Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1267

클라우드 서비스 환경의 개인정보 위탁을 위한 개인정보보호 관리체계 통제 연구*

박 대 하,[1†‡] 한 근 희[2]
[1]고려사이버대학교, [2]고려대학교

A Study on PIMS Controls for PII Outsourcing Management under the Cloud Service Environment*

Dae-Ha Park,[1†‡] Keun-Hee Han[2]
[1]The Cyber University of Korea, [2]Korea University

요 약

클라우드 컴퓨팅 서비스를 이용하는 클라우드 소비자는 사용자의 개인정보에 대한 처리를 위탁받은 클라우드 제공자의 법적 준거성을 검토 및 감독해야 하는 의무를 갖는다. 본 논문에서는 국내 개인정보보호법의 위탁 시 준수사항을 토대로 클라우드 및 개인정보 관련 국제 표준과 국내 인증 제도를 분석하여 클라우드 개인정보 위탁이 가능한 시나리오를 제시하고 클라우드 환경에서 개인정보 위탁자에 해당하는 클라우드 소비자와 개인정보 수탁자에 해당하는 클라우드 제공자 간의 위탁 관리를 위한 개인정보보호 관리체계 통제를 제안하였다. 본 논문의 클라우드 개인정보 위탁 통제항목은 클라우드 제공자에게 개인정보의 처리를 위탁하고자 하는 조직에서 개인정보보호법을 준수하기 위한 지침을 개발하거나 개인정보보호 관리체계 인증에서 위탁 관리를 점검하기 위한 기준의 개발에 활용이 가능하다.

ABSTRACT

Cloud consumers who use cloud computing services are obliged to review and monitor the legal compliance of cloud providers who are consigned the processes of the PII (personally identifiable information) from them. This paper presented possible scenarios for cloud PII outsourcing and suggested PIMS (personal information management system) controls for outsourcing management between cloud consumers and cloud providers by analyzing both international standards and domestic certification schemes related to cloud computing and/or privacy management based on the legal obligations for PII outsourcing from Korean “Personal Information Protection Act (PIPA)”. The controls suggested can be applicable for developing the guidance of complying with privacy laws in organizations or the checklist of PII outsourcing management in PIMS certification.

Keywords: Cloud Service, Privacy, PII Protection, ISMS, PIMS, PIPL, Outsourcing Control

I. 서 론

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

접수일(2013년 11월 25일), 게재확정일(2013년 12월 9일)
* 본 연구는 순천향대학교 산학협력단의 위탁연구과제 지원으로 수행하였습니다.
† 주저자, summer69@cyberkorea.ac.kr
‡ 교신저자, summer69@cyberkorea.ac.kr(Corresponding author)

높아지고 있으며[1], 국가적인 차원에서도 클라우드 산업의 활성화를 위한 노력(예: 2009년 "범정부 클라우드 컴퓨팅 활성화 종합계획" 발표)이 지속적으로 이루어지고 있다[2].

하지만 2008년 미국 NIST의 조사에 따르면 응답자 244명 중 74.6%가 클라우드 도입에 보안이 가장 큰 이슈로 지적하고 있으며, 2010년 일본 경제산업성의 클라우드 서비스 조사보고서에 따르면 응답자 500명 중 58%가 클라우드 서비스의 가장 큰 우려사항으로 서비스 제공자의 보안대책에 대한 정보 부족을 들고 있다[3]. 또한 2011년 가트너의 조사 결과에 따르면 기업의 최고정보책임자(CIO)는 클라우드 컴퓨팅 환경에서 보안 및 프라이버시에 대한 가장 높은 관심을 가지고 있다[4].

최근 공공기관의 클라우드 서비스 도입 과정에서 보안 적합성을 평가하기 위하여 미국 연방정부의 FedRAMP와 영국 정부의 G-Cloud 보안 보증 외에도 민간 주도 비영리기관인 CSA의 OCF(Open Certification Framework) 등 다양한 제도가 등장하여 시행되고 있다[5].

클라우드 보안 적합성 평가 제도에서는 개인정보(personal information) 또는 개인식별정보(PII; personally identifiable information)의 측면에서 법적 준거성(compliance) 문제를 매우 중요하게 다루고 있다. 특히 클라우드 컴퓨팅 서비스를 이용하는 고객인 클라우드 소비자(cloud consumer)의 입장에서는 사용자의 개인정보를 보호하기 위한 내부적인 노력과 더불어 개인정보의 처리를 위탁하게 되는 클라우드 제공자(cloud provider)의 법적 준거성을 검토 및 감독해야 하는 의무를 지니게 되므로 클라우드 환경에서 개인정보보호 관리를 위한 통제의 필요성이 대두되고 있다.

국제 표준화기구인 ISO/IEC에서는 기존의 정보보호 관리체계(이하 ISMS) 통제 표준인 ISO/IEC 27002를 기반으로 클라우드 환경의 개인정보보호를 위한 통제 표준 문서로 ISO/IEC 27018을 개발하고 있다[6]. 하지만 ISO/IEC 27018은 클라우드 제공자의 측면에서 개인정보를 보호하기 위한 통제의 구현을 제공하고 있어서 더 높은 법적인 의무를 지닌 클라우드 소비자의 개인정보보호 통제를 구현하는데 적합하지 않고, 특히 클라우드 소비자가 개인정보의 위탁 관리를 위한 기준으로 활용하기 어려운 문제를 안고 있다.

