Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.1245

클라우드 서비스 유형별 개인정보보호 방안

이 보 성,† 김 범 수‡
연세대학교 바른ICT연구소

Protection of Personal Information on Cloud Service Models

Bosung Lee,† Beomsoo Kim‡
Barun ICT Research Center, Yonsei University

요 약

클라우드 컴퓨팅의 성장과 더불어 클라우드 이용자 데이터 보안에 대한 우려가 증가하고 있으므로 이러한 우려를 감소시키는 것이 클라우드 컴퓨팅에서 필수적이다. 본 논문에서는 클라우드 컴퓨팅에 대한 정의 및 장단점을 설명하고 클라우드 컴퓨팅 발전법에서 정의하고 있는 이용자 정보 보호 규정에 대해 논한다. 다음으로 클라우드에서의 개인정보 보호 논점 및 개인정보 위·수탁에 관한 기존 연구 내용을 살펴본다. 그리고, 클라우드 서비스 유형에 따른 개인정보 저장 방식의 차이를 살펴보고 이로 인해 클라우드 서비스 별로 개인정보의 위·수탁 관계가 달라져야 함을 논한다. 이를 바탕으로 IaaS와 SaaS 클라우드 서비스 유형별로 개인정보를 보호하는 방안을 제안한다.

ABSTRACT

As cloud computing services become popular, the concern on the data security of cloud services increases and the efforts for the data security become essential. In this paper, we describe the pros and cons of cloud computing including the definition of cloud. Then, we discuss the regulations about the protection of user data defined in cloud promotion act. Previous studies related to the privacy protection and the entrustment of personal information in cloud computing are reviewed. We examine how to store the personal information depending on the cloud service model. As a result, we argue that the entrustment of personal information should vary according to the cloud service model and we propose how to protect the personal information on IaaS and SaaS cloud service models.

Keywords: Cloud Service Model, Cloud Promotion Act, Protection of Personal Information

I. 서 론

애플의 창업자인 스티브 잡스(Steve Jobs)는 지난 2011년 애플세계개발자회의(Apple Worldwide Developers Conference, WWDC)의 키노트 발표에서 디지털 시대의 중심이 PC에서 클라우드(Cloud)로 옮겨갈 것이라고 주장하면서 iCloud를 소개하였다. 그는 iCloud를 통해 문서, 사진, 음악 등의 콘텐츠뿐만 아니라 앱(응용프로그램, App)도 PC, 스마트폰, 태블릿 등 다양한 디바이스에서 언제 어디서나 인터넷을 통해 사용이 가능하다고 발표하였다. 이를 통해 IT 전문가들 사이에서 연구되고 전문적인 기업들 사이에서만 서비스되던 클라우드 컴퓨팅의 개념이 일반 대중들에게도 널리 확산되는 계기로 작용하였다. 현재 클라우드 컴퓨팅은 주요한 IT 자원 제공방식의 하나로 알려져 있으며, 2013년 현재 전 세계적으로 시장규모 368억불의 IT 산업으로 발전하였으며 2018년에는 그 규모가 1,275억불로 성장할 것으로 예상되고 있다. 이와 더불어 국내의 클라우드 컴퓨팅 산업은 2013년 3,932억원, 2014년

접수일(2015년 6월 9일), 수정일(2015년 8월 7일), 게재확정일(2015년 8월 13일)
† 주저자, bs.lee@barunict.kr
‡ 교신저자, beomsoo@yonsei.ac.kr (Corresponding author)

5,238억원의 시장규모를 갖는 산업으로 매년 30% 이상의 고성장이 예측되고 있다[1].

그런데 클라우드 상의 어디엔가 자신들의 데이터가 저장되고 그 관리를 클라우드 서비스 제공자에게 맡긴다는 점에서 데이터 보안 등에 대한 클라우드 컴퓨팅 이용자의 우려가 증가하고 있다. 따라서 클라우드 컴퓨팅의 발전을 위해서는 이용자의 보안 우려를 불식시키는 것이 필수적인 요소가 되었다. 특히 클라우드 컴퓨팅에서 개인정보 보호에 대한 우려가 증가하여 이에 대한 다양한 연구가 이루어지고 있어 클라우드 컴퓨팅 이용자의 보안 우려를 감소시키고자 하는 노력이 계속되고 있다.

전 세계적인 클라우드 컴퓨팅의 확산과 이용자 정보 보호 추세를 반영하여 국내에서도 2015년 3월 '클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률(이하, 클라우드 컴퓨팅 발전법)'이 국회를 통과하여 2015년 9월 시행되어 국내 클라우드 산업 발전과 이용자 정보 보호의 획기적인 전환점이 될 것으로 기대된다.

본 논문에서는 클라우드 컴퓨팅에 대한 정의 및 장단점과 함께 클라우드 컴퓨팅 발전법에서 정의하고 있는 이용자 정보 보호 규정에 대해서 알아보고자 한다. 그리고 클라우드에서의 개인정보 보호 논점 및 개인정보 위·수탁에 대한 기존 연구 내용을 살펴보고 클라우드 서비스 유형에 따라 개인정보 저장 방식의 차이가 발생하며 이에 따라 개인정보의 위·수탁 관계에서도 클라우드 서비스 유형에 따른 차이가 발생함을 논하고자 한다. 이를 통해 클라우드 서비스 유형별로 개인정보를 보호하기 위한 방안을 제안하고자 한다.

II. 클라우드 컴퓨팅 개요

이 장에서는 클라우드 컴퓨팅의 정의와 클라우드 서비스의 유형 및 장단점에 대해서 살펴보고자 한다.

2.1 클라우드 컴퓨팅의 정의

서론에서 언급한 애플의 iCloud 발표 이전에도 여러 IT 관련 전문기관이 클라우드 컴퓨팅에 대해서 다양한 정의를 내렸는데, 대표적인 것들로 다음을 들 수 있다.

