연구논문 정보화정책 제18권 제1호, 2011년 봄호, pp.24~44

클라우드 서비스 인증제도 수립을 위한 프레임워크

서 광 규*

요 약 지난 몇 년간 클라우드 서비스의 혁신은 IT발전에 기여한 가장 큰 잠재력을 가진 기술 중에 하나이다. 그러나 클라우드 서비스의 잠재력을 발휘하기 위해서는 서비스 제공자와 소비자관점에서 다양한 이슈들에 대한 명확한 정의와 이해가 필요하다. 현재의 클라우드 관련 연구들은 기술 자체에 중점을 두고 있으나, 클라우드 서비스를 둘러싸고 있는 비즈니즈 측면에서의 이슈들에 대한 이해도 시급하다. 점점 더 많은 개인과 기업의 정보들이 클라우드 서비스에 놓이게 되면, 주된 관심은 어떻게 안전하고 신뢰할 수 있는 클라우드 서비스를 제공할 것인가에 맞추어지게 된다. 따라서 성공적인 클라우드 서비스를 위해서는 클라우드 서비스의 안전성과 신뢰성을 보증할 수 있는 인증제도의 수립이 필요하다. 본 논문에서는 안전하고 신뢰할 수 있는 클라우드 서비스를 위한 인증제도의 프레임워크를 개발한다. 이를 위하여 클라우드 서비스 품질과 인증과 관련된 핵심 이슈들을 식별하고, 클라우드 서비스 영역과 클라우드 서비스 제공자 영역의 인증제도를 위한 시스템적인 프레임워크를 개발한다. 또한 개발된 인증제도의 평가방안도 제안한다.

주제어: 클라우드 서비스, 인증제도, 서비스 인증, 사업자 인증

A Framework for Establishing Cloud Service Certification Systems

Kwang-Kyu Seo

Abstract The evolution of cloud computing over the past few years is potentially one of the major advances in information technology. However, if cloud computing is to achieve its potential, there needs to be a clear identification and understanding of the various issues involved, both from the perspectives of the providers and the consumers of the technology. While a lot of research is currently taking place in the technology itself, there is an equally urgent need for understanding the business-related issues surrounding cloud computing service. As more and more information on individuals and companies are placed in the cloud service, concerns are beginning to grow about just how safe and reliable an environment it is. For successful implementation of cloud services, it is necessary to establish the certification systems to ensure the safety and reliability of cloud services. This paper provides a safe and reliable framework for cloud service certification systems. In order to develop it, the critical issues related to service quality and certification of cloud services have been identified and the systematic framework for certification systems of cloud services and service provider domains have been developed. An evaluation method for the developed certification systems is also proposed.

Keywords: cloud service, certification system, service certification, provider certification

2011년 3월 19일 접수, 2011년 3월 21일 심사, 2011년 3월 29일 게재확정

* 상명대학교 경영공학과 교수(kwangkyu@smu.ac.kr)

Ⅰ. 서론

최근 세계경제위기는 많은 기업들에게 원가절감에 대해 강한 동기를 부여하고 있다. 이에 기업들은 IT 비용 등의 원가절감을 통한 생존전략을 적극적으로 모색해야만 하는 상황에 놓이게 되었다.

이러한 상황은 클라우드 컴퓨팅 서비스(이하 클라우드 서비스)를 중요한 IT전략기술로 선정되게 하기도 했다. 특히 클라우드 서비스 기술이 기업의 IT인프라에 대한 유지보수 부담을 경감시키고, 사업초기 대규모 초기투자비용에 대한 부담도 경감시킬 수 있는 등 기업의 IT 혁신을 통한 비용절감을 이룰 수 있다는 기대로 관심이 증대되고 있다. 또한 스마트폰 등 모바일 단말기의 진화에 따른 활용기능 증가와 광대역 네트워크의 발달로 클라우드 기반의 유비쿼터스 모바일 서비스도 생활의 중심으로 부각되고 있다(김형곤 외, 2010).

구글, 아마존 등 인터넷 기업뿐만 아니라 마이크로소프트, IBM과 같은 IT 벤더들도 클라우드 서비스가 IT패러다임을 변화시킬만한 중요한 기술임을 주창하며 이를 구현한 서비스나 비전 및 대규모 투자계획을 통해 차기 주력사업으로 육성시킬 것임을 발표하고 있다(김창헌 외, 2010).

최근 SNS(Social Network Service), 데이터 트래픽, 웹 2.0 어플리케이션, 실시간 데이터 스트리밍 구현 등 동 분야의 급성장은 다양하면서도 빠르게 변화하는 IT환경의 진화를 요구하고 있으며 그 진화의 핵심에 클라우드 서비스가 조명되고 있다. 즉, 네트워크의 고도화와 웹의 급속한 진화와 더불어 급증하는 트래픽과 컴퓨팅 파워 문제를 해결하기 위한 대안으로 클라우드 서비스에 대한 관심이 높아지고 있는 것이다(Marston, et al., 2011; Svantesson, et al., 2010).

클라우드 서비스라는 개념은 2006년 9월 구글의 크리스토프 비시글리아(Christophe Bisciglia)라는 직원에 의해 구글의 CEO 에릭 슈미츠(Eric E. Schmidt)와의 회의에서 제안된 것으로 참여, 개방, 공유를 상징하였던 웹 2.0에 자유로움(Free)을 추가하여 웹 3.0이라고도 불렸다. 즉 소통과 디지털 민주주의의 상징에서 효율성과 확장성을 추구하는 비즈니스로의 관점 변화를 의미하는 개념이다. 클라우드 서비스로 진화하기 위해서는 인터넷상의 분산된 시스템과 자원을 공유하는 그리드(Grid) 방식의 분산기술 및 가상화 기술과, 컴퓨팅 파워와 저장공간에 대한 과금방식이 사용량에 따른 비용지불 방식인 유틸리티 방식의 과금모델이 적용되는 인터넷 환경이 요구된다(이강찬 외, 2010).

클라우드 서비스는 인터넷이 접속가능한 공간이면 언제 어디서나 어떠한 단말기로도 컴퓨팅 자원을 이용할 수 있게 해 주는 기술로써 클라우드 서비스 시대의 개막은 기존의 하드웨어 또는 소프트웨어 중심에서 서비스 중심의 비즈니스 모델로의 전환을 의미하는 것이다. 이에 관련 기업뿐만 아니라 공공기관, 개인에 이르기까지 모든 영역의 서비스 이용자들의 삶에도 큰 변화를 가져올 것이다. 이러한 클라우드 서비스는 기업 및 유관산업에 다양한 모습으로 발전하여, 새로운 산업과 많은 신규 일자리를 창출할 것으로 예상되고 있으며 동시에 클라우드 서비스의 보안이 중요한 이슈로 대두되고 있다(김미연 외, 2010; 이창범, 2010; 임철수, 2009; Paquette, et al., 2010; Subashini, et al., 2011; Taylor, et al., 2010).

한국 IDC가 발표한 '2011 국내 기업 IT 수요조사' 결과에 따르면, 국내 기업의 현재 클라우드 서비스를 사용하고 있는 비율은 13%로 아직은 미미한 수준으로 아직은 클라우드 서비스 도입과 그 확산이 활발히 이루어지지 않은 상황인데, 이는 클라우드 서비스가 기업정보화 시장에서 아직도 신뢰기반을 형성하지 못한데서 기인하고 있다고 할 수 있다. 클라우드 서비스가 기업정보화 시장에서 신뢰기반을 형성하기 위해서는 해결해야할 여러 가지 문제들이 있는데, 서비스 품질기준, 권한남용방지, 정보보호

등의 법규와 서비스 도입 지원 정책을 사전에 준비가 필요하다. 즉, 클라우드 서비스 확산에 따른 사업자와 소비자간의 품질분쟁, 서비스 이전, 정보 유출 처리 등에 대한 서비스 가이드라인과 서비스 품질기준, 정보보안 등의 법규와 인증체계를 마련해야 한다. 이를 위한 핵심 이슈 중에 하나가 클라우드 서비스 사업자가 제공하고 있는 서비스에 대해 믿을 수 있는 객관적인 평가를 통한 클라우드 서비스를 인증하고 이를 통한 시장에서의 신뢰를 확보하는 것이다. 이를 통하여 클라우드 서비스 산업 전반에 대한 불안감을 해소하고 서비스의 품질을 향상시킨다면 클라우드 서비스의 활성화는 물론, 국내 IT 산업의 국제 경쟁력 확보가 가능하다. 따라서 클라우드 서비스를 보다 활성화하기 위해서는 클라우드 서비스에 대한 안전성 · 신뢰성 · 지속성 제고를 통한 공급자와 이용자간 신뢰기반을 구축하여야 하는데, 이를 위해서는 보다 안전하고 신뢰할 수 있는 체계적인 클라우드 서비스 인증제도의 개발이 필요하다.

본 연구에서는 클라우드 서비스 이용자의 신뢰성을 제고하고 클라우드 서비스 시장의 조기 확산을 위하여 클라우드 서비스 인증제도를 위한 프레임워크를 제시하고, 이를 통하여 궁극적으로 클라우드 서비스 및 사업자의 품질 수준, 안정성 및 보안성 등을 평가 · 인증하여 클라우드 서비스에 대한 시장 수요의 확대를 도모하고자 한다.

Ⅱ. 클라우드 서비스 개념 및 서비스 제공유형

1. 클라우드 서비스 개념

클라우드(Cloud)라는 용어는 사용자가 필요한 작업을 제시하면 네트워크상의 어디엔가 이에 필요한 컴퓨팅 자원이 할당되어 작업을 실행할 수 있는 것을 의미한다. 이러한 개념에 기반한 클라우드 서비스는 사용자에게 언제 어디서나 인터넷 접속만으로 컴퓨팅 환경을 제공하는 주문형 IT 서비스로 정의할 수 있다. 인터넷상에서 서로 다른 물리적인 위치에 존재하는 각종 컴퓨터 자원들을 가상화 기술로 통합하여 사용자에게 언제 어디서나 필요한 양만큼 편리하고 저렴하게 사용할 수 있는 환경을 제공하는 기술을 말한다(민옥기 외, 2009a).

