개인정보의 법적·기술적 특성을 고려한 라이프 사이클(Life Cycle) 모델

The life cycle model considering legal and technical characteristics of personal data

장재영(Jaeyoung Jang)*, 박태환(Taehwan Park)**, 김범수(Beomsoo Kim)***
jyjang31@gmail.com, pth3030@nate.com, beomsoo@yonsei.ac.kr

초 록

최근 개인정보 보호를 이해하기 위해 라이프 사이클 모델을 활용하는 사례가 증가하고 있다. 현재 국내에서 사용하고 있는 모델은 크게 법적 기반 모델과 흐름 기반 모델이 있다. 이들 모델들은 정보통신망법의 개인정보 보호 조항 설명, 개인정보보호관리체계(PIMS), 개인정보 영향 평가 등 특정 목적에 맞게 개발되어 모델들 마다 개인정보 보호의 일반적 특징을 설명하는 데에 한계를 가지고 있다. 법적 모델은 개인정보의 저장을 간과하고 있어 개인정보 해킹 사고 분석 및 개인정보 보호에 적용되는 정보보호 기술을 설명하지 못하고 있으며, 흐름 기반 모델은 개인정보의 법적 준수(Compliance) 사항에 대한 설명이 어렵다.

이 연구에서는 개인정보의 법적 및 기술적 특징을 고려한 '개인정보의 동의·관리 기반 모델'을 제안한다. 동의·관리 기반 모델은 개인정보의 흐름 기반 모델을 기초로 하여 법적 동의(Consent)와 정보보호 기술 등을 포함한 관리(management)를 강조한 모델이다. 개인정보의 동의·관리 기반 모델은 개인정보의 종합적·체계적인 분석 및 대책 마련에 도움이 될 것으로 기대된다.

1. 개인정보보호

1.1 개요

IT가 일상화 된 현대 사회는 홈쇼핑, 홈뱅킹 등 인터넷 이용은 물론 사물, 개인의 일상을 기록한 라이프 로그 데이터 등이 결합하여 기존의 관리 및 분석 체계로는 감당할 수 없을 정도의 거대한 데이터 집합이 생겨나고 있다. '빅 데이터' 시대라고 불리는 이러한 새로운 현상은 페이스북, 트위터 등 SNS 이용 확산과 커뮤니케이션 방식의 변화 등 개인정보의 증가가 중요한 요인 중 하나이다[10][15].

개인정보란 이용자가 서비스를 위해 기업에 제공하는 주민등록번호, 성명, 주소 등의 식별 정보이다. IT 기업들은 이용자가

* 연세대학교 정보대학원 박사과정
** 연세대학교 정보대학원 석사과정
*** 연세대학교 정보대학원 교수

제공한 개인정보를 회원 인증, 서비스 제공, 민원처리에 활용한다. 최근에는 데이터 마이닝(Data mining) 기법을 활용하여 이용자의 행태 정보를 생성, 처리하여 마케팅에 활용하는 사례도 증가하고 있다[11].

IT 기업에서 개인정보의 활용은 기업 경영의 중요 요소 중 하나로 부각되고 있지만, 경쟁기업 및 외부 해커로부터 자사의 개인정보를 보호해야 하는 새로운 상황에 직면하고 있는 것도 주지의 사실이다. 이용자의 개인정보를 보호하는 것은 법, 정책 및 기술과 관련된 복잡하고 전문적인 영역이다. 개인정보는 다른 정보와 달리 기업이 수집했다고 해서 무제한적으로 활용하거나 보유할 수 없다. 개인정보는 법률에 따라 개인정보 주체로부터 동의를 받고 수집 당시부터 엄격하게 통제를 받는다. 목적이 달성되면 보유한 개인정보를 파기해야 한다[2]. 반면, IT 기업들은 수집한 개인정보를 법적으로는 개인정보 처리 시스템이라고 하는 데이터베이스(이하 'DB'라 한다)에 저장 및 관리한다. DB 에 저장된 개인정보는 외부의 침입에 대비해서 첨단 기술과 관리 기법 하에서 보호된다.

IT 기업이 개인정보를 효과적으로 보호하기 위해서는 개인정보 및 개인정보 보호에 대한 체계적이고 종합적인 분석이 선행되어야 한다. 복잡한 개인정보를 가장 효율적으로 이해하는 방법 중 하나는 IT 기업에 의해 개인정보가 수집되어 DB 에 저장·이용·파기되는 전체 프로세스를 분석하는 것이다. 개인정보의 이러한 프로세스를 개인정보의 라이프 사이클이라 한다[23][26]. 개인정보의 라이프 사이클은 IT 기업의 개인정보 보호 대책 수립, 영향평가, 인증, 컨설팅, 내부 관리 계획의 수립 등에 아주 유용하게 활용되고 있다.

현재 국내에서는 다양한 개인정보의 라이프 사이클 모델들이 활용되고 있다. 그러나 지금까지 개발되어 온 모델들은 개발 목적에 따라 개인정보 보호를 설명하는데 일정한 한계를 가지고 있다. 일부 모델들은 개인정보 법률 규정을 설명하기 위해 만들어졌다. 따라서, 개인정보의 라이프 사이클 중 DB 및 데이터 암호화, 접근제어 장비 등 기술적인 부분을 충분히 다루지 못하고 있다. 다른 모델들은 개인정보의 처리 흐름에 따라 라이프 사이클을 설명하고 있지만 개인정보의 법적·사회적 특성을 설명하지 못하고 있다. 또한, 국내에서 활용되고 있는 모델들은 공통적으로 온라인 맞춤형 광고, 모바일 광고 등을 위한 개인 행태정보 생성 현상을 설명하지 못하고 있다. 그리고 개인정보 보호의 전체 영역에서 중요하게 다루어지고 있는 동의 문제와 정보보호 기술의 중요성이 증대되고 있는 최근의 보호 기술의 강화 추세를 설명하는 데에도 한계가 있다.

이 연구에서는 개인정보의 법적·기술적 특징은 물론 최근 변화하고 있는 개인정보 보호의 기술적 환경을 고려한 라이프 사이클 모델인 '개인정보 동의·관리 기반 모델'을 제시하고자 한다. 이 모델은 개인정보의 라이프 사이클 외에도 전체 사이클에 기반이 되는 개인정보의 법적 동의(Consent)와 개인정보 보호 기술을

고려하였다. 개인정보 동의·관리 기반 모델은 개인정보 보호의 범위와 특징은 물론 IT 기업의 IT 보안 컨설팅, 사내 보안 대책 수립, 내부 관리계획 수립 등 개인정보 보호 대책의 체계를 수립하는데 도움이 될 수 있다.

