이학석사 학위논문

정부기관 간 민감정보 노출 방지를 위한 동형암호 도입방안에 대한 연구

2021년 2월

서울대학교 융합과학기술대학원
수리정보과학과 (디지털포렌식학 전공)
이 현 규

정부기관 간 민감정보 노출방지를 위한 동형암호 도입방안에 대한 연구

지도교수 천 정 희

이 논문을 석사 학위논문으로 제출함
2020년 12월

서울대학교 융합과학기술대학원
수리정보과학과 디지털포렌식학 전공
이 현 규

이현규의 석사 학위논문을 인준함
2021년 1월

위 원 장 국 웅 (인)

부위원장 천 정 희 (인)

위 원 박 상 준 (인)

국문초록

우리나라 정부기관에서는 은행 등 금융기관과 금융정보분석원을 통해 각 기관 고유 업무에 필요한 금융거래정보를 확보하고 있다. 국세청, 관세청, 검찰청, 경찰청과 같은 다양한 법집행기관이 각 기관 고유 업무에 활용하기 위해서 금융정보분석원으로부터 연간 수만 건의 금융거래 정보를 제공받고 있는 실정이다.

금융정보분석원은 은행과 증권사와 같은 금융사로부터 자금세탁 관련 혐의정보를 수집, 분석하여 불법거래, 자금세탁행위와 관련된다고 판단되는 금융거래 자료를 법집행기관에 제공하는 업무를 주로 하는 기관이다. 개인과 회사의 민감한 금융거래내역을 연간 수십만 건 이상 보고 받고 있으며, 법집행기관에서 특정인에 대한 금융정보를 요청하면 법적 요건 검토 후 해당 기관에 특정인의 금융거래정보를 회신하여 주고 있다.

본 논문은 이 과정에서 정부기관의 민감한 비밀정보가 필연적으로 외부에 노출될 수 밖에 없다는 점을 문제점으로 인식하고, 이를 동형암호 기술을 사용하여 효과적으로 보완할 수 있는 방안을 논해보았다. 정부기관에서 특정인의 금융거래정보를 요청할 때, 정부기관 고유 업무 대상자(세무조사 대상자, 수사 대상자, 체납자 등)들의 인적사항을 명시하여 금융정보분석원으로 보내야만 한다. 이는 정부기관 내에서도 절대 공개해서는 안되는 극히 민감한 개인정보에 해당하지만, 금융거래정보를 확보하여 활용하기 위해서 부득이하게 타 정부기관인 금융정보분석원에 정보를 노출시킬 수 밖에 없는 것이다.

본 논문은 이 문제점을 동형암호 기술을 이용하여 해결할 수 있을 것이라고 보았다. 민감정보 노출의 가장 핵심 원인은 금융정보분석원이 보유한 금융정보 데이터베이스 중에서 특정인의 금융정보를 검색하여 추출하기 위해서는 반드시 평문화 상태로 작업이 진행되

어야 한다는 점이다. 현재 상용화 되어있는 암호기술로는 암호화 상태로 연산이 이루어 질 수 없기 때문이다. 최근 연구가 활발히 이루어지고 있는 동형암호의 가장 큰 특징은 암호화 된 상태로 컴퓨터가 할 수 있는 모든 연산이 가능하다는 점이며, 이를 활용하면 민감정보 노출 없이 각 기관 간 정보협조를 원활히 할 수 있을 것으로 기대된다. 법집행기관에서 동형암호로 암호화 된 특정인의 명세를 전송하면 금융정보분석원에서는 이를 암호화 상태로 데이터베이스에서 검색 및 추출하는 방식이다.

본 논문에서는 위와 같이 동형암호를 활용하여 정부기관 간 민감정보 노출을 방지하기 위한 기본적인 시스템 제안 외에 추가로 비밀키의 분산 보관 방식으로 보안성을 한 층 높이는 방안과 동형암호 데이터베이스의 검색 연산 속도를 높일 수 있는 방안을 추가로 제안하였다.

주요어 : 동형암호, 금융거래정보, 금융정보분석원, FIU
학 번 : 2019-25554

Abstract

Lee Hyun-kyu
Mathematical Information Science,
Convergence Science and Technology
Seoul National University

Korean government agencies are securing financial transaction information necessary for their own business through financial institutions such as banks and the FIU. Various law enforcement agencies receive tens of thousands of financial transaction information annually from the FIU for use in their own business.

This thesis proposes a method to supplement the fact that sensitive and confidential information of government agencies is inevitably exposed to the outside by using homomorphic encryption technology.

The most important reason for the exposure of sensitive information is that in order to search and extract the financial information of a specific person from the financial information database held by the FIU, the work must be performed in a plain text state. Calculation cannot be performed in the encrypted state with the currently commercialized encryption technology. It is expected that the use of homogeneous encryption can facilitate

information cooperation between organizations without exposing sensitive information. In this paper, in addition to the basic system proposal to prevent the exposure of sensitive information between government agencies by using homomorphic encryption as above, in addition to the method of increasing the security by a distributed storage method of secret keys, and increasing the search operation speed of the homomorphic encryption database. An additional plan was proposed.

keywords : homomorphic encryption**, FIU,** financial transaction

Student number : 2019-25554

목 차

Ⅰ. 서론

1. 연구의 배경

최근 우리 사회가 급격히 디지털화 되면서 전세계적으로 개인정보의 중요성이 매우 높아지고 있다. 이름, 주민등록번호, 계좌번호, 주소, 가족사항 등 한 개인의 거의 모든 정보가 디지털 방식으로 변환되어 각 기관에서 운용하는 서버에 저장되어 있는 경우가 많으나, 편리해진 만큼 개인정보가 유출되면 그 피해가 크다고 할 수 있다. 최근 개인정보가 유출되거나 악용되는 사례가 빈번히 발생하고 있어 개인정보 보호에 대한 관심이 커지고 있는 상황이다.

그러면 민감한 개인정보를 가장 많이 보유하고 취급하는 정부기관에서의 개인정보 보안 수준은 어떠할까. 디지털사회로 접어들면서 정부기관간 고유업무를 위한 정보교환이 매우 잦아지고 있다. 우리나라 법집행기관인 국세청, 검찰청, 경찰청, 관세청 등은 원활한 법집행을 위해 다양한 기관과 정보를 교환하고 있는데, 정보교환 과정에서 개인정보 유출에 대한 가능성을 완전히 배제할 수는 없다. 일례로 금융정보분석원에서는 각 정부기관에서 요청하는 금융거래정보를 검색하여 전달하기 위해서 암호화된 민감정보[1)]를 필수적으로 복호화 하여 필요한 작업을 해야 하는데 이 과정에서 각 기관 민감정보를 여과없이 열람이 가능하기 때문이다.

따라서 본 연구에서는 정부기관 간 필수적인 정보교환 과정에서 개인정보 노출 우려가 없고 법 집행에 차질이 없는 정보교환 방식을 모색해 보고자 한다.

---

1) 수사대상자 정보, 세무조사 대상자 정보, 체납자 정보 등 각 기관에서 다루는 개인정보

2. 연구의 방법

먼저 현재 정부기관에서 취급되는 민감한 개인정보인 금융거래정보에 대해 알아보고, 정부기관에서 금융거래정보를 확보하여 사용할 수 있는 법적 근거와 국제기구의 금융거래정보 활용에 대한 권고사항을 살펴본다. 나아가 정부기관의 금융거래정보 교환과 취급실태 및 현재 금융거래정보 교환방식의 문제점, 위험성을 살펴보도록 한다.

이후 기존 교환방식의 문제점을 해결하기 위해 동형암호 기술을 이용한 정보교환 방식을 제안하고, 이를 정부기관 간 금융거래정보 교환에 적용하기 위해 정부기관 데이터베이스 암호화 방안, 비밀키 생성 및 보관의 주체 연구, 데이터베이스 검색방식 개선 등 구체적인 방식을 논해보도록 한다.

Ⅱ. 정부기관과 금융거래정보

1. 정부기관에서 취급되는 금융거래정보

우리나라 정부에서는 은행 등 금융기관과 금융정보분석원을 통해 각 기관 고유업무에 필요한 금융거래정보를 확보하고 있다. 금융정보분석원은 금융위원회 산하의 기관으로 2001년 11월 24일 '특정금융거래보고법 시행령'이 대통령령으로 공포되고, 동년 11월 28일 금융정보 분석원이 출범하여 현재까지 운영되고 있는 기관으로, 설치근거는 【재정경제부와그소속기관직제】(일부개정2001.11.24. 대통령령 제17417호 제4장의3) 규정에서 찾아볼 수 있다.

금융정보분석원은 법무부, 금융위원회, 국세청, 관세청, 경찰청, 한국은행, 금융감독원 등 관계기관의 전문 인력으로 구성되어 있으며,

금융기관 등으로부터 자금세탁관련 혐의정보를 수집, 분석하여 불법거래, 자금세탁행위 또는 공중협박자금조달행위와 관련된다고 판단되는 금융거래 자료를 법집행기관 (검찰청, 경찰청, 국세청, 관세청, 금융위, 중앙선관위 등) 제공하는 업무를 주업무로 하고, 금융기관등의 혐의거래 보고업무에 대한 감독 및 검사, 외국의 FIU와의 협조 및 정보교류 등을 담당하고 있다.

일례로 국세청에서는 세무조사 시 금융정보분석원이 보유한 세무조사 대상자의 의심거래보고정보(의심거래보고제도를 통해 금융정보분석원이 입수) 및 고액현금거래정보(고액현금거래보고제도를 통해 금융정보분석원이 입수)를 활용하며, 검찰청, 관세청 등 기타 법집행기관도 해당 고유업무를 집행하기 위해 금융정보분석원의 자료를 활용하고 있다.

법집행기관에서 고유업무 수행 시 확보하는 금융정보는 크게 두 가지로 나눌 수 있다. 금융기관으로부터 직접 전달받는 금융정보가 그 첫 번째이고, 금융정보분석원으로부터 전달받는 금융정보가 두 번째이다. 금융기관에서 취급하는 정보는 일반적인 예금 입출금 거래내역과 계좌별 잔고내역 등이지만, 금융정보분석원에서 취급하는 정보는 일반 금융전보와는 다른 성격을 가지고 있다.

1-1. 금융정보분석원 취급 금융정보

금융정보분석원은 의심거래보고제도와 고액현금거래보고제도를 통해 금융기관으로부터 특정 금융거래 내역을 수집하여 분석한다.

