홍 승 필 교수지도

석사학위청구논문

웹 시스템 환경 내 개인정보보호 메커니즘 분석 및 구현방안

- 접근제어 중심으로 -

2009

성신여자대학교 대학원

전산학과

김 경 진

웹 시스템 환경 내 개인정보보호 메커니즘 분석 및 구현방안

- 접근제어 중심으로 -

홍 승 필 교수지도

이 논문을 석사학위논문으로 제출함

2008년 11월

성신여자대학교 대학원

전산학과

김 경 진

인 준 서

김경진의 석사학위 논문으로 인준함.

심사위원 _____인

심사위원 _____인

심사위원 _____인

성신여자대학교 대학원

논 문 개 요

인터넷과 정보통신기술 발달에 따라 급변한 현대사회는 새로운 정보 역기능 문제(사이버테러, 개인정보 유출)를 계속 증가시키면서 정보화 사회에 대한 사람들의 우려가 가증되고 있다. 아울러 사이버 범죄가 인터넷 환경뿐만 아니라, 현실세계에 전이되면서 피해규모도 사회적으로 확산되어 가고 있는 실정이다. 개인정보 측면에서도 비즈니스 발전과 더불어 그에 준한 다양한 위험요소(개인정보 오남용, 도용, 불법 사용 등)도 증가되고 있는 추세이다. 이에 국회와 행정부는 개인정보 관련 법안 입법화를 추진하고 있지만, 실제로 개인정보보호의 법규 측면에서 다양한 개별법령으로 흩어져 있어 법규 간에 상충되는 부분이나 보호받지 못하는 부분이 존재하고, 더욱이 기술적 측면에서 개인정보를 보호하기 위한 표준화 대안은 아직 미비한 실정이다.

본 논문에서는 서두에서 제시한 다양한 사이버 위협으로부터 개인정보를 신뢰적으로 관리하고 활용할 수 있는 대안을 소개한다. 이 연구는 개인정보를 체계적으로 관리하기 위해 국내외 표준 및 개인정보보호 법·제도와 표준화 기술에 대한 선행연구 기반으로 개인정보보호 정책을 제안한다. 국내 개인정보보호의 기술적 측면에서 개인정보 표준화기술 언어인 APPEL을 이용해 개인정보보호정책을 표현하고 프라이버시 법 기반의 정책을 활용하여 효과적인 접근제어 및 통제가 가능한 개인정보보호 엔진 시스템을 분석·설계한다. 마지막으로 안전한 시스템 환경 내 체계적인 정보보호 정책 지원 방안 확립과 시스템 구현방안을 소개함으로써 실 적용성 및 응용방안의 가능성을 타진한다.

목 차

논문개요

I. 서 론 ---------- 01

II. 관 련 연 구 ---------- 03

1. 개인정보 침해요소 및 동향 ---------- 03

2. 개인정보보호 법·제도 ---------- 05

1) 국외 개인정보보호 가이드라인 ---------- 05

2) 국내 개인정보보호 관련 법 ---------- 06

3. 개인정보 관련 기술 ---------- 09

1) 개인정보보호 기술 ---------- 09

① PIT(Privacy Invading Technologies) ---------- 09
② PET(Privacy Enhancing Technologies) ---------- 11
2) 접근제어기술 ---------- 12
① RBAC(Role Based Access Control) ---------- 13
3) 표준화기술 ---------- 15
① P3P(The Platform for Privacy Preference Project) ---------- 15
② APPEL(A P3P Preference Exchange Language) ---------- 17
4. 개인정보보호 관련 연구 동향 ---------- 18

III. 웹 환경 내 개인정보보호 문제점 ---------- 20
1. 법·제도적 이슈 ---------- 20
2. 기술적 이슈 ----------

- - - - - - - - - - - 22

IV. PIPS(Privacy Information Protection System) **구현방안** - - - - - - - 24

V. **개인정보보호 정책엔진 메커니즘** - 26

1. 메커니즘 개요 - 26

2. 메커니즘 구조 - 27

3. 메커니즘 기능 - 30

1) 프라이버시 기반의 접근제어(Privacy-based Access Control) - - - - 30

2) 정책관리(Policy Management) - 32

① Human Readable Policy - 32

② Policy Analysis / Parsing - 34

③ Policy Gathering & Repository - 36

④ Policy Enforcement ---------- 38

VI. 시스템 설계 및 구현 ---------- 40

1. 데이터베이스 설계 ---------- 40

2. 시나리오 ---------- 42

3. 프로토타이핑 - 화면 구성 ---------- 44

1) 정책정보 ---------- 45

2) 관련법규 ---------- 49

VII. 기대효과 ---------- 51

VIII. 결 론 -- 53
참고문헌
ABSTRACT

그림 목차

그림 1. 개 인 정 보 침 해 신 고 현 황 ---------- 03
그림 2. The RBAC96 Model ---------- 14
그림 3. P 3 P 기 본 동 작 ---------- 16
그림 4. P3P-APPEL matching ---------- 17
그림 5. PIPS 구 성 도 ---------- 27
그림 6. 역 할 분 류 ---------- 30
그림 7. 제 안 한 프 라 이 버 시 기 반 의 RBAC 모 델 ---------- 31
그림 8. 개 인 정 보 보 호 정 책 분 류 표 ---------- 32
그림 9. OECD 기반의 개인정보보호 정책 관리 분류표 ---------- 33

그림 10. 마 케 팅 목 적 내 정 책 설 정 예 ---------- 37
그림 11. A P P E L 문 서 변 환 예 ---------- 38
그림 12. 관 련 개 인 정 보 법 규 시 스 템 적 용 화 면 예 ---------- 39
그림 13. 데 이 터 베 이 스 구 조 및 관 계 ---------- 40
그림 14. 결 제 정 보 제 공 요 청 시 나 리 오 ---------- 42
그림 15. 정 책 정 보 내 마 케 팅 요 청 정 책 화 면 예 ---------- 45
그림 16. 정책정보 내 마케팅 요청정책 추가 및 수정화면 예 ---------- 46
그림 17. A P P E L 문 서 표 현 예 ---------- 47
그림 18. 정 책 정 보 내 공 개 등 급 정 책 화 면 예 ---------- 47
그림 19. 정 책 정 보 내 기 밀 등 급 정 보 수 정 화 면 예 ---------- 48
그림 20. 관 련 법 규 내 O E C D 원 칙 에 적 용 된 법 률 화 면 예 ---------- 49
그림 21. 관련법규 내 OECD 원칙에 적용된 법률 수정화면 예 ---------- 50

표 목차

표 1. 유 형 별 접 수 현 황 ---------- 04
표 2. 국 제 기 구 의 개 인 정 보 보 호 가 이 드 라 인 ---------- 06
표 3. 우 리 나 라 주 요 개 인 정 보 보 호 관 련 법 률 ---------- 07
표 4. 개 인 정 보 침 해 기 술 ---------- 10
표 5. 개 인 정 보 보 호 기 술 ---------- 12
표 6. 법 제 도 적 이 슈 정 리 ---------- 21
표 7. 기 술 적 문 제 점 정 리 ---------- 22
표 8. 접 근 제 어 구 성 요 소 ---------- 31
표 9. 보 안 등 급

-- 35
표 10. 이용목적 분류 -- 36
표 11. 관련연구와 제안한 PIPS 비교 -- 51

Ⅰ. 서 론

정보통신기술의 발달은 현대사회의 빠른 변화를 가져오면서, 그의 관련 정보역기능의 피해발생도 점차 증가하고 있다. 특히, 많은 서비스 기관과 기업 및 단체들이 네트워크를 통해 개인정보 수집, 유통이 용이해지면서 프라이버시 침해에 대한 문제가 사회적 이슈로 등장하고 있다. 최근 G사가 1100만 여명에 달하는 사상 최대 개인정보 유출 사고는 기업의 허술한 정보관리 실태를 여실히 나타내는 사례였음을 보여주며, 이번 사건으로 개인정보보호에 중요성을 재인식 시키면서 관심이 증가되고 있다. 개인정보 유출은 그 자체로도 문제지만, 신원 도용, 금전적 피해 등과 같은 2차적 문제를 가져오고 있다는 점에서 더욱 심각하다. 이러한 사이버 범죄는 개인의 정신적, 경제적 피해뿐만 아니라 사회적 혼란을 가져오며, 개인정보 유출을 당한 기업은 기업의 신뢰도와 이미지 하락은 물론 경제적, 법적 소송으로 인해 경영 위험에 직면할 수 있다.

이와 같은 사회적 파급효과로 개인정보 데이터 보호를 위한 다양한 솔루션들이 등장하고 기업들은 보안환경을 갖추는데 노력하고 있다. 또한, 국내 개인정보보호법안 제정이 대두되면서 국회에서는 개인정보보호 관련 법안 마련에 적극 나서며 개인의 권리 이익을 보호하기 위한 입법화가 진행되고 있다. 하지만, 국내 개인정보보호 법은 부가적인 규정으로 탄생하면서 기본적인 체계를 갖추지 못하고 입법적 보완 조치가 이루어지지 않고 있다. 이러한 법적 방안에 근거하여 기업들의 보안인식이 미비하고 아울러 보안인프라가 부족하게 되면서 체계적인 기술적 대응방안의 마련이 어려워졌다.

이에 따라 본 연구에서는 웹 시스템 환경에서 안전한 개인정보 수집 및 이용하고, 법률 기반으로 체계적인 개인정보보호 정책 가이드라인을 제시하여 개인정보보호를 위한 관리 시스템을 소개한다.

논문의 구성은 다음과 같다. 1장은 논문의 개요와 프라이버시 문제점에 대해서 간략히 소개하고 2장에서는 개인정보의 침해 현황 및 개인정보를 보호하기 위한 관련 제도와 기술 동향에 대해 설명한다. 3장에서는 웹 환경 내 이슈별 개인정보보호 문제점에 대해서 논의한다. 4장은 제안하는 메커니즘의 구현방안을 제시하며, 5장은 법기반의 개인정보보호 정책엔진 메커니즘을 소개하고, 세부구성요소를 설명한다. 6장은 제안한 메커니즘 기반으로 구현한 프로토타이핑 및 시나리오를 보여주며 7장 기대효과와 마지막 8장 결론으로 구성한다.

Ⅱ. 관련연구

1. 개인정보 침해요소 및 동향

한국정보보호진흥원과 개인정보분쟁조정위원회가 개인정보 침해동향 및 분쟁조정사례 등을 분석한 결과에 따르면, 개인정보 침해 상담 및 신고건수가 2006년 23,333건보다 약 10% 증가한 25,965건으로 집계되었다. 이로써 2002~2007년 동안 개인정보 침해 발생이 지속적으로 증가 추세임을 보여준다(<그림 1> 참조)[15][19].

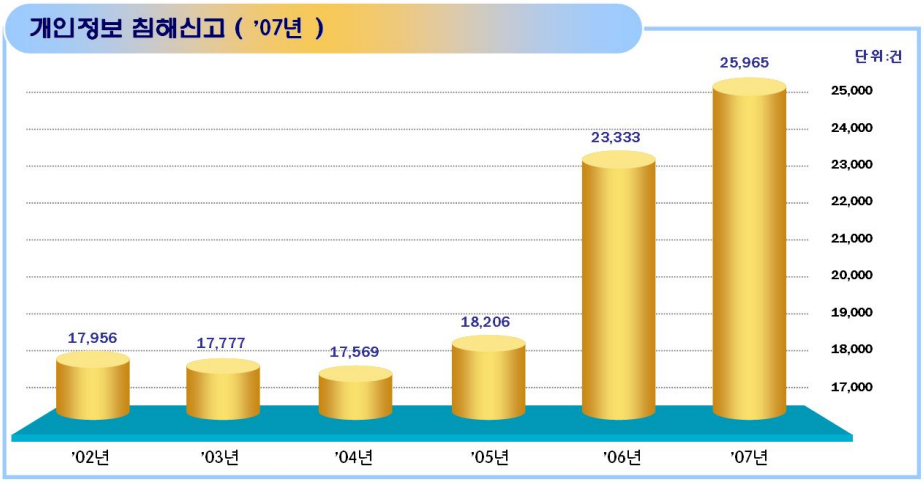

그림 4. 개인정보 침해신고 현황

2007년도 민원 접수유형을 <표 1>에서 살펴보면 정보통신망법 적용대상 민원은 4,382건으로 전체의 17%를 차지한 반면, 정보통신망법 적용이외의 민원 건수가 전체의 83%로 압도적인 비율을 차지하고 있다[19]. 그 중 주민번호 등 타인 정보의 훼손·침해·도용은 9,066건(전체 민원의 약 35%)으로 2006년에 비해 감소했지만 여전히 높은 비율을 보이고 있어 보다 근본적인 해결이 필요하다. 또한, 가장 높은 수치를 기록한 기타(정보통신망 법 규정

이외의 침해유형)에 대응하여 법제도 및 규제를 더욱 강화하는 방안이 필요하다는 것으로 분석된다.

표 1. 유형별 접수현황

접 수 유 형	2006년		2007년		증감율
	건수	비율	건수	비율	(%)
이용자 동의 없는 개인정보 수집	2,565	10.99	1,166(95)	4.49	▼55
개인정보 수집시 고지 또는 명시의무 불이행	27	0.12	7(2)	0.03	▼74
과도한 개인정보 수집	61	0.26	51(6)	0.20	▼16
고지·명시한 범위를 초과한 목적 외 이용 또는 제3자 제공	**917**	**3.93**	**1,001(190)**	**3.86**	▲9
개인정보 취급자에 의한 훼손·침해 또는 누설	206	0.88	123(20)	0.47	▼40
개인정보 처리 위탁시 고지의무 불이행	5	0.02	2(1)	0.01	▼60
영업의 양수 등의 통지의무 불이행	11	0.05	14(4)	0.05	▲27
개인정보관리책임자 미지정	23	0.09	10(2)	0.04	▼57
개인정보보호 기술적·관리적 조치 미비	**632**	**2.70**	**522(62)**	**2.01**	▼17
수집 또는 제공받은 목적 달성 후 개인정보 미파기	266	1.20	146(36)	0.56	▲45
동의철회·열람 또는 정정 요구 등 불응	**923**	**3.96**	**865(186)**	**3.33**	▼6
동의철회, 열람·정정을 수집방법보다 쉽게 해야 할 조치 미이행	484	2.10	461(85)	1.78	▼5
법정대리인의 동의 없는 이동의 개인정보 수집	23	0.10	14(2)	0.05	▼39
주민번호 등 타인 정보의 훼손·침해·도용	**10,835**	**46.4**	**9,066(75)**	**34.99**	▼16
기타(정보통신망법 규정 외의 침해유형)	**6,355**	**27.2**	**12,497(81)**	**48.13**	▲97
합 계	**23,333**	**100**	**25,965(847)**	**100**	▲11

※ ( )는 신고건수를 의미함 (출처 : 2007 개인정보분쟁조정사례집)

2. 개인정보보호 법·제도

1) 국외 개인정보보호 가이드라인

개인정보보호에 대한 논의가 국제기구에 의하여 처음 논의된 것은, UNESCO가 1970년 ICJ(International Commission of Jurists – 국제사법 재판소)에 프라이버시와 개인정보보호에 관한 보고서를 의뢰한 것이다. 이후, 1973년 세계최초 개인정보보호관련 국내입법인 스웨덴의 Datalag 제정이 이루어지고, 이어 미국에서 the Privacy Act of 1974를 제정하는 등 본격적인 개인정보보호법제가 발전되었다. 이후, 1980년대부터는 정보통신기술의 발전으로 인하여 컴퓨터에 의한 대량의 데이터 처리가 가능해짐에 따라 개인정보의 보호, 특히 전산 처리되는 개인정보의 보호필요성이 강하게 제기 되었고 이에 국제기구들은 이를 위한 여러 가지 방안과 지침을 제시하기 시작하였다[7].

