

금융기관 클라우드 시스템 도입을 위한 의사결정 모델에 대한 연구

이 희 석,[†] 김 인 석[‡]
고려대학교 정보보호대학원

A Study on the Decision Making Model for the Introduction of the Financial Institution's Cloud Systems

Hee-Seok Lee,[†] In-Seok Kim[‡]
Korea University, Graduate School of Information Security

요 약

클라우드 시스템 개념이 출현한지 10여년이 지났고, 비용의 효율성 및 보안성이 검증 되었음에도 불구하고, 금융 회사에서는 클라우드 시스템 도입을 주저하고 있다. 고객정보 유출과 관련한 금융당국의 강력한 규제가 주된 이유겠지만, 금융기관들의 클라우드 시스템 도입에 대한 방향성과 기준이 부재한 것도 중요한 이유라고 생각한다.

본 연구에서는 금융회사의 클라우드 시스템 도입에 대한 법적·제도적 제약사항을 살펴보고, 금융기관들이 IT 시스템을 구축할 때 클라우드 시스템 적용 가능 여부와 클라우드 시스템 구성 형태를 결정하는 의사결정 모델을 제시하고자 한다. 본 연구가 많은 금융기관들의 클라우드 시스템 도입 방향성을 수립하는데 많은 도움이 되기를 희망한다.

ABSTRACT

It has been 10 years since the concept of cloud system has emerged. Despite the fact that the cost-effectiveness and security of cloud systems has been proven, financial companies are reluctant to adopt cloud systems. Financial institutions are reluctant to adopt the cloud system because of the strong regulation of financial authorities in relation to the leakage of customer information. However, more important reason why financial institutions hesitate to introduce cloud systems is the lack of direction and standards for the introduction of cloud systems by financial institutions. This study examines the legal and institutional constraints on the introduction of cloud systems in financial institutions and suggests decision models for determining whether cloud systems can be applied and how cloud systems are configured when financial institutions construct IT systems. We hope that this research will be helpful for establishing direction of cloud system introduction of many financial institutions.

Keywords: Cloud system, Decision making model. Financial institutions

I. 서 론

1.1 연구의 배경

대부분의 금융기관에서는 많은 비용을 들여 정보

시스템을 자체적으로 구축해왔다. 금융기관 업무 고유의 특성에 따라 안전하고 신뢰할 수 있는 시스템 구축이 최우선이므로, 상품 처리를 담당하는 계정계 시스템 뿐만 아니라, 정보분석 시스템 및 회사 경영을 위한 경영지원 시스템까지 고 스펙의 자체 시스템

을 구축해왔다. 이는 시스템 구축과 유지 보수에 많은 비용을 초래하였고, 도입과정에서 시간이 많이 소요되어, 금융 트렌드 변화에 빠르게 대처하는데 많은 제약 요소가 되고 있다.

이런 비효율을 극복하고자 글로벌 기업들은 정보 시스템을 자체 구축하는 방식에서 서비스 이용량에 따라 비용을 지불하고, 필요시 즉시 공급받을 수 있는 클라우드 시스템으로 전환하고 있다. 미국을 비롯한 유럽, 일본 등의 해외 주요국에서는 클라우드 시스템 산업의 육성과 클라우드 서비스의 시장 선점을 위해 정부 차원에서 직접적인 기술 개발 투자와 함께 클라우드 컴퓨팅 기업을 적극 지원하고 있다. 특히 이들 해외 주요국의 금융회사들은 클라우드 시스템 산업을 차세대 IT 비즈니스 성패를 결정짓는 메가 트렌드로 인식하고 은행권을 중심으로 클라우드 서비스를 본격적으로 활용하고 있다[1].

그러나 국내의 경우는 클라우드 시스템에 대한 인식 및 신뢰가 부족하고 일부 불명확한 규정과 해석 차이로 도입에 어려움을 겪고 있다. 일부 금융회사들이 클라우드 기반의 시스템을 시범적으로 도입하고는 있지만, 개인의 고유식별 정보 포함에 따른 규제 등 정보보안 측면의 규제로 인해 클라우드 시스템 활성화가 낮은 상태이다. 그러나 이런 법적, 제도적 규제에 앞서 국내 금융기관의 클라우드 시스템 도입이 저조한 문제는 금융회사 자체의 클라우드 시스템 도입 전략 또는 방향성이 부재하다는 것이다.

1.2 연구의 목적

본 연구에서는 국내외 금융기관들의 클라우드 서비스 이용 현황을 파악하고, 클라우드 시스템의 보안 위협 및 사고 사례와, 클라우드 시스템 도입에 대한 법적·제도적 제약사항을 살펴보고, 금융회사가 클라우드 시스템 도입이 미진한 사유에 대해 알아보기로 한다. 본 연구에서는 금융기관들이 IT 시스템을 구성할 때 클라우드 시스템 적용 가능 여부와 클라우드 시스템 구성 형태를 결정하는 의사결정 모델을 제시하고자 한다. 의사결정 모델은 해당 시스템이 클라우드 시스템 도입과 관련한 법적 제도적 제약사항 준수 여부를 확인하고, 해당 업무시스템을 클라우드로 전환 시 서비스 유형과 상제 필요 클라우드 자원을 결정하는 모델이다.

II. 금융권 클라우드 시스템 이용현황

2.1 국내 클라우드 시스템 이용 현황

국내 금융권에서의 클라우드 서비스는 클라우드 컴퓨팅의 한 축을 이루고 있는 '가상화'에 초점이 맞춰져 있으며, 특히 금융당국이 금융사 전산센터에 대한 물리적 망 분리 의무화와 전 지점에 대한 점진적 망 분리 방침을 밝히면서 가상화 솔루션을 기반으로 클라우드 서비스가 전파되고 있는 상황이다. 하지만 이는 보안만을 강조한 조치로 클라우드가 갖는 본래 성격인 비용 절감, 유연한 자원의 재분배 등에 대해서는 효용성을 제대로 발휘하지 못하고 있다[1].

금융회사의 클라우드 시스템 도입사례로는 신한은행은 직원 PC의 가상화 저장공간을 구축하고 사내 문서 및 정보 공유 플랫폼으로 사용하고 있고, 기업은행도 고객센터의 업무 환경을 클라우드 컴퓨팅 환경으로 전환을 위해 상담용 PC 300 여대의 가상화 작업을 완료하였다. 금융권 시장 악화로 비용 절감에 관심이 높은 중소 금융사에서조차 클라우드 서비스 도입에 관심을 갖고 있다.(Table 1 참조)

Table 1. Introduction of Domestic Financial Cloud

Division	Company Name	Contents
Bank	Shinhan Bank	Create virtual storage space for employee PC and use it as an in-house document and information sharing platform
	Industrial Bank	Transform your customer center's work environment into a cloud computing environment
Securities	Samsung Securities	Use virtualization technology to enable mobile trading regardless of smartphone operating system (OS) and terminal
	Mirae Asset Securities	Applying virtualization technology to mobile trading system to connect to other smartphone or tablet PC and use it in the same user environment without resetting
Card	Kookmin Card	Establish a big data-based financial platform with kt

국내에서는 범정부 차원의 클라우드 발전법 시행 (2015.9) 및 2021년 클라우드 선도국가 도약을 위한 정책을 추진하여, 통신사와 대형 IT 업체 중심의 클라우드 서비스 제공 중이다. 국내 금융회사들은 클라우드 기반 시스템을 시범적으로 도입하고 있으나, 애플리케이션 등 기업 인프라 측면에서의 클라우드 서비스 도입은 아직 낮은 수준이다.

2018년 1월 금융감독원의 '금융회사의 클라우드 이용 현황'과 관련한 발표 자료에 따르면, 내부 업무 처리, 부가서비스 제공, 회사 상품 소개, 투자 정보 분석 등 고객 정보보호와 관련 없는 시스템 위주로의 활용이 늘어나고 있는 추세이나, 비중요 정보 처리 시스템의 경우 클라우드 시스템 적용이 가능하나, 고유식별정보 및 개인신용정보를 처리 하는 시스템은 비중요 시스템으로의 분리가 어려운 상황으로 금융회사 내부에서의 활용 확대가 어려운 상황이다[3]. (Table 2 참조)

Table 2. Current status of domestic financial companies' cloud adoption

Usage	Num	Ratio (%)	Specific examples
Internal Business Processing	22	42.3	Email, Electronic Form Management, Messenger, etc
Providing Additional Services	14	26.9	Recommend Album, Save Images, etc
Company · Product Introduction	9	17.3	Company and Brand, Book, Record, Exhibition, etc
Investment Information Analysis	4	7.7	OTC derivatives valuation, Information Analysis such as Exchange Rate, Index, Oil Price etc.
Insurance Accounting	2	3.9	Insurance Account Analysis, Change Warranty Option Analysis, etc.
Authorization	1	1.9	Storing Authentication-related Information
Sum	52	100.0	

2.2 국외 클라우드 시스템 이용 현황

미국, 영국, 중국 등은 클라우드의 중요성을 인식하고, 공공부문의 업무 혁신과 자국 기업의 경쟁력 강화를 위해 클라우드 정책을 추진하고 있다[4].

