FOCUS 1

클라우드 서비스 환경 내 개인정보보호 측면에서의 국내외 동향분석

이승훈*, 이우현**

클라우드 서비스 환경 내 국내외 법제도를 살펴보고 기술동향 및 이슈 분석을 통해 개인정보보호 측면에서의 나아갈 방향을 조망해보고자 한다.

* 한국인터넷진흥원 개인정보기술지원팀 책임연구원(sehlee@kisa.or.kr)
** 한국인터넷진흥원 개인정보기술지원팀 주임연구원(lwhyun@kisa.or.kr)

Ⅰ. 서론

클라우드 시장에 대한 관심이 뜨겁다. 클라우드 컴퓨팅은 주문형(on-demand) 서비스로 IT 자원을 제공하여 비용 절감과 협업의 기회를 도모하고 다양한 장치를 통한 접근성과 유연성 확보가 가능하므로 개인과 기업 등 클라우드 사용자의 호응이 높아지고 있으며, 국가적인 차원에서도 클라우드 산업의 활성화를 위한 노력(예: 2009년 "범정부 클라우드 컴퓨팅 활성화 종합계획" 발표)이 지속적으로 이루어지고 있다.

하지만 최근 애플의 iCloud 해킹으로 해외 유명인사들의 사진이 유출되었고, KT나 LG 유플러스의 클라우드 서비스에서 비밀번호를 5회 이상 틀려도 이용자 확인을 하지 않는 등 보안 문제가 불거지고 있다. 대부분의 기업에서는 클라우드 서비스의 도입 및 확산에 주요 장애요인으로 정보보안 및 개인정보보호 문제를 가장 시급히 해결해야 할 이슈로 인식하고 있다.

이에 ISO/IEC와 ITU-T 등 국제적인 표준기구와 국가별 표준기구 및 관련 산업계에서 클라우드 서비스 보안 및 개인정보보호에 대한 기술과 관리적 대책을 표준화하고 있다. 클라우드 컴퓨팅 보안에 대한 국제표준은 ISO/IEC JTC 1과 ITU-T 등 양대 국제표준기구에서 2010년경부터 개발을 착수하여 2014년 현재까지 작업이 진행 중이다. 클라우드 서비스 보안에 관련된 주요 용어의 정의는 JTC 1/SC 38(분산 어플리케이션 플랫폼 및 서비스)에서 국제표준 ISO/IEC 17788으로 발간하였으며 관련 클라우드 보안 아키텍처, 보안통제, 프라이버시 통제 등에 대한 표준화 작업이 현재 진행 중이다. NIST, ENISA 등 미국 및 유럽에서도 클라우드 보안에 대한 기준, 지침 등이 다수 개발되어 널리 사용되고 있으며, 그 결과에 해당하는 내용이 ISO/IEC와 ITU-T의 국제표준 작업에 반영되고 있다. CSA(Cloud Security Alliance) 등 산업계에서도 보안가이드 3.0, 클라우드 보안통제 3.1 등이 개발되어 많은 기업과 기관에서 참조 모델로서 사용되고 있으며, 그 내용도 국제표준으로 반영되고 있다.

본고에서는 각국의 법제도 현황을 살펴보고 클라우드 취약점에 따른 개인정보보호 방안은 어떤 것이 있는지 정리하고자 한다.

Ⅱ. 각국의 법제도

1. 개요

미국, 유럽 등 클라우드 선진국에서의 개인정보보호 관련 법 제도 현황을 분석하면 "클라우드 보안"이라는 범주 안에서 개인정보보호를 위한 대책을 포함시켜 다루고 있으며, 별도로 구분하여 시행하고 있지 않다.

〈표 1〉 각국의 법제도 현황

	EU	미국	일본	한국
개인정보 보호법 및 클라우드 관련법 동향	• 1998년 10월 EU 개인정보지침 발표 가맹국의 국내법과 조화 • ENISA(유럽정보보안기구) 주도 클라우드 환경의 활성화와 개인정보보호를 포함한 보안에 대한 범유럽적 지침과 규칙 발표	• 기존 여러 개별법의 개정을 통해 클라우드 환경에서 발생할 수 있는 보안 사고로부터 개인정보보호 • 민간 자율규제 원칙 • 클라우드 컴퓨팅법(Cloud Computing Act of 2012) 제안	• 총무성 가스미가세키 프로젝트(Kasumigaseki Project, 2013) 통해 클라우드 컴퓨팅 활성화와 법제도 마련 • 경제 · 산업성 'SaaS용 SLA' 가이드라인을 발표(개인정보 관리 및 취급과 보안 방법을 세분화)	• 국내 기업과 개인의 클라우드 서비스 이용량 증가에 따른 법적 마련은 미진 • 기존의 다양한 개인정보보호 관련법에 존재하는 클라우드 관련 조항 산재
법제도 정비	• EU 데이터 보호 지침 • EU 데이터 온라인 보호 지침 • 전자통신영역에서 개인정보처리 및 프라이버시 보호에 관한 지침	• 공적신용정보법 • 프라이버시법 • 금융프라이버시법 • 전자통신프라이버시법 • 컴퓨터보안법 • 의료프라이버시법	• 고도 정보통신 네트워크 사회 형성 기본법 • 개인정보보호법 • JIS Q 15001(PIM S)	• 개인정보보호법 • 정보통신망법 • 방송통신 이용자보호법 • 클라우드 개인정보보호 수칙

