情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

클라우드 컴퓨팅 서비스 제공자의 개인정보보호 조치 방안에 대한 연구*

유 우 영,† 임 종 인‡
고려대학교 정보보호대학원

A Study on the Privacy Security Management under the Cloud Computing Service Provider*

Woo-Young Yu,† Jong-in Lim‡
Graduate School of Information Security, Korea University

요 약

인터넷 기술을 활용한 클라우드 컴퓨팅 서비스의 확산에 따라 개인정보 유출 위험과 정보에 대한 통제가 불가능해질 수 있는 보안 위협이 증가되고 있으나, 현재 클라우드 컴퓨팅 서비스 제공자는 개인정보보호에 대한 충분한 보호조치를 서비스 이용자에게 제공하지 못하고 있는 상황이다. 본 논문에서는 클라우드 컴퓨팅 서비스에 대한 개인정보보호 고려 사항을 살펴보고, 클라우드 컴퓨팅 서비스 환경에서의 개인정보보호 위협에 대응하는 방안을 제안한다.

ABSTRACT

According to cloud computing service is increasing of using the Internet technology, it's increasing privacy security risks and out of control of security threats. However, the current cloud computing service providers does not provide to solutions of the privacy security management. This paper discusses the privacy security management issue of cloud computing service, and propose solutions to privacy information threats in cloud computing environment.

Keywords: Cloud Computing, Privacy Information Security

I. 서 론

클라우드 컴퓨팅이란 인터넷 기술을 활용하여 IT자원을 가상화하여 서비스를 제공하는 형태로 소프트웨어, 스토리지, 서버, 네트워크 등의 자원을 필요할 경우 필요한 만큼 사용하고 비용을 지불하는 컴퓨팅을 의미하며, 개방, 공유를 상징하는 웹 2.0에 자유로움을 추가한 웹 3.0이라고 불리기도 한다. 클라우드 컴퓨팅이란 새로운 기술이라기보다는 기존의 그리드 컴퓨팅, 유틸리티 컴퓨팅, 웹 서비스, 가상화 기술, 공개 소프트웨어 등의 기존 기술이 하나의 커다란 서비스로 융합된 기술이다. 클라우드 컴퓨팅의 활성화와 함께 기술 및 서비스의 종속성에 대한 이슈와, 클라우드 컴퓨팅의 보안 문제가 대두되고 있는데, 이러한 문제점을 해결하기 위한 기술 및 표준을 마련하기 위하여 여러 표준화 가구에서 표준화 작업 또한 진행 중에 있다.

클라우드 컴퓨팅 서비스는 IT 관련 사업뿐 아니라 국가경쟁력을 크게 좌우하는 산업으로 인식하여, 우리나라는 정부 차원에서 지식경제부, 방송통신위원회, 행정안전부 3개 부처가 공동으로 2014년 클라우드 선

접수일(2012년 2월 21일), 수정일(2012년 4월 10일), 게재확정일(2012년 4월 12일)
* 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21사업'의 지원비를 받았음.
† 주저자, wooyoung.yu@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

진국 도약을 위한 '클라우드 컴퓨팅 활성화 종합계획'을 발표하였다. 정부는 2014년까지 클라우드 컴퓨팅 시장을 6,739억원에서 2조 5천억원 규모로 키우고, 세계시장 점유율을 10%까지 확대하는 등 클라우드 컴퓨팅 강국 도약을 목표로 플랫폼, 응용서비스 분야의 핵심 기술 개발을 본격 추진하고 있다.

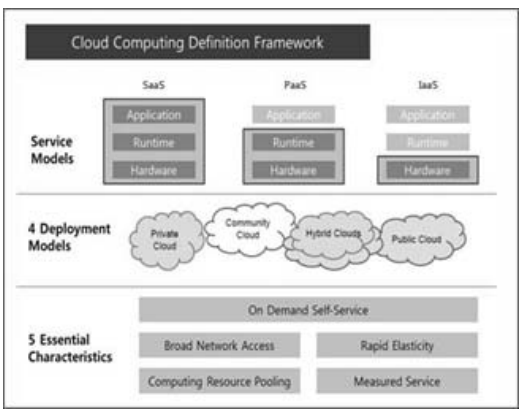
클라우드 컴퓨팅 서비스 활성화에 따라 서비스를 이용하는 개인 및 기업 이용자가 개인정보 침해사고에 대한 피해를 입게 될 수 있기 때문에, 클라우드 컴퓨팅 산업 활성화에 따른 개인정보보호 이슈 사항이 무엇인지 충분한 검토가 이루어져야 한다. 따라서 본 논문에서는 클라우드 컴퓨팅과 관련된 주요 개인정보보호 이슈 사항들에 대하여 살펴보고 클라우드 컴퓨팅 서비스 제공자 개선하여야 하는 개인정보보호에 대한 사항을 논의하고자 한다.

II. 클라우드 컴퓨팅의 특징

2.1 클라우드 컴퓨팅의 특징과 분류

클라우드 컴퓨팅은 사용자가 필요한 컴퓨팅 자원을 원하는 시점에 자유롭게 사용할 수 있다는 장점을 제공하고 있으며, 사용자는 필요한 시점에 시스템 규모와 사용 시간 단위로 자원을 사용하고 비용을 지불하면 된다. 한마디로 클라우드 컴퓨팅은 인터넷을 이용하여 IT 자원을 주문형으로 이용자에게 서비스 제공하는 컴퓨팅 환경을 말한다. 사용자는 클라우드 컴퓨팅 서비스 사업자가 제공하는 서비스를 이용하면 된다 [1].

