한국의 클라우드 서비스 인증제도와 미국의 FedRAMP의 비교 연구

서광규*

A Comparison Study between Korean Cloud Service Certification Systems and U.S. FedRAMP

Kwang-Kyu Seo*

요 약 최근 클라우드 서비스의 혁신은 정보통신기술에 기여한 가장 큰 잠재력을 가진 기술 중에 하나이다. 그러나 클라우드 서비스의 잠재력을 발휘하기 위해서는 서비스 제공자와 소비자관점에서 서비스의 보안, 성능, 가용성 등 다양한 이슈들에 대한 명확한 이해가 필요하다. 점점 더 많은 개인과 기업의 정보들은 물론 공공부문의 정보들도 클라우드 서비스에 놓이게 되면, 주된 관심은 어떻게 안전하고 신뢰할 수 있는 클라우드 서비스를 제공할 것인가에 맞추어지게 된다. 이러한 상황에 대응하기 위하여 한국에서는 클라우드 서비스 인증제도가 시행되고 있고 미국에서는 FedRAMP가 시행되고 있다. 본 연구에서는 두 인증제도의 비교분석을 수행하고 두 인증제도간의 차이점에 대하여 기술한다. 궁극적으로는 두 인증제도간의 비교연구 결과를 토대로 한국의 클라우드 서비스 인증제도의 발전방안에 대하여 제안한다.

주제어 : 클라우드 서비스, 인증제도, FedRAMP, 발전 전략

Abstract The evolution of cloud computing service over the recent years is potentially one of the major advances in information and communication technology. However, if cloud computing service is to achieve its potential, there needs to be a clear understanding of the various issues such as service security, performance and availability and so on, both from the perspectives of the providers and the consumers of the cloud service. As more and more information on individuals, companies and public sectors are placed in the cloud service, concerns are beginning to grow about just how safe and reliable an environment it is. In order to overcome these situations, the Korea cloud service certification system and U.S. FedRAMP were performed in each country. This paper aims at comparing and analyzing between Korean cloud service certification systems and U.S. FedRAMP and describing the difference between them. Eventually, we propose the improvement strategy of Korea cloud service certification systems based on the comparison results between them.

Key Words : Cloud Service, Certification System, FedRAMP, Improvement Strategy

1. 서 론

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[1, 2]. 또한 클라우드 서비스 기술이 기업의 IT인프라에 대한 유지보수 부담을 경감시키고, 사업초기 대규모 초기투자비용에 대한 부담도

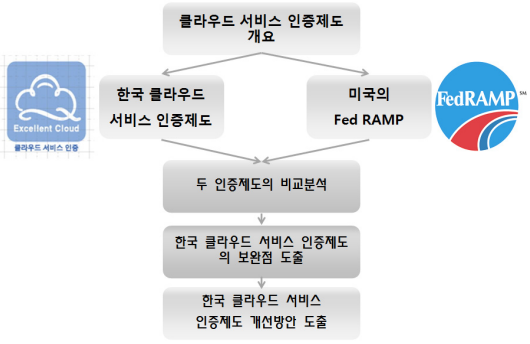
※ 본 논문은 2012년 한국산업경영시스템학회 추계학술대회 발표논문을 수정 및 보완하였음
*상명대학교 경영공학과 교수(교신저자)
논문접수: 2012년 10월 29일, 1차 수정을 거쳐, 심사완료: 2012년 11월 20일

경감시킬 수 있는 등 기업의 IT 혁신을 통한 비용절감을 이룰 수 있다는 기대로 관심이 증대되고 있다[3]. 이에 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 주력 사업으로 육성시킬 것임을 발표하고 있으며[4], 국내의 경우에도 KT, SKT, LGU+등 통신사업자를 비롯하여 NHN, 삼성 SDS 등 다양한 기업들도 클라우드 서비스 모델 및 사업전략을 발표하고 있다.

