

클라우드 관련 법·제도 고찰 및 발전 방향에 대한 제언 - 클라우드 서비스 인증제를 중심으로

조 흥 재*, 민 영 기**

요 약

클라우드 시장에서는 클라우드 서비스 비즈니스 모델의 우위 선점을 위한 글로벌 경쟁이 치열하게 진행되고 있으며, 이와 마찬가지로 국가간 클라우드 관련 정책 또한 빠르게 개발되고 있다. 이러한 클라우드 관련 정책의 일환에 있는 클라우드 서비스 인증제에 대해 살펴보고 발전 방향에 대해 제언하고자 한다.

I. 서 론

최근 클라우드에 대한 인식이 널리 확산되면서 세계적으로 클라우드 이용활성화를 위한 여러 정책들이 추진되는 추세이다. 특히, 클라우드는 ICT를 기반으로 하는 모든 산업에 융·복합이 가능하고 탄소배출량 감소, 비용 절감 등 장점이 많아 경기 침체기인 요즘 더욱 집중 조명되고 있는 실정이다.

또한, 클라우드 서비스는 IaaS를 중심으로 SaaS, PaaS, DaaS 등 비즈니스 시장이 광범위하고 사업자 입장에서는 락인(Rock-in) 효과가 강하게 작용할 수 있기 때문에 세계적으로 우위 선점을 위한 경쟁이 치열하게 전개되고 있다.

이러한 클라우드의 특성 상 국가 차원에서도 클라우드의 도입 촉진과 걸림돌인 보안 문제 등을 해결하기 위해 선진국을 중심으로 정책 개발이 활발히 진행되고 있으며, 우리 나라에서도 법·제 정비, 클라우드 테스트 베드, 인증제, R&D, 공공 클라우드 선제 도입 등 클라우드 관련 여러 정책들이 개발 및 진행되고 있다.

이러한 정책 중에서도 기업의 선순환적 기업 생태계를 유도하고 해외 선진국에 비해 뒤쳐진 기술력을 뒷받침하기 위해 이용활성화 정책이 빠르게 전개되고 있다. 클라우드 서비스 인증제는 이러한 이용활성화 정책의 일환으로 보안, 가용성, 신뢰성 등의 클라우드 서비스를

이용하고자 하는 이용자들에게 걸림돌이 되고 있는 문제점들을 점검하고 민간차원에서 검증하여 인증함으로써 이용자 신뢰기반을 마련하고 이용활성화를 도모코자 제정된 정책이다.

본 연구에서는 클라우드 서비스 인증제를 중심으로 클라우드 관련 법·제도를 고찰하고 향후 발전시켜 나가야 하는 정책적 방향에 대해 제언하고자 한다.

II. 클라우드 인증관련 해외 정책 동향 및 국내 관련 인증제도

1. 클라우드 서비스 개념

클라우드 서비스의 개념은 언제 어디서나 인터넷 접속만으로 컴퓨팅 환경을 이용하고 이용한 만큼 요금을 지불하는 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(민욱기 외, 2009a).

클라우드 서비스는 기본 기술인 가상화와 분산처리 기술을 기반으로 인프라 제공 서비스(IaaS, Infrastructure as a Service), 소프트웨어 제공 서비스(SaaS, Software as a Service), 플랫폼 제공 서비스(PaaS, Platform

* (사)한국클라우드서비스협회, 팀장, 주저자(chohj@kcsa.or.kr)

** (사)한국클라우드서비스협회, 사무국장, 교신저자(min@kcsa.or.kr)

as a Service)로 크게 나눌 수 있으며, 이 외에도 데스크탑 제공 서비스(DaaS, Desktop as a Service) 등 서비스 영역은 나날이 확대되어 가고 있는 실정이다.

특히, 소셜네트워크(SNS)의 활발한 성장과 빅데이터의 이슈 등은 한정된 물리적 자원에 대한 효율성의 극대화를 추구하게 되었고, 네트워크의 복잡성 및 N-Screen과 같이 사용단말의 증가로 인해 급증하는 전력 수요와 데이터 양을 수용하는데 있어서의 한계를 극복하기 위해 클라우드 컴퓨팅의 필요성이 더욱 증가하게 되었다.

또한, 전세계적인 경기침체로 인해 ICT 비용 절감 이슈는 기업들의 생존전략에 있어서 가장 우선적인 문제로 이를 극복하기 위한 전략적 방안의 하나로 클라우드 컴퓨팅의 도입을 고려하게 되었다.

하지만 클라우드 서비스는 기존의 '소유'라는 개념에서 '임대'라는 개념으로 변화되는 것이기 때문에 기업 정보, 사적 정보 등 정보에 대한 보안 이슈, 서비스 장애에 의한 불안감 이슈 등으로 인해 클라우드의 여러 장점들이 있음에도 불구하고 급속하게 확산되고 있지 못하는 실정이다. 국내의 경우 임대라는 인식의 전환이 더디고 클라우드에 대한 신뢰기반이 미약하여 해외에 비해 더욱 도입률이 저조한 것 또한 이러한 이유 때문이다.

