클라우드 컴퓨팅 활성화를 위한 법제도 개선방안

Methods of Improving the Legal System to Promote Cloud Computing

정보통신산업진흥원 정제호 박사

숭실대학교 김수동 교수

대중소기업 협력재단 국신욱 과장

한국클라우드서비스협회 민영기 사무국장

단국대학교 손승우 교수

SK C&C 신수정 상무

이화여자대학교 양희동 교수

한국인터넷진흥원 이종화 박사

요 약 문

클라우드 컴퓨팅은 회사가 자신의 인프라를 구축하여 시스템을 이용하는 것이 아니라 제3의 인프라를 이용하여 마치 지신의 컴퓨터처럼 자유롭게 사용하고 이용하는 신개념으로써 최근 IT산업의 새로운 모델로서 자리를 잡아가고 있다. 그러나 사용자의 데이터가 클라우드서비스 제공자의 서버에 저장되고 관리되는 특성으로 인해 갑작스런 서비스 중단이나 장애에 대한 사용자의 우려가 크고, 데이터 외부보관에 따른 기밀 유출, 클라우드 시스템 간 호환성 부족으로 인한 종속성에 대한 우려가 존재한다. 특히 사용자가 기업인 경우 갑작스런 서비스 장애, 서비스 제공자의 파산으로 인한 비즈니스 패해가 광범위할 수 있다. 이러한 위험에 대한 사전 대비는 클라우드 컴퓨팅 활성화를 위해 선행되어야 할 중요한 과제이다. 이에 본 고에서는 클라우드 컴퓨팅 사업자의 파산 및 시스템 장애에 따른 사용자 보호방안, 보안 및 정보유출 우려 해소방안 등을 탐색하였다. 또한 클라우드 컴퓨팅의 서비스 품질 확보를 위한 SLA가이드라인 제정방안과 기술적·제도적 대응전략을 제시하며, 마지막으로 클라우드 간 상호운용성 확보를 위한 기술적·제도적 대응방안을 제시하였다.

첫째, 클라우드 컴퓨팅 사업자 파산 등으로 인한 서비스 중단에 대한 사용자 보호방안에 대한 연구결과는 다음과 같다. 해외에서는 개발기업의 기술력을 보호하고 사용기업의 안정적 사업 수행을 보장하기 위한 기술자료 임치제도를 변형한 클라우드 임치제도를 이용하여 클라우드 사용 기업을 보호하고 있다. 클라우드 임치제도는 클라우드 컴퓨팅 제공기업의 시스템 및 데이터 등을 임치기관이 이중화하여 보호하면서, 클라우드 컴퓨팅 제공기업이 서비스를 중단하는 경우 임치기관이 한시적으로 클라우드 컴퓨팅 제공기업의 업무를 수행하는 제도이다. 클라우드 사용 기업은 한시적인 기간 동안 서비스를 대신 제공받으면서 새로운 서비스 제공업체를 찾을 수 있고 데이터의 멸실 등도 방지할 수 있다.

클라우드 컴퓨팅 활성화를 위해 국내도 정부차원에서 클라우드 컴퓨팅 서비스 제공사의 서비스 중단을 해소할 수 있도록 서비스 중단에 대한 법 · 제도적 장치 마련해야 할 것이다. 이를 위하여 정부는 소프트웨어산업 진흥법 등 관련 법률에 클라우드 표준약관 및 표준계약서, 그리고 이용자보호지침을 제정할 수 있는 법적 근거를 마련해야 할 것이다. 또한 자체적으로 이중화 설비를 마련하지 못하는 중소기업에 대해서는 정부가 일정 부분 지원하여 클라우드 임치제도를 활용하도록 하는 방안이

필요하다.

둘째, 클라우드 컴퓨팅 사업자의 시스템 장애 등으로 인한 일시적인 서비스 중단에 따른 사용자 보호방안은 다음과 같다. 클라우드 컴퓨팅 서비스 장애 발생과 관련하여 이용자 보호를 국내 법제도상의 장치로는 전기통신사업법 상에서 정보통신서비스 제공자의 이용(서비스)약관을 방송통신위원회에 등록하도록 하고, 이에 근거한 금전적인 보상이 유일하다. 그러나 법적용의 대상이 기간통신사업자, 별정통신사업자, 일부 부가통신사업자로 국한되어있어 새로운 컴퓨팅 서비스인 클라우드 컴퓨팅 사업자에 대한 고려는 이루어지지 않고 있다. 이에 현행 전기통신기본법 및 전기통신사업법 상에 클라우드 컴퓨팅에 대한 정의와 유형, 사업자 분류가 반영되도록 할 필요가 있다.

또한 정보통신망이용촉진및정보보호등에관한법률(이하 정통망법)에 의한 서비스 이용약관 관련 의무조항의 수준과 범위, 면책범위 등이 공급자 위주로 구성되어 있고, 손해배상의 대상도 서비스 중단과 같이 모호한 표현으로 되어 있어 실질적인 사용자 보호에는 미흡하다. 이에 정통망법 상의 서비스 중단 및 제한 범위를 공급자 위주가 아닌 수요자 중심으로 개선을 추진할 필요가 있으며, 이를 위해 동법 시행령 이용(서비스)약관 관련사항 개선하고 그 의무조항의 수준과 범위를 구체화할 필요가 있다. 또한 사업자별 이용(서비스) 약관상의 손해배상 범위 및 규모를 현실화하고, 손해배상도 가용률 기반의 표준 SLA가이드라인을 작상하고 이를 반영하여 배상의 수준과 범위를 차등화 할 필요가 있다. 또한 손해배상 규모를 현실에 맞게 상향 조정하고 사업자간 분쟁조정을 위한 분쟁조정체계의 구축을 고려해야 할 것이다. 서비스 사업자의 면책범위도 개선(원인불명의 서비스 장애에 대한 사업자 책임 부여 등)이 필요하다.

셋째, 클라우드 컴퓨팅의 보안 및 정보 유출에 따른 사용자 보호 방안에 대한 연구결과는 다음과 같다. 현재 정보보호와 관련한 관련법으로는 '정보통신망 이용촉진 및 정보보호에 관한 법률', '공공기관의 개인정보보호에 관한 법률', '신용정보이용 및 보호에 관한 법률', '통신비밀보호법'등이 있다. 정통망법은 현재의 법률로도 클라우드 컴퓨팅 사업자에 대한 정보보호를 규제할 수 있다. 그러나 IDC, ISP 등 기존 정보통신 서비스 사업자중심으로 클라우드 컴퓨팅 서비스 제공자에 대한 고려가 부재

하고 데이터의 물리적 위치 변경 시 데이터 보호 및 프라이버시 대응 요건이 충분히 제시되지 않고 있다. 또한 데이터를 보호하고 있는 물리적 위치가 해외일 경우 서비스 제공자의 물리적 시설에 대한 점검관련 법규 적용을 어떻게 해야 하는지 불명확하고, 안전진단 제도도 클라우드 컴퓨팅 서비스 사업자의 환경을 충분히 반영하지 못한다. 정보보호관리체계 인증제도 역시 보안항목이나 적용 대상이 클라우드 컴퓨팅 환경에는 적용되기 어려운 문제점이 있다. 또한 데이터가 국외에 물리적으로 분산되어 있을 경우 법률 적용의 이슈, 데이터가 국외로 이동 시 해당 국가의 정부에서 데이터를 조사할 수 있는 권한이 있는 경우 국내 공공기관이나 금융기관에 클라우드 컴퓨팅 서비스를 받도록 허용할 지 등의 이슈가 해결되지 않고 있다.

이에 클라우드 컴퓨팅 보안관련 법, 제도의 개선을 위해서는 클라우드 컴퓨팅 서비스 제공자의 보안/데이터보호 신뢰성 제고를 위한 법규 신설이 필요하며, 공공/금융기관에 대한 클라우드 컴퓨팅 서비스 사용 정책에 대한 법규 보완이 필요하다. 또한 데이터가 글로벌하게 분산 시 해당 데이터 및 데이터를 보관하고 있는 시스템, 시설에 대한 감사, 감독, 필요 시 수사를 현재의 국내 법 체계로 대응할 수 있는지 점검하여 보완할 필요가 있다. 이를 위해 '클라우드 컴퓨팅 데이터 보호에 관한 법규' 항목을 신설하거나, 기존의 '정보통신망 이용촉진 및 정보보호에 관한 법률'에 추가하여 반영하고 세부 지침을 제시하는 방안이 필요하다. 현재 정통망법에도 대부분의 보안지침이 포함되어 있어 신규법규 신설보다는 기존 법체계하에서 클라우드 컴퓨팅 보안 관련 항목을 반영하는 것이 더 효율적이라 할 수 있다.

한편 클라우드 컴퓨팅 보안관련 규정에는 데이터의 물리적 위치 변동에 따른 관리, 해킹대응방안, 접근권한, 프라이버시 침해방지, 데이터 유출 방지, 수사/소송 시 협조 등의 항목이 반영되어야 한다. 또한 기존의 안전진단 제도에도 클라우드 컴퓨팅 서비스 제공자 그룹이 추가로 반영되어야 한다. 법규 제정과 더불어 클라우드 컴퓨팅 서비스 제공자를 위한 보안 인증 제도를 도입을 고려할 필요가 있다. 인증제도 역시 현재의 KISA 정보보호관리체계(ISMS) 인증 제도를 보완하여 활용하는 방안과, 별도의 독립적인 보안 인증 제도를 수립하는 방안이 고려될 수 있다. 전자는 기존의 인증프로세스, 심사원 등 인증체계를 그대로 활용할 수 있다는 면에서 장점을 가지고 있으나 클라우드 컴퓨팅 서비스의 보안 문제가 명확히 해결되었다는 것을 인증하

기 어려운 단점이 있다. 후자는 클라우드 컴퓨팅 서비스의 보안 이슈를 명확히 대응할 수 있다는 장점이 있으나 별도 인증 제도를 운영에 따른 비효율성이 존재한다. 이에 컴퓨팅 서비스의 품질을 포함한 주요 영역을 다루는 포괄적인 인증체계를 도입하고, 보안을 그 중 하나의 요소로 고려하는 방안이 고려될 수 있다.

넷째, 클라우드 컴퓨팅의 서비스 품질 확보를 위한 SLA가이드라인 제정방안과 기술적·제도적 대응방안을 위한 연구결과는 다음과 같다. 현재 해외의 주요 클라우드 컴퓨팅 사업자들은 대표되는 가동시간보장률(Uptime guarantee)이 99.9% 이상으로 규정하여 서비스를 제공하고 있으나, 국내 클라우드 컴퓨팅 사업자들은 아직 SLA에 대한 개념이 미흡하며, 주로 이용약관에 따른 손해배상을 명시하고 있다. 그러나 그 구체성이나 피해보상의 수준과 범위가 클라우드 컴퓨팅 이용자의 요구수준을 충족시키기에는 매우 부족하다.

이에 국내 클라우드 컴퓨팅을 위한 표준 SLA가이드라인을 제정하여 보급할 필요가 있으며, 이를 위해 클라우드 컴퓨팅의 품질속성을 반영할 수 있는 측정지표를 명시하고 이를 SLA 가이드라인에 반영할 필요가 있다. 이 같은 품질속성은 MTBF (Mean Time Between Failure), MTTR (Mean Time To Repair), MTTF (Mean Time To Fail), MTD (Maximum Tolerable Downtime), ABA (Abandonment Rate), ASA (Average Speed to Answer)등과 같이 구체적으로 제시되어야 한다. 또한 서비스 품질 속성들이 지켜지고 있는지 확인 할 수 있도록 동적인 모니터링 환경을 제공 해야 한다. 이를 위해 시스템 설계를 위한 기술적 지침을 만들어 배포할 필요가 있으며, 그 주요 내용으로 동적 모니터링 기법과 서비스 오류에 대한 자동교정기법 등 주요한 기술적 요인들에 대한 기술적 대안을 포함할 필요가 있다. 또한 제도적으로는 클라우드 컴퓨팅 서비스 품질확보를 위한 인증제도를 마련하여 시행할 필요가 있다. 인증제도의 내용으로는 SLA가이드라인 준수여부와 정보보호 및 보인이슈 관리수준, 서비스 중단 및 장애에 대응한 전략적 대응체계(임치제 및 Mirroring등의 데이터보호방안) 보유여부 등을 포괄적으로 검토할 필요가 있다.

다섯 번째 클라우드 컴퓨팅의 상호운용성 확보를 위한 기술적, 제도적 지원방안에 대한 연구결과는 다음과 같다. 클라우드 컴퓨팅의 상호운용성이 확보되지 못할 경우

클라드우 컴퓨팅에서 상호운용성이 확보되지 못할 경우 사업자나 벤더로 부터의 데이터 고착화(Lock-in)가 발생하고, 사업자나 벤더의 플랫폼 또는 서비스로 종속될 수 있다. 특히 이종 클라우드 컴퓨팅간 서비스 연동 어려움, 개별적인 클라우드에 대한 별도의 솔루션 개발 등으로 인한 서비스 보급 지연 등이 발생할 수 있다. 이러한 문제점 해결을 위해 2009년 초부터 OCC, CCIF, OGF, DMTF, CSA 등의 사실 표준화 기구들이 클라우드 컴퓨팅 표준화를 위한 노력을 본격화하고 있으며, 우리나라도 '클라우드컴퓨팅포럼'을 중심으로 표준화 노력이 이루어지고 있다.

클라우드 컴퓨팅의 상호운용성 확보를 위해서는 표준화된 클라우드 플랫폼과 인터페이스 정의를 포함한 다양한 표준 규격의 개발과 확산을 지원해야 하며, 그 주요 이슈와 대상은 크게 요구사항, 공통프레임워크를 포함하는 '공통표준', 인터페이스, 데이터 교환 등을 위한 '데이터 고착화 방지표준', SLA 및 QoS확보를 위한 '서비스 품질 (QoS) 표준', 보안 프레임워크 및 메커니즘을 위한 '보안표준', 안전한 데이터 포맷 및 이용방식을 위한 '데이터 기밀성 및 감사성 (Auditability) 표준', 데이터의 소유권 관리를 위한 '데이터 소유권 표준', 사용자의 데이터 인증방식 및 규격과 관련한 '데이터 소유권 표준', 사용자의 데이터 보호방식 및 정책과 관련한 '데이터 프라이버시 표준', 클라우드 간 상호운용성 확보를 위해 필수적인 표준 프로토콜 및 데이터 포맷규격을 확보를 위한 '인터 클라우드 상호운용성 표준', 다중 디바이스 지원을 위한 '장치 독립성 표준' 등이 존재한다.

우리나라도 보다 세부적인 클라우드 컴퓨팅 상호운용성 확보를 위해 구체적인 표준화 대상 분야와 기술을 선정하여 논의를 진행시킬 필요가 있다. 특히 현재 정부가 추진 중인 공공부문 클라우드 컴퓨팅 도입계획과 관련하여 공공 간, 공공-민간 간 클라우드 상호운용성 확보를 위해 조속히 표준 프레임워크를 설정하고, 이를 적용해야 할 것이며, 클라우드 컴퓨팅 표준화를 위해 진행 중인 민간부문의 노력을 지원할 필요가 있다.

본 고에서는 사업자 파산에 따른 서비스 중단, 갑작스런 서비스 장애, 보안에 대한 우려, 서비스 품질 확보, 클라우드 간 상호운용성 부족으로 인한 소비자 선택권 제한 등 주로 수요자 관점에서 발생할 수 있는 우려를 해소하기 위한 기술적, 제도적 보호방안들을 살펴보았다. 그러나 제도적인 보호만으로는 시장 활성화는 요원하

며, 자칫 수요자 보호를 위해 공급자에게 과도한 법·제도적인 의무를 부과할 경우 오히려 시장 활성화에 저해가 될 수 있다. 이에 클라우드 컴퓨팅 시장 활성화를 위한 법·제도개선은 시장의 발전과 성숙도 등을 고려하여 이루어져야 할 것이다. 또한 시장 활성화를 위해서는 법·제도의 개선과 함께 기술개발 및 수요시장 활성화 등 보다 다양한 정책적 지원책이 필요하다. 이에 수요시장 활성화와 공급자 개발역량 강화를 위한 다양한 정책적 지원이 함께 추진되어야 할 것이다.

클라우드 컴퓨팅 시장은 지속적으로 확대되고, 그 수준과 범위도 현재의 PC를 넘어 넷북, 스마트폰 등으로 광범위하게 확산될 것이다. 그러나 아직까지 그 무한한 도전과 기회는 글로벌 기업들에 의해 주도되고 있다. 이제 막 꽃피우기 시작한 새로운 시장에서 우리나라의 IT기업과 SW기업들의 새로운 도약을 위한 전략설정과 정부의 현명한 대응이 요구된다.

Abstract

Recently, “cloud computing” has established itself as a new model in the IT industry, and as a new concept whereby companies can freely utilize the third infrastructure as if it were their own infrastructure, instead of developing and using their own proprietary system with their infrastructure. However, users are very concerned about unforeseen service interruptions or malfunctions as the data is saved and managed by the service operated by the cloud service provider. Also, there is concern about dependency due to leaks of confidential information (as the data is saved outside) and insufficient compatibility among cloud systems. In particular, if the user is an enterprise, and the service is stopped abruptly or the service provider goes bankrupt, the damage to the business could be enormous. Therefore, it is important that preparatory measures against such risks be taken to promote cloud computing.

Therefore, this paper reviews the method of protecting users against the cloud computing service provider’s bankruptcy and system malfunction, and resolved concerns about the risk of security and information leakage. In addition, this paper proposes a method of making an SLA guideline and technical and policy response strategies to secure the service quality of cloud computing. Lastly, it proposes technical and policy response methods to secure interoperability among cloud computing services.

First, we identified the following method of protecting users from service interruption caused by the cloud computing service provider’s bankruptcy. Overseas countries protect cloud computing use enterprises using the cloud computing deposit system that modifies the technical data deposit system, in order to protect the technical capability of development

companies and ensure that the business operations of enterprises using the service are stable. When the cloud computing deposit system is used, the deposit agency performs the duties of the cloud computing service provider temporarily in the event that the service provider stops the service, while protecting the system and data of the cloud computing service provider in duplication. Companies using the cloud computing could find a new service provider and prevent the loss of data while the deposit agency is providing the service temporarily.

To promote the use of cloud computing, Korea will also need to prepare laws and policies to cope with service interruption, so that service interruptions can be responded to at the governmental level. To that end, the government needs to prepare the appropriate legal grounds, including a cloud computing standard agreement, standard contract, and user protection guidelines according to the relevant laws and regulations, such as the Software Industry Promotion Law. In addition, the government needs to partially support small and medium-sized businesses which cannot afford to secure redundant equipment internally, so that they can utilize the cloud computing deposit system.

Second, users can be protected from temporary service interruptions caused by system malfunctions of the cloud computing service provider. In Korea the only legal policy for protecting users with regard to such malfunctions is stipulated in the Telecommunication Business Law, which requires registration of the service agreement with the Korea Communications Commission by the telecom service provider, so that monetary compensation can be made if the agreed service cannot be provided. However, the application service provider only includes the infrastructure communication service provider, special category service provider, and certain value-added communication service providers. As a

result, the new computing service provider (cloud computing service provider) is not considered at all. Therefore, it is necessary to reflect the definition, type, and service provider classification of cloud computing in the current Basic Telecommunication Law and Telecommunication Business Law.

In addition, the "Law regarding Promotion of the Use of the Information and Communication Network and Information Protection" (hereafter Information and Communication Network Law) stipulates the level and scope of mandatory clauses, and the scope of indemnity under the service use agreement for the preference of service providers. It also describes the damage compensation target ambiguously, like "server interruption". As such, it is insufficient to provide substantial protection to users, and thus it will be necessary to revise the Information and Communication Network Law in such a way that the scope of service interruption and limitation focuses on the consumers rather than the supplier. For this purpose, the item related to the use (service) agreement in the enforcement ordinance of this law should be improved and the scope and level of the mandatory clauses should be substantiated. In addition, the scope and scale of damage compensation in the use (service) agreement for each service provider should be readjusted to a realistic level, and standard SLA guidelines should be created for damage compensation based on the degree of availability; then, the scope and level of compensation needs to be differentiated by reflecting the newly created guidelines. In addition, the scale of damage compensation should be increased to a realistic level, and the establishment of a dispute mediation system should be considered in order to resolve disputes among service providers. The scope of exemption applicable to the service provider also needs improving (by imposing responsibility on the service provider

regarding service interruption resulting from unknown causes).

Third, the results of the study on cloud computing security and user protection against information leakage are as follows. Currently, the laws related to information security include the Information and Communication Network Law, the Law on Privacy Protection of Public Agencies, the Law on Credit Information Use and Protection, and the Communication Secrecy Protection Law. The current Information and Communication Network Law can regulate the information security of the cloud computing service provider. However, it focuses only on existing information and communication service providers such as IDC and ISP, while no consideration is given to the cloud computing service provider, and requirements for data protection and privacy protection are not fully presented when the physical location of the data is changed. In addition, if the physical location is an overseas country that protects the data, it is not clear how to apply the regulation related to inspection of the service provider's physical facilities, and the security diagnosis system doesn't fully reflect the environment of the cloud computing service provider. The certification policy for the information security management system has a problem in that its security item and application target cannot be applied to the cloud computing environment. In addition, if the data is distributed physically among overseas countries, the law application issue can arise. If the data is moved to an overseas country and the government of that country has the right to invest the data, the issue of whether a domestic financial institute or public agency will be allowed to use cloud computing service will remain unresolved.

Accordingly, a new law needs to be established to enhance the security and reliability of the data protection by the cloud computing service provider, in order to improve the laws and policies related to cloud

computing security. Also, the relevant laws and regulations need to be supplemented regarding the cloud computing service use of public/financial institutes. In addition, if the data is distributed globally, and the data, system, and facility storing the data need to be supervised and audited, it should be verified whether investment can be performed using the current domestic law, which should be supplemented if necessary. For this purpose, a new "Law regarding Cloud Computing Data Protection" needs to be established, or new articles need to be added to the Information and Communication Network Law, and the fine details need to be stipulated. As the current Information and Communication Network Law contains most security guidelines, it would be more efficient to reflect the items related to cloud computing security in that, rather than making a new law.

On the other hand, the regulations related to cloud computing security should include additional articles on such matters as managing changes in the physical location of data, countermeasures against hacking, access rights, privacy violation prevention, data leak prevention, and cooperation at the time of investigation/lawsuit. In addition, the current security diagnosis system should reflect the cloud computing service provider.

Besides establishment of the necessary law, the introduction of a security certification system for the cloud computing service provider needs to be considered. As regards the certification system, the ISMS (Information Security Management System) of the KISA (Korea Internet & Security Agency) could be supplemented, or a separate security certification system could be established. The former measure would have the advantage of utilizing the existing authentication system (certification system and reviewer) without the need for any change, but would also have the disadvantage of being unable to confirm whether the security

issue surrounding the cloud computing service is clearly resolved; the latter has the strength of being able to cope with the security issue in the cloud computing service clearly, but is inefficient as regards operation of the separate certification system. As a result, the introduction of a comprehensive certification system that handles major areas, including computing service quality, should be considered, with security as one of the components.

Fourth, the quality of cloud computing services can be secured, and the following SLD guidelines and technical and policy responses can be made. Currently, major overseas cloud computing service providers provide the service with an uptime guarantee of over 99.9%. However, domestic cloud computing service providers don't have the concept of the SLA sufficiently, and mainly specify damage compensation according to the user agreement instead. However, concreteness, level, and scope of damage compensation are quite insufficient to satisfy the cloud computing user's requirements.

Therefore, it is necessary to establish and diffuse standard SLA guidelines for cloud computing in Korea. To achieve this, measurement indices should be specified and reflected in the SLA guidelines, which would include the quality properties of cloud computing. The quality properties should be presented in detail - such as MTBF (Mean Time Between Failure), MTTR (Mean Time To Repair), MTTF (Mean Time To Fail), MTD (Maximum Tolerable Downtime), ABA (Abandonment Rate), and ASA (Average Speed to Answer). In addition, a dynamic monitoring environment should be provided to make it possible to check that the properties of service quality are being provided as agreed. For this purpose, technical guidelines for system design need to be composed and distributed, and their major contents need to include technical alternatives

regarding major technical factors, such as a dynamic monitoring technique and an automatic error correction technique. Also, a certification system needs to be established and implemented in order to secure the quality of the cloud computing service from the policy perspective. The content of the certification system needs to include conformance to the SLA guidelines, information security, security issue management level, and the availability of the strategic response system against service interruption and malfunction (data protection methods such as the deposit system and mirroring)

Fifth, the results of the study on technical and policy support methods to secure the interoperability of cloud computing are as follows. If the interoperability of cloud computing cannot be secured, data lock-in can occur by the service provider or vendor, or users can be dependent on the platform or service of a particular service provider or vendor. In particular it could be difficult to link services among heterogeneous cloud computing, or service distribution could be delayed due to the development of separate solutions for each cloud computing. Standardization organizations such as the OCC, CCIF, OGF, DMTF, and CSA have been doing their utmost to resolve these issues since early 2009, and standardization is being pursued in Korea - mainly by the "Cloud Computing Forum".

To secure the interoperability of cloud computing, the development and diffusion of various standard specifications should be supported, including a standardized cloud computing platform and interface definition. Major issues and targets include requirements: a "common standard" including a common framework; a data lock-in prevention standard for interface and data exchange; a "QoS standard" to secure the SLA and QoS; a "security standard" for a security framework and mechanism; a "data confidentiality

and audiability standard" for a secure data format and usage method; a "data property right standard" for data property right management; a "data property right standard" related to the user's data authentication method and specification; a "data privacy standard" related to the user's data protection method and policy; an "Inter-cloud interoperability standard" to secure the standard protocol and data format specifications, which are indispensable for interoperability among clouds; and a "device independency standard" to support multiple devices.

Korea also needs to select and discuss target areas and technologies for standardization in detail, in order to secure the interoperability of cloud computing in detail. In particular, the standard framework should be established and applied as quickly as possible to secure cloud computing interoperability among public bodies and between the public and private sectors, with regard to the government's plan to introduce cloud computing. The government also needs to support the efforts of the private sector to standardize cloud computing.

This study reviewed various technical and policy protection methods to resolve the concerns that may arise from the perspective of consumers, such as service interruption due to the service provider's bankruptcy, abrupt service malfunction, service quality, and the consumer's limited right of choice due to insufficient interoperability among cloud computing services. However, the market cannot be promoted with protection by the policy. If too excessive obligations are imposed on the service provider to protect the consumers, it could hinder market promotion. Therefore, improvements to the relevant law and policies regarding promotion of the cloud computing market should be made in consideration of market development and maturity; in addition, more diverse policy support is required to promote the market, such as technical development and

stimulation of market demand. Therefore, various policy support policies designed to promote market demand and strengthen the development capability of service providers should be implemented.

The cloud computing market is expected to grow continuously, and its level and scope will be expanded broadly to include Netbooks and smart phones as well as PCs. However, unlimited challenges and opportunities are driven by major global companies. As such, local IT companies and S/W companies must establish strategies for a new take-off, while the government must respond wisely in the fresh-blown new market.

목 차

제1장 서론 ····· 1
제 1 절 연구 배경 및 목적 ····· 2
제 2 절 연구 방법 및 구성 내용 ····· 3

제2장 클라우드 컴퓨팅 현황 및 문제점 ····· 5
제 1 절 클라우드 컴퓨팅 정의 및 유형 ····· 6
1. 클라우드 컴퓨팅의 정의 ····· 6
2. 클라우드 컴퓨팅과 타 컴퓨팅 용어와의 차이점 ····· 8
3. 클라우드 컴퓨팅의 유형 ····· 11
제 2 절 클라우드 컴퓨팅 시장동향 ····· 14
1. 클라우드 컴퓨팅 시장전망 ····· 14
2. 해외 시장 동향 ····· 16
3. 국내 시장동향 및 전망 ····· 17
제 3 절 국내 클라우드 컴퓨팅 시장 장애요인 ····· 21
1. 클라우드 컴퓨팅 확산의 장애요인 ····· 21
2. 법, 제도적인 문제점 ····· 23

제3장 클라우드 컴퓨팅 활성화를 위한 제도개선 방향 ····· 25
제 1 절 사업자의 파산 등에 따른 사용자 보호방안 ····· 26
1. 사업자 파산에 따른 문제점과 사례 분석 ····· 26
2. 사업자 파산 등에 따른 사용자 보호를 위한 해외사례 ····· 30
3. 사업자 폐업 등에 따른 사용자 보호를 위한 국내 현황 ····· 36
4. 서비스 중단방지 및 사용자 보호를 위한 법 · 제도 개선방안 ····· 41
제 2 절 일시적 서비스 장애에 따른 사용자 보호방안 ····· 43
1. 클라우드 컴퓨팅 서비스 장애의 개념 ····· 43

2. 클라우드 컴퓨팅 서비스의 장애 사례 ····· 45
3. 현행 법제도상의 서비스 사용자 보호 장치 ····· 52
4. 현행 법제도상의 문제점 ····· 56
5. 개선방안 ····· 63
제 3 절 사용자 보안우려 해소 방안 ····· 70
1. 클라우드 컴퓨팅 보안을 위한 해외 법, 제도 및 인증 현황 ····· 71
2. 클라우드 컴퓨팅 보안을 위한 국내 법, 제도 및 인증 현황 ····· 81
3. 클라우드 컴퓨팅 보안을 위한 법·제도 개선의 필요성 및 개선방안 ····· 95

제4장 클라우드 컴퓨팅 활성화를 위한 기술적 대응전략 ····· 107
제 1 절 클라우드 컴퓨팅 서비스 품질 확보 방안 ····· 108
1. 서비스 품질과 SLA의 중요성 ····· 108
2. SLA관련 국제표준 ····· 109
3. 클라우드 컴퓨팅 SLA 해외 사례 ····· 123
4. 국내 기업의 SLA현황 ····· 127
5. 클라우드 컴퓨팅 환경의 SLA 프레임워크와 서비스 품질 확보방안 ····· 128
제 2 절 클라우드 컴퓨팅 상호운용성확보방안 ····· 136
1. 클라우드 컴퓨팅 상호운용성의 필요성 ····· 136
2. 클라우드 컴퓨팅 상호운용성 확보를 위한 글로벌 동향 ····· 139
3. 클라우드 컴퓨팅 상호운용성 확보를 위한 국내 움직임 ····· 146
4. 클라우드 컴퓨팅 상호운용성 확보를 위한 기술적, 제도적 대안 ····· 147

제5장 결론 및 시사점 ····· 153

Table of Contents

1. Preface ····· 1

1.1 Study background and objectives ····· 2

1.2 Study method and composition ····· 3

2. Current status and issues surrounding cloud computing ····· 5

2.1 Definition and types of cloud computing ····· 6

2.1.1 Definition of cloud computing ····· 6

2.1.2 Difference between cloud computing and other computing terms ·· 8

2.1.3 Types of cloud computing ····· 11

2.2 Cloud computing market trend ····· 14

2.2.1 Prospects for the cloud computing market ····· 14

2.2.2 Overseas market trend ····· 16

2.2.3 Domestic market trend and prospects ····· 17

2.3 Obstacles to the domestic cloud computing market ····· 21

2.3.1 Obstacles to the expansion of cloud computing ····· 21

2.3.2 Legal and policy issues ····· 23

3. Policy improvement direction to promote cloud computing ····· 25

3.1 Methods of protecting users against service provider's bankruptcy ·· 26

3.1.1 Problems and case analysis with regard to service provider's bankruptcy ····· 26

3.1.2 Overseas cases of protecting users from service provider's bankruptcy ····· 30

3.1.3 Domestic status of user protection against closure of service provider's business ····· 36

3.1.4 Methods of improving the regulations and policies to prevent service interruption and protect users ····· 41
3.2 Methods of protecting users against temporary service interruption ·· 43
3.2.1 Concept of cloud computing service interruption ····· 43
3.2.2. Cases of cloud computing service interruption ····· 45
3.2.3 Service user protection systems under the current law and policy ····· 52
3.2.4 Problems with the current law and policy ····· 56
3.2.5 Improvement methods ····· 63
3.3 Method of resolving user's concerns about security ····· 70
3.3.1 Domestic law, policy, and authentication status for cloud computing security ····· 71
3.3.2 Overseas law, policy, and authentication status for cloud computing security ····· 81
3.3.3 Necessity and methods of improving laws and policies for cloud computing security ····· 95

4. Technical response strategy to promote cloud computing ····· 107
4.1 Method of securing the quality of the cloud computing service ····· 108
4.1.1 Importance of service quality and SLA ····· 108
4.1.2 International standards related to SLA ····· 109
4.1.3 Overseas cases of the cloud computing SLA ····· 123
4.1.4 SLA status of domestic corporations ····· 127
4.1.5 SLA framework and service quality securing method in the cloud computing environment ····· 128
4.2 Methods of securing cloud computing interoperability ····· 136

4.2.1 Necessity of cloud computing interoperability ····· 136
4.2.2 Global trend to secure cloud computing interoperability ····· 139
4.2.3 Domestic trend to secure cloud computing interoperability ····· 146
4.2.4 Technical and policy alternatives to secure cloud computing interoperability ····· 147

5. Conclusion and implications ····· 153

표 목 차

〈표 1-1〉 미국 CIO가 꼽은 클라우드 컴퓨팅의 5가지 장점과 문제점 ····· 2
〈표 2-1〉 클라우드 컴퓨팅 서비스의 주요 특성 ····· 6
〈표 2-2〉 클라우드 컴퓨팅과의 타 컴퓨팅과의 비교 ····· 10
〈표 2-3〉 SaaS의 기술발전에 따른 시장전망 ····· 12
〈표 2-4〉 시장유형별 서비스유형과 주요 사업자 서비스 ····· 13
〈표 2-5〉 클라우드컴퓨팅 서비스 시장전망(십억불) ····· 15
〈표 2-6〉 클라우드 컴퓨팅 해외정부 동향 ····· 16
〈표 2-7〉 주요사업자의 클라우드 컴퓨팅 서비스 유형 ····· 17
〈표 2-8〉 국내 주요부처의 클라우드 컴퓨팅 추진현황 ····· 18
〈표 2-9〉 국내 주요 중소기업 클라우드 제공사 ····· 18
〈표 2-10〉 국내 사업자의 클라우드 컴퓨팅 사업현황 ····· 19
〈표 2-11〉 클라우드 컴퓨팅 서비스 유형별 확산전망 ····· 20
〈표 2-12〉 클라우드 컴퓨팅 서비스의 Pros & Cons, 발전의 조건 ····· 22
〈표 3-1〉 NCC사의 임치서비스 유형 ····· 33
〈표 3-2〉 정부 소프트웨어 조달정책 등에 기술자료 임치제도 반영현황 ····· 38
〈표 3-3〉 정보통신망 이용촉진 및 정보보호 등에 관한 법률 ····· 44
〈표 3-4〉 연관 인터넷 서비스의 장애 범위 ····· 45
〈표 3-5〉 클라우드 컴퓨팅 서비스 장애 사례 ····· 46
〈표 3-6〉 국내외 DDoS 공격 피해 사례 ····· 50
〈표 3-7〉 인터넷 서비스별 손해배상 관련 이용(서비스)약관 비교 ····· 53
〈표 3-8〉 아마존 S3 SLA Service Credit ····· 55
〈표 3-9〉 구글 Apps SLA Service Credit ····· 55
〈표 3-10〉 정통망법상의 서비스 중단 및 제한 범위 ····· 58
〈표 3-11〉 정통망법상의 약관의 신고 및 관련 사항 ····· 59
〈표 3-12〉 서비스 장애 발생에 따른 이용약관별 손해배상 범위 ····· 60
〈표 3-13〉 인터넷 서비스별 면책 범위 이용(서비스)약관 비교 ····· 61

〈표 3-14〉 서비스 장애 유형별 사용자 보호 대상 기준 ····· 63
〈표 3-15〉 약관의 규제에 관한 법률 중 이용자 보호를 위한 우선 고려 대상 ····· 66
〈표 3-16〉 ISO27001의 11개 분야 ····· 78
〈표 3-17〉 SAS 70 리포트 내용 ····· 79
〈표 3-18〉 PCI DSS의 보안항목 ····· 80
〈표 3-19〉 클라우드 컴퓨팅 서비스 관련 주요 법률 ····· 83
〈표 3-20〉 안전진단대상별 기준 항목수 ····· 84
〈표 3-21〉 안전진단 구분별 세부내용 ····· 85
〈표 3-22〉 문서화 요구사항 ····· 88
〈표 3-23〉 클라우드 컴퓨팅 서비스 환경 적용 시 주요 이슈 ····· 89
〈표 3-24〉 클라우드 컴퓨팅 서비스 제공자 대상 신설 사항 ····· 91
〈표 3-25〉 안전진단의 기술적 보호조치 및 클라우드 컴퓨팅 서비스 적용 시 미흡항목 ····· 92
〈표 3-26〉 안전진단의 물리적 보호조치 및 클라우드 컴퓨팅 서비스 제공자 적용 시 미흡항목 ····· 92
〈표 3-27〉 정보보호관리체계 인증 통제항목 및 클라우드 컴퓨팅 적용 시 미흡항목 ····· 94
〈표 3-28〉 클라우드 컴퓨팅 보안 관련 항목 추가 사항 ····· 97
〈표 3-29〉 기술적 보호조치의 항목 및 세부구분 수정 사항 ····· 99
〈표 3-30〉 클라우드 컴퓨팅 보안 인증제도 수립 방안 ····· 101
〈표 3-31〉 클라우드 컴퓨팅 서비스 제공자를 위한 정보보호대책 개선안(예시) ····· 101
〈표 3-32〉 클라우드 컴퓨팅 서비스 제공자를 위한 정보보호인증 항목(안) ····· 104
〈표 4-1〉 고객과 서비스 제공자의 정의 ····· 109
〈표 4-2〉 ISO/IEC20000의 목적 및 구성 ····· 111
〈표 4-3〉 ISO/IEC20000 중 SLA관련 주요 내용 ····· 112
〈표 4-4〉 ITIL의 구성 ····· 114

〈표 4-5〉 SLA와 관련된 ITIL의 내용 ····· 115
〈표 4-6〉 COBIT의 정의, 목표 및 구성 ····· 116
〈표 4-7〉 Delivery and support ····· 117
〈표 4-8〉 COBIT과 ITIL의 비교 ····· 118
〈표 4-9〉 ISO/IEC 9126의 모델 구성 ····· 119
〈표 4-10〉 Google app' SLA 개요 ····· 124
〈표 4-11〉 Amazon S3 SLA개요 ····· 125
〈표 4-12〉 Amazon S2 SLA개요 ····· 125
〈표 4-13〉 MS Azure 주요 서비스의 SLA개요 ····· 126
〈표 4-14〉 국내 주요 IDC및 초고속 인터넷 서비스 중 손해배상관련 내용 ····· 127
〈표 4-15〉 SLA 측정치의 기본 규칙 ····· 129
〈표 4-16〉 클라우드 컴퓨팅에서의 SLA Metrics (예시) ····· 130
〈표 4-17〉 클라우드 컴퓨팅 상호운용성 확보의 중요성 ····· 137
〈표 4-18〉 클라우드 컴퓨팅의 상호운용성 이슈 ····· 138
〈표 4-19〉 클라우드 컴퓨팅 상호운용성을 위한 글로벌 표준화 활동현황 ····· 139
〈표 4-20〉 OCC(Open Cloud Consortium〉 표준화 활동현황 ····· 141
〈표 4-21〉 Open Cloud Manifesto 표준화 활동현황 ····· 142
〈표 4-22〉 OGF (Open Grid Forum) 표준화 활동현황 ····· 143
〈표 4-23〉 CSA (Cloud Security Alliance) 표준화 활동현황 ····· 145
〈표 4-24〉 클라우드 컴퓨팅 상호운용성 확보를 위한 표준화 대상 기술 ····· 148
〈표 5-1〉 클라우드컴퓨팅 활성화를 위한 법·제도 개선방안 요약 ····· 154

그 림 목 차

〈그림 2-1〉 클라우드 컴퓨팅을 위한 가상화 아키텍처 ····· 8
〈그림 2-2〉 클라우드 컴퓨팅 유형 ····· 11
〈그림 2-3〉 서비스 유형에 의한 클라우드 컴퓨팅 서비스 시장규모 ····· 15
〈그림 3-1〉 MS 사이드킥 서비스 제공체계 ····· 28
〈그림 3-2〉 Iron-Mountain사의 임치물 교부에 따른 백업 시스템 ····· 31
〈그림 3-3〉 Iron Mountain사의 SaaS Escrow ····· 32
〈그림 3-4〉 Clio 사의 데이터 임치 ····· 33
〈그림 3-5〉 임치제도 이용 절차도 ····· 38
〈그림 3-6〉 Google Apps Status Dashboard ····· 47
〈그림 3-7〉 Amazon S3 활용 예시도 ····· 48
〈그림 3-8〉 Amazon S3 Service Level Agreement ····· 55
〈그림 3-9〉 전자금융서비스 보안프로그램 구동 화면 ····· 65
〈그림 3-10〉 KT 인터넷 속도 테스트 화면 ····· 68
〈그림 3-11〉 클라우드 컴퓨팅 활성화에 따른 이슈 ····· 71
〈그림 3-12〉 ISO 27001인증 체계 ····· 77
〈그림 3-13〉 ISO 27001 인증 절차 ····· 77
〈그림 3-14〉 현행 정보보안 법률체계 ····· 82
〈그림 3-15〉 클라우드 컴퓨팅 서비스 시행 시 관련 주요 법률 ····· 82
〈그림 3-16〉 정보보호관리체계 ····· 87
〈그림 3-17〉 정보보호 관리과정 요구사항 ····· 87
〈그림 3-18〉 정보보호 대책 요구사항 ····· 88
〈그림 4-1〉 서비스레벨관리(SLM) 프로세스 ····· 109
〈그림 4-2〉 ISO/IEC 9126 국제표준 품질모델 ····· 119
〈그림 4-3〉 ISO/IEC 9126 소프트웨어 품질모델의 구조 ····· 120
〈그림 4-4〉 클라우드 컴퓨팅 서비스품질 중 확장성 안정 범위 ····· 122
〈그림 4-5〉 웹서비스 관리 표준 (WSDM) ····· 131

〈그림 4-6〉 오류자동 교정기법 개요 ····· 134
〈그림 4-7〉 다양한 클라우드 컴퓨팅 서비스들로 이루어진 그리드 ····· 138
〈그림 4-8〉 클라우드컴퓨팅포럼 조직도 ····· 146

제1장 서론

제 1 절 연구 배경 및 목적

제 2 절 연구 방법 및 구성 내용

제 1 절 연구 배경 및 목적

클라우드 컴퓨팅은 개개인이 사용하려는 컴퓨팅 자원을 자신의 인프라를 구축하지 않고서도 제3의 인프라를 이용하여 구름(Cloud)을 형성한 듯 마치 자신의 컴퓨터처럼 자유롭게 사용하고 그에 따른 비용을 지불하는 서비스 형태의 분산 컴퓨팅 환경이라고 할 수 있다. 사용자는 자신이 시스템을 구축하지 않고서도 필요한 만큼의 시스템 기능을 자유롭게 이용할 수 있으며, 클라우드 컴퓨팅 제공자는 서버클러스터 등 집적된 IT자원과 고도화된 가상화 기술을 활용하여 고효율의 서비스를 제공할 수 있는 장점이 있다.

그러나 사용자의 데이터가 클라우드서비스 제공자의 서버에 저장되고 관리되는 특성으로 인해 갑작스런 서비스 중단이나 장애에 대한 사용자의 우려가 크고, 데이터 외부보관에 따른 기밀 유출, 클라우드 시스템 간 호환성 부족으로 인한 종속성에 대한 우려가 존재한다. 특히 사용자가 기업인 경우 갑작스런 서비스 장애, 서비스 제공자의 파산으로 인한 비즈니스 패해가 광범위할 수 있다.

이러한 사용자들의 우려는 단순한 우려가 아닌 실제 상황으로도 종종 발생하고 있다. 구글이나 아마존과 같은 글로벌 기업들의 클라우드 컴퓨팅 서비스가 갑작스런 사고로 중단되는 사고가 발생하고 있으며, 갑작스런 폐업으로 인한 데이터 소유권 분쟁 사례도 실제 보고되고 있다. 이러한 사용자들의 우려는 클라우드 컴퓨팅 확산의 중요한 장애요인으로 작용한다. 미국 시장조사 기관인 IDC가 244명의 IT부서 임원 및 CIO를 대상으로 클라우드 컴퓨팅에 대한 설문을 실시한 결과, 데이터 손실 및 정보유출, 서비스품질의 우려 등으로 인해 도입을 꺼리고 있는 것으로 나타나 이 같은 사실을 뒷받침한다.

〈표 1-1〉 미국 CIO가 꼽은 클라우드 컴퓨팅의 5가지 장점과 문제점

장점		문제점	
배치용이	64%	시큐리티	75%
사용한 만큼만 지불	62%	성능	63%
사내 담당인력 감축	58%	유용성	63%
낮은 월 사용료	53%	통합의 어려움	61%
기능	50%	맞춤형 서비스 어려움	56%

그러나 이러한 사용자의 우려를 불식시킬 수 있는 법. 제도적인 인프라는 매우 부족한 상황이다. 국내의 현행 법.제도체계는 데이터센터를 보유하고 운영하는 사업자나 인터넷 서비스 제공사업자 등 일부 사업자들을 대상으로 법적인 의무와 책임을 명시하고 있을 뿐, 클라우드 컴퓨팅에 대한 정의나 시장구분, 사업자 유형도 명확하게 구분하지 못하고 있어 사용자의 서비스 품질에 대한 우려나 보안, 데이터 유실, 상호운용성 부재에 따른 종속성 우려와 같은 문제들에 효과적으로 대처하지 못하고 있다.

이에 현재 초기시장을 지나고 있는 클라우드 컴퓨팅의 본격적인 확산을 위해서는 이 같은 사용자의 우려를 분식시킬 수 있는 제도적인 보완이 필요하다. 이에 본고에서는 현재 제기되고 있는 주요 이슈들에 대한 사용자 보호방안과 법. 제도적인 개선방안을 살펴보고자 한다.

제 2 절 연구 방법 및 구성 내용

연구의 범위는 다음과 같다. 우선 2장에서는 클라우드 컴퓨팅의 정의와 시장유형, 클라우드 컴퓨팅 시장전망과 국내·외 사업자 동향, 국내시장에서의 성장가능성과 국내기업들의 경쟁가능성, 주요한 장애요인과 법·제도적인 이슈 등을 살펴본다.

3장에서는 크게 세 가지 영역에 대한 사용자의 보호방안에 대한 법·제도적인 개선사항을 제시한다. 첫 번째는 서비스제공자의 파산 등으로 인한 서비스 중단에 따른 사용자 보호방안과 법·제도적인 개선방안을 제시한다. 두 번째는 서비스제공자의 일시적 서비스장애에 따른 사용자 보호방안을 제시한다. 세 번째는 사용자의 보안우려에 대한 법·제도적인 대응방안을 제시한다. 이를 위해 국내외의 서비스 중단 및 장애, 보안침해 사례 등을 살펴보고, 해외 정부 및 사업자의 서비스 중단 및 보안침해 방지를 위하 제도적 대응방안을 살펴본다. 마지막으로 국내시장에서 사용자 보호를 위한 법. 제도 현황을 살펴보고, 이에 대한 개선방안을 탐색한다.

4장에서는 3장에서 지적된 문제점의 해결방안으로 서비스 품질 확보를 위한 SLA (Service Level Agreement) 가이드라인 제정방안과 클라우드 간 상호운용성 확보를 위한 기술적·제도적 개선방안을 모색한다. 이를 위해 IT서비스 아웃소싱에서 활용되고 있는 SLA의 국제적인 기준 및 해외사업자의 SLA현황 등을 살펴보고, 국내 사업자의 SLA수준 등을 비교 분석함으로써 SLA가이드라인 마련을 위한 시사점을 제시한다. 또한 클라우드 간 상호

운용성 확보를 위한 상호운용성 추진현황 및 문제점을 살펴보고, 상호운용성 확보를 위한 기술적, 법, 제도적인 보완방안을 제시한다.

마지막으로 5장에서는 3장, 4장에서 다루어진 주요 이슈들을 정리하고, 클라우드 컴퓨팅 시장 활성화를 위한 법. 제도적인 시사점을 제시한다.

제2장 클라우드 컴퓨팅 현황 및 문제점

제 1 절 클라우드 컴퓨팅 정의 및 유형

제 2 절 클라우드 컴퓨팅 시장동향

제 3 절 국내 클라우드 컴퓨팅 시장 장애요인

제 1 절 클라우드 컴퓨팅 정의 및 유형

1. 클라우드 컴퓨팅의 정의

컴퓨팅이 전기나 수도와 같이 유틸리티처럼 사용될 것이라는 개념은 이미 인터넷의 효시인 ARPANET[1]프로젝트가 시작되었을 때부터 전문가들에 의해 예견되었다. 그리고 40년이 지난 지금, 이들이 예상했던 컴퓨팅이 유틸리티로 제공되는 시대가 '클라우드 컴퓨팅'을 통해 실제 도래하고 있다.

클라우드 컴퓨팅에 대한 정의는 다양하게 이루어지고 있다. 리서치회사인 가트너는 '인터넷 기술을 활용하여 다수의 고객들에게 높은 수준의 확장성을 가진 IT자원들을 '서비스로 제공하는 컴퓨팅'[2]으로 설명한다. 또한 포레스터 리서치는 공통적인 특징으로 '표준화된 IT기반 기능'들이 IP(인터넷 프로토콜)을 통해 제공되며, 언제나 접근이 허용되고, 수요의 변화에 따라 가변적이며, 사용량이나 광고에 기반을 둔 과금모형을 제공하며, 웹 혹은 프로그램적인 (Control)인터페이스 제공'를 제시한다.[3]

〈표 2-1〉 클라우드 컴퓨팅 서비스의 주요 특성

주요 특징	세부 내용
표준화된 IT기반 기능	o 컴퓨팅, 저장장치, 네트워크, SW등을 포함하는 전반적인 IT 자원 o 제공되는 서비스 이외에 별도의 고객화(Customization)가 없으며, 서비스 제공자에 의해 제공되는 표준
IP망을 통한 접근	o IP망과 Http, REST[4], SOAP[5]등 웹기반 컴퓨팅 프로토콜 활용 o UI를 위해 OS에 중립적인 표준 웹 브라우저와 웹 표준 지원

1) Advanced Research Projects Agency Network
2) "a style of computing in which massively scalable IT-enabled capabilities are delivered 'as a service' to multiple customers using internet technologies" by Gartner(2007)
3) 'A forms of standardized IT-based capability-such as Internet-based services, software, or IT infrastructure-offered by a service provider that is accessible via Internet protocols from any computer, is always available and scales automatically to adjust to demand, is either pay-per-use or advertising-based, has Web-or programmatic-based control interfaces, and enables full customer self-service' by Forrester Research(2008)
4) Representational State Transfer
5) Simple Object Access Protocol

〈표 2-1〉 클라우드 컴퓨팅 서비스의 주요 특성(계속)

주요 특징	세부 내용
Always on과 수요에 따른 확장성 지원	o 서비스 제공자는 24시간 접근성과 고객수요의 변화에 따라 이에 대응하는 컴퓨팅 자원을 가변성 있게 지원
사용량이나 광고기반 과금	o 무료, 혹은 사용기반 과금으로 장기계약이나, 초기 셋업비용 등이 없음 (광고, 주/원단위 과금, 사용량기반 과금)
Web 혹은 Programmatic 기반 Control Interface	o 고객데이터 원격 호스트, RIA[6] 인터페이스(페이스북, MS virtual earth 3D 등) 제공 o 서버기반 인터페이스로 XML과 REST 스타일 SW Connection Standard (Flicker API, Amazon S3) 사용
사용자 셀프서비스	o 서비스제공자의 간섭 없이 고객 스스로 필요한 서비스를 설치, 관리, 종결 o 사용자는 Web-Interface나 Programmatic call을 통해 서비스 API에 접근

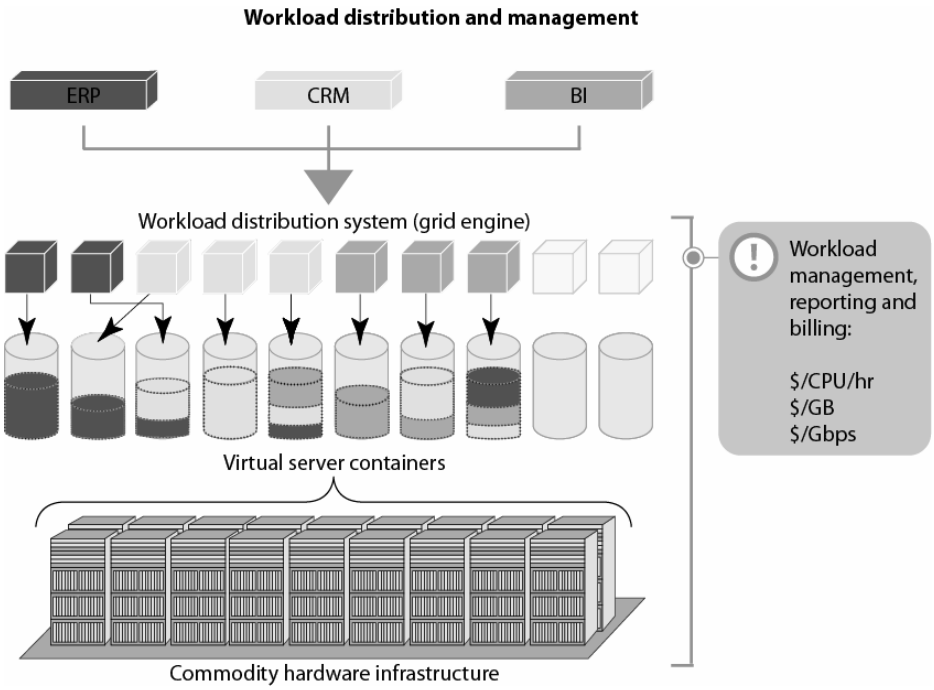
출처 : 포레스터 리서치(2008)[7]

이 같은 설명을 종합하면, 클라우드 컴퓨팅은 '인터넷을 통한 IT자원의 온디맨드 아웃소싱 서비스'로 볼 수 있다. 클라우드 컴퓨팅 환경에서 사용자들은 애플리케이션, 스토리지, OS, 보안 등 필요한 IT자원을 원하는 시점에 원하는 만큼 골라서 사용하게 되며, 사용량에 기반을 두어 대가를 지불한다. 이를 위해 서비스 제공자들은 여러 곳에 분산되어 있는 데이터센터를 가상화 기술로 통합하여 고객들이 필요로 하는 서비스를 제공한다.

클라우드 환경에서 서비스 제공자는 제한된 물리적인 인프라를 활용하여 다수의 사용자들이 자신만을 위한 IT인프라가 구축되어 있는 것과 같은 환경을 제공한다. 서비스 제공자는 이를 위해 여러 곳에 분산되어 있는 물리적 인프라를 가상화하여 가상의 자원풀(Resource Pool)을 구축하고 사용자의 작업요구수준(Workload)에 따라 이러한 자원들을 효율적으로 배분하여 사용한다. 따라서 서비스 제공자는 사용자의 수많은 서비스 요청에 대하여 실시간적으로 자원을 배분하고, 이를 어떻게 효율적으로 운영하느냐가 핵심역량이라고 할 수 있다. 이에 따라 자원의 효율적인 활용을 위해 일정수준 이상의 규모의 경제(Economy of Scale)를 달성하는 일이 경쟁력의 중요한 요소가 된다.

