홍 승 필 교수지도

석사학위청구논문

법·제도 기반의 개인정보 보호 및 제어 모델 설계 및 구현

2010

성신여자대학교 대학원

컴퓨터학과

정 지 희

법·제도 기반의 개인정보 보호 및 제어 모델 설계 및 구현

홍 승 필 교수지도

이 논문을 석사학위논문으로 제출함

2010년 5월

성신여자대학교 대학원

컴퓨터학과

정 지 희

인 준 서

정지희의 석사학위 논문으로 인준함.

심사위원 홍 승 필 인

심사위원 서 동 수 인

심사위원 홍 의 석 인

성신여자대학교 대학원

논 문 개 요

정보통신기술의 발달로 생활의 편리함과 유익성이라는 혜택이 제공되고 있지만, 이에 따른 역기능 문제로 인한 피해는 계속 증가하면서 정보화 사회에 대한 사람들의 우려가 가중되고 있다. 특히 개인정보 측면에서 정보의 오남용 및 불법 유출 등의 크고 작은 범죄의 표적이 되면서 개인의 정신적, 금전적 피해뿐 아니라 정보화 사회에 대한 불신으로 이어지는 심각한 상황을 야기하고 있다. 이에 국회와 행정부에서는 개인정보 관련 법안을 발표하고 있지만, 각처에 흩어져 있어 법규 간에 상충되는 부분이나 보호받지 못하는 부분이 존재하고, 더욱이 기술적 측면에서 개인정보를 보호하기 위한 표준화 대안은 미비한 실정이다.

이에 본 연구에서는 현존하는 개인정보보호에 관한 법률을 기반으로 개인정보를 보호하는 엔진을 제안한다. 특히 본 논문에서 개인정보보호 정책 엔진과 개인정보 접근제어 기능에 대해 중점적으로 다룬다. 이를 위해 현존하는 개인정보의 정의 및 개인정보를 보호하기 위한 제도적, 법적, 기술적인 방안을 연구하였다. 이를 기반으로 개인정보를 다루는 기관 및 기업의 주체별 구분과 해당 법률 및 국외 정책 분석하고, 법률 보호 하에 개인정보를 관리할 수 있는 방안 구축하였다. 또한 개인정보의 중요도에 따른 등급 구분과 이에 접근하는 사용자를 목적과 역할에 따라 차별화된 권한을 부여하여 개인정보를 접근제어 하도록 한다.

본 시스템을 통해 분산 환경 내 개인정보의 유통 및 관리가 법 기반으로 보다 안전한 환경에서 이루어지게 함으로써, 개인정보의 오•남용을 방지할 수 있는 방안이 될 것이다.

목 차

표 목 차

그 림 목 차

I. 개인정보 개요

1.1. 개인정보 정의

일반적 의미에서의 개인정보

일반적 의미에서 '개인정보'는 이름, 주민등록 번호, 주소 등 개인에 대한 일반적 정보뿐만 아니라, 가족정보, 학력, 병력, 소득, 의료, 정보, 사상, 취미 등 인적 정보 일체를 의미한다. 좁은 의미로서 지문, 홍채, 주민등록번호, 나이, 신장, 등 직접적으로 또는 여러 개의 개인정보를 조합하여 한 개인을 식별할 수 있는 개인정보를 의미한다.

'정보통신망법'에서의 개인정보

'정보통신망이용촉진및정보보호등에관한법률' 제2조 제1항 제6호는 '개인정보'를 생존하는 개인에 관한 정보로서 성명. 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호. 문자. 음성. 음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)라고 정의하고 있다. 즉 이는 특정 개인의 주체성을 식별할 수 있는 일체의 정보를 의미한다고 볼 수 있다.

'개인정보보호법'에서의 개인정보

또한 '공공기관의개인정보보호에관한법률' 제2조제2호는'개인정보'를 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함)라고 정의하고 있다.

이 법에서도 역시 개인정보는 개인의 정신, 신체, 재산, 사회적 지위, 신분 등에 관한 사실·판단·평가를 나타내는 공공기관의 컴퓨터에 의하여 처리되는 개인 식별이 가능한 일제의 개인정보를 의미한다. 여기에서 컴퓨터로

처리되는 개인정보의 범위 안에는 컴퓨터 내에 기록된 정보뿐만 아니라 입출력 물에 기록된 정보도 대상에 포함된다고 본다. 또한 개인정보의 집합체(개인정보화일)가 아닌 하나하나 낱개의 개별적 개인정보 사항이나 복제물, 컴퓨터 처리와 병행하여 수작업으로 처리 중인 정보도 역시 개인정보의 대상에 포함된다.

이밖에도 전자서명법 등의 개별법에서도 개인정보를 위와 동일하게 정의하고 있다. 또한 전기통신법, 신용정보의이용및보호에관한법를, 의료법 등의 개별법에서도 개인정보와 관련한 규정을 두고 있다.

국외에 있어서는 각 나라마다 그 사회문화의 발전 과정이 서로 다르고, 개인정보에 접근하는 사고방식이 다르기 때문에 개인정보에 관한 기본적 사상은 서로 상이할 수 있다. 그러나 개인정보가 무엇을 의미하는 것인가에 관한 정의는 이하에서 확인하는 바와 같이 서로가 거의 유사하다.

이러한 개인정보를 유형별로 정리해보면 [표 1]과 같다. 향후 유비쿼터스 환경에서는 개인정보의 유형이나 그 대상이 정보주체자체 뿐만 아니라, 물품정보 및 위치정보 등을 통한 개인의 라이프스타일까지 개인별 정보 파일로 정리되고 구체화 될 것으로 예상된다.[26]

[표 4] 개인정보의 유형

구분	개인정보유형
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 학교성적, 기술 자격증 및 전문 면허증, 이수한 훈련 프로그램, 동아리 활동, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등
소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득

기타수익 정보	보험(건강, 생명 등) 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격 테스트결과, 직무태도
법적정보	전과기록, 자동차교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(e-mail), 전화통화내용, 로그파일(log file), 쿠키(cookies)
위치정보	GPS나 휴대폰에의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

국외에서의 개인정보 정의

각국의 개인정보에 관한 법률상의 정의는 서로 상의하나, 공통적으로 “개인에 관한정보”(Personal Data)를 말하고 있으며, 정리하여 보면 개인정보는 식별된 또는 식별 가능한 개인에 대한 정보라고 정의할 수 있으며 구체적인 개인정보관련 해외규범에서의 정의는 아래 [표 2]와 같이 정리할 수 있다. [14]

[표 5] 국외 개인정보 정의

[주체] 출처	내용
[OECD] 개인정보 가이드라인	식별된 또는 식별가능한 개인(정보주체)에 관한 정보
[EU] '95 개인정보보호 지침	식별된 또는 식별가능한 자연인(정보주체)에 관한 정보, 단 식별가능한 사람은 특히 신원증명번호 또는 육체적· 심리적·정신적, 경제적 문화적 또는 사회적 신원 중 하나 이상의 요인을 참고하여 직접적 또는 간접적으로 식별될 수 있는 사람을 말함
[홍콩] 개인정보법	생존하는 개인에게 직접적 또는 간접적으로 관련되어 있고, 직접 또는 간접적으로 개인의 신원을 확인하기 위하여 이용할 수 있으며, 해당 정보에 대한 접근이나 처리가 이루어질 수 있는 형태의 정보

[일본] 개인정보의 보호에 관한 법률	생존하는 개인에 관한 정보로서 당해 정보를 포함하는 성명, 생년월일, 기타 기술 등에 의해 특정한 개인을 식별하는 일이 가능한 정보(다른 정보와 용이하게 결합하여 그에 의해 특정한 개인을 식별하는 것이 가능한 경우도 포함)
[영국] 정보보호법	해당정보 또는 해당정보와 정보 관리자가 소유하거나 소유하게 될 다른 정보를 결합하여 식별될 수 있는 생존 개인에 대한 정보
[캐나다] 프라이버시법	기록된 형태에 관계없이 식별가능한 개인에 관한 정보

1.2. 개인정보 위험분석

개인정보분쟁조정위원회에 접수되는 개인정보침해 관련 민원은 지속적으로 증가하는 추세를 나타내고 있다. 피해신고가 증가한 원인으로는 정보사회가 발달됨에 따라 사회 각 분야에서 인터넷과 정보통신기술의 사용이 일상화됨에 따라, 개인정보는 과거의 단순한 신분정도에서 오늘날에는 전자상거래, 고객관리, 금융거래 등 사회의 구성, 유지, 발전을 위한 필수적인 요소로 기능하면서 그 활용도가 높아짐에 있다. 또한 개인정보는 기업의 입장에서도 수익창출을 위한 재산적 가치로서 높게 평가되고 있으며, 정부와 공공기관에서도 각각의 통계나 정책자료로 쓰이면서 활용도가 높아지고 있다.

이러한 기업, 공공내의 개인정보 사용과 특성에 따른 침해 원인에 대해 살펴보면 다음의 [표 3]과 같다.

[표 6] 개인, 기업, 공공분야별 개인정보의 특성과 침해원인

	개인정보의 특성	개인정보 침해원인	개인정보 침해발생
개인	•개인정보 제공은 사이버 활동의 필수 요건 •개인정보를 자산, 재화로 인식	•타인 정보 사용에 대한 욕구(익명성) •웹 2.0 등장으로 인한 정보의 공개 공유 증가(블로그, UCC, P2P)	•주민번호 등 개인정보 도용 •고객정보 해킹 및 음성적 거래 •P2P 등에서의 개인정보 노출
기업	•타겟 마케팅, CRM 활용 •개인정보 확보는 경쟁력의 핵심	•인식 및 관리 부주의 •주민번호 수집 관행화 •통신시장 포화, 시장 경쟁 과열	•주민번호 등 개인정보 노출 •내부 직원 및 영업점에의 유출 •개인정보의 불법 수집 및 제공
공공	•서비스 고도화로 정보 활용 증가 •개인정보의 수집, 활용 형태가 민간 기업과 유사하게 진행	•인식 및 관리 부주의 •서비스 효율화를 위해 개인정보의 무단 활용을 문제 삼지 않는 풍토	•개인정보의 노출 •내부 취급자에 의한 유출

한국인터넷진흥원 개인정보침해신고센터에서 접수된 개인정보 침해건수와 개인정보 침해신고 상담건수를 살펴보면 '2008년 개인정보분쟁조정위원회에 접수된 개인정보 침해신고 상담건수는 총 39,811건으로 조사되었다.(아래 [표 4]) 이는 전년도 2000년에 접수된 2,035건과 비교하여 20배가량 증가한 수치로서, 개인정보침해 관련 민원이 꾸준히 증가하였음을 알 수 있다.

[그림 1]개인정보 침해건수

개인정보 침해 건수에 따른 유형별 건수를 분석한 것은 아래의 [표 3]과 같다. 2008년도 개인정보 침해건수를 살펴보면 총 39,811건으로 전년대비 약 53.3%가 증가하였다. 이 중 “신용정보침해 등 정보통신망법 적용대상 이외의 개인정보침해” 사례가 24,144건(60.6%)로 가장 많았으며, 전년도와 비교해 보면 약 93%가 증가함을 알 수 있다. 정보통신망법 적용 범위 내에서는 ‘주민번호 등 타인정보 훼손, 침해, 도용’ 사례가 10,148건(25.9%)로 가장 많았으며, 이는 전년도와 비교해서는 1,062건이 증가한 수치이다.

[표 3] 개인정보 침해 유형

구분	2004년	2005년	2006년	2007년	2008년
합계	17,569	18,206	23,333	25,965	39,811
개인정보 무단수집	564	1,140	2,565	1,166	1,129
개인정보 무단이용제공	784	916	917	1,001	1,037
주민번호 등 타인정보도용	9,163	9,810	10,835	9,086	10,148
회원탈퇴 또는 정정 요구 불응	2,312	771	923	865	949
법적용 불가 침해사례	2,768	4,401	6,355	12,497	24,144
기타	1,978	1,168	1,738	1,350	2,404

1.3. 개인정보보호 필요성

1970년 이후부터 세계적으로 개인정보의 유출 등과 관련하여 사생활의 보호의 필요성을 인식하게 되었고, 이에 OECD 국가들을 중심으로 국내법 차원에서 정보유출을 규제하기 시작하였다. 이러한 정보통신의 발달로 인한 정보환경의 변화가 개인정보와 관련하여 인간다운 생활의 보호 및 사생활 보호의 필요성이라는 새로운 제도적•법적 문제를 던져주었음을 잘 보여주고 있다.

국내에서도 여러 법률에서 개인정보보호에 관한 법률이 제정되었고, 2009년 개인정보의 기술적・관리적 보호조치를 위한 법률도 개정되었다. 아래의 [표 5]는 개정된 기술적・관리적 기준 개요를 나타낸다. [31]

[표 8] 개인정보의 기술적·관리적 보호조치 기준 개요

구 분	개인정보의 기술적 · 관리적 보호조치 기준
목 적	● 정보통신서비스 제공자등이 이용자의 개인정보를 취급함에 있어서 개인정보가 분실 · 도난 · 누출 · 변조 · 훼손 등이 되지 아니하도록 안전성을 확보하기 위함
관련 근거	● 법 제28조(개인정보의 보호조치) ● 법 시행령 제15조(개인정보의 보호조치)
주요 내용	● 이용자 개인정보의 안전한 취급을 위한 내부관리계획의 수립 · 시행의 보호조치 ● 이용자 개인정보에 대한 불법적인 접근을 차단하기 위한 접근통제 규칙, 침입차단시스템 및 침입탐지시스템의 설치 · 운영 등 보호조치 ● 개인정보취급자의 개인정보처리시스템에 대한 접속기록의 위조 · 변조 방지를 위한 보호조치 ● 이용자의 개인정보가 안전하게 저장 · 전송될 수 있도록 보호조치 ● 악성 프로그램의 침투 여부를 항시 점검 · 치료할 수 있도록 백신소프트웨어의 설치 · 운영 등 보안 조치 ● 기타 개인정보의 안전성 확보를 위해 필요한 보호조치
대상 사업자	● 정보통신서비스 제공자 ● 정보통신서비스 제공자로부터 개인정보를 제공받은 자 ● 개인정보 수집 · 취급 등을 위탁받은 자
성 격	● 반드시 준수해야 하는 최소한의 기준
강제 여부	● 3천만원 이하의 과태료(법 제76조제1항제3호) ● 2년 이하의 징역 또는 1천만원 이하의 벌금(법 제73조제1호) ● 위반행위와 관련한 매출액의 100분의 1 이하 과징금(제64조의3)

이렇듯 정보화 사회에 따른 개인정보 보호의 필요성에 따라 국내에서도 개인정보보호에 대한 기관 및 대중의 관심이 높아지고, 개인정보 보호 기술의 필요성을 인지하면서 이를 충족시킬 수 있는 시스템이 시급하다.

II. 개인정보 관련연구

2.1 법적, 제도적, 표준화 연구

2.1.1 국내 법적 관련 연구

1) 국내 개인정보보호 관련 법률

2006년 12월 22일 민간 IT분야의 개인정보를 관할하는 법률인 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'이 개정되어 2007년 1월26일 공포(2007년 7월11일 시행)됐다. 개정 법률은 '개인정보 수집·이용·제공에 대한 고지 및 동의 제도 개선', '사업자의 개인정보 수집 시 수집·이용목적, 수집항목, 보유 및 이용기간, 제3자 제공에 관한 사항을 이용자에게 명확히 알리고 동의를 의무화', '개인정보 취급에 대한 제반 방침을 이용자가 언제든지 확인할 수 있도록 취급방침의 공개'등을 주 내용으로 하고 있다.

2007년도 법령 개정과 함께 급변하는 IT환경에 적합한 개인정보보호법 제정을 위한 작업반을 구성해 법제 개선 연구를 진행했다. 현재 개인정보 법률은 공공기관의 '공공기관의 개인정보보호에 관한 법률', 민간의 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 등으로 나뉘어져 있다. 아래 [표 6]은 국내 개인정보보호 관련법 현황을 정리한 것이다. [26]

[표 9]국내 개인정보보호 관련법 현황

	분야	주요법률	기타 개인정보 관련법	기타 업무상 비밀준수규정
헌법	공공행정	공공기관의 개인정보 보호에 관한법률	·공공기관의 정보공개에 관한 법률 ·전자정부구현을 위한 행정업무 등의 전자화 촉진에 관한 법률, 주민등록법, 호적법 ·자동차관리법, 도로교통법, 국세기본법 ·국정감사 및 조사에 관한 법률, 통계법 등	·변호사법 ·법무사법 ·세무사법 ·관세사법 ·공인노무시법 ·외국환거래법
	정보통신	정보통신망	·통신비밀보호법	

		이용촉진 및 정보보호 등에 관한 법률	·위치정보의 보호 및 이용 등에 관한 법률 ·정보화 촉진 기본법, 정보통신기반보호법 ·전기통신사업법, 전자서명법 ·인터넷주소 자원에 관한 법률 등	·공증인법 ·은행법 ·근로기준법 ·노동위원회법 ·직업안정법 ·공인중개사의 업무 부동산 ·신고거래에 관한 법률 ·형법 제317조등
	금융/신용 (기타 상거래 포함)	신용정보의 이용 및 보호에 관한 법률	·금융실명거래 및 비밀보장에 관한 법률 ·독점규제 및 공정거래에 관한 법률 ·방문판매 등에 관한 법률 ·전자상거래 등에서의 소비자보호에 관한 법률 ·전자거래기본법, 보험업법, 증권거래법 등	
	의료	보호의료 기본법	·응급의료에 관한법률 ·장기등이식에 관한 법률 ·생명윤리 및 안전에 관한 법률 ·인체조직안전 및 관리 등에 법률 ·후천성면역결핍증예방법, 전염병예방법 등	
	교육	교육기본법	·초중등 교육법 ·교육정보시스템의 운영 및 관한 규칙	

2.1.2 국외 법적 관련 연구

1) 국외 개인정보보호 관련법 현황

세계 각국의 개인정보보호 법률 체계는 크게 유럽식 모델(일원적·포괄적 규제 모델)과 미국식 모델(이원적·부문별 규제 모델)로 구분되어 있다. 유럽 각국의 개인정보보호법은 사회 전 분야에 걸친 수집·이용 원칙, 정보주체의 열람·정정권, 집행·감독기구 등 포괄적 기준(캐나다, 호주, 뉴질랜드 등도 유럽식 모델과 유사)을 규정하고 있다. 아래 [표 7]은 국외 개인정보보호 관련법 현황을 정리한 것이다.