한국 IDC가 발표한 '2011 국내 기업 IT 수요 조사'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. 또한 최근 들어 공공 IT 자원의 민간 클라우드 전환에 대한 논의와 공공기관의 주도적인 민간 클라우드 이용에 따른 민간 클라우드 사업자 육성으로 국내 시장에 대한 경쟁력 강화 등 정부부처에서도 클라우드 이용 및 활성화를 위한 다양한 정책들을 펴고 있다. 그러나 클라우드 서비스가 공공부문 및 기업정보화 시장에서 신뢰기반을 형성하기 위해서는 해결해야 할 여러 가지 문제들이 있는데, 서비스 품질기준, 정보 보호, 권한남용방지 등의 법규와 서비스 도입을 위한 사전 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. 또한 공공부문에 클라우드 서비스가 적용되려면 보다 강화된 정부 차원의 클라우드 서비스의 인증이 필요하다.

이러한 요구사항을 반영하여 국내에서는 2011년에 방송통신위원회 중심으로 클라우드 서비스 인증제도가 개발되었고, 2012년에 민간중심의 클라우드 서비스 인증제도가 시행되어 2012년 6월에 제1호 인증기업이 발표되었다. 또한 미국에서는 FedRAMP(Federal Risk and Authorization Management Program)라는 클라우드 서비스 보안인증제도가 시행되고 있는데, 이는 미국의 클라우드 시장의 활성화를 위하여 정부 차원의 클라우드 인증제도이다.

본 연구에서는 한국의 클라우드 서비스 인증제도와 미국의 FedRAMP의 비교분석을 수행하고 두 인증제도 간의 차이점에 대하여 기술한다. 그리고 두 인증제도간의 비교연구 결과를 토대로 한국의 클라우드 서비스 인증제도의 발전방안에 대하여 제안하는데 이를 위한 연구 절차는 [그림 1]과 같다.



[그림 1] 제안하는 연구 절차

본 연구의 목적은 클라우드 서비스 이용자의 신뢰성을 제고하고 클라우드 서비스 시장의 조기 확산을 위하여 한국 클라우드 서비스 인증제도의 개선안을 도출하여 국내 인증제도의 고도화 방안을 모색하고, 이를 통하여 클라우드 서비스 및 사업자의 품질 수준, 안정성 및 보안성 등을 평가·인증하여 국내 클라우드 서비스에 대한 시장 수요의 확대 및 국내 클라우드 서비스의 국제 경쟁력 향상을 도모하고자 한다.

2. 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 서비

스 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: 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 있는 지도 서비스의 성능을 평가할 수 있는 주요 지표가 되고 있다.

추가적으로 클라우드 서비스 사용자 입장과 공급자 입장에서의 문제점을 살펴보면 클라우드 서비스에서의 사용자 및 공급자 보호 문제가 대두되는데, 클라우드 서비스의 활성화를 위해서는 클라우드 서비스에서의 사용자 보호 문제, 클라우드 서비스에서의 공급자 지원 및 보호 문제 등과 같은 문제들이 해결되어야 한다[5].

3. 한국의 클라우드 서비스 인증제도와 미국의 FedRAMP 비교 분석

3.1 한국의 클라우드 서비스 인증제도

한국의 클라우드 서비스 인증제도는 2012년 1월 방송통신위원회에서 클라우드 서비스 인증제를 발표하였고 클라우드 서비스 사업자로는 최초로 K사가 2012년 6월에 클라우드 서비스 인증을 획득하였다. 한국의 클라우드 서비스 인증제도는 클라우드 업체가 제공하는 서비스의 수준을 평가하여 필요한 체계 및 절차를 확보하고 있는 경우 인증을 부여하는 방식으로 한국클라우드서비스협회(KCSA)의 인증사무국에서 클라우드 서비스 품질, 보호, 기반 등 제공 분야를 심사하여 인증을 부여하는 민간 인증이다.

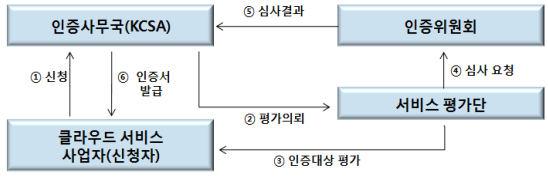
인증 대상은 클라우드 기술(가상화, 분산처리 등)을 활용하여, HW/SW 등 IT 자원을 인터넷에 접속하여 빌려 쓰고, 쓰는 만큼 이용료를 내는 서비스로써 클라우드 서비스 인증 신청 시점에 6개월 이상 서비스가 제공되고 있는 서비스를 그 대상으로 하며 현재에는 IaaS와 SaaS만을 인증 대상으로 한다. 그러나 기존의 단순한 웹 하드나 동영상 스트리밍 서비스는 인증 대상에서 제외하고 있다.

