

# 금융회사 클라우드 활성화를 위한 비중요정보처리시스템 지정방안 연구

장 명 도,<sup>†</sup> 김 인 석<sup>‡</sup>  
고려대학교 정보보호대학원

## Study on Designation of Non-Critical Information Processing System for Financial Company Cloud Computing Activation

Myong-do Chang,<sup>†</sup> In-seok Kim<sup>‡</sup>  
Graduate School of Information Security, Korea University

### 요 약

4차 산업혁명의 흐름과 IT자원의 효율적 사용이라는 요구가 맞물려 세계적으로 클라우드 컴퓨팅이 활성화 되고 있으며 국내도 관련 법 제정 및 각종 법안 등에 힘입어 그 사용이 증가하고 있다. 하지만 국내 금융회사는 보유정보의 중요도와 유출 등 사고 발생 시 파급효과로 인해 각종 규제를 받고 있어 상대적으로 활성화 되기 어려운 상황이다. 특히 중요하지 않은 정보를 취급하는 비중요 정보처리 시스템만 클라우드 컴퓨팅 사용이 가능하도록 하고 있는데 이를 구분하는 구체적 기준과 판단을 금융회사가 정하도록 하고 있다. 본 논문에서는 모호한 비중요 정보처리시스템 지정 기준을 구체화 하고 그 지정을 간편하게 할 수 있도록 하여 금융회사 클라우드 컴퓨팅을 보다 활성화 할 수 있는 방안을 제안하고자 한다.

### ABSTRACT

Cloud computing has been activated globally due to the demands of the 4th industrial revolution and the efficient use of IT resources, and domestic usage is also increasing due to legislation and related laws. However, domestic financial companies are subject to various regulations due to the importance of their information and the ripple effects of accidents such as outflows. Only non-critical information processing systems that handle non-critical information are allowed to use cloud computing. Financial companies are required to set specific criteria and judgment to distinguish them. In this paper, we propose a method to enable the financial company cloud computing to be more active by specifying the ambiguous non-essential information processing system designation standard and making it easier to designate.

**Keywords:** Cloud computing, non-essential information processing system

## 1. 서 론

클라우드 컴퓨팅(Cloud Computing)은 인터넷 기반 컴퓨팅의 일종으로 정보를 자신의 컴퓨터가 아

닌 인터넷에 연결된 다른 컴퓨터로 처리하는 기술을 의미한다. 공유 컴퓨터 처리 자원과 데이터를 컴퓨터와 다른 장치들에 요청 시 제공하여 언제 어디서나 접근이 가능한 주문형 접근을 가능하게 한다[1]. 이처럼 편리한 즉시성과 효율적인 자원 사용을 장점으로 하여 클라우드 컴퓨팅의 활용도는 급속하게 확대되어 실생활에 다양한 모습으로 서비스 되고 있다. 초기에는 단순한 웹 저장공간 제공 등에 그쳤던 서비

Received(05. 02. 2018), Modified(07. 11. 2018),  
Accepted(07. 16. 2018)

<sup>†</sup> 주저자, chang.myongdo@gmail.com

<sup>‡</sup> 교신저자, iskim11@korea.ac.kr(Corresponding author)

스가 근래에는 인터넷 상에서 서비스 할 수 있는 모든 것들로 확대되고 있다. 그 일례로 2017년 4월 네이버 클라우드 플랫폼을 시작하면서 클라우드 사업을 본격적으로 시작한 네이버는 컴퓨팅, 데이터, 보안, 네트워크 등 인프라 위주의 기술과 서비스를 제공 하였으나, 현재 검색, 음성인식, 지도 등과 같은 오픈 API 형태 제공은 물론이고 인공지능 플랫폼인 클로바(CloVA : Cloud Virtual Assistant) 까지 클라우드 컴퓨팅 환경에서 지원하고 있다.

위의 네이버 예제와 같이 최근에는 기본적인 온라인 상에서의 서비스는 물론이고 한발 더 나아가 4차 산업혁명의 시대에 새롭게 주목받고 있는 인공지능, 자율주행차, IoT 분야에까지 실로 다양한 분야에 클라우드 컴퓨팅이 적극 활용되고 있는데, 이는 인공지능의 머신러닝/딥러닝을 처리하기 위한 대용량의 빅데이터를 위해서는 유연한 고성능 인프라가 필수 요소이기 때문이다[2].

금융권에서도 클라우드 컴퓨팅을 이용하고자 하는 움직임이 많이 있었다. A은행은 최근 개최된 평창올림픽쿠폰을 판매하는 온라인 몰을 퍼블릭 클라우드를 사용하여 오픈 하였으며, B은행은 해외법인의 인터넷뱅킹 웹사이트를 클라우드로 전환하기도 하였고 C카드와 D저축은행은 빅데이터 분석 영역을 클라우드 컴퓨팅으로 전환 할 계획을 발표하기도 하였다. 하지만 이러한 금융회사들의 움직임에도 불구하고 타 업권에 비해 생각보다 그 실적은 미미한 상황이다. 2017년 12월말 현재 27개사 52개 업무용 시스템을 클라우드로 이용 중이며 이 중 카드사와 보험사가 각각 16건(30.8%) 으로 가장 많이 사용하고 있다. 사용업무 또한 개인정보를 처리하지 않는 내부업무 처리가 22건(42.3%)으로 가장 많으며, 그 외 대고객 부가서비스 14건(26.9%)과 회사 및 상품 소개 9건(17.3%) 순으로 다양한 업무에 활용하지는 못하고 있는 실정이다[3].

