情 報 保 護 學 會 誌
第21卷 第5號, 2011. 8

# 클라우드 컴퓨팅 개인정보보호 연구동향과 과제

박 대 하*, 백 태 석**

요 약

최근 들어 클라우드 컴퓨팅의 도입에 있어 보안 및 개인정보보호가 핵심적인 요구사항으로 주목받고 있으며, 국내외 여러 조직에서는 클라우드 컴퓨팅 환경에서의 개인정보보호의 중요성을 인식하여 전사적이고 체계적인 접근법에 기초한 연구가 진행되고 있다. 본 논문에서는 클라우드 컴퓨팅의 보안을 다룬 NIST SP 800-144 문서를 기반으로 정보보호관리체계(ISMS)에 대한 국제표준인 ISO 27002의 통제내용을 분석하고 이를 KISA-PIMS의 통제내용과 연결하여 도출하였다. 더불어, IPC 및 WPF 등 해외에서 연구한 클라우드 컴퓨팅 개인정보보호 위협 및 요구사항을 KISA-PIMS의 통제목적과 비교·분석하는 한편, 클라우드 컴퓨팅 개인정보보호의 향후 연구 과제를 제시하고자 한다.

## Ⅰ. 서 론

클라우드 컴퓨팅은 다른 물리적인 위치에 존재하는 컴퓨팅 자원을 가상화 기술로 통합해 제공하는 기술을 말한다. 곧 개인용 컴퓨터나 기업 서버에 개별적으로 저장해 둔 프로그램이나 문서를 인터넷으로 접속할 수 있는 대형 컴퓨터는 물론이고, 다양한 작업을 할 수 있는 이용자 중심의 컴퓨터 환경이다[1]. 클라우드 컴퓨팅은 비용이 적게 들고, 협업의 기회를 제공하며, 어떤 장치를 통해서도 접근할 수 있고, 고정비용이 들지 않으며, 보다 많은 유연성을 제공함과 동시에 에너지 절감 및 차세대 어플리케이션 구동이 가능하다[2]. 이는 개인과 기업에게 상당한 이점이며 다른 신규 기술보다 더욱 혁신적이고 효과적일 수 있다.

하지만 이런 신규 기술에 대한 장점에 치중한 나머지 잠재적 위험에 대한 연구 및 고찰이 심층적으로 이루어지지 않고 있다. 미국의 보안 컨설팅 업체 포네몬(Ponemon)이 2010년 미국 및 유럽 6개국의 127개 사업자를 대상으로 클라우드 서비스 보안 인식에 대한 설문 조사를 실시한 결과에 따르면, 미국은 73%, 유럽은 74%의 사업자가 클라우드 자원 보호를 위한 별도의 보안을 적용하지 않고 있는 것으로 들어났다. 다른 유사 조사에서도 이와 같은 우려들이 제기되어 왔으며, 다수의 개인사용자들 역시 클라우드에 저장되는 개인정보가 남용될 수 있다는 부분에 대해 가장 많이 염려하고 있다[1][3]. 또한, 2011년 Gartner CIO 조사 결과에 따르면, 기업 CIO들은 클라우드 컴퓨팅 환경에서 보안 및 개인정보보호에 대해 가장 관심을 가지고 있었다[4].

이와 같이 클라우드 환경에서의 보안 및 개인정보보호는 서비스의 성패를 가르는 매우 중요한 내부통제로 간주되고 있으며, ISO/IEC, NIST, Gartner, ENISA 등에서도 해외에서도 활발한 조사 및 연구가 진행되고 있다. 이러한 선행연구를 통해 제시된 개인정보보호 요구사항을 각 클라우드 환경에 맞게 적절히 구현할 경우 보다 안전하게 클라우드 컴퓨팅의 산업적 확장성을 강화하고 활용성을 높임으로써 이용자의 서비스 확대 및 자원의 효율적인 활용이 가능할 것이다[5].

본 논문에서는 주요 기관 및 조직에서 연구 중인 클라우드 컴퓨팅 개인정보보호 관련 이슈 및 요구사항을 각각 연구하는 한편, 한국인터넷진흥원(KISA)의 개인정보보호관리체계(PIMS)에서 통제항목으로 주어진 개인정보보호 요구사항과의 비교·분석을 통해 향후 연구과제를 제시하고자 한다.