클라우드 컴퓨팅은 제공되는 서비스의 형태에 따라 SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service)로 분류되고 있다. SaaS는 사용자가 소프트웨어 라이센스를 구매하지 않고 클라우드 서비스를 통하여 빌려 쓰는 것을 의미하며, 구글 오피스가 대표적인 예이다. PaaS는 사용자에게 소프트웨어를 개발할 수 있는 환경을 제공해 주는 서비스이며, 개발자는 클라우드 서비스에서 제공되는 개발 도구를 활용하여 어플리케이션을 만들어 사용할 수 있다. IaaS는 서버, 데스크탑, 스토리지 등 업무 처리를 위하여 필요한 인프라 자원을 빌려 쓰는 형태로 클라우드 서비스의 초기 모델로 IT인프라 비용을 관리하기 위한 형태의 서비스이다[2][3].



[그림 1] 클라우드 컴퓨팅 프레임워크[6]

[표 1] 클라우드 컴퓨팅 관련 기술[4][7]

요소 기술	개념	클라우드 컴퓨팅과의 비교
Grid Computing	많은 IT 자원을 필요로 하는 작업을 위해 인터넷상의 분산된 다양한 자원들을 공유하여 가상의 슈퍼컴퓨터 처럼 활용하는 방식	Grid Computing이 인터넷 상의 모든 컴퓨팅 자원을 통합하여 사용하는데 반해, 클라우드 컴퓨팅은 서비스 제공 사업자의 사유 서버 네트워크를 빌려서 활용
Utility Computing	서버, 스토리지 등 컴퓨팅 자원을 보유하지 않은 채 사 량에 따라 과금 되는 방식	클라우드 컴퓨팅의 과금 방식과 동일
SBC: Server Based Computing	서버에 응용 소프트웨어와 데이터를 저장해 두고 필요할 때마다 접속해서 쓰는 방식으로 모든 작업을 서버가 처리하는 방식	클라우드 컴퓨팅은 서비스 제공자의 가상화된 서버를 이용하고, SBC는 특정 기업 내 서버를 이용한다는 차원에서 구분되나, 서버 기반 컴퓨팅이 발전하면서 그 구분이 모호해짐
Network Computing	서버 기반 컴퓨팅처럼 응용 소프트웨어를 서버에 두지만, 작동은 이용자 컴퓨터의 자원을 이용하여 수행하는 방식	클라우드 컴퓨팅은 이용자 컴퓨터가 아니라 클라우드 상의 IT 자원을 이용하는 방식

2.2 클라우드 컴퓨팅 관련 요소 기술

클라우드 컴퓨팅과 관련된 기술은 크게 인터넷 환경에서 분산된 자원들을 공유하여 가상의 대용량 컴퓨

팅 환경을 구축하는 방식인 그리드 컴퓨팅(Grid Computing), 한 대의 컴퓨터에 여러 개의 운영체계를 사용하는 가상화 기법(Virtualization), 사용한 만큼 비용을 지불하는 유틸리티 컴퓨팅(Utility Computing), 서버에 접속하여 서버의 응용 프로그램을 활용하여 작업을 수행하는 서버 기반 컴퓨팅(Server Based Computing), 네트워크를 통하여 컴퓨팅 자원을 활용하는 네트워크 컴퓨팅(Network Computing) 기술 등이다[4].

2.3 클라우드 컴퓨팅 개인정보의 개념 및 범위

2.3.1 클라우드 컴퓨팅 환경에서의 개인정보의 개념

개인정보는 사회적, 법률적으로 다양하게 정의되고 있으며, 한국인터넷진흥원에서는 "개인의 신체, 재산, 사회적 지위, 신분 등에 관한 사실, 판단, 평가 등을 나타내는 일체의 모든 정보"라고 정의하고 있다. 또한, 단일 정보로 개인을 식별할 수 없더라도 다른 정보와 결합하여 개인을 식별할 수 있는 경우 개인정보에 포함된다. 개인정보의 넓은 의미로 가장 많이 사용되는 Privacy에 대하여 OECD Privacy Guidelines에서는 "사용자의 개인 정보의 사용 및 접근에 대한 이해를 보장하는 것"이라 명시하고 있으며, 본 논문에서는 클라우드 서비스의 개인정보를 클라우드 환경에서 수집, 저장, 처리 및 이용 되는 모든 정보를 의미하며 개인정보 처리과정에서 새롭게 생성되는 모든 정보를 포함한다. 클라우드 컴퓨팅 환경에서는 서비스 제공자와 이용자 간 정보 주체 및 소유에 따라 개인정보보호의 범위를 합리적으로 규정하고 통제 절차를 수립하는 것이 매우 중요하다.

2.3.2 클라우드 컴퓨팅 환경 개인정보보호 이슈

클라우드 컴퓨팅 환경 개인정보보호 이슈는 IT 환경의 일반적인 보안 이슈에 클라우드 환경에 적합한 요구사항이 혼재되어 있어 클라우드 컴퓨팅 환경 개인정보보호 요구사항을 NIST SP 800-144 "Guidelines on Security and Privacy in Public Cloud Computing" 문서를 기준으로, 한국인터넷진흥원 "클라우드 서비스 정보보호 안내서" 내용을 비교분석하여 클라우드 컴퓨팅에 대한 개인정보보호 이슈 항목을 도출하였다.

