情 報 保 護 學 會 誌
第20卷 第2號, 2010. 4

클라우드 컴퓨팅의 안전한 이용과 활성화를 위한 법적 과제

이 창 범*

요 약

클라우드 컴퓨팅 서비스의 많은 장점에도 불구하고 아직 기업들이 서비스의 가용성 및 데이터 보안, 자사 데이터에 대한 통제권 확보, 종속성 등의 문제로 클라우드 컴퓨팅 서비스의 이용을 꺼리고 있다. 이 같은 문제들은 기술개발, 표준화, 표준약관, 서비스수준협약(SLA) 등으로 어느 정도 해결이 가능하다. 그러나 데이터가 여러 국가에 복제되어 분산 저장될 경우 데이터의 국외이전 금지 문제, 데이터의 보관 및 파기 의무, IT 컴플라이언스, 수탁자의 불법행위에 대한 위탁자의 책임, 자신의 데이터센터에 저장된 불법정보에 대한 클라우드 서비스제공자의 책임범위, 클라우드 서비스제공자의 책임제한 등 현행법상의 법적 규제와 충돌되는 부분에 대해서는 법·제도적 접근과 검토가 필요하다.

클라우드 컴퓨팅 산업의 촉진 및 이용 활성화를 위해서는 구체적으로 다음과 같은 사항이 법제도적으로 검토되어야 한다. ① 클라우드 서비스나 솔루션을 시험할 수 있는 테스트베드 구축 등 시범사업 근거 마련, ② 분야별 특화된 클라우드 서비스 모델 개발 및 사업화를 위한 정부 시책 추진 및 지원 근거 마련, ③ 민·관의 포괄적 협력 기반 조성 및 정부의 기술 개발·연구 지원체계 마련, ④ 사전 인증 및 사후 보증체계 구축을 통한 클라우드 서비스의 신뢰성 및 안정성 제고, ⑤ 클라우드 서비스의 상호운용성 확보를 위한 표준화, ⑥ 클라우드 컴퓨팅의 정보보안, 개인정보보호 등 각종 법률 이슈와 예상되는 다양한 이해관계 충돌 문제에 대응할 수 있도록 서비스제공자와 이용자 대상의 지침 근거 마련, ⑦ 클라우드 속에 있는 기업의 정보자산에 대한 접근권 보장, ⑧ 정보자산의 실제 위치와 선택권 보장, ⑨ 정보자산의 부적절한 접근 방지와 오남용 방지, ⑩ 클라우드 서비스 제공기업 또는 서비스 자체의 영속성 보장, ⑪ 서비스 장애 책임범위와 분담, ⑫ 소프트웨어 라이선스 등에 대한 규정이 고려되어야 한다.

Ⅰ. 서 론

1.1 클라우드 컴퓨팅의 의의

클라우드 컴퓨팅(Cloud computing)이 정보사회의 새로운 패러다임으로 부각되고 있다. 클라우드 컴퓨팅은 스토리지(Storage), 서버, 데이터베이스, 소프트웨어, 정보(information) 등 각종 IT자원을 인터넷을 통해 온디맨드(on demand) 방식으로 이용자에게 제공하는 인터넷기반의 컴퓨팅이다. 클라우드 컴퓨팅 사업자는 IT자원의 소유권을 이용자에게 판매하는 것이 아니라 다양한 형태의 IT자원을 구비해 두고 필요한 만큼 이용자에게 "사용권"을 대여하거나 이용자의 사무(事務)나 정보를 "수탁"받아 관리 또는 처리해주는 서비스를 제공한다.

지금까지는 기업이든 정부든 또는 개인이든 업무에 필요한 IT자원을 대부분 구매해서 사용해야 하였지만, 클라우드 컴퓨팅 환경에서는 IT자원을 그때그때 필요한 만큼 사용료를 주고 빌려 쓰면 된다. 즉 IT자원의 사용 관행과 인식이 소유에서 공유의 개념으로 바뀌게 된다. 그런 의미에서 클라우드 컴퓨팅은 패러다임의 큰 변화라고 해도 좋을 것이다. 그래서 혹자는 클라우드 컴퓨팅을 하나의 기술이라기 보다는 새로운 IT 소비 트렌드를 표현하는 개념이라고 보기도 한다.

사실 그동안에도 몇몇 대형 인터넷 데이터센터(IDC)들과 호스팅사업자들이 개별 기업이나 개인이 직접 소유·운영하기에는 부담이 큰 서버 및 통신 장비와 전문 보안 시설·인력 등을 갖추어 놓고 인터넷을 통해 기업 및 개인 이용자에게 전산 설비나 네트워크 설비를 임대하거나 이용자의 설비를 유치하여 유지·보수 등의 서비스를 제공하는 사업을 해왔다. 그러나 클라우드 컴퓨팅 환경에서는 스토리지 대여나 서버 대여 이외에 소프트웨어, 플랫폼 등 각종 IT서비스가 전면적·종합적으로

* 한국인터넷진흥원 법제분석팀장 (miso4all@naver.com)

제공되며 기업이나 정부뿐만 아니라 개인에게까지 서비스의 범위가 확대된다.

이와 같이 클라우드 컴퓨팅 환경에서는 자사 업무 처리는 물론 고객 서비스 제공에 이용되는 모든 IT자원의 성능, 품질, 보안 등의 문제가 클라우드 컴퓨팅 사업자의 손에 달려있고 그에 대한 의존도가 높기 때문에 다양한 법적인 문제가 야기된다.

1.2 클라우드 컴퓨팅의 발달

클라우드 컴퓨팅의 개념에 대한 역사는 1960년대까지로 거슬러 올라간다. 1960년 존 맥카시(John McCarthy)는 "컴퓨테이션이 언젠가는 공공시설처럼 조직될 것이다(computation may someday be organized as a public utility)"라고 말한 바 있는데 여기서 우리는 클라우드 컴퓨팅에 관한 개념의 시초를 찾을 수 있다. 사실 클라우드 컴퓨팅은 1960년대에 미국에서 사용료를 받고 자신의 시설이나 설비를 다른 사람들이 이용할 수 있게 제공했던 사업들과 유사한 특징을 공유하고 있다.

"클라우드"라는 용어도 기존의 사설망 서비스와 통신의 품질은 비슷하지만 훨씬 저렴한 비용으로 서비스 제공이 가능한 가상사설망 서비스(VPN, Virtual Private Network)에서 차용해 온 것이다. VPN은 전용망이 아닌 인터넷망을 이용하기 때문에 별도로 값비싼 장비나 소프트웨어를 구입하고 관리할 필요가 없어 기존의 사설망 연결방식보다 비용이 대폭 절감되며, 또한 네트워크의 대역폭을 보다 효율적으로 활용할 수 있게 해 준다(위키피디아).

아마존은 닷컴 버블 이후 자신의 데이터 센터를 현대화함으로써 클라우드 컴퓨팅의 발전에 중요한 역할을 했다. 아마존의 데이터 센터도 대다수 다른 컴퓨터 네트워크와 마찬가지로 때때로 갑자기 증가하곤 하는 트래픽에 대비하여 자신의 자원을 10% 정도만 활용하고 나머지는 유휴자원으로 남겨두었다. 그러나 아마존은 새로운 클라우드 아키텍쳐가 현저한 내부 효율성 개선 효과를 가져온다는 사실을 발견하고 2005년부터 자사의 유휴자원을 활용해 유틸리티 컴퓨팅 기반 위에서 자사 웹 서비스를 통해 일반에게 클라우드 컴퓨팅 서비스를 제공하기 시작하였다.

이어서 2007년부터는 구글, IBM, 그리고 다수의 대학들이 대규모 클라우드 컴퓨팅 연구 프로젝트에 착수하고 있다.

1.3 클라우드 컴퓨팅의 유형

클라우드 컴퓨팅 서비스는 다양한 기준에 따라 유형화가 가능하나 여기서는 서비스의 내용에 따른 유형과 서비스의 대상·범위에 따른 유형으로 나누어 살펴보고자 한다.

