클라우드 서비스와 SaaS의 법적 이슈*

Legal Issues on Cloud Computing Service & SaaS

손승우(Son, Seungwoo)**

목 차

* 이 글은 2010. 6. 26. “스마트 소프트웨어, SaaS의 법적 이슈”란 주제로 제14회 한국정보법학회 정기심포지움(스마트 인터넷과 법・제도)에서 발제한 글을 기초로 한 것으로, 2009. 12. “SaaS 산업 활성화를 위한 법적 과제”라는 주제로 「IT미디어법연구」 창간호(단국대학교 법학연구소 IT미디어법센터)에 게재한 글의 일부를 담아 최근의 논의를 상당부분 분석・발전시켜 작성되었음을 밝힙니다. 그리고 제14회 정기심포지움에서 토론에 참여해 주시고 좋은 의견과 새로운 시각을 제시해 주신 강현구 팀장님(정보통신산업진흥원), 김병일 교수님(한양대), 신현석 부장님(한국 MS 플랫폼 총괄사업부)께 감사드립니다.

** 단국대학교 법학과 교수, 법학박사(S.J.D.).

요 약

클라우드 컴퓨팅(cloud computing)은 복수의 중앙 집중화된 대형 데이터센터를 가상화 기술로 통합해 IT자원을 온디맨드로 제공하는 모델로서 이용자는 인터넷을 기반으로 소프트웨어 등 필요한 IT 자원을 소유하지 않고 빌려 사용하고 그에 따른 사용료를 지급하는 서비스를 말한다. 클라우드 서비스는 차세대 IT 서비스로서 IT 자원의 구매, 구축 및 컨설팅 비용을 절감할 수 있고, 웹과 스마트폰과 같이 모바일을 통해 애플리케이션과 데이터에 접근할 수 있는 장점이 있다. 그러나 이러한 클라우드의 장점은 단점이 되기도 한다. 즉 클라우드 서비스는 제3자의 망과 솔루션을 빌려 이용하는 모델이기 때문에 갑작스런 서비스 중단의 위험과 외부 서버에 보관된 고객의 데이터 보안 및 이용자의 개인정보 유출 가능성 등에 대한 불안이 존재한다.

우선 서비스 중단으로 인한 이용자의 데이터 손실의 위험을 해결하기 위해 클라우드 에스크로우(cloud escrow) 제도의 도입이 필요하다. 클라우드 에스크로우는 컴퓨터 프로그램 임치와 이용자 데이터의 실시간 백업을 핵심으로 한다. 또한 서비스 중단이 장기화될 경우를 대비해서 중단된 서비스를 일정기간 유지해 주는 방안도 생각해 볼 수 있다. 나아가 서비스를 중단하게 될 경우 클라우드 서비스사업자는 그 사실과 대책 등을 이용자들이 알 수 있도록 통지하여야 한다.

개인정보 보호와 관련해서는 현행 정보통신망법이 규율하고 있으나 클라우드 사업자가 제공하는 서비스 이용 기업이 서비스를 운용하고 고객의 개인정보를 취급하는 경우에는 클라우드 서비스 이용자인 기업은 동법상의 정보통신서비스 제공자가 아니므로 고객의 개인정보를 보호하기 위한 규정이 필요하다. 또한 데이터의 국외 서버 저장에 대해 준거법과 관할의 문제도 해결되어야 할 사항이다.

한편 클라우드 서비스의 활성화를 위해서는 표준 SLA(Service Level Agreement)과 이용자보호지침 등이 마련되어야 한다. 국제적 수준의 표준 SLA에는 클라우드 에스크로우의 활용, 개인정보 보호, 개인정보의 국외 이전, 데이터에 대한 권리귀속, 서비스 중단에 대한 통지의무 등의 조치, 중단된 서비스의 유지, 계약의 해제, 환불, 피해구제, 비밀유지의무, 보험 등에 관한 규정이 포함되어야 한다. 나아가 SLA에 포함될 사항들에 관한 법적 기준과 지원체계 등을 마련하기 위해서는 입법적 접근도 고려되어야 할 것이다. 그리고 클라우드 컴퓨팅 산업의 발전에 장애가 되는 법령들을 개선하여 금융・교육・의료 등 분야로 그 적용을 확대할 수 있도록 하고, 또한 일본, 영국, 미국 등과 같이 공공 전반에 클라우드 서비스가 확산될 수 있도록 정부의 중장기적 계획수립과 이를 위한 입법적 근거를 마련하는 것이 요구된다.

주 제 어

SaaS, 클라우드 컴퓨팅, 클라우드 서비스, 개인정보, 데이터 보호, 서비스 중단, 백업, 에스크로우(임치), 서비스수준협약(SLA)

Ⅰ. 클라우드 서비스와 SaaS의 개념

1. 클라우드 서비스와 SaaS의 정의

클라우드 컴퓨팅(cloud computing)은 복수의 중앙 집중화된 대형 데이터센터를 가상화 기술로 통합해 IT 자원을 온디맨드(on demand)로 제공하는 모델로서 이용자는 인터넷을 기반으로 소프트웨어 등 필요한 IT 자원을 구매하거나 소유하지 않고 빌려 사용하고 그에 따른 사용료를 지급하는 서비스를 말한다.[1] 컴퓨팅이 전기나 수도와 같이 이용자를 위한 유틸리티로 제공된다는 점에서 클라우드 컴퓨팅을 "클라우드 서비스(cloud service)"라고도 한다.[2]

이러한 클라우드 컴퓨팅 모델은 최근 점차로 다양화되고 있다. 예를 들면 소프트웨어를 서비스로 제공하는 SaaS(Software as a Service), 응용프로그램 개발 기반을 서비스로 제공하는 PaaS(Platform as a Service)[3], IT 인프라스트럭처를 서비스로 제공하는 IaaS(Infrastructure as a Service)[4], 개인 클라우드(Private Cloud), 공공 클라우드(Public Cloud), 하이브리드 클라우드(Hybrid Cloud), 멀티 클라우드(Multi Cloud) 등이 있다. 클라우드 서비스는 현재 생성단계에 있는 차세대 IT 서비스로서 클라우드 시스템내의 정보들을 결합하여 새로운 지식과 부가가치를 창출할 수 있는 새로운 패러다임으로 회자되고 있다.

한편 SaaS(Software as a Service)는 소프트웨어의 여러 기능 중에서 이용자가 필요로 하는 서비스만 이용 가능하도록 한 소프트웨어로서 소프트웨어 유통방식의 근본적인 변화를 설명하는 개념으로 공급업체가 하나의 플랫폼을 이용해 다수의 고객에게 소프트웨어 서비스를 제공하고 이용자는 이용한 만큼 비용을 지급한다.[5]

---

1) Gartner, Cloud Computing and SaaS, 2010. http://www.gartner.com, 검색일: 2010.8.20.

2) 국내 클라우드 서비스 활성화를 위해 2009년 3월 13일 한국클라우드 서비스협회의회(CSKI)가 출범된 바 있으며, 2010년 초에 정부(방송통신위원회) 차원의 추진단이 구성되어 운영되고 있다.

3) PaaS(Platform as a Service)는 다시 APaaS(Application Platform as a Service)와 AIaaS (Application Infrastructure as a Service)로 나눌 수 있다. http://itechthoughts.wordpress.com/2010/02/23/cloud-computing-the-new-it-paradigm, 검색일: 2010.8.1.

4) IaaS(Infrastructure as a Service)는 다시 DaaS(Desktop as a Service), NaaS(Network as a Service), CaaS(Communication as a Service)로 나눌 수 있다. IaaS의 예로서 Google 앱, Amazon의 Elastic Computer Cloud Service, S3(Simple Storage Service) 등이 있다.

즉, SaaS는 기존의 패키지 소프트웨어와 같이 제품을 구매하고 이를 컴퓨터에 설치하여 사용하는 형태가 아닌 인터넷을 기반으로 소프트웨어를 빌려 사용하는 서비스로서 클라우드 서비스의 한 모델이다.

