「제2회 금융보안원 논문공모전」
수상 논문집

| 최우수 |

- **이분 그래프 기반의 악성코드 빅데이터 자동분석 플랫폼 연구**

| 우 수 |

- **금융규제 혁신을 위한 레그테크(RegTech)의 역할과 국내 레그테크 도입 방향**

| 장 려 |

- **금융회사의 보안 위험성향 프레임워크와 측정지표 개발에 관한 연구**
- **개인정보 활용을 위한 블록체인 기반의 개인정보 자기 통제 시스템**

금융보안원
FINANCIAL SECURITY INSTITUTE

이분 그래프 기반의 악성코드 빅데이터 자동분석 플랫폼 연구

이식* · 정성민* · 김동훈* · 문다민* · 최동현*
* 국민대학교 컴퓨터공학과

요 약

4차 산업혁명 빅데이터 시대에는 자동화된 분석 기술이 요구된다. 특히 악성코드와 같은 복잡한 바이너리 중심의 데이터는 소수의 전문 인력만이 수작업 분석이 가능하며, 그나마 제한된 분량의 소수의 데이터 분석만이 가능하다. 본 연구에서는 이분 그래프 이론을 적용하여 악성코드를 다각적 측면에서 분해하고 고유한 특징을 추출해내는 새로운 기술을 제안한다. 제안하는 기술을 사용하면, 악성코드에 대한 새로운 분석 방법론이 등장했을 때에도 새로운 이분 그래프 모델만을 하나 추가시킴으로써 쉽게 확장이 가능한 플랫폼 기술 구현이 가능해진다. 추출된 특징들은 인공지능 머신러닝 학습 데이터로 직접 활용될 수도 있으며, 유사한 악성코드를 찾는 유사도 측정 용도로도 활용될 수 있다. 본 연구에서는 다양한 정적 분석과 동적 분석 실전 기술을 활용해서 다수의 이분 그래프를 생성하고, 그래프 분석 결과를 합산하여 유사도 측정이 가능함을 보인다. 제안하는 기술의 전처리 과정, 이분 그래프 생성, 유사도 계산 등의 과정을 모두 파이썬 프로그램으로 구현하였으며, 하나의 유기적 플랫폼으로 동작할 수 있도록 설계하였다. 특히, 제안 기술의 우수성을 검증하기 위하여 국내 주요기관을 공격 대상으로 작성된 희귀 악성코드 파일 2,811개를 사용하여 다양한 실험을 진행하였다. 실험 결과로서 기존 보안 전문가들이 찾아내지 못했던 유사한 악성코드들의 상호 연계성을 최소 3,766건 이상 자동으로 찾아냈으며, 최근 악성코드 유사도 분석에서 많이 사용되고 있는 퍼지 해시 기술보다도 최소 3,582건 이상의 유사 파일 쌍을 찾아낼 수 있었다.

키워드

이분 그래프, 군집화, 악성코드 분석

목 차

I. 서론

취약한 내부 시스템 및 상대적으로 부주의하게 관리되는 직원용 PC, 기타 기기의 악성코드 감염은 국내외 금융기관의 사이버보안을 가장 위협하는 공격 방식 중 하나이다. 한 번 감염된 시스템은 공격자의 교두보로 연속적으로 활용되며, 내부망 주요 서버와 데이터를 연쇄적으로 손쉬운 공격대상으로 만들어주기 때문이다. 최근에는 국내 금융권만을 노리는 악성코드들이 자주 발견되고 있으며, 이들 배후에는 특정 공격그룹이 존재하고 있는 사실이 밝혀졌다 [1][2].

4차 산업혁명과 디지털 트랜스포메이션 시대에는 무한 복제가 가능한 디지털 데이터, 비약적으로 발전한 컴퓨팅 파워, 그리고 인공지능과 딥러닝으로 대표되는 최신 문제 해결 기법이 결합되어 전례 없는 사회적 변화를 만들어 내고 있다. 악성코드 제작자들과 사이버 공격자들도 이러한 기술적 발전에 힘입어 전례 없이 많은 양의 변종 악성코드를 생산해내고 있다. 전문 보안 인력의 수작업만으로는 도저히 감당하지 못할 많은 양의 악성코드들이 생산되고 있으며, 기존의 백신과 보안 제품을 우회할 수 있는지 테스트까지 마친 상태에서 사이버 공격에 투입되고 있다.

전통적으로 보안 전문가들은 본인만의 경험적 지식, 휴리스틱(heuristic)을 사용하여 악성코드를 분석하고 악성코드 사이의 공통된 특이점을 찾아내서 같은 공격그룹이 연루되어 있음을 밝혀낸다[1][2]. 이러한 기존 방식은 크게 두 가지 문제점을 갖는다. 첫째, 보안 전문가만이 알고 있는 휴리스틱 지식에만 의존하기 때문에, 그 범위를 넘어서는 분석과 프로파일링은 불가능하다. 둘째, 사람이 직접 분석하기 때문에 대량의 악성코드를 분석하는 것은 불가능하다. 이런 문제를 해결하기 위해서 악성코드의 유사도를 측정하는 다양한 연구들이 진행되고 있으며 [3][4][5][6][7][8], 유사한 파일 내용을 쉽게 찾을 수 있게 해주는 퍼지 해시(fuzzy hash) 이론과 구현 도구들이 개발되었다 [9][10].

본 논문에서는 보안전문가의 악성코드 분석 작업과 퍼지 해시를 적용하는 분석 기법의 한계를 뛰어넘는 새로운 악성코드 자동 분석 알고리즘과 구현 기술을 제시한다. 제안하는 알고리즘은 이분 그래프(bipartite graph)를 이용해서 악성코드와 악성코드의 특징(feature) 사이의 관계를 표현하고, 특징 출현 빈도에 따라 적절한 가중

치(weight)를 주고 가중치 기반의 유사도 값 계산이 가능하다. 악성코드로부터 다수의 특징을 추출하는 기법도 함께 제안한다. 제안하는 알고리즘은 프로그램으로 구현하였으며, 국내 주요 기관을 노린 2,811개의 희귀 악성코드 데이터 집합에 대해서 실제 테스트를 진행하였다. 실험을 통해서 보안 전문가의 수작업은 물론이고 퍼지 해시 기법을 적용하였을 때보다도 최소 3,582개의 거의 유사한 악성코드 쌍을 찾아내는 놀라운 결과를 얻었다. 즉, 보안 전문가와 퍼지 해시 기법으로는 찾아내지 못한 악성코드 간의 긴밀한 유사 관계를 최초로 찾아낸 것이며, 이들이 동일한 공격자 그룹에 의해서 제작되었음을 강하게 뒷받침해줄 수 있는 단서를 찾은 것이다. 본 논문이 악성코드 분석 연구 분야에 기여한 주요 내용을 요약하면 다음과 같다.

- 이분 그래프 이론을 이용해서 악성코드와 악성코드의 정적 및 동적 분석 결과로 얻어지는 특징 사이의 관계를 최초로 그래프 분석 모델로 만들었으며, 이분 그래프의 간선(edge)에 고유한 가중치를 부여하고 변형된 자카드 지수(Jaccard index)를 이용한 새로운 유사도 측정 알고리즘을 제안한다.
- 이분 그래프와 유사도 측정 모델, 악성코드 특징 추출 전처리 프로세스 모두를 프로그램으로 구현하였으며, 자동으로 분석 처리가 지원되는 하나의 플랫폼으로 설계하고 구현하였다.
- 국내 주요 기관을 공격 대상으로 제작된 희귀 악성코드 2,811개를 대상으로 본 논문에서 제안하는 분석 기술을 적용하는 실험을 진행했다. 실험 결과, 보안 전문가들과 퍼지 해시 함수 적용으로는 찾지 못했던 최소 3,582개의 유사한 악성코드 쌍을 처음으로 발견하였다.

II장에서는 기존의 휴리스틱 기반의 악성코드 분석 방법에 대해 요약한다. III장에서는 이분 그래프 기반의 악성코드 빅데이터 자동분석 플랫폼을 제안하고, 해당 플랫폼에서 악성코드 전처리 프로세스 과정, 이분 그래프 모델링 과정, 유사도 측정 과정을 설명한다. IV장에서는 실제 실험을 통해서 제안한 모델의 정확성을 검증하고, V장에서 결론을 맺는다.

Ⅱ. 기술 동향

1. 휴리스틱 기반의 악성코드 분석

악성코드 분석 전문가들은 악성코드를 분석하여 공격자, 제작자를 추적한다. 이러한 악성코드 분석은 새롭게 발생하는 침해사고, 공격들의 예상 시나리오나 은닉기법을 파악하는 데 도움이 되며 공격 대상이나 목표 등을 예측하여 피해 예방 및 대응을 가능케 한다. 이를 위해서 악성코드로부터 PDB(Program DataBase) 경로, DLL 파일명, 암호화 키, 문자열 정보, 고유 코드 및 스크립트와 같은 코드 정보 등 여러 특징을 추출하여 공통점을 찾아내는 방식이 사용된다.

(1) 문자열 정보 분석

악성 코드를 분석하면서 얻을 수 있는 중요한 단서 중 하나가 PDB 파일 디렉터리 정보이다. PDB란 비주얼 스튜디오를 통해 프로그램 개발 시 디버깅에 필요한 데이터베이스 파일이라고 보면 된다[1]. 이는 비주얼 스튜디오를 통해 빌드를 하면 자동으로 생성이 되고 별도의 옵션을 해주지 않으면 악성코드가 제작된 디렉터리 경로가 노출된다. 금융보안원에서 발행한 2017 사이버 위협 인텔리전스 보고서에 따르면 금융보안원에서 악성코드를 분석할 때 악성코드들이 공통으로 PDB경로에 라이플(rifle)이라는 단어들이 노출되어 라이플이라는 캠페인으로 명명하고 분석을 수행하여 이를 기반으로 라이플 캠페인에 라자루스(Lazarus), 블루노로프(Bluenoroff), 안다리엘(Andariel) 그룹 등이 연관이 되어있음을 확인하였다[1].

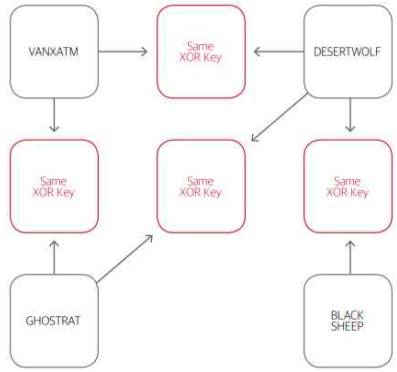
E: \ Data \ My Projects \ Troy Source Code \ tcp1st \ rifle \ Release \ rifle.pdb

<그림 1> pdb의 공통 스트링으로 공격그룹 추정 사례[1]

(2) 코드 정보 분석

공격자들을 분석, 추적할 때 코드들의 유사성을 많이 이용한다. 안랩의 ASEC의 보고서에 따르면 오퍼레이션 레드 갬블러 공격을 특정 그룹과 연관성을 지을 때 악성코드의 암복호화 패턴의 유사성을 이용하여 같은 그룹으로 추측하였다[12].

<그림 2> 암복호화 코드 유사성으로 공격그룹 추정 사례[12]



<그림 3> 암복호화 고유 패턴으로 공격그룹 추정 사례 [1]

공격자들은 악성코드 분석 난이도를 어렵게 하고 송수신 데이터 보호를 목적으로 암호화 기법을 사용한다[1]. 흔히 알려진 SHA-256, MD5와 같은 암호학적 해시(cryptographic hash) 기법을 사용하기도 하지만 공격자들이 제작한 고유 암호를 사용하기도 한다. 이러한 암호화 기법은 다른 코드에서는 보기 힘든 매우 특수한 함

수이기 때문에 특정 공격그룹을 연관 지을 수 있는 중요한 단서가 될 수 있다. 라이플 캠페인에서도 VANXATM, DESERTWOLF, GHOSTRAT, BLACKSHEEP과 같은 오퍼레이션이 서로 연관되었던 사실을 암복호화 패턴의 유사성을 통하여 확인하였다[1].

(3) 문제점 및 한계

앞서 소개된 악성코드 분석방법은 악성코드 분석 전문가에 의해 휴리스틱하게 분석하는 방법이다. 이러한 분석은 몇 가지 문제가 있다. 악성코드 분석은 휴리스틱 기반의 분석이기 때문에 악성코드 분석의 질과 정확성이 악성코드 분석 전문가의 개인역량에 좌지우지 된다. 그렇기 때문에 악성코드 분석 전문가의 지식을 넘어선 분석이 불가능하다. 또한 악성코드 전문가가 악성코드 하나하나 직접 하는 분석이기 때문에 새로 생기는 대량의 악성코드에 대해서 모두 분석을 하는 것은 불가능 하다. 그렇기 때문에 이러한 문제를 해결하기 위해서는 기존 전문 인력 휴리스틱 기반의 악성코드 분석 방법의 한계를 대체하는 자동화된 악성코드 분석방법이 필요하다.

2. 퍼지함수 기반의 악성코드 분석

암호학적 해시함수는 해시 함수의 일종으로 임의의 길이를 갖는 메시지를 입력하여 고정된 길이의 결괏값을 출력하는 함수이다. 파일의 내용이 한 비트만 달라져도 해시의 결과는 완전히 달라진다. 이런 특징 때문에 암호학적 해시함수는 파일의 체크섬 무결성 검증을 할 수 있다. 하지만, 같은 파일 두 개에서 하나의 파일에 1 바이트를 입력 스트링에 추가한다면, 두 파일은 여전히 거의 동일함에도 불구하고 암호학적 해시의 결과는 완전 다른 값을 가지게 된다.

퍼지 해시는 유사한 파일은 유사한 결괏값을 출력하도록 설계된 함수로서, 문서 검색 분야에서 많이 사용되며 최근에는 악성코드 분석에도 많이 활용되고 있다. 퍼지 해시는 파일 전체에 대한 해시 값을 한 번에 계산하지 않는다. 입력 값을 일정 크기 단위로 구분하여 각 단위 블록에 대한 해시 값을 만들어 낸다. 최종 해시함수 결과는 각 영역의 마지막 몇 바이트에 대한 해시 값을 이어붙인 값이 된다. 대표적 퍼지 해시 프로그램으로는 ssdeep이 있다[9]. ssdeep을 이용해 두 파일의 유사도를 비교할 수 있다. 비교 결과로서 0 ~ 100 점 사이의 값이 생성되며, 완전 동일한 파

일은 100점이 나온다.

```
$ ssdeep -b gettysburg-address.doc > sigs.txt
$ ssdeep -bm sigs.txt gettysburg-modified.doc
gettysburg-modified.doc matches gettysburg-address.doc (57)
```

<그림 4> ssdeep 프로그램 사용 방법[9]

악성코드 분야에서 퍼지 해시는 크게 두 가지 방식으로 많이 활용된다. 첫째, 악성코드 파일 전체에 대해서 퍼지 해시 값을 구해서 유사도를 비교한다. 둘째, 악성코드의 실행 코드 영역에 대해서 퍼지 해시 값을 구해서 유사도를 비교한다.

(1) 파일 전체 내용 유사도 비교

악성코드 파일에 대해 어떠한 가공도 거치지 않고 그 자체에 대해서 ssdeep을 적용시킬 수 있다. 즉, 윈도우즈 실행파일인 PE 파일들을 대상으로 ssdeep을 적용한다면 헤더 영역, 텍스트 영역, 데이터 영역이 모두 포함된 전체 파일들에 대해서 ssdeep 값을 구한다.

(2) 실행 코드 영역 유사도 비교

PE 파일에서 헤더와 데이터 영역을 제외하고 실행코드가 들어있는 텍스트 영역에 대해서만 ssdeep을 적용한다. 원본 PE 파일에서 텍스트 영역을 추출하는 전처리 과정을 거친 후 ssdeep을 이용해야 한다.

(3) 문제점 및 한계

대표적 퍼지 함수인 ssdeep은 다음과 같은 한계점을 갖는다.

첫째, 원본 파일 자체로 ssdeep을 적용할 때, 비교할 파일의 종류가 같으면 실제로 비교할 파일의 내용이 크게 다르더라도 유사도가 높게 계산될 수 있다. 가령 두 개의 내용이 전혀 다른 ppt 파일이 존재한다고 할 때, 파일 형식이 같기 때문에 파일의 사이즈가 작을수록 메타 데이터 영역이 크게 부각된다. 왜냐하면 메타 데이터 영역은 비슷한 내용이기 때문이다.

둘째, 퍼지 해시는 일반적으로 고정 크기 윈도우가 일정 조건을 만족할 때까지 한 바이트씩 전진하게 된다. ssdeep에서는 윈도우에 속한 콘텐츠의 내용의 해시 값을 블록 크기로 나누었을 때의 나머지가 블록 크기보다 하나 작을 경우가 발생할 때까지 전진시킨다[9]. 그런데 이 조건을 계속 만족하지 못하면 ssdeep의 최종 결괏값이 무의미하게 짧게 생성되어 파일간 유사도 비교가 거의 불가능하다.

셋째, ssdeep 퍼지 해시를 사용해서 비교할 파일의 크기가 2배 이상 차이가 나는 경우는 잘 동작하지 않는다. 최대 4배까지 유사도 측정이 가능할 수는 있지만, 일반적으로 파일 크기의 차이가 2배 이하일 때 안정적으로 동작한다. 그 이유는, ssdeep에서는 파일 크기에 따라 블록 크기가 정해지는데, ssdeep은 블록 크기와 블록 크기의 2배를 사용해서 해시 값 두 개를 각각 생성한다. 따라서 블록 크기가 2배 넘게 차이가 난다면 부분 구간을 생성하는 조건이 달라지기 때문에 일관성 있게 유사도를 측정할 수 없게 된다.

3. 기타 관련 연구

유사한 악성코드를 찾는 것은 사이버보안에서 중요한 연구 주제이며 다양한 연구가 진행되어왔다.

X. Hu 등은 패킹을 제거하는 방법을 도입하여 악성코드의 opcode 시퀀스를 메모리에서 추출하고 n-gram 적용 후 클러스터링을 적용하는 연구를 진행했다. Mutant-X로 이름이 붙은 이 방식은 기본적으로 정적 분석에 의존한다. 보안 전문가들이 분석한 4,821개의 악성코드 파일 집합과 온라인 사이트의 132,234개의 데이터 집합 두 가지에 대해서 실험을 진행했다. 이 논문은 악성코드 클러스터링 분야에서 많이 인용되고 있으며, 실험 방법론이 우수하다 [3].

Jang 등은 악성코드 정적 분석 정보를 기반으로 n-gram을 생성한 후, 고정 크기의 비트맵(bitmap)에 인코딩(encoding)하는 방식으로 악성코드의 특징을 표현하는 방법을 제안했다. 비트맵은 0으로 초기화되어 있는데, 특정 인덱스에 n-gram이 매핑되는 경우에는 1로 값이 바뀌며, 고정 길이를 가졌기 때문에 빠른 벡터 연산이 가능해진다. 자카드 인덱스의 변형 형태인 비트맵 연산으로 두 악성코드 사이의 유사도 값을 계산할 수 있으며, 이 값을 기반으로 클러스터링을 수행한다. Bitshred로 명명

된 이 기법은 많은 후속 연구에 영향을 주게 된다 [4].

고동우 등은 쿠쿠 샌드박스의 동적 분석을 이용해서 악성코드 API 콜 시퀀스를 추출하고, 종류가 다양한 함수들을 17가지 카테고리로 일반화(추상화)시킨 후 퍼지 함수에 적용해서 클러스터링 작업을 진행했다. 세 종류(ssdeep, simhash, TLSH)의 LSH(Locality Sensitive Hash) 함수를 사용해서 클러스터링 성능을 비교했으며, 이 중에서는 TLSH가 가장 우수한 성능을 나타냄을 보였다 [5].

한병진 등은 악성코드를 대표할 수 있는 특성 인자인 DNA 값을 생성하는 방법을 제안했으며, 추출된 DNA 값으로 유사한 악성코드를 찾는 기법을 제안했다. 특성 인자로서는 악성코드의 해시 값, 바이러스토탈(virusTotal) 분석결과, 패킹 여부 및 패커 정보, PE 헤더 분석 정보, API 정보, 스트링, LSH 값 등을 다양하게 활용하였으며, 각 특성 인자들의 결괏값들로 구성된 벡터를 자카드 인덱스 방식으로 변환하여 최종 유사도 값으로 사용했다 [6].

강홍구 등은 악성코드가 실행되는 과정에서 호출하는 API를 추출하여 2-gram 시퀀스와 호출빈도를 벡터로 생성하고, 벡터 간 유사도를 측정하는 방식으로 악성코드의 유사도를 측정하는 연구를 수행했다. 전통적인 코사인(cosine) 유사도 대신 최근 빅데이터 연구 분야에서 제안된 TS-SS 측정 기법을 사용하였는데, TS-SS 기법은 벡터들의 공간상의 거리 차이와 면적을 이용함으로써 코사인 유사도가 방향만을 측정함으로써 발생하는 단점을 극복할 수 있다고 알려져 있다 [7].

조인겸 등은 악성코드의 API 호출 정보를 하나의 긴 스트링으로 간주하고, 서로 다른 스트링 간의 서열 정렬 기법을 이용하여 유사도를 분석하였다. 서열 정렬 기법은 바이오인포매틱스 분야에서 DNA 등의 서열을 분석하는데 사용된다 [8].

김동진 등은 오픈소스 소프트웨어 모듈을 탐지하기 위해서 함수 수준에서의 특징정보를 추출하여 비교하는 방법을 제안했다. 오픈소스 라이선스에 관련되어 특정 모듈을 포함하고 있는지를 확인하는 문제는 악성코드의 유사도를 측정하는 문제와 깊이 관련되어 있다. 유사한 악성코드는 일반적으로 동일하거나 비슷한 함수 모듈들을 공통으로 포함하고 있는 경우가 많기 때문이다. 이 논문에서는 명령어 기반의

특징정보, 제어흐름 그래프 특징정보, 함수 수준의 구조적 특징정보를 사용해서 특정 오픈소스 소프트웨어 모듈이 포함되었는지를 판별한다[13].

많은 연구자들은 빅데이터 악성코드 분류 문제를 해결하기 위해 딥러닝 기술을 활용하고 있다.

Saxe 등은 악성코드와 정상 파일을 분류하는 문제에 대해 가장 단순한 딥러닝 모델인 심층 신경망(DNN, Deep Neural Network)을 이용해서 문제를 해결하였다. 약 50만 개의 데이터를 통해 악성코드 탐지 모델에 대한 학습 및 검증을 진행하였고, 실행 파일에서 쉽게 얻을 수 있는 특징 정보들을 가공하여 입력으로 사용하였다. 은닉층은 두 층만을 사용하였고, 비교적 적은 자원에 높은 효율을 내는 작은 네트워크를 설계하면서 95%의 정확도를 달성하였다[14].

최선오 등은 악성코드의 변종이나 제로데이 공격에 대응하기 위해 심층 신경망과 합성곱 신경망(CNN, Convolutional Neural Network)을 적용한 연구사례를 소개하였다. 실행 파일의 특징정보로써 opcode와 API 콜, 또는 악성코드의 시각화된 이미지를 딥러닝의 입력 데이터로 사용했고, 각 실험에 대해 약 95~99% 이상의 높은 성능을 보여주었다[15].

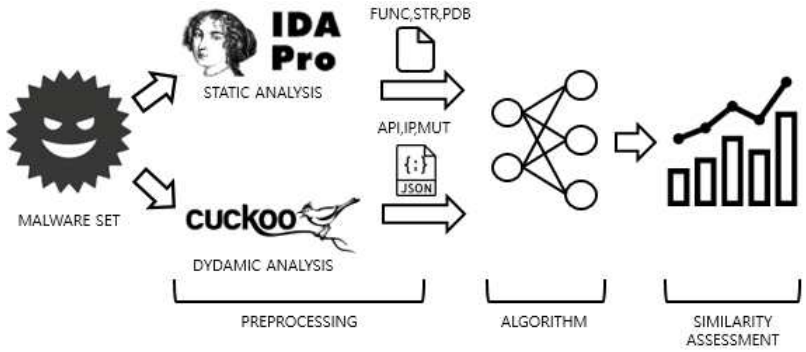
조영복은 악성코드를 이미지화하고 R-CNN 기반의 딥러닝 모델을 적용하여 악성코드 탐지 연구를 수행하였다. 딥러닝의 입력 데이터로 시각화한 이미지를 사용하여 악성코드 변종에 강인한 특성을 가지게 하였고, 최신 딥러닝 모델 중 하나인 R-CNN과 CNN을 결합하여 처리 시간을 단축시켰다. 주로 이미지 분야에 적용되었던 최신 기술을 악성코드 탐지 연구에 사용함으로써 두 분야가 연관성이 있음을 보여주었으며, 마이크로소프트에서 제공한 BIG 2015 데이터셋에 대해 실험을 진행한 결과 93.4%의 검출율과 98.6%의 정확도를 보였다[16].

Ⅲ. 악성코드 빅데이터 자동분석 플랫폼

1. 플랫폼 아키텍처

본 논문에서는 이분 그래프 모델에 기반하여 새로운 악성코드 빅데이터 자동분석 알고리즘 및 플랫폼인 ABMB(Automatic Big-data Malware analysis with Bipartite graph)를 제안한다. ABMB는 악성코드의 특징 정보를 다양한 측면에서 추출하여 이분 그래프 모델로 만들고, 특징 정보 노드에 적절한 가중치를 부여함으로써 모든 악성코드 파일 쌍에 대해서 유사도 점수를 부여한다. ABMB는 빅데이터 분석을 위한 확장성 측면에서 우수하며, 보안 전문가와 퍼지 해시 기술로는 놓치기 쉬운 유사한 악성코드 쌍을 찾을 수 있게 해주는 새로운 기술이다.

ABMB는 다음 그림과 같이 총 세 부분의 처리 프로세스로 구성된다. 첫 번째 단계로 악성 코드는 여러 분석 과정을 통해 의미있는 특징 정보를 수집하기 위한 전처리 과정을 수행한다. 두 번째 단계에서는 수집된 정보를 이용하여 이분 그래프 모델을 설계한다. 마지막 단계는 설계된 이분 그래프 모델을 이용한 유사도 평가 과정을 통해 유사 악성 코드 간의 관계를 찾는다.



<그림 5> 악성코드 빅데이터 자동분석 플랫폼(ABMB) 아키텍처

2. 악성코드 전처리 프로세스

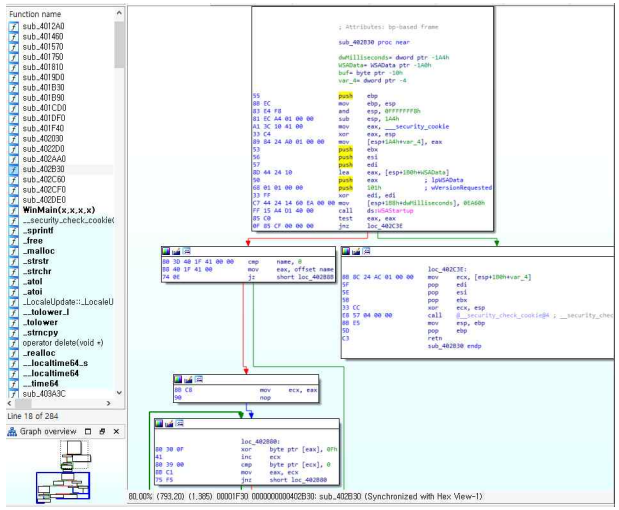
악성코드와 같은 복잡한 바이너리 데이터는 고유한 특징을 자동 추출하여 특징정보로 사용하는 데 어려움이 있다. 본 연구는 악성코드를 다양한 관점에서 분해하고 고유 특징정보 6개를 자동으로 추출할 수 있는 새로운 기술을 제안한다. 악성코드는 크게 두 가지 분석을 수행할 수 있는데, 파일을 실행하지 않고 그 자체의 내용을 최대 활용하여 진행하는 정적 분석과 격리된 공간이나 샌드박스 환경을 이용하여 파일을 실행하고 그 실행 흐름에 따른 행위 동작을 분석하는 동적 분석이 있다. 정적 분석은 빠른 시간 내에 끝낼 수 있지만 실행 압축이나 난독화 기법에 취약하고, 동적 분석은 비교적 긴 분석 시간을 필요로 하지만 양질의 행위 관련 정보를 얻을 수 있다. 두 분석 방법은 다루는 내용이 상이하기 때문에 두 정보를 모두 사용하면 더욱 깊이 있는 악성코드 분석을 진행할 수 있다. 본 연구는 정적 분석을 통한 세 가지의 정보와 동적 분석을 통한 세 가지의 정보를 소개하고, 추출 방법에 대해 설명한다.

(1) 정적 분석을 통한 정보수집

본 연구는 보다 확실한 정적 정보를 얻기 위해서 대표적인 디스어셈블러 중 하나인 IDA Pro를 사용하였다. IDA Pro는 디스어셈블러의 역할 뿐만 아니라 실행 흐름을 그래프로 보여주는 등 다양하고 편리한 기능을 제공하며, 양질의 정적 정보를 수집하는데 효과적이다[17]. 사용한 정적 특징 정보는 코드 데이터, PDB 정보, 문자열(string)이며 모두 IDA Pro를 통해 수집 가능하다.

1) 코드 데이터

IDA Pro를 통해 실행 파일을 디스어셈블하게 되면 어셈블리어로 표현된 결과를 얻을 수 있다. 디스어셈블의 결과는 주소 값, opcode, operand, 레지스터 정보 등을 표현하며, text, rdata 등의 서로 다른 섹션을 구분한다. 예시 파일에 대한 IDA 분석 결과는 아래와 같다.

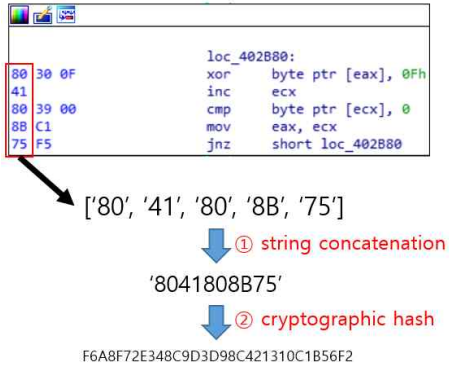


<그림 6> IDA pro를 이용한 정적 분석결과 예시

<그림 6>의 분석 결과는 크게 3개의 창으로 나타난다. 왼쪽 긴 창은 해당 파일을 이루고 있는 함수의 집합이다. 왼쪽 아래 창은 해당 함수의 그래프 관점을 간략화하고, 세부적인 내용은 오른쪽 전체 창을 통해 확인할 수 있다. 각 함수는 제어 흐름 그래프(Control Flow Graph)로 표현되며, 그래프의 노드는 코드로써 의미를 가지는 가장 작은 단위인 기본 블록(basic block)이고 간선은 블록 간 실행 흐름이다. 본 연구는 함수 단위의 의미 있는 코드 데이터를 사용하였다.

가. 기본 블록 정의

함수를 이루고 있는 원소는 기본 블록이기 때문에 기본 블록을 대표하는 값을 먼저 정의하였다. 기본 블록은 하나 이상의 opcode로 이루어져 있고 블록을 이루고 있는 opcode를 이어붙인 하나의 문자열로 대표할 수 있다. 이어붙인 문자열은 기본 블록의 크기에 따라 다를 수 있기 때문에 암호학적 해시함수(e.g. md5)를 적용하여 고정된 길이로 나타내도록 하였다.



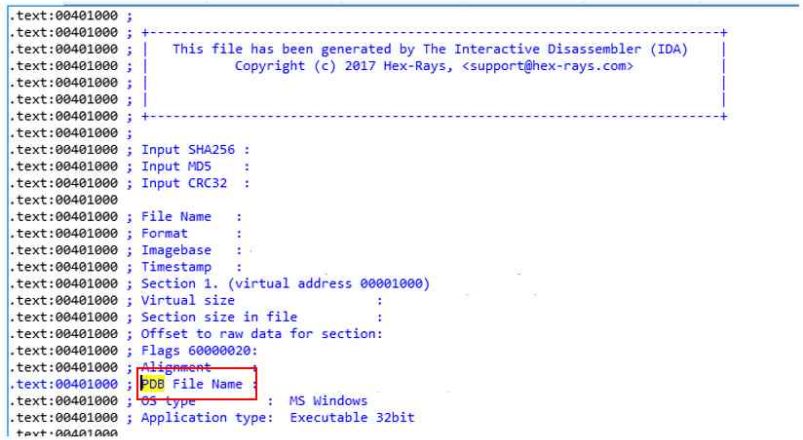
<그림 7> 기본 블록 정의 예시

나. 함수 대푯값 정의

기본 블록을 암호학적 해시 값으로 변환하면, 각 함수는 시그니쳐 값들의 집합으로 표현될 수 있다. 함수는 기본 블록들 사이의 흐름 그래프로 표현이 되지만, 본 논문에서는 편의상 기본 블록들로 구성된 집합으로 표현한다. 이 집합을 하나의 시그니쳐 값으로 다시 변환하고, 이 값을 해당 함수의 대푯값으로 사용한다. 집합을 하나의 대푯값으로 변환하기 위해서 집합의 모든 원소들을 XOR하여 하나의 값으로 정의한다. XOR 연산은 입력 순서에 관계없이 피연산자가 동일하면 동일한 결과를 반환하기 때문에, 집합을 하나의 값으로 표현하기 적합하다. 모든 악성코드는 정의한 함수 대푯값을 코드 데이터로 사용하며, 만약 악성코드에 함수가 존재하지 않을 경우 해당하는 코드 데이터는 존재하지 않을 수 있다.

2) PDB 정보

PDB는 Program DataBase의 약자이며, 마이크로소프트에서 개발한 디버깅 저장 파일이다. 확장자는 '.pdb' 이고, 흔히 개발자가 디버깅 모드를 실행할 경우 자동으로 생성되는 파일이다[11]. 일반적으로 정적 분석 도구를 통해 파일을 분석할 경우 간혹 PDB 파일의 저장 경로 정보를 포함하는데, IDA Pro도 이를 확인할 수 있다. PDB 정보는 악성코드 분석가에게 중요한 특징정보일 수 있다. 왜냐하면 만약 서로 다른 파일에 대해 동일하거나 상당 부분 유사한 PDB 정보가 나타났다면, 같은 개발 그룹이 만들었을 가능성이 상당히 높기 때문이다.



<그림 8> 정적 분석을 통한 PDB 경로 추출 예시

2017년 금융보안원의 사이버 위협 인텔리전스 보고서에서 소개하는 라이플 캠페인 역시 PDB 파일을 통한 그룹 분류를 하였기 때문에[1], PDB 경로 정보는 악성코드 그룹 분류를 하는 중요한 수집정보이다.

3) 문자열 정보

실행 파일의 문자열 정보는 파일의 추출 가능한 모든 ASCII 정보를 포함한다. 문자열 정보는 분석 결과를 통해 프로그램의 구현 정보 및 코드 인젝션과 같은 여러 추론을 할 수 있을 뿐만 아니라 같은 개발 그룹에 의해 구현되었을 경우 개발자의 시그니처가 포함되었을 가능성이 상당히 높다. 이는 악성코드를 그루핑하기 위한 좋은 정적 수집정보이다.