먼저 클라우드 컴퓨팅 서비스는 서비스의 내용에 따라 크게 인프라 서비스(IaaS, Infrastructure as a service), 플랫폼 서비스(PaaS, Platform as a service), 소프트웨어 서비스(Software as a service)로 구분할 수 있다. 인프라 서비스(IaaS)는 서버, 스토리지, 네트워크 등 인프라스트럭처를 가상화 환경으로 만들어 필요에 따라 인프라 자원을 사용할 수 있도록 제공하는 서비스이고, 플랫폼 서비스(PaaS)는 이용자(SW개발자)가 애플리케이션을 개발, 테스트, 구축할 수 있는 통합된 플랫폼을 제공하는 서비스로서 이용자는 PaaS를 통해 새로운 애플리케이션을 개발하기도 하고 다른 SaaS 서비스를 제공하기도 한다. 소프트웨어 서비스(Software as a service)는 일정관리, 주소록, CRM용 프로그램, 오피스 프로그램 등 다양한 소프트웨어를 웹을 통해 임대해 사용할 수 있도록 제공하는 서비스이다.

다음으로 클라우드 컴퓨팅 서비스는 서비스의 대상·범위에 따라 퍼블릭 클라우드(Public Cloud) 서비스, 프라이빗 클라우드(Private Cloud) 서비스, 앞의 양자가 혼합된 하이브리드 클라우드(Hybrid Cloud) 서비스로도 구분한다. 퍼블릭 클라우드(Public Cloud) 서비스는 원하는 사람은 누구든지 이용할 수 있도록 구현되

〈서비스 내용에 따른 구분〉

구 분	내 용
IaaS (Infrastructure as a service)	• 서버, 스토리지, 네트워크 등 인프라스트럭처를 가상화 환경으로 만들어 필요에 따라 인프라 자원을 사용할 수 있도록 하는 서비스
PaaS (Platform as a service)	• 이용자(SW개발자)가 애플리케이션을 개발, 테스트, 구축할 수 있는 통합된 플랫폼을 제공하는 서비스로, 이용자는 PaaS를 통해 새로운 애플리케이션을 개발하기도 하고 다른 SaaS 서비스를 제공하기도 함
SaaS (Software as a service)	• 일정관리, 주소록, CRM용 프로그램, 오피스 프로그램 등 다양한 소프트웨어를 웹을 통해 임대해 사용할 수 있도록 제공하는 서비스

는 서비스로 일반 이용자에게 사용량에 따라 과금하는 형태로 제공되고, 프라이빗 클라우드(Private Cloud) 서비스는 기업이나 공공기관 내부에 클라우드 컴퓨팅 환경을 구성해 직원이나 협력사만 이용할 수 있도록 폐쇄적으로 구현한 서비스이다. 프라이빗 서비스는 사설망에 클라우드 컴퓨팅의 개념을 적용한 것에 불과하며 어차피 이용자가 IT자원을 구매·구축하고 관리해야 한다는 비판을 받고 있다. 커뮤니티 클라우드(Communlty Cloud) 서비스는 비슷한 환경에 처해 있는 기관이나 단체들이 클라우드 컴퓨팅의 장점을 활용할 수 있도록 하기 멤버들에게만 폐쇄적으로 제공되는 서비스이다. 클라우드 컴퓨팅의 장점을 살리면서도 프라이버시, 데이터 보안, IT컴플라이언스 등의 문제를 해결할 수 있는 장점이 있다. 이에 비해 하이브리드 클라우드(Hybrid Cloud) 서비스는 퍼블릭 클라우드와 프라이빗 클라우드 서비스가 혼재된 형태로, 회사 기밀자료 등 중요자료는 프라이빗 클라우드에 보관하고 그밖의 자료는 퍼블릭 클라우드를 이용하는 형태이다.

1.4 클라우드 컴퓨팅의 장단점

일반적으로 클라우드 컴퓨팅 이용자들은 물리적인 IT 인프라를 보유하지 않는 대신에 제3자로부터 IT 인프라를 빌려 사용한다.

이에 따라 첫째, 클라우드 컴퓨팅 이용자는 각종 하드웨어, 소프트웨어 등의 구입에 소요되는 자본지출을 피할 수 있다. 초기 투입자본이 줄어든 만큼 진입장벽도 낮아져 산업발전과 고용창출에도 기여한다.

〈서비스 범위·대상에 따른 구분〉

구 분	내 용
퍼블릭 클라우드 (Public Cloud, External Cloud)	• 누구든지 이용할 수 있도록 구현되는 것으로 일반 이용자에게 사용량에 따라 과금하는 형태로 제공되는 서비스
프라이빗 클라우드 (Private Cloud, Internal Cloud)	• 회사 내부에 클라우드 컴퓨팅 환경을 구성해 직원이나 협력사만 이용할 수 있도록 폐쇄적으로 구현한 서비스
커뮤니티 클라우드 (Communlty Cloud)	• 비슷한 환경에 처해 있는 기관이나 단체들이 클라우드 컴퓨팅의 장점을 활용할 수 있도록 하기 멤버들에게만 폐쇄적으로 제공되는 서비스
하이브리드 클라우드 (Hybrid Cloud)	• 퍼블릭 클라우드와 프라이빗 클라우드 서비스가 혼재된 형태. 회사 기밀자료 등 중요자료는 프라이빗 클라우드에 보관하고, 부분적으로 퍼블릭 클라우드를 이용하는 형태 등

둘째, 물리적인 시설을 보유할 필요가 없게 됨에 따라 각종 IT자원을 운영·관리하기 위하여 별도로 구비해야 했던 보안설비와 전문인력도 필요 없게 된다. 즉 관리·운영 비용이 절감된다.

셋째, 순간적으로 급증하는 컴퓨터 작업이나 비정상적으로 급증하는 트래픽에 대비하여 개별 이용자들이 굳이 여유 IT자원을 확보하고 있어야 할 필요가 없어져 사회 전체적으로 비용절감 효과가 크다. 또한 IT자원의 중앙집중화가 가능해 건물이나 전기사용료와 같은 비용이 절감되며, 예상치 못하게 발생하는 순간 최고트래픽에 대한 대응능력(Peak-load capacity)이 향상된다.

넷째, 많은 클라우드 컴퓨팅 서비스들이 전기나 수도와 마찬가지로 유틸리티 방식으로 제공되기 때문에 IT자원에 대한 이용율을 높여 IT자원을 불필요하게 놀리면서 방치하는 상황을 방지할 수 있다.

다섯째, 이용자는 클라우드 컴퓨팅 사업자가 보유하고 있는 다수의 잉여 자원을 활용함으로써 시스템상에 장애가 발생하도라도 신속한 복구가 가능하여 비즈니스의 연속성을 확보하는 등 신뢰도를 높일 수 있다.

여섯째, 데이터의 중앙 집중화와 보안에 대한 투자증가로 보안능력이 향상될 수 있다. 특히 비용, 기술 등의 문제로 보안이 허술할 수 밖에 없는 중소기업이나 개인의 경우 클라우드 컴퓨팅 사업자가 전문적인 기술과 인력으로 데이터를 보호해 주기 때문에 데이터의 안전성을 확보할 수 있다.

일곱째, 이용자가 보유하고 있는 단말기의 종류나 저장 공간의 크기 그리고 이용자의 위치에 구애받지 않고 언제, 어디서나 웹브라우저를 통해 시스템에 접근할 수 있다. 모든 하드웨어, 소프트웨어 등은 클라우드 컴퓨팅 사업자에 의해 제공된다.

여덟째, 이용자는 클라우드 컴퓨팅을 이용할 때 어플리케이션 등을 자신의 컴퓨터(단말기)에 저장해 두어야 할 필요가 없기 때문에 컴퓨터 관리가 쉽고 항상 최신의 어플리케이션을 이용할 수 있다. 또한 이용자는 컴퓨터 관리에 필요한 복잡한 기술이나 인프라에 대한 전문지식이 필요 없게 되어 누구든지 보다 쉽게 컴퓨터를 이용할 수 있게 된다.

