

「제3회 금융보안원 논문공모전」

수상 논문집

| 대 상 |

- 특징 벡터 확장과 인공지능을 이용한 보안관제 규칙 생성 연구

| 최우수 |

- ETIR 모델 기반 SOAR 금융보안관제 설계 및 구축

| 우 수 |

- 2014년 카드정보 유출대란 이후 개정된 개인정보보호법 39조의 징벌적 손해배상 적용에 관한 법적 및 법경제학적 효용성 검토

| 장 려 |

- 금융 데이터 비식별화가 분석 모형 성능에 미치는 영향 연구
- 인슈어테크 산업 발전을 위한 규범 혁신 제안

특징 벡터 확장과 인공지능을 이용한 보안관제 규칙 생성 연구

명준우* · 김영재* · 문다민* · 허준녕* · 윤명근*

* 국민대학교 컴퓨터공학과

요 약

디지털 트랜스포메이션 시대를 맞아 금융보안 분야에도 인공지능 기술의 도입이 활발히 진행되고 있다. 특히, 보안관제 분야는 인공지능 기술이 접목되었을 때 기존에 사람이 직접 처리하고 있는 업무 중 단순 반복적 성격이 강한 업무들이 효과적으로 자동화될 수 있을 것으로 기대된다. 대부분의 보안관제센터에는 오랜 기간 관제요원들의 업무 경험을 축약시켜서 만든 침입탐지 이벤트 자동 처리 규칙들이 소프트웨어로 구현되어 실행된다. 이 규칙들은 사이트의 특성이 반영되어야 하므로 사람의 손으로 직접 개발되어 자주 업데이트가 되고 있으며, 따라서 규칙 관리의 어려움과 오류 발생의 위험이 존재한다. 본 논문에서는 일정 기간 수집된 보안관제 이벤트 데이터와 머신러닝 기술을 이용해서 자동으로 규칙 알고리즘을 구현해주는 인공지능 기술을 제안한다. 기존 연구와 다르게 침입탐지 이벤트에 등장하는 특징들을 그대로 사용하지 않고, 일부 특징을 자연어처리 방식으로 확장시킨 후 기존 특징들과 다시 결합하여 사용하는 방법을 제안한다. 또한, 인공지능이 올바르게 동작할 수 없는 학습데이터 부족 상황을 인식하게 하여 판별을 미루도록 하는 웨이버(waiver) 기술도 최초로 제안한다. 실제 보안관제센터에서 장기간 수집된 2백만 건 이상의 침입탐지 이벤트 데이터를 사용해서 실험한 결과, 본 논문에서 제안하는 방법은 보안관제요원이 수작업으로 개발한 이벤트 자동 처리 규칙 소프트웨어와 거의 동일한 성능을 보이는 것으로 확인되었다. 본 논문의 기술을 이용하면 보안관제요원들이 수작업으로 침입탐지 이벤트 처리 알고리즘을 개발 및 업데이트할 필요가 사라지므로 시간 소모적이고 오류가 잘 발생하는 작업을 크게 개선할 수 있으며, 관제요원들은 단순 형태의 사이버 공격은 인공지능에 맡기고 복잡한 사이버 공격을 탐지하고 분석하는 본연의 주요 업무에 더 집중할 수 있게 될 것이다.

키워드

특징 확장, 머신러닝, 침입탐지, 보안관제

목 차

I. 서론	(3)
II. 기술 동향	(6)
1. 해외 연구 동향.....	(6)
2. 국내 연구 동향.....	(10)
III. 인공지능 기반 침입탐지 이벤트 분석 연구.....	(12)
1. AIDE (AI-based intrusion DEtection) 구조.....	(12)
2. 특징 추출 및 확장.....	(14)
3. 신규 이벤트 웨이버	(17)
IV. 실험 및 검증	(20)
1. 실험 환경.....	(20)
2. 탐지 이벤트 분류 알고리즘 비교.....	(21)
3. 신규 이벤트 웨이버.....	(26)
V. 결론	(29)
참고문헌	(30)

I. 서론

인공지능은 디지털 트랜스포메이션 시대의 핵심기술로서 인식되고 있으며, 특히 빅데이터에 기반한 머신러닝 기술의 발전은 다양한 산업 분야에서 업무 방식에 큰 변화를 가져올 것으로 기대된다. 사이버보안과 금융보안 분야에서도 인공지능 기술을 도입하려는 시도가 활발히 진행되고 있다. 보안 분야에서는 전통적으로 악성코드와 보안관제 이벤트 데이터가 대량으로 생산되어왔으나, 그동안은 엄청난 데이터 양에 비해서 컴퓨터 자원과 인력이 부족하여 극히 제한된 분야에서만 데이터 기반의 업무 효율화가 시도되었으며 효과도 미비했다.

최근에는 컴퓨터 하드웨어의 비약적 성능 향상, 그리고 딥러닝을 중심으로 머신러닝 알고리즘의 발전과 대중화 성공에 힘입어 그동안 금융보안 분야에서 활용되지 못했던 빅데이터들이 본격적으로 연구 분석의 대상이 되고 있다. 보안 분야에서 가장 대표적인 빅데이터 분석 분야는 악성코드 분석과 보안관제 로그 분석이다. 하루에도 수십~수백만 건 이상이 발생하는 것으로 알려진 악성코드는 오래전부터 인공지능 기반의 분석 기술을 적용하기에 좋은 대상이었다[1][5]. 다수의 정보시스템과 보안 장비로부터 생성되는 이벤트 및 알람 로그도 이제는 인공지능 기술로 분석해 볼 만한 시대가 열린 것이다[2][4][6].

본 논문에서는 보안관제센터에서 발생하는 알람 이벤트 데이터를 학습하여 보안관제요원들이 장시간에 걸쳐 수작업으로 생성한 이벤트 처리 규칙과 거의 동일한 성능을 낼 수 있는 인공지능 기술을 제안한다. 국내 최대 보안관제센터 중 한 곳으로부터 8개월간 수집된 침입방지시스템(Intrusion Prevention System) 실제 로그 2백만 개 이상의 데이터를 사용하여 제안하는 기술의 우수성을 실험으로 검증하였다. 최종적으로 제안하는 기법은 정확도 99.97%, 정밀도 99.72%, 재현율 99.92%에 달하는 우수한 성능을 낼 수 있었다.

본 논문에서 제안하는 보안관제 인공지능 기술이 우수한 성능을 낼 수 있었던 이유는 크게 두 가지 새로운 기법이 도입되었기 때문이다.

첫째, 본 논문에서는 특징 확장이라는 새로운 특징 가공 기술을 제안한다. 침입방지

시스템 로그 데이터로부터 머신러닝을 위해서 특징을 추출하는 전통적인 방법은 각 기본 특징 필드(예: 출발지IP, 목적지IP, 수집장비, 이벤트명 등)값을 그대로 사용하거나, 긴 특징 필드 하나를 선택하여 여러 개의 특징들을 생성하는 방식이었다. 본 논문에서는 패킷(packet)의 페이로드(payload) 부분을 자연어처리 분야에서 자주 사용하는 DF(Document Frequency) 방식을 적용하여 여러 개의 특징들로 확장시켜 추출한 후, 다시 전체 기본 특징들과 통합하여 머신러닝을 위한 최종 특징 벡터를 생성해내는 새로운 기술을 제안하며, 이를 특징 벡터 확장 기법이라고 부른다.

둘째, 보안 전문가도 예측 불가능한 신규 이벤트명에 대해서는 머신러닝의 판단을 보류시키는 웨이버(waiver) 기법을 최초로 도입하였다. 침입방지시스템은 스트림매칭이나 통계적 측정량에 기반하여 침입탐지 알람을 생성하는데, 이러한 기준이 새롭게 업데이트가 되어 이전에 없던 새로운 이벤트명이 추가되는 경우가 있다. 이러한 경우는 일반적으로 과거 데이터만으로 학습한 모델로는 올바르게 분류하는 것이 불가능한데, 이는 보안 전문가들도 마찬가지이다. 새로운 이벤트명이 추가된 경우에는 보안 전문가들도 상당 기간 지켜보고 분석 과정을 거친 후에 정답인지 오답인지를 판별할 수 있기 때문이다. 따라서 학습데이터에서 등장하지 않았던 새로운 이벤트가 테스트 데이터에 처음으로 등장하는 경우는 머신러닝의 판단을 보류시키고 학습이 가능한 최소한의 데이터가 수집된 후 재학습시키는 방법을 도입한다.

우수한 정보 수집 능력과 연구 능력을 보유한 해외 보안 대기업에서는 보안관제 빅데이터에 기반한 머신러닝 기술이 새롭게 연구되고 있다[2][4][6]. 아쉽게도 국내는 데이터 공유와 산학 협력이 선진국처럼 활발히 진행되지 못하고 있어서 보안관제 데이터를 이용한 우수한 연구 논문이 발표되지 못하고 있는 실정이다. 본 논문에서는 국내 논문으로서는 매우 드물게 실제 보안관제센터로부터 장기간 수집되고 보안관제요원들이 정제된 라벨을 부여한 데이터 셋을 이용해서 머신러닝 기법으로 이벤트 분류에 성공한 인공지능 기법을 제안하며, 실제 데이터로 검증하였다. 본 논문의 장점과 의미를 요약하면 다음과 같다.

- 보안관제 로그 특징을 확장시키고 머신러닝 학습을 진행하는 새로운 기법을 제안한다. 보안관제 로그 이벤트 중 일부 필드를 자연어처리 기술로 분석하고 대표 특징들을 추출한 후, 원래 보안관제 로그에 포함되어 있던 다른 기본 특징들

과 합쳐서 머신러닝을 적용함으로써 정탐과 오탐의 분류 정확도를 높이는 새로운 기술을 제안한다.

- 보안 전문가도 예측이 불가능한 신규 탐지 이벤트명에 대해서는 인공지능이 판단을 보류하도록 하는 웨이버 기법을 새롭게 제안한다. 학습데이터에 등장하지 않았던 새로운 이벤트에 대해서는 최소한의 학습 데이터가 모일 때까지 기다렸다가 재학습을 진행함으로써 인공지능이 무의미하게 예측을 틀리게 하는 상황을 줄이게 된다.
- 국내 주요 보안관제센터에서 수집되고 관제요원에 의해서 라벨이 부여된 양질의 실제 보안관제 로그 데이터를 사용하여 머신러닝 학습과 테스트 실험을 진행하였다. 본 논문에서 제안하는 기법은 보안관제요원들이 장기간에 걸쳐 생성한 정탐/오탐 이벤트 판별 규칙과 비교했을 때 정확도 99.97%, 정밀도 99.72%, 재현율 99.92%에 달하는 우수한 성능을 내는 것을 확인하였다.

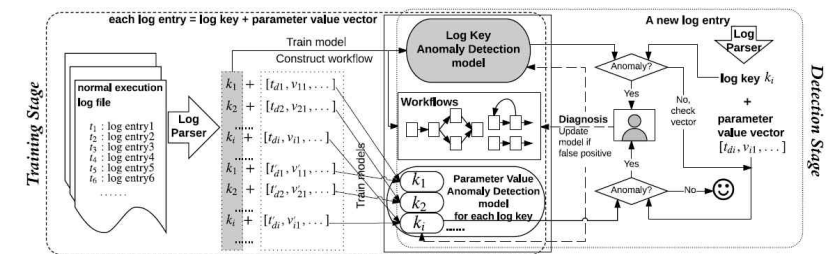
II장에서는 보안관제 데이터 분석과 인공지능 기술을 연계시키는 최신 연구 동향에 요약한다. III장에서는 본 논문에서 제안하는 인공지능 보안관제 기술을 제안한다. IV장에서는 실제 실험을 통해서 본 논문에서 제안하는 모델의 우수성을 검증하고, V장에서 결론을 맺는다.

II. 기술 동향

보안관제 로그 분석 연구는 ESM(Enterprise Security Management) 장비가 본격적으로 사용된 2000년대 초반부터 시작되었다[1]. 최근에는 SIEM(Security Information and Event Management)이라는 이름으로 불리고 있으며, 각종 보안장비와 서버, 통신장비 등으로부터 로그를 중앙 서버로 수집하고 분석 과정을 거쳐 이상징후 탐지와 공격 탐지를 수행한다. 로그 분석 기술의 주요 연구 대상은 데이터 수집, 저장, 가공, 분석 등 다양하며, 최근에는 빅데이터 플랫폼과 데이터마이닝, 인공지능 기반의 고급 분석 기술에 대해서 다양한 연구가 활발히 진행되고 있다.

1. 해외 연구 동향

최근 딥러닝이 인공지능 분야의 발전을 이끌고 있다. 이러한 연구 동향은 보안관제 데이터 분석 분야에도 영향을 주고 있다. 딥로그(DeepLog) 기술은 딥러닝 중에서도 RNN(Recurrent Neural Network)을 사용해서 시스템 로그에 대한 이상징후를 탐지한다[2]. 딥로그는 시스템 로그를 키(key) 부분과 인자(parameter) 부분으로 분리하며, 각각에 대해서 이상징후 발생을 찾는다. 정상 시스템 로그를 모은 학습데이터로부터 키 부분의 시퀀스(sequence)를 RNN에 학습시킨다. 학습된 RNN은 N개의 로그 시퀀스가 주어졌을 때 다음번 로그에 대한 예측값을 확률로서 생성할 수 있다. 높은 확률을 배정받은 상위 g개의 예측 로그 값들이 실제 로그 값을 포함하면 정상인 상황으로 판단하며, 그렇지 않으면 이상징후로 판단한다. <그림 1>은 딥로그 기술의 전체적인 구성과 동작 방식을 요약하고 있다.

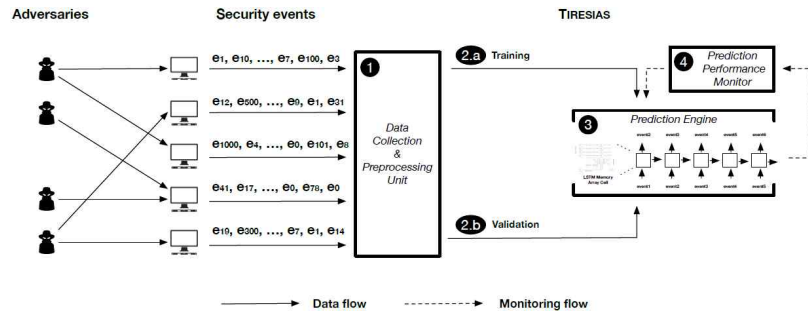


<그림 1> RNN을 사용하여 이상 징후 탐지를 시도하는 딥로그의 전체 구성도[2].

딥러닝 이전에도 전통적인 n-그램 언어 모델을 사용해서 이상징후를 탐지할 수 있

다 [3]. 학습 데이터에서 n 개의 시퀀스가 등장했을 때 다음으로 등장할 단어를 조건부 확률로서 계산이 가능하다. 딥로그 논문에 의하면 RNN을 사용하는 방식이 전통적인 n -그램 방식보다 우수한 성능을 보인다고 한다[2].

티레시아스(Tiresias) 논문에서는 호스트형 침입방지시스템(host-based intrusion prevention system)으로부터 침입탐지 이벤트를 수집하여 데이터 셋으로 사용하고 RNN 학습을 통해서 딥러닝 모델을 만드는 연구를 수행했다[4]. 로그 시퀀스를 RNN에 학습시키고 나면, 일정 개수의 로그 시퀀스를 RNN에 입력시켰을 때 다음번에 생성될 침입탐지 이벤트를 생성하는 것이 가능해진다. 정확도는 대략 90% 전후로 나온다. 저자들은 740,000대의 시만텍 IPS 장비로부터 4개월간 34억 개의 탐지 이벤트(서로 다른 이벤트 개수는 4,495개)를 수집하여 실험을 진행했다. RNN의 로그 이벤트 시퀀스 길이는 2-9를 학습시키고 다음번 로그 이벤트를 예측하게 하였다. <그림 2>는 티레시아스의 전체 구조를 보여준다.



<그림 2> 티레시아스: 침입방지시스템 로그를 RNN 학습하여 다음번 발생 이벤트를 예측하는 연구[4]

올해 발표된 테서랙(Tesseract) 논문에서는 최근 많이 진행되는 안드로이드 악성앱을 머신러닝으로 분류하는 연구들이 잘못된 실험 방법론을 사용하고 있다는 것을 지적한다[5]. 주제는 악성 앱이지만 동일한 비판이 보안관계 로그 분석 연구와 더 나아가서 모든 보안데이터 분석 연구에 대해서 유효하다. 저자들은 기존 연구들에서는 공간적 바이어스(spatial bias)와 시간적 바이어스(temporal bias)가 실험 데이터 셋에 반영되었기 때문에 거의 완벽한 머신러닝 정확도 결과물이 나왔다고 지적한다. 공간적 바이어스란 실제 정상앱과 악성앱의 비율을 고려하지 않고 실험실 환경에서 악성앱의 비율을 비정상적으로 높게 학습시키기 때문에 모델이 악성앱을 잘

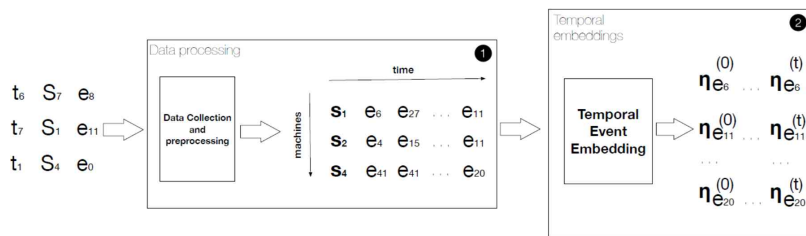
탐지하는 것으로 왜곡되게 학습이 된다는 현상을 나타낸다. 시간적 바이어스란 학습 데이터와 테스트 데이터가 특정 시점을 기준으로 앞쪽과 뒤쪽의 데이터로 나뉘어져야 하고, 동시에 정상과 악성 데이터가 비슷한 시점에 수집된 데이터여야 하는데, 기존 연구에서는 데이터 셋이 이렇게 구성되지 못하여 악성과 정상을 나누는 기준이 엉뚱한 곳에서 학습되어 모델의 성능이 좋게 보일일 수 있다. 예를 들어 악성데이터는 2018년에 수집하고 테스트데이터는 2019년에 수집했는데, 중간에 API 라이브러리가 업데이트되어 테스트데이터에는 특정 새로운 API가 포함되어 있다면 인공지능 모델은 이 API의 유무를 따져서 정상과 악성을 분류하게 된다. 주어진 데이터 셋에 대해서 정확도는 높아질 수 있겠지만 결코 바람직한 모델이 개발된 것이 아니며, 실제로 이런 모델은 데이터 셋이 바뀌면 형편없이 정확도가 낮아지게 된다. <그림 3>은 테서랙에서 공간적 바이어스와 시간적 바이어스 때문에 측정 지표 값이 우수하게 나온 모델들이 데이터 셋을 바꾸자 형편없이 지표가 나빠지는 것을 보여준다 (예: 0.97 --> 0.32).

Experimental setting	Sample dates	% mw in testing set Ts							
		10% (realistic)				90% (unrealistic)			
		% mw in training set Tr				% mw in training set Tr			
		10%	90%	10%	90%	10%	90%	10%	90%
	Training	ALG1 [4]		ALG2 [33]		ALG1 [4]		ALG2 [33]	
10-fold CV	GW: ■■■■■■	■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■	
	MW: ■■■■■■	■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■	
Temporally inconsistent	GW: ■■■■■■	■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■	
	MW: ■■■■■■	■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■	
Temporally inconsistent gw/mw windows	GW: ■■■■■■	■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■	
	MW: ■■■■■■	■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■	
Temporally consistent (realistic)	GW: ■■■■■■	■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■	
	MW: ■■■■■■	■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■		■ ■ ■ ■ ■	

<그림 3> 공간적 바이어스와 시간적 바이어스로 실험 데이터에 따라 성능 지표(F1스코어)가 크게 차이남을 보인 테서랙(Tesseract) 연구 [5]

자연어처리 분야에서 큰 성공을 거둔 word2vec 임베딩 모델을 보안데이터 분석에 활용하려는 연구가 시도되고 있다[6]. Shen 등은 Attack2vec을 최초로 제안하였는데, 침입방지시스템의 침입탐지 이벤트를 워드로 보고 로그 데이터를 자연어처리에서의 문장으로 간주하여 인공지능 학습을 진행하였다. 이러한 연구가 진행된 배경에는 사이버공격이 진행될 때 다양한 공격기술이 동시에 사용되는 경우가 많으며, 어떤 경우에는 여러 대의 보안장비에서 동시에 동일한 공격 시도가 목격되기 때문이다[4][7]. 즉, 특정 사이버 공격이 발생하면 침입탐지 이벤트 로그 중 몇 개가 그룹으로 발생하는 경우가 많으며, 이러한 로그 그룹을 해당 사이버 공격을 기술하는 특징으로 해석하자는 것이 핵심 아이디어다. 저자들은 시만텍 침입방지시스템에서

발생한 로그 기록을 문서로 간주하고, 중간 단어(이벤트)를 기준으로 앞뒤 각 여덟 개의 단어로 구성된 크기 17짜리 단어 윈도우를 사용하여 워드 임베딩을 구현했다. 2년 동안 수집된 침입차단시스템의 탐지 로그 1억 9천만 개를 학습 데이터로 사용하였으며, 서로 다른 이벤트의 개수는 8,000개이다. 입력층과 출력층은 원핫인코딩(one-hot-encoding)으로 크기 8,000의 벡터를 사용했으며, 임베딩층은 크기 50까지 벡터를 사용했다. <그림 4>는 attack2vec에서 워드 임베딩을 시키는 과정을 보여준다. s_i 는 서로 다른 침입방지시스템을 나타내며, e_j 는 이벤트명, t_k 는 수집된 시간을 표시한다. 임베딩 과정을 거치게 되면, 수집 기간 t_k 에 해당하는 e_j 의 임베딩 벡터는 $\eta_{e_j}^{(k)}$ 로 표시한다.



<그림 4> Attack2Vec에서 침입탐지 이벤트를 워드로 간주하여 임베딩시키는 과정[6]

Attack2vec에서 흥미로운 부분은 임베딩이 끝난 후 각 이벤트는 고유한 벡터로 환산될 수 있고, 따라서 이벤트간에 코사인 유사도 공식에 의한 유사도 계산이 가능해진다는 점이다[6]. 실제로 논문에서는 특정 이벤트가 주어졌을 때, 이와 가장 유사한 이벤트들을 찾아서 동시에 진행되는 공격 기법들로 해석한다. 또한, 임베딩을 1주일 단위로 재계산하는데, 벡터값이 많이 변경된 이벤트는 해당 공격 기법이 통하는 취약점이 공개되는 경우가 많았다는 흥미로운 분석결과를 제공한다. 이런 상황은 이벤트에 해당하는 과거의 벡터값과 현재의 벡터값을 코사인유사도로 유사도를 측정했을 때 유사도 값이 낮게 나오는 것으로 판별할 수 있다.

보안관제 로그의 양이 많아서 모두 처리할 수 있을 만큼 충분한 장비와 인력 확보가 어렵다는 것은 오래된 심각한 문제이다. 최근 파이어아이의 보고서에 따르면 전 세계의 37%의 기관에서는 매달 10,000개 이상의 이벤트 알람이 발생하고 있다고 한

다[8]. 이 수치는 하루에 1,500개 이상에 해당하며, 한 시간에 70개에 달한다. 특수 기관 몇 곳을 제외하고는 보안 인력이 적절히 처리하는 것이 불가능한 분량이다. 대부분의 알람은 오탐(false positive)에 해당하는데, 문제는 보안 인력들이 오탐 처리에 피로감을 느껴 진짜 공격이 진행되어도 분석을 하지 못한다는 점이다. 팔로알토의 보고서에서도 보안 도구에서 생성되는 알람 중 14% 만이 처리되고 있다고 한다[9]. 이러한 현상은 알람 피로(alert fatigue)라고 불리고 있으며, 올바른 보안관제 업무를 위해서 반드시 해결되어야 한다. 해결방법은 결국 오탐을 줄이는 것인데, 이 과정에서 설령 일부 사이버 공격 신호를 감지하지 못하더라도 오탐을 줄여야 한다고 파이어아이 보고서는 주장한다[8].

2. 국내 연구 동향

해외 주요 대학과 연구 기관이 보안관제에 딥러닝과 머신러닝 기술을 본격적으로 도입하고 있는 반면, 국내에서는 아직까지 전통적인 규칙 기반으로 업무를 진행 중인 경우가 많다. 최근에는 국내에서도 인공지능 기술을 보안관제 분야에 적용하려는 시도가 있으며, 아직 해외에 비해서 실제 데이터를 기반으로 실험을 진행하고 딥러닝의 첨단 기술을 적용하는 연구는 미비한 실정이다.

[1]에서는 인공지능 기반의 금융권 보안관제에 대한 국내외 동향 및 향후과제에 대해서 조사하였다. 인공지능과 보안에 대한 개요와 현재 침해데이터 공유 현황, 특히 국내외 주요 기관과 보안 업체들의 동향에 대해서 잘 정리하였다.

신익수 등은 IDF 보안이벤트를 분류하는 SVM(Support Vector Machine) 기계학습 모델을 제안하였다[10]. 과학기술사이버안전센터에서 수집한 실제 보안관제 데이터를 사용해서 실험을 진행하였으며, 침입탐지시스템의 기본적인 7개의 특징에 신규로 정의한 10개의 특징을 추가하여 F1 스코어 성능을 높일 수 있었다. <표 1>은 기본 7개의 특징과 새로 정의된 10개의 특징을 요약한다.

[11]에서는 오픈소스 플랫폼과 딥러닝 학습 도구를 이용하여 보안관제 로그를 분석하는 기술을 제안한다. 이상징후 탐지를 위해서 요구되는 사항들과 최근 많이 활용되고 있는 오픈소스 기반의 빅데이터 저장 및 처리 플랫폼, 그리고 딥러닝 개발 도구들에 대해서 조사하였다.

III. 인공지능 기반 침입탐지 이벤트 분석 연구

[12]에서는 자연어처리 분야에서 많이 사용하는 TF-IDF(Term Frequency-Inverse Document Frequency)를 웹 트래픽 분석에 적용하여 침입탐지 이벤트의 유효성을 검증하는 방법을 제안하였다. 웹 응답 트래픽에 포함되어 있는 웹 문서를 자연어 문장으로 간주하여 TF-IDF 가중치를 부여하여 취약하지 않은 문장을 구별하려는 연구를 시도했다.

구분	특징
기본 특징	source IP
	destination IP
	source port
	destination port
	event class
	priority
	protocol
추가 특징	Is source IP in the target network?
	Is source IP in the target network?
	Does the payload have 'Referer' ?
	Does the payload have '200 OK' ?
	How many does the payload have security-related strings?
	The TTL value in the payload
	The length of the payload
	Does web-server use common port?
	Which form does the payload use for 'Host' ?
	What kind of 'User-agent' does the payload use?

<표 1> [10]논문에서 사용한 침입탐지시스템 기본 특징과 추가된 특징

1. AIDE (AI-based intrusion DETection) 구조

본 논문에서는 자연어처리 기법을 적용하여 확장된 특징 벡터를 기반으로 보안관제 규칙을 생성하는 인공지능 모델인 AIDE(AI-based intrusion DETection)를 제안한다. AIDE는 침입탐지 이벤트로부터 추출 가능한 특징 정보를 일차적으로 추출하여 특징 벡터로 만들고, 확장 가능한 특징 정보를 선택하여 텍스트마이닝 기법인 DF(Document Frequency)를 계산하고 DF 값이 큰 상위 n개의 단어를 선정한 후 해당 단어들의 출현 여부를 특징 정보로 사용한다. 이는 단순히 하나의 값을 가지던 특징 정보를 유의미하게 확장하여 모델 학습에 더 많은 단서를 제공할 수 있는 기술이다.

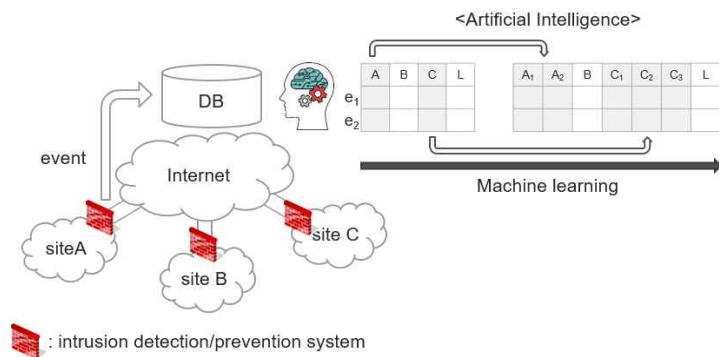
AIDE 연구에서는 기존 보안관제 이벤트가 라벨(label)이 결정되어 있다고 가정한다. 실제 실험에서 사용한 데이터도 국내 보안관제 센터로부터 수집된 이벤트 데이터셋이며 보안관제요원들이 수작업으로 라벨을 붙여놓은 상황이다. 라벨이 붙은 보안관제 이벤트를 학습 데이터로 사용하기 때문에 지도학습(supervised learning)을 사용하여 머신러닝 모델을 개발한다.

AIDE의 아키텍처는 <그림 5>와 같다. 먼저 침입탐지 이벤트는 여러 곳에 설치된 침입방지시스템(Intrusion Prevention System)을 통해 수집된다. 침입방지시스템은 네트워크를 지나가는 패킷을 조사하여 특정 스트링이나 시그니처(signature)를 포함하거나 일정한 통계적 값을 만족시키면 그에 해당하는 이벤트를 발생시킨다. 문제는 이벤트가 발생했다고 하여 실제 공격이 발생한 것은 아니기 때문에, 보안관제요원들은 이벤트에 대한 분석을 실시하여 정탐(true positive)과 오탐(false positive)을 구분하여 해당 이벤트에 정탐 또는 오탐 라벨을 붙인다. 라벨을 붙이는 방식은 보안관제센터별로 다르며 오랜 기간 축적된 경험과 사이트 특성이 반영되어 있다. 이벤트는 엄청난 숫자가 반복적으로 발생하기 때문에 정탐과 오탐의 기준을 규칙으로 만들고 소프트웨어로 구현하여 특정 조건을 만족하는 이벤트들은 규칙 소프트웨어

1) 본 논문에서는 이벤트(event), 알람(alarm), 로그(log)를 혼용하여 사용하며, 별다른 설명이 없는 경우 침입방지시스템이 발생시킨 것으로 간주한다.

에 의해서 자동으로 오탐과 정탐으로 분류가 된다. 이러한 규칙 소프트웨어는 사람의 손으로 직접 관리가 되므로 상당한 인적 자원이 투입되고 사람에 의한 오류 발생 가능성이 존재한다. AIDE는 이러한 수동 분석을 데이터에 기반한 머신러닝 방식으로 대체한다.

AIDE에서는 수집된 이벤트로부터 추출된 특징 정보들을 머신러닝 모델의 입력으로 사용되기 위해 특징 정보를 가공 및 확장하여 고정 크기의 벡터로 변환한다. 생성된 특징 벡터를 기반으로 머신러닝 모델의 학습이 진행되며, 완성된 학습 모델은 테스트데이터에 속한 이벤트에 대해 정탐 혹은 오탐으로 이진분류를 수행한다. 본 논문에서는 랜덤포레스트(Random Forest)를 사용하여 인공지능 모델을 개발하였다 [13]. 또한, 테스트 단계에서는 학습데이터에서 등장하지 않은 신규 이벤트에 대해 예측을 보류하는 기법을 선택적으로 적용할 수 있다.



<그림 5> 보안관제 규칙 자동 생성 인공지능(AIDE) 아키텍처

AIDE에는 새로운 특징 확장 기술과 신규 이벤트 웨이버 기법이 도입되었다. 먼저 특징 확장 기술은 학습 모델의 입력으로 사용하기 위해 선별된 특징을 그대로 사용하지 않고, 다양한 정보가 포함된 몇 개의 특징의 경우는 자연어처리 기법을 적용하여 다시 여러 개의 특징으로 유의미하게 확장한다. 그리고, 기존 특징들과 확장된 특징을 하나로 합쳐 머신러닝의 학습 입력 값을 생성한다. 신규 이벤트 웨이버 기법은 학습 이벤트에 등장하지 않았던 이벤트가 테스트 대상이 될 경우, 해당 이벤

트의 예측을 보류하는 기법이다.

본 연구에서는 특징 확장 기술을 적용하지 않은 모델 성능에 비해 2.4% 높은 성능인 99.92%의 성능을 얻음으로써 특징 확장 기술의 실효성을 증명하였으며, 신규 이벤트 웨이버 기법까지 적용하였을 때 AIDE 모델은 99.97%의 정확도를 보이며 보안 관제요원이 수작업으로 개발한 이벤트 자동 처리 규칙 소프트웨어와 거의 동일하게 동작하는 것이 확인되었다. 이는 본 논문의 기술을 이용하면 보안관제요원들이 수작업으로 침입탐지 이벤트 처리 알고리즘을 개발 및 업데이트할 필요가 사라지므로 시간 소모적이고 오류가 잘 발생하는 작업을 크게 개선할 수 있으며, 관제요원들은 단순 형태의 사이버 공격은 인공지능에 맡기고 복잡한 사이버 공격을 탐지하고 분석하는 본연의 주요 업무에 더 집중할 수 있게 될 것으로 기대된다.

이벤트 특징 정보	설명
Payload	네트워크 패킷의 실데이터 부분
DestinationIP	목적지 IP 주소
DestinationPort	목적지 포트 번호
ruleNumber	어떤 자동 처리 규칙에 의해 이벤트가 트리거되었는지 나타내는 부분
EventName	침입탐지 이벤트명 예) PortScanning ...
PacketDirection	패킷이 장비를 지나는 방향 (in-bound, out-bound)
JumboPayloadFlag	페이로드가 점보페이로드에 해당하는지 나타내는 플래그
Device	해당 이벤트 로그가 어디에 설치된 장비로부터 수집되었는지 나타냄
PacketSize	네트워크 패킷의 크기
SourceIP	출발지 IP 주소
SourcePort	출발지 포트 번호
Protocol	프로토콜 종류

<표 2> 침입탐지 이벤트 추출 특징 정보

2. 특징 추출 및 확장

침입탐지 이벤트로부터 추출할 수 있는 정보는 여러 가지가 있다. 본 연구에서는 여러 추출 가능한 정보 중 이벤트의 정오탐 분류에 유의미한 단서를 제공할 수 있

는 특징 정보를 선정하여 추출한다. 원본 이벤트는 28개의 특징 필드로 구성되어 있는데, 이 중에서 12개의 특징을 학습에 사용하였으며, <표 2>는 본 연구에서 사용한 이벤트 특징 정보가 요약되어있으며 <표 3>은 임의의 이벤트 e_k , e_{k+1} 를 통한 이벤트 특징 정보 예시를 나타내었다. <표 2>에 설명된 정보 중 확장 가능한 정보를 선정하여 머신러닝 모델이 분류를 위한 추가적인 특징을 학습할 수 있도록 해당 정보를 확장하는 새로운 기술을 제안한다.

이벤트 특징 정보	e_k	e_{k+1}
Payload	40d297bfff93e2 ...	bd131793ffffdfb ...
DestinationIP	112.112.112.1	119.119.119.1
DestinationPort	80	12345
TriggeredRule	{21:True, 22:True}	{19:True}
EventName	tcp port scanning	flooding
PacketDirection	out-bound	in-bound
JumboPayloadFlag	False	False
Device	3	6
PacketSize	876	799
SourceIP	131.132.134.135	121.122.124.125
SourcePort	13765	80
Protocol	TCP	TCP

<표 3> 침입탐지 이벤트 특징 정보 예시

AIDE에서는 <표 2>에 정리된 12가지 데이터필드 중 페이로드를 제외한 11가지 데이터필드의 값을 복잡한 가공없이 사용하고 페이로드 필드값은 텍스트마이닝의 DF를 적용하여 확장한다. DF는 텍스트마이닝에서 사용되는 개념으로 주로 문서 카테고리 분류에 쓰이며 특정 단어가 문서군 내 문서 중 몇 개의 문서에서 등장하는지를 나타낸다. 일반적으로 DF와 함께 사용되는 TF(Term Frequency)라는 개념은 하나의 문서에서 특정 단어가 몇 번 등장했는지를 나타내며 이는 해당 문서에서 특정 단어의 중요도를 의미하는 반면, DF는 문서군 내에서 해당 단어가 얼마나 흔하게 등장하는지를 의미한다. 따라서 일반적으로 DF의 역수를 취하여 문서군 내에서 해당 단어가 얼마나 희귀한지를 나타내는 IDF(Inverse Document Frequency)를 주로 사용한다. 그러나, 본 연구에서는 일반적인 DF가 갖는 의미와 다르게 해석된다.

<그림 6>은 실제 침입탐지 이벤트의 페이로드 부분을 아스키 문자열로 변환한 예시

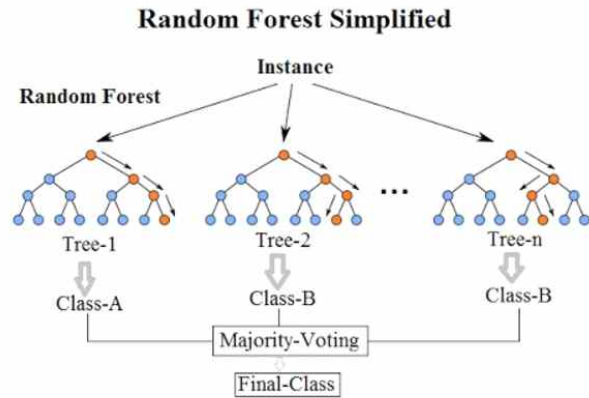
이다. 해당 이벤트는 웹과 관련되어있는데 <그림 6>과 같이 HTTP 상태 코드가 나타난다. 예시에 나타난 ‘200’ 상태 코드는 해당 패킷의 HTTP 요청이 받아들여졌음을 의미하며 침입탐지 이벤트에서 이는 성공적으로 공격 대상에게 연결되었다고 간주할 수 있다. <그림 6>은 실제 정탐 데이터, 즉 공격으로 판단된 침입탐지 이벤트의 페이로드이며 ‘200’ 이외에 리다이렉션(redirect)을 나타내는 ‘301’, ‘302’ 등 공격 대상의 연결에 실패를 나타내는 HTTP 상태 코드가 포함될 경우, 해당 침입탐지 이벤트에 대해 보안관제요원은 오탐으로 판단하였다. 웹 관련 침입탐지 이벤트의 경우에는 모두 페이로드에 HTTP 상태 코드를 포함하기 때문에 HTTP 상태 코드에 대해 높은 DF값을 기대할 수 있다. 따라서 DF값을 기준으로 상위 n개의 단어를 추출하였을 때 HTTP 상태 코드의 출현여부를 통해 정오탐을 판별하는데 중요한 단서를 제공하는 효과를 갖는다.

```
HTTP/1.1 200 OK
Date: Tue, 12 Feb 2019 16:04:07 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Tue, 12 Feb 2019 15:59:06 GMT
ETag: "6f1-581b4813ed8ba"
Accept-Ranges: bytes
Content-Length: 1777
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/java-vm
```

<그림 6> 실제 침입탐지 이벤트
아스키변환 페이로드 예시

AIDE 모델의 입력 벡터를 생성하기 위해서 먼저, 페이로드를 제외한 11가지 데이터필드 중 실수형 데이터필드는 정규화 과정 없이 그대로 사용하고 문자열 데이터필드는 암호학적 해시함수 md5를 통해 정수로 변환한 값을 사용하여 크기 11의 벡터를 생성한다. 페이로드 데이터필드에 저장되는 값은 16진수로 이루어져있는데 이를 아스키(ASCII) 문자열로 변환시킨다. 문자열로 변환된 페이로드 값은 파이썬(Python)의 split() 함수를 통해 해당 문자열에 등장하는 단어의 집합으로 다시 변환되며 각 단어의 집합을 하나의 문서로 간주하여 DF를 계산한다. 이렇게 계산된 DF값을 기준으로 상위 100개 단어를 추출하고 각 단어의 출현여부를 one-hot encoding을 통해 벡터화한다. 이 때, 페이로드 필드값의 아스키 변환이 불가능한 이벤트의 경우에는 크기 100의 영벡터로 변환된다. AIDE 모델에서는 위에 설명한 2가지 벡터를 연

결(concatenate)한 크기 111의 특징벡터를 입력으로 사용한다. 이를 통해 AIDE는 단순히 하나의 값을 가지던 특징을 다시 여러 개의 특징으로 유의미하게 확장하여 기존 특징들과 동등한 레벨의 특징으로 만들어서 모델 학습에 더 많은 단서를 제공할 수 있게 된다.



<그림 7> 랜덤포레스트 아키텍처[14]

AIDE 학습 모델은 랜덤포레스트를 사용하였다. 랜덤포레스트는 분류 및 회귀 분석에 사용되는 머신러닝 모델 중 하나로 앙상블(Ensemble) 기법 중 배깅(Bagging: Bootstrap Aggregating)에 해당된다. 의사결정트리(Decision Tree)이 갖는 학습데이터 의존성 문제를 해결하기 위해 등장한 모델이며, 랜덤포레스트 모델의 아키텍처는 <그림 7>과 같다. 랜덤포레스트의 학습방법은 모든 학습데이터셋을 임의 복원추출과정을 통해 서로 다른 n개의 학습데이터셋으로 나누고 각 데이터셋을 학습한 n개의 의사결정트리를 생성한다. 각각의 의사결정트리는 각자 다른 특징들에 대해 학습되며 테스트의 경우 생성된 n개 의사결정트리의 예측 결과를 종합하여 다수결로 최종 예측 결과를 선정함으로써 일반화 성능을 향상시킨다.

3. 신규 이벤트 웨이버

침입탐지 이벤트 자동 처리 소프트웨어에 내재된 이벤트 자동 처리 규칙은 오랜 기

간에 걸친 관제요원들의 업무 경험이 축약되어있다. 즉, 해당 규칙은 이미 등장했던 이벤트의 정보에 기반하여 정해지는데 경험적으로 세워진 규칙으로 인해 새롭게 등장하는 이벤트에 대해 잘못된 판단을 내리는 경우가 많다. 그 중에서도 새로운 공격에 대해 잘못된 판단을 내리는 경우는 보안관계 특성상 매우 위험하다. 본 연구에서는 학습데이터 등장하지 않은 신규 이벤트가 테스트데이터에 등장할 경우 해당 이벤트의 예측을 보류하는 웨이버 기법을 제안한다.

<Automation + Filtering>

Event name	학습 데이터		테스트 데이터		
	정탐회수	오탐회수	정탐회수	오탐회수	
e ₁	10,000	-	10,000	-	Simple filtering
e ₂	10,000	10,000	10,000	10,000	AI
e ₃	-	-	-	10,000	impossible
e ₄	-	10,000	10,000	10,000	change detection

<그림 8> 침입탐지 이벤트 이진분류 테스트케이스 세부 분류

<그림 8>은 침입탐지 이벤트 이진분류기의 테스트 단계에서 발생할 수 있는 세부 케이스를 표현한 그림이다. e₁의 경우는 학습데이터에서 해당 이벤트가 정탐과 오탐 중 한 가지 라벨값만 가지고 마찬가지로 테스트데이터에서도 학습데이터와 동일한 라벨만을 가지는 경우이며, 해당 경우에 인공지능을 적용하지 않더라도 간단한 필터링 알고리즘을 통해 분류할 수 있다. e₂의 경우는 학습데이터 내에서 정탐과 오탐이 혼재되어있으며 테스트데이터에도 정탐과 오탐이 혼재되어있는 경우를 나타내며 해당 경우에 일반적으로 인공지능을 통해 문제를 해결할 수 있다. e₃은 학습데이터에 등장하지 않았던 이벤트가 테스트데이터에 새롭게 등장하는 경우이다. 이 경우, 인공지능은 해당 이벤트에 대한 학습이 되어있지 않기 때문에 올바른 예측을 기대할 수 없다. e₄는 학습데이터에서 해당 이벤트가 정탐과 오탐 중 한 가지 라벨값만 가지고 있는 반면에 테스트데이터에서는 정탐과 오탐이 혼재되어서 나타나는 경우이다. 이 경우에 충분한 양의 데이터가 해당 이벤트에 대해 한 가지 라벨로만 학습되어있다면 테스트데이터에 대해 이상 탐지(Anomaly Detection)를 기대할 수 있다.

<그림 8>에 나타난 4가지 테스트케이스 중 e₃에 해당하는 경우만이 학습데이터에

한 번도 등장하지 않은 경우인데 보안관계 특성상 이러한 새로운 공격에 대해 잘못된 판단을 내리는 것은 매우 위험하다. 새로운 형태의 이벤트가 발생한 경우 해당 이벤트에 대해 선불리 정오탐 판별이 이루어지는 것보다 관제요원의 분석을 거쳐 정확한 정오탐 라벨을 업데이트하는 것이 우선되어야하기 때문이다. 따라서, 해당 경우에 학습데이터에 등장하지 않은 신규 이벤트에 대해 예측을 보류하는 웨이버 기법의 적용이 권장된다.

웨이버 기법은 모델 학습이 진행될 때 학습데이터에 등장하는 모든 이벤트명을 기억해두었다가 테스트 대상이 되는 모든 침입탐지 이벤트의 이벤트명을 검사하여 기억되지 않은 신규 이벤트명을 가질 경우 해당 이벤트의 예측을 보류한다. 테스트 단계가 종료되고 예측 보류된 이벤트들은 관제요원의 분석에 맡겨지며, 관제요원의 분석에 의해 정오탐이 분류된 신규 이벤트 데이터가 충분히 쌓일 경우, 신규 데이터를 학습데이터에 포함하여 모델을 재학습시키게 된다. 이러한 과정을 거침으로써, 관제요원들은 수작업으로 침입탐지 이벤트 처리 알고리즘을 업데이트할 필요가 없어지며 분석해야하는 이벤트가 크게 줄어들게 된다. 즉, 관제요원은 단순 형태의 공격은 인공지능에 맡기고 본연의 주요 업무인 기존과 다른 행동을 보이는 복잡한 공격 분석에 더 집중할 수 있게 된다.

IV. 실험 및 검증

본 논문에서는 실험을 통해 사람의 개입 없이 보안관계 침입탐지 이벤트 데이터와 머신러닝 기술로 실효성 있는 이벤트 처리 규칙 알고리즘이 생성될 수 있음을 확인하였다. 국내 보안관제센터 중 한 곳의 침입방지시스템에서 발생한 이벤트 데이터에 대해서 실험을 진행했으며, 해당 집합은 보안관제요원이 수작업으로 개발한 이벤트 자동 처리 규칙 소프트웨어에 의해 정탐 라벨과 오탐 라벨로 분류되어있다. AIDE는 723,320개 침입탐지 이벤트 데이터로 이루어진 테스트 데이터셋에 대해 99.92%의 정확도를 보였으며, 이 숫자는 이벤트로부터 추출한 정보를 전처리 과정 없이 특징으로 사용한 기본 모델의 정확도보다 약 2.4% 높음을 보이며 AIDE의 우수성을 증명한다. 또한, 테스트 단계에서 테스트데이터에 등장하는 신규 이벤트 예측을 보류하는 웨이버 기법을 AIDE 모델에 적용하여 99.97%의 성능을 보이며 AIDE의 성능을 한 단계 발전시킬 수 있었다.

1. 실험 환경

본 실험은 여러 기관에 설치되어있는 국내 보안관제센터 중 한 곳의 침입방지시스템들로부터 2018년 8월부터 2019년 3월에 걸쳐 수집된 총 2,166,757개의 침입탐지 이벤트 데이터를 기반으로 진행되었으며 그중 머신러닝 모델 학습을 위해 2018년 8월부터 2019년 1월 기간에 수집된 이벤트 데이터 1,443,437개를 사용하였고 모델 성능 테스트를 위해 2019년 2월과 3월에 수집된 이벤트 데이터 723,320개를 사용하였다. 해당 이벤트 데이터들은 보안관제전문가들의 분석에 의해서 생성된 이벤트 처리 규칙이 적용된 자동 처리 소프트웨어에 의해 정탐과 오탐으로 분류되었다. 학습 및 테스트데이터별 정탐/오탐 이벤트 개수는 <표 4>와 같다.

	정탐 이벤트 개수	오탐 이벤트 개수
학습데이터	609,212	834,255
테스트데이터	69,386	653,934

<표 4> 데이터별 정/오탐 데이터 개수

실험 및 검증은 다음과 같은 실험환경에서 진행되었다. Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz, 64GB 메모리, 500GB SSD + 5TB HDD로 구성된 데스크탑에서 병렬처리를 통한 빠른 학습을 위해 NVIDIA Geforce GTX 1080 Ti GPU를 장착하여 실

험을 진행하였다. 학습모델은 모두 파이썬으로 구현되었으며 랜덤포레스트 모델 사용을 위해 파이썬 머신러닝 라이브러리인 scikit-learn을 사용하였고 랜덤포레스트의 최종 예측 결과는 100개 의사결정트리의 예측 결과를 종합하여 다수결로 선정하였는데 이는 scikit-learn에서 제공하는 기본 설정이다.

2. 탐지 이벤트 분류 알고리즘 비교

본 논문에서는 AIDE의 성능 검증을 위해 서로 다른 두 가지 특징 추출 기법을 사용하는 NFT(Naive Feature Table)와 PFT(Payload Feature Table)의 성능과 비교하였다. NFT는 침입탐지 이벤트로부터 추출할 수 있는 유의미한 데이터필드 중 페이로드 필드를 제외한 11가지 데이터필드만을 복잡한 가공 없이 특징으로 사용하는 학습모델이다. NFT에서 사용하는 11가지 데이터필드는 AIDE와 동일한 방법으로 복잡한 가공없이 사용된다. PFT는 페이로드 정보만을 AIDE에서의 페이로드 정보 확장 방법과 동일하게 각 침입탐지 이벤트의 페이로드 필드만을 아스키(ASCII) 변환 후 텍스트마이닝의 DF 기법을 도입하여 가공한 특징벡터를 입력으로 사용하는 학습모델이다. 즉, NFT와 PFT는 AIDE의 입력을 각각 페이로드 정보 이외의 정보만을 학습한 모델과 페이로드 정보만을 확장하여 학습한 모델이 된다. NFT와 PFT의 학습은 AIDE와 동일한 랜덤포레스트를 사용하여 진행되었다.

본 논문에서는 학습모델의 평가를 위해 가장 널리 쓰이는 이진 분류 평가 결과 표현방법인 혼동행렬(Confusion Matrix)을 사용하였다. 혼동 행렬은 이진분류기의 예측 결과 분포를 나타내는데, 양성 그룹을 양성으로 올바르게 예측하거나(TP:True Positive) 음성 그룹을 음성으로 올바르게 예측한(TN:True Negative) 정탐, 양성 그룹을 음성으로 잘못 예측한 미탐(TN:True Negative), 음성 그룹을 양성으로 잘못 예측한 오탐(TP:True Positive)으로 표현된다. 본 실험에서는 정탐 그룹을 양성그룹, 오탐 그룹을 음성 그룹으로 지정하였다. <표 5>는 혼동행렬을 나타낸다.

	양성 예측	음성 예측
양성 그룹	정탐(True Positive)	미탐(False Negative)
음성 그룹	오탐(False Positive)	정탐(True Negative)

<표 5> 혼동 행렬

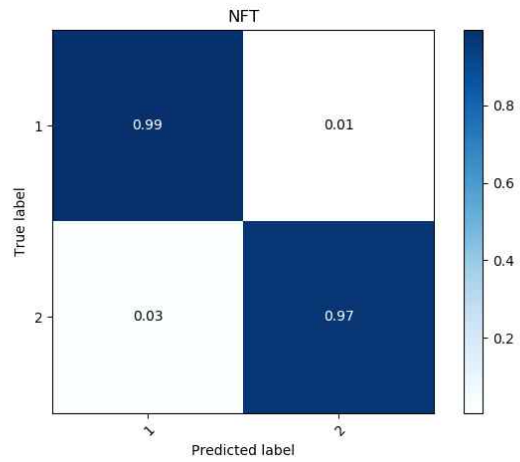
혼동행렬에서 표현되는 위 4가지 예측 결과를 통해 정확도(Accuracy), 정밀도(Precision), 재현율(Recall)과 같은 평가 지표를 정의할 수 있다. 정확도는 전체 예측 결과 중 올바르게 예측한 것의 비율을 의미하며 분류기의 전체적인 성능을 확인하는데 쓰인다. 정밀도는 양성으로 예측된 데이터 중 얼마나 많은 데이터가 실제로 양성 그룹에 속하는지를 비율을 나타내며, 재현율은 실제 양성 그룹 데이터에 대해 분류기가 얼마나 양성으로 올바르게 예측했는지 비율을 나타낸다. 수식 (1), (2), (3)은 각각 3가지 평가 지표의 계산 공식이다.

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \quad \dots \dots \dots (1)$$

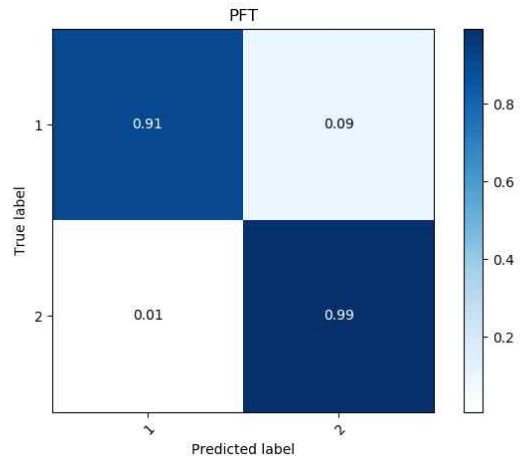
$$Precision = \frac{TP}{TP + FP} \quad \dots \dots \dots (2)$$

$$Recall = \frac{TP}{TP + FN} \quad \dots \dots \dots (3)$$

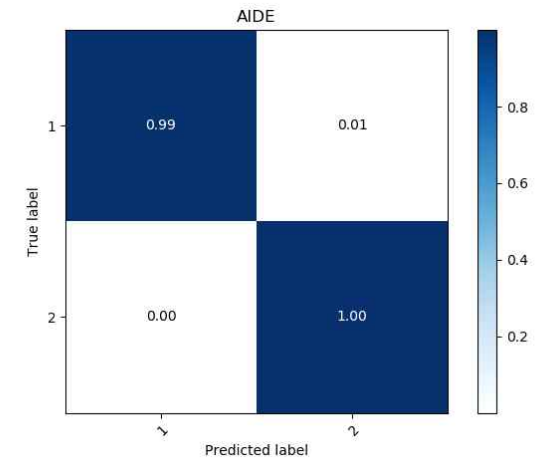
<그림 9>, <그림 10>, <그림 11>은 각각 테스트데이터에 대한 NFT, PFT, AIDE 모델의 예측 결과를 혼동행렬로 나타낸 것이다. 정탐라벨과 오탐라벨은 각각 1, 2로 표현되었다. 해당 혼동행렬에서 NFT 모델은 PFT 모델에 비해 정탐 이벤트 잘 맞추는 것을 확인할 수 있으며 반대로 PFT 모델은 NFT 모델에 비해 오탐 이벤트에 강인한 모습을 확인할 수 있다. AIDE 모델은 모든 테스트데이터에 대해 높은 정확도를 보이며 다른 두 모델에 비해 우수한 성능을 보임을 검증할 수 있었다. 3가지 혼동행렬을 토대로 3가지 평가 지표를 계산한 값은 <표 6>과 같다.