해외 주요국은 클라우드 컴퓨팅 산업의 육성을 위한 정책적인 기반 마련 뿐만 아니라 클라우드 서비스의 시장 선점을 위해 정부 차원에서 직접적인 기술 개발 투자와 클라우드 컴퓨팅 기업에 대해 적극 지원 중이다. 아마존 · 구글 · IBM · 세일즈포스닷컴 등 글로벌 IT기업들은 대표적인 클라우드 컴퓨팅 사업자로서 인프라 서비스(IaaS), 플랫폼 서비스(PaaS), 응용 소프트웨어 서비스(SaaS) 등 다양한 유형의 서비스 사업모델을 보유하고 있다[5]. (Table 4 참조)

이들 해외 주요국의 금융회사들은 클라우드 컴퓨팅 산업을 차세대 IT 비즈니스 성패를 결정짓는 메

Table 3. Major Countries' Cloud Policy Implementation Status

Division	Major policies
US	Establish policies to drive cloud adoption first, and enable public sector cloud utilization using security certification via security policies (FedRAMP, 2012) *US Department of State, Ministry of Finance, etc. 7 departments 101 (48 private clouds) Cloud use
UK	Build Public Procurement Service Governance to Enable Cloud (March, 2011), Open 'Cloud Store' to Drive Public Sector Cloud Use *About 2,000 companies (80 %) registered 19,533 services in stores
China	Announcement of the six key strategies for realizing the world's highest level of cloud * (January 2015), announcing the Internet Safety Act, which places the cloud data center within the country (2015). *Enhancing cloud supply capability (private cloud development), enhancing enterprise innovation capacity, e-government development, building cloud infrastructure, strengthening security, etc
France	Driving the creation of a cloud data center to secure sovereignty over the data held by U.S. cloud enterprises and to nurture the enterprise (2011) * Private and government jointly invest €150 million (about 180 billion won) in two cloud infrastructure projects

Table 4. Cloud Service business model comparison

Biz model	Key contents	Major Biz owner
Infra Service (IaaS)	Service computer resources that provide virtualized computing resources (virtual servers, virtual storage, virtual networks, etc.) are charged according to usage.	Amazon's Storage Service
Platform Service (PaaS)	A service that provides the foundation (platform) for new software developments	Google App Engine Services
App S/W Service (SaaS)	Service to provide a variety of applications in the form of On Demand	Salesforce .com's CRM service

가 트렌드로 인식하여, 은행권 중심으로 클라우드 서비스를 본격 활용 중이다.

미국을 포함한 아메리카권 뿐만 아니라 스페인, 네덜란드 등 유럽권, 호주, 일본 등의 아시아권 금융회사들도 클라우드 서비스 구현에 노력 중이다. 미국

금융권에서는 비민감 정보나 고객 불만을 클라우드 컴퓨팅을 통해 관리하거나 불만 패턴을 분석, 고객 만족도를 제고하는 전략을 추진 중이며, 대표적으로 씨티은행은 계정계에 보관하는 민감 개인 정보를 제외한 나머지 정보에 대해서 클라우드 기반의 서비스 환경을 제공한다. 일례로, 소프트웨어 개발 시 구축과 테스트, 모바일, 보안, 분석 서비스까지 전반의 업무 프로세스를 클라우드 상에서 제공하는 것은 소프트웨어의 실제 효용성을 검증할 수 있어 적용까지의 과정을 단축하는 효과가 있다.

스페인 금융권에서는 전 세계 직원 간 협업 증진을 지원해 줄 소프트웨어적 도구(tool)로서 클라우드 기반의 업무시스템을 도입·활용하고 있다. 스페인 마드리드에 본사를 둔 글로벌 은행인 BBVA (Banco Bilbao Vizcaya Argentaria)는 스페인 본사와 26개 해외지역 직원(약 11만 명) 간에 협업을 지원하기 위해 업무혁신 중심의 클라우드 시스템(Google Apps) 적용하였다. BBVA 은행은 협업 환경 구축을 통해 직원들의 더욱 빠르고 쉬운 의사결정, 그룹 내 창의적인 마인드 보유, 신상품 개발과 판매 기간 단축 등의 변화 기대한다.

Table 5. Major Foreign Financial Firms ' Cloud Services Status

Finance Co.	Service Content	Operation Model	Service Purpose
Citi Bank (US)	Introducing a cloud system for non-sensitive information areas	Hybrid Cloud	Increase customer satisfaction
USAA (US)	Introduction of integrated cloud-based authentication services(Verisign) to each subsidiary (Insurance, Banking and Card)	Community Cloud	Certification Services
BBVA (Spain)	Introducing a cloud-based business system (Google Apps) for collaboration between employees worldwide	Community Cloud	Internal business collaboration
DNB (Netherlands)	Introduced AWS cloud system support mobile banking and retail banking	Public Cloud	Data Storage Management Risk Management Analysis
Barclays (UK)	Introduced AWS cloud system for risk analysis	Public Cloud	Big Data Analysis
Deutsche Bank (Germany)	Introducing Cloud systems for Big Data analytics for intranet and intelligence	Hybrid Cloud	Financial fraud, Data Analysis
Common Wealth Bank (Australia)	Introduction of Hadoop-based data analysis cloud system for big data utilization	Hybrid Cloud	DB Integration
Tokyo Mitsubishi Bank (Japan)	Consolidate over 300 Distributed DBs into private cloud systems	Private Cloud	Prevent information leakage, maintain business continuity

네덜란드 중앙은행(De Nederlandsche Bank: 이하 DNB)은 아마존 웹 서비스(Amazon Web Service)에 기반을 둔 위험관리 분석 용도로서 퍼블릭 클라우드(Public Cloud)를 적용하였다. 네덜란드 중앙은행은 웹 사이트, 모바일 앱, 리테일 뱅킹, 신용분석 등 대부분의 업무를 아마존 웹서비스에서 구현하였다.

호주의 커먼웰스 은행(Commonwealth Bank)은 300여 개의 분산된 DB를 통합할 목적으로 오라클 기반의 프라이빗 클라우드(Private Cloud) 시스템을 적용하였다. 커먼웰스 은행은 과거 인터넷뱅킹과 모바일뱅킹 비중의 급속한 확대로 약 3억 달러의 IT 투자수요가 발생하자 클라우드 시스템 도입을 통해 DB 통합을 단행, 연평균 약 1억 달러의 IT 인프라 투자 및 관리 비용 절감 효과를 달성하였다.

일본 도쿄 미쓰비시 은행은 프로젝트 수행에 따른 정보 유출 문제 해결, 자연재해에 대비한 업무 연속성 유지 등의 목적 수행을 위해 시스템과 비즈니스 부서 대상으로 25,000여 대의 데스크탑 클라우드를 이용한 업무 환경을 구축하였다. 도쿄 미쓰비시 은행은 프로젝트를 위해 개별 PC를 지급하고 프로젝트가 끝나면 저장 정보를 삭제·반납하는 과정을 반복하면서 정보 유출 문제에 봉착하여 본사 전 직원과 지

점, 파트너사를 위해 총 60,000여 대의 컴퓨터를 데스크탑 클라우드로 구현할 예정이다(5).(Table 5 참조)

2.3 금융권 클라우드 시스템 보안위협 및 사고 사례

클라우드 서비스는 서비스를 구성하는 요소와 방법이 다양하기 때문에 이러한 특성에 따른 보안위협이 발생할 수 있다. '클라우드 서비스 정보보호 안내서'에 따르면 클라우드 보안위협을 ① 가상화 취약점 상속, ② 정보위탁에 따른 정보 유출 위협, ③ 자원 공유 및 집중화에 따른 서비스 장애, ④ 단말 다양성에 따른 정보 유출, ⑤ 분산처리에 따른 보안 적용의 어려움, ⑥ 법규 및 규제 문제 총 6가지로 분류하고 있다(6).(Table 6 참조)

클라우드 서비스의 사고의 주요 원인은 주로 하드웨어 등 시스템 오류, 천재지변 및 관리 실수가 대부분이나, 최근에는 해킹에 의한 장애도 일부 발생하고 있으며, 시스템의 중요도 및 활용도가 높아질수록 위협 요소는 증가할 것으로 예상된다(1).(Table 7 참조)

Table 6. Cloud service security threats

Security Threats	Threat content
Inherit virtualization vulnerability	<ul style="list-style-type: none"> - Malicious code infections and spread threats · Malicious code infection between host OS and guest OS · Proliferation to guest OS in the event of hypervisor infection - Service Availability Infringement
The threat of information leakage as a result of consigned information	<ul style="list-style-type: none"> - Information leakage by insiders · User information access due to admin's abuse of authority · Delete and modify guest OS data without user recognition - Accessing information from unauthorized users
Information leakage based on diversity and loss of user terminal	<ul style="list-style-type: none"> - Loss of terminal, Information leakage by weak security terminal
Service interruption due to resource sharing and focus	<ul style="list-style-type: none"> - Service interruption for all customers in case of system failure · Difficult to quickly identify the cause of service interruption · User can not recover and patch - It is vulnerable to attack such as DDoS when the central system location is exposed
Difficulty enforcing security as a result of distributed handling	<ul style="list-style-type: none"> - Increased authentication and access control complexity with resource shares and virtual machine dynamic rebalancing - Difficult to apply collective authentication and access control to distributed computing systems
Issues of law and regulation	<ul style="list-style-type: none"> - Responsibility for information leakage unknown - Difficult to detect audit trail as a result of sharing resources.

Table 7. Cloud service security incident case

Year	Cause	Type	Company	Key contents
2012	System error	Service failure	KT	Service failures due to uCloud server switch malfunction
			SalesForce	NA2 service interruption due to storage storage failure
	Management Mistake	Data loss	First Server	5,698 data losses due to errors during system upgrade
	Natural Disaster	Service failure	Amazon	Interruption of service, such as Netflix, Pin test and Instagram, due to a power failure caused by a storm
	Hacking	Spam	Drop box	Hacking Dropbox user accounts, leaking lists of emails from employee accounts and sending spam to those users
		Data Leakage	Dream Host	Log into DB to leak personal information
Apple	Hackers take advantage of 'Find My Mac Book' vulnerability to delete personal information			
2013	Management Mistake	Service failure	Amazon	An administrator mistakenly deleted the load balancing script, so it can not work properly with ELB and Netflix suffered connection failure.
	Hacking	Data Leakage	Enernote	User name, mail address, encrypted password has been leaked from the cloud system providing memo and information policy
			Adobe	Adobe server hacked, leaking 2.9 million personal information and part of SW source code such as Acrobat
ZenDesk	Hacked into the ZenDesk system to leak personal information			
2014	Hacking	Data Leakage	Apple	Hack into the accounts of the iPhone cloud to leak and distribute the photos of the Hollywood actor
2015	Management Mistake	Service failure	Amazon	Access to content such as Netflix, Airbnb, and IMDb is not available for 6 to 8 hours

III. 클라우드 시스템 이용 관련 제약사항

3.1 금융권 클라우드 시스템 관련 법규 현황

금융권 클라우드 시스템 적용을 위해 검토해야 할 주요 법규 및 가이드는 「클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률」(이하 '클라우드컴퓨팅법'), 「전자금융 감독규정」(2016. 10. 5 개정), 「금융회사의 정보처리 업무 위탁에 관한 규정」, 「개인정보 비식별 조치 가이드라인」, 금융보안원은 「금융권 클라우드 서비스 이용 가이드」 등 참조하여 적용 가능성 여부를 판단할 수 있다.