- 가트너: 인터넷 기술을 이용하여 확장성과 유연성을 갖는 IT 기반 기능을 서비스 형태로 제공하는 컴퓨팅 유형[2]
- 포레스터 리서치: 인터넷 기술을 이용하여 표준화된 IT기능(서비스, 소프트웨어 또는 인프라스트럭처)을 셀프서비스 형태로 제공하고 사용한 만큼 비용을 지불하는 컴퓨팅 유형[3]
- NIST: 언제, 어디서나 편리하게 공유된 컴퓨팅 자원(네트워크, 서버, 스토리지, 어플리케이션 및 서비스 등)을 네트워크를 통해 원하는 만큼 사용하는 컴퓨팅 모델로 서비스 제공자의 최소한의 작업이나 관리만으로 이러한 자원을 신속하게 제공하고 배포할 수 있는 모델[4]

이상의 정의에서 보듯이 "인터넷(또는 네트워크)"을 이용하여 "컴퓨팅 자원(IT 기능)"을 "서비스 형태"로 제공하고 "사용한 만큼 비용을 지불"하는 것이 클라우드 컴퓨팅의 중요한 특징이라고 할 수 있다. 이를 정리하면 다음과 같다.

- 클라우드 컴퓨팅: 하드웨어, 소프트웨어, 데이터 등 IT 자원을 네트워크를 통해 표준화된 서비스 형태로 제공하고 사용자는 언제, 어디서나 원하는 만큼 이러한 IT 서비스를 이용하고 사용한 만큼 비용을 지불하는 컴퓨팅 모델

2.2 클라우드 컴퓨팅 유형 분류

클라우드 컴퓨팅 유형은 제공 유형(Deployment Model)에 따라 사설 클라우드(Private Cloud), 공용 클라우드(Public Cloud), 혼합 클라우드(Hybrid Cloud) 및 커뮤니티 클라우드(Community Cloud)로 분류할 수 있으며, 서비스 유형에 따라 IaaS (Infrastructure as a Service), PaaS (Platform as a Service) 및 SaaS(Software as a Service)로 분류[4]할 수 있는데, Table 1.과 2.에 그 내용을 정리하였다.

2.3 클라우드 컴퓨팅의 장단점

클라우드 컴퓨팅은 사용자가 IT자원을 직접 소유하지 않고 클라우드 컴퓨팅 서비스 제공자의 자원을 필요할 때 빌려서 사용하기 때문에 IT자원의 활용률을 제고할 수 있을 뿐만 아니라 유휴 자원을 최소화할 수 있어 IT 인프라 도입 비용을 절감할 수 있다.

Table 1. Cloud Computing Deployment Models

Models	Description
Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers
Community Cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns
Public Cloud	The cloud infrastructure is provisioned for open use by the general public
Hybrid Cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability

Table 2. Cloud Computing Service Models

Models	Description
IaaS (Infrastructure as a Service)	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications
PaaS (Platform as a Service)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider
SaaS (Software as a Service)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure

뿐만 아니라 자원 할당 및 회수 등을 클라우드 서비스 제공자가 자동화된 방식으로 제공하므로 기존의 수주에서 수개월이 걸리던 IT 자원 할당 기간을 수 분에서 수 십 분 내로 단축할 수 있어 효율성이 크게 향상된다. 이와 함께 클라우드 컴퓨팅 사용자가 공통으로 사용하는 시스템이나 어플리케이션을 통합하여 유지 관리의 효율성을 제고할 수 있으며 표준 개발 플랫폼 등의 제공을 통해 개발 기간을 단축하고 개발 환경에 대한 중복 투자를 방지할 수 있는 등 경제성, 편리성 및 효율성에서 많은 장점이 있다.

반면 클라우드 컴퓨팅에서는 사용자의 모든 IT 자원이 클라우드 컴퓨팅 서비스 제공자의 데이터센터에 집중되므로 클라우드 서비스 장애 발생 시 사용자의 서비스가 중단될 수 있다는 서비스 안정성(availability) 이슈와 클라우드 서비스의 보안에 대한 안전성(security) 우려가 증가하고 있다. 특히 클라우드 서비스 이용자의 개인정보의 유출 가능성에 대한 우려와 해킹이나 사이버테러로 인한 이용자 정보의 유출 및 재해로 인한 데이터 손실 우려 등을 단점으로 들 수 있다[5].

III. 클라우드컴퓨팅 발전법의 이용자 정보 보호 관련 규정

전 세계적인 클라우드 컴퓨팅의 성장과 더불어 클라우드 컴퓨팅에서의 이용자 정보 보호와 신뢰 담보를 위한 법적·제도적 개선이 요구되어 왔다. 이러한 요구를 반영하여 2015년 3월 '클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률(이하, 클라우드 컴퓨팅 발전법)'이 국회를 통과하여 2015년 9월 시행되는데, 이 법에는 Table 3.에 요약한 바와 같이 클라우드에서의 이용자 정보 보호를 위한 규정이 정의되어 있다.

제4조에서는 클라우드에서의 이용자 보호에 관해서는 클라우드 발전법이 타 법률에 우선하지만 개인정보에 관해서는 기존의 '개인정보 보호법'과 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 등 관련 법에서 정하는 바에 따르도록 규정하여 이용자 정보 및 개인정보 보호에 대한 타 법률과의 관계를 규정하고 있다.

제26조에서는 이용자가 클라우드 컴퓨팅 서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려주도록 요구할 수 있음을 규정하여 클라우드 이용자 보호를 위한 정보 공개를 명시하고 있다. 이와 더불어 정보통신서비스 제공자에게 클라우드 컴퓨팅 서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭을 알려주도록 요구할 수 있음을 규정하고 있다.