클라우드 컴퓨팅은 이와 같이 여러 장점이 많지만 기술적 또는 법률적 측면에서 문제점도 적지 않다. 기술적

측면에서 클라우드 컴퓨팅 사업자들은 클라우드 컴퓨팅을 통해 오히려 보안능력이나 프라이버시가 강화될 수 있다고 주장하나 이는 일반화하기 어렵다.

첫째, 비용·기술면에서 보안능력이 취약할 수 밖에 없는 개인이나 중소기업의 관점에서 보면 부분적으로 보안 능력이 향상된다고 볼 수 있으나, 일반적으로는 데이터의 중앙 집중화에 따른 위험이 증가하고, 데이터가 수많은 디바이스와 도처의 저장공간에 분산 저장되기 때문에 보안문제가 그만큼 커지고 복잡해진다. 제3자의 손에 맡겨진 데이터에 대한 통제권의 상실도 큰 문제이다. 커뮤니티 클라우드나 하이브리드 클라우드의 경우에는 이런 단점을 방지할 수 있으나, 퍼블릭 클라우드의 경우에는 데이터에 대한 접근통제, 저장공간 특정 등의 문제가 클라우드 사업자의 양심이나 재량에 맡겨져 있다.

둘째, 클라우드 컴퓨팅 사업자는 자신의 지배하에 있는 민감정보나 개인정보에 대해서 보다 쉽게 통제권을 행사할 수 있고, 이용자와 자신 사이에 주고받은 통신이나 데이터를 의도적으로 모니터링하거나, 정부나 수사기관이 시도하는 각종 적법·불법 감청의 협력 파트너가 될 수 있다. 정부와 수사기관은 오로지 자신의 편의를 위해서 법률의 개정을 통해서라도 통신사업자들에게 이용자의 활동이나 사생활을 모니터링할 수 있는 보다 많은 권한을 부여하려 할 것이다.

이밖에도 클라우드 컴퓨팅의 이용이 활성화되기 위해서는 IT 컴플라이언스 준수, 클라우드 컴퓨팅의 품질보증, 클라우드 컴퓨팅 서비스 제공자의 교체·이전, 표준화 등 다양한 법률문제가 존재하게 되는데, 이들 법적 이슈 및 장애 요인에 대해서는 후술한다.

Ⅱ. 클라우드 컴퓨팅에 관한 국내법 개관

현재 국내법상 클라우드 컴퓨팅의 개념을 직접적으로 규정하고 있거나 클라우드 컴퓨팅을 규율하고 있는 법률은 존재하지 않는다. 그러나 클라우드 컴퓨팅은 현행법상 정보통신, 전기통신, 정보통신시스템 등의 전부 또는 일부를 구성함으로써 직·간접적으로 다양한 법률의 규제를 받게 된다.

2.1 민간분야에 있어서 클라우드 컴퓨팅관련 법률

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다)은 모든 형태의 정보통신서비스 제공에 적용되는 법률로서 클라우드 컴퓨팅 서비스도 동법의 적용을 받는다. 「정보통신망법」은 개인정보의 위탁처리 제한 및 수탁자에 대한 관리·감독(제25조), 개인정보관리책임자 지정(제27조), 개인정보의 기술적·관리적 보호조치(제28조), 개인정보의 누설금지(제28조의2), 개인정보의 파기(제29조), 개인정보의 국외이전 제한(제63조), 중요정보의 국외 이전 제한(제51조), 정보통신망 안전성·신뢰성 확보조치 의무(제45조), 집적정보통신시설사업자의 보호조치 및 보험가입 의무(제46조), 집적정보통신시설사업자의 긴급대응 의무(46조의2), 정보보호 안전진단 의무(제46조의3), 침해사고관련 정보제공·침해사고 신고·침해사고 원인분석 등(제48조의2~4), 청소년보호책임자 지정(제43조의3), 권리침해정보에 대한 임시조치의무(제44조의2) 등을 규정화고 있는 외에, 정보통신망 이용촉진 및 정보보호 등에 관한 시책 마련(제4조), 정보통신망 관련 기술·기기의 개발(제6조), 정보통신망의 표준화 및 인증(제8조, 제9조), 정보통신망 응용서비스 개발 촉진(제11조), 정보통신망 이용촉진 등 사업(제13조), 인터넷 이용의 확산(제14조), 인터넷 서비스의 품질 개선(제15조) 등과 같은 클라우드 컴퓨팅 기술개발 및 이용활성화를 위한 규정도 다수 두고 있다.

이 밖에 민간분야에서 클라우드 컴퓨팅 서비스를 제공함에 있어서 클라우드 컴퓨팅을 규제·제한하는 법률로는 전기통신사업법, 통신비밀보호법, 전자금융거래법, 전자서명법, 신용정보의 이용 및 보호에 관한 법률, 저작권법 등의 규정을 고려해야 하며, 클라우드 컴퓨팅을 지원·촉진하는 법률로는 앞에서 언급한 정보통신망법 이외에 「정보통신산업진흥법」을 고려해야 한다. 정보통신산업진흥법은 정보통신산업 진흥계획(제5조), 정보통신기술진흥 시행계획(제7조), 연구과제 등의 지정(제8조), 신기술의 사업화 지원 등(제9조), 정보통신 표준화의 촉진(제12조~제15조), 전문인력의 양성(제16조) 등의 규정을 두고 있다.

2.2 공공분야에 있어서 클라우드 컴퓨팅관련 법률

공공분야에서 클라우드 컴퓨팅 서비스를 제공하거나 이용하기 위해서는 먼저 「공공기관의 개인정보보호에 관한 법률」과 「전자정부법」 그리고 「정보통신기반보호법」, 「국가사이버안전관리규정」, 「보안업무규정」 등을 검토하여야 한다.

「공공기관의 개인정보보호에 관한 법률」은 「정보통신망법」만큼 다양한 규정을 두고 있지는 않지만, 개인정보의 기술적·관리적 보호조치(제9조제1항), 개인정보의 위탁처리관리(제9조제2항), 개인정보파일의 파기(제10조의2), 개인정보침해사실의 신고(제18조의2), 개인정보관리책임관의 지정(제20조) 등의 규정을 두고 있어 클라우드 컴퓨팅 사업자에게 개인정보의 처리를 위탁할 때에는 주의가 요망된다.

「전자정부법」은 전자정부 시스템의 안전한 이용 및 보호를 위하여 전자적 대민서비스 보안대책 수립·시행(제24조), 정보통신망 등의 보안대책 수립·시행(제56조), 행정기관 등의 정보시스템 감리(제57조), 권한 등의 위임·위탁(제73조) 등을 규정하고 있는 외에, 전자정부 활성화를 위한 다양한 조치들을 마련해 두고 있다. 예컨대 정보통신망 연계 및 행정정보 공동이용 등의 협력의무(제3조), 전자정부서비스 개발·제공(제16조), 유비쿼터스 기반의 전자정부서비스 도입·활용(제18조), 전자정부서비스의 보편적 활용을 위한 대책(제19조), 전자정부서비스의 민간 참여 및 활용(제21조), 전자문서의 작성·보관 의무(제25조), 행정정보 공동이용센터의 설치(제37조), 통합 정보통신망의 구축(제52조) 등을 규정함으로써 공공부문의 클라우드 컴퓨팅 서비스 이용 가능성을 널리 마련해 두고 있다.

이 밖에 행정기관이나 공공기관이 관리·운영하는 정보시스템은 「국가사이버안전관리규정」, 「보안업무규정」 등의 규정을 적용받게 되며, 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 「정보통신망법」에 따른 정보통신망 중에서 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 영향이 크거나, 침해사고의 발생가능성이 크거나, 해당 시설에 의해서 처리되는 업무의 국가사회적 중요성이 큰 시설에 대해서는 정부가 이를 '주요정보통신기반시설'로 지정해 「정보통신기반보호법」을 적용받게 할 수 있다. 주요정보통신기반시설로 지정을 받으면 해당 시설 관리자 또는 소유자는 해당 시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책을 수립·시행(제5조)해야 하며, 해당 시설에 대하여 정보보호 취약점 분석·평가(제9조)를 받아야 한다.