국내에서도 개인정보보호 관련 법률에 대한 준거성과 체계적인 관리 활동을 평가하는 개인정보보호 인증제도가 등장하고 있지만 클라우드 환경에 특화된 인증기준은 마련하고 있지 않은 상황이다.

본 논문에서는 국내외 클라우드 및 개인정보 관련 정보보호 관리체계 표준과 인증 제도를 분석하여 클라우드 환경에서 클라우드 소비자(개인정보 위탁자에 해당)와 클라우드 제공자(개인정보 수탁자에 해당) 간의 위탁 관리를 위한 개인정보보호 관리체계의 통제를 도출하고자 한다.

우선 2장에서는 국내에서 제정한 개인정보보호법을 토대로 개인정보 위탁 시 법적인 준수사항을 도출하고 이를 위탁자와 수탁자의 측면에서 구분한다. 다음으로 3장에서는 ISO/IEC 27001의 인증을 위해 클라우드와 개인정보 분야의 통제를 제공하는 표준(ISO/IEC 27017, 27018, 29151)을 분석하고, 국내 개인정보보호 인증 제도인 개인정보보호 관리체계(PIMS)와 개인정보 보호제(PIPL)의 위탁 관련 통제를 분석하여 법적 준수사항과 대응시킨다. 마지막으로 4장에서는 ISO/IEC 29001을 기반으로 클라우드 개인정보 위탁이 가능한 시나리오를 모델로 제시하고, 클라우드 서비스 환경에서 개인정보 위탁을 위한 관리체계 통제를 제안한다.

II. 개인정보 위탁 시 법적 준수사항

개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)에 따르면 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에 위탁하는 개인정보처리자를 "위탁자(consignor)"로, 개인정보 처리 업무를 위탁받아 처리하는 자를 "수탁자(fiduciary)"로 정의하고 있다[7]. 즉, 클라우드 소비자에 해당하는 조직(공공기관 또는 민간기업)에서 개인정보를 활용하는 업무 중 일부를 클라우드 서비스를 이용하여 수행하는 경우에 클라우드 소비자는 위탁자가 되고 클라우드 제공자는 수탁자에 해당하는 것으로 볼 수 있다.

Table 1은 개인정보보호법 제26조를 구성하고 있는 제1항부터 제7항까지의 내용을 위탁자가 준수해야 할 사항(C1~C6)과 수탁자가 준수해야 할 사항(F1~F3)으로 구분하고 있다. 제26조 제1항에 따라 제3자에게 개인정보의 처리를 위탁하는 경우에 위탁업무 수행 목적 외 개인정보의 처리 금지, 개인정보의 기술적·관리적 보호조치에 관한 사항, 그 밖에 개인정보의 안전한 관리를 위한 사항이 포함된 문서에 의해

야 함을 명시하고 있으나, 세부적인 준수사항을 도출하여 추후 통제와 연계하기 위하여 "표준 개인정보보호 지침"[8] 제2절(개인정보 처리의 위탁)의 내용을 준수사항(C1, C2, F1)에 기술하였다. 나머지 준수사항은 개인정보보호법 및 시행령에서 규정한 내용을 그대로 서술한 것이다.

Table 1. Legal obligations for PII consignor and fiduciary from "Personal Information Protection Act (PIPA)"

구분	준수사항	법조항
위탁자	C1. 수탁자를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등을 종합적으로 고려하여야 한다.	제26조 제1항
	C2. 수탁자의 처리 업무의 지연, 처리 업무와 관련 없는 불필요한 개인정보의 요구, 처리기준의 불공정 등의 문제점을 종합적으로 검토하여 이를 방지하기 위한 필요한 조치를 마련하여야 한다.	제26조 제1항
	C3. 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있는 방법(예: 인터넷 홈페이지)으로 공개하여야 한다.	제26조 제2항
	C4. 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우, 위탁하는 업무의 내용이나 수탁자가 변경된 경우에 해당 업무의 내용과 수탁자를 정보주체에게 알려야 한다.	제26조 제3항
	C5. 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 않도록 수탁자를 교육하고, 처리현황 점검 등으로 개인정보를 안전하게 처리하는지 감독하여야 한다.	제26조 제4항
	C6. 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상 책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.	제26조 제6항
수탁자	F1. 위탁받은 개인정보를 보호하기 위하여 "개인정보의 안전성 확보조치 기준 고시"에 따른 관리적·기술적·물리적 조치를 한다.	제26조 제1항
	F2. 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.	제26조 제5항
	F3. 수탁자에 관하여는 제15조부터 제25조까지(수집·제공·이용·파기 등), 제27조부터 제31조까지(이전제한, 안전조치 등), 제33조부터 제38조까지(영향평가, 유출통지, 권리보장 등) 및 제59조(금지행위)를 준용한다.	제26조 제7항

클라우드 서비스 환경의 개인정보 수탁자인 클라우드 제공자는 제26조 제7항(F1)이 요구하는 개인정보의 기술적·관리적 보호조치에 해당하는 동법 제29조(안전조치의무)와 이를 구체적으로 명시한 "개인정보의 안전성 확보조치 기준 고시"[9]에 따라 이행해야 한다.