2 장에서 일반적인 개인정보의 라이프 사이클인 수집·저장·이용·파기 과정을 정리하였다. 3 장에서는 국내에서 활용되고 있는 개인정보의 라이프 사이클 모델 현황을 알아본다. 4 장에서는 3 장에서 도출된 모델들의 장·단점을 고려한 대안 모델인 개인정보 동의·관리 기반 모델을 제시한다. 마지막 5 장은 기존 모델과 새로 제시한 동의·관리 기반 모델을 현행 '정보통신망 이용 촉진 및 정보보호 등에 관한 법률'(이하 '정보통신망법'이라 한다)과 하위 규정인 '개인정보의 기술적·관리적 보호 조치 기준'에 적용하여 실제 상황에 얼마나 유용한 모델인지를 검토하였다.

1.2 이론적 배경

개인정보 보호를 체계적으로 분석하기 위한 연구로는 크게 프레임워크와 라이프 사이클 연구가 있다. 프레임워크 연구들은 이용자, IT 기업, 국가적 차원으로 나뉜다. 이용자 차원에서는 이용자의 아이디 관리(ID Management) 또는 동의 방법이 주로 연구되고 있다[21][25][31]. 기업 수준에서는 PiMI, PORTIA, ISTPA 등 모바일 또는 인터넷 환경의 데이터 보안과 프라이버시 원칙을 만족 시키는 프레임워크 개발 분야가 있다[9]. 국가적 차원에서는 Safe Harbor Framework, APEC Framework 등의 연구가 있다[19][32]. 국내에서는 주로 기업 차원의 프레임워크 개발이 연구되었으며 관련 연구로는 홍승필[18]과 송유진·이동혁[3]의 연구가 있다.

개인정보의 라이프 사이클 모델은 주로 국내에서 논의되고 있다. 국내에서 개발된 라이프 사이클 모델들은 특정한 연구 결과가 아니라 실무적인 차원에서 개발되었다는 특징이 있다. 따라서, 개발 목적에 따라 다양한 모델이 있으나 아직까지는 체계적이지 못한 수준이다. 관련 연구로는 한국정보보호진흥원[13] 및 Kang, Lee and Song[34]의 연구가 있다.

국외에서는 개인정보 흐름을 중요하게 인식하고 있지만 국내처럼 별도의 라이프 사이클 모델로 발전하고 있지는 못하다[23][33]. 예를 들면 미국, 캐나다, 호주, 영국 등은 개인정보의 영향평가 시 개인정보의 흐름 분석을 평가 요소 중 하나로 다루고 있으며, 개인정보 흐름도나 다이어그램을 작성하도록 하고 있다. 그러나 라이프 사이클을 만들어 분석하거나 특정 흐름 모델을 제시하고 있지는 않다[14][22][24][27~30].

1.3 연구의 범위 및 방법

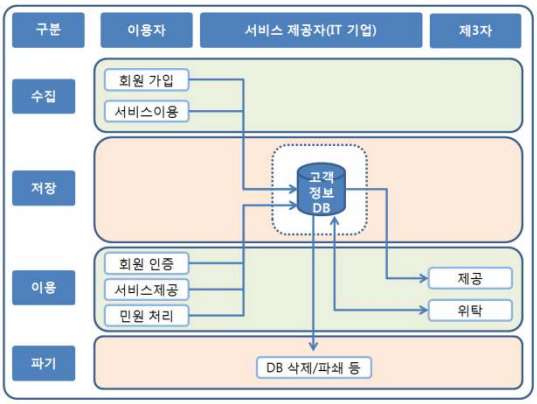
본 연구는 현재까지 개발된 개인정보의 라이프 사이클 모델들이 개인정보 보호 특성을 왜 정확히 설명하지 못하는가? 에 대한 문제의식에서 시작됐다. 따라서 현재까지 나와 있는 개인정보의 라이프 사이클 모델 현황 및 장·단점을 분석해 본 후 IT 활용 현실에 적합한 개인정보의 라이프 사이클 모델을 제시하고자 한다.

국내의 IT 기업에서 활용하고 있는 개인정보의 라이프 사이클 모델들을 대상으로 연구했다. 개인정보가 가지는 법적·사회적 정의와 보호 수준 등에 따라 나타날 수 있는 개인정보의 라이프 사이클 모델이 상이할 수 있으므로 동의·관리 모델의 적용 대상은 정보통신망법에 적용받는 민간 IT 기업으로 한정했다.

문헌연구(literature review)와 사례연구(case study)를 통해 정부 및 전문기관 등 규제기관에서 개발한 개인정보의 라이프 사이클 모델들을 분석했다. 분석 결과를 토대로 모델이 제시된 이유와 각 모델의 장·단점을 분석했다.

2. 개인정보의 라이프 사이클

개인정보는 이용자, 서비스 제공자인 IT 기업 및 제 3 자를 이해 당사자로 하고 있다. 이들 당사자들 사이에 발생하는 개인정보의 일반적인 라이프 사이클은 수집·저장·이용·파기 순이다. <그림 1>은 전형적인 개인정보 라이프 사이클 모델을 나타낸 것이다.



<그림 1> 개인정보의 라이프 사이클

개인정보의 라이프 사이클은 일반적으로 다음과 같이 설명되고 있다.

수집 단계: IT 기업은 이용자로부터 서비스 제공 또는 마케팅을 위해 개인 식별 정보를 수집한다. 개인 식별 정보에는 개인의 성명, 주민등록번호, 주소, 본적지, 출생지, 이메일 주소 등의 인적 정보를 포함한 신체적, 정신적, 재산적, 사회적 정보가 있다[1]. 이용자가 회원정보 등을 입력하고 웹사이트에 가입하거나 휴대전화의 개통을 위해 이동통신사 대리점에 가입 신청서를 제출하는 것이 수집 단계에 해당한다.

저장 단계: 이용자 등으로부터 수집한 개인정보는 DB 에 저장된다. 저장 단계에는 저장된 개인정보를 관리하는 내용도 포함된다. 관리란 개인정보보호 정책에 따라 권한이 부여된 취급자 등만이 개인정보를 활용할 수 있도록 하는 것이다. 여기에는 권한 관리, 암호화 등이 포함된다. 권한 관리는 취급자 수를 제한하기 위한 것이고, 암호화는 외부에 노출·유출되어도 개인정보를 알아 볼 수 없도록 하는 것이다[20].

이용 단계: 이용자로부터 수집 및 저장하여 보유하고 있는 개인정보는 회원 인증, 서비스 제공, 제품 홍보, 요금 정산, 제품 배달, 민원 처리 등에 사용된다. 이 외에도 개인정보를 제 3 자에게 제공하는 경우가 있다. 제 3 자 제공은 서비스 제공자의 특정 업무를 협력업체 등에 아웃소싱하는 '위탁'과 개인정보를 활용한 가치 창출을 위해 개인정보를 제 3 자에게 제공하는 '제휴'가 있다. 위탁의 경우

개인정보 관리 책임이 IT 기업에게 있고, 제휴는 개인정보를 제공 받은 제 3 자에게 있다.