인증 심사 영역은 <표 1>에서 보는 바와 같이 3대 분야(품질, 정보보호, 기반) 7개 항목(가용성, 확장성, 성능/속도, 데이터 관리 보안, 서비스 지속성, 서비스 지원)으로 구성되어 있으며 총 세부 심사 항목은 IaaS 105개(필수 항목: 39개 항목), SaaS 85개 항목(필수항목: 33개 항목)으로 이루어 졌으며, 평가는 서면 및 실사 평가를 실시한다.

〈표 1〉 한국 클라우드 서비스의 인증 심사 영역

인증영역	세부인증영역
서비스 품질	가용성(Availability) 성능(Performance) 확장성(Scalability)
서비스 정보보호	데이터 관리(Data Management) 보안(Security)
서비스 기반	서비스 지속성(Continuity) 서비스 지원(Support)

인증 획득 기준은 전체 심사 항목의 70% 이상을 획득하면 되는데, IaaS는 74개 항목을 SaaS는 60개 항목을 충족하면서 동시에 필수 항목을 충족하면 인증을 획득하게 되며, 항목간의 가중치 없다. 한국 클라우드 서비스 인증 추진 체계는 [그림 2]와 같다.



[그림 2] 한국 클라우드 서비스의 인증 추진 체계

3.2 미국의 FedRAMP

2010년 11월, 미국 CIO 협의회는 미국 정부 클라우드 컴퓨팅에 대한 시큐리티 평가 인정에 관한 제안서인

“Proposed Security Assessment and Authorization for Cloud Computing”을 발표하였다. 이 제안서는 미국 정부의 클라우드 컴퓨팅에 대한 시큐리티 관리와 복수의 평가 인정 모델을 심사하기 위해 작성된 것으로 이 작업은 CIO 협의회가 연방 정부용에 대한 안전한 클라우드 컴퓨팅 서비스를 제공하려는 목적의 첫 단계이다.

또한 연방정부의 기준은 FISMA(Federal Information Security Management Act)와 NIST(National Institute of Standards and Technology)와의 특별한 문서에 의하여 규정되어 있다. 이 규정은 시큐리티 인가를 이용함과 동시에 정부의 투명성과 공정성을 제공하기 위해 한번 허가를 주어서 일제히 사용하게 하는 사용하고 있으며, 보다 간소하고 효율적으로 클라우드 컴퓨팅 시스템을 조달하는 것을 촉진하도록 하고 있다[6].

클라우드 컴퓨팅에 요구되는 시큐리티 기준(baseline)은 NIST SP 800-53 Ver3. 연방 정보시스템과 조직 적용 시큐리티 통제 문서에 포함된 시큐리티 통제 항목들이다. 저급(Low Level) 및 중정도(Moderate Level)의 영향을 미치는 클라우드 서비스에 있어서 baseline(최저 기준)이라고 할 만한 시큐리티 요건의 리스트를 제시하였다. 이 리스트는 NIST SP800-53Rev3 (SP800-53 Recommended Security Controls for Federal Information Systems and Organizations)을 근간으로 작성되었으며 다음의 분류에서 총계 187개 항목으로 구성되어 있다. 연방 정부가 조달하는 클라우드 서비스는 접근제어, 자기 계발, 감사와 설명 책임, 승인과 운용 인가, 구성 관리, 긴급 시 대응계획, 식별과 인증, 사고 대응(Incident Response), 유지보수(Maintenance), 기록 매체 보호, 물리적 환경 보호계획 작성, 개인 시큐리티(Personal Security), 위험 평가, 시스템과 서비스 조달 등과 같은 요건이 만족되도록 요구되고 있다.

FedRAMP에서는 계속적인 모니터링(Continuous Monitoring)을 수행하는데, 이의 목적은 시스템 개발 라이프 사이클에 동적이며 계속적인 감시 프로그램을 도입하는 것이다. 이것은 시큐리티 관리를 개발 기간 전체에 걸쳐서 효율적으로 하기 위한 것이다. 이 방법은 클라우드 컴퓨팅 환경에 대한 감시 프로그램의 변경과 수정을 행하는 능력도 포함하고 있다. 클라우드 서비스 공급자의 정의는 넓게 연방 정부가 Amazon, Microsoft、Salesforce.com와 같은 벤더가 지원하는 Public Cloud를 이용하는 가능성도 열어놓고 있다.

