IDG
INTERNATIONAL DATA GROUP

IT WORLD CIO

IDG Summary

“진화하는 금융사기, 어떻게 막을 것인가”

금융사기가 개인화, 지능화, 조직화되며 점점 진화하고 있으며 금융기업들은 사기 거래들을 찾아내고자 전담 인력을 배치하고 사기방지 솔루션(Fraud Detection Solution, 이하 FDS)을 도입해 왔다. 금융사기를 100% 막을 수는 없지만, 사고 후 어떻게 대처하고 미래 사고의 개연성을 얼마나 막을 수 있느냐가 금융기업에겐 관건이다. 가장 빠르게 움직이는 기업들은 카드사, 보험사 등이며 점차 정부 기관, 통신사, 제조사 등도 FDS에 관심을 보이고 있다. 금융기업의 사기 적발 프로세스는 세관이나 세무의 허위 신고, 정부 지원금의 허위 청구를 찾아내는 것과 흡사하기 때문이다.

- 개인화 · 지능화 · 조직화되는 금융사기
- 사기탐지의 3요소 분석 · 시스템 · 사람
- 쉽고 빠른 분석 환경, 모델 자동 추천 기능, 개방성
- 금융 이외 타 산업으로 확산 적용 가능

Sponsored by
IBM

"진화하는 금융사기, 어떻게 막을 것인가"

김지관 | 한국IBM

금융사기가 진화하고 있다. 이러한 사고를 100% 막을 수 있는 솔루션이란 없다. 중요한 것은 사고가 발생했을 때 얼마나 신속하게 대처하고 이와 같은 사고가 반복해서 일어나지 않도록 조치를 취하느냐다.

개인화 · 지능화 · 조직화되는 금융사기

IT인프라가 매우 발달함에 따라 국내외를 가리지 않고 피싱, 파밍, 스미싱 등이 발생하고 있다. 이러한 금융사기는 개인화되고 지능화됐으며 조직화됐다는 것이 특징이다. 심지어 펜팔사이트, 소셜네트워크에서 일정 기간 동안 관계를 유지한 후 사기를 치는 경우도 있다. 서로 다른 국가나 먼 지역에 있는 사람과 친밀감을 형성한 후 선물을 보냈으니 기다리라고 한 후 위장 배송업체가 접근한다. 피해 대상자에게 이메일을 보내거나 문자를 보내 배송 현황을 파악하도록 유도한 후, 개인정보를 입력하면 그 정보를 가로채기도 하며 범죄 대상자에게 연락해 '세관 때문에 물건을 전달할 수 없으니 수수료를 내라' 고 연락해 그 수수료만 받아서 달아나기도 한다.

또한 사업하는 사람에게 접근해 일정 기간 동안 유대관계를 유지한 후 "내가 유력인사를 많이 안다" 또는 스스로 유력인사인 것처럼 가장해 "상품 샘플을 보내라"고 요구한 뒤 그 물건을 편취하는 경우도 있다.

이러한 사기 행각을 보면, 혼자가 아닌 여럿이 모여 각자의 역할을 맡아 시간을 가지고 접근하고 움직인다는 것이 특징이다.

과거 카드 도난분실과 같은 사고의 경우 패턴이란 게 있었다. 예를 들어 누군가가 카드를 훔쳤거나 분실 카드를 습득했을 때 그 카드의 사용 가능 여부를 시험해 본다. 보통은 편의점에서 소액 결제할 수 있는 '담배' 와 같은 물품을 사서 결제 승인이 떨어지면, 그 다음 유흥주점이나 백화점에 가서 큰 금액을 결제하는 패턴이었다.