이러한 이유로 인해 국내에서는 클라우드 서비스 인증제를 개발하였고 1단계로 민간협회를 통해 인증을 시작하였다.

2. 해외의 클라우드 인증 관련 정책

해외의 국내 클라우드 서비스 인증과 같이 클라우드 서비스에 대해 직접적으로 인증을 부여하는 제도는 마련되어 있지 않지만 미국은 정부를 중심으로 클라우드 보안에 관련된 인증을, 일본은 민간기관의 ASP·SaaS 인증을 운영하고 있으며, 유럽은 현재 유럽연합 27개국의 상호 다른 법 체계와 문화 등으로 인해 표준제정과 인증 작업이 어렵긴 하지만 추진 중에 있다.

가. 미국

미국은 클라우드와 관련하여 2009년 9월 '연방정부

클라우드 컴퓨팅 계획(Federal Cloud Computing Initiative)을 발표하고 계획에 따라 추진하고 있다. 이 계획은 클라우드 컴퓨팅 도입을 통해 인프라 구축 비용을 절감하고 IT 자원의 유연성을 제공하는 것을 주 내용으로 담고 있으며, 정부부처 및 기관이 선제 도입함으로써 이용활성화를 도모한다는 계획이다. 이와 관련하여 첫 프로젝트로 Apps.gov를 오픈하여 클라우드 애플리케이션과 서비스를 구매할 수 있도록 하였다.

2010년 5월에는 'State of Public Sector Cloud Computing'이라는 공공부문의 클라우드 컴퓨팅 도입 현황 정리 보고서를 발간하였고, 연방정부 데이터센터 통합 계획을 통해 2013년까지 모든 공공기관이 단계적으로 클라우드 컴퓨팅에 대해 도입을 고려하도록 권고했다.

또한, 미 조달청(GSA)은 2012년 6월 클라우드 서비스와 연계된 클라우드 보안인증 프로그램 Fed-RAMP(Federal Risk Authorization and Management Program)의 운영 계시를 발표하였고 인증평가를 위한 평가대행기관인 3PAO(Third Party Assessment Organization) 8곳을 선정하고 운영을 시작했다.

나. 일본

일본은 '가스미가세키 프로젝트'를 통해 중앙부처 대상의 클라우드 추진과 지자체 대상의 지자체 클라우드를 추진 중에 있으며, 최근 'i-Japan 전략 2015'에서 정보시스템 효율화를 위한 추진 정책을 명시하였다. 또한, 일본 경제산업성에서 발표한 2010년 자료에 따르면 일본은 클라우드 컴퓨팅으로 IT업계뿐 아니라 농업, 상업, 임업 등 산업별 컨소시엄 구성과 클라우드 접목을 도모하고 있다.

ASP 인증을 발전시킨 ASP·SaaS 인증은 웹사이트를 통해 사업자의 정보를 공개함으로써 잠재 이용자에 대한 정보를 제공하고 이를 통해 선택 및 이용할 수 있도록 하여 클라우드 서비스 이용활성화를 추진하고 있다. 공개정보는 필수 공개 항목과 선택 공개 항목으로 구분하고 있으며, 사업자간 공정한 경쟁을 유도하고 이용자에게 필요한 정보를 제공하는 정책을 민간단체를 통해 추진 중에 있다.

3. 국내의 클라우드 관련 인증제도

가. ASP 인증제도

국내에서는 2006년에서 2008년까지 2년간 ASP 산업 전반에 대한 불안감 해소와 솔루션의 품질 향상을 도모하기 위해 인증제가 실시되었다.

ASP 인증의 영역은 [표 1]와 같이 애플리케이션 인증과 사업자(서비스 환경) 인증으로 나눌 수 있으며, 이에 대한 정의는 다음과 같다(서광규, 2006)

- 애플리케이션 인증 : ASP 애플리케이션의 구조, 유용성, 확장성, 성능, 보안 등에 대한 적정성 및 적합성의 객관적인 평가를 통해 애플리케이션의 선택기준을 제시하는 애플리케이션 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 점검하여 서비스를 제공할 수 있는 사업체의 서비스 환경 인증

나. TTA GS 인증제도

정부는 국내 S/W산업의 경쟁력 제고 차원에서 S/W 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 GS 마크 제도는 시험·인증을 통한 품질 향상 극대화 와 정부공인 인증획득을 통한 제품의 신뢰도 증가, 국가적 차원의 지원을 통한 제품마케팅 지원 그리고 사전 검증된 고품질 S/W 공급으로 S/W 유통을 활성화하는데 그 목적을 두고 있다(벤처기업협회, 2008)

GS 인증은 패키지, 모바일, 임베디드 뿐만 아니라,

CRM, ERP, Groupware 등 모든 분야의 소프트웨어를 대상으로 하고 있다. 테스트 기준은 국제 표준에 근거한 한국형 평가모델 개발을 통해 2000년 8월부터 적용시켜 왔으며, 기능성, 신뢰성, 효율성, 사용성, 유지보수성, 이식성 등의 다양한 점검기준을 만족하는지의 여부를 평가하여 인증을 제공하고 있다.

