http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.22, No.4, November 2017, pp.39-51
https://doi.org/10.7838/jsebs.2017.22.4.039

비중요 정보처리시스템으로 한정된 국내 금융권 클라우드 시장 활성화를 위한 제안: 영미 사례를 중심으로

A Study on Cloud Computing for Financial Sector limited to Processing System of Non-Critical Information: Policy Suggestion based on US and UK's approach

도혜지(Hye-Ji Do)*, 김인석(In-Seok Kim)**

초 록

2016년 10월 금융당국은 금융권 내 클라우드 도입 활성화를 위해 전자금융감독규정의 망분리 조항을 개정하였다. 하지만 비중요 정보처리시스템의 데이터만 처리할 수 있도록 규제함으로써 정밀한 고객데이터 분석과 개인화 서비스를 제공하는 금융권에서는 이번 개정에 큰 변화를 느끼지 못하고 있다. 클라우드 서비스의 도입은 비용절감 및 업무혁신에 기여하는 바가 크며, 변화하는 정보통신기술 환경에 필수적인 요건이다. 따라서 보안과 신뢰성의 원칙을 고수하며 클라우드 도입에 유연하게 대처하기 위해서는 클라우드 서비스를 도입한 금융기관의 안정적 구현을 위한 정책에 대한 논의가 필요하다. 본 연구는 금융권 내 클라우드 도입 관련 제도의 한계와 변경 필요성을 검토하고, 영미의 사례분석을 통해 정책적 대안을 제시한다.

ABSTRACT

In October 2016, the NFSA (National Financial Supervisory Authorities) revised the network separation clause of the Regulation on Supervision of Electronic Financial Activities in order to promote the Cloud Computing implementation in the financial sectors. The new regulation, however, limits the Cloud Computing usage to non-critical information and its processing system. Financial institutions that provide customer data analysis and personalized services based on personal data regard current revision as unchanged as before. The implementation of Cloud Computing has greatly contributed to cost reduction, business innovation and is an essential requirement in ever-changing information communication technology environment. To guarantee both security and reliability of the implementation of the Cloud Computing in financial sectors, a considerable amount of research and debate needs to be done. This paper examines current Cloud Computing policies in the Korean financial sector and the challenges associated with it. Finally, the paper identifies policy suggestions based on both European Union and United States' approach as they have successfully introduced Cloud Computing Services for their financial sectors.

키워드 : 클라우드 컴퓨팅, 금융보안, 클라우드 정책
Cloud Computing, Financial Security, Cloud Computing Policies

본 연구는 미래창조과학부 및 한국인터넷진흥원의 "고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음(과제번호 H2101-16-1001).

* Co-Author, Graduate School of Information Security, Korea University(chicdo@korea.ac.kr)
** Corresponding Author, Graduate School of Information Security, Korea University(iskim11@korea.ac.kr)
Received: 2017-08-29, Review completed: 2017-10-11, Accepted: 2017-10-16

1. 서 론

작년 국내 클라우드 시장 규모가 약 1조 1천 900억 원으로 전년 대비 55.2% 성장했다[10]. 이는 작년부터 3년 일정으로 정부가 실행중인 '제1차 클라우드 컴퓨팅 발전 기본계획(2016~2018)의 효과가 나타난 것으로 보인다.

전 세계적으로 IT환경이 급변함에 따라 기업들이 관리해야 할 데이터양이 증가함으로써 IT자원에 대한 유지・보수 및 관리의 문제가 대두되고 있다[8]. 특히, 금융권은 IT시스템의 복잡화, 정보량의 증대로 사용되는 스토리지 영역이 매년 증가하고 있다. 이에 운용・관리상의 비용절감, IT의 유연성 제고, 상품 및 서비스 경쟁력 향상을 위한 IT 인프라 확보 등의 새로운 대안으로 클라우드 서비스(Cloud Service)가 부상하고 있다[5].

글로벌 금융회사들은 클라우드 서비스를 도입하는 방안을 추진 중이거나 이미 도입하여 운용하고 있다. 미국 장외 주식시장 나스닥(NASDAQ), 스페인의 뱅킨테르 은행, 싱가포르증권거래소 등이 클라우드 서비스를 도입하여 운영 중이다.

국내에서는 2015년 미래에셋증권이 아마존사의 클라우드 서비스(AWS)를 도입하면서 국내 금융권내 클라우드 서비스 도입에 대한 관심이 증가하였다. 우리나라는 지금까지 비교적 높은 수준의 금융규제로 인하여 클라우드 도입이 무산되었으나, 2016년 10월 감독규정이 개정되면서 클라우드 도입의 발판이 마련되었다. 하지만 현재 모든 정보처리시스템이 아닌 비중요 정보에 대한 정보처리시스템에만 클라우드 서비스 도입을 허용한 한계가 있다. 특히, 중요 정보처리시스템이 큰 비중을 차지하는 금융권에서는 비중요 정보처리시스템만의 클라우드 서비스 도입에 대해 회의적인 반응이며, 향후 이를 보완할 수 있는 정책이나 제도 마련 또한 미비한 실정이다. 또한 "금융권 클라우드 서비스 이용 가이드"에서 설명하고 있는 비중요 정보처리시스템 지정 가능 예시의 기준마저 모호하다. 가이드에서 설명하는 비중요 정보처리시스템 지정기준은 아래와 같다[6].

