홍 승 필 교수지도
박사학위 청구논문

신뢰할 수 있는 개인정보보호 접근제어 모델 연구

2013

성신여자대학교 대학원
컴퓨터학과
김 경 진

신뢰할 수 있는 개인정보보호 접근제어 모델 연구

홍 승 필 교수지도

이 논문을 박사학위논문으로 제출함

2012년 10월

성신여자대학교 대학원
컴퓨터학과
김 경 진

인 준 서

김경진의 박사학위 논문으로 인준함.

심사위원 _____인

심사위원 _____인

심사위원 _____인

심사위원 _____인

심사위원 _____인

성신여자대학교 대학원

논 문 개 요

정보화 사회의 발전으로 개인정보 수집 및 이용의 필요성이 높아짐에 따라 과도한 개인정보 수집 및 오남용으로 프라이버시 침해의 위험성 또한 크게 증가하였다. 이러한 지속적인 증가로 사람들의 우려 및 심각성 또한 고조되고 있다. 특히 공공기관의 경우에는 행정목적을 달성하기 위해 민감한 개인정보를 다량으로 보유하고 있는 경우가 많으므로 개인정보 유출 및 피해발생 시에는 사회적 파급효과가 크다. 이에 2011년부터 시행된 개인정보보호법으로 본격적인 관리감독 및 지원활동이 시작되면서 법적으로 개인정보보호의 의무사항이 강화되었으나, 인터넷이라는 노출된 환경에서 현실상 기술적으로 실체화되기 어려워 제도적인 방안을 시스템적으로 적용하는 것이 이슈되고 있다.

본 논문에서는 서두에서 개인정보보호 관련하여 국내외 표준 및 법제도, 기술에 대한 선행연구 기반으로 본 연구의 필요성 및 배경을 소개한다. 현 프라이버시의 위험 및 취약성을 분석하며 도출된 문제점의 대응방안으로 개인정보를 효과적으로 통제 및 제어하고 유용하게 관리하기 위한 개인정보보호 접근제어 모델을 제안한다. 효과적인 접근통제를 위해 국내 개인정보보호법을 적용한 기준 및 규정을 정의할 수 있는 정책관리로써 법을 시스템 내에 실행 가능한 정책으로 전환할 수 있도록 하는 자동화 시스템에 기반을 두어 새로운 컴플라이언스의 요구를 쉽게 수용할 수 있다. 또한 프라이버시 정책기반으로 역할기반 접근제어(RBAC)를 확장하여 보안정책을 적용하는데 있어 유연성을 제공할 수 있도록 모델을 정의한다. 아울러 정의한 모델의 구현방안을 소개함으로써 제안한 연구의 실행 가능성을 타진한다.

목 차

그림 목차

표 목차

Ⅰ. 서론

1. 연구의 필요성 및 목적

정보통신 기술의 발전으로 다양한 유관산업과 IT분야가 접목하게 되면서 공공기관이나 기업에게 무한한 경제적 가치를 지니는 개인정보의 수집 및 이용이 급격히 높아지고 있다. 이와 함께 기관이 보유하고 있는 개인정보 노출사고 역시 급증하면서, 기업 및 기관의 이미지 실추 및 경제적, 사회적으로도 막대한 손실을 발생시키고 있다. 특히, 공공기관의 경우에는 행정목적을 달성하기 위해 민감한 개인정보를 다량으로 보유하고 있는 경우가 많으므로 개인정보 유출 및 피해발생 시에는 사회적 파급효과가 훨씬 크다. 한국인터넷진흥원의 보고에 따르면[1], 개인정보 침해건수가 2011년 총 122,215건으로 전년대비 약 123% 이상 가파르게 증가한 수치를 보이면서 사회적으로 개인정보 관리에 대한 심각성이 고조되고 있다.

이러한 개인정보 유출사건의 빈번한 발생으로 심각한 문제가 되고 개인정보보호법의 필요성이 증가함에 따라 2011년 3월 29일 개인정보보호법이 공포되었으며, 그 해 9월 30일부터 전면 시행되었다[9,10]. 개정된 법은 법 적용되는 규율대상이 공공뿐만 아니라 민간 사업자에게도 확대되면서 본격적인 관리감독 및 지원활동이 시작으로 개인정보보호 의무사항을 강화하게 되었다. 개인정보보호법의 주요 개정 사항으로는 정보주체인 개인의 권리를 보장하고, 개인정보의 수집, 이용, 제공 등 처리단계에서 보호기준 및 규정을 마련하며, 고유식별정보의 처리제한 강화를 통해 최소한의 정보만을 수집해야 함을 규정하고 있다.

이러한 법적사항이 있음에도 불구하고, 개인정보를 처리하는 공공기관 및 민간 기업·단체의 부실한 관리 실태, 실수 또는 악의적 목적에서 이용자의 어떠한 동의 없이 개인정보를 무단 수집, 개인정보 내돌리기, 불법거래, 유

출 등으로 개인정보 침해문제가 여전히 심각하다. 특히 개인정보보호법의 발효에 따라 이전보다 침해 및 유출에 대해 많은 사람들이 법적 소송을 진행할 것으로 보인다.

이와 같은 개인정보 보안의 우려에도 법, 지침으로는 실제 개인정보가 안전하게 처리되는지 보장하기 어렵다. 즉, 노출된 웹 환경에서 법제도적 규정을 준수하는 기술을 실체화하기에는 컴플라이언스 기술이 미흡하다. 개인정보 취급지침이나 정책만으로는 개인정보에 대한 보호 사항이 언급되어있더라도 기술적으로 표현할 수 있는 안전조치 사항이 구체적이지 않으며, 실제 보안조치에 대해 확인하기 어렵다. 특히 개인정보보호법의 시행으로 이후 기업이나 기관의 유출사고에 대해 강력한 대응이 예상되어지며, 이에 따라 개인정보를 수집하는 기관에서는 법 또는 규정을 준수할 수 있는 보안 기술이 요구하고 있다.

이러한 이슈의 대안으로 본 연구에서는 웹 환경 내 개인정보의 위험 및 취약성을 분석하고, 이를 기반으로 국내 개인정보보호 관련 법규 및 정책을 준수할 수 있는 접근제어 모델을 소개한다. 이는 개인정보의 수집 및 이용, 제공 등 정책에 준한 체계적인 개인정보 처리를 가능하게 하여 개인정보를 안전하게 보호 및 관리해줄 수 있는 시스템 구축 방안 확립을 목표로 한다.

2. 연구의 범위

본 논문은 현재 개인정보 보호의 이슈 및 문제점을 파악하여 국내 개인정보보호 관련 법규를 준수할 수 있는 접근제어 모델을 제안한다.

본 연구에서 제안한 접근제어 모델의 체계적인 설계를 위해 노출된 웹 환경 내 개인정보의 활용도나 발생할 수 있는 개인정보 침해요인 및 위협요소를 파악하며, 이를 기반으로 다각적 측면에서 개인정보의 위협 및 취약점이 되는 위험을 분석한다. 또한, 국내외 표준화, 기술 등의 관련 연구 및 개인정보보호를 위해 수행된 프로젝트를 조사하고, 프라이버시 정책기반의 접근제어 관련한 선행 연구를 조사하여 비교·분석하고자 한다.

이를 기반으로 본 논문에서 접근제어 모델의 주요 기능인 정책을 위해 국내에서 작년에 시행된 개인정보보호 법안, 지침 등을 바탕으로 개인정보 보호를 위해 요구하고 있는 사항을 파악하여 시스템에 적용할 수 있도록 요구사항을 분류한다. 제시하는 접근제어 모델은 개인정보보호법 또는 향후 개정·보완이 있을 규정의 요구사항을 충족시키며 이를 준수할 수 있는 기술적 대응책을 마련하는데 목적이 있으므로, 본 논문에서는 시스템적으로 정의한 개인정보보호 정책을 통해 신뢰할 수 있는 개인정보보호 접근제어 모델을 제시한다.

아울러, 정의된 모델을 구현함으로써 연구기술의 실행 가능성을 보여주고, 보안성 분석 및 성능평가에 대한 비교·분석하여 제안하는 모델의 향후 활용 방안으로써의 가능성을 타진한다.

3. 논문 구성

1장은 연구의 개략적인 설명으로써 논문의 주요 목적을 간략히 소개하고 연구의 범위 및 방법을 살펴본다.

2장에서는 개인정보의 침해 현황 및 개인정보보호 관련하여 국내외 표준 및 법제도, 기술에 대한 관련연구 기반으로 본 연구의 필요성 및 배경을 소개한다.

3장에서는 개인정보 보호를 위한 정책기반의 접근제어와 관련된 선행 연구를 통해 학술적인 의미를 모색한다.

4장에서는 현재 개인정보보호의 한계와 위험을 다각적 측면으로 분석하며 문제점을 통해 요구사항을 충족할 수 있는 대안방안을 논의한다.

5장은 제안하는 개인정보보호 접근제어 모델을 소개하며, 이를 구성하고 있는 5가지 메커니즘에 대해 상세한 기능을 설명한다.

6장에서는 제안한 모델 기반으로 설계한 알고리즘과 데이터베이스, 구현한 프로토타이핑을 보여주며 실제 환경에서의 적용 가능성을 나타낸다.

7장에서 보안성에 대한 비교분석 및 시뮬레이션을 통해 처리성능에 대한 효과를 보여준다.

마지막으로 8장에서는 연구의 내용 및 결과를 요약하고, 본 연구의 의의 및 기대효과에 대해 제시한다.

Ⅱ. 개인정보보호의 이론적 배경

1. 개인정보보호 현황

1) 개인정보 정의 및 특성

개인정보의 개념은 정의에 따라 약간씩 차이가 있지만 일반적으로 OECD나 EU 지침에서처럼 개인과 정보와의 관련성과 식별가능성을 기본으로 하고 있으며, 최근에는 다른 정보와 용이하게 결합하면 개인을 식별할 수 있는 정보까지도 포괄하고 있다[7,31]. 국내 개인정보보호법에서는 '개인정보'를 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보로써, 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것도 포함하도록 규정하고 있다[9,10]. 즉, 본인의 의사에 반하거나 본인이 알지 못하는 상태에서 이용될 경우 정보주체(혹은 당사자)의 안녕과 이해관계에 영향을 미칠 수 있는 개인 관련 정보는 모두 개인정보라고 할 수 있다. OECD와 EU를 포함한 해외 주요국들은 개인정보를 아래와 같이 정의한다[6,48].

<표 1> 해외 주요국 개인정보 정의

법률	조항	내용
OECD 가이드라인	제1조	- 식별된 또는 식별 가능한 개인에 관한 정보
EU지침	제2조	- 정보주체의 신원이 확인되었거나 확인 가능한 정보
캐나다, 프라이버시법	제3조	- 신원을 확인할 수 있는 개인에 대한 정보
일본, 개인정보보호에 관한 법률	제2조	- 생존하는 개인에 대한 정보로서 특정한 개인을 식별할 수 있는 정보
호주, 프라이버시법	제6조	- 당해정보 또는 의견으로부터 신원이 명백하거나 확실시될 수 있는 개인에 관한 정보 또는 의견

영국, 개인정보보호법	제1조	- 신원을 확인할 수 있는 생존하고 있는 개인과 관련된 데이터 또는 정보 관리자가 보유하고 있거나 앞으로 그러할 가능성이 높은 기타 정보 - 데이터로부터 신원이 확인 가능한 생존개인과 관련된 데이터
프랑스, 정보처리축적 및 자유에 관한 법률	제4조	- 형식에 관계없이 개인을 식별할 수 있게 하는 정보로서 자연인 또는 법인이 처리하는 정보
독일, 연방 개인정보보호법	제3조	- 신원이 확인되었거나 확인 가능한 정보주체의 인적·물적 환경에 관한 일체의 정보
홍콩, 개인정보법	제2조	- 생존하는 개인과 직·간접적으로 관련된 모든 데이터로서, 개인의 신원을 직·간접적으로 확인하기 위해 사용할 수 있는 데이터 및 데이터 접근 또는 처리가 가능한 형식의 데이터

※ 출처 : 미국의 개인정보보호 법·제도 동향, 정보보호학회지, 2012

요약하자면, 개인정보 개념은 식별 가능한 개인에 관한 정보라고 정의하고 있다. 즉, 개인의 신체, 재산, 사회적 직위, 신분 등에 관한 사실, 판단, 평가 등을 나타내는 모든 정보를 말한다[7,50]. 주민등록번호, 주소, 휴대폰 번호 등 개인에 대한 일반적 정보뿐만 아니라 학력, 병력, 소득, 취미, 종교 등 여러 개의 개인정보를 조합하여 한 개인을 식별할 수 있는 개인정보를 말한다. 여기서 중요한 사실은 이러한 정의가 담아내는 개인정보의 범위가 고정되어 있는 것이 아니라 사회 환경의 변화와 기술발전으로 계속 확대된다는 점이다. 최근 정보통신의 발달로 전자우편주소, 신용카드 비밀번호, 로그파일, 쿠키(cookies) 정보, 위치정보, DNA 정보 등 새로운 개인정보가 계속 등장하고 있으며, <표 2>에서와 같이 다양한 개인정보 유형구분에 따라 구체적인 항목의 예를 나타낸다[3,6].

<표 2> 개인정보 유형별 종류(예)

유형구분	개인정보 항목
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, 동아리활동, 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
기타 수익정보	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, 자동차 교통 위반기록, 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 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

※ 출처 : 한국인터넷진흥원, 2012

개인정보의 정의가 확대되면서 프라이버시의 개념 및 의미, 영역 역시 정보사회가 발전함에 따라 점차 복잡해지고 다양해지고 있으며, 서로 다른 관점으로 다양한 형태가 제기되었다. 즉, 인터넷 상의 개인정보를 가지고 있는 프라이버시의 개념이 나타남에 따라 기존 개인정보의 개념의 범위가 확대되고 있다. 정보통신발달과 더불어 인터넷을 통해 개인정보의 오남용, 잘못된 관리, 프라이버시의 침해 등으로 이어져서 개인에 대한 정보를 제3자가 어떻게 관리하는가에 대해 정보주체가 관여할 권리를 중요하게 여기게 되었다[5,15].

최초의 프라이버시에 대한 정의는 1890년 미국의 Warren과 Brandeis에 의해 "홀로 있을 수 있는 권리(the right to be let alone)"로 이후 다양한 정의가 나오게 되었는데 개념들이 일치된 의견은 없으나, 현재 프라이버시의 본질에 대한 견해로써 Rober Ellis Smith의 견해[1]와 같이 개인정보를 프라이버시의 한 유형으로 파악하는 것을 지지하고 있다[7,60]. 최근 정보기술의 발전으로 자신에 관한 개인정보의 접근과 이용을 통제할 수 있는 개인의 능력이라는 Frederick Schauer의 정의로써 프라이버시를 개인정보와 동일시하는 경향으로도 나타내고 있다. L.Brandeis는 프라이버시가 개인의 혼자 있을 권리로써 민주주의의 가장 중요한 자유로 헌법에 반영되어야 하는 권리라고 하였으며[7,60], 이 의미와 부합되게 우리나라의 법적 프라이버시 정의는 헌법에서 제17조에 '모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다'라고 규정하고 있으며, 제14조 거주이전의 자유, 제15조 직업선택의 자유, 제16조 주거의 자유, 제18조 통신의 자유 등의 권리 명시 또한 프라이버시 보장을 의미한다. 이에 따라 헌법재판소는 사생활 비밀의 불가침, 사생활 자유의 불가침, 자기정보의 관리 통제를 사생활의 자유에 대한 내용으로

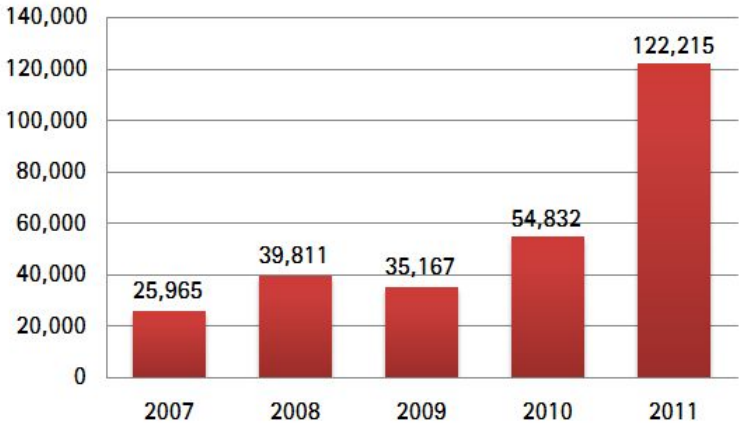
1) Robert Ellis Smith, Privacy and Curiosity from Plymouth Rock to the Internet, 2000/2004: "Just what is privacy? It is the desire of each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves."

모든 국민은 프라이버시를 침해당하지 않을 권리 및 자신의 정보를 통제할 수 있는 권리도 보장받을 수 있음을 제시하고 있다[15,16]. 프라이버시 역시 정보통신서비스의 발달과 이용확산에 따라, 정보통신서비스 이용과정에서 발생하는 정보들(전자우편주소, 로그파일, 쿠키정보, GPS 위치정보 등)도 개인정보의 범위에 포함시킬지에 대해서는 특정 개인의 식별정보와 연결되어 개인의 프라이버시에 영향을 미친다면 이러한 정보들도 보호 대상에 포함되어야 함이다.

이와 같이 개인정보에 대한 명확한 구분은 어려우나, 관련 정책의 수행이나 업무처리에 대한 목적으로 개인정보의 정의 범위 등을 분명하게 특정할 필요가 있다.

2) 개인정보 위협 현황

급변하는 경제 환경 및 신기술의 등장과 함께 정보화 사회의 발전으로 개인정보의 가공 및 활용이 용이해졌다. 그에 따라 기관이나 기업·민간 사업자로부터 정보주체의 어떠한 동의 없이 무한으로 수집 및 축적되고 처리할 수 있는 개인정보관리 시스템 구축이 가능해지면서, 개인정보의 도용 및 유출에 따른 피해가 끊임없이 발생하고 있다. <그림 1>은 2007년부터 2011년 동안 개인정보 침해신고 현황에 대한 조사 결과로써, 개인정보 침해동향 및 분쟁조정사례 등을 분석한 결과 2011년도 개인정보 침해 상담 및 신고 건수가 총 122,215 건으로 전년대비 약 123% 이상이 증가하였다[1]. 이는 개인정보 침해 발생이 지속적으로 증가 추세임을 보여주고 있으며, 특히 침해신고가 급증하게 된 것은 개인정보보호법이 시행됨에 따라 정보주체의 침해신고에 대한 인식과 자신의 권리보호를 위한 의식이 높아진 것이 주요 요인으로 분석된다.



<그림 1> 개인정보 침해 신고·상담 현황

※ 출처 : 인터넷침해대응지원센터, 2012

다음 표는 개인정보 피해구제·상담 현황을 제시해주는 통계표로써, 가장 크게 증가한 사례가 「주민번호 등 타인정보도용」이 67,094건으로 전년도 비교하여 약 560% 이상 증가하였다. 개인정보 신상이 유출되었다는 것은 1차적인 문제이고, 유출된 주민번호로 불법 매매, 금융계좌나 사이버머니 판매 등 명의도용을 통해 신분증 위조로써 각종 범죄와 사기에 악용될 가능성이 크므로, 이에 대한 조치가 시급히 필요하다고 여겨진다.

<표 3> 개인정보 침해 신고·상담 유형별 현황

(단위 : 건)

접수유형	2007	2008	2009	2010	2011
합계	**25,965**	**39,811**	**35,167**	**54,832**	**122,215**
개인정보 무단수집	1,166	1,129	1,075	1,267	1,623
개인정보 수집 시 고지 또는 명시 의무 관련	7	6	15	75	53
과도한 개인정보 수집	51	87	115	146	379
목적 외 이용 또는 제3자 제공 관련	1,001	1,037	1,171	1,202	1,499
개인정보 취급자에 의한 훼손·침해 등	123	125	158	158	278
개인정보 처리 위탁 시 고지의무	2	6	6	25	36

영업의 양수 등의 통지의무	14	9	6	22	64
개인정보관리책임자 관련	10	26	10	21	38
기술적·관리적 조치 미비 관련	522	1,321	819	1,551	10,958
수집·제공받은 목적 달성 후 개인정보 미파기	146	294	294	323	488
동의철회, 열람·정정 요구 관련	865	949	680	826	662
동의철회, 열람·정정을 수집보다 쉽게 해야 할 조치	461	503	603	630	800
아동의 개인정보 수집	14	27	19	35	71
주민번호등 타인정보도용	9,086	10,148	6,303	10,137	67,094
법적용 불가 침해사례	12,497	24,144	23,893	38,414	38,172

※ 출처 : 한국인터넷진흥원 개인정보침해신고센터, 2012

뿐만 아니라, 스마트 기기 및 신규 서비스 등의 확산 역시 급격히 증가한 개인정보 침해신고에 일조하여 신규 기술을 통해 개인정보 침해사고가 발생한 것으로 보이며, 인터넷 이용자, 즉 정보주체의 개인정보에 대한 관심 증가로 인해 향후에도 계속 증가할 것으로 예상된다.

기업관점에서는 개인정보, 즉 고객정보는 개인을 식별하여 마케팅에 활용할 수 있는 정보로 주민등록번호, 계좌번호, 카드번호, 거래내역, 신용정보, 선호도정보 등의 민감한 정보를 포함하고 있어 기업의 개인정보관련 보안에 대한 관심이 집중되고 있으며, 개인정보보호법 적용에 따라 이전보다 법적용사업자가 늘어남에 따라 개인정보보호의 의무가 강화되었다. 하지만, 개인정보보호법 제정에도 불구하고 개인정보 유출 사고는 여전하였다. 조사된 개인정보 침해발생 건수를 보면[6,54], 국민 1인당 2번이상의 개인정보 유출피해를 입은 것으로 피해가 재발된 것으로 추측할 수 있다. 또한, 개인정보 유출의 대부분이 해킹 위험에 노출되어 있는 회원정보였고 실수로 유출된 건수를 제외한 모두 관리 소홀 및 해킹으로 개인정보가 유출되었다.

이는 개인정보보호 수준을 제고하며, 악의적 행위에 대해 강력히 처벌하고, 대상에 따라 맞춤형 정책 개발, 취약분야에 대해 기술지원을 지속하는 등 안전성 확보를 위한 조치가 지속적으로 필요함을 알 수 있다.

<표 4> 2008년 이후 개인정보 유출 현황

일시	사례	유출규모	사고원인
2008년 2월	온라인경매업체	1863만	해킹
2008년 9월	정유업체	1151만	고의
2010년 3월	쇼핑몰	2000만	해킹
2011년 4월	캐피탈업체	175만명	해킹
2011년 6월	대부업체, 저축은행 등	1900만명	해킹
2011년 7월	포털업체	3500만명	해킹
2011년 8월	프린터업체	35만명	해킹
2011년 11월	게임업체	1,320만명	해킹

※ 참조 : 한국인터넷진흥원, 2011

기업뿐만 아니라, 정보화 사회의 급속한 발전으로 대국민 서비스를 제공하는 행정 분야 역시 신규 정보통신기술을 활용한 첨단서비스를 제공하기 위해 개인정보의 의존도와 활용도가 점차 높아지고 이와 함께 과도한 개인정보 수집 및 오·남용으로 인해 국민들의 프라이버시 침해의 위험성 또한 크게 높아지고 있다. 행안부에 따르면[6], 10개의 정부산하 공공기관을 대상으로 개인 정보 파기 실태에 대한 특별 점검을 하는 과정에서 적발되었다. 점검했던 공공기관 6개가 보유하고 있는 개인 정보 가운데 7억998만 건이 보유 기간을 초과한 것으로 확인되었다. 공공기관은 행정목적을 달성하기 위해 민감한 개인정보를 다량 수집 및 보유하고 있는 경우가 많음에 비해, 수집되는 다량의 개인정보는 개인정보 관리 기간을 초과해 관리하는 등 부실함을 보이고 있으며, 정부의 개인정보 관리가 취약해 수집된 개인정보를

실수 및 고의로 인해 타인에게 유출하는 개인정보 침해 행위가 빈번히 발생하고 있는 실정이다.

3) 국내외 법제도 및 표준

개인정보보호와 관련하여 세계 각국에서는 다양한 법·제도를 제정, 시행하고 있으며 특히 정보통신망을 이용한 대량의 개인정보의 수집, 취급 등이 용이해지면서 전자적 형태의 개인정보보호와 관련한 법률이 다수 존재하고 있다.

<그림 2> 국내외 개인정보보호 관련 법체계

○ 국외 개인정보보호 관련 법규 및 가이드라인

대표적으로 미국은 개인정보보호에 관한 사항을 규정하고 있는 기본법은 없지만 각 부문별 개인정보보호를 위한 법규범을 마련하고 있다[6,8,12]. 즉, 공공부문에만 법률을 적용하며 민간부문은 개별법[2]에 따라 규제할 수 있도

2) 민간부문의 개별법으로는 어린이온라인프라이버시보호법(COPPA), 공정신용보고법(FCRA), 금융제도개혁법(GLBA) 등 제정

록 하며 민간의 개별법이 없는 분야는 자율적 지침을 준수하도록 하며 개인정보 유출 시에는 사법적 처리를 할 수 있는 자율규제 방식을 준수한다. 개인정보보호체계는 공공부문과 민간부문으로 구분되며 공공부문은 1974년 제정된 프라이버시법(Privacy Act)이 일반법 역할을 하고 민간부문에서는 각 영역별로 필요성에 의하여 개별법을 제정하였으며, 개인정보보호를 위한 독립적인 감독기구는 없으나, 연방거래위원회가 개인정보보호 관련 법률 집행 및 준수여부를 감독하는 권한 행사하고 있다. 프라이버시법의 주요내용은 최소한의 개인정보를 수집·보유하도록 제한하고 본인의 서명요청 및 사전동의 없이는 개인정보를 개시할 수 없도록 규정하나, 통계나 법집행, 의회조사 등 행정목적인 경우에는 예외로 개인정보의 수집 및 활용이 가능하다.

유럽연합은 각 유럽국가의 개인정보보호 기본법으로써 공공부문과 민간부문을 통할하는 기본법을 마련하고 개인정보보호를 위한 독립된 감독기구를 설치 및 운영하도록 규정하고 있는 정뷰규제 방식을 준수한다[6,12]. 개인정보보호를 위한 감독기구는 개인정보보호정책을 담당하고 조사권 등을 가지며 개인정보의 수집 및 이용을 감시하면서 위반행위에 대한 제재를 행사하고 있으며, 개인정보보호 관련 규범은 개인정보보호지침(Directive on Privacy Protection 95/46/EC)과 프라이버시 및 전자통신에 관한 지침(Directive on Privacy and Electronic Communication 2002/58/EC)을 기반으로 준용하고 있다. 개인정보보호지침은 유럽연합 회원국에게 개인정보보호에 대한 책임을 부과하고 권리 보장을 목적으로, 명확한 개인정보 목적명시와 이를 준수하는 정보수집, 개인정보의 정확성 유지 및 갱신 등 정책을 규정하고 있으며, 프라이버시 및 전자통신에 관한 지침은 전기통신분야에서의 프라이버시 보호를 목적으로 하여 개인정보의 처리과정 보호와 통신에서 개인위치정보 보호, 스팸메일 발송 제한 등을 규제하고 있다.