[표 10]국외 개인정보보호 관련법 현황

나 라	법률 명 및 시행 시기
영국	정보보호법, 1998
프랑스	정보처리파일 및 자유에 관한법률, 1978
독일	연방정보보호법, 1974
스웨덴	개인정보법, 1998

스페인	개인정보보호기본법, 1999
네덜란드	개인정보보호법, 1999
미국	프라이버시법, 1974 / 컴퓨터에 의한 정보조합과 프라이버시보호에 관한 법률, 1988 / 건강보험책임법

미국은 공공부문의 경우 '프라이버시보호법(Privacy Act)' 등 법률을 통해 엄격히 규율하고 있는 반면, 민간부문은 법률을 통한 규제보다 시장 자율 규제에 중점을 두고 있다. 민간 부문의 개인정보보호법은 의료, 운전면허, 비디오 대여, 아동 프라이버시 등 특정영역에 한해 입법되고 있다. 국내외를 막론하고 정보보호에 대한 규정은 꾸준히 강화되고 있으나, 개인 및 기업의 정보를 빼내기 위한 사이버 범죄 역시 날로 그 수법이 고도화되고 있어 이에 대한 우려 역시 커지고 있는 상황이다. [14]

2) OECD 개인정보보호 8대 원칙

개인정보의 국제법적·제도적 측면에서 중요한 연구 방향 중 한 가지는 OECD(Organization for Economic Co-operation and Development) 에서 제시하는 "프라이버시 보호 및 국제적 유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transporter Flows of Personal Data)" 부분이다. OECD 기준은 주로 정보주체의 동의 절차에 대한 명시가 중요한 내용으로 포함되어 있다. 즉 개인정보에 대한 관리가 정보주체의 동의절차와 수집경로 그리고 이용목적에 대한 고지가 어떻게 이루어지고 있는가 하는 점이 중요한 문제이다. 이에 대한 기준으로는 아래와 같은 8가지 원칙이 중요시 되어 지고 있다. 아래 [표 8]은 OECD에서 지정하는 개인정보보호 관련 8가지 기본 원칙을 정리한 것이다. [2]

[표 11]OECD의 개인정보 보호 원칙

원칙	내용
수집 제한의 원칙	개인데이터의 수집에는 제한을 두어야 한다. 어떠한 개인 데이터도 합법적이고 공정한 절차에 의하고 가능한 경우에는 데이터주체에게 알리거나 동의를 얻은 연후에 수집하여야 한다.
정확성 확보의 원칙	개인데이터는 그 이용목적에 부합되는 것이어야 하며 이용 목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것 이어야 한다.
목적명시의 원칙	개인정보는 수집 시 그 수집목적이 명확히 제시되어야 하며, 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립되어야 하고 목적이 변경될 때마다 명확화 될 수 있는 것으로 제한되어야 한다.
이용제한의 원칙	개인정보는 목적명확화의 원칙에 의하여 확인된 목적 이외의 다른 목적을 위해 개시, 이용, 그 밖의 사용에 제공되어서는 안 된다. 다만 정보주체의 동의가 있거나 법률의 규정에 의한 경우에는 예외로 한다.
안전성 확보의 원칙	개인데이터는 그 분실 또는 불법적인 액세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 함으로써 보호하여야 한다.
공개의 원칙	개인데이터와 관련된 개발, 실시, 정책에 대하여는 일반적 인 공개정책을 취하여야 한다. 개인데이터의 존재, 성질 및 그 주요 이용 목적과 함께 데이터관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 한다.
개인참여의 원칙	개인은 자기에 관한 정보의 소재를 확인할 권리를 가지며, 필요한 경우에는 자신에 관한 정보를 합리적인 기간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 통지 받을 권리를 갖는다. 이러한 권리가 거부된 경우에 개인은 그 이유를 구하고 거부에 대하여 이의를 제기하거나 데이터의 폐기, 정정 및 보완을 청구할 권리를 갖는다.
책임의 원칙	데이터관리자는 위의 제 원칙을 실시하기 위한 조치에 따를 책임이 있다.

그 외 개인정보 관련 표준화 연구들에 대한 가이드라인은 아래 [표 9]와 같이 정리 할 수 있다. [7]

[표 12]해외 개인정보보호 가이드라인

	OECD	ISTPA	IPC	APE	P3P
정보수집	수집제한	수집제한	수집제한/동의	수집제한	개인정보를 수집하는 자
정보수집	데이터	검증	정확성	무결성	수집되는

	정확성				개인정보 항목
정보수집 목적	목적명확화	적절성	목적확인	목적 고지	수집목적
정보활용	이용제한	사용제한	제한된 사용/ 동의	개인정보 활용	제 3자와 공유하는 개인정보
정보저장 및 보안	안전보호	보안	보호책	보안조치	개인정보 수령인
정보공개	활용정책 공개	공개	개방성/동의	열람 및 수정	인간이 판독할 수 있는 형식
감사	개인참가	참여	개인접근/ 도전적인 참여 의식(권리부여)	선택	개인정보 정정 가능 여부
	책임	책임	책임	책임/피해 예방	자료를 유지하기 위한 정책

2.1.3 제도적 연구

개인정보보호기술은 이미 다양한 솔루션이나 기술이 상당수 개발되어 있고 또한 진행 중에 있다. 대표적인 기술로는 익명화 기술, W3C(the World Wide Web Consortium)에서 개발한 P3P, OECD에서 개발한 프라이버시정책생성기(Privacy Policy Statements Generator), 사용자들이 쿠키 수용여부를 결정하며 저장된 정보가 공개될 수 있는지를 판단하는 쿠키 관리 통제(Cookie Manager or Blockers) 기술, 암호화를 통해 전자메일 메시지, 저장된 파일, 온라인에서 커뮤니케이션을 보호할 수 있게 하는 기능을 제공하는 암호화 소프트웨어(Encryption Software) 등이 존재한다. 이렇게 대표적인 개인정보보호기술은 프라이버시보호를 위한 효율적인 방법 중 하나로 구분되어 개발하고 발전되고 있다. 또한 최근에는 개인정보침해기술에 대응하여 크게 6개 영역(에이전트기반기술, 웹 기반 익명성 제공기술, 네트워크 기반 기술, 암호화 기술, 정책협상 기술, 내부정보보안기술)에 걸쳐 세부 개인정보보호기술을 분류될 수 있다. [3][4][16][17][29]

[표 13] 개인정보보호 기술

분 야	방 법
웹 기반의 익명성 제공 기술	정보의 노출 자체와는 무관하게 정보와 소유자 간의 관계나 송수신자 간의 관계를 비밀로 하여 사용자의 개인정보보호를 제공하는 기술로 사용자들 간의 비연결성을 통하여 익명성을 제공하는 기술
에이전트 기술	개인정보보호를 위한 에이전트(agent)는 사용자가 파악하기 쉽지 않은 인터넷상에서의 정보 유출에 대해 사용자를 대신하여 통제해 주는 역할
네트워크 기반 기술	현실적으로 가장 빈번하게 일어나는 개인정보 침해 사고들은 네트워크 환경에서 정보를 전달할 때 중간에 가로채거나 수정하거나 또는 단순히 그 데이터를 보기만 하는 행동들에 의해 발생하며 이를 예방하는 기술
정책협상기술 (P3P)	웹사이트 운영자에게 이용자 자신의 정보를 관리할 수 있는 권한을 넘겨주는 것이며 이용자 정보가 잘못된 방법으로 사용되지 않도록 보호하기 위해 만들어짐. 따라서 웹 브라우저나 다른 사용자 도구로 하여금 자동적으로 해당 웹사이트의 프라이버시에 관한 정보를 읽고 사용자가 미리 설정해 놓은 정보공개 수준과 비교하여 정보를 선별적으로 제공
암호화 기술	암호화를 통해 자신의 전자 메일 메시지, 저장된 파일, 그리고 온라인에서의 커뮤니케이션을 보호할 수 있게 하는 기능을 제공함. 한번 암호화가 이루어지면 오직 그 당사자만 암호화된 정보에 대한 디지털 키를 가지고 그 정보를 열람하며, 디지털 키는 브라우저, 생체인증, 스마트카드 등과 결합하여 생성됨
내부 정보보안기술	주요 기술정보, 개인정보, 국가기밀 등 이권에 관계된 정보가 유출됨을 보호하는 기술. 대표적으로 정보유출 주체에 정보접근권한자를 배제한 내부자로 한정한 기술과 내부 통신 내용을 모니터링하거나, 시스템 내부에서 일어나는 기술적인 침입을 탐지/방어하는 기술을 탑재.

2.1.4 국내 관련 연구동향

국내에서 진행되고 있는 개인정보보호 관련 프로젝트 분석 및 정리하면 다음과 같다.[8][14][22][23]

[표 14] 국내 개인정보보호 관련 프로젝트

프로젝트명	특징		비고
접근통제 기반 개인정보관리 모델	기관	• 한국정보보호진흥원 • 수탁기관 : 전남대학교	적용된 정책이 OECD 기반이라서 국내 적용 시 고려됨
	특징	• 접근통제기반 개인정보보호 관리 모델 연구의 목적으로 기존 프라이버시 관련 연구 동향 및 기술 조사와 분석 • 프라이버시 강화형 역할기반 접근통제정책 표현 언어를 제안	
인터넷 개인정보 노출방지 및 프라이버시 보호 방안	기관	• 한국정보보호진흥원 • 수탁기관 : (사)사이버경제사회연구소	법률과 사례 현황 중심의 연구로 시스템의 적용 등 구체적인 해결방안 제시 미비
	특징	• 인터넷상의 개인정보 노출원인 분석하고, 노출 방지를 위한 법제도 개선 방안 • 개인정보 검색과 프라이버시 보호방안 연구 • 웹 2.0 등 IT 트렌드 변화와 프라이버시 보호에 관한 연구	
전자정부 서비스 사용자인증, 권한관리 레벨화 방안 연구	기관	• 한국정보보호진흥원 • 수탁기관 : 경원대학교 산학협력단	현업에의 적용 방안, 민간 사업화 분야에 대한 활용방안이 미비
	특징	• 전자정부 인증프레임워크의 해외 벤치마킹 실시하여 방향성 도출 • 대한민국 전자정부서비스 사용자인증 프레임워크 제시 - 주요구조정의, 절차정의, 적용사례	
유비쿼터스 환경에서의 정보보호 정책 방향	기관	• 한국정보보호진흥원 • 수탁기관 : 지식경제부	동향과 트렌드 분석의 보고서이므로 프로젝트 수행에 있어서 정책 분석 참고자료로 활용
	특징	• 통합적인 관점의 위험관리를 위한 사회주체별 요구사항들을 제시 • 개인정보침해 및 기타 사이버 범죄를 예방하고 수사하기 위한 디지털 포렌식 관련 기술 및 법/제도 분석	

2.2. 기술적

2.2.1 개인정보보호 기반 기술

1) 신분확인

가. ID/Password 방식

지식 기반 인증 시스템은 현재 가장 널리 사용되고 있는 패스워드 기반 인증 및 개인 식별번호를 이용하는 인증시스템이다. 이 경우 보안은 자신만이 알 수 있다고 인정되는 정보를 소유하고 있음을 증명함으로써 인증시스템으로부터 신원을 확인 받게 된다. 이것은 사람의 기억력을 기초로 하고 있으며 다음과 같은 방식으로 분류할 수 있다. 보안 시스템의 사용자 확인을 위해, 사용자는 고유한 ID와 일정한 패스워드를 사용한다. 패스워드는 본인과 보안시스템 서버 외에는 모르는 것이 원칙이므로 패스워드를 알고 있다는 것은 그 사람이 이전에 보안시스템 서버에 패스워드를 등록했던 사람이라는 것을 의미한다. 패스워드 방식은 신원 확인에 있어 가장 기본적이면서도 간단한 방식이므로 현재 대부분의 회원제 웹 사이트에서 채택하고 있는 방법이다. 이 때 패스워드는 개별적인 특성을 갖기 위해 일정한 길이 이상일 것, 또 흔하지 않은 것이어야 한다는 제약을 받는다.

나. 공개키 기반 구조(Public Key Infrastructure)의 인증서 방식

공개키 암호기술은 보안이 필요한 응용 분야에 널리 사용된다. 공개키 암호 기술에서는 비밀키와 공개키를 이용한다. 비밀키는그 소유자만이 알고 있고 공개키는 공개된다. 공개키를 공개하는 문제는 비밀키를 소유자만이 알도록 하는 것보다 얼핏 보기에 매우 단순한 것 같지만 실제 구현시 공개키를 공개하는 데에 사용되는 메커니즘(공개키 디렉토리, 게시판 등)이 자체적으로 안전하지 않아 누구나 쉽게 접근하여 정보를 변경할 수 있으므로 공개키의 위/ 변조 문제를 야기시킨다. 다음과 같은 경우를 생각해 보자. A가

B에게 문서를 비밀리 보내고자 하는 경우 A는 B의 공개키로 그 문서를 암호화할 것이다. 그런데 제 3자인 C가 공개키 디렉토리에 접근하여 B의 공개키를 자신의 공개키로 바꾸어 버리고 전송되는 암호문을 중간에 가로채 버린다면 A가 원래 문서를 보내려고 했던 B가 아닌 C가 그 문서를 읽게 될 것이다.

이렇게 공개된 공개키가 위·변조되지 않았음을 보장하는 문제 즉, 공개키의 무결성을 보장하기 위해 등장한 것이 공개키 기반구조 (PKI:Public Key Infrastructure)이다. 공개키 기반구조에서는 공개키를 공개하는 대신 공개키와 그 공개키의 소유자를 연결하여 주는 인증서(certificate)를 공개한다. 인증서는 신뢰할 수 있는 제 3자(인증기관)의 서명문이므로 신뢰 객체가 아닌 사람은 그 문서의 내용을 변경할 수 없도록 한다.

PKI를 구성하는 최소 객체들은 아래의 [표 12]와 같다. [19]

[표 15] PKI 구성 요소

객체	설명
등록기관 (RA: Registration Authority)	공개키 기반구조를 구성하는 가장 핵심 객체로 그 역할 및 기능에 따라 계층적으로 구성되며 여러 명칭으로 불리 운다. 아래 세 기관 모두를 통틀어 인증기관이라 한다. - 정책승인기관(PAA : Policy Approving Authority) - 정책 인증 기관(PCA: Policy Certification Authority) - 인증기관(CA: Certification Authority)
인증기관	인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자사이에 등록기관을 두어 인증기관대신 사용자들의 인증서 신청 시 그들의 신분과 소속을 확인하는 기능을 수행한다. 사용자들의 신분을 확인한 후, 등록기관은 인증서 요청에 서명을 한 후 인증기관에게 제출한다. 인증기관은 등록기관의 서명을 확인한 후 사용자의 인증서를 발행한 후 등록기관에게 되돌리거나 사용자에게 직접 전달한다. RA는 조직 등록기관(ORA: Organizational Registration Authority)라고도 불린다.
디렉토리	인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서취소목록등을

객체	설명
	저장 및 검색하는 장소로 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버(인증기관)는 DAP(Directory Access Protocol)나 LDAP(Lightweight DAP)[3]를 이용하여 X.500 디렉토리 서비스를 제공한다. 인증서와 상호 인증서 쌍은 유효기간이 경과된 후에도 서명 검증의 응용을 위해 일정기간동안 디렉토리에 저장된다.
사용자	PKI내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다.

2) 접근제어

접근제어는 각 자원에 대한 기밀성, 무결성, 가용성 및 합법적인 이용과 같은 정보보호 서비스에 직접적으로 기여하게 되며 이러한 서비스들의 권한 부여를 위한 수단이 된다.

대부분 컴퓨터 시스템의 사용자는 시스템을 사용하기 위하여 식별(identification)과 인증(authentication)이라고 하는 검사과정을 통하여 시작된다. 식별과 인증은 각 시스템 자원을 보호하기 위한 외부의 1차적인 보호 계층이다.

접근제어의 여러 방법은 아래와 같다.

가. 임의적 접근통제 (DAC)

주체나 또는 그들이 속해 있는 그룹들의 신분에 근거하여 객체에 대한 접근을 제한하는 방법을 DAC이라고 정의한다. 접근통제는 임의적이므로 어떠한 접근 허가를 넘겨줄 수 있다. 또한, DAC은 자주 "need-to-know"을 시행하고, 접근통제가 권한을 가지고 있는 개인에 의하여 변경될 수 있다는 의미에서 자유 재량권을 갖고 있다.

DAC 정책은 각 주체에 대하여 시스템 객체들에 부여된 권한을 명시하는 권한부여 규칙을 요구한다. 접근 요청은 DAC 메커니즘에 의하여 검사되고

권한부여 규칙이 존재하고 해당접근이 검증되는 주체에게만 허가된다. 이것은 소유권을 통한 행정 관리적 제어가 분산됨을 의미한다. 그러나 DAC은 중앙집중관리에서도 적합하며, 이 경우에 권한부여는 시스템 관리자에 의하여 관리될 것이다. DAC 정책은 권한 부여자 또는 다른 책임 있는 사람으로부터 권한 부여에 따르는 통제의 상실을 피하기 위하여 보다 복잡한 권한부여 메커니즘을 필요로 한다.

나. 강제적 접근통제 (MAC: Mandatory Access Control)

객체에 포함된 정보의 비밀성(레이블로 표현된 허용등급)과 이러한 비밀성의 접근 정보에 대하여 주체가 갖는 권한(즉, 접근허가(clearance))에 근거하여 객체에 대한 접근을 제한하는 방법을 MAC이라고 한다.

접근통제를 위한 MAC정책은 분류된 시스템 데이터와 각 등급의 사용자 간에 강력한 보호를 위하여 요구되는 많은 정보들을 적용한다. MAC은 또한 하위 비밀등급의 객체로 정보의 흐름을 방어하기 때문에 흐름-제어(flow-control) 정책으로 정의될 수 있다. 데이터에 대한 접근은 주체와 객체가 갖는 보안등급의 정의를 통한 강제적인 정책에 의하여 결정된다.

MAC 정책은 DAC 정책에 비하여 일반적으로 다음과 같은 특성을 갖는다. 첫째, MAC정책은 객체의 소유자가 변경할 수 없는 주체들과 객체들 간의 접근통제관계를 정의한다. 둘째, 한 주체가 한 객체를 읽고 그 내용을 다른 객체에게 복사하는 경우에 원래의 객체에 내포된 MAC 제약사항이 복사된 객체에 전파(propagate)된다. 셋째, MAC 정책은 모든 주체 및 객체에 대하여 일정하며, 어느 하나의 주체/객체 단위로 접근 제한을 설정 할 수 없다. 즉, MAC이 어느 한 객체를 접근하지 못하면, 이때에 그 주체는 그러한 특정의 비밀 등급을 갖는 모든 객체들을 접근하는 것이 금지될 것이다.