다. 녹색 인증제도

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

녹색인증제는 2010년 4월부터 자원 및 환경위기에 대한 극복과 저탄소 녹색성장 지향을 위해 녹색산업 투자 집중 도모를 목적으로 시행되고 있다.

녹색인증제의 대상은 녹색기술, 녹색사업 및 녹색전문기업확인으로 이루어지며, 녹색기술 분야는 [표 2]와 같이 그린에너지, 녹색기술, 신성장동력 등에서 제시된 10대분야 61개 중점분야 중심의 세부기술 및 핵심(요소) 기술범주에 해당되는 분야이다.

III. 클라우드 서비스 인증제

1. 클라우드 서비스 인증제 개관

클라우드 서비스 인증제는 경제정책조정회의에서 2011년 5월 '클라우드 컴퓨팅 확산 및 경쟁력 강화전략'을 발표하고 이에 대한 일환으로 방송통신위원회에서 추진하여 시행한 제도이다.

방송통신위원회에서는 인증제 마련을 위해 2010년 '클라우드 서비스 인증제도 도입 방안 연구'를 통해 클라우드 서비스 인증 프레임워크를 개발하였고 2010년

[표 1] ASP 인증영역

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

부터 2011년까지 국내·외 산·학·연·관의 클라우드 관련 기술자 및 법·제도 전문가들의 의견수렴을 거치면서 보완되어 2012년 2월 민간인증으로 출발하였다.

또한, 2011년 9월 ‘클라우드 서비스 SLA 가이드’ 배포를 통해 혼잡 되어 있는 클라우드 서비스 SLA 또는 이용약관 등에 도입할 수 있도록 제시하였고, 클라우드 서비스 인증제에서 이에 대한 도입 여부 등을 점검하도록 하였다.

클라우드 서비스 인증제에 대해 방송통신위원회에서는 국내 도입시기에는 이용활성화를 위해 민간인증으로 추진하고 시장발전도에 따라 2단계 정부인증으로 추진하는 목표를 세우고 있으며, 이를 뒷받침 할 수 있도록 ‘클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률’ 제정안을 2012년 8월 입법예고 하였다.

2. 클라우드 서비스 인증 평가항목

클라우드 서비스 인증은 클라우드 서비스의 원활한 제공을 위해 반드시 갖추어야 할 필수 항목들과 선택적으로 갖출 수 있도록 하는 일반항목들로 구성되어 있다. 클라우드 서비스는 인터넷을 기반으로 서비스를 온 디맨드 방식으로 이용자가 원하는 만큼 제공하고 전기요금처럼 이용한 만큼 과금 하는 특징을 갖고 있기 때문에 이러한 특징들을 고려하여 세부평가항목을 도출하였다(2011. 서광규).

평가영역과 평가항목은 이러한 클라우드 서비스의 특징과 기존의 IT 아웃소싱 방법론, 정부의 정책 및 지침, 그리고 SAP 인증제도 및 관련 인증제도를 종합·검토하여 도출하였고, 클라우드 서비스 자문위원회와 관련업계 전문가 등을 통하여 제안항목의 타당성을 검증하였다. 이 과정을 통하여 도출된 평가영역으로 가용성, 확장성, 성능, 데이터관리, 보안, 서비스 지속성, 서비스 지원으로 7개 영역을 구분하고 세부 평가항목을 도출하였다.

이와 관련하여, IaaS의 경우는 39개의 필수 항목과 66개의 일반항목으로 총 105개의 세부항목을 점검하게 되며, SaaS의 경우 33개의 필수 항목과 52개의 일반항목으로 총 85개의 세부항목을 점검한다. PaaS는 아직 국내 도입이 미미하여 현재의 인증제에서는 다루지 않는다.

클라우드 서비스 인증제의 인증 종류는 ‘클라우드 서비스 인증’과 ‘클라우드 서비스 우수 SLA 인증’의 두



(그림 1) 서비스 품질 인증평가 프로세스

종류로 구분되며, 클라우드 서비스 인증은 전체 항목 중 필수 항목은 반드시 모두 통과해야 하고 전체 평가점수가 평가항목 수의 70% 이상을 획득해야 인증이 부여된다. 그리고, 클라우드 서비스 우수 SLA 인증의 경우 클라우드 서비스 인증의 평가항목 외에 3가지 추가 항목을 만족시켜야 인증을 부여받는다. 3가지 추가항목은 첫째, 클라우드 서비스의 월평균 가용성이 99.5% 이상 유지해야 하고, 둘째, ISMS 또는 ISO27001의 인증을 취득하여야 하고, 셋째, 글로벌 수준의 위약금 조항을 반드시 구비하여야 한다.

클라우드 서비스 인증제의 큰 영역으로 구분할 경우 가용성, 성능, 확장성은 서비스 품질의 영역으로 구분지을 수 있으며, 데이터관리와 보안은 서비스 정보보호의 영역으로, 서비스 지속성과 서비스 지원은 서비스 기반의 영역으로 분류할 수 있다. 또한, 클라우드 서비스 인증제의 특징은 S/W 품질 평가와 같은 기술적 테스트 평가와는 다르게 ISO 인증과 같이 필요시 실사를 포함하여 문서위주의 평가를 진행한다.