「클라우드컴퓨팅법」 제21조는 '다른 법령에서 인가·허가·등록·지정 등의 요건으로 전산시설·장비·설비 등을 규정한 경우 해당 전산시설 등에 클라우드 컴퓨팅 서비스가 포함되는 것으로 본다.' 라고 하여 클라

우드 컴퓨팅 서비스 이용에 대해서 "원칙 허용, 예외 금지"라는 이른바 네거티브 규제 원칙을 적용하고 있으나, 법 제4조(다른 법률과의 관계)에서는 클라우드 컴퓨팅 법은 다른 법률에 우선하여 적용하여야 한다. 다만, 개인정보 보호에 관하여는 「개인정보 보호법」, 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」 등 관련 법률에서 정하는 바에 따르도록 되어 있어 개인 정보 보호가 우선으로 적용됨을 알 수 있다. 법 제 23조 제2항에서는 클라우드 서비스 제공자가 제공하는 서비스에 대해 정보보호 기준의 준수여부 확인을 인준기관이 평가·인증하여 이용자들이 안심하고 클라우드 서비스를 이용할 수 있도록 클라우드 보안 인증제도를 시행하고 있다.

이와 관련하여 금융위원회는 클라우드컴퓨팅 등 새로운 IT 기술 및 핀테크 산업 발전 등 변화된 현실에 맞게 「전자금융 감독규정」을 개정(2016. 10.

5) 하여 금융회사는 고객정보 처리시스템을 제외한 일부 전산시스템에 대하여 클라우드 컴퓨팅을 이용할 수 있도록 '비중요 정보처리시스템'의 지정기준과 절차를 정하고, 비중요 정보처리시스템으로 지정될 경우에 물리적 망 분리 등의 적용을 배제하여 클라우드 컴퓨팅 서비스를 이용할 수 있도록 하였다.

금융보안원의 「금융권 클라우드 서비스 이용 가이드」에서 개인의 고유식별 정보(「전자금융 감독규정」은 별도 정의를 두고 있지 않으나, 「개인정보보호법」에서 규정한 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호를 의미) 또는 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인 신용정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정할 수 없으나, 「개인정보 비식별 조치 가이드라인」을 준수하여 비식별화된 고유식별정보 또는 개인신용 정보를 처리하는 시스템은 클라우드 시스템 서비스 이용이 가능함을 예시하고 있다.

글로벌 클라우드 컴퓨팅 서비스 제공자들의 경우 데이터 센터를 세계 각지에 두고 있기 때문에 글로벌 기업이 제공하는 클라우드 컴퓨팅 서비스의 경우 개인 정보가 국경을 넘어서 저장되거나 국가 간에 재유통될 수 있으나, 개인 정보를 「개인정보 비식별조치 가이드라인」(2016.6.30.)에 따라 비식별 조치된 경우에는 더 이상 개인 정보가 아니므로 개인정보 국외 이전 제한 규정의 적용을 받지 아니한다.

금융분야는 「금융회사의 정보처리 업무 위탁에 관한 규정」으로 개정(2015. 7.)되면서 국외 IT회사 등 제3자에 대한 정보처리 업무 위탁이 가능해짐에 따라 금융 분야에서도 클라우드 컴퓨팅 서비스를 이용하는 것이 원칙적으로 가능해졌다.

금융보안원의 「금융권 클라우드 서비스 이용 가이드」에서 비중요 정보처리시스템의 지정기준, 클라우드 컴퓨팅 서비스 제공자 선정, 클라우드 컴퓨팅 서비스 이용 시 보호대책, 재해복구 및 침해 사고 대응 관리 등을 안내하고 있다.

클라우드 시스템 적용을 위해 비중요 정보처리시스템으로의 지정되는 것이 우선이며, 고유식별정보 또는 개인신용 정보를 비식별화 조치를 통해 비중요 정보화 가능성을 검토하여 적용범위의 확대와 국가간의 서비스 확대 등을 기대 할수 있으며, 민간기업의 클라우드 서비스 확대를 위해 클라우드 보안 인증제도 등의 시행 등이 진행되고 있다[2].

3.2 비중요 정보처리 시스템 지정 방법

2016년 10월 금융위원회는 「전자금융감독규정」을 개정하면서 고객정보 처리시스템을 제외한 일부 전산시스템에 대하여 클라우드 시스템을 이용할 수 있도록 비중요 정보처리시스템의 지정기준과 절차를 정하고, 비중요 정보처리시스템으로 지정될 경우에 물리적 망 분리 등의 적용을 배제하여 클라우드 컴퓨팅 서비스를 이용할 수 있도록 하였다.

전자금융감독 규정에서는 비중요 정보처리시스템 지정에 대해 다음과 같이 가이드하고 있다.

① 금융회사 또는 전자금융업자는 자체적으로 수립한 정보자산 중요도 평가 기준에 따라 전자금융거래의 안전성 및 신뢰성에 미치는 영향이 현저히 낮은 정보처리시스템을 비중요 정보처리시스템으로 지정할 수 있다. 다만, 개인의 고유식별 정보 또는 「신용정보의 이용 및 보호에 관한 법률」에 따른 개인신용 정보를 처리하는 정보처리시스템은 비중요 정보처리시스템으로 지정할 수 없다.

② 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템 지정 시 제8조의2에 따른 정보보호 위원회의 심의·의결을 거쳐야 한다.

③ 금융회사 또는 전자금융업자는 제1항에 따라 비중요 정보처리시스템을 지정한 날로부터 7일 이내에 금융감독원장이 정하는 양식에 따라 정보자산 중요도 평가 기준, 지정 결과, 관리 방안 등을 포함한 보고서를 금융감독원에 제출하여야 한다.

④ 금융감독원장은 제3항에 따라 제출한 보고서를 검토한 결과, 평가 기준, 지정 결과, 관리 방안 등이 적합하지 않다고 판단되는 경우에는 금융회사 또는 전자금융업자에 대하여 개선·보완을 요구할 수 있다. 또한, 비중요 정보처리시스템만 존재하는 전산센

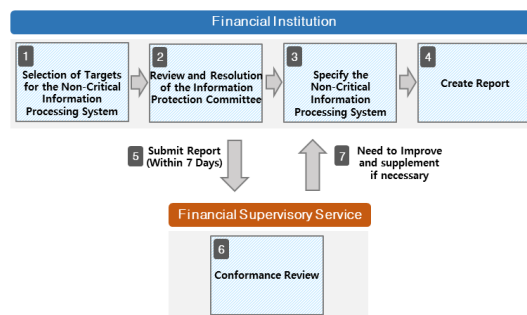


Fig. 1. Procedures for specifying non-critical information processing systems

터에 대해서 전산센터의 국내 위치, 무선통신망 설치 금지, 인터넷 등 외부 통신망의 물리적 분리 제약사항을 두지 않고 있다.

금융보안원의 클라우드 서비스 이용 가이드에서는 비중요 정보처리시스템 지정 시 다음의 사항을 고려하도록 하고 있다.

① 처리 정보의 중요도(고객정보, 사내정보, 공개 정보 등) 및 정보 위·변조·유출 시 파급효과 고유식별 정보 또는 개인신용 정보를 처리(송신, 수신 또는 전달 포함)하는 경우 비중요 정보처리시스템으로 지정 불가. 다만, 「개인정보 비식별 조치 가이드라인」을 준수하여 비식별화하거나, 사내직원 등 전자금융 거래와 관련 없는 고유식별정보 또는 개인신용정보는 처리 가능

② 침해 사고 또는 장애 발생 시 타 시스템의 업무 연속성 저해 수준 등 타 시스템과의 연계성, 연계된 타 시스템의 업무 중요도(전자금융 거래업무, 단순 정보 제공 업무 등)

③ 복구 목표시간 등 해당 정보처리시스템의 업무 중요도

④ 운영, 개발, 테스트 시스템 및 단순 설비 등 정보처리시스템의 용도

⑤ 고객 또는 사내 직원 등 이용자 유형에 따른 해당 정보처리시스템 이용자 수(외부, 내부 등 이용자 유형 별 해당 정보처리시스템 이용자 수)

금융회사가 자체적인 판단 기준으로 정보 자산의 중요도를 판단하기 위한 점검 절차 수립이 요구되며, 고유식별정보, 개인신용정보등의 비식별화 조치가 되었을 경우 클라우드 서비스의 적용 가능성에 대한 기준이 필요하다.

3.3 금융권 클라우드 시스템 도입절차

금융보안원에서는 클라우드 시스템 도입 시 준수해야 할 사항을 클라우드 제공자 선정, 클라우드 제공자 계약, 이전 및 전환 계획 수립 3영역으로 분류하여 가이드 하고 있다.

첫째, 클라우드 제공자 선정에서는 ① 장애 대응, 침해사고 대응체계 구축 등 보안성, ② 클라우드 제공자의 국내 법규 준수 여부, ③ 금융회사의 내부통제 절차를 클라우드에 적용 가능 여부, ④ 금융회사의 기존 정보보호시스템, 보안솔루션과 상호 호환 가능 여부, ⑤ 특정 클라우드 제공자에게 종속되지 않도록 클라우드 간의 상호 호환 가능 여부, ⑥ 재무구조,

수익 및 신용도 등 클라우드 제공자의 신뢰성에 관한 사항, ⑦ 기타 금융회사 자체적으로 수립한 선정 기준 등을 고려해야 한다.

둘째, 클라우드 제공자와의 계약에서는 ① 클라우드 제공 범위, ② 클라우드 이용 시 발생하는 정보에 대한 금융회사의 소유권, 저작권 및 지식 재산권, ③ 클라우드 제공에 따른 정보보호의 역할과 책임(상호 연대책임을 포함) 및 비밀유지에 관한 사항, ④ 클라우드 제공자에 대한 금융회사 및 금융당국의 해당 외부주문과 관련된 자료제출 요구 및 검사 수용의무, ⑤ 정보보호 관련 법적 요구사항 및 정책 준수에 관한 사항, ⑥ 금융회사의 정보가 저장되는 국가의 명칭 등 정보 제공에 관한 사항, ⑦ 클라우드 제공자의 재위탁에 관한 사항 ⑧ 손해배상 및 계약해지에 관한 사항, ⑨ 클라우드 전환 및 종료 시 정보의 안전한 파기 및 반환에 관한 사항, ⑩ 기타 리스크관리 등을 위하여 필요한 보안 요구사항 등을 고려해야 한다.