<그림 9> NFT 모델 예측 결과 혼동행렬



<그림 10> PFT 모델 예측 결과 혼동행렬

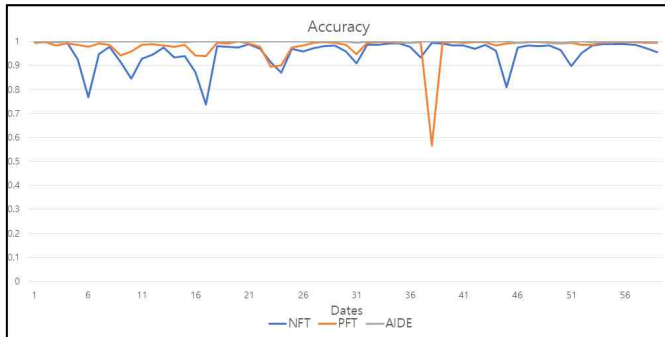


<그림 11> AIDE 모델 예측 결과 혼동행렬

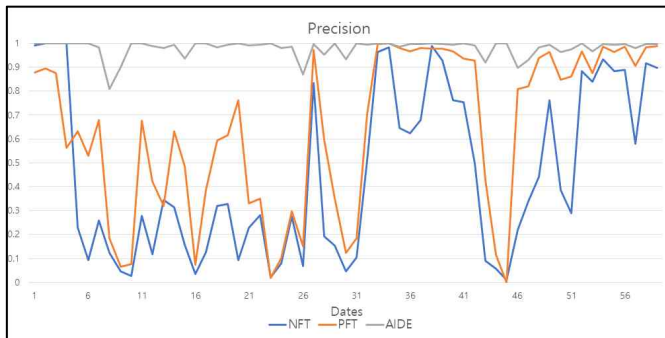
모델	정확도	정밀도	재현율
NFT	97.52	79.53	99.42
PFT	98.45	92.94	90.77
AIDE	99.92	99.72	99.41

<표 6> 침입탐지 이벤트 분류 모델별 성능 평가 지표

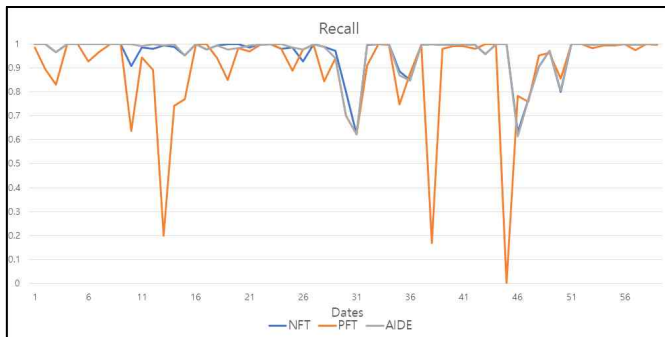
<그림 12>, <그림 13>, <그림 14>은 NFT, PFT, AIDE의 성능을 2019년 1월부터 2019년 2월에 수집된 테스트데이터를 일별로 나누어 3가지 평가 지표에 따라 비교한 그래프이다. 모든 그래프 대부분의 구간에서 AIDE가 NFT, PFT보다 높은 성능을 보임을 확인할 수 있다.



<그림 12> 이벤트 분류 알고리즘별 정확도 성능 비교



<그림 13> 이벤트 분류 알고리즘별 정밀도 성능 비교

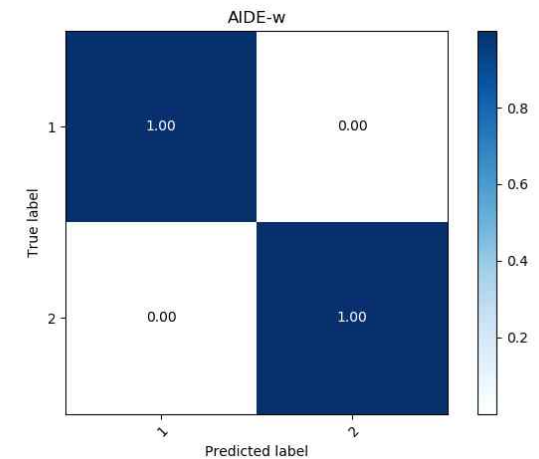


<그림 14> 이벤트 분류 알고리즘별 재현율 성능 비교

3. 신규 이벤트 웨이버

본 실험에서는 학습데이터 미등장 이벤트를 웨이버하는 기법을 AIDE에 적용하여 AIDE와 성능을 비교하였으며 웨이버를 적용한 AIDE 모델을 AIDE-w라 명명하였다. 두 모델의 성능 비교는 탐지 이벤트 분류 알고리즘 비교 실험과 동일한 평가 지표를 사용하여 진행되었다.

<그림 15>는 AIDE-w 모델의 예측 결과를 혼동행렬로 나타낸 것이다. AIDE 모델 예측 결과 혼동행렬인 <그림 11>과 비교했을 때, AIDE-w 모델의 미탐이 AIDE 모델에 비해 개선된 것을 확인할 수 있다. <표 7>는 두 모델의 혼동행렬을 토대로 3가지 평가 지표를 계산한 값이다. 미탐이 개선된 AIDE-w 모델이 재현율 성능해서 유의미한 상승을 보이며 정확도 향상에 기여하였음을 확인할 수 있다.



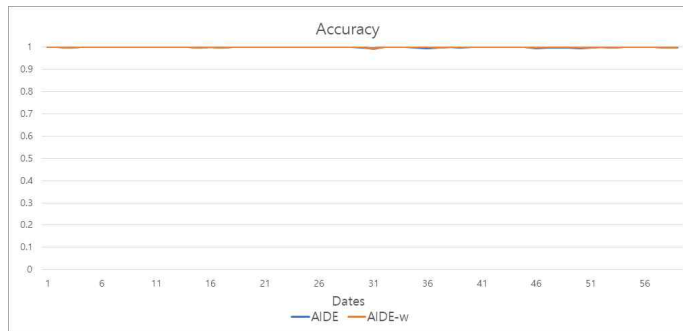
<그림 15> AIDE-w 모델 예측 결과 혼동행렬

모델	정확도	정밀도	재현율
AIDE	99.92	99.72	99.41
AIDE-w	99.97	99.72	99.92

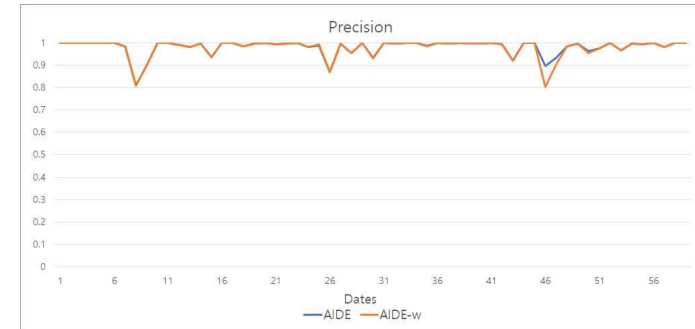
<표 7> 침입탐지 이벤트 분류 모델별 성능 평가 지표

<그림 16>, <그림 17>, <그림 18>은 AIDE와 AIDE-w의 성능을 2019년 1월부터 2019

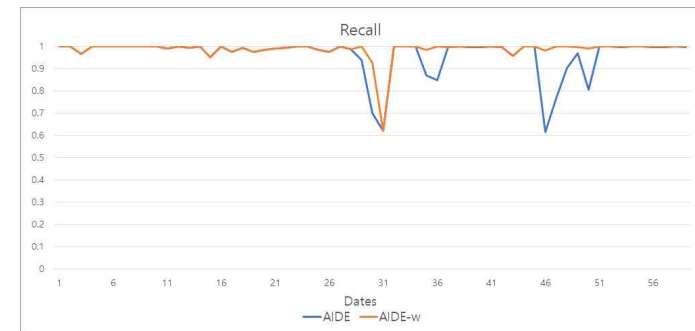
년 2월에 수집된 테스트데이터를 일별로 나누어 3가지 평가 지표에 따라 비교한 그래프이다. <그림 16>에서는 모든 구간에서 AIDE-w 모델이 100%에 근사한 정확도 성능을 보이며 AIDE 모델을 능가했고, <그림 17>에서는 <표 7>에서 두 모델의 정밀도 성능에서 확인할 수 있듯이 대부분의 구간에서 유사한 성능을 보이나 그래프의 46일차 부분에서 AIDE-w 모델의 성능이 더 나빠보이는 구간이 발견된다. 하지만, 실제로 46일차 테스트 결과를 보았을 때, 이는 신규 이벤트를 테스트데이터에서 제외시키는 웨이버의 특성상 전체 테스트 이벤트 개수의 감소로 인해 정밀도 계산 과정에서 분자가 작아지기 때문에 정밀도 성능도 감소하는 것으로 확인된다. <그림 18>에서는 AIDE-w 모델이 AIDE 모델에 비해 눈에 띄게 좋은 성능을 보이는 구간이 확인된다. 결과를 살펴보면 테스트데이터에 등장하는 신규 이벤트에 대해 AIDE 모델이 오답을 내는 경우가 많았던 반면에, AIDE-w 모델은 해당 이벤트들을 제외하여 재현율 계산 과정에서 분모만 작아져 재현율 성능 향상을 확인할 수 있었다.



<그림 16> AIDE와 AIDE-w 모델 정확도 성능 비교



<그림 17> AIDE와 AIDE-w 모델 정밀도 성능 비교



<그림 18> AIDE와 AIDE-w 모델 재현율 성능 비교

V. 결론

본 논문에서는 침입탐지 이벤트를 자동으로 처리할 수 있는 규칙 알고리즘을 생성해낼 수 있는 새로운 머신러닝 기술을 제안하였다. 국내 보안관제센터로부터 장기간 수집된 침입탐지 이벤트 데이터 셋을 사용하여 머신러닝 연구가 진행되었으며, 침입탐지 이벤트에서 추출한 특징 정보를 자연어처리 기법을 적용하여 유의미하게 확장시키고 기본 특징 정보들과 결합하여 학습 입력 값을 생성함으로써 기존의 특징 정보를 가공 없이 사용하는 모델에 비해 우수한 성능을 보였다. 또한, 학습데이터에 등장하지 않은 신규 이벤트가 테스트데이터에 등장할 경우 해당 이벤트의 예측을 보류하는 웨이버 기법을 적용하여 99.97%의 높은 정확도를 보이며, 보안관제요원들이 장기간에 걸쳐서 수작업으로 생성한 이벤트 자동 처리 소프트웨어와 거의 동일하게 동작하는 것을 실험으로 확인하였다.

대부분의 보안관제센터는 오랜 기간에 걸쳐서 관제요원들이 작성해 놓은 정탐과 오탐을 구분하는 규칙 소프트웨어가 개발되어 있으며 수시로 업데이트된다. 규칙 소프트웨어를 관리하기 위해서 많은 사람의 시간과 노력이 요구되며, 사람의 실수가 개입될 위험도 있다. 본 논문에서는 관제요원들이 알람 이벤트에 붙여놓은 라벨을 기반으로 머신러닝에 의해 정탐과 오탐을 정확히 구분할 수 있는 알고리즘이 자동으로 생성되는 인공지능 기술을 제안했다. 본 연구에서 제안하는 기술이 실제 관제 업무에 적용되면, 보안 전문가들이 수작업으로 침입탐지 이벤트 처리 알고리즘을 개발 및 업데이트할 필요가 사라지므로 시간 소모적이고 오류 발생이 쉬운 작업을 개선할 수 있으며, 관제요원들은 본연의 주요 업무에 더 집중할 수 있을 것으로 기대된다.

[참고문헌]

- [1] “인공지능 기반 금융권 보안관제 동향 및 향후과제”, 금융보안원, 전자금융과 금융보안, 제8호, pp. 41-63, April, 2017.
- [2] M. Du, F. Li, G. Zheng, and V. Srikumar, “DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning,” ACM CCS’17, 2017
- [3] C. Manning and H. Schutze, “Foundations of statistical natural language processing. MIT Press, 1999.
- [4] Y. Shen, E. Mariconti, P. Vervier, and G. Stringhini, “Tiresias: Predicting Security Events Through Deep Learning,” ACM CCS’18, 2018
- [5] F. Pendlebury, F. Pierazzi, R. Jordaney, J. Kinder, and L. Lavallaro, “TESSERACT: Eliminating Experimental Bias in Malware Classification across Space and Time,” USENIX Security’19, 2019
- [6] Y. Shen and G. Stringhini, “ATTACK2VEC: Leveraging Temporal Word Embeddings to Understand the Evolution of Cyberattacks,” USENIX Security’19, 2019
- [7] B. Kwon, V. Srinivas, A. Deshpande, and T. Dumitras, “Catching worms, trojan horses and pups: Unsupervised detection of silent delivery campaigns,” NDSS’17, 2017
- [8] “NINE STEPS TO ELIMINATE ALERT FATIGUE,” FireEye, 2016
- [9] “How to Help SOC Analysts Fight ‘Alert Fatigue’ ” [Internet], <https://blog.paloaltonetworks.com/2019/07/help-soc-analysts-fight-alert-fatigue/>, 2019.8.29
- [10] 신익수, 송중석, 최장원, 권태웅, “기계학습 기반 IDS 보안이벤트 분류 모델의 정확도 및 신속도 향상을 위한 실용적 feature 추출 연구“, 정보보호학회논문지, pp.385-395, 2018.4
- [11] 강용석, 신용태, “오픈소스 기반 Deep Learning 기술을 활용한 보안관제시스템의 Anomaly Detect Model 연구“, 정보과학회지, pp.51-60, 2017.9
- [12] 김효석, 김용민, “TF-IDF를 이용한 침입탐지 이벤트 유효성 검증 기법“, 정보보호학회논문지, pp.1489-1497, 2018.12
- [13] A. Liaw and M. Wiener, “Classification and regression by random forest,” R

News 2/3, 18-22, Dec., 2002

[14] W. koehrsen, Random Forest Simple Explanation [Internet], Available: <https://medium.com/@williamkoehrsen/random-forest-simple-explanation-377895a60d2d>, 2019.8.29.

ETIR 모델 기반 SOAR 금융보안관제 설계 및 구축

김민준* · 정채덕** · 박민규* · 박준욱*** · 우성훈*

* BNK부산은행 정보보호부

** SK인포섹 EQST 전략해킹팀 *** SK인포섹 관제담당

요 약

해킹이나 컴퓨터 바이러스와 같이 정보 가치를 훼손하는 사이버 공격은 전략·전술적으로 고도화된 지능형 지속 위협(APT, Advanced Persistent Threat) 형태로 지속 발전하고 있으며, 이러한 고도화된 해킹은 비즈니스 환경을 위협하여 기업 경쟁력을 약화시킨다. 기업은 정보화 역기능에 따른 부작용을 최소화할 수 있도록 사이버 공간에서 발생하는 위협을 관리하여야 하며, 당면한 위협에 대한 적절한 보호 대책을 마련하는 정보보호 거버넌스 활동을 지속적으로 수행해야 한다. 이를 위해, 정보를 다루는 주체 간 상호작용을 통해 보안 관련 이벤트를 수집하고 저장 및 분석하는 빅데이터 처리기술에 기반을 둔 시스템인 SIEM(Security Information and Event Management)을 도입하였다. 특히 금융회사에서는 최근 이와 관련한 고도화 사업을 진행하고 있으며 지난 운영 경험과 신기술을 적용한 전문 솔루션을 도입하고 있다. 그러나 SIEM을 도입했더라도 사이버보안 침해사고에 적절한 대응을 할 수 있는 전문가의 부재 등의 사유로 보안 위협으로부터 벗어날 수 없게 되었다. 한편 SIEM의 보안사고 대응에 초점을 맞춘 SOAR(Security Orchestration, Automation and Response)의 개념이 소개되기도 하였다. 본 논문에서는 SIEM에서 생성된 이벤트 및 티켓의 효과적이고 적절한 대응을 위한 ETIR 위협평가 모델을 소개하고, 제안한 모델기반의 고도화된 SIEM이 SOAR의 구성요소 기능과 유사함을 분석한다. 마지막으로 부산은행에서 구축한 ETIR 모델 기반의 동적 통합보안관제 모니터링 구성을 소개한다.

키워드

ETIR, SOAR, SIEM, 정보보호, 보안관제, 인텔리전스, 위협관리

목 차

I. 서론	3
II. 관련연구	4
1. 정보보호 위험관리 연구 동향	4
2. 위협 및 취약점 분석 연구 동향	6
3. SOAR 개요.....	6
III. ETIR 모델 기반 SOAR 금융보안관제	8
1. ETIR 위험평가 모델	8
2. 통합보안관제 설계 및 구축	11
IV. 동적 통합보안관제 모니터링	28
1. 이기종 Dashboard 연동.....	28
2. 동적 모니터링	29
3. 활용 사례 및 성과	30
V. 결론	33

I. 서론

최근 IT 정보기술의 혁신적인 발전으로 비즈니스 전반에 걸쳐 정보화가 가속화되었다. 이는 업무생산성 향상에 기여하는 기업 경영의 핵심 요소가 되었지만, 정보화 역기능에 따른 여러 가지 부작용을 초래하였다[1]. 특히 해킹이나 컴퓨터 바이러스와 같이 정보 가치를 훼손하는 사이버 공격은 전략·전술적으로 고도화된 지능형 지속 위협(APT, Advanced Persistent Threat) 형태로 발전하였다. 이러한 고도화된 해킹은 비즈니스 환경을 위협하여 기업 경쟁력을 약화시킨다[2, 3].

따라서, 기업은 정보화 역기능에 따른 부작용을 최소화할 수 있도록 사이버 공간에서 발생하는 위협을 관리하여야 하며, 당면한 위협에 대한 적절한 보호 대책을 마련하는 정보보호 거버넌스 활동을 지속적으로 수행해야 한다[4, 5]. SIEM(Security Information & Event Management)은 정보를 다루는 주체 간 상호작용을 통해 보안 관련 이벤트를 수집하고 저장 및 분석하는 빅데이터 처리기술에 기반을 둔 시스템이다. SIEM 시스템은 FFIEC, COBIT, ISO 27002, PCI 등 표준화된 거버넌스 체계에서 강조하는 자산 중심 위협관리를 구체화하여 정보보호 업무성과에 긍정적인 영향을 준다[6, 7].

SIEM 시스템을 성공적으로 도입 및 운영하기 위해서는 적용 실패사례 연구가 선행되어야 한다. 최근 기업들은 SIEM을 도입하여 조직을 위한 정보보호 활동을 수행하려 하지만, 여러 실패 요인으로 인해 목표 달성에 어려움을 겪고 있다[8]. 가트너를 비롯한 주요 연구기관의 보고서를 종합하면, SIEM 시스템에 대한 관리와 대응 인력이 부족하고, 현장의 빅데이터 처리기술과 비즈니스 관련 지식이 융합되지 못하면서 시스템 내에 불필요한 정보 순환 문제(Garbage In, Garbage Out)가 발생하여 초기 도입 취지에 부합하지 않는 방향으로 활용 범위가 제한되는 사례를 주된 실패 요인으로 꼽는다. 따라서, 사이버 위협으로부터 벗어나기 위해서는 SIEM 시스템을 활용한 사고대응 체계 개선이 필요하게 되었다.

2017년 가트너는 “기술 인력, 전문성, 예산 부족과 더불어 적대적 위협 발생이 증가하고 있는 현 과제를 해결하기 위해 조직은 SOAR(보안 운영 자동화 및 대응, Security Orchestration, Automation and Response) 기술을 검토하고 있다” 고 밝혔다. SOAR는 다양한 보안 위협에 대한 대응 프로세스를 자동화하고 조율해 SOC(Security Operation Center) 직원의 단조롭고 반복적인 업무를 효과적으로 줄이고, 각종 보안 이벤트를 빠르고 정확하게 대응할 수 있게 도와주는 새로운

보안 패러다임이다. 최근 3년간 부산은행에서는 적은 운용 인력 및 높은 시스템 구축비용을 고려하여, 기 구축된 SIEM 시스템 고도화 및 워크플로우 기반 위협관리를 위해 자체적으로 ETIR 모델을 설계하였다. 2019년 전반기에 ETIR의 주요기능이 포함된 통합보안관제체계를 구축하였으며, 사무실 내 정보보호 관제센터를 구성하고 SK인포섹의 전문 보안관제 인력을 추가 배치하였다.

본 논문에서는 최근 부산은행 통합보안관제의 혁신적인 재설계 및 구축 노하우를 SOAR 기능과 연관하여 소개한다. 특히 사이버위협에 대응 자동화를 위하여 정보보호 위협관리의 일부인 위협평가 프로세스를 활용하여 SIEM 환경에서 정량적인 사고탐지가 가능한 ‘ETIR 위협평가 모델’을 제안한다. 또한 관리가 어려운 보안자산 및 직원유형 등 금융기업의 특성을 고려하여, ITIL의 CMDB(Configuration Management DataBase) 기반의 보안관제를 위한 상황정보(Context)를 구성하였다. 이는 다양한 소스로부터 발생한 정보를 통합하고 상황 관점에서 상호연관성 분석을 통해 상황인식 보안을 구현할 수 있으며, 효율적인 사고탐지를 위해 표준화된 취약성 및 공격 패턴 식별 방법과 상황정보 기술을 응용하면 발생하는 사고에 대한 탐지 정확도를 높일 수 있다. 마지막으로 구축한 ETIR모델 기반 보안관제체계를 효과적으로 모니터링하기 위해 구성한 동적 통합보안관제 모니터링을 소개한다.

II. 관련 연구

1. 정보보호 위협관리 연구 동향

국제표준인 ISO/IEC 27000에서는 조직이 정보자산을 안전하게 보호하도록 가이드한다. 여기에 속하는 여러 표준 중 ISO/IEC 27001에서는 정보 보안 관리 시스템(ISMS, Information Security Management System)에 대한 요구사항을 설명하고, 정보 위협관리에 관한 통제 권고사항 목록을 상세히 기술한다. 이 표준과 관련한 정보 위협관리를 체계적으로 수행하기 위한 다양한 방법론이 있다[9].

(1) EBIOS

정보시스템과 관련된 위험분석, 평가, 이행에 관한 방법으로 1995년 프랑스 국가 안보국의 프랑스 총리 직속 부속기관인 DCSSI에 의해 만들어졌다.

(2) MEHARI

이해관계자(운영관리자, CISO, CIO, 위험관리자, 감사원 등)가 정보 및 IT 자원과 관련된 위험을 평가하고 관리할 수 있도록 한다. ISO 13335와 ISO 27005 위험관리 표준을 준수하고, ISO 27001에 기술된 ISMS 프로세스를 만족한다. 1996년 CLUSIF에 의해 개발되었고 Risicare사의 소프트웨어에서 지원하는 위험분석 및 관리 방법이다.

(3) NIST SP(Special Publication) 800-30

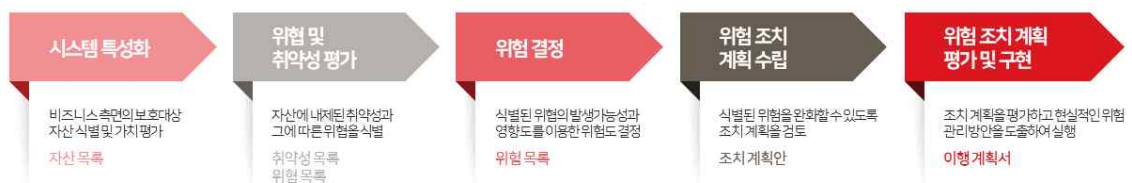
미국 표준 기술 연구소에서 미연방 정보시스템 및 조직의 정보보호 위험평가를 수행하기 위해 만들어졌다. 조직 레벨, 실무 처리 레벨, 정보 시스템 레벨에 해당하는 세 단계로 위험 평가를 수행함으로써 상위 결정권자나 임원의 위험 결정에 필요한 정보를 제공한다.

(4) CRAMM

1987년 영국 정부의 CCTA(지금의 OGC)에서 만든 위험관리 방법론으로 정량적 방법론보다 정성적 방법론에 가깝다. 세 가지 단계를 체계적으로 수행할 수 있는 소프트웨어 기반 도구를 지원한다.

(5) ISO 27005

정보보호 위험관리 지침을 제공하여 ISO 27001에 기술된 ISMS 프로세스를 만족하고, 위험관리 접근법을 기반으로 체계적인 정보보호 활동을 구현할 수 있도록 설계되었다. 특정 위험분석 방법을 기술하지는 않으나 위험관리 프로세스 절차를 설명하고 있어, 조직의 정보를 위협할 수 있는 위험을 관리하고자 하는 모든 조직에 적용할 수 있다[10].



<그림 1> 정보보호 위험관리 단계

<그림 1>은 앞에서 소개한 위협관리 방법론들을 정보보호 위협관리 단계로 나타낸 것이다. 대부분의 잘 구성된 위협관리 방법론들은 시스템 특성화, 위협 및 취약성 평가, 위협 결정, 위협 조치 계획 수립, 위협 조치 계획 평가 및 구현의 다섯 단계 절차로 일반화가 가능하다[9]. 따라서, ISO 27005를 준수하는 제안 모델은 일반화된 정보보호 위협관리 절차를 준수하면서 다른 방법론들의 절차와도 상호보완적인 관계로 발전시켜 나갈 수 있다.

2. 위협 및 취약성 분석 연구 동향

위험평가의 척도가 되는 위험도를 정밀하게 측정하기 위해 위협 및 취약성 분석과 관련한 다양한 연구들이 있다. 네트워크 및 로직 다이어그램을 이용한 소프트웨어의 취약성과 위협을 식별하는 Microsoft의 TMA(Threat Modeling Analysis)는 체계적인 방법론과 도구를 통해 기존 취약성 진단 도구로 식별이 어려운 요소를 식별하여 상세한 취약성 및 위협 목록을 작성할 수 있으며, 이 과정에서 식별된 위협이나 취약성을 체계적으로 분류하는 것은 상위 개념인 위험 영역을 결정하는 데 도움이 된다[12-13].

위험분석 과정에서 도출되는 영향도와 발생 가능성은 식별된 자산 가치와 함께 위험 모델의 핵심 요소로써 이를 객관적으로 구하려는 시도가 있다[9, 14]. 공격자 관점에서 공격 그래프를 구성하여 위협이 현실화될 수 있는 공격 경로를 파악하는 도구인 CySeMol (Cyber Security Modeling Language)는 객관적 위험분석을 수행하기에 유용하며 [11] 위협의 발생 가능성을 고려한 확률기반 분석에 관한 연구는 위험도를 보다 객관성 있게 표현한다[15-17].

3. SOAR 개요

다양한 보안솔루션의 로그를 수집하여 분석하는 SIEM은 엄청난 작업량을 요구하고 있기 때문에, 이를 해결하기 위해 최근에 SOAR의 개념이 소개되었다. 국내외 보안솔루션 기업 등에서 SOAR에 대한 정의 및 소개를 하고 있으며, 2018년 FireEye에서 정의한 내용은 다음과 같다.

- SOAR란? 수집된 모든 로그 및 이벤트를 바탕으로 위협 인텔리전스와 능동적 탐지를 통해 침해정보와 영향도를 도출하고 이를 개선하기 위한 시스템 변경을 자동화 할 수 있게 하는 플랫폼

대부분의 기업들이 사이버보안 목표를 이루지 못하는 이유를 기술 및 도구가 아닌 정책과 사람이라고 판단하기 때문에, 금전적 및 정책적 효율성 측면의 고도화된 통합보안관제인 SOAR가 이를 해결할 수 있다. 또한, FireEye에서 소개된 기존 통합보안관제의 문제점들을 다음 <표 1>과 같이 소개하였다[19]. 본 논문에서는 <표 1>에서의 문제점들을 개선하기 위해 재설계한 통합보안관제체계를 소개한다.

구분	내용
가시성 부족	침해사실을 발견하기까지 172일 소요
쏟아지는 경보	매일 10,000여건의 보안 경보 발생
전문인력 부족	2020년까지 보안전문 일자리 150만 공석
상황정보 부재	침해 발견 후 대응하기까지 32일 소요
너무 많은 솔루션	기업당 85개의 보안 솔루션 도입

<표 1> 기존 통합보안관제의 문제점

SOAR는 다음 <표 2>와 같이 3대 보안대응 영역으로 나눌 수 있으며, 다음 장에서 해당 영역을 기준으로 설계 및 구축한 통합보안관제체계를 기술한다.

보안대응 영역	내용
SOA	(Security Orchestration and Automation) - SOAR의 핵심기능으로 단조롭고 반복적인 프로세스를 자동화시키는 영역임 - 다양한 이기종의 솔루션을 연동하여 전체 대응 프로세스의 효율성이 증대함
SIR	(Security Incident Response) - 보안 사고의 유형별로 보안 사고 대응 정책에 의해 미리 정해진 절차(Playbooks)를 관리하는 영역임

	- 사고를 상황에 맞게 파악하고 정해진 절차에 따라 업무를 수행함으로써 사고 감지 및 대응을 가속화함
TIP	(Threat Intelligence Platforms) - 다양한 유형의 위협 데이터를 실시간으로 수집 및 상관 분석하는 영역임 - 위협 데이터를 활용한 추론 및 정오탐 분석 자동화로 분석가의 의사결정에 도움을 주어 업무 효율을 높임

<표 2> SOAR 보안대응 영역

Ⅲ. ETIR 모델 기반 SOAR 금융보안관제

본 장에서는 부산은행에서 자체 설계한 ETIR 위협평가 모델을 소개하고, 설계한 모델과 SOAR의 연관성을 분석한다. 또한 구축 사례를 ETIR 모델의 각 단계 관점에서 기술한다.

1. ETIR 위협평가 모델

(1) 구성요소 및 단계

ETIR 위협평가 모델은 실무적인 관점의 SIEM 환경에서 체계적인 위협평가를 수행하기 위하여 설계하였다. 제안 모델에서는 예측가능한 공격자의 위협 행위로부터 피해 정도를 예측하고, 인지된 사고에 대한 사실관계를 파악하여 비즈니스적 위험 기준에서 위험 완화 전략을 수립한다. 이러한 일련의 과정은 SIEM 내에서 정보화되어 처리되며, 각 단계는 <그림 2>와 같이 이벤트(Event), 티켓(Ticket), 사고(Incident), 위험(Risk) 구성요소로 나타낼 수 있다. 위험을 식별/진단/해결하는 일관된 접근방식과 자동화된 프로세스를 통해 전체 은행 환경 전반의 정보보호 위협요소를 통합된 형태로 파악하는 것이 목표이다.



<그림 2> ETIR 위험평가 모델

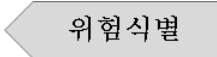
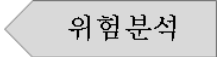
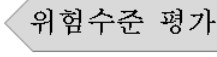
이벤트(Event)는 자산 및 보안솔루션에 대한 모든 행위 로그이며, 침해 및 유출 판정에 사용할 기초 근거 자료로 활용된다. SIEM에서 설정된 룰에 의해 탐지된 이벤트가 티켓(Ticket)이며, 이러한 티켓은 관제팀에서 위험 분석 및 대응해야 할 이벤트이다. 티켓을 소명처리하는 과정에서 실제로 발생한 위험이거나 즉시 또는 추가 피해를 입힐 수 있는 티켓을 인시던트(Incident)로 분류한다. 식별된 인시던트의 위험을 평가하여 비즈니스 측면의 피해 등 위험(Risk)을 측정한다. ETIR 모델의 각 단계별 수행 내용은 다음과 같다.

- ① 위험식별 : 자산의 운용에 따라 발생하는 로그로부터 추출된 상황 정보를 흐름과 설정 유형으로 구분하고, 이를 이용하여 공격과 관련성이 높은 이벤트를 식별함.
- ② 위험분석 : 해당 이벤트가 수용 가능한 기술적인 영향 범위를 넘어서면 티켓을 발급하고, 정보보호 담당자는 발급된 티켓과 관련된 이벤트가 비즈니스에 악영향이 있었는지를 조사함.
- ③ 위험수준 평가 : 발급된 티켓이 수용 범위를 초과하는 인시던트로 판단되면, 비즈니스 위험 측면에서 연관성을 맺음.

(2) SOAR 연관성

ETIR 모델의 구성요소와 SOAR의 연관성은 <표 3>과 같다. SOAR는 수집 및 분석되는 각종 보안 이벤트로부터 빠르고 정확하게 사건을 인지하고 골든 타임 내에 대응하며, 이 과정에서 도출되는 각종 위험들을 비즈니스 인텔리전스(또는 기업 거버넌스) 관점에서 관리하기 위한 프레임워크이다. 한편 SOAR는 탐지→선별검사→대응→우선순위화 단계로 구분할 수 있으며, 탐지 및

우선순위화는 SOAR의 Orchestration 영역과 맵핑된다. 또한 선별검사 및 대응 단계는 TIP와 SIR 영역의 기능과 맵핑되고, 전체적인 과정에서 Automation이 활용된다.

ETIR 모델		SOAR		
구성요소	단계	구성요소	단계	세부단계
Event	 위험식별	SOA	탐지	Collect
				Decision Making
Ticket	 위험분석	TIP, SIR, Automation	선별검사	Threat Hunting
				Investigation
	Human Intervention			
Incident	 위험수준 평가		대응	Workflow
		Remediate		
Risk		SOA	우선 순위화	Measure
				Risk
				Business Intelligence

<표 3> ETIR 모델과 SOAR 연관성

<표 3>의 SOAR의 세부단계와 ETIR 구성요소에 대한 업무절차 관점에서의 연관성은 다음과 같이 나타낼 수 있다.

- Event : 전체적인 과정은 각종 보안시스템으로부터 정보를 수집(Collect)하여 상황에 맞는 정보를 구성한다. 수집 정보는 상황을 인지하는 데 필요한 특징을 나타내는 설정정보와 자산의 행위로 인해 발생하는 흐름정보로 이루어진다. 분석가는 이 정보로부터 선별검사 대상인 티켓을 추출하는 의사결정(Decision making)을 하게 된다.
- Ticket : 티켓이 추출되면 조사(Investigation) 과정을 거치게 된다. 조사에 필요한 정보가 부족하면 별도로 위협 헌팅(Threat hunting) 과정을 거칠 수 있으며, 조사 과정이 완료되면 이해 관계자 간 중재(Human intervention)를 거쳐 사고를 판별한다.
- Incident : 사고로 판별된 티켓에 대해서는 사고의 특성에 맞는

대응(Response)을 수행한다. 사전 정의된 처리절차(Workflow)를 통해 골든 타임 내 사고처리를 완료하고, 예방할 수 있는 개선(Remediate) 사항을 도출하여 이행한다.

- Risk : 사고의 발생은 그에 따른 위험(Risk)을 증가시킨다. 사고에 따른 위험을 기업의 거버넌스에 적합하도록 측정(Measure)하여 비즈니스 인텔리전스(Business Intelligence) 형태로 경영진에게 정보를 제공한다.

2. 통합보안관제 설계 및 구축

본 절에서는 자체 설계한 ETIR 위험평가 모델 기반의 통합관제체계를 소개하며, 업무 단위(이벤트) 및 절차를 고려하여 ETIR 모델의 단계(위험식별, 위험분석, 위험수준 평가)별로 구분한다. <표 4>는 부산은행에서 SOAR 세부단계 구축을 위해 적용한 솔루션 목록이다.

ETIR 구성요소	SOAR 세부단계	관련 솔루션명 (제조사)
Event	Collect	SONAR (이디엄)
	Decision Making	
Ticket	Threat Hunting	Netwitness (RSA), Secudium Intelligence (SK인포섹), GeoIP (Maxmind)
	Investigation	SONAR (이디엄), Netwitness (RSA), Secudium Intelligence (SK인포섹), GeoIP (Maxmind), Qlik Sense (클릭테크)
	Human Intervention	SONAR (이디엄)
Incident	Workflow	SONAR (이디엄), Archer (RSA)
	Remediate	Archer (RSA)
Risk	Measure	Archer (RSA)
	Risk	Archer (RSA)
	Business Intelligence	Qlik Sense (클릭테크)

<표 4> ETIR 모델 관련 솔루션

※ SONAR는 SIEM 제품군, Netwithness는 네트워크 포렌식 툴, Secudium Intelligence는 위협정보 수집 서비스, GeoIP는 IP 위치정보 서비스, Qlik Sense는 시각화 제품군, Archer는 위협관리 도구임.

(1) 위협식별 단계

위협식별 단계는 이벤트로부터 위협 가능성이 있는 티켓을 추출하는 과정이며, 중요 자산에 대한 위협 행위를 자동으로 식별하여 보안 담당자가 확인해야 할 대상인 티켓을 발행하도록 설계하였다.

1) 정보자산 식별 및 평가

보호해야 할 정보자산 식별과 중요도 평가는 사고가 탐지되었을 때, 대응 우선순위를 결정하는 과정을 수행하는 데 필수적인 요소이다. 목록화 대상은 관리대상 범위에 따라 평가에 필요한 정보를 기재하여 저장하는데 그 대상은 다음과 같다.

- 기업 내부에서 관리되는 행정, 비즈니스 정보 혹은 데이터 자체
- 정보의 생성, 이용, 가공, 전송, 저장, 폐기를 목적으로 사용되는 자산
- 정보를 보호할 목적으로 운영되는 자산

정보자산 목록 구성은 정보자산 이름, 정보자산 분류, 정보자산 유형, 정보자산 소유자의 네 가지 필수 정보와 정보자산 가치를 대표하는 필드로 구성된다. 중요도를 제외한 항목은 자산 소유자가 작성하고, 중요도 항목인 CIA는 비즈니스와 정보자산 간 관계에 따라 비즈니스 절차 설계자가 주어진 체크리스트를 사용하여 평가한다. 이는 정보자산이 비즈니스 활동에 따라 형성되어 유지, 관리되는 도구로서 존재 가치를 얻기 때문이다. 부산은행에서는 정보자산이 포함된 최소한의 상황정보를 구성하기 위해 수많은 시행착오가 있었으며, 최종적으로 <표 5>과 같이 상황정보를 구성하였다.

구분	구성 내용
설정정보	직원/부서/직무, 직원 근태상태, 보안자산, 서버계정, 자산담당자, 단말IP, 네트워크 세그먼트, 통합코드 마스터

사건정보	티켓 발행 및 처리, 인시던트 발행 및 처리
위협정보	외부 위협정보, 내부 위협정보, 외부IP 위치정보
서비스정보	DMZ 서비스, 대외 서비스
변화정보	설정정보 변화, 사건정보 변화, 위협정보 변화, 서비스정보 변화
흐름정보	세션(네트워크, 메일), 매체 반/출입

<표 5> 상황정보 구성

취약성은 실제로 공격 구현이 가능한 설계 및 운영상 오류로 ISO 27005에서는 하나 이상의 위협들로 인해 익스플로잇 될 수 있는 자산 또는 자산 그룹의 약점으로 정의한다. 취약성은 위협의 구성요소이자 공격을 실현할 목적으로 사용되는 익스플로잇의 재료이므로 취약성을 식별하는 것은 상위 개념인 위협과 공격을 식별하는 기초가 된다. 취약성 목록은 자산에 노출된 취약성이 무엇이며 공격자에 의해서 악용될 능력 정도와 취약점이 실현될 경우 요구가치에 대한 영향도를 파악할 수 있다. 이를 위해 자산이 등록되면 자동으로 자산의 CVE 기반의 취약성을 식별하기 위해 Nexpose 솔루션을 활용한다. <그림 3>은 자산등록 및 평가 절차를 나타내며, 대부분의 단계는 자동화로 수행된다.



<그림 3> 자산등록 및 평가 절차

2) 공격 행위 식별 및 평가

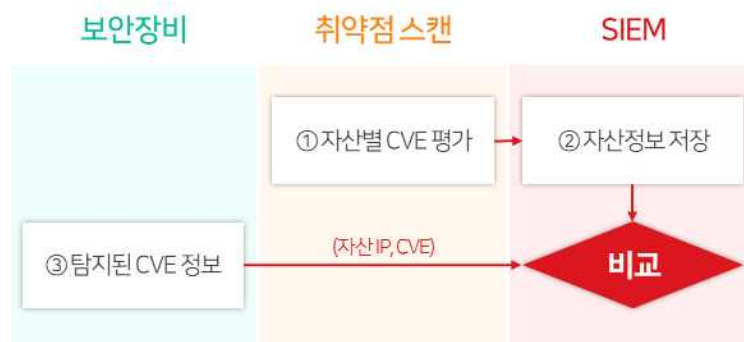
자산에 대한 취약성을 파악하면 그 자산을 공격하려는 행위를 식별해낼 수 있다. CAPEC(Common Attack Pattern Enumeration and Classification)은 공격 패턴과

해결책 및 완화 방안에 대한 데이터베이스로 공격하려는 행위를 표준화하여 SIEM에서 공격 행위가 실제로 발생함을 감지하는 규칙을 작성할 때 활용할 수 있다.

식별된 취약성을 이용하여 해당하는 공격 패턴을 찾는 방법은 취약성 분류 코드인 CWE(Common Weakness Enumeration)를 이용하면 가능하다. CVE(Common Vulnerabilities and Exposures)는 CWE 분류 코드가 기본적으로 부여되고 CVE 코드를 식별하지 못한 취약성은 보안 담당자가 직접 CWE를 지정한 후 MITRE 단체의 CWE 분류 코드와 연결된 CAPEC 코드를 얻는다.

CAPEC의 스키마로부터, 공격의 발생 가능성과 심각도에 관한 값을 얻을 수 있다. 공격의 발생 가능성은 공격의 발생빈도를 낮음, 중간, 높음과 같은 평가 라벨로 표시하고, 마찬가지로 공격의 심각한 정도를 심각도 변수로 나타낸다. 이 두 변수를 취약성의 악용 가능성, 요구가치 영향도와 함께, 기술적 위험도 계산에 사용하였다.

한편 <그림 4>와 같이 정보자산 식별 과정에서 확인된 자산별 CVE 취약점을 활용하여 보안장비(FW, IPS 등)에서 탐지된 공격이 해당 자산에 유의미한 위협이었는지 판단한다. 이를 위해 공격 탐지명과 CVE를 맵핑시킬 수 있는 다양한 보안장비에 대한 도입 및 검토를 진행하고 있다.

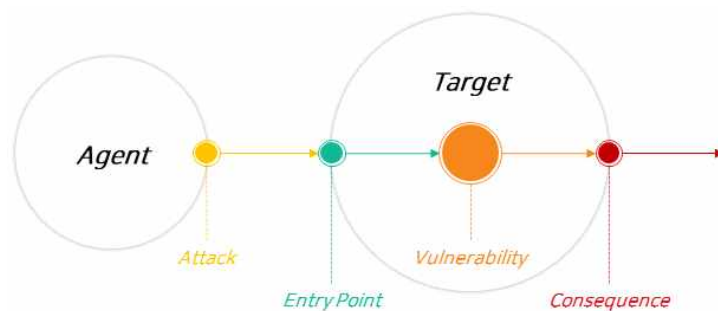


<그림 4> CVE 기반 공격 위험성 식별

3) 이벤트 추출

ETIR 모델에서 관찰대상 이벤트로 간주하는 것은 위협원이 공격 대상의 취약성에 가할 수 있는 행위 후보이다. 이렇듯 공격과 관련된 수많은 이벤트를 식별하면 그 중 보안 담당자의 확인이 필요한 티켓과 실제 피해가 있음을 나타내는 인시던트의 추출이 쉬워지고, 추출된 티켓 또는 인시던트와 관련된 추가적인 공격 이벤트를 재검토하여 찾아낼 수 있다.

하나의 이벤트는 <그림 5>와 같이 위협 행위를 가하는 주체인 Agent, 주체가 할 수 있는 위협인 Attack, 위협 행위가 작용할 수 있는 대상인 Target, 위협 행위가 대상의 취약성에 작용하기 위해 통과하는 진입 지점인 Entry Point, 대상에 내재한 취약성인 Vulnerability, 대상의 취약점이 주체의 행위와 작용한 결과인 Consequence로 구성된다. 이것은 공격의 가장 기본적인 구성요소를 나타낸다.



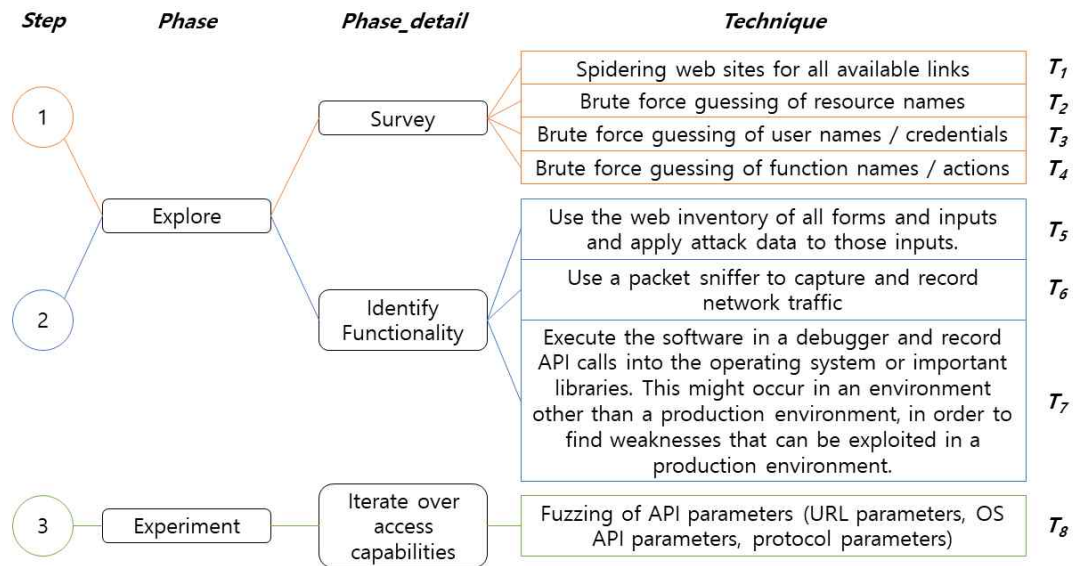
<그림 5> 공격 이벤트 구성

하나의 이벤트에는 이 여섯 가지 구성요소가 모두 존재해야 하며 어느 하나라도 존재하지 않으면 이벤트로 보지 않는다. 이것을 기준으로 식별된 자산과 내재한 취약성, 상황 정보를 활용하여 관찰대상 이벤트를 정의하고 탐지 규칙을 만든다.

보호해야 할 자산에 가할 수 있는 공격을 탐지하기 위해, 식별된 취약성과 관련하여 그 취약성에 가할 수 있는 일반적인 행위 패턴, 패턴에 의한 공격대상 자산의 진입지점 노출 여부, 그리고 그 행위 패턴을 실행할 수 있는 공격자의 특성을 활용한다. 실무적으로, 식별된 취약성의 일반화된 분류 코드(CWE)를 통해 일반화된 공격 행위 패턴(CAPEC)을 얻을 수 있고, 해당 취약성이 존재하는 자산의 노출된 진입점을 경유하여 CAPEC에 정의된 행위를 하는 공격자를 찾는다.

CAPEC에 정의된 행위를 탐지하기 위한 한 가지 예로서, CAPEC 데이터 내에 존재하는 Execution_Flow 필드를 활용할 수 있다. 이 사전 정의된 필드는 공격과 관련된 실행 흐름 속에서 공격으로 이어지는 행위를 파악하여 관찰대상 이벤트를 정의하는 데 도움을 준다.

<그림 6>의 예시는 「CAPEC-1. ACL에 의해 기능이 제대로 제한되지 않음」에 대한 Execution_Flow 필드를 분석한 내용을 보여준다. 사고탐지 규칙을 구성하기 위해 Technique 필드에 나타난 공격을 구성하는 단위 행위를 순서대로 T₁ ~ T₈로



<그림 6> Execution_Flow 필드로부터 얻는 정보

정의하고, 상황인식 관점의 각종 흐름 정보를 이용해 실제 발생하는 공격 이벤트를 식별한다. 이후 Step 필드를 통해 행위 간 관계를 정의한다. Technique 필드 값이 같은 행위는 OR 연산으로, 다른 행위는 AND 연산으로 간주한다면 이벤트 추출을 위한 단위 행위 간 관계식은 아래와 같다.

$$Attack = (T_1 \oplus T_2 \oplus T_3 \oplus T_4) \otimes (T_5 \oplus T_6 \oplus T_7) \otimes T_8$$

4) 티켓 추출

현실적으로 취약성을 아무리 제거한다고 해도 실제 기업 환경의 특성상 다양한 취약성이 존재하기 마련이며, 성숙한 취약성 진단 활동을 해나가는 조직일수록 자산 취약성 데이터가 활발히 확보되어 관찰대상 이벤트에 관한 탐지 수가 증가하게 된다. 그러나 모든 공격 이벤트에 대해 담당자가 대응하기에는 무리가 있으며 공격 이벤트 중에는 직접적인 확인을 요구하지 않는 수용 가능한 이벤트도 있으므로, 수많은 공격 이벤트 중에서 특히 관찰해야 하는 대상을 따로 선별해야 하는데 이 과정을 티켓 추출 혹은 티켓팅이라 하고 선별된 이벤트를 티켓 이벤트라 한다.

티켓 이벤트를 선정하기 위해 위험도를 사용하며, 위험도는 자산의 가치에 따라 자산에 영향을 끼치는 피해의 정도 및 위험이 발생할 가능성을 감안하여

인시던트와 취약성을 각각 분리하여 산출한다. 위험도 평가 산식은 다음과 같다.

$$Risk\ Value = Asset\ Value + \{(Concern\ Value \times 2) \times Likelihood\}$$

- Risk Value : 티켓의 위험도
- Asset Value : CIA 평가값 (최소 3, 최대 9)
- Concern Value : 위험 · 취약성을 포함한 값 (최소 1, 최대 3)
- Likelihood : 발생가능성 (최소 1, 최대 2)

여기서, Likelihood를 수치 형태로 변환하여 연산하기 위해 취약성과 공격은 서로의 발생 가능성에 기여한다는 것을 근거로 <표 6>과 같은 기준을 적용한다.

상 (Top10)	중 (Top11~50)	하 (Top51~)
2	1.5	1

<표 6> 공격 발생가능성 수치화

하나의 공격이 여러 개의 취약성을 활용할 경우에 취약성의 관계가 AND이면 공격을 성공시키기 위해 모든 취약성을 악용해야 하므로 Exploitability는 개별 취약성 악용 용이성의 곱의 형태이며, OR 관계이면 하나의 취약성만 실현하면 되므로 개별 취약성 악용 용이성 중 최대값이 된다.

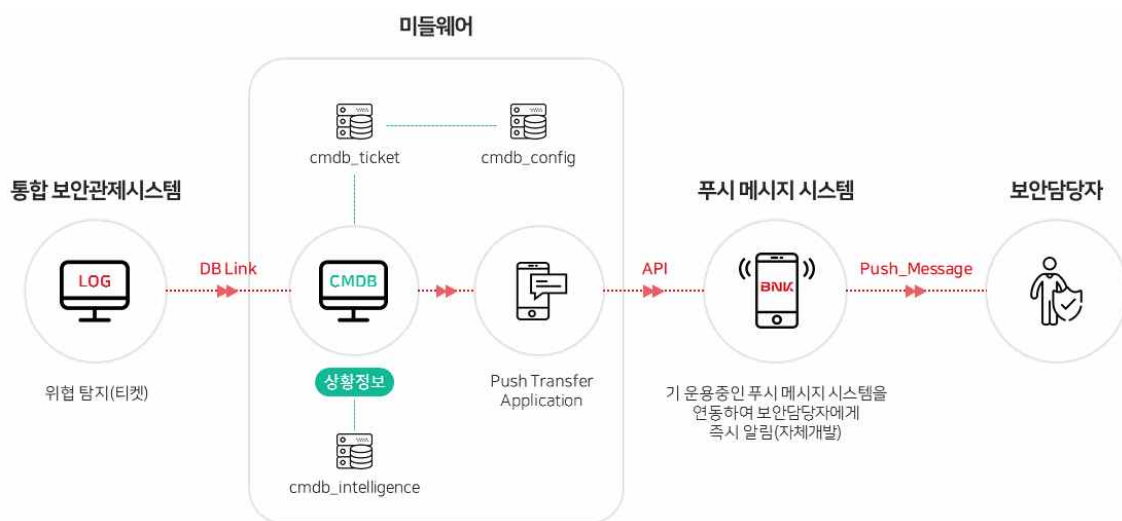
산출된 위험의 정도에 따라 정보보호조직의 능력 수준에 따라 대응할 이벤트를 선별하기 위한 기술적 위험도 임계치를 정해준다. SIEM은 정해진 규칙에 따라 공격과 관련된 이벤트를 관찰하고 그 위험도가 임계치 수준을 벗어나면 정보보호조직 담당자가 확인해야 할 티켓을 발행한다. 이 방식을 이용하면 같은 공격 패턴이 감지되더라도 자산의 중요한 정도에 따라, 자산이 보유한 취약성이 공격에 영향 받는 정도와 악용되었을 가능성에 따라 관찰해야 할 이벤트를 적절히 추출해주는 효과를 얻는다.

빅데이터 솔루션(Logpresso)에 기반한 SONAR 솔루션은 수집된 보안장비 로그를 <그림 7>과 같이 실시간 및 배치로 룰을 설정할 수 있으며, 룰에 의해 탐지된 로그(이벤트)를 티켓으로 설정할 수 있다.

한편 룰에 의해 탐지된 티켓 중에서 위험도가 높은 경우에는 <그림 8>과 같이 해당 티켓과 관련된 담당자에게 자체개발한 푸시메시지시스템을 통해 경고알림을 제공한다.



<그림 7> SIEM 실시간 탐지 룰 목록



<그림 8> 경고알림시스템 구성

ETIR모델의 위험식별 단계에서 SOAR 구성요소와 관련된 내용은 다음 <표 7>과 같다.