2. EU의 법제도 현황

EU는 연합체의 성격으로 법제도의 성격이 지침이나 규칙이기 때문에 유럽 각 국가에 의무적으로 적용되지는 않는다. 초기 EU의 클라우드 컴퓨팅 환경은 활성화가 중점이었지만 클라우드 환경의 변화와 최근 미국과의 개인정보 이전에 대한 갈등으로 클라우드 환경에서의 개인정보보호에 대한 관심이 높아지고 있다. EU의 클라우드 컴퓨팅은 유럽위원회(EC)와 유럽정보보안기구(ENISA)에서 주도적으로 이끌고 있으며 이들 위원회와 기구에서 클라우드 환경의 활성화와 개인정보보호를 포함한 보안에 대한 범 유럽적 지침과 규칙을 만들어 발표를

하고 있다. EU의 경우 대부분의 클라우드 컴퓨팅 서비스 기업이 미국 기업이라는 것에 중점을 두어 EU 클라우드 컴퓨팅 서비스 기업의 지원과 더불어 SLA의 중요성을 부각시키고 있다. 이와 더불어 클라우드 서비스 이용자들의 개인정보가 해외로 유출되는 것을 막기 위한 해외 클라우드 컴퓨팅 서비스 기업들에 대한 규제도 하고 있다.

3. 미국의 법제도 현황

개인정보에 관련된 문제가 발생하는 경우 각 영역의 개별법에 의해 규제를 받고 있다. 최근 연방정부와 의회 주도로 클라우드 컴퓨팅 관련 법안과 기존 법안들의 개정안들이 제안 및 개정되고 있다. 개별법 측면에서는 개인의 프라이버시 관련 법률들에서 클라우드 환경의 개인정보에 대한 취급 및 보호에 대한 광의적인 내용들을 포함하고 있다.

1) GLB Act(Gramm-Leach Bliley Act, 1999) : 기업들로 하여금 고객정보 보호방법에 대해 설명한 보안계획서를 직접 작성하도록 하여 클라우드 사용자로 하여금 개인정보를 안전하게 보호한다는 것에 대한 신뢰도를 생성 할 수 있도록 하고 있다.

2) 전기통신비밀보호법(ECPA, 2001) : 클라우드 환경에서의 비인가된 접근 및 정보 공개를 원칙적으로 금지함으로서 클라우드 서비스 소비자의 개인 프라이버시를 보장받을 수 있도록 하고 있다.

3) 애국법(USA PATRIOT Act, 2001) : 컴퓨터를 통한 외부자의 공격에 대한 법집행 절차로서 감시와 조사권을 좀 더 폭넓게 인정하여 클라우드 컴퓨팅 서비스를 통한 국가적 개인정보의 유출 등을 방지하기 위한 법으로서의 역할을 하고 있다.

4. 일본의 법제도 현황

미국, EU와 같이 클라우드 컴퓨팅 환경에 직접적인 법제도는 아직 마련이 되어 있지 않지만 총무성을 중심으로 가스미가세키 프로젝트(Kasumigaseki Project, 2013)를 통해 일본만의 클라우드 컴퓨팅 활성화와 법제도를 마련하고 있다. 초기 클라우드 도입시에는 개인정보

보호에 관련된 내용은 대부분 각 분야별 개별법의 개정을 통한 확대적용이 주류였으나 2011년 클라우드 서비스 업체 'First Server'의 초대형 전산장애로 대규모의 개인정보가 유출되고 소실되면서 클라우드 환경에서의 개인정보보호의 중요성이 부각되었다. 이후 일본에서는 총무성을 중심으로 공공기관과 대기업의 클라우드 서비스에 있어서 개인정보 보유 및 관리에 대한 가이드라인을 만들어 배포하고 있다. 개별법적으로 클라우드 컴퓨팅 환경에서 개인정보 보호에 대한 내용을 포함하고 있는 법률들을 각 분야별 정부 기관에서 개정과 가이드라인 발표를 통해 시행하고 있다.