6) Rich Internet
7) 'Is Cloud Computing Ready For The Enterprise?', Forester Research (2008)

〈그림 2-1〉 클라우드 컴퓨팅을 위한 가상화 아키텍처



출처 : 포레스터리서처(2008)[8]

사용자들은 서비스 제공자가 제공하는 서비스 카탈로그를 통해 원하는 서비스를 요청하고, 서비스 제공자의 시스템관리 모듈은 이 같은 요청에 대하여 가상화된 서버 네트워크를 통해 필요한 리소스를 조달하게 된다. 따라서 사용자들은 서비스를 이용만 할 뿐 어떻게 서비스가 제공되고, 자신의 데이터와 정보가 어디에 보관되는지, 어느 곳에 위치한 서버가 활용되는지 등 세부적인 정보는 알지 못한다. 이 때문에 클라우드 컴퓨팅을 통해 유통되는 데이터 관리의 문제가 중요한 사용자와 서비스 제공자 간의 중요한 이슈로 떠오르고 있다.

2. 클라우드 컴퓨팅과 타 컴퓨팅 용어와의 차이점

인터넷을 컴퓨팅의 핵심 인프라로 활용하고자 하는 시도들은 이미 이전부터 있어왔다. 그리드 컴퓨팅, 서버기반 컴퓨팅(Server Based Computing), 유틸리티 컴퓨팅(Utility

8) 'Is Cloud Computing Ready For The Enterprise?', Forrester Research (2008)

Computing), SaaS 등이 그러하다. 그렇다면 클라우드 컴퓨팅은 이전에 나타났던 컴퓨팅과는 무엇이 다른가?

사실 이러한 컴퓨팅 용어의 차이들은 바라보는 사소한 관점의 차이일 뿐 다른 기술이나 새로운 개념의 등장은 아니다. 그럼에도 불구하고 이러한 차이는 많은 사용자들에게 적지 않은 개념의 혼돈을 야기해 왔다.

우선 클라우드 컴퓨팅과 그리드 컴퓨팅, 그리고 유틸리티 컴퓨팅과의 관계를 살펴보자. 그리드 컴퓨팅은 대용량의 컴퓨팅 리스소를 필요로 하는 문제해결을 위해 인터넷 상에 분산된 컴퓨팅 리소스들을 연결하여 가상의 슈퍼컴퓨터와 같이 사용하는 컴퓨팅 모델로 주로 과학, 수학 등 학술적인 분야에서 활용된다. 클라우드 컴퓨팅은 분산된 IT자원을 통합하여 사용한다는 차원에서 그리드 컴퓨팅의 분산 컴퓨팅 환경과 유사하다. 그러나 그리드 컴퓨팅은 인터넷을 통해 서버와 PC등 유휴의 컴퓨팅 자원을 활용한다는 개념인데 비해, 클라우드 컴퓨팅은 개별적인 서비스 사업자의 가상화된 서버 네트워크를 이용한다는 차원에서 차이가 난다. 즉, 그리드(Grid)가 인터넷상의 모든 컴퓨팅 리소스를 연결하는 그물망을 의미한다면, 클라우드(Cloud)는 사업주체인 서비스 제공자가 제공하는 사유화된 컴퓨팅 (서버) 네트워크를 의미한다고 볼 수 있다.

유틸리티 컴퓨팅은 사용자가 컴퓨팅 자원을 전기나 수도와 같은 유틸리티와 같이 필요할 때마다 연결하여 사용하고 사용량에 따라 대가를 지급하는 과금모형으로 볼 수 있다. 클라우드 컴퓨팅은 인터넷 상의 분산 시스템을 활용하여 컴퓨팅 자원을 서비스로 이용하고, 사용량에 기반 하여 대가를 지불한다. 따라서 기술적으로는 그리드의 분산 컴퓨팅을, 과금모형으로는 유틸리티 컴퓨팅을 채택하는 컴퓨팅 개념으로 볼 수 있다.

그렇다면 서버기반 컴퓨팅과 네트워크 컴퓨팅과는 어떤 차이가 있을까? 서버기반 컴퓨팅은 서버에 애플리케이션과 데이터를 두고 필요할 때마다 접속해서 사용하는 방식이다. 따라서 모든 처리가 100% 서버에서 이루어지고, 클라이언트는 단순히 입출력만을 처리하는 씬클라이언트의 역할을 담당한다. 클라우드 컴퓨팅이 저사양의 단말기를 통해서도 서버에서 처리되어 제공되는 높은 수준의 서비스를 이용할 수 있다는 차원에서 서버기반 컴퓨팅이 가지는 특성을 포함하고 있다.

그러나 서버기반 컴퓨팅은 사용자를 위한 물리적인 서버가 제공하고 이에 대한 활용의 권한도 사용자가 가지고 있는데 비해, 클라우드 컴퓨팅에서 사용자는 가상화된 서버네트워크를 통해 서비스를 이용할 뿐 물리적인 서버에 대한 정보나 권한을 가지지 못한다. 따라서 서버기반 컴퓨팅에서 사용자가 추가적인 컴퓨팅 용량이 필요할 경우 물리적인 서버를

추가하게 되지만, 클라우드 컴퓨팅에서 사용자는 단지 원하는 서비스를 선택하여 사용만 할 뿐 물리적인 서버의 증설에 관여하지 않는다. 다만, 서버기반 컴퓨팅도 웹의 발전과 함께 클라우드 컴퓨팅의 환경을 수용하며 발전해가고 있어 점차 그 구분점이 모호해지고 있다.

〈표 2-2〉 클라우드 컴퓨팅과의 타 컴퓨팅과의 비교

	주요 개념	클라우드 컴퓨팅과의 관계
Grid Computing	높은 컴퓨팅 리소스를 필요로 하는 작업의 수행을 위해 인터넷 상의 분산된 다양한 시스템과 자원들을 공유하여 가상의 슈퍼컴퓨터와 같이 활용하는 방식 (분산 컴퓨팅 아키텍처)	Grid방식의 분산 컴퓨팅과 Utility 개념의 과금모형을 혼합한 컴퓨팅 방식
Utility Computing	컴퓨팅 리소스를 구매하거나 소유하지 않고, 가스, 전기등과 같이 유틸리티로 필요할 때마다 사용하는 방식(사용량 기반 과금모형)	
Server Based Computing	서버에 애플리케이션과 데이터를 두고 필요할 때마다 접속해서 사용하는 방식 (클라이언트는 입. 출만 처리. 모든 작업은 100% 서버가 처리-Thin Client 방식)	클라우드 컴퓨팅은 가상화된 분산 컴퓨팅에, SBC는 특정 기업의 서버에 중심 중심을 둔다는 차원에서 개념적으로 구분. 그러나 SBC가 발전으로 점차 구분이 모호해 짐
Network Computing	SBC와 비슷하나, 애플리케이션을 서버에서 로드하여 로컬에서 수행하는 형태 (이용자의 CPU를 사용하여 동작)	이용자의 컴퓨팅 리소스보다는 클라우드 상의 IT 리소스를 사용하므로 개념적 구분
SaaS	서비스 제공자의 서버에 저장된 SW를 인터넷을 통해 서비스로 이용하는 SW 딜리버리 모형	클라우드 컴퓨팅은 모든 IT자원을 서비스로 활용한다는 차원에서 보다 SaaS를 포함하는 포괄적인 개념

출처 : 정제호(2008)

네트워크 컴퓨팅은 서버에 애플리케이션을 저장하여 사용한다는 점에서는 서버기반 컴퓨팅과 유사하나, 애플리케이션을 서버로부터 로드하여 로컬에서 실행하기 때문에 자신의 컴퓨팅 자원을 상당부분 사용하게 된다는 점에서 차이가 난다[9]. 클라우드 컴퓨팅은 클라우드 상에서 IT자원을 서비스로 이용한다는 차원에서 네트워크 컴퓨팅과는 개념적인 구분이 가능하다.

그렇다면, SW를 서비스로 사용하는 SaaS(Software as a Service)와는 어떻게 다른가?

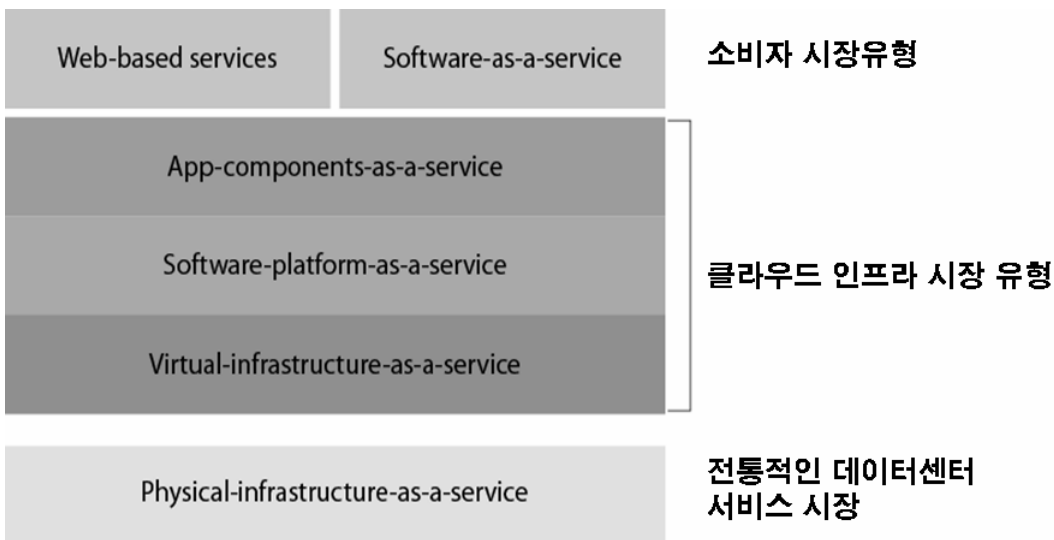
9) 류한석(2007.05), "Server Based Computing", SW인사이트 정책리포트,

클라우드 컴퓨팅은 SaaS를 가능하게 하는 기반 컴퓨팅환경이자, SaaS를 포함하는 광범위한 IT자원에 대한 아웃소싱 모형이다. 즉, SaaS와 클라우드 컴퓨팅은 아웃소싱 모델로써의 공통점을 공유하지만, SaaS는 SW를 중심으로, 클라우드 컴퓨팅은 SW는 물론 보다 폭넓은 IT자원을 포괄적으로 아웃소싱 한다는 차원에서 개념적인 차이가 존재한다.

3. 클라우드 컴퓨팅의 유형

클라우드 컴퓨팅 서비스는 서비스 이용자의 유형에 따라 두 가지로 구분가능하다. 첫 번째는 소비자 시장이며, 두 번째는 IT구매자 시장이다. 최종 소비자 시장은 클라우드 컴퓨팅 서비스를 최종 소비하는 집단이며, IT구매자 시장은 클라우드 컴퓨팅 서비스를 활용하여 인터넷기반 비즈니스를 수행하는 기업들이다.

〈그림 2-2〉 클라우드 컴퓨팅 유형



출처 : 포레스터 리서치(2008)[10]

1) 소비자 시장 : 개인소비자(Web-based Service)와 기업소비자(SaaS)

소비자 시장은 크게 개인 소비자와 기업 소비자 시장으로 구분된다. 개인 소비자 시장은

10) 'Is Cloud Computing Ready For The Enterprise?', Forrester Research (2008)

블로그와 위키, 소셜네트워킹 서비스 등과 같이 웹기반 서비스 시장으로 광고기반 수익에 기반을 두는 시장이다. 구글이나 MS, 야후 등의 많은 클라우드 컴퓨팅 서비스 제공자들은 소비자 시장을 중심으로 성장하고 있으며, 이를 기반으로 기업용 SaaS 시장으로 영역을 확장하고 있다[11].

두 번째는 기업 소비자 시장이다. 이 시장은 기업의 IT환경을 클라우드 환경으로 전환하고자 하는 기업들의 수요로 가입자 과금모형에 기반을 둔 기업용 SaaS시장으로 볼 수 있다. 클라우드 컴퓨팅이 초기 도입단계를 넘어 본격적인 성장단계로 진입하기 위해서는 기업시장이 중요한 역할을 한다.

SaaS는 높은 유지보수 비용과 복잡하고 경직된 시스템과 과금체계 등 기존의 라이센싱 모델을 대체하며, 재무적 유연성을 제공함에 따라 빠른 성장이 기대된다. 그러나 아직까지 기술적인 한계와 기업 인프라의 미비로 인해 아직 1세대와 2세대를 중심으로 특정 분야의 기능성을 제공하는 서비스들이 대부분을 차지하고 있다. 그러나 점차 기업프로세스가 표준화되고 SOA 등 기업 IT인프라에 유연성이 확보되면서 점차 기업의 주요 IT인프라 영역을 담당하는 3세대 외 4세대 서비스로까지 확장되고 있는 추세이다.

〈표 2-3〉 SaaS의 기술발전에 따른 시장전망

	제 1세대	제 2세대	Challenge Gap	제 3세대	제 4세대
지원 수준	기본적인 업무 프로세스지원	데이터 관리를 포함하는 기능적 효율성 지원	o SOA 도입	기업내부 프로세스 통합지원	Business Ecosystem 지원
특성	단순 기능성을 제공하는 ASP	기본적인 커스토마이징 및 데이터 통합지원	o 기업프로세스 표준화	고객 및 자원, 회사데이터 통합	부서간/파트너와의 협업프로세스 지원
도입 분야	세금, 회계 관리 등 특수영역의 보편화된 서비스	CRM, 영업 등 고객서비스 제공분야	o 기존시스템과의 통합을 위한 중계표준	고객/자원/데이터 등 통합솔루션을 개별 서비스관점에서 제공	복잡한 자원 접근 권한 관리 지원

출처 : 가트너 (2006) 수정

11) 구글이나 MS는 SOHO를 대상으로 하는 SaaS시장 진출을 위해 'Apps For your Domain'이나 'Office Live'와 같은 SaaS서비스를 앞세워 광고와 가입자기반 과금모형을 혼합한 새로운 비즈니스 모델을 가지고 시장에 진출한 바 있음

2) IT구매자 시장

애플리케이션 컴포넌트 서비스, 플랫폼 서비스, IT인프라 서비스 IT구매 시장은 클라우드 인프라를 활용하여 서비스를 재생산함으로써 웹을 기반으로 하는 비즈니스를 수행하고자 하는 사업자 수요이다. 개발자들이 접근할 수 있는 자원의 수준에 따라 어플리케이션 컴포넌트 서비스시장, SW 플랫폼 서비스 시장, 가상인프라 서비스 시장으로 나눌 수 있다. 애플리케이션 컴포넌트 서비스는 개발자들을 위해 다양한 애플리케이션 모듈들을 제공하는 서비스로 구글의 캘린더 API나 세일즈포스닷컴의 AppExchange API등이 있다. 개발자들은 새로운 애플리케이션 개발을 위해 처음부터 개발을 하지 않고, 서비스 제공자가 제공하는 API를 통해 신속하게 애플리케이션을 개발할 수 있다.

〈표 2-4〉 시장유형별 서비스유형과 주요 사업자 서비스

시장 유형		제공서비스 사례	주요 사업자 서비스
소비자 시장	웹기반 서비스	o 인터넷 기반 서비스 (Blog, Wiki, Social Service)	o 구글 o Mysapce.com
	SW 서비스 (SaaS)	o Office 생산성 애플리케이션 o 협업 솔루션 o 기타 클라이언트 애플리케이션	o 구글 Apps for your Domain o MS Office Live o IBM Bluehouse
IT구매자 시장	애플리케이션 컴포넌트 서비스	o 서비스나 애플리케이션 개발을 위한 API와 웹기반 SW모듈 (애플리케이션 레이어 수준)	o 아마존 flexible payment API o 구글 Calendar API o 세일즈포스닷컴 AppExchange API
	SW 플랫폼 서비스 (PaaS)	o 신규 어플리케이션 개발을 위한 개발 플랫폼 (미들웨어 레이어 수준) - Hosted App Platform Server, Hosted DB - Hosted Data 관리, Massage Queue 등	o 아마존 SimpleDB, Simple Storage Service(S3), Simple Queue Service o 구글 App Engine o MS SQL Server Data Service o 세일즈포스닷컴 Force.com
	가상인프라 서비스 (IaaS)	o 가상서버, 가상Storage, 가상네트워크 o 시스템 관리	o 아마존 Elastic Compute Cloud(EC2)

출처: 포레스터 리서치 수정(2008)[12]

SW 플랫폼 서비스는 어플리케이션 단의 API 제공수준을 넘어 미들웨어 까지 포괄적인 개발 플랫폼을 제공하는 서비스로, 세일즈포스닷컴의 Force.com[13]서비스가 대표적이다. 애플리케이션 개발 벤더들은 서비스 제공사업자가 제공하는 플랫폼 상에서 DB와 애플리케이션 서버, 파일관리 시스템과 관련한 솔루션 등 미들웨어까지 확장된 IT자원을 활용하여 새로운 애플리케이션을 만들어 사용할 수 있다.

마지막으로 가상인프라 서비스는 개발자들과 IT기업들이 필요로 하는 가상의 IT인프라 자원을 포괄적으로 제공하는 서비스로 대표적으로는 아마존의 E2C서비스가 있다. 사용자들은 가상서버와 저장장치, 가상네트워크, 시스템관리 등 모든 가상의 자원들을 사용할 수 있고, 초기 인프라 구축비용 없이도 자신들의 비즈니스 모형을 구축하고, 웹을 통해 서비스를 제공할 수 있다.

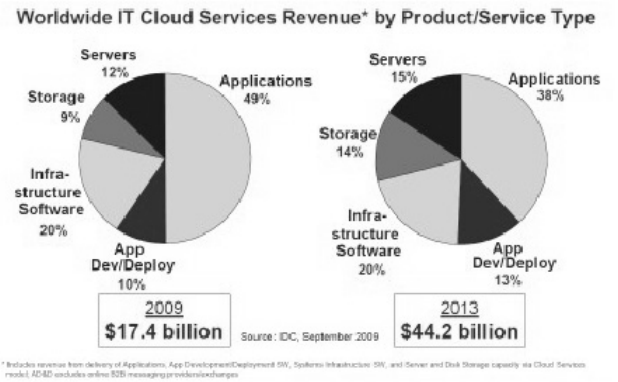
제 2 절 클라우드 컴퓨팅 시장동향

1. 클라우드 컴퓨팅 시장전망

망의 고도화와 가상화 기술발전, 경제위기에 따른 IT비용절감 압력, 그린IT화와 맞물려 클라우드 컴퓨팅 시장이 빠르게 성장하고 있다. 클라우드 컴퓨팅은 조만간 IT산업의 중추적 역할을 수행할 것으로 전망되고 있다. IDC는 향후 5년간 클라우드 컴퓨팅 서비스에 대한 지출이 급증하여 2009년 174억 달러의 시장이 2013년에는 442억 달러에 이를 것으로 전망하고 있으며, IT시장에서 차지하는 비율도 2008년 9%에서 2012년 25%로 상승할 것으로 예측하고 있다.

12) 'Is Cloud Computing Ready For The Enterprise?', Forrester Research (2008)
13) 과거 APEX 플랫폼에서 Force.com으로 명칭 변경

〈그림 2-3〉 서비스 유형에 의한 클라우드 컴퓨팅 서비스 시장규모



[출처] IDC's New IT Cloud Services Forecast: 2009-2013

비즈니스 프로세스 아웃소싱을 클라우드 컴퓨팅에 포함시키고 있는 가트너는 클라우드 컴퓨팅 시장이 2008년 464억 달러에서 2013년 1500억 달러로 확대될 것으로 전망한다. 클라우드 컴퓨팅 시장 획정에 따른 두 기관의 전망치는 차이가 나고 있지만 시장성장률(CAGR)은 26~27%수준으로 비슷하게 나타나고 있다. 특히 가트너의 전망에 따르면 2013년 전체 클라우드 컴퓨팅 시장의 70% 이상을 비즈니스 프로세스 서비스가 차지하는 것으로 나타나고 있다. 이는 IaaS나 PaaS와 같은 인프라 성 서비스들을 활용하여 다양한 솔루션에 기반을 둔 비즈니스 프로세스 아웃소싱 서비스를 이용하는 기업들이 크게 증가하게 될 것임을 보여주는 전망치이다.

〈표 2-5〉 클라우드컴퓨팅 서비스 시장전망(십억불)

	2008년	2009년	2010년	2011년	2012년	2013년	CAGR (%)
Business Process Services	38.9	46.6	57	71.4	91.5	119.3	25.1
Applications	5.04	6.52	9.6	11.4	14.6	20.2	32
Application Infrastructure	1.52	1.61	1.71	1.83	1.98	2.26	8.3
System Infrastructure	0.96	1.56	2.53	4.19	6.1	8.37	53.8
Total	46.4	56.3	70.8	88.8	114.2	150.1	26.5

출처 : 가트너 (2009)[14]

2. 해외 시장 동향

클라우드 컴퓨팅은 다가올 미래가 아닌 이미 현재 진행형이다. 이미 세계 각국은 정부 주도하에 클라우드 컴퓨팅의 도입을 추진 중이다.

〈표 2-6〉 클라우드 컴퓨팅 해외정부 동향

국가	주요 내용
미국	o 국방부(DISA)는 '08년 말 데이터센터의 운영비용 절감 및 인프라 활용률 제고를 위해 가상 서버기반의 클라우드 컴퓨팅 센터 구축
	o 연방총무성(GSA)은 내년까지 행정부 통합 전산지원을 위한 클라우드 프레임워크를 통해 클라우드 컴퓨팅 체계 수축 예정
일본	o '09년 3월, 디지털 일본 창조 프로젝트의 일환으로 '15년까지 전정자정부 지원을 위한 중앙부처 클라우드 컴퓨팅 도입 계획 '가스미가세키 클라우드' 계획 발표
영국	o '09년 6월 공공부문 데이터센터 혁신전략의 일환으로 정부에서 사용하는 전산자원을 클라우드 컴퓨팅 기반으로 제공하는 계획 발표 ('12년 완료 예정)
중국	o 중앙정부차원의 구체적인 발표는 없으나, 우시(Wixi)지역의 경제개발프로젝트 일환으로 추진 중인 SW파크 건립 시 입주자 대상 클라우드 컴퓨팅 센터를 구축하여 IaaS, PaaS서비스 제공

출처 : 전자신문(2009)[15]

그동안 전자상거래나 검색, IT서비스 분야에 종사하던 아마존, 구글, IBM, MS등의 기업들도 클라우드 컴퓨팅 시장으로 발 빠르게 움직이고 있다. 구글은 웹기반 서비스시장에서 SW서비스 시장과 IT인프라 시장으로 확장가고 있다. 아마존은 대표적인 클라우드 컴퓨팅 사업자로서 시장을 주도하면서 애플리케이션 컴포넌트와 플랫폼, 나아가 가상인프라에 이르기까지 가장 광범위한 클라우드 컴퓨팅 서비스를 제공하고 있다. 구글이나 아마존과 같은 클라우드 컴퓨팅 서비스 사업자들의 전략은 점차 소비자 시장을 넘어 클라우드 인프라 시장까지 통합적인 클라우드 컴퓨팅 서비스의 제공을 목표로 한다. 특히 개발환경으로써의 플랫폼을 서비스로 제공함으로써 제3의 개발자들의 참여를 통해 다양한 애플리케이션들과 서비스들을 거래되는 거래시장(Market Place)구축을 새로운 비즈니스 모델로 활용하고자

14) Gartner, 2009.03 - Forecast: Sizing the Cloud; Understanding the Opportunities in Cloud Services

15) 전자신문, 2009년 12월 6일 '클라우드 컴퓨팅 해외도입현황'

하는 모습이 나타나고 있다[16]. 또한 MS는 개발환경과 SW거래시장을 제공하는 PaaS서비스로 Azure의 베타버전을 테스트 중이며, IBM은 Blue클라우드 전략을 통해 자사의 데이터센터를 유틸리티로 제공하고자 하는 IaaS서비스를 제공 중이다.

〈표 2-7〉 주요사업자의 클라우드 컴퓨팅 서비스 유형

주요사업자	주요 서비스	서비스 개요
아마존	EC2	o 사용자들에게 가상의 서버를 제공하는 IaaS 서비스
구글	AppEngine	o 제3의 개발자가 구글 서버자원을 활용, App 개발을 지원하는 PaaS서비스
세일즈포스닷컴	Force.com	o 개발환경과 마켓플레이스를 제공하는 PaaS 서비스
MS	Azure	o 개발환경과 AppStore 제공하는 PaaS 서비스
IBM	Blue 클라우드	o 자사의 데이터 센터를 유틸리티로 제공하는 IaaS서비스

3. 국내 시장동향 및 전망

국내 클라우드 컴퓨팅 시장도 매우 역동적으로 변하고 있다. 정부 차원에서도 범부처적인 협력을 통해 클라우드 컴퓨팅 시장 활성화를 위한 대응전략을 서두르고 있며, 특히 미국이나 일본 등과 같이 정부통합전산센터에서 클라우드 인프라 구축을 준비 중이며, 다양한 분야에서의 시범사업도 준비 중이다.

16) 예를 들어 세일즈포스닷컴은 SW플랫폼인 Force.com을 통해 개발자들에게 편리한 개발환경을 제공하고, 이를 통해 만들어진 솔루션들이 AppExchange를 통해 거래되도록 하면서 비즈니스 서비스 포탈 사업자로서의 비즈니스 전략을 구현 중. 현재 AppExchange는 제3의 개발자들이 만든 애플리케이션의 거래시장으로 발전하고 있으며, 세일즈포스닷컴은 이를 활용한 수익공유모형을 제시하고 있다. 이러한 거래시장을 기반으로 하는 비즈니스 모델은 구글이나 MS, 애플과 같은 대부분의 클라우드 컴퓨팅 서비스 사업자의 핵심적인 비즈니스 모델로 추진 중

〈표 2-8〉 국내 주요부처의 클라우드 컴퓨팅 추진현황

부처	특징	주요 내용
지식경제부	그린 IT와의 결합	o 그린 IT를 클라우드 플랫폼에 적용, 자원 활용률을 높인 친환경 클라우드 컴퓨팅 인프라를 구축 o 클라우드 컴퓨팅 인프라에 주목하고 있음 - 클라우드 컴퓨팅 테스트베드 구축을 위한 '독립형 컴포넌트 기반 페타급 플랫폼 개발' - 클라우드 컴퓨팅 원천 기술을 개발하는 '신뢰성 컴퓨팅 기반 기술 개발' 연구과제사업에 착수
방송통신위원회	서비스 중심접근	o 종합유선방송사업자 (SO)가 공동 사용할 수 있는 클라우드 구축 및 첨단 개인화 방송 서비스 인프라를 조성 o 중소벤처 지원을 위해 클라우드 컴퓨팅 서비스 테스트베드 구축할 방침
행정안전부	효율적인 정부 구현	o 정부통합전산센터를 클라우드 인프라로 발전시켜나갈 방침으로 2012년까지 4158억 원을 투자 할 예정 o IT 자원을 신청 받아 논리적으로 할당하기 위한 HW통합 사업을 추진 중 o 정부전산센터를 이용해 정부기관 뿐 아니라 개인과 기업 등을 대상으로 클라우드 형태의 전자정부 서비스를 제공할 계획

출처 : 성병용 (2009), 보완[17)]

기업의 경우 세일즈포스닷컴, 한국EMC, VM웨어 코리아 등 해외기업의 진출이 가시화되고 있으며, 이에 대응한 국내 기업들의 대응도 빨라지고 있다. 특히 KT, 삼성SDS 등의 국내 통신사와 대형IT서비스기업의 진출이 두드러지게 나타나고 있으며, 클루넷, 넥스알, 공영 DBM 등이 CDN, CRM등의 틈새시장을 공략 중이다.

〈표 2-9〉 국내 주요 중소기업 클라우드 제공사

사업자	서비스 내용
넥스알	- 대용량 데이터 처리 기술인 하둡을 바탕으로 다양한 어플리케이션 제공
한국 EMC	- 모지 : 개인 PC에 새로 추가되거나 수정된 데이터를 EMC 클라우드 인프라에서 제공 백업하는 서비스
클루넷	- CCN(Cloud Computing Network) : 네트워크와 스토리지 자원의 가상화를 통한 클라우드 컴퓨팅 제공
VM웨어 코리아	- VM웨어 v스피어4 : 클라우드 컴퓨팅을 통합 관리할 수 있는 운영체제

17) 성병용, 국내기업의 클라우드 컴퓨팅 동향 및 전략, SW인사이트 정책리포트, 2009.07

LG CNS와 삼성SDS는 IaaS서비스를 위한 인프라 구축에 집중하고 있으며, 중장기적으로 SaaS와 PaaS분야의 서비스 오퍼링도 함께 준비 중인 것으로 알려지고 있다. 그러나 시장 환경이 불투명하고, 기술적인 문제도 여전히 남아있어 우선은 IaaS서비스에 집중할 것으로 알려지고 있다. 한편 통신사업자인 SKT의 경우 기존 통신망을 활용하여 IaaS서비스를 제공하는 한편, 개발플랫폼으로서의 PaaS서비스, 부하 테스트 소프트웨어의 기능을 서비스하는 T퍼포먼스(SaaS)서비스를 소개했다. 이중 PaaS서비스는 국내최초의 서비스 이자, 국내 유일의 퍼블릭 클라우드 컴퓨팅 서비스로 주목받고 있다.

〈표 2-10〉 국내 사업자의 클라우드 컴퓨팅 사업현황

업체	산업군	주요 내용	파트너	서비스 영역
A사	통신	IaaS 서비스 제공을 목표로 서비스 모델과 기술검증 추진	HP (우선협상대상자)	IaaS(1차), PaaS, SaaS
B사	통신	클라우드 인프라 구축	MS	IaaS
SKT	통신	SKT 통신망을 통한 인프라스트럭처 서비스	ANC	IaaS, PaaS
		클라우드 컴퓨팅 플랫폼을 통한 개발파트너에 IT자원과 개발환경 지원	IBM	
		T퍼포먼스: 부하테스트 SW지원	HP	SaaS
LG CNS	IT서비스	MS 다이내믹 데이터센터로 클라우드 인프라스트럭처 구현	MS	IaaS
			MS	IaaS
삼성 SDS	IT서비스	클라우드 컴퓨팅 센터 구축	-	IaaS

출처 : 전자신문[18)]

향 후 국내 시장에서의 기업용 클라우드 컴퓨팅은 IaaS와 SaaS 중심으로 성장할 전망이며, PaaS의 확산은 적지 않은 시간이 소요될 전망이다. 이는 구글, MS등 해외의 주요사업자들의 국내 PaaS서비스 진출이 가시화되지 않고 있는 상황에서, 국내기업들의 경우 개발자 참여를 통한 애플리케이션의 개발과 테스트, 유통을 안정적으로 지원할 수 있는 충분한 플랫폼 기술역량이 확보되지 못했기 때문이다.

18) 전자신문, 2009년 12월 6일 '클라우드 컴퓨팅 국내도입현황'

〈표 2-11〉 클라우드 컴퓨팅 서비스 유형별 확산전망

부처	특징	주요 내용
수요 시장	IaaS	o 자체적인 IT인프라 구축에 부담이 큰 중소. 중견기업과 IT자원에 대한 가변성이 큰 인터넷서비스 기업 등의 수요가 확대될 전망 o 은행, 대기업 등 대형 수요기업은 이미 자체적인 인프라를 구축하고 있어, 충분한 레퍼런스가 확보되지 않은 클라우드 컴퓨팅 서비스에 유보적 o 중. 장기적으로 재무적 효용성과 서비스 안정성이 확보될 경우 IT서비스 계열사를 통해 프라이빗 클라우드 컴퓨팅 도입이 예상
	PaaS	o 주요 수요시장은 솔루션 기업과 ISV이나 현재 국내시장에서는 참여할 만한 플랫폼이 부재로 당분간 도입이 지연될 것으로 전망 o IaaS, SaaS의 확산과 함께 플랫폼 기술역량을 확보한 대형 IT서비스 기업과 통신사를 중심으로 점진적인 확산 예상
	SaaS	o 중소. 중견 기업을 대상으로 CRM 등 SaaS가 확산되고, 네트워크 부하가 가변적 인터넷 기업을 중심으로 CDN 등의 서비스가 확산 중 o 다양한 서비스 출시되고, 레퍼런스가 확보될 경우 IT인프라 및 SW에 대한 부담이 큰 중소기업을 중심으로 IaaS와 SaaS가 확산될 전망 o 공공부문의 경우 국가 마스터플랜 수립을 통해 전자정부 구축에서 클라우드 컴퓨팅의 도입을 모색 중
공급 시장	IaaS	o IBM, EMC 등 해외 사업자와 삼성SDS, LG CNS, KT 등 국내 사업자의 시장진출이 가시화. 이에 사업자간 경쟁에 의해 저렴한 양질의 서비스가 제공되며 수요시장 확산을 촉발할 전망
	PaaS	o 구글, MS 등 해외사업자의 경우 국내시장 직접진출은 부진. 국내사업자는 기술역량 부족으로 본격 진출 한계
	SaaS	o CRM 등의 솔루션 시장을 중심으로 해외기업의 직접 진출이 이루어지면서 글로벌 솔루션 기업과 국내 기업 간 경쟁이 본격화할 전망 o 딘. CRM이외 솔루션 분야시장형성은 매우 저조. 국내 시장은 아직까지는 SaaS 보다는 단품위주 ASP를 중심으로 형성

다만 SaaS의 경우 기존 ASP(Application Service Provider)의 수준과 범위가 확장되며 빠르게 성장 중으로 CRM(Customer Relationship Management)등 표준화된 프로세스를 지원하는 분야(예, 주유소)와 네트워크나 스토리지 등 컴퓨팅자원의 수요가 가변적인 CDN(Content Delivery Network)등 HW와 연계된 웹 비즈니스 영역 (중소 포털 및 방송사)을 대상으로 확산 예상된다. 실제 SK C&C는 계열 주유소 대상 시범서비스를 준비중이며, 클루넷은 웹 솔루션과 HW가 연계된 CDN서비스로 빠르게 성장 중이다. 그러나 SaaS역시 CRM이나 ASP중심의 단품 서비스, 웹기반 솔루션을 넘어서 기업 내부 프로세스를 통합적으로 지원하거나, 기업 Ecosystem을 지원하는 전문 솔루션은 다소 시간이 소요

될 것으로 전망된다.

IaaS 역시 통신사업자, 대형IT서비스 사업자 등 높은 브랜드와 서버운영역량, 마케팅 역량을 보유한 사업자 중심으로 서비스 확대 전망이다. 다만 미션 크리티컬한 업무를 수행하는 금융계열기업과 대기업들은 현재와 같은 시스템을 유지하며 점차 프라이빗 클라우드를 중심으로 도입하게 될 전망. 단, 일부 대기업은 계열 IT서비스기업의 클라우드 컴퓨팅 서비스 확산 지원을 위해 부분적으로 도입하며, 점차 확산될 것으로 예상된다.

제 3 절 국내 클라우드 컴퓨팅 시장 장애요인

1. 클라우드 컴퓨팅 확산의 장애요인

클라우드 컴퓨팅은 현재 초기 도입단계(Early Adopters Market)를 지나고 있다. 그러나 본격적인 성장단계로 진입하기 위해서는 광범위한 기업시장에서의 수요확산이 중요하다. 그러나 이를 위해서는 기업 사용자들이 가지고 있는 몇 가지 우려를 불식시켜야 하는 과제가 남아있다.

첫 번째는 서비스의 안정성(Reliability)에 대한 우려이다. 대표적인 클라우드 컴퓨팅 사업자인 아마존의 서버 및 스토리지 컴퓨팅 서비스인 'S3 서비스'는 2008년 2월 15일 약 2시간가량 중단되면서 수천 개의 기업과 개발자들, 30여만 명의 사용자들이 피해를 입었다. 비록 2시간에 불과한 사고였지만, 미션 크리티컬한 업무를 수행하는 기업의 경우(예를 들어 은행과 같은 경우) 그 피해가 매우 클 수 있다.

두 번째는 클라우드 속에 던져진 자료들과 정보들에 대한 불안감이다. 사용자들은 자신들의 핵심 데이터와 정보를 외부의 서버에 저장하는데 대한 우려를 가지고 있다. 특히 분산컴퓨팅과 가상화를 통해 IT자원의 효율성을 극대화시키는 특성 상 사용자들은 정작 자신의 핵심적인 데이터가 어디에 저장되어있고, 어떻게 관리되고 있는지 알 수 없다.

세 번째는 낮은 표준화 수준으로 인한 서비스 전환의 어려움이다. 대부분의 클라우드 사업자들은 자체적인 플랫폼을 통해 서비스를 제공하고 있다. 개발자들은 사업자들이 제공하는 개발환경에서 이들이 제공하는 가이드라인과 룰(프로그래밍 언어와 데이터 저장구조, 시스템 아키텍처)에 따라 어플리케이션을 개발하며, 한 클라우드에 속한 사용자들은 다른 클라우드로 전환이 어렵다. 결국 사용자 입장에서는 중. 장기적으로 하나의 클라우드 사업자

에 종속될 수 도 있다는 우려가 존재한다.

또한 레거시 인프라로 인한 전환비용도 쉽지 않은 문제이다. 사용자 측면에서는 검증되지 않은 새로운 컴퓨팅 환경을 도입하기 보다는 기존 IT인프라에 대한 투자와 이의 활용성을 높이는데 집중하는 것이 더 안전할 수 있다. 또한 새로운 환경에 대한 직원들의 적응, 기존 시스템과 새로운 시스템과의 충돌 등 예상치 못한 비용들이 발생할 수 있는 상황에서 기업들은 모험적인 선택을 회피하기 쉽다.

특히 클라우드 컴퓨팅을 통해 얻을 수 있는 상대적인 편익을 정확하게 계산하기 어렵다는 점도 기업의 선택을 어렵게 하는 요소이다. 예를 들어 중장기적으로 IT인프라를 인하우스로 구축하는 것과 클라우드 컴퓨팅 서비스를 이용하는 것 중 어느 것이 투자효율성이 높을 것인지, 명확한 ROI(투자대비수익)에 의해 결정을 내려야 하는 기업입장에서는 클라우드 컴퓨팅 서비스의 선택이 어려울 수 있다. 다만 다양한 경쟁자의 등장으로 가격이 표준화되는 모습을 보이고 있으며, 사용자로 하여금 예상비용을 손쉽게 계산해 볼 수 있는 환경이 제공되고 있어 이러한 부분은 점차 완화될 수 있을 것으로 보인다. 실제 아마존을 비롯한 많은 클라우드 컴퓨팅 서비스제공자들은 사용자들이 직접 예상되는 클라우드 컴퓨팅 서비스 이용비용을 계산할 수 있는 시뮬레이션 프로그램을 제공 중이다.

〈표 2-12〉 클라우드 컴퓨팅 서비스의 Pros & Cons, 발전의 조건

Pros	Cons
o 사용도가 낮은 IT자원에 대한 자산구매를 회피하여 운영비용 절감 o 갑작스런 IT자원의 수요변화에 대한 저렴하고 신속한 대응 가능 o 필요한 자원의 선택적 구매와 사용량기반 대가 지불의 합리적인 가격모델 o 자산의 운영비화로 재무적 유연성 확보 o 해커와 같은 외부 침입 및 공격 시스템 및 데이터 보호용이	o 클라우드 컴퓨팅 서비스의 안정성에 대한 우려 (Reliability) o 클라우드에 주요데이터와 정보를 저장하는데 따른 보안상의 우려(Security) o 표준의 부족으로 인한 아른 클라우드로의 전환 어려움 (Portability) o 기존의 레거시 인프라로부터의 전환에 따른 기회비용 및 정확한 투자편익 계산의 어려움
초기도입기를 넘어 성장단계 진입을 위한 조건	
o 클라우드 컴퓨팅 서비스의 QoS보장과 SLA(Service Level Agreement) 제공 o 기업수요를 충족시킬 수 있는 애플리케이션/서비스의 고도화 o Best Practice 및 기업 레퍼런스의 확대 (보안에 대한 우려 불식) o 주요 SW기업들의 적극적인 클라우드 컴퓨팅 서비스 시장 진출을 통한 경쟁 활성화	

출처 : 정제호(2008)[19]

2. 법, 제도적인 문제점

클라우드 컴퓨팅에 대한 기업 사용자들의 우려가 적지 않음에도 불구하고, 아직 국내 법. 제도는 이러한 우려를 불식시키기에는 부족한 점이 적지 않다.

첫째, 신규 서비스인 클라우드 컴퓨팅을 다룰 수 있는 법체계가 부재하다. 현재 정보통신서비스에 대한 정보보호의 경우, '정보통신망 이용촉진 및 정보보호 등에 관한 법률'을 통해 규제하고 있으나, 그 대상이 주로 대형 망사업자, IDC사업자, 포털사업자, 게임서비스사업자, 전자상거래 사업자, 직전 3개월간 일평균 이용자 수가 1만 명 이상의 정보서비스 사업자로 제한하고 있어 클라우드 컴퓨팅 서비스를 제공하는 다양한 사업자를 포괄하고 있지 못하다. 또한 서비스 장애로 인한 사용자 피해보상의 경우도 동법에 의해 서비스 제공자의 보험가입이 의무화되어 있으나, 그 대상이 집적된 정보통신시설을 운영, 관리하는 사업자(통상 IDC사업자)로 국한되어 클라우드 컴퓨팅 사업자에 대한 고려는 미흡하다.

둘째, 클라우드 컴퓨팅 서비스 장애에 따른 사용자 보상규정도 미흡하다. 서비스 장애 시 현재는 개별 사업자의 사용약관에 따라 보상규정을 제시하고 있다. 그러나 대부분의 사업자 이용약관은 장애시간에 따른 이용료의 일부 감액 정도가 일반적이며, 별도의 피해보상 규정은 부재하다. 그러나 광범위한 IT자원을 빌려 사용하는 클라우드 컴퓨팅의 특성 상 서비스 장애로 인한 기업의 피해는 심각할 수 있다.

셋째, 기업정보 및 개인 사생활 보호를 위한 제도적 안전장치가 미비하다. 클라우드 컴퓨팅으로의 전환 시 PC 및 자체서버를 사용하던 방식에서 인터넷과 연결된 클라우드를 활용함에 따라 해킹 등으로 인한 기업정보 및 데이터 유출 등 보안 우려가 확대되고 있다. 기업 영업비밀(혹은 지재권) 및 대외비와 같은 민감한 기업 정보 유출 시 그 피해는 매우 클 수 있다. 특히 서비스 제공 사업자의 파산 시 서버의 소유권에 책임소재가 불분명해지는 상황에서 기업 핵심 데이터에 대한 접근이 어려울 수 있으며, 이는 자칫 사용자 기업들의 연쇄적인 파산이나 비즈니스 수행 불능상황을 양기할 수 있다.

마지막으로 클라우드 간 표준부재로 사업자 전환이 어려운 현실에서 서비스 중단 시 사용자 데이터만으로는 시스템의 정상적인 운용과 복구에 한계가 존재한다. 실제 사용자의 기업정보나 데이터의 경우 법적 소유권이 사용자에 있으나, 가상머신 및 플랫폼에 대한 소유권은 클라우드 컴퓨팅 서비스 제공사업자에 있다. 대부분의 클라우드 컴퓨팅 서비스의

19) 정제호, 클라우드 컴퓨팅의 현재와 미래, 그리고 시장전략, SW인사이트 정책리포트, 2008.10

경우 서버 가상화나 데스크톱 가상화, PaaS등의 경우 하위 가상머신 및 플랫폼과 연동되어 서비스가 제공되고 있어, 가상머신과 플랫폼 정보가 제공되지 않을 경우 단순 데이터만으로는 시스템의 복구가 사실상 어려운 상황이다. 따라서 클라우드 컴퓨팅 간 상호운용을 위한 표준화가 이루어지지 않은 상황에서 사용자가 비록 데이터의 접근 권한이 있다하더라도 이를 활용할 수 있는 시스템이 부재한 상황에서는 여전히 심각한 문제가 발생할 수 있으며, 이러한 상호운용성의 부족은 클라우드 컴퓨팅 사업자에 대한 사용자의 선택권을 제한하는 문제도 발생한다.

현재 클라우드 컴퓨팅 시장은 이제 초기 시장을 지나고 있다. 망의 고도화와 가상화 기술발전, 경제위기에 따른 IT비용절감 압력과, 그린 IT화에 맞물려 클라우드 컴퓨팅이 많은 기업들의 주목을 받고 있다. 그러나 본격적인 시장의 성장은 핵심 고객층인 기업사용자의 본격적인 도입이 이루어 져야 가능하다. 이를 위해서는 기업들이 가지고 있는 보안이나, 서비스 품질, 서비스 제공자 파산에 따른 서비스 연속성 보장, 클라우드 간 상호운용성 확보 등 다양한 우려들이 해결되어야 가능하다. 이러한 관점에서 본 연구에서는 클라우드 컴퓨팅 서비스의 활성화를 위한 다양한 이슈들을 살펴보고, 이에 대한 법, 제도적인 해결방안을 모색한다.

제3장 클라우드 컴퓨팅 활성화를 위한 제도개선 방향

제 1 절 사업자의 파산 등에 따른 사용자 보호방안
제 2 절 일시적 서비스 장애에 따른 사용자 보호방안
제 3 절 사용자 보안우려 해소 방안

제 1 절 사업자의 파산 등에 따른 사용자 보호방안

1. 사업자 파산에 따른 문제점과 사례 분석

클라우드 컴퓨팅은 서비스 제공사를 중심으로 시스템이 운영되기 때문에 해결해야 할 몇 가지 문제를 가지고 있다.

첫째, 클라우드 컴퓨팅을 이용하는 업체가 해당 서비스를 제공받지 못함으로 인해 수행하던 기능을 전혀 사용할 수 없게 됨에 따라 그와 관련된 일체의 프로세스가 일시에 정지하여 사용자는 막대한 피해를 입을 수 있다.

둘째, 지금까지 이용하였던 데이터의 훼손이나 손실의 문제이다. 클라우드 컴퓨팅을 제공하는 회사가 갑작스런 금융위기 등으로 인해 파산·폐업 등을 한다면 그간 서비스를 이용하였던 회사는 지금까지 보유하였던 정보 및 데이터를 전부 이용할 수 없게 될 것이다. 이러한 상황이 발생한다면 클라우드 컴퓨팅을 이용하였던 업체는 경영상 큰 손실을 예상할 수 있으며, 심각한 경우에는 사업의 영업기반까지 흔들리게 되어 연쇄적인 부도를 예상할 수 있을 것이다.

셋째, 클라우드 컴퓨팅 서비스 제공자의 시스템 간 상호 호환성의 문제가 발생할 것이다. 만일 서비스를 제공하는 업체가 부도·폐업 등으로 인해 서비스를 중단하는 경우에도 서비스 이용 업체는 다른 클라우드 컴퓨팅 업체를 선정하여 동일한 서비스를 제공받을 것으로 예상되는데, 이 때 클라우드 컴퓨팅 업체 간 시스템 부분에서 호환이 되지 않으면 이전 이용하였던 클라우드 컴퓨팅 서비스에 의해 생성된 데이터는 무용지물이 될 것이다.

그러나 다행히도 아직까지 클라우드 컴퓨팅 서비스 중단으로 인한 피해 사례가 많지 않고 있다. 이는 클라우드 컴퓨팅 시장이 태동하는 단계이기 때문에 아직까지 클라우드 컴퓨팅을 제공하는 기업이 많지 않기 때문이다. 그러나 최근에는 클라우드 컴퓨팅 서비스를 제공 업체에서 서비스 중단에 따른 피해 사례들이 조금씩 늘어나는 추세이다.

이러한 서비스중단에 대한 문제는 글로벌 대기업인 마이크로소프트사나 구글 사에서 제공하는 클라우드 컴퓨팅 서비스에도 발생하고 있으나, 대부분 서비스 중단은 시설이나 관리 능력이 열악한 중소기업이 더 취약할 수밖에 없다. 특히 우리나라의 경우에는 대부분 클라우드 컴퓨팅 서비스 제공사는 SaaS를 중심으로 하는 작은 중소기업이 대부분이다.

일례로 지난 12월에 발족한 한국 클라우드 컴퓨팅 연구조합의 43개 회원사들을 살펴보

면 KT, 아시아나 IDT 등의 일부 기업을 제외하고 대부분 중소기업이 조합 회원으로 가입하여 활동하고 있다.[20] 이에 상대적으로 영세한 중소기업은 대기업에 비해 파산·폐업 등에 쉽게 노출되어 있으며, 서비스를 이용하는 사용자에게도 지속적인 유지보수를 담보하지 못하고 있다.

가. 서비스 미 이용으로 인한 피해

클라우드 컴퓨팅 서비스의 중단문제는 영세한 기업에서 더욱 빈번히 발생하지만 세계적인 글로벌 기업에서도 이러한 정보관리 위험은 중소기업뿐만 아니라 대기업에게서도 빈번히 발생하고 있다. 최근 구글의 클라우드 기반 서비스인 검색부터 구글 뉴스, 구글 맵스 등이 불통되는 사고가 올 해 몇 차례 일어나 이용자들이 많은 불편을 겪었다. 이를 업무적으로 이용하고 있는 사람들은 비즈니스 차원에서도 막대한 손실을 입었을 것이다.

또한, 최근에 발생한 가장 큰 서비스 중단에 대한 SW 업계의 선두주자라고 할 수 있는 마이크로소프트사의 모바일 기기인 '사이드킥[21]'에서 제공하는 클라우드 컴퓨팅 서비스에서 발생되었다.

이는 사이드킥의 MS 서버에서 발생한 심각한 오류로 인해 09년 10월 초부터 데이터 손실과 접속장애가 계속됨에 따라 발생을 하였으며, MS사는 사이드킥의 판매를 당분간 중단한다고 발표하였다. 그러나 더욱 심각한 것은 손실된 데이터는 복구가 불가능 할 것으로 보임에 따라 서비스 이용고객으로부터 항의가 빗발치고 있으며, 피해 규모는 아직 발표되지 않았지만 최소 수천 명에 달할 것으로 추정된다. 이번 사이드킥 사고로 그동안 구글과 경쟁하며 클라우드 컴퓨팅과 모바일 시장 선점 기회를 노렸던 MS는 자존심에 큰 상처를 입게 되었다. [22]

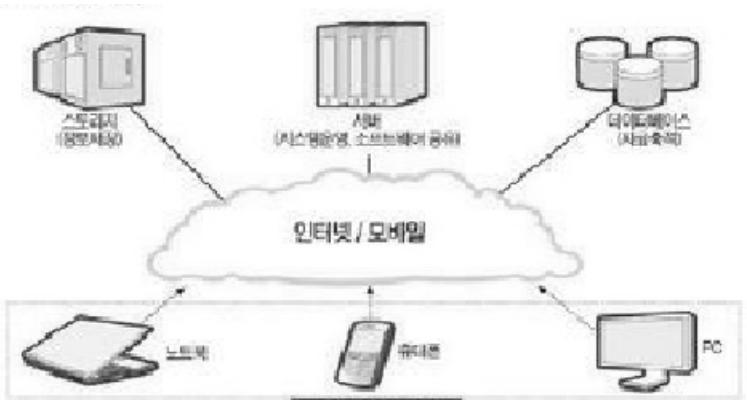
---

20) 한국클라우드 컴퓨팅연구조합 http://www.cccr.or.kr

21) 사이드킥 서비스는 사용자의 주소록과 일정표, 사진 등 각종 데이터를 단말기 자체 대신 인터넷에 연결된 서버에 저장해 기기가 바뀌어도 언제든 데이터를 볼 수 있게 해 주는 서비스를 제공하고 있다.

22) 이미나, "MS 망신살… 사이드킥 고객 데이터 몽땅 날아가", 한국경제('09.10.13)

〈그림 3-1〉 MS 사이드킥 서비스 제공체계



나. 데이터 손실로 인한 피해사례

클라우드 컴퓨팅에서 시스템을 이용하지 못하여 생기는 문제보다 더욱 큰 문제는 사용기업이 생산한 데이터의 손실 및 멸실 이다. 클라우드 컴퓨팅 서비스는 다른 기업에 의해 다시 이용을 하면 되지만 생산된 데이터는 서비스 제공사가 사업을 정리하고 서비스를 중단하면 원상복구가 힘들기 때문이다.

구체적인 사례는 지난 2008년 8월 "Linkup"이라는 온라인 스토리지 서비스를 제공하고 있는 너바닉스(Nirvanix)사는 고객 정보의 45% 가량을 손실하고 난 후 사업소가 패쇠되었다. 이 결과 20,000여명의 유료 사용자는 디지털 편집물(음악, 사진, 비디오)을 잃게 되었으나, 서비스 제공사와 스토리지 업체는 책임을 서로에게 떠넘기고 있을 뿐 정작 고객 정보 손실에는 아무도 책임을 지지 않았다. [23]

또한 클라우드 컴퓨팅 제공사와 데이터 저장사와가 별개의 회사의 경우에도 서비스 중단에 대한 문제점이 심각하게 발생할 수 있다. 특히 우리나라의 경우, 클라우드 컴퓨팅 제공하는 상당수의 중소기업이 회사의 영세성 때문에 자체 서버를 구입하지 않고 제3의 스토리지 서비스 제공사를 이용함에 따라, 서비스 중단 시 사용자 데이터 보호의 책임문제에 대해 서로 책임을 떠넘기고 있어 결국 피해는 사용 기업에게 전가되고 있는 실정이다. 이러한 문제로 인한 대표적 사례는 넥서브 사의 사례이다.

클라우드 컴퓨팅의 일부인 SaaS 서비스를 제공하던 사업자인 넥서브라는 회사가 경영상의 어려움으로 서비스를 중단하였으며, 넥서브 사는 서버를 임대하던 IDC가 통신비 및 유

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

지보수 비용의 미납으로 서버 제공을 중단하면서 사용 기업에게 피해가 전가된 사건도 있었다. 결국 이러한 문제가 발생하면 해당 서비스를 이용하던 사용자는 해당 서비스를 이용하지 못하여 업무의 지장을 초래할 것이다. 그리고 최악의 경우에는 클라우드 컴퓨팅 서비스 이용사는 회사의 핵심 정보를 잃어버리게 되어 계속적인 사업수행에 어려움을 겪음에 따라 최악의 경우에는 클라우드 컴퓨팅 이용사의 연쇄적인 부도까지도 예측할 수 있다.

서비스 중단 및 데이터 소멸 등은 사업자의 부도만 해당되는 것은 아니다. 최근 해킹기술의 발달로 인해 클라우드 제공사의 시스템이 심각하게 훼손된다면, 클라우드 컴퓨팅 서비스를 이용하는 업체는 막대한 피해를 입게 될 것이다.

KT와 LG데이콤의 IDC(인터넷데이터센터)에 인터넷 네트워크 및 데이터 관리를 맡기고 있는 중소기업 사이트에 대한 DDoS[24] 공격이 늘어나고 있다. 자체 IDC를 운영하는 중소기업까지 합하면 피해 규모는 훨씬 많을 것으로 업계는 보고 있다. LG데이콤 IDC의 경우 지난 7월 84건이던 DDoS 공격이 8월 113건,9월 139건,10월 156건 등으로 계속 증가하고 있다. KT IDC에 대한 DDoS 공격도 지난 7월 489건에서 8월 215건으로 줄었다가 9월에 다시 420건으로 크게 늘었다.

이렇듯 클라우드 컴퓨팅 서비스 제공사는 악의적 해커에 의한 시스템 해킹 또는 시스템 오류 등이 발생한다면 클라우드 컴퓨팅 서비스는 중단이 되어 사용자는 일시적으로 서비스를 제공받지 못할 뿐만 아니라, 클라우드 서비스 제공사 서버에 있는 데이터가 손실되어 많은 어려움을 겪을 것으로 예상되어 진다. 이에 해킹에 인한 서비스 중단 및 데이터 훼손·멸실 등에 대해서도 방지할 수 있는 대비책 마련도 절실한 실정이다.

