이상행위 탐지시스템 기술의 발전 방향

임형진
금융보안원

요 약

최근 핀테크 산업이 이슈가 되면서 금융 업무를 더 효율적으로 만드는 기술 중 하나로서 이상행위 탐지시스템(FDS)이 관심을 받고 있다. 이상행위 탐지시스템은 금융업무의 리스크 관리를 위한 기술로 주로 활용되고 있다. 본고에서는 이상행위 탐지시스템의 개념을 소개하고, 은행, 카드, 보험 등 금융권 적용분야를 살펴보고자 한다. 또한, 각 금융업무의 리스크 관리 목적뿐만 아니라 FDS를 활용한 침해사고 대응 활동을 소개하면서 기술 발전 방향을 고찰하도록 한다.

Ⅰ. 서 론

최근 핀테크가 큰 화두가 됨에 따라 함께 관심을 받게 된 것이 바로 '이상행위 탐지시스템(FDS)'이다. 기존에는 이용자의 단말기에 각종 보안프로그램을 설치함으로써 보안성을 향상시켰지만, 현재는 이용자 보호를 위한 보안체계가 편의성 중심으로 개편됨에 따라 거추장스러운 보안프로그램을 걷어내고 보안성을 강화하기 위해서 활용되고 있다.

금융권에서는 오래전부터 이 기술을 폭넓게 사용하고 있으며, 현재는 그 영역을 넓혀 나가고 있는 상황이다. 해외의 경우도 마찬가지로 다양한 산업군에서 이를 활용하고 있을 뿐만 아니라, 국가적 차원에서 효율적인 대응을 위해 이상행위, 사고 관련 정보 등을 공유하면서 적극적인 자세로 대처하고 있다. 세계적으로 핀테크(FinTech)에 대한 관심이 뜨거워짐에 따라 'OO페이'와 같은 간편결제 서비스를 경쟁하듯 내놓고 있다. 이용자가 더 쉽고 간편하고 빠르게 이용할 수 있도록 다양한 기술을 접목한 서비스들을 내놓고 있지만, 편의성을 위해 각종 보안 프로그램이 제거됨에 따라 보안성이 낮아지게 되었다. 이러한 이유로 다양한 금융업무의 리스크 관리 목적으로 다시 주목받고 있는 기술이 바로 '이상행위 탐지시스템(FDS, Fraud Detect System)'이다.

해외의 경우 국가적 차원에서 부정행위 근절을 위해 공공기관과 민간기관이 서로 협력하여 다양한 노력을 펼치고 있다. 최근 국내에서도 국가정보원을 중심으로 사이버위협정보 공유센터 설치와 관련된 법률안이 제출됨에 따라 정보 공유를 통한 효율적 대응이 가능해 질 것으로 예상된다. 본문에서는 국내외 이상행위 탐지기술 활용 사례와 현황에 대해 살펴보고, 기술 발전 방향을 전망해보고자 한다.

Ⅱ. 이상행위 탐지시스템의 이해

1. 이상행위(Fraud) 정의

'Fraud'라는 용어는 사기, 기만, 범죄행위, 이상행위 등의 뜻을 가지며, 사전적 의미로는 속임수나 거짓말로 돈이나 금융 혜택을 얻는 범죄, 불법적이거나 정직하지 못한 방법으로 사람들을 속이는 것 또는 사람이라고 정의하고 있다.

표 1. 이상행위의 유형

구 분	관련 세부 내용
개인	사전 요금 지불, 투자사기, 비(非)투자, 신뢰 위치 남용
기업	기업 서비스 사기, 기관 투자 사기, 비즈니스 거래 사기, 일반 거래 사기, 지적 재산권 사기, 은행 및 신용 관련, 보험관련 사기, 전화관련 사기, 도박관련 사기
자선 및 비영리	자선부분의 내부사기, 수집 및 자선 보조금 사기
시장 남용	내부자 정보, 시장 조작, 반 경쟁 행위
회계	세금사기, 혜택사기(국가적)
공공 부문	자선부분의 내부사기, 공공 조달 및 보조금, 지방세 혜택 사기, 공공부문 서비스 제공
활동 지원	신분도용, 부패, 물리적 준비 행위, 정보 · 통신 · 기술 준비 행위, 머니 이동

이상행위는 비즈니스, 금융 등 다양한 분야에서 정의되고 있으며, 분야별 종류 또한 다양하게 존재한다. 이상행위 방지 활

동이 가장 활발하게 되고 있는 곳은 유럽지역이며, 특히 영국의 경우 이를 위한 다양한 기관들이 운영되고 있다. 영국의 중대(重大) 부정 단속국(SFO, Serious Fraud Office)[1]에서는 이상행위 유형을 다음과 같이 구분하고 있다[2].

이하 본문에서는 유사한 용어가 혼용되어 사용하는 것을 방지하기 위해 별도의 명칭을 사용하는 부분을 제외하고, 용어는'이상행위'라고 통칭한다.

2. 이상행위 탐지시스템

이용자 혹은 기업의 금전적 손실, 정보 유출 등 이상행위를 통해 발생될 수 있는 악의적인 행위들을 탐지하고 차단하기 위해 고안된 시스템이다. 이와 유사하게는 이상행위 방지시스템(Fraud Prevent System), 위협 관리 시스템(Risk Management System) 등이 존재하며, 불리는 명칭만 다를 뿐 이상행위를 탐지 · 예방하려는 목적은 동일하다.

이상행위 탐지시스템의 기본 흐름은 〈그림 1〉와 같이 '수집 ▶ 분석(탐지) ▶ 대응'의 3가지 핵심 기능으로 구성된다[3][4][12]. 첫 번째로 '수집'은 이용자 단말기(PC, 스마트폰 등) 정보, 네트워크 정보, 이용자 정보 등 이용 시 발생되는 정보, 기업에 저장된 정보들을 의미한다. 두 번째 '분석'은 수집된 정보들의 상관관계 분석(Correlation Analysis)[2], 통계 분석, 스코어링 분석 등 다양하게 연구된 분석 방법을 통해 이상행위 여부를 판단한다. 세 번째 '대응'은 정상일 경우 이용자의 분석 데이터 정보를 업데이트하고, 비정상일 경우 탐지 이후 지속적인 행위를 불가능 하도록 막거나 관리자에게 통보하는 등의 행위를 취한다.