금융회사는 다음 각 호의 사항을 고려하여 전자금융거래의 안전성 및 신뢰성에 미치는 영향이 낮은 시스템을 비중요 정보처리시스템으로 지정할 수 있다.

- 처리 정보의 중요도 및 정보 위・변조・유출 시 파급효과
- 침해사고 또는 장애 발생 시 타 시스템의 업무 연속성 저해 수준 등 타 시스템과의 연계성
- 복구 목표시간 등 해당 정보처리시스템의 업무 중요도
- 운영, 개발, 테스트 시스템 등 정보처리시스템의 용도
- 고객 또는 사내직원 등 이용자 유형에 따른 해당 정보처리시스템 이용자 수 등

※ 고유식별정보* 또는 개인신용정보** 처리(송신, 수신 또는 전달 포함) 시 지정 불가

* 「개인정보보호법」 제24조 및 동법 시행령 제19조 각 호에서 정한 정보로서, 주민등록번호, 여권번호, 면허번호, 외국인등록번호가 이에 해당됨

** 「신용정보의 이용 및 보호에 관한 법률」에서 정한 정보

※ 다만, 「개인정보 비식별 조치 가이드라인」(2016년 7월)을 준수하여 비식별화하거나, 사내직원 등 전자금융거래와 관련 없는 고유식별정보 또는 개인신용정보는 처리 가능

본 논문은 금융권 클라우드 서비스 활성화를 위한 현행규제의 변경 필요성을 제시하고, 영국과 미국의 금융권 클라우드 도입 사례분석을 통해 정책적 대안을 제시한다.

2. 금융권 클라우드 서비스 도입 필요성

금융권 클라우드 서비스 도입으로 인한 긍정적인 요소를 파악하고 국내외 사례를 통해 금융권 클라우드 서비스의 필요성을 알아보고자 한다.

2.1 금융권 클라우드 서비스를 통한 혁신적인 변화

클라우드는 유연성, 경제성, 효율성 측면에서 금융권 서비스 제공에 혁신적인 변화를 가져올 수 있다(<Table 1> 참조). 대표적인 사례로 국내 유안타증권에서는 시장 상황에 따른 다양한 시나리오와 검증에 클라우드를 활용함으로써 자사 금융상품의 리스크 관리 분석시간을 단축하였고, 비용을 절감하였다. 미국의 캐피탈원(Capital One)은 클라우드를 도입 후 데이터 센터를 8개에서 2개로 줄여 유지·보수비용을 크게 절감하였다. 또한 스페인의 글로벌 은행인 BBVA는 클라우드 기반 업무시스템을 도입하여 본사와 약 11만 명에 달하는 26개 해외 자사 직원 간의 빠르고 쉬운 의사결정, 신상품 개발과 판매기간 단축 등의 변화를 이끌어 냈다[16]. 국내외 수많은 사례를 통해 클라우드 서비스를 이용하는 금융회사들의 혁신적인 경영 사례가 입증되었다. 국내 도입 시 클라우드 서비스는 효율적인 금융시스템 기반 조성에 주도적인 역할을 할 수 있을 것이다.

2.2 국내 금융권 클라우드 활성화 정책

정부는 국내 클라우드 활성화를 위해 2015년 9월 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률'을 시행하였으며, 'K-ICT 클라우드 컴퓨팅 활성화 계획'을 확정(2015. 11)하였다. 이에 금융당국은 제도의 유연성 확보요구와 클라우드 활성화 정책을 반영하여 클라우드 도입과 관련된 조항을 일부 개정하였다. 새로 개정

〈Table 1〉 Characteristics of Cloud Service Usage & Benefit of Implementation within Financial Sector

Characteristic	Details	Benefit of Implementation within Financial Sector
Flexibility	Computing resources can be allocated flexibly when demanded	Offers range of financial IT services such as new product simulation, credit risk analysis, etc. with greater flexibility (ex: Yuanta Securities Korea Co.)
Economic	Cloud Computing is Pay-as-you-go model that charges based on usage, which is economical	Efficient management of isolated systems and reduced cost of additional infrastructure and management (ex: Capital One)
Efficiency	As a shared IT resource, Cloud Computing guarantees efficiency through business continuity	Provide a virtualized business environment with efficient management that guarantees business continuity without constraints of time and place. (ex: BBVA)

〈Table 2〉 Changes in law to Promote Cloud Computing Services

	Prior to Revision	After the revision
Restriction on Outsourcing	'Provision on consignment processing of information of financial companies' Article 4, July, 2015.	
	Outsourcing of information processing is limited to head office branches overseas, and re-commissioning is prohibited (Except when approved by Director of Financial Supervisory Service)	Removed existing clause that limits outsourcing to third parties. Allowing outsourcing to third parties such as IT specialized companies
Network separation	'Electronic Financial Supervision Regulations Article'Article 14-2 (5), October, 2016.	
	Financial institution that operates within the country must set up Data Center and Disaster Recovery Centers within the country. Setting up Wireless communication network is prohibited.	The regulation will no longer apply to non-critical information systems.

