제 1 장 서론

1. 연구의 배경 및 목적

정보통신의 발달과 범국가적인 정보통신 서비스의 급속한 확산은 사회 각 분야의 정보화 진행은 물론 경제활동까지 변화시키고 있다. 이러한 경향은 e-business 환경과 접목되면서 시간적·공간을 초월한 새로운 비즈니스 패러다임을 맞이하게 되었고, 기업들은 글로벌 경제 환경 내에서의 경쟁력을 확보하기 위해 부단한 노력을 기울이고 있다. 즉, 기업들은 정보시스템을 e-business 관련 인프라 또는 경영혁신의 도구로 적극 활용하여, 고객에 대한 실시간 요구사항을 신속히 파악하고 고객의 행동을 예측함으로써, 경영의 효율성과 효과성을 극대화시키고자 주력하고 있다.

이러한 배경 하에 기업들은 치열한 경쟁 사회에서의 선두자리에 오르고자 경제적 핵심 자산인 개인정보를 무분별하게 수집, 축적, 통합, 가공함으로써 고객의 성향 및 행위패턴을 분석하여 일괄적으로 데이터베이스화 시키고 있다. 또한 이러한 개인정보를 수집함에 있어 기업들 사이에서는 고객과의 실 거래가 일어나지 않더라도 웹 사이트에 회원가입을 유도시킴으로써 잠재고객에 대한 정보를 획득하여 마케팅 전략을 수립하고자 하는 성향이 증가하고 있다. 이에 따라 e-business 환경에서도 사생활 침해에 대한 우려 및 전자상거래에 대한 신뢰저하 등과 같은 부작용이 적지 않게 발생하고 있다. 즉, 인터넷을 이용한 전자상거래는 불특정 다수의 개인이나 기업을 대상으로 하기 때문에 비대면 거래에 의한 거래 당사자 간의 신분 확인이 네트워크 환경 내에서 이루어지고 있다. 이때, 거래기반 환경에서 거래가 성립되기 위해 반드시 필요한 요소 중의 하나가 신용/재무정보인 민감한 개인정보라는 점에서 고객들의 불안 심리는 지속적으로 증가하고 있다는 점이다. 이와 같이 디지털화된 민감한 개인정보가 네트워크 환경 안에서 유출 될 경우 흔적이 남지 않기 때문에 이를 발견하거나 정보 유출자를 색출하는 데에는 상당한 어려움이 있다고 하겠다.

또한 현재 국내에서는 이러한 피해사고에 대응 및 보완할 수 있는 기술적, 법/제도적인 가이드라인이 부재한 실정이기 때문에 국내에 적합하고 엄격한 법적 규제

및 처벌에 관한 개정이 요구되어지며, 이를 기반으로 개인정보를 보호하기 위한 인프라 시스템 구축 및 연구 또한 시급한 실정이라 하겠다.

본 논문에서는 개인정보보호정책에 따른 지침 및 절차에 준한 사용자별 레벨을 부여하고, 그에 따른 적합한 속성대비 접근통제를 부여함으로써, 보다 안전하게 개인정보를 관리·통제할 수 있는 방안을 제시하였다. 또한 제시한 방안을 기존의 정보보호 기술과 접목하여 시스템 환경 측면에서의 신뢰를 기반으로 개인정보 공유 및 활용할 수 있는 방안을 제안하였다.

본 논문의 구성은 다음과 같다. 1장에서는 논문의 개요에 대해 간략히 소개하였고, 2장 관련연구에서는 개인정보의 정의 및 개요와 그에 대한 국내·외 개인정보보호 관련기술 및 표준화를 소개하였다. 3장에서는 e-business 환경에 대한 현황을 살펴보고, 사례연구(CRM – Customer Relationship Management)프로세스를 통해 개인정보 침해 우려 및 문제점을 제시하였다. 4장에서는 신뢰할 수 있는 개인정보보호 정책모델인 TPM(Trusted Privacy Policy Model)에 대한 아키텍처를 제안하였으며, 4가지 주요 메커니즘에 대하여 기술하였다. 5장에서는 TPM 구조에 대한 분석 설계 및 Prototyping 을 통한 적용 방안에 대하여 제시하였고, 마지막으로 6장에서는 결언 및 향후 연구에 대해 알아보았다.

제 2 장 관련 연구

2.1 개인정보

2.1.1 개인정보의 정의

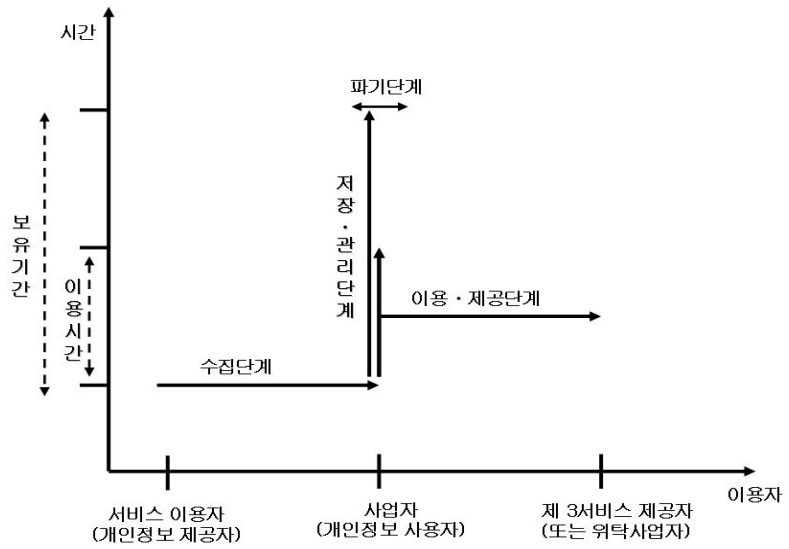
개인정보란 “생존하는 개인에 관한 정보로서 성명・생년월일・주민등록번호 등에 의하여 개인을 알아볼 수 있는 부호・문자・음성・음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)”를 말한다.[1][2][3]

개인정보의 유형에 따라 일반정보, 가족정보, 교육정보, 등과 같이 분류 할 수 있으며, 이를 세부적으로 정리하면 아래와 같이 (표 2-1)로 정리되어질 수 있다.[17][46]

(표 2-1) 유형별 개인정보

유형구분	개인정보의 종류
일반정보	이름, 주민등록번호, 주소, 전화번호, 성별
가족정보	가족구성원들의 이름, 출생지, 생년월일, 작업, 전화번호
교육정보	한국사항, 기술자격증 및 전문면허, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타 소유차량, 상점 및 건물 등
동산정보	보유현금, 저축현황, 현금카드, 주식, 채권, 예술품, 보석
소득정보	현재 봉급, 봉급경력, 보너스 및 수수료, 이자소득, 사업소득
기타수익정보	보험(건강, 생명 등), 가입현황, 회사의 판공비, 퇴직프로그램
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 압류 통보 기록
법적정보	전과기록, 자동차교통위반기록, 구속기록, 이혼기록, 납세
의료정보	가족병력기록, 과거의료기록, 정신질환기록, 각종 의료정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등

2.1.2 개인정보의 단계별 생명주기



(그림 2-1) 개인정보의 생명주기

· **수집단계** : 서비스 제공자가 서비스 이용자의 개인정보를 수집하는 단계이다. 이 단계에서 수집되는 개인정보는 정적인 개인정보와 동적인 개인정보로 나눌 수 있는데, 정적인 개인정보는 새로운 서비스 가입 시에 서비스 제공자의 요구에 의해서 서비스 이용자가 제공하여 서비스 탈퇴시까지 지속되는 개인정보를 말하고, 동적인 개인정보는 RFID 나 LBS 서비스를 위해 서비스 이용자가 제공하는 위치정보, 인터넷 접속 상황을 알려주는 쿠키 정보 등을 의미한다.

· **저장 및 관리 단계** : 서비스 제공자가 서비스 이용자의 개인정보를 저장하고 이를 관리하는 단계이다. 이 단계에서는 수집된 개인정보를 데이터베이스 등에 저장하고, 개인정보보호정책에 따라 허가받은 자만이 해당 개인정보에 접속할 수 있는 권한 관리 등이 이루어진다. 또한 서비스 이용자가 서비스에 대한 탈퇴를 요청하면 해당 개인정보에 대한 이용 및 제공은 종료되지만 법률적인 근거에 의해 개인정보를 일정기간 보유하여야 하므로, 서비스 탈퇴자의 개인정보는 즉시 파기되지 않고 보유기간 동안 관리체계에서 파기 전까지 저장하고 편리하게 된다.

· **이용 및 제공단계** : 서비스 제공자가 서비스 이용자의 개인정보를 여러 가지 필요에 의해 이용하는 단계이다. 일반적으로 정적인 정보는 서비스 이용자 인증이나 인터넷 쇼핑 등의 기본 서비스, 이벤트 등 부가서비스를 위해 이용되며, 필요에 의해 개인정보보호정책에 명시하고 서비스 제공자 외 제 3 서비스 제공자에 제공되

기도 한다. 따라서 이용 및 제공단계에서는 서비스 제공자의 서비스 가입부터, 탈퇴 시까지 서비스 제공자가 저장 및 관리하고 개인정보 일부를 이용하거나 제공하게 된다.

· **파기단계** : 서비스 제공자가 서비스 이용자의 개인정보 저장 및 관리기간 종료 시 파기하는 단계이다. 이 단계에서는 정적인 개인정보는 서비스 탈퇴이후에 발생하지만 위치정보나 쿠키 정보 등 동적인 개인정보는 서비스 탈퇴하는 시점이 아니라 서비스에는 가입되어 있지만, 요청한 서비스가 종료되면 일정 기간 후에 파기되어야 한다.

즉, 서비스 이용자의 개인정보는 일반적으로 서비스 사업자가 수집하여, 이를 필요 기간 동안 저장하여 관리하고, 관리기간 중 필요 기간 동안에는 이를 이용 및 제공하여, 보유 기간이 종료되면 즉시 파기하게 된다. 이러한 일련의 생명주기를 도식화하면 (그림 2-1)과 같다. 개인정보는 개인이 특정 서비스를 이용하고자 하는 경우, 서비스 사업자의 요청을 통해 수집되며, 수집된 개인정보는 서비스 제공자가 저장하여 관리하게 된다. 서비스 제공자는 필요에 의하여 개인정보를 이용하거나 타인에게 제공하게 되며, 서비스 이용자가 서비스를 탈퇴하더라도 법률적인 근거에 의해 일정 기간 보유한 후, 파기하게 한다. 특히 서비스 사업자는 개인정보에 관한 일련의 프로세스에 대해서 이를 개인정보보호정책으로 표현하여 서비스 이용자에게 반드시 알려주어야 한다.[4][20]

2.1.3 개인정보 침해유형 및 침해현황

1) 개인정보 침해 유형

개인정보의 수집, 저장, 및 관리, 이용 및 제공, 파기 등의 개인정보의 모든 생명주기 단계에서의 각 단계별 개인정보 침해유형을 요약한 것이다.[4][44][47]

(표 2-2) 개인정보 침해유형

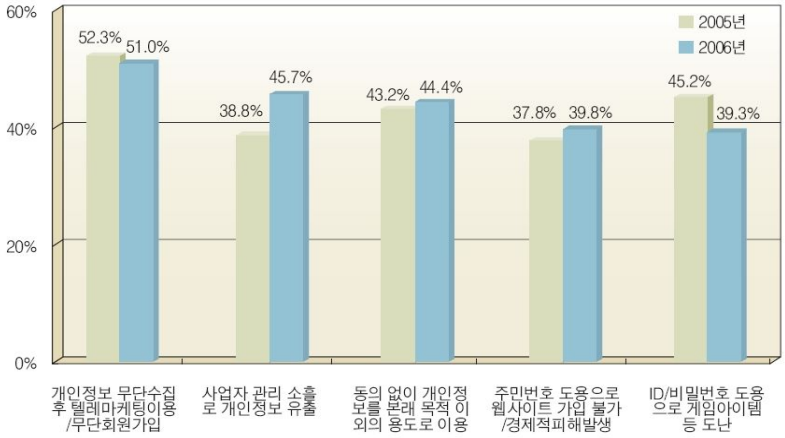
단계	침해유형	침해요인
수집	부적절한 접근과 수집	불필요한 개인정보 수집
		개인정보보호정책에 명시되지 않은 개인정보 수집
		사용자 동의 없이 개인정보 수집
	부적절한 모니터링	동의 없이 개인의 인터넷 활용이나 사생활을 모니터링
저장 및 관리	부적절한 저장	수집된 개인정보를 불법적인 유출 유협이 있는 상태로 저장
		수집된 개인정보를 개인정보보호정책에 명시된 수집 목적 달성 시점이나 저장기간 이후에도 저장 상태 유지
	개인정보의 노출	동의 없이 개인정보 노출
		권한관리, 시스템/서비스 오류로 개인정보 노출
		관리자 또는 이용자의 실수로 개인정보 노출
이용 및 제공	부적절한 분석	동의 없는 개인정보 분석
		수집된 개인정보의 부적절한 분석
	원하지 않는 영업행위	동의 없는 상품광고, 광고성 정보 제공
	부적절한 개인정보 제공	개인정보보호정책에 명시되지 않은 위탁사업자나 제 3 서비스 제공자에 개인정보 제공
		개인정보보호정책에 명시된 위탁사업자나 제 3서비스 제공자에게 명시되지 않은 개인정보 항목을 제공
		개인정보를 제 3자에게 양도하는 등 불법적 거래
파기	보유기간 외 개인정보 저장	개인정보보호정책에 명시된 보유기간 이후에 개인정보를 파기하지 않고 저장
	부적절한 개인정보의 파기	파기해야할 개인정보에 대한 비파기
		권한관리의 오류로 권한없는 이용자가 개인정보 파기
		보유기간이 경과하지 않은 개인정보의 파기

2) 개인정보 침해현황

개인정보는 정보통신망의 발전과 급변하는 경제 환경 및 신기술의 부합으로 네트워크 환경 내에서의 개인정보 가공 및 활용이 용의해졌다. 그에 따라 정부나 민간단체로부터 정보주체의 어떠한 동의 없이 무한대로 수집·축적·처리·가공을 이용한 개인정보통합관리시스템의 구축이 가능해지면서 개인정보 누출 및 불법취득에 대한 피해가 끊임없이 발생하고 있다[2][3]. 실제 2006년에 발생한 피해사례 경우 '리니지 Ⅱ' 28만여 건의 명의도용 피해 발생('06.2), 유명 결혼정보회사 해킹으로 회원정보 54만 건 노출('06.8),[5][8] 구글 검색 사이트에 90만명 주민등록번호 노출('06.8), 건강보험 1만 4천명 개인정보 유출('06 10) 등과 같이 크고 작은 일련의 개

인정보 보도들이 사회적·경제적·국제적으로 이슈화된바 있다.[6][7]

아래 (그림 2-2)는 2005~06년 한해 동안 개인 인터넷 사용자를 대상으로 실시한 설문 조사 결과로써 2006년을 기준으로 "개인정보 무단수집 후 텔레마케팅 이용/무단회원가입"유형이 51.0% 차지하였고, 두 번째로는 "사업자 관리 소홀로 개인정보 유출"의 유형이 45.7%를 차지하고 있다.[10][11]

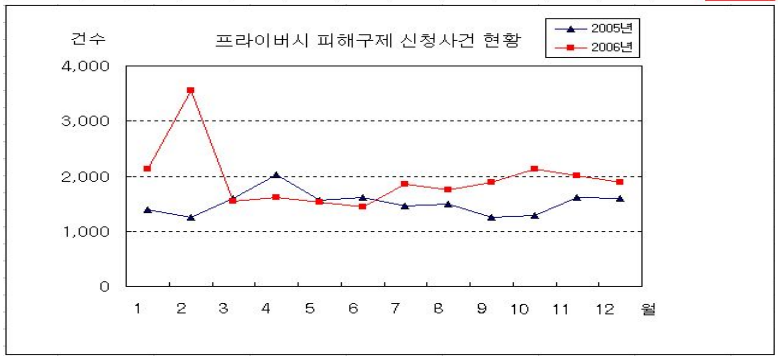


(그림 2-2) 개인정보/프라이버시 침해 경험률

다음 (표 2-3)은 2005~2006년 동안 월별 개인정보 피해구제·상담 현황을 으로써, 2006년 피해 접수 건수는 총 23,333건이며, 이는 2005년에 접수된 18,206건에 비해 약 28% 증가한 수치를 나타내고 있다.[9][10]

(표 2-3) 2005~2006년 피해구제 신청현황

	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	합계
2005년	1,387	1,253	1,601	2,031	1,555	1,618	1,462	1,500	1,253	1,285	1,620	1,591	18,206
2006년	2,131	3,561	1,538	1,613	1,521	1,439	1,859	1,746	1,885	2,133	2,016	1,891	23,333



개인정보 오·남용으로 인해 당해 개인정보 주체는 인격권, 재산권 및 심신상의

안전을 위협받을 수 있다. 개인정보의 오·남용으로 인한 피해 형태는 다음과 같이 정리 될 수 있다.[3][19]

- 명의도용에 따른 신용사기로 인한 재정적 피해 가능성
- 명의로 도용한 자가 행한 명예훼손, 모욕 등으로 인해 형사 사건의 혐의자가 될 수 있음.
- 수집된 개인정보가 부정확·부적정한 경우 개인정보 주체에 대한 그릇된 판단을 초래할 수 있음.
- 지속적인 개인정보 수집으로 인한 사생활 감시로 불/유쾌 및 불편이 초래되거나 사회적 활동에 지장을 초래할 수 있음.
- 원하지 않는 광고성 정보 등의 수신으로 인한 생활의 평온 파괴의 가능성

등과 같이 매우 다양하게 나타날 수 있다.