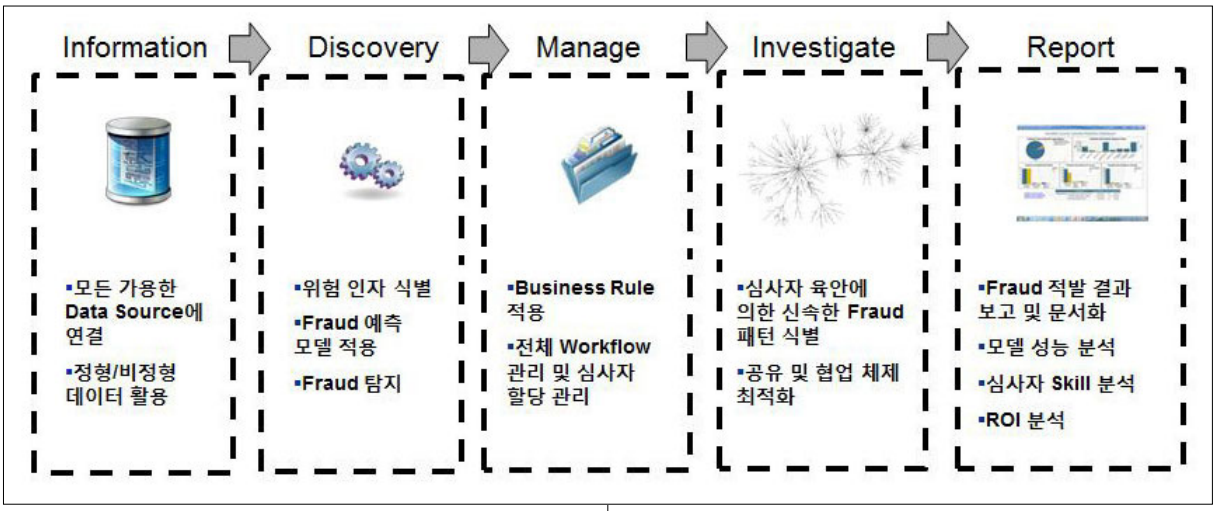
그러나 카드 사고는 점차 고도화되어, POS(Point of Sales)의 해킹으로 대량 유출된 카드 정보가 여기저기로 나뉘어 판매된 후 발생하는 카드 위변조 사고와 같은 형태로 진화되었다. 이러한 사고는 전 세계 어느 지역에서 카드가 사용될 지 알 수 없으며 해킹된 시점과 카드가 도용된 시점까지는 어느 정도 시간차가 있어 카드사가 대처하기 어렵다는 것이 특징이다. 최근의 금융사기는 패턴이 없기 때문에 예측이 어렵고 파괴력은 크다.

패턴 사고와 비패턴 사고는 군대에서 말하는 대칭전력과 비대칭전력에 비유할 수 있다. 대칭전력은 재래식 무기로 대변되는 반면 비대칭전력은 현대식 무기의 사용 또는 전산망 공격 등의 전자전을 의미한다. 따라서 대칭전력은 파괴력이 상대적으로 약하고 예측이 가능한 편이지만, 비대칭전력은 파괴력이 강하며 예측이 힘들다.

최근의 금융 사고는 비패턴 금융사고가 그 중심을 이루고 있으며, 그 중에서도 특히 카드 정보유출 및 위변조와 같은 사고는 상당 부분이 발급사의 책임이라는 점에 주목할 만 하다. 따라서 카드사는 자사의 손실 방어를 위해 이미 발생하고 있는 사고에 대하여도 피해를 최소화하도록 해야 한다.

금융사기를 100% 막을 수는 없다. 문제는 사고가 발생하고 난 후 어떻게 대처하느냐며, 미래 사고의 개연성을 얼마나 막을 수 있느냐가 금융기업에겐 관건이다. 여기서 핵심은 사후약방문일지라

그림 1 | 기업의 사기탐지 업무 흐름



도 얼마나 빨리 대처해 리스크를 최소화하느냐다.

사기탐지의 3요소 분석 · 시스템 · 사람

사기탐지 업무에서 중요한 3요소는 분석, 시스템, 사람이다. 이 3요소는 기업의 사기탐지 업무 효율의 극대화를 위해 전 프로세스(〈그림 1〉 기업의 사기탐지 업무 흐름)에서 최적의 조화를 이룰 필요가 있다.

먼저 분석이라 함은 기업의 가용한 정보를 기반으로 사고 패턴을 분석한 후, 모델링을 통해 향후 발생할 사고의 개연성을 확률로 계산해내거나 Business Rule을 통해 분석자의 경험 및 직관을 반영함을 의미한다.

또한 시스템은 전체 Workflow를 관리하며 심사자에게 사고 의심건을 최적으로 할당(Allocation)하는 일, 분석자와 심사자에게 쉽고 빠르게 양질의 분석 결과를 도출하고 심사할 수 있는 환경을 제공하는 일, 일련의 활동들에 대한 Review 및 Feedback이 가능하도록 지원하는 일 등을 포괄적으로 의미한다.

마지막으로 사람은 심사자를 의미하며, 분석을 통해 탐지된 사고 의심건에 대해 사기 여부를 최종 판별하는 역할을 수행한다. 이 때 심사자의 능력에 따라 할당 건수가 달라지기 때문에 이에 대한 관리를 어떻게 하느냐는 전체 사기적발 실적을 좌우하는 중요한 요소가 된다.