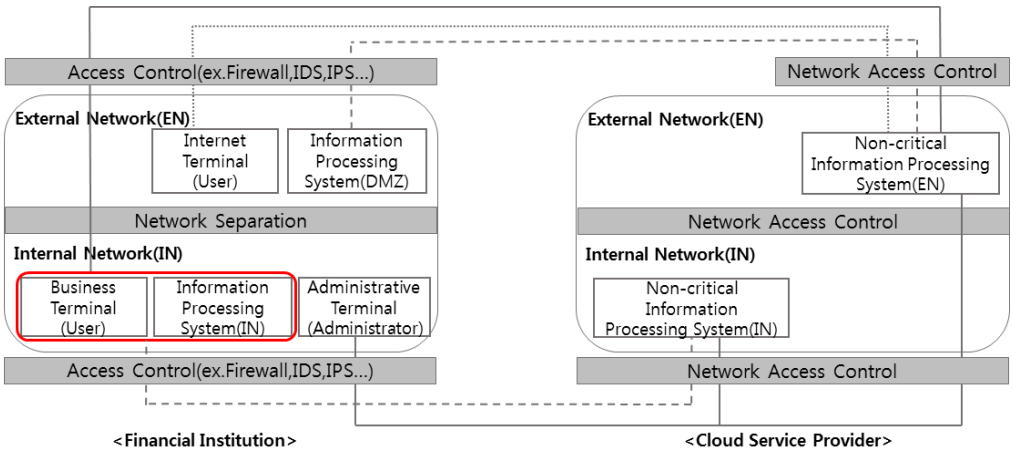
된 조항은 금융권내 재위탁 허용과 비중요 시스템에 대한 망분리를 허용함으로써 클라우드 도입의 장애물을 제거하였다(<Table 2> 참조).

전자금융감독규정 제14조의 2(비중요 정보처리시스템 지정) ⑤ 제1항의 비중요 정보처리시스템만 위치한 전산실에 대해서는 제11조 제11호 및 제12호, 제15조 제1항 제5호를 적용하지 아니한다.

- (제11조 제11호) 국내에 본점을 둔 금융기관 및 전산실 및 재해복구 센터는 국내에 설치할 것
- (제11조 제12호) 무선통신망을 설치하지 아니할 것
- (제15조 제1항 제5호) 전산실 내에 위치한 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것

이에 추가적으로 금융보안원에서는 '금융권 클라우드 서비스 이용 가이드'(2016. 10)를 발간하여 금융회사 및 전자금융업자가 클라우드 서비스 이용 시 준수해야할 사항을 권고하였다. 해당가이드는 이용대상, 도입절차, 이용 시 준수사항, 자산관리 및 침해사고 대응, 사후관리가 기술되어있다[6]. 가이드 내 핵심 요구사항은 망분리 및 비중요 처리시스템에 관한 내용이다. 본 가이드를 토대로 망분리 조항 완화로 인해 클라우드 서비스가 금융회사 내부 연계 시 보호 가능한 대책을 <Figure 1>에 정리하였다. <Figure 1>에 따르면 망분리가 허용되어 클라우드 서비스 제공자의 내외부망에 있는 정보처리시스템을 사용할 수 있다. 하지만 비중요 정보에 한하여 클라우드 서비스를 제공 받을 수 있다. 추가적으로 금융권에서 도입할 수 있는 클라우드 서비스가 비중요 정보 서비스에 국한 되어 있기 때문에 해당 가이드에서는 비중요 정보처리시스템 선정기준과 처리할 수 있는 정보의 범위를 기술하였다.

이와 같이 최근 금융권의 클라우드 서비스 도입 활성화 움직임에 맞추어 해당 법령이 개정됨에 따라 금융권 내 클라우드 서비스 도입이 전적으로 현실화 되었다. 하지만 중요 정보처리시스템 및 개인신용정보는 제외됨으로써 적용 가능한 영역이 제한되어 있다.