파기 단계: IT 기업 등 서비스 제공자는 수집한 목적이 달성되면 개인정보를 즉시 파기해야 한다. 파기란 개인정보를 재생할 수 없도록 하는 것이다. 이용자가 회원 탈퇴를 하거나 IT 기업이 폐업하는 경우 또는 특정 이벤트가 종료되는 등의 경우가 파기 단계이다. 이 외에도 이용자가 동의를 철회하는 경우도 개인정보를 즉시 파기해야 한다. 파기에는 Structured Query Language(SQL) 명령어 등을 이용하여 DB 에서 데이터를 지우는 것은 물론 강력한 자기장을 발생시키는 디가우저(Degausser)를 활용한 하드디스크 파괴, 쇄절기를 이용한 문서의 파쇄 등 물리적 항목도 포함된다.

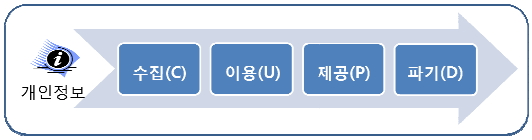
3. 개인정보의 라이프 사이클 모델 현황

개인정보의 라이프 사이클 모델은 사용 목적에 따라 다양하다. 국내에서는 법률적 측면에서 만들어진 'CUPD 모델' 및 'PIMS 모델'과 개인정보의 흐름 측면에서 만들어진 'CSUD 모델' 및 '영향평가 모델'이 있다. 참고로 지금까지 국내에서 활용하고 있는 개인정보의 라이프 사이클은 사용 영역은 존재하나 모델명이 없어서 필자가 논문의 편의를 위해 이름을 임의로 부여했다.

3.1. 법률 기반 모델

3.1.1 수집(C)·이용(U)·제공(P)·파기(D) 모델

<그림 2>의 수집(Collection)·이용(Use)·제공(Provision)·파기(Deletion) 모델(이하 'CUPD 모델'이라 한다.)은 정보통신망법의 개인정보 보호 규정 각 절 제목을 토대로 만들어졌다. 2001 년 7 월에 개정된 정보통신망법의 개인정보 보호 규정 제 4 장은 '제 1 절 개인정보의 수집', '제 2 절 개인정보의 이용 및 제공', '제 3 절 이용자의 권리' 순이었다. CUPD 모델은 제 1 절 제목을 그대로 가져오고 2 절의 제목을 분리하여 '이용'과 '제공' 단계를 만들었다. 마지막으로 라이프 사이클이라는 단어의 의미를 살리기 위해 제 1 절 하단에 있던 파기 부분을 별도로 분리했다.



<그림 2> CUPD 모델

CUPD 모델의 수집 단계는 수집 시 동의, 개인정보 수집 제한 등의 내용이 포함되어 있다. 이용 단계는 목적 외 이용 금지, 개인정보관리책임자의 지정, 개인정보의 보호조치로 구성되어 있다. 제공 단계는 동의 없는 제 3 자 제공 금지 및 개인정보 처리 위탁 규정, 영업의 양수 등의 통지 등을 다루고 있다. 마지막으로 파기 단계는 수집 또는 제공 받은 목적을 달성한 때에는 즉시 파기하는 내용으로 이루어져 있다[4]. <표 1>은 CUPD 모델의 세부 구성을 정리한 것이다.

<표 1>] CUPD 모델의 세부 구성

구분	내용
수집	개인정보의 수집 개인정보의 수집의 제한 등

이용	목적 외 이용 금지 개인정보관리 책임자 지정 개인정보의 보호조치
제공	동의 없는 제 3 자 제공 금지 개인정보의 위탁 규정 영업의 양수 등의 통지
파기	개인정보의 파기

CUPD 모델은 정보통신망법의 개인정보 보호 규정을 기반으로 하고 있다. 이 모델은 개인정보 보호 규정이 처음 만들어질 당시의 모델이므로 모델에 포함되는 세부적인 항목의 수가 적고 라이프 사이클에서 이용과 제공을 구분하고 있다는 것이 특징이다. 반면, CUPD 모델은 일반적인 개인정보 처리 프로세스를 반영하지 못하고 있다. IT 기업의 개인정보 흐름은 일반적으로 수집·저장·이용·파기 순이다. 특히, 개인정보의 흐름 단계 중 저장 단계를 라이프 사이클 모델에 포함시키지 않고, 이용 단계의 하위 개념에 포함시키고 있는 것은 문제이다. 이렇게 되면 CUPD 모델을 적용할 경우 SK 컴즈, 농협, Nexon, 현대캐피털 등의 해킹 사고가 개인정보 이용 과정에서 발생한 것으로 잘못 해석될 수 있다. 또한, 개인정보 보호에서 가장 중요한 동의 부분이 모델에서 다루어 지지 않고 있다. 동의는 개인정보 보호의 제 1 원칙이다. 동의는 개인정보의 라이프 사이클 전 영역에서 다루어져야 한다. CUPD 모델에서는 파기 단계를 개인정보의 이용 목적 달성 후 파기하는 경우로 한정한 것도 문제이다. 1997 년 7 월 정보통신망법의 개인정보 조항이 처음 만들어졌을 때 이미 이용자가 동의를 철회할 경우 수집한 개인정보를 지체 없이 파기하도록 하고 있다.

3.1.2 개인정보보호관리체계(PIMS) 모델

CUPD 모델은 개발 당시에는 유용했을지 모르지만 2007 년 1 월 26 일에 정보통신망법이 전면 개정되면서 활용도가 떨어진 모델이다. 최근에는 개정된 법령을 반영한 개인정보보호관리체계 (Personal Information Management Systems(PIMS), 이하 'PIMS'라 한다.) 모델을 더 많이 사용하고 있다. PIMS 란 IT 기업이 개인정보를 자율적으로 관리할 수 있도록 만든 인증 체계이다. PIMS 에서는 사업자가 개인정보 보호 수준을 인증하는 방법으로 <그림 3>의 개인정보의 라이프 사이클 모델을 활용하고 있다. PIMS 모델은 CUPD 모델과 같이 정보통신망법의 개인정보 보호 규정을 설명하기 위해 만들어졌다. CUPD 모델은 라이프 사이클이라는 단어의 의미를 살리기 위해 당시의 정보통신망법 제 1 절 하단의 파기 부분을 라이프 사이클에 포함시켰다. 반면, PIMS 모델은 정보통신망법의 개인정보 보호 규정의 각 절 제목을 수정 없이 라이프 사이클에 반영했다. 정보통신망법이 2007 년에 개정되었을 때 절의 제목은 '제 1 절 개인정보의 수집·이용 및 제공 등', '제 2 절 개인정보의 관리 및 파기 등'이다 [5].