〔표 2〕 클라우드 컴퓨팅 보안 및 개인정보 이슈

구분	내용
1. Governance	클라우드 환경에서 정책, 절차 및 표준과 관련된 거버넌스 수립 뿐 아니라, 설계, 구현, 테스트, 사용 및 서비스 적용 및 모니터링에 대한 통제 도구 마련
2. Compliance	개인정보보호에 대한 법과 규제 준수 (Law and Regulations, Data Location, Electronic Discovery)
3. Trust	서비스 제공자는 보안과 개인정보보호에 대하여 높은 수준의 통제 및 절차의 투명성을 제공 (Insider Access, Data Ownership, Composite Services, Visibility, Ancillary Data, Risk Management)
4. Architecture	클라우드 서비스에 대한 소프트웨어 및 하드웨어 전체에 대한 구성요소와 관련된 보안 및 개인정보보호 통제 기술 (Attack Surface, Virtual Network Protection, Virtual Machine Images, Client-Side Protection)
5. Identity and Access Management	민감한 정보와 개인정보에 접근에 대한 인증, 접근 통제를 위한 보호조치 (Authentication, Access Control)
6. Software Isolation	클라우드 환경의 가상화 및 소프트웨어 격리 (Hypervisor Complexity, Attack Vectors)
7. Data Protection	클라우드 서비스 제공자의 데이터 관리에 대한 적합성 (Value Concentration, Data Isolation, Data Sanitization)
8. Availability	서비스 거부 공격, 장애, 자연 재해, 취약점 등에 대하여 서비스 가용성 보장을 위한 방안 (Temporary Outages, Prolonged and Permanent Outages, Denial of Service)
9. Incident Response	클라우드 사업자는 침해사고 확인, 분석, 대응, 데이터 수집 및 보존 등에 대한 절차 마련 (Data Availability, Incident Analysis and Resolution)

III. 클라우드 컴퓨팅 서비스

3.1 클라우드 컴퓨팅 서비스 장점

클라우드 컴퓨팅 서비스 이용자는 물리적 IT인프라를 보유하지 않고 서비스 제공자로부터 IT인프라를 임대하여 사용하고, 원격의 서버에 중앙 집중식으로 데이터를 저장하게 되어 분산된 컴퓨터 환경에 비하여 효율적으로 정보 접속에 대한 모니터링을 실시할 수

〔표 3〕 클라우드 컴퓨팅 서비스 장점

	구분	장점
1	IT인프라 초기 투자 비용 최소화	IT인프라 구성을 위하여 하드웨어, 소프트웨어 등에 대한 초기 투자 비용을 줄일 수 있어, 서비스 활성화에 기여한다.
2	IT인프라 운영 비용 절감	물리적 IT인프라를 소유하지 않음으로 IT인프라 운영 관리에 따르는 설비와 운영 인력 비용을 절감할 수 있다.
3	긴급 상황 대응 능력 향상	대용량 IT인프라를 보유한 클라우드 컴퓨팅 서비스 사업자의 IT자원을 활용하여 서비스 이용 급증 또는 DDoS 등의 비정상 트래픽 폭주 등의 비상 상황에 대응할 수 있는 능력이 증대된다.
4	보안 위협 대응 능력 향상	IT인프라의 중앙 집중화로 보안시스템 또는 관리시스템에 대한 투자가 취약한 중소 규모 서비스 이용자에게 클라우드 컴퓨팅 사업자의 전문적인 기술지원이나 보안투자를 통하여 데이터 보호를 위한 안정성을 확보할 수 있다.
5	서비스 이용 효율성 증대	SaaS와 같은 경우 클라우드 컴퓨팅 환경의 어플리케이션을 이용하게 됨으로, 어플리케이션 관리가 편리하고 항상 최신의 어플리케이션을 이용할 수 있으며, 서비스 이용자는 관리에 필요한 복잡한 기술이나 전문 지식을 습득할 필요가 없어진다.
6	모바일 클라우드 컴퓨팅	모바일 클라우드 컴퓨팅으로 특정 운영체제 기반의 어플리케이션 한계를 극복하여, 웹을 통하여 소프트웨어, 플랫폼 등의 IT인프라 서비스를 다양한 모바일 단말에서 이용할 수 있다.

있다. 또한, 가상화 기술을 이용하여 데이터 복구 및 시스템 교체 작업을 쉽고 빠르게 수행할 수 있으며, 새로운 보안 위협에 대하여 대응 방안을 쉽게 적용할 수 있는 등 많은 장점들을 가지고 있다.

3.2 클라우드 컴퓨팅 서비스 적용 사례

2010년 전 세계 클라우드 컴퓨팅 시장규모는 1,095억 달러에서 연평균 34.0%의 높은 성장률을 기록하며 2014년에는 3,434억 달러에 이를 전망이라고 한다. Garter는 클라우드 컴퓨팅이 기업의 IT서비스 기반이 될 것으로 예측하였으며, Merrylinch는 소프트웨어 시장의 연평균 성장률은 6%인데 반해, 클라우드 컴퓨팅 시장의 연평균 성장률은 30%를 기록할 것이라고 전망하였다[8].