그 이유는 금융업의 특성 상 고객의 개인 식별정보는 물론 거래에 필요한 각종 민감정보를 처리하고 있어 관련 사고 발생 시 재산에 대한 직, 간접적 피해가 매우 크기 때문이다. 이에 따라 클라우드 컴퓨팅을 활용하기 위해서는 이를 보호하기 위한 다양한 규제를 만족 시켜야만 하게 되었다. 본 연구에서는 클라우드 컴퓨팅에 대한 정보보호 동향과 금융권에서 클라우드 컴퓨팅이 활성화 되기 위한 고려사항들을 알아보고, 현재 구체적인 기준이 없는 금융권 클라우드 컴퓨팅 활용을 위한 비중요 정보처리시스템 지정

에 대한 모델을 제시하여 보고자 한다.

## II. 관련연구 및 동향

### 2.1 클라우드 컴퓨팅의 정의

클라우드 컴퓨팅이란 용어는 2006년 9월 구글 직원 크리스토프 비시글리어(Christophe Bisciglia)가 유휴 컴퓨팅 자원에 대한 활용을 제안하며 최초로 사용 되었으며, 이후 2008년부터 전 세계 IT 분야의 트렌드로 확산 되었는데, 이용자는 IT자원을 필요한 만큼 빌려서 사용하고 서비스 부하에 따라 실시간 확장을 지원 받으며 사용한 만큼만 대가를 지불하는 새로운 컴퓨팅 환경이라고 할 수 있다. 특히 해당 서비스 사용자들은 클라우드 컴퓨팅이나 IT에 대한 전문적인 지식과 기술 없이도 인터넷을 통해 편리하게 애플리케이션, 스토리지, OS 보안 등 자신이 필요한 IT 자원을 원하는 시점에 필요로 하는 만큼만 대가를 지불하고, 서비스를 제공받을 수 있게 되었으며, 기업은 자사의 IT 자원을 보유하고 관리하는 대신, 전기회사에서 공급하는 전기를 이용하듯 간단하고 저렴한 비용으로 IT자원을 빌려서 사용함으로써 관리부담 없이 쉽고 저렴한 서비스를 이용할 수 있게 되었다[4].

Table 1. Definition of Cloud Computing

Institution name	Definition
NIST(National Institute of Standards and Technology)	Users borrow and use IT resources (software, storage, servers, networks) as needed, real-time scalability according to service load, cost-effective computing
Gartner	A form of computing that utilizes Internet technology to provide highly scalable resources to many customers as a service
Forrester Research	Standardized IT-based functions are provided in IP, are always accessible, are variable in response to demand changes, pay for based on usage or advertising.

	and provide a web or programmatic interface
IBM	Environments that can distribute large amounts of data in the Internet virtual space using web-based application software and import or process the data from various terminals such as computer, mobile phone, and PDA
TTA(Telecommunications Technology Association)	Based on virtualization and distributed processing technology, it means a computing environment that rents large-scale IT resources through the Internet and pays as much as it uses.

2.2 클라우드 컴퓨팅의 활용 현황

각 분야별로 다양한 클라우드 컴퓨팅 도입 및 활용에 대한 연구가 진행 되었다. 김동호, 이정훈, 박양표는 각 기업이 클라우드 컴퓨팅을 도입하기 위한 의도에 영향을 미치는 주된 요인을 클라우드 컴퓨팅의 특성 별 가설을 세워 연구 하였는데, 기존에 생각 하였던 확장성, 민첩성, 보안성 보다도 효율성, 경제성, 신뢰성 과 같은 경제적 요인에 도입 의도의 주된 요인이 있다는 연구 결과를 얻었다[5]. 강상백 의 연구는 국내 공공기관 클라우드 컴퓨팅 도입 활성화를 위한 전략으로 미국 공공기관에서 사용하는 SDLC(System Development Life Cycle) 프로세스를 활용하는 방안을 제시 하였다[6].

금융분야에 대한 적용 연구도 있었는데, 민상식, 성재모는 금융서비스에 클라우드 컴퓨팅 활용이 가능한 5가지 모델(Front End 모델, Processing 모델, Storage 모델, Service 모델, Community Unit 모델)을 제시 하였다[7].

클라우드 컴퓨팅으로 인해 발생 가능한 정보보호 이슈 관련 연구도 활발히 진행 되었는데, 김성준 의 연구는 클라우드 컴퓨팅 환경에서 정보를 보다 안전하고 효율적으로 관리하기 위해서는 정보보호관리체계 (Information Security Management System) 수립이 필요함을 주장 하였고[8], 유우영, 임종인의 연구에서는 클라우드 시스템 내 개인정보에 대한 보

호 이슈 해결을 위해 명확한 SLA(Service Level Agreement) 수립, 데이터 저장위치 고지, 데이터 보존관련 절차와 책임 명확화, 개인정보보호 관리체계 인증 등을 해결방안으로 제시하였다[9]. 또한 정원준의 연구에서는 '표준화된 클라우드 SLA 가이드'를 통해 책임소재, 배상액, 면책규정 등을 명확히 규정한 합의 체계가 구축되어야 한다고 주장하였다[10].

이러한 다양한 연구 및 활성화 방안에 힘입어 글로벌 공용(Public) 클라우드 시장 매출액은 매우 빠른속도로 성장하여 왔고 더욱 큰 증가폭으로 사용이 활성화 될 전망이다. 미국의 ICT분야 시장조사 기업인 IDC사는 2016년 965억 달러(약 11조원)에서 2020년 1,950억 달러(약 219조원)에 이르고, 연평균 증가율(compound annual growth report: CAGR)은 20.4%가 될 것으로 예상하고 있다.