가. 서비스 품질

서비스 품질의 영역안에는 가용성, 성능, 확장성의 3개의 영역으로 구분되며, 각각의 영역에 대한 정책의 수립여부 점검에서부터 서비스 기능, 논리구조, 물리구조 등의 클라우드 서비스 구조의 유용성과 적합성에 대한 점검과 조직 및 책임설정, 시스템 도입 및 관리 등에 대해 세부점검 항목을 평가한다.

1) 가용성

가용성은 클라우드 서비스의 제공자가 이용자에게 서비스 약정에 따라 상시적으로 서비스를 제공하기 위

해 제반 사항 및 조치에 대해 점검한다.

2) 확장성

확장성은 클라우드 서비스 제공자가 이용자의 수요에 유연하게 자원을 확장하여 제공할 수 있도록 필요한 정책, 인적·물적 자원 등을 갖추고 있는지 평가한다.

3) 성능

성능은 클라우드 서비스 제공자가 서비스의 속도 등의 품질을 보장하기 위해 적절한 성능을 유지하여야 하며, 이를 위해 필요한 정책, 인적·물적 자원 등을 갖추고 있는지 평가한다.

나. 서비스 정보보호

서비스 정보보호 영역안에는 데이터관리와 보안의 2개의 영역으로 구분되며, 각각의 영역에 대한 정책의 수립여부 점검에서부터 이용자의 정보를 보호하기 위한 보안 기술 등에 대해 평가한다.

1) 데이터관리

데이터관리는 클라우드 서비스 제공자가 이용자의 데이터를 안전하게 보호 및 관리하기 위해 필요한 정책과 인적·물적 자원 등을 갖추고 있는지 평가한다.

2) 보안

보안은 조직의 보안을 효과적으로 구현하기 위해 관

[표 2] 가용성 측정항목 및 설명

| 인증 영역 | 측정항목 | 설 명 | |
|-------|------|--------------|--|
| 가용성 | 1.1 | 정책수립 | 클라우드 서비스 제공자는 서비스의 가용성 수준을 보장하기 위해 물리적 자원 보유/관리, 가상화 등 클라우드 관련 기술 적용 현황, 시스템 운영/관리 방법 등을 포함한 가용성 정책을 수립하고, 이를 문서화하여야 한다. 또한 해당 정책은 관련 법령 등에서 제시하는 바를 준수하여야 한다. |
| | 1.2 | 목표제시 및 결과 통지 | 클라우드 서비스 제공자는 이용자에게 서비스 가용성 수준을 사전에 문서를 통해 제시하여야 하며, 이용자가 주기적으로 가용성 수준을 알 수 있도록 관련 프로세스를 마련하여야 한다. |
| | 1.3 | 조직 및 책임설정 | 클라우드 서비스 제공자는 이용자에게 제시한 가용성 수준을 보장하기 위해 조직 및 인력을 적절히 배치하여야 하며, 해당 직무는 책임성 있게 수행되어야 한다. |
| | 1.4 | 시스템 도입/관리 | 클라우드 서비스 제공자는 서비스의 가용성 수준을 보장하기 위해 가상화, 분산 컴퓨팅 등의 적절한 클라우드 기술/소프트웨어 등을 도입하여 시스템을 구성하여야 한다. 또한 장애에 대비하여 모니터링, 이중화, 유지/보수할 수 있도록 준비되어야 한다. |
| | 1.5 | 내부관리 | 클라우드 서비스 제공자는 서비스의 가용성 한계에 대비하여 이를 예측/분석/개선하고, 필요한 기술 자료를 보유/관리하여야 한다. |

[표 3] 확장성 측정항목 및 설명

| 인증 영역 | 측정항목 | 설 명 | |
|-------|------|-----------|---|
| 확장성 | 2.1 | 정책수립 | 클라우드 서비스 제공자는 서비스의 확장성 수준을 보장하기 위해 서비스 지원범위, 시스템 구조, 이용량 예측, 인프라 확장계획 등을 포함한 확장성 정책을 수립하고, 이를 문서화하여야 한다. |
| | 2.2 | 수준제시 | 클라우드 서비스 제공자는 이용자에게 서비스 확장성 수준을 사전에 문서를 통해 제시하여야 하며, 이용자가 주기적으로 확장성 수준을 알 수 있도록 관련 프로세스를 마련하여야 한다. |
| | 2.3 | 조직 및 책임설정 | 클라우드 서비스 제공자는 이용자에게 제시한 확장성 수준을 보장하기 위해 조직 및 인력을 적절히 배치하여야 하며, 해당 직무는 책임성 있게 수행되어야 한다. |
| | 2.4 | 시스템 도입/관리 | 클라우드 서비스 제공자는 서비스의 이용량에 따라 서비스의 중단 없이 자원을 동적으로 확장하거나 축소할 수 있도록 시스템을 구축하여야 한다. 또한 이용량 변화에 신속적으로 대응할 수 있도록 모니터링, 유지/보수, 추가적인 물리적 자원 확보가 가능하도록 준비되어야 한다. |
| | 2.5 | 내부관리 | 클라우드 서비스 제공자는 서비스의 확장성 한계에 대비하여 이를 예측/분석/개선하고, 필요한 기술 자료를 보유/관리하여야 한다. |

리 체계를 수립유무, 물리적 시설 및 설비를 보호하기 위한 보호 방안이 마련 유무, 취약성 분석 실시와 그에 대한 적절한 대책을 마련하고 적용하는지에 대해 평가한다.