개인정보 위탁자인 클라우드 소비자는 제26조 제2항(C3)에 따라 위탁하는 업무의 내용(또는 클라우드 서비스 정보)과 수탁자인 클라우드 제공자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개해야 하며, 제26조 제6항(C6)에서는 수탁자가 법을 위반하여 발생한 손해배상책임에 대해 위탁자가 책임을 질 수 있도록 규정하고 있어서 제26조 제4항(C5)에 따라서 개인정보를 위탁한 클라우드 소비자는 이를 수탁한 클라우드 제공자의 교육과 보호조치의 이행을 감독할 의무를 갖는다.

클라우드 서비스 환경의 재판관할권 문제, 지적재산권 문제, 지리적인 분산 문제, 일시적 복제 문제 등[10]으로 인해 현실적으로 개인정보보호법 준거성의 보장이 어려울 수 있다. 국제 표준은 대부분의 국가와 산업 분야에 적용 가능한 현실성 있는 통제의 제공을 목표로 하므로 클라우드 및 개인정보보호를 위해 개발된 국제 표준과 국내 개인정보보호법의 준수를 요구하는 국내 개인정보 관리체계 인증제도의 통제를 함께 반영하여 준거성과 실현가능성의 균형을 이룬 개인정보 위탁 관리 방안의 도출이 필요하다.

III. 클라우드 및 개인정보보호 관련 통제 분석

3.1 ISO/IEC 27017, 27018, 29151 통제

국제적인 ISMS 인증의 요구사항인 ISO/IEC 27001과 정보보호 통제의 최적 실무를 제공하는 ISO/IEC 27002를 기반으로 클라우드 및 개인정보보호 분야에 대한 인증을 제공할 수 있도록 하기 위하여 ISO/IEC JTC 1의 SC 27에서는 다양한 표준 문건을 개발 중이다[6]. 클라우드 컴퓨팅 서비스의 정보보호 통제를 제공하는 ISO/IEC 27017[11]은 클라우드 소비자(클라우드 고객이라고도 함)와 클라우드 제공자로 구분하여 각각 구현 방법을 제시하고 있다. 또한 공공(public) 클라우드 환경에 특화된 프라이버시를 보장하기 위한 데이터 보호 통제를 ISO/IEC 27018[12]로 개발하고 있다. 일반적인 범주의 개인

정보를 보호하기 위한 통제는 ISO/IEC 29151[13]에서 다루고 있다. Table 2는 3 가지 국제 표준과 본 논문에서 다루고자 하는 통제의 범위를 정리하여 보여준다.

본 논문에서는 최종적으로 클라우드 소비자가 개인정보를 클라우드 제공자에게 위탁할 경우에 법적 준거성을 유지하면서 개인정보보호 관리체계를 수립하는데 도움이 되는 통제를 도출하고자 한다. 도출된 통제는 클라우드 제공자에게 직접적으로 적용하려는 목적은 아니지만 클라우드 소비자의 요구사항을 충족하도록 클라우드 제공자가 수행해야 하는 활동을 간접적으로 명시하게 된다.

Table 2. Control scope comparisons among cloud and privacy related ISO/IEC standards

범위 / 표준	클라우드 소비자	클라우드 제공자	개인정보 보호
ISO/IEC 27017	O	O	X
ISO/IEC 27018	X	O	O
ISO/IEC 29151	X	X	O
본 논문의 통제	O	△	O

ISO/IEC 27018에는 Table 3과 같이 ISO/IEC 27002의 통제 항목 이외에 추가적으로 클라우드 개인정보보호를 위하여 클라우드 제공자가 수행해야 하는 통제사항을 제시하고 있다[12]. 이 내용은 정보통신 시스템에서 개인정보를 보호하기 위한 프레임워크를 명시하고 있는 ISO/IEC 29100의 10 가지 프라이버시 원칙에 따라 정리한 것이며, “1. 동의 및 선택”, “2. 합목적성 및 명세”, “3. 수집 제한”, “4. 데이터 최소화”, “5. 사용, 보유, 공개 제한”, “6. 정확성 및 품질”, “7. 개방성, 투명성, 공지”, “8. 개인 참여 및 접근”, “9. 책임추적성”, “10. 정보보호”, “11 프라이버시 준거성”으로 구성된다[14]. 통제 항목에 부여한 앞 번호는 해당하는 원칙의 번호와 일치(예: “4.1 임시파일의 안전한 삭제”는 “4. 데이터 최소화”의 통제 항목)한다.