한편 제27조에서는 법원의 제출명령이나 법관이 발부한 영장에 의하지 아니하고는 이용자의 동의 없

Table 3. Regulations for the protection of user data in cloud promotion act

Article	Keyword	Description
Article 4	Relationship with other Acts	· Cloud promotion act shall take precedence over other acts in regard to protect user in cloud · Personal information shall be governed by related acts such as 'Personal information protection act' and 'Act on promotion of information and communications network utilization and information protection, etc.'
Article 26	Request for information for protection of user	· request for the State's name storing user data to cloud computing service provider · request for the State's name storing user data to information and communications service provider for use of cloud computing service
Article 27	Providing a third person	· prohibited to use or provide a third person with user data without obtaining the consent of user or without order to submission of courts or warrant issued by judges
	Return and destruction of user data	· return or destroy the user data when the business ends

이 이용자 정보를 제3자에게 제공하거나 서비스 목적 이외에 이용할 수 없도록 하여 제3자 제공 여부에 대한 규정을 명확하게 하고 있다. 이와 더불어 사업 종료 시 이용자 정보를 반환하거나 파기하여야 한다고 규정하고 있다.

이상을 요약하면 클라우드에서의 개인정보에 관해서는 개인정보보호법과 정보통신망법을 따르도록 규정하고 기존의 법률에 정의되지 않았던 클라우드에 저장된 개인정보의 물리적 저장 위치 및 해외 이전에 관한 사항, 사생활 보호, 수사기관과 제3자 제공에 관한 사항 및 클라우드 저장 정보의 반환, 보존 및 파기 등에 관한 사항은 클라우드 컴퓨팅 발전법에 규정하여 클라우드 컴퓨팅 서비스 제공자가 개인정보를 포함한 이용자 정보 보호에 노력하도록 하고 있다는 점에서 법률 제정의 의의를 찾을 수 있다.

IV. 클라우드의 개인정보 위·수탁 관계 연구

클라우드 컴퓨팅에서의 개인정보보호에 관한 기존의 연구는 클라우드에서의 개인정보의 운영·위탁에 관한 연구[6][7], 클라우드에 저장된 개인정보의 물리적 저장 위치 및 해외 이전에 관한 연구[6][7][8], 사생활 보호, 수사기관과 제3자 제공에 관한 연구[6] 및 클라우드 저장 정보의 반환, 보존 및 파기 등에 관한 연구[6][8]가 선행되었다.

이러한 연구 중 클라우드에서의 개인정보의 운영·위탁에 관한 연구[6][7]를 보면, 클라우드 서비스에서는 사용자가 자신의 컴퓨팅 자원이 아닌 서비스 제공자의 하드웨어와 소프트웨어를 이용하여 자신의 데이터를 처리하고 이를 클라우드 컴퓨팅 서비스 제공자의 저장 장치에 저장하게 되므로 최종 사용자의 개인정보 또한 클라우드 컴퓨팅 서비스 제공자의 저장 장치에 저장된다. 따라서 클라우드 컴퓨팅의 최종 사용자와 클라우드 서비스를 이용하여 정보통신서비스를 제공하는 기업(이하, 정보통신서비스 제공자)과 클라우드 컴퓨팅 서비스 제공자의 관계에서 정보통신서비스 제공자는 최종 사용자의 개인정보를 클라우드 컴퓨팅 서비스 제공자에게 위탁하고, 클라우드 컴퓨팅 서비스 제공자는 이를 수탁하여 처리함으로써 정보통신망법 제25조에서 정의되어 있는 개인정보 취급 위탁에 관련된 조항의 영향을 받는다[6][7]고 하였다.

그런데, 클라우드 컴퓨팅 서비스 구성의 특수성과 서비스 형태를 고려할 때 클라우드 서비스 이용자(정보통신서비스 제공자, 위탁자)는 수탁자(클라우드 컴퓨팅 서비스 제공자)의 선임에 대해서만 책임을 묻고 관리·감독의 의무나 책임은 면제하는 것이 타당하다는 견해[6]와 클라우드 서비스의 경우 일반적인 IT 업무 위탁과는 달리 위탁자가 도처에 분산되어 있는 클라우드 컴퓨팅 서비스 제공자(수탁자)의 서버 및 데이터 센터를 관리·감독하기가 현실적으로 어려우므로 클라우드 컴퓨팅에서는 개인정보 취급 위탁 등의 조항 적용의 완화가 필요하다는 견해가 있다[7].

한편, 또 다른 연구[9]에서는 클라우드에서의 개인정보 위탁 모델을 시나리오 별로 8가지로 분류하여 클라우드 사용자(개인), 클라우드 소비자(위탁자),클라우드 제공자(수탁자) 및 클라우드 제공자(제3자) 간의 개인정보 위·수탁 관계를 시나리오 별로

분류하였는데, 이 논문에서 분류한 내용은 클라우드의 최종 사용자(개인)와 클라우드를 사용하는 정보통신서비스 제공자(클라우드 소비자) 및 클라우드 컴퓨팅 서비스 제공자 간의 다양한 위·수탁 관계를 고려하였다는 점에서 의미가 있다. 본 연구에서는 추가적으로 클라우드 서비스 유형에 따라 최종사용자, 정보통신서비스 제공자 및 클라우드 컴퓨팅 서비스 제공자 간의 개인정보 위·수탁 관계를 고려하고 이에 대한 처리 방안을 알아보고자 한다.

