Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1191

금융 클라우드의 데이터 국지화에 대한 비판적 고찰

장 우 경,† 김 인 석‡
고려대학교 정보보호대학원

A Critical Review on Data Localization in the Financial Cloud

Woo-Kyung Jang,† In-Seok Kim‡
Graduate School of Information Security, Korea University

요 약

정부는 2019년 1월 금융 분야의 클라우드 이용 활성화를 위해 전자금융감독규정을 개정하였다. 하지만 클라우드 정책 및 규제들이 금융회사들의 자율적인 보안활동을 저해하거나 국민의 기본권을 일부 제한할 수 있어 금융권에서는 중요정보를 클라우드로 이용하려는 움직임이 거의 나타나지 않고 있다. 또한, 중요정보는 국내에만 두도록 하는 데이터 국지화 정책은 클라우드 이용 활성화를 가로막는 대표적인 규제이며, 이는 해외 사업자에 대한 차별문제도 야기시킨다. 따라서 데이터를 통해 디지털 금융혁신 기반을 제공할 클라우드를 활성화하기 위한 정책 및 규제 개선이 필요하다. 본 연구는 국내외 금융회사에 대한 클라우드 정책현황을 알아보고 국내 금융회사에 대한 정책 및 규제들을 분석하였다. 이를 통해 국내 금융회사에 대한 클라우드 정책의 한계와 문제점을 도출하고 금융회사의 클라우드 이용 활성화를 위한 데이터 국지화 규제 개선방안 등 정책적 대안을 제시하고자 한다.

ABSTRACT

In January 2019, the government revised the regulation on electronic financial supervision to revitalize the use of cloud in the financial sector. However, as cloud policies and regulations cloud undermine financial firms' autonomous security activities or restrict some of the people's basic rights, there has been little movement in the financial sector to use important information as the cloud. In addition, the data localization policy, which requires important information to be kept only in Korea, is a representative regulation that prevents the revitalization of cloud use, which also creates discrimination problems for overseas operators. Therefore, policy and regulatory improvements are needed to enable the cloud to provide a foundation for digital financial innovation through data. This study looked into the current status of cloud policies for domestic and foreign financial companies and analyzed policies and regulations for domestic financial companies. Through these efforts, the government aims to draw up limitations and problems in cloud policies for domestic financial companies and propose policy alternatives, such as measures to improve regulations on localizing data for financial companies to revitalize their use of cloud.

Keywords: Cloud Computing, Data Localization, Information Security, Improvement of Regulations

I. 서 론

정보통신기술(internet and communication technology)이 발전함에 따라 인공지능, 사물인터넷(IoT), 빅데이터, 클라우드 등의 기술이 등장하게 되었다. 이러한 정보기술을 바탕으로 IT 융·복합 환경이 급속하게 변화하였고, 대량으로 생성되는 데이터를 처리하기 위해 기존 인터넷 데이터 센터에서 클라우드 데이터 센터로 전환이 이루어지고 있다[1]. 글로벌 IT 기업들은 전 세계적으로 클라우드 데이터

Received(07. 11. 2019), Modified(08. 09. 2019), Accepted(08. 27. 2019)
† 주저자, wjang79@korea.ac.kr
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

센터를 증가시키는 추세이며, 클라우드 시장 공략을 위해 해당 지역에 리전 형태의 데이터 센터도 만들고 있다. 우리나라도 최근 공공과 금융 분야에서 클라우드 관련 규제를 완화함에 따라 아마존, MS, 구글 등 글로벌 IT 기업들이 국내에 대규모 클라우드 데이터 센터를 구축 중에 있고, 국내 포탈기업도 자체 클라우드 데이터 센터를 통해 글로벌 IT 기업과 경쟁을 시작하려는 추세이다.

가트너에 따르면 17년부터 21년까지 전 세계 공용 클라우드 시장이 연평균 약 17.6%씩 성장하며, 국내 공용 클라우드 시장은 2021년까지 연평균 20.5% 증가할 것으로 전망하고 있다. 또한, 기업들의 멀티 클라우드 및 하이브리드 클라우드에 대한 수요가 증가함에 따라 IaaS와 PaaS의 통합 서비스에 대한 수요가 늘어날 것이며 이에 따라 향후 클라우드 시장의 성장은 IaaS와 PaaS가 주도할 것으로 보고 있다[2]. 이에 반해 국내에서는 SaaS가 전체 시장의 43.4%를 점유하여 가장 큰 비중을 차지할 것으로 예상하고 있다[2].

한편, 클라우드 사용이 증가함에 따라 보안 사고도 계속 발생하고 있다. 과거에는 주로 하드웨어 등의 시스템 오류부터 관리자에 의한 실수가 주로 발생했으나 최근에는 해킹 등 외부요인에 의한 사고도 발생하고 있다. 18년 11월에는 전 세계 1위 퍼블릭 클라우드인 아마존웹서비스(AWS)에서 장애가 발생하였다. 장애는 국내 서울 리전에서만 발생한 것으로 일본, 싱가포르 등의 리전을 동시에 이용하는 멀티 클라우드를 적용한 기업은 장애가 발생하지 않았다. 비록 보안 사고는 아니었지만 클라우드 데이터 센터 장애로 서비스가 중단되면서 금융 분야에서는 클라우드 이용 확대에 대한 고민을 할 수 밖에 없게 되었다. 클라우드를 이용하려는 금융회사는 서비스 중단에 대비한 백업정책을 수립해야 하며, 정부나 감독당국은 국내외 클라우드 사업자들에 대한 규제 및 정책을 정비할 필요가 있다.

금융권에서는 최근 전자금융감독규정을 개정하여 클라우드 규제를 완화하였으며, 고유 식별정보 등 금융회사의 민감한 정보들도 클라우드 데이터 센터에서 관리를 할 수 있게 되었다[3]. 그러나 국내 금융회사의 클라우드 이용에 대한 전자금융 감독 및 정책은 해외 사업자에 대해 국내 사업자와 동등한 조건에서의 서비스 제공을 어렵게 만들고 있다. 국내 이용자의 데이터 주권 보호를 위해 이용자 정보를 국외로 이전하는 것을 제한하는 데이터 국지화 규제는 비용문제, 대리인 지정 및 관리, 국내인증 획득 등 해외 사업자에 대한 차별을 야기함으로써 금융회사들의 클라우드 활성화를 제한하는 대표적인 경우이다.

본 연구에서는 국내외 금융회사에 대한 클라우드 정책 현황을 살펴보고 국내 금융회사에 대한 정책 및 규제들을 분석하였다. 그 중 국내 금융회사의 클라우드 확대 관련한 데이터 국지화 규제 정책을 진단하여 금융 분야에서의 클라우드 이용 활성화를 위한 데이터 국지화 규제 개선방안을 제시하고자 한다.

II. 금융 클라우드 정책 및 규제현황

2.1 국내현황

2.1.1 정보처리 위탁제도 개선

2015년 7월 정부는 「금융회사의 정보처리 업무 위탁에 관한 규정」을 개선하여 금융회사 이외의 제3자에게 정보처리 업무 위탁이 가능하도록 하였다. 금융업의 본질적 업무는 위탁을 금지하되 기존의 포괄적이고 단순했던 본질적 업무는 상세히 규정하였다. 이 규정에서는 클라우드 컴퓨팅 서비스의 위탁 가능여부는 명확히 규정하지 않았고 명시적인 규정도 존재하지 않았다[4].