〈Figure 1〉 An Example of Security Measures within Financial Institution Network Connected to External Cloud Computing

3. 기존연구 동향

국내 클라우드 도입 관련 연구들은 크게 개인정보보호 조치방안 및 클라우드 관련 보안 사고에 바탕을 두어왔다. 특히 클라우드 서비스 자체의 보안이슈와 개인정보보호 문제를 중심으로 논의가 지속적으로 이루어져왔다. 각 연구들을 살펴보면 먼저, 유우영, 임종인[20]은 클라우드 서비스 제공자가 서비스 가용성 측면의 품질 보증에 대해서만 보증하고 있는 상황이고 개인정보보호와 관련된 데이터 보존 방법, 데이터보관에 대한 물리적 위치 고지 등 개인정보보호를 위한 보호장치를 충분히 마련하여야 한다고 주장한다[20]. 박완규[14]는 클라우드 컴퓨팅 환경에서의 개인정보의 이전의 문제를 지적하고 세이프하버(Safe Harbor) 협정 마련, 이용자의 개인정보보호 책임을 강화 등으로 리스크를 줄이는 방안을 제시했다[14]. 또한 임철수[13]와 김정훈, 황용석, 김성현, 조시행[9]은 클라우드 보안이 선결 과제이며 이러한 보안 사고를 방지하기 위한 기술적 요소들 및 대응 방안을 제시했다[9, 13].

각 연구들에서 동일하게 주장하는 바로는 클라우드 서비스 제공자는 가용성 측면 뿐만 아니라 보안 측면에서 해킹, 악성코드 등으로부터 개인정보를 보호해야한다고 보았으며, 이를 위해 새로운 제도 도입 및 기존 법률 정비, 기술적 보호관리 등을 요구했다.

클라우드 도입에 대한 정책적 연구가 전혀 이루어지지 않았던 것은 아니다. 백승익, 신지연, 김종우[1]는 우리나라의 클라우드 컴퓨팅 확산을 위한 정책은 서비스 소비자 중심이 아닌 서비스 공급자 중심이고, 민간 중심이 아닌 정부 중심이고, 이런 불균형은 우리나라의 빠른 클라우드 컴퓨팅 확산을 방해할 것이라 주장했다. 또한, 이정구, 민대환, 권헌영[12]는 2016년 9월에 시행된 '클라우드컴퓨팅 발전 및 이용자보호에 관한 법률'에 대해 「정보통신망법」과 「개인정보보호법」에서도 각각의 법이 제정 및 개정될 당시 고려하지 않았던 클라우드 서비스의

특징을 고려하여 함께 개정될 필요가 있다고 주장했다[12].

이처럼 지금까지는 대부분 클라우드 서비스 자체의 보안에 대한 연구가 지속되었다. 하지만 최근 정부에서는 클라우드 서비스 도입 활성화를 위해 망분리 조항을 완화 했음에도 불구하고 정밀한 고객데이터 분석과 고객 특화 서비스를 제공하는 금융권에서는 비중요 정보처리시스템의 망분리만 허용한 이번 정책에 대한 근본적인 대책에 대해 논의 되지 아니하였다.

4. 금융권 클라우드 도입에 대한 이해

금융권 클라우드 도입 대안 제시에 앞서 국제 사례를 알아보고자 한다. 이는 대안 제시 시 예상되는 침해 요인을 해소하고 클라우드 도입 기준을 변화 시킬 수 있는 기초 자료가 된다.

4.1 네덜란드 금융권 클라우드 도입 사례

국내에서는 중요 정보처리시스템 도입을 제한 시킨 것에 반해 EU의 많은 나라들은 금융부문에 클라우드를 도입해 안전하게 사용 중이다. 특히, 유럽의 감독 당국이 클라우드 기반의 서비스의 과제를 해결하고 금융기관이 어떻게 클라우드 서비스를 사용하고 있는지 국가, 기업 그리고 서비스 제공자의 적절한 역할 분담에 대해 살펴보고자 한다.

네덜란드의 DNB(De Nederlandsche Bank)는 유럽 금융 기관의 클라우드 기반 서비스를 사용하는 것을 허용하는 법률을 제정한 창시자 중 하나이다. DNB는 네덜란드의 은행 및 기타 금융 기관이 가이드라인을 따른다면 웹사이트, 모바일 애플리케이션, 소매 금융 플랫폼, 고성능 컴퓨팅 및 신용 위험 분석 솔루션을 포함한 다양한 서비스에 AWS, Salesforce, IBM, KPN and Microsoft Azurek의 클라우드 서비스를 사용 할 수 있다고 발표했다. 가이드라인에 따르면 DNB가 금융기관에서 사용되는 IT 인프라를 감독하여 그 규정을 준수하고 있는지 서비스의 사용이 요구 사항을 충족하는지 확인할 의무가 있다고 명시되어있다. 또한, 금융기관은 IaaS 클라우드 기반 서비스를 사용하기 위해 다음 요구 사항을 충족해야한다고도 알려져 있다[2].