일본은 정부 행정기관에 적용되는 일반법으로 행정기관이 보유한 개인정

보에 관한 법률과 공공 및 민간 공통으로 적용되는 개인정보보호에 관한 법률을 제정하여 개인정보 취급에 대한 최소한의 규칙을 명시하며, 사업 분야에 따라 자율적으로 대처할 수 있는 사업자 자율성을 인정하는 개인정보보호법을 준수한다[6,12]. 개인정보보호 감독기구를 별도로 설치하지 않고, 각 개인정보취급사업자가 개인정보보호 정책을 수행하고 소관사업의 주무장관이 직접 집행 및 감독하고 있다. 개인정보보호에 관한 법률의 목적은 개인정보의 유용성과 개인의 권리이익을 보호하고 있으며, 민간사업자의 개인정보 취급에 관해서는 최소한의 규칙을 정한 가이드라인에 준수하며 사업자의 자율성을 중시하며, 개인정보 취급의 예외인정 범위를 규정하여 헌법상 보장된 자유를 보호[3]하고 있다.

정리하자면, 미국은 개인정보보호에 관한 사항을 규정하고 있는 기본법은 없지만 각 부문별 개인정보보호를 위한 법규범을 마련하고 있다. 또한, 개인정보보호를 위한 독립적인 감독기구는 없으나, 연방거래위원회가 개인정보보호 관련 법률 집행 및 준수여부를 감독하는 권한을 행사하고 있다. 유럽연합은 미국과는 다르게 공공부문과 민간부문을 통할하는 기본법을 마련하고 개인정보보호를 위한 독립된 감독기구를 설치 및 운영하도록 규정하였다. 일본 역시 공공과 민간부분에 적용할 수 있는 개인정보보호에 관한 법률을 적용하나 독립된 별도의 감독기구는 존재하지 않고 주무장관이 직접 집행 및 감독한다. 이와 같이 개인정보보호 법제도와 관련한 대표적인 주요국가는 유럽연합, 미국, 일본으로 성격과 특징, 기능, 권한 면에서 서로 다른 형태를 보이고 있으며, 우리나라의 경우에는 공공 및 민간부문에 적용할 수 있는 개인정보보호법을 제정한 일본과 방식이 유사하며, 일부 사업자 및 회사에 대해서는 개별법을 우선적으로 적용할 수 있도록 한다[8,12,14].

이러한 주요 해외국가들의 개인정보보호 관련 법규를 마련하게 되는 기

3) 헌법상 보장된 표현·학문·종교 등의 자유를 인정하여 보도·학술기관과 종교단체 등의 활동은 개인정보취급 사업자의 의무에 적용되지 않음

틀의 대표적인 것이 OECD 개인정보보호 가이드라인이다[30]. 프라이버시에 대한 논의는 OECD에서 1978년대부터 시작하였으며, 논의의 결과 1980년 '프라이버시 보호와 개인 데이터의 국제유통에 관한 가이드라인에 관한 이사회 권고'라는 가이드라인을 채택하였고, 개인정보의 사생활권 보호, 정보의 자유로운 유통 장려, 국내사생활보호입법에 의한 자유로운 정보유통에 대한 부당한 제한방지, 관련국내법규정과의 조화를 주목적으로 하고 있는 가이드라인의 8대원칙을 제시하고 있다[7,30]. 8대 원칙에 대한 사항은 아래와 같다.

<표 5> OECD 8대 원칙

원칙	내용
수집 제한의 원칙	개인데이터의 수집에는 제한을 두어야 한다. 어떠한 개인 데이터도 합법적이고 공정한 절차에 의하고 가능한 경우에는 데이터 주체에게 알리거나 동의를 얻은 후에 수집하여야 한다.
정확성 확보의 원칙	개인데이터는 그 이용목적에 부합되는 것이어야 하며 이용 목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것이어야 한다.
목적 명시의 원칙	개인정보는 수집 시 그 수집목적이 명확히 제시되어야 하며, 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립되어야 한다. 목적이 변경될 때마다 명확화 될 수 있는 것으로 제한되어야 한다.
이용제한의 원칙	개인정보는 목적명확화의 원칙에 따라 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 자신의 정보소재를 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	데이터 관리자는 원칙을 실시하기 위한 조치에 따를 책임이 있다.

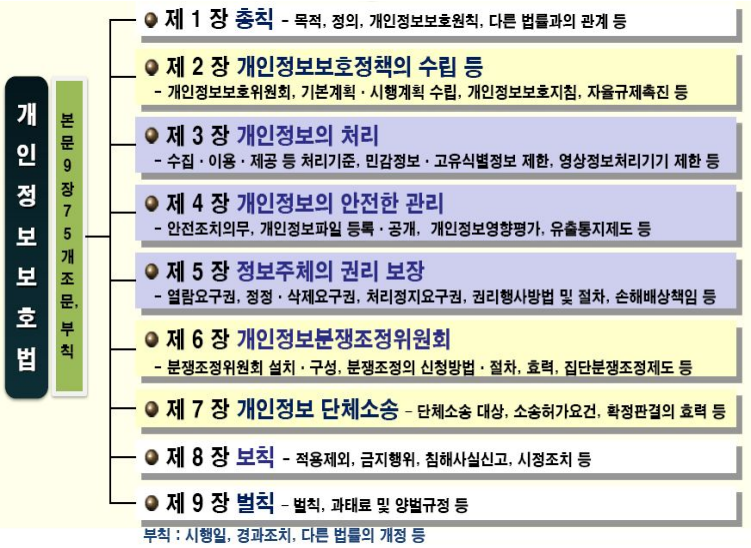
우리나라의 경우에도 개인정보보호법이 OECD가 제정한 8대 원칙에 기초하고 있으므로, 개인정보보호의 본질을 이해하기 위해서는 OECD에서 제시하는 원칙을 파악하여, 본 연구에서 제시하는 개인정보보호를 위한 요구사항으로써 적용한다.

ㅇ 국내 개인정보보호 관련 법제도 및 표준화

기존 개인정보보호 관련 법률에서는 개별법으로 분산되어 산재하면서 법 적용에 사각지대가 발생하고 개별법들 간의 상이한 원칙 및 처리기준으로 적용이 혼란스러웠다. 이에 개인정보보호와 관련된 법체계를 일원화하고 개인의 권익 보호를 강화하기 위해 2011년 3월 29일 개인정보보호법이 공포되었으며, 같은 해 9월 30일을 기준으로 시행되었다[8,9,15]. 이는 비영리 기관, 오프라인 사업자 등이 법적용 대상에서 배제되어 발생하는 개인정보보호 사각지대 발생 문제를 해소하고 개인정보 침해사고의 사전 예방과 사후 구제를 위해 공공과 민간에 모두 적용되는 법이다.

개인정보보호법 발효에 따른 주요 내용으로는 업무 목적으로 개인정보를 처리하는 공공기관 및 민간 기업·단체가 규율대상으로 확대되고, 전자문서를 포함한 수기 문서로 기록된 개인정보도 보호대상에 포함된다. 또한 개인정보의 수집 및 제3자 제공시에는 정보주체의 동의를 받아야 하고, 개인정보 이용 및 제공은 최소화하며, 처리 목적 달성 시에는 지체없이 파기할 수 있는 보호기준과 규정을 마련하였다. 주민번호 등 법령에 따라 개인을 고유하게 구별하기 위해 부여된 고유식별정보는 원칙적으로 처리를 금지하며, 인터넷에서 서비스를 이용하기 위해서는 주민번호를 대체할 수 있는 전자

서명, 아이핀 등 방법을 의무적으로 제공하여 고유식별정보의 처리제한을 강화한다. 또한, 정보주체의 개인정보를 열람·정정·삭제 및 처리정지를 보장하고 권리행사 방법을 규정하여 정보주체의 권리보장을 강화하며, 개인정보 유출 사실에 대해서도 정보주체에게 통지할 수 있도록 한다. 개인정보보호위원회 신설과 개인정보분쟁조정위원회에 따라 개인정보에 관한 분쟁조정 업무를 신속하고 공정하게 처리하기 위하여 기능을 강화한다[3,8,9]. 이러한 주요 사항을 바탕으로 <그림 3>과 같이 개인정보보호법의 구성 체계를 개정하였다.



<그림 3> 국내 개인정보보호법 구성 체계

※ 출처 : 국가정보보호백서, 2011

<표 6> 개인정보보호법 시행에 따른 주요 사항

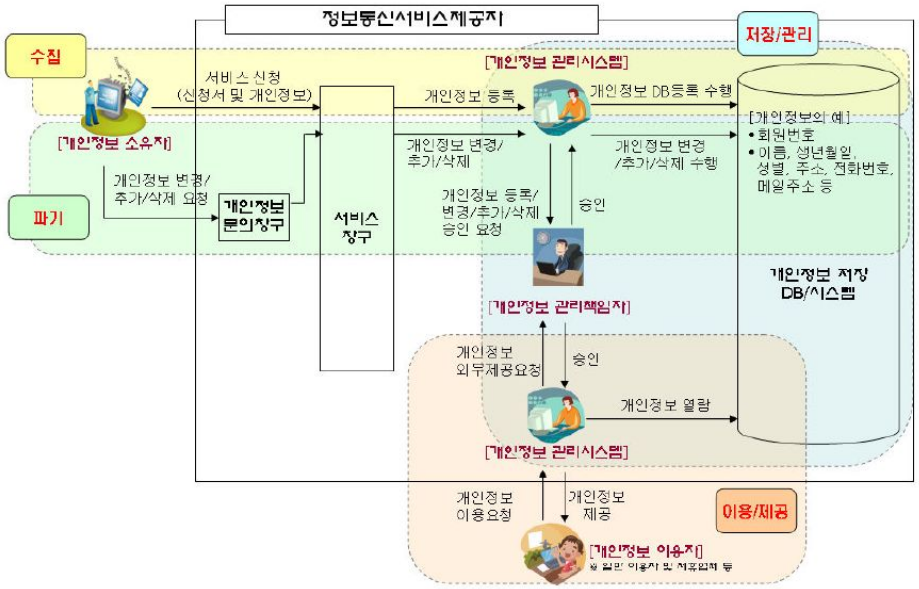
구분	법 시행 내용
규율대상	• 공공·민간 통합 규율로 법 적용대상 확대 -오프라인 사업자, 의료기관, 협회·동창회 등 비영리단체 -국회·법원·헌법재판소·중앙선거관리위원회 등으로 확대
보호범위	• 컴퓨터 등에 의해 처리되는 개인정보파일 • 동사무소 민원신청서류 등 종이문서에 기록된 개인정보도 포함

수집·이용 및 제공기준	• 공공·민간을 망라하는 개인정보 처리원칙과 기준 제시
고유식별정보 처리 제한	• 고유식별정보는 원칙적 처리 금지 -정보주체의 별도 동의, 법령의 근거가 있는 경우 등은 예외 허용 • 고유식별정보 처리시 암호화 등 안전조치 확보의무 명시 • 인터넷상 주민등록번호 외의 회원가입 방법 제공 의무화 대상 확대
영상정보 처리기기 규제	• 공개된 장소 설치·운영하는 영상정보처리기기 규제를 민간까지 확대 • 기존 CCTV에서 네트워크 카메라까지 규율대상 확대 • 공중 화장실·목욕탕·탈의실 등 사생활 침해 우려가 큰 장소는 설치 금지
텔레마케팅 등 규제	• 마케팅 목적의 개인정보처리에 대한 동의는 다른 개인정보 처리에 대한 동의와 묶어서 동의를 받지 않도록 명시적 규정 -정보주체가 알기 쉽도록 고지 및 동의 • 마케팅 업무 위탁시 정보주체에게 위탁업무내용 및 수탁자를 고지
개인정보파일 등록·공개 및 영향평가	• 공공기관 대규모 개인정보파일 구축 등 침해위험이 높은 경우 사전영향 평가 실시 의무화 (민간은 자율시행)
유출 통지	• 개인정보 유출사실 통지 및 신고의무 의무화
집단분쟁조정	• 집단분쟁조정도입 (재판상 화해 효력 부여)
단체소송	• 단체소송 도입 (권리침해 중지)
위원회	• 대통령 소속 개인정보보호위원회 설치 -공공·민간부문 개인정보보호정책 심의·의결 기구

※ 출처 : 행정안전부, 2011

개인정보보호법 시행으로 개인정보를 취급하는 대부분의 법 적용대상자인 민간 사업자들에 대해 의무가 강화되면서 개인정보보호 수준을 높이기 위한 보안 서비스 및 기술 도입이 요구될 것으로 보인다. 특히, 개인정보보호법의 제정으로 개인정보보호 체제, 보안 정책 등 구축하기 위한 컨설팅 시장이 확대될 것으로 보이며, 본 논문에서 제안한 법규기반의 개인정보를 안전하게 사용 및 관리에 대한 연구는 꼭 필요한 기술이라 사료된다.

이러한 개인정보를 안전하게 보호하기 위해서는 정보수집 단계부터 파기 단계까지 전체 개인정보 생명주기 단계에 보호체계가 마련되어야 한다. 개인정보를 수집 및 저장, 관리, 이용하는 정보통신 서비스 제공자가 사용자의 개인정보를 안전하고 효율적으로 관리할 수 있도록 <그림 4>에서와 같이 개인정보의 생명주기별 관리를 위한 보안모델 표준 및 처리시스템을 제시한다[11,18,52]. 이를 기반으로 개인정보 생명주기별 보안 요구사항은 각 기관 및 기업의 환경에 따라 선별적으로 적용될 수 있다.



<그림 4> 개인정보 생명주기별 보안 관리모델

※ 출처 : 한국정보통신기술협회, 2007

개인정보 생명주기는 정보통신서비스 제공자가 개인정보 소유자의 개인정보를 수집하고 이를 저장·관리 및 개인정보 이용자에게 제공하며, 개인정보 보유기간이 종료된 이후 해당 개인정보를 파기하는 일련의 개인정보 관리의 단계를 의미한다. 상기 그림에서 정보통신서비스 제공자가 개인정보 소유자의 개인정보를 수집하고, 이를 저장 및 관리하며 제휴업체 등과 같은 개인정보 이용자에게 고객의 개인정보를 제공하는 개인정보 생명주기에 따

른 일련의 개인정보 처리 흐름을 설명하고 있다.

다음의 <표 7>에서는 개인정보 생명주기를 개인정보 수집, 저장 및 관리, 이용 및 제공, 파기의 4단계로 나누고, 각 단계에 대한 정의 및 단계별 수행되는 개인정보 처리 내용을 나타낸다.

<표 7> 개인정보 생명주기별 주요내용

단계	생명주기별 주요내용
수집	정보통신서비스제공자가 서비스를 이용하고자 하는 개인정보 소유자의 개인정보를 수집하는 단계이다. 수집되는 개인정보는 정적인 개인정보와 동적인 개인정보로 나눌 수 있는데, 정적인 개인정보는 새로운 서비스 가입 시에 정보통신서비스 제공자의 요구에 의해 개인정보 소유자가 제공하여 서비스 탈퇴 시까지 지속되는 개인정보를 말하고, 동적인 개인정보는 RFID나 LBS 서비스 등 특정 서비스 이용자가 제공하는 위치정보, 인터넷 접속 상황을 알려주는 쿠키 정보 등을 의미한다. 즉, 정보통신서비스이용자의 서비스 이용신청(가입)과 동시에 자신의 개인정보를 서비스 제공자에게 제공함으로써 이루어진다.
저장 및 관리	정보통신서비스 제공자가 개인정보 소유자의 개인정보를 저장하고 이를 관리하는 단계이다. 수집된 개인정보를 데이터베이스 등에 저장하고, 개인정보보호정책에 따라 허가받은 자만이 해당 개인정보에 접속할 수 있는 권한 관리 등이 이루어진다. 또한, 개인정보 소유자의 요청이 있는 경우, 개인정보관리책임자의 승인 하에 해당 개인정보를 변경 및 추가하거나 파기하는 등 저장된 개인정보에 대한 관리가 이루어진다.
이용 및 제공	정보통신서비스 제공자가 개인정보 소유자의 개인정보를 여러 가지 필요에 의해 이용 하는 단계이다. 예를 들어 수집·관리하고 있는 개인정보에 대해 개인정보관리책임자의 승인 하에 위탁업체나 제휴업체 등 제 3자에게 제공함으로써 이루어진다. 일반적으로 정적인 개인정보는 서비스 이용자 인증이나 인터넷 쇼핑 등의 기본 서비스 및 이벤트 등의 부가서비스를 위해 이용되며, 필요에 의해 개인정보보호정책에 명시하고 서비스 제공자 외 제 3서비스 제공자에 제공되기도 한다. 따라서 이용 및 제공 단계에서는 개인정보 소유자의서비스 가입부터 ,탈퇴 시까지 정보통신서비스 제공자가 저장 및 관리하고 있는 개인정보 일부를 이용하거나 제공하게 된다.
파기	정보통신서비스 제공자가 개인정보 소유자의 개인정보를 해당 정보의 보유기간이 종료하면 즉시 파기하는 단계이다. 예를 들어 인터넷 서비스 이용

	중단(탈퇴) 및 요청 서비스 종료 시 개인정보관리책임자의 승인 하에 해당 개인정보를 파기한다. 이 단계에서 정적인 개인정보는 서비스 탈퇴 이후, 즉 개인정보 보유기간 종료 시 파기되지만, 서비스 받는 동안 발생하는 위치정보나 쿠키 정보 등 동적인 개인정보는 전체 서비스를 탈퇴하는 시점이 아니라 요청한 서비스가 종료되는 시점에서 지체 없이 파기된다.

※ 출처 : 한국정보통신기술협회, 2007

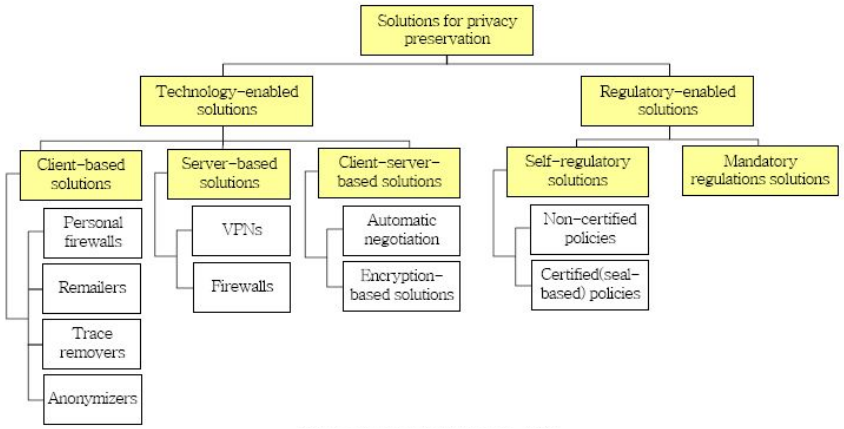
2. 개인정보보호 관련 표준화 기술

1) 개인정보보호 기술

개인정보보호 기술(PET : Privacy Enhancing Technologies)의 개념은 다양하게 정의되고 있다. 먼저 유럽의회에서는 개인정보보호 기술의 의미를 “일반사용자 또는 기술 관리자들에게 어떠한 환경에서 얼마나 많은 혹은 어느 수준의 정보를 공개하고 처리할 것인가를 결정할 수 있는 능력을 제공하는 기술”로 정의하고, AT&A의 Lauren Hall은 OECD 정보보호 작업반회의에서 발표한 의미는 “식별 가능한 정보를 수집 혹은 처리하지 못하도록 하거나 최소화함으로써 정보시스템의 기능적 손해 없이 개인의 프라이버시를 보호하는 다양한 종류의 기술”로 정의하고 있다[17,31]. 이처럼, 개인정보보호기술이란 종류가 다양하고 계속적으로 발전하는 개념이어서 그에 대한 정의 역시 다양하며, 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[11,13].

다양한 연구를 통해서도 개인정보보호 기술에 대해 분류하고 있다. Abdelmounaam에서는 개인정보보호기술을 <그림 5>와 같이 기술 기반 솔루션과 정책관련 솔루션으로 분류하고 있다[7,56]. 그림에서 분류하고 있는 기술 기반 솔루션(Technology-enabled solutions)은 사용자 정보를 보관하고 있는 개인 컴퓨터에 대한 클라이언트 기반 기술(Client-based solutions), 사용자 정보를 관리하고 서비스를 제공하기 위한 서버 기반 기술

(Server-based solutions), 그리고 클라이언트와 서버 간에 유통되는 개인정보를 위한 클라이언트-서버 기반 기술(Client-server-based solutions)로 구분된다. 정책 관련 솔루션(Regulatory-enabled solutions)은 사용자 정보를 관리하는 서버가 자체적으로 규정을 정의 및 제어하는 자율 규제 솔루션(Self-regulatory solutions)과 정부에서 개인정보보호 관련 법률을 제정하고 적용하는 의무 규제 솔루션(Mandatory regulations solutions)이 있다[30,56].



<그림 5> 프라이버시 기술 분류

※ 출처 : IEEE Security&Privacy, 2003

기술 기반 솔루션에서 클라이언트 기반 기술에는 개인 방화벽(Personal firewalls), 리메일러(Remailers), 경로 제거 기술(Trace removers), 익명성 기술(Anonymizers)이 포함된다. 개인 방화벽 기술은 개인 사용자 시스템에서 방화벽과 관련된 기술이며, 리메일러는 메일 전송의 익명성을 제공하는 서비스 기술로 송신자의 정보를 숨긴 후 수신자에게 전달하고 수신자의 답장을 대신 송신자에게 보내주는 기술이다. 또한 경로제거 기술은 인터넷 사용자의 웹 사용 정보가 노출되지 않도록 기록을 제거하는 기술이며, 익명성 기술은 웹 사용자가 자신의 IP 주소 등의 정보를 숨길 수 있는 기술이다. 서버 기반 기술은 VPN과 방화벽 기술(Firewalls)로 분류된다. 이 기술들은 개인정보보호 기술이라기보다는 정보보호 분야의 일반적인 기술이므로 본 논문에서는 설명을 제외한다. 클라이언트-서버 기반 기술은 자동 협상 기술

(Automatic negotiation)과 암호화 기반 기술(Encryption-based solutions)로 구분된다. 자동 협상 기술은 클라이언트와 서버가 각각 프라이버시 정책을 정의하고 협상을 통해 개인정보를 유통 및 관리하는 기술로써, W3C의 P3P가 대표적이다. 암호화 기반 기술은 클라이언트간의 개인정보 교환에 있어 대칭키, 비대칭키 등을 이로써 PGP 기술이 대표적이다[56,63]. 상기 분류에서 정책 관련 솔루션에 해당하는 기술들은 법률 및 정책 정의에 따라 개인정보보호를 하는 것으로써 본 연구와 비슷한 목적을 제공하고 있다.

다른 연구에서는 개인정보침해기술에 대응하여 크게 6개 영역(에이전트기반기술, 웹 기반 익명성 제공기술, 네트워크 기반기술, 암호화 기술, 정책협상 기술, 내부정보보안기술)에 걸쳐 세부 개인정보보호기술을 분류하였다[13,63]. 다음 <표 8>에서는 영역별로 개인정보보호기술에 관해 살펴본다.

<표 8> 개인정보보호 기술의 6개 영역 구분

분야	방법	종류
웹 기반의 익명성 제공 기술	• 소유자 간의 관계 및 송수신자 간의 관계를 비밀로 하여 사용자의 개인정보보호를 제공하는 기술 • 사용자들 간의 비연결성을 통하여 익명성을 제공하는 기술	-클라이언트 익명성 제공 기술 (Anonymizer, Onion Routing, Crowds) -서버 익명성 제공 기술 (Janus, Rewebber network)
에이전트 기술	• 사용자 파악이 어려운 웹상에서의 정보 유출에 대해 사용자를 대신하여 통제해 주는 역할	-쿠키매니저 -에드브로커 -스파이웨어 필터 등
네트워크 기반 기술	• 개인정보 침해사고들은 네트워크 환경에서 정보를 전달할 때 중간에 가로채거나 수정 및 단순히 그 데이터를 보기만 하는 행동들에 의해 발생하며 이를 예방하는 기술	-방화벽 -침입탐지시스템(IDS) -프락시 서버
정책협상 기술	• 웹 사이트 운영자에게 이용자 자신의 정보를 관리할 수 있는 권한을 넘겨줌으로써 이용자 정보가 잘못된 방법으로 사용	-P3P

	되지 않도록 보호하기 위해 만들어짐 • 웹 브라우저나 다른 사용자 도구로 하여금 자동적으로 해당 웹사이트의 프라이버시에 관한 정보를 읽음 • 사용자가 미리 설정해 놓은 정보공개 수준과 비교하여 정보를 선별적으로 제공	
암호화 기술	• 암호화를 통해 전자 메일 메시지, 저장된 파일, 온라인 커뮤니케이션을 보호 • 암호화가 이루어지면 오직 그 당사자만 암호화된 정보에 대한 디지털 키를 가지고 정보를 열람 • 디지털 키는 브라우저, 생체인증, 스마트 카드 등과 결합하여 생성	-SSL -키 교환 프로토콜 (RSA, DES, MD5, Diffie-Hellman 등)
내부정보 보안기술	• 주요 기술정보, 개인정보, 국가기밀 등 이권에 관계된 정보가 유출됨을 보호 • 정보유출 주체를 내부자로 한정하며, 내부 통신 내용을 모니터링 • 시스템 내부에서 일어나는 기술적인 침입을 탐지·방어하는 기술을 탑재	-서버 보안 솔루션 (Secure OS 등) -문서 보안 솔루션 (DRM, IRM 기술 등) -데이터 보안 솔루션 -이메일 모니터링

이와 같은 개인정보보호기술은 프라이버시 보호를 위한 효율적인 방법 중 하나로 구분되어 개발하고 발전되고 있으며, 본 논문에서는 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호 및 개인정보 처리에 관해 규정한 주요법안 내용을 기반으로 개인정보 정책에 준한 기술과 접근제어 통제기술, 관련된 표준화 기술에 대해 기술하였다.

2) 접근제어 기술

접근제어란 사용자가 접근할 수 있는 자원의 범위를 제한하여 허가되지 않은 접근을 방어하는 것이다. 즉, 컴퓨팅 자원, 통신 자원 및 정보자원 등에 대하여 읽기, 쓰기, 실행 등의 접근 여부를 허가하거나 거부하는 기능으로써, 자원에 대한 기밀성·무결성·가용성 및 합법적인 이용과 같은 정보

보호 서비스에 직접적으로 기여하게 되며 이러한 서비스들의 권한 부여를 하게 된다. 대표적인 접근제어 모델의 종류는 강제적 접근통제(MAC : Mandatory Access Control)와 임의적 접근제어(DAC : Discretionary Access Control), 역할기반 접근제어(RBAC : Role Based Access Control) 등이 있다[7,49].