규칙-기반 정책은 사용자 및 타깃별로 부여된 기밀 분류에 따른 정책과 조직 내의 각 부서별로 구분된 기밀 허가에 따르는 정책으로 표현될 수 있다.

다. 역할기반 접근통제(RBAC: Role-Based Access Control)

RBAC의 개념은 1970년대 다중 사용자의 다중 응용을 위한 온라인 시스템에서 시작되어 현재 접근통제의 표준인 MAC 및 DAC의 대안으로서 많은 관심을 집중시키고 있다. RBAC의 가장 큰 동기는 관리자가 수행하기 어려운 보안관리 과정을 능률적으로 처리하고 공공기관 및 기업에 특정한 보안정책을 명료하게 표현하고 시행하기 위함이었다. RBAC에서는 관리자에게 누가, 언제, 어디에서, 어떤 행동을 수행할 수 있는지 규정할 수 있는 권한이 주어진다.

기능적인 측면에서 RBAC의 핵심은 역할과 관련된 행동을 나타내는 연산(operation)과 역할(role)의 구성원으로 표현될 수 있는 사용자(user)이지만, 아래의 [표 13]과 같은 추가적인 요소를 가지고 있다.

[표 16] RBAC의 기본 구성 요소

구성요소	설 명
사용자(Users)	사용자의 집합으로 시스템을 사용하는 사람들을 의미한다.
역할(Rolls)	조직내의 업무들의 집합으로 수행 가능한 권한과 책임으로 구성된다.
연산(Operations)	하나 혹은 그 이상의 보호된 RBAC 객체들의 집합에 접근하기 위한 특정한 접근 방식이다.
주체(Subject)	일-대-다 관계를 가진 활성화된 사용자 프로세스이다.
제약조건(Constraint)	제약조건은 사용자 배정, 역할 할당, 권한 배정, 그리고 세션 등 모든 구성요소에 적용될 수 있다. 그리고 제약 조건의 예로는 임무 분리와 최대 사용자 수(cardinality) 등이 있다.
객체(Ojbect)	시스템에 의해서 관리되는 대상을 의미한다.
권한(Permission)	특정한 객체에 대해 수행 가능한 연산들의 집합이다.

RBAC에서 사용자와 역할은 다대다(many-to-many) 관계를 가지고 있다. 예를 들어, 한 사용자는 하나 이상의 역할과 관련될 수 있고, 하나의 역할은 한명 이상의 사용자를 가질 수 있다. 역할은 한 조직의 일에 따라 다양한 형태로 생성될 수 있다. 역할과 관련된 연산은 역할의 구성원에게 특정 행

동을 수행하도록 강요한다.

이러한 RBAC의 대표적인 제약 조건을 살펴보면 다음과 같다.

첫째, 상호배타(Mutual Exclusion)이다. 같은 사용자는 임무의 분리를 위해 상호 배타적인 집합 내에서 하나만의 역할에 할당될 수 있다. 임무의 분리는 한 사용자가 동시에 가질 수 없는 역할이나 동시에 수행할 수 없는 역할들을 위반하지 않으면서 정해진 연산을 수행하는 것이다. 임무 분리 정책에는 정적 임무 분리(Static Separation of Duty, SSD)와 동적 임무(Dynamic Separation of Duty, DSD)가 있다. 정적 임무 분리는 이미 권한을 가진 역할들과 상호배제가 아닌 역할일 때만 역할의 구성원이 될 수 있다. 동적 임무 분리는 역할이 활성화되는 시점에 기준을 두고 있다. 두 역할이 상호 배제이더라도 역할의 구성원이 될 수 있다. 그러나 동시에 두 역할을 활성화시킬 수는 없다.

둘째 카디널리티(Cardinality)이다. 사용자 할당 제약의 또 다른 예로서 역할은 멤버의 최대 숫자를 제한할 수 있다. 예를 들어 각 분야의 대표는 단 한 사람만이 할당될 수 있다. 유사하게 각 사용자가 맡게 되는 역할의 수도 제한할 수 있다. 이것을 카디널리티(cardinality) 제약이라고 한다.

RBAC의 장점에 대해 살펴보면 다음과 같다.

우선 관리자에게 편리한 관리 능력을 제공한다. 전통적인 접근통제 메커니즘의 경우 사용자의 접근권한 관리는 매우 성가신 작업이다. 그러나 RBAC의 경우 사용자의 자격과 책임에 따라 역할의 구성원으로 사용자를 지정하고 부여된 사용자의 업무에 따라서 사용자를 역할의 구성원에서 제외하고 새롭게 추가하는 것이 쉽게 이루어질 수 있다. RBAC에서는 연산은 사용자 개인별로 어떤 연산을 수행하도록 허가하는 것이 아니라 오로지 역할과 관계가 있으므로 조직의 기능 변화에 따라 역할과 관련한 연산의 삭제 및 추가 역시 자유롭게 이루어질 수 있다.

또한, 접근을 통제하고자 하는 객체단위로 접근통제를 수행하는 기존의 방법과는 달리 관리자는 역할, 역할계층(hierarchy), 관계(relationship), 제약(constraint)의 정립을 통하여 사용자의 행동을 정적 또는 동적으로 규제할 수 있으므로 시스템 관리자에게 객체단위가 아닌 추상적인 개념으로 접근을 통제할 수 있다. 따라서 RBAC은 업무를 수행하는 실제 환경에 자연스럽게 접목할 수 있다.

라. 접근통제 리스트(ACL: Access Control List)

ACL은 어떤 사용자들이 객체에서 어떤 행위를 할 수 있는지 나타낸다. ACL의 유지와 접근통제의 시행은 본질적으로 시스템 책임이다. ACL은 관련된 객체에 대하여 주체의 접근 권한을 반영한다. 그러므로 직무 기반 정책을 포함한 신분 기반 접근통제정책은 ACL을 사용하여 실현될 수 있다. 또한, ACL의 기본적인 개념은 특정의 선택된 사용자 엔트리에 대해서 접근통제조건을 추가하여 수행하는 것과 같이 여러 가지 방법으로 확장 될 수 있다.

이러한 ACL 메커니즘은 구분될 필요가 있는 사용자(개인, 그룹, 또는 직무)가 비교적 소수 일 때와 그러한 사용자의 분포가 안정적일 때 가장 적합하다. 그러나 대상이 되는 사용자가 너무 많고 자주 변경될 때 문제가 발생 할 수 있다. 다른 메커니즘과는 달리 ACL은 타깃 단편들이 넓은 영역인 경우에 적합하다. 또한, 타깃의 소유자 또는 관리자가 이전에 부여된 권한을 사용하기 용이한 장점이 있다. ACL 메커니즘은 FTAM(File Transfer, Access, and Management)과 디렉토리 응용분야에서 일반적으로 사용된다. [14]

2.2.2 개인정보 보호 강화 기술 (PET: Privacy Enhanced Technology)

개인정보들이 사용자의 동의 없이 유출되는 것을 막기 위한 방법들 중 대표적으로 사용되는 기술들 즉, 사용자들의 정보들이 빠져나가는 것을 막는 PET(privacy enhancing technology) 기술은 아래와 같이 요약한 [표 12]로 보여 질 수 있다. [26]

[표 14] PET 기술 분석 및 요약

분류	서비스	특징	기술
Web 기반 기술	클라이언트의 익명성 제공	웹 사용자의 인터넷 이용에 관련된 정보를 숨기고 암호화를 통한 데이터 트래픽의 내용을 숨긴다.	· Anonymizer · Onion Routing · Crowds
	서버의 익명성 제공	URL 암호화를 통한 익명성을 제공하고 브라우저의 암호화, 데이터스트림의 암호화를 통한 데이터의 무결성 및 보안 제공한다.	· Janus
Network 기반 기술	네트워크상에서 정보의안전성과 신뢰성 제공	접근통제, 침입탐지, 침입차단, 패킷 및 침입 경로 추적 암호화와 복호화, 인증을 통해 안정성 제공한다.	· Proxy · Firewall · IDS · IPS
Agent 기반 기술	인터넷상의 정보 유출에 대해 통제	다른 소프트웨어와는 다르게 에이전트는 스스로 판단하여 행동하는 자율성을 가진다.	· Cookie manager · Ad blocker · Spyware Filter

2.2.3 개인정보 침해 대응 기술 (PIT : Privacy Invading Technology)

개인정보 침해 대응 기술(PIT)은 컴퓨터 환경 내 개인정보 관련 오·남용 또는 악의의 피해가 발생 할 수 있는 분야에 대하여 기술적 관점에서 체계적으로 분석하고 대응 할 수 있는 기술적 체계 구성을 이야기 하는 것으로 요약은 [표 15]과 같다. [14][15]

[표 18] 개인정보 침해 기술 분석표

침해대응기술	방 법
TCP/IP 주소	· TCP/IP 주소의 분배 및 관리 체계 특성 때문에 인터넷 이용 시 TCP/IP 주소를 추적하여 이용자 신원을 확인하는 것은 용이.
도메인 네임	· E-mail의 출처를 확인하는 것은 매우 간단하며, 누구나 ISP정보와 E-mail 이용자의 ID를 이용하여 이용자의 계정을 확인.
프로세스 순차 번호(PSN)	· Intel사는 자사가 개발하는 펜티엄 III칩에 고유의 프로세서 일련번호를 부여하여 인터넷에 접속하는 특정 컴퓨터의 이용자의 신원 정보와 연결시켜 전자상거래에 있어서 인증 목적을 이용.
IPv6	· IPv6의 계획은 인터넷 상의 모든 장치에 고정된 주소를 할당하는 것.

침해대응기술	방 법
	· IPv6의 새로운 주소는 하드웨어 속에 내장될 것이고, 추적 가능한 정보를 포함 하게 된다. 이것은 마치 영구적인 쿠키를 심는 것과 동일 개념.
쿠키	· 쿠키 파일을 이용하여 인터넷 이용자의 신원을 쉽게 파악할 수 있음. · 첫째는 쿠키는 로그인정보(예컨대 이름, 주소 비밀번호 등)을 불러내는 데에 사용될 수 있음. · 둘째, 쿠키에 담긴 정보와 마케팅 데이터베이스에 있는 이용자의 이름, 주소, 이전의 소비경보 등을 상호 비교함으로써 이용자의 신원 확인이 가능.
웹을 통한 유출 (버그, Malware, 피싱 등)	· 웹 버그는 온라인 이용자가 모르는 사이에 이용자에 관한 정보를 유출해 하거나 심지어 이용자의 시스템을 파괴할 수 있는 기술.
스파이웨어	· 무료 또는 유포로 배포되는 소프트웨어에 들어 있는 일종의 프로그램 모듈을 통칭. · 해당 소프트웨어를 설치한 컴퓨터 이용자가 인터넷을 서핑할 때 이용자의 개인 정보나 온라인 활동 정보를 스파이웨어를 설치한 회사의 서버에 지속적으로 전 송하는 것이 주된 기능.
고성능 스파이웨어 기술	· 스파이웨어를 탐지하기 위해 사용되는 백신이나 안티 스파이웨어 솔루션 등을 우 회하기 위해, 스파이웨어를 통해 수집된 정보를 작은 크기로 나누어 컴퓨터 파일 시스템 상에 보이지 않는 틈새 공간(slack space)에 임시 저장한 다음, 특정 시간대의 내외부의 특정인에게 전송하는 방법을 이용.
무선 랜 (WLAN) 해킹	· WLAN 사용자가 액세스 포인트에 접속할 때, 해커가 가상의 액세스 포인트를 이 용하여 사용자의 중요한 개인정보를 모니터링하게 됨.
웹 메일의 첨부파일 유출	· 웹 메일 첨부파일 유출기법은 기존 e-mail이나 웹 메일을 모니터링하여 데이터를 유출하는 방식에서 한 단계 진화하여, 웹 메일에 첨부된 파일을 encoding하는 방식으로 주로 기업이 운용하는 메일 모니터링 프로그램을 우회하여 기밀 정보를 유출하는 방법.
스테가노그래피 (Stegenography)	· 이미지 및 오디오 파일에 중요한 파일이나 메시지를 첨부할 수 있는 스테가노그래피 기법이 확산될 전망.
접속세탁 (connection laundering)	· 해커가 여러 국가를 경유하여 해킹을 할 경우, 중간 단계에 해커 그룹이 운용하는 기명경로(ancoymizer)를 거쳐 해커에 대한 역추적이 불가능하게 하는 방법.
위치측정 정보	· GPS, RFID, 또는 휴대전화기의 위치 측정 내용을 인터넷을 통해 사용자 동의 없이, 개인의 위치 정보가 유출 되는 방법

III. 개인정보보호엔진 (Privacy Compliance Engine)

3.1. 개요 및 구성도

PCE(Privacy Compliance Engine) 메커니즘은 개인정보를 신뢰적이고 효율적으로 관리 및 통제하는 PIPS의 일부분으로써, PIPS는 총 7가지 기능을 제공하여 개인정보를 안전하게 보호 및 관리하며 체계적인 정보보호 정책 지원 방안을 확립한다.

PIPS의 7가지 기능에 대해 간략히 살펴보면 다음과 같다.

① 유무선 통합 개인정보 관리(인증) 기능

PKI 표준화 기반의 공인인증서를 통해 통합 사용자 인증 모듈을 설계 하고, 개인정보 정책에 준한 속성 인증 연동 및 관리 방안 개발과 무선(WIPI) 환경 내 암호화(WPKI) 기반의 Notice 기능 연동을 통하여, 실시간 개인정보 보호 및 알림 기능을 제공한다.

② 개인정보보호 정책 엔진 기능

국내외 관련 법/제도 기반의 개인정보 정책 생성 및 접근제어 기능의 분석/설계를 통해 법/제도 기반의 적합하고 일괄적인 접근제어 방안을 확립하고, 다양한 형태의 응용 방안을 적용한 개인정보보호 엔진을 개발한다.

③ 불법 정보 오남용 방지 및 접근제어

역할/목적/항목별 중요도에 따라 분류하고, 개인정보의 순서도를 분석하여 접근제어 설계를 한다. 이를 국제 규범을 기반으로 개인 정보의 오남용 방지 및 접근제어 방안을 강화한다.

④ 사용자 사전 동의 및 Notice 기능

개인정보의 민감한 중요정보에 대해서는 사용자 동의를 먼저 구하는 방식을 적용하고, 기타 개인정보는 임의의 동의 없이 사용되거나, 해킹 또는 오/남용으

로 의심 시에는 사용자에게 먼저 적당한 조치를 취할 수 있는 기능을 개발한다.

⑤ 디지털 포렌식 기능

개인정보를 효과적으로 보호하기 위하여 주기적인 정보 교류 시 실시간 감시, 개인정보 사용 관리 기능과 로그 분석, 패턴 분석, 리포트 기능 등을 연동한 디지털 포렌식기능을 한다.

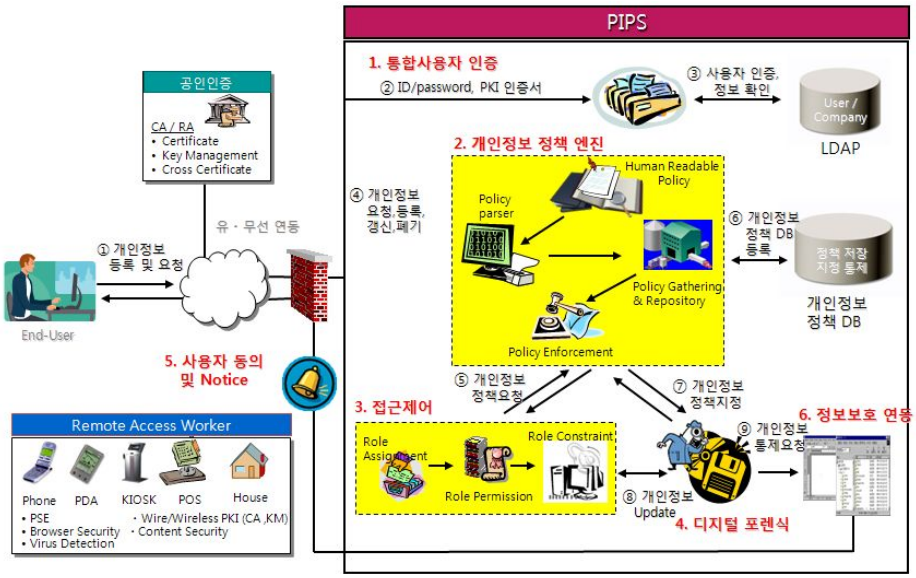
⑥ 안전성(Security Compliance) 기능

개인정보의 효율적인 신뢰성 확보와 기존 보안 솔루션과의 연동(Network 보안, PKI, 모니터링 등)을 고려하여, 안전한 개인정보 시스템 구축의 인프라 구성 및 그 활용 방안을 제시한다.

⑦ 내부사용자 접근제어 기능

조직 내 접근제어를 위한 내부사용자를 정의하고 역할별 구분을 통해 관련법에 따른 설계하여 정보의 권한별 접근제어를 가능하게 한다.

아래의 [그림 2]는 PIPS의 전체 구성도이다.



[그림 2] 개인정보보호 정책엔진 PIPS

PIPS의 7가지 기능 중 색칠된 네모 박스의 두 부분이 2.개인정보보호 정책 엔진 기능과 3.접근제어 기능을 담당하는 PCE 메커니즘으로, 이에 대해 다음절에서 상세히 다룬다.

3.2. Privacy Compliance Engine 메커니즘

3.2.1 개인정보보호 정책 엔진 기능

PIPS 내 개인정보보호 정책엔진 메커니즘에 관한 것으로 개인정보의 위험 분석과 개인정보보호 관련 연구 동향 및 기술현황을 바탕으로 국내 법 및 국외 표준화 기반으로 개인정보보호의 정책을 제시한다. 이는 개인정보보호 관련 법/제도를 이용함으로써 개인정보보호가 자동적으로 설정되어 개인정보를 체계적으로 관리한다.

이를 위해 법률분석을 통해 주체별 정의와 이용약관 분석을 하고 이를 적용한다. 또한 국외 정책 OECD의 개인정보보호 가이드라인을 분석하여 국내 개인정보보호법에 적용한다. 국내 법률 분석 및 국외 정책 분석을 통하여 개인정보 등급별 접근제어를 가능하도록 한다.