- DNB에 사전에 클라우드 컴퓨팅 사용의사 보고
- 표준적인 위험 분석 실시
- 금융감독법(Wet op het financieel toezicht-Wft)에 규정된 요구사항 충족
- DNB에 심사 권한 부여
- 계약에 계약종료관련 조항 포함

4.2 스위스 금융권 클라우드 도입 사례

스위스의 금융당국인 FINMA(The Swiss FInancial Market Supervisory Authority)는 은행 및 증권 딜러에 대한 건정성 및 리스크 중심의 감독을 실시하고 있다. 특히 FINMA는 라이센싱과 법규제 준수를 주기적으로 체크하고 있다. 규모, 복잡성, 위험 구조에 따라 은행, 보험회사, 공동 투자 제도, 자율 규제기관(self-regulatory organisations, SROs) 그리고 직접 후순위 금융 중개 기관(directly subordinated financial intermediaries(DSFIs)

을 6개의 감독 category들로 분류한다. 라이센스 보유자는 채권자, 투자자, 시스템 전체에 대한 잠재적인 위험에 미치는 영향, 스위스 중앙은행의 명성에 따라 6개의 감독 category로 분류된다. 이때, 심각한 위험에 노출 되어있거나 세계적으로 중요한 시스템일 경우 category 1에 해당이 되며, category 6은 매우 낮은 위험성을 가지고 있기 때문에 세심한 감독에서 제외된다[7].

이처럼 유럽에서는 금융당국의 구체적인 가이드라인을 통해 금융기업에서 안전한 클라우드 도입을 가능하게 하고 있다.

5. 국내 금융권 클라우드 도입에 대한 분석 및 문제점

5.1 현행 정책의 한계와 충돌

클라우드 관련 조항인 전자금융감독규정 제14조의2는 중요 단말을 제외한 비중요 단말에 대해 클라우드 서비스를 허용하였다. 비중요 단말의 경우 개인신용정보를 처리 할 수 없는데 이는 금융권에서 클라우드를 도입하려고 하는 취지에서 벗어난다. 왜냐하면 금융 서비스 제공자는 중요 정보를 이용하여 이용자에게 특화된 서비스를 제공하기 때문이다. 하지만, 현행법상 외부 클라우드 서비스 제공자에게 중요 정보가 담긴 내부데이터를 전송하기 위해서는 비식별화 조치가 이루어져야한다. 전송된 비식별화 데이터는 분석 후 다시 금융사 내부 시스템으로 들어오는데, 이때 해당 결과에 대한 고객 당사자를 식별할 수 없어 데이터의 활용 가치는 떨어지게 된다.

또한 금융권 클라우드 서비스 이용 가이드에서 설명하고 있는 비중요 정보처리시스템 지정 가능 예시의 기준이 모호하다. 예로 가이드에서는 “금융 서비스를 제공하지 않는 기관 대표 홈페이지”를 비중요 정보처리시스템 지정예시로 들었는데 현존하는 대부분의 은행 대표 홈페이지 및 홍보용 홈페이지 또한 회원가입 및 로그인 기능을 갖추고 있어 사실상 중요 정보처리시스템으로 분류될 수 있기 때문이다.

현행 정책은 망분리 기준완화를 통해 금융권의 클라우드 정착을 시도하였으나 그 범위가 비중요 단말에 한정되어 있어 활성화 저해가 불가피 하다. 따라서 현행 정책상 클라우드 서비스 도입의 장애가 되는 요소를 타개하고 안전한 클라우드 이용을 보증 할 수 있는 정책이 모색되어야한다.

5.2 클라우드의 침해사고 사례

클라우드 서비스의 보안성 논란은 지속적으로 제기 되어왔다. 2009년 이베이의 클라우드 기반 결제 시스템인 페이팔이 2시간 동안 정지되면서 수백 만 명의 사람들이 서비스 이용에 불편을 겪었으며, 2011년 아마존 EC2는 미국 버지니아 북부데이터센터 장애로 11시간 동안 서비스가 중단된 사건이 있었다[19]. 그 외에도 <Table 3>과 같이 해킹 및 악성코드, 관리실수 등 끊임없는 클라우드 서비스 보안사고가 발생하고 있다[4].

이처럼 국내 금융회사에 클라우드 서비스가 도입된다면 위와 같은 보안사고 가능성을 경감시키기 위한 정책적・기술적・관리적 조치가 추가로 요구될 가능성이 크다.

〈Table 3〉 Cloud Service security incident cases

Type	Service provider	Year	Detail
Hacking and Malware	Adobe	2013	Adobe server was hacked, 2.9 million private information and part of SW source code such as Acrobat leaked
	ZenDesk	2013	Personal information leakage caused by ZenDesk system hacking
	Evernote	2013	Cloud service that provides a memo/information organizing tool caused user name, e-mail address, encrypted password leakage
	Dream Host	2012	Personal information leakage caused by DreamHost DB hacking
	Dropbox	2012	Leakage of user email list for email spam
Service Failure	KT	2012	Failure of service caused by uCloud server switch and storage failure
	Salesforce	2012	Discontinuation of NA2 service due to storage failure
DoS Attack	Fujitsu	2011	DoS Attack caused service failure
Natural disaster & Management Mistake	Amazon	2013	Administrator mistakenly deleted the script to load balancing that led to ELB failure and Neflix service suffered connection failure
	First Server	2012	Loss of 5,698 data due to an error during system upgrade
	Amazon	2011	Electricity outage caused by lightning strike that led to EC2 error for 11 hours and 190 services simultaneously

6. 대안 제시 및 개선사항

영국의 금융 서비스 산업은 세계 3대 지휘본부(Command Center)라 불리며 런던 시내에서만 500개 이상의 은행 지점이 운영될 만큼 금융업이 발달되어있다[18]. 미국 또한 이에 버금가는 막강한 글로벌 금융 지대로 분류된다. 이러한 금융선진국의 클라우드 서비스 도입은 전 세계적으로 크나큰 파급효과를 지니기 때문에 해당 국가의 행보에 따라 국내 금융 클라우드 정책 또한 새로운 국면을 맞게 될 가능성이 높다.

