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

The Journal of Society for e-Business Studies
Vol.20, No.4, November 2015, pp.103-126
http://dx.doi.org/10.7838/jsebs.2015.20.4.103

한국의 공공기관 클라우드 컴퓨팅 도입 활성화 전략: 미국 연방 공공기관 클라우드 컴퓨팅 도입현황 시사점 및 시스템 개발 수명주기(SDLC) 프로세스 전략을 중심으로

Cloud Computing Strategy Recommendations for Korean Public Organizations: Based on U.S. Federal Institutions' Cloud Computing Adoption Status and SDLC Initiative

강상백(Sang-Baek Chris Kang)*

초 록

그 동안 한국 공공기관에서 클라우드 컴퓨팅 도입은 그다지 활발하지는 않았다. 그 이유 중의 한 가지는 한국은 클라우드 컴퓨팅 도입 이전 이미 세계최고 수준의 전자정부를 구축하였고, 정부에서는 클라우드 컴퓨팅을 주관하는 전담 컨트롤 타워와 이를 추진할 수 있게 하는 법령 제도 등이 없었기 때문이라고 할 수 있다. 그러나 이러한 상황은 2015년 9월 클라우드 법이 시행되어 매우 변화될 것으로 전망된다. 미국의 공공기관 클라우드 도입은 FedRAMP(Federal Risk Assessment and Management Program)에서 주도적으로 추진하고 있는데, 이는 미국의 Cloud First 정책과 연계된다. 미국 연방기관의 클라우드 서비스 도입과 관련하여 미국의회조사국(Congressional Research Service; 이하 CRS)에서는 2015년 1월 연방정부의 클라우드 도입과 관련된 보고서를 출간하였고, 이는 한국의 공공기관 클라우드 도입 정책에 좋은 지침이 될 것으로 판단된다. 본고에서는 (1) 한국의 클라우드 법의 중요한 사안을 분석하고 (2) 최근 미국 연방정부의 클라우드 서비스 도입 현황을 분석하며, (3) 시스템 개발 수명주기(SDLC) 기반의 도입 활성화 전략 프레임워크에 대하여 제안하였다.

ABSTRACT

Compared to other countries, cloud computing in Korea is not popular especially in the government sector. One of the reasons for the current not-fully-blossomed situation is partly by early investment in huge government datacenters under Korea's e-government initiative; let alone, there was no strong control tower as well as no enforcing law and ordinances for driving such cloud computing initiative. However, in 2015 March 'Cloud Computing and Privacy Security Act' (hereinafter, Cloud Act) had been passed in the Parliament and from September 2015 Cloud Act was deployed in Korea. In U.S., FedRAMP (Federal Risk Assessment and Management Program) along with Obama Adminstration's 'Cloud First'

* Korea Local Information Research & Development Institute(KLID)(chriskang@klid.or.kr)
Received: 2015-09-08, Review completed: 2015-11-03, Accepted: 2015-11-19

strategy for U.S. federal institutions is the key momentum for federal cloud computing adoption. In 2015 January, U.S. Congressional Research Service (CRS) has published an extensive monitoring report for cloud computing in U.S. federal institutions. The CRS report which monitored U.S. government cloud computing implementation is indeed a good guideline for Korean government cloud computing services. For this reason, the purpose of the study is to (1) identify important aspects of the enacted Korean Cloud Act, (2) describe recent U.S. federal government cloud computing status, (3) suggest strategy and key strategy factors for facilitating cloud adoption in public organizations reflecting SDLC strategy, wherein.

키워드 : 클라우드 컴퓨팅, 미국 연방정부 클라우드 컴퓨팅 도입, 클라우드 컴퓨팅 전략 및 핵심 요인들
Cloud Computing, US Federal Cloud Computing Adoption, Cloud Computing Strategy and Key Factors

1. 서 론

클라우드 컴퓨팅은 IT 자원(인프라, 플랫폼, 서비스 등)을 인터넷 기반으로 제공하는 서비스로 급속한 네트워크의 발달 및 안정화로 전 세계적으로 다양하게 추진되고 있다. 특히 민간부분에서는 애플과 구글 등 주요 IT업체에서 웹 기반의 개인파일 저장 및 공유가 실시간으로 가능한 B2C 클라우드 컴퓨팅 서비스를 제공하고 있으며, 민간 B2B 시장에서도 게임 업체 및 다국적 기업의 탄력적인 네트워크 수요 환경에 대응하는 최적의 솔루션으로 클라우드 컴퓨팅은 빠르게 부상하고 있다.

국내에서도 클라우드 컴퓨팅에 대한 관심은 학계/산업계에서 지속적으로 있어 왔다. 주로 이동통신사 및 ICT 서비스 업체들을 중심으로 클라우드 컴퓨팅이 추진되고 있으나, 국내 공공기관의 클라우드 컴퓨팅 활용도는 이해 비해 상대적으로 낮은 수준이다[36]. 한국의 경우 세계적인 수준의 전자정부가 가입자망의 광대역화는 물론 대규모 정부 데이터센터 구축 등을 통해 매우 일찍 시작 되었고, 그 결과 UN 전자정부 연속 3회 1위를 달성할 수 있었다. 이러한 전자정부의 성공적인 구축 및 운영과는 달리 그 동안 정부의 클라우드 도입은 다른 국가의 비하여 다소 전개가 늦었다고 할 수 있다[36].

그러나 이러한 공공기관의 클라우드 서비스 도입 지연은 급격한 환경 변화를 맞이하게 되었다. 2015년 3월 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률 제정안'(이하 클라우드법) 이 국회를 통과하여 비로소 2015년 9월 28일에 시행되었기 때문이다. 다만, 동 클라우드법에 의한 공공기관 클라우드 서비스는 의무사항이 아니라 권장사항이기는 하나, 공공기관이 클라우드 서비스 이용을 하지 않으려면 반드시 불가 사유를 스스로 입증해야 하는 절차가 있기 때문에 사실상 도입을 강제하는 효과가 있다고 볼 수 있다. 정보통신산업진흥원(NIPA)에 따르면 9월 법 시행 이후 공공기관의 클라우드 서비스 확대로 2017년에는 1조 6000억 원의 신규 클라우드 관련 시장이 열릴 것으로 예측하고 있으며[12], 클라우드 법은 국내 전자정부 구축 시 활용 되었던 시스템통합(SI) 중심의 전산자원 개발 관행을 바꿀 것으

로 전망되고 있다. 그 이유는 공공기관은 클라우드 컴퓨팅을 통하여 서비스 활용 범주에 맞는 범용성 높은 인프라, 플랫폼, 애플리케이션을 빌려 쓰고, 이를 이용료 기반으로 처리할 수 있어 그간 전산자원 개발의 다단계 하도급 관행에 따른 품질 저하 및 발주 이슈가 상당 부분 개선될 수 있기 때문이다.

한국의 경우 선진국에 비해 특히 공공기관의 클라우드 서비스 도입 및 관련 기술개발이 지연되어 공공 클라우드 컴퓨팅 도입이 빨랐던 국가들에 비하여 기술 및 운용 측면에서의 격차가 존재하고 있다. 따라서 해외 유명 IT업체에 의한 국내시장 잠식 및 핵심기술의 의존도가 높아질 것으로 판단되고 있는데, 특히 아마존(EC2), 구글(GCE), 마이크로소프트(Azure) 등 글로벌 IT 솔루션 기업들에 대한 의존도가 높아질 것으로 예상된다[39].

한편, 미국은 오바마 대통령의 주요 아젠다로 클라우드 컴퓨팅을 연방 정부의 IT 예산을 절감하기 위한 주요 방안으로 2009년부터 추진하고 있다. FCCI(Federal Cloud Computing Initiative)에 따라 FedRAMP(Federal Risk Authorization and Management Program)에 근거하여 주로 행정관리, 조달 등 기밀성이 높지 않고 투입대비 비용절감 효과가 큰 분야 위주로 클라우드 컴퓨팅을 적용하여 유지비용을 절감하고 있다[28].

그 동안 한국은 클라우드 서비스 인증제를 마련하고 범정부 차원의 인프라 중복투자 방지와 서비스 연계를 위하여 클라우드 서비스 추진계획과 로드맵 등을 마련하여 왔으나, 최근까지 정부차원의 법령 제정 및 범부처 추진조직 등의 설립은 더딘 편이었다. 그러나 2015년에는 동 클라우드 법 시행 관련 시장과 생태계에 많은 변화가 있을 것으로 예상되는데, 이를 위한 정부차원의 공공기관 클라우드 도입 확산 정책 및 산업 활성화 방안이 필요한 시점이라고 사료된다.

특히, 한국의 경우는 공공기관 클라우드 서비스 도입이 다소 늦었으므로 이번 법 시행을 계기로 공공기관의 클라우드 서비스 사용 확대는 물론, 국내 클라우드 컴퓨팅 업체의 경쟁력 제고, 생태계 조성, 비용 절감 및 이용자 정보보호 수준 제고 등의 당면 목표를 함께 추진해야 할 것으로 생각된다.

본고에서는 이러한 공공기관의 클라우드 서비스 생태계 전환에 따른 전략의 수립에 대하여 미국의 연방 클라우드 컴퓨팅 도입 현황을 분석하고, 시스템 개발수명주기(SDLC) 기반 공공기관의 클라우드 컴퓨팅 관련 프로세스를 도입하는 방향의 전략 프레임워크를 제시하였다.