1) 국내 법 분석

정보화추진위원회에서 추진되고 있는 정보화정책 관련 법 과 한국인터넷진흥원(KISA)에서 제안하고 있는 개인정보보호 관련 법 을 주체 및 개인정보 생명주기 타입별로 구분하여 법을 적용하였다. 먼저, 사용된 법률에 대한 간략한 설명은 아래의 [표 16]과 같다.

[표 19] 주체별 개인정보보호 관련 법률

주체	관련법	설명
이용자	소비자 기본법률	소비자의 권리와 책무, 국가·지방자치단체 및 사업자의 책무, 소비자단체의 역할 및 자유 시장경제에서 소비자와 사업자 사이의 관계를 규정함과 아울러 소비자정책의 종합적 추진을 위한 기본적인 사항을 규정한다.
사업자	전자거래 기본법 법률	전자거래의 법률관계를 명확히 하고 전자거래의 안전성과 신뢰성을 확보하며 전자거래의 촉진을 위한 기반을 조성한다.
	금융실명거래 및 비밀보장에 관한 법률	실지명의에 의한 금융거래를 실시하고 그 비밀을 보장하여 금융거래의 정상화를 기함으로써 경제정의를 실현한다.
	신용정보의 이용 및 보호에 관한 법률	신용 정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 기하며 신용정보의 오용·남용으로부터 사생활의 비밀등을 적절히 보호한다.
공공기관	공공기관의 개인정보보호에 관한 법률	공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모한다.

이에 대한 PCE에 적용하는 법률은 총 7개로 아래와 같다.

① 정보통신망 이용촉진 및 정보보호 등에 관한 법률
(일부개정 2009.04.22 법률 제9637호)

② 공공기관의 개인정보보호에 관한 법률
(일부개정 2008.02.29 법률 제8871호)

③ 전자거래기본법 법률 (일부개정 2009.05.22 법률 제9708호)

④ 금융실명거래 및 비밀보장에 관한 법률
(일부개정 2008.12.31 법률 제9324호)

⑤ 신용정보의 이용 및 보호에 관한 법률
(일부개정 2009.04.01 법률 제9617호)

⑥ 소비자기본법률 (일부개정 2008.12.26 법률 제9257호)

⑦ 보건의료기본법률 (일부개정 2008.03.28 법률 제9034호)

2) 국외 정책 분석

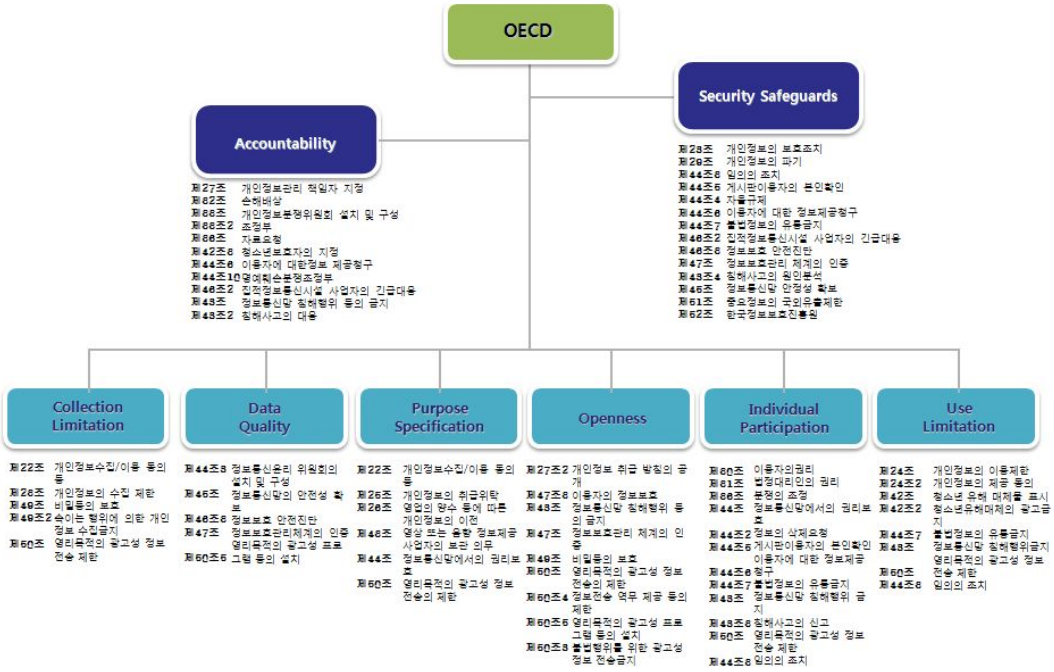
존재하는 다양한 국외 정책 중 대표적인 OECD의 개인정보보호 가이드라인을 분석하였다. OECD 8대 개인정보보호 가이드라인 분석을 통해 국내 개인정보보호법과 적용하여 이를 시스템에 사용한다.

가. OECD 내 국내 개인정보보호법 적용

국내 개인정보보호법규는 정보통신망을 이용한 대량의 개인정보 수집 및 취급 등이 용이해지면서 정보통신 서비스 이용자의 자기정보통제권 보장이 될 수 있도록 개인정보보호법안이 추진되고 있다.

이러한 현황으로 국내 관련 추진 법안의 체계적인 분류를 위해 글로벌 표준인OECD의 8원칙을 권고 규제로써 PCE에 적용한다. OECD(Organization for Economic Cooperation and Development)는 경제협력개발기구로써 '프라이버시보호 및 개인정보의 국가 간의 유통에 관한 지침'을 채택하였다. OECD 가이드라인의 8가지 원칙(공개원칙, 개인 참여, 수집제한, 목적명시, 데이터 정확성, 이용제한, 책임, 안전성) 중 책임과 안전성을 제외한 6가지 원칙이 PCE에서 적용되어 개인정보보호 법(정보통신망 이용촉진 및 정보보호 등에 관한 법률)과 매핑 하여 관리된다. [그림 3]은 국내법(정보통신망 이용촉진 및 정보보호 등에 관한 법률)을 활용하여 개인정보정책 분류표를 작성하였다.

OECD의 8가지 원칙 중 6가지 원칙으로 수행되는 기능을 분류하고 위반 시 나머지 2가지 원칙인 책임(Accountability)과 안전성(Security Safeguard) 부분을 이행하도록 구성한다. 즉, 정책 분류표 기반에서 이용목적 불일치 및 필요이상의 정보수집요구 등 위반이 발생할 때, 책임과 안전성에 관련된 처벌법에 따라 이행할 수 있다.



[그림 3] OECD 8대 원칙에 따른 국내 법 적용

3) 국내 법 기반의 정책 관리

가. 법률 내 주체정의

PCE 서비스를 사용하는 자(주체)로서 PCE 관리자부터 이용자까지 총 7가지의 주체역할로 구분하였다. 주체별 법내 정의는 다음 [표 17]과 같다.

[표 20] 주체 분류 및 세부 사항

	역할	정의
S0	PIPS 관리자	Privacy Information Protection System 내에 개인정보를 취급하고 관리하는 자를 말한다.
S1	정부 (공공 기관)	<<공공기관의 개인정보보호에 관한 법률>> 제2조(정의) “공공기관”이라 함은 국가행정기관·지방자치단체 그 밖의 공공단체 중 대통령령이 정하는 기관을 말한다. <<보건의료기본법>> 제3조(정의) “공공보건의료기관”이라 함은 국가·지방자치단체 기타 공공단체가 설립·운영하는 보건의료기관을 말한다.

S2	전자거래 사업자	<<전자거래기본법>> 제2조(정의) “전자거래사업자”라 함은 전자거래를 업으로 하는 자를 말한다. <<신용정보의 이용 및 보호에 관한 법률>> 제2조(정의) “신용정보제공 이용자”라 함은 고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻어지거나 만들어낸 신용정보를 신용정보업자 또는 신용정보집중기관에게 제공하거나 신용정보업자 또는 신용정보집중기관으로부터 신용정보를 지속적으로 제공받아 본인의 영업에 이용하는 자로서 대통령령이 정하는 자를 말한다. <<소비자기본법>> 제2조(정의) “사업자”라 함은 물품을 제조(가공 또는 포장을 포함한다)·수입·판매하거나 용역을 제공하는 자를 말한다.
S3	정보통신 서비스 제공자	<<정보통신망 이용촉진 및 정보보호 등에 관한 법률>> 제2조(정의) “정보통신서비스 제공자”란 「전기통신사업법」 제2조제1항 제1호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
S4	금융	<<신용정보의 이용 및 보호에 관한 법률>> 제2조(정의) “신용정보업자”라 함은 신용정보업을 영위할 목적으로 제4조의 규정에 의하여 금융위원회의 허가를 받은 자를 말한다. “신용정보집중기관”이라 함은 신용정보를 집중하여 관리·활용하는 자로서 제17조제1항의 규정에 의하여 등록한 자를 말한다. <<금융실명거래 및 비밀보장에 관한 법률>> 제2조(정의) 1. “금융기관”이라 함은 다음 각목에 정하는 것 가. 한국은행·한국산업은행·한국수출입은행·중소기업은행 및 은행법에 의한 금융기관 나. 장기신용은행법에 의한 장기신용은행 다. 자본시장과 금융투자업에 관한 법률에 따른 투자매매업자·투자중개업자·집합투자업자·신탁업자·증권금융회사·종합금융회사 및 명의개서대행회사 라. - 마. 상호저축은행법에 의한 상호저축은행과 그 중앙회 바. 농업협동조합법에 의한 농업협동조합과 그 중앙회 사. 수산업협동조합법에 의한 수산업협동조합과 그 중앙회 아. 축산업협동조합법에 의한 축산업협동조합과 그 중앙회 자. 인삼협동조합법에 의한 인삼협동조합과 그 중앙회 차. 신용협동조합법에 의한 신용협동조합과 그 중앙회 카. 새마을금고법에 의한 금고와 그 연합회 타. -

		파. - 하. 보험업법에 의한 보험사업자 거. 우체국예금•보험에관한법률에 의한 체신과서 너. 기타 대통령령이 정하는 기관
S5	의료	<<보건의료기본법>> 제3조(정의) “보건의료기관”이라 함은 보건의료인이 공중 또는 특정 다수인을 위하여 보건의료서비스를 행하는 보건기관·의료기관·약국 기타 대통령령이 정하는 기관을 말한다.
S6	이용자	<<정보통신망 이용촉진 및 정보보호 등에 관한 법률>> 제2조(정의) “이용자”란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다. <<전자거래기본법>> 제2조(정의) “전자거래이용자”라 함은 전자거래를 이용하는 자로서 전자거래 사업자 외의 자를 말한다. <<소비자기본법>> 제2조(정의) “소비자”라 함은 사업자가 제공하는 물품 또는(시설물을 포함한다.)을 소비생활을 위하여 사용(이용을 포함한다)하는 자 또는 생산활동을 위하여 사용하는 자로서 대통령령이 정하는 자를 말한다.

나. 생명주기 관련 개인정보보호 법 정책주기

생명주기는 개인정보 처리에 해당하는 과정을 개인정보 생명주기라 말하며, 생명주기를 4단계로 나누고, 각 단계에 대한 정의 및 수행되는 개인정보 처리 내용은 다음과 같이 정리될 수 있다.

[표 21] 개인정보 생명주기 분류

생명주기 단계	설명
수집	개인정보 소유자의 개인정보를 수집하는 단계.
저장 및 관리	개인정보 소유자의 개인정보를 저장하고 이를 관리하는 단계.
이용 및 제공	개인정보 소유자의 개인정보 일부를 여러 가지 필요에 의해 이용하는 단계
파기	개인정보 소유자의 개인정보를 보유기간이 종료하면 즉시 파기하는 단계.

다. 주체관련 개인정보보호법 정책정의

법 보호 하에 있는 PCE 사용자를 관리자를 제외한 6가지 주체로 구분 후, 해당 주체에 관련되는 개인정보보호 법을 생명주기별로 구분하여 적용하였다. 생명주기에 맞춰 OECD의 6개 원칙을 적용한 후, 주체와 개인정보 생명주기에 맞춰 구분한 법률은 아래의 [표 19]와 같다.

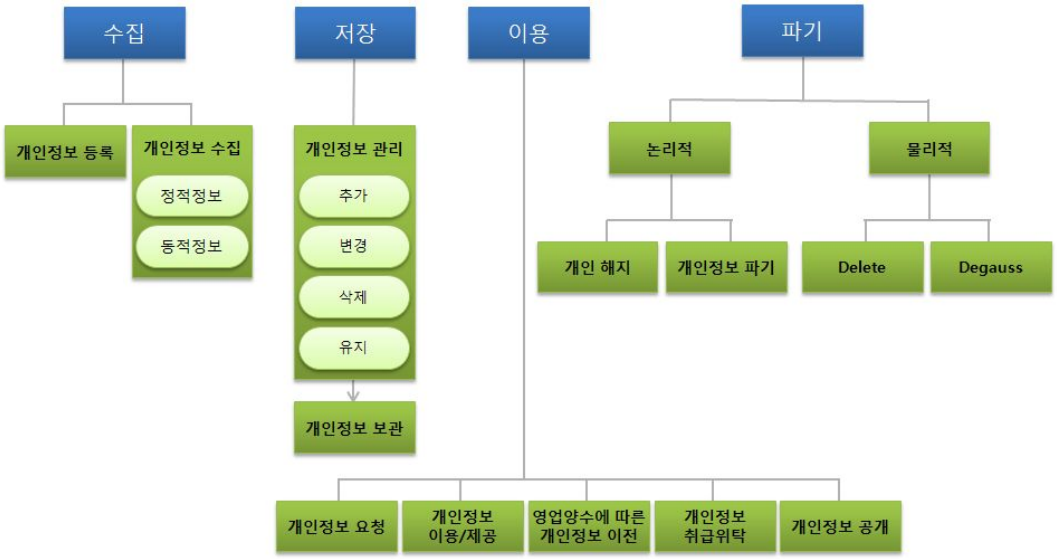
[표 22] 주체 및 개인정보 생명주기 분류 표

생명주기 / OECD / 주체	수집	저장	이용	파기
	수집제한	데이터 정확성	사용제한	공개
	목적 명시		개인 참여	
정부	(2)제3조2 개인정보보호의 원칙 (3)제14조 암호제품의 사용			
	(2) 제4조 개인정보의 수집 (2) 제7조2 개인정보보호방침 (3) 제12조 개인정보보호	(3) 제13조 영업비밀보호	(2) 제8조 개인정보 파일대장의 작성 (2) 제10조 처리 정보의 이용 및 제한 (2) 제12조 처리정보의 열람 (3) 제13조 영업비밀보호	(2) 제10조2 개인정보파일의 파기
전자거래 사업자	(3)제14조 암호제품의 사용			
	(3)제12조 개인정보 보호 (3)제17조 전자거래사업자의 일반적 준수사항	(3)제13조 영업비밀보호	(3)제13조 영업비밀보호	(1)제29조 개인정보의 파기
정보통신 서비스 제공자	(1)제22조 개인정보의 수집, 이용, 동의 등 (1)제49조 비밀 등의 보호			
	(1)제23조 개인정보의 수집 제한 등	(1)제28조 개인정보의 보호 조치 (1)제28조 개인정보의 누설 금지	(1)제28조 개인정보의 보호 조치 (1)제28조2 개인정보의 누설금지	(1)제29조 개인정보의 파기
금융	(4)제4조 금융거래의 비밀보장 (5)제26조 신용정보업자 등의 금지사항 (5)제27조 업무목적 외 누설금지 등			
	(5)제13조 수집, 조사의 원칙	(4)제4조3 거래정보 등의 제공내용의 기록, 관리	(5)제24조 개인신용정보의 제공, 이용의 제한	(1)제29조 개인정보의 파기
의료	(7)제13조 비밀보장			
	(7)제53조 보건의료통계, 정보관리시책	(7)제53조 보건의료통계, 정보관리시책	(7)제11조 보건의료에 관한 알 권리	(1)제29조 개인정보의 파기
이용자	(1)제30조 이용자의 권리 등 (6)제15조 개인정보의 보호			
	(5)제31조 법정대리인의 권리		(7)제11조 보건의료에 관한 알 권리	

이를 통해 개인정보가 관리 및 이용되는 과정에서 기본이 되는 법률과 정책을 적용하여 안전하게 보호되도록 한다.

라. 주체기반의 정책관리 정의

개인정보의 관련 법 분석한 내용을 개인정보의 생명주기에 맞춰 다양한 개인정보의 이용 타입을 구분한다. 이를 통해 개인정보를 사용하는 목적에 따라 세부적으로 법을 적용할 수 있도록 한다. 생명주기에 따른 타입은 [그림 4]와 같다.



[그림 4] 생명주기별 타입 구분

기본적으로 적용되는 법 이외에 세부적으로 분류한 타입을 토대로 구분된 주체에 맞춰 개인정보보호 관련법을 적용하였다. 다음은 개인정보보호 관련 법률을 주체와 타입에 맞춰 분류한 표이다. 이를 생명주기 4단계에 따라 살펴보면 아래와 같다.

① 수집

수집 단계에는 개인정보 소유자가 입력한 정보를 등록하는 타입과 이 정보를 수집하는 타입에서의 금지사항 등을 추가적으로 나타낸다.

[표 23] 수집 단계에서의 주체별 정책

	정부	전자거래 사업자	정보통신서비스 제공자	금융	의료	이용자
개인정보 등록			(1) 제23조 주민등록번호 외의 회원가입 방법 개인정보의 수집 제한 등			(7)제13조 비밀보장
개인정보 수집			(1) 제49조2 속이는 행위에 의한 개인정보의 수집금지 등 (1)제50조2 전자우편주소의 무단 수집행위 등 금지 (1)제50조5 영리목적의 광고성 프로그램 등의 설치	(5) 제15조 수집·조사의 제한 (5) 제16조 수집·조사 및 처리의 위탁		

② 저장

저장 단계에서 개인정보를 관리 및 보유 하며 발생할 수 있는 삭제 요청 처리에 관한 사항 및 관리자의 준수 사항을 명시하고 있다.