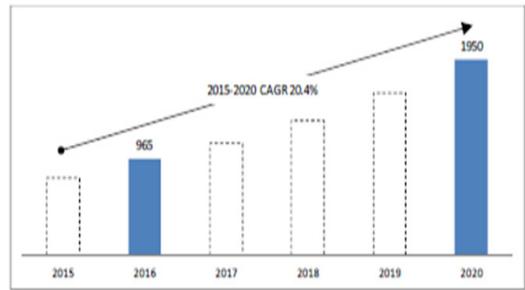


Fig. 1. World Public Cloud Computing Market Outlook(Unit: billion dollars)

서비스 유형별로 시장을 구분하여 보면 퍼블릭 클라우드에는 SaaS(Software as a Service)가 대부분을 차지하고 있으며, 프라이빗 클라우드에는 사업자가 개별 고객을 위한 공간을 할당하여 주는 것을 받아 구성하는 방식(hosted private cloud) 보다는

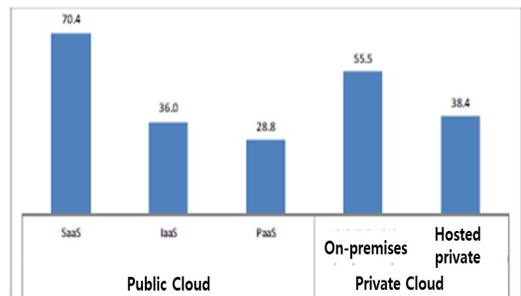


Fig. 2. Configuring the World Cloud Computing Market(Unit : %)

내부에 자체적으로 클라우드 데이터 센터를 구축하는 방식(on-premises private cloud)이 55.5%로 과반수 이상을 차지하고 있다[11].

국내 클라우드 컴퓨팅 시장의 규모는 매출액 기준으로 2014년 5천3백억원에서 2017년 1조5천억원으로 3년만에 3배에 가까운 시장 확대 규모를 보였다. 기업 규모별로 살펴보면 중견기업 이상은 2016년, 중소기업은 2017년에 전년도 대비 50% 가까운 시장 확대 규모를 나타내어 중소기업까지 산업계 전반적으로 클라우드 컴퓨팅 시장이 확대된 모습을 보여 주고 있다[12]. 특히나 공공분야에서는 다양한 연구와 정부의 클라우드 컴퓨팅 활성화 시책으로 인해 정부통합전산센터 클라우드인 G클라우드를 비롯하여 119개 기관 624개 시스템이 클라우드를 도입, 운영 중이며 188개 기관이 2018년 까지 신규 도입할 예정이다[13].

또한 공공 기관에 클라우드를 먼저 전환하고 낮은 등급 자원부터 단계적으로 민간 클라우드 이용을 확대하겠다는 취지로 공공부문의 원스탑 클라우드 조달 체계를 마련하고, 파급효과가 큰 초중고 교육과 정부 R&D 등에서 선도 프로젝트를 추진하여 우수 사례를 도출할 예정이다. 민간부문 클라우드 확산을 위해서는 법령 유권해설서 마련 및 시범사업 등을 통해 인식 변화를 도모할 예정이다[14].

금융분야 에서도 최근 클라우드 컴퓨팅 활성화를 위한 다양한 움직임이 있었는데, 금융감독원은 금융권역 별 클라우드 컴퓨팅 이용 현황<표2>을 발표 하면서 비중요 정보처리 시스템 지정 등 어려운 현안에 대한 FAQ를 예정하는 등 금융회사의 편의성을 제공할 예정이라고 언급 하였다[3].

Table 2. Cloud computing usage by financial sector users

financial Area	domestic financial		Overseas financial	
	Cloud provider	subsidiary	Cloud provider	subsidiary
Bank (2)	2			
Security (7)	3		4	
Insurance (16)	8	1	1	6

Credit Card (16)	16			
Etc. (11)	6		5	
Total (52)	35 (67.3%)	1 (1.9%)	10 (19.2%)	6 (11.6%)

### 2.3 클라우드 컴퓨팅 관련 정책 현황

#### 2.3.1 클라우드컴퓨팅 관련 정책

백승익, 신지연, 김종우 의 연구는 정부의 클라우드 컴퓨팅 활성화 정책에 대한 다양한 프레임워크 기반 분석을 통해 우리나라 클라우드 정책이 소비자 중심보다는 공급자 중심이고, 민간 중심이 아닌 정부 중심으로 이루어져 있어 발전에 한계가 있을 수 있으며, 클라우드 데이터 보호를 위한 법률 제정과 민간 서비스 활성화를 위한 제반환경 개선 정책이 필요하다는 사실을 확인 및 주장 하였다[15].

이러한 요구 사항에 따라 2015년 3월 ‘클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률’을 제정해 2016년 9월에 시행 하였고, 해당 법안에는 ‘정부육성 근거 마련’, ‘제도 개선’, ‘이용자 보호’ 등의 항목이 포함되어 국내 클라우드 사업의 활성화를 촉진하고 이용자가 안전하게 서비스를 사용할 수 있는 근거를 마련하게 되었다[16]. 또한 행정자치부에서는 2016년 6월 ‘개인정보 비식별 조치 가이드라인’을 통해 개인정보의 비식별 조치 기준과 활용 범위 등을 제시하였다.