다. 서비스 기반

서비스 기반 영역안에는 서비스 지속성과 서비스 지원의 2개의 영역으로 구분되며, 각각의 영역에 대한 정책의 수립여부, 지원체계, 이용자의 서비스 만족도를 제고하기 위한 각종 기술 지원, 제공방식 등에 대해 평가한다.

1) 서비스 지속성

클라우드 서비스 이용자가 믿고 서비스를 이용할 수

있도록 사업자가 인적·물적 기반을 확보 및 관리하고 있는지에 대해 평가한다.

2) 서비스 지원

클라우드 서비스 제공자가 이용자의 서비스 만족도를 제고하기 위해 기술지원, 제공방식의 다양성, 수준의 보장 등에 관련하여 체계 및 프로세스를 갖추고 있는지 평가한다.

3. 클라우드 서비스 인증제 운영체계 및 평가방법

본 절에서는 클라우드 서비스 인증제 운영체계 및 클라우드 서비스 인증제도의 평가방법을 간략하게 기술하기로 한다.

[표 4] 성능 측정항목 및 설명

| 인증 영역 | 측정항목 | | 설 명 |
|-------|------|--------------|--|
| 성능 | 3.1 | 정책수립 | 클라우드 서비스 제공자는 서비스의 성능(속도) 수준을 보장하기 위해 서비스 지원 범위, 네트워크 확보 현황, 시스템 구성, 예방 활동 등을 포함한 성능 정책을 수립하고, 이를 문서화하여야 한다. |
| | 3.2 | 수준제시 | 클라우드 서비스 제공자는 이용자에게 서비스 성능 수준을 사전에 문서를 통해 제시하여야 하며, 이용자가 주기적으로 확장성 수준을 알 수 있도록 관련 프로세스를 마련하여야 한다. |
| | 3.3 | 조직 및 책임설정 | 클라우드 서비스 제공자는 이용자에게 제시한 성능 수준을 보장하기 위해 조직 및 인력을 적절히 배치하여야 하며, 해당 직무는 책임성 있게 수행되어야 한다. |
| | 3.4 | 자원확보 및 유지/관리 | 클라우드 서비스 제공자는 서비스의 성능을 우수하게 유지하기 위해 적절한 수준의 하드웨어 및 네트워크 자원을 확보하여야 한다. 또한 이를 최신으로 유지하기 위해 노력하여야 한다. |
| | 3.5 | 예방활동 및 품질 측정 | 클라우드 서비스 제공자는 클라우드 시스템을 주기적으로 업그레이드하고, 품질을 측정하는 등 클라우드 서비스의 성능을 유지하도록 해야 한다. |
| | 3.6 | 내부관리 | 클라우드 서비스 제공자는 서비스의 속도를 보장/개선하기 위해 이를 예측/분석/개선하고, 필요한 기술 자료를 보유/관리하여야 한다. |

[표 5] 데이터관리 측정항목 및 설명

| 인증 영역 | 측정항목 | | 설 명 |
|--------|------|---------------|--|
| 데이터 관리 | 4.1 | 정책수립 | 클라우드 서비스 제공자는 데이터를 안전하게 보호/관리하기 위한 정책을 수립하고, 이를 문서화하여야 한다. 또한 해당 정책은 관련 법령 등에서 제시하는 바를 준수하여야 한다. |
| | 4.2 | 조직 및 책임설정 | 클라우드 서비스 제공자는 이용자의 데이터를 안전하게 보호/관리하기 위해 조직 및 인력을 적절히 배치하여야 하며, 해당 직무는 책임성 있게 수행되어야 한다. |
| | 4.3 | 백업시스템 확보 및 관리 | 클라우드 서비스 제공자는 재해, 재난, 무단 접근 등 위협으로부터 이용자의 데이터를 안전하게 보호/관리하기 위해 백업 시스템을 확보/관리하여야 한다. |
| | 4.4 | 백업시행 및 복구테스트 | 클라우드 서비스 제공자는 서비스의 신뢰성을 확보하기 위해, 정책 또는 계약 등에서 정하는 바에 따라 백업을 주기적으로 시행하고, 복구 능력을 관리하여야 한다. |
| | 4.5 | 데이터 반환 및 폐기 | 클라우드 서비스 제공자는 고객이 원하거나 법령이 정하는 바에 따라, 데이터를 반환하거나 폐기할 수 있도록 정책을 마련하고, 이에 따라 조치하여야 한다. |

먼저, 클라우드 서비스 인증제의 운영체계는 (그림 2)와 같이 운영된다. 클라우드 서비스 인증을 위해서는 클라우드 서비스 인증위원회, 서비스 평가단, 집행기관인 인증사무국으로 구성되는데 이들의 역할을 기술하면 다음과 같다.