[표 24] 저장 단계에서의 주체별 정책

	정부	전자거래 사업자	정보통신서비스 제공자	금융	의료	이용자
개인정보 관리	(2)제6조 개인정보 파일의 보유·변경시 사전협의 (2)제7조2 개인정보 보호방침 (2)제 8조 개인정보 파일대장의 작성 (2)제14조 처리정보의 정정 및 삭제 등	(3)제17조 전자거래 사업자의 일반적 준수사항	*유지 (1)제27조2 개인정보 취급방침의 공개 (1)제44조3 임의의 임시조치 (1)제47조3 이용자의 정보보호 *삭제 (1)제44조2 정보의 삭제요청 등	(5)제18조 신용정보의 정확성 및 최신성의 유지		(5)제31조 법정대리인의 권리 *삭제 (5)제44조2 정보의 삭제요청 등
개인정보 보유				(5)제20조 신용정보관리 책임의 명확화 및 업무처리기록의 보존		

③ 이용

이용 단계에서는 개인정보를 열람하거나 이용할 때의 제한 사항과 방법, 개인정보의 이전 및 취급 위탁시의 처리 방법에 대한 법률로 구성된다.

[표 25] 이용 단계에서의 주체별 정책

	정부	전자거래 사업자	정보통신서비스 제공자	금융	의료	이용자
개인정보 요청	(2)제12조 처리정보의 열람 (2)제13조 처리정보의 열람제한 (3)제24조 전자거래의 표준화 (3)제28조 전자거래 통계 등 실태조사			(5)제25조 신용정보의 열람 및 정정청구 등		
개인정보 이용 및 제공	(1)제44조7 불법정보의 유통금지 등	(1)제44조7 불법정보의 유통금지 등	(1)제24조 개인정보의 이용 제한 (1)제24조2 개인정보의 제공 동의 등 (1)제44조 정보통신망에서의 권리보호 (1)제44조7 불법정보의 유통금지 등 (1)제47조3 이용자의 정보보호 (1)제50조4 정보 전송 역무 제공 등의 제한			(1)제44조 정보통신망에서의 권리보호
영업양수에 따른 이전	(3)제31조14 공인전자문서보관소 영업의 양도·양수 등	(3)제31조14 공인전자문서보관소 영업의 양도·양수 등	(1)제26조 영업의 양수 등에 따른 개인정보의 이전	(5)제14조 공공기관에 대한 신용정보의 열람 및 제공요청등		
개인정보 취급위탁	(2)제11조 개인정보 취급자의 의무		(1)제25조 개인정보의 취급위탁	(5)제16조 수집·조사 및 처리의 위탁		
개인정보 공개	(2)제7조 개인정보파일의 공고			(5)제22조 신용정보 활용체제의 공시		

④ 파기

파기 단계의 정책은 개인정보의 소유자가 개인정보 해지 요청 시 정보의 삭제와 파기에 관련된 법률을 나타낸다.

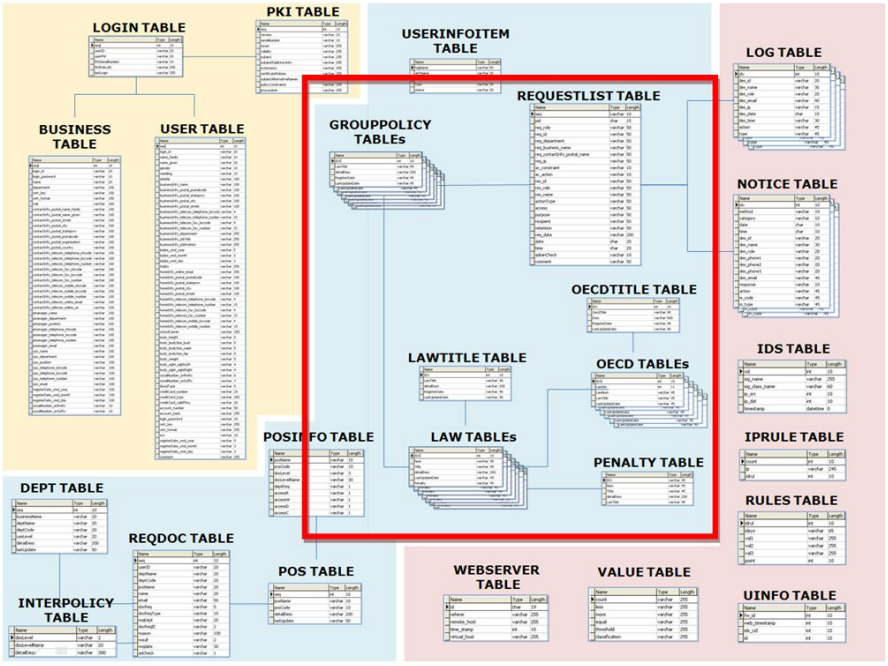
[표 26] 파기 단계에서의 주체별 정책

	정부	전자거래 사업자	정보통신서비스 제공자	금융	의료	이용자
개인정보 관리	개인해지 (2)제14조 처리정보의 정정 및 삭제 등 개인정보파기 (3)제24조 전자거래의 표준화 (3)제31조15 전자문서보관등 영업의 폐지	개인정보파기 (3)제31조15 전자문서보관등 영업의 폐지	개인정보파기 (1)제27조2 개인정보 취급방침의 공개 (1)제30조 이용자의 권리 등 (1)제44조2 정보의 삭제요청 등	개인정보파기 (5)제18조 신용정보의 정확성 및 최신성의 유지		개인정보파기 (1)제44조2 정보의 삭제요청 등
개인정보 보유				(5)제21조 폐업 시 보유정보의 처리		

4) DB 구성

이와 같이 분리된 개인정보보호 관련 정책은 Database에 저장 및 관리하여, 개인정보 이용 요청 시 시스템이 자동적으로 해당 법률을 적용할 수 있도록 한다. 아래의 [그림 5]는 PIPS의 전체 DB 테이블로 정책 엔진에 사용되는 DB 구성 내역은 아래와 같다.

- **RequestList Table** - APPEL 문서로 정보 요청 한 것을 파싱하여 Table에 저장되어 있고, 이후 Log 기록과 사용자 Notice 기능에 연결되어 사용된다.
- **GroupPolicy Table** - 국내 개인정보보호관련 법률들로 개인정보 요청 시 해당되는 법률이 적용되도록 한다.
- **Law Table** - 국내 관련 법률들 내에 법항 및 세부내용들로 구성된다.
- **OECDTitle Table** - OECD 원칙들이 항목 별 분류되어 있다.
- **OECD Table** - 해당 OECD 원칙에 적용되는 국내 개인정보보호관련 법이 적용된 테이블이다.
- **Penalty Table** - 개인정보보호관련 법에 적용되는 벌칙이 저장되어 있다.



[그림 5] PCE DB 테이블 구성

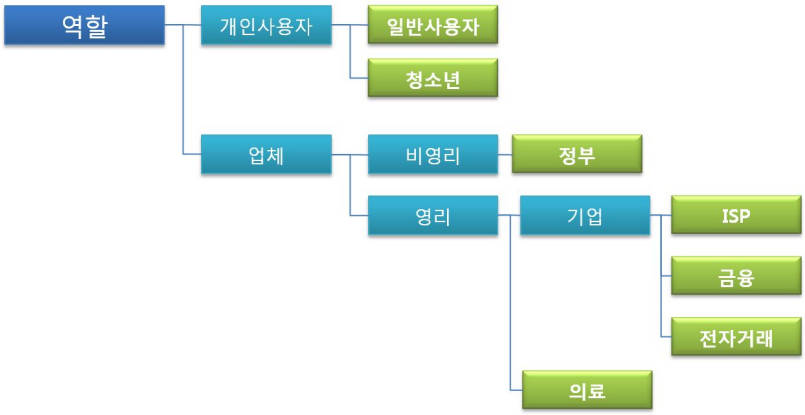
3.2.2 개인정보 접근제어 기능

개인정보 접근제어 기능은 업체에서 필요로 접근하고자 하는 개인정보에 대해 요청자의 역할과 정보의 이용 목적에 따라 접근제어를 가능하게 한다. 이때 개인정보를 다루는 XML 기반의 표준 언어를 통해 법률을 적용하고 이를 시스템에서 자동적으로 분석하여 요청에 반영되도록 한다.

1) 역할분류

PCE에서 업체별로 그룹이 분류되고 그룹 내에 있는 세부적인 역할에 할당 되어 적합한 권한이 주어진다. 권한은 조직의 구조를 유연하게 반영할 수 있는 역할기반의 접근제어(Role Based Access Control)를 이용하여 사용자의 역할에 맞는 제한된 권한을 갖는다. 이는 권한을 개인에게 직접 부여하는 것이 아니라 PCE 시스템에서 필요로 하는 역할을 분류하여 개인정보

이용 권한을 부여하는 것으로 시스템을 이용하는 사용자들을 편리하게 관리할 수 있고 사용자에게 할당되는 이용기능이나 책임을 추가 및 삭제하기 용이하다. PCE의 사용 주체는 위의 장(3.2.1 개인정보보호 정책 엔진 기능의 3) 국내 법률 내 주체정의)에서 다루었던 주체 6가지로, 아래 [그림 6]은 사용자의 역할을 계층적으로 보여준다.



[그림 6] 사용주체 계층 분류

2) 목적분류

개인정보이용을 위한 목적을 분류한다. 이는 분류된 목적을 이용하여 기업이 개인정보를 요청하면 PCE 시스템에서 목적에 맞추어 필요한 개인정보만을 제공하게 하여 필요 이상의 정보남용을 막는다. 이용목적을 생명주기별로 나누어 분류하면 아래의 [표 25]와 같다.

[표 27] 개인정보 이용 목적 분류

수집	**상품가입**		새로운 서비스 상품 가입 및 신청 시 개인정보 수집
	회원가입		웹 사이트 및 서비스에 사용자 회원 가입
저장 및 관리	**DB 저장**		수집 된 회원 개인정보 DB 저장
	권한관리	Admin	저장 및 관리하는 관리자
		Staff	저장 된 정보를 다루는 내부자

이용	본사	**마케팅**	홍보 마케팅 시 필요한 정보
		통계	통계 자료 산출 시 필요한 정보
		결제	결제 시 필요한 정보
		서비스	서비스 제공 시 필요한 정보
		조회	고객정보 조회 시 필요한 정보
	제 3사	**마케팅**	홍보 마케팅 시 필요한 정보
		통계	통계 자료 산출 시 필요한 정보
		결제	결제 시 필요한 정보
		서비스	서비스 제공 시 필요한 정보
		위탁	타 업체로의 고객정보 위탁 및 이전
파기	**파기**		저장 및 관리 중인 개인정보 파기

각각의 목적에 따라 주체별 접근 등급을 구분하여 적용한다.

3) 항목분류

여러 사항의 개인정보가 이용되는 단계에서 보다 효율적이고 체계적으로 개인정보를 보호하기 위해 APPEL 표준 언어를 사용하여 적용한다. (이에 대한 상세한 설명은 아래의 5) APPEL에서 다루도록 한다.) APPEL을 통해 이용되는 개인정보항목을 표준으로 정해진 태그를 이용한다. 국내 법률이 반영되어 새로 추가된 항목 또한 포함되어 있다. APPEL에서 사용하는 태그를 적용한 개인정보 항목을 중요도에 따라 P1-P6로 나누고, 개인정보보호진흥원에서 발표한 개인정보의 유형별로 나누어 적용한 표이다. P1은 결제정보와 비밀번호와 같이 가장 중요하게 보호되어야 할 정보이고, 등급이 높아질수록 중요도가 낮고 공개가능 정도가 높은 정보로 구성된다.

[표 28] 개인정보 항목별 유형 및 등급 구분

등급	태그명	속성명	유형					
			일반 정보	의료/ 건강 정보	기호/ 성향 정보	금융 정보	사회적 정보	기타
P6	U.login.id	회원 아이디	V					
	U.name.*	회원 이름	V					
P5	U.ext	정책공개등급						V

	U.gender	성별	V					
	U.wedding	결혼	V					
	U.jobtitle	업종					V	
	U.business-info.postal.name	회사 이름					V	
	U.business-info.postal.street	회사 주소					V	
	U.business-info.telecom.telephone	회사 번호					V	
	U.business-info.telecom.fax	회사 팩스					V	
	U.business-info.department	부서명					V	
	U.business-info.job-title	직책					V	
	U.business-info.job-position	직업					V	
P4	U.bdate	생년월일	V					
	U.hobby	취미			V			
	U.home-info.online.email	e-mail						V
P3	U.home-info.postal.*	집주소	V					
	U.home-info.telecom.telephone	집 전화번호	V					
	U.home-info.telecom.fax	팩스번호	V					
	U.home-info.telecom.mobile	핸드폰 번호	V					
	U.school-carrier	학력					V	
	U.body.height	키		V				
	U.body.body-size.*	신체사이즈		V				
	U.body.weight	몸무게		V				
	U.body.sight.*	시력		V				
P2	U.social-number	주민등록번호	V					
	U.blood-type	혈액형		V				
P1	U.credit-card.number	카드 번호				V		
	U.account.number	계좌번호				V		
	U.account.bank	거래은행				V		
	U.credit-card.valid-thru	유효기간				V		
	U.credit-card.type	카드 회사				V		
	U.login.password	로그인 비밀번호	V					

4) 접근제어

아래의 [표 27]은 목적과 역할에 따라 접근 가능한 정보의 등급을 정보의 생명주기에 따라 분류한 것이다. P1, P2와 같이 정보보호 등급이 높은 항목은 꼭 필요한 목적을 가지고 합당한 역할을 가진 사용자에게만 접근이 가능하도록 한다. PCE는 개인정보의 이용 및 제공단계에서의 안전한 개인정보 사용을 목표로 하고 있기 때문에 이용 및 제공단계에 초점을 맞춘다.

[표 29] 생명 주기에 따른 이용 목적 및 개인정보 접근 제어

			정부	금융	전자통신	전자거래	의료	이용자
수집	상품가입			P1-P6	P2-P6 (의료 정보 제외)	P2-P6 (의료 정보 제외)	P2-P6	P1-P6
	회원가입							
저장 및 관리	DB저장			P1-P6	P2-P6	P2-P6	P2-P6	P1-P6
	권한관리	Admin		P1-P6	P2-P6	P2-P6	P2-P6	-
		Staff		P3-P6	P3-P6	P3-P6	P3-P6	-
이용	서비스 본사	마케팅		P3-P6	P3-P6	P3-P6	P3-P6	-
		통계		P3-P6	P3-P6	P3-P6	P3-P6	-
		결제		P1	-	-	-	-
		서비스		P2-P6	P2-P6	P2-P6	P2-P6	-
		조회		P1-P6	P2-P6	P2-P6	P2-P6	P1-P6
	서비스 제3사	마케팅		P3-P6	P3-P6	P3-P6	P3-P6	P3-P6
		통계		P3-P6	P3-P6	P3-P6	P3-P6	P3-P6
		결제		P1	-	-	-	-
		서비스		P3-P6	P3-P6	P3-P6	P3-P6	P3-P6
		위탁		P1-P6	P2-P6	P2-P6	P2-P6	-
파기				P1-P6	P2-P6	P2-P6	P2-P6	P1-P6

5) APPEL

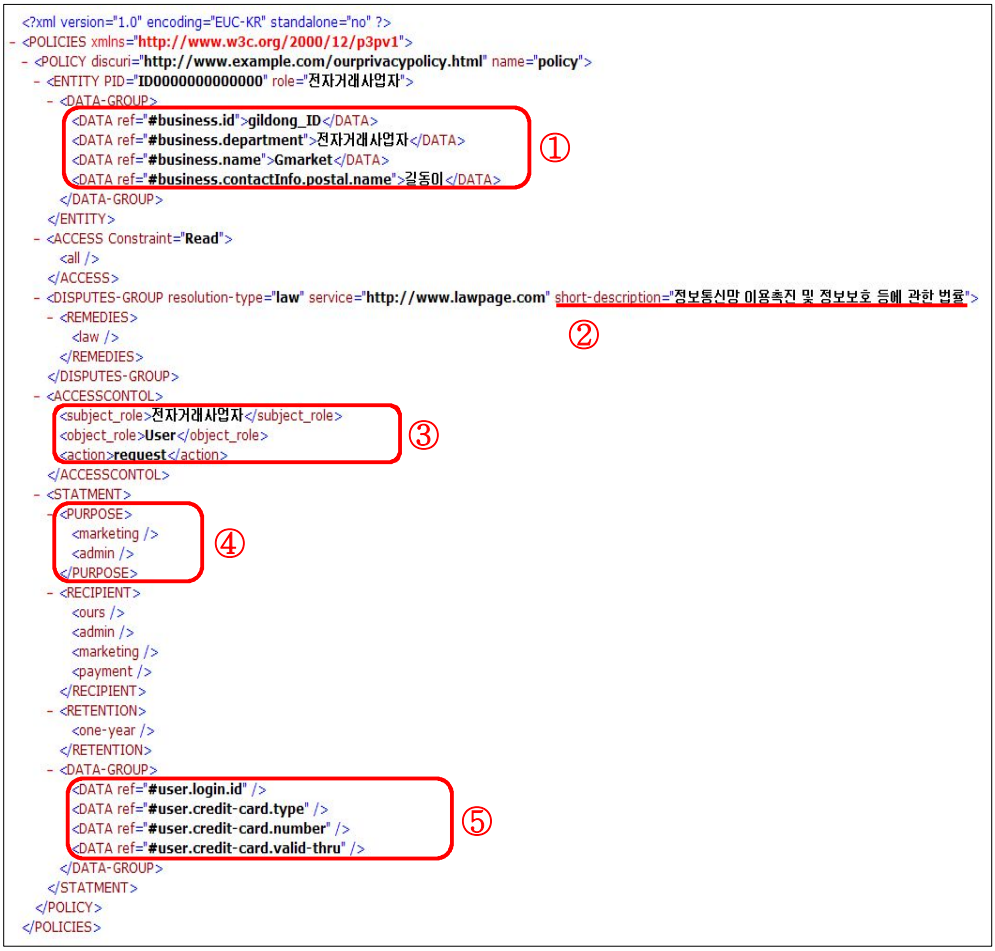
PCE에서 효과적으로 개인정보를 보호하기 위해 개인정보가 이용되는 내역을 APPEL문서를 이용한다. 이는 정보통신서비스 제공자와 서비스 이용자 사이에서 개인정보보호정책을 자동분석이 가능한 XML 형식으로 표현하는 규격이다. 국내의 실정이나, 개인정보보호 관련 법류에서 정하고 있는 개인정보보호정책에 대한 의무고지사항을 반영하여 국내 환경에 적합하게 이

용하였다. 다음 [표 28]은 APPEL의 주요 활용 형식을 나타낸 것이다.