SaaS는 기존의 ASP(Application Service Provider)와 같이 임대형 모델이라는 점은 동일하지만 ASP와 달리 멀티태넌트(Multi-Tenant) 개념에 의한 커스토마이징(customizing)이 가능하여 구축 및 유지보수 비용, 인건비 등의 비용 절감을 기대할 수 있다. 또한 최근에는 웹 3.0 환경에서 뿐만 아니라 스마트폰과 같은 모바일 기반에서도 사용할 수 있어 새로운 수익모델을 창출하고 있다. 클라우드 컴퓨팅은 하드웨어와 소프트웨어를 포함한 보다 광의의 IT 서비스모델로서 대기업이 이를 주도하는 반면[6], SaaS는 소프트웨어 중심의 중소기업에 의한 서비스가 많다는 점에서 차이가 있다.

기술적인 관점에서 클라우드 서비스와 SaaS는 엄밀히 구별되는 개념이지만 양자 모두 인터넷을 기반으로 고객이 필요로 하는 다양한 IT 서비스를 임대 방식으로 제공하고 있다는 점에서 동일하다.[7] 이로 인하여 서비스의 갑작스런 중단 위험, 고객 데이터의 손실, 개인정보 유출 등이 법적 쟁점이 대두되고 있다. 따라서 이하에서 양자의 공통된 주요 법적 이슈를 논함에 있어서 보다 광의의 개념인 클라우드 서비스라는 용어로 통칭하고 필요한 경우에만 양자를 구별하여 사용하겠다.

2. 클라우드 서비스의 장단점

(1) 클라우드 서비스의 장점

클라우드 컴퓨팅은 소프트웨어 등 개개의 IT 자원을 이용자가 직접 구축하지 않고서도 제3자의 인프라를 이용하여 구름(cloud)을 형성한 듯 마치 자신의 컴퓨터처럼 자유롭게 사용할 수 있는 분산 컴퓨터 환경이므로 구매, 구축 및 컨설팅 비용을 절감

---

5) 위키피디아 백과사전, http://en.wikipedia.org/wiki/SaaS, 검색일: 2010.6.19. ; 한국정보통신기술협회, 『정보통신용어사전』, 2008.

6) 해외 주요 클라우드 서비스 사업자인 Amazon, Google, Apple, IBM, Intel, Del・HP, Microsoft 등은 다양한 모델개발로 세계 시장을 선점해 가고 있는 반면, 국내 주요 사업자인 KT, SKT, 삼성, LG 등은 클라우드 컴퓨팅 시장에 대한 초기투자 단계에 있다.

7) David Narkiewicz, *Legal Tech Forecast: Cloudy, with only a Chance of Purchasing New Software*, 32 Pennsylvania Lawyer 56, 56 (March/April, 2010).

할 수 있고, 네트워크를 통해 인프라스트럭처(infrastructure), 애플리케이션(application), 데이터(data) 등에 어디서나 접근이 가능하여 관리가 용이하므로 변화하는 비즈니스 요구에 신속하게 대처할 수 있는 등의 장점을 지니고 있다. 현재 클라우드 서비스는 新성장 산업으로서 산업전반으로 그 활용이 확대되고 있다. SaaS의 경우 회계, 고객서비스(Help Desk), 고객관계관리(Customer Relationship Management: CRM), 인사서비스(HR), 이메일, 주소록, 자동비용청구(Computing Billing and Invoice), 급여 시스템, 일정관리, 오피스 프로그램 등의 분야를 중심으로 활용되고 있다.[8)]

전 세계적으로 클라우드 서비스와 같이 주문형(on-demand) 방식의 서비스에 대한 기업의 호응이 점차로 증가하고 있으며 국내에서도 클라우드 서비스 산업의 활성화를 위해 정부와 민간 차원의 협력을 강화하고 있다. THINKstrategies의 조사에 따르면 약 1/3에 해당하는 기업들이 on-demand 소프트웨어를 이미 채용하고 있으며 43%는 SaaS를 고려 중에 있는 것으로 나타났다.[9)] 그리고 아시아 태평양 지역 기업의 경우 75%가 올해 말까지 SaaS에 대한 투자를 늘릴 것으로 전망되고 있다.[10)] 또한 가트너(Gartner)는 2011년까지 새로운 비즈니스 소프트웨어의 25%가 SaaS로 이동할 것으로 전망하였다.[11)] 그 밖에도 IDC 조사에 따르면 주문형 소프트웨어 시장의 수익이 2006년에 36억 달러에서 2011년까지 연평균 성장률(CAGR)이 32%로 성장하여 148억 달러에 달할 것으로 전망하고 있다.[12)] 또한 IDC는 향후 5년간 클라우드 서비스에 대한 지출이 급증하여 2009년 174억 달러의 시장이 2012년에는 420억 달러에 이를 것으로 전망하고 있으며, IT시장에서 차지하는 비율도 2008년 9%에서 2012년 25%로 상승할 것으로 예측하고 있다.[13)]

---

8) SaaS를 사용하고 있는 250개 기업을 대상으로 한 설문조사 결과. Information Week 2007년 4월호. SaaS의 대표적인 기업으로는 세일즈포스닷컴(Salesforce.com), 구글(Google), 마이크로소프트(Microsoft), SAP 등이 있다.

9) 2006 THINKstrategies/Cutter Consortium Survey. <http://www.thinkstrategies.com>, 검색일: 2010. 6. 20.

10) "아태지역 기업 75%, SaaS 투자 늘릴 것", 전자신문, 2010.6.15. 시장조사기관 가트너는 '2010년 아태지역 SaaS 전망'을 통해 조사 기업 중 80%가 전사자원관리(ERP), 고객관계관리(CRM) 등의 기업 애플리케이션을 SaaS로 사용하고 있다고 밝혔다.

11) Gartner Dataquest, November 2006.

12) IDC, Worldwide Software on Demand 2007-2011 Forecast, April 2007.

13) IDC's New IT Cloud Services Forecast: 2009-2013.

(2) 클라우드 서비스의 단점

웹 또는 모바일 기반의 임대형 서비스는 동전의 양면처럼 클라우드 서비스의 장점이 곧 단점으로 작용하기도 있다. 우선 클라우드 서비스는 제3자의 망과 솔루션을 빌려 이용하는 모델이기 때문에 갑작스런 서비스 중단 위험과 고객의 데이터를 외부 서버에 보관하고 있다는 막연한 불안감이 존재하게 된다. 특히 중소기업이 대부분을 차지하는 SaaS 시장에서 이러한 SaaS의 태생적 한계를 어떻게 해결하느냐에 따라 이 산업의 성공여부가 결정될 것이다.

둘째, 클라우드 서비스 이용자는 개인정보의 유출 가능성에 불안감을 떨치기 힘든 반면, 사업자는 네트워크 해킹과 같은 사이버테러로 인한 개인정보의 유출이나 불가항력적 재해로 인한 데이터 손실에 대한 위험을 안고 있다. 이러한 문제는 기술적 보안과 함께 법적 장치의 마련이 검토되어야 할 것이다.

셋째, 앞서 밝힌 클라우드 서비스의 여러 장점으로 인하여 최근 그 적용영역이 점차로 확대되고 있음에도 불구하고 대부분의 활용은 일정한 민간영역에 머물고 있다. 공공영역에서 예산절감을 할 수 있는 클라우드 서비스 모델을 받아들이지 못하는 이유는 앞서 지적한 클라우드 서비스의 단점 때문이기도 하지만 사실상 플랫폼을 보유하고 있는 신뢰성 있는 국내 기업이 존재하지 않는다는 것이 큰 이유이다. 또한 금융・교육・의료 등 새로운 분야에 클라우드 서비스를 적용하고자 함에 있어서 관련 법령이 장애 요소로 작용하는 경우도 있다.

이 밖에도 국내에서는 클라우드 “서비스 수준협약(Service Level Agreement: “SLA”)”이 표준화되어 있지 않아 서비스 이용자의 보호책이 미흡하고, 클라우드 서비스산업을 진흥하기 위한 법・제도적 환경과 기술적・물리적 기반들이 충분히 갖추어져 있지 않은 상태이다.