2.3 그 밖의 클라우드 컴퓨팅관련 법률

클라우드 컴퓨팅 서비스의 제공 및 이용 과정에서 발생하는 소비자(또는 이용자) 권리보호에 대해서는 소비자기본법, 독점규제 및 공정거래에 관한 법률, 약관의 규제에 관한 법률, 표시·광고의 규제에 관한 법률 등이 적용된다. 특히 클라우드 컴퓨팅 서비스의 품질보증, 서비스 불이행, 요금 분쟁, 끼워팔기, 허위·과장광고, 유인행위, 불공정거래행위 등과 같은 소비자 권리침해 행위에 대해서는 클라우드 컴퓨팅 서비스라고 하더라도 예외없이 현행법이 그대로 적용된다.

또한 영업비밀이나 산업기술 유출 행위에 대해서는 「부정경쟁방지 및 영업비밀보호에 관한 법률」, 「산업기술의 유출방지 및 보호에 관한 법률」, 형법 등이 적용된다.

마지막으로 7.7 디도스 사건(2009년 7월 7일)을 계기로 현재 정부가 추진하고 있는 「악성프로그램의 확산 방지 등에 관한 법률」이 제정되면 해당 법률의 일부가 클라우드 컴퓨팅 사업자들에게도 적용될 것으로 예상된다. 예컨대 악성프로그램 정기점검, 소프트웨어 보안패치, 백신프로그램 제공, 모의 해킹대응훈련 협력, 그밖의 침해예방 및 침해대응 협력 의무 등이 적용될 수 있을 것이다.

Ⅲ. 클라우드 컴퓨팅에 관한 법적 이슈

클라우드 컴퓨팅은 현행법이 미리 예상하지 못했던 서비스로서, 클라우드 컴퓨팅 서비스가 원활하게 제공되고 이용이 활성화되기 위해서는 앞에서 열거한 다양한 법률적 요건을 충족해야 한다. 그러나 클라우드 컴퓨팅의 특성상 그 특성이 현행법의 규제 내용과 충돌되는 부분이 적지 않다. 따라서 클라우드 컴퓨팅 서비스가 활성화 되기 위해서는 그 같은 발전 장애요인을 제거하거나 합리적으로 개선될 필요가 있다.

클라우드 컴퓨팅 서비스의 모습이 아직 명확하게 제시되지 않고 발전 단계에 있기 때문에 이를 둘러싼 법률적 이슈를 정확하기 제시하는 것은 쉽지 않다. 이런 이유들로 인해 국내외를 막론하고 클라우드 컴퓨팅의 법률적 이슈에 대해서는 아직 심도있는 논의가 이루어지지 않고 있다. 프라이버시, 보안 등과 관련한 문제가 일부 제시되고 있기는 하나 클라우트 컴퓨팅에 특화된 법적 이슈는 제시되지 못하고 있다.

본고에서는 클라우드 컴퓨팅에서 일반적으로 문제될 수 있는 법적 이슈들을 중심으로 그 개요를 살피고자 한다.

3.1 가용성 · 안전성에 대한 사업자의 책임

클라우드 컴퓨팅 시스템에 장애가 발생하여 서비스가 중단되거나 정보가 손실되는 등의 문제가 발생할 가능성은 충분히 존재한다. 이 같은 상황에 대비하여 클라우드 컴퓨팅 사업자가 어느 범위까지 서비스의 가용성과 안전성을 보증할 것인가를 결정하는 것은 클라우드 컴퓨팅 서비스의 신뢰 확보와 안정적 성장 기반 마련을 위해 매우 중요한 사항이다.

이용자는 클라우드 컴퓨팅 서비스가 언제든지 이용 가능하고 자신들의 정보가 손실될 위험이 없다는 점이 보증될 것을 요구할 것이다. 그러나 IT의 특성상 클라우드 컴퓨팅 사업자가 365일 내내 100%의 무사고를 보장하는 것은 현실적으로 불가능하다. 또한 현실적으로 클라우드 컴퓨팅 사업자가 많은 위험을 부담하면 할 수록 즉 높은 수준의 서비스 수준을 보장하면 할 수록 부과 요금이 증가할 수밖에 없을 것이다(구태언).

현재 구글 앱스(Google Apps), 아마존 웹서비스(Amazon Web Services) 등 외국의 주요 클라우드 컴퓨팅 사업자들은 서비스 가용성에 대한 보증을 제공하지 않거나 이용약관에 면책약관을 포함시켜 서비스 중단이나 정보손실 등에 대한 책임을 회피하고 있다.[1)]

〈Google 표준형 애플리케이션 계약〉

13. 보증의 면책조항. 고객은 각 서비스에 버그, 결함, 오류 및 시스템 오류를 일으킬 수 있는 기타 문제가 포함되어 있을 수 있음을 이해하고 이에 동의합니다. 따라서 모든 콘텐츠, 소프트웨어(소프트웨어에 대한 모든 업데이트 또는 수정사항 포함), 기능, 자료 및 본 서비스를 통해 제공되거나 액세스 가능한 정보를 포함하는 서비스와 이에 수반되는 모든 설명서는 '있는 그대로' 제공되며, 이에 따른 모든 사용의 책임은 전적으로 고객에게 있습니다. 관련 법률이 허용하는 한도 내에서, Google 및 라이센스 제공자는 상품성, 특정 사용 및 재산권 비침해에 대한 보증을 포함한 모든 명시적, 묵시적, 법적 보증을 하지 않습니다. Google은 본 서비스의 올바른 사용에 대해 책임을 지지 않습니다. Google 및 라이센스 제공자는 본 서비스를 통해 액세스할 수 있는 콘텐츠나 정보에 대해 어떠한 진술도 하지 않습니다. Google은 Google(또는 제3자)이 본 서비스에 대한 업데이트나 개선기능을 발표한다는 어떠한 진술도 하지 않습니다. Google은 본 서비스에 포함된 기능이 중단되지 않는다거나 오류가 없다고 보증하지 않습니다. 일부 관할지역에서는 묵시적 보증의 배제를 허용하지 않으므로, 위와 같은 책임배제는 고객에게 적용되지 않을 수도 있습니다. 이러한 상황이 발생할 경우, 허용되는 범위 내에서 묵시적인 보증은 유효일자로부터 구십(90)일 동안으로 제한됩니다. 본 서비스는 무장애 서비스가 아니며, 서비스를 잘못 사용할 경우 사망, 인명피해 또는 환경훼손의 결과를 초래할 수 있는 핵시설, 항공교통 관제 또는 생명유지 장치의 작동('위험 활동')을 위해 사용하도록 설계 또는 제작되지 않았습니다.
<출처 : http://www.google.com/apps/intl/ko/terms/standard_terms.html (2010. 2. 23. 접속)>

〈Amazon Web Services 소비자 이용약관〉

11.8. Limitations of Liability. NEITHER WE NOR ANY OF OUR LICENSORS SHALL BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER LOSSES (EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) IN CONNECTION WITH THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, ANY SUCH DAMAGES RESULTING FROM: (i) THE USE OR THE INABILITY TO USE THE SERVICES; (ii) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS AND SERVICES; OR (iii) UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR CONTENT. IN ANY CASE, OUR AGGREGATE LIABILITY UNDER THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU TO US HEREUNDER FOR THE SERVICES. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES OR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES. ACCOR- DINGLY, SOME OR ALL OF THE ABOVE EXCLUSIONS OR LIMITATIONS MAY NOT APPLY TO YOU, AND YOU MAY HAVE ADDITIONAL RIGHTS.
14.2. Governing Law. By using the Services, you agree that the laws of the State of Washington, without regard to principles of conflicts of laws, will govern this Agreement and any dispute of any sort that might arise between you and us. The parties expressly exclude application of the United Nations Convention for the International Sale of Goods to this Agreement.
<출처 : http://aws.amazon.com/agreement/#11 (2010. 2. 23 접속)>

그러나 이용약관에서 과도한 면책규정을 넣는 것은 각국의 약관규제법 위반 가능성이 크다. 예컨대 영국의 경우, 「소비자계약의 불공정조항에 관한 규칙(Unfair Terms in Consumer Contracts Regulation 1999)」[2)]에

1) Miranda Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law", 「Technology and Society」, Volume 6, no.1, 2009 4. pp.6-7 참조.