[표 30] APPEL 표준 형식

```
<appel:RULESET xmlns:appel="http://www.w3.org/2002/04/APPELv1"
                    xmlns:p3p="http://www.w3.org/2000/12/P3Pv1"
                    crtdby="W3C"crtdon="2001-02-19T16:04:02+01:00">
    <POLICIES xmlns="http://www.w3c.org/2002/01/P3Pv1">
        <DATASCHEMA> 개인정보 항목 정의 </DATASCHEMA>
        <POLICY name="개인정보취급방침의 이름" opturi ="회원정보 변경
         페이지 URI" discuri ="개인정보취급방침 고지 페이지 URI">
        <ENTITY서비스 제공 기관 정보 </ENTITY>
        <ACCESS> 이용자 및 법정대리인의 권리 </ACCESS>
        <DISPUTES-GROUP>
            개인정보 관련 고객서비스 조직 등 정보
        </DISPUTES-GROUP>
        <STATEMENT>
            개인정보 수집 및 파기 방법, 수집 및 이용 목적, 제3자 제공
            및 위탁 여부, 보유 및 이용기간, 수집하는 개인정보
        </STATEMENT>
        <STATEMENT>
            <NON-IDENTIFIABLE>
                인터넷 접속 파일 등 개인정보를 자동으로 수집하는
                장치의 설치·운영 및 그 거부에 관한 사항을 직접
                서술
            </NON-IDENTIFIABLE>
        </STATEMENT>
    </POLICY>
</POLICIES>
```

아래의 [그림 7]은 PCE에서 생성된 APPEL 문서의 예시로, '전자거래사업자'가 marketing을 목적으로 고객의 개인정보 중 id와 신용카드 정보를 요청하는 사항에 대한 APPEL 문서이다.



[그림 7] APPEL 문서 예시

상세 내역에 대해 살펴보면, ①번 항목 부분은 개인정보를 요청하는 요청자의 정보이다. 국내법 규정에 맞게 개인정보 관리자의 정보를 표기한다. ②번 항목 부분은 현재 이루어진 요청이 적용되는 법률을 나타낸다. ③번 항목은 차례대로 정보 요청자의 역할, 개인정보 소유자의 역할(현재 사용자), 개인정보 요청 타입을 나타낸다. 요청에 대한 목적명시 부분은 ④번 항목 부분의 <PURPOSE>에서 알 수 있다. 끝으로 ⑤번 항목은 요청자가 이용하고자 하는 개인정보의 항목이다. 현재 개인정보 소유자의 ID값과 신용카드

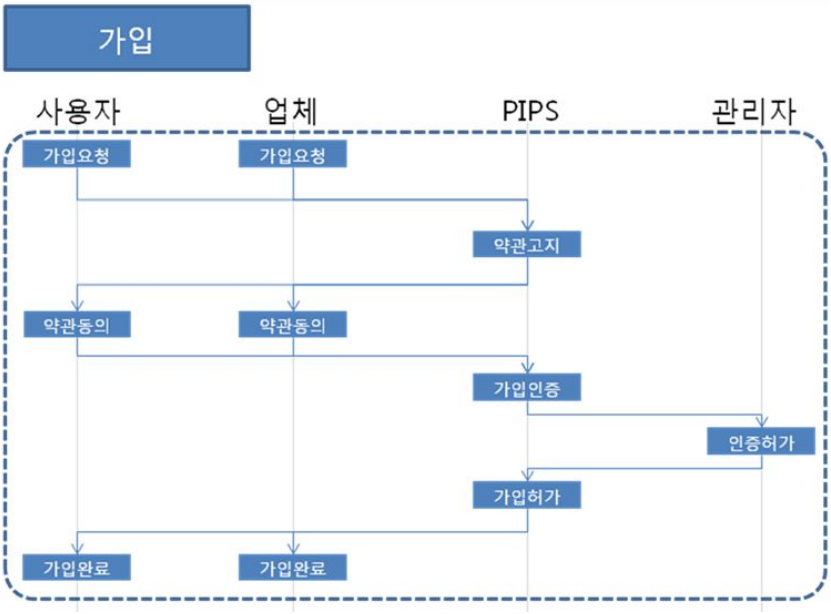
번호와 유효기간을 요구하고 있다. 이외에 기존에 제시된 개인정보 관련 항목과 PCE 내 필요에 맞게 'ENTITY PID', 'subject_role', 'object_role', 'action'등을 추가하였다. PCE의 개인정보 접근제어 시 필요한 요청자의 PKI 인증번호에 따른 역할과 주체의 역할 및 이용 목적을 명시하고 이를 이용하여 해당 법과 적용하여 법률 보호 하에 개인정보 접근을 가능하도록 한다.

6) 플로우차트

개인정보에 대한 접근 제어 과정을 단계별 플로우차트로 나타내면 다음과 같다.

가. 가입

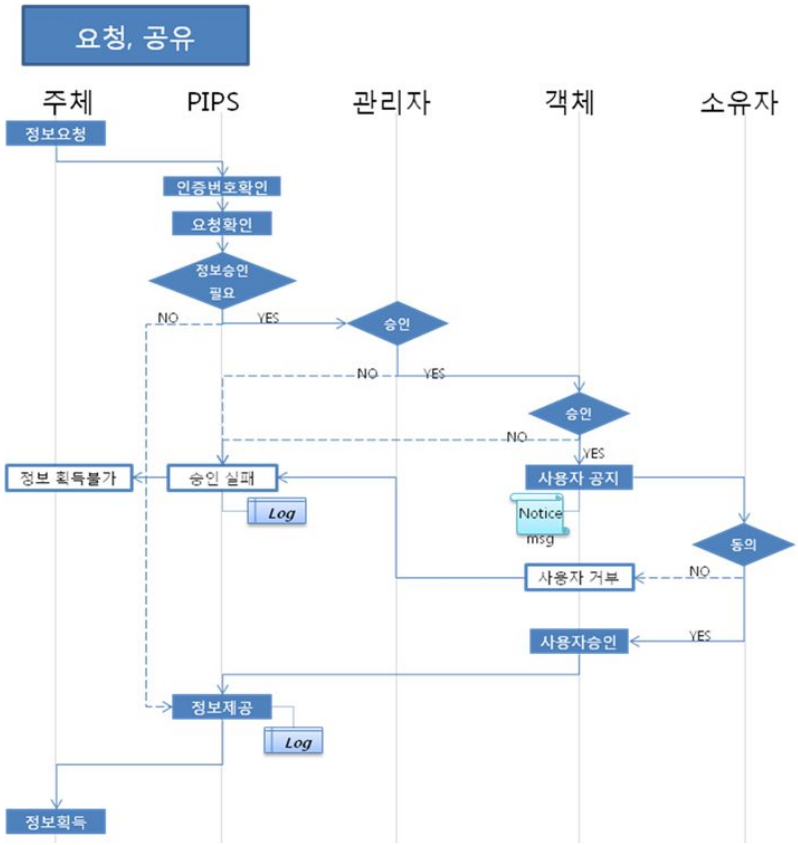
PCE에 사용자와 업체가 PCE에 가입하는 과정이다. 가입요청이 들어오면 PCE는 해당 역할에 맞는 약관을 고지한다. 이에 동의한 후 가입이 완료된다.



[그림 8] 가입 시 Flowchart

나. 요청, 공유

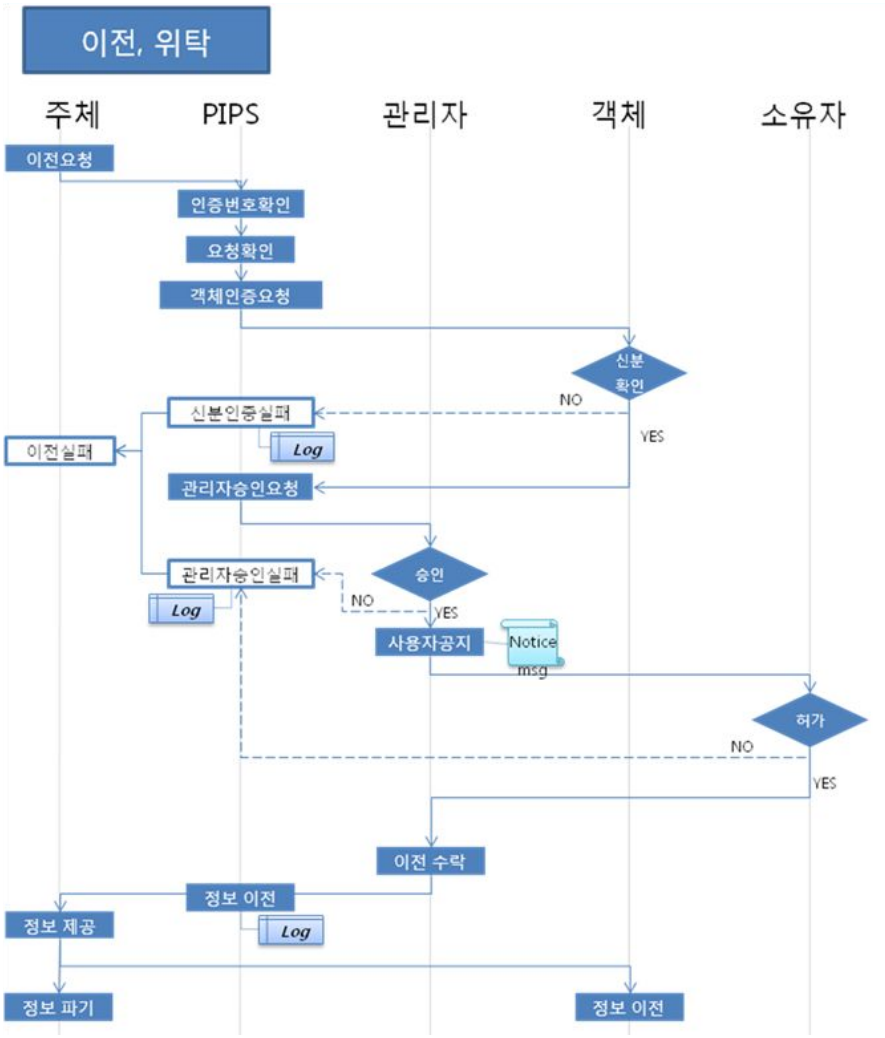
PCE를 통해 요청자(주체)가 개인정보를 요청하고, 목적과 주체의 역할에 따라 정보를 공유하게 되는 과정을 나타낸 그림이다. 주체는 PCE로 로그인 시 인증서를 통해 권한을 부여 받게 되고 이에 따라 고객의 개인정보를 요청한다. 일반적인 정보인 경우 목적과 역할에 따라 요청한 정보가 관리자의 승인으로 제공되게 되고, 만일 민감하거나 보안 등급이 높은 정보의 경우 객체, 즉 개인정보의 소유자에게 제공 동의를 받고 난 후 정보가 제공되게 된다. 이때 관리자나 소유자가 정보 제공을 거부하게 되면, 거부 사항에 대해 로그 기록을 남겨서 불법적인 정보 유출이 없도록 한다.



[그림 9] 요청, 공유 시 Flowchart

다. 이전, 위탁

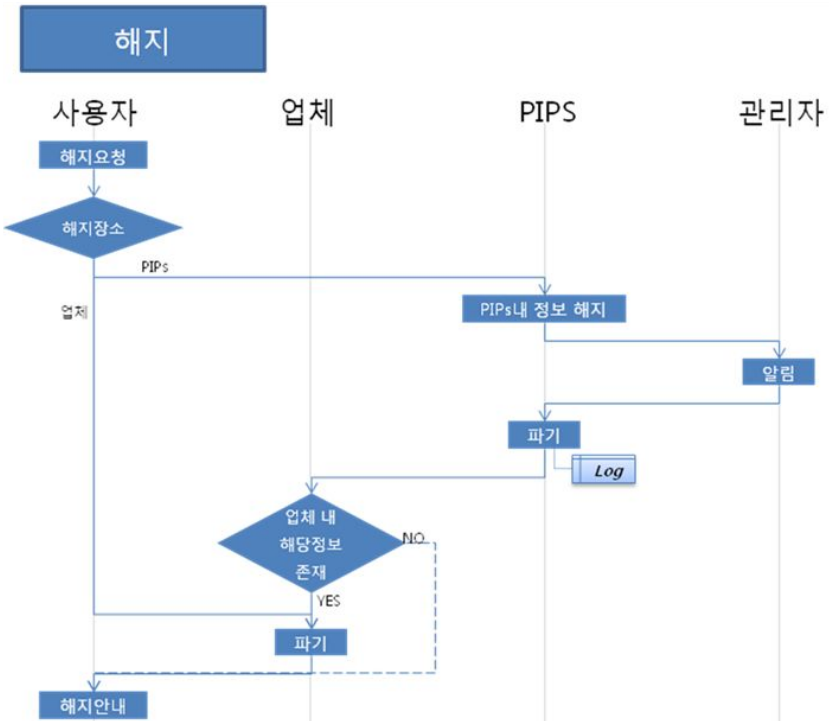
회사의 상황에 의해 관리하는 개인정보를 다른 제3자에게 이전하는 경우를 나타낸다. 전체적인 흐름은 요청, 공유와 비슷하지만 객체에 대한 신분확인을 통해 개인정보를 이전하기에 합당한 업체인지 확인하는 단계가 요청, 공유와 다르다.



[그림 10] 이전, 위탁 시 Flowchart

라. 해지

사용자가 PCE에서 보관, 관리하고 있는 정보에 대한 해지를 요구하는 사항이다. 국내에서는 사용자가 자신의 개인정보에 대한 파기 요청을 하거나 서비스 이용해지를 신청할 경우 즉시 파기해야 한다. 하지만, 예외적으로 보유기간을 갖는 경우가 발생하며 이 경우, 보유 근거가 되는 법률을 확보하고 이를 고지해야 한다.



[그림 11] 해지 시 Flowchart

3.3. PCE 알고리즘

3.3.1 개인정보보호 정책엔진

개인정보보호 정책엔진의 알고리즘은 다음과 같다.

Algorithm Policy Management

```
db_url ← DB 접속 URL;
db_name ← DB에 생성된 DB명;
db_pwd ← DB 접속 패스워드;
Class.forName(연결 드라이브 명 / MySQL);
conn ← getConnection(db_url,db_name,db_pwd);
// 의무적 규제 변수 정의
lawNumber ← 웹페이지에서 의무적 규제에 해당하는 국내 개인정보보호 법항
penalty ← 웹페이지에서 의무적 규제에 해당하는 국내 개인정보보호 관련 벌칙
lawTitle ← 웹페이지에서 의무적 규제에 해당하는 국내 개인정보보호 법률명
lawContents ← 웹페이지에서 의무적 규제에 해당하는 국내 개인정보보호 법 세부내용
// 권고 규제 변수 정의
idx ← 웹페이지에서 권고규제에 해당하는 OECD 원칙
relatedLaw ← 웹페이지에서 권고규제와 관련한 국내 개인정보보호 법항
// 주체별 변수 정의
roleIdx ← 웹페이지에서 주체별에 해당하는 주체값
lifeCycle ← 웹페이지에서 주체별에 해당하는 생명주기
type ← 웹페이지에서 주체별에 해당하는 생명주기 유형
relatedLaws[]← 웹페이지에서 주체에 해당하는 관련 국내 개인정보보호 법항 리스트

switch (policyMngt)
    caseOBLIGATORY:
if (lawNumber=NILorlawTitle=NIL)then
    error "입력 값이 없습니다.";
else then
{
    switch(event)
        caseINSERT:
            if(lawInsert(idx,lawNumber,lawTitle,penalty,lawContents)=TRUE)thenreturntrue;
        caseMODIFY:

if(lawModifyUpdate(titleIdx,idx,lawNumber,lawTitle,penalty,lawContents)=TRUE)thenreturntrue;
 case DELETE:
            if(lawDelete(titleIdx,idx)=TRUE)thenreturntrue;
}
    caseRECOMMEND:
```

```
if (idx=NILorrelatedLaw=NIL)thenerror"입력 값이 없습니다.";
else then
if (oecdModify(idx,relatedLaw))thenreturntrue;
    caseSUBJECT:
if (roleIdx=NILorlifeCycle=NILortype=NIL)then
    error "입력 값이 없습니다.";
else then
if (subjectLawModifyConfirm(idx,relatedLaw)=TRUE)then
return true;

// 주체별 - Modify
subjectLawModifyConfirm(roleIdx,lifeCycle,type,relatedLaws[]){
    // MySQL에서 제공하는 delete 문법 이용
    sql← "delete from ubpolicy where lifecycleTag = ?";
    pstmt← conn.prepareStatement(sql);
    pstmt.setString(1,lifeCycle);
    pstmt.executeUpdate();
    relatedLawLength← relatedLaws.length;
    // relatedLaw 업데이트
    fori← 0 torelatedLawLength{
        strData[]← relatedLaws[i].split("[/]");
        lawTitleIdx← strData[0];
        lawTitleStr← strData[0];
        lawNum← strData[1];
// lawTitle 알기
// MySQL에서 제공하는 select 문법 이용
        sql← "select * from law where Num = ?";
        pstmt← conn.prepareStatement(sql);
        pstmt.setString(1,lawNum);
        rs← pstmt.executeQuery();
        if(rs.next()≠ NIL) then{
            lawValue.setLaw_num(rs.getString("Num"));
            lawValue.setLaw_title(rs.getString("Title"));
// MySQL에서 제공하는 insert 문법 이용
sql2 ← "insert into rolepPolicy values (null, ?, ?, ?, ?, ?, sysdate())";
pstmt2 ← conn.prepareStatement(sql2);
            pstmt2.setString(1,lifeCycle);
            pstmt2.setString(2,type);
pstmt2.setInt(3, lawTitleIdx);
pstmt2.setString(4, lawValue.getLaw_num());
pstmt2.setString(5, lawValue.getLaw_title());
pstmt2.executeUpdate();
```

```
        }
    }
    return true;
    }
    // OECD - Modify
    oecdModify(titleIdx,relatedLaw){
    // MySQL에서 제공하는 delete 문법 이용
    sql ← "delete from oecd";
        pstmt← conn.prepareStatement(sql);
        pstmt.executeUpdate();
        // relatedLaw 업데이트
        strData[]← 관련법(relatedLaw)을 구분하여 배열에 저장
        fori← 0 tostrData.length{
            sql← "select Num, Title from law where Num = ?";
            pstmt← conn.prepareStatement(sql);
            pstmt.setString(1,strData[i]);
            rs← pstmt.executeQuery();
            if(rs.next()≠ NIL) then
            {
                lawValue.setLaw_num(rs.getString("Num"));
                lawValue.setLaw_title(rs.getString("Title"));
                // MySQL에서 제공하는 insert 문법 이용
                sql← "insert into oecd values (null, 1, ?, ?, sysdate());";
                pstmt← conn.prepareStatement(sql);
                pstmt.setString(1,lawValue.getLaw_num());
                pstmt.setString(2,lawValue.getLaw_title());
                pstmt.executeUpdate();
              }
         }
        // MySQL에서 제공하는 update 문법 이용
        sql← "update OecdTitle set LastUpdateDate = sysdate() where IDX = ?";
        pstmt← conn.prepareStatement(sql);
        pstmt.setInt(1,titleIdx);
        pstmt.executeUpdate();
        if(exception)thenreturnfalse;
        returntrue;
    }
    // 법 - Insert
    lawInsert(idx,lawNumber,lawTitle,penalty,lawContents){
        // MySQL에서 제공하는 insert 문법 이용
        sql← "insert into law values (null, ?, ?, ?, sysdate(), ?)";
        pstmt← conn.prepareStatement(sql);
        pstmt.setString(1,lawNumber);
```

```
        pstmt.setString(2,lawTitle);
        pstmt.setString(3,lawContents);
        pstmt.setString(4,penalty);
        pstmt.executeUpdate();
        if(exception)thenreturnfalse;
        return true;
    }
    // 법 - Modify
    lawModifyUpdate(titleIdx,idx,lawNumber,lawTitle,penalty,lawContents){
        // MySQL에서 제공하는 update 문법 이용
    sql ← "update law set Num = ?, Title = ?, detailDesc = ?, LastUpdateDate = sysdate(),
Penalty = ? where idx = ?";
    pstmt ← conn.prepareStatement(sql);
        pstmt.setString(1,lawNumber);
        pstmt.setString(2,lawTitle);
        pstmt.setString(3,lawContents);
        pstmt.setString(4,penalty);
        pstmt.setInt(5,idx);
        pstmt.executeUpdate();
        if(exception)thenreturnfalse;
        returntrue;
    }
    // 법 - Delete
    lawDelete(titleIdx,idx){
        // MySQL에서 제공하는 delete 문법 이용
    sql ← "delete from law7 where idx = ?";
        pstmt← conn.prepareStatement(sql);
        pstmt.setInt(1,idx);
        pstmt.executeUpdate();
        if(exception)thenreturnfalse;
        returntrue;
    }
```

3.3.2 개인정보 접근제어

개인정보 접근제어의 알고리즘은 다음과 같다.