V. 클라우드 서비스 유형별 개인정보 처리 방안

앞에서 살펴본 클라우드 컴퓨팅 발전법에서의 이용자 정보 보호 규정과 클라우드에서의 개인정보보호에 관한 기존의 연구는 클라우드 컴퓨팅 서비스 제공자가 이용자의 개인정보와 데이터를 모두 저장하고 있다는 사실을 전제로 하고 있다. 이에 따라 클라우드 컴퓨팅 발전법에서도 클라우드 컴퓨팅 서비스 제공자로 하여금 이용자의 개인정보와 데이터에 대해 보호를 하도록 규정하고 있다. 그런데 클라우드 서비스의 유형에 따라 특정 클라우드 컴퓨팅 서비스 제공자는 이용자 정보를 저장하고 있음에도 불구하고 해당 이용자 정보에 대한 접근 권한을 갖지 못할 수 있다. 이러한 경우 클라우드 컴퓨팅 서비스 제공자의 이용자 정보 보호에 대한 책임과 의무가 과도해져서 이용자 보호와 서비스 제공에 제약이 생길 수 있어 클라우드 사업자의 대외 경쟁력 확보 등에 어려움이 발생할 수 있다. 그러므로 이 장에서는 클라우드 서비스 유형별로 개인정보와 개인정보를 제외한 이용자 정보가 저장되는 방식을 비교하고 이에 따른 클라우드 컴퓨팅 서비스 제공자의 이용자 정보 보호 범위에 대해서 논하고자 한다.

5.1 클라우드 서비스 유형별 이용자 정보 저장 방식

클라우드 서비스 유형에 따른 이용자 정보 저장 방식의 차이를 논하기에 앞서, 클라우드 서비스 이용자의 정의를 명확하게 할 필요가 있다. 클라우드 컴퓨팅 서비스에서의 이용자라 함은 클라우드 서비스를 이용하는 최종사용자와 클라우드 서비스를 이용하여 최종사용자에게 정보통신서비스를 제공하는 정보통신서비스 제공자를 포함한다. 이는 클라우드 컴퓨팅 발전법 제2조제4호와 제26조를 통해 유추할 수 있다.

- 제2조4호 “이용자 정보”란 클라우드 컴퓨팅서비스 이용자(이하 “이용자”라한다)가 클라우드 컴퓨팅서비스를 이용하여 클라우드 컴퓨팅 서비스를 제공하는 자(이하 “클라우드 컴퓨팅 서비스 제공자”라 한다)의 정보통신자원에 저장하는 정보로서 이용자가 소유 또는 관리하는 정보를 말한다.
- 제26조(이용자 보호 등을 위한 정보 공개) ① 이용자는 클라우드 컴퓨팅 서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려주도록 요구할 수 있다. ② 정보통신서비스를 이용하는 자는 정보통신서비스 제공자에게 클라우드 컴퓨팅 서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭을 알려주도록 요구할 수 있다.

제2조제4호에 따르면 클라우드에 정보를 저장하는 자를 이용자라고 정의하고 있으므로, 제26조제2호에서 정의한 대로 정보통신서비스 제공자가 클라우드 컴퓨팅 서비스를 이용할 경우 최종사용자와 정보통신서비스 제공자 모두 클라우드 서비스의 이용자가 된다. 이 때, 클라우드 서비스 유형에 따라 최종사용자의 개인정보에 대한 클라우드 컴퓨팅 서비스 제공자의 책임과 의무를 명확하게 규정할 필요가 발생한다.

이 논문에서는 클라우드에서 제공되는 정보통신서비스를 통해 최종사용자, 정보통신서비스 제공자, 클라우드 컴퓨팅 서비스 제공자 간의 개인정보 처리 관계를 서비스 유형별로 살펴보고자 한다.

- 사례 1: 최종사용자 A는 정보통신서비스 제공자 B의 정보통신서비스를 이용하고, 정보통신서비스 제공자 B는 클라우드 컴퓨팅 서비스 제공자 C의 IaaS 클라우드에서 가상 서버와 가상 스토리지를 임대하여 정보통신서비스를 최종사용자 A에게 제공한다.

Fig.1.에 사례 1의 개인정보 및 사용자 데이터 저장 방식이 나타나 있다. 먼저 정보통신제공자 B는 가상서버와 가상디스크를 임대하기 위하여 IaaS 클라우드 컴퓨팅 서비스 제공자 C의 회원으로 가입하고 B 자신의 개인정보를 C에게 ①의 경로를 통해 제공한다. C는 B의 개인정보를 인증 DB(그림에서 ID DB)에 저장한다. 이 때, B의 개인정보처리자는 클라우드 컴퓨팅 서비스 제공자 C가 된다. 그리고 B는 C의 클라우드 인프라에서 가상서버와 가상디스크를 임대하여 최종사용자 A에게 정보통신서비스를

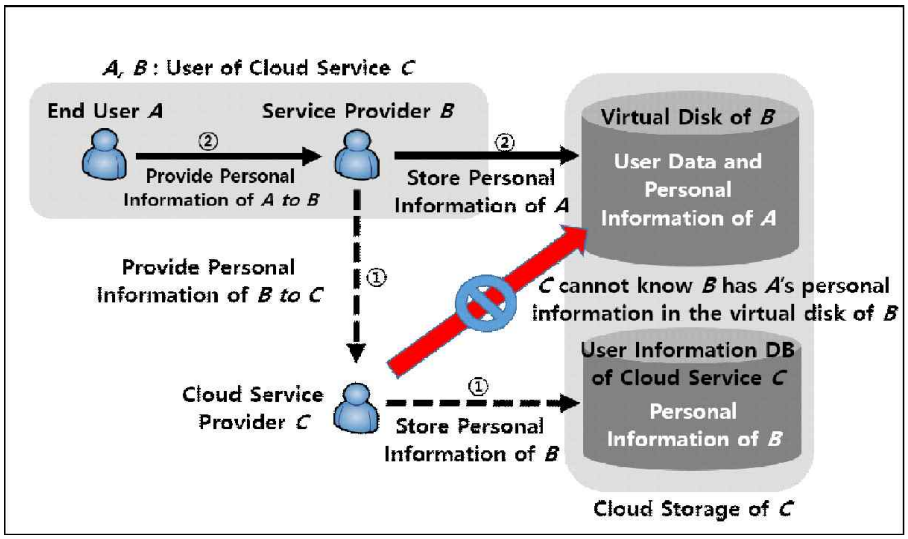

Fig. 1. Storage of personal information and user data in IaaS cloud

제공한다.