다. 클라우드 컴퓨팅 서비스 업체 간 호환성 부재로 인한 피해사례

클라우드 컴퓨팅 서비스 제공업체가 서비스를 중단하는 경우, 클라우드 컴퓨팅 서비스 이용업체는 해당 업무를 계속적으로 수행하기 위해 클라우드 업체의 변경이 필수적이다. 그러나 클라우드 업체 간 데이터나 시스템에 대한 호환규정 등이 전무하기 때문에 클라우드 업체 간 서비스에 대한 호환은 어렵다. 이에 클라우드를 이용하는 사업자는 서비스 업체에 종속되어 업체 변경 등이 불가능하다. 인포메이션위크가 클라우드 컴퓨팅 서비스의

24) 여러 대의 컴퓨터를 일제히 동작시키는 방법으로 특정 사이트를 공격하는 해킹 방식의 하나. 시스템을 파괴해 더 이상 정상적인 서비스를 할 수 없도록 만드는 게 주된 목적이다. 국내에선 지난 7월 7일부터 10일까지 좀비PC(바이러스에 감염돼 기능이 정지되고 바이러스 전파 목적으로 쓰이게 된 PC)를 통해 악의적으로 유포된 악성코드가 주요 정부기관,포털사이트, 은행사이트 등을 공격하면서 주목받았다

일종인 SaaS를 이용하는 업체를 대상으로 설문조사를 실시한 결과, SaaS 사용자 중 40%는 새로운 벤더로의 전환이 어렵다고 조사되었다.

한편, 클라우드 업체에서도 호환을 위한 움직임이 클라우드 업체에서는 업체 간 서로 데이터나 시스템에 대해 호환성을 가질 수 있도록 하게 위해 지난 3월 IBM을 주축으로 약 10여개의 업체가 클라우드 컴퓨팅 환경에서의 제품 호환성을 위해 '클라우드개방선언문(The Open Cloud Manifesto)'을 발표하기도 했다. 그러나 아마존, 구글, MS등 클라우드 컴퓨팅 패러다임을 주도하는 글로벌 기업들이 불참함으로써 개방선언문도 그들만의 행사로 끝난 바 있다.[25)]

2. 사업자 파산 등에 따른 사용자 보호를 위한 해외사례

해외의 경우 클라우드 컴퓨팅 사업자의 갑작스러운 파산 및 폐업에 대비한 대응으로는 기술자료 임치제도[26)]가 대부분이며 별도의 법·제도적 중단방지 장치는 없는 상황이다. 특히 미국에서도 클라우드가 초기시장으로 아직까지 표준화된 SLA도 거의 없을 뿐만 아니라 무료로 제공하는 클라우드 컴퓨팅의 경우에는 서비스 수준을 약정하고 있는 SLA도 거의 없는 실정이다. 이는 대부분 제공되고 있는 클라우드 컴퓨팅 서비스 제공사가 일반 이용자를 대상으로 무료로 제공되고 있기 때문에 책임도 없다고 인식하여 SLA를 마련하지 않은 것으로 보인다.

반면 유료로 운영하고 있는 대형 클라우드 컴퓨팅 사업자들은 서비스 중단에 따른 내용을 SLA에 반영하여 서비스 중단에 따른 제공사의 패널티를 명시하고 있다. 대형 클라우드 제공사는 경제력이 바탕이 되기 때문에 파산·폐업 등에 대해 비교적 자유롭고, 자체적인 미러링 또는 백업 시스템을 갖추고 있기 때문에 임치제도를 활용하지 않고 스스로 데이터를 보호하는 시스템을 구축하고 있다.

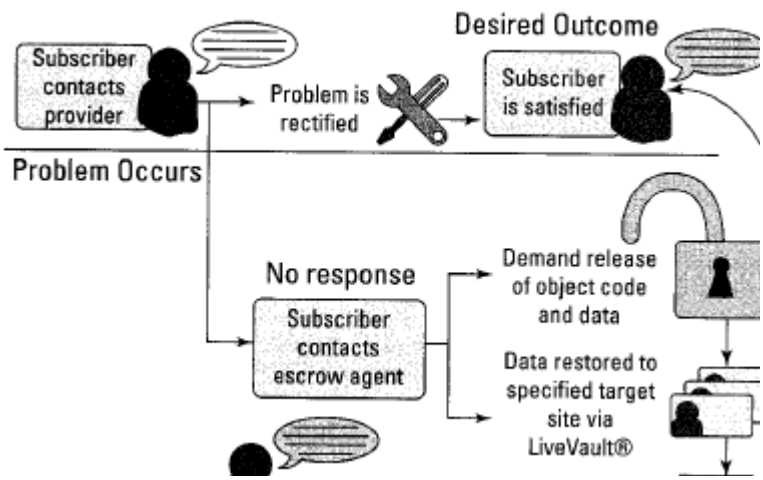
중소 클라우드 컴퓨팅 사업자들 역시 사용자들에게 신뢰를 부여하기 위하여 서비스의 지속성을 확보하기 위해 제 3의 기술임치회사를 통해 자사의 시스템과 데이터를 실시간적으로 업데이트하고 있다.

클라우드 컴퓨팅과 관련한 기술임치 서비스를 제공하는 기업은 세계 제1의 미국 기술임

25) 백지영, '창간4주년기획/ 클라우드 컴퓨팅③' 클라우드 컴퓨팅의 현안과제 '산적', (2009.06.08일)
26) 개발자의 소스코드, 실행프로그램 등을 제3의 임치기관이 보관하고 있다가, 개발기업이 파산·폐업 등이 발생하는 경우 해당 임치물을 사용 기업에게 제공하여 해당 기술의 신뢰성을 보호하여 주는 제도

치회사인 Iron Mountain사와 영국 제1의 기술임치회사인 NCCGlobal사 등이 있다. NCCGlobal의 SaaS EscrowTM SolutionsThere와 Iron Mountain사의 LiveVault 서비스는 기존의 소프트웨어 임치가 치유하지 하지 못하는 SaaS 서비스의 갑작스런 중단으로부터 발생한 고객의 중요한 데이터 상실의 문제를 해결해 주고 있다. 특히 Iron Mountain사는 Cloud 또는 SaaS 고객의 데이터에 대한 실시간 백업을 위하여 200TB이상의 데이터를 관리하고 있다.[27)]

〈그림 3-2〉 Iron-Mountain사의 임치물 교부에 따른 백업 시스템 [28)]



클라우드 임치는 클라우드 컴퓨팅 서비스의 특징을 감안하여 예기치 못한 서비스 중단 시에 클라우드 컴퓨팅 서비스 운용 소프트웨어(application)에 대한 기술 자료를 임치할 뿐만 아니라 고객의 데이터에 대한 보호도 함께 제공함으로써 클라우드 컴퓨팅 서비스의 신뢰성을 제고할 수 있는 수단을 제공한다. 클라우드 에스크로우(Escrow)는 기존의 소프트웨어임치에 사용자의 데이터에 대한 관리를 동시에 제공한다는 점에서 차별화 된다고 할 수 있다.

우선 클라우드 에스크로우는 클라우드 애플리케이션의 목적코드 및 소스코드(source codes) 기타 관련 기술 자료를 중립적인 제3자인 임치기관에 보관해 둠으로써 장기간의 서비스 중단을 대비할 수 있다. 만일 클라우드 컴퓨팅 서비스 업체가 파산 등의 사유로 서

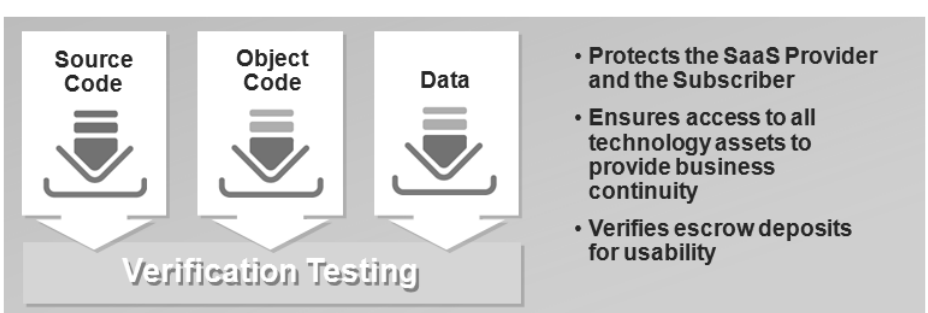
27) Iron Mountain사 홈페이지 〈http://www.ironmountain.com〉 (2009.11.20. 방문)
28) Richard Kane, "Software Escrow For Dummies", Wiley Publishing.INC, p.42.

비스를 더 이상 제공할 수 없는 경우 사용자는 임치된 기술 자료를 교부받아 스스로 또는 동종 클라우드 업체의 조력으로 서비스 중단의 장기화로 인해 발생할 수 있는 피해를 막을 수 있다. 이러한 형태의 임치는 기존의 소프트웨어임치와 기본적으로 동일하다고 할 수 있다.

그런데 이러한 클라우드 애플리케이션의 관련 기술 자료를 임치하는 것만으로는 클라우드 컴퓨팅 서비스의 중단으로 발생하는 피해를 완전히 해소할 수 없다. 즉, 클라우드 컴퓨팅 서비스 중단으로 인해 사용자의 데이터 일부 또는 전부에 대한 접근을 할 수 없다면 사용자는 물론 당해 기업의 주주들에게도 중대한 악영향을 미치게 된다. 일반적으로 클라우드 컴퓨팅 서비스를 이용하는 동안에는 사용자가 자신의 데이터를 자신의 컴퓨터에 백업받을 수 없기 때문에 클라우드 사업자의 백업지원에 의존할 수밖에 없다. 따라서 예상치 못한 클라우드 컴퓨팅 서비스의 중단에 대비하여[29] 클라우드 임치기관으로 하여금 실시간(real time)으로 자동 백업을 하게 하는 것은 클라우드 임치의 핵심이라고 할 수 있다. 현재 많은 클라우드 컴퓨팅 서비스 업체들이 고객의 데이터에 대한 백업지원을 하고 있으나 대부분 시간적 공백이 있거나 일정치 않은 백업 서비스를 하고 있다.

또한 클라우드 컴퓨팅 서비스 기업이 자사 시스템에 백업하거나 제3의 IDC(Internet Data Center)에 데이터를 보관하는데 IDC도 파산, 천재지변 등의 사유로 서비스 중단을 하는 경우가 있을 수 있다. 따라서 신뢰성 있는 제3의 기관이 고객의 데이터를 실시간으로 백업해 줌으로써 원거리 서버 데이터를 유사시 완전히 복구해 줌으로써 고객이 언제라도 필요한 때에 자신의 데이터에 대한 접근을 가능하도록 할 필요가 있다.

〈그림 3-3〉 Iron Mountain사의 SaaS Escrow

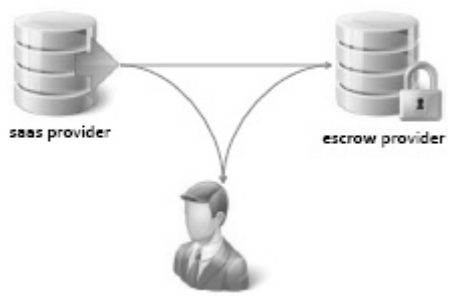


29) 세일즈포스닷컴(salesforce.com)의 경우 3개의 IDC가 있으며 모든 데이터는 실시간으로 백업되고 있다. 또한 시스템이 다운된 경우 offline 버전, 즉 PC에 설치되어 있는 버전이 작동되도록 하고 있다. 평소는 온라인에서 사용하다가 비상시에는 offline에서도 사용할 수 있도록 하고 있다.

또한 이러한 클라우드 임치를 통해 클라우드 컴퓨팅 서비스에 대한 전체를 보호받기보다 데이터를 우선적으로 보호하기 위해서는 일부 업체는 데이터 임치(Data Escrow) 서비스를 통해 1차적으로 사용기업의 데이터에 한하여 보호를 해 주고 있다. 이러한 방식은 기존의 클라우드 컴퓨팅 서비스와 동일하게 시스템을 구축하는 클라우드 임치보다는 훨씬 비용 적으로 적게 소요될 수 있으나, 시스템의 연속성인 사용에는 담보하지 못하는 장점을 가지고 있다.

이에 미국의 임치 서비스 회사들은 선별적으로 클라우드 임치 서비스를 이용할 것인지 데이터 임치서비스를 이용할 것인지 선택하도록 하고 있다.

〈그림 3-4〉 Clio 사의 데이터 임치



또한 유럽 제1의 임치기업인 NCCGlobal사도 미국의 Iron Mountain사와 같이 클라우드 임치 서비스를 유형별로 세분화하여 차별화된 서비스를 제공하고 있다.

〈표 3-1〉 NCC사의 임치서비스 유형

구분	서비스 내용	비고
일반 임치	- 클라우드 컴퓨팅 서비스와 관련된 정보를 모두 임치하고 임치물의 교부조건이 발생하였을 경우에는 사용 기업이 해당 기술을 유지보수	소극적 임치 (기존 임치제도의 확장)
완전 임치	- NCC 기술전문가가 클라우드 컴퓨팅 서비스와 동일한 시스템을 클라우드 컴퓨팅 서비스 제공사에서 구축하고 테스트까지 실시 - 유지보수 매뉴얼, 개발사양서 등까지 작성하여서 임치	적극적 임치
데이터 저장	- NCC사의 데이터 저장 공간을 이용하여 클라우드 컴퓨팅 서비스 사의 데이터를 저장 - 기간별 저장(1일, 1주일, 1달)도 가능하고 실시간 데이터 저장도 선택에 의해 가능	

한편 각국 정부들도 주요 시스템이나 솔루션의 공공조달 시 기술자료 임치를 통해 서비스의 안정성과 지속성을 보장하고 있다.

가. 미 국

기술자료 임치제도는 미국에서 가장 활발하게 이루어지고 있다. 이러한 이유는 미국이 세계 소프트웨어산업 등을 주도하고 있기 때문에 그에 따른 사회적 요구가 많기 때문이다. 미국은 지적재산권의 보호의식이 보편화되어 있어 소기업의 지적재산권이라도 발주기업에 귀속하지 않고 보호된다. 이에 따라 사용자들이 소기업이 개발한 시스템이나 솔루션을 신뢰하고 사용할 수 있도록 하기위하여 믿을만한 제 3의 기업을 통해 서비스의 연속성을 보장할 수 있도록 하는 사회적 시스템으로 기술임치제도가 활용되어 왔다. 실제 포천지(Fortune) 선정 1천개 기업의 약 80%가 적어도 1개 이상의 소프트웨어를 임치기관에 임치하고 있다고 보고되고 있다.[30] 이에 세계적인 보안기업인 RSA, IBM사도 사용 기업에 대한 신뢰성을 부여와 담보의 목적을 위해 미국의 대표적 임치기관인 Iron-Mountain사 등에 임치를 하고 있는 것으로 조사되고 있다.[31]

정부 및 공공기관도 오픈라인 방식의 소프트웨어를 도입함에 있어 서비스 제공자의 중단에 대비하여 임치제도를 관련 법·제도에 반영하고 적극적으로 활용하고 있다.

뉴욕 주에서는 조달계약서에 임치제도를 반영하여 뉴욕 주가 소프트웨어의 소스코드를 확보하지 못할 경우에는 소스코드를 제3의 임치기관에 안전하게 임치하여야 함을 명시하고 있고[32] 테네시 주도 주요한 소프트웨어를 도입하면서 서비스 중단에 대비하여 임치제도를 활용하고 있다.

또한 미국 일부 주의 선거법은 각종 선거의 전자개표 과정에서 공정 및 정확성에 대한 시비가 생길 경우에 대비하여 전자투표 개표 소프트웨어의 소프트웨어를 임치하도록 규정하고 있다. 캘리포니아에서는 이와 같은 내용의 법조항을 1990년 1월 1일을 기하여 발효하였다. 이는 전자투표 집계가 허술한 보안 때문에 손상될 우려가 있으며 부정확하다는 지적을 불식시키기 위해 도입되었으며, 특약사항에 개표용 소프트웨어의 판매중단이나 개발회

30) Anthes, G. H., "The Dangers Behind Software", COMPUTERWORLD(Dec.21,1998). HTTP://www.computerworld.com/cwi/stor/o,1199,NAV47〈uscore〉STO33324,00.html.(2003.10.08 검색)

31) Iron-Mountain사 홈페이지 참조(http://www.ironmountain.com/knowledge/ipm/collateral.asp).

32) 뉴욕 주 조달계약(Directory General Specifications for Procurement Contracts) 제88조에 의하면 임치제도를 통해 유지보수 방안을 확보함을 명시하고 있다.

사의 영업중단 시에도 선거공무원이 임치물을 교부받아 유지 보수할 수 있도록 명시하여 제도를 운용하고 있다.

나. 캐나다

미국과 인접한 캐나다도 미국의 영향을 받아 기술자료 등의 거래 시 임치제도가 거래의 안전장치로서 정착되어 널리 사용되고 있다. 그리고 캐나다의 변호사들은 기술자료 등의 거래에 관해 법률적인 자문을 하는 경우 구매자들에게 임치조항을 계약에 포함하도록 권고하고 있다. 캐나다에서도 미국과 마찬가지로 국가가 사용하고 있는 소프트웨어 등 기술정보에 대해 안전성을 보장할 수 있도록 국가 조달기관인 PWGSC(Public Works and Goverment Service Canada)는 표준조달 조항 및 조건 매뉴얼인 SDMS(Software Development/ Modification Service) 매뉴얼에 소프트웨어 임치제도를 반영하고 있다. 이 매뉴얼의 제10조에 의하면 정부에 소프트웨어를 납품하는 기업은 자사의 선택과 비용으로 임치를 하거나 소스코드를 양도해야 한다.[33] 이에 대부분의 개발기업은 소프트웨어의 소스코드를 정부에게 양도하지 않고 기술자료 임치제도를 이용하여 제3의 임치기관에 임치물을 보관하고 있다[34].

다. 영 국

유럽에서의 기술자료 임치제도는 미국·캐나다 보다 활성화가 되지는 않았지만 영국, 네덜란드 등의 국가를 중심으로 기술자료 임치제도가 확산되고 있다. 영국은 기술자료 임치제도 도입초기에는 국가적 차원에서 임치제도를 활성화하기 위해 국립전산원인 NCC

33) SDMS 매뉴얼 10조에 의하면 정부계약 상대자는 다음의 둘 중 하나를 선택하여야 한다.
(a) 정부가 주문한 소프트웨어를 인수한 때로부터 30일 이내에 정부에 그 소프트웨어를 위한 소스코드를 양도하거나,
(b) 위 (a)에서 언급한 기한 내에 수치인(Escrow Agent)에게 소스코드를 양도하여야 한다.

34) 캐나다 조달매뉴얼 SDMS
4. If Pre-Existing Software forms part of the Custom Software, and if the Contract does not otherwise require the Contractor to deliver the source code for that software to Canada or to put that source code into escrow for the benefit of Canada, the Contractor shall, at its option and expense, either:
(a) deliver the source code for that software to Canada within thirty (30) days following acceptance of the Custom Software by Canada; or
(b) deliver that source code, at the time mentioned in paragraph (a), to an escrow agent approved by the Minister to be held in trust by that agent for release to Canada upon the occurrence of any of the following events:

(National Computing Centre)에서 1981년 소프트웨어임치제도를 도입하여 운영하였다. 이후 영국에서 기술거래를 하는 경우 임치제도 이용이 필수적인 안전장치로 도입됨에 따라 1999년 NCC Group이라는 독자적인 회사로서 분리되어 임치제도를 운영하고 있고 고객의 수도 10,000여 사가 넘는 유럽에서 가장 큰 임치기관으로 성장하였다.

영국의 국가·공공기관도 미국 등과 유사하게 국가 운영 소프트웨어의 안전한 사용을 위해 국가 조달기관 OGC/OGCbs의 조달 매뉴얼인 S-CAT(Service Catalogue For The Public Sector)[35]에 임치조항을 명시하여 국가 조달 소프트웨어는 NCC Group사에 임치하도록 하고 있다.

영국의 대표적 임치기관인 Ncc Group사는 미국의 임치기업과 같이 임치계약을 다양하게 변형하여 활용하고 있다. 인터넷 웹사이트의 컨텐츠, 웹상의 클라이언트, 서버프로그램 등을 총괄하여 보호할 수 있는 웹사이트 임치(Web Escrow)제도를 운영하고 있으며, 또한 회사의 기밀 및 데이터 등의 기밀을 보호하기 위한 자료 임치제도(Data Escrow)와 재무관련 정보를 확인 및 보호할 수 있는 재무 임치제도(Financial Escrow)도 운영하고 있다.

3. 사업자 폐업 등에 따른 사용자 보호를 위한 국내 현황

가. 사업자 폐업 등에 따란 사용자 보호제도

현재 전기통신사업법에서는 사업자가 폐업을 하거나 제공 중이던 서비스를 중단할 경우 이를 주무부처인 방송통신위원회에 신고하도록 하고 있다[36]. 이 조항은 별정통신사업자 또

35) 영국 조달계약서 매뉴얼 S-CAT의 Escrow Arrangements
C5.18 Where requested by the CUSTOMER in the Services Order, the CONTRACTOR shall place the Source Code of the Deposited Software in escrow with the NCC Group plc within one month of acceptance by the CUSTOMER in accordance with Clause A5 on the basis of the standard agreement or on such other terms as the CUSTOMER, the CONTRACTOR and the NCC Group plc shall agree.
C5.19 The CONTRACTOR shall ensure that the Deposited Software shall include material modifications, developments, updates, patches, enhancements or other modifications to the Software from time to time.

36) '전기통신사업법'내 사업자 서비스 중단 관련 사용자 보호조항
제27조 (사업의 휴지 · 폐지등)
①별정통신사업자 또는 부가통신사업자가 그 사업의 전부 또는 일부를 휴지 또는 폐지하고자 하는 때에는 그 휴지 또는 폐지예정일 30일전까지 그 내용을 당해 역무의 이용자에게 통보하고 방송통신위원회에 신고(정보통신망에 의한 신고를 포함한다)하여야 한다.
②별정통신사업자 또는 부가통신사업자인 법인이 합병외의 사유로 인하여 해산한 때에는 그 청산인(해산이 파산에 의한 경우에는 파산관재인을 말한다)은 지체 없이 이를 방송통신위원회에 신고(정보통신망에 의한

는 부가통신사업자가 사업의 전부 또는 일부를 휴지·폐지하게 될 경우에 그 사실을 이용자에게 통지하도록 하여 갑작스런 사업 중단으로부터 이용자를 보호하기 위해 마련된 조항이다. 클라우드서비스 제공자를 전기통신사업법상 부가통신사업자로 간주 할 경우 이 조항의 적용이 가능하다. 따라서 클라우드 컴퓨팅 서비스의 일부 또는 전부가 휴지 또는 폐지되는 경우에는 그 휴지 또는 폐지예정일 30일전까지 그 내용을 서비스 이용자에게 통보하여야 할 것이다. 이로써 이용자는 서비스 중단에 대비하여 데이터를 백업받거나 중단에 대한 대비책을 강구함으로써 피해를 최소화할 수 있다. 동법 제78조에서 동 조항을 위반하여 신고를 하지 아니한 사업자에게 1천만 원 이하의 과태료를 부과하고 있다.

그러나 만일 클라우드 사업자가 이러한 의무를 이행하지 않거나 또는 서비스 중단이 갑작스럽게 발생한 경우에는 여전히 이용자 데이터를 효과적으로 보호할 수 없게 된다. 따라서 갑작스런 서비스의 중단에 대비한 이용자 데이터 보호와 서비스 중단 후 서비스의 유지 등에 관한 조치가 여전히 필요하다.

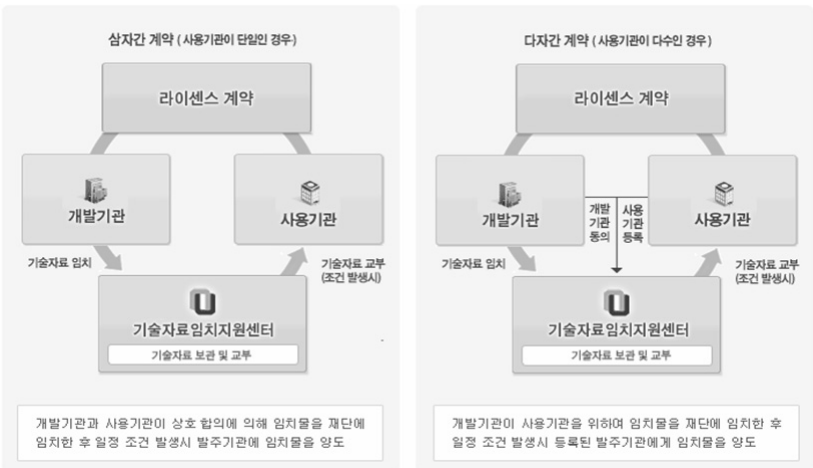
나. 클라우드 임치제도 활용 현황

클라우드 컴퓨팅 분야는 아직까지 국내에 생소한 서비스임에 따라 제도적인 안전장치에 대한 기반이 부족한 실정이다. 국내에서는 1990년대 후반 IT벤처기업을 중심으로 IMF를 극복하기 위해 IT 중소기업이 우후죽순처럼 설립되었다. 그에 반해 중소기업은 경영상, 기술상의 어려움으로 많은 기업이 시장에서 도태되었다.

이에 해당 기술을 사용하고 있는 기업들은 해당 기술에 대한 소스코드, 실행프로그램, 사양서 등을 전혀 보유하지 못해서 사용 소프트웨어에 대한 유지보수가 불가능한 상황이었다. 저작권위원회(舊, 프로그램심의조정위원회)에서는 이러한 문제를 해결하기 위해 다양한 연구조사를 수행하였다. 해외에서는 이를 해결하기 위해 1970년대부터 임치제도를 활용하여 개발기업의 파산·폐업에 대해 대비하고 있었다. 이에 저작권위원회에서도 미국, 영국 등의 사례를 조사하고 국내에 맞게 벤치마킹을 실시하여 1999년부터 소프트웨어 임치제도를 운영하였다.

신고를 포함한다)하여야 한다.

〈그림 3-5〉 임치제도 이용 절차도



출처 : 대·중소기업협력재단(2009)

정부에서도 임치제도를 활용하여 해당 기술에 대한 신뢰성을 도모하고 개발기업의 지적재산권을 동시에 보호하기 위해 법·제도에 임치제도를 반영하여 적극 활용토록 하고 있다.

〈표 3-2〉 정부 소프트웨어 조달정책 등에 기술자료 임치제도 반영현황[37)]

구 분	반 영 내 용
기획재정부	- 공공기관 납품 시 용역계약 일반조건(회계예규 2200.04-161-1)에 제도 반영('06.9)
지식경제부	- 공공기관이 SW 발주 시 안정장치를 마련하기 위해 SW 분리발주 가이드 라인에 제도 반영('07.5)
공정거래위원회	- SW 및 전자·전기업종 표준하도급계약서에 제도 반영('05.9,'05.11·'06.7)
방위사업청	- 국방기술의 안전성을 확보하기 위해 방위사업관리규정에 기술자료 임치제도 반영 ('09.1)
조달청	- SW부문 정부 조달 시 기술자료 임치제도를 이용한 기업에게 가산점을 부여(정보통신부 고시 제2007-51호(SW 기술성 평가기준))
중소기업청	- 대·중소기업 상생협력 촉진에 관한 법률에 임치제도 반영('07.05) - 기술자료 임치제도 운용요령 제정('09.05) - 구매조건부 관리규정에 기술자료 임치제도 반영('08.12)

37) 대중소기업협력재단, 알기 쉽고 편리한 기술자료 임치제도, 2008, 14면.

이러한 문제는 비단 소프트웨어를 직접 설치하는 방식(On-Premise)에서만 발생하는 것은 아니다. 결국 서비스 중단에 따른 문제는 클라우드 컴퓨팅에서도 동일한 문제가 예상되어 지고 있으며, 일부 클라우드 업체에서는 자발적으로 임치제도를 변형·활용하여 해당 기술에 대한 안전성을 보장하고 있다.

지난 2006년 국내 중소기업인 D사는 클라우드의 일종인 ASP를 이용하여 "국내 레미콘 차량 위치관제 및 출하 관리" 서비스를 구축하고 제공하였다. 이 회사는 시장 확대를 위해 국내 대기업에 해당 서비스를 납품하려고 하였으나, 대기업은 중소기업인 D사의 파산·폐업 등에 대한 우려를 가지고 있었다. 만일 D사가 파산·폐업 등이 발생한다면 대기업은 해당 서비스를 전혀 제공받지 못하여 막대한 손실이 예상되었기 때문이었다. 이에 대기업인 S사의 서비스의 신뢰성을 위해 "국내 레미콘 차량 위치 관제 및 출하관리"에 관계되는 소스코드 및 일체의 기술에 대해 임치제도 이용을 요청하였다. 이는 D사가 파산을 하면 대기업은 해당 임치정보를 이용하여 동일한 시스템을 구축하여 지속적 서비스를 이용하기 위함이었다. 이에 D사와 대기업은 임치제도를 이용하여 해당 기술에 대한 신뢰성을 담보할 수 있었다.

그러나 이와 같은 사례는 일부 업체에서만 자체적으로 활용한 사례일 뿐, 대부분 업체가 인식부재와 비용에 대한 부담 등으로 기술임치를 적극 활용하지 못하고 있는 실정이다. 또한, 제도적으로도 직접 설치하는 방식(On-Premise)에 대한 기술임치를 고려하고 있을 뿐, 데이터가 서비스제공자의 원격 서버에 저장되어 제공되는 클라우드 컴퓨팅에 대한 고려는 이루어지지 못하고 있다. 이에 따라 사업자의 폐업이나 서비스 중단에 따른 데이터 유실 등의 문제는 여전히 해결해야 할 숙제로 남아있다.

다. 국내 클라우드 사업자의 데이터 백업조치 현황

국내 클라우드 사업자 중규모가 있는 기업의 경우에는 고객 데이터를 보호하기 위한 백업시스템이 중소사업자에 비해 상대적으로 잘 정비되어 있다. 현재 국내기업들을 대상으로 서비스를 제공 중인 세일즈포스닷컴(Salesforce.com)의 경우 미국에 3개의 IDC를 분산하여 설치하고 있다(샌프란시스코 인근에 주된 IDC를 두고, 다른 곳의 2개 IDC는 백업센터 및 DR(Disaster Recovery)센터로서의 역할). 세일즈포스 사는 모든 데이터를 실시간으로 미러링(mirroring)[38]하여 보관하고 있다. 따라서 고객이 데이터를 수정할 때마다 동일한

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

데이터가 다른 저장장치에 이중으로 보관되게 된다.[39] 이 회사는 미러링서비스를 통해 고객의 신뢰를 얻고 있으며 서비스 계약서에 데이터분산 보관에 관한 조항을 두고 있다[40].

또한, 세일즈포스닷컴(Salesforce.com)은 사용자(관리자)의 요청이 있는 경우 원하는 시간에 자신의 데이터를 백업 받을 수 있도록 하고 있다. 사용자로부터 백업 요청이 있으면 IDC에 있는 시스템 내부에서 자동으로 해당데이터의 백업이 수행되고 그 결과를 요청한 사용자에게 통보하게 된다. 그러면 사용자(관리자)는 자사의 정보를 자사에 있는 서버나 PC에 내려 받을 수 있게 된다. 그러나 이 작업은 한번 수행 되면 48시간이 지난 후에야 가능하므로 48시간 간격으로 수행될 수 있는 기능이다.

따라서 세일즈포스닷컴은 IDC차원에서 미러링을 통해 세일즈포스닷컴의 전체 데이터를 자동적으로 백업을 수행하고 있고, 또한 48시간 백업을 통해 사용자의 요청이 있는 경우 자동으로 사용자의 데이터에 한해 백업해주는 서비스를 제공하고 있다.

한편, 국내 클라우드서비스 기업의 고객 데이터 백업에 대한 다른 예를 보면 다음과 같다. 즉 백업주기는 일일백업(1일 1회 증가한 데이터에 대한 백업)과 주간백업(주 1회 전체 데이터 백업)로 하고 있으며, 백업준수율((백업실시건수/백업계획건수) *100)의 목표수준은 99% 이상이다. 시스템 장애 복구시간은 장애 발생 후 1시간 이내이며, 백업은 멀티태넌스 기술이 적용되고 있어서 고객사별 백업은 별도로 수행하지 않고, 전체 시스템 백업으로 수행하고 있다.

위에서 설명한 미러링(mirroring)의 경우 설비 · 장치 및 운용에 있어서 많은 비용이 요구되므로 국내 대부분의 중소 클라우드 사업자의 경우 차선책으로 디스크를 자기 테이프에 정기적으로 백업하는 형태로 고객 데이터를 보호하고 있다. 만일 1주 단위로 백업을 할 경우 백업을 하지 못하는 7일간은 데이터 손실의 위험에 노출되어 있게 된다. 현재 국내에선 클라우드 임치를 도입하기 위한 제도적 장치가 마련되어 있지 않은 상태이고, 또 중견 클라우드 사업자에 비해 중소 클라우드 컴퓨팅 서비스제공자들은 영세성으로 인해 이용자 데이터 보호를 위한 시스템 및 방안을 마련하지 못하고 있다. 따라서 중소 사업자의 경쟁력을 높이는 한편 이용자도 보호할 수 있는 대안이 마련될 필요가 있다.

---

39) 세일즈포스닷컴 http://blogs.salesforce.com/features/2006/03/mirrorforce.html (2009.11.20. 방문)

40) 세일즈포스사의 데이터보호 조항

SLA(Service Level Agreement) "5.3 Customer Data.

As between SFDC and Customer, Customer exclusively owns all rights, title and interest in and to all Customer Data. Customer Data is deemed Confidential Information under this Agreement. SFDC shall not access Customer's User accounts, including Customer Data, except to respond to service or technical problems or at Customer's request.

4. 서비스 중단방지 및 사용자 보호를 위한 법·제도 개선방안

클라우드 임치서비스(Cloud Escrow Service)는 클라우드 컴퓨팅 서비스의 중단 방지는 물론 사용자 데이터까지 실시간으로 보호해 줌으로써 클라우드 컴퓨팅 서비스의 단점을 보완할 수 있다. 그러나 현재 국내의 기술자료 임치제도로서는 소프트웨어 등 기술 자료만을 임치할 수 있을 뿐 사용자의 데이터를 실시간으로 백업하거나 서비스 중단 이후에도 당해 서비스를 일정기간 유지해 주는 서비스는 제공하지 못하고 있다. 특히 중견 서비스 사업자에 비해 영세한 중세 서비스제공자의 경우 이용자 데이터 보호를 위한 충분한 조치를 갖추고 있지 않으므로 인하여 데이터 손실이 반복적으로 발생할 경우에는 클라우드 컴퓨팅 서비스 자체에 대한 신뢰성에 훼손을 가져다 줄 수 있다.

이에 정부는 클라우드 컴퓨팅 사업자의 파산 등으로 인한 갑작스러운 서비스 중단으로부터 사용자를 보호하기 위한 제도적 지원방안을 모색할 필요가 있다. 그러나 클라우드 컴퓨팅 서비스의 중단 방지 및 이용자 보호를 위한 법제도 대응 방안에 있어서, 앞서 언급한 클라우드 임치제도를 클라우드 컴퓨팅 서비스제공자에게 의무화시키는 방안을 고려해 볼 수 있으나 아직 활성화되지 않은 클라우드 시장에서 중소 클라우드 사업자에게 이러한 의무부과는 현실적으로 큰 부담으로 작용할 수 있다. 따라서 정부가 클라우드 컴퓨팅 서비스 이용자를 보호하기 위한 지원환경을 마련해 주고 그러한 지원책을 중소사업자가 적극적으로 활용할 수 있도록 하는 방안이 바람직할 것이다.

가. "표준 SLA" 및 "클라우드 이용자보호지침" 마련

우선 서비스 제공자와 고객 간에 체결되는 계약서에 이용자의 데이터보호를 위한 일정한 법적 보호책(safeguard)을 마련하는 것이 중요하다. 통상 서비스 사업자는 재정적 부담 등으로 인하여 서비스이용약관에 사업자 일방에게 유리한 조항을 두는 경우가 많으므로 이용자 데이터 보호를 위한 충분한 조치를 규정하고 있지 않은 경우가 대부분이다. 국내 실정이 맞는 표준 클라우드 SLA의 제정은 클라우드 산업 활성화를 위해 전제되어야 할 요소이다.

또한 이용자를 보호하고 관련 시장의 건전한 발전을 위하여 클라우드 사업자의 자율적 준수를 유도할 수 있는 클라우드서비스 이용자 보호지침의 제정도 필요하다. 이를 위해서는 「소프트웨어산업 진흥법」 등 관련 법률에 표준 SLA 및 이용자보호지침 제정의 근거를 마련할 필요가 있다. 예컨대, 지식경제부장관으로 하여금 클라우드서비스의 건전한 거래 확

립과 이용자의 보호를 위하여 클라우드사업자의 자율적 준수를 유도하는 지침(“클라우드이용자보호지침”)을 관련 분야의 기관 및 단체의 의견을 들어 정할 수 있도록 하고, 또한 클라우드 컴퓨팅 서비스사업자는 서비스 시 이용자 보호를 위하여 데이터 손실, 과오금의 환불, 서비스 중단조치, 계약의 해지·해제 등으로 발생하는 이용자 피해보상 등의 내용이 포함된 표준약관을 마련하여 서비스이용자에게 명시하는 방안이 고려될 수 있다.

나. 표준 SLA를 통한 클라우드 임치제도 활성화 지원

특히 제정된 SLA가이드라인이나 이용자 보호지침을 통하여 클라우드 임치제도의 도입을 활성화시킬 필요가 있다. 그러나 중소기업이 대부분을 차지하는 국내 클라우드 컴퓨팅 산업에서 별도의 비용이 드는 임치제도의 도입이 어려우며, 이러한 서비스를 전문적으로 제공하는 사업자도 부재하다. 이에 정부는 소 서비스 사업자 중 경쟁력 있는 사업자를 선별하여 클라우드 산업을 육성할 수 있는 지원방안을 마련할 필요가 있다. 이를 위해 정부는 클라우드 지원센터(Cloud Service Center)를 설치하여 실시간 백업은 물론 보안서비스와 기술자료 임치서비스를 제공하고, 나아가 클라우드 컴퓨팅 서비스 중단 시에도 일정기간 동안 서비스를 유지해 줄 수 있는 지원체계를 마련할 필요가 있다.

다. 서비스 중단에 대한 통지의무 강화 및 안전장치 마련

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 규정하고 있다. 또한 2008년 12월 5일 공정거래위원회와 방송통신위원회는 주요 통신사업자의 인터넷 이용약관상의 불공정약관조항을 자진하여 수정 또는 삭제하도록 조치를 했는데, 이 중에는 시스템의 개선공사 등의 불가피한 사유로 서비스를 제공할 수 없는 경우 홈페이지 공지로 서비스를 중지할 수 있도록 허용하고 있다.

그러나 서비스 중단사실을 홈페이지 공지만으로 가능하게 한 것은 예측할 수 없는 피해를 유발할 수 있기 때문에 고객에게 부당하게 불리하다. 따라서 사업자가 클라우드 컴퓨팅 서비스를 중단하게 될 경우 그 사실을 이용자들이 알 수 있도록 통지를 의무화하되, 통지는 이용자들이 서비스 중단에 실질적으로 대비할 수 있도록 사업자가 인식하는 즉시 이루어져야 하며 그 방법과 내용이 명확하여야 할 것이다. 또한 중단의 기간과 피해보상 및 대책 등에 관한 내용도 통지에 포함되어야 할 것이다.

그러나 현실적으로 사업자가 파산하는 경우 의무를 수행하여야 하는 대상자체가 사라지게 되는 만큼 제도적으로 해결하는 데에는 한계가 존재한다. 따라서 사업자 파산 시 발생할 수 있는 사용자의 피해를 최소화 할 수 있는 안전장치를 마련해야 한다.

이와 관련하여 가장 중요한 부분 중 하나가 데이터의 즉시적인 이용이 가능하도록 하는 것이다. 원칙적으로는 사용자가 생성한 데이터의 권한은 이용자에게 있다. 그러나 클라우드 컴퓨팅 서비스사업자가 IDC의 서버를 임대하여 서비스를 제공하는 경우 IDC사업자로부터 서버에 저장되어 데이터를 즉시 넘겨받아 사용할 수 있어야 하나, 클라우드 컴퓨팅 사업자의 대한 채권을 확보하고 있는 IDC 입장에서는 자사의 서버나 그 안에 저장된 데이터를 즉시 이용가능 하도록 허용하기 어렵다. 그러나 사용자인 기업의 입장에서는 자사의 데이터를 즉시 이용하기 어려울 경우 기업운용에 심각한 어려움을 겪을 수 있다. 따라서 정부는 클라우드 컴퓨팅을 통해 생성되는 자료의 소유권과 이용권에 대한 사용자의 권한을 강화하고, 이를 즉시 이용할 수 있는 제도적 안전장치를 마련할 필요가 있다.

이와 관련하여 보험제도의 도입을 생각해 볼 수 있다. 미국 대부분의 클라우드 데이터 임치기관들은 임치물과 데이터 손실에 대비하여 높은 수준의 보험에 가입하고 있다. 그러나 우리나라의 경우 이러한 종류의 보험제도가 확립되어 있지 않다. 보험가입은 문제의 근본적인 해결책은 아니나 사후적 보완적으로 고려해 볼 수 있으며 표준 클라우드 SLA에 규정하는 것이 바람직할 것이다.

제 2 절 일시적 서비스 장애에 따른 사용자 보호방안

1. 클라우드 컴퓨팅 서비스 장애의 개념

클라우드 컴퓨팅 서비스는 웹 기반으로 컴퓨팅 자원을 저렴하게 빌려 쓰는 차세대 인터넷 서비스로, 클라우드 및 인터넷 서비스 장애의 개념에 대해 법률상으로 별도 정의하고 있지는 않다. 단 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정통망법)에서 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 정보통신서비스 제공자에 대한 원론적인 의무사항과 손해배상을 규정하고 있으며, 인터넷 서비스의 품질 향상 및 안정적 제공 보장을 위하여 인터넷 서비스 품질의 측정 · 평가 및 사용자 안내를 할 수 있도록 되어 있는 수준이다.

〈표 3-3〉 정보통신망 이용촉진 및 정보보호 등에 관한 법률

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
3. “정보통신서비스 제공자”란 「전기통신사업법」 제2조제1항 제1호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

제3조(정보통신서비스 제공자 및 사용자의 책무) ① 정보통신서비스 제공자는 사용자의 개인정보를 보호하고 건전하고 안전한 정보통신서비스를 제공하여 사용자의 권익보호와 정보이용능력의 향상에 이바지하여야 한다.

제15조(인터넷 서비스의 품질 개선) ① 지식경제부장관은 인터넷 서비스 사용자의 권익을 보호하고 인터넷 서비스의 품질 향상 및 안정적 제공을 보장하기 위한 시책을 마련하여야 한다.
② 지식경제부장관은 제1항에 따른 시책을 추진하기 위하여 필요하면 정보통신서비스 제공자단체 및 사용자단체 등의 의견을 들어 인터넷 서비스 품질의 측정 · 평가에 관한 기준을 정하여 고시할 수 있다.
③ 정보통신서비스 제공자는 제2항에 따른 기준에 따라 자율적으로 인터넷 서비스의 품질 현황을 평가하여 그 결과를 사용자에게 알려줄 수 있다.

제32조 (손해배상) 사용자는 정보통신서비스 제공자등이 이장의 규정을 위반한 행위로 손해를 입으면 그 정보통신서비스 제공자등에게 손해배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

제46조 (집적된 정보통신시설의 보호) ① 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.
② 집적정보통신시설 사업자는 집적된 정보통신시설의 멸실, 훼손, 그 밖의 운영 장애로 발생한 피해를 보상하기 위하여 대통령령으로 정하는 바에 따라 보험에 가입하여야 한다.

정통망법에 의거하여 정보통신서비스 제공자는 이용(또는 서비스)약관을 통해 서비스 장애의 범위와 이에 따른 손해배상 규정을 세부적으로 명기하고 있으며, 이러한 관련 법률 및 주요 정보통신서비스 제공자의 이용약관 등을 토대로 볼 때 클라우드 컴퓨팅 서비스 장애란 ‘서비스 제공자의 귀책사유로 인해 사용자가 일정시간(2시간 또는 4시간) 이상 서비스를 제공받지 못하는 것’을 의미한다고 볼 수 있을 것이다. 또한 정통망법에 의하면 이러한 장애 발생 시 정보통신서비스 제공자는 서비스 장애에 따른 사용자의 피해를 보상할 의무를 지니고 있다.

〈표 3-4〉 연관 인터넷 서비스의 장애 범위

o 초고속 인터넷 서비스 : **서비스 제공자의 귀책사유**로 인해 서비스 제공이 **3시간 이상(사용자의 인지·통보 후) 중단된 경우**에 손해배상 규정을 이용약관에 명기 o 웹 하드 서비스 : **서비스 제공자의 귀책사유**로 인해 서비스 제공이 **2시간 이상(사용자의 인지·통보 후) 중단된 경우**에 손해배상 규정을 이용약관에 명기 o IDC 서비스 : **서비스 제공자의 귀책사유**로 인해 서비스 제공이 **4시간 이상(사용자의 인지·통보 후) 중단된 경우**에 손해배상 규정을 이용약관에 명기 o 인터넷 포털 서비스 - 네이버 : **손해배상 규정 없음** - 다 음 : 서비스 제공자의 귀책사유로 인해 **유료 서비스 중단 및 제공하지 못한 경우 이용요금 환불** 규정을 이용약관에 명기

클라우드 컴퓨팅 서비스 장애는 인터넷 서비스와 마찬가지로 인터넷(회선), 시스템 에러·교체, 바이러스 감염, 침해사고 등 여러 가지 요인에 의해 발생 가능하며, 언제라도 일어날 수 있는 개연성을 내포하고 있다. 그러나 중요한 것은 클라우드 컴퓨팅 서비스의 경우, 사용자의 정보를 서비스 제공자의 서버에 올려놓고 컴퓨팅 자원을 빌려 쓰는 서비스로서, 서비스 장애에 따른 정보 유실 및 비즈니스 적 손실의 규모는 기존 인터넷 서비스와 비교하여 커질 것으로 추정된다. 또한 클라우드 컴퓨팅 서비스는 인프라스트럭처, 미들웨어 플랫폼, 소프트웨어 및 애플리케이션 등까지 포괄하는 서비스로, 단일 사업자 또는 복수 사업자가 서비스 제공에 참여가능하기 때문에 서비스 장애에 따른 손해배상의 귀책에 대한 분쟁이 일어날 소지가 클 것이다.

따라서 이러한 클라우드 컴퓨팅 서비스의 특성을 감안하여 특화된 사용자 보호방안 강구를 위한 선제적인 관련 법제 정비가 필요하며, 간과해서는 안 될 것이 사용자 보호방안과 더불어 클라우드 컴퓨팅 서비스 도입 촉진 및 활성화를 위한 서비스 제공자 및 도입자 측면의 유인책도 강구되어야 할 것이다.

2. 클라우드 컴퓨팅 서비스의 장애 사례

클라우드 컴퓨팅 서비스 장애는 인터넷(회선), 시스템 에러·교체, 바이러스 감염, 침해사고 등 다양한 요인에 의해서 발생할 수 있다. 이 중에서 인터넷(회선) 문제에 따른 서비

스 장애는 클라우드 컴퓨팅 서비스 제공자의 귀책사유로 보기에는 무리가 있는 관계로 본고에서는 시스템 고장 및 교체에 따른 장애와 바이러스 감염 및 침해사고 등에 따른 장애 등 두 가지사례에 대해서 고찰하고자 한다.

가. 시스템(장비) 에러 및 교체에 따른 서비스 장애 사례

최근에 발생된 클라우드 컴퓨팅 서비스의 장애사례는 대부분 시스템(장비)의 에러 또는 교체에 의한 것으로, 구글 G-메일의 반복되는 장애, 윈도우 애저 테스트버전 다운, 아마존 S3 서비스 장애 및 MS 사이드킥 서비스 중단 등이 대표적이다.

〈표 3-5〉 클라우드 컴퓨팅 서비스 장애 사례

구 분	주요 내용
구글 지메일의 반복되는 장애	o 2009년 9월 24일, 2시간 장애 발생(9월 중 2번째 서비스 중단 사태) o 고객 대상 무료 서비스로 보상·배상 요구 없음 o 발생원인 : 라우팅 에러부터 서버 유지 보수 문제 등 다양한 원인으로 추정
아마존 S3 서비스 일시 중단	o 2008년 여름, 7~8시간 장애 발생 o 2008년 초, 인증요청의 쇄도로 인한 서비스 중단 등
세일즈포스닷컴 서비스 장애	o 2009년 1월 6일 1시간 동안 서비스 중단 o 발생원인 : 코어 네트워크 장비의 메모리 배치 에러
MS 사이드킥 서비스 중단	o 2009년 10월 12일 MS가 미국 이동통신사 T모바일 USA를 통해 제공하던 스마트폰 서비스 사이트 킥에서 대규모 데이터 손실 및 접속장애 발생으로 서비스 중단 o 사이드킥 사용자의 개인정보(연락처, 일정, 사진 등) 유실로 법원에 소송 중 o 발생원인 : 사이드킥의 MS 서버 오류 추정(상세 원인 불명)
윈도우 애저 테스트 버전다운	o 2009년 3월 클라우드 컴퓨팅 네트워크인 윈도우 애저, 테스트 과정 중 중단 사고 발생 o 발생원인 : 원인 불명

1) 구글 G-메일의 반복되는 장애

G-메일은 구글에서 제공하는 SaaS(Software as a Service) 방식의 대표적인 클라우드 컴퓨팅 서비스로, 일정관리·웹오피스 등 Google Apps와의 완벽한 호환과 대용량 등의 장점으로 급성장하고 있다. 그런데 2009년 9월 24일부터 26일까지 구글 지메일에 부분적인 장애가 발생하였다. 이번 사고는 2월에 이어 2번째 발생된 서비스 장애로, Google

Apps Status Dashboard[41]를 통해 확인되었다. 장애 원인으로는 유럽에 있는 데이터센터에서 정기적인 서버 정비 작업에서 한 지역의 서버로 데이터를 이동시키는 중 코드에 예기치 못한 에러(라우팅 에러)가 발생하여 주변 데이터센터까지 과부하를 일으킨 것이라 해명하였지만, 세부적인 원인에 대해서는 아직까지 규명하지 못하고 있는 실정이다.

구글 측은 서비스 장애 발생 후 1시간 만에 시스템 정상화 시켰으며, 이로 인해 서비스 이용을 하지 못한 유료(Premier Edition) 사용자에 한해서 Google Apps Service Level Agreement에 의거 보상하였다. 이메일은 기업 사용자에게 미션 크리티컬한 애플리케이션으로, 만약 지메일이 신뢰성을 잃게 되면 기업 사용자은 지메일 사용을 꺼리게 되고 이는 구글이 서비스하는 다른 클라우드 컴퓨팅 서비스에도 영향을 미칠 것이다. 이러한 우려로 인해 구글 내부에서도 상용 이메일 서비스와 일반 사용자 이메일 인프라를 구분하자는 요구까지 있을 정도이다.

〈그림 3-6〉 Google Apps Status Dashboard

Google Apps Status Dashboard

이 페이지에는 Google 애플리케이션 서비스의 성능 정보가 표시됩니다. 따로 언급되지 않은 경우 이 상태 정보는 Google 애플리케이션을 사용하는 기업용 서비스뿐만 아니라 일반 서비스에도 적용됩니다.

언제든지 아래에 나열된 서비스의 현재 상태를 여기에서 확인할 수 있습니다. 다른 정보를 보거나 문제를 신고하려면 Google 애플리케이션 도움말 센터를 방문하세요.

	오늘의 상태	09. 9. 26.	09. 9. 25.	09. 9. 24.	09. 9. 23.	09. 9. 22.	09. 9. 21.
Gmail	✔ 문제 없음	❶	❶	❶	✔	✔	✔
Google 캘린더	✔ 문제 없음	✔	✔	✔	✔	✔	✔
Google 토크	✔ 문제 없음	✔	✔	✔	✔	✔	✔
Google 문서 목록	✔ 문제 없음	✔	✔	✔	✔	✔	✔
Google 문서	✔ 문제 없음	✔	✔	✔	✔	✔	✔
Google 스프레드시트	✔ 문제 없음	✔	✔	✔	✔	✔	✔
Google 프리젠테이션	✔ 문제 없음	✔	✔	✔	✔	✔	✔
Google 사이트 도구	✔ 문제 없음	✔	✔	✔	✔	✔	✔
Google Video for business	✔ 문제 없음	✔	✔	✔	✔	✔	✔
관리자 제어판	✔ 문제 없음	✔	✔	✔	✔	✔	✔

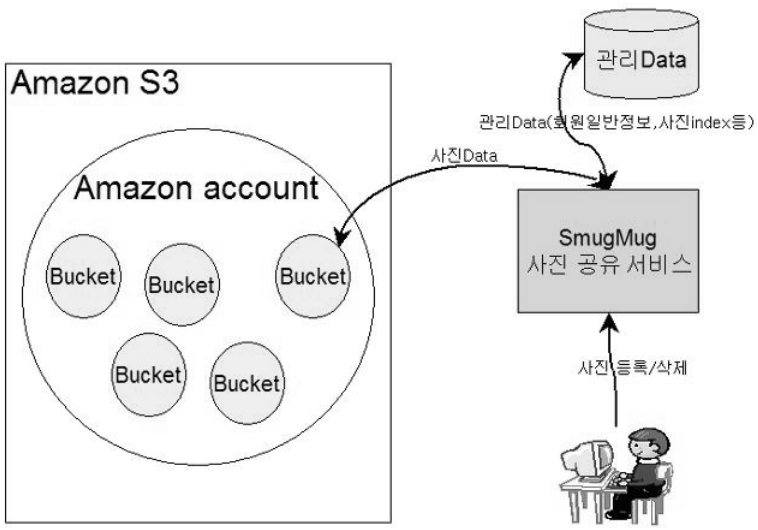
2) 아마존 S3 서비스 일시 중단 사례

아마존 S3(Simple Storage Service)은 데이터 저장 및 검색 기능을 갖춘 가상화된 스토리지를 웹 기반으로 제공하는 대표적인 클라우드 인프라(IaaS : Infrastructure as a Service) 서비스로, 데이터 유형에 관계없이 인터넷을 통해 어디서나 데이터 저장 및 액세

41) Google Apps(메일, 캘린더, 인스턴트 메신저, 문서 도구 등)에 대한 서비스 상태를 실시간으로 모니터링 하는 서비스

스가 가능하며 최소한의 중단 시간으로 또는 중단 시간 없이 매우 빠르게 시스템을 복구할 수 있도록 설계되었다.

〈그림 3-7〉 Amazon S3 활용 예시도



※ Bucket : 데이터 저장 단위

그러나 이러한 내결함성을 지닌 S3이었지만, 지난 2008년 2월 15일 오전 05시부터 09시까지 아마존의 S3 서비스가 다운되는 사고가 발생하였다. 사고 당시 아마존 S3 서비스를 통해 웹 호스팅 서비스를 이용하는 고객 33만 명이 해당 시간 동안 서비스를 이용하지 못하였으며, 수천 개의 중소기업이나 개발자들이 큰 피해를 입은 것으로 추정되었다.