Algorithm User-AccessControl-Request

```
db_url ← DB 접속 URL;
db_name ← DB에 생성된 DB명;
db_pwd ← DB 접속 패스워드;
Class.forName(접속되는 데이터베이스 드라이브 명);
conn ← getConnection(db_url,db_name,db_pwd);
// APPEL 문서 파싱
if (valueDefine(server_ip,server_port,db_name,db_id,db_pwd,ip)=TRUE)then{
    directory← 요청한 APPEL 파일이 있는 디렉토리
    filename← APPEL 파일 명
    while(TRUE){
        client← server.accept();
        is ← client.getInputStream();
        out ← new FileOutputStream(newFile(directory,filename));
        i ← 0;
        while(i← is.read() ≠ -1)
            out.write(i);

// XMLParsing
doc ← APPEL 파일;
root ← APPEL 내 XML 최상위 태그;
ENTITY ← root.getElementsByTagName("ENTITY");
PID ← ENTITY.item(0).getAttributes().item(0).getTextContent();
role ← ENTITY.item(0).getAttributes().item(1).getTextContent();
ACCESS ← root.getElementsByTagName("ACCESS");
constraint ← ACCESS.item(0).getAttributes().item(0).getTextContent();
ACTION ← root.getElementsByTagName("action");
action ← ACTION.item(0).getTextContent();
DATA ← root.getElementsByTagName("DATA");
req_user_info[] ← new String[DATA.getLength()-8];
b_id ← DATA.item(0).getTextContent();
b_name ← DATA.item(1).getTextContent();
b_department ← DATA.item(2).getTextContent();
b_con_name ← DATA.item(3).getTextContent();
b_con_email ← DATA.item(4).getTextContent();
b_con_loccode ← DATA.item(5).getTextContent();
b_con_number ← DATA.item(6).getTextContent();
```

```
b_ip ← DATA.item(7).getTextContent();
// 요청정보
u_id ← DATA.item(8).getTextContent();
for a← 0 toDATA.getLength();
if ( a>7)then
req_user_info[a-8]← DATA.item(a).getAttributes().item(0).getTextContent();
PURPOSE ← root.getElementsByTagName("PURPOSE");
purpose[]← new String [PURPOSE.getLength()];
RECIPIENT ← root.getElementsByTagName("RECIPIENT");
recipient[]← new String[RECIPIENT.getLength()];
RETENTION ← root.getElementsByTagName("RETENTION");
retention ← RETENTION.item(1).getNodeName();
// 요청정보 저장
SaveDB_Request(PID,role,b_id,b_department,b_name,b_con_name,b_ip,constraint,action,u_id,u_role,u_name,purpose,recipient,retention,req_user_info,strDate,strTime,"N");
// 로그기록
SaveDB_Log(b_id,b_con_name,req_role,b_ip,u_id,u_name,u_role,event,strDate,strTime);
        }
}
if (admincheck=TRUE)then{
    sql← "select seq, req_id, date, time, req_role, actionType, res_id, req_data, req_contactInfo_postal_name, res_name, res_role " +"from RequestListTable" + "where seq = ?";
pstmt← conn.prepareStatement(sql);
pstmt.setString(1, seq);
rs ← pstmt.executeQuery();
if (rs.next()≠ NIL) {
    req_id ← rs.getString("req_id");
    req_time← rs.getString("date") + " " + rs.getString("time");
    req_role← rs.getString("req_role");
    req_constraint← "read";
    action_type← rs.getString("actionType");
    res_id← rs.getString("res_id");
    req_info← rs.getString("req_data");
    req_name← rs.getString("req_contactInfo_postal_name");
    res_name← rs.getString("res_name");
    res_role← rs.getString("res_role");
    email← "";
    text← 보낼 메시지;
```

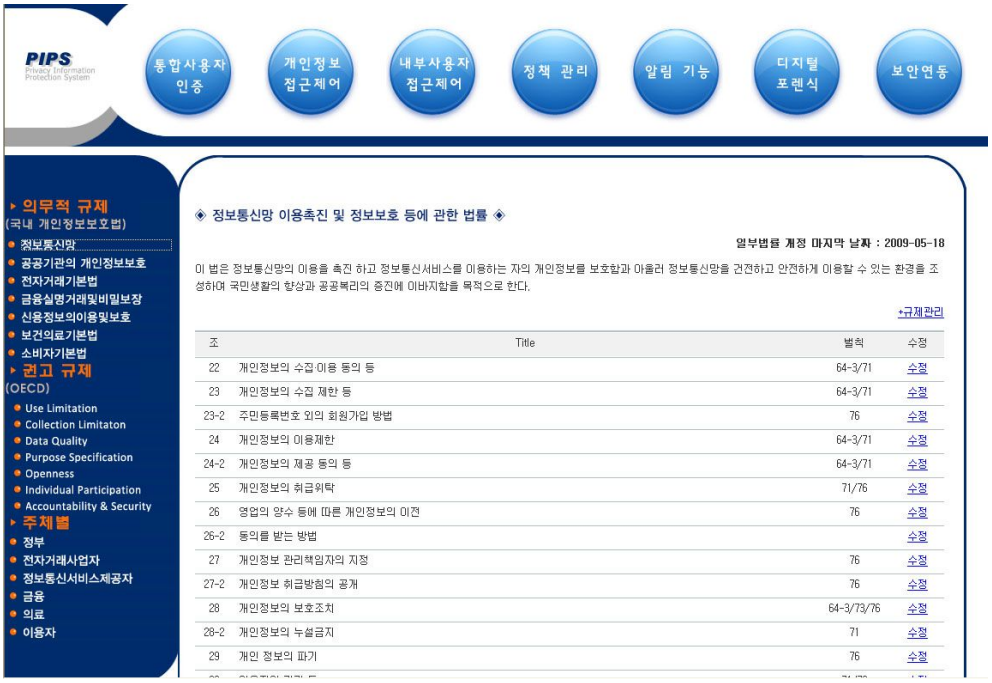
```
if (adminCheckResult=ACCEPT)then{
// 사용자에게 메일 보내기
props.put("mail.smtp.host", ip 주소);
transport.send(mailMessage);
// 관리자 확인 업데이트
sql ← "update request set adminCheck = 'Y' where seq = ?";
pstmt ← conn.prepareStatement(sql);
pstmt.setString(1, seq);
pstmt.executeUpdate();
// Notice 기록
SaveDB_Notice(method,category,strDate,strTime,m_code,m_type,req_id,req_name,r
eq_role,res_id,res_name,res_role,email,resp,action);
// Notice 로그기록
SaveDB_LogNotice(res_id,res_name,res_role,email,method,category,m_type,action,r
esp,strDate,strTime);
if (purpose=General)then
            return ACCEPT;
else if(purpose=SENSITIVE)then
   return WAITING;
}
else if (adminCheckResult=DENY)then{
// 요청자에게 메일 보내기
props.put("mail.smtp.host", ip 주소);
transport.send(mailMessage);
// 관리자 확인 업데이트
sql ← "update request set adminCheck = 'Y' where seq = ?";
pstmt ← conn.prepareStatement(sql);
pstmt.setString(1, seq);
pstmt.executeUpdate();
// Notice 기록
SaveDB_Notice(method,category,strDate,strTime,m_code,m_type,"관리자", "관리자
", "관리자", req_id, req_name, req_role, email, resp, action);
// Notice 로그기록
SaveDB_LogNotice(res_id,res_name,res_role,email,method,category,m_type,action,r
esp,strDate,strTime);
returnDENY;
        }
   }
}
else then
   return;
```

3.4. 프로토타이핑

3.4.1 개인정보보호 정책 엔진

정책관리는 PCE를 국내 개인정보보호 관련 법제도 및 국외 표준화 기반으로 자동관리 하는 기능이다.

1) 의무적 규제 (국내 개인정보보호 법)



[그림 12] 의무적규제 화면

의무적 규제는 국내 개인정보보호 관련법에 대한 것으로 총 7가지의 법률을 준수한다. 이는 관련 법률 내 개인정보보호 법을 리스트화로 보여주며, 관리자는 개인정보보호 관련법이 개정되거나 삭제되었을 시 정책관리를 통해 법을 업데이트 한다.

2) 권고 규제 (OECD)

[그림 13] 권고규제 화면

경제협력개발기구(OECD : Organization for Economic Cooperation and Development)가 제정한 '프라이버시보호 및 개인정보의 국가 간의 유통에 관한 지침'을 채택하였다. 이는 총 8가지 원칙이 존재하며 PCE 시스템에서 적용되는 원칙 내 개인정보보호 법과 매핑 하여 관리된다. 관리자는 적용되는 개인정보보호 법을 수정 및 삭제와 같은 업데이트를 통해 법 개정 시 시스템 적용이 가능하다.

3) 주체별

[그림 14] 주체별 화면

법 보호 하에 있는 사용자를 6가지 주체로 구분하여 개인정보보호 법에 적용한다. 주체별로 적용되는 법은 크게 세 부분으로 보여준다. 먼저, '법률 내 주체정의'로써 해당 주체에 법률적 정의를 설명한 다. 다음은 주체에게 관련하는 개인정보보호 법을 리스트로 보여주며 '규제관리'를 통해 주체에 적용하는 법을 추가 및 수정, 삭제할 수 있다. 마지막 주체에게 해당하는 법을 생명주기별로 구분하여 개인정보보호 관련법을 적용한다. 생명주기에 따라 '규제관리'를 통해 법을 추가 및 수정, 삭제할 수 있다.

3.4.2 개인정보 접근 제어

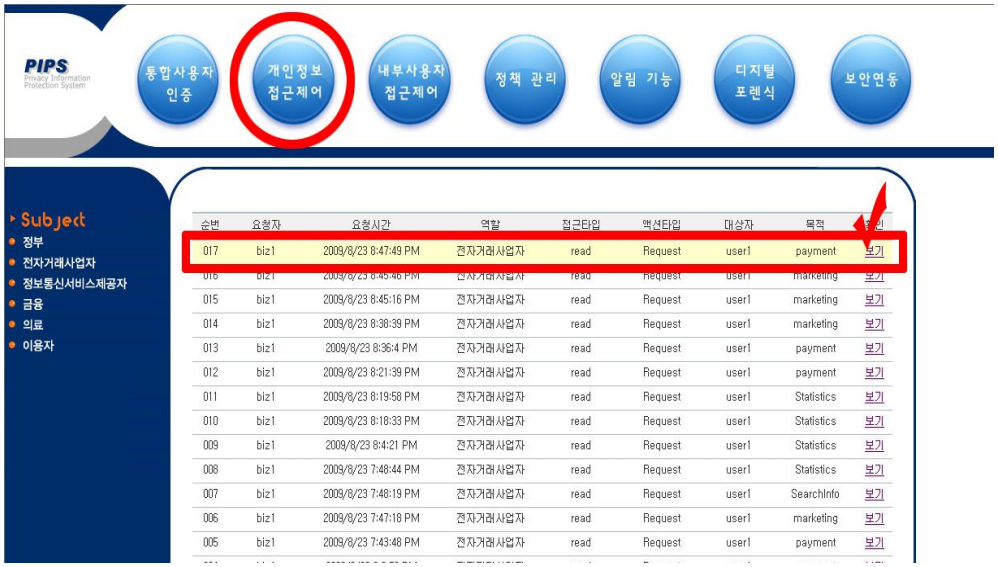
개인정보 접근제어를 관리하는 화면을 나타낸다. 관리자에 의해 정보를 요청한 사람의 접근권한을 변경할 수 있다.

1) 요청 사항 리스트

첫 화면으로는 개인정보를 요청한 사항에 대한 리스트가 뜬다.

요청 사항 리스트는 정보요청 순서에 따른 순번, 요청자와 요청시간, 역할, 접근타입, 액션타입, 대상자, 목적, 확인을 보여준다.

관리자가 확인하지 않은 사항인 경우 노란색 배경으로 표시되어 새롭게 들어온 요청임을 나타낸다.



[그림 15] 요청 사항 확인 전 리스트

요청 사항에 대하여 '보기'를 클릭하게 되면, 선택한 요청 사항에 대한 상세 내용을 보여주는 페이지로 넘어간다.

2) 요청 사항 상세내역

요청사항에 대한 상세정보는 [그림 15]와 같다.

[그림 16] 요청 정보 상세화면

각 항목에 대한 설명은 아래와 같다.

① 요청자 정보

개인정보를 요청하는 사람의 ID, 인증서의 인증번호, 이름, 역할을 나타낸다.

② 대상자 정보

개인정보 소유자로 소유자의 ID, 인증서의 인증번호, 이름, 역할을 나타낸다.

③ 상세정보

요청자가 개인정보를 요청한 목적, 시각, Action Type, 요청한 개인정보 항목, 개인정보의 민감도를 나타낸다.

④ 역할기반 접근제어

접근제어를 나타내는 부분으로 총 4가지로 구성되어 있다.

ㄱ) 개인정보 등급구분

개인정보를 중요도와 항목별로 나누어 분류한다. 요청자가 요청한 정보를 분류에 따라 보여준다.

ㄴ) 접근 제어 상태

요청한 항목에 대하여 접근 가능, 불가능을 나타내고 불가능인 경우 법적인 이유가 근거로 제시된다.

ㄷ) 등급설명

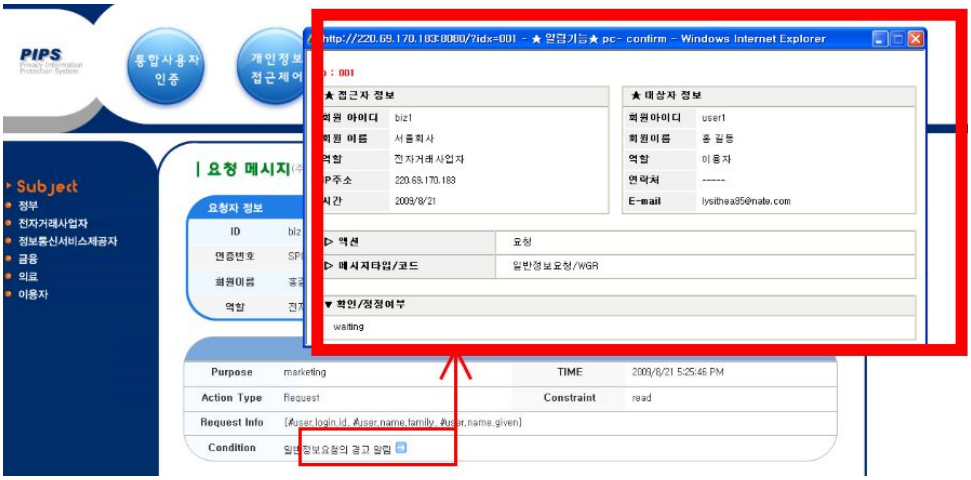
위의 'ㄱ)'에서 등급별로 구분된 정보에 대한 등급 설명을 나타낸다.

ㄹ) 세부사항

세부사항은 'ㄱ)' 에서 분류된 항목별, 등급별 정보에 대한 세부 설명과 구성된 개인 정보 항목들을 나타낸다.

3) 고객 동의 확인

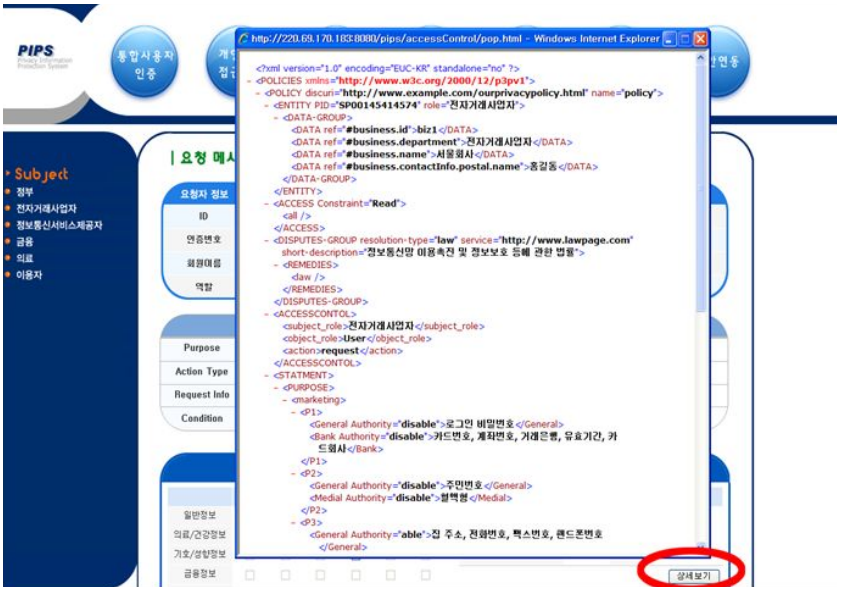
요청한 정보가 민감하거나 중요도가 높은 정보인 경우 고객의 동의가 필요하다. 고객에게 e-mail이나 모바일을 이용하여 개인정보를 요청하는 접근자와 요청 사항에 대해 안내를 한 후, 고객의 동의가 얻어진 경우에 요청자에게 정보가 제공되게 된다.