따라, 이용자가 약관에 동의하였더라도 모든 가능한 사고에 대한 책임을 배제하는 면책조항은 불공정조항에 해당되어 이용자에게 구속력이 없다고 봄(제8조제1항)[3]. 또한 「국제물품매매 계약에 관한 UN 협약(United Nations Convention on Contracts for the International Sale of Goods 1980)」 제35조에 따르면, 클라우드 컴퓨팅 사업자도 동종 물품의 통상적인 사용목적에 맞는 물품을 인도할 의무가 있다. 우리나라의 「약관의 규제에 관한 법률」 제7조도 면책조항을 금지하고 있는데, 클라우드 서비스제공자가 상당한 이유없이 사업자의 손해배상범위를 제한하는 조항을 이용약관에 포함하는 것은 동법 위반이 될 수 있다.[4]

따라서 서비스 중단이나 정보손실에 대한 클라우드 컴퓨팅 사업자의 책임을 무조건 배제하는 것은 법률적 측면에서는 물론 클라우드 컴퓨팅 사업의 안정적인 발전을 위해서도 바람직스럽지 못하다. 클라우드 컴퓨팅 서비스가 이용자들의 신뢰 위에서 안정적으로 발전하기 위해서는 사업자와 이용자가 적절하게 위험을 분담할 필요가 있다. 무조건적인 면책도 문제지만 무제한적인 책임도 안 된다. 즉 클라우드 컴퓨팅 사업자의 책임범위를 합리적인 선에서 제한할 필요가 있다.

그 하나의 방법이 클라우드 컴퓨팅 서비스에 관한 표준서비스약관을 제정하는 것이다. 약관을 통해 사전에 서비스의 정의, 품질, 보증, 사고관리, 보상, 고객의 의무 등에 관한 사항을 명확히 할 필요가 있다. 커뮤니티 또는 하이브리드 클라우드 서비스의 경우에는 사업자와 이용자가 합의를 통해 이른바 「서비스 수준 협약(SLA : Service level Agreement)」을 체결해 클라우드 컴퓨팅 서비스의 품질에 대한 보증이나 책임 범위를 자율적으로 정할 수 있을 것이나 퍼블릭 클라우드 서비스의 경우에는 시장기능에만 맡길 수 없으므로 약관 신고제 또는 등록제, 약관 개선명령제 등과 같은 적절한 통제장치를 마련해 클라우드 컴퓨팅 사업자에 의한 불공정거래행위를 차단할 필요가 있다.

그런가 하면, 다른 한편으로는 클라우드 컴퓨팅 사업자가 파산의 공포에서 벗어나 안정적으로 서비스를 공급할 수 있도록 하기 위해서는 배상책임보험제도를 도입해 클라우드 컴퓨팅 사업자의 배상책임 범위를 그가 얻은 이익에 비례하여 감당할 수 있는 범위 내로 제한하여야 하고 사고 위험도 널리 이용자들에게 분산시킬 수 있게 해야 할 것이다. 이를 통해 이용자는 사고 발생시 클라우드 컴퓨팅 사업자가 배상능력이 없더라도 정당한 피해 보상도 보장받을 수 있다.

3.2 불법정보 등에 대한 사업자의 관리 · 감독 책임

EU에서는 클라우드 컴퓨팅 사업자가 「EU 전자상거래지침」[5]상 단순접속매개, 캐싱, 호스팅 등의 서비스를 제공하는 매개서비스제공자(intermediary service providers)에 해당되는지에 대하여 논란이 있다. 클라우드 컴퓨팅 사업자가 이 지침에서 규정하고 있는 매개서비스제공자에 해당할 경우, 자신이 전달·저장하는 정보를 모니터하거나 불법적인 행위를 가리키는 사실·상황을 적극적으로 찾아낼 의무가 없고 불법적인 행위나 정보에 대해 알지 못하거나 알 수 없는 경우에는 면책될 수 있다(EU 전자상거래 지침 제12조~제15조). 우리나라에서도 전화나 팩스와 같은 전기통신서비스를 제공하는 전화사업자의 경우 자신의 망을 통해 전송 또는 유포되는 불법정보에 대해서 책임을 지지 않지만, 포털의 경우에는 판례상 자사 게시판 등에 게시된 불법정보에 대해서 책임이 인정되는 경우가 있다.

특히 우리나라 정보통신망법은 정보통신서비스제공

2) 동 규칙은 EU의 「소비자 계약의 불공정 조항에 관한 유럽공동체 지침(EC Directive on Unfair Terms in Consumer Contracts) (93/13/EEC)」을 자국에서 시행하기 위해 제정된 것이다.

3) 공정거래위원회 웹사이트 게시글, "외국의 불공정약관 사용실태", 2006. 4. 6. http://www.consumer.go.kr/consumer/open_content/industry/co_indu_info_view.php (2009. 12. 23. 접속)

4) 「약관의 규제에 관한 법률」 제7조 (면책조항의 금지) 계약당사자의 책임에 관하여 정하고 있는 약관의 내용 중 다음 각호의 1에 해당하는 내용을 정하고 있는 조항은 이를 무효로 한다.
1. 사업자, 이행보조자 또는 피용자의 고의 또는 중대한 과실로 인한 법률상의 책임을 배제하는 조항
2. 상당한 이유없이 사업자의 손해배상범위를 제한하거나 사업자가 부담하여야 할 위험을 고객에게 이전시키는 조항
3. 상당한 이유없이 사업자의 담보책임을 배제 또는 제한하거나 그 담보책임에 따르는 고객의 권리행사의 요건을 가중하는 조항 또는 계약목적물에 관하여 견본이 제시되거나 품질·성능등에 관한 표시가 있는 경우 그 보장된 내용에 대한 책임을 배제 또는 제한하는 조항

5) 「역내 시장의 특정 전자상거래에서 정보사회서비스의 법적 측면에 관한 지침(Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market)」

자에게 청소년 보호조치, 불법정보의 삭제·차단, 권리 침해 정보에 대한 임시조치, 권리자의 요청에 따른 권리 침해자에 관한 신상정보 제공, 게시판 이용자의 본인확인 의무 등 다양한 의무를 부과하고 있고, 저작권법 역시 저작권 보호의무 등을 부여하고 있다. 그러나 현행법상 정보통신서비스제공자가 적극적으로 불법정보를 모니터링해서 삭제 등의 조치를 취할 의무가 있는지에 대해서는 명확하지 않다. 이에 따라 2008년 11월 28일 국회에 제출된 정보통신망법 전부개정안(정부안)은 많은 인권운동가와 사업자들의 반대에도 불구하고 정보통신서비스제공자에게 적극적인 모니터링 의무를 부과하고 있다.

클라우드 컴퓨팅 사업자는 그가 제공하는 서비스의 내용과 방법에 따라 통상 전기통신역무를 제공하는 전기통신사업자이거나 영리목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자에 해당하므로 「정보통신망법」상 정보통신서비스제공자의 개념에 해당한다. 따라서 클라우드 컴퓨팅 사업자도 다른 정보통신서비스제공자와 마찬가지로 청소년 유해매체물, 불법정보 등에 대해 청소년 보호조치, 삭제·차단조치 등의 의무를 부담하며, 더 나아가 적극적인 모니터링 의무를 부담해야 하는 경우도 있을 수 있다.