5. 한국의 법제도 현황

한국은 클라우드 도입 초기 다른 국가들과는 달리 정부차원의 클라우드 도입이 미진한 편이다. 하지만 기업들의 클라우드 도입으로 클라우드 서비스 이용자는 증가하였고, 최근 대규모 개인정보 유출로 인해 클라우드 컴퓨팅과 서비스 이용자 보호에 대한 중요성이 부각되고 있다. 클라우드 도입 초기 2011년 7월 방송통신위원회가 '클라우드 개인정보보호 수칙(안)'을 공표하였다. 이 수칙에는 클라우드 컴퓨팅 서비스 이용자들을 보호하기 위한 조치들을 포함하여 SLA의 내용을 포함하였다.

개별법 측면에서는 기존의 개인정보보호를 위해 제정된 법안들의 개정 및 적용범위와 대상의 수정을 통해서 시행되고 있다.

- 개인정보보호법은 개인정보의 수집, 처리 및 보호에 대한 기본적 사항들을 종합적으로 규율하고 있다. 개인정보보호법 이외에 인터넷상의 개인정보를 보호하는 법제도로 정보통신망법과 방송통신위원회의 방송통신 이용자 보호법이 있다.
- 정보통신망법은 1986년 '전산망 보급 확장과 이용촉진에 관한 법률'로 시작되어 2001년 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'로 전부 개정되어 오늘날까지 흐름에 맞추어 개정이 이루어지고 있다. 주요 내용으로는 주기적으로 정보통신서비스 제공자 등이 이용자에게 개인정보 이용내역을 통지하도록 하여 이용자의 알 권리를 보장한다. 그리고 이용자가 자신의 정보에 대한 통제권을 강화하고 있다.
- 방송통신 이용자보호법은 현행 전기통신사업법, 방송법 및 정보통신망법 등에 산재한 이용자 보호 관련 규정을 통합하고, 이용자 역량 강화 및 피해구제제도 개선방안 등을

추진하여 이용자의 피해를 줄이고 권리를 더욱 강화할 방향으로 추진될 예정이다.

종합적으로 한국의 경우 도입 초기 정부차원의 도입이 미진한 결과 국내 기업들과 개인의 클라우드 서비스 이용량은 증가하였지만, 이에 따른 법적 마련은 보완되지 못하는 모습을 보였다. 최근 일련의 대량 개인정보 유출 사태로 범정부적 대대적인 클라우드 컴퓨팅에 대한 규제들이 마련되고 있지만 기존의 다양한 개인정보보호법에 존재하는 클라우드 관련 개인정보에 대한 법제도들이 산재하고 있다.

Ⅲ. 개인정보보호 관련 기술동향

1. 클라우드 프라이버시 중심 설계(PbD)