최종사용자 A는 B의 정보통신서비스를 이용하기 위하여 B가 제공하는 정보통신서비스에 회원으로 가입하고 ②의 경로를 통해 자신의 개인정보를 B에게 제공한다. 그리고 B는 C에게서 임대한 가상디스크에 최종사용자 A의 개인정보와 이용자 데이터를 저장한다. 이 때, A의 개인정보처리자는 정보통신서비스제공자 B가 된다.

이 때, 클라우드 컴퓨팅 서비스 제공자 C는 A의 개인정보와 B의 개인정보 모두를 자신의 스토리지에 저장하고 있고, 최종사용자 A와 정보통신서비스 제공자 B가 모두 클라우드 컴퓨팅 서비스 제공자 C의 이용자가 된다. 그럼에도 불구하고, C는 B가 임대한 가상디스크 내에 A의 개인정보 저장 유무에 대해서는 알 수가 없다. 이는 IaaS 클라우드의 기본적인 사상으로 C는 B에게 가상디스크와 가상서버 등 인프라를 제공했을 뿐, B가 그 인프라로 어떤 서비스를 제공하고 어떤 데이터를 저장하는지에 대해서는 관여하지 않기 때문이다. 즉, IaaS 클라우드 서비스는 가상 자원을 제공한다는 것 외에는 데이터센터에서 물리적인 IT 자원(서버와 스토리지)을 제공하는 것과 개념적으로 동일하기 때문이다. 따라서 IaaS 클라우드 컴퓨팅 서비스 제공자 C는 최종사용자 A의 개인정보에 대해서는 관여할 필요가 없게 된다.

- 사례 2: 최종사용자 D는 정보통신서비스 제공자 E의 정보통신서비스를 이용하고, 정보통신서비스 제공자 E는 클라우드 컴퓨팅 서비스 제공자 F의 SaaS 클라우드의 정보통신서비스를 임대하여 정보통신서비스를 최종사용자 D에게 제공한다.

Fig.2.에 사례 2의 개인정보 및 사용자 데이터 저장 방식이 나타나 있다. 먼저 정보통신서비스 제공자 E는 F의 정보통신서비스를 임대하기 위하여 SaaS 클라우드 컴퓨팅 서비스 제공자 F의 회원으로 가입하고 E 자신의 개인정보를 F에게 ①의 경로를 통해 제공한다. F는 E의 개인정보를 자신의 클라우드 스토리지에 저장한다. 이 때, E의 개인정보처리자는 클라우드 컴퓨팅 서비스 제공자 F가 된다. 그리고 E는 F의 SaaS 클라우드의 정보통신서비스를 임대하여 최종사용자 D에게 정보통신서비스를 제공한다.

최종사용자 D는 E의 정보통신서비스를 이용하기 위하여 E가 제공하는 정보통신서비스에 회원으로 가입하고 ②의 경로를 통해 자신의 개인정보를 E에게 제공한다. 그리고 E는 F의 클라우드 스토리지에 최종사용자 D의 개인정보와 이용자 데이터를 저장한다. 이 때, D의 개인정보처리자는 정보통신서비스제공자 E가 된다.

그런데, 클라우드 컴퓨팅 서비스 제공자 F는 D의 개인정보와 E의 개인정보 모두를 자신의 스토리지에 저장하고 있고, 최종사용자 D와 정보통신서비스제공자 E가 모두 클라우드서비스 F의 이용자로 F자신의 정보통신 서비스를 이용하고 있으므로, F는 최종사

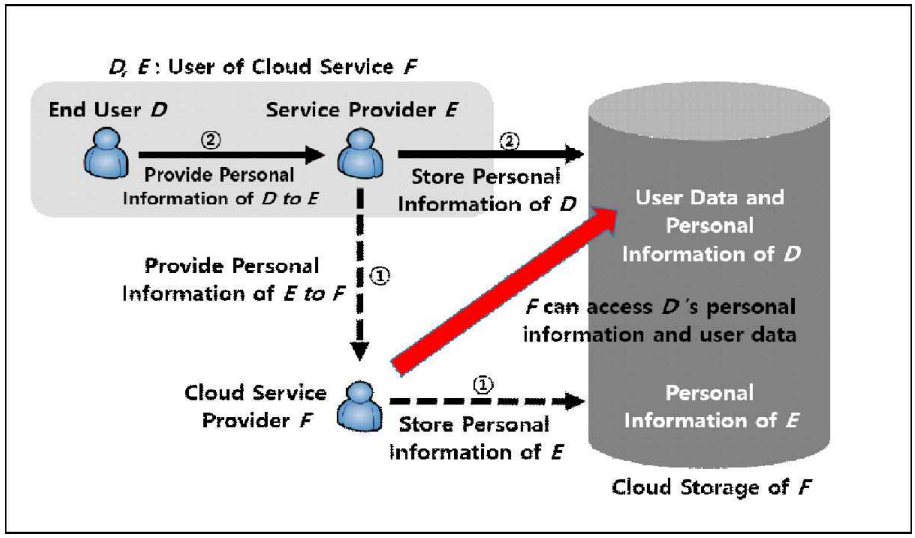

Fig. 2. Storage of personal information and user data in SaaS cloud

용자 D의 정보에 대해서도 접근이 가능하다. 이는 소프트웨어를 빌려 쓰는 SaaS 클라우드의 기본적인 사상으로 F는 E에게는 자신이 제공하는 정보통신서비스에 대한 회원유치와 관리 등을 위임했을 뿐 최종 사용자는 F의 정보통신서비스를 직접 이용하기 때문이다. 따라서 SaaS 클라우드 컴퓨팅 서비스 제공자 F는 최종사용자 D의 개인정보에 대한 처리에도 관여하게된다. 그러므로 최종 사용자 D의 개인정보를 수집하는 것은 E이나 실제로는 F가 D의 개인정보를 처리하게 되어, E와 F사이에는 최종사용자 D의 개인정보에 대한 위·수탁 관계가 명확하게 정의되어야할 필요가 발생한다.