<그림 3> PIMS 모델

PIMS 모델은 개인정보를 수집(Collection)·이용(Use)/제공(Provision)·관리(Management)/파기(Deletion)하는 3 단계

로 되어 있다. 개인정보 수집 단계는 최소의 개인정보 수집, 중요(민감)정보 수집 제한, 간접 수집 시 조치, 정보주체의 동의, 법정대리인의 동의획득 및 고지, 동의기록 보관, 취급방침 마련 등으로 되어 있다. 개인정보 이용/제공 단계는 목적 내 개인정보 이용, 이용자의 불만 처리, 열람정정 요구권 보장 및 처리, 동의 철회, 이용자 고지 및 동의, 위탁자 책임, 제 3 자 제공 시 동의, 제 3 자 보안 관리, 개인정보 이전 시 보호 조치, 해외 이전 시 보호조치 등을 포함하고 있다. 마지막으로 관리/파기 단계는 개인정보 파기 시 내부 규정을 마련하고 이에 따라 개인정보의 수집 목적이 달성된 경우 개인정보를 안전한 방법으로 지체 없이 파기하는 내용을 담고 있다[7]. <표 2>은 PIMS 모델의 세부 항목을 정리한 것이다.

<표 2> PIMS 모델의 세부 구성

구분	내용
수집	최소한의 정보 수집
	중요 정보 수집 제한
	간접 수집 시 조치
	정보주체의 동의
	법정대리인 동의획득 및 고지
	동의기록 보관
	개인정보취급방침
이용/제공	목적 내 개인정보 이용
	이용자의 불만 처리
	열람정정요구권 보장 및 처리
	동의철회
	이용자 요청의 처리
	이용자 고지 및 동의
	위탁자 책임
	외부위탁관리 감독
	외부위탁계약 관련사항
	제 3 자 제공 시 동의
	제공받은 개인정보의 관리
	제 3 자 보안관리
	제 3 자 제공 시 계약 관련사항
	개인정보 이전 시 보호조치
	개인정보 이전 받을 시 보호조치
	해외 이전 시 보호조치
관리/파기	개인정보의 저장 및 관리
	파기규정
	파기시점
	파기방법
	목적 달성 후 보유

PIMS 모델은 사업자가 정보통신망법의 의무 사항을 준수하고 있는 지를 인증하기 위해 개발되었다. PIMS 모델은 최근에 개발되어 현행 정보통신망법의 내용을 가장 잘 반영하고 있는 모델이기도 하다. 이 모델은 기존의 4 단계 모델을 1 단계 줄인 3 단계로 되어 있다. 따라서, 개인정보의 라이프 사이클 모델 중 가장 단순한 모델이다. 수집하는 개인정보에 간접 수집 시 조치 사항을 두어 쿠키, 위치정보 등 동적인 정보를 포함하여 수집 단계의 정보를 구체화 했다는 장점을 가지고 있다. 반면, PIMS 모델은 CUPD 모델과 동일한 단점을 가지고 있다. 최근에 개발된 모델임에도 개인정보에서 정보보호 기술이 차지하는 중요성을 간과하고 있기도 하다. 행태정보의 생성, SNS 이용의 보편화, 스마트폰 대중화에 따른 위치정보 정확도 증가와 같은 최근의 개인정보 현상 또한 반영하고 있지 못한 모델이다[10].

3.2 흐름 기반 모델

3.2.1 수집(C)·저장(S)/관리(M)·이용(U)/제공(P)·파기(D) 모델

<그림 4>의 수집(Collection)·저장(Storage)/관리(Management)·이용(Use)/제공(Provision)·파기(Deletion)모델(이하 'CSUD 모델' 이라 한다)은 개인정보 보호에서 정보보호 기술의 중요성이 부각되던 시기에 개발되었다[6]. CSUD 모델은 현재 '개인정보 생명주기별 보안 관리모델'로 한국정보통신기술협회 정보통신 단체 표준으로 제정되어 활용되고 있기도 하다[16].

<그림 4> CSUD 모델

CSUD 모델은 개인정보의 라이프 사이클을 4 단계로 분류하고 있다. 수집 단계는 인터넷 서비스 이용자의 서비스 이용신청과 동시에 자신의 개인정보를 IT 기업에게 제공하는 단계이다. 수집되는 개인정보는 성명, 연락처 등의 정적 정보 외에 위치정보, 인터넷 접속 기록 등의 동적 정보를 포함하고 있다. 저장/관리 단계는 수집된 개인정보를 DB 등에 저장하고 개인정보보호정책에 따라 허가 받은 자 만이 해당 개인정보에 접속할 수 있는 권한 관리 등을 다루고 있다. 이용/제공 단계는 개인정보 소유자의 개인정보를 여러 가지 필요에 의해 이용하는 것으로 위탁업체나 제휴업체 등 제 3 자에게 제공하는 내용을 포함하고 있다. 마지막으로 파기 단계는 해당 개인정보의 보유기간이 종료하여 파기하는 것을 말한다. 정적인 개인정보는 서비스 탈퇴 이후 동적인 개인정보는 전체 서비스 탈퇴 시점이 아닌 요청한 서비스가 종료되는 시점에 파기하는 것을 말한다. <표 3>는 CSUD 모델의 세부 내용을 정리한 것이다.

<표 3> CSUD 모델의 세부 구성

구분	내용
수집	서비스 이용신청과 함께 제공되는 정보 (정적 및 동적 정보를 포함)
저장/관리	개인정보를 DB 에 저장 허가 받은 자만이 개인정보에 접속
이용/제공	서비스 이용 제 3 자 제공과 위탁
파기	보유기간 종료 후 파기 (정적 정보는 해당 서비스 종료 후 파기)

CSUD 모델은 CUPD 모델과 달리 개인정보의 흐름을 기반으로 만들어졌다. 또한, 정보통신단체표준으로 되어 있어 개인정보의 라이프 사이클 모델 중 공신력이 가장 높다. 이 모델은 정보 보안 관리 모델을 위해 개발된 모델이므로 사업자의 보안 수준을 평가하고 정보보호 관점에서 필요한 조치를 취하기 쉽다는 장점이 있다. PIMS 모델과 같이 쿠키, 위치정보 등 동적인 정보를 포함하여 수집 대상을 확장하기도 했다. 또한 CUPD 모델에서 간과하고 있는 저장과 관리 단계를 강조했다는 점이 특징이다. 이 모델을 적용할 경우 IT 기업 입장에서는 DB 보안 솔루션, 개인정보에 대한 접근 권한 등 정보보호 기술의 적용이 쉽고, 해킹, 취급 부주의 등 보안 사고에 대한

분석 및 대처가 용이하다. 반면, CSUD 모델은 프로세스만을 고려하여 개인정보의 법적 특성을 설명하기 어렵다는 단점이 있다. 특히, 모델의 세부 사항은 너무 일반적인 사항으로 구성되어 개인정보 보호 규정 적용을 위해서는 별도의 법률 검토가 필요하다. 저장과 관리를 같은 단계에서 설명하고 있어 개인정보의 수집, 이용/제공, 파기 단계에서의 보안 등 기술적인 관리 부분을 간과하고 있는 점 또한 문제이며 CUPD 모델과 같이 개인정보의 동의와 철회 부분을 설명하지 못하고 있다는 단점도 가지고 있다.