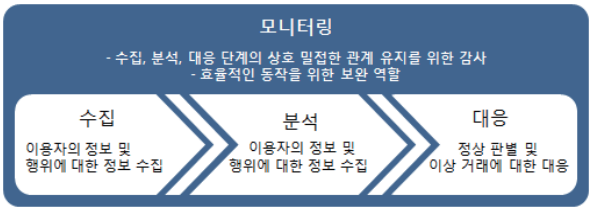

그림 1. 이상행위 탐지시스템의 주요 기능

하지만 이상행위 탐지시스템을 운영하면서 주의해야 할 사항들이 존재한다. 해킹 등에 의해 정보가 유출될 경우 그에 따른 피해는 상당할 것이다. 따라서 정보 유출이 되더라도 피해를 최소화하기 위해서 민감한 정보를 배제하거나 암호화 혹은 대체 식별 정보를 활용하는 것을 고려할 수 있다. 분석과 대응에 있어서 과탐 혹은 오탐으로 인해 민원이 발생 할 수 있기 때문에 과도한 차단보다는 적절하게 대응할 수 있는 수준에서 정책을 적용하는 것이 좋으며, 이를 탐지하기 위해 적용된 분석방법을 수정하여 적용함으로써 유기적인 관계로 대응해 나가야 한다.

금융권에서 이 기술을 활용하여 이상금융거래 탐지시스템, 보험사기 예방시스템, 카드부정 적발시스템 등 다양하게 사용되고 있으며, 이밖에도 내부자 부정행위 적발, 개인정보 부정사용 방지 등 보안전반적인 분야에서도 널리 사용되고 있다[5].

Ⅲ. 적용 분야

1. 카드 사고 예방시스템

가. 정의

카드 사고예방 시스템은 카드거래[3]에 대해 이용자 패턴 분석, 사고패턴, 사고의심 점수 등 종합 분석을 통해 의심거래에 대해 이상해위에 대한 징후가 있을 경우 거래중단 혹은 추가인증 절차를 통해 사고를 예방하는 시스템을 말한다. 유사하게는 카드사기 방지시스템, 카드사기 모니터링 시스템 등이 있으며, 불리는 명칭만 다를 뿐 카드 사고 예방을 목적으로 한다.

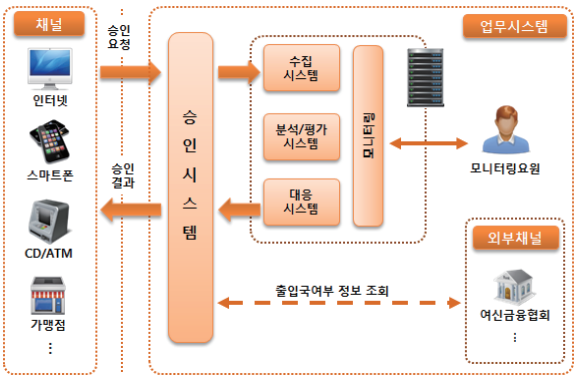

그림 2. 데이터 흐름도

나. 등장배경

카드 사고예방 시스템은 일찍이 1990년대에 도입되었는데, 이것은 카드의 이용실적 및 부정사용과 관련성이 있다. 1990년대 초부터 카드 이용실적은 지속적으로 증가하고 있는 추세이

1 1987년 설치한 정부부처로 불법 정치자금, 부패, 사기사건 등을 전담하는 정부 · 의회로부터 독립된 반부패 기관이다.

2 두 변수의 상호 연관성에 대한 통계적 유의성을 검증해 주는 통계분석 기법이다.

3 카드거래는 신용카드, 체크카드, 선불카드 등 다양한 유형이 있으며, 운영하는 금융회사에 따라서 통합 혹은 별도 운영하기도 한다.

며, 2000년대 초반 현금서비스의 무분별한 사용으로 이용실적이 일시적으로 급증하였으나, 2003년 관련 규제로 인해 이용실적이 다소 감소하였다. 다만, 일시불과 할부거래에 대해서는 지속적으로 증가하여, 20년간 약 20배 이상의 카드 이용실적이 증가하였다.

2000년대부터는 비대면 거래가 크게 증가하였는데, 이는 스마트기기 보급과 모바일 쇼핑의 증가와 관련이 있다. 스마트폰은 2018년 전 세계 보급률이 50%를 넘어설 것으로 예상된다. 국내 인터넷쇼핑 시장규모 또한 PC를 통한 인터넷쇼핑은 감소할 것으로 보이나, 모바일을 이용한 거래는 증가할 것으로 예상하고 있다. 이용매체 및 카드 이용의 확산으로 인해 부정사용량도 지속적으로 증가하고 있다. 이렇듯 카드 이용이 증가하고, 이에 따른 부정사용도 증가함에 따라 카드사에서는 이용자들의 피해를 막기 위해 카드 사고예방 시스템을 도입하여 운영하고 있다.

다. 탐지방법

이상행위를 탐지하기 위해서는 다양한 정보를 수집하는 것이 무엇보다도 중요하다. 카드 사고예방 시스템에서는 회원 프로파일, 카드 프로파일, 가맹점 프로파일, 최신 사고 유형, 위치정보 등을 활용한다. 수집된 정보는 다양한 분석 알고리즘에 의해 부정거래 유무를 판단하며, 카드 승인 이전 혹은 경우에 따라 사후 거절을 발생시킴으로써 부정거래를 방지한다.

수집되는 정보의 프로파일은 카드사 회원들이 카드를 사용하는 금액, 패턴 등의 이용 성향, 소지하고 있는 카드별 사용 성향, 해당 가맹점들 이용고객, 금액 등의 성향과 위치 정보 등 이상 유무를 판단하는데 도움이 되는 정보들을 수집한다.

이상행위를 탐지하는 실제 예로써, '지역간 비정상 거래 발생'이 있다. 마지막으로 발생한 거래가 서울 여의도의 한 편의점에서 정상적인 거래가 발생한 후, 30분이 채지나지 않은 시간에 부산 해운대에서 동인한 카드가 승인 요청이 발생한 경우이다. 서울에서 부산까지 이동하는 방법은 비행기, 열차, 자동차 등이 존재하지만, 가장 빠르게 이동하더라도 최소 1시간 이상의 시간이 소요된다. 하지만 마지막 거래 후 30분 이내에 부산에서 거래가 발생한 건에 대해서는 카드 복제로 인한 부정거래로 판단할 수 있다.

이외에도 해외 승인 요청 건에 대해서는 출입국관리사무소의 시스템을 통해 출국 여부를 확인하여 실제 이용자가 해외로 출국한 사실이 있는지 여부를 가지고 판단하기도 한다. 이렇듯 다양한 경로를 통해 수집되는 정보는 이용자가 정상적으로 카드를 사용하였는지 확인하는데 이용된다.