## Ⅱ. 클라우드 컴퓨팅 보안 및 개인정보보호

### 2.1 클라우드 컴퓨팅 보안

클라우드 환경에서의 보안은 일반적인 정보보호의

* 고려사이버대학교 정보관리보안학과(summer69@cyberkorea.ac.kr)
** 중앙대학교 일반대학원 정보시스템학과(yoo sj99@nate.com)

요구사항을 포함함과 동시에 클라우드 환경에 적합한 추가적인 요구사항을 필요로 한다. 본 논문은 클라우드 컴퓨팅 보안 및 개인정보보호 분석을 위하여 NIST SP 800-144 문서를 선정하였으며 해당 문서에 기술된 요구사항을 ISO/IEC 27002 표준 문서의 통제사항과 비교·분석하여 관련 항목을 도출하였다.

최근 NIST(미국표준기술연구소)는 2011년 1월 'NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing', 과 'NIST SP 800-145 The NIST Definition of Cloud Computing'란 이름의 표준 문서를 발간하였으며, 2011년 5월 'NIST SP 800-146 Cloud Computing Synopsis and Recommendations'를 작성하는 등 클라우드 컴퓨팅 보안 표준 연구를 활발히 진행하고 있다[6][7][8].

〔표 1〕 NIST 클라우드 컴퓨팅 주요 보안 및 개인정보보호 이슈

| |
|---|
| 1. 거버넌스(Governance) |
| 클라우드의 어플리케이션 개발 및 서비스 조항에 적용되는 정책, 절차 및 표준과 관련한 조직적 사례 확장<br>시스템 생명주기에 걸쳐 해당 사례가 지켜지는지 감사 메커니즘 및 도구 마련 |
| 2. 준거성(Compliance) |
| 다양한 종류의 법과 규제를 통하여 개인정보보호에 대한 의무를 강요<br>조직의 요구사항 및 계약 조건 만족 여부 확인 |
| 3. 신뢰성(Trust) |
| 보안 및 개인정보보호 통제·절차의 투명성과 관련한 메커니즘을 클라우드 제공자에 의해 계약에 포함 및 위험 관리 프로그램 설립 |
| 4. 아키텍처(Architecture) |
| 클라우드 제공자는 서비스를 제공함에 있어 전체 시스템의 생명 주기 및 구성요소와 관련한 보안 및 개인정보보호 통제 기술에 대한 이해 |
| 5. ID 및 접근관리(Identity and Access Management) |
| 인증, 권한부여, ID 및 접근관련 기능을 위한 적절한 보호 장치 확립 |
| 6. 소프트웨어 격리(Software Isolation) |
| 클라우드 제공자가 사용하는 가상화 및 기타 소프트웨어 격리 기술에 대한 이해 |
| 7. 데이터 보호(Data Protection) |
| 클라우드 제공자의 데이터 관리 솔루션에 대한 적합성 평가 |
| 8. 가용성(Availability) |
| 장기적인 분열 및 심각한 재해 발생 시 운영의 즉각적인 복구 방법 확립 |
| 9. 사고 대응(Incident Response) |
| 사고대응에 대한 계약 조항 및 절차를 이해 |

이 중 NIST SP 800-144에서는 공공 클라우드 서비스의 계획, 검토, 협상 및 착수와 관련하여 고려하여야 할 보안 및 개인정보보호 방안에 대해 명시하였으며 각각의 내용은 [표 1]과 같다[6].

본 표준은 공공 클라우드 컴퓨팅과 그와 관련된 보안 및 개인정보보호 과제 해결을 위한 개요를 제공하는 것이 주된 목적이다. 특히, 클라우드 서비스 제공자의 주요 고려사항과 더불어 공공 클라우드 아웃소싱과 관련한 가이드라인을 제공하고 있다. 클라우드 컴퓨팅 보안과 개인정보보호를 유사한 이슈로 이해하고 있고 클라우드 아웃소싱 과정을 위험 및 시스템 생명주기 관리 측면에서의 문제 해결을 제안하고 있는 것이 특징이며, 개인정보보호와 직접적인 연관성은 부족하지만 추후 연구 과제를 도출해 내기 위한 기반으로 사용할 수 있다.

### 2.2 클라우드 환경에서의 개인정보보호의 개념 및 정의

클라우드 환경에서의 개인정보보호 연구를 수행하기에 앞서 조직 및 개인의 개인정보에 대한 정확한 범위 및 개념을 정의하는 것이 선행되어야 한다.

국외 문서에서 가장 많이 쓰이는 프라이버시(privacy)는 매우 넓은 의미로 사용되고 있다. OECD Privacy Guidelines에서는 '사용자의 개인 정보(personal information)의 사용 및 접근에 대한 이해를 보장하는 것'이라 명시하고 있으며 이는 개인 정보에 대한 침해 보장을 중점으로 하고 있다[9]. 한편, 본 논문에서 언급하고 있는 개인정보보호란 프라이버시의 개념을 광의적으로 해석하였으며, 정보의 공적·사적 성격을 불문하고 개인에 관련되는 모든 정보의 일체를 의미하고 있다[10]. 또한 정보의 주체는 단순히 개인뿐만 아니라 비즈니스 및 정부 기관 등 조직 차원으로의 확대하여 해석하고 있다.