클라우드 서비스는 가상화와 분산처리 기술을 기반으로 IT 자원이 통합된 클라우드를 통해 사용자에게 소프트웨어, 플랫폼, 인프라 등의 IT 서비스를 제공하는 것이다. 클라우드 컴퓨팅 서비스가 도입되면서 기업의 IT 자원에 대한 인식이 막대한 투자를 통한 '소유'에서 개념에서 '임대(Rental)'로 변화하고 있다. 기업들은 '구매'를 통해 시스템 등을 보유 및 유지 · 보수하는 것이 아니라, 필요에 따라 필요한 시스템을 빌려 쓰고 사용량을 기준으로 이용요금을 지불하는 것으로 인식이 변화하고 있는 것이다.

기존의 IT환경에서 기업들은 각종 서버 및 PC 등 관리해야 할 IT자원의 수가 증가함에 따라, 이에 대한 유지 · 보수 및 관리의 문제가 점점 커지게 되었다. 뿐만 아니라, 모든 시스템들이 통합전산망으로 연결되어있어, 기업의 내부 인프라의 복잡성이 증가됨에 따라 수행해야 하는 유지 보수비가 기하급수적으로 증가하게 되어, 비용절감 대책이 대두되었다.

이에 따라 기업들은 네트워크의 복잡성 및 사용단말의 증가로 인해 급증하는 전력수요와 데이터양을 수용하는데 있어서의 한계를 체감하게 되었다. 또한 기업의 비즈니스 규모와 형태가 복잡하게 발전하면서, 기존 IT 시스템과 신규로 도입되는 시스템과의 연계 필요성이 증가하고 있었기 때문에, 내부적으로 메인프레임이 가지고 있던 장점과 분산 컴퓨팅의 장점을 유지하면서, 외부적으로는 하나의 시스템처럼 동작하는 클라우드 컴퓨팅이 필요하게 되었다. 또한 외부환경으로는 전세계적 경기불황의 여파로 기업의 비용절감 이슈가 대두되면서, 이를 극복하기 위한 전략적 방안으로 클라우드 컴퓨팅이 등장하기 시작하였다.

2. 클라우드 서비스 제공 유형

기존에 존재하고 있던 다양한 유형의 IT자원들의 이용방식을 새롭게 혁신한 만큼 클라우드 서비스는 다양한 유형으로 제공되고 있다. 클라우드 컴퓨팅 서비스는 제공되는 형태에 따라 대표적으로 세 가지로 분류할 수 있다(김형곤 외, 2010; 민옥기 외, 2009b; 이주영, 2010).

첫째, 응용소프트웨어 서비스 (SaaS, Software as a Service)로써 표준화된 솔루션을 표준적인 방법으로 네트워크를 통해 제공받아 손쉽게 업무에 적용이 가능한 서비스이며, 가장 일반적인 유형의 클라우드 컴퓨팅 서비스로 인식되고 있다. 하나의 가상적인 서버와 솔루션을 모든 사용자가 사용할 수 있어, 기존의 인프라가 가지고 있던 약간의 공간적 제약까지도 해결 할 수 있다.

둘째, 플랫폼 서비스 (PaaS, Platform as a Service)는 개발환경에 최적화 되도록 한 것으로써, 기업이 큰 비용 부담 없이 개발 및 업무에 활용 할 수 있다. 개발자는 클라우드 컴퓨팅의 가상화된 하드웨어와 소프트웨어를 언제든지 제공 받을 수 있다. 플랫폼서비스는 어플리케이션 디자인, 개발, 테스트 등 개발 프로세스와 관련된 환경의 제공이 가능하다.

셋째, 인프라 서비스 (IaaS, Infrastructure as a Service)는 기업이 속해 있는 산업환경, 기업규모, 비즈니스 모델로 인해 기존의 표준화된 솔루션을 도입하지 못하는 기업에 제공할 수 있는 서비스 유형이다. 이 서비스는 가상화된 인프라 환경만을 사용할 수 있게 제공해 주며, 직접 서버에서 서비스를 구성하듯이 가상 서버에 서비스를 구성하고 관리하게 함으로써 기업이 가지는 기본 인프라에 부담을 덜어주는 효과가 있다.

이상의 클라우드 서비스의 해외사례는 〈표 1〉과 같은데, 기존의 기업들은 업무용으로 운영체제(OS) 및 문서프로그램, 스프레드 쉬트 등의 다양한 소프트웨어를 구매한 후, 개인화된 단말(PC)에 저장하고

〈표 1〉 해외기업의 서비스 사례

대분류	중분류	사례
SaaS	응용 소프트웨어 서비스	GoogleApps, Salesforce.com Apps, Apple MobileMe, Nokia OVI, IBM Bluehouse
	웹 기반 서비스	HP Snapfish, MS Office Live, HP Magcloud
	응용 소프트웨어 컴포넌트 서비스	Amazon FPS(Flexible Payments Service) API, Google MAP API, Google Calendar APIs, Yahoo! Maps API
PaaS	엔터프라이즈 플랫폼 서비스	GigaSpaces, Oracle SaaS platform
	호스티드 플랫폼 서비스	Google AppEngine, Salesforce Force.com, MS Azure, Sun Caroline, Cloudera
IaaS	데이터베이스 클라우드	Amazon SimpleDB, Google Base, MS SDS
	서비스 미들웨어 클라우드 서비스	Amazon SQS(Simple Queue Service)
	스토리지 클라우드 서비스	Amazon S3(Simple Storage Service), EMC Mozy/Atmos, Rackspace CloudFiles
	컴퓨터 클라우드 서비스	Amazon EC2(Elastic Compute Cloud), Saw is Cloud Compute

출처: 민옥기 외, 훤히 보이는 클라우드 컴퓨팅, 전자신문사, 2009

〈표 2〉 해외기업의 도입사례

기업명	도입시스템	서비스 현황
Google	구글 앱스	Gmail, 구글토크, 구글 캘린더, 구글 문서관리
MS	Window Azure	클라우드용 운영체제(서비스 호스팅 및 관리, 로우레벨 스토리지 및 컴퓨팅, 네트워킹)
Amazon	S3, EC2	가상저장장치(S3), 가상서버(EC2)
AT&T	Synaptic Storage as a Service	온라인 Storage
BT(영국)	BT Virtual Data Centre(VDC)	기업의 통합 커뮤니케이션, 모바일 환경, 데이터 센터 등 인프라
FT(프랑스)	Flexible Computing	기업 비즈니스 아웃소싱
NTT(일본)	VANADIS SaaS	Platform Application 개발환경 제공
	그린데이터센터	서버, 스토리지, OS 등을 필요에 따라 가상서버 단위로 제공

주기적 업데이트를 수행해야 했던 불편함과 비용 및 유지보수의 애로사항을 클라우드 서비스를 통해 해결할 수 있다.

해외에서는 클라우드 컴퓨팅 서비스의 사업성 및 성장가능성이 입증됨에 따라 구글, MS, AT&T, Amazon, IBM, NEC 등의 수많은 기업들이 경쟁적으로 관련시장에 참여하고 있다. 특히 구글과 MS는 IT패러다임이 효율성과 확장성을 지향하는 클라우드 컴퓨팅 환경으로 전환되는 것에 대비하기 위해 대규모 투자를 진행하고 있다.

국내의 경우는 공공기관 및 여러 산업에서 응용이 가능한 형태로 도입했으며, 추진을 검토중인 기업들이 점차적으로 증가하고 있는 추세이다. 또한 앞서 언급한바와 같이 범정부 차원의 클라우드 컴퓨팅 활성화 계획을 공표하고 클라우드 컴퓨팅 서비스의 도입과 확산방안을 강구하고 있다. 행정안전부는 정부통합 전산센터 및 국가 정보화 사업 시스템 개발에 필요한 환경, 지역정보 통합센터에 클라우드 컴퓨팅 서비스를 도입키로 하였다. 지식경제부의 경우는 가상 데스트탑의 국산 원천기술 확보 및 3스크린 동기화 서비스를 가능하게 하는 퍼스널 클라우드 컴퓨팅 시범사업과 클라우드 기반 그린 PC 시스템 시범사업

〈표 3〉 국내기업의 도입사례

구분		도입시스템	설명
정부	교과부	SBC(Server Based Computing)	Thin Client 단말을 통한 가상서버에서 가상 PC 구동
공기업	한국전력	클라우드 PC 파일럿 테스트 과제	
금융	우리금융그룹	커뮤니티 클라우드	그룹의 IT인프라 pool을 구성한 후, 가상화 기술을 통해 은행 · 증권 · 보험 등 계열사별로 분리운영
건설	동부건설	IT자원의 가상화	서버와 데스크탑 부문 가상화
통신	온세텔레콤	클라우드 컴퓨팅 컨택센터 서비스	클라우드 컴퓨팅 기반의 콜센터

〈표 4〉 국내에서 제공중인 서비스 현황

기업명	서비스명	개시일자	서비스 소개
NHN	N드라이브	2010.5	개인화된 모바일 웹하드
KT	U 클라우드	2010.6	컴퓨터에 저장되어 있는 데이터를 Ucloud 서버에 안전하게 백업, 언제 어디서든 빠르게 데이터를 열람하거나 복원할 수 있는 백업서비스
LG U+	U+ 박스	2010.7	고객이 PC나 스마트폰 등을 이용해 업로드한 컨텐츠를 스마트폰은 물론 다양한 인터넷 기기를 통해 어디서나 실시간으로 감상할 수 있는 멀티미디어 NScreen 서비스

도 추진중이다. 방송통신위원회는 IPTV부문에 클라우드 컴퓨팅 서비스 기술을 접목한 시범사업을 추진중이다(김형곤 외, 2010).