가장 먼저 OECD는 “프라이버시보호와 개인정보의 국제적 유통에 관한 가이드라인”을 채택하여 각국의 개인정보보호를 위한 노력과 국내입법의 제정을 권고하였고, APEC은 회원국 간의 전자 상거래 촉진을 위해 APF를 개발하여 개인정보 및 개인정보보호를 도모하였다. EU에서도 개인정보 취급 규정 기반으로 개인정보 처리와 프라이버시권을 보호하며 유통을 촉진할 수 있도록 지원하였다[13].

이러한 국제기구들이 공통으로 제시하는 목적은 개인정보 사용을 위한 서비스 개발을 하고 이용자가 쉽게 이해할 수 있는 명확하고 간결한 개인정보보호 정책을 세우는 것이다. 이를 기반 하여 정보수집, 정보활용, 정보저장, 정보공개, 정보보안, 접근제어, 감사 등의 기술적인 뒷받침을 요구하고 있다[12].

주요 개인정보보호 관련 표준화 가이드라인은 <표 2>로 정리할 수 있다[2][7].

표 2. 국제기구의 개인정보보호 가이드라인

기구	가이드라인 지침
OECD	◆ Organization for Economic Cooperation and Development ◆ 1980년 개인정보보호지침에서 언급된 원칙들을 재확인하고, 개인정보보호에 대한 이용자 및 소비자의 요구사항을 수렴하는 역할을 담당 ◆ 공적·사적 부분에서 개인정보의 사생활 권 보호, 정보의 자유로운 유통 장려, 자유로운 정보유통에 대한 부당한 제한방지, 관련국내법규정과의 조화 ◆ '프라이버시보호와 개인정보의 국제적 유통에 관한 가이드라인' 8원칙 제안
APEC	◆ Asia-Pacific Economic Cooperation (Conference) ◆ APEC 회원국 간의 전자 상거래 촉진을 위해 APF(APEC Privacy Framework)를 개발 ◆ APF 원칙들은 개인정보의 원활한 국제적 이전을 촉구하여 전자상거래를 활성화하는 동시에 개인정보 및 개인정보보호를 도모 ◆ 개인정보보호 관련 9가지 원칙을 제정
EU	◆ 개인정보취급에 대한 규정 ◆ 회원국 국민의 기본권 및 자유를 보호하고 개인정보 처리와 관련한 프라이버시권을 보호하여 EU국가 간의 개인정보의 자유로운 유통을 촉진
UN	◆ 프라이버시 보호를 위해 국가들 간의 자유로운 정보의 이동 및 상기 원칙의 준수여부를 감독할 독립기구의 설치 등에 대하여 규정 ◆ 개인정보 파일을 규율하는 6가지 원칙을 제시
ISTPA	◆ The International Security, Trust, and Privacy Alliance ◆ 개인정보의 표준, 도구, 기술을 연구 및 평가하고 개인정보보호 프레임워크를 정의하기 위해 구성된 전 세계 기업과 기술 공급자들의 연합 ◆ 『ISTPA 개인정보보호 프레임워크』는 개인정보보호 원칙과 운영에 대해서 하위 레벨의 개인정보보호 서비스와 성능으로 정확하게 구체화 ◆ 개인정보보호 8원칙을 제시
IPC	◆ Information and Privacy Commissioner ◆ 개인정보보호와 접근 이슈들에 대한 연구를 지휘하고 개인정보보호와 접근 이슈에 대하여 공공 교육을 지원 ◆ 고객들의 개인정보를 잘 관리할 수 있는 방법을 제시해주는 자체관리 평가도구인 PDT 개발 ◆ 개인정보보호에 대한 10가지 원칙 제안

특히, OECD 개인정보보호 가이드라인 8원칙은 각국의 개인정보보호 관련 법제도, 가이드라인에 모델이 되었으며, 각국의 공공부문이나 민간부문에 광범위하게 받아들여지고 있다.

2) 국내 개인정보보호 관련 법

국내 개인정보보호는 헌법을 중심으로 공공부문과 민간부문의 이원화된

법체계로 구성된다. 현행 개인정보보호법의 체계는 공공부문의 법률과 민간 부문 중 정보통신 부문 및 신용부문 등의 주요 법률과 기타 개별법규의 체계로 이해되고 있다[5].

현행 입법체계를 표로 정리하면 다음과 같다[11].

표 3. 우리나라 주요 개인정보보호 관련 법률

분야	주요법률	기타 관련법	기타 규정
공공행정	**공공기관의 개인정보보호에 관한 법률**	◆ 공공기관의정보공개에관한 법률 ◆ 전자정부법, 주민등록법, 호적법 ◆ 자동차관리법, 도로교통법, 국세기본법 ◆ 국정감사및조사에관한 법률, 통계법 등	◆ 변호사법 ◆ 법무사법 ◆ 세무사법 ◆ 관세사법 ◆ 공인노무사법 ◆ 외국환거래법 ◆ 공증인법 ◆ 은행법 ◆ 근로기준법 ◆ 노동위원회법 ◆ 직업안정법 ◆ 공인중개사의 업무 및 부동산 신고거래에 관한 법률 ◆ 형법 제317조 등
정보통신	**정보통신망 이용촉진및 정보보호등에관한 법률**	◆ 통신비밀보호법 ◆ 위치정보의보호및이용등에관한 법률 ◆ 정보화촉진기본법, 정보통신기반보호법, 전기통신사업법, 전자서명법 ◆ 인터넷주소자원에관한 법률 등	
금융/신용	**신용정보의 이용및보호에관한 법률**	◆ 금융실거래및비밀보장에관한 법률 ◆ 독접규제및공정거래에관한 법률 ◆ 방문판매등에관한 법률 ◆ 전자상거래등에서의소비자보호에관한 법률 ◆ 전자거래기본법, 보험업법, 증권거래법 등	
의료	**보건의료기본법 의료법**	◆ 응급의료에관한 법률 ◆ 장기등이식에관한 법률 ◆ 생명윤리및안전에관한 법률 ◆ 인체조직안전및관리등에관한 법률 ◆ 후천성면역결핍증예방법, 전염병예방법 등	
교육	**교육기본법**	◆ 초중등교육법 ◆ 교육정보시스템의운영에관한 규칙 등	

(출처 : 한국정보보호진흥원, 2008)

<표 3>을 살펴보면, 정보통신기술의 발달로 개인정보에 대한 침해가 증가하면서 개인정보보호 관련법령 정비가 지속적으로 이루어짐을 알 수 있다. 공공부문에 있어서는 개인정보보호에 관한 일반법으로 '공공기관의 개인정보보호에 관한 법률'로 컴퓨터에 의해 처리되는 개인정보의 취급에 관하여 필요한 사항을 정해준다. 또한, 전자정부법, 공공기관의 정보공개에 관한 법률, 주민등록법, 호적법, 자동차관리법, 도로교통법, 국세 기본법 등으

로 개별법에 개인정보보호에 관한 규정이 있다. 민간부분에 있어서는 일반적으로 정보통신망의 이용 활성화, 개인정보의 보호, 청소년 보호, 정보통신망의 안전성 확보 및 스팸에 관한 규제와 정보통신망에서의 명예훼손 등에 대한 벌칙을 규정해주는 '정보통신망 이용 촉진 및 정보보호에 관한 법률'이 있으며, 신용정보에 대해서는 통신비밀보호법, 위치정보 보호에 대해서는 위치정보의 보호 및 이용 등에 관한 법률이 제정되어 있다. 이외에 실지명의에 의한 금융거래를 실시하고 그 비밀을 보장을 위한 금융실명거래 및 비밀보장에 관한 법률, 전자거래기본법 등 개별법에 따른 규정들이 있다[5][11].

3. 개인정보관련 기술

1) 개인정보보호 기술

개인정보보호 표준 가이드라인이나 입법의 기본 정신은 개인의 권리를 존중하며 꼭 필요한 최소정보만을 제공하여야 한다는 것이다. 그러나 정보통신기술의 발전에 따라 개인정보침해기술(PIT – Privacy Invading Technologies)도 급변하여 상기 기본정신을 무색하게 하고 있다. 이러한 개인정보침해기술에 대응하기 위해 다양한 형태로 개인정보보호기술(PET – Privacy Enhancing Technologies)이 개발되었고, 현재도 연구되고 있다.

① PIT(Privacy Invading Technologies)

현재 컴퓨터 시스템 및 네트워크 등은 사용자들에게 편리성을 제공하고 효율성을 높이기 위해 신원확인을 용이하게 하고 있다. 이러한 기술 개발은 개인정보침해기술(PIT)도 발전시키고 있어 컴퓨터 환경 내 개인정보 관련 오남용 및 악의적 피해가 증가되고 있다.

특히, 사회 전반적으로 해킹, 분산 서비스거부 공격, 악성코드 감염 등 침해사고로 인하여 국가기관·첨단기업 중요자료 절취, 개인정보 유출, 프라이버시 침해, 금전적 갈취 등의 위협이 지속적으로 발생하고 있다. 2007년도에는 웹 2.0도입과 UCC 대중화로 인하여 인터넷의 새로운 패러다임이 도래하였으며, 이에 대한 정보화 역기능도 중요한 이슈로 대두되고 있다. 또한, 인터넷 뱅킹에 대한 메모리 해킹, 디지털 포렌식 기술의 사회 이슈화, 기밀정보 유출에 대응하기 위한 내부자 보안의 중요성 부각 등이 주요 사이버 위협이라 할 수 있다[5]. 이러한 정보역기능 침해기술로 스팸메일, 개인정보의 유출, 피싱(Phishing)이나 파밍(Pharming)에 따른 개인적인 피해가 증가하고 있으며 이는 심각한 사회문제로 대두되고 있다. 개인정보침해기술의 요약은 <표 4>와 같다[14].

표 4. 개인정보침해기술

침해 기술	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 ISP 정보와 E-mail 이용자의 ID를 이용하여 이용자의 계정을 확인
Processor Serial Number (PSN)	◆ Intel 사는 자사가 개발하는 Pentium III 칩에 고유의 프로세서 일련번호(Serial number)를 부여하여 인터넷에 접속하는 특정 컴퓨터의 이용자의 신원 정보와 연결시킴으로써 전자상거래에서 인증 목적으로 이용
IPv6	◆ IPv6의 계획은 인터넷 상의 모든 장치에 고정된 주소를 할당 하는 것 ◆ IPv6의 새로운 주소는 하드웨어 속에 내장될 것이고, 추적 가능한 정보를 포함. 이것은 마치 영구적인 쿠키를 심는 것과 동일 개념.
쿠키(cookie)	◆ 쿠키 파일을 이용하여 인터넷 이용자의 신원 파악 - 첫째, 쿠키는 로그인정보(ex. 이름, 주소 비밀번호 등)를 알아내는 데에 사용될 수 있음. - 둘째, 쿠키에 담긴 정보와 마케팅 데이터베이스에 있는 이용자의 이름, 주소, 이전의 소비정보 등을 상호 비교함으로써 이용자의 신원 확인 가능
웹 버그 (Web bug)	◆ 웹 버그는 온라인 이용자가 모르는 사이에 이용자에 관한 정보를 유출하거나 심지어 이용자의 시스템을 파괴할 수 있는 기술
스파이웨어 (spyware)	◆ 무료 또는 유포로 배포되는 소프트웨어에 들어 있는 일종의 프로그램 모듈을 통칭 ◆ 해당 소프트웨어를 설치한 컴퓨터 이용자가 인터넷을 서핑 할 때 이용자의 개인정보나 온라인 활동 정보를 스파이웨어 회사 서버에 지속적으로 전송하는 것이 주된 기능
고성능 스파이웨어 기술	◆ 스파이웨어를 탐지하는 안티 스파이웨어 솔루션 등의 백신으로 우회하여 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
WLAN 환경	◆ WLAN 사용자가 액세스 포인트에 접속할 때, 해커가 가상의 액세스 포인트를 이용하여 사용자의 중요한 개인정보를 모니터링하게 됨
웹 메일의 첨부 파일 유출	◆ 웹 메일 첨부파일 유출기법은 기존 e-mail이나 웹 메일을 모니터링 하여 데이터를 유출하는 방식에서 한 단계 진화하여, 웹 메일에 첨부된 파일을 encoding하는 방식으로 주로 기업이 운용하는 메일 모니터링 프로그램을 우회하여 기밀 정보를 유출하는 방법
Steganography	◆ 이미지 및 오디오 파일에 중요한 파일이나 메시지를 첨부하는 기법 ◆ 오사마빈라덴이 알카에다 조직원과의 연락을 위해 사용된 것으로 보고되면서 널리 알려짐
접속 세탁	◆ 해커가 여러 국가를 경유하여 해킹을 할 경우, 중간 단계에 해커 그룹이 운용하는 기명경로를 거쳐 해커에 대한 역추적이 불가능하게 하는 방법
위치측정 정보 침해	◆ GPS 또는 휴대전화기의 위치 측정 내용을 인터넷을 통해 사용자 동의 없이 개인의 위치 정보가 유출 되는 방법

② PET(Privacy Enhancing Technologies)

개인정보보호기술(PET)의 개념은 다양하게 정의되고 있다. 먼저 유럽의회에서는 개인정보보호기술의 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 작업반 회의에서 발표한 의미는“식별 가능한 정보를 수집 혹은 처리하지 못하도록 하거나 최소화함으로써 정보시스템의 기능적 손해 없이 개인의 프라이버시를 보호하는 다양한 종류의 기술”로 정의하고 있다. 이처럼, 개인정보보호기술이란 종류가 다양하고 계속적으로 발전하는 개념이어서 그에 대한 정의 역시 다양하다[18].

개인정보보호기술은 이미 다양한 솔루션이나 기술이 상당수 개발되어 있고 또한 진행 중에 있다. 대표적인 기술로는 익명화 기술, W3C(the World Wide Web Consoritium)에서 개발한 P3P, OECD에서 개발한 프라이버시정책 생성기(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[17]. 또한 최근에는 개인정보침해기술에 대응하여 크게 6개 영역(에이전트기반기술, 웹 기반 익명성 제공기술, 네트워크 기반기술, 암호화 기술, 정책협상 기술, 내부정보보안기술)에 걸쳐 세부 개인정보보호기술을 분류될 수 있다. <표 5>에서 영역별로 개인정보보호기술에 관해 간단히 살펴본다[16].

표 5. 개인정보보호기술

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 - 쿠키매니저, 에드브로커, 스파이웨어 필터 등
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 - Proxy, 방화벽, IDS 등
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 - SSL 등
내부정보보안기술	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. - Secure OS, HIDS/HIPS, DRM 등

2) 접근제어 기술

접근제어란 사용자가 접근할 수 있는 자원의 범위를 제한하는 것이다. 즉, 컴퓨팅 자원, 통신 자원 및 정보자원 등에 대하여 읽기, 쓰기, 실행 등의 접근 여부를 허가하거나 거부하는 기능을 말한다. 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[20].

먼저 임의적 접근통제는 정보객체를 요청하는 사용자의 신원에 근거를 두고 접근허가를 결정하는 정책이다. 이 방식은 접근권한의 통제가 정보객체의 소유자에 의해 다른 사용자에게 허가되거나 철회될 수 있으며, 정보객체의 소유자의 재량에 따라 접근통제가 이루어진다. 강제적 접근통제 정책보다 유연한 정보보호 메커니즘을 제공할 수 있는 장점이 있으나, 확장성이 부족하고 소유자 재량에 따라 접근통제가 쉽게 변경 가능하여 상업 환경 적용에 부적합한 특성을 가지고 있다.

강제적 접근통제는 시스템 보안 관리자에 의해 부여된 사용자와 정보객체의 보안 등급에 의해 정보에 대한 접근허가 여부를 결정한다. 이는 정보객체와 사용자에게 배정되는 보안 등급이 체계적으로 잘 정의될 수 있고 매우 엄격한 정보의 흐름만을 허용하여 임의적 접근통제보다 안전하다. 하지만, 군사 분야와 같은 매우 특정 영역에만 적용되는 단점을 가지고 있어서 이 정책 역시 융통성이 필요한 일반적인 기업환경에 적용하는데 문제점이 있다[4].