2.1.2 금융감독원의 전자금융 감독규정 개정

금융감독원은 2016년 10월 비중요 정보처리시스템 지정 관련하여 전자금융감독규정을 개정하였다. 금융회사 및 전자금융업자는 클라우드 컴퓨팅 이용을 위해 고객정보를 처리하지 않는 정보처리시스템 등 전자금융거래에 미치는 영향이 낮은 시스템을 비중요 정보처리시스템으로 지정할 수 있도록 하였다. 해당 시스템은 물리적 망분리 등 클라우드 이용이 제한되는 규정이 적용되지 않았지만, 개인 신용정보와 고유식별정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정이 불가하도록 하였다.

이 개정으로 금융권의 클라우드 이용 활성화와 변화된 현실에 맞도록 합리적으로 규제를 개선하고자 하였지만, 전자금융거래에 미치는 영향이 낮은 시스템에 대한 명확한 기준이 없었다. 그리고 금융회사 자체적으로 비중요 정보처리시스템을 지정할 수 있는 것처럼 보이지만 금융보안원의 「금융권 클라우드 서비스 이용가이드」를 제시하고 있어 자율적인 규제가

형식적으로 운영될 위험성이 크다는 문제점도 있었다[4].

금융위원회는 최근 금융 분야의 디지털화가 폭넓게 확산되고 클라우드 이용 확대 관련한 추가 규제 완화 필요성이 지속적으로 제기됨에 따라 금융회사가 자율적으로 안전하게 클라우드를 활용할 수 있도록 19.1.1일부터 전자금융 감독규정을 개정 시행하였다. 과거 비중요 정보만 클라우드에서 처리하도록 하였으나, 고유 식별정보, 개인 신용정보 등 중요 정보도 클라우드에서 이용 가능하도록 허용하였다. 금융회사가 별도의 안전성 기준을 수립하고 자체 정보보호위원회에서 안전성을 평가하도록 하는 등 내부통제 절차도 강화하였다. 또한, 정보의 중요도에 따라 클라우드 이용현황을 감독당국에 보고하는 등 감독을 강화하였으며, 개인 신용정보 처리는 국내 소재 클라우드에 한해 허용하도록 하였다[3].

2.2 해외현황

2.2.1 미국

미국은 검사협의회(FFIEC)에서 2012.7월 발표한 「아웃소싱 클라우드 컴퓨팅」을 통해 금융권의 클라우드 이용 시 유의사항을 명시하고 있다. 주요내용으로는 금융기관의 데이터 무결성, 기밀성 보호를 위한 통제사항 확인, 재해복구(DR), 업무연속성 계획(BCP) 적절성 확인 등이 있다. 소비자 데이터가 국외에서 저장 또는 처리될 경우 해당 국가의 관련 규정을 확인해야 하며, 계약 시 금융기관의 프라이버시 관련 책임과 보안사고 시 보안의무, 정보유출 시 보고 의무 등 법적 의무도 명시하고 있다[5]. 또한, 클라우드 서비스 또는 제품에 대한 보안성 인증심사 및 도입 승인 과정을 통합하여 수행하는 정부기관 공통의 클라우드 서비스 인증심사 제도인 연방 위험승인 관리 프로그램(FedRAMP)를 활용하고 있다[6].

2.2.2 유럽(EU)

EU 산하의 유럽은행청(European Banking Authority)에서는 클라우드 이용자 유의사항 등을 명시한 「클라우드 제공자 업무 위탁에 대한 권고」를 발표(18.7월 발효)하였다. 이 권고는 기존 유럽은행감독위원회의 Guidelines on Outsourcing (06.12월)을 토대로 클라우드 특수성을 고려하여 보완되었으며, 클라우드를 활용하려는 금융회사에 위험식별 및 규제 관련 명확성을 제공하고 있다[7]. 주요 내용으로는 금융회사가 중요도 평가를 통해 선별된 중요업무를 클라우드 제공자 위탁 시 관할당국 통보 및 감사권을 부여하는 등의 계약을 해야 한다. 또한, 클라우드 제공자가 위치하는 국가의 데이터 처리 위치를 고려할 것을 명시하고 있다[5].

2.2.3 영국

영국은 16년 7월 금융감독청(Financial Conduct Authority)에서 금융회사 클라우드 이용의 명시적 허용 및 컴플라이언스를 명시한 「클라우드 및 제3자 IT 아웃소싱 관련 지침」을 발표하였다. 이 지침에서는 금융회사가 중요 업무의 아웃소싱 시 명확한 문서화와 클라우드 제공자 등에 대한 리스크 관리 및 데이터 접근 관할지 등을 명시하고 있다[5].

2.2.4 싱가포르

싱가포르는 통화청(Monetary Authority of Singapore)에서 클라우드 서비스를 아웃소싱의 하나로 명시하고 「아웃소싱 가이드라인」을 준수하도록 규정하고 있다. 금융회사가 클라우드 제공자에 대한 위험관리를 수행해야 하며, 데이터 접근, 기밀성, 무결성 보장과 클라우드 제공자에 대한 관리 감독 책임 등에 대한 내용을 제시하고 있다[5].

2.3 국내 금융 클라우드 정책 및 규제 분석

2.3.1 주요 국가들의 규제방식과 비교

주요 선진국은 클라우드 이용을 직접 규제하지 않고 가이드라인 등을 통해 자율적으로 준수하도록 하고 있다. EU는 금융회사의 클라우드 서비스 이용 관련한 기본원칙만 정의하고 세부사항은 자율적으로 하도록 맡기고 있다[7]. 영국과, 싱가포르 등도 EU와 유사하게 금융당국의 지침 또는 가이드라인으로 운영하는 반면 미국은 금융당국 차원의 특별한 규정 없이 검사협의회(FFIEC)에서 클라우드 이용 유의사항을 명시하고 있다[8].

국내에서도 최근 개정한 전자금융감독규정에서 클라우드 이용범위를 확대하여 표면상으로는 금융회사가 클라우드를 자율적으로 이용할 수 있도록 한 것으

로 볼 수 있으나 해외 국가들과 달리 전자금융감독규정에서 클라우드 이용 관련한 사항을 일부 규정하고 있다. 자율보안을 제시하면서 비중요 정보처리시스템 지정 등 감독 규정상에 제한을 두어 실제로 금융회사들이 자율적인 보안을 하지 못하도록 하고 있다.

2.3.2 규제방식의 역전현상

금융위원회에서 2016년 전자금융감독규정을 개정하여 도입한 비중요 정보처리시스템 지정은 네거티브 규제방식[1]이라고 하였다. 즉, 금융회사 자체적으로 전자금융거래의 안전성이나 신뢰성에 미치는 영향이 낮은 시스템을 비중요 정보처리시스템으로 지정할 수 있도록 하면서 개인 신용정보나 고유 식별정보는 포함되지 못하도록 하였다. 원칙은 허용하면서 예외는 금지하는 네거티브 방식을 주장하면서 중요정보가 포함된 대다수의 은행 업무를 클라우드를 이용하지 못하도록 한 것은 허용되는 원칙보다 금지되는 예외가 더 큰 사항으로 자칫 포지티브 방식으로 규제방식이 바뀌는 것으로 볼 수 있다[10]. 이는 네거티브 방식이 국민에게 자유권을 더 보장한다[11]는 측면에서 보면 포지티브 방식으로의 역전현상으로 국민의 자유권 보장이 감소되는 것으로 해석할 수 있다.

금융회사에서 중요정보도 클라우드를 이용할 수 있도록 한 것은 네거티브 규제방식의 예외금지가 원칙 허용보다 역전될 수 있는 위험성은 다소 해결할 수 있을 것으로 보인다. 그러나 이 개정사항도 네거티브 규제방식의 본질이 약화될 수 있는 사항이 있다. 전자금융 감독규정 개정사항에서는 금융 분야 특수성을 반영한 안전성 확보조치 등 금융권 클라우드 이용, 제공기준을 제시하였다. 이는 금융회사가 준수해야 할 사항들을 규정함으로써 금융회사 자율에 맡기기보다는 규정중심적인 규제에 가깝다고 할 수 있다. 즉, 네거티브보다는 포지티브 규제방식에 가까워질 수 있다.