Table 3. Privacy controls for cloud provider from ISO/IEC 27018

통제항목	통제내용
1.1 정보주체 권한에 대한 상호협력	클라우드 제공자는 자신이 보유한 개인정보에 정보주체가 접근, 수정, 삭제할 수 있는 권한을 행사할 수 있도록 하는 클라우드 소비자의 의무에 협력하여야 한다.
2.1 클라우드 소비자의 목적	계약에 따라 처리되는 개인정보는 클라우드 서비스 소비자의 지시를 벗어난 목적으로 처리되지 않도록 대책을 수립해야 한다.
2.2 클라우드 제공자의 상업적 사용	계약에 따라 처리되는 개인정보는 동의 없이 마케팅이나 광고의 목적으로 사용되지 않음을 보장하기 위한 대책을 수립해야 하며, 서비스의 수용을 조건으로 동의가 이루어지지 않아야 한다.
4.1 임시파일의 안전한 삭제	개인정보가 포함된 임시 파일과 문서는 정해진 기간 내에 삭제 또는 폐기되도록 대책을 수립해야 한다.
5.1 개인정보 공개 공지	클라우드 제공자와 클라우드 소비자 간의 계약으로 법집행 기관에 의한 개인정보의 공개 요청을 법적으로 결부하여 정보주체에게 공지하여야 하며, 다른 경우에는 공개를 금지해야 한다.
5.2 개인정보 공개 기록	개인정보의 공개는 내용, 대상, 시간을 포함하여 기록하여야 한다.
7.1 개인정보 처리 하도급 계약 공개	클라우드 제공자가 개인정보를 처리하기 위해 하위 클라우드 제공자를 이용할 경우에 사전에 해당 클라우드 소비자에게 공지해야 한다.
9.1 위반사항 공지	클라우드 제공자는 개인정보에 대한 비인가된 접근이나 처리 장비 및 설비에 대한 비인가된 접근으로 인해 개인정보의 손실, 노출, 변경이 발생하면 관련된 클라우드 소비자에게 즉각적으로 공지해야 한다.
9.2 관리적 보안 정책 및 지침에 대한 유지	개인정보보호 절차를 구현하기 위한 보안 정책과 원칙이 문서로 명시된 주기에 따라 갱신을 통해 유지되도록 대책을 수립해야 한다.
9.3 개인정보 반환 이전 폐기	클라우드 제공자는 개인정보의 반환, 이전, 폐기에 대한 정책을 수립하고 클라우드 소비자에게 알려야 한다.
10.1 비밀유지서약	클라우드 제공자의 통제 하에서 개인정보에 접근하려는 자가 기밀성 의무를 지킬 수 있도록 대책을 수립해야 한다.
10.2 하드카피 매체의 생성 제한	개인정보를 보여주는 하드카피 매체의 생성을 제한하기 위한 대책을 수립해야 한다.
10.3 데이터 복구 통제 및 로그기록	데이터 복구 활동을 위한 절차와 로그가 존재함을 보장하는 대책을 수립해야 한다.
10.4 역외 저장매체 상의 데이터 보호	조직의 구역을 벗어난 매체에 포함된 개인정보는 승인된 절차에 따르며 데이터 암호화 등으로 비인가자가 접근할 수 없도록 절차를 수립해야 한다.

통제항목	통제내용
10.5 암호화되지 않은 저장매체의 사용	암호화가 허용되지 않는 물리적 매체 및 이동식 장비는 불가피한 경우를 제외하고는 사용하지 않도록 하고, 해당 매체와 장비의 사용을 기록하는 대책을 수립해야 한다.
10.6 공개 네트워크 전송 시 암호화	공개된 네트워크로 전송되는 개인정보를 암호화하기 위한 대책을 수립해야 한다.
10.7 하드카피 매체의 안전한 폐기	하드카피 매체를 폐기할 경우에는 횡단절삭, 분쇄, 소각 등의 방법을 사용하여 안전하게 폐기해야 한다.
10.8 고유한 식별자의 사용	저장된 개인정보에 두 명 이상이 접근할 경우에는 각각 식별, 인증, 권한부여를 위해 구분되는 식별자를 소유함을 보장하는 대책을 수립해야 한다.
10.9 승인된 사용자 기록	정보시스템에 인가된 접근을 시도하는 사용자의 최신 기록 또는 프로필을 유지해야 한다.
10.10 식별자 관리	비활성화 또는 폐지된 식별자는 다른 개인에게 허용되지 않도록 대책을 수립해야 한다.
10.11 데이터 처리 계약 대책	클라우드 소비자와 클라우드 제공자 간의 계약은 정보보호를 보증하고 통제자의 지시를 벗어난 목적으로 처리하지 않도록 구체적인 기술적 및 조직적 대책을 명시하고 있어야 한다.
10.12 하도급 개인정보 처리	개인정보를 처리하는 클라우드 제공자와 하위 클라우드 제공자 간의 계약은 클라우드 제공자의 정보보호 및 개인정보보호 의무를 충족하는 구체적인 기술적 및 조직적 대책을 명시하고 있어야 한다.
11.1 개인정보의 지리적 위치	클라우드 제공자는 가능한 경우에 개인정보가 저장되는 국가를 명시하고 문서화하는 정책을 수립해야 한다.
11.2 개인정보의 의도된 목적지	데이터 전송 장비를 거쳐 개인정보가 의도된 목적지(조직 또는 개인)에게 정확하게 전달됨을 보장하기 위한 대책을 수립해야 한다.

ISO/IEC 27018의 통제 사항을 Table 1의 개인정보보호법 준수사항을 토대로 관련 내용을 대응시켜 보면 Table 4와 같이 나타낼 수 있다. 안전성 보호조치에 해당하는 "10. 정보보호" 통제 항목은 주로 클라우드 제공자가 준수해야 하는 사항이지만 보안 사건이 발생하면 "9.1 위반사항 공지"를 통해서 클라우드 소비자에게 알려야 하고 클라우드 소비자는 이를 확인할 의무를 가지게 된다.

ISO/IEC 27018의 통제 내용은 수탁자인 클라우드 제공자를 중심으로 기술되어 있으므로 위탁자인 클라우드 소비자의 준수사항과 관련된 통제 사항은 ISO/IEC 27017과 ISO/IEC 29151의 내용을 연계하여 도출해야 한다.