2. 클라우드 기술 및 시장 현황

2.1 클라우드 시장 및 기술 동향

2.1.1 세계 클라우드 시장

글로벌 클라우드 시장은 2014년 693.1억 달러로 분석되고 있다[12]. 특히 이중 아마존AWS(Amazon Web Service)은 시장 점유율 28.5%로 1위이며, 마이크로소프트, IBM, 세일즈포스, 구글 등이 추격을 하고 있는 상황이다. 특히 아마존 AWS는 최근 미국의 CIA 전산구축 프로젝트에서 IBM을 누르고 약 7,000억 원 규모의 사업을 수주하여 IT 패러다임 전환의 충격을 주고 있으며, 향후 클라우드 시장의 판도

에 대하여 많은 시사점을 남기고 있다. 또 다른 조사기관인 TBR에 따르면, 2015년 전 세계 프라이빗 클라우드 시장은 35%, 퍼블릭 클라우드 시장은 25%, 하이브리드 클라우드 시장은 50% 이상 성장할 전망할 것으로 예측할 만큼 클라우드 관련 시장은 성장의 잠재력이 큰 시장으로 예측된다.

한편 아마존이 선점한 IaaS(Infrastructure-as-a-Service) 시장에 구글이 '구글컴퓨트엔진(GCE)' 서비스를 시작하면서 업계 간 경쟁이 더욱 치열해 질 것으로 보이며, 마이크로소프트는 약 8%의 점유율을 보이고 있지만, 전년대비 154%의 가장 높은 성장률을 기록하였는데 이는 마이크로소프트의 Azure 솔루션이 아마존AWS 대비 가격 경쟁력이 있기 때문이다.

현재 클라우드 시장은 보안, 안정성 등에 대한 소비자의 신뢰도 향상으로 성장동력은 확보하였으나, 아직도 클라우드 서비스의 보안은 중요한 화두로 남아 있다. 왜냐하면 인터넷 광대역망 수준이 지역별로 큰 편차를 보이거나, 커넥티드 서비스가 단절이 되는 경우의 클라우드는 In-house 서비스 보다 약점이 있어 이로 인한 위험 또한 더욱 커질 수 있기 때문이다. 예를 들어, 12월 24일 아마존AWS 장애로 인한 Netflix사의 사건은 일래스틱로드밸런싱(ELB) 서비스 문제로 인하여 아마존의 미국 동부 버지니아 데이터센터에서 제공하는 ELB 서비스가 제대로 작동하지 못하면서 발생하였는데, 이로 인하여 Netflix를 비롯한 인터넷서비스가 20시간 이상 제공되지 않았다. 이러한 사례에서 볼 수 있듯이 클라우드 서비스는 접속성, 보안은 물론, 사람의 실수/오류로 인한 발생하는 문제점으로부터 함께 발생될 소지가 있다. 이러한 이슈들은 클라우드 서비스와 시스템이 고도화되면서 문제가 해소되겠지만, 다른 한편으로 클라우드의 시장이 지속적으로 풀어가야 할 숙제라고 할 수 있을 것이다.

2.1.2 클라우드 기술 동향

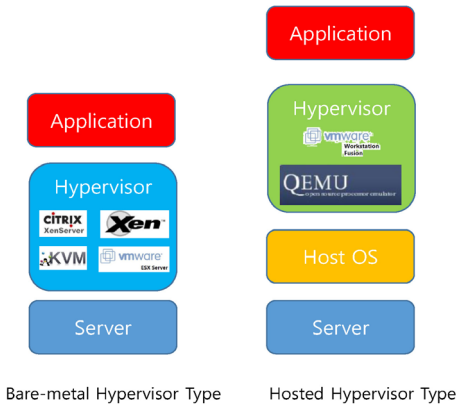
미국국립표준기술원(NIST)은 클라우드의 종류, 특성을 '서비스 모델(Delivery Model)'과 '배치 모델(Deployment Model)'로 구분하였고, 이러한 구분은 클라우드 컴퓨팅의 대표적인 분류 기준으로 적용되고 있다. 사실 두 가지 기준 모두 상호독립적인 개념은 아니며 어느 기준/축으로 클라우드 컴퓨팅을 구분하느냐에 따른 차이라고 볼 수 있다. 클라우드 컴퓨팅의 서비스 모델과 배치 모델 관련하여 그 동안의 연구에서 많은 논의가 있어 왔으므로, 본고에서는 클라우드 컴퓨팅의 핵심적 요소인 하이퍼바이저 및 이에 관련된 보안 권고사항, 그리고 오픈소스 클라우드 플랫폼인 오픈스택(Open-Stack) 기술의 발전 방향을 중심으로 클라우드 서비스 기술 동향을 정리하였다.

2.1.2.1 하이퍼바이저(Hypervisor) 및 보안

가상화(Virtualization)는 단일의 물리적 IT 자원이 동시에 다수의 가상화된 IT 자원으로 사용될 수 있게 기술을 의미하는데, 기존 클라이언트-서버 환경 하에서는 단일의 하드웨어에서 단일의 운영체계가 해당하는 하드웨어를 구동시키나, 가상화는 동시에 복수개의 가상화된 논리적 서버를 동시에 구동할 수 있고, 또 각각의 가상머신에서는 유닉스, 리눅스, 윈도우즈 등 서로 다른 종류의 운영체계(OS)가 상호 독립적으로 운영될 수 있다.

클라우드 컴퓨팅에서 가장 중요한 기술 요소 중 하나인 가상화는 하이퍼바이저(Hypervisor)

에 의하여 구현이 되며, 하이퍼바이저는 호스트 컴퓨터에서 가상머신과 하드웨어 사이에 위치하여 다수의 운영체계(OS)를 동시에 실행하기 위한 논리적 플랫폼(Platform)을 의미한다. 하이퍼바이저는 가상화 머신 모니터(Virtual Machine Monitor, VMM)이라고도 불리우며, 게스트 운영체계의 실행 관련, CPU, 메모리 등을 포함하는 하드웨어 자원을 각 가상머신에 논리적 할당하며, 자원 스케줄링을 담당한다. 하이퍼바이저는 크게 Native(Bare-Metal) Type과 Hosted Type으로 나뉘며, 하이퍼바이저가 물리적 하드웨어상에서 제어/동작하는 지의 여부에 따라 나뉠 수 있다. 클라우드 컴퓨팅에서 하이퍼바이저는 Citrix사의 Xen, 리눅스의 KVM, 마이크로소프트의 Hyper-V, VMware의 vSphere/ESXi-process 등이 시장에서 주로 이용되고 있다.



〈Figure 1〉 Types of Hypervisor: Bare-Metal and Hosted Type

NIST Special Publication 800-125-A "Security Recommendations for Hypervisor Deployment" 2014년 보고서에 따르면 하이퍼바이저는 5개의 기능에 충실해야 한다고 정의하고 있는데, 이는 (1) 가상머신의 독립화 (2) 접근 제어 및 장비 에뮬레이션, (3) 게스트 가상머신에 대한 우선적 명령 실행, (4) 가상 머신 관리, (5) 하이퍼바이저와 연동을 위한 파라미터 값 조정 등이며, 동 보고서는 22가지 하이퍼바이저 구축 시 보안 권고사항을 포함하고 있다. 22가지의 권고 사항 중 중요한 것은 Bare-Metal 하이퍼바이저 Type은 Host 운영체계가 따로 없으므로 외부 공격을 줄일 수 있으며, 하드웨어가 제어되는 가상화 하이퍼바이저 플랫폼이 단순 소프트웨어 기반 가상화 플랫폼 보다 안정적임을 강조하였다. 또한 하이퍼바이저는 반드시 Boot 설정 선택기능을 두어 인증받지 못한 드라이버의 이용자가 접근할 수 없도록 하는 장치가 마련되어야 한다고 권고하였다. 또한 가상머신 사용 메모리 총량은 물리적 메모리 총량 대비 높지 않아야 하며, 비율은 1.5:1을 권장하고 있다. 하이퍼바이저는 메모리 관리 옵션이 있어야 하며, 최대 사이즈 조정 기능 및 가상머신 자원 이용 충돌시 우선순위를 지정할 수 있어야 하고, 가상머신에 할당된 가상 CPU의 수는 하이퍼바이저 호스트의 CPU 코어수보다 작아야 한다고 제안하였다. 특히 가상머신 이미지 라이브러리는 반드시 하이퍼바이저 호스트 외부에 위치하여야 하며, 접근제어와 디지털 서명 등이 지원되어야 한다고 권장하고 있다. 보안 정책 메커니즘은 가상머신 바깥에 위치하여야 하며 이는 통상적으로 신뢰성 있는 보안가상장치(Security Virtual Appliance)의 형태로 존재하여야 함을 아울러 권장하였다.