현재 국내에서 기업들이 상용중인 클라우드 컴퓨팅 서비스는 대부분이 가상화를 이용한 storage 서비스이다. 대표적인 기업으로는 통신기업인 LG U+, KT와 IT기업인 네이버가 선도적으로 서비스를 제공하고 있다.

3. 클라우드 서비스의 문제점

경기 침체로 기업에서는 비용을 줄일 수 있는 대안인 클라우드 서비스는 최소한의 초기 비용으로 서비스를 얻을 수 있고 서비스 구축이 기존의 방식에 비해 빠르며 유지관리비가 저렴하다는 장점이 있다. 그럼에도 불구하고 클라우드 서비스는 보안성 및 가용성과 같은 문제점을 포함하고 있는데 이를 살펴보면 다음과 같다.

- 보안 문제: IT 시장에서 새로운 기술이 도입될 때마다 가장 문제가 되는 것이 보안 문제이다. 클라우드 서비스 역시 이러한 문제를 피해 갈 수 없었다. 클라우드 공급자는 보안 문제를 해결하기 위해 특화된 기술(예, 암호화), 프로세스(예, 검증 가능성) 및 검증 표준(예, PCI 및 ISO 27001) 등을 사용하고 있음에도 불구하고 현재로써 아주 중요한 데이터와 중대한 프로세스에는 클라우드 서비스를 사용할 가능성은 낮다.
- 가용성 문제: 기업에서는 클라우드 서비스를 받기 위해서는 인터넷을 필히 이용해야 한다. 하지만, 인터넷 액세스가 용이하지 않거나 서비스 공급자의 시스템이 고장을 일으킬 경우 서비스를 받을 수 없게 된다. 기존의 ASP 공급자 입장에서 고객에게 확신을 심어주기 위해 사용하는 방법 중의 하나는 위약조항을 포함하는 계약서를 만들고는 있지만 클라우드 서비스를 확산하기 위해 근본적으로 언제 어디에서나 서비스를 받을 수 있는 시스템 구축에 좀 더 많은 노력을 기울여야 한다.
- 성능 문제: 인터넷 스피드 및 대역폭은 클라우드 서비스의 성능과 밀접한 관련이 있다. 얼마나 빠르게 얼마나 많은 데이터를 전송 시킬 수 있는지도 서비스의 성능을 평가할 수 있는 주요 지표가 되고 있다.

추가적으로 클라우드 서비스 사용자 입장과 공급자 입장에서의 문제점을 살펴보면 다음과 같은 클라우드 서비스에서의 사용자 및 공급자 보호 문제가 대두되는데, 클라우드 서비스의 활성화를 위해서는 다음과 같은 문제들이 해결되어야 한다.

1) 클라우드 서비스에서의 사용자 보호 문제

클라우드 서비스의 많은 장점에도 불구하고, 사용

자들은 여러 가지 측면에서 불안감을 가지고 있다. 특히 클라우드 서비스에 문제가 발생할 경우 사용자가 얼마나 보호될 수 있는가에 대한 우려가 매우 크다. 최근 구글 Gmail의 접속 장애, 트위터의 사내 자료 유출, 아마존의 서비스 중단 등으로 사용자의 불안감이 커지고 있기 때문에 클라우드 컴퓨팅 서비스에 대한 안정성과 신뢰성 확보에 대한 요구가 갈수록 높아지고 있는데, 클라우드 서비스에서의 사용자 보호문제로는 다음과 같은 점이 고려되어야 한다.

- 사업자 파산: 사업자가 파산하는 경우, 클라우드 서비스의 사용자 입장에서는 손해가 막대할 수밖에 없다. 사업자가 파산하는 경우, 기존에 서비스 이용자는 안정적으로 서비스를 이용하지 못해 지금까지 서비스를 이용해 진행하던 업무가 정지되게 되며 또한 데이터가 훼손되거나 손실되는 경우, 지금까지 클라우드 서비스에 보유하고 있었던 정보들이나 데이터를 잃게 된다. 만일 서비스 제공자의 파산 이후 또 다른 서비스 제공자를 찾는다고 하여도 기존에 제공받던 서비스를 동일하게 제공받을 수 있는지, 업체들 간 시스템 부분에서 호환이 가능한지의 문제들이 발생할 수 있다. 해외에서는 사업자 파산에 따른 피해 축소를 위해 대부분의 기술자료 임치제도를 활용하고 있는데, 국내에서도 클라우드 서비스를 위한 임치제도의 실행이 필요하다.
- 서비스 중단 및 장애: 클라우드 컴퓨팅 서비스가 중단되거나 장애가 발생하는 경우에도 사용자는 서비스 공급자가 파산하는 경우와 유사한 피해를 입게 된다. 특히 클라우드 서비스는 인터넷과 마찬가지로 각각의 서비스와 컴퓨터가 네트워크로 연결되어 있어 바이러스 감염이나 해킹 등의 침해사고 등에 취약하여 언제라도 서비스에 장애가 발생할 수 있는 가능성이 있다. 게다가 클라우드 컴퓨팅 서비스는 사용자의 정보를 서비스 제공자의 서버에 저장해놓는 형태로 제공되기 때문에 서비스 장애에 따른 정보 유실이나 손실의 규모는 여타 다른 인터넷 기반 서비스보다 훨씬 크다. 이를 예방하기 위해서는 클라우드 서비스 사업자의 이용 약관규정에서 서비스 장애에 따른 손해배상의 범위를 명확히 규정하는 것이 필요하며 손해배상의 면책 규정을 일방적인 사업자 입장만을 고려하는 것이 아니라 서비스 이용자의 입장을 함께 고려함으로써 서비스 이용자들이 서비스를 이용하는 데에 있어서 가지는 불안감을 해소해 줄 수 있어야 한다.
- 사용자의 정보보호: 클라우드 서비스의 핵심 기술은 가상화이다. 따라서 사용자가 저장해 놓은 데이터의 위치 파악이 어려울 뿐만 아니라 외부 공격에 취약하고 관리자가 권한을 오남용하는 경우 민감한 개인정보의 유출 위험이 크다. 그럼에도 불구하고 현행법에 의하면 사용자의 개인정보 보호에 예외가 되는 법조항들이 다수 존재하며 정보 유출로 인하여 개인이 큰 피해를 입은 경우에도 현행범으로는 서비스 제공자에게 벌금을 부과할 뿐 구체적으로 피해자에 대한 보상이 명시되어 있지 않아 클라우드 서비스의 사용자들에게 정보보호에 관한 불안감을 해소시켜 주기에는 미흡하다.
- 플랫폼의 독립성 강화: 플랫폼의 독립성이란 플랫폼이 운영체제 또는 단말기에 상관없이 작업을 수행할 수 있는 것을 의미한다. 클라우드 서비스에서는 플랫폼의 독립성 강화가 무엇보다 중요하다. 클라우드 서비스 사업자가 갑작스럽게 파산을 하거나 사업을 폐지하는 경우, 기존에 해당 서비스를 이용하던 사용자들은 다른 서비스로의 전환이 불가피한데, 이 경우 플랫폼이 독립적인 경우, 사용자들은 별다른 전환비용 없이 손쉽게 다른 서비스로 옮겨갈 수 있게 된다. 따라서 클라우드 서비스에 있어서 플랫폼의 독립성 강화는 사용자들의 권리와 정보를 보호해 줄

수 있는 제도적 장치의 연장선이라 할 수 있다.

2) 클라우드 서비스에서의 공급자 지원 및 보호 문제

공급자의 측면에서 볼 때 사용자가 불안감을 느끼는 사항들은 모두 공급자에게도 불안감으로 작용될 수 있다. 공급자 측면에서 바라본 사용자의 불안감은 크게 사용자 정보의 보안성과 안전성으로 나눌 수 있다. 공급자의 입장에서는 사용자의 정보의 보안 유지와 사용자 정보의 손실을 방지하기 위해 안전성을 유지되어야 하지만 이에 대한 대책은 현재로서는 미비한 수준이다. 추가적으로 클라우드 서비스는 시작된 지 얼마 되지 않아 이에 대한 이해도나 지원이 빈약하며 인적자원이나 법 · 제도 측면에서의 지원이 미흡한 점도 공급자들이 클라우드 서비스를 공급하는데 문제점이 될 수 있다.