그러므로 클라우드 환경에서 존재하는 개인정보란 클라우드 서비스 산업의 제공자 및 이용자와 관련한 모든 정보를 의미하고, 클라우드 컴퓨팅 서비스에 업로드 되는 정보뿐만 아니라, 수집, 저장, 처리 및 가공 등을 통해 새롭게 발생하는 모든 정보를 포함한다고 할 수 있다. 이에 따라 클라우드 환경 특성상 해당 정보의 주체 및 소유권에 따라 개인정보보호의 범위 및 대상이 상이할 수 있기 때문에 서비스 계약 조건 등 관련 법규·정책 등에 의한 합리적인 통제가 점차 중요해 지고 있다.

### 2.3 클라우드 환경에서의 개인정보보호의 중요성 및 문제점

클라우드 컴퓨팅과 같은 정보통신 기술의 발전에 따라 정보의 수집, 저장, 유통이 손쉬워지고, 상업적인 서비스는 물론이고 공공행정이나 교육 등 다방면에 걸쳐 정보주체의 개인정보 수집 및 활용이 용이해짐에 따라 그에 대한 보호조치 및 정보주체의 권리보장이 요구되고 있다.

현재 국내외 기업과 공공기관에서는 다양한 개인정보를 획득하고 관리하며 이용함으로써 조직 본연의 역할을 수행하고 있다. 조직이 가지고 있는 정보를 보호하는 것은 현대와 같이 인터넷에 기반을 둔 정보시스템을 운영하는 대부분의 기업에서 더욱 중요한 문제가 되고 있으며, 특히 클라우드 환경에서는 조직의 개인정보 보유량 및 위탁 관리의 증가 등으로 인해 개인정보보호의 중요성이 증대되고 있다. 이러한 정보들 중에는 외부에 공개되는 경우 심각한 피해가 발생하는 정보들이 있으며, 또한 정보의 파손은 개인의 피해와 더불어 해당 조직의 업무를 정상적으로 수행할 수 없게 만든다.

또한, 클라우드 서비스 과정에서 더 나은 서비스 제공 및 개발을 위해 수집되는 이용자 개인정보는 이러한 순기능에 집중한 나머지 이용자의 개인정보 자기결정권을 침해하게 되는 경우가 발생할 수 있다. 이는 재산권, 교육권, 사회보장수급권 등과 같은 기본권의 침해로 이어질 수 있으며, 클라우드 서비스 제공자 측면에서도 이에 해당하는 서비스의 목적 자체를 저해하는 요소로 발전될 수 있다.

이와 더불어 클라우드 서비스 특성상 서비스 제공자와 사용자간의 미흡한 커뮤니케이션, 제공자의 부주의성, 사용자의 무관심 등 이해관계자의 정보보호에 대한 인식이 부족한 것이 현재 실정이다. 심지어 일부 기업은 자사에서 클라우드 솔루션을 이용하고 있는지도 알지 못하는 경우도 있어 IT 자원 제공자 및 사용자에 대한 책임성 및 인식 재고의 필요성이 증대되고 있다.

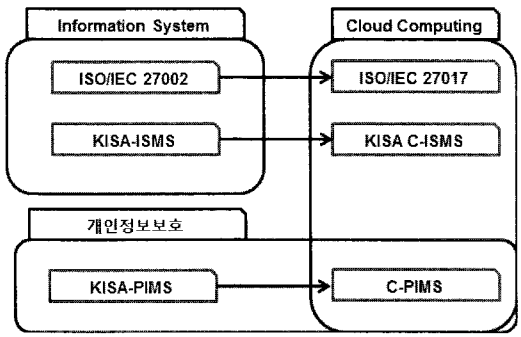
하지만 현재 클라우드 컴퓨팅은 다방면에서 보완 되고 발전되고 있으며, 이러한 잠재적 위험 요인을 충분히 상쇄시킬 수 있는 장점들을 보유하고 있다. 최근 들어 클라우드 환경에서의 보안 및 개인정보보호에 대하여 여러 조직에서 심층적인 연구를 진행하고 있으며, 특히 클라우드 환경에서의 개인정보의 중요성을 인식하고 이에 대한 전사적이고 체계적인 접근법에 대한 연구가 진행되고 있다.