이하에서는 이러한 클라우드 서비스의 한계점을 중심으로 클라우드 서비스 사업자의 법적 지위와 주요 법적 이슈를 검토해 보고 그 해결방안을 제시하여 클라우드 서비스산업의 활성화에 기여하고자 한다.

Ⅱ. 서비스 중단과 데이터 보안

1. 데이터 보안의 필요성

클라우드 서비스를 이용하는 기업이 가장 우려하는 것은 서비스의 갑작스런 중단으로 인한 이용자 데이터의 훼손이나 멸실이다. 특히 SaaS는 웹기반에서 소프트웨어를 서비스 형태로 제공하므로 컴퓨터프로그램과 고객 데이터를 항시 지속적이고 안정적으로 사용하게 해주는 것이 서비스의 핵심이다. 이와 같이 클라우드 서비스는 고객이 적시에 정보시스템에 접근하여 서비스를 효율적으로 이용할 수 있는 "가용성(availability)"을 갖추고 있어야 한다.[14] 서비스의 효율적인 운용은 물론 사고나 재앙이 발생하더라도 신속하고 완전하게 복구할 수 있어야 한다.

그런데 만일 SaaS 서비스 제공자가 폐업, 파산, 천재지변, 재해 등의 사유로 이용자에게 서비스를 더 이상 제공하지 못할 경우 당해 서비스 이용자들은 갑작스런 서비스 중단으로 큰 피해를 입을 수 있다. 이는 기업의 규모가 클수록 시스템의 안정성 보장이 요구되는데, 이를 보장하지 못할 경우에는 막대한 경영상의 손실을 입게 되고 심각한 경우에는 기업의 영업기반까지 흔들리게 될 수 있다. 특히 SaaS 업체의 경우 대부분 중소기업이 많아 대기업에 비해 파산・폐업 등에 노출될 가능성이 높아 서비스의 안정적 사용을 보장할 방안이 필요하다.

클라우드 서비스 중단 시 피해를 최소화하기 위해 서비스 업체간 상호 호환성이 문제된다. 즉 서비스를 제공하는 업체가 부도・폐업 등으로 인해 서비스를 중단하는 경우에도 서비스 이용 업체는 다른 유사 클라우드 업체를 선정하여 동일한 서비스를 제공받을 것이 예상되는데, 이 때 서비스 업체간 시스템이 호환되지 않으면 기존 클라우드 서비스에 의해 생성되었던 데이터를 사용할 수 없으므로 무용지물이 될 것이다.

클라우드 서비스의 중단 사례를 살펴보면, 구글의 클라우드 컴퓨팅 기반 서비스인 검색부터 구글 뉴스, 구글 앱스 등이 불통되는 사고가 최근 몇 차례 발생하여 이용자들에게 큰 불편을 초래하였으며, 이를 업무적으로 이용하고 있던 사람들에게도 막대한 손실을 발생시켰다. 또한 최근 Microsoft社의 모바일 기기인 '사이드킥'[15]에서 제공하는 클라우드 서비스의 심각한 오류로 인하여 2009년 10월 초부터

---

14) 1992년 11월에 발표된 OECD 보안가이드라인(Guidelines for the Security of Information Systems)에서 보안의 개념으로 가용성(availability), 완전성(integrity), 기밀성(confidentiality)을 들고 있다. Working Party on Information Security and Privacy, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, OECD, 2005, at 3-4.

데이터 손실과 접속장애가 계속됨에 따라 Microsoft社는 사이드킥의 판매를 당분간 중단한다고 발표한 바 있다. 그러나 더욱 심각한 것은 손실된 데이터의 복구가 불가능할 것으로 예상되면서 서비스 이용고객으로부터 거센 항의가 제기되어 세계적인 기업의 명성에 손상을 입게 되었다.[16]

또한 파일 공유를 위한 사회 네트워크 서비스 및 온라인 스토리지 서비스를 제공하고 있던 "The Linkup"은 2007년 6월 15일 시스템 관리자의 과실로 약 350만 고객의 데이터가 삭제되어 고객 정보의 45% 가량을 유실하고, 2008년 8월 결국 사업을 폐쇄하기에 이르렀다.[17] 그러나 더 큰 문제는 서비스 제공사와 스토리지 업체가 책임을 서로에게 떠넘길 뿐 고객 정보의 손실에 대한 책임을 아무도 지지 않았다는 것이다.[18]

2. 서비스 중단의 대비방안

(1) 클라우드 에스크로우

클라우드 서비스의 갑작스런 중단으로 인한 이용자 데이터의 손실을 방지할 방안으로서 미국, 유럽 등 주요국을 중심으로 최근 활용되고 있는 클라우드 에스크로우(Cloud Escrow)를 고려해 볼 수 있다. 클라우드 에스크로우는 기술임치(technology escrows)의 한 종류이다. 기술임치란 시스템의 유지보수, 기술탈취방지, 담보, 기술이전 등의 목적을 위하여 기술보유기업이 스스로 또는 기술의 사용기업과 합의하여 SW 소스코드, 도면, 매뉴얼 등 영업활동에 유용한 기술상 또는 경영상 정보를 신뢰성이 있는 제3의 기관(임치기관)에 보관하고, 계약상 일정한 조건이 발생하면 임치물을 특정 상대방에게 교부해 주는 제도이다.[19]

---

15) 사이드킥 서비스는 이용자의 주소록과 일정표, 사진 등 각종 데이터를 단말기 자체 대신 인터넷에 연결된 서버에 저장해 기기가 바뀌어도 언제든 데이터를 볼 수 있게 해 주는 서비스를 말한다.

16) "MS 망신살… 사이드킥 고객 데이터 몽땅 날아가", 한국경제, 2009.10.13.

17) The Linkup은 사건이 발생한 이후 일부 데이터를 복원하기는 하였지만 약 20,000여명의 유료 이용자가 음악, 사진, 비디오 등 디지털 편집물을 잃게 되었다.

18) 위키피디아 백과사전, http://en.wikipedia.org/wiki/The_Linkup 검색일: 2010.6.18.

19) 보다 자세한 내용을 위하여, 손승우, "기술임치제도에 관한 고찰", 「중앙법학」 제9집 제2호, 2007.8.31, 721면; 기술자료임치제도, 대·중소기업협력재단, 2008; 국신욱, "기술자료 임치제도(Escrow)의 법률적 고찰", 연세대학교 법무대학원 석사학위논문, 2008.2.

기술임치와 관련된 국내 제도는 2003년 「저작권법」 (구 컴퓨터프로그램보호법)에 도입된 "프로그램임치(소프트웨어 임치)"[20]와 2007년 「대·중소기업 상생협력 촉진에 관한 법률」(이하 "상생법"이라 한다)에 도입된 "기술자료 임치제도"[21]가 있다. 전자는 소프트웨어 이용자의 안정적인 기술사용을 보장한 제도로 프로그램 저작권을 보유하고 있는 기업이 이용권자를 위하여 소스코드, 매뉴얼 기타 관련 자료를 신뢰성 있는 제3의 기관에 보관해 두었다가 저작권자의 폐업 등으로 인하여 유지·보수를 계속할 수 없게 되는 등 계약상의 일정한 조건이 발생한 경우 당해 기관이 소스코드 등을 사용권자에게 교부함으로써 사용권자는 안전하고 지속적으로 소프트웨어를 사용할 수 있다. 반면, 후자의 경우는 수·위탁 거래관계에서 위탁기업이 거래상 우월적 지위를 이용하여 수탁기업으로부터 지적재산권을 탈취하거나 기술정보의 제공을 강요하는 등의 불공정 거래관행을 시정할 목적으로 도입되었다.