IBM은 사기탐지 업무 3요소를 지원하는 제품군들을 보유하고 있다(〈그림 2〉 IBM 스마터 애널리틱스 시그니처 솔루션 참조).

이들은 유기적인 관계를 바탕으로 시너지를 극대화함으로써, FDS로서의 빠른 시간내 투자 회수 및 잠재적 추가 사고 발생 방지를 가능하게 해준다.

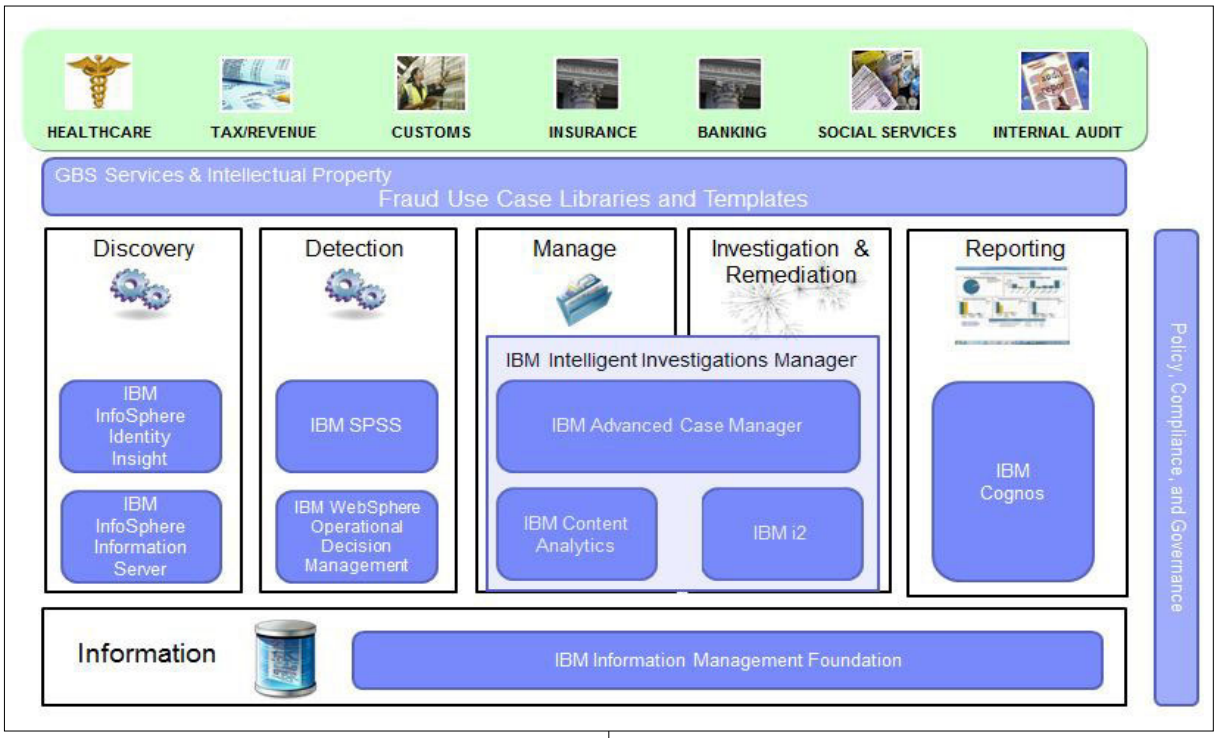
만약 기업에 사고가 발생한다면 피해 규모뿐 아니라 이에 대처하는 시간적, 인적 손실은 매우 클 것이다. FDS는 이미 발생한 사고에 대해 대응할 뿐 아니라, 그 존재만으로도 잠재적인 사고 가능성을 막아준다.

특히 앞서 언급한 사기 탐지의 3요소에서 가장 중요한 것은 바로 분석이며, 이 분석 성능은 사기탐지율(Detection Rate)와 오인식률(False Positive Ratio)로 가늠할 수 있다. 사기탐지율은 전체 사고 중 분석 모델에 얼마나 찾아내느냐에 대한 것이며, 오인식률은 심사자에게 할당된 사고 의심건 중 실제 사고건과 정상건간의 비율에 대한 것이다. 성능이 뛰어난 분석툴은 사기탐지율이 높고, 오인식률이 낮은 제품이다.