SOAR 구성요소	위험식별 단계
SOA	- 보안관제대상 자산을 SIEM과 동일하게 통합 관리하며, 각 자산에서 발생한 로그를 실시간으로 수집함

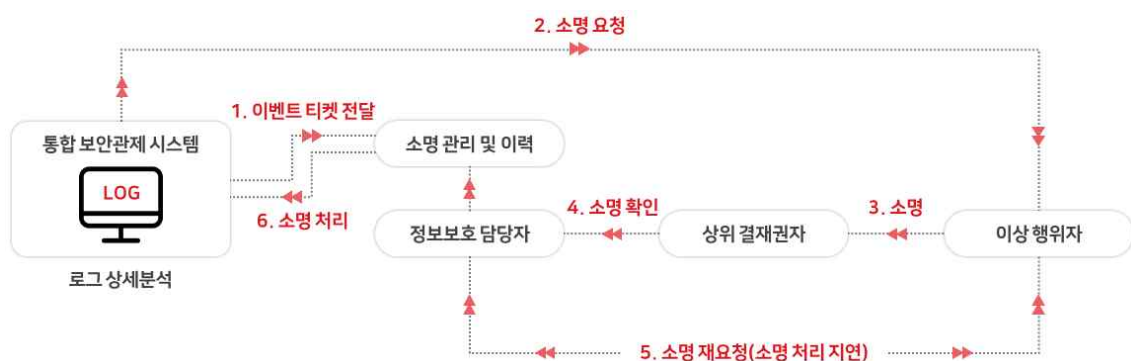
	<ul style="list-style-type: none"> - 자산의 위험도는 Archer에서 자동으로 담당자의 CIA 평가가 할당되며, Nexpose를 활용하여 자동으로 자산의 CVE 위험을 식별함 - 위험도 계산식을 활용하여 발생한 이벤트에 대한 티켓을 자동으로 발행함
TIP	<ul style="list-style-type: none"> - 자산 위험도 측정 솔루션을 활용하여 자산의 취약점을 CVE 관점으로 관리함

<표 7> 위험식별 단계와 SOAR 구성요소

(2) 위험분석 단계

1) 티켓 조사

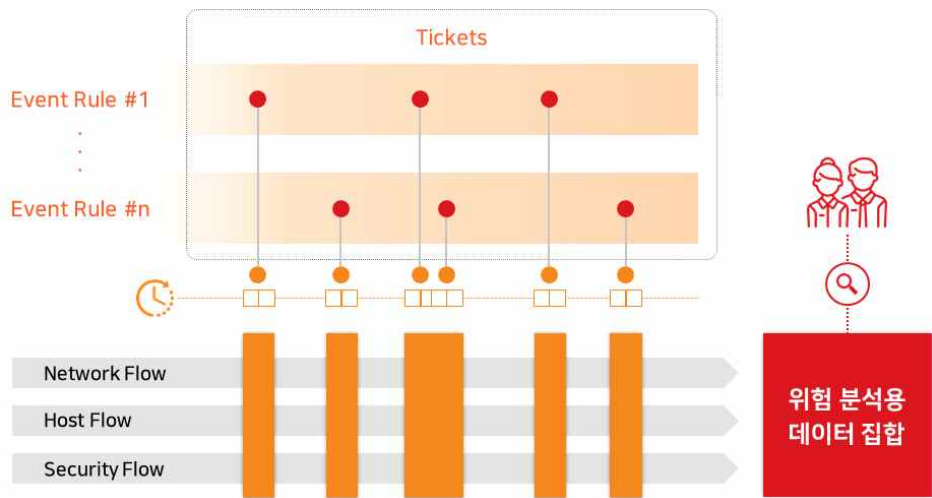
정보보호 담당자는 티켓을 조사하여 오용 탐지 여부와 자산 혹은 비즈니스에 손실이 있는지를 조사하기 위해 분석가에게 심화 분석을 요청하고 그 결과를 바탕으로 관련자들에게 <그림 9>과 같이 소명처리를 수행한다. 소명 프로세스는 자동소명과 수동소명으로 구분되며, 자동소명은 소명대상자를 자동으로 지정하는 것이고 수동소명은 보안관계 담당자가 티켓의 내용을 분석하여 소명대상자를 지정하는 것이다. 자동소명 대상 티켓은 보안감사(감사자) 및 자산 가용성 알림(자산담당자)과 같이 소명처리자가 명확한 경우이며, 자동소명은 소명 프로세스를 보다 효율적으로 처리할 수 있다.



<그림 9> 소명 프로세스

분석가의 심화 분석은 티켓이 발생하기 전후의 다른 티켓과 티켓이 되지 못한 이벤트, 상황인식 관점의 Flow 정보를 활용하여 공격하기 직전과 직후의 행위를 관찰한다. 이를 통해 공격자의 동기, 의지, 기술 수준, 공격에 따른 피해 범위를 유추할 수 있으며, 소명은 이를 파악하는데 유용한 프로세스이다. 관련자들에게 티켓과 관련된 사유를 직접 소명 받아 분석가의 분석 결과와 대조하여 티켓의 인시던트화 여부를 결정한다.

이러한 티켓 조사 과정에서 분석가가 분석을 효과적으로 수행할 수 있도록 도와주는 데이터 집합을 구성할 수 있다. 분석가는 티켓 조사 과정에서 티켓 발생 지점 근처의 정보들을 조사하는 경향이 있다. 이를 위해 티켓 발생 지점을 식별하여 전후의 관련 Flow에 해당하는 정보를 모아주는 프로세스를 SIEM으로 구현하는 방식은 <그림 10>과 같다.



<그림 10> 위험분석을 위한 데이터 집합 확보 방안

각 이벤트 탐지 규칙에서 나오는 티켓의 발생시간을 중심으로 미리 설정된 전후의 기초적인 조사범위 시간 내에 있는 이벤트와 관련된 Flow를 추출하여 위험분석을 위한 데이터 집합을 구성한다. 이벤트와 관련된 Flow는 출발지 및 도착지가 공격자이거나 공격대상인 모든 이벤트를 말한다.

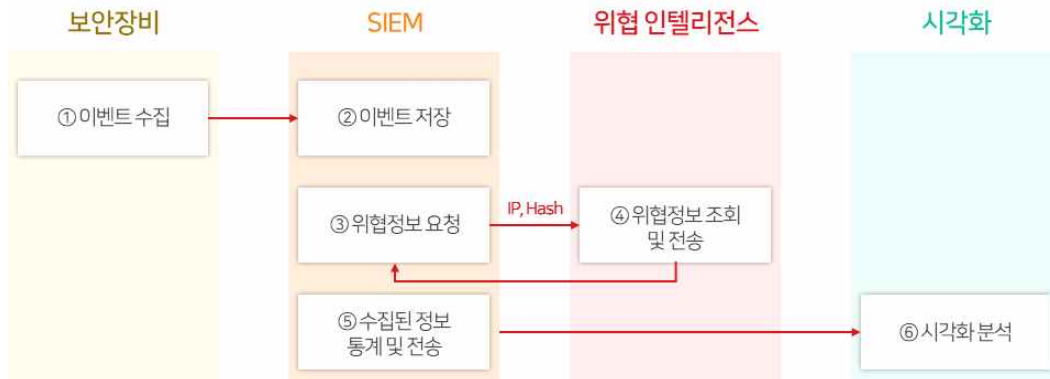
한편 다양한 관점에서 분석을 효과적으로 수행하기 위해 시각화 솔루션(Qlik Sense 등)이 필요하며, 시각화 솔루션은 실무에서 대량의 데이터로부터 관련이 있을 가능성이 큰 정보를 추출하여 분석 활동에 효율성을 제공한다.

부산은행에서는 3년 전에 개인정보 관련 업무에 활용하기 위해 시각화 솔루션을 도입하였으며, 최근에는 보안관계 업무에서 위협 분석을 위해 확대 도입하였다. 시각화 솔루션의 화이트&그레이 기법은 쉬운 데이터 필터링과 이기종 로그를 통합관리 할 수 있기 때문에, 효율적으로 동일 식별자 (사번, IP 등)에 대한 다양한 분석을 할 수 있다. <그림 11>은 2019.7월에 발생한 악성 메일을 시각화 솔루션에서 분석하는 화면이다.



<그림 11> 악성 메일 분석(시각화 솔루션)

특히, 이기종 보안장비의 로그를 시각화 솔루션을 활용하여 분석할 때, 위협에 대한 빠른 판단을 위해 IP 및 파일정보(파일명, Hash 값)에 대한 위협 인텔리전스 정보 및 위치정보를 연동한다. 이를 위해 <그림 12> 과 같이 SK인포섹의 위협 인텔리전스 서비스와 Maxmind의 GeoIP 서비스를 도입하였으며, 보안장비(IPS, DDoS 등)에서 수집된 IP 및 파일 Hash값에 대한 위협정보를 API 방식으로 실시간 수집한다.



<그림 12> 위협분석을 위한 위협 인텔리전스 수집 및 시각화

마지막으로 분석 결과에 따라 사고로 판단되는 것은 사건의 발생 순서에 근거한 타임라인 차트로 작성하고, 발급된 티켓을 인시던트화 한다. 사고가 아니라고 판단되는 경우에는 사유를 기재하고 일시적 오류인지, 이벤트 탐지 규칙의 개선이 필요한지에 따라 향후 동일한 오용 탐지가 발생하지 않도록 이벤트 룰을 정비한다.

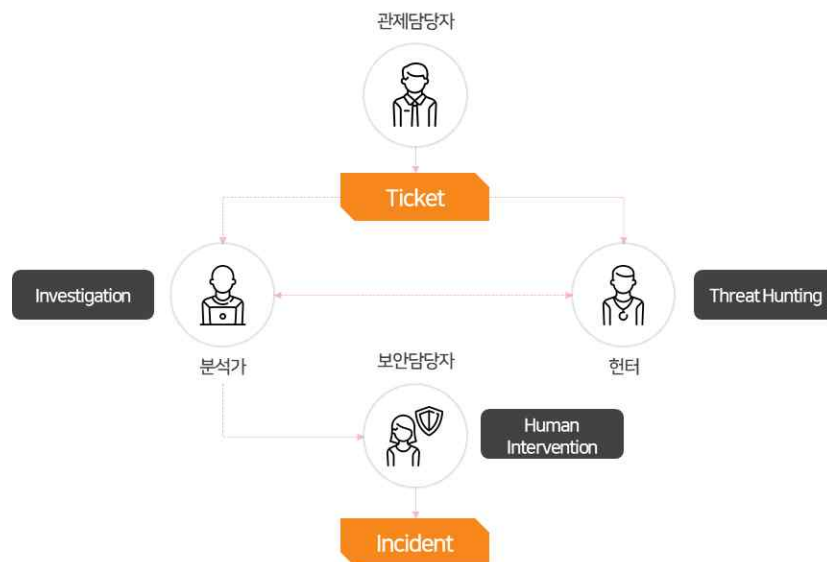
2) 인시던트 생성

인시던트는 위협이 실체화된 것이며, 티켓에 대해 False positive 검증을 수행한 결과로 직·간접적인 피해가 있다고 보는 티켓 이벤트이다. 인시던트 생성 방법은 사고의 수를 합리적으로 낮게 유지하여 침해사고 대응팀의 사고 대응 시간을 줄여줄 뿐 아니라, 분석 정확도가 높아지므로 조직의 비즈니스 프로세스를 보호하는 데 매우 유용하다. 발급하는 인시던트의 헤더 영역은 고유 ID를 포함하여 위협 헤더가 더 붙게 된다. 위협 헤더의 각 영역의 값은 사전 정의된 위협 분류, 영향, 원인, 주체, 심각도 영역에서 해당하는 값을 채우는 형식으로 조합한다.

- 위협 분류 : 발생한 인시던트가 어떠한 위협 분류에 속하는가를 검토한다. 이를 통해 위협에 직접적인 요인으로 작용하는 위협이 어떤 것들이 있는지 구분할 수 있으며 개선해야 하는 위협을 신속하게 식별하여 의사결정 요소로 활용할 수 있다.
- 위협 영향 : 실체화된 인시던트가 정보보호 3요소 중 어느 부분에 영향을 주었는가를 검토한다.

- 위협 원인 : 실제화된 인시던트가 어떠한 원인에 의해서 발생했는가를 검토한다.
- 위협 주체 : 실제화된 인시던트를 일으킨 주체에 대한 정보를 검토한다. 위협 주체를 분석함으로써 공격 동기와 의지, 기술 수준을 파악하고 향후 침투 행위를 예측할 수 있다[18].
- 위협 심각도 : 실제화된 인시던트에 따른 심각도를 다음의 기준에서 평가한다. 이 평가는 비즈니스 위협 요소와 연결시키는 근거가 된다.

SOAR에서 Threat Hunting과 Investigation 과정은 <그림 13>과 같이 유기적인 의사소통을 통해 Human Intervention을 위한 기초자료를 생성한다. 발생된 티켓에 대하여 헌터는 추가적인 증거를 찾아 분석가에게 IOC(Indicators of Compromise, 침해지표) 형태로 제공하고 분석가는 그 티켓과 관련된 IOC 들을 연관 분석한다. 이 때, 판단 근거가 되는 IOC가 부족할 경우, 헌터에게 추가적인 증거 수집을 통한 IOC 제공을 요청한다.



<그림 13> 인시던트 생성을 위한 역할 및 절차

이 과정에서 수집된 각종 증거(Artifact)들은 상위 개념인 분석 단계에서 사용되기 위해 IOC와 같은 형태로 일반화된다. Threat Hunting은 OS나 네트워크의 하위 레벨 지식을 요구하는데, 다른 어떤 단계보다 분석가의 역량에 의존적인 과정이다.

EDR(Endpoint Detection & Response)과 같은 솔루션은 이러한 Threat Hunting 과정의 결과로서 만들어진 도구이며, 이것은 Threat Hunting 과정을 상당부분 절약하면서 Investigation 과정을 수행하도록 해준다.

다만, 상황에 따라 Investigation 과정에서 증거들이 다소 부족하여 Threat Hunting 과정을 요구할 경우가 있고, 이 과정을 통해 얻어지는 Artifact는 Investigation에 사용하며, Artifact를 자동화하는 방법으로 EDR을 고도화할 수 있다. 이는 네트워크 관점에서도 마찬가지다.

Threat Hunting은 운영체제와 네트워크 관점에서 수행될 수 있으며, 티켓의 유형에 따라 분석 방법이 결정될 것이다. 헌터는 EDR이나 IPS 등 기존 보안 장비에서 찾지 못하는 요소를 찾을 수 있어야 한다. 이러한 활동을 위해서는 여러 가지 포렌식 도구들을 활용하는 것이 적합하며, 포렌식 도구는 판단이 중요한 것이 아니라 대상을 있는 그대로 파악하여 보여주는 것이 관건이다. 대상을 보여줄 때 추가적인 정보를 테깅해서 보여줄 수 있으나 판단은 이 도구를 사용하는 헌터의 몫이다. 운영체제를 헌팅하기 적합한 솔루션은 Encase와 같은 툴이며, 네트워크를 헌팅하기 위해 네트워크 분석 전문 솔루션인 Netwitness를 도입하였다.

또한 인시던트로 식별된 경우에 즉시적인 대응을 위해, 단말 EDR 솔루션의 관리 기능(네트워크 차단/허용, 단말 알림, 파일 수집 등)에 대한 API 개발을 개발사에 의뢰하였다. API가 개발되면 SIEM의 소명 프로세스 과정에서 사전에 정의한 대응을 소명 화면에서 수행할 수 있기 때문에, 업무 효율성 및 대응 즉시성이 증대될 것으로 기대된다.

ETIR모델의 위험분석 단계에서 SOAR 구성요소와 관련된 내용은 다음 <표 8>와 같다.

SOAR 구성요소	위험분석 단계
SOA	<ul style="list-style-type: none"> - 이기종 솔루션의 로그를 시각화 솔루션에 연동하였기 때문에 다양한 관점의 위협 분석이 효과적임 - 티켓 프로세스의 효율적인 자동화를 위해 보안감사 및 가용성 티켓의 소명 대상자는 자동으로 설정함
SIR	<ul style="list-style-type: none"> - 티켓으로 식별된 위협 이벤트를 미리 정해진 SIEM의 소명 절차를 활용하여 파급력 및 사고 유무를 식별함

	- 인시던트에 대한 즉시적 대응을 위해 단말 EDR 솔루션의 통제 기능을 소명 절차에 연동함
TIP	- 효율적인 위협분석을 위해 위협 객체인 IP 및 파일 Hash값에 대한 위협 인텔리전스를 수집하고 시각화함

<표 8> 위협분석 단계와 SOAR 구성요소

(3) 위험수준 평가 단계

위험수준 평가 단계는 발생한 인시던트를 비즈니스 측면의 위험으로 표현하는 과정이며, 기술적 측면보다는 조직적인 관점에서 임직원들이 이해하기 쉽게 표현하는데 초점을 맞춘다. 비즈니스 측면의 위험은 다음과 같이 5가지의 카테고리로 구분하였다.

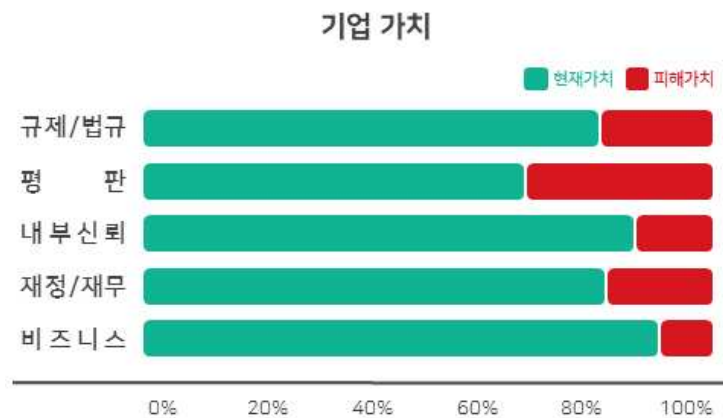
- 비즈니스 위험 : 업무, 서비스의 연속성이나 품질과 관련된 피해
- 재정/재무 위험 : 손해배상, 복구 등 금전적 손해와 관련된 피해
- 내부신뢰 위험 : 내부 질서의 붕괴, 구성원 간의 불신 등과 관련된 피해
- 평판 위험 : 기업 이미지 실추와 관련된 피해
- 규제/법규 위험 : 상위 법령 혹은 내규를 위반함에 따른 제재조치, 처벌에 관한 피해

인시던트가 발생하면 대응되는 비즈니스 위험이 존재하며, 이것은 앞서 계산한 기술적 위험도와는 다른 비즈니스 측면의 위험을 고려해야 한다. <그림 14>과 같이 인시던트로 인해 정보자산이 어떠한 단위절차에 요구가치를 만족하지 못한다면 해당 단위절차의 실패로부터 연속적인 비즈니스 위험 증가를 초래한다. 단위절차의 실패에 따른 심각도를 인시던트 심각도 기준에서 아래와 같이 평가하고, 단위절차와 다른 구성요소 간 포함관계에 의해 비즈니스 위험을 최신화해야 한다.



<그림 14> 정보자산과 비즈니스 구성요소 간 가치 기여관계

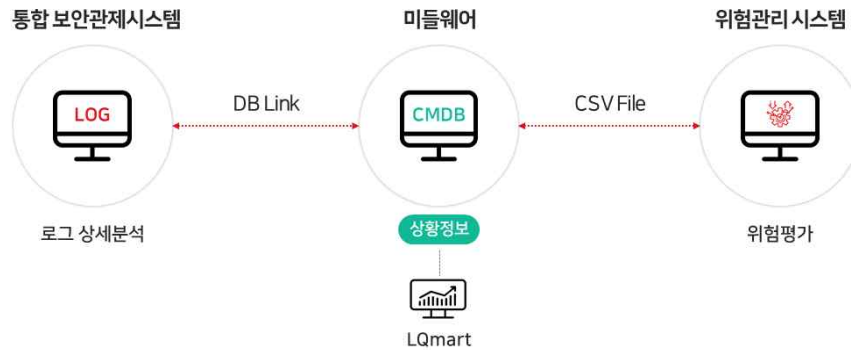
<그림 14>에서 각 비즈니스 요소는 정보자산의 기능을 활용하여 “비즈니스, 재정/재무, 내부신뢰, 평판, 규제/법규” 영역에 가치를 부여한다. 만약 이 기능과 관련된 정보자산에 어떠한 공격이 가해져 기능 서비스가 불가능해지는 경우 단위절차는 정상적인 기능을 할 수 없다. 말은바 가치를 다하지 못하는 단위절차는 상위 개념인 절차와 역할 영역에도 영향을 주게 되고, 기업 거버넌스 입장에서 바라볼 때 피해가 초래된다.



<그림 15> 기업 가치의 표현 예시

<그림 15>는 어떠한 피해가 발생했을 때, 현재가치에서 피해 가치만큼의 손실이 발생했음을 보여주는 예시이다. 이러한 지표를 통해, 발생한 피해 가치를 어떻게 만회할 것인지를 고민할 수 있게 된다. 해당 정보자산의 기능을 복구하거나 재개발하여 서비스를 재개할 것인지, 단위절차를 바꾸어 위험을 회피할 것인가를 결정해야 한다. 모든 과정에는 비용과 시간이라는 지출이 발생하게 되어 경영진 차원의 의사결정이 필요하다. 제안 모델은 경영진의 의사결정에 필요한 데이터를 제시한다.

관련 데이터를 제공하기 위해 RSA의 Archer 솔루션을 도입하였으며, 보안관제 시스템의 인시던트 정보를 효율적으로 활용하기 위해 <그림 16>와 같이 SIEM 역할을 수행하는 SONAR 솔루션과 연동을 자동화하였다.



<그림 16> SIEM과 위험관리시스템 연동

또한 위험관리시스템의 중요 데이터를 SIEM의 Dashboard를 이용하여 <그림 17>과 같이 구성하였으며, 인시던트 및 위험 처리현황을 중점으로 나타내었다.



<그림 17> SIEM의 위험관리시스템 Dashboard

ETIR모텔의 위험수준 평가 단계에서 SOAR 구성요소와 관련된 내용은 다음 <표 9>과 같다.

SOAR 구성요소	위험수준 평가 단계
SOA	- 보안관제 결과를 위험관리 프로세스에 실시간으로 반영하기 위해 SIEM과 위험관리시스템의 데이터를 자동화하여 연동함

SIR	- 인시던트로 식별된 티켓에 대하여 Archer에서 자체 정의한 위험수준 평가 업무를 수행함
-----	---

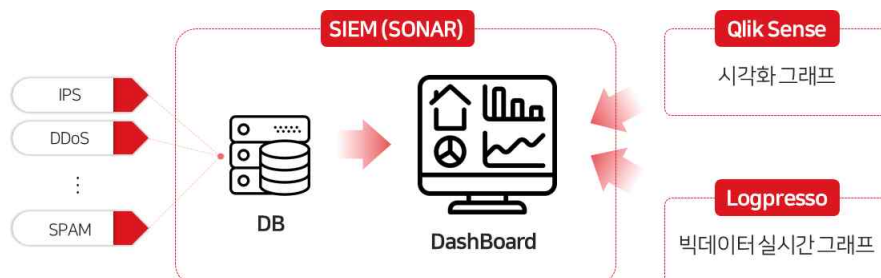
<표 9> 위험수준 평가 단계와 SOAR 구성요소

IV. 동적 통합보안관제 모니터링

본 장에서는 ETIR관점의 유기적인 통합모니터링을 위해 구축한 동적 통합보안관제 모니터링을 소개한다. 통합보안관제를 위해 이기종 Dashboard를 연동(매쉬업 기능 적용)하였으며, 동적 모니터링을 위해 그래프 생성 및 화면 구성이 간단한 위젯으로만 설계하였다.

1. 이기종 Dashboard 연동

본 논문에서 설계 및 구축한 보안관제체계는 다양한 관점에서의 운영과 관리를 하기 위해 이기종의 보안시스템이 도입되었다. 고도화된 공격으로부터 안전한 금융망을 위해서는 다 수의 솔루션을 관리해야 되지만 금융권에서 다 수의 솔루션을 관리하기 위한 정보보호부서의 인원은 충분하지 못하다. 이러한 현실적인 금융권 정보보호부서의 상황으로 인해 다 수의 솔루션에서 도출되는 로그의 심화분석 및 상관분석은 제한적이다. 부산은행에서는 이러한 한계점을 극복하기 위하여 <그림 18>과 같이 이기종 보안솔루션의 로그를 SIEM 솔루션(SONAR)의 Dashboard로 표현하고, 특히 다차원 분석을 위한 시각화 솔루션의 그래프를 SIEM 솔루션의 Dashboard에 iframe 기능을 활용하여 표현하였다. 또한 동일 제조사의 빅데이터 솔루션의 실시간 그래프도 SIEM 솔루션에 연동하였다.



<그림 18> 이기종 Dashboard 연동

시각화 그래프와 연동으로 인하여 시각화 솔루션의 강점인 상관분석, 다양한 그래프, 스토리텔링 등의 기능을 SIEM에서 유기적으로 활용하게 되었다. 이로 인해 비전문가도 유의미한 심화분석을 할 수 있으며, 짧은 시간에 분석이 가능하다.

2. 동적 모니터링

다양하고 복잡한 유형의 외부위협들을 모니터링하기 위해서는 매우 많은 정적 모니터링 그래프를 사전에 구성해야 되며, 특수한 공격의 경우에는 관련 모니터링이 제한적일 수 있다. 이러한 문제점을 해결하기 위해 부산은행에서는 동적으로 통합보안관제를 모니터링할 수 있는 위젯으로만 보안관제 모니터링을 구성했다. 위젯은 SIEM의 Dashboard에서 제공해주는 기본 기능이며, 그래프를 변경하거나 신규로 생성하기에 간편하게 설계되어 있다.

<그림 19>은 현재 부산은행 관제센터의 모니터링 화면이며, 10대의 멀티비전 및 월컨트롤러 설치로 자유로운 화면 구성도 가능하다. 10대의 멀티비전이 하나의 솔루션의 Dashboard처럼 보이지만 3종의 솔루션 그래프 및 10여종의 솔루션 데이터를 나타내고 있다. 최초에 화면을 구성하기 위해 1일(8H)이 소요되었으며, 수정되거나 추가되는 화면은 1H 이내에 변경이 가능하였다.



<그림 19> 정보보호 관제센터

평시 부산은행 관제센터는 ETIR 관점의 모니터링을 위한 Dashboard를 <그림

20>과 같이 10대의 멀티비전에 구성하였으며, 전문 보안관제 인력(부산은행 1명, SK인포섹 2명)이 실시간으로 이벤트 분석 및 티켓 처리 업무를 수행한다.



<그림 20> ETIR기반 모니터링 Dashboard

부산은행은 SK인포섹 보안관제 전문 인력과 3년 동안 협업하여, 2019.05월에 관제센터 및 ETIR기반 모니터링 관제체계가 구축 완료되었다. 현재 SIEM의 인텔리전스 API 호출 기능을 적용 중이며, 향후에는 인공지능 기술 등을 활용하여 보다 효율적이고 정확한 보안관제체계를 구축할 예정이다. 또한 지속적으로 발전하고 있는 APT 공격을 식별 및 차단하기 위해, 이벤트 수집 및 티켓 룰을 주기적으로 고도화하여 운영할 계획이다.

3. 활용 사례 및 성과

(1) 보안활동보고서 통합

부산은행은 매일 다수의 정기보고서를 하나의 통합된 보안활동보고서로 작성하고 있다. 시각화솔루션에서 보관된 데이터를 다양한 다차원 그래프를 통해 부서 내 수기로 작성하였던 일간, 월간보고서를 자동화 및 통합하게 되었다. 하지만 매년 일관되고 정형화된 보고서 형식은 다양하고 고도화된 보안위협을 이해하기에는 부족하다. 이에 따라 <그림 21>과 같이 평소 보안관제 활동을 통해 식별된 위험분석을 기반으로 의미 있는 보고서를 작성하고 있다.



<그림 21> 보안활동보고서 통합

(2) 메일제목 유사도 측정 및 악성메일 탐지

2019년에도 다수의 직원을 대상으로한 악성메일 공격이 발생하였으며, 신규 패턴의 악성파일을 첨부한 악성메일은 관련 보안솔루션 패치 시간까지 탐지가 불가능한 상황도 나타났다. 부산은행에서는 보안솔루션이 탐지를 못하는 상황에서 악성메일 유포현황을 5분 이내에 식별하였으며, 향후 동일한 유형의 공격을 차단하기 위한 룰을 SIEM에 설계 및 적용하였다.

<그림 22>과 같이 부서원의 악성메일 의심 신고로 부터 5분 이내에 관련 솔루션 로그 분석 및 시각화 다차원 분석을 하였으며, 악성메일의 내부 영향도를 식별하고 유사한 유형의 악성메일 차단 정책을 적용하였다.



<그림 22> 신규패턴 악성메일 식별 및 대응

특히 최근에 발생한 악성메일은 <표 10>과 같이 메일 제목과 파일명이

동일하거나 유사도가 높은 것으로 확인되었다.

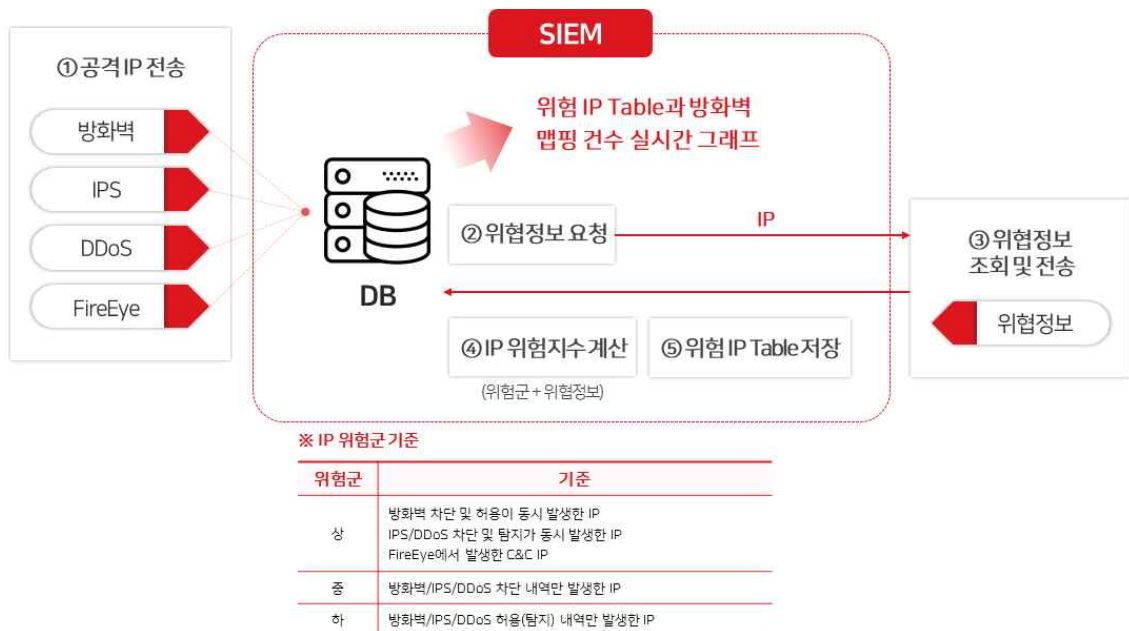
발생일자	악성메일 제목	악성메일 파일명
2018.11.20	- Thanksgiving Day email ~ - Thanksgiving Day ~ - The Thanksgiving Day ~	
	- INVOICE FO-99-23432	
2019.02.27	- 인보이스 XX-XX-2019	- 인보이스 XX-XX-2019.xls
	- 송장_0019XXXX	- 송장_0019XXXX.doc
2019.03.06	- 0603_XXXXXXXXXXXX	- 0603_XXXXXXXXXXXX.xls
2019.03.07	- 한국 헌법 재판소에서 기자	- 07-03-2019.rar
	- 증명서	- 증명서.doc
2019.07.25	- 대한항공 e-티켓 확인증	- e-Ticket 확인증_XXXX.iso

<표 10> 악성메일 제목 및 파일명 현황

이와 같은 악성메일 추이에 따라, 메일제목 및 파일명의 유사도를 측정하여 유사도가 높은 메일이 다 건 수신될 경우에 티켓을 발생하도록 SIEM 룰을 추가하였다. 또한, 평소 악성메일로 차단되는 메일 중에서 메일 제목이 기존 패턴과 다른 메일이 감지되면 티켓을 발급하도록 설정하였다. 유사도를 측정하는 방식은 TF-IDF, 확장 자카드 계수, 코사인 유사도 등을 활용하였다.

(3) 보안장비 탐지IP 정보와 위협 인텔리전스 융합

다양한 기관에서 주기적으로 위협IP 정보를 수집하고, 해당 IP를 방화벽 및 DDoS 장비에서 차단한다. 하지만, 정보 수집 주기가 일일/주간으로 실시간성을 제공하지 못하며, 그로 인해 부산은행 등 금융기관을 대상으로 발생하는 실제적인 위협 IP 정보 (위험도가 높아 즉시 차단이 필요한 IP) 식별이 제한적이다. 이러한 문제점들을 해결하기 위해 <그림 23>과 같이 외부 인텔리전스 서비스를 활용하여, 차단 정책이 적용되지 않은 IP 중 부산은행을 직접적으로 공격한 대상을 식별하는 룰을 SIEM에 적용하였다.



<그림 23> 보안장비 탐지 IP 정보와 위협 인텔리전스 융합

SIEM에서 보안장비(IPS, DDoS, FireEye)에서 차단/탐지한 IP 및 방화벽 차단/허용 IP를 수집하여 주기적으로 해당 IP별 위협정보를 수집한다. 이후, 위험군과 위협정보를 종합하여 위험지수를 계산하고, 위협 IP Table에 결과를 저장한다. SIEM에서는 위협 IP Table에 등록된 IP와 방화벽 실시간 로그를 맵핑하여 그래프를 출력한다. 전 과정은 자동화되며, 최신화된 위협IP에 대한 통신내역을 모니터링 할 수 있다.

V. 결론

최근 고도화된 APT 공격 등이 다양한 경로로 유입되고 있으며, 이러한 공격이 내부망에 감염될 경우에는 금융기업의 특성상 상당한 피해가 초래된다. 사이버 공간에서 발생하는 위험들을 실시간으로 식별하고 적절한 대응을 하기 위하여, 본 논문에서는 위협평가를 위한 ETIR 모델을 설계하고 적합한 솔루션과 SIEM을 연동하였다. 특히 부산은행 정보보호부 담당자가 금융보안관계 업무를 수행하면서

제약사항이 되었던 자산관리 일관성 및 통일성을 위해 CMDB를 구성하였다. 또한 제안한 보안관제체계의 특징점을 SIEM의 단점들을 해결하기 위해 소개된 SOAR의 기능(SOA, SIR, TIP)과 연관하여 분석하였다. 게다가 부산은행은 고도화된 보안관제체계를 보다 효율적으로 운영하기 위하여 SONAR 솔루션의 위젯기능만으로 관제 모니터링 화면을 구성하였고, 이기종 솔루션의 그래프 및 실시간 데이터를 SONAR의 iframe을 이용하여 단일 Dashboard에서 출력하였다. 구축한 보안관제체계를 통해 위협분석 기반 보안활동보고서를 통합할 수 있었으며, 악성메일의 제목 유사도를 측정하여 신종 악성메일을 탐지할 수 있는 룰을 SIEM에 적용할 수 있었다.

최근에는 매우 다양한 유형의 위협이 발생하고 있기 때문에, 시기적절한 관점의 보안관제모니터링 및 대응이 중요한 시기이다. 이러한 관점에서 제안한 보안관제체계의 가장 큰 장점은 보안관제 담당자가 “원하는 대로, 즉시적으로, 자동으로” 필요한 정보를 모니터링 및 분석할 수 있다는 것이다.

[참고문헌]

- [1] 정윤수. “기업 정보화 역기능에 따른 피해를 최소화하기 위한 기업 정보 처리 모델 설계”, 중소기업융합학회논문지 (구 중소기업정보기술융합학회논문지), 6(2), 11-17, 2016.
- [2] Virvilis, N., & Gritzalis, D. “The big four-what we did wrong in advanced persistent threat detection?. In 2013 International Conference on Availability, Reliability and Security,” pp. 248-254. IEEE., 2013.
- [3] Ask, M., Bondarenko, P., Rekdal, J. et. al. “Advanced persistent threat (APT) beyond the hype,” Project Report in IMT4582 Network Security at Gjovik University College, 2013.
- [4] Cyber Security Governance: A Component of MITRE’s Cyber Prep Methodology. MITRE TECHNICAL REPORT, 2010.
- [5] Khoo, B., Harris, P., & Hartman, S., “Information security governance of enterprise information systems: An approach to legislative compliant”, International Journal of Management and Information Systems, 14(3), 49-55, 2010.
- [6] 장상수, 노봉남, 이상준, “정보보호 관리체계 운용이 정보보호 성과에 미치는 영향”, 정보과학회논문지: 정보통신, 40(1), 58-69, 2013.
- [7] Ula, M., Ismail, Z., & Sidek, Z. M., “A Framework for the governance of information security in banking system”, Journal of Information Assurance & Cyber Security, 2011, 1-12, 2011.
- [8] Oliver Rochford, “Overcoming Common Causes for SIEM Deployment Failures.”, Gartner, G00260858, 2014.
- [9] Faris, S., Ghazouani, M., Medromi, H., Sayouti, A., “Information security risk Assessment—A practical approach with a mathematical formulation of risk”, International Journal of Computer Applications, 103(8), 36-42, 2014.
- [10] Information technology - Security techniques - Information security risk management. INTERNATIONAL STANDARD ISO/IEC 27005:2018 Edition, 2018.
- [11] 엄진국, 권현영, “SIEM 을 이용한 침해사고 탐지방법 모델 제안”, 한국인터넷방송통신학회 논문지, 16(6), 43-54, 2016.

- [12] Tripathi, A., Singh, U. K., “Estimating risk levels for vulnerability categories using CVSS” , International Journal of Internet Technology and Secured Transactions, 4(4), 272-289, 2012.
- [13] Goel, S., Williams, K., Dincelli, E. “Got phished? Internet security and human vulnerability” , Journal of the Association for Information Systems, 18(1), 2, 2017.
- [14] Elmontsri, M. “Review of the strengths and weaknesses of risk matrices” , Journal of Risk Analysis and Crisis Response, 4(1), 49-57, 2013.
- [15] Chung, Y. J., Kim, I., Lee, N., Lee, T., et. al., “Security risk vector for quantitative asset assessment” , In International Conference on Computational Science and Its Applications, pp. 274-283. Springer, Berlin, Heidelberg, 2005.
- [16] Holm, H., Shahzad, K., Buschle, M., et. al., “P CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language” , IEEE Transactions on Dependable and Secure Computing, 12(6), 626-639, 2014
- [18] Hindriks, H. N., “Vulnerability analysis of cyber security modelling language models using probabilistic logic” , Master’s thesis, University of Twente, 2016.
- [18] Karahasanovic, A., Kleberger, P., Almgren, M., “Adapting Threat Modeling Methods for the Automotive Industry” , In Proceedings of the 15th ESCAR Conference (pp. 1-10), 2017.
- [19] 파이어아이코리아, “보안 운영 효율 극대화 방안 - SOAR에 길이 있습니다!” [Internet], Available: <https://m.post.naver.com/viewer/postView.nhn?volumeNo=15562880&memberNo=35755396>.

2014년 카드정보 유출대란 이후 개정된 개인정보보호법 39조의 징벌적 손해배상 적용에 관한 법적/법경제학적 효용성 검토

강동혁* · 최지완** · 채호정*** · 기광민****

* 연세대학교 상경대학 경제학전공

** 고려대학교 경영대학 경영학전공

*** 고려대학교 문과대학 노어노문학전공

**** 고려대학교 경영대학 경영학전공

요 약

2014년, KB국민카드를 비롯한 카드3사의 개인정보유출 사건이 발생한 이래, 국내 손해배상제도의 난점을 보완하고자 배상액 한도를 실손해액의 3배까지 책정할 수 있는 징벌적 손해배상 제도가 개인정보보호법, 하도급법 등을 비롯한 다양한 법률에 도입되어 왔다. 그러나 법안 입안 당시 제도의 정당성에 대한 분석이 다소 직관적인 방법에 의존하였고, 대륙법에 기초하면서 배심제에 기반을 두지 않는 우리나라 법과 상충되는 부분이 있다는 비판이 존재한다. 국민적 요구에 따라 도입된 징벌적 손해배상제도는 오늘날 16개 법률에 적용되고 있지만 지난 9년간 판례는 단 12건에 불과하며, 특히 개인정보보호법에서 징벌적 손해배상제도가 적용된 판결은 전무하다. 따라서 귀납과 직관 이외의 방법을 통한 당해 제도의 효용성 분석이 필요할 것으로 판단하였으며, 경제학적 모형을 통한 실효성 분석을 고려해보게 되었다. 본 논문은 서두에서 징벌적 손해배상제도의 역사와 법리상의 논점 등을 개괄하고, 이후 경제학적 모형을 기반으로 당해 제도가 개인정보 보호에 유의미한 효과가 있는지 분석하여, 결론에서는 제도의 보완점까지 제시하고자 한다.

키워드

징벌적 손해배상, 개인정보보호법, 3배 배상, 비대칭 정보

목 차

I. 금융보안과 징벌적 손해배상제도	(1)
II. 징벌적 손해배상제도의 배경	(3)
1. 징벌적 손해배상의 정의와 기능.....	(3)
2. 징벌적 손해배상의 역사.....	(4)
III. 징벌적 손해배상의 법리 검토	(8)
1. 민형사상의 구분.....	(8)
2. 손해배상액의 상한.....	(9)
3. 부당이득 취득 가능성 및 기업의 활동 위축.....	(11)
IV. 미시경제학적 모형을 통한 문제인식	(11)
1. 문헌 검토 및 직관.....	(11)
2. 기초적인 사회 후생 모형과 최적 유의수준.....	(14)
3. 개인정보 유출 사고와 관련한 모형의 주된 가정.....	(15)
4. 단일 피해 유형과 징벌적 손해배상.....	(16)
5. 소비자의 기대에 변동이 발생했을 시의 단일 피해 유형 모형.....	(19)
6. 다중 피해 유형을 고려한 모형으로의 확장.....	(20)
7. 부의 외부효과를 반영하는 사회적 최적과 사측의 선택.....	(24)
8. 과실 책임 및 비대칭 정보 하의 모형.....	(26)
V. 결과 및 후속과제 제안	(29)
1. 모형의 소결 및 제안사항.....	(29)
2. 모형을 활용한 이론 정립의 한계점 및 확장 가능성.....	(32)

I. 금융보안과 징벌적 손해배상제도

영미법에서 기원한 징벌적 손해배상제도는 민, 형사상 책임을 구별하는 국내 법체계와의 부조화, 모호한 배상액 판단 기준, 기업 활동 위축 가능성 존재 등 비판적인 견해들로 인해 우리나라의 실정에 맞게 독특한 형태로 도입되었다. 우리나라의 징벌적 손해배상제도는 손해배상의 상한액을 3배로 제한하고 있어 ‘3배 배상제도(Treble Damage)’라 불리기도 하며, 개별입법의 형태로 2019년 현재 총 16개의 법률에 적용되고 있다. 그 중에서도 ‘개인정보 보호법’은 금융보안과 직결되는 영역이라 볼 수 있는데, 오늘날 핀테크 산업이 활성화되면서 금융보안의 중요성에 대한 인식도 높아지고 있다. 특히, 핀테크의 발전은 소비자들이 자신의 개인정보 혹은 금융자산이 안전할 것이라는 신뢰에 기반을 두기 때문에 금융기업들은 소비자들의 개인정보보호에 최선을 다할 의무가 있으며, 금융보안에 중대한 과실이 발견될 경우 개인정보보호법 39조에 의거한 징벌적 손해배상의 책임자에 해당될 수 있다.

‘개인정보 자기결정권’은 개인정보 보호의 근간이 되는 법익이다. 정보주체에게 자신의 정보가 공개, 이용될 결정권을 부여함으로써, 그에 반한 상대방 혹은 제3자의 행위를 불법행위로 규정한다. 특히, 최근에는 전자상거래상에서 개인정보가 마케팅, 상거래의 중요 요소로 사용됨으로써 발생하는 경제적 가치에 주목하고, 그에 대한 재산권을 인정하는 견해도 존재한다. 한편, 개인정보는 물건이 아니기 때문에 소유의 대상이 될 수 없고, 그에 따라 개인과 그 개인에 관한 정보 사이에 물권적인 재산관계를 인정하기 어렵다는 반론도 제기된다. 그러나, 설령 개인정보에 대한 재산권이 받아들여지지 않더라도, 그에 관한 정보주체의 법적 이익이 어떠한 형태로든 존재하고 인정되는 이상, 개인정보가 권한 없는 제3자에게 ‘유출’된 경우는 정보주체의 법적 침해 문제, 즉 손해배상의 문제를 발생시킨다. 판례에 따르면, 개인정보의 ‘유출’은 개인정보가 정보주체의 통제에 반하여 제3자가 그 내용을 열람할 수 있는 상태에 이르는 것을 의미한다.

2014년 1월, KB국민카드, 농협은행, 롯데카드에서 합계 1억 400만 건(국민 5,300만 건, 농협 2,500만 건, 롯데 2,600만 건)의 개인정보유출 사건이 발생했다. 유출된 데이터에는 이름, 주민등록번호, 주소, 전화번호 등의 개인 식별정보를 비롯하여 계좌번호, 신용카드번호, 유효기간, 신용한도금액, 카드신용정보 등과 같은 금융정보까지 포함되어 있었다. 뒤이어, 100만여 명의 피해자들이 제기한 100여 건 이상의 소송,

사법부 역사상 가장 많은 수의 당사자가 참여한 손해배상청구소송이 제기되었다. 1심 재판 중 실체법적으로 가장 논란이 된 쟁점사안은 원고들의 정신적 손해 발생 여부였다. 위자료 배상을 청구하는 원고들에 맞서 카드 3사는 막연한 불안감을 법적 손해라 보기 어렵다며 항변했다. 2016년, 처음으로 선고된 1심 판결은 KB국민카드와 농협은행 각각에 원고 1인당 10만원을 배상할 것을 명했다. 이에 일부 원고는 손해액 액수가 과소하다며 항소하였고, 반면 카드 3사는 원고 전체에게 각각 10만 원씩 배상할 경우 카드사가 도산할 위험에 처하는데, 이것이 당해 사건의 중함에 비해 과도한 처분이라며 마찬가지로 항소하였다. 그러나 서울고등법원은 쌍방의 항소를 모두 기각했고, 사건은 결국 대법원으로 넘겨졌다. 한편, 롯데카드는 2010년, 2013년 두 차례의 정보유출이 발생하였으나, 1심 법원은 2010년의 경우에 대해서만 유출된 정보 중 일부가 범인의 손을 떠나 시중에 유통되었다는 이유로 원고들의 정신적 손해를 인정했고, 2013년 유출 사건에서는 사건 발생 직후 범인이 검거되어 정보가 시중에 유통되지 않았으므로 원고들의 정신적 손해 발생을 인정하지 않았다. 이후, 서울고등법원은 롯데카드 2010년 유출에 관한 위자료 금액을 7만원으로 감액하였고, 2013년 유출에 관한 1심 판결의 결론은 변경하지 않았다. 나머지 개별 사건들의 경우, 대표 사건의 결과를 원고와 피고가 따르는 내용의 화해 권고가 받아들여지고 있다. 초유의 사건 발생으로 위자료의 산정이 다른 사건에 의해 결정되는 등 법원은 법리 적용에 어려움을 겪고 있고, 그 과정에서 개인정보유출로 인한 손해배상 제도가 가진 난점들이 속속 드러나고 있는 것이다.

이에, 2015. 7. 24. 법률 제13423호로 개정된 개인정보 보호법 제39조 제3항과 2016. 3. 22. 법률 제14080호로 개정된 정보통신망법 제32 조 제2항에서 개인정보처리자의 고의 또는 중과실로 인한 개인정보 유출 등에 관하여 실제 손해액의 3배 이내에서 징벌적 손해배상을 명할 수 있다는 규정이 신설되었다. 위 개정 정보통신망법의 의안 원문은 그 제안 이유를 “현행법상 법정손해배상제로 개인정보 유출에 대한 손해배상책임을 물고 있으나 법정손해배상제만으로는 ‘재산적 피해’ 보전 어려움 및 피해 방지의 실효성 의문이 제기되는 상황임. 이에 징벌적 손해배상제를 도입해 정보통신서비스 제공자의 책임성을 강화하고자 함.” 이라고 밝히고 있고, 가결된 법률 역시 개정 이유를 “정보통신망을 통한 개인정보의 유출은 그 피해 정도가 지대하며, 유출된 개인정보로 인한 ‘2 차 피해’의 발생 가능성이 높아 이에 대한 시급한 대책 마련이 필요함” 이라 밝혔다.

그러나 2019년 현재, 국내에서 개인정보보호법의 신설된 규정에 기반하여 실제로 징벌적 손해배상이 적용된 사례는 전무하다. 징벌적 손해배상제도는 2011년에 하도급법 개정을 통해 우리나라에 처음으로 도입된 이후 현재 16개 법률에 적용되고 있지만, 실제 판례는 9년간 단 12건에 불과하였다. 그 마저도 하도급법에 집중되어 있었고 상술하였듯이 개인정보보호법에서는 판례가 전무하였기 때문에, 판례를 통해서 제도의 실효성을 귀납적으로 입증하기엔 불가능하다고 판단하였다. 특히, 3배로 규정된 손해배상액의 상한의 정당성과, 징벌적 손해배상 제도 그 자체에 기업의 불법행위를 저지할 수 있는 억제효과가 있는지 여부는 법안 입안 당시 매우 중요하게 고려되어야 할 사항임에도, 그 증명과정이 충분치 못하였다고 사료된다. 따라서, 본 논문은 기초적인 경제학적 모형을 바탕으로 징벌적 손해배상제도가 개인정보 보호에 유의미한 효과가 있는지 알아보고, 더 나아가 당해 제도의 보완점을 분석, 제시하고자 한다.

II. 징벌적 손해배상제도의 배경

1. 징벌적 손해배상의 정의와 기능

징벌적 손해배상이란 가해자가 악한 의도를 갖고 불법 행위를 한 경우 민사 재판에서 가해자를 징벌할 목적으로 부과하는 손해배상으로, 실 손해액을 초과한 액수를 부과하는 제도이다. 즉, 가해자의 비도덕적 행위에 대하여 민사적 손해배상을 넘어서 제재를 가하는 형벌적 성격을 동시에 지니고 있으며, 현재 이 제도는 영미법을 근간으로 한 나라에서 주로 활용되고 있다. 대한민국 법원도 징벌적 손해배상에 대한 정의를 시도한 적이 있는데, “가해자가 고의성을 가지고 위법행위를 하는 경우에 손해를 보상해줄 뿐 아니라, 가해자의 위법행위를 징벌하고 제지하기 위해서 가해지는 손해배상으로서 보통법(common law)상으로 인정되고 있는 구제방법의 일종인 바, 이는 손해배상을 주목적으로 두고 있는 민사법 체계에서 인정되지 아니하는 형벌적 성질을 갖는 배상형태” 라고 정의하였다¹⁾. 위 정의에서 알 수 있듯이 징벌적 손해배상은 ‘처벌’의 기능을 수행함으로써 피해자의 상태 회복을 목표로 하는 보상적 손해배상과 다르며, 비재산적 손해에 대한 보상적 손해배상의 의미를 가지는 위자료와도 구별된다. 또한 징벌적 손해배상은 법원이 부과하고 피해자에게 귀속된다는 점에서 국가가 환수하는 과징금, 과태료 및 벌금과도 구별된다.

1) 서울지법 동부지원 선고 93가 합19069 판결, 1995

징벌적 손해배상제도는 교육, 처벌, 제지, 보상, 법 집행 등의 기능을 수행한다²⁾. 징벌적 손해배상은 불법 행위를 저지른 사람을 처벌하는 법 집행의 기능을 수행하며, 피해자의 권리와 이익을 증명하고 가해자를 처벌함으로써 간접적으로 교육의 기능을 수행한다. 또한 전보적 손해배상 범위를 초과한 범위를 피해자에게 보상하고, 피해자가 승소할 경우 소송비용 공제를 통해 발생하는 비용을 지불하여 보상의 기능을 수행한다. 마지막으로 징벌적 손해배상은 앞서 언급한 기능, 특히 ‘제지’ 기능을 통해서 잠재적인 불법행위자들에게 증가될 배상액과 제재를 인식하게 함으로써 불법적 행위를 사전에 차단하는 기능을 수행한다.

2. 징벌적 손해배상의 역사

(1) 고대법

고대법에서는 민사상의 책임과 형사상의 책임이 따로 분리되어 있지 않았고, 피고의 불법 행위를 처벌하기 위해 원고가 입은 손해액 보다 훨씬 큰 금액을 피고에게 부과하는 배수적 손해배상(Multiple Damages)제도가 인정되었다. 배수적 손해배상제도가 피고를 처벌하고 배상하는 등의 형사책임을 지우기 때문에 오늘날의 징벌적 손해배상 제도와 기원이 다르다는 의견도 존재한다.³⁾ 하지만 현재의 징벌적 손해배상제도 역시 형식은 민사책임이지만 그 실질은 형사책임이라는 점에서 배수적 손해배상제도가 징벌적 손해배상제도의 기원이라고 볼 수 있다.

기원전 2250년경의 함무라비 법전은 배수적 손해배상제도를 채택한 법전으로, 이는 현대의 징벌적 손해배상적 성격을 가지고 있다. 법전 제8조에서는 ‘사람이 소, 양, 나귀, 돼지, 선박을 훔쳤는데 그것이 신전이나 궁전의 것이면 30배를, 평민의 것이면 10배를 물어야 하며, 도둑이 그렇게 할 능력이 없으면 그를 죽인다.’ 고 규정했고, 제112조에서는 ‘사람이 여행을 위해 금, 은, 보석을 타인에게 맡기고 되돌려 받고자 할 때 만약 재산을 넘겨주지 않을 경우, 원소유자는 소유사실을 증명하고 재산을 맡은 이는 원주인에게 해당 재산의 5배를 배상해야 한다 ⁴⁾’ 고 규정하였으며, 이는 징벌적 손해배상의 기원으로 여겨진다. 이후 기원전 1400년경의 히타이트 법(Hittite Laws)에서는 ‘황소나 말 한 마리를 훔쳤을 때, 15마리의 황소나 말로 갚아야 한다’ 는 규정이 있었고, 기원전 200년경에 만들어진 힌두의 마누법전(Code of

2) David G. Owen ,A PUNITIVE DAMAGES OVERVIEW, 1994

3) Alan Calnan, “Ending the Punitive Damage Debate” , 1995, p.105

4) Robert Francis Harper, “The Code of Hammurabi King of Babylon” , 1904

Manu) 에서도 절도 등의 부정행위에 대해서는 배수적 손해배상 제도가 인정되었다. 기원전 450년 초기 로마법에서도 배수적 손해배상제도를 인정하였다. 로마법 제 8 표 15항은 ‘도품장낙도와 도품전치도에 대한 벌금은 도품가액의 3배액이다.’ 라고 규정하였고, 16항에서는 ‘현행범이 아닌 절도를 이유로 소구하는 경우에는 (피고는) 2배액으로 손해를 배상한다.’ 라 규정하였다. 허용하지 않은 한도 이상의 고리대금업을 실시한 경우 8조 18항에서는 ‘고리대주는 4배액의 패소판결을 받는다⁵⁾’ 고 규정하였다.

우리나라에서는 고조선의 8조법을 시작으로 배수적 손해배상 제도가 인정되었다. 8조법 3항에 의하면 ‘남의 물건을 훔친 사람은 노비로 삼는데, 노비가 되지 않으려면 1인당 50만을 배상해야 한다.’ 라고 규정되어 있다. 고조선의 근본정신을 이어받은 것으로 보이는 부여의 법 제도 하에서도 배수적 손해배상 제도를 찾아볼 수 있다. 부여의 4조목의 법에 대한 기록 중 ‘도둑질을 했을 때 12배를 갚아야 한다.’ 라는 규정이 존재하며, 고구려에서도 ‘도둑질한 자는 열 배로 갚아야 한다.’ 라는 기록을 찾아볼 수 있다.