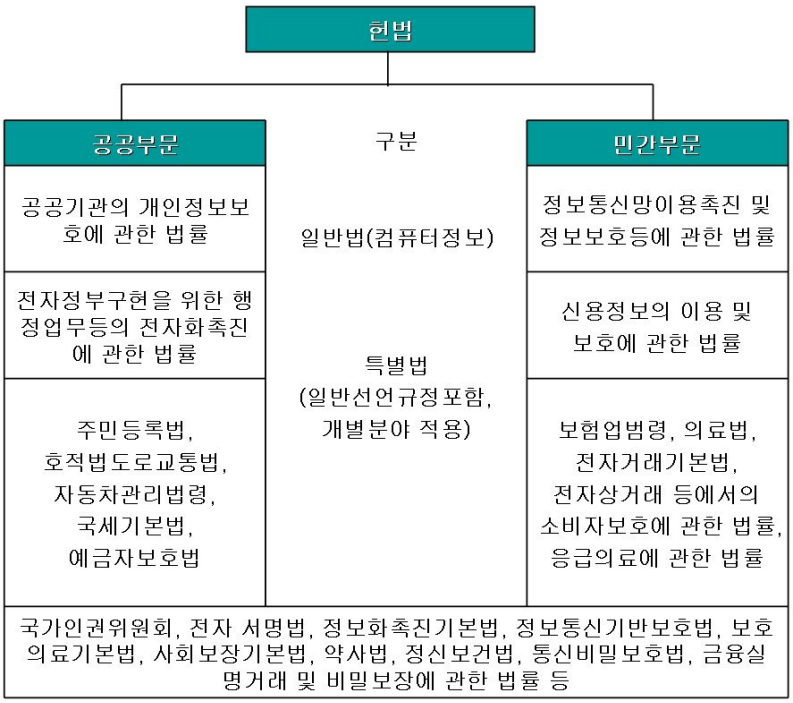
이와 같이 정보기술의 발달에 대한 e-business의 활성화는 우리에게 보다 많은 혜택과 편리함을 제공하고 있지만, 그에 대한 개인정보의 역기능(개인정보 오·남용, 정보의 위험, 위협, 취약점 등)도 나날이 증가한다는 점에서 개인정보보호에 대한 중요성이 대두되고 있다고 하겠다. 다시 말해 개인정보 역기능에 대응 되어질만한 적절한 보호장치가 구비되지 않는다면, 인터넷과 정보기술은 개인이 남긴 정보의 흔적을 통해 민감한 개인사생활 부분까지도 속속들이 밝혀낼 수 있다는 것이다. 즉, 이러한 사생활이 보호받지 못하는 환경에서의 디지털 정보사회의 발전은 무의미한 것일지도 모른다. 이에 따라 개인의 정보를 보호하기 위한 기술적·법/제도적으로 명확히 정의하고, 신속히 대체할 수 있는 방안을 마련하는 것이 절실히 필요하다고 하겠다.

2.2 개인정보보호 표준 및 동향

2.2.1 국내 개인정보 법규

우리나라의 개인정보보호법제는 헌법과 개별 법률로 이루어지다가 공공부문의 행정전산망사업이 상당부분 성과를 보여 공공정보의 전산화가 이루어짐에 따라 컴퓨터로 처리하는 개인정보를 보호하기 위한 「공공기관의 개인정보보호에 관한 법률」이 제정되었다. 1994년 제정된 이 법률은 정보사회의 개인정보 즉, 정보주체의

자기정보통제권이나 정보적 자기결정권 등으로 일컬을 만한 인식이 생긴 이후의 의미 있는 일반입법이라 할 수 있다. 이는 공공부문에서 컴퓨터로 처리되는 개인정보를 보호하기 위한 일반법으로 제정되었으며, 민간부문의 경우 1995년 「신용정보의 이용 및 보호에 관한 법률」의 제정을 비롯해 여러 개별 법률에 개인정보의 보호조항이 삽입되기에 이르렀다. 그러나 신용정보의 이용 및 보호에 관한 법률의 경우 신용정보를 보호하려는 목적보다는 신용정보를 제한적으로 이용해 관련 산업을 진흥시키고자 하는 목적이 더 강한 것이라 할 수 있으며, 다른 개별법에 삽입된 개인정보보호 관련 조항과 일반적 · 선언적 규정에 불과했다. 이후 초고속망 등 정보통신망이 확충되고 이를 통한 개인정보의 수집 및 유통이 일반화 되어 민간부문의 개인정보보호 체계에 대한 반성이 일어남에 따라 1999년 기존의「전산망보급 확장 및 이용촉진에 관한 법률」의 제명을「정보통신망 이용촉진 등에 관한 법률」로 바꾸고 미흡하나마 정보통신망을 통해 수집 및 유통, 활용되는 개인정보를 보호하기 위한 법제의 기틀을 마련하게 되었다. 그러나 공공부문의 개인정보보호법제가 단일법제를 마련하고 있는 것에 비하면 이 역시 초보적 단계에 불과했다. 이후 2001년 이 법률의 제명을 다시「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 바꾸면서 개인정보 관련 조항을 대폭적으로 개선함으로써 공공부문과 비슷한 보호 수준에 이르렀다. 요약하자면, 우리나라의 개인정보 보호체계는 공공부문과 민간부문으로 나뉘어 그 법적 근거 및 추진체계를 달리하고 있으며, 아래 (그림 2-3)은 우리나라 개인정보보호 관련법규체계를 요약한 것이다. 공공부문은 개인정보 보호에 관한 일반법으로서 「공공기관의 개인정보 보호에 관한 법률」(이하 「개인정보보호법」이라함)이 있으며, 「전자정부 구현을 위한 행정업무 등의 전자화 촉진에 관한 법률」및 주민등록법 등의 개별법에 개인정보 보호에 관한 규정이 산재해있다. 한편 민간부분은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」, 「통신비밀보호법」, 「정보통신 기반 보호법」, 「금융실명거래 및 비밀보장에 관한 법률」등의 개별법에서 개인정보에 관한 사항을 규정하고 있다. 외국의 입법례를 보면 우리나라와 같이 공·사 부문을 구별하면서 별개의 법률로 규율하고 있는 나라(미국), 공·사 부문을 구별하지 않고 단일 법률로 규율하고 있는 나라(스웨덴, 영국), 공·사 부문을 구분하되 단일 법률로 규율하고 있는 나라(독일, 프랑스)등으로 대별할 수 있다.[3][42]



(그림 2-3) 우리나라 개인정보보호 관련법규체계

2.2.2 국외 개인정보보호 법규

2.2.2.1 OECD 프라이버시 보호 원칙

OECD는 1980년 9월 국가간의 합법적이고 자유로운 정보유통 및 정보처리 산업의 보호를 도모할 목적으로 OECD「프라이버시보호와 개인정보의 국가간유통에 관한가이드라인(Guidenlines on the Protection of Privacy and Transbordor Flows of Personal Data) 이하 'OECD 개인정보보호지침'」을 이사회 권고 형식으로 채택하였다.[12][14][15] 이 지침 중 회원국에게 권고하는 최소한의 규정으로 발표된 국내적용에 있어서의 개인정보보호의 8개 원칙은 개인정보보호 관련법과 제도 및 지침의 모델이 되어 EU지침을 비롯한 각국의 공공부문 및 민간부문에서의 개인정보의 규제 원칙으로 광범위하게 받아들여지게 되었다. 이 지침은 총 5장으로 되어 있으며, 제1장은 총칙, 제2장은 국내적용상의 기본원칙, 제3장은 국제적 적용상의 기본원칙, 제4장은 국내실시, 제5장은 국제협력으로 구성되어 있다. 이 지침은 공적부문과 사적부문 모두 적용하도록 권고하고 있다.[43][44]

1) 국내 적용상의 기본원칙

(표 2-4) OECD 프라이버시 8대원칙

원 칙	내 용
수집제한	개인데이터의 수집에는 제한을 두어야 한다. 어떠한 개인 정보도 합법적이고 공정한 절차에 의하고 가능한 경우에는 데이터주체에게 알리거나 동의를 얻은 연후에 수집하여야 한다.
정확성확보	개인데이터는 그 이용목적에 부합되는 것이어야 하며 이용 목적에 필요한 범위 안에서 정확하고 완전하며 최신의 것이어야 한다.
목적명시	개인정보는 수집 시 그 수집목적이 명확히 제시하고, 그 후의 이용은 수집목적의 실현 또는 수집목적과 양립되어 목적이 변경될 때마다 명확화 될 수 있는 것으로 제한되어야 한다.
이용제한	개인정보는 목적명확화의 원칙에 의하여 확인된 목적 이외의 다른 목적을 위해 개시, 이용, 그 밖의 사용에 제공되어서는 안 된다. 다만 정보주체의 동의가 있거나 법률의 규정에 의한 경우에는 예외로 한다.
안전성확보	개인데이터는 그 분실 또는 불법적인 액세스, 파괴, 사용, 수정, 개시 등의 위험에 대하여 합리적인 안전조치를 함으로써 보호하여야 한다.
공 개	개인데이터와 관련된 개발, 실시, 정책에 대하여는 일반적인 공개정책을 취하여야 한다. 개인데이터의 존재, 성질 및 그 주요 이용 목적과 함께 데이터관리자의 식별, 주소를 명확하게 하기 위한 수단은 용이하게 이용할 수 있어야 한다.
개인참여	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.
책 임	데이터관리자는 위의 제 원칙을 실시하기 위한 조치에 따를 책임이 있다.

2.2.2.2 EU(European Union)

프라이버시권과 정보를 가질 권리 혹은 알 권리 사이의 조화와 인터넷상에서의 정보 오·남용으로 인한 타인의 권리침해 방지가 필요하고, 또한 국경을 넘어서의 개인보호 수준이 같아지도록 해야 하는 필요성이 대두되자, EU는 개인정보보호에 관하여 강력한 정책을 추진하여 정보통신서비스제공자의 책임을 요구하는 법제와 판례를 보이고 있다. EU는 개인정보가 소비자 보호나 전자상거래의 부속물이 아닌 인격권 보호의 한 부분으로서, 정부가 직접 개입하여 엄격히 보호하여야 한다는 입장을 고수하고 있다. 이에 따라 인권보호와 기본권 자유를 위한 유럽협약 108의 제

8조와 EU의 일반법인 EU개인정보보호지침은 유럽 사회 내에서의 프라이버시권의 보호에 관한 높은 수준을 추구하고 있다. EU개인정보보호지침은 유럽에 걸쳐 이미 제정되어 있는 이와 관련된 각 회원국간의 국내법 원칙의 차이를 제거하고 다양한 법률들을 조화시키기 위한 기준을 마련하고자 하기 위함이다. 이에 회원국은 1998년 10월 25일까지 동 지침이 규정하고 있는 내용에 일치하도록 국내법을 제정 또는 개정하여 개인정보보호원칙을 설정, 개인정보보호기구 설치, 개인정보보호원칙을 불이행하는 경우 제재권 등을 규정하고 있다.

적절한 보호수준은 지침의 주요원칙에서 드러나고 있는데, 이 중 미국과의 마찰을 일으킨 몇 가지 문제를 살펴보면, 첫째, 정보주체에게 당해 정보의 수집에 대한 정확하고 충분한 정보를 제공한 후, 데이터주체의 정보에 대한 동의의사표시에 관한 문제이다. 개인정보를 목적이외의 사용 혹은 공개하고자 한다면, 이에 앞서 개개인의 동의가 필요한 opt-in(동의조건부)방식을 사용하여 미국의 opt-out(반대유보)방식보다 더 많은 권한을 정보 주체에게 주고 있다. 두 번째, 개인정보보호를 위한 독립된 감독기구의 설치에 관한 문제이다. 제6장에서 감독기관과 개인데이터 처리에 관련된 개인보호에 관한 작업반에 관한 규정을 하고 있다. 개인정보보호 감독기구는 위탁받은 임무를 수행함에 있어 완전히 독립적이어야 하고 정보통신서비스제공자의 개인정보보호처리 이행에 관한 확인절차를 수립해야 한다. 그리고 정보에 접근할 수 있는 권한과 감독의무를 이행하는데 필요한 정보를 수집할 권한을 가지고, 각 회원국이 채택한 규정의 영역내의 적용에 대한 감시를 책임진다. 또한 원칙을 이행하지 않을 경우, 법적 제재 수단의 확립을 통하여, 개인이 자신의 정보를 침해당하였을 때 구제절차를 수립할 수 있도록 하고 있다. 세 번째는 제 3국으로의 개인정보 전송에 관한 문제이다. 제25조와 제26조로 구성되어 있는 제4장에서 제 3국으로의 개인데이터 전송에 관한 규정을 하고 있다.[13][16]

2.3 개인정보보호 관련기술

2.3.1 접근통제기술(Access Control)

식별 및 인증된 사용자가 허가된 범위 내에서 시스템 내부의 정보에 대한 접근을 허용하는 기술적 방법을 접근 통제라고 하며, 이러한 접근 통제 정책은 임의적 접

근통제와 강제적 접근통제로 분류될 수 있다.

2.3.1.1 임의 접근통제(DAC : Discretionary Access Control)

임의 접근통제에서는 주체나 주체가 속해 있는 그룹의 식별자에 근거하여 객체에 대한 접근을 제한하는 방법이다. 임의 접근통제는 접근을 요청하는 사용자의 식별에 기초하여 어떤 객체에 대해 사용자가 접근 권한을 추가 혹은 삭제할 수 있다는 의미에서 임의적이다.[22]

따라서 임의 접근통제 정책에서는 모든 개개의 주체와 객체 단위로 접근 제한이 설정되며, 객체의 소유주에 의하여 접근 제한이 변경 가능한 각 주체와 각 객체간의 접근통제 관계를 정의하고 있다. 즉 임의의 접근 권한을 가지고 있는 사용자는 임의의 다른 사용자에게 접근 권한을 부여할 수 있다. 그러나 최초로 객체에 내포된 임의 접근 통제 관계를 정의하고 있다. 즉 임의의 다른 사용자에게 접근 권한을 부여할 수 있다. 그러나 최초로 객체에 내포된 임의 접근 통제 관계는 복사된 객체에 전파될 수 없다. 그러므로 어떤 사용자가 어떤 한 파일을 읽고 복사할 경우에 원래의 파일에 부여된 허가권이 복사한 파일에 적용되지 못한다.

(표 2-5) 식별기반(개인, 그룹기반)의 예

	object x	object y	object z
user a	read, modify manage		read, modify manage
user b		read, modify manage	
user c1	read	read, modify	
user c2	rad	read, modify	

개인기반정책(individual based policy)이란 위의 (표 2-5)에서 보는 것과 같이 어떤 사용자가 어떤 행동을 할 수 있는지를 각 목표별로 목록에 표현하는 방법으로서 object x에 대해서 user a에게 읽기와 변경, 관리의 권한을 부여하고 user c1, user c2,에게는 읽기 권한만을 부여하고 있다. 이처럼 임의의 목표 별로 그에 대해 개인별 권한을 부여하는 정책을 목표기반 정책이라고 이는 개인에 한 목표에 접근하기 위해 최소 권한이 원칙에 의하여 접근 권한을 부여하게 된다.

그룹기반정책(group based policy)은 다수의 사용자가 하나의 목표에 대하여 접근 권한을 부여하는 방법이다. 이는 대형 시스템에서 객체에 대한 접근 통제 정책을 효율적으로 부여하고 관리하는 한 방법이다. 예에는 user c1과 user c2는 같은 user c라는 그룹에 속하므로 object x와 object z에 대해 같은 접근 권한을 부여 받고 있다.

임의 접근 통제의 단점으로는 접근 권한의 부여를 오직 식별자에만 의존하고 있어 데이터의 의미(semantics)에 대해 아무런 지시도 갖고 있지 않아 데이터의 의한 통제를 할 수 있는 방법이 전혀 없다. 식별자가 도용당할 경우 임의 접근 통제정책이 파괴될 수 있다는 취약점을 가지고 있다. 트로이 목마와 같은 은닉 공격에 매우 취약하다.[18][21]

2.3.1.2 강제적 접근통제(MAC : Mandatory Access Control)

강제적 접근 통제는 규칙기반 정책(rule based policy)과 동일한 것으로 비밀성을 포함하고 있는 객체에 대해 있는 권한(Authorization)에 근거하여 객체에 접근을 제한하는 정책이다. 따라서 정보에 대한 비밀 등급이 정해지고 해당 등급에 대한 접근 권한이 주체에게 부여되면 모든 주체와 객체 사이에 동일한 접근 권한이 부여된다. 이는 강력한 정보보호 메커니즘을 이루게 한다. 또한 강제적 접근 통제에서는 객체에 대한 접근 권한이 상위비밀 등급에서 하위 비밀 등급으로만 허가되기 때문에 흐름제어(flow control)정책으로 정의되기도 한다.[23]

객체의 소유자에 의하여 변경할 수 없는 한 주체와 하나의 객체간의 접근통제가 가능하고 최고 객체에 내포된 강제접근 통제관계는 복사된 파일에도 그대로 승계되어 적용된다.

강제적 접근 통제 정책을 구현하기 위한 메커니즘으로 보안 레이블(Security lable)이나 MLP(multi level policy)같은 것들이 있다. MLP는 정부나 안보기관 등의 비밀 정보 분류가 필요한 환경에서 적용되고 있다. 즉 각 객체에 대해 (그림 2-4)와 같은 비밀 등급을 부여하고 사용자는 해당되는 접근 허가 등급을 부여 받아 객체에 접근할 수 있다.