하지만 여전히 정부주도 정책으로 인하여 공공부문에 한정되어 있고, ICT기술에 대한 별도 법률 제정으로 인하여 타 법과의 충돌의 소지를 내포하고 있으며, 비식별 조치 가이드라인 또한 가이드라인에 그쳐 법적인 실효성은 없는 상태이다. 이정구, 민대환, 권현영은 관련 연구를 통해 2016년 9월 에 시행된 해당 법률에 대해 「정보통신망법」과 「개인정보보호법」에서도 각각의 법이 제정 및 개정될 당시 고려하지 않았던 클라우드 서비스의 특징을 고려하여 함께 개정될 필요가 있다고 주장 하였다[17].

### 2.3.2 금융권 클라우드 컴퓨팅 관련 정책

금융권 클라우드 컴퓨팅 활성화를 위한 정책 연구도 있었다. 도혜지, 김인석은 연구를 통해 비중요 정보처리시스템의 데이터만 처리할 수 있도록 규제하고 있어 고객데이터 분석 및 개인별 맞춤 서비스 제공이 필요한 금융권의 클라우드 서비스 활성화에 걸림돌이 되고 있으며, 비중요 정보처리시스템 지정 대신 영국과 미국의 사례를 통한 감독당국 접근권, 보안인증제와 같은 대안이 필요하다고 주장 하였다[18]. 하지만 아직 개인신용정보의 해외반출 시 문제점 등을 이유로 극히 일부의 상황을 제외하고는 비중요 정보처리시스템 지정을 통해서만 클라우드 컴퓨팅을 사용할 수 있다.

금융감독원은 전자금융감독규정 내 비중요 정보처리시스템 지정 기준 및 절차를 추가하여 금융회사 및 전자금융업자의 클라우드 서비스 사용을 위한 비중요 정보처리시스템 지정에 대해 근거를 마련 하였으며 [19], 금융보안원은 2016년 9월 가이드 제정 및 배포를 통하여 금융회사 클라우드 서비스 사용에 대한 고려사항을 제시 하였으나 가장 중요한 비중요정보처리시스템 지정 기준으로는 범용적인 기준과 몇가지 예시 사항만을 제시하고 있어 금융회사 별 지정에 어려움이 존재한다[20].

Table 3. Considerations when using a financial company cloud computing

Item	Contents
cloud computing Target audience	<p>Non-Critical Information Processing System Designation Criteria and Procedures</p> <p>1) A financial company can designate a system with low impact on the safety and reliability of electronic financial transactions as a non-critical information processing system</p> <p>2) When a cloud company complies with the "Electronic Financial Supervisory Regulations", it can use the cloud without specifying a non-essential information processing system</p>

cloud computing introduction	<p>1) Selection and contract of cloud service provider</p> <p>2) Set up a transition plan to migrate to a cloud service</p>
use cloud computing	<p>1) Protection measures when using the cloud computing</p> <p>2) Link with internal systems of financial companies</p>
cloud computing Management	<p>1) Manage "Service Level Agreement"</p> <p>2) Cloud asset management</p> <p>3) Disaster recovery and incident response management</p>
ex post facto management	Switching Cloud computing and Closing

### III. 금융회사 클라우드 컴퓨팅 고려사항

#### 3.1 개인정보 비식별화

개인정보란 살아 있는 개인에 관한 정보로서 개인을 알아볼 수 있는 정보이며, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보를 포함한다. 금융회사가 개인정보를 클라우드 컴퓨팅에 활용하기 위해서는 식별이 불가능하도록 비식별화 조치를 취해야만 한다. 개인정보에 대한 사전 검토를 통하여 대상 시스템에 존재하는 식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등)에 대해 적절한 비식별 조치(가명처리, 총계처리, 데이터 삭제, 데이터 범주화, 데이터 마스킹 등)를 취해야 한다.

이후 별도의 개인정보 영향평가 수행기관을 통하여 비식별화에 대한 적정성 평가를 수행해야 하는데, 주로 K익명성(k-anonymity), 1-다양성(1-diversity),

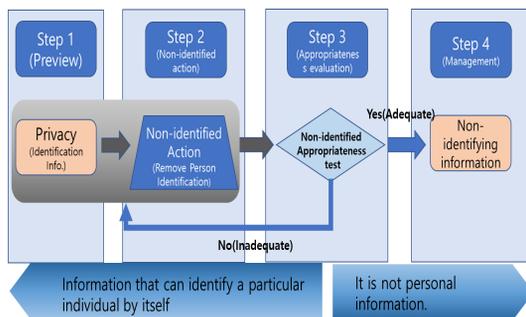


Fig. 3. Personal information non-discrimination procedure

t-근접성(t-closeness) 등을 사용하여 익명화 및 비식별화 수준과 재식별 가능성을 평가한다. 그 결과 비식별화 조치가 적정하다고 평가 된 경우 이를 클라우드 컴퓨팅에 사용 가능하며 사후 관리 절차(재식별화 되지 않도록 주기적인 평가 및 관리)를 진행한다 [21].

### 3.2 비중요 정보처리시스템 지정

#### 3.2.1 정의와 범위

전자금융감독규정 개정안에 따른 비중요 정보처리시스템의 정의는 다음과 같다.

**금융회사 또는 전자금융업자가 자체적으로 수립한 정보자산 중요도 평가기준에 따라 지정한 '전자금융거래의 안전성 및 신뢰성에 미치는 영향이 현저히 낮은' 정보처리시스템**

즉 클라우드 사용을 원하는 금융회사가 자체적인 평가 기준을 마련하고, 그 기준에 따라 해당 시스템을 평가한 결과 '시스템이 전자금융 거래에 미치는 영향이 극히 낮다'라는 결과가 나올 경우 비중요 정보처리시스템으로 지정이 가능하다. 이처럼 중요도 평가를 반드시 수행하여야만 하고, 전자금융거래의 안전성과 신뢰성을 고려하여 선정하여야 할 것을 요구 하였으나 지정에 대한 구체적 기준과 방식 일체는 금융회사에 일임 하였다.