라. 시스템 구성

카드 사고예방 시스템은 〈그림 2〉과 유사하게 구축하여 운영하고 있다. 온라인 및 오프라인에서 카드가 긁혀 승인요청이 오면 이용자 성향, 카드 성향, 가맹점 성향 등 다양한 정보들을 수집한 후 해당 승인요청 건에 대한 위험평가를 내린다. 위험평가를 위한 방법으로는 통계학적, 의사결정나무, 회귀분석 등 다양한 방식을 통해 이상 유무를 판단한다. 다만, 블랙리스트[4]에 등록된 정보가 발견될 경우 즉각 차단하기도 한다. 판단 결과에 이상 여부가 탐지될 경우 모니터링요원에게 즉각 알리고, 내용 확인을 통해 최종적으로 승인 거절을 내리도록 시스템이 구성된다.

2. 보험사기 방지시스템

가. 정의

보험사기 방지시스템은 고의로 교통사고, 의료사고 등을 발생시켜 보험계약상 지급 받을 수 없는 보험금을 취득하는 행위를 사고기록, 설계사평판, 병원평판, 사고와 관련된 상관관계 등을 분석하여 보험금이 부정하게 수령하지 못하도록 보험사기를 예방하는 시스템을 말한다.

보험사기 유형으로는 고의 사고, 허위 · 과다 사고, 피해과장 사고 등이 있으며, 주로 허위 · 과다 사고 관련이 70%를 넘는다. 대개 병원, 보험설계사, 변호사 등과 사전 모의를 통해 고의사고를 유발하여 과다한 보험료를 청구하는 것이 일반적이다.

나. 등장배경

1990년대 말부터 생계형 범죄, 조직폭력배 개입 등 보험금을 부정하게 타려는 사기범죄가 등장하였으며, 연평균 50%에 가깝게 증가폭을 이어나갔다. 금융당국에서는 지속적으로 증가하는 보험사기 근절을 위해 2001년부터 보험사기 예방을 위한 시스템을 구축할 것을 권고하면서 등장하게 되었다. 2004년 금융감독원은 보험사기인지시스템을 도입하여 사기혐의 점수를 통해 혐의자 적발하며, 보험개발원에서도 보험사고정보를 집중시켜 보험사기 징후를 진단하기 위한 시스템을 구축하였다[6].

이외에도 보험사기전담 특별조사팀(SIU, Special Investigation Unit) 운영, 보험범죄 합동대책반 운영, 시스템 개선 등 지속적인 노력으로 보험사기를 근절하기 위해 노력하고 있다. 하지만 생계형 범죄, 지능화 범죄 등 보험사기는 지속적으로 증가하고 있는 추세이다. 건강보험심사평가원에서는 2010년 기준 보험금 누수규모가 약 3조 4천억원으로 추정하고 있는데, 이는 적발 금액의 10배 가량의 수치이다. 결국 이 피해는 정상 이용자들의 보험료 인상과 관련이 있기 때문에 지속적으로 보험사기 방지시스템 도입과 개선 등의 요구가 이루어진다.

4 주요 감시가 필요한 정보를 말하며, 보통 사고 정보와 관련된 IP, MAC 등 의미한다.

표 2. 보험사기 주요 유형

구분	세부유형
고의 사고	자살, 자해, 살인, 상해
허위 · 과다 사고	허위(과다)입원, 허위(과다)장해, 사고내용조작, 피해자(물) 끼워 넣기, 음주, 무면허 운전, 차량도난, 운전자 바꿔치기
피해과장 사고	자동차사고, 병원 과장청구, 정비공장 과장청구

다. 탐지방법

보험금 지급은 카드 결제나 이체 거래와 같이 즉시성을 요구하지 않아 상대적으로 분석시간이 길고, 추가적인 정보 수집이 가능하다는 장점이 있다. 하루에도 많은 사고가 발생하고, 이를 처리하기 위해 보험금 지급 요청이 들어오고 있으나, 이를 수작업을 통해 이상 유무를 판단하는 것은 어렵다. 따라서 보험금 지급 요청 시 요구되는 최소한의 정보를 이용하여 의심사고 여부를 판단한다.

예를 들어 4년간 순차적으로 3개의 생명보험을 가입하고, 사고 3개월 직전 계약변경으로 사망보험금을 증액시킨다. 이후 아내는 운전자 과실로 위장하여 바다로 고의 추진/추락시켜 살해 한 후, 사망보험금 지급 신청을 한다. 보험가입 상황을 제외한 부분에서는 안내의 과실로 인한 사망이 정상적으로 비춰질 수 있지만, 과도한 생명보험 가입 및 사망보험금 증액의 경우 보험사기조사팀을 통해 정말조사를 거쳐 보험금 지급여부를 결정한다.

금융회사에서는 사고의 종류에 따라 수집 · 활용 될 수 있는 정보는 각각 상이하며, 주로 자동차보험사기와 관련해서는 모집자, 병원(평판, 의사 등), 지급횟수, 사고자와의 관계 등 다양한 정보를 수집하여 보험사기 여부를 확인한다.

이밖에도 금융감독원에서는 보험사기 인지시스템을 구축하여 조직화 · 지능화되는 보험사기를 적극적으로 대처하기 위해 운영하고 있으며, 보험계약 과다 가입여부, 보험금 지급횟수, 사고 유형 등에 따른 보험사기지표를 개발하여 인별 · 그룹별 혐의도를 산정하여 조사대상을 선정할 수 있으며, 단계별로 가해자, 피해자, 동승자 관계를 자동으로 추출하고 혐의자를 확장하면서 사고관련성 및 공모여부를 판단할 수 있다. 구체적 혐의가 있는 사람에 대해서는 보험금 예상편취규모 및 사기유형을 확인 할 수 있도록 다각화하여 보험사기를 탐지한다. 이와 유사하게 생명보험협회에서는 보험계약과 사고정보, 보험대출 정보를 가지며, 손해보험협회는 실본보험 계약정보를, 보험개발원에서는 자동차보험 계약정보와 보험효율 산정을 위한 광범위한 보험금 지급 정보를 활용하여 보험사기를 탐지한다.

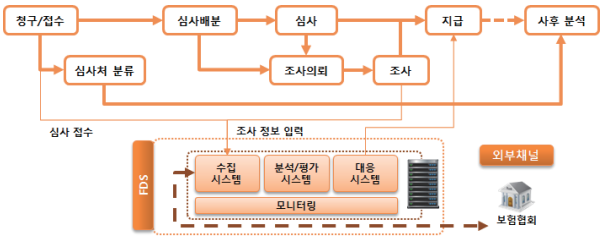

그림 3. 업무 프로세스에 따른 시스템 구성

라. 시스템 구성

보험사기 방지시스템은 〈그림 3〉와 유사하게 구축하여 운영하고 있다. 보험금 청구 접수가 되면, 심사 여부를 결정하고, 이후 사고유형 및 위협 수준에 따라 심사 혹은 추가 조사 프로세스를 걸친 후 지급여부를 결정한다. 보험금이 지급된 이후에도 지속적인 사후 분석을 통해 보험사기와 연관되어 있음을 확인하면, 부당반환 청구 등의 조치를 통해 지급된 보험금을 환수시킬 수 있도록 한다.