〔표 4〕 클라우드 컴퓨팅 서비스 사례

구분	분류	사례
IaaS	서버클라우드 서비스	Amazon EC2(Elastic Compute Cloud), Saw is Cloud Compute
	미들웨어 클라우드 서비스	Amazon SQS(Simple Queue Service)
	스토리지 클라우드 서비스	Amazon S3(Simple Storage Service)
	데이터베이스 클라우드 서비스	Amazon SimpleDB, Google Base, MS SDS
PaaS	엔트프라이즈 플랫폼 서비스	GigaSpaces, Oracle SaaS platform
	호스티드 플랫폼 서비스	Google AppEngine, Salesforce Force.com, MS Azure, Sun Caroline, Cloudera
SaaS	응용 소프트웨어 서비스	GoogleApps, Salesforce.com Apps, Apple MobileMe, Nokia OVI, IBM Bluehouse
	웹 기반 서비스	HP Snapfish, MS Office Live, HP Magcloud
	응용 소프트웨어 컴포넌트 서비스	Amazon FPS(Flexible Payments Service) API, Google MAP API, Google Calender APIs, Yahoo! Maps API

클라우드 서비스는 모바일기기에서의 저장용량 한계를 극복하여 인터넷 환경에서 자유롭게 데이터를 저장하고 활용할 수 있는 기능을 제공하고 있으며, 별도의 응용프로그램 없이 클라우드 컴퓨팅을 이용하여 Word, Excel, PowerPoint 등을 이용할 수 있는 Google Docs, Soonr 등의 서비스는 PC와 모바일 기기에서 웹을 통하여 오피스 문서를 자유롭게 작성, 저장, 활용하는 기능을 제공하고 있다.

3.3 클라우드 서비스 사업자별 서비스 제공 현황

국내외 클라우드 컴퓨팅 서비스는 IaaS (Infrastructure as a Service) 형태의 서비스가 주류를 이루고 있으며, 일부 SaaS (Software as a Service) 형태의 서비스가 제공되고 있다. 현재 급격하게 확산되고 있는 IaaS 서비스에 대하여 서비스 이용 약관 및 서비스레벨협정(SLA) 관점에서 보안 및 개인정보보호 요구사항 만족 여부를 분석하고자 한다. 클라우드 서비스 제공자는 서비스에 대한 책임사항과 가용성 보장에 대한 책임을 제시하고 있으며, Google

〔표 5〕 클라우드 서비스 사업자별 서비스 제공 내용

구분	내용
Google Apps	* Service Level Agreement Google Apps SLA는 Google Apps 서비스의 웹 인터페이스가 올바르게 작동할 경우 고객에게 99.9%의 서비스 이용 가능 시간을 보장하고, Google이 약속한 대로 서비스를 제공하지 못하여 서비스 성능 문제가 발생한 경우 서비스 크래딧을 받을 수 있음. http://www.google.com/apps/intl/ko/terms/sla.html
Amazon EC2	* Service Level Agreement Amazon EC2는 고객에게 99.95%/년의 서비스 이용 가능 시간을 보장하며 이를 달성하지 못한 경우에 고객은 서비스 크래딧을 받을 수 있음. http://aws.amazon.com/ec2-sla/
Amazon S3	* Service Level Agreement Amazon S3는 고객에게 99.9%의 서비스 이용 가능 시간을 보장하며 이를 달성하지 못한 경우에 고객은 서비스 크래딧을 받을 수 있음. http://aws.amazon.com/s3-sla/
SKT Tcloud	* 이용약관 손해배상 관련 내용 회사는 고객에게 책임이 없는 사유로 서비스를 이용하지 못한 사실을 고객이 회사에 통지한 때(고객의 통지 전에 회사가 그러한 사실을 알게 된 경우는 회사가 그러한 사실을 알게된 때)로부터 3시간 이상 계속 서비스를 제공하지 못하거나 월 누적장애시간이 24시간을 초과하여 고객이 손해를 입은 경우 고객의 청구에 의해서 손해를 배상함. http://www.tcloudbiz.com/usr/member/memberMgmt/memberJoinStep2.do
Host-way Flex Cloud	* 이용약관 손해배상 관련 내용 사의 명백한 귀책 사유로 고객이 서비스를 이용하지 못하는 경우에는 회사가 고객에게 손해를 배상함. 회사의 명백한 귀책사유로 이용고객이 서비스를 이용하지 못하는 경우에는 이용고객이 그 사실을 회사에 통보하여 확인한 시점(또는 그 전에 회사가 그 사실을 알았거나 알 수 있게 된 시점)부터 지속적인 4시간 이상의 서비스제공 중지시간에 대하여 협의 후 배상함. http://www.hostway.co.kr/cloud_server.html
LG U+	* 이용약관 손해배상 관련 내용 1시간 이상의 서비스 제공 중지 시간에 대하여 배상함. http://www.cloudn.co.kr/index.cloudn
KT	* 이용약관 손해배상 관련 내용 월 가용성(%)에 따라 손해 배상 함. - 99%~99.9% 미만(7.20 hours~43.2 minutes) : 10% 할인 - 99% 미만(7.20 hours 이상) : 25% 할인 https://office.ucloud.com/svc/regist/index.kt

〔표 6〕 클라우드 서비스 사업자별 서비스 제공 수준

클라우드 컴퓨팅 개인정보보호 이슈	클라우드 서비스 제공 수준
1. Governance	○
2. Compliance	○
3. Trust	○
4. Architecture	◎
5. Identity and Access Management	○
6. Software Isolation	◎
7. Data Protection	○
8. Availability	●
9. Incident Response	◎

및 Amazon의 경우 SLA를 구비하여 제시하고 있고, 국내 서비스 제공자의 경우 유사한 내용을 서비스 이용약관에 포함하고 있다.