1) PbD 7원칙과 클라우드 환경에서의 적용 방안

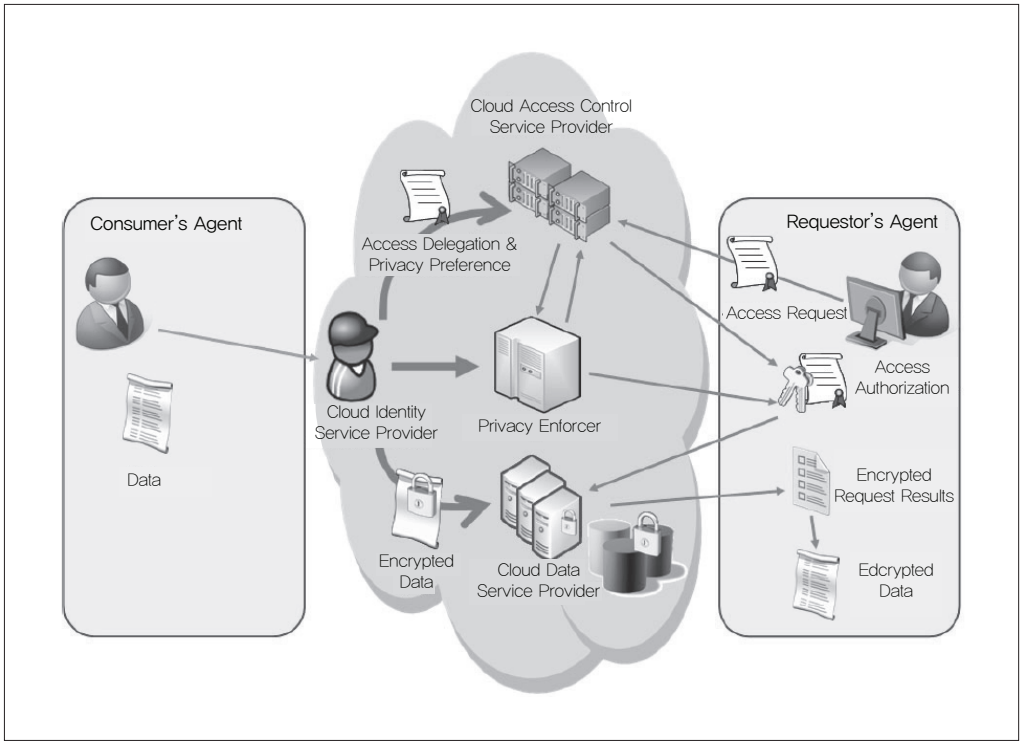
〈표 2〉 프라이버시 중심 설계 7 가지 원칙

원칙	설명
1. 반응적이 아닌 선제적으로; 교정이 아닌 예방으로 (Proactive not reactive; Preventive not remedial)	프라이버시 위험이 실제로 발생하기를 기다리거나 일단 프라이버시 위반이 발생한 이후에 해결하는 교정책을 제공하기 보다는 발생 자체의 방지를 목표로 두어야 한다.
2. 프라이버시 기본 설정 (Privacy as the default)	개인정보는 정보시스템 또는 업무 준칙에 따라 자동적으로 보호됨을 최대한 보장해야 한다. 개인이 자신의 개인정보를 보호하기 위한 별도의 활동이 필요하지 않도록 시스템에 기본적으로 설정되어야 한다.
3. 프라이버시 내장 설계 (Privacy embedded into design)	정보시스템과 업무 준칙의 설계와 아키텍처에 프라이버시가 내장되어야 한다. 따라서 프라이버시는 시스템의 기능을 손상시키지 않고도 핵심적인 역할을 하는 필수 구성요소가 되어야 한다.
4. 완전 기능성 – 제로섬이 아닌 포지티브섬 (Full functionality positive–sum, not zero–sum)	이해상충(trade–off)을 발생시키는 구식의 제로섬 접근법이 아니라 모든 적법한 이해관계와 목표에 이익을 줄 수 있는 "윈윈(win–win)"방식을 추구해야 한다. 즉, 프라이버시 대 보안과 같은 이분법을 피하고 함께 공존하여야 한다.
5. 전체 생명주기 보호 (End–to–end lifecycle protection)	최초 개인정보를 수집할 때부터 시스템에 내장되어 개인정보의 전체 생명주기를 거쳐 안전하게 확장되어야 한다. 최종 프로세스에서 모든 개인정보는 적시에 안전하게 폐기되도록 보장해야 한다.
6. 가시성과 투명성 (Visibility and transparency)	어떤 업무 준칙 또는 기술을 사용하더라도 명시한 약속과 목적에 따라 운영되고 있음을 모든 이해관계자가 독립적인 검증이 가능하여야 한다. 프라이버시의 구성요소와 운영은 사용자와 제공자 모두에게 가시적이고 투명하게 유지되도록 한다.
7. 사용자 프라이버시 존중 (Respect for user privacy)	강력한 프라이버시 기본 설정, 적절한 통지, 사용자 친화적 선택권의 부여 등과 같은 대책을 제공함으로써 개인의 이익을 최대한 보장하는 아키텍처와 운영자를 요구한다.

프라이버시 중심 설계(Privacy by Design; PbD)의 개념은 1990년대에 Ann Cavoukian 박사에 의해 무한히 증가하는 대규모의 네트워크화 된 데이터 시스템에서 발생하는 문제점을 다루기 위해 최초로 제안되었다. 초기에는 PET(Privacy-Enhancing Technology, 프라이버시 강화 기술)이라 불리는 기술적 영역을 중심으로 PbD가 논의되었다가, 현재는 프라이버시 보호를 위한 방법론과 정책까지 그 영역을 확장하고 있다.