의심거래보고제도란, 금융거래(카지노에서의 칩 교환 포함)와 관련하여 수수한 재산이 불법재산이라고 의심되는 합당한 근거가 있거나 금융거래의 상대방이 자금세탁행위를 하고 있다고 의심되는

합당한 근거가 있는 경우 이를 금융정보분석원장에게 보고하도록 하는 제도이다. 불법재산 또는 자금세탁행위를 하고 있다고 의심되는 합당한 근거의 판단주체는 금융회사 종사자이며, 그들의 주관적 판단에 의존하여 생성되는 정보다. 의심거래보고건수는 2010년 6월 30일부터 의심거래보고 기준금액이 2천만원에서 1천만원으로 하향 조정되고, 2013년 8월 13일부터 의심거래보고 기준금액이 삭제됨에 따라 크게 증가되고 있는 추세이다. 의심거래 보고책임자는 특정금융거래정보 보고 및 감독규정의 별지 서식에 의한 의심스러운 거래 보고서에 보고기관, 거래상대방, 의심스러운 거래내용, 의심스러운 합당한 근거, 보존하는 자료의 종류 등을 기재하여 온라인 또는 실물로 보고하고 있다.

고액현금거래보고제도는 일정금액 이상의 현금거래를 FIU에 보고토록 한 제도이다. 1일 거래일 동안 1천만원 이상의 현금을 입금하거나 출금한 경우 거래자의 신원과 거래일시, 거래금액 등 객관적 사실이 금융정보분석원으로 자동 보고된다. 해당제도 도입 당시에는 보고 기준금액이 5천만원이었으나, 2008년부터 3천만원, 2010년부터 2천만원, 2019년 7월부터 1천만원으로 단계적으로 인하하여 운영되고 있다. 위와 같이 현금거래를 보고하도록 한 것은 1차적으로는 출처를 은닉하고 위장하려는 대부분의 자금세탁거래가 고액의 현금거래를 수반하기 때문이며, 또한 금융기관 직원의 주관적 판단에 의존하는 의심거래보고제도만으로는 금융기관의 보고가 없는 경우 불법자금을 적발하기가 사실상 불가능하기 때문이다.

고액현금거래보고제도의 경우 미국을 시작으로 호주, 캐나다 등 주로 선진국에서 도입하여 운영하여 왔으나 최근들어 대만, 과테말라, 슬로베니아, 베네수엘라 등으로 그 도입이 점차 확대되어 가고 있다. 보고기준금액은 각 국이 결정하므로 국가에 따라 다르나, 미

국, 호주, 캐나다 등 주요국에서는 1만달러를 기준금액으로 하고 있다[2].

[표1. 국가별 고액현금거래보고 기준금액]

국가	기준금액	보고대상기관
미국	USD 10,000 이상	은행, 증권브로커와 딜러, 자금서비스업, 카지노 등
캐나다	CAD 10,000 이상	은행, 신탁회사, 생명보험회사, 증권딜러, 환전업자, 회계사(법인), 부동산 중개인, 카지노 등
호주	AUD 10,000 이상	은행, 보험회사 및 보험중개인, 금융서비스업, 신탁회사, 변호사 또는 법무법인, 카지노 등

1-2. 금융정보분석원으로부터 확보하는 금융정보

금융정보분석원이 정부기관에 제공하는 대상이 되는 정보는 다음과 같다.

① 불법재산 등으로 의심되는 거래라고 금융기관이 금융정보분석원에 보고한 정보('의심거래보고정보')

② 고액 현금거래여서 금융기관이 금융정보분석원에 보고한 정보('고액현금거래정보')

③ 금융정보분석원이 외국의 금융정보 분석기구로부터 제공받은 정보

④ 위 세 가지 정보 및 금융정보 및 금융정보분석원이 통보받은 외국환거래자료 등의 정보를 금융정보분석원이 정리하거나 분석한 정보

단, 정부기관에서도 정부기관 행정집행을 위한 모든 경우에 금융정보분석원으로부터 금융정보를 요청하여 사용할 수 있는 것은 아니고, 법률에 정한 엄격한 경웅에 한정하여 해당 정보를 요청하여 사용할 수 있다. 일례로 국세청에 제공대상이 되는 정보는 다음의

2) 금융정보분석원 홈페이지 참조

조사업무와 징수업무와 관련된 특정금융거래정보에 한한다.

① 조세탈루혐의 확인을 위한 조사업무에 필요하다고 인정되는 정보로서 다음의 어느 하나에 해당하는 정보

㉠ 고액현금거래정보와 조세탈루혐의와 관련된 의심거래정보의 내용이 중복되거나 밀접하게 관련되는 경우의 해당 정보

㉡ 매출액이나 재산·소득 규모에 비추어 현금거래의 빈도가 높거나 액수가 과다하여 조세탈루의 의심이 있는 경우의 해당 정보

㉢ 역외탈세(域外脫稅)의 우려가 있는 경우의 해당 정보

㉣ 그 밖에 조세탈루의 우려가 있는 경우로서 국세청장이 혐의를 제시하는 경우의 해당 정보

② 조세체납자에 대한 징수업무에 필요하다고 인정되는 정보

1-3. 금융기관으로부터 확보하는 정보 및 확보요건

정부기관은 타당한 사유가 있을 경우 금융기관으로부터 직접 금융정보를 확보하여 활용할 수 있다. 다만, 금융실명거래 및 비밀보장에 관한 법률 제4조에 따르면, 금융회사 등에 종사하는 자는 명의인의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료를 타인에게 제공하거나 누설하여서는 아니되며, 누구든지 금융회사 등에 종사하는 자에게 거래정보 등의 제공을 요구하여서는 아니된다. 단서조항으로, 다음 각 호의 어느 하나에 해당하는 경우로서 그 사용 목적에 필요한 최소한의 범위에서 거래정보 등을 제공하거나 그 제공을 요구하는 경우에는 그러하지 아니다하고 규정되어 있다.

일례로 국세청에서는 다음과 같은 사유가 있을 경우 해당 법에

따라 금융기관으로부터 금융정보를 확보하여 활용할 수 있다.

① 금융실명법에 따르면 국세청은 다음과 같은 요건을 만족하는 경우 거래정보 등을 금융기관 등에 요구할 수 있음

㉠ 금융회사 등의 특정점포에 대해 거래정보 등을 요구할 수 있는 경우

- 조세에 관한 법률에 따라 제출의무가 있는 과세자료 등의 제공

- 소관 관서의 장이 상속·증여 재산의 확인, 조세탈루의 혐의를 인정할 만한 명백한 자료의 확인, 체납자의 재산조회, 「국세징수법」 제14조제1항 국세의 납기 전 징수에 해당하는 사유로 조세에 관한 법률에 따른 질문·조사를 위하여 필요로 하는 경우

㉡ 금융회사 등의 거래정보 보관·관리부서에 대해 거래정보 등 일괄조회를 요구할 수 있는 경우

- 부동산의 보유기간, 보유 수, 거래 규모 및 거래 방법 등 명백한 자료에 의하여 특정 부동산거래와 관련한 소득세 또는 법인세의 탈루혐의가 인정되어 그 탈루사실의 확인이 필요한 자에 대한 거래정보등의 제공을 요구하는 경우

- 체납액 1천만원 이상인 체납자의 재산조회를 위하여 필요한 거래정보 등의 제공을 국세청장·지방국세청장의 명의로 요구하는 경우

② 국세청장 및 지방국세청장은 금융실명법 외에도 상증법 및 과세자료법에 따라 금융회사 등의 장에게 금융재산에 관한 과세자료 및 금융거래정보를 일괄하여 조회할 수 있음

㉠ (상증법 제83조제1항) 다음에 해당하는 자의 상속·증여세를 결정·경정하기 위한 조사

- 직업, 연령, 재산 상태, 소득신고 상황 등으로 볼 때 상속세나 증여세의 탈루 혐의가 있다고 인정되는 자
- 인별 재산과세자료의 수집·관리대상이 되는 상속인·피상속인 또는 증여자·수증자

㉡ (과세자료법 제6조) 명백한 조세탈루 혐의를 확인하기 위하여 필요한 경우로서 금융거래 관련 정보나 자료에 의하지 아니하고는 조세탈루 사실을 확인할 수 없다고 인정되면 조세탈루의 혐의가 있다고 인정되는 자에 한하여 금융거래정보를 요구할 수 있음

2. 금융거래정보 확보의 법적 근거

2-1. 금융정보분석원의 금융정보 확보

금융정보분석원에서는 '특정금융거래정보의 보고 및 이용 등에 관한 법률'(이하 특금법)에 따라 은행, 증권사, 보험회사 등의 금융기관으로부터 개인 혹은 법인의 금융거래정보를 수집하여 보관하고 있다.

【특금법 제4조】 불법재산 등으로 의심되는 거래의 보고 등[3)]

【특금법 제4조의2】 금융회사등의 고액현금거래 보고[4)]

---

3) ① 금융회사 등은 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 지체없이 그 사실을 금융정보분석원장에게 보고하여야 한다.

4) ① 금융회사등은 5천만원의 범위에서 대통령령으로 정하는 금액 이상의 현금(외국통화는 제외한다)이나 현금과 비슷한 기능의 지급수단으로서 대통령령으로 정하는 것(이하 "현금등"이라 한다)을 금융거래등의 상대방에게 지급하거나 그로부터 영수(領收)한 경우에는 그 사실을 30일 이내에 금융정보분석원장에게 보고하여야 한다.

② 금융회사등은 금융거래등의 상대방이 제1항을 회피할 목적으로 금액을 분할하여 금융거래등을 하고 있다고 의심되는 합당한 근거가 있는 경우에는 그 사실을 금융정보분석원장에게 보고하여야 한다.

2-2. 정부기관의 금융정보 확보

금융정보분석원은 아래와 같은 법령에 근거하여 국세청, 검찰청 등 법집행기관에게 개인 및 법인(회사)의 금융거래정보를 제공하고 있다. 다만 제공하는 정보의 민감성과 관련하여 해당 사유를 엄격하게 검토하여 정보제공 여부를 결정하고 있으며, 법에 명시된 정보제공사유에 해당하지 않을 경우 법집행기관의 정보제공요구를 거부할 수 있다.

【특금법 제7조】 수사기관 등에 대한 정보제공

① 금융정보분석원장은 불법재산·자금세탁행위 또는 공중협박자금조달행위와 관련된 형사사건의 수사, 조세탈루혐의 확인을 위한 조사업무, 조세체납자에 대한 징수업무, 관세 범칙사건 조사, 관세탈루혐의 확인을 위한 조사업무, 관세체납자에 대한 징수업무 및 「정치자금법」 위반사건의 조사, 금융감독업무 또는 테러위험인물에 대한 조사업무(이하 "특정형사사건의 수사등"이라 한다)에 필요하다고 인정되는 경우에는 다음 각 호의 정보(이하 "특정금융거래정보"라 한다)를 검찰총장, 국세청장, 관세청장, 중앙선거관리위원회, 금융위원회 또는 국가정보원장에 제공한다. (이하생략)

추가로 국세청의 경우 국세청의 고유업무(세무조사업무, 체납징수업무 등)를 위해 납세자의 금융거래정보를 매우 다양하고 적극적으로 활용하고 있는데, 국세청은 납세자의 금융거래정보를 다음의 법률에 근거하여 확보하고 있다.