3. 이상금융거래 탐지시스템

가. 정 의

이상금융거래 탐지시스템은 인터넷뱅킹 및 스마트폰 뱅킹 등과 같이 비대면으로 이루어지는 자금이체 행위에 대한 이용자 패턴분석, 사고패턴 등 종합적인 분석을 통해 이상징후 포착시 거래중단 혹은 추가인증을 통해 사고를 예방하는 시스템을 말한다. 국내에서는 기존의 카드 사고예방 시스템에서 활용되는 것을 자금이체로 확대 적용한 것이다.

나. 등장배경

2013년 7월『금융전산 보안 강화 종합대책』에서 언급한 후 급속도록 은행권역 및 증권권역 등에 구축할 것을 권고함으로써 등장하게 되었으며, 이는 인터넷뱅킹과 스마트폰뱅킹 등 비대면 채널을 통한 뱅킹 서비스 이용자가 급증하였기 때문이다. 인터넷뱅킹 전체 등록자 수는 증가하고 있으며, 이는 모바일뱅킹 중 스마트폰뱅킹 이용자가 증가하였기 때문이다.

또한, 지속적으로 증가하는 보안위협 또한 중요한 부분일 것이다. 한국은행[7]의 발표에 의하면 2013년도에는 전년대비 약 15배가량 크게 증가하였다. 2013년 당시 파밍, 스미싱의 등장으로 인해 이를 인지하지 못한 이용자들이 PC와 스마트폰이 악성코드에 감염됨에 따라 공인인증서, 이체정보 등이 유출되었으며, 궁극적으로 이용자의 금전적 피해까지 이어졌다.

다. 탐지방법

전자금융서비스는 인터넷뱅킹, 스마트폰뱅킹, 폰뱅킹 등 다양한 서비스를 제공하고 있으며, 이용자는 이러한 서비스를 이용하기 위해서 PC, 스마트폰, 전화기, CD/ATM 등 다양한 채널을 이용한다[3][4]. 다양한 채널들에서는 서로 다른 단말정보, 네트워크 정보, 거래정보 등을 생성되어 이용자의 프로파일을 작성하는데 이용된다. 이용자 프로파일은 전자금융서비스를 이용하는 정상적인 범주를 나타낸다. 소액거래를 주로 이용하는 이용자가 수신자와의 거래가 없으며, 고액을 이체하는 경우는 이상거래로 의심해 볼 수 있는 것이다.

이용자의 이용 평균치에서 벗어나는 경우, 수신자와의 거래내역이 없는 경우, 해외에서 접속하는 경우 등 다양한 방법론, 알고리즘을 통해 이상 유무를 판단할 수 있다. 이상행위라고 판단되더라도 모든 거래를 이상행위로 단정하기보다는 오탐, 과탐 등을 고려하여 추가인증을 수행하는 것이 좋다. 다만, 과거에 발생한 사고 거래와 일치하는 경우에는 차단하는 것이 효과적으로 대응하는 것이다.

예를 들면 '중국발(해외) 새벽시간 자금 이체'가 있다. 이용자의 단말기가 악성코드에 의해 감염된 후 자금이체에 필요한 공인인증서 및 인증정보를 해커에게 탈취 당함으로써, 해커는 중국에서 정상적인 로그인을 통해 불법 자금이체를 시도한다. 하지만 정상 이용자의 특성상 이체 시간대가 다르고, 중국으로의 출국 여부가 확인되지 않았음에도 불구하고 중국에서 거래가 발생한 점으로 미루어 볼 때 부정거래로 판단할 수 있다.

이상금융거래 탐지시스템에서도 카드사기 방지시스템에서 활용하는 출국자 정보를 이용하여 보다 효과적으로 탐지하기 위해 변화되고 있다.

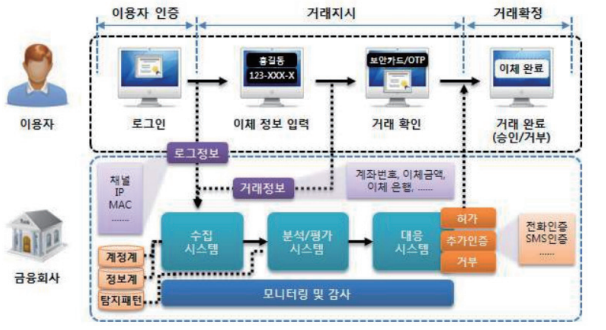

그림 4. 「이상금융거래 탐지시스템」과 금융거래절차 간 상호연동 예

라. 시스템 구성

이상금융거래 탐지시스템은 아래의 〈그림 4〉과 유사하게 구축 · 운영하고 있다. 자금 이체는 실시간으로 이루어지기 때문에 이용자 측면에서는 이체가 완료되기 이전에 이상 유무를 판단해야 하며, 금융회사 측면에서는 거래 원장이 생성되기 이전에 판단되어야 한다. 이상금융거래 탐지시스템을 운영하는 금융회사의 정책에 따라 달리 적용될 수 있으며, 블랙리스트 등록된 단말정보 혹은 네트워크 정보로 유입되는 경우 접속 당시 차단하여 대응 할 수도 있지만, 이상행위로 간주하고 해당 행위를 기록하고 최종 원장이 생성되기 전에 거절 할 수도 있다.

또한, 일부 접속자가 몰리거나 시스템 이상으로 인해 정상적으로 동작하지 않는 경우 이체 거래에 영향을 주어 이체 거래가 발생되지 않아 장애를 야기할 수 있다. 이럴 경우를 대비해서 이상금융거래 탐지시스템을 이중으로 구성하기도 하며, 일정 분석 시간이 지나가면 사후탐지로 처리하는 경우가 있다. 사후탐지는 영업점 시간이 끝난 이후에 시스템에 무리가 가지 않는 시간에 이루어지며, 새로운 룰 혹은 분석 시간이 충분히 필요할 경우 이루어진다.

이상금융거래 탐지시스템은 금융회사의 환경적 요건에 따라 달리 적용될 수 있으며, 다양한 수집 정보를 효과적이고 단시간에 분석하기 위해 빅데이터 시스템과 결합되어 운영되기도 한다.

4. 기업 내부 이상행위 탐지시스템

가. 정 의

기업 내부적으로 운영되는 보안관리, 네트워크 관리, 부대설비 관리, 서버 관리 등 모든 보안 시스템에서 발생되는 로그를 통합 관리하여 모니터링 하는 시스템을 말한다. 각각의 보안 시스템들은 발생되는 로그를 기록하며, 특정 이상치 값을 초과하는 경우에만 경보를 알려주게 설정되어 있다. 하지만 각각의 로그들의 연관성을 분석해보면 정상/의심 수치 범위 안에서 이상행위를 탐지할 수가 있다. 또한, 사고 발생 시 연관성 분석을 통해 사고 분석이 용이하도록 도와주는 시스템이다[8].