[그림 17] 사용자 동의 상태 확인

4) APPEL 문서 생성

요청자가 개인정보를 요구한 항목에 대한 접근 가능, 불가능 여부를 상세보기 하면, 요청한 사항에 대한 APPEL 문서가 보이게 됩니다. 이 문서에는 요청자의 회사 정보와, 관련법에 대한 내용, 이용 목적, 요청 개인정보가 나타나있다.



[그림 18] 요청상태 APPEL 문서 생성

5) 요청 항목 관리자 확인

개인정보를 요청하는 이의 역할과 목적에 따라 허용된 범위 이외의 개인정보를 요청하는 경우, 관리자의 확인이 필요하다.

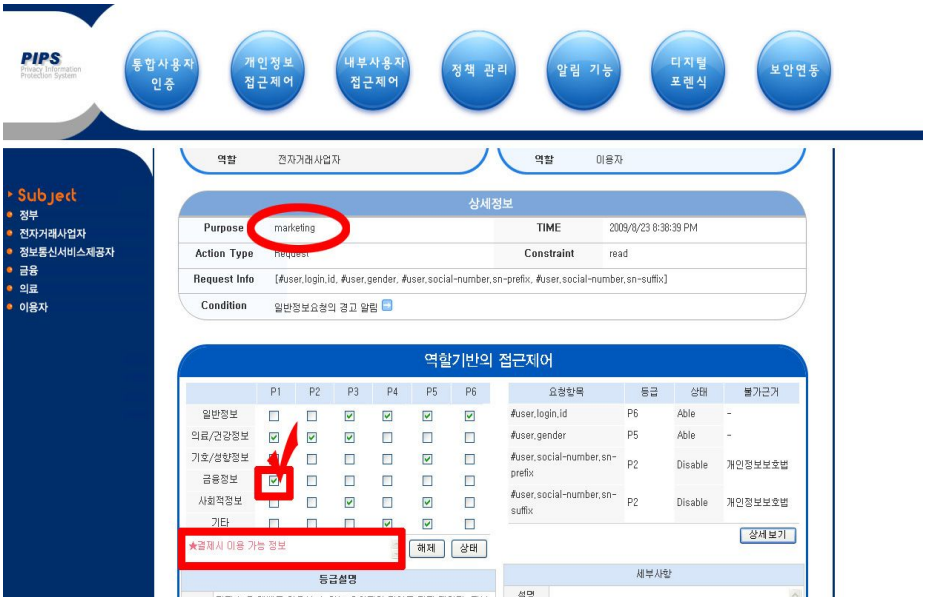
초기에는 목적과 역할에 맞는 항목이 체크되어 나타납니다. 체크된 항목 이외는 비 활성화되어 접근 가능한 정보의 상태를 나타낸다.

[그림 19] 요청 항목 확인

[해제]버튼을 누르면 비활성화 된 항목이 활성화된다. 만일, 체크된 항목 이외의 사항을 요청한 경우 관리자는 [해제] 버튼을 누르고 해당 사항을 체크하여 요청을 수락할 수 있다. [해제]버튼을 한 번 더 누르게 되면 이전 상태(초기 목적과 역할에 맞게 체크된 상태)로 나타낸다.

[그림 20] 요청 항목 해제 상태

만일 관리자가 해제 버튼을 눌러 모든 체크박스가 활성화 된 상태에서 추가적으로 제공할 정보를 선택할 때 PCE는 역할과 목적에 따라 제한된 정보의 경우 알림 메세지를 보여준다.



[그림 21] 목적에 맞는 정보 요청

[상태] 버튼은 최종 요청 승인 사항과 접근 제어 상태를 확인하는 버튼이다. 요청자가 접근하고자 하는 정보 중 접근 불가능(Disable)한 정보가 없다면, “요청 승인 가능” 알림창이 뜬다.

[그림 22] 요청 정보 상태 확인

[그림 23] 상태 확인 알림 창 – 승인

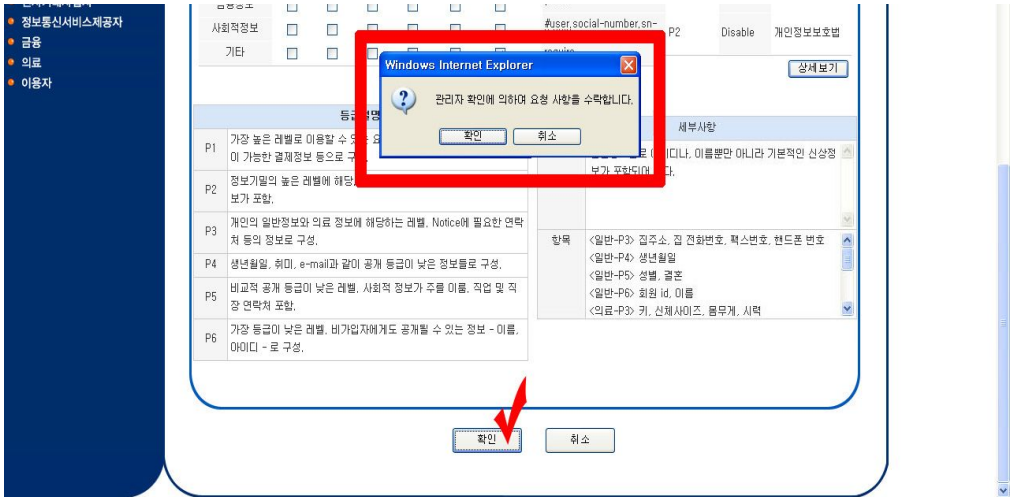
요청자가 접근 하고자 하는 정보 중 역할이나 목적 외의 정보를 요구하고, 관리자가 이를 승인하지 않은 경우, “요청 거부 항목 포함” 알림창이 뜨게 된다.

[그림 24] 상태확인 알림 창 – 거부

하단의 [확인] 버튼을 통해 관리자는 최종적으로 요청사항을 수락 혹은 거부를 한다.

[그림 25] 최종 요청 확인

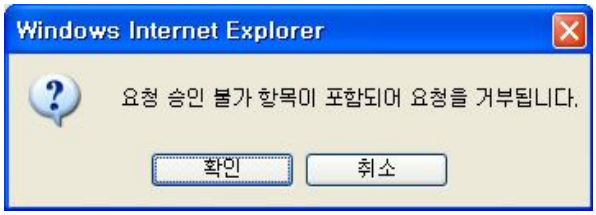
“요청 승인” 상태인 경우 “관리자 확인에 의하여 요청 사항을 수락합니다.” 라는 메시지 창이 뜨며, “확인”을 누르게 되면 요청은 최종 수락되며, 초기의 리스트 화면으로 넘어간다. “취소” 버튼을 누르면 현재 페이지로 돌아온다.



[그림 26] 요청 수락 화면

다음은 확인 버튼을 눌렀을 때 다른 경우를 나타낸다.

“요청 거부 항목 포함” 상태인 경우 “요청 승인 불가 항목이 포함되어 요청을 거부됩니다.” 라는 메시지 창이 나온다. 이때 “확인”을 누르게 되면, 요청은 거부되고 리스트 화면으로 돌아간다. “취소”를 누르게 되면 현재 페이지로 돌아온다.



[그림 27] 요청 거부 알림 창

만일 관리자가 “상태” 버튼을 누르지 않은 경우(최종 상태 확인을 안한 경우), “요청 사항의 [상태] 버튼을 확인해주세요.” 라는 메시지를 통해 상태를 최종 확인하도록 한다.

[그림 28] 상태 확인 요청

관리자가 요청사항을 최종적으로 확인 한 후 리스트로 돌아간 경우, 초기 확인 전 노란 배경색이 하얀색으로 바뀌어 관리자가 확인한 사항임을 나타낸다.

[그림 29] 요청 사항 확인 후 리스트 확인

IV. 기대효과 및 향후 연구

4.1. 기대효과

본 연구는 개인정보의 분산·공유가 필요한 모든 분야에서 법기반의 신뢰적인 솔루션을 제공함으로써, 개인정보를 안전하게 관리하고 통제할 수 있는 환경을 제공할 것이라 사료된다.

특히 개인정보보호 정책 엔진은 국내법과 OECD의 개인정보보호 가이드라인에 의해 체계적으로 개인정보보호 정책을 정의함에 따라 사용자로 하여금 자신의 프라이버시를 보호할 수 있도록 하고, 기업 입장에서는 법률 보호 하에 정보 수집 및 활용이 가능하다. 개인정보 침해 발생 및 해당 절차 위반 시 관련 법규에 의해 즉시 대응할 수 있도록 하여 법의 사각지대를 악용한 범죄 행위를 막을 수 있다.

또한, 역할기반의 접근제어를 이용한 설계는 기업 및 조직 내 적용 가능성이 유연하며, 사용자를 역할별로 할당하여 관리가 수월하고, 역할에 따라 제한적인 권한을 부여함으로써 개인정보를 효과적으로 보호할 수 있다. 이는 제 3자에게 정보 접근을 통제함으로써 개인정보 유출 및 정보의 손실을 예방한다.

이렇듯 개인정보와 법률들을 하나의 일원화된 시스템으로 관리하면서 개인정보를 안전하게 보호하고, 역할 및 목적에 따른 개인정보의 제한적 접근 권한을 부여함에 따라 불법적인 개인정보 수집 및 유출 사고를 예방할 수 있다.

4.2. 향후 연구

현재 국회에 계류 중인 개인정보보호법안이 곧 통과된다는 전망에 따라 이와 관련되어 발의되는 법안을 새롭게 정책엔진에 적용하여 최신 법률의 보호 하에 개인정보보호가 이루어 질 수 있도록 해야 한다. 이와 함께 새로운 법률이 추가·개정됨에 따라 관리자와 사용자 모두 이를 편리하게 적용하고 열람할 수 있도록 엔진의 정량화 작업이 s필요하다.

또한, 국내외 법률과 정책 뿐 아니라 특정 기관이나 사내에서 사용 되는 내부의 규정과 역할을 적용하여 사용되는 기관 내부의 특성에 따라 보다 안전한 보호 환경을 구축할 수 있도록 한다. 뿐만 아니라 기관별 사업 영역의 특성에 따라 사용하는 개인정보가 다르므로(예, 의료정보, 결제정보) 요청자의 접근 등급과 개인정보의 등급 및 사용 범위를 유동적으로 적용할 수 있도록 하여 사용성을 높일 수 있도록 한다.

끝으로, 현재 시스템에 의해 일괄적으로 구분된 개인정보의 등급을 개인정보 소유자의 의견 반영 및 선택이 가능하도록 연구하여 보다 주체적으로 개인정보를 보호할 수 있는 환경을 구현 할 계획이다.

V. 결론

정보사회가 발달됨에 따라 사회 각 분야에서 인터넷과 정보통신기술의 사용이 일상화됨에 따라 개인정보는 과거의 단순한 신분정도에서 오늘날에는 전자상거래, 고객관리, 마케팅 등 기업 활동 및 사회구성의 필수적인 요소로서 기능하면서 그 활용도가 높아짐에 있다. 또한 정보가 기업의 경쟁력을 좌우함에 따라 개인정보의 오·남용에 대한 피해는 급증하고 있다.

하지만 현재 국내의 개인정보보호를 위한 체계 및 시스템은 정보화 시대의 발달에 발맞춰 따라가지 못하고 있는 실정이다. 각 처에서 관련 법규를 발표하고 있지만, 분산되어 존재하여 중첩 및 보호 받지 못하는 곳이 존재하고 이를 적용하는 기술 및 시스템이 부족하다. 그리하여 이를 악용한 범죄행위가 발생하여도 법적 처벌 및 보상을 제대로 받지 못하게 되는 경우가 생기게 된다. 개인정보의 유출 사고 시 개인은 정신적, 금전적 피해 뿐 아니라 사회 활동에 까지 악영향을 미칠 수 있으므로 개인정보의 관리는 보다 안전하게 지켜져야 한다.

이에 국내 관련 법규와 정책 기반의 개인정보보호 엔진 PCE(Privacy Compliance Engine)을 제안하였다. 이를 통해 법 보호 하에 개인정보가 지켜질 수 있는 방안을 제시하고, 개인정보의 노출 민감도에 따라 접근 권한을 구분하여 개인정보의 제한적인 사용을 통해 원치 않는 개인정보 사용을 예방할 수 있다. 향후 개인정보 보호가 필요한 기업 및 공공기관의 내부 규정에 맞추어 시스템을 적용 및 정량화 작업하여 보다 체계적인 개인정보보호 시스템을 구축할 것이다. 이로써 발전되어 가는 정보화 시대, 유비쿼터스 사회에 우려되는 정보화의 역기능을 최소화 하는데 그 대처방안이 될 수 있을 것이라 사료된다.

VI. 참고 문헌

[1] Ravi Sandhu, “Rationale for the RBAC96 family of access control models”, The first ACM Workshop on Role-based access control, Article No.9, 1996.

[2] OECD, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", 2001.

[3] Internet Education Foundation, “The P3P Implementation Guide”, http://p3ptoolbox.org/guide/, 2005.

[4] The W3C “The Platform for Privacy Preferences 1.1 (P3P1.1) Specification”, Available at http://www.w3.org/P3P/implementations, 2006.

[5] The W3C “A P3P Preference Exchange Language 1.0 (APPEL1.0)”, Available at http://www.w3.org/TR/2002/WD-P3P-preferences-20020415, 2002.

[6] 한국인터넷진흥원, “개인정보보호 기술 및 표준화 동향”, 2006.

[7] 한국인터넷진흥원, “개인정보보호 기술, 제품 및 활용사례 분석”, 2006.

[8] 한국인터넷진흥원, “접근통제기반 개인정보관리 모델 연구”, 2007.

[9] 한국인터넷진흥원, “개인정보의 기술적·관리적 보호조치 기준 해설서”, 2009.

[10] 한국정보통신기술협회, “개인정보보호정책 설정 및 협상 규격”, 2007.

[11] 김영삼 외 2인, “u-IT 환경에서의 개인화서비스를 위한 개인정보 보호 방안 연구”, 전자통신동향분석 제 25권 제2호, 2010.

[12] 노종혁, 진승헌, “웹 환경에서 정책 기반 개인정보보호 기술”, 전자통신동향분석 제22권 제4호, 2007.

[13] 이윤희, 정창성, “PKI 기반 보안운영체제의 권한인증설계” 한국컴퓨터종합학술대회, 2007.

[14] 홍승필, “개인정보보호 개론 : 사례연구 및 기술 중심으로”, 한티미디어, 2009.

[15] 지식경제부, “유비쿼터스 환경에서의 정보보호 정책 방향”, 2008.
[16] 이동훈, “개인정보보호의 중요성과 보호기술”, 한국소프트웨어산업협회, 2007.
[17] 이재광, 장종수, 박기식, “사이버공간에서의 개인정보보호”, 정보와사회 12호, 2007.
[18] 한국정보보호진흥원, “접근통제기반 개인정보관리 모델 연구”, 2007.
[19] 한국정보통신기술협회, "전자서명 인증서 프로파일", 정보통신단체표준, 2006.
[20] 한국정보통신기술협회, "디렉토리: 공개키와 속성인증서에 대한 프레임워크", 정보통신단체표준 TTAS.IT-X509/R4, 2007.
[21] 중소기업청, “중소기업 산업기밀관리 실태조사 보고서”, 2008.
[22] 개인정보분쟁조정위원회, “2009 개인정보분쟁조정사례집”, 2009.
[23] 한국인터넷진흥원, “인터넷 개인정보 노출방지 및 프라이버시 보호 방안 연구”, 2007.
[24] 한국정보사회진흥원, “전자정부서비스 사용자인증 및 권한관리 레벨화 방안 연구”, 2007.
[25] 한국인터넷진흥원, “2009 국내 지식정보보안산업 시장 및 동향 조사”, 2009.
[26] 국가정보원/방송통신위원회, “2009 국가정보보호백서”, 2009.
[27] 한국인터넷진흥원, “APEC ECSG 개인정보보호 논의 동향”, 2006.
[28] PISA Project, “Handbook of Privacy and Privacy-Enhancing Technologies”, http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf, 2003.
[29] IITA 기술정책정보단, “개인 정보보호 기술 동향”, 2005.
[30] Konstantina Stoupa and Athena Vakali, “Policies for Web security Services”, Idea Group Publishing, 2006.
[31] 방송통신위원회, “개인정보의 기술적·관리적 보호조치 기준 해설서”, 2009.
[32] 한국인터넷진흥원, “개인정보의 안전한 수집, 저장, 및 관리, 이용, 제공, 파기를 위한 개인정보 관리모델 연구”, 위너다임, 2006.

Abstract

Design and implementation for privacy information protection and control model based on law and policy

Jeoung, Ji-hee
Dept. of Computer
Graduate School
Sungshin Women's University

Although lots of benefit and convenience are provided because of the development of information and communication technology, the concern over an information society is growing as the damages keep rising for its adverse effect.

Especially, as the abuse of personal information and its illegal leak are targeted of any misdemeanor or felony, it brings a serious situation connected to the distrust to information society as well as one's mental and financial damage.

The National Assembly and the administration are stated bills related to the personal information. However, as the information is scattered over places, some parts are conflicted with the bills and are not properly protected. Moreover, there are few alternatives of standardization to protect the personal information as a technological side.

Due to the reasons above, we suggest the engine to protect the personal information on the base of the privacy protection related laws.

This thesis concentrates on the privacy protection engine and the function of access control to the personal information. We have also studied institutional, legal and technical ways to protect and make definition of the existing personal information.

Based on this research, we analyzed any related laws and foreign policies, as well as classified the companies and institutions handled the personal information by subjects. Also, we made plans to manage the information under the protection of law.

In addition, the engine can sort grades at the importance of the personal information, and give a differentiated right to users who access to it by their rules and purpose as a way of control.

Through this system, any abuse of personal information can be controlled as the management and circulation of personal information are handled in more safety environment on the basis of the law.