동 사고의 원인에 대해서 아마존(웹서비스 팀)은 일부 사용자들의 과도한 인증 요청으로 인한 서버 과부하가 최종 원인이라고 해명하였고, 피해를 입은 사용자에게는 Amazon S3 SLA(Service Level Agreement)에 명시된 Service Credit에 의거해 보상하였다.

3) 기타 장애 사례

전 세계 6만여 개 회사를 대상으로 온라인 CRM 서비스를 제공하는 세일즈포스닷컴의 경우 2009년 1월 6일 코어 네트워크 장치의 메모리 할당 오류로 인해 온라인 CRM 서비스가 한 시간 동안 중단되는 장애가 발생하였다. 기업 대상으로 다양한 호스팅 및 클라우드 컴퓨팅 서비스를 제공하는 랙스페이스는 2009년 6월 29일 데이터센터 발전기 고장으로

인해 정전 및 고객 서버가 수 시간 다운되는 사례가 발생하여 고객들에게 250~350만 달러를 손해배상 해야 했다.

MS의 대표적인 클라우드 개발환경 서비스(PaaS : Platform as a Service)인 윈도우 애저가 지난 2009년 3월 중단되는 장애가 발생했다. 장애 원인은 규명되지 않았으며, 테스트 과정에서 발생한 장애로 사용자 대상의 손해배상은 이뤄지지 않았다.

2009년 8월에 이베이의 페이팔 온라인 지불결제 시스템이 네트워크 하드웨어 에러로 인해 2시간 정도 장애를 일으키면서 수백만 명의 고객이 거래를 마무리하지 못하는 사례가 발생하였다. 이로 인해 페이팔은 수백만 달러의 손실을 입은 것으로 추정되며, 거래업체에게 손해배상 규모에 대해서는 밝혀지지 않았다.

클라우드 컴퓨팅 서비스라고 할 수는 없지만 기존 인터넷 서비스에서도 시스템(장비) 에러 등에 의한 장애 사례를 살펴 볼 수 있으며, 2007년 8월 7일 LG데이콤과 LG파워콤의 초고속 인터넷망에 오류가 발생하여 1시간 여 동안 서비스가 중단된 사례가 대표적이다. 장애의 주요 원인은 라우터 장비의 일시적인 동작 오류(전송장치인 라우터 장치의 CPU 점유율이 순간적으로 높아지면서 속도 저하, 즉 CPU가 감당할 수 있는 처리 능력 한계치 도달, 제 속도를 감당 못함)였으며, 해당 서비스 제공자는 시스템을 재부팅한 후에야 서비스를 복구할 수 있었다.

나. 바이러스 감염 및 침해 사고 등에 의한 클라우드 컴퓨팅 서비스 장애

클라우드 컴퓨팅 서비스에 대한 장애는 주로 시스템(장비) 에러 및 교체 등에 의한 것으로 바이러스 감염 및 침해사고 등에 따른 클라우드 컴퓨팅 서비스 장애 사례는 아직 많지 않으며, 2009년 8월 초 분산서비스거부(DDoS)[42] 공격으로 인해 2시간 동안 홈페이지 접속이 되지 않아 서비스가 중단된 트위터(Twitter) 사례가 대표적이다.

이는 클라우드 컴퓨팅 서비스가 아직 활성화되지 않았기 때문인 것으로 사료되며, 모든 정보가 한 곳에 집중화 되는 서비스 특성상 클라우드 컴퓨팅 서비스가 본격적으로 확산되면 많은 해커들의 주 타겟이 될 것으로 예상된다.

최근 인터넷 서비스 사고는 「7 · 7 DDoS(분산서비스 거부) 공격」피해 사례처럼 다양한 방법으로 홈페이지 접속 장애 및 개인 정보 유출 등 인터넷 서비스의 취약점을 이용 특정 사이트를 공격, 금전을 요구하는 형태로 지능화되고 있는 추세로, 클라우드 컴퓨팅 서비스

42) 여러 대의 공격자를 분산 배치하여 동시에 '서비스 거부 공격(Denial of Service attack ; DoS)'을 함으로써 시스템이 더 이상 정상적 서비스를 제공할 수 없도록 만드는 해킹 방식

에서도 이에 대한 대응방안 강구가 필요하다.

2009년 7월 7일부터 9일까지 3차에 걸쳐 DDoS 형태로 국내외 사이트를 공격해 인터넷 접속 장애를 일으킨 중대 장애 사례가 발생하였다. 청와대, 국회, 국가정보원, 안철수연구소, 행정안전부, 조선일보, 국민은행 및 백악관 등 국내외 주요 핵심 인터넷 사이트를 공격하여 대량의 유해 트래픽을 발생시켜 접속 지연 및 서비스 장애를 유발하였다.

이에 대해 정부에서는 DDoS 공격 탐지 후 대국민 주의경보를 발령하고 악성코드 유포 사이트로 추정되는 101개 사이트를 차단하였으며, 한국인터넷진흥원(KISA)-ISP-백신개발기업 등 민·관 협력을 통해 감염 PC 추적 및 백신을 처방하는 등 발 빠른 조치를 취하였다. 그러나 악성코드에 감염된 IP가 약 11만 여 대, 악성코드에 의한 PC 손상 피해접수는 총 1,353건에 달하는 등 적지 않은 피해를 감수해야 했으며, 이외에도 국내외 DDoS로 인한 피해 사례는 〈표 3-6〉와 같다.

〈표 3-6〉 국내외 DDoS 공격 피해 사례

구분	일시	피해자	세부 내용	비고
국내	'06.11월	국내 화상채팅 업체	o 업체 서비스 중단 o ISP 백본, 국제회선 부하 증가	금품요구
	'07.10월	게임아이템 거래업체	o 홈페이지 접속장애(수~15Gbps 트래픽)	금품요구
	'08.2월	O게임	o 동남아 쪽으로부터 공격을 받아 사이트 일시적 폐쇄	국외→국내
	'08.3월	O증권 사이트	o 협박성 DDoS 공격(중국해커) o 해당 사이트 접속장애 발생	금품요구
	'08.6월	국내 O당 홈페이지	o 홈페이지 접속장애	
	'08.7월	국내 포털 사이트 카페	o 카페에서 탈퇴당한 10대 내국인이 중국 사이트에서 공격 툴을 구입 후 보복공격	보복성
	'08.12월	반크 홈페이지 공격	o 일본 네티즌의 공격 홈페이지 접속장애	국외→국내

〈표 3-6〉 국내외 DDoS 공격 피해 사례(계속)

구분	일시	피해자	세부 내용	비고
해외	'09.3월	디카 커뮤니티 O	o 홈페이지 접속장애	금품요구
	'06.12월	폴란드 특정 서버 공격	o 전체 ISP에 걸쳐 산발적으로 발생하고, 국내 인터넷에도 지연현상 발생	국내→국외
	'07.2월	Root DNS 서버	o 13개 루트DNS 중 6개가 공격 받음	
	'07.4월	에스토니아 정부, 의회 등 주요 사이트	o 러시아 해커에 의해 약 2주간의 공격으로 피해 사이트 접속불능	국가 사이버전
	'07.9월	전자지불홈페이지 www.e-gold.com (미국)	o Virus 감염PC가 C&C로 부터 악성코드 다운로드후 공격	
	'08.8월	그루지야 국방부, 외교부 등 주요 정부사이트	o 러시아 해커들에 의해 그루지야 국방부, 외교부 등 주요 사이트가 공격을 받음	국가 사이버전
	'09.1월	키르기즈스탄 ISP	o 러시아 해커에 의해 해당국의 인터넷 마비	국가 사이버전

※ 출처 : 방송통신위원회 보도자료(2009.7.8)

클라우드 컴퓨팅 서비스의 경우 해커 및 기타 서비스 장애를 유발 할 수 있는 다양한 침해 원인에 대해서 장시간 또는 장기간 서비스 장애를 유발 시켰을 경우, 서비스를 이용하는 기업 및 개인 사용자들이 클라우드 컴퓨팅 서비스 사업자로부터 가상의 공간에 저장해 둔 주요 데이터를 서비스 중지로 인해 이용할 수 없는 사태가 발생 될 수 있다.

최근 미국, 영국, 일본, 중국 등 클라우드 컴퓨팅 서비스를 국가 정책적으로 추진해 나가고 있는 만큼 서비스 장애로 인한 데이터 사용이 용이하지 못할 경우 국가적으로 비상사태 문제로까지 이어질 수 있는 개연성이 매우 크며, 클라우드 컴퓨팅 서비스가 활성화 되고 이용자가 확대될수록 그 피해는 더 커진다.

국내에서는 클라우드 컴퓨팅 서비스 활성화를 위해 지식경제부, 방송통신위원회, 행정안전부 등 관련 국책연구기관 등 IT서비스 사업자 및 관련 분야 사업들이 노력을 기울이고 있는 만큼, 클라우드 컴퓨팅 서비스 장애 방지를 위한 국가차원의 구체적이고 종합적인 대응방안 마련이 시급하다.

3. 현행 법제도상의 서비스 사용자 보호 장치

가. 국내 인터넷 서비스 사업자의 사용자 보호 장치

현재 클라우드 컴퓨팅 서비스를 포함한 인터넷 서비스 장애에 따른 사용자 보호 및 손해배상에 대해서는 관련법과 정보통신서비스 제공자의 이용(서비스)약관을 통해 규정하고 있다. 전기통신사업법 제29조 제5항에서는 별정통신사업자 또는 부가통신사업자에게 서비스 이용약관을 방송통신위원회에 신고하도록 의무를 부과하고 있다[43]. 이는 부가통신사업자의 이용약관상에 불공정한 조항이 있는지를 심사하기 위한 것으로 이용자보호를 위한 규정이다.

이에 따르면 인프라 서비스를 제공하는 사업자나 이를 이용하여 서비스를 제공하는 별정통신, 혹은 부가통신 사업자는 방송통신위원회에 약관을 제출하여 심의를 받아야 한다. 그러나 현재 클라우드 컴퓨팅 서비스에서 이용자 데이터 보호를 위한 합리적인 조치나 절차에 관한 법적 기준이나 가이드라인 등이 없고, 또 기술적인 지원환경이 구축되지 않은 상태이다.

또한 동법 제33조에 의하면 이용자보호를 위한 조항으로 이용자의 의견 또는 불만의 처리와 그 원인이 되는 사유의 발생과 이의 처리지연에 따른 손해의 배상에 관해 규정하고 있다[44]. 이러한 조항에 따라 초고속인터넷 서비스나 IDC, 웹하드 등의 서비스를 제공하는 사업자들은 손해배상과 관련한 이용약관을 통해 피해보상의무를 지고 있다. 그러나 서비스 약관을 신고하고 피해보상의 의무를 지는 사업자는 법에서 정한 일정규모 이상의 정보통신서비스 제공자로 한정되어 있어 새로운 컴퓨팅 서비스인 클라우드 컴퓨팅을 포괄적으로 포함하지는 못하고 있다.

또한 지금까지 업무보조수단으로서 활용되었던 인터넷이나 웹하드, IDC등을 넘어 기업 전

43) '전기통신사업법' 상 이용약관 신고의무 조항 - 제29조 (이용약관의 신고 등)
① 기간통신사업자는 그가 제공하고자 하는 전기통신역무에 관하여 그 역무별로 요금 및 이용조건(이하 "이용약관"이라 한다)을 정하여 방송통신위원회에 신고(변경신고를 포함한다)하여야 한다. 다만, 사업규모 및 시장점유율 등이 대통령령으로 정하는 기준에 해당하는 기간통신역무의 경우에는 방송통신위원회의 인가(변경인가를 포함한다)를 받아야 한다.
⑤ 별정통신사업자 또는 부가통신사업자가 기간통신사업자의 전기통신회선설비를 이용하는 경우에 그 전기통신회선설비의 이용에 대하여는 제1항의 규정에 의한 이용약관을 적용한다.

44) '전기통신사업법' 상 사용자 불만처리 의무조항 - 제33조 (이용자 보호)
① 삭제 〈1999.5.24〉
② 전기통신사업자는 전기통신역무에 관하여 이용자로부터 제기되는 정당한 의견이나 불만을 즉시 처리하여야 한다. 이 경우 즉시 처리가 곤란한 경우에는 이용자에게 그 사유와 처리일정을 통보하여야 한다.
③ 제2항의 규정에 의한 의견 또는 불만의 원인이 되는 사유의 발생과 이의 처리지연에 따른 손해의 배상은 제33조의2의 규정에 의한다.

체의 프로세스를 지원하는 토털 IT인프라 아웃소싱의 형태의 클라우드 컴퓨팅이 가지는 산업적인 파급효과를 고려할 때 현재의 피해보상의 수준에 대한 적정성도 논란이 되고 있다.

〈표 3-7〉 인터넷 서비스별 손해배상 관련 이용(서비스)약관 비교

구분	관련 약관	비고
초고속 인터넷 서비스	회사는 이용고객이 서비스를 이용하지 못하여 그 사실을 회사에 통보한 때로부터(또는 그전에 회사가 그 사실을 알게 된 때에는 그때로부터) 계속 **3시간 이상 서비스가 중지되는 경우** 및 월별(매월 1일부터 말이 기준) 서비스 장애 발생 **누적 시간이 12시간을 초과할 경우**에는 서비스 이용료를 포함한 최근 3개월(3개월 미만인 경우는 해당기간 적용)의 **1일 평균요금을 24로 나눈 요금에 서비스 제공 중지시간을 곱하여 산출한 금액의 3배를 이용고객과 협의하여 배상**합니다. 이 경우 단수가 1시간 미만인 경우에는 1시간으로 합니다.	QooK (제28조) · XPEED (제35조) · SK브로드밴드 인터넷 (제27조) 약관
	③ OO은 OOO 인터넷 이용고객의 고장복구 소요시간이 **고장접수 후 24시간을 초과하는 경우 초과시간에 따라 시간당 정액요금의 10배를 1월 정액요금 한도 내에서 이용고객에게 배상**합니다. 단, 서비스 장애가 제1항의 각호에 해당하는 경우와 다음 중 하나에 해당하는 경우에는 배상하지 아니합니다. 1. 산간오지, 도서 등 OO 유지보수 직원이 상주하지 않는 지역 2. 제1항에 의해 기 배상받은 경우	QooK 인터넷 서비스 제28조 (손해배상)
웹하드 서비스	1. OOO의 귀책사유로 고객이 서비스를 이용하지 못하는 경우, OOO은 이에 대한 손해배상을 합니다. 다만 고객이 서비스 이용불가 사실을 OOO에 접수한 이후 **2시간 이내 서비스가 정상화된 경우는 제외**합니다. 2. OOO의 귀책사유로 고객이 서비스를 이용하지 못하는 경우에는 고객이 그 사실을 OOO에 통보하여 확인한 때(그 전에 OOO이 그 사실을 알았거나 알 수 있게 된 때)로부터 계속 **2시간 이상의 서비스 제공 중지** 시간에 대하여 최근 3개월(3개월 미만인 경우에는 해당기간 적용)의 **1일 평균요금에 서비스 제공 중지 시간을 24로 나눈 수를 곱하여 산출한 금액의 3배를 배상**합니다. 이 경우 단수가 1시간 미만인 경우에는 1시간으로 합니다.	LG데이콤 제22조 (손해배상범위)

〈표 3-7〉 인터넷 서비스별 손해배상 관련 이용(서비스)약관 비교(계속)

구분	관련 약관	비고
IDC 서비스	2. 회사의 귀책사유로 고객이 서비스를 이용하지 못하는 경우 고객이 그 사실을 회사에 통보하여 확인한때 또는 회사가 그 사실을 알았거나 알 수 있었을 때로부터 기산하여 계속 **4시간 이상의 서비스 제공 중단** 시간에 대해 배상합니다. 3. 제2항의 손해배상금액은 고객이 청구 받은 최근 3개월분(3개월 미만인 경우에는 해당기간 적용) 요금의 **일 평균액을 24로 나눈 시간당 평균액**에 이용하지 못한 시간수를 곱하여 **산출한 금액의 3배**를 고객과 협의하여 배상합니다. 이 경우, 이용하지 못한 시간이 1시간미만의 경우에는 1시간으로 봅니다.	SK브로드밴드 제49조 (손해배상)

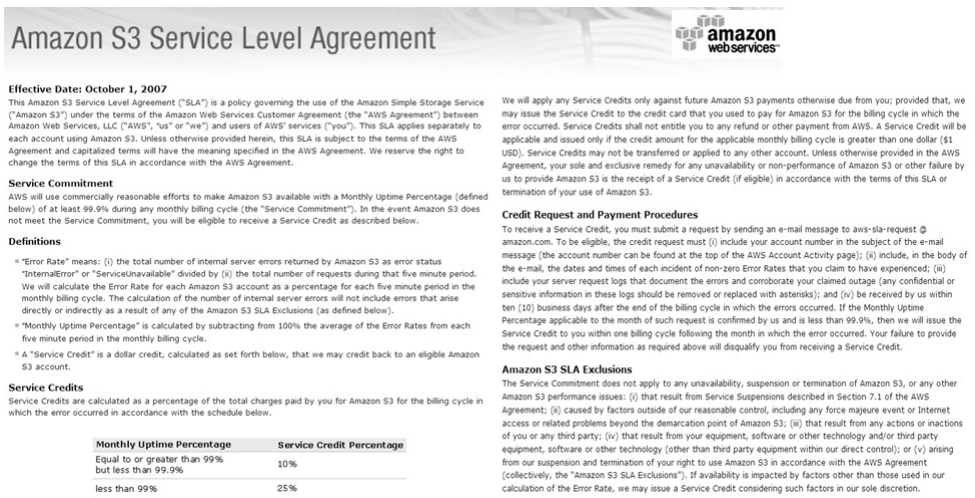
나. 해외 클라우드 컴퓨팅 서비스 사업자의 사용자 보호 장치

미국 등 해외의 경우도 국내와 마찬가지로 아직 초기시장인 클라우드 컴퓨팅에 대하여 사용자를 보호하는 법·제도는 미비하다. 그러나 클라우드 컴퓨팅 사업자들은 서비스 장애에 대한 고객들의 우려를 불식시키기 위하여 자체적으로 세부적인 서비스 품질기준을 마련하여 적용하고 있다.

세일즈포스닷컴, 구글, 아마존, MS 등 대부분의 사업자들은 이용약관 내 구체적인 SLA (Service Level Agreement)를 만들어 공개하고, 이를 통해 사용자의 서비스 선택권을 보장하고 있으며, 서비스 가용률을 핵심으로 서비스 품질을 보장하고 있다. 이와 함께 우수한 기술력을 바탕으로 지속적인 서비스 업그레이드 및 철저한 서비스 관리 정책을 병행하여 추진 중이다.

아마존은 S3, EC2, SimpleDB 등 클라우드 컴퓨팅 서비스 사용자에 대해 SLA상에 Service uptime 99.99%를 유지할 것을 홈페이지에 명시하고 있으며 서비스 중단 발생 시에는 중단시간(downtime)을 계산하여 Service Uptime 비율에 해당하는 Service Credit Percentage를 적용하여 가용률 기반으로 지역, 사용량에 따라 차등적으로 〈그림 3-8〉과 같이 보상하고 있다.

〈그림 3-8〉 Amazon S3 Service Level Agreement



Amazon S3 Service Level Agreement

amazon web services

Effective Date: October 1, 2007

This Amazon S3 Service Level Agreement ("SLA") is a policy governing the use of the Amazon Simple Storage Service ("Amazon S3") under the terms of the Amazon Web Services Customer Agreement (the "AWS Agreement") between Amazon Web Services, LLC ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account using Amazon S3. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon S3 available with a Monthly Uptime Percentage (defined below) of at least 99.9% during any monthly billing cycle (the "Service Commitment"). In the event Amazon S3 does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "Error Rate" means: (i) the total number of internal server errors returned by Amazon S3 as error status "InternalError" or "ServiceUnavailable" divided by (ii) the total number of requests during that five minute period. We will calculate the Error Rate for each Amazon S3 account as a percentage for each five minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon S3 SLA Exclusions (as defined below).
- "Monthly Uptime Percentage" is calculated by subtracting from 100% the average of the Error Rates from each five minute period in the monthly billing cycle.
- A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon S3 account.

Service Credits

Service Credits are calculated as a percentage of the total charges paid by you for Amazon S3 for the billing cycle in which the error occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 99% but less than 99.9%	10%
less than 99%	25%

We will apply any Service Credits only against future Amazon S3 payments otherwise due from you; provided that, we may issue the Service Credit to the credit card that you used to pay for Amazon S3 for the billing cycle in which the error occurred. Service Credits shall not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability or non-performance of Amazon S3 or other failure by us to provide Amazon S3 is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA or termination of your use of Amazon S3.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a request by sending an e-mail message to aws-sla-request @ amazon.com. To be eligible, the credit request must (i) include your account number in the subject of the e-mail message (the account number can be found at the top of the AWS Account Activity page); (ii) include, in the body of the e-mail, the dates and times of each incident of non-zero Error Rates that you claim to have experienced; (iii) include your server request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks); and (iv) be received by us within ten (10) business days after the end of the billing cycle in which the errors occurred. If the Monthly Uptime Percentage applicable to the month of such request is confirmed by us and is less than 99.9%, then we will issue the Service Credit to you within one billing cycle following the month in which the error occurred. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon S3 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon S3, or any other Amazon S3 performance issues: (i) that result from Service Suspensions described in Section 7.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon S3; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (v) arising from our suspension and termination of your right to use Amazon S3 in accordance with the AWS Agreement (collectively, the "Amazon S3 SLA Exclusions"). If availability is impacted by factors other than those used in our calculation of the Error Rate, we may issue a Service Credit considering such factors in our sole discretion.

출처 : http://aws.amazon.com/s3-sla(2009.12

〈표 3-8〉 아마존 S3 SLA Service Credit

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 99 % but less than 99.9 %	10 %
less than 99 %	25 %

구글의 경우는 구글 Apps Premier Edition 유료 사용자에 한정하여 Google Apps Service Level Agreement에 Service Credit 보상 기준을 〈표 3-9〉와 같이 명시하고 있으며 서비스 장애 발생 시 가용률을 기반으로 사용료의 일정비율을 보상하고 있다.

〈표 3-9〉 구글 Apps SLA Service Credit

Monthly Uptime Percentage	Days of Service added to the end of the Service term, at no charge to Customer
〈 99.9 % - ≥ 99.0 %	3 %
〈 99.0 % - ≥ 95.0 %	7 %
〈 95.0 %	15 %

이처럼 클라우드 컴퓨팅 사업자들은 자체적인 SLA기준을 마련하여 공개하고 있으며, 고객들이 서비스 장애 발생 여부를 실시간 적으로 모니터링 할 수 있는 모니터링 시스템을 제공함으로써 서비스에 대한 고객들의 신뢰확보에 주력하고 있다.

그러나 아직 상용화된 클라우드 컴퓨팅 서비스가 부족하고 영세한 사업자들이 많은 우리나라의 경우 아직 SLA에 대한 개념이 취약하고, 실시간 모니터링 체계 등 고객들의 신뢰확보를 위한 사업자들의 노력도 부족한 상황이다.

4. 현행 법제도상의 문제점

클라우드 컴퓨팅 서비스를 포함한 인터넷 서비스 장애 시 서비스 제공자의 귀책사유로 인해 피해를 입은 사용자는 정보통신사업법 및 정통망법에 근거하여 정보통신망 사업자별 이용(서비스)약관에 의거 보호 및 보상을 받을 수 있게 된다. 그러나 클라우드 컴퓨팅 서비스의 특성을 감안 시 포괄적으로 적용하기에는 현행 법체계에서 다루고 있는 사업자의 범위가 제한적이며, 손해배상 범위 및 규모, 사업자의 면책 범위 등과 관련 다소의 문제점을 내재하고 있다. 또한 정통망법에서는 서비스 중단 및 제한의 기준을 외부로부터의 침해사고로 규정하고 있어 클라우드 컴퓨팅 서비스 사업자와 이용자에게 불리하게 작용 될 수 있다.

가. 전기통신사업법상에서의 문제점

전기통신사업법은 전기통신사업의 발전과 이용자 편의를 도모함으로써 공공의 복리를 증진을 목적으로, 주요 사업자가 제공해야 하는 역무의 범위와 책임을 명시하고 있다. 현행 전기통신사업법에서 규정하는 사업자의 구분은 크게 기간통신사업자, 별정통신사업자, 부가통신사업자로 각각의 역무에 따라 부과되는 책임도 틀려진다.[45].

45) '전기통신사업법' 상 사업자 구분 -제4조(전기통신사업의 구분등)
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.
③ 별정통신사업은 다음 각 호의 1에 해당하는 사업으로 한다.
1. 제5조의 규정에 의한 기간통신사업의 허가를 받은 자(이하 "기간통신사업자"라 한다)의 전기통신회선설비등을 이용하여 기간통신역무를 제공하는 사업
2. 대통령령이 정하는 구내에 전기통신설비를 설치하거나 이를 이용하여 그 구내에서 전기통신역무를 제공하는 사업
④ 부가통신사업은 기간통신사업자로부터 전기통신회선설비를 임차하여 제2항의 규정에 의한 기간통신역무

그러나 전기통신사업법은 1990년대 들어 통신과 인터넷 비즈니스의 영역이 크게 확장됨에 따라 해당 사업자의 책임과 의무를 규정하는 법으로 통신과 인터넷, SW의 융합되어 급속하게 발전하고 있는 클라우드 컴퓨팅 사업자에 대한 책임과 의무를 규정하기에는 부족한 측면이 있다.

예를 들어 현행 전기통신사업법에서는 전기통신서비스를 이용하는 사용자의 보호를 위해 이용약관을 방송통신위원회에 신고하도록 되어 있다. 이러한 의무조항은 기간통신서비스를 제공하는 통신사업자나 이들의 회선을 임대하여 기간통신서비스를 제공하는 별정통신사업자, 기간통신망을 임대하여 부가서비스를 제공하는 일정규모 이상의 부가통신사업자를 대상으로 하는데, IDC사업자의 서버를 임대하여 SaaS, PaaS등의 서비스를 제공하는 클라우드 컴퓨팅 사업자의 이용약관을 신고여부는 명확하지 않으며, 실제 많은 SaaS 사업자들이 이용약관을 신고하지 않고 있다.

현행 법체계상에서 클라우드 컴퓨팅 사업자는 가상 인프라서비스를 제공하는 IaaS사업자는 기간통신 사업자에 준하는 규제를, 이들의 IT인프라를 임대하여 SaaS, PaaS 등의 서비스를 제공하는 클라우드 컴퓨팅 사업자는 부가통신사업자로 분류하여 규제의 적용이 가능할 것이다.

그러나 부가통신서비스 사업자는 다양한 인터넷사업자와 전자상거래기업 등을 포괄하고 있어 SaaS나 PaaS서비스 제공자로 그 영역을 한정하기 어렵다. 이는 클라우드 컴퓨팅 활성화를 위해 검토되고 있는 다양한 제도의 적용에 있어서도 문제를 야기할 여지가 있다.

예를 들어 사용자 보호를 위한 클라우드 컴퓨팅 서비스 이용자보호 약관이나 서비스 가이드라인, 인증체계 등이 만들어 졌을 경우 이를 적용할 수 있는 클라우드 컴퓨팅 서비스 사업자의 유형이 정의되어 있지 않아 실질적인 법적용 대상을 규정하기 어렵다.

나. 정통망법 상에서의 문제점

정통망법에서는 직접정보통신시설에 외부로부터 침해사고가 발생하여 심각한 장애를 일으켰을 경우와 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있을 경우에 대해 서비스의 전부 또는 일부를 중단하거나 제한 할 수 있는 규정을 두고 있다. 특히 이용자에 대해서는 서비스 사업자가 보호조치를 취하도록 요청하여 이를 이행하지 않을 경우 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있어 클라우드 컴퓨팅

외의 전기통신역무(이하 “부가통신역무”라 한다)를 제공하는 사업으로 한다.

서비스 이용자가 필요한 시점에 필요한 정보를 이용하지 못하는 사태가 발생할 수 있는 개연성을 내포하고 있다.

이와 관련, 정통망법에서는 서비스의 중단 및 제한의 범위를 〈표 3-10〉과 같이 규정하고, 이용(서비스) 약관상에 명기하여 이용자 보호를 위한 조치를 이행하고 있다. 그러나 클라우드 컴퓨팅의 경우 서비스 중단에 따른 사용자들의 경제적 손실이 막대할 것으로 예상되는 상황에서 서비스 중단 및 제한 범위가 사업자 위주로 명시되어 있어 보다 이용자의 관점에서 서비스 중단의 제한범위를 설정하고, 그 기준도 구체화할 필요가 있다.

〈표 3-10〉 정통망법상의 서비스 중단 및 제한 범위

구분	내 용
제46조의2 (집적정보통신시설 사업자의 긴급대응)	① 집적정보통신시설 사업자는 다음 각 호의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있다. 1. 집적정보통신시설을 이용하는 자(이하 "시설이용자"라 한다)의 정보시스템에서 발생한 이상 현상으로 다른 시설이용자의 정보통신망 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우 2. 외부에서 발생한 침해사고로 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되는 경우 3. 중대한 침해사고가 발생하여 방송통신위원회나 한국인터넷진흥원이 요청하는 경우 ② 집적정보통신시설 사업자는 제1항에 따라 해당 서비스의 제공을 중단하는 경우에는 중단사유, 발생일시, 기간 및 내용 등을 구체적으로 밝혀 시설이용자에게 즉시 알려야 한다. ③ 집적정보통신시설 사업자는 중단사유가 없어지면 즉시 해당 서비스의 제공을 재개하여야 한다.
제47조의3 (이용자의 정보보호)	① 정부는 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 권고하고, 침해사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있다. ② 주요정보통신서비스 제공자는 정보통신망에 중대한 침해사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있으면 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다.

또한, 정통망법 시행령 제55조 이용자 보호 조치의 요청에 관한 약관사항에서는 이용자

보호조치 불이행에 따른 접속 제한 기간 등 보호조치 내용, 부당한 접속 제한 등에 대해 약관상에 명기하고 있지만, 구체적인 내용에 대한 언급이 되어 있지 않다.

뿐만 아니라 현재 정통망법에서 약관의 신고를 통신과금서비스사업자와 서비스 관련 약관 내용을 정하여 인허가 및 관리감독 기관인 방송통신위원회에 신고하여 계약체결 시 이용토록 하고 있다. 그러나 정통망법 시행령 제55조에 따라 약관에 포함하여야 하는 내용이 매우 제한적으로, 서비스 이용자의 권리보호를 위해서는 부족하다.

이에 클라우드 컴퓨팅 서비스 특성에 맞는 표준 이용(서비스) 약관 제정 마련이 시급히 이루어져야 할 것이다. 특히 최근 국내에서도 이동통신사업자 및 IT서비스 업체를 중심으로 클라우드 컴퓨팅 서비스를 추진하고 있는 만큼 빠른 시일 내에 클라우드 컴퓨팅 서비스 이용자 보호를 위한 표준 이용(서비스) 약관 제정 및 가이드라인을 마련 등 보급하여 불필요한 문제를 사전에 차단할 필요가 있다.

〈표 3-11〉 정통망법상의 약관의 신고 및 관련 사항

구분	내 용
제56조 (약관의 신고 등)	① 통신과금서비스제공자는 통신과금서비스에 관한 약관을 정하여 방송통신위원회에 신고(변경신고를 포함한다)하여야 한다. ② 방송통신위원회는 제1항에 따른 약관이 통신과금서비스이용자의 이익을 침해할 우려가 있다고 판단되는 경우에는 통신과금서비스제공자에게 약관의 변경을 권고할 수 있다.
시행령 제55조 (이용자 보호조치의 요청에 관한 약관사항)	법 제47조의3제4항에 따라 이용자에 대한 보호조치의 요청에 관하여 이용약관으로 정하여야 하는 사항은 다음 각 호와 같다. 1. 이용자에게 보호조치를 요청할 수 있는 사유 및 요청하는 방법 2. 이용자가 하여야 할 보호조치의 내용 3. 이용자가 보호조치를 이행하지 아니할 경우 정보통신망으로의 접속 제한 기간 4. 이용자의 보호조치 불이행에 대하여 부당한 접속 제한을 한 경우 이용자의 이의제기 및 배상 절차

다. 사업자별 이용(서비스) 약관상의 문제점

1) 손해배상 범위 및 규모

기존 인터넷기반으로 서비스를 제공하는 사업자별 이용약관을 비교해 보면 고객이 서비스를 이용하지 못하여 그 사실을 회사에 통보 또는 그전에 회사가 그 사실을 알게 된 시점

이후 최소 2시간~4시간 이상 서비스 제공이 중단 된 경우 공통적으로 일 평균액을 24로 나눈 시간당 평균액에 이용하지 못한 시간수를 곱한 값의 3배수를 보상하고 있다.

〈표 3-12〉 서비스 장애 발생에 따른 이용약관별 손해배상 범위

약관 구분	손해배상 범위	금액 산정 기준
초고속 인터넷서비스	o 3시간 이상 서비스 중지 경우 o 장애발생 누적시간 12시간 초과 시(월 기준)	o [(1일 평균금액/24시간)×장애발생 시간×3배] ※1시간미만의 경우 1시간 산정
웹하드 서비스	o 2시간 이상 서비스 중지 경우 o 효력시점 이후 2시간 이내 정상화의 경우 해당 안 됨	o [(1일 평균금액/24시간)×장애발생 시간×3배] ※1시간미만의 경우 1시간 산정
IDC 서비스	o 2시간 이상 서비스 중지 경우	o [(1일 평균금액/24시간)×장애발생 시간×3배] ※1시간미만의 경우 1시간 산정

그러나 클라우드 컴퓨팅에서 중요한 것은 서비스의 가용성의 수준으로 '서비스의 중지'라는 표현은 그 책임소재를 밝히는데 매우 부족하다. 예를 들어 서비스 가용률 50%의 경우 이를 중지로 볼 수 있을 것이냐의 문제가 발생하기 때문이다.

이에 아마존, 구글 등 해외 클라우드 컴퓨팅 서비스의 경우 서비스 가용률 기반의 엄격한 기준을 규정하고 있으며, 서비스 장애 발생 시 SLA 상의 가상률에 따라 사용료의 일정 비율을 차등 보상하고 있다. 이는 클라우드 컴퓨팅 서비스 사용자가 인터넷을 이용해 IT자원을 사용한 만큼 요금을 서비스 제공자에게 지불하는 종량제(Useflex) 방식임을 감안한 것으로 국내의 경우도 단순히 서비스 중단이라는 공급자 위주의 막연한 표현이 아닌 세부적인 서비스 가용률에 따른 사용자 보호규정을 마련해야 할 필요가 있으며, 향후 클라우드 컴퓨팅 서비스 제공에 따른 표준 SLA(Service Level Agreement) 제정에 있어 이를 반영할 필요가 있다.

그리고 클라우드 컴퓨팅 서비스는 가용성 99.999%의 24시간×365일 무중단(Seamless) 서비스 제공을 특성으로 하고 단일 사업자 또는 복수의 사업자자 참여 가능한 모델로서, 복수 사업자가 참여하는 클라우드 컴퓨팅 서비스의 경우 장애에 따른 피해규모가 상대적으로 클 것으로 사료되는 바, 장애 시 현재 인터넷 서비스에서 제시하고 있는 손해배상 규모를 상회하는 기준을 검토하는 등 클라우드 컴퓨팅 서비스 특성에 맞게 조정이 이루어져야 할 것이다.

2) 서비스 사업자의 면책 범위

서비스 사업자의 면책범위는 서비스 유형별 이용약관 비교에서 볼 수 있듯이 초고속 인터넷 서비스 이용약관, 웹하드 서비스 이용약관, IDC 서비스 등 인터넷 서비스별로 상이한 면책 범위를 규정하고 있으며, 그 내용이 애매모호하고 포괄적일 뿐 아니라 일부는 서비스 제공자(초고속인터넷서비스사업자 지칭)에게 유리하도록 되어 있다.

초고속 인터넷 서비스의 경우 사업자는 정통망법에 의거 안전진단 수검의 의무를 지니며 당시 과학기술 수준으로 결함의 존재를 발견할 수 없는 경우 등에 대해서는 책임지지 않도록 되어 있다. 그리고 웹하드 서비스는 관련 시스템 변경, 교체 등으로 인한 일시적인 서비스 제공 중단 및 무료 서비스 등에 따른 사용자의 손실에 대해서도 사업자의 책임이 면책되도록 되어 있다. IDC 서비스의 경우에는 사용자가 자료 백업을 하지 않아 발생하는 사고(손해) 또는 타 통신사업자의 서비스 장애로 인한 경우 등에 대해 사업자에게 책임을 면책토록 하고 있다. 이에 대해 클라우드 컴퓨팅 서비스 사업자 및 이용자가 부적당한 면책 범위로 인해 피해를 입지 않도록 관련 면책 범위를 구체화하여 명시토록 하여야 할 것이다.

〈표 3-13〉 인터넷 서비스별 면책 범위 이용(서비스)약관 비교

구분	관련 약관	비고
초고속 인터넷 서비스	OO은 “정보통신망이용촉진및정보보호등에관한법률” 제46조의 3에 따라 안전진단을 수검하고, 정보통신 접속서비스 사업자로서 선량한 관리자의 주의의무를 다한 경우에는 침해사고 등에 대한 책임을 지지 아니하며, 다음과 같을 경우에 책임을 지지 않습니다. 1. 서비스를 제공할 당시 과학 기술수준으로 결함의 존재를 발견할 수 없는 경우 2. 서비스를 제공할 당시의 법령이 정하는 기준을 준수하였음에도 발생하였을 경우 3. 비암호화된 무선구간에서의 통신내용 및 정보유출의 경우	QooK 제23조 (침해사고에 대한 면책규정)
	①3.타사 서비스 및 단말기기 등의 장애 ⑥회사는 제22조침해사고에 대한 면책규정)에 해당하는 경우 손해배상 책임이 면제됩니다.	SK브로드밴드 제27조 (손해배상및 면책)
	⑦회사는 이용고객이 제9조제⑩항의 보호 장비를 설치하지 아니하여 발생한 손해나 귀책사유로 인한 서비스 이용의 장애에 대하여 책임이 면제됩니다. ⑧회사는 제30조에 해당하는 경우에는 책임이 면제됩니다. ※제30조(침해사례에 대한 면책 규정)	LG XPEED 제35조 손해배상

〈표 3-13〉 인터넷 서비스별 면책 범위 이용(서비스)약관 비교(계속)

구분	관련 약관	비고
웹하드 서비스	1. OOO은 각 호의 1에 해당하는 경우에는 손해배상을 하지 않습니다. ㄷ. 전시통신서비스 특성상 불가피한 사유로 서비스 제공이 불가능하거나 관련 시스템(SW 포함)의 변경, 교체 등을 위하여 일시적으로 서비스 제공을 중단하는 경우 ㅁ. OOO 이외의 타 통신사업자와 관련하여 사용자에게 어떠한 손해가 발생한 경우 ㅂ. 무료로 제공되는 서비스와 관련하여 사용자에게 어떠한 손해가 발생한 경우 ㅅ. 게시판, 알림판, 쪽지, 게스트폴더, 바이러스 체크와 같이 무료로 제공되는 보조기능과 관련하여 사용자에게 어떠한 손해가 발생한 경우 ㅊ. 계약만료 또는 요금 미납의 결과로 사용자 계정이 정지되거나, 보관 파일이 삭제된 후 이에 따르는 손익의 경우 ㅌ. 매주 화요일, 금요일에 웹하드 휴지통 폴더의 자료 삭제를 실시하며, 이에 대한 불이익에 대한 책임은 사용자에게 있습니다.	LG데이콤 제24조 (면책)
IDC 서비스	4. 고객 소유 또는 임대 장비 시스템에 자료 백업을 하지 않아 사고가 발생한 경우(하드웨어의 결함에 대비한 자료의 백업을 하지 않은 경우) 5. 고객의 정보시스템 보안관리 소홀로 침해사고가 발생한 경우 8. 타 통신사업자의 서비스 장애로 인한 경우	SK브로드밴드 제51조 (면책)

3) 서비스 사용자 보호 대상 기준

현행 정통망법 및 서비스 사업자별 이용(서비스)약관 상에서는 클라우드 컴퓨팅 서비스를 이용하는 사용자 보호대상 기준이 명확하지가 않아 서비스를 이용하는 주체별로 혼란을 야기 시킬 수 있다. 이는 클라우드 컴퓨팅 서비스가 인터넷 접속을 통해 서비스 제공 · 이용이 가능함에 따라 서비스 장애 유형별 사용자 보호 대상 기준이 〈표 3-14〉과 같이 달라질 수 있다.

이와 관련하여 현행 법체계상에서는 클라우드 컴퓨팅 서비스 특성에 맞는 서비스 보호 대상 구분 및 기준이 명시 되어 있지 않으며, 서비스 사업자 유형별 이용(서비스)약관에서 서비스 장애 발생 시 손해 범위 및 배상 책임만을 명시해 두고 있다. 이 역시 서비스 사업자별로 정하는 기준에 따라 상이함으로, 법체계상에 서비스 장애 유형별 대상 기준을 명확

히 하여 손해배상에 대한 주체를 구분토록 하여야 할 것이다.

〈표 3-14〉 서비스 장애 유형별 사용자 보호 대상 기준

서비스 장애 유형	대상 기준	
	서비스 사업자	서비스 이용자
인터넷 서비스 장애로 인한 서비스 제공 및 이용 불능의 경우	초고속인터넷서비스사업자 (예)KT, SKT, LGT 등	클라우드 컴퓨팅 서비스 사업자 클라우드 컴퓨팅 서비스 이용자
시스템의 오류 및 기타 원인으로 서비스 장애 발생의 경우	클라우드 컴퓨팅 서비스 사업자	클라우드 컴퓨팅 서비스 이용자

아울러, 클라우드 컴퓨팅 서비스 장애 발생에 따른 이용자의 피해를 최소화하는 것도 중요하지만 사전에 발생 가능한 서비스 장애에 대해 대응체계를 마련하여 예방해 나가는 것 또한 클라우드 컴퓨팅 서비스 이용자 보호 못지않게 매우 중요한 부분이다.

5. 개선방안

가. 전기통신기본법 및 전기통신사업법상의 재검토

현행 전기통신기본법 및 사업법 제정 당시 그 주요 대상은 통신서비스와 인터넷 서비스가 중심으로 클라우드 컴퓨팅을 담기에는 부족함이 있다. 실제 현행 법체계 하에서는 클라우드 컴퓨팅에 대한 정의나 서비스의 형태, 사업자의 유형 등이 정의되어 있지 못하다. 이는 인증체계나 이용약관 등 클라우드 컴퓨팅 사용자를 위한 별도의 보호방안이 만들어져도 그 적용대상을 규정하기 어렵게 할 수 있다.

물론 현행 법체계 하에서도 IaaS사업자를 기간통신사업자나 별정통신사업자로, PaaS, SaaS사업자를 부가통신사업자로 간주하는 방안도 검토가 가능하다. 그러나 법제정이나 개정 당시 전혀 고려되지 않았던 새로운 형태의 서비스가 등장하고 있는 상황에서 기존의 법체계하에서 지정된 사업자 구분을 활용하기에는 무리가 따른다. 클라우드 컴퓨팅이 통신서비스와 인터넷 서비스와 온라인을 통해 서비스를 제공받는 다는 입장에서 많은 부분 공통분모가 있지만, 서비스 제공자가 사용자인 기업들의 데이터와 업무 프로세스를 직접 관리하고, 지원한다는 점에서 제공되는 서비스의 특성과 목적이 통신서비스나 인터넷 서비스와 상이하기 때문이다. 따라서 클라우드 컴퓨팅의 활성화를 위한 법·제도의 개선은 새로운 모습

으로 진화하고 있는 클라우드 컴퓨팅 사업의 변화를 담아 새롭게 정의할 필요가 있다. 이는 크게 클라우드 컴퓨팅을 위한 신규 법 제정과 기존 전기통신기본법 및 전기통신사업법의 개정을 통해 가능하다.

신규 법 제정은 기존의 법체계 하에서 접근하기 어려운 클라우드 컴퓨팅의 정의나 유형 등을 규정하고, 이에 따른 사업자를 구분하여 책임과 의무를 부여할 수 있다는 장점이 있다. 그러나 현행 정보통신기본법이나 사업법 등 기존 법체계를 그대로 유지하는 상황에서 새로운 법을 신설할 경우 중복규제의 우려가 존재하고, 비슷한 유형의 서비스에 대하여 서로 다른 법을 적용하는 등 전반적인 법체계에서의 혼선이 발생할 수 있다.

기존 법체계의 개정은 새로운 클라우드 컴퓨팅에 대한 서비스 체계를 어떻게 반영할 것이냐 하는 문제가 존재한다. 즉 기존 기간통신사업자, 별정통신사업자, 부가통신사업자로 구분된 사업자 분류시스템 하에 클라우드 컴퓨팅 사업자를 어떻게 구분하고, 유형화할 것이냐의 문제이다.

어떠한 방안이든 결국 기존 법체계에 대한 전반적인 재검토는 불가피하다. 이를 통해 클라우드 컴퓨팅에 대한 정의와 서비스 구분, 시장 및 사업자의 유형을 세부적으로 구분함으로써 클라우드 컴퓨팅의 활성화를 위한 (기업)사용자 보호를 위한 새로운 책임의 부여 등이 가능하도록 법체계를 정비할 필요가 있다.

나. 정통망법상의 개선 방안

1) 서비스 중단 및 제한 범위 개선

앞서 전술한 바와 같이 클라우드 컴퓨팅 서비스의 특성상 침해사고로 인하여 서비스 사업자로부터 서비스 중단 및 제한 조치를 통보 받아 이용을 하지 못하는 경우에 대해 정통망법상의 관련 내용인 제46조의2(직접정보통신시설사업자의 긴급대응)와 제47조의 3(이용자의 정보보호)에 대한 서비스 중단 및 제한 범위에 대해 다음과 같이 개정하여 서비스 이용자에 대한 보호 조치를 강화해야 할 것이다.

현재 정통망법에서 규정하고 있는 서비스 중단 및 제한의 주된 원인인 침해사고로인해 심각한 장애 발생의 경우 이용자에서 서비스 사업자로 귀책사유가 변경되어야 할 것이며, 아울러 서비스 사업자는 이용자의 정보통신망이 침해사고로 인한 심각한 장애가 발생하지 않도록 자체적인 대응방안을 마련토록 명시해야 한다. 클라우드 컴퓨팅 서비스는 이용자가

다양한 디바이스 장치를 통해 필요한 시기에 인터넷에 접속하여 필요한 IT자원 빌려서 사용하는 방식인 점을 감안하였을 경우, 이용자가 직접 침해사고에 대한 보안 조치를 취하기에는 클라우드 컴퓨팅 서비스 사용에 대한 필요성이 현저히 떨어지게 될 것이기 때문이다.

2) 이용(서비스)약관 관련사항 개선 및 구체화

정통망법 시행령 제55조 이용자 보호조치의 요청에 관한 약관사항에서 클라우드 컴퓨팅 서비스 환경에 맞도록 1호~3호의 조문 중 이용자가 보호조치에 관련된 내용은 서비스 사업자로 변경되어야 할 것이며, 또한, 인터넷을 통한 전자금융서비스 사례를 벤치마킹하여 서비스 이용자가 인터넷을 통해 해당 홈페이지 접속 시 자동으로 보안 프로그램이 구동 될 수 있도록 관련 법령 및 이용약관에 관련 사항을 구체화시켜 현 정통망법에서 규정된 이용자의 보호조치 의무에 대한 대응책을 마련, 서비스 사업자 등록 및 신고 시 필수 이행사항으로 명문화 시키는 노력도 필요할 것이다.

〈그림 3-9〉 전자금융서비스 보안프로그램 구동 화면

3) 분쟁발생에 따른 우선 법령 범위 명문화

현행 정통망법에서는 이용(서비스)약관 신고를 서비스 사업자가 약관을 정하여 방송통신위원회에 신고하는 절차로 이루어져 있으며, 신고 시 동법 시행령 55조(이용자 보호조치의 요청에 관한 약관사항)에 4가지 필수 항목을 두어 규정하고 있다. 이에 관련 필수 항목을 보면 이용자에게 보호조치를 요청할 수 있는 사유 및 요청 방법, 이용자가 하여야할 보호조치의 내용, 불이행에 따른 이의제기 및 배상절차 등이 명문화되어 있지만, 그 외이용(서비스) 약관 관련 사항에 대해서는 명문화되어 있지 않다. 만약 서비스 장애로 인해 분쟁이 발생 되었을 경우, 서비스 이용자는 손해를 입을 수 있다.

이러한 서비스 이용자 손해를 사전에 방지하기 위하여, 현재 약관의 규제에 관한 법률에서 〈표3-2-12〉와 같이 규정하고 있는 이용자 보호를 위한 우선 고려 대상 법령들을 정통망법 시행령 상에 명기하거나 또는 분쟁발생 시 정통망법에 앞서 약관의 규제에 관한 법률이 우선 적용 될 수 있도록 현행 정통망법을 개선하여 서비스 사업자의 오남용 방지 등 불공정 거래를 차단하여야 한다.

〈표 3-15〉 약관의 규제에 관한 법률 중 이용자 보호를 위한 우선 고려 대상

제7조 (면책조항의 금지) 계약당사자의 책임에 관하여 정하고 있는 약관의 내용 중 다음 각 호의 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 이유 없이 사업자의 손해배상범위를 제한하거나 사업자가 부담하여야 할 위험을 고객에게 이전시키는 조항
3. 상당한 이유 없이 사업자의 담보책임을 배제 또는 제한하거나 그 담보책임에 따르는 고객의 권리행사의 요건을 가중하는 조항 또는 계약목적물에 관하여 견본이 제시되거나 품질·성능 등에 관한 표시가 있는 경우 그 보장된 내용에 대한 책임을 배제 또는 제한하는 조항

제9조 (계약의 해제·해지) 계약의 해제·해지에 관하여 정하고 있는 약관의 내용 중 다음 각 호의 1에 해당되는 내용을 정하고 있는 조항은 이를 무효로 한다.

1. 법률의 규정에 의한 고객의 해제권 또는 해지권을 배제하거나 그 행사를 제한하는 조항
2. 사업자에게 법률에서 규정하고 있지 아니하는 해제권·해지권을 부여하거나 법률의 규정에 의한 해제권·해지권의 행사요건을 완화하여 고객에 대하여 부당하게 불이익을 줄 우려가 있는 조항
3. 계약의 해제 또는 해지로 인한 고객의 원상회복의무를 상당한 이유 없이 과중하게 부담시키거나 원상회복청구권을 부당하게 포기하도록 하는 조항
4. 계약의 해제·해지로 인한 사업자의 원상회복의무나 손해배상의무를 부당하게 경감하는 조항

〈표 3-15〉 약관의 규제에 관한 법률 중 이용자 보호를 위한 우선 고려 대상(계속)

5. 계속적인 채권관계의 발생을 목적으로 하는 계약에서 그 존속기간을 부당하게 단기 또는 장기로 하거나 묵시의 기간연장 또는 갱신이 가능하도록 정하여 고객에게 부당하게 불이익을 줄 우려가 있는 조항 제10조 (채무의 이행) 채무의 이행에 관하여 정하고 있는 약관의 내용 중 다음 각 호의 1에 해당되는 내용을 정하고 있는 조항은 이를 무효로 한다. 1. 상당한 이유 없이 급부의 내용을 사업자가 일방적으로 결정하거나 변경할 수 있도록 권한을 부여하는 조항 2. 상당한 이유 없이 사업자가 이행하여야 할 급부를 일방적으로 중지할 수 있게 하거나 제3자로 하여금 대행할 수 있게 하는 조항 제11조 (고객의 권익보호) 고객의 권익에 관하여 정하고 있는 약관의 내용 중 다음 각 호의 1에 해당되는 내용을 정하고 있는 조항은 이를 무효로 한다. 1. 법률의 규정에 의한 고객의 항변권, 상계권 등의 권리를 상당한 이유 없이 배제 또는 제한하는 조항 2. 고객에게 부여된 기한의 이익을 상당한 이유 없이 박탈하는 조항 3. 고객이 제3자와 계약을 체결하는 것을 부당하게 제한하는 조항 4. 사업자가 업무상 알게 된 고객의 비밀을 정당한 이유 없이 누설하는 것을 허용하는 조항

다 사업자별 이용(서비스) 약관상의 개선방안

1) 손해배상 범위 및 규모

① 가용률 기반의 손해배상 범위 규정화 및 표준 SLA(Service Level Agreement) 반영

현행 인터넷 서비스 이용약관에 따르면 장애로 인해 2~4시간 이상 서비스가 중단된 경우 그 손해를 보상하도록 규정되어 있는데, Seamless 및 Useflex 방식의 클라우드 컴퓨팅 서비스 특성을 감안하여 서비스 가용률 기반으로 개정할 필요가 있다. 현재 국내에서는 SLA가 강제 사항이 아닌 서비스 사업자의 권고 및 선택 사항으로 규정되어 있어, 인터넷 서비스를 제공하는 사업자 중 SLA를 적용하고 있는 사업자를 찾아보기 힘들 정도이다. 이에 관련 법령 및 제도상에 필수 권고 사항으로 규정 할 수 있도록 노력을 기울여야 할 것이다.

아울러, 해외 선진국들의 SLA 적용 사례를 벤치마킹하여, 클라우드 컴퓨팅 서비스 특성에 맞는 표준화된 SLA 제정 및 서비스 사업자 및 이용자를 위한 가이드라인도 만들어져야 한다. 또한, 서비스 품질 측정과 관련하여 이용자가 품질 수준을 확인 할 수 있도록 의무적

으로 표시할 수 있게끔 법제도적 뒷받침도 마련되어야 할 것이다. 만약, 서비스 사업자가 품질 측정을 위한 시스템이 제반사항이 구축되지 않은 경우에는 인터넷 품질 측정 가능한 기관(한국정보화진흥원 인터넷 품질테스트 및 KT 인터넷 속도 테스트 등 관련 기관)에 위탁 등 외주를 통한 방식으로 이용자에게 정보를 제공할 수 있도록 조치하여야 한다.

〈그림 3-10〉 KT 인터넷 속도 테스트 화면

② 손해배상 규모의 상향 조정 및 분쟁조정체계 마련 검토

전술한 바와 같이 클라우드 컴퓨팅 서비스는 단일 사업자 또는 복수의 사업자자 참여하여 서비스를 제공하고 그 수익을 공유하는 서비스 모델로서, 장애 발생에 따른 손해의 파급효과 또한 클 것이다. 따라서 현재 인터넷 서비스 이용약관 등에서 규정하고 있는 손해배상 규모에 대한 면밀한 비교·분석을 통해 그 규모를 상황에 맞게 조정할 필요가 있다.

아울러 장애 발생에 따른 원인규명과 분쟁 조정 등을 위한 관련 법제 정비가 필요하다. 현행법상 개인정보보호, 인터넷주소 및 전자상거래 등에 국한되어 분쟁조정위원회가 구성·운영되고 있으나 클라우드 컴퓨팅 서비스 활성화에 따른 분쟁이 증가할 것으로 사료되는바 이에 대한 선제적 대응방안 수립이 필요하다.

③ 사용자 자율주도의 실시간 서비스 모니터링 시스템 구비

기술 및 서비스 관점에서 구글의 Dashboard와 같이 사용자가 실시간으로 자신이 사용하는 서비스의 가용현황을 모니터링 할 수 있는 장치를 마련하고 법제도적으로 의무화하는 방안도 검토할 필요가 있다. 이러한 시스템이 구비하게 됨으로써 사용자는 서비스의 장애 시점 및 현황 등을 파악함으로써 클라우드 컴퓨팅 서비스의 품질 제고에 대한 능동적으로 참여와 사용자의 권익보호를 위한 기반을 마련하게 될 것이다.