3.2.2 개인정보 영향평가 모델

개인정보 영향평가(Privacy Impact Assessment(PIA))란 개인정보를 활용하는 새로운 개인정보 처리 시스템의 도입 및 기존 시스템의 중대한 변경 시 시스템의 구축·운영이 고객 및 국민의 프라이버시에 미칠 영향에 대하여 미리 조사·분석·평가하는 체계적인 절차이다[12]. 개인정보 영향평가는 개인정보파일을 신규 구축하거나, 기존에 구축된 개인정보파일의 취급 절차를 변경하거나, 개인정보 파일을 타 기관과 연계·제공하는 경우 등에 사용된다. '개인정보 영향평가 모델'은 CSUD 모델과 같이 개인정보의 흐름을 기반으로 한다. <그림 5>와 같이 이 모델은 수집(Collection)·보유(Retention)·이용(Use)/제공(Provision)·파기(Deletion) 단계로 되어있다. 또한, 2011 년 9 월 통합 '개인정보 보호법' 제정으로 인해 모든 공공기관은 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 개인정보 영향평가를 하도록 되어 있어 최근에 활용도가 가장 높은 모델이다[8].

<그림 5> 개인정보 영향평가 모델

개인정보 영향평가 모델에서는 개인정보의 라이프 사이클을 수집·보유·이용/제공·파기의 4 단계로 구분하고 있다[17]. 개인정보 수집 단계는 정보주체의 개인정보를 취득하는 단계로서 통상적인 웹사이트 회원 가입, 서면 신청서 작성, 민원 접수 등을 포함하고 있다. 보유 단계는 수집한 개인정보를 보유하는 단계로서 보유한 개인정보를 안전하게 관리하며 정보 주체의 개인정보 열람·정정 권리의 보장 등의 내용으로 되어 있다. 이용/제공 단계는 취득·저장한 개인정보를 수집한 공공기관 외의 제 3 의 기관에게 정보를 제공하는 행위 등을 포함한다. 마지막으로 파기 단계는 수집 및 이용 목적이 달성된 개인정보를 파기하는 단계이다. <표 4>는 '영향평가 모델'의 세부 내용이다.

<표 4> 영향평가 모델의 세부 구성

구분	내용
수집	웹사이트 회원 가입 서면 신청서 작성
보유	개인정보의 안전한 관리 개인정보 열람.정정 권리
이용/제공	취득·저장 개인정보의 제 3 자 제공
파기	수집 및 이용 목적 달성 정보의

파기

개인정보 영향평가 모델은 CSUD 모델과 같이 개인정보의 흐름을 기준으로 만들어졌다. 이 모델은 IT 기업 측면에서 자사의 시스템 전반을 분석하고 보안 등 대책을 수립하는데 활용도가 높다. 특히, 보유라는 개념에 저장과 관리를 모두 포함시켜 CSUD 모델에 비해 모델을 단순화 시켰다. 개인정보의 라이프 사이클 모델 중에 개인정보의 흐름을 가장 잘 표현하고 있는 모델이기도 하다. 반면, 영향평가 모델은 PIMS 모델과 같이 IT 기업에 의한 개인정보 생성을 다루고 있지 않다. 개인정보의 동의와 이용자 권리 부분인 철회 절차도 누락되어 있다. 보안 측면에서 만들어진 모델임에도 보안을 보유 단계에만 국한시켜 수집·이용/제공·파기 단계에서의 보안의 역할을 간과하고 있다는 단점도 있다.

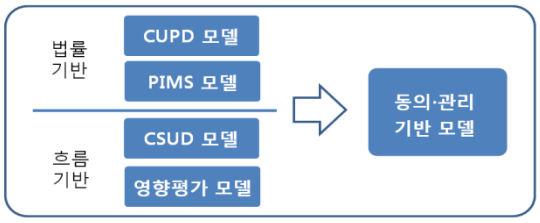
CUPD 모델과 PIMS 모델은 법률에 기반하여 만들어져 법률 적용이 쉬우나 프로세스 이해도가 떨어지는 문제가 있다. CSUD 모델과 개인정보 영향평가 모델은 개인정보 흐름 기반으로 만들어져 프로세스 이해도는 높으나 정보통신망법 상의 개인정보 보호 규정들과 연결시켜서 설명하기가 어렵다. 또한, 본 장에서 설명한 4 개의 라이프 사이클 모델 모두 동의와 철회를 모델에서 설명하고 있지 않고, 보안 및 관리 이슈를 제한된 영역에서만 설명하고 있다는 단점이 있다. <표 5>는 지금까지 설명한 개인정보의 라이프 사이클 모델의 장·단점을 정리한 것이다.

4. 개인정보 동의.관리 기반 모델

<표 5> 라이프 사이클 모델 비교

모델	장점	단점	적용 분야	공통적 한계
CUPD	법률 적용이 쉬움 모델이 단순함	저장 단계 설명이 곤란 프로세스 이해도가 낮음	법률측면	'동의'와 '철회'를 모델에서 설명하고 있지 않음
PIMS	법률 적용이 쉬움 최신 법률 개정 사항을 반영	프로세스 이해도가 낮음		
CSUD	프로세스 이해도가 높음 보안 기술 적용도가 높음	법률 적용이 곤란	흐름측면	모든 단계를 아우르는 보안 문제를 제한적인 단계에서만 설명
영향평가	프로세스 이해도가 높음 보안 기술 적용도가 높음	법률 적용이 곤란		

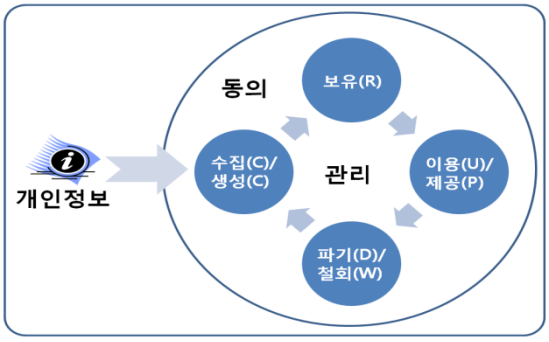
3 장에서 살펴본 개인정보의 라이프 사이클 모델 중 개인정보의 법적·기술적 특성을 모두 반영하고 있는 모델은 없다. 따라서, 법률과 개인정보의 흐름은 물론 보안을 포함한 관리까지를 고려한 '개인정보 동의·관리 기반 모델'로 발전하는 것이 바람직하다. <그림 6>는 개인정보의 라이프 사이클 모델의 발전 방향이다.