- 사업의 보안성 확보: 클라우드 컴퓨팅의 문제점으로 가장 많이 지적되는 것은 서비스의 보안성이다. 사용자 측면에서 언급한 대로 해킹 등의 외부 공격과 관리자의 오남용 문제로 인해 사용자들은 보안성에 대해 우려할 수 있다. 사용자의 우려는 곧 공급자의 우려로 번질 수 있는데, 사용자의 정보에 대한 보안성을 확보하지 않은 상태에서 서비스를 시행하다가 보안 문제로 인해 사용자가 피해를 입는다면 공급자 역시 이에 대한 손해배상을 준비해야 한다. 하지만 현재 사용자에 대한 배상 범위와 액수도 정확하지 않아 많은 문제가 발생할 것으로 예상된다.
  때문에 공급자는 서비스 공급에 있어서 충분한 보안 대책을 세우고 클라우드 서비스에 맞는 보안 요소를 보장할 수 있는 법규를 만들어야 한다. 이 외에도 클라우드 컴퓨팅으로 인해 새로 나타나는 기술들인 가상화 서버에 대한 보안 항목을 추가하거나 기존 체계에서 소홀히 다뤄진 데이터에 대한 복구 또는 임치 등을 규정하는 항목 또한 추가되거나 새로이 클라우드 서비스의 인증체제를 만들어 나갈 필요성이 있다.
- 상호 호환가능성을 통한 서비스 안정화: 공급자간의 호환성은 클라우드 서비스를 안정화 시킬 수 있다. 단기적인 시각으로 볼 때 호환성은 각 사업자간의 특성을 통합하여 이윤을 감소시킬 수 있다. 그리하여 현재 공급자간의 호환성에 대해서는 클라우드 서비스 산업에서 크게 이루어지지 않고 있다. 또한 이를 규정하는 법제도 또한 미흡하여 서비스를 안정화 하는데 있어서 많은 문제점을 야기하고 있다. 먼저 모든 사업자들이 상호호환성과 표준화를 통해 사고율을 낮추고 개념을 일관성 있게 정리하여 전체적인 시장의 크기를 넓힌 뒤에 각 공급자가 개별적인 사업 아이템을 들고 나와야 수익성을 확보할 수 있다.
- 공급자의 역량 강화: 공급자 측면에서 볼 때 정부나 민간 부분의 인력 지원, 조세 감면, 제도적 보완, 규제 완화 등의 직접적인 지원도 중요한 요소 중의 하나이다. 그러나 클라우드 서비스는 기술이 도입되어 실제로 서비스가 실시된 지 얼마 안 된 관계로 클라우드 서비스를 사용하는 기업에 대한 지원 제도가 미비합니다. 먼저 클라우드 서비스를 실행하는 기업에 대한 정의가 모호하며 지원에 대한 범위가 정해져 있지 않다. 이로 인해서 클라우드 서비스를 제공하는 기업의 경우 그 지원의 대상과 규모가 정확하지 않아 지원이 어려우므로 이에 대한 대책마련이 필요하다.
- 인증제도: 인증제도는 제품 및 기술의 효과를 보증하여 사용자가 신뢰를 갖고 사용할 수 있도록 하는 방식이다. 현재 클라우드 서비스가 도입된 지 얼마 되지 않은 상황에서 인증제도는 대다수의 클라우드 서비스에 대해 알지 못했던 사람들에게 신기술과 서비스에 대한 불안감을 줄여줄 수 있다. 이로 인해 공급자들은 사용자들의 신뢰를 얻어 좀 더 과감하게 기술과 서비스를 개발하여 클라우드 서비스 산업을 활성화시킬 수

있게 될 것이다.

이상에서 살펴본 바와 같이 클라우드 서비스 사용자나 공급자 모두를 위해서는 클라우드 서비스 인증제도의 마련이 필수적이라 하겠다. 클라우드 서비스 인증제도는 클라우드 서비스에서 발생할 수 있는 많은 문제점을 해결할 수 있고 사용자와 공급자간의 신뢰하고 안심할 수 있는 서비스 제공을 위한 핵심 요소라고 할 수 있다. 따라서 본 연구에서는 이러한 문제점을 해결하기 위한 클라우드 서비스 인증제도 수립을 위한 프레임워크를 제안하고자 한다.

Ⅲ. 클라우드 서비스 인증제도를 위한 프레임워크

1. 관련 인증제도 고찰

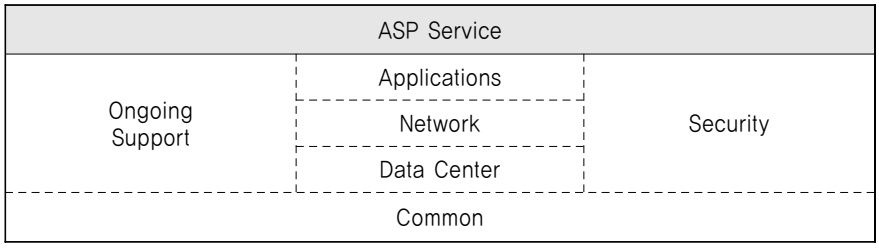
1) ASP 인증제도

ASP 인증제도는 ASP 솔루션 인증을 통하여 부적절한 솔루션에 의한 ASP 산업 전반에 대한 불안감을 해소하고 솔루션의 품질을 향상에 도움을 주고자 개발된 것으로 2006년부터 2년간 ASP 인증제도가 시행되었다.

ASP 인증 및 평가체계 개발을 위하여 ASP 서비스의 모든 ASP 계층을 다루도록 하였고, 공급자와 수요자 관점을 구분하였는데, ASP의 구성구조는 〈그림 1〉과 같다.

〈그림 1〉의 ASP 구성요소를 기반으로 ASP 인증영역을 구분하였는데 이는 〈표 5〉와 같다. 〈표 5〉에서 보는 바와 같이 ASP 인증영역을 어플리케이션 영역과 사업자(서비스 환경)영역으로 구분하였는데 이에 대한 정의는 다음과 같다 (서광규, 2006).

- 어플리케이션 인증 : ASP 어플리케이션의 구조, 유용성, 확장성, 성능, 보안 등에 대한 적정성 및 적합성의 객관적인 평가를 통해 어플리케이션의 선택기준을 제시하는 어플리케이션 인증
- 사업자(서비스 환경) 인증 : ASP 서비스 업체의 ASP 서비스에 대한 안정성, 신뢰성 기반의 서비스 제반 환경 인증으로서 서비스의 영속성 및 기능성에 대한 집중적 점검과 준비상태를 점검하



〈그림 1〉 ASP 구성 요소

〈표 5〉 ASP 인증영역

인증 영역	구성요소	정 의
애플리케이션	Application	요구되는 비즈니스 기능을 제공하는 기업용 애플리케이션
사업자 (서비스 환경)	Common	서비스 제공에 필요한 조직구성 및 현황
	Network	논리적, 물리적 접속환경
	Data Center	인프라스트럭처를 포함하는 H/W 등 서비스 제공능력
	Ongoing Support	시스템 유지보수, 컨설팅, SI, 교육, 핼프데스크 운영 등의 대고객 서비스

여 서비스를 제공할 수 있는 사업체의 서비스 환경 인증

2) TTA의 GS(S/W품질)인증제도

정부는 국내 S/W산업의 경쟁력 제고 차원에서 S/W의 품질 경쟁력 제고와 신뢰도 증진을 위해 한국정보통신기술협회(TTA)를 품질시험 · 인증기관으로 지정하여 엄격한 테스트와 공정한 시험 등 일련의 테스트절차를 거쳐 TTA의 품질인증을 받은 S/W 제품에 한해 GS(Good Software)마크를 부여하는 제도를 도입했다. 이 GS마크 제도는 시험 · 인증을 통한 품질향상 극대화와 정부공인 인증획득을 통한 제품의 신뢰도 증가, 국가적 차원의 지원을 통한 제품마케팅 지원 그리고 사전 검증된 고품질 S/W 공급으로 S/W유통을 활성화하는데 그 목적을 두고 있다(벤처기업협회, 2008).

현재 TTA에서 실시하고 있는 S/W 품질인증은 패키지, 모바일, 임베디드, 컴포넌트, e-Biz, Web-based S/W, Game, GIS, ERP, CRM, KMS, Groupware 및 보안 S/W 등 모든 분야의 소프트웨어를 대상으로 하고 있다. TTA는 국제 표준에 의거 2000년 8월부터는 한국형 평가모델을 개발하여 적용하고 있으며, 기능성, 신뢰성, 효율성, 사용성, 유지보수성, 이식성 등 다양한 기준에 근거해 테스트

〈표 6〉 녹색기술 인증대상

10대 분야	61개 중점분야
01. 신재생 에너지	01. 태양광 02. 연료전지 03. 에너지 저장 04. 풍력 05. IGCC 06. 청정연료 07. 해양에너지
02. 탄소저감	01. CCS 02. Non-CO2 온실가스처리 03. 원자력
03. 첨단수자원	01. 히트펌프 02. 자연친화적 하천관리 03. 담수플랜트 04. 자연재해대응 시스템 05. 통합수자원관리 06. 수계수질평가 /관리 07. (해)수처리 08. 고효율 농업용수 09. 고도 수처리
04. 그린IT	01. LED 02. 시스템 반도체 03. 차세대 디스플레이 04. 그린SW & 솔루션 05. 그린컴퓨팅 06. 그린 임베디드 SW 07. 차세대 센서 네트워크 08. Digital 선박 09. 스마트그리드 10. 그린 방송통신
05. 그린차량	01. 그린카 02. 저공해 고효율 차량 03. 그린농기계 04. Wise Ship 05. 첨단 철도 06. 그린자전거
06. 첨단그린 주택 · 도시	01. U-City 02. ITS(지능형 교통시스템) 03. GIS(공간정보) 04. 저에너지 친환경주택
07. 신소재	01. 초경량 마그네슘 소재 02. Ionic Liquid 소재 03. 나노탄소 융합소재 04. 기능성 나노필름 05. 농산자원유래 천연소재 06. 친환경 농자재 07. 차세대 센서 네트워크
08. 청정생산	01. 국제환경규제대응 02. 무오염생산 03. 자원순환
09. 첨단그린 주택 · 도시	01. 생태환경변화 대응 02. 생물자원 03. 저투입생산 04. 첨단자동화 시스템 05. 식품생산 06. 안전유통
10. 첨단그린 주택 · 도시	01. 기후변화예측 및 모델링 02. 기후변화 영향 평가 및 적응 03. 폐기물 및 폐자원 04. 유기성 부산물 자원화 05. 친환경제품 06. 생태계 보전 및 복원 07. 유해성 물질 모니터링 및 환경정화

출처: http://www.greencertif.or.kr/

하고 있다. 또한 2002년 7월부터는 세계적인 S/W 품질테스트 인증기관인 미국의 VeriTest사와 MOU 체결을 통해 국제 시험 · 인증 서비스를 제공하고 있다.

3) 녹색 인증제도

녹색인증은 정부의 저탄소 녹색정책의 일환으로 녹색투자 지원 대상 및 범위를 명확히 규정하고, 투자를 집중하고자 녹색기술 또는 녹색사업이 유망 녹색분야인지 여부를 확인하여 인증을 부여하는 제도이다 (한국산업기술진흥원, 2010).