셋째, 이전 및 전환 계획 수립에서는 ① 이전·전환하고자 하는 자산 목록 등 이전·전환 범위, ② 시스템 성능, 용량, 보안 위협 등 업무 영향도, ③ 금융회사 내부 업무시스템과의 연계, ④ 이전·전환에 따른 업무연속성, ⑤ 이전·전환 단계별 발생 가능한 문제점 분석 및 예방대책 등을 고려해야 된다.

마지막으로 금융회사는 시스템을 클라우드로 이전 또는 타 클라우드로 전환하고자 하는 경우 「금융회사의 정보처리 업무 위탁에 관한 규정」 제7조에 따라 금융감독원장에게 보고하여야 한다(7).

3.4 금융권 클라우드 시스템 이용시 보호대책

금융보안원에서는 클라우드 시스템 이용 시 금융회사의 자산 및 정보를 보호하기 위하여 다음과 같은 보호 조치를 하도록 권고하고 있다.

첫째, 금융회사는 클라우드 제공자의 외부망에 위치한 비중요 정보처리시스템에 대해서는 동일 클라우드를 이용하는 외부기관의 통신망과 분리·차단하고 접속을 금지하여야 한다.

둘째, 금융회사는 클라우드 제공자의 내부망에 위치한 비중요 정보처리시스템에 대해서는 인터넷 등 외부 통신망 및 동일 클라우드를 이용하는 외부기관의 통신망과 분리·차단하고 접속을 금지하여야 한다.

셋째, 금융회사는 업무용 단말기 및 내부망에 위치한 정보처리시스템을 클라우드 제공자의 내부망에 연결하거나, 관리용 단말기를 클라우드에 연결해야

하는 경우 「전자금융 감독규정 시행세칙」의 망 분리 대체 정보보호 통제 수칙을 준수하고 전용회선 또는 전용회선과 동등한 보안 수준을 갖춘 가상의 전용회선(VPN 등) 사용해야 한다.

넷째, 금융회사는 업무용 단말기 및 내부망에 위치한 정보처리 시스템을 클라우드 제공자의 외부망에 연결해야 하는 경우 「전자금융 감독규정 시행세칙」의 망 분리 대체 정보보호 통제 수칙을 준수하여야 한다.

다섯째, 금융회사는 단말기 및 정보처리시스템을 클라우드 제공자의 내부망에 연결해야 하는 경우 암호화된 통신채널을 사용하여야 한다[7].

IV. 금융권 클라우드 시스템 도입에 대한 문헌 연구

4.1 선행연구 분석

클라우드 도입과 관련된 연구들은 클라우드 서비스의 보안관리 체계의 확립과 이에 맞는 개인정보 보호를 체계에 대해 논의가 되었으며, 금융기관의 특화된 관점에서 볼 때 클라우드 시스템 확대를 위해 규정 개정 및 가이드 등을 제시하고는 있지만, 명확한 기준제시와 이해가 부족함을 지적하고 서비스 제공자의 보안 수준과 법률 준수 여부를 평가할 수 있는 체계 수립의 필요성에 대해 논의되고 있다.

도혜지,김인석[8]의 “비중요 정보처리시스템으로 한정된 국내 금융권 클라우드 시장 활성화를 위한 제언”에서는 클라우드 관련 법 제정 이후 클라우드 시장은 조금씩 성장하고는 있으나, 금융권에서는 크게 실감하지 못하고 있는데, 이는 최근 개정된 전자금융 감독규정은 비중요 정보처리시스템에만 클라우드 서비스 도입을 허용하고, 보안 이슈에 대한 명확한 대책을 제공하지 못하고 있기 때문이며, 국내 클라우드 시스템의 활성화를 위해 중요 정보 처리 시스템도 클라우드를 적용 할 수 있는 명확한 가이드 제공이 필요하며, 금융권에 특화된 보안 인증제를 도입해 클라우드 서비스 제공자의 보안수준과 법률 준수 여부를 평가·보증할 수 있는 환경 구현이 필요함을 제시하고 있다.

보안인증제도의 필요성에 대해서 정준화[9] “클라우드 컴퓨팅의 현황과 과제”에서 우리나라의 클라우드 컴퓨팅 기술 수준은 2017년말 기준으로 미국 대

비 72.4% 수준으로, 이는 유럽·일본뿐만 아니라 중국보다도 낮고, 기업의 클라우드 이용율(종사자 10인 이상 기업의 클라우드 컴퓨팅 이용율)은 OECD 33개국 국가 평균은 24%인데 비해 우리나라는 12.9%로 전체 국가중 27위 수준이다. 국내의 클라우드 컴퓨팅 산업을 활성화하기 위해서는 첫째, 클라우드 컴퓨팅 기술개발 및 표준화, 전문인력 양성, 안정적인 데이터 센터 기반 마련등이 필요하며 둘째 클라우드 컴퓨팅의 수요 확대를 위한 정보제공 및 인식 개선 셋째로 안전한 이용을 위해 클라우드 컴퓨팅 보안강화, 보안인증 제도의 개선의 필요성을 제시하였다.

클라우드 시스템의 활용을 높이기 위한 제도적 보완책에 대해 이창범[10]의 “클라우드 컴퓨팅의 안전한 이용과 활성화를 위한 법적 과제”에서는 클라우드 컴퓨팅 산업의 촉진 및 이용 활성화를 위해서는 사전 인증 및 사후 보증 체계 구축을 통한 클라우드 서비스의 신뢰성 및 안정성 제고, 클라우드 서비스의 상호 운용성 확보를 위한 표준화, 클라우드 컴퓨팅의 정보 보안, 개인 정보보호 등 각종 법률 이슈와 예상되는 다양한 이해관계 충돌 문제에 대응할 수 있도록 서비스 제공자와 이용자 대상 지침 근거 마련, 클라우드 속에 있는 기업의 정보자산에 대한 접근권 보장, 정보자산의 실제 위치와 선택권 보장, 정보자산의 부적절한 접근 방지와 오남용 방지 등이 법 제도로 검토해야 한다고 주장하고 있다.

신경아,이상진[11] “클라우드 컴퓨팅 서비스에 관한 정보보호 관리 체계”에서는 정보보호 관리체계는 조직의 보안관리 및 IT 운영의 보안 지표로 활용되어 왔으며 클라우드 서비스를 위한 기존 IT 환경과는 다른 관점의 보안 관리와 평가기준이 필요하다 하였음.

클라우드 서비스의 핵심요소를 클라우드 위협관리 영역으로부터 도출하고, 클라우드 핵심요소에 치우쳐 기본적인 보안관리가 누락되지 않도록 기존 정보보호 관리체계의 모든 통제 영역을 포함하되, 클라우드 보안관리 영역에 맞는 정보보호 관리 체계를 제안하였다.

이보성,김범수[12] “클라우드 서비스 유형별 개인 정보보호 방안”에서는 클라우드 서비스 유형에 따라 개인 정보의 저장 방식이 달라지며 이에 따라 개인정보의 처리 및 보호 방안이 달라질 수 있음을 제시하였다.

클라우드에서 서비스를 제공하는 정보통신서비스

제공자 및 클라우드 컴퓨팅 서비스 제공자 간의 권한과 의무를 명확하게 규정함으로써, 클라우드 산업 활성화와 이용자 정보 보호라는 목표를 달성할 수 있다고 예측하였다.

유우영, 임종인[13] “클라우드 컴퓨팅 서비스 제공자의 개인 정보보호 조치 방안에 대한 연구”에서는 클라우드 컴퓨팅 서비스의 많은 장점으로 인해 민간 기업에서 클라우드 컴퓨팅을 이용한 서비스 환경 구축에 대한 요구 사항이 커질 것으로 예상되기 때문에 클라우드 서비스 제공자는 개인 정보보호와 관련된 데이터 보존 방법, 데이터 보관에 대한 물리적 위치 고지, 개인 정보보호와 관련된 법률 분쟁 발생시 재판관할권 문제 등에 대하여 이용자 개인 정보보호를 위한 보호장치를 마련하는 등 클라우드 서비스 이용자 보호를 위한 제도 및 책임 기준을 마련할 필요가 있음에 대해 논의하였다.

백승익, 신지연, 김중우[14] “국내 클라우드 정책 분석 및 발전 방향에 관한 연구”에서는 우리나라 정부에서 클라우드 컴퓨팅 확산을 위해 소개한 정책을 평가·분석한 결과, 우리나라의 클라우드 컴퓨팅을 위한 정책은 소비자 중심이 아닌 서비스 공급자 중심이고, 민간 중심이 아닌 정부중심으로 이러한 불균형은 우리나라의 빠른 클라우드 컴퓨팅 확산을 방해 할 것이라는 주장을 하였다.

유기조[15] “클라우드 컴퓨팅 도입 가이드”에서는 클라우드 컴퓨팅은 ICT 기술 경쟁력을 확보 할 수 있으며, IT운영의 효율성 측면에서 도입의 활성화가 필요하나, 서비스를 사용하기전에 SLA에 대한 주의 깊은 검토를 해야 하며, 클라우드 데이터와 웹 브라우저의 관리 측면에서 불패 보안 취약점에 대한 면밀한 검토를 통해 클라우드 서비스의 신뢰성 확보가 필요함을 언급하고 있으나 구체적인 적용 방안에 대한 의견 제시는 부족하였다.

김성철[16] “클라우드 컴퓨팅 활성화를 위한 정책 개선 방안에 관한 연구”에서 클라우드 서비스 활성화를 위해 법·제도적 기반 확충을 위한 기반 마련을 언급하면서 클라우드 컴퓨팅 서비스는 지리적 환경에 제약을 받지 않는 글로벌 서비스 라는 점에서 인프라, 제공사업자 및 이용자에 대하여 각종 국내법의 적용에 한계가 발생할 가능성이 매우 높기 때문에 각국의 법령 및 규제 현황에 대한 조사·분석을 통해 국내에서도 동일한 수준의 법규 마련이 필요하며, 클라우드 도입시 영향도가 높은 금융, 의료, 교육 등의 산업군에 대해 전산설비 구비의무를 완화하고, 조세

인센티브 등을 제도를 도입하여 클라우드 활성화를 유도하여야 한다고 표현하고 있다.