5.2 클라우드 서비스 유형별 개인정보 위·수탁 관계

4장에서 논한 바와 같이 클라우드에서의 개인정보 위·수탁에 관련된 기존의 연구에서는 사례 1과 사례 2 모두 정보통신서비스 제공자가 최종 사용자의 개인정보를 클라우드 컴퓨팅 서비스 제공자에게 위탁하고, 클라우드 컴퓨팅 서비스 제공자가 수탁자로서의 의무를 갖게 되어 개인정보보호법 등에서 규정한 개인정보 처리 방안을 따르는 것이 타당하다[6][7]고 주장하였다. 그러나 사례 1의 IaaS 클라우드에서와 같이 정보통신서비스 제공자 B가 가상 서버와 가상 디스크를 임대하여 자체적으로 정보통신서비스를 제공할 경우 클라우드 컴퓨팅 서비스 제공자 C는 B의 정보통신서비스를 이용하는 최종 사용자 A의 개인정보에 대해서는 저장 유무를 알 수 없게 된다. 따라서 이 경우 정보통신서비스 제공자 B와 클라우드 컴퓨팅 서비스 제공자 C간에는 최종 사용자 A의 개인정보에 대한 위·수탁 관계는 성립하지 않는다고 보는 것이 타당하다.

반면 사례 2에서는 최종 사용자 D의 개인정보는 클라우드 컴퓨팅 서비스 제공자인 F가 저장하고 이를 처리하게 되므로, 기존의 연구 결과에서와 마찬가지로 정보통신서비스 제공자인 E와 클라우드 컴퓨팅 서비스 제공자인 F사이에는 최종 사용자 A의 개인정보 처리에 대한 위·수탁 관계가 성립한다고 보는 것이 타당하다.

5.3 클라우드 컴퓨팅 발전법의 서비스 유형별 이용자 정보 보호 규정

이 절에서는 3장에서 설명한 클라우드 컴퓨팅 발전법에 클라우드 서비스 유형별로 이용자 정보 보호에 관한 규정이 정의 되어 있는지를 알아보고자 한다. IaaS, PaaS, SaaS 등 클라우드 서비스 유형에 대한 내용은 컴퓨팅 발전법에서는 특별히 정의되어 있지 않으나 시행령 제정안[11]에는 제3조에 다음과 같이 클라우드컴퓨팅 서비스가 정의되어 있다.

- 서버, 스토리지, 네트워크 등을 제공하는 서비스
- 응용프로그램 등 소프트웨어를 제공하는 서비스
- 응용프로그램 등 소프트웨어의 개발·배포·운영·관

리 등을 위한 환경을 제공하는 서비스
- 그 밖의 제1호 내지 제3호의 서비스를 2이상 결합 또는 복합한 서비스

위의 서비스는 각각 IaaS, SaaS, PaaS 및 두 가지 이상의 서비스가 결합된 서비스로 이해하면 타당하다.

그런데 법률과 시행령 제정안 모두에서 서비스 유형별로 이용자 정보 보호에 관한 구분이 특별히 정의되어 있지 않으므로 클라우드 서비스 유형에 관계없이 클라우드 컴퓨팅 서비스 제공자는 최종사용자 뿐만 아니라 자신의 클라우드에서 서비스 중인 정보통신서비스 제공자의 정보도 모두 보호해야 한다.

5.4 클라우드 서비스 유형별 침해사고 등의 통지

클라우드 컴퓨팅 발전법 제25조 침해사고 등의 통지 항목에 따라 클라우드 컴퓨팅 서비스 제공자는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제2조 제7호에 따른 침해사고가 발생한 때와 이용자 정보가 유출된 때 그 사실을 해당 이용자에게 알려야 한다. 그런데, IaaS 클라우드에서 정보통신서비스 제공자(사례 1의 B)가 제공하는 서비스에 침해사고가 발생한 경우 클라우드 컴퓨팅 서비스 제공자(사례 1의 C)가 이를 감지하고 이용자에게 통지하는 것은 과도한 트래픽이 유발되거나 다른 이용자에게 영향이 파급되기 전까지는 현실적으로 불가능하다. 따라서 이 조항은 IaaS 클라우드 컴퓨팅 서비스 제공자에게 정보통신서비스 제공자의 침해 사고에 대한 책임까지를 부과하는 것으로 과도하다고 볼 수 있다. 반면 SaaS 클라우드 서비스의 경우에는 클라우드 컴퓨팅 서비스 제공자가 자신이 제공하는 서비스에 대한 즉각적인 침해를 감지하고 이에 따른 조치를 이행하는 것이 타당하다.

한편, IaaS 클라우드에서 서비스 중인 정보통신서비스 제공자의 서비스에서 최종사용자의 개인정보 침해사고가 발생할 경우에 정보통신서비스 제공자는 개인정보보호법에 따라 침해 대응 조치를 이행하는 것이 명확한 반면 IaaS 클라우드 컴퓨팅 서비스 제공자는 클라우드 컴퓨팅 발전법에 따라 이용자정보 침해로 규정하여 대응할 것인지 또는 개인정보보호법에 따라 대응 조치를 취해야 할 것인지가 명확하지 않다. 따라서 침해사고 대응 규정 또한 클라우드 서비스 유형별로 달라져야 한다.