Top Secret
Secret
Confidential
Restricted
Unclassified

(그림 2-4) 비밀등급(예)

보안 레이블은 데이터 항목이나 물리적인 자원과 같은 객체, 그리고 주체에 부여된 보안 속성 정보의 집합이다. 주체인 사용자는 로그인하는 과정에서 사용자 식별(ID)과 패스워드는 물론 자신에게 부여된 신원허가(clearance)를 입력한다. MAC메커니즘을 위한 신원허가는 비밀 등급과 카테고리로 구성된다. 객체에도 보안 레이블이 붙여진다. 사용자가 생성한 객체들은 객체가 담고 있는 정보의 비밀성에 따라 이에 적합한 비밀 등급과 카테고리 코드가 부여된다. 주체와 객체의 보안 레이블을 바탕으로 접근통제를 한다. BLP(bell and LaPadula)모델에 기초하여 메커니즘을 구현한다.[18][25]

2.3.2 사용자인증기술

2.3.2.1 PKI(Public Key Infrastructure)

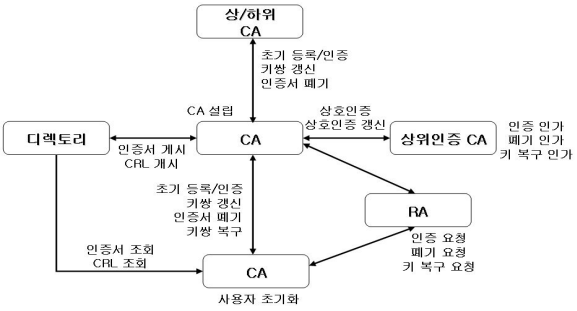
공개키 기반구조는 일반적으로 데이터의 안전한 전송을 위해 사용되는 공개키 암호 응용에 대한 전자인증서 발행과 획득, 조회, 검증 등을 수행할 수 있는 인증서 관리 기반 구조 즉, 전자인증서를 이용한 공개키 관리구조를 말한다. 또한 이러한 전자인증서의 발행과 배포 등의 관리를 수행하는 믿을 수 있는 인증기관(CA : Certificate Authority)들간의 신뢰 구조를 말하기도 한다.[24] 특히 공개키 기반구조는 공개키 암호를 기반으로 하는 전자서명의 무결성(integrity), 송신부인봉쇄(source non-repudiation), 인증(authentication)등의 보안 서비스가 안정적으로 제공될 수 있도록 하는 것이 주요 목적이다. 또한 각 개인 또는 기관 등에서 소유하고 있는 공개키 값을 서로 인정하는 행위인 인증(certification)기능과 인증내용이 유효한지를 확인하는 행위인 검증(validation)기능이 공개키 기반구조가 제공하는 가장 기본적인 기능이다. 공개키 기반구조에서는 일반적으로 위의 두 가지 기능의 효율적인 수행을 위하여 전자인증서(digital certificate)와 인증기관의 개념을 사용한다.

즉, 개별적으로 소유하고 있는 공개키 값과 자신들의 신원 정보를 공식적으로 연결하는 매체로서 전자인증서를 사용하며, 전자인증서를 발행하고 발행된 전자인증서의 내용을 보증하고 관리하는 기능을 인증기관이 수행하도록 하는 것이다.

이와 같이 공개키 기반구조는 공개키 전자인증서의 발행, 취소, 배포 등과 같은 전자인증서 관리에 관련된 구성요소 및 기능의 정의, 인증 구조의 확립 등에 관련된 관리적, 기술적 제반 사항을 체계적으로 수립하여 공개키 관리의 효율성을 제고하고, 공개키 암호기술이 제공하는 보안 서비스가 안정적으로 이루어 질 수 있도록 하기 위한 기술이다.[26]

1) PKI구성 요소

PKI를 구성하는 최소 객체들은 등록기관(RA :Registration Authority), 인증기관, 디렉토리, 사용자로 구성되어있으며 그에 대한 구조(그림 2-5)이다.[25]



(그림 2-5) PKI 구조

(1) 인증기관 (CA : Certificate Authority)

공개키 기반구조를 구성하는 가장 핵심 객체로 그 역할 및 기능에 따라 계층적으로 구성되며 여러 명칭으로 불린다. PKI전반에 사용되는 정책을 생성하고 PKI구축의 루트 CA로의 역할을 하는 정책승인기관(PAA : Policy Approving Authority)과 PAA 아래 계층으로 자신의 도메인 내의 사용자와 인증기관(CA)이 따라야 할 정책을 수립하고 인증기관의 공개키를 인증하고 인증서, 인증서취소목록 등을 관리하는 정책인증기관(PCA : Policy Certification Authority)과 PCA 아래 계층으로 사용자의 인증서를 발행하고 필요에 따라 취소하는 인증기관(CA : Certification

Authority)등 세 기관 모두를 인증기관이라 한다.

(2) 등록기관 (RA : Registration Authority)

인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자 사이에 등록기관을 두어 사용자들의 인증서 신청 시 인증기관 대신 그들의 신분과 소속을 확인하는 기능을 수행한다. 사용자들의 신분을 확인하고 인증서 요청에 서명을 한 후 인증기관에게 제출한다. 인증기관은 등록기관의 서명을 확인한 후 사용자의 인증서를 발행하여 등록기관에게 되돌리거나 사용자에게 직접 전달한다. RA는 조직 등록기관(ORA : Organizational Registration Authority)이라고도 한다.

(3) 디렉토리 (Directory)

인증서와 사용자 관련 정보, 상호 인증서 쌍 및 인증서취소목록 등을 저장하고 검색하는 장소로, 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버(인증기관)는 DAP(Directory Access Protocol)나 LDAP(Lightweight DAP)를 이용하여 X.500디렉토리 서비스를 제공한다. 인증서와 상호 인증서 쌍은 유효기간이 경과된 후에도 서명 검증의 응용을 위해 일정기간 동안 디렉토리에 저장된다.

(4)사용자(User)

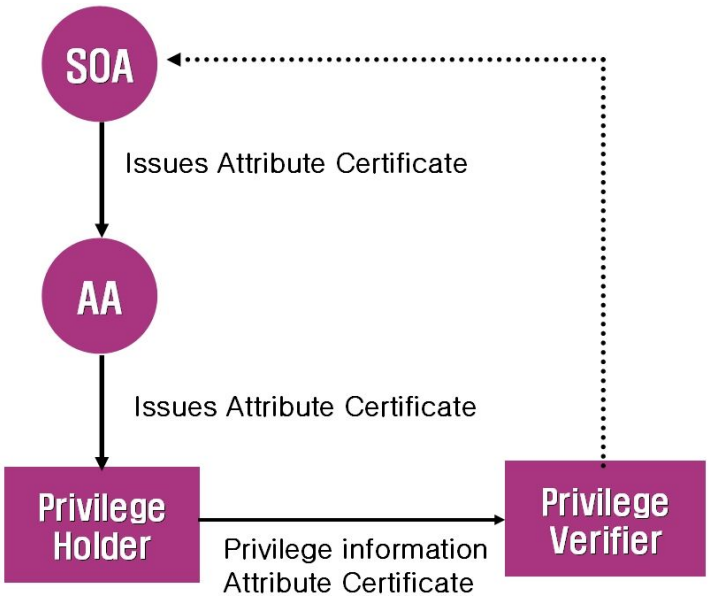
PKI내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미하며 다음의 기능을 수행한다.

① 자신의 비밀키/공개키 쌍을 생성할 수 있어야 한다.
② 공개키 인증서를 요청하고 획득할 수 있어야 한다.
③ 전자 서명을 생성 및 검증할 수 있어야 한다.
④ 특정 사용자에 대한 인증서를 획득하고 그 상태를 결정할 수 있어야 한다.
⑤ 인증 경로를 해석할 수 있어야 한다.
⑥ 디렉토리를 이용하여 자신의 인증서를 다른 사용자에게 제공할 수 있어야 한다.
⑦ 인증서 취소 목록을 해석할 수 있어야 한다.
⑧ 비밀키가 분실 또는 손상되거나 자신의 정보가 변했을 때(예 : 조직의

탈퇴)인증서 취소를 요청할 수 있어야 한다.

2.3.2.2 PMI(Privilege Management Infrastructure)

PMI는 인증서 구조에 사용자에 대한 속성 정보를 제공하여 권한 관리가 가능하도록 하는 속성인증서를 발급, 저장, 유통을 제어하는 기반구조이다. PKI가 단순한 사용자의 신원확인만을 제공하는 여권이라면 PMI는 사용자의 속성정보를 통해 다양한 접근제어가 가능한 비자와 같은 역할을 수행한다. 이러한 속성 인증서가 정보보호 메커니즘으로 활용되기 위해서는 속성 인증서의생성기관, 속성 인증서 소유주, 응용 서비스 시스템 등에서 원활히 동작할 수 있어야 한다. PMI는 속성 인증서의 발급, 저장, 유통, 검증 등을 포괄하는 권한관리 기반구조로서 PMI를 구성하는 다양한 방법에 의해서 속성 인증서의 활용방식과 응용 서비스 환경이 영향을 받게 된다. 아래 (그림 2-7)은 PMI의 구조를 표현하고 있다.



(그림 2-6) PMI의 구조

SOA(Source Of Authority)는 전자서명기반의 루트CA(Certificate Authority)와 유사한 역할을 하는 기관으로 Privilege Verifier가 신뢰하는 속성인증기관이다. AA(Attribute Authority)는 SOA로부터 권한의 전부 또는 일부를 위임받아 속성인증서 발급업무를 수행한다. Privilege Holder는 인증서를 통해 AA로부터 권한에 대

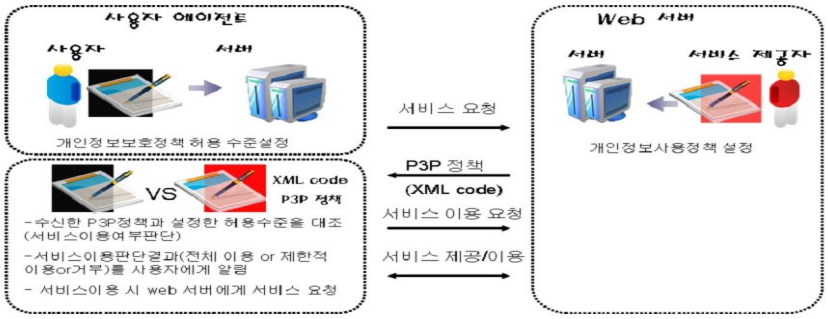
한 소유권을 보증 받은 자로서 전자서명기반의 END-Entity에 해당한다. Privilege Verifier는 속성인증서를 받아 권한을 판별한다.[27][28]

2.3.3 개인정보보호기술

2.3.3.1 P3P(Platform for Privacy Preferences Project)

P3P는 웹사이트에서 사용자 프라이버시를 보호하기 위한 개인정보 정책을 기술하는 W3C(the World Wide Web Consortium)에서 제정한 표준화된 프라이버시 보호 기술이다. P3P의 근본 목표는 웹 브라우저나 다른 사용자 도구가 에이전트를 통해 자동적으로 해당 웹사이트의 프라이버시에 관한 정보를 읽고 사용자가 이미 설정해 놓은 정보공개 수준과 비교하여 정보를 선별적으로 제공한다.[29][30]

웹사이트의 개인정보 정책은 개인이 프라이버시에 민감한 데이터에 대해서 어떻게 사용하도록 할 것인가를 지정할 수 있으며 이 정책에 맞는 동안에만 개인정보를 사용할 수 있도록 제안한다. 개인정보 정책은 웹사이트 방문객들과 신뢰받는 관계를 만들어내는데 사용되는 주요한 컴포넌트로 기업이나 개인이 수집한 데이터, 특정 목적에 의해 수집된 데이터의 사용, 특정 사람에게 데이터의 사용허가 등을 기술한다. 개인정보 정책은 웹사이트에서 설정하여 사용자에게 보여지며 사용자는 이 정책을 기반으로 정보 공개수준을 설정하고 선별적으로 개인정보를 제공할 수 있다.[31][32]



(그림 2-7) 사용자에이전트와 웹 서버의 P3P 동작 개요

위의 (그림 2-7)은 임의의 사용자가 임의의 웹 서비스를 이용하려고 한다고 가정하여 일반적인 P3P 동작을 설명한다. 서비스 제공자는 자사의 모든 웹 페이지에 P3P 정책을 적용하고 있으며, 사용자는 해당 주소를 웹 브라우저에 입력하면 사용자의 브라우저를 사용하고 있다고 가정한다. 사용자가 해당 주소를 웹 브라우저에 입력하면 사용자의 브라우저는 그 페이지를 위한 P3P정책(XML code)을 자동적으로 받아올 수 있다. P3P정책은 그 사이트가 자신의 홈 페이지에서 수집하는 개인정보를 명시하며, 수집된 개인정보에 대한 이용여부 등을 명시한다. 이러한 P3P정책을 수신한 사용자 에이전트는 사용자가 설정한 정책과 대조하여, 해당 정책을 사용자가 수용할 수 있는 것인지 판단을 하며 사용자에게 통보하며 해당 홈페이지의 서비스 이용여부를 결정한다. 예를 들어 사용자가 설정한 정책이 수신한 P3P정책을 수용할 수 있는 범위라면 사용자 에이전트는 해당 사이트에 서비스 이용 요청을 하게 되고 자신의 개인정보를 공개하게 되며 서로간의 통신이 이루어진다. 반면 수용불가능한 정책의 범위라면 사용자에게 알리고 사용자는 서비스 이용 요청을 하지 않게 된다.[33]

2.3.3.2 XML(Extensible Markup Language)

XML은 1996년 W3C에 의해서 제안되었으며, HTML과 SGML의 장점을 수용하여 만들어진 Markup 언어이다. SGML은 문서 구조에 필요한 태그를 정의 할 수 있으며 내용까지도 포함하는 언어이다. 주로 기술문서의 정의를 위하여 사용되었던 언어이지만 복잡한 것이 단점이었다. HTML에서는 태그가 미리 정의 되어 있으며, 화면상에서 어떻게 표현되는지에 대한 정보이다. XML은 HTML을 확장하고 SGML의 복잡성을 없앤 언어로서 태그를 정의하여 문서의 구조정의가 가능한 언어이다. XML은 기업 내에서 사용되는 전표, 신청서, 견적서, 기술 문서, 멀티미디어 등의 모든 데이터를 표현하는데 사용 될 수 있다.[34][35]

1) XML의 특징

(1) 확장성(Extensibility)

XML은 TAG의 정의를 사용자가 원하는 대로 할 수 있다. 그러므로 사용자 는 문서의 태그에 자신이 원하는 적합한 의미를 내포하는 이름을 정의하고, 사용 할 수 있으며, 이는 문서가 구조적인 특징을 가질 수 있도록 한다.

(2) 문서구조(Structure)의 정의

XML에서 사용자는 태그를 정의함에 있어 단순히 새로운 태그를 생성 시키는 것 뿐만 아니라 각각의 태그들간의 관계를 정의함으로써 구조적인 문서를 작성할 수 있도록 지원한다.

(3) 유효성(validity)

XML에서는 문법상에 오류가 존재하지 않도록 엄격한 유효성 검사가 존재한다.

(4) 자료의 저장과 표현(Presentation)의 분리

XML문서는 내용을 가지고 있으면서, 표현에 대한 정의는 포함하고 있지 않다. 이는 전적으로 문서의 내용과 표현을 분리하고자하는 의도이며, 이러한 특징은 같은 문서에 대하여 다양한 표현방식이 가능하도록 지원하며, 재사용적인 측면에서도 뛰어남을 알 수 있다.

XML은 인터넷상에서 자료를 보여주거나, 특정 프로그램데이터 저장, 멀티 미디어의 표현, 전자상거래, 학술적인 용도 등 한마디로 XML의 응용 분야는 무궁무진하다고 할 수 있다. 앞서 언급 했던 것처럼 뛰어난 확장성을 가지고 있기에 사용자는 자신이 필요하면 경우에 맞는 적정한 문서의 구조를 정의하고, 그에 따라 DTD(Document Type Declaration)를 생성하고, 그에 맞추어 데이터를 저장하기만 하면 되는 것이다. 문서 검색에 있어서는 문서에 정의된 TAG가 의미를 가지고 있으므로 단순한 검색의 차원을 넘어선, 좀 더 질의(Query)에 근접한검색결과를 가져다줄 수 있으며, SMIL(Synchronic Multimedia Integration Language)와 같은 멀티미디어의 표현에 필요한 새로운 언어를 정의할 수도 있다.

2.3.4 개인정보보호 관련 모델

2.3.4.1 PISA(Privacy Incorporated Software Agent)

2001에 시작된 PISA(Privacy Incorporated Software Agent)프로젝트는 네트워크 환경에서 개인정보 유출 없이 사용자를 대신하여 복잡한 업무를 수행하는 지능형 소프트웨어 에이전트 모델을 구축하는 프로젝트이다. 즉, 사이버 공간에서 찾고자 하는 데이터의 정확한 수집을 사용자 대신에 지능적으로 수행할 수 있는 에이전트인 지능형 소프트웨어 에이전트(Intelligent Software Agent : ISA)를 개발하는 것이다.

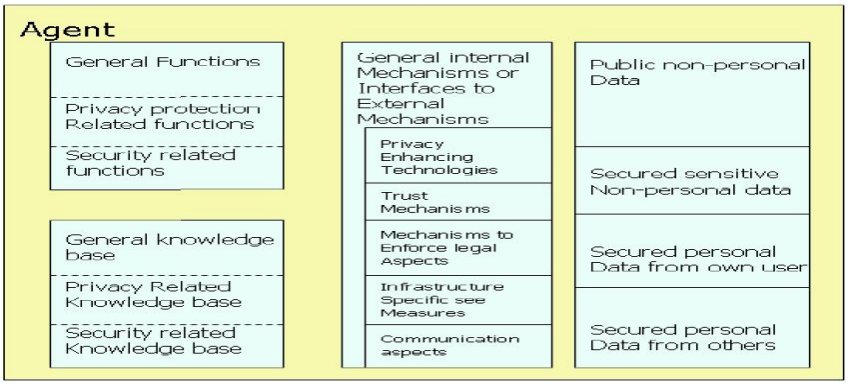
지능형 소프트웨어 에이전트는 복잡한 네트워크 환경 하에서 사용자의 편의를 제공하기 위해 독립적으로 작동하는 소프트웨어와 하드웨어를 지칭한다. 여기에는 일반적인 개인 에이전트, 특정 작업을 수행하는 에이전트 그리고 개인정보의 보호를 고려하는 서비스 에이전트 등 세 가지 종류의 ISA가 있다. ISA는 자동화된 방식으로 업무를 처리하기 위해 에이전트는 사용자의 개인정보를 소유하게 된다. 이는 ISA기술이 프라이버시에 대한 중대한 위협이 된다는 것을 명백히 드러내는 것이다. 따라서 ISA 개발 시 개인정보 보호가 중요 과제로 간주되고 있다.