클라우드 에스크로우를 도입하기 위해서는 서비스에 사용되는 애플리케이션(applications) 임치뿐만 아니라 이용자의 데이터에 대한 실시간 백업(real time back-up)이 요구된다. 현재 한국저작권위원회와 대·중소기업협력재단은 애플리케이션의 소스코드 등 자료만을 임치하고 있고 데이터 백업을 위한 시설이나 지원체계를 갖추고 있지 못하다. 클라우드 에스크로우는 특정 시점의 소프트웨어의 소스코드 및 기술자료 뿐만 아니라 서비스를 통해 생성되는 이용자의 데이터도 임치를 한다는 점에서 기존의 기술임치와 차이가 있다.[22]

그리고 고객의 데이터는 저작권법상 데이터베이스에 해당될 수 있다. 왜냐하면 데이터베이스를 구성하고 있는 소재의 선택·배열 또는 구성 그 자체가 창작성을

---

20) 저작권법 제101조의7 제1항에서 "프로그램의 저작재산권자와 프로그램의 이용허락을 받은 자는 대통령령으로 정하는 자(이하 이 조에서 "수치인"이라 한다)와 서로 합의하여 프로그램의 원시코드 및 기술정보 등을 수치인에게 임치할 수 있다."고 규정하고 있으며, 제2항에서 "프로그램의 이용허락을 받은 자는 제1항에 따른 합의에서 정한 사유가 발생한 때에 수치인에게 프로그램의 원시코드 및 기술정보 등의 제공을 요구할 수 있다."고 규정하고 있다.

21) 대·중소기업 상생협력 촉진에 관한 법률 제25조 제12호에서 위탁기업이 정당한 사유없이 수탁기업의 기술자료를 요구하는 행위를 준수사항의 하나로 규정하고, 제24조의2 제1항에서 "수탁기업과 위탁기업은 전문인력 및 설비 등을 갖춘 기관으로서 대통령령으로 정하는 제3의 기관(이하 "임치기관"이라 한다)과 서로 합의하여 기술자료를 임치기관에 임치할 수 있다."고 규정하고 있다.

22) 손승우, "SaaS 산업 활성화를 위한 법적 과제", 56면.

지니고 있다면 그 데이터베이스는 편집저작물로서 보호받을 수 있고, 그렇지 못한 경우라도 데이터베이스의 제작 또는 그 소재의 갱신・검증 또는 보충에 인적 또는 물적으로 상당한 투자를 하였다면[23] 일정한 보호를 받을 수 있다.[24] 따라서 프로그램임치의 대상과 고객의 데이터베이스는 모두 저작권법의 보호 대상에 포함된다.

따라서 클라우드 에스크로우는 기존의 소프트웨어임치의 기능에 더해서 예기치 못한 서비스 중단에도 고객의 데이터를 보호해 줄 수 있는 유용한 수단을 제공한다. 즉 클라우드 서비스는 소프트웨어를 빌려 쓰는 모델이기 때문에 소프트웨어와 데이터를 자사 내부에 두고 있지 않으므로 서비스를 제공하는 기업이 폐업, 파산 등을 하는 경우 고객은 서비스를 더 이상 이용하지 못할 뿐만 아니라 자신의 중요한 데이터를 분실하게 될 위험이 존재한다. 이러한 위험에 대처하기 위한 클라우드 에스크로우는 클라우드 애플리케이션뿐만 아니라 이용자의 데이터에 대한 관리가 동시에 이루어진다.[25]

한편, 현재 국내 클라우드 서비스 업체들은 고객의 데이터에 대한 백업지원을 일정부분 제공하고 있으나 대부분은 시간적 공백이 있거나 일정하지 않은 백업 서비스를 제공하고 있다. 이에 반해, 해외 클라우드 임치기관의 경우 예기치 못한 클라우드 서비스의 중단에 대비하여 클라우드 애플리케이션뿐만 아니라 고객의 데이터를 실시간(real time)으로 자동 백업해 주는 서비스를 제공함으로써 고객이 원거리에서도 자신의 데이터에 언제든지 접근할 수 있도록 한다.[26]

앞서 언급한 바와 같이, 국내 영세한 클라우드 서비스 사업자의 경우 자체적인 이용자 보호체계를 충분히 갖추지 못하고 있는데 이로 인한 고객 데이터 손실사건

---

23) 저작권법 제2조 제20호.

24) 데이터베이스 제작자에게는 당해 데이터베이스의 전부 또는 상당한 부분을 복제・배포・방송 또는 전송할 권리를 부여하고 있고(저작권법 제93조), 데이터베이스제작자의 권리는 데이터베이스의 제작을 완료한 때부터 발생하며, 그 다음 해부터 기산하여 5년간 존속한다(저작권법 제95조).

25) THINKstrategies, A Whitepaper for SaaS Customers and Vendors, Iron Mountain <www.thinkstrategies.com>

26) 미국의 Iron Mountain사는 웹기반의 SW 실시간 서비스인 SaaS의 안정적인 사용을 보장하기 위하여 2007년부터 'SaaSProtect Escrow Service'를 제공하고 있다. Iron Mountain사의 LiveVault는 수많은 고객과 서버를 보호하기 위하여 200TB이상의 데이터를 관리하고 있다. http://www.ironmountain.com, 검색일: 2010.6.10. 영국의 최대 기술임치회사인 NCCGlobal사도 최근 SaaS Escrow서비스를 제공하고 있다.

이 계속하여 발생한다면 고객의 피해는 물론 나아가 클라우드 서비스 자체에 대한 신뢰를 손상시킬 수 있다. 따라서 정부는 이러한 문제를 해결하기 위해 우수한 중소 클라우드 서비스 기업을 발굴하고 클라우드 에스크로우를 지원하기 위한 체계 및 법적 근거를 마련하도록 할 필요가 있다.

(2) 중단된 서비스의 유지

클라우드 임치와 함께 클라우드 서비스 중단의 장기화로 인해 발생할 수 있는 이용자의 큰 피해를 최소화하기 위한 방안이 모색되어야 한다. 그 하나의 방안으로서 클라우드 서비스가 중단되더라도 이를 일정기간 유지해 주는 방법을 고려해 볼 수 있다. 예컨대, 미국의 EscrowTech社는 클라우드 서비스의 중단을 대비하여 데이터 실시간 백업은 물론 시스템을 동일한 환경으로 이중 보관해 주는 서비스를 제공하고 있다.[27] 따라서 고객의 데이터가 업데이트될 때마다 백업이 자동적으로 이루어지고, 서비스가 장기적으로 중단되더라도 백업시스템에 의해 일정기간 서비스를 제공할 수 있다.

이와 같이, 클라우드 서비스의 중단 사유가 발생한 경우에도 당해 서비스를 일정기간 지속해 줄 수 있다면 이용자의 손해를 효과적으로 예방할 수 있을 뿐만 아니라 클라우드 서비스에 대한 신뢰성을 제고시켜 관련 산업의 활성화에 기여할 수 있을 것이다. 이 밖에도 서비스 중단에 앞서 이용자에게 서비스 중단에 대한 통지를 의무화하고, 정부의 지원으로 서비스 중단 시 동종 서비스 사업자로 하여금 일정 기간 당해 서비스를 유지하게 하는 방안을 생각해 볼 필요가 있다.[28] 그러나 이를 위해서는 클라우드 서비스 플랫폼 및 미들웨어 등이 표준화되어 상호 호환성이 있어야 하는데 국내 클라우드 서비스 환경은 아직 그러한 체계를 갖추고 있지 못하다. 이 또한 국내 시장이 해결해야 될 과제이다.

---

27) 필자는 2009년 11월 유타주 린든시에 소재한 EscrowTech社(http://www.escrowtech.com)를 방문하여 Jon Christiansen 사장을 면담하였다. 보다 자세한 내용을 위하여, 손승우 "기술자료 임치제도 법·제도적 개선을 위한 조사·연구", 대·중소기업협력재단 연구보고서, 2009.12. 참조. 이하 중단된 서비스의 유지와 관련된 내용은, 손승우·김태열·지석구, "SW 산업의 신성장을 위한 "SaaS 임치"의 도입 방안", 「법학논총」 제33권 제2호, 단국대학교 법학연구소, 2009.12.30, 93-94면 참조.