Address	Length	Type	String
.rdata:004…	0000000F	C	bad allocation
.rdata:004…	00000007	C	(null)
.rdata:004…	00000008	C	(8PX₩a₩b
.rdata:004…	00000007	C	700WP₩a
.rdata:004…	00000008	C	₩b`h``
.rdata:004…	0000000A	C	xpxxxx₩b₩a₩b
.rdata:004…	0000000F	C	CorExitProcess
.rdata:004…	00000009	C	HH:mm:ss
.rdata:004…	00000014	C	dddd, MMMM dd, yyyy
.rdata:004…	00000009	C	MM/dd/yy
.rdata:004…	00000009	C	December

<그림 9> 정적 분석을 통한 문자열 추출 예시

문자열 정보는 주로 프로그램의 상수 값으로 이루어져 있다. 주로 데이터 섹션을 통해 추출되고, 프로그램의 여러 의미를 파악할 수 있다. 한 예시로 위 그림에서는 프로그램이 날짜에 대한 정보를 가지고 있는 것을 확인할 수 있다.

```
581 : function WCCR__registerContentHandler(contentType, uri, title) {
582 :   this._updateContentTypeHandlerMap(contentType, uri, title);
583 :   this._saveContentHandlerToPrefs(contentType, uri, title);
584 :   if (contentType == TYPE_MAYBE_FEED) {
585 :     // Make the new handler the last-selected reader in the previ
586 :     // and make sure the preview page is shown the next time a fe
587 :     var pb = Cc[\"@mozilla.org/preferences-service;1\"].
588 :              getService(Ci.nsIPrefService).getBranch(null);
589 :     pb.setCharPref(PREF_SELECTED_READER, \"web\");
590 :     var supportsString =
591 :       Cc[\"@mozilla.org/supports-string;1\"].
592 :       createInstance(Ci.nsISupportsString);
593 :       supportsString.data = uri;
594 :     pb.setComplexValue(PREF_SELECTED_WEB, Ci.nsISupportsString,
595 :                        supportsString);
596 :     pb.setCharPref(PREF_SELECTED_ACTION, \"ask\");
597 :     this._setAutoHandler(TYPE_MAYBE_FEED, null);
598 :   * Update the content type -> handler map. This mapping is not pe
599 :   * registerContentHandler or _saveContentHandlerToPrefs for that
600 :   * @param   contentType
601 :   *          The content Type being handled
```

<그림 10> 문자열로 나타난 소스코드

위 그림은 소스코드가 문자열 정보로 나타난 경우인데, 이는 일반적이지 않은 상황이며 코드 인젝션을 의심할 수 있다.

(2) 동적 분석을 통한 정보수집

일반적으로 동적 분석은 격리된 환경이나 샌드박스를 활용하여 진행하는 경우가 대부분이다. 본 연구에서는 쿠쿠 샌드박스 환경을 활용하였고[18], 자동화하기 위한 스크립트를 구현하였다. 쿠쿠 샌드박스의 분석 결과는 JSON 형식의 리포트로 구성되기 때문에 특정 정보 추출에 용이하다. 리포트의 내용은 파일 정보, 정적, 동적 분석 결과, 네트워크 정보, 시그니처 정보 등의 방대한 정보를 포함하고 있으며, 유용한 특정 정보를 찾는 작업은 중요하다. 사용한 동적 특징 정보는 API 집합, IP 주소, 뮤텍스(Mutex) 정보이며, 모두 쿠쿠 샌드박스 리포트를 통해 수집 가능하다. 본 연구에서는 파일당 분석 시간을 3분(기본 2분 + 추가 1분)으로 진행하였다.

<그림 11> 쿠쿠 샌드박스 결과 리포트 구성 요소

<그림 11>와 같이 쿠쿠 샌드박스 리포트는 다양한 구성 요소 포함하고 있다. 그 중 API 정보와 뮤텍스 정보는 행위 속성에서, 그리고 IP 주소 정보는 네트워크 속성에서 확인할 수 있다.

1) API 정보

API(Application Programming Interface)란 응용 프로그램에서 사용할 수 있도록 운

영 체제나 프로그래밍 언어가 제공하는 기능을 제어할 수 있게 만든 인터페이스를 의미한다. 일반적으로 프로그램에서 많이 사용하는 API는 윈도우즈 API 등이 존재한다[19].

<그림 12> 쿠쿠 샌드박스 API 정보 예시

<그림 13> 쿠쿠 샌드박스 네트워크 정보 예시

<그림 12>에서 "behavior-processes-1-calls" 속성을 살펴보면 프로세스 1번이 NtAllocateVirtualMemory API를 409번 호출하는 것을 확인할 수 있다. 본 연구는 유사한 파일은 호출하는 API 또한 유사할 것이라고 기대하기 때문에 API 이름 정보들을 집합으로 저장하고, 주요 정보로 사용한다.

2) IP 주소 정보

쿠쿠 샌드박스는 파일을 분석할 때, 분석 파일이 네트워크 행위를 하는지 감시 및 탐지하고, 이를 기록한다. C&C 서버와 통신을 하는 악성코드가 실행된다면, 네트워크 정보는 매우 중요한 정보이다. 네트워크 정보는 IP 주소 정보 뿐 아니라 DNS 정보, smtp 등의 특정 프로토콜 정보도 포함한다. 그 중에서도 IP 주소 정보는 짧지만 직관적이고 확실한 정보를 제공하기 때문에 중요한 수집 정보로 활용할 수 있다.

본 연구에서는 TCP 패킷의 도착 IP 주소를 수집 정보로 사용한다.

3) 뮤텍스 정보

```
HANDLE CreateMutex(
  LPSECURITY_ATTRIBUTES lpMutexAttributes,
  BOOL bInitialOwner,
  LPCTSTR lpName
);
```

<그림 14> 뮤텍스 정의 함수

프로그램 개발자가 프로그램이 다중으로 실행되는 것을 방지하기 위해 뮤텍스를 설정할 수 있다[20]. 쿠쿠 샌드박스 리포트에서 제공하는 뮤텍스 정보는 개발자가 설정한 뮤텍스 정보를 포함하고 있다. 뮤텍스를 설정하고자 하는 경우 내부적으로 <그림 14>에 있는 CreateMutex() 함수를 호출하게 되는데, 함수의 인자로 고유 뮤텍스 정보를 나타내는 문자열이 필요하다. 같은 개발 그룹이라면 뮤텍스 인자 생성에 필요한 문자열 역시 동일할 가능성이 높기 때문에 특징 정보로 활용한다.

3. 이분 그래프 모델

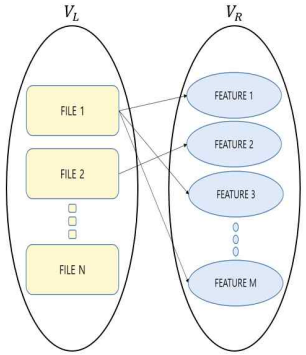
본 논문에서는 악성코드 사이의 유사 관계를 표현하기 위해서 이분 그래프(bipartite graph) 모델을 사용한다. 이분 그래프는 노드(node)와 간선(edge)으로 구성되는 그래프의 한 종류이다. 그래프를 G=(V,E)로 표현하면, V가 노드의 집합이며 E가 간선의 집합이다. 이분 그래프에서는 V가 다시 두 개의 상호배타적 부분집합인 V_L과 V_R로 나뉘며, 따라서 $V=V_L \cup V_R$과 $V_L \cap V_R=\varnothing$가 성립한다[21]. <그림 15>는 본 논문에서 사용할 이분 그래프의 표현 기호를 요약한다.

$$G = (V, E)$$
$$V = V_L \cup V_R \ (V_L \cap V_R = \emptyset)$$
$$V_L = \{v_{l0}, v_{l1}, \dots, v_{l(n-1)}\}, |V_L| = n$$
$$V_R = \{v_{r0}, v_{r1}, \dots, v_{r(m-1)}\}, |V_R| = m$$
$$E = \{e_{lr} | \ v_l \in V_L \ and \ v_r \in V_R : e_{lr} = (v_l, v_r)\}$$

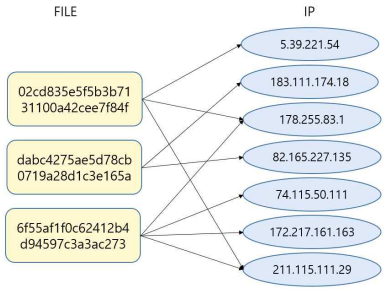
<그림 15> 이분 그래프 표현 기호

앞 장에서는 여섯 가지 서로 다른 특징 정보를 사용해서 악성코드를 표현했다 (함수, PDB, 문자열, API 집합, IP 주소, 뮤텍스). 본 장에서는 이분 그래프 모델을 사용해서 악성코드와 각 특징 정보의 연관성을 표현하며, 이에 기반하여 악성 코드 사이의 유사도 값을 정의한다. <그림 16>은 악성코드와 특징 정보로 구성되는 이분 그래프를 나타낸다. V_L은 항상 악성코드가 노드에 해당하는데, 악성코드의 md5 값을 사용해서 노드를 표현한다. V_R은 특징 정보가 노드를 형성한다. 악성코드 v_i가 특징 정보 v_j를 생성한 경우에는 두 노드 사이를 간선으로 연결하고, 이 간선을 e_{ij}로 표현한다. 본 논문에서는 여섯 개의 특징 정보 각각에 대해서 이분 그래프 모델을 생성하며, 따라서 여섯 개의 이분 그래프가 존재한다.

만약 IP 주소가 특징 정보인 이분 그래프라면, <그림 17>와 같이 표현된다. 예를 들어 md5 시그니처 값이 02cd835e5f5b3b7131100a42cee7f84f인 악성코드 파일이 IP 주소 5.39.221.54, 178.255.83.1, 211.115.111.29와 통신을 시도했다는 정보를 알 수 있다. 또한 IP 주소 178.255.83.1은 md5 시그니처 값이 각각 02cd835e5f5b3b7131100a42cee7f84f과 6f55af1f0c62412b4d94597c3a3ac273인 악성코드 파일과 관련되어 있다는 것을 표현한다.



<그림 16> 악성코드와 특징 정보로 구성된 이분 그래프



<그림 17> 악성코드와 IP 주소로 구성된 이분 그래프

이분 그래프는 각 특징 정보 별로 악성코드들의 연관 관계를 시각적으로 보기 좋게 나타낸다. 또한, 새로운 특징 정보가 등장하였을 때에는 해당하는 이분 그래프만 추가적으로 생성하면 되기 때문에 확장성이 우수하다. 또한, 이분 그래프 상의 노드와 간선의 개수를 고려하여 가중치를 설정하기가 쉽기 때문에 악성코드 사이의 유사도를 다양한 방식으로 정의할 수 있는 장점이 있다.

4. 유사도 정의 및 측정 방법

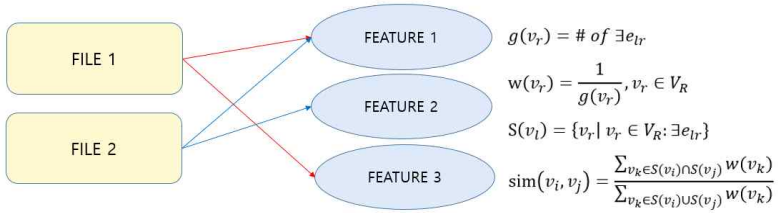
특징 정보 별로 이분 그래프가 생성되면, 한 쌍의 악성코드 파일에 대해서 유사도를 정의할 수 있다. 본 논문에서는 유사도 정의를 위해서 각 특징 정보 노드에 가중치를 부여한다. 특징 정보 노드가 다수의 악성코드에 연결되어 있다면, 해당 특징 정보가 한 쌍의 악성코드에 동시에 포함되어 있더라도 둘 사이가 특별히 유사하다고 보기는 어렵다. 반대로, 어떤 특징 정보 노드가 유일하게 한 쌍의 악성코드에만 연결되어 있다면, 두 악성코드는 이 특징 정보 노드로 인해서 유사도가 높게 산정되는 것이 바람직하다. 이러한 가정은 자연어처리 분야에서 문서와 워드 사이의 관계에 가중치를 주는 TF-IDF(Term frequency-inverse document frequency) 기법과 일맥상통한다고 볼 수 있다.

특징 정보 노드의 가중치 값은 해당 노드가 연결되어 있는 간선의 개수의 역수로 정의된다. 본 논문에서는 노드 v에 연결되어 있는 간선의 개수를 g(v)로 함수처럼 표현한다. 노드 v의 가중치를 w(v)라고 한다면, $w(v) = \frac{1}{g(v)}$가 성립한다. 여기서 v는 V_R에 속하는 원소이다. 이제 두 악성코드 FILE1과 FILE2가 주어졌다고 가정하고, 각각을 v_i와 v_j로 표현한다. 둘 사이의 유사도는 sim(v_i, v_j)로 표시하며, 다음과 같이 정의한다.

$$sim(v_i, v_j) = \frac{\sum_{v_k \in S(v_i) \cap S(v_j)} w(v_k)}{\sum_{v_k \in S(v_i) \cup S(v_j)} w(v_k)} \quad \text{----------(1)}$$

수식(1)은 항상 0부터 1 사이의 값을 갖기 때문에 비교 지표로 사용하기에 편리하

며, 1에 가까울수록 유사도가 높음을 나타낸다. <그림 18>은 가중치와 유사도에 대한 간단한 예시이다. 두 개의 악성코드 파일인 FILE1과 FILE2가 존재하고, 세 개의 특징정보 노드가 존재한다. FILE1은 특징정보 1, 3을 포함하고, FILE2는 특징정보 1, 2를 포함한다. 특징정보 1의 경우 이어진 간선이 2개이기 때문에, 특징정보 1의 가중치는 1/2 이다. 마찬가지로 특징정보 2, 3의 가중치는 각각 1, 1이다. 따라서, 두 파일의 유사도는 (1/2) / (1/2 + 1 + 1) = 1/5로 계산된다.



<그림 18> 이분 그래프 상에서 특징 노드의 가중치 및 두 파일 사이의 유사도 정의

Ⅳ. 실험 및 검증

본 논문에서는 실험을 통해서 보안 전문가와 퍼지 해시 함수로는 찾아내지 못했던 유사 악성코드 쌍을 ABMB에 의해서 찾아낼 수 있음을 확인하였다. 국내 주요 기관을 공격 대상으로 하는 악성코드 집합에 대해서 실험을 진행했으며, 해당 집합은 악성코드 분석 전문가에 의해서 9개 그룹으로 분류가 된 상태였다. ABMB는 최소 3,766개의 매우 유사한 악성코드 쌍을 새롭게 찾아냈으며, 이 숫자는 퍼지 해시 함수를 적용했을 때보다도 3,582개를 더 찾아낸 것으로서 ABMB의 우수성을 증명한다.

1. 실험 데이터 소개

본 실험은 2811개의 악성코드 데이터를 기반으로 실험을 진행하였으며 모든 악성코드는 32비트 PE 파일로 구성되어있다. 이 악성코드들은 보안 전문가들에 의해서 분석되었으며, 다양한 분석 기준에 의해서 총 9개의 그룹으로 분류되었다. 하나의 악성코드는 하나의 그룹에만 속해있다. 공격그룹 별로 포함된 악성코드의 개수는 <표 1>과 같다.

공격 그룹	파일 개수
0그룹	305개
1그룹	107개
2그룹	657개
3그룹	107개
4그룹	34개
5그룹	322개
6그룹	637개
7그룹	634개
8그룹	10개
전체	2811개

<표 1> 공격그룹별 악성코드 파일 개수

2. ABMB 분석 결과

모든 악성코드 파일에 ABMB를 적용하였으며, 총 6개의 특징 정보 별로 이분 그래프를 생성했다. 즉, 정적 분석과 동적 분석, 그리고 전처리 과정을 통해서 함수, PDB, 문자열, API 집합, IP 주소, 뮤텍스 정보를 추출하였으며, 이를 바탕으로 이분

그래프를 생성하고 모든 파일 쌍 간의 유사도를 계산했다. 본 실험에서는 ABMB 알고리즘을 적용했을 때, 두 파일의 유사도 값이 특정 임계값 이상인 경우에 한하여 두 파일을 유사 파일로 간주하였다. 임계값으로는 1.0, 0.9, 0.8 세 가지 경우를 각각 고려했다. 실험결과를 보여주는 그림에서 이 임계값들에 대응하는 그래프는 각각 “threshold:1.0”, “threshold:0.9”, 그리고 “threshold:0.8”로 표현된다.

<그림 19>는 악성코드를 정적 분석하여 얻어진 뮤텍스 특징 정보를 기준으로 이분 그래프 생성과 파일 쌍의 유사도 계산을 ABMB 알고리즘으로 실행한 결과이다. x축은 보안 전문가가 분류해 놓은 공격그룹 라벨의 쌍을 나타낸다. 총 9개의 공격그룹이 존재하므로, 36(=9*8/2)개의 쌍이 존재하며 이 값들이 x축을 구성한다. 즉, x축의 “1_0”의 의미는 한 쌍의 악성코드 파일들이 ABMB 알고리즘에 의해서 유사한 관계로 발견되었는데, 하나는 보안 전문가에 의해서 1번 공격그룹으로, 하나는 0번 공격그룹으로 분류가 되었다는 것을 의미한다. 즉, 이 파일들은 뮤텍스 특징 정보를 기준으로 ABMB 알고리즘에 의해서 매우 유사하다고 판별이 되었음에도 불구하고 보안 전문가에 의해서 서로 다른 공격그룹으로 분류되었다는 것을 의미한다. y축은 그러한 악성코드 파일 쌍이 ABMB에 의해서 몇 개가 발견되었나를 나타낸다. x가 “1_0”에서 y값이 약 1,000에 해당하면, 그룹 0의 악성코드와 그룹 1의 악성코드 중 약 1000개의 쌍이 서로 유사하다고 ABMB 알고리즘으로 측정된 것이다. 즉, y값이 크면 클수록 해당 x값을 구성하는 2개의 공격그룹은 뮤텍스 특징 정보를 기준으로는 유사도가 높게 해석될 수 있다. 실제 뮤텍스 특징 정보가 어느 정도의 신뢰도를 주는지는 추가 연구가 필요하다.

<그림 20>~<그림 24>는 각각 스트링, IP 주소, PDB, API 집합, 함수 특징 정보를 기준으로 ABMB 알고리즘을 적용한 결과를 나타낸다. PDB를 제외하고는 모두 유의미하게 높은 y값이 도출되었다. 즉, 보안 전문가들에 의해서 발견되지 못했던 유사 악성코드 파일들이 ABMB 알고리즘으로는 찾아질 수 있음이 확인된 것이다. 단, 뮤텍스와 IP 주소는 다양한 x값에 대해서 1 이상의 y 값을 확인할 수 있었는데, 그렇다고 해서 해당 파일 쌍이 매우 유사하다고 단정 짓기는 어렵다. 가령 IP 주소 중에서는 C&C 서버의 주소가 아닌 정상 서버의 IP 주소도 존재하는데(예: 구글), 이러한 IP 주소가 한 쌍의 악성코드에서 등장했다고 하여 두 악성코드의 유사도가 실제로 높다고 결론 내리는 것은 바람직하지 않기 때문이다. <그림 22>에서와 같이 PDB는

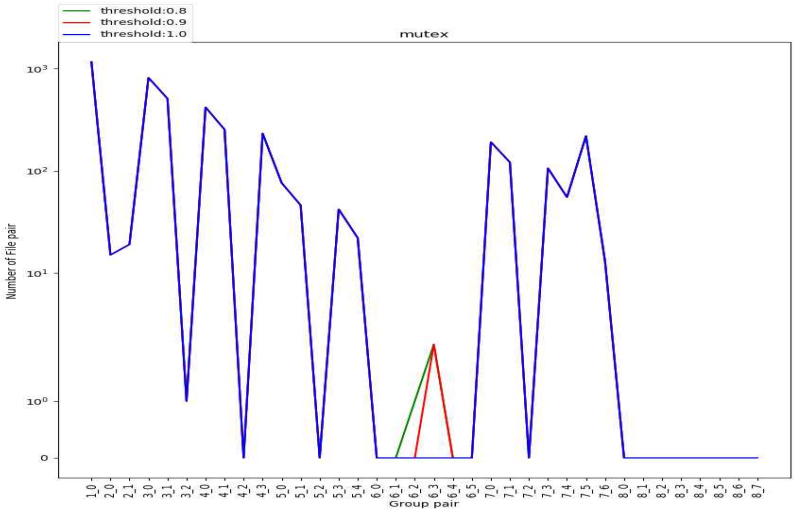
모두 0의 값이 나왔는데, 이는 0.8 이상의 높은 임계값으로는 “/” 문자로 워드를 구분하여 이분 그래프를 이용하는 방식으로 구현되는 ABMB 알고리즘으로는 유사파일을 찾는 것이 어려움을 나타낸다.

반면에 <그림 23>과 <그림 24>는 정적 분석과 동적 분석의 대표적인 특징 정보인 API집합과 함수를 이용한 ABMB 알고리즘 적용 결과를 보여주는데, 동일한 x값에서 y값이 동시에 높아지는 현상이 발견된다. 한 쌍의 악성코드 파일이 두 그래프에서 모두 유사도가 높은 것으로 발견되었다면, 이 파일들은 실제로도 매우 유사한 파일로 해석하는 것이 타당하다. 하지만 이 둘은 이미 다른 공격그룹에 배정이 되었다. 상세한 추가 분석 과정을 통해서 이 둘이 실제로 동일 공격그룹에 재배정될 가능성이 있음을 합리적으로 추측해볼 수 있겠다. 두 그래프는 서로 공통점과 차이점을 가지고 있다. API 집합 기반의 분석과 함수기반의 분석 모두 6번 그룹과 7번 그룹, 0번 그룹과 2번 그룹의 쌍의 개수가 다른 그룹의 쌍에 비해 많다. 그에 비해 2번 그룹과 7번 그룹은 3번 그룹과 5번 그룹은 서로 다른 결과를 보여준다. 이는 정적 분석으로 분석한 코드가 상당히 비슷함에도 불구하고 실제 동적 분석으로 실행된 API 집합에서는 다른 양상을 보이는 것이다. 원인을 분석한 결과, 많은 경우 악성코드가 패킹되어 실제 악성 행위를 하는 코드가 은닉화되고 정적 분석을 통해 노출되는 암복호화 코드의 유사성으로 인하여 이런 결과가 나온다는 것을 알 수 있었다.

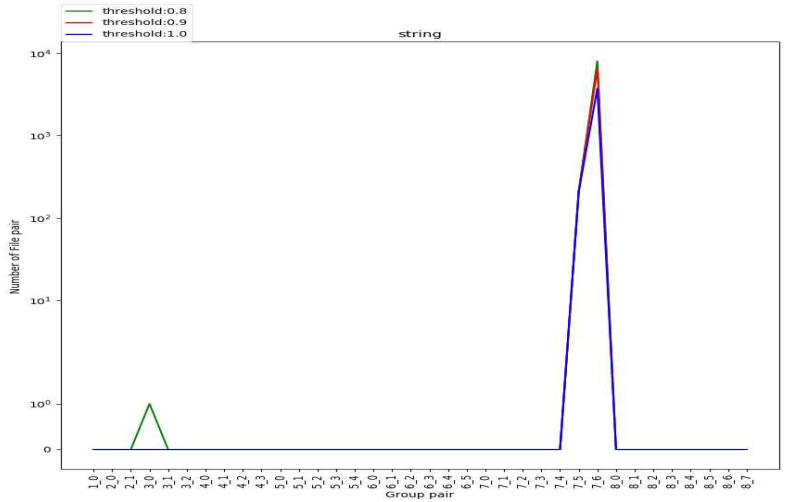
만약, 어느 악성코드 파일 쌍이 <그림 19>~<그림 24>의 모든 그래프 또는 다수의 그래프에서 유사 파일 쌍으로 발견되었다면, 이 파일 쌍은 실제로도 매우 유사할 가능성이 높다. 다만 어떤 이유에 의해서 또는 미처 유사 관계를 확인하지 못하여 보안 전문가에 의해서 다른 공격그룹으로 배정된 것이다. <그림 25>는 6개의 ABMB 그래프 중 x개의 그래프에서 유사하다고 판별된 파일 쌍의 개수를 나타낸다. x의 최대값은 4인데, 4개의 ABMB 알고리즘에서 유사하다고 판별된 파일 쌍의 개수는 1,000개보다는 작다는 것을 알 수 있다.

본 논문에서는 3개 이상의 ABMB 알고리즘에서 유사하다고 판별된 파일 쌍에 주목했다. 이 정도면 안전하게 유사 파일로 간주할 수 있다고 판단했으며, 단지 보안 전문가에 의해서 다른 공격그룹으로 분류되었다고 볼 수 있다. <그림 26>은 3개 이상의 ABMB 알고리즘에서 유사하다고 판별된 파일 쌍에 대해서 보안 전문가들이 이

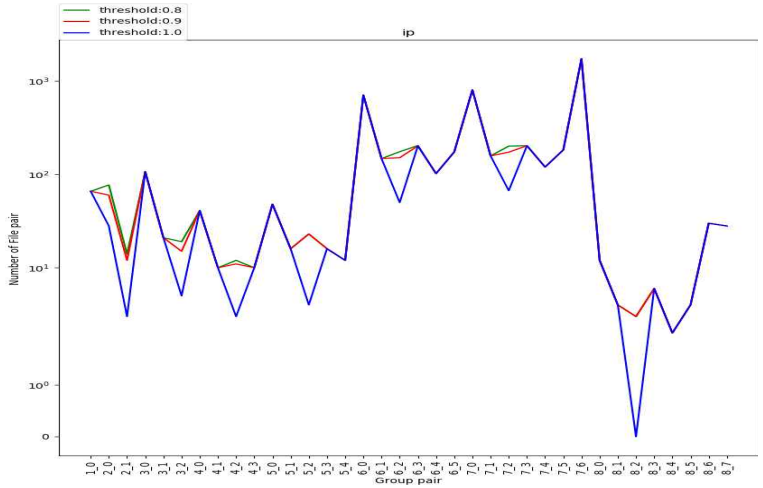
쌍을 어떻게 분류했는지를 보여준다. 이 그래프에서 x축은 각 그룹별 서로 다른 쌍을 의미를 하고 y축은 세 개 이상의 요소에서 비슷한 유사도를 가진 쌍의 개수를 의미한다. 따라서 이 그래프에서 y값이 높다는 것은 해당되는 두 개의 그룹이 ABMB 알고리즘으로는 상당히 유사하게 측정되었다는 것을 의미한다. 이 그래프에서는 대표적으로 (0,1), (1,3), (5,7), (6,7)의 그룹이 서로 다른 그룹이지만 상당히 유사하게 나타났다.



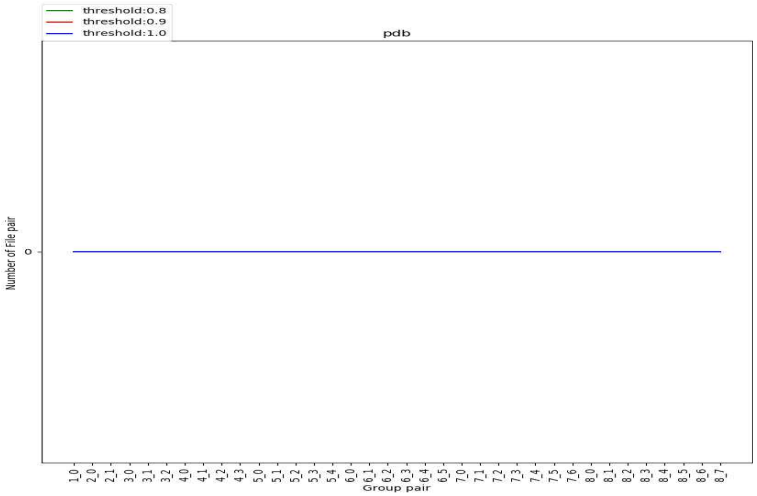
<그림 19> 뮤텍스 정보로 ABMB가 새롭게 발견한 유사파일 쌍의 개수 (공격그룹 쌍 vs 파일 쌍의 개수)



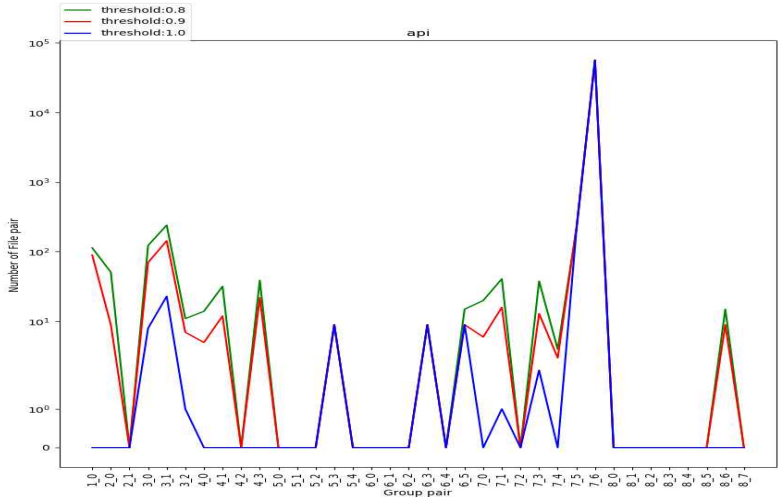
<그림 20> 문자열 정보로 ABMB가 새롭게 발견한 유사파일 쌍의 개수 (공격그룹 쌍 vs 파일 쌍의 개수)



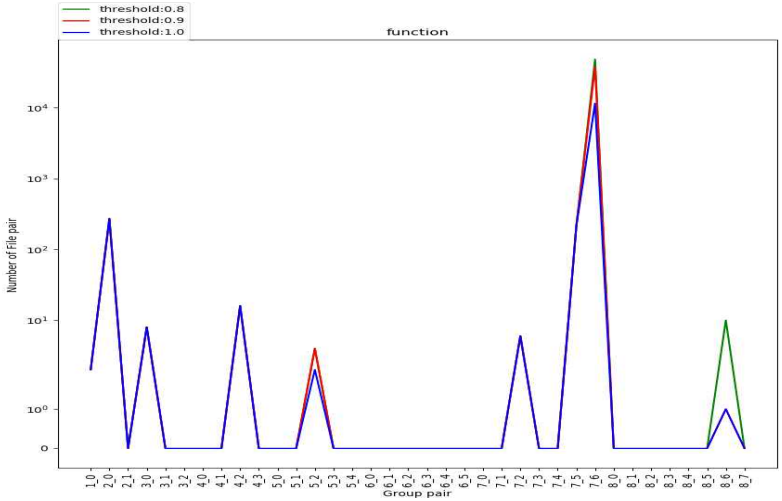
<그림 21> IP 주소 정보로 ABMB가 새롭게 발견한 유사파일 쌍의 개수 (공격그룹 쌍 vs 파일 쌍의 개수)



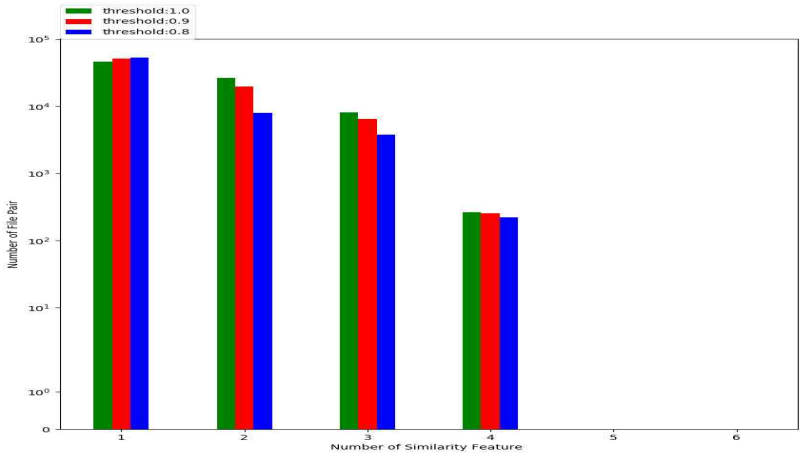
<그림 22> PDB 정보로 ABMB가 새롭게 발견한 유사파일 쌍의 개수 (공격그룹 쌍 vs 파일 쌍의 개수)



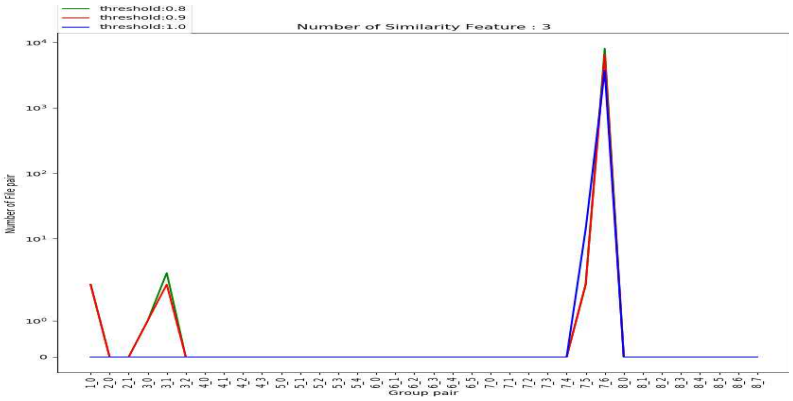
<그림 23> API 집합 정보로 ABMB가 새롭게 발견한 유사파일 쌍의 개수 (공격그룹 쌍 vs 파일 쌍의 개수)



<그림 24> 함수 정보로 ABMB가 새롭게 발견한 유사파일 쌍의 개수 (공격그룹 쌍 vs 파일 쌍의 개수)

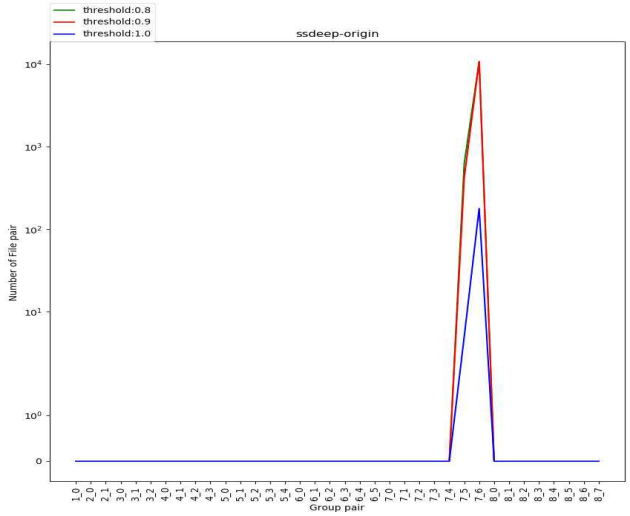


<그림 25> x개의 특징 정보에서 유사하다고 판별된 파일 쌍의 개수
(특징 정보 수 vs 파일 쌍의 개수)



<그림 26> 3개의 특징 정보에서 유사하다고 판별된 파일 쌍의 분포
(공격그룹 vs 파일 쌍의 개수)

3. 퍼지 함수 실험



<그림 27> ssdeep을 적용한 정보에 따른 공격그룹 예측 오차

퍼지 함수 중 가장 유명한 ssdeep을 사용해서 유사 파일의 쌍을 구하는 실험을 진행했다. 본 실험의 목적은 본 논문에서 제안하는 ABMB가 기존의 ssdeep 기술보다 얼마나 우수한지를 확인하는 것이다. 악성코드 파일에 대해서 ssdeep을 적용하고, 모든 파일 쌍에 대해서 유사도를 비교하였다. <그림 27>과 같이 ssdeep은 제한된 공격그룹 쌍에 대해서만 유사파일을 찾는 것을 확인할 수 있었다. 특히, 임계값을 가장 높게 설정한 "threshold:1.0" 그래프의 경우는 184개의 유사 파일 쌍을 찾는데 그쳤는데, 이는 동일한 상황에서 ABMB가 찾아낸 최소 3,766개에 비해서 크게 낮은 수치이다. 즉, ABMB는 기존 악성코드의 유사도를 측정하기 위해서 가장 많이 사용되는 ssdeep보다 우수한 성능을 보임을 확인할 수 있었다. 이러한 이유는 앞 장에서 기술한 것처럼 ssdeep은 파일의 크기가 2배 이상 차이가 날 경우 유사성 검사를 제대로 수행하지 못하는 등 근본적 한계가 있기 때문이다.