또한 전자금융감독규정 개정안 에서는 비중요 정보처리시스템의 범위를 아래와 같이 한정하였다.

**다만, 개인의 고유식별정보 또는 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인신용정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정할 수 없다.'**

개인식별정보(주민번호, 운전면허번호, 여권번호, 외국인등록번호 등)와 신용정보(계좌번호, 신용카드번호 등)에 대하여 클라우드 서비스를 사용하게 될 경우 정보유출 사고 가능성의 증가 등을 감안하여 해당 정보를 가진 시스템은 비중요 정보처리시스템 지정이 불가하도록 한정하였다.

단, 「개인정보 비식별 조치 가이드라인」(16.7월)을 준수하여 비식별화 하거나, 사내직원 등 전자금융

거래와 관련 없는 고유식별정보 또는 개인신용정보는 처리 가능하도록 예외를 두고 있다[20].

#### 3.2.2 지정기준

금융회사 내 시스템의 중요도 평가에 대한 지정 기준은 금융감독원의 '전자금융감독규정'과 금융보안원에서 제정 및 배포한 '금융회사 클라우드 컴퓨팅 사용 가이드'에서 제시된 기준과 그 예제를 통하여 각 금융회사가 자체적으로 지정하게 되어 있으나 이를 측정하기 위한 기준과 방법이 광범위하고 명확하지 않아 어려움이 있다.

Table 4. Designation Considerations for Non-critical Information Processing System in Financial Institutions

Item	Considerations
Processing information	1) Information Valuation 2) information forgery, Modulation, leakage effect
Other System Connectivity	Level of interference with other systems in case of an incident or disability
System Importance	Importance of information processing system tasks such as recovery target time
system Usage	Uses of Information Processing System(Operating systems, development / test systems and simple facilities, etc.)
Number of system users	Applicable by user type such as outside (customer), inside (in-house) Information processing system users

#### 3.2.3 지정절차

금융회사는 클라우드 컴퓨팅 사용을 위한 비중요 정보처리시스템 지정 필요 시 자체적인 기준에 따라 이를 평가 및 지정한 뒤 그 결과를 조직 내 정보보호 위원회를 통해 심의, 의결하여야 한다. 정보보호위원회 의결절차를 통해 지정이 완료되면 그 결과 보고서에 검토결과, 평가기준, 지정결과 및 관리방안을 작성하여 7일 이내 금융감독원에 제출하여야 한다. 금융감독원은 보고서 검토 후 필요 시 개선/보완 등을 요구할 수 있으며 금융회사는 이를 반영하도록 되어 있다.

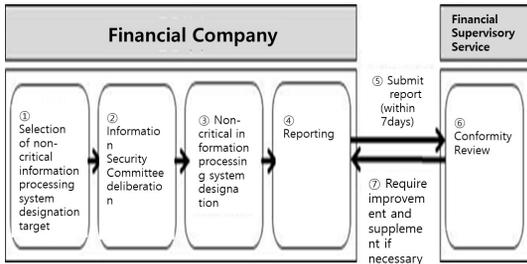


Fig. 4. Procedures for designating non-critical information processing systems

IV. 금융회사 비중요 정보처리시스템 지정방안

이와 같이 현재 금융회사에서 클라우드 컴퓨팅을 사용하기 위해서는 대상 시스템을 '비중요 정보처리시스템'으로 지정 하여야 한다. 물론 이러한 절차 없이 클라우드 컴퓨팅을 사용하는 방법도 있는데 그러한 경우 '전자금융감독규정의 보안기준을 (모두) 충족하는 클라우드 서비스 공급자로부터 서비스'를 받아야만 한다. 전자금융감독규정을 충족하는 기준은 다양한 법률적 해석이 가능하며 금융회사가 아닌 클라우드 업체가 이를 모두 준수하기도 매우 어렵기에 금융회사로서는 금융감독원의 별도 비조치 의견 등 법률적 해석 없이는 이를 활용하기 어렵다. 따라서 본 논문에서는 '비중요 정보처리시스템 지정'의 구체적인 방안에 대하여 제시해 보고자 한다.

4.1 평가 항목 및 가중치

비중요정보처리시스템 지정을 위한 평가 항목은 '대상 시스템 내 개인정보 보유 및 관리현황', '시스템 내 정보의 중요도와 유출 및 위.변조 시 파급효과', '대상 서비스가 장애 및 침해사고 등으로 인한 중단 발생 시 조직에 미치는 영향도' 라는 3개의 구분으로 분류한 뒤 각 구분별로 측정 항목을 세분화 하여 총 11개 항목을 도출 하였다. 금융회사는 각 항목 별 현황을 평가한 뒤 그 결과를 토대로 상, 중, 하 3등급으로 구분하여 가중치를 부여한다.

4.1.1 개인정보 영향도

수집, 보관, 처리하는 정보 중 개인정보에 대한 속성, 유형 및 보유건수 등을 고려하여 해당 정보유

출 시 영향도를 평가한다. 정보의 속성, 유형, 건수, 위변조 발생 시 영향도의 4가지 특성을 기준으로 측정하여 가중치를 산정한다. 고유식별정보의 경우 전자금융감독규정에 의거하여 비중요 정보처리시스템 지정이 불가능 하므로 가중치 부여가 불가하되, 이를 비식별화 하였을 경우는 중요정보 가중치인 2를 적용한다. 식별정보가 아닌 민감정보의 경우에도 최고 가중치 3을 부여하고 비식별화 하였을 경우 2를 부여하여 암호화, 마스킹 등 추가 대책을 통해 비중요 정보처리시스템으로 지정 및 클라우드 활용이 가능하도록 하였다. 또한 개인정보 보유건수의 경우 해당 시스템에서 최근 1년 간 보유 하였던 건수의 최대값으로 한다.