(2) 근대 영국법

고대의 배수적 손해배상제도는 근대 영국의 배수적 손해배상제도로 이어졌다. 1275년 4월 최초로 영국 의회에서 배수적 손해배상제도를 인정하는 법률이 제정되었는데, 이 법률에 의하면 ‘(1) 수도자에 대하여 불법으로 권리를 침해하는 경우 (2) 보안관 혹은 지역, 왕실 공무원의 사무실 남용하는 경우 (3) 일방적인 검토로 인해 동물에게 피해를 입히는 경우 (4) 남작 혹은 토지 관리인이 관할 구역을 넘어서 강탈하는 경우⁶⁾ 피고가 원고에게 2배의 손해배상을 지급해야 한다.’ 1275년 법률이 제정된 이후에도 영국에서는 배수적 손해배상을 정하는 법률이 지속적으로 새로이 제정되었다.

이후 1763년에 영국의 보통법에서 처음으로 징벌적 손해배상 제도를 인정하는 판례가 나왔다. 1763년 허클 대 머니(Huckle v. Money) 판결에서는 공무원의 억압적인 권력남용 행위를 인정해 300파운드의 손해배상금을 지불하라고 판결하였다⁷⁾. 또 다른 사건인 윌크스 대 우드(Wilkes v. Wood) 사건은 출판업자가 적법한 영장 없이

5) 최병조, “12표법(대역)” 「서울대학교 법학」, Vol.32, p.157-176, 1991

6) Statute of Westminster I, in 1 STATUTES OF THE REALM 26, 1275

7) Huckle v. Money, 95 Eng. Rep. 768, 769; 3 Wils. K.B. 205, 1763

압수수색을 당한 사례로 1,000파운드의 손해배상금을 지불하라고 판결했다.⁸⁾ 이후 1964년 룩스 대 버나드(Rookes v. Barnard and Others) 사건 판결을 통해서 현대적 의미의 징벌적 손해배상제도가 확립되었다. 당시 데블린 판사(Lord Devlin)는 공무원에 의한 억압적 권력 남용 행위가 있거나, 피고가 자신의 불법행위로부터 얻은 이익이 원고에게 손해배상을 지급하고도 이득이 남을 것으로 예상한 경우, 법률에 명문된 규정이 있는 경우에만 징벌적 손해배상 인정이 가능하다고 판결했다⁹⁾. 이러한 원칙은 1972년의 카셀 대 브룸 (Cassel Co., Ltd. v. Broome) 사건판결, 1997년의 엘튼 존 대 엠지엔 (Elton John v. MGN) 판결 등 추후의 사건에도 반영되고 있다.

(3) 미국

징벌적 손해배상제도는 영국에서 도입된 이후 발전하여 현재는 미국에서 가장 활발하게 활용되고 있다. 미국에서 최초로 징벌적 손해배상제도가 인정된 사건은 1784년의 Genay v. Norris 판결¹⁰⁾이다. 의사가 환자의 술에 장난으로 칸타리스(발포제)를 타고 환자는 이를 모르고 마셨다가 병이 발생하여 징벌적 손해배상이 인정된 사례이다. 1791년에는 뉴저지주 법원의 Coryell v. Colbaugh 약혼해제사건 판결에서 ‘장래 이와 유사한 행위의 재발방지와 다른 사람에게 본보기가 될 수 있도록 징벌적 손해배상이 필요하다’고 인식¹¹⁾하였고, 이 판결 이후로 미국의 각 주에서 징벌적 손해배상제도를 도입하기 시작하였다. 1852년에는 제조물 책임에 대한 징벌적 손해배상제도가 인정되었으며, 1953년까지 여러 유형의 징벌적 손해배상제도에 관한 법률이 제정되었다. 연방법이나 주법에서 명확하게 징벌적 손해배상의 정의나 배상액을 규정하고 있지는 않지만, 그 동안의 판례를 살펴보면 각 주마다 세부 내용에는 차이가 존재한다. 루이지애나, 미시간, 네브래스카, 뉴햄프셔, 사우스다코다 이상 다섯 개 주는 징벌적 손해배상 제도 자체를 인정하지 않는다. 앨라배마와 알래스카 등 29개 주는 주법을 통해 징벌적 손해 배상을 인정하지만 배상액에 있어서는 상한을 두고 있으며, 뉴욕, 캘리포니아 등 16개 주는 상한이 없는 징벌적 손해배상제도를 인정하고 있다.¹²⁾

주요사례로는 1987년 펜즈오일 대 텍사코(Pennzoil Co v. Texaco Inc.) 사건에서

8) Wilkes v. Wood, 98 Eng. Rep. 489, 498, 1763

9) Rookes v. Barnard, AC 1129 (HL), 1963

10) Genay v. Norris, 1 S.C.L. 6 (1 Bay), 1784

11) Coryell v. Colbough, 1 N.J. 77, 1791

12) Wilson Elser, Punitive Damages Review, 50-State Survey, 2014

Pennzoil이 게티 사(Getty)를 인수하기로 협약을 체결한 상태에서 텍사코(Texaco)가 뒤늦게 게티 사를 인수하자 펜즈오일 사(Pennzoil)가 텍사코에 소를 제기하여 100조 달러 상당의 손해 배상을 받아낸 사건¹³⁾, 2008년 엑슨 대 베이커(Exxon Shipping Co. v. Baker) 사건에서 엑슨 발데즈(Exxon Valdez) 호의 기름 유출에 대하여 연방 대법원이 징벌적 손해배상의 비율을 실 손해와 1:1로 제한하여 500만 달러의 징벌적 손해배상 지급을 명령¹⁴⁾한 사건, 2014년 앵겔 대 레이놀즈 담배사(Engel v. R.J. Reynolds Tobacco) 사건에서 담배회사에 대한 집단소송에서 원고들에게 236억 달러의 징벌적 손해배상을 인정¹⁵⁾한 사건 등이 있다.

(4) 한국

우리나라에서도 징벌적 손해배상의 도입에 대한 논의가 활발하게 이루어졌고, 2011년 3월 11일 ‘하도급거래 공정화에 관한 법률’ 개정에 의해 국내에 처음으로 도입되었다. 해당 개정 법률은 원청 업체인 대기업이 하도급 업체의 유망한 기술을 가로채 유용하여 손해가 발생했을 시에 최대 3배까지 손해액을 부과하는 것을 그 내용으로 한다. ‘하도급법’에서 징벌적 손해배상제도가 처음으로 도입된 이후 다른 법률에서도 징벌적 손해배상제도의 도입이 꾸준히 이루어졌다. ‘기간제 및 단시간근로자 보호 등에 관한 법률’, ‘신용정보의 이용 및 보호에 관한 법률’, ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률 개정’, 그리고 ‘대리점 거래의 공정화에 관한 법률’의 제정 등을 통해 징벌적 손해배상제도가 우리의 현행법 체제 하에 자리 잡게 되었으며, 현재 징벌적 손해배상제도를 규정하고 있는 법률은 총 16개에 이른다.

영미법 체제 하에서 징벌적 손해배상 제도와의 차이점은 불법행위 전반에 대해 일괄적으로 징벌적 손해배상 제도를 도입하고 있는 영미법과 달리 우리나라에서의 징벌적 손해배상 제도는 개별입법으로 이루어져 있다는 점이다. 상술하였듯이 배상액에 한도를 두지 않는 영미법의 징벌적 손해배상제도와 달리 배상액을 최대 3배의 한도 내에서 규정하고 있다는 것 역시 우리나라 징벌적 손해배상제도의 특징이다. 이는 통상 우리가 징벌적 손해배상제도의 도입을 통해 얻고자 하는 범죄 억제 효과에 영향을 주지 못하는 결정적 이유 중 하나로 간주되기도 한다. 미국의 경우 소송

13) Pennzoil v. Texaco, Inc., 481 U.S. 1, 1987

14) Exxon Shipping Co. v. Baker, 554 U.S. 471, 2008

15) Engle v. RJ Reynolds Tobacco Co., 122 F. Supp. 2d 1355 (S.D. Fla. 2000)

으로 넘어가 패배할 시에는 징벌적 손해배상으로 인해 더 큰 금액을 배상해야 할 것을 염려해 피해자와 사전 합의를 보려고 시도하는 경우가 많다. 반면에 우리나라의 경우, 기업이 소송에서 패배하더라도 한정된 금액만 물어주어도 되기 때문에 피해자와의 사전 합의에 적극적으로 나서지 않으며, 따라서 징벌적 손해배상의 주목적인 범죄 재발 방지 역할의 제대로 수행하지 못한다는 한계를 지닌다.

Ⅲ. 징벌적 손해배상의 법리 검토

우리나라는 민사와 형사를 엄격히 분리하는 대륙법 체계를 바탕으로 한 시민법적 지도이념에 따라 징벌적 손해배상제도의 도입에 난관이 있었으나, 개별법을 중심으로 특정한 법 위반행위 (불법행위)에 대하여 실 손해의 3배를 부과하는 형태의 징벌적 손해배상제도가 도입되기 시작하였다. 징벌적 손해배상제도의 도입에 있어 가장 논란이 되는 부분은 크게 당해 제도와 우리 형사법 체계가 조화를 이룰 수 있는지 여부, 실 손해의 3배로 규정된 손해배상액의 상한이 적정한지 여부, 집단피해 불법행위의 영역에 있어서 중복적 배상, 부당 이득이 발생할 수 있다는 문제이다. 그 외에도 징벌적 손해배상제도를 도입하게 되면 현실적으로 기업의 활동이 위축될 수도 있다는 우려 등도 충분히 제기될 수 있는 문제이다. 이하에서는, 앞서 소개한 논의점의 핵심 내용을 간략히 소개한다.

1. 민형사상의 구분

징벌적 손해배상은 민사적 구제수단이지만, 징벌의 성격을 지닌다는 점에서 준형사법(Quasi-criminal)이라 칭한다. 그러나 민사와 형사를 분명히 구별하는 대륙법 계열의 우리 형사법 체계에서 이러한 Quasi- 제재를 인정하는 것은 무리가 따른다. 입증 책임의 부담, 형벌권 발동의 주체, 집행 강제 등 민사와 형사는 절차의 차이가 존재하기 때문이다. 이에, 징벌적 형사제도가 우리 형사법 체계에 편입될 수 있는지 여부가 당해 제도의 도입 당시 논란이 되었다.

우리 형사법 체계에 징벌적 손해배상제도가 부합한다는 입장은 먼저 손해배상과 형사제재 모두 가해자의 행위교정이라는 특별 예방적 효과와 가해자 이외의 일반인의 행위억제라는 일반 예방적 효과의 목적을 지니고 있음을 지적한다. 그 근거로 민법상 불법행위책임에 대한 위자료가 제재와 예방의 성격을 인정한 우리 대법원 판례를 들고 있다. 위자료의 성격이 순수 손해배상인지 사적 제재인지에 대한 논란

이 있으나, 순수한 손해배상으로 이해된다는 것이 판례의 관점이다.

또한 이 입장에서는 앞서 손해배상과 마찬가지로 영미법의 피해회복명령 또는 원상회복명령 역시 형벌의 일종으로 인정되고 있고, 독일법 체제에서도 원상회복명령이 형벌과 결합되어 부과될 수 있다는 점에 집중하였다. 즉, 비교법적으로도 형법영역 속에 민사적 손해배상의 일정 요소가 편입되고 있다는 점을 근거로 하였으며, 이는 곧 국가가 금전귀속의 주체가 아닐지라도 제재의 의미를 지닐 수 있다는 것이다. 즉 징벌적 손해배상은 제재를 주된 기능으로 하는 형사법적 기능과 전보를 부수적 기능으로 하는 민사법적 기능을 동시에 가지고 있으며, 그 본질은 불법행위에 대한 처벌과 억제를 바탕으로 한 제재적 목적과 법을 준수하도록 함으로써 질서를 유지하는 형사법적 기초에 근거하고 있다.

그러나 민사상의 손해배상과 형사상의 제재를 구별하는 핵심은 금전의 귀속주체뿐 아니라, 형벌권 발동의 주체와 입증책임의 소재, 소송구조의 뿌리 등이 종합적으로 검토되어야 한다는 것이다. 이러한 지적에 대해 형사체계로의 편입을 긍정하는 입장은 대륙법계에서도 형벌권의 발동에 사인소추를 인정하고 있는 점, 배상명령제 도처럼 민사적 손해배상이 이미 형사절차에 도입되어 있다는 점, 징벌적 손해배상이 예방효과와 제재의 성질을 가진다는 점을 근거로 제시하고 있다. 그러나, 소추주체가 아닌 판단주체가 누구인지가 중요하다는 점, 배상명령의 본질은 민사절차가 담당하고 있는 점, 통상의 손해배상 역시 예방효과를 가진다는 점 등의 의견이 반론으로 제시됨으로써 논의는 아직 계속되는 중이다. 민·형사책임을 준별하는 현행 법체계 내에서 개별 법령 개정을 통한 징벌적 손해배상 제도의 도입은 법 원칙에 대한 중대한 예외를 인정하는 것이므로 그러한 예외를 정당화할 수 있는 특별한 사정이 인정되는지 신중하게 판단할 필요가 있을 것이다.

2. 손해배상액의 상한

전통적인 전보배상 즉, 실 손해 배상의 원칙을 관철한다면 피해자의 손해를 전보하는 데 한계가 있으며, 사실상 피해자의 구제를 부인하는 결과를 가져온다. 또한 대량의 피해자를 양산하거나 실 손해를 측정하기 어려운 비재산적 손해를 야기하는 경우에는 불법행위를 사전에 예방하고 억제하는 것이 매우 중요하다. 피해자의 권리구제와 위반행위의 예방, 억제를 위하여 전보배상의 예외를 인정할 필요가 있다. 이에, 징벌적 손해배상제도는 실제 손해 이상의 배상액을 피해자에게 취득하게 함

으로써 피해자로부터 불법행위를 적발, 고발하도록 촉진한다. 한편, 가해자에게는 법규위반 행위를 억제시킨다는 점에서 법을 실행, 준수하도록 하는 기능을 갖는다. 문제되는 점은 헌법상의 과잉금지의 원칙, 비례의 원칙, 공서양속 등 여러 기준에 비추어 볼 때 어느 정도의 배상액이 합리적이라 할 수 있는가이다. 미국의 경우에는 배상액이 지나치게 고액화 되는 것을 방지하기 위해 많은 주에서 각 제정법으로 배상액의 상한을 일률적으로 제한하거나 전보배상액의 일정 배수 이하로 제한하고 있고, 독점규제법, 소비자보호법, 차별금지법, 저작권법에서는 3배 배상을 그 상한으로 정하고 있다. 중국 역시, 식품안전법에서 10배 배상을 규정한 것 외에는 통상 3배 배상원칙을 취하고 있다. 프랑스 입법시안은 불법행위법에 일반조항의 형식으로 실 손해액의 2배를 상한으로 규정하고 있다.

같은 맥락에서 우리나라 개별 법률들은 예외 없이 실 손해액의 3배를 징벌배상액의 상한으로 정하였다. 이는 배상액의 지나친 고액화를 차단하기 위해 법관이나 배심의 재량 여지를 축소하기 위한 의도를 품고 있다. 한편, 우리나라의 하급심에서는 헌법상 비례의 원칙에 따라 우리나라에서 인정되는 상당한 금액을 “현저히 초과하는 부분”에 한하여 선량한 풍속 기타 사회질서에 반한다는 취지로 판결한 바 있다. 16) 피해자의 실질적인 구제와 침해행위의 예방과 억제를 위해 3배 배상제도가 적합하고도 필요한 수단임을 인정하더라도, 비례의 원칙상 이를 통하여 얻고자 하는 이익과 침해자가 입게 되는 불이익과의 균형이 유지되어야 함은 헌법상의 당연한 요청이기 때문이다.

또한, 실 손해의 3배를 배상액의 상한으로 정한 현행 법률들의 산정근거와 적정성에 의문을 제기하는 견해 역시 적지 않다. 우선, 징벌배상의 당초 목적인 불법행위의 억지와 제재를 달성하는데 3배의 배상액으로는 한계가 있기 때문에, 그 상한을 확대하거나 폐지해야 한다는 주장이 있다. 특히, 배수 상한의 근거가 무엇인지 불분명하다 의견은 현행 3배 배상제도가 그 입법과정에서 직관적 결정에 의해 이루어진 측면이 있고, 법관에게 각종 고려요소들을 참작하여 감액할 수 있는 재량까지 부여되었기 때문에 적절한 법 집행력을 담보하기 어렵다고 한다.

그러나, 배수의 과도한 확대나 배수 상한의 폐지는 손해배상제도의 안정성을 위협할 수 있고, 배액배상을 지향하는 국제적 입법 동향에도 부합하지 않는다는 입장

16) 부산지방법원 2009.01.22. 선고 2008가합309 판결; 서울지법 동부지원 1995.2.10 선고 93가합19069 판결

역시 그에 팽팽히 맞서고 있다. 입법 정책적으로 불가피하게 예외를 인정해야 할 경우에도 매우 신중한 접근이 필요하다고 생각된다. 이에, 본 논문은 경제학적 관점에서 현재의 징벌적 손해배상 제도의 3배 배상이 당해 법률의 목적을 유효하게 달성할 수 있는지 여부를 분석하고자 한다.

3. 부당이득 취득 가능성 및 기업의 활동 위축

징벌적 손해배상 제도는 실 손해 이상의 배상액을 피해자에게 귀속시킴으로써, 우연한 횡재(우발적 과잉소득; windfall)를 발생시킨다. 달리 말해, 징벌적 손해배상은 피해자가 입은 실·손해를 온전히 보전하는 것을 넘어 과잉구제 또는 부당이득을 부여함으로써, 남소로 인한 사회적 비용을 증가시킬 수 있다. 또한, 행위자에 대한 과잉 억제를 불러와 결과적으로 기업의 활동을 위축시킬 우려가 존재한다.

이에 반해, 단순히 전보적 손해배상액만이 가해자에게 요구될 경우, 손익분석의 결과 오히려 불법행위를 행하는 편이 더 큰 이익이 될 수 있다. 이에, 기업이 더 큰 이익을 위하여 불법행위를 감행하는 경우가 발생할 가능성이 적지 않으므로 징벌적 손해배상을 인정하여야 한다는 의견이 있다. 또한, 소송비용과 시간 등이 전보적 손해배상을 통해 얻을 수 있는 이익보다 클 경우, 불법행위의 예방이 충분치 않을 수 있기 때문에 징벌적 손해배상의 도입에 찬성하는 의견도 볼 수 있다. 한편, 과도한 손해배상으로 인한 기업의 위축 혹은 파산 등을 우려하는 의견이 있으나, 고의적 가해자인 기업의 경우 오히려 파산을 시키거나, 억제 효과를 통해 건전한 기업으로 거듭나도록 하는 것이 시장경제와 사회정의에 도움이 된다는 주장도 있다. 또한, 원고에게 지급되는 실 손해 이상의 손해배상액이 부당하게 보일 수 있지만, 피해자가 소송을 끝까지 포기하지 않고 진행하여, 결과적으로 가해행위를 억제할 수 있는 효과가 있다 점을 고려해볼 때, 당해 제도의 도입은 충분한 이유가 있다는 견해 역시 존재한다.

IV. 미시경제학적 모형을 활용한 문제인식¹⁷⁾

1. 문헌 검토 및 직관

위와 같은 정의와 역사를 가진 징벌적 손해배상제도에 비추어 볼 때, 징벌적 손해

17) 아래에서 언급되는 내용 중 이론적 토대는 대부분 게임이론: 전략과 정보의 경제학(김영세 저, 8판, 2012) 및 Game Theory and the Law(Baird, Picker, Gertner, 1998)을 참고하였음.

배상제도는 실제 손해액의 적게는 3배, 많게는 수백 배에 달하는 배상액을 잠재적 피해자에게 배상하도록 하는 성격을 띠는 점에 주목해야 한다. 앞서 언급한 사례들을 보면, 높은 수준의 배상액을 책정을 하는 것에는 결국 고의적으로 피해를 유발할 위험의 예방과 배상의 두 차원을 모두 달성하고자 하는 정책적 목표가 있음이 명확하다. 2014년 카드 정보 유출 대란이 있는 이후 개정된 개인정보보호법에 도입된 최대 3배까지의 배상액 범위의 명문화는 과도한 손해배상액 책정을 방지함과 동시에 앞서 언급한 정책적 목표를 실현하기 위함일 것이다. 이 때, 개인정보 보호법상에서 문제가 되는 개인정보 유출 등에 대한 사측의 책임은 직접적으로 정보 보호에 관한 주의를 기울여야 됨에도 그만큼 주의를 기울이지 않는다는 차원에서 발생하며, 중국에는 사회적으로 바람직한 수준 이상의 주의를 기울이도록 강제하는 차원에서 징벌적 손해배상 제도를 도입한 것이다.

일반적으로 이러한 징벌적 손해배상제도의 도입에 관한 고찰은 폴린스키(A.M. Polinsky)와 샤벨(Steven Shavell)의 1988년 연구(이하 “PS 1998”)에서 이루어진 바를 중요하게 다룬다. 해당 연구에 따르면, 징벌적 손해배상제도가 유의미하게 작용하는 사안은 가해자(기업)가 피해자에게 손해를 발생시킬 만한 행위를 하고도 손해에 대한 배상책임을 피해갈 확률이 존재하는 경우라고 한다. 이 때, 그러한 특수 사례에 한하여 책임 회피가 발생할 확률을 고려한 축소된 기대 배상액을 실제 발생할 손해액의 수준만큼 배가한다면 그것이야말로 가장 적절한 징벌적 손해배상제도의 활용이라고 한다.

위와 같은 연구와는 별개로, 다양한 측면에서 징벌적 손해배상제도의 법경제학적 효용에 관한 연구가 이루어진 바 있다. 대표적으로 차크라바티(Chakravarty, 2017)에 따르면 폴린스키(1997)에서 언급한 법적으로 정해진 최적의 유의성 비용(Stipulated Optimal Care)이 쌍방의 주의를 필요한 사안에 대해 피해 당사자들끼리 상대방이 취한 전략적 선택(유의 비용에 대한 지출 등)을 모른다는 가정 하에서는 과실 책임(Negligence Rule)과 징벌적 배상을 혼합한 제도를 마련하는 것으로 교정이 가능하다고 한 바 있다. 란데오 등(C. Landeo et.al, 2007)은 징벌적 배상 가능성에 따른 기대 배상액이 너무 높다는 비판에 따라 나타난 여러 보완책들을 경제학적으로 논의하였다. 이는 PS 1998 연구를 고려하여, 법원의 오판율이 낮은 경우, 미국에서 논의되고 있는 비경제적 손해에 관한 배상 제한 (Damage Cap)이 피고에게 책임이 충분히 있는 사건에 대한 실제 재판의 실행 횟수를 감소시킬 수 있음에 주목하였다. 과

도하게 높은 배상액을 주장할 수 있는 원고들 때문에 발생하는 인적/금전적 재판 비용의 폭증을 고려한 정책일 수 있지만, 반대로 징벌적 배상 제도의 예방적 성격을 약화시킬 수 있다고 저자들은 주장한다. 동시에 다른 측면에서 제안된 징벌적 배상액의 일부 국가 환원을 골자로 한 분할 배상(Split Award)의 경우 피고가 심각하게 부주의한 원고를 직면할 가능성을 늘리면서, 소를 제기한 건수에 따라 얻는 기대 수익이 증가하고 따라서 소의 제기 건수가 역으로 증가할 가능성이 있다고 한다. 리(Robert Rhee, 2012)의 연구는 또한 배상액의 변동 가능한 범위가 클 때 발생하는 위험(리스크)의 이해를 바탕으로 재정학적 연구방법론을 활용하여 실제 판결을 통해 결정되는 최적 배상액과 재판까지 가지 않고 합의를 통해 이루어진 배상액이 차이가 상당히 있을 수 있다는 점에 주목하였다. 이를 그는 차익거래(Arbitrage)의 측면에서 이해하려고 시도하였는데, 대표적으로 빈도는 낮지만 피해 규모가 큰 사건들의 경우에는 기업이 징벌적 손해배상이 가능한 재판에 직면하였을 때 기업의 합의금 제시액이 최적 수준보다 높게 책정될 가능성이 있다는 점이 중요하다. 반면 일반적으로 기대 범위 안쪽의 징벌적 손해배상이 이루어질 것으로 여겨지는 경우에는 피해자가 판결을 통한 최적 배상액보다 더 적게 합의를 볼 가능성이 있다는 점도 주목할 가치가 있다. 정책 목표를 실제 판결까지 가는 건수를 줄이되 합의금의 규모가 징벌적인 제도 하에서의 최적 수준과 가능하면 일치하도록 하는 것으로 두고 법률을 고안할 필요가 있음을 제시한다. 이러한 연구들은 결국 근본적으로 샤벨(1980), 루이 카플로(Louis Kaplow)와 샤벨(2002) 등이 논의한 다양한 사건 특성에 관한 엄격 책임과 과실 책임의 적절한 선택에서 파생되어 나타난 징벌적 손해배상의 특성에 대해 더욱 깊게 고찰해 볼 필요를 다양한 모형을 통해 제시한다.

따라서 본 연구에서는 위에 언급된 연구들이 제시한 징벌적 손해배상의 주된 방향성을 이해하고, 이를 2014년 카드 정보 유출 대란 이후 개인정보보호법이라는 특수한 사례에 관한 현실적인 차원의 가정들을 포함하여 단순하지만 명료하게 해당 법안에 대한 징벌적 손해배상 적용의 잠재적 한계점을 고찰하고자 한다. 이는 앞서 언급한 PS 1998의 주장처럼, 단순히 100% 미만의 배상 확률의 역수만큼을 배가한 징벌적 배상은 시장에서 기업과 소비자의 기대가 일치하지 않을 때 최적의 유의수준을 보장하지 못할 수 있다는 점에 방점을 두고 있다.

이외에도 현재 한국의 금융시장에서 이루어지는 개인정보 관리 환경과, 개인정보를 수집 후 상당 기간 보유하는 금융산업의 특성상 대규모 유출사건 발생 시의 파

급효과를 부의 외부효과(Negative Externality)로 이해하는 차원까지 논의를 확장하는 것 또한 하나의 목표이다. 이는 실질적으로 본인의 개인정보를 수집한 금융사 등이 보안사고를 일으키지 않았음에도 다른 기업 등에서 발생한 유사한 사고가 시장에서의 불안을 야기할 수 있다는 점에서도 중요할 수 있다. 이를 고려할 때, 실제로 모든 금융사가 최적의 유의수준은 시장 내의 효과 이외의 부수적 경제적 손실 효과를 감안해서 결정되어야 한다는 측면에서 주장되는 징벌적 손해배상제도의 적용에 관해서도 고찰해볼 수 있을 것이다.

2. 기초적인 사회 후생 모형과 최적 유의수준

앞으로 언급될 사회 후생의 기초적 모형은 징벌적 손해배상제도의 개인정보보호 법에의 적용을 논의할 때에 반복적으로 사용될 토대모형으로 상정한다. 그러나 일반적인 경우와는 달리 개인정보 유출이라는 사안에 관해서는 피해의 종류를 1차 피해(h_1)와 2차 피해(h_2)로 별도로 둘 수 있다. 여기에서 1차 피해란 유출이라는 사건 자체에 따른 가치적, 정신적 손실을 뜻하지만 2차 피해는 유출된 정보가 암시장에서의 거래 등을 통해 불법적 목적으로 사용되거나, 금전적 손실을 유발한 것을 의미한다. 이들 각각에 대해서 기업이 대응할 수 있는 행동이 상이한 만큼, 본 연구에서는 각 피해 유형에 대해 기업이 투자할 수 있는 유의 비용을 개별적으로 부여한다. 예를 들어, 1차 피해의 경우 기업은 충분한 수준의 시스템 방화벽을 구축하고, 보안암호 변경 및 보안 시스템에 대한 지속적 투자가 곧 유의 비용이지만, 2차 피해의 경우는 범죄 이용가능성에 관한 기업과 관의 정보공유나 혹시 모를 유출 파일에 대한 재암호화와 같은 별도의 차원으로 이해할 수 있다. 물론, 모형을 더 복잡하게 한다면 2차 피해의 발생 가능성은 시차와 조건부 확률을 고려한 모형을 이용하여야 하지만, 좀 더 직관적인 문제의 이해를 위해 두 피해 유형을 독립적 피해로 상정한다. 맥락을 포함하여 가법적 사회 후생모형을 고려하면, 다음을 알 수 있다.

$$\begin{aligned}
 (1) \quad W(\text{사회 후생}) &= U_{\text{소비자}} + U_{\text{기업}} \\
 &= u(q) - pq - q(p(x)(h_1 - T) + f(y)(h_2 - T)) + pq - q(c + x + y + p(x)T + f(y)T) \\
 &= u(q) - q(c + x + y + p(x)h_1 + f(y)h_2)
 \end{aligned}$$

이는 단위 서비스 사용량당 피해 발생을 감안한 모형으로, (1)의 수식에서 사용된 기호와 주요 가정은 다음과 같다.

부 호	의 미	부 호	의 미
q	서비스 단위 수량	u(q)	소비자 효용 함수
p	단위 서비스 가격	c	서비스 제공 단위비용
p(x)	1차 피해 확률	x	1차 피해 유의 비용
h _i	피해액 (i = 1, 2)	T	소비자에게의 배상액
f(y)	2차 피해 확률	y	2차 피해 유의 비용

주요 가정

1. 각 피해 유형에 대한 한계확률은 0보다 작고, 2차 도함수는 0보다 크다.
2. 소비자의 효용 함수에는 한계효용 감소가 적용된다.
3. 유의 비용을 0만큼 투자하면 피해는 100% 확률로 발생한다.

<표 1> 모형의 주된 표기 및 가정

위의 가정과 모형을 바탕으로, 최적의 유의 수준 및 서비스 수요량에 대한 1차 조건(First Order Condition)을 고려하여 계산한다면, 다음의 결과가 도출된다.

$$(2) \quad \text{Max}_{(x,y,q)} W$$

$$\frac{\partial W}{\partial x} = 0 \leftrightarrow -1 = p'(x)h_1 \quad \text{s.t.} \quad x = x^* (\text{최적 1차 유의 비용})$$

$$\frac{\partial W}{\partial y} = 0 \leftrightarrow -1 = f'(y)h_2 \quad \text{s.t.} \quad y = y^* (\text{최적 2차 유의 비용})$$

$$\frac{\partial W}{\partial q} = 0 \leftrightarrow u'(q) = c + x^* + y^* + p(x^*)h_1 + f(y^*)h_2 \quad \text{s.t.} \quad q = q^* (\text{최적 수요량})$$

위의 1차 조건을 만족하는 값들(x^* , y^* , q^*)이 시장에서 선택된다면 사회 후생이 극대화된다. 이는 경제주체들의 효용을 가산하여 가장 크도록 하는 직관을 바탕으로 할 때 위와 같다고 할 수 있다. 그러나 현실적으로 피해의 유형에 대해 기업의 책임을 인정하는 법원의 행태가 상이한 점을 바탕으로 본 연구에서는 징벌적 손해배상을 개인정보 보호법에 적용할 때의 잠재적 한계점을 알아본다. 들어가기에 앞서 유의할 것은, 일반적인 사안과 달리 위의 후생 문제는 두 가지 유형의 피해와 독립적인 피해 발생의 연속확률분포를 배정하였다는 점이다. 징벌적 손해배상제도의 목적은 두 피해 유형 모두에 대해 사회적으로 최적의 유의 비용을 기업이 부담하도록

할 수 있는지 여부이며, 제도의 밑바탕은 역수배를 응용한 PS 1998의 직관에 기초한다. 추후에는 모형을 확장하여 그들의 징벌적 손해배상에 관한 직관이 부의 외부 효과가 있는 개인정보 피해 사안에 대해서도 적절한 방법인지를 알아볼 것이다.

3. 개인정보 유출 사고와 관련한 모형의 주된 가정

다음의 주요 가정은 모형을 단순하면서도 현실적으로 이해하기 위해 연구 전반에 걸쳐 활용할 가정들이다.

- (1) 기업은 독점적 기업으로 상정한다. (개인정보 유출 사고를 당하는 기업들은 상당 수 과점적 영향력을 시장에서 행사하는 기업들인 경우가 있다. 모형을 통해 직관적인 결과를 얻기 위해 필요한 가정이다.)
- (2) 소비자들은 기업의 보안에 대한 유의 정도를 간접적으로나마 유추할 수 있으며, 이를 기준으로 서비스의 소비량을 결정한다.
- (3) 재판 및 소송비용 등은 미미한 것으로, 결과적으로는 배상 책임을 모두 법원의 판결 하에 결정이 된다.
- (4) 개인정보 유출 사고에 관하여 소비자는 유의 비용 및 책임을 지지 않으며, 법원은 엄격 책임제도 하에서 판결한다. (이는 현실적으로 소비자가 고의 또는 과실로 금융사 등에 제공된 개인정보를 유출할 가능성이 미미하다는 점에 착안한다.)
- (5) 기업은 본인이 재판을 통해 손해를 배상하게 될 확률을 정확히 인지하고 있다. 이를 다음과 같이 표기한다.

$$(3) \lambda(\text{배상확률}) \in (0,1)$$

- (6) 1차 및 2차 피해는 사실상 같은 시간대에 독립적 확률로 나타난다.
- (7) 기업은 어떠한 개인정보 관련 보안사고에 관해서도 기업은 무조건적으로 법적인 손해배상 책임을 진다는 점을 고지하며, 소비자들은 재판을 통해 손해를 배상하게 될 확률을 인지하지 못한다. (이는 약관 등에 관해 일반적인 소비자들이 충분히 숙고하여 읽거나 하지 않는 등의 행태를 고려한 가정이다.)
- (8) 1차 피해보다 2차 피해의 피해 규모가 상대적으로 매우 크다.

4. 단일 피해 유형과 징벌적 손해배상

먼저, 어떤 시점에 단 한 가지 피해 유형만 존재하는 보안사고를 겪는 가능성에 직면해 있다고 가정하자. 이는 모형을 더 현실에 맞게 발전시키기에 앞서 징벌적 손해배상 제도가 가장 단순한 상황에서 앞서 언급한 직관에 기초하여 적용되었을 때 후생을 최적화하는 전략을 각 주체가 선택하도록 하는지를 알아보기 위해서이다. 이러한 단일 피해에 대해, 기업은 사고가 발생하여 본인이 배상하여야 하는 확률은 $p(x)$ 가 아닌 $\lambda p(x)$ 로 인지하며, $\lambda \in (0, 1]$ 이다. 이를 통해 PS 1998의 책임 회피 확률에 근거한 징벌적 고려가 가능하다. 이러한 맥락에서, 역진 귀납법의 논리를 적용한 기업의 선택을 생각해보자.

엄격 책임을 기초로 하여 단일 피해 유형에 대해 기업의 기대 수익을 가장 먼저 분석해 볼 때, 기업이 배상을 하게 될 확률을 통해 기대 배상액을 과소평가할 때와 그렇지 않을 때를 비교해 본다면 다음과 같다.

$$(4) U_{\text{기업}} = pq - q(c + x + p(x)h_1) ; \text{과소평가 안할 시}$$

$$(5) U_{\text{기업}} = pq - q(c + x + \lambda p(x)h_1); \text{과소평가 할 시, } \lambda \in (0, 1]$$

이 때, 기업이 유의 비용을 책정한 이후에 소비자가 소비 선택을 내리는 상황을 상정하되, 앞서 언급한 주요 가정을 반영하여 소비자들은 기업이 100% 확률로 피해가 발생하는 경우 책임을 진다고 하자. 소비자의 기대 효용으로부터 소비자의 수요 함수를 도출할 수 있다. 이는 다음과 같다. 수요 함수는 기대 효용함수를 소비량에 대해 미분한 후 정리한 결과이다.

$$(6) U_{\text{소비자}} = u(q) - pq \leftrightarrow p = u'(q); \text{ 소비자의 수요 함수}$$

소비자의 수요 함수를 기업이 역순으로 자신의 유의 비용 책정에 고려한다면, 다음과 같은 결과로 이어진다.

$$(4-1) U_{\text{기업}} = q^* u'(q) - q(c + x + p(x)h_1) ; \text{과소평가 안할 시}$$

(5-1) $U_{\text{기업}} = q^* u'(q) - q(c + x + \lambda p(x)h_1)$; 과소평가 할 시, $\lambda \in (0,1]$
 이러한 기대 수익을 기업이 극대화할 때, 1차 조건은 다음으로 귀결된다.

$$(4-2) \quad \frac{\partial U_{\text{기업}}}{\partial x} = 0 \leftrightarrow -1 = p'(x)h_1 \quad s.t. \quad x = \dot{x}; \text{과소평가 안할 시}$$

$$(5-2) \quad \frac{\partial U_{\text{기업}}}{\partial x} = 0 \leftrightarrow -1 = \lambda p'(x)h_1 \quad s.t. \quad x = \ddot{x}; \text{과소평가 할 시}$$

$$(4-3) \quad \frac{\partial U_{\text{기업}}}{\partial q} = 0 \leftrightarrow u'(q) = c + \dot{x} + p(\dot{x})h_1 - qu''(q) \quad s.t. \quad q = \dot{q}; \text{과소평가 안할 시}$$

$$(5-3) \quad \frac{\partial U_{\text{기업}}}{\partial q} = 0 \leftrightarrow u'(q) = (c + \ddot{x} + \lambda p(\ddot{x})h_1) - qu''(q) \quad s.t. \quad q = \ddot{q}; \text{과소평가 할 시}$$

위의 수식들을 요약하면 다음과 같다. 기본적으로 과소평가를 할 시, 엄격 책임을 적용하더라도 기업은 실제로 기대되는 피해에 대한 규모를 h_1 보다 작은 λh_1 으로 기대하게 되며, 이에 따라 실제로 배상해야 하는 기대 규모가 줄어들면서 기업은 과소평가를 안 할 때보다 더 작은 수준의 유의비용($x = \ddot{x}$)을 책정하게 된다. 이는 매우 직관적인 결과인데, 문제는 결과가 모두 실현된 이후에는, 실제로 사고가 일어난 이후에 소비자가 배상을 받지 못할 확률이 $(1-\lambda)$ 만큼 존재하기 때문에 실제로는 소비자의 애당초 기대 효용보다 훨씬 작은 수준의 효용을 유발할 수밖에 없으며, 단위당 피해액이 충분히 크다면 실제의 기대 효용은 오히려 음수가 될 수 있다.

그렇다면, 소비자와 기업이 기대하는 사고의 발생 확률과 실제 배상 확률이 일치하여, 기대되는 손해액과 배상액을 일치시키는 방향으로 법률을 교정하기 위해서는, 다음과 같이 배상 확률의 역수만큼 기업의 배상기대액을 증액하여 판결하면 된다는 것이 징벌적 손해배상 제도의 가장 기초적인 이유이다.

$$(5-4) \quad U_{\text{기업}} = pq - q\left(c + x + \lambda^* \left(\frac{1}{\lambda}\right) p(x)h_1\right); \text{과소평가 할 시, } \lambda \in (0,1]$$

이와 같은 징벌적 손해배상 제도를 적용한다면, 소비자가 기대하는 효용이 수식(5)와 같다고 가정한다면 결과적으로 수식(2)에서 도출되는 사회적 최적 수준의 유의 비용과 정확하게 일치하도록 기업의 선택을 강제할 수 있다.

그러나 주된 문제는, 징벌적인 손해배상 제도를 논의할 때 빠짐없이 등장하는 쟁점으로서, 소비자들이 발생 빈도가 그렇게 높지 않은 사고에 대해서 징벌적으로 배상액을 받아낼 수 있을 때, 그들의 기대 효용이 왜곡된다는 점이다. 이는 소비자들이 징벌적 배상이라는 특수한 형태의 제도가 금융보안 사고와 같은 특정한 사건에 대해 적용된다는 점을 명확하게 인지한다고 가정할 때를 뜻한다. 이러한 문제에 직면하는 경우, 앞서 언급한 이상적 결과가 도출되지 않을 수 있다.

5. 소비자의 기대에 변동이 발생했을 시의 단일 피해 유형 모형

징벌적 목적으로 배가된 배상액에 관하여 소비자가 인지하고 있는 상황을 가정해 보자. 이에 따라 소비자들은 잠재적으로 사고의 발생으로 인한 손배소를 진행할 시에 높은 배상액을 통해 오히려 인지된 손실보다도 이득이 발생한다고 이해할 가능성이 있다. 이 때, 소비자들의 효용 함수가 다음과 같이 변동할 수 있다.

$$(7) U_{\text{소비자}} = u(q) - pq + qp(x)\left(\frac{1}{\lambda} - 1\right)h_1 \leftrightarrow p = u'(q) + p(x)\left(\frac{1}{\lambda} - 1\right)h_1; \text{ 소비자의 수요 함수}$$

소비자의 경우 징벌적인 배상액을 통해 사고에 의한 손실액보다 더 큰 규모의 배상을 엄격 책임 하에서 받을 수 있다는 점을 인지하지만, 기업이 실제 배상해야 하는 확률이 1보다 작다는 (즉, 100% 확률로 배상을 받을 수는 없다는) 사실을 인지하지 못한다는 점에 주목해야 한다. 이를 징벌적 손해배상을 인지한 독점적인 사측의 기대 이윤 함수인 수식 (5-4)에 대입 후 최적화 문제를 풀다면 다음과 같다.

$$(5-5) U_{\text{기업}} = q^* \left\{ u'(q) + p(x)\left(\frac{1}{\lambda} - 1\right)h_1 \right\} - q(c + x + p(x)h_1) \\ = qu'(q) - q\left(c + x + \left(2 - \frac{1}{\lambda}\right)p(x)h_1\right); \text{과소평가 할 시, } \lambda \in (0, 1]$$

$$(5-6) \frac{\partial U_{\text{기업}}}{\partial x} = 0 \leftrightarrow -1 = \left[2 - \left(\frac{1}{\lambda}\right) \right] p'(x)h_1 \text{ s.t. } x = \bar{x}$$

이에 관하여, 손해배상 확률인 λ 가 어떤 이유에서 0.5 또는 그 미만이라고 가정해 보자. 이 때, 수식(5-6)에서 $2 - (1/\lambda)$ 은 0보다 작은 값을 가지게 되며, 이는 유의 비용을 추가로 투자하더라도 결국 기업 입장에서는 소비자의 기대가 바뀌었다는 가정 하에 손실만 유발하는 관계로 수식 (5-6)의 조건을 기업이 결코 만족시킬 수 없게 된다. 따라서, 기업은 도리어 아예 가능하면 작은 수준의 유의 비용만 투자하고 마

는 극단적인 결과를 초래하게 된다.

반면, 손해배상 확률이 0.5보다는 높지만 1보다는 작은 값을 가질 때, 수식 (5-6)의 우측 항을 수식 (4-2)의 결과와 대조하여 보자.

$$(4-2) \quad \frac{\partial U_{\text{기업}}}{\partial x} = 0 \leftrightarrow -1 = p'(x)h_1 \text{ s.t. } x = \bar{x}; \text{과소평가 안할 시}$$

이 때, (5-6)의 $2 - (1/\lambda)$ 은 0보다는 크지만 1보다 작은 값을 가지게 되어, $[2 - (1/\lambda)]h_1$ 은 (양수 값을 가지는 단위 손해분)보다는 작은 값을 가지게 된다. 이때도 앞서 언급한 바와 마찬가지로, 기업은 \bar{x} 의 유의 비용을 책정하는데, 이 때 $\bar{x} < \dot{x}$ 이 성립하게 되어, 이때도 단위 서비스당 유의 비용을 기업은 최적수준보다 낮게 선택한다. 이를 직관적으로 이해하자면, 소비자가 징벌적 배상액만 인지하고 실제 배상을 받을 확률인 λ 에 대한 인지가 결여되어 있을 경우, 독점적 기업은 역으로 소비자가 인지한 잠재적인 이득을 소비자 수요 함수로서 기업의 전략 선택에 반영하게 된다. 그렇기에 소비자가 인지한 잠재 이익을 독점적 가격의 설정을 통해 기업이 흡수하는 과정에서 도리어 최적의 수준보다 유의 비용을 덜 지출하는 결정을 하게 될 가능성이 있다.

6. 다중 피해 유형을 고려한 모형으로의 확장

앞서 살펴본 단일 피해 유형에 관한 논의는 징벌적 손해배상 제도가 소비자의 기대 효용과 기업의 기대 이윤에 영향을 주는 상황에서 독점적 기업이 전략 선택에 우위에 있는, 매우 자연스러운 상황을 다루었다. 소비자가 배상 확률에 대한 인지가 없다는 현실적인 가정이 기업에게 역으로 유의 비용을 최적 수준보다 더 낮게 책정하는 유인을 제공할 수 있다는 점을 가장 단순한 상황을 통해 살펴본 바, 이 결과를 다중 피해 유형이 있는 금융사의 개인정보 보안사고 상황에 맞추어 확장해볼 필요가 있다. 개인정보 유출 사고에 의한 민사소송에서 유출 자체에 의한 정신적, 가치적 손해(1차 피해)에 관해 배상을 하는 기업은 다수 있었으나, 습득한 자가 해당 개인정보를 이용하여 범죄적 이득을 챙겨서 발생하였거나 발생할 가능성이 있는 피해(2차 피해)에 관해서는 배상 책임을 인정하지 않는 경우가 많다는 점이 이와 같은 모형을 고려하는 이유이다. 이를 반영하여 다양한 상황을 고려해 보면 다음과 같다.

(1) 엄격 책임이 적용되지만 2차 피해에 관하여 항상 배상 받지 못하는 경우

앞서 적용된 맥락을 재방문하여, 명시된 법상으로는 엄격 책임이 적용되고 있다고 하자. 1차 피해에 대하여는 유출 사고의 발생 시 기업의 책임회피 확률이 없다고 가정하되, 2차 피해에 대해서는 라는 1 미만의 배상 확률이 적용된다고 하자. 이 때, 사측의 기대 이윤은 다음과 같다.

$$(8) \quad U_{\text{기업}} = pq - c(x + y + p(x)h_1 + \lambda f(y)h_2)$$

그러나, 소비자들은 엄격 책임이 100% 확률로 적용된다는 가정 하에서 효용을 계산한다면, 수식 (6)의 기대 효용을 보유하게 된다.

$$(6) \quad U_{\text{소비자}} = u(q) - pq \leftrightarrow p = u'(q); \text{ 소비자의 수요 함수}$$

이를 반영하여, 독점적인 금융사는 다음과 같이 역진 귀납을 통해 유의 비용 등을 결정한다.

$$(9) \quad \frac{\partial U_{\text{Firm}}}{\partial x} = 0 \leftrightarrow -1 = p'(x)h_1 \quad s.t. \quad x = \hat{x} = x^*$$

$$(10) \quad \frac{\partial U_{\text{Firm}}}{\partial y} = 0 \leftrightarrow -1 = \lambda f'(y)h_2 \quad s.t. \quad y = \hat{y} < y^*$$

$$(11) \quad \frac{\partial U_{\text{Firm}}}{\partial q} = 0 \leftrightarrow u'(q) = c + \hat{x} + \hat{y} + p(\hat{x})h_1 + \lambda f(\hat{y})h_2 - qu''(q) \quad s.t. \quad q = \bar{q}$$

수식 (9)와 수식 (10)을 비교하면, 결국 책임 면피의 확률이 존재하는 피해 유형에 한해서 사측은 단위당 유의 비용을 사회적인 최적 수준보다 적게 책정할 소지가 있다는 점을 알 수 있다. 개인정보 보호법에 의해 개인정보 유출에 의한 피해에 대하여 법적으로는 엄격 책임이 적용된다 하더라도, 본 연구에서 정의한 2차 피해에 대해서는 실질적으로 배상 책임을 회피할 가능성이 존재한다면 해당 유형의 피해에 관해서만 기업은 유의 비용을 적게 선택한다면 보편적인 징벌적 손해배상의 직관에 의해 이러한 유형의 피해를 특정하여 징벌적 배상을 수행해야 할 것이다.

하지만 현재 한국의 개인정보보호법 39조는 이러한 피해 유형을 구분하지 않고

징벌적 배상을 선고할 수 있도록 하고 있다. 이 때, 두 가지 의문점을 살펴보아야 한다. (1) 징벌적 배상액이 유출 사고가 발생한 기업이 대부분 책임을 회피할 수 없는 1차 피해에 관하여도 책정이 되는 것은 기업이 사회적으로 최적 수준의 주의를 기울이도록 강제할 수 있는가? (2) 2차 피해 유형에 대해서 적용된 징벌적 배상제도는 실제로 기업이 해당 종류의 피해에 대해 사회적으로 최적 수준의 주의를 기울이도록 할 것인가?

(2) 징벌적 손해배상이 모든 피해 유형에 적용될 시

한국의 현행법상 개인정보의 유출 등에 관한 피해는 개인정보보호법 39조에 의해 최대 3배의 배상을 받을 수 있다. 이를 단순화하여, 3배라는 배상이 확정적으로 적용된다고 가정하고, 이것이 앞서 밝혔듯 포괄적으로 모든 피해 유형에 대해 적용된다고 가정해보자. 이에 따른 기업의 기대 이윤은 다음과 같다.

$$(12) \quad U_{\text{기업}} = pq - c(x + y + 3p(x)h_1 + 3\lambda f(y)h_2)$$

또한 징벌적 배상 이면의 배상을 받을 실제 확률에 대한 인지가 없는 소비자는, 당 법령을 알고 있는 상태에서는 다음의 기대 효용을 가지며, 수식 (14)는 이로부터 도출된 소비자의 역수요 함수로 독점적 기업은 이를 알고 있다.

$$(13) \quad U_{\text{소비자}} = u(q) - pq + q\{2p(x)h_1 + 2f(y)h_2\}$$

$$(14) \quad p = u'(q) + 2\{p(x)h_1 + f(y)h_2\}$$

따라서, 독점적 금융사의 기대 이윤에 역수요 함수를 대입하고, 최적화 문제를 풀어보면 다음이 도출된다.

$$(12-1) \quad \frac{\partial U_{\text{기업}}}{\partial x} = 0 \leftrightarrow -1 = p'(x)h_1 \quad s.t. \quad x = x' = x^*$$

$$(12-2) \quad \frac{\partial U_{\text{기업}}}{\partial y} = 0 \leftrightarrow -1 = (3\lambda - 2)f'(y)h_2 \quad s.t. \quad y = y' < y^*$$

$$(12-3) \quad \frac{\partial U_{\text{기업}}}{\partial q} = 0 \leftrightarrow u'(q) = c + x' + y' + p(x')h_1 + (3\lambda - 2)f(y')h_2 - qu''(q) \quad s.t. \quad q = q'$$

먼저, 3배의 고정적 손해배상을 적용하는 경우, 징벌적 손해배상을 적용하지 않아도 되는 1차 피해 유형에 대해 기업은 사회의 최적 수준과 다르게 유의 비용을 책정할 유인이 없음을 수식 (12-1)의 결과를 통해 알 수 있다. 이는 독점적인 기업이 자신의 전략을 선택하는 단기 게임에서는, 소비자들의 효용함수로부터 역수요 함수를 자사의 기대 이윤에 반영하기 때문에 발생하는 결과이다. 직관적으로, 독점적 기업이라는 가정을 따른다면 사측은 잠재적으로 소비자가 징벌적 손해배상을 통해 실현할 수 있는 이익 분을 서비스의 단위 가격을 높게 매김으로써 상쇄해버릴 수 있기 때문에 별도의 영향이 발생하지 않는다.

다음으로, PS 1998의 직관에 따르면 당연히 징벌적 손해배상을 적용해야하는 2차 피해 유형에 관하여는, 사회적인 최적 수준보다 더 낮은 수준의 유의 비용을 선택할 유인이 남아있음을 수식 (12-2)를 통해 확인할 수 있다. 이는 $(3\lambda - 2)$ 라는 가중치의 등장에 따른 것인데, 사전에 정의한 바 λ 는 0과 1사이의 값을 가지기 때문에, 해당 가중치의 값은 1보다는 작고 -2보다는 크다. 단일 피해 유형을 고려했을 때에는 이러한 경우 가중치 값이 0보다 작다면 기업은 가능하면 작은 수준의 유의 비용을 선택한다. 명백히, 1단위 만큼 유의 비용을 더 높게 책정하는 것은 기업의 입장에서 오히려 손실을 유발하기 때문이다. 0보다 크지만 1보다 작은 경우 기업은 사회적 최적 수준보다 적은 유의 비용을 선택한다. 이는 수식 (12-2)에서도 마찬가지로 기 때문에, 결과적으로 사측에서는 어떠한 경우든 최적 수준의 유의 비용 미만을 고려할 것이라는 점이 중요하다. 이러한 결과는 또다시 독점적 기업이 소비자의 수요 함수를 자신의 기대 이윤에 반영하여 전략을 선택할 수 있다는 점에 기인한다.

따라서, 단순히 3배의 정량적 손해배상을 법에 포괄적으로 명시하는 것만으로 징벌적 손해배상의 직관적 효과를 기대하기가 힘들다는 것을 위의 모형을 통해 알 수 있다. 한걸음 더 나아가, 이를 다중 피해에 관해 말 그대로 2차 피해에 대한 배상 확률의 역수만큼 증액하여 법령을 정한다면 어떻게 될 것인지를 동일한 방법으로 유추해볼 수 있다.

2차 피해의 배상 확률의 역수만큼 손해액에 곱하여 증액하는 형태의 징벌적 배상은, 기업에게 다음과 같은 기대 이윤을 형성하게 한다.

$$(14) \quad U_{기업} = pq - c\left(x + y + \frac{1}{\lambda}p(x)h_1 + \frac{1}{\lambda}\lambda f(y)h_2\right) = pq - c\left(x + y + \frac{1}{\lambda}p(x)h_1 + f(y)h_2\right)$$

그러나, 모형의 주요 가정 중 2번째에 의해, 또다시 소비자들은 잠재적으로 사고의 발생에 따른 이익을 기대하게 됨으로써 다음과 같은 기대 효용을 가지게 된다.

$$(15) \quad U_{\text{소비자}} = u(q) - pq + q \left\{ \left(\frac{1}{\lambda} - 1 \right) p(x) h_1 + \left(\frac{1}{\lambda} - 1 \right) f(y) h_2 \right\}$$

이에 따라 소비자의 역수요 함수는 다음과 같다.

$$(16) \quad p = u'(q) + p(x) \left(\frac{1}{\lambda} - 1 \right) h_1 + f(y) \left(\frac{1}{\lambda} - 1 \right) h_2$$

이를 고려하는 독점적 기업은, 결국 다음의 기대 이윤을 상정하고 자신의 이윤을 극대화하는 방향으로 전략을 선택하게 된다.

$$(14-1) \quad U_{\text{기업}} = \left\{ u'(q) + p(x) \left(\frac{1}{\lambda} - 1 \right) h_1 + f(y) \left(\frac{1}{\lambda} - 1 \right) h_2 \right\} - c \left(x + y + \frac{1}{\lambda} p(x) h_1 + f(y) h_2 \right) \\ = qu'(q) - q \left(c + x + y + p(x) h_1 + \left\{ 2 - \frac{1}{\lambda} \right\} f(y) h_2 \right)$$

수식 (14-1)에 의거하여 이윤 극대화를 달성하기 위한 1차 조건을 살펴보면 다음과 같다.

$$(14-2) \quad \frac{\partial U_{\text{기업}}}{\partial x} = 0 \leftrightarrow -1 = p'(x) h_1 \quad s.t. \quad x = x'' = x^*$$

$$(14-3) \quad \frac{\partial U_{\text{기업}}}{\partial y} = 0 \leftrightarrow -1 = \left\{ 2 - \left(\frac{1}{\lambda} \right) \right\} f'(y) h_2 \quad s.t. \quad y = y''$$

$$(14-4) \quad \frac{\partial U_{\text{기업}}}{\partial q} = 0 \leftrightarrow u'(q) = c + x'' + y'' + p(x'') h_1 + \left\{ 2 - \left(\frac{1}{\lambda} \right) \right\} f(y'') h_2 - qu''(q)$$

수식 (14-2), (14-3)과 (14-4)의 결과를 토대로 해석하면, 특정한 피해 유형에 대해 배상 책임이 발생할 확률의 역수만큼을 적용하는 경우도 유사한 결론이 나타난다. 소비자의 기대 효용 함수에서 도출되는 역수요 함수를 알고 있는 사측의 독점적 입장에서는, 배상 확률의 역수배 형태의 징벌적 배상을 산정하더라도 해당되는 2차 피해 형태에 대해 사회적으로 가장 바람직한 유의 비용을 고르도록 강제하기가 힘들다. 수식 (14-3)에서 특히 $2 - (1/\lambda)$ 항은 항상 1의 값보다는 작게 나타나는데, 극단적으로 이러한 가중치가 0보다 작아지는 경우에는 앞선 논리대로 기업은 아예 주

의를 기울이지 않거나 정말 최소한의 주의만 기울이는 선택도 할 수 있을 것이다.