① 금융실명거래 및 비밀보장에 관한 법률 제4조제1항제2호

② 상속세 및 증여세법 제83조 등

③ 과세자료의 제출 및 관리에 관한 법률 제6조

④ 소득세법 제164조제1항, 제170조제1항 등

⑤ 법인세법 제120조, 제122조 등

3. 국제기구의 권고사항 및 정보활용 필요성[5)]

OECD 등 국제기구는 국세청, 검찰청 등 정부의 법집행기구와 금융정보분석원의 협력을 강조하며 철저하고 다양한 안전조치 하에서 금융정보분석원이 보유한 정보에 대한 법집행기구의 접근 확대를 권고하고 있다. 특히 세무당국의 금융거래 정보의 접근 및 활용확대는 조세범죄 및 금융범죄에 대한 범정부적 대응 측면에서 다음과 같은 장점이 있을 것이다.

먼저, 조세행정의 측면의 장점으로 의심거래보고 정보 등의 금융거래 정보는 잠재적 납세불순응 영역을 식별할 수 있는 새로운 형태의 정보 소스를 제공하며, 세금 산정 및 체납 정리에 도움을 줄 수도 있고, 특정 산업부문·납세자 집단·지역별로 탈세위험 요인을 식별하는 모형이나 분석기법의 개발 및 고도화에 도움이 되며, 세무조사 대상을 보다 잘 선정하는 데에도 기여할 것이며, 특히 기존 세무당국이 보유한 자료와 연계하여 활용한다면 그 효과는 더 커질 것이다. 일례로 국세청에서는 현재 빅데이터를 세정지원, 세무업무, 조사업무 등 국세청 고유업무에 매우 적극적으로 적용하여 활용하고 있는데, 업무특성상 금융거래정보와의 시너지효과는 매우 클 것으로 판단된다.

한편, 세무당국은 금융거래정보를 세무목적으로 활용하는 가운데

5) 금융거래정보의 국세행정 활용실태 및 개선방안 연구(홍익대학교)

조세범죄 외의 금융범죄를 발견할 수 있고, 이를 다른 법집행기관과 공유한다면, 세무당국은 금융범죄에 대한 범정부적인 대응에 큰 기여를 할 수도 있으며 기업의 대표자뿐만 아니라 그 지배구조와 주요 관계자에 대한 정보를 파악하는 지식과 경험이 풍부한 세무당국은 고소득 범죄자 대응 측면에서 다른 법집행기구를 지원하는 것이 가능할 것이다.

Ⅲ. 금융거래정보 교환의 지속적인 확대

1. 금융거래정보 활용 확대

최근 우리 사회는 급격하게 디지털화 되고 개인의 모든 생활 및 금융자산 등이 기록으로 남는 시대가 되었다. 이와 같은 관점에서 볼 때 개인의 생활은 매우 편해졌다고 볼 수 있으나, 다른 방면으로는 개인의 모든 정보가 기록으로 남기 때문에 개인정보 보호가 더욱 필요해졌다고 볼 수 있다.

정부기관에서는 각 기관의 고유 행정업무를 위해 이러한 개인정보를 확보하여 사용할 수 있다. 검찰에서는 고소사건의 수사를 위해 개인정보를 사용하고, 국세청에서는 세무조사와 체납세금 징수를 위해 개인정보를 사용한다. 마찬가지로 경찰, 해경, 선관위 등 정부기관에서 개인정보가 필요한 경우 일정 요건에 맞춰 신청을 하면 어떤 개인의 개인정보를 모두 볼 수 있는 것이다.

특히 정부기관에서 어떤 사건을 접할 때 당사자의 자금흐름을 보면 많은 부분을 알 수 있게 된다. 금융정보에 가장 민감한 것은 아마도 국세청일 것이다. 국세청에서는 해당 업무가 모두 금융과 연관된 것이기 때문에 금융정보 활용도가 정부기관에서 가장 높다. 아래 항목에서 통계로 입증되겠지만 국세청에서는 매년 금융거래정보의

활용이 매우 큰 폭으로 증가하고, 각 법집행기관의 활용도 또한 지속적으로 증가하고 있는 추세이다.

1-1. 금융거래정보의 수집 및 활용 증가

자금세탁 의심거래보고 접수 건수는 2005년 이후 연평균 증가율이 약 39%에 달할 정도로 폭발적으로 증가하는 추세다. 10년 전 2008년에는 92,093건에 불과했지만 2018년 972,320건으로 10배 이상 증가하였으며, 이는 금융정보에 대한 중요성과 필요성 인식과 각 금융사 전산시스템 고도화에 기인하는 것이다.

특히 전체 금융거래정보 보고건수 대비 은행권의 비중이 2018년에는 80%로 큰 비중을 차지하고 있는데, 이는 가상자산(가상화폐 등)의 취급 증가로 은행권의 가상자산에 대한 정보비중이 큰 폭으로 늘어났기 때문이다. 6)

[표2. 연도별·월별 의심거래보고 접수 건수]

월별 의심거래보고 접수 건수 (단위:STR건)

구분	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	합계
2002	16	11	11	14	13	11	8	15	21	38	64	53	275
2003	74	92	75	105	77	94	184	133	162	247	195	306	1,744
2004	270	203	318	356	411	442	305	337	403	508	550	577	4,680
2005	602	370	674	937	941	1,425	1,466	1,551	1,518	1,411	1,210	1,354	13,459
2006	1,945	2,014	1,513	1,553	1,610	1,751	1,813	2,094	2,114	2,180	2,667	2,895	24,149
2007	3,009	3,245	4,378	4,215	4,566	4,033	3,956	4,776	3,945	4,347	6,769	5,235	52,474
2008	6,745	6,780	8,179	7,867	7,020	7,421	8,187	7,553	7,360	8,668	9,352	6,961	92,093
2009	11,164	7,655	8,136	11,221	10,040	12,087	14,297	11,024	12,153	11,962	11,556	14,987	136,282
2010	15,872	12,768	16,228	21,021	17,998	20,346	26,405	21,265	18,535	22,649	20,637	22,344	236,068
2011	22,725	28,532	39,226	30,897	27,618	26,950	26,582	24,513	25,048	23,253	26,384	27,735	329,463
2012	23,915	22,504	23,448	21,165	23,576	26,322	23,720	24,790	24,535	23,943	25,907	26,416	290,241
2013	28,247	21,724	27,580	26,172	27,195	24,336	31,045	38,074	31,607	42,836	42,507	37,419	378,742
2014	44,297	33,961	45,157	44,247	38,731	39,207	45,009	40,458	37,921	42,939	45,838	43,660	501,425
2015	56,267	40,138	54,732	51,916	47,853	48,077	45,841	47,078	58,534	55,149	58,252	60,239	624,076
2016	70,757	53,793	70,107	55,952	59,020	59,602	95,664	53,201	42,400	44,125	48,201	50,534	703,356
2017	41,423	38,716	48,996	44,098	39,056	41,763	42,032	45,506	46,667	34,454	46,269	50,928	519,908
2018	50,075	43,035	72,949	73,126	76,960	95,613	84,218	71,008	87,527	105,761	101,696	110,352	972,320

6) 자금세탁방지 2018 연차보고서(금융정보분석원)

국내 법집행기관의 요구에 따른 정보제공 건수는 매년 증가하고 있다. 특히 2013년 특정금융정보법 개정으로 정보제공 요건범위가 확대됨에 따라 법집행기관의 수사 및 조사 시 금융정보분석원이 보유한 특정금융거래정보의 활용이 크게 확대되었다. 통계상으로도 2014년 제공건수가 전년 대비 360% 이상 급증하였다.[7)]

[표3. 최근 국내 법집행기관의 요구에 의한 정보 제공건수]

최근 6년간 국내 법집행기관의 요구에 의한 정보 제공건수

구 분	검찰청	경찰청	국세청	관세청	금융위	선관위	해경청	국정원	합 계
2013	623	385	4,093	306	0	3	33	0	5,443
2014	691	332	23,032	1,306	3	82	22	0	25,468
2015	2,678	400	26,187	1,252	1	1	6	0	30,525
2016	894	343	32,901	680	5	7	4	19	34,853
2017	509	358	37,114	449	2	1	5	1	38,439
2018	523	481	36,562	441	0	5	11	0	38,023
합 계	5,918	2,299	159,889	4,434	11	99	81	20	134,728

2013년 특정 금융거래정보의 보고 및 이용에 관한 법률 개정사항은 아래와 같다.

개정 전 (시행2012.12.11.)	개정 후 (시행2013.11.14.)
제7조【수사기관 등에 대한 정보제공】 ①금융정보분석원장은 불법재산·자금세탁행위 또는 공중협박자금조달행위와 관련된 형사사건의 수사, 조세 범칙사건 조사, 조세범처벌법 제3조에 따른 범칙혐의 확인을 위한 세무조사 업무, 관세 범칙사건 조사, 관세법 제270조에 따른 범칙혐의 확인을 위한 관세조사업무	제7조【수사기관 등에 대한 정보제공】 ①금융정보분석원장은 불법재산·자금세탁행위 또는 공중협박자금조달행위와 관련된 형사사건의 수사, <u>조세탈루혐의 확인을 위한 조사업무, 조세체납자에 대한 징수업무</u>, 관세 범칙사건 조사, 관세탈루혐의 확인을 위한 조사업무, 관세체납자에 대한 징수업무 및 정치자금

7) 자금세탁방지 2018 연차보고서(금융정보분석원)

및 정치자금법 위반사건의 조사 또는 금융감독업무에 필요하다고 인정되는 경우에는 다음 각 호의 정보를 검찰청장, 국세청장, 관세청장, 중앙선거관리위원회 또는 금융위원회에 제공한다. 1. 제4조제1항 또는 제2항에 따라 금융회사 등이 보고한 정보 2. 제8조제1항에 따라 외국금융정보분석기구에서 제공받은 정보 3. 제1호 및 제2호의 정보 또는 제4조의2 및 제6조에 따라 보고·통보받은 정보를 정리하거나 분석한 정보	법 위반사건의 조사또는 금융감독 업무에 필요하다고 인정되는 경우에는 다음 각 호의 정보를 검찰총장, 구세청장, 관세청장, 중앙선거관리위원회 또는 금융위원회에 제공한다. 1. 제4조제1항 또는 제4조의2에 따라 금융회사 등이 보고한 정보 중 특정형사사건의 수사등과의 관련성을 고려하여 대통령령으로 정하는 정보 4. 제8조제1항에 따라 외국금융정보분석기구로부터 제공받은 정보 중 특정형사사건의 수사등과의 관련성을 고려하여 대통령령으로 정하는 정보 5. 제1호 및 제2호의 정보 또는 제4조의2및제6조에따라 보고·통보받은 정보를 정리하거나 분석한 정보