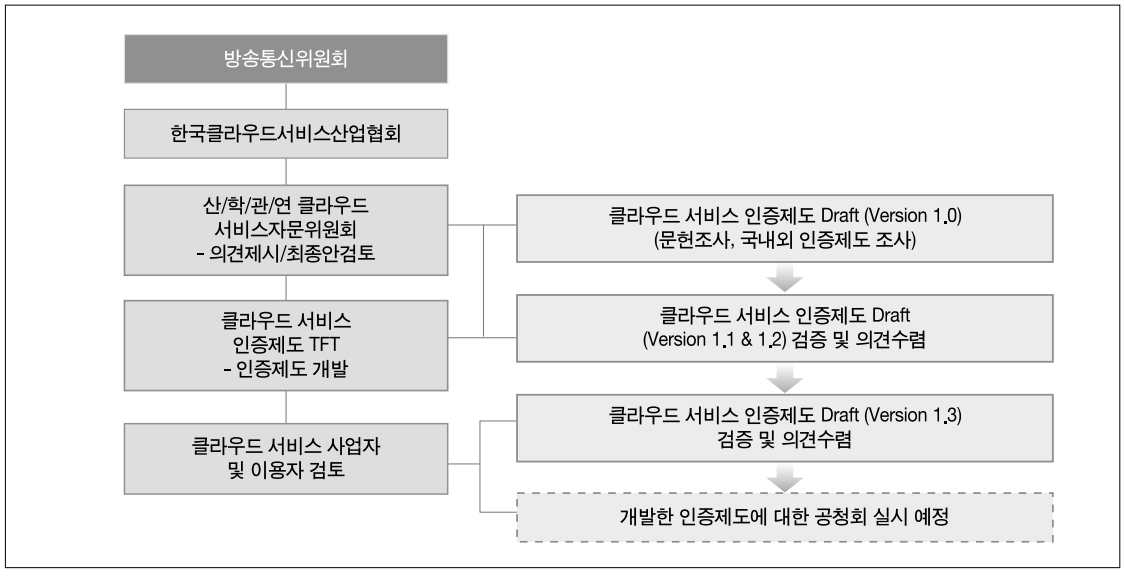
녹색인증제의 도입배경은 자원 및 환경위기를 극복하고 신국가발전 기반으로 저탄소 녹색성장을 지향하며 녹색산업에 투자에 집중하기 위하여 도입되어 2010년 4월부터 시행되고 있다.

녹색인증 대상은 녹색기술, 녹색사업 및 녹색전문기업확인으로 이루어져 있는데, 녹색기술 인증대상 분야는 그린에너지(2009. 2월), 녹색기술(2009. 5월), 신성장동력(2009. 5월) 등에서 제시된 기술범주를 감안하여, 10대 분야, 61개 중점분야 중심으로 세부기술 및 핵심(요소)기술 선정하였고 각 핵심(요소)기술별로 국내외 기술동향 분석, 전문가 자문을 통해 세계적으로 도입기 또는 성장기에 위치한 수준의 기술 규격을 제시하였다.

〈표 6〉은 녹색기술 인증대상 (10대 분야 및 61개 중점분야)을 나타낸 것으로, 특히 04. 그린 IT 분야의 일부 중점분야는 클라우드 컴퓨팅과도 연관이 높은 항목들을 포함하고 있다.

2. 클라우드 서비스 인증제도 개관

먼저 클라우드 서비스 인증제도 수립을 위한 프레임워크를 개발하기 위해 진행한 연구절차는 〈그림 2〉와 같다. 본 연구는 방송통신위원회 주관으로 한국클라우드서비스협회에서 산 · 학 · 관 · 연의 클라우드 서비스 및 관련 법 · 제도 전문가들로 구성된 자문위원회를 구성하였다. 자문위원회를 중심으로 클라우드 서비스 인증제도의 프레임워크 개발을 위한 TFT가 구성되어 클라우드 서비스 인증제도의 프레임워크를 위한 초안을 개발하였다. 개발한 초안은 2차에



〈그림 2〉 클라우드 서비스 인증제도 개발 단계 및 검증절차

걸친 자문위원회의 회의를 통해 개발 내용을 토의하였고, 개발 내용의 타당성을 검증하였다. 2차에 걸친 회의 후 작성된 인증제도의 draft는 국내 유·무선 통신사를 비롯하여 클라우드 서비스를 제공하고 있는 업계 전문가들을 대상을 설명회를 갖고 개발 내용을 검토하였다. 설명회의 주요 내용은 사업자 입장에서 인증제도의 타당성과 수용여부를 토의하였고, 개발한 draft의 수용성과 타당성 모두를 검증받았다. 추가적으로 클라우드 서비스 이용자 입장에서의 인증제도의 draft를 검증받기 위한 대표 이용자들을 선정하여 이용자회의도 진행하여 개발안의 수용성과 타당성 모두를 역시 검증받았다. 현재에는 최종 개발된 클라우드 서비스 인증제도 수립을 위한 프레임워크에 대한 공청회를 준비하고 있으며, 빠른 시간 내에 개발된 인증제도의 공청회가 진행될 것으로 기대한다.

클라우드 서비스의 인증대상으로는 국내 사업자가 신청 시점에 제공 중인 클라우드 서비스를 대상으로 인증 추진이 가능할 것으로 판단되나, 클라우드 서비스 중 IaaS 및 SaaS에 대해 인증을 먼저 실시하고, PaaS의 경우에는 아직까지 서비스 시장 내에서의 충분한 이해가 부족하고 제공되고 있는 서비스가 부족한 상황으로 향후 인증제 실시를 위한 여건 등 관련 동향을 파악하여 추후에 인증을 실시하는 것이 바람직해 보이므로, 본 연구에서는 PaaS 인증을 위한 심사항목 개발은 제외하기로 하며 이는 향후 연구과제로 남겨 두기로 한다.

클라우드 서비스 인증제도의 수립을 위한 프레임워크의 개발 내용을 간략하게 기술하면 다음과 같다. 먼저 클라우드 서비스 인증제도를 위해 기존의 수행해오던 인증제도들과 정부에서 제시한 정책과 지침 등(방송통신위원회, 2010; 정보통신부, 2000; 행정안전부, 2010)을 참고로 하되, 클라우드 서비스를 위해 적용된 세부 기술적인 요소 및 클라우드 서비스의 특징 등을 모두 고려하여 세부 심사영역 및 항목으로 개발하였다. 이를 위하여 본 연구에서는 클라우드 서비스의 라이프사이클을 통해 모든 클라우드 서비스 계층을 다루도록 하였고, 공급자와 수요자 관점을 모두 고려하였다. 라이프사이클은 기존의 IT 아웃소싱 방법론을 위한 기반자료인 국내 3대 아웃소싱 방법론(한국정보화진흥원, LG-EDS, 삼성 SDS)과 ORACLE사 등의 아웃소싱 도입방법론을 참조하였다. 또한 기반 기술 분석을 위해 해외기업/기관 및 국내기업/기관에서 제시한 클라우드 서비스 아키텍처를 참조하였고, 국내에서 시행된 ASP 인증제도(서광규, 2006)의 세부 연구결과 및 관련 인증제도의 내용도 참조하였다.

이를 통하여 도출된 클라우드 서비스의 인증내용은 클라우드 서비스 및 클라우드 서비스 사업자(2개 영역)에 걸쳐 평가를 실시하고, 영역별 일정 점수 이상을 획득하는 경우 서비스 인증하는 것으로 제안하였다. 클라우드 서비스 인증제도는 클라우드 서비스 인증(Cloud Service Certification)과 클라우드 서비스 사업자 인증(Cloud Service Provider Certification)으로 구분하여 실시될 수 있다.

클라우드 서비스 인증은 클라우드 서비스의 원활한 제공을 위해 반드시 갖추어야 할 필수 항목들을 도출하여 평가영역 및 세부평가항목을 도출하였다. 클라우드 서비스는 인터넷을 기반으로 서비스를 온 디맨드 방식으로 제공하고 과금하므로 이와 같은 특징을 포함한 특징들을 모두 고려하여 세부평가항목을 도출하였다. 평가영역과 평가항목은 이러한 클라우드 서비스의 특징과 기존의 IT 아웃소싱 방법론, 정부의 정책 및 지침, 그리고 ASP 인증제도 및 관련 인증제도를 종합·검토하여 도출하였고, 클라우드 서비스 자문위원회와 관련업계 전문가 등을 통하여 제안항목의 타당성을 검증하였다. 이 과정을 통하여 도출된 평가항목으로 구조 및 적합성, 가용성, 성능, 보안성 등을 클라우드 서비스 영역으로 평가하되, IaaS와 SaaS의 서비스 유형에 따라, 서비스의 특징을 반영하는 일부 요소를 달리하여 추가로 평가항목을 도출하였다. 클라우드 서비스 사업자 인증은

클라우드 서비스 제공자의 경영환경, 안정성 및 관리 운용성 등 서비스 제공 환경을 평가하기 위한 항목으로 클라우드 서비스 인증항목과 동일한 과정을 거쳐서 도출하였는데 도출된 항목을 IaaS 혹은 SaaS의 클라우드 서비스를 안전하고 지속적으로 서비스할 수 있는 제공업자인지를 평가하는 항목으로 도출하였고, 이의 타당성은 전문가집단을 통하여 검증하였다.