클라우드 서비스 인증위원회는 인증 최종심의 등 인증과 관련한 주요 사항을 심의하기 위하여 구성하며, 역

할은 최종 심의, 클라우드 서비스 평가기준 제·개정 등 인증제도와 관련된 주요 사항을 의결한다. 서비스 평가단은 인증 신청이 접수된 클라우드 서비스에 대해 평가기준에 따라 문서 및 실사로해 평가를 수행하고 평가단장은 평가결과를 인증위원회에 보고한다. 인증사무국은 인증 업무의 효율적인 수행과 운영을 위해 현재 비영리 협회에서 담당하고 있으며, 인증신청서 접수 및 서

[표 6] 보안 측정항목 및 설명

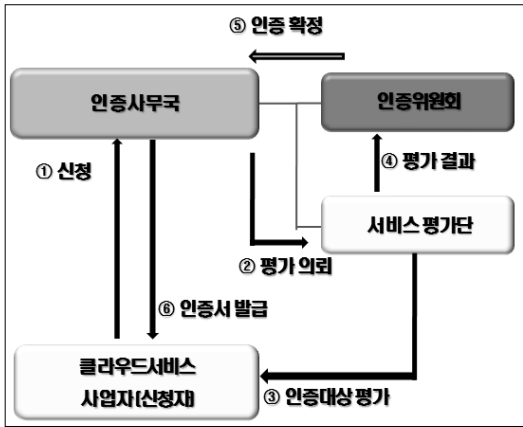
| 인증 영역 | 측정항목 | | 설 명 |
|-------|------|---------------|---|
| 보안 | 5.1 | 정책수립 | 클라우드 서비스 제공자는 데이터를 안전하게 보호/관리하기 위한 정책을 수립하고, 이를 문서화하여야 한다. 또한 해당 정책은 관련 법령 등에서 제시하는 바를 준수하여야 한다. |
| | 5.2 | 조직 및 책임설정 | 클라우드 서비스 제공자는 이용자의 데이터를 안전하게 보호/관리하기 위해 조직 및 인력을 적절히 배치하여야 하며, 해당 직무는 책임성 있게 수행되어야 한다. |
| | 5.3 | 백업시스템 확보 및 관리 | 클라우드 서비스 제공자는 재해, 재난, 무단 접근 등 위협으로부터 이용자의 데이터를 안전하게 보호/관리하기 위해 백업 시스템을 확보/관리하여야 한다. |
| | 5.4 | 백업시행 및 복구테스트 | 클라우드 서비스 제공자는 서비스의 신뢰성을 확보하기 위해, 정책 또는 계약 등에서 정하는 바에 따라 백업을 주기적으로 시행하고, 복구 능력을 관리하여야 한다. |
| | 5.5 | 데이터 반환 및 폐기 | 클라우드 서비스 제공자는 고객이 원하거나 법령이 정하는 바에 따라, 데이터를 반환하거나 폐기할 수 있도록 정책을 마련하고, 이에 따라 조치하여야 한다. |
| | 5.6 | 정보보호 정책수립 | 클라우드 서비스 제공자는 정보보호정책을 수립하고, 이를 구체적으로 시행하기 위한 정보보호 지침, 절차, 매뉴얼을 포함하여야 하며, 보안책임을 명시적으로 규정하여야 한다. 또한 보안과 관련된 법규의 준수 여부를 검토해야 한다. |
| | 5.7 | 조직 및 책임 설정 | 클라우드 서비스 제공자는 서비스 정보보호를 위해 조직 및 인력을 적절히 배치하여야 하며, 해당 직무는 책임성 있게 수행되어야 한다. 특히, 이용자의 보안 요구사항을 접수하고 반영하기 위한 프로세스를 수립하여야 한다. |
| | 5.8 | 정보자산 관리 | 정보 자산에 대하여 소유자, 관리자, 사용자를 확인하고, 적절한 통제 유지를 위해 책임 소재를 명확히 하여야 한다. |
| | 5.9 | 인증 및 접근 관리 | 접근통제는 데이터, 프로그램, 주요 시스템, 네트워크 등에 대한 접근 제어를 포함하여야 하며, 여기에는 보안요구사항, 데이터 및 서비스 접근 시의 법적, 계약적 제한, 네트워크상의 접근권한 관리 등을 포함하여야 한다. |
| | 5.10 | 정보보호 교육 | 정보보호 인식제고 및 실제 운영에 필요한 교육·훈련 계획을 종합적으로 수립하고 이행하여야 한다. |