28) 손승우·김태열·지석구, 위의 글, 93-94면 참조.

Ⅲ. 클라우드 서비스와 정보보호

1. 법적 지위

클라우드 서비스를 제공함에 있어서 고객의 개인정보가 클라우드 사업자의 서버에 저장되므로 개인정보의 처리와 관련된 법규와의 관계를 검토할 필요가 있다. 개인 또는 회사의 정보유출을 규율하는 법률로서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다), 「공공기관의 개인정보보호에 관한 법률」, 「전자금융거래법」, 「부정경쟁방지 및 영업비밀 보호에 관한 법률」(이하 "부정경쟁방지법"이라 한다) 등이 있다.

우선 클라우드 서비스 사업자는 「전기통신사업법」에 따른 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자에 해당하므로 정보통신망법 제2조제3호상의 정보통신서비스 제공자이며 정보통신망법상의 개인정보보호에 관한 규정의 적용을 받는다.[29] 그런데 IaaS와 같이 서버·스토리지·네트워크 등 인프라스트럭처를 제공하는 자가 「전기통신사업법」 제4조제2항의 기간통신사업자가 되는지가 문제된다. 비록 IaaS가 네트워크 등 인프라 자원을 제공하지만 이는 클라우드 서비스제공자로서 초고속 정보통신망을 기반으로 서비스를 제공하는 것이므로 「전기통신사업법」상 부가통신사업자에 해당된다고 볼 수 있다.[30] 따라서 클라우드 사업자가 정보통신망법 제22조에 따라 개인정보를 이용하려고 수집하는 때에는 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다.

그리고 동 법상 "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상

---

29) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 3. ""정보통신서비스 제공자"란 「전기통신사업법」 제2조제1항제1호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다."

30) 전기통신사업법 제4조(전기통신사업의 구분 등)
① 전기통신사업은 기간통신사업, 별정통신사업 및 부가통신사업으로 구분한다.
② 기간통신사업은 전기통신회선설비를 설치하고, 이를 이용하여 공공의 이익과 국가산업에 미치는 영향, 역무의 안정적 제공의 필요성 등을 참작하여 전신·전화역무등 대통령령이 정하는 종류와 내용의 전기통신역무(이하 "기간통신역무"라 한다)를 제공하는 사업으로 한다.
- 제3항 생략 -
④ 부가통신사업은 기간통신사업자로부터 전기통신회선설비를 임차하여 제2항의 규정에 의한 기간통신역무외의 전기통신역무(이하 "부가통신역무"라 한다)를 제공하는 사업으로 한다.

등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말하므로(동법 제2조제6호) 자연인이 아닌 법인의 정보는 동법의 보호대상이 되지 못한다. 이 경우 기업의 정보가 부정경쟁방지법상 영업비밀에 해당하는 경우에는 이 법에 의해 별도의 보호를 받을 수 있다.[31]

그런데 클라우드 사업자가 서비스를 직접 제공하지 않고 고객인 기업이 서비스를 빌려 그 기업의 최종이용자에게 서비스를 제공하는 경우가 있을 수 있다. 만일 클라우드 서비스 고객사가 정보통신망법상 정보통신서비스 제공자에 해당되지 않는 경우에는 비록 그 기업이 최종이용자의 개인정보를 취급하는 경우라도 동법의 적용을 받지 않으므로 개인정보 보호에 사각이 발생한다.[32] 따라서 이러한 문제를 해결하기 위한 입법적 대책이 필요하다. 이와 관련하여 행정안전부가 입법예고한 개인정보보호법안[33]이 이러한 결점을 보충해 줄 수 있을 것으로 본다.

2. 클라우드 서비스와 개인정보 보호

기업이 고객 개인정보를 클라우드 서비스제공자로 하여금 처리하게 하는 경우 기업은 자사 고객의 개인정보가 어떻게 관리되는지 알기 어려우므로 클라우드 사업자에 대한 일정한 관리·감독 책임을 부담하는데 어려움이 있다. 「EU 개인정보보호지침」 (EU Data Protection Directive)에서는 기업이 개인정보관리자(Data controller)로서 자신이 정한 정보처리 목적과 방법에 따라 정보주체의 개인정보를 직접 취급하는 클라우드 서비스제공자의 행위에 대해 관리·감독 책임을 진다.[34]

---

31) 「부정경쟁방지 및 영업비밀 보호에 관한 법률」 제2조제2호에서 영업비밀이란 "공연히 알려져 있지 아니하고 독립된 경제적 가치를 가지는 것으로서 상당한 노력에 의하여 비밀로 유지된 생산방법, 판매방법 기타 영업활동에 유용한 기술상 또는 경영상의 정보를 말한다."고 규정하고 있다. 따라서 영업비밀로서 보호받기 위해서는 비공지성, 비밀관리성, 경제적 유용성, 기술상 또는 경영상의 정보 등의 요건을 만족해야 한다.

32) 이민영, "클라우드 컴퓨팅 법제 관련 검토의견", 클라우드컴퓨팅 법제연구반 제3차 회의 자료, 한국인터넷진흥원, 2010.6.7.

33) 개인정보보호법안의 필요성에 대하여 2008년부터 논의되어 왔지만 개인정보보호위원회 독립 문제가 걸림돌이 되어 정부와 국회 간의 대립이 해결되지 못한 채 현재까지 제정이 늦춰지고 있다.

34) ENISA, "Cloud Computing : Benefits, Risks and Recommendations of Information Security", 2009.11.9, 103; 한국인터넷진흥원, 클라우드 컴퓨팅의 법적 이슈, 2010.3.9, 11면.

또한 정보통신망법 제46조제1항에서 “타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(이하 “집적정보통신시설 사업자”라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다.”고 규정하고 있다. 클라우드 서비스 사업자는 타인의 정보통신서비스 제공을 위하여 직접된 정보통신시설을 운영·관리하는 사업자에 해당될 수 있으므로 정보통신시설에 대한 접근 통제 및 각종 재해 및 테러 등 위협으로부터 정보통신시설을 보호하기 위한 물리적·기술적 조치 등을 취해야 한다.[35]

또한 동조 제2항에서 “집적정보통신시설 사업자는 집적된 정보통신시설의 멸실, 훼손, 그 밖의 운영장애로 발생한 피해를 보상하기 위하여 대통령령으로 정하는 바에 따라 보험에 가입하여야 한다.”고 규정하고 있다. 따라서 클라우드 사업자는 집적된 정보통신시설인 클라우드 컴퓨팅 시스템의 멸실, 훼손, 그 밖의 운영장애로 발생한 이용자의 피해를 보상하기 위하여 서비스 개시와 동시에 책임보험에 가입하여야 한다.[36]

한편, 해외 클라우드 서비스의 경우 개인정보가 특정 국가 또는 여러 곳에 분산되어 저장될 수 있는데, 개인정보의 국외 이전에 대해 국가별로 상이한 규제를 두고 있다. 대표적인 클라우드 서비스 기업인 세일즈포스닷컴(Salesforce.com)의 경우

---

35) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제37조제1항에서 “타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(이하 "집적정보통신시설사업자"라 한다)가 법 제46조제1항에 따라 정보통신시설의 안정적 운영을 위한 보호조치는 다음 각 호와 같다.

1. 정보통신시설에 대한 접근 권한이 없는 자의 접근 통제 및 감시를 위한 기술적·관리적 조치
2. 정보통신시설의 지속적·안정적 운영을 확보하고 화재·지진·수해 등의 각종 재해와 테러 등의 각종 위협으로부터 정보통신시설을 보호하기 위한 물리적·기술적 조치
3. 정보통신시설의 안정적 관리를 위한 관리인원 선발·배치 등의 조치
4. 정보통신시설의 안정적 운영을 위한 내부관리계획(비상시 계획을 포함한다)의 수립 및 시행
5. 침해사고의 확산을 차단하기 위한 기술적·관리적 조치의 마련 및 시행

36) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 제38조제1항에서 “집적정보통신시설사업자는 법 제46조제2항에 따라 사업 개시와 동시에 책임보험에 가입하여야 한다.”고 규정하고 제2항에서 사업자가 가입하여야 하는 책임보험의 최저보험금액을 별표로 정하고 있다.