VI. 서비스 유형별 개인정보보호 방안 제안

6.1 클라우드 서비스 유형별 개인정보처리자 구분

이상에서 살펴본 바와 같이 IaaS 클라우드와 SaaS 클라우드 간에는 클라우드 컴퓨팅 서비스 제공자가 최종 사용자의 개인정보와 데이터를 저장하는 방식에 큰 차이가 존재함을 알 수 있다. 그러나 클라우드 컴퓨팅 발전법에서는 클라우드 서비스 유형에 따른 개인정보 보호 방안이 명확하게 구분되어 있지 않으므로 본 논문에서는 다음과 같이 클라우드 서비스 유형에 따라 개인정보처리자를 명확하게 정의하고 이에 따라 클라우드 컴퓨팅 서비스 제공자의 책임과 의무를 규정할 것을 제안하고자 한다.

6.1.1 클라우드 서비스를 직접 사용

최종사용자가 클라우드 컴퓨팅 서비스 제공자와 직접 계약을 맺어 서비스를 제공받을 경우에는 클라우드 서비스의 유형에 관계없이 클라우드 컴퓨팅 서비스 제공자가 최종사용자의 개인정보처리자로서의 책임과 의무를 갖도록 한다.

6.1.2 클라우드 서비스 이용자가 정보통신 서비스를 최종사용자에게 제공하는 경우

클라우드 서비스 이용자가 최종사용자에게 클라우드 컴퓨팅 서비스를 이용하여 정보통신서비스를 제공하는 경우는 클라우드 서비스를 이용하는 정보통신서비스 제공자에 해당한다. 이때는 클라우드 서비스 유형에 따라서 다음과 같이 개인정보처리자를 구분하는 것이 타당하다.

- 정보통신서비스 제공자가 IaaS 클라우드 서비스를 이용하여 최종사용자에게 정보통신서비스를 제공할 때는 정보통신서비스 제공자가 최종사용자의 개인정보처리자로서의 책임과 의무를 갖는다. 이 때, IaaS 클라우드 컴퓨팅 서비스 제공자는 최종사용자의 개인정보처리자가 아님을 명시하도록 한다.
- 정보통신서비스 제공자가 SaaS 클라우드 서비스를 이용하여 최종사용자에게 서비스를 제공할 때는 정보통신서비스 제공자가 최종사용자의 개인정보처리자로서의 책임과 의무를 갖되, SaaS 클

라우드 컴퓨팅 서비스 제공자와 위·수탁 계약을 통해 최종사용자의 개인정보를 수탁하는 것이 타당하다.

6.2 개인정보를 제외한 이용자 정보 처리 방안

IaaS 클라우드의 경우 개인정보를 제외한 최종사용자의 이용자 정보도 정보통신서비스 제공자가 임대한 가상디스크 내에 저장되므로, 이에 대한 침해 사고는 가상 서버에 대한 침해를 통해 발생한다. 이 때 최종사용자의 이용자 정보 유출에 대해서는 일차적으로 정보통신서비스 제공자가 책임을 지고 IaaS 클라우드 컴퓨팅 서비스 제공자는 하이퍼바이저 보안 침해 또는 클라우드 서비스 관리자에 의한 가상디스크의 유출 등에 대해서만 책임을 지도록 하는 것이 타당하다.

반면, SaaS 클라우드 컴퓨팅 서비스 제공자의 경우는 최종사용자의 이용자 정보 또한 정보통신서비스 제공자를 대신하여 직접 처리하게 되므로, 이용자 정보에 대해서도 정보통신서비스 제공자와 위·수탁 계약을 체결하도록 하는 것이 타당하다.

Table 4.에 최종사용자, 정보통신서비스 제공자 및 클라우드 컴퓨팅 서비스 제공자간의 개인정보와 이용자 정보에 대한 처리자 및 위·수탁 관계에 대한 요약이 나타나 있으며, Table 5.에는 클라우드컴퓨팅 발전법에서 개선이 필요한 조항에 대해서 요약하였다.

VII. 결론 및 향후 연구 방향

본 논문에서는 클라우드 컴퓨팅 환경에서의 개인정보 보호에 관련된 기존의 연구결과를 살펴보고 클라우드 컴퓨팅 발전법에서 규정하고 있는 이용자 정보 보호 방안에 대해서 알아보았다. 그리고 클라우드 서비스 유형에 따라 개인정보의 저장 방식이 달라지며 이에 따라 개인정보의 처리 및 보호 방안이 달라질 수 있음을 예시하였다.

이와 더불어 정보통신서비스 제공자가 IaaS 클라우드 서비스를 이용하여 최종사용자에게 서비스를 제공할 때는 정보통신서비스 제공자가 최종사용자의 개인정보처리자로서의 책임과 의무를 갖고 IaaS 클라우드 컴퓨팅 서비스 제공자는 최종사용자의 개인정보처리자가 아님을 명시할 것을 제안하였다. 한편, 정보통신서비스 제공자가 SaaS 클라우드 서비스를 이용하여 최종사용자에게 서비스를 제공할 때는 정보통신서비스 제공자가 최종사용자의 개인정보처리자로서의 책임과 의무를 갖되, SaaS 클라우드 컴퓨팅 서비스 제공자와 위·수탁 계약을 통해 최종사용자의 개인정보를 수탁하는 것이 타당하다고 제안하였다.