클라우드 서비스와 관련하여 과거에는 이용자의 정보보호를 위한 법률적 제안사항으로 서비스의 확대가 어려운 상황이었다. 최근 규정 개정 및 가이드 등을 제시하고는 있지만, 명확한 기준제시와 이해가 부족하여 클라우드 활성화에는 많은 어려움이 있음을 선행연구에서는 논의하고 있으나, 이를 개선하기 위한 이행방안에 대한 제시가 없어 본 논문에서는 현재 금융회사들이 적용하고 있는 현황을 중심으로 현실적인 대안을 제시하고자 한다.

V. 금융기관 클라우드 시스템 도입 의사결정 모델

5.1 클라우드 시스템 도입 의사결정 모델 구성

금융권 클라우드 시스템 도입 의사결정 모델은 크게 ① 클라우드 시스템 적용 가능성 검토, ② 클라우드 시스템 서비스 유형 및 적용방법 결정, ③ 클라우드 시스템 서비스 상세 구성요소 도출, 3단계로 구분하여 구성하였다.

첫째, 클라우드 시스템 적용 가능성 검토는 신규 도입 또는 클라우드로 이전하려는 시스템이 법적 제약사항을 만족하는지 또는 해당 시스템이 클라우드 시스템으로 전환 시 비용 절감, 가용성 및 확장성, 기술 용이성 기타 운영의 효율성 등의 적정성을 검토하는 부분이다.

둘째 클라우드 시스템 서비스 유형 및 적용방법 결정 부분은 신규 또는 이전 시스템이 클라우드로 전환 효용성이 있을 경우, 어느 구성 방식으로 하는 것이 최대 효과를 가져올 수 있는지 판단하는 모델이다.

셋째, 클라우드 시스템 서비스 상세 구성요소 도출은 클라우드 구성 방식이 도출된 이후 필요한 상세 H/W 및 S/W 또는 필요 서비스가 무엇인지 도출하

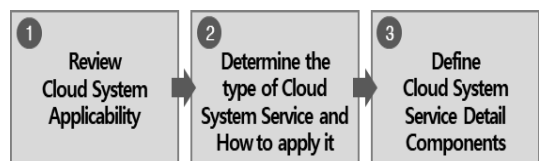


Fig. 2. Cloud Systems Implementation Decision Model Definition Procedures

는 모델이다.

5.2 클라우드 시스템 적용 가능성 검토 모델

클라우드 시스템 적용 가능성 검토 모델은 클라우드 시스템 관련 금융감독법규를 기반으로 크게 ① 처리 정보의 중요성, ② 시스템 운영의 효율성 부분으로 구분하였다. 2개 영역의 평가배점은 처리정보의 중요성을 60점, 시스템 운영의 효율성을 40점으로 구성하였다. 처리정보의 중요성과 시스템 운영의 효율성은 2영역 모두는 클라우드 시스템 도입 기준에 있어 중요한 판단 기준이다. 처리정보의 중요성이 정보보안적 측면의 도입기준 이라면, 시스템 운영의 효율성은 실질적 시스템 운영에 대한 현실적 문제이다. 따라서 2가지 판단기준은 우선순위를 정할 수 없을 만큼 둘 다 중요하지만, 본 연구에서는 처리 정보의 중요성을 시스템 운영의 효율성보다 클라우드 시스템 도입 판단기준에 우선순위를 두었다.

금융회사의 현실적인 입장에서 시스템 운영의 복잡성, 돌발 상황 대응의 신속성, 운영 비용 등 시스템 운영의 효율성이 더 중요할 것이다.

그러나 시스템이 회사 내부가 아닌 외부에 있는 만큼 고객정보 등 민감정보의 대량 유출사고 발생 시 회사의 평판 리스크에 치명적 타격에 따른 비즈니스 연속성에 문제가 발생하여 해당 시스템의 운영 자체를 할 수 없는 경우가 발생할 수 있기 때문이다.

그렇다고 미래의 불확실한 돌발 상황에 대비한 처리정보의 중요성만 상대적으로 높은 비율의 평가 배점을 부여 할 경우에는 클라우드 시스템으로 전환이 현 시스템 운영 대비 비용적인 측면, 운영의 효율적인 측면에서 불리함에도 불구하고, 클라우드 시스템으로 전환이 적절하다는 판단이 나올 수 있는 오류를 범할 수 있다.

따라서 본 연구에서 클라우드 시스템 도입 기준에 대한 2개 영역의 평가 배점 기준은 처리정보의 중요성이 시스템 운영의 효율성보다 평가배점에 있어 우선순위를 가지되, 그 차이를 최소화하고자 6:4의 평가배점 비율을 정의하였다.

또한 전자금융감독규정에 따라 중요정보의 비식별화가 이루어지지 않은 시스템은 클라우드 시스템 도입 자체가 불가한 것으로 정의하였다. 즉 중요정보의 비 식별화 미조치는 본 도입 검토 모델 이전 Knock-Out 요건으로 처음부터 도입 불가 기준을 마련하였다.

처리 정보의 중요성은 다시 ① 정보의 속성 ② 비 식별화 조치 ③ 정보의 규모 ④ 정보 유출시 파급효과로 구분하고 각 항목의 점수가 높을수록 중요 시스템이라 판단하여 클라우드 시스템으로 전환이 어렵고, 점수가 낮을수록 클라우드 시스템으로 구축이 용이한 것으로 판단하였다.

평가항목의 총 배점 60점 중 고유 식별 정보의 포함 유무를 처리 정보의 중요성 평가에 가장 중요한 항목으로 20점으로 부여하고, 나머지 항목은 균등하게 10점으로 부여하였다.

각 항목별 세부 항목으로는,

첫째 정보의 속성은 고유 식별정보와 기타 식별정보로 구분하고, 고유 식별정보가 포함될 경우는 해당 정보의 비 식별화 조치를 전제로 하였다.

앞서 말한바와 같이 비 식별화 조치를 하지 않았을 경우는 전자금융감독규정에 따라 클라우드 시스템 구축 자체가 불가한 것으로 정의하였다.

둘째 비 식별화 조치 방법은 비 식별화 강도가 강한 순으로 데이터 삭제, 통계 및 범주 처리, 데이터 암호화, 데이터마스킹으로 분류하고 강도가 강할수록 클라우드 시스템 구축이 용이한 것으로 판단하였다.

셋째 정보의 규모는 데이터량이 적을수록 정보 유출 리스크가 적어지므로 클라우드 시스템 구축이 용이한 것으로 판단하였다.

마지막으로 정보 유출시 파급효과는 대외 신뢰도 및 업무 서비스 영향도가 낮을수록 비 중요시스템으로 클라우드 시스템 전환이 용이한 것으로 판단하였다.

Table 8은 앞서 말한 클라우드 시스템 적용가능성 검토 기준 중 처리 정보의 중요성 평가항목과 평가기준, 평가배점을 도표화 한 것이다.

시스템 운영의 효율성 평가 항목은

① 이용자 수 ② 타 시스템 연계성 ③ 시스템 가용성 ④ 시스템 용도 ⑤ 시스템 구성 ⑥ 자원 사용률 ⑦ 비용으로 구분하였다. 처리 정보의 중요성과 동일하게 각 항목의 점수가 높을수록 중요 시스템이라 판단하여 클라우드 시스템으로 전환이 어렵고, 점수가 낮을수록 비 중요시스템으로 클라우드 시스템으로 구축 및 전환이 용이한 것으로 판단하였다.

평가항목의 총 배점은 40점으로, 타 시스템 연계성 시스템 용도, 자원 사용률, 전환비용 평가항목을 시스템 운영의 효율성의 중요 판단 기준이라고 판단하고 높은 배점을 부여하였다.

각 항목별 세부 평가 항목으로는,

Table 8. Criteria for the importance of processing information

Division		Evaluation standard	Points	Remarks
Information's Property	Unique Identification Information	Resident registration number, Passport number, Alien registration number, Driver's license number 1.No information available : 0 2.Perform non-Identification :20	20	Unique identification information is based on non-Identification
	Other Identification Information	Address, e-mail, IP, Anniversary Information, account number, medical record, Copyright information and other information 1.No non-Identification : 10 2.With non-Identification : 0	10	
Perform Non-Identification	How to Perform non-Identification	1.Delete Data : 1 2.Statistics and Categories : 3 3.Data Encryption: 5 4.Data Masking:10	10	
Scale of Information	Amount of Data	1.More than 100,000 :10 2.More than 10,000 & Less than 100,000 : 5 3.Less than 10,000 : 1	10	
Spillover Effect on Information Leakage	External Reliability and Business Service Impact	1.Business service interruption : 10 2.Partial suspension of business services : 5 3.Less impact on business services :1	10	
Sum			60	

첫째 이용자 수는 내부 이용자 수와 고객 이용자 수로 구분하고 이용자 수가 적을수록 클라우드 시스템 전환이 용이한 것으로 판단하였다.

둘째 타 시스템 연계성은 장애 시 연계시스템 파급효과와 연계시스템 중요도로 구분하였다. 장애 시 연계시스템의 파급효과가 적고, 연계시스템의 중요도가 낮을수록 비 중요시스템으로 클라우드 시스템 전환이 용이한 것으로 판단하였다.

셋째 시스템 가용성은 시스템 이중화 구성, 장애 시 목표 복구 시간, 수기작업 대체 가능 여부로 구분하고, 시스템 이중화 강도가 약하고, 목표 복구 시간이 길고 수기작업 대체가 가능할수록 비 중요시스템으로 클라우드 시스템 구축 및 전환이 용이한 것으로 판단하였다.

넷째 시스템 용도는 시스템의 업무 성격으로 대고객 서비스가 아닌 내부 지원용 시스템일수록 장애 시 파급효과가 적어 클라우드 시스템 구축 및 전환이 용이한 것으로 판단하였다.

다섯째 시스템 구성은 특정 H/W 및 S/W에 종속적이지 않고 범용 표준 구성일수록 클라우드 시스템 구축 및 전환 용이한 것으로 판단하였다.

여섯째 자원 사용율은 시스템의 자원 사용률이 균등하지 않고 Peak 시의 자원 사용율의 편차가 클 경우 클라우드로 구축 시 자원의 탄력적 사용이 가능

하여 클라우드 시스템 구축 및 전환이 용이한 것으로 판단하였다.