V. 결론

본 논문에서는 이분 그래프를 이용하여 다각적 측면에서 악성코드 사이의 유사도를 측정할 수 있는 새로운 알고리즘과 프로그램 구현 방법을 제안했다. 제안하는 기술을 사용하면, 기존의 보안 전문가들의 휴리스틱 지식과 퍼지 해시 함수로는 찾을 수 없었던 깊은 관련성이 의심되는 매우 유사한 악성코드 쌍을 찾을 수 있으며, 특히 동일 공격그룹으로 강하게 의심되는 악성코드 리스트를 자동으로 생성하는 것이 가능하다. 실험을 통해서 국내 주요 기관을 공격 대상으로 하는 희귀 악성코드 데이터 셋을 대상으로 제안하는 기술의 우수성을 증명하였다. 제안하는 기술의 범위에는 새로운 알고리즘 이론과 실제 구현한 프로그램 코드가 포함되며, 전처리부터 유사 악성코드 리스트 반환까지 자동 처리가 가능한 플랫폼까지 포함된다. 제안 기술은 국내 금융권을 노리는 공격그룹을 검출하는데 있어서 편리하고 강력한 자동화 도구로서 보안 전문가의 업무 능력을 크게 향상시킬 수 있을 것으로 기대되며, 사이버공격에 사전 대비할 수 있는 보안 도구로서 활용될 수 있을 것이다.

향후에는 본 논문에서 제안한 기술로 분석된 유사한 악성코드 정보들을 빅데이터로 누적시킴으로써 국내 주요기관을 노리는 악성코드 그룹 및 배후 공격그룹을 체계적으로 자동 프로파일링하는 서비스에 대해서 후속 연구가 진행될 예정이며, 이 과정에서 인공지능, 빅데이터, 스토리지 등 다양한 컴퓨팅 분야의 기술들이 융합되는 연구를 진행할 예정이다. 또한, 처리되는 악성코드 개수를 현재 수천 개에서 향후 수백만 개로 확장했을 때에도 확장성 있게 프로그램이 동작할 수 있도록 관련 연구를 진행할 예정이다.

참고문헌

[1] “2017 사이버 위협 인텔리전스 보고서-국내를 타깃으로 하는 위협그룹 프로파일링”, 금융보안원, 경기도, Aug 2017.

[2] “Andariel Group 동향 보고서”, 안랩 시큐리티 대응센터 분석연구팀, 경기도, May 2018.

[3] Xin Hu, Kang G. Shin, Sandeep Bhatkar et. al., “MutantX-S: Scalable Malware Clustering Based on Static Features,” *USENIX ATC*, University of Michigan, State of Michigan, 2013.

[4] J. Jang, D. Brumley, and S. Venkataraman, “BitShred: Feature Hashing Malware for Scalable Triage and Semantic Analysis,” *ACM CCS*, 2011.

[5] 고동우, 김휘강, “API 콜 시퀀스와 Locality Sensitive Hashing을 이용한 악성코드 클러스터링 기법에 관한 연구”, 정보보호학회논문지, vol 27, no 1, pp. 91-101, 2017.2.

[6] 한병진, 최영한, 배병철, “악성코드 DNA 생성을 통한 유사 악성코드 분류기법”, 정보보호학회논문지, vol 23, no 4, pp. 679-694, Aug 2013.

[7] 강홍구, 김경한, 유대훈 외 2명, “악성코드 행위기반 유사도 측정 기법 연구”, *한국통신학회 추계종합학술발표회*, Nov 2017.

[8] 조인겸, 임을규, “서열 정렬 기법을 이용한 악성코드 유사도 분석의 성능 개선”, 정보과학회 컴퓨팅의 실제 논문지, vol 21, no 3, pp. 263-268, Mar 2015.

[9] J. Kornblum, “Identifying Almost Identical Files Using Context Triggered Piecewise Hashing,” Digital Investigation Journal, vol 3, pp. 91-97, Sep 2006.

[10] Y. Li, S. C. Sundaramurthy, A. G. Bardas et. al., “Experimental Study of Fuzzy Hashing in Malware Clustering Analysis”, *CSET 15 Proceedings of the 8th USENIX Conference on Cyber Security Experimentation and Test*, pp. 8-8, 2015.

[11] Wikipedia, Program database[Internet], Available: https://en.wikipedia.org/wiki/Program_database, 2018.07.30.

[12] Ahnlab, ASEC 리포트 vol 91[Internet], Available: https://www.ahnlab.com/kr/site/securityinfo/asec/asecReportView.do?groupCode=VNI001, 2018.07.30.

[13] 김동진, 조성제, “함수 수준 특징정보 기반의 오픈소스 소프트웨어 모듈 탐지”, 한국정보과학회 정보과학회논문지, vol 42, no 6, pp. 713-722, Jun 2015.
[14] J. Saxe and K. Berlin, “Deep neural network based malware detection using two dimensional binary program features”, MALWARE ’15 Proceedings of IEEE Malicious and Unwanted Software (MALWARE), pp. 11-20, Aug 2015.
[15] 최선오, 김영수, 김종현 외 1명, “딥러닝을 이용한 악성코드탐지 연구 동향”, 정보보호학회지, vol 27, no 3, pp. 20-26, Jun 2017.
[16] 조영복, “딥러닝 기반의 R-CNN을 이용한 악성코드 탐지 기법”, 한국디지털콘텐츠학회 논문지, vol 19, no 6, pp. 1177-1183, Jun 2018.
[17] IDA Pro, IDA Pro[Internet], Available: https://www.hex-rays.com/products/ida/index.shtml, 2018.07.30.
[18] Cuckoo Sandbox, Cuckoo Sandbox[Internet], Available: https://cuckoosandbox.org/, 2018.07.30.
[19] Wikipedia, API[Internet], Available: https://ko.wikipedia.org/wiki/API, 2018.07.30.
[20] Microsoft, CreateMutex()[Internet], Available: https://msdn.microsoft.com/ko-kr/library/ms919034.aspx, 2018.07.30.
[21] Wikipidia, 이분 그래프[Internet], Available: https://ko.wikipedia.org/wiki/이분_그래프, 2018.07.30.

금융규제 혁신을 위한 레그테크(RegTech)의 역할과 국내 레그테크 도입 방향

- 영국 금융당국의 역할을 중심으로 -

주 문 호*

* 고려대학교 정보보호대학원 정보보호학과

요 약

금융권에서의 빅데이터 활용 잠재 가치는 최상위권으로 평가되고 있으며, 디지털 기술의 발전으로 금융 시장에서 거래되는 데이터의 양 또한 기하급수적으로 증가하고 있다. 뿐만 아니라 지속적인 규제환경의 변화로 인해 규제이행을 위해 요구되는 데이터도 증가하고 있기에, 앞으로 금융권에서 복잡화·다각화될 규제들을 대응하기 위해서는 상당히 많은 자원, 인력, 비용이 요구될 것으로 예상된다. 이에 대응하여 최근 AI 기반의 준법감시시스템이 등장하는 등 첨단기술을 통한 규제준수 자동화 처리에 대한 기대감이 증가하고 있다. 앞으로 다가올 양적 규제(Quantitative Regulatory)의 시대에 있어, 동적 금융규제(Dynamic Financial Regulation) 대응을 통해 문제를 해결하고자 하는 것이다.

규제(Regulation)와 기술(Technology)의 합성어인 레그테크(RegTech)는 규제 준수를 도와주는 기술로써, 미국, 영국 등 금융선진국을 중심으로 점차 시장이 조성되고 있으며, 금융당국들은 국가적 차원에서 레그테크 산업을 적극 도입하기 위해 적극 노력 중이다. 그러나 레그테크는 아직 법률적·학술적으로 확립된 개념이 아니며, 그 범위와 활용 가능성에 대한 연구 또한 부족하여 금융당국이 레그테크 도입 및 활성화 정책을 수립하고자 함에 있어 어려움을 겪고 있는 상황이다.

이에 본 논문은 레그테크와 관련한 다양한 학술적, 실무적 논의들을 종합 검토하고 영국 금융당국의 레그테크 정책 추진사례를 실증 분석하여 레그테크의 발전모델 및 시사점을 도출하고, 이를 통해 국내 금융권의 레그테크 도입 가능성과 향후 과제에 대해 논의해보고자 한다.

키워드

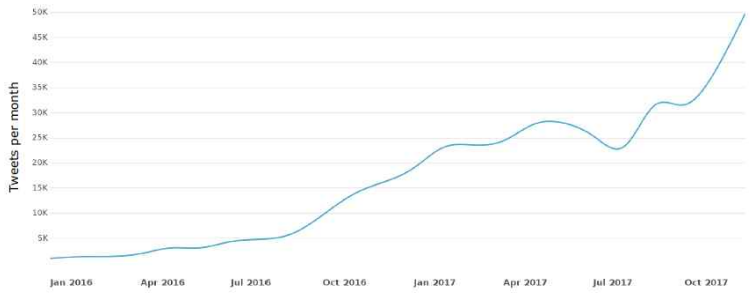
빅데이터, 핀테크, 레그테크, 금융규제, 규제대응, 금융당국, RegTech

목 차

Ⅰ. 서 론

최근 빅데이터, 인공지능, 블록체인 등 다양한 신기술의 발전과 금융-非금융 간 융합으로 인해 금융 산업에서도 4차 산업혁명으로의 변화가 가속화되고 있다. 맞춤형 금융서비스, 신용평가 체계의 고도화, 비대면 금융거래의 확대, 지급결제수단의 간편화·다양화 등이 새로운 금융 산업의 패러다임을 이끌 것으로 예측되나, 기존과는 전혀 다른 차원의 금융 환경 변화로 인해 사이버공격을 통한 금전적 피해의 심화, 전자금융사기 및 개인정보보호 위협 증대, 지능화된 금융 범죄 등 새로운 위험요인도 함께 등장하고 있다. 이에 금융당국은 과학기술의 발전과 신기술의 도입으로 인해 야기되는 다양한 위험에 대한 보호 장치로써 다양한 규제 및 규정을 새롭게 도입하고 있으며, 금융기관이 감당해야할 준법의무의 수준은 이전까지 없었던 강도로 강화되고 있다. 이러한 규제 환경의 변화는 금융당국의 규제 관리감독 책임을 가중시키고 있으며, 규제의 당사자인 금융기업들의 컴플라이언스 인력 및 비용 부담 또한 증대되고 있는 상황이다.

이 때문에 금융 업계에서는 금융 규제 관련 요구사항을 빈틈 없이 충족시키고, 규제 변화에 유연하게 대응하면서도 관련 비용을 줄여줄 수 있는 기술적 방안에 대한 필요성이 부각되었고, 이에 대한 해결책으로 금융 규제 대응을 위한 IT 新기술이라 불리는 레그테크(RegTech : Regulatory Technology) 개념이 고안되었다. 실제 2016년 이후 레그테크는 세계적으로 큰 이슈가 되고 있으며, 레그테크 관련 스타트업들이 본격적으로 금융 업계에 뛰어들고 있는 상황이다.



<그림 1> 2016년 이후 트위터 상 레그테크(RegTech) 언급 증가 추이

그러나 레그테크는 아직 업계·학계에서 그 개념과 범주가 확립되지 않았고, 레그테크의 활용 가치와 성장 가능성 또한 제대로 예측되지 않고 있는 상황이기에, 금융당국이 레그테크의 도입 및 활성화를 위한 정책 및 전략을 수립함에 있어 불확실성이 큰 실정이다.

이에 본 논문은 레그테크의 개념과 특성을 파악하여 국내 환경에 적합한 레그테크 도입 방향을 제언하는 것을 목적으로 한다. 본 논문은 Ⅱ장에서 금융규제 환경 변화에 따른 컴플라이언스 혁신 방안으로 레그테크를 주목하고, Ⅲ장에서 레그테크의 개념과 가치, 확장 가능성에 대해 고찰한다. 또한 Ⅳ장을 통해 레그테크 관련 정책을 가장 활발하게 추진하여 가시적인 성과를 내고 있는 금융 선진국인 영국 사례를 분석하여 레그테크 활성화를 위한 금융당국의 역할과 시사점을 도출하도록 하며, 이를 기반으로 Ⅴ장에서 레그테크의 발전모델을 제시하고 국내 레그테크 도입 방향에 대해 제언하고자 한다.

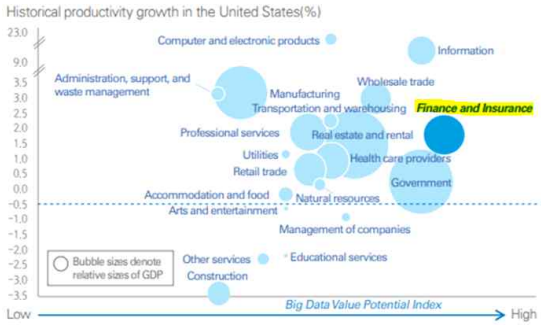
Ⅱ. 금융 규제 환경의 변화와 컴플라이언스 혁신의 필요성

1. 데이터 사회의 도래와 금융 규제 환경의 변화

Dell Technologies의 Michael Dell 회장은 지난 2018년 4월 30일 개최된 Dell Technologies World 2018 컨퍼런스에서 "2020년에는 한 군데 도시에서 불과 하루 동안 생산되는 데이터가 무려 200페타바이트(PB)에 다다를 것"이라고 예측하였다. 또한, "데이터는 Digital Transformation을 가속하는 연료로서 AI와 머신러닝, 5G 같은 기술을 통해 제품과 서비스를 향상시키고, 그 과정에서 다시 수많은 데이터가 생성되는 선순환 구조가 디지털 혁신의 속도를 가속화시킨다"며 디지털 변혁(Digital Transformation) 사회가 코앞에 다가왔음을 강조하였다. 실제로 최근 인공지능(AI), 사물인터넷(IoT) 등 빅데이터 구현을 위한 선행기술이 시장을 주도하면서 빅데이터 시장이 급속 성장하고 있으며, 이에 따라 글로벌 빅데이터 시장은 2026년까지 약 847억 달러에 이를 것으로 예상되고 있다.[1] 이는 본격적으로 데이터 사회가 도래함에 따라 사회 전반의 모든 현상들이 데이터로 기록되어 활용되고 있으며, 방대한 데이터를 수집하고 이를 빠르고 효율적으로 이해하여 활용할 수 있는 능력이 향후 시장에서 경쟁우위를 점할 수 있는 중요한 요소가 될 것이라는 것을 의미한

다.

금융권도 예외는 아니다. McKinsey는 금융권에서 빅데이터의 잠재 가치를 전체 산업 중 최상위권으로 분류하였으며(<그림 2>), IDC는 2020년까지 세계 데이터 시장에서 금융 분야가 상위 5개 산업으로써의 영향력을 계속적으로 행사할 것으로 내다보았다(<그림 3>). 금융권 기업이 빅데이터 활용을 본격화하면서 빅데이터를 수익 창출의 핵심원으로 취급하고 있으며, 고객 맞춤형 서비스 등 고객 중심 경영을 위해서도 빅데이터를 다양한 방식으로 활용하고 있다.[2]



<그림 2> 산업 분야별 빅데이터 잠재 가치 비교

Source : US Bureau of Labor Statistics; McKinsey Global Institute analysis, 2010.

이와 같이 금융권이 많은 양의 데이터를 보유하게 되고 다양한 목적으로 활용하게 됨에 따라 이와 관련한 새로운 위험이 발생하게 되었고, 이에 대응하기 위한 금융규제방식 또한 빠른 속도로 변화하고 있다. 금융거래 데이터가 기하급수적으로 증가함에 따라 FATCA(Foreign Account Tax Compliance Act)[1], AML(Anti-Money Laundering law)[2], 불공정 거래 감시 등 금융 규제 대응을 위한 실시간 데이터 분석에 많은 비용과 자원이 투입되고 있다. 핀테크의 확산에 의해 새로운 사업 모델이 발달함에 따라 거래 분석의 복잡성이 증가하고 있으며, 위험 분석, 내부 통제 등 규

1) 미국 국세청(IRS)이 해외 금융회사로부터 미국 납세자가 보유한 제공받을 수 있도록 한 법률로써, 세계 금융회사들이 미국 납세자가 보유한 5만달러 이상 계좌에 대한 정보를 미 국세청(IRS)에 제공하도록 의무화한 조항이며, 버락 오바마 정부가 2010년 도입한 역외탈세 방지법의 일부이다. 이를 어기는 금융회사에 대해선 미국 내 소득의 30%를 원천징수하는 불이익을 준다. (한경 경제용어사전)

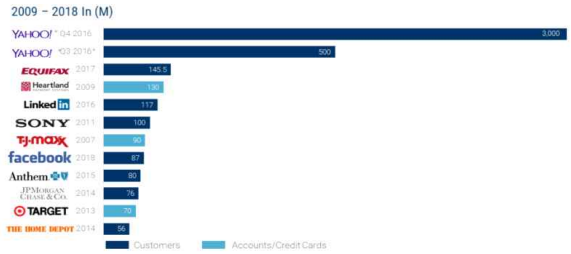
2) 資金洗濯防止法. 각종 범죄와 부정·비리로 조성된 자금을 출처가 드러나지 않도록 위장하는 것을 방지하기 위한 법률. 미국의 경우 '자금세탁' 과정을 차단하기 위해 1만 달러 이상의 현금 입출금은 모두 국세청에 보고하도록 하고 있으며, 영국은 5천 파운드(약 7백만 원) 이상을 은행에 예치할 경우 출처와 조성 경위를 밝히도록 되어 있다. (행정학사전, 2009. 1. 15., 대영문화사)

제이행을 위해 문서, 음성, 이메일 등 점차 더 다양한 비정형 데이터 분석이 필요해짐에 따라 데이터 분석을 위한 인력 및 비용 부담의 가중은 한동안 계속될 것으로 보인다.

<그림 3> 2016-2020년 세계 데이터 시장 주요 산업 분포

Source : IDC Worldwide Semiannual Big Data and Analytics Spending Guide, 2015.

또한 금융 기관 및 기업이 고객 서비스를 제공하기 위해 보유하는 개인정보가 증가함에 따라, 해킹 사고 등으로 유출되는 개인정보의 양과 그 파급력 또한 증대되고 있고(<그림 4>), 이에 대응하기 위해 개인정보보호와 관련한 규제도 세계적으로 강화되고 있는 추세에 있다. 빅데이터 사회의 도래에 따라 규제 이행을 위해 요구되는 데이터도 증가한 것이다. 뿐만 아니라 인공지능, 딥러닝 등 지능형 기술이 최근 급속도로 발전되면서 비구조화된 데이터가 풍부한 금융산업이 큰 영향을 받고 있으며, 기술 변화를 반영한 규제기관의 규제프로세스의 변화가 요구되고 있다.[3]



<그림 4> 최근 기업 개인정보 유출 사건의 규모 (2009-2018년)

Source : CBInsight, "Regtech:What It Is,Why Now,&Why It Matters" , Research Briefs, 2017.11.

실제로 2008년부터 2015년 중 금융규제 변화 비율은 이전에 비해 492% 증가하는 등 금융규제의 변동성은 지속적으로 확대되고 있으며[4], 2018년부터 GDPR[3], PSD 2[4], MiFID II/MiFIR[5] 등의 규제가 연달아 신규 적용되는 등 금융권이 대응하여야 할 규제 환경이 급격히 변화되고 있다.

2. 금융당국의 규제 관리감독 책임 증대

금융 시장에서 가장 중요한 것은 정보인데, 고도화된 빅데이터 처리가 가능해짐으로써 정보 처리의 양과 속도 그리고 정확성이 급격히 상승되었고, 여기에 인공지능 기술까지 접목되면서 금융시장, 금융회사, 감독기관 모두에게 상당한 영향을 미치고 있다. 기술 발전이 이전과 비교할 수 없을 만큼 빠른 속도로 진행됨에 따라, 금융당국이 기존의 금융시장을 규율해 왔던 규제 방식도 변화가 필요해졌으며, 금융 산업을 둘러싼 규제 환경이 빠르게 변화하면서 정부의 규제 관리 책임도 갈수록 증대되고 있는 상황인 것이다.

금융 산업은 빠르게 기술의 변화를 활용하여 수요자의 의사를 반영하고 서비스 다양화를 시도하기 때문에, 금융당국은 이러한 기술의 변화속도를 미리 탐지하고, 앞서 규제와 감독으로 연결시켜야 한다.[4] 따라서 금융당국의 규제관리 역할이 상당히 중요하며, 금융당국은 규제기관의 규제 프로세스에서부터 빠르게 기술의 변화를 반영하고 대응하도록 해야 한다.

이에 대한 중요성을 가장 잘 보여주는 사례가 Flash Crash 사태이다. Flash Crash는 2010년 5월 6일 미국 다우지수가 5분 만에 9.2% 하락한 후 3분 만에 회복한 사건으로, 약 6천억 달러(한화 약 600조)의 손실이 발생하였다. 해당 사건은 초단타 매매 기법인 스푸핑을 이용하여 인위적인 매도로 주가 하락을 유도하여 차익을 실현한 금융 사기로 밝혀졌으며, 규제당국은 2009년부터 이를 인지하였으나 대응에는 실패하였다. 금융당국은 초당 거래 기록을 분석할 수 있는 체계를 구축하고 있었지

3) 개인정보보호 규정(General Data Protection Regulation; GDPR). 유럽의회에서 유럽 시민들의 개인정보보호를 강화하기 위해 만든 통합 규정으로 2018년 5월 25일부터 적용됨.

4) 결제서비스 지침(Second Payment Services Directive; PSD2). PSD는 모든 유럽 경제 지역의 지불에 대해 동일한 규칙을 적용하여 효율적이고 통합된 시장을 만들기 위한 공통 규칙으로, 유럽은행감독청(EBA)이 규정한 결제 서비스 지침 개정안인 PSD2가 2018년 1월 13일부터 적용됨.

5) 금융상품시장지침(Market in Financial Instrument Directive; MiFID II)/금융상품시장규정(Market in Finencial Instrument Regulation; MiFIR). EU 단일 금융시장 구축을 목표로 시행되었으며 EU 내 금융거래시 거래소, 금융기관 및 투자자 등이 준수해야하는 지침인 MiFID가 개정 작업을 거쳐 발표된 MiFID II는 준비기간을 거쳐 2018년 1월 3일부터 적용됨. MiFID II와 더불어 제정된 MiFIR은 회원국에 직접 적용되는 규정임.

만 실제 거래는 1/1,000,000초 단위로 이루어졌기 때문이다.

<그림 5> Flash Crash 사태로 인한 다우지수 하락

Source : WallStreet Journal, "Flash Crash course", 2015.04.22.

미국 증권당국 SEC(U.S. Securities & Exchange Commission)은 해당 문제의 해결을 위해 10억 개 이상의 모든 거래 데이터들을 최소 6개월에서 1년 동안 수집하고 분석하여야 한다는 의견을 내놓았다.[5] 금융당국에게 엄청난 양의 데이터를 보관하고, 이를 실시간으로 빠르고 정확하게 분석할 수 있는 역량이 요구된 것이다. 이러한 역량이 없다면 문제에 '대응' 하기는커녕 문제를 '인식' 조차 못할 수 있다. 이에 따라 이후 미국 증권거래위원회는 빅데이터 및 클라우드 기반의 MIDAS(Market Information Data Analytic System) 시스템을 도입하여 증권 시장의 모든 거래 정보를 과학적으로 분석하고 있다. Flash Crash 사태는 기술이 발전되고 금융시장 환경이 변화됨에 따라 전통적인 금융규제방식 및 기술이 한계에 도달하여 새로운 유형의 위험이 발생한 대표적 사례이자, 금융당국이 새로운 규제 환경 내에서 강화된 규제관리 책임을 이행하기 위해 규제와 기술을 결합한 중요한 선례라고 볼 수 있다.

국내에서는 최근 삼성증권의 주식배당 입력 오류 사건이 이슈가 되었다. 업계에서는 직원의 도덕성 해이, 공매도 시스템의 허점 등 다양한 원인 등이 결합되어 발생한 사건으로 해석하였지만, 주식거래시스템 및 내부통제 시스템이 이러한 위험을 선제적으로 예방하고 즉각 대응할 수 있도록 설계되었다면 근본적으로 막을 수 있는 사건이었을 것이라 생각된다. '1000원' 을 '1000주' 로 입력하는 것이 가능했다는 점, 배당금 지급 시 단위 항목에서 '원' 과 '주' 의 선택 항목이 없었다는 점, 발행주식수를 초과하는 수량의 주식물량이 입고되어도 시스템 상 오류로 인식

되지 않았다는 점, 주식배당 오류 발생 시 이를 감지하고 차단할 수 있는 통제장치가 없었다는 점 등 프로세스 전 과정에서 문제가 발생하였다.[6] 이에 업계에서는 금융당국이 후속조치 중 하나로 효율적인 내부통제를 위해 규제 대응을 도와주는 기술적 방안을 강조하는 정책과 제도를 실시할 가능성이 높은 것으로 보고 있다.[7] 삼성증권의 주식배당 입력 오류 사건은 금융시장에서 벌어질 수 있는 불법 행위나 실수로 인해 발생할 수 있는 불확실한 리스크들을 선제적 기술 설계를 통해 최소화 시킬 수 있음을 보여준다.

국제적인 규제 변화 및 글로벌화 움직임도 금융당국의 규제 관리감독 부담을 증대시키는 큰 요인이다. 2008년 금융위기 이후 높은 수준의 자본건전성 유지, 파생상품 투자 제한 등 전세계적으로 수많은 규제들이 도입되면서 각국 정부의 관리감독 부담이 증대되어 왔다. 또한 종래 금융 기관의 준법에 대한 요구는 과거 각 국가의 금융 감독기관에 의해 행해져서 이행 일정이나 이행 수준이 각 국가별로 자율적으로 이루어져 왔으나, 최근 첨단기술의 발전으로 국가 간 경계가 사라지자 최근 FATF(국제자금세탁방지기구)나 FATCA[6]/CRS[7]처럼 각 국가 간의 협정에 의해 정해진 국제 표준 협약을 따르는 것으로 변화되어가고 있다. FATF와 같은 글로벌 감독기구가 설립되는 등 금융 시스템의 글로벌화에 따라 준법의 기준 및 제도가 글로벌화 되고 있고, 국제 표준 및 각 국의 법률의 빈번한 변경으로 인해 새롭게 감독하고 대응하여야 할 법규 및 규정 또한 늘어나고 있다. 이와 같은 국제 표준들은 전 세계 금융기관을 대상으로 동시 적용되는 추세이며, 선택이 아닌 의무 사항으로 적용 되기 때문에 금융당국의 규제감독 부담의 심화는 피할 수 없는 현실이 될 것으로 보인다. 이에 맞춰 국내 금융규제 또한 기존의 AML에 더하여 RBA, FATCA, CRS 등 신규 규제 및 제도가 지속적으로 생겨남에 따라 기존 AML의 고도화 등 지속적인 고도화 사업을 추진할 것으로 전망된다.[8] 이에 대응하여 금융정보분석원(KoFIU)에서는 2019년으로 예정되어 있는 국가 상호평가에 맞추어 더욱 강도 높은 이행 수준 제고를 독려 중인 상황이다.[9]

이처럼 금융 당국은 증가하는 새로운 규제 및 변경 요건 그리고 그 복잡도의 증가로 단기간 내 규제 대응을 해야 하는 새로운 위기를 맞고 있으며, 이는 금융기관의

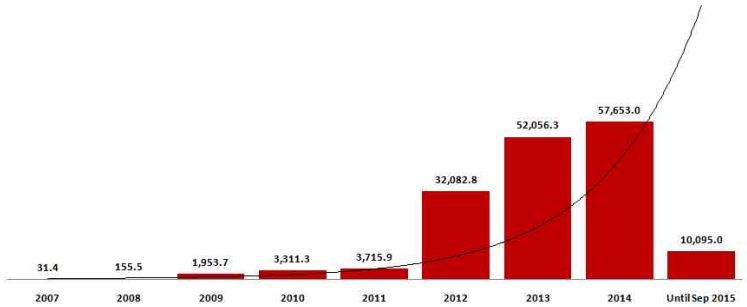
6) 해외금융계좌 신고법(Foreign Account Tax Compliance Act). 세계 금융회사들이 미국 납세자가 보유한 5만 달러 이상 계좌에 대한 정보를 미 국세청(IRS)에 제공하도록 의무화한 미국 법률로, 미국 납세의무자의 역외 탈세 방지를 위해 버락 오바마 정부가 2010년 도입함. (한경 경제용어사전)

7) OECD CRS(OECD Common Reporting Standard). 글로벌화 된 시장 환경과 이에 따른 금융시장의 글로벌 확산으로 인하여, 해외 금융 자산에 대한 조세가 시급하고도 중요한 문제로 부각됨에 따라, G20에서 OECD에 의뢰하여 개발한 글로벌 AEOI 표준

전략과 사업방향, 나아가 국가 금융 산업 경쟁력에도 상당한 영향을 미치기에, 각국의 금융당국들은 보다 효율적이고 실질적인 규제 감독 체계를 구축할 수 있는 방안을 고민하고 있는 상황이다.

3. 금융기업의 규제이행 부담 증가

규제 환경의 변화는 금융당국의 규제 관리감독 책임도 가중시키지만, 규제의 직접 당사자인 금융기업에게 더욱 큰 영향을 미친다. 사후규제 체계로의 전환, 징벌적 손해배상 강화 등 최근 급격한 속도로 이루어지고 있는 글로벌 규제 패러다임 전환은 금융 기업에게 상당한 부담으로 다가오고 있다. 실제로 2008년 이후 미국 은행의 규제위반 횟수 및 벌금이 지속적으로 증가하고 있으며 2014년도까지 벌금 및 합의금으로만 1,600억 달러 이상의 지출이 발생하였다.(<그림 6>)



<그림 6> 글로벌 금융기관에 의한 벌금 및 합의금 현황(USD Mn)(2007-2015년)

Source : LTP Team, "Strategic Analysis of RegTech: A Billion-Dollar Opportunity", Lets Talk Payment, 2016.04.

보스턴컨설팅그룹(BCG)은 2008년 글로벌 금융위기 이후 자금 세탁, 시장 조작, 테러 자금 조달 등에 대한 규제가 강화되면서 전 세계 은행이 3,210억 달러(약 369조원) 이상의 벌금을 낸 것으로 분석했다.[10] 한 예로 미국 재무부 산하의 금융범죄단속반 'FinCEN'은 플로리다 주 지브롤터 프라이빗 뱅크(Gibraltar Private Bank)와 트러스트 컴퍼니(Trust Company)에 자금세탁방지(AML) 프로그램의 '상당한' 결함을 이유로 벌금 400만 달러를 부과하였다.[11]

우리나라의 경우도 예외는 아니다. 지난 해, 농협은행의 뉴욕지점은 뉴욕 금융감독

청(NUDFS)로부터 AML(자금세탁방지) 대응이 미흡하다는 이유로 1,100만 달러(한화 약 129억)의 과태료를 부과하였다. 농협은행 뉴욕지점의 지난해 수익은 67억원으로, 수익보다 규제대응실패로 인한 과태료가 2배를 상회하는 수준이다. 형식적인 규제 대응 정도에 만족하였던 농협은행과 달리 미 금융당국은 AML 대응과 관련해 특별히 정형화된 모델을 요구한 것이 아니라 시스템의 완비여부, 전문인력의 확보, 본점과 해외지점간 의사결정 프로세스의 적절성 등 실질적이고 효과적인 규제 대응 수단을 갖추는 것을 요구하였다. 이와 함께 AML 대응 이슈는 은행권의 글로벌뱅킹(국외전산)시스템 고도화 이슈와도 맞물리면서 점점 더 넓은 프로젝트 개발 범위를 요구하는 상황이다. 이에 농협은행 뉴욕지점은 AML 시스템 구축은 물론 관련 전문인력을 추가 채용하여 미국 금융당국으로부터 받은 제재를 이행하고 있는 상태이며, 국내 다른 시중은행도 뉴욕지점의 준법감시인 인력을 기존 2~5배 수준으로 증원하였다.[12] 디지털 데이터의 폭발과 한정된 컴플라이언스 전문가 공급은 현재 금융회사 컴플라이언스 업무의 비용 효율성을 가장 저해하는 요소이며[12], 컴플라이언스 불이행에 대한 규제는 금융 기관의 치명적 이미지 손상 혹은 천문학적인 벌금으로 인해 기업의 생존과 직결되고 있다.

규제 위반 벌금뿐만 아니라 규제 준수를 위한 비용 자체도 상당한 수준으로 증가하고 있다. 금융회사의 법규준수 비용은 당기 순이익의 5% 이상을 차지하고 있으며, 해당 비용은 해마다 40%씩 증가할 것으로 예측되고 있다.[13] 금융당국은 규제 이행 확인을 위해 금융기업에게 엄청난 양의 데이터를 요구하고, 관련 보고서 작성을 요청하며, 이를 위해서는 상당한 비용과 인력이 투입될 수밖에 없는 것이다. 실제로 글로벌 금융기관들이 컴플라이언스 대응에 쓰고 있는 비용은 2017년 기준 약 80조원에 달하며, 설문조사 결과 전체 금융기업 임원의 89%가 향후 2년동안 컴플라이언스 대응 관련 부서에 투입하는 비용을 늘릴 것이라고 답했다.[14]

사실 규제 이행에 쓰이는 비용은 기업의 부가가치를 높이거나 투자대비 이익이 눈에 보이지 않는 측면이 있기에 기업 입장에서는 비용 투입이 상당히 망설여질 수밖에 없다. 이 때문에 소규모 자본으로 시작하는 신규 스타트업들은 컴플라이언스를 위한 비용이 예상되는 이익에 비해 과도할 시 사업 자체를 포기하는 경우가 발생할 수 있다. 예를 들어 소액 해외 송금업을 하려는 핀테크 업체는 자금세탁 및 테러자금 방지 시스템 구축을 위해 큰 비용을 지출해야 할 것이다.[15] 반면 비교적 투자 여력이 있는 대기업에게도 계속적으로 변화하는 규제에 대응하기 위한 비용 부담은 새로운 사업 시도에 대한 위축으로 연결될 수 있다.

4. 컴플라이언스 혁신의 필요성

종래의 사람(인력) 의존적 규제, 사후 적발 위주 규제는 '빅데이터(Bigdata)', '인공지능(AI)', '자동화 및 최적화' 등으로 대표되는 새로운 환경 변화에 대응하기엔 한계점에 도달하였다. 앞으로의 컴플라이언스 대응은 점점 데이터 지향적이며, 기술 의존적인 형태로 변화할 것이다. 빠른 속도로 변화하는 규제 환경에 적응하지 못한다면, 금융당국은 불법이 발생하여도 인지하지 못하거나 인지하고도 문제를 해결할 수 없는 상황이 도래할 것이고, 규제감독 및 규제이행에 투여하는 사회적 비용은 천문학적으로 상승하여 국가 금융 산업의 경쟁력을 낮출 것이다.