Table 5. Personal information impact assessment items and weights

Item	Explanation	Applicable matter	weight
Privacy property	Unique Identification Information	Resident registration number, Passport number, Driver's license number, Foreigner registration number	Not assignable (unidentified:2)
	Credit Information	Account Number, Credit and check card number, Credit rating etc.	
	Sensitive information	Thought/belief, Join/Leave of Union or party, Political view, Sex life, etc.(Privacy Invasion Information)	3 (unidentified:2)
Medical Information	Health status, medical records,		

	medication history, family history of major diseases, etc.	
Location information	GPS and other personal location identifiable information	
Identification information	Name, address, email, mobile phone number, birth date, gender, etc.	2
Human information	Education, occupation, height, weight, marital status, family matters, friendship, hobbies, etc.	
IT Information	IP address, MAC address, cookie information, site visit information, etc.	1
Non-identifying information	Unidentified information, statistical information, subscriber orientation, etc	
Other information	ID, occupation, other internal identification information, etc.	
No personal information	If you do not hold or handle	

		personal information	
Personal information type	Unstructured data	Handling information is informal by file / image / voice etc.	3
	Formal data	Handling information formatted in DB	
	Important Information Masking	Handling information is masked for important information	2
	encrypted	Handling information is encrypted	1
Number of personal information	No personal information	If you do not hold or handle personal information	
	More than 1 million personal information	If you hold or handle more than 1 million personal information	3
	Less than 1 million personal information	If you hold or handle less than 1 million personal information	2
	No personal information	If you do not hold or handle personal information	1

4.1.2 정보 중요도

수집, 보관, 처리하는 정보 자체의 중요등급 및 그에 따른 중요도를 평가하여 해당 정보자산이 유출되었을 경우 영향을 평가한다. 정보유출 영향도, 정보접근성, 정보특수성, 위변조 영향도 및 가능성 등의 특성에 대해 평가하고 등급을 분류하되 서비스와

연관이 있는 자산들에 대한 최대값을 가중치로 정한다. 정보 중요도의 항목 별 가중치의 경우 정보 자체가 조직에 미치는 중요도는 물론 고객에 대한 영향도를 주요 고려사항으로 감안 하였다. 취급정보가 대외비에 해당하거나 유출 시 조직의 존폐 위협 또는 중대한 손실을 끼칠 우려가 있는 경우 가중치 최고점을 부여하여 비중요 정보처리시스템 지정이 어렵도록 하였고, 특히 위변조 관련 평가를 통해 가중치를 부여함으로써 정보 위변조 시 고객 서비스에 대한 영향과 무결성 검증 가능여부를 감안하도록 하여 고객의 2차 피해를 예방할 수 있도록 하였다.

Table 6. Information importance evaluation items and weights

Item	Explanation	Level	weight
Influence of information leakage	If there is a risk of significant loss or disadvantage to the organization at the time of leakage	High	3
	If there is a risk of loss to your organization in the event of a spill, your competitors may be beneficial to your business, or your business strategy may be inevitable	Medium	2
	If there is no damage or minimal impact on the performance of the organization in case of leakage	Low	1
Information accessibility	If information access is	High	3

	limited to a specific person in the organization (executive, department head, etc.)		
	If information access is limited to internal departments	Medium	2
	Information access is granted not only within the organization but also outside	Low	1
Information specificity	User's personal information	High	3
	Unidentified User Personal Information	Medium	2
	Not employee or personal information	Low	1
Forgery and alteration influence	If there is a significant obstacle or loss of the organization's business and service in the event of forgery or alteration of the asset	High	3
	In the event of fraud or tampering, some of your organizational tasks and services are expected to fail or be damaged.	Medium	2
	Assumed forgery and tampering have minimal	Low	1

	impact on organizational tasks and services		
Possibility of forgery	When asset forgery and tampering are likely and verification of data integrity is difficult in forgery and tampering	High	3
	If there is a possibility of forgery and tampering with the asset, but integrity verification can be performed during data falsification and tampering	Medium	2
	If there is little chance of forgery and tampering with the data and data integrity can be verified during data falsification and tampering	Low	1

4.1.3 서비스영향도

클라우드 컴퓨팅 전환을 원하는 서비스에 대해 시스템 장애 또는 침해사고 등으로 인한 중단 발생 시 조직과 고객에게 미치는 영향도를 평가한다. 서비스 영향도, 서비스 속성, 서비스 복구 목표시간(RTO : Recovery Time Objectives) 등의 항목에 대한 등급을 산정하되 서비스와 연관이 있는 자산들에 대한 최대값을 가중치로 정한다. 조직의 연속성 유지를 위한 주요 서비스 또는 금융회사 본연의 서비스인 경우 가중치를 높게 부여하여 취급정보의 중요도가 떨어지더라도 비중요정보처리시스템 지정을 신중히 검토할 수 있도록 하였다.