Table 4. Mapping PIPA obligations into controls of ISO/IEC 27018

구분	개인정보보호법 준수사항	ISO/IEC 27018 통제 항목
위탁자	C1	9.2, 10.11
	C2	1.1, 10.1
	C3	7.1, 11.1
	C4	2.2
	C5	9.3
	C6	9.1
수탁자	F1	10.2~10.10, 11.2
	F2	2.1, 10.12
	F3	4.1, 5.1, 5.2,

3.2 국내 PIMS, PIPL 위탁 관련 통제

국내에서는 기업의 개인정보보호 활동을 체계적이고 지속적으로 수행하기 위해 필요한 보호조치 체계를 구축하였는지 점검하고 일정 수준 이상의 기업에 인증을 부여하는 PIMS 인증 제도가 2011년부터 한국인터넷진흥원(KISA)을 인증기관으로 하여 시행 중이다. KISA의 ISMS 인증에서 요구하는 관리과정과 통제를 기반으로 개인정보보호법과 정보통신망법(정보통신망 이용촉진 및 정보보호 등에 관한 법률)에 따른 개인정보 생명주기 요구사항을 통제로 적용하고 있다[15].

KISA의 PIMS는 일반적인 조직 내부의 개인정보보호 관리 활동에 중점을 두고 있어서 클라우드 환경의 개인정보보호 위험을 적절하게 다루지 못하고 있으며, 기존 연구[16]에서 이와 같은 문제점을 지적하고 ISO/IEC 27017의 내용을 반영하여 클라우드 컴퓨팅 환경의 PIMS 통제의 적용 방법을 제안한 사례도 있다.

KISA의 PIMS에서 개인정보 위탁과 관련된 통제사항과 점검항목을 도출하면 Table 5와 같다. 통제사항의 번호(예: 2.2.2)는 "개인정보보호 관리체계 인증 등에 관한 고시"[17]의 생명주기 요구사항에서 부여한 번호와 동일하며, 점검항목에 부여한 번호는 타 제도의 점검항목과 비교가 쉽도록 순서대로 부여한 것(예: 2.2.2.6은 2.2.2의 6 번째 점검항목)이다. PIMS에서 위탁 관련 통제사항을 포함하고 있는 도메

인(통제 영역)은 “2. 개인정보 이용 및 제공에 따른 조치”, “3. 개인정보 관리 및 파기에 따른 조치”이다.

Table 5. Controls in KISA PIMS related to PII outsourcing

통제사항	점검항목
2.2.2 열람정정 요구권 보장 및 처리	2.2.2.6 외부위탁 또는 제3자에게 제공한 개인정보가 있을 경우 이에 대해서도 정정 및 동의철회에 대한 조치를 취하고 결과를 확인하는가?
2.3.1 이용자 고지 및 동의	2.3.1.1 제3자에게 이용자의 개인정보를 처리 업무를 위탁하는 경우 관련 사항을 이용자에게 알리는가?
	2.3.1.2 개인정보 취급위탁에 대한 동의 획득시, 개인정보 수집시와 동일한 방법으로 동의를 받는가?
	2.3.1.3 개인정보 취급 위탁 시 수탁업체 변동 또는 위탁업무 범위 및 계약상의 변동사항이 발생할 경우 이용자로부터 별도의 동의절차를 거치고 있는가?
2.3.2 위탁자 책임	2.3.2.1 위탁사는 개인정보 취급 목적을 미리 정하고, 수탁사가 취급목적을 벗어나서 이용자의 개인정보를 취급하지 않도록 관리하는가?
	2.3.2.2 수탁사가 개인정보취급 시 법규정을 위반하였을 경우 처리 및 배상에 관한 절차가 있는가?
2.3.3 외부위탁관리 감독	2.3.3.1 수탁업체로부터 개인정보보호와 관리상황을 주기적으로 보고 받고, 정기 또는 수시점검을 통해 관리감독하고 있는가?
	2.3.3.2 개인정보 취급 위탁 시 수탁사 직원에 대한 보안교육을 하고 있는가?
	2.3.3.3 수탁사 및 외부로부터의 개인정보처리시스템 접근내역을 기록하고 남기고 있는가?
	2.3.3.4 개인정보 위탁계약 종료 시 수탁사로부터 개인정보를 회수·파기하고 있는가?
2.3.4 외부위탁계약 관련사항	2.3.4.1 외부위탁 계약 시 개인정보보호에 관한 요구사항을 사전에 분석하였는가?
	2.3.4.2 외부위탁 계약 시 개인정보보호와 관련한 법적요건 및 조직의 개인정보보호 정책을 만족하기 위한 요구사항을 계약서상에 명시하였는가?
	2.3.4.3 외부위탁 계약서는 수탁사의 의무 및 책임에 대하여 개인정보보호책임자 지정, 정기적인 관리현황 보고, 위탁사에 의한 이행점검, 개인정보 침해 발생 시 대책 및 책임의 관계 관련 조항을 포함하고 있는가?
3.1.3 파기시점	3.1.3.3 개인정보를 파기하여야 하는 경우, 위탁 또는 제3자에게 제공한 개인정보도 함께 지체없이 파기하는가?

최근(2013년도)에는 한국정보화진흥원(NIA)에서 개인정보보호법에 따른 준거성과 개인정보보호체계(관리체계) 및 개인정보 보호대책을 소상공인, 중소기업, 대기업 및 공공기관을 대상으로 평가하여 인증을 부여하는 개인정보보호 인증제(이하 PIPL)가 등장하였다[18].

Table 6은 NIA의 PIPL에서 개인정보 위탁과 관련된 통제사항과 세부 점검항목을 도출한 것이다. PIPL은 인증 대상에 따라 평가할 통제사항이 다르지만 위탁 관련 통제사항은 법적 준거성을 기반으로 하므로 모든 대상(소상공인, 중소기업, 대기업, 공공기관)이 반드시 준수해야 하는 요구사항에 해당한다.