클라우드 컴퓨팅 서비스 제공자의 서비스 이용 약관 및 SLA를 살펴보면 서비스 가용성에 대한 최소한의 서비스에 대하여 보증하고는 있으나, 클라우드 컴퓨팅 서비스 이용에 따른 개인정보보호에 대한 내용은 서비스 이용자에게 제공되지 않고 있어 보완이 필요해 보인다.

IV. 클라우드 컴퓨팅 환경에서의 개인정보보호 조치 방안

클라우드 컴퓨팅 서비스를 이용하는 서비스 이용자의 개인정보자기결정권을 보장하고 서비스 제공자의 잠재적 개인정보보호 업무 위험을 줄이기 위한 고려사항을 살펴보고 이에 대한 개선 방향을 제시한다.

4.1 클라우드 컴퓨팅 서비스에 대한 개인정보보호 고려사항

4.1.1 개인정보의 물리적 저장 위치

개인정보를 수집 이용하는 사업자가 클라우드 컴퓨팅 서비스를 이용하여 이용자에게 서비스를 제공할 경우 이용자의 개인정보가 보관되는 데이터 보관의 지리적 위치의 다양성으로 인하여 개인정보보호와 관련된 법률적 이슈가 발생할 경우 서버 위치 중심의 법률적 관할권 결정이 어려울 수 있다. 개인정보 소유 주체인 개인의 개인정보자기결정권을 보호하기 위한 조건을

갖추기 위하여 클라우드 컴퓨팅 서비스를 제공하는 다국적 기업 또는 국가 간에 국제적 협력에 대한 문제가 발생할 가능성이 크다[9][10].

4.1.2 개인정보 보관 위치에 따른 해외 이전 이슈

[정보통신망 이용촉진 및 정보보호 등에 관한 법률] 제63조 (국외 이전 개인정보의 보호)에는 서비스 제공자가 개인정보를 국외로 이전하려면 이용자의 사전 동의를 받도록 규제하고 있다. 클라우드 컴퓨팅 서비스를 통한 기업 활동 영역의 확대로 인하여 개인정보가 국내에 머무르지 않고 해외에 위치한 서버에 저장될 경우 개인정보의 해외 이전과 관련된 이슈사항이 발생할 수 있음으로 개인정보주체의 개인정보자기결정권이 보호될 수 있도록 하여야 한다.

4.1.3 개인정보의 보존 및 파기

개인정보 주체의 개인정보자기결정권 보장 차원에서 개인정보 삭제 요청이 있거나 제공되는 서비스가 종료될 경우 사업자는 정당한 또는 합리적인 사유가 없을 경우 지체 없이 이용 중인 개인정보를 즉시 삭제하여야 하며, 서비스 이용자에게 제공된 개인정보가 완전하게 파기 되었는지, 향후 법률적 분쟁 발생 시 법률적 요구사항을 충족하도록 관리되고 있는지 보증할 수 있어야 한다.

분야별 개별 법률에 의한 개인정보 보존연한이 상이하여 획일적으로 단일화된 보존 정책을 적용하기 어려우며, 클라우드 컴퓨팅 서비스를 이용하는 사업자는 개인정보 제공자의 서비스 탈퇴 또는 이용자에게 제공되는 서비스가 종료된 이후에도 현행 개별 법률에 따라 개인정보를 보존하고 관리하여야 한다[9].

[표 7] 법률에 의한 개인정보 보존 연한

법률	내용	보존 연한
신용정보의 이용 및 보호에 관한 법률	제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존) ② 신용정보회사등은 다음 각 호의 사항에 대한 기록을 3년간 보존하여야 한다. 1. 의뢰인의 주소와 성명 또는 정보제공·교환기관의 주소와 이름 2. 의뢰받은 업무 내용 및 의뢰받은 날짜 등	3년
국세기본법	제85조의3(장부 등의 비치와 보존) ② 제1항에 따른 장부 및 증거서류는 그 거래사실이 속하는 과세기간에 대한 해당 국세의 법정신고기한이 지난 날부터 5년간 보존하여야 한다. 다만, 제26조의2제1항제5호에 해당하는 경우에는 같은 호에 규정한 날까지 보존하여야 한다.	5년
특정 금융거래 정보의 보고 및 이용 등에 관한 법률	제4조(불법재산 등으로 의심되는 거래의 보고 등) ④ 금융회사등은 제1항 또는 제2항에 따라 보고를 하였을 때에는 대통령령으로 정하는 바에 따라 그 보고와 관련된 다음 각 호의 자료를 보고한 날부터 5년간 보존하여야 한다.	5년
통신비밀보호법	제13조 (범죄수사를 위한 통신사실 확인자료제공의 절차 ⑦전기통신사업자는 검사, 사법경찰관 또는 정보수사기관의 장에게 통신사실 확인자료를 제공한 때에는 자료제공현황 등을 연 2회 방송통신위원회에 보고하고, 당해 통신사실 확인자료 제공사실등 필요한 사항을 기재한 대장과 통신사실 확인자료제공요청서등 관련자료를 통신사실확인자료를 제공한 날부터 7년간 비치하여야 한다.	7년
상법	제33조 (상업장부등의 보존) ① 상인은 10년간 상업장부와 영업에 관한 중요서류를 보존하여야 한다. 다만, 전표 또는 이와 유사한 서류는 5년간 이를 보존하여야 한다.	5년
전자상거래 등에서의 소비자 보호에 관한 법률 시행령	제6조(사업자가 보존하는 거래기록의 대상등) ① 법 제6조제3항의 규정에 의하여 사업자가 보존하여야 할 거래기록의 대상·범위 및 기간은 다음 각호와 같다. 다만, 통신판매중개자는 자신의 정보처리시스템을 통하여 처리한 기록의 범위내에서 다음 각호의 거래기록을 보존하여야 한다. 1. 표시·광고에 관한 기록 : 6월 2. 계약 또는 청약철회 등에 관한 기록 : 5년 3. 대금결제 및 재화등의 공급에 관한 기록 : 5년 4. 소비자의 불만 또는 분쟁처리에 관한 기록 : 3년	6월~5년
정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령	제66조의8(거래기록의 보존기간 및 방법) ① 통신과금서비스제공자는 법 제58조제4항 및 제5항에 따라 다음 각 호의 사항에 관한 기록을 해당 거래를 한 날부터 1년간 보존하여야 한다. 다만, 건당 거래 금액이 1만원을 초과하는 거래인 경우에는 5년간 보존하여야 한다.	1년, 5년