FedRAMP 및 클라우드 서비스 제공자에 의한 클라우드 컴퓨팅 시스템의 모니터링에 대해서 그 내용과 보고 회수를 제시하고, 보고 기준에 대해서는 FISMA의 기준과 정합성을 도모하고 있다. 다음의 항목의 보고로 구성되어 있다. 연방 정부가 조달한 클라우드 서비스는 이들 항목에 대해서 계속적인 모니터링을 실시하며 정기적으로 보고서를 작성하도록 요구되고 있다. 클라우드 서비스 공급자(Cloud Service Provider; CSP)는 정기적으로 다음과 같은 보고와 결과물을 제출하여야 한다.

1) 전시스템의 취약점 조사(패치 관리) 보고서(매월)
2) FDCC(Federal Desktop Core Configuration) 컴플라언스 준수 증명(매분기)
3) 긴급 시 대응 계획(매년)
4) Plan Of Action & Milestones 개선(매분기)
5) 변경 관리 프로세서 (매년)
6) 침투 테스트(매년)
7) 관리에 대한 제3자 검증 및 타당성 확인(6개월)
8) 스캔에 의한 경계 변경 없음의 확인(매분기)
9) 시스템 구성 관리 소프트웨어(매분기)
10) FISMA보고의 데이터(매분기)
11) 문서 경신(매년)
12) 긴급 시 대응계획과 테스트보고서(매년)
13) Duty Matrix 분리(직무 분장)(매년)
14) 정보보호 인식제고 및 트레이닝(매년)

FedRAMP의 목적은, 정부가 이용하는 정보시스템/서비스가 적당한 정보보호를 보증하는 것, 중복 노력을 배제하고 위험 관리의 비용을 절감하는 것, 연방 기관용의 정보 시스템/서비스를 신속하고 효율적으로 조달될 수 있도록 하는 것이며, 이에 따른 평가 · 승인 절차는 NIST가 책정한 위험 관리에 관한 문서 SP800-37Rev1을 기준으로 이 절차상의 FedRAMP 사무국, 클라우드 담당 기관(Sponsoring Agency), 클라우드 서비스 제공업자의 역할을 제시하고 있다.

이러한 목적 하에 FedRAMP의 평가 · 승인의 절차의 기본적인 흐름은 클라우드 서비스를 도입하려는 각 부청이 해당 클라우드 서비스의 담당 부청이 되어 FedRAMP에 클라우드 이용 신청을 행하며 FedRAMP가 해당 클라우드 서비스가 제반 기준을 만족하고 있는 지를 평가하여 기준이 만족하고 있다는 사실이 확인된다면 FedRAMP가 해당 클라우드 서비스의 이용을 승인하는

것이다. 또한, 담당 부청이 클라우드 서비스를 도입한 후에는 FedRAMP가 클라우드 서비스의 계속적인 모니터링을 감독한다[7].

3.3 두 인증제도의 비교분석

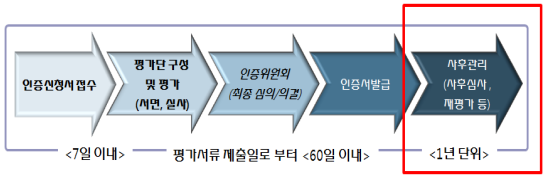
본 절에서는 전술한 바와 같이 한국의 클라우드 서비스 인증제도와 미국의 FedRAMP의 비교분석 결과를 토대로 두 인증제도간의 차이점에 대하여 기술한다.

먼저 두 인증제도의 인증 주체를 살펴보면 한국 클라우드 서비스 인증제도는 한국클라우드서비스협회(KCSA) 인증사무국에서 인증위원회를 두어 인증을 부여하는 민간인증인데 반하여 미국 FedRAMP는 미국 연방정부 인증이다.

두 번째 인증 대상을 살펴보면 한국 클라우드 서비스 인증제도는 IaaS와 SaaS 클라우드 서비스와 각 서비스 제공자를 인증대상으로 하나, FedRAMP는 클라우드 컴퓨팅 보안인증 프로그램으로 그 초점이 보안인증이다.