또한 하이퍼바이저 내 설치된 빌트인(Built-in) 방화벽은 가상머신 관리와 호스트의 포트와 프로토콜을 제어하는데 만 이용되어야 할 것으로 권고하였다. 가상 머신 및 하이퍼바이저의 호스

〈Table 1〉 Security Recommendations for Adopting Hypervisor Platforms (Special Publication 800-125-A, 2014, NIST, pp.16-31, summarized and reprinted)

Item	Recommendations
1	A Type 1 (Bare-metal) hypervisor provides more security assurance than a Type 2 (Hosted) hypervisor, due to the reduced attack surface and the consequent reduced list of vulnerabilities to be addressed.
2	A Hypervisor platform with hardware assisted virtualization (both instruction set and memory management) provides greater security assurance than one with purely software assisted Virtualization
3	The hypervisor that is launched should be part of a platform and an overall infrastructure that contains: (a) Hardware that supports an MLE and standards-based TPM and (b) Attestation process that should contain capabilities to take advantage of these so as to provide a chain of trust starting from the Hardware to all Hypervisor components.
4	A functional Hypervisor management console with smaller code and disk footprint and smaller number of exposed interfaces can provide better security assurance as it facilitates easier verification and also because of the fact that it presents a smaller attack surface.
5	The hypervisor should have a boot configuration choice to disallow the user of non-certified drivers. Further, if architecture permits, the running of QEMU process for each application VM should be confined to an unprivileged VM so as to limit the impact of a faulty device driver code to the operation of the corresponding application VM.
6	The ratio of the combined configured memory of all VMs to the RAM memory of the virtualized host should not be very high. A typical ratio adopted is 1.5 : 1. In other words if a virtualized host has 64GB of RAM, then the combined configured memory of all VMs running on it should not exceed 96 GB.
7	The hypervisor should have configuration options available to specify a guaranteed physical RAM for every VM (that requires it) along with a limit to this valu, and to specify a priority value for obtaining the required RAM resource in situations of contention among multiple VMs.
8	The number of virtual CPUs allocated to any VM deployed should be strictly less than the total number of cores in the hypervisor host.
9	The hypervisor should provide features to specify a lower and upper bound for CPU clock cycles needed for every deployed VM as well as a feature to specify a priority score for each VM, to facilitate scheduling in situations of contention for CPU resources from multiple VMs.
10	The VM image library should reside outside of the hypervisor host, should have strict access control and each of the images checked out from the library should have a digital signature attached to it as a mark of authenticity and integrity.
11	There should be a mechanism for security monitoring and security policy enforcement of VM operations - malicious processes running inside VMs and malicious traffic going in and out of VM. This monitoring and enforcement mechanism forms the foundation for building Anti-Virus (AV) and Intrusion Detection & Prevention (IDPS) solutions.
12	Solutions for Security Monitoring and security policy enforcement of VMs should be based “outside of VMs” and should leverage the virtual machine introspection capabilities of the hypervisor. Generally such solutions involve running a security tool as Security Virtual Appliance (SVA) in a security hardened (trusted) VM.
13	The access control solution for VM administration should have the granular capability both at the permission assignment level as well as at the object level. Another desired capability for the access control solution is the ability to specify deny permission to some specific objects within a VM group.

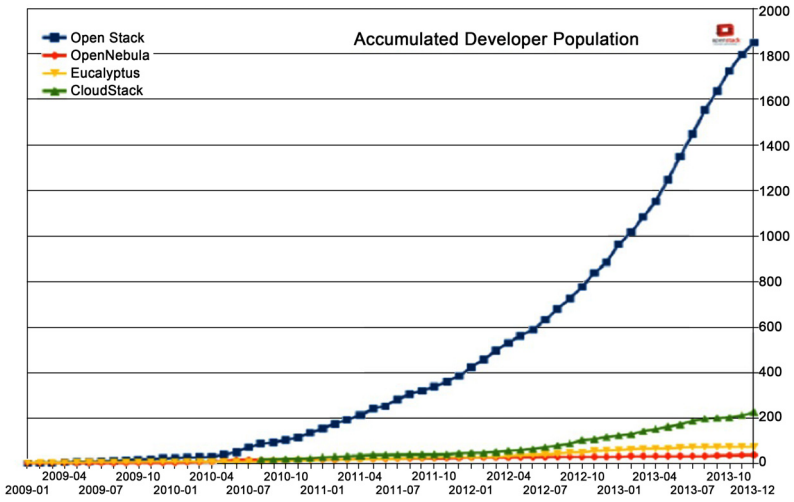
Item	Recommendations
14	The number of user accounts (including privileged accounts) requiring direct access to hypervisor host should be limited to bare minimum (i.e., two or three).
15	The user accounts (including privileged accounts) on the hypervisor host must be integrated with the enterprise directory infrastructure in order to enable authentication through robust authentication protocols (e.g., Kerberos), enable enforcement of some corporate security policies (e.g., password policies) as well as handle changes to user account list (addition and deletion of user accounts).
16	The remote access protocol used to access the hypervisor service console should have configuration options available to: completely deny access (i.e., disable remote access via specific protocols), deny hypervisor root account access and restrict access only to a specified list of administrative accounts.
17	Use Hypervisor features that enable: (a) definition of a complete set of configuration settings (Gold Configuration) for a hypervisor deployment (b) automate application of those configuration settings to a new or existing hypervisor installation and (c) check compliance of existing hypervisor installation against those configuration settings, if available, in order to minimize manual configuration errors that may increase the security risk.
18	A good hypervisor patch management practice should be in place to keep the hypervisor current with all relevant patches.
19	The built-in firewall for the hypervisor should only be configured to allow ports and protocols (network traffic) needed for enabled services in the hypervisor, such as management and specialized security agents and third-party applications.
20	It would be preferable to have a hypervisor logging feature that generates logs in a standardized format to help leverage the use of tools with good analytical capabilities as well as the feature to transmit log records in real time over a secure channel to an external server for fault tolerance..
21	Protection for VM Management and Hypervisor Host & Software administration functions can be ensured by placing the management interface of the hypervisor in a dedicated virtual network segment and enforcing traffic controls using a firewall.
22	Communication from a given VM to the enterprise (physical) network should be enabled by establishing multiple communication paths within the virtualized host. This is usually accomplished by providing multiple physical network adapters (pNICs) for traffic from a particular VM to reach the enterprise network.

* Acronyms: VM (Virtual Machine), MLE(Measured Launch Environment), TPM(Trusted Platform Module).

트와 소프트웨어 관리기능 등은 가상 네트워크 세그먼트(vNIC, vLAN 활용)에 위치시켜야 하며, 방화벽 등으로 트래픽 관리가 가능하여야 한다고 주장하였다. NIST에서 권고된 하이퍼바이저 보안사항은 <Table 1>과 같다. 이와 같은 NIST의 하이퍼바이저 구축시 권장사항은 클라우드 서비스 도입을 고려하는 기관의 정보관리책임자 및 관련자에게 클라우드 컴퓨팅 구축 시 기술적 보안문제 해결에 하나의 가이드가 될 것으로 판단된다.

2.1.2.2 오픈스택(Open-Stack)

오픈소스 클라우드 구축기술인 오픈스택에 대하여 다양한 시장 및 전문가 의견이 공존하고 있다. 최근 SK 텔레콤에서는 오픈스택에 대하여 적극적인 투자를 하겠다고 천명하였고, 클라우드 구축 솔루션업체 및 하드웨어 벤더들의 경우도 오픈스택의 활용을 긍정적으로 보고 있다. 다만, 기술의 성숙도 측면에서 스토리지와 네트워크 관리 기술의 개발은 다소 완성도



〈Figure 2〉 Number of Developers for Cloud Platforms([3], p. 21)

가 높지 않다고 평가하고 있다. Zdnet(2015)은 오픈스택에 참여 중인 한 네트워크 장비 솔루션 공급업체 관계자와의 인터뷰에서 “오픈스택에서 컴퓨팅 모듈인 노바는 이미 개발이 몇 년째 개발이 적용된 상태로써 프라이빗 클라우드 환경에선 잘 작동하는 편이지만, 네트워크 플러그인인 ‘뉴트론’은 아직 갈 길이 멀다는 평가가 대부분”이라고 언급하였다[39].

모바일 환경에서도 개발 및 테스트 관련 오픈스택이 활용되고 있는데, 다음카카오에서는 오픈스택을 활용하고 있다고 한다. 모바일 인터넷 서비스 개발 특성상 개발 사이클이 짧고 빠르기 때문에 오픈스택을 통한 서버 증설 및 개발, 그리고 가상머신의 폐쇄가 수월한 오픈스택을 활용하기 때문이다. CIO매거진(2015)에 따르면 시스코와 IBM은 오픈스택 업체를 인수하였고, 이러한 인수는 향후 전산 운영/개발 환경이 자체 구축방식에서 클라우드로 이전되는 패러다임의 변화라고 할 수 있다[6]. 이러한 환경에서 오픈스택은 차별화될 수 있는 요소로 판단되며 향후 오픈스택의 이용은 더욱 많아지고 모듈 등의 완성도도 더불어 향상될 것으로 기대된다.

다양한 오픈소스 클라우드 플랫폼 중에서도 오픈스택의 플랫폼 관련 개발자 수가 다른 플랫폼에 비하여 월등하게 커지고 있는 것을 볼 수 있으며 <Figure 2>, 이는 공공기관을 포함하여 향후 클라우드 서비스 제공시 완성도가 높은 다양한 애플리케이션 등이 오픈소스 기반으로 제공이 될 수 있는 클라우드 서비스 환경이 보다 더 가까워지고 있다고 볼 수 있다.