2.3.3 법률근거의 부재

전자금융감독규정의 비중요 정보처리시스템 규정(제14조의2)은 상위 법률인 전자금융거래법에서도 제한하지 않는 개인의 고유 식별정보나 개인 신용정보 배제를 임의로 규제하는 것이다. 신기술이라 광범위한 위임입법이 불가피하더라도 규제 법정주의 원칙을 벗어난 규제는 정당화될 수 없다. 다른 한편으로는 신기술 특성상 신속한 사회변화에 대응해야 한다는 특수성이나 클라우드 서비스에 따른 개인정보유출 방지 등 정보보호를 위한 규제라고 정당화할 수 있을 것이다. 그러나 그것이 진정 정당화되기 위해서는 전자금융거래법에서 관련사항을 먼저 정의하고 그것을 전자금융거래법의 하위 규정인 전자금융감독규정에서 방향을 제시하는 방법이 되어야 한다[10].

또한, 금융보안원에서 발간한 「금융분야 클라우드 컴퓨팅서비스 이용 가이드」에서는 금융회사가 클라우드 서비스 이용 시 준수해야 할 절차를 제시하고 있고, 금융회사가 적절한 보안 대책을 수립·운영하기 위해 이 가이드를 활용할 수 있다고 한다. 이와 유사하게 공공기관도 「공공기관 민간 클라우드 이용 가이드라인」의 기준을 만족하지 못하면 클라우드 서비스를 이용할 수 없었다. 이것은 공공기관 클라우드 확산의 걸림돌로 오랫동안 지적되어 왔으며, 법률로 정해져 있지도 않은 가이드라인으로 국민의 기본권을 제한하는 대표적인 사례였다.

금융 분야에서도 상위 법률인 전자금융거래법에서 클라우드 관련하여 비중요 정보처리시스템 지정 제한에 대한 구체적인 위임 없이 전자금융감독규정과 금융보안원의 가이드라인을 통해 국민의 기본권을 제한할 수 있는 경우라 할 수 있다.

2.3.4 감독방법

앞에서 살펴본 주요국들은 권고나 지침 등을 통해 클라우드 제공업체의 감독 관련 사항을 계약서에 명시적으로 포함하도록 하고 있으며, 금융회사가 클라우드 제공업체에 대한 접근권이나 현장 감사권 등 관리감독 책임을 가진다. EU나 영국은 클라우드 제공업체를 직접 감독하고, 미국이나 싱가포르는 금융회사를 통해 간접적으로 감독하고 있다[8]. 간접적 감독은 우리나라의 전자금융거래법에서 금융회사가 전자금융보조업자를 감독하는 방식과 유사하다고 할 수 있다.

우리나라는 클라우드 이용 시 금융회사가 안전성 확보조치 및 계약 내용 등을 감독당국에 보고하도록 하였다. 그리고 EU나 영국처럼 클라우드 이용 계약

1) 규제는 특정한 활동이나 행위를 허용하는지 또는 금지하는지에 따라 포지티브(원칙금지-예외허용), 네거티브(원칙허용-예외금지) 방식으로 구분된다. 이 중 네거티브 방식이 국민에게 자유권을 보다 보장한다는 측면에서 주목받고 있다[9].

서에 금융회사와 감독당국의 조사·접근권을 명시하도록 하고 있다. 또한, 금융회사가 중요도 높은 업무를 클라우드로 서비스하기 위해서는 실제 이용하고자 하는 날의 7 영업일 이전에 금융감독원장에게 관련 서류를 구비하여 사전에 보고하여야 한다.

감독당국에 사후보고가 아닌 사전 보고는 금융회사의 자율보안 활성화 취지에 반할 뿐만 아니라 정부가 금융회사에 대한 규제를 직접적으로 행사하는 것으로 볼 수 있다. 그리하여 네거티브 규제가 아닌 포지티브 규제가 되어 국민의 기본권을 제한하게 될 수 있다. 더불어 클라우드 사업자가 감독당국의 감독을 받도록 함으로써 클라우드 사업자의 부담도 높아질 것이다.

2.3.5 데이터 국외 이전 제한

클라우드 데이터의 물리적 위치 관련하여 주요 선진국에서는 권고, 지침, 가이드라인 등을 통해 금융회사의 준수사항을 가이드 하고 있다.

우리나라도 사고 발생 시 법적 분쟁, 이용자 보호, 감독 관할 등을 고려하여 고유 식별정보 또는 개인 신용정보를 처리할 경우 해당 정보를 처리하는 모든 시스템과 관리시스템을 국내에 설치하도록 하고 있다. 이는 신속한 장애 대응 및 복구가 가능하도록 국내의 전산센터 내에 필수 운영인력이 상주하도록 하는 것이며, 장애 발생 사실을 신속하게 통지하고 대응하도록 요구하는 것이다.

2018년 11월 발생한 AWS 장애 사례를 통해 하나의 클라우드를 이용하는 기업들은 해당 클라우드 장애 발생 시 장애가 완전히 복구될 때까지 기다려야만 한다는 것을 알 수 있었다. 이로 인해 크고 작은 장애가 발생해도 서비스를 계속 할 수 있는 멀티, 하이브리드 클라우드에 대한 관심이 높아질 것으로 보인다. 그러나 중요정보의 국외 이전을 제한하고 있어 한 국가 내에서 멀티 클라우드를 이용하면 쉽게 해결될 수 있을 것 같지만, 영리를 목적으로 하는 기업 입장에서는 멀티 클라우드 이용에 따른 비용 부담이 적지 않을 것이다. 클라우드 기업체 여러 곳과 계약관계를 맺어야 하며 관리를 위한 인력 및 비용도 많이 소요될 것이다. 자칫 유휴자원의 효율적 활용을 통한 비용 절감이라는 클라우드 본연의 장점이 퇴색할 우려가 있다. 국내의 경우 아직 클라우드 시장이 초기 단계이고 장애 사례가 많지 않아 멀티클라우드의 필요성과 인식은 낮다. 하지만 금융회사 입장에서는 개인 신용정보의 국외 이전 제한 속에서 고품질의 안정적인 금융 서비스를 제공해야 하는 과제를 안게 된 것이다.

한편 전 세계 클라우드 시장은 아마존(AWS), MS, IBM 등 글로벌 IT 기업들이 점유하고 있다[12]. 이 해외 사업자들은 금융회사가 쉽게 데이터 분석을 할 수 있는 플랫폼을 낮은 비용의 클라우드로 제공하고 있으며, 국내 금융회사들이 이 플랫폼을 이용한다면 클라우드를 통해 고객 맞춤형 금융서비스를 적시에 제공할 수 있을 것이다. 그러나 우리나라의

Table 1. Comparison of Cloud Policy in Countries

Country	Policy Name	Institution Name	Regulated type	Supervisory Type
United States of America	Outsourced Cloud Computing	Federal Financial Institutions Examination Council	None	Indirect Supervision
EU	Recommendations on Outsourcing to Cloud Service Providers	European Banking Authority	Recommendation	Direct Supervision
United Kingdom	Guidelines for firms outsourcing to the cloud and other third party IT service	Financial Conduct Authority	Instruction	Direct Supervision
Singapore	Guidelines on Outsourcing	Monetary Authority of Singapore	Guideline	Indirect Supervision
Republic of Korea	Electronic Financial Supervision Regulation	Financial Services Commission	Regulation	Indirect Supervision

데이터 국외 이전 제한 규제는 전 세계 클라우드 시장을 점유하고 이끌고 있는 해외 사업자들의 국내시장 진입을 제한함으로써 클라우드 활성화를 가로막고 있다[12].