종전에는 조세 범칙사건 조사, 조세범 처벌법 제3조에 따른 범칙혐의 확인을 위한 세무조사 업무에만 제한적으로 사용되었으나, 2013년 11월 14일 관련 법 개정 이후 조세탈루 혐의 확인을 위한 조사업무, 조세 체납자에 대한 징수업무에 폭넓게 사용할 수 있게 되었다. 때문에 위 표에서 보듯이 국세청에서 금융거래정보를 요청하여 활용한 실적은 2013년 4,093건에서 2014년 23,023건, 2015년 26,187건 2016년 32,901건, 2017년 37,114건, 2018년 36,562건으로 매우 큰 폭으로 증가하였으며, 이는 6년간 모든 법집행기관에서 요청한 정보의 92.5%에 달한다

국세청에서는 금융정보분석원으로부터 수보받은 금융정보를 세무조사 업무와 체납징수 업무에 활용하고 있으며, 세무조사의 경우 해당 금융정보를 활용하여 2018년 기준으로 2조 4천억원 이상의 추징

실적을 거뒀으며, 체납징수의 경우 2018년 5천억원 이상의 체납세액을 징수하는 실적을 달성했다.[8)]

[표4. FIU 제공정보 이용 조사실적]

FIU 제공정보 이용 조사실적			
			[단위 : 건, 억원]
구분	조사건수 (1)	추징세액 (2)	건당추징세액 (3=2/1)
2014년	10,254	23,518	2.3
2015년	11,956	23,647	2.0
2016년	13,802	25,346	1.8
2017년	12,391	23,918	1.9
2018년	**14,514**	**24,635**	1.7

[표5. FIU 제공정보 체납징수 활용실적]

FIU 제공정보 체납징수 활용실적			
			[단위 : 명, 억원]
구분	체납자 수 (1)	현금징수 (2)	건당징수세액 (3=2/1)
2014년	2,175	2,112	1.0
2015년	2,428	3,244	1.3
2016년	4,271	5,192	1.2
2017년	7,148	6,670	0.9
2018년	**6,128**	**5,035**	**0.8**

8) 국세청, 국세통계연보

1-2. 효과적인 정책집행을 위한 금융정보 활용 확대

위에서 말한 것과 같이 국세청에서 금융정보를 가장 많이 요청하고 가장 많이 활용하는 것은 국세청의 주요 업무가 세금과 관련된 것이라는 이유가 크다. 우리나라의 경우는 증빙없이 현금거래되는 영역에서 세금을 탈루하는 행위가 심각한 수준으로 알려져있다. 최근 신용카드 및 현금영수증을 발행하는 경우가 많아 우리나라의 세원 투명성은 개선되었지만, 고소득사업자의 현금매출 누락 등과 같은 과거의 고질적인 폐단은 완전히 개선되지 않았다.

[표6. 세무조사 결과 고소득 자영업자의 소득적출률 추이]

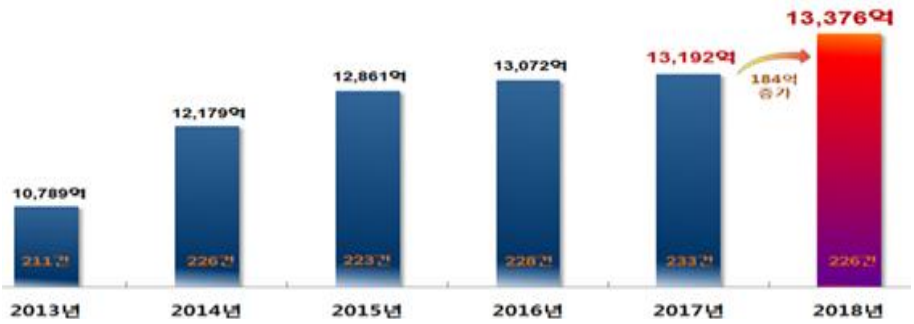
(단위: 명, 억원, %)

구분	조사인원	부과세액	실제소득 ①=②+③	신고소득 ②	적출소득 ③	소득 적출률 ④=③/①
2006	993	5,615	31,886	16,040	15,846	49.7
2007	574	3,728	18,916	10,028	8,888	47.0
2008	482	3,019	13,639	7,560	6,079	44.6
2016	967	6,330	22,626	12,901	9,725	43.0
2017	908	6,719	22,324	10,801	11,523	51.6
2018	881	6,959	23,769	11,066	12,703	53.4

자료: 국세청 보도자료 및 심기준 의원실 보도자료

뿐만 아니라 해외 송금을 통한 역외탈세, 해외의 조세회피처에 가짜 회사를 세우고 회사 자금을 빼돌리는 페이퍼 컴퍼니 탈세 등 수법이 점점 정교해지고 진화하고 있다. 게다가 유튜브를 통한 개인들의 수익창출, SNS마켓의 난립, 인플루언서의 광고비수입 등 기존의 과세인프라로 포착이 어려운 과세 사각지대를 이용한 탈세행위가 점점 늘어나고 있는 추세다[9].

[표7. 연도별 역외탈세 규모]



또한 체납징수 업무의 경우도 마찬가지이다. 악질적인 고액 체납자들의 경우에는 본인의 금융자산을 숨겨놓은 채 세금을 체납하는 경우가 다반사인데, 2013년 관련 법 개정으로 금융거래정보를 폭넓게 활용하기 시작하면서 체납징수 업무에도 금융정보를 사용하여 체납자들의 금융재산을 추적하여 징수할 수 있게 되었다.

검찰이나 경찰 등 수사기관의 금융정보 활용의 경우도 마찬가지라고 볼 수 있다. 예전처럼 단순히 차명계좌를 이용한 자금세탁에서 벗어나, 회사 자금을 횡령하거나 범죄자금을 마련하는데 점점 복잡하고 다양한 방법이 사용되고 있으며 범죄자들도 수사기관이 금융정보를 볼 수 있다는 것을 알고 있기 때문에 점점 새로운 방법을 개발하는 것이다.

위에서 본 것처럼 법 집행기관의 고유업무 수행을 위해서는 금융정보 활용이 필수적인 상황이며, 시간이 갈수록 탈세 혐의자, 체납자, 범죄 혐의자들의 자금은닉 수법들이 교묘해지기 때문에 점차 금융정보의 필요성이 더해질 것으로 예상된다.

9) 국세청 보도자료

2. 금융거래정보의 접근 및 활용에 관한 국제기구 권고사항[10)]

OECD에서는 심각한 범죄에 대응하기 위하여 정부기관 간의 협력을 강조하며, 특히 세무당국이 고유업무를 수행하는 가운데 발견한 자금세탁이나 테러자금 조달 등과 같은 범죄 행위를 다른 법 집행기구에 쉽게 통보할 수 있도록 합법적인 통로를 구축할 것을 권고한 바 있다. 이와 관련하여 2012년 2월 자금세탁방지국제기구는 조세범죄와 연관된 혐의가 있는 금융거래 또한 금융정보분석원에 보고해야 하는 사항 중 하나로 채택하기도 하였다.

2015년 OECD는 정부기관 간 정보공유 시 정보유출 방지를 위한 보호수단을 마련하기 위해서 세 가지 요소를 제안하였다.

① 정보의 기밀성을 보장하고 정보 사용의 목적을 적절하게 제한하는 것을 법률로 규정하고, 정보의 부적절한 사용 및 노출에 대해서는 처벌 및 제제가 필요함

② 금융거래정보가 지정된 목적으로만 사용될 수 있고 권한없는 사람이나 정부기관에 공개되는 것을 방지하기 위한 절차가 마련되어야 함. 이를 위해서 정보취급자에 대한 심사, 정보의 접근 제한, 기밀보호와 관련된 모든 측면에 대한 시스템적 통제가 필요함.

③ 보안규정 위반에 대한 처벌과 제제를 가하는 법적 근거가 마련되어야 하며, 적절한 행정자원 및 절차가 필요함

2-1. 금융거래정보 공유방식에 따른 모델[11)]

10) 금융거래정보의 국세행정 활용실태 및 개선방안 연구(홍익대학교) 인용

11) “조세범죄 및 기타 금융범죄에 대응하기 위한 정부부처 간 효과적인 협력(Effective Inter-Agency Cooperation in Fighting Tax Crimes and Other Financial Crimes)에 관한 보고서

이번에는 외국의 세무당국과 금융정보분석원 간 금융거래정보를 공유하는 방식과 현황을 조사한 OECD의 주요 결과를 본다. OECD는 회원국과 비회원국을 포함한 51개 국가의 현황을 조사하여 제시하였다.

① 1유형 : 세무당국이 금융정보분석원 보유 정보 데이터베이스에 직접 접근 가능한 방식이며, 세무당국이 필요할 때 정보를 즉각 활용할 수 있어 적시성이 높음

② 2유형 : 일정한 유형에 해당하는 금융정보를 금융정보분석원에서 세무당국의 요청과 관계없이 의무적으로 공유하는 방식이며, 어떤 정보를 공유하는지 결정의 문제가 있음

③ 3유형 : 일정 유형의 정보에 대하여 세무당국과의 공유 여부를 금융정보분석원이 판단하고 결정하여 공유하는 방식이며, 양 기관의 협의에 따라 공유되는 정보가 어떤 수준인지 결정될 가능성이 있음

④ 4유형 : 세무당국이 요청하는 경우에만 금융정보분석원에서 정보를 공유하는 방식이며, 사장되는 정보가 상당수 있고 정보활용에 적시성이 낮음

⑤ 5유형 : 금융정보분석원의 보유정보를 세무당국과 공유하지 않음

2-2. 주요국의 금융거래정보 활용 모델[12)]

일반 세무행정에서 금융거래정보를 활용하는 국가별 현황은 아래와 같음

공유모델	국가명
1유형	미국, 영국, 호주, 아일랜드, 말레이시아 5개국
2유형	아제르바이잔, 벨기에, 체코, 독일, 가나, 아이슬란다, 인도 등 10개국
3유형	오스트리아, 브라질, 덴마크, 한국, 프랑스, 그리스, 이스라엘 등 16개국
4유형	코스타리카, 에콰도르, 라트비아, 스웨덴 등 6개국
5유형	캐나다, 칠레, 콜롬비앋, 에스토니아, 핀란드 등 14개국

12) OECD보고서(2017)

조세 범칙조사에서 금융거래정보를 활용하는 국가별 현황은 아래와 같음

공유모델	국가명
1유형	미국, 영국, 호주, 아일랜드, 말레이시아 등 7개국
2유형	한국, 일본, 벨기에, 체코, 독일, 인도, 스페인 등 21개국
3유형	오스트리아, 캐나다, 덴마크, 핀란드, 프랑스, 그리스 등 17개국
4유형	에콰도르, 아제르바이잔, 부르키나 파소 3개국
5유형	엘살바도르, 조지아, 스위스 3개국

Ⅳ. 금융거래정보 취급실태

1. 정부기관 간 금융정보 교환 방식

국세청, 검찰청 등 정부기관에서는 일정 요건에 해당하는 경우 금융정보분석원으로부터 의심거래정보 및 고액현금거래정보 등 금융정보를 수보하여 각 기관 고유업무에 활용할 수 있다.