먼저 임의적 접근통제는 권한 있는 사용자가 임의적으로 다른 사용자에게 객체에 대한 접근을 허용할 수 있는 기법으로 정보객체를 요청하는 사용자의 신원에 근거를 두고 접근허가를 결정한다[7]. 이 방식은 접근권한의 통제가 정보객체의 소유자에 의해 다른 사용자에게 허가되거나 철회될 수 있으며, 정보객체의 소유자의 재량에 따라 접근통제가 이루어지기 때문에 어떠한 사용자든 임의적으로 정보에 접근이 가능토록 되어 있어 보안상 문제가 될 수 있다. 이에 안전한 서비스를 제공하기 위해서는 강제적 접근통제 기법을 적용해야 한다. 강제적 접근통제는 시스템 보안 관리자에 의해 부여된 사용자와 정보객체의 보안 등급에 의해 정보에 대한 접근허가 여부를 결정한다[7]. 즉, 각 객체(자원)에 비밀 등급을 부여하고, 사용자를 포함한 각 주체에 허가 등급을 부여한 후 주체가 객체에 접근할 때마다 자격을 체크하여 강제적으로 통제하는 것이다. 이는 정보객체와 사용자에게 배정되는 보안 등급이 체계적으로 잘 정의될 수 있고 매우 엄격한 정보의 흐름만을 허용하여 임의적 접근통제보다 안전하다.

하지만, 강제적 접근통제는 군사 분야와 같은 매우 특정 영역에만 적용되는 단점을 가지고 있어서 융통성이 필요한 일반적인 기업환경에 적용하는데 문제점이 있다. 반면 임의적 접근통제는 강제적 접근통제 정책보다 유연한 정보보호 메커니즘을 제공할 수 있는 장점이 있으나, 확장성이 부족하고 소유자 재량에 따라 접근통제가 쉽게 변경 가능하여 보안적인 취약 문제가 발생할 수 있다[32].

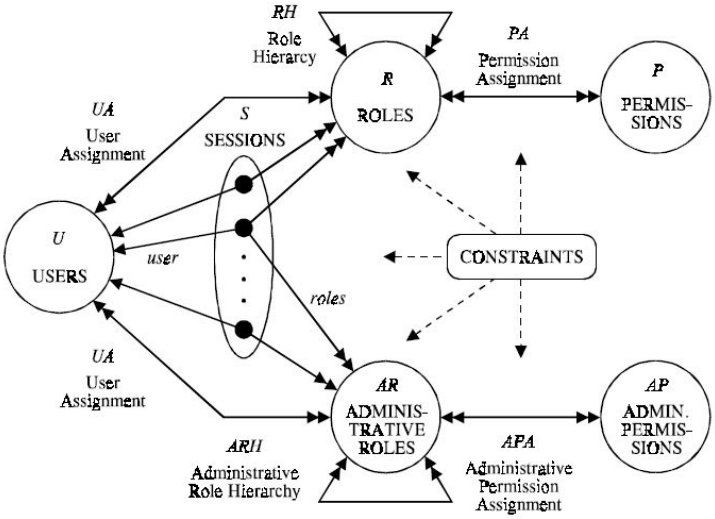
이러한 문제로써 일반 회사조직 및 상업 환경 적용을 위해 역할기반 접

근통제가 널리 연구되고 있다. 기존 접근통제의 표준인 강제적 접근통제 및 임의적 접근통제의 대안으로 제시되고 있으며, 연구기업 환경뿐만 아니라 데이터베이스, 운영체제 등에 적용될 수 있는 매우 유연한 접근통제 정책으로써 이론적으로 기존 접근통제 정책보다 수행하기 어려운 보안관리 과정을 효율적으로 처리하고 특정기관 및 기업에 내부 보안정책을 명확하게 표현하는 등 능률적인 접근권한 관리를 수행할 수 있는 장점을 가지고 있다[49,33]. 아래는 본 연구의 기본이 될 수 있는 기술로써 역할기반 접근통제의 특징 및 기능을 알아본다.

- **역할기반 접근제어(RBAC, Role Based Access Control)**

역할기반 접근제어는 1970년대에 개척된 온라인 시스템의 개념으로 시작되었으며, 사용자가 기업이나 조직의 정보 자원을 임의로 접근할 수 없도록 제한함으로써 기존 접근통제의 표준인 강제적 접근제어 및 임의적 접근제어의 대안으로 연구되고 있다. 역할기반 접근제어 모델에서 사용자는 객체를 임의로 접근할 수 없도록 하는 대신에 접근 권한이 역할(Role)에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 이는 조직 내에 이용될 수 있는 매우 유연한 접근 통제 정책으로 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다[7,19]. 즉, 기업의 업무적 역할 및 책임에 따라 인가권한을 역할에 할당하여 구성원이 되며, 접근 구조의 변경 없이도 역할 변경을 쉽게 할 수 있어 사용자들의 권한 관리를 효율적으로 할 수 있도록 지원한다[33]. 이러한 기능을 기반으로 관리자에게 누가, 언제, 어디에서, 무슨 행동을 수행할 수 있는지에 대해 규정할 수 있다.

<그림 6>은 역할기반 접근제어 모델로 나타낸다[25,26].



<그림 6> The RBAC96 Model

<그림 6>에 표현된 모델에서 핵심 구성요소는 역할과 관련된 행동을 나타내는 연산과 역할의 구성원으로 표현될 수 있는 사용자이다[25,26]. 사용자(*U* : USERS)는 사용자의 집합으로 시스템을 사용하는 사람들을 의미하며 인간의 행동이나 자율적인 에이전트도 포함된다. 역할(*R* : ROLES)은 조직 내 업무 및 직무의 집합으로 수행 가능한 권한과 책임감을 고려하여 구성된다. 즉, 이와 연관된 의미를 가진 직무나 기능으로 이름을 정의할 수 있으며 한 조직의 일에 따라 다양한 형태로 생성될 수 있다. 여기서 제시한 사용자 할당(*UA* : User Assignment)은 사용자와 역할이 다-대-다(many-to-many) 관계이므로 한 사용자는 하나 이상의 역할과 관련될 수 있고, 하나의 역할은 한 명 이상의 사용자를 가질 수 있다. 권한(*P* : PERMISSIONS)은 특정한 객체에 대해 수행 가능한 접근방식의 집합으로써, 시스템에서 하나 이상의 대상 및 자원에 대한 접근 허가 및 거부 등의 제한을 나타낸다. 권한 할당(*PA* : Permission Assignment) 또한 다-대-다(many-to-many) 관계이므로 하나의 역할은 여러 권한을 제공할 수 있고, 하나의 권한 역시 여러 역할에 부여될 수 있다. 이러한 관계는 객체 및 자원을 접근하는 일반 사용

자뿐만이 아니라 정보를 다루는 관리자에게도 역할(*AR* : ADMINISTRATIVE ROLES)과 권한(*AP* : ADMINISTRATIVE PERMISSIONS)이 적용된다. 역할기반 접근제어는 접근을 통제하고자 하는 단위로 기존의 방법과는 달리 역할 계층(*RH* : Role Hierarchy), 관계(Relationship), 제약(Constraint)에 대한 정립을 통해 사용자의 행동을 규제할 수 있다. 특히, 역할 계층은 부분적인 순서체계 안에서 구성된 것으로 상위 역할은 하위 역할로부터 그 허가권한이 전파된다[19,35].

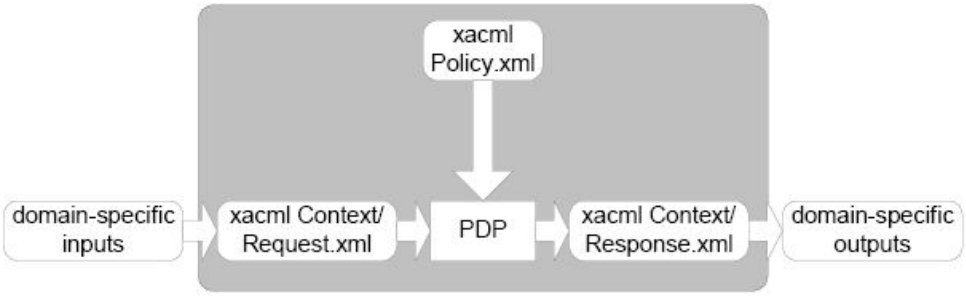
이러한 특징은 업무를 수행하는 실제 환경에서 역할기반 접근제어를 자연스럽게 적용할 수 있는 점이다. 또한, 역할의 개념을 사용함으로써 사용자와 그들의 권한들을 효과적으로 관리할 수 있으며, 조직 내 개인에게 접근 권한을 인가할 때 발생할 수 있는 잠정적인 에러, 복잡성, 비용 등을 줄일 수 있는 강력한 구조이다.

3) XACML (eXtensible Access Control Markup Language)

개인정보를 보호하기 위해 P3P, EPAL, XACML 등 다양한 정책 표현언어 연구가 진행되고 있다. 본 논문에서는 조직 및 기업의 보안정책을 위해 효율적인 정책 표현을 제공하는 XACML에 대해 알아본다.

조직 내 보안정책 표현은 각각의 시스템에서 독립적으로 관리되고 있는 경우가 일반적이며, 보안정책의 수정에는 많은 비용이 소요되거나 신뢰성이 떨어진다. 기업에서 보안정책을 시행하는데 있어서 보안 대책에 대한 통합성을 확보하는 것은 사실상 어려우며, 보안정책을 표현할 수 있는 공통적인 언어의 필요성이 높아지고 있다. 이에 OASIS(Organization for the Advancement of Structured Information Standards)는 정당한 자원 요청 개체에게만 권한을 부여하여 자원들을 접근할 수 있도록 XML 기반의 접근제어 정책 언어인 XACML을 표준화 기술로 진행하였다[20]. 이는 XML의 문법(syntax)과 의미(semantics)가 보안정책 언어의 유일한 요구사항들을 만족

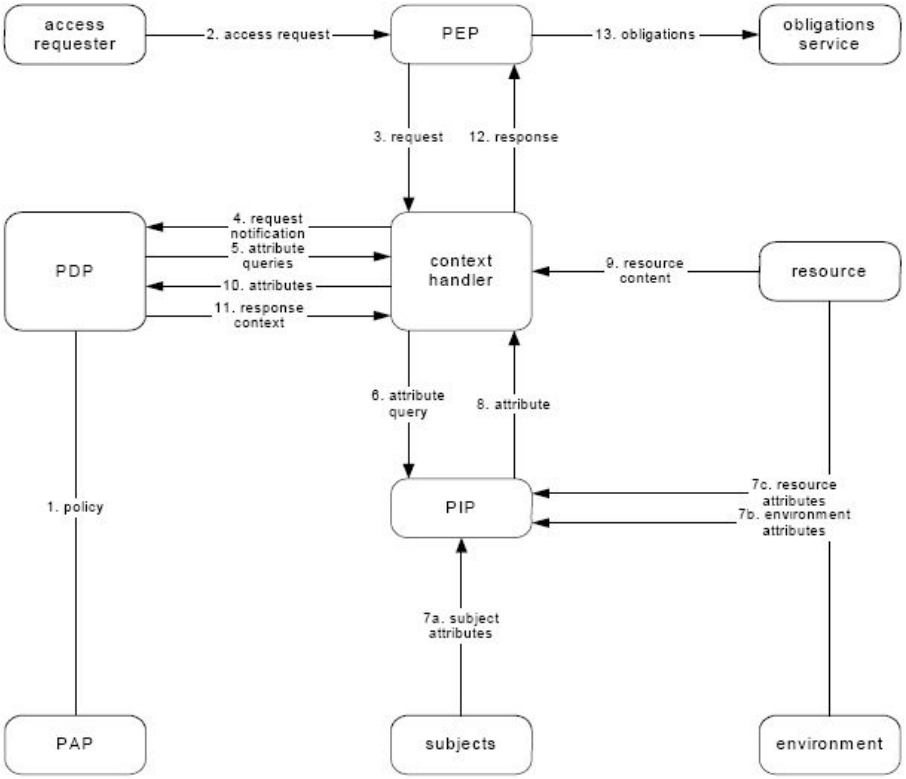
시킬 수 있을 만큼 쉽게 확장될 수 있고, 주요 플랫폼과 툴 벤더들이 XML을 지원하기 때문이다. 특히 대 기업과 같이 매우 복잡하게 구성된 공유 자원을 사용할 수 있는 접근제어 서비스를 제공해 줄 수 있으며, XML 기반이기 때문에 다양한 플랫폼에 적용이 용이하며, 통합적인 접근제어를 가능하게 할 수 있다[20,22]. XACML의 명세는 <그림 7>과 같이 이용자가 요청을 하면 시스템이 자동으로 정책판단을 하고 그 결과로써 응답할 수 있도록 접근제어 정책(Policy)과 요청 컨텍스트(Request), 그리고 응답 컨텍스트(Response)를 XML로 명세할 수 있도록 XML 스키마를 제공한다[20].



<그림 7> XACML 문맥

※ 출처 : OASIS, Extensible access control markup language(XACML) V3.0., 2012

시스템이 XACML을 이용해 접근통제를 수행하기 위해서는 <그림 8>에 표현된 것처럼 PEP(Policy Enforcement Point), PDP(Policy Decision Point), PAP(Policy Administration Point) 등의 요소들이 상호작용한다[20]. 자원 요청자(access requester)가 접근요청을 하면 요청 컨텍스트를 생성하여 컨텍스트 핸들러(context handler)에게 보내고, 컨텍스트 핸들러는 요청 컨텍스트를 PDP에게 보내 권한 결정을 요청한다. PDP는 PAP가 설정해 놓은 정책을 반영하여 요청자의 접근가능 여부를 판단해 응답 컨텍스트를 생성하고, 컨텍스트 핸들러를 거쳐 응답결과를 PEP에게 보낸다. PEP는 의무조치(obligation service)와 함께 접근을 허가한다[20,21].



<그림 8> XACML 데이터 흐름

※ 출처 : OASIS, Extensible access control markup language(XACML) V3.0., 2012

본 연구에서는 이와 같은 데이터 흐름을 기반으로 범용적으로 사용할 수 있는 XML 기반의 보안 정책을 명세하는 것을 주목적하여 인터넷 환경에서의 다양한 응용 서비스를 적용 및 서비스의 보안성을 높이는데 기여할 수 있을 것으로 보인다.

Ⅲ. 개인정보보호에 관한 선행연구

1. 개인정보보호 관련 모델 연구 검토

정보보호 및 개인정보보호와 관련된 법률, 표준 등에서 명시되는 다양한 요구사항들을 통합적으로 관리하기 위해서는 국내·외에서 보편적으로 사용되는 정보보호 관리 및 개인정보 관리 프레임워크가 필요하다. 아래는 국내외에서 추진했던 개인정보보호 모델 및 프레임워크 프로젝트를 설명한다[11,12,39].

- PORTIA (Privacy, Obligations, and Rights in Technologies of Information Assessment)[7,11] – 예일대와 스탠포드에서 진행한 프로젝트로써, 특정 시스템 환경에서의 민감한 정보를 다루는 하나의 효과적이고 개념적인 프레임워크를 개발로써 프라이버시 침해 환경을 개선한다. 주요 연구 주제는 개인정보보호를 위한 데이터 마이닝 및 감독을 하고, P2P 시스템 안에서의 민감한 데이터 처리를 제공한다. 또한 데이터베이스 시스템을 위한 정책 실행 도구를 개발하며 ID의 탈취와 보호에 대한 연구를 수행한다.
- PISA (Privacy Incorporated Software Agent)[29] – EU와 캐나다에서 수행한 프로젝트로써, 네트워크 환경에서 개인정보 유출 없이 사용자를 대신하여 복잡한 업무를 수행하는 지능형 소프트웨어 에이전트(ISA) 모델을 개발하는 것이 목적이다. 개인정보를 보호하기 위한 정책 메커니즘을 통해 프라이버시 보호 기능을 제공하며, 에이전트 기술, 데이터 마이닝, 암호화 등의 기술이 요구된다.
- PRIME (Privacy and Identity Management for Europe)[28] – EU에서 수행한 프로젝트로써, 통합된 Identity 관리 시스템들이 프라이버시를

강화하는 실제적 발전을 위한 설계에 주요 목적을 두고 있다. 즉, 하나의 컴포넌트의 프라이버시에 집중하기 보다는 통합된 프라이버시의 해결책으로써, 정보 사회의 법적·사회 경제적·기술적 측면에서 개인의 자치권을 유지하면서 프라이버시 강화형 Identity 관리 솔루션을 구축한다.

- PiMI (Privacy in the Mobile Internet)[7,11] – 모바일 환경에서의 프라이버시 증대에 대한 기술적인 솔루션을 제안한다. 즉, 모바일 인터넷 환경에서 트래픽 데이터, 위치 데이터, CPI(Capabilities and Preference Information), 컨텐츠 데이터와 같은 개인데이터들의 개인정보보호 취약성을 해결하는 적절한 데이터 보안과 보안정책 구현을 제시한다.
- BS10012 (Data protection on Specification for a personal information management system)[7,11] – 1998년에 제정된 영국 DPA(데이터 보호법률)의 요구사항에 대한 컴플라이언스 향상을 위해 조직의 개인정보 관리체계를 수립하고 운영하기 위한 개인정보보호 프레임워크를 제시한다.
- PIMS (Personal Information Management System)[27] – 국내에서 개인정보보호 강화를 목적으로 2010년에 개발한 개인정보보호 프레임워크를 제시한다. 이는 개인정보보호 관리 체계의 정의, 관리 체계 구성 요소 및 구축방법에 대하여 기술하고 있으며, 조직에서 관리체계 구축 시 구체적인 실행방법을 개인정보 관리과정, 보호대책, 생명주기 3가지의 큰 틀로 구분한다.
  - ✓ 개인정보 관리 과정은 개인정보보호 정책 수립 및 조직 구성, 침해위험 분석에 따른 보호대책 적용계획, 위험관리 과정을 통한 개인정보 관리계획 도출과 계획 내 대책 구현 및 운영, 이후 검토와 모니터링을 포함하는 사후 관리를 지속적으로 수행
  - ✓ 개인정보보호 대책은 관리 체계를 구축하고 운영하기 위해 요구되

는 기술적, 관리적, 물리적 보호 대책에 대한 세부적인 내용

✓ 개인정보 생명 주기는 개인정보 취급 생명 주기와 관련된 법적 요구 사항을 개인정보 수집에 따른 조치, 개인정보 이용 및 제공에 따른 조치, 개인정보 관리 및 파기에 따른 조치로 구분하여 실행 방법

○ IDMS(Identity Management System)[7,37] – ETRI에서 개발한 Identity 관리 시스템으로, 사용자, 서비스, 정보통신기기 등 네트워크에 연결되는 개체의 identity 속성, 신원 증명서, 정보 이용 자격 등을 포함한 네트워크 Identity의 생명주기를 전체적으로 관리해주는 플랫폼 기반 구조이다.

기본적으로 관련연구들은 개인정보보호 표준화 기술(P3P, XACML 등)로 정책 표현을 제공하고 기존 개인정보보호기술(PET)을 통해 사용자인증 및 암호화, 익명성이 보장된다. 또한, 시스템 내 프라이버시 정책을 정의 및 설계하여 그 기반으로 개인정보를 관리 및 보호할 수 있도록 하였다[11,13]. 그러나 관련연구를 통해 살펴본 프라이버시 정책 제도는 현행 개인정보보호 법 관련 대비하여 체계적인 기술적 구현이 미흡하고, 기존의 접근제어의 이용으로 동적인 상황에 즉각 대응하기 어렵다. 특히, 현재 국내기준에 맞춰진 개인정보보호법 기반의 개인정보 관리 기술이 미비하여, 서비스 이용 시 개인정보보호의 보장이 확실한지 확인할 수 있는 방안은 미흡하다.

2. 학술적 선행연구 검토

본 논문은 개인정보보호를 위한 접근제어에 중점을 두고 연구함으로써, 선행연구는 개인정보보호를 위한 정책기반으로 접근제어 모델을 제시하는 논문을 살펴보았다.

접근제어 모델 중에서도 이론적으로 이상적인 역할기반 접근제어를 이용하여 프라이버시 보호를 할 수 있는 연구들이 많이 나왔으며 특히, 역할기반 접근제어 모델을 확장하여 연구한 논문은 다양하게 존재한다. Qun Ni et al.[40, 41]은 프라이버시 정책을 지원하는 역할기반 접근제어 확장형 모델(P-RBAC : Privacy-aware Role Based Access Control)로써 사용자(User), 역할(Role), 데이터(Data), 액션(Actions), 목적(Purposes), 조건(Conditions), 의무사항(Obligations)으로 이루어진 모델을 제안하고 있다. OECD에서 제시한 원칙 및 프라이버시 규정을 표현하기 위해 여기서는 조건 표현을 위한 LC_0라 불리는 조건 언어(Condition Language)를 사용하여 구조화된 방식으로 규칙을 표현하고 있다. P-RBAC에서 제약(constraints)에 해당하는 조건의 표현을 명확히 하고 권한할당 및 의무수행에 대해 조건이 모호한 표현들을 탐지하여 우선순위를 비교하는 알고리즘을 제시한다. 따라서 해당 논문을 통해 다양한 프라이버시 기반의 접근제어 확장 방식 및 정책표현에 대한 이해는 구할 수 있었지만, 적용되는 프라이버시 규정을 표현하기 위해서 조건을 표현하는 부분에 한계가 있으며, 시스템적으로 구현하는 측면에서는 조건 및 의무수행에 따른 안전성과 책임추적성에 대한 방안은 미흡해 보인다.

역할기반 접근제어 모델을 확장한 다른 논문으로써, 유비쿼터스 컴퓨팅 환경을 위한 상황과 직무-역할 기반의 접근제어 메커니즘(CA-TRBAC : Context Aware-Task Role Based Access Control)을 제시하고 이를 기반으로 시스템을 설계할 수 있는 연구방안을 소개하고 있다[42]. 이 논문은 접근제어 정책을 상황정보 기반으로 하는 CA-TRBAC을 통해 수시로 변하는 상황

정보를 보안 서비스에 실시간으로 적용할 수 있도록 제안하고 있다. 하지만 역할기반 접근제어를 조직에 적용하기에는 논문에서 제시한 구체적 정책 정의가 미흡하며, 유비쿼터스 환경 내 상황인식 정의를 하는데 동적 변수가 많이 존재할 것으로 이에 대한 구체적인 방안을 제시하지 않는 이상 중복이나 오버헤드가 많이 발생하여 적용하기에는 어려움이 있을 것으로 예상된다.

프라이버시를 적용하고 확장하는 역할기반 접근제어 모델에 대한 연구뿐만 아니라, 안전성 확보를 위해 프라이버시 보호 관련 법률을 적용하여 개인정보를 수집하거나 이용하는 등 개인정보 처리 시에 보호를 의무화하도록 규정하는 정책기반의 모델들도 연구되고 있다. RBAC에 기초한 통합형 프라이버시 보호 모델[43]은 기존의 P-RBAC[40, 41], 목적모델, 의무모델의 프라이버시 모델을 통합하여 RBAC 기반 통합 프라이버시 보호 모델(IPP-RBAC : Integrated Privacy Protection Model based on RBAC)을 설계하고 이를 기초로 한 XML 정책 언어 모델을 제안하였다. 그리고 제안모델을 의료정보 시스템에 적용시켜 실행 가능성을 나타내었다. 이 논문은 포괄적인 프레임워크를 제공하며, P-RBAC의 구성요소들을 자동으로 관리할 수 있도록 정책에 적합한 언어를 제공하고 있으나, 여전히 조건을 표현하는 정책표현이 제한적이며, 법규 및 규정에 대한 의무화에 대해 보장받을 수 있는 안전성 확보가 표현되어 있지 않다. Ahmed AL Faresi et al.의 정책기반의 접근제어[36]를 보면, 사례로써 HIPAA(Health Insurance Portability and Accountability Act)의 프라이버시 규정을 기반으로 접근제어를 의료정보 시스템에 적용한 연구이다. 이 연구는 HIPAA를 준수하는 PHI(Protected Health Information) 접근 및 기록방안과 개인정보보호를 위한 ITEPP(IT-enforceable privacy policy) 모델을 제시한다. 이로써, 헬스 케어를 위한 프라이버시 접근제어 강화 솔루션을 표현하고 있으며, 개인정보를 소유하고 있는 환자의 프라이버시를 보호하기 위해 동적이고 새로운 환경에 적용할 수 있는 강화된 정책을

제공하고 있다. 하지만 HIPAA를 적용하는 세부적인 구성요소(purpose, condition, obligation 등)의 구체적 정의가 미흡하여 정책을 어떻게 제시하는지에 대해서는 알 수 없었으며, 해외 서비스에 적합한 내용이라 국내 규정에 적용하기에는 제한이 있다.

정보기술의 발전으로 인해, 새로운 서비스 환경에서 정책기반의 접근통제가 다양하게 연구하고 있다[53,55]. 특히 최근 몇 년간 급증한 소셜 미디어의 환경에서는 개인과 관련된 정보를 안전하게 관리할 수 있는 프라이버시 기술이 중요해졌다[51]. 이에 대해 최향창[38]은 소셜 미디어 환경에서 안전한 정보공유와 활용에 대해 연구를 수행하였다. 소개한 모델은 소셜 환경에서 공유되는 개인정보의 접근통제를 개인정보 소유자가 결정할 수 있도록 하고 프라이버시 보호를 보장하는 정책들을 개별적으로 수립하여 안전한 접근통제가 가능할 수 있도록 제안하였다. 이 논문은 적용하고자 하는 표준기술을 설명하고 있으나, 소셜 미디어와 결합하기에는 미흡해 보이며 개인정보 유형분류를 제시한 타당성도 부족하여, 향후 연구가 더 필요할 것으로 보인다. Schneier의 연구[44] 역시 소셜 미디어 환경에서 이용되는 정보로 발생할 수 있는 개인 성향에 대한 분석을 통해 발생할 수 있는 위협과 소셜 미디어 환경에서 이용되는 정보에 대한 분류에 기반을 둔 프라이버시 접근법에 관한 연구를 하였다.

이와 같은 다양한 역할기반 접근제어 연구에서 프라이버시를 실현하기 위한 기술로 W3C의 P3P와 OASIS의 XACML을 이용하는 연구 등이 있다[57, 58]. P3P(Platform for Privacy Preference)는 정보통신서비스 제공자와 서비스 이용자 사이에서 개인정보보호정책을 자동 분석할 수 있도록 XML 형식으로 표현하는 플랫폼이다[13,63]. 이는 개인정보보호 정책을 자동적으로 검색하여 적절하다고 판단되는 경우에 자신의 개인정보를 제공할 수 있도록 지원하기 위해 개인정보보호 정책 표현을 제공하고 의사결정 작업을 자동화하는 기술적 메커니즘을 제공한다. 하지만 P3P는 다른 표준기술들에 비해

간단한 표현방법을 제공하여 명확한 프라이버시 정책언어를 표현하기에는 제한이 있다. 또한 개인정보가 이용되는지에 대한 추적이 어렵기 때문에 명시한 개인정보 수집 목적으로 정확하게 사용되었는지에 대한 규정이 없어 안전성 보장 마련이 필요하다. XACML(eXtensible Access Control Markup Language)은 OASIS에서 제공하는 접근통제 표준 언어이다[20,24]. 이 언어는 정당한 자원 요청자에게만 권한을 부여하여 자원을 접근할 수 있도록 XML 기반으로 제공한다. 즉 규칙 및 정책이 정의된 프로그램 라이브러리를 이용하여 접근제어에 대한 정책 관리, 비밀성 제공, 정책 무결성 보장, 정책에 대한 식별, 신뢰모델을 제공될 수 있다.