나. 등장배경

정보보호 산업 규모는 지속적으로 성장하고 있으며, 이것은 보안 사고와도 관련성이 있다. 지난해 미국에서 발생한 Target 社의 정보 유출 사고의 경우 매장에 설치된 포스단말기가 해킹되어 고객의 개인정보 7천만건, 카드정도 4천만건이 유출되었다. 이로 인해 Target社가 배상해야할 금액은 약 3조 8천억원 정도로 추산된다.

최근까지도 기업에서 정보보호 투자에 소홀하였으나, 고객정보유출 등으로 기업에 막대한 기업 이미지, 물질적 피해가 발생하므로, 정보보안 투자를 늘려 보안 사고를 예방하기 위해 노력

하고 있다.

기업 보안을 위해 다양한 보안 솔루션이 등장하게 되었으며, 관리의 편의성을 위해 별도의 관리 시스템을 두었다. 새로운 보안 솔루션이 도입됨에 따라 관리 시스템 및 관리 인력이 추가되는 등의 불편함이 증가하였다. 하지만 통합 보안 관제 시스템은 관리적 측면에서의 업무 효율성과 수집된 정보들의 연관성을 함께 분석할 수 있기 때문에 효율적인 대응이 가능하다.

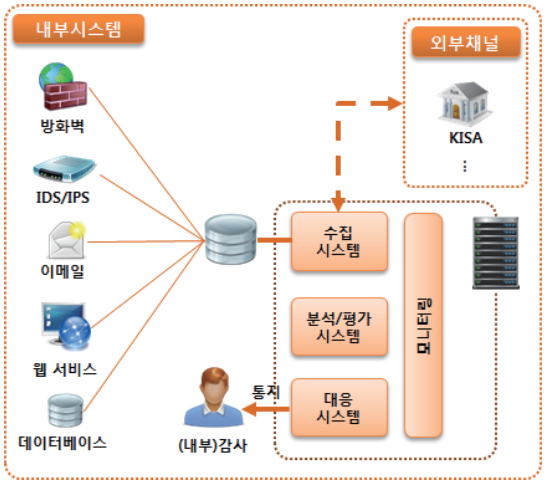

그림 5. 통합 보안 관제 시스템 내부 구성도

다. 탐지방법

기업 내부에서 발생할 수 있는 위협은 APT를 통한 정보 유출, 내부자 공모를 통한 정보 유출, 비인가 데이터 접근, 데이터 무단 변경 등 다양하다. 위협의 행위는 PC, 노트북, 스마트 기기 등 단말기를 통해서 이루어지며, 정상적인 이용절차에 의해서는 보안 프로그램이 설치되어 있으며, 내부 네트워크를 이용하므로 다양한 로그가 발생되어 기록된다. 하나의 보안 프로그램에서 기록된 로그를 통해 위협 여부를 확인 할 수는 있지만 탐지의 정확성은 높지 않을 것이다.

개인정보를 다루는 업무는 하는 업무 담당자는 개인정보 검출 프로그램에 매번 탐지될 것이다. 하지만 이것은 정상적인 업무이기 때문에 하나의 보안 프로그램으로만 이상행위 여부를 판단하는 것은 어렵다. 따라서 생성된 파일 내부에 개인정보가 기록되어 있는지, 이를 파일 암호화 해제를 요청한 후 기존에 메일 리스트 발송 이력이 있는지를 확인함으로써 종합적인 위협 분석이 가능하다.

일련의 사고를 시나리오 기반으로 작성한 후 행위가 순차적 혹은 유사하게 발생되는 경우를 이상행위로 간주 할 수 있으며, 평소보다 많은 개인정보를 보유하거나 트래픽을 발생하는 경우와 같이 정상 수치 범위를 넘어가는 경우에도 의심해 볼 필요가 있다.

라. 시스템 구성

통합 보안 관제 시스템은 기업 내부에서 발생되는 모든 정보를 수집하여 분석하기 때문에 기업의 규모에 따라 수집되는 정보의 양이 상당할 것이다. 일부 기업에서는 기업의 기술적인 위협으로부터 보호하기 위한 수단으로 이용하기도 하지만, 내부 감사 등 수집 정보의 영역을 넓혀 활용 범위를 확장시켜 활용한다. 수집되는 데이터의 크기가 커질수록 빅 데이터 분석 기술이 요구되고, 생성되는 데이터를 빅 데이터에 입력함으로써 효율적인 분석이 가능하도록 시스템을 구성한다.

5. 기 타

이상행위 탐지시스템은 이 밖에도 자금세탁방지시스템, 개인정보 부정사용방지 시스템, 내부자 부정행위 탐지 등 다양한 보안 분야에서 활용되고 있으며, 스포츠 승부조작 등 비(非) 보안 분야에서도 폭 넓게 이용되고 있다. 정상 집단에서 이상행위를 하는 비정상 집단을 탐지해내는 방법으로는 블랙리스트, 그레이리스트[5], 화이트리스트[6]와 같이 비교 대상 정보와 일치하는지에 따라 판별하는 방법이 기본적으로 활용된다. 하지만 위협은 새롭게 등장하며, 활용 기술 또한 고도화됨에 따라 이러한 이분법적 방법으로 탐지하는 것은 매우 어렵다. 상관관계분석, 빅데이터를 활용한 분석, SNS를 이용한 관계도 분석 등 다양한 분석 방법들이 국내외에서 고안되고 있으며, 이를 실제 적용함으로써 효과적인 탐지 및 대응을 수행하고 있다.

Ⅳ. FDS를 활용한 침해사고 대응활동

국내 금융권의 경우 공동으로 이상행위를 대응하기 위한 공유시스템을 운영중이다. 보험사기 방지 및 대포통장 등 일부 정보에 대해서만 공유함으로서 공동 대응을 하고 있다. 비금융권의 경우 한국인터넷진흥원에서 사이버 위협 정보를 공유하기 위해 시스템을 구축함으로써, 효율적으로 사이버 위협을 대응하기 위해 노력하고 있다. 반면 해외의 경우, 범정부적 차원에서 국가기관, 민간기관 등이 상호 협력하여 효율적으로 대응할 수 있도록 정보 공유 시스템을 구축하여 운영하고 있다[9][10][11].

5 블랙리스트와 관련성이 있어 관심 있게 여겨야할 정보를 의미하며, 예를 들자면 사고 IP 주소가 이용된 IP 주소 대역을 의미한다.