상기 언급한 접근제어 방식은 조직에 적용하기에는 문제가 있어 최근에는 역할기반 접근통제가 연구되고 있다. 이는 기업 환경뿐만 아니라 데이터베이스, 운영체제 등에 적용될 수 있는 매우 유연한 접근통제 정책으로, 임의적 또는 강제적 접근통제 정책보다 정보에 대한 추상적인 접근통제와 효율적인 접근권한 관리를 수행할 수 있는 장점을 가지고 있다[21]. 본 절에서는 이러한 장점을 이용할 수 있는 역할기반 접근통제에 대해서 상세히 소개한다.

① RBAC(Role Based Access Control)

역할기반 접근제어(RBAC – Role Based Access Control)는 1970년대에 개척된 온라인 시스템의 개념으로 다중 사용자, 다중 애플리케이션과 함께

시작되었다. 역할기반 접근제어 모델에서 사용자는 객체를 임의로 접근할 수 없도록 하는 대신에 접근 권한이 역할에 부여되고 사용자는 적절한 역할에 소속되어 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 이는 조직 내에 이용될 수 있는 매우 유연한 접근 통제 정책으로 현실 세계에서 수행하는 업무적 역할에 따라 인가권한을 역할에 할당하고, 사용자들의 권한 관리를 효율적으로 할 수 있도록 지원한다[4][20].

<그림 2>는 기본 RBAC 모델이다[30].

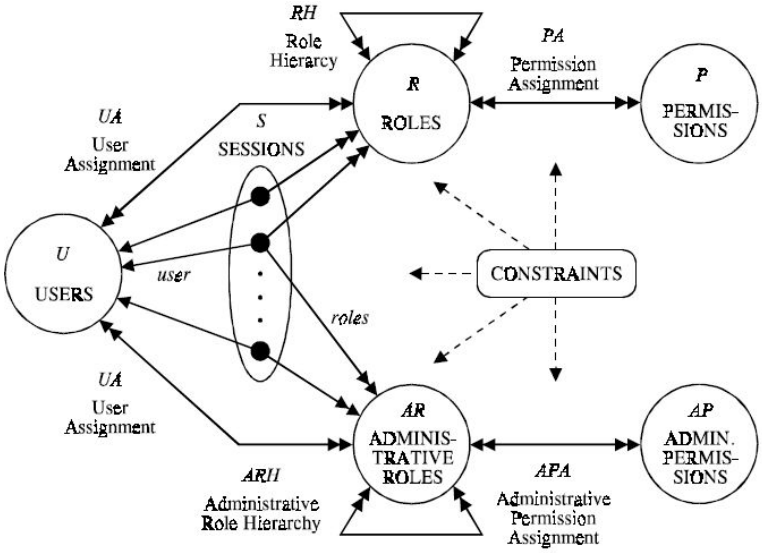

그림 5. The RBAC96 Model

이 모델의 사용자(U - USERS)는 인간의 행동이나 자율적인 에이전트를 나타낸다. 반면에 역할(R - ROLES)은 조직에서 역할에 속해 있는 멤버들에게 주어진 권한과 책임감을 고려하여 연관된 의미들을 가진 일의 기능이나 이름이다. 권한(P - PERMISSIONS)은 시스템에서 하나 이상의 대상에 대한 접근의 특성 형태에 대한 허가이다. 또한, 제시한 사용자 할당(UA - User Assignment)과 권한 할당(PA - Permission Assignment)은 다-대-다 관계를 가지고 있다. 즉, 사용자는 많은 역할의 구성원일 수 있으며, 하나의 역할은 많은 사용자를 가질 수 있다. 역할은 많은 허가를 할 수 있으며, 하나의 역

할은 많은 사용자를 가질 수 있다. 제약조건은 사용자 할당과 권한 할당에서 관찰되어야만 하는 규칙을 서술한다. 역할 계층(RH – Role Hierarchy)은 역할의 계층적인 구조와 제약조건의 특정한 형식을 나타낸다. 이는 부분적인 순서체계 안에서 구성된 것이며, 예를 들어 상위 역할은 하위 역할로부터 그 허가권한이 전파된다[20][21].

역할기반 접근제어 모델은 역할의 개념을 사용함으로써 사용자와 그들의 권한들을 효과적으로 관리할 수 있다. 또한 조직 내 개인에게 접근 권한을 인가할 때 발생할 수 있는 잠정적인 에러, 복잡성, 비용 등을 줄일 수 있는 강력한 구조이다[15].

3) 표준화 기술

본 절에서는 프라이버시 정책 기반의 개인정보보호 관련 표준화 기술을 설명한다.

① P3P(The Platform for Privacy Preference Project)

W3C의 P3P(The Platform for Privacy Preference Project)는 정보통신서비스 제공자와 서비스 이용자 사이에서 개인정보보호정책을 XML 형식으로 표현하는 규격이다. 이는 개인정보보호 정책을 자동적으로 검색하여 적절하다고 판단될 경우, 자신의 개인정보를 제공한다. 즉, P3P는 개인정보를 취급하는 서비스 제공자가 자신의 개인정보보호 정책을 표준 형식으로 표현할 수 있는 기반을 제공하고 의사결정 작업을 자동화하는 기술적 메커니즘을 제공한다[3].

P3P는 2002년 4월 개인정보보호정책을 표현하기 위한 방법을 제시하고 있는 P3P v1.0 표준권고안이 발표하였다. P3P v1.0에서 제시하는 P3P정책의 기술 규격은 P3P 개인정보보호 정책의 구문과 의미, 정책을 웹 자원에 연계시키기 위한 메커니즘 등을 정의한다. P3P정책은 개인정보보호 정책을

표현하기 위한 P3P 어휘들을 사용하여 작성된 정책고지문들로 이루어지며, 또한 P3P 기본 데이터 스키마의 엘리먼트들을 참조한다. 이 기본 데이터 스키마는 모든 P3P 사용자 에이전트들이 인식해야 하는 엘리먼트들에 대한 표준 집합이다. 그러나 개인정보보호정책은 각 국가별로 적용되는 개인정보보호법규가 상이하여 2005년 1월에 각 국가별 관련 법규를 포함할 수 있도록 하는 P3P v1.1 권고안이 발표되었다[22].

P3P의 기본 동작은 사용자 에이전트와 웹 서버 주체로 이루어진다. <그림 3>과 같이 사용자가 P3P기능이 내장되어 있는 웹 브라우저에 입력하면 사용자의 브라우저는 그 페이지를 위한 P3P 정책을 자동적으로 받아올 수 있다. P3P정책을 수신한 사용자 에이전트는 사용자가 설정한 정책과 대조하여, 해당 정책을 사용자가 수용할 수 있는 것인지 판단을 하며 사용자에게 통보해 해당 홈페이지의 서비스 이용 여부를 결정한다[3][32].

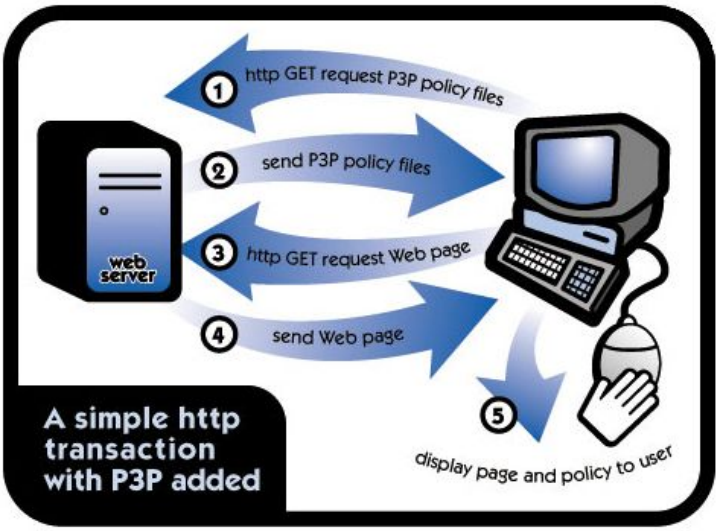

그림 6. P3P 기본동작

P3P는 1997년부터 W3C 주도로 AOL, HP, 마이크로소프트 등 업계와 시민단체가 참여하여 진행하였으며, 2001년 개발이 완료된 후 시험 운용 끝에 2002년 4월에 국제표준으로 승인되었다. 마이크로소프트는 인터넷 익스플로

러 6.0에 P3P 기능을 일부 채택하였고, AT&T는 P3P와 관련된 제품을 무료로 제공하고 있다[10].

② APPEL(A P3P Preference Exchange Language)

P3P와 더불어 W3C는 사용자가 자신의 정책을 표현하고 P3P 에이전트들 간에 P3P 정책을 교환할 수 있도록 APPEL(A P3P Preference Exchange Language)을 제안한다[10]. APPEL은 웹 사이트의 개인정보정책과 사용자 에이전트의 정책을 비교하기 위해 사용자가 제공할 수 있는 정보를 표준화할 수 있는 표준 언어이다. 즉, 웹 사이트가 제시하는 P3P 정책에 대해 사용자가 이를 요청, 제한, 차단할 수 있는 방법을 표현할 수 있도록 언어를 제공한다[23].

APPEL은 자신이 설정하는 정책 내에서 선호도를 표현할 수 있다. 이는 정책을 표준화할 수 있는 APPEL로 표현함으로써, 상이한 그룹 내 다양한 사용자 에이전트들에게 자신의 정책파일을 전송하면, 정책을 비교하고 접근 여부 및 개인정보 이용이 가능하다[27]. <그림 4>는 P3P와 APPEL의 표현방법의 비교를 보여준다[29].

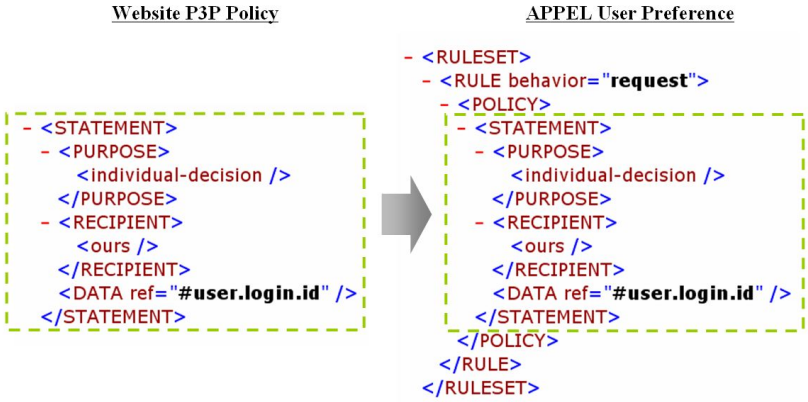

그림 7. P3P-APPEL matching

4. 개인정보보호 관련연구 동향

인터넷 서비스의 발전은 개인정보의 활용도를 높이면서 개인정보 유출사고와 같은 정보역기능의 피해를 증가시키고 있다. 이러한 문제점을 해결하기 위해 국내외에서 개인정보보호에 관한 기술 및 연구가 활발히 진행 중이다. 국외의 대표적인 연구는 PORTIA, PISA, PRIME, PiMI가 있고 국내에는 ETRI에서 개발한 IDMS가 있다.

- PORTIA(Privacy, Obligations, and Rights in Technologies of Information Assessment) – 특정 시스템 환경에서의 민감한 정보를 다루는 하나의 효과적이고 개념적인 프레임워크를 개발한다. 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 진행 중이다.
- PISA(Privacy Incorporated Software Agent) – 네트워크 환경에서 개인정보 유출 없이 사용자를 대신하여 복잡한 업무를 수행하는 지능형 소프트웨어 에이전트 모델을 구축하는 프로젝트이다. 개인정보를 보호하기 위한 정책 메커니즘을 통해 프라이버시 보호 기능을 제공한다.
- PRIME(Privacy and Identity Management for Europe) – 통합된 identity 관리 시스템들이 프라이버시를 강화하는 실제적 발전을 위한 설계에 주요 목적을 두고 있다. 단지 하나의 컴포넌트의 프라이버시에 집중하기 보다는 통합된 프라이버시-강화 해결책을 강화시키고 있다.
- PiMI(Privacy in the Mobile Internet) – 모바일 환경에서의 프라이버시 증대에 대한 기술적인 솔루션을 제안하고 논의한다. 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[2][3].

- **IDMS(Identity Management System)** – 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[10].

Ⅲ. 웹 환경 내 개인정보보호 문제점

1. 법 · 제도적 이슈

웹 환경에서 발생하는 개인정보 침해에 대비하여 현재 우리나라의 경우, 개인정보 또는 정보프라이버시의 보호를 위한 법령들이 입법화 되고 있다. 하지만 개인정보보호 법령이 부분적으로 제정되면서, 다양한 분야에서 산재되어 있어 법적 보호의 공백과 사각지대가 빈발하고 법규간의 상충되는 부분이 존재한다[11]. 즉, 분산된 법률은 체계적인 기본 시스템을 갖추지 못하고 있어 개인의 자기정보 통제를 위한 법제를 포괄하는 개인정보보호 통합체제의 구축을 필요로 한다. 이는 하나의 통합된 법률에서 규율하는 통합일반법을 통해 공·사 부문에 공통적으로 적용되는 실효성 있는 법적 규율과 규율체계의 실체가 통합적인 법제에 담겨야 할 것이다[7].

이렇게 분산된 법률을 하나로 합침과 동시에 이를 감독, 관리할 독립기구를 신설해야 한다는 논쟁도 제기되고 있다. 우리나라의 경우 개인정보보호법에 의해 공공부문으로 국무총리 산하에 설치되어있는 '개인정보보호 위원회'가 있지만 심의 기능만 가지고 있을 뿐 독자적인 기능은 가지고 있지 않다[9]. 이러한 현행 개인정보보호 감독기구에 의해서는 개인정보권이 제대로 보장될 수 없다는 문제로, 공·사양부문에 모두 관할권을 가진 강력한 보호 기구를 신설되어야 한다[7].

그러나 국내 법률의 경우, 공공부문과 민간부문에 일정부분 일반법의 역할을 하는 법률을 이미 갖고 있는 상황에서 무리하게 두 법률을 하나로 통합하는 입법체계는 현시점에서 다소 추진상의 어려움이 있다[7]. 개인정보보호 감독기구 역시 현행의 행정자치부, 정보통신부 등의 일반법 소관부처

뿐만 아니라 재정경제부 및 금융감독위원회, 보건복지부, 교육인적자원부 등 개별 행정주체가 모두 감독기구인 셈이므로 개인정보 보호를 위한 정책 수립, 실태조사 및 지침 수립 등의 주요 업무를 하는 기관이 영역별/부처별로 분산되어 있기 때문에 일관성 있는 개인정보 보호체계가 정립되지 못하고 있다[9].

아울러, 정보통신서비스제공자 등의 사업자가 지켜야할 개인정보보호 관련 법규준수율이 정부의 노력에도 불구하고 낮은 수준이며, 현행 법규에 의한 개인정보보호 고지의 의무 및 개인정보의 기술적·관리적 보호조치의 의무화 등의 준수율은 정부의 지속적인 계도조치 및 단속으로 꾸준히 증가하고 있으나 아직은 미미한 실정이다[8]. 이러한 법제도적 문제점을 <표 6>으로 정리하였다.