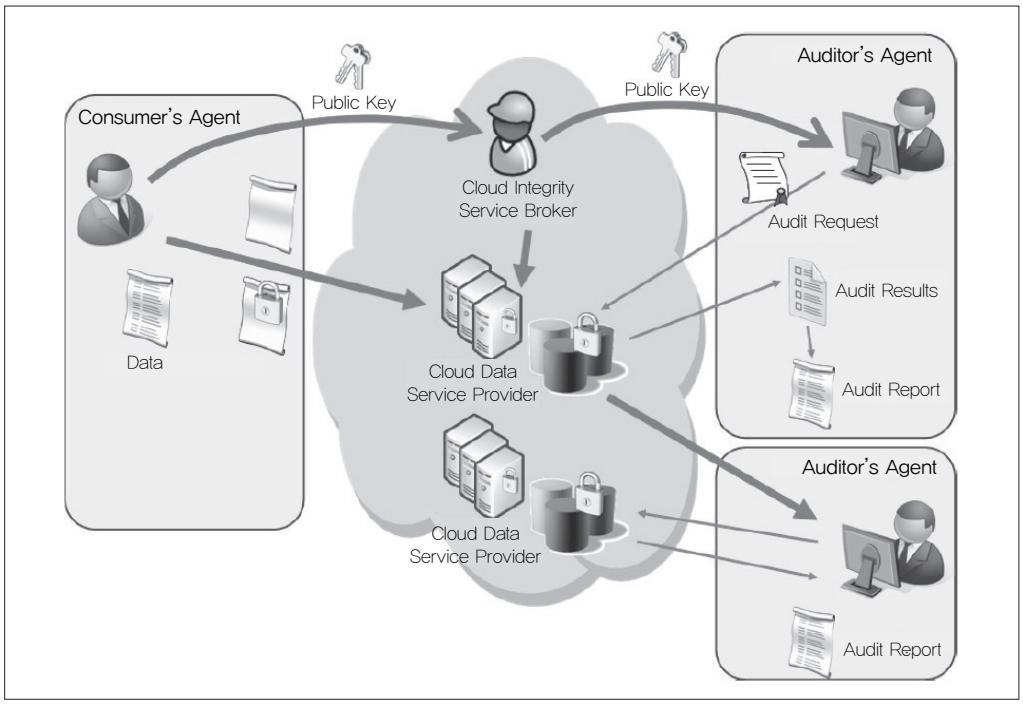
2) 클라우드 환경의 PbD 적용 아키텍처

PbD 원칙을 적용하여 클라우드 환경에서 수집 또는 생성되는 개인정보를 보호하고 적절한 접근을 유지하며 개인정보에 대한 무결성을 보장하기 위하여 가능한 아키텍처는 다음과 같다.



출처: NEC and IPC, "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach", 2010

[그림 1] 프라이버시 보호와 적절한 접근 유지 방안



출처: NEC and IPC, "Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach", 2010

[그림 2] 프라이버시 보호와 무결성 유지 방안

2. 클라우드 프라이버시 강화 기술(PET)

정보주체와 서비스 제공자 간에 사전 합의된 프라이버시 정책에 따라 개인정보의 안전한 처리를 통제하도록 개인을 지원하기 위한 기술이다. 개인정보의 생명주기에 따른 프라이버시 강화 기술을 열거하면 프라이버시 정책 언어, 암호화, 익명화 및 가명화, 매체 폐기 기법을 들 수 있다.

〈표 3〉 클라우드 프라이버시 강화 기술

개인정보 생명주기	OECD 프라이버시 원칙	개인정보보 대책	클라우드 PET 기술
수집 및 생성	수집 제한의 원칙 목적 명확화의 원칙	데이터 최소화	프라이버시 정책언어 (P3P, EPAL 등)
저장	책임의 원칙 안전성 보호의 원칙 정보 정확성의 원칙	기밀성, 무결성 제공	암호화 (Adaptive PM S, 동형 암호화 등)
제공 및 처리	이용 제한의 원칙 개인 참여의 원칙	데이터 접근통제	익명화 및 가명화 (ID 관리시스템)
폐기	공개의 원칙 삭제 권한	기밀성	매체 폐기 기법

Ⅳ. 이슈

1. 클라우드 컴퓨팅 환경에서의 정보보호 관련 이슈

클라우드 컴퓨팅에서 현재 대두되고 있는 몇 가지 근본적 문제점은 다음과 같다.

1) 시스템의 복잡성(system complexity) : 클라우드 컴퓨팅 환경은 다양한 구성요소를 지니고 있어 업그레이드 및 기능 개선에 있어 사용자간 상호작용의 증가에 의한 개인정보에 대한 분실, 무단 사용 · 수정의 위험성을 지닌다.

2) 다중 임차 환경(multi-tenant environment) : 클라우드 서비스는 서비스 제공자와 소비자 그리고 사용자와 사용자간에 다양한 구성 요소 및 자원을 공유하게 된다. 이 때 비인가 정보 공유의 위험성이 존재한다.

3) 인터넷 연결 서비스(Internet-facing services) : 높은 비용과 보안책 구성에 대한 부담으로 사용자의 개인정보가 위험에 노출되는 상황이 증가하고 있다.

4) 통제의 손실(loss of control) : 클라우드 서비스의 발전에 따라 데이터가 기하급수적으로 증가하고 있음. 지속적인 모니터링과 업데이트가 필요

2. 클라우드 컴퓨팅 환경에서의 개인정보보호 관련 이슈

본고에서는 3개 기관(NIST, ENISA, CSA)에서 발표한 보안 및 개인정보보호 이슈를 비교분석하였다.