III. 데이터 국외 이전 관련 법률 및 연구동향

3.1 데이터 국외 이전 관련 법률

우리나라 개인정보보호법제에서는 데이터 국외 이전 관련하여 개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)에서 규정하고 있다.

개인정보보호법에서는 개인정보처리자가 국외의 제3자에게 개인정보 제공 시 다음의 사항을 알리고 동의를 받아야 하며, 법을 위반하는 내용으로 국외 이전 계약 체결을 하지 못하도록 하고 있다.

① 개인정보를 제공받는 자
② 개인정보를 제공받는 자의 개인정보 이용 목적
③ 제공하는 개인정보의 항목
④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
⑤ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

한편, 정보통신망법에서도 이용자의 개인정보에 관해 법을 위반하는 국제계약을 체결하지 못하도록 하고 있다. 하지만, 이용자 개인정보를 국외에 제공하는 것뿐만 아니라 처리위탁, 보관까지 동의를 받도록 함으로써 개인정보보호법보다 포괄적으로 규정하고 있다. 또한, 서비스 제공자가 동의를 받으려면 다음의 사항을 이용자에게 모두 알려야 한다.

① 이전되는 개인정보 항목
② 개인정보가 이전되는 국가, 이전일시 및 이전방법
③ 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
④ 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

3.2 데이터 국외 이전 관련 연구

데이터 국외 이전 관련 연구들은 대부분 이전 제한에 대한 법제의 문제점 및 대안을 제시하였다.

김현경[13]은 "데이터 국지화 정책의 세계적 흐름과 그 법제적 함의"에서 데이터 국지화 정책의 주요 국가 동향, 데이터 국지화 규범의 법적쟁점을 통해 국지화 도입의 필요성을 주장하였다. 김유림[14]은 "개인정보 국외 이전에 관한 법제 정비 방안"에서 우리나라 개인정보 국외 이전 관련 법제의 문제점을 해외 주요 국가들과 비교하여 법제 정비 방안을 제시하였다. 기존의 법제 문제점 및 대안을 제시한 연구와 달리 이규엽 등[15]은 "국경 간 데이터 이동에 관한 국제적 논의 동향과 대응 방안"에서 데이터 국외 이전 관련하여 주요 국가들과 국내의 법제를 비교하였으며, 단순 법제정비 정책 제안이 아닌 데이터 규제의 영향도를 정량적으로 실증 분석하였다는데 의의가 있다.

기존의 개인정보법제상에서의 데이터 국외 이전 관련 연구와 달리 노현숙[16]은 클라우드 서비스에서 개인정보의 국외이동에 관한 법적 문제에 대해 계약, 국내법, 국제협력 측면의 방안을 제시하였다. 반면, 강철하[17]는 클라우드 환경에서 개인정보 국외 이전에 대한 법체계 정비뿐만 아니라 클라우드 사업자 및 개인정보보호 관련기관의 지위 문제에 대한 개선안을 제안하였다. 그러나 클라우드 사업자의 법적 지위에 대한 개인정보보호법제에서의 규율체계 정립만을 제시하였으며 데이터 국외 이전 관련 클라우드 이용 활성화에 대한 방안을 제시하지는 않았다.

그동안 클라우드의 이용 활성화를 위한 연구와 논의가 없었던 것은 아니다. 도혜지[18]는 비중요 정보처리시스템 지정 등 금융권 클라우드 정책의 한계를 주요 국가들의 사례와 비교하여 금융권 클라우드 보안 인증제 도입 등 클라우드 이용 활성화를 위한 정책적 대안을 제시하였다. 이희석[19]은 "금융기관 클라우드 시스템 도입을 위한 의사결정 모델에 대한 연구"에서 금융회사들이 클라우드 시스템 도입 시 구성방안을 결정할 수 있도록 여러 가지 모델을 제시하였다. 임제상[20]은 "금융회사 클라우드 활성화를 위한 보안정책" 연구에서 클라우드 보안위협에 따른 보안 요구사항을 고려한 금융회사 적용모델을 서비스 유형별로 제시하였다. 이는 금융회사가 중요정보를 클라우드에서 이용할 경우 참조할 수 있는 모델을 제시하였다는 것에 의의가 있다.

그러나 금융회사들이 클라우드 이용 시 중요정보는 국내에만 두도록 하는 데이터 국지화 규제로 인해 금융 클라우드 이용이 활성화되지 못하고 있다. 그동

안 데이터 국외 이전과 클라우드 이용 활성화 등에 관해 많은 연구가 있어 왔지만 데이터 국지화 규제 속에서 클라우드 이용을 활성화하기 위한 구체적인 개선방안은 논의되지 못하였다.

IV. 국내외 금융 클라우드 국지화 실태 및 문제점

4.1 데이터의 속성

데이터는 의미 있는 정보를 가진 모든 값을 뜻한다. 데이터 자체는 단순한 사실에 불과하고 정보는 사용자의 의사결정에 도움을 주는 가공된 데이터들의 집합이다. 데이터는 데이터 사용자의 의지와 관계없이 다른 곳으로 이동될 수 있다. 데이터가 클라우드에 보관되는 경우 하나의 고정된 위치에 놓여있지 않고 복제되거나 여러 부분으로 나뉘어서 다양한 장소에 저장될 수도 있다. 이 경우 국내에 한정될 수도 있고 그렇지 않을 수도 있다. 클라우드 환경이 아닌 일반적인 경우에도 특정 순간에 데이터가 저장된 장소나 이동경로는 알 수가 없다. 마찬가지로 클라우드에 데이터를 저장할 경우 이용자는 데이터가 보관될 장소를 결정할 수 있는 권한을 가지고 있지 못하고 어디에 저장되어 있는지 조차 알 수도 없는 경우가 많다. 일반적으로 클라우드에 저장된 데이터는 효율적으로 관리하기 위해 여러 위치에 저장되고 복제된다[13].

이러한 데이터의 이동성과 분할 저장되는 특성 등으로 데이터가 현재 어디에 있는지 알기 어려우며, 이용자가 그 데이터를 통제하거나 관리하는 것도 어렵다. 또한, 미국의 클라우드법(Cloud Act)처럼 해외로 이전된 클라우드 저장 정보에 대해 접근 권한을 가지고 다른 국가에 대한 데이터를 압수수색 하는 등 데이터 주권을 침범하는 사례도 있을 수 있다. 이러한 데이터 속성들에 기인한 데이터 규범 제한이 데이터 국지화이며, 몇몇 국가에서는 자국의 국가안보나 데이터 주권 보장을 위해 법률로 제정하는 사례도 있다.

4.2 데이터 국지화

데이터 국지화란 자국민의 정보 주권을 보호하기 위해 데이터의 국가 간 이동을 통제하는 조치로 정보를 처리하는 시스템을 자국 내에 두도록 강제하거나 자국 내에서만 처리하도록 제한하는 것을 말한다. 정보가 국외로 전송되는 것을 금지할 수도 있고, 정보가 국경 너머로 이전되기 전에 정보주체의 사전 동의나 승인을 요구할 수도 있다. 또한, 정보의 사본이 국내에 저장될 것을 요구하거나 데이터가 수출될 때 세금을 부과할 수도 있다[21]. 데이터 국지화는 자국민의 개인정보보호와 데이터 경쟁력 확보를 위한 전 세계적인 추세이며, 주요 국가들의 금융회사들은 국외에 위치한 클라우드를 이용하지 않고 대부분 자국 내에 위치한 리전을 통해 클라우드 서비스를 이용하고 있다.