PIMS와 유사하게 통제사항의 번호(예: 6.1.1)는 “개인정보 보호 인증제 운영에 관한 규정”[19]에서 부여한 번호와 동일하며, 점검항목에 부여한 번호는 타 제도의 점검항목과 비교가 쉽도록 순서대로 부여한 것(예: 6.1.1.5는 6.1.1의 5 번째 점검항목)이다. 위탁

Table 6. Controls in NIA PIPL related to PII outsourcing

통제사항	점검항목
6.1.1 개인정보의 열람 정정 삭제	6.1.1.5 개인정보를 정정 삭제하여야 하는 경우, 위탁사에게 제공한 개인정보도 함께 지체 없이 처리하는가?
7.2.1 교육 및 훈련 시행	7.2.1.2 개인정보보호 교육 대상은 개인정보보호 책임자 및 개인정보취급자(수탁직원 포함)를 포함하는가?
7.3.2 보안서약서	7.3.2.2 개인정보를 취급하는 외부직원(위탁직원 포함) 등에 대하여 위탁계약서에 책임과 의무를 명시하고 개인정보보호 서약서를 징구하고 관리하는가?
7.4.1 외부위탁계약	7.4.1.1 개인정보 처리업무를 제3자에게 위탁하는 경우 문서화된 계약서 등에 의하여 이루어지고 있는가?
	7.4.1.2 위탁계약서에 위탁업무 목적 외 처리금지, 개인정보의 기술적 관리적 보호조치 등 법률에서 정한 사항들을 포함하고 있는가?
7.4.2 정보주체 고지	7.4.2.1 위탁자는 정보주체(이용자 등)가 언제든지 수탁자의 정보를 확인할 수 있도록 관보 또는 인터넷 홈페이지 등의 방법으로 공개하였는가?
	7.4.2.2 위탁자가 재회 또는 서비스를 홍보하는 등 그 업무범위에서 제3자에게 업무를 위탁하는 경우, 위탁업무의 내용과 수탁자의 정보 등을 정보주체에게 서면, 전자우편 등의 방법으로 알리고 있는가?
7.4.3 위탁자 관리	7.4.3.1 위탁자는 수탁자가 개인정보를 안전하게 처리하는지를 주기적으로 감독하는가?
	7.4.3.2 위탁자는 개인정보 취급 목적을 미리 정하고, 수탁자가 취급목적을 벗어나서 이용자의 개인정보를 취급하지 않도록 관리하는가?

관련 통제사항을 포함하고 있는 심사 영역은 "6. 정보주체 권리보장"과 "7. 관리적 안전성 확보조치"이다.

Table 7은 국내 개인정보보호법의 관련 규정에 따라 PIMS와 PIPL의 통제사항과 점검항목을 대응시킨 것이다. PIPL은 개인정보보호법을 근거로 수립된 제도이므로 위탁 관련 통제항목이 모두 법 준수사항에 대응이 되지만, PIMS는 정보통신망법의 준수사항(2.3.2.2, 2.3.3.3)도 포함하고 있어서 개인정보보호법 준수사항과 대응이 되지 않는 부분도 존재한다(유사한 목적으로 연결해 보면 2.3.3.3은 F1으로, 2.3.2.2는 F3에 대응이 가능함).

Table 7. Mapping PIPA obligations into checklists of PIMS and PIPL

구분	개인정보보호법 준수사항	점검항목	
		PIMS	PIPL
위탁자	C1	2.3.4.2	7.4.1.1
	C2	2.3.4.3	7.4.1.2
	C3	2.3.1.1	7.4.2.1
	C4	2.3.1.2 2.3.1.3	7.4.2.2
	C5	2.3.3.2	7.2.1.2
		2.3.3.1	7.4.3.1
	C6	2.3.2.1	7.4.3.2
수탁자	F1	2.2.2.6	6.1.1.5
	F2	2.3.4.2	7.3.2.2
	F3	2.3.3.4	6.1.1.5

IV. 클라우드 개인정보 위탁 정보보호관리 통제

4.1 클라우드 개인정보 위탁 모델

클라우드 환경에서 개인정보를 위탁하는 경우는 다양한 상호작용으로 나타날 수 있다. 서비스 형태로 제공되는 자원의 계층(예: SaaS, PaaS, IaaS 등)에 따라 다를 수 있고, 서비스의 배치 방식(예: 공공 클라우드, 사설 클라우드, 복합 클라우드 등)에 따라 다를 수 있다[20]. 또한 일반 개인이 직접 클라우드 제공자의 서비스를 임차하는 퍼스널 클라우드의 경우는 클라우드 제공자가 위탁자가 될 수도 있고 위탁이 발생하지 않을 수도 있다.

ISO/IEC 29100에 의하면 클라우드 소비자는 개인정보를 처리하는 목적과 방법을 결정하는 통제자(PII controller)의 역할을 수행하고, 클라우드 제공자는 통제자의 요청에 따라 개인정보를 처리하는 처리자(PII processor; 개인정보보호법의 개인정보처리자와는 다름)에 해당하는 것으로 볼 수 있다. 따라서 정보주체(PII principle)인 개인 클라우드 사용자와 클라우드 소비자 및 클라우드 제공자(공급자 체인을 따른 추가적인 제3자 클라우드 제공자도 포함) 간의 개인정보 이동을 ISO/IEC 29100의 8 가지 시나리오를 토대로 재구성하면 Table 8과 같다.