1) PISA 구조

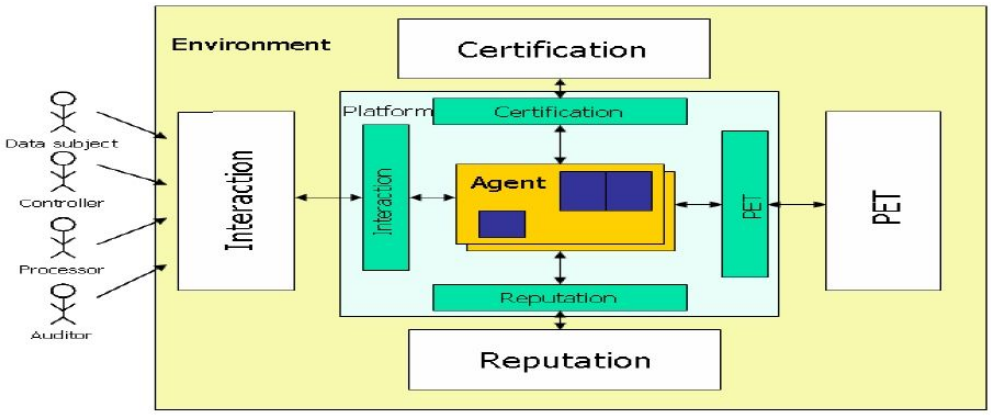
개인정보에 대한 침해 공격으로부터 ISA를 보호하기 위해서 ISA에는 다음과 같은 부분이 필요하다.

- 개인정보 보호 관련 기능을 내장하고 있어야 하며, 이러한 개인정보 보호 기능을 갖는 PET와 같은 메커니즘이나 인터페이스를 갖고 있어야 한다.
- 정책의 노하우를 내장하고 있어야 하며 데이터 보호 지침에 따라 개인정보를 보호하기 위해 정책을 수행할 메커니즘을 갖고 있어야 한다.

ISA는 대상이 데이터 주체(Data Subject), Controller 혹은 Processor의 역할을 하는가에 따라 논리적으로 나뉘어 있다. 데이터 주체는 Natural Person에 연관되며, Controller와 Process는 Natural Person, Legal Person 모두에 연관된다. PISA에서 개인정보 보호는 PET, 증명(Certification), 상호작용(Interaction), 평가(Reputation)의 조합으로 이루어진다. 이러한 내용을 그림으로 나타내면 (그림 2-8)과 (그림 2-9)와 같다.



(그림 2-8) PISA의 에이전트 구조



(그림 2-9) PISA 모델

2) 요소기술

PISA프로젝트는 네트워크 환경에서 개인정보 유출 없이 사용자를 대신하여 복잡한 업무를 수행하는 소프트웨어 에이전트 모델을 만들고자 하는 것이 핵심이다. 이를 위해서 PISA 프로젝트의 기본적인 모델은 다음과 같은 여러 발전된 기술을 통합하고 있다.

(1) 에이전트 기술 : 에이전트는 주어진 업무를 수행할 때 실제로 능동적으로 정보를 수집해야하는 인공지능 정보 검색을 위한 소프트웨어이다. 예를 들어, 에이전트는 영화의 장르나 영화에 나온 배우들은 기반으로 사용자가 좋아하는 영화가 무엇인지를 학습할 수 있어야 하며 실제적으로 사용자가 좋아하는 영화가 출시되었을 때 티켓을 구매할 수 있는 판단력을 가져야 할 것이다.

(2) 데이터 마이닝 : 데이터 마이닝은 방대한 데이터베이스에서 이전에는 알려지지 않은 정보를 자동적으로 추출해 내는 기술로서 개인정보 보호에 반드시 필요한 기술 중의 하나이다. 웹 상에서의 데이터 마이닝을 통해 사람이 수행하기에는 많은 양의 웹 사이트가 분석되어지고 웹 사이트로부터 노출되는 위험이 평가되며 개인정보 침해가 감지된다.

(3) 암호화 : 개인정보 보호 차원뿐 아니라 업무 내용의 기밀성을 위해서 데이터의 암호화가 필수적이다.

(4) 시스템 설계 기술 : 개인정보 보호 관련 법률 및 표준을 실제로 구현하기 위해서 기술적 자문 역할을 하고, 법적인 조건을 기술적 단계로 만드는 시스템 설계 기술이 요구된다.[39][42]

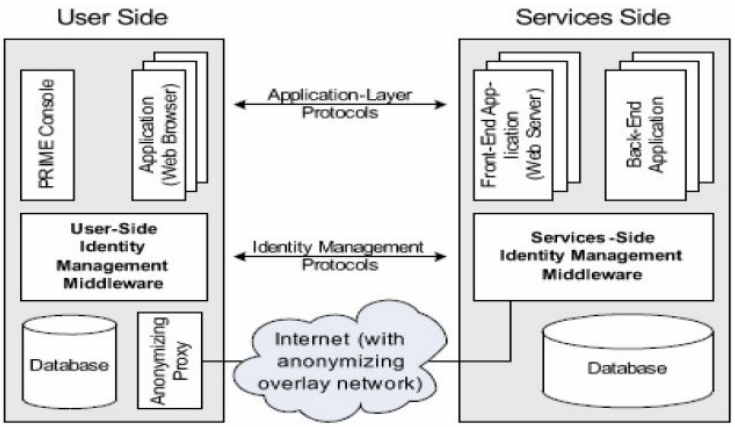
2.3.4.2 PRIME(Privacy and Identity Management for Europe)

PRIME(Privacy and Identity Management for Europe) 프로젝트는 유럽의 주요 연구단체들을 중심으로 W3C 등 주요 표준화기관과 연계된 개인의 프라이버시 보호를 위한 프로젝트이다. PRIME 프로젝트는 개인들이 정보화 사회에서 그들의 행위와 무관하게 스스로 개인정보를 제어하여 그들의 자치를 보호하는데 목적이 있다. 정보, 사회, 경제, 전문적인 분야를 총괄하는 정보화 사회 전반에 걸쳐 개인정보를 제공하도록 하고 최종 사용자에게 개인정보를 제공하는 ID관리에 초점을 맞추고 ID관리의 개인정보를 위한 프레임워크를 제안하기 위해 프로젝트를 수행하고 있다. 이것은 개인들이 정보화 사회에서 그들의 행위와 무관하게 스스로 개인정보를 제어하고 그들의 개인정보 보호를 제공받고 정부, 경제, 전문 분야 등 정보화 사회의 전반에 걸쳐 개인정보 제공을 위해 연구를 수행 중이다. 또한 편리한 컴퓨터 사용자 인터페이스, 온톨로지(ontology), 인증, 암호화 기술을 기초로 하고 최신의 ID 관리 기술과도 상호 동작하고 프로그램 개발자나 서비스 제공자, 애플리케이션 운영자 등 특정 산업과도 잘 적응되도록 표준 기술을 개발한다. 즉 사용자 자신이 그들의 ID를 관리하고 개인정보를 통제할 수 있는 기술을 개발하고 나아가 이 개인정보가 강화된 ID 관리 기술을 퍼베이시브 컴퓨팅(pervasive computing)까지 확대시키는 것이다. 이를 위해서는 현재의 컴퓨팅 환경뿐만 아니라 미래 환경의 다양한 컴퓨팅

시나리오, 개인정보와 보안을 통한 통신과 검증뿐만 아니라 개인정보를 위한 다양한 기능을 제공하는 방안에 대하여 연구하고 있다.

1) PRIME 구조의 운용

PRIME 구조는 사용자와 서비스 제공자를 위한 프라이버시와 identity관리의 포괄적인 해결책을 제공한다. 사용자 관점에서는 개인정보와 증명을 위한 중앙 보관장소를 제공하는 이것을 보호하기 위해 소프트웨어 층을 두고 있다. 서비스 제공자측면에서 사용자가 자신의 데이터를 사용할 때 상호작용할 수 있는 구조를 제공한다.[42][49]



(그림 2-10) PRIME 구조의 운용

제 3 장 e-business 환경 내 문제점

3.1 e-business

3.1.1 e-business 정의 및 동향

e-business는 인터넷뿐만 아니라 EDI(Electronic Data Interchange)나 CALS(Commerce At Light speed) 등의 컴퓨터 네트워크를 인프라로 하여, 고객이나 파트너 기업과 온라인으로 거래하는 전자상거래를 비롯해서, 고객, 파트너, 종업원, 주주 등에 대한 정보제공이나 마케팅 활동의 응용 등에 네트워크(Network-base)에서 이루어지는 업무 활동 기반을 폭넓게 의미한다.[37]

아더앤더슨은 e-business란 “네트워크화된 기술을 이용하여 상품, 서비스, 정보 및 지식의 전달과 교환을 효율적으로 하는 것이다”라고 정의하고 있다. 또한 e-business는 단순한 최신 기술의 결합이 아니라, 비즈니스를 온라인상에서 확장하여 고객과의 관계를 비약적이고 개선하고, 거래 파트너간의 비즈니스 프로세스를 합리화하며, 또 거기에 드는 비용을 대폭적으로 절감한다. 즉, 이것은 전자상거래에서 한걸음 더 나아가 보다 넓은 관점에서 비즈니스 역할 전체를 포괄적으로 파악하는 개념이라 하겠다. 다음은 산업자원부가 발표한 최근 우리나라의 e-business 추진 동향으로써 아래 (표 3-1)과 같다.[36][40]

(표 3-1) 한국의 최근 e-business 추진동향 **(단위 : 억원)**

구분	2001년	2002년	2003년	2004년	2005년	2006년
전자상거래	118조	177조	235조	314조	351조	390조
시장규모	9,800	8,100	0,250	0,790	1,440	1,093
(증가율)	(107%)	(49%)	(32%)	(34%)	(12%)	(12%)
총거래액	1,308조원	1,386조원	1,555조원	1,627조원	1,676조원	1,8996조원
전자상거래율	9.1%	12.8%	15.1%	19.3%	21.0%	20.5%

3.1.2 e-business 유형

e-business 유형은 참여하는 경제주체들, 즉 고객 또는 소비자(Customer), 기업(Business), 정부(Government) 간의 관계를 기준으로 구분하는 것이 일반적이다.[36][39]

1) B2B(Business-to Business, 기업간 전자상거래)

기업 간에 발생하는 주문, 조달, 생산, 판매, 물류 등의 기업활동 정보를 네트워크상에서 교환한다. 현재 e-비즈니스의 중심이 B2C에서 B2B로 전환되었으며, e-마켓플레이스(e-Marketplace : 다수의 기업 구매자와 판매자가 제품(부품, 완제품)을 최적의 조건으로 서로 사고 팔 수 있도록 하는 인터넷상의 가상공간 등이 대표적인 유형이다.

2) B2C(Business to Customer Transaction)

기업이 고객에게 제품, 서비스를 전달하는 수단으로서, 인터넷 쇼핑몰에서 이루어지는 가장 일반적인 전자상거래를 말한다. 기업과 소비자가 거래당사자로서 인터넷을 통하여 상품 또는 용역에 대한 매매계약을 체결하는 계약당사자가 되기 때문에 이러한 경우 기업의 우월적 지위 또는 사이버공간상의 공간적 제약으로 인하여 특히 소비자 보호, 개인정보보호 등의 법률적 문제가 특히 중요시 된다.

3) B2G(Business to Goverment)

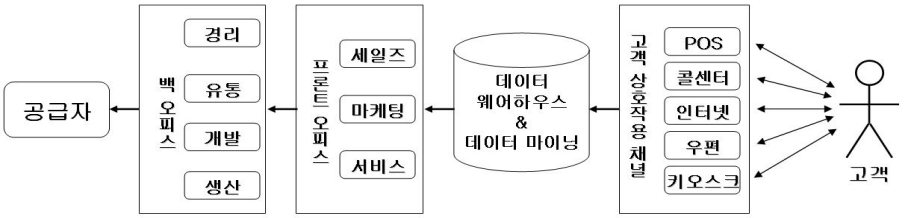
정부가 민원업무 및 행정서류를 처리하거나 기업 또는 기업과의 거래활동을 할 때 인터넷 등의 네트워크 통해 처리하는 것이다. 전자정부(e-Goverment), G2B(국가종합전자조달시스템), B2G(기업・정부간 전자상거래), G2C(정부・개인 간 전자상거래) 등이다.

4) C2C(Customer to Customer, 소비자 거래)

개별 개인간에 이루어지는 형태의 거래로서 개인과 정보공유 서비스인 P2P(Peer to Peer)서비스가 대표적이다. 즉 개인 간 거래는 개인과 개인이 중간 유통과정을 거치지 않고 직접 인터넷을 이용하여 이루어지는 형태의 거래를 말한다. 이러한 거래는 컨텐츠 뿐만 아니라 개인이 소유한 지적 정보까지 공유할 수 있기 때문에 시장규모도 커질 전망이다.

3.2 사례분석

3.2.1 CRM 정의

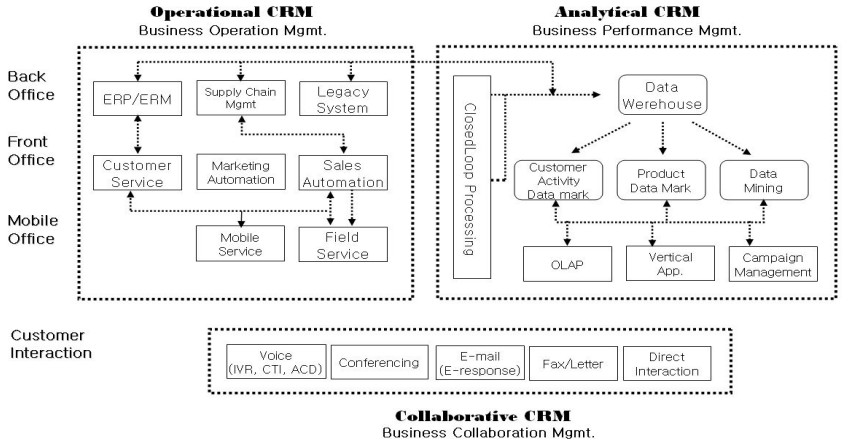


(그림 3-1) CRM 개념

CRM(Customer Relationship Management)은 고객에 대한 정확한 이해를 바탕으로 고객이 원하는 제품과 서비스를 지속적으로 제공함으로써 고객을 오래 유지시키고 결과적으로 고객 평생가치를 극대화, 수익성을 높일 수 있는 통합된 고객 관계 관리 프로세스로 정의할 수 있다. 즉, 신규고객획득, 기존 고객유지, 수익성 등을 향상시키기 위하여 지속적인 커뮤니케이션을 통해 고객의 행동을 이해하고 영향을 끼치기 위한 광범위한 접근이라고 할 수 있다.[39]

3.2.2 CRM의 유형과 정보기술 적용

CRM의 유형은 크게 운영적(operational)CRM, 분석적(analytical)CRM, 그리고 협업적(Collaborative)CRM으로 구분할 수 있으며, CRM의 유형들에 대해 관련된 정보기술 내역을 제시한 MetaGroup의 아키텍처는 아래 (그림 3-2)와 같다.[38][39]



(그림 3-2) CRM의 유형과 정보기술의 적용

1) 운영적(Operational CRM)

CRM의 구체적인 실행을 지원하는 시스템이다. 기존의 ERP 시스템이 조직 내부의 관리 효율화를 담당하는 시스템(Back-end)임에 반하여, Operational CRM은 조직과 고객간의 관계 향상, 즉 조직의 전·방위 업무를 지원하는 시스템(Front-end)이다. 이것은 주로 영업과 서비스를 위한 시스템이다.

2) 분석적(Analytical CRM)

분석적 CRM은 영업/마케팅/서비스 측면에서 고객정보를 활용하기 위해 고객 데이터를 추출, 분석하는 시스템이다. 이를 통해 사업에 필요한 고객/시장 세분화, 고객 프로파일링, 제품 컨셉의 발견, 캠페인 관리, 이벤트 계획, 프로모션 계획 등의 기회 및 방법에 대한 아이디어가 도출될 수 있다. 고객 데이터의 과학적인 분석을 위하여 데이터 마이닝 기술이 매우 중요한 이슈로 부각되며, CRM의 다른 구성 요소인 Operational CRM, Collaborative CRM과 밀접하게 연관되도록 Closed-Loop을 구성하여야 한다.

3) 협업적(Collaborative CRM)

1990년대 후반기부터 인터넷을 기반으로 한 비즈니스의 성장 및 오프라인 기업의 온라인화가 가속화되면서 인터넷에 대응하는 신 개념의 CRM이다. 협업은 분석

과 운영 시스템의 통합을 의미한다.

다음 (표 3-2)는 CRM 시장 부분 및 특·장점에 대하여 정의한 표이다.

(표 3-2) 국내기업의 산업별 CRM 도입방향

산업부문	접근방식	도입 시 기대성과	향후과제
금융	수익성 높은 VIP 고객군 선별	차별화된 고객서비스 제공, 위험관리, 수익성관리의 과학화	개인 및 가구세대별 데이터베이스의 통합관리
통신	통화료 경쟁보다 고객성향에 맞춘 이벤트 초점	고객의 니즈를 사전에 예측/해결	영업(본사)과 판매(대리점)부문을 통합한 CRM 적용
유통	가격에 민감한 고객과 관계에 민감한 고객 구분	할인점과 백화점간 역할 분담, 광고비 절감과 신상품 행사 프로모션의 적중률 증가	대형 외국업체 상륙에 따른 우수 고객 이탈방지
닷컴	가입자 확보 보다 실질적 수익성 확보에 주력	e-CRM으로 실시간 고객관리, 1:1마케팅을 통한 특화된 서비스 제공	매일 축적되는 많은 양의 데이터의 가공시간 및 비용극복
가전자동차	차별화된 고객만족 마케팅, 전략적 제휴를 통한 공동마케팅	차별화된 고객서비스제공, 귀족마케팅 실시. 모바일 세일즈 구현	현장(대리점, 영업소)에서 고객데이터를 수집해 정확도 제고

3.3 CRM 환경내의 개인정보 문제점

CRM의 등장은 인터넷의 급속한 확산과 디지털 정보기술의 접목을 통해 e-business라는 새로운 기업의 경영환경과 마케팅 패러다임의 변화에 따른 영향으로 고객의 가치가 중요하게 부각되면서 나타나게 되었다. 즉, e-business는 기업의 가치사슬 전체에 걸친 모든 프로세스를 자동화 및 최적화시킴으로써, 기업 활동의 효율성을 증대시키고 외적으로는 고객에게 새로운 가치를 제공함으로써 경쟁우위를 확보하고자 하는 것이다.