또한, 클라우드 컴퓨팅 서비스를 제공하는 사업자가 파산이나 폐업 등으로 해당 서비스가 중단되는 경우 클라우드 컴퓨팅 서비스 이용자에게 저장된 정보를 이전 또는 폐기할 수 있는 방안이 마련될 필요가 있으며, 클라우드 컴퓨팅 서비스에 보관되어 관리되는 개인정보에 대한 권리가 클라우드 컴퓨팅 서비스를 이용하는 사업자에게 있다고 보기 어려우며, 개인정보를 제공한 정보 주체에게 저장된 정보의 권리가 있다고 할 수 있다.

4.1.4 개인정보처리시스템 운영 위탁

클라우드 컴퓨팅 서비스를 이용하는 개인 또는 사업자는 IT서비스를 클라우드 형태로 제공받기를 원하지만, 자신의 데이터가 타인 또는 타 기업과 공유되기를 원하지 않으며, 개인정보 취급 업무와 관련된 서비스를 클라우드 서비스 형태로 이용할 경우에도 안정성과 안전성이 동시에 제공되기를 서비스 이용자는 원한다.

또한, 클라우드 컴퓨팅 서비스를 이용하는 사업자는 개인정보 유출/노출 등 개인정보 침해 사고에 대한 관리계획 및 대응 방안을 마련하여야 하며, 개인정보보호에 대한 법률적 요구사항이 충족되도록 하여야 한다. 또한, 침해사고 발생 시 보안 사고에 대한 책임 소재가 여전히 중요한 이슈로 남아 있다.

클라우드 컴퓨팅은 IT자원을 직접 보유하고 관리하는 대신 저렴한 비용으로 필요한 만큼 자원을 빌려서 사용하고, 사용한 만큼 비용을 지불하여, 시장 및 사업 환경 변화에 유연하게 대처할 수 있도록 확장성을 제공하고 업무 효율성과 생산성도 향상시킬 수 있다. 그러나 이러한 효용성에도 불구하고 정보보호 및 안정성, 신뢰성 측면에서 사용자들의 우려가 나타나고 있으며, 2008년 7월 Amazon S3 서비스의 8시간 서비스 중단 사고, 2009년 9월 Google Docs 서비스 해킹 사고 등의 문제에서 보여준 바와 같이 서비스 확산을 위하여 반드시 해결해야 하는 문제들이 있다.

4.2 클라우드 컴퓨팅 서비스 제공자의 개인정보보호

4.2.1 클라우드 컴퓨팅 사업자의 개인정보보호 조치 방안

첫째, 클라우드 컴퓨팅 서비스제공레벨 수립

클라우드 컴퓨팅 서비스 이용자는 서비스 제공자에게 대가를 지불하고 클라우드 컴퓨팅 서비스를 제공받는 임대차 계약을 체결하는 것으로, 서비스 이용자가 클라우드 컴퓨팅 서비스 제공자와 하드웨어, 소프트웨어를 포함한 IT서비스를 제공에 대한 계약상 책임사항은 일반적으로 약관에 포함된 포괄적인 권리의무 관계에 의하여 설정되지만, 이용 약관은 포괄적인 권리와 의무 관계에 대한 계약의 형태로 나타나기 때문에, 개인정보보호에 대한 서비스 제공 범위와 법률적 책임사항이 향후 불명확하게 나타날 수 있다.

SLA란 기대되는 서비스 수준에 대하여 서비스 계약 당사자간 사전에 협약을 체결하는 것으로, 계약상 약관에 정해진 서비스 제공 내용을 구체화하는 역할을 가지며, 개인정보보호에 대한 사항은 법률적 이슈가 발생할 수 있음으로 SLA를 통하여 명확히 할 필요가 있다. 따라서, 현재의 서비스 가용성 등 부분적인 책임사항 보장만으로는 실질적인 개인정보보호에 대한 위험을 관리하기 어려우며, 클라우드 컴퓨팅 서비스의 특성 상 이용자가 자신의 데이터가 어디에 보관되고 어떻게 관리되고 있는지 알기 어렵기 때문에 서비스 약관을 개선하여 서비스 제공자는 이용자의 개인정보보호에 대한 서비스 제공 범위를 상호 협약하고 관리체계를 개선하여 향후 법률적 논란의 소지를 사전에 해소하기 위하여 클라우드 컴퓨팅 개인정보보호 요구사항이 포함된 계약 및 서비스제공레벨 협정을 체결하여야 한다.