7. 부의 외부효과를 반영하는 사회적 최적과 사측의 선택

개인정보에 대한 보안사고에서 발생할 수 있는 부의 외부효과는 대표적으로 사고가 발생한 기업 이외에도 개인정보를 수집 및 보유하는 서비스나 상품을 사용하는 소비자들이 존재한다는 사실에서 기인한다. 일반적으로 이러한 보안 사고의 빈도가, 비유하자면 교통사고만큼 자주 발생하지는 않는다는 점이 이러한 부정적인 부수효과를 발생시키는 원인일 수 있다. 또한 규모가 큰 사고의 경우에는 각종 미디어를 통해 크게 보도가 되는 등 시장과 여타 경제주체들의 심리적 동요를 이끌어낼 수 있는 충분한 가능성이 있다. 이에 따라 다음과 같은 부수적인 사회적 효과가 있다고 가정하자.

$$(17) \quad U_{Min} = -q\{p(x)h_1 + f(y)h_2\} < 0$$

이러한 부의 외부효과는 서비스 이용 규모, 사고의 발생 확률에 비례적으로 그 절대값이 커지는 성격을 가지도록 가정해 보았다. 주의할 것은, 부정적 외부효과 등은 재판을 통해 배상을 받을 수 있는 확률 등과는 일단은 무관하게 설정되었다는 점이다. 수식 (17)의 부의 외부효과를 포함하여 조성된 사회 후생 함수는 각 경제 주체의 이윤 함수와 외부효과 함수의 합으로 구성한다.

$$\begin{aligned} (18) \quad W &= U_{\text{소비자}} + U_{\text{기업}} + U_{Min} \\ &= u(q) - pq - qp(x)(h_1 - T) - qf(y)(h_2 - T) + pq \\ &\quad - q(c + x + y + p(x)T + f(y)T) - q\{p(x)h_1 + f(y)h_2\} \\ &= u(q) - q(c + x + y + 2p(x)h_1 + 2f(y)h_2) \end{aligned}$$

이러한 사회 후생을 극대화하는 1차 조건과 그 해를 고려하면, 다음의 결과가 나타난다.

$$Max_{(x,y,q)} W$$

$$(18-1) \quad \frac{\partial W}{\partial x} = 0 \leftrightarrow -1 = p'(x)2h_1 \quad s.t. \quad x = x^*$$

$$(18-2) \quad \frac{\partial W}{\partial y} = 0 \leftrightarrow -1 = f'(y)2h_2 \quad s.t. \quad y = y^*$$

$$(18-3) \quad \frac{\partial W}{\partial q} = 0 \leftrightarrow u'(q) = c + x^* + y^* + p(x^*)2h_1 + f(y^*)2h_2 \text{ s.t. } q = q^*$$

이 때, 사회적인 최적 수준의 유의 비용이란 앞선 모형들과는 다르게 더 높게 책정되어야 함이 명확하다. 이는 수식 (18-1)과 (18-2)에서 구체적 수치로 나타나는데, 1단위 만큼 더 유의 비용을 투입함으로써 증가하는 사회 후생이 부의 외부효과를 감소시키는 분만큼 가중되어 2배로 나타나기 때문으로 파악된다.

그렇다면, 일례로 수식 (18)을 고려하여, 잠정적으로 단순히 2배의 배상을 하도록 법령이 현시점에 강제하고 있다고 가정하자. 한눈에 보기에, 지나치게 작은 유의 비용을 선택하는 행위가 감소시키는 사회 후생이 2배가 된 것과 유사한 상황이기에 때문에, 배상액을 2배로 올린다면 문제가 해결될 것처럼 생각할 수 있다. 현시점에서는, 앞서 언급한 책임을 회피할 확률 등은 다루지 않고 먼저 모형을 살펴본다. 이 경우의 기업의 기대 이윤은 다음과 같다.

$$(19) \quad U_{\text{기업}} = pq - q(c + x + y + 2p(x)h_1 + 2f(y)h_2)$$

그러나 이러한 법적 장치 하에서 소비자들은 손해의 발생 확률 대비 잠재적인 이득을 산정하게 되는 결과로 이어진다. 이는 다음의 기대 효용을 의미한다.

$$(20) \quad U_{\text{소비자}} = u(q) - pq + qp(x)h_1 + qf(y)h_2$$

다시, 앞서 가정했던 주요 사항들을 적용하면 본 연구에서는 독점적인 기업을 가정하였기에, 사측은 소비자의 역수요 함수를 도출하고 기대 이윤을 산정하게 된다. 이 때, 기업이 발견하는 역수요 함수는 다음과 같다.

$$(21) \quad p = u'(q) + p(x)h_1 + f(y)h_2$$

이를 기업의 기대 이윤 함수인 수식 (19)에 대입하면, 기업은 다음과 같은 이윤을 기대한다.

$$(19-1) \quad U_{\text{기업}} = q\{u'(q) + p(x)h_1 + f(y)h_2\} - q(c + x + y + 2p(x)h_1 + 2f(y)h_2) \\ = qu'(q) - q\{c + x + y + p(x)h_1 + f(y)h_2\}$$

주요하게, 2배의 손해배상액을 책정한 이후에 도출된 수식 (19-1)은 결국 엄격책임 하에서 일반적으로 기업들이 상정하는 기대 이윤과 다르지 않다는 점이다. 기업

이 역수요 함수를 도출하여 전략에 반영할 수 있는 시장 장악력을 가졌기 때문이다. 하지만 결과적으로 수식 (19-1)에서 기업이 선택할 유의 비용은 부의 외부효과가 없다는 가정 하에서는 사회적 최적 수준일 수는 있지만, 수식 (18)의 사회 후생 함수 아래에서는 그보다 더 적다. 이러한 결과들을 앞선 모형들처럼 책임 회피 확률이 존재하는 모형에 다시 적용한다면, 매우 직관적으로 실제 사회적 최적만큼의 유의 비용보다 더 적은 수준의 유의 비용을 기업들이 선택할 것으로 사료된다.

8. 과실 책임 및 비대칭 정보 하의 모형

앞서 언급한 모든 모형은 먼저 책임을 회피할 확률이 외생적으로 존재한다는 가정 하에서, 엄격 책임이 법리적으로 적용되는 사안에 대해 징벌적 손해배상 제도의 이상적 적용이 실제로 이상적인 결과로 나타날 수 있는지를 알아본다. 하지만 법리적으로도 개인정보보호법 39조가 기업 측에서 충분한 책임을 기울였음을 증명하였다는 전제 하에는 책임을 지지 않는다는 점이 앞서 언급한 모형의 현실성을 약화시킬 수 있으므로, 이를 보완하기 위해 다음을 고려하였다. 본 모형에서는 직관적인 이해를 위해 하나의 피해 유형을 가진 경우를 살펴보았다.

먼저, 사회적으로 최적 수준인 유의 비용 x^* 를 기준으로, 법관은 이 이상의 유의 비용을 기업이 투자하였을 경우 배상 책임을 인정하지 않는다고 가정하자. 반면에 이 미만으로 유의 비용을 투자하였을 경우, 금융사는 개인정보 및 보안사고에 관하여 수배(앞서 언급한 3배)의 손해액을 배상해야 한다고 가정하자. 이번에는 금융소비자가 기업이 투자한 유의 비용을 알지 못한다고 가정한다. 그렇기에 금융소비자의 경우, 50% 확률로 사측에서 충분한 유의 비용을 들였다고 예측하고, 50% 확률로 그렇지 않다고 상정하다. 금융소비자는 구체적으로 얼마의 유의 비용을 기업이 들였는지 여부를 알 수 없지만, 충분한 유의 비용을 사측이 들인 경우에는 x^* 를 들였을 것임을 사측의 우월 전략으로써 알고 있으며, 그렇지 않은 경우에는 사실상 100% 확률로 사고가 발생할 것이라고 고려한다.

$$(22) \quad U_{\text{소비자}} = u(q) - pq - \frac{1}{2}qp(x^*)h_1 + \frac{1}{2}q(3-1)h_1 \leftrightarrow p = u'(q) + \frac{1}{2}\{2 - p(x^*)\}h_1$$

반면에 기업의 경우, 선택할 수 있는 경우의 수는 다음과 같다.

- (1) 기업이 최적 수준 이상의 유의 비용을 투자하기로 하는 경우, 우월 전략은

(23-1) $U_{기업} = pq - q(c + x^*) = \left(u'(q) + \frac{1}{2} \{2 - p(x^*)\} h_1 \right) q - q(c + x^*)$; 최적 수준 이상 투자시 정확히 최적 수준인 x^* 를 투자하는 것이 된다. 다음의 수식 (23)에서 보듯, 최적 수준 이상을 투자한다면 모든 책임을 확실하게 지지 않을 수 있으며, 추가적인 투자는 일방적인 비용 부담이 되기 때문이다. 독점적 금융사가 이윤을 극대화하는 결정을 한다면, 다음을 극대화하는 서비스 수량을 시장에 공급한다고 볼 수 있다.

이 경우, 기업이 선택하는 극대화 수량은 다음을 만족한다.

$$(24-1) \quad \frac{\partial U_{기업}}{\partial q} = 0 ; \quad u'(q) = c + x^* - \frac{1}{2} \{2 - p(x^*)\} h_1 - qu''(q), \quad q = q^*$$

이를 본래의 이윤 함수에 대입하면, 최종적으로 기업의 이윤은 다음이 된다.

$$(25-1) \quad U_{기업} = -(q^*)^2 u''(q^*) > 0 \quad (\because u''(q) < 0, \text{ 한계효용 체감})$$

(2) 기업이 최적 수준 미만의 유의 비용을 투자하기로 하는 경우, 기업은 실제 배상에 있어서 3배의 징벌적 책임을 진다. 책임을 회피할 확률이 없다면 기업은 다음의 기대 이윤 함수를 가지게 된다.

$$(23-2) \quad U_{기업} = pq - q(c + x + 3p(x)h_1) = \left(u'(q) + \frac{1}{2} \{2 - p(x^*)\} h_1 \right) q - q(c + x + 3p(x)h_1)$$

이를 극대화하는 유의 비용 및 공급 수량을 살펴보면 다음이 도출된다.

$$(24-2) \quad \frac{\partial U_{기업}}{\partial x} = 0 ; 3p'(x)h_1 = -1 \leftrightarrow x = x^{**} < x^*$$

유의 비용은 앞선 모형에서 살펴본 바와 같이 유의 비용을 사회적 최적 수준보다 더 적게 설정하려고 하는 기업의 경우 실제로 사회적 최적 수준 미만에서 이윤을 극대화하는 수준을 선택하는 것은 가능함을 보여준다.

반면, 수량의 결정은 다음을 통해서 결정된다.

$$(24-3) \quad \frac{\partial U_{\text{기업}}}{\partial q} = 0 ; \quad u'(q) = c + x^{**} - \frac{1}{2} \{2 - p(x^*)\} h_1 + 3p(x^{**}) h_1 - q u''(q), \quad q = q^{**}$$

수식 (24-1)에 의해 결정된 서비스 수량을 투자한 결과로 실현될 기업의 이윤은 다음과 같다.

$$(25-2) \quad U_{\text{기업}} = -(q^{**})^2 u''(q^*) > 0 \quad (\because u''(q) < 0, \text{ 한계효용 체감})$$

마지막으로, 수식 (25-1)과 (25-2)를 비교했을 때, 가장 간략하게 모형을 이해하기 위해서 강한 가정으로, 금융소비자의 서비스 수량에 대한 효용 함수 $u(q)$ 에 대해 2차 도함수가 상수 값으로 고정되었음($u''(q) = k > 0$)을 전제하자. 그 때, 기업은 명확하게 다음의 경우에 더 낮은 수준의 유의 수준을 고르는 전략을 선호하게 된다.

$$(26) \quad q^{**} > q^* > 1$$

결과적으로 수식 (26)은, 독점적 금융사가 과실 책임 하의 3배 손해배상의 성격을 띤 징벌적 손해배상을 직면한다고 하더라도, 규정된 “충분한 유의 비용” 미만을 선택하더라도 해당 규정을 지킬 때보다 더 많은 서비스 수량을 공급하는 것을 최선으로 여기게 될 때, 규정을 지키지 않을 유인이 발생함을 뜻한다.

직관적으로 이는 현실에서의 상황에 어느 정도 부합한다. 앞서 언급하였듯, 독점적 금융사의 입장에서는 소비자의 수요 함수를 어느 정도 유추할 수 있다. 이 때, 이를 가격 및 수량의 결정에 이용할 수 있는 독점적 금융사가 도리어 소비자가 기업의 유의 비용에 대한 투자 정도를 정확하게 알지 못한다는 점을 활용하여 더욱 많은 수량을 시장에 공급함으로써 이윤을 늘리고 도리어 보안 등 부수적 요소에 관한 투자를 게을리할 수 있다. 현실에서는, 은행이나 카드사 등에서 각종 부가 혜택 등을 활용하여 과도하게 카드를 발급하는 등의 행태가 이러한 이론적 모양새에 부합한다고 할 수 있음에 유의할 필요가 있다.

이를 앞서 고려한 엄격책임 하의 모형에서의 주요 가정과 연결하여도 이러한 결과가 크게 달라지지 않을 것이다. 앞선 가정에서는 독점적 금융사가 소비자들이 명확하게 충분한 유의 비용을 기업이 투자하였다고 믿도록 강제할 수 있음을 가정하였기 때문이다. 이는 비대칭 정보를 활용하는 독점적 금융사가 가진 우위를 한층 강화한 것에 불과하다.

V. 결과 및 후속과제 제안

1. 모형의 소결 및 제안사항

본 연구에서 활용한 여러 모형은 금융산업에서 적용되고 있는 개인정보보호법 39조의 징벌적 손해배상제도의 효용성에 관하여 가장 이상적인 차원에서의 징벌적 손해배상의 적용 및 현재 국내에 적용되고 있는 3배 배상액 책정의 효용성에 관하여 논의하였다. 이를 통해 간단하게나마 알 수 있는 사실은 다음과 같다.

먼저, 징벌적 손해배상이란 이상적인 경우 외생적 요인에 의해 금융사측에서 개인 정보 유출 등의 보안 사고와 관련하여 배상책임을 회피할 확률이 존재할 경우, 실제 배상 확률의 역수배만큼을 가산하는 방향이라고 기존의 이론에서는 제시되었음에도 이는 특정한 가정 아래에서 만족되지 못한다. 가장 중요하게는, 소비자들이 이러한 배상의 확률에 관한 정보를 명확하게 알지 못한 상황에서 단순히 손해액의 수배에 달하는 배상액을 얻을 수 있을 것을 기대하게 된다면, 금융사들은 이를 전략적으로 활용할 수 있다. 이는 사측에서 소비자들이 손해액 이상의 배상을 얻을 수 있음을 기대한다는 점을 역이용하여 독점적인 가격 설정을 통해 금융소비자의 효용을 사측의 이윤으로 치환함을 뜻한다. 동시에 사측에서는 이러한 전략적 우위 때문에 보안에 관한 유의 비용을 사회적인 최적 수준만큼 투자하지 않는 결정을 내릴 수 있다. 이러한 결과는 단순히 3배라는 상한을 두는 것으로는 해결되지 않을 수 있다.

또한, 별도의 제약사항이 없다는 가정 하에서 엄격 책임하의 독점적 금융사에 여러가지 유형의 보안 피해 유형에 대해 징벌적 손해배상을 포괄적으로 적용하여도 무관함을 알 수 있다. 이는 외생적인 요인(법관의 오류 등)에 의해 사측이 피해에 대해 배상하지 않아도 될 가능성이 원래부터 없는 피해 유형에 대해 과도한 배상액을 책정할 때, 사측이 과도하게 해당 유형의 피해를 예방하는 데에 비용을 쓰게 될 것인지에 대한 논의이다. 그러나 정보적 우위 하에서 앞선 경우와 마찬가지로 사측은 가격 및 공급 수량에 대한 전략적 선택을 통해 기대되는 배상액의 추가분만큼의 손실을 매우면서 별도로 추가적인 보안 투자 등을 하지 않을 것으로 기대되었다.

이에 더해, 사회적인 파장 및 금융시장의 불안을 야기할 수 있는 보안 사고의 부의 외부효과를 반영한다면 문제가 심화됨을 알 수 있었다. 이는 금융사들의 일반적

인 사고 하에서는 부의 외부효과가 사측의 이윤과 직접적으로 결부되지 않는다는 판단 하에 사회적으로 바람직한 수준의 유의 비용보다 더 적게 비용을 책정할 가능성 때문이다. 또한 이 때 발생하는 소비자 기대의 왜곡 때문에, 단순히 부의 외부효과 규모의 고려한 징벌적 손해배상을 시행하는 경우 사측은 충분한 주의를 기울이지 않을 가능성이 남아있음을 보였다.

이러한 논의들은 공통적으로 징벌적 손해배상을 시행하는 경우 금융소비자들의 기대 효용이 잘못된 방향으로 왜곡될 가능성 때문에 발생함에 주목해야 한다. 대표적으로, 이상적인 징벌적 손해배상을 산정할 수 있다고 고려한 경우에도, 금융소비자가 배상 받을 확률이 외생적으로 1 미만으로 존재한다는 사실을 금융소비자가 모르는 경우 사측에서는 이를 활용할 유인을 가지게 된다. 마찬가지로 부의 외부효과를 교정하는 수단으로 금융소비자에게 사고에 관한 배상액을 수배 이상 받을 수 있도록 한다면, 실질적으로는 금융소비자가 가지게 되는 배상에 대한 과도한 기대 때문에 도리어 금융사측에서는 이윤과는 별개로 유의 비용을 충분히 투자하지 않을 유인을 가진다. 따라서 여러 문제(금융사 측이 책임 회피에 성공할 가능성, 금융시장에서의 부의 외부효과 고려 등) 때문에 사측이 충분한 주의를 기울이지 않는 문제를 교정하기 위해 징벌적인 손해배상제도를 활용하는 경우 사측의 기대 배상액의 규모를 늘리는 것 외에도, 소비자가 기대하는 배상액이 실제 손해액을 넘지 않도록 하는 것이 매우 중요할 수 있다.

이러한 문제를 교정하기 위한 정책은 다양한 방향이 될 수 있다. 간접적으로는, 금융소비자에게 법정 손해배상액의 규모, 손해배상의 구체적 판례 및 개별 사례에서의 배상 가능성 등을 친숙하게 소개하는 등 징벌적 손해배상에 의해 왜곡된 금융소비자의 기대가 형성되지 않도록 하는 것을 들 수 있다. 보다 직접적인 방법으로는, 굳이 징벌적인 손해배상을 택하지 않고 수배의 배상액을 산정하되 실제 손해액을 초과하는 분은 국가에 귀속하는 것을 들 수 있다. 후자의 경우는 해외의 징벌적 손해배상에 관한 정책연구에서는 분할 배상(Split Award)라는 정책으로 구체화되어 논의되고 있음을 관찰할 수 있다는 점에서, 한국에서도 소비자(금융소비자)의 기대 측면에서의 징벌적 손해배상을 법제적, 경제학적 차원에서 보다 심도 있게 관찰해야 한다.

마지막으로, 실제로는 비대칭 정보 하에서 개인정보보호법 39조는 엄격 책임이 아니라 과실 책임 하에서 운영되는 특성을 띠는 점에 기대어 모형을 변형해보았다.

그 결과, 독점적 금융사의 경우 사회적으로 바람직한 수준 미만의 유의 비용을 기업이 선택할 유인이 있을 가능성을 유추하였다. 사회적으로 바람직한 수준보다 더 낮은 비용을 지출하고, 사고가 발생 시 징벌적(3배) 배상을 하더라도, 이 때 기업이 선택할 최적의 금융서비스 공급 수량이 굳이 사회적 최적인 유의수준 이상을 선택할 경우의 공급 수량보다 많다면, 금융사는 금융서비스를 증량하고 기대 이윤을 늘리는 것으로 징벌적 배상에 의한 기대 비용을 상쇄할 수 있었다. 이러한 가능성을 고려할 때, 금융사가 개인에게 금융상품이나 서비스에 가입하도록 과도하게 권유하는 등의 행태가 허용되는 경우 사측에서는 보안 비용 등에 대한 투자를 소홀히 할 가능성이 있음을 알아보았다. 이는 개별 금융사가 금융소비자에게 금융서비스나 신용카드 등을 발급하는 과정에서 정부가 더욱 면밀하게 감시하고 과도한 공급 등을 규제하는 것이 개인정보보호법에 적용된 징벌적 배상 제도가 바르게 역할을 수행하도록 하는 하나의 단초가 됨을 시사한다.

2. 모형을 활용한 이론 정립의 한계점 및 확장 가능성

본 연구의 중요한 한계점은, 모형을 통해 살펴볼 때 사용한 여러 가지 가정사항들이 현실과 부합하지 않을 가능성이 있다는 점이다. 일례로, 일반적으로 금융산업은 독점 시장이라기보다는 정부에 의해서 진입이 극히 제약되는 과점시장으로 보는 것이 바람직함에도, 본 연구에서는 직관적인 이해를 위해 독점 시장을 가정하였다는 점이 있다. 뿐만 아니라, 개인정보보호법에 대해 징벌적 손해배상이 적용된 지도 이미 수년이 지났지만, 실제로는 3배 또는 그 미만이라도 법원이 징벌적 손해배상을 인정한 판결이 흔치 않다는 점도 주요하다. 이는 현실에서 금융소비자들이 보안 사고 등에 대한 피해에 대해 실질적인 판례 등을 통해 징벌적 손해배상을 받을 수 있다고 기대하기에는 어렵다는 의미이다. 결국 매우 단순한 이론을 적용한다면 징벌적 손해배상이 법적인 효용을 발휘하기 위해 앞서 언급한 분할 배상 등의 정책을 고려할 필요가 드러나지만, 실제 재판 결과 등이 이론에서의 가정 사항 등을 만족하지 못한다면 모형을 통해 앞서 언급한 정책제안점들의 의의가 퇴색될 수 있다는 점은 주의해야 할 것이다.

또한, 본 연구에서 사용한 모형은 엄격 책임 및 과실 책임 하에서 단기 게임인 개인정보보호법의 징벌적 손해배상을 살펴보았으나, 이보다 동적(Dynamic)인 모형을

고려할 필요가 있다. 특히, 기업이 사회적인 최적보다 주의를 덜 기울이는 것이 여러 기에 걸친 게임에서 안정적인 균형전략일지를 살펴보아야 한다는 점이다. 이를테면, 소비자의 기대가 매 기마다 고정된 함수일 수도 없을 뿐더러, 한 번 보안사고가 난 이후에는 소비자의 기대에도 상당한 변화가 나타날 것임을 기업이 고려하는 경우에도 과연 기업은 계속 부주의한 수준의 보안 투자를 할 것인가? 이는 동적인 모형 및 실증분석을 통해 면밀하게 파악해야 할 것이다.

모형을 통한 검토 이상으로, 이론적인 바탕에서의 정책적 논의를 벗어나 실증적인 분석을 통해 개인정보보호법에 적용된 징벌적 손해배상의 효용을 평가할 필요가 있다. 이는 계량적으로 실제 금융산업 현장에서 정보 보안 및 소비자 보호에 어느 정도의 투자가 되고 있는지를 민간차원에서는 알 수 없다는 점에서 비롯된다. 특히나 개인정보보호법 등 관계 법령에 징벌적 손해배상이 도입된 이후에 금융사가 실제로 해당 분야에 대한 투자를 상대적으로 늘렸는지 등을 파악하는 것은 이를 관리감독하는 정부부처 등에서 수행해야하는 역할이다. 그렇기에 본 연구는 개인정보보호법의 개정이라는 맥락 하에서도 환경적 뒷받침이 없다면 배상액의 증액만으로는 기업이 충분한 주의를 기울이도록 하는 데에는 한계가 있을 수 있다는 점을 강조하는 데에 그친다.

마지막으로, 징벌적 손해배상은 단순히 충분한 주의를 기울이도록 강제하는 수단으로서의 효용 이외에도 연구가 활발히 이루어진 바 있다. 합의를 통한 배상액 산정이 이루어지는 경우 실제 배상 및 납소 가능성에 관한 연구(Rhee, 2012)나, 징벌적 배상 제도를 보완하는 여러 제도에 관한 연구(Landeo, 2007), 이에 관해 미국의 헌법이라는 법제적 차원에서 수행한 연구(Zipursky, 2005) 등 다양한 차원에서의 논의가 2000년대 이후로 계속되고 있다. 그러나 국내에서는 상당 부분 법제적 차원에서 적용할 수 있는 범위에 대한 논의가 주가 될뿐더러, 특히 개인정보보호법에 대한 징벌적 손해배상의 적용에 대해서는 지엽적으로 법리적 검토¹⁸⁾가 있을 뿐 법에 관한 이론적, 실증적 검토가 아직 많이 부족한 것이 사실이다. 본 연구도 이러한 한계에서 벗어나지 못하며, 단순히 기존의 이론적 도구를 가지고 가정 사항이 성립되

18) 이에 관하여 징벌적 손해배상이 개인정보보호법에 적용될 시 배상액의 합리적 산정을 할 수 있도록 하는 법제적 방안이나 징벌적 손해배상의 특별법 제정에 관한 논의(김미혜, 2008)이나 2014년 이후 국회에 제출되었던 개인정보보호법 개정안에 대한 법리 및 사례 중심의 논의(송동수 성기만, 2014), 징벌적 손해배상을 적용해서는 안 된다는 주장에 관한 여러 합리적 이유 및 현재의 법제 안에서 유사한 기능을 하도록 하는 방안에 관한 연구(최나진, 2014), 징벌적 배상 제도를 기능하게 하기 위한 배심제의 점진적 도입을 주장하는 연구(이용인, 2018) 등을 참고.

지 않는 여러 경우 등을 고려할 때 나타나는 착안 사항을 제시하는 데에 그치고 있다. 때문에, 본 연구 이후로는 해당 제도에 관하여 징벌적 손해배상에 의한 남소의 가능성, 재판 횟수 및 합의/소송 비용의 효율성 차원, 기업에 대한 재정적 리스크의 차원 등 다양한 측면에서 금융산업에서의 징벌적 손해배상에 대한 연구가 계속되어야 할 것이다.

[참고문헌]

- [1] 전승재, 권현영, “개인정보 유출로 인한 손해배상 제도에 관한 고찰-신용카드 개인정보 유출 소송을 통해 드러난 제도적 한계를 중심으로”, 서울대학교 공익산업법센터, pp.28-51, 2018.
- [2] David Owen, “A punitive Damages Overview:Function, Problems and Reforms“, Ph. D., University of South Carolina, South Carolina, 1994
- [3] Alan Calnan, “Ending the Punitive Damage Debate“, Depaul Law Review, vol 45, pp. 101-105, 1995
- [4] Robert Francis Harper, “The Code of Hammurabi King of Babylon about 2250 B.C.“, Ph. D., The University of Chicago Press, Illinois, 1904
- [5] 최병조, “12표법(대역)”, 서울대학교 법학, vol.32, pp157-176, 1991
- [6] STATUTES OF THE REALM 26, Statue of Westminster I, Parliament, 1275
- [7] Wilson Elser, Punitive Damages Review 50-State Survey, WilsonElser, NewYork, 2014
- [8] 김정환, “징벌적 손해배상의 적절한 운영방안에 관한 연구”, 사법정책연구원, 경기도 고양시, 32-9741568-001269-01, 2019
- [9] 전한덕, “금융소비자보호 관련 집단소송 및 징벌적 손해배상제도 도입 당부에 관한 논의”, 한국보험법학회 보험법연구, 11권 1호 pp. 265-299, 2017
- [10] 이민영, “개인정보권의 침해와 징벌적 손해배상제도”, 정보통신정책, 제18권 8호 통권 392호 pp.14-35, 2006
- [11] 박성민, “징벌적 손해배상제도의 형사체계편입에 대한 비판적 고찰 -하도급법상의 적용제한을 중심으로-”, 홍익대학교 법학연구소, pp. 191-211. 2017.
- [12] 양승현, “징벌적 손해배상 제도의 도입 논의 및 입법 현황 검토”, 보험연구원, pp. 1-7. 2019.
- [13] 윤강일, 이민경, 김규문 외 1명, “징벌적 손해배상제도의 도입”, 경성대학교 법학연구소, pp. 257-275. 2017.
- [14] 이종구, “전보배상과 징벌적 손해배상 및 3배 배상제도에 관한 연구-개인정보보호법상의 3배 배상제도의 도입에 즈음하여-”, 한국경영법률학회, pp. 447-486. 2015.
- [15] 김영세, “게임이론: 전략과 정보의 경제학”, 8판, 박영사, pp. 25, 85-90, 151-164, 2018
- [16] Douglas Baird et al., “Game Theory and the Law”, 1판, Harvard University Press, pp. 6-75, 1998
- [17] Benjamin C. Zipursky, “A theory of punitive damages”, Texas law Review, vol 84, pp. 105-171, Nov. 2005

- [18] Surajeet Chakravarty, David Kelsey, “Ambiguity and Accident law” , Journal of Public Economic Theory, vol 19, no. 1, pp. 97-120, Mar. 2016
- [19] Claudia M. Landeo et al., “Deterrence, Lawsuits, and Litigation Outcomes Under Court Errors” , The Journal of Law, Economics, and Organization, vol. 23, no. 1, pp. 57-97, Apr. 2007
- [20] Robert J. Rhee, “A Financial Economic Theory of Punitive Damages” , Michigan Law Review, vol 11, no. 1, pp. 33-88, Oct. 2012
- [21] Alan M. Polinsky, Steven Shavell, “Punitive Damages: An economic Review” , Harvard Law Review, vol. 111, no. 4, pp. 869-962, Feb. 1998
- [22] Steven Shavell, “Strict Liability versus Negligence” , Journal of Legal Studies, vol 9, no. 1, pp 1-25, Jan. 1980
- [23] Louis Kaplow, Steven Shavell, “Economic Analysis of Law” , Handbook of Public Economics, Vol 3. pp. 1667-1671, 1674-1677, 1680, Jan. 2002
- [24] 김미혜, “개인정보침해에 대한 구제방안으로서 징벌적 손해배상에 관한 연구” , 아주법학, 2권 1호, pp. 49-77, 2008
- [25] 송동수, 성기만, “개인정보 유출에 대한 구제방안으로서 징벌적 손해배상” , 토지공법연구, 제67집, pp. 175-120, 2014
- [26] 최나진, “징벌적 손해배상 제도에 관한 비판적 고찰” , 학위논문(박사), 고려대학교 대학원, 2014
- [27] 이용인, “징벌적 손해배상보다 배심제가 먼저다” , 민주법학, 68권 0호, pp. 153-202, 2018

금융 데이터 비식별화가 분석 모형 성능에 미치는 영향 연구

류승주* · 오동춘** · 허준범***

* 신한카드 전략기획팀 과장

** 신한금융지주회사 디지털전략팀 차장

*** 고려대학교 컴퓨터학과 부교수

요 약

빅데이터 분석 기술의 등장과 발전에 따라 빅데이터 관련 산업 시장도 빠르게 성장하고 있다. 특히, 금융분야는 양질의 데이터가 축적되어 있고, 경제적 활용가치가 매우 높은 것으로 평가되고 있다. 그러나 해외 선진국의 금융시장에 비해 국내 금융권의 데이터 활용은 아직 기대에 미치지 못한다. 최근, 정부는 카드사에 빅데이터 제공서비스를 운영할 수 있도록 허용하고 금융산업 전반에 빅데이터 활성화를 추진하고 있다. 금융권의 데이터 거래는 안전한 고객정보의 비식별화와 적정 수준의 모형 성능을 보장되어야 한다. 하지만 기존의 비식별화 연구는 대부분 개인의 프라이버시 보호 관점으로 수행되었거나 의료 데이터를 사용하여 실험하였기에 금융권에 적용하기에는 한계가 있었다.

이 연구에서는 금융 데이터의 비식별화가 모형 성능에 미치는 영향을 분석하여, 비식별화 수준을 준수하면서 모형 성능을 유지할 수 있는 방안으로 ‘준식별자별 범주화 레벨을 최소화하는 조합’을 제시하였으며, k-익명성 수준에 따른 성능하락폭을 줄이고 분석모형의 성능 불안정을 방지할 수 있는 데이터셋의 규모를 측정하였다. 또한 금융분야의 도메인 지식을 활용하면 모형 성능의 하락폭을 최대 50% 가깝게 줄일 수 있고, 최소한의 하락폭을 찾기 위한 실험의 횟수를 대폭 줄일 수 있다는 것을 확인하였다.

키워드

빅데이터, 비식별화, k익명성, 금융데이터, 모형 성능, 준식별자, 범주화

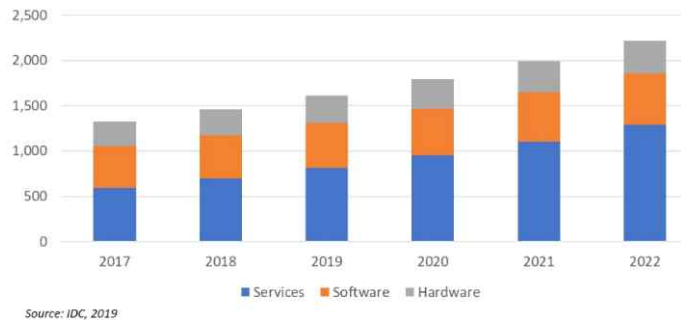
목 차

I. 서론	(3)
1. 연구의 배경	(3)
2. 연구의 목적	(4)
3. 논문의 구성	(5)
II. 이론적 배경 및 관련 연구	(6)
1. 비식별화 기법	(6)
2. k-익명성 기법	(8)
3. 비식별화 최적화 기법	(9)
III. 금융데이터 분석모형 선정 및 비식별화 방식 제안	(11)
1. 기존 연구의 문제점	(11)
2. 금융데이터의 분석모형 선정 방식	(11)
3. 준식별자 선정 및 비식별수준 검증	(12)
4. 분석 모형의 성능하락을 최소화한 비식별 방안	(13)
IV. 실험 및 결과	(14)
1. 실험 모형 및 데이터셋	(14)
2. 최적 기반 분석 모형 선정	(14)
3. 준식별자 선정과 비식별화 전후 비교	(15)
4. 비식별화 성능 분석	(18)
V. 결론	(22)
[참고문헌]	(23)

I. 서론

1. 연구의 배경

데이터는 4차 산업혁명 시대의 원유(原油)라고 불리우며 관련 기술의 발전에 따라 빅데이터의 중요성과 시장의 규모는 커지고 있다. 한국 IDC는 국내 빅데이터 및 분석 시장은 향후 5년간 연평균 10.9%로 성장하여 2022년 약 2조2천억원의 규모에 이를 것으로 전망된다고 하였다.[1]



〈그림 1, 국내 빅데이터 및 분석 시장 전망 2018-2022, IDC〉

또한 정부도 “데이터 규제혁신의 목표는, 데이터의 개방·공유를 확대하여 활용도를 높이는 것”, “이를 통해 신기술과 신산업, 새로운 제품과 서비스를 창출해야 함. 개인정보 보호 원칙을 지키면서 안전한 데이터를 활용할 수 있도록 규제를 개선하는 것”이라는 기조에 따라 데이터 관련 규제혁신과 투자계획을 발표하였다. [2] 이처럼 데이터 산업의 중요성과 정부의 지원의지에도 불구하고 국내 빅데이터 산업의 활성화는 기대에 못 미치는 수준이다. 한국데이터산업진흥원이 조사한 ‘2018 데이터산업 현황 조사’에 따르면 2018년 기준 우리나라 기관과 기업의 빅데이터 이용률은 10%에 불과하며, 2018년 스위스 국제경영개발대학원(IMD)이 발표한 전 세계 디지털 경쟁력 순위 보고서에 따르면 우리나라의 빅데이터 활용 순위(Use of big data and analytics ranking)는 63개국 중 31위에 머물렀다. [3] 또한 금융사의 경우 2014년 카드 3사의 1억580만건의 개인정보 유출 사태 이후 내부 데이터의 강력한 보호 정책 추진 등으로 적극적인 데이터 활용에 대한 목소리를 내기가 어려웠다.

국내 데이터 산업 환경과는 달리 글로벌 빅데이터 시장에서는 다양한 성공사

례가 생겨나고 있다. 미국의 ‘데이터마이너’社は 트위터 데이터를 분석해 유용한 정보를 제공함으로써 맞춤형 광고와 마케팅을 수행하고 있다. 구글의 헬스케어 자회사인 ‘베릴리’社は 30만명의 안구 스캔 Data로 심혈관 질환 진단 등의 분석 및 컨설팅 사업을 수행한다.[4] 또한 중국의 경우 알리바바·텐센트 등 2천개의 기업이 참여한 데이터 유통 플랫폼 ‘GBDEX’를 통해 공공·민간 데이터 중개와 거래 및 가공, 가치평가 서비스 등의 새로운 데이터 거래 시장을 열었다.[5]

빠르게 성장하는 글로벌 빅데이터 시장에 비해 ICT 강국인 한국의 경우, 국내 활용도는 사실상 Zero에 가까운 상황이다. 다행히, 2018년부터 빅데이터 관련 사업의 활성화를 위한 관련 3법(개인정보보호법, 정보통신망법, 신용정보법) 개정안의 발의 되었으며, 빅데이터의 활용·활성화·구축·도입의 규제혁신 과제가 발표되는 등 데이터 활용 기회가 열리기 시작하고 있다. 이중, 데이터 거래는 카드사에게 새로운 수익원 창출의 기회로 주목받고 있다. 고객의 실제 움직임과 다양한 상품·서비스에 대한 선호를 알 수 있는 카드 데이터는 제조, 유통, 통신, 타금융사 등 광범위한 산업분야의 기업들이 사용을 원하고 있다. 금융당국도 빅데이터 제공서비스를 운영할 수 있도록 ‘여전업 감독규정’을 개정하는 등 제도적 장치를 마련해 주었다.[6]

2016년 6월 정부의 “개인정보 비식별 조치 가이드라인” 발간 이후 민간·공공에서는 개인정보의 비식별화 후 여러 업종간의 데이터 결합을 통해 새로운 사업 모델을 발굴을 시도하고 있다. 이를 위해 각 기업에서는 보유하고 있는 고객 정보를 비식별한 후 데이터 거래소 등을 통해 제공하고, 필요한 데이터는 구매하여 이용하는 사례가 늘어나고 있다.[7] 정보유출의 위험성이 상존하는 데이터 거래에 있어 적정 수준의 비식별화는 가장 큰 과제이다. 비식별화는 데이터에서 개인을 식별할 수 있는 요소를 삭제하거나 대체하여, 개인을 알아볼 수 없도록 하는 조치이다.[8] 정부·고객의 입장에서 개인정보 보호는 데이터의 활용보다 중요한 가치이다. 때문에 비식별화의 수준이 부족하면 다른 정보와 결합하여 개인 식별이 가능해지는 잠재위험이 상존한다. 반면, 데이터를 활용하려는 기업의 입장에서 높은 수준의 비식별화를 적용하면 데이터의 변형에 따른 정확도가 떨어져 모형의 성능이 하락한다. 이에 따라, 데이터 기반의 분석 모형 성능과 개인정보 보호의 안정성 모두를 보장할 수 있는 최적의 비식별화 방법이 필요하게 되었다.

2. 연구의 목적

이 논문에서는 카드사가 보유한 금융데이터를 기반으로 비식별화가 분석모형 성능에 미치는 영향을 분석한다. 다음의 세 가지 주제를 고려하여 ‘금융데이터의 최적 비식별화 기준’을 찾고자 실험을 진행하였다.

- ① 정부 기관의 권고수준인 $k=3$ 비식별화를 적용했을 경우 모형 성능은 얼마나 하락하는가?
- ② 같은 비식별화 수준하에서 모형의 성능 하락을 최소화하는 비식별화 방법은 무엇인가?
- ③ 데이터 제공량과 비식별화 수준(k 값)에 따라 모형 성능에 미치는 영향은 어떻게 달라질 것인가?

먼저, 금융데이터 특성에 맞는 기반모형을 선정하는 방식과 k -익명성 기반의 비식별화 처리 방식을 제안한다. 이를 통해 비식별화에 따른 기반모형의 성능 하락을 확인하여, k -익명성을 만족하면서 기반 모형의 손실을 최소화 할 수 있는 방안을 제시한다. 실험한 결과 ‘준식별자별 범주화 레벨을 최소화하는 조합’을 선택했을 경우, 통계적 데이터 훼손율이 가장 낮은 조합을 선택했을 경우에 비해 F1-score 기준으로 모형의 성능하락폭이 1.04에서 0.27로 급격히 감소함을 확인하였다. 또한, k -익명성 수준(k -값)과 데이터량의 변화에 따른 기반 모형의 성능을 측정한 결과, 최소 15만건의 데이터셋을 확보해야 k -익명성 수준에 따른 성능하락폭을 줄이고 데이터 훼손에 따른 분석모형의 성능이 불안정해지는 것을 방지 할 수 있음을 알 수 있었다. 마지막으로, 모형 성능에 큰 영향을 미치는 변수에 대해 사전에 파악하고 해당 변수에 대해 최소한의 비식별화를 적용함으로써 모형 성능의 하락폭을 최대 50%에 가깝게 줄일 수 있었다. 이러한 사전 분석 과정을 우선 수행하는 것이 최소한의 하락폭을 찾기 위한 단계와 시간을 대폭 줄일 수 있는 방안이라는 것을 제안한다.

3. 논문의 구성

논문의 구성은 총 5장으로 되어 있으며, 주요 내용은 다음과 같다. 제1장은 연구 배경과 목적 및 연구 논문의 구성을 설명하였다. 제2장은 데이터 비식별화의 개념과 비식별화 방법의 하나인 k -익명성에 대한 기존 연구 그리고 데이터 효용성 기반의 비식별화 연구에 대해 살펴보았다. 제3장은 금융데이터 기반의 분석

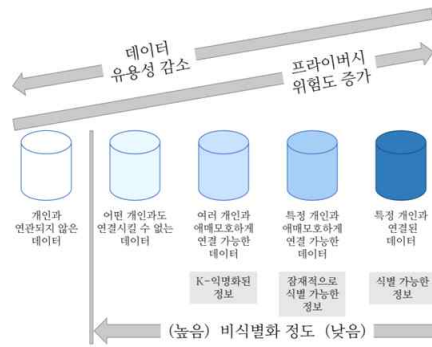
모형을 선정하는 방식과 비식별화 처리 방안을 제안한다. 제4장에서는 제안한 방식을 바탕으로 모형 성능을 측정하고, 최적의 비식별화 방안에 대해 제시한다. 마지막으로 5장에서는 이 논문의 결론을 정리하고 금융회사 입장에서의 기대 성과를 기술한다.

II. 이론적 배경 및 관련 연구

1. 비식별화 기법

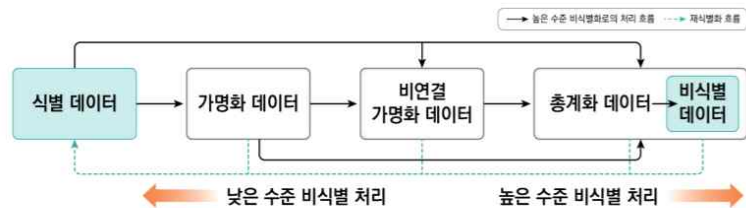
데이터 비식별화의 정의는 Data Set에서 개인을 식별할 수 있는 요소를 삭제하거나 대체하여, 개인을 알아볼 수 없도록 하는 조치이다. 직접 또는 간접적인 방법으로도 식별이 되지 않도록 해야 한다. 여기서 간접적 방법이란 ‘식별정보’를 제거하더라도, ‘다른정보’와 결합하면 개인을 알아볼 수 없도록 조치해야 함을 의미한다. ‘식별정보’는 그 자체만으로 개인을 식별할 수 있는 이름, 주민번호 등과 같은 식별자를 지칭한다. ‘다른정보’는 결합을 통해 간접적으로 개인을 식별할 수 있는 회사, 나이, 주소 등 준식별자를 말한다.

미국 상무부 산하의 표준화 기구인 NIST가 2015년 10월 발간한 “개인 식별정보의 비식별 처리” 가이드에서는 특정인과 정보 간 연결 가능성 등 비식별화 데이터 유형에 따라 프라이버시 침해 위험성의 정도를 표현하는 개념을 제시하였다. 비식별화 정도가 높을수록 데이터의 유용성은 떨어지지만 프라이버시 침해 위험도는 낮아진다. 특히, 데이터 비식별화를 위한 방법으로 삭제, 마스킹 등의 다양한 방법들을 설명하였고, 비식별화는 단일한 기법만 존재하는 것이 아니라 개별적인 활용 목적이나 상황에 따라 다양한 비식별 처리 기법이 수행될 수 있음을 제시하였다. [9][10]



〈그림 2, 비식별화 수준에 따른 데이터 유용성과 프라이버시 위험도〉

빅데이터 분석에 요구되는 데이터의 형태는 데이터의 사용 목적 및 처리 방법 등에 따라 정의된다. 데이터의 구성을 위해서는 개인을 식별할 수 있는 정보, 개인을 식별하는데 활용될 수 있는 속성이 포함되어야 한다. <그림 3>에서와 같이 ‘식별 데이터 형태’는 비식별 처리가 수행됨에 따라 점차적으로 가장 높은 수준인 ‘비식별 데이터 형태’로 변환되는 것을 알 수 있다. [9]



(출처 : ITU-T draft Recommendation X.fdp(2017.3))

〈그림 3, 데이터 처리과정의 데이터 형태와 비식별 수준〉

비식별화의 적정성을 평가하는 방법은 ‘k-익명성(k-Anonymity)’, ‘1-다양성(diversity)’, ‘t-근접성(t-closeness)’가 가장 널리 쓰이고 있다. 이 논문에서는 프라이버시 보호를 위한 기본 모델이며, 개념이해가 가장 쉬운 k-익명성을 비식별화 평가 척도로 선정하였다. k-익명성은 식별 정보를 제거한 후, 준식별자가

같은 사람이 최소 k명 이상이 되도록 하는 것이다. 예를 들어, ‘신한카드 전략 기획팀에 다니는 36세 과장은 대출이 많다’라는 간접적 정보를 기반으로 김신한(1-익명성)을 유추할 수가 있다. 이 정보에서 식별정보인 나이를 변형하여 ‘신한카드 전략기획팀에 다니는 30대 과장은 대출이 많다’로 비식별화 하면 김신한, 오전산, 박전략 3명으로 3-익명성 처리가 되는 것이다. 한국과 미국에서는 최소 3-익명성(k=3) 이상을 만족할 것을 권고하고 있다. k값을 높이는 기법에는 가명처리(Pseudonymization), 총계처리(Aggregation), 데이터 삭제(Data Reduction), 데이터 범주화(Data Suppression), 데이터 마스킹(Data Masking) 등이 있다.[11]

가장 많이 쓰이는 비식별화 방식은 ‘데이터 범주화’이다. 데이터 범주화는 머신러닝 적용이 용이하고 데이터 Domain 지식 기반으로 최적의 범주화가 가능하다는 장점이 있다. 데이터 범주화란 준식별자의 속성값을 더 큰 범위 값으로 수정하여 해당 속성 값을 지니는 레코드들이 여러 개 존재하도록 만드는 것이다. 범주화의 Level이 올라갈수록 정보의 양이 줄어들어 다른 정보와 결합해도 개인을 식별할 수 없게 된다.



〈그림 4, 준식별자 ‘직장정보’의 범주화 예시〉

2. k-익명성 기법

Sweeney와 Samarati는 ‘식별정보’를 제거하더라도 ‘다른정보’를 이용하여 고객 정보 노출이 가능하다는 것을 증명하였으며 이 문제를 해결하기 위해 k-익명성 개념을 제안하였다.[12] k-익명성은 데이터 집합에서의 각 기록들이 적어도 k-1개의 다른 기록들과 구별되지 않도록 데이터를 변형하여 프라이버시를 보호하는 기법이다. 신윤경은 k-익명성 알고리즘 관련 측도 연구에서 k-익명성의 필

요성에 대해 다음과 같이 정의하였다. k의 값이 커질수록 개인이 식별될 확률은 1/k를 넘지 못하게 되어 개인정보의 노출 위험(disclosure risk)이 줄어들지만 데이터의 이용 가치를 말하는 데이터 유용성(data utility)이 변화하게 되는 단점이 생긴다. 따라서 개인정보의 노출 위험을 최소화하고 데이터 유용성을 최대화하는 것이 데이터 변형의 궁극적인 목표라고 할 수 있다.[13]

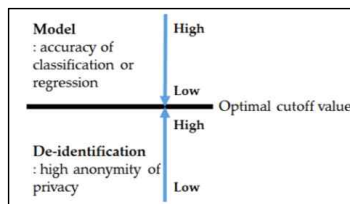
Roberto J 등은 Optimal k-익명성 방식을 제안함으로써, Sweeney/Samarati가 제안한 k-익명성의 Datafly, MinGen, AllMin 알고리즘과 달리 비용(cost)이라는 측도를 사용하여 최적의 k-익명화를 찾는 실험 결과가 유의미함을 보여주었다.[14] k-익명성을 적용한 비식별화 연구는 의료 데이터 기반으로 많은 연구가 진행되었다. Florian Kohlmayer 등은 최적 k-익명성 알고리즘 6개를 이용하여 공개된 의료 데이터셋 5가지를 대상으로 성능테스트를 수행하여 각 알고리즘별 효율성을 측정하였다.[15]

3. 비식별화 최적화 기법

김승환 등은 최적 절단값을 이용한 비식별화 방안을 제시하였다. k-익명성을 만족할 경우 발생하는 정보손실을 엔트로피(entropy)변화로 측정하였다. 준식별자에 대한 범주화 변환을 수행한 후 다음의 식을 적용하여 엔트로피를 계산하였다. 여기서 P_i 는 i번째 범주의 상대빈도(확률)을 나타낸다.

$$entropy(S) = \sum_{i=1}^C -p_i \log(p_i)$$

그리하여 정보손실이 커지면 예측 모형 정확도가 감소한다는 것을 확인하였다. 그러나 정보손실이 실제 통계적 모형 정확도에 어느 정도 영향을 주는지 사전에 알 수 없어, 비식별화 처리와 정보손실 간의 최적 관계를 찾기 위해 절단값(cutoff value)를 구하는 방식을 제안하였다.



<그림 5, 최적 절단값을 이용한 비식별화>

<그림 5>과 같이 개인정보의 익명성과 모형의 성능이 서로 반비례함으로 빅데이터 플랫폼의 사용자가 비식별화 과정에서 준식별자의 중요도에 따라 익명성의 수준을 조정하는 방법 등을 제안하고 <테이블 1>과 같이 준식별자의 범주화 변환에 의한 예측 정확도 감소량을 증명하였다.[16]

Transformation	Prediction accuracy	Reduced accuracy
Sex	85.96%	0.00%
Age(5 years old)	85.99%	-0.03%
Age(10 years old)	85.84%	0.12%
Work class	85.94%	0.02%
Marital status 1	85.96%	0.00%
Marital status 2	85.64%	0.31%
Convert all (5 years old, marital status 1) 5-anonymity(×)	86.19%	-0.23%
Convert all (10 years old, marital status 2)	85.55%	0.41%
Convert all (5 years old, marital status 1) 5-anonymity(O)	93.04%	-7.08%

<테이블 1, 변환에 의한 예측 정확도 감소량>

황치광 등은 서비스 기반의 익명화 기법을 연구하였다. 서비스에 활용될 속성은 낮은 수준의 익명화를 수행하여 실제 사용될 정보의 유용성을 높이고, 그와 함께 연결 공격을 방지하여 하나의 원본 데이터 테이블에서 둘 이상의 익명화된 테이블을 동시에 제공할 수 있는 익명화 기법을 제안하였다. 동일한 데이터 테이블을 이용하여 서비스 A ‘연령별 대표 질병’과 서비스 B ‘소득별 의료이용의 형평성’이라는 각각의 서비스 목적에 맞게 준식별자의 익명화를 다르게 적용하여 데이터의 정보 손실량이 증가하는 것을 억제하였다. [17]

III. 금융데이터 분석모형 선정 및 비식별화 방식 제안

1. 기존 연구의 문제점

기존의 데이터 익명화 관련 기술과 연구는 정보보호 관점에서 개인의 프라이버시를 얼마만큼 지킬 수 있느냐에 초점이 맞춰져 있었다. 또한 관련 실험에 의료 정보 데이터가 많이 활용되다 보니 금융산업의 특성에 맞는 최적의 비식별화 방식을 선정하기 어려웠다. 기존 연구에서 제안된 비식별화 방식이 금융사에서 보유한 빅데이터 분석 환경과 데이터셋 속성과 맞지 않아 연구결과를 현장에 바로 적용하기가 어렵다는 한계도 존재했었다.

최근 금융권은 빅데이터의 적극적 활용을 위해 자체 빅데이터 플랫폼을 보유하고 있으며, 각 사업영역에 따라 데이터 기반의 모형 개발이 매우 활발해지고 있다. 해당 플랫폼에서 개발된 모형이 비식별화된 데이터에서도 비슷하거나 최소한의 성능 하락으로 이용되어야 타 업종의 기업에 데이터와 모형제공이 가능할 수 있다.

때문에 이 연구에서는 금융회사의 빅데이터 플랫폼에 맞는 환경과 모형개발에 사용되는 보편적인 알고리즘을 기반으로 하여 최적의 분석 모형을 선정하는 방안을 먼저 제안한다. 또한 분석 모형에 사용되는 금융 데이터셋의 준식별자 선정과 최적의 비식별화 방식을 제안하여 비식별화된 데이터를 사용하더라도 성능 하락은 최소화 시킬 수 있는 방안을 제시한다.

