적 이슈화 되었다. 2005년에는 악성프로그램을 이용한 최초의 인터넷뱅킹 사고가 사회적 이슈가 되었다[6]. 2006년 이후에는 단순히 악성 프로그램을 이용한 인터넷뱅킹 사고를 넘어 공인인증서나 자금을 노리는 여러 해킹사고로 발전하였다. 그 예로 대출사기, 인터넷 피싱, 파밍, 메모리해킹 등의 신종 전자금융 사기행위가 대폭 증가하였으며 정부역시 전자금융사고 발생이후 지속적인 대응을 하고 있으나 공격자가 공격의 방식을 바꾸면 쉽게 우회가 가능하기에 최근에는 여러 가지 우회 수법들이 등장하고 있다[7].

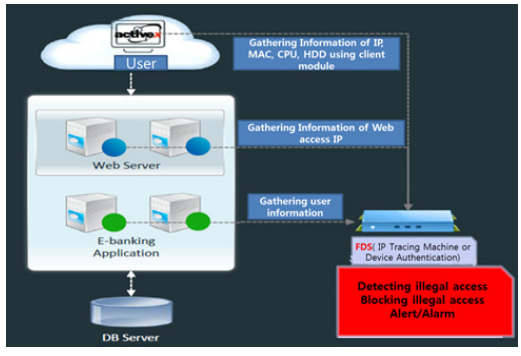
따라서 이상과 같이 인터넷, 스마트폰뱅킹 및 텔레뱅킹을 이용한 이상전자금융사고 발생이 높아지면서 이를 사전에 적발하는 FDS구축이 금융권 전반으로 확산되고 있으며 스마트기기 및 인터넷보급이 확산되고 이에 대한 위협이 증가함에 따라 전자금융거래에 대한 안전성 강화를 위해 FDS의 고도화 및 확대도입이 필요해 지고 있다[8].

본 연구에서는 기존의 FDS시스템이 가지고 있는 한계를 극복하고 고도화 하고자 최근 주목받고 있는 빅데이터 기술을 활용한 FDS구축 모델을 제시하고 향후 발전방향에 대하여 제안하고자 한다.

2. 기존 현황 및 대응방안

2.1 기존 구축 시스템의 형황 및 문제점

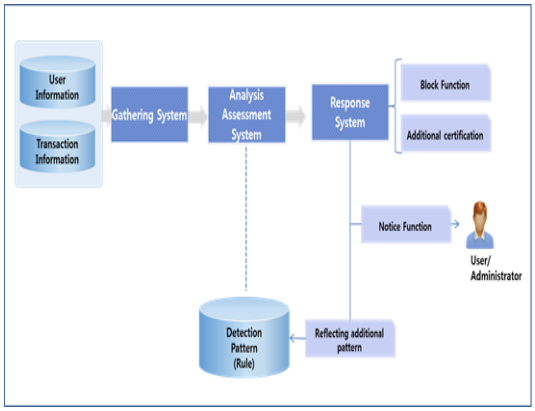
기존에 구축된 이상금융거래 탐지시스템(FDS)의 경우 IP추적기 혹은 디바이스 인증을 통하여 부정접속의 탐지 혹은 차단하고 경고나 알림 기능을 부여하는 시스템이 대다수 이었다[Fig. 2]. 이는 웹과 사용자의 특정 플랫폼에 치우친 기술방식의 사용에 따른 한계가 존재하고 단말기 정보나 Context정보, 거래내용 등을 종합적으로 분석하지 못하였으며 단말정보 수집의 종류 및 방식의 한계에 따른 유일성 확보와 사기방지에 문제가 있었다. 또한 수집, 탐지, 분석, 대응, 관리, 운영, 감사 기능이 통합되지 못하고 개별구축에 따른 문제점을 보여 왔다[5].



[Fig. 2] Existing FDS system

2.2 정부의 가이드라인

이상의 문제점들을 개선하고 이상금융거래 탐지의 효과성을 향상하기 위하여 한국의 경우 [금융보안연구원]에서 2014년도에 '이상금융거래 탐지시스템 기술 가이드'를 발표하였고 이 가이드에 따르면 이상금융거래 탐지시스템은 다양하게 수집된 정보를 종합적으로 분석하여 이상금융거래 유무를 판별하는 복합적인 시스템으로 크게 정보수집기능, 분석 및 탐지 기능, 대응기능, 모니터링 및 감사 기능의 4가지 기능으로 이루어 져야 하며 각 기능은 상호 호환 또는 연동되어 구성되도록 제안하고 있다[9]. 이 가이드에 따라 현재 대부분의 FDS구축이 이루어지는 추세이며 가이드에서 제시하는 세부적인 구조는 아래 [Figure 3]의 그림과 같다.