마지막으로 비용은 매몰비용과 데이터 이전비용으로 구분하고, 클라우드 시스템으로 이전 시 기존 시스템의 매몰 비용이 작고, 데이터 이전 비용도 작을수록 비용 효율성이 커지므로 클라우드 시스템 구축 및 전환이 용이한 것으로 판단하였다.

클라우드 시스템 적용 가능성 검토 최종 평가는 처리 정보의 중요성 평가점수와 시스템 운영의 효율성 평가점수의 상관관계 매트릭스를 만들어 매트릭스 상 2개 영역의 점수가 교차한 값을 최종 평가점수로 산정한다. 이 최종평가 점수가 30점 이하일 때 클라우드 시스템 구축이 가능한 것으로 판단한다.

		The Importance of Processing Information													
		0	5	10	15	20	25	30	35	40	45	50	55	60	
The Efficiency of System Operations	0	0	5	10	15	20	25	30	35	40	45	50	55	60	
	5	5	10	15	20	25	30	35	40	45	50	55	60	65	
	10	10	15	20	25	30	35	40	45	50	55	60	65	70	
	15	15	20	25	30	35	40	45	50	55	60	65	70	75	
	20	20	25	30	35	40	45	50	55	60	65	70	75	80	
	25	25	30	35	40	45	50	55	60	65	70	75	80	85	
	30	30	35	40	45	50	55	60	65	70	75	80	85	90	
	35	35	40	45	50	55	60	65	70	75	80	85	90	95	
	40	40	45	50	55	60	65	70	75	80	85	90	95	100	

Fig. 3. Cloud Systems Scoring Matrix

Table 9. Criteria for Evaluating the Efficiency of System Operations

Division	Evaluation item	Evaluation standard	Points	Remarks
User count	Internal User Count	1.More than 100 People : 2 2.More than 10 People : 1 3.Less than 10 People : 0	2	The same time Number of accessors
	Client User Count	1.More than 1000 People : 3 2.More than 100 People : 2 3.Less than 100 People : 1	3	
Connection with other systems	Failure-In Connection System Ripple Effect	1.Interruption of the Linked System : 5 2.System Performance Degradation : 3 3.Less Influenced:1	5	
	Linked System Important	1.Client Service : 3 2.Internal Analysis System : 2 3.Internal Support System : 1	3	
System Availability	Configuring System Redundancy	1.Real-time Redundancy : 3 2.Redundant System : 2 3.Single-System : 1	3	
	Recovery from Failures	1.Within 3 hours : 3 2.Within 6 hours : 2 3.Within 24 hours : 1	3	
	Manual Work Alternative Possible	1.Non-Substitutability : 2 2.Substitutability : 1	2	
System purpose	System Configuration Purpose	1.Client Service : 2 2.Internal Service System : 1	2	
System Configuration	Specific System Dependencies	1.Dedicated Architecture : 2 2.Standard Architecture :1	2	
Resource usage rate	A Change in the Use of Resources	1.More than 70% :5 2.More than 50% :3 3.Less than 50% :1	5	
Cost	Sunk Cost	1.More than 1 billion won : 5 2.More than 500 million won : 3 3.Less than 500 million won : 1	5	
	Data Transfer Cost	1.More than 500 million won : 5 2.More than 300 million won : 3 3.Less than 300 million won : 1	5	
Sum			40	

5.3 클라우드 시스템 서비스 유형 및 적용방법 결정 모델

클라우드 시스템 적용 서비스 유형 결정 모델은 이미 알려진 IaaS, PaaS, SaaS 3개의 서비스 모델 및 해당 모델에 적용되는 시스템 구축 방법을 결정하는 모델이다. 이 모델은 가트너의 클라우드 전환 방식 5가지 모델[17]에 2가지 모델 Remain 과 Retire를 추가하여 총 서비스 적용 방법은 7개로 분류하였다.

첫째 Remain은 신규 시스템 구축 또는 현 시스

템 전환을 클라우드로 적용 불가능한 모델이다. 클라우드로 구축 시 시스템 운영의 효율성이 현 시스템 운영보다 떨어지는 경우이다.

둘째 Retire는 단순 백업용 데이터 보관에 해당되는 모델이다. 클라우드 서비스 모델이 IaaS인 경우에 해당된다. 소스코드, 미들웨어, 프레임워크, 데이터베이스 등 중요 IT시스템 자원은 그대로 현 시스템을 사용하고 오직 백업 데이터만 보관하기 때문에 어떠한 변경 개발도 필요 없고, 시스템 구조도 매우 단순하다.

셋째 Rehost는 기존의 사용하던 데이터베이스,

어플리케이션, 운영체제 등을 동일하게 다른 하드웨어 환경으로 이동하는 경우이다. 클라우드 서비스 모델이 IaaS인 경우에 해당된다. 현재 사용 중인 어플리케이션과 미들웨어를 그대로 이미지화하여 클라우드 시스템에 업로드하는 방식으로, 신속한 클라우드 시스템 구축이 가능하다. 어플리케이션 및 아키텍처 변화가 없어 구축 비용은 적으나, 확장성이 떨어지는 단점도 있다.

넷째 Refactor는 기존 어플리케이션의 데이터베이스 및 미들웨어 등을 변경하여 클라우드 환경으로 이전하는 경우이다. 클라우드 서비스 모델이 PasS인 경우에 해당된다. Rehost에 비해 미들웨어 및 데이터베이스의 수정이 필요하기 때문에 이행 난이도가 있으며, 비용도 Rehost 보다 많이 소요되는 방식이다.

다섯째 Revise는 기존 어플리케이션을 분해하여 Rehost와 Refactor를 조합하여 적용하는 방법이다. 클라우드 서비스 모델이 PaaS인 경우에 해당된다. 기존 어플리케이션의 소스코드 변경과 미들웨어의 변경이 동시에 발생하므로 복잡한 아키텍처 구조로 성능 문제가 발생할 수 있다.

여섯째 Rebuild는 기존 어플리케이션을 재설계하거나, 어플리케이션을 클라우드 기술을 통해 신규개발하여 최적의 클라우드 어플리케이션을 개발하는 방법이다. 클라우드 서비스 모델은 PaaS인 경우에 해당된다. 기존 어플리케이션과 데이터모델을 고객 맞춤화하여 성능 향상을 할 수 있는 장점이 있으나, 기존의 소스코드 및 개발 프레임워크가 반드시 유지되지 않는다는 단점도 있다.

마지막으로 Replace는 클라우드 환경에서 제공되는 소프트웨어를 사용하는 방법이다. 클라우드 서비스 모델은 SaaS인 경우에 해당된다. 기존 어플리케이션을 새로운 클라우드 전용 어플리케이션으로 대체하는 방식이라 적용이 매우 용이하고 최신 기술이 적용된 어플리케이션을 항상 이용 가능하다는 장점이 있으나, 특정 부분의 커스텀이징이 어려울 수 있다는 단점도 있다.

앞서 말한 7가지의 클라우드 서비스 유형 및 적용 방법 결정을 위한 평가 모델은 ① 시스템 인프라 관점, ② 어플리케이션 특성 관점, ③ 업무 정책 관점, ④ 운영 및 데이터 이행 관점에서 진단 항목을 구성해 보았다.

첫째 시스템 인프라 관점은 해당 기관이 OS, 서버, 스토리지, DBMS 등 시스템 운영 역량을 보유

Table 10. Types of cloud services

Service Model	How to apply the service		Remarks
-	Remain	-	Cloud not Applicable
IaaS	Retire	Archiving	Data Storage
	Rehost	Lift & Shift	Follow the Current Operating Environment
PaaS	Refactor	Lift & Reshape	Optimize Specific Service Clouds
	Revise	Reshape & Lift	Rehost & Refactor
	Rebuild	Cloud Native	Apply Cloud Architecture
SaaS	Replace	Drop & Shop	Replace with New Service

여부, 현 시스템 사용 소프트웨어가 가상화 환경 지원 여부, 현 시스템 인프라의 재구성 가능 여부로 구성하였다.

둘째 어플리케이션 특성 관점은 어플리케이션 소스의 리컴파일 적용 가능 여부, 요구사항 변화 여부, 어플리케이션 변경사항 적용 속도, 어플리케이션이 OS 및 특정 제품에 대한 종속성 여부, 어플리케이션 재설계 가능 여부, 컴포넌트 모듈화 등 최신 개발 방법론 적용 가능 여부, 3 tier구조 웹 어플리케이션 여부, 오픈소스 사용 여부, Java 및 C# 이외 프로그램 언어 사용 여부, 다른 웹어플리케이션 또는 클라우드 상 어플리케이션과 연동 가능 여부, 클라이언트 단말에서 접근여부로 구성하였다.

셋째 업무정책 관점으로는 업무 프로세스의 변경 가능 여부, 통합 연계 등 시스템 프로세스 변경 가능 여부, 테이블 컬럼 추가, 속성 변경 등 데이터 모델 변경가능 여부로 구성하였다.

마지막으로 운영 및 데이터 이행 관점은 클라우드 적용 속도, 비용 대비 운영의 효율성, 시스템 부하 예측의 어려움에 따른 확장성 고려 여부로 구성하였다.

Table 12는 7가지의 클라우드 시스템 적용 방법을 결정하기 위한 기준을 정리한 것이다.

각 진단 질문에 대한 응답의 결과가 (Y or N) 7 가지 클라우드 시스템 적용 방법과의 연관도 순서를 1 ~ 7까지 부여해 보았다. 클라우드 시스템 적용방법이 해당질문과의 연관도가 전혀 없으면 0으로 표시하였다. 예를 들어 가장 첫 질문인 인프라 영역의 운영역량으로 “현 시스템의 담당자가 시스템 운영에 대한 역량을 충분히 보유하고 있는가?” 의 질문의 결과가 ‘Y’ 이면 이 질문은 Retire 방법과 가장 연관도가 높고 Replace 방법과 가장 연관도가 없는 질문이다. 질문의 결과가 ‘N’ 이면 이 질문은 Rehost 방법과 가장 연관도가 높고 Remain 방법과 가장 연관도가 없는 질문이다. 연관순서에 대해 점수산정을 위한 가중치는 Table 11과 같이 정의하였다. 연관도가 제일 높은 1인 경우는 40%, 연관도가 제일 없는 7인 경우는 3%, 전혀 없는 경우는 0%로 정의하였다. 따라서 ① 대 분류 배점과 ② 상세 분류 배점 ③ 진단질문에 대한 연관도 배점의 곱으로 각 진단질문에 대한 점수를 산출하였다. 각 진단질문별 점수의 합이 가장 큰 서비스 적용 방법이 해당시스템의 클라우드 시스템 적용방법으로 정의하였다.