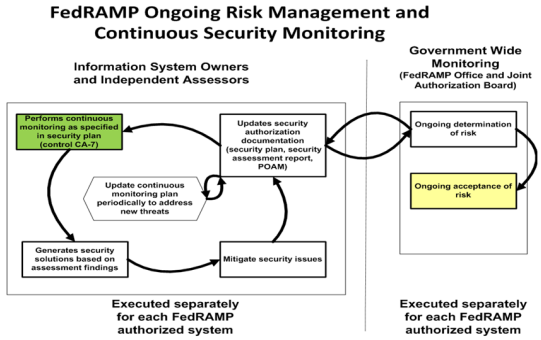
세 번째 두 인증제도가 모두 포함하고 있는 보안 인증 항목을 비교 분석하여 보면, 한국 클라우드 서비스 인증제도는 보안항목과 관련된 것이 총 10개 카테고리의 총 20개 항목으로 이루어져 있고, 미국 FedRAMP는 NIST SP800-53Rev3(SP800-53 Recommended Security Controls for Federal Information Systems and Organizations)을 근간으로 작성되었으며 총 187개 보안 항목으로 이루어져 있다.

마지막으로 보안 관리/감독 체계를 비교 분석하여 보면 한국 클라우드 서비스 보안 인증제도 추진 프로세스는 [그림 3]에서 보는 바와 같이 인증신청서를 접수하고 평가단을 구성하여 평가가 이루어지고 최종심의 및 의결이 인증위원회에서 이루어진다. 그 이후에 인증서를 발급하고 1년 단위로 사후관리가 이루어진다.



[그림 3] 한국 클라우드 서비스 인증제도의 추진 체계

이에 반해 미국의 FedRAMP의 관리/감독 체계는 [그림 4]와 같다. 미국의 인증체계는 세부적인 인가절차 및 체계적인 인증과정/표준화(문서화)가 이루어져 있고, 각 항목에 맞는 관리/감독 주기를 가지고 있으며 정부 차원의 폭 넓은 위험 관리 및 지속적인 보완 모니터링 체계를 가지고 있다.



[그림 4] 미국 FedRAMP의 위험 관리 및 지속적인 보안 모니터링 체계

이상에서 기술한 두 인증제도의 비교분석을 종합하여 정리하면 <표 2>와 같다.

〈표 2〉 두 인증제도간의 비교 분석

구분	한국의 클라우드 서비스 인증제도	미국의 FedRAMP
인증 주체	민간인증	연방정부인증
인증 대상	IaaS, SaaS 서비스와 서비스 제공자	클라우드 컴퓨팅 보안 프로그램
보안 항목	총 10개 카테고리의 총 20개 항목	총 187개 보안항목
보안 관리 체계	1년 단위로 전체 사후관리	각 항목에 맞는 서로 다른 관리/감독 주기 및 정부 차원의 지속적인 위험관리 및 보안 모니터링

4. 한국 클라우드 서비스 인증제도의 개선 방안

전장에서의 두 인증제도간의 비교 분석 결과를 토대로 한국의 클라우드 서비스 인증제도의 개선방안을 제시하면 다음과 같다.

먼저, 한국의 인증제도의 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 클라

우드 서비스 제공자 인증 모두의 영역에서 보안영역이 가장 중요한 항목이므로 이에 대한 가중치를 높이는 것이 필요하다. 그리고 실제로 인증심사를 실시하는 과정에서는 서류 심사의 비중보다는 실사 등의 비중을 높일 필요성이 있어 보이므로 이를 검토해 봄직하다.

두 번째는 한국의 클라우드 서비스 인증제도는 전술한 바와 같이 민간인증제도로 실효적인 측면에서 미국의 연방정부인증과 같은 실효성이 부족하다. 이는 향후 한국에서 공공부문에서 클라우드 서비스를 적용하려고 할 때에도 문제가 발생할 여지가 있다. 따라서 한국의 인증제도는 미국의 FedRAMP와 같이 국정원, 방송통신위원회, 지식경제부, 행정안전부 등 정부부처의 유기적인 협력과 역할분담으로 정부 인증제로의 고도화가 필요하다.