2. 금융데이터의 분석모형 선정 방식

먼저 기반 모형의 조건은 다음과 같다. 이 연구에 적합한 기반 모형에는 과거 결과데이터로 학습한 후 모형을 생성하는데 적합한 Supervised Learning인 Logistic Regression, Decision Tree, Random Forest 3개를 사용한다. 또한 데이터셋에는 인구통계학적 속성값과 금융거래 정보가 포함되어 있어야 한다.

최적의 분석모형 선정을 위해 다음의 방식을 제안한다. 데이터셋을 예측 모형의 가장 기본적인 알고리즘인 Logistic Regression에 적용하고, 산출한 모형의 성능을 바탕으로 다른 알고리즘의 성능을 측정할 기준을 산정한다. 모형의 성능 측정에는 Precision과 Recall 그리고 이 둘의 조화 평균값인 F1-score를 주요 지표로 사용한다. 또한 보조 지표로 데이터의 분포가 심하게 불균형할 때 사용되는 AUPRC를 추가하여 측정 및 비교한다.

F1-Score 등으로는 최적의 기반 모형 선정을 위한 정밀한 측정에 한계가 있다. 이를 해결하기 위해 알고리즘별 예측 모형의 Score와 실제 가입 확률을 비교하는 방안을 제시한다. <그림 6>과 같이 각 모델별 고객 Segment의 Score값을 산출하면 머신러닝 모형의 성능을 상세하게 측정 할 수 있다. 고객별 Score를 산출하기 위해 아래와 같은 처리단계를 수행한다.

1) Training Set을 통해 3개 모델별로

고객별 예측 Score 산출 :

100점(가입) ~ 0점(거절)

2) 고객별 Segment를 구분하기 위해

10점 단위로 Grouping

3) Test Set으로 실제 가입 확률 산출

및 정확성 검증

4) Lift 값을 추가 산출하여 해석

※ Lift 값 : 평균반응률(12%=1) 대비

주어진 집단(Group)에서의 반응률

ex) Lift = 2이면 평균 대비 2배 (반응률 24%)

1	Score	3	4	5
2	가입확률	LIFT	인원수	
90점대	0.843070	5.053646	7857.0	
80점대	0.556194	3.334016	4698.0	
70점대	0.384316	2.303723	4374.0	
60점대	0.266328	1.596459	5114.0	
50점대	0.192945	1.156580	5670.0	
40점대	0.136588	0.818754	5674.0	
30점대	0.102133	0.612218	5111.0	
20점대	0.063432	0.380232	3689.0	
10점대	0.049912	0.299192	1142.0	
0점대	0.001114	0.006679	46670.0	

<그림 6. 고객 Score별 측정예시>

5) 점수대별 인원수 매칭 : 실제 TM 에서의 활용도 검증

3. 준식별자 선정 및 비식별수준 검증

데이터셋의 변수 중 어떤 변수를 비식별화 하여 익명성 값을 높일 것인지 결정하는 것은 매우 중요한 사항이다. 이 연구에서는 다음의 2가지 기준에 따라 준식별자 및 비식별화 대상을 선정하였다. 첫째, 정부기관인 한국정보화진흥원의 ‘개인정보 비식별화에 대한 적정성 자율평가 안내서’에 따라 식별자·준식별자 기준을 적용한다. 둘째, 변수의 비식별화를 위한 Level Depth를 고려하였다. Level Depth가 깊어서, 보다 많은 경우의 수로 비식별화 할 수 있는 항목을 준식별자 대상으로 우선하여 적용한다. 선정된 준식별자는 범주화 기법을 사용하여 각 준식별자에 대한 비식별화를 진행한다.

비식별 수준은 정부기관에서 권고하는 최소 수준인 3-익명성을 기준으로 선정하였다. 3-익명성을 만족하는 비식별자간 범주화 Level 조합을 도출하기 위해 ARX Data Anonymization (익명화) 프로그램을 이용한다. [18]

4. 분석 모형의 성능하락을 최소화한 비식별 방안

분석 모형의 성능하락을 최소화 하기 위한 비식별 방안은 다음과 같다.

첫째, 준식별자별 범주화 레벨을 최소화하는 조합을 선택한다. 예를 들어 4개의 준식별자가 있고 각 준식별자의 범주화 Level Depth가 3이라고 가정하면, 발생 가능한 준식별자 조합의 최대 갯수는 $3^4 = 81$ 개가 존재한다. 각 준식별자의 최소 범주화 레벨인 (1,1,1,1)이 데이터 속성의 특징 손실을 최소 할 수 있기 때문에 특정 준식별자의 범주화 Level Depth를 최대한 높여서 k-익명성을 만족하는 것 보다 모형 성능 하락폭을 최소화 시킬 수 있다.

둘째, 데이터셋의 규모를 일정 수준 이상으로 최대한 확대한다. 데이터셋의 규모가 클수록 동일한 k-익명성을 만족시키기 위한 데이터 범주화 레벨이 낮아지면서 분석 모형의 손실을 최소화 할 수 있다. 데이터 범주화 레벨이 낮아지면, 준식별자에 대한 데이터 손실률이 감소함으로써 분석모형의 성능을 어느 수준 이상으로 유지시킬 수 있다.

셋째, 모형 성능에 많은 영향을 미치는 변수를 사전에 파악하고 최소한의 비식별화를 적용한다. 이 방식을 적용하기 위해서는 데이터셋과 전반적인 도메인에 대한 경험이 풍부해야 한다. 일반적으로 모형 개발시, 변수들에 대한 상관관계를 분석하여, 특정 변수가 모형 성능에 일방적인 영향을 미치지 않도록 제외하거나 조정처리를 한다. 때문에 어떠한 변수가 해당 모형의 성능에 큰 영향을 주는지에 대해서는 데이터 분석가의 경험과 여러 차례에 걸친 실험을 통해 추정해야 한다.

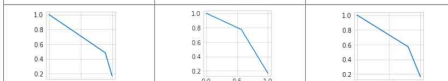
IV. 실험 및 결과

1. 실험 모형 및 데이터셋

이 연구에서는 ‘보험 상품 텔레마케팅 반응 예측’ 모형을 기반 모형으로 선정하였다. 해당 모형은 결과(Y)값이 0(실패) / 1(성공)로 나뉘어져 있어서 모형 성능 판단이 용이 하였으며 나이·소득·생애주기·지역 등 모형에 활용되는 변수 중 준식별자로 적합한 영역이 많다. 또한, 타 업종 상품을 판매할 때도 카드 Data가 유의미함을 보여줄 수 있으며, 향후 Data Sales에 용이하다는 장점을 가지고 있다. 데이터셋은 신한카드의 ‘18년 보험 상품 텔레마케팅 데이터를 기반으로 구성하였다. 보험 상품 가입에 영향을 미칠 것으로 예측되는 변수 23개를 선정하였다. 나이, 성별, 지역, 카드한도, 병원/온라인/화재 보험 이용 금액, 연소득, 라이프스타일, 신용/체크카드 회원여부, 론 회원여부, 탑스클럽 등급 등으로 구성되었다. 고객별 ‘18년 실제 마케팅 성공/실패 여부를 포함하여 성능 측정이 가능한 데이터셋을 작성하였다. 데이터셋은 총 30만건이며 마케팅 성공은 5만건, 실패는 25만건으로 마케팅 성공률 16.7%의 특징을 가지고 있다. 데이터셋의 Training, Test 분리는 7:3으로 하였다. 데이터셋 구성, 분석모형개발, 성능 측정은 신한카드 빅데이터 플랫폼에서 수행하였다.

2. 최적 기반 분석 모형 선정

3개의 Supervised Learning 알고리즘의 성능을 측정한 결과, <그림 7>과 같이 F1-Score/AUPRC 기준으로 Decision Tree, Random Forest 모형의 분석 성능이 우수한 것으로 확인되었다.

	Logistic Regression		Decision Tree		Random Forest	
	예측		예측		예측	
Confusion Matrix	실제 0	60646	실제 0	72506	실제 0	65865
	실제 1	1640	실제 1	6489	실제 1	2886
성능지표	Precision	0.4826	Precision	0.7747	Precision	0.5780
	Recall	0.8908	Recall	0.5678	Recall	0.8078
	F1-Score	0.6260	F1-Score	0.6653	F1-Score	0.6689
	AUPRC	0.6957	AUPRC	0.7073	AUPRC	0.7053
						

<그림 7, 비식별화 전, 알고리즘별 성능 측정결과>

보다 우수한 모형을 정확히 찾기 위한 알고리즘별 고객Score, Lift값, 인원수 매칭 측정결과는 <그림 8>과 같다. Logistic Regression은 Score 90점대 이후 가입확률이 급격히 낮아졌다. 또한 80점대 이하의 Over-fitting이 많이 된 모형으로 확인되었다. Decision Tree은 Score 90점대의 가입확률이 94.5%, 80점대가 81% 등 예측 Score와 가입확률이 잘 매칭된 정확한 모형으로 확인되었다. 다만, 0~10 점대 인원수가 많은 것이 다소 아쉬우나 이 부분은 타겟 마케팅에 이용하면 단점을 보완할 수 있을 것으로 보인다. 마지막으로 Random Forest는 점수대별로 인원수를 고르게 뽑아내어 다수 마케팅에 유리한 측면이 있다. 그러나 70점대 이하로는 Over-fitting이 심한 것으로 확인되었다. 예측 Score와 실제 가입확률의 정확도를 고려하여 이 연구에서는 Decision Tree 알고리즘을 모형의 성능 측정에 활용하기로 결정하였다.

Logistic Regression					Decision Tree					Random Forest				
Score	가입확률	LIFT	인원수		Score	가입확률	LIFT	인원수		Score	가입확률	LIFT	인원수	
90점대	0.843070	5.053646	7857.0		90점대	0.945702	5.668860	4328.0		90점대	0.932494	5.589686	4370.0	
80점대	0.556194	3.334016	4698.0		80점대	0.816678	4.895445	1451.0		80점대	0.708141	4.244837	4115.0	
70점대	0.384316	2.303723	4374.0		70점대	0.735661	4.409800	1203.0		70점대	0.551708	3.307123	4187.0	
60점대	0.266328	1.596459	5114.0		60점대	0.639160	3.831342	2048.0		60점대	0.392377	2.352039	4014.0	
50점대	0.192945	1.156580	5670.0		50점대	0.534378	3.203244	1978.0		50점대	0.274879	1.647720	4562.0	
40점대	0.136588	0.818754	5674.0		40점대	0.452292	2.711190	3469.0		40점대	0.185490	1.111888	6933.0	
30점대	0.102133	0.612218	5111.0		30점대	0.333333	1.998113	3516.0		30점대	0.136241	0.816672	7384.0	
20점대	0.063432	0.380232	3689.0		20점대	0.246531	1.477788	3675.0		20점대	0.079228	0.474917	5541.0	
10점대	0.049912	0.299192	1142.0		10점대	0.148829	0.892134	14352.0		10점대	0.046889	0.281069	2218.0	
0점대	0.001114	0.006679	46670.0		0점대	0.013005	0.077957	53979.0		0점대	0.001093	0.006550	46675.0	

<그림 8, 알고리즘별 Score, 가입확률, LIFT, 매칭인원수 결과>

3. 준식별자 선정과 비식별화 전후 비교

3.3의 준식별자 선정 기준에 의해 선정된 4개의 비식별자 변수는 <테이블 2>와 같이 ①나이, ②소득, ③생애주기(라이프스테이지), ④지역 이다. 비식별화를 위해 보험예측 모형의 변수 중 식별자인 고객번호, 우편번호(주소)는 삭제처리를 하였다. 데이터셋 9 ~ 23번 항목은 카드사 내부 생성 데이터로써 일반적으로 고객을 식별할 수 있는 항목으로 보기 어렵다. 비식별자인 나이, 소득, 생애주기, 지역은 <그림 9>와 같이 각각 범주화 기준을 정하였다.

NO	변수	가이드 기준	Level Depth	비 고
1	고객번호	식별자		삭제
2	우편번호 (주소)	식별자		삭제
3	신용한도	준식별자	3	분산/표준편차 불균형으로 제외
4	나이	준식별자	3	논문기준 선정
5	소득	준식별자	3	논문기준 선정
6	생애주기(라이프스테이지)	준식별자	2	논문기준 선정
7	지역	준식별자	3	논문기준 선정
8	성별	준식별자	1	Level Depth가 낮아 제외
9	병원이용액			
10	온라인이용액			
11	화재보험납부액			
12	인바운드상담가능구분코드			
13	신용카드회원여부			
14	체크카드회원여부			
15	카드론이용여부			
16	가맹점주고객타			
17	카드사Tops등급			
18	신한그룹Tops등급			
19	한부이용경과월			
20	현금서비스이용경과월			
21	카드론이용경과월			
22	신용카드발급경과월			
23	복지카드보유여부			

<테이블 2, 변수별 식별자, 준식별자 선정 결과>

① 나이

Level 3	19~83세 (전체)															
Level 2	19~50세								51~83세							
Level 1	19~34세				35~50세				51~66세				67~83세			
Level 0	19	19	34	35					51	83

② 소득

Level 3	전체							
Level 2	~4천만				4천만~			
Level 1	~2천만		2~4천만		4~6천만		6천만~	
Level 0	~1천만	1~2천만	2~3천만	3~4천만	4~5천만	5~6천만	6~7천만	7천만~

③ 생애주기 (라이프스테이지)

Level 2	1~7 (전체)						
Level 1	1~3		3~5		5~7		
Level 0	1	2	3	4	5	6	7

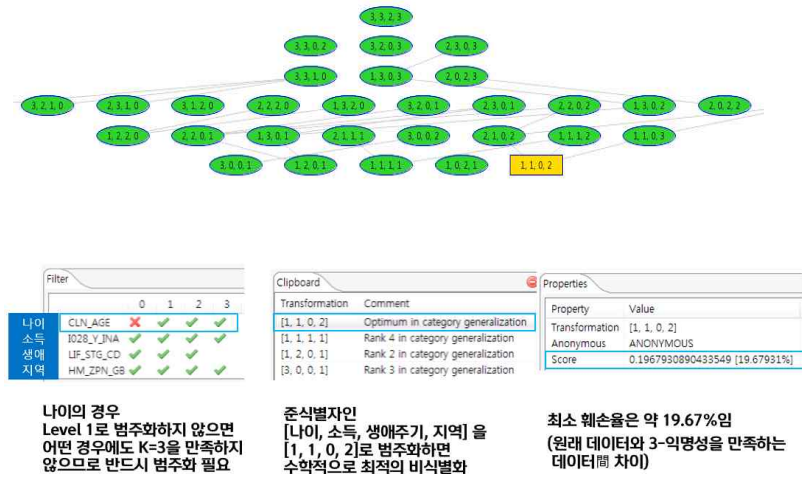
1. 미분류
2. 싱글
3. 신혼
4. 영유아어린이자녀가족
5. 청소년자녀가족
6. 성인자녀가족
7. 실버

④ 지역

Level 3	대한민국 (전체)															
Level 2	1~8위								9~17위							
Level 1	1~4위 (소득기준)				5~8위				9~12위				13~17위			
Level 0	서울	울산	세종	경기	대전	광주	전남

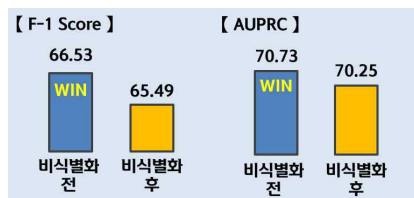
<그림 9, 준식별자 4개의 범주화 기준>

다음 단계로, ARX를 이용하여 3-익명성 만족 조합을 확인하기 위해 ARX에 데이터셋을 load한 후, 4개 비식별화에 대한 범주화 방식을 설정하고 k=3 익명성을 만족하는 준식별자의 조합을 측정하였다. ARX에서는 <그림 10>과 같이 데이터셋의 3-익명성을 만족하는 32가지 Case를 도출하였다.



<그림 10, k=3을 만족하는 준식별자의 Level 조합 Tree map와 해석>

ARX에서 계산된 데이터 훼손율이 가장 낮은 조합 [1,1,0,2]을 적용하여 비식별한 데이터를 기반모형인 Decision Tree에 적용한 결과 모형의 성능이 기존 대비 약 0.5~1% 하락하였다. 데이터 비식별화 처리 후, 예상했던 대로 일정 수준의 성능 하락은 발생하였다.



<그림 11, 비식별화 전후 모형 성능 비교>

4. 비식별화 성능 분석

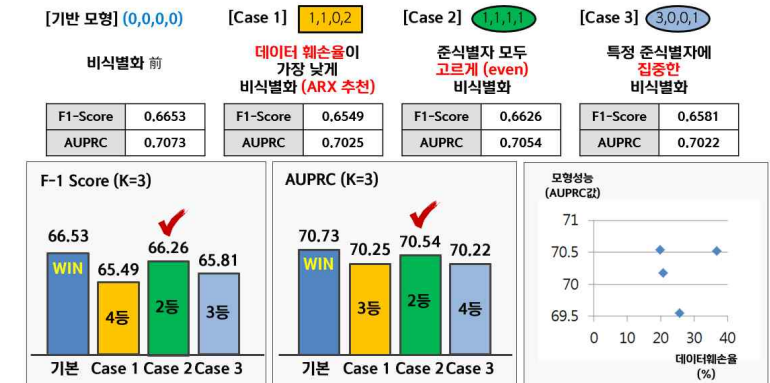
(1) 준식별자별 범주화 레벨을 최소화 적용

ARX에서 도출해준 3-익명성을 만족하는 32가지 Case 중 4개 준식별자 항목을 모두 고르게(even) 비식별화한 [1,1,1,1]과 특정 준식별자에 최고 Level을 적용함으로써 극단적 3-익명성을 만족한 [3,0,0,1] 조합에 대해 추가 성능 분석을 수행하였다.



<그림 12, 3-익명성을 만족하는 대표 3개 Case 선정>

3개 Case의 비식별화 후 성능 비교 결과는 <그림 13>과 같다.

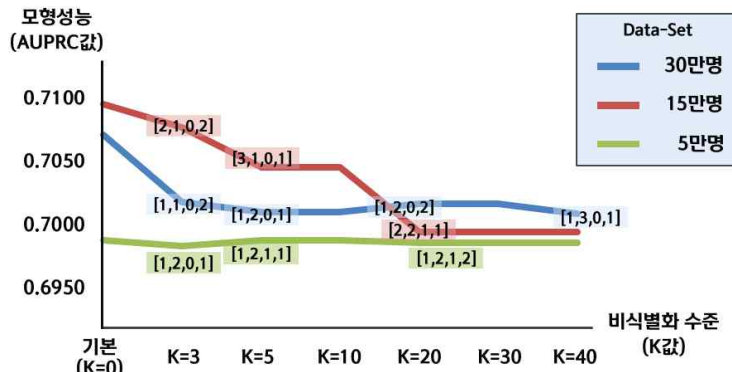


<그림 13, 대표 3개 Case의 비식별화 후 성능 결과 비교>

성능을 판단하는 2개 지표(F1-Score, AUPRC)를 기준으로 하였을 때, 4개의 준식별자를 모두 낮도록 고르게(even) 비식별화 하는 Case 2가 가장 성능 하락폭이 작았다. 데이터 훼손율이 가장 낮은 Case 1로 비식별화를 진행하면 반복 분석 없이 바로 비식별화 Level 조합 기준을 적용하기 때문에 편리할 수 있다. 하지만 다른 Level 조합이 더 우수한 성능을 낼 수 있기 때문에, 무조건 훼손율 기반의 비식별화 Level 조합 선정은 지양하고 Domain 지식을 활용한 다양한 Case로 성능검점 과정을 거쳐야 한다. 이 실험을 통해 통계적 데이터 훼손율이 낮은 준식별자별 범주화 조합이 모형 성능의 하락을 최소화 하는 비식별화 조합이라고 단정 지을 수 없음을 확인하였다.

(2) 데이터셋의 규모를 일정 수준 이상으로 확대

데이터셋의 규모와 k-익명성의 요구수준에 따라 측정된 모형 성능변화는 다음과 같다. 단, K-값(0 ~ 40) X 데이터수량변화 (5만, 15만, 30만) X 비식별화 Level 조합 (약30case)을 모두 측정하기 위한 경우의 수는 약 3,600가지나 되기 때문에 측정 과정에 통일된 기준을 적용하기 위해 ARX에서 계산된 가장 낮은 데이터 훼손율의 비식별자 Level 조합을 측정 기준으로 선정하였다.



<그림 14, k-값 / 데이터 수량 변화에 따른 성능 비교>

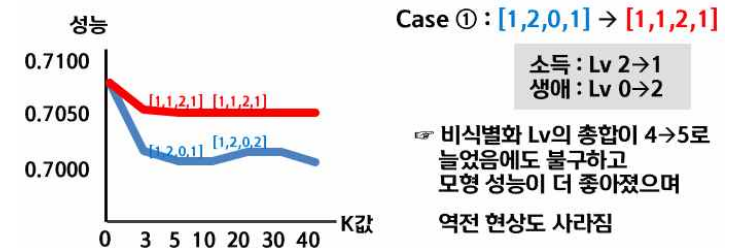
<그림 14>에서 볼 수 있듯이, 예상대로 k-값 증가(=강한 비식별화)에 따라 분석 모형의 성능은 전반적 우하향되고 있다. 특히, 15만, 30만 Data의 경우 k=40까지 비식별화 수준을 높였을 때 약 1% 가량의 성능하락이 발생하였다.

데이터의 규모가 가장 작은 5만 Data는 비식별화 前에도 성능이 낮고, k-값 증가시 오히려 성능이 오르는 역전현상도 나타남에 따라 5만건 정도의 Data는 비식별화 후 데이터로 사용하기엔 문제가 있는 것으로 확인되었다. 15만 Data의 모형성능이 30만 Data의 모형성능 보다 높게 나타난 이유는, 랜덤 Sampling으로 데이터셋을 생성하였으므로 어떤 고객의 Data가 수집 되었는지에 따라 소수점 단위의 차이가 발생한 것으로 추정된다. 30만 Data 모형에서 k=5보다 k=19에서 성능이 좋아지는 역전현상이 발생한 것은 훼손율 기반의 준식별자 범주화 레벨 조합 선정에 대한 한계점으로 보인다.

위 실험을 통해 데이터의 양이 일정 수준을 넘으면, k-값이 증가(비식별화 강화)되어도 성능 하락폭은 미미하고 데이터 규모가 클수록 k-값 증가가 성능 하락에 미치는 영향은 작다는 것을 확인할 수 있었다.

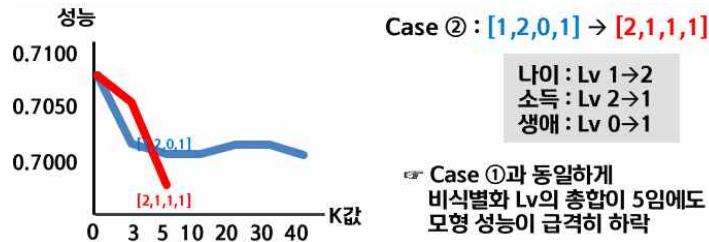
(3) 모형 성능에 많은 영향을 미치는 변수에 대한 최소한의 비식별화

훼손율 기반의 비식별화 기준선정의 한계를 재확인하기 위해, 준식별자의 비식별화 Level을 모두 고르게(even)하는 비식별화 조합을 재적용 후 모형의 성능을 측정하였다. 4개의 준식별자에 대한 Level을 고르게 할 수 있는 Level 조합은 [1,1,2,1] 과 [2,1,1,1]이며 각 조합별 성능 측정결과는 다음과 같다. Level 조합 [1,1,2,1] 적용 후 측정결과 비식별화 Level의 총합이 4에서 5로 증가하였음에도 불구하고 모형 성능이 더 좋아졌으며 역전현상도 사라졌다. 이는 ‘소득수준’ 변수에 대한 비식별화 레벨을 낮추고 ‘생애주기구분’ 변수를 높였을 때 발생한 것으로 보아, 이번 모형에는 ‘소득수준’ 변수가 ‘생애주기구분’ 보다 중요한 변수로써 작용 된다는 것을 추측할 수 있다.



<그림 15, 준식별자 level [1,1,2,1]로 변경, k값별 성능 비교 >

Level 조합 [2,1,1,1] 적용 후 측정된 결과, Case ①과 동일하게 비식별화 Level의 총합이 5임에도 모형 성능이 급격히 하락하였다. ‘나이’ 변수의 비식별화 Level을 1 증가 시키고, 나머지 2개 변수는 하양 조정 하였음에도 매우 큰 폭으로 성능이 하락하였다. 이는 ‘나이’ 변수의 정보가 다른 2개 변수에 비해 모형의 성능에 매우 중요한 요소임을 알 수 있다.



<그림 16, 주식별자 level [2,1,1,1]로 변경, k값별 성능 비교>

위 실험을 통해 ‘나이’, ‘소득’ 이 다른 주식별자에 비해 모형성능에 큰 영향을 미치고, 생애주는 성능에 유의미한 영향을 주지는 않았음을 발견하였다. 따라서 비식별화시 가능하면 ‘나이’, ‘소득’ 주식별자에 대한 비식별화 Level 수준을 최소한으로 낮추는 방식으로 비식별화 기준을 선정하는 것이 중요하다는 것을 알 수 있다. 데이터 도메인에 대한 지식과 경험이 있다면, 어떤 변수가 보다 중요한 요소인지를 사전에 파악할 수 있다. 이러한 사전 분석 과정과 경험은 불필요한 실험횟수를 감소시키고 보다 우수한 비식별화 방향성 도출을 가능하도록 한다.

V. 결론

이 연구에서는 금융회사의 데이터 거래 활성화를 위해 필요한 최적의 비식별화 방식을 제안하였다. 주식별자별 최소한의 범주화 레벨을 적용시키고 일정 수준 이상의 데이터셋 규모를 확보한다면 기존 데이터를 비식별화 하더라도 분석 모형의 성능 하락을 최소화 시킬 수 있음을 확인하였다.

일정 수준 이상의 데이터량을 초과하면, 비식별화된 데이터량과 모형성능에는 큰 상관관계 없다. 또한, k-값에 따라 모형성능이 비례(linear) 해서 감소하는 것이 아니라 특정 임계 수준에 도달할 때 마다 계단식으로 하락하는 것을 볼 수 있다. 연구 결과에 따라 금융기관이 외부에 비식별화된 데이터를 제공할 경우, 정부 가이드 라인 k=3 수준에서 15만건 이상의 데이터를 생성하면 안전한 비식별화 데이터와 함께 원본 데이터와의 유사한 수준의 모형 성능을 보장 할 수 있음을 확인하였다.

또한, 도메인 지식과 데이터셋의 속성별 특징에 대한 사전지식은 최적의 비식별화 방식을 찾는 데 큰 도움이 된다는 것을 정확한 수치를 통해 증명하였다. 영향도가 높은 주식별자를 사전에 파악하여, 해당 주식별자의 비식별화 Level을 최소화하고, 모형에 영향력이 낮은 주식별자 중심의 비식별화 수준을 강화하면서 익명성(k) 값을 높이는 것이 최적의 비식별화 방안이다.

비식별화된 데이터를 사용하면 분석 모형 성능의 하락은 명확하다. 그러나 소수점 단위 성능 하락(3-익명성 기준)이 금융 Data에 있어 Critical한 수준은 아니므로, 비즈니스 관점에서의 금융 데이터 거래 효용성에는 영향을 주지 않는다고 판단된다. 기존 연구에 주된 척도로 이용되는 통계적 데이터 훼손율이 모형성능 하락폭을 최소화 하는 기준이 아니라는 것을 확인하였다. 때문에 비식별화의 편의성만을 고려하여 통계적 데이터 훼손율이 가장 낮은 범주화 방식으로 일괄 비식별화 할 경우에는 최적의 성능을 보장할 수 없다.

향후 정부의 빅데이터 산업 활성화 정책에 따라 데이터 거래가 활발히 이루어지는 환경이 조성되면, 이 연구 결과가 고객 정보는 보호하고 분석 모형의 성능 하락 폭은 최소화하는 데에 도움이 되어 데이터 거래의 활성화에 기여 할 것이라 기대한다.

[참고문헌]

- [1] 한국IDC보고서, “국내 빅데이터 및 분석시장 전망, 2018-2022”, 14 Feb 2019, <https://www.idc.com/getdoc.jsp?containerId=prAP44864019>, 2019.05.01
- [2] 데이터 경제 활성화 규제혁신 현장 방문 행사, 대통령 연설문 (2018.8.31)
- [3] 스위스 국제경영개발대학원(IMD), 2018년 세계 디지털경쟁력 순위 보고서(IMD WORLD DIGITAL COMPETITIVENESS RANKING 2018)
- [4] The Verge news article, 'Google' s new AI algorithm predicts heart disease by looking at your eyes', James Vincent, Feb 19, 2018
- [5] 박소영, 장현숙, “빅데이터 거래의 한중 비교 : 기업 활용을 중심으로”, 한국 무역협회, Trace Focus 2018년 16호,
- [6] 금융위원회, 금융감독원, 「카드산업 경쟁력 제고 및 고비용 영업구조 개선방안」, 카드사가 업무관련 취득정보(빅데이터)를 분석·제공·자문할 수 있도록 ‘여전업 감독규정’ 개정 (2019.4.9.)
- [7] 우순규, “금융산업에서 빅데이터 기반의 개인정보 비식별 조치에 영향을 미치는 요인에 관한 연구”, 박사학위논문, 숭실대학교, 2018.
- [8] 행정자치부·한국정보화진흥원, “개인정보 비식별화에 대한 적정성 자율평가 안내서”, 2014.12
- [9] 임형진, “빅데이터 환경에서의 개인정보 비식별 처리 방법 분석”. 전자금융과 금융보안 제8호, 11-37, 2017.
- [10] S. Garfinkel, “De-Identification of Personal Information,” NISTIR, 8053, 2015.
- [11] 김종선, 이혁기, 정기정, 정연돈 공저, “데이터 익명화”, 휴먼싸이언스, 2019
- [12] Latanya Sweeney “k-anonymity : A model for protection privacy,” International Journal of Uncertainty, Fuzziness and Knowledge-based systems, pp. 557-570, 2002.
- [13] 신윤경, “K-익명성 알고리즘 관련 측도들에 대한 연구”, 석사학위논문, 국민대학교. 2008.
- [14] Robert J. Bayardo, Rakesh. Agrawal, “Data Privacy through Optimal k-Anonymization,” icde, pp. 217-228, 21st International Conference on Data Engineering (ICDE'05), 2005.
- [15] Florian Kohlmayer, Fabian Prasser, Claudia Eckert, Alfons Kemper, Klaus A.

Kuhn, Highly Efficient Optimal K-Anonymity For Biomedical Datasets, 2012, IEEE.

- [16] 전승환, 전성해, “데이터 비식별화를 이용한 빅데이터 통합”, Journal of Korean Institute of Intelligent Systems Vol.29, No. 3, June 2019, pp.235-241.
- [17] 황치광, 최종원, 홍충선, “데이터 유용성 향상을 위한 서비스 기반의 안전한 익명화 기법 연구”, Journal of KIISE, Vol. 42, No. 5, pp. 681-689, 2015.5
- [18] <http://arx.deidentifier.org>

인슈어테크 산업 발전을 위한 규범 혁신 제안

- 방법론 및 해결 방안을 중심으로 -

김영석* · 김영우**

* 중앙대학교 법학전문대학원 법학전공

** 서강대학교 법학전문대학원 법학전공

요 약

보험산업에서는 전통적으로 정보 비대칭으로 인한 도덕적 해이와 역선택, 그리고 보험 사각지대라는 문제가 발생해왔다. 이를 해결하기 위해 기존에도 이미 여러 시도가 이루어져왔지만, 최근 인슈어테크(InsureTech)는 관련 문제를 해결하기 위한 가장 획기적인 방안으로 주목받고 있다. 실제로 미국, 영국, 중국 등 주요 선진국에서는 규제 완화 혹은 공격적인 지원정책을 통해 인슈어테크 산업을 육성하고 있다. 이를 통해 소비자, 보험사, 정부의 효용 및 사회후생은 증진할 것으로 기대된다.

각종의 4차 산업 혁명 기술은 인슈어테크의 핵심을 이루며, 획기적인 효율화 혹은 패러다임의 전환을 주도한다. 사물인터넷(IoT)을 통한 건강증진 프로그램은 정보 비대칭을 해소할 뿐만 아니라 위험 자체를 줄이는데에 유용한 도구이다. 인공지능(Artificial Intelligence)은 보험사의 비용을 대폭 절감하고, 보다 적합한 서비스 제공을 가능케 한다. 빅데이터(Big Data)를 통한 위험 분석으로 새로운 시장의 개척과 효율적인 상품 개발이 이루어진다. 블록체인(Blockchain)을 통해 보안에 안전을 기하면서 보험금 청구 절차도 간소화할 수 있다. 또한 P2P 보험이 정보 비대칭의 문제를 구조적으로 해소할 수 있는 대안으로 제시되고 있다.

이러한 신기술을 활용하고, 이를 활용한 신상품을 개발에 있어서 법적 근거를 마련하는 것은 필수적이다. 하지만 보험업법을 포함한 우리나라의 관련 법제는 아직 인슈어테크 도입에 소극적인 것으로 보인다. 본 연구는 국내 인슈어테크 활용을 촉진하기 위해 기존의 연구를 종합하여, 방법론적 관점과 실체적 관점에서 구체적인 해결 방안을 제시하였다. 이는 입법기관 및 정부가 본 연구를 참고하여 입법적·정책적 판단을 내리는 것을 실질적으로 돕기 위함이다.

키워드

인슈어테크, 규제 샌드박스, 사물인터넷, 인공지능, 빅데이터, 블록체인, P2P 보험

목 차

I. 서론	3
II. 인슈어테크의 의의 및 현황	4
1. 종래 보험산업의 특성과 한계	4
2. 인슈어테크의 의의 및 가치	8
3. 주요국 인슈어테크 산업 동향	10
4. 인슈어테크 산업을 둘러싼 국내 주체들의 입장	15
5. 소결: 국내 인슈어테크 활용에 관한 법적 문제	17
III. 국내 인슈어테크에 관한 법적 문제를 해결하기 위한 방법론	18
1. 법령의 제정·개정의 선택과 특별법 문제	18
2. 기존 법령 개정	19
3. 특별법 제정	20
4. 규제 샌드박스(Regulatory Sandbox)	22
5. 인슈어테크 활성화를 위한 입법 방안	26
IV. 국내 인슈어테크 활용에 관한 법적 쟁점 및 개정 방안	26
1. 국내 인슈어테크 활용에 관한 주요 법적 쟁점 개관	26
2. 사물인터넷(IoT) 기반의 건강증진 프로그램을 통한 보험료 할인	27
3. AI(Artificial Intelligence)를 활용한 보험모집 및 업무 자동화	33
4. 빅데이터를 활용한 위험 분석	37
5. 블록체인을 활용한 보험금 청구 간소화 및 모바일 증권 진위 판별 ..	43
6. P2P 보험의 도입	46
V. 결론	49

I. 서론

보험은 위험을 회피하려는 인간의 욕구를 동종·다수의 위험을 결합하는 방식으로 실현한, 그 자체로 혁신적인 발명품이다.¹⁾ 보험은 인간 생활상의 위험을 획기적으로 제거하고 감소하는 데에 기여해왔지만, 정보 비대칭(Information Asymmetry)으로 인한 도덕적 해이(Moral Hazard), 역선택(Adverse Selection), 그리고 보험 사각지대라는 한계점을 갖고 있어 보험산업의 완전한 효율화는 요원해 보였다.

하지만 최근 핀테크(FinTech)를 필두로 금융 분야에 신기술을 도입하여 소비자의 편의를 증진하고 기업의 비용을 절감하려는 움직임이 일고 있다.²⁾ 금융 분야 중에서도 특히 보수적인 보험 분야에서도 인슈어테크(InsureTech)라는 명칭으로 각종의 ICT 기술 활용이 모색되고 있다. 전 세계적으로 사물인터넷(IoT), 인공지능(Artificial Intelligence), 빅데이터(Big Data), 블록체인(Blockchain) 등의 4차 산업 혁명 기술을 활용하여 기존 보험산업의 한계를 극복하려는 시도가 이루어지고 있다.³⁾

그러나 우리나라의 경우 아직까지 인슈어테크를 실제 보험산업에 적극적으로 활용하기에 어려움이 많다. 기술의 실효성이 파악되더라도 실제 이를 사업에 활용하는 것은 또 다른 문제이다. 신기술에 친화적이지 않은 촘촘한 규제는 다른 국가 대비 우리나라에서의 인슈어테크 발전을 가로막는 장애물로 여겨진다. 본 연구에서는 기존 보험산업의 한계를 극복할 인슈어테크 산업의 발전이 원활히 이루어질 수 있도록 관련된 법적 문제를 해결하기 위한 방법을 구체적으로 제시하고자 한다.

본 논문은 인슈어테크 산업 발전을 위한 규범 혁신의 방향을 제안하는 것을 목적으로 한다. 본 논문의 II장에서 보험의 한계를 극복하기 위한 인슈어테크의 의의 및 각국 인슈어테크 산업 현황을 파악하고 관련 주체들의 이해관계를 서술하여 논의의 필요성을 확인한다. III장에서 국내 인슈어테크 활용에 관한 법적 문제를 해결하기 위한 방법론으로 기존 법령 개정, 특별법 제정, 규제 샌드박스 등의 방법을 소개한다. IV장에서 국내 인슈어테크 활용에 관한 주요 법적 쟁점을 검토하고 전술한 방법론을 활용하여 해결 방안을 제시한다. 마지막으로 V장에서 이상의 연구를 종합하여 향후 국내 인슈어테크 규범 혁신의 방향과 관련 주체들의 자세를 제안한다.

1) Howard C. Kunreuther, “보험과 행동 경제학”, 제1판, 박영사, pp.22, 2018.

2) 신혜란, “한국 ICT기업의 금융업 진출 (핀테크) 발전방안 연구: 미국 중국과의 대표 사례 비교분석을 중심으로”, 석사, 성균관대학교 일반대학원, 서울, 2015

3) 전수용·안상진, “4차 산업혁명 기술경쟁력 분석 및 시사점: 사물인터넷을 중심으로”, KISTEP Issue Weekly pp.8. 한국과학기술기획평가원, 2018. 8.

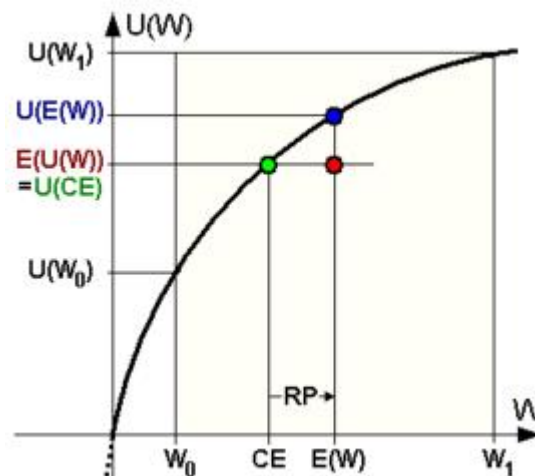
II. 인슈어테크의 의의 및 현황

1. 종래 보험산업의 특성과 한계

(1) 보험산업의 의의

보험(保險, Insurance)은 인간 생활상 필연적으로 발생할 수밖에 없는 여러 위험을 제거하거나 감소시키기 위해 고안된 시스템이다. 보험의 기본 원리는 위험을 스스로 감당하기 어려운 개인들이 모여 위험을 한데 결합하는 것이다.

<그림 1> Utility function of a risk-averse (risk-avoiding) individual⁴⁾



위험회피(Risk Averse) 성향을 가지는 보통의 사람의 경우, 보험료라는 일정한 비용을 지불하더라도 치명적인 위험을 막아주는 보험에 가입할 유인이 매우 높다.⁵⁾ 또한, 개인 수준에서 치명적인 위험이라 하더라도 이러한 위험을 한데 결합하여 관리하는 보험사 입장에서는 그리 치명적인 것이 아니다. 동종의 위험을 다수 결합하는 보험사는 개인이 자신의 위험을 온전히 감당하는 경우에 비해 기댓값의 분산을 확연히 줄일 수 있기 때문이다. 대수의 법칙과 포트폴리오 이론을 통하여 밝혀졌듯이, 보험 계약을 체결하는 표본의 수를 일정 수준까지 늘림으로써 체계적 위험을

4) Wikipedia, Risk aversion, [Internet], Available: https://en.wikipedia.org/wiki/Risk_aversion, 2019.08.30

5) 김철현·임용택, “위험회피와 보험수요에 관한 연구”, 산업경제연구 pp.224. 한국산업경제학회, 2003. 6.

제외한 비체계적 위험은 거의 0에 수렴하도록 할 수 있다.

이러한 보험 시스템의 경제학적 가치로 인해, 위험을 회피하려는 개인과 그들의 위험을 결합하여 이익을 추구하려는 보험사의 이해관계는 일치했고 보험산업은 큰 발전을 이룩할 수 있었다. 특히 최근에는 해상, 화재, 생명, 자동차보험 등 전통적인 보험 분야를 넘어서 여행자 보험 상품이 개발되는 등 보험이 다루는 영역이 어느 때보다 넓어진 상태이다. 물론 그만큼 경쟁도 치열해졌다. 또한, 사보험 뿐만 아니라 국민연금과 건강보험 등 공적 보험의 영역도 한층 넓어진 것이 현대 보험산업의 특징이다.

(2) 보험산업의 문제

종래 보험산업이 부흥할 수 있었던 원리가 ‘위험 회피(Risk Aversion)와 위험 결합(Risk Pooling)’ 이라면, 보험산업의 한계로 거론되었던 개념이 바로 ‘도덕적 해이(Moral Hazard)’ 와 ‘역선택(Adverse Selection)’ 이다.

보험산업에서 이야기하는 도덕적 해이에는 사전적 도덕적 해이와 사후적 도덕적 해이가 있다.⁶⁾

사전적 도덕적 해이란 보험 가입자가 위험 발생 시의 손해에 비하면 훨씬 적은 주의 비용을 들여 피할 수 있는 위험임에도 불구하고 사회 최적점 수준으로 충분히 주의하지 않아 위험을 발생시키는 것을 의미한다. 쉽게 말해 자동차보험에 가입한 운전자가 보험의 보장을 믿고 덜 주의하여 운전하는 것, 생명보험에 가입한 사람이 보험의 보장을 믿고 건강에 해로운 행위를 일삼는 것을 예로 들 수 있다. 이러한 행동은 개인적으로는 이익이 될 수 있을지언정 해당 보험에 가입한 다른 계약자들에게는 불필요한 손해를 끼치게 된다. 가장 큰 문제는 이러한 보험의 특성 자체가 필연적으로 이기적 개인의 사전적 도덕적 해이를 유도하게 되어 그 정도는 다르더라도 이러한 행태가 많은 보험 가입자들로부터 발생하게 된다는 것이다. 그리고 그로 인한 위험 발생의 증가는 만인의 사전적 도덕적 해이로 인한 만인에 대한 보험료 상승으로 고스란히 이어져 결국 충분히 주의하지 않은 본인들에게도 손해로 되돌아오게 된다. 보험 업계는 이러한 사전적 도덕적 해이를 막기 위하여 충분히 주의를 다하는 가입자에게 인센티브를 제공하는 방식을 취하는 등 여러 노력을 강구

6) 김광호, “실손형 의료보험에 대한 본인부담금 보장금지가 도덕적 해이에 미치는 영향”, 한국경제학보, Vol. 18, No. 2, pp.324-325. 연세대학교 경제연구소, 2011. 12.

하였으나, 보험업법상 특별이익 지급액에 한계가 존재하는 등의 이유로 인해 도덕적 해이가 보험산업에서 완전히 제거되는 데에는 무리가 있었다.⁷⁾

도덕적 해이에는 위험 발생 전 충분히 주의를 다하지 않아 발생하는 사전적 도덕적 해이가 있는가 하면, 사후적 도덕적 해이도 있다. 사후적 도덕적 해이란 위험 발생 후에 본인의 피해액을 확대하는 등 왜곡하거나 계약상 본인의 과실이 있음에도 불구하고 이를 숨기고 보험금을 타내는 이른바 보험사기를 말한다. 이 역시 보험사뿐만 아니라 선량한 다른 보험 가입자들에게 고스란히 피해를 끼치게 되므로 보험산업의 전통적인 문제로 거론되었다. 이를 해결하기 위해 보험사는 보험금 지급 심사 과정에서 여러 방법들을 고안하였으나, 이 역시 완전히 제거하기는 힘든 것이 현실이다. 특히 사후적 도덕적 해이의 경우 보험금을 지급하지 않으려는 보험사와 보험사기로 보험금을 지급받으려는 소비자 간에 소송으로 분쟁이 장기화되는 경우도 있고, 이러한 소송에서 보험사가 패소할 시에는 선량한 보험사와 보험 가입자들의 손해가 더욱 막대해진다는 문제가 있다.

또 한 가지의 문제는 역선택이다. 보험산업에서의 역선택이란 일반적으로 보험에 자발적으로 가입하는 사람들은 위험 발생 정도가 큰 사람일 가능성이 높다는 것이다.⁸⁾ 보험사가 예상되는 보험 가입자에 대한 평균을 내어 보험료를 산정할 때 이렇게 산출한 평균보다 위험한 사람이 주로 보험에 가입하고 평균보다 덜 위험한 사람은 보험에 덜 가입하게 되어 보험사의 손해가 예상보다 높아지게 된다. 극단적으로, 이러한 현상이 계속적으로 발생할 경우 결국 위험한 사람만이 남게 되어 보험을 통하여 위험을 효과적으로 제거할 수 없는 수준으로 가입자 규모가 줄어들 수 있고 결국 해당 보험 상품의 시장 자체가 소멸할 수 있다는 추측으로 귀결된다.

역선택은 위험도가 낮은 사람들을 높은 사람들과 구분해내지 못할 경우 위험도가 낮은 사람들이 위험을 효과적으로 회피할 수 없게 된다는 점에서 문제가 된다. 다시 말해 위험도가 높은 사람들이 보험에 가입하는 것이 문제가 아니라, 그들을 구분하여 위험의 정도에 맞게 보험료를 내도록 만드는 시스템을 구축하지 못할 경우 위험도가 낮은 사람들은 본인의 위험 정도에 비해 비효율적으로 과다한 보험료를 부담해야 된다는 것이 문제이다. 이에 보험사는 꼼꼼한 계약심사(Underwriting) 혹은 보험사 간의 정보 공유를 통해 역선택 문제를 어느 정도 보완하고 있지만 이 역시 완벽하게 제거하는 데에는 한계가 있었던 것이 사실이다.

7) 「보험업법」 제98조 제1호.

8) 노세진·하태욱, “자동차보험 시장에서의 역선택 현상에 관한 연구”, 경영교육저널 제13권, pp.42-43. 대한경영교육학회, 2008. 06.

정보 비대칭으로 특정 분야의 보험시장이 생성되지 못하여 이 분야 위험을 회피하고자 하는 소비자의 욕구가 좌절되고 보험사의 이익 창출 기회가 실현되지 못하는 이른바 ‘보험 사각지대’의 문제도 기존 보험산업의 한계로 꼽힌다. 현행 보험업법상 P2P 보험이 허용되지 않기 때문에, 보험사가 제공하는 보험 이외에 위험회피를 원하는 사람들끼리 자발적으로 보험을 결성하는 것은 현재 불가능한 상황이다.⁹⁾ 물론 보험에 관한 정보를 충분히 확보한 보험사가 주도적으로 보험 상품을 개발하는 것은 일반적이고 당연하게 보이지만, 온라인을 통한 정보 공유가 활성화되어 있고 이해관계가 일치하는 사용자들끼리 연결 가능한 인프라를 갖춘 최근에는 기존의 보험 개념을 벗어나 보험 가입자들끼리 자발적으로 형성하는 보험을 상정해 볼 수 있을 것이다. 종래의 보험산업은 주로 보험사가 개발한 상품에 국한되었고, 보험사가 개발하지 않은 상품에 관한 수요가 있는 소비자들이 자발적으로 자신의 위험을 보장하는 보험을 개발할 수 없었다. 위험을 회피하고자 하는 이들의 욕구가 좌절됨에 따라 잠재적인 사회 후생 증진의 기회가 가로막힌 측면이 있었다.

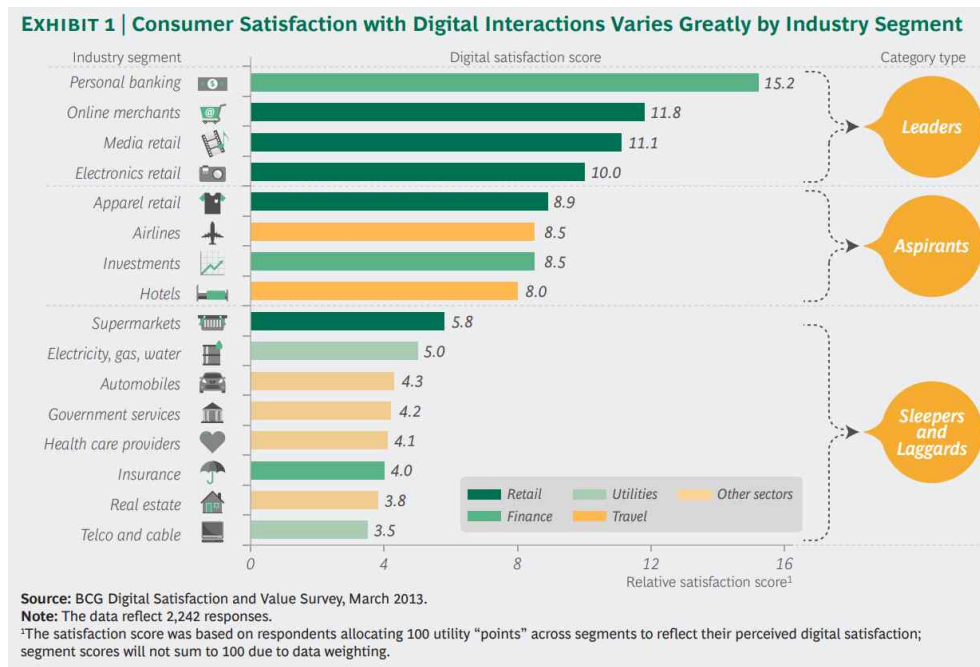
요컨대, 도덕적 해이와 역선택, 그리고 보험 사각지대의 문제는 정보 비대칭(Information Asymmetry)으로 인해 발생하는 보험의 맹점으로 보험산업을 비효율적으로 만든 주된 원인이었다. 또한 보험산업이 사회 구성원들의 위험회피에 상당 부분 기여하였음에도 불구하고, 위험을 더욱 줄이거나 혹은 거의 완벽하게 제거하는 수준에까지는 이르지 못하게 만든 원인이기도 하다.

나아가 보험금을 청구하는 과정에서의 절차적 복잡성도 종래 보험산업의 문제점으로 거론되었다. 아직까지도 대부분의 보험 상품에서 보험 가입자는 보험금을 청구하기 위해 오프라인으로든 온라인으로든 특정 서류를 손수 확보하여 보험사에 제출하여야 한다. 기술이 충분히 발전하였음에도 불구하고 가장 보수적인 금융 산업인 보험에서는 계약 체결에서부터 보험금 지급까지의 과정에서 아직도 전통적인 방식을 고수하고 있다. 이러한 보험산업의 보수성 때문에 2013년 BCG가 조사한 ‘온라인 소통 상대적 만족도’ 설문 자료에서는 보험업이 16개 산업 중 14위를 차지하기도 하였다.¹⁰⁾

9) 「보험업법」 제2조 제2항, 제4조 제1항.

10) BCG, Digital Satisfaction and Value Survey, [Internet], Available: http://image-src.bcg.com/Images/BCG_Delivering_Digital_Satisfaction_May_2013_tcm9-97767.pdf, 2019.08.30

〈그림 2〉 산업분야별 디지털 소통 상대적 만족도



2. 인슈어테크의 의의 및 가치

보험 소비자 입장에서 보험에 가입하는 목적은 위험의 감소 혹은 제거에 있다. 그러나 전술한 것처럼 보험이 이러한 목적을 충실히 수행하는 과정에 상당한 위험 요인들이 존재하는 것이 현실이다. 아울러 보험산업의 치열한 경쟁으로 인해 보험사들은 생존 자체에 위협을 받고 있기도 하다.¹¹⁾

이러한 상황에서 위험을 회피하고자 하는 소비자의 목적을 더욱 충실히 돕고, 치열한 보험산업 하에서 보험사의 새로운 활로를 모색해줄 개념이 대두되고 있다. 바로 인슈어테크(InsureTech)다. 인슈어테크란 보험(Insurance)과 기술(Technology)의 결합어로, 종래의 보험에 ICT 기반의 기술을 결합하는 것을 의미한다.¹²⁾ 4차 산업혁명 속에서 핀테크(FinTech)가 금융과 기술의 결합을 통해 시너지를 창출하는 개념으로 활용되었듯이, 금융 분야에서도 독보적이고도 고유한 위치를 차지하는 보험 분야에도 ICT 기술을 도입하려는 인슈어테크 움직임이 활발하다.

11) 정중영·김형도, “무한경쟁 시대의 손해보험산업 현황과 활로”, 대한경영학회지 제43호, pp.648-650. 대한경영학회, 2004. 04.

12) 김은석·김영준, “인슈어테크 디지털 보험플랫폼서비스의 사용자 수용의도에 관한 연구”, 경영학연구 제48권 제4호, pp.997. 한국경영학회, 2019. 08.

〈표 1〉 인슈어테크 이전과 인슈어테크 도입 후 기술의 비교¹³⁾

구분	인슈어테크 이전	인슈어테크
목적	기존 보험 서비스의 효율적인 개선	기존 금융기관을 우회하거나 기술을 통해 보험 생태계를 구축하여, 소비자의 금융서비스 수요 충족
주요기업	IBM, SAS와 같은 대형 IT기업	스타트업, 보험사
수익모델	기기판매, 라이선스 비용 등	기본적인 수익 이외 광고, 데이터 판매 등 다양한 수익기반 보유

인슈어테크는 다양한 기술을 보험산업의 니즈에 맞게 적용함으로써 보험소비자와 보험사 모두의 이익에 기여한다. 사물인터넷(IoT), 빅데이터(Big Data), 인공지능(AI), 블록체인(Blockchain) 등 4차 산업 혁명의 핵심이 되는 기술들을 적극 활용하여 보험 소비자의 목적 실현과 보험사의 이익 증대를 추구한다. 실제로 올해 5월 22일 금융감독원이 공개한 ‘보험회사 인슈어테크 활용 현황’을 보면 보험사들이 인슈어테크 도입을 위해 박차를 가하고 있음을 알 수 있다.¹⁴⁾

인슈어테크는 앞서 언급한 보험산업에서의 여러 한계점들을 해결하는 도구가 될 수 있다는 점에 가치가 있다. 정보 비대칭의 문제로 보험사가 겪었던 도덕적 해이와 역선택 문제는 인슈어테크를 통해 상당 부분 해결될 수 있다. 가령 사물인터넷을 통해서 보험 가입자가 스스로 위험을 줄이는 데에 동참하고 이를 보험사가 실시간으로 파악하는 것을 그 예로 들 수 있다. 이 경우 보험 가입자는 자신의 위험을 줄일 수 있게 되며, 보험사는 위험 감소로 인한 혜택을 누리고 이를 보험료 인하로 환원하여 궁극적으로 보험 가입자가 이익을 분배받을 수 있게 한다. 결과적으로 보험의 목적이 더욱 효과적으로 달성되고 보험사도 불필요한 비용을 줄일 수 있어 사회 후생이 증대된다. 빅데이터를 통한 위험 분석은 보다 효율적인 보험 설계를 가능케 하며, 정보 비대칭을 상당 부분 해소하여 도덕적 해이 및 역선택, 그리고 보험사각지대의 문제를 줄이는 데에 기여할 수 있다. 인공지능을 이용해 업무를 자동화한다면 보험사는 계약심사 과정에서 보다 효율적이고 정확한 판단을 내릴 수 있게 된다. 보험사의 합리적인 가격 책정은 당연히 보험사뿐만 아니라 보험 소비자들에게도 도움이 된다. 블록체인을 활용하여 보험금 청구 과정에서 절차적 복잡성을 줄이고, 보안 문제를 효과적으로 해결할 수 있게 된다. P2P 보험으로의 패러다임 전

13) 박소정·박지윤, “인슈어테크 혁명: 현황 점검 및 과제 고찰”, 보험연구원, pp. 29. 2017. 08.