정부기관 간 금융정보 교환은 기본적으로 공문의 방식으로 이루어진다. 정부기관에서 해당 고유업무 대상자(국세청의 경우 세무조사 대상자, 체납자 등이며, 검찰이나 경찰의 경우 사건수사 대상자)를 특정하여 금융정보분석원에 공문으로 요청하면 금융정보분석원에서는 보유하고 있는 의심거래정보 및 고액현금거래정보 중에서 관련 정보를 발췌하여 정보를 요청한 정부기관에 회신하여 준다.

과거에는 정부기관 간 전자공문을 교환하는 방식으로 이루어지고, 개인의 금융정보도 전자공문에 첨부파일로 포함하는 방식으로 정보교환이 시행되었으나, 최근에는 금융정보분석원과 법집행기관 간 전용 시스템을 구축하여 시스템을 통하여 정보교환이 이루어진다.

과거 공문상에 기입하던 특정인의 정보를 전용 시스템 상에 입력

하고, 정보조회 사유를 기입하여 금융정보분석원으로 발송하면 금융정보분석원에서 해당 시스템을 통하여 관련 정보를 회신하여 주는 방식이다. 법집행기관에서는 정보취급자가 해당 시스템에 접속하여 금융정보를 내려받은 후 업무에 활용하게 되며, 이러한 방식으로 전송받은 금융정보를 업무에 활용했을 경우 법에 따라 활용 결과를 금융정보분석원에 회신하여 준다.

2. 금융거래정보의 민감성

이번에는 정부기관 간 교환되는 금융거래정보의 민감성에 대하여 논의해본다. 법집행기관이 활용하는 대표적인 금융거래정보인 의심거래정보와 고액현금거래정보의 경우를 살펴본다.

의심거래정보에는 다음과 같은 정보가 포함되어 있다.

① 의심스러운 거래자

② 거래발생일자 및 거래발생 장소(영업점)

③ 금융거래 수단, 금융거래 방법

④ 혐의거래로 판단한 사유 및 종합 의견 기록

⑤ 의심스러운 거래자에 관한 정보(거래자명, 국적, 실명번호)

⑥ 거래자 자택주소, 직장주소, 생년월일, 성별, 전화번호, 여권번호

⑦ 거래자 직업, 사업내용, 직위, 부서명, 사업자등록번호

⑧ 거래발생일시 및 거래점명, 거래수단, 상품, 거래종류, 원화 거래금액

⑨ 의심거래에 사용된 계좌정보, 계좌개설일자 등

마찬가지로 고액현금거래정보의 경우 다음과 같은 정보가 포함되어 있다.

① 거래자명

② 실명번호, 주소, 전화번호, 국적

③ 거래일자, 거래일시, 거래계좌번호

④ 금융회사, 거래영업점명, 영업점 주소, 거래채널, 거래금액 등

⑤ 수취인계좌번호, 수취금융기관, 수취인성명

[표8. 고액현금거래정보 예시]

거래자	실명번호	거래일자	거래일시	금융회사	거래수단	거래금액	상대회사	수취인계좌	수취인
홍길동	8101281000000	2020-09-23	13:13:27	우리은행	현금	30,000,000	신한은행	10021290000	성춘향
홍길동	8101281000000	2020-09-23	13:15:31	우리은행	현금	13,000,000	농협	3120033222	김홍자
홍길동	8101281000000	2020-09-23	13:17:20	우리은행	현금	52,000,000	농협	3120033222	김홍자

위의 금융정보 항목에서 보듯이 사실상 금융정보 당사자인 개인에 대한 모든 정보가 포함되어 있다. 정부기관이 금융거래정보를 입수하면 누가 어디서 얼마를 누구와 어떤 수단으로 거래했으며, 직업이 무엇이고 왜 해당 거래를 발생했는지에 대한 상세한 정보를 확보할 수 있다. 때문에 금융거래정보원에서 취급하는 의심거래정보와 고액현금거래정보는 단순 금융거래내역만 포함된 것이 아니라, 개인에 대한 거의 모든 정보가 포함된 매우 민감한 정보라고 할 수 있다.

3. 금융거래정보 오·남용 방지 및 개인정보 보호 조치[13)]

금융거래정보 오·남용 방지와 개인정보 보호 관련해서는 기본적으로 금융실명법에 규정되어 있다.

① 금융실명법 상의 금융거래의 비밀보장 규정

13) 금융거래정보의 국세행정 활용실태 및 개선방안 연구(홍익대학교) 16page 참고

금융실명법 제4조 제1항에서는 금융회사 등에 종사하는 자는 명의인[14]의 서면상의 요구나 동의를 받지 아니하고는 그 거래정보 등을 타인에게 제공하거나 누설하지 못하도록 하며, 누구든지 금융회사 등에 종사하는 자에게 거래정보 등의 제공을 요구하여서는 아니된다고 규정하고 있다. 다만, 법에서 정한 금융거래 조회요건을 만족하는 경우 그 사용 목적에 필요한 최소한의 범위에서 거래정보 등을 제공하거나 그 제공을 요구할 수 있다(금융실명법 제4조 제1항).

위의 경우에도 금융거래 정보 등을 알게 된 자는 그 알게 된 거래정보 등을 타인에게 제공 또는 누설하거나 그 목적 외의 용도로 이용하여서는 아니되며, 누구든지 거래정보 등을 알게 된 자에게 그 거래정보 등의 제공을 요구하여서는 아니된다(금융실명법 제4조 4항).

또한 금융실명법(제4조 제1항 또는 제4항)을 위반하여 제공 또는 누설된 거래정보 등을 취득한 자[15]는 그 위반 사실을 알게 된 경우 그 거래정보 등을 타인에게 제공 또는 누설하여서는 아니된다고 규정하고 있음.

② 금융실명법 상의 벌칙 규정

금융거래의 비밀보장 규정을 위반한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 하고 있음(금융실명법 제6조 제1항).

③ 금융실명법 상의 거래정보 등의 요구 절차 규정

거래정보 등의 제공을 금융기관 등의 특정점포에 요구하는 자는 다음 사항이 포함된 금융위원회가 정하는 표준양식에 의거하여 거래정보 등을 요구하도록 규정(금융실명법 제4조 제2항)

㉠ 명의인의 인적사항

14) 신탁의 경우에는 위탁자 또는 수익자를 말한다
15) 그로부터 거래정보 등을 다시 취득한 자 포함

㉡ 요구 대상 거래기간

㉢ 요구의 법적 근거

㉣ 사용 목적

㉤ 요구하는 거래정보 등의 내용

㉥ 요구하는 기관의 담당자 및 책임자의 성명과 직책 등 인적사항

④ 금융실명법 상 거래정보 등의 제공사실의 통보 규정

무분별한 금융조회를 방지하기 위해 금융조회 후에는 금융조회 대상에게 그 사실을 차후에 서면으로 통보하도록 명시하고 있음. 금융회사 등은 명의인에게 서면상의 동의를 받아 거래정보 등을 제공한 경우나 법에서 정한 금융거래 조회요건을 만족하여 거래정보 등을 제공한 경우에는 제공한 날로부터 10일 이내에 제공한 거래정보 등의 주요 내용, 사용 목적, 제공받은 자 및 제공일 등을 명의인에게 서면으로 통지해야 한다(금융실명법 제4조의2 제1항). 다만, 법에서 열거한 특정 사유[16]로 통보의 유예를 서면으로 요청받은 경우에는 유예요청기간[17] 동안 통보를 유예하여야 한다.

4. 현재 교환방식의 문제점 및 위험성

위에서 현재 정부기관 간 금융정보 교환은 기본적으로 공문의 방식으로 이루진다고 했다. 최근에는 전자적 시스템 방식으로 바뀌었

16) 특정사유란 다음 세 가지를 말한다(금융실명법 제4조의2 제2항)
1. 해당 통보가 사람의 생명이나 신체의 안전을 위협할 우려가 있는 경우
2. 해당 통보가 증거 인멸, 증인 위협 등 공정한 사법절차의 진행을 방해할 우려가 명백한 경우
3. 해당 통보가 질문, 조사 등의 행정절차의 진행을 방해하거나 과도하게 지연시킬 우려가 있는 경우

17) 위 사유 중 두 번째와 세 번째의 경우 그 유예 요청기간이 6개월 이상이라고 하더라도 유예요청기간은 6개월로 한다.

지만, 공문의 효력을 대체할 뿐 기본적인 교환방식은 동일하다. 그렇다면 현재의 이러한 교환방식에는 어떤 문제점이 있는지 알아보자.

예를 들어 국세청과 금융정보분석원 간의 정보교환을 보겠다. 국세청에서 세무조사 대상자를 선정하고 세무조사를 착수하는 경우 일부 경우를 제외하고는 모든 경우 금융정보분석원에 세무조사대상자의 금융정보를 요청하여 세무조사에 활용하고 있다. 이 때 심각한 개인정보 노출 문제가 발생하게 된다.

국세청에서는 거의 대부분의 세무조사 대상자의 금융정보를 금융정보분석원에 요청하여 활용하기 때문에, 마찬가지로 거의 대부분의 세무조사 대상자 정보를 금융정보분석원에 이관하게 된다. 금융정보를 요청하기 위해서는 아래와 같은 정보를 명시하여 공문(시스템입력)으로 금융정보분석원에 요청하도록 되어있다.

① 조사대상자 실명번호(주민등록번호, 사업자번호 등)

② 세무조사 대상기간, 세무조사 기간

③ 정보요청사유

④ 정보요청의 근거가 되는 법률

⑤ 정보요청인 목록 등

위 항목에서 보듯이 국세청에서 세무조사 대상자의 금융정보를 확보하기 위해서는 누구에 대하여 어떤 사유로 세무조사를 실시하는지, 또 그 관련인이 누구인지 등 모든 정보를 금융정보분석원에 이관해야만 조사대상자의 금융정보를 확보할 수 있는 것이다.

이는 국세청 뿐 아니라 검찰, 경찰 등 모든 법 집행기관에서도 마찬가지라고 할 수 있다. 검찰과 경찰에서는 수사대상자의 모든 정보를 금융정보분석원에 공개해야만 금융정보를 받아올 수 있고, 선관

위, 관세청도 동일한 경우가 발생한다.

대부분의 정부기관에서는 해당 기관이 취급하는 개인정보를 철저히 보호하고 있다. 세무조사 대상자가 누구인지, 현재 누가 세무조사를 받고 있는지는 절대 공개하고 있지 않다. 검찰의 수사대상자는 누구인지, 내사 대상자는 누구인지 공개하지 않으며, 경찰 등 모든 법집행기관에서도 마찬가지이다. 하지만 현재의 정보교환 방식으로 보면 국내 모든 법 집행기관이 중요한 법집행 대상자의 정보를 금융정보분석원에 공개하고 있는 실정이다.

만약 금융정보분석원의 서버가 해킹의 피해를 입는다면 현재 국내의 모든 세무조사대상자, 세무조사 예정자, 검찰·경찰에서 수사중인 국민에 대한 정보가 노출될 우려가 있다.