이런 환경에서 기업들은 타 기업과의 차별된 서비스를 제공하기 위하여 고객의 특성을 분석 및 관리함으로써, 최고의 잠재적 수익과 영향력 있는 고객을 추출하여 전략적 목표를 기반 할 수 있는 CRM의 필요성이 증가하고 있는 추세이다.

하지만 이러한 기반에서의 개인정보 수집 및 활용 시 정보주체의 어떠한 동의없이 불법수집 및 개인정보의 오·남용의 문제가 점점 대두되고 있는 실정이다. 예를

들면 기업들은 업무 효율은 물론 경영효과를 극대화시키기 위해 외주업체인 아웃소싱회사에게 민감한 개인정보를 어떠한 기술적/법적인 통제 또는 제한 없이 제공함으로써 사용자의 정보가 필요이상으로 사용되어지고 있다는 것이다. 또한 이렇게 수집된 개인정보는 고도화된 기술 및 시스템을 통해 고객의 성향부터 행동패턴까지 분석되어질 수 있어 사생활침해에 대한 우려가 증대되고 있는 실정이다. 뿐만 아니라 고객확보에만 목표를 두고자하는 홈쇼핑, 콜센터, 영업점으로부터 제공되었던 고객정보 및 구매정보와 같은 민감한 정보들은 사용 후 일괄적인 폐기조치 없이 데이터베이스에 잔존되어 기업의 영리를 목적으로 정보를 활용(스팸메일・이동전화 음성. 문자광고 메시지를 전송)함으로써 사생활 침해에 대한 문제의 심각성이 현존하고 있다는 것이다. 다음 (표 3-3)은 CRM프로세스 내에 개인정보관리에 대한 취약점 및 위험정도를 정리한 표이다.

(표 3-3) CRM프로세스내의 개인정보 침해 문제점

CRM의 종류	주 요 특 징	문제점
고객관리를 위한 Call Center /홈쇼핑 /영업점	· 고객 관계관리 기능 · 기업의 대내외적 위상제고 기능 · 종합정보센터로서의 기능	· 고객정보 확장, Lead Qualification을 통한 고객정보 및 구매 정보를 수집/활용 후 일괄적인 폐기 없이 기업의 영리 목적으로 활용가능
텔레마케팅 아웃소싱	· 기업의 비용절감, 위험분산, 경영의 유연성과 효율성을 극대화하기 위해 외부의 전문공급업체에게 맡김. - 고객이탈방지 및 고객활성화, 감사전화, 맴버쉽 마케팅	· 필요이상의 민감한 개인정보가 어떠한 기술적/법적인 통제 또는 제한 없이 외부업체에게 제공되어짐에 따라 개인정보 오·남용에 대한 문제 발생가능
고객관리를 위한 전자메일응답 관리시스템	· 고객의 전자메일에 대해 실시간으로 메일 서버를 모니터링 하면서 기존에 학습된 분류방법에 의해 내용이 분석 이해되어 자동으로 내용 회신 및 담당 관리자에 의해 처리되는 시스템	· 고객이 제시한 메일과 그에 대한 사용자의 기존 이력 및 내역 서비스에 대한 정보를 담당 관리자에 의해 처리되어짐으로써 개인정보 유출에 대한 문제발생 가능
데이터마이닝	· 이전의 고객정보를 기반으로 유의한 패턴을 찾아내는 기술 - 사례기반추론, 협업 필터링, 장바구니분석 등의 기술이 있음	· 고도화된 기술 및 시스템을 통해 고객의 성향부터 행동패턴까지 분석되어질 수 있어 사생활침해에 대한 우려가 높음

이와 같이 개인정보 침해 우려 부분에 있어 개인정보 보호 측면에서 고려되어져야 할 주요 이슈 및 대응방안은 아래와 같이 정리될 수 있다.

· **익명성(Anonymity) 또는 아호(Pseudonymity)**: 사용자 정보는 불법적 또는 악의적 목적으로서의 인용 측면에서 보호 하고자 필요시 사용자 정보에 대한 책임추적성(Accountablity)이 보장되어야 하며, 적용되는 목적에 따라 다른 등급 차원에서의 익명성이 보장 되어야 한다.

· **사용자 동의(Notice)**: 웹 시스템 환경 내 점점 개인정보가 분업화, 다각화 되어지면서, 한번 입력 된 개인정보가 필요한 곳에 효과적으로 사용 되어 지는 방법과

정보가 필요한 곳에서만 사용자의 동의아래 사용되어 질 수 있는 방안이 필요하다.

· **정보의 수집 및 제어(Information gathering and Access):** 사용자는 필요시 자기 정보에 대하여 접근 및 변경이 용이하여야 한다. 혹 사용자의 동의 없이 개인정보에 접근하고, 수집하려 할 때를 고려하여 제도적, 기술적 측면에서 개인정보를 보호하기 위한 접근 제어 방안은 매우 중요한 개인정보 해결방안 중의 하나이다.

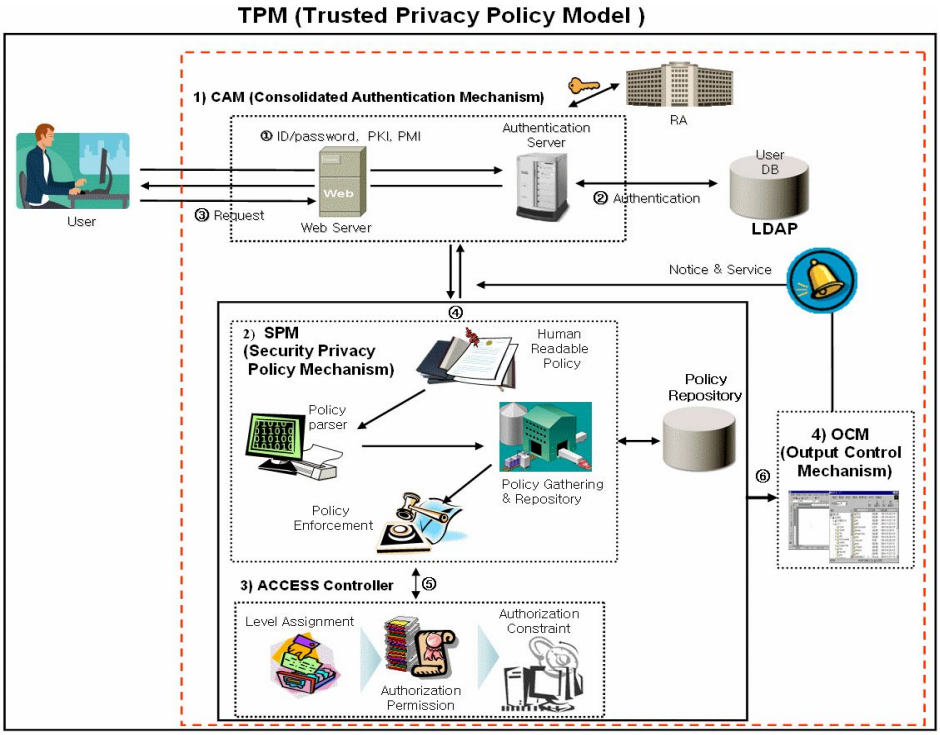
· **정보보안(Security):** 개인정보를 활용(수집 및 관리· 운영) 측면에서 기술적, 제도적, 관리적 측면에서 혹 발생 될 수 있는 위험 요소에 대하여 그 피해를 최소화하기 위한 예방이 필요하며, 모니터링·교정 측면에서 정보보안 기술 및 정책, 절차 및 지침 등을 활용 하여야 한다.

위의 사례를 기반으로, 개인정보에 대한 침해유형은 크게 다음 6가지로 구분해 볼 수 있다. 1) 부적절한 접근과 수집, 2) 부적절한 모니터링, 3) 부적절한 분석, 4) 부적절한 이전, 5) 원하지 않은 영업행위, 6) 부적절한 저장 등이 있으며, 이는 지식정보사회의 발달과 더불어 점점 증가하는 e-business 환경 내 사용되는 개인정보들은 개인적으로나 사회적으로 1)개인의 사적 공간, 2)개인의 안전성, 3)사회적 배제(Social Exclusion) 초래, 4)기업과 소비자 사이에 힘의 불균형 측면에서 중대한 위협이 될 수 있다.

제 4장 개인정보보호 모델(TPM)

4.1 TPM Architecture

본 논문에서는 앞서 제시된 개인정보 관리에 대한 문제점을 해결하기 위해 신뢰할 수 있는 개인정보 보호모델(TPM-Trusted Privacy Policy Model)을 제시하였다. TPM은 4가지 주요메커니즘(1. 통합사용자 인증 메커니즘-CAM, 2. 개인정보정책 메커니즘-SPM 3. 접근통제메커니즘-Access Controller 4. 안전한 개인정보 분배 메커니즘-OCM)으로 구성되어있으며, 그 기본 구조는 아래 (그림 4-1)과 같다.

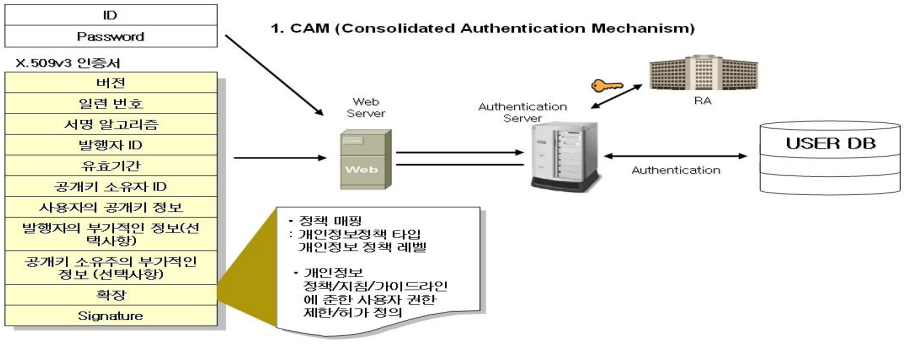


(그림 4-1) TPM Architecture

사용자가 웹사이트로부터 원하는 서비스를 제공받고자 접근을 시도할 때, 가장먼저 ① ID/Password 또는 PKI/PMI를 활용하여 Web Server에 접근한다. ② 이렇게 제공된 정보는 검증된 기관으로부터 확인 및 검증을 받은 후, ③ 사용자별 정보공유 수준에 적합한 정책할당을 요청한다. ④ 인증된 사용자 정보는 정책저장소에 정의되어있는 정책을 기반으로 시스템 환경에서 활용/설정(삭제, 수정, 폐기)될 수 있도록 변환시킨다. 이때, ⑤ 서비스 제공자는 ACCESS Controller를 활용하여 사용자 정보와 서비스 제공자의 정책을 비교, 분석한 후 사용자 속성대비 레벨에 대한 권한을 부여한 뒤, ⑥ XML기반의 OCM메커니즘을 활용하여 안전한 정보배분 및 Notice 기능을 제공 받는다.

4.2 TPM Mechanism

4.2.1 CAM(Consolidated Authentication Mechanism)



(그림 4-2) CAM(Consolidated Authentication Mechanism)

CAM(Consolidated Authentication Mechanism)은 사용자가 TPM(Trusted Privacy Policy Model)모델에 접근하고자 할 때 필요한 허가를 사용자 신분/권한을 확인하기 위한 검증단계 메커니즘이다.

즉, ID/Password 또는 X.509 V3.0 인증서를 통해 접근 가능하며, X.509 V3.0 인증서를 활용할 경우 암호화 기반의 강한 신분확인(Strong Authentication)을 가능하게 한다. 또한 X.509 V3.0 인증서의 구성요소 중에 인증 정책 등 여러 가지 사항을 포함할 수 있는 확장필드를 활용함으로써 미리 정의된 개인정보 정책/지침/가이드라인을 기반으로 사용자별 정책 타입 및 레벨이 정의되었을 때 권한에 맞는 접근 제한 및 허가가 가능하도록 활용되어질 수 있는 메커니즘이라 할 수 있다. 이러한 구조는 향후 프라이버시에 관련해서 익명성과 아호에 대한 문제를 책임추적성을 통해 보호되어질 수 있으며, SPM(Security Privacy Policy Mechanism)에서 미리 할당된 개인정보 정책을 기반으로, 그에 준한 사용자 속성 및 검증하는 기능을 수행할 수 있다.

4.2.2 SPM(Security Privacy Policy Mechanism)

SPM은 e-business 환경 내 개인정보를 공유 및 사용하기에 앞서 개인정보정책을

바탕으로 비즈니스의 중요 정도를 고려하며 개인정보의 활용, 공개, 보안정도를 적절한 정책, 절차, 가이드라인을 제시해주는 메커니즘이다. 즉, 개인정보 정책을 생성 및 변경, 수정, 검증할 수 있는 SPM는 OECD 프라이버시 보호 8대 원칙을 기준으로 공개 여부를 명시함으로써, 개인정보교환 및 공유나 타 기관과의 연동 시 정보의 중요도 및 등급별 역할 기반에 접근통제가 가능할 수 있도록 기준점을 제시하는 역할을 한다. 또한 이러한 메커니즘은 관리자나 운영자에 의한 통제 및 관리가 가능하도록 설계의 기본이 되어 체계적이고 독립적인 프라이버시 보호 방안을 제시할 수 있을 뿐만 아니라 개인정보 DB와 연동 시 정보의 무결성 보장에 필요한 핵심 부분이다.

아래 (표 4-1)은 개인정보 정책에 준하여 개인정보별 공개수준 정도를 5등급으로 분류하여 나타낸 표로써 이름/성별과 같은 기본적인 정보는 보안정도가 가장 낮은 P5 등급을 설정하였고, 주민등록번호/신용정보와 같은 민감한 개인 기밀정보는 P1 또는 P2와 같은 높은 보안등급으로 설정되어짐을 보여주고 있다.

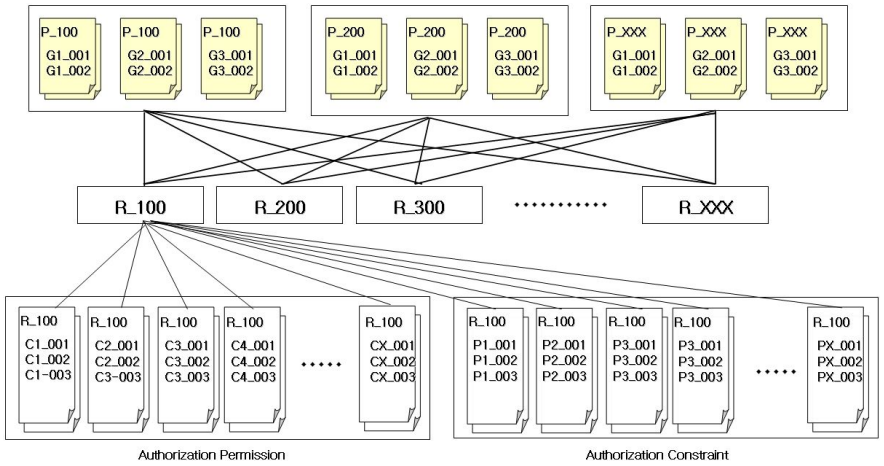
(표 4-1) 유형별 사용자정보를 활용한 보안등급 분류표

사용자 정보	의미	개인정보 정책 지정 및 상세 내역
이름	사용자 이름	한글(일반정보:P4)　영문/한자(P3)
성별	남/여 구분	P4 / P5
나이	사용자 나이	10-20, 20-30,30-40 (P4 / P5) 정확한 나이(P3)
주소	사용자 주소	지역구 구분-서울,경기(P4 / P5) / 정확한 나이(P3 / P2)
직업	사용자 직업	직업 일반:학생,전문직 등 (P4 / P5) 상세정보 직책, 직장주소, 연락처 (P3 / P2)
학벌	사용자 교육 정도	교육 일반 : 석사이상/대졸/고졸 (P4 / P5) 상세:학교명,전공,학점 등 (P3 / P2)
전화번호	사용자 연락처	집전화 / 핸드폰 / 직장전화 / 비상연락처 (P3 / P2)
주민번호	사용자 신분정보	(P1/P2)
지불정보	사용자 지불정보	신용카드/직불,후불카드 번호, 만료기간, 카드 타입 (P1)
의료진료정보	사용자 진료정보	병명/진료기관,처방정보,감염성여부 (P1/P2)
구매정보	사용자구매 정보	구매상품종류, 구매 비용, 횟수, 구매장소, 구매방식등(P2/P3)
재산여부	사용자재산정도	자동차,토지,주식등 (P1/P2/P3)
전과 여부	사용자범죄여부	범죄유형, 구속여부, 구속시 복역기간등 (P1/P2)

이렇게 각각에 5단계로 분류된 개인정보는 관련 분야/기관별 항목에 맞는 적합한 정책을 매핑시키기 위하여 역할 및 책임에 대한 세부사항들을 정의하여 개인정보 절차라 명시하였다. 이와 같이 분류된 절차 항목은 다시 운용자/최종 관리자가 실제 환경에서 통제 및 처리할 있도록 좀 더 명확하고 자세하게 분류/설정하는 가이드라인을 제시하였다.