Table 7. Service impact assessment items and weights

Item	Explanation	Level	weight
Service Impact	Failure to provide service using handling information will cause serious disruption to the entire organization or customer service.	High	3
	Failure to provide service using handling information If the service causes some disruption to some business or service of the customer	Medium	2
	When the service using the handling information is not available When the range of occurrence of the disability is low or the range of influence is extremely small	Low	1
Service attributes	Services for providing financial services that have a direct impact on customers	High	3
	Services for development and testing of financial services do not have a direct impact on financial services.	Medium	2
	Services for internal business	Low	1

	operations that do not affect financial services		
RTO (Recovery Time Objective)	Need recovery within 3 hours after failure	High	3
	Need recovery within 24 hours after failure	Medium	2
	If you do not have a separate recovery target time or are selected in a range of more than 24 hours	Low	1

4.2 항목별 가중치 평가 방식

클라우드 컴퓨팅 서비스를 활용하고자 하는 시스템에 대한 항목별 가중치를 평가한다. 평가를 위해서는 취급정보 및 시스템에 대한 사전자료 검토는 물론 필요 시 시스템에 대한 실사, 담당자 인터뷰 등의 다양한 방법을 통해 항목별 가중치를 산정하고 이를 각 구분별로 합산하여 산정한다.

Table 8. How to use in weight evaluation

Evaluation method	How	pros and cons
Review materials	Review the related materials provided at the time of request or from time to time (Network diagram, DB schema, security measure definition, encryption status, etc.)	Objective and detailed review possible, but there is a risk if there is a discrepancy between the data and the actual configuration
interview	Review of operation status or policy through interview	It is possible to grasp the current status in detail but it is required to filter subjective

		judgment
Actual check	Direct access to the system	There is a way to get the most accurate information and a limit of manpower and time
Expert Review	Review through expert groups	It is possible to make an accurate judgment in less time, but there is a lack of data leakage concern and understanding of unique work in the organization

4.2.1 개인정보 영향도 평가

평가하고자 하는 자산의 개인정보 영향도 평가항목 별 가중치를 합산하여 평가결과를 산정한다.

Table 9. Personal information impact weighting evaluation method

division	How to calculate by item	Evaluation results
Impact of privacy	Personal information property weight(1~3)	Sum result of each item weights = 3 ~ 9
	Personal information type weight(1~3)	
	Personal information count weight(1~3)	

4.2.2 정보중요도 평가

평가하고자 하는 자산의 정보중요도 평가항목 별 가중치를 합산하여 평가결과를 산정한다.

Table 10. Information importance weighting evaluation method

division	How to calculate by item	Evaluation results
Information Importance	Information leakage impact weight(1~3)	Sum result of each item weights = 5 ~ 15
	Information accessibility weighting(1~3)	
	Information specificity weight(1~3)	
	Forgery influence weight(1~3)	
	Weight for forgery possibility(1~3)	

4.2.3 서비스 영향도 평가

평가하고자 하는 자산의 서비스 영향도 평가항목 별 가중치를 합산하여 평가결과를 산정한다.

Table 11. Service Impact Weighting Method

division	How to calculate by item	Evaluation results
Service Impact	Service Impact Weight(1~3)	Sum result of each item weights = 3 ~ 9
	Service attribute weight(1~3)	
	RTO weight(1~3)	

4.3 비중요 정보처리시스템 지정

4.3.1 중요도 평가대상 선정

개인정보 영향도의 각 측정항목 가중치의 합을 통해 개인정보 중요도를 산정한 뒤 그 범위에 따라 정보처리시스템 중요도 평가대상을 선정한다. 개인정보 가중치 합산 결과가 허용 불가능한 범위(7~9)인 경우 중요 정보처리시스템으로 분류하여 클라우드 컴퓨팅 사용이 불가능하다. 합산 결과가 허용 가능범위(3~6)인 경우 정보처리시스템 중요도 평가대상으로 선정하여 평가를 실시한다.

$$\text{개인정보 중요도} = \text{개인정보 영향도 가중치 합} (3\sim9)$$

Table 12. Selection method of importance evaluation object based on the influence of personal information

Item	range	Classification
Privacy importance	7~9	Important information processing system
	3~6	<b>Information processing system importance evaluation target</b>

4.3.2 중요도 평가 및 비중요 정보처리시스템 지정

정보처리시스템 중요도 평가대상의 '정보중요도 각 항목 가중치의 합' 과 '서비스영향도 각 항목 가중치의 합' 을 합산하여 정보처리시스템 중요도를 최종 산정한다.

$$\text{정보처리시스템 중요도} = \text{정보중요도 가중치 합} (5\sim15) + \text{시스템영향도 가중치 합}(3\sim9)$$

산정된 중요도가 허용범위 이상(17 ~ 24)인 경우 중요 정보처리시스템으로 분류하여 클라우드 지정이 불가능하며, 허용범위 이내(8 ~ 16)인 경우 비중요 정보처리시스템 으로 분류하여 클라우드컴퓨팅 활용이 가능하다.

Table 13. Selection method of non-critical information processing system using information processing system importance

Item	range	Classification
Importance of Information Processing System	17~24	Important information processing system
	8~16	<b>Non-critical information processing system</b>

## V. 결 론

반도체, 자동차, 스마트폰 등 우리나라를 세계 10위의 경제대국으로 키웠던 기간산업들이 이제는 한계에 다다르고 있다. 또한 4차 산업혁명이라는 새로운 패러다임이 시작되는 시점에 세계 각국은 관련 산업의 육성을 위해 발벗고 나서고 있는 상황이다. 우리나라 또한 클라우드, 빅데이터, 블록체인 등 관련 산업에 대한 특별법을 제정하고 정부 주도의 산업 육성에 힘쓰고 있다. 하지만 금융권에서는 이와 같은 신기술의 활성화가 더디게 진행되고 있는데 이는 강력한 관련법률로 인한 사전 진입장벽이 높은 것이 큰 원인 중의 하나라고 할 수 있다. 개인정보보호법과 전자금융거래법 등에서 요구하는 사항을 만족하며 클라우드 컴퓨팅을 활용하기란 굉장히 어려운 것이 현실이다. 특히 클라우드 컴퓨팅을 위해서는 개인정보에 대한 비식별화와 함께 비중요 정보처리시스템 지정이라는 큰 숙제가 존재하게 된다.