결국 Table 12는 사용자가 해당 진단 질문에 ‘Y’ 또는 ‘N’로 응답만 할 경우 기 정의된 점수의

합으로 클라우드 시스템 적용 방법을 결정할 수 있는 모델을 만든 것이다.

Table 11. Rate of scoring of questions associated with each service type

Association	①	②	③	④	⑤	⑥	⑦	-
Scoring rate	40%	20%	15%	10%	7%	5%	3%	0

클라우드 시스템 서비스 적용방법 결정을 위해 대 분류 배점 비율과 상세항목의 배점 비율, 그리고 질문연관도 배점 비율 3개 항목의 곱의 결과를 산출한다. 질문연관도 배점은 각 질문에 대한 결과 (Y or N) 에 대한 연관도 점수를 산출한다.

최종 서비스 적용방법 결정은 앞서 말한 7가지의 적용 방법별 각 진단 질문에 대한 평가결과 점수의 최종합이 제일 높은 서비스 적용 방법을 해당시스템의 클라우드 시스템 적용 방법으로 정하였다.

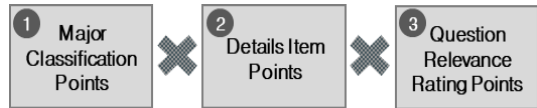


Fig. 4. Determine how to apply final cloud system services

Table 12. How to Apply Cloud Service Diagnose Table

① Main Category		② Detail Category	③ Diagnostics content	Result	Remain	Retire	Rehost	Refactor	Revise	Rebuild	Replace
Infra (50%)	Operational Capability	10%	Does the organization have the capability to operate the system?	Y	2	1	3	4	5	6	7
				N	1.00	2.00	0.75	0.50	0.35	0.25	0.15
	Virtualization Environmental Support	20%	Does your software support your virtualized environment?	Y	6	7	1	3	2	4	5
				N	0.50	0.30	4.00	1.50	2.00	1.00	0.70
	Infra Reconstruct-able	70%	Can the system infrastructure be reconfigured to be cloud-optimized?	Y	2	1	7	5	6	4	3
				N	2.00	4.00	0.30	0.70	0.50	1.00	1.50
Application (30%)	Recompile	10%	Recompile source code is it applicable?	Y	6	7	4	1	2	3	5
				N	0.15	0.09	0.30	1.20	0.60	0.45	0.21
				Y	5	6	1	0	4	2	3
				N	0.21	0.15	1.20	0.00	0.30	0.60	0.45

Applic-ation (30%)	Requirements Changed	9%	Does it require frequent business changes?	Y	6	7	4	2	3	1	5	
				N	0.14	0.08	0.27	0.54	0.41	1.08	0.19	
	Rate of Change Application	9%	Should the change be applied faster than other systems?	Y	0	0	1	4	3	0	2	
				N	0.00	0.00	1.08	0.27	0.41	0.00	0.54	
	Dependencies for a particular product	9%	Is there a problem with the current system being dependent on a particular product?	Y	6	7	4	2	3	1	5	
				N	0.14	0.14	0.08	0.54	0.41	1.08	0.27	
	Application Redesign Status	9%	Can you invest time and money to redesign and optimize your application?	Y	0	0	1	2	3	4	5	
				N	0.00	0.00	1.08	0.54	0.41	0.27	0.19	
	Possibility to Apply the Latest Methodology	9%	Will you apply the latest technology methodology?	Y	6	7	4	3	2	1	5	
				N	0.14	0.08	0.27	0.54	0.41	1.08	0.19	
	Web Application Structure	9%	3 tier structure web application?	Y	6	0	1	2	4	5	3	
				N	0.14	0.00	1.08	0.54	0.27	0.19	0.41	
	Use Open Source	9%	Are you using a variety of products such as open source and commercial products?	Y	5	6	4	1	3	2	7	
				N	0.19	0.14	0.27	1.08	0.41	0.54	0.08	
Applic-ation (30%)	Progaming Language Type	9%	Is it used in a variety of programming languages other than Java,C #?	Y	5	6	2	4	3	1	7	
				N	0.19	0.14	0.54	0.27	0.41	1.08	0.08	
	Cloud Application Interlink	9%	Need to be able to work with applications on the cloud system?	Y	6	0	4	1	3	2	5	
				N	0.14	0.00	0.27	1.08	0.41	0.54	0.19	
	Client Terminal Access	9%	Access from various users and terminals	Y	6	7	5	2	3	4	1	
				N	0.14	0.08	0.19	0.54	0.41	0.27	1.08	
	Work Policy (10%)	Possible Change of Business Process	40%	Can the processes be changed?	Y	0	0	1	0	2	0	0
					N	0.00	0.00	1.08	0.00	0.54	0.00	0.00
		Possible System Process Changes	20%	Is it possible to integrate and modify the system processes to a higher level	Y	6	7	5	2	3	4	1
					N	0.20	0.12	0.28	0.80	0.60	0.40	1.60
		Possible Data Model Change	40%	Do we need to maintain the current system in the data model, location, etc?	Y	5	0	1	3	2	4	0
					N	0.28	0.00	1.60	0.60	0.80	0.40	0.00
					Y	5	6	4	2	1	3	7
					N	0.14	0.10	0.20	0.40	0.80	0.30	0.06
				Y	0	0	5	3	4	2	1	
				N	0.00	0.00	0.14	0.30	0.20	0.40	0.80	
				Y	5	6	1	2	3	4	7	
				N	0.28	0.20	1.60	0.80	0.60	0.40	0.12	
				Y	0	0	5	4	3	2	1	
				N	0.00	0.00	0.28	0.40	0.60	0.80	1.60	

Data Migration (10%)	Cloud Transition Speed	40%	Need to get to the cloud faster than other systems?	Y	6	7	1	2	3	5	4
					0.20	0.12	1.60	0.80	0.60	0.28	0.40
				N	4	5	7	6	3	1	2
					0.40	0.28	0.12	0.20	0.60	1.60	0.80
	Operational Efficiency	20%	Should the operational efficiency be significantly higher than that of other systems?	Y	6	7	3	4	5	1	2
					0.10	0.06	0.30	0.20	0.14	0.80	0.40
				N	6	0	3	2	1	4	5
					0.10	0.00	0.30	0.40	0.80	0.20	0.14
	Scalability	40%	Is it difficult to predict the load and requires high scalability considerations?	Y	6	7	3	2	5	1	4
					0.20	0.12	0.60	0.80	0.28	1.60	0.40
				N	6	7	2	4	1	3	5
					0.20	0.12	0.80	0.40	1.60	0.60	0.28

5.4 클라우드 시스템 적용 서비스 구성 요소 결정 모델

클라우드 시스템 적용 서비스 구성요소 결정은 앞서 클라우드 적용 가능성 검토와 클라우드 시스템 서비스 유형 및 적용 방법 결정 모델 이후 구체적으로 클라우드 서비스를 받기 위한 상세 클라우드 서비스 또는 시스템 구성요소를 도출하기 위한 모델이다.

클라우드 서비스 모델 별 질문을 통해 각 질문에 대한 결과가 'Y' 일 때 필요 구성요소를 매칭하는 방법으로 구성하였다.

인프라 서비스인 IaaS는 모든 적용방법에 대해 공통적으로 필요하며 PaaS 와 SaaS는 클라우드 서비스 적용 유형 및 개별적 특성에 따라 서비스 구성 요소를 도출하기로 하였다.

첫째 IaaS는 클라우드 서비스 적용 방법이 Remain이 아닌 모든 서비스 적용 방법이 해당되는 부분으로, 컴퓨터, 스토리지, 네트워크로 분류하고 컴퓨터는 다시 일반적인 CPU 및 메모리를 가상화 기술로 제공하는 General 서비스, 단순 반복적인 병렬 수치 연산 또는 고성능 그래픽 환경을 위한 GPU, 통합 OS 환경에서 독립된 가상화 환경이 필요한 Container 서비스, 사용자가 원하는 환경을 가상화 환경으로 제공시 자동셋업을 할 수 있는 Bare Metal 서비스로 구분하였다. 스토리지는 고

성능 저장공간인 Block Storage, 일반적인 데이터 저장용 Object Storage, 주기적으로 특정 시점에 대한 백업 서비스인 Back Up Storage, 사용자의 행위, 데이터 등을 실시간 보관이 필요한 Archive Storage 로 구분하였다. 네트워크는 가상전용망 생성을 위한 VPN, 기간 시스템의 네트워크 연결을 위한 L2 스위치, 기간시스템에 네트워크 연결시 라우팅을 위한 L3 스위치, 클라우드 시스템을 구성한 여러 개의 가상서버에 대한 부하분산이 필요한 L4 스위치, URL 접근을 위한 DNS, 통신 허용 및 거부 를 위한 방화벽, 외부 네트워크의 공격으로부터 보호를 위한 IPS로 구분하였다.

둘째 PaaS는 클라우드 서비스 적용 방식이 Refactor, Revise, Rebuild에 해당하는 경우로 DBMS 서비스, 미들웨어 서비스, 분석 플랫폼, 서비스, 시스템 연계 서비스로 분류하였다. DBMS 서비스는 일반적인 DB관리를 위한 DBMS, DBMS 백업 서비스, DBMS 서비스의 연속성을 위한 Clustering, DBMS 실시간 복제를 위한 Mirroring으로 분류하였다. 미들웨어 서비스는 가상화 웹 어플리케이션 서버(WAS), 모바일 기반 어플리케이션 개발 플랫폼, 어플리케이션 소스의 형상 변경 관리 서비스로 분류하였다. 분석 플랫폼은 AI 기반(머신러닝/딥러닝) 분석 플랫폼과 데이터베이스 기반 비즈니스 분석/통계 플랫폼인 BI 플랫폼, 비정형 대량 데이터 분석을 위한 Big data 플랫폼으로 분류하였다. 시스템 연계는 API 서비스와 Integration 서비스로 분류하였는데, API 서비스는 시스템 연계 인터페이스를 클라우드 상에서 손쉽게 만들 수 있도록 제공하는 서비스이며, Integration은 클라우드 상에서 다양한 시스템과의 연계를 위해 채널과 인터페이스를 표준화하고 관리하

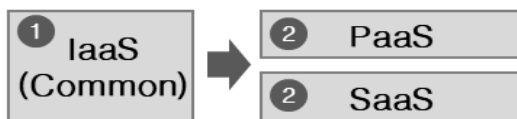


Fig. 5. Order of deriving cloud service components

도록 제공하는 서비스이다.