2) 서비스 사업자의 면책 범위

앞에서 살펴본 바와 같이 현행 인터넷 서비스 관련 법률 및 이용약관 등에서는 서비스 사업자 중심의 면책범위를 규정하고 있으나 서비스 사용자 중심의 개선이 요구되며, 이를 위해 클라우드 컴퓨팅 서비스에 특화된 별도의 특별법을 제정하지 않는 한 관련 법령 및 이용(서비스)약관 등의 개정을 추진해야 할 것이다.

① 원인불명의 서비스 장애에 대한 사업자 책임 부여

일부 초고속 인터넷 서비스 이용약관에서 서비스를 제공할 당시 과학 기술 수준으로 결함의 존재를 발견할 수 없는 경우에는 사업자의 면책을 부여하고 있으나 해외 클라우드 컴퓨팅 서비스의 경우 원인불명의 경우라도 고객 서비스 차원에서 손해배상을 하는 것이 추세로 삭제하는 것이 적절할 것으로 사료된다.

② 타사 서비스 및 단말기기 등의 장애에 대한 사업자 책임 부여

클라우드 컴퓨팅 서비스 자체가 통신망 및 사용자의 단말기기에 상관없이 웹을 통해 요청하는 서비스를 제공해야 하기 때문에 다양한 단말기기와의 인터페이스 및 이종 클라우드 컴퓨팅 서비스 상호운용·운용에 대해 국제 표준화 및 기술개발 등이 활발히 진행되고 있어 클라우드 컴퓨팅 서비스 특성상 통신망 및 단말기기는 무의미하다. 이에 현재 인터넷 서비스 이용약관 등에서 규정하고 있는 타사 서비스 및 단말기기 등의 장애에 대한 사업자의 면책규정은 삭제 또는 개정되어야 할 것이다.

③ 사용자의 보호 장치 미설치 시 사업자의 면책규정의 개정

클라우드 컴퓨팅 서비스는 사용자의 모든 정보와 애플리케이션 등이 사업자의 서버에서 구동되기 때문에 사용자는 단순기능을 지닌 저사양의 단말기기 및 인터페이스 장치만 갖고

있으면 된다. 이러한 클라우드 컴퓨팅 서비스 특성상 현재 인터넷 서비스 이용약관 등에서 규정하고 있는 사용자가 보호 장치를 설치하지 않은 경우, 사용자가 백업하지 않은 경우 및 사용자의 보안관리 소홀 등에 의해 발생하는 손해의 면책규정을 적용하는 것은 무리가 있다.

④ 사용자 보호 대상 기준에 따른 면책범위 명확화

클라우드 컴퓨팅 서비스의 경우 서비스 이용자의 인터넷 장애가 아닌 서비스 사업자의 장애로 인해 서비스를 이용 할 수 없을 경우 손해배상을 요구하여 할 수 있다. 이 경우 서비스 사업자가 인터넷 서비스 장애로 인해 서비스를 제공하지 못한 경우에는 손해배상 책임에 대해서는 면책되어야 한다.

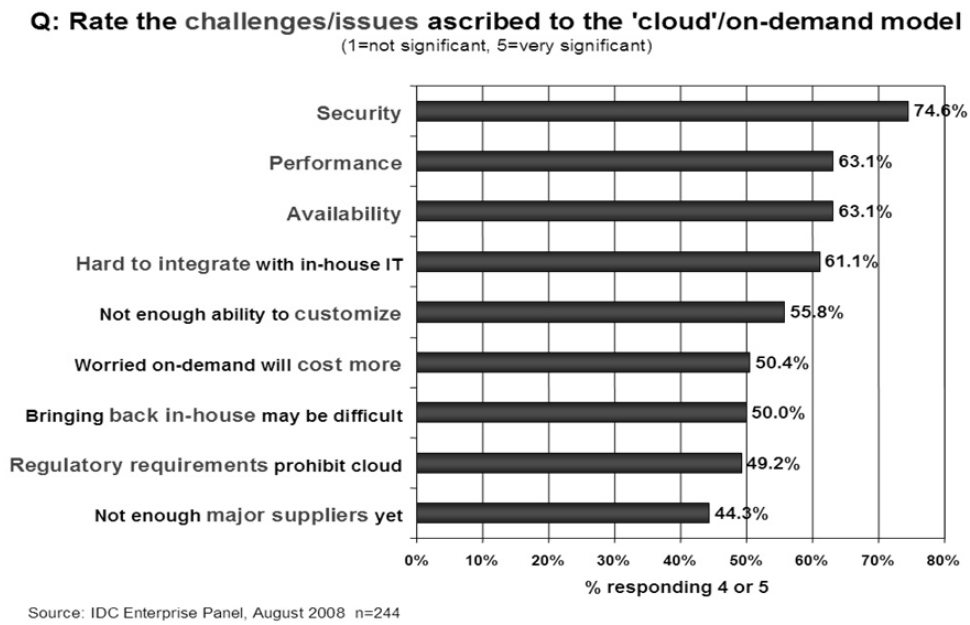
클라우드 컴퓨팅 서비스 특성상 초고속 인터넷 서비스 이용 대상은 클라우드 컴퓨팅 서비스 사업자와 클라우드 컴퓨팅 서비스 최종 이용자로 서비스 장애 원인이 인터넷 서비스 장애일 경우 클라우드 컴퓨팅 서비스 사업자의 면책범위에 명시하여 보호하여야 한다. 다만 사업자가 고의적으로 인터넷 서비스를 장애를 발생시켰을 경우에는 면책하지 않는다.

위와 같이 클라우드 컴퓨팅 서비스 활성화를 위한 기존 인터넷 서비스 법 · 제도 안에서의 사용자 보호를 위한 문제점 및 개선방안을 도출하였다. 개선방안이 실질적으로 적용되고 실효성을 갖기 위해서는 민 · 관의 유기적인 협력이 절실히 요구되며, 아울러 클라우드 컴퓨팅 서비스에 대한 요소기술의 개발과 보안체계 마련 등이 뒷받침되어야 할 것이며, 본고에서 목적으로 하는 클라우드 컴퓨팅 서비스 활성화를 위해서는 사용자 보호방안 뿐 아니라 클라우드 컴퓨팅 서비스를 도입하고자 하는 기업과 서비스를 개발하고 제공하는 기업에 대한 지원방안 또한 병행 검토되어 마련되어야 할 것이다.

제 3 절 사용자 보안우려 해소 방안

클라우드 컴퓨팅은 가상화를 기반으로 하고 있어 데이터의 위치 파악이 어렵고, 보안 측면에서 악성코드나 해킹 등 외부공격에 쉽게 노출될 수 있으며, 관리자 권한 오남용 등을 통한 개인정보 등 이용자의 민감한 정보가 대량 유출될 위험이 존재한다. 기업 입장에서도 이러한 문제가 완벽하게 해결되지 않은 상태에서는 고객 DB 등 핵심 기업정보를 클라우드에 의존하는 것 자체를 주저할 수밖에 없다.

〈그림 3-11〉 클라우드 컴퓨팅 활성화에 따른 이슈



출처: IDC Enterprise Panel 2008.8

클라우드 컴퓨팅의 활성화와 더불어 이러한 위험에 대한 충분한 대비가 되지 않을 경우, 매우 큰 사회적 파장을 불러올 수 있음에도 불구하고 이를 위한 국가, 산업 차원에서의 법적, 제도적 장치는 마련되어 있지 않다. 따라서 본 장에서는 이러한 클라우드 컴퓨팅 보안 문제 해결을 위한 국내 법규 및 제도적 측면에서의 개선 방안을 제시해 보고자 한다.

1. 클라우드 컴퓨팅 보안을 위한 해외 법, 제도 및 인증 현황

가. 국외 정보보호 법, 제도 현황 및 분석

현재 클라우드 컴퓨팅과 관련된 국외 정보보호 인증체계는 ISO27001이 유일하며, 이 역시 강제규칙은 아니다. 기타 SAS70 등과 같은 일반적인 감사표준이 존재하나 이것 역시 정보보호 관련 구체적인 규제요건을 언급하기보다는 리스크와 관련된 전반적인 프로세스를 평가하는 기준이고, 적용 대상은 미국 내로 제한되어 있다[46].

46) [참조: Gartner, What You Need to Know About Cloud Computing Security & Compliance, 2009/07/13]

이 밖에, 2009년 3월 미국 NIST(National Institute of Standards and Technology)에서 클라우드 컴퓨팅 서비스 보안 표준(Standard) 마련을 위한 조직을 신설하고, 표준화 계획을 발표했다. 클라우드 컴퓨팅 보안과 직접적으로 규제하는 국외 법·제도는 아직까지는 없으나, 서비스 제공자의 조직, 프로세스, 기술, 정보 등과 연관된 보안측면의 법·제도는 현재도 존재하므로 이의 현황을 국가별로 살펴보도록 한다.

1) 미국의 정보보호 관련 법제도

클라우드 컴퓨팅을 이용하는 기업은 민감한 정보(데이터, 파일, 기록 등)를 제3자인 클라우드 컴퓨팅 제공자에게 위탁하게 된다. 미국의 다수 연방법 및 관련 규정은 제3자와 계약을 맺는 경우, 프라이버시와 보안을 요구하고 있다. 예를 들어, 사회보장번호나 운전면허번호의 사용에 대한 제한 등이다. 다음은 미국에서의 이와 관련된 법규 현황이며, 주로 개인의 프라이버시를 침해하지 않는 기준을 정의하고 있다.

① 전기통신 프라이버시법(ECPA)

「전기통신 프라이버시법(ECPA : Electronic Communications Privacy Act of 1986)」은 전자통신기록에 불법적으로 접근하거나 보유정보를 허가 없이 공개하는 것을 예방하고자 제정된 것으로 핸드폰, 이메일 및 기타 전기통신에 대한 접근 표준을 정하고 수신자 식별 가능 정보, 로그기록 및 통화 기록 등 전송 기록에의 접근 표준을 설정하고 있다.

ECPA는 일반적으로 개인정보를 보호하기 위한 목적을 띄고 있으나, 구체적인 예외사항 및 법집행기관의 개인정보침해 우려가 있는 수사절차를 명시함으로써 객관적이고 투명한 수사를 할 수 있는 기틀을 마련하고 있다.

② 의료보험의 이전과 그에 수반되는 책임에 관한 법(HIPPA)

미국은「의료보험의 이전과 그에 수반되는 책임에 관한 법(HIPPA: Health Insurance Portability and accountability Act of 1996)」을 1996년 연방법으로 제정하여 의료정보, 재정정보 및 정부시스템에 대한 보안과 프라이버시의 중요성을 강조하고 있다. HIPPA는 전자적 형태의 개인 의료정보보호를 의무화하고 의료기관에 개인 의료정보보호 정책을 작성·시행할 것을 요구하고 있다.

③ Gramm-Leach Bliley Act(GLBA)

금융기관의 정보보호를 규율하는 Gramm-Leach Bliley Act_가 1999년부터 시행되었다. GLBA는 금융기관의 고객 개인정보보호 활동을 제안하는 2개의 가이드라인 외에 고객 개인정보 폐기방법 등도 제시하고 있다. 1999년 연방금융기관검사위원회(FFIEC: The Federal Financial Institutions Examination Council)는 금융기관의 리스크 관리 체계의 순위를 정하는 정보기술통일평가 시스템(URSIT: Uniform Rating System for Information Technology)을 개발했다.

④ SOX법(Sarbanes-Oxley Act of 2002)

SOX법은 미국에서 기업의 대형 부정회계 사건이 잇달아 발생하자 기업 회계와 재무보고의 투명성을 높이기 위해 2002년 제정한 법으로, 미국의 증권거래소에 상장되어 있는 모든 기업에 적용되어 증권거래위원회(SEC: Securities and Exchange Commission)에 재무보고서 제출을 의무화한 연방법이다. SOX법은 외국 기업이라도 미국 증권시장에서 주식을 공개한 경우에 원칙적으로 적용된다. 모두 11개의 장으로 구성된 SOX법 중 경영진의 책임을 증가시키는 동시에 실질적인 대응이 필요한 항목은 동 법령의 3장 '법인의 책임'의 302조 '재무보고에 대한 법인책임'과 4장 '강화된 재무정보 공시'의 404조 '내부통제에 대한 경영진 평가'라 할 수 있다.

2) 영국의 정보보호 관련 법·제도

영국은 다른 EU 회원국과 비교해 개인정보보호나 사이버범죄 대응에 선구적으로 관련 정책을 추진해왔다.

① 데이터보호법

「1984년 데이터보호법(Data Protection Law)」에서는 데이터 보호 등록소(Data Protection Register)와 등록관(Registrar)을 두고 등록제를 운영하였다. 데이터이용자와 컴퓨터 정보회사에 의한 등록에 관한 규정을 두었는데, 이들은 데이터보호등록부에 등록할 의무를 규정하고 있었다. 그런데 이는 사실상 일종의 허가제에 가까운 것이었으며, 컴퓨터의 이용이 비약적으로 증가함에 따라 이러한 규제가 불가능하다는 인식이 높아졌다.

② 프라이버시 및 전자통신규칙 2003

「프라이버시 및 전자통신규칙(Privacy and Electronic Communications(EC Directive)

Regulations 2003」은 EU의 전자통신부문 프라이버시지침(2002/58/EC)을 반영하여 제정되었다. 동 규칙은 통신서비스의 보안문제, 통신의 비밀보장과 관련하여 쿠키 거부권 및 개인정보의 보호, 트래픽 정보의 처리에 관한 기준, 위치정보 처리기준, 항목별 청구서, 발신자번호표시, 가입자 전화번호부 등의 프라이버시 보호 문제 등을 규정하고 있다. 또한 전자적인 수단(전화, 팩스, 이메일, 문자메시지, 영상메시지, 비디오 등)과 자동전화호출시스템을 이용한 직접마케팅메시지 전송과 프라이버시에 관한 사항을 규정하고 있다.

③ 조사권한규제법

「조사권한규제법(RIPA: Regulation of Investigatory Powers Act 2000)」은 통신감청에 관한 법률이다. 동 법은 인터넷이나 컴퓨터 암호화기술의 발전으로 인해 도입된 법으로, 일반인을 모니터하기 위한 기술을 기반으로 하고 있다.

3) 독일의 정보보호 관련 법률

독일의 법률은 독자적 통치권한이 주어진 16개 주가 각각 국가적 성격의 법률을 가지면서 하나의 국가를 형성하는 연방국가체제의 법률을 취하고 있다. 이러한 연방제를 취하므로 주마다 각종 법제도가 다르다.

① 정보통신법

2004년 제정, 2005년 3월 14일 개정된 「정보통신법(Telecommunications Act/TeleKommun ikationsgesetz-TKG)」은 정부기관의 기밀누설 방지, 데이터의 안전성 확보 및 네트워크 침해사고 방지를 위해, ISP 등 정보통신 서비스를 제공하는 모든 책임자는 고객정보를 정부에서 접근 가능한 상태로 할 의무가 있으며, 그러한 데이터는 정부의 감시기관이 직접 접근할 수 있도록 해야 한다고 규정하고 있다.

② 연방 데이터보호법(BDSG)

독일의 개인정보를 보호하기 위한 기본법인 「연방데이터보호법(Federal Data Protection Act(BDSG), 1990년 제정, 2003년 1월 14일 개정)」은 개인정보 정의에서부터 정보주체의 권리와 정보처리자의 각종 의무, 제3국으로의 정보이전, 비디오감시, 익명성, 스마트카드, 민감한 정보의 수집 등에 대한 내용을 포함하고 있다. 이 법은 2003년 EU의 개인정보보호 지침을 반영하기 위해 개정되었다.

③ 정보통신서비스 정보보호법(TDDSG)

「정보통신서비스 정보보호법(TDDSG : Gesetz uber den Datenschutz bei Teledliensten)」이 제정되어 시행되고 있다. 동 법은 정보통신서비스 이용관계에서의 개인정보수집·처리를 규율함에 따라 인터넷 포털사이트 운영자, 이메일서비스 제공자, 온라인 게임서비스 제공자 등의 정보통신서비스 제공자가 고객정보를 이용·처리하는 행위에 직접적으로 적용된다.

4) 일본의 정보보호 관련 법률

일본은 2001년 수립된 e-Japan 전략에 의해 일본을 세계 최첨단의 IT국가로 만들려는 노력을 지속적으로 추진하고 있다. 일본의 정보보호 관련 법률도 e-Japan 전략의 수립에 즈음하여 정비되었다. 일본의 정보보호 법체계는 「고도정보통신 네트워크 사회형성 기본법」, 「특정 전기 통신 서비스 제공자의 손해배상 책임의 제한 및 발신자 정보의 개시에 관한 법률」 및 개인정보보호 관련 법률 등이 있다.

① 고도 정보통신 네트워크 사회 형성 기본법

일본의 대표적인 IT법률은 「고도 정보통신 네트워크 사회 형성 기본법(IT기본법)(2000년 법률 제 144호)」이다. 동 법률은 고도 정보통신 네트워크 사회의 형성에 관한 시책을 신속하고 중점적으로 추진하는 것을 목표로 하고 있으며, 네트워크의 안전성 및 신뢰성, 개인정보보호의 확보를 기본방침 중 하나로 정해 정보보호 법제도의 기본적인 방침이 되고 있다.

② 특정 전기통신서비스제공자의 손해배상 책임 제한 및 발신자 정보의 개시에 관한 법률

인터넷 이용자의 권리침해로부터 일정 부분 온라인서비스제공자를 보호하고 정보의 유통을 촉진시키기 위하여 동법이 제정되었다. 이법은 인터넷상 프라이버시 침해 등을 방지하기 위한 새로운 법률로서 2001년 11월 공포되었다. 인터넷에서 송수신되는 정보에 의해서 피해를 받은 경우에 전기통신서비스제공자 등에 대한 배상책임에 일정한 기준을 마련함과 동시에 정보의 발신자를 공시하는 권리를 인정하는 내용이다.

③ 개인정보보호 관련 법률

주소·전화번호·메일주소 등 개인정보의 적정한 관리를 목적으로 하는 일본의 「개인정보보호법」은 2005년 4월부터 시행되고 있다. 동 법은 정보의 부정취득과 누출을 막기 위

한 여러 의무를 기업과 단체에 부과하고 있다. 규제 대상은 사업목적으로 개인정보를 소지하고 있는 기업 · 개인사업자 · 상점 · 단체 등으로 총 5,000명 이상의 정리된 개인정보를 가지고 있는 곳이며, 이를 위반할 경우 각각 사업을 관할하는 성 · 청장으로부터 권고 · 명령을 받는다. 만일 이에 따르지 않을 경우 6개월 이상의 징역 또는 30만 엔 이하의 벌금에 처할 수 있도록 되어 있다.

④ 사이버범죄 관련 법률

일본은 2001년 「EU의 사이버범죄조약」에 가입하여 2004년 국회의 비준을 거치고 국내법에 반영하기 위해 「범죄의 국제화 및 조직화 그리고 정보처리의 고도화에 대처하기 위한 형법 등의 일부를 개정하는 법률안」등을 정비하기 위해 노력하고 있다. 해킹, 바이러스 유포 등 정보시스템관련범죄 방지를 위해 「부정액세스행위 금지 등에 관한 법률」이 제정되어 1999년 8월부터 시행되고 있다. 주요 내용으로는 부정액세스행위를 조장하는 행위 및 타인의 식별정보를 무단으로 제공하는 행위를 금지하고 액세스 관리자에 의한 방어조치 등을 다루고 있다.

나. 정보보호 인증관련 현황 및 분석

1) ISO 27001(정보보안경영시스템 인증)

ISO 27001은 국제표준화기구 ISO(International Standards Organization)가 제정하고 관리하는 정보보호관리체계 관련 시스템을 심사하고 인증하는 제도로 1998년 제정된 BS7799-2를 근간으로 해서 2005년 제정되었으며, 정보보호분야에서 최고의 권위를 인정받고 있다.

수많은 기업이나 조직이 보안 문제로 어려움을 겪고 있으며, 보안문제를 처리할 시스템이 미비하고 기술적인 한계를 나타내고 정보의 중요성에 대한 인식이 부족한 현실적인 문제가 많이 발생하면서 이를 극복하고자 본 인증제도를 제정하게 되었다. ISO 27001은 국제표준으로 각 국가별로 인정기관 및 인증기관을 지정·운영하고 있으며, 인정기관 내에 인증위원회를 두어 인증결과를 심의하고 의결하게 된다.

〈그림 3-12〉 ISO 27001인증 체계

인증 심사는 문서심사와 현장심사로 이루어지며, 인증유효기간은 3년으로 인증취득 후 연1회 이상 사후관리 심사를 받아야 한다.

〈그림 3-13〉 ISO 27001 인증 절차

현재 약 70여개 국가에서 약 8,000개의 기업이 인증을 취득하고 있으며, ISO27001은 11개 분야 133개 항목에 대해 심사를 하고 있다.

〈표 3-16〉 ISO27001의 11개 분야

항 목	설 명
정보보안 방침(Security policy)	정보보안에 대한 경영방침과 지원 사항에 대한 통제구조 확인
정보보안 조직(Organization of Information Security)	조직 내에서 보안을 효과적으로 관리하기 위한 보안조직구성 및 책임과 역할에 대한 규명
자산 관리(Assets management)	조직의 자산에 대한 분류 및 이에 따른 적절한 보호프로세스 검토
인적 자원보안 (Human resources security)	사람에 의한 실수, 절도, 부정수단이나 설비의 잘못사용으로 인한 위험을 감소하기 위한 대응방안 확인
물리 및 환경보안(Physical and environment security)	비 인가된 접근, 손상과 사업장과 정보에 대한 영향을 방지하기 위한 대응책 여부
의사소통 및 운영관리 (Communication and operations management)	정보처리 설비의 정확하고 안전한 운영을 보장하기 위한 대응방안 존재 여부
접근통제(Access control)	정보에 대한 접근통제를 하기 위한 대응책 여부
정보시스템 인수, 개발 및 유지보수(Information system acquisition development & maintenance)	정보 시스템 내에 보안이 수립되었음을 보장하기 위한 대응방안 존재 여부
정보보안 사고관리(Information security incident management)	정보 시스템과 관련된 정보보안사고와 취약점이 허용된 시기 이내에 적절한 교정행동과 의사가 전달되는지 여부
사업 연속성 관리(Business continuity management)	사업 활동에 방해요소를 완화시키며 주요 실패 및 재해의 영향으로부터 주요사업활동을 보호하기 위한 프로세스 존재 여부 검토
부합성(Compliance)	범죄 및 민사상의 법률, 법규, 규정 또는 계약 의무사항 및 보안요구 사항의 불일치를 회피하기 대응책 여부

동남아시아에서 가장 많은 인증 실적을 올리고 있으며, 특히 일본(약 5,000개)이 인증 취득에 적극적이다. 국내의 경우는 2008년 기준으로 약 90개 기업이 ISO27001 인증을 취득하였으며, 매년 꾸준히 증가하고 있는 추세이다.

2) SAS 70 감사

SAS 70(Statement on Auditing Standards No. 70: Service Organizations)은 미국

공인회계사협회(AICPA, American Institute of Certified Public Accountants)에서 개발한 국제적으로 널리 통용되는 감사 기준이다. SAS 70 감사는 네트워킹 및 관련 프로세스를 통한 통제를 포함하는 서비스 제공자 환경에 대한 심도 있는 감사로 인식되고 있다. 내부회계 감사 제도로써 SAS 70 감사는 데이터 보호방법을 검증하게 된다.

서비스제공자(service provider)는 SAS70 감사 또는 서비스 감사자의 검사를 받은 후 그 결과물인 서비스 감사자 리포트를 사용자 조직에 제출한다. SAS 70 리포트는 기업의 데이터를 보호하기 위해 누가 정확히 어떤 조치를 취하고 있는지를 나타내게 된다. 제 1 유형 감사(Type I audit)는 서비스의 공급자가 고객에 대한 정보공개로 설명되는 내부 통제를 가지고 있는지의 여부를 포함하며, 제 2 유형(Type II)은 실제로 작동하고 있는 해당 통제를 테스트 한다. 그리고 제 1 유형의 경우는 특정시점에서의 기관의 감사상태를 보고하며, 제 2 유형에서는 최소 6개월 이내의 기관의 감사상태를 보고한다. 즉 제 1 유형은 2009년 7월 30일의 감사상태이며, 제 2 유형은 2009년 1월 30일부터 7월 30일까지의 감사상태이다.

〈표 3-17〉 SAS 70 리포트 내용

리포트 내용	Type I Report	Type II Report
1. 독립서비스 회계감사관의 리포트(의견)	포함	포함
2. 통제에 대한 서비스 조직의 설명서	포함	포함
3. 독립적인 서비스 회계감사관에 의해 제공되는 정보; 운영효과성에 대한 서비스 회계감사관의 점검내용 설명과 점검결과를 포함	선택	포함
4. 서비스조직에 의해 제공되는 기타 정보(예, 용어 풀이)	선택	선택

출처: http://www.sas70.com

3) PCI 보안 표준

PCI DSS(Payment Card Industry Data Security Standard)는 비자, 마스터카드 등 세계적인 카드 회사가 주축이 되어 2006년 PCI 보안표준위원회가 설립되면서 제정한 지불카드 업계 정보보안 표준규격이다. 이 규정은 고객의 데이터를 저장, 처리, 전송하는 카드 가맹점과 서비스 사업자가 준수하도록 권고 하고 있다. 국외에서는 PCI DSS를 이행하지 않는 가맹점 등에 카드결제 승인을 거부하는 등의 강도 높은 제제를 적용하고 있다. 우리

나라도 PCI DSS 요구사항을 충족시킬 수 있도록 대책을 강구하고 있다.

PCI DSS가 규정하고 있는 보안요구 사항은 네트워크 침입차단 시스템 구축 및 관리, 저장 데이터의 보호, 백신프로그램의 주기적인 업데이트와 이용 등 12개 이다.

〈표 3-18〉 PCI DSS의 보안항목

구 분	요 구 사 항
안전한 네트워크의 구축과 유지	- 요구1: 데이터 보호를 위한 방화벽의 설치 및 관리 - 요구2: 시스템 패스워드 및 기타의 보안 매개변수로 벤더가 제공하는 고유 값 사용금지(패스워드 변경 필요)
카드소유자 데이터 보호	- 요구3: 저장 데이터 보호 - 요구4: 공용네트워크를 통한 카드소유자데이터와 민감한 정보의 전송 암호화
취약점 관리 프로그램의 유지	- 요구5: 백신프로그램의 정기적인 업데이트와 이용 - 요구6: 보안 시스템과 어플리케이션의 개발 및 유지
강력한 접근통제 방법 이행	- 요구7: 업무상 필요 정보에 대한 접근 제한 - 요구8: 컴퓨터에 접속 시 개인별 고유 ID의 할당 - 요구9: 카드소유자 데이터에 대한 물리적 접근 통제
정규 모니터링과 네트워크 검사	- 요구10: 카드소유자 데이터와 네트워크 자원에 대한 모든 접근의 모니터링과 추적 - 요구11: 보안시스템과 절차의 정기적인 검사
정보보안 정책의 유지	- 요구12: 고용직원 및 하청업자 등에 대한 정보보안 정책의 유지

이상의 국외 보안 표준은 우리기업에서 향후 클라우드 컴퓨팅을 도입할 때 검토하여야할 주요한 기준이 된다. 무엇보다도 보안이 우선시되어야 하는 클라우드 컴퓨팅에서 이러한 기준에 따른 시스템의 도입과 서비스의 제공으로 클라우드 컴퓨팅 서비스를 안전하게 이용할 수 있게 된다.

ISO27001은 국제 표준화 기구에서 제정하여, 국제적으로 인정받는 표준으로, 정보보호 관리체계에 대한 유일한 국제 인증으로써의 희소성을 가지고 있으며, 기존의 다른 ISO 인증제도에 영향을 미치고 있다. ISO9001(품질경영시스템), ISO14001(환경경영시스템) 등 기존의 ISO 관련 인증 제도가 국제 표준으로써 성공적으로 정착하여, ISO27001의 경우 그 영향을 받아 국제 표준으로 빠르게 인식되어지고 있으며, 한편 기업의 입장에서 보면, 기업의 정보보호 수준을 국제적인 수준으로 향상시킬 수 있으며, 해외 사업을 하는 경우 이에

대한 부분을 대외적으로 인식시킬 수 있다.

또한 SAS 70으로 보안을 완전히 보증할 수 있는 것은 아니지만 SaaS를 중심으로 한 보안 프로세스를 점검하는데 도움이 된다. 보안에 있어서 SaaS 서비스 업체가 매년 SAS 70 II와 같은 독립적인 보안 감사 기관의 감사를 받았는지 살펴야 하며, 보안 감사 결과 보고서를 정기적으로 요구하는 것이 필요하다. 그리고 국내에서도 PCI DSS 기준이 의무화 되어 있지 못하나 향후 클라우드 컴퓨팅 서비스가 지불방식에도 변화를 가져올 것이며 이러한 기준의 의무화를 통해 보안을 강화해야 할 것이다.

4) 기타

이상의 인증관련 기준이외에도 민간 기업에서 최근에 클라우드 환경에서의 정보보안의 최선의 방법을 가이드로 제시하고 있다. 2009년 11월 세계적인 정보보안 기업인 EMC의 RSA 정보보안 사업부는 클라우드 환경에서의 정보보안 가이드를 발표하였다. 클라우드환경을 위한 ID와 정보의 보안: 신뢰환경 구축을 위한 최신사례(Identity and Data Protection in the Cloud: Best Practices for Establishing Environments of Trust)'보고서를 통해 클라우드서비스의 신뢰환경 구축을 통해 기업 데이터 및 사용자의 정보보호를 위한 방법과 방향을 제시하고 있다. 본 보고서에는 ① 클라우드서비스 구조에서 신뢰관계 구축, ② 컴플라이언스와 사기범죄 등에서 보안유지 방안, ③ 데이터 규정 준수 등의 3개 분야로 나눠 설명하고 있다.[47)]

2. 클라우드 컴퓨팅 보안을 위한 국내 법, 제도 및 인증 현황

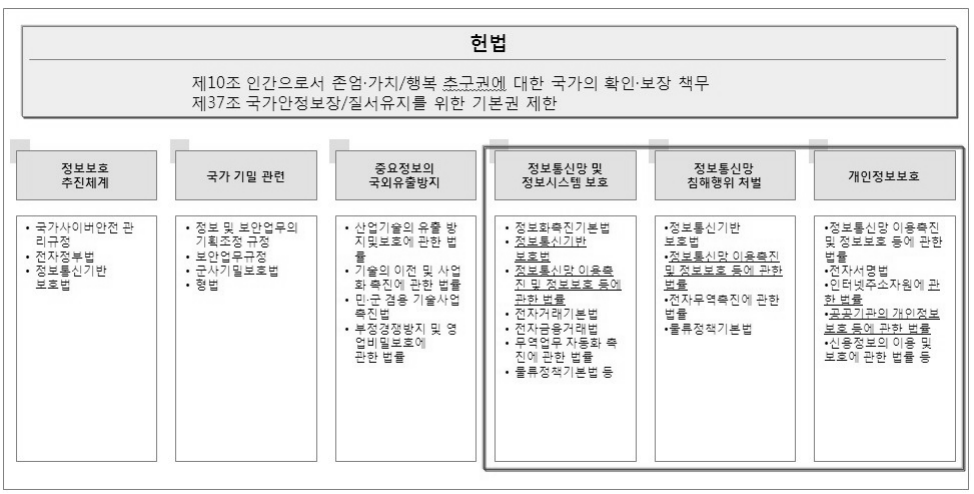
본 장에서는 클라우드 컴퓨팅 서비스의 특징을 고려하여 클라우드 컴퓨팅 서비스 제공자에 대한 보안 관련 국내 법·제도에 대한 현황 및 문제점을 파악해 보고자 한다.

가. 국내 법, 제도 및 인증 현황

국내에서 클라우드 컴퓨팅 정보보안과 관련된 법률체계는 다음과 같이 매우 광범위하다.

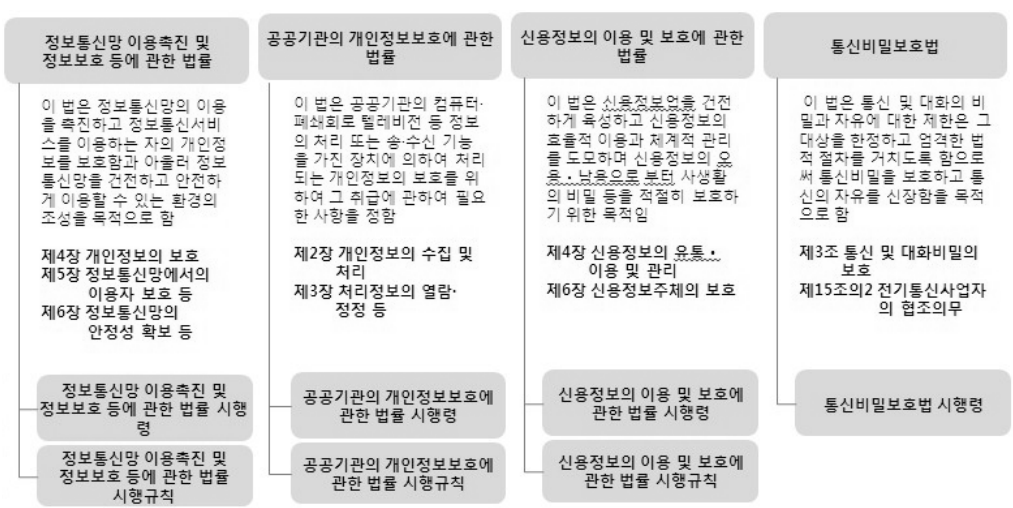
47) RSA(2009. 11), 'Identity & Data Protection in the Cloud'

〈그림 3-14〉 현행 정보보안 법률체계



그러나 핵심적으로 연관될 수 있는 법률은 〈그림 3-15〉와 같이 4가지로 정리할 수 있다.

〈그림 3-15〉 클라우드 컴퓨팅 서비스 시행 시 관련 주요 법률



이들 4개의 법률에 대해 관련항목과 주요 관련 사항은 〈표 3-19〉과 같다.

〈표 3-19〉 클라우드 컴퓨팅 서비스 관련 주요 법률

구 분	대 상	관련 항목	주요 관련 사항
정보통신망 이용촉진 및 정보보호에 관한 법률	민간	제4장 개인정보의 보호 제5장 정보통신망에서의 이용자 보호 등 제6장 정보통신망의 안전성 확보 등 - 안전진단 제도 - 정보보호관리체계인증	o 해당 법률은 정보통신서비스를 이용하는 자의 개인정보를 보호와 정보통신망을 안전하게 이용할 수 있는 환경조성이 주요 목적 o 클라우드 컴퓨팅 서비스 제공 시 이 서비스를 이용하는 이용자의 개인정보에 대한 보호이슈 및 보안관련 규제 관한 법이 직접적으로 연관
공공기관의 개인정보보호에 관한 법률	공공	2장 개인정보의 수집 및 처리 3장 처리정보의 열람, 정정 등	o 해당 법률은 공공기관의 정보처리 시 개인정보의 보호를 위해 그 취급에 관해 필요한 사항을 정의 o 공공기관의 정보처리 서비스가 클라우드 환경에서 이루어질 경우, 개인정보보호이슈는 이 법과 직접적으로 연관
신용정보보호법	금융	4장 신용정보의 유통 및 관리 6장 신용정보주체의 보호	o 해당 법률은 신용정보의 오용, 남용으로부터 사생활의 비밀을 보호하기 위한 목적o 신용정보의 처리가 클라우드 환경에서 이루어질 경우, 정보보호이슈는 이 법과 직접적으로 연관되어 있다.
통신비밀보호법	전체	3조 통신 및 대화비밀의 보호 15조 전기통신사업자의 협조 의무	o 해당 법률은 국민의 통신 비밀을 보호하기 위한 목적. 그러나 국가보안사범과 범죄사건에 대해서는 예외적인 감청과 검열을 허용 o 클라우드 컴퓨팅 서비스 환경에서의 검열과 감청에 대해 이 법은 직접적 연관

이 법률들 가운데에서 클라우드 컴퓨팅 서비스 사업자의 보안에 가장 직접적인 연관이 되는 법률은 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』이다. 본 법률의 적용 대상자는 정보통신 서비스 대상자로서 전기통신사업법 제2조 제1항 제1호에 따른 전기통신사업자와 영리를 목적으로 하는 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로 규정되어 있다[48]. 특히 본 법률 중 클라우드 컴퓨팅과 관련이 있는 영역은 정보보호 안전 진단 제도와 정보보호관리체계 인증 제도이다. 이에 두 영역을 중심으로 현황과 클라우드 컴퓨팅 적용 시 이슈에 대해 검토한다.

48) "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 일부 인용

1) 정보보호 안전진단제도

정보보호 안전진단은 정보통신망 이용촉진 및 정보보호에 관한 법률 제46조의 3에서 정하는 자인 전기통신사업자, 집적정보통신시설 사업자 등을 대상으로 한다. 그 목적은 ISP, IDC, 쇼핑몰 등의 정보통신망에 대한 침해사고 예방을 위하여 해당 업체 혹은 기관들이 관리적, 기술적, 물리적 정보보호지침을 이행하고, 안전진단을 받게 함으로써 정보통신망 및 정보통신서비스에 대한 안정성 및 신뢰성을 확보하고자 하는 것이다[49]. 현재 클라우드 컴퓨팅 서비스를 수행하는 업체도 일부는 정보통신망 이용촉진 및 정보보호에 관한 법률의 정보통신서비스 제공자에 해당된다.

안전진단 수행기관은 안전진단 대상 기업들의 정보통신망 또는 집적정보통신시설에 대하여 매년 정보보호지침에 따른 정보보호 안전진단을 수행 한다. 이 경우 안전진단 수행기관은 15명 이상의 정보보호 기술 인력을 보유하고 최근 3년 이내에 정보보호컨설팅을 수행한 실적이 있는 법인이어야 한다.[50]. 현재 안전진단 기준은 21개 항목의 관리적 보호조치, 24개의 기술적 보호조치, 3개의 물리적 보호조치의 총 48개 세부조치 항목으로 구성되어 있고 안전진단대상별 기준 항목 수는 〈표 3-20〉와 같다.

〈표 3-20〉 안전진단대상별 기준 항목수

구분		총	ISP	IDC	VIDC	기타
관리적	정보보호 조직의 구성·운영	5	5	5	1	5
	정보보호계획 등의 수립 및 관리	6	6	6	0	6
	인적보안	5	5	5	5	5
	이용자 보호	1	1	1	1	1
	침해사고 대응	1	1	1	1	1
	정보보호조치 점검	1	1	1	1	1
	정보자산 관리	2	2	2	2	2
기술적	네트워크 보안	3	3	2	0	1
	정보통신설비 보안	21	21	13	7	19

49) http://www.kisa.or.kr/kisa/iscs/jsp/iscs.jsp
50) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조의 3

〈표 3-20〉 안전진단대상별 기준 항목수(계속)

구분		총	ISP	IDC	VIDC	기타
물리적	출입 및 접근보안	2	0	2	0	0
	부대설비 및 시설 관리 운영	1	1	1	0	0
합계		48	48	39	18	41

이행해야 할 관리적, 기술적, 물리적 조치의 구분별 세부내용은 〈표 3-24〉와 같다.

〈표 3-21〉 안전진단 구분별 세부내용

구분		세부내용
관리적	정보보호 조직의 구성·운영	- 정보보호조직의 구성 - 정보보호책임자의 지정 - 정보보호조직 구성원의 역할
	정보보호계획 등의 수립 및 관리	- 정보보호방침의 수립·이행 - 정보보호실행계획의 수립·이행 - 정보보호실무지침의 마련 준수
	인적보안	- 내부인력 보안 - 외부인력 보안 - 위탁운영 보안
	이용자 보호	- 정보보호 정보제공
	침해사고 대응	- 침해사고 대응계획의 수립·이행
	정보보호조치 점검	- 보호조치의 자체 점검
	정보자산 관리	- 정보통신설비 및 시설의 현황관리
기술적	네트워크 보안	- 트래픽 모니터링 - 무선서비스 보안 - 정보보호시스템 설치·운영

〈표 3-21〉 안전진단 구분별 세부내용(계속)

구분		세부내용
기술적	정보통신설비 보안	- 웹서버 보안 - DNS 서버보안 - DHCP 서버보안 - DB 서버보안 - 라우터/스위치보안 - 정보보호시스템 보안 - 취약점 점검 - 접근통제 및 보안설정 관리 - 관리자 계정의 비밀 번호 관리 - 로그관리 - 보안패치 관리 - 백업 및 복구
물리적	출입 및 접근보안	- 정보통신시설의 출입·접근 통제
	부대설비 및 시설 관리 운영	- 백업설비 및 시설 설치·운영

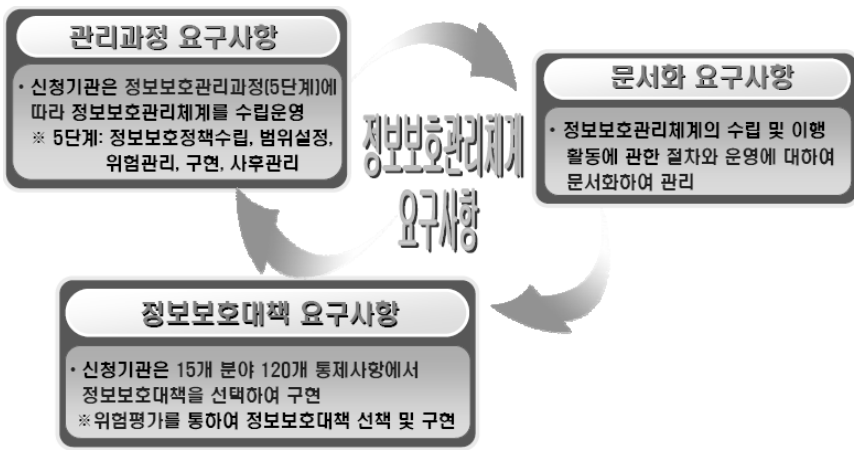
2) 정보보호관리체계 인증

정보보호관리체계 인증은 정보통신망 이용촉진 및 정보보호에 관한 법률 제47조에 의해 제공된다. 해당 법률의 목표는 정보통신망의 안정성 및 신뢰성을 확보하기 위하여 기술적·물리적 보호조치를 포함한 종합적 관리체계를 수립 및 운영하도록 하여 국내 정보보호 수준을 향상 시키고자 하는 것이다. 본 관리체계 인증은 정보보호 관리과정, 문서화, 정보보호 대책 3부분으로 구성되어 있다. 정보보호 관리과정은 5단계, 14가지의 통제사항으로 구성되고, 문서화 과정은 3개의 통제사항으로 구성되며, 정보보호 대책은 15분야, 120개 통제사항으로 구성된다.

관리체계 인증을 받는다는 의미는 정보보호 정책 수립, 관리체계의 범위설정, 위험관리, 구현, 사후 관리, 문서화, 정보보호를 위한 실질적인 자산의 분류, 조직구성, 교육·훈련, 접근 통제 등 기술적 내용을 모두 포함하는 대책을 갖추고 있음을 인정받는다는 것이다.

정보보호 인증을 받기 위해서는 다음 그림과 같이 관리과정 요구사항, 문서화 요구사항, 정보보호 대책 요구사항을 만족시켜야 한다.

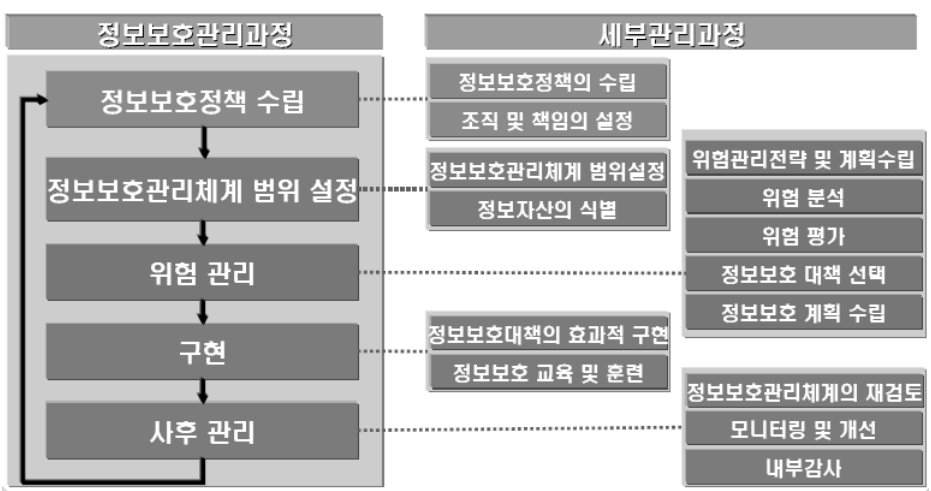
〈그림 3-16〉 정보보호관리체계



출처: KISA 정보보호관리체계 인증 소개자료

이 중 정보보호 관리과정 요구사항은 다음과 같이 정보보호정책 수립부터 사후 관리까지 5단계로 구성되어 있다.

〈그림 3-17〉 정보보호 관리과정 요구사항



출처: KISA 정보보호관리체계 인증 소개자료

정보보호관리체계 가운데서 문서화 요구사항은 다음과 같다.

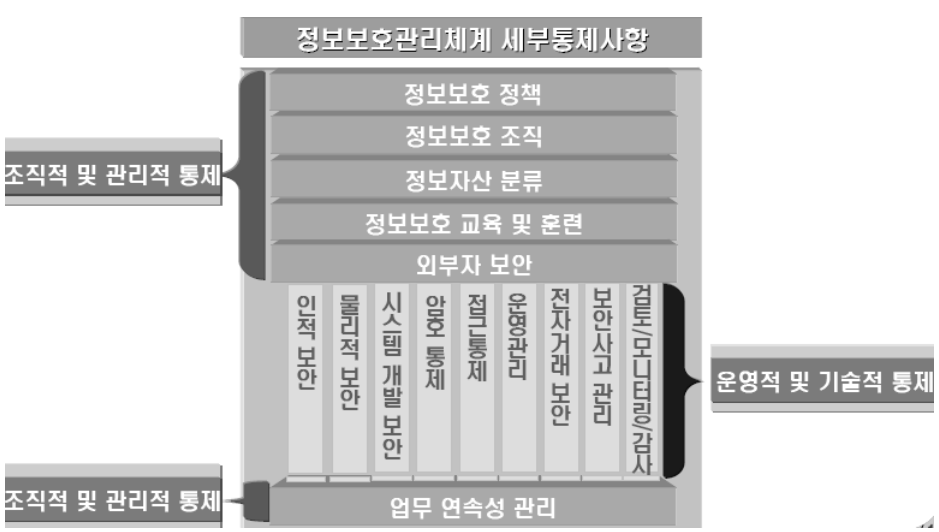
〈표 3-22〉 문서화 요구사항

구 분	항 목	내 용
문서화 요구사항	문서요건	정보보호관리체계 수립 및 이행 관련 내용의 문서화
	문서의 통제	문서 관리의 통제를 정의한 절차 수립 및 이행
	운영기록의 통제	정보보호관리체계 운영 기록 절차 수립 및 유지관리
요구문서	정보보호 정책서	
	위험분석 평가보고서	
	정보보호 계획서	
	정보보호 대책 명세서	
	정보보호관리체계 내부감사 결과보고서	
	주요정보통신설비의 목록과 시스템 구성도	
	정보보호 관례체계와 관련 있는 주요문서 목록	

출처: KISA 정보보호관리체계 인증 소개자료

정보보호 대책 요구사항은 다음의 표와 같이 조직적 및 관리적 통제대책, 운영적 및 기술적 통제대책의 두 가지로 나뉘어져 있다.

〈그림 3-18〉 정보보호 대책 요구사항



출처: KISA 정보보호관리체계 인증 소개자료

나. 현재 법/제도의 클라우드 컴퓨팅 서비스 환경 적용 시 이슈

4개의 법률에 대해 클라우드 컴퓨팅 서비스 환경 적용 시 주요 이슈는 다음과 같다.

〈표 3-23〉 클라우드 컴퓨팅 서비스 환경 적용 시 주요 이슈

	대상	관련 항목	적용 시 주요 이슈
정보통신망 이용촉진 및 정보보호에 관한 법률	민간	제4장 개인정보의 보호 제5장 정보통신망에서의 이용자 보호 등 제6장 정보통신망의 안전성 확보 등 - 안전진단 제도 - 정보보호관리체계인증	- 현재의 법률로도 클라우드 컴퓨팅 사업자에 대한 정보보호를 규제할 수 있음 - 해당 법률은 IDC, ISP 등 기존 정보통신 서비스 사업자에 대해서는 서비스 제공 시 보안의무에 대해서 구체적으로 명시하고 있으나 클라우드 컴퓨팅 서비스 제공자에 대해서는 명시하지 않았기 때문에 클라우드 컴퓨팅 사업자가 구체적으로 어느 그룹에 해당될 지 논란의 소지가 있음 - 데이터의 물리적 위치 변경 시 데이터 보호 및 프라이버시 대응 요건이 충분히 제시되지 않고 있음 - 데이터를 보호하고 있는 물리적 위치가 해외일 경우 서비스 제공자의 물리적 시설에 대한 점검관련 법규 적용을 어떻게 해야 하는지 불명확 - 안전진단 제도는 클라우드 컴퓨팅 서비스 사업자의 환경을 충분히 반영하지 못함 - 정보보호관리체계 인증도 일반적인 보안항목을 기준으로 일반적인 사업자를 대상으로 하고 있어 클라우드 컴퓨팅 환경에는 적용되기 어려움
공공기관의 개인정보보호에 관한 법률	공공	2장 개인정보의 수집 및 처리 3장 처리정보의 열람, 정정 등	- 현재의 법률로도 클라우드 환경에서의 개인정보 보호를 규제할 수 있음 - 그러나 데이터가 국외에 물리적으로 분산되어 있을 경우에 해당 법률이 적용 가능한가의 이슈 - 데이터가 국외로 이동 시 해당 외국정부에서 데이터를 조사할 수 있는 권한이 있는 경우 국내 공공기관이 클라우드 컴퓨팅 서비스를 받도록 허용할지 이슈

〈표 3-23〉 클라우드 컴퓨팅 서비스 환경 적용 시 주요 이슈(계속)

	대상	관련 항목	적용 시 주요 이슈
신용정보보호법	금융	4장 신용정보의 유통 및 관리 6장 신용정보주체의 보호	- 현재의 법률로도 클라우드 환경에서의 개인정보나 신용정보보호를 규제할 수 있음 - 그러나 데이터가 국외에 물리적으로 분산되어 있을 경우에 해당 법률이 적용 가능한가의 이슈 - 데이터가 국외로 이동 시 해당 외국정부에서 데이터를 조사할 수 있는 권한이 있는 경우 국내 금융기관이 클라우드 컴퓨팅 서비스를 받도록 허용할지 이슈
통신비밀보호법	전체	3조 통신 및 대화비밀의 보호 15조 전기통신사업자의 협조 의무	데이터가 국외에 분산되어 있을 경우 협조의무에 대해 해당 법률이 적용 가능한가의 이슈 존재

특히 본 법률 중 클라우드 컴퓨팅과 직접적인 관련이 있는 정보보호 안전 진단 제도와 정보보호관리체계 인증 제도의 적용 시 세부적인 이슈는 다음과 같다.

1) 정보보호 안전진단제도

안전진단 제도의 경우 현재 대상에 클라우드 컴퓨팅 서비스제공자가 별도로 명시되어 있지 않다. 이에 먼저 아래의 표와 같이 클라우드 컴퓨팅 서비스 제공자를 별도 대상으로 신설해야 한다.

〈표 3-24〉 클라우드 컴퓨팅 서비스 제공자 대상 신설 사항

구 분		총	ISP	IDC	VIDC	기타	클라우드 컴퓨팅 서비스제공자 (신설 필요)
관리적	정보보호 조직의 구성·운영	5	5	5	1	5	기존의 항목 적용
	정보보호계획 등의 수립 및 관리	6	6	6	0	6	
	인적보안	5	5	5	5	5	
	이용자 보호	1	1	1	1	1	
	침해사고 대응	1	1	1	1	1	
	정보보호조치 점검	1	1	1	1	1	
	정보자산 관리	2	2	2	2	2	
기술적	네트워크 보안	3	3	2	0	1	수정 보완 필요
	정보통신설비 보안	21	21	13	7	19	
물리적	출입 및 접근보안	2	0	2	0	0	
	부대설비 및 시설 관리 운영	1	1	1	0	0	
합 계		48	48	39	18	41	

또한 클라우드 컴퓨팅 서비스 제공자를 위한 세부 보호조치를 정의해야 한다. 기존의 관리적 보호조치는 클라우드 컴퓨팅 서비스 제공자에게도 동일하게 적용될 수 있다. 그러나 기술적, 물리적 보호조치는 적용을 위해서는 수정, 보완되어야 한다. 클라우드 컴퓨팅 서비스 제공자에게 기술적, 물리적 보호조치를 적용하기 위해서는 1) 현재의 IDC나 ISP서비스 제공자에게 요구하는 보안조치 보다 전반적인 보안대책이 강화되어야 하며, 2) 클라우드 컴퓨팅 서비스 제공자에게는 접근통제, 데이터 보안과 서비스 보안이 더 강화되어 요구되어야 한다.[51].

51) 현재의 IDC나 ISP서비스 제공자에게 요구하는 보안 조치는 네트워크 보안과 서버 보안이 중심이 되고 있다.

〈표 3-25〉 안전진단의 기술적 보호조치 및 클라우드 컴퓨팅 서비스 적용 시 미흡항목

안전진단 항목	세부구분	충분	불충분	클라우드 컴퓨팅 적용 시 미흡항목
네트워크 보안	트래픽 모니터링		○	
	무선서비스 보안	○		
	정보보호시스템 설치・운영	○		
정보통신설비 보안	웹서버 보안	○		
	DNS 서버 보안	○		
	DHCP 서버 보안	○		
	DB 서버 보안		○	DB보안이 초점이 되는 것이 아니라 데이터 보안이 초점이 되어야 함. 프라이버시 항목도 별도로 정의되어야 함
	라우터/스위치 보안	○		
	정보보호 시스템 보안	○		
	취약점 점검		○	클라우드 컴퓨팅에 특화된 점검항목 필요
	접근통제 및 보안설정 관리		○	서비스에 대한 접근통제가 더욱 강화되고 차별화 되어야 함
	관리자 계정의 비밀번호 관리	○		
	로그 관리		○	클라우드 컴퓨팅에 특화된 점검항목 필요
	보안패치 관리	○		
	백업 및 복구		○	클라우드 컴퓨팅에 특화된 점검항목 필요

IDC나 ISP의 경우 물리적 환경이 단일화 되어 있어 물리적 보안영역이 명확하다. 그러나 클라우드 컴퓨팅 서비스의 경우 물리적 환경이 분산된다. 이에 물리적 보안의 영역이 클라우드 컴퓨팅 서비스를 제공하는 모든 물리적 환경으로 확대되어야 한다.