본 논문에서는 국내 금융회사에서 클라우드 컴퓨팅 활용을 위한 비중요 정보처리시스템 지정의 구체적인 방법 및 기준을 고민해 보고자 하였다. 그 결과 클라우드 컴퓨팅을 적용하고자 하는 서비스 및 취급 정보를 대상으로 크게 개인정보 영향도, 정보 중요도, 서비스 영향도의 3개 영역으로 구분한 뒤 각 영역 별 항목을 선정하여 개인정보 영향도와 정보처리시스템 중요도를 산출하고 그 결과에 따라 비중요 정보처리시스템을 지정할 수 있는 방안을 제시 하였다.

하지만 본 모델은 국내 금융회사에 한정된 방법으로서 향후에는 해외에 본사를 둔 글로벌 금융회사나 해외에 지점을 둔 국내 금융회사 등 해외 현지법까지 고려 가능한 방안 또는 정책에 대한 연구가 필요하다.

또한 근본적으로 금융회사에 클라우드를 활성화시키기 위해서는 개인신용정보 해외반출 금지, 비중요 정보처리시스템 지정 또는 감독규정을 모두 준수하는 클라우드 서비스 사용 등과 같은 규제에 대한 근본적인 완화 방안이 논의되어야 할 것이다.

## References

- [1] Wikipedia, <https://ko.wikipedia.org/wiki/cloudcomputing>
- [2] Choi J.R., Song Y.M., Kim C.H., Kim S.J., "Cloud Computing Industry Trends for Artificial Intelligence", *Electronic Telecommunications Trend Analysis*, 32(5), pp. 107-116, October 2017
- [3] Financial Supervisory Service, "Financial companies' use of cloud computing", pp.2-3, January 2018
- [4] Kang W.Y., "Recent Trends in Cloud Computing Services", *Internet & Security Issues*, pp. 19-24, October 2017
- [5] Kim D.H., Lee J.H., Park Y.P., "A Study of Factors Affecting the Adoption of Cloud Computing", *The Journal of Society for e-Business Studies*, 17(1), pp. 111-136, February 2012
- [6] Kang S.B., "Cloud Computing Strategy Recommendations for Korean Public Organizations - Based on U.S. Federal Institutions' Cloud Computing Adoption Status and SDLC Initiative-", *The Journal of Society for e-Business Studies*, 20(4), pp.103-126, December 2015
- [7] Min S.S., Seung J.M., "Cloud computing application model and security technology research in financial sector", *Journal of the Korea Institute of Information Security & Cryptology*, 21(8), pp. 40-45, December 2011
- [8] Kim S.J., "Information Security Plan on Cloud Computing - Information Security Management System", *Korean Review of Corporation Management*, 1(2), pp. 194-208, August 2010
- [9] Yu W.Y., Lim J.I., "A Study on the Privacy Security Management under the Cloud Computing Service Provide", *Journal of the Korea Institute of Information Security & Cryptology*, 22(2), pp. 337-346, April 2012
- [10] Jeong W.J., "Legal Issues for Activa-

- ting Cloud Computing". *Information and communication broadcasting policy = ICT & media policy*, 27(2), pp. 25-33, February 2015
- [11] Jeong J.H., "Current Status and Challenges of Cloud Computing", *NARS issue report*, 313, pp. 17-21, December 2017
- [12] Na Y.J., Oh S.J., Kwon H.J., "2017 Cloud Industry Survey Summary Report", pp. 11-12, December 2017
- [13] Future Creation Science Department, "Public sector cloud computing introduction demand survey result disclosure", pp. 1-2, January 2017
- [14] Future Creation Science Department, "2017 K-ICT cloud computing activation enforcement plan", pp. 1-3, January 2017
- [15] Baek S.I., Shin J.Y., Kim J.W., "Exploring the Korean Government Policies for Cloud Computing Service", *Society for e-Business Studies*, 18(3), pp. 1-15, August 2013
- [16] National Law Information Center, "Law Concerning Development of Cloud Computing and User Protection", July 2017
- [17] Lee J.K., Min D.H., 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*, 24(1), pp.81-91, March 2017
- [18] Do H.J., Kim I.S., "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", *The Journal of Society for e-Business Studies*, 22(4), pp.39-51, November 2017
- [19] National Law Information Center, "Electronic Financial Supervision Regulations", 2016
- [20] Financial security officer, "Guide to Using Financial Services in the Cloud", pp. 1-15, October 2016
- [21] Future Creation Science Department, "Personal Information Non-Identification Action Guidelines", pp. 3-16, June 2016

---

**〈저자 소개〉**

---



장 명 도(Myong-do Chang) 정회원  
2002년 2월: 고려대학교 전산학 학사  
2017년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정  
<관심분야> 전자금융보안, 클라우드보안, 블록체인



김 인 석 (In-seok Kim) 종신회원  
1973년: 홍익대학교 전자계산학과(학사)  
2003년: 동국대학교 정보보호학과(석사)  
2008년: 고려대학교 정보경영공학과(박사)  
2009년~현재: 고려대학교 정보보호대학원 교수  
<관심분야> 전자금융보안, IT감사, 전자금융법규