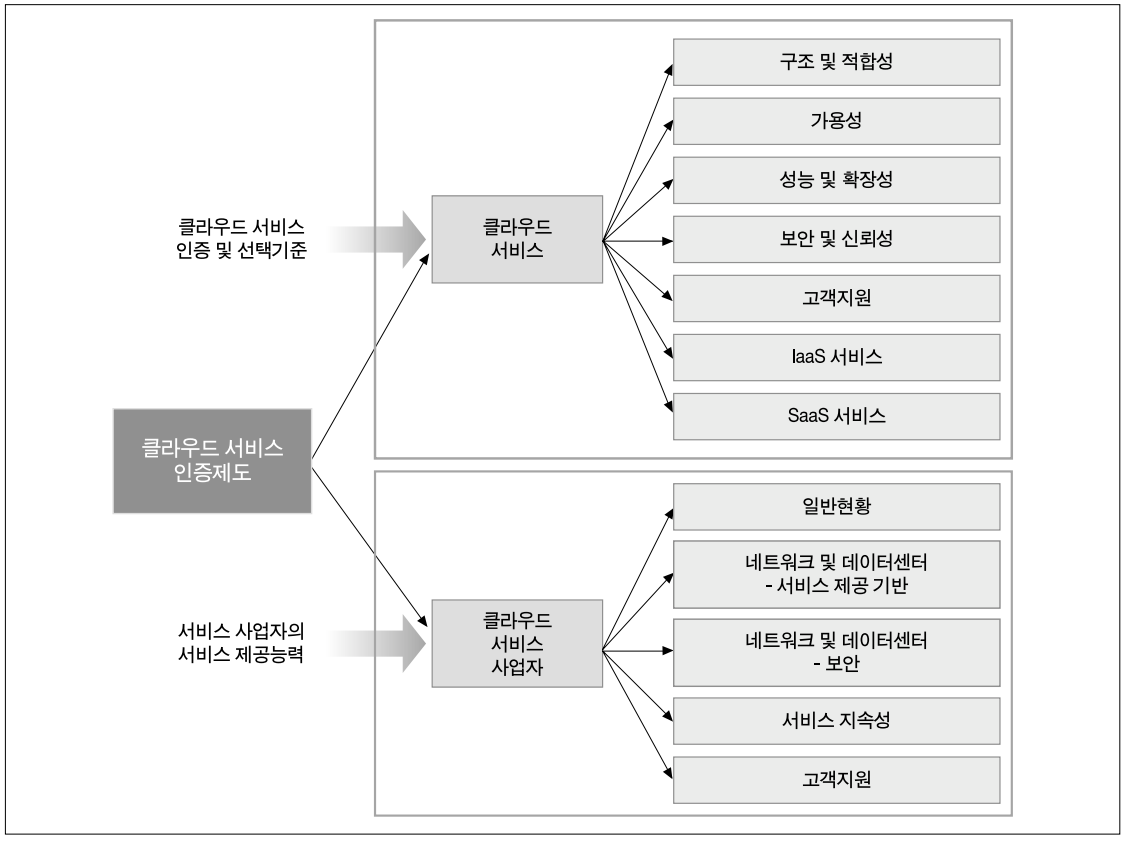
3. 클라우드 서비스 인증제도의 세부평가항목

클라우드 서비스 인증제도를 위해서는 '클라우드 서비스' 및 '클라우드 서비스 제공 사업자'의 2개 영역에 다하여 평가할 수 있는데, 클라우드 서비스는 구조검토 및 적합성, 가용성, 성능 · 확장성, 보안 · 신뢰성, 고객지원 등 5개 영역을 종합적으로 평가하되, 서비스별(IaaS와 SaaS) 추가 항목을 두어 평가기준을 차별화한다. 클라우드 사업자는 일반 현황, 네트워크/데이터센터(서비스제공 기반 및 보안), 서비스 지속성, 고객 지원 등 5개 영역을 종합적으로 평가하는데 최종 도출된 클라우드 서비스 인증범위 및 평가항목은 〈그림 3〉과 같고, 제안된 세부평가항목을 설명하면 다음과 같다.

1) 클라우드 서비스 공통평가 기준

(1) 구조검토 및 적합성

본 항목은 클라우드 서비스의 기능, 논리 구조,



〈그림 3〉 클라우드 서비스 인증범위 및 평가항목

물리 구조 등 클라우드 서비스 구조의 유용성과 적합성을 평가한다.

(2) 가용성

본 항목은 클라우드 서비스가 인터넷을 통하여 다수의 사용자에게 제공되는지 평가한다.

(3) 성능 및 확장성

본 항목은 클라우드서비스의 성능, 안정성 및 확장성을 유지 · 개선하기 위한 서비스 제공자의 활동이 이루어지고 있는지를 평가한다.

(4) 보안 및 신뢰성

본 항목은 클라우드 서비스 이용자의 정보를 보호하기 위한 보안 정책, 보안 기술 등을 평가한다.

(5) 고객지원

본 항목은 이용자 지향적인 클라우드 서비스를 위하여 서비스 정책, 고객 지원 프로세스(모니터링, 유지 보수, 가이드 제공 등)를 수립하여 지원하고 있는지를 평가한다.

〈표 7〉 구조검토 및 적합성 심사항목

심사영역	심사항목		비고(심사자료)
구조검토 / 적합성 (3개항목)	1.1	이용자가 클라우드 서비스의 기능을 쉽게 이해할 수 있고 적용 분야에 활용할 수 있는 명확하고 상세한 설명서 존재유무	서비스 상세 설명서 또는 백서
	1.2	이용자가 클라우드 서비스의 논리 구조를 쉽게 이해하고, 적용 분야에 활용할 수 있는 명확하고 상세한 설명서 존재 유무	인프라스트럭처의 논리적 구성도
	1.3	이용자가 클라우드 서비스의 물리적 구조를 쉽게 이해하고, 적용 분야에 활용할 수 있는 명확하고 상세한 설명서 존재 유무	인프라스트럭처의 물리적 구성도

〈표 8〉 가용성 심사항목

심사영역	심사항목		비고(심사자료)
가용성 (3개항목)	2.1	동시에 다수의 이용자의 클라우드 서비스에 접속 지원 여부	기술구현자료 인프라 운용검증
	2.2	이용자가 다양한 접속환경(웹, 모바일 등)을 통한 접속 지원 여부	인프라 운용검증
	2.3	이용자의 클라우드서비스 상시 이용성 지원 여부	인프라스트럭처 가용성 테스트 보고서

〈표 9〉 성능 및 확장성 심사항목

심사영역	심사항목		비고(심사자료)
성능/확장성 (4개항목)	3.1	클라우드 서비스의 성능을 유지하기 위한 주기적 테스트 시행 여부	성능 테스트 보고서
	3.2	클라우드 서비스의 안정성을 유지하기 위해 주기적으로 테스트 시행 여부	안정성 테스트 보고서
	3.3	클라우드 서비스의 수요(이용자 등)가 증가할 경우, 서비스의 성능을 안정적으로 유지할 수 있는 방안 유무	인프라스트럭처 기술지침서 성능테스트보고서
	3.4	클라우드 서비스의 이용자가 증가할 경우 Scalability 확보 여부	인프라스트럭처 기술지침서

〈표 10〉 보안 및 신뢰성 심사항목

심사영역	심사항목		비고(심사자료)
보안 / 신뢰성 (9개항목)	4.1	클라우드서비스 제공에 따른 보안 정책과 보안 채널을 보유여부	보안정책 및 채널 관련 문서
	4.2	인가받지 않은 이용자의 접근제어 적용 여부	접근제어 기술문서/ 어플리케이션 기술지침서/ACL
	4.3	이용자를 검증하기 위한 통합 인증 절차를 확보여부	인프라스트럭처 기술지침서 single sign - on 제공 여부
	4.4	클라우드서비스 이용자 데이터의 기밀성 및 무결성을 확보 여부	인프라스트럭처 기술지침서
	4.5	클라우드서비스 이용자 보호를 위해 방화벽을 도입여부	인프라스트럭처 기술지침서
	4.6	인가받지 않은 이용자의 접근을 방지하고 추적하기 위해 로그 파일 분석을 통한 감시 · 추적 등의 관리 대책을 도입여부	인프라스트럭처 기술지침서/ 로그분석 보고서
	4.7	메시지의 송수신 레벨(전송 레벨 제외)에서 부인 방지 기능을 제공 여부	인프라스트럭처 기술지침서
	4.8	메시지의 송수신 레벨(전송 레벨 제외)에서 개인 프라이버시 보호 기능 제공 여부	인프라스트럭처 기술지침서
	4.9	서비스 및 데이터에 대한 장애 대책 유무	인프라스트럭처 기술지침서 장애대책 관리 지침서

〈표 11〉 고객지원 심사항목

심사영역	심사항목		비고(심사자료)
고객지원 (4개항목)	5.1	클라우드 서비스 수준을 유지하기 위한 서비스 정책을 수립 및 시행여부	SLA/인프라 기술지원 문서
	5.2	클라우드 서비스에 문제가 발생한 경우, 이용자를 지원하기 위한 프로세스가 존재유무	인프라 기술지원 문서
	5.3	클라우드 서비스 이용자의 기술적 문제를 해결하기 위한 기술지원 문서를 보유 및 시행 여부	인프라 기술지원 문서
	5.4	클라우드서비스 제공 과정에서 서비스의 장애 등을 파악하기 위한 모니터링 기술 및 시스템을 보유 및 시행 여부	모니터링 보고서

2) IaaS 및 SaaS 서비스 평가 기준

(1) IaaS의 구조검토 및 적합성

본 항목은 IaaS 서비스를 제공하기 위한 가상화 기술 등 클라우드 관련 기술 적용여부를 평가한다.