금융당국은 기술의 변화속도를 미리 탐지하여 불법행위를 사전 차단하고 이를 적합한 규제와 감독으로 연결시킬 수 있는 역량을 갖추어야 하며, 증가하는 새로운 규제 및 변경 요건을 빠른 시간 안에 파악하여 효율적인 규제 감독체계를 구축하여야 한다. 금융기업은 징벌적 손해배상의 강화, 규제준수에 투입되는 비용 증대에 대응하기 위해 새로운 규제준수 전략을 모색하여야 할 시점이다. 빅데이터 분석 역량의 고도화, 인공지능(AI)을 활용한 규제 대응 자동화, 규제 변화에 따른 위험 예측과 사전 대응전략 수립 등 미래 금융 규제환경에 적합한 기술적 접근이 필요하다.

Ⅲ. 레그테크(RegTech)의 출현 : 양적 규제 시대의 대안

1. 레그테크 개념과 주요 기능

(1) 레그테크의 정의 확립

레그테크(RegTech)란 규제(Regulation)와 기술(Technology)의 합성어로, 일반적으로 각종 리스크를 예방하고 관리하기 위한 금융당국·금융기업의 준법감시, 규제이행, 내부통제 등 컴플라이언스(Compliance) 업무를 보다 효율적으로 할 수 있도록 도와주는 기술을 포괄한다. 그러나 레그테크에 대해 국가별·기관별로 정의하는 바가 다르며 아직 사회적·학술적으로 개념이 확립되지는 않은 상황이다.

정부 차원에서 레그테크의 개념을 처음 설립하고 홍보한 국가는 금융 선진국인 영국이다. 영국 금융행위감독청(Financial Conduct Authority; FCA)은 레그테크에 대해 "기존 기능보다 효율적이고 효과적으로 규제 요구사항에 대응할 수 있는 기술"이라고 정의하였다.[16] 앞서 국제기관으로서는 국제 금융협회(Institute of International Finacne; IIF)가 레그테크를 "빅데이터(Bigdata), 클라우드(Cloud), 머신러닝(Machine Learning) 등의 신기술을 활용해 금융 관련 법규 준수 및 규제에 대한 대응보고를 유효하게 하는 기술"로 정의한 바 있다.[17]

금융 분야의 전문가들도 이와 비슷한 시각으로 레그테크를 바라보았다. 미국 상품선물 거래위원회(Financial Commitity Futures Trading Commission)의 전무이사인 Kari Larsen은 "레그테크는 규제 준수 분야에 종사하는 사람들을 돕는 혁신적인 기술 진보이며, 앞으로 규정준수 현황 및 관련 의무사항을 더욱 쉽고 효율적으로 모니터링하게 될 것"라며 레그테크의 높은 발전 가능성을 전망하였고[18], 금융 기금관리 플랫폼 회사 Fund Recs의 CEO인 Alan Meaney는 "레크테크는 핀테크(FinTech)나 페이테크(PayTech)등 Tech로 명명되는 용어들의 혼합물이자 또 다른 형태이며, 그간 소프트웨어가 규제 분야에서 20년 이상 사용되어 왔지만 소프트웨어와 비 소프트웨어 서비스 간의 차이가 현저히 벌어짐에 따라 레그테크 서비스가 각광받고 있다"며 레그테크 개념에 대한 이해와 함께 최근 레그테크가 이슈화되는 이유를 설명하였다.[19] BBVA Research의 디지털 규제 전문가인 Javier Sebastian은 레그테크에 대해 "클라우드 컴퓨팅(Cloud Computing), 빅데이터(Bigdata), 블록체인(BlockChain)과 같은 새로운 기술을 활용하고 있는 기업들의 모든 활동 부문에 거쳐 기업이 규제 요건을 준수할 수 있도록 지원하는 솔루션"이라고 소개하였다.[20] HSBC 그룹의 혁신 본부장인 Christophe Chazot 또한 레그테크를 "규제 프로세스에 대한 기술적 솔루션"이라며 규제준수 분야에 대해 진화된 형태의 솔루션으로서의 가치를 강조하였다.[21]

이와 같이 대부분의 기관과 전문가들이 레그테크를 규제 분야에서의 의무사항 준수를 더욱 효율적으로 도와주는 기술, 서비스, 솔루션 등으로 정의하는 가운데, 한 발 더 나아가 레그테크를 규제가 초래하는 위험을 예측하고 관리하는 위험관리의 관점에서 바라보는 시각도 존재한다. 2016년 발간된 Deloitte 보고서는 "규제 분야는 기술의 관리를 받아야하는 많은 서비스 중 하나"라며, 레그테크를 "기업이 가지고 있는 위험(Risk)을 더욱 잘 이해하고 관리할 수 있도록 도와주는 민첩한 규제 기술"이라고 정의하였다. 덧붙여 Deloitte의 위험 자문 전문가인 Sean Smith는 "레그테크는 기업의 일상적인 작업을 자동화시켜주고 규정 준수 및 보고의무 충족과 관련한 작업의 복잡성으로 인한 운영 위험을 줄여줄 수 있다"며 장기적으로 레그테크가 컴플라이언스 기능의 강화와 데이터에 입각한 위험관리를 위한 핵심 기술이 될 것이라고 예측하였다.[22]

학계에서도 규제 위험관리 관점에서 레그테크의 역할에 대해 기대를 표하고 있다. Butler&Brooks는 "레그테크의 개념에 위험관리(Management of Risk)의 관점이 내재되어 있으며, 레그테크는 더 나은 의사결정을 지원하고, 규칙에 따르지 않는 사용자를 찾을 수 있는 능력을 가지고 있다"고 주장하였다. 나아가 그들은 레그테크가 더욱 현명한 규정 준수를 통해 위험을 통제할 수 있는 프레임워크를 제공할 수 있을 것이라고 전망하였다.[23]

기관 및 전문가	RegTech에 대한 정의
영국 FCA	• 기존 기능보다 효율적이고 효과적으로 규제 요구사항에 대응할 수 있는 기술[16]
국제 금융협회	• 빅데이터(Bigdata), 클라우드(Cloud), 머신러닝(Machine Learning) 등의 신기술을 활용해 금융 관련 법규 준수 및 규제에 대한 대응보고를 유효하게 하는 기술[17]

Kari Larsen	• 규제 준수 분야에 종사하는 사람들을 돕는 혁신적인 기술 진보이며, 규정준수 현황 및 관련 의무사항을 더욱 쉽고 효율적으로 모니터링할 수 있게 해주는 체계[18]
Alan Meaney	• 핀테크(FinTech)나 페이테크(PayTech)등 Tech로 명명되는 용어들의 혼합물이자 또 다른 형태이며, 그간 규제 분야에서 20년 이상 사용되어 온 소프트웨어의 효과가 최근 극대화되어 나타나는 서비스[19]
Javier Sebastian	• 클라우드 컴퓨팅(Cloud Computing), 빅데이터(Bigdata), 블록체인(BlockChain)과 같은 새로운 기술을 활용하고 있는 기업들의 모든 활동 부문에 거쳐 기업이 규제 요건을 준수할 수 있도록 지원하는 솔루션[20]
Christophe Chazot	• 규제 프로세스에 대한 기술적 솔루션[21]
Deloitte	• 기업이 가지고 있는 위험(Risk)을 더욱 잘 이해하고 관리할 수 있도록 도와주는 민첩한 규제 기술[22]
Sean Smith	• 기업의 일상적인 작업을 자동화시켜주고 규정 준수 및 보고의무 충족과 관련한 작업의 복잡성으로 인한 운영 위험을 줄여주는 기술[22]
Butler&Brooks	• 위험관리(Management of Risk)의 관점을 내재하는 개념으로, 규제준수와 관련하여 더 나은 의사결정을 지원하고, 규칙에 따르지 않는 사용자를 찾을 수 있는 능력을 가지고 있는 기술[23]

<표 1> RegTech에 대한 세계 주요 기관 및 전문가들의 정의

결과적으로 현재까지 논의된 레그테크의 개념은 규제 요구사항에 대해 보다 효율적이고 보다 빠르게 대응할 수 있는 기술이자, 기존 규제준수 관련 솔루션의 진보된 형태이며, 규제와 관련된 다양한 위험들을 기술로써 담보해줄 수 있는 위험 관리 방안으로 정의할 수 있을 것이다.

(2) 핀테크(FinTech)와 레그테크(RegTech)의 관계

핀테크(FinTech)는 금융(Finance)과 기술(Technology)의 합성어로, 일반적으로 금융과 IT의 융합을 통한 금융서비스 및 산업의 변화를 통칭한다. 최근 수 년 동안 세계 금융 시장에서 상당히 주목을 받고 있는 핀테크는 세계 주요 기관에서 기능과 비즈니스 모델에 따라 다양한 분류가 시도되고 있다.

IT조사 및 분석 업체인 Venture Scanner에서는 2015년 핀테크기업 1,072개 기업을 조사하여 핀테크의 영역을 주요 기능에 따라 결제 및 송금 분야(지급 결제, 송금), 대출 및 자금 조달 분야(대출, 자본 조달, 크라우드 펀딩, 소비자 금융), 자산 관리 분야(개인 자산 관리, 개인 투자, 기관 투자), 금융 플랫폼 분야(비즈니스 도구, 금융 조사, 금융 인프라) 등 총 12개 분야로 분류하였다.[24]

핀테크 분류	세부 분류
결제 및 송금	• 지급 결제(payments) • 송금(remittances)
대출 및 자금 조달	• 대출(lending) • 자본 조달(equity financing) • 크라우드 펀딩(crowd funding) • 소비자 금융(consumer banking)
자산 관리	• 개인 자산 관리(personal finance) • 개인 투자(retail investments) • 기관 투자(institutional investments)
금융 플랫폼	• 비즈니스 도구(business tools) • 금융 조사(financial research) • 금융 인프라(banking infrastructure)

<표 2> 기능에 따른 핀테크의 분류 (Venture Scanner, 2015)

반면 영국 무역 투자청(UK Trade&Investment)에서는 핀테크를 비즈니스 모델에 따라 간편하고 저렴한 서비스를 제공하며 수수료를 부과하는 지급 결제(payments) 분야, 개인 또는 기업 고객과 관련된 다양한 데이터를 수집, 분석하여 새로운 부가가치를 창출하는 데이터 분석(data and analytics) 분야, 기존 방식보다 효율적이고 혁신적인 금융 업무 및 서비스 관련 소프트웨어를 제공하는 금융 소프트웨어 시장

(financial software market), 금융기관을 통하지 않고도 자유롭게 금융거래를 할 수 있는 다양한 거래 기반을 제공하는 플랫폼(platform) 분야 등 4가지로 분류하였다.[25]

핀테크 분류	세부 사항
지급 결제 (payments)	• 간편하고 저렴한 서비스를 제공하며 수수료 부과
데이터 분석 (data and analytics)	• 개인 또는 기업 고객과 관련된 다양한 데이터를 수집, 분석하며 새로운 부가가치 창출
금융 소프트웨어 시장 (financial software market)	• 기존 방식보다 효율적이고 혁신적인 금융 업무 및 서비스 관련 소프트웨어 제공
플랫폼 (platforms)	• 금융기관을 통하지 않고도 자유롭게 금융거래를 할 수 있는 다양한 거래 기반 제공

<표 3> 비즈니스 모델에 따른 핀테크의 분류 (UK Trade&Investment, 2014)

그렇다면 핀테크(FinTech)와 레그테크(RegTech)의 관계는 어떻게 이해하여야 할까? 2015년 3월 영국 정보 과학 보좌관이 발표한 보고서에서는 "핀테크는 금융 규제 및 보고를 강화하기 위해 규제 및 규정 준수 분야에 적용될 가능성이 있으며, 이는 투명하고 효율적이며 효과적인 규제 기술을 위한 새로운 매커니즘이 될 것"이라는 전망이 제시되었다.[27] 핀테크의 영역 중 금융 규제 및 보고 분야를 강화하기 위한 영역이 특수하게 발전할 수 있다는 것이다. 이러한 관점에서 레그테크는 새로운 핀테크라고 볼 수도 있고[19][22], 금융분야에서 핀테크의 하위 트리라고 볼 수도 있을 것이다.[20] 국내에서도 레그테크는 핀테크의 발전과정에서 필수적으로 파생된 전문 영역으로 보는 시각이 일반적이다.[28]

영국에서는 기술을 기반으로 한 금융서비스 혁신을 전통 핀테크(Traditional FinTech)로, 혁신적 비금융기업이 직접 금융서비스를 제공하는 것을 신흥 핀테크(Emergent FinTech)로 정의하고 있다.[26] 나아가 전통 핀테크를 금융 서비스 부문을 지원하는 전통적 금융회사의 '촉진자(facilitators)' 역할로, 신흥 핀테크를 기존의 금융 서비스를 새로운 기술로 차별화하는 혁신적 소형 기업들로 구성된 '방해자(disruptors)'로 비유하기도 한다.[29] 레그테크는 혁신 기술을 기반으로 규제를 금융회사의 프로세스에 내재화시켜 금융회사의 중요 영역인 컴플라이언스 영역을

지원하기에, 전통적 금융회사의 '촉진자' 역할을 하는 전통 핀테크에 가깝다고 할 것이다. 그러나 소형 스타트업들이 새로운 금융 분야로 뛰어들 때의 규제 리스크를 선제적으로 분석하고, 해당 위험에 대한 준법대응의 역할을 레그테크 외주업체에 맡기는 경우, 레그테크가 신흥 핀테크의 범주에도 포함될 수 있을 것이라 생각된다.

(3) 레그테크의 특징과 핵심 기능

국제 금융 협회(IIF)는 2016년 발표한 레그테크 분석 보고서를 통해 컴플라이언스와 관련되어 해결하여야 할 문제 및 레그테크가 해결할 수 있는 7가지 영역을 발표하였다.[17]

1) 자본 및 유동성 보고에 필요한 고품질의 구조화된 데이터 수집 및 집계
2) 현재의 컴퓨팅 능력, 노동력 및 지적 용량으로 해결하기 힘든 위험관리 모델링, 위험 시나리오 분석 및 예측
3) 실시간 결제 거래 모니터링 시 낮은 품질 및 결제 시스템의 결합으로 인해 나타나는 병목 현상의 해결
4) 보다 효과적인 솔루션의 사용을 통한 고객 및 법적 당사자의 식별
5) 금융 기관의 내부 문화 및 행동 모니터링, 고객 보호 프로세스 준수를 위한 고효율의 정성적 정보 분석 역량
6) 다양한 규제 업무의 자동화 및 규정 준수 효율성 증대
7) 금융기관에 적용되는 새로운 규정에 대한 파악 및 해석, 조직 전체 책임 부서마다 상이한 규정 준수 의무의 효율적 배분

본 보고서는 레그테크가 해당 영역의 문제들을 모두 해결할 수 있는 솔루션을 구현하기엔 아직 상당한 장벽이 있지만, 머신 러닝(Machine Learning), 로보틱스(Robotics), 인공지능(Artificial Intelligence), 암호학(Cryptography), 생물학(Biometrics), 블록체인 및 분산장부(Blockchain and other distributed ledgers), APIs(Application programming interfaces), 공유 유틸리티 기능 및 클라우드 어플리케이션(Shared utility functions and cloud applications) 등의 신기술을 융합을 통해 중대한 역할을 할 수 있을 것이라고 예상하였다.[17] 나아가 컴플라이언스 및 위험관리와 관련되어 인공 지능(Artificial Intelligence), 머신러닝 및 신경언어학 프로그래밍(Machine

Learning & NLP), 로보틱스(Robotics), 사이버보안(Cyber Security), 지식기반 온톨로지(Ontologies & Knowledge Bases), 스마트 계약(Smart Contract), 블록체인 BLT(Block Chain BLT), SQL 기술, NoSQL Data lakes Hadoop, 데이터 분석(Data Analytics), 데이터 거버넌스(Data Governance)과 같은 심화 기술들이 레그테크 적용 기술로 응용될 수 있을 것이다.[31]

이와 같이 레그테크가 기여할 수 있는 다양한 영역과 응용기술들이 있지만, 레그테크 혁신 연구소를 설립한 BBVA는 그 중에서도 레그테크가 수동 프로세스의 자동화, 분석 보고 프로세스 단계의 연결, 데이터 품질 개선, 데이터의 시각화 기술 개발에 초점을 맞추어야 한다고 주장하였다.[30] 이는 현재의 컴플라이언스 솔루션이 급격한 규제의 변화에 대응하여 가장 한계에 부딪힌 부분들이며, 신기술의 발전과 응용을 통해 가장 먼저 해결이 필요한 부분이기도 하다.

Deloitte는 레그테크가 기존의 규제 관련 기술과 대비하여 새롭고 흥미롭다고 생각되는 4가지 특징들을 다음과 같이 소개하였다.[22]

1) 민첩성(Agility) : 복잡하게 얽힌 데이터 셋으로부터 유의미한 데이터를 빠르게 추출하고 정리할 수 있음
2) 속도(Speed) : 보고서를 신속하게 구성하고 생성할 수 있음
3) 통합(Integration) : 솔루션의 가동 및 실행 시간 단축
4) 분석(Analytics) : 분석 도구를 사용하여 기존 빅데이터의 데이터셋을 지능적으로 추출하고 동일한 데이터를 여러 용도로 사용하는 등 가능성을 확장

반면, 조창훈의 연구에서는 레그테크의 3요소를 ① 금융업무에 대한 이해, ② IT의 적용, ③ 규제(Regulation)로 꼽으며, 레그테크 서비스와 기존 컴플라이언스 산업의 본질적인 차이점은 감독당국과 금융회사 사이의 적극적인 양방향 소통임을 강조하였다.[32] 나아가 곽기웅의 연구에서는 양방향성이라는 레그테크의 특성을 포함하여 기존 컴플라이언스 솔루션과 레그테크의 차이점을 ① 양방향성, ② 표준화, ③ 자동화, ④ 오픈소스, ⑤ 실시간성, ⑥ 빅데이터 및 클라우드 기반, ⑦ 신기술의 적극적 활용 등 7가지로 제시하였다.(<표4>)[33]

특징	설명	차이점	
		기존 컴플라이언스 솔루션	레그테크
양방향성	• 감독당국과 금융회사 사이의 적극적인 양방향 소통과 단기간 내 정기적인 피드백을 시스템적으로 지원하는 특성	어려움	가능
표준화	• 원장 또는 자료의 저장과 제출을 위한 데이터 및 프로토콜의 표준화 가능 여부	제한적 가능	가능
자동화	• 데이터 수집과 추출 그리고 유효성 체크 등의 자동화 또는 인공지능화 여부	가능	가능
오픈소스	• 오픈소스 형태의 컴플라이언스 시스템을 지향하므로 적용 시간과 비용의 최소화 측면에서 중요한 요소	어려움	가능
실시간성	• 상황에 맞게 신속한 데이터 변환 및 분석이 가능해야 하는 요소	가능	가능
빅데이터 및 클라우드 기반	• 빅데이터 저장 및 분석을 클라우드 기반에서 구현하여 비용 및 확장성을 확보하는 여부	제한적 가능	가능
신기술의 적극적 활용	• 인공지능, 블록체인, 생체인증 등 신기술 채용 여부	제한적 가능	가능

<표 4> 컴플라이언스와 레그테크의 차이 (조창훈, 2014)(곽기웅, 2016)

즉, 기존에도 금융 컴플라이언스 업무를 적은 비용으로 효율화하고자 하는 노력은 있어왔으나 레그테크는 규제환경의 변화 및 고객의 요구에 보다 빠르게 실시간으로 대응할 수 있다는 점, 자동화를 통한 빠른 업무 처리 서비스를 제공해줄 수 있다는 점, 단순히 금융기관이 금융회사에게 수직적으로 규제이행을 요구했던 단방향의 규제를 데이터를 통한 적극적 소통을 통해 현장에서의 규제이행 상황에 대한 피드백을 주고받을 수 있는 양방향의 규제로 전환시켜줄 수 있다는 점 등에서 우위를 지닌다고 볼 수 있다.

2. 컴플라이언스 영역에 있어서의 레그테크의 가치

규제준수 및 규제대응에 관해 논의함에 있어 '2015년 미국에서 가장 영향력 있는 경제학자' 이자 영국 중앙은행 수석 이코노미스트인 앤디 홀데인(Andy Haldane)은 레그테크 개념이 이슈화되기 이전부터 미래의 컴플라이언스가 나아가야할 중요한 방향을 제시하였다. 그는 2014년 버밍엄 대학(Birmingham University)의 기조연설에서 아래와 같이 기술이 주도하는 데이터 모니터링 체계에 대한 비전을 공유하였다.

"저에게는 꿈이 있습니다. 그것은 미래지향적이지만 현실적이기도 합니다. 우리는 머지않아 모니터 은행을 사용하는 스타트랙(Star Trek) 의자에 앉아 거의 실시간으로 전 세계의 자금 흐름을 추적할 수 있을 것입니다. 그것은 재무의 흐름, 경제 정책 효과와 상관관계를 도표화하는 세계 지도가 될 것입니다." [34]

이처럼 금융 기관 및 감독 기관은 글로벌 금융의 모든 부분에서 실시간 금융 정보를 모니터링 및 분석하여 안전하고 효율적인 금융 시스템을 구축하기를 원한다.[35] 데이터의 흐름과 규제 변화를 실시간으로 추적하고자하는 이러한 비전은 십여 년 전부터 존재해왔다. 2008년 글로벌 금융 위기(Global Financial Crisis) 이후로 규제의 형태와 그 강도가 크게 변화하자 규제와 관련한 기술 개발은 새로운 전환점을 맞이하기 시작했다. 금융 시장, 금융 기관, 금융 서비스 업체들에게 규제 준수 분야가 큰 주목을 받기 시작하였으며, 이에 따라 미국거래증권위원회(Securities and Excahange Commission; SEC)는 규제 개선을 위해 데이터에 대한 통찰력을 사용하는 것을 검토하기 위해 경제 및 위험 분석 부서를 신설하기도 하였다.[36] 이러한 노력들은 최근 핀테크의 급속한 진화와 발전으로 인해 실효성 있는 기술로의 구현이 가능하게 되었고 최근에 와서는 '레그테크' 라는 용어로 명명되는 새로운 차원의 혁신을 기대하고 있는 것이다.

현재 금융보안 규제 및 가이드는 60종을 상회할 정도로 복잡하다. 금융업에 있어 국가의 경계가 점점 희미해지고 있는 상황에서 FATF, FATCA/CRS와 같은 국제 표준 협약도 갈수록 증가하고 있고, 금융산업 변화에 따른 규제 고려사항의 복잡화로 세계 각국의 금융 규제도 날로 복잡해지고 있는 실정이다.(<표5>)

국가	금융 관련 법률 및 규제
미국	• 은행업 : Dodd-Frank WallStreetReform and Consumer Protection Act • 대금업 : 각 주법 • 송금·결제업 : 은행비밀법, 미국애국자법, 각 주법 • 증권업 : 연방업, JOBS법 • 보험업 : 각 주법
일본	• 은행업 : 은행법 • 대금업, 송금·결제업 : 대금업법, 할부판매법, 출자법, 자금결제법 • 증권업 : 금융상품거래법 • 보험업 : 보험업법
영국	• 은행업, 대금업, 증권업 : 금융서비스시장법 • 송금·결제업 : 결제서비스 규제 • 증권업 : 금융상품거래법
독일	• 은행업 : 신용제도법 • 송금·결제업 : 결제서비스 규제 • 증권업 : 개인투자자보호법 • 보험법 : 보험감독법
EU	• 결제 서비스 지침 등
싱가폴	• 은행업 : 은행법 • 대금업 : 대금업자법 • 증권업 : 증권선물법 • 보험업 : 보험감독법

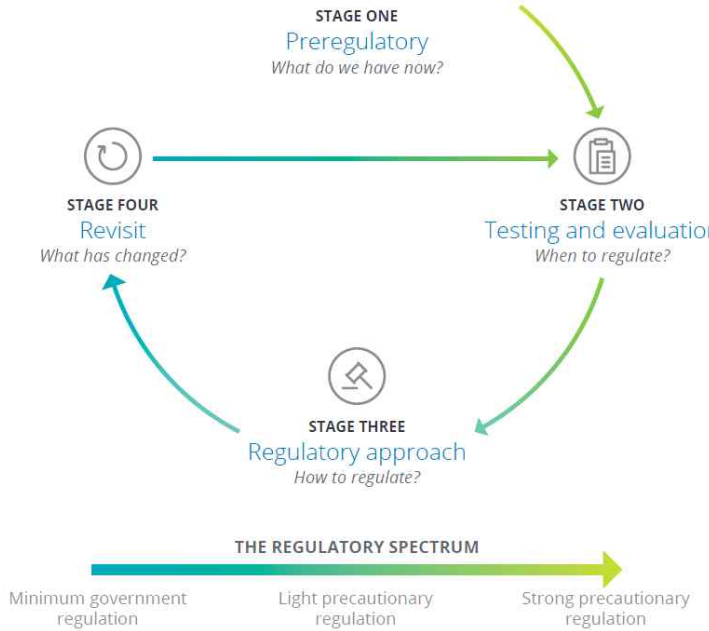
<표 5> 금융 산업 변화에 따른 세계 각국의 금융 관련 법률

금융 당국도 규제의 증가로 감독해야할 대상 기관이 지속적으로 증가함에 따라 관리 부담이 커졌다. 이미 취약점평가 대상 기관이 300개가 넘고 전금업자의 수는 100개를 넘어선 상황이다. 금융 당국 입장에서는 규제준수 사항을 상시 모니터링 할 수 있는 체계가 필요해졌다. 이름 하여 양적 규제(Quantitative Regulatory)의 시대가 도래한 것이다. 우리는 이제 비트(bits)와 바이트(bytes) 형태로 실시간으로 쏟아져 나오는 새로운 디지털 세계의 질서를 문서와 단어로 규정되어 있는 합법적 규제의 틀에 녹여 내어야한다.

이러한 규제 환경의 급격한 변화에 따른 새로운 위험들과 이에 대응하기 위한 비용의 상승은 기업에게도 복잡한 규제 환경에 적응하기 위한 효과적이고 지속 가능

한 방법을 개발하도록 압력을 가하고 있다.[14] 이에 대한 대안이자 양적 규제의 시대의 최선의 해법으로 제시되는 것이 바로 레그테크 시스템의 구축이다.

레그테크는 고급 모델 및 알고리즘, 기계 학습 및 향상된 실시간 분석 기능을 연결하여 규제준수와 관련한 다른 소프트웨어 솔루션보다 우수한 효과를 창출할 수 있다.[21] 현재 준법감시 업무의 효율성을 개선하기 위해 인공지능(AI) 기반의 레그테크가 확산되고 있는 추세에 있으며, 세계경제포럼(World Economy Forum; WEF)은 2025년까지 글로벌 금융기관의 35%가 인공지능(AI) 기반의 준법감시시스템을 도입할 것으로 예상하고 있다.[37]



<그림 7> 미래의 규제와 관련한 중대 질문사항

Source : Deliotte Center for Government Insights analysis, 2018

한편, Deloitte는 다가올 미래의 규제에 관해 정책결정자와 규제자들이 고민할 것으로 예상되는 중대한 질문사항을 다음과 같이 4가지로 예상하였다.[38] (<그림 7>)

1) 해당 분야와 관련된 규제의 현재 상태는 어떠한가?
2) 규제를 위한 적절한 때는 언제인가?
3) 적합한 규제의 관점은 무엇이 되어야하는가?
4) 규제가 처음 적용된 이후의 변화는 무엇인가?

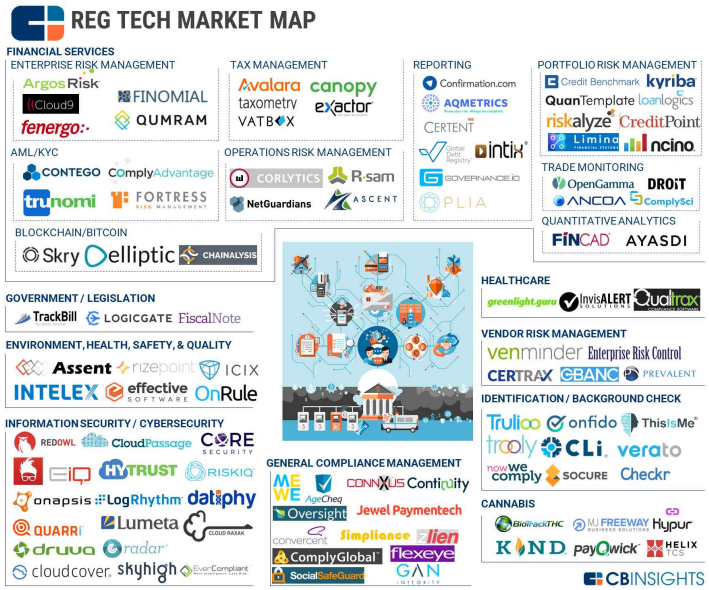
이는 미래의 규제 환경은 규제의 종류와 양이 갈수록 다양하고 많아지기 때문에 현재의 규제 요건들과 적용 상태를 파악하기 힘들 것이며, 이에 따라 자연스레 새로운 규제를 적용하여야 할 적절한 시기와 접근법을 택하기도 어려워질 것이고, 규제의 효과성에 대한 측정과 감독도 어려워질 것이라는 예측을 질문의 형식으로 치환한 것이 아닐까 생각된다. 규제 관리/감독을 위해서는 정확한 수준의 규제 관련 위험 진단과 예측을 통한 위험의 관리가 핵심인데, 양적 규제 시대에서는 이러한 관리/감독이 쉽지 않다는 것이다.

레그테크가 해결할 영역은 이러한 미래의 규제 환경의 요구지점과 정확히 맞닿아 있다. 레그테크는 규제의 코드화와 표준화를 통하여 장기적으로 규제 요건을 컴퓨터가 이해할 수 있는 데이터로 변환할 것이며 텍스트, 음성 등 모든 정형 및 비정형 데이터를 분석하고 준법감시 업무를 자동화시키어 현재의 규제 요건과 규제의 수준을 빠르게 파악할 것이다. 금융회사의 규제 이행에 대한 실시간 파악과 규제위험의 실시간 관측은 금융당국이 규제를 만들고 시행할 시기를 결정할 때 상당히 중요한 자료로서의 가치를 가질 것이다. 또한 새로운 비즈니스 모델을 개발하려는 회사가 현재의 규제에 대한 위험 시뮬레이션을 시도할 수 있을 것이며, 새로운 규제로 변화되는 상황을 대비하여 해당 규제를 미리 적용해보고 규제와 관련한 위험을 최소화시키는 방안을 선제적으로 마련할 수도 있다. 금융 당국은 이를 응용하여 정책 효과의 측정을 통한 과학적 규제를 실현시킬 수 있을 것이다.

3. 레그테크 시장의 성장과 레그테크 기업의 약진

최근 바젤위원회는 '효과적인 리스크 데이터 집계 및 리스크 보고 원칙'[39]을 발표하며 글로벌 은행들이 리스크 데이터 능력을 제고하고 규제대응 역량을 확보할 것을 압박하고 있고, 금융기관들 역시 금융 리포팅, 소비자 보호, 보안 등 규제 이행 체계 전반을 고도화하고자 하는 욕구가 늘어나면서 레그테크 시장의 성장은 점

차 속도를 내고 있다. 미국, 영국, 호주, 싱가포르 등 선진 금융당국은 이미 금융 컴플라이언스 영역에 인공지능과 머신러닝을 활용한 혁신적인 레그테크 전략을 도입, 장려하고 있으며, FinCEN, 뉴욕연방준비은행(FRB NY), 통화감독청(OCC) 등 미국의 대표적인 규제 기관은 물론 금융전문지 더 뱅커(The Banker)가 평가하는 자산 기준 전 세계 상위 10대 은행 중 9곳이 인공지능과 머신러닝을 활용한 SAS의 레그테크 솔루션을 활용하고 있다.[11] '레그테크(RegTech)' 용어 자체는 생긴지 몇 년 되지 않았지만 레그테크와 관련된 신생 회사는 5년 전부터 생겨났다. 시장 관점에서 볼 때 대기업이 레그테크 신생 기업들과 합병 또는 인수를 시작한다면 레그테크 생태계는 앞으로 더욱 폭발적인 성장을 할 것으로 예측된다. 현재는 주로 규제 인지 솔루션 분야의 하위 범주로 레그테크 기업들이 성장하고 있으며, 해당 기업들의 핵심 기능은 규제 데이터 분석 도구를 제공하고, 규제 요구사항을 자동으로 업데이트 하는 것에 초점이 맞춰져 있다.[20]



<그림 8> 레그테크 시장의 분야별 지도 (CB Insight, 2017)

그러나 레그테크 시장의 범위가 규제 인지 분야로 한정되지는 않는다. 레그테크 기업들은 규제 프로세스와 서류 작업을 간소화하고 효율화할 수 있는 방대한 기술 영역으로, 수많은 분야들에 적용되어 다양한 소프트웨어, 서비스 및 도구를 제공하고 있다. 지난 5년 간 레그테크 기업들은 337건의 계약을 통해 약 23억 달러의 자금을 조달하였다. 대부분의 신생 기업은 금융 서비스 부문의 규정 준수에 초점을 맞추고 있지만 의료 분야, 식품 분야, 약물 분야, 사이버보안 분야, 블록체인 분야, 심지어 대마초 관련 분야까지 확대되어 성장하고 있다. 데이터 컨텐츠 조사기업 CB Insight는 100개가 넘는 민간 기업을 레그테크 분야로 식별하고 9개의 범주로 기업들을 분류하였다.(<그림 8>) 해당 기업들은 2015년부터 주식 투자를 받아왔고 적어도 1백만 달러의 펀딩을 받았다. 세부 범주와 대표 기업들은 다음과 같다.[40]

분류	세부 설명	대표 레그테크 기업
AML[8]/KYC[9]	은행이 의도적/비의도적으로 범죄 요소에 의해 사용되는 것을 막는 AML 요구사항 및 고객의 신원을 확인하기 위한 KYC 도구 제공	• Trunomi • ComplyAdvantage
블록체인 /비트코인	비트코인과 관련한 위험 평가를 수행하고 블록체인 기술관련 규제 등을 모니터링	• Skry • Elliptic
기업 위험 관리	기업의 다양한 영역에 영향을 미치는 광범위한 위험 유형을 해결	• Fenergo • Argos Risk
운영 위험 관리	금융 서비스 조직의 일상적인 운영 위험을 관리할 수 있는 소프트웨어 제공	• Rsam • NetGuardians
포트폴리오 위험 관리	금융 서비스 회사가 부당한 투자를 하지 않도록 투자 포트폴리오 상태를 평가하고 모니터링할 수 있는 도구를 제공	• Kyriba • nCino
정략 분석	위험 분석 및 양적 위험 모델링을 통해 신용, 시장 및 유동성 위험을 확인할 수 있는 도구를 제공	• FINCAD • Ayasdi

8) Anti-Money Laundering(자금세탁방지)

보고	데이터 분석을 통합하여 보고를 수행하고, 정기적이고 임시적인 보고를 자동화하며, 미래의 보고를 위해 중앙에서 정보를 관리할 수 있는 소프트웨어 제공	• Capital Confirmation • Certent
세금 관리	필요한 세금 수입을 수집하고, 기록을 관리하며 정부가 필요로 하는 요소를 지원하는 소프트웨어 제공	• Avalara • Canopy Tax
거래 모니터링	직원들이 거래 제한사항을 준수하는지 확인하고 무단거래 고객의 거래 활동을 모니터링할 수 있는 소프트웨어를 제공	• OpenGamma • Droit Fintech

<표 6> 금융 서비스 산업과 관련된 레그테크 기업 분류

세계 시장에서도 레그테크는 더 이상 작은 산업이 아니다. 핀테크 벤처 캐피털 H2 Ventures와 다국적 컨설팅 그룹 KPMG는 매년 '세계 100대 핀테크 기업'을 선정하는데, 레그테크 기업으로 분류된 회사는 100개 회사 중 2016년도에는 8개 기업이, 2017년도에는 6개 기업이 선정되었다.[41][42] 주요 분야는 보고서 생성, 운영 리스크 관리, 블록체인, 정부 및 법률, 보안, 컴플라이언스와 관련된 영역이었으며, 해당 보고서는 레그테크 기업들의 약진을 특히 주목할 필요가 있음을 강조하였다.