둘째, 데이터 저장 위치를 명확히 고지하기

클라우드 서비스에서의 데이터 저장 위치는 서비스 제공자 및 이용자 측면에서 매우 중요한 사항이다. 데이터 저장 위치가 해외에 있을 경우 개인정보보호와 관련된 법률 분쟁이 발생하였을 때 데이터에 대한 통제권을 행사하기 어렵고, 재판 관할권과 관련된 이슈가 발생할 수 있다. 따라서 클라우드 서비스 제공자는 이용자에게 데이터가 저장되는 데이터베이스 서버의 위치와 데이터 통제권에 대하여 이용자에게 고지하고 이용자가 서비스 이용을 선택할 수 있도록 하여야 한다.

또한, 클라우드 서비스를 이용하는 사업자는 클라우드 서비스 제공자와 개인정보보호와 관련된 국내법을 준수하도록 서비스 이용 계약에 명시적으로 표시하는 것이 필요하다.

셋째, 저장 데이터에 대한 접근 통제 및 처리 방침

서비스 제공자는 이용자의 개인정보 또는 기밀정보

를 보호하기 위하여 데이터에 임의로 접근하여서는 안 된다. 따라서, 이용자 개인정보보호를 위하여 이용자 데이터 접근 범위와 접근 시 이력을 기록하도록 하는 내용을 계약에 명시하고 클라우드 서비스 제공자가 민감한 정보와 개인정보에 접근하는 통제 절차와 방법을 구체적으로 제시하여야 한다. 또한, 서비스 형태에 따라 개별 법률적인 데이터 보관 주기를 준수하기 위하여 구체적인 데이터 보존 절차를 명시하고 이에 대한 배상의 책임을 명기하는 것이 필요하다.

넷째, 데이터 보관을 위한 백업/복구 수준 보장

이용자의 민감 데이터 보호와 개인정보 데이터에 대한 법률적 데이터 보관 의무를 이행하기 위하여 클라우드 서비스 제공자는 데이터 백업 및 복구 체계에 대한 적절한 관리 체계를 갖추고 서비스를 제공하여야 한다.

$$\text{백업 준수율}(\%) = \frac{\text{실시된 백업 건수}}{\text{계획된 백업 건수(총 건수)}} \times 100$$

* 계획된 백업 건수 : 서비스 계약 또는 서비스제공 레벨협정(SLA)에 의한 백업 요구 건수
* 실시된 백업 건수 : 클라우드 서비스 제공자에 의하여 실시된 백업 건수

4.2.2 클라우드 컴퓨팅 서비스 개인정보보호 관리체계 인증

서비스에 대한 개인정보보호 관리체계에 대한 보증을 위하여 법률적으로 규제를 강화하는 방법이 있겠으나, 과도한 규제로 인한 산업 활성화가 저해될 위험이 있다. 따라서, 클라우드 컴퓨팅 서비스 제공자를 위한 개인정보관리체계에 대한 인증제도 도입이 필요하다. 클라우드 컴퓨팅 서비스에 대한 독립된 인증 체계를 도입할 수도 있겠으나, 한국인터넷진흥원(KISA)에서 시행 중인 개인정보보호관리체계(PIMS) 인증 분야(관리과정, 보호대책, 생명주기)의 구성요소를 유지하면서 클라우드 컴퓨팅 서비스와 관련된 내용을 보완하고, 개인정보보호에 대한 서비스 제공 수준 보증을 위한 항목을 구체화하고 서비스 제공 범위에 맞도록 세부 점검 내역을 수정하여 적용하는 것이 필요하다.

또한, 클라우드 컴퓨팅 서비스 제공자를 위한 독립적인 인증 제도 도입이 고려될 수 있다. 클라우드 서비스별 통제 범위를 분석하여 인증 체계를 개발하는 것이 필요한데, 이를 위해서는 클라우드 컴퓨팅 서비스에 대한 국내외 표준과 개인정보보호에 대한 규제 분석이 선행되어야 하겠다.