〈표 3-26〉 안전진단의 물리적 보호조치 및 클라우드 컴퓨팅 서비스 제공자 적용 시 미흡항목

안전진단 항목	세부구분	충분	불충분	클라우드 컴퓨팅 적용 시 미흡항목
출입 및 접근 보안	정보통신시설의 출입・접근 통제		○	클라우드 컴퓨팅 서비스를 하는 모든 영역으로 확대
부대설비 및 시설 운영・관리	백업설비 및 시설 설치・운영		○	클라우드 컴퓨팅 서비스를 하는 모든 영역으로 확대

또한 현재의 안전진단 수행기관이 수행하는 안전진단은 국내 영토 내에서 벌어지는 정보통신서비스의 행위에만 국한되는 것으로 국경을 넘어서는 정보통신 서비스 행위에 대한 지침이 별도로 검토되어야 한다. 기타 정보통신망 이용촉진 및 정보보호 등에 관련된 몇 가지 항목에 있어도 조금 더 구체적인 보완이 필요하다. 기본적으로 클라우드 컴퓨팅은 인터넷을 통해 동적으로 확장 가능한 가상화된 컴퓨팅 자원을 서비스하는 것이다. 이러한 클라우드 컴퓨팅의 서비스 특성으로 인하여 서비스의 제공자와 사용자의 물리적 위치의 상이함에 따른 문제와 데이터의 물리적 위치에 따라 법률의 적용이 어려울 수 있다는 것이 기존 법률의 한계이다.

2) 정보보호관리체계 인증

KISA의 정보보호관리체계인증을 클라우드 컴퓨팅에 적용할 경우 적용 가능한 영역과 한계 영역이 존재한다. 이는 KISA의 정보보호관리체계 인증뿐 아니라 ISO27001도 동일하게 가지고 있는 이슈이다. KISA의 정보보호관리체계 인증은 기업의 일반적인 정보보호환경에 포괄적으로 적용하기 위해서 설계되었기 때문에 전반적인 인증 프레임워크는 클라우드 컴퓨팅에서도 동일하게 적용할 수 있다. 즉, 인증심사 절차, 인증 심사원 교육 등의 인증관리적인 요소들은 동일하게 적용할 수 있다는 의미이다. 또한 '관리과정 요구사항'도 동일하게 적용할 수 있다. 클라우드 컴퓨팅 보안도 일반 보안과 동일하게 정보보호정책을 정의해야 하고, 범위를 정하며, 위험평가를 수행하고 이에 따른 대책을 구현하며 사후관리 해야 한다.

그러나 정보보호대책 요구사항은 동일하게 적용하기 어렵다. KISA의 정보보호관리체계의 세부 통제사항들은 특수한 환경에 적합한 사항이 아니라 일반적 보안영역에 관련된 사항이기 때문에 광의로 해석한다면 클라우드 컴퓨팅 서비스 보안영역에 대해서도 적용할 수 있다. 그러나 클라우드 컴퓨팅 환경에서 조금 더 적합한 서비스개발보안, 접근통제, 운영보안 등에 대해서 현재 인증 항목들이 충분히 다루기 어렵다. 적용하기에 미흡한 영역은 다음의 표에서 제시하였다.

〈표 3-27〉 정보보호관리체계 인증 통제항목 및 클라우드 컴퓨팅 적용 시 미흡항목

통제 분야	세부통제사항	충분	불충분	클라우드 컴퓨팅 적용 시 미흡영역
정보보호 정책	정책의 승인 및 공표, 정책의 체계, 정책의 유지관리	○		
정보보호 조직	조직의 체계, 책임과 역할	○		
외부자 보안	계약 및 서비스 수준협약, 외부자 보안			
정보자산 분류	정보자산의 조사 및 책임할당, 정보자산의 분류 및 취급			
정보보호 교육 및 훈련	교육 및 훈련프로그램 수립, 교육훈련의 시행 및 평가	○		
인적보안	책임할당 및 규정화, 직원의 적격 심사, 주요직무 담당자 관리, 비밀유지	○		
물리적 보안	물리적 보호구역, 물리적 접근통제, 데이터 센터 보안, 장비보호, 사무실 보호	○		
시스템개발 보안	분석 및 설계, 구현 및 이행, 변경관리		○	클라우드 컴퓨팅 서비스 개발을 위한 보안항목 미흡
암호통제	암호정책, 암호사용, 키관리	○		
접근통제	접근통제 정책, 사용자 접근 관리, 접근통제 영역		○	클라우드 컴퓨팅 서비스에 특화된 접근통제 항목 미흡
운영관리	운영절차와 책임, 시스템 운영, 네트워크 운영 및 문서 관리, 악성소프트웨어 통제, 원격 컴퓨터 및 원격 작업		○	클라우드 컴퓨팅 운영에 관련된 특화된 보안항목 미흡
전자거래 보안	교환합의서, 전자거래, 전자우편, 공개서버의 보안관리, 이용자 공지사항	○		
보안사고 관리	대응계획 및 체계, 대응 및 복구, 사후관리	○		
검토, 모니터링 및 감사	법적 요구사항 준수 검토, 정보보호 정책 및 대책 준수 검토, 모니터링, 보안감사	○		
업무연속성 관리	업무연속성 관리체계 수립, 업무연속성 계획 수립과 구현, 업무연속성 계획 시험 및 유지관리		○	클라우드 컴퓨팅에 특화된 업무연속성 관리 항목 미흡

3. 클라우드 컴퓨팅 보안을 위한 법·제도 개선의 필요성 및 개선방안

클라우드 컴퓨팅 서비스는 가상화 (Virtualization) 기반기술을 이용하며, 이는 사용자에게 보이는 하나의 논리적 서버를 구현하기 위하여 물리적으로 분산되어 있는 독립적인 여러 개의 작은 서버들을 논리적으로 결합하는 방식으로 구현된다. 이러한 기술적인 특징 때문에 클라우드 컴퓨팅 서비스 제공자의 보안 관련 규제를 위한 현행 법규는 그대로 적용하기 어려운 것이 현실이다. 이로 인해 보안의 신뢰성을 제공하지 못한다면 이 서비스의 활성화는 요원하다고 할 수 있다.

국외의 법, 제도 현황 분석 결과 클라우드 컴퓨팅 서비스 보안에 특화된 법, 제도는 아직까지 제시되지 않고 있고 기존의 법, 제도를 기반으로 클라우드 컴퓨팅 서비스 보안을 요구하고 있다. 그러나 최근 미국 등을 중심으로 '클라우드 컴퓨팅데이터보호법'에 관한 논의가 이루어지고 있고 일본의 경우 2008년 'ASP, SaaS의 정보보안 대책 가이드라인'이 공표되어 전체 Cloud서비스 제공자는 아니지만 ASP, SaaS사업자의 서비스에 대한 정보보안대책에 대한 지침을 제시하고 있다.

클라우드 컴퓨팅 서비스 보안에 특화된 보안 인증제도도 아직은 마련되어 있지 않다. 그러나 주요 클라우드 컴퓨팅 서비스 제공자들은 자사 서비스의 신뢰성을 고객에게 제시하기 위해 기존의 보안 인증제도인 ISO27001이나 SAS70을 활용하고 있었다. 또한 최근에는 CSA를 중심으로 클라우드 컴퓨팅 서비스에 특화된 보안인증제도 수립을 준비하고 2010년 초에 이를 발표할 예정으로 있다. 국내도 마찬가지로 클라우드 컴퓨팅 서비스 보안에 특화된 법, 제도는 아직 제시되어 있지 않다.

'정보통신망 이용촉진 및 정보보호에 관한 법률'은 현재의 법률로도 클라우드 컴퓨팅 사업자에 대한 정보보호를 규제할 수 있으나 I) 해당 법률은 IDC, ISP 등 기존 정보통신 서비스 사업자에 대해서는 서비스 제공 시 보안의무에 대해서 구체적으로 명시하고 있으나 클라우드 컴퓨팅 서비스 제공자에 대해서는 명시하지 않았기 때문에 클라우드 컴퓨팅 사업자가 구체적으로 어느 그룹에 해당될 지 논란의 소지가 있고, ii) 데이터의 물리적 위치 변경 시 데이터 보호 및 프라이버시 대응 요건이 충분히 제시되지 않고 있으며, iii) 데이터를 보호하고 있는 물리적 위치가 해외일 경우 서비스 제공자의 물리적 시설에 대한 점검관련 법규 적용을 어떻게 해야 하는지 불명확하고 iv) 안전진단 제도는 클라우드 컴퓨팅 서비스 사업자의 환경을 충분히 반영하지 못하며 v) 정보보호관리체계 인증도 일반적인 보안항목을 기준으로 일반적인 사업자를 대상으로 하고 있어 클라우드 컴퓨팅 환경에는 완벽히 적

용되기 어려운 문제점이 있다.

‘공공기관의 개인정보보호에 관한 법률’ 이나 ‘신용정보보호법’, ‘통신비밀보호법’도 현재의 법률체계로 클라우드 환경에서의 개인정보나 신용정보보호를 규제할 수 있으나 I) 데이터가 국외에 물리적으로 분산되어 있을 경우 법률 적용의 이슈 ii) 데이터가 국외로 이동 시 해당 외국정보에서 데이터를 조사할 수 있는 권한이 있는 경우 국내 공공기관이나 금융기관에 클라우드 컴퓨팅 서비스를 받도록 허용할 지 등의 이슈가 해결되지 않고 있다.

일부 클라우드 컴퓨팅 서비스 제공자들은 안전진단이라는 제도 하에서 매년 의무적으로 서비스의 보안성 검증을 받고 있으며, 정보보호관리체계 인증을 통해 자사 서비스의 신뢰성을 외부로 표현할 수 있다.

그러나 안전진단제도가 클라우드 컴퓨팅 서비스에 특화되지 않아 클라우드 컴퓨팅 서비스의 신뢰성을 보장해 줄 수 없으며 모든 클라우드 컴퓨팅 서비스 제공자에게 해당되지 않을 수 있다. 또한 정보보호관리체계 인증도 일반적인 보안 인증제도일 뿐 아니라 강제성이 없어 고객들에게 클라우드 컴퓨팅 서비스의 신뢰성을 검증해 줄 수 있는 제도적 장치는 없다고 해도 과언이 아니다. 이러한 법, 제도 상황 하에서 고객들이 안심하고 클라우드 컴퓨팅 서비스를 받기는 어렵다. 이에 따라 클라우드 컴퓨팅 서비스 활성화를 위해서는 보안관련 법, 제도의 개선이 필수적이다.

현행 법 체계를 볼 때 클라우드 컴퓨팅 보안관련 법, 제도 변화에는 다음과 같은 방향이 필요하다.

- o 클라우드 컴퓨팅 서비스 제공자의 보안/데이터보호 신뢰성 제고를 위한 법규 신설
  클라우드 컴퓨팅 서비스 제공자가 자사의 서비스에 대해서 보안 대책을 충분히 이행하고 클라우드 컴퓨팅 특성에 맞는 데이터보호를 충분히 하고 있음을 보장할 수 있도록 하는 법규 신설 필요
- o 공공/금융기관에 대한 클라우드 컴퓨팅 서비스 사용 정책에 대한 법규 보완
  데이터가 국외로 분산되는 경우 국내의 공공/금융기관이 클라우드 컴퓨팅 서비스를 받도록 허용할지의 여부 제시
- o 감사/감독/수사의 관련된 정책에 대한 법규 보완
  데이터가 글로벌하게 분산 시 해당 데이터 및 데이터를 보관하고 있는 시스템, 시설에 대한 감사, 감독, 필요 시 수사를 현재의 국내 법 체계로 대응할 수 있는지 점검

이러한 대응을 위해서 통합된 ‘클라우드 컴퓨팅 보안 법’을 신설할 필요까지는 없다. 기

존의 법체계에서도 클라우드 컴퓨팅 보안에 특화되지는 않았지만 공통되는 부분은 상당히 다두고 있기 때문에 기존의 법규 중 미진한 부분을 보완하되, 신설할 부분을 신설하는 것이 효율적일 수 있다.

이러한 방향 하에서 2) 3)번은 기존의 법을 약간 보완하는 수준으로 접근하고 1)을 위해서는 '클라우드 컴퓨팅 서비스 제공자에 대한 정보보호 법규' 또는 '클라우드 컴퓨팅 데이터 보호에 관한 법규' 항목을 신설하여 추가 반영할 필요가 있다.

추가 반영이 필요한 보안규정은 클라우드 컴퓨팅 관련 독립된 신규 법률에 포함하는 방안과 기존의 '정보통신망 이용촉진 및 정보보호에 관한 법률'에 추가하여 반영하고 세부 지침을 제시하는 방안이 있다. 정보통신서비스 제공자에 대한 보안관련 지침이 기존의 '정보통신망 이용촉진 및 정보보호에 관한 법률'에 대부분 포함되어 있으므로 여기에 클라우드 컴퓨팅 보안 관련 항목을 반영하는 것이 더 효율적이라 할 수 있다.

클라우드 컴퓨팅 보안관련 규정에는 데이터의 물리적 위치 변동에 따른 관리, 해킹대응 방안, 접근권한, 프라이버시 침해방지, 데이터 유출 방지, 수사/소송 시 협조 등의 항목이 반영되어야 한다. 또한 기존의 안전진단 제도에도 클라우드 컴퓨팅 서비스 제공자 그룹이 추가로 반영되어야 한다.

〈표 3-28〉 클라우드 컴퓨팅 보안 관련 항목 추가 사항

	대상	이슈	법 제도 방향
정보통신망 이용촉진 및 정보보호에 관한 법률	민간	- 현재의 법률로도 클라우드 컴퓨팅 사업자에 대한 정보보호를 규제할 수 있음 - 해당 법률은 IDC, ISP 등 기존 정보통신 서비스 사업자에 대해서는 서비스 제공 시 보안의무에 대해서 구체적으로 명시하고 있으나 클라우드 컴퓨팅 서비스 제공자에 대해서는 명시하지 않았기 때문에 클라우드 컴퓨팅 사업자가 구체적으로 어느 그룹에 해당될 지 논란의 소지가 있음 - 데이터의 물리적 위치 변경 시 데이터 보호 및 프라이버시 대응 요건이 충분히 제시되지 않고 있음 - 데이터를 보호하고 있는 물리적 위치가 해외일 경우 서비스 제공자의 물리적 시설에 대한 점검관련 법규 적용을 어떻게 해야 하는지 불명확 - 안전진단 제도는 클라우드 컴퓨팅 서비스 사업자의 환경을 충분히 반영하지 못함 - 정보보호관리체계 인증도 일반적인 보안항목을 기준으로 일반적인 사업자를 대상으로 하고 있어 클라우드 컴퓨팅 환경에는 적용되기 어려움	- 클라우드 컴퓨팅 서비스 보안 관련 항목 신규 추가 - 클라우드 컴퓨팅 서비스 제공자를 위한 안전진단, 클라우드 컴퓨팅 서비스 인증제도 등 추가보완 필요

〈표 3-28〉 클라우드 컴퓨팅 보안 관련 항목 추가 사항(계속)

	대상	이슈	법 제도 방향
공공기관의 개인정보보호에 관한 법률	공공	- 현재의 법률로도 클라우드 환경에서의 개인정보 보호를 규제할 수 있음 - 그러나 데이터가 국외에 물리적으로 분산되어 있을 경우에 해당 법률이 적용 가능한가의 이슈 - 데이터가 국외로 이동 시 해당 외국정부에서 데이터를 조사할 수 있는 권한이 있는 경우 국내 공공기관이 클라우드 컴퓨팅 서비스를 받도록 허용할지 이슈	- 기존의 법률로 클라우드 환경에서 적용 가능함 - 제시된 이슈만 대응하여 보완하는 정도
신용정보 보호법	금융	- 현재의 법률로도 클라우드 환경에서의 개인정보나 신용정보보호를 규제할 수 있음 - 그러나 데이터가 국외에 물리적으로 분산되어 있을 경우에 해당 법률이 적용 가능한가의 이슈 - 데이터가 국외로 이동 시 해당 외국정부에서 데이터를 조사할 수 있는 권한이 있는 경우 국내 금융기관이 클라우드 컴퓨팅 서비스를 받도록 허용할지 이슈	- 기존의 법률로 클라우드 환경에서 적용 가능함 - 제시된 이슈만 대응하여 보완하는 정도
통신비밀 보호법	전체	데이터가 국외에 분산되어 있을 경우 협조의무에 대해 해당 법률이 적용 가능한가의 이슈 존재	- 기존의 법률로 클라우드 환경에서 적용 가능함 - 제시된 이슈만 대응하여 보완하는 정도

현재 시행 중인 안전진단 제도의 대상은 ISP, IDC, 쇼핑몰 등에 제한되어 있으므로 클라우드 컴퓨팅 서비스 대상자들은 이 제도에 포함되는 경우도 있고 그렇지 않은 경우도 있다. 이에 정보통신망법 개정을 통해 '클라우드 컴퓨팅 서비스 제공자'를 별도 대상그룹으로 하고 이들을 모두 이 제도에 포함시킬 필요가 있다. 이를 통해 클라우드 컴퓨팅 서비스 제공자 그룹들을 위한 안전진단 항목을 정의하고 이들이 모두 안전진단을 받게 함으로써 클라우드 컴퓨팅 서비스에 대한 안전성과 신뢰성을 확보하는 것이 바람직하다.

안전진단 제도에 클라우드 컴퓨팅 서비스를 포함시키기 위해서는 현재의 기술적 보호조치의 항목 및 세부구분 일부를 수정, 보완할 필요가 있다.

〈표 3-29〉 기술적 보호조치의 항목 및 세부구분 수정 사항

항목	세부구분	주요 개선사항
네트워크 보안	트래픽 모니터링	
	무선서비스 보안	
	정보보호시스템 설치·운영	
정보통신설비 보안	웹서버 보안	
	DNS 서버 보안	
	DHCP 서버 보안	
	DB 서버 보안	1. DB 서버 보안 (DBMS 포함) 2. 데이터 보안 - 암호화, 접근내역 관리 등
	라우터/스위치 보안	
	정보보호 시스템 보안	
	취약점 점검	
	접근통제 및 보안설정 관리	1. 인증/권한관리 보완 - 사용자 인증/권한관리 세분화 - 권한변경 내역의 기록관리 등 2. 접근통제 영역 추가 필요 - 모바일, VoIP를 통한 접근통제 - 가상화 서버 접근통제 - 어플리케이션/서비스 접근통제 등 - DB 접근통제 등
	관리자 계정의 비밀번호 관리	
	로그 관리	
	보안패치 관리	
	백업 및 복구	1. 백업 및 복구 - 서비스 이용자별 백업, 복구 체계 2. 사업연속성/재해 복구 - 서비스 다운타임 최소화 - 사업연속성 계획, 보고체계 등

법규 제정과 더불어 클라우드 컴퓨팅 서비스 제공자를 위한 보안 인증제도를 도입을 고려할 필요가 있다.

서비스 제공자들의 신뢰성을 보장받기 위해 가장 좋은 방안은 '인증제도'를 도입하는 것이다. 클라우드 컴퓨팅 서비스의 신뢰성을 보장받을 수 있는 통제기준들을 정의하고 이 기준을 충족하는 서비스 제공자에게 인증을 부여한다면 고객들이 해당 서비스를 신뢰하게 되고 서비스의 이용은 확대될 것이다. 또한 인증은 1회만 부여하는 것이 아니라 지속적인 유지관리를 통해 인증요건들을 지속적으로 만족하고 있음을 증명하여야 할 필요가 있다.

이 때 제 3자의 기관에서 인증된 제공자만이 서비스를 제공하게 해야 하는 것이 '보안'관점에서는 가장 바람직한 방안이지만 과도한 규제의 위험이 있다면 민간 기업들에 대한 서비스 제공시에는 선택적으로 할 수 있도록 하되, 공공기관에 대한 서비스 제공시에는 필수적으로 하게 하는 방안이 있다.

이에 클라우드 컴퓨팅 서비스 제공자를 위한 보안 인증제도 수립에는 1) 현재의 KISA 정보보호관리체계(ISMS) 인증제도를 활용하여' ISMS for 클라우드 컴퓨팅(가칭)' 인증제도를 수립하는 방안과 2)) 클라우드 컴퓨팅 서비스 제공자를 위한 독립적인 보안 인증제도를 만드는 두 가지 방안이 가능하다.

전자는 기존의 KISA의 정보보호인증제도를 활용하고 그 중 하나의 영역으로 클라우드 컴퓨팅 보안 인증제도를 지정하는 방안이다. 이 방안은 기존의 인증프로세스, 심사원 등 인증체계를 그대로 활용할 수 있다는 면에서 상당한 장점을 가지고 있다. 그러나 클라우드 컴퓨팅 서비스에만 국한된 것이 아니라 클라우드 컴퓨팅 서비스의 보안 문제가 명확히 해결되었다는 것을 인증하기 어려운 단점이 있다.

후자는 독자적인 인증제도를 수립하는 것이다. 클라우드 컴퓨팅 서비스 제공자를 위한 독자적인 인증제도인 만큼 범위도 명확하고 클라우드 컴퓨팅 서비스의 보안 이슈를 명확히 대응할 수 있다는 장점이 있다. 그러나 클라우드 컴퓨팅 보안만을 위한 별도의 인증제도를 운영하기 위해서는 비효율성이 존재한다. 물론 이 인증제도가 클라우드 컴퓨팅 보안에만 국한되는 것이 아니라 클라우드 컴퓨팅 서비스 전체 범위로 이루어지고, 보안은 그 중 하나의 요소로 위치한다면 이 방안은 효과성 뿐 아니라 효율성도 충분히 담보할 수 있다.

〈표 3-30〉 클라우드 컴퓨팅 보안 인증제도 수립 방안

방 안	장 점	단 점	권 고 안
KISA의 보안인증제도 활용	이미 기존의 인증 스킴이 있으므로 효율적	클라우드 컴퓨팅 서비스에 특화되지 않음	클라우드 컴퓨팅 서비스 보안만을 인증한다면 이 방안이 적합함
독립적 보안인증제도 수립	클라우드 컴퓨팅에 특화됨	클라우드 컴퓨팅 보안만을 고려한 인증은 비효율적	클라우드 컴퓨팅 서비스에 대한 전반적인 인증프로그램을 가져가고 보안은 그 중 하나라면 이 방안이 적합함

① 현재의 KISA ISMS 인증제도를 활용하는 방안

기존의 정보보호관리체계(ISMS) 인증 스킴(관리과정, 문서화, 정보보호대책 요구사항)은 그대로 유지하되, 클라우드 컴퓨팅 서비스 제공자를 위한 특화된 인증 항목들을 반영하여 'ISMS for 클라우드 컴퓨팅'을 개발하는 것이다. 이를 위해서는 정보보호인증을 위한 세부 통제사항 중에 접근통제, 운영 보안, 데이터 보안 등의 전반적인 내용을 수정, 보완하여 클라우드 컴퓨팅 서비스 제공자 환경에 보다 더 적합하도록 구성한다.

〈표 3-31〉 클라우드 컴퓨팅 서비스 제공자를 위한 정보보호대책 개선안(예시)

통제 분야	세부 통제사항	주요 개선사항
정보보호 정책	• 정책의 승인 및 공표 • 정책의 체계 • 정책의 유지관리	제공자의 자체 정책뿐만 아니라, 이용자별 서비스에 따라 차별화된 정보보호 정책 보유
정보보호 조직	• 조직의 체계 • 책임과 역할	1. 전담조직 의무화 - 정보보호 전담조직 및 인력 확보 (Dedicated) - 이용자의 Compliance 이슈 대응 인력 할당 2. 제공자와 계약을 한 다수의 보안시스템 벤더 책임, 역할 범위 명확화 3. 플랫폼/어플리케이션/데이터보안 등 영역별 전문가로 구성된 위원회 구성 운영
외부자 보안	• 계약/서비스 수준협약 • 외부자 보안	1. SLA 계약을 통한 보안요건 추가 의무화 (이용자/제공자, 제공자/벤더 등) 2. 외부자 통제요건 구체화 언급 필요 - 서약서 징구, 주기적인 교육 - 인증/권한관리, 접근통제, 감사(로깅 포함) - 법규 등 준수관리(compliance) 의무 준수 3. 이용자의 동의 없는 제3자 업무 위탁 및 정보제공 엄격한 제한 내용 포함

〈표 3-31〉 클라우드 컴퓨팅 서비스 제공자를 위한 정보보호대책 개선안(예시)(계속)

통제 분야	세부 통제사항	주요 개선사항
정보자산 분류	• 정보자산 조사/책임할당 • 정보자산 분류 및 취급	
정보보호 교육 및 훈련	• 교육/훈련프로그램 수립 • 교육훈련의 시행/평가	
인적보안	• 책임할당 및 규정화 • 직원의 적격 심사 • 주요직무 담당자 관리 • 비밀유지	기밀정보 취급 직원에 대한 내용 보완 - 퇴사 시에도 정보보호서약서 징구 의무화 - 개인정보 등 민감정보 취급 직원은 별도의 기밀유지 서약서 추가 징구
물리적 보안	• 물리적 보호구역 • 물리적 접근통제 • 데이터 센터 보안 • 장비보호, 사무실 보호	분산된 환경 특성상 출입통제, 모니터링 적용이 전 사이트로 확대되어야 함 장비, 저장매체 등의 반출입 통제사항 추가 문서 보안 (파쇄기 설치 등)
시스템개발 보안	• 분석 및 설계 • 구현 및 이행, 변경관리	신규 어플리케이션 서비스 Open시 보안성검토 의무화 - 보고체계 등 프로세스 정립 - 해킹 가능성, 악성코드 보유 여부 점검
암호통제	• 암호정책, 암호사용, • 키관리	암호사용 영역을 구체화 - 이용자/서비스 정보 전송구간 암호화 - DB 암호화 (Storage) - 문서/디스크 암호화 적용 - 시스템 원격 접근시 암호화 (VPN 적용) 등
접근통제	• 접근통제 정책 • 사용자 접근 관리 • 접근통제 영역	1. 접근통제 영역 추가 - 모바일(스마트폰 등), 무선 통한 접근통제 - 내부 직원의 웹, 메신저, P2P 등 접근통제 및 Contents Filtering 등 포함 2. DDoS 방지체계 구축 의무화 내용 추가 3. 네트워크 접근통제시 최신 ICT 기술 포함 - VoIP 접근방지 위한 IPS 도입 등 4. 권한 변경내역 기록 관리 강화 내용 보완 5. 데이터 보안 내용 강화 - 민감 정보(DB) 직접접근 금지 (권한관리, 접근시 승인절차 수립) - DB 접근내역 모니터링 및 기록 관리 - 특히 관리자, 위탁직원 관리 철저 내용 포함

〈표 3-31〉 클라우드 컴퓨팅 서비스 제공자를 위한 정보보호대책 개선안(예시)(계속)

통제 분야	세부 통제사항	주요 개선사항
운영관리	• 운영절차와 책임 • 시스템, 네트워크 운영 및 문서 관리 • 악성소프트웨어 통제 • 원격 컴퓨터 작업	1. 보안시스템 운영 영역 구체화 - F/W, IDS/IPS, DDoS, 유해사이트 차단 등 2. 가상화(Virtualization) 보안 취약점 해결 3. 직원 (특히 관리자) PC 보안강화 내용 포함 - PC방화벽, 백신, 암호화, 매체제어 등 의무화 원격 접속 시 제한사항 추가 4. 원격 작업 시 인증절차 강화 내용 추가 - ID/패스워드 외의 추가 인증수단 적용 의무화 (OTP, Token 등) 5. 서비스 이용자별 저장 DB의 논리적 분리 6. 중앙 집중화된 관리 서비스 (Managed Security Service) 제공 포함
전자거래 보안	• 교환합의서, 전자거래 • 전자우편, 공개서버의 보안관리 • 이용자 공지사항	
보안사고 관리	• 대응계획 및 체계, 대응 및 복구, 사후관리	보안사고 발생 시 신속히 이용자에게 보고할 수 있는 체계(정책/조직/절차 등) 구축 의무화
검토, 모니터링 및 감사	• 법적 요구사항 준수 검토, 정보보호정책 및 대책 준수 검토 • 모니터링, 보안감사	이용자의 법규 준수를 위한 협력사항 포함 - 정보통신망법, PCI DSS 등 이용자의 법규 준수를 충분히 지원하고 있는지에 대한 정기적 점검
업무연속성 관리	• 업무연속성 관리체계 수립 • 업무연속성 계획 수립과 구현 • 업무연속성 계획 시험 및 유지관리	다수 이용자의 중요 정보를 통합하여 관리하므로 장애복구(DR)센터 등 업무의 연속성을 보장할 수 있는 강화된 방안을 반영

② 클라우드 컴퓨팅 서비스 제공자에 특화된 독립적인 인증제도 도입

다른 대안으로써 클라우드 컴퓨팅 서비스 제공자를 위한 독립적인 인증제도를 도입하는 것이다. 이를 위해서는 두 가지 요소가 필요하다.

- 클라우드 컴퓨팅 서비스 제공자들에게 특화된 통제 항목들이 개발되어야 함

- 인증 스킴과 역할이 정의되어야 함.

전자를 위해서는 CSA (Cloud Security Alliance: 2008년 창립된 클라우드 컴퓨팅 보안을 위한 비영리협회)의 기준 등 국/내외적인 보안기준을 기반으로 다음의 표와 같은 통제 항목을 개발 할 수 있다.

〈표 3-32〉 클라우드 컴퓨팅 서비스 제공자를 위한 정보보호인증 항목(안)

영역	세부 통제사항	주요 내용
지배구조 및 위험관리 체계 (governance & risk mgmt.)	• 정책, 조직, 프로세스 • 위험평가/관리	- 클라우드 컴퓨팅 서비스의 범위 등 정의 - 지배구조(정책, 조직, 프로세스) 정립 - 제3자(벤더 등)로 인한 위험 등 위험요소 식별, 평가 및 관리
법규 대응 (legal)	• 계약서 • 법적의무 사전 정의	계약서를 통한 보안요건 정의 - 계약서에 서비스에 따른 보안요건 정의 - 정보 요청에 대한 제공자의 의무 등 포함 - 계약 이외 목적의 정보 오남용 금지
전자 증거 (e-Discovery)	• 전자 증거 보관	- 법규 요구가 있을 경우 전자 증거 제시 의무 충실 (이용자, 제공자간 책임/역할 정의) - 데이터(재무자료, 로그 등)의 신뢰성 보장을 위한 보안시스템 구비
준거성 및 감사 (compliance & audit)	• 법적 요건 준수 검토 • 보안감사	- 감독기관/감사 규제 대상 자료/시스템의 분류, 물리적 위치(백업포함) 등 이해 - 이용자의 다양한 법제도 요구사항 준거(정통망법, PCI DSS)
정보주기 관리 (info. lifecycle mgmt.)	• 정보 분리 • 정보주기 관리	- 정보의 논리적 분리 및 통제현황 관리 - 정보 보관, 폐기 등 절차 준수 - 주기적인 정보의 백업/복구 테스트 수행 - 정보취급 직원의 직무분리
보안, 사업연속성 재해관리 (Business Continuity, DR)	• 보안 베이스라인 관리 • 사업연속성, 재해관리	- 보안 베이스라인 수립 및 준수 - 이용자의 주기적인 보안검사 허용 (사업연속성, 재난관리 계획의 적정성)
데이터센터 운영 (Data Center Operation)	• 용량, 성능, 가용성	- 아키텍처, 인프라 등의 계약(SLA)에 따른 서비스 만족여부 확인 - 성능, 용량, 가용성 등의 수용 - 아키텍처(IaaS,PasS 등)에 따른 어플리케이션 영향도 평가

〈표 3-32〉 클라우드 컴퓨팅 서비스 제공자를 위한 정보보호인증 항목(안)(계속)

영역	세부 통제사항	주요 내용
사고대응, 보고, 복구 체계 (incident mgmt.)	• 대응계획 및 체계 • 대응, 복구, 사후관리	- 사고대응을 위한 어플리케이션 로그관리 - 다중 이용자 환경에서의 사고대응을 위해 웹 방화벽, 프락시, 로그관리 도구 필요 - 서비스 다운타임 최소화를 위한 협업체계
어플리케이션 보안	• 개발 보안 • 가상화 보안	- 어플리케이션 개발주기 보안 (코드의 안전성 확보 등 해킹 대응) - 가상화 서버의 보안성 확보 - 기타 어플리케이션 보호 및 관리
암호화 (Encryption)	• 암호 사용 • 암호키 관리	- 데이터 저장 시 암호화 적용 - 암호키 관리 (제공자로부터 격리)
통합인증관리 (IAM)	• 인증 • 권한 관리	- 견고한 ID 및 권한관리 체계 구축 - 이용자를 위한 강화된 패스워드 정책 적용 - 기타 SSO 등 이용자 인증/권한관리 강화 방안 강구
스토리지 (Storage)	• 위치 • 스토리지 폐기	- 스토리지의 물리적 위치 확인 - 다중 이용자의 저장정보 보호통제 적용 - 스토리지 폐기 절차
가상화 (Virtualization)	• 가상화 서버 보안	- 가상화 서버 보호방안 (인증, 접근통제 등) - 가상화 서버 가용성, 안정성 확보

클라우드 컴퓨팅 서비스 제공자를 위한 정보보호인증제도 적용은 다음과 같은 4가지 방안이 있을 수 있다.

방안1. 특화된 인증제도를 도입하고 필수로 하고, 인증을 획득한 기업만이 클라우드 컴퓨팅 서비스를 하게 함

방안2. 기존의 ISMS인증제도의 한 부분으로 클라우드 컴퓨팅 서비스에 대한 인증제도를 도입하고 필수로 함

방안3. 특화된 인증제도를 도입하고 선택으로 함

방안4. 기존의 ISMS인증제도의 한 부분으로 컴퓨팅 서비스에 대한 인증제도를 도입하고 선택으로 함

방안1이 가장 강력한 방안이고 방안 4가 가장 약한 방안이다. 인증제도를 필수로 하여 인증을 받은 업체만이 클라우드 컴퓨팅 서비스를 할 수 있게 하는 첫 번째 방안이 고객의 신뢰획득에 있어서는 가장 바람직한 방안이다. 그러나 이 방안은 정부가 시장을 너무 규제한다는 반대에 직면할 수 있는 위험이 있다. 이에 절충안으로 민간기관의 서비스의 경우 인증을 선택으로 하되, 공공기관 서비스의 경우 인증을 필수로 지정하는 방안을 활용할 수 있다. 현재 정보보호컨설팅의 경우 정보보호컨설팅 전문업체로서 인증받은 회사만이 공공기관의 정보보호컨설팅을 수행할 수 있는 자격을 가지고 업무를 수행하게 하는 제도가 이미 실행되고 있기 때문에 이러한 방안은 충분히 적용가능 하다.

제4장 클라우드 컴퓨팅 활성화를 위한 기술적 대응전략

제 1 절 클라우드 컴퓨팅 서비스 품질 확보 방안

제 2 절 클라우드 컴퓨팅 상호운용성확보방안

제 1 절 클라우드 컴퓨팅 서비스 품질 확보 방안

1. 서비스 품질과 SLA의 중요성

클라우드 컴퓨팅은 광범위한 IT자원을 외부의 서비스 제공자에게 제공받는 아웃소싱 서비스이다. 아웃소싱 상황 하에서, 서비스 공급자로 하여금 고객사가 기대하는 서비스의 수준을 정의하고 정확히 제공할 수 있도록 하는 것이 중요하다. 특히 클라우드 컴퓨팅의 경우 서비스 중단이나 장애 등으로 인한 피해가 광범위하고, 사용자인 기업에 미치는 영향이 치명적일 수 있어 서비스 품질을 담보할 수 있는 SLA(Service Level Agreement)의 수준과 범위가 서비스 제공자 선택에 중요한 역할을 하게 된다.

현재 유사 클라우드 컴퓨팅이라 할 수 있는 초고속인터넷이나 ASP 등을 제공하는 국내 사업자들의 경우 SLA라는 개념은 희박하며, 이용약관의 형태로 서비스를 제공 중이다. 또한 피해보상의 대상이나 수준도 모호하게 설정되어 있다. 예를 들어 피해보상은 '서비스 중단'으로 보호하게 표현되고, 보상도 서비스 장애사실을 확인한 고객이 직접 서비스 이용자에게 신고한 경우 이루어진다. 그러나 고객이 서비스의 품질이나 장애여부를 확인할 수 있는 어떠한 모니터링 시스템도 제공하지 않고 있다.

이에 비해 해외 클라우드 컴퓨팅 사업자들은 SLA에 기반을 둔 명확한 피해보상 기준을 제시하고, 이를 실시간으로 모니터링 할 수 있는 시스템을 제공한다. 특히 단순히 서비스 장애라는 표현이 아닌 서비스 가용율과 같이 서비스 품질을 측정할 수 있는 명확한 품질속성을 설정하고, 일정기준에 미달하는 경우 서비스 가용율의 수준에 따라 차등 화된 보상을 제공한다. 또한 고객들이 이러한 품질속성들을 실시간적으로 모니터링 할 수 있는 신뢰할 수 있는 시스템을 제공한다.

이에 본고에서는 국내 클라우드 컴퓨팅 활성화를 위해 SLA 확산을 위한 가이드라인을 제시하고, 서비스 품질확보를 위한 기술적, 제도적 방안을 제시한다. 이를 위해 우선 IT서비스 등 유사클라우드 컴퓨팅 서비스에 대한 SLA 국제표준과 소프트웨어 품질평가에 대한 국제표준, 국내. 외 주요 사업자의 SLA현황을 살펴본다.

2. SLA관련 국제표준

가. IT서비스 아웃소싱 SLA 국제표준

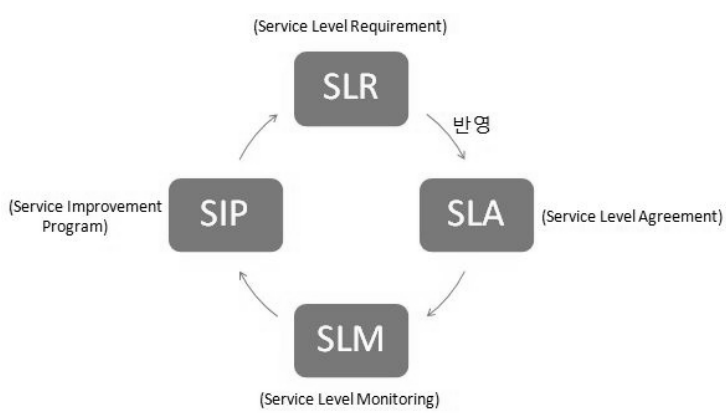
그동안 통신사업자는 서비스 종류별로 네트워크 환경과 관련된 각종 성능지표(performance metrics, 또는 품질지표)를 조합하여 구성하여 왔다. 최근에는 이것이 음성통신이나 특정의 데이터통신 분야에 한정하여 이루어졌는데 이제는 DSL, Web Hosting이나, IP서비스 제공자 즉 ISP사업 분야에도 적용되고 있다. 여기에서, IT서비스를 제공받는 조직 혹은 사람은 누구나 고객이며, 일반적으로 IT조직이 IT서비스 제공자(Provider)에 해당된다. 일반적으로 SLM 분야에서 고객과 서비스 제공자에 대한 정의는 다음과 같다.

〈표 4-1〉 고객과 서비스 제공자의 정의

고객	o IT서비스를 제공 받는 조직 혹은 개인 o 조직을 대표하여 IT서비스 구매와 관련된 계약을 체결하도록 권한을 위임받은 자 o 서비스 최종 사용자와는 다를 수 있음
서비스 제공자	o 일반적인 IT조직을 의미 o 조직을 대표하여 IT서비스 제공과 관련된 계약을 체결하도록 권한을 위임받은 자

또한, SLM은 일반적으로 다음과 같이 네 단계로 이루어진 순환적인 프로세스를 가진다.

〈그림 4-1〉 서비스레벨관리(SLM) 프로세스



SLR (Service Level Requirement)단계에서는 현업 사용자와의 인터뷰 등을 통해서 서비스 수준 요구사항을 정의하고, 협의하며 그 결과를 반영하여 SLA를 작성하게 된다. SLA에는 일반적으로 서비스 수준 목표 (Service Level Objective, 이하 SLO), 그 수준의 도달 여부에 따른 인센티브와 페널티 등의 내용들이 포함된다. 이후 SLA 내용이 제대로 이행되고 있는 지를 지속적으로 감시 감독하는 서비스 수준 모니터링(Service Level Monitoring, 이하 SLM)을 거치며 기존의 SLA 수준보다 높은 요구 사항을 일시적으로 반영하는 서비스 개선 계획(Service Improvement Program, 이하 SIP)을 실행하게 된다. SIP(Service Improvement Program) 단계에서의 요구사항은 그 서비스 수준이 이루어지지 않았다 하더라도 페널티가 반영되지 않으며, 단지 다음 주기에서의 SLA 요건을 작성하는데 참고가 된다.

IT 서비스를 제공 받는 고객사(Beneficiary)와 서비스 공급자는 서로의 상호관계를 올바르게 인식해야 하며 각자의 요구사항 및 기대치에 대한 정의를 하고, 이에 대한 명확한 합의를 반드시 이루어야 한다. 이에 대한 관리 방법의 하나가 바로 서비스 수준 합의서(Service Level Agreement, 이하 SLA)이다.

서비스 아웃소싱 상황 하에서 SLA의 사용의 필요성이 인지되고 보편화됨에 따라, SLA에 포함되어야 할 항목들과 SLA 의 기본 구조, 그리고 역할, 사후 모니터링, SLM 프로세스 통제 등과 관련하여 몇 가지 국제적 표준이 제안되었다. 대표적인 국제 표준으로는 ISO/IEC 20000, Information Technology Infrastructure Library V3(이하 ITIL v3), Control Objectives for Information and related Technology 4.1(이하 COBIT 4.1) 등이 있다. 그 세 가지의 표준에 대해서 간략히 살펴보고자 한다.

1) ISO/IEC20000

ISO/IEC20000(이하 ISO 20000)은 IT서비스 관리(ITSM: IT Service Management)를 위한 최초의 국제표준으로 2005년에 제정되었다. ISO 20000은 기존에 ITSM의 표준으로 활용되던 BS 15000 (British Standard 15000)을 개편하여 IT서비스 관리 활동에 대한 요건을 명확히 정의한 국제적인 표준이다. ISO20000은 서비스 프로세스의 효과증가와 IT서비스 품질의 객관적 평가, 고객 요구에 부합하는 ITSM제공, IT서비스 효율성 제고를 위한 통합적 접근 방식제공의 목적을 위해 제정되었으며, 크게 10개의 분야로 수성되어 있다.

〈표 4-2〉 ISO/IEC20000의 목적 및 구성

	세부내용
구성	1. Scope
	2. Terms & Definitions
	3. Planning and Implementing Service Management
	4. Requirements for a Management System
	5. Planning and Implementing New or Changed Services
	6. Service Delivery Processes
	7. Relationship Processes
	8. Control Processes
	9. Resolution Processes
	10. Release Processes

ISO 20000-1은 ISO20000-1과 ISO20000-2의 두 가지 파트로 나뉘어져 있으며 첫 번째 파트는 비즈니스에 통합된 IT 서비스를 통해 고객의 요구에 순응할 수 있는 명세(Specifications)를 10가지의 섹션으로 나누어서 설명하며, 두 번째 파트인 ISO20000-2는 'Code of practice' 즉 수행방안으로 ISO20000-1의 범주 안에서 최선의 실무(Best practice)들을 소개한다.

10개 섹션들 중 SLA와 가장 연관성이 높은 항목은 5. Planning and Implementing New or Changed Services, 6. Service Delivery Processes, 7. Relationship Processes가 있으며 그 내용은 〈표 4-3〉과 같다.

이에 따르면 SLA는 문서화되어 이용자에 의해 동의되어야 하며, 서비스 수준이 명확하게 모니터링 되어야 함을 명시하고 있다. 또한 서비스의 가용성은 세부적으로 측정되고 기록되도록 하고 있으며, 접근권한이나 응답시간 등이 이에 포함되도록 하고 있다

〈표 4-3〉 ISO/IEC20000 중 SLA관련 주요 내용

주요 항목		세부내용
5. Planning and implementing new or changed service		o 제안서에서 고려해야 할 것들과 시스템 구축 계획을 작성해야 할 때 고려해야 할 요소들(비용, 조직적, 기술적 혹은 상업적인 영향) 설명 o 계획에서 포함되어야 할 요소들(역할과 책임소재 구분, 각 이해관계자간의 의사소통, 서비스 관리 프레임워크와 서비스에서의 변화 등)에 관한 내용이 포함
6. Service Delivery Process	o SLA와 직접적으로 관계되는 내용들을 서술해 둔 항목	
	6.1 Service level management	o 정의된 서비스 수준은 하나 혹은 그 이상의 SLA로 문서화되어야 하고, 공급자와 관계자에 의해 동의되어야 함 o SLA는 변화 관리 프로세스에 연계되어야 하며, 최신 성을 보장하기 위하여 정기적으로 검토되어야만 함. o 서비스 수준은 지속적으로 모니터링 되어야 하며 SLA 요건 사항에 부합되지 않는 사항들은 보고되어야 함.
	6.2 Service reporting	o 각 서비스의 정체성과 목적 그리고 대상자, 데이터 출처를 포함한 명확한 서비스 리포트가 있어야 함 o 서비스 리포트는 서비스 수준 목표에 반하는 행위, 부적합한 이슈들 등이 포함되어야함 (이를 통해 의사 결정과 효율적인 커뮤니케이션을 위한 이해 당사자 간의 합의가 이루어진, 신뢰성 있고 정확한 서비스 리포트가 가능)
	6.3 Service continuity and availability management	o 가용성과 연속성은 비즈니스 계획단계, SLA, 위험 관리의 근간이 되어야 하며, 가용성과 연속성 계획은 미미한 실패부터 중대한 서비스 실패까지 모든 환경에 적합하도록 최소 1년에 한 번씩 검토되어야 함 o 가용성은 측정되고 기록되어야 하며 계획되지 않은 비가용성 사항에 관해서는 적절한 조치가 취해져야 함 o 접근 권한과 응답 시간 등은 요구 사항에 포함되어야 함.
	6.4 Budgeting and accounting for IT services	o IT 자산과 공유 자원, 간접비, 보험 등에 관한 명확한 정책과 프로세스가 존재해야만 하며 효율적인 재무적 통제와 승인 프로세스 필요 o 서비스 변경은 적절한 변화 관리 프로세스를 통해서 비용이 산정되고 승인되어야 한다.
	6.5 Capacity management	o 현재의 용량과 예측되는 용량과 성과를 고려한 용량 관리를 위한 용량 계획이 있어야함. o 외부의 환경 변화와 관련한 영향도 고려되어야만 하며 예측 분석을 가능하게 하는 데이터와 절차를 포함해야 한다.

〈표 4-3〉 ISO/IEC20000 중 SLA관련 주요 내용(계속)

주요 항목		세부내용
6. Service Delivery Process	6.6 Information security management	o 적절한 보안 통제는 정보 보안 정책의 요구사항을 수립하고 서비스 혹은 시스템 접근과 관련한 위험을 관리하여야 한다.
7. Relationship processes	o 서비스 제공자는 고객을 포함한 이해 관계자들을 파악하고 문서화해야 하며 적어도 일 년에 한 번씩 서비스 제공자와 고객은 제공 중인 서비스를 검토하고 변화 사항들을 SLA에 포함해야 함	
	7.1 Business relationship management	o 관계 프로세스는 Business relationship과 Supplier management의 두 가지 측면을 고려해야 함
	7.2 Supplier management	o 요구 사항과 범위, 서비스 수준과 의사소통 프로세스는 SLA로 문서화되어야 하며 참여하는 모든 관계자가 동의해야 한다. 또한 공급자들과의 SLA는 비즈니스의 SLA와 연계되어야 한다. o 하위 공급자(Subcontracted Supplier)와 주 공급자(Lead Supplier)간의 역할은 문서상에 명확하게 정의되어야 함

2) ITIL V3

흔히 IT부서는 많은 돈이 투자되지만 반면 수익성이 떨어지는, 수입과는 직접적인 관련이 없는 부서로 인식되기 쉽다. IT의 성과가 가시화되지 않기 때문인데, IT가 제공하는 모든 것이 서비스 개념으로 인식하는 것이 ITSM(IT Service Management)이다. ITSM의 개념의 도입을 돕기 위해 성공사례, 모범사례(best practice)를 소개하는 것이 Information Technology Infrastructure Library(이하 ITIL)이다. ITIL는 IT서비스(ITSM)와 개발과 운영에 관한 정책과 개념들로 이루어져 있으며 IT조직이 필요에 맞게 적용할 수 있는 IT Best Practice들과 체크리스트, 절차들로 이루어져 있다.

최초의 Version. 1을 거쳐 현재는 2007년에 발간된 Version. 3이 최신판이며, 영국의 Office of Government Commerce (OGC)에 의하여 만들어졌다. 현재 ITSM에 있어ITIL의 위상은, 비록 ISO 20000과 같이 국제적으로 공인된 표준은 아니지만 전 세계적으로 사실상의 표준(De facto standard) 으로 받아들여지고 있으며 ITSM의 방법론이나 프레임워

크로 산업계에서 널리 채택하고 있고 공공기관을 통해서도 급속히 확대되고 있다.

그렇다면 앞에서 간략히 소개된 ISO20000과 ITIL은 어떤 관계일까? ISO 20000의 전신인 BS 15000은 ITIL을 기반으로 하고 있으며, 여러 나라의 국가적인 표준으로 제정, 준수되었으며 이후 ISO 20000표준이 제정되어 전 세계적인 인지도가 높아지고 있다. 많은 국가에서 기업들이 ITIL의 ITSM사례를 중심으로 기준을 수립하였고 그 기준에 일치하는지를 독립된 제3자가 객관적으로 심사해주는 것으로 ITSM을 제대로 수행하고 있는가의 척도는 ISO20000인증의 취득여부로 판가름 나게 된다.

ITIL의 주요 장점은 기업의 표준화된 IT실천모델을 제시[52]하고, 효과적인 IT운영을 통한 고객만족[53]이 가능하다는데 있으며 크게 5개 분야로 구성되어 있다.

〈표 4-4〉 ITIL의 구성

세부내용	
ITIL의 구성	1. Service Strategy
	2. Service Design
	3 .Service Transition
	4. Service Operation
	5. Continual Service Improvement

이중 SLA과 관련된 부분은 서비스 설계(Service Design), 서비스 운영(Service Operation), 지속적인 서비스 향상(Continual Service Improvement)등이 있다. 그 세부내용을 살펴보면 〈표 4-5〉과 같다.

52) 이를 위한 주요 특징은) IT변경사항에 대한 관리, 통제권의 향상, 2) IT비용관리 프로세스를 통한 IT비용 절감, 3) IT와 비즈니스를 연계 관리, 4) IT관리도구의 적용을 위한 프로세스 확립, 5) 아웃소싱에 대한 결정을 위한 프레임워크 준비, 5) 상호 대화를 위한 참조 모델, 6) 체계적이고 명확한 IT조직체계 확립 등이 있음

53) 이를 위한 주요 특징은 1) 문서로 상세하게 잘 정리된 IT 서비스, 2) 보다 안정적인 IT운영환경, 3) 제공 서비스에 대한 품질 보증에 따라 신뢰성 증가, 4) 신속한 신규 IT서비스 착수, 5) 명확한 대화 통로 제공 등이 있음

〈표 4-5〉 SLA와 관련된 ITIL의 내용

주요항목	세부내용
2. Service Design	o 비즈니스와의 관계 형성 o 현재의 요구와 목표에 대한 협의 및 합의 그리고 모든 운영 서비스에 대한 SLA문서화 및 관리 o 미래 요구 및 목표에 대한 협의 및 합의 그리고 모든 제안된 신규 및 변경 서비스를 위한 SLR 문서화 및 관리 o 미래 요구 및 목표에 대한 협의 및 합의 그리고 모든 제안된 신규 및 변경 서비스를 위한 SLR 문서화 및 관리 o SLA목표 달성을 보장할 수 있는 적합한 수준의 OLA 개발 및 관리 o SLA목표를 달성할 수 있도록 UC내 합의 내용 검토 o 다른 프로세스와의 연결을 통한 서비스 장애 발생 억제, 서비스 위험요소 감소, 서비스 품질 향상 o 모든 서비스에 대한보고 및 결과 관리와 SLA 미달성 사항 및 취약요소 검토 o 서비스와 프로세스 향상을 위한 서비스 향상 계획(SIP)의 촉진과 조정
4. Service Operation	o 서비스 운영에 관한 지침과 사례(practices)로 구성 o 서비스 지원과 수행(support and delivery)에 있어서 효율성과 효과성을 얻도록 하여 고객에게 가치를 제공할 수 있도록 o 서비스 운영에 있는 가이드, 방법, 도구 등을 크게 두 가지 관점의 통제(사전 예방적인 관점과 사후 대응적인 관점)로 구분 o 가용성 관리, 수요관리, 용량의 최적화, 장애 해결 등에 도움
5. Continual Service Improvement	o 서비스 설계와 도입, 운영을 통해 고객을 위한 가치를 만들고 유지하는데 필요한 도구들을 제공 o 품질관리, 변경관리, 역량의 향상 등과 관련된 원칙과 사례, 방법들을 다룸 o 서비스 품질, 운영의 효율성, 비즈니스 연속성의 향상 등을 달성 o 서비스 전략/서비스 설계/서비스 운영 전환과 관련

서비스 설계는 서비스와 서비스 관리 프로세스의 설계 및 개발에 대한 가이드를 제시한다. 여기에서는 전략적 목표를 서비스 포트폴리오와 서비스 자산으로 전환하는 방법과 설계에 대한 원칙을 다룬다. 서비스 설계의 범위는 새로운 서비스에 대한 것만은 아니고 기존 서비스에 대한 변경과 개선 등을 포함한다. 조직은 이 가이드를 통해 서비스 관리를 위한 설계 역량을 향상시킬 수 있을 것이다. 서비스 설계 원칙, 설계 프로세스, 서비스 수준 관리 등의 소항 목으로 이루어져있다.

서비스 수준 관리는 비즈니스 대표자와 함께 적합한 IT 서비스 목표를 협상, 합의하여 문서화하고 합의된 서비스 수준으로 서비스 제공자가 서비스를 제공하고 있는지 모니터링

하고 보고하는 일련의 활동들로, 모든 IT 서비스 제공 조직에 있어 핵심적인 프로세스로 합의되고 문서화된 서비스 수준 목표에 대한 책임을 가지며 IT의 모든 활동들에 있어 SLA와 SLR에 대한 책임을 갖는다. SLM에서 합의된 서비스 수준 목표를 비즈니스의 요구사항에 맞춰 적합하고 정확하게 설정한다면, 서비스 제공자는 비즈니스 요구에 부합한 서비스 제공이 가능할 것이며 고객이나 사용자 측면에서 의 서비스 품질 기대와 요구에 충족할 수 있는 서비스 제공이 이루어 질 것이다.

3) COBIT 4.1

COBIT 4.1(Control Objective for Information and related Technology 4.1)은 정보시스템감사통제협회(Information System Audit and Control Association,이하 ISACA)에 의해 개발 된 IT 관리 목적의 프레임워크이다. IT보안 및 통제 부문에서의 모범적인 업무 수행 방법에 대한 일반적으로 적용가능하고 인정되는 기준으로 개발되었다. 여기서 '일반적으로 적용가능하고 인정되는'의 의미는 회계에서 GAAP(Generally Accepted Accounting Principle)에서의 의미와 동일하게 사용된다.