5. 소결

결론적으로 현재의 금융거래정보 확보 방식은 각 법집행기관 고유의 비밀 정보를 금융정보분석원에 여과없이 노출하여 금융정보를 가져오게 되므로 많은 문제점을 내포하고 있다. 최근 몇 년 간 법집행기관에서 요청하여 활용하는 금융거래정보가 폭발적으로 증가하고 있는데, 이는 앞으로도 계속 증가할 전망이다.

그러므로 각 법집행기관의 고유업무에 관한 비밀정보 노출의 우려를 최소화하고 만약 해킹피해로 정보가 노출되더라도 식별이 불가능하게 암호화하여 업무에 활용할 수 있는 방안을 모색해야 한다.

Ⅴ. 문제 해결을 위한 착안

1. 기존 교환방식의 핵심 문제점

앞에서 언급한 금융거래정보의 교환방식의 문제점의 핵심사항을 다시 짚어보자.

① 금융정보분석원에 금융거래정보[18] 집중

② 법집행기관에서는 고유업무 수행을 위해 금융거래정보 확보 필요

③ 엄격한 법적 요건을 맞추기 위해 법집행기관 고유의 비밀정보[19]를 적시하여 금융정보분석원에 금융거래정보 요청

④ 금융정보분석원은 법집행기관의 비밀정보를 열람한 후 관련 금융정보 발췌

앞에서도 기술했듯이 기존 금융정보 교환방식의 핵심 문제점은 금융정보분석원이 법집행기관에서 요청한 대상자의 금융정보를 발췌하여 전달하기 위해서는 해당 대상자의 명단과 요청사유를 확인하고 법에 명시된 요건에 부합하는지 확인해야 한다는 데에 있다. 금융정보분석원에서 금융정보 취급에 따른 법적 보안절차를 철저히 지키기 위해서는 다른 기관의 비밀정보를 열람할 수 밖에 없는 딜레마가 생기는 것이다.

2. 동형암호 기술을 이용한 해결책 모색

2-1. 착안점

위에서 살펴본 금융거래정보 취급에 대한 문제점은 모두 민감정보가 평문화 된 상태로 검토된다는 점에서 기인한다. 기관 간 데이터 전송 단계에서는 암호화 된 상태로 전송되지만, 기관 담당자가

18) 의심거래보고정보, 고액현금거래정보, 이 정보로 금융정보분석원이 자체 분석한 정보 등

19) 국세청의 경우 세무조사 대상자, 탈세혐의 분석 대상자, 체납자 등을 말하며, 검찰·경찰의 경우 수사 대상자 등 극히 민감한 개인정보를 뜻함

데이터의 확인을 위해서는 반드시 평문 상태로 검증을 해야만 한다. 이 과정에서 정부기관의 민감정보가 노출되는 현상이 발생한다.

이러한 문제를 해결하기 위해서 가장 중요한 점은 정보의 취급자가 본인이 어떤 정보를 취급하는지 알 수 없어야 하며, 국내 모든 법 집행기관의 민감정보가 취합되는 금융정보분석원에서 보유한 금융정보를 발췌하여 법집행기관에 전달할 때, 해당 작업자가 본인이 어떤 특정인에 대한 정보를 취급하는지 알 수 없는 것이 최선이다. 정보를 요청하는 법집행기관에서도 해당 기관의 민감정보가 노출되지 않아 안심하고 금융정보를 요청하여 활용할 수 있고, 금융정보분석원에서도 개인정보 침해가 발생할 여지가 없다.

현재 상용화된 일반적인 암호화 기술로 위와 같은 검색이 이루어질 수 있을까. 일반 암호화 기술은 데이터를 검색하고 데이터 간 연산을 수행할 때 복화화 과정이 반드시 필요하다. 즉, 암호화 된 데이터베이스를 가지고 있더라도, 해당 데이터베이스 내에서 작업을 하기 위해서는 반드시 복호화 과정을 거쳐야하고, 복호화 된 평문 데이터를 가지고 각종 작업을 수행해야만 한다. 본 논문에서 가장 쟁점이 되는 부분이 바로 복호화 된 데이터의 보안성 문제인데, 이러한 점에서 볼 때 일반 암호화기술로는 해결될 수 없을 것이다.

강조한 것처럼 논점에서 가장 중요한 점은 암호화 된 상태에서 데이터 검색 및 연산이 이루어져야 한다는 사실이다. 본 논문에서는 이러한 점을 동형암호를 이용하여 적용방안을 연구해본다.

2-2. 암호화의 개요[20)]

암호는 간단히 말해서 사용자가 안전하지 않은 네트워크나 저장

20) 천정희 외 2, 개인정보가 보호되는 동형암호기반 금융데이터분석(2018) 내용 중 인용

소에 데이터를 안전하게 공유하는 방법이다. 암호알고리즘은 키 생성, 암호화와 복호와의 세 단계로 이루어지는데, 키 생성 단계에서는 암호화키와 복호화키를 생성하고 암호화 과정에서는 평문에 암호화키를 적용하여 암호문으로 바꾸며 복호화 과정에서는 암호문에 복호화키를 적용하여 원래의 평문을 복구한다. 암호화키와 복호화키가 동일한 경우를 대칭키암호(symmetric key encryption)라 하고, 동일하지 않은 경우를 비대칭키 암호(asymmetric key encryption) 혹은 공개키암호(public key encryption)라고 한다.

공개키 암호가 나오기 전에는 암호를 주고받는 두 명의 사람 사이에 비밀키를 먼저 설정하여 공유하고 암호화 된 정보를 공유할 수 밖에 없었다. 이런 방식은 예전의 작은 사회규모에서는 사용이 가능하겠지만 오늘날과 같이 대규모 네트워크환경을 기반으로 하는 전 세계적인 통신이 가능한 시대에는 사용할 수 없는 방식이다. 때문에 공개키 암호화 방식이라는 새로운 기술이 도입되었다. 공개키 암호 기술은 암호화키를 공개하여 누구나 암호화를 할 수 있지만, 복호화 키는 비밀로 하기 때문이 특정 복호화키를 소유하는 사람만이 복호화가 가능하여 암호화된 정보를 알 수 있게 된다. 이러한 비밀키 알고리즘은 두 당사자 간에 비밀키를 공유하지 않고도 안전한 통신이 가능하게 한다. 이 때 보통 암호화키를 공개키, 복호화 키를 비밀키라고 부른다.

공개키 암호의 안전성 모델은 매우 엄격하여 기반문제가 안전한 경우 공격자가 고른 두 개의 평문중 하나를 암호화시켜서 주고 이것이 어느 평문의 암호문인지를 맞추게 하는 게임에서 승률이 1/2보다 크게 높지 않아야 하며, 정량적으로는 안전성 지수가 λ인 암호의 경우 추가승률이 $1/2^{\lambda}$ 이상이 되지 않아야 한다. 이 과정에서 공격자가 원하는 평문은 마음대로 암호화 해볼 수 있다고 가정해도 구

분이 불가능한 경우를 선택평문공격에 대한 구별불능 안전성이라고 하고, 복호화 과정에 대한 힌트를 얻기 위해 문제로 주어진 암호문 이외의 임의의 암호문에 대한 복호화 요청에도 구분이 불가능한 경우를 선택암호문에 대한 구별불능안전성이라고 한다.

2-3. 기존 암호화의 문제점[21)]

현대 사회에서 일반적으로 사용되는 암호는 엄격한 안전성을 바탕으로 안전성 가정에 맞추어 적절히 사용한다면 수학적으로 안전성을 보장한다. 암호의 안전성은 당연히 비밀키가 안전하게 보관되어야 한다는 것이 중요하다. 이 문제는 최근 컴퓨터와 인터넷의 발달로 암호의 사용이 매우 빈번해지고 이에 따라 비밀키를 사용해야 하는 일이 많아지면서 공격자가 비밀키를 획득할 가능성이 더욱 커지고 있다는 점에서 매우 중요한 문제이다. 실제로 Snowden이 발표한 리포트(The Washington Post. 2013.6.10.)에서는 미국 NSA에서 악성코드 등을 통해 세계 각 나라의 암호에 쓰이는 비밀키를 획득하고 이를 이용하여 주요 정보들을 해독하여 수집하고 있다고 폭로하고 있다.

기업이 보관하고 있는 데이터 역시 암호화하면 안전성이 높아질 것이라고 기대하지만 현실에서는 그렇지 않은 경우가 많다. 우리나라에서는 개인정보보호법에 따라 주민번호 암호화 의무조치를 시행하고 있지만 개인정보 유출사고는 끊이지 않고 있다. 이는 저장된 데이터를 활용할 때마다 복호화를 해야하고 그 때마다 비밀키를 꺼내야 하는데 이 때 악성코드 등을 이용하는 해커에게 비밀키가 탈취될 수 있기 때문이다.

---

21) 천정희 외 2인의 위 논문 인용

이에따라 비밀키의 사용빈도를 줄이기 위해 비밀키 없이도 암호화한 상태로 여러 가지 연산을 수행할 수 있는 암호가 현대암호학의 주요 연구목표가 되었다. 이 경우 사용자가 데이터를 볼 때에는 비밀키가 필요하나 그 이외에는 비밀키를 이용하지 않고 처리함으로써 비밀키를 안전한 곳에 보관할 수 있고 해커의 공격에 대비할 수 있는 것이다.

2-4. 동형암호 기술

위에서 서술했듯이 최근 현대사회에서는 보편적으로 수많은 사람들이 다양한 정보를 활용하기 위한 암호와 방법으로 공개키 암호를 사용하고 있다. 공개키 암호는 암호키와 암호를 해독하는 복호화키 중 암호화키를 외부에 공개하여 상대방은 공개된 암호화키를 이용하여 정보를 보내고, 자신은 자신만이 가진 복호화키를 이용하여 수신된 정보를 해독할 수 있도록 한 정보 암호화 방식이다.

공개키 암호방식의 경우는 키의 크기가 크고, 또한 각 키는 특수한 성질을 요구하기 때문에 비밀키 암호화 방식의 키와 같이 사용자가 직접 원하는 키를 만들지는 못한다. 많이 사용되는 공개키 암호방식의 키 크기는 높은 안전성을 갖도록 하기 위하여 현재 사용되는 공개키 암호 방식 보안 제품 중 RSA는 1,024bits의 키를 사용하고 있다.[22)]

그러나 암호화된 데이터를 대상으로 직접적으로 필요한 자료를 검색하거나 통계적으로 처리, 가공하는 것이 불가능하다. 따라서 서버에 저장된 데이터를 이용하여 작업을 수행하기 위해서는 먼저 암호화된 상태로 보관중인 데이터를 일시적으로 복호화 한 뒤 작업을

22) 두산백과 [공개키 암호방식]

해야 하는데, 그 과정에서 비밀키나 복호화된 자료가 서버 관리자에 의해 임의로 저장되거나 해커에 의해 유출될 수 있다[23].