Table 8. Scenarios for PII cloud outsourcing

시나리오	클라우드 사용자 (개인)	클라우드 소비자 (위탁자)	클라우드 제공자 (수탁자)	클라우드 제공자 (제3자)	위탁 가능
a)	개인정보 전송	개인정보 수신	-	-	-
b)	-	개인정보 전송	개인정보 수신	-	O
c)	개인정보 전송	-	개인정보 수신	-	O
d)	개인정보 수신	개인정보 전송	-	-	-
e)	개인정보 수신	-	개인정보 제공	-	O
f)	-	개인정보 수신	개인정보 제공	-	O
g)	-	개인정보 제공	-	개인정보 수신	-
h)	-	-	개인정보 제공	개인정보 수신	-

본 논문에서 정보보호관리 보안통제를 도출하고자 하는 시나리오는 b)와 c)와 같이 클라우드 소비자와 클라우드 제공자 간의 위탁 협약을 기반으로 클라우드 사용자가 위탁자인 클라우드 소비자에게 제공한 개인정보를 수탁자인 클라우드 제공자에게 전달하거나 클라우드 사용자가 클라우드 제공자에게 직접 제공하는 경우를 위탁 관리가 가능한 형태로 본다. e)와 f)의 경우는 클라우드 제공자가 정보주체인 클라우드 사용자와 처리 요청자인 클라우드 소비자에게 개인정보를 보내주는 시나리오이므로 위탁 관리의 범주에 포함된다. 4 가지 경우는 모두 클라우드 소비자와 클라우드 제공자 간에 SLA(Service Level Agreement)와 같은 위탁 계약을 체결하는 것을 전제로 한다.

a)와 d)는 수탁자인 클라우드 제공자가 개입하지 않으므로 위탁 관계가 이루어지지 않으며, g)와 h)는 클라우드 제공자에 대한 클라우드 소비자의 통제 의무가 발생하지 않는 제3자 제공의 경우(예: 정보주체의 동의 또는 다른 법적 근거를 토대로 제공)에 해당하므로 위탁 관계에서 제외시킬 수 있다. 단, h)는 클라우드 제공자 간의 서비스 계약을 통해 위탁 관계를 유지

할 수 있으며, 이 경우에는 b)와 동일한 통제를 적용할 수 있다.

4.2 클라우드 개인정보 위탁 통제항목 도출

클라우드 서비스를 사용하는 클라우드 소비자가 정보주체인 클라우드 사용자의 개인정보를 클라우드 제공자에게 위탁하는 경우에 Table 9와 같은 위탁 관리 통제항목을 도출할 수 있다.

통제 항목의 명칭은 Table 1에서 제시한 개인정보보호법의 위탁자 준수사항을 토대로 하였고, 통제 내용은 Table 3의 ISO/IEC 27018의 클라우드 제공자에 대한 통제 내용에 대응할 수 있는 ISO/IEC 29151의 위탁 관련 개인정보보호 통제 내용을 추출하여 ISO/IEC 27017의 클라우드 관련 용어로 조정한 것이다. 최종적으로 국내 환경에 적합한 통제 내용으로 다듬기 위하여 PIMS와 PIPL의 관련 통제사항과 점검항목을 반영하였다.

Table 9. Cloud PII outsourcing controls

통제항목	통제내용
1. 클라우드 제공자 선정	클라우드 소비자는 개인정보를 위탁할 클라우드 제공자를 선정하기 위한 정책을 문서화하고 개인정보보호와 관련한 법적 요구사항을 명시한 위탁계약서를 사전에 준비하여야 한다.
2. 클라우드 제공자 계약	클라우드 소비자는 클라우드 제공자에게 위탁한 개인정보에 대한 정보주체의 권한 행사, 안전성 확보조치, 정기적인 관리현황 보고 및 이행점검 가능, 사고 발생시 대응 등의 의무와 책임을 포함한 위탁계약을 체결하여야 한다.
3. 클라우드 제공자 공개	클라우드 소비자는 개인정보를 수탁한 클라우드 제공자의 정보를 정보주체인 이용자에게 공개하여 동의를 획득하고, 하위 클라우드 제공자에게 재위탁이 존재하는지 확인하여 공지하여야 한다.
4. 클라우드 제공자 변경 공지	클라우드 소비자는 클라우드 제공자의 변경이나 위탁한 서비스 업무 범위 및 계약상의 변동이 발생할 경우 정보주체에게 공지하고 별도의 동의를 받기 위한 절차를 수립하여야 한다.
5. 클라우드 제공자 관리 감독	클라우드 소비자는 개인정보를 수탁한 클라우드 제공자가 직원에 대한 보안교육을 수행하고 있는지 확인하고, 개인정보의 안전한 처리와 법적 준수사항을 주기적으로 보고 받아 필요시 점검을 통해 관리 감독하여야 한다.
6. 클라우드 제공자 사고 대응	클라우드 소비자는 위탁한 개인정보에 대한 침해사고로 인한 피해가 발생하면 클라우드 제공자와 공조하여 신속히 정보주체에게 고지하고, 위탁계약을 위반한 사건이 발생한 경우에 계약 해지를 포함한 법적 책임을 부여할 수 있는 대응 방안을 마련하여야 한다.