6.1 영국 제도 분석 및 국내 정책의 개선사항

국내 금융권 클라우드 도입시 비중요 정보처리시스템에만 국한된 이유로 크게 두 가지를 들 수 있다.

- 첫째, 개인신용정보 해외 반출 및 금융당국이 접근 할 수 없는 관할로의 이전
- 둘째, 보안 이슈 및 법률적 책임 기준 부재

앞으로 클라우드 서비스를 활성화시키기 위해서는 위와 같은 근본적인 문제에 대한 확실한 대안이나 조치가 필요하다.

영국은 금융당국의 데이터 접근가능성을 기반으로 클라우드 도입을 허용하였다. 이는 데이터가 클라우드 상에서 특정 지역에 국한되지 못하는 어려움을 인지하여 지역기반의 요구사항보다는 당국의 접근가능성 여부를 필수 요구사항으로 설정한 것이다. 하지만 국내

현행법에는 중요 데이터를 저장하는 서버가 국내에 있어야 한다는 지역기반 정책이 시행되고 있다. 국내 클라우드 도입 활성화를 위해서는 지금의 물리적인 요건이 아닌 클라우드의 본래 특성에 대해 이해하고 이에 걸맞은 기준을 제시해야한다. 두 번째로 영국은 법률적 책임 기준의 문서화 및 법적효력이 있는 구체적인 계약을 통해 클라우드 서비스 제공자와의 이해관계를 명확화 시켜 발생할 수 있는 분쟁요소를 최대한 잠식시키려는 노력을 하였다. 국내에서도 클라우드 서비스를 도입하려는 금융기관들을 위해 명확한 법률적 책임 기준과 계약시 준수사항 등을 명시한 가이드를 제공하여 그들의 부담과 분쟁요소를 줄여주어야 한다.

영국의 금융감독청(Financial Conduct Authority)은 가이드를 배포・보완하여 클라우드의 안전한 도입을 위한 정책 근간을 지속적으로 마련하고 있다[3]. 국내에서도 중요 정보처리시스템 환경에서 안전한 클라우드 활용을 위해 꾸준한 가이드 작업 진행이 필요하다.

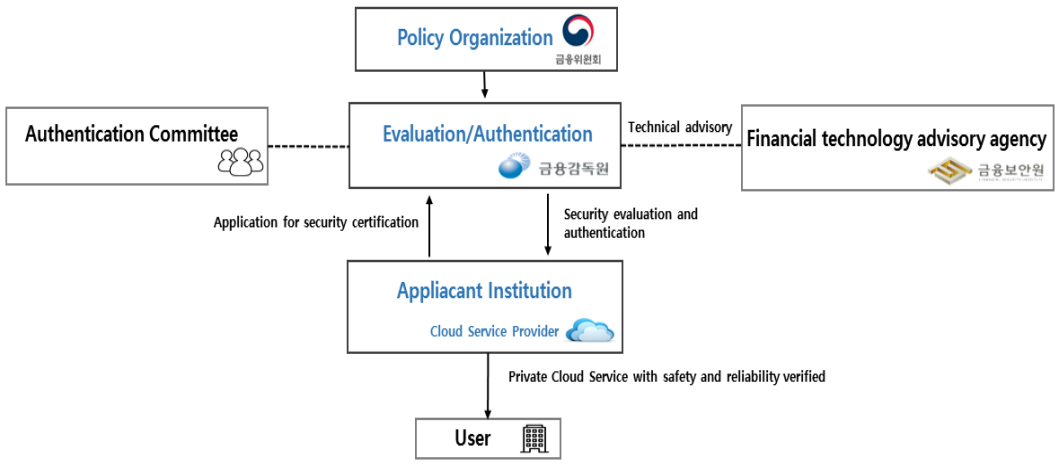
6.2 미국 제도 분석 및 국내 정책의 개선사항-국내 금융권 클라우드 보안인증제 제안

클라우드 서비스 제공자 단에서의 보안이 완벽히 이루어지기 위해서는 금융권의 보안인증체계가 자리잡혀야한다. 보안인증체계는 클라우드 서비스 제공자의 보안 및 정책 준수사항을 검증함으로써 금융회사들이 안심하고 서비스 이용할 수 있는 발판을 제공한다.