앞서 설명한 프라이버시 표준 언어를 적용하여 접근제어와 상호 보완하는 기술로써 연구되고 있다. Jianning Geng[23]는 프라이버시 정책을 표현할 수 있는 프라이버시 관리 프레임워크(Personalized privacy policy management framework)를 연구하며 프라이버시 관리에 대해 정보주체가 직접 참여할 수 있도록 하고, 정책은 규제명시 뿐만 아니라 사용자가 한눈에 쉽게 이해할 수 있도록 제안하였다. 여기서 표준화되고 가독성이 좋은 프라이버시 정책을 위해 기존의 표준기술인 P3P, Privacy Bird, Nutrition Label for Privacy 등을 이용하였다. 이 논문을 통해 프라이버시 정책을 시스템에 적용할 수 있도록 명시적으로 표현함으로써 모호함에 대한 문제를 대안을 제시하였으나, 사용자 개인의 맞춤으로 정책을 적용할 수 있게 했다는 의미를 내세우기에는 설명이 부족하고 정책에 대한 충돌부분에 예외를 위한 설명도 짧아서 좀 더 연구가 필요한 부분이라 사료된다.

접근제어 모델을 실제 환경에 적용할 수 있는 방안 연구도 존재한다. 실 환경에서 정형화된 역할기반 접근제어 모델을 설계 및 구현하는 논문[34, 46]은 보안 모델을 기반으로 시스템에 개발을 할 수 있는 프레임워크(Assurance Management Framework, AMF)를 제시한다. 이 논문에서는 보안 모델과 시스템 개발 사이의 차이(gap)을 감소하는 설계로써 실증적 프레임

워크를 제안하며, 보안모델을 표현하고 정책을 명시 및 검증하며 설계 시 자동적으로 보안을 수행하는 도구를 통해 proof-of concept protype[4]을 검증한다. 또한, 제안한 AMF와 통합하여 접근제어 시스템을 위한 자동적인 검증과 적합성 테스트를 구성하는 방법론[45]을 제시하여 안정된 기술을 제안한다. 그러나 접근제어에 대한 자동 분석으로써 위반 발생 시 즉각 탐지가 가능하지만 이러한 사고를 예방하기에는 제한이 있다. 즉, 자동적으로 개발할 시에는 규제 제한(constraint)의 명시에 사각지대가 발생하거나 중복되는 명시가 존재할 수 있는 문제점을 지닌다.

4) 프로그램 개념(concept)이 기술적으로 실현 가능한 것인지를 검증하는 것

3. 선행연구 검토에 대한 분석

접근제어 관련 선행연구의 공통적인 이슈는 역할기반 접근제어에 포함된 역할(role)이나 조건(condition), 의무(obligation) 등의 구성요소에 대한 구체적인 정의 및 구조화된 방식으로 표현되어야 한다는 점이다.

본 연구는 역할기반 접근제어 모델에서 프라이버시의 확장하는 방안으로써 프라이버시 규정 및 원칙들의 본질을 명확하게 표현하기 위해 구체적 제한(constraint) 표현으로 명시할 수 있도록 한다. 이는 여러 연구에서도 다양한 표준기술을 적용하고 있으나, 기본 표준기술이 시스템에 적용할 수 있도록 구조화되면서 정책 표현의 제약은 여전하므로 이에 대한 방안 제시 및 이를 보완할 수 있는 대안도 고려해야 할 부분이다. 이론적으로 정의한 모델을 실 환경에 적용하는 방안 역시 추상적 표현을 시스템적으로 구현하는 측면에서 정책이 중복되거나 예외적으로 충돌이 발생되는 부분을 최소화할 수 있는 방안 마련이 필요하다. 특히 빠르게 성장하고 있는 웹 환경에서 역할기반 접근제어의 동적인 요소는 사고대응의 유연성을 제공할 수 있으므로 중요하게 고려돼야 한다. 이와 같이 실 환경에 적용방안을 고려하기 위해서 구체적인 적용방안 및 사례를 제시하여 접근제어 모델의 이해를 도울 수 있도록 한다.

본 연구에서는 프라이버시 규정 적용을 위해 작년에 시행된 개인정보보호법을 기반으로 기술적 대응방안을 제시할 수 있도록 한다. 현재 개인정보보호 규정을 준수한 연구는 시작단계로 수행 중이며, 기존 제시하는 방안의 기술적 효과가 높다할지라도 이를 운영함에 있어 준수해야할 규정, 운영 관리 등 보안 규정을 수립하는 정책적인 측면을 고려해야 할 필요가 있다.

따라서 본 논문에서는 법규를 준수하는 효율적인 보안 통제 수단이 필요하다는 점에서 개인정보보호 접근제어 모델의 연구 방안을 모색하였다.

Ⅳ. 개인정보보호 한계와 요구사항

1. 다각적 측면에서 개인정보보호 문제점

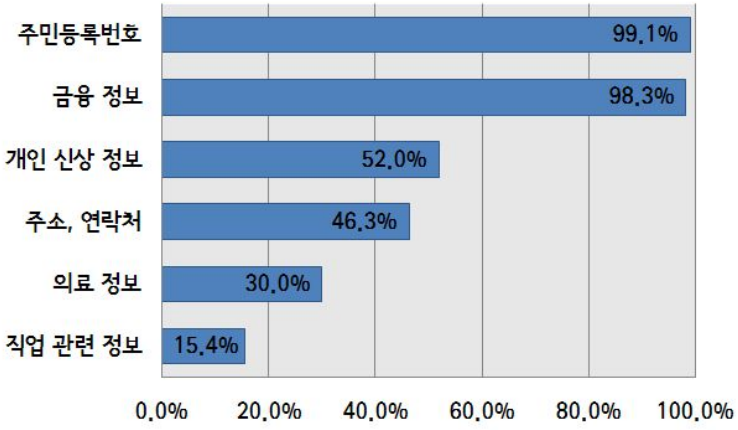
인터넷의 발전에 따라 개인정보의 활용도가 높아지면서 개인정보보호의 중요성이 대두되고 있다. 이에 국내는 2011년 개인정보보호법에 대한 시행을 통해 개인정보의 중요성에 대한 법적 및 제도적 체계화를 시작하게 되었다[9,10]. 하지만 법제도를 준수한 개인정보보호 방안에 비해 개인정보 오남용 방지 및 체계적인 기술적 대응방안은 인프라나 보안기술 미흡 등으로 인하여 개인정보 보호의 체계적 이행이 어려운 실정이다. 기관이나 업체에서 개인정보를 활용하여 업무에 이용하거나 제3자에게 위탁할 수 있는 서비스는 이전부터 존재하였지만, 개인정보보호에 대한 인식부재로 인해 개인정보 침해기술에 대비하여 대응할 수 있는 축적된 기술력이 취약하다.

개인정보는 급변하는 환경 및 신기술의 등장으로 가공 및 활용이 용이해지면서, 정부나 단체로부터 과도한 개인정보의 수집 및 축적, 처리 등을 이용한 개인정보 관리시스템 구축이 가능해지면서 개인정보 도용 및 유출에 따른 피해가 끊임없이 발생하고 있다. 여러 통계나 보도 자료에서 알 수 있듯이 시스템은 실제로 해킹에 의하여 국내 기업 및 사이트가 보유한 개인정보가 유출되거나, 개인정보 데이터베이스를 보유한 기업의 직원을 매수하여 개인정보를 대량으로 유출하는 사례가 빈번하게 발생하고 있다. <그림 9>에서 보고된 것처럼, 이미 개인정보 유출로 인한 집단 소송이 다수 발생 및 진행 중에 있으며, 국내 개인정보보호법이 시행되면서 이후 개인정보 유출로 인한 소송이 더욱 많아질 것으로 예상된다[3,6]. 더욱이 기관 및 기업의 이미지 타격 역시 매출감소와 더불어 심각한 피해를 입을 수도 있다.

<그림 9> 개인정보 침해관련 집단소송 현황

※ 출처 : 한국인터넷진흥원, 2012

이렇게 개인정보를 다량으로 취급하는 기업의 경우에는 개인정보의 위협 및 취약점에 대비하여 안전성과 관리감독을 통해 사고에 대비하는 것이 필요하다. 기업뿐만이 아니라 이용자, 서비스제공자 등에서도 역시 개인정보의 허술한 관리실태 등으로 보안이 위험한 실정이다.



<그림 10> 어떤 정보가 유출되면 소송을 하겠는가?

※ 출처 : 방송통신위원회, 2011

개인정보의 유출 관련한 설문조사에 따르면[4,5], '개인정보가 유출되었을 경우 해당 기업·기관을 대상으로 법적인 소송을 진행하겠는가'란 질문에 응답자의 80.9%가 진행할 것이라고 답해, 개인정보 유출사고에 대한

소송의지가 높은 것으로 나타났다. 특히 주민등록번호와 금융정보가 유출되었을 때 소송의지가 매우 높은 것으로 나타났다. 이러한 결과는 개인정보보호법 시행으로 개인정보 소송절차가 보다 명확해지면서 유출 시 많은 사람들이 소송을 진행할 것으로 예측되며, 기업에게는 장기적으로 정보보호 체계를 정비하고 전략적으로 유출보안의 위협에 대한 대안이 필요할 것으로 보인다. 이에 따라 공공기관 및 민간·단체의 프라이버시 보호의 필요성이 더욱 증대되고 있다.

ㅇ 관리적 측면 이슈사항

개인정보의 관리적인 면에서는 정보주체의 개인정보보호에 대한 인식 및 인지가 중요하다. 개인정보의 유출 및 침해에 대한 보도나 공지 등을 통해 사고가 많이 발생함을 인지하게 되면서 사용자들도 과거보다는 프라이버시에 대한 관심이 증대되고 있다. 개인의 프라이버시 보호방안 연구 자료[5]에 따르면[59], 프라이버시와 개인정보보호에 대한 이용자 인식과 인지가 매우 높게 나타나며 이는 사용자가 프라이버시에 대한 경각심을 일깨워 사회적 문제로 인식하고 있음이 분명하다는 것이다.

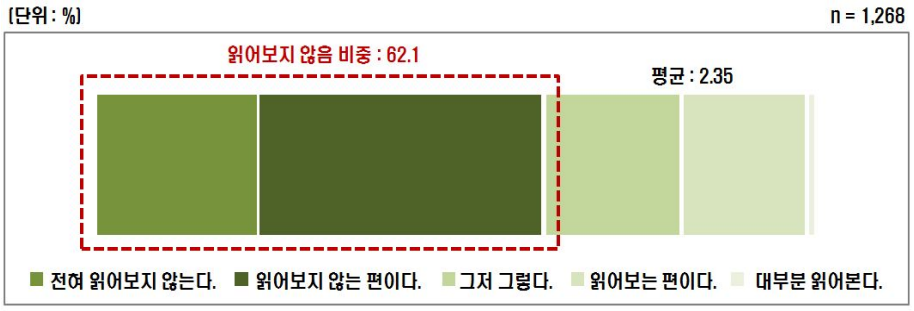
<그림 11> 프라이버시와 개인정보보호에 대한 인지도

※ 출처 : 방송통신정책연구원, 2010

하지만 이러한 관심에 비해 그와 관련된 정책사항에 대해서는 잘 숙지하고 있지 않다. 즉, 서비스를 이용하기 위해 인터넷 사이트에 가입하나 이용

5) 연구 자료에 따르면, 패널을 활용한 온라인 조사를 실시하였으며, 온라인 패널 1만5천여명 중에 인식조사가 가능한 연령대인 만 19~49세를 대상자로 선정하여 조사

자 약관은 읽지 않고, 사이트 가입 시 제공되는 이용자 정보에 대한 노출에 대해 무관심한 태도가 대부분이다.



<그림 12> 이용자 약관에 대한 관심도

※ 출처 : 방송통신정책연구원, 2010

정보주체의 프라이버시 인지와 아울러 개인정보를 다루는 처리자의 프라이버시에 대한 인지도 중요하다. 이는 프라이버시 준수사항을 지킴으로써 직접적으로 개인정보보호 관리에 반영되기 때문이다. 특히나 개인정보보호법의 입법화로 인해 개인정보에 대한 관리감독이 시행되면서 정보보호 수준과 관심이 증대되었다[2]. 기관 및 업체는 개인정보보호 관련하여 내부적으로 업무개선 및 보완을 수행하고 있다. 하지만 앞서 2장에서 개인정보보호 침해현황을 조사한 바와 같이 아직도 안전한 보안 조치사항은 부족하며 관리소홀로 인해 많은 부분의 보완이 필요한 것으로 조사되었다[1,6].

관리적인 이슈사항을 정리하면, 인터넷 사용자들은 프라이버시의 중요성이나 보호를 위한 경각심은 높은 편이나, 이를 보호하는 구체적인 방법에 대한 규정 및 준수사항의 인지는 낮은 편이다. 이를 보완해 줄 수 있도록 개인정보 처리자는 개인정보를 다루는 시스템의 관리적인 면을 고려하여 개인정보 사고발생의 최소화를 마련해야 한다.

○ 법·제도적 측면 이슈사항

급변하는 사회에 맞춰 개인정보를 이용하는 신규 서비스가 확산되면서

개인정보 역시 보안 위협 우려가 확산되고 있다. 특히, 개인정보의 활용도가 높아지면서 관련법에서는 개인의 권리를 존중하며 꼭 필요한 최소정보만을 제공해야 한다고 요구하고 있다. 하지만, 이러한 법제도적인 장치는 개인정보에 대한 보호 사항이 언급되어있더라도 명시되어 있는 부분이 구체적이지 않아 실제 시스템이나 기술적으로 법 적용에 어려움이 되고 있다. 서비스를 제공하기 위한 약관에도 개인정보보호에 대한 처리 사항의 정확한 명시는 확인하기 어렵다[8,15].

법제도뿐만 아니라, 개인정보보호를 위한 표준화의 미비로 일관성 있는 개인정보보호 방안이 어렵다[14]. 국내 개인정보보호법은 법적용 대상이 확대되어 일반 사업자까지 규제 대상이 되고, 발효된 법의 근거로 제도적 방안에 대한 논의가 지속적으로 이루어지고 있으나, 해외 사이트 및 서비스의 경우에는 제한적 본인 확인제, 임시조치 등 국내법 적용에 문제가 있어, 개인정보 침해 등의 대처방안이나 이용자 보호측면이 미흡하여 국내 이용자들의 권리침해 발생의 우려가 있다. 특히, 급부상인 소셜 네트워크 서비스(SNS), 클라우드 등에 대한 신규 서비스 역시 법제도적인 장치가 미흡하여 신규 서비스들의 이용에 있어 정보보안을 위한 대안이 필요하다[38,51].

개인정보보호법이 시행된 지 1년이 지났지만 개인정보 유출사고는 여전하다. 개인정보보호법과 개인정보를 이용하는 현실간의 공백을 좁히고 이러한 법을 기술적으로 적용할 수 있도록 명확하게 명시하거나, 개인정보 취급지침이나 약관을 통해서 법적 보호를 위한 대안이 구체적으로 마련되어야 한다. 즉, 개인이 자기정보를 통제하고 안전하게 개인정보가 관리될 수 있음을 보장 받을 수 있도록 인프라 구축이 마련되어야 한다.

ㅇ 기술적 측면 이슈사항

새로운 기술 개발 및 발전과 함께 신규 서비스가 확산되면서 개인정보 위협 우려를 나타내고 있으며, 이를 위해 법제도적인 마련에도 불구하고 이

를 적용할 수 있는 기술적인 사항은 미흡한 현황이다[14,17]. 한 예로 관련 법에서 사용자의 동의를 받고 개인정보를 수집해야 함을 명시하고 있음에도 불구하고, 사용자의 동의를 받지 않은 개인정부 수집 기술이 남용되고 있는 실정이다[50]. 이는 기업이나 기관에서 개인의 다양한 성향 및 일반정보, 심지어 민감한 정보까지도 활용하여 업무 및 서비스에 반영하려는 요구 때문에 자체적으로 정보를 획득할 수 있는 기술을 이용하는 것이다.

<표 9> 개인정보 수집 기술 [50]

종류	수집 방법	문제점
Cookie & Super Cookie	웹사이트에서 사용자의 로그인 및 개인정보를 저장하기 위한 텍스트 파일	Super cookie의 경우, 일반 cookie와는 다른 위치에 저장되므로 삭제 어려움
Beacon	웹페이지 · 이메일이 로드되거나 특정 이벤트 발생 시, 사용자 정보 전달	JavaScript로 작성된 beacon을 통해 다양한 정보 추출 가능
History Stealing	웹브라우저에 악성코드 실행으로 웹사이트의 링크 목록을 생성 및 랜더링하고 결과를 서버에 전송	별도의 플러그인 설치 없이도 사용자의 접속 기록 알 수 있으며, 침해 여부 인지 어려움
Fingerprint	사용자 장치의 특징을 조합하여 장치를 식별할 수 있는 기술	웹브라우징을 하는 도중에 모두에게 공개되기 때문에 누구나 추적 가능

이와 같은 개인정보 보안의 우려에도 개인정보보호법, 지침으로는 개인정보가 안전하게 처리되는지 보장하기는 어려우며, 법제도적 사항을 준수할 수 있는 인프라 기술의 부족으로 제도 및 규정을 준수할 수 있는 기술을 실체화하는 것 역시 어렵다.

하지만 개인정보를 다량으로 처리하고 다루는 기관 및 기업에게는 장기적으로 정보보호 체계를 정비하고 전략적으로 개인정보 침해 및 유출 위협

에 대한 기술적 대안이 필요하다. 즉, 기술적 측면으로 시행된 개인정보보호 관련 법규를 적용 및 준수하기 위한 컴플라이언스 기술이 마련되어야 한다.

2. 개인정보보호를 위한 요구사항

상기 개인정보의 보안이슈들을 살펴보면 정보통신의 발전으로 개인정보의 활용도가 높아지면서 웹에서 이용되는 개인정보를 효과적으로 통제 및 제어할 수 있는 신뢰기반의 체계적 보호 방안이 필요해졌다. 특히 개인정보보호법의 시행으로 기업에 대한 유출사고에 대해 강력한 대응이 예상되어지면서, 개인정보를 수집하는 기관 및 기업에서는 법을 준수할 수 있는 보안 기술이 요구되고 있다.

앞서 살펴보았던 웹 환경 내 개인정보를 처리하고 활용하는 시스템의 이슈 및 요구사항은 다음과 같다.

- ○ 관리적 – 정보주체의 개인정보보호에 대한 인식 미흡
  - 개인정보를 다루는 처리자가 지켜야 하는 법규 준수 낮음
  - 개인정보보호에 대한 고지 의무사항 준수 미비
- ○ 제도적 – 개인정보 취급지침이나 정책만으로는 보안 보장 확인 어려움
  - 표준화 미비로 일관성 있는 개인정보보호 방안이 어려움
- ○ 기술적 – 개인정보보호 관련 법제도를 준수한 컴플라이언스 기술 미흡
  - 프라이버시 정책기술의 표현상 한계 및 기술적 인프라 부족

이를 기반으로 개인정보의 위협 및 취약점에 대비한 법규를 준수할 수 있는 기술적 대응방안을 마련한다. 본 논문에서 개인정보보호를 위한 확장된 접근제어 모델을 소개하고 구현방안을 제시한다. 과거에는 개인정보보호 관련법이 다양한 분야에 산재되어 있었으나, 현재는 제정된 개인정보보호법으로 일관성 있는 보호 체계가 정립되었다. 이를 이용하여 사용자는 신뢰기반의 웹 환경에서 서비스를 이용할 수 있도록 하고, 기관 및 사업자 측면에서는 법적 보호 하에 안전한 서비스를 제공해 줄 수 있도록 한다. 또한 자연언어로 작성된 개인정보보호법을 시스템 정책에 적용할 수 있도록 자동

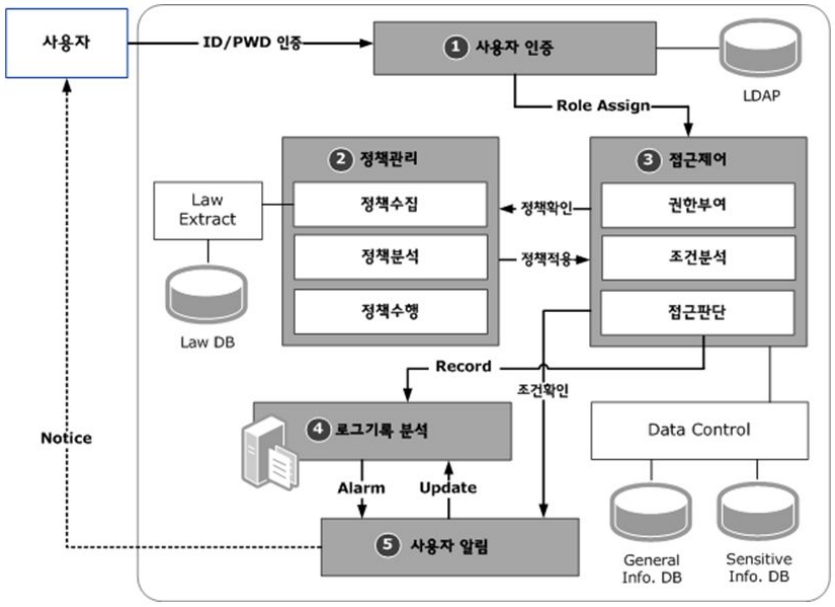
변환 시스템이 기반이 되는 기술적 지원을 고려한다. 시스템적으로 정립된 보안 정책을 구현하는데 있어서 유연성을 제공해 줄 수 있는 역할기반 접근제어(RBAC) 모델을 확장하여 개인정보를 효과적으로 통제 및 제어한다. 역할의 업무적 권한과 책임에 따라 사용자를 설정할 수 있어 접근 구조나 내부적인 시스템 체계 변경 없이도 역할의 변경이 유연하게 적용될 수 있다.

본 연구는 개인정보를 이용 및 활용하는데 신뢰할 수 있는 사용에 대한 접근제어 모델을 제시함으로써, 개인정보의 요청 및 공유 시 보안정책에 준한 체계적인 정보제공을 가능하게 한다. 이는 정책에 준수하여 개인정보를 안전하게 보호 및 관리해줄 수 있는 시스템 구축 방안을 확립하는 것을 목표로 한다.

V. 개인정보보호 접근제어 모델

1. 접근제어 모델 개요

정보통신기술의 발전으로 개인정보의 오남용 및 유출 등 역기능 피해가 계속 증가하면서, 정보화 사회에 대한 사람들의 우려가 가중되고 있다. 이러한 문제점의 대안으로 본 연구에서는 개인정보를 신뢰적이고 효율적으로 접근제어 할 수 있는 모델을 제시하였다.



<그림 13> 신뢰할 수 있는 개인정보 접근제어 모델

개인정보보호를 위한 방안은 다음과 같다. 사용자가 원하는 서비스를 제공받고자 접근을 시도할 때, 우선 ① ID/PWD 또는 PKI를 활용하여 웹 서버에 접근한다. 이렇게 제공된 정보는 검증된 기관으로부터 확인 및 검증을 받은 후, ② 사용자별 정보공유 수준에 적합한 정책할당을 요청한다. 인증된 사용자 정보는 정책저장소에 정의되어있는 보안정책을 기반으로 활용

및 설정될 수 있도록 변환될 수 있다. 이때, ③ 서비스 운영자는 접근제어를 활용하여 사용자 정보와 서비스 제공자의 정책을 비교, 분석하여 적절한 역할대비 권한을 부여한 뒤, ④ 처리내역에 대해 기록한다. 이후, ⑤ 사용자에게 안전한 정보 배부 및 사용자 알림을 통해 제공 받는다. 이러한 5가지의 기능을 포함하여 정의한 접근제어 모델은 <그림 13>과 같이 제시한다. 사용자가 웹 환경에서 서비스를 제공받기 위해 서버에 접근했을 때, 관리자 측면에서 시스템 내부에 개인정보 보안정책을 기반으로 적용되어지는 방법을 제시하는 구조이다.

제시한 접근제어 모델은 5가지 기능으로 1) 사용자 인증, 2) 개인정보보호법 기반인 정책을 제시하는 컴플라이언스 정책관리, 3) 신뢰기반의 개인정보처리를 위한 접근제어, 4) 사고발생 및 위험 등 로그기록 분석, 5) 사용자 알림 기능을 제공하여 개인정보를 안전하게 보호 및 관리해주고 개인사용자뿐만 아니라, 공공·민간 등 단체 기관의 개인정보보호에 대하여 체계적인 보안정책과 함께 신뢰할 수 있는 서비스를 제공할 수 있다.

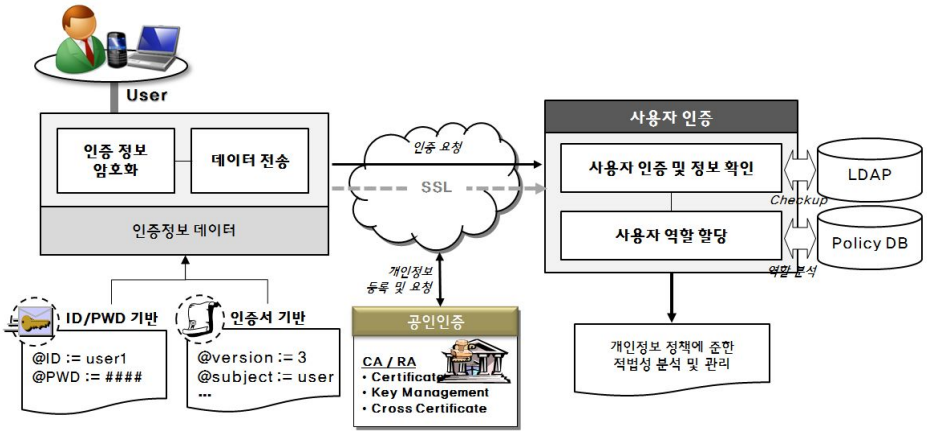
5가지 메커니즘의 방안은 다음과 같다. 먼저 사용자 인증은 사용자의 개인정보를 원하는 기업이나 요청자의 신분확인을 위해 기본속성을 저장하고 검증할 수 있는 기능으로써 X.509 인증서를 통해 암호화 기반의 신분을 확인한다. 검증된 사용자는 역할에 따라 권한을 부여하여 접근통제를 하고 시스템에서 자동적으로 분석하여 접근처리에 반영된다. 불법정보의 오남용 방지를 위한 접근제어는 역할기반의 접근제어 구조로써 정보의 중요도에 따른 설정과 사용자의 역할(접근 레벨)에 따라 유동적으로 통제할 수 있다. 정책관리는 개인정보보호 법·제도 기반의 적합하고 일괄적인 접근제어를 처리할 수 있는 방안을 수립한다. 즉 개인정보보호의 법규를 정립하고 개인정보를 체계적으로 관리할 수 있도록 하여 보안정책이 충돌하게 되어도 시스템 적으로 우선순위를 검사하여 이를 방지할 수 있도록 한다. 사용자가 정보를 수집, 이용 및 제공 시에는 개인의 권리를 존중하며 기본적으로 꼭

필요한 최소정보만을 제공해야한다고 요구하지만, 필요시 개인정보의 민감한 중요정보에 대해서는 사용자의 동의를 먼저 구하는 방식을 적용하고, 개인정보 오남용, 유출로 의심되는 행위 발견 시에는 관리자에게 알림으로 제공, 사용자에게도 통보하여 적당한 조치를 취할 수 있는 기능을 제공할 수 있도록 정립한다. 이러한 보안정책을 자동 변환될 수 있도록 XACML을 이용하여 기술적 언어를 제공한다. XACML은 보안정책을 적용하는데 XML 기반의 언어로써 향후 정책이 추가 및 수정기능이 변경되어도 유연성 및 확장성으로 설정이 용이하다. 이러한 메커니즘의 수행은 개인정보를 효과적으로 보호하기 위하여 선진 표준화 방안이나 관련 법·제도를 적극 수용할 수 있는 체제 확립을 목표로, 주기적인 정보 교류 시 실시간 감시, 개인정보 사용 관리 기능과 로그 분석, 패턴 분석, 리포트 기능 등을 제공하는 정보보호 솔루션 연동으로 위반 시 법적 근거를 제시하도록 하여 책임추적성을 제공한다.