(2) SaaS의 구조검토 및 적합성

본 항목은 어플리케이션 기능, 성숙도, 데이터

〈표 12〉 IaaS의 구조검토 및 적합성 심사항목

심사영역	심사항목		비고(심사자료)
구조검토 / 적합성 (1개항목)	1.1	IaaS 서비스를 제공하기 위하여 가상화 기술, 분산컴퓨팅 기술, 시스템 관리 기술 또는 미터링 기술 등 클라우드 서비스 관련 기술의 적용여부	기술적용문서

〈표 13〉 SaaS의 구조검토 및 적합성 심사항목

심사영역	심사항목		비고(심사자료)
구조검토 / 적합성 (4개항목)	2.1	어플리케이션 기능에 대해 이용자가 쉽게 이해하고 사용할 수 있는 명확하고 상세한 설명서가 존재 유무	어플리케이션 상세설명서/ 백서
	2.2	어플리케이션의 적용된 기술의 성숙도 모델 (Level) 설명서의 존재 유무	관련문서 점검
	2.3	SaaS 서비스의 데이터 전송시 호환성을 지원여부	인프라 운용검증
	2.4	SaaS 서비스의 데이터 간섭유무	서비스구조 기술문서

〈표 14〉 SaaS의 가용성 심사항목

심사영역	심사항목		비고(심사자료)
가용성 (2개항목)	3.1	SaaS 어플리케이션의 무결성 점검	어플리케이션 무결성테스트 보고서
	3.2	총 사용시간과 접근 가능시간 점검	총사용시간과 서비스 접근가능 시간분석보고서

호환성 및 데이터 간섭 여부 등을 평가한다.

(3) SaaS의 가용성

본 항목은 어플리케이션의 무결성 및 접근 가능시간 점검 기능 등을 평가한다.

3) 클라우드 서비스 사업자 평가항목

(1) 일반현황

본 항목은 클라우드 서비스 사업자의 기업명, 설립년도, 대표자, 조직 · 인력 현황, 과금 체계 등 일반현황을 점검하여 클라우드서비스를 제공할 수 있는 경영 기반이 갖추어져 있는지를 평가한다.

(2) 네트워크 및 데이터센터 – 서비스 제공 기반

본 항목은 클라우드 서비스 사업자가 서비스를 제공하기 위해 하드웨어 및 소프트웨어 자원, 지원 · 협력 기관, 기술 인력의 전문성 등 서비스 제공을 위한 기반 시설의 확보 여부 및 유지 활동을 하고 있는지 평가한다.

(3) 네트워크/데이터센터 – 보안

본 항목은 클라우드 서비스 사업자가 이용자의 데이터 보호 및 침해 사고 방지 등을 위하여 물리적 · 기술적 · 관리적 차원에서 보안 계획을 수립하고 시행하는지를 평가한다.

〈표 15〉 일반현황 심사항목

심사영역	심사항목		비고(심사자료)
일반현황 (3개항목)	1.1	클라우드 사업자의 정체성/서비스 제공가능성 검증	사업자등록증 /위탁계약서/ 재무제표
	1.2	클라우드 사업자의 조직 및 인력 수준의 안정성 검증	조직도/인적자원 현황
	1.3	클라우드 사업자의 과금 체계는 합리성 평가	계약서, SLA, 이용약관

〈표 16〉 네트워크 및 데이터센터(서비스 제공 기반) 심사항목

심사영역	심사항목		비고(심사자료)
네트워크/ 데이터센터 (4개항목)	2.1	클라우드 서비스를 제공하기 위한 전산설비 확보 여부	호스팅 및 IDC 사용계약서
	2.2	클라우드 서비스를 제공하기 위해 서버, 스토리지, 네트워크 등 하드웨어 자원의 확보 여부	하드웨어 장비 목록표/ 점검 활동표
	2.3	클라우드 서비스를 제공하기 위해 모니터링 도구, 소프트웨어 등을 사용한 인프라스트럭처 점검 여부	인프라스트럭처 S/W 점검표/ 모니터링 보고서
	2.4	클라우드서비스를 지속적으로 제공하기 위한 기술 지원 인력 보유 유무	관련 직원의 자격증 및 경력증명서 또는 IDC 사용계약서

〈표 17〉 네트워크 및 데이터센터(보안) 심사항목

심사영역	심사항목		비고(심사자료)
보안 / 신뢰성 (7개항목)	3.1	클라우드 서비스의 이용자 보호를 위한 물리적 보안 대책을 수립 및 시행 여부	보안정책 문서/ 전산실무 지침서
	3.2	보유한 전산설비의 출입통제 실시여부	출입통제 관리 문서
	3.3	클라우드 서비스의 침해사고 방지를 위한 활동(방화벽, IDS 등) 실시 여부	보안 정기점검서
	3.4	클라우드 서비스의 보안취약 사항(바이러스 등)의 주기적 점검여부	보안취약점검 보고서
	3.5	서버(server)-클라이언트(client) 간 전송 정보를 보호하기 위한 데이터 암호화 지원여부	파일암호화 및 무결성 점검 문서
	3.6	클라우드 서비스 보안을 위해 네트워크 보안, 메일보안, 웹보안, 서버보안을 위한 보안항목(네트워크, 메일, 웹, 서버, 단말, 운용관리)에 대한 주기적으로 점검여부	시스템접근권한 명시문서/ 서비스 관련 SW점검표
	3.7	클라우드 서비스 보안을 위해 사업자의 주기적인 보고, 서버룸의 보안 운용관리 절차서, 기타 관리 및 운용방법 규정서, 갱신절차서 등 운용관리를 위한 주기적인 활동 여부	보안정책 문서/ 시스템운영지침서

〈표 18〉 서비스 지속성 심사항목

심사영역	심사항목		비고(심사자료)
서비스 지속성 (4개항목)	4.1	클라우드 서비스의 QoS를 유지하기 위해 서비스 이용 확대에 대응한 계획을 수립여부	성능 테스트 보고서
	4.2	서비스 중단 등 장애를 복구하기 위한 프로세스(장애내역 통지 등) 또는 대책 수립 및 시행여부	안정성 테스트 보고서
	4.3	클라우드 서비스의 성능을 유지하기 위해 기술. · 관리상의 내부 프로세스 확보여부	인프라스트럭처 기술지침서 성능테스트보고서
	4.4	클라우드 서비스를 지속적으로 제공하기 위해 백업, 싱크 및 복구 대책 수립 및 시행 여부	인프라스트럭처 기술지침서

〈표 19〉 고객지원 심사항목

심사영역	심사항목		비고(심사자료)
고객지원 (5개항목)	5.1	이용자를 지원하기 위해 표준 설치 계획, 서비스 구축 계획, 서비스 시행 계획 수립 및 시행여부	표준설치 계획서/서비스구축 계획서 /서비스 시행 사전계획서
	5.2	클라우드 서비스를 원활하게 사용할 수 있도록 서비스(환경, 애플리케이션이용방법, 접속방법, 서비스 범위 및 내용 등)에 대한 이용자 교육 실시여부	교육지원 활동표/교육자료
	5.3	서비스 사후 고객 지원을 위한 인력 및 조직을 확보 및 사후관리 시행 여부	고객사후 지원 · 관리 계획서
	5.4	이용자의 서비스 만족도를 유지 · 보증하기 위한 활동(서비스 만족도 평가, 서비스 수준의 계약서 명시 등)시행 여부	SLA
	5.5	서비스 중단 등 피해 발생 시 이용자에 대한 보상 대책(보상 규정, 보험가입 여부 등) 마련 및 시행여부	SLA/보험가입계약서

(4) 서비스 지속성

본 항목은 발생 가능한 클라우드 서비스 중단에 대해 서비스의 지속성을 담보하기 위한 기술적 관리적 조치 계획을 수립하고 시행하고 있는지를 평가한다.

(5) 고객지원

본 항목은 클라우드서비스의 체계적 수행과 고객 교육, 품질 보증, A/S 등 고객 지원을 위한 활동을 하고 있는지를 평가한다.

4. 클라우드 서비스 인증체계 및 인증제도 평가 방법

본 절에서는 클라우드 서비스의 인증체계 및 클라우드 서비스 인증제도의 평가방법을 간략하게 기술하기로 한다.

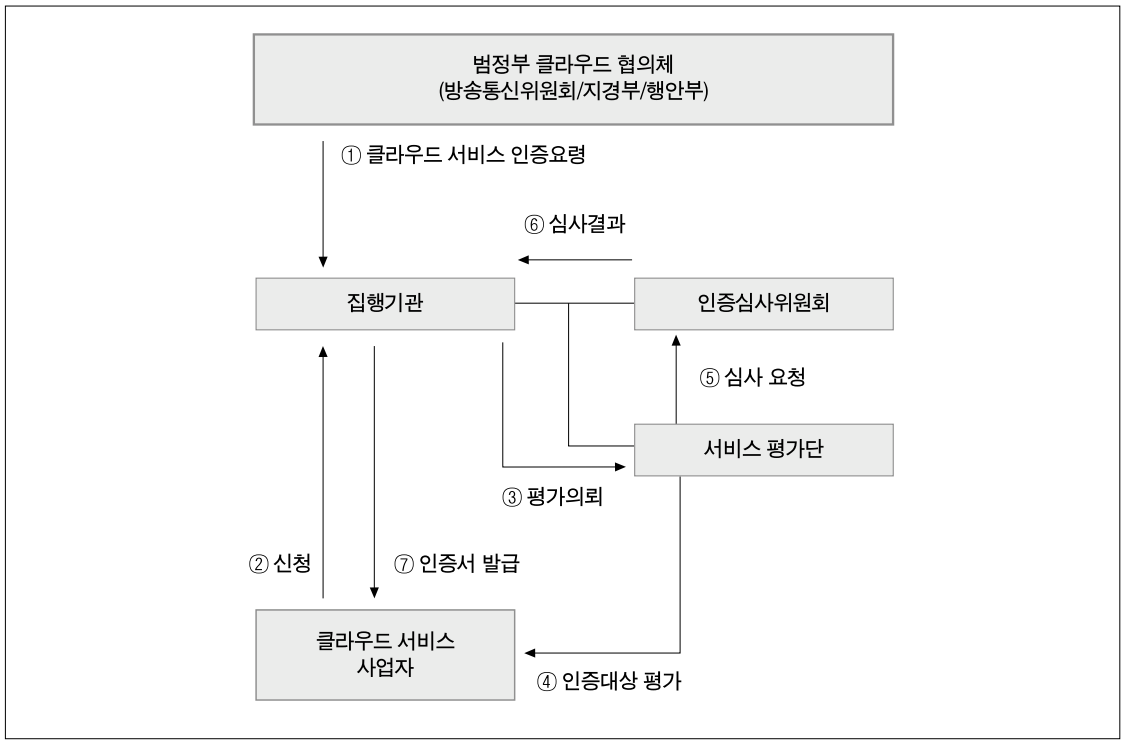
먼저, 클라우드 서비스의 인증체계는 〈그림 4〉와 같이 추진할 계획이다. 클라우드 서비스 인증을 위해서는 클라우드 서비스 인증심사위원회, 심사위원회 및 집행기관으로 구성되는데, 이들의 역할을 기술하면 다음과 같다.