14) 금융감독원, “보험회사 인슈어테크 활용 현황”, pp.1. 2019. 05.

환으로 전에 없던 보험 시장이 창출되어 보험 사각지대의 문제가 해소될 수 있다.

이처럼 인슈어테크는 금융 분야에서도 가장 보수적으로 여겨져 온 보험업의 작동 방식에 혁신을 가하여 보험 소비자와 보험사 모두의 이익을 추구하고 사회 후생에 기여한다. 나아가 혁신 과정에서 발생할 수 있는 여러 보안 문제에 대한 기술적 대응을 통해 더욱 안전하고 신뢰 가능한 보험 시스템을 구축할 수 있게 한다.

3. 주요국 인슈어테크 산업 동향

(1) 서설

최근 선진국의 정부와 기업들은 이미 그 효과성과 가치가 입증되고 있는 핀테크 만큼이나 인슈어테크 도입에도 적극적인 행동을 취하고 있다. 보험 분야는 사회적 안전과도 직결된 분야인만큼, 정부 차원에서도 인슈어테크를 지원할 당위성은 충분하다. 핀테크의 도입 과정에서 이미 실효성이 입증된 여러 기술들을 보험산업에 알맞게 적용하는 것만으로 충분한 효과를 누릴 수 있기 때문에 핀테크의 발전과 인슈어테크의 발전은 양립 불가분의 관계에 있다고도 볼 수 있다. 이 장에서는 미국, 영국, 중국 등 해외의 사례를 통해 인슈어테크 산업이 어떠한 양상으로 발전하고 있는지 살펴보고 이들 국가와 한국의 인슈어테크 산업 현황을 비교해본다.

(2) 미국

FT Partners(2016) 자료에 따르면, 전 세계 인슈어테크 자금 조달의 75%가 북미에서 이루어지고 있다.¹⁵⁾ 또한 같은 자료에 따르면, 인슈어테크 자금 조달 규모 상위 20개 기업 중 17개 기업이 미국 기업이다. 인슈어테크 발전의 중심지가 미국이라고 감히 평가할 수 있는 이유다. 특히 전술한 상위 17개 기업 중 14개 기업이 건강보험을 제공하는 기업으로 알려져 건강보험 분야에서 인슈어테크 도입이 활발해졌음을 알 수 있다.

미국은 네거티브(Negative) 규제와 비조치 의견서를 통해 인슈어테크 산업을 촉진하고 있다.¹⁶⁾ 네거티브 규제를 통해서는 명시적으로 금지한 사항 이외에는 원칙적

15) 박소정·박지윤, “인슈어테크 혁명: 현황 점검 및 과제 고찰”, 보험연구원, pp. 38. 2017. 08.

16) 배재광, “글로벌 핀테크 산업동향-미국편”, 한국인터넷진흥원, pp. 13. 2015. 05.

으로 전면 허용하는 방식을 취하고 있다. 또한 비조치 의견서를 통해 감독기관이 허용한 사업을 더 이상 징계하지 못하도록 하고 있는데, 이를 통해 합법적으로 혁신 사업을 진행할 수 있도록 보장한다. 이러한 일련의 제도가 규제로 인한 불확실성을 감소시키는 역할을 하여 인슈어테크 사업 성장에 기반이 되고 있다.

특히 미국 내에서 건강보험 분야의 인슈어테크를 촉진한 요인으로는 오바마케어 법 및 원격의료 규제 철폐, 개인의료정보보호 관련법 등이 꼽힌다.¹⁷⁾ 기존의 불필요한 규제를 완화하고, 새로운 산업이 발전하는 과정에서 발생할 것으로 예상되는 법적 쟁점에 관하여 선제적으로 규정함으로써 산업의 발전을 촉진하면서도 법적 안정성을 확보할 수 있었다.

한편 스타트업의 본산인 실리콘 벨리에서는 스타트업 인큐베이터인 플러그앤플레이(Plug and Play)에서는 인슈어테크 프로그램이 시행되고 있다.¹⁸⁾ 미국의 대표적인 인슈어테크 스타트업 레모네이드(Lemonade)는 인공지능 챗봇(Chatbot)인 마야(Maya)와 짐(Jim)을 통해 보험가입과 보험금 지급을 3분 내에 처리하는 시스템을 개발하는데 성공하였다. 이 시스템에 의하면 보험 소비자는 간편한 계약심사 과정을 통해 보험 가입이 가능하다. 또한 보험금 수령 시에도 긴 대기 없이 3분 내에 처리가 되도록 함으로써 소비자의 편의를 제공했다. 보험사 입장에서조차 챗봇을 활용하여 인건비를 대폭 절감하는데 성공하여 신생 스타트업임에도 불구하고 기존의 보험사와 경쟁할 수 있는 발판을 마련하였다.

미국 내 IT 기업의 보험산업 투자도 활발하다. 구글(Google)은 오스카 헬스케어 보험과 협약을 맺고 손목 웨어러블 기기를 제공하여 많이 걷는 보험 가입자에게는 보험료를 인하해주는 건강 프로그램을 제공하고 있다. 이처럼 미국 내 IT 기업의 빅데이터와 보험사의 노하우가 결합한 인슈어테크 서비스의 제공으로 기업 경쟁력의 강화와 보험의 본래 목적 달성을 통한 소비자 효용 증진에 긍정적인 효과가 기대된다.

(3) 영국

2015년부터 2017년 1월까지 전세계 인슈어테크 딜의 5%가 영국에서 이루어졌으며, 이는 미국, 독일에 이어 세계 3위에 해당하는 수치이다. 전통적으로 보험과 금

17) 박소정·박지윤, “인슈어테크 혁명: 현황 점검 및 과제 고찰”, 보험연구원, pp. 120. 2017. 08.

18) 박운호, “[대한민국 희망 프로젝트]K592>인슈어테크”, 전자신문, 2018.12.16.
<<http://www.etnews.com/20181214000287?m=1>> 2019.8.30. 최종방문.

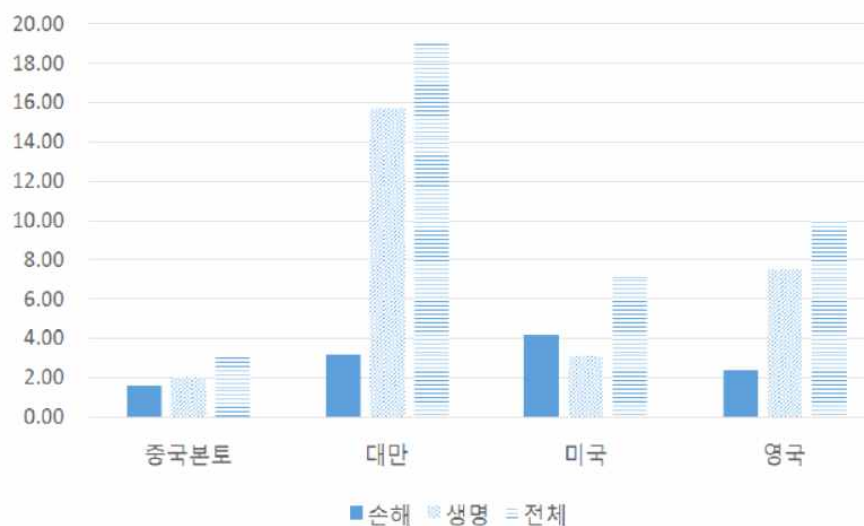
용 분야에서 강세를 보였던 영국이기에 브렉시트 등의 위협 요인 속에서도 선도를 이어나가기 위한 정부 차원의 노력이 이루어지고 있다.¹⁹⁾

영국은 2014년 FCA 산하에 핀테크 기업을 지원하는 이노베이션 허브(Innovation Hub)를 두어 복잡한 금융규제를 안내하고, 신상품 출시를 위한 승인을 조력하고 있다. 규제 샌드박스에 대한 검토, 관련 종사자들 간의 네트워킹 제공, 규제 안내 및 규제 완화 검토를 담당하고 있다.²⁰⁾

특히 규제 샌드박스(Regulatory Sandbox)가 영국의 핀테크 및 인슈어테크 산업 발전에 큰 보탬이 되고 있다. 규제 자체를 완화한 미국과는 달리, 영국에서는 규제를 본격적으로 완화하기 앞서 규제 샌드박스를 둬으로써 충분한 소비자 보호 조치 하에 신상품을 테스트하는 기간을 갖는다. 그리고 테스트 결과에 따라 향후 지속적으로 규제를 완화할지 여부를 검토한다.

(4) 중국

<그림 3> 글로벌 보험상품 보급률²¹⁾



19) BI Intelligence, UK still attractive for insurtech [Internet], Available: <http://uk.businessinsider.com/uk-still-attractive-for-insurtech-2017-4>, 2019.08.30

20) 삼정 KPMG 경제연구원, “국내외 핀테크(Fintech) 규제 동향 분석”, 삼정 KPMG Issue Monitor 제71호, pp.8, 2017. 05.

21) 박소정·박지윤, “인슈어테크 혁명: 현황 점검 및 과제 고찰”, 보험연구원, pp. 130-132. 2017. 08.

중국은 손해보험과 생명보험을 합한 보험상품 보급률(GDP 대비 프리미엄)이 3%로, 대만 19%, 미국 7.3%, 영국 10%에 비해 매우 저조한 편이다. 이는 중국에서 보험시장이 아직 충분히 성장하지 못했음을 의미함과 동시에, 인구 규모를 고려하였을 때 향후 중국의 보험시장이 크게 성장할 잠재력을 갖고 있음을 함축한다. 중국은 이미 핀테크 분야 등에 활용 중인 다양한 4차 산업 혁명 기술을 인슈어테크에 적용함과 동시에 적극적인 투자를 감행하고 있다. Oliver Wyman의 자료에 따르면 중국 인슈어테크 시장은 2015년 약 370억 달러에서 2020년 약 1740억 달러로 4.5배 가량 성장할 것으로 예상된다.²²⁾

한편 전술한 FT Partners(2016) 자료에 따르면, 전세계 인슈어테크 자금조달 규모 1위의 기업은 중국의 중안보험(Zhongan Insurance)이다. 중안보험의 자금조달 규모는 약 9억 3100만 달러에 달하며, 이는 미국에서 가장 높은 자금조달 규모를 보인 오스카보다도 2000만 달러 이상 높은 수치이다. 중국의 보험사 역시 미국과 마찬가지로 다양한 4차 산업 혁명 기술들을 보험산업에 접목시키고 있다. 중안보험은 사물인터넷을 기반으로 한 웨어러블 장치를 기반으로 보험료 할인 혜택을 제공하는 건강보험을 출시하였다. 중안보험 및 안심보험은 각각 알리바바와 텐센트가 제공하는 클라우드 서비스를 업무에 활용하여 효율성을 기하고 있다.

한편 중국 상하이보험거래소는 보험 계약 내용의 조작을 방지하기 위한 목적으로 9개 중국 보험회사의 참여하에 블록체인을 시범적으로 활용하기도 하였다. 또한 전술한 레모네이드와 마찬가지로 중국평안보험 및 태강보험 등도 인공지능을 활용하여 고객 서비스를 제공하고 있다. 또한 2015년 중국 정부가 구이양(貴陽) 빅데이터 거래소를 설립하여 인슈어테크의 핵심을 이루는 빅데이터를 기업간에 거래할 수 있는 환경을 조성하였다. 또한 보험감독관리위원회를 통해 각종 규제를 완화하고 문제가 발생할 경우 사후 조치를 취하는 방식으로 산업 발전을 우선시하고 있다.

특기할만한 것은, 중국의 IT 기업과 보험사가 협업하여 원스톱 솔루션 서비스를 출시하고 있다는 것이다. 알리바바는 기존부터 AI와 빅데이터 기술을 꾸준히 연구하고 축적한 끝에, 관계 회사인 앤트파이낸셜과의 협업으로 요율 산정과 손해사정 업무를 담당하는 인공지능 원스톱 솔루션을 출시하였다. 세계에서 가장 많은 인구를 바탕으로 충분한 빅데이터를 확보해온 중국 IT 기업이기 때문에, 이러한 빅데이터에 기반한 인공지능을 개발하여 인슈어테크 서비스를 제공할 경우 그 실효성이 매우 높을 것으로 판단된다.

22) Oliver wyman and Zhongan, "China Insurtech", Industry Report, pp.6, 2016.

중국의 인슈어테크 도입은 비단 기성 기업에 그칠 뿐만 아니라, 스타트업을 통해서도 이루어지는 중이다. 실제로 중국의 인슈어테크 스타트업 기업에 대한 투자 건수는 2014년에 비해 2016년 4배 이상 증가하였다.

(4) 한국

국내에서도 보험산업에서의 치열한 경쟁과 성장 둔화를 극복하기 위해 인슈어테크 도입 움직임이 활발하다. 이러한 기업의 수요에 발맞추어 정부 차원에서는 미국처럼 기존의 포지티브(Positive) 규제를 네거티브 규제로 개정하거나, 영국처럼 규제 샌드박스를 도입하는 방식으로 대응하고 있다. 또한 전술한 미국이나 중국에서의 경우처럼 국내에서도 IT 기업과 보험사의 협업이 이루어지고 있다. 모바일이 대중적으로 활성화된 국내 시장의 특성상 보험사는 SKT, KT 등의 통신사나 카카오 등 대형 정보서비스 업체와의 협약을 바탕으로 기술을 보험산업에 적용해내고 있다.

〈표 2〉 국내보험사의 ICT 기술 도입 현황²³⁾

구분	기관명	시기	주요내용
판매채널	미래에셋생명	2016년 11월	모바일 금융 및 보험 오픈마켓통합 비교, 판매 사이트 오픈
상품개발	흥국화재	2016년 12월	(KT와 협약) 운전습관연계보험(UBI) 상품 체험단 운영
유통/판매	라이나생명	2016년 11월	카카오톡 기반의 ‘챗봇(Chatbot)’ 서비스 도입
언더라이팅	푸르덴셜생명	2016년 12월	FICO 기술 접목, 신규 계약 언더라이팅 업무 40-50% 자동화
마케팅 및 고객관리	한화생명	2016년 9월	빅데이터를 활용한 고객관리 선진화 시스템 구축

한편 기업들의 인슈어테크 도입에 발맞추어, 보험산업에서의 기술 적용을 가로막았던 기존 규제를 완화함과 동시에 적극적인 지원 정책도 이루어지고 있다. 금융위원회 산하의 핀테크 지원센터는 인슈어테크를 포함한 핀테크 분야에서의 법률자문과 자본조달 및 금융사 간 네트워킹을 돕는 역할을 수행하고 있다.²⁴⁾

23) 윤일영, “보험과 기술의 융합, 인슈어테크”, Weekly TIP, Vol. 63, pp.9. 융합연구정책센터, 2017. 03.

24) 금융감독원, “핀테크 동향 및 IT 감독방향”, pp. 2. 2014. 12.

상단의 자료에서 볼 수 있듯이 국내 보험사는 온라인 및 모바일을 통한 판매 채널의 다각화, 사물인터넷 도입을 통한 효율적인 보험 상품 개발, AI 기술을 도입한 보험모집 및 계약심사 자동화, 빅데이터를 활용한 계약심사 및 고객관리, 모바일을 통한 보험금 청구의 간소화 등 다방면에서 신기술을 도입하여 보험소비자의 효용과 보험사의 이익 증진을 도모하고 있다.

이는 보험산업에서의 새로운 파이를 창출하는 데에 기여할 뿐만 아니라 앞서 언급한 기존 보험산업에서의 한계를 극복할 수 있는 대안이라는 점에서 가치가 있다. 또한 보험산업에서의 한계 극복을 통해 보험산업의 본래 목적이기도 한 사회 전체의 위험 수준 감소에 기여할 수 있다는 점에서 공익적 타당성도 지니고 있다. 따라서 이를 적극적으로 장려하기 위한 정부의 규제 완화와 지원정책은 합당하며, 시행과정에서의 부작용을 효과적으로 통제할 수 있다면 소비자, 기업, 정부 세 경제 주체 모두가 Win-Win할 수 있을 것이다.

4. 인슈어테크 산업을 둘러싼 국내 주체들의 입장

(1) 소비자

인슈어테크 발달로 인해 최종적으로 가장 큰 혜택을 받게 되는 것은 소비자이다. 기업의 경우 초기에 비용 감소와 이익 증대를 누리지만 동질적인 서비스의 경우에는 시장에서 다른 보험사와의 가격 경쟁을 통해 종국적으로 가격을 인하하게 되고 균형점에 도달할 것이기 때문이다. 따라서 소비자는 기술로 인한 편리함과 보험 가입 비용의 감소라는 이점을 누리게 된다.

위험의 감소와 제거가 소비자 입장에서 보험 가입의 목적인데, 인슈어테크는 경제 주체가 보다 덜 위험하게 행동하도록 유도하여 궁극적으로 이러한 목적 실현에 도움을 줄 수 있다. 가령 사물인터넷을 통한 보험 상품은 소비자로 하여금 본인의 행동을 조절하여 위험의 빈도와 심도를 낮추게끔 할 것이다. 또한 이러한 행동 변화는 보험사를 통해 감지되어 소비자가 보험료 인하의 혜택을 누릴 수 있게 될 것이다. 또한, 보험사가 AI를 활용함에 따른 비용 감소는 결국 소비자가 부담하는 보험료의 감소로 이어지며, 정교한 서비스 제공 시에는 인간이 보험을 모집하는 경우보다 적절한 계약심사를 통해 보험에 가입할 수 있다는 장점도 있다. 빅데이터를 활용할 경우 보다 적합한 보험 상품을 제공받거나 새로운 보험 상품이 등장하여 소

비자가 혜택을 누릴 수 있게 된다. 블록체인 기술을 활용하여 보다 간단하고 안전하게 보험금을 청구할 수 있게 된다. P2P 보험을 통해 자발적인 단체 결성을 통한 위험 회피가 가능해진다.

다만 사물인터넷이나 빅데이터 기술 등의 도입을 통해 소비자의 개인정보가 유출될 위험성이 높아질 우려가 있다. 따라서 이러한 문제를 정책적, 기술적으로 담보하기 위한 노력이 요구될 것이다.

(2) 기업

기업 차원에서 인슈어테크는 성장의 기회이자 경쟁에서의 생존을 위한 도구이다. 인슈어테크를 적극 도입하는 보험사는 보험 산업 내 치열한 경쟁에서 비롯된 포화 상태에서 벗어나 기술 도입으로 인한 이익을 선점할 수 있다. 사물인터넷, 인공지능, 빅데이터, 블록체인 등의 기술을 통해 보험사의 비용을 절감하거나 정보 비대칭의 문제를 상당 부분 해소할 수 있다. 정보 비대칭의 문제를 해소할 경우 보험의 전통적인 한계인 도덕적 해이와 역선택, 보험 사각지대 등의 문제를 극복할 수 있음은 물론이다. 비용 절감과 신상품을 통한 시장 개척으로 보험사는 성장의 기회를 마련할 수 있다.

또한 미래에는 인슈어테크의 활용이 더 이상 특별한 것이 아닌 일반화될 수 있다. 이 시기에 인슈어테크를 활용하는 것은 보험사 입장에서 선택이 아닌 필수가 될 것이다. 따라서 그러한 상황이 오고 나서 개발 및 활용에 뒤늦게 참여하는 것보다는 먼저 해당 분야에 투자를 통해 선두로서 이익을 선점하고, 소비자들을 상대로 충분한 기간 인슈어테크 브랜드로 입지를 다지는 것이 유리할 수 있다. 한편 인슈어테크 발달 초기에 정부의 시혜적인 재정 지원이 이루어질 경우 기업 입장에서 선두주자로서 시장에 참여할 유인은 더욱 커질 수 있을 것이다.

보험사뿐만 아니라 기존의 IT 기업 등에게도 인슈어테크는 기회가 될 수 있다. 미국, 중국 등에서도 IT 기업이나 모바일, 포털 관련 기업들이 빅데이터 수집 및 처리 능력을 바탕으로 보험사와 활발한 협업을 진행하고 있다.²⁵⁾ 국내에서도 이미 통신사 및 정보통신업체와 보험사가 협업한 사례가 있다. 빅데이터를 토대로 유의미한 패턴을 분석할 능력을 갖춘 기업들은 보험사와의 협업을 통해 보험 분야에서 혁신적인 상품을 개발하고 서비스를 제공할 수 있을 것이다. 정보 비대칭 등의 문제로

25) 박소정·박지윤, “인슈어테크 혁명: 현황 점검 및 과제 고찰”, 보험연구원, pp. 41. 2017. 08.

비효율성이 심각한 보험산업에서 협업을 통하여 효율적인 상품과 서비스를 제공할 수 있다면 보험 시장의 선두로써 소비자들에게 각광받을 수 있음은 물론이다.

(3) 정부

정부 입장에서는 소비자와 기업 모두에게 이익이 되는 인슈어테크 산업 발전을 지원할 동기가 충분하다. 특히 인슈어테크 산업의 발전은 최근 대두되는 핀테크 산업의 발전과도 유관하며 기술 발전을 통해 여타 산업에도 긍정적인 영향을 줄 수 있다는 점에서 주목받고 있다. 특정 산업에서의 기술 발전이 다른 산업의 발전으로 이어지는 선순환을 통해 국가 경제에 활력을 제고하고, 편리한 기술을 통해 국민들의 생활 수준 또한 향상될 수 있다.

특히 인슈어테크가 보험산업에의 기술 적용이라는 점에 공익적 의의를 찾을 수 있다. 보험은 위험의 감소와 제거를 목적으로 하는데, 이는 국가가 완벽하게 관리할 수 없는 개별 국민의 경제적 안전을 보장하는 역할을 한다. 따라서 민간의 사보험을 대상으로 혁신 기술이 적용될 경우 이러한 안전 보장에 관한 국가의 책무도 크게 경감되고, 실제로 국민의 삶의 질을 향상시켜주어 정부가 추구하는 공익적 목적을 실현할 수 있다. 따라서 인슈어테크 발전을 위해 정부가 규제 및 정책적으로 지원 정책을 펴는 것은 사회의 필요에도 부합한다고 할 수 있다. 향후 국민연금 등 정부 주도로 시행하는 공적 보험에 있어서도 인슈어테크를 적용하여 보다 효과적인 운영이 가능해짐은 물론이다.

미국의 경우 규제를 완화하여 기업의 자유도를 높이고, 영국의 경우 규제 샌드박스를 통해 인슈어테크 도입의 장(場)을 마련해주었다. 중국의 경우 정부의 막강한 개입을 통해 도입 과정에서의 부작용을 감수하더라도 산업의 발전을 우선시하는 태도를 보이고 있다. 우리나라 정부의 경우 규제 완화와 정책 지원이 이루어지고 있지만 아직까지 그 효과는 미비한 편이다. 따라서 다른 나라의 사례를 참고하여 국내에서 인슈어테크 산업 발전을 도모하기 위한 실효성 있는 규제 완화와 지원 방식은 무엇인지 검토할 필요가 있다.

5. 소결: 국내 인슈어테크 활용에 관한 법적 문제

전술한 대로, 세계의 여러 기업들이 인슈어테크의 가치에 주목하여 이를 활용한

상품과 서비스를 개발하고 있다. 각국 정부 또한 이러한 흐름에 발맞추어 규제 완화와 정책적 지원으로 대응하고 있다. 인슈어테크 산업 발달에 따라 소비자들의 편의성이 제고되고 소비자의 니즈를 더욱 잘 충족할 수 있을 것으로 기대된다.

국내에서도 인슈어테크를 결합한 서비스를 다수 도입하고 있지만, 여전히 다른 국가에 비해 발전 속도나 정도는 더딘 편이다. 특히 4차 산업혁명 기술을 보험 사업에 적용함에 있어서 ‘규제’로 인한 한계가 뚜렷하다. 이러한 한계는 국내 인슈어테크의 발전 속도를 늦추고, 큰 규모의 투자가 이루어지지 못하도록 한 원인으로 꼽힌다. 실제로 전술한 FT Partners(2016) 자료의 내용에 따르면, 전 세계 인슈어테크 자금 조달의 75%를 차지한 북미에 비해 아시아 지역은 8%에 그쳤다. 같은 아시아권역 국가인 중국과 비교해보아도 국내 인슈어테크 관련 투자의 부족함은 여실히 드러난다. 중국의 경우 인슈어테크 관련 규제를 우선 완화하여주고 문제가 발생할 경우 사후 조치를 취하는 방식으로 적극적인 지원을 하고 있으며 이를 통해 중국 보험사들의 적극적인 인슈어테크 투자를 유도하고 있다. 반면 국내에서는 촘촘한 규제와 그로 인한 규제 리스크(Legal Risk) 탓에 새로운 기술을 적용하더라도 소극적으로 활용할 수밖에 없는 상황이다. 기술 개발을 통한 효과를 온전히 누릴 수 없는 규제 환경이기에 인슈어테크 분야에 보다 적극적이고 공격적인 투자를 감행하기 어렵다.

규제를 완화하는 것뿐만 아니라 적극적인 정부 정책이 필요하다. 가령 중국의 경우 구이양 빅데이터 거래소를 설립하여 빅데이터를 안전하게 거래하고 활용할 수 있는 환경을 조성하였다.²⁶⁾ 이처럼 경우에 따라서는 규제의 완화뿐만 아니라 목적 달성을 위한 창의적인 정책을 통해 산업의 발전을 효율적이고 효과적으로 도모할 수 있을 것이다.

이러한 점을 종합적으로 검토하였을 때 현재 국내 인슈어테크 산업은 보다 적극적인 규제 완화, 그리고 때로는 정부 정책을 결합한 방식을 통해 더욱 크게 성장할 수 있을 것이다.

26) 박소영·장현숙, “빅데이터 거래의 한·중 비교: 기업 활용을 중심으로”, 한국무역협회, pp. 3-11. 2018. 04.

Ⅲ. 국내 인슈어테크에 관한 법적 문제를 해결하기 위한 방법론

1. 법령의 제정·개정의 선택과 특별법 문제

현재 우리나라 보험업과 관련된 규제는 대부분 포지티브(positive) 규제이다. 포지티브 규제는 사전에 법률로 명확하게 정한 것만 할 수 있기 때문에 국내 인슈어테크 산업의 발전을 저해하고 있는 원인으로 꼽혀왔다. 이를 해결하기 위하여 금융당국은 다방면으로 노력하고 있다. 사전규제 성격이었던 금융감독 체계를 사후규제 성격인 네거티브(negative) 규제로 바꾸어 나가고 있고, 그 대표적인 사례로 보안성심의 규정이었던 전자금융감독규정 제36조가 2016년 6월 사후 검증으로 개정되는 등 소기의 성과를 거두었다.

이에 그치지 않고, 장기적으로 다양한 주체가 인슈어테크 산업에 적극적으로 참여하도록 장려하기 위해서는 국내에 산재한 법적 쟁점에 대한 파악과 이를 바탕으로 한 적절한 개정 방안이 필요하다. 그 가운데, 본 연구에서는 대표적으로 ① 법령의 개정 ② 법령(특별법)의 제정, 그리고 이들을 통해 ③ 규제 샌드박스의 활성화에 대해 검토한다. 구체적으로는 각 방법에 대해 정립된 일반론과 이를 바탕으로 인슈어테크에 어떻게 적용할 것인지를 연구한다.

2. 기존 법령 개정

(1) 일반론²⁷⁾

기존 법령에서 규정한 제도를 보완하거나 새로운 사항을 규율하더라도 유사한 분야를 규율하는 법령이 있어 그 법령을 개정함으로써 쉽게 반영할 수 있는 경우라면 기존 법령을 개정하는 것이 일반적이고, 전혀 새로운 분야를 규율하거나 기존의 여러 법령에서 규율하고 있는 사항을 아울러 체계적·종합적으로 규율할 필요성이 있다면 특별법을 포함한 새로운 법령을 제정하는 것이 일반적이다.

요컨대 입법정책적으로 입법 목적을 실현하는 데 어느 쪽이 유리한지, 어느 쪽이 입법 경제적인지, 어느 쪽이 법체계의 정합성 유지에 적합한지, 어느 쪽이 국민이

27) 법제처, 『법령 입안·심사 기준』, pp. 10. 2019.

법을 이해하는 데 도움이 되는지 등을 고려해서 결정해야 한다.

현재 우리나라는 행정규제기본법 제4조(규제법정주의)에 따라 모든 규제를 법률에 직접 규정하는 것을 원칙으로 하되 규제의 세부내용은 법률 또는 상위 법령의 구체적인 위임에 따라 하위법령(대통령령, 총리령, 부령, 조례·규칙 등)으로 정할 수 있도록 하고 있다. 규제법정주의를 엄격하게 지키기 위해서는 기존 법령의 제정 또는 개정의 방식으로 인슈어테크와 관련된 규제 문제를 해결하는 것이 좋을 것이다. 그러나 이를 따르다 보면 규제 완화를 위해서는 해당 사안에 대해 입법과정이 필수적으로 수반되어야 하는데, 인슈어테크를 포함한 4차 산업혁명 시대의 분야에서 사전에 예측하여 법령을 완벽하게 입안하기란 사실상 불가능에 가깝기에 고민이 필요하다.

(2) 인슈어테크에의 적용

오늘날 인슈어테크는 보험업법을 포함한 금융업법 전반에 걸쳐 새로운 사항의 규율을 요하는 분야이다. 유사한 분야를 규율하는 기존의 법령이 존재하기는 하나, 효율성과 경제성의 측면에서 볼 때, 이에 더하여 규정을 보완하거나 추가하기 쉽지 않은 분야도 다수 있다. 더불어 기존 법령을 일괄적으로 개정할 경우 다음과 같은 형평의 문제도 발생한다.

전통적인 거대한 규모의 보험사들에 대해서는 그들이 법의 목적과 취지를 잠탈하거나 우회하여 부당한 이득을 추구하는 것을 엄격히 막을 필요가 있을 것이며, 반면 새로운 기술을 통해서 새로운 시장을 창출하고 소비자에게 편익을 제공하는 기업들에게는 오히려 혁신을 장려할 필요가 있을 것이다.

이러한 요소를 고려하다 보니 국내에서는 기존 법령의 개정이 잦지는 않다. 그럼에도 기존 핵심 기본법의 개정이 이루어짐으로써 긍정적인 파급력을 갖는 경우가 있다. 특히 현재 시점에서 파악할 수 있는 위험과 오용 가능성 등이 명백한 분야에 대해서는 기존 법령 개정의 방식으로 이를 명시화할 필요가 있다. 이를 통해 해당 분야를 통해 규율을 받는 법인 또는 자연인의 예측 가능성 증대를 달성할 수 있을 것이고, 보다 안정적 토대 위에서 인슈어테크 산업의 성장을 이끌 수 있을 것이기 때문이다. 우리나라는 「행정규제기본법 개정안」을 통해서 기존 법령 개정 방식을 인슈어테크를 포함한 혁신 분야에 대해 규제 샌드박스 제도를 병행하기 위해 활용한 바 있다.

구체적으로는 「행정규제기본법 개정안」 내에 우선허용-사후규제 원칙 명문화, 신기술 제품 및 서비스 관련 규제의 신속 확인 및 신속 정비 의무 부과, 규제특례 적용 시 고려사항 명시, 3년 단위의 신산업 규제정비 기본계획 수립·시행 내용 등을 포함해 2019년 7월 17일부터 시행하였다. 본 법령이 직접 특정한 처분을 명하고 있지는 않으나, 기본법으로써 아래에 기술할 규제 샌드박스의 활용 가능성을 높이는 토대로써 역할하고 있다.

3. 특별법 제정

(1) 일반론²⁸⁾

최근 특정한 입법정책의 수행에 효과적으로 대응하고, 특정한 정책에 대한 국민의 관심을 불러일으켜 입법 목적을 원활하게 달성하기 위해 각종 특별법·특례법·특별조치법 등의 명칭으로 특별법이 많이 제정되고 있다.

특별법은 새로운 분야의 입법 수요의 반영 또는 기존 법제도에 대한 예외적인 상황이나 내용을 규정해야 할 필요성이 있는 경우에 주로 만들어진다. 그러나 특별법이 다수 양산되면 법체계가 혼란스러워져 법규범 상호 간의 충돌과 모순으로 체계 정당성을 침해할 여지가 커진다. 또한, 국민 여론과 정치적인 이유에 따라 급히 입법이 진행되는 경우에는 합리성에 대한 검토가 부족할 여지도 있으며, 법령이 특정 문제나 특정 지역에만 특례를 인정하는 등의 처분적 내용을 규정함으로써 형평상의 문제가 발생할 수 있다. 더구나 특별법이 많아지면 법체계가 복잡해져 수범자 입장에서 법을 이해하기 어렵게 되고 법체계에 대한 신뢰성도 낮아질 수 있다. 따라서 특별법은 제정에 앞서 신중하게 검토할 필요가 있다.

구체적으로는 특별법의 제정 필요성과 실효성과 적합성, 기존 법령과의 조화 등을 종합적으로 검토해 신중히 결정하여야 하며, 부득이 특별법을 제정하거나 특례를 규정해야 할 필요가 있다고 판단되는 경우에는 특별법이 평등의 원칙, 비례(과잉금지)의 원칙, 책임주의 원칙 등 헌법상 원칙을 위반하는 것이 아닌지, 기존의 일반법과의 관계에서 해석·적용 시에 모순되거나 충돌되는 부분이 없는지 등에 대한 체계적인 검토가 필요하다. 또한, 해당 법률이 어떤 법률이나 내용에 관한 특례나 특별 규정인지를 목적 규정에서 명확히 드러나도록 명시해야 할 것이다. 이 경우

28) 법제처, 『법령 입안·심사 기준』, pp. 11. 2019.

적용되는 일반법이 하나라면 해당 일반법을 적시하여 그에 대한 특례를 규정한다는 것을 명시할 수도 있지만, 다수의 일반법에 대한 특례를 규정하는 경우에는 어느 하나의 일반법만을 적시하는 것이 곤란하므로 특례의 내용 등을 표시하는 방법도 자주 활용된다.

(2) 인슈어테크에의 적용

인슈어테크 분야의 경우에는 위에서 논의한 바와 같이 포지티브(positive) 규제로 인해 그 발전이 더딘 경우가 잦다. 따라서 이를 네거티브(negative) 규제 형태로 변화시키는 것이 요구되고 있는 것이 실정이다. 그러나 이를 기존 법령 내로 편입시키면 인슈어테크로 보기 어려운 분야 또는 부적절한 주체의 참여를 통해 금융업과 보험업 내의 시장이 혼란스러워질 가능성이 크다. 따라서 위 일반론에서 검토한 내용에도 불구하고, 현재 국내 환경에서는 기존 법령의 개정보다는 특별법 제정을 통한 특례 적용이 더 적절한 사례가 다수 존재한다.

정부와 국회 역시 이러한 필요성을 느껴 정부는 4차 산업혁명 시대 혁신적인 성장을 위해 도입한 ‘규제 샌드박스 제도 도입 등에 관한 규제 혁신 5개 법률’ 중 다수가 특별법의 형태를 띠고 있다. 정부는 특별법과 특례 규정을 통해 규제 샌드박스 제도를 도입하고자 하였으며, 기존의 포지티브(positive) 규제 체제에서 ‘우선 허용-사후규제’를 표방하는 네거티브(negative) 규제 체계로 패러다임을 전환함으로써 신기술·신산업 분야를 활성화하며 혁신적인 성장을 달성하고자 하고 있다.

위에서 정부가 추진한 규제 혁신 5개 법률 중 위 개정 법률이 2019년 1월 17일 시행되었고, 「금융혁신지원 특별법」은 2019년 4월 1일 시행되어 이미 금융위원회의 검토를 통해 5월 15일부터 혁신금융서비스 8건이 지정되어 시행되고 있다.

「정보통신 진흥 및 융합 활성화 등에 관한 특별법」(이하 ‘정보통신융합법’)과 「산업융합 촉진법」(이하 두 법률을 통칭하여 ‘개정 법률’이라고 한다)이 2018년 10월 16일 일부 개정되어 2019년 1월 17일 시행되었다. 이 외에 「규제자유특구 및 지역특화발전특구에 관한 규제 특례법」은 2019년 4월 17일 시행되었다.²⁹⁾ 이러한 법률들은 ‘한국형 규제 샌드박스 5법’ 등으로 불리며 규제 샌드박스 활성화에 기여하고 있다는 평가를 받고 있다. 정부가 기존 법령의 개정과 특별법의 제정을 통

29) 박광배 손경민, “ICT융합·산업융합 규제 샌드박스가 시행되었습니다”, 법률신문, 2019.2.22. <<https://www.lawtimes.co.kr/Legal-Info/LawFirm-NewsLetter-view?serial=151010>> 2019.8.24. 최종방문.

해서 일관적으로 추구하고 있는 목표인 규제 샌드박스에 대해서 이어 검토하도록 한다.

4. 규제 샌드박스(Regulatory Sandbox)

(1) 일반론³⁰⁾

위 특별법의 내용 중 하나인 규제 샌드박스(Regulatory Sandbox)라는 새로운 형태로 입법 정책의 목적을 달성할 수도 있다. 규제 샌드박스는 일반적으로 제한된 조건 하에서 새로운 제품 및 서비스에 대한 규제를 풀어주는 제도 또는 특례를 의미하며, 신산업과 신기술 분야의 시험적 운영을 가능하게 한다. 규제 샌드박스의 ‘샌드박스(Sandbox)’ 용어는 아이들이 안전한 환경에서 자유롭게 뛰어노는 모래놀이터(Sandbox)에서 유래하였다. 우리나라도 금융위원회 주도하에 2016년부터 금융과 IT 융합 등에 대해 테스트베드 역할을 하는 규제 샌드박스 도입을 추진하였다. 한국의 현재 규제체계로는 신기술과 신산업의 빠른 변화를 신속히 반영할 수 없다는 인식하에 적극적으로 이에 임하고 있다.

(2) 인슈어테크에의 적용

위에서 언급한 기존 법령의 개정과 특별법의 제정 등을 통해서 우리나라가 달성하고자 하는 목표는 규제 샌드박스 확장을 통해 4차 산업혁명 시대의 경쟁력 확보이다. 인슈어테크 역시 4차 산업혁명 시대의 핵심 분야 중 하나이며, 특히 핀테크 산업과 밀접한 관계를 맺고 있기에 이러한 정부의 입법정책에 따른 영향을 크게 받고 있다. 현재 국내의 규제 샌드박스 관련 법규의 진행 경과를 다음과 같다.

30) 법제처, 『법령 입안·심사 기준』, pp. 11. 2019.

〈표 3〉 한국형 규제 샌드박스 5법 개요³¹⁾

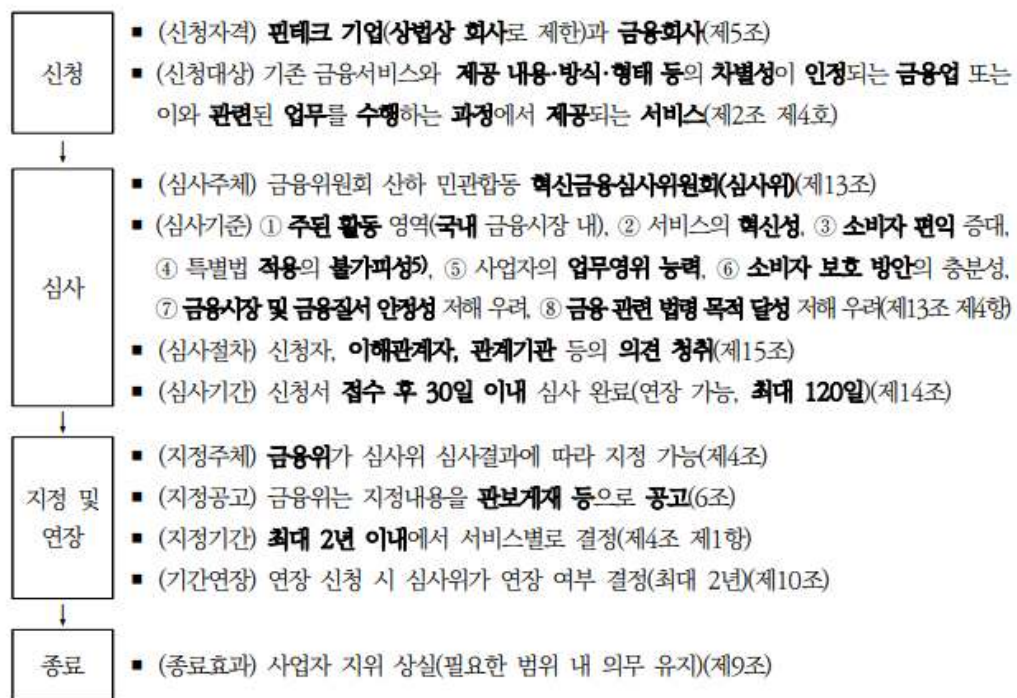
법명	진행경과	주요 내용
행정규제기본법	2019.7.17. 시행	<ul style="list-style-type: none"> ■ 우선허용-사후규제 원칙 명문화 ■ 신기술 제품 및 서비스 관련 규제의 신속 확인 및 신속 정비 의무 부과 ■ 규제특례 적용 시 고려사항 명시 ■ 3년 단위의 신산업 규제정비 기본계획 수립·시행
규제자유특구 및 지역특화발전특 구에 관한 규제특례법	2019.4.17. 시행	<ul style="list-style-type: none"> ■ 규제자유특구 내의 지역혁신성장사업 또는 지역전략산 업에 대한 규제의 신속확인 ■ 실증을 위한 규제특례 및 임시허가 제도 도입
정보통신진흥 및 융합 활성화 등에 관한 특별법	2019.1.17. 시행	<ul style="list-style-type: none"> ■ 우선허용-사후규제 원칙 명문화 ■ 실증을 위한 규제특례제도 도입 - 현행 법령상 추진이 불가능한 정보통신융합 신기술 및 서비스에 대하여 제한적 시험이나 기술적 검증을 위해 규제의 전부 또는 일부 적용 배제 ■ 임시허가제도 보완 - 규제공백이 있거나, 현행규제의 적용 여부가 불명확 또는 불합리한 정보통신융합 신기술 및 서비스에 대하여 2년의 범위에서 임시 허가
산업융합 촉진법	2019.1.17. 시행	<ul style="list-style-type: none"> ■ 우선허용-사후규제 원칙 명문화 ■ 산업융합 신제품 및 신서비스 관련 규제의 신속 확인 의무 부과 ■ 실증을 위한 규제특례제도 도입 - 산업융합 신제품 및 서비스의 시험·검사를 위해 관련 규제의 전부 또는 일부의 적용 ■ 임시허가제도 도입 - 규제공백이 있거나, 현행규제의 적용 여부가 불명확/불 합리한 산업융합 신제품 및 신서비스에 대하여 2년의 범 위에서 임시 허가
금융혁신지원 특별법	2019.4.1. 시행	<ul style="list-style-type: none"> ■ 혁신금융서비스 관련 규제의 신속확인 의무 부과 ■ 혁신금융서비스 지정(2년 이내)제도 도입 - 필요시 일부 금융규제 적용 배제

31) 박명금, “규제완화를 위한 법제업무의 개선방안 연구”, 법제처, pp. 91. 2019.

위의 법들은 기존의 법령 및 규제를 완전히 개정하거나 신규 법령을 제정하지 않으면서도 혁신기업들이 유연하게 새로운 영역에서의 사업을 할 수 있도록 하는 것을 그 주목적으로 하고 있다. 현재 시행되고 있는 규제 샌드박스 관련 법률은 정보통신분야(「정보통신 진흥 및 융합 활성화 등에 관한 특별법」)와 산업융합분야(「산업융합 촉진법」), 그리고 금융분야(「금융혁신지원 특별법(이하 금융혁신법)」) 등이다. 인슈어테크의 경우, 해당 기술 또는 사업의 모형에 따라 본 분야에 모두 해당할 가능성이 크다. 더불어 행정규제기본법 또한 위에서 언급한 바와 같이 규제 샌드박스를 지원하고자 개정되어 현재 시행되고 있다.

특히, 이 중 금융혁신법은 인슈어테크와 매우 밀접한 관계를 맺고 있다. 상당수의 인슈어테크가 금융과 밀접한 연관을 맺고 있기 때문이다. 현행 금융혁신법에서는 혁신금융서비스 지정을 통해 규제 특례를 인정하고 있는데 그 구체적인 절차는 다음과 같이 진행된다.

〈그림 4〉 금융혁신법에 따른 혁신금융서비스 지정 절차³²⁾



32) 양승현, “금융혁신지원특별법의 주요 내용 검토”, 보험연구원, pp. 3. 2018.

위의 절차를 통해 혁신금융서비스 지정을 받게 되면, 그 범위 내에서 서비스를 영위할 수 있으며, 금융혁신법 제16조 내지 제17조에 따라서 특례가 인정된 해당 금융 관련 법령상 규제가 적용되지 않는다. 다만 그 적용 대상은 법률에 열거된 금융 관계 법률 및 대통령령으로 정하는 법령으로 한하고 있으며, 타 행정기관 소관 법령의 경우에는 해당 기관의 동의를 통해 특례를 지정할 수 있다.

더불어 규제 특례로 인하여 소비자 보호가 취약해질 수 있기 때문에 이에 대해서도 엄격히 규정하고 있다. 금융감독원 등이 특별법 등의 준수 여부를 감독하며, 사업자의 업무 및 재산 상황을 지속적으로 검사한다. 또한 사업자는 소비자 보호 및 위험 관리 방안을 마련해야 하며 동시에 준수하여야 한다. 이용자에게 손해가 발생한 경우 손해배상책임을 넓게 인정하며, 배상책임도 이행할 수 있도록 보장 장치를 마련하여야 한다. 구체적으로 손해배상 소송에 있어 사업자가 고의·과실에 대한 입증책임을 지도록 하였으며, 배상을 할 수 있도록 보험에 가입하거나 금융위원회와의 협의를 거쳐 배상방안을 마련해야 하도록 규정되어 있다.

위에서 검토한 바와 같이 장기적으로 일시적 가이드라인을 넘어 입법안을 만들어 나가는 것도 매우 중요하기 때문에 혁신금융심사위원회는 지정 기간 만료 이후에도 서비스를 지속적으로 제공할 수 있도록 관련 행정기관에 법령의 제정 또는 개정을 권고할 수도 있다.

5. 인슈어테크 활성화를 위한 입법 방안

위에서 언급한 기존 법률의 개정과 특별법의 제정, 그리고 이를 통한 규제 샌드박스 활용은 모두 각각의 장점과 단점을 갖고 있다. 규제 샌드박스, 특히 핀테크와 관련된 규제에서 선도적 지위를 지닌 영국, 싱가포르를 비롯한 외국의 사례를 검토해 볼 때, 각국의 법체계와 시장에 적절한 방법을 선택해서 적용하는 것이 중요하다.

우리나라도 국내 법체계와 현황에 대한 이해를 바탕으로 각 분야와 해당 법률을 검토하여 적절한 대응을 하여야 할 것이다. 일부 분야에 대해서는 그 과정에서 인슈어테크의 빠른 변화 등을 고려할 때, 오로지 입법만으로 완벽한 법제 체계를 형성하는 것은 어려운 것이며, 금융위원회·금융감독원·금융보안원 등의 적극적인 참여가 필요할 것이다.

인슈어테크 시장의 빠른 성장 속도와 국내 시장에 미치는 영향을 고려할 때, 핵

심 규제들에 대하여 어떠한 유형의 방안을 활용하여 대처할 것인지와 그 파급 효과를 분석하는 것은 매우 중요하다. 다음 장에서 국내의 핵심 인슈어테크 쟁점에 대해 논의하고 위에서 검토한 방안을 토대로 입법·행정 수단을 포함한 적절한 대응 방안을 제안하고, 그 영향을 분석하고자 한다.

IV. 국내 인슈어테크 활용에 관한 법적 쟁점 및 개정 방안

1. 국내 인슈어테크 활용에 관한 주요 법적 쟁점 개관

본 연구에서는 4차 산업혁명 기술 중에서도 기존 보험산업의 한계를 극복하고 고부가가치를 창출할 것으로 기대되는 인슈어테크를 중심으로 국내에서의 활용에 관한 법적 쟁점을 검토해본다.

① 사물인터넷 기반의 건강증진 프로그램을 통한 보험료 할인, ② AI를 활용한 보험모집 및 업무 자동화, ③ 빅데이터를 활용한 위험 분석, ④ 블록체인을 활용한 보험금 청구 자동화 및 모바일 증권 진위 판별, ⑤ P2P 보험의 도입 순서로 각각의 주제에 대하여 발생 가능한 법적 쟁점과 이를 해결하기 위한 개정 방안을 제시하기로 한다.

2. 사물인터넷(IoT) 기반의 건강증진 프로그램을 통한 보험료 할인

(1) 법적 쟁점

〈그림 5〉 금융당국이 제시한 ‘건강증진형 보험상품’³³⁾



우리나라 정부는 사물인터넷을 ‘정보통신기술 기반으로 모든 사물을 연결해 사람과 사물, 사물과 사물간에 정보를 교류하고 상호 소통하는 지능형 인프라 및 서비스 기술’로 정의하고 있다.³⁴⁾ 즉 사물인터넷은 실시간으로 사람과 사물, 사물과 사물 간에 데이터를 공유할 수 있게 해주는 기술로 보험 분야에서 오랫동안 난제로 여겨졌던 정보 비대칭 문제를 가장 확실하게 해소해줄 방법으로 기대되고 있다. 이를테면 건강보험 분야에서 보험회사가 보험 계약자로부터 얻고자 하는 건강 관련 정보를 보험 계약자가 착용하는 웨어러블 기기를 통해 실시간으로 파악하는 것이 대표적인 예라고 할 수 있다. 이는 정보 비대칭 해소 및 정보 습득에 필요한 비용의 현저한 감소를 통해 보험사에게 이익이 된다.

또한 이러한 웨어러블 기기는 단순히 보험사에게 정보를 제공할 뿐만 아니라 보

33) 금융위원회·금융감독원, “건강증진형 보험상품 가이드라인”, pp.6-7. 2017. 11.

34) 행정안전부, “정부사물인터넷 도입 가이드라인”, pp.3. 2019. 07.

험 소비자가 스스로 위험을 줄이도록 인센티브를 부여한다는 점에 의의가 있다. 웨어러블 기기가 보험 소비자의 특정 행동을 감지하거나 건강 관련 지표를 파악하고, 이러한 행동이나 지표가 건강증진에 유익한 신호로 여겨지면 보험료 할인의 혜택을 제공하는 것이다. 이러한 시스템 하에서 보험 소비자는 자신이 건강한 행동을 하고 있다는 신호 보내기(Signaling)를 통해 보험료를 낮출 수 있게 된다. 보험 소비자가 보험료 할인 혜택을 받기 위해 건강에 유익한 행동을 하고, 건강 지표를 개선하는 동안 실제로 위험의 빈도와 심도가 낮아지게 된다. 결국 보험사와 보험 소비자 모두 정보 비대칭의 해소를 통해 위험의 감소라는 혜택을 누릴 수 있게 된다.

이처럼 사물인터넷을 활용한 건강보험의 획기적 변화는, 기존에 보험사가 담보하기 꺼리던 분야로의 사업 진출을 용이하게 해줄 수 있다. 과거에는 정보가 불확실하거나 위험성이 높아 보험 상품이 형성되지 못했던 시장도 웨어러블 기기를 통한 정보 비대칭 해소와 위험 감소를 통해 새롭게 개척되고, 보험사와 보험 소비자는 서로에게 이익이 되는 거래를 할 수 있게 된다.

문제는 이와 같이 보험사와 보험 소비자 모두에게 이로울 것으로 여겨지는 사물인터넷을 실제 건강보험 분야에 도입하는데 있어 법적 쟁점이 산재해있다는 것이다. 현행법상 문제의 소지가 있는 쟁점은 다음과 같다.

① 보험사가 웨어러블 기기를 활용하여 시행하는 건강증진 프로그램이 의료법상 ‘의료행위’에 해당하여 위법한지 여부

② 건강증진 프로그램의 진행 경과에 따른 보험료 할인이나 페이백이 보험업법 제98조에서 금지하는 특별이익의 제공에 해당하여 위법한지 여부

우선 ①번 의료법 쟁점을 검토해보면, 보험사는 의료법상 의료행위를 할 수 있는 주체가 아니다.³⁵⁾ 그런데 만일 웨어러블 기기를 활용한 건강증진 프로그램이 의료행위에 해당한다면 이는 위법한 행위가 된다. 의료법상 의료행위의 개념은 불명확한 상황이어서 국내 보험사들은 자칫 의료법에 저촉될 우려가 있는 건강증진 프로그램 사업을 선뜻 시행하지 못하고 있다. 이처럼 의료법상 의료행위의 판단기준이 모호하기 때문에 2019년 5월 보건복지부는 ‘비의료 건강관리서비스 가이드라인 및 사례집(1차)’를 작성하여 배포하였다.³⁶⁾ 또한 금융위원회와 금융감독원은 아예 해

35) 「의료법」 제27조 제1항.

당분야를 특정하여 ‘건강증진형 보험상품 가이드라인’을 배포하였다. 보험사들이 인슈어테크를 활용한 건강보험 상품을 도입함에 있어서 산재하는 법적 불확실성을 해소해주기 위한 정부 차원의 노력이다. 하지만 가이드라인은 어디까지나 가이드라인이기 때문에 그보다 상위의 개념인 법령이 그대로 존속하는 한 여전히 보험사는 법적 위험을 가질 수밖에 없다. 실제 가이드라인 상에도 법령의 제정 및 개정이나 판례의 변경, 그리고 유권해석의 변경에 따라 당해 내용이 변경될 수 있다고 기술되어 있다. 따라서 정부 차원에서 제시한 가이드라인 상 비의료기관에서 제공 가능한 행위를 보다 상위의 개념인 법령으로 입법하여 보험사의 법적 위험을 완화할 필요가 있을 것으로 보인다.