2. 메커니즘 구조 및 기능

1) 사용자 인증 기능

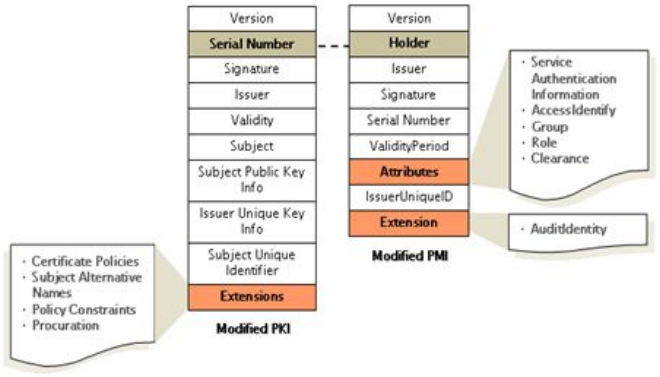
사용자 인증은 사용자의 신분 확인을 위해 기본 속성을 저장하고 검증할 수 있는 메커니즘이다. 인증서를 통한 암호화 기반의 신분 확인 후 개인 정보 보호 정책에 준한 사용자의 속성을 PKI의 확장 필드를 활용한다. 메커니즘에 대한 세부적 구조는 다음과 같다.



<그림 14> 사용자 인증 구성도

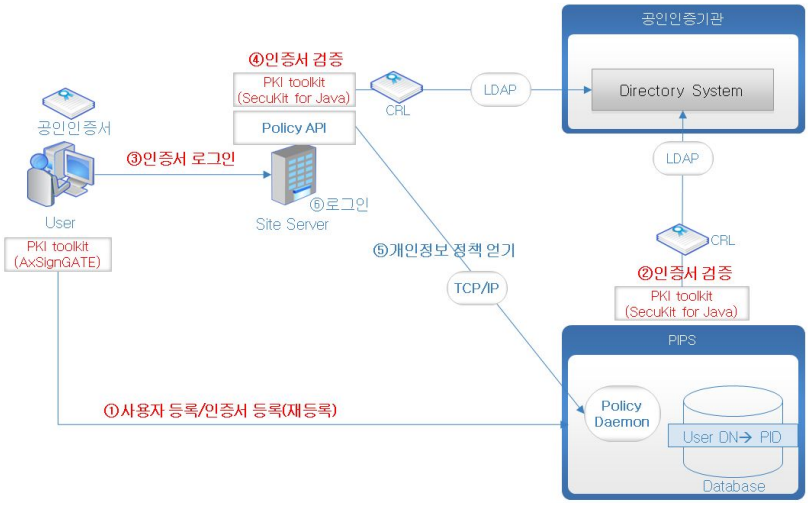
사용자의 주요인증 방안으로 신분확인(Identity Authentication)은 사용자가 정당한 사람인지를 확인하는 과정으로 여러 요소들을 이용하여 신분을 확인할 수 있다. 사용자 신분확인에 이용할 수 있는 요소들로는 아이디, 패스워드를 이용하거나 인증서를 이용, 특히 X.509 v3.0 표준을 준수하는 공인인증서와 인증서 암호를 이용하여 암호화 기반의 강력한 신분확인을 바탕으로 사용자를 검증할 수 있다. 사용자 신분 확인과 함께 이용되는 인증 요소는 웹에 접속하는 정보를 확인하여 식별 및 진위를 판단할 수 있는 인증 방안을 제안한다. 이러한 인증 방안은 PKI 기반으로 컴퓨터 또는 단말 간의 송·수신 데이터에 대한 암·복호화 및 전자서명 검증을 지원한다. 여기서 이

용되는 PKI 속성은 <그림 15>에서와 같이 확장필드를 이용하여 역할정보를 저장하며 웹 환경에서의 정보사용 목적, 적절성 등의 기본적인 통제를 제공, 그에 준한 정책 수행 및 적용할 수 있다.



<그림 15> 보안정책 적용위한 PKI 속성

아래 그림은 ID/PWD와 인증서를 통해 본 연구에서의 연동 및 적용성을 고려한 프로세스를 나타낸다.



<그림 16> 사용자 인증 프로세스

① 시스템에 인증서 검증을 위한 PKI Toolkit이 사전에 설치되어 있어서 사용자 등록을 수행하며, 등록시 사용자의 정보 중 어떤 것을 사용하

는지에 대한 정의를 한다.

- 인증서 등록시 해당 인증서가 사용자의 것이 맞는지 확인하기 위하여 신원확인 검증을 수행하여야 한다.
- 사용자 고유명, 인증서 일련번호 저장한다.

② 사용자가 등록하거나 가지고 있는 공인인증서를 이용한 서비스 사이트에 로그인 수행한다.

- 서비스 사이트에는 해당사용자의 개인정보정책을 얻기 위한 Policy API가 설치되며, 서비스 사이트와 제안 시스템간의 데이터 통신시 암호화 수행한다.

③ 사용자가 제출한 공인인증서에 대한 검증을 수행한다.

- 공인인증기관의 디렉토리 서버를 이용하여 인증서 검증 수행한다.

④ 인증서 검증이 성공한 경우 Policy API를 통하여 해당 사용자의 개인정보정책을 얻는다.

⑤ 해당 개인정보의 정책에 따라 사이트의 등록을 수행한다.

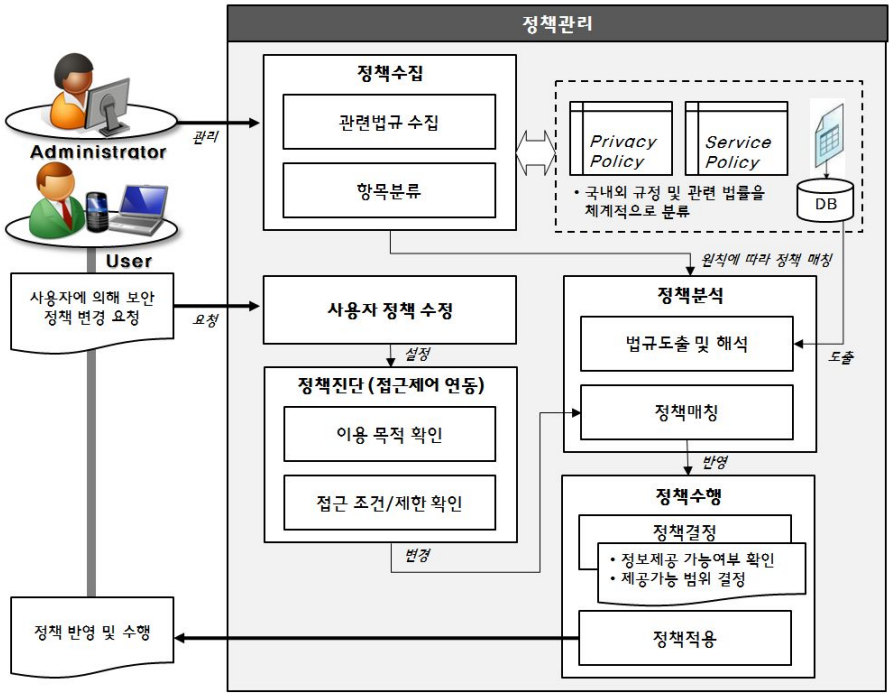
시스템의 신원 확인과 권한 인증을 받은 사용자는 이용하는 인증방식에 따라 보안수준의 차등을 두어 사용 목적의 적절성, 접근제한 등의 판단에 대한 결정을 할 수 있다. 이러한 인증기술은 1차적으로 허가받지 못한 사용자의 접근을 제어하고 불법적인 접근에 자원을 보호할 수 있는 통제하며, 설정된 보안등급과 속성정보를 가지고 이후 보안정책 기반의 접근 제어가 이루어진다.

2) 정책관리 기능

정보통신망을 이용해 대량의 개인정보 수집 및 취급 등이 용이해지면서 정보주체의 자기정보통제권 보장이 될 수 있도록 개인정보보호 법안이 시

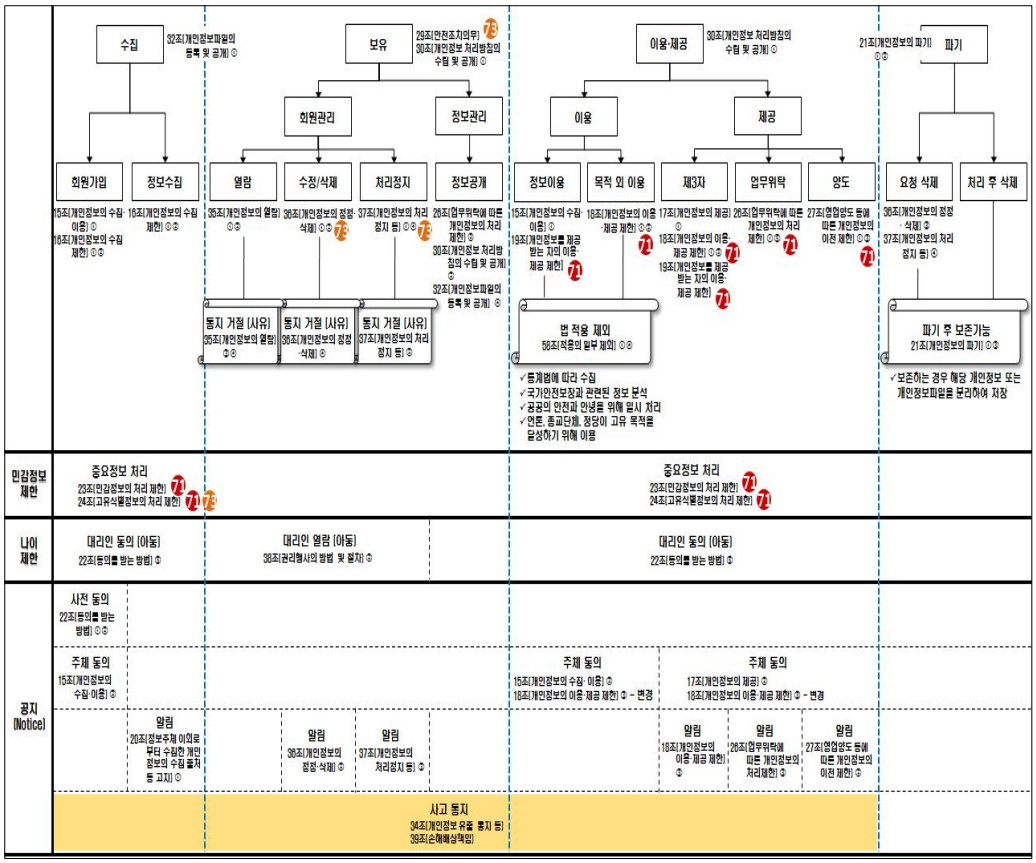
행되고 있다. 개인정보보호법은 개인정보 처리 과정을 수집, 이용, 제공 등의 단계로 나눠 개별 보호기준을 마련했고, 개인정보에 접근하는 사람은 접속기록 등을 보관하도록 안전조치 의무를 부과했으며 대규모 개인정보가 유출됐을 경우에는 관계기관에 신고하도록 하는 내용을 포함하고 있다. 이러한 법규를 체계적으로 시스템화하여 적용할 수 있도록 개인정보 생명주기 단계별 분석을 통해 접근제어를 적용할 수 있도록 법 보호하의 정책을 정립한다.

특히 개인의 권리를 존중하며 꼭 필요한 최소정보만을 이용·제공해야한다고 요구하고 있지만, 필요시에 개인 동의 없이 개인 금융정보, 주민정보 등이 사용되었을 때 처벌을 위한 명확한 법적 대응 방안을 제시하고 아울러 개인정보를 수집 및 저장·관리, 이용 시에 위반이 발생할 때 관련 처벌법에 따라 이행할 수 있도록 기준 및 가이드를 설정한다.



<그림 17> 정책관리 구성도

본 메커니즘은 문서로 배포되어 있는 개인정보보호법, 제도, 지침 등을 자동적으로 시스템화하여 관리할 수 있도록 하며, 이는 사전연구로 조사했던 개인정보 생명주기 단계별 분석을 통해 접근제어를 매칭한 후 법 보호하의 정책을 제시 할 수 있는 체계를 수립한다. <그림 18>은 개인정보 생명주기 단계를 기반으로 개인정보보호법을 적용하여 개인정보 수집, 보유, 이용, 제공 및 공유 등에 대한 프로세스 발생 시 정의된 정책에 의거하여 규정과 처벌을 제시할 수 있도록 분류표 및 개인정보 기준안을 설정한다.



<그림 18> 개인정보 생명주기 단계별 정책 Taxonomy

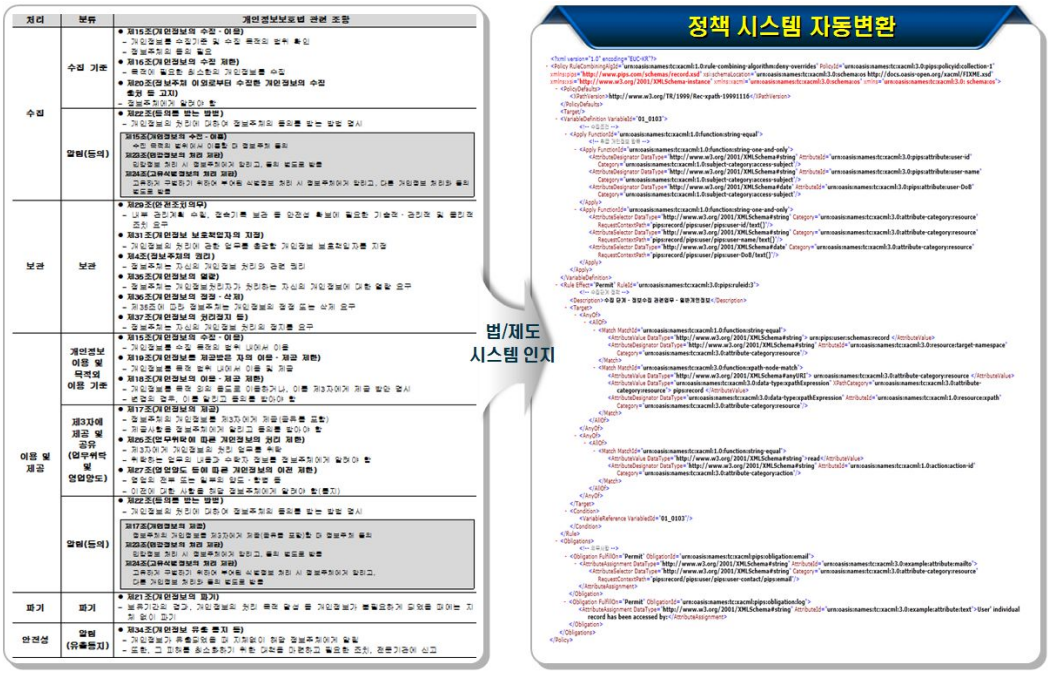
정책 분류표는 정보통신망을 이용한 대량의 개인정보 수집 및 취급 등이 용이해지고 개인정보의 활용도가 높아지면서 개인정보보호 법제도적인 측

면에서는 개인의 권리를 존중하며 꼭 필요한 최소정보만을 이용해야한다고 요구하고 있지만, 필요시 또는 이용목적 불일치 및 필요이상의 정보수집요구 등 위반이 발생할 때, 책임·안전성에 관련된 처벌법에 따라 이행할 수 있다. 개인정보 처리에 해당하는 과정을 생명주기라 말하며, 생명주기를 4단계로 나누고, 각 단계에 대한 정의 및 수행되는 개인정보 처리 내용은 다음과 같이 정리될 수 있다.

- 수집단계 : 무분별한 개인정보 수집을 제한하는데 목적을 두고 있어서 어떠한 개인정보도 합법적이고 공정한 절차에 의해서 수집되어야 하며, 수집정보, 주체(역할), 수집제한으로 구성한다.
- 보유단계 : 이용목적에 필요한 범위 안에서 정보 내용이 정확하고 최신의 것을 유지하기 위해 검사 및 검증을 통해 정보의 완전성을 보호한다. 개인정보와 관련된 개발 및 처리 수행에 대해서는 일반적인 공개정책을 취하여야 한다. 즉, 무단으로 개인정보를 수집 및 오남용 방지를 위해 정보관리 및 파기를 지정하고, 불이행 시 분쟁해결을 통해 관련법규를 따르도록 구성한다.
- 이용 및 제공 단계 : 개인정보를 보호하기 위해 수집정보 및 정보관리를 명확히 명시해야 한다. 정보주체의 동의가 있는 경우이거나 법률의 규정에 의한 경우가 아니면 개인정보 이용이 제한된다. 정보이용을 제한하기 위해 역할 및 정보등급 별로 이용제한을 구성하고, 제공 시 목적과 조건에 따라 이용절차에 의해 처리될 수 있도록 구성한다.
- 파기단계 : 개인정보 소유자의 개인정보를 보유기간이 종료하면 즉시 파기한다.

이러한 보호정책 및 절차를 기준으로 역할기반의 접근제어 기능과 연동하여 정책을 적용할 수 있도록 한다. 이는 개인정보 정책을 적용한 역할 기반 접근제어로써 체계적인 통제 방안을 제공한다. 정의된 기준 및 규정은

파싱을 통해 <그림 19>와 같은 구조 기반으로 표현될 수 있다. 이후 정의된 기준 및 규정을 기반으로 설계하고 시스템 내 실행 가능한 정책으로 전환한다. 자동 변환되는 처리로써 새로운 컴플라이언스의 요구를 쉽게 수용할 수 있으며, 서비스 운영자나 관리자는 개인정보보호 및 서비스에 대한 법 개정 및 보완이 필요할 시, 시스템 정책을 변경하거나 재설정할 수 있도록 하여 환경변화와 상황에 즉시 대응할 수 있도록 한다.

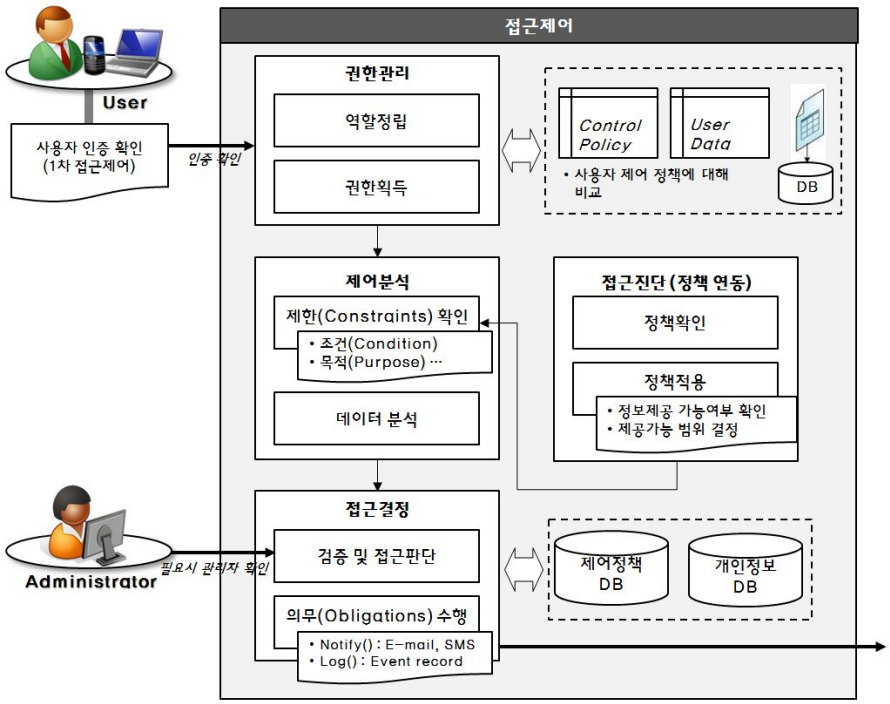


<그림 19> 법·제도 시스템 자동 인지 및 해석

정책설정을 통해 웹 서비스에서 개인정보가 이용될 있는 단계(수집, 보유, 이용 및 제공, 파기)에 따라 정의된 정책에 의거하여 관련 법규를 제시하고 처벌로 통제하여 운영자가 일관성 있는 정책을 수행할 수 있도록 한다. 특히 정책 기반의 위험 분석 및 모니터링을 통한 감시 및 감사로써 개인정보 사용 내역을 관리하고 발생할 수 있는 사고에 대해 법적 증빙체계를 지원할 수 있다.

3) 접근제어 기능

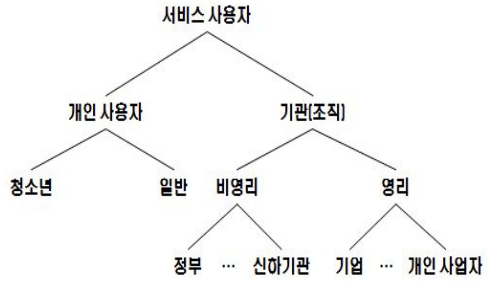
안전한 서비스를 이용하기 위해서 접근제어 기능은 보안의 필수 요소라 볼 수 있다. 이는 1차적 접근제어인 사용자 인증을 통해 사용자별로 권한을 할당하여 개인정보 및 데이터에 대한 접근성을 통제할 수 있다. 개인정보 오남용 방지 및 접근제어 보안을 위한 구조는 <그림 20>과 같이 제시될 수 있다. 접근제어 메커니즘은 웹 환경 내 동적으로 변화하는 자원의 유동성 및 이동성에 따라 적용할 수 있도록 역할기반 접근제어(RBAC)의 구조를 확장하여 접근정책을 적용한다.



<그림 20> 접근제어 구성도

개인정보 접근제어에서 권한관리는 역할기반 구조를 적용함으로써, 인증을 통해 인증된 사용자를 역할에 할당하고 그에 해당하는 조건 및 제한을 적용한다. 또한 사용자의 신분을 유지하고 적합한 권한을 할당하기 위한 사

용자 인증 정보를 분석하며, 사용자의 접근이 적절한지 확인하여 사용자에게 권한을 부여한다. 접근제어 구조에서 개인정보 활용 시에 이벤트 발생이나 이상 징후의 감지 등의 환경 변화는 사용자에게 할당된 역할이 동적으로 변경되어 권한 부여를 할 수 있다.



<그림 21> 역할 계층구조

<그림 22> 보안등급 기준

이와 같이 역할기반 접근제어 구조는 웹 환경을 이용하는 환경 구조에 대해 유연하게 반영할 수 있고, 동적으로 변하는 사용자의 역할에 맞게 제한된 권한을 가질 수 있다. 위 그림에 표현된 바와 같이 사용자의 역할에 따라 권한이 부여되어 개인정보 관리자 관점에서도 자원 이용의 적절성, 접근통제 등 권한에 대한 추가 및 수정이 용이하다. 정책관리에서 제시한 개인정보 정책 및 절차를 기준으로 본 연구에서는 아래 표와 같은 개인정보 중요도를 고려한 기준안을 설정한다.

<표 10> 개인정보 영향도에 따른 자원 보안등급

영향도	등급	적용기준	적용기준 설명	유형구분	개인정보 항목
5	S	S	서비스 관련 정보	통신정보	로그파일
				위치정보	GPS, 휴대폰 위치정보
				법적정보	납세, 전과 등 기록
	P3	P4	단독으로 개인을 식별, Risk 매우 높음 (암호화 지정)	일반정보	주민등록번호
					패스워드, 사번

				신용정보	계좌번호
				소득정보	소득액, 봉급경력
4	P1 + P2	P3	P1과 P2 정보가 결합하여 개인 식별이 가능		
3	P2	P2	단독으로 개인을 식별, Risk 낮음	일반정보	ID, 이름, 주소, 전화번호,
				통신정보	전자우편
2	P1	P1	개인 식별은 어려우나, P2, P3과 조합될 경우 위험	의료정보	과거의 진료기록, 신체장애, 혈액형
				고용정보	회사주소
1	G	P0	개인정보로 가치가 매우 낮은 정보	일반정보	습관, 취미 등

정의된 개인정보 중요도를 기반으로 제어(Constraints) 분석을 통해 이용 목적 및 조건을 분석하며 사용자가 접근 조건으로 적절한지 확인하고 이용되는 데이터, 즉 개인정보의 중요도나 가치 등의 특성에 따라 보호 정도의 차등을 둔다. 이는 개인정보의 보안 등급을 사전에 정립하며 이용하려는 사용자의 권한에 따라 접근 허용이 결정된다. 또한 개인정보 중요도에 따라 자원의 보안등급이 구분되어져 있어 사용자의 권한에 의해 접근 할 수 있도록 한다.