3개의 IDC를 미국 내에 분산하여 설치하고 주된 서버와 백업서버 등의 기능을 각각 수행하여 데이터를 이중 보관하고 있다.[37]

우리나라의 경우 정보통신망법 제63조제2항에서 정보통신서비스 제공자 등이 이용자의 개인정보를 국외로 이전하려면 개인정보의 항목, 이전되는 국가, 이전 일시 및 방법 등에 관한 사항을 이용자에게 사전에 고지하고 동의를 받아야 한다고 규정하고 있다.[38] 따라서 합법적인 해외 클라우드 서비스를 이용할 경우에는 이용자의 동의를 획득하기 때문에 문제가 되지 않으나 계약상 지정된 국가 외의 지역으로 이전하거나 백업하는 경우에는 별도의 동의를 받아야 할 것이다. 그러나 현재 클라우드 서비스의 SLA에서 고객 정보나 데이터의 보관 장소 및 이전 등에 관하여 표시하지 않거나 상세히 규정하지 않은 경우가 많다.

「EU 개인정보보호지침」에서는 개인정보의 제3국으로의 이전을 원칙적으로 금지하고 예외적으로 EU위원회 또는 회원국이 상대국에서 개인정보가 적절한 수준으로 보호된다고 결정하는 경우에는 이전이 허용된다.[39]

이와 관련하여, 서버를 해외에 두고 서비스를 제공하는 클라우드 사업자가 수집한 개인정보를 제3자에게 유출하는 경우 현실적으로 그 증거를 확보하기란 매우

---

37) 세일즈포스社는 샌프란시스코 인근에 주된 IDC를 두고, 다른 두 IDC에 백업센터 및 DR(Disaster Recovery)센터를 두고 있으며, 모든 데이터를 실시간으로 미러링(mirroring)하여 보관하고 있다.
http://blogs.salesforce.com/features/2006/03/mirrorforce.html 검색일 : 2009.11.20.

38) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제63조 ① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니 된다. ② 정보통신서비스 제공자등은 이용자의 개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다. ③ 정보통신서비스 제공자등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.
1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

④ 정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

39) EU 개인정보보호지침(Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data) 제25조제1항. 박훤일, "EU 개인정보보호지침의 역외적용", 「통상법률」 통권 43호, 107면, 2002.2.

어려운 일이다. 이를 해결하기 위해서 밀러링(mirroring)[40] 백업서버를 국내에 두도록 하는 방안을 생각해 볼 수 있다. 밀러링 시스템을 갖추고 있을 경우 고객이 데이터를 수정할 때마다 동일한 데이터가 다른 저장장치에 이중으로 보관되므로, 만일 클라우드 서비스 사업자가 수집한 개인정보를 국외로 유출할 경우 수사당국은 밀러링 서버를 통해 정보유출 사실의 증거를 확보할 수 있다. 그러나 밀러링 시스템의 설비・장치 및 운용에 있어서 많은 비용이 드는 문제가 있으므로 일정 규모 이상의 고객을 확보하고 있는 사업자에 대해서만 동 시스템을 갖추도록 하거나 사업자로 하여금 국내 통합전산센터를 활용하도록 유도할 필요가 있다.

한편 중소 클라우드 사업자에게 고가의 백업시스템을 의무화하는 것은 바람직하지 않으므로 우수 중소사업자를 발굴하여 일정한 지원을 제공하는 것이 국내 클라우드 서비스산업의 활성화에 도움이 될 것이다. 이는 앞서 상술한 클라우드 에스크로우 제도와 밀접한 관련이 있으므로 연계하여 고려되어야 한다.

그리고 데이터의 국외 서버 저장에 대해 준거법과 관할의 문제도 해결되어야 할 사항이므로 추가적인 연구가 필요하다고 본다.[41]

Ⅳ. 클라우드 서비스의 적용확대

1. 공공분야

클라우드 서비스의 다양한 장점에도 불구하고 그 적용범위는 제한적이다. 우선 클라우드 서비스 이용자 대부분이 중소기업에 해당한다. 대기업은 세일즈포스닷컴과 같은 소수의 클라우드 서비스업체를 제외하고 클라우드 서비스 보안성과 안정성에 대한 불안감으로 다른 클라우드 서비스 업체를 신뢰하지 않는 듯하다.[42] 특히 이러한 문제는 공공영역에서 두드러지게 나타나고 있다. 클라우드 서비스가 예산절감에 효과가 있음에도 불구하고 공공기관은 자신의 정보를 원격지에 위치한 서

40) 미러링(mirroring)이란 장비의 고장, 천재지변 등 사고로 인하여 데이터가 손실되는 것을 막기 위하여 데이터를 하나 이상의 장치에 중복 저장하는 것을 말한다.

41) 클라우드 서비스에 있어서 개인정보 보호에 관하여, 우성엽, "클라우드 컴퓨팅과 관련된 법적 쟁점",「Law & Technology」제6권 제3호, 2010.5.

42) 한국소프트웨어진흥원, "SW의 서비스화에 따른 시장전망과 정책방향", 정책보고서, 2007, 78면.

버에 저장하는 것을 불안해 한다. 더욱이 신뢰성 있는 플랫폼을 보유하고 있는 클라우드 서비스 업체 대부분이 외국계라는 점도 이러한 문제를 더욱 어렵게 만든다.

정부는 「2008년도 예산안편성 및 기금운용계획안 작성 지침」을 개정하기 이전까지 소프트웨어를 유형 물품으로 보고 패키지형태의 소프트웨어만을 조달대상으로 삼았기 때문에 SaaS 형태의 소프트웨어 사용은 불가능하였다. 그런데 기획재정부(구 기획예산처)가 2008년 지침을 개정하면서 "ASP서비스 이용에 따른 임차료" 항목을 새롭게 포함시키면서 공공기관도 클라우드 서비스를 사용할 수 있게 되었고, 서비스 사용료를 매월 지불하는 통신비와 같이 회계 처리할 수 있게 되었다.[43]

그러나 클라우드 서비스에 대한 인식이 여전히 사회 전반적으로 부족하므로 공공영역에 대한 홍보와 교육이 강화될 필요가 있고, 나아가 동 산업의 활성화를 위해 엄격한 보안성을 요하지 않는 업무영역부터 클라우드 서비스 모델을 도입해 나가는 방안을 모색해 볼 필요가 있다. 이러한 점에서 일본 우정본부가 상당한 논의와 이해를 거쳐 우정사업 관리시스템 일부에 클라우드 서비스를 도입한 사례[44]와 미국의 "스토어프런트", 영국의 G-클라우드, 일본의 "가스미가세키 프로젝트" 등 공공 전반에 클라우드 서비스를 도입하기 위한 중장기 계획 등을 참고해 볼 수 있을 것이다.[45]

나아가 행정안전부가 운영하고 있는 '정부통합전산센터'[46]를 통하여 공공분야에 필요한 클라우드 서비스를 개발하여 그 적용을 확대하는 방안도 고려해 볼 수 있다. 이를 위해서는 현재 부처별로 관리하고 있는 서버 등 자원을 클라우드 컴퓨팅 환경에 맞는 통합시스템을 구축함으로써 전자정부 클라우드를 촉진하는 것이 중요하다. 또한 위에서 논의한 클라우드 서비스의 안전성, 보안, 시스템 호환, 개인정보 보호 등의 동일한 문제를 해결해야 한다.

2. 금융・의료・교육 분야

---

43) 기획예산처, "2008년도 예산안편성 및 기금운용계획안 작성 지침", 2007.10, 150면.

44) 손승우, "SaaS 산업 활성화를 위한 법적 과제", 66면.