<그림 6> 라이프 사이클 모델의 발전 방향

동의·관리 기반 모델은 개인정보 흐름 기반 모델의 일반적 프로세스인 수집·보유·이용·파기 단계를 기반으로 한다. 여기에 최근의 기술 발전 방향을 고려하여 일부 항목을 수정·보완하는 방향으로 모델을 제시했다. 이전 모델에서 중요하게 고려하고 있지 않은 동의와 관리를 라이프 사이클 전체와 연관지어 설명했다. 파기 부분에서 간과하고 있는 이용자의 동의 철회 부분은 파기 부분에서 같이 기술했다. <그림 7>은 개인정보 동의·관리 기반 모델 개념도이다.

개인정보 동의·관리 기반 모델은 세부적으로 다음과 같이 기술할 수 있다.



<그림 7> 개인정보 동의·관리 기반 모델

수집/생성 단계: 기존 모델에서는 수집을 이용자가 제공하는 개인정보 만으로 국한시켰다. 그러나 IT 기업은 이용자 PC 의 쿠키정보를 수집하거나 검색결과, 접속지 IP, 스마트폰 위치 등의 행태정보를 수집하고 있다. 따라서, 수집 단계에서는 이용자에 의한 수집 외에 사업자에 의한 수집을 포함시키는 것이 바람직하다.

보유 단계: 이용자 또는 타인으로부터 제공된 개인정보는 IT 기업의 DB 에 저장된다. 이 외에 IT 기업은 이용자를 프로파일링하여 새로운 개인정보를 생성하기도 한다. 일부 모델에서는 보유 단계를 저장 또는 보유로 정의하고 있다. 두 단어의 사전적인 차이는 거의 없으나 이 논문에서는 IT 기업이 능동적으로 개인정보를 생산하는 내용이 포함되어 있으므로 저장 보다는 '보유'를 사용하기로 한다.

이용/제공 단계: 이용 단계에서는 IT 기업이 자사의 서비스 등을 위해 개인정보를 이용하는 단계이다. 차이가 있다면 이전의 모델에서는 서비스 만을 위한 것으로 이용 단계를 제한했으나 최근에는 개인정보의 생성을 위해서도

개인정보를 이용하고 있다는 점이다. IT 기업의 개인정보 활용이 증가함에 따라 제공 단계도 복잡해지고 있다. 그러나 이전 모델에서 설명하고 있는 개인정보의 이용과 위탁, 제 3 자 제공의 범주 안에 포함되는 수준이다.

파기/철회 단계: 사업자가 수집·저장·이용/제공한 개인정보는 목적이 달성되면 파기해야 한다. 이 외에도 이용자의 철회 요구에 의해 개인정보 수집·이용/제공 목적이 달성되지 않았음에도 불구하고 해당 개인정보를 파기해야 하는 경우도 있다. 이 경우도 개인정보를 복구할 수 없도록 완전히 파기해야 한다. 파기와 철회는 사용하는 목적이 다르므로 단계를 파기와 철회 둘 다 사용하는 것이 바람직해 보인다.

전체 라이프 사이클 모델에서 빠져 있거나 일부만 표현하고 있는 동의와 관리를 모델에 반영한다. 동의와 관리는 라이프 사이클 전반과 관련이 있다. 동의는 개인정보 수집 과정 중 일부로 생각하는 경우가 많다. 그러나 수집 단계 외에 이용 단계에서는 제 3 자 제공 및 위탁 단계에서 동의하고, 삭제 단계의 경우도 이용 목적이 달성된 개인정보의 파기도 동의와 관련이 있다. 정보통신망법 제 22 조에서도 개인정보 수집 시 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목, 개인정보의 보유·이용 기간을 명시하고 동의를 받도록 하고 있다. 수집·이용 목적은 개인정보의 라이프 사이클의 이용·제공 단계에 해당한다. 개인정보의 보유·이용 기간은 저장·파기 단계에 해당한다.

관리는 개인정보의 저장 단계 중 일부로 간주하는 경우가 많다. 그러나 개인정보 수집 시는 개인정보의 해킹 방지를 위해 Secure Socket Layer(SSL) 또는 TLS(Transport Layer Security(TLS) 등의 기술이 적용된다. 이용 단계에서의 SSL/TLS 적용 및 취급 사업자에 대한 관리, 개인정보 제공 시 기술적 조치 항목도 관리에 해당한다. 삭제의 경우도 DB 에서의 개인정보 삭제는 물론 저장 매체인 하드디스크 파괴, 문서 파쇄 등이 관리와 관련이 있다. 따라서 동의와 관리는 라이프 사이클 전반을 포함할 수 있도록 모델을 구현하는 것이 바람직하다.

관리의 대부분이 정보보호와 관련이 있어서 보안 또는 정보보호라는 개념을 사용할 수도 있다. 그러나, 취급 사업자 관리 및 현행법상 기술적 조치 외에 관리적 조치도 의무화하고 있고 있으므로 포괄적인 의미인 관리를 사용하는 것이 타당하다.

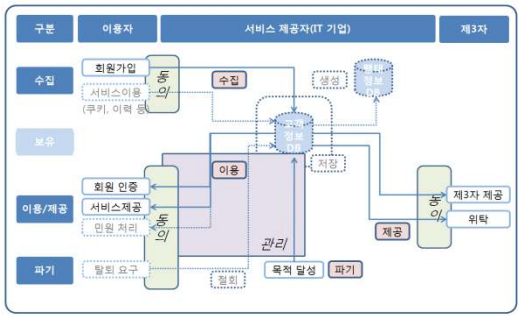
모델의 구성에 있어서는 라이프 사이클의 의미를 살리고, 동의는 외부, 관리는 내부와 관련이 있다는 것을 강조하는 측면에서는 모델을 원형으로 구현하는 것이 바람직해 보인다. 다만, 이는 편의상의 구분으로 동의나 관리는 IT 기업 환경의 내·외부와 관계가 있는 요소이다.

<표 6>은 동의·관리 모델을 동의와 관리 관점에서 정리한 것이다. 정리를 위해 활용된 개인정보 보호 규정은 정보통신망법과 동법의 하위 조항인 개인정보의 기술적·관리적 보호 규칙이다.