## III. 주요 연구 동향 및 분석

국내외 클라우드 컴퓨팅 및 개인정보보호에 대한 표준과 평가제도에 대한 활발한 연구가 진행되고 있다. 본 장에서는 본 논문의 연구 방법 및 개요에 대해 설명하는 한편, 이와 관련한 연구 동향을 살펴보고 각각을 KISA-PIMS와 비교·분석하여 관련 통제사항을 도출하고자 한다.

### 3.1 연구 및 분석 개요

현재 ISO/IEC SC27에서는 정보보호관리체계(ISMS)에 대한 국제표준 문서인 ISO/IEC 27002를 NIST SP 800-144의 요구사항과 비교 및 분석하여 클라우드 환경에 적합한 ISMS 통제 내용을 포함한 ISO/IEC 27017의 개발이 제안되어 있다[11]. 이와 유사하게 KISA에서도 클라우드 환경을 고려한 ISMS에 대한 연구를 2010년부터 진행하는 한편, KISA-ISMS를 기반으로 새롭게 제정된 '개인정보보호법과 정보통신망 이용촉진 및 정보보호 등에 관한 법률'(정보통신망법)을 적용하여 KISA-PIMS를 개발하였다[12].




〔그림 1〕 주요 연구 동향 및 개요

하지만 KISA-PIMS의 경우 기관 및 기업과 같은 조직이 대상이 되는 반면, 사용자 조직에 초점이 맞춰진 클라우드 컴퓨팅 개인정보보호 요구사항을 완벽히 만족하지 못하고 있다. 이에 따라 본 논문에서는 KISA- PIMS가 개발된 방법과 마찬가지로 클라우드 환경을 고려한 PIMS를 편의상 C-PIMS로 명명하고, ISO/IEC 27002의 클라우드 컴퓨팅 개인정보보호 관련 항목 도출, 국외 클

라우드 컴퓨팅 개인정보보호 이슈 및 요구사항과 KISA-PIMS와의 비교·분석 등의 세부 목표를 달성하고 그에 따른 추후 연구 과제를 제시하고자 한다([그림 1] 참고).

### 3.2 C-PIMS의 통제내용 도출

ISO/IEC 27017은 앞서 소개한 NIST SP 800-144에서 언급한 클라우드 컴퓨팅 보안 및 개인정보보호 요구사항을 기반으로 하여 ISO/IEC 27002의 통제내용을 클라우드 환경에 적합하게 변경·추가·삭제하였으며, 본 장에서는 이를 바탕으로 ISO/IEC 27017에서 제안한 내용 중 개인정보보호 관련 사항을 선정하고 이를 KISA-PIMS와 비교·분석하였다.

KISA-PIMS의 통제 영역과 통제 분야를 기준으로 ISO/IEC 27017의 제안 내용을 반영한 C-PIMS의 주요 통제내용은 [표 2]와 같다.

### 3.3 클라우드 컴퓨팅 개인정보보호 요구사항 vs KISA-PIMS

본 장에서는 클라우드 환경에서의 개인정보보호에 대한 선진 연구 사례를 살펴보고 핵심 개인정보보호 이슈 및 문서별 특징에 대해 기술하는 한편, KISA-PIMS와의 비교·분석을 통하여 관련 통제목적을 선정하였다.

#### 3.3.1 Privacy by Design

캐나다 온타리오의 IPC(정보 및 프라이버시 위원회 사무국)는 90년대 중반부터 개인정보보호와 관련된 연구를 시작하였다. 조직이 수집·사용·폐기하는 개인정