〈표 4-6〉 COBIT의 정의, 목표 및 구성

	세부내용	
정의	o IT거버넌스를 위해 필요하며 정보 및 시스템의 무결성을 제공하는 통제모델 o 기술적인 이슈와 사업 위험에 대한 통제 요구사항의 괴리를 보완하기 위해 관리자가 사용할 수 있는 IT거버넌스 프레임워크 도구	
목표	o 경영진과 업무 프로세스 책임자에게 IT와 관련된 위험을 이해하고 관리하기 위해 IT관리 모델 제공	
구성	Plan & Organise	o IT가 경영목적에 달성할 수 있는 최선의 방법과 계획 수립 o 의사소통, 관리, 적절한 조직과 기술 인프라 수립
	Acquire & Implement	o IT전략을 실현하기 위해 IT솔루션 개발 및 구입 o 비즈니스 프로세스 구현 및 통합, 기존 시스템 변경과 유지보수
	Delivery & Support	o 필요한 서비스를 제공하는 것으로 서비스 제공과 연속성 관리 o 사용자에 대한 서비스 지원, 데이터 및 운영 설비
	Monitor & Evaluate	o IT프로세스가 제대로 수행되는지 여부를 품질과 통제 준수 측면에서 평가 o 성과관리, 내부통제 모니터링, 법규 준수, 거버넌스 제공

COBIT의 네 가지 구성요소 중 SLA와 가장 깊은 관련성을 가지는 부분은 'Delivery and Support'이다. 'Deliver and support' 도메인은 직접적으로 SLA와 관련이 있는 부분이며 통제 목적으로 서비스 수준의 정의, 지속적인 SLA의 검토와 성과 검토, 이해관계자의 식별, 가용성 관리 등을 다루고 있으며 그에 대한 성숙도 수준을 최저 단계인 Non-existent부터 Initial/Ad Hoc, Repeatable but intuitive, Defined, Managed and measurable, Optimised까지의 다섯 단계로 분류, 어떠한 상황이 각각의 단계에 속하는지를 자세하게 나타내고 있다. 〈표4-7〉은 해당 도메인의 하위 프로세스를 나타낸다.

〈표 4-7〉 Delivery and support

DS1	Define and Manage Service Levels
DS2	Manage Third-party Services
DS3	Manage Performance and Capacity
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS6	Identify and Allocate Costs
DS7	Educate and Train Users
DS8	Manage Service Desk and Incidents
DS9	Manage and Configuration
DS10	Manage Problems
DS11	Manage Data
DS12	Manage the Physical Environment
DS13	Manage Operations

COBIT과 ITIL은 함께 사용되었을 때 IT거버넌스와 ITSM에 있어서 하향식(Top to bottom) 접근 방법을 제공한다. COBIT은 모든 범주의 IT활동들에 있어서 전체적이며 완전한 관점에서 경영진의 우선순위와 목표를 관리한다. 이를 통해 모든 이해 관계자들을 공통적인 통합 접근법에 초점을 맞추도록 한다. ITIL은 서비스 관리에 있어서의 최선의 실무를 통해 이를 지원한다. COBIT과 ITIL이 함께 사용되었을 때 두 가지 표준의 효력이 확장되며 비용 효과적인 구축 자원의 사용이 가능해질 것이다. SLA에 관한 내용을 담고 있는

COBIT의 'Deliver and support'도메인과 ITIL의 각 항목들을 아래 표에 대응시킨 표의 일부이다.

〈표 4-8〉 COBIT과 ITIL의 비교

COBIT		ITIL
Control Objective	Name	
DS1	Define and manage service levels	SS 2.2 What are services? SS 3.4 Service structures SS 5.3 Service portfolio management SS 8.1 Servie automation SD 1 Introduction SD 2 Service management as a practice SD 2.1 What is service management? SD 2.2 What are services? .....
DS1.1	Service level management framework	SS 2.6 Functions and processes across lifecycle SS 4.3 Develop strategic assets .....

출처 : IT Governance Institute, COBIT Mapping : Mapping of ITIL v3 with COBIT 4.1 (2009.11)

나. 클라우드 컴퓨팅 서비스의 품질 모델 및 메트릭

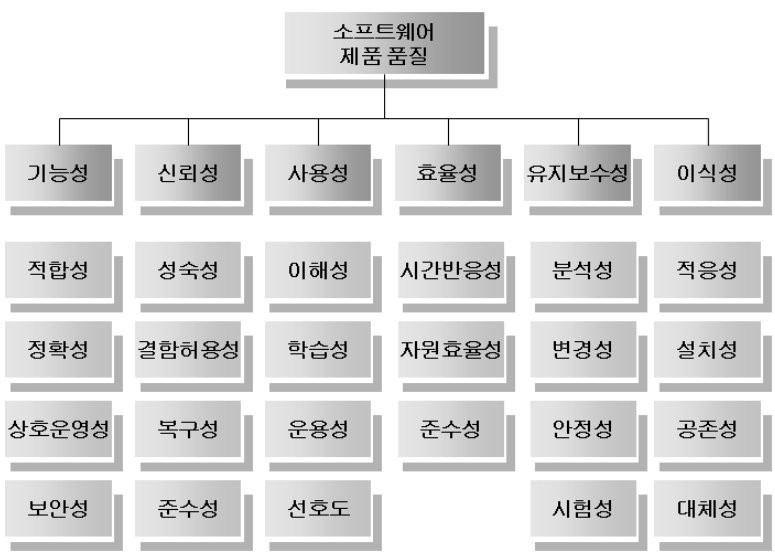
클라우드 컴퓨팅 서비스의 QoS는 대부분 하드웨어, 소프트웨어, 네트워크 등 기술적인 요소에서 결정된다. 그러나 클라우드 컴퓨팅 서비스를 품질평가 할 수 있는 국제표준 품질 모델의 적용은 이루어지지 않고 있다. 이에 소프트웨어 품질평가 모델인 ISO/IEC 9126과 같은 국제표준 품질모델의 도입이 검토될 수 있다. ISO/IEC 9126의 모델 구성은 〈표4-9〉와 같다.

〈표 4-9〉 ISO/IEC 9126의 모델 구성

구분	내 용
Part 1 품질모델 (Quality Model)	o 품질 특성 및 하위 특성에 대한 정의를 규정함
Part 2 외부 메트릭 (External Metrics)	o 제품이 규정된 조건에서 사용될 때 요구사항을 만족시키는 정도
Part 3 내부 메트릭 (Internal Metrics)	o 제품이 규정된 조건에서 요구사항을 만족시키기 위해 제품의 설계와 실제코드가 어떤 품질을 갖는가 있는가에 대한 정도
Part 4 사용품질 메트릭 (Quality In Use Metric)	o 완성된 후에는 외부 품질 평가를 통해 품질 요구사항이 만족되는가를 확인

ISO/IEC 9126은 소프트웨어 품질 속성을 여섯 가지 특성으로 구분하며, 이러한 품질 특성은 다시 세분화되어 이에 따른 세부 메트릭(평가항목)을 제시하고 있다. 다음은 ISO/IEC 9126 국제표준 품질모델이다.

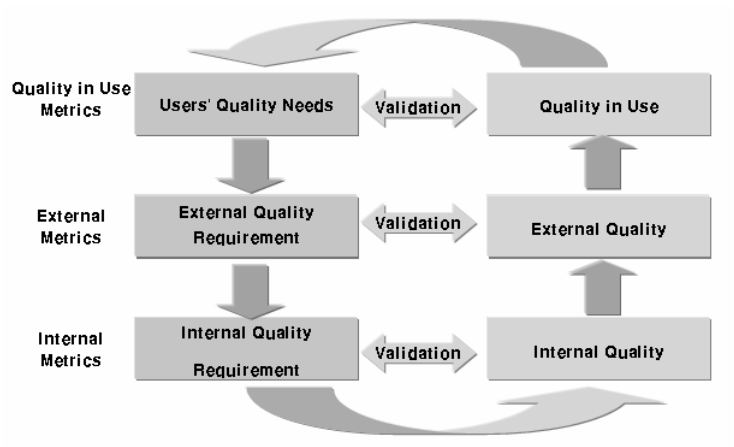
〈그림 4-2〉 ISO/IEC 9126 국제표준 품질모델



이를 기반으로 품질모델 내의 여러 요소들을 내·외부적 품질과 사용 중 품질 등이 어떤 의미를 갖는가 알 수 있다. 설계 및 코딩의 검토 단계에서는 내부 품질을 측정하고, 대상

소프트웨어가 완성된 후에는 외부 품질 평가를 통해 품질 요구사항이 만족되는가를 확인한다. 사용 중 품질이란 제품이 특정 환경에서 사용될 때 사용자의 작업 효율성, 생산성, 안정성, 만족도 등 사용자의 요구를 충족시키는 정도를 말한다. 사용 중 품질에 대한 평가는 고객에게 인도된 후, 향후 수정 작업이나 유사 프로젝트를 위하여 실제 현장에서 사용자에 의해 평가되는 것이다. 다음은 ISO/IEC 9126 소프트웨어 품질모델의 구조이다.

〈그림 4-3〉 ISO/IEC 9126 소프트웨어 품질모델의 구조



ISO/IEC 9126에 정의된 품질특성들 중에서 클라우드 컴퓨팅 서비스에 적용될 수 있는 품질특성도 있다. 예를 들면, 보안성(Security), 안정성(Stability), 적응성(Adaptability)의 경우 클라우드 컴퓨팅 서비스를 품질평가 하는데 사용될 수 있다. 보안성의 경우 사용자들의 개인정보 등에 대한 내용이 클라우드 컴퓨팅 환경에서 노출 되면 안 되기 때문에 클라우드 컴퓨팅 환경에서 보안성은 매우 중요한 품질항목이다. 안정성은 네트워크 상태나 클라우드 컴퓨팅 서비스가 사용자에게 항상 안정된 상태로 서비스 될 수 있어야 하기 때문에 이 또한 중요한 품질평가 항목이다. 적응성은 사용자가 원하는 클라우드 컴퓨팅 서비스가 존재하지 않거나 비슷한 기능을 제공하는 서비스가 있을 경우 이를 사용자가 만족할 수 있도록 클라우드 컴퓨팅 서비스가 적응해야 하기 때문에 중요한 품질평가 항목이다.

다음은 이들을 품질측정 할 수 있는 ISO/IEC 9126메트릭에 대한 예제이다.

■ 보안성 (개념-프로그램과 자료에 대해 인가되지 않은 접근을 방지 할 수 있는 정도)

계산식	x=(A/B)	값 범위
항목 정의	A : 측정 중 시스템과 데이터에 접근되는 수	0 ≤ X ≤ 1
	B : 측정 중 시스템과 데이터에 접근할 수 있는 모든 방법에 대한 수(보안, 로긴, 암호화 등)	
1에 근접할수록 보다 좋은 성능을 지닌 것으로 평가함.		

■ 안정성(개념-SW변경으로 인해 예상치 못한 결과를 최소화하는 SW 능력의 정도)

변경 성공률(Change Success Ratio)		
개념	환경설정 변경 후 SW를 유지하는 동안 오류 없이 운용하는 능력	
계산식	X=Na / Ta	값 범위
항목 정의	Na : SW를 변경 후 운용하는 동안 오류 발생 수	0 ≤ X
	Ta : SW 변경 후 명시된 기능 수행 동안의 작동 시간	
작을수록 좋은 성능을 지닌 것으로 평가함		

■ 적응성(개념-SW제품이 기본적으로 제공하는 방법만으로 다른 환경에서 변경할 수 있는 SW 능력의 정도)

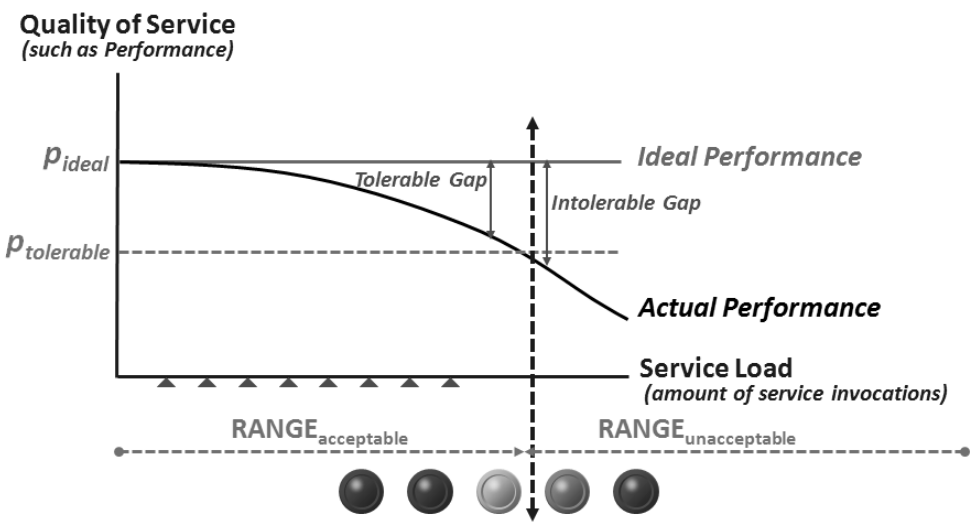
이식 편리성(Change Success Ratio)		
개념	사용자가 SW 제품을 자신의 시스템 환경에 쉽게 적응시킬 수 있도록 구현되어 있는지를 의미	
계산식	X=(B / A) / C	값 범위
항목 정의	B : 전체 SW를 설치하거나 셋업 변경 시 총 소요 시간	0 ≤ X ≤ 1
	A : 설치하거나 셋업 변경 횟수	
	C : 설치하거나 셋업 변경 시 요구되는 평균 소요 시간	
1에 근접할수록 보다 좋은 성능을 지닌 것으로 평가함.		

■ 확장성 (Scalability)

확장성은 기존 시스템에서 원하는 목적을 위해 추가적인 기능이나 데이터를 추가할 수 있는 능력 또는 추가 시 소요되는 비용의 정도를 나타낸다. 확장성이 좋을수록 그 시스템

은 다양한 사용자의 요구를 만족시킬 수 있고 변화하는 사용자들의 요구사항에도 신속히 대응할 수 있다. 클라우드 컴퓨팅에서 제공하는 서비스는 사용자의 컴퓨터가 아닌 제공자의 서버에 설치되기 때문에 사용자는 임의로 서비스의 기능을 확장할 수 없다. 따라서 서비스 제공자는 사용자가 확장된 서비스를 원할 때 확장된 서비스를 이용할 수 있게 하여야 한다. 따라서 서비스 제공자는 언제나 서비스의 확장성이 좋은 서비스를 제공하기 위해서 관리해야 할 필요가 있다. 다음은 확장성의 안정된 범위를 나타낸 그림이다.

〈그림 4-4〉 클라우드 컴퓨팅 서비스품질 중 확장성 안정 범위



▣ 가용성 (Availability)

가용성은 사용자가 특정 시스템이나 그 시스템에 속한 기능을 필요로 할 때 그 것을 사용할 수 있는 정도를 나타낸다. 가용성이 높은 시스템이나 기능은 사용자에게 더 많은 신뢰를 얻기 때문에 그 것의 사용빈도 또한 높아진다.

클라우드 컴퓨팅은 다양한 사용자들이 필요로 하는 재사용성이 높은 서비스를 제공자의 서버에 설치하고 서비스 사용자들은 이를 원격에서 접속하여 사용한다. 이렇게 원격에서 사용자 서버에 설치된 서비스를 사용하기 때문에 사용자가 이용하는 서비스의 수행 결과가 서버와 네트워크의 성능에 의존적이게 된다.

만약 제공자 서버 또는 네트워크상에 문제가 발생해서 사용자가 서비스를 이용할 수 없

게 되면, 사용자는 필요한 서비스를 필요할 때에 사용하지 못하기 때문에 예상한 결과를 얻지 못하게 된다. 이것은 서비스 결과를 바탕으로 계획된 모든 비즈니스에 부정적인 영향을 미치기 때문에 금전적인 손실과 중요 데이터의 손실 등의 문제를 야기할 수 있다.

▣ 성능 (Performance)

성능은 클라우드 컴퓨팅 서비스의 매우 중요한 품질평가 소요 중 하나이다. 클라우드 컴퓨팅 서비스 특징상 언제 어디서든 이용 가능해야 하기 때문에 언제 어디서든 사용자가 클라우드 컴퓨팅 서비스를 사용할 때는 늘 똑같은 응답속도가 보장 되어야 한다. 그러기 위해서는 클라우드 컴퓨팅 서비스는 확장성이 좋아야 이에 따른 성능 또한 높아진다. 따라서 품질평가 요소 중 확장성과 성능은 밀접한 관계를 가지고 있다. 이러한 관계가 품질평가 요소에 반영 되어야 하고 이를 기반으로 품질평가가 이루어 져야 한다.

▣ 기타

- 재사용성 (Reusability)
- 효율성 (Efficiency)
- 신뢰성 (Reliability)

3. 클라우드 컴퓨팅 SLA 해외 사례

클라우드 컴퓨팅에 관련하여 비교적 최근에 제시한 Google, Amazon, Microsoft의 서비스 제공자와 사용자간의 SLA에 대해 먼저 알아본다.

1) Google app' SLA

구글 App's의 SLA는 다음과 같다.

〈표 4-10〉 Google app' SLA 개요

What	“Web interface”를 작동하며 Gmail, Google 캘린더, Google토크, Google 워드 프로세서에 사용할 수 있는 구글 사이트
Uptime guarantee (가동시간[54] 보장)	99.9%
Time period	월별로 측정한다.
Penalty	3, 7 또는 서비스의 15일 무료, 월별 가동시간 비율에 따라 적용

“Downtime”은 서버의 장애를 의미하는데 만일 5% 이상의 사용자 에러가 발생된다면 중단된다. 서버 오류는 평가를 기반으로 측정된다. “Down Period”의 경우 특정 도메인(기업이나 고객)별로 연속적으로 10분 이상 지속되는 장애를 다운타임 기간으로 정의하고 있다.

“Monthly uptime percentage”는 가용시간(율)을 의미하며 한 달 단위로 계산된다. 한 달을 30일로 가정하면 계산식을 다음과 같다.

o 1개월=(30×24×60)=43,200분
o t=위에서 정의된 ‘다운타임 기간’의 총 합
o 월간 가용시간(율)=(43,200-t)/43,200

따라서 한 달 동안 10분간 지속된 장애가 한번 있었다면 월간 가용시간(율)=99.976%이고 다섯 번이라면 99.884%가 되므로 산술적으로 한 달이라는 기간 동안에 10분 이상 지속된 다운타임의 총 합이 40분을 넘지 않으면 구글의 SLA는 만족된다.

“Service Credit"[55]조항은 위에 세 가지 안전 조치에도 불구하고 구글이 장애를 초래했을 경우 제공한다는 보상의 내용이다. 가용성이 99.0%~99.9%일 경우는 유료 사용일 을 3일 연장 해주고 95%~99.0%의 가동률을 기록하면 7일, 95% 이하일 경우는 15일을 연장해 준다.

54) 컴퓨터 시스템이나 컴퓨터 시스템에 연결되어 있는 하드웨어 장치가 가동하여 사용할 수 있는 시간의 양 또는 비율. 반대 용어는 고장 시간이다.

55) 서비스 중단 발생 시에는 중단시간(downtime)을 계산하여 Service Uptime 비율에 해당하는 Service Credit Percentage를 적용

2) Amazon.com' SLA

아마존의 대표적인 클라우드 컴퓨팅 서비스인 S3와 S2의 SLA는 다음과 같다.

① Amazon S3

〈표 4-11〉 Amazon S3 SLA개요

What	Amazon Simple Storage Service
Uptime guarantee	99.9%
Time period	"any monthly billing cycle"
Penalty	10-25% of total charges paid by customer for a billing cycle, based on the monthly

"Error rate"는 아마존 S3에 의해 "Internal Error"나 "Service Unavailable"로 표시되어 나타나는 내부서버 에러의 수를 5분 동안 응답한 총 횟수로 나눈 것으로 매월 결제주기 내에서 각 5분 동안 백분율을 통해 각 아마존 S3계정에 대한 에러비율을 계산한다. 내부 서버에러의 계산 값은 아마존 S3 SLA에 포함되지 않으면 어떤 결과도 포함시키지 않는다.

"Monthly uptime percentage"는 요금청구서 주기에서 100%평균에서 각 5분 동안의 에러비율을 뺀 것이다. 기타 사항도 아마존 S3지불에 준하여 service credit을 적용한다.

② Amazon EC2

〈표 4-12〉 Amazon S2 SLA개요

What	Amazon Elastic Compute Cloud service
Uptime guarantee	99.95%
Time period	"the preceding 365 days from the date of an SLA claim"
Penalty	"a Service Credit equal to 10% of their bill for the Eligible Credit Period"

"Annual Uptime Percentage"는 사용 기간 동안, 아마존의 EC2가 사용 불가능한 지역에 있는 동안의 5분 기간을 100%에서 뺀 값이다. 만일 아마존 EC2서비스를 365일 미만

의 기간 동안 사용했다면 서비스기간은 여전히 365일이다. 그러나 서비스의 사용은 당신의 서비스 사용기간 이전의 날짜들은 100% 지역 이용가능성이 있는 것으로 간주된다. 성공적인 서비스 크레딧 승인 이전에 발생한 작업 중단은 미래의 승인을 위해 사용할 수 없다. 연간가동시간은 아마존 EC2 SLA Exclusion으로부터 도출한 작업 중단 시간을 제외한다. "Unavailable" 은 5분 동안 외부접속이 끊겨서 대체instance[56]를 할 수 없는 상태이다.

3) Microsoft Windows Azure' SLA

Windows Azure Compute 서비스의 경우 서로 다른 롤 (web role / worker role)이 디플로이[57]되어 업그레이드와 폴트가 발생할 경우에도 최소 99.95%의 가용성을 제공한다. 또한 디플로이되어 있는 각 role을 모니터링하기 때문에 특정 role instance가 반응을 하지 않을 경우 2분 이내에 이를 수정하기 위한 조치가 실행된다. Windows Azure Storage 서비스의 SLA는 제대로 된 형식의 요청인 경우 최소 99.9%의 가용성을 제공할 예정이며 Storage 계정은 인터넷 게이트웨이에 항상 연결되어 있도록 제공될 예정이다.

〈표 4-13〉 MS Azure 주요 서비스의 SLA개요

Window Azure	o Computer와 Storage를 위한 SLA가 별도로 존재 - Compute에 대해서는 2개 이상의 role instance를 배포하고, Fault 및 Upgrade 도메인을 사용하는 경우 99.95%의 가동률을 보장 - Role instance가 작동하지 않는 경우 적절한 조치를 취하기 위해 2분 이내에 탐지한 후 문제를 해결하기 위해 모니터링을 실시 - Storage 영역은 데이터의 추가, 수정, 조회, 삭제 요청이 제대로 동작하게 하기 위해 99.9%의 가동률을 보장. Storage 계정은 인터넷 게이트웨이에 항상 연결되어 있도록 제공
SQL Azure	o SQL Azure의 SLA는 역시 한달 기준으로 달 평균 99.9%의 가용성을 보장 - 5분 간격으로 한 달간 측정하여 고객의 요청이 SQL Azure의 게이트웨이에서 거부되는 것을 unavailable하다고 판단하여 측정 - 최하 SLA기준인 SQL Azure 기준으로 99.9%(=43.2분/30일)의 가동률을 보장

56) 인스턴스는 추상화 개념 또는 클래스 객체, 컴퓨터 프로세스 등과 같은 템플릿이 실제 구현된 것이다.
57) 정보기술 특히 분산 컴퓨팅에서 통용되는 용어로 넓게 퍼뜨린다는 의미

〈표 4-13〉 MS Azure 주요 서비스의 SLA개요(계속)

.NET Services	o .NET Services의 SLA에 관해서는, Uptime이나 SLA에 관한 전반적인 사항은 Windows Azure에서와 거의 유사하나 기술과 용어에 차이가 있어서 차이 존재 - .NET Service Bus를 사용하는 경우 고객의 사용하는 endpoint와 Azure의 인터넷 게이트웨이 사이의 연결이 끊긴 경우 unavailable이라고 정의 - 제대로 작성된 고객의 요청을 적절하게 처리하지 못한 경우에도 서비스가 unavailable하다고 정의 - 한 달을 기준으로 매 5분 간격으로 모니터링 하여 unavailable을 측정하며, Windows Azure가 제공하는 SLA를 기준으로 가동률은 99.95%(=21.6분/30일) 보장

4. 국내 기업의 SLA현황

현재 국내 클라우드 컴퓨팅 서비스는 초기시장으로 아직까지 해외 사업자의 SLA와 같이 서비스 가용성에 기준한 손해배상기준을 제시하지 못하고 있다. 현재 유사 클라우드 컴퓨팅 서비스라 할 수 있는 국내 주요 IDC서비스와 웹하드 서비스, 초고속 인터넷 서비스의 경우 SLA가 아닌 이용약관에 기준한 손해배상 기존을 제시하고 있으며 그 주요 내용을 살펴보면 〈표 4-14〉와 같다.

〈표 4-14〉 국내 주요 IDC및 초고속 인터넷 서비스 중 손해배상관련 내용

주요서비스	손해배상 관련내용
IDC	2. 회사의 귀책사유로 고객이 서비스를 이용하지 못하는 경우 고객이 그 사실을 회사에 통보하여 확인한 때 또는 회사가 그 사실을 알았거나 알 수 있었을 때로부터 기산하여 계속 4시간 이상의 서비스제공중단시간에 대해 배상 3. 제2항의손해배상금액은 고객이 청구 받은 최근 3개월분(3개월 미만인 경우에는 해당기간 적용) 요금의 일 평균액을 24로 나눈 시간당 평균액에 이용하지 못한 시간수를 곱하여 산출한 금액의 3배를 고객과 협의하여 배상
LG 데이콤 웹하드	1. LG데이콤의 귀책사유로 고객이 서비스를 이용하지 못하는 경우, 이에 대한 손해를 배상합니다. 다만, 고객이 서비스 이용불가 사실을 LG데이콤에 접수한 이후 2시간이내 서비스가 정상화된 경우는 제외 2. LG데이콤의 귀책사유로 고객이 서비스를 이용하지 못하는 경우에는 고객이 그 사실을 LG데이콤에 통보하여 확인한 때 (그 전에 LG데이콤이 그 사실을 알았거나 알 수 있게 된 때)로부터 계속 2시간 이상의 서비스제공 중지시간에 대하여 최근 3개월(3개월 미만인 경우에는 해당기간 적용)의 1일 평균요금에 서비스 제공중지시간을 24로 나눈 수를 곱하여 산출한 금액의 3배를 배상

〈표 4-14〉 국내 주요 IDC및 초고속 인터넷 서비스 중 손해배상관련 내용(계속)

주요서비스	손해배상 관련내용
SK 브로드밴드	1. 회사는 고객에게 책임 없는 사유로 서비스를 이용하지 못한 사실을 고객이 회사에 통지한 때(그 전 회사가 안 경우 알게 된 때)로부터 3시간 이상 계속 서비스를 제공하지 못하거나 월 누적 장애시간이 12시간을 초과하여 고객이 손해를 입은 경우 고객의 청구에 의하여 배상 2. 제1항의 손해배상 금액은 고객이 청구 받은 최근 3개월분(3개월 미만인 경우에는 해당기간 적용) 요금의 일평균금액을 24로 나눈 시간당 평균액에 이용하지 못한 시간 수를 곱하여 산출한 금액의 3배를 고객과 협의하여 배상한다. 3. 제19조 ⑤항에 의한 손해배상 금액은 고객이 청구 받은 최근 3개월분(3개월 미만인 경우 에는 해당기간 적용) 요금의 일평균금액에 보상기준일을 곱하여 산출한 금액의 3배를 최대 기본료 3개월분 이내에서 보상
KT Qook	1. 이용고객에게 책임 없는 사유로 서비스를 이용하지 못한 사실을 이용고객이 케이티에 통지한 때(그전에 케이티가 그 사실을 안 경우는 알게 된 때)로부터 3 시간 이상 계속 서비스를 제공하지 못하거나 월 누적장애시간이 12 시간을 초과하여 고객이 손해를 입은 경우 이를 배상 2. 제1항의 손해배상금액은 이용고객이 해당 월에 적용받는 요금의 일 평균액을 24로 나눈 시간당 평균액에 이용하지 못한 시간 수를 곱하여 산출한 금액의 3 배를 이용고객과 협의하여 배상

국내 유사 클라우드 컴퓨팅 서비스의 이용약관을 보면 크게 세 가지 측면에서 유사하다. 첫째는 서비스 가용률 저하에 따른 손해배상이 아닌 서비스 중단 시의 손해배상을 원칙으로 하고 있으며, 둘째 고객이 서비스 장애를 발견하여 사업자에게 신고한 후 일정 시간동안 장애에 대한 복구가 이루어 지지 않을 경우 배상하도록 되어 있다. 세 번째, 서비스의 현황을 실시간으로 확인할 수 있는 모니터링 시스템은 제공하지 않고 있어, 실제 장애가 일어나도 고객이 이를 직접 경험한 후에야 신고를 할 수 있다.

5. 클라우드 컴퓨팅 환경의 SLA 프레임워크와 서비스 품질 확보방안

클라우드 컴퓨팅 서비스는 제공자가 범용으로 사용될 목적의 서비스를 개발한 후, 이를 서비스 저장소에 등재하고, 사용자는 이를 구독하는 형태로 사용한다. 또한, 클라우드 컴퓨팅 서비스는 제공자의 서버에서 실행되고, 사용자에게는 이 정보가 제공되지 않는다. 따라서 클라우드 컴퓨팅 서비스를 사용하는 중에 SLA에 명시되어 있는 서비스 품질(Quality of Service, QoS)이 제공되지 않을 경우 사용자의 업무에 큰 지장을 줄 수 있다. 따라서

QoS를 확보하기 위한 구체적인 방안이 마련될 필요가 있다. 이에 본고에서는 클라우드 컴퓨팅에서의 서비스 품질 확보를 위한 기술적, 제도적 대응방안을 제시한다.

가. 클라우드 컴퓨팅 서비스품질 확보를 위한 기술적 제언

1) 클라우드 컴퓨팅 SLA가이드라인 마련 및 세부 품질속성 정의

클라우드 컴퓨팅의 서비스 품질 확보를 위해서는 우선 서비스 품질 모델로서의 SLA와 그 구성요인으로서의 측정치(metric)들을 명확히 할 필요가 있다. 이를 통해 서비스 제공자가 '서비스 중단'과 같은 막연한 기준이 아닌, 세부적인 서비스 품질과 서비스 가용성에 따라 서비스 장애 등에 따른 피해보상 기준이 구체적으로 제시하여야 한다.

어떠한 측정(metric, indicator)를 사용해야 하는가는 산업군, 아웃소싱 상황을 둘러싼 주변 환경, 관련 법규와 표준, SLA에서 제공되는 서비스의 종류에 따라서 달라질 것이다. 앞의 아마존, 구글 등의 사례에서 살펴보았듯이, 클라우드 컴퓨팅과 관련한 아웃소싱 상황하에서 가장 중요한 척도는 '가용성'이며, 이 가용성을 구성하는 세부적인 요소들을 기준으로 측정치들을 구성할 필요가 있다. 여기서는 클라우드 컴퓨팅으로 제한하여 SLA에 포함되어야 할 측정치를 살펴본다. 우선 SLA의 측정치에 일반적으로 적용될 규칙은 다음과 같다.

〈표 4-15〉 SLA 측정치의 기본 규칙

가능한 간단하게	o '가용성'은 측정하기 어렵지 않다. 곧, 서비스가 제공되는가 그렇지 않은가? o 가능하다면, 서버, 네트워크, 어플리케이션 등으로 측정치를 개별적으로 설정하지 말라.
서비스 제공자의 관점이 아닌 사용자의 관점에서	o 서비스 사용자가 이해할 수 있도록 하라. o 시간단위(시, 분, 초), 수리에 걸리는 시간(MTTR:Mean Time To Repair)등으로 보기 쉽게 표현하라.

클라우드 컴퓨팅의 사례에 제한하여, SLA에 포함될 측정치를 생각해보면 다음과 같은 요소들이 포함될 필요가 있다.

〈표 4-16〉 클라우드 컴퓨팅에서의 SLA Metrics (예시)

Metrics	정의	세부사항
MTBF (Mean Time Between Failure)	(일반적으로)하드웨어 등의 고장 상황 사이의 간격	o 대형 Plant기기 또는 데이터센터 등의 신뢰성척도로 사용 o 길수록 좋다.
MTTR (Mean Time To Repair)	고장 상황 하에서, 수리하여 복구하는데 걸리는 시간	o 짧을수록 유리하다.
MTTF (Mean Time To Fail)	마지막 복구 상황에서 다시 고장 상황이 발생하는데 걸리는 시간	o MTBF = MTTF + MTTR
MTD (Maximum Tolerable Downtime)	조직의 업무나 제공되는 서비스가 회복할 수 없는 손실을 입지 않도록 중단을 허용할 수 있는 최대시간	o 자원과 서비스의 중요도 혹은 개별고객들의 QoS에 따라서 등급별로 구분할 수 있다. (예. 중요치 않음, 보통, 중요함, 치명적)
ABA (Abandonment Rate)	서비스 응답을 하지 못한 상황의 비율	o 헬프데스크, DBMS, 네트워크 등의 가용성 척도로 사용
ASA (Average Speed to Answer)	고객의 요청에 응답하는데 걸리는 시간	o 짧을수록 유리하다. o 클라우드 컴퓨팅 상황 하에서 서비스 사용자가 어플리케이션, 데이터를 불러들이는데 걸리는 시간

이와 함께 서비스 가용성에 따른 세부적인 피해보상의 수준을 차별화하여 설정하여 활용하도록 할 필요가 있다.

2) 클라우드 컴퓨팅에 대한 동적인 모니터링 시스템 구축

클라우드 컴퓨팅 서비스는 일반 소프트웨어 시스템과 달리, 소비자가 소유권을 갖고 있지 않다. 또한 클라우드 컴퓨팅 서비스는 블랙박스(Blackbox) 형태로 소비자에게 배포되고, 소비자의 의도와 상관없이 업그레이드 될 수 있다. 클라우드 컴퓨팅 서비스는 여러 사용자가 재사용할 수 있도록 만들어지고 배포되기 때문에, 서비스 제공자 역시 의도하지 않은 상황이 발생할 수 있다. 이로 인하여, 클라우드 컴퓨팅 환경에서의 서비스 관리는 일반 소프트웨어 시스템보다 관리가 어려우며, 서비스 제공자가 모든 관리를 하기 힘든 환경이다.

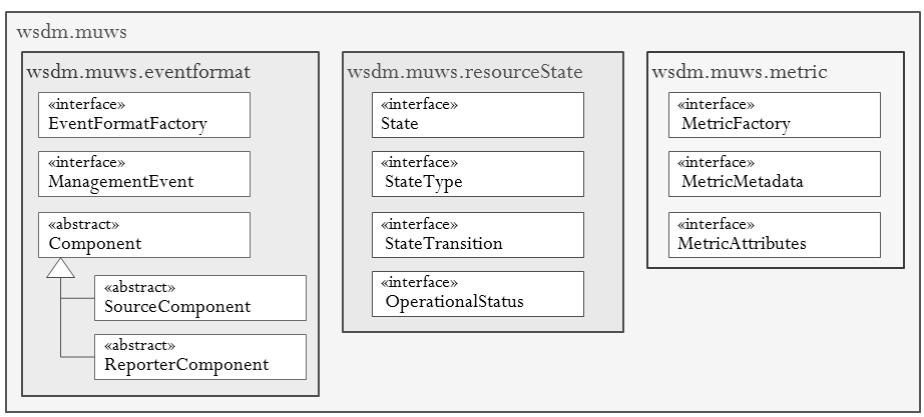
이에 클라우드 컴퓨팅의 서비스 품질을 구성하는 품질속성을 정의하는 것은 물론 이러한

품질 속성을 실시간 적으로 모니터링 하는 것이 중요하다. 클라우드 컴퓨팅 서비스 모니터링 시스템은 클라우드 컴퓨팅 서비스와 관련한 데이터를 가져와서 시각화하여, 현재 클라우드 컴퓨팅 서비스의 상태를 확인이 가능하도록 한다. 또한, 관련 데이터를 제공하기 위한 API를 제공하여 결함 분석이나, 서비스 유지 보수를 지원하는 다른 도구에서 필요한 데이터를 이용할 수 있는 메커니즘을 제공한다.

서비스 모니터링 시스템은 SLA에 지정된 품질 속성(메트릭)을 기준으로 수집 데이터를 결정해야 한다. 하지만 클라우드 컴퓨팅 서비스의 제한적 가시성으로 인하여 모니터링을 통한 데이터의 수집이 힘들다. 또한 클라우드 컴퓨팅 서비스는 필요에 따라 동적으로 구성될 수 있기 때문에, 데이터의 수집 역시 동적으로 이루어져야만 확실한 데이터의 수집이 이루어질 수 있다. 따라서 동적 모니터링을 위한 클라우드 컴퓨팅 서비스의 인터페이스를 별도로 정의하고, 모니터링 대상이 되는 데이터 및 정보 수집 과정을 정의해야 한다.

또한 클라우드 컴퓨팅 서비스의 모니터링 인터페이스도 서비스 외부에서 대상 서비스의 품질 속성에 대한 데이터를 수집할 수 있도록 기능을 제공해야 한다. 동적 모니터링을 위한 클라우드 컴퓨팅 서비스의 인터페이스는 〈그림 4-5〉에서 설명하는 WSDM과 같은 서비스 관리를 위한 표준문서를 참조하여 정의할 수 있다.

〈그림 4-5〉 웹서비스 관리 표준 (WSDM)



WSDM은 분산된 다른 서비스의 상태를 모니터링하고 관리하기 위해 OASIS에서 정의된 서비스 표준이다. WSDM을 이용하여 인터페이스를 정의한 서비스는 다른 서비스에서 해당 서비스에 접근하여 관련 데이터를 수집하는 것을 허용할 수 있고, 서비스에 영향을 미칠 수

있는 행위자가 정의되어 있다면 외부에서 접근하여 호출할 수 있게 한다. 물론 서비스 외부에서 수집할 수 있는 데이터는 서비스 제공자가 인터페이스로 허용한 값에 한하여 가능하게 된다. 또한 클라우드 컴퓨팅 서비스의 품질은 서비스 외적인 요소에 의해서도 많은 영향을 받기 때문에, 서비스의 외부 환경에 대한 동적 모니터링 역시 수행되어야 한다. 즉, 서비스가 배치된 서버의 상태와 서비스가 참여하고 있는 ESB의 상태, 총 서비스 호출 메시지의 수와 같은 외적인 환경에 대한 모니터링 역시 고려되어야 한다.

모니터링의 대상이 되는 데이터는 서비스 호출 수와 수행 시간, 반응속도와 같은 전통적인 모니터링 데이터와 대상 서비스의 상태와 품질 값과 같은 데이터가 수집될 수 있다. 서비스수준협약에서 지정된 품질 속성들과 관련된 데이터는 반드시 모니터링이 되어야 하며, 대상 서비스의 품질에 영향을 미칠 수 있는 외부 환경에 대한 데이터도 식별되어 수집되어야 한다.

3) 동적인 모니터링 환경제공을 위한 시스템 설계 지침 제공 및 적용

클라우드 컴퓨팅 서비스의 품질 평가 및 관리를 위해서는 클라우드 컴퓨팅 서비스의 현재 상황을 인지할 수 있어야 한다. 예를 들어 클라우드 컴퓨팅 서비스의 응답 시간을 확인하려면, 클라우드 컴퓨팅 서비스를 요청한 시간과 요청에 따른 반환 값이 돌아가는 시간을 알아야 한다. 그렇지만 제공되는 서비스가 원격에서 실행되고, 블랙박스(Blackbox)의 형태를 지니고 있어 서비스의 내부를 볼 수 없고, 네트웍을 사용함에 따른 품질의 불안정성을 가지고 있다. 따라서 실시간 모니터링을 통하여, SLA에서 지정된 품질 속성들의 값을 계산하여, 동적 품질 보증을 하도록 해야 하며, 다음과 같은 기술적 기법들의 적용이 필요하다.

① 동적으로 클라우드 컴퓨팅 서비스를 모니터링 기법의 적용

클라우드 컴퓨팅 서비스를 동적으로 모니터링 하려면 크게 두 가지 접근 방법이 있다. 먼저, 클라우드 컴퓨팅 서비스가 배치되어 있는 미들웨어 (예를 들어 Enterprise Service Bus)를 활용하는 것이다. 이런 미들웨어는 기본적인 정보를 모니터링하기 위한 API를 제공하는데, 이런 API를 이용하면 클라우드 컴퓨팅 서비스의 기본적인 정보는 가져올 수 있다.

그러나 API를 이용하여 가져오는 정보는 제약적이며, 미들웨어마다 다를 수 있다. 그러므로 추가적인 데이터를 가져오기 위해서는 미들웨어를 통해 전달되는 메시지를 가져오는 방법을 사용할 수 있다. 이는 악용될 경우 클라우드 컴퓨팅 서비스 사용자의 privacy 문제를 야기할 수 있으므로 주의하여야 한다. 다른 방법으로는 미들웨어 자체를 확장하여 클라

우드 컴퓨팅 서비스를 모니터링 하는 기능을 제공하는 방법이다. 이 방법에서는 관점 지향 프로그래밍 (Aspect-oriented programming)의 개념을 활용할 수 있다.

두 번째는, 클라우드 컴퓨팅 서비스를 관리 가능한 클라우드 컴퓨팅 서비스로 만들어서 배포할 수 있게 하는 것이다. 앞에서 말한 바와 같이 클라우드 컴퓨팅 서비스의 품질 모델이 정의되면, 품질 모델에 정의된 품질 메트릭에 필요한 요소들을 가져올 수 있도록 관리 인터페이스 (Manageability Interface)를 정의하고, 이를 구현하면 관리 가능한 클라우드 컴퓨팅 서비스로 배포할 수 있다. 관리 가능한 클라우드 컴퓨팅 서비스를 만드는 방법은 두 가지가 있다. 먼저 클라우드 컴퓨팅 서비스 자체에 관리 성을 추가하는 방법이다. 이 방법의 장점은 특정 미들웨어에 의존적이지 않고, 표준화된 클라우드 컴퓨팅 서비스 품질 모델을 따르고 있으므로 호환성 및 적용성이 높을 수 있다. 둘째, 미들웨어를 활용하는 방법보다 정교한 값을 가져올 수 있다. 미들웨어를 활용할 경우 미들웨어를 거쳐 클라우드 컴퓨팅 서비스의 품질을 측정하므로, 시간 관련된 품질 속성의 경우 클라우드 컴퓨팅 서비스 자체의 품질이라기보다 미들웨어에서 인식하는 클라우드 컴퓨팅 서비스의 품질이 될 수 있다.

그렇지만 모든 클라우드 컴퓨팅 서비스 제공자가 이런 관리 인터페이스를 준수한 클라우드 컴퓨팅 서비스를 만드는 것은 제한적이 될 수 있으며, 클라우드 컴퓨팅 서비스의 성능에도 영향을 줄 수 있다. 이에 첫 번째 방법의 장점을 취하고, 두 번째 방법의 단점을 보완하는 방법으로 동적 모니터링 에이전트를 추가하여 클라우드 컴퓨팅 서비스를 관리 가능한 클라우드 컴퓨팅 서비스로 개발하는 방법이다. 이 방법은 실제 클라우드 컴퓨팅 서비스는 동적 모니터링 에이전트와 참조할 수 있는 API만 제공하고, 실제 관리 인터페이스를 구현하고 데이터 정보를 모으는 기능은 동적 모니터링 에이전트에 구현하는 방법이다. 이 방법을 위해서는 기존에 있는 디자인 패턴 (예를 들어 Observer 패턴, Decorator 패턴 등)을 사용할 수 있다.

② 실행시간에 발생하는 서비스 오류 (Fault)에 대한 자동 교정기법의 적용

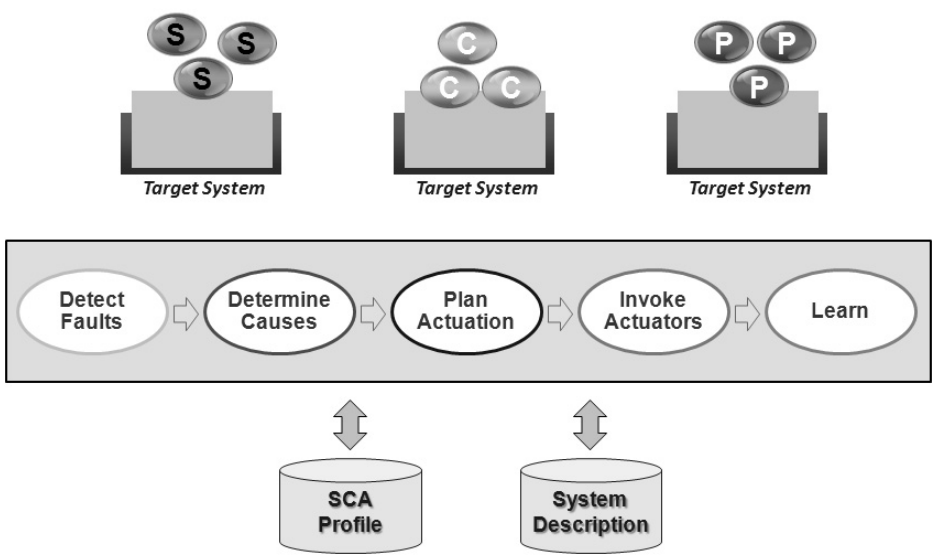
클라우드 컴퓨팅 서비스는 전통적인 소프트웨어와 달리 클라우드 컴퓨팅 서비스의 소유권이 클라우드 컴퓨팅 서비스 사용자에게 있지 않다. 클라우드 컴퓨팅 서비스 제공자의 입장에서는 제공자 서버에 설치되어 있는 하나의 클라우드 컴퓨팅 서비스를 여러 명이 동시에 접속하여 사용하는 경우가 빈번하다.

이로 인하여 실행시간에 발생하는 서비스 오류는 서비스 사용자가 제어할 수 없고, 서비스 제공자 역시 제어하기 힘들다. 예를 들어 동시에 클라우드 컴퓨팅 서비스를 100명만 사

용하고 있다고 하자. 실행시간에 서비스 오류가 발생하는 것을 실시간으로 처리하려면, 서비스 제공자 입장에서는 100명의 관리자가 필요하게 된다. 이를 해결하기 위한 방법이 서비스 오류 자동 교정 기법이다. 이 기법은 IBM에서 제안한 자율 컴퓨팅을 응용하여 개발할 수 있다.

자율 컴퓨팅 (Automatic Computing, 이하 AC)은 사람의 직접적인 조정 없이 자율적인 방식 하에 스스로가 관리하도록 시스템을 설계하는 방식이다 . AC는 시스템을 자율적으로 관리할 수 있는 주요 원칙들을 제안하고 있으므로, 서비스 관리에 관한 기술적 이슈들은 AC의 기법들을 사용하여 해결될 수 있다. 즉, 서비스 관리 작업의 대부분이 AC를 적용함으로써 자동화가 가능해진다. 오류 자동 교정 기법은 일반적으로 다음과 같은 순서로 수행될 수 있다.

〈그림 4-6〉 오류자동 교정기법 개요



'오류 발견(detect)' 단계에서는 관리 대상 서비스로의 호출을 모니터링 한 결과를 기반으로 비정상 상태 (abnormality)를 알아낸다. 여기서 모니터링한 결과는 동적 모니터링을 통하여 이루어진다. 비정상 상태란 실제 서비스에서 전달된 결과 값과 기대치 사이에 현저한 차이를 나타내는 관찰 가능한 상황 혹은 서비스의 상태를 일컫는다.

'원인 결정' 단계에서는 발견된 오류를 유발할 수 있는 원인을 결정한다. 우리는 이전 진

단 기록을 관리하고 원인 결정과 관련 있는 전문 지식을 축적할 수 있는 SCA 프로파일이라는 특화된 지식 베이스를 사용 한다.

‘치료(해결) 계획 (plan)’ 단계에서는 결정된 원인을 해결할 수 있는 가장 효과적인 치료(해결) 방법을 결정하고, 선택된 관련 모듈의 실행 계획을 세운다. SCA 프로파일은 이전 치료(해결)들의 기록을 관리하고 치료(해결) 계획과 관련 있는 전문 지식들을 축적한다. 치료(해결)와 관련된 모듈의 실행 계획은 현재의 클라우드 컴퓨팅 서비스 환경, 관리되는 서비스의 특징, 서비스의 현재 상태가 반드시 고려되어야 하므로 상당히 기술적인 작업이다.

치료(해결)와 관련된 모듈 호출 (invoke)’ 단계에서는 서비스 혹은 서비스가 수행되고 있는 SOA 환경에서의 원인을 해결하기 위하여 치료(해결)와 관련된 모듈을 실행한다. 치료(해결)은 관리되는 서비스들의 내부 또는 외부 (즉, 환경)에서 실행될 수 있다. 내부적인 치료(해결)를 위해 관리 서비스는 치료(해결)를 지원하는 인터페이스를 구현해야 하며 외부적인 치료(해결)는 일반적으로 클라우드 컴퓨팅 서비스 미들웨어 또는 Enterprise Service Bus 인터페이스와 같은 서비스 버스를 통해 실행된다.

‘Learn’ 단계에서는 SCA 프로파일이라는 지식베이스를 업데이트한다. SCA 프로파일은 치료(해결) 적용을 통해 획득할 수 있는 새로운 기록과 측정값, 서비스 사용자에 의해 평가되는 만족도로 업데이트되어야 한다. 이 프로파일을 업데이트하는 것은 원인을 보다 정확하게 진단하고, 보다 효과적인 치료(해결)하기 위해 매우 중요하다.

나. 클라우드 컴퓨팅 서비스 품질 확보를 위한 제도적 대안

1) 클라우드 컴퓨팅 서비스 품질 인증제도 마련

앞서 설명한 서비스 품질확보를 위한 기술적 노력들과 함께 병행되어야 하는 부분이 바로 서비스 품질 인증제도이다. 클라우드 컴퓨팅 ‘서비스 품질 인증제도’는 SLA가이드라인에서 명시된 서비스 품질속성들이 제대로 관리되고 있는지, 고객을 위한 실시간 모니터링 시스템과 복구 시스템 등 서비스 장애에 대비한 소비자 보호조치들이 제대로 마련되어 있는지, 데이터 보안이나 Mirroring(실시간 데이터 백업), 임치제도 등과 같이 서비스 중단이나 장애에 대비한 준비가 잘 갖추어져 있는지 등을 종합적으로 평가하고 그 결과를 고객들에게 제공함으로써 고객의 선택권을 넓히고, 사업자들의 사용자 보호를 위한 투자와 준비를 촉진하도록 하기 위함이다.

이를 위해 클라우드 컴퓨팅 서비스 사업자가 제공하는 서비스에 대하여 이를 시험하고 최소한의 QoS가 보장되는지를 시험한 후, 이를 인증하도록 할 필요가 있으며, 이를 위해서는 다음과 같은 요소들이 준비되어야 한다.

① 인증 대상이 되는 클라우드 컴퓨팅 서비스의 범주와 대상 정의

인증제도의 도입을 위해서는 우선 인증대상이 되는 클라우드 컴퓨팅 서비스의 범주와 대상을 정의해야 한다. 이는 현행 법체계의 개선과 함께 추진될 필요가 있다. 현재 통신서비스와 인터넷서비스 중심으로 구성되어 있는 전기통신기본법, 전기통신사업법, 정통망법 등에 클라우드 컴퓨팅을 도입함으로써 클라우드 컴퓨팅의 서비스 유형을 구분하고, 인증대상이 되는 클라우드 컴퓨팅 서비스의 유형과 사업자의 형태를 정의할 필요가 있다.

② 서비스 인증 프로세스, 즉 절차와 세부 지침을 정의

인증대상이 되는 서비스의 범주와 대상이 정해지면, 서비스 인증을 위한 프로세스가 구체적으로 정의될 필요가 있다. 즉 인증의 신청에서부터 시험, 결과 통지 등 모든 절차를 마련하고, 절차별로 준수되어져야 하는 세부지침을 정의해야 한다. 세부지침으로는 구체적으로 어떠한 항목을 측정의 대상으로 삼을 것이며, 인증을 만족시키는 기준 등을 정의해야 한다.

③ 인증을 위한 시험 기법 제정 및 인증기관의 자격 및 책임정의

인증을 위해 필요한 세부 항목들과 기준들이 제시되면, 이를 실질적으로 측정할 수 있는 세부적인 시험기법이 마련되어야 한다. 이와 함께 어떠한 기관이 인증을 수행할 것인지에 대한 자격과 그에 따른 책임도 정의되어야 한다.

제 2 절 클라우드 컴퓨팅 상호운용성확보방안

1. 클라우드 컴퓨팅 상호운용성의 필요성

클라우드 컴퓨팅 서비스의 건전한 발전과 활성화를 위해 가장 먼저 선결되어야 하는 요소가 상호운용성의 확보인데, 그 이유는 현재 제품화된 다양한 클라우드 컴퓨팅 서비스들은 각기 다른 플랫폼과 인터페이스 제공 방식으로 인해 서로 다른 벤더 또는 사업자가 제공하

는 클라우드 컴퓨팅 서비스간의 자유로운 연동이 불가능하기 때문이다. 이는 향후 클라우드 컴퓨팅 서비스가 확산될 경우 이용자의 데이터와 서비스가 클라우드 컴퓨팅 서비스 제공자나 벤더에게 종속되는 등의 매우 심각한 문제를 야기할 수 있게 된다. 이 밖에도 클라우드 컴퓨팅을 통한 상호운용성 확보는 다양한 서비스의 개발과 이용환경을 가능하게 함으로써 클라우드 컴퓨팅 서비스의 활성화를 촉진시키게 된다.

〈표 4-17〉 클라우드 컴퓨팅 상호운용성 확보의 중요성

클라우드 컴퓨팅 상호운용성 확보가 필요한 이유 5가지
1. 사업자나 벤더로 부터의 데이터 고착화(Lock-in) 탈피
2. 사업자나 벤더의 플랫폼 또는 서비스로 부터의 종속성 탈피
3. 개방형 API를 통한 클라우드 컴퓨팅 서비스 개발 효율성 제고
4. 다양한 클라우드 컴퓨팅 서비스 이용 환경 제공 (효율적 클라우드 컴퓨팅 서비스 보급)
5. 이종 클라우드 컴퓨팅 서비스간 연동 가능 (하이브리드 클라우드 실현)

따라서, 향후 클라우드 컴퓨팅 서비스가 활성화되기 위해서는, 특정 벤더나 사업자에 서비스와 데이터가 종속되지 않는 환경 속에서 다양한 이용자 환경과 수요를 효과적으로 지원할 수 있도록 하는 상호운용성 확보에 대한 기술적 지원 및 정책적 대응이 매우 중요하다.

클라우드 컴퓨팅 서비스의 상호호환성 확보는 각 사업자의 독립적 비즈니스 모델을 침해하지 않는 범위 내에서 협의된 형태의 상호 호혜적인 표준화된 플랫폼과 표준화된 인터페이스의 사용을 통해서 가능하다. 상호운용성에 관한 정의를 전산학에서의 일반적인 정의와 클라우드 컴퓨팅 서비스에서의 정의로 정리한다. 일반적인 전산학 분야에서의 상호운용성에 관한 정의는 다음의 ISO 정의와 IEEE 정의가 대표적이다.

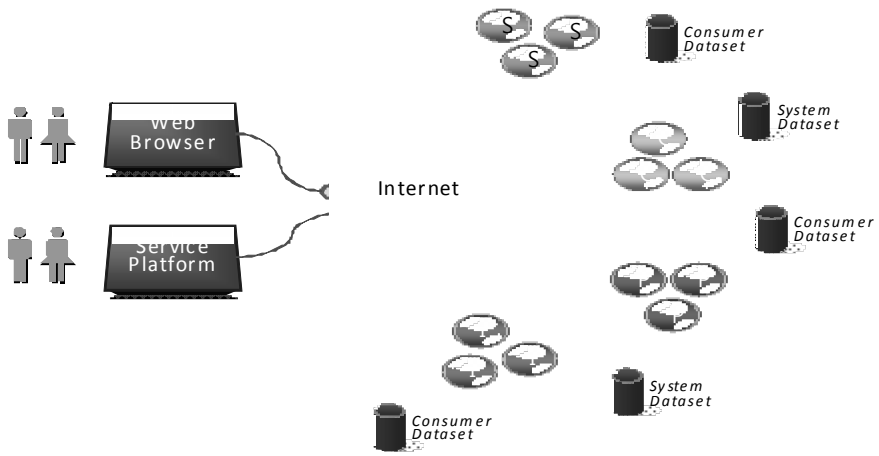
> "The capability of the software product to interact with one or more specified systems [ISO9126]."
> "The ability of two or more systems or components to exchange information and to use the information that has been exchanged [IEEE610][IEEE610.12]."