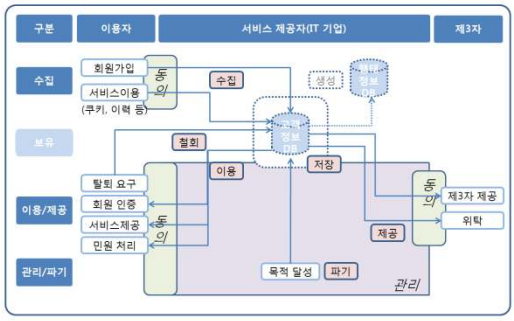
5. 동의·관리 기반 모델의 적용

IT 기업의 개인정보 활용 환경을 3 장에서 설명한 모델에 적용해 보면 <그림 8>, <그림 9>, <그림 10>, <그림 11>과 같이 나타낼 수 있다. 그림은 각 연구자의 분류에 따라 다르게 구현될 수 있으나 본 연구에서는 가능하면 라이프 사이클 모델의 원문 내용을 최대한으로 고려하려 노력했다.

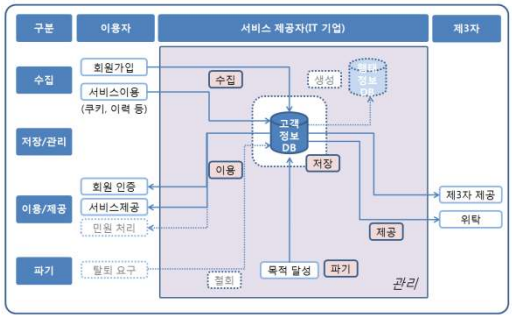
이들 모델들은 라이프 사이클에서 개인정보의 저장 부분의 설명이 누락되어 있거나 개인정보 수집에서 법적 동의 부분이 빠져 있는 등의 문제점을 보이고 있다. 따라서 기존의 모델들을 이용할 경우 개인정보 보호 전체를 체계적으로 이해하고 설명하는 데에 한계가 있다.



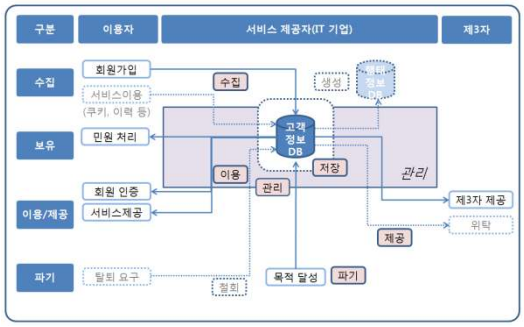
<그림 8> IT 기업 환경에 CUPD 모델 적용



<그림 9> IT 기업 환경에 PIMS 모델 적용

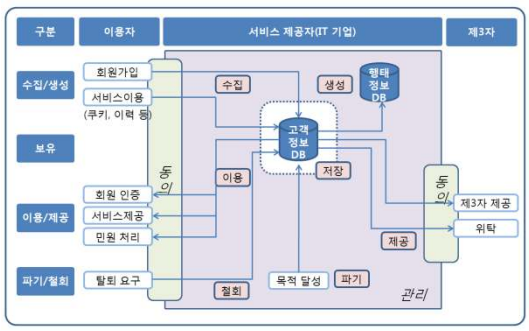


<그림 10> IT 기업 환경에 CSUD 모델 적용



<그림 11> IT 기업 환경에 영향평가 모델 적용

반면, 4 장에서 설명한 <그림 12>의 개인정보 동의·관리 기반 모델을 IT 기업의 개인정보 활용 환경에 적용해 보면 동의와 관리를 기반으로 수집/생성, 보유, 이용/제공, 파기/철회의 전체 영역이 포함됨을 알 수 있다. 따라서 다른 모델에 비해 IT 환경에 적용했을 경우 적합도가 높은 모델임을 알 수 있다.



<그림 12> IT 기업 환경에 개인정보 동의.관리 기반 모델 적용

<표 6> 동의·관리 기반 모델에 따른 개인정보 라이프 사이클

<table>
<tr><th colspan="2">구분</th><th>수집</th><th>보유</th><th>이용/제공</th><th>파기/철회</th></tr>
<tr><td rowspan="3">법률</td><td>조항</td><td>주민번호 등 민감정보 수집 금지
최소정보 수집
주민번호 대체 수단 마련
접속정보파일 자동 생성</td><td>개인정보 누출 통지제
목적 달성된 개인정보 별도 보관</td><td>목적외 이용 금지
필수정보외 수집 시 서비스 제공 거부 금지
주민번호 이용 금지
취급위탁사실 고지
양수양도에 따른 개인정보 이전
국외 개인정보 이전
수탁자의 손해배상 책임 의제
이용내역 통지
열람 및 제공 오류의 수정</td><td>파기 절차 및 방법
이용기간 통보제
이용 및 보유기간 후 즉시 삭제
이용 철회 요구 시 개인정보 삭제</td></tr>
<tr><td rowspan="2">동의</td><td colspan="4">수집.이용.제공 등의 동의 철회권, 법정 대리인의 동의</td></tr>
<tr><td>수집 시 사전 동의</td><td>보유 및 이용 기간, 보유 항목</td><td>제 3 자 제공 동의
취급위탁시 동의</td><td>이용목적 달성 후 파기</td></tr>
<tr><td rowspan="2">보안 및 관리</td><td>조항</td><td>SSL
비밀번호 룰 설정</td><td>DB 암호화
차단시스템의 설치
주민번호 저장금지
접속기록 위변조 방지</td><td>SSL
취급사업자 관리.감독</td><td>DB 삭제
HDD 파괴
문서 파쇄</td></tr>
<tr><td>공통</td><td colspan="4">관리 책임자 지정, 취급방침 공개, 고충처리, 누설 금지, 취급자 최소화, 내부관리계획의 수립, 백신소프트웨어 설치</td></tr>
</table>

6. 결론

이 연구에서 검토한 CUPD 모델과 PIMS 모델은 법률을 설명하거나 적용하기 위해 개발되었다. CSUD 모델과 개인정보 영향평가 모델은 IT 기업이 정보보호 관점에서 개인정보를 보호하기 위해 개발되었다. 개인정보 라이프 사이클이 이렇게 특정 목적에 따라 개발됨에 따라 개인정보의 법적 특성과 기술적 특성을 설명하는데 일정부분 한계를 보이고 있다. 특히, 동의와 관리 단계가 개인정보 전체 라이프 사이클과 연관이 있는 중요한 개념임에도 불구하고 일부 라이프 사이클 단계에서만 설명이 되고 있다. 이 연구를

통하여 위에서 언급한 문제점들을 반영한 새로운 개인정보의 라이프 사이클 모델인 개인정보 동의·관리 모델을 제시했다.