[Fig. 3] FDS Structure & Main function of FDS

또한 이 가이드에서 제시하는 주요 기능은 아래와 같다.

① 정보수집기능 : 이상금융거래 탐지의 정확성을 위해 크게 '이용자 매체환경 정보'와'사고 유형 정보'의 수집 기능

② 분석 및 탐지기능 : 수집된 정보는 이용자 유형별, 거래유형별 다양한 상관관계 분석 및 규칙 검사 등을 통해 이상행위를 탐지하는 기능

③ 대응기능 : 분석된 이상 금융거래 행위에 대한 거래 차단 등의 대응 기능

④ 모니터링 및 감사기능 : 수집, 분석, 대응 등의 종합적인 절차를 통합하여 관리하는 모니터링 기능과 해당 탐지 시스템을 침해하는 다양한 유형에 대한 감시기능

상기 언급한 4가지 기능이 금융거래에 개입되어 상호 연동되어져야 하고 전체시스템이 안정성과 효율성을 가져야 한다. 이상의 기능을 요약하면 아래 <Table 1>와 같다[9,10].

〈Table 1〉 Summary of FDS Main Function

Category	Function
Gathering Information	Gathering information of user media environment
	Gathering information of accident types
Analysis & Detection	Correlation analysis of gathering information ; user types, transaction types
	Fraud detection through rules prosecutors
Response	Response function of detected abnormal financial transactions.
Monitoring & auditing	Total monitoring management of gathering, analysis, detection, response functions
	Various audit function for penetrating FDS
Interworking between internal components	
Interworking with legacy systems.	
Stability & Performance of total system.	

2.3 개선 모델

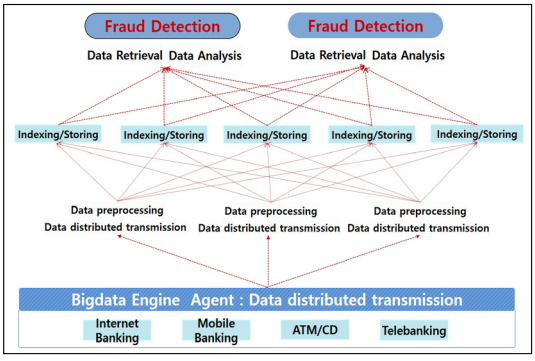
2.1, 2.2항에서 에서 명기한 기존 FDS 에 내재한 문제점 및 '이상금융거래 탐지시스템 기술 가이드'의 시스템 구성에 관한 권고안을 참고해 볼 때 FDS시스템을 구축하는데 있어 가장 중점을 두어야 할 부분은 데이터 수집 측면에서 데이터의 수집과 통합적인 FDS 운영을 위해 다양한 채널, 즉 ATM, 모바일 뱅킹, 그리고 인터넷 뱅킹 등의 다양한 채널 금융거래에서 사기행위 탐지를 위한 마스터 데이터를 구축하고, 데이터를 분류하고, 수집하여 활용하는 사기행위 데이터베이스 모델을 정의해야 한다. 또한, 데이터의 분석 측면에서 단기간 대응을 위한 사기행위 탐지 룰 분석과 장기적인 대응을 위한 모델링으로 구분할 수 있다. 사기행위 탐지룰은 모델에서 사기행위라고 인지하기 어려운 새로운 형태의 사기행위 패턴이 발생되거나 신용카드 또는 계좌 정보의 유출에 의해 피해가 예상될 때 활용 될 수 있다.[4]

결론적으로 FDS구축 시의 가장 큰 리스크 고려요인은 데이터 수집 후 분석에 의한 미탐지(FDS내 정상거래로 탐지했으나 실제 금융사기 거래에 해당하는 경우)와 과오탐지(FDS내 이상거래로 탐지했으나 실제 정상거래인 경우)를 최소화하는 것이며 이를 달성하기 위하여 시나리오 기반 탐지를 보완하는 탐지방식이나 시나리오 기

반 탐지에 대한 추가 분석이 필요하다.