<그림 9> 세계 100대 핀테크 기업 中 레그테크 기업의 약진

9) Know Your Customer

또한 2018년 한 해에만 RegTech Capital Markets Conference[10], RegTech Summit APAC[11]·유럽[12]·미국[13], COMPLY[14], RegTech Rising[15], The Reality of RegTech[16], The RegTech Convention[17], RegTech MENA[18], Global RegTech Summit[19] 등 전 세계에 레그테크만을 주제로 하는 컨퍼런스들이 상당 수 개최되었거나 개최될 예정이다. 이는 레그테크에 대한 학문적 연구, 동향 및 기술 공유에 대한 전 세계의 관심이 상당히 높은 상황임을 여실히 보여주고 있다.

4. 레그테크의 확장 가능성에 대한 고찰

앞장에서는 레그테크의 정의 및 범위를 핀테크의 종속되는 하위 영역, 기존 컴플라이언스 솔루션이 고도화된 솔루션 정도로 설명하였다. 그러나 레그테크가 단순히 '기술'의 영역이 아니라 금융 산업의 '법규' 영역의 목적 및 기능으로 확장될 수도 있다는 점에서 핀테크에 종속되는 영역, 혹은 하위 영역으로만 한정짓는 것은 레그테크의 발전 가능성에 족쇄를 채우는 것일 수도 있다.

핀테크의 목적은 '금융서비스의 편의성 및 보안성 개선'이지만 레그테크의 목적은 '금융회사의 업무처리 비용절감 및 효율성의 개선'에 가깝다. 레그테크의 서비스 영역이 금융 규제의 적용·이행·관리·감독 전반에 큰 영향을 미치고, 정책 입안자 및 금융당국의 규제 결정 체계의 패러다임을 바꾸는 수준까지 발전될 수 있다면 레그테크는 더이상 '금융 서비스의 편의성 및 보안성 개선'을 위한 금융 기술인 핀테크의 하위 영역이 아닌 핀테크의 확장적 영역 혹은 독립적인 영역으로 성장할 수 있을 것이다. CIO 글로벌 네트워크 그룹의 창립자인 Cavallo가 레그테크(RegTech)를 기술(Technology), 규제(Regulation), 금융 서비스(Financial Services), 핀테크(FinTech)의 누락된 부분을 연결시키고 강점을 강화시키는 미싱링크(Missing Link)[20][43]라고 표현한 것도 이러한 시각의 연장선이라고 볼 수 있다.

10) http://regtechconference.co.uk/
11) http://finance-edge.com/regtechapac/
12) http://finance-edge.com/regtecheu/
13) http://finance-edge.com/regtechus/
14) https://comply2018.com/
15) https://finance.knect365.com/regtech-rising/
16) https://www.bankdirector.com/conferences/reality-regtech-2018/
17) https://www.regtech-convention.com/en/
18) https://www.regtechmena.com/
19) http://fintech.global/globalregtechsummit/
20) 전체를 이해하거나 완성하는 데 필요한 중요 요소

세계적인 회계법인인 EY는 2016년 발표한 “Innovating with RegTech” 보고서에서 규제 변화 및 위험관리 프레임워크에 대비한 레그테크 생태계 모델을 제시하였다.[44] 해당 레그테크 생태계 모델은 규제자(Regulator), 전문 서비스 회사(Professional services firms), 금융 기관(Financial Institutions)와 더불어 레그테크 기업(RegTech firms)을 생태계의 핵심 주체 중 하나로 인정하고 있다. 레그테크 기업은 현재는 규제 및 위험관리 프레임워크에 대응한 솔루션 조정을 위해 기업 및 규제기관 간 이해협력을 증진하는 분야에 주로 초점을 맞추고 있다고 기술하였으며, 향후 사업자 및 규제기관의 요구 사항을 충족하는 레그테크 솔루션의 개발, 개발된 솔루션이 광범위한 위험관리 프레임워크 및 규제 요구사항에 호환되는지 여부를 관리하는 역할을 맡게 될 것으로 예상하였다.

주체	현재의 중점 분야	예상되는 역할
규제자 (Regulator)	대화 촉진 및 시장 동향 수집	• 규제 컴플라리언스 혁신에 대한 지속 추진 • 레그테크 생태계의 다양한 부분에 대한 효율성 및 협업 촉진 • 공통된 통합 표준 작성 및 계약 규칙에 대한 지침 개발 지원
레그테크 기업 (RegTech firms)	규제 및 위험 관리 프레임워크에 대응한 솔루션을 조정하기 위한 기업 및 규제 기관 간 이해협력 증진	• 사업자 및 규제기관의 요구 사항을 충족하는 솔루션의 개발 • 개발된 솔루션이 광범위한 위험관리 프레임워크 및 규제 요구사항에 호환되는지 확인
전문 서비스 회사 (Professional services firms)	요구사항 및 솔루션 이해를 위한 생태계 전반의 업무	• 규제 표준, 기관 요구사항 및 공급업체 솔루션의 통합 추진 • 공급자와 사용자 연결 • 신규 시장 진입자에 대한 지원 • 새로운 레그테크 솔루션 구현과 관련된 위험에 대한 사전 예방 및 관리 • 규제, 시스템 및 규정준수 전환 지원

금융 기관 (Financial Institutions)	단기·장기적 관점에서의 레그테크 전략 및 로드맵 개발	• 레그테크를 채택 • 레그테크 솔루션의 내부 개발

<표 7> 레그테크 생태계 : 현재의 중점 분야 및 예상 역할 (EY, 2016)

이처럼 레그테크는 핀테크 사업 영역이 아닌 별도의 생태계를 구축하여 기능하고 있다고 볼 수도 있으며, 향후 레그테크 기업도 독립적인 생태계의 주체로써의 핵심적 역할을 확보해갈 것으로 생각된다.

Ⅳ. 영국의 레그테크 추진 사례 분석 : 금융당국의 역할을 중심으로

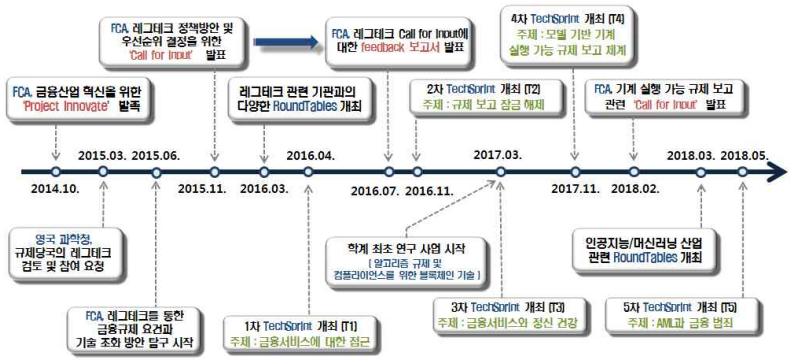
1. 영국 FCA의 레그테크 지원배경과 추진경과

영국은 2008년도 금융위기 이후 금융계와 IT산업의 융합 및 정부의 적극적 육성정책으로 핀테크(FinTech) 산업의 발전 속도가 매우 빠른 것으로 평가받고 있다. 글로벌 금융회사의 본사 다수가 영국 내에 위치하고 있고, 금융회사의 대규모 지원 덕도 있지만, 영국의 핀테크 산업 성장의 핵심 동력은 정부의 적극적인 핀테크 육성정책에 있다. 2014년 8월 재무장관인 오스본이 영국을 '글로벌 핀테크 도시'로 선언하였고[45], 이후 해당 기조에 따라 다양한 핀테크 산업 육성 정책들이 발표되기 시작하였다. 특히 영국 금융당국인 금융감독청(Financial Conduct Authority; 이하 FCA)에 의해 다양한 지원프로그램이 고안되고 시행되었다.

핀테크 육성 정책의 가장 대표적인 것이 FCA가 2014년 10월 설립한 'Project Innovate'이다. Project Innovate는 금융 산업 혁신과 관련하여 신생 업체들의 요구사항을 이해하고, 어떻게 규제를 완화해나갈 것인가를 고민하는 것을 핵심 역할로 삼고, 금융 산업과 관련 다양한 혁신서비스 담당 업무들을 수행한다. Project Innovate는 새로 출현하는 핀테크 서비스가 어떠한 금융규제를 위반할 가능성이 있는지를 사전에 확인 및 검토하고 이를 가능하게하기 위하여 현행 금융규제 중 조정가능사항을 파악하여 핀테크 기업에 대해 자문해주거나, 기술혁신을 가로막는 요소들을 해소시키는 방안을 모색하여 사전에 조정하는 등 종합적인 혁신지원정책을 수행하고 있다. 해당 지원 프로젝트는 첫 해에만 177개의 회사를 지원하였으며, 지원 회사 숫자는 8개월 후 거의 300개까지 증가하였다. Project Innovate는 또한 혁신센터(Innovation Hub)를 설치하여 핀테크 스타트업을 직·간접적으로 지원하는 프로그램도 함께 실행하고 있다. 예컨대 핀테크 사업을 하려는 자가 새로 시도하는 서비스가 어떤 금융규제에 저촉될 수 있는지에 대해 문의한 경우 이를 검토하여 개별적으로 자문을 해준다거나 핀테크 생태계(fintech ecosystem) 환경이 만들어질 수 있도록 절차와 정책을 마련하는 일을 추진하고 있는 것이다.[46][47]

영국의 핀테크 육성 정책은 자연스럽게 규제 요건을 쉽고 빠르게 이해할 수 있도록 하고 이에 대한 규제대응을 도와주는 레그테크에 대한 관심으로 이어진다. 이 때문에 영국 규제당국은 핀테크 기술을 규제 시스템에 도입함으로써 규제 및 컴플

라이언스에 소요되는 비용을 절감하고 효율성을 높이는 방안으로 레그테크를 택하고 레그테크를 지원하기 위한 관심과 투자를 아끼지 않기 시작한다. 2015년 3월 영국 정부의 과학청(Government Office for Science)이 영국의 핀테크 시장의 성장과 발전을 지원하는 방법에 대한 보고서에서 규제 당국이 레그테크에 대해 검토하고 지원에 참여할 것을 요청한 것을 계기로[48], FCA는 금융규제 요건과 기술이 레그테크를 통해 어떻게 조화를 이룰 수 있을지 탐구하기 시작하였다. FCA는 이후 레그테크에 대한 정책을 어떻게 진행해야할지 알아보고, 정책의 우선순위를 결정하기 위해 의견수렴 절차인 "Call for Input(CPI)"를 발표하여 레그테크 관련 이해관계자들에게 광범위한 의견을 구하였다.[49] 이는 기존의 금융서비스 회사와 기술 공급업체, 핀테크 신상 기업들로부터 100건 이상의 서면 응답을 받으며 상당한 수준의 관심을 받았다. 2016년 7월, FCA는 해당 의견수렴에 대한 피드백 보고서를 발표한다.[50]



<그림 10> 영국 금융당국 주도의 레그테크 연구모임 및 정책 추진 경과

2016년 3월부터는 다양한 양자 회의를 개최하여 4개의 라운드테이블(Tech UK, Burges Salmon, JWG, Innovate Finance)를 개최하여 250명 이상의 이해당사자들의 의견을 청취하기도 하였다.[51] 이를 통해 FCA가 레그테크와 관련하여 주안점을 갖고 추진하여야 할 정책의 방향을 설정하였다. 이어 FCA는 지속적으로 IT기업, 금융산업, 전문가가 모두 참석하여 의견을 개진하고 레그테크가 나아가야할 방향을 자유롭게 개인할 수 있는 모임이자 해커톤(Hackathon)[21]의 일종인 TechSprint 이벤트를 진행하기 시작하였다. 2016년 4월부터 1차 TechSprint(T1:Access to Financial

Services)[52]를 개최하기 시작하여 2016년 11월에 2차 TechSprint(T2:Unlocking Regulatory Reporting)[53], 2017년 3월에 3차 TechSprint(T3:Financial Services and Mental Health)[54], 2017년 11월 4차 TechSprint(T4 : Model-Driven Machine Executable Regulatory Reporting)[55], 2018년 5월 5차 TechSprint(T5:AML/Financial Crime TechSprint)[56]까지 개최한 바 있다. 레그테크와 관련한 원탁회의인 라운드테이블 행사도 2017년 12월, AML 및 디지털 ID기술 산업과 관련된 라운드테이블, 2018년 인공지능I/머신러닝 산업과 관련된 라운드테이블 등 다양한 주제와 심화된 내용으로 지속 개최되고 있다.[51]

연도		추진 경과
2014년	10월	• 금융 산업 혁신과 관련 규제 완화를 위한 'Project Innovate' 발족
2015년	3월	• 영국 과학청, 규제당국의 레그테크 검토 및 참여 요청
	6월	• FCA, 레그테크를 통한 금융규제 요건과 기술 조화 방안 탐구 시작
	11월	• FCA, 레그테크 정책방안 및 우선순위 결정을 위한 "Call for Input on Supporting the development and adoption of RegTech" 발표
2016년	3월	• 레그테크 관련 기관과의 다양한 RoundTables 개최
	4월	• 1차 TechSprint 개최(T1) ✓ 주제 : 금융서비스에 대한 접근
	7월	• FCA, 레그테크 '15년 11월에 발표했던 Call for Input에 대한 Feedback 보고서(Feedback Statement on Call for Input) 발표
	11월	• 2차 TechSprint 개최(T2) ✓ 주제 : 규제 보고 잠금 해제
2017년	3월	• 학계 최초 레그테크 연구사업 시작 ✓ 주제 : 알고리즘 규제 및 컴플라이언스를 위한 블록체인 기술
		• 3차 TechSprint 개최(T3)
		✓ 주제 : 금융서비스와 정신 건강
	8월	• 규제 보고시스템을 위한 분산 장부 기술 관련 연구 사업 시작
	11월	• 4차 TechSprint 개최(T4) ✓ 주제 : 모델기반 기계 실행가능 규제 보고 체계
	12월	• AML/디지털 ID 기술 산업 관련 RoundTables 개최
2018년	2월	• FCA, 기계 실행가능 규제보고 관련 CII 보고서 "Call for Input on Machine-Executable Regulatory Reporting" 발표
	3월	• 인공지능/머신러닝 산업 관련 RoundTables 개최
		• 첫 번째 내부 분석 해커톤(Hackathon) 개최
	5월	• 5차 TechSprint 개최(T5) ✓ 주제 : AML과 금융범죄

<표 8> 현재까지의 영국의 레그테크 추진 경과

2. 레그테크 이해관계자들에 대한 의견 수렴 결과[22]

FCA는 2015년 11월, "Call for Input on Supporting the development and adoption of RegTech"를 발표하여 레그테크 관련 전문가들과 이해관계자들을 대상으로 향후 FCA가 레그테크를 위해 취해야 하는 발전계획과 주요 사안들에 대해 의견을 수렴하고자 하였다.[49] 이에 대한 결과는 FCA가 2016년 7월 발표한 Feedback 보고서[50]를 통하여 세부적으로 소개되었다. 영국의 레그테크 이해관계자들이 레그테크를 어떤 시각으로 바라보고, 어떤 부분을 실제 필요로 하는지를 살펴보는 것은 향후 우리나라의 레그테크 도입 방향 및 발전계획 수립에도 상당히 좋은 참고가 될 수 있을 것으로 보인다. 따라서 본 장에서는 해당 보고서의 주요 답변 요지를 상세 분석하고 시사점을 도출해보도록 하겠다.

FCA가 레그테크 이해관계자들에게 의견을 구한 핵심 질문은 ① 어떤 레그테크의

21) 해커톤(Hackathon)은 해킹(hacking)과 마라톤(marathon)의 합성어로 일반적으로는 디자이너, 개발자, 기획자 등이 팀을 꾸려 마라톤을 하듯 긴 시간 동안 아이디어 창출, 기획, 프로그래밍 등의 과정을 통해 시제품 단계의 결과물을 만드는 대회를 뜻한다.

22) 본 장은 영국 FCA의 "Feedback Statement : Call for input on supporting the development and adopters of RegTech" 보고서를 번역하여 분석한 것이다.

도입이 필요한가?, ② 레그테크의 도입에 있어 금융당국(FCA)의 역할은 무엇이어야 하는가?, ③ 레그테크로 인한 혁신을 방해하는 것은 무엇인가?, ④ 도움이 될 만한 규제나 정책은 무엇인가? 등 4가지이다. 조사 대상은 기술 공급자 43%, 컨설턴트 23%, 금융서비스 종사자 23%, 학계 종사자 3%, 법률 회사 종사자 3%, 스타트업 종사자 3%등 총 350명의 응답자가 답변하였다.

(1) 어떤 레그테크가 도입이 필요한가?

첫째, 정보 공유를 효율화시키어 효율성과 협동성을 높일 수 있는 기술을 필요로 하였다. 응답자들은 종래의 보고 체계를 대체할 수 있는 새로운 데이터 제공・수집 기술을 통해 규제 데이터를 보다 유연하게 제공할 수 있도록 하여 규제 보고 부담 및 비용을 줄이기를 희망했다. 또한 클라우드/클라우드 컴퓨팅의 고도화를 통해 기업이 더 나은 통찰력을 확보하길 원했으며, 공유 유틸리티 및 금융사 소통 플랫폼 개발을 통한 업계의 의사소통 체계의 확산 및 유연성 증대를 기대하였다.

둘째, 규제 사항에 대한 해석의 차이를 좁혀 효율성을 촉진할 수 있는 기술의 통합 및 표준화를 필요로 하였다. 응답자들은 규제 텍스트를 프로그래밍 언어로 변환하는 기술을 통한 규제이행의 자동화를 기대하였으며 동시에 공유 데이터 망 및 API 플랫폼 제공을 통한 시스템 통합과 호환성 향상이 요구된다고 응답하였다. 나아가, 기업이 규제와 상호작용하여 시스템과 프로세스에 미치는 영향을 이해할 수 있도록 하는 개념인 로보 핸드북(Robo-Handbook) 기술의 개발이 필요함을 주장하기도 하였다.

셋째, 데이터를 단순화하고 보다 나은 의사 결정 및 자동화 기능을 가능하도록 하는 예측・학습・단순화 기술을 필요로 하였다. 방대한 양의 정형 데이터, 비정형 데이터를 해석할 수 있는 빅데이터 분석 솔루션, 실시간 위험을 분석할 수 있는 위험 및 규정준수 모니터링 솔루션, 모델링/시각화 기술, 머신러닝 및 인지기술의 개발을 요청하였으며 응답자들은 이를 통해 규제적용결과의 예측과 부작용에 대한 선제 파악이 가능할 것으로 보았다.

넷째, 규제 및 규정준수 프로세스를 새로운 차원으로 나아갈 수 있도록 하는 기술을 기대하였다. 규제를 프로그램 코드로 자동 적용하여 규제준수 비용 및 인건비의 감소를 기대하였고, 시스템 모니터링/시각화 기술을 통해 기업 전체의 기술 자산을 시각화하고 비효율성을 개선하길 원했다. 또한 신기술인 블록체인/분산원장, 생체인

식기술 등이 규제 준수 분야에 적용되어 시스템의 투명성을 보다 높이고 규제준수 프로세스가 새로운 차원, 새로운 방향으로 변화되기를 원하였다.

(2) 레그테크 도입에 있어 금융당국(FCA)의 역할은 무엇이어야 하는가?

응답자들은 금융당국이 본인들의 기대사항을 명확히 인지하고 해당 방향으로 산업 표준과 지침을 제시하여, 금융회사 간 데이터 및 프로세스의 통합을 원활히 이끌어 줄 것을 요구하였다. 이를 통해 비용을 절감하고 데이터의 품질을 향상시키며, 회사의 효율성 증대를 기대하였다.

또한 금융당국가 앞으로의 당면과제를 해결하기 위해 규제당국과 금융회사 간 관계와 인터페이스를 개선해야함을 강조하였다. 미래 비전에 대한 공유와 지속적인 협업이 앞으로의 레그테크 상품 개발에 중요하다는 생각인 것이다.

마지막으로, 관련 기준을 충족한 기업 및 제품에 대한 FCA의 인증이 필요하다고 주장하였다. 응답자들은 FCA 인증제도가 새로운 레그테크 규제 도구의 보급과 투자 확대를 이끌 것이며, 업계의 표준・지침 수용률을 증가시키고, 비용 절감을 촉진할 것이라고 예상하였다.

(3) 레그테크로 인한 혁신을 방해하는 것은 무엇인가?

응답자들은 레그테크가 널리 채택되지 못하게 하는 방해요소가 무엇일지에 대해서도 의견을 개진하였다. 응답자들은 규제 및 규제기관에 대한 불확실성, 신기술에 대한 신뢰 부족이 기업들을 신중하게 만들고 있다고 생각했다. 이러한 불확실성 때문에 기업들은 얼리어답터가 되기를 포기하고 있으며, 규제기관의 공식 승인만을 기다리고만 있다는 것이다. 그들은 금융당국이 가상 샌드박스(Virtual Snadbox)와 같은 정책을 통해 기술을 입증할 수 있도록 지원하고 불확실성을 해소할 수 있도록 도와주기를 희망하였다.

또한 응답자들은 데이터에 대한 접근, 처리, 저장과 관련한 표준의 부족이 신기술의 개발 및 채택을 저해하고 있다고 생각하였으며 데이터 표준, 보고의 기준 등의 통일성을 요구하였다. 규제 변경에 대한 전달 체계에 대해서도 의문을 제기하였다. 응답자들은 금융당국이 규제 변경사항에 있어 공정한 통지를 제공하여야 하며, 시행에 앞서 제안된 규제에 대한 협의 문서를 발행하고 주어진 피트백에 대한 공지를

해야한다고 주장하였다. 또한 규제에 대비할 시간을 확보해주고, 기관 및 기술전문가의 협력을 촉진시킬 것을 요구하였다.

(4) 도움이 될 만한 규제나 정책은 무엇인가?

응답자들의 제안에는 새로운 규제사항을 기계가 인식할 수 있는 형식으로 정의하는 방안이 포함되었다. 규제를 기계가 인식할 수 있는 기술이 개발된다면, 국제적으로 규제의 일관성과 호환성을 높일 수 있고, 공통된 글로벌 규제 분류 체계가 확립될 수 있다는 것이다. 또한 이러한 체계는 규제 실행의 속도, 규제의 효율성을 이끌 것이며, 규제 당국의 요건을 쉽게 이해하고 이행할 수 있도록 보장할 것이라고 예측했다. 또한 글로벌 기준과의 차이가 없어진다면 법률을 수정하는 비용 부담이 줄어들며, 업계도 상당한 혜택을 누릴 수 있다고 주장하였다.

영국 FCA는 레그테크 이해관계자들의 의견수렴결과 대부분을 실제 레그테크 지원 정책에 반영하여 핵심 추진 분야로 선정하고 업계와의 지속적인 의사소통을 통해 추진해나가고 있다. 기계가 읽을 수 있는 버전으로의 핸드북(HandBook) 현대화, 규제의 통합 및 표준화 추진, 지능형 규제 조력·조언 체계 개발, 블록체인 기술을 사용한 규제 및 규정 준수 자동화 추진 등이 대표적이며, 이외에도 기계 실행가능 규제보고(Machine-Executable Regulatory)에 대한 Call for Input을 발행하는 등 업계의 의견을 수렴하고자하는 의지를 계속해서 가져가고 있다.

3. 레그테크 활성화를 위한 영국 금융당국의 역할과 시사점

영국은 글로벌 금융위기 이후부터 레그테크 산업과 상위 범주에 있는 핀테크 산업을 엄청난 속도로 성장시켜왔다. 2008년 이후부터 영국의 핀테크 관련 거래 규모는 매년 74%씩 증가하였고 투자 규모는 2013년까지 약 8배 증가하였다. 영국의 핀테크 관련 투자 규모는 매년 약 51%씩 성장해왔는데, 이는 같은 기간 전 세계 핀테크 투자 평균 상장률(26%) 및 캘리포니아의 성장률(23%)이 훨씬 넘는 비율이다.[57]

이러한 성장 배경에는 금융당국이 산업 성장을 위한 우수한 산업 생태계(Ecosystem) 구축이라는 핵심 동력이 있었다는 의견이 지배적이다. 글로벌 컨설팅 업체 Emst&Young에 따르면 글로벌 핀테크 허브 중 영국이 가장 우수한 핀테크 생

태계를 갖춘 것으로 나타났다.[58] 이는 영국정부가 일찍이 런던 동부에 기술 클러스터인 테크 시티(Tech City)를 조성하고, 다양한 정부 지원 프로그램을 통한 투자 및 제도적 지원을 지속했을 뿐만 아니라 기존의 금융서비스 산업과 IT산업 간의 유기적 협력 시스템을 구축하기 위해 지속적으로 노력한 덕분이다.[59] 기업이 성장하기 위해서는 기업에 대한 직접적 지원뿐 아니라 기업이 성장하는데 필요한 경제적·사회적 환경 조성이 필수적이기에, 산업 성장을 위한 우호적 생태계 구축을 위한 금융당국의 적극적 지원정책은 적극 참조할만한 가치가 있다.

주요 핀테크 허브 지역	인력 (Talent)	자본 (Capital)	정책 (Policy)	수요 (Demand)	총점
영국	**2**	**3**	**1**	**3**	**9**
캘리포니아	1	1	6	2	10
뉴욕	3	2	7	1	13
싱가포르	4	7	2	6	19
독일	6	4	5	5	20
호주	5	5	3	7	20
홍콩	7	6	4	4	21

<표 9> 주요 핀테크 허브별 핀테크 생태계의 수준 비교 (EY, 2016)

[비교 순위 : 1 = 높음, 7 = 낮음]

영국 금융당국은 규제 개선 및 완화를 통한 혁신적 규제환경을 조성하는 데에도 적극적인 노력을 하였다. 글로벌 금융위기 이후 영국은 기존 금융 감독체계의 문제점을 해결하기 위한 방안으로 2013년 4월 금융 감독체계를 건전성 감독기구(Prudential Regulation Authority; PRA)와 금융행위 감독기구(FCA)로 이원화하였으며, 소비자 보호를 목적으로 하는 FCA는 금융시장의 투명성 및 경쟁력 강화를 위해 혁신적 핀테크 산업을 적극 지원하는 데 집중하였다. 특히 FCA는 기업의 불법 행위에 대한 전통적인 감독 역할을 넘어 핀테크 스타트업 기업들의 시장 진출을 직접적으로 지원하고, 신규 상품의 출시 전 안전성을 강화하는 등 보다 적극적인 역할을 수행하였다.[59] 특히 신규 핀테크 사업 지원 전담 부서로 신설된 혁신센터(Innovation Hub)는 금융당국의 승인을 받기 위해 숙지해야하는 지원 요건들을 보다

쉽게 이해하도록 도와주고 실질적인 준비 과정을 지원하여 레그테크 기업들이 시장에 진출하기 위해 수반되는 비용 및 위험을 낮추어주고 원활히 시장에 정착하는데 큰 도움을 주었다.

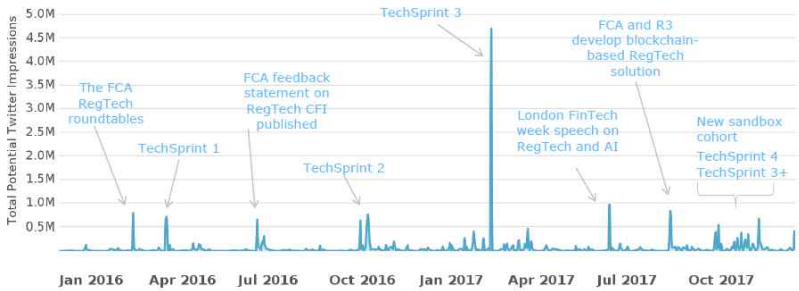
영국의 레그테크 지원 정책 중 가장 큰 역할을 한 것으로 평가받는 것은 규제 샌드박스(Regulatory Sandbox)이다. 규제 샌드박스는 FCA가 Project Innovate의 일환으로 도입한 규제정책으로[60], 혁신적인 금융 서비스 기업들에게 '실험의 장'을 제공하기 위해 도입한 것이다. 규제 샌드박스란 위험성이 있는 활동을 할 수 있음에도 어떤 규제에 제한을 받지 않고 혁신적인 제품과 서비스, 사업 모델 등을 마음껏 테스트 해볼 수 있는 안전 영역을 제공하는 것을 의미한다. FCA는 금융상품 및 서비스가 시장에 출시될 때까지의 잠재적 비용 절감, 자금조달에 대한 접근성 개선, 혁신적 상품의 시장화라는 세 가지 이점을 사업자에게 제공하도록 하는 것을 목표로, 세부 기준을 설정하여 모든 기업에게 공정하고 투명한 기회를 준다. 규제 샌드박스 이용 신청 자격은 ① 기업이 샌드박스의 범위 안에 있는가?, ② 기업이 진정한 혁신을 보여주는가?, ③ 기업이 소비자에게 이익을 제공하는가?, ④ 기업이 샌드박스를 필요로 하는가?, ⑤ 기업은 심사를 받을 준비가 되어 있는가? 등 5가지 이다. 규제 샌드박스 이용 기업으로 선정된 기업은 실험하고자 하는 상품이나 서비스에 대해 FCA의 사안 별 개별 지침을 적용받으며, 제한적 상황 하에서 특정 규제들에 대한 적용을 면제받는다. 또한 비조치서면 의견서를 통해 샌드박스 이용 기간동안 규제 적용을 배제 받을 수 있는 혜택을 받는다.

이와 같이, 영국은 레그테크 기업 등의 새로운 금융 서비스가 시장 경쟁 및 소비자의 이익에 미치는 영향이 긍정적으로 판단되는 경우 제도적 유연성을 발휘하여 소비자 및 기업의 이익을 최대화할 수 있도록 혁신적인 규제 환경을 조성하였다. 이는 레그테크 서비스를 제공하고자하는 스타트업이 시장의 선택을 받거나 정부의 승인을 받기까지 소요되는 비용과 시간을 절감할 수 있도록 해주며, 서비스의 시장성이나 위험성을 사전에 점검하고 개선함에 있어 중요한 역할을 하고 있다.

레그테크 분야에 집중하여 투여한 FCA의 정책도 상당히 다양하다. 2016년 4월부터 현재까지 5번에 걸쳐 개최한 TechSprints 행사는 레그테크 서비스의 중요한 문제를 평가하고 해결하기 위해 시장 참여자들이 반드시 논의하여야 하는 공통의 과제들에 대해 함께 협력하고 고민할 수 있는 논의의 장을 제공하고 있다.[61] TechSprints는 매번 다른 도전과제를 선정하여 해결책을 모색하고, 기술 혁신의 잠재적인 이점을 극대화시키는 촉매 역할을 하고 있다. 금융당국이 주도하여 TechSprints와 같은 해

커톤(Hackathon) 행사를 개최한다는 것은 정부만이 학계·산업계·시민사회계 등 다양한 이해관계자 사이의 중재자, 조정자 역할을 할 수 있고, 논의 결과를 정책에 즉각 반영할 수 있다는 점에서 상당히 긍정적인 의의를 가진다고 볼 수 있다. 금융당국이 정책을 추진하기 이전에 CFI를 먼저 발표하고 의견을 수렴하는 것도 이러한 노력의 연장선이라고 볼 수 있다.

영국 FCA는 TechSprints 개최나 CFI를 발표하는 것 이외에도 레그테크와 관련하여 혁신 기술의 개발 우선순위나 실제 사용 사례를 파악하고 규제/정책에 대한 설명을 제공하기 위해 업계와의 대화 기회를 지속적으로 만들고 있으며, 기업들이 마주한 규제 관련 도전을 해결하기 위한 인큐베이터 프로그램을 만들고 있다. 뿐만 아니라 FCA는 직접 레그테크 솔루션을 실험하고 개발하며, 연구 프로젝트에 있어 영국 주요 대학들과 제휴를 맺고 있다.[51]



<그림 11> 영국 금융당국 주도의 정책추진에 따른 레그테크 논의의 증가

[2016년 1월~2017년 10월 간 트위터 잠재 노출도(Twitter Potential Impressions) 측정 결과]

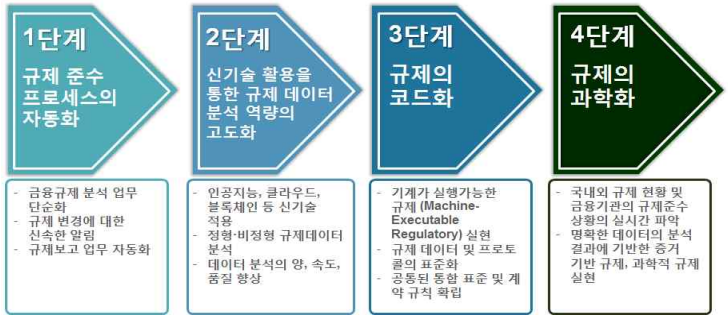
영국 금융당국의 정책적 노력이 레그테크 관련 이해관계자들의 관심 제고와 산업 발전에 큰 역할을 하고 있다는 것은 FCA가 주요 정책을 발표하거나 레그테크 관련 연구모임을 개최할 때마다 트위터 상의 레그테크 언급 빈도 및 노출도가 증가하는 것(<그림 11>)을 통해서도 실질적으로 체감할 수 있다. 이는 금융당국이 금융당국, 금융회사 및 기술개발 업체 등 레그테크 이해관계자 간의 의견개진과 협업의 창구 역할을 주도적으로 수행하고 있음을 보여준다.

V. 결 론 : 레그테크의 발전 모델과 국내 레그테크 도입 방향

1. 레그테크의 발전 모델 제시

본 논문에서 레그테크의 정의와 범주에 대해 검토한 결과, 현재의 레그테크는 핀테크의 하위 영역으로, 기존의 컴플라이언스 솔루션이 고도화된 형태로써, 규제와 관련된 다양한 위험들을 기술로 담보해줄 수 있는 위험관리 방안으로 파악되었다. 그러나 레그테크의 가능성은 단순히 기술의 영역에 한정되는 것이 아니라 금융 규제산업의 전체를 바꿔놓을 수 있을 정도로 무궁무진하다. 레그테크의 발전은 금융서비스의 형태와 발전방향에 영향을 미칠 것이며, 금융당국의 규제 방식을 바꾸어 놓을 수 있고, 새로운 규제표준을 구축하도록 하는 촉매제가 될 수도 있다. 영국 FCA가 레그테크 이해관계자들로부터 받은 요구사항과, 이를 기반으로 영국 금융당국이 업계와 함께 연구 중인 내용들도 이러한 레그테크의 발전 가능성을 뒷받침한다.