3.3 위탁자의 수탁자에 대한 관리·감독 등 책임

기업이 클라우드 컴퓨팅 사업자에게 아웃소싱한 IT 업무가 실패하여 서비스가 중단되거나 데이터가 분실·훼손된 경우, 클라우드 컴퓨팅 서비스 이용 기업은 자신의 고객들에게 직무상 부주의(professional negligence)에 따른 계약상의 책임을 지거나 의무 태만에 따른 민사상의 불법행위 책임(tortuous liability)을 져야 한다. 서비스 이용 기업은 위탁자로써 수탁자의 선임·감독에 대해서 책임을 져야하고, 법령(정보통신망법 등)에 따라서는 수탁자에 대한 관리·감독 책임도 져야 하기 때문이다. 더 나아가 정보통신망법(제25조제5항)은 수탁자가 개인정보 취급위탁을 받은 업무와 관련하여 법을 위반해 이용자에게 손해를 발생시킨 경우 그 수탁자를 손해배상책임에 있어서 정보통신서비스제공자의 소속 직원으로 보는 등 위탁자에 대해서 다양한 책임을 지우고 있다. 「EU 개인정보보호지침」을 기준으로 보면, EU에서도 기업은 개인정보관리자(Data controller)로서 자신이 정한 정보처리 목적과 방법에 따라 정보주체의 개인정보를 직접 취급하는 클라우드 컴퓨팅 사업자(external data processor)의 행위에 대해 관리·감독 책임을 진다.[6]

그러나 전형적인 IT아웃소싱과 달리, 클라우드 컴퓨팅 서비스에서는 서비스 이용자이자 동시에 IT업무 위탁자인 기업은 수탁자인 클라우드 컴퓨팅 사업자를 효율적으로 통제·감독하기 어렵다. 전형적인 IT아웃소싱의 경우, 아웃소싱을 맡긴 고객은 통상적으로 데이터가 어디에서 처리되고 있고 어디에 저장되어 있는지를 알고 있고 데이터센터의 위치가 정해져 있다. 반면, 클라우드 컴퓨팅 서비스에서는 데이터가 전 세계의 데이터센터에 분산되어 저장될 수 있고, 여러 곳에 데이터의 복사본이 존재할 수 있다. 그렇기 때문에 기업은 자사의 고객 개인정보가 어떻게 관리되고 어느 서버에 저장되는지 알기 어렵고, 클라우드 컴퓨팅사업자의 정보 처리를 효과적으로 감시·통제하고 합법적인 방식으로 정보처리가 이루어지고 있는지를 확인하는 것이 곤란하다.[7] 특히 기업이 여러 나라의 클라우드 컴퓨팅 사업자에게 개인정보를 처리하도록 하는 경우, 개인정보관리자로서 기업의 통제권이 더욱 상실될 수 있다.

따라서 클라우드 컴퓨팅 서비스의 경우 정보통신망법상의 관리·감독 책임이나 손해배상책임을 그대로 적용하기 어려운 측면이 많다. 클라우드 컴퓨팅 서비스의 제공 및 이용 관계는 기업 IT업무의 아웃소싱 또는 위·수탁관계라기 보다는 차라리 IT서비스의 이용·소비라고 보는 것이 더 정확할 수 있다. 즉 기업은 이용자 또는 소비자로써 시장에서 클라우드 컴퓨팅 서비스를 구입해 이용하는 것에 불과하다. 일반적으로 클라우드 컴퓨팅 사업자를 선택함에 있어서 자신의 업무를 위탁한다는 관념이 희박하고, 따라서 자신이 관리·감독해야 할 대상이라는 사실을 인식하기 어렵다. 그러나 클라우드 컴퓨팅 서비스의 이용을 IT업무 위탁으로 보든 서비스의 구매·이용으로 보든 현행법상 클라우드 컴퓨팅 서비스의 성능·품질·안전성 등의 결여로 인한 사고에 대한 책임은 클라우드 컴퓨팅 서비스 이용자가 질 수 밖에 없다.

클라우드 컴퓨팅 서비스의 제공자와 이용자의 관계,

6) ENISA, "Cloud Computing : Benefits, risks and recommendations for information security", 2009.11.9. p.103 참조.

7) 계약이나 약관으로 데이터센터의 위치를 특정할 수 있다고 하더라도 그것만으로 클라우드 컴퓨팅 사업자를 관리·감독하는 데는 한계가 있다.

클라우드 컴퓨팅 서비스의 구성상 특수성 등을 고려할 때 서비스 이용자(주로 기업 이용자일 것이다)에게는 위탁자로써 수탁자의 선임에 대해서만 책임을 묻고 관리·감독 의무나 사용자로써의 책임은 면제 내지 완화하는 방안이 강구될 수 있을 것이다. 이 경우 예상치 못한 이용자(최종 소비자)의 피해는 보험제도 등을 통해 해결되어야 할 것이다.

3.4 개인정보 및 중요정보의 국외 이전 제한

EU를 포함한 다수의 국가들이 개인정보보호법에 의해 개인정보의 국외이전을 금지하고 있다. 개인정보를 국외로 이전하려면 그 나라의 법이 자국법보다 더 강하게 개인정보를 보호하고 있거나 계약 등에 의해서 개인정보보호를 위한 안전장치가 확보되어야 한다. 그런데 클라우드 컴퓨팅 서비스를 이용할 경우 개인정보가 다수의 국가에 분산 저장되고 수시로 데이터가 오갈 수 있기 때문에 동 법률과 충돌할 가능성이 크다.

우리나라 「정보통신망법」도 정보통신서비스제공자 등이 이용자의 개인정보를 취급함에 있어서 동 법을 위반하는 사항을 내용으로 하는 국제계약의 체결을 금지하고 있고, 또한 이용자의 개인정보를 국외로 이전하려면 미리 이용자에게 1) 이전되는 개인정보 항목, 2) 개인정보가 이전되는 국가, 이전일시 및 이전방법, 3) 개인정보를 이전받는 자의 성명, 4) 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간 등을 알리고 그의 동의를 받도록 하고 있다. 이용자의 동의를 받은 경우에도 정보통신서비스제공자 등이 실재로 개인정보를 국외로 이전하는 때에는 개인정보보호를 위한 기술적·관리적 보호조치를 취해야 하고, 국외에서 개인정보를 이전받는 자와 미리 협의하여 이를 계약내용 등에 반영하여야 한다(제63조).

그밖에도 정부는 국내의 산업·경제 및 과학기술 등에 관한 중요 정보가 정보통신망을 통하여 국외로 유출되는 것을 방지하기 위하여 정보통신서비스 제공자 또는 이용자에게 1) 정보통신망의 부당한 이용을 방지할 수 있는 제도적·기술적 장치의 설정, 2) 정보의 불법파괴 또는 불법조작을 방지할 수 있는 제도적·기술적 조치, 3) 정보통신서비스 제공자가 취급 중 알게 된 중요 정보의 누출을 방지할 수 있는 조치 등의 필요한 조치를 하도록 할 수 있다(제51조).

그러나 오늘날 서버, 데이터베이스, 스토리지 등의 물리적 공간이 어느 나라에 위치하느냐는 그다지 중요하지 않다. IT자원의 물리적 공간이 해외에 존재하더라도 얼마든지 기술적·관리적인 보호장치를 취할 수 있고 원격으로도 시스템 관리·감독이 가능하기 때문이다. 따라서 해외의 사업자나 국가가 국내 이용자 또는 소비자들의 개인정보를 저장하고 있는 데이터베이스 등에 직접 접근해서 개인정보를 이용·제공하는 경우가 아니라면, 즉 국내 소비자들의 개인정보를 저장·관리하기 위해 단순히 서버, 데이터베이스, 스토리지 등의 물리적 위치를 해외에 두는 것이라면 굳이 개인정보의 국외 이전을 금지하거나 제한할 필요는 없다고 본다. 현행법(정보통신망법 제63조)의 해석상으로도 단순히 개인정보 데이터베이스 등의 물리적 위치를 해외에 두는 것은 개인정보의 국외 이전으로 보지 않을 여지가 충분하나 입법적으로 이를 보다 명확화하는 것이 필요하다.

3.5 IT 컴플라이언스와 정보보호

클라우드 컴퓨팅 서비스는 많은 시스템이 연결되어 있어 다양한 공격루트가 존재하고, 침해사고 발생시 피해가 급속히 확산될 수 있으며 DDoS 공격 등에 취약할 수 있다. 이용자의 정보가 클라우드 컴퓨팅 사업자의 서버에 집중 보관·관리되기 때문에 서버의 불안정으로 인한 침해사고가 발생하는 경우에 대규모 피해가 발생할 가능성이 있다.[8] 또한 클라우드 서비스에서 처리되는 정보는 통상 암호화되지 않기 때문에, 내부자에 의한 악의적인 유출이나 오·남용, 외부 해킹에 의한 정보유출시 피해가 커질 위험이 있다.