Table 10은 본 논문에서 제안한 클라우드 개인정보 위탁 통제와 Table 1의 개인정보보호법 준수사항을 대응한 것이며, 위탁자뿐만 아니라 수탁자에 대한 준수사항을 같이 명시하여 개인정보를 취급하는 클라우드 제공자의 협업이 필요함을 보여주고 있다.

Table 10. Comparisons between cloud outsourcing controls and PIPA obligations

클라우드 개인정보 위탁 통제항목(제안)	개인정보보호법 준수사항	
	위탁자	수탁자
1. 클라우드 제공자 선정	C1	-
2. 클라우드 제공자 계약	C2	-
3. 클라우드 제공자 공개	C3	-
4. 클라우드 제공자 변경 공지	C4	F2
5. 클라우드 제공자 관리 감독	C5	F1, F2
6. 클라우드 제공자 사고 대응	C6	F2, F3

V. 결 론

본 논문에서 제안한 클라우드 개인정보 위탁 통제 항목은 클라우드 서비스 환경에서 클라우드 제공자에게 개인정보의 처리를 위탁하고자 하는 조직(공공기관 또는 민간기업)에서 국내 개인정보보호법을 준수하기 위한 지침을 개발하는데 활용이 될 수 있다. 또한 PIMS 또는 PIPL과 같은 개인정보보호 관련 인증을 클라우드 소비자에게 적용하여 위탁 관리의 준거성을 점검하기 위한 심사 기준의 개발에도 도움을 준다. 통제를 도출하기 위한 본 논문의 분석 과정은 국제 표준에서도 클라우드 개인정보 보안에 대한 지속적인 표준 개발이 이루어지고 있어서 국가적인 차원에서 한국의 입장을 반영하기 위한 기고문을 작성하는데 참고할 만한 모델이 될 것이다.

실제로 개인정보보호 관리체계 인증 제도에 적용하려면 통제에 대한 세부적인 점검항목과 인증 대상을 위한 구현 지침의 개발에는 후속 작업이 필요하지만 다양한 클라우드 서비스 환경과 개인정보보호법 이외의 개인정보 관련 법규에 대한 분석이 필요하므로 추후 연구과제로 남겨두기로 한다.

References

[1] Christopher Barnatt, "A brief guide to cloud computing," Constable & Robinson, pp. 22-28, Apr. 2010.

[2] Sang-Dong Lee, "The strategic steps of cloud services in Korea," Journal of KIISE, 28(12), pp. 34-38, Dec. 2010.

[3] Nakao Koji, "The art of information security technology for introducing cloud," Network Security Forum 2011, Tokyo, Jan. 2011.

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

[5] Suk Gwon Chang, "Development strategies and policy challenges for cloud service," Telecommunications Policy Review, 24(9), pp.1-22, May 2012.

[6] Dae-Ha Park, "Trends of information security and privacy international standardization," Review of KIISC, 23(4), pp.47-52, Aug. 2013.

[7] NIA, "Comparison of Personal Information Protection Act (PIPA), its enforcement ordinance, regulations and guideline," Nov. 2012.

[8] MOSPA, "Standard privacy protection guideline," Nov. 2011.

[9] MOSPA, "Criteria and manual for assuring security of personal information," Nov. 2011.

[10] Park, Young Gyu, "An analysis of legal issues in cloud computing," Journal of Bubjo, 61(8), pp.185-222, Aug. 2012.

[11] ISO/IEC 5th WD 27017, "Code of practice for information security controls for cloud computing services based on ISO/IEC 27002," Jun. 2013.

[12] ISO/IEC 1st CD 27018, "Code of practice for data protection controls for public cloud computing services," Jun. 2013.

[13] ISO/IEC 1st WD 29151, "Code of practice for PII protection," Jun. 2013.

[14] ISO/IEC 29100, "Privacy framework," Dec. 2011.

[15] KISA, "Introduction to Personal Information Management System (PIMS) certification," Dec. 2010.

[16] Dae-Ha Park, Tae-Suk Baik, "Research trends and challenges for privacy protection in cloud computing," Review of KIISC, 21(5), pp.47-54, Aug. 2011.

[17] Korea Communications Commission, "Notification of PIMS certification," Sep. 2013.

[18] NIA, "Textbook for training PIPL auditors," Oct. 2013.

[19] MOSPA, "Regulations for operating PIPL," Oct. 2013.

[20] NIST SP 500-292, "NIST cloud computing reference architecture," Sep. 2011.

〈저자소개〉

박 대 하 (Dae-Ha Park) 종신회원
1992년 2월: 고려대학교 컴퓨터학과 학사
1994년 2월: 고려대학교 컴퓨터학과 석사
2004년 8월: 고려대학교 컴퓨터학과 박사
2004년 3월~현재: 고려사이버대학교 정보관리보안학과 교수
〈관심분야〉 정보보호관리체계, 개인정보보호, 소셜 네트워크 보안, 클라우드 컴퓨팅 보안, 데이터베이스 보안, PKI, 신뢰 모델 등

한 근 희 (Keun-Hee Han) 종신회원
서울과학기술대학교 학사
한양대학교 과학대학원 석사
고려대학교 컴퓨터학과 박사
현재: 고려대학교 융합소프트웨어전문대학원 교수
〈관심분야〉 시큐어 코딩, 정보보호관리체계, 개인정보보호, 클라우드 컴퓨팅 보안, 스마트의료보안, 스마트자동차보안 등