[표 7] 서비스 지속성 측정항목 및 설명

| 인증 영역 | 측정항목 | | 설 명 |
|---------|------|----------|--|
| 서비스 지속성 | 6.1 | 서비스 지속역량 | 클라우드 서비스 제공자는 서비스를 지속적으로 제공할 수 있도록 사업 목표를 수립하고, 재무 상태, 전산자원, 기타 인적/물적 자원 등 기본적인 경영 기반을 유지하여야 한다. |
| | 6.2 | 조직 및 인력 | 클라우드 서비스 제공자의 조직 및 인력은 안정적인 클라우드 서비스를 제공하기에 적합하여야 한다. 또한 주요 서비스 수준은 주기적으로 경영진에 보고되어 관리될 수 있어야 한다. |
| | 6.3 | 예산 계획 | 클라우드 서비스 제공자는 안정적인 서비스 제공을 위해 필요한 예산 계획을 수립하여야 한다. 또한 이를 통제/승인하기 위한 프로세스를 마련하여야 한다. |
| | 6.4 | 변경 관리 | 클라우드 서비스 제공자는 서비스 및 시스템의 변경에 대하여 그 내용을 명확히 정의하고, 관련 프로세스를 문서화하여야 한다. 또한 결과를 기록하고, 이를 서비스 개선에 반영하여야 한다. |

[표 8] 서비스 지원 측정항목 및 설명

| 인증 영역 | 측정항목 | 설 명 | |
|--------|------|--------------|---|
| 서비스 지원 | 7.1 | 이용자 서비스 정책수립 | 클라우드 서비스 제공자는 서비스 수준을 유지하고 이용자의 요구에 적절히 대응하기 위해 이용자 서비스 정책을 수립하여야 한다. |
| | 7.2 | 고객지원 체계 | 클라우드 서비스 제공자는 서비스에 문제가 발생하는 경우에 대비하여 이용자를 지원하기 위한 프로세스 및 시스템 등을 보유하여야 한다. |
| | 7.3 | 서비스 제공방식 다양성 | 클라우드 서비스는 다양한 단말 및 각종 운영 체제, 브라우저 등을 통해 제공될 수 있어야 한다. |
| | 7.4 | 서비스수준 보증 | 클라우드 서비스 제공자는 이용자의 서비스 만족도를 유지/보장하기 위해 적절한 프로세스를 마련하고, 손해배상, 보험가입 등 필요한 활동을 하여야 한다. |
| | 7.5 | 서비스 이전 | 클라우드 서비스 제공자는 이용자가 다른 클라우드 서비스 제공자를 선택하여 서비스를 이전하려는 경우 이를 지원할 수 있는 방안을 마련하여야 한다. |
| | 7.6 | 이용자 교육 | 이용자가 서비스를 원활하게 이용할 수 있도록 이용 방법, 범위 및 내용 등에 대해 이용자 교육을 실시하거나 이에 준하는 매뉴얼을 제공하여야 한다. |



[그림 2] 클라우드 서비스 인증제 운영체계

류 검토, 서비스 평가 계획수립 및 보고 등 인증제 운영을 위한 제반 사항을 담당한다.

4. 법에서의 클라우드 서비스 인증

본 절에서는 2012년 8월 입법 예고된 ‘클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제정안’에서 다루고 있는 인증에 대해 간략하게 기술하고자 한다.

법에서는 공공기관 등에서 클라우드 컴퓨팅 도입·이용을 위해서는 클라우드컴퓨팅서비스 제공자가 정부가 수행하는 정보보호인증을 받도록 할 수 있게 조문이 구성되어 있으며, 정보보호 인증의 내용, 방법 및 절차에 관하여는 대통령령으로 정하는 바에 따르도록 되어 있다.

또한, 클라우드컴퓨팅서비스의 품질 및 신뢰성을 높

이기 위해 클라우드컴퓨팅서비스를 대상으로 인증을 실시할 수 있도록 되어 있으며, 심사기준 등 필요한 사항을 고시할 수 있게 되어 있으며, 인증을 취득한 사업자에게 동법에서 따른 지원을 우선적으로 받을 수 있도록 구성되어 있다.

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률은 정부 인증을 통해 공공부문의 클라우드 도입을 위한 기반 조성 및 민간부문에서의 클라우드 이용을 촉진, 클라우드 사업자에 대한 인센티브, 이용자의 데이터를 보호하기 위한 장치마련 등 클라우드의 산업 발전뿐만 아니라 클라우드 생태계의 포괄적인 접근으로 방송통신위원회에서 추진하고 있다.

IV. 결 론

클라우드 서비스는 비용의 절감, 그린 IT 실현, 스마트 오피스 구현 등 장점이 많은 반면에 이용자의 사적 정보에 대한 유출의 불안감, 장애 발생 등으로 인한 손해 발생 등 적지 않은 불안감을 내포하고 있는 것이 사실이다. 이러한 문제점들을 해결하기 위해 국내 뿐만 아니라 클라우드 서비스 선진국가에서도 형태는 다르지만 신뢰기반 구축과 이용활성화라는 측면에서 여러 가지 해결 방안을 마련하고 실행하고 있다. 특히, 클라우드 서비스는 과거 그리드 컴퓨팅, 유틸리티 컴퓨팅 등의 기술적인 발전과 ASP, 웹하드 등의 서비스적인 발전이 함께 어우러지면서 탄생된 인터넷 기반의 서비스로 앞으로 더욱 빠르게 진화되고 세계 경쟁이 치열해 질 것으로 예상하고 있다. 그렇기 때문에 이용자의 신뢰기반 구축 이슈는 매우 중요한 부분이고 클라우드 서비스 인

증제에 대한 연구도 반드시 필요하다.