〈표 4〉 NIST의 클라우드 컴퓨팅 주요 보안 및 개인정보보호 이슈

항목	설명
거버넌스 (Governance)	• 클라우드의 어플리케이션 개발 및 서비스 조항에 적용되는 정책, 절차 및 표준과 관련한 조직적 사례 확장 • 시스템 생명주기에 걸쳐 해당 사례가 지켜지는지 감사 메커니즘 및 도구 마련
준거성 (Compliance)	• 다양한 종류의 법과 규제를 통하여 개인정보보호에 대한 의무를 강요 • 조직의 요구사항 및 계약 조건 만족 여부 확인
신뢰성 (Trust)	• 보안 및 개인정보보호 통제 · 절차의 투명성과 관련한 메커니즘을 클라우드 제공자에 의해 계약에 포함 및 위험 관리 프로그램 설립
아키텍쳐 (Architecture)	• 클라우드 제공자는 서비스를 제공함에 있어 전체 시스템의 생명 주기 및 구성요소와 관련한 보안 및 개인정보보호 통제 기술에 대한 이해
ID 및 접근관리 (Identity & Access Management)	• 인증, 권한부여, ID 및 접근관련 기능을 위한 적절한 보호 장치 확립
소프트웨어 격리 (Software Isolation)	• 클라우드 제공자가 사용하는 가상화 및 기타 소프트웨어 격리 기술에 대한 이해
데이터 보호 (Data Protection)	• 클라우드 제공자의 데이터 관리 솔루션에 대한 적합성 평가
가용성 (Availability)	• 장기적인 분열 및 심각한 재해 발생 시 운영의 즉각적인 복구 방법 확립
사고대응 (Incident Response)	• 사고대응에 대한 계약 조항 및 절차를 이해

〈표 5〉 ENISA 정보보호 및 개인정보보호 위험

항목	설명
거버넌스의 손실 (Loss of Governance)	• 고객은 보안에 영향을 주는 여러 이슈에 대해 제공자를 직접 통제하고자 하지만 SLA만으로 이러한 통제를 보장할 수 없다.
공급자 의존 (Lock-in)	• 클라우드 서비스에 대한 호환성을 보장할 수 있는 도구나 표준이 아직 부족하다.
격리실패 (Isolation Failure)	• 자원을 공유하는 임차인 간에 저장소, 메모리, 네트워크를 분리시키는 메커니즘이 실패할 가능성이 존재한다.
관리 인터페이스 취약성 (Management interface compromise)	• 서비스 제공자의 고객 관리 인터페이스는 원격 접근 및 웹 브라우저를 통한 접근에 취약하다.
데이터 보호 (Data protection)	• 클라우드 고객은 클라우드 제공자의 데이터 처리 방식을 효과적으로 점검하기 어려우므로 부적절한 데이터 처리가 발생하기도 한다.
안전하지 않거나 불완전한 데이터의 삭제 (Insecure or incomplete data deletion)	• 데이터 삭제 요청을 통해 대부분 파기되더라도 다른 추가 복사본이 존재할 수도 있다. • 부적당한 데이터 파기는 개인정보를 재사용할 위험을 발생시킨다.
악의적인 내부자 (Malicious insider)	• 종종 악의적인 내부자에 의한 사고는 훨씬 큰 피해를 줄 수 있다.
고객의 보안 기대치 (Customers'security expectations)	• 고객의 보안 수준에 대한 인식은 제공자가 제공하는 실제 보안 수준과 다를 수 있으며, 제공자는 추가 비용을 줄이기 위해 일부 보안을 포기할 수 있다.
가용성 체인 (Availability Chain)	고객의 단말로부터 인터넷을 통한 접속으로 서비스를 이용하므로 일부 네트워크의 장애로 전체 시스템이 중단될 수 있다.