미국의 'FedRAMP', 영국의 'UK G-Cloud' 그리고 한국의 '클라우드 서비스 보안인증제'는 정부기관에 클라우드 서비스를 공급할 의도를 가지고 있는 민간기업의 보안수준과 법률 준수여부를 평가・보증함으로써 이용기관의 보안우려를 해소하였다[11, 17].

현행 클라우드 서비스 보안인증제는 공공기관을 대상으로만 시행되며 평가・인증・자문기관 또한 공공분야에 한정되어있다. 금융회사의 보안우려를 해소하기 위해서는 금융권에 특화된 보안인증체계 도입이 필요하다. 이를 위해서는 금융시스템에 대한 이해가 높은 금융보안원이나 금융당국의 참여를 유도하여 금융권에도 안전하고 신뢰성 있는 클라우드 서비스 제공이 보증될 수 있어야한다. 평가・인증의 종류는 최초평가, 사후평가, 갱신평가로 구분된다(<Figure 2> 참조). 금융권 클라우드 평가・인증 체계의 예시를 <Figure 3>과 같이 정리하였다. 클라우드 서비스 제공자가 평가・인증기관인 금융감독원에 보안인증 신청을 한다. 학계, 연구기관, 기술자문기관등 클라우드 금융시스템관련 전문가 5~10명으로 구성된 인증위원회와 금융부문 기술자문기관인 금융보안원의 도움을 받아 보안성 평가를 진행하고 정책기관인 금융위원회와 함께 해당 신청기관의 인증을 부여한다. 그로인해 클라우드 서비스를 사용하려는 이용자는 안전과 신뢰성이 검증된 민간 클라우드 서비스를 이용할 수 있다.

〈Figure 2〉 Type of Evaluation/Authentication



〈Figure 3〉 An Example of Financial Cloud Service Evaluation/Authentication Process

6.3 FI, NFSA 그리고 CSP의 협동

유럽 금융 산업은 점차 클라우드 컴퓨팅을 도입하고 있다. 그러나 서비스 채택 방식이 아직 성숙하지 않고, 대부분의 금융 기관(Financial Institution, FI)은 여전히 사내 인프라에 의존하고 있다. FI가 사용하는 가장 일반적인 방법은 Public Cloud와 Private Cloud를 공동으로 사용하는 Hybrid Cloud 방식이다. 또한 금융당국(National Financial Supervisory Authorities, NFSAs)도 개인정보보호 및 규정 준수의 우려에서 Private Cloud가 금융 시장에 전체적으로 적합하다고 생각하고 있다.

ENISA 보고서에서는 금융 분야의 클라우드 서비스 사용을 이해하고 클라우드 서비스 공급자(Cloud Service Provider, CSP)와 FI에게 클라우드 서비스의 안전한 사용을 지원하기 위해 작성 되었다고 언급했다. 또한, 설문조사와 인터뷰를 통해 수집 된 정보에 의해 클라우드 서비스 도입을 촉진하기 위한 단기 과제로 세 가지를 제시했다[15].

- 첫째, 정보 격차의 축소
- 둘째, 명확하고 적절한 목적의 규제 지침 제공
- 셋째, 준수의 간소화와 합리화

EU와 마찬가지로 국내에서도 위와 같은 과제를 해결하기 위해서는 FI, NFSA 그리고 CSP의 끊임없는 소통과 협력이 필요하다.

7. 결 론

클라우드 관련법 제정으로 인해 국내 클라우드 시장(매출액) 규모는 1조 1,892억 원으로 2015년(7,663억 원)보다 55.2% 성장해 최초로 1조 원에 돌파하였다[10]. 정부의 노력으로 클라우드 시장이 조금씩 눈에 띄는 성과를 거두고 있는 반면 금융권에서는 크게 실감하지 못하고 있다. 왜냐하면 최근 개정된 전자금융감독규정은 비중요 정보처리시스템에만 클라우드 서비스 도입을 허용하고, 보안이슈에 대한 명확한 대책을 제공하지 못함으로써 금융권

내 클라우드 활용이 극히 제한되어있기 때문이다.

최근 국내 기업에서는 IT부문에 투자를 보류하거나 예산을 대폭 삭감하고 있다. 이에 기업들은 IT부분 비용 절감 방법으로 클라우드 컴퓨팅(Cloud Computing)을 도입하는 사례가 증가하고 있다. 또한 데이터 관리 및 유지・보수가 용이하고 업무 효율성 증대와 비용 절감이라는 효과를 얻을 수 있다는 점에서 많은 기업에서 이러한 전산 자원 형태를 채택하고 있다. 하지만 대부분 고객의 중요 정보를 이용한 서비스를 제공해야하는 금융권에서는 클라우드 서비스의 혜택을 누리지 못하고 있다.