쉽고 빠른 분석 환경, 모델 자동 추천 기능, 개방성

FDS의 '분석'에 해당하는 IBM SPSS Modeler는 크게 3가지 강점이 있다. 첫째, 쉽고 빠른 분석 환경을 제공한다는 점이다. 이는 SPSS Modeler가 그래픽사용자인터페이스(GUI)를 기반으로 전 모델과정을 처리할 수 있는 강점에 기인한다. SPSS Modeler는 캔버스라는 화면 안에서 프로그램 코

그림 2 | IBM 스마터 애널리틱스 시그니처 솔루션(2페이지 내용 참조)



딩 방식이 아닌 Drag-and drop 방식, 그리고 메뉴 및 대화상자를 통해 편리하고 자유롭게 구현될 수 있다.

분석을 통해 얻고자 하는 것은 프로그래밍 자체가 아닌 '통찰력' 일 것이며, 분석자가 쉽고 빠르게 배워 업무에 즉각적으로 반영하고 대응할 수 있는 SPSS Modeler의 분석 환경은 급변하는 사고 트렌드에 대처하는데 매우 큰 강점임에 틀림 없다.

둘째, 최적 모델 자동 추천 기능이 있다는 점이다. 많은 통계 모델 알고리즘이 있지만 그 가운데서도 분석자는 자신이 익숙한 알고리즘을 사용하는 경향이 있다. SPSS Modeler는 분석 주제에 맞는 모든 가용한 알고리즘을 적용하여 다양한 모델을 생성한 후 모델 성능을 기준으로 최적 모델을 추천해 준다.

가령 카드사의 FDS 모델로서 주로 사용되는 뉴럴 네트워크(Neural Network)[1]는 사기탐지율이 높지만, 블랙박스라서 설명하기 어려운 모델이다. 대출 심사, 보험 심사, 신용 등급평가에서는 뉴럴 네트워크를 사용하지 않는다. 만약 고객이 전화해 '왜 대출이 거절됐는지, 왜 보험금을 돌려받을 수 없는지' 에 대해 물으면 알려줘야 하는데 뉴럴 네트워크는 결과만 제공해 주고 이유를 알려주지 않기 때문이다.

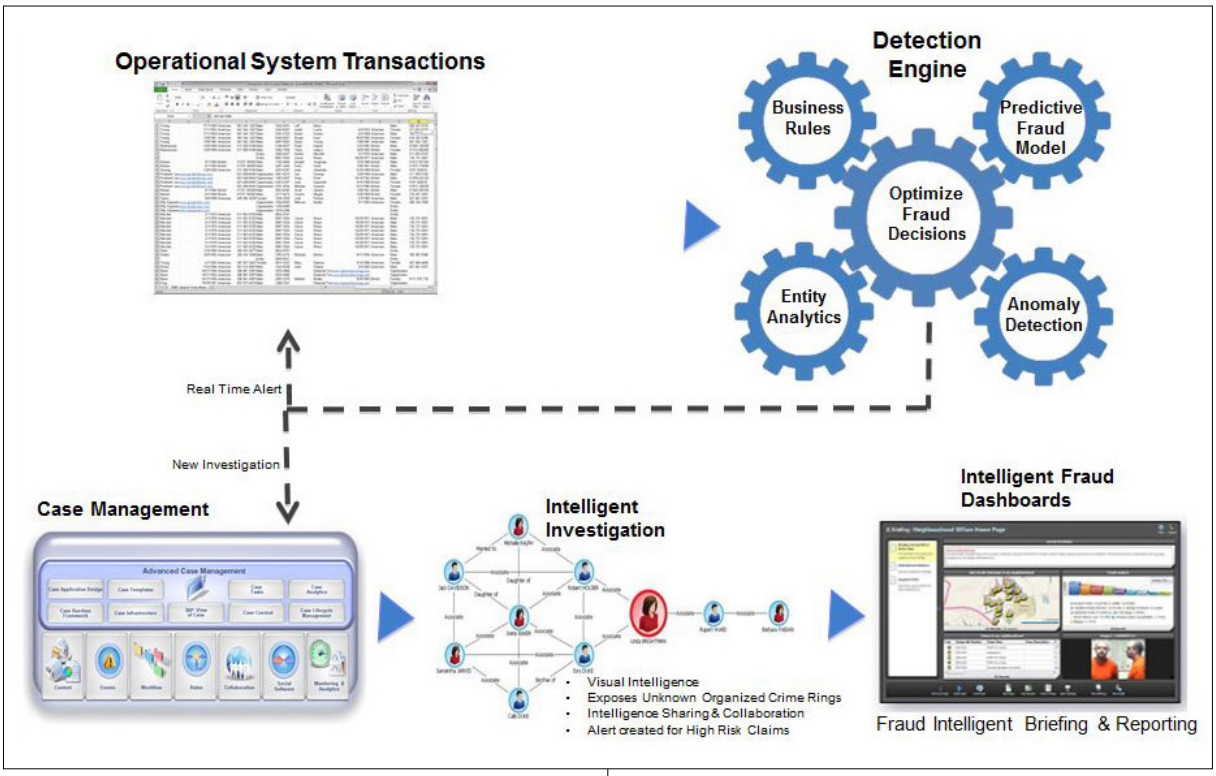
반면, 카드 사기는 고객에게 이유를 설명할 필요가 없다. 뉴럴 네트워크가 탐지율이 높고 성능이 좋으며, 카드 승인 거절을 굳이 고객에게 설명하지 않아도 되기 때문에 카드사 사이에서는 보편화 돼 있다.