따라서 클라우드 컴퓨팅 사업자는 서비스를 제공하는 과정에서 데이터를 안전하게 처리, 저장, 관리하기 위해 필요한 정보보안 조치를 취해야 한다. 이 같은 정보보안 조치에는 정보의 라이프사이클 관리를 위한 정책 및 프로세스 확립, 내부자 보안위협 관리·감시, 애플리케이션 보안, 암호화 및 키관리, 데이터센터에 대한 현장검사 등과 같은 조치가 포함되어야 하며 주의의무의 범위에 대한 기준의 정립이 요구된다. 이에 따라 각국은 정보보호를 위한 법제를 보다 강화할 것으로 예상된다.

8) 2009년 3월 17일 미국의 전자프라이버시정보센터(EPIC)는 구글 클라우드 컴퓨팅 서비스의 정보보안 및 프라이버시 위협에 대해 연방거래위원회(FTC)에 민원을 제기하기 이에 대한 조사를 요청한 바 있다.

문제는 클라우드 컴퓨팅 사업은 국경을 넘어서 이루어지기 때문에 각국의 정보보호법을 동시에 충족하여야 한다는 점이다. 클라우드 컴퓨팅 서비스 제공자뿐만 아니라 클라우드 서비스 이용 기업도 각국의 보안 및 프라이버시 관련 IT컴플라이언스를 준수하지 않을 경우, 법적 소송 등의 문제에 직면할 수 있다. 따라서 우리나라 기업들도 국내법 외에 미국의 사베인즈 옥슬리법(Sarbanes Oxley Act), HIPPA(Health Information Portability and Accountability Act), 프라이버시 영향평가, ISO 27001 보안 인증 등 기업의 위험관리 및 투명성 강화를 위해 국제적으로 널리 알려진 각종 규제를 충족하기 위한 조치를 취해야 한다.

또한, IT 컴플라이언스와 관련해서는 정보 보관(data retention)에 대해서 각국의 입법례가 서로 달라서 어느 나라의 규제를 준수해야 하는지가 논란이 있을 수 있다. 길게 보관해도 법을 어기는 것이 될 수 있고 너무 짧게 보관해도 법을 어긴 결과를 초래하기 때문이다.

3.6 서비스 종속화와 클라우드 사업자의 교체 · 이전

클라우드 컴퓨팅 사업자는 각자가 자체적인 플랫폼으로 이용자에게 서비스를 제공하기 때문에 하나의 클라우드 컴퓨팅 서비스를 이용하기 시작하면 이용자는 서비스를 제공받고 있는 사업자를 쉽게 교체하기 어렵다. 자사의 모든 정보를 클라우드 컴퓨팅 사업자가 보관하고 있기 때문에 클라우드 컴퓨팅 사업자의 협력이 없이는 정보의 회수가 어렵고, 설사 정보를 회수할 수 있다고 하더라도 다른 클라우드 컴퓨팅 서비스를 제공하는 사업자와 서비스 표준화가 되어 있지 않다거나 어플리케이션의 호환성이 보장되어 있지 않으면 정보를 활용할 수 있는 방법이 없다.

이에 따라 이용자는 중·장기적으로 하나의 클라우드 컴퓨팅 사업자에게 종속될 수밖에 없게 되고 부당한 요금인상, 서비스 질 저하, 피해복구 지연 등 서비스제공자에 의한 갖가지 횡포를 감수해야 할 가능성이 크다. 따라서 이용자가 언제든지 자신의 정보 등을 회수하고 다른 사업자에게로 이전할 수 있도록 이용자의 권리를 보장해야 하며, 이와 같은 이용자의 권리가 실현될 수 있도록 사업자간 서비스 표준화, 어플리케이션 호환성 등을 법률적으로 보장해야 할 것이다.

3.7 사생활 및 영업비밀 보호와 압수 · 수색

클라우드 컴퓨팅 서비스의 데이터센터가 있는 국가는 국가안보, 범죄수사 등을 목적으로 해당 데이터센터에 저장된 정보에 광범위하게 접근, 취득할 가능성이 커진다. 미국의 경우 「애국법(USA PATRIOT Act, 2001)」, 「미국 보호법(Protect Americana Act, 2007)」, 해외정보감시법(Foreign Intelligence Surveillance Act, 2008)」 등에서 국가안보 목적으로 정부에 의한 영장없는 감청 등이 허용되고 있어, 클라우드 컴퓨팅 사업자의 서버에 저장되어 있는 이용자 정보에 대한 전자감시 문제가 논란이 되고 있다.

영국의 경우도 「조사권한 제한법(Regulation of Investigatory Powers Act 2000)」 Part II, 제28조가 공무원들에게 컴퓨터에 저장된 데이터에 접근하기 위해 영장을 획득할 수 있는 범위를 넓게 인정하고 있다. 대표적인 사례가 영국의 경제적 안녕을 목적으로 한 컴퓨터 데이터 접근권이다.[9]

우리나라도 통신비밀보호법, 전기통신사업법 등에 의해서 정보 · 수사기관에게 영장없이 컴퓨터에 저장된 데이터를 요구할 수 있는 권한이 폭넓게 인정되고 있고, 형사소송법(제106조)상 전자우편 등의 디지털정보가 마치 물건과 같이 취급되고 있는 점을 악용하여 정보 · 수사기관들이 디지털 정보를 압수 · 수색함에 있어서 압수 · 수색의 대상과 범위를 특정하지 않는 포괄적 압수수색이 관행화되다시피 하고 있다. 클라우드 컴퓨팅 사업자가 운영하는 데이터센터에는 보다 많고 다양한 정보들이 혼재되어 있을 수 있다는 점을 감안한다면 해당 범죄와 무관한 정보가 정보 · 수사기관의 손에 넘어가지 못하게 하는 안전장치가 필요하다. 특히 사생활 정보나 영업비밀이 정보 · 수사기관의 손에 넘어간다면 이용자의 사회생활이나 사업에 치명적인 영향을 미칠 수 있다.

위와 같은 국내법이 없더라도 개인정보보호 또는 사생활보호 법규가 미비한 국가나 독재적 경찰국가 또는 국제협정을 존중하기 않는 국가는 국가안보나 자국의 이익 등을 위해 자국에 있는 클라우드 컴퓨팅 데이터센터 시스템이나 데이터를 압수할 수 있고, 법집행을 위해 필요한 범위 이상의 개인정보에 권한없이 접근할 위험

9) Miranda Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law", 「Technology and Society」, Volume 6, no.1, 2009 4. p.4.

이 있다. 특히 클라우드 컴퓨팅 사업자가 해외에 서버를 둔 경우에는 국내 기업의 산업기밀 유출 등의 문제가 발생할 수도 있다.

이점 개인정보 및 중요정보의 국외이전 제한 완화 문제와 밀접한 관련이 있는 사항으로서, 클라우드 컴퓨팅 사업자는 이처럼 사생활과 영업비밀이 법에 의해서 보호받지 못하거나 국가권력에 의해서 사생활과 영업비밀이 침해받기 쉬운 국가에는 데이터센터를 두는 것은 피해야 할 것이다.

3.8 기타

이밖에 클라우드 컴퓨팅 서비스에서는 각종 정보가 서비스 제공자의 수중에 맡겨져 있기 때문에 서비스 이용자가 직접 관리할 때보다 영업미밀 누설, 저작권 침해 등의 문제를 발생할 소지가 높다. 계약이나 법률에 의해서 보호받을 수 있다고 하더라도 한번 누설되거나 침해된 권리는 완전히 복구되기 어렵다.