3. 국내 클라우드 법 및 관련 문헌 연구

3.1 국내 클라우드 법 분석

2015년 3월 ‘클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률 제정안’(이하 클라우드 법)

〈Table 2〉 The Contents from Law and Ordinances of 2015 Korean Cloud Act

Item	Contents
Priority	• The Cloud Act has a priority to other IT related Acts. • Aligned with existing individual information security law and other ICT related laws.
Plan	• The 3 year plan is supported and supervised by Minister of the Ministry of Future Planning, Science, and ICT. • The 7th clause of a special law on Information and Telecommunication and Convergence Facilitation stipulates organizing a committee for reviewing and confirming the plan. • Related ministers of the cabinet can be participated in the committee to set up and proceed the plan.
Budget support	• Related central ministries will be funding R&D and starting pilot projects for cloud computing implementation.
SME participation	• Government will support SME's with cloud computing expertise. • The head of central government will be making a guideline to augment participation of SME's.
Project	• Public organizations should try to adopt cloud computing and when making a budget planning, they should consider adopting cloud computing as a priority. • Public organizations should make best efforts to use cloud computing service.
Providing information of cloud computing needs	• The heads of government agencies are required to report cloud computing needs information and their plans more than once a year to the ministry of Science and ICT Future planning (MSIP). • The Minister of MSIP will be sharing the information to cloud computing service providers more than once a year.
Industrial complexes for cloud computing	• Government and local municipalities will be providing industrial complexes to facilitate cloud computing usage. • The Minister of MSIP has a privilege to request to the Minister of Land and Transportation for appointing industrial complexes.
Inclusion in cloud computing service	• If other law and ordinances define/circumscribe the permission and approval of IT resources, cloud computing service elements can be included in those IT resources as well.
Quality level	• The Minister of MSIP will announce the relevant service level agreement of cloud computing as well as information security protection. • Request for meeting of setting up a service level to cloud service providers
Standard contract form	• The Minister of MSIP will constitute and update the standardized contract form of cloud computing service for information security after discussing with the head of fair trade commission. • Request for using the standardized contract forms to cloud service providers
Facing issues and incidents	• Cloud service providers should report to user organizations if there are incidents of intrusion, leaking of user information, service suspension; and if it is the case of user information leaking, cloud service providers should report to the Minister of MSIP. • The Minister of MSIP should execute an immediate action to protect users as well as recovery actions for incidents.
User information security	• Cloud service user organizations can request the user information that are classified as a government information. • If the Minister of MSIP considers opening an information can increase user information security, he/she can request opening of the user information.
Penalties of user information mal-usage	• Cloud service providers will be fined 5 years of prison confinement or imposed of 50,000 USD penalties, if they provide user information without permission and approval. • Cloud service providers should return all the information when the contract is over. If it is not returnable, the service provider should destruct the information, unless otherwise 10,000 USD penalties will be imposed.
Damage compensation	• Cloud service providers will be in damage compensation if they cannot provide the proofs of waiver to any damages

이 국회를 통과하여 2015년 9월 시행되었다. 이번 법은 클라우드 컴퓨팅 발전을 촉진하기 위한 각종 시책의 추진 근거를 마련하여 선진 클라우드 컴퓨팅 도입 국가에 대비하여 다소 늦어진 클라우드 컴퓨팅 산업의 도입을 촉진하고, 연관 산업 생태계 조성, 이용자 보호방안을 마련해 이용자가 클라우드 컴퓨팅을 이용할 수 있는 환경을 마련하기 위한 법이라고 할 수 있다. 다만 일부 법학자들의 경우, 이번 규정이 클라우드 컴퓨팅에 대한 깊은 기술적 고려가 없고 기획입법의 성격이며, 동 법안의 정의규정과 클라우드 서비스 규정 흠결로 인하여 여러 가지 문제가 발생할 수 있는 소지가 있다는 견해를 나타냈다[29]. 클라우드 법은 법제도 관점에서 지속적으로 개선될 것으로 여겨지며, 본고에서는 클라우드 법 자체의 항목과 관련된 법/제도 측면의 검토는 연구 범위에 부합하지 않아서 생략하였다.

3.2 국내 공공기관 클라우드 도입 관련 선행 연구

국내 공공기관의 클라우드 도입과 관련하여 2015년 현재 국내 기관의 보고서 및 학술 연구 등이 다수 진행 되었다. 다만 국내 공공 클라우드 도입 관련 외국의 사례를 벤치마킹하여 개별적인 기관의 추진 전략의 방향에서 작성된 연구는 거의 없었으며, 특히 가설-검증을 통한 인과분석을 진행한 확증적 연구는 전무하였다. 이러한 상황은 국내 공공클라우드 서비스가 점차적으로 도입되고 있는 구축환경과 무관하지 않다고 판단되며, 따라서 본고에서는 가설-검증의 확증적 논문이 아닌 국내 공공 클라우드 관련 논문 및 관련 선행 연구 등을 폭 넓게 조사/분석하였다.

지방정부의 클라우드 시스템에 대하여 지방자치단체 정보화 담당자 210명을 대상으로 조사한 연구에서는 중앙집중형, 지역분산형, 이원화, 현 체제 유지보수 네 가지 선택 중 통계적으로 유의미한 차이는 보이지 않았으나 지역분산형이 가장 높은 선호 추진모델로 조사되었다. 클라우드 도입은 지방전자정부 구현에 성공적일 것이라고 하는 응답이 유의미하게 조사되었으며, 선택 서비스는 데스크탑 가상화가 가장 높게 나타났다고 분석되었다[16]. 지역정보화를 위한 예산/재정에 관한 연구에서는 중앙정부에 의존하는 경직성 지역정보화 예산 재원을 보완하거나 대신할 수 있는 지방정부의 자주적 재원 중심의 지역정보화를 추진할 수 있는 방안 제시 중 민간자본을 유치할 수 있는 대안에 대하여 제시하였다[21]. 클라우드 서비스 인증제도 수립을 위한 프레임 워크 관련 연구에서는 클라우드 서비스 인증제도의 세부 평가항목을 클라우드 서비스, 클라우드 서비스 사업자 카테고리로 나누었고, 이를 구조 및 적합성, 가용성, 성능 및 확장성, 보안 및 신뢰성, 고객지원, IaaS 서비스, SaaS 서비스로 나누어 분석하였다. 클라우드 서비스 사업자 항목으로는 일반현황, 네트워크 및 데이터센터, 서비스 제공기반 및 보안, 서비스 지속성, 고객 지원으로 분류하고 평가항목 등에 대한 보완사항 등에 대하여 제시하였다[31, 33, 38]. 또한 도입의 큐브모델을 제시하여 클라우드 컴퓨팅 타입, 클라우드 컴퓨팅 채널, 클라우드 도입 방법 등의 세 가지 축에서 분석하는 방안을 제시하기도 하였다.

미 연방정부 클라우드 서비스 보안인증제도(FedRAMP) 관련 연구에서는 FedRAMP(Federal

Risk and Authorization Management Program)에 대하여 주로 소개하였고, 이를 기반으로 한국의 ISMS(Information Security Management System) 인증과 비교하였으며, 한국도 FedRAMP와 같은 이중인증, 평가대행기관 등을 이용하여 비용과 시간을 절약하는 인증절차의 필요성을 강조하였다. 또한 국내의 클라우드 서비스 인증 제도는 혜택이 상대적으로 미흡하며, 인증획득 시 얻을 수 있는 다양한 정부차원의 혜택을 고려하는 것이 필요함을 제안하였다[33].

국내 클라우드 정책분석 및 발전방향에 관한 연구에서는 외국 학자들의 3가지 정책 프레임워크에서의 향후 클라우드 정책 수립 시 고려사항들을 제안하였으나 연구가 진행된 시기상 최근 2015년 정부의 '정부 3.0 클라우드 추진정책'의 평가지표 등과는 다소 차이가 존재한다[1]. 국내 공공 클라우드 서비스 적용 우선순위 도출에 관한연구에서는 해외 공공부문 클라우드 사례의 SRM(Service Reference Model) 매핑을 통해 대국민서비스와 정부내지원서비스, 공통기술서비스 하위 서비스별로 많이 적용된 사례 빈도수를 활용하여 우선순위를 도출하였는데, (1) 대국민 서비스 순위: ① 지식활동, ② 공공안전, ③ 사회복지, ④ 국민건강 등이며, (2) 정부 내 지원 서비스: ① 정보화, ② 대민관계, ③ 업무관리, ④ 재정 등이고, (3) 공공 클라우드 서비스 우선순위 도출을 가중치를 통해서 제시하였다[38]. 다만 동 연구는 클라우드 시스템의 실제 구축에 있어서 미국의 사례에서처럼 클라우드 서비스가 서비스 유형별 도입이 아니라, 도입 기관별로 해당 업무에 맞추어 시작이 되었음을 언급하지 않았던 점이 미국의 접근법과는 다소 다른 접근으로 분석된다.

클라우드 도입 방안 이외에도 국가차원에서의 발전전략과 정책과제들을 도출한 연구도 있었는데, 이 연구에서는 2015년 글로벌 클라우드 강국 도약의 국가비전 달성을 위하여 데이터 센터 및 모바일 클라우드 전략분야를 육성하고, 국가정보화 관련 경직성을 정비 3,000억 원을 절감, 2015년까지 클라우드 서비스 15% 도입률 달성 목표하는 것을 제안하였다. 또한 정책과제로 클라우드 친화적 법제도 환경조성, 공공 부문 IT 인프라의 클라우드화, 클라우드 산업의 국제경쟁력 강화, 클라우드 데이터센터의 육성, 클라우드 시장 기반 조성의 6개 과제를 제시하여 국가차원에서 국제경쟁력을 가질 수 있는 정책적 대안을 제시하였다[4].

클라우드의 활용을 교육에 적용한 연구도 있었는데, 동 연구에서는 클라우드 컴퓨팅 환경기반 스마트 교육 프레임워크를 제안하였고, 시범 운용 시에는 Public 클라우드, 시범운용 후에는 교과부 전용 클라우드센터를 구축해야한다고 주장하였다. 또한 법률적으로 ① 국내외 데이터 저장 위치에 따른 적용 법률, ② 사용자가 데이터 복구・폐기가 자유로워야 하는 이슈, ③ 시스템 보안 및 서비스 제공자의 보안 인식문제, ④ 저작권 침해 등에 대한 지적재산권 보호 이슈, ⑤ 시스템 장애발생, 개인정보 유출, 해킹 이슈 ⑥ 사고발생시 손실보상에 관한 이슈 등에 대한 대비가 필요하다고 언급하였다[11].