하지만 다양한 환경 변화에 따라 최적 모델은 늘 변화될 가능성이 있으며, 따라서 업무 특성별로 잘 맞는다고 알려진 모델들에 대하여도 그 틀을 벗어나 다양한 모델링 기법의 적용 및 시도가 필요한 시점이다.

셋째, 개방성이다. SPSS Modeler는 타 시스템과의 인터페이스 및 조화를 중시하는 사상을 기반으로 만들어 졌다. 따라서 기업의 기존 IT환경이 비 IBM 제품들로 이뤄졌다 해도 여기에 SPSS Modeler만 도입해 기존 IT투자를 보호할 수 있도록 해준다.

1. 인간의 뇌 기본 구조 조직인 뉴런(neuron)들간의 상호 작용 및 그들이 형성하는 네트워크에 착안하여 만든 수학적 모델

그림 3 | IBM의 안티-프로드 솔루션(3페이지 내용 참조)



금융 이외 타 산업으로 확산 적용 가능

타 산업에 비해 리스크 방지가 강력히 요구되는 금융기업들에서 FDS의 수요가 가장 많다. 특히 금융기업들은 정부 규제 때문에 일련의 솔루션들을 도입하고 내부적으로 충당금도 보유해 놓고 있다. 제도도 발달했지만, 무엇보다도 금융은 사기에 대에 어떻게 대응할 지에 대한 인식도 빠르게 확산됐고 그만큼 FDS에 대한 높은 기대치를 가지고 있다.

현재는 FDS가 금융 이외에 다른 산업으로도 확산되는 추세다. 외국의 경우, 세무나 세관에서 허위 신고를 잡아내기 위해 FDS를 도입하기도 한다. 국내에서는 양육비나 보육료 지원에서 허위 청구가 있을 수 있는데, 여기에 FDS를 도입할 수 있다.

해외 통신사들이 FDS를 도입하는 경우도 있다. 보통 가입자들은 지역, 시간, 요금제, 상품 등에서 각자의 통화 패턴을 보여주는데, 어느 날 갑자기 이 패턴에서 벗어난 통화나 데이터 사용이 포착된다면 통신사가 직접 전화를 걸어 분실이나 도난 휴대폰인지를 확인하고 통화를 중지시키는 조치를 취할 수도 있다. 이는 기존의 카드사들이 사기탐지와 비슷하다.

공공, 통신 이외에도 제조기업도 FDS를 사용할 수 있다. 제조업의 예지정비(Predictive Maintenance), 제품의 불량 감시 등은 금융기업들의 사기탐지와 모델링 과정도 흡사하다. 금융기업이 고객의 특성과 실시간으로 일어나는 거래 정보를 조합하고 외부 데이터 반영해 사기(Fraud)냐 아니냐를 판단하는데, 여기서 고객을 제품이나 품질 데이터로 바꾸고 거래 정보를 설비, 센서 데이터로 바꾸면 제조기업에서의 디텍터(Detector)가 된다. 금융과 제조는 서로 산업이지만 같은 모델링 구조와 방법론 가지고 있다.

SPSS Modeler는 고객 분석, 운영, 리스크 3가지 영역에서 사용할 수 있다. 고객 분석에서는 프레딕티브 커스터머 애널리틱스(Predictive Customer Analytics)를, 운영에서는 프레딕티브 오퍼레이션 애널리틱스(Predictive Operation Analytics)를, 리스크에서는 프레딕티브 리스크 애널리틱스(Predictive Risk Analytics)를 각각 적용할 수 있다. CIO

● **김지관** 과장은 한국IBM 소프트웨어그룹에서 Business Analytics(SPSS)를 담당하고 있다.