6 블랙리스트와 반대되는 개념으로 허용되는 대상을 지정하는 목록을 의미한다.

1. 금융권

국내의 경우 이상행위 정보 공유를 위한 시스템을 구축을 진행하고 있으며, 반면 해외에서는 국가적 차원에서 정보 공유를 위한 체계를 구축하여 운영하고 있다.

가. 국내 사례

가. 1. 금융보안원의 FDS 정보공유 시스템

국내에서는 2014년 12월부터 금융감독원 주체로 이상금융거래 탐지시스템 구축 및 고도화를 위해 'FDS 추진 협의체'를 구성하고 금융권 FDS 고도화 로드맵 1.0을 발표하였다. 금융회사간 FDS 구축 · 운영 관련 노하우 공유 및 FDS 공통기준을 마련하고, 금융회사의 신속한 전자금융사고 탐지 및 대응체계를 조속히 갖추도록 유도한다는 계획이다.

금융보안원에서는 FDS 정보공유 시스템을 구축하여 추진 중에 있으며, 각 금융회사에서 탐지된 이상행위 정보 혹은 의심되는 정보를 금융회사간 공유를 추진하고 있다. 또한, 유관기관 및 관련 기업으로부터 사이버 위협 정보를 수집 · 공유함으로써, 효율적이고 선제적인 대응이 가능하도록 할 것이다. 이를 위해서는 이상행위의 탐지 정보의 표현 규격 및 전송 규격을 만듦으로써, 효율적인 정보공유가 이루어 질 수 있도록 한다.

나. 해외 사례 : 영국

영국은 다양한 이상행위를 방지하기 위해 노력하고 있는 대표적인 국가로서, 카드 사기 방지 시스템은 1990년대 초반에 도입하였다. 하지만 신종 범죄, 카드 복제 등 지속적인 증가로 인해 2004년엔 칩앤핀(Chip-and-PIN[7]) 기술을 도입하여 카드 사기 감소에 도입이후 지속적으로 감소하였다.

하지만, 비대면거래(CNP, Card Not Present[8]) 증가 및 칩앤핀의 보안 강화로 인해 상대적으로 취약한 비대면 결제의 취약성으로 인해 2007년부터 다시 증가세로 돌아섰다. 이후 기관들은 사기 정보를 서로 공유할 수 있도록 체제를 마련하여 2008년부터는 카드로 인한 사기 손실액이 점차 줄어든 것을 확인 할 수 있다.

이렇게 정보공유는 이상행위를 탐지하여 사고를 줄이는데 큰 도움을 주고 있으며, 관련된 내용은 다음과 같다.

나.1. 이상행위 정보 공유 시스템(FISS, Fraud Intelligence Sharing System)

2008년, 영국 카드 협회(UK Cards Association)와 이상행위 통제 위원회(Fraud Control Steering Group)이 서로 협력하여 FISS를 구축하였다. FISS는 공유 가능한 데이터베이스를 기반으로 금융사기에 대한 의심스러운 정보를 금융회사 간에 공유할 수 있도록 하고, 이상행위 발생 시 관련 정보를 보다 빠르게 제공하는 역할을 수행한다.

FISS를 통해서 블랙리스트 정보(이름, 생년월일, 주소, 전화번호, 이메일 등)를 받을 수 있고, 범죄자들에 의해 표적이 되는 고위험(High-Risk)군을 식별할 수 있다. 데이터베이스는 온 · 오프라인 사고 데이터를 포함하고 있고, 유사 사고에 대하여 정보공유를 통해 사전 대응하고 있다. FISS의 검증된 데이터는 런던 경찰(City of London Police)이 운영하는 국가범죄수사국(NFIB, National Fraud Intelligence Bureau)[9]으로 보내져서 범죄수사 진행에도 지원한다.

영국 금융사기 대응기관(Financial Fraud Action UK) 발표에 따르면, 2011년 5월 기준으로 FISS에 가입된 은행 2곳에서 약 5.9백만 파운드(한화 약 100억원) 이상 손실을 예방하였다. 2009년 이후, 온라인 뱅킹 사기 손실액이 2011년까지 점진적으로 감소하였으나, 비즈니스 계정을 대상으로 한 범죄가 증가하면서 2014년의 피해액이 급격하게 증가하였다.

나.2. 이상행위 방지 서비스(CIFAS – UK's Fraud Prevention Service)

CIFAS(Credit Industry Fraud Avoidance System)[10]는 정부와 금융기관이 이상행위 정보를 이상행위 방지 데이터베이스를 통해서 데이터를 서로 공유할 수 있다. 특히, CIFAS 시스템을 통해 확인된 정보만 구별하여 의심되는 상세정보 뿐만 아니라 이상행위로 인해 오용되는 계좌정보, 보험, 기타 청구에 대한 정보도 교환한다.

CIFAS의 서비스는 이상행위 유형들(신분도용, 보험사기 등)을 분석 · 탐지하여 2013년도에는 전년도 대비 약 11%가량 사고를 감소시켰다. CIFAS에 의해 식별된 2013년 전체 사기 유형들 중 60% 이상은 은행 계정 탈취와 같은 신분 도용(Identity Fraud)[11]으로서, 약 12% 사고율을 감소시켰다

CIFAS는 신분 도용을 방지하기 위해 국가 이상행위 데이터베이스(National Fraud Database)를 활용하여 대응 중이며, 2가지 데이터베이스로 구성된다.

7 신용카드에 전자 칩을 내장하여 사용자가 서명 대신 비밀 번호를 입력하여 신분을 증명하게 하는 시스템이다.

8 온라인거래, 모바일 거래 등의 비대면 거래를 의미한다.

9 국가범죄수사국는 런던 경찰이 주관하는 전 세계에서 가장 발달된 경찰 정보 시스템(Police Intelligence System)들 중 하나로써, 이전에 서로 연결되어 있지 않은 수백만 개의 사기 기록들 처리하고 분석한다. 문제가 되는 금융 사기의 전체적인 그림을 제공함. 또한, 정부 지원을 받는 부서국으로서, 사기 범죄에 대응하여 경찰강력반과 공공 및 민간 기관과 파트너 관계를 맺는다.

10 1988년에 설립된 비영리 사기 방지 서비스 단체로써, 은행, 보험사, 카드사, 통신사, 공공기관 등 약 300여개의 회원사들로 구성된다.

11 개인의 생년월일, 재무 상세사항, 비밀번호 등과 같은 개인정보를 탈취하여 사기를 일으키는 범죄이다.