금융 서비스 산업이 발전하자 핀테크와 관련된 활동이 폭발적으로 증가한 반면 레그테크 시장은 아직 그 수요를 따라가지 못하고 있다.[21] 앞으로 금융 서비스 산업의 발전에 따라 레그테크가 필요한 영역은 더욱 넓어질 것이며, 레그테크의 발전 가능성과 발전 단계를 미리 예측하고 장기적인 관점으로 투자하지 않는다면 산업의 수요를 적시에 충족시키기 힘들 것으로 생각된다. 따라서 본 장에서는 본 논문에서 도출한 시사점들과 현재 업계에서의 레그테크 논의를 종합하여 레그테크의 발전 단계를 제시해보고자 한다.



〈그림 12〉 레그테크의 발전모델

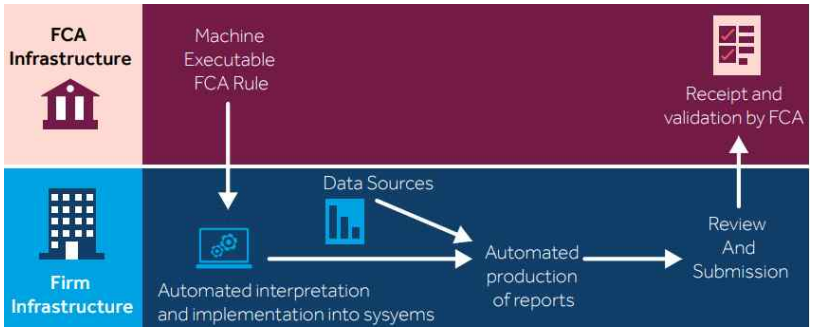
우선 레그테크 발전의 첫 번째 단계는 '규제준수 프로세스의 자동화' 단계이다. '레그테크(RegTech)'라는 단어가 등장하기 이전부터 금융업계에서는 규제와 관련된 비효율성을 개선하고 인건비를 감축시키기 위해 규정준수 업무의 자동화를 위해 노력해왔다. 규제준수 프로세스의 자동화는 컴플라이언스 분야의 전통적인 목표인 것이다. 실제 전 세계 레그테크 회사들이 2017년도 1분기에 투자를 받은 목적 중 핵심은 프로세스의 자동화였다.[62] 기존의 단순한 금융규제 분석 업무를 단순화시키고 규제 변경에 대해 신속히 알려주며, 규제보고 업무를 자동화시켜 준다면 규제준수 업무의 효율성 및 효과성을 극대화시키고 관련 인력과 비용을 감축시킬 수 있을 것이다.

레그테크 발전의 두 번째 단계는 '신기술 활용을 통한 규제 데이터 분석역량의 고도화' 단계이다. 레그테크라는 용어가 이슈가 되고 레그테크 기업이 급격히 성장하고 있는 이유는 인공지능, 딥러닝, 클라우드/클라우드 컴퓨팅, 블록체인 등 신기술이 해당 분야에 적용되기 시작했기 때문이다. 기업들은 규제준수와 관련된 비용과 위험에 대한 부담을 줄이기 위해 기업 내·외부 데이터와 규제 데이터를 수집하고 분석하여 보다 나은 의사결정을 위한 통찰력을 가지길 원한다. 신기술의 등장은 규제준수 프로세스를 단지 자동화시키는 수준을 넘어 정형·비정형 규제 데이터를 분석할 수 있는 능력을 선물하였고, 나아가 엄청난 양의 데이터를 빠른 시간 안에 학습하여 유의미한 가치를 창출할 수 있는 시대를 열어주었다. Deloitte가 제시한 민첩성(Agility), 속도(Speed), 통합(Integration), 분석(Analytics)이라는 레그테크의 4가지 특징[22]은 모두 신기술의 발전과 도입을 통한 것이라고 볼 수 있다. 점차 금융회사는 레그테크를 활용한 규제 데이터 분석역량의 고도화를 통해 규제준수의 편의성을 획기적으로 높여갈 것이며, 금융당국은 양적 규제(Quantitative Regulatory)에 대응하여 다양한 국내외의 규제준수 사항에 대한 상시 모니터링 체계를 구축해나갈 것이다.

레그테크 발전의 세 번째 단계는 '규제의 코드화' 단계이다. 규제 데이터 분석역량이 고도화된다고 해도 결국 규제는 텍스트 기반의 문서 형태로 배포되며, 규제에 대한 해석, 기업 시스템에의 적용, 금융당국으로의 보고로 이어지는 대부분의 규제준수 과정은 인간의 몫이다. 이로 인해 규제에 대한 서로 다른 해석과 일관되지 않은 보고 형태로 인한 규제 리스크가 반드시 발생한다. 또한 규제의 자동화로 인한 속도 향상도 인간이 해당 프로세스에 개입됨으로 인해 한계가 있을 수밖에 없다. 레그테크의 발전으로 인해 기계가 인간 대신 규제를 해석하고, 손쉽게 적용할 수

있다면 이러한 규제 리스크를 최소화시킬 수 있다.

영국 FCA는 규제준수 영역이 인간의 해석에 덜 의존하도록 만들기 위해 기계가 해석할 수 있고, 기계가 실행가능한 규제(Machine-Executable Regulatory)에 대해 연구하기 시작하였으며 2차 TechSprint 행사에서 건전성 감독기구(PRA)의 일부 핸드북 규칙을 언어로 바꿀 수 있다는 것을 증명하는 개념 증명(Proof of Concept)를 처음으로 개발해내었다.[63]



<그림 13> 규제보고 규칙의 해석과 적용을 자동화시킨 개념증명모델 (FCA, 2018)

FCA는 이러한 가능성을 기반으로 규제를 기계가 이해하고 실행할 수 있는 언어로 코드화하고, 이를 실제 금융규제에 적용할 수 있도록 발전시켜나갈 예정이다. 인간이 기계가 이해할 수 있는 규제를 만들고, 기계가 인간의 규제를 이해하고 적용할 수 있다면 기존 규제의 패러다임은 확연히 바뀔 것이고, 실시간으로 쏟아져 나오는 디지털 세계의 영역 또한 합법적 규제의 틀로 끌어들일 수 있을 것으로 생각된다.

규제의 코드화가 완성되기 위해서는 금융당국이 금융회사들이 규제와 관련 정보와 원장을 저장하고 제출하기 위한 데이터 및 프로토콜을 표준화시켜야 한다. 또한 규제준수 자동화 모델을 위해 규제 관련 용어를 정의하고, 공통된 통합 표준 및 계약 규칙에 대한 지침을 개발하여야 하며 규제보고의 기준도 통일시켜야 할 것이며, 종래의 공급업체의 솔루션 또한 규제당국의 인증을 통해 통합시켜야할 것이다.

레그테크 발전의 네 번째 단계는 '규제의 과학화' 단계이다. 규제의 코드화 단계가 산업 전반에 걸쳐 완성되었다면, 규제당국은 표준화된 규제 프로토콜을 기반으

로 현재 적용되는 국내외 규제의 현황을 한눈에 파악하고, 금융기관 각각의 규제준수 상황을 실시간으로 파악할 수 있는 체계를 구축할 수 있을 것이다. Deloitte가 제시했던 미래의 규제 환경에서 필요로 하는 ① 규제의 현재 상태, ② 규제를 위한 적절한 시기, ③ 적합한 규제의 관점, ④ 규제의 적용 효과 등 4가지 중대 질문[38]에 대한 답을 레그테크로 인해 비로소 파악할 수 있게 되는 것이다.

또한 레그테크로 인해 규제준수 상황의 실시간 파악 및 규제 효과측정이 가능하게 된다면 금융 분야에서 빅데이터 기반의 과학행정의 일환인 증거기반 정책(Evidence Based Policy)을 실현할 수 있도록 해줄 것이다. 증거기반 정책이란 증거를 활용해 정책을 수립하고 이를 기반으로 정책을 실행하고자 하는 개념으로, 정책 결정의 명분을 제공하고 신속한 정책 결정을 가능케 하며, 정책결정과 집행과정에서의 갈등 해결, 정책의 질적 측면 개선 등의 효과를 얻을 수 있다. 증거기반 정책의 측면에서, 규제 준수사항에 대한 실시간 파악과 그에 따른 위험에 대한 실시간 관측은 규제당국이 정책과 규제를 만드는 데 있어 큰 도움이 될 것이며, 새로운 규제의 도입으로 인한 규제효과의 예측도 가능해질 것이다. 이로 인해 규제당국은 종래의 임의적 추론에 의한 규제가 아니라 명확한 데이터의 분석과 결과에 기반 한 과학적 규제를 실현할 수 있게 된다.

2. 국내 레그테크 도입 방향과 향후 과제

지난 몇 년간 정부와 업계의 노력으로, 우리나라에서도 핀테크가 하나의 새로운 산업 영역으로 형성되어가고 있다. 핀테크 기업의 수는 2018년 4월 말 기준 217개로 1년 전의 145개 대비 49.7% 가량 증가하였고, 전자금융업자도 95개로 전년대비 11.8% 가량 늘었다.[64] 금융회사들은 핀테크 기업과 제휴하여 핀테크 서비스를 활용하기 시작하였으며, 인터넷전문은행의 개시로 본격적인 핀테크의 확산기가 시작되었다고 해도 과언이 아니다.

그러나 핀테크 산업의 발전 추세에도 유독 국내의 레그테크의 도입 및 활성화는 더딘 실정이다. 우리나라에서의 레그테크에 대한 인식은 아직 전무하거나, 규제대응 업무를 효율화할 수 있는 기술이라는 인식 정도에 머무르고 있으며, 앞으로 발생할 컴플라이언스 문제들은 기존의 준법감시 인력을 늘리는 것으로 해결가능하다고 생각하는 모양새이다. 레그테크에 대한 무지와 무관심 속에 자연스레 레그테크 산업 생태계 구축은 물론이고 관련 스타트업조차 나오지 못하고 있다.

복잡화・디지털화되는 규제 변화의 움직임 속에 국내 금융당국이 먼저 레그테크 도입을 위한 의지를 내비쳤다. 2017년 최흥식 금융감독원장은 ‘레그테크(RegTech) 도입 및 활성화 과제’ 세미나에서 “레그테크는 단기적으로 투자비용을 발생시키겠지만 조금 더 기간을 길게보면 규제 대응과 리스크 관리 능력을 고도화하고 효율성을 높여 금융회사의 전체적인 비용절감 효과가 더 클 것”이라며 레그테크 산업 육성을 적극 지원할 것을 천명하였다.[65] 본 세미나를 통해 금융당국은 레그테크를 감독당국의 업무 범위에 포함함과 동시에 레그테크 도입 세부 추진방향을 발표하였는데, 그 내용은 크게 ① 금융감독 역량 강화를 위한 빅데이터 분석 체계 구축, ② 보고서 제출 및 관리를 위한 레그테크 서비스 제공, ③ 인공지능(AI), 빅데이터 분석을 활용한 소비자 보호 강화, ④ 금융보안 레그테크 인프라 구축 등으로 금융당국이 선제적으로 내부 레그테크 시스템을 구축하겠다는 것이다. 국내 금융당국은 국내 레그테크 인프라 구축을 공공재적 성격으로 보고 금융당국과 금융회사간 소통과 연계를 견인하는 정책 허브 역할을 수행하는 것을 목표로 하고 있다.

본 논문에서 제시한 레그테크 발전모델에 대입해보면 국내 레그테크 도입 수준은 아직 1단계에 집중하고 있는 것으로 보인다. 금융당국이 제시한 금융분야 레그테크 추진 계획에서는 향후 레그테크의 발전계획을 금융보안 레그테크 체계 마련에 집중하는 ‘도입기’, 레그테크 체계 정착 및 활성화를 목표로 하는 ‘성장기’, AI 등 新 IT기술을 활용한 레그테크 고도화를 추진하는 ‘확대기’로 제시하였다.[66] 국내 금융당국은 우선적으로 현재의 IT기술을 중심으로 한 규제 프로세스 자동화(레그테크 발전모델 1단계)에 집중하고, 신기술의 도입을 통한 레그테크의 고도화(레그테크 발전모델 2단계)를 점진적 목표로 설정한 것이다.

반면 영국의 경우 이미 레그테크 발전모델 2단계에 해당하는 신기술을 활용한 규제준수 서비스를 제공하는 레그테크 스타트업들이 금융시장에서 활발히 활동하고 있으며, 이러한 레그테크 기업들이 실제 적용될 수 있는 분야들에 대해서도 FCA 주도의 활발한 논의가 이루어지고 있다. 또한 금융 감독기관은 금융회사에 대한 감독업무의 효율성 개선을 위해 레그테크 신생업체의 솔루션을 이미 도입하여 사용 중에 있다.[67] 나아가 영국 금융당국은 기계가 실행가능한 규제(Machine-Executable Regulatory)대한 개념증명을 개발하고 실제 적용이 필요한 요구사항에 대해 Call for Input을 발행하는 등 ‘규제의 코드화’ 단계인 레그테크 발전모델 3단계로 나아갈 만반의 준비를 하고 있다고 판단된다.

우리나라는 서방 국가에 비해 컴플라이언스 실패로 인해 천문학적인 벌금이나 과

태료 등 엄청난 규제준수 비용을 감내해야하는 경우가 적으며, 국내 금융회사는 컴플라이언스 비용을 IT 비용과 별개로 구분하여 컴플라이언스 부서의 인건비 중심으로만 생각하는 경향이 있어 아직까지는 국외에 비해 레그테크에 대한 관심이 적은 편이다.[68] 그러나 영국 등 글로벌 레그테크 발전 수준이 3, 4단계까지 나아간다면, 규제 이행 및 감독에 있어 규제준수 관련 기술을 별개로 생각할 수 없을 것이고, 글로벌 규제들은 코드화, 표준화되어 레그테크를 통하지 않는 규제 업무는 불가능해질 것이다. 그 때에는 먼저 표준을 제시하고 솔루션을 통합하는 국가가 글로벌 금융시장의 주도권을 가져갈 것이고, 우리나라가 레그테크 산업 경쟁에서 뒤쳐진다면 또다시 패스트 팔로워(Fast follower) 전략을 택하는 것 말고는 선택지가 없을 것이다.

이 때문에 우리나라도 다가올 양적 규제의 시대, 컴플라이언스 혁신의 시대를 대비하여 레그테크의 중요성을 인식하고 장기적 시각으로 관련 기술과 산업을 육성해 갈 필요가 있다. 특히 우리나라는 금융당국의 정책방향이 산업 발전과 규제 환경 변화에 상당히 큰 영향을 미치는 국가이기 때문에, 금융당국이 규제의 혁신을 이끌고 실질적인 산업발전의 구심점 역할을 하고 있는 영국의 사례가 아주 좋은 참고 모델이 될 수 있다. 영국 FCA는 혁신센터(Innovation Hub)와 규제 샌드박스를 통해 레그테크 개발을 적극 장려하고 있다. 기술과 솔루션의 개발 및 상용화는 민간 기업이 가장 잘 할 수 있는 영역이기에 우리나라도 新금융서비스를 실제 금융시장과 유사한 가상환경에서 사전 테스트해볼 수 있는 Virtual Test-Bed의 대상에 레그테크와 관련한 스타트업의 참여를 적극 유도하여 집중 육성할 필요가 있다.

또한 규제가 기술에 명확히 반영되기 위해서는 금융당국, 금융회사 및 기술개발업체 등 이해관계자 간 지속적 논의 및 협의가 필요하므로 이들이 정기적으로 지식과 정보를 공유하고 협업의 교두보를 마련할 수 있는 기회를 만들어주는 역할을 금융당국이 주도적으로 수행하여야 한다. 규제당국과 업계 전문가들이 지켜보는 가운데 혁신 기술을 테스트할 수 있는 영국의 TechSprints나 해커톤 행사 등을 개최하는 것도 고려할 필요가 있다. FCA가 CFI의 발행을 통해 레그테크 이해당사자들의 의견을 듣고 이를 기반으로 레그테크 정책을 추진하는 것처럼, 금융당국의 정책이 산업 및 시장과 동떨어진 추상적 정책을 수립하는 것이 아니라 산・학・연의 의견을 적극적으로 수용하는 것으로부터 정책 개발을 시작해야 할 것이다.

레그테크는 핀테크의 영역을 넘어서 독립적이고 확장적인 영역으로 성장할 수 있는 무한한 가능성을 지녔으며, 금융 규제의 전체 판도를 바꿀 ‘게임 체인저(Game

changer)’로 기대되고 있다. 규제준수 업무의 효율성 향상을 위해 레그테크를 활용할 주체는 주로 금융기관들이지만, 레그테크 산업을 활성화 시키고 레그테크와 규제 환경을 실제 연동시키는 것은 금융당국만이 할 수 있는 역할이다. 국내 금융당국이 레그테크의 중요성을 인지하고 장기적인 관점에서 국내 실정에 맞는 레그테크 생태계를 조성해줄 것을 기대한다.

참고문헌

[1] Jeff Kelly, “Big Data Vendor Revenue and Market Forecast 2011-2026”, Wikibon, 2015.03.31.
[2] International Quality and Productivity Center, “Big Data Analytics for Finance Service Survey Report 2018”, 2018.
[3] 안수현, “지능형 인공지능(AI)의 발전에 따른 자본시장법제 정비방향과 과제”, 증권법 연구, Vo. 18, No. 3, p.139, 2017.
[4] 금융보안원, “금융권 레그테크 국내외 최근 동향 및 시사점”, p.5, 2018.
[5] U.S. Securities & Exchange Commission, “Report of the staffs of the CFTC and SEC to the joint advisory committee on emerging regulatory issues”, Fidndings Regarding the Market Events of May 6, 2010, 2010.10.30.
[6] Digital Daily, “삼성증권 배당금 입력 착오, 증권거래시스템 총체적 난국 드러내”, Available : http://www.ddaily.co.kr/news/article.html?no=167664, 2018.04.09.
[7] Digital Daily, “내부통제 부실 도마, ‘레그테크’ 다시 주목”, Available : http://www.ddaily.co.kr/news/article.html?no=167678, 2018.04.10.
[8] 옥타솔루션, “REGTECH 전망과 도입 필요성”, 레그테크(RegTech) 도입 및 활성화 과제 세미나 발표자료, p.7, 2017.
[9] Digital Daily, “핀테크도 감시 대상...강화되는 글로벌 AML규제, 어떻게 대응할 것인가?”, Available : http://www.ddaily.co.kr/news/article.html?no=157408, 2017.06.25.
[10] Business News, Banks paid $321 billion in fines since financial crisis: BCG, Reuters Staff, Available : https://www.reuters.com/article/us-banks-fines/banks-paid-321-billion-in-fines-since-financial-crisis-bcg-idUSKBN1692Y2, 2017.03.03.
[11] 조민기, “인공지능(AI)과 머신러닝을 활용한 레그테크 성공 전략”, 디지털데일리 전문가기고, 2018.06.19.
[12] 중앙일보, “미국 금융당국, 농협은행 뉴욕지점에 과태료 118억원 부과”, Available : https://news.joins.com/article/22227217, 2017.12.22.
[13] Accenture Consulting, “Compliance : Dare to be different”, 2017 Compliance risk study, 2017.04.17.

[14] Medici Research Report, “Strategic analysis of RegTech : A hundred billion-dollar opportunity”, 2016.04.01.
[15] Financial News, “금융사 준법감시도 AI가 맡는 시대 온다”, Available : http://www.fnnews.com/news/201710191709582706, 2017.10.19.
[16] UK Financial Conduct Authority, FCA Innovate, Available : https://www.fca.org.uk/firms/regtech, 2017.09.12.
[17] Institute of International Finance, “RegTech in Financial Services : Technology Solutions For Compliance And Reporting”, 2016.03.
[18] Gregory Roberts, “Fintech Spawns Regtech to Automate Compliance With Regulations”, Bloomberg BNA, 2016.06.22.
[19] John Rampton, “Everything you need to know about RegTech-The new FinTech”, Guest post on DUE, Available : https://due.com/blog/everything-need-regtech-new-fintech/, 2016.10.21.
[20] Luz Fernández Espinosa, “10 Keys to understand what regtech is all about”, BBVA Research, Available : https://www.bbva.com/en/10-keys-understand-regtech/, 2016.05.23.
[21] Institute of International Finance, “RegTech : Exploring Solutions for Regulatory Challenges”, Research Note, Available : https://www.iif.com/topics/regtech/regtech-exploring-solutions-regulatory-challenges, 2015.10.29.
[22] Devid Dalton, et.al., “RegTech is the New Fintech? : How agile regulatory technology is helping firms better understand and manage their risks”, Deloitte, Available : https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/financial-services/performancemagazine/articles/lu-how-agileregulatory-technology-is-helping-firms-better-understand-and-manage-their-risks-24052016.pdf, 2016.
[23] Tom Butler, et.al., “On the role of ontology-based RegTech for managing risk and compliance reporting in the age of regulation”, Journal of Risk Management in financial Institutions, Henry Stewart Publications, Vol. 11, no 1, pp.19-33, 2018.
[24] Venture Scanner, “Fintech ecosystem update”, Available : http://insights.venturescanner.com/2015/04/07/fintech-ecosystem-update-april-2015, 2015.04.07.
[25] UK Trade&Investment, “Landscaping UK fintech”, Available : https://www.gov.uk/government/publications/landscaping-uk-fintech, 2014.08.06.
[26] Bernard Lunn, “How Traditional and Emergent Fintech could converge and change Finance”, Daily Fintech, Available : https://dailyfintech.com/2016/12/05/how-traditional-and-emergent-fintech-could-converge-and-change-finance/, 2016.12.05.
[27] UK Government Office for Science, “FinTech Futures : The UK as a World Leader in Financial Technologies”, Available : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf, 2015.03.18.
[28] 조창훈, “국내 레그테크의 시장성 검토 및 도입 시 고려사항”, 전자금융과 금융보안, Vol. 8, p.73, 2017.04.
[29] Chris Skinner, “What is ‘FinTech’?”, Chris Skinner’s Blog, Available : https://thefinanser.com/2015/01/ghgh.html/, 2018.07.25.
[30] BBVA, “Banking Outlook“, BBVA. BBVA FINANCIAL SYSTEMS UNIT, Available : https://www.bbvaresearch.com/wp-content/uploads/2016/03/Banking-Outlook-Q116.pdf, 2016.03.
[31] Tom Butler, et.al., “On the role of ontology-based RegTech for managing risk and compliance reporting in the age of regulation”, Journal of Risk Management in financial Institutions, Henry Stewart Publications, Vol. 11, no 1, p.23, 2018.
[32] 조창훈, “국내 레그테크의 시장성 검토 및 도입 시 고려사항”, 전자금융과 금융보안, Vol. 8, pp.49-71, 2017.04.
[33] 곽기웅, “IT와 규제가 만난다 RegTech”, Koscom, Available : http://dfrc.kif.re.kr/wp-content/uploads/2018/07/IT%EC%99%80-%EA%B7%9C%EC%A0%9C%EA%B0%80-%EB%A7%8C%EB%82%98%EB%8B%A4-RegTech.pdf, 2016.11.21.
[34] Andy Haldane, Speech at the Maxwell Fry Annual Global Finance Lecture: Managing Global Finance as a System, Birmingham University. 2014.10.29.

[35] Stefano Battiston, et al., “Complexity Theory and Financial Regulation”, SCIENCE Published by AAAS, Available : http://www.isigrowth.eu/wp-content/uploads/2016/05/battiston2016complexity.pdf, 2016.02.19.
[36] Scott R. Peppet, “Smart Mortgages”, Privacy and the Regulatory Possibility of Infomediation, Available : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1458064, 2009.08.22..
[37] World Economic Forum, “Deep Shift : Technology Tipping Points and Societal Impact”, 2015.09.
[38] Deloitte Insights, “The future of regulation : Principles for regulating emerging technologies”, A report from the Deloitte Center for Government Insights, 2018.
[39] Bank for International Settlements, “Principles for effective risk data aggregation and risk reporting”, Basel Committee on Banking Supervision, Available : https://www.bis.org/publ/bcbs239.pdf, 2013.01.
[40] CB Insight, “Regtech Market Map : The Startups Helping Businesses Mitigate Risk and Monitor Compliance Across Industries”, RESEARCH BRIEFS, Available : https://www.cbinsights.com/research/regtech-regulation-compliance-market-map/, 2017.02.06.
[41] H2 VENTURES, et.al., “2016 FINTECH 100 : Leading Global Fintech Innovators”, 2016.
[42] H2 VENTURES, et.al., “2017 FINTECH 100 : Leading Global Fintech Innovators”, 2017.
[43] Marco Antonio Cavallo, “How RegTech closes the gap between technology and financial services”, CIO From IDG, Available : https://www.cio.com/article/3190162/it-industry/how-regtech-closes-the-gap-between-technology-and-financial-services.html, 2017.04.18.
[44] EY, “Innovating with RegTech”, Available : https://www.ey.com/Publication/vwLUAssets/EY-Innovating-with-RegTech/$FILE/EY-Innovating-with-RegTech.pdf, 2016.
[45] FINANCIAL TIMES, “Osborne wants London to be ‘global centre for fintech’ ”, Available : https://www.ft.com/content/1f24a25e-886f-11e5-90de-f44762bf9896, 2015.11.11.
[46] 안수현, “영국의 핀테크관련 법제도와 지원정책 : 지급결제산업을 중심으로”, 강원법학, 제29권, pp.179-219, 2016.10.
[47] UK FCA Project Innovate, Financial Conduct Authority, Available : https://www.fca.org.uk/firms/fca-innovate.
[48] UK Government Office for Science, “FinTech Futures : The UK as a World Leader in Financial Technologies”, 2015.03.
[49] UK Financial Conduct Authority, “Call for Input : Supporting the development and adoption of RegTech”, 2015.11.
[50] UK Financial Conduct Authority, “Feedback Statement : Call for Input on supporting the development and adopters of RegTech”, 2016.07.
[51] Nick Cook, “RegTech at the FCA”, UK Financial Conduct Authority Financial Services Club, 2018.02.07.
[52] UK Financial Conduct Authority, “Consumer Access TechSprint”, Available : https://www.fca.org.uk/events/techsprints/consumer-access-techsprint, 2016.04.18.
[53] UK Financial Conduct Authority, “Unlocking regulatory reporting TechSprint”, Available : https://www.fca.org.uk/events/techsprints/unlocking-regulatory-reporting-techsprint, 2016.11.09.
[54] UK Financial Conduct Authority, “Financial services and mental health TechSprint”, Available : https://www.fca.org.uk/events/techsprints/financial-services-and-mental-health-techsprint, 2017.03.07.
[55] UK Financial Conduct Authority, “Model driven machine executable regulatory reporting TechSprint”, Available : “https://www.fca.org.uk/events/techsprints/model-driven-machine-executable-regulatory-reporting-techsprint”, 2017.11.20.
[56] UK Financial Conduct Authority, “AML and Financial Crime International TechSprint”, Available : https://www.fca.org.uk/events/techsprints/aml-financial-crime-international-techsprint,

2018.05.22.
[57] UKTI, “Fintech The UK’s unique ecosystem for growth”, Available : https://www.slideshare.net/MehmetBasaran/fintech-the-uks-unique-environment-for-growth, 2014.11.05.
[58] EY, “UK FinTech On the cutting edge : An evaluation of the international FinTech sector”, Available : https://www.ey.com/Publication/vwLUAssets/EY-UK-FinTech-On-the-cutting-edge/%24FILE/EY-UK-FinTech-On-the-cutting-edge.pdf, 2016.
[59] 양효은, “영국의 핀테크 산업 지원정책 및 시사점”, 대외경제정책연구원 World Economy Today, Vol. 16, No. 31, 2016.11.08.
[60] UK Financial Conduct Authority, “Regulatory sandbox”, Available : https://www.fca.org.uk/publication/research/regulatory-sandbox.pdf, 2015.11.
[61] UK Financial Conduct Authority, Available : https://www.fca.org.uk/firms/regtech/techsprints, 2017.09.11.
[62] TRANSATLANTIC, “The Future of RegTech for Regulators : Adopting a Holistic Approach to a Digital Era Regulator”, 2017.06.
[63] UK Financial Conduct Authority, “Call for Input : Using technology to achieve smarter regulatory reporting”, Available : https://www.fca.org.uk/publication/call-for-input/call-for-input-smarter-regulatory-reporting.pdf, 2018.02.
[64] 정유신, “핀테크 2단계 확산을 위한 과제”, 한국금융 FN칼럼, Available : http://www.fntimes.com/html/view.php?ud=20180603225738347 0dd55077bc2_18, 2018.06.04.
[65] M이코노미뉴스, “첨단 금융범죄 막는다, ‘레그테크(RegTech)’”, Available : http://www.m-economynews.com/news/article.html?no=20770, 2017.11.18.
[66] 김용태, “레그테크 활성활르 위한 금융당국의 역할”, 레그테크(RegTech) 도입 및 활성화 과제 세미나 발표자료, 2017.10.19.
[67] VIZOR, Available : https://vizorsoftware.com/clients/
[68] 조창훈, “국내 레그테크의 시장성 검토 및 도입 시 고려사항”, 전자금융과 금융보안, Vol. 8, pp.74-75, 2017.04.

금융회사의 보안 위험성향 프레임워크와 측정지표 개발에 관한 연구

김기삼* · 권대암** · 권보성**· 이지수**· 이지은**
* 중앙대학교 일반대학원 산업융합보안학과
** 중앙대학교 산업보안학과

요 약

4차 산업 혁명이 점차 본격화되면서 금융 산업에서도 ICBM(IoT, Cloud, Big Data, Mobile)과 같은 혁신적 디지털 기술을 활용하여 맞춤형 금융서비스, 핀테크, 레그테크 등 새로운 서비스가 개발되고 있으며 이에 따른 다양한 보안위험이 점증하고 있다. 이러한 상황적 변화에 따라 금융당국에서는 컴플라이언스 기반의 보안체계가 아닌 위험관리 기반 보안활동을 강조하는 자율보안체계를 시행 중에 있다. 자율보안체계를 구현하기 위해서는 금융회사의 상황을 고려한 최적의 위험관리가 핵심적인 성공요인이라고 할 수 있다. 그러나 대부분의 금융회사는 과거의 컴플라이언스 기반의 보안활동에 익숙해져 있어 보안 위험관리 활동은 형식적인 수준에 수행되고 있으며, 특히 중소 금융회사의 경우 위험관리 구현은 미흡한 실정이다.

위험관리를 위해서는 우선 금융회사의 대내외 환경, 비즈니스 전략과 목표와 연계된 조직의 보안 위험성향(Risk Appetite)을 파악하는 것이 필수적이라고 할 수 있다. 즉, 보안 위험성향에 대한 분석과 식별 활동은 위험관리 초기 활동으로서 허용가능한 위험수준(Acceptable Level of Security Risk)을 결정하는 것이며 이는 추후 위험관리 프로세스에서 발생하는 제반 의사결정 과정에 있어 판단기준을 제공한다.

따라서 본 논문에서는 위험관리 프레임워크와 관련 위험성향 선행연구 분석을 통하여, 금융회사의 보안 위험관리 전략 수립을 위한 위험성향 프레임워크를 개발하고 보안 위험성향 수준 및 유형을 가시적으로 식별할 수 있는 측정지표를 개발하였다. 또한 개발된 위험성향 지표의 실무적 타당성을 검토하기 위해 금융실무 전문가들로 구성된 자문위원회를 통해 적용가능성과 중요성을 검토하였다.

키워드

위험관리, 위험성향, 금융보안, 위험 성향 프레임워크, 위험 성향 지표

목 차

I. 서 론

ICBM(IoT, Cloud, Big Data, Mobile), 인공지능(AI), 5G와 같은 디지털 기술이 빠르게 혁신적으로 진화하고 있다. 이런 용어를 'Disruptive Technology' 즉 '파괴적 신기술'이라고 부른다. 이 파괴적인 신기술을 바탕으로 기업들은 물리적인 자원과 디지털 자원이 융합함으로써 새로운 가치와 기회를 만들어 내는 디지털 비즈니스 세계로 나아가고 있다.

금융 산업에서도 다양한 영역에서 디지털 비즈니스로의 패러다임이 바뀌고 있다. 파괴적인 신기술은 금융 소비자들의 행동과 선호를 변화시킨다. 시간과 장소, 결제 수단에 구애 받지 않고 빠르게 간편한 결제가 가능해지는 지급결제수단의 간편화 및 다양화부터 시작하여, 입출금, 보험, 대출까지 시중 은행의 거의 모든 서비스를 비대면으로 제공한다. 또한 핀테크로 요약될 수 있는 새로운 기술의 도입은 데이터의 분석 및 생산·저장 능력을 향상시켜 다품종·소량의 고객 맞춤형 상품 개발을 촉진시키고 있다.

이렇게 파괴적인 기술은 금융서비스를 제공하는 기업에게 다양한 기회를 제공하기도 하지만 이에 따라 보안 위험도 점차 증가하고 있다. 이용자 편의성 중심의 서비스 출시와 금융·IT기술융합, 새로운 기술 도입에 따른 신규 보안 취약점과 개인금융 정보 공유채널·매체 증가에 따른 정보 유출이 가능해진 것이다. 이러한 상황적 변화에 대응하기 위해 금융 산업은 컴플라이언스 기반의 보안체계가 아닌 위험관리 기반 보안활동을 강조하는 자율보안체계를 시행 중에 있다. 이때 자율보안체계는 핀테크 산업 활성화를 위해 IT보안규제의 패러다임을 사전규제에서 사후규제로의 전환을 추진함에 따라, 금융회사 스스로 내부통제 및 정보보안을 향상시키고 핀테크 시대에 부응하는 자율적 보안체계를 수립하는 것을 의미한다. 다시 말해서, 자율보안체계란 금융회사가 스스로 다양한 기술 선택권을 가지고 보안 점검 및 관리체계를 구축하며 최고의사결정자 책임 하에 실질적 보안역량 향상을 이루는 것을 말한다.

그러기 위해서는 금융회사의 상황을 고려한 최적의 위험관리가 핵심적인 성공요인이라고 할 수 있다. 금융회사의 IT 보안상 위험은 해당 금융회사가 가장 잘 파악할 수 있으며, 위험관리는 비용이 아닌 투자의 개념으로 인식, IT부문(정보&시스템)에 한정된 것이 아니라 전 비즈니스 영역으로 보는 관점이 변화하는 금융 패러다임에 대응하는 자율보안체계에서 필요하다 [1]. 그러나 대부분의 금융회사는 과거의

컴플라이언스 기반의 보안활동에 익숙해져 있어 보안 위험관리 활동은 형식적인 수준에 수행되고 있으며, 특히 IT 감사 및 보안 전문 인력이 부족한 중소 금융회사의 경우 위험관리 구현은 미흡한 실정이다.

'2018년도 IT·핀테크 감독검사 업무설명회'에서 금융감독원은 금융회사의 위험관리 강화를 위해서는 정보보호 활동을 경영전략에 연계하고, 이사회와 경영진이 IT보안에 대한 역할을 자체적으로 향상시키는 등 올바른 금융회사의 보안 지배구조를 구축하는 것이 필수적이라고 강조했다 [2]. 이렇듯 금융회사의 위험관리를 비즈니스 전략과 연계하기 위해서는 금융회사의 대내외 환경, 비즈니스 전략과 목표와 연계된 조직의 보안 위험성향(Risk Appetite)을 파악하는 것이 중요하다. 즉, 보안 위험성향에 대한 분석과 식별 활동은 위험관리 초기 활동으로서 허용 가능한 위험수준(Acceptable Level of Security Risk)을 결정하는 것이며 이는 추후 위험관리 프로세스에서 발생하는 제반 의사결정 과정에 있어 판단기준을 제공한다.