셋째 SaaS 는 클라우드에서 표준화된 프로그램 제공 서비스로 주로 전사적으로 사용되는 공통프로그램 또는 솔루션이 해당된다. 글로벌, 국내 그룹 또는 전사적 인사관리 시스템으로 표준화된 인사관리를 위한 인사관리시스템(HCM), 고객관리, 고객분석, 마

케팅 제공 등을 위한 전사적으로 표준화된 시스템인 고객관리 시스템(CRM) 마지막으로 자산관리, 회계 관리, 기타 경영관리 등 각각의 업무 영역에 대한 통합 관리 시스템인 자원관리 시스템(ERP) 등이 주요 SaaS 클라우드에서 제공하는 소프트웨어이다.

Table 13. Q&A table for Cloud Detailed Service Release by Cloud Application Method

Cloud application method		Cloud Component Extraction Diagnostics	Result	Cloud Detail Service (Component)	Remarks			
Common	IaaS	Compute Services						
		For common applications Virtualization of Servers and Memory Is it necessary to provide?	Y, N	General				
		Simple, repetitive parallel numeric operations or high performance graphics Computation for the environment Do you need resources?	Y, N	GPU				
		Do you need a virtualized environment that is independent from a converged OS environment?	Y, N	Container				
		Is it possible to automatically set up the environment (OS, runtime, application, etc.) when providing the virtualization environment?	Y, N	Bare Metal				
		Storage Services						
		Accessible from a single server or multiple servers need high-performance storage?	Y, N	Block Storage				
		Do I need a typical performance storage space accessible through the network IP address in the form of a file system?	Y, N	Object Storage				
		Periodically, the backup services for a particular point in time is it necessary?	Y, N	Back Up Storage				
		Is it necessary to store the behavior and data of users in real time?	Y, N	Archiving Storage				
		Network Services						
		Need to encrypt network communications between company and cloud provider?	Y, N	VPN				
		Do you need a switch port that can be networked to an existing system?	Y, N	L2 Swich				
		Do network connections to existing systems require gateways and routing?	Y, N	L3 Swich				
		Do you need load balancing across multiple virtual servers that have configured cloud systems?	Y, N	L4 Swich				
		Do you need a URL to access the services you are offering?	Y, N	DNS				
		Should cloud services allow or deny specific network communications?	Y, N	Firewall				
		Should cloud services be protected from outside network attacks?	Y, N	IPS				
		Refactor Revice Rebuild	PaaS	DBMS Services				
				Is it necessary to store and maintain large amounts of data in a table format ?	Y, N	DataBase		
				Does DataBase require a management system?	Y, N	DBMS		
Need regular backups in case of DataBase loss?	Y, N			DBMS BackUp				
		Do I need a highly available environment for	Y, N	Clustering				

		DBMS service continuity?				
		Do you need a high availability data environment with real-time database replication?	Y, N	Mirroring		
		Middleware services				
		Do you need a web application server that can generally operate and manage applications between clients and servers?	Y, N	Web Application Server		
		Does it require a mobile analytics platform, such as mobile-based application development tools, management screens, and service links?	Y, N	Mobile Develop Platform		
		Is it necessary to distribute and manage the configuration change management of application source code to dev/test servers?	Y, N	Develop		
		Is there a need to answer natural language queries, such as an immediate response to a customer's question, and to implement them?	Y, N	Chatbot Platform		
		Analysis Platform Services				
		Is it necessary to provide standard development tools and algorithms to create machine running and deep learning models?	Y, N	AI Develop Platform		
		Do we need an analytics platform for our database based analytics, statistics, and visualization services?	Y, N	BI Develop Platform		
		Does it require a platform to analyze massive amounts of unstructured data, such as SNS data, other than internal data?	Y, N	Big Data Platform		
		System-linked services				
		Is it necessary to create an API for other system access and to provide interface features?	Y, N	API Service		
		Does the cloud require integration of channels and interfaces, such as MCI/EAI?	Y, N	Interation Service		
		Replace	S a a S	Application Services		
Does the organization need standardized human resource management with national and external enterprise-wide human resources management systems?	Y, N			HCM Solution Service		
Is it necessary to have a enterprise-wide standardized system for customer management, customer analysis, and marketing delivery?	Y, N			CRM Solution Service		
Does it require a unified management system for each business area, such as asset management, accounting management, and other management functions?	Y, N			ERP Solution Service		

VI. 결 론

금융회사는 고객의 금융 자산과 개인 정보를 안전하게 관리하여야 한다. 또한 금융회사는 국가 경제를 떠받치는 역할을 하기 때문에 위험한 상황에 빠지지 않도록 관리되어야 한다. 이러한 이유로 고객 데이터 저장과 관리에 대한 규제, 개인 정보 보호에 대한 규제, 컴퓨터 처리 장치 관리에 대한 규제 등 다양한 규제 요건을 충족시키기 위해서는 금융회사의 클라우드 이용 활성화는 제한이

따를 수밖에 없다.

하지만, 클라우드 시스템은 AI, 빅데이터 분석, IOT, 자율 자동차 등 전 세계적으로 최고의 화두인 4차 산업 혁명의 주요 컨텐츠로 부인할 수 없는 시대 흐름이다. 장기적으로 클라우드 도입을 준비하고 시도하지 않으면 글로벌 경쟁에서 뒤처질 것임은 분명하다.

금융기관이 고객 정보 유출 등 중요 정보 데이터의 관리 문제인 보안 영역 부분에만 치중하고, 감독기관의 컴플라이언스 준수에만 신경 쓴다면 결코 클라우드 시스템

은 도입될 수 없을 것이다.

따라서 본 의사결정 모델은 금융기관들이 현 감독기준의 제약사항을 준수하고, 내부의 명확한 기준을 수립하는데 많은 도움이 될 것이라고 기대한다. 금융회사의 규모와 내부업무 프로세스, 보유 고객정보, 운영 시스템 등이 상이하여 본 모델이 꼭 들어맞지는 않을 수도 있지만 큰 틀에서의 방향성은 일치한다고 판단된다. 또한 금융기관의 상황에 맞게 본 모델의 단위 영역들은 수정해 가면서 사용할 수 있을 것이다.

금융기관들이 본 의사결정 모델을 통해 감독기관의 클라우드 시스템 도입에 필요로 하는 컴플라이언스를 준수하고 최적의 구성 방법을 도출해 내어 훌륭한 시범 사례를 만들고 이를 공유해 나가면, 금융산업에도 클라우드 시스템은 반드시 활성화되어 나갈 것이다.

하지만 금융당국의 정책적인 지원없이 개별 금융회사만의 노력만으로는 금융 산업의 클라우드 도입의 확산은 한계가 있을 것이다. 국내 금융회사의 글로벌 진출을 효과적으로 뒷받침하기 위해서도 국내 금융회사들의 클라우드 활용 역량이 갖추어져야 하겠지만 금융당국도 금융기관이 클라우드 시스템의 확산을 위해 현 규제 사항들이 적절한지 재검토하고 규제를 위한 규제가 아니라, 실효성 있는 규제 방안을 만들어내는 선도 역할이 필요할 시점이다.

References

- [1] Financial Security Institute, "Current status analysis of financial industry Cloud service", E-Finance and Financial Security, Oct. 2015
- [2] Government of the Republic of Korea, "A handbook of Major legislation of Cloud Computing", Nov.2017
- [3] Financial Supervisory Service (FSS), "The Present Status of Financial Cloud Utilization" FSS press release, Jan. 2018
- [4] Financial Security Institute, "Cloud Computing Concepts and Industry Trends" Reserch report of FSI, Sep. 2016
- [5] KB Financial Group (kbf), "The Case and Prospects for the Introduction of Cloud Services in the Financial Sector" Reserch report of kbf, Jul. 2015
- [6] Korea Internet and Security Agency (KISA), "Cloud Service Information Protection Guide", pp. 18-21, Oct. 2011
- [7] Financial Security Institute, "Financial Cloud Service Usage Guide", pp. 18-21, Oct. 2016
- [8] Hye-Ji Do, In-Seok Kim, "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, pp. 11-12, Nov.2017
- [9] Jung Joon Hwa, (National Assembly Research Service), "Status and Challenges of Clauding Computing", pp. 5-6, Dec.2017
- [10] Changbeom Yi, Legal Challenges for Secure Utilization and Activation of Cloud Computing, pp. 11-12, Apr.2010
- [11] Kyoung-a Shin, Sang-jin Lee, "Information Security Management System On Cloud Computing Service", pp. 2-3, Feb.2012
- [12] Bosung Lee, Beomsoo Kim, "Protection of Personal Information on Cloud Service Models", pp. 10-11, Oct.2015
- [13] Woo-Young Yu, Jong-in Lim, "A Study on the Privacy Security Management under the Cloud Computing Service Provider", pp.10, Apr.2012
- [14] Seung Ik Baek, Ji Yeon Shin, Jong Woo Kim, "Exploring the Korean Government Policies for Cloud Computing Service", pp. 2-14, Aug. 2013
- [15] Yoo Ki Jo, "Introduction to Cloud Computing", pp. 1-7, Dec.2011
- [16] Kim Sung-Cheol, "A Study on the Policy Agenda for the Adoption of Cloud Computing", pp. 1-8, May.2015
- [17] Analysts Explore Application Modernization at Gartner Application Architecture, Development & Integration Summit, pp. 16-17, Jun.2011

〈 저 자 소 개 〉



이 회 석 (Hee-seok Lee) 정회원
1995년 2월: 동국대학교 회계학과 졸업
2016년 9월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
<관심분야> 클라우드, 전자금융보안, 금융IT컴플라이언스



김 인 석 (In-seok Kim) 정회원
2008년: 고려대학교 정보경영공학과 박사
2009년~현재: 고려대학교 정보보호대학원 교수 FDS 산업포럼 회장, 한국정보보호학회 운영위원
<관심분야> 전자금융보안, 금융IT컴플라이언스, FIN TEC