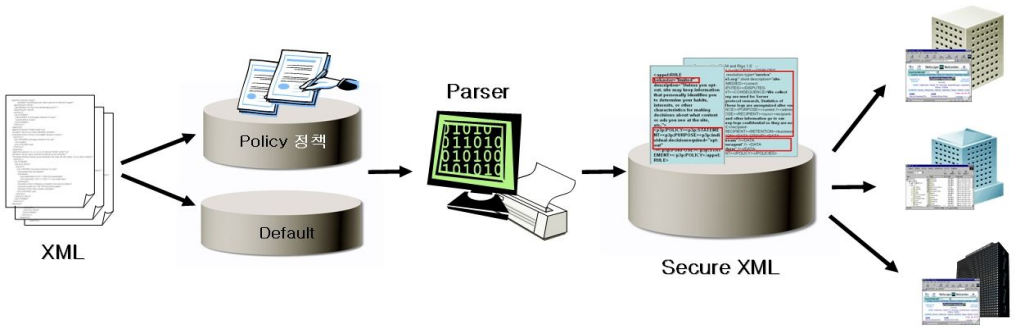
4.2.3 ACM(Access Control Mechanism)

ACM은 사용자가 기업이나 조직의 정보자원을 임의로 접근할 수 없도록 사용자의 속성대비 접근 권한의 대한 레벨을 부여하여, 적절한 권한에 소속됨으로서 레벨에 맞는 최소 자원만을 접근할 수 있도록 제공하는 메커니즘이다. 즉, 앞서 설명한 등급별 개인정보를 기준으로 사용자 속성정보의 제공정도를 기반으로 등급별 또는 역할 기반의 접근 통제가 시스템 관리자로부터 가능하도록 설계되어졌다. 아래 (그림 4-3)은 관리자 측면에서 개인정보를 속성대비 레벨 및 권한을 부여하는 가이드라인을 제시하고 있다.



(그림 4-3) ACCESS Controller

4.2.4 OCM(Output Control Mechanism)



(그림 4-4) OCM (Output Control Mechanism)

OCM은 SPM으로부터의 할당 받은 개인정보 정책 기반의 접근제어를 수행하기위하여 자기 기술적인(self-describing) 표현이 가능하도록 고안된 XML(Extensible Markup Language) 문서들이나 XSL(Extensible Stylesheet Language)과 같은 기술들을 이용하여, 타 기관시스템과의 커뮤니케이션 및 트랜잭션을 처리하는 메커니즘이다. 이러한 구조는 적합한 개인정보 정책 기반의 사용자 인증 후 사용자 개인정보를 필요로 하는 유관기관과 사용자, 유관기관들 간의 개인정보 교류시 안전하고, 활용이 용이하도록 제공함으로써 개인정보 교환 및 개인정보 요청 후 적용되어짐을 보여준다.

또한 사용자 입장에서는 타 개인정보 시스템에서 자기 정보의 공개 정도를 이해하고, 필요시 직·간접적인 통제 방안을 원활히 수행 할 수 있도록 P3P를 활용하였다. 특히 개인정보의 오남용문제에 관련해서, 개인정보 사용 시 그 사용 범위와 목적 등을 고려한 개인정보 알림("Notice")기능을 수행한다.

이와 같은 구조는 다양한 애플리케이션들을 실행하는 플랫폼 및 운영체제를 갖는 거래 사이에서 상호운용성(interoperability)을 제공한다.

제 5 장 TPM 분석 설계 및 구현

5.1 TPM 구현 시나리오

1) 사용자 A

사용자 A는 C회사의 웹 사이트를 통해 구매가 아닌 단지 이벤트 정보 및 이슈정보만을 제공받고자 한다. 하지만 이러한 혜택을 받기 위해서는 민감한 개인정보인 이름, 주민번호, 집 주소, 전화번호 등에 대한 가입절차를 거쳐야만 원하는 서비스를 제공받을 수 있다.

2) 사용자 B

사용자B는 D회사의 웹사이트를 구경 중에 필요한 물품을 발견하였고, 이를 구매하고자 한다. 하지만 구매하고자 하는 사이트는 신뢰할만한 인증마크 및 확인여부가 전혀 존재하지 않아 구매절차단계에서 필요로하는 사용자정보(주민번호, 주소) 및 결제정보를 기재하는 것에 대해 망설이고 있다.

3) TPM (Trusted Privacy Policy Model)적용 방안

TPM 시스템은 앞서 제시한 고객들이 보유하고 있는 문제점들을 해결하기 위해 제안된 모델이라 설명할 수 있다. TPM 시스템을 활용할 수 있는 주요대상은 1. 일반사용자 또는 구매사용자 2. 서비스제공업체(웹사이트 운영회사), 대기업, 공공기관, 금융기관 등으로 분류되어질 수 있다.

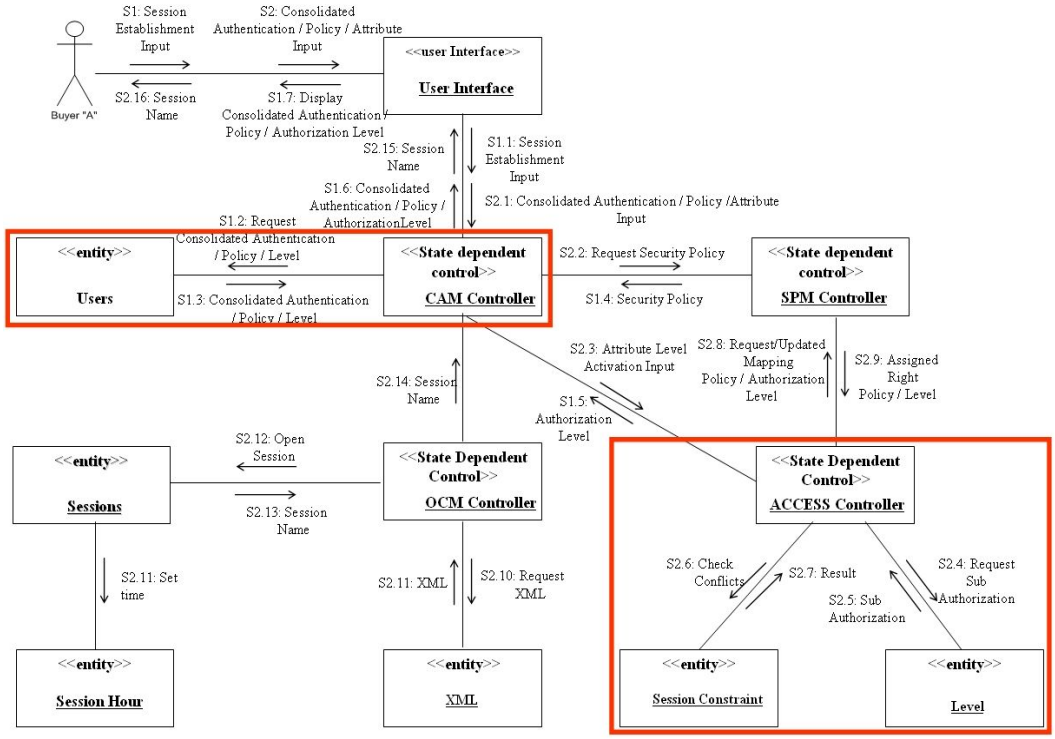
즉, 일반사용자 또는 구매사용자의 경우 웹사이트, 기업, 공공기관, 금융기관 등과 같은 업체로부터 필요로 하는 정보를 제공받거나 신뢰할 수 있는 웹사이트로부터 물건을 선택하고 신용카드를 활용한 구매절차를 밟고자 할 때 TPM 시스템에 가입해야만 한다.

또한 고객에게 서비스를 제공하고자 하는 서비스 제공업체, 기업, 공공기관, 금융기관 등의 경우 마케팅 전략에 활용되어질 고객정보 또는 구매를 하고자하는 고객이 신용결제가 가능한 사용자임을 인증/승인을 확인받고자 할 때 TPM 시스템에 가입하여야만 한다.

5.2 TPM 분석 설계

5.2.1 TPM(Trusted Privacy Policy Model) 전체 구성도

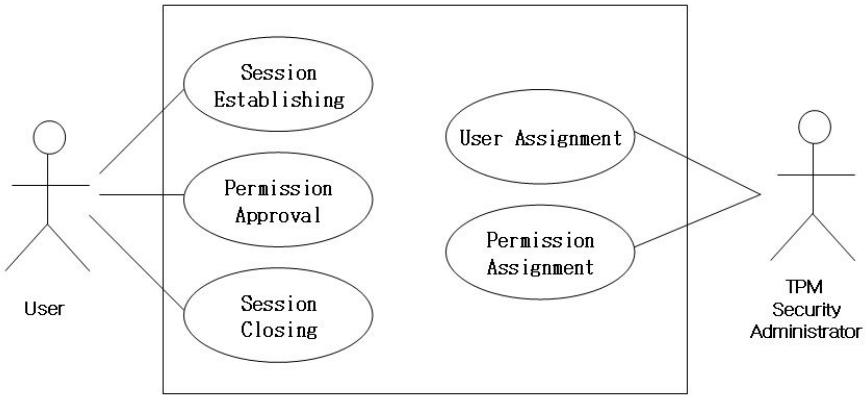
다음은 앞서 제시된 문제점을 해결하기 위하여 4가지 구성으로 이루어진 TPM의 주요 메커니즘 중 통합 사용자 인증메커니즘과 접근통제 메커니즘을 활용한 문제해결 방안을 제시하였다. 아래 (그림 5-1)은 e-business 환경내에 TPM 모델이 적용되어질 때 UML을 통해 표현해 보았으며, 이중에서 CAM(통합 사용자 인증메커니즘)과 ACM(접근통제 메커니즘)의 적용방안에 대해 소개하겠다.



(그림 5-1) 개인정보정책 분석설계도

5.2.2 CAM(Consolidated Authentication Mechanism)-통합사용자인증

TPM 시스템의 일부인 CAM에서는 아래 (그림 5-2)에서 보여주듯이 사용자와 TPM 보안 관리자를 유스케이스를 활용하여 표현하였다.



(그림 5-2) User CAM 유스케이스

사용자는 세션이 성립될 때 TPM 보안 운영자로부터 사용자 신분에 적합한 세션을 확립 받는다. 보안담당자는 속성대비 사용자에게 적절한 레벨을 부여함으로써, TPM 시스템에 접근 시 적합한 사용자이지 확인한다.

다음은 유스케이스의 세션확립에 대한 명세부분이다.

(표 5-1) 유스케이스 세션확립 명세

- Use case : 세션을 확립한 유스 케이스 - Actors : 사용자 - Precondition: System idle - Description : 세션확립을 위한 사용자 최근정보

다음은 통합 사용자 인증에 대한 상세 설명은 아래 (표 5-2)와 같다.

(표 5-2) 사용자 등록 절차

사용자 등록
[S1] 초기화 확립을 위한 사용자 정보를 넣는다. [S1.1-7] 사용자 인터페이스는 접근통제메커니즘에게 초기화확립에

대한 정보를 보낸다. 접근통제메커니즘은 사용자 요소로부터 사용자 속성대비 레벨을 요청한다.

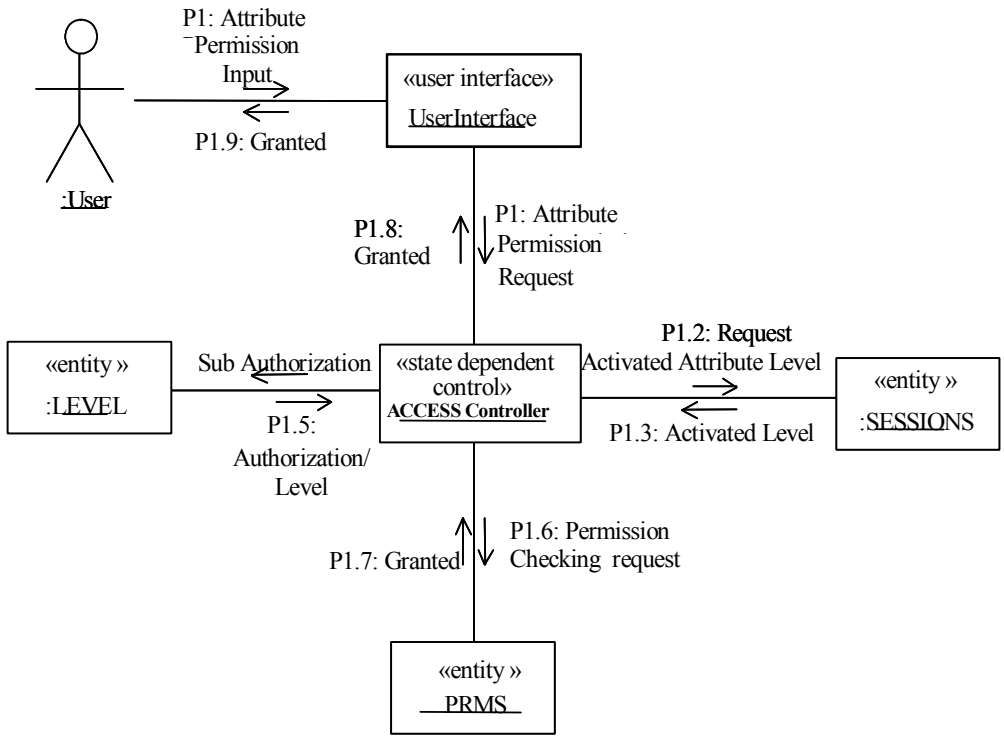
사용자 요소는 접근통제메커니즘에게 사용자 속성대비 레벨을 응답한다. 만약 적합한 레벨에 대한 사용자의 요소가 존재하지 않을 경우, 접근통제메커니즘은 사용자 인터페이스를 통해 경고 메시지를 보낸다. 접근통제메커니즘은 레벨을 보유한 요소에게 사용자의 하위 권한정보를 요청하며, 레벨 요소는 사용자의 하위 권한정보를 추론하여 접근통제메커니즘에게 응답한다. 접근통제메커니즘은 사용자 인터페이스에게 사용자가 보유하고 있는 레벨을 보낸다. 사용자 인터페이스는 초기화의 활동을 위해 사용자가 선택할 수 있는 속성대비 레벨을 보여준다.

[S2] 사용자는 초기화가 수행된 상태에서 속성을 입력한다.

[S2.1-8] 사용자 인터페이스는 접근통제메커니즘에게 초기화 수행을 위한 입력값을 보낸다. 접근통제메커니즘은 적합한 접근통제 요소가 선택되어진 사용자의 속성 값 대비 레벨과 제한 사항을 확인 요청한다. 초기화 제한적 요소는 접근통제메커니즘에게 제한된 사항과 속성대비 등급의 결과를 응답한다. 만약 속성 대비 등급이 제한사항을 갖고 있을 경우 접근통제메커니즘은 사용자의 인터페이스를 통해 경고 메세지를 보낸다. 접근 통제 요청 메커니즘은 초기화 요소로부터 초기화가 열렸음을 확인한다. 초기화 요소는 초기화 요소로터 시간설정을 요청하고 접근통제에게 초기화의 이름을 응답한다. 접근통제메커니즘은 사용자 인터페이스에게 초기화 이름을 보낸다. 사용자 인터페이스는 세션 이름을 화면에 보여준다.

5.2.3 ACM (Access Controller Mechanism)

시스템은 사용자 정보(속성)대비 적합한 접근 제어 및 통제가 이루어지는 메커니즘이다. 즉, 사용자의 속성을 통해 시스템의 허가 및 제한정도가 결정되는 것이다. 다음 (그림 5-3)은 UML을 활용한 접근통제 메커니즘을 설명하고 있다.



(그림 5-3) UML을 활용한 접근통제

(표 5-3)은 유스케이스를 활용한 접근통제 메커니즘을 명세한 부분이다.

(표 5-3) 유스케이스 적합한 접근통제 명세

- Use case : Permission Checking 유스 케이스
- Actors : 사용자
- Precondition : 사용자의 활성화된 세션
- Description : 사용자는 업무를 수행하기 요청을 시도한다.

이와 같이 접근통제메커니즘은 사용자의 속성 값 대비 레벨정도에 대한 접근승인/거부 및 검증이 어떻게 요구되어지는지 설명하고 있으며, 그에 대한 상세 설명은 아래 (표 5-4)와 같다.

(표 5-4) 접근통제 절차

접근에 대한 승인 절차

[P1] 사용자는 초기화를 승인받기 위해 이름 또는 성별에 관한 속성 정보를 입력한다.

[P1.1] 사용자 인터페이스는 접근통제메커니즘에게 허가승인에 대한 정보를 보낸다.

[P1.2] 접근통제메커니즘은 초기화 요소로부터 수행가능 한 레벨을 요청한다.

[P1.3] 초기화 요소는 사용자의 속성대비 접근 가능한 레벨을 권한을 접근통제메커니즘에게 보낸다. 만약 사용자의 이름이 초기화상태에 존재하지 않을 경우, 접근통제는 사용자 인터페이스를 통해 경고 메세지를 보낸다.

[P1.4] 접근통제메커니즘은 레벨 요소로부터 사용자의 접근 가능한 하위 권한을 요청한다.

[P1.5] 레벨 요소는 접근통제에게 사용자의 하위권한과 레벨에 대한 정보를 응답한다.

[P1.6] 접근통제는 사용자가 원하는 승인을 얻기 위해 사용자의 하위권한과, 사용자의 접근가능한 레벨을 적합한 접근제어메커니즘으로부터 인가승인을 요청한다.

[P1.7] 적합한 접근통제 요소는 접근통제에게 사용자 속성대비 권한승인을 확인한다. 만약 권한허가가 승인되지 않는다면, 접근통제는 사용자의 인터페이스를 통하여 사용자에게 경고를 보낸다.

[P1.8] 접근통제메커니즘은 사용자 인터페이스의 승인을 보낸다.

[P1.9] 사용자 인터페이스는 사용자에게 승인화면을 보여준다.