4.3 데이터 국지화 사례

데이터 국지화는 데이터를 규제하는 강도에 따라 3가지 유형으로 나눌 수 있다[22].

첫 번째, 분리된 네트워크를 원칙으로 하는 유형으로서 정부에 의해 언제든지 데이터 통제가 가능하여 가장 강력한 규제이며 중국, 이란 등이 이에 해당된다. 두 번째, 모든 데이터에 대해 국지화를 원칙으로 하되 예외적으로 국외 이전을 허용하는 경우이다. 러시아, 인도 등이 대표적이며 이 경우는 자국 내 데이터 유통이 원칙이나 극히 예외적인 경우 국외 이전을 허용한다. 세 번째 개인정보 등 특정 데이터에 대한 국지화를 원칙으로 하는 경우이며 대부분의 유럽과 북미 국가들이 추구하는 유형이다.

4.3.1 중국

중국은 2015년 7월 사이버공간의 주권과 국가안보, 공공이익을 수호하고 건전한 정보화 발전을 촉진하기 위해 사이버보안법을 제정하였으며, 2017년 6월 1일 발효되었다. 이 법은 네트워크 전반을 망라한 규제법으로서 네트워크에 대한 통제 강화, 사이버 공격 방어, 중국의 이용자 정보를 보호하는 정부의 역량 강화를 위해 만들어졌다. 이 법에서는 핵심기반시설운영자가 중국에서 수집·생산한 국가안보, 경제발전, 공공의 이익과 밀접한 관련 있는 중요 데이터나 개인정보의 국외 이전은 제한하고 있다. 영업목적상 필요한 경우 네트워크 운영자는 보안 평가를 통과해야 해당 정보를 국외로 이전할 수 있게 하는 등 개인정보에 대한 처리기준을 강화하였다[23].

4.3.2 베트남

베트남은 2013년 이후 인터넷을 이용한 통화 메시지(Over The Top)가 발달함에 따라 인터넷 통화, SM 서비스의 제공 및 이용의 관리에 관한 규정을 도입하였다. 이 규정에서는 해외 사업자가 베트남 국내 사업자와 계약을 체결하거나 베트남 국내에 최소한 하나의 서버를 설치하도록 하여 데이터 국지화에 대해 명시하고 있다[24].

베트남 공안부는 사이버 안전과 국가 안보를 위해 2017년 6월 사이버보안법 초안을 발표하여 의견을 수렴하였으며, 2018년 6월 국회에서 최종안이 통과되어 사이버보안법이 2019년 1월 1일 발효되었다. 베트남 국민의 개인정보를 수집, 이용, 분석, 처리하여 서비스를 제공하는 국내외 기업은 이용자의 정보를 반드시 베트남 현지에 보관하여야 하며, 정보통신망을 통해 베트남 내에서 서비스를 제공하는 국외 기업은 베트남에 지사나 대리 사무소를 설립해야 한다고 명시되어 있다[25].

4.3.3 러시아

러시아는 데이터국지화법과 테러방지법을 통해 외국 기업에게 러시아 이용자를 추적하고 러시아 정부가 요구하는 경우 개인정보를 제공하도록 강제하고 있다. 러시아 데이터국지화법은 2015년 9월 1일에 발효되었으며 러시아 내에서 수집된 러시아 이용자의 개인정보는 반드시 러시아 내에 물리적으로 위치하고 있는 서버나 데이터베이스에 저장·처리되어야 하며, 러시아인의 개인정보는 국외 이전 규칙에 의해서만 국외 이전이 가능하다. 이러한 데이터국지화법은 러시아내의 러시아인과 외국회사에 적용되며, 온라인을 통해 러시아로 물품을 배송하는 외국회사에도 적용된다[26].

4.3.4 EU(유럽연합)

EU(유럽연합)은 자연인에 관한 기본권과 개인정보보호에 대한 권리를 보호하고 EU 역내에서 개인정보의 자유로운 이동을 보장하는 것을 목적으로 하는 일반 개인정보보호법(General Data Protection Regulation)을 2018년 5월 적용하였다. GDPR은 개인정보 삭제권, 처리 제한권, 개인정보이동권, 반대권 등의 신규 권리 추가 및 기존 권리 명확화를 통해 정보주체의 권리를 확대·강화하였다. EU는 EU 역내 수집된 개인정보의 역외이전을 원칙적으로 금지하지만, 다음과 같은 경우에는 역외이전을 허용하기도 한다[27].

① 적정성 결정(adequacy decision)을 통해 개인정보보호 관련 법제가 적절한 수준의 보호를 보장하고 있다고 인정된 나라로 이전하는 경우
② '적절한 보호조치(appropriate safeguards)의 제공', '정보주체의 권리 행사 보장', '효과적인 법적 구제 수단의 존재'에 모두 해당하는 경우
③ 명시적 동의(explicit consent), 계약의 이행 또는 정보주체의 요청으로 필요한 경우, 공익의 중요한 이유 등과 같은 특정 상황에서 예외 요건에 해당하는 경우

EU의 GDPR에 개인정보의 국외 이전을 금지하는 명시적 조항은 없지만, EU보다 개인정보보호 수준이 낮은 나라로의 이전을 금지함에 따라, 이러한 복잡한 절차 없이 EU 역내에 서버를 설치하여 개인정보를 보관·처리하는 것도 데이터 국지화라고 볼 수 있다.

4.4 우리나라 금융의 클라우드 이용과 데이터 국지화

4.4.1 클라우드 이용 동향

우리나라는 18년 3월 기준으로 총 38개 금융회사(73건)에서 업무처리, 부가서비스 제공 등의 목적으로 클라우드 시스템을 이용하고 있다. 그동안 전자금융감독규정이 개정(19.1)되기 전까지는 보안사고 예방을 위해 고유 식별정보, 개인 신용정보를 제외한 비중요 정보에 한해 퍼블릭 클라우드 이용을 허용하고 있었기 때문에 주로 개인정보와 관련이 없는 내부처리업무나 상품소개 등에 활용되고 있었다[8].

반면, 해외 주요 국가들은 금융회사의 핵심 업무를 클라우드를 이용하여 활발하게 사용하고 있다[12]. 내부 업무처리나 부가서비스 등 활용분야가 제한적인 국내에 비해 해외는 클라우드를 통해 금융회사 고유의 서비스 제공 등 다양한 방식으로 클라우드 서비스를 이용하여 고객 서비스를 제공하고 있다.

영국의 Oaknorth bank는 영국 최초 클라우드 기반 은행으로 은행 핵심 업무 등 모든 업무를 클라우드에서 운용하고 있다. 클라우드의 잘 갖춰진 인프

라를 활용함으로써 기존보다 빠른 시스템 변경과 최신기술 적용 및 급격한 작업부하 처리로 예금유치, 대출신장 등의 효과를 확보할 수 있었다. 미국의 온라인 1위 은행인 Capital One은 핵심 업무인 캐피탈뱅킹과 콜센터 등에 클라우드를 적용하여 신규 어플리케이션 배포시간을 단축시켰고 싱가포르 최대 은행인 DBS은행도 고객용 웹사이트 및 리스크 관리 업무에 클라우드를 적용하여 비용절감 효과를 얻었다[12].

4.4.2 데이터 국지화의 긍정적 영향

클라우드 사업자가 해외에 데이터를 두게 되면 국내법 적용이 어려워질 수 있다[28]. 만일 해외 사업자의 관리 소홀 등으로 개인정보 유출 등 보안사고 발생 시 국내 이용자를 보호할 수 없게 된다. 이처럼 데이터 국지화는 사고 발생 시 법적분쟁이나 사고대응, 소비자 보호 및 감독관할, 개인정보보호 등의 문제에 쉽게 대응할 수 있다. 해외 주요국의 데이터 국지화 관련법에서도 국가와 자국민의 중요정보를 보호하기 위해 물리적으로 자국에 강제함으로써 데이터 침해에 대한 확인 및 조사, 대응을 신속하게 할 수 있도록 규정하고 있다.