이에 따라 암호화된 데이터를 대상으로 이를 복호화하지 않은 상태로도 사용자가 검색을 하거나 통계처리와 같은 연산을 할 수 있게 하는 암호체계인 완전동형암호(Fully Homo-morphic Encryption) 기술에 대한 연구가 활발히 진행되었다.

동형(homomorphic)이라는 용어는 수학에서 다루는 동형성(homomorphism)에서 온 것으로 이는 연산이 정의된 두 개의 집합 사이의 연산을 보존하는 맵핑을 말한다. 즉, 동형암호는 평문 공간과 암호문 공간이라는 두 개의 집합에서 대표적인 연산인 덧셈, 곱셈을 보존하는 암호체계이다[24].

평문 m1과 m2의 암호문을 각각 c1=E(m1), c2=E(m2)라고 하고, E를 암호화 함수라고 정의할 때, 일반적인 공개키 암호 시스템에서는 비밀키가 없다면 암호문인 c1, c2만으로는 평문에 대한 아무런 정보를 얻을 수가 없다. 그러나 평문에 연산을 한 뒤 암호화한 값이나 평문을 암호화를 한 암호문을 연산한 값이 같게 되는 동형암호 체계에서는 비밀키가 없어도 아래와 같이 암호문만으로도 평문에 대한 연산 결과를 암호화한 값을 얻을 수 있게 된다.

$E(m1+m2)=E(m1)+E(m2)=c1+c2$

$E(m1\times m2)=E(m1)\times E(m2)=c1\times c2$

여기서 나아가 상수곱, XOR, AND 등의 모든 논리 연산을 횟수 제한 없이 보존하는 암호체계를 완전동형암호[25]라고 한다.

---

23) 정명인, 완전동형암호 기술의 연구 동향. 한국과학기술정보연구원, 한국콘텐츠학회논문지 13권 8호, 2013. 37면
24) 정명인의 위 논문, 38면
25) 정명인의 위 논문, 38면

컴퓨터가 하는 모든 연산은 AND, OR, NOT과 같은 논리연산의 합성으로 이루어져 있으므로, 위 논리연산만 암호화된 상태에서 수행할 수 있으면 이를 반복하여 임의의 연산을 암호화한 상태에서 수행할 수 있게 되므로, 완전동형암호 기술은 암호화된 데이터를 이용하여 컴퓨터로 가능한 모든 연산을 수행할 수 있게 해준다[26]. 따라서 평문에 특정한 단어가 포함되어 있는지, 평문에 특정 개인정보가 포함되어 있는지에 대하여 암호화된 상태의 암호문으로도 검색하는 것이 가능하다.

완전동형암호는 암호화된 상태의 데이터에 대해서도 컴퓨터로 할 수 있는 모든 연산을 원하는 대로 수행할 수 있으므로 검색이나 통계적인 분석뿐만 아니라 기계학습이나 영상처리 등 매우 복잡한 연산에도 적용할 수 있다는 장점이 있다. 다만, 완전동형암호는 컴퓨터가 하는 모든 연산을 암호화한 상태로도 수행할 수 있는 이론적 강점이 있는 반면 평문연산에 비해 암호문 연산의 효율성에서는 떨어진다는 단점이 있다. 그러나 응용 연산의 종류에 따라 속도의 차이가 크기 때문에 개별 연산에 대하여 최적화하여 적용하는 방법으로 효율성을 높일 수 있다. 또한 동형암호 연구가 아직은 초기단계이므로 알고리즘의 개발에 따라 효율이 크게 향상될 여지가 있다. 예를 들면, 동형암호 연산 중에 가장 비효율적인 재부팅시간이 2011년도에는 30분이었던 것이 2013년에는 0.32초, 2015년에는 0.02초까지 계산속도가 빠르게 개선되고 있다[27].

결론적으로, 암호화된 데이터로 다양한 연산을 하거나 이를 바탕으로 키워드 검색을 수행하더라도 굳이 평문을 알 필요가 없으므로 평문이 유출될 위험이 없다. 이것이 동형암호 기술이 개인정보 보호에 유용한 이유이다.

---

26) 정명인의 위 논문, 39면
27) 천정희 외 2, 개인정보가 보호되는 동형암호기반 금융데이터분석(2018) 내용 중 인용

Ⅵ. 동형암호 기술을 이용한 금융거래정보 교환방식

1. 금융거래정보 교환에서의 동형암호 적용개념

위에서 보았듯이 동형암호는 복호화하지 않고 암호화 된 상태에서 컴퓨터로 할 수 있는 모든 연산을 수행할 수 있으므로 비밀키 노출의 우려가 매우 적다. 또한 외부로의 비밀키 노출에 따른 개인정보 유출 뿐만 아니라, 정부기관 간 데이터 교환을 위한 정보검색 과정에서 복호화 된 데이터를 보고 작업하는 공무원의 데이터 확보 또한 불가능하다. 이런 특징을 가진 동형암호는 각자 고유의 민감정보를 가지고 해당 고유업무를 수행하는 정부기관 간 데이터 공유에 반드시 필요한 부분이라고 할 수 있다. 다만, 현재 가장 많이 사용되는 공개키 암호화 방식으로는 작업 전 복호화가 필수로 선행되어야 하므로 불가능한 작업방식이기 때문에 사용할 수 없었다.

이번에는 민감한 금융거래정보가 집중되어있는 금융정보분석원의 데이터베이스를 암호화하고, 각 정부기관 간 정보교환을 동형암호를 적용하여 진행하는 방식을 논하여본다.

2. 정부기관 간 데이터베이스 암호화 방안

정부기관 간 금융거래정보를 교환하는 방식을 동형암호화 하는데 있어, 우선적으로 선행되어야 할 것은 금융거래정보가 집중되어있는 금융정보분석원의 금융거래정보 데이터베이스를 암호화 하는 것이다. 가장 큰 문제점으로 지적되는 부분이 금융정보분석원에서 각 정부기관의 민감정보를 여과없이 볼 수 있다는데 있으므로, 모든 정보를 암호화 된 상태에서 작업을 할 필요가 있다.

동형연산을 위해서는 각 데이터베이스는 동일한 키로 암호화 되어야 하는데, 이를 위해 신뢰할 수 있는 인증기관을 통해 공개키 pk

와 비밀키 sk를 생성한다. 데이터의 복호화에 필요한 비밀키 sk는 $sk=sk_A+sk_B$를 만족하도록 sk_A와 sk_B를 랜덤하게 잡아서 두 기관이 각각 비밀키 sk_A와 sk_B를 나누어 가진다[28]. 금융정보분석원은 보유하고 있는 금융거래정보 데이터베이스를 공개키 pk로 동형암호화하여 운영한다. 이 때 금융정보분석원에서 자체적인 분석을 위해 운영하는 데이터베이스는 암호화 할 필요는 없고, 타 정부기관에서 금융거래정보를 요청했을 때 해당 대상자의 금융거래정보를 검색하여 발췌하는데 사용할 데이터베이스를 별도로 동형암호화하여 운영하여야 한다. 다시말해 자체 운용 서버와 금융기관 간 정보교환에 사용하는 서버는 철저히 독립적으로 운영되어야 한다는 것이다. 이렇게 암호화된 데이터는 동형암호의 성질에 의해서 암호화된 채로 컴퓨터가 알 수 있는 모든 연산을 수행할 수 있고, 비밀키가 sk_A와 sk_B로 분리되어 있어 어느 한 기관의 비밀키로는 데이터를 복호화 할 수가 없으므로 기밀성이 철저히 유지된다고 할 수 있다[29].

3. 비밀키 생성 및 보관의 주체

일반적으로 모든 암호화 작업에서는 비밀키의 관리가 가장 중요하다. 암호화된 정보를 모두 평문화 할 수 있는 비밀키는 암호화 방식에 따라 관리하는 주체가 다르지만, 신뢰할 수 있는 인증기관이 생성하고 관리하는 방법을 보편적으로 사용할 수 있을 것이다.

일반 암호의 경우 비밀키를 사용하여 복호화 과정을 거친 후 평문화된 데이터를 기반으로 검색과 연산 작업을 수행하지만, 동형암호의 경우 비밀키 없이 동일한 연산을 수행할 수 있다.

---

28) 천정희 외 2, 개인정보가 보호되는 동형암호기반 금융데이터분석(2018) 내용 중 인용

29) 천정희 외 2, 개인정보가 보호되는 동형암호기반 금융데이터분석(2018) 내용 중 인용

위와 같이 동형암호를 사용할 경우 비밀키 없이 필요한 연산을 수행할 수 있지만, 정부기관 간 안전한 금융거래정보 교환을 위해 금융정보분석원과 각 법 집행기관 간 비밀키의 생성자와 보관자는 어떻게 될 것인지 생각해 볼 필요가 있다.

우선 금융정보분석원을 정보제공자라고 하고 법집행기관을 정보요청자라고 한다면, 암호화 된 데이터를 취급하는 곳과 복호화 된 데이터를 취급하면 안되는 곳, 복호화 된 데이터를 취급하는 곳을 나누어 볼 수 있다.

① 암호화 데이터 취급자 : 정보요청자, 정보제공자

② 복호화 데이터 취급자 : 정보요청자

③ 복호화 데이터 취급불가 : 정보제공자

먼저 정보요청자는 자신들의 민감한 보안정보를 정보제공자에게 온전히 전송해야만 필요한 데이터를 받을 수 있기 때문에 정보를 암호화하여 전송한다. 정보제공자는 정보요청자가 제공한 암호화된 정보를 가지고, 정보제공자 본인의 암호화 서버에서 필요한 작업을 수행한다. 이 때 정보요청자와 정보제공자는 동일한 비밀키로 암호화(동형암호화) 된 데이터베이스에서 작업을 해야 하며, 정보제공자는 정보요청자가 제시한 민감정보를 전혀 몰라야 한다. 이렇게 발췌한 정보를 정보요청자에게 다시 보내주는데, 정보요청자는 작업 결과물을 암호화된 상태로 수보하여 이를 복호화 하여 업무에 사용하게 된다.

3-1. 비밀키의 보관 : 정보요청자

위의 과정에서 정보제공자는 정보요청자가 제시한 정보를 알아서도 안되고, 알 필요도 없으므로 복호화 데이터를 취급할 필요가 전혀 없다. 만약, 정보요청자와 정보제공자 두 기관 사이에 비밀키를 누가 가지고 있어야 하느냐는 문제가 생긴다면 답은 여기에서 찾을 수 있을 것이다. 정보요청자는 본인들에 요청한 금융정보를 업무에 활용하기 위해서 복호화 과정을 거쳐야 하고, 정보제공자는 요청한 정보를 검색하여 회신하는 역할에만 한정되기 때문에 복호화 프로세스를 가질 필요가 없는 것이다. 이는 정보요청자의 민감정보를 전혀 외부로 노출시킬 필요가 없기 때문에 매우 바람직한 모델이라고 할 수 있다.

3-2. 비밀키의 보관 : 신뢰할 수 있는 기관

비밀키를 신뢰할 수 있는 기관이 관리하는 방법은 정보요청자만 비밀키를 가지고 있을 경우 정보제공자의 데이터베이스가 암호화 되어있다고 하더라도 정보요청자가 전체를 복호화 할 수 있을 것이라는 불안감이 생길 때 사용할 수 있는 방법이다.