클라우드 서비스 인증심사위원회는 인증 심사 등 인증과 관련한 주요 사항을 심의하기 위하여 '인증심사위원회' 구성 · 운영하는데, 인증심사위원회의 역할은 인증심사, 클라우드 서비스 평가기준(안) 및 기타 클라우드 서비스 인증 대상 포함 여부 및 인증 가이드라인 제 · 개정 등 인증제도와 관련된 주요 사항을 의결한다. 클라우드 서비스 집행기관은 민간기간으로 인증 업무를 효율적으로 수행하기 위하여 클라우드 서비스에 관한 업무를 하고 있는 비영리법인을 집행기관으로 둔다. 클라우드 서비스 집행기관의 역할은 인증신청서 접수 및 서류 검토, 서비스평가계획의 수립 · 보고 및 신청업체에 대한 일정 통보, 서비스평가 실시 및 결과 보고 등을 수행한다. 서비스평가단은 인증 신청을 받은 기업체를 대상으로 평가기준에 따라 서비스를 평가한다.

클라우드 서비스 인증제도의 평가방법을 간략하게 기술하면 다음과 같다.

평가방식은 '클라우드 서비스' 및 '클라우드 서비스 제공 사업자' 분야의 2개 영역에 걸쳐 평가를 실시하되, 항목별 점수산정은 리커드 척도법(5점 혹은 7점)을 적용하여 평가한다.

클라우드 서비스 인증은 클라우드 서비스와 클라우드 서비스 제공 사업자 인증 중 하나만 받을 수도



〈그림 4〉 클라우드 서비스 인증제도 추진체계

있고, 두 가지 모두를 받을 수 있는데, 이는 클라우드 서비스 운영형태에 따라 다르다. 두 인증영역의 모든 항목은 필수항목으로 반드시 필요한 요소들로만 구성되어 있어, 세부 항목들은 최저기준인 동시에 공통필수항목이다. 따라서 클라우드 서비스 인증과 클라우드 서비스 제공 사업자 인증을 위해서는 모든 필수항목에 대한 일정 점수를 이상을 반드시 받아야만 한다. 항목별 점수산정은 5점 척도법(SD법) 적용하여 최소한 3점 이상의 점수를 받도록 하는 영역별 과락과 총점 과락 모두를 적용한다.

현재 평가방법에는 항목간의 중요도 차이가 있음에도 불구하고 이에 대한 가중치 설정이 되어있지 않은 상황이다. 즉, 모든 평가항목의 가중치는 동일한데, 향후에는 국내 실정에 맞는 항목간 가중치 부여가 필수적이라 하겠다. 특히 클라우드 서비스 인증과 클라우드 서비스 제공자 인증 모두의 영역에서 보안영역이 가장 중요한 항목이므로 이에 대한 가중치를 높이는 것이 필요하다. 그리고 실제로 인증심사를 실시하는 과정에서는 서류심사와 실사가 모두 필요한 경우도 있고, 한 가지만 필요한 경우도 있으므로 이는 각 항목의 특징에 따라 평가를 진행한다. 추가적으로 평가항목중에 기타 인증제도와 중복되는 경우에는 기타 인증을 인정하여 해당항목은 심사없이 인정한다.

현재의 인증제도의 평가방법에서는 모든 가중치를 동일한 가중치로 놓고 평가한다. 향후에는 평가항목의 중요도에 따른 가중치 산정을 위해 다수의 전문가 설문조사와 AHP (Analytic Hierarchy Process) 기법 등을 적용하여 항목간의 가중치를 평가할 것이다.

Ⅳ. 결론

클라우드 서비스 산업이 발전함에 있어 클라우드 서비스 제공업체가 각각의 독특한 특성을 반영해서 성공적인 서비스를 제공할 수 있을 것인가에 대한 문제가 제기될 수 있다. 클라우드 서비스는 독립적인 서비스 제공자와 고객간의 필요에 의해서 서비스 계약이 이루어진다. 이는 독립적이고 일시적이라는 계약을 위한 평가가 빈번히 이루어져야 하고, 이에 따라서 클라우드 서비스의 안전성 및 신뢰성 문제가 발생하게 되는데, 이러한 문제를 해결하고 국내 클라우드 서비스 산업의 발전을 위해서는 클라우드 서비스를 위한 안전하고 신뢰할 수 있는 체계적인 인증제도의 수립의 필요하다. 또한 클라우드 서비스 비즈니스 모델에서는 다양한 형태의 서비스 공급자들이 포함됨에 따라, 각각의 서비스 공급업자들이 적절한 서비스 능력을 가지고 있는지에 대한 인증이 필요하다.

본 연구에서는 이러한 문제를 해결하기 위한 클라우드 서비스 인증제도를 위한 프레임워크를 개발하였는데, 이를 위하여 클라우드 서비스 인증과 클라우드 서비스 제공 사업자 인증사업자 인증영역으로 구분하여 인증방안에 개발하였다. 이 결과 클라우드 서비스 인증을 위해서는 구조검토 및 적합성, 가용성, 성능 · 확장성, 보안 · 신뢰성, 고객지원 등 5개 영역의 평가항목을 개발하여 이를 종합적으로 평가하되, 서비스별(IaaS, SaaS) 추가 항목을 두어 평가 기준을 차별화하였다. 클라우드 서비스 제공 사업자 인증을 위해서는 일반 현황, 네트워크/데이터센터-서비스제공 기반, 네트워크/데이터센터-보안, 서비스 지속성, 고객 지원 등 5개 영역의 평가항목을 개발하였고, 이를 평가하기 위한 평가방법도 제안되었다.

추후 연구로는 본문에서도 기술한 바와 같이, PaaS 서비스의 인증을 위한 평가항목이 개발되어야 하고, 기개발한 세부 평가항목들 간의 중요도에 따라 가중치가 부여방법도 개발되어야 한다. 또한 클라우드 서비스 공급자와 수요자간의 계약이 적절한 품질을 유지하며 수행되고 있는지를 평가하지 위한 구체적인 클라우드 서비스 감리방법론의 개발도 필요하다.

■ 참고문헌

김미연 · 문호건 · 박영만 (2010). 「안전한 클라우드 컴퓨팅 환경을 위한 보안 시스템 연구」. 서울: KT경제경영연구소.

김창현 · 이원주 · 전창호 (2010). "클라우드 컴퓨팅 연구 동향." 「한국컴퓨터정보학회지」, 18(1): 1-8.

김형곤 · 이용성 (2010). "클라우드 컴퓨팅 현황 및 향후 전망." 「정보와 통신」, 27: 31-34.

민옥기 · 김학영 · 남궁한 (2009). "클라우드 컴퓨팅 기술 동향." 「전자통신동향분석」, 24(4): 1-13.

민옥기 · 이미영 · 허성진 · 김창수 (2009). 「훤히 보이는 클라우드 컴퓨팅」. 서울: 전자신문사.

방송통신위원회 (2010). "정보보호 관리지침(방송통신위원회 훈령 제77호)."

벤처기업협회 (2008). "표준화 및 시험인증 서비스 제공기관-TTA(한국정보통신기술협회)." 「벤처다이제스트」, 118: 12-15.

서광규 (2006). "체계적인 ASP 인증 방법론에 관한 연구." 「IE Interfaces」, 19(1): 62-69.

이강찬 · 이승윤 (2010). "클라우드 컴퓨팅 표준화 동향 및 전략." 「전자통신동향분석」, 25(1): 90-99.

이주영 (2010). 「클라우드 컴퓨팅의 특징 및 사업자별 제공 서비스 현황」. 서울: 정보통신정책연구원.

이창범 (2010). 「클라우드 컴퓨팅의 안전한 이용과 활성화를 위한 법적 과제」. 서울: 한국정보보호학회.

임철수 (2009). "클라우드 컴퓨팅 보안 기술." 「정보보호학회논문지」, 19(3): 14-17.

정보통신부 (2000). "IDC 시설안전, 신뢰성기준(정보통신부 고시)."

한국산업기술진흥원 (2010). 「녹색인증자료집」. 서울: 한국산업기술진흥원 녹색인증사무국.

행정안전부 (2010). "정보시스템 감리기준(행정안전부 고시 제2010-30호)."

Marston, S. & Li, Z. & Bandyopadhyay, S. & Zhang, J. & Ghalsasi, A. (2011). "Cloud

computing - The business perspective." *Decision Support Systems*, 51(1): 176-189.

Paquette, S. & Jaeger, P. T. & Wilson, S. C. (2010). "Identifying the security risks associated with governmental use of cloud computing." *Government Information Quarterly*, 27(3): 245-253.

Subashini, S. & Kavitha, V. (2011). "A survey on security issues in service delivery models of cloud computing." *Journal of Network and Computer Applications*, 34(1): 1-11.

Svantesson, D. & Clarke, R. (2010). "Privacy and consumer risks in cloud computing." *Computer Law & Security Review*, 26(4): 391-397.

Taylor, M. & Haggerty, J. & Gresty, D. & Hegarty, R. (2010). "Digital evidence in cloud computing systems." *Computer Law & Security Review*, 26(3): 304-308.