본 논문은 국내 금융권에 클라우드 서비스 도입을 위한 방안으로 해외 사례를 분석하여 대안을 제시하였다. 영국에서는 데이터 접근가능성을 기반으로 클라우드 도입을 허용하고, 법률적 책임 기준을 문서화나 구체적인 계약을 통해 문제를 해결해 나가고 있다. 우리나라도 이에 명확한 가이드 제공 및 서비스 제공자와의 이해관계를 해소하여 중요 정보처리시스템도 클라우드 서비스로 안전하게 사용할 수 있는 대안을 제시 할 필요가 있다. 두 번째로 금융권에 특화된 보안인증제를 도입해 금융기관에 클라우드 서비스 제공자의 보안수준과 법률 준수여부를 평가・보증함으로써 이용기관의 보안우려를 해소할 수 있다. 또한, 공신력 있는 보안 인증을 해준다면 클라우드 수요자들의 의식 개선을 하는데 도움이 될 것이다. 마지막으로 금융기관(FI), 금융 당국(NFSA) 그리고 클라우드 서비스 제공자(CSP)의 끊임없는 소통과 협력을 통해 안전한 클라우드 도입에 힘써야한다.

References

[1] Baek, S. I., Shin, J. Y., and Kim, J. W., “Exploring the Korean Government Policies for Cloud Computing Service,” The Journal of Society for e-Business Studies, Vol. 18, No. 3, pp. 1-15, 2013.

[2] DNB, Cloud computing: the rules, Available: http://www.dnb.nl/en/news/dnb-nieuwsbrieven/nieuwsbrief-banken/nieuwsbrief-banken-februari-2015/dnb319119.jspm, 2015.

[3] Financial Conduct Authority (FCA), “FG 16/5-Guidance for firms outsourcing to the ‘cloud’ and other third-party IT services,” Finalised guidance, 2016.

[4] Financial Security Institute, “Concept of cloud computing and industry trends,” 2016.

[5] Financial Security Institute, “Current status analysis of financial industry cloud service,” E-Finance and Financial Security, pp. 33-57, 2015.

[6] Financial Security Institute, “Guide for using the financial industry cloud service,” 2016.

[7] FINMA, Available: https://www.finma.ch/en/supervision/our-approach-to-supervision.

[8] Kim, H. G. and Lee, Y. S., “Current status and future prospects of cloud computing services,” The Journal of The Korean Institute of Communication Sciences, Vol. 27, No. 12, pp. 31-34, 2010.

[9] Kim, J. H., Hwang, Y. S., Kim, S. H., and Cho, S. H., “How to handle malicious code of cloud computing infrastructure and case,” Korea Institute of Information Security And Cryptology, Vol. 20, No. 2, pp. 51-55, 2010.

[10] Korea Association of Cloud Industry, “Survey on actual condition of cloud industry in 2016,” National IT Industry Promotion Agency(nipa), 2017.

[11] Korea Internet and Security Agency (KISA), “KISA, Evaluate and certify the protection level of Cloud Service information,” KISA press release, 2016.

[12] Lee, J. K., Min, D. H., and Kwon, H. Y., “Issues and Suggestions for “Act on the Development of Cloud Computing” and Protection of its Users,” Journal of Information Technology Applications & Management, Vol. 24, No. 1, pp. 81-91, 2017.

[13] Lim, C. S., “Security technology of cloud computing,” Korea Institute of Information Security And Cryptology, Vol. 19, No. 3, pp. 14-17, 2009.

[14] Pak, W.-Q., “Solutions to Problems regarding Transfer of Korean Personal Information to the U.S. in the Cloud Computing Environment,” Kyungpook National University Law, Vol. 38, pp. 455-478, 2012.

[15] Rossen Naydenov, Dimitra Liveri, Lionel Dupre, and Eftychia Chalvatzi, “Secure Use of Cloud Computing in the Finance Sector,” enisa, p. 11, 2015.

[16] Security Technology Research Team, “Case examples of domestic and overseas cloud service use cases,” Research report of Financial Security Institute, 2016.

[17] Seo, K.-K., “Introduction and utilization of cloud computing in overseas public sector,” The Federation of Korean Information Industries(FKII) ISSUE REPORT, 2015.

[18] Wikipedia, https://en.wikipedia.org/wiki/Economy_of_the_United_Kingdom#Financial_and_business_services.

[19] Yang, H. D. and Hwang, S. W., “Outline of security threat of cloud computing and proposal for direction for realizing creative economy,” Internet & Security Focus, pp. 66-83, 2013.

[20] Yu, W.-Y. and Lim, J.-I., “A Study on the Privacy Security Management under the Cloud Computing Service Provider,” Journal of The Korea Institute of Information Security and Crytology, Vol. 22, No. 2, pp. 337-346, 2012.

저 자 소 개

도혜지	(E-mail: chicdo@korea.ac.kr)
2016년~현재	고려대학교 정보보호대학원 금융보안학과 (석사과정)
관심분야	클라우드, 전자금융보안, 핀테크

김인석	(E-mail: iskim11@korea.ac.kr)
2008년	고려대학교 정보경영공학과 (박사)
2009년~현재	고려대학교 정보보호대학원 교수
	FDS산업포럼 회장, 한국정보보호학회 운영위원
관심분야	전자금융보안, 금융 IT 컴플라이언스, FIN TEC