〔표 2〕 C-PIMS 통제내용

| 영역 | 도메인 | C-PIMS 통제내용 |
|---|---|---|
| 개인정보보호 대책요구사항 | 1. 개인정보보호정책 | • 개인정보정책에 클라우드 컴퓨팅 서비스의 사용을 적용하기 위한 지침, 표준, 절차의 수립 |
| | 2. 개인정보보호조직 | • 클라우드 서비스를 사용하여 개인정보를 처리하는 내부 부서의 책임자 및 담당자 지정 |
| | 3. 개인정보 분류 | • 클라우드 서비스 명칭과 서비스 제공자를 식별하여 사용자 조직의 자산목록으로 문서화<br>• 개인정보 관리 자산 분류 기준에 클라우드 서비스에 대한 기준 포함<br>• 클라우드 서비스를 거치는 개인정보 흐름의 분석 |
| | 4. 교육 및 훈련 | • 클라우드 서비스의 사용 규정, 관리적 및 기술적 보호대책에 대해 개인정보취급자가 필수적으로 알아야 하는 사항을 교육에 포함 |
| | 5. 인적보안 | • 클라우드 서비스를 사용하는 개인정보취급자의 최소한으로 제한 |
| | 6. 침해사고 처리 및 대응 | • 클라우드 서비스 제공자의 관제 시스템을 이용한 개인정보 사고의 모니터링<br>• 클라우드 서비스 제공자와 개인정보 사고에 대한 보고채널 유지<br>• 클라우드 서비스에서 발생하는 개인정보 사고에 대한 처리 및 복구절차 개발 |
| | 7. 내부검토 및 감사 | • 클라우드 서비스의 개인정보보호에 대한 법적 요구사항 정의<br>• 클라우드 서비스에 대한 접속 기록의 보존, 검토 및 감사 |
| | 8. 기술적 보호조치 | • 클라우드 서비스의 개인정보취급자 권한 관리<br>• 클라우드 서비스 제공자의 개인정보 접근 제한<br>• 클라우드 서비스의 데이터베이스에 저장된 개인정보 암호화<br>• 클라우드 서비스의 변경에 따른 개인정보 영향평가 |
| | 9. 물리적 보호조치 | • 클라우드 서비스 제공자의 개인정보 처리시설에 대한 물리적 보호구역 지정 및 물리적 접근통제 |
| 생명주기 준거요구사항 | 1. 개인정보수집에 따른 조치 | • 클라우드 서비스의 이용자가 개인정보보호취급방침을 쉽게 확인할 수 있도록 공개 |
| | 2. 개인정보 이용 및 제공에 따른 조치 | • 클라우드 서비스의 이용자가 개인정보의 열람 또는 이용 및 제공내역을 요구할 수 있는 방법 |
| | 3. 개인정보 관리 및 파기에 따른 조치 | • 파기 요청 시 클라우드 서비스에 저장된 개인정보를 복구할 수 없도록 파기하는 방법 |

보에 대한 중요성 및 적절한 개인정보보호 통제 사례를 통한 가치 창출에 대한 내용을 필두로 'Privacy by Design(PbD)'이란 개념을 지지하고 나섰다. 2010년 8월 'ISO/IEC JTC 1/SC 27 Information technology - Security techniques'에서는 'Reaching for the Cloud'와 'Modelling Cloud Computing Architecture without Compromising Privacy'란 이름의 문서를 발행하였는데 두 문서는 모두 IPC에서 작성되었다[13][14].

PbD의 주요 내용은 아래의 7가지 원칙을 기반으로 하고 있으며 각각의 내용은 [표 3]과 같다[15]. 이와 더불어 PbD에서는 클라우드 환경에서의 개인정보보호 위험에 대해 [표 4]와 같이 기술하고 있다[13].

IPC에서 발행하는 문서의 경우 모든 문서가 PbD의 원칙을 따르고 있으며, 클라우드 서비스의 개발을 위한

〔표 3〕 PbD 프라이버시 7 원칙

| |
|---|
| P1. 대응적이 아니라 선행적으로(Proactive not Reactive; Preventative not Remedial) |
| 개인정보보호 침해사건은 선행적으로 예방하는 형태로 이루어져야 함 |
| P2. 프라이버시 기본 설정(Privacy as the Default) |
| 개인정보는 어떠한 IT 시스템이나 실무에서도 기본적으로 보호되어야 하며 적절한 제한이 유지되어야 함 |
| P3. 설계에 내재한 프라이버시(Privacy Embedded into Design) |
| 설계 및 IT 시스템 등에 직접적으로 반영되어야 하며 핵심 기능이 전달되기 위한 필수요소로 여겨져야 함 |
| P4. 기능의 완전성(Full functionality-Positive-Sum, not Zero-Sum) |
| 모든 법적 요구사항을 수용함과 동시에 win-win방식으로 이루어져야 하며, 클라우드 서비스의 기능과 개인정보보호 통제 모두 최대화를 통해 기술적인 잠재력을 이끌어낼 수 있어야 함 |
| P5. 종단 간 생명주기 보호(End-to-End Lifecycle Protection) |
| 개인정보의 생명주기 전체에 걸쳐 관리가 이루어져야 하며, 접속·업로드·수정 및 통제에 대한 역량을 제공할 수 있어야 함 |
| P6. 가시성과 투명성(Visibility and Transparency) |
| 모든 이해관계자들에게 기술된 규정 및 목적에 따라 운영하여야 하며, 모든 시스템 및 환경에 대한 명확한 설명이 존재하여야 함 |
| P7. 사용자 프라이버시 존중(Respect for User Privacy) |
| 서비스 제공자는 개인정보보호에 대한 사용자의 흥미를 유지해야함과 동시에 사용자 중심의 아키텍처 설계가 요구됨 |