3. 구축사례

이상과 같이 FDS의 고도화 및 기존 FDS문제점을 개선하기 위하여 '이상금융거래 탐지시스템 기술 가이드'의 권고안에 준용하여 한국의 IT서비스 회사인 T사는 빅데이터 엔진을 기반으로 외부침해, 내부정보유출, 이상금융거래에 대한 다양한 형태의 정형 및 비정형 금융거래 이벤트 데이터를 실시간으로 수집 및 저장하고 과학적인 연관 분석 기법을 활용하여 비정상 행위를 탐지 및 차단할 수 있는 기능을 구현하였다.



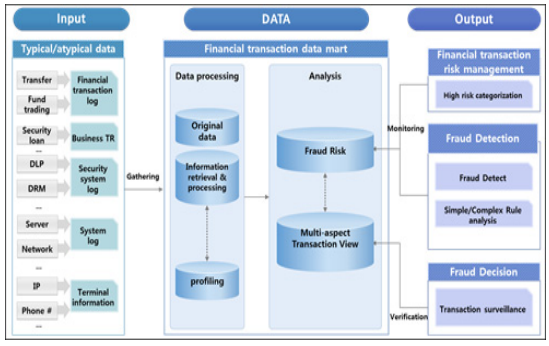
[Fig. 4] Real-time distributed processing structures, Bigdata.

금융사기 행위 징후를 분석하기 위해서는 일 수GB이상의 대용량 로그 및 데이터의 실시간 수집 및 장기간에 걸친 원본 거래 데이터의 수집을 기반으로 시계열, 실시간 분석이 필요하며 금융거래 이상 징후 사전예측 및 이상금융거래 실시간 탐지, 대응이 필요하다. 아울러 금융사기행위 탐지율을 높이기 위해서는 전체 고객 거래 데이터를 대상으로 비정상 금융거래 행위 분석, 위험도 산출 기준 정교화를 통한 이상금융거래 탐지율 고도화 등 다양한 측면의 과학적 분석 기법적용이 필요하다. 또한 업무 로그와 트랜잭션 로그의 증가 및 변경 시 데이터 처리에 대한 신속하고 유연한 대응 체계가 필수적 일 것이다.

이상의 요구 사항을 충족하기 수집/저장 성능을 확보하고 CEP(Complex Event Processing) 엔진에 기반을 둔 병렬/분산 처리를 통해 실시간 분석 성능을 보장하고 수집서버와 관리 서버를 분리하여 Scale out 방식의 유연한 확장이 가능한 빅데이터 처리기술이 유용하다고 할 수 있을 것이다[11].

본 연구에서는 위의 [Fig. 4]에서와 같이 다양한 채널에서 발생하는 다양한 데이터에 대한 수집 및 처리체계를 분산 구조화 하여 데이터 병목구간을 제거하였다. 이러한 구조는 빅데이터에서 검증된 구조로서 대용량 서버 내에서 처리되는 것과 동일한 성능을 보장한다. 또한, 각 구간별 특정 서버의 장애가 전체 시스템의 기능과 성능에 미치는 영향을 최소화한 구조라고 할 수 있다.

실제 T사는 이상의 기능을 구현한 플랫폼을 활용하여 한국의 A금융사에 FDS를 구축하였으며 이를 통해 다양한 형태의 업무 로그를 수집하여 빅데이터 분석 마트를 구축한 후 고급분석을 통해 이상거래 위험군의 분류 및 거래 이상 징후를 탐지하고 이상거래 판정 업무를 지원하였다. 본 구축 시스템의 논리적인 구성도는 [Fig. 5]와 같다.



[Fig. 5] Logical conceptual diagram of FDS Application ('A' Financial corporation)

이를 통해 대용량 데이터 저장소 및 분석 인프라 및 분산 병렬처리 프로세스를 통한 장기 데이터 분석환경을 구축 하였으며 빅데이터 분석 기술을 활용한 FDS 고도화를 구현 하였다.

4. 구축결과

구축결과 비대면 채널 이용자별 거래현황 및 탐지현황 등 다양한 현황분석 및 통계정보 보고서를 제공하도록 구현 하였으며 이 경우 빅데이터 엔진에 오픈소스 'R' 분석 도구를 연계하여 활용하였다. R시스템의 경우 빅데이터 분석관련 에코시스템에서 실시간/비실시간 분석 아

키텍처에 통계를 통한 시각화를 위하여 별도의 프로그래밍을 통해 구현될 수 있는 오픈소스 솔루션이다[11]. 다만 한계점으로 별도의 프로그램 능력이 요구되는 도구이므로 경량화 되고 쉽게 사용이 가능한 라이브러리 구축이 필요하다. 본 연구에서도 이상의 한계점을 고려하여 구현하였으며 'R'을 통해 상용 고급 솔루션을 대체하여 초기 도입비용을 절감하였다.