표 3. CIFAS의 국가 이상행위 데이터베이스 특징

종 류	특 징
국가 이상행위 데이터베이스 (NFD)	– 수십만 개의 사기 유형들이 기록된 데이터로, 상호 간의 데이터 공유를 가능케 함(매년 20만개 이상의 사기 유형들이 데이터베이스에 업데이트됨) – 저장된 사기 기록들은 자동으로 영국 국가범죄수사국(NFIB)을 통해서 경찰에 보고됨
내부 이상행위 데이터베이스 (IFD)	– 직원의 사생활을 보호하는 프레임워크 內에서 데이터를 공유 함으로써, 내부적 사기 발생률을 줄임

나.3. 금융 범죄경보 서비스(FCAS, Financial Crime Alerts Service)

영국은행가협회(BBA, British Bankers'Association)[12]는 금융 범죄 위협을 방지 할 수 있는 새로운 접근 방법의 일환으로 FCAS를 시작하였으며, 기술 파트너인 BAE Systems[13]에서 개발되었다. FCAS는 12개의 정부기관과 법 집행기관 그리고 국가 범죄 기관(National Crime Agency)과의 파트너 관계에서 정보공유(정부 및 법 집행기관의 데이터 활용)를 위해 국가 차원으로 금융 범죄에 대응한다.

FCAS는 금융권에 보다 더 특화되어 기존의 영국 은행들과 국가범죄수사국 사이에서 사용되고 있는 플랫폼기반으로 구축될 예정이며, 사이버 금융보안에 대한 취약점을 실시간으로 제공 가능한 정보 시스템으로 사이버 보안 위협, 금융범죄에 대응하는 역할을 수행한다. 2014년 9월 BBA발표에 따르면, FCAS는 기존 정보 공유 파트너쉽을 통해 약 1,700억원의 손실을 방지하였다.

2. 비금융권

비금융권에서는 기관과 민간이 서로 협력하여 사이버 위협 정보를 공유하기 위한 체계를 마련하였다. 국내뿐만 아니라 해외의 대응 현황에 대해 소개한다.

가. 국내 사례

가.1. 사이버위협정보 분석 공유시스템(C-TAS)

2014년 8월, 한국인터넷진흥원(KISA)에서 사이버 침해 사고에 대한 신속한 대응을 위해 각종 사이버위협 정보의 수집 · 분석 · 공유체계를 고도화한 사이버위협 정보 분석 · 공유 시스템인'C-TAS(Cyber Threats Analysis System)'를 본격적으로 운영하였다. C-TAS는 사이버위협 정보(악성코드 정보, 명령제어 서버 정보, 취약점 및 침해사고 분석정보 등)를 체계적으로 수집하고, 종합적으로 연관 분석해 관계기관 간 자동화한 정보 공유를 목적으로 하는 예방 · 대응 시스템이다.

그림 6. 사이버 위협정보 분석공유시스템

공유 정보는 5개 그룹(위협 도메인 · IP, 사이버사기 도메인 · IP, 악성 파일, 취약점, 보고서) 36종 정보(악성코드 유포지, 경유지, C&C, 공격 IP, 피싱, 파밍, CVE, PoC, 기술문서, 분석보고서 등)를 공유하고 있으며, 점차 수집 · 공유 항목을 확대 추진하고 있다. 외부로 제공되는 정보는 업종 별로 상이하다. 금융부문에는 공격 IP만을 제공하고 있으며, 게임부문에는 악성코드 유포지 URL, 경유지 URL, 어뷰징 공격 IP, C&C 도메인 및 IP, 공격 IP 등을 제공하고 있다.

각종 침해정보는 사이버 위협 정보 표현 규격CTEX(Cyber Threat Expression)으로 표시되어 통일된 형태로 자동 작성될 수 있도록 하며, 외부 기관으로 자동으로 전파될 수 있도록 한다. C-TAS와 C-TEXT는 유기적으로 연결된 침해사고 전반을 바라볼 수 있는 눈을 가지게 된 것으로써, 사고 발생 전 사이버 테러 이상 징후를 파악하여 선제적으로 대응하여 피해를 최소화하기 위해 노력하고 있다.

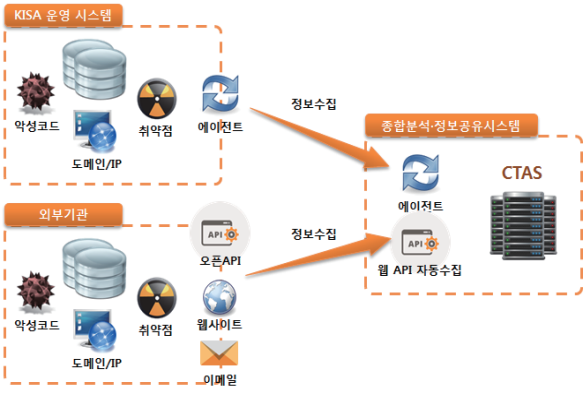

그림 7. 내 · 외부 위협정보 수집 체계

12 영국은행가 협회는 1919년에 설립된 비영리 기관으로써, 253개의 영국 은행 및 관련 금융기관을 회원사로 둔 기관이다.

13 영국의 방위산업체이다.

나. 해외 사례

나.1. (미국) 사이버 위협 정보 표현/전송 규격

국토안보부(DHS)는 사이버 위협에 효율적으로 대응하기 위해 안전한 정보공유 체계 구축의 필요성을 인지하고, 산하 MITRE를 통해 2013년 4월 사이버 위협 정보 전송 규격인 TAXII(Trusted Automated eXchange of Indicator Information)를 발표하고, 10월에는 사이버 위협 표현 규격인 STIX(The Structured Threat Information eXpression)를 발표하였다.

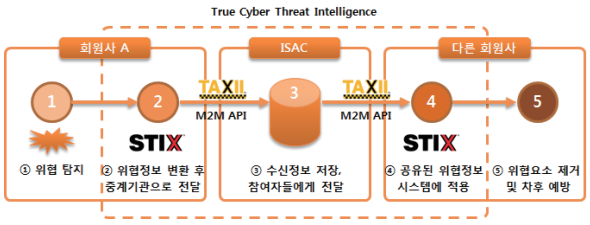

그림 8. STIX/TAXII 체계 구성 및 설명

STIX/TAXII는 ISAC(Information Sharing Analsis Center) 및 CSIRT(Computer Security Incidenct Response Team), 정보보호산업군 등 누구나 사용 할 수 있도록 개발하였다. STIX는 8가지 구성요소로 사이버 위협정보를 구조화하고, TAXII는 실시간으로 공유하기 위한 자동 전송 규격을 지원하기 위해 4가지 서비스 규격을 정의하고 있다. 또한, 참여조직간의 형태를 고려하여 3가지 모델(P2P, 중앙분배형, P2P-중앙분배 결합형)을 지원한다.