※ P = Principle

〔표 4〕 PbD 클라우드 컴퓨팅 개인정보보호 위험

| |
|---|
| RA1. 사법권(Jurisdiction) |
| 국가별 데이터 보호와 관련한 법과 접근법이 상이하므로 다중의 사법권에 포함될 수 있으며 이에 대한 증재가 요구됨 |
| RA2. 새로운 데이터흐름의 생성(Creation of New Data-streams) |
| 클라우드 모델은 방대한 규모의 새로운 데이터를 생성하고, 이는 정보 중계자 및 제공자에게 노출될 수 있으며, 본래의 목적을 넘어서 사용될 수 있음 |
| RA3. 보안(Security) |
| 클라우드 서비스 제공자는 데이터와 흐름을 보호하기 위하여 현재 온라인 뱅킹이나 소매업에서 사용되는 암호화 기법을 사용해야하나 대부분이 그렇지 못함 |
| RA4. 데이터 침해(Data Intrusion) |
| 클라우드 서비스 제공자, 정부 및 관련 기관에 의한 사용자 데이터의 접속 및 활용 등이 가능할 수 있으며, 사용자는 이러한 침해에 대해 인지하지 못하는 경우가 발생할 수 있음 |
| RA5. 합법적인 접근(Lawful Access) |
| 합법적인 접근 자체로는 문제가 없지만 해당 목적을 넘어선 접근이 이루어 질 수 있으며, 이해 대해 인지하지 못할 수 있음 |
| RA6. 처리(Processing) |
| 처리를 아웃소싱 하는 경우, 사용자는 데이터에 대한 통제권자로서 접속·수정·삭제 절차가 적절하고 적합함을 보장하여야 함 |
| RA7. 처리 데이터의 오용(Misuse of Processing Data) |
| 클라우드 제공자가 처리자로서 처리하는 활동과 처리 이외의 활동으로 구분하여 접속을 제한·관리하여야 함 |
| RA8. 데이터 영속성(Permanence of Data) |
| 계약이 완료된 후에 데이터는 클라우드 인프라에서 영구적으로 제거되고 언제 제거가 완료되는지 확인하여야 함 |
| RA9. 데이터 소유권(Ownership of Data) |
| 새로운 데이터흐름을 통해 생성된 데이터의 소유권은 불확실해 질 수 있으며, 해당 데이터의 생산 및 존속에 대해 고려하여야 함 |

※ R = Risk, A = 문서 번호

기술적 보안에 초점이 맞춰져 있다. 또한, 조직차원에서 정보보호보다 개인정보보호를 더 넓은 개념으로 이해하고 있다는 점이 특징이다. 다시 말해, PbD는 개인정보보호 활동이 정보보호활동의 일환이 아니라, 정보보호 활동의 주체는 개인정보보호이며 정보보호 활동을 개인정보보호 활동을 위한 구성요소로 인지하고 구현되어야 한다는 확장된 개념의 개인정보보호에 대해 설명하고 있다.

이러한 원칙을 기반으로 제시한 9가지 클라우드 컴

퓨팅 개인정보보호 위험을 KISA-PIMS와의 비교·분석을 통해 관련 통제목적을 [표 5]와 같이 도출하였다.

[표 5] PbD 클라우드 컴퓨팅 개인정보보호 위험 vs KISA-PIMS 통제목적

| Code | KISA-PIMS | |
|---|---|---|
| | 영역 | 통제목적 |
| RA1 | 생명주기준거 요구사항 | 2.6 해외 이전 시 개인정보보호<br>3.1 개인정보조사 및 책임할당 |
| RA2 | 생명주기준거 요구사항 | 2.4 제3자 제공시 개인정보보호 |
| RA3 | 개인정보보호 대책요구사항 | 8.2 암호통제 |
| RA4 | 개인정보보호 대책요구사항 | 7.3 모니터링<br>8.2 암호통제 |
| RA5 | 개인정보보호 대책요구사항 | 7.1 법적요구사항준수검토 |
| RA6 | 개인정보보호 대책요구사항 | 8.3 운영통제 |
| RA7 | 개인정보보호 대책요구사항 | 8.1 접근통제 |
| RA8 | 생명주기준거 요구사항 | 3.1 개인정보의 관리 및 파기 |
| RA9 | 생명주기준거 요구사항 | 1.2 개인정보수집 시 고지 및 동의 획득 |

### 3.3.2 World Privacy Forum

WPF(World Privacy Forum)는 2003년 출범한 다국적 비영리 연구·교육 단체로 금융, 의료 등 다양한 분야에서 발생하는 개인정보보호 관련 문제에 대해 주로 다루고 있다. 2009년 2월 미국 변호사 Robert Gellman이 WPF에서 작성한 'Privacy in the Cloud: Risks to Privacy and Confidentiality from Cloud Computing'이란 이름의 보고서에서는 클라우드 컴퓨팅 개인정보보호와 관련하여 다음과 같은 제안을 하고 있다[16].