사실 국내 공공정보화의 경우 다른 나라에 비하여 상당히 진전이 빠른 편이며, 클라우드 서비스 도입시 신규시스템 도입의 경우와 기존 시스템의 전환으로 나누어 고려함이 필요하다[38]. 특히, 신규 시스템을 도입하는 경우는 새로운 업무 프로세스 파악과, 파악된 업무

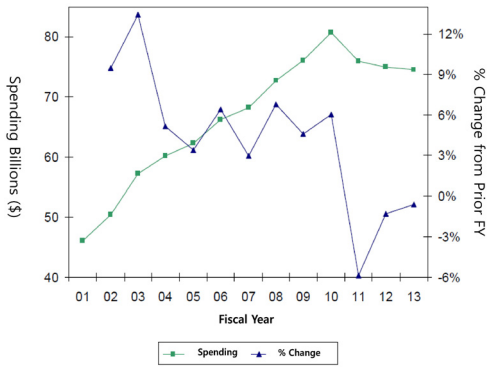
를 구현하는데 있어서 비용의 효율 및 기술의 적합도가 중요하며 이로 인하여 시스템 개발 수명주기(SDLC)의 분석/설계/구축 프로세스가 중요하다고 할 수 있다.

레가시 시스템의 클라우드 전환의 경우는 기존 업무 프로세스가 잘 구현되어 있으나 데이터 이동에 부담이 증가한다고 할 수 있어 전환과정에서 발생할 수 있는 데이터의 변형 등에 대한 고려가 중요하다고 보고되었다[34, 38]. 이러한 점으로 미루어 보아 향후 공공 클라우드 서비스 도입에 있어서는 데이터의 구조화, 개별 데이터의 중요성 및 특성에 대한 체계적 관리가 선결 되어야 공공기관의 클라우드 컴퓨팅 도입이 경제성, 보안성, 효율성 등을 만족시킬 수 있을 것으로 판단된다.

4. 미국의 연방 클라우드 서비스 현황

4.1 CRS 보고서 내용 요약

2015년 1월 발간된 미국 의회조사국의 "Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management"는 미국 연방정부의 FCCI (Federal Cloud Computing Initiative) 정책 관련 발생할 수 있는 문제점과 방향성 등에 대한 폭넓은 전문가의 의견이 포함된 의회의 조사 보고서이다. 미 오바마 대통령에 의하여 강력하게 추진되고 있는 연방 클라우드 서비스에 대하여 다소 중립적인 시각에서 미국의 연방 클라우드 컴퓨팅 서비스를 분석하였다는 점에서 미국의 연방 공공 클라우드 서비스 현황을 객관적으로 볼 수 있다는 점이 장점으로 분석된다.



〈Figure 3〉 U.S. Federal IT Investment appeared in CRS Report ([8], p. 14, reprinted)

미국의 연방 공공기관의 클라우드 서비스 도입과 관련하여 2011년에서 2012년 사이 구축된 IaaS(Infra-as-a-Service)와 PaaS(Platform-as-a-Service)는 그 수요가 반 이상 감소하였으며, SaaS(Service-as-a-Service)는 다소 증가하였다. 미국 공공기관 IT 투자액은 2010년 약 81조 원까지 가장 가파르게 상승한 후, 대략 70조 원 중반으로 감소하였다고 보고되었다 (<Figure 3> 참조).

한편, 연방 클라우드 컴퓨팅 도입으로 인하여 약 960억 원이 절감되었다고 분석되었으며, 도입기관의 수는 101개로 늘어났다. 또한 연방정부는 IT 투자의 중복성을 배제하고 예산을 줄이기 위한 방안으로 관리예산처(OMB) 중심으로 클라우드 컴퓨팅 서비스를 추진하고 있으나, 기관별 특성에 따라서 클라우드 서비스화 할 수 없는 데이터/자원의 데이터 거버넌스 확립과 비 클라우드 IT 투자에 대한 평가가 함께 중요하다고 언급하였다.

4.2 미국 연방 공공기관의 클라우드 서비스 도입 관련 혜택 및 우려

이와 별개로 2014년 9월 미국 연방회계감사원(Government Accountability Office, GAO)는 미국 관리예산처(OMB)의 'Cloud First Policy'에 연방 클라우드 서비스 도입에 따른 장점과 우려할 점이 공존한다고 언급하였다. 즉, 미국 연방 공공기관의 클라우드 컴퓨팅 도입 장점에 대하여 6가지 측면 <Table 3>을 제시하였고, 클라우드 컴퓨팅 도입이 더 빠르게 추진되지 않은 이유에 대하여도 함께 분석하였다(<Table 4> 참조).

클라우드 서비스 도입의 장점과 관련하여 비용절감, 에너지 사용의 효율화, 가용성, 신속성, 보안성, 신뢰성 등의 측면에서 장점들이 있는데, 우선 클라우드 도입으로 인하여 불필요한 연방정부 IT시스템의 투자를 대폭 줄일 수 있는 점이 제시되었다. 또한 대형 전산센터의 경우 태양광이나 풍력 등 신재생에너지를 전력으로 일부 이용할 수 있어 기후변화에 대응할 수 있는 장점도 함께 있다는 점을 강조하였다. 가용성의 경우, 서버 자원 등의 갑작스러운 트래픽의 증가에도 불구하고 빠르게 용량을 확장하여 필요한 만큼 이용할 수 있는 점이 가장 큰 장점으로 보고되었으며, 복수의 클라우드 데이터 센터를 활용할 수 있어 데이터의 신뢰성이 높아졌다는 점 또한 큰 장점으로 부각되었다. 미국 연방 공공기관의 클라우드 서비스의 실제 도입결과, 상기와 같은 장점이 보고되고 있다는 점은 향후 국내에서도 공공기관의 클라우드 서비스 또한 분명한 도입 가치가 있을 것으로 판단된다.

이러한 보고된 장점 이외에도 문제점 등도 함께 분석되었는데 <Table 4>, 특히 이러한 이슈 등은 국내 공공기관의 클라우드 서비스 도입과 관련하여 매우 중요한 시사점이 될 것으로 판단된다. 첫째로, 미국 연방기관의 클라

〈Table 3〉 Benefits of Adopting Cloud Service in U.S. Public Organizations ([8], p. 21 summarized)

Category	Benefits
Cost Saving	• Government institutions are generally using a limited portion of overall computing facilities • Cloud system can decrease IT system investment and operation cost which would be high in legacy systems
Energy Efficiency	• More energy efficient than local server architecture • Energy savings are reported in many cases • New and renewable energy sources such as photovoltaic and/or wind power can be invested to large data centers
Availability	• No limits for device dependency • Internet connections are critical for seamless service
Agility	• Cloud system can support easy operations and upgrade of applications • Applications that needs much memory can be a good candidate for cloud computing because of strong computing capacity
Security	• There are a number of strong security vehicles in cloud computing
Reliability	• Cloud computing basically stores data in duplicated places against cyber-attacks

〈Table 4〉 Issues of Adopting Cloud Service in U.S. Public Organizations ([8], p. 21 summarized)

Category	Issues
Confirmation to federal security requirements	New security requirements are continuously updated; but there are few service providers to keep up with the new updates with respect to threats, weak points, technology, etc.
Overcoming silos among departments	Migration to cloud computing means changing to a new business model and this change causes another challenges in departments
Observing new infrastructure requirements	Existing network infrastructure and bandwidth may not be aligned with the new cloud computing requirements
Expertise of migration	There are shortages of experts in the field of cloud system migration from legacy architectures
Budgets for implementation	Cloud computing adoption is another factor for increasing budgets of initial implementation

우드 도입의 보안조건은 강력한 수준으로 지속적으로 추가되고 있는데 비하여, 이에 발맞추어 강력하게 보안조건을 준수할 수 있는 사업자들이 많지 않다는 점이 보고되었다. 국가 데이터와 관련된 보안수준은 빠르고 정교하게 변하는 외부의 공격에 대비하여 높을수록 좋을 것이다. 그러나 시장에서 이를 지킬 수 있는 사업자가 만약 존재하지 않는다면 클라우드 서비스 도입 의도 자체를 퇴색시킬 수도 있을 것으로 생각되며, 정부는 그 균형점을 찾을 수 있는 대안을 모색하여야 할 것이다.

두 번째 이슈는 클라우드 도입이 조직 내 새로운 문제를 야기한다는 것인데, 클라우드 도입과 관련하여 부서간의 소통은 물론 데이터의 공유 등이 우선적으로 필요할 것으로 보인다. 셋째로, 클라우드 도입이 클라우드 컴퓨팅 서비스를 위한 데이터 인프라 등의 요구사항에 못 미칠 수 있다는 점도 중요한 사안으로, 특히 국내 지방자체단체 중 서울, 경기 등 예산/재정 자립도가 높은 지역을 제외하고 중소도시의 경우는 클라우드 구축 전산 인프라가 열악할 수 있다고 생각된다. 따라서 국내 공공기관 클라우드 도입은 사전에 중앙정부와 지방정부의 도입을 구분하여 각 기관의 인프라가 클라우드 서비스를 감내할 수 있는 범위에서 클라우드 서비스를 도입하거나, 혹은 단계별로 인프라를 점진적으로 개선하며 적용할 수 있도록 추진되어야 할 것이다.

5. 국내 공공기관 클라우드 서비스 도입전략 프레임워크

5.1 도입전략 프레임워크 관련 선행연구

국내와 달리 2011년 미국 정부는 도입을 위한 로드맵을 작성하였고, '선택(Select)' → '제공(Provision)' → '운영(Manage)' 세 가지 축의 클라우드 도입전략 프레임워크를 제시하였다(<Table 5> 참조)[37].