〔표 8〕 클라우드 컴퓨팅 서비스 제공자를 위한 개인정보보호 관리체계(PIMS) 개선 방향

통제 분야	세부 내용	주요 개선 사항
개인정보보호 대책 요구사항	1. 개인정보보호 정책	▪ 클라우드 컴퓨팅 서비스 유형별 개인정보관리 정책, 지침, 절차
	2. 개인정보보호 조직	▪ 클라우드 서비스 사용 조직의 보안책임자 지정
	3. 개인정보 분류	▪ 클라우드 서비스 제공 유형에 따른 정보자산 분류 체계
	4. 교육 및 훈련	▪ 클라우드 서비스에 대한 기술적/관리적 보호조치 교육
	5. 인적보안	▪ 클라우드 환경에 접근하는 개인정보취급자 최소한으로 제한
	6. 침해사고 처리 및 대응	▪ 클라우드 제공자와 사용자 간의 침해사고 보고 채널 유지 ▪ 클라우드 환경에서 발생한 개인정보 침해사고 처리 및 복구 절차
	7. 내부검토 및 감사	▪ 클라우드 환경에 대한 법률적 요구사항 정의 ▪ 클라우드 환경에서의 접속기록 보존 및 검토/모니터링 절차
	8. 기술적 보호조치	▪ 클라우드 환경의 인증,권한부여, 접근통제에 대한 적절한 보호조치 ▪ 클라우드 환경의 개인정보 취급자 권한에 대한 영향평가 ▪ 가상화 클라우드 플랫폼에서의 개인정보처리시스템에 대한 통제 및 절차의 투명성 보장
	9. 물리적 보호조치	▪ 클라우드 환경 개인정보처리시스템의 물리적 접근통제 및 보호조치
생명주기 준거 요구사항	1. 개인정보수집에 따른 조치	▪ 클라우드 서비스 개인정보처리방침의 명확화
	2. 개인정보 이용 및 제공에 따른 조치	▪ 클라우드 환경 개인정보처리시스템 위탁에 따른 보호조치 ▪ 클라우드 서비스 사용자의 개인정보 접속 이력, 이용 및 제공 내역 제공 방안
	3. 개인정보 관리 및 파기에 따른 조치	▪ 클라우드 환경에서의 데이터 보존 관리 및 파기에 대한 관리 방안 및 보호조치

V. 결 론

클라우드 컴퓨팅 서비스의 많은 장점으로 인하여 서비스 이용자가 확대되고 있으며, 기업 이용자뿐만 아니라 개인 이용자의 이용도 확대되고 있으나, 현재 서비스 제공 기업들이 서비스 가용성 측면의 부분적인 품질 보증에 대해서만 보증하고 있는 상황이다. 2012년도 이후 민간 기업에서도 클라우드 컴퓨팅을 이용한 서비스 환경 구축에 대한 요구사항이 커질 것으로 예상 된다. 따라서 클라우드 서비스 제공자는 개인정보보호와 관련된 데이터 보존 방법, 데이터 보관에 대한 물리적 위치 고지, 개인정보보호와 관련된 법률 분쟁 발생 시 재판관할권 문제 등에 대하여 이용자 개인정보보호를 위한 보호장치를 충분히 마련하여야 하며, 클라우드 컴퓨팅 서비스 제공자는 서비스 제공 유형에 따라 개인정보보호와 관련된 사항들을 충분히 검토하고 서비스 이용 계약에 관련 내용이 포함되도록 하는 것이 필요하다.

또한, 사업자가 개인정보보호와 관련하여 고려해야 할 제도는 전기통신기본법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 위치정보보호법, 개인정보보호법 등이 있지만, IT서비스를 이용한 인터넷 서비스의 특징과 사회적 변화를 충분히 반영하고 있지는 못하다. 클라우드 컴퓨팅 서비스의 유형이 반영된 개인정보 관리 체계 요구사항을 제도적으로 구체화할 필요가 있으며, 서비스 제공자 및 이용자 보호를 위하여 서비스 표준 약관 및 서비스수준협약(SLA)에 대한 보호 장치 또한 마련되어야 하며 이을 위하여 "약관규제법" 등에서 클라우드 서비스 이용자 보호를 위한 제도 및 책임기준을 마련할 필요가 있다.

참고문헌

〔1〕 http://en.wikipedia.org/wiki/Cloud_computing

〔2〕 NIST, "Working Definition of Cloud computing" 2009.08

〔3〕 M. Armbrust, et al., "Above the Clouds: A Berkeley View of Cloud Computing", University of California, Department of EECS, Technical Report No. UCB/EECS-2009-28, Feb. 2009

〔4〕 김일태, "클라우드 컴퓨팅을 활용한 비즈니스 연구: 모바일 클라우드 사례를 중심으로", 석사학위논문, 포항공과대학교, 2011년 2월.

〔5〕 NIST, "Guidelines on Security and Privacy in Public Cloud Computing", NIST SP 800-144, Dec. 2011

〔6〕 NIST, "The NIST Definition of Cloud Computing", NIST SP 800-145, Sep. 2011

〔7〕 NIST, "DRAFT Cloud Computing Synopsis and Recommendations", NIST SP 800-146, May 2011

〔8〕 이주영, "클라우드 컴퓨팅의 특징 및 사업자별 제공 서비스 현황", 방송통신정책, 제22권 제6호, pp.6, 2010년

〔9〕 Bruce Robertson, "Top Five Cloud - Computing Adoption Inhibitors", Gartner Research, ID Number. G00167920, May 2009

〔10〕 이창범, 이대희, 이민영, 이병준, 정준현, 김현정, 고영하, "클라우드컴퓨팅 활성화를 위한 법제도 개선방안 연구", 한국인터넷진흥원 연구보고서, 2010년 12월

〔11〕 박대하, 백태석, "클라우드 컴퓨팅 개인정보보호 연구동향과 과제", 정보보호학회지, 제21권 제5호, pp.37-44, 2011년 8월.

〈著者紹介〉

유 우 영 (Woo-Young Yu) 정회원
2008년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호정책, 정보법학, 개인정보보호, 클라우드 컴퓨팅 등

임 종 인 (Jong-In Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 이학석사
1986년 2월: 고려대학교 수학과 이학박사
2000년 10월~현재: 고려대학교 정보보호대학원 원장
2012년 1월~현재: 고려대학교 사이버국방학과 교수
現 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안 전문기술위원회 위원장, 산업기술보호위원회 위원, 국방부 정보화책임관 자문위원 등
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 사이버전, 융합기술보안 등