또한 본 연구를 통해 기존 시스템 대비 구축된 빅데이터 기술을 활용한 분석 주체를 크게 시나리오 고도화, 과거 패턴 유사도 분석, 사고사례 기반 매칭분석, 계좌 네트워크 분석 등으로 구분할 수 있다.

첫 번째 시나리오 고도화 분석을 통한 False Alarm (과다탐지, 오탐)을 최소화 하여 테스트 운영 결과 기존 시나리오 Detect탐지 대상의 약 40%의 감소 효과를 나타냈다. 시나리오 고도화 분석의 구축 배경은 과거 이상금융거래 사례를 기반으로 만들어진 시나리오 내 변수의 임계점이 변수의 전체분포를 반영하지 않기 때문에 데이터 정탐율을 높이기 위하여(즉, 과다탐지를 방지하기 위하여) 변수의 전체분포 또는 변수간의 상관관계를 파악하여 시나리오 임계값의 타당성을 판단할 수 있는 근거자료(데이터 기반 분석을 통한 결과)를 생성하였다.

두 번째 과거 패턴유사도 검색을 통해 사용자별 접속 단말기, 사용자 변경정보, 이체정보의 과거패턴과 현재패턴을 비교하여 과거 패턴대비 현재패턴이 매우 변화된 사용자를 탐지할 수 있도록 구축하였다.

세 번째로는 과거 금융사고 사용자의 패턴을 중심으로 유사한 사용자를 조사하거나 금융사고 사례중심으로 유사한 패턴을 분석하였다.

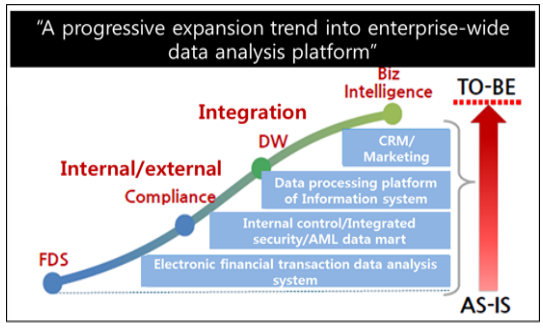
네 번째로는 계좌 네트워크 분석으로 계좌와 계좌간의 관계에서 이체의 흐름에 중심에 있는 계좌를 탐지하는 등 사회관계망(SNA Visualization) 분석을 통해 정량적 파악이 어려운 신규패턴을 도출 하였다.

5. 향후 제안

향후에도 핀테크(Fin-Tech)의 지속적인 보급과 급속히 성장함에 따라서 다양한 비대면 채널을 통한 전자금융의 비율은 더욱 증가할 것으로 전망되며 이면에는 다양한 형태의 보안에 대한 위협이 발생할 것이다. 따라서 이상금융거래에 대응한 진화된 FDS에 관련한 필요할 것으로 예측되며 데이터 분석, 보안과 관련된 기업들도 새로운 기회로 받아들이고 대비하는 자세가 필요할 것으로 보인다[12].

본 연구를 통해서 빅데이터 기술과 일반적인 실시간 예측 분석 기술인 CEP(Complex Event Processing) 엔진에 기반 하여 데이터의 수집. 저장.파싱. 인덱싱. 분석/보고 등의 기능을 수행하였다. 향후에도 이상과 같은 'Data-Driven 기술'의 향상과 "고급 분석 역량"을 통한 FDS고도화가 필요할 것이다. 최근에는 실제 일부 금융권에서 선도적으로 인공지능(AI) 딥러닝 기술을 적용한 FDS를 도입 및 도입을 예정 하는 등 FDS 고도화를 위하여 노력을 진행하고 있다[13,14,15].

이러한 신기술을 FDS에 융합 시키는 것을 물론이고 아울러 이상의 기능이 독자적으로 수행되는 것이 아닌 내부/외부 컴플라이언스 대응과 통합 DW를 넘어 전사 데이터분석 플랫폼[Fig 6]으로 점진적으로 확장 시켜 나갈 것을 제안한다.