5.3 TPM Prototyping 적용방안

5.3.1 개발 환경

본 연구는 다음 (표 5-5), (표 5-6)와 같은 하드웨어와 소프트웨어의 환경에서 개발되었다.

(표 5-5) 하드웨어 환경

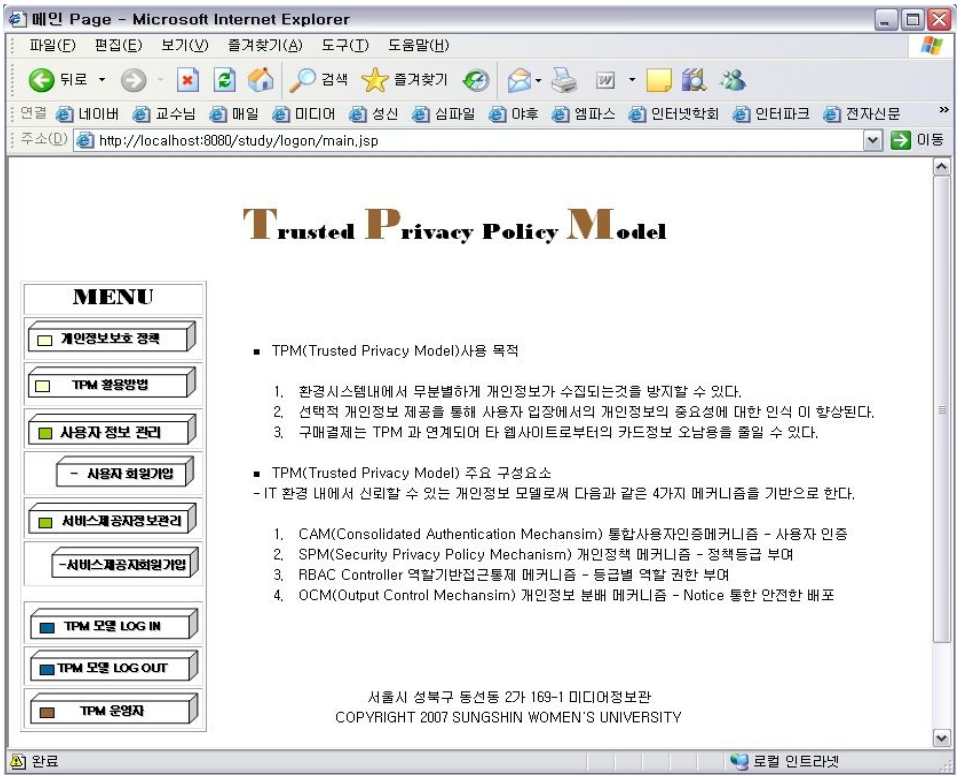
구 분	사 양
CPU	Pentium IV 2.14GHz
RAM	512MB
HDD	320G

(표 5-6) 소프트웨어 환경

구 분	사 양
OS	Microsoft Windows XP Pro
웹서버	Apache Web Server 5.0
DBMS	MySQL 5.0
개발언어	HTML, JSP, JavaScript, Java
웹브라우저	Internet Explorer 6.0 이상

5.3.2 Prototyping

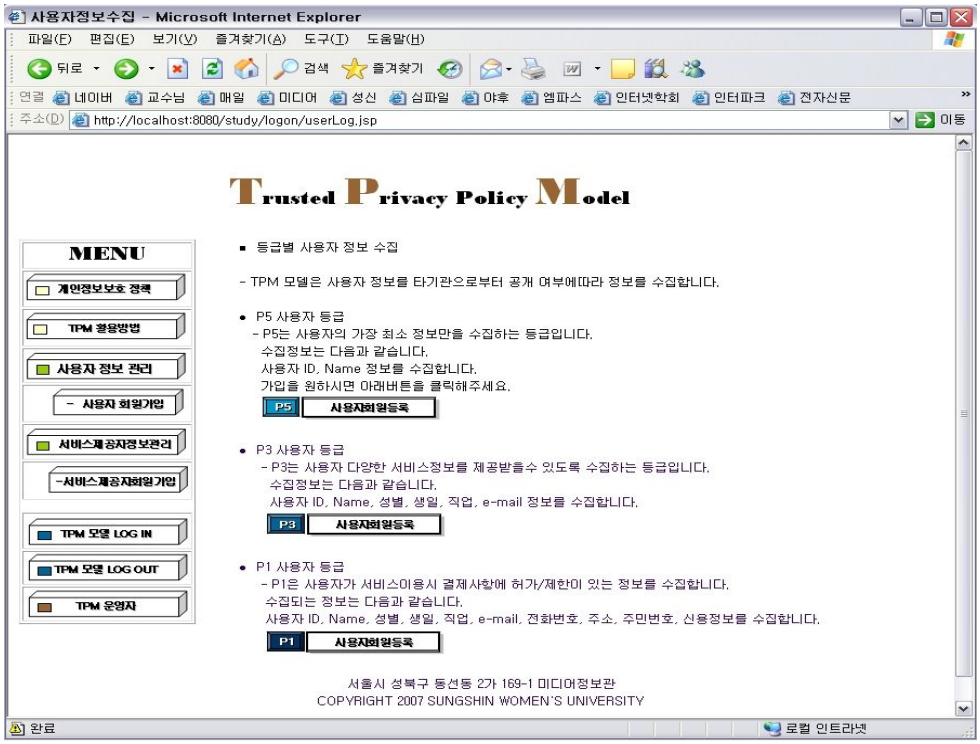
아래 (그림 5-4)는 TPM 시스템 메인화면이다.



(그림 5-4) TPM 시스템의 Main 화면

1) 일반사용자 및 구매고객

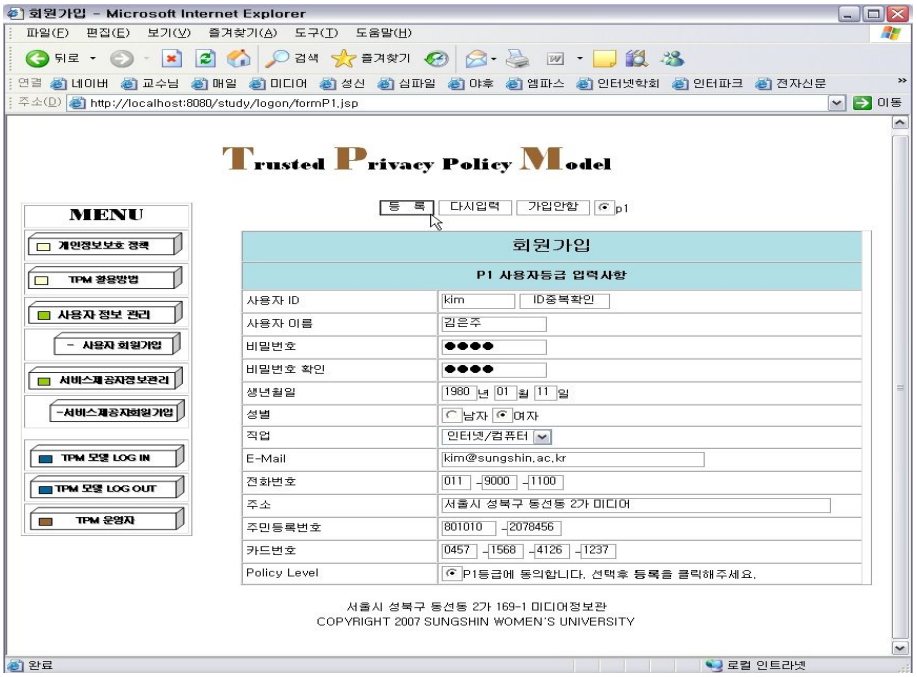
일반사용자 및 구매를 원하는 고객은 TPM 시스템에 가입을 해야 한다. 아래 (그림 5-5)는 사용자 입장에서의 등급별 회원가입을 제시하고 있는 화면으로써, 사용자별 등급은 5단계로 분류되어질 수 있으나, 본 논문에서는 3단계(P5등급, P3등급, P1등급)만을 프로토타이핑을 통해 제시하였다. P5등급은 가장 기본적인 사용자 정보로서 아이디, 성명만을 수집하는 등급을 말한다. P5 등급의 사용자는 타 기업의 쇼핑몰 사이트에 접근 시 단지 서비스정도만을 체크할 수 있으며, 부가적인 정보서비스 혜택은 받을 수 없다. 아래 (그림 5-5)는 개인정보 수집정도에 대해 등급을 분류한 화면으로써, 사용자가 원하는 등급에 가입할 수 있도록 제시하는 화면이다.



(그림 5-5) 등급별 사용자 정보수집화면

P3등급은 사용자 아이디, 이름, 성별, 생일, 직업, E-mail 정보를 수집하는 등급으로서, 이곳에 가입한 사용자는 타 웹 쇼핑몰에 접근 시 서비스 제공업체에서 제공하는 다양한 서비스 및 혜택을 부여받을 수 있다. 단, 여기에서 사용자 아이디, 이름, 성별, 직업, e-mail에 대한 고객정보를 웹 서비스 업체에게 공유해야만 가능하다. 하지만 이러한 정보 공유 역시 사용자 선택사항중의 하나이다. 아래 (그림 5-6)은 사용자가 P3등급에 가입 시 보여질 수 있는 화면이다.

(그림 5-6) P3 사용자등급 입력화면

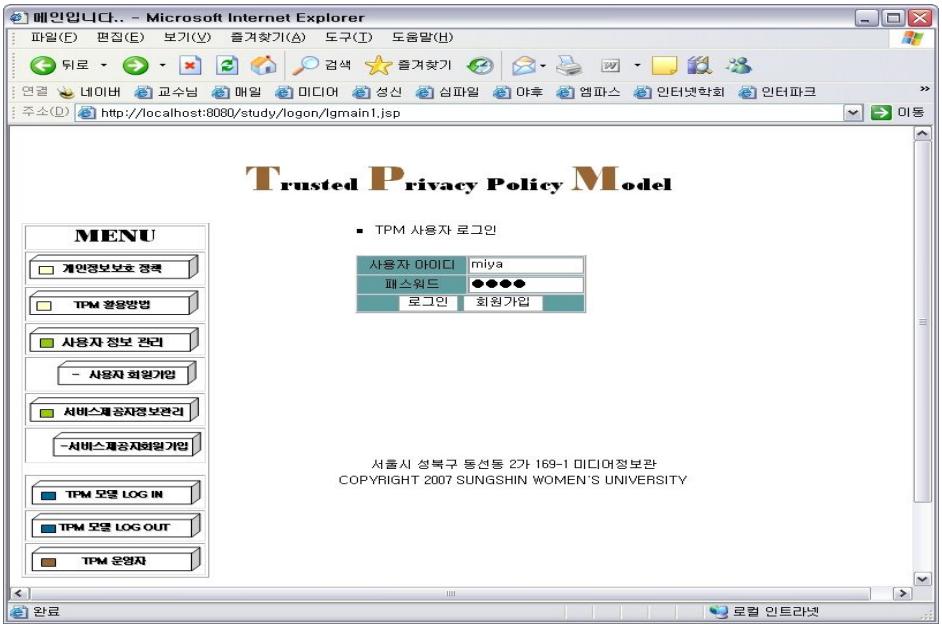


(그림 5-7) P1 사용자등급 입력화면

위의 (그림 5-7)은 P1등급 가입화면으로써 P3등급 가입 입력절차 보다 자세한 개인정보를 수집하고 있음을 알 수 있으며 주소, 주민등록번호, 신용카드번호 등이 그 추가적인 정보라고 하겠다. 이러한 정보 수집은 타 웹 사이트로부터 원하는 물품을 구입하고자 할 때 반드시 필요한 정보이다. 즉, 결제는 TPM시스템과 결제기관이

연계되어져 있기 때문에 타 웹 사이트 내에서 결제정보 및 민감한 개인정보를 입력할 필요가 없다는 것이다.

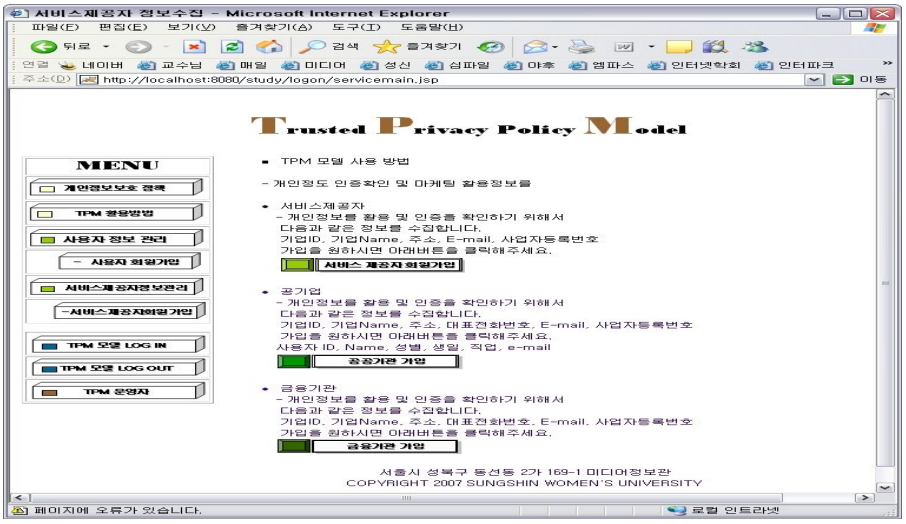
아래 (그림 5-8)은 사용자가 타 기업 사이트에 접근하기전에 TPM 시스템에 접근하여 로그인 할 때 보여질 수 있는 화면이다.



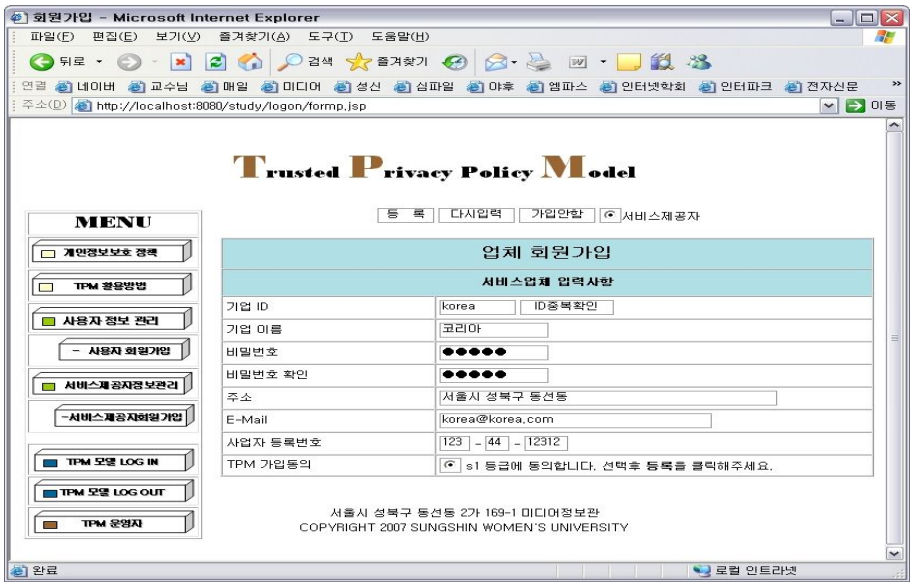
(그림 5-8) 사용자 로그인화면

2) 서비스 제공자 부문

다음은 마케팅에 전략을 수립하고자 개인정보를 필요로 하는 기업 또는 구매를 통한 거래가 발생 시 사용자 신용정보 상태를 승인 확인을 받고자하는 웹사이트 업체, 금융기관, 공공기관의 경우 반드시 TPM 시스템에 가입해야만 한다. 아래 (그림 5-9)는 TPM 시스템의 가입되어질 수 있는 업체 및 기관을 분류한 화면이며, (그림 5-10)은 서비스 제공자 입장에서의 TPM시스템에 가입할 때 수집되는 정보를 제시하고 있다.

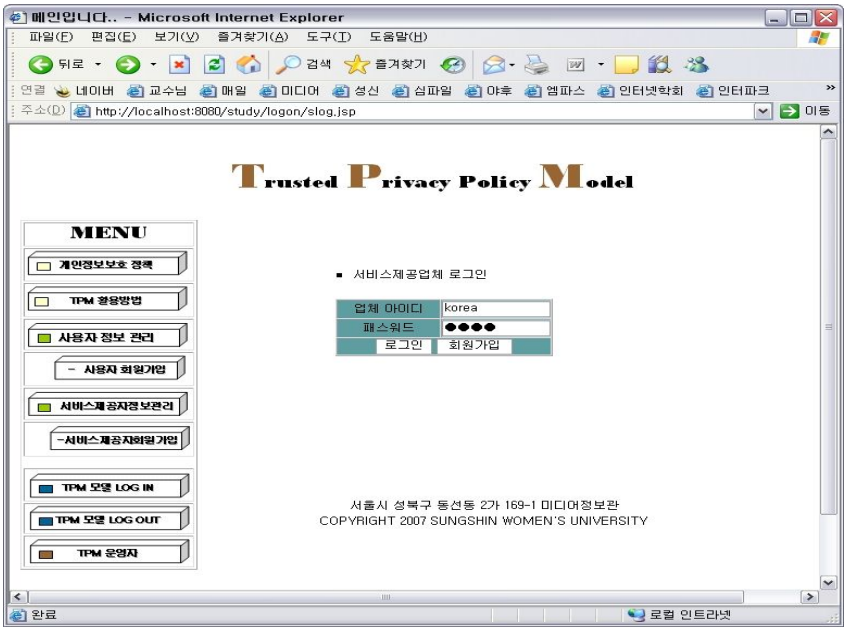


(그림 5-9) 서비스별 수집정보 화면

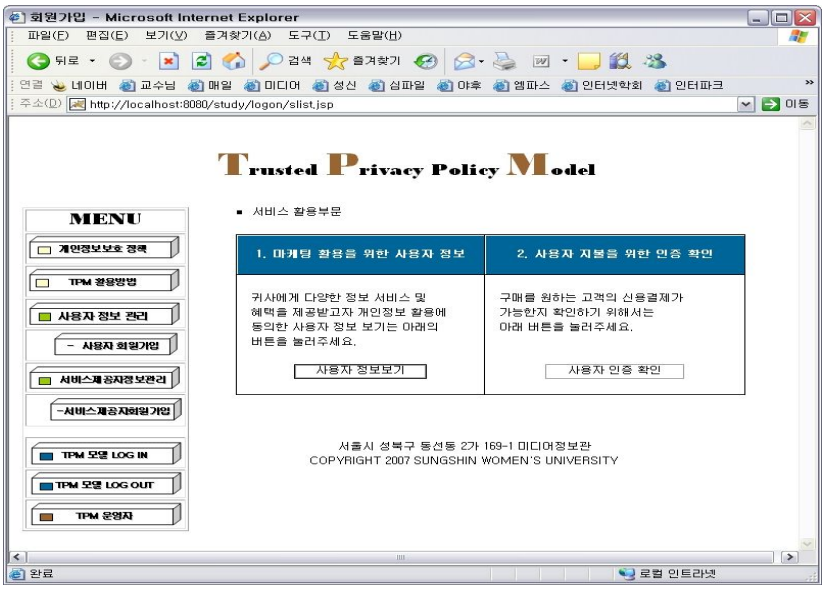


(그림 5-10) 서비스 제공자 가입화면

아래 (그림 5-11)은 서비스제공업체에서 TPM 시스템에 접근을 위한 로그인 화면을 보여주고 있다.