정보요청자와 정보제공자가 모두 서로를 통제하고 싶을 때는 비밀키를 신뢰할 수 있는 기관에 위탁하여 필요한 경우에만 허가를 받아 복호화하여 사용한다. 이때 반드시 필요한 절차는 복호화 하는 기관에서 비밀키를 받아서 사용한 기록을 남겨놓아야 한다는 것이다. 신뢰할 수 있는 기관에서 비밀키를 관리하는 정책을 사용하는 것의 전제는 정보제공자와 정보요청자를 동등한 입장에서 보고, 서로 정보에 접근하는 경로를 견제하겠다는 의미가 크기 때문에 누가 언제 비밀키를 사용하는지 철저한 기록관리가 필요하다.

3-3. 비밀키의 보관 : 비밀키 분산(정족수 완전동형암호[30])

비밀키의 생성 및 관리를 정보요청기관이 전담하는 것 보다는 신뢰할 수 있는 기관에게 위임하여 활용하는 것이 보안성 측면에서는 더 높다고 할 수 있다. 이 절에서는 더욱 높은 보안성을 보여줄 것으로 생각되는 정족수 완전동형암호를 활용한 비밀키 분산 방법에 대하여 논해본다.

정족수 완전동형암호는 Asharov 등이 Eurocypt 2012에서 learning with errors(LWE) 문제를 기반으로 하여 제안한 방식이다. n개의 참여자들 간에 수직적인 상하구조가 없도록 탈중앙화 동형암호를 설계하였으며 이 때 복호화는 구성원의 참여자들이 모두 만장일치로 동의해야만 한다.

즉, 완전한 비밀키를 어느 한 기관에 맡겨놓는 방식에서 탈피하여, 비밀키를 분산한 후 정보요청자, 정보제공자, 신뢰할 수 있는 기관과 같이 서로 견제가 가능한 세 개의 기관서 관리하도록 하는 것이다. 비밀키가 나뉘어져 있기 때문에 어느 한 기관에서 가진 일부의 비밀키를 가지고서는 완전한 복호화가 불가능하고, 복호화 과정이 필요한 경우 세 기관 모두 만장일치로 동의하여 비밀키를 결합[31]한다면 완전한 비밀키로 복호화가 가능한 방식이다.

세 가지 방법 중 가장 보안성이 높은 방식이며, 정보제공자와 정보요청자가 서로의 기관을 견제하면서 민감정보 노출 없이 정보를 교환할 수 있는 방식이다.

4. 암호화 데이터베이스의 검색방식 개선

동형암호는 정보교환 시 민감정보 노출을 방지하는데 탁월한 대

---

30) 정진혁, 가변적인 정족수 완전동형암호와 키 생성 프로토콜을 통한 탈중앙화에 관한 연구 참조

31) $sk = sk_A + sk_B + sk_C$ 로 완전한 비밀키 생성

안이 될 수 있는 암호화 방식이다. 즉, 컴퓨터가 하는 모든 연산을 암호화한 상태로도 수행가능하지만, 평문 연산에 비해 연산 효율성이 떨어진다는 단점이 있다. 그러나 이는 연산의 종류에 따라 속도의 차이가 크기 때문에 개별 연산에 대하여 최적화하여 적용하는 방법으로 효율성을 높일 수 있는 부분이다[32].

[표8. 공개키 암호와 동형암호의 성능 비교]

	공개키 크기	암호문 크기	평문 크기	암호화 시간	복호화 시간	덧셈 시간	곱셈 시간	허용 depth	안전성
RSA	2048bit	2048bit	-	6.1ms	205.5ms	-	-	-	-
ECC	193bit	80B	-	8.7ms	18.1ms	-	-	-	-
Helib[6]	343KB	105KB	≤1KB	17ms	6ms	0.6ms	54.3ms	6	128bit
SEAL2.4v[7]	2000KB	224KB	≤1KB	5.9ms	1.6ms	0.2ms	24ms	9	128bit
HEAAN[8]	80KB	96KB	16KB	43ms	12ms	5ms	100ms	6	128bit

금융거래정보 교환에 동형암호를 사용할 경우, 아래의 금융거래정보 구성 예시를 보고 검색연산에 필요한 시간을 단축하는 방법을 생각할 수 있을 것이다.

[표9. 고액현금거래정보 예시]

거래자	실명번호	거래일자	거래일시	금융회사	거래수단	거래금액	상대회사	수취인계좌	수취인
홍길동	8101281000000	2020-09-23	13:13:27	우리은행	현금	30,000,000	신한은행	10021290000	성춘향
홍길동	8101281000000	2020-09-23	13:15:31	우리은행	현금	13,000,000	농협	3120033222	김홍자
홍길동	8101281000000	2020-09-23	13:17:20	우리은행	현금	52,000,000	농협	3120033222	김홍자

위의 고액현금거래정보에서 정보교환 시 가장 중요한 필드는 무엇인가. 아마도 거래자 실명과 실명번호일 것이다. 정보제공자가 암호화 데이터베이스를 준비할 때, 위의 전체 필드를 대상으로 암호화를 하여 사용하고 정보요청자가 제시한 명단에 대해 암호화 데이터베이스를 검색한다면 많은 시간이 걸릴 것이다. 때문에 효율적인 연

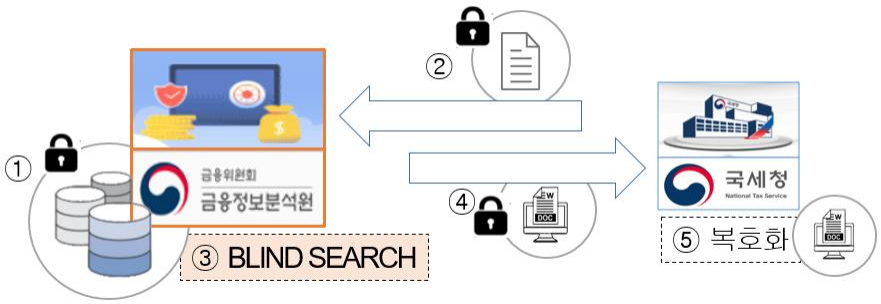
32) 천정희 외 2인, 위 논문에서 참고

산과 빠른 검색시간을 보장하기 위해서는 일정 필드만 암호화하여 연산에 사용하는 방식이 필요하다.

따라서 정보제공자가 완전동형암호화 된 데이터베이스를 구축할 때에는 위 금융거래정보의 예시에서 나오는 바와 같이 거래자 성명, 거래자 실명번호에 대해서만 동형암호화 하고, 나머지 필드는 정보요청자가 제시한 명단과 암호화 명단을 검색하는 암호화 연산 이후에 매칭시켜 데이터를 완성하는 방식을 사용하는 것이 유리하다.

5. 동형암호 적용 금융거래정보 교환 시스템 제안

위에서 논의한 내용을 바탕으로 정부기관 간 동형암호를 적용한 금융정보거래 시스템을 아래와 같이 구축할 수 있다.



① 정보제공기관에서 보유한 금융정보를 동형암호화 하여 데이터베이스 구축한다.

② 정보요청기관에서는 정보요청 대상자의 명세를 동형암호화하여 정보제공기관에 전달한다.

③ 정보제공기관은 동형암호화 데이터베이스를 바탕으로, 동형암호화 된 요청명단과 매칭하여 검색작업을 수행한다. 이 단계에서는 정보제공기관의 작업자가 정보요청기관이 정보제공을 요

청한 대상자의 명세를 알 수 없기 때문에 의도치 않는 민감정보 노출이 원천 차단된다.

④ 정보제공기관은 ③번 단계에서 검색한 결과물(금융거래정도 등)을 암호화 상태로 정보요청기관에 제공하게 된다.

⑤ 정보요청기관은 전송받은 금융거래정보를 복호화 하여 수사, 세무조사, 체납징수 등 고유 업무에 사용한다.

Ⅶ. 결론

최근 미국의 금융정보분석원인 FinCEN[33]이 관리하는 2100여건에 달하는 글로벌 5대 은행들의 의심거래활동보고서가 유출되어 전 세계적으로 큰 파장이 일어났던 사건이 발생[34]했다. 이 정보유출 사건은 미국 금융계에 큰 파장을 일으키고 관련 은행 주식이 폭락하는 등 미국 증시에 까지 영향을 미쳤다. 이처럼 민감한 정보 유출, 특히 금융거래와 관련한 정보의 의도치 않은 노출은 전 세계적으로 큰 충격이 될 소지가 다분하다.

만약 FinCEN에서 관리하던 정보가 동형암호 방식으로 암호화되어 있었다면 유출로 인한 피해가 지금처럼 크지는 않았을 것으로 생각된다. 기관 자체적으로는 복호화를 위한 비밀키를 가지고 있지도 않고, 혹시 부분 비밀키를 가지고 있다 하더라도 완전한 복호화를 위해서는 다른 기관의 비밀키가 추가로 필요하기 때문에 평문이

33) FinCEN : 미국 재무부산하 기관으로 1990년 설립되었으며 불법 자금세탁 등 미국 및 국제적 금융 범죄를 방지하기 위해 관련 정보를 수집, 분석하여 보고서를 제출하는 기관. FInCEN의 의심활동 보고서는 은행 등 금융기관의 불법적인 활동이나 거래를 감시하고 적발하는 보고서로 노출된다면 금융기관의 신뢰도에 결정적인 영향을 미칠 수 있음.

34) “은행들 2조달러 불법 거래 관여” 핀센(FinCEN) 유출 파장 (뉴스핌 외, 2020.09.21.)

그대로 유출될 가능성은 없다.

지금처럼 개인정보가 모두 전산화되어 관리되는 사회에서는 개인정보의 유출로 인한 피해가 막심하며, 특히 정부기관에서 관리하고 사용하는 개인정보는 매우 민감한 정보가 포함되어 있을 가능성이 높다. 정부기관의 정보유출 방지를 위해서는 동형암호 기술을 이용한 암호화 방식이 대안이 될 수 있을 것이다.

[참고문헌]

□ 국내 연구자료

홍익대학교, 금융거래정보의 국세행정 활용실태 및 개선방안 연구, 2019
금융정보분석원, 자금세탁방지 2018 연차보고서, 2018

□ 국내 출판자료

금융정보분석원, 자금세탁방지 2018 연차보고서, 2018
국세청, 국세통계연보 2019

□ 국내 논문

천정희 외 2, 개인정보가 보호되는 동형암호기반 금융데이터 분석, 2018
정명인, 완전동형암호 기술의 연구 동향, 2013
정진혁, 가변적인 정족수 완전동형암호와 키 생성 프로토콜을 통한 탈중앙화에 관한 연구, 2019

□ 해외 자료

OECD, Effective Inter-Agency Cooperation in Fighting Tax Crimes and Other Financial Crimes, 2017