4.4.3 데이터 국지화와 해외사업자 차별

4.4.3.1 비용측면

국내 금융회사 중요정보의 클라우드 이용 관련 개정사항은 클라우드 서비스를 제공하는 해외 사업자에게는 상대적으로 불리하게 작용할 수 있다.

개정된 감독규정에 따르면 금융회사의 중요정보를 클라우드에서 이용하려면 데이터 센터가 국내에 위치하여야 한다. 네이버 등의 국내 사업자들은 아마존 등 해외 사업자들을 추격하는 클라우드 후발주자로써 기존의 리테일 데이터 센터 형태에서 하이퍼스케일 데이터 센터 형태로 변경하고 있다. 그러나 국내에 데이터 센터가 없는 해외 사업자들은 국내의 IDC를 임대하거나 국내에 데이터 센터를 신규 구축함에 따라 많은 비용이 소요될 것이다.

4.4.3.2 대리인 지정 및 관리부담

또한 국내에 주소 또는 영업소가 없으며 이용자 수, 매출액 등을 고려하여 대통령령으로 정하는 기준에 해당하는 사업자는 국내 대리인을 서면으로 지정하여야 한다[29]. 이는 국외 정보통신서비스 제공자 등에 의한 개인정보보호 담보가 충분하지 않다는 지적에 따라 정보통신망법의 규정이 일부 개정된 사항(19.3.19 시행)으로 대리인의 행위를 해외 사업자의 행위로 간주할 수 있다. 국내 사업자와는 달리 국내에 주소를 두지 않은 해외 사업자는 금융회사 클라우드 서비스 제공을 위해 대리인 지정과 그에 대한 관리 책임까지 추가로 부담하고 있는 것이다.

4.4.3.3 국내규제 충족을 위한 국내인증 획득

해외 사업자는 기본적으로 우리나라의 규제와 정책을 준수해야 한다. MS 등 일부 사업자들은 국내 사업자들과의 경쟁에서 뒤쳐지지 않기 위해 국내의 정보보호 관리체계(ISMS) 인증을 획득하기도 했다[30].

이는 해외 사업자들이 국내 금융 클라우드 시장 선점을 위해 정부에서 제시하는 인증을 획득하여 시장 경쟁력을 확보하겠다는 노력의 일환으로 볼 수 있다. 물론 싱가포르 클라우드 보안인증 등 해외 인증 획득 시 안전성 평가항목을 생략해 주기도 한다. 그러나 국내 사업자와의 경쟁력 우위를 점하기 위한 해외 사업자의 국내인증 획득 노력은 국내 사업자와의 차별이나 공정한 경쟁을 저해하는 것이라는 논란이 될 수 있다.

V. 금융 클라우드 국지화 개선방안

5.1 데이터 국지화 규제 개선 필요성

그동안 국내 금융회사들이 N사 전산센터 마비, 카드 3사 개인정보 유출사고 등 수많은 보안 사고를 겪으며 금융당국은 금융 클라우드 정책 수립 및 제도 개선에 보수적인 입장이었다. 그 결과 과도한 개인정보 규제 등으로 한국의 클라우드 트래픽(1%대)은 주요국가(80%대)에 비해 아주 미비한 수준이었다[31]. 반면, 미국 기업의 클라우드 사용 이유 1위가 보안이라는 점은 개인정보는 보호만 할 것이 아니라 보호와 활용의 균형이 함께 이루어져야 한다는 것을 시사하고 있다[31].

이번 감독규정 개정으로 금융권은 클라우드 플랫폼을 이용하여 빅데이터나 인공지능 기술을 보다 자

유롭게 활용하고 혁신적인 서비스도 출시하게 되어 국내 금융 산업의 경쟁력도 향상될 것으로 기대하고 있다. 그러나 여전히 중요정보는 국내에만 두도록 함으로써 클라우드 사업자에 대한 차별문제와 데이터 주권 수호를 위한 데이터 국지화로 정보보호가 오히려 약화되는 등 부작용이 있을 수 있다.

일반적으로 글로벌 클라우드 서비스는 데이터 센터가 국내에 있더라도 운영관리는 해외에서 이루어지며 국내에서는 세일즈 역할만 한다. 금차 개정사항에 관리시스템을 국내에 두어야 한다는 조항은 해킹 등의 보안사고 발생 시 사고 확인과 관리 감독의 어려움을 해소할 수 있다는 측면에서는 긍정적으로 평가할 수 있다. 그러나 해외 사업자는 국내 금융회사의 클라우드 서비스 제공을 위해 관리시스템과 인력을 국내에 두어야 하는 부담을 안게 되었다.

전자금융감독규정에서는 금융회사가 클라우드 서비스 제공자와 계약을 체결할 때 금융당국의 검사와 감독이 원활하게 수행될 수 있도록 금융당국의 조사 및 접근에 협조할 의무를 명시하도록 하고 있다. 그럼에도 불구하고 우리 정부의 해외 사업자에 대한 행정, 사법권 집행 등의 통제는 여전히 어려울 것으로 보인다. 2018년 11월의 AWS 사고 발생 시 우리 기업의 서비스 피해에 대해 정부가 조사, 제제 등에 한계를 드러낸 것을 보면 해외 사업자에 대한 감독 정책이 제대로 반영될 수 있을지 의문이다. 그리고 정부에서는 미국의 클라우드법에 의해 미국 수사기관이 국내에 위치한 해외사업자의 서버에서 우리 국민의 개인정보를 감청하거나 수집하는 행위를 알지 못할 수도 있다.

이처럼 금융회사가 중요정보를 클라우드에서 이용하게 하면서 데이터 국지화 규제를 펼치는 제도는 해외 사업자에 대한 차별문제 해소, 개인정보 보호 및 활용의 균형 유지, 클라우드 활성화 등을 위해 개선이 필요하다.

5.2 데이터 국지화 규제 개선 방안

5.2.1 데이터 보호 수준별 규제 도입

앞에서 살펴본 대로 해외 사업자들은 국내 클라우드 사업자에 비해 데이터 센터 신규 구축 등 데이터 국지화 규제로 인한 상대적인 차별을 받을 수 있다.

이러한 클라우드 사업자에 대한 상대적인 차별을 예방하기 위해 "데이터 보호 수준별 상벌제[2]"를 도입할 것을 제안한다. 클라우드 사업자가 개인정보보호 관련 법규를 준수하는 수준에 따라 스코어링을 하여 점수가 높을 경우 세금을 감면시켜 주는 등 혜택을 준다. 반대로 법규를 준수하지 않아 점수가 낮을 경우 높은 세금과 벌금을 책정하고, 금융회사에 대한 클라우드 서비스 사업을 일정기간 제한하도록 한다. 법규 준수여부의 측정은 금융회사가 클라우드 서비스 제공자의 안전성을 평가하는 단계에서 이루어질 수 있으며, 클라우드 서비스 제공자 평가항목으로 반영되는 것도 가능하다. 낮은 점수 사업자의 서비스 재개 가능여부 또한 서비스 제공자 안전성 재평가를 통해 결정할 수 있도록 한다.