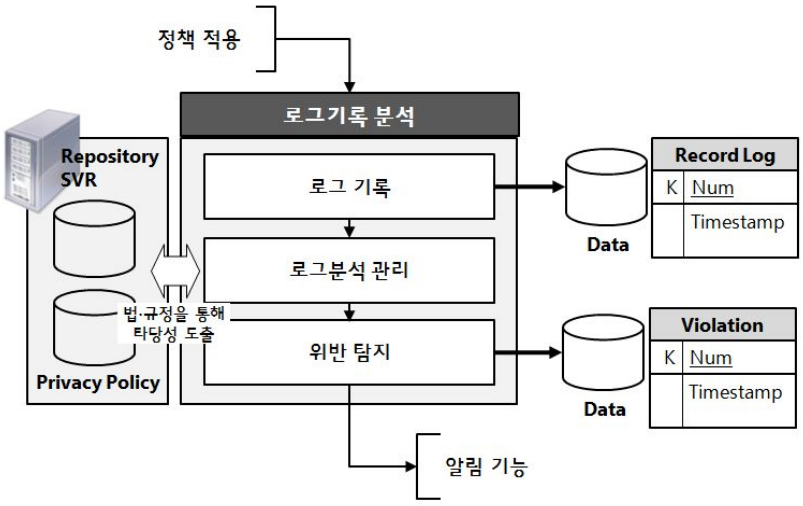
시스템의 결정이 불분명하거나 접근 정보의 위험도가 높다면 접근결정에서 관리자의 확인을 통해 정보의 접근제어를 검증한다. 이러한 과정으로 사용자에게 최소한의 권한을 주어 권한 없는 자의 정보 접근을 제어하고 개인정보 유출 및 정보 손실을 예방하기 위한 기능을 수행할 수 있도록 한다. 또한 데이터는 보안 등급별로 강화된 암호화 기법을 이용하여 데이터를 보안할 수 있다.

본 연구의 접근제어 기능은 정책관리와 유기적 연동 관계를 통해 정보 및 자원들에 대한 접근이 다양한 정책을 통해 제어 될 수 있다. 이와 같은 접근제어 기준 방안으로 실제 개인정보 교류 시 서비스 운영자 측면에서는

웹 환경 내 서비스를 이용하거나 자원을 공유하는 사용자에게 보안기준에 준수한 정책을 적용하여 정보를 이용할 수 있고 시스템 관리자 측면에서는 정보 관리의 복잡성 및 유지비용, 잠재적인 실수 등을 감소할 수 있으며 개인정보 이용에 대한 법제도의 근거 기반을 확보할 수 있다.

4) 로그기록 분석 기능

본 연구의 로그기록 분석에서는 이용자의 개인정보를 안전하게 보호하기 위해 웹 환경 내에서 발생할 수 있는 보안위협 분석을 통해 관리와 지속적인 모니터링을 바탕으로 발생할 수 있는 위협에 대해 예방적 차원의 대책을 마련한다. 또한 사전에 보안 사고를 방지하고 사고 발생 후에도 신속한 사고원인 파악 및 대응에 필요한 의사결정을 지원하여 추가적인 피해를 방지 할 수 있는 구성도를 제시한다.



<그림 23> 로그기록 분석

디지털정보 및 데이터는 개인정보의 침해 및 노출 행위에 대한 법적 평가 관련하여 사실관계의 진위여부를 입증해 주는 증거로서 중요한 의미를

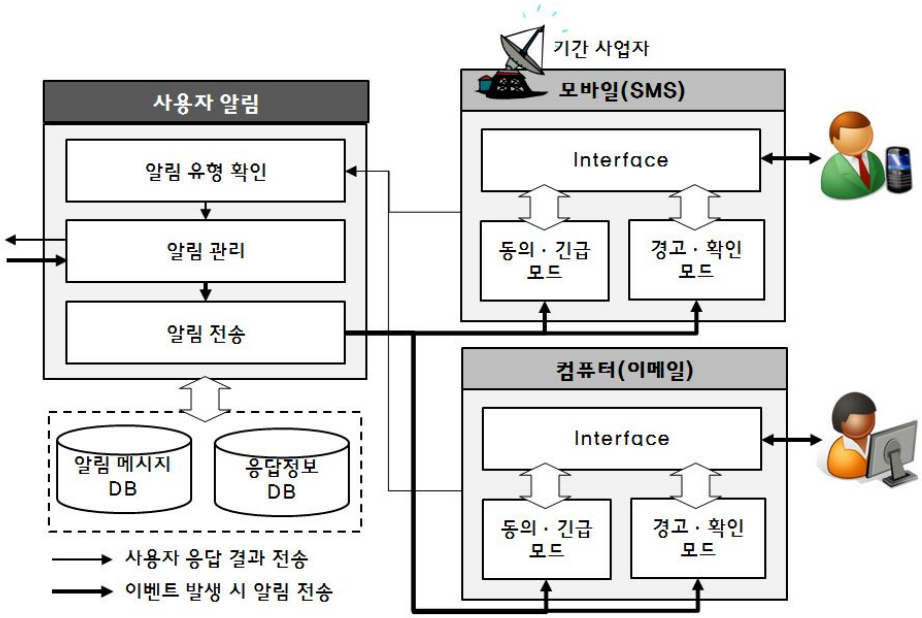
가진다. 개인정보보호법을 바탕으로 본 연구의 로그기록 분석 기능은 해킹 등 개인정보 침해의 위험에 대응할 수 있는 법적 근거가 될 것이며 이를 위해 사용자의 개인정보 수집, 접근요청, 알림 (메시지 발송 및 수신 등) 의 모든 행위에 대한 로그를 기록하며, 그에 따른 국내 개인정보보호법을 적용시켜 개인정보 유 노출 시에 법적인 증거를 제시할 수 있는 토대를 마련할 수 있도록 한다.

우선 로그기록 분석 메커니즘은 로그기록을 바탕으로 개인정보 관련 취약점 및 위협정보를 수집한다. 또한 시스템 자체의 취약점을 진단하여 발견된 취약점에 대한 위협을 결정한다. 결정된 위협을 바탕으로 발생할 수 있는 위험을 정량적으로 측정하여 관리자에게 위험으로 인해 발생할 수 있는 피해를 계량화 및 통계적으로 제공한다. 아울러 알림 기능으로 각종 분석자료 및 연관정보, 위협 정보 및 공격발생 여부를 이메일, SMS 등을 이용하여 고지하여 이를 사용자 알림 메커니즘과 연동하여 서비스를 제공한다. 이러한 기능은 지속적인 모니터링 기능과 연동하여 웹 컴퓨팅 서비스를 구성 및 이용하는 대상을 포함하여 이상 현상 및 행위를 탐지하며, 개인정보 유·노출에 대한 사고발생을 최소화한다. 이후 모니터링을 통한 로그 및 기타 기록물을 분석하여 서비스 이용자의 개인정보에 대한 위협관리 대책을 수립할 수 있다.

5) 사용자 알림 기능

관련법과 규정에 따르면 개인정보를 열람하거나 정정 및 삭제 등의 처리에 대해 정보주체의 권리행사를 할 수 있으며, 시스템 관리자가 개인정보 유출 사실을 인지하였을 때 즉시 해당 정보주체(사용자)에게 관련 사항을 통지하도록 하여 정보주체의 권리보장을 강화할 수 있는 규정이 명시되어 있다. 이에 본 연구에서는 개인정보 유·노출 등의 국내외 법제현황을 참고

하여 웹 환경에서 개인정보 오남용 방지를 위한 알림 및 동의(Notice) 기능을 제안한다.



<그림 24> 사용자 알림 구성도

이는 개인정보의 교류 중 민감한 정보에 대하여 사용자 동의를 먼저 구하는 방식을 적용하고, 기타 개인정보는 임의의 동의 없이 사용되거나, 해킹 또는 오·남용으로 의심 시에는 관리자와 사용자에게 알려 적당한 조치를 취할 수 있어야 한다. 웹 환경에서의 개인정보의 유·노출뿐만 아니라 개인정보의 수집, 저장 및 관리, 이용, 파기의 개인정보 생명주기별로 정보주체의 동의나 확인이 필요한 상황을 분류하여 이메일 및 SMS를 통해 사용자에게 자신의 개인정보가 어떻게 쓰이고 있는지 고지하도록 한다. 개인정보 관련 사항의 고지에서 고려해야 할 사항을 기반으로 사용자 알림 기능에서 사용자에게 통보할 수 있다. 알림기능 메시지는 동의(Consent), 확인(Confirm), 경고(Warning), 긴급(Alert) 4가지로 분류되며, 이 메시지를 해당하는 정책을 적용시켜 고지의 정당성을 제시한다.

사용자 알림 기능은 향후 위협분석 및 모니터링 기술과 연동하여 웹 환경에서 발생 할 수 있는 개인정보의 도용에 대한 사고발생 및 위험에 즉시 대응할 수 있고 정보주체에게 알려줄 수 있도록 한다.

<표 11> 사용자 알림 분류 및 처리방법

구분	타당성	처리방법
Consent	○ 사용자에게 동의가 필요한 경우 보내는 메시지 ☞ 수집 또는 목적 외 개인정보 이용할 경우 별도 동의 필요	동의/거부 버튼 클릭 시 응답을 체크하고 로그를 기록
Confirm	○ 사용자에게 확인이 필요한 사항을 알려주는 메시지 ☞ 타 기관에 정보제공 및 공유, 위탁 시 정보주체에게 알림	메일 수신확인 시 응답을 확인하고 로그를 기록
Warning	○ 침입이 우려되는 상황이거나, 사용자의 동의가 필요한 경우 보내지는 메시지 ☞ 개인정보 유출 및 사고예방을 위해 이상징후 시 정보주체가 조치를 취할 수 있도록 알림	시스템에 즉시 접속하여 관련문제 해결 후 응답을 확인하고 로그를 기록
Alert	○ 정보가 침입되었음을 사용자에게 통지하는 메시지 ☞ 개인정보 침해 및 사고발생에 대해 신속한 유출통지 필요	메일 수신확인 시 응답을 확인하고 로그를 기록

VI. 시스템 설계 및 구현

1. 알고리즘 제시

제안한 접근제어 모델 연구를 기반으로 인가권한을 가지고 있는 자로부터 개인정보의 안전성을 보장할 수 있도록 설계방안을 마련한다. 본 논문에서는 주요한 기능으로써 접근제어, 정책관리, 알림(Notice) 수행을 중점으로 알고리즘을 제시하였다. 먼저 개인정보 정책관리와 접근통제를 위한 알고리즘은 개인정보에 대해 중요도에 따라서 등급별로 분류하여 보안을 효과적으로 할 수 있도록 도와주고, 정보누출 및 유출시 발생할 수 있는 위험성에 대해서 알려줄 수 있는 알림(Notice) 기능을 제시하여 개인정보보호를 위한 관리 방안을 마련한다.

개인정보 접근통제 알고리즘은 개인정보를 효과적으로 보호하기 위해서 허가되지 않은 자가 개인정보데이터에 접근하지 못하도록 통제한다. 또한, 허가받은 자에 의한 보안위협을 고려하여 접근통제 방법을 통해 역할할당 및 제한적인 권한부여로써 개인정보 데이터를 보호하는 알고리즘을 설계한다. 접근통제는 중요도에 따라 데이터의 보호가 필요하며, 데이터에 대한 접근은 주체와 객체가 갖는 보안 등급의 정의를 통해 결정된다. 즉, 아래 알고리즘은 개인정보의 민감한 중요도에 따라 보안등급이 구분되며 정보를 요청한 접근자의 목적이나 권한에 따라 정보를 제공할 수 있는 접근통제에 대한 알고리즘 설계를 표현한다.

Algorithm 개인정보 접근통제

```
1:  if IsValidating(user.id, user.pwd, user.cert) = true then
2:      if CheckCert(user.cert) = true then
3:          sg_level ← CheckSecurityLevel(user.cert)
4:          id_tag ← PolicyId(user.cert, sg_level, timestamp)
5;          return true
```

```
6;      end if
7:  else
8:      return false
9:  end if
10: if CheckAuth(id_tag) = ACCEPT then
11:     role ← AssignRole(id_tag)  // give all permissions to user
12:     pur ← UsePurpose(request, action, id_tag)
13:     id_access ← CheckAccessControl(id_tag, role, pur)
14:     sub_data ← AccessCustomerData(id_access)
15:     LogRecord(adm_id, Today())
16:     Audit(user.id, id_tag, role, pur, timestamp)
17:     return sub_info
18: else if CheckAuth(id_tag) = RESTRICT then
19:     role ← AssignRole(id_tag)  // give limited permissions to user
20:     pur ← UsePurpose(request, action, id_tag)
21:     id_access ← CheckAccessControl(id_tag, role, pur)
22:     switch id_access
23:         case P4 and S:
24:             sub_data ← AccessSubjectData(P4 and S)
25:             check_result ← AlertAdministrator(user, sub_data)
26:             if check_result is confirmed then
27:                 Notice(CONSENT, sub_data.id, pur, sub_data.contact)
28:             end if
29:             Audit(user.id, id_tag, role, pur, timestamp)
30:         case P3:
31:             sub_data ← AccessCustomerData(P2)
32:             Notice(CONFIRM, sub_data.id, pur, sub_data.contact)
33:             Audit(user.id, id_tag, role, pur, timestamp)
34:         case P2:
35:             sub_data ← AccessSubjectData(P3)
36:             Notice(CONFIRM, sub_data.id, pur)
37:             Audit(user.id, id_tag, role, pur, timestamp)
38:         case P1:
39:             sub_data ← AccessSubjectData(P4)
40:             Notice(WARNING, sub_info.id, pur)
41:         case P0:
42:             sub_data ← AccessSubjectData(P5)
43:     end switch
44:     LogRecord(adm_id, Today())
45:     return sub_data
46: else if CheckAuth(id_tag) = DENY then
47:     role ← AssignRole(id_tag)  // give denied permissions to user
48:     pur ← UsePurpose(request, action, id_tag)
```

```
49:         Audit(user.id, id_tag, role, pur, timestamp)
50:         return false
51:     end if
```

정책관리는 자동적으로 보안정책을 처리하고 명료하게 표현 및 이행하는 것이 중요하다. 본 연구에서 국내 법률을 시스템에 적용하여 정책을 설정하고 기술적으로 표현하여 수행할 수 있는 알고리즘을 개발한다. 정립된 보안정책을 시스템적으로 관리자가 추가 및 수정이 가능하도록 설계하고, 정책의 설정 및 파싱을 통해 개인정보를 시스템적으로 관리하며, 정책은 시스템으로 이용될 수 있는 XML 기반의 언어를 사용하여 자동변환을 한다. 즉, 사용자가 정보 접근을 허용하고, 이용하는데 정의한 정책에 의거하여 제공하며, 행위에 따라 규정 및 처벌을 제시할 수 있다.

Algorithm 정책관리

```
1:  requestPolicy ← 시스템에 정의된 요청정책
2:  purposePolicy ← 시스템에 정의된 이용목적정책
3:  result ← false
4:  check ← false
5:  if action is happend then  // Human Readable Policy
6:      i ← 1
7:      while i ≤ requestPolicy.length do
8:          if reqeustPolicy[i].idx = action then
9:              guideidx ← GuideDefineTable(reqeustPolicy[i].relatedguide)
10:             lawidx ← LawDefineTable(guideidx)
11:             if lawidx ≠ null then
12:                 ReadPolicy(user, guideidx, lawidx)
13:                 go to next step
14:             end if
15:         end if
16:         i++
17:     end while
18: end if
19: if policy is requested then // Policy Analysis / Parsing
20:     i ← 1
21:     while purposePolicy[i].idx = user.policy.usepurpose do
22:         parsingResult ← ExecuteParser(puropsePolicy)
23:         result ← ExecutePolicyMatch(parsingResult)
24:         if result = true then
```

```
25:                 PolicyGatheringRepository(result)
26:                 PolicyEnforcement(user, policy)
27:                 return true
28:             else
29:                 return false
30:             end if
31:             i++
32:         end while
33:     end if
34:     Function PolicyGatheringRepository(policy) { // Policy Gathering & Repository
35:         policy ← SelectPolicyInfo(user, xmlContext, accessControl, condition)
36:         if CheckPolicyCollision(policy) = true then
37:             InsertPolicyDB(policy)
38:             doc ← XMLDocumentConvert(policy)
39:             return doc
40:         end if
41:     }
42:     Function PolicyEnforcement(user, policy) { // Policy Enforcement
43:         if policy is updated then
44:             check ← CheckUpdatePolicy(policy)
45:             if check = true then
46:                 UpdatePolicy(num, guideTitle, lawTitle)
47:                 result ← ViewPolicy(policy)
48:                 if result = true then
49:                     InsertPolicyDB(num, oecdIdx, lawidx)
50:                     SendEnforcementMsg(user)
51:                 end if
52:             end if
53:         end if
54:     }
```

시스템 내에서 정보가 변경되거나 추가, 삭제와 같은 특별한 이벤트 발생 시에 로그를 기록한다. 이러한 로그정보는 불법적인 침입여부나, 문제 발생 시 복구 및 대응책을 위한 자료로 사용되며, 법적인 문제 발생에도 중요한 증거로 사용한다. 로그기록 분석 메커니즘에서는 누가 어떠한 정보를 왜 이용했는지에 대한 로그 정보를 데이터베이스에 저장하여 혹시라도 발생할 수 있는 피해를 최소화하는데 목적을 둔다. 적용되는 이유 및 근거는 보안정책에 관련된 법제도에서 이용될 수 있음을 고지한다. 해당절차를 이행하지 않았거나 명시된 목적에 불일치 및 정보 누출 등의 위반이 발생할 경우

적합한 조치를 취하고 책임추적성에 의해 처벌을 이행할 수 있도록 한다.

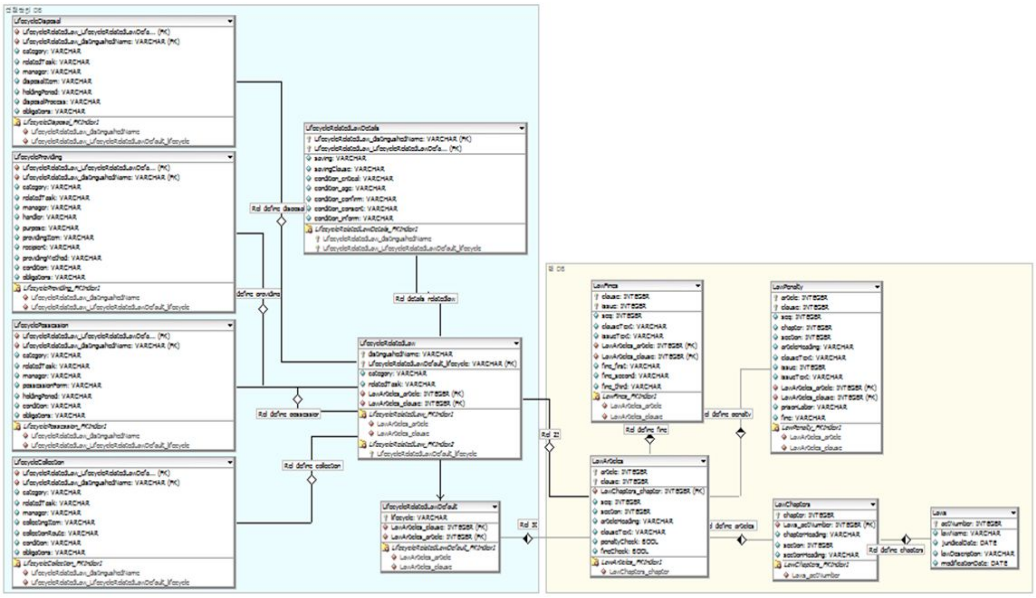
Algorithm 알림

```
1:  resp ← false
2:  chk_notice ← CheckNotice(pur, role, condition)
3:  if chk_notice ≠ null then
4:      switch chk_notice
5:          case CONSENT:
6:              sub_data ← SelectUserData(sub_id)
7:              resp ← SendMsg(sub_data.name, sub_data.contact, msgConsent)
8:              if resp = true then
9:                  give all permission to user
10:             end if
11:             RecordLogFile(user_id, sub_id, pur, resp, timestamp)
12:         case CONFIRM:
13:             sub_data ← SelectUserData(sub_id)
14:             resp ← SendMsg(sub_data.name, sub_data.contact, msgConfirm)
15:             RecordLogFile(user.id, sub.id, pur, resp, timestamp)
16:         case WARNING:
17:             sub_data ← SelectData(sub_id)
18:             resp ← SendMsg(sub_data.name, sub_data.contact, msgWarning)
19:         case ALERT:
20:             sub_data ← SelectData(sub_id)
21:             resp ← SendMsg(sub_data.name, sub_data.contact, msgAlert)
22:     end switch
23:     AdminMonitoring(adm_id, action, timestamp)
24: else
25:     return false
26: end if
27: if event is generated then
28:     imp_level ← ImportantCheck(event)
29:     if imp_level = HIGH then
30:         result ← AdminCheck(imp_level, event)
31:         if result ≠ null then
32:             Notice(WARNING, sub_id, event)
33:             Audit(sub_id, id_tag, role, event, timestamp)
34:         else
35:             Deny(sub_id)
36:         InsertLogDB(sub_id, event, timestamp)
37:     else if imp_level = MIDDLE then
38:         AdminCheck(imp_level, event)
39:         Audit(sub.id, id_tag, role, event, timestamp)
40:         InsertLogDB(subject.id, event, timestamp)
41:     else if imp_level = LOW then
42:         InsertLogDB(sub.id, event, timestamp)
43: end if
```

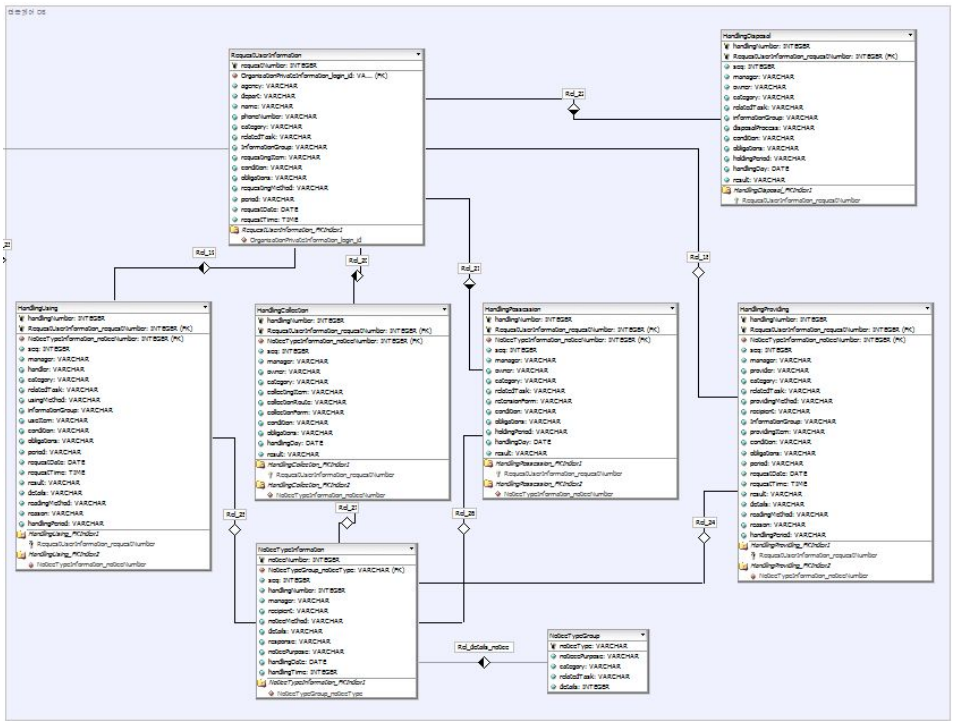
2. 데이터베이스 설계

개인정보는 수집단계를 통해 데이터베이스에서 필요로 하는 개인정보를 수집하고 저장한다. 저장되는 개인정보의 중요도, 유출시 파급효과 등을 고려하여 수집목적 동안에만 유효하도록 관리하며, 저장된 개인정보는 개인정보 담당 책임자에 의해 관리된다. 또한, 개인정보 이용자가 서비스 제공자에게 서비스를 요청하고 필요에 의해 데이터베이스에 저장된 정보를 안전하게 사용하도록 하여 처리한다. 마지막으로 수집된 개인정보는 정해진 목적 동안에만 사용되어야 하고 정해진 목적이 달성되면 안전하게 파기되어야 한다. 이러한 생명주기 기반의 개인정보보호 관련 보안정책을 적용하기 위해서는 시스템적인 구축이 필요하다.

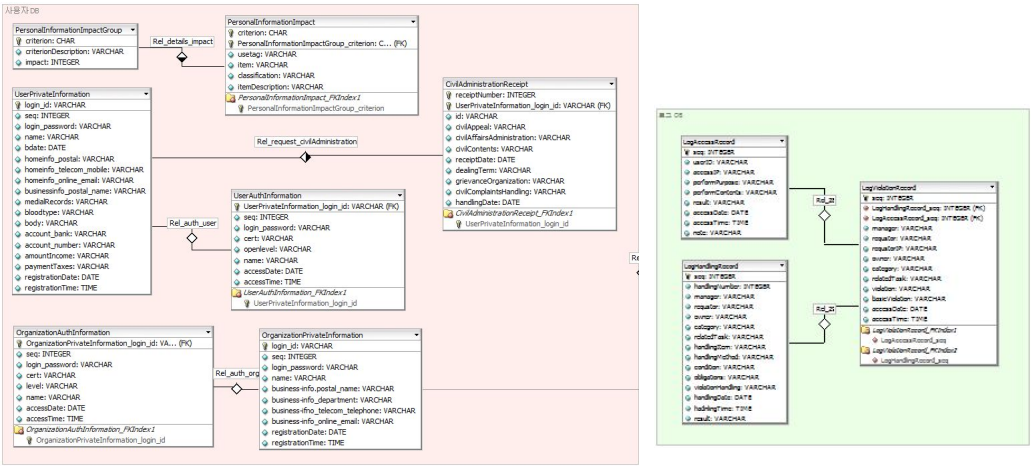
아래 그림은 전체 데이터베이스 설계에서 접근제어 및 정책관리에 수행되는 DB 구성도와 개인정보를 보유하는 사용자 DB, 처리내역을 기록하는 로그 DB를 나타낸다.



<그림 25> 정책 DB



<그림 26> 접근제어 DB



<그림 27> 사용자 DB와 로그 DB

본 연구에서 사용자 DB는 개인정보의 비밀성 및 무결성 등 보안을 제공하기 위해서는 생명주기 단계별 처리에 따라 감사기능을 수행할 수 있도록

하며, 로그파일로써 보유한다. 정보의 중요도, 위험도 등을 고려하여 보안레벨이 높으면 감사로그는 필수 항목으로, 상대적으로 중요도가 낮고 데이터베이스 시스템에 따라 생성여부가 결정되는 로그는 선택항목으로 구분하여 사고발생 및 위험 로그를 기록하여 책임추적성을 제공한다.

3. 프로토타이핑

신뢰할 수 있는 접근제어 모델을 기반으로 본 연구는 실 환경에서의 적용 가능성을 위해 프로토타이핑으로 구현하였다. Window 7 운영체제에서 구현되며, 웹 환경은 Apache HTTP Server 2.2.2를 지원한다. 개발 언어는 웹 JSP와 JAVA 언어를 사용하였으며 DBMS는 MySQL 5.0을 사용하고, 이클립스 Tool을 이용하여 관리자가 이용할 수 있는 인터페이스 화면을 구성한다. 관리자는 사용자 정보에 대해서 해당하는 범위 내에서 모든 정보 접근이 가능하도록 하고 읽을 수 있게 한다. 또한 관리자는 정책정보와 국내 관련법규를 추가 및 변경, 삭제가 가능하여야 하며, 개인정보의 누출사고 발생 및 사고 대응을 위한 인터페이스 구성을 갖는다. 화면구성의 상세설명은 다음과 같다.