45) 일본 스마트 클라우드 연구회 보고서, 스마트 클라우드 전략, 2010.5.; "클라우드컴퓨팅 시장 물꼬 틀까", 머니투데이, 2009.12.30.

46) 정부통합전산센터는 2002년 범정부적 효율적인 운영을 위한 혁신방안(BPR)에 따라 2005년 11월 설치되었다.

공공분야와 마찬가지로, 금융・의료・사이버대학 분야에서도 관련 법령의 규제로 인하여 경제적 효용성이 높은 클라우드 서비스 도입에 상당한 제약을 받고 있다.

우선, 금융기관이 미션 크리티컬(mission critical)한 시스템에 클라우드 컴퓨팅을 적용하기란 결코 쉬운 일이 아니다. 예컨대, 「전자금융거래법」과 「전자금융감독규정」에서 금융감독원장에게 위임한 사항과 그 시행에 필요한 사항을 규정한 「국내 전자금융관리규정 시행세칙」 제7조 제11항에 따르면 "국내에 본점을 둔 금융기관의 전산실 및 재해복구센터는 국내에 설치할 것"으로 규정하고 있다. 즉 금융기관 또는 전자금융업자는 반드시 Host 서버 및 관련 기기를 국내에 두어야 하므로 해외 특정국에 서버를 두고 있는 주요 클라우드 서비스의 경우 국내 금융시스템에 도입할 수 없다. 금융기관은 매년 금융감독원으로부터 감사를 받는데, 이를 위반할 경우 신규업무에 대해서 일정기간 동안 인허가를 불허할 수 있고, 또 대표이사의 연임을 불허할 수도 있다. 물론 국내에 서버를 둔 클라우드 서비스의 경우에는 동 세칙의 적용을 받지 않는다.

그런데 일부 동남아시아 국가를 제외하고, 미국, 일본, 유럽 등 주요 선진국에서 금융 전산실의 위치를 국내로 제한하는 규정을 둔 경우가 많지 않으며, 관련 규정을 두고 있는 경우라도 효율적인 시스템의 도입을 위하여 그 규정을 합목적적으로 해석하거나 사회적 합의를 통해 클라우드 서비스를 도입하고 있다.

둘째, 사이버교육 분야에 있어서도 클라우드 서비스를 도입하는데 관련 법령이 장애가 되고 있다. 원격대학을 위한 평생교육시설의 설비를 규정한 「평생교육법 시행령」[47] 제54조 제2항에서 "원격대학 형태의 평생교육시설은 각종 서버, 통신장비 및 매체제작장비 등 원격교육에 필요한 설비를 확보하여야 한다."라고 규정하고 있어 자가시스템을 의무화하고 있다. 따라서 이 규정은 컴퓨팅 자원을 빌려 사용하는 클라우드 서비스의 사이버교육 분야로의 진출을 가로막고 있다.

셋째, 위의 문제는 「의료법」[48]에서도 찾아 볼 수 있다. 즉 의료법 제23조 제1항에서 의료기관은 진료기록부 등을 「전자서명법」에 따른 전자서명이 기재된 전자문서로 작성・보관할 수 있는데, 이 경우 동조 제2항에서 의료기관은 전자의무기록을 안전하게 관리・보존하는 데에 필요한 자가 시설과 장비를 갖추도록 규정하고 있다.

클라우드 서비스산업이 주요 선진국에 비해 활성화되지 못하는 이유는 클라우드

47) 「평생교육법 시행령」, 대통령령 제22269호, 2010. 7.12, 타법개정.

48) 「의료법」, 법률 제10387호, 2010. 7.23, 일부개정.

서비스 보안성과 안정성에 대한 신뢰도가 부족한 것이 가장 크지만 이용기업이 자신의 데이터를 원격지에 있는 타인의 서버에 보관해 둔다는 막연한 불안감과 사회적으로 보편화되지 못한 서비스에 대한 경험부족도 원인이 되고 있다. 또한 앞서 살펴본 바와 같이, 클라우드 서비스 산업이 성장하는데 관련 법령이 걸림돌이 되기도 한다.[49] 따라서 이를 극복하기 위해서는 기술개발 노력과 함께 기존의 법·제도를 새로운 IT 환경에 맞도록 개선하는 노력도 기울여야 할 것이다. 이를 통하여 클라우드 서비스의 적용확대와 산업의 발전을 기대할 수 있다.

Ⅴ. 맺음말 : 법적 해결방안

이상의 논의를 종합해 볼 때, SaaS 등 클라우드 서비스 산업이 정부의 육성책에 힘입어 성공적으로 시장을 형성하고, 나아가 국가 경쟁력을 제고하는데 실질적으로 기여하기 위해서는 관련 기술 및 서비스 모델 개발과 아울러 입법적 지원책이 필요하다. 위에서 상술하지 않았지만 클라우드 서비스 산업진흥을 위해서는 기술 및 다양한 모델개발, 보안, 인증, 표준화, 전문 인력양성, 사업자 교육 및 모니터링, 불필요한 규제 법령 정비, 비밀준수의무 등 다양한 이슈들을 포함해야 한다. 이상에서 검토한 내용을 바탕으로 클라우드 서비스에서 들어난 법적 과제를 해결하기 위해 몇 가지 해결방안을 제시하면 다음과 같다.

첫째, “표준 클라우드 서비스 수준협약(SLA)” 및 “클라우드 이용자보호지침”의 제정이 필요하다. 현재 국내에서는 클라우드 서비스를 위한 표준 SLA가 존재하지 않으므로 클라우드 서비스산업이 활성화될 경우 불필요한 분쟁과 사회적 비용이 증대될 수 있다.[50] 따라서 국제적 수준의 표준 SLA의 마련이 요구되는데, 표준 SLA에는 가동률, 클라우드 임치제도의 활용, 개인정보 보호, 개인정보의 국외 이전, 데이터에 대한 권리귀속[51], 서비스 중단에 대한 통지의무, 서비스복구시간 등 조치, 중단된 서비스의 유지, 계약의 해제, 환불, 피해구제, 비밀유지의무 등에 관한 규정이 포함되어야 한다. 또한 클라우드 서비스사업자의 자율적 준수를 유도할

49) “의료기관·사이버대학은 클라우드 `컴퓨팅 사각지대`”, 전자신문, 2010.8.25 자 기사.

50) 미국은 IT 관련 협회 주도로, 일본은 정부 주도로 표준 SLA 제정을 추진해 왔다.

51) 서비스사업자가 서버를 임대하는 경우에는 IDC 사업자의 서버에 보관되므로 클라우드 사업자의 폐업·파산 시에 이용자 데이터를 되돌려 받기가 용이하지 않은 문제가 있다. 따라서 데이터에 대한 명확한 귀속 관계를 규정할 필요가 있다.

수 있는 클라우드 서비스이용자 보호지침의 제정도 요구된다. 이를 위해서는 관련 법률에 표준 SLA 및 이용자보호지침의 제정에 관한 법적 근거를 마련할 필요가 있다.

둘째, 클라우드 에스크로우 및 서비스 중단에 따른 지원체계를 마련하기 위한 법적 근거를 마련할 필요가 있다. 즉 일정 규모 이상의 클라우드 서비스사업자에 대해서는 사용자의 데이터 보호방안으로서 클라우드 에스크로우를 의무화시키고, 중소 클라우드 서비스 사업자에 대해서는 실시간 백업 등 일정한 지원을 제공함으로써 고객 데이터 보호는 물론 클라우드 서비스에 대한 신뢰성을 제고시키는 방향으로 정책을 정하는 것이 바람직하다.

셋째, 서비스 중단에 대한 통지의무를 둘 필요가 있다. 클라우드 사업자가 서비스를 중단하게 될 경우 그 사실을 이용자들이 알 수 있도록 통지를 의무화하여야 한다. 통지는 이용자들이 서비스 중단에 실질적으로 대비할 수 있도록 사업자가 인식하는 즉시 이루어져야 하며 그 방법과 내용이 명확하여야 한다. 또한 중단의 기간과 피해보상 및 대책 등에 관한 내용도 함께 통지되어야 한다. 이와 관련해서, 「전기통신사업법」 제27조제1항에서 부가통신사업자가 그 사업의 전부 또는 일부를 휴지 또는 폐지하고자 하는 때에는 그 휴지 또는 폐지예정일 30일전까지 그 내용을 당해 역무의 이용자에게 통보하고 방송통신위원회에 신고하도록 한 규정을 참고할 수 있다.