표 6. 법제도적 이슈 정리

법제도적 문제점	대응 방안
개인정보보호 법령들이 다양한 분야에서 산재되어 법적 보호가 불안정	개인정보보호 통합 체제 구축
개인정보보호 주요업무 처리하는 기관이 분산되어 있어 일관성 있는 보호 체계가 어려움	독립적인 개인정보보호 감독기구 신설
개인정보보호 관련 법규준수율이 낮은 수준	정보의 지속적인 계도조치 및 단속

이와 같은 문제들은 국내 법제도적 환경을 고려한 개인정보를 보호하는 방안이 필요하며, 규범적으로는 기술 중립적이고 헌법 친화적인 입법을 제정하는 법제 정비가 필요함이 있어 지난 17대 국회는 개인정보보호와 관련된 3개 법안을 발의하고 통합안 도출에 힘을 썼음에도 법안 마련에 실패, 결국 공은 18대 국회로 넘어왔다. 현재는 개인정보보호법안을 발의한 상태며 정부에서는 행안부가 지난 6월 공청회에 이어 개인정보보호법 제정안을 입법예고한 상태다[11]. 중요한 것은 다른 법안에 우선순위가 밀려 방치되어 있다가 17대 국회처럼 임기가 만료되면서 폐기 되서는 안 되고 18대 국회에서는 개인정보보호법안을 꼭 처리해야 한다는 것이다.

2. 기술적 이슈

컴퓨팅 환경 내 개인정보 관련 오남용 또는 피해의 대안으로 다양한 기술들이 개발되었다. 이러한 기술들의 문제점을 정리하면 <표 7>로 요약할 수 있다.

표 7. 기술적 문제점 정리

기 술	문제점
RBAC	◆ 주체 위주의 접근제어로 동적인 상황변화에 부적합
P3P	◆ 프라이버시 정책 표현이 간단하여 정책 표현상의 한계 ◆ 사용자들의 P3P 존재 인식 미비
APPEL	◆ 작동 시 부하 발생 및 반응속도 느림 ◆ 사용자의 직접입력을 필수로 하여 사용용이성을 감소시킴
EPAL	◆ 프라이버시 정책과 별개로 구성되어 접근통제가 어려움
XACML	◆ 복잡한 정책 생성이 가능하지만, 아직 정형화가 필요

정리된 기술적 문제점을 세부적으로 설명하면 다음과 같다.

먼저, 접근제어 중 하나인 RBAC은 1992년 소개된 이후, 업체들이 자신들의 제품과 데이터베이스 관리 시스템, 보안관리 및 네트워크 관리 시스템 등에 RBAC의 기능들을 구현하기 시작하였으나, 표준화된 기능 정의가 없이 구현돼 RBAC의 유용성과 의미가 불확실하고 혼돈을 초래하였다. 이러한 문제들로 미국 정부와 산업체들은 NIST에서 RBAC 표준안을 개발하게 되었다[1]. 하지만, RBAC은 주체 위주의 접근제어 정책을 세우는 것에만 초점이 맞춰져 있어 수시로 변하는 상황에서는 접근제어 수행 및 제어가 어렵다.

개인정보보호의 표준화 기술인 P3P는 웹 환경에서 개인정보를 보호하기 위한 것으로 다른 표준들에 비해 간단한 표현방법을 제공한다. 즉, 자연언어로 되어있는 정책 내 부정확한 의미의 프라이버시 정책언어를 컴퓨터가 인식하는 정확한 프라이버시 정책언어로 표현될 수 없다. 그리고 많은 사용자들이 매일 웹 브라우저를 사용하고 있지만 아직 P3P에 대한 존재를 인식

하고 있는 사용자는 IT 관련 특히 정보보호 관련 종사자 외에는 거의 없는 실정이다[10][24].

또한, P3P기반의 APPEL은 사용자가 직접 자신의 선호도 정책을 입력해야만 자동적으로 작동되는 메커니즘이며 이는 사용자의 사용용이성을 감소시킨다. 아울러, APPEL의 사용이 부하를 낳게 하고 반응 속도가 느려져 결과적으로 웹 사용상의 불편을 초래하게 된다. 그리고 표현상의 한계점이 있어 특히 규칙을 표현하기에는 XML 기반의 APPEL이 한계가 많은 것으로 알려지고 있다[6].

다음 EPAL은 기업 내 고객 정보와 같은 프라이버시 정보에 대한 정책을 수립하고 이를 교환하고 판단하기 위한 기술이다[10]. EPAL 내에 사용자 카테고리(User categories) 구성원은 데이터를 사용하는 개인을 말하며, 데이터 접근제어 시 프라이버시 정책과는 구분되어 접근여부가 결정된다[31]. 즉, 프라이버시 정책과는 별개로 구성된 모델로 개인정보보호기반의 접근제어가 어렵고, 정책충돌 발생 시 해결하지 못한다.

프라이버시 정책을 생성할 수 있도록 해주는 표준이라는 점에서 P3P, EPAL과 비슷한 기술인 XACML은 XML기반의 언어로 구성된 정책모델로 잘 알려져 있다. 이는 기업 내 데이터 접근 및 사용자 정보를 보호하기 위한 기술로 보다 다양하고 복잡한 프라이버시 정책을 생성하고 관리할 수 있다. 객체(자원과 목적)의 계층적 구조를 지원하지만, 각 계층들의 의미가 명백하지 않고, 정책 충돌을 피할 수 없다[10][31].

Ⅳ. PIPS(Privacy Information Protection System) 구현방안

앞에서 살펴본 바, 웹 시스템 환경에서 개인의 프라이버시를 보장하기 위해서는 법제도 및 기술적 보완이 요구된다. 본 논문에서는 이러한 요구사항을 PIPS(Privacy Information Protection System)에 적용하여 개인정보를 관리 및 보호한다. PIPS는 개인정보보호 시스템으로 서울시 산학연 협력사업 지원으로 수행중인 프로젝트이며, 본 연구는 PIPS 내의 일부인 정책 메커니즘 기능의 구현방안을 제안한다.

먼저, 개인정보보호 법이 다양한 분야에 산재되어 있으므로 법적 보호가 불안정한 상태에서 일관성 있는 보호 체계가 필요하다. 국제 표준 가이드라인인 OECD 프라이버시 원칙 대비 국내 개인정보보호 관련법을 적용하여 사용자에게 법적 보호 하에 안전한 서비스 이용을 제공한다. 즉 기존 정보보안 관리자에 의해 생성된 시스템 정책에서는 시스템의 보안 기능을 제공하지만 프라이버시 정의와 원칙에 기반으로 설정되지 않아 프라이버시를 위반할 수 있기에 이를 예방할 수 있다. 이러한 프라이버시 보호 정책은 자동화 시스템에 기반을 두어 이용함으로써 사용자는 자신의 정책을 관리하고 관리자는 국내 개인정보보호 법 개정 및 보완 시 정책을 변경 및 설정할 수 있도록 하여 상황에 즉시 대응할 수 있도록 한다. 시스템 관리자가 중앙에서 정책을 관리하면서 정책충돌을 예방하고, 만약 정책이 충돌하여도 시스템 적으로 우선순위를 검사하여 이를 방지한다.

또한, 개인정보보호를 상이한 그룹 간 연동성을 제공하기 위해 P3P와 APPEL을 이용한 표준화 기술로 정책을 제공한다. APPEL를 통해 프라이버시 정책 파일을 자동으로 비교할 수 있는 기능을 제공함으로써 인터넷 사

용자가 자신의 개인정보를 보호할 수 있도록 한다. 아울러, P3P 정책 표현에 역할기반의 접근제어의 표현을 추가하여 단순한 P3P 정책 표현을 확장한다.

효과적인 통제 및 제어를 위해 프라이버시 정책을 추가한 역할기반의 접근제어 모델을 적용하여 관리자의 보안 관리를 유용하게 하며 사용자에서 개인정보보호를 제공한다. 사용자의 역할을 신뢰정도 및 사회적 위치 등을 고려하여 구분하고 PMI의 확장필드를 이용하여 역할을 알 수 있게 한다. 또한 관리자와 사용자에게 시스템 인터페이스를 제공하여 정책 및 정보관리에 유연하게 대처할 수 있도록 한다.

Ⅴ. 개인정보보호 정책엔진 메커니즘

1. 메커니즘 개요

인터넷 발달로 인한 사이버 위협의 대안으로 현재 서울시 산학연 협력사업의 지원 사업으로 개인정보의 신뢰적인 관리 및 활용할 수 있는 PIPS 솔루션을 연구하고 있다. PIPS는 Privacy Information Protection System의 약자로 6가지 기능 (① 통합사용자 인증, ② 불법정보 오남용방지 및 접근제어 기능, ③ 개인정보보호 정책엔진 기능, ④ 안전성 기능, ⑤ 사용자 사전동의 및 Notice 기능, ⑥ 디지털 포렌식 기능) 기술 연구가 진행 중이다. 본 논문에서는 PIPS 내에 개인정보보호 정책엔진 메커니즘에 관해서 제안하며, 개인정보의 위험 분석과 개인정보보호 관련 연구 동향 및 기술현황을 바탕으로 국내 법 기반인 개인정보보호의 정책을 제시한다. 또한 프라이버시가 적용된 역할기반 접근제어의 정책을 설정하고, 설정된 정책에 따라 사용자의 개인정보 이용 및 활용에 대한 통제를 실시한다. 정의된 메커니즘의 구조를 기반으로 설계 및 구현에 대해 기술한다. 제안된 메커니즘의 구현은 활용화 방안으로 사례 적용하여 실제 환경에서의 응용방안이 가능성을 제시한다.

2. 메커니즘 구조

PIPS(Privacy Information Protection System) 개발의 전체 아키텍처 구성도는 <그림 5>에 나타낸다. 본 연구에서 개발한 개인정보보호 정책엔진은 크게 1) 프라이버시 기반의 접근제어(Privacy-based Access Control)와 2) 정책관리(Policy Management) 2개의 부분으로 구성된다. 접근제어 부분은 역할기반 접근통제(RBAC)를 통해 사용자를 역할로 구분하고 역할에 해당하는 권한을 사용자에게 부여한다. 개인정보를 관리하는 정책관리 부분은 프라이버시 보호 법 기반의 정의된 정책에 따라 개인정보 사용에 대한 허가/거부 여부를 결정한다. 또한, 사용자가 요청한 정책을 파싱하여 시스템 정책과 비교하고 그 기반으로 개인정보보호 및 관리를 수행한다. 접근 허가된 요청자의 요구에 의해 개인정보를 전송한다.

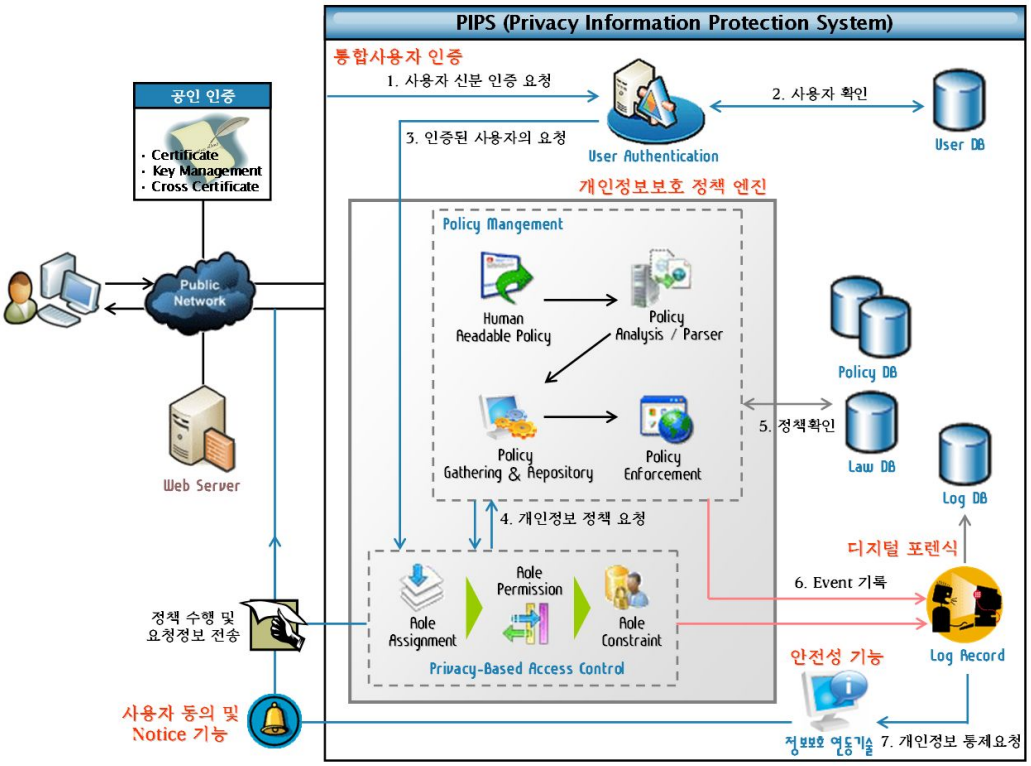

그림 8. PIPS 구성도

본 논문에서 제안한 개인정보보호 정책엔진 메커니즘은 자동적으로 개인정보를 관리하고 개인정보보호 정책 기반의 접근통제를 통해 사용자에게 안전하고 신뢰할 수 있는 서비스를 제공하는 것이 중요하다. 이 정책의 표현 및 수행을 위한 주요 구성 모듈의 기능은 다음 알고리즘으로 표현하였다.

Algorithm Privacy-Based Policy Management (*user, policy*)

```
1:  requestPolicy ← An array of strings provided by the request policy in PIPS
2:  purposePolicy ← An array of strings provide by the use-purpose policy in PIPS
3:  i = 1
4:  result = false
5:  check = false
6:  if login(user.id, user.pwd) = true then
7:      if user.auth = accept then
8:          // Human Readable Policy
9:          if action is happend then
10:             while i ≤ reqeustPolicy.length do
11:                 if reqeustPolicy[i].idx = action then
12:                     oecdidx = Oecd-Define-Table(reqeustPolicy[i].relatedOecd)
13:                     lawidx = Law-Define-Table(oecdidx)
14:                         if lawidx ≠ null then
15:                             Read-Policy(user, oecdidx, lawidx)
16:                         end if
17:                 end if
18:                 i++
19:             end while
20:         end if
21:         // Policy Analysis / Parsing
22:         if policy is requested then
23:             i = 1
24:             while purposePolicy[i].idx = user.policy.usepurpose do
25:                 parsingResult = Execute-Parser(puropsePolicy)
26:                 result = Execute-Policy-Match(parsingResult)
27:                 if result = true then
28:                     Policy-Gathering-Repository(result)
29:                     Policy-Enforcement(user, policy)
30:                     return true
31:                 else
32:                     return false
33:                 i++
34:             end while
35:         end if
36:     end if
37: end if
38: // Policy Gathering & Repository
39: Policy Gathering & Repository(policy) {
40:     policy = Select-PolicyInfo(user, appelContext, accessControl, condition)
41:     if Check-Policy-Collision(policy) = true then
42:         Insert-PolicyDB(policy)
43:         doc = APPELDocument-Convert(policy)
```

```
44:         return doc
45:     end if
46: }
47: // Policy Enforcement
48: Policy Enforcement(user, policy) {
49:     if policy is updated then
50:         check = Check-Update-Policy(policy)
51:         if check = true then
52:             Update-Policy(num, oecdTitle, lawTitle)
53:             result = View-Policy(policy)
54:             if result = true then
55:                 Insert-PolicyDB(num, oecdIdx, lawidx)
56:                 Send-EnforcementMsg(user)
57:             end if
58:         end if
59:     end if
60: }
```

3. 메커니즘 기능

1) 프라이버시 기반의 접근제어(Privacy-Based Access Control)

개인정보를 효과적으로 보호하기 위해서는 허가되지 않은 자(제3자)에게 개인정보를 이용 및 제공하지 못하도록 접근통제가 필요하다. 이를 위해 역할기반 접근제어의 구조를 확장하여 체계적인 통제방안을 제안한다.

제안한 메커니즘에서 정의하고 있는 역할은 자신의 개인정보를 소유하고 있는 개인사용자와 개인정보를 요청하는 업체 두 그룹으로 구분한다. 개인사용자는 자신의 정보를 관리하고 모든 이용이 가능하며, 업체는 기관 내 정보를 이용 및 수정할 수 있다. 업체의 그룹에는 비영리 기관(신뢰기관 - 국가산하기관, 정부)과 영리기관(비 신뢰기관 - 금융권, ISP 등)으로 계층적 관계를 설정한다(<그림 6> 참조).