미국 정부 도입전략 프레임워크 중 도입 활성화를 위해서는 예정기관의 자체적인 클라우드 서비스 준비도 파악이 중요한 것으로 분석되

〈Table 5〉 2011 U.S. Government's Cloud Computing Implementation Strategy Framework

Select	Provision	Manage
• Selecting IT services that will be migrated to cloud computing • Defining core values for migration such as efficiency, agility, innovation, etc. • Identifying cloud service readiness such as security level, solution availability from market, technology cycle, etc.	• Reflecting the needs from department and units • Guaranteeing interoperability and integration • constituting a contract with service providers that meet a certain requirements • Identifying legacy system is remaining values when providing cloud computing services	• Different approach to IT; as a service rather than as an asset • Learning new technologies in this domain • Monitoring SLA and improving capability through compliance • Re-evaluation of service providers, risk minimization with profit maximization

었다. 즉, 도입 예정기관의 데이터 거버넌스(Data Governance)가 확립이 되어야 준비도가 높다고 할 수 있을 것이다. 데이터 거버넌스는 기관에서 사용하는 데이터의 가용성, 유용성, 통합성, 보안성을 관리하기 위한 정책과 프로세스를 포함하며, ISO/IEC 38500에 언급된 것처럼 기관의 목적에 부합하는 IT 및 데이터 등에 대한 이용-지시-모니터링의 프레임워크를 의미한다[9]. 한편, 한 선행 연구에서는 조직의 데이터 거버넌스 역량에 대한 123명의 IT전문가를 대상으로 설문조사를 시행하였고[10] 조직의 데이터 거버넌스 역량에 대하여 측정을 하였다. 71%에 해당하는 기관들은 중간이거나 낮은 수준으로 응답을 하였다. 데이터 거버넌스를 확립하는 단계는 기관에서 ①데이터에 대한 조사 및 발견, ②데이터 이용 프로세스 디자인, ③활용, ④유지보수, ⑤중복 데이터 정의/활용의 5단계로 정의하고 있으며 이는 시스템 개발수명주기 이론처럼 순환한다고 언급하고 있다[19].

미국의 조사결과에서도 기관의 데이터 거버넌스의 수준은 높은 수준이 아니라고 조사되었으며, 특히 공공기관의 경우는 기관의 데이터 거버넌스가 명확하게 확립이 된 후에야 조직의 목적에 부합하는 클라우드 시스템을 효과적으로 도입할 수 있을 것으로 전망된다. 사실 미국에서도 공공기관의 실제 클라우드의 도입/적용은 2012년에서야 활성화 되었다. 한국에서는 비교적 빠르게 2010년 정보화진흥원에서 클라우드 컴퓨팅의 공공부문 적용 방안에 대하여 보고서를 작성하였고, 적용 5단계를 <Table 6>과 같이 제시하였다.

정보화진흥원의 클라우드 컴퓨팅 공공부문 적용 5단계 도입방안에서는 전자정부 서비스의 클라우드 SaaS 전환이 우선적으로 고려되었다고 할 수 있다. 미국 연방정부 클라우드 서비스 도입에서도 볼 수 있듯이 최근까지 다른 국가의 공공기관 클라우드 서비스 도입은 IaaS 기반 클라우드 인프라 도입이 우선적으로 추진되어 왔다. 이는 부처별 다양한 기능 및 컨텐츠를 처리할 수 있는 통합 클라우드 플랫폼 기반 시스템 개발이 쉽지 않았고, 인프라 구축/유지보수 등의 비용이 상대적으로 커서 클라우드 인프라 전환으로 효과를 빠르게 볼 수 있는 부분이 IaaS를 통하여 가능하였기 때문으로 추정된다.

또한 한국의 행정안전부(현 행정자치부)에서는 '정부 3.0과 클라우드 유형 프레임워크'를

제시하였다. 이 프레임워크에서는 6개의 클라우드 서비스를 ① 클라우드 서버, ② 클라우드 PC, ③ 클라우드 저장소, ④ 웹기반 업무SW, ⑤ 클라우드 개발환경, ⑥ 클라우드 플랫폼 등으로 선정하였다. 또한 중점 추진 과제로 클라우드 서버, 클라우드 저장소, 웹기반 업무SW 등을 확정하였다. 클라우드 서버는 정부통합전산센터에서 이미 2012년부터 추진되어 오고 있으며, 2012년 시범운영 결과 운영비용의 40%, 서버 설치 공간의 60% 절감이 보고되었다[14].

그 동안 제시되고 있는 클라우드 서비스 전략 프레임워크는 어찌 보면 공공 클라우드 시장

〈Table 6〉 2010 NIA's Five-Phases Plan for Implementing Cloud Computing in Korean Public Organizations

	Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
Contents	• Email systems by SaaS (Pilot Project)	• e-document system by SaaS (1st phase) • Building K-Cloud Center	• G-Apps Implementation • GAP Introduction • e-document system by SaaS (in a central government)	• W-Cloud Center Implementation (1st phase) • e-document system by SaaS (in a local government) • Strong G-Apps and GAP implementation	• W-Cloud Center Implementation (Final) • Transactions between K-Cloud and W-Cloud • e-document system by SaaS (Completion) • Facilitation plan for SW on GAP
Requirements	• Law for cloud computing • Facilitating ICT usage, credit information, security • Cloud Computing EA • Defining Security requirements	Setting SLA standards	• GBP Completion • Database Re-engineering • Law and ordinances for G-Apps and GAP	• Distributing manuals and documents for GAP	• Finalizing law and ordinances for system resource interactions
Parallel Process	• K-Cloud Center transition plan • SLA standards plan • Technical standards for cloud computing	• W-Cloud Center implementation plan • Standards for cloud computing • Public sector BPM • G-Apps implementation plan • e-document system by SaaS	• W-Cloud Center implementation plan • e-document system by SaaS (local government 1st phase) • GAP and G-Apps facilitation plan	• Law and ordinances for system resource transaction/ exchange • W-Cloud Center Implementation (2nd phase) • e-document system by SaaS (completion)	• Transition to cloud computing

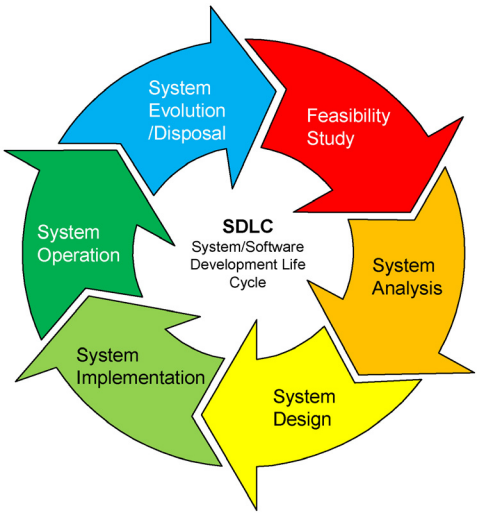
* Acronyms: SaaS: Software-as-a-Service, K-Cloud: central government cloud data center, W-Cloud: local government (wide area) cloud data center, GAP: Government Application Platform.

전체에 대한 거시적 성격의 정책 프레임워크라고 할 수 있다. 그러나 공공기관은 각자 다양한 분야의 자체적인 내부 비즈니스 프로세스 및 데이터를 보유하고 있고, 처한 상황이 다를 수밖에 없다. 즉, 클라우드 법에 적용을 받는 공공병원, 국공립 대학교, 공사, 수협/신협/농협 등등 다양한 공공기관이 존재하고, 이제는 클라우드 서비스 도입 기관 중심의 미시적인 활성화 전략 수립이 필요한 시점이라고 판단된다.

5.2 도입 활성화 전략 프레임워크 제안

공공기관의 클라우드 서비스 도입, 특히 중앙정부와 지방정부의 클라우드 도입 서비스 활성화를 위해서는, ① 미국/한국의 클라우드 서비스 도입 전략 프레임워크를 벤치마킹하고, ② 미국 연방 공공기관 클라우드 도입사례의 문제점을 분석하여, ③ 이를 도입 공공기관의 측면에서 보다 구체화된 전략을 수립하는 것이 적절하다고 보인다. SDLC는 정보 시스템 개발, 구축 등에 있어서 가장 효과적인 방법으로 여겨지고 있다[32]. 특히, SDLC는 보안기능이 통합되는 시스템에 있어서 각 개발 프로세스별로 조율할 수 있어서 보안기능이 중요한 이슈인 클라우드 시스템 도입에 있어서 적절한 모형 중의 하나라고 할 수 있다[32].

CRS 보고서에서 언급된 미국 공공기관 클라우드 도입의 여섯 가지 장점을 극대화하고, 다섯 가지 저해요인에 대한 효과적인 대응 전략을 시스템 개발 수명주기(SDLC)에 맞추어 각 단계별로 전략을 수립하고, 구축 방향에 대하여 실천방안을 수립하는 것이 공공기관의 클라우드 도입을 가속화할 수 있을 것으로 판단된다(<Figure 4> 참조).



〈Figure 4〉 Implementing System Development Life Cycle (SDLC) to Cloud Computing Adoption Process in Public Organizations

SDLC란 PLC(Product Life Cycle)와 같은 의미를 시스템 개발에 적용시킨 것이다.