본 연구에서는 이용자 신뢰기반 구축의 일환인 클라우드 서비스 인증제에 대해 살펴보고 관련 인증 및 해외 클라우드 정책현황을 분석한 결과를 토대로 다음과 같은 발전 방향을 제안하고자 한다.

현재의 클라우드 서비스 인증제는 클라우드 서비스 레벨을 직접적으로 반영하지 않고 있기 때문에 기술적 난이도, 서비스 난이도 등을 고려하여 개선 및 고도화 하는 연구가 필요하다고 판단된다. 이는 제공되는 클라우드 서비스에 대해 품질 경쟁을 유도할 수 있고 이용자에게도 좀 더 서비스의 비교·선택 할 수 있는 객관적인 정보제공이 가능하기 때문이다. 또한, 서비스 제공자 입장에서 서비스 레벨에 따라 가격정책을 차별화 할 수 있기 때문에 양질의 서비스 제공에 따른 이익 창출에도 영향을 줄 수 있다. 그리고, 기술적인 테스트 결과에 대한 반영이 필요하다. 현재 클라우드 서비스 인증은 문서 및 실사 위주로 평가되기 때문에 실질적인 테스트를 진행하여 그 결과를 인증평가에 반영한다면 인증에 대한 신뢰성 및 완성도가 높아질 것으로 판단된다. 마지막으로 클라우드 서비스의 제공자 및 이용자들이 법적인 지원과 보호에 대한 보장을 받을 수 있다면 클라우드 서비스 이용활성화는 더욱 촉진 될 것으로 기대되며, 법적 기반에서의 클라우드 서비스 인증제에 대한 연구도 필요하다고 판단된다.

참고문헌

[1] 서광규, “클라우드 서비스 인증제도 수립을 위한 프레임워크”, 정보화정책논문집 제18권 제1호, pp. 22-24, 2011

[2] 신선영, 송석현, “국내 공공 클라우드 서비스 적용 우선순위 도출에 관한 연구: 해외 공공부문 클라우드 사례의 SRM 매핑을 통해”, Internet and Information Security, 제3권 제3호, pp. 67~89, 2012.

[3] 민욱기, 김학영, 남궁한, “클라우드 컴퓨팅 기술 동향”, 전자통신동향분석, 24(4), 1~13, 2009.

[4] 민욱기, 이미영, 허성진, 김창수, “흔히 보이는 클라우드 컴퓨팅”, 전자신문사, 2012.

[5] 서광규, “체계적인 ASP 인증 방법론에 관한 연구”, IE Interfaces, 19(1), 62~69, 2006.

[6] 정제호, 김수동, 국신욱, 민영기, 손승우, 신수정, 양

희동, 이종화, “클라우드 컴퓨팅 활성화를 위한 법제도 개선방안”, 정보통신산업진흥원, 정책연구센터 09-03, 2009.

[7] 한국산업기술진흥원, “녹색인증자료집”, 한국산업기술진흥원 녹색인증사무국, 2010.

[8] GSA, “Ensuring secure cloud computing for the Federal Government”, Jun 2012.

[9] GCN, “FedRAMP aims to authorize 3 cloud providers by year’s end”, Jun 2012.

[10] HM Government, “Government ICT Strategy”, 2010.

[11] UK Cabinet Office, “One Year On: Implementing the Government ICT Strategy. 2012

[12] UK Cabinet Office, “One Year On: Implementing the Government ICT Strategy. 2012

[13] Marston, S. & Li, Z. & Bandyopadhyay, S. & Zhang, J. & Ghalsasi, A. “Cloud computing-The business perspective.” Decision Support Systems, 51(1), 176-189. 2011

<著者紹介>



조 흥 재 (Heung-Jae, Cho)
 2001년 2월 : 수원대학교 응용통계학과 졸업
 2003년 2월 : 중앙대학교 통계학과 경제학 석사
 2012년 8월 : 서울과학기술대학교 IT정책대학원 공공정책 박사수료
 <관심분야> 클라우드 서비스, 클라우드 컴퓨팅, 정보보호, 인증, 표준, 지능형 로봇



민 영 기 (Young-Gi, Min)
 1999년 2월 : 서울시립대학교 도시공학과 졸업
 2009년 2월 : 서울시립대학교 경영대학원 경영학 석사
 2011년 3월~현재 : 서울과학기술대학교 IT정책대학원 공공정책 박사과정
 <관심분야> 클라우드 서비스, 클라우드 컴퓨팅, 정보보호, 인증, 지능형로봇