〈표 6〉 CSA 9가지 클라우드 컴퓨팅 상위 위협

항목	설명
데이터 도난 (Data Breaches)	• 다중 임차인 클라우드 서비스 데이터베이스가 적절하게 설계되지 않은 경우, 하나의 클라이언트의 응용 프로그램에서 하나의 결함은 공격자가 해당 클라이언트의 데이터뿐만 아니라 다른 모든 고객의 데이터를 얻을 수 있다.
데이터의 손실 (Data Loss)	• 악의적인 해커의 공격이나 서비스 제공자의 부주의로 데이터가 삭제될 수 있다. • 화재, 홍수 또는 지진 등의 재해로 데이터가 손실될 수 있다.
서비스 트래픽 하이재킹 (Account or Service Traffic Hijacking)	• 사용자의 자격 증명에 있어 공격자의 접근이 사용자의 활동과 거래를 도청할 수 있는 경우, 데이터를 조작하여 위조된 정보를 반환할 수 있다.
안전하지 않은 인터페이스 및 API (Insecure Interfaces & APIs)	• 클라우드 컴퓨팅의 인터페이스나 API에 제3자가 참여하면서 또 다른 위험성을 증가시킬 수도 있다.
서비스 거부 (Denial of Service)	• 클라우드 특징 중 하나인 가용성으로 인해 과도한 비용이 발생하여 소비자가 서비스 거부를 당할 수 있다.
악의적인 내부자 (Malicious Insiders)	• 비즈니스 파트너나 내부자가 데이터를 공격할 수 있는 악의적인 내부자일 수 있다.
클라우드 서비스의 남용 (Abuse of Cloud Services)	• 클라우드의 남용은 악성코드나 불법 소프트웨어의 공유를 통해 악의적인 공격자를 양산할 수 있다.
적정 주의의무의 부족 (Insufficient Due Diligence)	• 클라우드 환경, 서비스, 운영 책임에 대한 충분한 이해가 부족하면 적정 수준의 위험을 관리하기 어렵게 된다.
공유 기술의 취약점 (Shared Technology Vulnerabilities)	• 제3자와의 기술 공유를 통해 클라우드 제공자의 인프라와 플랫폼에서 효율적으로 서비스를 제공할 수 있지만 새로운 위협과 취약점을 발생시킨다.

3개 기관의 위험요인 분석을 요약하면 NIST의 경우, 클라우드 컴퓨팅 전반에 걸쳐 위험에 대해 분석을 하고 있다. 클라우드 환경상의 사용자 개인정보보호에 대한 기술적 위험을 중점적으로 다루기보다는 전체적인 큰 틀에서의 책임성, 컴플라이언스, 신뢰구조, 아키텍처 등 거버넌스 차원에서의 위험들을 제시한 점이 특징이다. ENISA에서도 기술적인 측면보다는 서비스 제공자와 사용자간의 개인정보보호 이슈들을 중점적으로 다루고 있다. 따라서 SLA를 통해 클라우드 환경에서 서비스 제공자와 사용자간에 사용자의 개인정보를 어떻게 관리하고 보호할 것인지에 대해 언급하고 있다. 그리고 ENISA의 또 다른 특징은 개인정보를 보호하는데 있어서 단순히 제공자만의 책임보다는 사용자도 제공자와 함께 책임감을 가져야 한다는 점을 강조하면서 불완전하고 안전성이 보장되지 않는 데이터 파기의 위험성을 지적하고 있다. CSA의 경우에는 클라우드 컴퓨팅의 위험을 서비스 트래픽 하이재킹, 안전하지 않은 인터페이스 및 API와 같은 시스템과 네트워크 요소들이 포함된 기술적인 측면을 강조하고 있으며 최종적으로는 사용자의 개인정보에 피해를 입을 수 있다는 점을 설명하고 있다.

또한 데이터의 도난과 손실을 언급하면서 개인의 데이터를 관리 운영하는데 있어서 여러 가지 위험상황에 대한 보호적 차원의 방안들을 강구할 필요성을 강조하고 있다. 앞의 위험들은 전반적으로 개인정보보호에 대해서 직접적인 언급은 하고 있지 않지만 기술적 측면이나 관리적인 측면에서의 접근을 통해 개인정보를 보호하고 있다. 클라우드 초기에는 기술적인 측면이 강조되었지만, 기술이 발전하고 이에 따라 위험도 보다 함께 변화하면서 제공자뿐만 아니라 사용자도 책임이 있다는 점이 주목할 점이라 할 수 있다.

Ⅴ. 시사점

클라우드 서비스는 빅데이터와 더불어 차세대 유망 분야중 하나이다. 하지만 보안 문제와 사생활 침해 우려로 인해 도입이 지연되고 있다. 본 고에서는 각국의 법제도 현황을 살펴보았는데 종합적으로 현재의 전 세계의 클라우드 컴퓨팅 환경을 직접적으로 관리 및 규제를 하는 법제도는 없거나 마련 중에 있다. 이는 클라우드 도입 초기에 각국의 클라우드 컴퓨팅 정책이 개인정보보호가 아닌 활성화에 치중한 것에 기인했다고 볼 수 있을 것이다. 현재 각국 법제도의 화두는 개인정보의 관리와 해외 이전을 들 수 있다. 클라우드 컴퓨팅 서비스를 제공자의 대부분이 미국기업인 점을 감안하면 앞으로의 각국의 클라우드 법제도의 쟁점은 개인정보의 해외유출을 어떻게 방어하고 예방할 것인지가 될 것이다. 그렇기 때문에 각국에서 클라우드 컴퓨팅에 대한 법제도의 준비를 서두르고 개인정보를 어떻게 관리하고 보호 할 것인지가 중심을 이루고 있는 실정이다. 국내의 경우 정부차원의 클라우드 환경에서의 개인정보보호 관련 법안(클라우드 컴퓨팅 발전 및 이용자 보호에 관한 법률)이 제안되었지만 안전성이 떨어진다는 이유로 늦춰지고 있다. 내용을 살펴보면 개인정보 보호보다는 진흥에 치우쳐 있다는 느낌이 강하다. 이는 개인정보 보호에 치중하는 해외의 흐름과 비교해 볼 때 상당히 뒤쳐져 있는 모습이다. 방송통신위원회의 클라우드 SLA 도 마찬가지다. 가용성 중심으로 서비스의 품질 · 백업과 관련된 내용 위주로 구성되어 있어 개인정보 보호 관련 내용은 부족한 수준이다. 클라우드 컴퓨팅 관련 보안 문제가 계속 불거지는 만큼 사용자들이 안심하고 클라우드 서비스를 이용할 수 있는 환경 조성 마련이 필요하다. 정부의 내실있는 클라우드 정책이 필요한 때이다.