SDLC의 일반적 순서는 (1) 타당성 조사(Feasibility Study) 단계-조직적/경제적/기술적/운영적/동기적 타당성 검토 (2) 시스템 분석 단계(Systems Analysis)-조직분석/현재 시스템 분석/시스템 고객 요구사항 분석 (3) 시스템 설계 단계(Systems Design)-인터페이스 설계/데이터 설계/프로그램 설계 (4) 시스템 구축 단계(Systems Implementation)-하드웨어, 소프트웨어 획득/테스팅/시스템 전환 (5) 시스템 운영 단계(Systems Operation)-시스템 유지/보수/개선 (6) 시스템 확산 단계(System Evolution/Disposal)-시스템의 성과 평가를 통한 확산/중지/개선 등 모색 등으로 구분할 수 있다.

다양한 개발방법론(폭포수 모형, 프로토타

〈Table 7〉 Strategic Key Factors for Vitalizing Public Organization Cloud Computing Adoption

SDLC Phases	Strategic Key Success Factors
Feasibility Study Phase	• Setting as the most important phase of public organization's cloud computing service implementation • Research supports for identifying core values of adopting cloud service in terms of economic/technical/operational feasibility • Strong investigation for identifying a data governance in the organizations needed • Pre-evaluate the capabilities of cloud computing service providers regarding technical expertise and supports • If an organization adopting cloud computing has no data governance inside, additional data governance project should be launched before actual implementation of cloud computing
System Analysis Phase	• Additional analysis on legacy system and business processes • Identifying system migration milestones • Considering an open-source based platform which can be independent against specific vendor locked-in platforms • Identifying special requirements of institutions • Most public organizations can be implementing Private and/or Hybrid type cloud computing. Especially, local governments have their e-government systems named *Se-ol* System and *Local Administration System*. For this reason, any duplicate investment issues regarding the systems should be cleared in advance
System Design Phase	• Interface design/data architecture design/application architecture design • At the system design phase, exploring the chances of using outside marketplace modules • As stated in the CRS report, additional plan for legacy system even after the implementation of cloud system is critical • Design on the basis that public data are stored inside of Korean territory and not stored in the cloud data center located in foreign countries • Consider cloud based back-up system • Public organizations have many fixed location PC's inside. For this reason, cloud computing should be designed reflecting the fact that fixed PC's are more focused than mobile access
System Implementation Phase	• At the system implementation phase, interoperability between cloud system and legacy system, test of modules, training of operational staffs are important • Reliability and security standard check
System Operation Phase	• Establish systematic technical support process for any incidents • CRS Report has pointed that expert operation staffs are very limited. For this reason, from the planning stage, system operation and maintenance staffs should be considered
System Expansion/Exit Phase	• Identify key success factors if the system is valuable, unless otherwise describe any issues and problems for modification or exit of the system

입 모형, 나선형 모형, 반복 점증적 모형 등등 다수)에 대해서도 세밀하게 적용할 수 있으나, 개발 방법론은 전략이라기보다는 시스템 개발 방법의 측면이므로, 본고에서는 세부적으로 다루지 않고 일부 방향성에 대해서만 언급하였다. 시스템 개발 수명주기에 맞추어 각 단계에서 중요한 클라우드 도입전략의 중요 핵심 요인(Key Success Factor) 등은 아래 표와 같다(<Table 7> 참조).

CRS 보고서에서 언급된 클라우드 서비스의 장점과 이슈 등을 SDLC 프로세스에 적용하면 다음과 같다. 첫 번째인 타당성 조사(Feasibility Study) 단계로, 동 단계가 어찌 보면 클라우드 서비스 도입에 있어서 가장 중요한 단계라고 할 수 있을 것이다. 왜냐하면 조직의 클라우드 서비스 도입가치 등을 명확하게 정의하고, 도입기관의 데이터 거버넌스 등을 체계적으로 하여 어떠한 데이터를 클라우드화 할 지 정의하고 기획하는 것이 중요하기 때문이다[32]. 두 번째 단계인 시스템 분석 단계(Systems Analysis)에서는 특히 기존 레거시 시스템 등에 대한 분석이 중요한데, 이 단계에서는 플랫폼을 구축 시 오픈소스로 갈 것 인지, 벤더 종속적인 플랫폼으로 갈 것 인지 사전 준비가 되어야 할 것이다.

세 번째인 시스템 설계 단계(Systems Design)에서는 인터페이스 설계 등이 중요한데, 클라우드 구축이외에도 클라우드화 되지 않는 데이터/레거시 시스템 연계에 대한 디자인이 아울러 중요할 것으로 보인다. 한국의 공공기관의 데이터가 민간기업의 데이터처럼 다른 나라의 클라우드 데이터 센터에 저장되지 않게 하는 클라우드 시행세칙의 적용도 중요한 디자인 항목이라고 할 수 있다.

네 번째 시스템 구축 단계(Systems Implementation)에서는 공공 클라우드에 적합한 하드웨어, 소프트웨어 등을 사전에 테스트하고, 시스템 이전계획 등이 적절히 수립되어야 할 것이다. 다섯 번째 시스템 운영 단계(Systems Operation)에서는 중단없는 시스템 운영이 될 수 있도록 시스템을 튜닝하고 운영하는 운영역량의 보유가 중요한데, 이를 위해서는 클라우드 관련 역량을 보유한 시스템 운영 책임자가 내부에 반드시 있어야 할 것으로 분석된다.

마지막으로 시스템 확산 단계(System Evolution/Disposal)에서는 공공기관 클라우드 도입이 조직의 예산과 성과, 보안 측면의 안정성 등에 대하여 어떠한 영향을 미치는 지에 대하여 명확한 평가를 진행하고 이를 바탕으로 확산할지 아니면, 클라우드 시스템 의존도를 줄일지 등을 결정하여야 할 것이다[38].

5.3 지방 공공기관 클라우드 서비스

2015년 9월부터 시행된 클라우드 법은 중앙정부 뿐 아니라 지방정부 등의 클라우드 서비스를 모두 적용된다. 그러나 지금까지 진행되어 온 지역정보화는 다소 중앙정부 중심이었다고 할 수 있다. 즉, 중앙정부 주도로 지역정보화 사업을 추진하다보니 지역정보화 사업에서 '지역'은 없고 '정보화'만 있다는 의견도 제기 되었다[21]. 또한, 중앙정부의 주도로 추진되는 지역정보화 사업의 경우는 초기에는 중앙 행정기관의 주도로 진행이 되지만, 사업 종료 후 운영/유지보수에는 재정 자립도가 낮은 지방 정부가 운영을 해야 하는 어려움이 있다고 보고되었다[21].

지방정부의 클라우드 서비스 도입 또한 예외가 아니라고 판단된다. 예를 들어 지방 정부

에 필요하지 않거나 과도하게 범위가 넓은 클라우드 서비스를 중앙부처에서 일방적으로 추진하는 것은 클라우드 서비스의 핵심적인 가치를 훼손할 가능성이 높으며, 특히 데이터 거버넌스 체계가 구축되지 않은 지방정부 및 공공기관의 경우 이러한 어려움은 더욱 커질 것으로 전망된다.

중앙부처에서 추진하는 정부 3.0 클라우드 추진계획에도 클라우드 ISP(정보화계획) 및 법제도 개선안을 도출하고 범부처 확산으로만 클라우드 도입 로드맵이 정의되었으며, 중앙정부와 지방정부를 구분하여 확산전략을 고려하고 있지 않은 것도 문제이다. 또한 한 연구에서는 지방자치단체 정보화 담당자 210명을 대상으로 시도, 시군구, 광역단체의 클라우드 추진모델에 대하여 조사하였는데, 중앙집중형(39명), 지역분산형(69명), 이원화(55명), 현 체제 유지보수(33명)의 네 가지 선택 중 지역분산형이 가장 높은 추진모델로 조사되었다[16]. 다만, 동 연구에서 통계적으로 네 가지 유형 구분이 유의미하지 않은 점($p = 0.585$)때문에 후속 보완조사가 있어야 할 것으로 판단되나 현 체제 유지를 주장하는 응답자도 중앙집중형 선호 수준만큼 많았던 결과에서 볼 수 있듯이, 지방정부의 클라우드 서비스 도입은 중앙정부 보다도 더 신중하게 접근되어야 할 것으로 사료된다.

6. 결 론

국내 공공기관의 클라우드 컴퓨팅 도입전략 수립은 다양한 차원에서 접근이 가능하다. 기존 연구 및 조사보고서들에서도 언급되고 있듯이, 도입 가능한 클라우드 서비스 유형은 데스크톱 가상화, 애플리케이션 가상화, 클라우드 스토리지는 물론, 단순 이메일 서비스 사용, 클라우드 기반의 교육 이러닝 프로그램 등등 그 범위는 더욱 확대될 수 있다.

미국의 공공기관 클라우드 도입 로드맵에서는 준비단계에서 클라우드 서비스로의 이전 가치가 무엇인지를 명확히 하고, 보안, 시장 가능성, 정부의 준비도, 기술의 순환주기 등을 반드시 파악할 필요가 있다고 강조하고 있는데, 이는 다분히 도입기관 차원의 전략 및 준비/기획이 필요한 것을 의미한다. 지금까지 국내 공공기관 클라우드 서비스 도입연구는 주로 거시적 정책 관점에서 도입 활성화를 이야기하였다면, 본고는 개별 공공기관 차원에서의 보다 미시적 관점에서 시스템 개발수명주기(SDLC) 프로세스를 활용하는 도입 활성화 전략 프레임워크를 제시하였다.

사실 클라우드 서비스 도입 시 가치와 핵심요인에 대한 기관의 준비도 파악이 물론 중요하나, 전 절에서 언급하였듯이 실무적으로 더 중요한 것은 도입기관의 전산환경이 얼마나 클라우드 도입에 적합한 지 우선적으로 파악하고, 그에 맞는 데이터 거버넌스 구조를 먼저 확립하는 것이라고 할 수 있다.