[Fig. 6] Roadmap proposal for future FDS

REFERENCES

[1] S. H. Jeong, H. N. Kim, Y. S. Shin, T. J. Lee, H. K. Kim. "A Survey of Fraud Detection Research based on Transaction Analysis and Data Mining Technique", J. of the Korea Institute of Information Security and Cryptology, Vol. 25, No. 6, pp. 1525-1539, 2015.

[2] http://blog.skinfosec.com/220714943937

[3] http://skypotato-note.tistory.com/21

[4] T. E. Kim, J. M. Lee, S. H. Hwang, G. Y. Gim. "A Study of Finance Fraud Detection System Operation Framework", Asia-pacific J. of Multimedia Services

Convergent with Art, Humanities, and Sociology, Vol. 5, No. 4, pp. 9-17, 2015.
[5] http://blogattach.naver.net/ff6ae356407475c2e50b6d5d6584fa8126748fd4/20150408_47_blogfile/netni_1428478980994_H8zAiv_pdf/141127-ca-sec-seminar-presentation-deck-02.pdf?type=attachment
[6] S. D. Yoo, K. D. Choi, "A meta-analysis survey of the research on domestic e-banking", Journal of digital Convergence, Vol. 13, No. 4, pp. 175-189, 2015.
[7] E. Y. Park, J. W. Yoon, "A Study of Accident Prevention Effect through Anomaly Analysis in E-Banking", The J. of Society for e-Business Studies, Vol. 19, No. 4, pp. 119-134, 2014.
[8] http://blog.daum.net/prkisdi/3256
[9] "Fraud Detection System Technical Guide", Financial Security Institute, Republic of Korea, 2014.
[10] https://www.kisdi.re.kr/kisdi/fp/kr/publication/selectResearch.do?cmd=fpSelectResearch&curPage=1&sMenuType=3&controlNoSer=13&controlNo=13733&langdiv=1&searchKey=TITLE&searchValue=국내금융권의&sSDate=&sEDate=
[11] S. J. Lee, D. H. Lee, "Real time predictive analytic system design and implementation using Bigdata-log, J. of the Korea Institute of Information Security and Cryptology, Vol. 25, No.6, pp. 1399-1410, 2015.
[12] S. H. Lee, D. W. Lee, "FinTech - Conversions of Finance Industry based on ICT", Journal of the Korea Convergence Society, Vol. 6, No. 3, pp. 97-102, 2015.
[13] http://www.dt.co.kr/contents.html?article_no=2017021702109958032001
[14] http://www.dt.co.kr/contents.html?article_no=2017020702100658032001
[15] http://www.dt.co.kr/contents.html?article_no=2017012502100558032002

저자소개

강 재 구(Jae-Goo Kang) [정회원]

- 2015년 9월 ~ 현재 : 한성대학교 일반대학원 스마트융합컨설팅학과 박사과정
- 2012년 6월 ~ 현재 : 'T' 社 차장
- CISA, PMP, ITIL, SCJP
- 경영지도사, ISO9001/14001심사원보, 기술신용평가사 2급(정보통신)

<관심분야> : ICT융합, 신사업 기획/발굴, M&A, R&D기획, 기업회생

이 지 연(Ji-Yean Lee) [정회원]

- 2015년 9월 ~ 현재 : 한성대학교 일반대학원 스마트융합컨설팅학과 박사과정
- 2008년 12월 ~ 현재 : 'T' 社 부장

<관심분야> : 전략기획, 매니지먼트, ICT융합, 신사업 기획/발굴, BPO

유 연 우(Yen-Woo You) [정회원]

- 2002년 2월~2008년 4월 : 중소기업기술정보진흥원(컨설팅, 경영/기술혁신, CSR, IT, R&D기획, 기술사업화)
- 2008년 9월 ~ 현재 : 한성대학교 지식서비스&컨설팅학과 교수, 스마트 융합컨설팅학과 교수, 한성대학교 지식서비스&컨설팅연구원 원장
- 2011년 1월 ~ 현재 : 소상공인진흥원 신사업 발굴 및 평가 운영위원
- 2011년 11월 ~ 현재 : 제주관광공사 성과평가 위원

<관심분야> : Consulting(Strategy, PM, 성과평가, MOT), CSR, Technology Innovation, Management Innovation, Service R&D, Franchise, 1인창조기업, 지식재산, ICT융합, 정책, 기술사업화, R&D기획