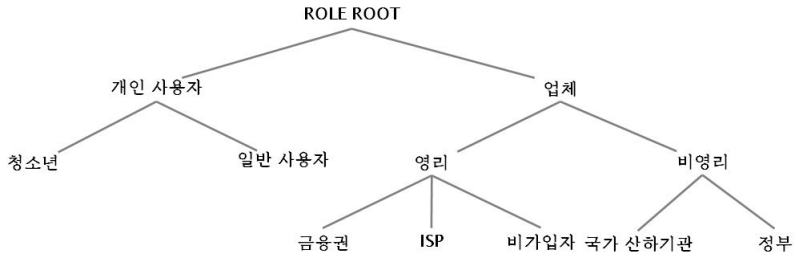

그림 9. 역할 분류

이와 같이 분류된 역할에 사용자를 할당하고 개인정보 이용에 대한 제한적인 권한을 부여한다. 프라이버시 보호를 위한 접근제어를 위해 기존의 역할기반 접근제어 모델에 이용목적, 조건에 따라 접근이 제한될 수 있도록 모델을 확장하여 접근통제를 한다. 즉, 인증을 통해 신분을 확인한 요청자를 적절한 역할에 할당하여 이용목적과 필요조건을 검사하여 제한된 권한을 요청자에게 부여한다. <그림 7>은 제안한 메커니즘에 적용하는 접근제어 모델이고, <표 10>는 접근제어 모델의 구성요소를 보여준다.

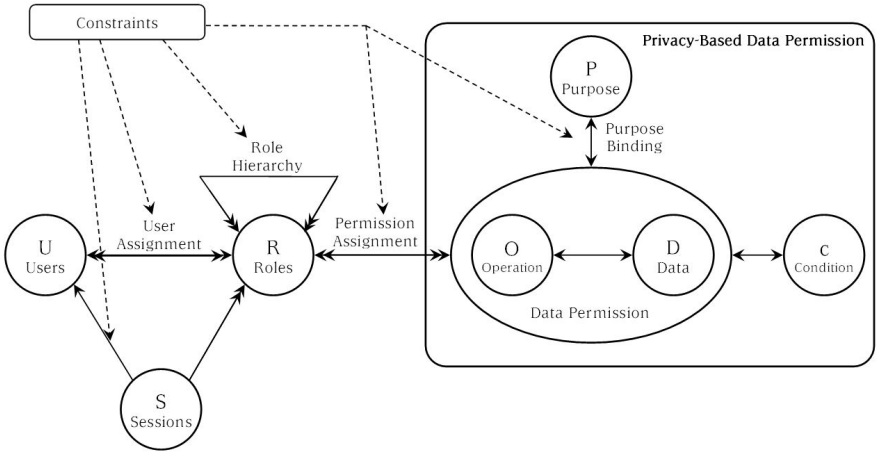

그림 10. 제안한 프라이버시 기반의 RBAC 모델

표 8. 접근제어 구성요소

요 소	설 명
Users	시스템을 이용하는 사용자 또는 요청자
Roles	시스템에서 신뢰그룹 및 사회적 직위 분류된 역할 정의 *Roles* = {*User*, *ISP*}
Sessions	동적으로 사용자가 역할에 할당될 수 있도록 관여
Operation	하나 혹은 그 이상의 보호된 객체들(개인정보)의 집합에 접근하기 위한 특정 접근방식 *Operation* = {*Create*, *Read*, *Write*, *Delete*}
Data	시스템에 의해서 관리되는 대상 (사용자의 개인정보) *Data* = {*UserBasicInfo*, *ConductInfo*, ... *CreditInfo*}
Purpose	요청자가 정보를 이용하는 목적들을 정의 *Purpose* = {*Marketing*, *Delivery*, ... *Payment*}
Condition	데이터에 접근하기 위해 필요한 조건 *Condition* = {*AgeLimit, OwnerCertify, ... ParentsConsent*}
Constraints	사용자가 역할에 할당되는 조건, 역할 개인정보 권한 할당, 정보 이용에 필요한 제약조건 등

U는 사용자 또는 요청자로 시스템에 접근 시, User Assignment로 R에 할당된다. R은 위에 정의한대로 역할이 구분되며, 역할에 배정된 권한들 사이에 Role Hierarchy 관계를 가지므로 권한부여가 상속관계를 갖는다. R의 Permission Assignment로 사용자는 접근 기능 및 권한을 배정받는다. 접근

방식은 이용연산 O를 통해 개인정보 데이터 D를 접근할 수 있고, 이를 Data Permission이라 한다. D에 접근 시, 개인정보를 이용하는 목적 P를 확인하고, 필요한 조건 C를 검사하여 접근의 허가/거부 여부를 확인한다. 즉, 요청자의 요구에 따른 개인정보 접근은 요청자의 역할 및 요청목적, 조건에 따라 접근이 제한되고 이용할 수 있는 권한이 달라진다.

2) 정책관리(Policy Management)

① Human Readable Policy

Human Readable Policy를 통해 체계적인 분류로 정책을 설정하고 기술적으로 표현하여 개인정보보호 정책을 수행할 수 있도록 하는 기능이다.

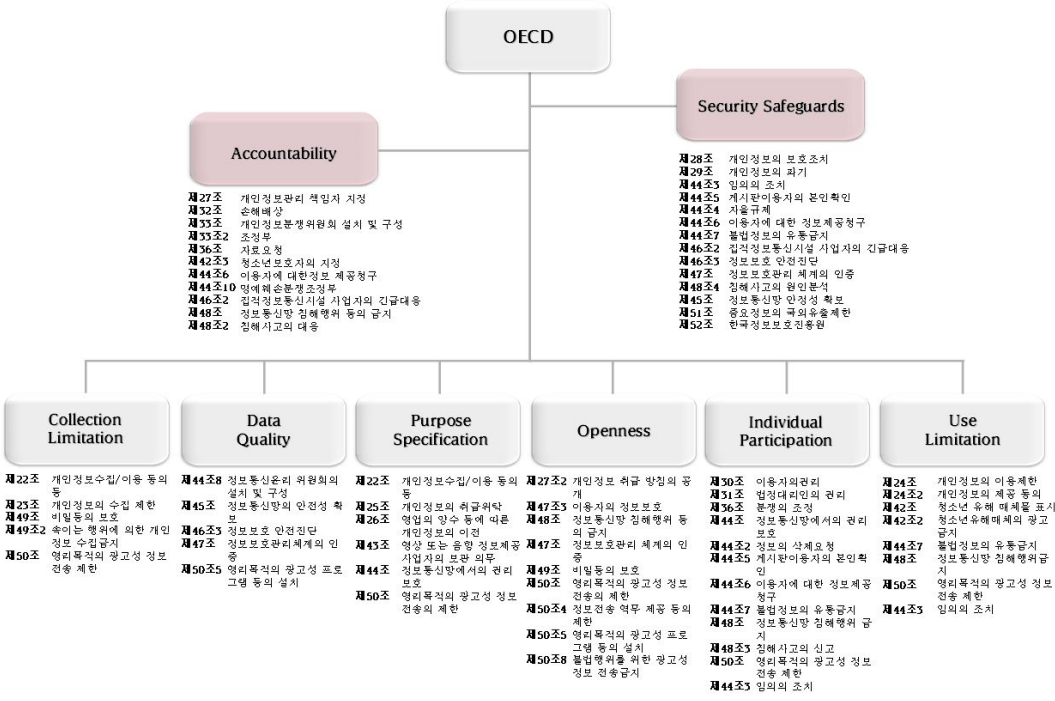

그림 11. 개인정보보호 정책 분류표

국내 개인정보보호법규는 정보통신망을 이용한 대량의 개인정보 수집 및 취급 등이 용이해지면서 정보통신 서비스 이용자의 자기정보통제권이 보장

될 수 있도록 개인정보보호 법안이 추진되고 있다. 국내 관련 추진 법안의 체계적인 분류를 위해 글로벌 표준인 OECD의 “프라이버시보호와 개인정보의 국제적 유통에 관한 가이드라인 8원칙”을 기반으로 국내 법(정보통신망 이용촉진 및 정보보호 등에 관한 법률)을 활용하여 <그림 8>과 같이 개인정보정책 분류표를 작성하였다.

이렇게 작성된 개인정보보호 정책 분류표를 기반으로 개인정보 수집·공유·유통·분배에 대한 프로세스 발생 시 정의된 정책에 의거하여 규정 및 처벌을 제시할 수 있도록 <그림 9>와 같이 구성한다.

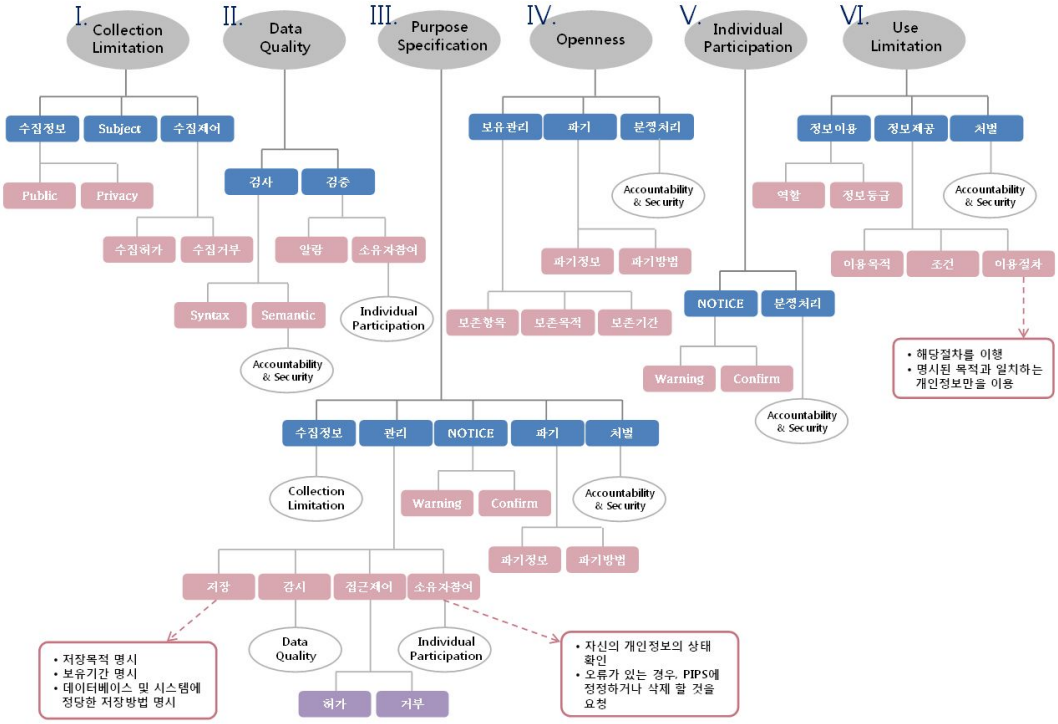

그림 12. OECD 기반의 개인정보보호 정책 관리 분류표

이는 OECD의 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, 책임&안전성에 관련된 처벌법에 따

라 이행 할 수 있다. 세부적으로 살펴보면, 1) 수집 제한(Collection Limitation)은 무분별한 개인정보 수집을 제한하는데 목적을 두고 있어서 어떠한 개인정보도 합법적이고 공정한 절차에 의해서 수집되어야 하며, 수집정보, 주체(역할), 수집제한으로 구성한다. 2) 데이터 정확성(Data Quality)은 이용목적에 필요한 범위 안에서 정보 내용이 정확하고 최신의 것을 유지하기 위해 검사 및 검증을 통해 정보의 완전성을 보호한다. 3) 목적 명시(Purpose Specification)는 개인정보를 보호하기 위해 수집정보 및 개인정보관리를 명확히 명시해야하며, 개인정보이용 후 정보를 파기시켜 오용이나 불법복사 등의 위험을 예방하고 불이행시 처벌규정에 따르도록 구성된다. 4) 공개(Openness)원칙은 개인정보와 관련된 개발 및 실시, 정책에 대해서는 일반적인 공개정책을 취하여야 한다. 즉, 무단으로 개인정보를 수집 및 오남용 방지를 위해 정보보유 관리 및 정보파기를 지정하고, 불이행시 분쟁해결을 통해 관련법규를 따르도록 구성하였다. 5) 개인 참여(Individual Participation)는 자신의 정보를 확인하고 접근할 수 있는 권리를 갖는 '프라이버시권의 보호' 수단의 일부로 Notice 기능과 권리를 보호하기 위한 분쟁처리로 구성된다. 6) 이용제한(Use Limitation)원칙은 정보주체의 동의가 있는 경우이거나 법률의 규정에 의한 경우가 아니면 개인정보 이용이 제한된다. 정보이용을 제한하기 위해 역할 및 정보등급 별로 이용제한을 구성하고, 제공시 목적과 조건에 따라 이용절차에 의해 처리될 수 있도록 구성하였다.

② Policy Analysis / Parsing

정책을 기술적으로 적용 및 설정하기 위해 파싱/분석하는 기능이다. 개인정보는 국내관련 법률에서 규정하고 있는 정보통신서비스제공자의 전자적 게시에 대한 의무사항을 반영한 "개인정보보호 정책 설정 및 협상규격 (한국정보통신기술협회, 2007)"기반으로 개인정보항목을 설정한다. 이러한 개인정보항목의 접근제어를 위해서는 중요도에 따라 데이터의 보호가 필요하

다. 데이터에 대한 접근은 주체와 객체가 갖는 보안 등급의 정의를 통해 결정된다. 이는 개인정보의 민감한 중요도에 따라 보안등급이 구분되며 시스템 사용자가 설정한 정책 공개등급을 통해 자신의 정보를 이용할 수 있는 요청자의 역할이나 권한 및 자신의 접근권한이 설정된다. 기본적으로 개인정보는 필수항목과 선택항목으로 구분하며, “개인정보의 안전한 수집, 저장 및 관리, 이용, 제공, 파기를 위한 개인정보관리 모델 연구 (한국정보보호진흥원, 2006)”문서 기반으로 정보의 보안등급을 <표 9>와 같이 P1 – P5로 나누었다.

표 9. 보안등급

등급	항목	기밀등급 / 공개등급
P1	◆ 패스워드 ◆ 수입 ◆ 장애여부 ◆ 결제정보 (카드회사, 카드번호)	가장 높은 레벨로 정보를 이용할 수 있는 요청자의 권한도 가장 제약적이다
		가장 높은 공개등급으로써 자신의 개인정보 소유주만이 정보이용 가능하다.
P2	◆ 신원확인번호 (주민등록번호, 운전면허번호, 여권번호) ◆ 재정정보 (거래은행, 계좌번호)	정보기밀의 높은 레벨에 해당하며, 민감한 정보로 구성
		신뢰기관 역할 이상이 개인정보이용이 가능하다. 하지만 민감한 정보 이용시에는 소유주의 동의 및 인증확인을 받아야 한다.
P3	◆ 연락처 (이메일, 집전화번호, 핸드폰번호, 집주소) ◆ 학위 ◆ 혈액형	필요 연락처 등의 정보에 대해서 제한할 수 있도록 구성
		중간 공개등급으로 권한이 낮은 가입자들은 이용 불가. 권한이 높은 등급이면 개인정보 수집 및 이용이 가능하다.
P4	◆ 공개등급 ◆ 회사정보 (부서, 전화번호, 주소)	비가입자에게 정보가 제공되지 않고 요청자 권한에 따라서 정보 이용이 가능
		사용자가 설정할 수 있는 낮은 등급으로 권한이 낮은 자들이 민감한 정보 이용시 사용자의 동의가 필요하다
P5	◆ 아이디 ◆ 이름	가장등급이 낮은 레벨로 비가입자에게도 공개될 수 있는 정보로 구성
		공개등급을 정의하지 않을 시에 디폴트로 적용된다. 이는 가장 기본적인 공개등급으로 비가입자를 제외한 나머지 가입자들이 사용자에게 개인정보를 요청 및 이용 가능하다.