해외 사업자의 경우 우리나라에 데이터 센터를 설립하면서 투자한 많은 비용에 대하여 높은 수준의 개인 정보보호 활동을 통한 세금 감면으로 국내 클라우드 사업의 경쟁력을 확보할 수 있을 것이다. 마찬가지로 국내 사업자들도 세금 감면 혜택을 얻기 위해 정보보호 수준 향상을 위한 노력을 하게 될 것이다. 이러한 선의의 경쟁 관계를 통해 국내 사업자와 해외 사업자 모두 정보보호 수준이 더욱 향상되어 궁극적으로는 이용자에게 안전하고 편리한 금융 클라우드 서비스를 제공할 수 있을 것이다. 더불어 전 세계 클라우드 시장의 대부분을 점유하고 있는 해외 사업자들로부터 높은 수준의 클라우드 서비스를 제공받을 수 있게 될 것이다.

5.2.2 해외 사업자 감독 강화를 위한 법제 마련 및 국제 공조체계 구축

금융회사의 클라우드 이용에 대한 규제 개선과 함께 해외 사업자에 대한 데이터 주권 확보가 필요하며, 금융당국이 해외 사업자를 관리 감독할 수 있는 법적 근거나 제도 마련이 필요하다. 이것은 해외 사업자를 통제하기 보다는 궁극적으로 이를 이용하는 이용자 정보의 보호가 더욱 더 중요하기 때문이다.

이를 위해 해외 사업자가 국내 이용자 권리를 침해했을 때 집단소송이나 침해에 대한 입증, 손해배상 산정 및 청구방법 등 정부나 감독기관이 우리 이용자를 위한 제도를 만들어야 한다. 또한, 해외 사업자가 국내 이용자 정보를 이용하려면 우리나라에서 수립한 정보보호 관련 법률 및 제도를 준수할 것을 약정하고

2) 이 제도는 사업자의 법규준수는 필수조건이어야 하며 제도의 악용을 예방하기 위해 법규 미 준수 시 벌금부과 등 별도의 규제를 둘 수 있다.

이를 위반할 경우 우리나라 법의 집행을 받는다는 등 사법 관할권 적용에 대해 관련 국가 간 협약이나 조약을 체결하는 것이 필요하다.

5.2.3 해외 사업자 감독 수준별 감사 차별화

해외 사업자에 대한 차별을 없애고 선의의 경쟁을 통한 정보보호 수준 향상을 위해 "해외 사업자 감독 수준별 감사 차별화"를 제안한다. 사업자의 감독 수준에 따라 감사수준, 감사주기 등을 달리 할 수 있다.

5.2.3.1 감사수준 차별화

이것은 상호주의 원칙 하에서 우리나라에 대한 상대국의 정책을 반영하여 차별화된 감사를 실시하는 방법이다. 해외 사업자가 속한 국가의 개인정보보호 법제나 관련 인증 제도를 국내법제나 인증 제도와 비교하여 감사나 감독을 면제하거나 경감시켜 준다. 또는, 감사 결과 등급을 측정하여 등급별 감사 수준을 미리 정의할 수 있다. 등급을 1 ~ 5등급으로 분류하여 1등급은 기본항목만 점검하고, 5등급은 모든 항목을 점검하는 등 등급별 감사수준을 달리 한다.

5.2.3.2 감사주기 차별화

감사등급 이외에 감사주기를 차별화 할 수 있다. 감사 결과 등급이 우수한 사업자는 감사 주기를 길게, 미흡한 사업자는 감사 주기를 짧게 함으로써 사업자들은 감사를 받지 않기 위해 정보보호 수준 향상에 힘쓸 것이다.

이처럼 클라우드 사업자에 대한 관리 감독 개선이 궁극적으로 금융회사의 경쟁력 향상과 안전한 금융환경을 유지할 수 있게 되는 것이다.

5.2.4 전자금융 기반시설 확대 및 클라우드용 취약점 분석, 평가기준 개발

전자금융거래법에 따르면 금융회사는 안전성과 신뢰성 확보를 위해 전자금융기반시설에 대한 취약점을 분석·평가하고 그 결과를 금융위원회에 보고하여야 한다.

금융회사가 클라우드 사업자를 통해 금융 서비스를 제공하게 될 경우 클라우드 사업자의 인프라 및 서비스 또한 전자금융기반시설로 볼 수 있어 관련 법률 준수를 위한 기반시설 지정이 이루어져야 한다.

이는 금융회사의 전자적 침해에 대한 리스크 관리 및 보안 강화를 위해 반드시 필요한 사항으로써 정부와 관련 기관을 통해 관련 법률 개정이 선행될 필요가 있다.

클라우드 사업자의 인프라 및 서비스가 전자금융기반시설로 지정될 경우 관련 법에 의해 매년 취약점 분석, 평가를 반드시 실시하여야 한다. 클라우드 환경에서는 기존 전자금융기반시설에서 발생할 수 있는 일반적인 보안위협 뿐만 아니라 클라우드 고유의 보안위협[3]도 발생할 수 있다[32]. 그래서 금융회사가 클라우드를 이용하여 금융서비스를 제공할 경우 기존의 취약점 분석 평가 기준으로는 클라우드 전자금융기반시설에 대한 점검에 한계가 있을 수밖에 없다. 따라서, 클라우드 고유의 위협에 대응할 수 있는 취약점 분석 평가가 이루어질 수 있도록 클라우드 전자금융기반시설에 특화된 취약점 분석, 평가기준 개발이 반드시 필요하다.

VI. 결 론

최근 금융의 디지털화, 데이터 활용의 중요성 증대에 따라 대량의 데이터를 낮은 비용에 처리 가능한 클라우드의 중요성이 점점 높아지고 있다. 이에 따라 고유 식별정보, 개인 신용정보 등 금융 분야의 중요정보도 클라우드에서 이용 가능하도록 전자금융감독규정이 개정되었다.

그러나 금융 분야의 클라우드 정책 및 규제들이 금융회사들의 자율적인 보안활동 방해, 규제방식의 역전현상에 의한 국민의 기본권 제한, 해외 사업자에 대해 동등한 조건에서의 서비스 제공 어려움 등을 야기하며 금융회사의 클라우드 이용이 활성화되지 못하고 있다.

한편, 우리나라 이용자 보호 및 감독관할권 문제 등으로 중요정보의 클라우드 이용 시 모든 시스템을 국내에 두도록 하는 데이터 국지화 정책은 국내 금융회사의 클라우드 이용 활성화를 가로막는 대표적인 규제이다. 이는 비용문제, 대리인 지정 및 관리, 국내인증 획득 등 해외 사업자에 대한 차별문제를 발생

3) 클라우드 고유의 보안위협에는 클라우드 서비스를 관리하는 인터페이스나 API 공격, 가상자원의 취약점을 이용한 공격, 공유기술의 취약점을 이용한 공격 등이 있다[32].

시킨다.

이러한 해외 사업자에 대한 차별문제 해소, 개인정보 보호 및 활용의 균형, 클라우드 활성화 등을 위해 데이터 국지화 규제에 대한 개선방안을 제안하였다. 첫 번째, 데이터 보호수준별 상벌제를 도입하여 클라우드 사업자의 개인정보보호 수준을 세금 부과의 기준으로 활용할 수 있다. 이는 국내외 사업자들의 선의의 경쟁관계를 통해 정보보호 수준 향상과 안전하고 편리한 금융 클라우드 서비스를 이용자에게 제공할 수 있다. 두 번째, 해외 사업자 감독 강화를 위한 법제 마련 및 국제 공조체계 구축이 필요하다. 해외 사업자에 의한 우리국민의 권리침해 예방과 국내 이용자 정보보호를 기대할 수 있다. 세 번째 해외 사업자에 대한 차별방지와 정보보호 수준 향상을 위해 해외 사업자 감독 수준별 감사 차별화를 제안하였다. 이는 클라우드 사업자에 대한 관리 감독 개선으로 안전한 클라우드 금융환경을 제공하는 효과를 얻을 수 있을 것이다. 마지막으로 금융회사가 이용하는 클라우드 인프라 및 서비스를 전자금융기반시설로 확대 지정하고 클라우드 전용 취약점 분석 및 평가기준 개발이 필요하다.