참고문헌

국립전파연구원 (2013). “클라우드 서비스 환경에서 개인정보보호 프레임워크 및 요구사항”, 방송통신표준.

국립전파연구원 (2013). “클라우드 서비스 환경에서 정보보호 프레임워크 및 요구사항”, 방송통신표준.

금융보안연구원 (2010). “금융부문 클라우드컴퓨팅 보안 가이드”

박대하 · 한근희 (2013). “클라우드 서비스 환경의 개인정보 위탁을 위한 개인정보보호 관리체계 통제 연구”, 정보보호학회 논문지.

박대하 · 백태석 (2011). “클라우드 컴퓨팅 개인정보보호 연구동향과 과제”, 정보보호학회지.

박대하 · 백태석 (2011). “클라우드 컴퓨팅 개인정보보호 연구동향과 과제”

방송통신위원회 (2011). “클라우드 서비스 제공자 개인정보보호 수칙”

방송통신위원회 (2011). “클라우드서비스를 위한 SLA 가이드”

선재훈 (2010). “Cloud Computing의 개인 정보 보안을 위한 취약점 분석”, 한국융합보안학회 정보보안논문지.

송석현 (2012). “클라우드 컴퓨팅 SLA에 대한 고려사항”, TTA Journal.

안전행정부 고시 (2011). “개인정보의 안전성 확보조치 기준”

안전행정부 (2014). “개인정보보호 실태점검단 교육자료”

유우영 · 임종인 (2012). “클라우드 컴퓨팅 서비스 제공자의 개인정보보호 조치 방안에 대한 연구”, 정보보호학회 논문지.

이상동 (2010). “K-클라우드 서비스,” 정보과학회지.

정현철 (2011). “클라우드 서비스 보안 위협 및 보안대책”, The Clouds 2011.

KISA (2011). “클라우드 서비스 정보보호 안내서”

NIA (2013). “2013년 상반기 개인정보보호 해외 법제 동향”

Cloud Standards Customer Council (2012). “Practical Guide to Cloud Service Level Agreements Version 1.0”

C. Barnatt (2010). “A brief guide to cloud computing,” Constable & Robinson, pp. 22-28.

Cognizant (2012). “Understanding Cloud Security Challenges”

CSA (2013). “The Notorious Nine Cloud Computing Top Threats in 2013”

CSA (2010). “Top Threats to Cloud Computing V1.0”.

CSA Privacy Level Agreement Working Group (2013). “Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union”.

ENISA (2009). “Cloud Computing – Benefits, risks and recommendations for information security”.

Gartner (2011). “Cloud computing ranks as the top concern of CIO’s agendas for 2011,”

ISACA (2009). “Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives”

ISO/IEC 1st CD 27017 (2014). "Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002"

ISO/IEC 4th WD 27017 (2012). "Code of practice for information security controls for cloud computing services based on ISO/IEC 27002"

ISO/IEC DIS 27018 (2014). "Code of practice for PII protection in public clouds acting as PII processors"

ITU-T (2012). "Privacy in Cloud Computing", ITU Workshop on Cloud Computing.

ITU-T (2012). "Privacy in Cloud Computing", Technology Watch Report.

JIS Q 15001 (2006). "Personal information protection management systems - Requirements"

Nakao Koji (2011). "The art of information security technology for introducing cloud," Network Security Forum 2011.

New Zealand Government (2014). "Cloud Computing - Information Security and Privacy Considerations"

NIST SP 800-122 (2010). "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"

NIST SP 800-144 (2011). "Guidelines on Security and Privacy in Public Cloud Computing"

NIST SP 800-144 (2011). "Guidelines on Security and Privacy in Public Cloud Computing"

PISA Consortium (2003). "Handbook of Privacy and Privacy-Enhancing Technologies"