위의 보안등급별로 구분한 항목 기반으로 개인정보를 이용하는 목적을

정의한다. 요청자가 개인정보를 요청하면 메커니즘은 자동적으로 정의된 이용목적을 비교하여 개인정보의 접근여부를 확인한다. 이용목적에 따라 민감한 정보를 다루는 목적과 일반적인 정보를 다루는 목적 크게 2 부분으로 구분한다.

- Sensitivity

  민감한 정보를 다루는 목적들로 구분하며, 지불정보를 필요로 하는 결제, 계좌번호 및 금융정보를 필요로 하는 환불, 개인연락처가 필요한 구매와 배송, 교환 등의 목적으로 분류된다.

- General

  일반적인 정보만을 다루는 목적들로 기업의 광고나 기본적인 정보만을 제공하는 마케팅, 연락처와 주민번호를 입력하지 않고 필요한 정보만을 제공하는 이벤트 등의 목적으로 분류한다.

표 10. 이용목적 분류

분류	목적	항목
Sensitivity	결제	카드회사, 카드번호, 유효기간
	환불	거래은행, 계좌번호
	구매	이메일, 집전화번호, 핸드폰번호
	배송	핸드폰번호, 직장주소, 집주소
	교환	이메일, 집전화번호, 핸드폰번호
General	광고	이메일
	마케팅	성별, 나이
	이벤트	이메일

<표 10>은 쇼핑몰 사례 중심으로 이용목적을 정의하였다. 이렇게 분류된 목적을 통해 요청자가 개인정보를 요청하면 시스템에서 목적에 맞추어 필요한 개인정보만을 제공하게 된다.

③ Policy Gathering & Repository

APPEL(A P3P Preference Exchange Language, W3C) v1.0 기반으로 국내

관련 법규 반영한 정책 구문 설정 체계와 간결한 정책, 데이터 스키마의 규격을 정의하였다. 이는 APPEL로 표현할 수 있는 개인정보 데이터와 정책을 설정한다. 즉, 해당 요청목적에 대해서 접근제어를 하는 방법과 APPEL로 표현하는 방법을 설정하며"목적"정책에 따라 어떠한 정보를 누가, 어떤 목적 하에 접근할 수 있는지를 표현하고 접근제어를 위해 이용연산과 정보에 대한 허용여부 및 필요조건을 정의한다. 이렇게 구성된 개인정보보호 정책을 시스템적으로 관리자가 추가 및 수정 가능하도록 설계한다. 또한, Policy Analysis / Parsing에서 개인정보보호 정책의 설정과 파싱을 통해 정책을 분석한 후, 사용자가 개인정보 접근요청 시 사용자 정보와 개인정보의 사용목적, 요청할 개인정보 등을 P3P의 정책설정 언어인 APPEL로 자동 변환하여 적용한다.

<그림 10>에서 마케팅 목적 내에 요청자 정보와 APPEL로 정의되는 목적 및 이용할 수 있는 개인정보 항목 등 정책을 설정한다.

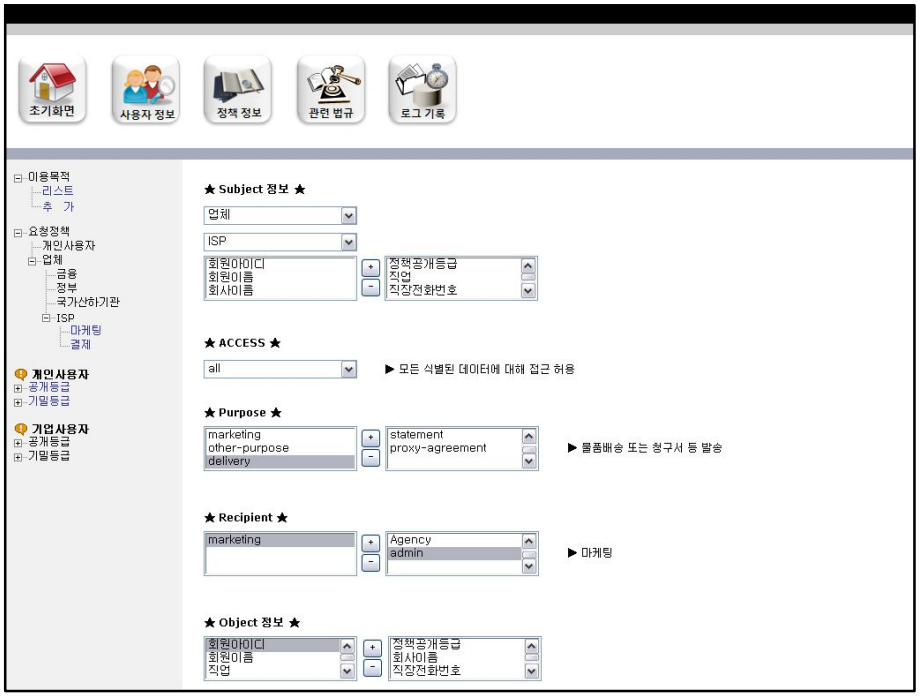

그림 13. 마케팅 목적 내 정책 설정 예

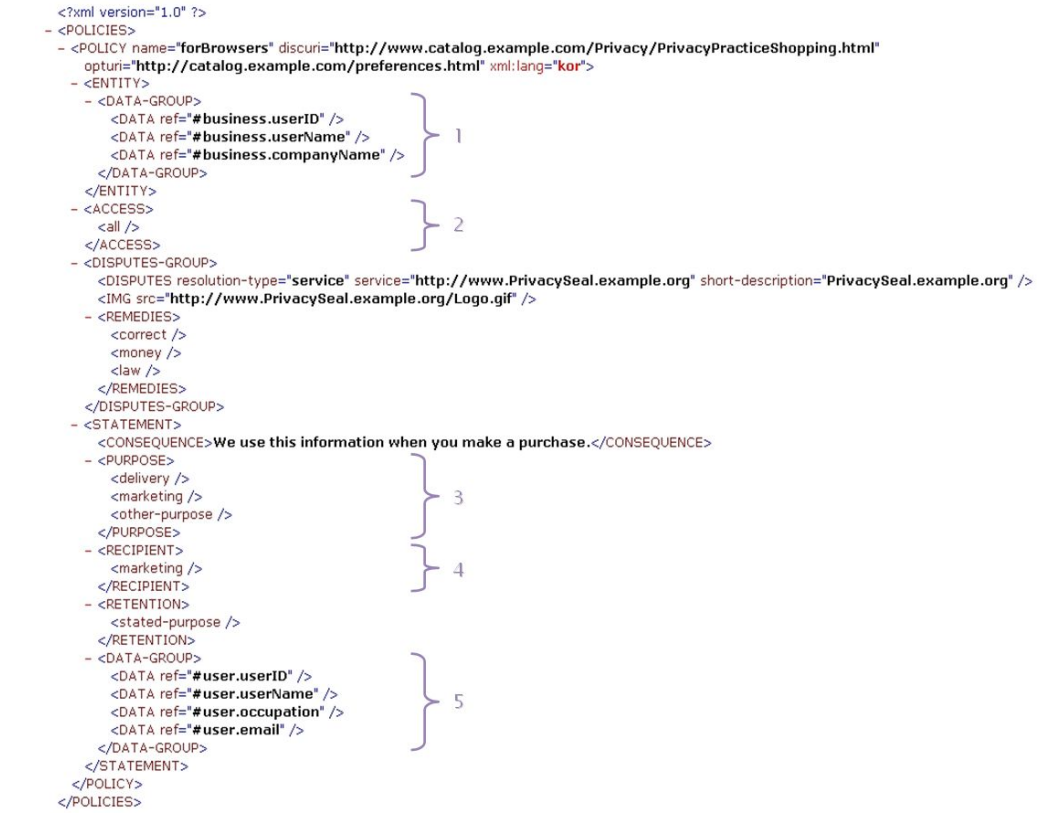

그림 14. APPEL 문서 변환 예

정책을 추가하면 <그림 11>과 같이 APPEL 문서로 표현된다. (1)에서 요청자의 정보를 설정하며, (2)의 <ACCESS>에서 접근제어를 설정한다. (3)에서 APPEL 정책 문법으로 표현되는 <PURPOSE>를 통해 이용목적에 대해 정의하고, (4) <RECIPIENT>로 요청자가 접근할 수 있는 목적의 권한을 설정하며, 적합하다면 (5) <DATA-GROUP>에서 정의된 개인정보 항목이 이용이 가능하다.

④ Policy Enforcement

시스템 내에서 정보가 변경되거나 추가, 삭제와 같은 사건발생 시 관련 처벌법규에 따라 대응한다. 즉, 해당 절차를 이행하지 않았거나 명시된 목적에 불일치하는 행위, 정보 누출 등의 위반이 발생할 경우 관련 법제도를

통해 책임추적성 역할을 하여 관련 벌칙 및 처벌이 이행된다. 또한, 현행 법제도의 보완 및 개정 시 관리자가 시스템에 적용할 수 있도록 <그림 12>와 같이 개인정보법규 시스템 적용화면을 제공한다.

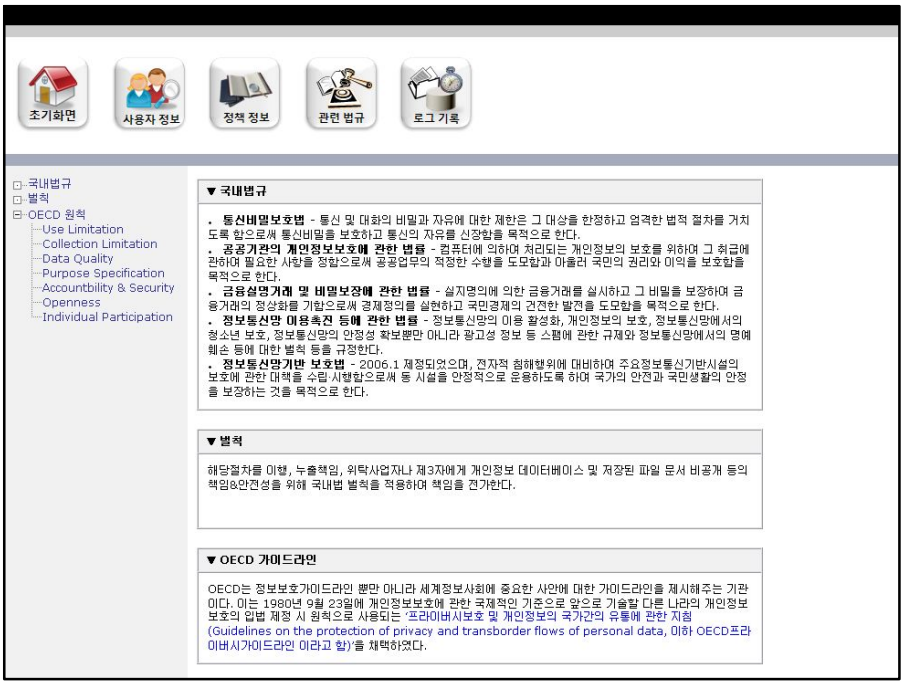

그림 15. 관련 개인정보법규 시스템 적용화면 예

Ⅵ. 시스템 설계 및 구현

1. 데이터베이스 설계

개인정보를 안전하고 효율적으로 관리하기 위해서 “개인정보 생명주기별 보안 관리모델 (한국정보통신기술협회, 2007)”표준을 기반으로 개인정보보호 정책을 제시하여 OECD 원칙에 관련 법규를 적용하고 정책 DB를 설계한다. <그림 13>은 개인정보보호 정책엔진 메커니즘 내의 정책 데이터베이스의 구조 및 관계를 나타낸다.

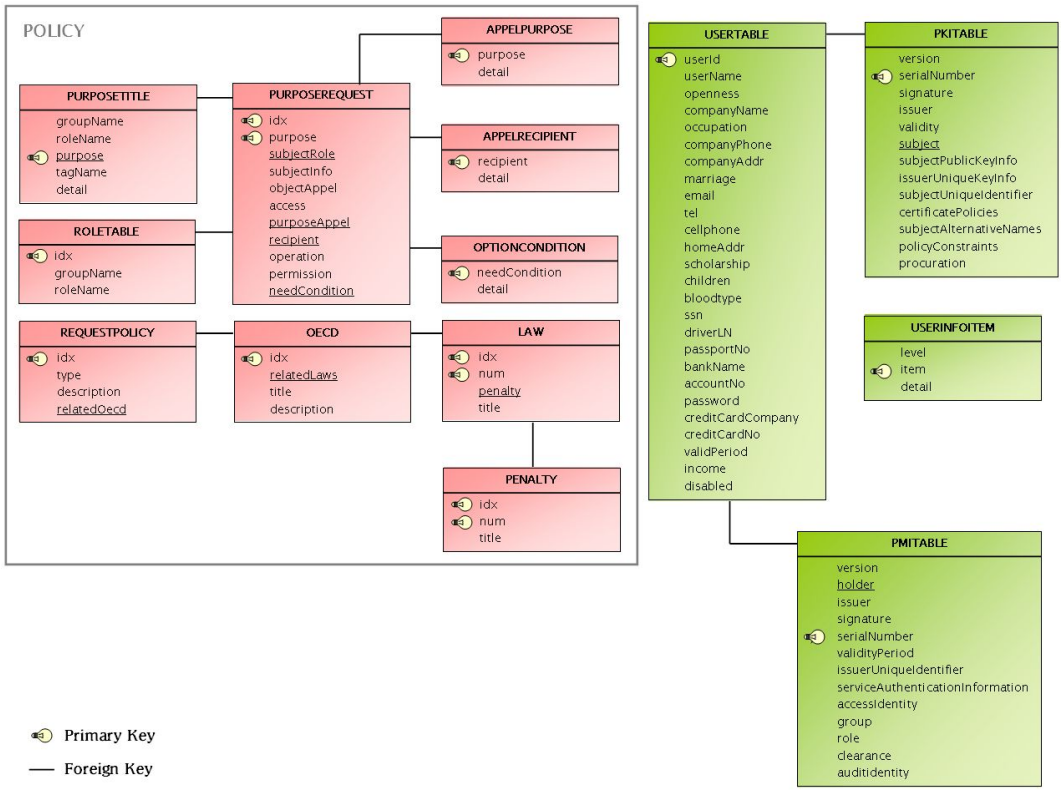

그림 16. 데이터베이스 구조 및 관계

정책 관련 테이블은 10개 테이블로 구성된다. 이용목적에 따라 정책 정보

를 가지고 있는 PurposeRequest와 PurposeRequest내 APPEL 정책을 매치하는 AppelPurpose, AppelRecipient, 필요한 조건을 정의하는 OptionCondition 테이블이 존재한다. 이는 APPEL v1.0에서 정의하고 있는 APPEL정책을 이용하기 위해 데이터베이스 테이블로 저장하여 이용할 수 있도록 한 것이다. 역할별로 요청 및 접근 제한할 수 있는 RoleTable을 정의하여 그룹 및 역할이 저장되어 그에 해당하는 권한 및 책임이 적용되도록 한다. 요청자의 요청정책에 따라 RequestPolicy를 통해 어떠한 OECD 원칙 하에서 관련 법규가 적용되는지 테이블에 저장되어 관리되도록 구현되어있다. 또한 개인정보보호를 위한 정책은 관리자 인터페이스를 이용해서 관리되며 관리자가 정책 추가 및 수정, 삭제하면 테이블 내 데이터가 업데이트 된다.

개인정보를 저장하는 테이블은 사용자 인증을 위해 PKI와 PMI가 관련되어 저장되며 항목의 기밀보안등급은 UserInfoItem에 정의되어있다.