세 번째로는 전술한 바와 같이 클라우드 서비스에서는 무엇보다도 보안이 가장 중요한데, 한국 클라우드 서비스 인증제도는 미국 FedRAMP에 비해 보안 인증 심사 항목의 상대적으로 취약하다. 따라서 한국의 인증제도는 미국 FedRAMP를 벤치마킹하여 보안 인증심사항목을 강화하는 것이 필요하다.

마지막으로 미국 FedRAMP의 심사항목 및 심사과정, 모니터링 등은 모두 표준화 및 문서화되어 있는데 한국도 이를 좀 더 구체적으로 보완할 필요성이 있다. 그리고 미국 FedRAMP의 실행 가능한 계속적인 모니터링, 보고 횟수와 FISMA 규정을 준수하는 클라우드 컴퓨팅 제공업자를 위한 책임 등에 대한 명확한 절차 등의 내용을 보완 및 실행할 필요성이 있다. 추가적으로 잠재적 평가 및 인가 어프로치를 위한 위험 관리 프레임워크에 따르는 인가의 모든 입장, 인가 프로세서, 연방 기관과 클라우드 서비스 제공자를 위한 역할과 책임 등의 내용을 보완 및 실행하는 것도 필요하다.

5. 결 론

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 인증제도가 필요하다. 또한, 클라우드 서비스 비즈니스 모델에서는 다양한 형태의 서비스 공급자들이 포함됨에 따라, 각각의 서비스 공급업자들이 적절한 서비스 능력을 가지고 있는지에 대한 인증이 필요하다. 이러한 요구사항을 반영하여 국내에서는 2011년에 방송통신위원회 중심으로 클라우드 서비스 인증제도가 개발되었고, 2012년에 민간중심의 클라우드 서비스 인증제도가 시행되고 있다. 또한 미국에서는 연방 정부 주도의 FedRAMP라는 클라우드 서비스 보안인증제도가 시행되고 있는데, 이는 미국의 클라우드 시장의 활성화를 위한 정부 차원의 클라우드 인증제도이다.

본 연구에서는 한국의 클라우드 서비스 인증제도와 미국의 FedRAMP의 비교분석을 수행하였고, 인증제도간의 차이점에 대하여 기술하였다. 두 인증제도간의 비교연구 결과를 토대로 한국의 클라우드 서비스 인증제도의 발전방안을 제안하였는데, 한국 클라우드 서비스 인증제도의 경우 미국 FedRAMP에 비해 보안 인증 심사 항목의 취약하므로 보안 인증심사항목 강화하여 인증제도의 신뢰도 및 안정성 향상이 필요하다. 또한 현재에는 인증제도 획득시 클라우드 서비스 제공자들이 얻을 수 있는 혜택이 상대적으로 미흡하므로 현재의 인증 제도를 정부차원의 인증으로 고도화시키고, 인증획득 시 얻을 수 있는 다양한 정부차원의 혜택을 보완하여 인증 제도를 더욱 더 활성화하여 클라우드 산업을 활성화하는 것이 필요하다.

참 고 문 헌

[1] Marston, S. et al. (2011). Cloud computing - The business perspective, Decision Support Systems, 51(1), 176-189.

[2] Svantesson, D., Clark, R.(2010). Privacy and consumer risks in cloud computing. Computer Law & Security Review, 26(4), 391-397.

[3] Kim, H. K., Lee, Y. S. (2010). Status and Prospects of Cloud Computing Service. Information and Communication, 27, 31-34.

[4] Kim, C. H., Lee, W. J., Jung C. H. (2010). Research

Status of Cloud Computing. Journal of The Korea Society of Computer and Information, 18(1), 1-8.
[5] Seo, K.-K. (2011). A Framework for Establishing Cloud Service Certification Systems. Information Policy, 18(1), 24-44.
[6] FedRAMP JAB (2012). FedRAMP Baseline Security Control.
[7] FedRAMP GSA (2012). FedRAMP Concept of Operations.

서 광 규

・2002년 8월: 고려대학교 산업공학과 (공학박사)
・1997년 9월~2003년 2월: 한국과학기술연구원(KIST) 선임연구원
・2003년 3월~현재: 상명대학교 경영공학과 교수
・관심분야: 경영정보시스템, 클라우드 컴퓨팅, 디지털 산업정책, IT 융합 등
・E-Mail: kwangkyu@smu.ac.kr