클라우드 컴퓨팅에서의 상호운용성은 서비스를 제공하기 위해 여러 조직이 효율적으로 정보를 교환하고, 그 정보를 사용할 수 있는 능력이로 정의할 수 있다. 조직에는 국민, 기업, 정부가 있으며, 효율적인 정보 교환을 위해 이들 조직 간의 일관된 정보 흐름이 정의되

어야 하며, 효율적으로 정보를 사용하기 위해서는 정보를 처리 하는 프로세스 및 기술에 관한 일관된 원칙과 표준이 정의되어야 한다.

다음의 그림은 이러한 클라우드 컴퓨팅 서비스들이 형성하고 있는 클라우드 그리드(Grid)를 나타낸다.

〈그림 4-7〉 다양한 클라우드 컴퓨팅 서비스들로 이루어진 그리드



이러한 클라우드 그리드환경에서의 상호운용성은 다음과 같은 이슈들이 존재한다.

〈표 4-18〉 클라우드 컴퓨팅의 상호운용성 이슈

클라우드 컴퓨팅 상호운용성 관련 문제점
1. 클라이언트 프로그램에서 기대하는 인터페이스와 클라우드 컴퓨팅 서비스간의 인터페이스 불일치(No Match) 및 부분일치(Partial Match) 문제
2. 하나의 클라우드 컴퓨팅 서비스가 실행되는 과정에 다른 클라우드 컴퓨팅 서비스를 실행(Invoke)하는 경우, 상호운용에 따른 인터페이스 불일치 문제
3. 서비스 저장소에 등재되어 운영되는 클라우드 컴퓨팅 서비스가 유지보수에 따라 인터페이스나 기능성 등의 변경으로 인한 상호운용 문제
4. 특정 도메인에서 요구되는 국. 내외 표준 인터페이스가 있을 경우, 이를 준수하지 못한 클라우드 컴퓨팅 서비스의 상호 연동 문제

이러한 문제들은 정부기관의 공공 서비스나 공공 정보를 공유할 목적의 클라우드 컴퓨팅 서비스일 경우, 더욱 중요한 이슈가 된다. 그 이유는 공공 서비스와 상용 개별(Private) 시

스템이나 서비스간의 상호운용의 빈도가 높기 때문이다.

2. 클라우드 컴퓨팅 상호운용성 확보를 위한 글로벌 동향

클라우드 컴퓨팅 서비스의 상호운용성 확보 노력은 다양하게 진행되고 있는 표준화 활동으로 대변될 수 있으며, 주로 클라우드 컴퓨팅 서비스의 상호운용성 확보를 위한 표준개발을 목표로 클라우드 컴퓨팅 서비스 연동을 위한 플랫폼 표준화 및 개방형 인터페이스 표준화 등을 포함하고 있다. 클라우드 컴퓨팅 관련 표준화 활동은 대부분 최근 '09년부터 시작되었으며, OCC, CCIF, OGF, DMTF, CSA 등의 사실표준화 기구를 통해 이루어지고 있다. 지난해 말 공식표준화 기구로서는 처음으로 ISO/IEC JTC 1에서 클라우드 컴퓨팅 연구그룹을 신설하여 클라우드 컴퓨팅 표준화에 착수하였다.

클라우드 컴퓨팅 관련 표준화 활동은 대부분 최근 '09년부터 시작되었으며, OCC, CCIF, OGF, DMTF, CSA 등의 사실표준화 기구를 통해 이루어지고 있다. 지난해 말 공식표준화 기구로서는 처음으로 ISO/IEC JTC 1에서 클라우드 컴퓨팅 연구그룹을 신설하여 클라우드 컴퓨팅 표준화에 착수하였다.

〈표 4-19〉 클라우드 컴퓨팅 상호운용성을 위한 글로벌 표준화 활동현황

표준화 단체명	주요 표준화 내용 및 현황	착수시기
오픈 그리드 포럼 (OFG: Open Grid Forum)	OCCI(Open Cloud Computing Interface) WG 구성을 통하여 클라우드 컴퓨팅 인프라를 위한 오픈 클라우드 컴퓨팅 인터페이스 표준화 착수	'09. 04
클라우드 컴퓨팅 상호호환성 포럼 (CCIF: Cloud Computing Interoperability Forum)	글로벌 클라우드 컴퓨팅 에코시스템 개발 및 단일화 된 클라우드 인터페이스 개발 착수	'09. 06
분산 관리 태스크 포스 (DMTF: Distributed Management Task Force)	가상화 (개방형 가상화 포맷 표준) 관련 표준화 개발 및 개방형 클라우드 표준화 인큐베이터 생성	'09. 03
오픈 클라우드 매니페스토 (Open Cloud Manifesto)	IBM을 중심으로 하는 미국기업 위주의 표준화 연합	'09.03
오픈 클라우드 컨소시움 (OCC: Open Cloud Consortium)	인터 클라우드 간 상호호환성 표준개발, 학계가 중심의 비영리 컨소시엄	'09. 01

〈표 4-19〉 클라우드 컴퓨팅 상호운용성을 위한 글로벌 표준화 활동현황(계속)

표준화 단체명	주요 표준화 내용 및 현황	착수시기
클라우드 보안 협의체 (CSA: Cloud Security Alliance)	클라우드 컴퓨팅 보안 관련 유즈케이스 및 보안 가이드라인 개발	'09. 06
스토리지 네트워킹 산업 협회 (SNIA: The Storage Networking Industry Association)	스토리지 관련 표준, 기술, 교육 등을 지원하는 비영리 단체로서 최근 Cloud Storage Initiative (CSI) 구성을 선언하고 성공적인 클라우드 스토리지 시장 확대를 위한 관련 기술문서 및 인터페이스 표준화 등을 추진 중	'09. 04
ETSI(European Telecommunications Standards Institute)	ETSI TC(Technical Committee) GRID를 통하여 클라우드 컴퓨팅의 IaaS를 Telco 진영에서 사용하기 위한 표준 기반의 검증 도구와 글로벌 표준 개발을 추진 중	'09.03
국제전기통신연합 (ITU-T)	2009년 국제전기통신연합 통신부문 연구반 17 (SG17) 회의에서 클라우드 컴퓨팅 및 기타 최근 보안 이슈에 대한 전략을 위하여 대응반을 개설	'09.09
ISO/IEC	JTC 1 에서는 SGCC(Study Group on Cloud Computing)을 신설하고, 클라우드 컴퓨팅 관련 표준화 이슈 분석 및 표준개발 추진 중	'09.10

본 고에서는 이중 오픈 클라우드 컨소시움, 오픈 그리드 포럼, 오픈 클라우드 매니페이토, 분산관리TF, 클라우드 보안 연합의 구성 및 활동 등에 대하여 보다 자세히 알아본다.

가. OCC (Open Cloud Consortium)

OCC는 2008년 미국의 대학 연구소를 중심으로 설립되어 클라우드 컴퓨팅의 공개표준에 대하여 연구를 진행 중이다. 주요 활동은 대용량 데이터 클라우드를 위한 표준과 상호운용에 관한 워킹그룹, 개방형 클라우드 테스트베드 워킹그룹, 클라우드 사이의 정보공유와 보안에 관련된 워킹그룹, 표준 클라우드 성능 측정과 평가 시스템에 관한 워킹그룹 등 4개 워킹그룹을 통해 이루어지며, 주요현황은 〈표 4-23〉와 같다.

〈표 4-20〉 OCC(Open Cloud Consortium〉 표준화 활동현황

구성	주요내용
목적	o 상호운용을 위해 클라우드 컴퓨팅 및 프레임워크에 대한 표준의 개발을 지원 o 클라우드 컴퓨팅을 위한 벤치마크를 개발 o 클라우드 컴퓨팅에 대한 참조구현과 Open Source 참조구현을 지원 o Open Cloud Testbed라 불리는 클라우드 컴퓨팅을 위한 Testbed를 관리. o 클라우드 컴퓨팅에 관련된 Workshop과 행사를 후원.
주요 참여자	o Member : Aerospace, CISCO, MIT Lincoln Labs, Northwestern University, Open Data Group, Sector Project, University of Illinois at Chicago, Yahoo
	o Contributing Members : Calit2, Johns Hopkins University, National Lambda Rail,University of Chicago
주요활동	o Working Group on Standards and Interoperability For Large Data Clouds (대용량 데이터 클라우드를 위한 표준과 상호운용성에 관한 워킹그룹) - 클라우드 컴퓨팅의 구조를 대중화를 위해 Google 기술보고서를 사용 - 클라우드 컴퓨팅의 구조는 Google에서 개발한 소프트웨어 프레임워크 MapReduce와 Open Source Hadoop system활용 - 주목적은 대용량 데이터 Cloud들 사이의 상호운용을 위해 표준개발 · Hadoop, Thrift, Sector와 Pig 사이의 상호운용 평가. · ‘Storage clouds와 Compute clouds의 표준 인터페이스 연구 · ‘대용량 데이터를 위한 적절한 벤치마킹 대상 탐색 o The Open Cloud Testbed Working Group (개방형 클라우드 테스트베드 워킹그룹) - Open Cloud Testbed 운영/관리 (Testbed는 네트워크 연결을 위해 Cisco C-Wave와 UIC Teraflow Network를 사용 - 두 네트워크는 National Lambda Rail에 의해 제공되는 파장을 사용 o The Open Science Data Cloud (OSDC) Working Group (클라우드 사이의 정보 공유와 보안에 관련된 워킹그룹) - 과학적인 데이터를 위한 대용량 데이터를 운영/관리. - 클라우드 사이의 정보 공유를 위한 표준과 표준 기반 구조에 초점 - 다른 기관에 속하여 다른 권한과 정책을 가진 클라우드 사이의 정보 공유와 보안에 대해 연구 o Intercloud Testbed Working Group(표준 클라우드 성능 측정과 평가 시스템에 관한 워킹그룹) - 다양한 클라우드 컴퓨팅 제공자들의 성능, 보안, 품질을 비교할 수 있는 용이한 방법을 제공 - 사용 케이스(Use Case)를 다듬고, 요구사항을 수집하여 벤치마크를 개발하는 것을 목표 - CCIF(Cloud Computing Interoperability Forum)과 협조 관계

〈표 4-20〉 OCC(Open Cloud Consortium〉 표준화 활동현황(계속)

구성	주요내용
현황	o Yahoo는 OCC에 500node와 2천개의 코어 클러스터 기부(Open Cloud Testbed와 Open Science Data Cloud 그리고 Intercloud Testbed에 사용) o 고성능 Computing을 위한 국제컨퍼런스에서 광범위한 지역 Cloud에 집약적인 애플리케이션 지원하는 새로운 기술을 이끎.

나. Open Cloud Manifesto

아마존, 구글, MS등 경쟁기업들에 비해 클라우드 컴퓨팅에서 다소 뒤쳐진 IBM은 업체들이 주도하고 있는 다양한 클라우드 간의 상호운용을 가능하도록 하기위해 '09년 3월30일 클라우드 컴퓨팅 개방 선언문(The Open Cloud Manifesto)를 발표하였으며, 이에 150여개 이상의 IT기업들과 수요기업들이 지원하게 된다. 이를 통해 모든 컴퓨터 업체가 클라우드 컴퓨팅 서비스를 공개하여 상호운용이 가능하도록 하며, 고객들이 어려움 없이 서비스 공급업체를 변경할 수 있도록 하자는 것이다. 그러나 현재 시장을 주도하고 있는 마이크로소프트사와 세일즈포스닷컴, 아마존 등이 참여를 거부하면서 시장에서의 주도권 쟁탈이 가열되고 있다.

〈표 4-21〉 Open Cloud Manifesto 표준화 활동현황

구성	주요내용
목적	o 미국 기업의 경쟁력에 기여 o 기업설립 초기에 과다한 IT비용 지출하지 않아도 IT 경쟁력을 갖춤 o 기업의 정보와 IT 시스템으로 인한 경쟁력 차이 줄임 o 美 중소기업 경쟁력 증진에 기여 o 소프트웨어와 하드웨어뿐만 아니라 소비자를 대상으로 서비스를 제공 o 클라우드 컴퓨팅에 맞는 컴퓨터, 사이트, 부품개발 등 관련 사업 시장 확대
주요 참여자	o EMC, IBM 인터넷 시큐리티 시스템, Novell, SUN Microsystems, AT&T, CISCO Systems, 레드햇, VM웨어
주요활동	o 통제할 수 없는 시스템에 대한 보안성 강화 o 표준 인터페이스 상호작용을 위한 데이터 및 응용프로그램 확장 o 데이터와 응용프로그램의 이식성을 높이기 위해 표준 인터페이스 제공 o 표준화된 Cloud Infra를 위해 Governance 및 관리 강화 o 더 나은 서비스 수행을 위해 지속적인 모니터링 실시

〈표 4-21〉 Open Cloud Manifesto 표준화 활동현황(계속)

구성	주요내용
현황	o 클라우드 컴퓨팅과 관련한 법률, 기술, 관리 등 클라우드 컴퓨팅 공급업체와 고객이 반드시 해결해야 하는 포괄적인 이슈에 관하여 설명한 “클라우드 컴퓨팅의 주요 분야 포커스 가이드(Guidance for Critical Areas of Focus in Cloud Computing)” 기술 논문 배포 예정 o 클라우드 컴퓨팅 솔루션을 안전하게 도입하기 위한 권위 있는 가이드를 제공하기 위해 거버넌스, 법률, 네트워크 보안, 감사, 애플리케이션 보안, 스토리지, 암호화, 가상화, 리스크관리 등 여러 분야의 저명한 전문가들을 합류 o 보안을 위한 Best Practice 이용 촉진과 다른 형태의 컴퓨팅을 보호할 수 있는 방법에 관해 교육

다. OGF (Open Grid Forum)

오픈그리드포럼은 클라우드 컴퓨팅 등장 이전부터 그 기반이 되는 그리드 컴퓨팅환경에서의 상호운용성 확보를 위해 지속적인 표준화 활동을 전개해 왔으며, 최근에는 그 중 IaaS 분야에서 클라우드에 인터페이스 할 수 있는 현실적인 솔루션을 제공하는 것을 목표로 OCCI-WG(Open Cloud Computing Interface WG)를 구성하여 활동 중이다. 이들은 클라우드 컴퓨팅 기반구조의 원격관리를 위한 API Specification개발을 목표로 한다. 원격관리 기능에는 배치, 자율적 스케일링(Automatic Scaling), 모니터링 등의 공통 업무가 포함이 되며, 다양한 상용 클라우드들[58]과의 상호운용성을 고려하여 연구가 진행되고 있다.

〈표 4-22〉 OGF (Open Grid Forum) 표준화 활동현황

구성	주요내용
목적	o 급속한 진화와 응용 분산컴퓨팅의 채택을 유도하는 역할을 수행 o 기업과 연구자들의 생산성을 향상하고 혁신적인 애플리케이션과 인프라를 개발 o Open Forum을 통하여 공동체를 형성하여 트렌드를 탐색 o 최고의 모델을 공유하고 표준으로 만드는 일을 수행
구성	o Platinum Organizational Member : Microsoft
	o Gold Organizational Member : Fujitsu, Mimos, Oracle, Sun microsystems
	o Silver Organizational Members : Altair Engineering, Canarie CYBERA, Fermila, Grid Consortium Japan, Grid Forum Korea, NetAPP, SDSC, SAS, UNICORE

58) Amazon EC2 API, ElasticHosts API, FlexiScale API, GoGrid API, Sun Cloud API 등

〈표 4-22〉 OGF (Open Grid Forum) 표준화 활동현황(계속)

구성	주요내용
주요활동	o OGF는 3개의 그룹으로 구분 - Working Groups : 하나 이상의 document들을 통하여 표준을 정의 - Research Groups : 문서를 작성하거나 워크숍을 통해 관심이 가는 주제를 조사 - Community Groups : Community를 조직하여 필요요건 정의와 워크숍 운영, 문서작성을 담당 ※ 연례 전원참석 미팅, 워크숍, Group Sessions, 다른 조직과의 위치 통합을 수시로 실시함 o 주요 활동 목표 - Grid 혁신을 위한 Open Forum 개최 - 그리드 상호운용성을 위한 개방형 표준 개발 - Grid Community의 핵심 인물과 조직들을 결집하여 활성화를 위한 장애요소를 제거하고, 베스트프랙티스를 도출 - 현 산업표준과새 사양들과 일치시키도록 다른 표준 개발 조직들과 협업
현황	o Cyberinfrastructures Requirements - 상호운용성을 위한 Community의 필요사항을 듣기 위해 워크숍을 개최 - EGEE와 TeraGrid간에 정보를 제공하기 위해 연속적으로 워크숍을 개최중 ※ 첫 번째 워크숍 OGF-26에는 UK e-Science와 UK NGS, Teragird, Globus 등이 참여. 이를 통해 OGF Informational Document를 제작 o Production Grid Interoperability - Production Grid Infrasturcture인 WG는 상호운용표준을 수립하기 위해 결성 - EGEE, OSG, NAREGI, NorduGrid, TeraGrid, NGS 등이 참여

라. CSA (Cloud Security Alliance)

클라우드 컴퓨팅의 확산에 따라 가장 큰 장애요소인 보안이슈에 대응하기 위해 미국의 기업들을 중심으로 클라우드 시큐리티 얼라이언스(Cloud Security Alliance, www.cloudsecurityalliance.org, 이하 CSA)가 출범했다.

CSA는 클라우드 컴퓨팅 제품을 도입하는 업체들에 보안에 관한 조언을 제공하는 한편, 베스트 프랙티스 이용을 촉진하고 클라우드 컴퓨팅이 다른 형태의 컴퓨팅을 보호할 수 있는 방법에 관한 교육을 제공한다. CSA는 2009년 4월, "Cloud Security Alliance issues Guidance for Critical Areas of Focus in Cloud Computing"을 발표하고, 아키텍처, 관리, 운용측면에서 구분된 15개의 도메인에서 고려해야 할 보안 이슈에 대한 방향성을 제시했다.

〈표 4-23〉 CSA (Cloud Security Alliance) 표준화 활동현황

구성	주요내용
목적	o 클라우드 컴퓨팅에서 보안을 보장하기 위해 최고의 실행방법의 사용을 촉진 o 클라우드 컴퓨팅을 사용함에 있어 다른 컴퓨팅들을 보호하도록 교육을 제공 o 클라우드 컴퓨팅의 보안 유지를 위해 비영리적으로 조직된 공동체.
구성	o Affiliates Member : ASP-SaaS, bdigital, OWASP, Jericho, ISACA, OpenGridForum, ENISA
	o Corporate Member : AbsoluteSoftware, ArcSight, at&t, cisco, FIBERLINK, McAfee, Iron Mountain, HP, NetWitness, Microsoft, Ping Identity, Qualys, rackspace, RSA, sonoa, terremark, verizon, vmware, websense, zscaler
주요활동	o 클라우드 컴퓨팅의 소비자와 공급자간의 필요한 보안요구사항과 보증인증들에 관해 상호 이해 o 개별 연구들이 클라우드 컴퓨팅의 보안을 위한 최고의 관행이 되도록 촉진 o 보안솔루션들의 적절한 사용을 촉진하는 교육프로그램과 홍보프로그램 런칭 o 이슈들에 대한 합의목록을 만들고, 클라우드 보안 인증에 대한 가이드를 생성
o 현황	o ENISA와 파트너쉽 채결 o IT 회계 교육과 도구를 제공하기 위해 ISACA와 협업 o OWASP와 함께 웹의 특정 이슈들에 대한 동업자들의 평가 o CSA guidance Ver.2를 2009년 11월의 발표 o 산업, 정부, 특정의 이익을 위한 Working group 운영 o 클라우드 공급자와 소비자 간에 멤버십 체결

마. 분산 관리 TF (Distributed Management Task Force)

DMTF는 1992년 설립된 표준 개발기구로 기업과 기관, 개인회원이 멤버로 활동하고 있다. 현재 AMD, Broadcom, CA, Inc., Cisco, Citrix, Dell, EMC, Fujitsu, HP, Hitachi, IBM, Intel, Microsoft, Novell, Oracle, Sun Microsystems, VMware 등이 회원으로 참여하고 있다. 이들은 표준화를 위한 공동개발을 수행하고, 다양한 단체 및 학계와도 제휴를 통해 개방형 클라우드를 위한 노력을 기울이고 있다.

현재 클라우드 컴퓨팅 시장을 주도하고 있는 다양한 기업들이 참여하며, 표준화 작업에서 자사의 영향력 확대를 위해 노력 중이다. 네트워크상에서 분산되어 있는 다양한 시스템과 디바이스에 대한 관리 표준을 정하기 위해 WBEM(Web-Based Enterprise Management) 표준을 제정했고 이것을 마이크로소프트에서 구현한 것이 WMI 이다. 현재 DMTF는 WBEM 표준에서 다양하고 분산된 시스템 자원들에 대한 정보를 액세스하기 위해 단일 데

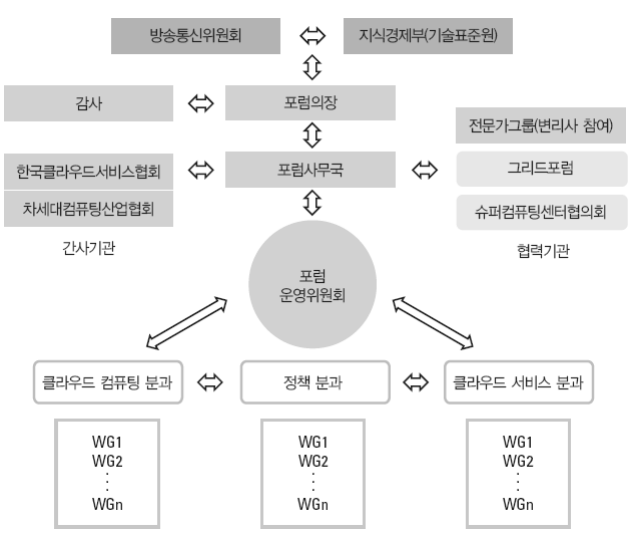
이터 스카마를 표준으로 제정하고, 이 스키마를 기준으로 자원정보를 액세스하도록 권고 한다. 이 데이터 스키마 표준은 CIM(Common Information Model)로서 WMI 역시 CIM 스키마를 따르고 있다.

VMware도 시스템관리 정보표준 모델기능과 구조에 대한 표준을 제정하는 DMTF에 vCloud API를 제공하였다. vCloud API는 VMware-vCloud 이니시어티브의 일부분으로써, 애플리케이션의 이동과 프로비저닝, 운영 등 내•외부 클라우드 환경에서 구동할 수 있도록 돕는 역할을 하는 것으로, VMware는 이를 통해 자사의 vCloud API가 향후 클라우드 컴퓨팅 서비스의 기준 제시의 밑거름이 되기를 기대하고 있다.

3. 클라우드 컴퓨팅 상호운용성 확보를 위한 국내 움직임

국내에서는 아직 클라우드 컴퓨팅 서비스의 상호운용성 제공을 위한 공식적인 지침이나 표준이 마련되지 않았으며, 올해부터 본격적인 클라우드 컴퓨팅 관련 표준 개발에 착수할 예정이다. 지난해 한국과학기술정보연구원(KISTI)을 주축으로 한 '한국클라우드컴퓨팅협의회(CCKI)'와 차세대컴퓨팅협회를 중심으로 한 '클라우드컴퓨팅산업포럼'이 개별적으로 신설되어 활동을 전개하다가 '09년 7월 통합기구의 형태로 '클라우드컴퓨팅포럼(CCF)'가 출범되어 클라우드 컴퓨팅 관련 표준화 및 법제도 개선안 개발 등을 추진하고 있다.

〈그림 4-8〉 클라우드컴퓨팅포럼 조직도



클라우드 컴퓨팅 포럼은 관련 포럼 및 협의체들의 국가적 차원에서 통합 포럼 구성하고, 기술개발의 표준화 방향 제시, 기술표준화 연구개발, 국제표준화 활동지원, 클라우드 컴퓨팅 및 서비스 관련 응용산업 분야 법-제도 개선안 도출, 정책건의를 목적으로 컨퍼런스 개최 등 다양한 활동을 수행 중이다.

국내 표준화 관련해서는 지난해 말 정보통신기술협회(TTA) 산하에 클라우드 컴퓨팅 프로젝트 그룹(PG420)의 신설이 결정되었으며, 올해부터 정보통신표준개발지원 사업의 일환으로 '클라우드 컴퓨팅 표준 개발' 사업이 착수되는 등 본격적인 클라우드 컴퓨팅 관련 표준개발 작업에 들어갈 예정이다.

또한, 최근 행안부, 지경부, 방통위 3개 부처가 공동으로 범정부 차원의 '클라우드 컴퓨팅 활성화 종합계획'을 마련하여 국내 클라우드 컴퓨팅 서비스의 조기 활성화 및 상용화 촉진을 위한 정책을 수립하고 추진을 시작하였다.

4. 클라우드 컴퓨팅 상호운용성 확보를 위한 기술적, 제도적 대안

가. 클라우드 컴퓨팅 상호운용성 확보를 위한 기술적 대안

1) 클라우드 컴퓨팅과 관련된 개념 및 용어에 관한 표준 정의

클라우드 컴퓨팅 개념이 학계와 산업계의 관심을 받아오고 있지만. 클라우드 컴퓨팅에 대한 정확한 정의 및 관련 개념 및 용어에 대한 표준화는 이루어지고 있지 않다. 서로 다른 이해도와 용어 및 개념을 가지고 클라우드 컴퓨팅 서비스를 개발하게 되면, 클라우드 컴퓨팅의 장점을 극대화하여 사용하기 어렵다. 그러므로 클라우드 컴퓨팅 정의와 관련 개념 및 용어에 대한 표준화 작업이 필요하게 된다. 이러한 표준화 작업을 통하여 국내의 클라우드 컴퓨팅 서비스들 개발자와 사용자들 간의 불일치한 이해를 해소하고, 나아가 상호운용성이 높은 클라우드 컴퓨팅 서비스 개발을 유도하여 클라우드 컴퓨팅 서비스의 주요 장점 중 하나인 재사용성을 극대화할 수 있도록 한다.

2) 도메인별 클라우드 컴퓨팅 서비스의 인터페이스 표준화

기술적 측면에서 클라우드 컴퓨팅 서비스의 상호운용성 확보를 위해서는 전술한 바와 같이 표준화된 플랫폼과 인터페이스 정의를 포함한 다양한 표준 규격의 개발이 필요로 된다.

기본적으로는 동일한 방식으로 클라우드 컴퓨팅 서비스를 이용하기 위한 공통 프레임워크가 필요로 되며, 이를 기반으로 클라우드 데이터와 서비스를 접근할 수 있도록 하는 인터페이스(API) 및 데이터 규격 표준 개발이 필요로 된다. 또한, 현재 클라우드 컴퓨팅 서비스의 중요한 이슈 중 하나인 안전하고 신뢰성 있는 서비스 제공을 위한 관련 규격 개발은 필수적이라고 할 수 있다. 이러한 문제가 해결될 때, 비로소 클라우드 컴퓨팅 이용 환경은 데이터 및 서비스의 고착성 문제를 해결하고, 서비스의 가용성을 극대화시킬 수 있게 된다.

〈표 4-24〉 클라우드 컴퓨팅 상호운용성 확보를 위한 표준화 대상 기술

표준화 이슈		대상 표준화 항목(안)
1	일반 공통	요구사항, 공통 프레임워크, 보급 시나리오
2	데이터/서비스 고착화 (Lock-in)	공통 인터페이스(API), 데이터 교환 규격, 자원 표현 방식 및 규격
3	서비스 품질 (QoS)	SLA (Service Level Agreement), QoS 파라미터
4	보안	보안 프레임워크 및 메커니즘
5	데이터 기밀성 및 감사성 (Auditability)	안전한 데이터 포맷 및 이용 방식
6	데이터 소유권	사용자 데이터 인증 방식 및 규격
7	데이터 프라이버시	사용자 데이터 보호 방식 및 정책
8	소프트웨어 라이센스	서비스 이용료 산정 방식
9	인터 클라우드 상호운영성	클라우드 간 프로토콜 및 데이터 규격
10	장치 독립성	다중 디바이스 지원 방식

클라우드 컴퓨팅 서비스의 상호운용성 확보를 위한 표준화 대상기술의 상세 내용은 다음과 같다.

① 공통표준

기본적으로 클라우드 컴퓨팅 서비스 제공을 위한 제반 요구사항에 대한 정의가 필요하며, 이를 기반으로 클라우드 컴퓨팅 서비스에 대한 최소한의 공통 프레임워크 등에 대한 규격 정의가 필요하다. 또한 실질적인 보급 확산을 위한 다양한 시나리오(Public Cloud, Private Cloud, Hybrid Cloud, Business Specific Cloud 등)에 대한 상세 정의도 요구된다.

② 데이터 고착화(Lock-in) 방지 표준

클라우드 컴퓨팅 서비스에서 보안과 함께 가장 우려하는 이슈가 특정 클라우드 컴퓨팅 서비스 제공자에게 데이터와 서비스가 종속되어 향후 타 클라우드 컴퓨팅 서비스로의 전환(migration) 또는 연동 등이 힘들어질 수 있다는 것이다. 이는 클라우드 컴퓨팅 서비스 이용 고객에게 서비스 이용의 자율성과 유연성을 침해하는 사항으로서, 서비스 제공자가 다르더라도 이용자는 동일한 서비스를 자유롭게 제공받을 수 있어야 한다. 따라서 이는 플랫폼과 서비스 환경에 독립적인 공통의 서비스 인터페이스(API), 데이터 교환 규격 그리고 자원 표현 방식 등을 표준화함으로써 해결이 가능하다. 이는 현재 전 세계적으로 클라우드 컴퓨팅 관련 사실 표준화 기구에서 가장 활발하게 진행되고 사안이기도 하며, 다만 서로 다른 사실표준화 기구에서 서로 다른 자신들 만의 표준 인터페이스들이 난무할 수도 있다는 것이 경계해야 할 사항이기도 하다.

③ 서비스 품질(QoS) 표준

클라우드 컴퓨팅 서비스가 본격적으로 상용화 될 경우, 가장 중요한 것이 제공되는 클라우드 컴퓨팅 서비스의 품질(Quality of Service)을 어떻게 규정하고 해당 규정에 따라 제공자와 사용자 간의 계약(SLA)을 맺을 것인가이다. SLA란, 서비스 제공자 측과 서비스 이용자 측에서 사전에 합의한 서비스 수준의 제공을 보증시키는 것으로, 법적으로 구속력이 있는 계약이 된다. 따라서 이러한 표준화 관점에서는 합리적인 SLA를 맺도록 하기 위한 기술적 측면의 품질 규격 (서비스 가동률, 성능 파라미터 등)을 개발할 수 있도록 해야 한다.

④ 보안 표준 (공통 프레임워크 표준)

클라우드 컴퓨팅 서비스의 가장 단점으로 지적되는 사항이 바로 클라우드 컴퓨팅 특성상 서비스의 불확실성으로부터 오는 안전성 보장 문제이다. 이는 자신의 데이터가 내 로컬 스토리지가 아닌 외부에 존재한다는 것, 네트워크 기반 온라인 서비스의 영속성에 대한 불안감으로부터 기인한다. 따라서 기술적 측면에서 클라우드 컴퓨팅 서비스의 보안성 유지를 위한 체계화된 프레임워크 구조가 필요로 되며 이를 기반으로 안전한 서비스 제공을 위한 다양한 보안 메커니즘 등이 표준 규격의 형태로 제공되어야 한다.

⑤ 데이터 기밀성 및 감사성(Auditability) 표준

데이터 기밀성이란 정보를 인가된 사람들에게만 정보를 공개하는 것 즉, 전송되는 데이

터의 내용을 완벽하게 보호하여 해킹 등의 부적절한 데이터 침해 행위가 발생하더라도 허가되지 않은 사용자가 임의의 정보 접근을 방지하는 보안 서비스를 말한다. 감사성(Auditability)은 모든 이벤트 및 액션의 내용을 로깅하며, 해당 로그(Log)의 내용은 감사의 목적을 갖고 있으므로 절대 변경 불가해야하며, 권한이 부여된 관리자의 경우에만 볼 수 있어야 한다. 따라서 엔터프라이즈 클라우드와 같이 기업용 등으로 이용되기 위해서는 이러한 기밀성과 감사성 지원을 표준화된 방법으로 로깅하고, 메시지를 교환할 수 있도록 해야 한다.

⑥ 데이터 소유권 표준

데이터 소유권(ownership)이란 데이터를 분류하고, 완전하고 정확하게 데이터를 유지하는 것을 보장할 수 있도록 하는 책임을 부여하는 것을 의미한다. 데이터 소유권의 핵심은 특정 직원에게 컴퓨터 데이터를 보호하는 책임을 부여함으로써 책임 소재를 명확히 하는 것이다. 클라우드 컴퓨팅 서비스에서 이를 위한 데이터 소유자, 데이터 관리자, 데이터 사용자 등의 데이터 소유권에 대한 구분 권한 설정 방법에 대한 표준화된 규격 개발이 필요로 되며, 이러한 기술적 방법과 함께 법제도 측면에서도 소유권에 대한 지원 규정 등도 요구된다.

⑦ 데이터 프라이버시 표준

스마트폰 등 고성능 모바일 디바이스의 보급으로 인해 데이터의 이동성이 증가하고, 클라우드 컴퓨팅의 도입에 따라 데이터가 클라우드로 이전됨으로써 개인의 주요 정보 보호와 조직의 업무 연속성을 보장하기 위한 데이터의 관리, 보존·복구·소유·접근관리의 중요성이 증가할 것으로 예측된다. 따라서 클라우드 컴퓨팅 서비스 환경에서는 개인과 기업의 정보를 보호하고 기업 서비스의 연속성을 보장하기 위한 데이터 관리·보존·복구·소유 전반에 대한 표준화가 요구된다.

⑧ 인터 클라우드 상호운용성 표준

인터 클라우드(inter-cloud)란 클라우드들이 서로 연결된 “클라우드의 클라우드”라고 할 수 있으며, 서로 다른 클라우드들 간의 상호운용성을 보장은 클라우드 컴퓨팅 서비스의 확산을 위해 반드시 해결되어야 하는 사항이다. 따라서 인터 클라우드 컴퓨팅 서비스를 위한 새로운 표준화된 프로토콜과 데이터 포맷 규격은 반드시 고려되어야 한다.

⑨ 장치 독립성 표준

현재의 클라우드 컴퓨팅은 기본적인 단말을 노트북 및 데스크톱PC 등을 대상으로 서비스가 이루어지고 있다. 그러나 유비쿼터스 단말 형태의 다양한 단말을 고려할 경우 클라우드 컴퓨팅 서비스는 단말에 독립적인 형태로 제공되어야 한다. 이를 위하여, 클라우드 컴퓨팅 및 관련 서비스를 고려한 다양한 단말의 특성을 기술하고 단말의 특성 정보를 제공하며, 이러한 단말 정보를 기반으로 클라우드 컴퓨팅 단말에 서비스가 최적화되어 제공될 수 있도록 하는 표준화가 요구된다.

아울러, 이와 같은 클라우드 컴퓨팅 서비스 상호운용성 표준은 다양한 형태의 테스트베드 구축을 통해 상용화를 위한 실효성 및 가용성 등에 대한 검증 작업이 병행되어야 할 것이다. 현재, 정부에서는 클라우드 컴퓨팅 서비스 표준의 검증 작업과 함께 중소기업 등에게 다양한 클라우드 컴퓨팅 서비스 개발 환경을 제공하기 위한 테스트베드를 지원할 예정이다.

나. 상호운용성 확보를 위한 제도적 대안

1) 공공부문 클라우드 상호운용성 확보를 위한 표준 프레임워크 제정

국내 공공부문의 정보화를 담당하고 있는 한국정보화진흥원 (NIA)은 과거 전자정부 상호운용성 확보를 위해 공공 시스템과 서비스의 상호운용에 관한 연구를 수행한 바 있다. 그러나 이는 SOA기반 공공 서비스 상호운용에 관한 것으로, SOA 기반의 서비스와 클라우드 컴퓨팅 서비스의 공통된 부분을 제외하면, 클라우드 컴퓨팅 서비스와 직접 관련된 방향, 표준, 제도는 다루지 않고 있으며, 그 기술적 수준도 클라우드 컴퓨팅 환경을 지원하기에는 매우 미흡한 수준이다.

현재 정부는 클라우드 컴퓨팅 시장 활성화를 위해 정부통합전산세터 내 범정부 클라우드 인프라를 구축함으로써 개별 부처별로 분산되어 있는 서버 풀을 전 부처 '통합 풀'로 재정비할 계획이다. 이에 공공 클라우드 간, 공공과 민간 클라우드 간 상호운용성과 호환성 확보를 위한 표준 프레임워크를 제정하여 확산 시킬 필요가 있다.

2) 민간부문 클라우드 컴퓨팅 상호운용성 확보를 위한 표준화 활동 지원

클라우드 간 상호운용성 확보는 정부의 역할만으로는 한계가 있으며, 민간의 적극적인 역할이 필요하다. 이를 위해 민간부문에서 추진되고 있는 표준화 작업을 적극 지원하고, 공공부문의 표준화와 연계하여 추진함으로써, 표준의 확산을 지원할 필요가 있다. 또한 국내를 넘어서 글로벌 차원에서 진행 중인 다양한 표준화 활동들을 지원하여야 할 것이다.

제5장 결론 및 시사점

본 고에서는 클라우드 컴퓨팅 시장 활성화를 위한 법·제도 개선방안을 살펴보았으며, 그 주요 내용을 요약하면 〈표 5-1〉와 같다.

〈표 5-1〉 클라우드컴퓨팅 활성화를 위한 법·제도 개선방안 요약

연구 분야	주요결과
사업자 파산 등 서비스 중단에 따른 사용자 보호방안	o 클라우드 컴퓨팅 임치제도 도입 및 클라우드 컴퓨팅 서비스 센터를 통한 임치제도 활성화 지원 o 표준 SLA제정 및 이용자 보호지침 제정 - 임치제도 도입 반영 - SLA 및 이용자 보호지침에 서비스 중단에 대한 사전 통지 의무화 - SLA 및 이용자 보호지침에 사용자 데이터에 대한 소유권한 명시 - SLA 및 이용자 보호지침에 중단된 서비스 유지방안 마련 - 보험활용 활성화
일시적 서비스 중단에 따른 사용자 보호방안	o 전기통신기본법 및 전기통신사업법에 클라우드 컴퓨팅 정의, 유형, 사업자 분류 반영 o 정통망법에서 언급된 서비스 중단 및 제한 범위 개선, 이용(서비스)약관 관련사항 개선 및 구체화, 분쟁발생에 따른 우선 법령 범위 명문화 - 손해배상 범위 및 규모 구체화 . 가용률 기반의 손해배상 범위 규정 및 표준 SLA반영 . 손해배상 규모의 현실화 및 분쟁조정체계 마련 . 사용자 자율주도의 실시간 서비스 모니터링 시스템 구비 - 사업자의 면책범위를 공급자 중심에서 수요자 중심으로 재검토
클라우드 컴퓨팅 보안 및 정보보호방안	o 클라우드 컴퓨팅 보안/데이터보호 신뢰성 제고를 위한 신규법규 제정 혹은 '정통망'법 개정 및 세부지침 마련 - 데이터의 물리적 위치변동에 따른 관리, 해킹대응방안, 접근권한, 프라이버시 침해방지, 데이터 유출방지, 수사/소송 협조 등 항목 반영 - 보안점검 대상자에 클라우드 컴퓨팅 서비스 제공자 그룹 추가 - 공공/금융기관 클라우드 컴퓨팅 서비스 사용 정책에 대한 법규 보완 o 보안인증제도 도입 - KISA정보보호관리체계(ISMS) 인증제도를 보완₩활용 (기존체계수정시) - 서비스 품질 인증체계에 포함하여 추진 (신규 인증체계 도입 시)

〈표 5-1〉 클라우드컴퓨팅 활성화를 위한 법·제도 개선방안 요약(계속)

연구 분야	주요결과
클라우드 컴퓨팅 서비스 품질 확보방안	o 표준 SLA가이드라인을 제정. 보급 및 가용성에 따른 대가 차등화 - 품질속성을 반영하는 측정지표를 개발하여 SLA가이드라인에 반영 . Mean Time Between Failure, Mean Time To Repair, Mean Time To Fail, Maximum Tolerable Downtime, Abandonment Rate, Average Speed to Answer 등의 서비스 가용성 지표 설정 - SLA 모니터링을 위한 동적 모니터링 기법, 서비스 오류에 대한 자동 교정기법 등 주요한 기술지침 마련 및 적용 o 클라우드 컴퓨팅 서비스 품질(QoS) 인증제도를 마련 - SLA가이드라인 준수여부와 정보보안 관리수준, 임치제 및 Mirroring지원 여부 등을 포괄적으로 점검하여 인증 부여 - 인증체계, 시험기법 및 기준, 인증심사기관 및 자격 등 제정
클라우드 간 상호운용성 확보방안	o 표준화된 클라우드 플랫폼과 인터페이스 정의를 포함한 다양한 표준 규격의 개발 o 공공부문 클라우드 상호운용성 확보를 위한 표준 프레임워크 제정 o 민간부문 클라우드 컴퓨팅 상호운용성 확보를 위한 표준화 활동 지원

연구결과를 종합하면 다음과 같은 시사점을 얻을 수 있다.

현재 클라우드 컴퓨팅 관련 사업자의 책임과 의무를 부과할 수 있는 법체계는 전기통신기본법, 전기통신사업법, 정통망법 등이 있다. 그러나 이상은 통신서비스와 인터넷 서비스를 고려하여 제정된 법체계로 네트워크, 하드웨어, 소프트웨어, 인터넷 사업자가 함께 생태계를 이루고 있는 클라우드 컴퓨팅 산업의 특성과 시장변화를 충분히 고려하고 있지 못하다. 이에 클라우드 컴퓨팅의 정의 및 서비스, 사업자 유형 등을 반영하여 규제의 수준과 범위를 설정하고, 제도 적용을 위한 대상을 구체화할 수 있도록 현행 법체계의 개선을 추진할 필요가 있다.

또한 클라우드 컴퓨팅의 활성화를 위한 가장 큰 고객은 기업들이다. 이들은 서비스 이용 중에 사업자가 갑작스레 파산을 하거나 서비스를 중단할 경우 그 피해가 심각할 수 있다. 이에 사업자 부도 및 서비스 중단에 대비하여 지속적 서비스 제공을 위한 법제도적 안전장치 마련하여야 하며, 이를 위해 부도 등 사업자가 서비스를 제공하기 어려운 경우, 제3의 사업자가 서비스를 재개할 수 있도록 클라우드 컴퓨팅 서비스 에스크로우(Escrow) 제도를 조속히 활성화시킬 필요가 있다. 특히 클라우드 컴퓨팅의 특성을 반영하여 기존의 기술임

치제도의 범위를 데이터 관리 및 보호로까지 확대 적용할 필요가 있다. 또한 사용기업의 지속적인 사업수행을 위해 사고발생시 제3의 클라우드 컴퓨팅 사업자로의 전환이 용이하도록 서비스 간 상호운용성 표준제정 및 적용의 의무화도 고려할 필요가 있을 것이다.

한편 사용자가 자신의 데이터가 어디에 보관되고, 어떻게 관리되고 있는지 알기 어려운 클라우드 컴퓨팅의 특성 상 사용자 기업의 기업 정보보호 및 개인 사생활 보호를 위한 제도 보완도 시급하다. 이를 위해 클라우드 컴퓨팅 사업자의 데이터 보안 및 영업비밀 유출 방지를 위한 의무조항을 설정하고, 이에 대한 법적 책임기준을 마련할 필요가 있다.

또한 클라우드 컴퓨팅의 서비스 품질에 대한 사용자들의 우려를 해소하고, 사업자들의 서비스 품질 개선 노력을 제고하기 위해 서비스 수준, 데이터 보호, 백업, 장애 지원을 포함하는 SLA 가이드라인 제정하고, 공적인 신뢰공여를 위한 인증체계를 도입할 필요가 있다.

특히 본 연구에서는 포함되지 않지만, 해외 서비스사업자의 국내 진출이 이어지고, 해외 서버를 통한 직접적인 서비스 제공이 일반화되고 있는 상황에서 국경 간(cross-border) 클라우드 컴퓨팅 서비스 제공 시, 데이터의 소재 및 관련 법 적용대상 국가 제도에 대한 명확한 기준 마련될 필요가 있다.

본 고에서는 사업자 파산에 따른 서비스 중단, 갑작스런 서비스 장애, 보안에 대한 우려, 서비스 품질 확보, 클라우드 간 상호운용성 부족으로 인한 소비자 선택권 제한 등 주로 수요자 관점에서 발생할 수 있는 우려를 해소하기 위한 기술적, 제도적 보호방안들을 살펴보았다. 그러나 제도적인 보호만으로는 시장 활성화는 요원하며, 자칫 수요자 보호를 위해 초기부터 공급자에게 과도한 법·제도적인 의무를 부과할 경우 오히려 시장 활성화에 저해가 될 수 있다. 이에 클라우드 컴퓨팅 시장 활성화를 위한 법·제도개선은 시장의 발전과 성숙도 등을 고려하여 수행하되, 지속적인 연구를 통해 사전적인 검토와 준비가 이루어져야 할 것이다.

클라우드 컴퓨팅 시장의 활성화를 위해서는 법·제도의 개선과 함께 기술개발 및 수요시장 활성화 등 보다 다양한 정책적 지원책이 필요하다. 이에 조세특례법을 활용한 중소기업의 클라우드 컴퓨팅 이용활성화를 지원[59]하고, 공공부문 클라우드 컴퓨팅 선제도입을 통한 초기 시장 활성화를 추진할 필요가 있다. 이와 함께, 핵심기술 개발 및 웹 기반 솔루션으로의 전환 지원 등 공급자 역량 강화 등 다양한 수요·공급차원의 지원책들이 병행될 필요

59) 현행 조세특례법은 CRM 등을 SaaS 방식으로 이용하는 기업에 대해 연간 이용료의 3%(중소기업은 7%)를 세액 공제 중

가 있다.

지금까지 자신의 개인용 컴퓨터에 소프트웨어를 설치하여 사용하는 방식의 컴퓨팅환경은 점차 클라우드를 활용하는 방식으로 진화해 갈 것이며, 그 도구도 현재의 PC를 넘어 넷북, 스마트폰 등으로 광범위하게 확산될 것이다. 이제 그 무한한 기회를 위한 도전과 기회는 막 시작되고 있다. 글로벌 기업들이 선도하고 있는 새로운 시장에서 우리나라의 IT기업과 SW기업들의 새로운 도약을 위한 전략설정과 정부의 현명한 대응이 요구되는 시점이다.

〈참고문헌〉

[1] 구본재 외,『경영혁신을 위한 IT거버넌스』,네모북스, 2006
[2] 기술경제연구부, “네트워크 경제연구팀, 99-03 ”,한국전자통신연구원, p.45-48
[3] 남효순 · 정상조, 인터넷과 법률, 법문사, 2002
[4] 대중소기업협력재단, “알기쉽고 편리한 기술자료 임치제도”, 2008
[5] 민영기, “클라우드 컴퓨팅 서비스 활성화를 위한 장애요소 및 대응방안”, TTA Journal No.125, 2009
[6] 방송통신위원회 보도자료, 2009.7.8
[7] 성병용, “국내기업의 클라우드 컴퓨팅 동향 및 전략”, “SW인사이트 정책리포트”, 2009.07
[8] 손승우 외, “SaaS(Software as a Service) Escrow 제도 도입방안 연구”, 한국SW진흥원, 2008.12
[9] 시로타 마코토, “클라우드의 충격”, 제이펍
[10] 유은재 · 윤미영, “주요국의 사이버 보안 추진전략과 시사점”, NIA CIO Report vol.15, 2009.8
[11] 임종인, “사이버 보안 정책 및 법제도 현황”, TTA Journal No.118, 2008.7/8
[12] 정제호, 클라우드 컴퓨팅의 현재와 미래, 그리고 시장전략, SW인사이트 정책리포트, 2008.10
[13] 정보통신부 · 한국정보보호진흥원, 민간사이버안전매뉴얼, 2004
[14] 전자통신동향분석, 제19권 6호, 2004.12
[15] 조희준, “ITIL:IT 경력개발과 IT서비스관리의 사실상의 표준",마이크로소프트웨어, 2009
[16] 차건상, “최근의 보안사고 동향분석에 따른 전자정부 보안대책”, 전자정부포커스, No.06, 2008
[17] 한국경제, “MS 망신살… 사이드킥 고객 데이터 몽땅 날아가”, 2009.10.13
[18] 황경태,『COBIT 4.0 한글판』,한국정보시스템감사통제협회, 2006
[19] Buyya, R., C.S. Y대, S. Venugopal, J. Broberg & I. Brandic. . Cloud

Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. Future Generation Computer Systems, 25, 599-616, 2009

[20] Chris Davis,『IT Auditing:Using Controls to Protect Information Assets』, Mcgraw hill, 2006

[21] eGIF6.1, Cabinet Office, e-Government Interoperability Framework Version 6.1, Cabinet Office, Mar.18, 2005.

[22] EIF2.0, Preparation for Update European Interoperability Framework 2.0 - FINAL REPORT, Gartner, 2007.4.6

[23] ISACA,『COBIT 4.1』, 2007

[24] itSMF NL,『ITIL 기반의 IT 서비스 관리』,네모북스, 2006

[25] Motahari-Nezhad, H.R., B. Stephenson and S. Singhal. Outsourcing Business to Cloud Computing Services: Opportunities and Challenges. HP Laboratories, 2009

[26] NIKKEI COMMUNICATIONS, p.68-69, 1999.06.07

[27] NIKKEI COMMUNICATIONS, p.112-119, 1999.06.21

[28] OGC,『Information Technology Infrastructure Library V3』, 2007

[29] SAGA3.0, KBSt unit, Standards and Architectures for eGovernment Applications, Bundersministerium des Innern, 2006.10

[30] Ricahard Kane, "Software Escrow For Dummies", Wiley Publishing.INC

관련법령 및 약관

[1] 독일, 정보통신법(Telecommunications Act/ Telekommunikationsgesetz-TKG)

[2] 독일, 연방데이터보호법(Federal Data Protection Act(BDSG)

[3] 독일, 정보통신서비스 정보보호법(TDDSG : Gesetz uber den Datenschutz bei Telediensten)

[4] 미국, 전기통신 프라이버시법(ECPA : Electronic Communications Privacy Act of 1986)
[5] 미국, Gramm-Leach Bliley Act(GLBA)
[6] 미국, SOX법(Sarbanes-Oxley Act of 2002)
[7] 법제처, 공공기관의 개인정보보호에 관한 법률
[8] 법제처, 신용정보의 이용 및 보호에 관한 법률
[9] 법제처, 전기통신사업법
[10] 법제처, 정보통신망 이용촉진 및 정보보호 등에 관한 법률
[11] 법제처, 통신비밀보호법
[12] 약관의 규제에 관한 법률
[13] 영국, 데이터보호법(Data Protection Law)
[14] 영국, 프라이버시 및 전자통신규칙(Privacy and Electronic Communications (EC Directive) Regulations 2003
[15] 영국, 조사권한규제법(RIPA: Regulation of Investigatory Powers Act 2000)
[16] 일본, 고도 정보통신 네트워크 사회 형성 기본법(IT기본법)(2000년 법률 제144호)
[17] 일본, 특정 전기 통신 서비스 제공자의 손해배상 책임의 제한 및 발신자 정보의 개시에 관한 법률
[18] 일본, 개인정보보호 관련 법률
[19] 일본, 사이버범죄 관련 법률
[20] 일본, 범죄의 국제화 및 조직화 그리고 정보처리의 고도화에 대처하기 위한 형법 등의 일부를 개정하는 법률안
[21] 일본, 부정액세스행위 금지 등에 관한 법률
[22] 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령
[23] CSA(Cloud Security Alliance), Security Guidance for Critical Areas of Focus Cloud Computing V2.1 EU, 사이버범죄조약
[24] Gartner, What You Need to Know About Cloud Computing Security & Compliance, 2009.7.13

[25] IDC Enterprise Panel 2008.8, 클라우드 컴퓨팅 활성화에 따른 이슈
[26] ISO, ISO9001(품질경영시스템)
[27] ISO, ISO14001(환경경영시스템)
[28] ISO, ISO27001(정보보안경영시스템 인증)
[29] KISA, 정보보호관리체계인증
[30] KISA, 정보보호 안전진단
[31] KT QooK 인터넷 이용약관
[32] LG 데이콤 웹하드 서비스 이용약관
[33] LG XPEED 인터넷 서비스 이용약관
[34] NIST(National Institute of Standards and Technology), 클라우드 컴퓨팅 서비스 보안 표준
[35] PCI 보안표준위원회, LLC(2008.10), PCI DSS Requirements and Security Assessment
[36] PCI 보안표준위원회, (Payment Card Industry Data Security Standard) Procedures, v1.2
[37] RSA(2009. 11), Identity & Data Protection in the Cloud
[38] SKT브로드밴드 초고속 인터넷 서비스 이용약관
[39] SKT브로드밴드 IDC 서비스 이용약관

웹사이트 (Website)

[1] 한국클라우드 컴퓨팅연구조합 http://www.cccr.or.kr (2009.12.2. 방문)
[2] 위키피디아 백과사전, http://en.wikipedia.org/wiki/The_Linkup (2009.12.5. 방문)
[3] Iron Mountain, http://www.ironmountain.com (2009.11.20. 방문)
[4] 세일즈포스닷컴 http://blogs.salesforce.com/features/2006/03/mirrorforce.html (2009.11.20. 방문)

[5] SAS70, http://www.sas70.com
[6] www.itsmfi.org
[7] www.isaca.com
[8] www.kolonbenit.com
[9] blog.naver.com/nd1426
[10] www.lyzeum.com
[11] www.imaso.co.kr
[12] www.wikipedia.org
[13] www.itfind.or.kr
[14] www.moleg.go.kr
[15] www.kolonbenit.com
[16] ETNEWS, http://www.etnews.co.kr, 2006.02
[17] BPEL07 WebServicesBusinessProcessExecutionLanguageVersion2.0, OASIS-Standard, OASIS, http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html, 2007.4.11
[18] Kob06, "SOA governance: Preveniting rogue services", NetworkWorld, http://www.networkworld.com/supp/2006/ndc3/062606-ndc-soa-governance.html, 2006.6
[19] http://www.cooolguy.net/184
[20] http://kingcrap.com/110
[21] http://charlz.wordpress.com/2007/02/23/googleappssla99point9/
[22] http://blog.paran.com/paraner/4741365
[23] http://www.transparentuptime.com/2008/12/saas-slas-state-of-union.html
[24] http://www.tta.or.kr/data/weekly_view.jsp?news_id=609
[25] http://www.nextsourcing.org

정책연구센터 09-03

클라우드 컴퓨팅 활성화를 위한 법제도 개선방안

2009년 12월 18일 인쇄
2009년 12월 21일 발행

발행인 정 경 원
발행처 정보통신산업진흥원
138-711 서울특별시 송파구 가락본동 79-2 NIPA빌딩
TEL. 02-2141-5000 FAX. 02-2141-5199
인쇄처 신생용사촌 (TEL. 02-426-4415)