- 사용자관리 – 사용자의 역할 및 권한을 확인하며, 개인정보에 대해서도 보여준다. 관리자는 사용자의 역할 변경이 가능하다..
- 법률관리 – 개인정보보호법을 체계적·자동적으로 시스템화하여 관리할 수 있도록 한다.
- 정책관리 – 개인정보 정책 설정 및 분석을 기반으로 보안정책을 관리할 수 있고, 시스템 관리자가 중앙에서 정책을 관리하면서 정책충돌을 예방하고, 만약 정책이 충돌하여도 시스템적으로 우선순위를 검사하여 적합한 정책이 적용될 수 있도록 한다.
- 접근제어 – 관리자에 의해 개인정보를 요청한 사용자의 접근권한과 개인정보 데이터의 접근 권한을 변경할 수 있다.
- 로그기록 – 로그기록은 가입이나 이용, 제공 등의 이벤트에 대해서 로그를 기록한다.

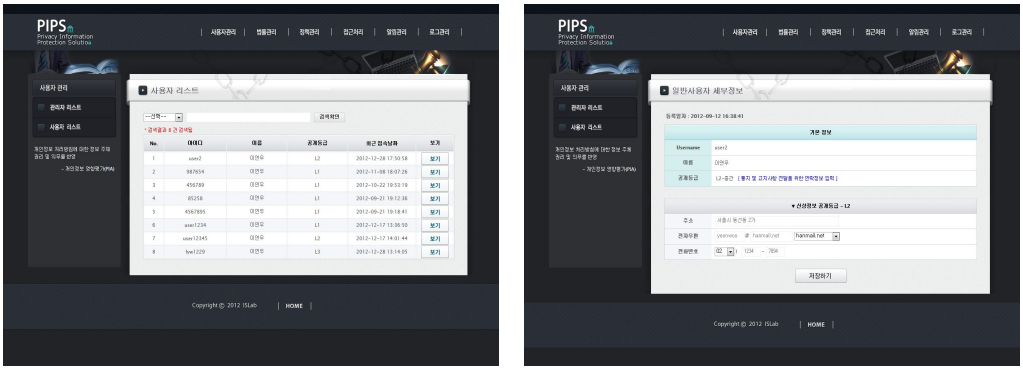
다음 그림은 관리자에게 제공하는 인터페이스의 첫 화면을 보여준다.

<그림 28> 관리자 첫 화면

관리자는 첫 화면에서 전체 이용통계현황을 확인할 수 있으며, 요청된 접근 수와 현재까지 발생된 위반사항 및 처리사항을 간략한 그래프로 알 수 있도록 한다.

1) 사용자관리 화면

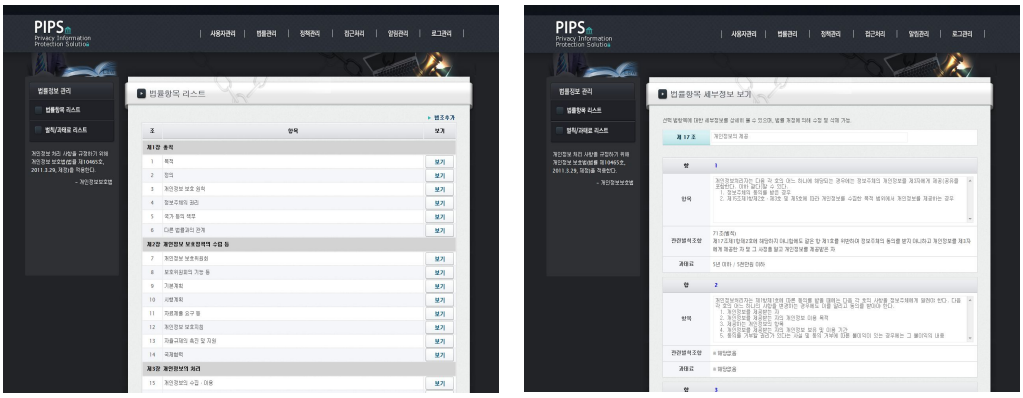
사용자의 인증을 위해 알고 있는 아이디, 패스워드와 함께 자신이 보유한 공인인증서를 기반으로 인증을 한다. 관리자 화면에서 사용자 정보와 함께 사용자의 역할, 권한 등의 정보에 대해서 정보를 확인할 수 있다.



<그림 29> 사용자관리 화면

2) 법률관리 화면

법률관리는 본 논문에서 제시한 모델에서 정책관리 메커니즘의 수집에 해당하는 부분으로써, 국내 개인정보보호 법 기반으로 <그림 30>와 같이 인터페이스를 제공한다.



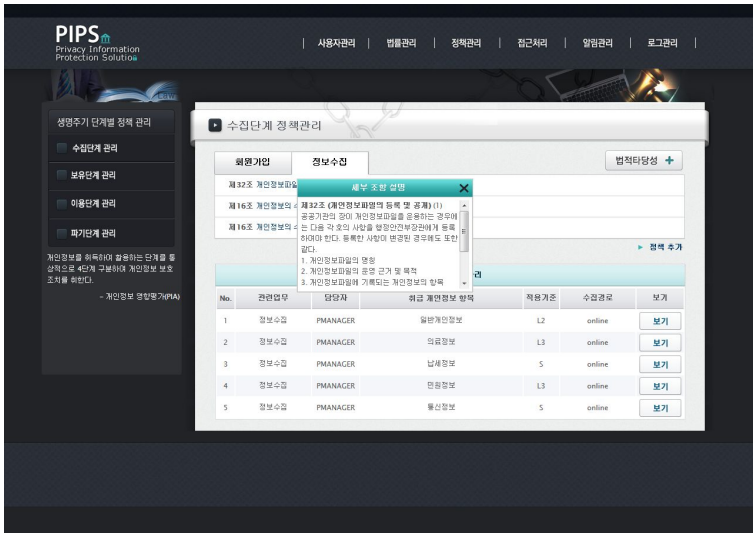
<그림 30> 법률관리 화면

이는 국내 개인정보보호법을 준수하며, 개인정보보호법의 조항을 리스트로 보여준다. 관리자는 개인정보보호법이 개정되거나 삭제되었을 시 법률관리를 통해 법을 업데이트 한다.

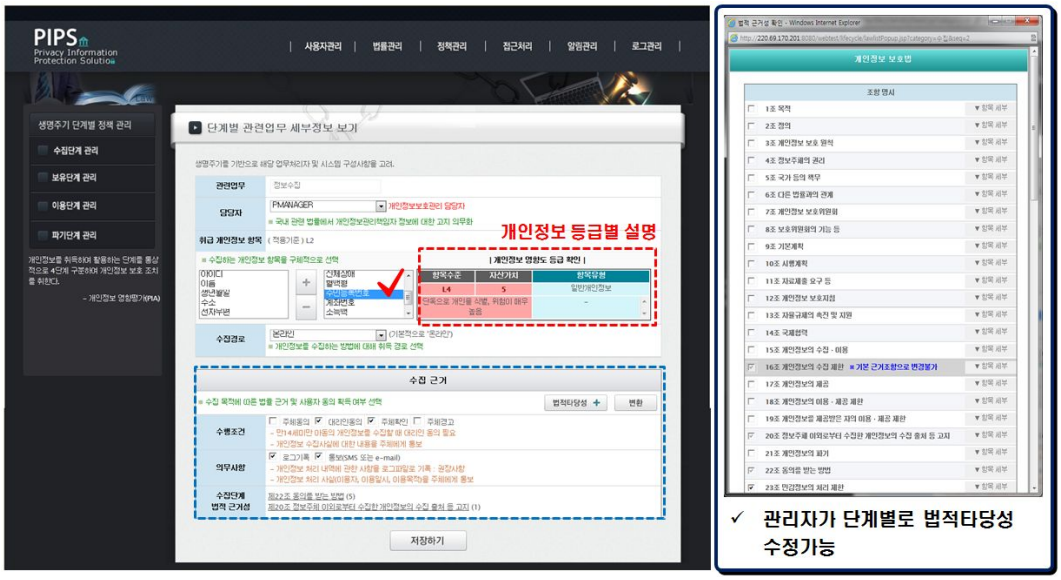
3) 정책관리 화면

정책관리는 국내 콘텐츠 및 정보보호 관련 법제도 기반의 자동화 시스템이다. 시스템은 정책수집, 정책분석, 정책생성으로 구분하여 정책을 관리한다. 법률관리를 통해서 개인정보보호법을 수집하고 정책분석은 수집된 정보보호 법규 항목을 기반으로 정의된 원칙과 목적에 의거하여 분석을 수행한다. 관리화면에는 개인정보 생명주기 단계로 구분하여 관련 법규항목을 업데이트할 수 있다. 정책생성은 개인정보 이용주기, 목적, 조건 등 분석된 정책 기반으로 정보보호 정책 기술문서를 생성하는 단계이다. 정책 기술문서

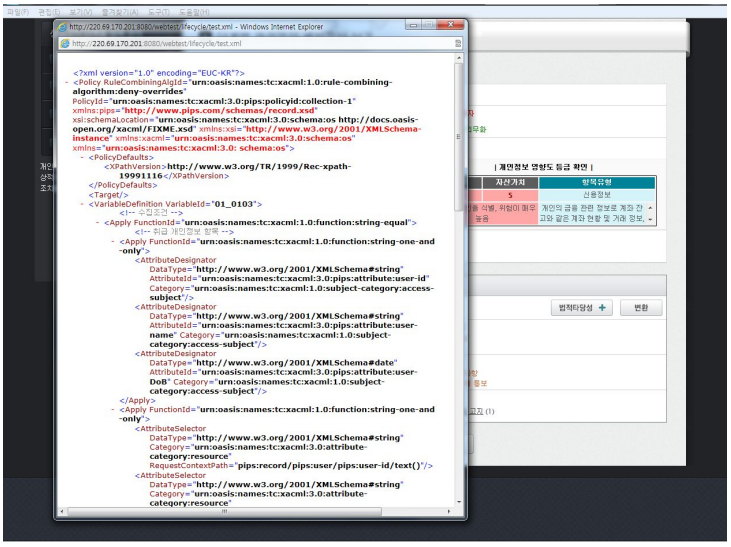
는 시스템 정책을 기술하고 사용자가 이용할 수 있는 규약을 정의하여 표현한다.



<그림 31> 정책관리 리스트 및 관련조항 설명 화면



<그림 32> 정책관리 세부보기와 법적근거성 화면



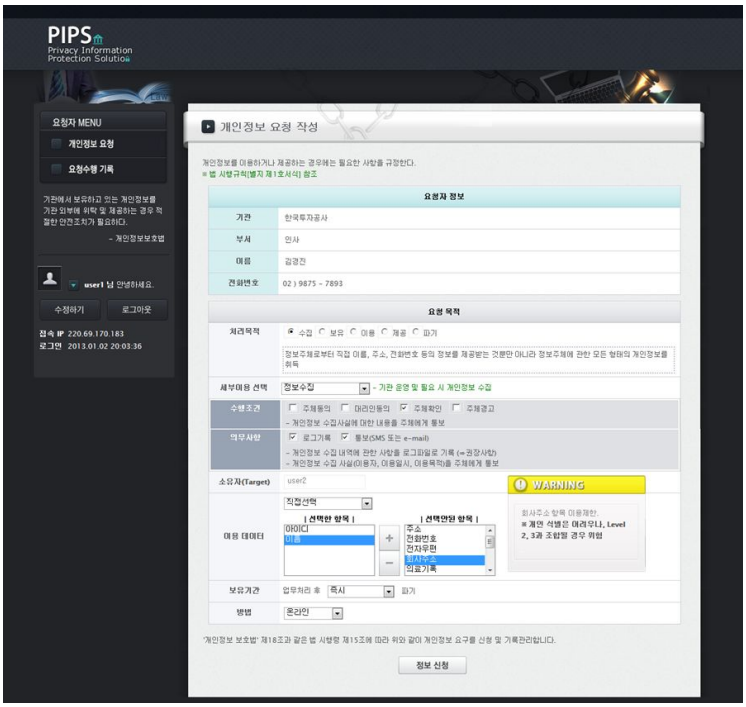
<그림 33> 정책을 XACML로 변환 화면

4) 접근제어 화면

사용자는 개인정보를 이용하기 위해 요청자 화면을 통해서 개인정보 접근을 요청한다. <그림 34>를 보면 개인정보를 요청하는 사용자에 대한 정보는 상단에 위치하고 아이디와 이름 등 요청자의 간단한 신상정보를 보여준다.

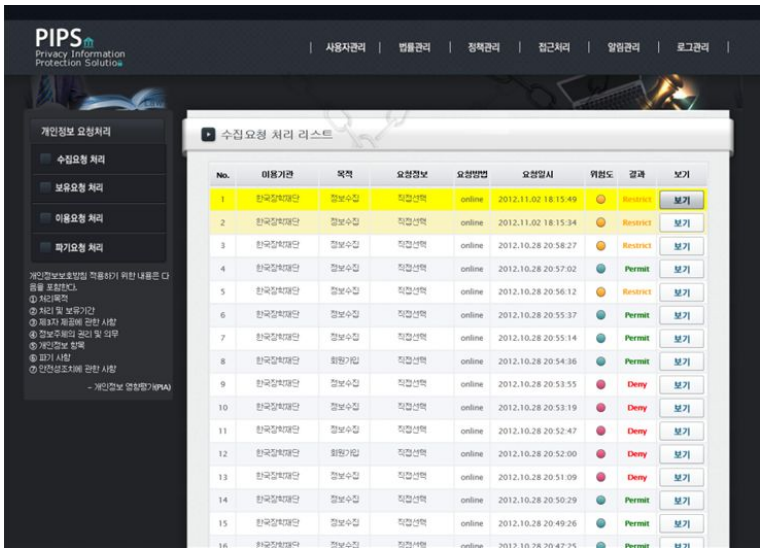
하단에는 접근 요청하려는 정보를 목적에 맞게 선택하고 요청하도록 한다. 처리목적으로써 수집부터 파기까지 어떤 목적으로 사용할 것인지에 대해 선택하면 이에 맞춰 세부 이용목적 변경된다. 세부 이용목적에 따라 반드시 필요한 조건 및 의무사항을 자동적으로 선택되며 요청자는 이를 확인할 수 있다. 접근하고자 하는 데이터에 대해 기본적으로 제공되는 그룹을 선택할 수도 있지만 데이터 항목을 요청자가 직접 선택할 수도 있다. 여기서 선택된 항목에 대해 접근가능한지를 알 수 있도록 간단한 설명을 나타낸다. 요청정보를 모두 입력하였다며 정보신청으로써 접근을 요청할 수 있

다. 이 때 XACML 문서로써 전송된다.



<그림 34> 개인정보 요청신청 화면

접근처리는 <그림 35>와 같이 요청한 리스트 화면을 보여준다.



<그림 35> 접근제어 화면

관리자에 의해 정보를 요청한 사용자의 접근권한을 변경할 수 있다. 접근제어의 첫 화면은 접근제어 요청사항 리스트로써, 관리자가 확인하지 않은 사항은 체크표시로 새롭게 들어온 요청임을 표현한다. 요청 사항을 자세히 보여주는 창은 아래 그림과 같다.

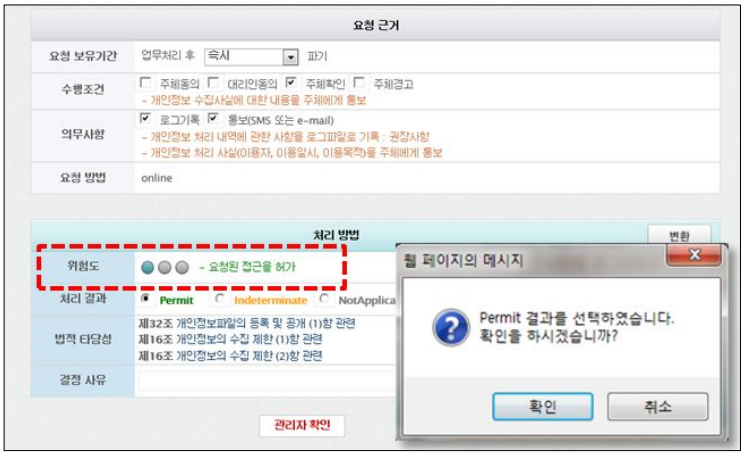
<그림 36> 접근제어 상세정보 화면

① 요청자 세부정보 : 개인정보를 요청하는 사람의 ID, 인증번호, 이름, 역할을 나타낸다.

② 요청 목적 및 일시 : 개인정보 소유자의 ID와 함께 요청자가 개인정보를 요청한 목적, 일시, 요청방법, 요청한 개인정보 항목, 개인정보의 민감도 등을 나타낸다.

③ 요청근거 / 처리방법 : 요청한 정보의 보유기간과 함께 접근제어 정보를 포함하고 있어 요청 목적에 따른 수행조건(Condition), 의무사항(Obligations)을 알 수 있다. 해당 접근요청의 위험도를 나타내고 처리에 대한 법적 근거성을 확인할 수 있다.

상세정보를 확인한 후, 개인정보를 요청하는 이의 역할과 목적에 따라 허용된 범위 이외의 개인정보를 요청하는 경우 관리자의 확인이 필요하다. 우선적으로 시스템에 정의된 정책에 맞춰 처리 결과가 선택되어진다. 요청한 정보가 민감하거나 중요도가 높은 정보인 경우 관리자 검증을 통해서 정보주체에게 이메일이나 모바일을 이용하여 요청 사항에 대해 안내를 한 후 동의여부의 결과에 따라 접근처리를 수행한다.



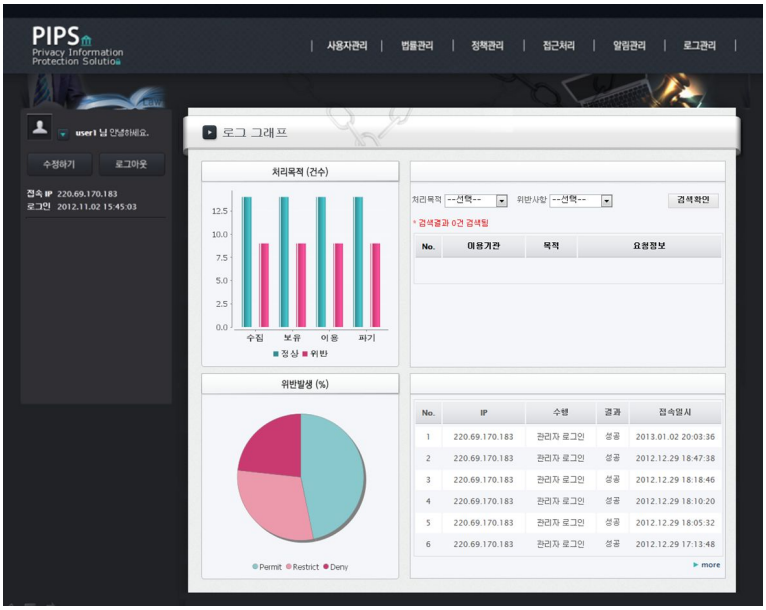
<그림 37> 접근제어 화면에서 관리자 확인

5) 로그관리 화면

개인정보 처리내역 기록관리는 개인정보 안전조치 의무의 기술적 보호방법으로 권장하고 있다. 본 연구의 로그관리는 수집이나 이용, 제공 등의 이벤트에 대해서 로그를 기록한다. <그림 38>에서 개인정보 이용현황을 통계 그래프로 나타내며, 이는 개인정보 생명주기 단계별로 정상처리와 위반사항

을 확인할 수 있도록 하고 전체 개인정보 처리에 대해 위반발생을 (%)로 확인할 수 있다. 즉, 사고발생 및 침해사고 시에는 주체에게 유출사실을 통보할 수 있도록 하고, 개인정보 처리내역의 기록으로 권한을 벗어나거나 과도하게 많은 개인정보를 조회하는 자를 분석하여 그래프로 나타낸다.

또한 개인정보 처리내역에 관한 사항은 로그파일로 기록되어 처리내역에 대해 처리주체, 처리일시, 처리목적, 처리결과 등에 대해 로그를 기록 및 보관하여 표시된다. 이러한 기록은 상세보기를 통해 더 세부적인 정보 및 이용기록에 대한 확인할 수 있다.



<그림 38> 로그관리 화면

Ⅷ. 보안성 분석 및 성능평가

1. 보안성 비교분석

개인정보보호법에 따라 개인정보의 법적 준거성 확보를 위해 최소한의 요구사항인 개인정보의 안전성 확보조치 기준을 만족해야 한다. 이를 위해서는 기술적·관리적 보호조치 등의 세부기준이 검토되어야 한다. 이는 개인정보의 안전성 확보조치 기준에 제시되어 있으며, 본 논문에서는 이러한 기준 기반으로 보안성을 검토한다.

[개인정보의 안전성 확보조치 기준]

- ✓ 내부관리계획의 수립·시행
- ✓ 접근 권한의 관리
- ✓ 비밀번호 관리
- ✓ 접근통제 시스템 설치 및 운영
- ✓ 개인정보의 암호화
- ✓ 접속기록의 보관 및 위/변조 방지
- ✓ 보안프로그램 설치 및 운영
- ✓ 물리적 접근방지

위와 같이 개인정보 처리자가 개인정보를 처리함에 있어서 개인정보를 분실·도난·유출·변조·훼손되지 아니하도록 안전성을 확보하기 위해서 제시하는 기준은 내부관리계획의 수립·시행, 접근 권한의 관리, 비밀번호 관리, 접근통제 시스템 설치 및 운영, 개인정보의 암호화, 접속기록의 보관 및 위·변조 방지, 보안프로그램 설치 및 운영, 물리적 접근방지의 이행을 필요로 하고 있다.[8,10] 하지만 앞에서 설명한 바와 같이 개인정보 보호법은 발효된 시기는 최근이며 현재 이를 준수할 수 있는 기술연구는 추진 중으로 아직 대안은 부족하다. 제안한 모델은 개인정보보호 관련 법규를 준수하는 정책기반으로 안전한 개인정보 사용 및 관리의 방안으로 신뢰할 수 있는

접근제어 모델을 제안하였다. 즉 보안성의 정성적 평가를 통해 본 절에서 제안한 모델의 개인정보에 대해 안전성 확보가 되는지를 다른 연구와 비교한다.

본 논문에서는 법 준수하는 보안성이 얼마나 효율적이고 안전한 관리를 하는지 설명하고자 한다. 여기에서는 개인정보를 처리하는 시스템에 대한 제안이므로 관리계획 및 물리적인 측면을 제외한 시스템적인 측면에서만 보안성을 살펴보고자 한다. 보안성은 안전성이 확보된 방법을 사용하고 있는지, 접근통제가 적절하게 이루어지고 있는지 등을 검토한다.

보안성 기준으로 접근 권한의 관리는 시스템이 업무 목적 외 불필요한 접근을 최소화하고 사용자의 이동 및 역할 변경 시 인가되지 않는 접근을 차단하는데 있다. 이를 위해 업무나 책임의 권한은 차등 부여되어야 하며 변경이 발생되면 지체없이 권한을 수정할 수 있도록 관리되어야 한다. 역할 기반 접근제어를 실 환경에 적용할 시 직책, 부서 및 인사이동에 대해서는 역할로 구분되며 업무 범위별 권한에 대해서는 역할 권한 할당으로 차등 부여될 수 있도록 한다.

비밀번호 관리도 안전성 확보조치에 중요하다. 안전한 비밀번호는 제3자가 쉽게 추측할 수 없으며 해킹을 통해서도 알아낼 수 없거나 알아내는데도 많은 시간이 요구되는 것을 의미한다. 즉, 추측하기 쉬운 숫자나 문자 등을 비밀번호로 이용되지 않도록 설정, 비밀번호는 암호화하여 저장 등의 방식으로 시스템을 구성하는 것이 필요하다.

접근통제 시스템에서는 불법적인 접근 및 침해사고 방지를 위해 비인가자의 접근을 차단할 수 있도록 한다. 기본적으로 침입 차단 프로그램을 사용하여 불법적인 접근을 차단하는 방식을 제공한다.

개인정보의 암호화는 비밀번호, 바이오정보, 주민등록번호 등과 같은 주요 개인정보가 암호화하지 않고 시스템에 저장되거나 네트워크를 통해 전송될 경우, 불법적인 노출 및 위·변조 등의 위험이 있으므로 암호화 등의

안전한 보호조치가 제공되어야 한다. 특히나 법 시행 이후 주민등록번호 등 식별정보를 포함하는 시스템을 구축하는 경우, 암호화를 즉시 이행하여야 한다.

접속기록은 개인정보의 저장 및 수정사항, 데이터 접근내역 등을 자동으로 기록하는 로그 파일을 생성하여 최소 6개월 이상 안전하게 보관·관리하여야 한다.

이러한 보안성 기준을 기반으로 다른 연구들이 제안한 접근제어 모델의 기능을 비교하고 차이점을 살펴본다. 정책기반 접근제어 모델에 대한 연구는 정보화 사회의 발전으로 개인정보의 수집 및 활용이 용이해지면서, 개인정보보호에 관한 기술 및 연구가 활발히 진행 중이다. 이는 3장에서 선행연구에 대한 소개와 함께 분석사항을 기술하였으며, 본 절에서는 이를 기반으로 P-RBAC[40,41], IPP-RBAC[43], ITEPP[36], 그리고 프라이버시 관리 프레임워크(Personalized privacy policy management framework)[23]의 연구를 비교·분석한다. 아래 표는 보안성 비교에 사용된 5개의 접근제어 모델의 목적과 설계방안, 정책 적용기법에 관하여 정리한 것이다.

<표 12> 선행연구의 연구 비교

	P-RBAC [40, 41]	IPP-RBAC [43]	ITEPP [36]	Jianning Geng [23]	제안
연구 목적	RBAC 확장형 모델을 통해 프라이버시 지원	RBAC 기반 통합형 프라이버시 지원	HIPAA를 준수하는 프라이버시 보호	프라이버시 정책을 표현하는 프레임워크	규제 기반의 접근제어로 안전한 개인정보관리
설계 방안	OECD 원칙, 프라이버시 규정을 정책 표현	RBAC 기반 기존 모델 통합, 구성요소 자동 관리	접근 및 기록방안 등 접근제어	표준기술을 이용하여 프라이버시 규제표현	법규 및 표준기술을 이용한 자동 접근제어
정책 적용 기법	LC_0으로 접근제어 정책표현	표준기술 준수하는 XML 정책	표준기술 준수하는 XML 정책	표준기술 준수하는 XML 정책	XACML 정책 언어

역할기반 접근제어 확장형 모델(Privacy-aware RBAC)은 OECD에서 제시한 원칙 및 프라이버시 규정을 기반으로 프라이버시 접근통제 모델을 제시하는 것이 목적으로써 요구사항에 맞게 정책표현을 명확히 하고 권한확인 및 의무수행을 한다. RBAC에 기초한 통합형 프라이버시 보호 모델(IPP-RBAC)의 경우에는 포괄적인 프레임워크로 RBAC의 구성요소가 자동으로 관리할 수 있도록 하며 XML기반의 정책을 표현하고 있다. HIPAA를 준수하는 ITEPP(IT-enforceable privacy policy) 모델을 제시하여 개인정보를 소유하고 있는 환자의 프라이버시를 보호하기 위해 시스템에 적용할 수 있는 강화된 정책을 제공하고 있다. 프라이버시 정책을 표현할 수 있는 프라이버시 관리 프레임워크는 정책을 명시뿐만 아니라, 사용자의 가독성을 위해 표준기술을 이용하여 제시하고 있으며, 또한 시스템에 적용할 수 있도록 명시적으로 표현하고 있다. 제안하는 모델의 경우에는 규제 기반의 접근제어로 안전한 개인정보 관리를 할 수 있도록 모델을 제시하여 접근통제가 가능하도록 하며 XACML을 이용하여 시스템적으로 정책을 명시할 수 있는 연구를 하였다. 각 모델의 보안성 기준으로 <표 13>과 같이 분석하였다.