2. 시나리오

PIPS는 앞서 제시한 대로 개인정보보호 시스템 솔루션으로써 본 논문에서 제안한 개인정보보호 정책엔진 메커니즘 기능이 포함되어 있다. 본 장에서는 PIPS 기반으로 웹 환경에서 사용자가 쇼핑몰에서 제품구입 시 필요한 사용자 정보만을 제공할 수 있도록 개인정보보호 정책을 설정하여 사용자의 프라이버시를 보호하는 시나리오를 나타낸다. 즉, 어떤 사용자가 쇼핑몰의 제품을 구입요청 했을 때 쇼핑몰은 구입·결제에 해당하는 사용자의 정보를 얻기 위해서는 PIPS Server에 결제이용을 위한 개인정보를 요청하면 PIPS Server는 개인정보보호 정책에 맞춰 개인정보 제공의 허용/거부를 할 수 있다. 이러한 결제정보 제공요청을 위한 시나리오는 <그림 14>로 표현된다.

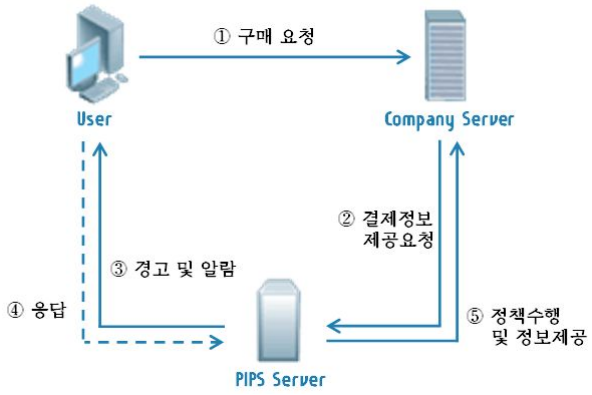

그림 17. 결제정보 제공요청 시나리오

앞에서 제안한 개인정보보호 기반의 쇼핑몰 서비스 제공 적용가능성을 나타내기 위해서는 User와 쇼핑몰은 PIPS에 가입된 자임을 가정하고, User는 역할기반 접근제어를 통해 '일반사용자'로 할당되며 쇼핑몰은 'ISP(Internet Service Provider)'역할로 할당된다. 또한 결제이용에 대한 정책은 시스템에 정의되어져 있는 상황에서 시나리오를 전개한다.

[1 단계] User는 쇼핑몰에서 제품을 구입 요청한다.

[2 단계] 쇼핑몰은 구입요청을 처리하기 위해 PIPS에게 User의 결제정보를 요청한다. PIPS는 사용자의 정책공개등급을 검사하여 적합한 사용자인지 확인하고, 동시에 사용자의 결제정보가 있는지 확인한다. 결제정보가 존재한다면 OECD의 "Use Limitation"원칙에 의거하여 이용목적에 대한 정책을 검사하고 필요조건을 확인한다.

[3 단계] 요청정책이 적합하다면, 결제정보를 요청하기 위해 OECD의 "Individual Participation"원칙에 의거하여 User에게 사용자 동의 메시지를 보낸다.

[4 단계] User는 결제정보 이용에 대한 동의 응답을 한다.

[5 단계] PIPS는 쇼핑몰에게 결제정보를 XML 파일로 변환하여 사용자 정보를 제공한다.

3. 프로토타이핑 – 화면구성

개인정보보호 정책엔진 메커니즘은 Window XP 운영체제에서 구현되며, 웹 환경은 Apache HTTP Server 2.2.2를 지원한다. 언어는 웹 PHP 5.1.4와 C++을 사용하였으며 DBMS는 MySQL 5.0을 사용하고, Microsoft Visual Studio 2005 Tool을 이용하여 구현하였다. 이 기반으로 관리자가 이용할 수 있는 인터페이스 화면을 구성한다. 관리자는 사용자 정보에 대해서 모든 정보 접근이 가능하도록 하고 읽을 수 있게 한다. 또한 정책정보와 국내 관련 법규를 추가 및 변경, 삭제가 가능하여야 하며, 개인정보의 누출사고 발생 및 사고 대응을 위한 인터페이스 구성을 갖는다. 화면구성의 상세설명은 다음과 같다.

- **사용자정보** : 시스템에 가입된 사용자의 역할 및 권한을 확인하며, PKI와 PMI 정보에 접근이 가능하고, 사용자 개인정보에 대해서도 보여준다. 대신 관리자는 사용자 정보에 관해서 추가 및 변경, 삭제는 불가능하다.
- **정책정보** : 시스템 내 정책정보에 대해서 추가, 수정 및 삭제가 가능하도록 한다. 목적별 요청정책과 사용자의 공개등급, 개인정보의 기밀등급을 변경할 수 있도록 한다.
- **관련법규** : OECD의 원칙 기반으로 시스템에서 적용되는 관련법규를 설정한다.
- **로그기록** : 사용자의 행동 및 Notice 기능에 관한 로그기록과 요청자가 개인정보를 요청한 로그기록에 대해서 알 수 있도록 한다.

본 연구에서는 상기 PIPS가 관리자에게 제공하는 인터페이스 구성 중 정책정보와 관련법규를 통해 개인정보보호 정책에 접근한다.

1) 정책정보

관리자가 이용하는 개인정보보호 정책정보 화면은 크게 두 부분으로 시스템 정책관리 메뉴와 메뉴에서 선택한 요소가 정의된 정책 및 리스트를 보여주는 보기 화면으로 구성된다.

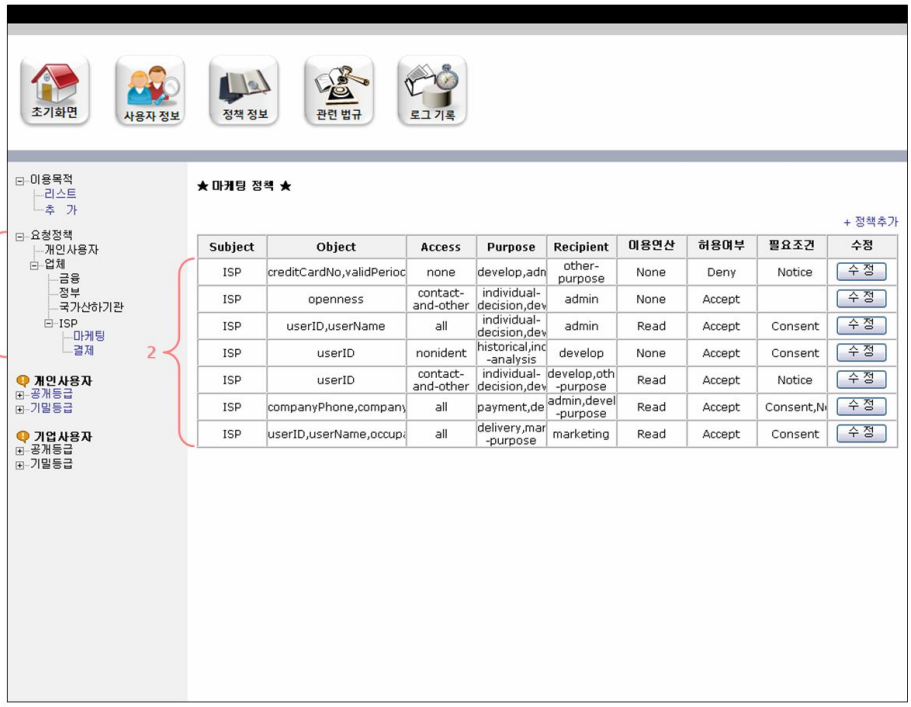

그림 18. 정책정보 내 마케팅 요청정책 화면 예

<그림 15>는 정책정보에서 요청정책에 관한 화면을 보여준다. (1)은 정책을 역할별로 구분하여 정책 설정한 것을 보여줄 수 있도록 하며, 해당 목적에 정의된 정책을 선택하였을 때, (2)와 같이 설정된 정책이 리스트형태로 나타난다. 정책 리스트는 누가(Subject), 어떠한 개인정보(Object)를 접근(Access)할 때, 조건(필요조건)이 무엇이고 허용(허용여부)이 가능한지 등을 확인할 수 있다. 정책을 추가 및 수정할 시, <그림 16> 화면이 보여진다. 요청자의 정보(역할 및 신상정보)는 (1)에서 정의되며 APPEL 문서로 정의된

정책 설정은 (2)에서 Access, Purpose 및 Recipient로 표현된다. APPEL의 내부적인 태그설명은 클릭 시 오른쪽에 설명되어진다. (3)은 이용할 수 있는 개인정보항목이 정의되고, (4)를 통해 허용여부 및 이용연산과 정책이 적용되기 위해 필요한 조건으로 접근제어가 설정된다. 이후, 정의된 정책은 <그림 17>의 APPEL 문서로 자동 표현된다. 이는 개인정보보호 정책 분류표를 기반하여 자동적으로 문서를 변환하며, Policy Analysis / Parsing에서 표준 기술인 APPEL를 통해 시스템은 사용자의 권한 및 이용목적을 검사하고 사용자가 설정한 정책과 시스템 내에 정의한 정책을 비교하여 적합한지 확인한다.

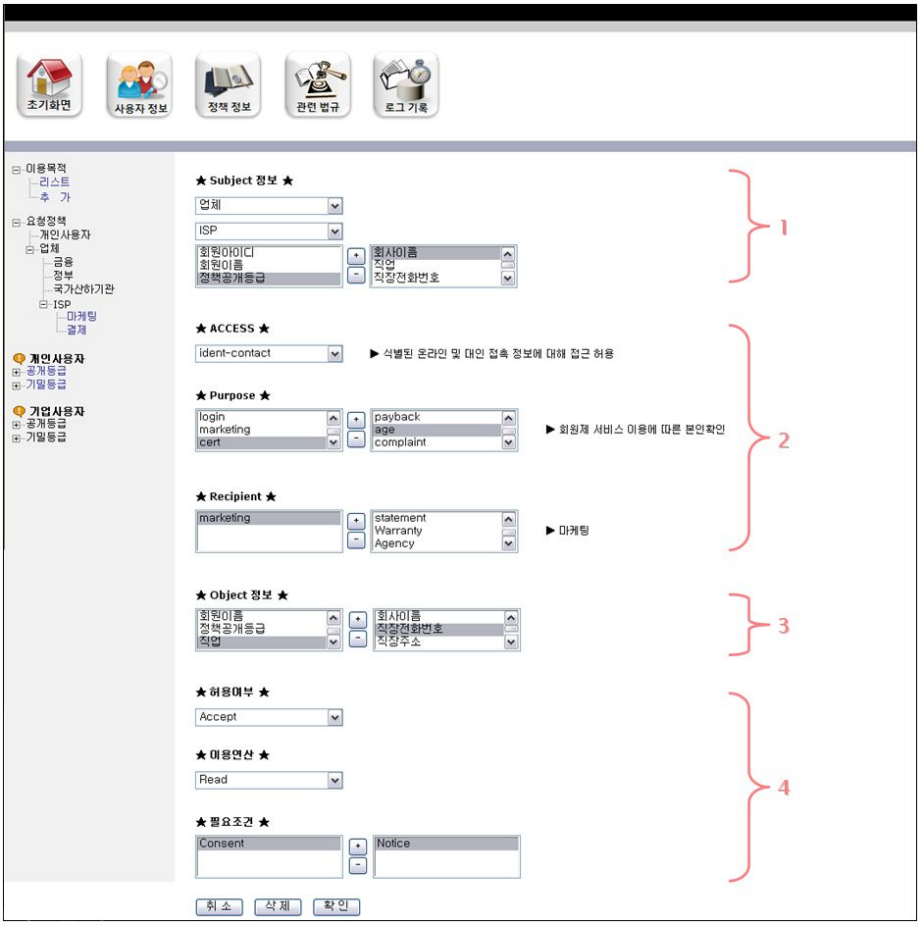

그림 19. 정책정보 내 마케팅 요청정책 추가 및 수정화면 예

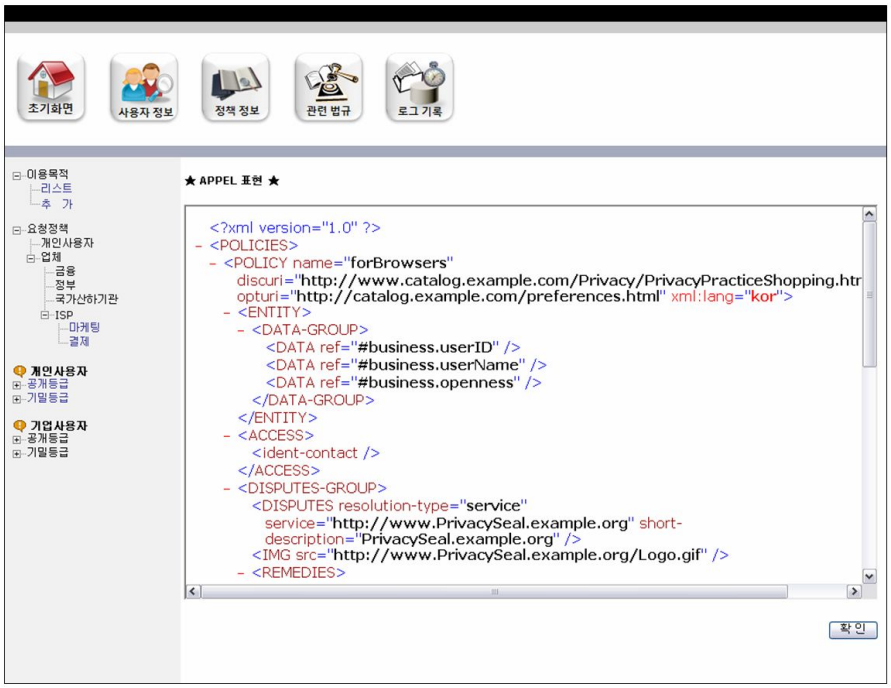

그림 20. APPEL 문서 표현 예

그림 21. 정책정보 내 공개등급 정책화면 예

<그림 18>은 시스템 관리자가 정보이용의 공개등급 정의를 설정한다. 사용자는 공개등급 설정에 따라서 접근할 수 있는 요청자의 역할 및 이용목적이 달라진다. 공개등급 정책의 정의는 시스템 관리자가 추가 및 변경이 가능하다. (1)은 공개등급 설정을 개인정보보호 정책 기반으로 보안등급 구분한 것을 Default인 D등급부터 가장 높은 VH등급으로 표현한 것이다. 해당 등급을 선택하면 (2)와 같이 정의되어있는 정책이 리스트별로 표현된다. 리스트 세부내용을 보면, 자동으로 부여되는 인덱스 값(IDX)으로 등급이름을 가지며 정책을 식별할 수 있도록 한다. 또한, 정보이용이 가능한 사용자 역할(이용자)과 접근할 수 있는 개인정보항목(Object) 및 접근할 때 이용 가능한 연산이나 필요조건과 허용여부에 따른 정책이 정의된 것을 볼 수 있다. 정책추가를 통해 관리자는 정책을 추가할 수 있고 정의된 정책은 수정이 가능하다.