미국의 금융 ISAC에서는 사이버 위협 정보공유 체계를 구축하고 있으며, 이를 금융기업, 지자체, FBI, US-CERT 등이 활용하고 있다. 앞서 소개한 KISA의 C-TAS또한 STIX/TAXII를 참조하여 개발되었다.

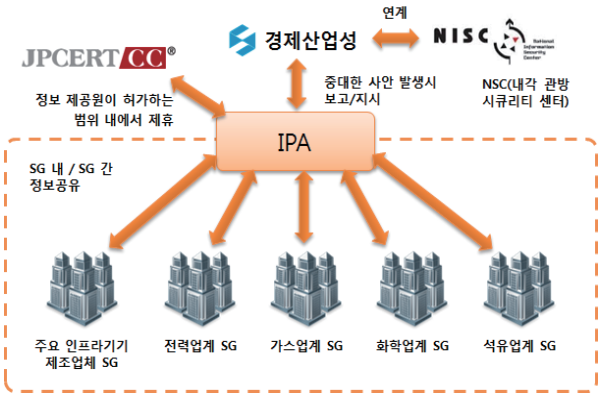

그림 9. IPA 및 참여기업, 관계기관 간 정보공유 관계도

나.2. (일본) 사이버 정보 공유 이니셔티브(J-CSIP)

IPA(Information-technology Promotion Agency)[14]기관의 J-CSIP(Initiative for Cyber Security Information sharing Partnership of Japan)를 중심으로 정보공유가 이루어지고 있다. IPA는 사이버 공격을 대응하기 위해 5대 산업, 45개 참여기업(13.12월 기준) 정보공유 체계를 발족 · 운영한다. 정보공유에 대한 정책 및 운영은 IPA와 참여기업 SIG(Specfial Interest Group)간 NDA를 체결한 것으로 시작되고, 참여기업은 정보제공처에 대한 정보와 민감한 정보를 익명화하여 탐지된 사이버 공격 정보를 IPA에 제공하면, 분석정보를 추가하여 정보제공자의 승인을 얻어 공유 가능한 정보를 공유한다.

정보공유 체계를 확립한 후 단순히 정보가 공유되는 것이 아니라 공격동향 및 공격의 상관관계에 대해 파악이 가능해졌다. IPA는 통합거점으로 역할을 수행함에 따라 분석정보의 생산 및 향후 예상되는 고객에 대한 대책검토가 가능해졌다. 공공기관인 IPA가 허브위치를 담당함으로서 사업자의 이해관계를 중재할 수 있으며, DNA를 전제로 하기 때문에 정보 제공 및 공유 시 신속한 판단 및 대응이 가능하다는 이점이 있다. 신속한 정보공유는 전체에 효과적인 공격 탐지 및 방어가 가능하며, 아래는 정보공유의 선례이다.

V. 결 론

이상행위 탐지시스템은 다양한 분야에 적용되어 활용되고 있으나, '수집 ▶ 분석(탐지) ▶ 대응'의 3가지 핵심 기능은 변함이 없다. 다만, 어떠한 정보를 수집하고 분석하는가에 차이점이 존재할 뿐이다. 일부 금융회사에서는 이상금융거래 탐지시스템을 활용하여 내부감사 기능을 추가하여 활용하기도 한다. 분석하는 수집과 분석하는 방법의 차이가 있을 뿐 핵심 기능이 추가로 요구되는 것은 아니기 때문이다. 하지만 데이터가 수집되는 저장소가 외부로 노출될 경우 커다란 문제를 발생시킬 수 있기 때문에, 각기 다른 시스템을 가지고 통합관리 할 수 있는 구조로 만드는 것이 보다 안전하게 운영할 수 있는 방법이라고 생각된다.

또한, 영국의 사례와 같이 다양한 범죄를 예방하기 위해 통합전략을 수립하고, 개인과 기업을 보호하기 위한 의무로서 적극적으로 개입하였다. 영국정부는 이상행위를 심각한 사회문제로 인식, '2005년 Fraud Review'를 시작으로 방지 대책 마련에 본격적으로 돌입하였다. 이후 법 제정, 기구 설립, 정보 공유 등을

14 日 경제산업성 산하의 IT, 정보보안 관련 전문기관이다.

제안하였으며, 2008년 10월 NFA(National Fraud Authority)가 설치되면서 국가차원에서의 전략 수립, 공 · 사협조체계 강화, 공 · 사 · 민관간 정보공유, 정보공유 시 중복 또는 충돌 문제 해결, 교육 및 홍보 등의 업무를 수행하고 있다.

현재 국내 금융권에서는 이상행위 탐지 정보 공유 시스템을 구축함으로써 체계적인 대응을 준비해 나아가고 있다. 효율적으로 활용하기까지는 많은 시행착오를 겪게 될 것이며, 다양한 보안위협 및 관련 법 이슈 등이 존재 할 것이다. 하지만 영국의 선진사례를 통해 문제를 해결해 나감으로써, 개인과 기업 나아가 국가적인 손실을 막는데 크게 이바지 할 수 있을 것이다.

약 력

임 형 진

2006년 성균관대학교 공학박사
2007년~2015년 금융보안연구원 보안기술연구팀장
2011년~2015년 ITU-T Recommendation X.1157(FDS) 에디터
2015년~현재 금융보안원 보안기술연구팀
관심분야: 금융보안, 핀테크 보안, 개인정보 비식별처리

참고문헌

[1] 매경이코노미, "국내 핀테크 현황 :'페이'열풍 넘어 P2P · 블록체인 다변화", 2016.
[2] 영국중대(重大) 부정 단속국(SFO, Serious Fraud Office), http://www.sfo.gov.uk/
[3] Lim HyungJin, et al., "Recommendation X.1157 : Technical capabilities of fraud detection and response for services with high assurance level requirements", ITU-T, 2015.
[4] 임형진, 한승우 외, "이상금융거래 탐지시스템 가이드", 금융보안연구원, 2014.
[5] 임형진, "이슈리포트 : 최신 해외 금융보안기술 현황 및 전망", 금융보안연구원, 2011.
[6] 보험개발원, http://www.kidi.co.kr/
[7] 한국은행, http://www.bok.or.kr/
[8] 한승우, "CINDER(Cyber Insider Threat) 프로젝트 소개와 해외 동향 보고서, 금융보안연구원, 2014.
[9] KIRI Weekly 제 231호, "부정행위 방지를 위한 공공기관간 · 공사기관 간 정보공유에 대한 소고", 2013.4.29.
[10] 박철민, 조정식, "국외 사이버 위협 정보공유의 체계조사", 한국인터넷진흥원 Report, 2014.1.
[11] Financial Fraud Action UK, "Fraud The Facts 2015", 2015.
[12] 한승우, "금융권 이상행위탐지기술 이용현황 및 전망", 전자금융과 금융보안, 2015.7.