관련 선행연구와 비교 분석해 보면, 기본적으로 암호화나 사용자 인증 기술이 제공되며 네트워크 환경에서 정책기반으로 개인정보를 보호할 수 있도록 설계하였다. 그러나 제시한 정책 제도가 구조화는 되어있으나, 명확한 보안정책 표현에 대해서는 제한적이여서 기관 및 조직 내 실제 적용 가능성에는 문제가 있다. 법적인 규제 적용을 위한 처리내역의 접속기록 역시 구체적인 적용방안에 대한 안전성 확보조치가 부족하다.

본 연구에서 구현방안으로 제시한 시스템은 국내 법제도 기반의 개인정보보호 원칙을 이용하여 정책을 설계하였다. 정책표현에 있어 접근제어 기술인 XACML을 제공함으로써 이후 확장 및 다른 기술과의 연동이 용이하고 알림 기능을 이용하여 개인의 권리를 보호한다. 또한 정책관리에 인터페이스를 제공하여 관리자가 정책을 수정 가능하도록 방안을 제시하였다.

<표 13> 선행연구의 보안성 분석 비교

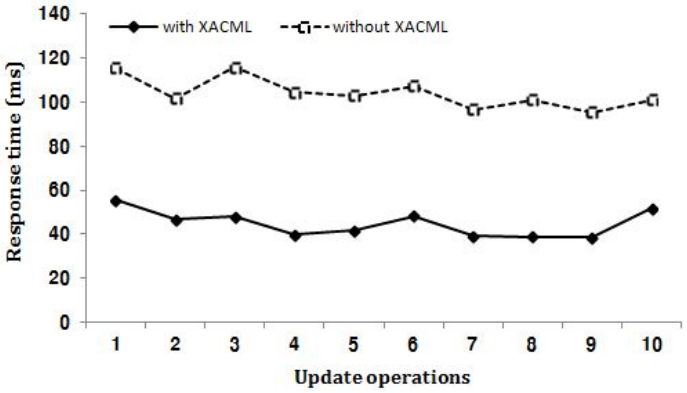
	P-RBAC [40, 41]	IPP-RBAC [43]	ITEPP [36]	Jianning Geng [23]	제안
접근권한 관리	역할권한 차등 부여	역할권한 차등 부여	역할권한 차등 부여	역할할당	역할권한 차등 부여
비밀번호 관리	비밀번호 암호화 저장,	-	-	비밀번호 규칙 적용	비밀번호 암호화 저장, 규칙 시스템 적용
접근통제 시스템 설치·운영	비인가 접근통제, 정보 범위구분, OECD기반 통제	비인가 접근통제, 정보 보안등급, OECD기반 통제	비인가 접근통제, 법규기반 통제	비인가 접근차단, 법규기반 통제	비인가 접근차단, 정보 보안등급, 법규기반 통제
개인정보 암호화	암호화 기술 적용하지만 범위언급 없음	식별정보 암호화	암호화 기술 적용하지만 범위언급 없음	-	식별정보 암호화
접속기록 및 위·변조 방지	처리내역 기록	추가기능 가능	추가기능 가능	정책에만 명시	처리내역 기록, 사고발생 탐지

2. 처리성능 실험평가

본 연구의 실 적용을 위한 시스템 개발 기반으로 보안에 관련된 기능적인 측면을 평가하고자 시뮬레이션을 수행하였다. 시스템 서버는 Intel Pentium 2GHz 256 DDR RAM의 컴퓨터 상에서 구현된 것으로, 개발도구는 이클립스를 사용하였으며, 프로그램 개발을 위해 운영체제 Window7에 Java 1.6 JDK가 사용되어 서버 프로그램이 실행되었다. 서버 프로그램을 Tomcat으로 실행하게 되면 앞서 프로토타입에서 보여진 것처럼 사용자가 시스템에 접속할 수 있다. 사용자는 이 화면을 통해 개인정보의 주체, 목적, 조건 등을 선택하여 시스템에 요청할 수 있다. 시스템에서는 자동으로 선택된 내용이 XACML로 전송되며, 이를 파싱 및 분석하여 시스템에 보여주게 된다. 본 절에서는 시뮬레이션을 통해 연구의 목적과 유사한 개인정보보호 접근제어를 수행하는 기존 구현 시스템과 비교하여 주요 기능을 중점으로 성능을 실험하였다.

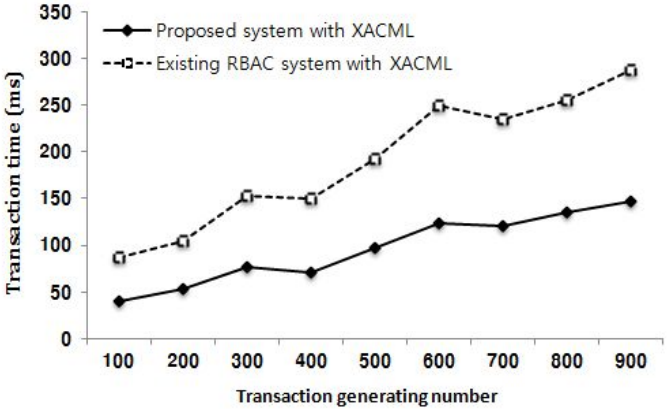
정책관리의 처리 성능의 비교분석은 다음과 같다. 제안한 모델은 사용자가 요청한 정보와 결과 처리를 위한 응답정보, 그리고 개인정보보호 규칙을 정의한 정책을 XACML로 표현하여 시스템적으로 변수 및 값을 매칭 하는데 이용한다. 이러한 처리 방안은 XML 기반의 XACML이라는 언어를 이용함으로써 개인정보 항목의 중요도에 따라 필요한 수행조건과 의무사항을 단계적으로 검사한다.

<그림 39>는 XACML 언어를 이용하여 보안정책을 적용했을 때와 적용되지 않았을 때의 성능차이를 비교하였다. 그래프는 처리 방안에 대한 인터페이스와 제공되는 정책, 프로세스가 유사한 상태에서 수행된 것으로 기존의 처리방법보다 XACML을 적용하는 것이 접근 처리의 시간이 빠르다는 것을 알 수 있으며 이는 정책을 매핑하거나 검색하는데 시간을 단축시킨다.



<그림 39> XACML 적용 처리 비교

아래는 접근제어 관련한 비교분석으로써, 제안한 모델은 기존 역할기반 접근제어(RBAC)에 프라이버시를 확장하여 사용자를 역할에 할당하고, 역할 권한이 접근요청에 적합한지 판단하여 접근통제를 하는 것이다. 이러한 프로세스는 RBAC에서 필요없는 XACML의 요소는 제외하고 필수 구성요소만 포함하여 수행할 수 있도록 한다. 즉, 불필요한 요소의 포함은 수행 및 검색이 비효율적이며 무의미한 설정이나 행위를 유발시킬 수 있다. 따라서 본 제안은 필요한 연산만 할 수 있는 구성요소를 포함한다. 아래 그래프는 RBAC을 XACML로 표현하여 수행한 기존 연구와 제안 연구를 비교하였다.



<그림 40> RBAC의 처리 비교

이는 역할기반을 확장하여 제안한 접근제어 모델의 유연성과 확장성 기반하여, 보안정책을 적용함에 있어서도 XML 기반의 기술을 이용함으로써, 접근처리에 시간을 단축시킨다. 결과적으로 본 연구는 기존의 연구들에 비해 안전한 보안기능을 만족시키면서 접근처리 시간은 빠르다는 것을 알 수 있다. 따라서 본 논문에서 구현한 시스템은 향후 성능이 좋은 것으로 평가되며 개인정보를 다루는 많은 분야에 적용 가능하리라 예상된다.

Ⅷ. 결론 및 향후연구

1. 연구의 의의 및 기대효과

정보통신기술의 발전으로 개인정보의 오남용 및 유출 등 역기능 피해가 지속적으로 증가하면서, 정보화 사회에 대한 사람들의 우려가 가증되고 있다. 이에 개인정보보호 법제도적인 측면에서는 개인의 권리를 존중하며 꼭 필요한 최소정보만을 이용 및 제공해야한다고 요구하고 있지만, 필요시 또는 악의적 목적으로 개인정보의 오남용 및 유출 등 사고 발생의 우려와 개인정보의 산발적인 관리 체계 및 관리자 책임성에 대한 문제가 대두되고 있다.

본 연구에서는 웹 환경에서 서비스를 이용하기 위해 사용자 자신의 개인정보를 제공하고 기관 및 서비스 업자 등의 서비스 제공자는 개인정보보호 관련 법규 및 정책을 준수할 수 있는 보호 하에 개인정보를 이용할 수 있도록 한다. 더욱이, 본 논문에서는 개인정보의 수집 및 이용, 제공 등 정책에 준한 체계적인 개인정보 처리를 가능하게 하여 개인정보를 안전하게 보호 및 관리해줄 수 있는 시스템 구축 방안을 확립하는 것에 의의를 두고 있다.

이를 위해 사전에 개인정보보호의 법·제도 동향에 대해 살펴보고, 프라이버시를 위한 관련 표준화 기술인 XACML과 역할기반 접근제어(RBAC)에 대해서 알아보았으며, 프라이버시 관련 프로젝트뿐만 아니라 학술적 연구들에 대해 조사 분석하였다. 이를 기반으로 웹 환경 내 개인정보의 이슈를 다각적으로 분석하여 문제점을 도출하고 이를 보완할 수 있는 사항을 고려하여 안전한 개인정보 사용 및 관리 방안으로써 신뢰할 수 있는 접근제어 모델을 제안하였다. 개인정보보호 관련 법률을 기반으로 개인정보를 신뢰적이고 효율적으로 접근 통제할 수 있는 기능을 적용하여 무분별한 개인정보

수집 및 활용을 예방하고, 인터넷 이용자들은 프라이버시를 보호 받을 수 있도록 한다. 또한, 접근제어 기술인 XACML을 이용하여 확장성 및 상이한 그룹 간의 연동성을 제공하며, 주기적인 정보 교류 시 실시간 감시, 개인정보 사용 관리 기능과 로그 분석, 패턴 분석, 리포트 기능 등의 기술로 규정 위반 시 법적 근거를 제시하도록 하고 책임추적성을 제공한다. 구현방안을 통해 관리자와 사용자에게 시스템 인터페이스를 제공하여 정책 및 정보관리에 유연하게 대처할 수 있는 대안을 제시한다.

본 연구에서는 개인정보의 요청은 개인정보의 중요도와 개인정보를 요구하는 서비스의 보안등급에 따라 유동적으로 개인정보 항목에 대해 접근 결정이 되므로, 개인정보 오·남용에 대해 보다 유연하게 대응할 수 있을 것이다. 또한 개인정보보호 관련 법률에 기반을 둔 정책설정, 정책에 준한 개인정보 검증 및 통제, 개인정보 제공에 대한 처리사실을 실시간 통지 등의 보안 기능을 수행하여 더욱 안전한 개인정보 보호 기능이 강화될 것이다. 아울러 본 논문에서 제시하는 시스템 구현 방안을 통해 개인정보를 안전하게 보호 및 관리해주고 개인 사용자뿐만 아니라, 공공·민간 등 관련 기관의 개인정보보호에 대하여 체계적인 보안정책과 함께 신뢰할 수 있는 서비스로 응용방안 연구가 될 것으로 기대된다.

2. 향후연구 방향

본 연구를 통해서 개인정보의 제공 사실을 사용자에게 통지하고 개인정보를 이용하는 요청자를 기록함으로써 개인정보가 이용되는 경로를 명확하게 파악하여 개인정보 오·남용을 방지할 수 있다. 그러나 접근 권한을 부여받은 허가자, 내부자 등에 의해 개인정보 유·노출을 차단하는데 기술의 제한이 있다. 이를 위해 본 논문에서는 민감 정보에 대해서는 암호화로써 처리하였으며, 모든 처리내역을 기록하여 요청자 및 관리자에게 책임추적성을 제공하고, 사용자 동의 및 통지 기능을 통해 개인정보 오남용에 대해 즉시 조치를 취할 수 있도록 하는 예방차원의 제한적인 대안을 제공하고 있다. 이는 향후 본 논문에서 제안하는 모델의 실제 적용의 더욱 보안성이 높고 효율적인 결과를 위해서는 사고발생 후의 대안기술 마련의 추가 연구가 필요할 것으로 보인다.

또한, 데이터적인 개인정보 뿐만이 아니라, 개인이 보유하고 있는 콘텐츠 등 성장하고 있는 정보화 시대에 맞춰 확장된 개인정보의 보호를 위해 다양한 모니터링 기술 및 로그기술 등 디지털 포렌식과 관련된 정보보호 솔루션과 연동하여 향후 발생할 수 있는 정보 도용에 대해 법적 근거 기반을 확보하는 인프라를 구현할 수 있도록 하여 개인정보를 더욱 강화할 수 있는 연구가 필요하다.

아울러 본 논문에서 살펴보았듯이 최근 개인정보보호법의 제정으로써 법적 근거에 맞춰 개인정보 침해 및 사고를 대응하기 위한 연구가 추진되거나 진행 중으로써, 실제 솔루션이나 기존 연구에 대해 각 기능적인 면에서는 비교하였으나, 전반적인 면에서는 실질적인 효과를 분석하지 못하고 자료를 토대로 하여 성능 및 효과를 분석해보았다. 따라서 향후 다양한 기술들이 지속적으로 연구되고, 이를 기반으로 비교하면 보안성 및 성능 부분에서의 결과를 명확히 알 수 있을 것이다. 더욱이 본 연구는 개인정보보호법

및 규정을 준수할 수 있는 기술을 제공하는 선례 연구로 실 환경의 적용 기술을 위한 확장 및 개인정보 안전성을 확보하는 기술로 국내외 연구 개발의 참고가 될 수 있도록 하며, 향후 실제 IT 환경 내 아키텍처 적용 가능한 연구로 소프트웨어 개발자나 운영자 입장에서 도움이 되는 응용 연구가 될 것으로 사료된다.

참고 문헌

[1] 인터넷침해대응지원센터, “개인정보침해신고 상담건수”, 2012.

[2] 오현식, “개인정보보호법, 정보보안 시장 성장‘가속페달’”, NETWORK TIMES, Vol.1, 2011, pp.168-173.

[3] 한국인터넷진흥원, “2011 국가정보보호백서”, 2012, pp.116-118.

[4] 차건상, 한호현, 신용태, “개인정보보호법의 자율규제 확보를 위한 효과적인 개인정보관리체계 인증제”, 정보과학회논문지 제39권 제3호, 2012.

[5] 진성철, 김인경, “인터넷 이용자의 개인정보 유출 가능성에 대한 심리적 불안에 관한 연구”, 한국전자통신학회논문지 제6권 제5호, 2011.

[6] 개인정보보호위원회, “2012 개인정보보호 연차보고서”, 2012.

[7] 홍승필, “개인정보보호 개론”, 한티미디어, 2009.

[8] 윤종수, “개인정보보호법제의 개관”, 정보법학 제13권 제1호, 2009, pp.179-209.

[9] 정보화전략실 개인정보보호과, “개인정보 보호법의 주요내용”, 행정안전부, 2011.

[10] 대한민국국회,“개인정보 보호법”, 법률 제10465호, 2011.

[11] 홍승필, “개인정보보호 프레임워크 개발”, 한국인터넷진흥원, 2009.

[12] 임종인, “주요 국가의 개인정보보호 동향 조사”, 한국인터넷진흥원, 2009.

[13] 남기효, 박상중, 강형석, 남기환, 김성인, “개인정보보호기술의 최신 동향과 향후 전망”, 정보보호학회지 제18권 제6호, 2008, pp.11-19.

[14] 신용녀, 김학일, 전명근, “개인정보보호 참조 아키텍처와 국제표준화 동향”, 정보보호학회지 제21권 제5호, 2011, pp.12-20.

[15] 김운석, "개인정보보호 2.0시대의 개인정보보호법 개관", 法學硏究 제22권 제2호, 2011, pp.9-42.

[16] 장현미, 김경진, 김혜리, 정지희, 홍승필, "인터넷 환경 내 개인정보 보호 아키텍처 설계 방안", Entrue Journal of Information Technology Vol.8 No.1, 2009.

[17] 손태경, "안전한 개인정보 보호 방안 연구", 숭실대학교 정보과학 대학원 학위논문, 2011.

[18] 이기혁, "국내 통신 사업자의 개인정보 생명주기 분석을 통한 유출 방지 시스템", 건국대학교 대학원 벤처전문기술학과 학위논문, 2010.

[19] Qun Ni, Alberto Trombetta, Elisa Bertino, and Jorge Lobo, "Privacy management: Privacy-aware role based access control", Proceedings of the 12th ACM Symposium on Access Control Models And Technologies (SACMAT) '07, 2007, pp.41-50.

[20] Organization for the Advancement of Structured Information Standards, "OASIS: Extensible access control markup language(XACML) V3.0. OASIS Specification", Available at http://www.oasis-open.org/committees/xacml, 2012.

[21] Goran Sladi´c, Branko Milosavljevi´c, Zora Konjovi´c, and Milan Vidakovi´c, "Access Control Framework for XML Document Collections", Computer Science and Information Systems (ComSIS), Vol.3 No.8, 2011, pp.591-609.

[22] Diala Abi Haidar, Nora Cuppens-Boulahia, Frederic Cuppens, and Herve Debar, "An Extended RBAC Profile of XACML", Proceedings of Symposium on Web Society (SWS)'06, 2006.

[23] Jianning Geng, Lin Liu, and Barrett R. Bryant, "Towards a Personalized Privacy Management Framework", Proceedings of

SESS'10, 2010.

[24] Gail-Joon Ahn, Hongxin Hu, and Jing Jin, "Security-Enhanced OSGi Service Environments", IEEE Transactions on Systems, Man, and Cybernetics, Vol.39 No.5, 2009, pp.562-571.

[25] ANSI/INCITS 359-2004, "Information Technology-Role Based Access Control", International Committee for Information Technology Standards, 2004.

[26] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein and, Charles E. Youman, "Role-based access control models", IEEE Computer, Vol.29 No.2, 1996, pp.38 - 47.

[27] 방송통신위원회, "개인정보보호 관리 체계(PIMS)", 방송통신표준 KCS.KO-12.0001, 2011.

[28] Jan Camenisch, Marit Hansen, "PrimeLife's Legacy", Privacy and Identity Management for Life, 2011, pp.505-506.

[29] PISA Project. "Handbook of Privacy and Privacy-Enhancing Technologies", Available at http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf, 2003.

[30] 노종혁, 진승헌, "웹 환경에서 정책 기반 개인정보보호 기술", 전자통신동향분석 제22권 제4호, 2007, pp.144-155.

[31] Organization for Economic Co-operation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", Available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, 1980.

[32] L. Dai and K. Cooper, "Helping to meet the security needs of enterprises: Using FDAF to build RBAC into software architectures", Proceedings of the 5th International Conference on Software

Engineering Research and Practice, 2006, pp.790-796.

[33] Gail-Joon Ahn and Hongxin Hu, "Towards Realizing a Formal RBAC Model in Real Systems", Proceedings of Symposium on Access Control Models And Technologies (SACMAT)'07, 2007.

[34] Hongxin Hu and GailJoon Ahn, "Enabling Verification and Conformance Testing for Access Control Model", Proceedings of Symposium on Access Control Models And Technologies (SACMAT)'08, Estes Park, 2008.

[35] Isabel F. Cruz, Rigel Gjomemo, Benjamin Lin, and Mirko Orsini, "A Location Aware Role and Attribute Based Access Control System", Proceedings of SIGSPATIAL International Conference on Advances in Geographic Information Systems(ACM GIS)'08 , 2008.

[36] Ahmed AL Faresi, Duminda Wijesekera, and Khaled Moidu, "A comprehensive privacy-aware authorization framework Founded on HIPAA Privacy Rules", Proceedings of SIGHIT International Health Informatics (IHI) Symposium'10, 2010, pp.637-646.

[37] 조영섭, 진승헌, "Digital Identity 관리 기술 현황 및 전망", 전자통신동향분석 제22권 제1호, 2007.

[38] Hyang-Chang Choi, "A Study on Access Control based on the Policy for Privacy Protection in the Social Media Environment", Internet and Information Security, Vol.1 No.2, 2011, pp.46-70.

[39] Hong S.-P., Kim K.-J., Kang S.-M. and Kim J.-H., "Development of Framework for Privacy Information Protection - Case Study and Issue in Korea -", INFORMATION, vol.13, 2010, pp.604-620.

[40] Qun Ni, Elisa Bertino, Jorge Lobo, Carolyn Brodie, Clare-Marie Karat, John Karat, and Alberto Trombetta, "Privacy-aware role-based

access control", ACM Transactions on Information and System Security (TISSEC), Vol.13, No.3, 2010.

[41] Qun Ni, Elisa Bertino, Jorge Lobo, and Seraphin B. Calo, "Privacy-Aware Role-Based Access Control", IEEE Security & Privacy (IEEESP), Vol.7, No.4, 2009, pp.35-43.

[42] 엄정호, 박선호, 정태명, "유비쿼터스 컴퓨팅 환경을 위한 보안통제가 강화된 접근제어 시스템 설계에 관한 연구", 정보보호학회논문지 제18권 제5호, 2008, pp.71-81.

[43] 조혁현, 박희만, 이영록, 노봉남, 이형효, "RBAC에 기초한 통합형 프라이버시 보호 모델", 정보보호학회논문지 제20권 제4호, 2010, pp.135-144.

[44] Schneier. B., "A taxonomy of social networking data", IEEE Security & Privacy, Vol.4, No.8, 2010.

[45] Hongxin Hu, Gail-Joon Ahn, "Constructing Authorization Systems Using Assurance Management Framework", IEEE Transactions on Systems, Man, and Cybernetics, Vol.40, No.4, 2010, pp.396-405.

[46] Karsten Sohr, Michael Drouineaud, Gail-Joon Ahn, and Martin Gogolla, "Analyzing and Managing Role-Based Access Control Policies", IEEE Transactions on Knowledge and Data Engineering (TKDE), Vol.20, No.7, 2008, pp.924-939.

[47] Seng-Phil Hong, Gail-Joon Ahn, and Wenjuan Xu, "Access Control Management for SCADA Systems", IEICE Transactions (IEICET), Vol.91-D, No.10, 2008, pp.2449-2457.

[48] 전은정, 김학범, 염흥열, "미국의 개인정보보호 법·제도 동향", 정보보호학회지 제22권 제1호, 2012, pp.47-57.

[49] Hongxin Hu, "Assurance Management Framework for Access

Control Systems", Computer Science and Engineering, Arizona State University, 2012.

[50] 김승현, 진승헌, "개인정보 수집 기술 및 대응방안", 전자통신동향분석 제27권 제4호, 2012.

[51] Gail-Joon Ahn, Mohamed Shehab, and Anna Cinzia Squicciarini, "Security and Privacy in Social Networks", IEEE Internet Computing (INTERNET), Vol.15 No.3, 2011, pp.10-12.

[52] 한국정보통신기술협회, "개인정보 생명주기별 보안 관리모델", 정보통신단체표준 TTAS.KO-12.0053, 2007.

[53] Elisa Bertino, Carolyn Brodie, Seraphin B. Calo, Lorrie Faith Cranor, Clare-Marie Karat, John Karat, Ninghui Li, Dan Lin, Jorge Lobo, Qun Ni, Prathima Rao, and Xiping Wang, "Analysis of privacy and security policies", IBM Journal of Research and Development (IBMRD), Vol.53 No.2, 2009.

[54] 김지현, 고현국, "개인정보, 국민 1인당 2번이상 털려 … 5년간 1억 2700만명분 유출", 동아일보, 2011.

[55] Kyong-jin Kim, Seng-phil Hong, and Joon Young Kim, "A Study on Policy-based Access Control Model in SNS", IJMUE, Vol.7 No.3, 2012.

[56] A.Rezqui, A. Bouguettaya, and M.Y. Eltoweissy, "Privacy on the Web: Facts, Challenges, and Solutions", IEEE Security & Privacy, Vol.1, 2003.

[57] W3C, "The Platform for Privacy Preferences 1.1 (P3P 1.1) Specification", 2006.

[58] Boontawee Suntisrivaraporn, Assadarat Khurat, "Formalizing and Reasoning with P3P Policies Using a Semantic Web Ontology",

Multi-disciplinary Trends in Artificial Intelligence, Lecture Notes in Computer Science, Vol.7080, 2011, pp 87-99.

[59] 이원태, 유지연, 박현유, 김위근, "방통융합 환경에서 정보의 자유와 개인의 프라이버시 보호방안 연구", 정보통신정책연구원, 2010.

[60] 채승완, 민경식, 황성원, 원순재, "개인정보의 경제적 가치 분석에 관한 고찰", 한국정보보호진흥원, 2007.

ABSTRACT

A Study on Trusted Model for Privacy Information Protection based on Access Control

Kim, Kyong-Jin
Dept. of Computer Science
The graduate school
Sungshin Women's University

With the spread of new web environments such as cloud and social network, usage of personal data has increased sharply. In addition, new technologies are collecting more personal data than ever before. And with personal data usage increasing, concerns about the easy access to personal information have also risen. The latest report on the number of privacy breaches(2012) suggests that it accounted for about 123 percent increased from the previous year. According to these records, personal data can be accessed and may be disclosed even without the knowledge of the information owners. In other words, there are still many potential personal problems. For this reason, this work considered it necessary to develop the model for privacy protection.

In order to protect and manage the personal data more efficiently, it is very important to take into account the impact of privacy laws. In this thesis, I briefly describe the Korea's privacy law, and outline some related research, and privacy technologies in the web environments. This

work also discusses security and privacy concerns related to web environment services. This thesis introduces a trusted model for the privacy information protection based on access control. Proposed the model aimed to protect and prevent the privacy information in vulnerable network environments. Also, it includes privacy rules to ensure compliance with privacy laws, regulations, and guidelines, and helps to protect users from potential dangers. This work examines the practical applicability of the model by prototyping the system implementation method in the web environment. And it is compared and analyzed several related models, and also carries out to predict the performance of security. Finally, I conclude and discuss some ideas for future research work.