제안한 이 방안들이 금융회사의 클라우드 이용 활성화와 전자금융 감독에 대한 표준화된 규제와 정책이 되기를 기대한다. 하지만 이 개선방안들은 현실적으로 클라우드를 활용하고자 하는 금융회사들이 직접 방안을 구현하거나 제도를 만들기 어렵다. 국가 간 협력이나 법률, 제도의 제정 및 정비도 수반되어야 한다. 또한, 금융회사의 중요 정보에 대한 클라우드 이용이 활성화되고 안정화되기 위해서는 정부나 감독당국의 지휘 하에 금융회사들과 클라우드 사업자가 제도 정착 및 안정화를 위해 함께 협력해야 한다. 이러한 이상적인 상황이 이루어진다면 금융회사들은 신기술 활용의 기반이 될 클라우드에서 빅데이터, 인공지능 등과 접목하여 고객의 Needs를 극대화할 수 있는 안전한 금융 서비스를 제공할 수 있을 것이다.

금융회사의 클라우드 이용 활성화를 위한 데이터 국지화 규제 개선방안을 도출했다는 데 그 의의가 있다. 하지만, 규제 개선방안에 대한 세부적인 체크리스트와 적용방안을 수립하지 못했다는 것에는 한계점이 존재한다. 향후 연구에서는 전문가 설문조사 등을 통해 금융회사와 클라우드 사업자에 실질적으로 적용 가능한 체크리스트를 수립하고 검증하는 연구가 필요해 보인다.

References

[1] Hye-In Hwang, "Trends and implications of global data center changes," Korea Information Society Development Institute, 30(20), pp. 15, Nov. 2018

[2] Maeng-Soo Kang, "Cloud computing market trends and prospects," KDB Economic Research Institute, KDB survey monthly bulletin 758, pp. 60-62, Jan. 2019

[3] "Revised Electronic Financial Supervision Regulations,Enforcement," Financial Services Commission, 7-Dec. 2018, Available : http://www.fsc.go.kr/info/ntc_news_list.jsp?menu=7210100&bbsid=BBS0030

[4] Hyun-chul Kim, "Legal problems of cloud computing regulatory reform," a law-abiding gun, 42(4), pp. 9-10, Dec. 2018

[5] Financial Security Agency, "Guide for using the financial industry cloud service," pp. 88, Jan. 2019

[6] Mi Rim Yoon, "Introduction and utilization of cloud computing in overseas public sector," 2015-04, The Federation of Korean Information Industries(FKII), pp. 17, Aug. 2015

[7] Bong-Sik Ko, "Major contents and implications of european banking authority's recommendations on outsourcing to cloud service providers," 11(2018-01), Financial Security Agency, pp. 124-128, Jan. 2018

[8] "A plan to expand the use of cloud in the financial sector," Financial Services Commission, 16-Jul. 2018, Available : http://www.fsc.go.kr/info/ntc_news_list.jsp?menu=7210100&bbsid=BBS0030

[9] Seung-Pil Choi, "Legal review on deregulation," A Study on the Construction Methodology 12(1), pp. 331-332, 2011
[10] Hyun-chul Kim, "Legal problems of cloud computing regulatory reform," a law-abiding gun, 42(4), pp. 17-21, Dec. 2018
[11] Seung-Pil Choi, "Legal review on deregulation," A Study on the Construction Methodology 12(1), pp. 321, 2011
[12] "Cloud and Financial Transformation," Financial Services Commission, 28-May. 2019, Available : http://www.fsc.go.kr/info/ntc_news_list.jsp?menu=7210100&bbsid=BBS0030
[13] Hyun-Kyung Kim, "A study on the legal issues of data attributes and localization norms," Korea Public Land Law Association, Public Land Law Review 78, pp. 216-218, May. 2017
[14] Yoo Rim Kim, "A study on legal system improvement for the Transborder flow of Personal Information," Master, SungKyun Kwan University, Oct. 2018
[15] Kyu Yub Lee, Moonhee Cho, Jungu Kang, and Minji Kang, "Cross-Border data flows: discussions and countermeasures," Policy Analysis 18-18 Korea Institute for International Economic Policy, 2018
[16] Hyun Sook Noh, "A study on the transfer of personal information outdoor in cloud services," doctorate, Korea University, Aug. 2015
[17] Chul Ha Kang, "The legal issues and improvement directions of the transborder flow of personal information in cloud environments," Journal of Law & Economic Regulation 10(2), pp. 301-327, Nov. 2017
[18] Hye Ji Do, "A study on cloud computing for financial sector limited to processing system of non-critical information : policy suggestion based on US and UKs approach," The Journal of Society for e-Business Studies, 22(4), pp. 39-51, Nov. 2017
[19] Hee Seok Lee, "A Study on the decision making model for the introduction of the financial institution's cloud system," Master, Korea University, May. 2018
[20] Je Sang Im, "A study on security policy for vitalizing financial company cloud," Master, Korea University, Dec. 2017
[21] Anupam Chander and Uyen P. Le, " Breaking the Web: data localization vs. the global internet," Emory Law Journal, Forthcoming: UC Davis Legal Studies Research Paper no.378, pp 3, Apr. 2014
[22] Hyun-Kyung Kim, "A study on the legal issues of data attributes and localization norms," Korea Public Land Law Association, Public Land Law Review 78, pp. 241, May. 2017
[23] Korea Information Society Agency, "Global internet censorship and control trends and implications," Hot Issue Report, pp 9-10, Oct. 2017
[24] Hwon-Il Park, "A study on the localization of personal information," Kyung Hee Law 52(4), pp 146-148, Dec. 2017
[25] Young-Ki Kim, "Major contents and implications of the vietnam cyber security act," 14(2018-10), Financial Security Agency, pp. 162-164, Dec. 2018
[26] Korea Information Society Agency, "Global internet censorship and

control trends and implications," Hot Issue Report, pp 7-8, Oct. 2017
〔27〕 Korea Internet & Security Agency, "Guidelines for EU general privacy act (GDPR) for the korean enterprise," pp. 16, Aug. 2018
〔28〕 Won Joon Jung, "Legal problems to activate cloud computing : the issue about personal information protection," Korea Information Society Development Institute, 26(20), pp. 45, Nov. 2014
〔29〕 Kyung-Jin Choi, "Data sovereignty and user information protection in cloud computing," NIPA-06-S00002-01, National IT Industry Promotion Agency, pp. 174, Feb. 2019
〔30〕 "MS korea, obtain isms certification, the second foreign country after amazon", Digital Daily, 28-Nov. 2018, Available : http://www.ddaily.co.kr/news/article/?no=175325
〔31〕 Min-hwa Lee, "Prerequisites for the fourth industrial revolution, cloud data innovation," 35th Forum, KCERN, pp 5. Apr. 2017
〔32〕 Financial Security Agency, "Guide for using the financial industry cloud service," pp. 20, Jan. 2019

〈저자소개〉

장 우 경 (Woo-kyung Jang) 정회원
2005년 2월: 한남대학교 전자정보통신 졸업
2018년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 정보보호 컴플라이언스, 클라우드, 전자금융보안

김 인 석 (In-seok Kim) 종신회원
2008년: 고려대학교 정보경영공학과 (박사)
2009년~현재: 고려대학교 정보보호대학원 교수 FDS산업포럼 회장, 한국정보보호학회 운영위원
〈관심분야〉 전자금융보안, 금융 IT 컴플라이언스, 핀테크