또한 클라우드 컴퓨팅 서비스 이용 기업이 파산하는 경우, 클라우드에 존재하는 해당 기업의 영업비밀, 고객정보 등에 대한 이용, 관리, 파기 등도 문제될 수 있다. 클라우드 컴퓨팅 서비스를 제공하는 서비스제공자와 클라우드 서비스 이용 기업의 고객 사이에는 아무런 계약관계가 없기 때문에 이용 기업이 파산하거나 사용료를 연체할 경우 그 기업의 소비자가 불측의 피해를 볼 수 있다. 따라서 이용 기업의 소비자를 보호하기 위한 적절히 장치가 반영되어야 한다.

Ⅳ. 맺음말

클라우드 컴퓨팅 서비스의 많은 장점에도 불구하고 아직 기업들이 서비스의 가용성, 데이터 보안, 자사 데이터에 대한 통제권 확보, 종속성 등의 문제로 클라우드 컴퓨팅 서비스의 이용을 꺼리고 있다. 그러나 이 같은 문제들은 기술개발, 표준화, 표준약관, 서비스수준협약(SLA) 등으로 어느 정도 해결이 가능하다.

하지만, 데이터가 여러 국가에 복제되어 분산 저장될 경우 데이터의 국외이전 금지 문제, 데이터의 보관 및 파기 의무, IT 컴플라이언스, 수탁자의 불법행위에 대한 위탁자의 책임, 자신의 데이터센터에 저장된 불법정보에 대한 클라우드 서비스제공자의 책임범위, 클라우드 서비스제공자의 책임제한 등 현행법상의 법적 규제와 충돌되는 부분에 대해서는 법·제도적 접근과 검토가 필요하다.

클라우드 컴퓨팅 산업의 촉진 및 이용 활성화를 위해서는 구체적으로 다음과 같은 사항이 법제도적으로 검토되어야 한다. ① 클라우드 서비스나 솔루션을 시험할 수 있는 테스트베드 구축 등 시범사업 근거 마련, ② 분야별 특화된 클라우드 서비스 모델 개발 및 사업화를 위한 정부 시책 추진 및 지원 근거 마련, ③ 민·관의 포괄적 협력 기반 조성 및 정부의 기술 개발·연구 지원체계 마련, ④ 사전 인증 및 사후 보증체계 구축을 통한 클라우드 서비스의 신뢰성 및 안정성 제고, ⑤ 클라우드 서비스의 상호운용성 확보를 위한 표준화, ⑥ 클라우드 컴퓨팅의 정보보안, 개인정보보호 등 각종 법률 이슈와 예상되는 다양한 이해관계 충돌 문제에 대응할 수 있도록 서비스제공자와 이용자 대상지침 근거 마련, ⑦ 클라우드 속에 있는 기업의 정보자산에 대한 접근권 보장, ⑧정보자산의 실제 위치와 선택권 보장, ⑨ 정보자산의 부적절한 접근 방지와 오남용 방지, ⑩ 클라우드 서비스 제공기업 또는 서비스 자체의 영속성 보장, ⑪ 서비스 장애 책임범위와 분담, ⑫ 소프트웨어 라이선스 등에 대한 규정이 고려되어야 한다.

참고문헌

<국내문헌>

[1] 김성훈/이종화/이응용/한정화, "차세대 디지털 패러다임 「클라우드 서비스」와 정보보호", 「CSO Briefing」, 한국정보보호진흥원, 2009. 4.

[2] 김재우/신현석/장현춘, "클라우드 컴퓨팅 기술의 전략적 의미와 활용", 「SW Insight 정책리포트」, 한국소프트웨어진흥원, 2009. 7.

[3] 김희연, "미국의 클라우드 컴퓨팅 이용 현황", 「정보통신정책」, 정보통신정책연구원, 2008. 10.

[4] 성병용, "국내 기업의 클라우드 컴퓨팅 동향 및 전략", 「SW Insight 정책리포트」, 한국소프트웨어진흥원, 2009. 7.

[5] 이창범/강이석, "클라우드 컴퓨팅 관련 법적 이슈 및 관련 산업 발전에의 시사점 - 이용자 정보보호와의 관계를 중심으로-", 한국정보보호진흥원, 2009. 3.

[6] 정제호, "클라우드 컴퓨팅의 현재와 미래, 그리고 시장전략", 한국소트프웨어진흥원 정책연구센터, 2008. 10.

[7] 한국과학기술정보연구원, "클라우드 컴퓨팅 동향",

「클라우드컴퓨팅포럼 워크숍」, 2009. 12. 2.
[8] 한국소프트웨어진흥원 정책연구센터, "클라우드 컴퓨팅 확산의 10대 장애 요소", 「SW Insight 정책 리포트」, 한국소프트웨어진흥원, 2009. 5.
[9] 한국정보화진흥원, "범국가 차원의 ICT신기술 패러다임 : 클라우드 컴퓨팅 활성화 전략", 「CIO REPORT」 Vol. 17, 2009. 11.

<국내웹사이트>
[1] 공정거래위원회 : www.consumer.go.kr.
[2] 한국클라우드서비스협회 : www.kcsa.or.kr.
[3] 한국클라우드컴퓨팅연구조합: www.cccr.or.kr.

<해외문헌>
[1] Andrew Joint / Edwin Baker / Edward Eccles, "Hey, you, get off of that cloud?", 「Computer Law & Security Review」, 2009.
[2] Barry Reingold, Ryan Mrazik, "Cloud Computing : The Intersection of Massive Scalability, Data Security and Privacy", 「Cyberspace Law」, 2009. 6.
[3] Cloud Security Alliance(CSA), "Security Guidance for Critical Areas of Focus in Cloud Computing", 2009. 4.
[4] David Navetta, "Legal Implications of Cloud Computing-Part One(the Basics and Framing the Issues)", 2009. 9. 12.
[5] David Navetta, "Legal Implications of Cloud Computing-Part Three(Relationships in the Cloud)", 2009. 10. 21.
[6] ENISA, "Cloud Computing : Benefits, risks and recommendations for information security", 2009. 11. 9.
[7] Jeffrey F. Rayport/Andrew Heyward, "Envisioning the Cloud : The Next Computing Paradigm", Marketspace, 2009. 3. 20.
[8] Laurin H. Mills, "Legal Issues Associated with Cloud Computing", NIXON PEABODY LLP, 2009. 5. 13.
[9] Microsoft, "Privacy in the Cloud Computing Era : A Microsoft Perspective", 2009. 11.
[10] Miranda Mowbray, "The Fog over the Grimpen Mire : Cloud Computing and the Law", 「Technology and Society」, Volume 6, no.1, 2009 4.
[11] Paula J. Bruening / Bridget C. Treacy, "Cloud Computing : Privacy, Security Challenges", 「PRIVACY & SECURITY LAW」, 2009. 3. 9.
[12] Peter Mell / Tim Grance (NIST, Information Technology Laboratory), "Effectively and Securely Using the Cloud Computing Paradigm", 2009. 10. 7.
[13] Philip Nolan, "Cloud Computing : the Legal Issues", Mayson Hayes+Curran, 2009. 2. 25.
[14] Robert Gellman, "Privacy in the Clouds : Risks to Privacy and Confidentiality from Cloud Computing", WORLD PRIVACY FORUM, 2009. 2. 23.
[15] Tanya Forsheit, "Legal Implications of Cloud Computing-Part Two(Privacy and the Cloud)", 2009. 10. 17.
[16] Tanya Forsheit, "Legal Implications of Cloud Computing-Part Four(E-Discovery and Digital Evidence)", 「INFORMATION LAW GROUT」 2009. 11. 27.
[17] Tanya Forsheit, "International Regulatory Issues in the Cloud", 2009. 9. 30.

<해외 웹사이트>
[1] Electronic Privacy Information Center(EPIC) : www.epic.org.
[2] INFORMATION LAW GROUP: inforlawgroup.com.
[3] Marketspace : www.marketspaceglobal.com.

〈著者紹介〉

이 창 범 (Changbeom Yi)
정회원
1988년 8월: 동국대학교 법과대학 졸업
1996년 8월: 동국대학교 법과대학 일반대학원 졸업(법학박사)
1988년 3월~1999.12: 한국소비자원 책임연구원
2001년 11월~현재: 한국인터넷진흥원 수석연구원
<관심분야> 정보보호법, 인터넷법, 과학법, 소비자보호법