넷째, 다양한 클라우드 서비스 모델에 따라 개인정보 보호의 사각지대가 발생하지 않도록 법제도 개선이 필요하다. 특히 클라우드 서비스를 직접 이용하는 고객이 그 서비스를 운용하면서 고객정보를 다루는 경우에도 충분한 개인정보 보호가 이루어져야 한다. 또한 해외 서버를 통해 개인정보가 유출되는 경우 최소한의 증거를 확보할 수 있도록 일정 규모이상의 사업자에게 밀러링(mirroring) 백업서버를 국내에 갖추도록 하거나 사업자로 하여금 국내 IDC를 활용하도록 유도할 필요가 있다.

다섯째, 클라우드 서비스의 신뢰성을 높이고 불측의 데이터 손실에 대비하기 위하여 보험제도의 도입을 생각해 볼 수 있다. 미국 대부분의 SaaS 등 클라우드 데이터 임치기관들은 애플리케이션 관련 임치물과 데이터 손실에 대비하여 높은 수준의 보험에 가입하고 있다. 그러나 우리나라의 경우 이러한 종류의 보험제도가 확립되어 있지 않아 현실적인 어려움이 존재한다. 보험가입은 문제의 근본적인 해결책은 아니지만 사후구제 방안으로 고려해 볼 수 있으며 표준 SLA 및 관련 법령에

포함되어야 할 것이다.

끝으로, 경제적 효율성 등이 높은 클라우드 서비스의 활성화를 선진국 수준으로 끌어올리기 위해서는 클라우드 서비스에 대한 신뢰성을 높일 수 있도록 정부의 솔선수범이 필요하다. 앞서 살펴본 바와 같이, 클라우드 컴퓨팅 산업의 발전에 장애가 되는 법령들을 개선하여 금융・교육・의료 등 분야로 그 적용을 확대할 수 있도록 하고, 나아가 일본, 영국, 미국 등과 같이 공공 전반에 클라우드 서비스가 확산될 수 있도록 정부의 중장기적 계획수립과 이를 위한 입법적 근거를 마련하는 것이 요구된다.

* 논문최초투고일: 2010년 6월 26일; 논문심사(수정)일: 2010년 7월 21일; 논문게재확정일: 2010년 8월 20일

참 고 문 헌

1. 국내문헌

국신욱, “기술자료 임치제도(Escrow)의 법률적 고찰”, 연세대학교 법무대학원 석사 학위논문, 2008.2.

기획재정부, “2008년도 예산안편성 및 기금운용계획안 작성 지침”, 2007.10.

대·중소기업협력재단, 기술자료임치제도, 2008.

박훤일, "EU 개인정보보호지침의 역외적용“, 「통상법률」 통권 43호, 2002.2.

손승우, “기술임치제도에 관한 고찰”, 『중앙법학』, 제9집 제2호, 2007.8.31.

_____, “SaaS 산업 활성화를 위한 법적 과제”, 「IT미디어법연구」 창간호, 단국대학교 법학연구소 IT미디어법센터, 2009.12.

_____, “기술자료 임치제도 법·제도적 개선을 위한 조사·연구”, 대·중소기업협력재단 연구보고서, 2009.12.

손승우·김태열·지석구, “SW 산업의 신성장을 위한 "SaaS 임치”의 도입 방안”, 「법학논총」 제33권 제2호, 단국대학교 법학연구소, 2009.12.30.

이민영, “클라우드 컴퓨팅 법제 관련 검토의견”, 클라우드컴퓨팅 법제연구반 제3차 회의 자료, 한국인터넷진흥원, 2010.6.7.

일본 스마트 클라우드 연구회 보고서, 스마트 클라우드 전략, 2010.5.

우성엽, “클라우드 컴퓨팅과 관련된 법적 쟁점”, 「Law & Technology」 제6권 제3호, 2010.5.

한국소프트웨어진흥원, “SW의 서비스화에 따른 시장전망과 정책방향”, 2007.

한국인터넷진흥원, 클라우드 컴퓨팅의 법적 이슈, 2010.3.9.

한국정보통신기술협회, 『정보통신용어사전』, 2008.

“아태지역 기업 75%, SaaS 투자 늘릴 것”, 전자신문, 2010.6.15 자 기사.

“의료기관·사이버대학은 클라우드 `컴퓨팅 사각지대`”, 전자신문, 2010.8.25 자 기사.

“클라우드컴퓨팅 시장 물꼬 틀까”, 머니투데이, 2009.12.30 자 기사.

“MS 망신살… 사이드킥 고객 데이터 몽땅 날아가”, 한국경제, 2009.10.13 자 기사.

Information Week 2007년 4월호.

2. 외국문헌

IDC Software as a Service Adoption Study, 2005.

David Narkiewicz, Legal Tech Forecast: Cloudy, with only a Chance of Purchasing New Software, 32 Pennsylvania Lawyer 56 (March/April, 2010).

ENISA, “Cloud Computing : Benefits, Risks and Recommendations of Information Security”, 2009.11.9.

Gartner Dataquest, November 2006.

Gartner, Cloud Computing and SaaS, 2010. http://www.gartner.com

IDC, “Worldwide Software on Demand 2007-2011 Forecast”, April 2007.

IDC's New IT Cloud Services Forecast: 2009-2013.

OECD, Working Party on Information Security and Privacy, The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries, 2005.

THINKstrategies, A Whitepaper for SaaS Customers and Vendors, Iron Mountain, http://www.thinkstrategies.com

위키피디아 백과사전, http://en.wikipedia.org/wiki/The_Linkup

_____, http://en.wikipedia.org/wiki/SaaS

세일즈포스사 홈페이지, http://blogs.salesforce.com/features/2006/03/mirrorforce.html

Abstract

SaaS(Software as a Service), referred to as software on demand, is a method of software deployment over the Internet in that a software vendor provides subscription-based, web-hosted software. Neither the software nor the data is loaded on the consumer's hardware. Today, more SaaS providers are putting their Web-based business application on a widening number of mobile devices including a handheld smartphone. From legal standpoint, cloud computing is the same as SaaS, which is also refers to data and software applications that are housed in cyberspace instead of residing on servers or PCs physically located in users.

In spite of many benefits of the cloud service, it also has drawbacks. The primary concern is if the service provider you decide to use goes out of business, there is a risk because it is managed by the provider and the data is stored at the central server. The best way to solve this problem is a cloud service escrow, which protects user's data in the event of the service provider's bankruptcy. The cloud escrow includes not only a deposit account for the source codes but also real-time back-up systems for data, so that securing access to the data can be ensured. In addition, it can prevent serious damages caused by longer discontinuity of the service, by taking over operation of application by someone other than the provider.

Second, certain situation of cloud service does not qualify for the Korean Online Privacy Protection Law. For example, a cloud provider's terms of service agreement may be the only privacy protections applicable to its customers who operate a cloud service for their customers(end-users). Also, choice of law and jurisdiction for oversea server is an issue to be solved.

In order to revitalization of cloud computing market, this article suggests all issues above have to be solved by legislative methods including governmental regulations and supports for small & medium business. Korean government should also provide a standard service level agreement (SLA) and guideline for user protection. The SLA should include desirable standards on privacy protection, data protection such as cloud service escrow, oversea transmission of individual information, notification duty and actions for discontinuity of the service, ownership of data, remedies, insurance, etc. Moreover, Korean government should reform laws and regulations that interfere with extension of cloud computing service to the areas such as finance, cyber education and medical service.

Keywords: SaaS(Software as a Service), Cloud Computing, Cloud Service, Escrow, Personal Information, Data Back-Up, Security, Service Level Agreement