이어서 ②번 보험업법 쟁점을 살펴보면, 건강증진 프로그램을 통해 보험 소비자가 위험을 감소시키는 행위를 하는 경우 그에 대한 정보를 보험사가 수집하여 보험료 할인 등의 혜택을 제공하는 것이 현행 보험업법 제98조의 특별이익 제공 금지에 해당하는지가 문제된다.³⁷⁾ ‘건강증진형 보험상품 가이드라인’상 질병, 사망보험 등 건강관리 노력과 관련된 상품의 경우 웨어러블 기기 구매비용이나 보험료 할인, 캐쉬백 등의 혜택을 허용하고 있다. 그러나 현행 보험업법 제98조에서는 대통령령으로 정하는 금액을 초과하는 금품의 지급을 금지하고 있어 보험료 할인 이외에, 소비자의 노력으로 인한 위험 감소에 대한 인센티브로서 금전을 지급하는 것을 원칙적으로 금지하고 있다. 현행 보험업법 시행령에서는 보험계약 체결 시부터 최초 1년간 납입되는 보험료의 100분의 10과 3만원 중 적은 금액을 “대통령령으로 정하는 금액”으로 하고 있어 이를 초과하는 금액에 대한 페이백이 불가능한 상황이다. 보험 계약을 지속하지 않는 소비자의 경우에는 보험료 할인이 아닌 페이백을 통해서 자신의 건강관리 노력에 대한 보상을 받아야 하는데, 현행법상 이러한 소비자들이 건강증진 프로그램을 통한 혜택을 온전히 누리지 못할 우려가 있다. 이는 건강증진형 보험상품 가이드라인에 기술된 건강증진형 보험상품 활성화의 5대 기본원칙 중 ‘위험 감소의 혜택은 계약자에게 충분히 환급해야 한다.’는 제1원칙에도 반한다. 특정한 건강보험의 경우 보험 소비자가 어떠한 행위를 하느냐에 따라 위험의 빈도와 심도를 크게 낮출 수 있는데, 현행법은 이러한 소비자에 대한 마땅한 보상을 제한하고 있다는 점에 문제가 있다. 따라서 이러한 보험업법 규정을 개정하거나

36) 보건복지부, “비의료 건강관리서비스 가이드라인”, pp.3. 2019.05.

37) 「보험업법」 제98조 제1호.

시행령의 기준을 완화함으로써 페이백 가능범위를 확장할 필요가 있을 것이다.

(2) 의료법 쟁점에 관한 제정 방안

1) 현행

현행 의료법 제27조 제1항은 의료인이 아니면 누구든지 의료행위를 할 수 없다고 규정하고 있다. 따라서 사물인터넷을 활용한 보험사의 건강증진 프로그램이 의료행위에 해당된다고 해석되는 경우 이는 위법한 것이 된다. 보험사의 건강증진 프로그램 중 현행 가이드라인 상으로 의료행위에 해당되지 않는다고 해석되는 것은 법령으로도 입법하여 예측 가능성을 높일 필요가 있다.

2) 제정안 및 기대효과

가이드라인의 내용을 입법에 반영하여 법제화하고 보험사 및 서비스 개발과 관련된 이해관계자들의 법적 예측 가능성을 확보할 필요가 있을 것이다.

제정안은 다음과 같다.

제정안
제3조의6(비의료기관) ① 이 법에서 “비의료기관”이란 제3조의 의료기관에 해당하지 않고 건강관리서비스를 제공하는 것을 업으로 하는 곳을 말한다. ② 비의료기관은 다음 각 호와 같이 구분한다. 1. 체육시설을 통하여 건강관리서비스를 제공하는 자 2. 소프트웨어 개발을 통하여 건강관리서비스를 제공하는 자 3. 보험 상품을 통하여 건강관리서비스를 제공하는 자
제27조의2(비의료기관이 제공 가능한 건강관리서비스) ①비의료기관은 다음 각호의 건강관리서비스를 보건복지부령으로 정하는 범위에서 제공할 수 있다. 1. 건강정보의 확인 및 점검 2. 객관적 정보의 제공 및 분석 3. 건강목표 설정 및 관리

4. 상담·교육 및 조언

② 제1항에도 불구하고 보건복지부령으로 정하는 일부 질환군 및 만성질환에 대하여는 의료인의 판단·지도·감독·의뢰 하에서만 건강관리서비스를 제공할 수 있다.

위 입법이 이루어질 경우, 다음과 같은 효과가 기대된다. ① 총칙상 의료기관과 구분되는 비의료기관을 명시함으로써 체육시설업, 소프트웨어 개발업, 보험업에 종사하는 자가 법적 확신을 바탕으로 의료행위와 구분되는 건강관리서비스를 제공할 수 있게 된다. ② 비의료기관이 제공 가능한 건강관리서비스의 유형을 제시하되, 각 유형의 구체적 범위는 보건복지부령에 위임함으로써, 전문적이고 기술적인 사항에 관하여 관련 부처가 상황에 따라 유동적인 개정할 수 있게끔 한다. ③ 일부 질환군 및 만성질환에 대한 건강관리서비스는 의료인의 통제를 받도록 하여 의료법 개정에 따른 부작용을 방지한다. ④ 의료 비용이 GDP에서 차지하는 비중이 증가하고, 고령화 사회로 진입한 최근의 국내 상황을 고려하였을 때, 보험산업의 한계를 극복하고 국민 건강 수준도 크게 향상시킬 수 있을 것으로 기대되는 건강증진형 보험상품을 판매할 법적 근거를 마련한다는 점에서 의의가 있다.³⁸⁾

(3) 보험업법 쟁점에 관한 개정 방안

1) 현행

현행 보험업법 제98조 제1호는 보험사가 보험 계약자나 피보험자에게 금품을 제공하거나 제공하기로 약속하는 것을 금지하고 있다. 이 규정으로 인해 건강증진 프로그램을 결합한 보험상품에 있어서 보험료 할인 이외에 금전을 환급해주는 형태의페이백이 법적으로 제한받고 있다. 이 규정은 건강관리를 통해 위험 감소에 기여한 소비자에게 합당한 혜택이 돌아가는 것을 부당하게 제한하고 있으므로 개정이 필요하다.

2) 개정안 및 기대효과

38) 주현지, “보건의료비 GDP 대비 2배 경충... 서글픈 고령화 사회”, 디지털타임스, 2019.05.19. <www.dt.co.kr/contents.html?article_no=2019052002100351037001> 2019.8.30. 최종방문.

보험업법 제98조 제2항을 추가하여 제1항 제1호에도 불구하고 위험 감소에 기여한 보험계약자에게는 금전을 환급할 수 있도록 개정하여야 한다.

개정안은 다음과 같다.

현행	개정안
제98조(특별이익의 제공 금지) 보험계약의 체결 또는 모집에 종사하는 자는 그 체결 또는 모집과 관련하여 보험계약자나 피보험자에게 다음 각 호의 어느 하나에 해당하는 특별이익을 제공하거나 제공하기로 약속하여서는 아니 된다. 1. 금품(대통령령으로 정하는 금액을 초과하지 아니하는 금품은 제외한다) 2. 3. 4. 5. 6. 7. 생략	제98조(특별이익의 제공 금지) ① 보험계약의 체결 또는 모집에 종사하는 자는 그 체결 또는 모집과 관련하여 보험계약자나 피보험자에게 다음 각 호의 어느 하나에 해당하는 특별이익을 제공하거나 제공하기로 약속하여서는 아니 된다. 1. 금품(대통령령으로 정하는 금액을 초과하지 아니하는 금품은 제외한다) 2. 3. 4. 5. 6. 7. 생략 ② 제1항 제1호에도 불구하고 보험계약의 체결 또는 모집에 종사하는 자는 그 체결 또는 모집과 관련하여 보험계약자나 피보험자에게 그 보험계약이 보장하는 위험의 감소에 기여한 대가로 금품을 제공하거나 제공하기로 약속할 수 있다.

위 입법이 이루어질 경우, 다음과 같은 효과가 기대된다. ① 사물인터넷을 활용한 건강증진형 프로그램 보험상품의 핵심을 이루는, 보험 소비자에 대한 혜택 제공이 합법화된다. 기존에는 위험 감소에 기여한 경우에도 보험료 할인 등 제한적인 방식으로만 혜택 제공이 가능하였다. 그렇지만 개정 시 웨어러블 기기의 구매비용이나 현금 페이백 등 다양한 방식의 혜택 제공이 원활해질 것으로 기대된다. ② 혜택 제공의 방법이 다양화됨에 따라 사물인터넷을 활용한 건강증진 보험상품도 보다 다양한 유형으로 출시되어 보험사의 이익과 보험소비자의 위험 감소 및 효용 증진에 기여할 수 있을 것으로 기대된다.

3. AI(Artificial Intelligence)를 활용한 보험모집 및 업무 자동화

(1) 법적 쟁점

AI(Artificial Intelligence)는 4차 산업혁명 시대의 핵심 쟁점 중 하나로, 산업 전 방위에 걸쳐서 인공지능이 미칠 영향은 매우 크다. 보험업을 포함한 금융업에서도 인공지능의 역할에 대한 많은 논의가 이루어져 왔다. 그 중, 대표적인 것인 보험업에서 AI를 바탕으로 한 로보어드바이저 활용에 대한 논의이다. 로보어드바이저는 다음과 같이 4단계로 나눌 수 있는데, 어느 수준까지 전통적 보험산업에 개입할 수 있는가가 핵심 쟁점이 되어왔다.

<표 4> 로보어드바이저(RA, Robo-advisor)를 활용한 서비스 유형 구분³⁹⁾

	고객(자문형)	금융회사(일임형)
RA Back office 활용	(1단계) 자문인력이 RA의 자산배분 결과를 활용하여 고객에게 자문	(2단계) 운용인력이 RA의 자산배분 결과 활용하여 고객 자산 직접 운용
RA Front office 서비스	(3단계) RA가 사람의 개입 없이 자산배분 결과를 고객에게 자문	(4단계) RA가 사람의 개입 없이 고객자산을 직접 운용

기존 자본시장과 금융투자업에 관한 법률(이하 ‘자본시장법’)에 따르면 투자권유자문인력·투자운용인력이 아닌 자는 투자자문이나 투자일임 업무를 수행할 수 없도록 정하고 있었다.⁴⁰⁾ 엄격하게 담당자를 분리하여 책임을 명확히 하고, 부작용을 최소화하고자 하는 입법의도를 담은 것이다. 이러한 법률에 의하여 얼마 전까지 로보어드바이저(Robo-advisor, 이하 ‘RA’)는 후선에서 간접적인 업무수행만 가능한 상태였다. RA는 사람이 아니기 때문에 유사한 판단 능력이 존재한다 하더라도 ‘투자권유자문인력’ 또는 ‘투자운용인력’으로 분류될 수 없었고, 사람이 업무를 수행하는 과정에서 말 그대로 자산배분 결과를 제공하는 정도의 보조 수단으로 여겨져 왔다.

39) 금융위원회, “금융상품 자문업 활성화 방안”, pp. 11. ,2016.

40) 자본시장법 제98조 제1항 제3호. 다만 시행령에서 예외 사유를 정할 수 있도록 하고 있으나, 2017년의 개정 전까지는 시행령상 자본시장법 제98조 제1항 제3호에 대한 예외 사유 조항이 없었다.

그러나 2017년 5월 8일 자본시장법 시행령 및 금융투자업규정이 개정되었다. 해당 개정에 따르면 일정 요건을 갖춘 RA가 사람의 개입 없이 직접 고객에게 투자자문이나 투자일임 서비스를 제공하는 것이 가능하다. 구체적으로 법령에서는 전자적 투자조언장치⁴¹⁾를 활용하여 일반투자자를 대상으로 투자자문업 또는 투자일임업을 수행하는 경우⁴²⁾ 예외적으로 허용하고 있다.

현재 보험업법에서는 “모집을 할 수 있는 자는 다음 각호의 어느 하나에 해당하는 자이어야 한다”고 밝히고 있다. 각호에서는 보험설계사, 보험대리점, 보험중개사, 보험회사의 임원 또는 직원을 밝히고 있다. 보험회사 역시 금융업과 유사한 소비자 보호를 위해 보험모집에 관한 수수료 등 지급을 최대한 금지하고 있다. 즉, 금융법과는 달리 현행 보험법상으로는 인공지능(AI, Artificial Intelligence)을 활용해 보험모집 행위를 할 수 있다고 밝히지 않고 있다.

현행 법령을 해석하건대, 보험업법 제83조에서 밝히고 있는 자가 인공지능을 활용해 보험모집을 하는 것에 대한 별도의 규제는 없는 것으로 보인다. 그러나 인공지능이 기능, 분석결과를 제공하는 수준을 넘어서 직접 보험모집 행위를 볼 수 있는 단계에 이르는 것은 추가적인 법적 근거 조항이 필요할 것으로 본다는 것이 기존 법령에 대한 해석이었다.

(2) 개정 방안

1) 현행

그러던 중, 2019년 5월 AI인슈어런스 로보텔러 업체인 페르소나시스템에 대해 혁신성을 인정하여 보험업법 제83조 1항 제1호에 대한 규제 샌드박스를 허용했다. 다만, 소비자 보호 등을 위해 AI를 통한 최대 모집 건수는 연간 1만 건으로 한정하며

41) 자본시장법 시행령 제2조의 제6호에 따르면 다음의 요건을 갖추어야 한다.

가. 활용하는 업무의 종류에 따라 다음의 요건을 갖추 것.

1) 집합투자재산을 운용하는 경우: 집합투자기구의 투자목적·투자방침과 투자전략에 맞게 운용할 것

2) 투자자문업 또는 투자일임업을 수행하는 경우: 투자자의 투자목적·재산상황·투자경험 등을 고려하여 투자자의 투자성향을 분석할 것.

나. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제7호에 따른 침해사고(이하 “침해사고”라 한다) 및 재해 등을 예방하기 위한 체계 및 침해사고 또는 재해가 발생했을 때 피해 확산·재발 방지와 신속한 복구를 위한 체계를 갖추 것.

다. 그 밖에 투자자 보호와 건전한 거래질서 유지를 위해 금융위원회가 정하여 고시하는 요건을 갖추 것

42) 자본시장법 시행령 제99조 제1항 제1조의2.

DB손해보험을 통해서만 판매하고, 체결된 계약 전건에 대해 통화품질 모니터링을 실시하는 것, 여기서 발생하는 모든 민원, 분쟁과 소송 등은 DB손해보험이 1차 책임자로 전담 처리할 것 등의 부가조건을 붙여 혁신금융서비스로 지정했다. 부가조건을 통해 상대적으로 취약해질 수 있는 소비자 보호를 제고하고자 한 것이다. 물론 소비자도 위험만을 부담하는 것은 아니다. 인공지능을 통한 24시간 보험계약 모집으로 소비자가 원하는 시간에 언제든지 상담, 계약 체결이 가능해 소비자 편의의 증대가 가능하다.

현재 DB손해보험과 페르소나시스템의 경우, 위 III에서 언급하였던 규제 샌드박스(Regularity Sandbox) 형태의 방식을 채택한 것으로 보인다. 그러나 AI를 활용한 보험모집과 업무 자동화는 빠르게 업계 전반으로 확대될 가능성이 높다. 이에 대해서 매번 심사를 통해 규제 샌드박스를 도입하는 것은 비경제적일 수 있다. 또한, 각기 다른 심사를 거친 RA가 난립할 경우 오히려 시장에 혼란을 초래할 수도 있다는 단점도 갖고 있다. 물론 현 시점에서는 본 규제 샌드박스를 통해 관련 법령이 더욱 구체적으로 정해질 수 있을 것으로 기대되나, 본 연구에서는 현재 수준에서 유의미한 개정 방안을 제안함으로써 입법의 촉진을 목표로 한다.

2) 개정안 및 기대효과

이미 2017년 1월 12일 EU 의회에서는 AI와 로봇을 둘러싼 여러 가지 현안을 해결하여 관련 산업을 촉진하기 위한 내용을 담은 로봇 결의안을 통과시킨 바 있다. 해당 결의안에서는 향후 가장 정교화된 자율 로봇(the most sophisticated autonomous robot)에게는 전자적 인간(electronic person)으로서의 법적 지위를 창설하는 것을 고려할 수 있다는 내용이 포함되어 있었다.⁴³⁾ 이러한 점들을 고려하여 현행법의 개정안을 제안하고자 한다.

이를 위해서 보험업법 제99조의 개정 또는 시행령·시행규칙 개정을 통해서 근거 규정을 두는 방식을 선택할 수 있을 것이다. 본 개정안에서는 제99조의 개정안을 제안하도록 한다.

개정안을 포함한 신규대조표는 다음과 같다.

43) European Parliament, "Report with recommendations to the Commission on Civil Law Rules on Robotics, 59.f)항", <http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html>

현행	개정안
<p>제99조(수수료 지급 등의 금지) ① 보험회사는 제83조에 따라 모집할 수 있는 자 이외의 자에게 모집을 위탁하거나 모집에 관하여 수수료, 보수, 그 밖의 대가를 지급하지 못한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.</p> <p>1. 2. 생략</p> <p>3. 그 밖에 대통령령으로 정하는 경우</p> <p>② 모집에 종사하는 자는 다음 각 호의 어느 하나에 해당하는 경우 이외에는 타인에게 모집을 하게 하거나 그 위탁을 하거나, 모집에 관하여 수수료·보수나 그 밖의 대가를 지급하지 못한다.</p> <p>1. 보험설계사: 같은 보험회사등에 소속된 다른 보험설계사에 대한 경우</p> <p>2. 보험대리점: 같은 보험회사와 모집에 관한 위탁계약이 체결된 다른 보험대리점이나 소속 보험설계사에 대한 경우</p> <p>3. 보험중개사: 다른 보험중개사나 소속 보험설계사에 대한 경우</p>	<p>제99조(수수료 지급 등의 금지) ① 생략</p> <p>1. 2. 생략</p> <p>3. <u>전자적 투자조언장치를 활용한 투자 보조업무</u></p> <p>4. 그 밖에 대통령령으로 정하는 경우</p> <p>② 생략</p> <p>1. 보험설계사: 같은 보험회사등에 소속된 다른 보험설계사에 대한 경우</p> <p>2. 보험대리점: 같은 보험회사와 모집에 관한 위탁계약이 체결된 다른 보험대리점이나 소속 보험설계사에 대한 경우</p> <p>3. 보험중개사: 다른 보험중개사나 소속 보험설계사에 대한 경우</p> <p>4. <u>전자적 투자조언장치: 대통령령으로 정하는 요건을 충족한 전자적 투자조언장치에 대한 경우</u></p>

위 입법이 이루어질 경우, 우선 ① 업무 프로세스 간소화가 가능하다. 대표적인 경우가 업무 자동화다. 한 예로 최근 DB손해보험은 ‘RPA(Robot Process Automation)’ 시스템을 도입했다. RPA는 PC 기반으로 업무를 수행하는 사람 행동을 로봇 소프트웨어가 동일하게 모방해 자동으로 업무를 수행할 수 있게 도우며, 보고서 작성, 계약관리, 전자문서관리, 자료수집, 모니터링, 지수 업데이트 등 총 28개의 업무가 RPA를 통해 수행할 수 있다. 이를 통해 연간 약 2만9000시간이 절감될 것으로 예상된다.⁴⁴⁾

② AI 기술을 활용하여 보험 체결 건수 증대 및 저렴한 보험의 공급이 가능하다. 중국 중안보험⁴⁵⁾은 AI 기술, 특히 머신러닝을 활용해 개별적인 개인 맞춤형 보험 상품, 특히 게임아이템이나 인터넷 결제 안전보험 등을 판매하고 있다. 더불어 AI를 활용해 보험료 산출과 인수 심사, 보험금 지급 등 대부분 업무를 자동화해 인건비의 64%를 절감하였다. 중안보험 직원 1인당 보험 체결 건수는 89만 건으로 한국 보험사 직원이 1인당 2천700건을 체결하는 것에 비해 329배로 매우 높은 수치를 보였다. 중안보험은 인공지능, 빅데이터 등을 활용해 보험상품 고객 맞춤화, 고객의 상황에 맞는 가격 책정이 가능해졌고, 1인당 보험료가 28위안(4천800원) 상당의 고객 맞춤형 소액보험 상품을 출시하는 성과를 달성하였다.

③ 더불어 AI를 활용한 머신 러닝 예측 모델을 보조하여 다양한 보험상품의 손해를 등을 줄이고 있다. DB손해보험의 경우, 이를 통해 자동차보험의 손해율에 악영향을 끼칠 수 있는 물건(계약)을 기존보다 2배 가량 더 많이 찾아내는 결과를 보이기도 했다. 구체적으로 개인 대상 자동차보험 영업채널에 대해 각 11개의 예측 모델을 생성했다. 사고발생률, 건(件) 당 손해액, 대(臺) 당 손해액 등을 기반으로 모델을 제작하여 활용하였다.⁴⁶⁾

4. 빅데이터를 활용한 위험 분석

(1) 법적 쟁점

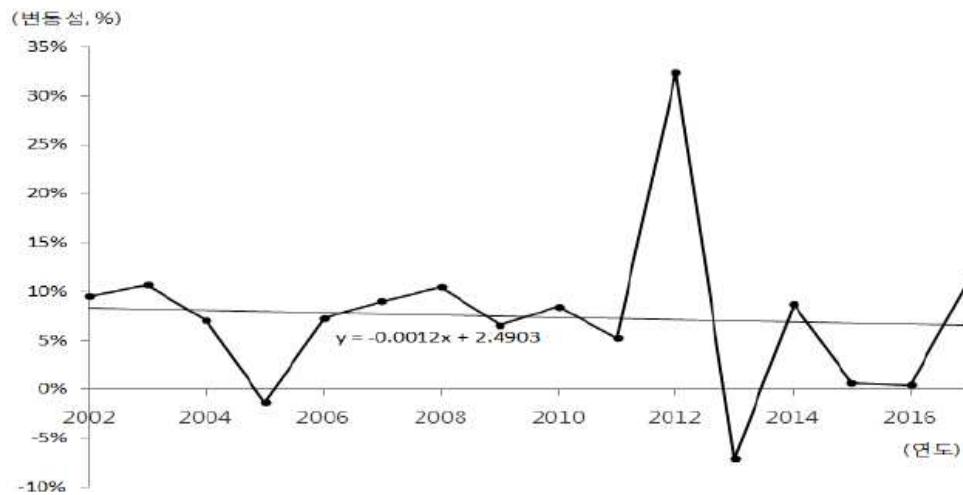
빅데이터는 기존의 방식으로 다루기 어려운 수준의 복잡하고 많은 양의 데이터를 의미한다. 빅데이터의 대표적인 특성으로는 주로 5V(Volume, Variety, Velocity, Variability, Veracity)를 꼽고 있다. 즉, 데이터의 양과 자료의 다양성, 자료의 생성 및 처리 속도, 정보의 변동성, 신뢰성 부족 등이 핵심 요소이다. 빅데이터는 인공지능과 이를 활용한 머신러닝, 그리고 통계 등 다양한 분야와 결합하여 그 의미가 확장된다. 이러한 빅데이터가 인슈어테크에서 어떠한 의미를 갖는지는 다음 논의를 통해서 확장하도록 한다.

44) 배준희, “‘변해야 산다’ 보험 CEO ‘인슈어테크’ 혁신 바람-로봇이 보험심사·계약…빅데이터로 상품화”, 매일경제, 2019.05.13. <<https://www.mk.co.kr/news/business/view/2019/05/312035>> 2019.8.24. 최종방문.

45) 중안보험은 2013년 10월 설립된 온라인 손해보험사로 알리바바(19.9%), 텐센트(15%), 평안보험(15%)등이 합해 설립한 회사다.

46) 손예술, “‘인슈어테크’ 시대 성큼…보험사 경쟁력 AI가 가른다”, ZDNet Korea, 2019.05.14. <<https://www.zdnet.co.kr/view/?no=20190514145755>> 2019.8.24. 최종방문.

<그림 6> 보험업 수익 변동성⁴⁷⁾



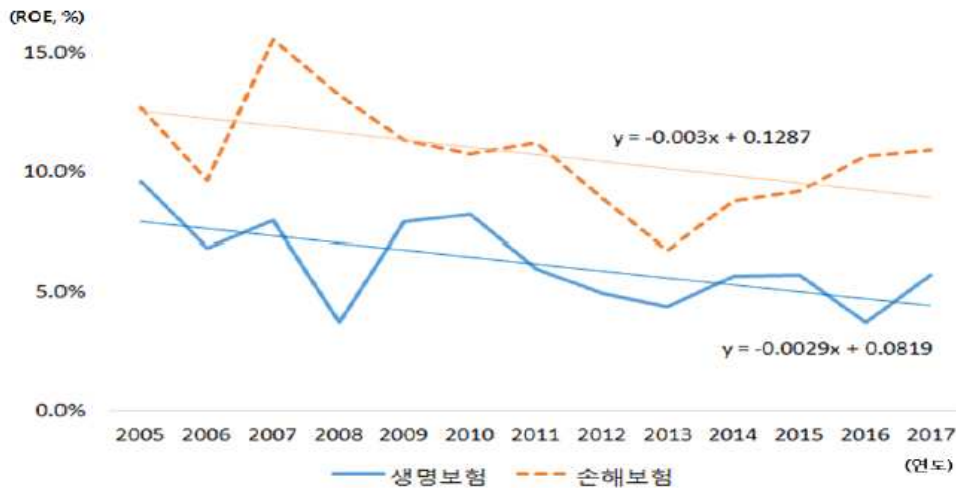
주: 국내 생명 손해 보험회사의 보험영업 수입+투자 수입의 연도별 변화율임. 2012년의 급격한 상승은 연금보험 판매 급증에 의한 것이며, 2013년의 감소는 회계제도 변화(FY→CY)에 의한 것이었음.

자료: 금융감독원, 금융통계시스템

현재 우리나라 보험산업은 성장이 정체된 상태이다. 위에서 볼 수 있듯이 2002년부터 2008년까지 꾸준한 성장을 보인데 반해, 금융위기를 겪은 이후에는 경제 성장의 둔화와 시장 내 불안감 확산, 시장 포화 등으로 인하여 성장폭이 크게 감소한 상태이다. 결국 이러한 영향으로 인하여 보험산업 내의 자본 대비 수익률(ROE)의 경우 감소하고 있는 추세이다.

47) 최창희·홍민지, “빅데이터 활용 현황과 개선 방안”, 보험연구원, pp. 12. 2018.12.

〈그림 7〉 보험산업 ROE(당기순익/자본)⁴⁸⁾



주: 손해보험은 장기보험을 취급하는 종합손해보험회사만 취함함

자료: 금융감독원, 금융통계시스템

이러한 상황 속에서 보험사에게 빅데이터를 활용한 인슈어테크는 매우 매력적인 수단이 된다. 빅데이터를 활용함으로써 전통적인 보험시장에서는 발견되지 않았던 시장을 찾아내 규모를 확대할 수 있으며, 적절한 곳에 비용을 투자함으로써 효율화를 달성할 수도 있다. 또한, 데이터를 통해 정보 비대칭이나 역선택 등의 문제를 해결함으로써 적절한 상품을 개발할 수 있다는 장점도 있다. 실제로 해외에서는 이미 상품개발과 인수 심사, 고객 서비스 개선, 보험사기 예측, 리스크 관리 등에 적극적으로 활용하고 있다.

국내에서는 2016년 오렌지라이프가 빅데이터 미래창조과학부와 한국정보화진흥원 주관 하에 마케팅, 보유계약관리, 보험사기예측, 리스크 관리 모델을 구축한 바 있으며 한화생명 등도 이와 같이 빅데이터의 활용 방안에 대하여 연구하였으며 실제 활용하고 있기도 하다.

그러나 국내는 해외에 달리 많은 보험사들이 규제의 장벽에 부딪히고 있다. 이러한 문제의 원인으로는 전무 인력의 조달, 내부 관리 체계의 부실 등이 꼽히고 있으나, 이보다 큰 문제는 엄격한 개인정보보호법으로 인해 애초에 데이터 자체의 확보가 어렵다는 것이다.

48) 최창희·홍민지, 위의 글, pp. 13.

(2) 개정 방안

1) 현행

현행 개인정보보호법은 ‘개인정보’의 의미를 ‘“개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)’를 말한다.⁴⁹⁾ 고 하여 매우 포괄적으로 정의하고 있으며, 개인정보의 제공을 엄격하게 규제하고 있다. 보험회사의 빅데이터 사용은 개인정보보호법 외에도 「신용정보의 이용 및 보호에 관한 법률」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」과도 밀접한 관계에 있다. 3개 법률은 모두 징벌적손해배상과 법정손해배상 조항을 포함하고 있어 고의 또는 중대한 과실로 개인정보가 유출된 경우에 개인정보처리자에게 실제 발생한 손해 이상의 손해배상책임을 부과할 수 있으며, 피해자의 증명이 없더라도 법원이 정해진 범위 내에서 손해배상금을 정할 수 있기 때문에 상당한 책임을 부담하게 되어 있다.

개인정보 유출사고로 인한 피해 등을 고려할 때, 엄격한 책임이 필요한 부분이 있으나 현재는 기업들은 사실상 빅데이터를 활용하기 어렵다. 자유롭게 데이터가 이동하기 어려우며 진정한 의미의 빅데이터 구축 자체가 어려운 상황이다. 그나마 금융지주회사 계열 보험회사는 다양한 자회사를 갖고 있기 때문에 데이터의 확보가 가능하나, 독립법인으로 존재하는 회사 또는 영세한 스타트업 등의 경우에는 애초에 빅데이터 확보 자체가 어려워 해당 분야의 혁신을 추구하기 어려운 상황이다. 일부 주어지는 공공데이터 등을 활용하더라도 각 보험업 내부의 주체가 원하는 데이터를 충분히 확보할 가능성은 매우 낮다.

2) 개정안 및 기대효과

따라서 개인정보보호법의 개정을 통해서 기업들이 빅데이터 공유를 촉진함과 동시에 소비자 보호를 달성할 수 있도록 할 필요가 있다. 이에 대한 필요성에 공감한 금융위원회는 지난 2018년 3월, ‘금융분야 데이터활용 및 정보보호 종합 방안’을 발표하기도 하였다. 그러나 이미 지난 몇 년간 국내와 해외의 환경 차이로 인하여

49) 「개인정보보호법」 제2조 제1항.

빅데이터 산업 관련 경쟁력은 격차를 보이게 되었다. 따라서 이를 해결하기 위하여 기존 연구를 바탕으로 법령의 개정과 특별법 제정 방안을 제안한다.

기존 법령의 개정 방안은 다음과 같다.⁵⁰⁾

현행	개정안
제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.	제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 처리할 수 있다.
제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다. 1. 정보주체의 동의를 받은 경우 2. 제15조제1항제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우	제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다. 1. 정보주체의 동의를 받은 경우 2. 제15조제1항제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

위의 제15조에 대한 개정안의 ‘처리’는 수집·생성·이용·제공·공개 등을 모두 포함한다. 기존 우리나라 개인정보보호법이 개인정보의 제3자 제공을 원칙적으로 금지하고 있기 때문에 위와 같은 규정의 변화를 통해 보다 넓게 처리할 수 있는 가능성을 열어두는 것을 입법의 목적으로 하였다.

이 외에도 2018년 8월에 있었던 ‘규제혁신점검회의’ 등의 내용을 바탕으로 특별법 제정을 하는 것도 검토해 볼 만한 방안이 될 수 있다. EU 입법 사례를 통해 볼 때, 익명정보와 가명처리정보 개념을 도입하고 데이터에 대한 처리는 비교적 자유롭게 허용하는 특별법을 둬으로써 개인정보보호와 빅데이터 산업 활성화 목적을 얼마간 달성할 수 있을 것으로 보인다. 구체적으로 비식별조치를 통해 익명정보의 경우, 개인정보보호법 적용 대상에서 예외로 삼는 방안이 있다. 구체적으로 다음과 같

50) 이인호, “개인정보보호법제의 시급한 개선과제”, 법연, Vol 58, No.6. pp.1-4. 한국법제연구원, 2018. 3.

은 단계를 거치게 된다.

〈표 5〉 비식별 조치 및 사후관리 절차⁵¹⁾

단계	조치사항	내용
1단계	사전 검토	개인정보에 해당하는지 여부를 검토 후, 개인정보가 아닌 것이 명백한 경우, 법적 규제 없이 자유롭게 활용
2단계	비식별 조치	정보집합물(데이터 셋)에서 개인을 식별할 수 있는 요소를 전부 또는 일부 삭제하거나 대체하는 등의 방법을 활용, 개인을 알아볼 수 없도록 하는 조치
3단계	적정성 평가	다른 정보와 쉽게 결합하여 개인을 식별할 수 있는지를 「비식별 조치 적정성 평가단」을 통해 평가
4단계	사후 관리	비식별 정보 안전조치, 재식별 가능성 모니터링 등 비식별 정보 활용 과정에서 재식별 방지를 위해 필요한 조치 수행

위의 1단계에서 3단계에 이르는 과정, 즉 3단계에서 ‘적정’ 평가를 받기 전에는 그 개인정보를 ‘그 자체로 특정 개인을 알아볼 수 있는 정보(다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보 포함)’로 보는 것으로 한다. 그러나 3단계에서 ‘적정’ 평가를 받은 이후부터는 비식별 정보로서 더 이상 개인정보가 아닌 것으로 추정한다. 단, 이 경우에도 다른 정보와 결합하여 재식별 되지 않도록 필수적인 관리조치를 이행해야 한다는 조건을 부가해야 한다. 이러한 과정을 통해 개인정보를 비식별정보로 확정하게 됨에 따라, 산업 일선에서 데이터를 활용할 수 있는 가능성이 크게 증가할 것으로 예상된다.

현재는 비식별 조치에 대하여 명확한 법제화가 부족한 상태나, 정부가 2018년 8월의 ‘규제혁신점검회의’에서 이에 대한 법제화 의사를 밝힌 만큼 특별법의 형태로 제정하여 특례 규정을 두는 것이 타당할 것이다. 이 외에도 특별법을 통해 특수한 경우에는 규제 샌드박스를 통해 빅데이터를 처리할 수 있는 통로 역시 마련해 두어야 할 것이다.

개정을 통한 효과를 달성하기 위해서는 입법뿐 아니라 행정적 측면의 접근도 필요하다. 금융위원회는 지난 6월 ‘금융 빅데이터 인프라 오픈 행사’에서 ‘금융분야 빅데이터 거래소’의 설치에 대해 발표한 바 있다.

51) 한국인터넷진흥원, “개인정보 비식별 조치 가이드라인”, pp. 3. 2018.

〈그림 8〉 금융분야 원스톱 데이터 거래소⁵²⁾



거래소를 통해 인슈어테크 기업과 금융회사, 스타트업, 대학 및 연구소 등은 신사업 모델을 개발하거나 연구를 할 때 사용할 금융 데이터를 사고 팔 수 있다. 이는 올해 내로 금융보안원 내에 설립되어 시범 거래가 예정되어 있다. 거래소의 설치에 관하여는 입법을 통해 장기적인 운영을 위한 가이드라인을 확정할 필요가 있을 것으로 보인다. 이러한 거래소 설치를 통해 건전성을 유지하며, 활발하게 빅데이터 분야의 산업과 혁신을 달성할 수 있을 것이다.⁵³⁾

5. 블록체인을 활용한 보험금 청구 간소화 및 모바일 증권 진위 판별

(1) 법적 쟁점

블록체인(Blockchain)은 중앙집중형 네트워크와 달리 네트워크 참여자 모두가 정보를 공유하는 분산형 네트워크의 특징을 가지는 것으로, 분산원장 기술(DLT: Distributed Ledger Technology)이라고 불리기도 한다. 이는 과거에 중앙집중형 네트

52) 금융위원회, “금융분야 데이터 주요 인프라 구축방향”, pp. 13. 2019.6.3.

53) 김영기, “[금융보안원 김영기 원장] 데이터 혁명으로 가는 길 ‘금융보안’”, 한국금융, 2019.6.24.

워크만을 공약하면 쉽게 위·변조할 수 있던 것에 반해, 모든 참여자의 정보를 속여야 하므로 위·변조가 거의 불가능하며, 자연스럽게 신뢰성과 투명성이 높다.

이러한 특징 때문에 보험업계에서는 블록체인을 현장에서 활용하고자 노력하고 있다. 보험업계를 포함한 전통 금융회사들은 중앙 서버에 거래 기록을 보관해 왔는데, 블록체인 기술을 도입하면 거래 정보를 P2P(Peer to Peer) 방식을 기반으로 블록에 담아 차례로 연결하여 모든 참여자가 공유하게 된다. 이를 통해 보안성 강화, 처리과정에서의 신뢰성 증진, 그리고 감시가능성의 확대와 비용 절감 등의 긍정적 효과를 달성할 수 있다.⁵⁴⁾

그러나 이 과정에서 개인정보보호법, 전자금융거래법 등과 관련된 블록체인의 적용 대상과 효력, 안전성, 책임 등의 민감한 문제들이 산재해 있어 이를 해결할 필요성이 존재한다.

(2) 해결 방안

1) 현행

특히 보험사가 거래 내역을 독점적으로 처리하는 현재, 우리나라는 소비자가 보험계약 체결과 수익자 변경을 비롯한 다양한 업무를 처리할 때마다 보안을 위해서 반복적으로 공인인증서를 통한 본인인증을 진행해야 한다. 이는 매우 비효율적이고 보험서비스 전반에 대한 접근성을 낮추는 요인 중 하나가 되고 있다.⁵⁵⁾

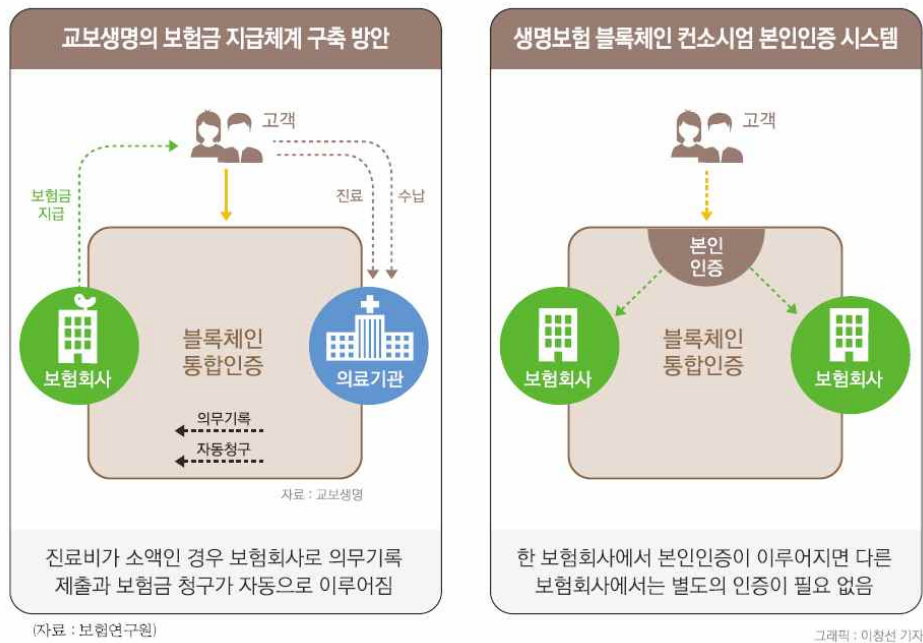
해당 분야에 블록체인 기술을 활용한다면 소비자는 최초 1회 블록체인 내에서 본인 인증함으로써 보험계약 만료시까지 신분을 보장받을 수 있으며, 이는 경제성과 편의성 측면에서 획기적인 혁신이 될 것이다. 또한 보험금 청구 과정에서 검증이 신속하고 안전하게 이루어질 것이며, 진위 판별이 용이해진 모바일 증권의 유통도 활발해질 수 있을 것이다.

국내에서도 ‘교보생명’이 보험금 지급에 대하여 블록체인 기술을 활용하였다.

54) 김현수·권혁준, “보험산업의 블록체인 활용: 점검 및 대응”, pp 14. 보험연구원, 2018.11.

55) 방영석, “보험업계 블록체인 기술 활용 모호한 기준에 ‘발목’”, 보험매일, 2018.04.23.
<<http://www.fins.co.kr/news/articleView.html?idxno=77683>> 2019.8.24. 최종방문.

〈그림 9〉 교보생명 블록체인 기반 인증 시스템⁵⁶⁾



위와 같은 과정을 통해 블록체인 기술을 활용하여 본인인증을 간소화시키고 이전 보다 보험금 청구과정을 신속하고 편리하게 진행할 수 있도록 하였다. 뿐만 아니라 블록체인을 통해 고객이 병원 등 의료기관에서 진료를 받고 수납을 하면 병원에서 보험 계약자 확인을 진행해 보험회사로 의무기록 제출과 보험금 청구가 자동으로 이루어지는 시스템을 만들었다. 즉, 보험회사와 의료기관 두 곳에서 이중으로 본인 인증을 해야 하는 불편함이 공동망 구축을 통해 해소될 수 있었다.

2) 해결안 및 기대효과

블록체인이 장기적으로 광범위하게 활용되고 발전하기 위해서는 위에서 언급하였던 개인정보보호법과 전자금융거래법에 대한 개정이 필요할 것이다. 블록체인의 특성상 거래자 다수와 정보를 공유하는 알고리즘이 필수적인데 이 과정에서 개인의 정보를 합법적으로 공유할 수 있도록 하는 방안에 대한 고민이 필요하다. 더불어 만약 블록체인이 적용된 상태에서 악의적 정보 유출이나 기타 사고가 발생할 경우,

56) 김민경, “교보생명발 보험산업 블록체인 혼풍”, 한국금융, 2017.09.25.
 <<http://www.fntimes.com/html/view.php?ud=189485>> 2019.8.24. 최종방문.

그에 대한 책임 소재를 정하는 것도 법으로 사전 규정이 필요한 부분이다. 법규가 미비할 경우, 자칫 해당 블록체인에 참여한 모두가 무한책임을 지는 형태가 될 수도 있기 때문이다. 이는 선의의 참여자에게 지나치게 가혹하다.

더불어 전자금융거래법 및 동법 시행령에서는 적용대상(법 제3조 및 시행령 제2조), 전자자금거래계약의 효력(법 제12조), 안전성의 확보의무(법 제21조), 정보보호 최고책임자의 지정(법 제21조의 2, 시행령 제11조의 3), 전자금융기반시설 취약점 분석·평가(법 제21조의 3, 시행령 제11조의 4) 등을 정하고 있다. 전자금융거래법은 블록체인처럼 분산형 시스템을 염두에 두지 않은 상태이기 때문에 기존 중앙집중형 네트워크 시스템에 적합하게 설계되어 있다.⁵⁷⁾

현재 시점에서 이 모든 사안에 대한 법령을 개정하기는 다소 이를 수 있다. 아직 국내에 블록체인과 관련된 논의가 성숙한 상태는 아니기 때문이다. 블록체인 기술이 어느 정도 확산되고 성숙되었을 때, 비로소 관련 규제의 개정을 논할 수 있을 것이다. 실제 2016년 5월 유럽의회에서도 블록체인에 대해서는 불간섭주의(Hands-off Approach) 결의안(Smart Regulation)을 통과시키고 집행위원회에 제출하였으며, 정부의 선제적 규제(Preemptive Regulations)보다는 세심한 모니터링(Precautionary Monitoring)을 정책 기본 기조로 삼자는 의견이 제시되었다.⁵⁸⁾

우리나라 역시 최근 확산되고 있는 블록체인 컨소시엄과 정부 기관을 중심으로 논의를 지속한 후에 구체적인 입법안을 제시하는 것이 타당할 것이다. 그럼에도 불구하고 정부가 불확실성을 줄이기 위해 적절한 가이드라인을 지속적으로 제시해주는 것이 필요하다. 가이드라인을 통해 규정의 과도기에서 블록체인 기술 경쟁력을 유지함과 동시에 선의의 이용자들을 보호할 수 있을 것이다.

6. P2P 보험의 도입

(1) 법적 쟁점

종래의 보험은 주로 다수의 보험 계약자가 스스로 감당할 수 없는 개별 위험을 거대한 보험사로 전이하고, 보험사는 이러한 위험을 결합함으로써 획기적으로 위험을 감소 혹은 제거하는 방식으로 운영되었다. 하지만 이러한 보험 시스템으로는 정

57) 이대기, “블록체인의 활용과 규제 현황”, pp. 29. 한국금융연구원, 2017.6.

58) 이대기, 위의 글, pp. 25.

보 비대칭에서 기인한 도덕적 해이와 역선택, 그리고 보험 사각지대의 문제를 완전히 해결할 수 없었다. 최근 해외에서는 이를 극복하기 위한 구조적 대안으로 P2P 보험이 등장하기 시작하였다.⁵⁹⁾

P2P 보험은 보험사가 위험을 인수하지 않고, 위험을 공유하려는 소비자들을 상대로 플랫폼을 제공하며 일정한 수수료만을 취하는 형태로 운영된다. P2P 보험에서는 동일한 위험을 회피하고자 하는 지인들을 모아 소규모 그룹을 형성하여 위험을 공유하는 것이 가능하다. 이러한 P2P 보험의 소규모성 때문에 위험 발생의 변동 가능성이 높다는 단점도 있지만 지인 기반으로 형성된 위험 공유 그룹은 정보 비대칭을 획기적으로 낮출 수 있다. 또한 기존에 보험사가 다루기 꺼려하는 보험상품을 소비자가 자발적으로 생산하여 위험을 회피할 수 있다는 장점도 있다. 이처럼 기존 보험의 단점을 확실히 보완할 수 있다는 점에서 P2P 보험이 주목 받고 있다.

P2P 보험은 그 특성에 따라 다음의 네 가지 형태로 분류할 수 있다.⁶⁰⁾ 보험사와 소규모 그룹 사이에서 보험계약을 중개하는 브로커 형(Bought by many 등), 일부 위험에 대하여는 소규모 그룹 자체적으로 커버하고 큰 위험에 대하여는 기존의 보험을 이용하는 일부 손실 공유형(Friendsurance, Guevara, InsPeer 등), 전체 위험에 대하여 소규모 그룹 자체적으로 해결하는 전체 손실 공유형(Teambrella, Cycle Syndicate 등), 원수사는 일정 수수료만을 취득하고 잉여 재원은 가입자 지정 단체에 기부하는 원수사 형(Lemonade 등)이 바로 그 종류이다.

해외에서는 다양한 종류의 P2P 보험이 등장하고 있는데 반해 아직까지 우리나라에서는 P2P 보험 도입이 미비하다. 그 이유는 바로 현행 보험업법 제2조 제2호와 제4조 제1항의 규정 때문이다.⁶¹⁾ 보험업법 제2조 제2호는 보험업을 ‘보험상품의 취급과 관련하여 발생하는 보험의 인수(引受), 보험료 수수 및 보험금 지급 등을 영업으로 하는 것으로 규정하고 있다. 따라서 상기한 P2P 보험의 네 가지 종류 중 최종적으로 보험사가 위험을 인수하는 브로커 형을 제외하면 현행 보험업법이 인정하는 보험업이 아닌 셈이 된다. 그리고 보험업법 제4조 제1항이 보험업을 경영하려는 자는 보험종목별로 금융위원회의 허가를 받아야 한다고 규정하고 있어 P2P 보험을 경영하기 위해서는 금융위원회의 허가도 필요한 상황이다.

59) 김규동, “P2P보험의 특징 및 활용 사례”, 보험연구원, pp. 9-16. 2018. 04.

60) 박소정·박지윤, “인슈어테크 혁명: 현황 점검 및 과제 고찰”, 보험연구원, pp. 56-63. 2017. 08.

61) 「보험업법」 제2조 제2호, 제4조 제1항.

(2) 해결 방안

1) 현행

현행 보험업법의 총칙에 해당하는 규정인 제2조 제2항은 보험업의 정의를 보험상품의 취급과 관련하여 발생하는 보험의 인수, 보험료 수수 및 보험금 지급 등을 영업으로 하는 것으로 규정하고 있다. 또한 보험업법 제4조 제1항은 보험업을 경영하려는 자는 보험종목별로 금융위원회의 허가를 받아야 한다고 규정하고 있다.

2) 해결안 및 기대효과

P2P 보험은 보험산업의 오랜 문제로 지적된 정보 비대칭의 문제를 해소할 수 있을 것으로 기대되며, 특히 위험도가 높아 가입이 거절되거나 상품 자체가 존재하지 않아 보험상품에 가입할 수 없었던 소비자들의 가입을 촉진함으로써 사회 후생을 증진할 것으로 기대된다. 반면 기존의 보험사에 비해 소규모의 인원이 위험을 부담하는 방식으로 운영되기 때문에 변동성이 크다는 단점을 갖는다. 이처럼 P2P 보험은 보험소비자에게 전에 없던 효용을 제공하는 반면에 보험업의 미덕으로 여겨지는 안전성 측면에서는 다소 불확실성을 갖고 있는 것이 현실이다. 따라서 기존의 규정을 개정하는 방식보다는 규제 샌드박스를 통해 한시적으로 규제의 빗장을 풀어줌으로써 P2P 보험이 혁신적이고 안전한 상품으로써 보험산업에 자리 잡을 기회를 부여하는 것이 바람직할 것이다.

이와 관련하여 최근 금융위원회는 금융혁신지원 특별법을 통해 핀테크 분야의 여러 서비스들을 혁신 금융 서비스로 지정하여 규제 샌드박스 대상으로 인정한 바 있다. 보험업계에서는 대표적으로 재가입 시 간단한 절차만으로 계약 체결이 가능한 여행자보험 On-Off 서비스가 인정받은 바 있다.⁶²⁾

따라서 P2P 보험을 경영하고자 하는 기업들 역시 금융혁신지원 특별법 제5조의 혁신금융서비스 지정 신청을 통해 규제 샌드박스를 인정받을 수 있다. 제2조 제1호, 제4조 제2항 제5호에 따르면 혁신 금융 서비스 지정 시 보험업법 일부 규정의 적용을 배제할 수 있다. 금융위원회가 P2P 보험의 서비스 모델을 충분히 검토하여 혁신

62) 차은지, “오늘부터 ‘켰다 끄는’ 여행자보험 가입 시작...새바람 불까”, 한국경제, 2019.6.12. <<https://www.hankyung.com/economy/article/2019061297696>> 2019.8.30. 최종방문.

금융 서비스로 지정한 후에는 2년의 범위 내에서 전술한 보험업법 제2조 제2항과 제4조 제1항의 규정을 적용하지 않을 수 있다.

따라서 보험상품의 취급과 관련하여 발생하는 보험의 인수, 보험료 수수 및 보험금 지급 등을 영업으로 하지 않는 P2P 보험의 경우에도 보험업으로 인정될 수 있고, 혁신금융서비스 지정 후에는 보험 종목별로 금융위원회의 별도 허가를 받지 않더라도 보험업을 경영할 수 있다.

이러한 규제 샌드박스를 선제적으로 활용하고 향후 부작용이 발생한다면 P2P 보험과 관련한 문제를 해결하기 위한 별도의 규정을 기존 보험업법 혹은 특별법으로 법제화하는 방식도 생각해볼 수 있을 것이다. 물론 P2P 보험이 그 가치를 인정받고 하나의 상품으로 충분히 자리잡은 후에는 총칙에 관련 제규정을 신설하여 확실한 법적 근거를 마련하여야 할 것이다.

① P2P 보험 판매의 근거에 있어서 우선 규제 샌드박스의 방식을 선택함으로써 신산업 하에서 발생할 수 있는 문제점을 조기에 파악하고 차후에 이를 충분히 반영한 법제화가 가능하다. ② P2P 보험의 판매가 가능해짐에 따라 정보 비대칭의 문제가 해소된 상품이 개발되고 종래 보험에 가입할 수 없었던 소비자들의 가입을 촉진하여 사회 후생이 증진된다. ③ 부수 효과로 Lemonade와 같은 원수사 형의 P2P 보험은 잔여 이익을 기부에 활용하기 때문에 경우에 따라서는 이로 인한 부의 재분배나 공익 실현에 기여할 수 있다.

V. 결론

지금까지 인슈어테크 산업 발전을 위한 규범 혁신의 필요성과 방법론, 그리고 개정안 및 해결방안에 대하여 검토해보았다. 생활 곳곳에 산재한 여러 종류의 위험을 제거 또는 감소시켜 안전한 사회 형성에 일조하는 보험산업은 예나 지금이나 중요하다. 최근 급속도로 발전하고 있는 4차 산업 혁명 기술을 활용한 인슈어테크를 통해, 보험산업은 본연의 목적을 보다 충실하고도 다각적으로 수행할 수 있을 것이다. 더불어 기존 보험산업에서 소외되었던 집단도 보험으로 인한 효용을 누릴 수 있게 함으로써 공익의 증대도 이끌 수 있다.

본 논문에서도 살펴보았듯이, 인슈어테크 적용과 관련한 법적 문제를 해결하기 위한 방법론의 선택은 매우 중요하다. 기존 법령을 개정하는 방식, 특별법을 제정하

는 방식, 그리고 그 안에 포함되는 규제 샌드박스의 방식 각각 장단점을 갖고 있으며 상황에 따라 어느 것이 가장 적절한 해결책인지는 달라질 수 있기 때문이다. 특히 기존 법률과의 조화나 악용 가능성 등 다양한 변수에 대한 검토를 통해 관련 문제를 해결하기 위한 가장 적합한 방법을 선택하여야 할 것이다.

각 기술의 활용에 관한 법적 문제를 해소함에 있어서 이와 관련된 경제 주체들의 이해관계를 충분히 고려하는 것도 중요하다. 입법기관이나 정부는 구체적인 개정이나 제정 등에 앞서 이해관계자들의 의견을 충분히 수렴하고 이를 반영하려는 노력을 하여야 한다. 현대 사회에서의 법(法)은 단순히 규제를 할 뿐만 아니라, 특정한 가치를 촉진하는 역할을 수행한다. 이처럼 사회 구성원들에게 긴요한 영향을 미치는 법 제정과 개정 과정에서는 가능한 다양한 의견을 수렴하고 실현 가능한 타협점을 찾아나가는 것이 중요하다. 그것은 입법자와 정부의 의무이기도 하다.

기존 제규정에 의해 인슈어테크의 혜택을 온전히 누리지 못하고 있는 보험 소비자와 보험사가 보다 적극적으로 제정 및 개정 검토를 입법기관과 정부에 요청하는 것도 필요하다. 가령 전술한 혁신금융서비스의 경우 제도의 존재만으로 영업의 자유나 그 효과가 담보되는 것이 아니다. 기술을 사업에 온전히 활용하기 위해서는 그 제도를 이용하는 주체의 참여와 노력이 필요하다. 이처럼 법규의 영향을 받는 주체들의 적극적인 참여에 호응하여 입법기관 및 정부에서는 보험 경영과 보험 구매 현실에 부합하는 제도와 정책을 마련하기 위해 치열하게 고민하여야 한다.

인슈어테크의 활용과 관련된 법적 쟁점을 둘러싸고 보험 소비자, 보험사, 정부의 세 경제주체가 지속적으로 의견을 제시하고 수렴하는 입법 문화가 형성될 때에 비로소 기술 친화적인 법제 하에서 우리나라의 인슈어테크도 발전의 날개를 달 수 있을 것이다.