첫 번째, 클라우드 컴퓨팅은 개인정보보호 및 조직정보와 매우 밀접한 관계를 가지고 있다. 사용자의 데이터가 멀리 떨어진 서버에 저장되는 방식은 이제 새로운 것이 아니며 이에 따라 개인정보보호 및 정보의 기밀성에 대한 확실한 보증이 요구되어야 한다(RB1).

두 번째, 사용자의 개인정보에 대한 위험은 클라우드 제공자에 의해 작성된 서비스 계약 조건 및 개인정보보호 정책에 의해 좌우된다. 이는 클라우드 제공자가 계약 조건 및 정책을 수정하게 되거나 위법하여 정보를 수집할 수 있으며, 이에 대해 사용자 역시 자세한 서비스 조건에 대해 인지하고 있어야 한다(RB2).

세 번째, 일부 클라우드 이용자의 경우 개인정보가 본래의 목적을 넘어서 제3자에게 제공될 수 있다. 절차상의 보호 등을 통하여 이러한 정보노출을 예방하고 제한할 수 있다(RB3).

네 번째, 클라우드 서비스가 제공하는 원격 저장소는 개인정보에 대한 법적 보호가 취약하여 외부자로부터의 감시나 검색 등의 대상이 되기 쉬우므로 이에 대한 추가적인 정보보호 및 감사 요구사항을 구현하여야 한다(RB4).

다섯 번째, 클라우드 환경에서 정보가 저장되는 물리적인 장소에 대한 적절한 통제 및 보호가 이루어져야 한다. 데이터가 물리적으로 저장된 장소가 위치한 특정 국가에서 따르는 법적 요구사항을 만족하여야 한다(RB5).

여섯 번째, 클라우드 환경의 개인정보는 클라우드 제공자에 의해 사용자 공지 없이 이동 및 복사 될 수 없으며, 상이한 사법권 간의 이동 및 전송으로 인해 상이한 법적 요구사항에 처할 수 있다(RB6).

일곱 번째, 불확실한 법은 반대로 사용자의 개인정보

[표 6] WPF 클라우드 컴퓨팅 개인정보보호 위험 vs KISA-PIMS 통제목적

| Code | KISA-PIMS | |
|---|---|---|
| | 영역 | 통제목적 |
| RB1 | 개인정보보호대책요구사항 | 8.1 접근통제<br>8.2 암호통제 |
| RB2 | 생명주기준거요구사항 | 2.3 외부위탁 시 개인정보보호 |
| RB3 | 개인정보보호대책요구사항 | 7.1 법적요구사항준수검토 |
| RB4 | 개인정보보호대책요구사항 | 7.3 모니터링 |
| RB5 | 개인정보보호대책요구사항 | 9.1 물리적 보안대책 |
| RB6 | 생명주기준거요구사항 | 2.6 해외 이전 시 개인정보보호 |
| RB7 | 개인정보보호대책요구사항 | 1.3 정책의 유지관리 |
| RB8 | 개인정보보호대책요구사항 | 5.1 개인정보 취급자관리 |

※ R = Risk, B = 문서 번호

보호 및 기밀성 유지에 장애가 될 수 있다. 새로운 기술은 예측할 수 없이 개발되는 것과 반대로 현행법은 그러한 흐름을 반영하지 못하는 경우가 있으며, 이는 급변하는 클라우드 환경에 적합하지 않을 수 있다(RB7).

여덟 번째, 클라우드 컴퓨팅 산업이 더 명확한 정책 및 사례를 도입하게 된다면 사용자는 개인정보보호 및 기밀성 관련 위협에 대해 더 나은 평가 및 대처가 가능할 것이다(RB8).

위 위험요소는 개인정보보호를 위한 세부적인 기술적 통제사항 보다는 법적·규제적 준거성 관련 위험요소를 기술하였으며, 대상이 미국에 위치한 클라우드 제공자에 맞춰져 있다는 것이 특징이며, 이와 연결되는 KISA-PIMS의 통제목적은 [표 6]과 같다.