본 논문에서는 클라우드 서비스 유형을 IaaS와 SaaS 두 가지로 구분하여 설명하였는데, 최근 클라우드 컴퓨팅 서비스 제공자는 IaaS, PaaS, SaaS 서비스 등을 혼합하여 제공하는 것이 보편적으로, 실제 서비스 제공자의 이용 계약 등을 분석하여, 최종사용자와 클라우드에서 서비스를 제공하는 정보통신서비스 제공자 및 클라우드 컴퓨팅 서비스 제공자 간의 권한과 책임을 명확하게 구분하는 방안에 대한 추가 연구가 필요할 것이다. 또한 클라우드에 저장된 개인정보의 물리적 저장 위치 및 해외 이전에 관한 논점, 사생활 보호, 수사기관과 제3자 제공에 관한 논점 및 클라우드 저장 정보의 반환, 보존 및 파기 등에 관한 논점 등에 대해서도 클라우드 서비스 유형별로 구체적인 연구가 계속되어야 할 것이다. 이를 통해 보다 안전하고 신뢰성 있는 클라우드 서비스가

Table 4. Proposal for protection of personal information and user information on cloud service models (CSP : Cloud Service Provider, ISP : Information and communications service Provider)

Scenario	Subject of Information	Personal Information Manager	User Information Manager	Entrustment between ISP and CSP
Cloud service provider(CSP) provides cloud service to end user on IaaS/SaaS	end user	CSP	CSP	-
Information and communications service provider(ISP) provides information and communications service to end user on IaaS	end user	ISP	ISP	-
Information and communications service provider(ISP) provides information and communications service to end user on SaaS	end user	ISP	ISP	O

Table 5. Proposal for amendment of cloud promotion act with regard to the protection of personal information and user information on cloud service models

	Proposal for amendment	Description for amendment
Article 2 (Definitions)	add definition of "user of cloud computing services"	· The term "user of cloud computing services" means "end user" who uses information and communications resources rendered by "provider of cloud computing services" and "provider of information and communications services" who provides information and communications services to "end user" using cloud computing services
Article 2.4	clarify the definition of "user data" by including "personal information"	· The term "user data" means the data which are stored in information and communications resources rendered by "provider of cloud computing services" and which are owned and managed by users of cloud computing services, including "personal information"
Article 27 (Protection of user data)	add provisions about the protection of personal information of end user on cloud service models	· "provider of information and communications services" who provides information and communications services to "end user" using servers, storages and networks rendered by "provider of cloud computing services", is responsible for the protection of personal information of "end user" as "personal information manager" · "provider of information and communications services" who provides information and communications services to "end user" using softwares including applications rendered by "provider of cloud computing services", is responsible for the protection of personal information of "end user" as "personal information manager". In such case, "provider of cloud computing services" is responsible for the entrustment of the personal information of "end user"

제공될 수 있도록 정책적, 기술적인 보완이 지속되어야 하며 최종사용자, 클라우드에서 서비스를 제공하는 정보통신서비스 제공자 및 클라우드 컴퓨팅 서비스 제공자 간의 권한과 의무를 명확하게 규정함으로써, 클라우드 산업 활성화와 이용자 정보 보호라는 클라우드 컴퓨팅 발전법의 목표 달성에 기여할 수 있기를 기대한다.

References

[1] Ministry of Science, ICT and Future Planning, "The National Assembly passed the Cloud Computing Industry Promotion Act", Press Release, Mar. 2015

[2] Gartner, "Cloud Computing", http://blogs.gartner.com/it-glossary/cloud-computing/

[3] James Staten, Simon Tates, and Ben Echols, "TechRadarTM For Infrastructure & Operations Professionals: Cloud Computing, Q3 2009," Forrester, 2009

[4] Peter Mell, and Timothy Grance, "The NIST Definition of Cloud Computing", NIST SP800-144, Sep. 2011

[5] Seungwoo Son, "Legal Issues on Cloud Computing Service & SaaS," Korea Association For Informedia Law, Informedia Law, vol. 14, no. 1, Jun. 2011

[6] Yeun-Dek Chung, "The Legal Study of Protection of Personal Information in Cloud Computing Service," Korea Association For Informedia Law, Informedia Law, vol. 15, no. 3, Feb. 2012

[7] Won-joon Jeong, "Legal Issues for Promotion of Cloud Computing (I) -Issues on the Protection of Personal Information-," ICT & Media Policy, vol. 26, no. 20, Nov. 2014

[8] W. Yu, and J. Lim, "A Study on the Privacy Security Management under the Cloud Computing Service Provider," Journal of The Korea Institute of Information

Security and Cryptology, vol. 22, no. 2, pp. 337-346, Apr. 2012
〔9〕 D. Park, and K. Han, "A Study on PIMS Controls for PII Outsourcing Management under the Cloud Service Environment," Journal of The Korea Institute of Information Security and Cryptology, vol. 23, no 6., pp. 1267-1275, Dec. 2013
〔10〕 Ministry of Science, ICT and Future Planning, "Korea Cloud Initiative," Jan. 2014
〔11〕 Ministry of Science, ICT and Future Planning, "Enactments of decree of the Act on the Development of Cloud Computing and Protection of Users," May. 2015

〈저자소개〉

이 보 성 (Bosung Lee) 정회원
1994년 2월: 서울대학교 항공우주공학과 졸업
1996년 2월: 서울대학교 항공우주공학과 석사
2005년 2월: 서울대학교 항공우주공학과 박사
2015년 1월~현재: 연세대학교 바른ICT연구소 연구원
2015년 5월~현재: 정부통합전산센터 클라우드 기술위원회 자문위원
2015년 9월~현재: 사이버안전훈련센터 겸임교수
〈관심분야〉 클라우드컴퓨팅, 정보보호, 산업보안, 전산유체역학, 병렬처리

김 범 수 (Beomsoo Kim) 종신회원
1999년: 미국 University of Texas at Austin (Ph.D)
1999년~2002년 : 미국 University of Illinois at Chicago, 조교수
2002년~현재: 연세대학교 정보대학원 교수, 부원장
2014년~현재: ISACA Korea(한국정보시스템감사통제협회) 회장
2014년~현재: 연세대학교 바른ICT연구소 소장
〈관심분야〉 정보보호정책 및 제도, 프라이버시 권리, 개인정보 보호, 전자상거래, 정보경제학