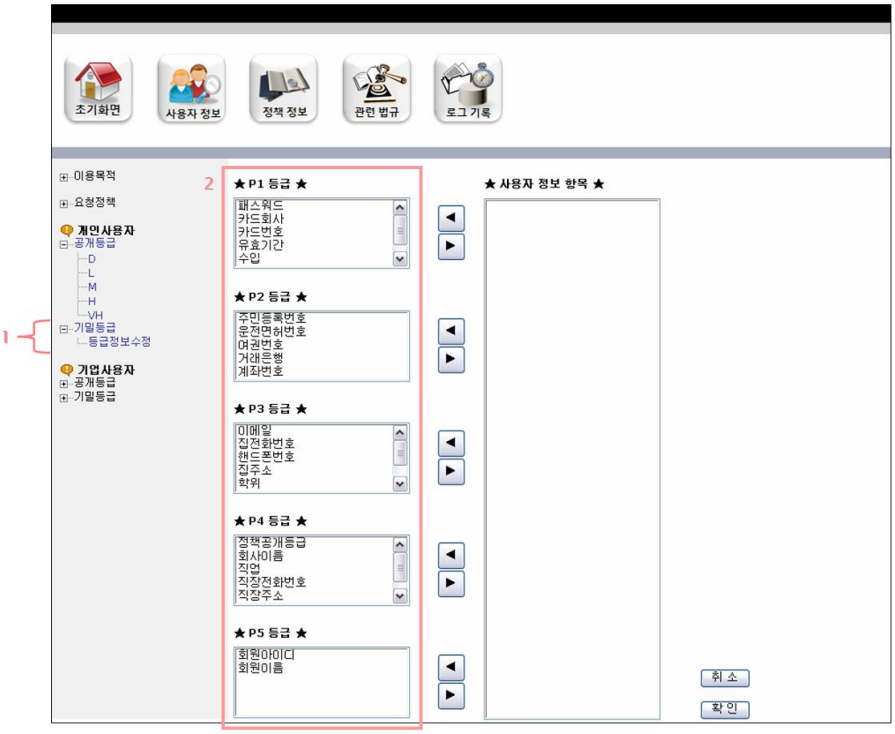

그림 22. 정책정보 내 기밀등급 정보수정화면 예

<그림 19>는 기밀등급에 관한 인터페이스의 구성이다. (1)은 기밀등급이 어떻게 정의되어 있는지 화면으로 보여주고 기밀등급정보 수정이 가능하도록 메뉴를 제공한다. (2)는 등급정보를 수정할 때 보여주는 화면이다. 이는 중요도에 따라 개인정보 항목을 P1등급에서 P5등급까지 관리자가 설정가능하다. P5등급은 누구나 접근할 수 있는 개인정보 항목으로 구성되며 P1등급은 가장 중요하고 민감한 정보로 구성하도록 관리자가 정의한다.

2) 관련법규

OECD 원칙 기반으로 국내 법률을 설정하여 시스템 정책을 관리하는 부분이다. OECD 8가지 원칙에 따라 국내 현행 법률을 설정하고, 관련 처벌법규도 정의할 수 있다. 국내 법률이 개정·보완 시 시스템 관리자가 수정 가능하도록 인터페이스를 제공한다.

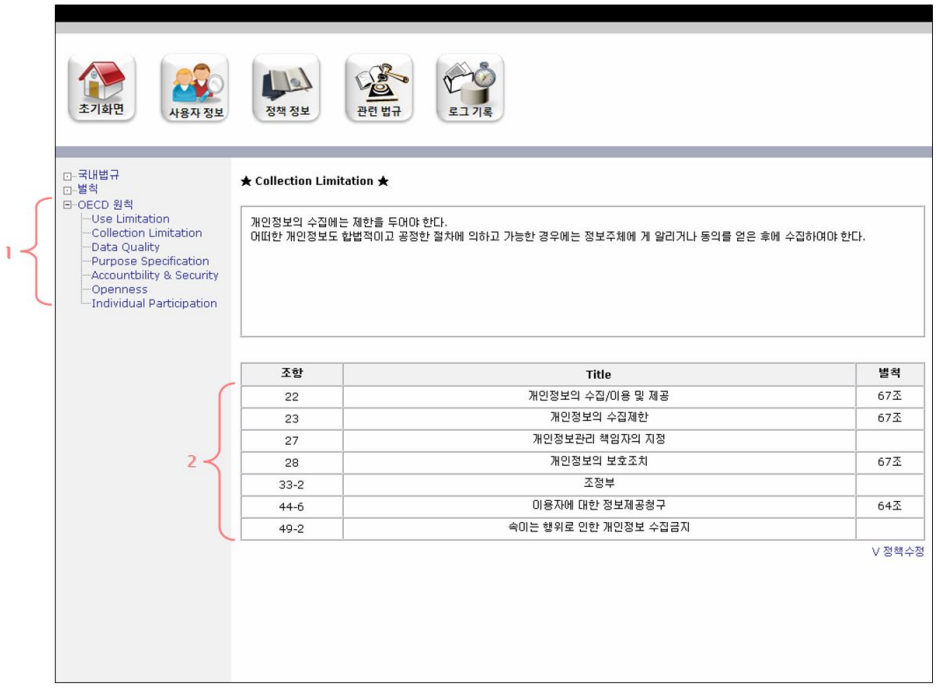

그림 23. 관련법규 내 OECD 원칙에 적용된 법률화면 예

<그림 20>은 OECD 기반의 적용된 국내 법률을 보여주는 화면이다. (1)은 OECD의 8가지 원칙 중 책임과 안전성을 제외한 6가지 원칙에 대해서 제시되어 있고, 해당하는 OECD 원칙의 상세설명과 함께 이 원칙의 국내 개인정보보호 법률이 (2)와 같은 리스트로 정의되어 있다.

그림 24. 관련법규 내 OECD 원칙에 적용된 법률 수정화면 예

'정책수정'을 클릭하면 <그림 21>과 같이 관리자가 직접 개인정보보호 관련법을 해당 OECD 원칙에 추가 및 삭제할 수 있다. 이를 통해 현행 개인정보보호 법규가 개정되면 즉시 대응 가능하도록 하며, 개인정보 이용 및 수집 등에 대한 프로세스 발생 시 정의된 정책에 의거하여 규정 및 처벌을 제시할 수 있도록 구성한다.

Ⅶ. 기대 효과

본 연구에서 국내법 기반 개인정보보호 정책엔진 메커니즘에 대한 제안으로 국내외 개인정보보호에 관한 연구들과 본 연구에서 제안한 시스템을 비교분석하여 효율성을 추정하였다.

표 11. 관련연구와 제안한 PIPS 비교

			PORTIA	PISA	PRIME	PiMI	IDMS	PIPS
환경	유선 환경		∨	∨	∨		∨	∨
	무선 환경				∨	∨		∨
관련 기술	개인정보보호 표준화기술	P3P	∨		∨	∨		∨
		EPAL						
		XACML			∨		∨	
		APPEL						∨
	접근제어	기존의 접근제어	∨		∨		∨	
		역할기반 접근제어						∨
	PET	사용자인증	∨	∨	∨	∨	∨	∨
		암호화	∨		∨		∨	∨
		익명성			∨	∨		∨
	Notice 기능					∨		△
	Monitoring 기능		∨	∨	∨	∨	∨	△
관련 제도	프라이버시 정책 제시		∨	∨	∨	∨	∨	∨
	국제 표준 가이드라인	OECD		∨				∨
		EU			∨	∨		
		APEC						
	현행 개인정보보호 법 적용			∨	∨	∨		∨
	법 관련 기술구현			∨				∨
기타	처리방식	중앙처리			∨		∨	∨
		분산처리	∨	∨		∨		
	사용자 인터페이스 제공			∨	∨		∨	∨
	관리자 참여		∨		∨	∨	∨	∨
	정책 자동화 기능			∨	∨		∨	∨
	정책 충돌 해결		∨				∨	△

※ ∨: 구현 △: 향후 추가구현

<표 11>은 대표적인 개인정보보호 관련 연구와 본 논문에서 제안한 PIPS를 개인정보보호 관련제도 및 기술 관점에서 비교 분석하여 간략히 정리한 표이다.

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. 그러나 제시한 프라이버시 정책 제도는 현행 개인정보보호 법 관련 대비하여 체계적인 기술적 구현이 미흡하고, 기존의 접근제어의 이용으로 동적인 상황에 즉각 대응하기 어렵다. 특히, 현재 국내기준에 맞춰진 프라이버시 법 기반의 개인정보 관리 기술이 미비하여, 서비스 이용 시 개인정보보호의 보장이 미흡하다.

이러한 문제점을 고려하여 본 논문에서 제안한 메커니즘은 국내 개인정보보호 관련법을 기술적으로 적용 가능하도록 구현하였다. 국내에서 개인의 권리 이익을 보호하기 위해 개인정보보호 관련법을 체계적인 정책으로 제시하여 이를 기술적으로 적용 및 설계한다. 사용자는 프라이버시 보호 하에 안전한 서비스를 제공받고, 개인정보 요청자는 법률 기반에서 정보수집 및 정보 활용이 가능하다. 이를 통해 규정위반 시 법적 근거를 제공함으로써 시스템적으로 법률 기반의 개인정보를 보호할 수 있다.

또한 개인정보보호 정책을 효율적으로 적용하기 위해 역할기반 접근제어 모델을 이용함으로써 권한 관리가 용이하고 조직 내 보안정책 표현이 유연하다. 이는 사용자를 역할에 할당함으로써 관리자에게 사용자 관리를 용이하게 해주고 제한적인 사용자의 권한으로 자원에 대한 접근 통제를 함으로써 개인정보 유출 및 정보의 손실을 예방하여 관리의 효율성을 높여줄 것이다.

Ⅷ. 결론 및 향후 연구

본 논문에서는 개인정보보호의 법·제도 동향에 대해 살펴보고 관련 표준화 기술인 P3P, APPEL 및 RBAC에 대해서 조사하였다. 또한, 웹 환경 내 개인정보의 이슈를 분야별로 분석하여 연구에 이용할 수 있는 문제점을 도출하였다. 이를 기반으로 본 연구는 안전한 개인정보 사용 및 관리 방안으로써 국내법률 기반 개인정보보호 정책엔진 메커니즘을 제안하였다. 이는 노출된 환경에서 국내 개인정보보호 법을 시스템화 하여 사용자에게 안전한 서비스를 제공하고, 기업 및 개인정보 요청자는 법률 보호 하에 정보수집 및 활용이 가능하도록 기술적으로 구현방안을 제시하였다. 또한 국내 개인정보보호 법률을 역할기반 접근제어를 적용함으로써 무분별한 개인정보 수집 및 이용을 예방하고, 웹 환경 내 사용자들은 프라이버시를 보호 받을 수 있다. 신뢰할 수 있는 개인정보보호 정책엔진 메커니즘의 정의는 기존의 접근제어에 비해 개인정보의 중요도와 개인정보 요청자의 역할등급에 따라서 유동적으로 개인정보 항목에 접근 가능한지가 결정되므로 개인정보의 수집 및 활용에 대해서 유연성과 실적용의 우수성을 고려하며, 실제 IT 환경 내 아키텍처 적용 가능한 연구로 소프트웨어 개발자나 운영자 입장에서 도움이 되는 응용방안 연구가 될 것이다.

향후, PIPS 솔루션 개발을 위해 제안한 개인정보보호 정책 및 접근제어의 기반으로 개인정보 오·남용 방지를 위한 Notice를 추가하여 사전 동의 및 경고 등의 기능이 연구되어야 할 것이다. 또한, 정보보호 모니터링 기술과 체계적인 로그 데이터의 분석기술을 통한 디지털 포렌식 기능에 대한 구현이 요구되며, 제안한 솔루션의 안전성 기능을 위한 정보보호 시스템과 연동 및 실 적용성에 대해 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] 강신범, “EAM/SSO 기술과 동향”, 경영과 컴퓨터, 2004.

[2] 강연정, “개인정보보호 기술 및 표준화 동향”, 한국정보보호진흥원, 2006.

[3] 강연정, 김지연, 이향진, “개인정보보호정책 설정 및 협상 기술 분석”, 한국정보보호진흥원, 2006.

[4] 공개SW기반 조성팀,“공개SW보안 운영체제에 관한 연구”, 한국소프트웨어진흥원, 2005.

[5] 국가정보원, “2008 국가정보보호백서”, 2008.

[6] 권오병, “프라이버시 보호 상황인식 시스템 개발을 위한 쌍방향 P3P 방법론”, 경영정보학연구 제18권 제1호, 2008. pp.145-162.

[7] 김성태, “보험고객정보의 이용과 프라이버시 보호의 상충문제 해소방안”, 보험개발원 보험연구소, 2007. pp.41-64.

[8] 김성훈, 이종화, 김인호, “개인정보보호 관련 법규 준수율 제고 방안”, 한국정보보호진흥원, 2007.

[9] 김창곤, “u-City 구축촉진을 위한 법·제도적 기반환경 연구”, 한국정보사회진흥원, 2006.

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

[11] 민경식 외 11, “유비쿼터스 환경에서의 정보보호정책 방향”, 한국정보보호진흥원, 2008. pp.51-52.

[12] 박석 외 3, “개인정보보호 기술, 제품, 및 활용사례 분석”, 한국정보보호진흥원, 2006.

[13] 변순정, “APEC ECSG 개인정보보호 논의 동향”, 한국정보보호진흥원, 2006.

[14] 송유진, 남택용, 장종수, 손승원, “개인 정보보호 기술 동향”, IITA 기술정책정보단, 2005.

[15] 윤권일, “개인정보보호 전문교육”, 한국정보보호진흥원, 2007.

[16] 이동훈, “개인정보보호의 중요성과 보호기술”, 한국소프트웨어산업협회, 2007.

[17] 이동훈, “전자정부와 개인정보보호”, Information Security Review 1권 2호, 2004. pp.69-85.

[18] 이재광, 장종수, 박기식, “사이버공간에서의 개인정보보호”, 정보와사회 12호, 2007.

[19] 정연수, 김미현, 최윤정, “2007 개인정보분쟁조정사례집”, 개인정보분쟁조정위원회, 2007.

[20] 조은애, 문창주, 백두권, “QSGi 서비스 플랫폼에서 RBAC 기반의 사용자 접근제어 프레임워크”, 정보과학회논문지 제34권 제5호, 2007. pp.405-422.

[21] 최재규, “RBAC을 이용한 ESM 모델연구”, 주간기술동향 통권 1312호, 2007.

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

[23] (주)위너다임, “개인정보의 안전한 수집, 저장 및 관리, 이용, 제공, 파기를 위한 개인정보 관리모델 연구”, 한국정보보호진흥원, 2006.

[24] Annie I. Anton, Elisa Bertino, Ninghui Li and Ting Yu, “A roadmap for comprehensive online privacy policy management”, Communications of the ACM, Vol.50 No.7, 2007.

[25] Information Commissioner's Office, “Data Protection Technical Guidance Note”, *http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.*

pdf, 2006.

[26] Internet Education Foundation, "The P3P Implementation Guide", *http://p3ptoolbox.org/guide/.*

[27] Konstantina Stoupa and Athena Vakali, "Policies for Web security Services", Idea Group Publishing, 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] Pranam Kolari, Li Ding, Lalana Kagal, Shashidhara Ganjugunte, Anupam Joshi, and Tim Finin, "Enhancing P3P Framework through Policies and Trust", UMBC Technical Report, 2004.

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

[31] Qun Ni, Alberto Trombetta, Elisa Bertino, Jorge Lobo, "Privacy-aware Role Based Access Control", The 12th ACM symposium on Access control models and technologies, 2007. pp.41-50.

[32] The World Wide Web Consortium, "P3P 1.0 Implementations", *http://www.w3.org/P3P/implementations*, 2005.

Abstract

The Analysis and Implement of the Privacy Information Protection Mechanism in Web based System Environments

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

With the development of the information technology and the internet, new problems of IT re-engineering(e.g., cyber crime, personal information abuse) are increasing ever before, and the concern of overall information society is also rapidly increasing. Further, the cyber crime has moved from the internet environment to the real world, the estimates of damage have become more diffused. As the business related to aspect of personal information is being developed, various risk factors such as personal in-formation abuse, mis-usability, and illegal distribution are getting more im-portant problems in these days. Even though the government continued to promote personal privacy protection law, there is a lack of counter-proposal related to secure and privacy.

In this thesis work, I introduce how to analysis and implement of the privacy information protection mechanism in web based system environments. I suggested the privacy information protection policy based on preliminary studies of standardization technology, regulations and laws

for protection in personal information. The privacy policy in the technol-ogy aspect of personal information protection is represented as APPEL(A P3P Preference Exchange Language) which is one of the standardization technologies, and I describe the analysis and design of the PIPS(Privacy Information Protection System) engine that effective access control to sup-port law-based privacy policy. Lastly, I also introduced how to build and design of the policy for systematic information protection in a secure manner, I prototyped the privacy information protection mechanism which provides law-based privacy protection for feasible approach in real system environments.