또한 새롭게 개정된 위험관리 국제 표준 'ISO 31000:2018'에서는 거버넌스, 목표, 운영, 전략 등 비즈니스 모든 측면에서 위험관리와의 통합을 강조하였으며 [3]. 전사적 위험관리 프레임워크인 'COSO ERM Integrating with Strategy and Performance'에서는 비즈니스 목표를 달성하기 위한 일정수준의 위험감수와 함께 위험관리를 전략·성과와 연계 및 통합하는 것의 중요성을 부각시키기도 했다 [4].

종합해보면, 금융회사는 파괴적인 기술들을 활용하여 디지털 비즈니스 세계로 진입하였으며, 디지털 비즈니스의 이점과 함께 예측하지 못하는 수많은 위험들을 가지고 있다고 할 수가 있다. 이러한 환경 변화에 대응하기 위하여, 금융회사는 컴플라이언스 기반이 아닌 금융회사 고유 위험기반의 자율보안체계를 구축하였으며, 자율보안체계 하에서 성공적인 위험관리를 위해서는 보안 위험관리 전략 수립을 위한 조직의 위험성향 파악이 중요하다. 따라서 위험관리 프레임워크와 관련 위험성향 선행연구 분석을 통하여, 금융회사의 보안 위험관리 전략 수립을 위한 위험성향 프레임워크를 개발하고 보안 위험성향 수준 및 유형을 가시적으로 식별할 수 있는 측정지표가 필요하다고 할 수가 있다.

Ⅱ. 이론적 배경 및 선행연구

1. 위험관리 프레임워크

(1) ISO 31000 (위험관리 표준)

ISO 31000은 조직의 관리 프로세스와 연동하기 위한 위험관리 프레임워크를 통해 조직이 직면한 위험을 식별, 평가 및 완화할 수 있도록 하는 위험관리에 대한 국제 표준이다. 조직과 그 맥락에 대한 이해에 주안점을 두며, 이는 해당 표준의 프레임워크에서 알 수 있다.

‘상황설정’, ‘위험식별’, ‘위험분석’, ‘위험평가’, ‘위험처리’의 순서로 이루어진 프로세스의 가장 첫 단계는 상황설정이다. 상황설정은 위험관리 프레임워크를 각 조직에 맞추어 개별적으로 적용하기 위한 것으로, 여기서의 ‘기준’은 ‘위험의 기준’을 의미한다. 즉, 위험관리를 위해 조직은 우선적으로 감수하거나 하지 않을 위험의 양과 유형을 분류해야 한다. 나아가 이는 조직의 가치, 자원, 목표를 반영해야 하며, 조직의 의무와 이해관계자의 인식을 고려할 필요가 있다 [3].

(2) COSO ERM 프레임워크 (전사적 위험관리 프레임워크)

COSO ERM 프레임워크는 전사적 측면에서 기업의 목적을 달성하기 위한 합리적 대응 방안을 생각하고, 기업에 영향을 주는 잠재적인 위험을 파악하여 일정한 수준 내에서 위험을 적절히 관리하게 도와주는 프로세스이다.

이때 일정한 수준이란, 기업이 어느 정도의 위험을 수용할 수 있는가의 문제로, 위험성향을 말하는 것이며, 코소(COSO)는 조직이 목표를 추구할 때 반드시 위험성향을 정해야 함을 명시하고 있다. 위험성향은 넓은 의미에서 조직이 어떤 가치를 추구할 때 수용할 수 있는 위험의 양을 의미한다. 결국 조직에 ERM을 효율적이며 효과적으로 반영하기 위해서는 위험성향이 우선적으로 설정되어야 하며, 이것이 조직전반에 인식되고, 지속적으로 모니터링 될 필요가 있다 [4].

(3) ISO/IEC 27005 (정보보호 위험관리 표준)

ISO/IEC 27005는 정보보호 위험관리 표준으로서, 위험관리 프로세스는 ISO 31000과 대략적으로 일치한다고 볼 수가 있다. ISO/IEC 27005는 상황설정 단계가 매우 중요하다고 할 수가 있다. 전체 프로세스 및 상황설정에 영향을 미치는 위험관리의 목적을 결정해야하며, 정보보안 위험관리에 필요한 기본적인 기준을 설정해야 한다. 여기서 말하는 기본적인 기준은 위험관리 방법과 위험평가 기준을 말한다. 또한 ‘위험분석’ 단계에서 위험수준을 산정하며, 이에 따라 ‘위험평가’ 단계에서 위험의 수준을 위험평가 기준과 위험 수용 기준에 대해 비교하여 평가한다. 이러한 과정을 통해 최종적으로 위험의 처리 방법이 도출되는 것이다. 결과적으로 프로세스의 첫 단계에서 위험을 어떠한 기준으로 평가할 것인지, 즉 어느 정도의 위험을 수용할 것인지를 정해야만 다음 단계로 넘어갈 수 있으며, 이는 후속 단계인 위험평가와 위험처리 방법에 큰 영향을 미친다. 또한 위험 수용 기준은 조직의 정책, 목표, 목적 및 이해관계자의 이해에 따라 달라지며 법 및 규정 측면, 운영, 기술, 재무, 사회적 및 인적 요인을 고려하여 위험 수용 기준을 결정해야 한다고 명시하였다 [5].

2. 위험성향(Risk Appetite) 선행연구 분석

(1) 위험성향(Risk Appetite)의 개념

위험성향이라는 단어는 최근에 새롭게 대두된 것이 아니다. 특히 개인의 투자와 관련하여 재무 분야에서 위험성향이 오랫동안 통용되어 사용되어 왔다. 마취(March)와 사피라(Shapira)는 부정적인 결과가 있더라도 개인이 선택하게 되는 부정적인 결과의 정도로 투자결정에 영향을 주는 변수라고 하였다 [6]. 또한 어윈(Irwin)은 행동의 결과가 불확실하거나 손실의 확률이 있을 때, 행동에 기꺼이 참여하려는 정도라고 정의하였으며 [7], 그라블(Grable)은 재무의사결정시에 사람들이 기꺼이 받아들이려는 불확실성의 최대치라고 정의하였다 [8].

이것을 조직의 관점으로 바라보면 위험성향은 조직이 기꺼이 감당할 수 있다고 생각하는 위험의 크기를 말한다. 대부분의 조직은 손실을 회피하고자 하며, 다만 회피하고자하는 손실의 크기가 조직마다 다르다. 조직의 위험수용성향은 절대적인 개념이 아니고 위험추구와 위험회피의 연속체 상에 위치하는 상대적인 개념이지만, 감당할 수 있는 손실의 크기에 따라 위험회피형, 위험중립형, 위험추구형으로 구분하기도 한다 [9].

(2) 전사적 위험관리(ERM)의 위험성향

1) 정보 시스템 감사・조정 협회(ISACA) 위험성향 프레임워크

정보 시스템 감사・조정 협회(ISACA)는 위험성향을 '한 단체가 임무를 수행하기 위해 기꺼이 받아들이는 위험의 양'이라고 정의하며, 이는 오직 조직 임무의 맥락과 관련이 있고 조직이 위험을 대하는 태도를 결정하는데 도움이 된다고 한다. 또한 명확히 설정된 위험 성향은 위험 관리자들이 어떤 종류의 위험이 수용 가능한지 명확히 인지할 수 있게 도와준다고 언급한다.

좋은 위험성향 프레임워크를 만들기 위해서는 위험회피 및 위험전가 비용을 고려하고 조직의 핵심 위험을 정의해야 하며, 각 위험이 업무 목표와 명확하게 연결되어 있어야 한다. 또한 위험성향을 표현하기 위해 등급화 된 척도를 마련해야 하고 위험 의사결정을 위한 기관을 지정해야 하며, 위험을 단일적으로 보지 말고 총체적으로 보아야 한다 [10].

2) 프라이스워터하우스쿠퍼스(PwC) 위험성향 프레임워크

프라이스워터하우스쿠퍼스(PwC)는 위험성향을 '회사의 전반적인 위험수용가능범위 내에서 회사가 수용하고자 하는 위험의 양'이라고 정의한다. 위험성향을 적절히 표현할 때 조직이 취하고 싶은 위험을 명확히 인지할 수 있고, 다양한 이해관계자들과 지속적인 의사소통을 위한 기반을 세울 수 있으며, 고위 경영층의 위험에 대한 태도를 정확히 표현할 수 있어 조직과 CRO에게 이득이 된다고 언급한다.

또한 위험을 회사의 희망 수익 및 성장수준의 맥락에 놓고 보는 것이 매우 중요하며 위험 성향과 문화 간 관계, 경제적 자본 역시 고려할 것을 강조한다. 또한 정량적이지 않아 측정하기 어려운 위험 역시 관리를 소홀히 해서는 안 되며 위험성향을 업무와 연계시켜야 한다고 언급 한다 [11].

3) 딜로이트(Deloitte) 위험성향 프레임워크

딜로이트(Deloitte)는 위험성향을 '기업이 전략을 추구함에 있어 부담할 의향이 있

는 위험'이라고 정의하며, 좋은 위험성향 프레임워크를 만들기 위한 6가지의 고려사항을 제시한다. 우선, 프레임워크가 재무・비재무 위험을 모두 포함해야 하고, 이사회의 위험성향이 직원들에게 전달되어 전반적인 위험성향이 업무에도 반영될 수 있도록 하는 것이 필요하다고 설명했다. 또한 직원들은 기업의 위험성향과 그 영향에 대해 올바르게 이해해야 하며, 고위 임직원들은 위험성향을 기업에 반영하기 위해 노력해야 한다. 의사결정 과정에서 역시 위험성향을 고려해야 하고, 직원들이 허용된 위험성향 한계 내에서 행동하도록 장려해야 한다 [12].

(3) 위험성향 프레임워크의 적용

1) 대영 도서관(The British Library)의 위험성향

대영 도서관은 세계 최대 규모의 도서관 중 하나로써, 조직의 목표 달성에 부정적인 영향을 미치는 위험을 관리하기 위해 '위험관리 정책 프레임워크(Risk Management Policy Framework)' 2017년 5월에 발표하였다. 이 문서에 의하면 위험성향을 수립하기 위한 고려할 위험 영역으로 비즈니스 연속성, 재무적, 디지털 시스템 보안, 서비스 제공, 이사회 주요 포트폴리오 및 거버넌스, 물리 보안, 컴플라이언스, 직원, IT 인프라, 정보관리, 브랜드, 학계 평판, 기관 평판, 물리적 환경으로 분류하였다 [13].

2) 미국 통화감독청(OCC)의 위험성향

미국 통화감독청은 미국 재무부의 부서로서 연방 은행 시스템을 관리할 수 있는 고유한 권한을 위임받은 독립기관이다. 미국 통화감독청에서는 위험 성향을 기관이 임무를 수행하는 동안 수용할 위험의 수준과 유형으로 정의 내린다.

또한 위험 성향의 영역을 감독 위험, 인적 자원 위험, 전략 위험, 평판 위험, 기술 위험, 운영 위험, 법률 위험, 외부 위험, 재무 위험으로 분류하였는데 이러한 위험을 허용하는 정도를 낮음, 보통, 높음으로 구별을 지었다 [14].

3) 영국 재무부 (HM TREASURY)의 위험성향

영국 재무부는 정부의 공공 재정 정책 및 경제 정책을 개발하고 집행하는 영국의 부서이다. 영국 재무부에서는 위험 성향을 이사회가 기꺼이 위험을 받아들이려는 의지에서부터 받아들이지 못하는 거부감에 이르기까지의 스펙트럼으로 정의 내린다.

영국 재무부에서는 위험 평가에 대한 구체적인 기준으로 재무, 서비스, 대중의 우려와 신뢰, 대중에 대한 위험의 정도, 위험의 실현 가능성에 대한 가역성, 위험을 둘러싼 증거의 신뢰도, 위험이 조직・이해 관계자・파트너・타인에 미치는 영향・위험에 대한 방어 능력 등의 요소를 제시하였는데 이러한 기준들이 전체 위험 관리에 걸쳐 일관되고 체계적으로 적용되는지를 기준으로 삼았다 [15].

3. 국내외 금융권 위험관리 동향

(1) 금융회사의 자율보안체계에서의 보안

금융산업은 핀테크 산업 활성화를 위하여 IT보안규제 중심의 패러다임을 사전규제에서 사후규제로의 전환을 추진함에 따라, 금융회사 스스로 내부통제 및 정보보안을 강화하고 핀테크 시대에 걸맞은 민간 중심의 자율적 보안체계를 수립하는 위험기반의 보안활동을 수행하고 있다. 또한 18년도 금융감독원 업무 계획에 따르면, 디지털 리스크 전반에 대한 상시감시 강화, 인터넷 전문은행의 리스크 관리・내부통제 체계에 대한 정교한 상시감시 전개, 금융플랫폼 변화에 따른 리스크 요인 점검 강화 등 리스크 중심의 금융감독을 구현하겠다고 발표하였다[16]. 또한 美 뉴욕주 사이버보안 요구사항(23 NYCRR 500)에서는 뉴욕 주의 모든 금융기관에 주기적으로 위험평가를 수행하도록 규정하기도 했다[17].

(2) 금융회사의 위험기반의 보안 활동

위험관리를 위해서는 비즈니스 전략 및 목표와 연계된 조직의 보안 위험성향(Risk Appetite)을 파악하는 것이 필수적이라고 할 수 있다. 그러나 금융회사의 위험관리의 중요성이 커지고 있는 시점에서, 관련연구가 부족한 실정이며, 비즈니스 목표와 연계된 보안 위험성향에 대한 연구는 더욱 그러하다.

앞서 언급한 바와 같이 위험성향은 조직이 비즈니스 목표를 달성 하고자 할 때, 수용할 의향이 있는 위험의 수준을 의미한다. 즉, 적절한 위험성향의 도출을 위해서

는 비즈니스 목표가 고려될 필요성이 있다. 특히 파괴적인 기술들로 인하여 복잡해지고 수많은 위험들을 내재하고 있는 디지털비즈니스 환경에서는 더욱 그러하다고 할 수가 있다. 다국적 컨설팅 기업인 액센츄어(Accenture)에서는 새로운 디지털 비즈니스 환경에서는 단순히 기존의 비즈니스 목표뿐만이 아닌, 다양한 시각에서의 비즈니스 목표 고려가 필요함을 주장한다. 그리고 채택 가능한 비즈니스 목표는 비용효율성, 수익성, 업무 생산성, 민첩성 등이 해당한다고 제시하고 있다 [18].

또한 IT분야에 특화된 미디어 조사서비스를 제공하는 인터내셔널데이터그룹(International Data Group, IDG)은 디지털비즈니스 세계로 나아가는 목적으로 더 빠른 출시 기간을 뜻하는 민첩성과 충성도 강화 등을 뜻하는 수익증대, 시스템을 구축하거나 확장하는데 들어가는 비용 절감 등을 이야기하고 있다 [19].

(3) 금융회사의 평판 위험관리의 필요성

최근 2018년 4월에 발생한 삼성증권 배당 사고로 인해서 금융회사의 평판 훼손 등 무형자산 위험 관리의 중요성이 부각되고 있다. 보험연구원은 기업의 평판훼손 관련 보고서에서, 기업의 무형자산 비중이 크게 상승하면서 평판에 대한 훼손이 재무성과에 미치는 영향이 커지게 됨으로, 데이터 구축 등 위험 관리 방안이 필요하다고 분석했다. 또한 무형자산 가치는 기업 정보 유출과 기업의 내부적 요인 등에 의해 심각하게 훼손될 수 있다고 경고하였으며, 신뢰를 기반으로 하고 있는 금융회사는 평판 위험 관리에 주의를 기울일 필요가 있다고 이야기하였다 [20][21].

4. 시사점

위에서 조사한 위험관리 프레임워크들을 종합해보면, 조직은 감수하거나 하지 않을 위험의 양과 유형의 분류가 필요하며, 비즈니스 목표를 추구할 때 반드시 위험성향을 설정하고, 이 위험성향이 조직 전반에 인식 및 지속적으로 모니터링 되는 것이 중요하다고 할 수가 있다. 또한 정보보호 위험관리에서는 조직의 목표, 목적, 정책 및 이해관계자의 이해에 따라 위험성향이 달라지며 법 및 규정 측면, 운영, 기술, 재무, 사회적 및 인적 요인을 고려하는 것이 위험 수용기준을 결정함에 있어서 고려해야 할 중요한 요소이다.

위험성향은 조직이 전략 또는 비즈니스 목표를 추구할 때 기꺼이 감당할 수 있다

고 생각하는 수용 가능한 위험의 크기를 말한다. 각 위험은 비용 효율성, 민첩성, 업무 생산성, 수익성 등 업무 목표와 명확하게 연결되어 있어야 하며 위험성향을 표현하기 위해, 위험회피, 위험중립, 위험추구 형으로 등급화 된 척도를 마련되어야한다. 위험성향은 정량적이지 않아 측정하기 어려운 위험 역시 관리를 소홀히 해서는 안되며, 위험성향을 업무와 연계시키는 것이 중요하다. 전사적인 위험성향을 수립할 때 재무, 운영, 기술, 평판, 컴플라이언스, 문화적인 요소를 고려하며 특히 고객들의 신뢰를 기반으로 하는 금융회사의 경우 평판 위험을 고려하는 것이 매우 중요하다.

위험성향이 비즈니스 목표를 달성하면서 위험을 관리하는 중요하고 필수적이라는 것을 많은 사람들이 이야기하고 있지만, 위험성향에 대해 측정방법과 같은 구체적인 방향을 제시하는 연구가 부족하다. 이렇듯 조직의 전사적 위험성향에 관한 연구는 많지 않으며, 보안관련 위험성향에 관한연구는 전무한 실정이다. 이것이 위험관리의 금융회사의 보안 위험관리 전략 수립을 위한 위험성향 프레임워크를 개발하고 보안 위험성향 수준 및 유형을 가시적으로 식별할 수 있는 측정지표가 필요한 이유이다.

Ⅲ. 금융회사 보안 위험성향 프레임워크 및 측정 지표 개발

1. 보안 위험성향 프레임워크 개발

본 논문에서는 앞서 조사한 위험관리프레임워크, 위험성향 선행연구, 금융권의 위험관리 동향을 분석하여, 위험성향 수립 시에 고려해야 할 사항들을 도출 하였다.

구분	내용	비고(출처)
재무	보안 투자금액 선정 관련 제한된 예산	ISO/IEC 27005, British Library, OCC, HM TREASURY
기술	암호화, 접근통제, 네트워크 보안 등 기술적 업무 제약사항	ISO/IEC 27005, British Library, OCC, HM TREASURY
운영	시스템 생명주기에서의 보안 백업, 로그기록 및 모니터링 등 보안관리 활동의 운영	ISO/IEC 27005, British Library, OCC, HM TREASURY
문화	보안에 대한 경영진 및 이사회, 직원, 파트너들의 인식 및 문화	ISO/IEC 27005, British Library, OCC, HM TREASURY
컴플라이언스	법규 및 사내 보안정책 또는 보안인증제도	ISO/IEC 27005, British Library, OCC, HM TREASURY
평판	대중들이 인식하고 있는 조직의 보안 관련 평판	British Library, OCC, HM TREASURY

<표 1> 금융회사의 보안 위험성향 고려사항 매핑

금융회사의 보안 위험성향의 고려 사항을 도출하기 위하여, ISO/IEC 27005 정보보호 위험관리 프레임워크에서 제시한 ‘비즈니스 기준’, ‘재무’, ‘기술’, ‘운영’, ‘사회 및 인도주의적 요소’, ‘법/규제적 측면’의 6가지 위험 수용 기준(Risk acceptance criteria)을 가지고 매핑(Mapping) 하였으며, 영국재무부, 미국 통화감독청 등 위험성향 선행연구 및 금융권의 위험관리 동향을 반영하여 ‘평판’이라는 요소를 추가하였다. 금융회사의 각 보안 위험성향 고려사항은 다음과 같다.

‘재무’는 조직의 보안 투자금액 선정 시 제한된 예산과 관련한 위험고려사항을 뜻하며, ‘기술’은 보안 통제를 위한 암호화, 접근통제, 네트워크 보안 등 기술적 업무 제약사항을 말한다. ‘운영’의 경우, 보안관리 활동을 운영하기 위한 시스템 생명주기에서의 보안 백업, 로그기록 및 모니터링 관련 사항 등을 의미하며 ‘문화’의 경우, 경영진 및 이사회, 직원, 파트너들의 가지고 있는 보안에 대한 인식 및 문화가 위험성향에 크게 작용한다. ‘컴플라이언스’는 금융조직이 준수해야 할 금융관련 감독 규정 등 법규와 각 금융회사의 사내 규정 또는 보안인증제도등이 포함된다고 할 수가 있다. 마지막으로 ‘평판’에서는 보안 신기술 도입 또는 보안사고로 인하여 대중들이 인식하고 있는 금융회사의 평판을 의미 한다.

위험성향은 조직이 전략 또는 비즈니스 목표를 추구함에 있어 수용할 의향이 있는 위험의 크기를 말한다. 때문에 비즈니스 목표를 함께 고려할 필요가 있다. 비즈니스 목표는 미국의 다국적 경영 컨설팅 기업 액센츄어(Accenture)의 비즈니스 가치 모형 등 선행연구를 바탕으로 하였으며, 각 목표의 정의는 다음과 같다.

① 비용 효율성 : 시스템을 확장 또는 구축하는 데 투입되는 비용 및 그 결과로 얻어지는 효용의 측면에서 본 경제성을 의미한다.

② 수익성 : 조직이 효율적으로 관리되고 있는 정도를 나타내는 종합적 지표로 시장가치 비율, 생산성 등 다양한 형태로 나타나게 된다.

③ 업무 생산성 : 업무의 결과물과 결과물을 산출하기 위해 사용되는 인력, 시설, 자본, 시간 등의 자원 간의 비율을 의미한다.

④ 민첩성 : 새로운 비즈니스 창출 기회에 서비스와 제품의 새로운 버전을 반복적으로 빠르게 출시하거나 신속하게 적응하는 능력 등을 의미한다.

앞서 살펴 본 위험을 수용할 때 고려해야 할 6가지 요소와 비즈니스를 수행할 때의 4가지 목표를 바탕으로 도출한 위험성향 프레임워크는 아래의 그림과 같다. 즉, 해당 프레임워크는 금융권 조직에서 보다 효율적이며 효과적으로 위험성향을 도출하는데 반영해야할 요소들을 포함한다.

<그림 1> 금융권 보안 위험성향 프레임워크

2. 보안 위험성향 지표 개발

앞선 금융회사의 위험성향 프레임워크의 '재무, 기술, 운영, 문화, 컴플라이언스, 평판'의 6개 분야에 대한 보안 위험성향 수준 및 유형을 가시적으로 식별하기 위해서는 측정가능한 지표의 개발이 필요하다. 그렇기 때문에 금융권의 적합한 F-ISMS 인증기준 점검항목과 정보보호 위험관리 표준인 ISO 27005를 참고하여 세부 측정지표를 도출하였다.

구분	측정 지표	F-ISMS 점검 항목
재무적	금융 보안투자 금액을 선정할 때, 보안의 가치 대비 비용을 중요시하는 정도	2.2 역할 및 책임
	금융 보안 관련 의사결정을 할 때, 타 조직에 비해 내·외부 경제 상황에 영향을 받는 정도	관리과정 3.1 위험관리
	조직의 IT자신 및 소프트웨어를 변경할 때, IT자산 및 소프트웨어의 보안 수준 대비 변경 비용을 중요시하는 정도	11.1 운영 절차 및 변경 관리
기술적	금융회사의 암호화 정책을 수립할 때, 보안 수준의 향상 대비 업무의 편리성에 초점을 맞추는 정도	9.1 암호정책
	금융 시스템 및 DB에 접근권한을 설정할 때, 보안의 수준 대비 관리와 업무의 효율을 중시하는 정도	10.2 접근권한 관리
	금융회사의 접근통제 정책을 수립할 때, 업무의 효율, 편리, 비용을 고려하여 필수적인 접근통제 정책에 의지하는 정도	10.1 접근통제 정책
운영적	금융 시스템 생명주기에 보안을 적용할 때, 보안 수준 대비 비용, 업무의 효율, 생산성 등을 고려하는 정도	11.1 운영 절차 및 변경 관리
	금융 업무관련 정보를 백업할 때, 업무의 효율을 고려하여 필수적인 백업 외에 추가적인 백업 횟수 정도	11.6 로그관리 및 모니터링
	금융 시스템 로그기록 및 모니터링 검토 주기 설정 시에 업무 효율 및 속도를 고려하여 검토 주기를 설정하는 정도	11.6 로그관리 및 모니터링
	금융 공급자관계 보안 정책 수립 시, 관련 절차의 복잡성이나 효율성 고려하여 정책의 실행 여부 정도	3.2 외부자보안 이행
문화적	조직의 직원들이 업무를 진행할 때, 보안 관련 요소 대비 업무의 진행 속도와 효율을 중요시하는 정도	6.2 인사규정
	직원의 금융 보안교육 진행시, 업무의 생산성, 민첩성 등을 위하여 필수적인 교육만 진행하는 정도	6.2 인사규정
	인사 고과 시에, 보안관련 규정 준수 여부 또는 보안 관련 상·벌점 수여 여부의 작용 정도	6.2 인사규정

	고용 전/중/후의 보안 관련 사항을 처리할 때, 보안 대비 처리의 편리성이나 속도에 치중하는 정도	6.2 인사규정
컴플라이언스	금융 조직 내에 규정을 수립하고 검토하기 위한 위원회의 형성 및 개최 횟수 정도	2.1 조직체계
	금융 조직 내에 규정을 수립할 때, 업무의 편리성과 효율성을 고려하는 정도	1.3.2 정책시행 문서 수립
	금융 보안 인증 관련, 비용 또는 업무 효율을 고려하여 필수적인 인증 외 추가적 보안인증 활동 여부	1.3 정책의 유지 관리
평판	다른 금융회사 조직 대비 소셜 네트워크나, 뉴스기사에 영향을 받는 정도	1.2.2 대응 및 복구
	조직이 대중에게 안전하고, 신뢰가 있는 이미지를 갖고 있는 정도	12.2 대음 및 복구
	다른 금융회사 조직 대비 금융회사 조직 내에 회사 평판을 관리하기 위한 활동 여부	12.1 절차 및 체계

<표 2> 금융회사의 보안 위험성향 측정 지표

설문지의 척도는 '매우 아니다, 아니다, 보통이다, 그렇다, 매우 그렇다'에 1점부터 5점까지의 등간척도로 설정하였다. 각 설문 항목의 점수가 높을수록 보안 위험 성향은 위험 추구에 가까우며, 반대로 낮을수록 보안 위험 성향은 위험 적대에 가까움을 나타낸다. 또한 프레임워크에서 보안 위험 성향의 여섯 분야인 '재무, 기술, 운영, 문화, 컴플라이언스, 평판' 중 특정 분야에 가중치를 두지 않았기에, 각 설문 항목 점수의 단순 합산이 아닌, 각 항목별로 설문 항목 점수들의 평균을 산출하여 더한 값을 설문 결과의 값으로 하였다. 설문 결과 값은 1점이 최저점이고 5점이 최고점으로, 위험적대(1점), 위험회피(2점), 위험중립(3점), 위험감수(4점), 위험추구(5점)으로 등급화 하였다. 설문 시 결과 값은 다음과 같이 산출된다(소수점 두 번째 자리에서 반올림).

재무적	기술적	운영적	문화적	컴플라이언스	평판
(5+3+4)/3 =4	(3+4+2)/3 =3	(5+2+3+2)/4 =3	(5+2+1+2)/4 =2.5	(2+1+3)/3 =2	(4+4+5)/3 =4.3
총점: (4+3+3+2.5+2+4.3)/6 = 3.1					
결과: 위험 중립					

<표 3> 금융회사의 보안 위험성향 측정 값(예시)

Ⅳ. 전문가 검토 결과 및 활용방안

1. 전문가 검토 결과

본 연구는 위험관리 프레임워크의 이론적 고찰과 금융회사의 위험관리 동향, 위험성향의 선행 연구들을 통해, 보안 위험성향 고려 분야 6가지와 비즈니스 목표 4가지로 이루어진 금융회사의 보안 위험성향 프레임워크를 만들었다. 또한 만들어진 프레임워크를 가지고 조직의 보안 위험성향의 위치를 가시적으로 보여 줄 수 있는 20개의 측정지표를 개발하였다.

보안 위험성향에 대한 국내 연구 현황을 고려해보았을 때, 정량적인 방법으로는 깊이 있는 결과를 도출하기 어렵다고 판단하였다. 따라서 개발된 측정 지표들에 대한 중요성(materiality)과 실현가능성(feasibility) 검토를 위하여 포커스 그룹 인터뷰(FGI) 방법을 선정하였다. 포커스 그룹은 주제와 관련하여 공통된 특성을 가진 전문가들 간의 상호작용을 통해서 연구자가 제시한 연구주제에 대하여 자료를 수집하는 방식이다. 형성된 그룹 내에서 상호작용을 가지며 전문가들의 경험 및 신념을 이끌어 낼 수 있다 [22]. 포커스 그룹은 <표 4>와 같이, 업권별 금융회사의 보안업무 관련 종사자, 금융회사의 위험관리 관련 프로젝트 경험이 있는 컨설턴트, 보안 위험관리 전문가들로 구성하였으며, 참여 대상자는 모두 최소 10년 이상의 경력을 보유하였다.

	그룹 인터뷰 참여자	전문분야
1	컨설턴트1	위험관리
2	컨설턴트2	위험관리
3	은행권 보안업무 종사자	보안관리
4	증권 보안업무 종사자	보안관리
5	핀테크 관련 IT회사 보안업무 종사자	위험관리
6	금융권 위험관리 업무 종사자1	IT위험관리
7	금융권 위험관리 업무 종사자2	IT위험관리
8	일반 기업 보안업무 종사자	위험관리

<표 4> 포커스 그룹 인터뷰 참여자

본 연구에서 수행하는 포커스 그룹 인터뷰 절차는 다음과 같다. 1차 검토에서 기존 선행연구 분석 결과를 기반으로 금융회사의 보안 위험성향 프레임워크의 개발에

대한 의견 수렴 절차를 수행하고, 2차 검토에서는 측정지표 개발에 대한 검토를 진행하였다. 3차 검토에서는 설문지 작성 및 심층면접을 진행하였다. 설문지는 개발되어진 측정지표의 중요성과 실현가능성을 리커드 5점 척도를 사용하여 조사하였으며, 추가로, 개발된 측정 지표에 대한 개선사항 또는 제언에 대하여 작성하도록 하였다. 설문이 끝난 후 약 60분에 걸쳐 전문가들 간의 토론 및 의견교환을 나누는 시간을 진행하여 개발된 지표의 타당성을 검토하였다.

보안 위험성향 측정지표의 전문가 인터뷰 설문 기각/채택의 기준은 카프레라(Cabrera)의 연구를 참고하여 [23], 중요성과 실현가능성의 항목 모두 2.5 이상인 경우는 채택하고, 두 항목 중 하나의 항목만 2.5 이하인 경우에는 기각/채택 여부를 전문가 검토 및 의견 수렴 후에 결정하도록 하였다. 반면에, 중요성과 실현가능성의 항목이 모두 2.5 이하인 경우에는 기각하였다.

그룹 인터뷰를 통한 전문가 검토 결과, 20개의 보안 위험성향 측정지표에 대한 중요도는 모두 2.5 이상으로 높게 검토되었다. 그러나 측정지표의 실현가능성에 대한 검토 결과, 3개의 측정지표가 2.5 이하로 검토되었다.

첫 번째 '재무적'항목에서는 조직이 금융회사 내외부의 경제 상황에 크게 영향을 받는가를 측정하기 어렵다는 문제가 지적되었다. 이에 따라 내외부의 경제 상황 영향을 측정하기 위한 적절한 지표의 도출에 대한 필요성이 제기되었다.

두 번째 '문화적' 항목에서는 고용 전/중/후의 보안 관련 사항을 처리할 때 보안 수준 대비, 처리의 생산성이나 속도에 치중하는 정도를 측정하기 어렵다는 문제가 지적되었다. 이에 생산성이나 속도는 조직별 인식에 차이가 있기 때문에 일관된 기준의 수립보다는, 각 금융회사에 적합한 기준을 도출할 필요성이 있다.

마지막으로 '컴플라이언스'항목에서는 금융 조직 내에 규정을 수립하고 검토하기 위한 위원회의 형성 및 개최 횟수 정도를 일괄적으로 측정하기 어렵다는 문제가 지적되었다. 이에 '위원회'의 범위를 어디까지 할 것인지에 대한 구체적인 기준의 수립이 필요하다.

영역	측정지표	중요성(Materiality)	실현가능성(Feasibility)
재무	보안투자금액	3.63	3.38
	금융 내•외부 경제상황	3.25	2.38
	금융 시스템 변경비용	3.50	3.38
	평균	3.46	3.04
기술	암호화 정책	3.25	3.25
	DB 접근권한 설정	3.63	3.38
	네트워크 접근통제	4.13	3.13
	평균	3.67	3.25
운영	금융 생명주기 보안	3.13	3.38
	금융 중요 정보 백업	3.13	3.25
	로그기록 및 모니터링	4.38	3.75
	금융 공급자 관계 보안	3.88	3.00
	평균	3.63	3.34
문화	직원의 금융 보안 인식	4.00	3.13
	금융 보안교육 정도	3.75	3.13
	상벌점의 인사고과 반영	3.88	3.00
	고용 전중후 보안	3.25	2.25
	평균	3.72	2.88
컴플라이언스	위원회의 규정 검토	3.63	2.25
	금융 보안 규정의 수립	3.25	3.25
	금융 보안 인증 활동	3.63	3.13
	평균	3.55	2.88
평판	소셜네트워크, 언론 영향	4.38	3.50
	대중의 금융회사 인식	4.00	3.63
	평판 관리 활동	4.00	3.63
	평균	4.13	3.58
합계		3.68	3.16

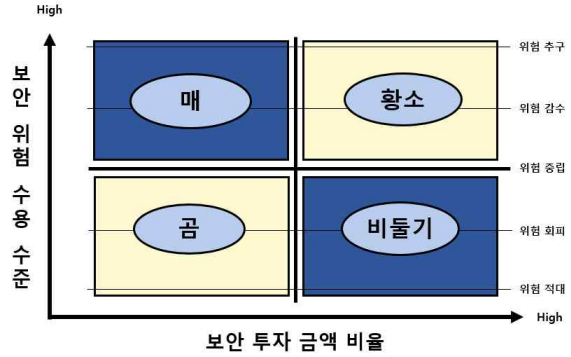
<표 5> 전문가 그룹 인터뷰 결과

또한 참여자의 보안 위험성향에 대한 추가적 제언 내용으로, 측정된 지표의 점수와 보안투자 금액을 고려하여 보안전략 수립에 있어서의 활용방안 제시가 필요하다는 의견이 다수였다. 그렇기 때문에 측정된 지표를 활용하여 보안 전략을 수립할 수 있는 보안 위험성향 매트릭스를 추가로 제시하였다.

2. 활용방안

본 논문에서는 위와 같은 위험 성향 수준 도출의 활용 방안으로 다음의 매트릭스를 제시한다. BCG매트릭스는 기업의 전략적 비즈니스 분석모델로서 사업조직 내의 효율적인 자원배분 및 기술개발 등의 문제를 해결하기 위하여 사용되어 왔다. 또한 자원의 투입에 대한 산출을 측정하고 기업이 직면한 상황을 인식하게 하여 최선의

방안을 도출할 수 있도록 도와주는 분석도구이다 [24]. 본 연구에서는 이를 보안 위험 성향에 적용하여, 다음의 <그림2>를 도출하였다.