## IV. 결 론

클라우드 컴퓨팅은 기존의 인터넷 기반 컴퓨팅에 비하여 경제성과 우수성을 고려해볼 때 주목할 만한 패러다임임이 확실하다. 이러한 신규 전략기술의 도입에 앞서 보안문제를 해결하여야 하며, 그 중 개인정보보호는 기업의 사활을 좌우할 수 있는 핵심 보안 문제로 우선적으로 고려하여야할 요소이다.

하지만 현재 국내 클라우드 서비스 도입 및 보안 관련 연구 활동은 상대적으로 뒤처져 있는 것이 사실이다. 현재 가시화 되고 있는 일부 서비스 및 기술을 제외하고는 대부분이 여전히 초기단계이며 클라우드 컴퓨팅 보안과 관련한 표준 및 전문 인력이 부족한 실정이다.

국내 클라우드 서비스는 이러한 차세대 IT 전략의 세계적인 시장 주도권을 잡기위한 필사적인 노력이 요구된다. 국내 ICT업체들의 연구 환경 및 신기술 개발 속도를 고려해봤을 때 양질의 서비스 구축이 가능할 것이라 하지만, 정부 및 공공·민간 기업들은 이러한 클라우드 컴퓨팅 기술 도입에 앞서, 보안 문제들을 인지하고 예방할 수 있는 법적, 정책적, 기술적 제도 마련이 필요하다.

이에 따라 국외 선진 사례 및 연구 등을 통해 제시된 클라우드 컴퓨팅 개인정보보호 요구사항을 국내 클라우드 환경에 맞게 적절히 구현하여 안전한 클라우드 컴퓨팅의 구축을 도모하여야 한다. KISA-PIMS를 활용하여 기존의 제도와의 연계성을 고려하는 한편, 나아가 클라우드 컴퓨팅 개인정보보호와 관련한 국제 표준 관리체계의 발전을 위한 연구 및 투자가 이루어져야 한다.

이러한 정부·기업·연구기관 간의 협력을 통해 클라우드 컴퓨팅 환경에서 개인정보보호의 철저한 관리가 가능해 진다면 경쟁력 있는 클라우드 서비스 제공과 함께 클라우드 컴퓨팅 주요국으로 발전할 수 있는 계기가 될 수 있을 것이다.

## 참고문헌


[1] 민옥기, "흰히 보이는 클라우드 컴퓨팅," pp. 42, 2009년 10월

[2] 클라우드 컴퓨팅, Christopher Barnatt, pp. 22-28, 2010년 4월

[3] Security of Cloud Computing Providers, Ponemon, pp 1-2, 2011년 4월

[4] Gartner, "Cloud computing ranks as the top concern of CIO's agendas for 2011," pp. 4-9, 2011 1월

[5] 김학범, 전은정, 김성준, "클라우드 컴퓨팅 환경에서의 보안 관리에 관한 연구," pp. 1-2, 2011년 2월

[6] NIST, "NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing," 2011년 1월

[7] NIST, "NIST SP 800-145 The NIST Definition of Cloud Computing," 2011년 1월

[8] NIST, "NIST SP 800-146 Cloud Computing Synopsis and Recommendations," 2011년 5월

[9] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 1980년 9월

[10] 홍성찬, 황인호, "프라이버시권에 있어서의 개인정보보호에 관한 연구," pp. 16-17, 2001년 10월

[11] www.iso.org/iso/standards_development, International Organization for Standardization

[12] isms.kisa.or.kr/kor/intro/pimsIntro01.jsp, 한국인터넷진흥원

[13] ISO/IEC, "ISO/IEC JTC 1/SC 27 Reaching for the Cloud", 2010년 8월

[14] ISO/IEC, "ISO/IEC JTC 1/SC 27 Modelling Cloud Computing Architecture without Compromising Privacy," 2010년 9월

[15] IPC, "2009 Privacy by Design - The 7 Foundational Principles," 2009년 8월

[16] Robert Gellman, "Privacy in the Clouds," 2009년 2월

## 〈著者紹介〉

**박 대 하 (Park Dae-Ha)**
종신회원
1992년 2월: 고려대학교 컴퓨터학과 학사
1994년 2월: 고려대학교 컴퓨터학과 석사
2004년 8월: 고려대학교 컴퓨터학과 박사
<관심분야> 정보보호관리체계, 개인정보보호, 클라우드 컴퓨팅 보안 등

**백 태 석 (Baek Taesuk)**
학생회원
2010년 2월: 중앙대학교 정보시스템학과 학사
2010년 3월: 중앙대학교 정보시스템학과 석사과정
<관심분야> 정보보호관리체계, 클라우드 컴퓨팅 보안, 개인정보보호 등