데이터 거버넌스가 명확하지 않은 공공기관은 보안 정책의 수립, 클라우드 영향의 파급력 등을 정확하게 측정할 수 없을뿐더러, 이로 인하여 클라우드 서비스 도입이 어려울 수 있다. 미국 연방 공공기관의 도입사례 등에서 볼 수 있듯이, 클라우드 서비스로의 이전을 담당할 수 있는 전문가의 부족 등은 반드시 선결되어야 할 과제이기도하며, 공공기관의 클라우드 서비스 촉진을 위해서는 반드시 해당기관의 데이터 거버넌스가 명확하게 정의가 되어야

할 것이다. 마지막으로 클라우드 법은 중앙정부뿐 아니라 지방정부까지도 영향을 끼칠 수 있고, 오히려 중앙정부보다 지방 공공기관에 더욱 더 다양한 클라우드 서비스의 활용이 있을 수 있음에도 불구하고, 지금까지는 지방공공기관 클라우드 서비스 도입 방안에 대하여는 심도있게 연구되지 않았다고 보인다.

본 연구는 국내 공공 클라우드 컴퓨팅 도입에 대하여 전략적 프레임워크를 제안하고 있으나 국내의 다양한 공공기관-특히 지방정부 등-의 성격에 맞는 개별적인 클라우드 컴퓨팅 도입 전략에는 여러 다른 전략적 핵심요인이 있을 것으로 판단된다. 그러한 시각에서 SDLC는 미국의 NIST에서 권고하고 있는 클라우드 컴퓨팅 도입의 방법론이기는 하나, 다른 방법론이 국내 도입 상황에 더 적합할 수 있는 사실은 본 연구의 한계이며, 향후 연구에서 공공기관의 전략 프레임워크를 실행하는 방안과 함께 다루었으면 하는 것이 저자의 바람이다. 미래의 클라우드 컴퓨팅 연구는 중앙정부와 지방정부를 구분하여 클라우드 서비스 도입 가치 등에 기반을 두는 전략이 마련되어야 할 것이며, 지방정부의 유지보수 예산 절감, 레거시 시스템 및 비 클라우드 서비스 통합/구축/유지/보수 등을 종합적으로 고려하는 전략이 함께 수립되어야 할 것이다.

References

[1] Baek, S., Shin., J., and Kim, J., “Exploring the Korean Government Policies for Cloud Computing Service,” Journal of the Society for e-Business Studies, Vol. 18, No. 3, pp. 1-14, 2013.

[2] Chang, C., “Case and Lessons Learned from Cloud Computing Implementation in Public Organizations,” Local Informatization Magazine, Vol. 74, pp. 22-31, 2012.

[3] Chang, H., “OpenStack Introduction and Demo for Beginners,” OpenStack Summit, 2014.

[4] Chang, S., “Strategy and Action Plans for Cloud Service,” Broadcasting and Communication Policy, Vol. 24, No. 9, pp. 1-22, 2012.

[5] Chang, S., Sohn, K., and Shin, H., “An Analysis on the U.S. FedRAMP,” Weekly Technology Trend, NIPA, pp. 11-24, 2013.

[6] CIO Magazine, “What are the implications of Cisco and IBM’s merging of open-stack companies?” [URL] http://www.ciokorea.com/news/25469.

[7] Dahlberg, T. and Nokkala T., “A Framework For The Corporate Governance of Data-Theoretical Background and Empirical Evidence,” Business, Management and Education, Vol. 13, No. 1, pp. 25-45, 2015.

[8] Figliola, P. M. and Fischer, E. A., “Overview and Issues for Implementation of the Federal Cloud Computing Initiative: Implications for Federal Information Technology Reform Management,” US Congressional Research Service (CRS), 2015, 1.

[9] Goetz, M., “Data Governance Will Shine In The Data Economy,” KM World Magazine,

pp. 10-11, 2013, July/August.

[10] Gregory, A., "Data Governance- Protecting and Unleashing the Value of Your Customer Data Assets-Stage 1: Understanding Data Governance and Your Current Data Management Capability," Journal of Direct, Data and Digital Marketing Practice, Vol. 12 No 3, pp. 230-248, 2011.

[11] Han, S., Feasibility Study on Strategic Planning to Build a Cloud Computing Environment for Smart Education, KERIS Issue Report, 2011.

[12] IT Daily, "Cover Story 2015, Cloud Computing will be launching strongly," [URL] http://www.itdaily.kr/news/articleView.html?idxno=58706.

[13] Kim, J., "Public Cloud Computing Model for Smart Office Environment Implementation," TTA Journal, Vol. 148, pp. 50-54, 2013.

[14] Kim, J. and Kim, E., "Policy and Status of Government Cloud Computing," Information Science, pp. 32-39, 2014.

[15] Kim, S., Choi, Y., and Jang S., "Building Future e-Government Service Based on Cloud Computing Architecture," Journal of Information Technology and Architecture Vol. 7. No. 3, pp. 269-280, 2010.

[16] Kim, T., Hwang, S., Suh S., and Kim D., "Designing Cloud Computing System for Local Governments: In Pursuit of an Optimal Model Utilizing Case Study and Feasibility Study, Journal of Korean Association for Regional Information Society, Vol. 18, No. 1, pp. 85-107, 2015.

[17] Koh, G., "A Study on Security-Enhanced Cloud Service E&C(Evaluation and Certification) Scheme," Journal of Security Engineering, Vol. 9, No. 6, pp. 481-494, 2012.

[18] Korea Cloud Service Association, Cloud Infra(Open Cloud), KCSA, 2014.

[19] Kundra, V., "25 Point Implementation Plan to Reform Federal Information Technology Management," The White House, 2010, 9.

[20] Kundra, V., "Fedral Cloud Computing Strategy," The White House, 2011.

[21] Lee, M., "How to Ensure the Financial Resource Diversity of Local Information Project: A Exploratory Study from the Institutional Perspective," The Korean Journal of Local Government Studies, Vol. 17, No. 4, pp. 387-407, 2014.

[22] Ministry of Security and Public Administration(MoSPA), Government 3.0 Cloud Implementation Plan, MoSPA, 2013.

[23] Ministry of Security and Public Administration(MoSPA), Guideline for Cloud Office Environment in Public Administration Organizations, MoSPA, 2012.

[24] National Information Agency Report, A Study on the Introduction of the Certificate System to Activate the Cloud Service, NIA, 2010.

[25] National Information Agency Report, Analysis of Service Cases and New Public Services Based On The Cloud Computing,

NIA, 2012.

[26] National Information Agency Report, Cloud Policy Support for the Activation of Public Service Broadcasting Communication Convergence, NIA, 2012.

[27] National Information Agency Report, The Study on Applying Cloud Computing for Public Sector, NIA, 2010.

[28] NIST, US Government Cloud Computing Technology Roadmap Vol. 1 and 2, Department of Commerce, 2014.

[29] Oh, K., "Critical Review on Cloud Act in Korea," Democratic Legal Studies, Vol. 56, pp. 247-276, 2014.

[30] Ra, J., "A Study on Cloud Computing Service Features," Journal of Digital Contents, Vol. 12, No. 3, 2011.

[31] Ra, J., Lee, J., Shin S., Kim J., and Choi, Y., "Classification Model for Cloud-based Public Service," Journal of Information Technology and Architecture, Vol. 10. No. 4, pp. 509-516, 2013.

[32] Radack, S., "The System Development Life Cycle(SDLC)," National Institute of Standard and Technology(NIST) Special Publication(SP) 800-64, 2009.

[33] Seo, K., "A Comparison Study between Korean Cloud Service Certification Systems and U.S. FedRAMP," The Journal of Digital Policy & Management, Vol. 10, No. 11, pp. 59-65, 2012.

[34] Shin, S. and Song, S., "A Priority Study for Applying Public Cloud Services in Korea by Mapping the SRM with Overseas Cloud Services in the Public Sector," Internet and Information Security, Vol. 3, No. 3, pp. 67-89, 2012.

[35] Shin, Y., "A Study on Personal Information Security Policy in Cloud Service Expansion," Korea Society of Public Administration, Winter Conference, pp. 1674-1692, 2012.

[36] Song, I., "Sensitivity Analysis of Quasi-Governmental Agencies' Decisions for Cloud Computing Service," Journal of Internet Computing and Services, Vol. 16, No. 1, pp. 91-100, 2015.

[37] Song, S., "Consideration of Cloud Computing SLA," TTA Journal, Vol. 139, pp. 59-64, 2012.

[38] Song, S., Kim. J., Ra, J., and Lee, J., "A Study on Adopting Model for Cloud-based public service," The Journal of Digital Policy and Management, Vol. 11, No. 5, pp. 63-72, 2013.

[39] Zdnet news, "A Perspective of Openstack betting of SKT, long-term investment will be the success factor," [URL] http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150206180553.

저 자 소 개

강상백	(E-mail: chriskang@klid.or.kr)
1997년	한양대학교 경제학과 (학사)
2002년	University of Illinois at Urbana-Champaign 경제학과 (석사)
2007년	University of Missouri-St. Louis 경영학과 (박사)
2000년~2007년	한국전자통신연구원 (ETRI) 연구원
2007년~2008년	LG Uplus 단말데이터본부 부장
2008년~2014년	SK C&C 중동 지사장 (Dubai)
2014년~2015년	KIST 부설 녹색기술센터 글로벌협력부장
2015년~현재	한국지역정보개발원(KLID) 글로벌협력부장
관심분야	전자정부, 모바일, 클라우드, 핀테크, 전기자동차, 기후변화 대응, 글로벌 협력