동의·관리 모델은 개인정보가 수집·저장·이용·파기 되는 전체 개인정보 프로세스를 기반으로 최근의 개인정보 보호 환경 변화를 고려한 모델이다. 이 모델은 라이프 사이클을 수집/생성·보유·이용/제공·파기/철회 단계로 구분하고 사이클을 선형이 아닌 원형 모델로 정의했다. 또한, 개인정보 전체 프로세스와 관련이 있는 동의와 관리 부분을 강조했다. 동의는 외부 환경과 관련이 있으므로 라이프 사이클 모형의 외부에 위치하게 함으로써 환경에 영향을 받는 요소임을 나타냈다. 관리는 모형의 안쪽에 놓음으로써 IT 기업의 내부 환경 및 기술과 관련이 있는 항목임을 표현했다. IT 기업의 개인정보 활용 환경에 모델들을 대입해 본 결과 새로 제시한 동의·관리 모델이 다른 모델에 비해 현실 환경에 더욱 더 들어맞는 것을 하였다.

개인정보 보호 특성과 최근의 개인정보 보호 환경을 고려한 동의·관리 모델이 제시됨에 따라 IT 기업은 자사의 개인정보 관리 대책, 사내 개인정보 감사, 개인정보 영향 평가 등에 본 모델의 활용이 가능하다. 다만, 동의·관리 모델은 기존의 모델에 비해 복잡하다는 단점이 있다. 이는 기존 모델들이 간과하고 있던 내용들을 동의·관리 모델에 적극 반영했기 때문이다. 또한, 개인정보의 특성상 개인정보를 정의하고 있는 특정 법률을 기반으로 모델을 구성해 IT 기업을 제외한 다른 분야에서 적용에 제한을 받을 수 있다는 점과 한국의 상황에만 적합한 모델이라는 점이 한계이다. 따라서 향후에는 동의·관리 모델을 일반적인 개인정보 보호 환경을 고려하여 수정하는 후속 연구가 필요해 보인다.

참고문헌

[1] 방송통신위원회.한국인터넷진흥원, 정보통신서비스 제공자를 위한 개인정보보호 가이드, 2009 년 12 월

[2] 백윤철.이창범.장교식, 개인정보보호법, 한국학술정보(주), 2008.

[3] 송유진.이동혁, "개인정보의 라이프 사이클에 따른 프라이버시 보호 프레임워크," 한국정보보호학회지, 제 16 권 제 4 호, pp.77-86, 2006. 8 월

[4]「정보통신망이용촉진및정보보호등에관한법률」제 4 장, 2001. 7 월 개정.

[5]「정보통신망이용촉진및정보보호등에관한법률」제 4 장, 2007. 1 월 개정.

[6] 정보통신부, u-프라이버시 환경 구축을 위한 개인정보보호기술 개발 추진 방향(중장기 기술개발 계획(안)), 2005. 12.

[7] 한국인터넷진흥원, 개인정보보호관리체계 인증준비 안내서(사업자용), 2010. 12.

[8] 한국인터넷진흥원, 「개인정보법」 조문별 설명자료, 2010 년 4 월.

[9] 한국인터넷진흥원, 개인정보 보호 프레임워크 개발, 2009.

[10] 한국인터넷진흥원, “빅데이터 시대, 새로운 가능성과 해결과제”, 인터넷 & 시큐리티 이슈, 2012 년 2 월.

[11] 한국인터넷진흥원, 유비쿼터스 환경에서의 개인정보 활용 및 보호방안 연구, 2009.
[12] 한국정보보호진흥원, 개인정보 영향평가 기준 정비 방안에 관한 연구, 2005.
[13] 한국정보보호진흥원, 개인정보의 안전한 수집, 저장 및 관리, 이용, 제공, 파기를 위한 개인정보 관리모델 연구, 2006 년 12 월.
[14] 한국정보보호진흥원, 해외 주요국가 개인정보 영향평가제도 연구, 2008.
[15] 한국정보사회진흥원, “新가치창출 엔진, 빅 데이터의 새로운 가능성과 대응 전략”, IT & Future Strategy, 제 18 호, 2011.
[16] 한국정보통신기술협회, 정보통신단체 표준 개인정보 생명주기별 보안 관리모델, TTAS.KO-12.0063, 2007. 12.
[17] 행정안전부.한국인터넷진흥원, 공공기관 개인정보 영향평가 수행안내서, 2011.
[18] 홍승필·이철수, "유비쿼터스 컴퓨팅 환경내 개인정보보호 프레임워크 적용 방안," 한국정보보호학회논문지, 제 16 권 제 3 호, pp.157-164, 2006. 6 월
[19] APEC, APEC Privacy Framework, 2005.
[20] Cary Meltzer & Doris Baker, Cryptography Decrypted, 2001.
[21] Hassina Meziane·Salima Benbernou, "A dynamic privacy model for web services," Computer Standards & Interfaces 32, pp.288-304, 2010.
[22] Homeland Security, Privacy Impact Assessments: The Privacy Office Official Guidance, June 2010.
[23] Huanchun Peng·Jung Gu, "Towards Compliance and Accountability: a Framework for Privacy Online," Journal of Computer, VOL.4, No.6, pp.494-501, JUNE 2009.
[24] Information Commissioner's office, The ICO Privacy impact assessment handbook, 2007.
[25] Maryam Jafari-Lafti·Chin-Tser Huang·Csilla Farkas, "P□F: A User-Centric Privacy Protection Framework", 2009 International Conference on Availability, Reliability and Security, IEEE, pp.386-391, 2009.
[26] Mary-Anne Williams, "Privacy Management," the Law & Business Strategies, 2009 International Conference on Computational Science and Engineering, pp.60-67, 2009.
[27] Office of the New Zealand Privacy Commissioner, Privacy Impact Assessment Handbook, 2002.
[28] Office of the Privacy Commissioner (Australian Government), Privacy Impact Assessment Guide 2006, 2006.
[29] Roger Clarke, “Privacy impact assessment: Its origins and development,” Computer Law & Security Review 25, pp.123~135, 2009.

[30] The Treasury Board Secretariat of Canada, Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks, 2007.

[31] U. Jendricke and D. tom Markotten, "Usability Meets Security - the Identity Manager as Your Personal Security Assistant for the Internet," the 16th Annual Computer Security Applications Conference, pp.344-351. 2000.

[32] U.S. DOC, Safe harbor, 2000.

[33] Weider D. Yu·Sharanya Doddapaneni·Savitha Murthy, "A Privacy Assessment Approach for Serviced Oriented Architecture Applications," Proceedings of Second IEEE International Symposium on Service-Oriented System Engineering(SOSE'06), IEEE, 2006

[34] Yeonjung Kang·Hyangjin Lee·Kilsoo Chun·Junghwan Song, "Classification of Privacy Enhancing Technologies on Life-cycle of Information," International Conference on Emerging Security Information, Systems and Technologies, IEEE, pp.66-70, 2007.

[35] 김범수 외 13 명, 스마트 시대 정보보호 전략과 법 제도, 2011.