<그림 2> 금융회사의 보안 위험 성향 매트릭스

<그림 2>의 세로축인 '보안 위험 수용 수준'은 설문조사 결과 도출된 조직의 보안 위험 수용 수준을 의미하며, 가로축인 '보안 투자 금액 비율'은 조직의 규모 대비 보안 투자 금액의 비율을 의미한다.

금융시장에서는 '비둘기', '매', '곰', '황소' 등 동물들에 비유하여, 시장 상황이나 투자자의 투자 성향을 설명하기도 한다. 넓은 의미의 '비둘기'는 성향이 공격적이지 않고, 온건한 방법을 취하려는 사람을 뜻하는 말이며, '매'는 사납고 공격적인 매의 습성처럼 강경하게 일을 처리하는 보수강경파를 말할 때 매파라고 말한다. 또한 '곰'은 증권시장에서 곰이 아래로 내려찍는 싸움 자세를 취하는데 빗대어 하락장을 베어 마켓(Bear market)이라 부르며, 이에 비해 황소는 뿔을 위로 치받는 싸움 자세를 취하여 상승장을 불 마켓(Bull market)이라 부른다 [25]. 이를 비유한 보안 위험성향 영역에 대입하여 보면, 각 영역에 속하는 각 조직들은 다음의 보안 관리 전략이 요구될 수 있다.

'비둘기'의 영역에 포함되는 조직은 비록 보안투자금액 비율이 높은 편이나, 조직의 보안 위험 수용 수준이 낮다. 따라서 '비둘기'의 영역에 포함되는 조직은 보안투자에 다소 많은 금액을 사용 하지만, 조직의 보안 관리 전략 수정이 요구되지 않을 수 있다.

'매'의 영역에 포함되는 조직은 비록 보안투자금액 비율은 낮으나, 위험 수용

수준이 높다. 따라서 '매'의 영역에 포함되는 조직은 다소 많은 위험을 감수하긴 하나, 조직의 보안 관리 전략 수정이 요구되지 않을 수 있다.

'곰'의 영역에 포함되는 조직은 보안투자 금액이 낮은 편임에도 불구하고, 낮은 위험 수용 수준을 가지고 있다. 따라서 '곰'의 영역에 포함되는 조직은 조직의 위험성향을 수정하거나, 보안 투자 금액 비율을 더욱 높이도록 조직의 보안 관리 전략 수정이 요구될 수 있다.

'황소'의 영역에 포함되는 조직은 보안위험 수용 수준이 낮음에도 불구하고, 많은 보안 투자 금액 비율을 가지고 있다. 따라서 '황소'의 영역에 포함되는 조직은 조직의 보안위험성향에 적합한 효율적 보안투자를 위해, 보안 투자 금액 비율을 다소 줄이도록 조직의 보안 관리 전략 수정이 요구될 수 있다.

V. 결 론

본 연구는 위험관리 프레임워크와 관련 위험성향 선행연구 분석 및 금융회사의 위험관리 동향을 통해서 금융회사의 보안 위험성향 프레임워크를 개발하고 20개의 보안 위험성향 수준 및 유형을 가시적으로 식별할 수 있는 측정지표를 개발 하였다. 기존의 위험성향에 대한 연구는 개인의 투자성향에 대한 지표로서의 역할에 대해 많은 논의가 이루어졌었으며, 조직의 전사적인 위험관리 활동으로서의 위험성향에 대한 연구도 측정방법이나 측정 고려요소에 대한 구체적인 방안이 제시되지 못했다. 더군다나 보안에 대한 위험성향의 연구는 전무한 실정이다. 금융회사는 금융회사가 가진 특수성 때문에 위험성향을 측정하고 관련 보안 전략을 수립하는 것이 필수적이라고 할 수가 있다. 개발된 금융회사의 보안 위험성향 지표(Indicators of Security Risk Appetite)는 이러한 면에서 중요한 의미를 지닐 것으로 사료된다.

본 연구의 한계점은 다음과 같다. 첫 번째, 본 연구는 국내 금융회사의 보안 위험성향에 관한 연구가 부족한 실정임에 따라, 포커스 그룹 인터뷰(FGI)로 타당성을 측정하여 일반화에 대한 어려움이 존재한다. 따라서 향후 다변량 분석, 요인분석 등 정량적인 연구가 필요하다. 둘째, 개발되어진 지표는 대부분이 정성적 지표이다. 그렇기 때문에 정량적인 데이터 수집 유형과 방법이 필요할 것으로 보인다. 이에 따라 향후, 정성적 지표 데이터를 객관화하여 측정할 수 있는 지표로 변환할 필요성이 있다. 셋째는 측정된 위험성향에 대한 구체적인 보안전략이 제시되지 않았다는 점이다. 그렇기 때문에, 측정된 위험성향을 가지고 전략을 수립하는 보안 전략 수립

에 대한 연구가 필요할 것으로 보인다.

효과적 건강관리를 위해 자신의 체질을 잘 알아야 하듯이, 보안 위험관리를 위해서는 우선적으로 위험성향에 대한 파악이 매우 중요하다. 이 연구의 결과는 보안관리 활동의 근본이지만 아직 제대로 수행하지 못하고 있는 위험관리 활동의 첫 단추를 꿰는 중요한 역할을 수행할 것으로 기대한다.

참고문헌

[1] 금융위원회·금융감독원, 금융IT부문 자율보안체계 확립 방안 [Internet], Available: https://www.fsc.go.kr/downManager?bbsid=BBS0030&no=97272, 2018.7.5.

[2] 중앙일보, 금감원, 금융회사 IT리스크 관리 '자율평가 가이드라인' 마련 [Internet], Available: http://news.joins.com/article/22427541, 2018.7.5.

[3] "Risk management 31000", ISO, Switzerland, ISBN 978-92-67-10784-4, 2018.

[4] "COSO ERM Integrating with Strategy and Performance", COSO, California, P254469-01 0516, 2017.

[5] "ISO/IEC 27005:2014", ISO, Geneva, 2014.

[6] March, J. G., & Z. Shpira, "Managerial Perspectives on risk and risk taking", Management Science, vol 33, no 11, pp. 1404-1418, Nov. 1987.

[7] Irwin. Jr.CHARLES E, "Adolescence and Risk Taking: How Are They Related?" In Nancy J.Bell and Robert W.Bell, Adolescent Risk Taking, pp. 7-28, Newbury Park, CA: Sage, 1993.

[8] Grable, John E, "Financial risk tolerance and additional factors that affect risk taking in everyday money matters", Journal of Business & Psychology, vol 14, no 4, pp. 625-630, Jun. 2000.

[9] 정순희, 신민경, "재무위험수용성향과 위험자산보유율 관련 변수에 관한 연구", Financial Planning Review, vol 4, no 4, pp. 1-20, Nov. 2011.

[10] Mukul Pareek, "What Is Your Risk Appetite?", ISACA, Illinois, vol 4, 2013.

[11] Richard Barfield, "Risk appetite - How hungry are you?", PwC, London, 2016.

[12] Rick Porter, Peter Matruglio, Tim Oldham외 11명, "Risk appetite frameworks How to spot the genuine article", Deloitte, New York, 2014.

[13] 조창훈, 배재권, "금융IT 컴플라이언스 시스템 구축요소에 관한 탐색적 연구: 컴플라이언스 전문가 심층인터뷰를 중심으로", Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol 7, no 6, pp. 785-795, June. 2017.

[14] "Enterprise risk appetite statement", OCC, Washington, 2016.

[15] "Setting and communicating your risk appetite", HM Treasury, London, ISBN-13 978-1-84532-195-6, 2006.

[16] “2018년 금융감독원 업무계획”, 금융감독원, 서울특별시, 2018.

[17] “23 NYCRR 500”, New York State Department of financial services, New York, 2017.

[18] “Growth Strategies for a Digital World”, Accenture, Dublin, 2014.

[19] “디지털 트랜스포메이션 가이드”,IDG, Boston, 2017.

[20] 한겨레, 삼성증권 사고 계기 “평판 훼손 리스크 관리 시급” [Internet], Available: http://www.hani.co.kr/arti/economy/finance/841535.html#csidx5b208b2cd353ab285f7353d71b1e91c, 2018.7.7.

[21] 정원석, “기업평판위험관리의 중요성”, 보험연구원, 서울특별시, 2017.

[22] David L. Morgan, “Foucs groups as qualitative research”,군자출판사, pp.88, 2007.

[23] Cabrera, D., Mandel, J. T., Andras, J. P. “What is the crisis? efining and prioritizing the world’s most pressing problems”. Front Ecol Environ, 6(9), 469-475. 2008.

[24] 전성해, 방상성, 신영근외 2명, “자기조직화 지도와 매트릭스분석을 이용한 특허분석시스템의 공백기술 예측”, 한국콘텐츠학회논문지, vol 10, no 2, pp. 462-480, Feb. 2010.

[25] 기획재정부, “최신 시사경제용어 사전”, 온이퍼브, 2017.

개인정보 활용을 위한 블록체인 기반의 개인정보 자기 통제 시스템

이경모* 성기정**

*부경대학교 정보보호학 협동과정

**부경대학교 IT융합응용공학과

요 약

최근 사물 인터넷(IoT)의 확산으로 정보의 수집량이 방대해지고 인공지능(AI)과 결합한 빅데이터 산업이 성장함에 따라 수집된 정보에 포함된 개인정보의 활용 기회가 증가하고 있지만 개인정보 처리 시 사전 동의 절차에 따른 제약사항 및 높은 설비 투자비용 때문에 개인정보가 포함한 데이터의 활용이 확대되지 못하고 있다. 또한 기존 서비스 사업자(개인정보처리자) 중심의 개인정보 동의 방식은 실질적인 정보주체의 개인정보 자기결정권을 보장하지 못하며 이에 현대 환경을 고려한 개인정보주체 중심의 개인정보 처리 동의 모델이 필요하다. 따라서 본 논문에서는 개인정보 처리 동의 절차를 블록체인 스마트 컨트랙트를 기반으로 구성한 개인정보 자기 통제 시스템을 제안하며 이를 통해 개인정보주체의 실질적 자기결정권을 보장하고 개인정보 제공에 대한 수익 모델을 제시한다. 또한 제안 시스템 구성을 위한 보안 요구사항 및 시스템의 장점을 제시한다.

키워드

개인정보, 자기정보결정권, 블록체인, ID관리, 스마트 컨트랙트

목 차(14 포인트)

Ⅰ. 개인정보

1. 개인정보

(1) 개인정보의 정의 및 새로운 개인정보 처리 방식의 필요성

최근 사물인터넷(IoT) 및 소셜 네트워크 등에서 수집된 다양한 정보들은 빅데이터(Big Data) 처리 기술 및 인공지능(AI)의 도움으로 소비자 타겟 마케팅 등에 활용되며 사업의 핵심 자산으로써 가치를 창출한다. 하지만 수집된 정보 안에는 다양한 형태의 개인정보가 포함되며 이러한 개인정보에 대한 처리를 올바르게 수행하는 것은 향후 해결해야할 과제로 남아 있다. 개인정보는 각국마다 약간의 차이는 있으나 국내에서는 “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 것으로 정의한다[1]. 한편 정보 수집 채널이 다양화됨에 따라 개인정보 처리와 관련된 몇 가지 고려사항이 발생하였다. 첫 번째 사항은 많은 국가에서 개인정보의 처리 시 사전에 개인정보주체의 동의를 얻어야하지만 수집 채널의 다양화 및 상호 정보가 연계되는 현대의 환경에서는 수집된 정보에 포함된 개인정보 별 개인정보주체의 동의를 얻는 것이 매우 어렵다는 점이다.

이에 최근 별도로 추가 동의 없이 개인정보를 비식별화하여 처리하는 기술이 빅데이터 및 AI 산업과 관련하여 주목을 받고 있으나 역시 정보의 연계과정에서 식별가능성을 완전히 없애는 것은 현실적으로 어려우며 비식별화된 개인정보에 대해서도 개인정보 주체에게 주기적 이용 통지가 필요하다.

또 다른 고려사항은 현재 서비스 사업자(개인정보처리자) 중심의 동의 방법(홈페이지의 회원가입 혹은 별도의 양식 작성)을 통한 개인정보 처리 동의 방식으로는 향후 다양한 정보 수집원에서 수집되는 개인정보의 처리 동의를 받는데 한계가 있다는 점이다.

결론적으로 현대 환경에서는 서비스 사업자 위주의 개인정보 처리 동의 방법이 아닌 개인정보주체가 개인정보가 포함된 데이터의 소유권을 가지고 이를 개인정보처리자에게 제공해주는 개인정보주체 중심의 방법이 요구되며 주체에게 개인정보 및 비식별화된 정보의 이용내역을 주기적으로 알릴 수 있는 별도의 통지 채널 역시 요구된다. 또한 이러한 개인정보주체 중심의 시스템에서는 현재 대규모 서비스 사업자(개인정보처리자)가 제공하는 수준과 유사한 높은 수준의 안전성을 갖추면서도 개인정보주체가 구축 및 운영할 수 있도록 비용을 고려하여 설계되어야 한다.

2. 자기결정권

(1) 자기결정권과 개인정보주체의 이익

자기정보관리 통제권 혹은 개인정보자기결정권이란 자신에 관한 정보를 보호받기 위하여 자신에 관한 정보를 자율적으로 결정하고 관리할 수 있는 권리를 의미하며 근거는 헌법 제 10조 1문의 인간의 존엄과 가치 및 행복추구권과 제 17조 사생활의 비밀과 자유를 이념적 기초로 하는 명시되지는 않은 독자적인 기본권이다.

최근 우리나라의 경우 2018년 3월 대통령 개헌에서 국민의 기본권 관련 조항에서 정보의 유통과 관련된 알권리 및 자기정보통제권을 정보 기본권으로 신설하였다. 이는 개인정보를 개인정보처리자만의 자산이 아닌 개인정보주체의 자산으로 보아 개인정보주체 스스로 수명관리 및 삭제와 이용에 관해 통제할 수 있는 근거를 마련한 것이었으며 최근 2018년 5월 개인정보보호규정(General Data protection Regulation, GDPR)이 발효되어 국내외적으로 자기결정권에 관한 중요성이 커졌다.

하지만 개인정보의 활용을 통해 기업이 얻는 실질적 이익에 비해 개인정보주체가 얻는 이익은 개인정보처리자가 제공하는 서비스의 이용에 국한되는 경우가 많으며 서비스와 직접적 연관 없이 함께 수집되어 처리되는 개인정보가 포함된 데이터는 개인정보주체에게 이익을 줄 수 없다. 따라서 향후 개인정보 처리 동의 방식은 서비스 중심이 아닌 개인정보주체와 개인정보가 중심이 되어야 하며 각 개인정보별 제공량과 현황 등을 파악하여 이를 기반으로 개인정보 주체에게 실질적 이익을 돌려주는 것이 개인정보주체의 자기결정권 보장을 위한 필수적 요소일 것이다.

Ⅱ. 블록체인

1. 블록체인 및 블록체인 응용

(1) 블록체인 기반의 신원관리

블록체인 기술은 나카모토 사토시에 의해 2009년 제안되었으며 암호학적 기술과 합의 메커니즘 등을 통해 상호 신뢰하지 않는 환경에서 신뢰된 하나의 결과를 만들어내는 기술이다. 최초 비트코인이라는 전자적 화폐의 교환 목적으로 개발되었으나 튜링 불완전성 때문에 활용할 수 있는 분산 어플리케이션이 제한되었다. 이후 등장한 수많은 블록체인들은 스마트 컨트랙트로 불리는 블록체인에서 실행되는 코드 및 스마트 컨트랙트의 실행환경을 지원하여 다양한 분산 어플리케이션 개발 플랫폼으로써 사용되었다[2].

블록체인의 특징으로는 실제 현실세계의 신원과 연관되지 않는 가명주소를 사용하며 가명주소를 하나의 신원으로 보고 이와 연결된 정보를 스마트 컨트랙트를 통해 처리 및 블록체인에 저장하는 블록체인 기반의 신원관리 모델이 최근 연구되고 있다[3-4]. 또한 블록체인 기반의 신원관리 모델의 확장으로 블록체인 기반의 접근권한 관리 시스템이 제안되었다[5-6].

결론적으로 본 논문에서는 기존에 제안되었던 블록체인 기반의 접근권한 관리 시스템을 확장하여 블록체인의 가명주소를 실제 개인정보주체의 신원과 조건부로 연결시켜 개인정보주체가 직접 자신의 개인정보에 대한 접근권한을 스마트 컨트랙트 기반으로 부여 및 관리하는 시스템을 제안한다. 이를 통해 개인정보주체가 직접적인 개인정보자기결정권을 가지며 무결한 접근권한관리 및 트랜잭션 기반으로 블록체인에 기록되는 이용내역 등에 기반하여 실질적인 개인정보주체의 이익을 주장할 수 있다.

2. 보안 요구사항

(1) 시스템 보안 요구사항

1) 허위 신원에 대한 안전성

블록체인의 가명 주소 생성 시 비용없이 주소 생성이 가능하여 의도적인 공격자는 임의의 블록체인 주소를 생성하여 악의적인 행동을 할 수 있어 이에

대한 실제 현실세계의 신원에 대한 검증이 요구된다[7].

2) 다수에 의한 안전성

별도의 블록체인을 구성하거나 참여자 수가 적은경우 PoW(해시기반의 작업 증명)를 사용하는 공개형 블록체인은 51% 공격[8]에 취약할 수 있어 이에 대해 적절한 참여자만을 네트워크에 참여시키는 통제 방안이 요구된다.

3) 기밀성 문제

개인정보 등 민감정보에 대한 기밀성은 블록체인의 공개 검증성 및 투명성과 상충되며 이를 고려하여 시스템으 설계하여야 한다.

4) 조건부 익명성 & 책임 추적성 보장

일반적인 상황에서는 개인에 대한 추적이 불가능하지만 법적 책임 추적성 확보를 위해 특정 상황에서는 개인에 대한 추적이 가능해야 하며 블록체인 주소를 특정 조건하에 개인과 연관시킬 수 있어야 한다.

Ⅲ. 시스템 모델

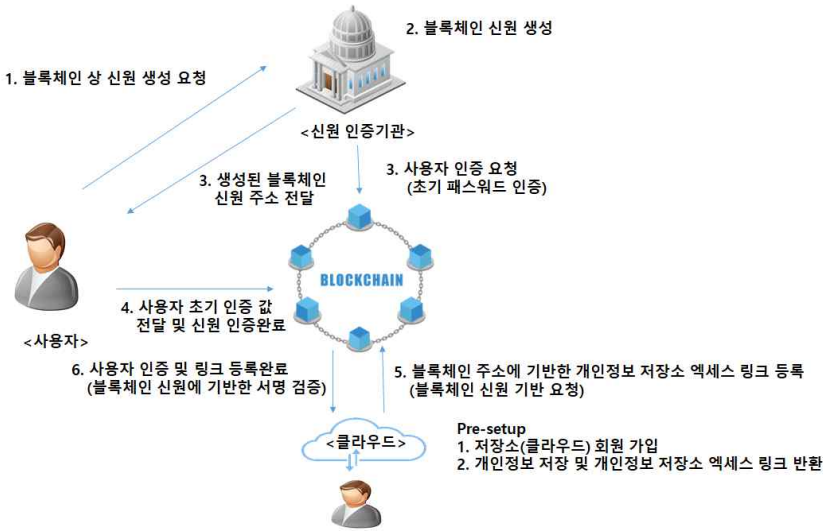
1. 시스템 모델 및 장점

(1) 시스템 모델

1) 개인정보주체와 블록체인 가명주소의 연결 및 개인정보 저장소 설정

가. 개인정보주체와 블록체인 가명주소의 연결

<그림 1>과 같이 사용자는 최초 네트워크 참여를 위해신원 인증기관에게 요청하면 신원 인증기관은 임의의 블록체인 주소를 생성하는 트랜잭션을 만들고 신원 인증기관을 송신자로 하여 개인정보주체(사용자)가 사용할 ID를 블록체인에 공표한다. 이후 사용자는 이메일/휴대폰 인증 등을 통해 전달받은 OTP의 값을 컨트랙트를 통해 인증하면 생성한 ID에 대한 소유권을 신원 인증기관으로부터 양도받아 실제 현실세계의 신원과 블록체인 가명주소가 연결된다. 이러한 신원 인증기관의 참여를 통해 허위신원의 참여를 막는다.



<그림 1>

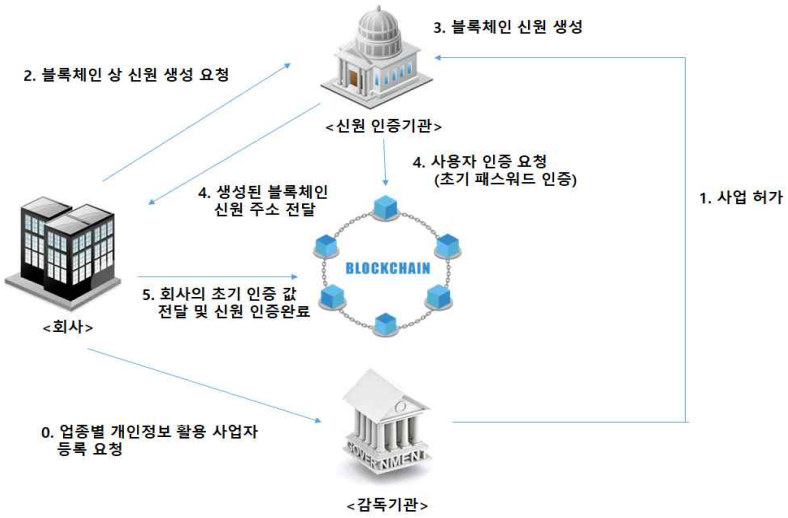
나. 개인정보 저장소 설정

사용자는 개인정보 제공을 위한 사전 단계로써 개별적으로 사용하는 저장소(클라우드와 같은 안전한 저장소)에 회원가입 등의 인증절차를 거쳐 개인정보를 암호화된 형태로 저장하며 개인정보 저장소는 저장소에 접근 할 수 있는 권한을 스마트 컨트랙트와 연동하여 검증되도록 한다. 이후 “가” 과정에서 생성된 사용자의 블록체인 주소를 기반으로 개인정보 저장소의 엑세스 링크를 블록체인에 등록하며 개인정보 저장소의 링크를 얻기 위해서는 개인정보주체가 부여한 접근 권한이 있는 개인정보처리자(회사)만이 해당 링크에 접근이 가능하며 추가적 안전성을 위해 링크에 접근 시 추가 인증을 요구할 수 있다.

2) 개인정보 처리자와 블록체인 가명주소의 연결

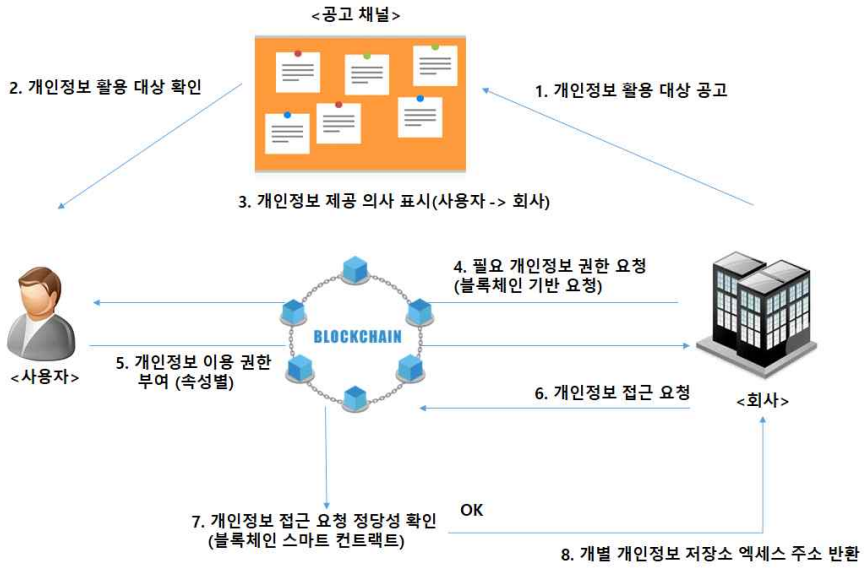
가. 개인정보 처리자와 블록체인 가명주소의 연결

개인정보를 처리하려는 기업은 별도 감독기관의 허가와 함께 신원 인증절차를 개인정보주체와 동일한 방법으로 수행하며 감독기관은 신원인증 기관과 연계하여 블록체인 신원에 대해 통제하는 신뢰기관 및 감독기관의 역할을 수행한다.



<그림 2>

3) 블록체인 기반의 개인정보 처리 요청 - 동의 모델



<그림 3>

가. 개인정보 처리 요청 공고 및 확인

안전한 공고 채널을 수립하여 이를 통해 개인정보처리자와 개인정보주체 간 개인정보 처리 요구에 대한 의사를 표시 및 승낙하며 이러한 공고채널의 링크 혹은 공고정보(이용약관 등 정보)는 해시화된 형태로 <그림3>의 4

단계의 트랜잭션에 포함될 수 있다.

나. 개인정보 권한 요청 단계

개인정보 권한의 요청단계로써 <그림3>의 1 - 3 단계에서 사용자는 자신이 개인정보 처리자의 요청 조건에 맞으면 자발적으로 블록체인 주소만을 공개하여 이를 이용하여 기업이 개인정보 제공 요청을 할 수 있도록 하며 (4 단계) 이후 5 단계에서 사용자는 자신의 결정에 따라 회사의 블록체인 주소에 대해 접근권한을 부여하며 이는 스마트 컨트랙트를 통해 처리된다. 이후 4단계에서 포함된 공고정보와 요청된 사항이 다를 경우 이는 사용자의 입장에서 정보를 제공하지 않을 수 있으며 회사의 입장에서도 동일하게 사용자의 부정행위를 블록체인을 통해 공개 검증 가능하다.

다. 개인정보 접근단계

승인된 권한을 통해 개인정보 처리자는 스마트 컨트랙트에 요청하며 스마트 컨트랙트는 송신자의 서명 검증과 개인정보 처리 권한 검증을 거친 뒤 신뢰된 저장소의 링크를 반환하며 신뢰된 저장소와 별도채널을 구성하여 개인정보의 처리를 수행할 수 있다.

(2) 장점

제안 시스템에서는 사용자의 입장에서 접근성이 높은 클라우드 사업자 등을 신뢰된 개인정보 저장소로 설정하며 접근권한 관리와 이용내역 등 무결하게 보호되어야 하는 기록들은 블록체인을 통해 구성하였다. 이러한 시스템 구성 시 다음과 같은 장점 및 기대효과가 있다.

1) 개인정보를 이용한 산업의 활성화

충분한 인프라 없이 단기간 개인정보를 처리하여야 하는 기업의 경우 개인정보의 유지 및 보관을 위한 높은 비용 대신 블록체인 기반으로 개인정보 처리 동의 즉 권한을 부여 받아 안전한 개인정보 저장소와 통신하여 소규모의 개인정보 처리를 수행할 수 있으며 이를 통해 개인정보를 활용한 산업이 활성화 될 수 있다.

2) 새로운 사업 모델의 파생

제안 시스템을 적용 시 다음과 같은 새로운 사업 모델이 파생 될 수 있다.

가. 개인정보의 안전한 유지 및 보관을 위한 개인정보 저장소 관리 사업

나. 개인정보 저장소와 사용자의 개인정보 이용 동의 및 개인정보 동의를 관리를 해주는 사업

다. 개인 대 개인 간 개인정보 처리 동의 중개 사업

라. 개인정보가 포함된 데이터의 1차 처리 및 개인정보 저장소에 집적하는 사업

3) 사회적 투명성

참여하는 감독 기관 및 개인정보 관련 중재자(개인정보 분쟁 조정위원회 등)의 경우 투명하게 각 기업 혹은 개인이 처리한 개인정보에 대한 이용 내역을 블록체인을 통해 확인하여 부정행위 및 분쟁을 처리할 수 있으며 개인정보 관련 사고 시 개인정보 처리자 책임주의 원칙의 관점에서 개인정보처리자의 신원이 추적되고 관리될 수 있기 때문에 사회적 투명성이 증가한다.

4) 개인정보주체의 권익

해당 시스템을 적용 시 개인정보 주체는 개인정보 처리 제공에 대한 선택권을 가질 수 있으며 트랜잭션 기반의 처리 동의를 통해 수치적으로 환산 가능하므로 이를 기반으로 정보주체의 권익을 요구할 수 있다.

(3) 사용한 검증 기술

제안시스템에서는 블록체인 주소와 실제 개인정보주체의 신원을 연결시킬 수 있는 방법과 블록체인 송신자 검증 로직을 통해 사용자 인증을 제공하며 다음 두 가지 기술적인 부분의 사항을 제안한다.

1) 블록체인 주소와 현실세계의 신원과 연결 기술

일반적으로 블록체인의 경우 가명의 주소(블록체인 주소)를 사용하여 정보주체는 블록체인에서 실제신원과 연결성을 갖지 않지만 제안 시스템에서는 다음의 절차를 통해 상호 연결하며 이는 신원 인증기관만이 실제신원과의 연결성을 알 수 있다.

가. 초기 패스워드의 설정(신원 인증기관)

나. 신원 인증 (OTP 전달)

다. 초기 패스워드 및 송신자 검증 후 ID와 실제 신원의 연결

2) 송신자 검증에 기반한 사용자 인증

기존 환경과 달리 블록체인 환경에서는 메시지 송신자에 대한 서명 검증이 가능하여 사용자가 소유한 개인키를 기반으로 생성된 서명만으로 패스워드의 역할을 대체할 수 있으며 이를 통해 사용자의 편리성을 확보하면서도 위조 불가능한 서명을 통해 안전한 방식으로 사용자를 인증한다.

2. 구현

(1) 신원 인증기관의 설정

```
address owner;

constructor() public {
        owner = msg.sender;
}

modifier onlyOnwer() {
        require(owner == msg.sender);
        _;
}
```

- 사용하는 블록체인 모델은 컨소시엄 블록체인으로써 최초 컨트랙트 배포자는 신원 인증기관이 되며 신원 인증기관의 블록체인 주소를 화이트 리스트로 설정하여 이를 트랜잭션 검증 조건에 추가하면 허위 신원 생성을 방지할 수 있다.
- 수식자 onlyOwner를 통해 신원 인증기관만 일부 기능에 접근할 수 있도록 하여 최초 신원 생성과 OTP의 생성을 수행하도록 하였음.

(2) 블록체인 주소와 개인정보주체 간 연결

```
struct userInfo {
        string id;
        uint blockNumber;
        bytes32 otp;
}

mapping(address => userInfo) user;
mapping(string => bool) duplicate;

function join(string _id) public {
        require(!duplicate[_id]);
        user[msg.sender].id = _id;
        user[msg.sender].blockNumber = block.number;
        duplicate[_id] = true;
}
```

- 개인정보 주체(사용자)는 신원 등록 요청 시 아이디(ID)만을 입력하고 (4) 과정의 OTP 생성을 위한 블록의 높이 등을 변수로 저장하며 매핑 변수인 duplicate을 통해 아이디 중복 검사를 구현하였음.

(3) 사용자(개인정보주체) 인증

```
uint private index;

mapping(string => address) subOwner;

function certificate(uint _otp) public {
        require(user[msg.sender].otp == keccak256(_otp);
        subOwner[user[msg.sender].id] = msg.sender;
        index = index +  block.timestamp % 2 +  1;
        delete user[msg.sender].otp;
}
```

- 사용자로부터 받은 OTP number을 해시화하여 비교하며 인증받은 사용자의 주소를 매핑 subOwner을 이용해 저장함.
- 양의 정수 index는 1 또는 2의 값을 증가시켜 OTP 생성시의 고유성을 확보하였음.
- 향후 OTP의 재사용 등을 고려하여 사용자와 매핑된 해시화된 OTP number을 삭제하였음.

(4) OTP 생성

```
function createOTP(address _user) onlyOwner pulic {
        uint _nextBlock = user[_user].block +  1;
        if(block.number <= _nextBlock) waiting about several seconds
        bytes32 _blockHash = blockhash(_nextBlock);
        bytes32 _seed = keccak256(_blockHash, _user, index_);
        user[_user].otp = keccak256(uint(_seed) % 900000 +  100000);
        securely transfer OTP number to user's e-mail
}
```

- 미래의 블록 해시 값을 현 시점에서 알 수 없기 때문에 이러한 예측 곤란성을 이용하여 OTP를 구현하였음.

(5) 개인정보 처리자의 요청

```
struct state {
        mapping(uint => bool) agreement;
}

struct info {
        mapping(address => state) name;
        mapping(address => state) phone;
        mapping(address => state) email;
        mapping(address => state) addr;
}

struct company {
        mapping(string => userInfoQuery) userList;
}

struct userInfoQuery {
        string id;
        mapping(uint => bool) name;
        mapping(uint => bool) phone;
        mapping(uint => bool) email;
        mapping(uint => bool) addr;
}

mapping(string => info) access;
mapping(address => company) query;

function requestName(string _id, uint _flag) public {
        if the user agrees {
                access[_id].name[msg.sender].agreement[_flag] = true;
                query[msg.sender].userList[_id].id = _id;
                query[msg.sender].userList[_id].name[_flag] = true;
        }
}

function getName(string _id, uint _flag) public view returns (bool) {
        return query[msg.sender].userList[_id].name[_flag];
}
```

- 각 개인정보처리자(회사)는 개인 정보별로 동의 요청 및 조회가 가능 하도록 구현하였음.

Ⅳ. 결론

본 논문에서는 블록체인 기반의 개인정보 처리 동의 시스템을 제안하였다. 시스템에서는 블록체인 기반의 개인정보 처리 동의 시스템과 집적된 개인정보 저장소의 개념 및 공고채널을 통해 개인정보 처리 동의의 새로운 방향을 제시하였으며 이를 통해 개인정보를 이용한 사업 분야의 확대 및 소규모 개인정보처리자의 개인정보처리 비용 부담을 완화할 수 있다. 또한 개인정보 주체에게 실질적인 개인정보 제공에 관한 권한을 부여하여 개인정보 주체의 권익 주장을 보장할 수 있다.

참고문헌

[1] 개인정보 보호법, [시행 2017.10.19.] [법률 제14839호, 2017.7.26., 타법개정]

[2] Buterin, Vitalik. “Ethereum white paper, 2014.“ [Internet], Available https://github.com/ethereum/wiki/wiki/White-Paper (2013).

[3] Tobin, Andrew, and Drummond Reed. “The Inevitable Rise of Self-Sovereign Identity.“ The Sovrin Foundation (2016).

[4] Baars, D. S. “Towards self-sovereign identity using blockchain technology” .MS thesis. University of Twente (2016).

[5] Karafiloski, Elena, and Anastas Mishev. “Blockchain solutions for big data challenges: A literature review.“ Smart Technologies, IEEE EUROCON 2017-17th International Conference on. IEEE, (2017).

[6] Zyskind, Guy, and Oz Nathan. “Decentralizing privacy: Using blockchain to protect personal data.“ Security and Privacy Workshops (SPW), 2015 IEEE. IEEE, (2015).

[7] Newsome, James, et al. “The sybil attack in sensor networks: analysis & defenses.“ Proceedings of the 3rd international symposium on Information processing in sensor networks. ACM, (2004).

[8] Ali, Muneeb, et al. “Blockstack: A Global Naming and Storage System Secured by Blockchains.“ USENIX Annual Technical Conference. (2016).