(그림 5-11) 서비스 제공자 로그인화면

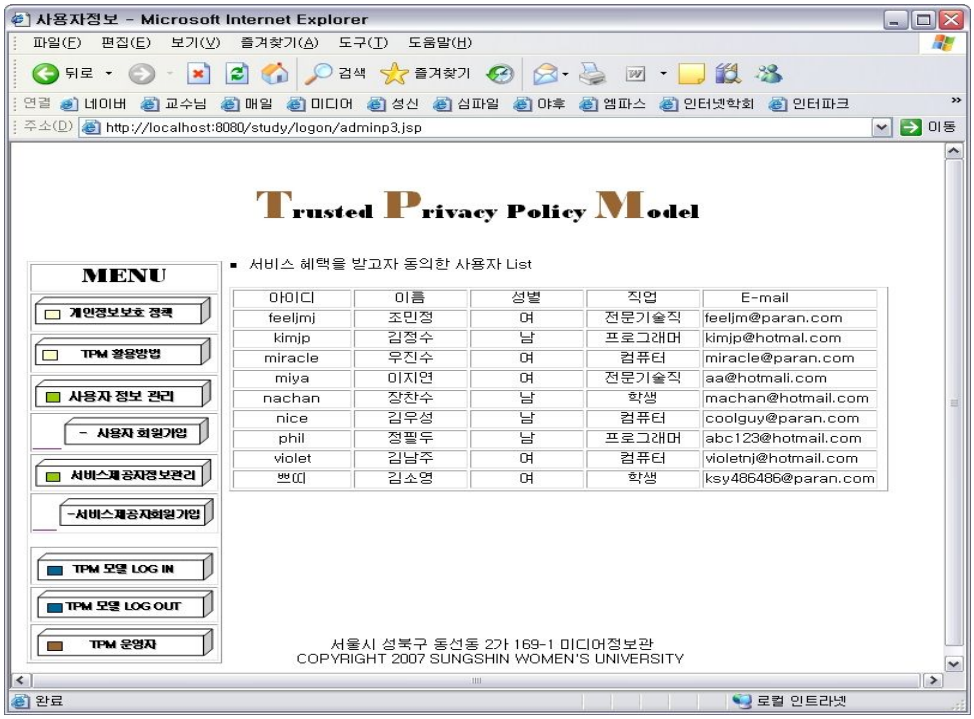


(그림 5-12) TPM 서비스 활용화면

위 (그림 5-12)는 서비스제공업체가 로그인 후 TPM 시스템의 서비스를 이용 받을 수 있는 부분은 2가지로 분류된다. 1. 마케팅 활용을 위한 사용자 정보 서비스 경우, 로그인 한 웹 서비스 제공자로부터 다양한 정보 제공은 물론 혜택을 받고자 개인정보 제공의 동의한 사용자 정보만을 제공받을 수 있다. 2. 사용자 지불을 위한 인증 확인 서비스 경우에는 사용자가 서비스제공자의 회사로부터 물품을 구매하고자 할 때 사용자의 신용결제 부분에서 요구한 물품의 금액에 대한 지불능력이 가능

/불가능한지 검증해 주는 서비스를 제공한다.

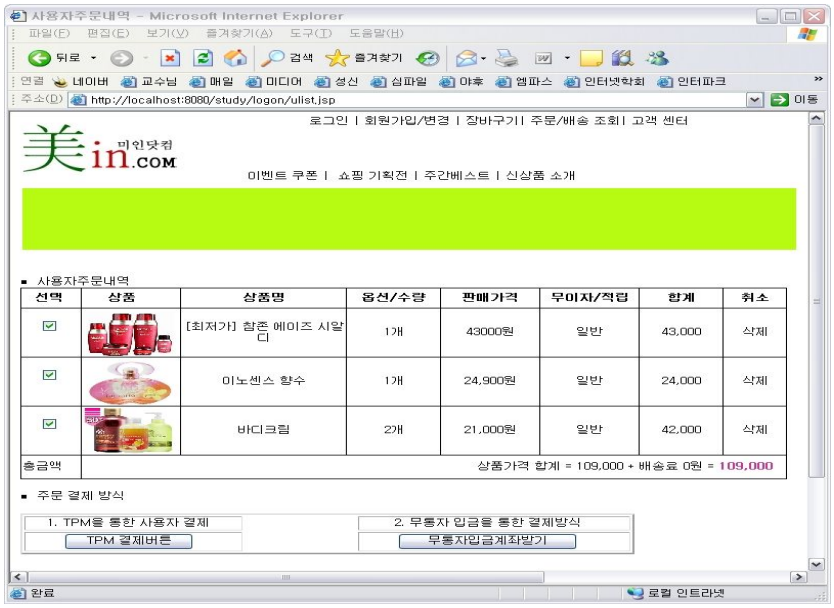
아래 (그림 5-13)은 서비스제공업체가 1. 마케팅 활용을 위한 사용자 정보 서비스를 클릭했을 때 나타나는 화면으로써, 보다 자세한 정보를 얻고자 원할 때는 고객의 동의 절차가 필요하다.



(그림 5-13) 사용자정보 활용 동의한 사용자화면

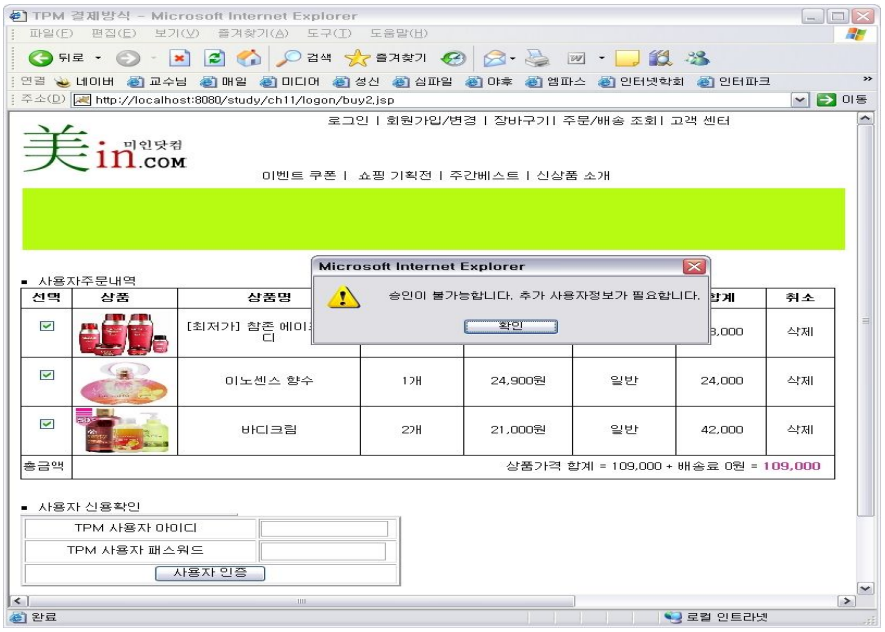
3) 사용자가 물품구매 시 승인 절차 부분

아래 (그림 5-14)는 사용자가 웹 사이트로부터 물품을 구매하고자 할 때 주문 결제하는 화면을 보여주고 있으며, 1. TPM을 통한 결제방식과, 2. 무통장 입금을 통한 결제방식으로 구분되어진다. 본 논문에서는 1. TPM을 통한 결제방식을 제안하고자 한다. 즉, 사용자는 구매하고자 하는 웹 사이트에게 어떠한 지불정보를 제공할 필요가 없으며, 단지 TPM 지불결제 버튼을 클릭했을 때 TPM 시스템을 통한 사용자 결제를 확인 받을 수 있다.

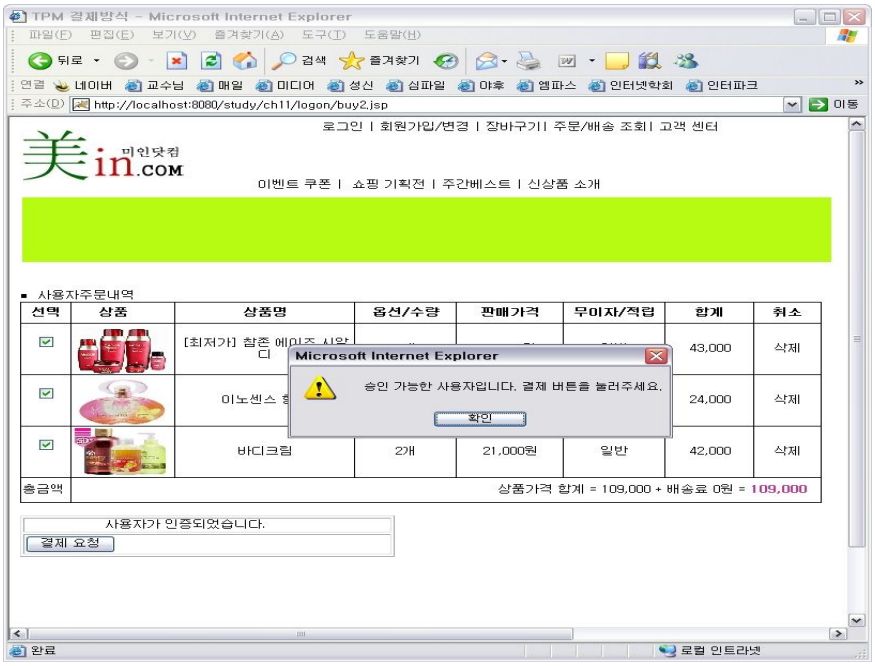


(그림 5-14) 주문결제화면

만약 TPM시스템에 가입한 사용자가 P1 등급의 가입이 아닌 P2~P5에 가입한 사용자의 경우 결제가 불가능한 상태를 나타내며, 아래 (그림 5-15)와 같이 추가 사용자 입력을 요구하는 메시지를 전달받게 된다. 하지만 P1에 등록된 사용자의 경우는 TPM 시스템으로부터 사용자에 대한 지불승인이 가능한 메시지를 받음으로써, 신용결제가 바로 이뤄질 수 있는데 이는 (그림 5-16)과 같다고 할 수 있다.



(그림 5-15) 결제 불가능한 사용자 화면



(그림 5-16) 결제 가능한 사용자화면

제 6장 결론 및 향후 연구

초고속 인터넷망의 획기적인 확산과 디지털 정보기술의 접목으로 인해 범세계적으로 시간적·공간적 한계를 넘어선 경제활동이 급속히 증가하고 있다. 그에 따라 대량의 개인정보는 거래를 기반으로 다양한 이 기종 시스템을 통해 이용 및 유통이 활발하게 일어나고 있는 실정에서 이를 안전하게 보호할 수 있는 기술적/표준적/제도적인 체계가 미흡한 실정이라 하겠다. 또한, e-business 환경 내 정보기술이 혁신적으로 발전함에 따라 기업들 사이에서 고객정보 보유량만이 기업의 핵심 경쟁력임을 인지하게 되었다. 이에 따라 본 논문에서는 고객의 개인정보를 무작위로 수집하는 CRM 프로세스 환경에서의 사생활 침해우려의 문제점을 살펴보고, 신뢰를 기반으로 한 모델 TPM(Trusted Privacy Policy Model)을 제안하였다.

본 모델은 강한 사용자통합인증 메커니즘과 유형별 개인정보의 중요도에 따른 등급을 설정하여 사용자 정보(속성)대비 레벨에 대한 권한을 부여함에 따라 접근통제의 흐름절차를 UML을 통해 분석·설계하고 프로토타이핑을 적용해 보았다. 이러한 모델을 실제 e-business 환경에 적용해 보았을 때, 사용자측면에서는 선택별/분별적 개인정보를 제공함으로써 기업/서비스업체로부터 불필요한 개인정보 활용 및 오남용 방지는 물론 사용자들로부터 개인정보의 중요성에 대한 인식 수준을 향상시킬 수 있다. 또한 서비스제공자측면에서는 사용자별 정보공개 수준에 따라 차별화된 서비스 및 마케팅을 제공할 수 있는 기대효과를 가지고 있다.

향후연구에는 유비쿼터스 환경 내에 개인정보를 보다 안정적이고 신뢰할 수 있도록 시스템 기반의 개인정보 정책 설정 및 관리, 안전한 개인정보 배포 방안에 대한 연구부분과 디지털 포렌식과 연계한 개인정보보호 방안에 대해 연구할 계획이다.

참고문헌

[1] Michael Friedewald, Elena Vildjiounaite, Yves Punie and David Wright "Privacy, identity and security in ambient intelligence : A scenario analysis", Telematics and Informatics, Volume 24, Issue 1, Pages 15-29, February, 2007.

[2] Zia Hayat, Jeff Reeve and Chris Boutle, "Ubiquitous Security for Ubiquitous Computing", Information Security Technical Report, In Press, Accepted Manuscript, Available online, 2, June, 2007.

[3] 개인정보보호백서 2003, 한국정보보호진흥원, 2003.

[4] "개인정보의 안전한 수집, 저장 및 관리, 이용, 제공, 파기를 위한 개인정보 관리 모델 연구", 한국정보보호진흥원, 2006.

[5] 정영태 기자, '리니지 명의도용 '중국해커들 소행 추정', SBS, 2006. http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1000076718

[6] '구글에 90만 명 주민번호 '무방비' 노출', SBS, 2006. http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1000149536&category=N1&section=03

[7] '건강보험 1만 4천 명 개인정보 유출', SBS, 2006. http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1000179556

[8] '결혼정보회사 홈페이지 해킹, 54만명 정보 빼내 ', SBS, 2006. http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1000157017

[9] "개인 및 민간기업 정보 트렌드 분석", 한국정보보호진흥원, 2007.

[10] 한국정보보호진흥원, 2006년 개인정보 피해구제 및 상담 사례분석, 2006.

[11] 2007년 국가정보보호백서, NIS 국가정보원, MIC 정보통신부, 2007.

[12] 한국정보보호진흥원, OECD의 국가간 프라이버시법 시행에 대한 논의 및 제안,

2006.

[13] 서계원, “정보 프라이버시와 개인정보보호의 보호”, 2006.

[14] Jean-Philippe Cotis, “Economic Policy Reforms : Going for Growth 2006”, OECD Publishing, 7, February, 2006.

[15] 권두언, "정보시스템과 네트워크의 보호를 위한 OECD 가이드라인 - 정보보호 문화를 향하여" 경제협력개발기구, 2007.

[16] 박훤일, “EU의 개인정보보호 요구에 대한 분석과 대응방안”, 한국정보보진흥원, 2002.

[17] 성윤모, “정보화와 프라이버시 보호”, korea Cadastral Survey Corp, 2004.

[18] 한명묵, 이철수, “정보보호 개론”, 2005.

[19] 강달천, “정보사회의 개인정보보호”, 한국정보보호진흥원, 2007.

[20] “개인정보보호 전문교육-개인정보보호 법률 및 피해사례” 한국정보보호진흥원, 2007.

[21] Ram Krishnan, Ravi Sandhu and Kumar Ranganathan, "PEI models towards scalable, usable and high-assurance information sharing", Sophia Antipolis, France, SACMAT'07, Pages 145-150, June 20-22, 2007.

[22] Xinwen Zhang, Songqing Chen, Michael J. Covington and Ravi Sandhu "Towards Application-Transparent Trusted Computing with Mandatory Access Control", ASIACCS'07, Pages 117-126, March 20-22, 2007.

[23] Matt Henricksen, William Caelli, and Peter Croll, "Securing Grid Data Using Mandatory Access Control", Conferences in Research and Practice in Information Technology (CRPIT),Vol. 68, 2007.

[24] Yong Lee, Jeail Lee and JooSeok Song, "Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce Communications",Volume, 30, Issue 4, Pages 893-903, February, 2007.

[25] 홍승필, 김영철, “정보보호의 이해”, 2004.

[26] Derek Ebeling and Rob Santos, "Public Key Infrastructure visualization", JCSC 23, Pages 247-254, 1 October, 2007.

[27] 박배효, “속성인증을 이용한 응용 서비스 모델 연구”, 한국정보보호진흥원, 2005.

[28] S. Farell and R. Housley, "An Internet Attribute Certificate Profile for Authorization,", PKIX WorkingGroup, June 2001.

[29] G. Karjoth, M. Schunter, E. Van Herreweghen, and M. Waidner, "Amending P3P for Clearer Privacy Promises", 14th International Workshop on Databased and Expert Systems Applications(DEXA'03), 2003.

[30] Lorrie Faith Cranor, "P3P : Marking Privacy Policies More Useful", IEEE Security and Privacy, 2003.

[31] W3C, "The Platform for Privacy Preferences 1.1(P3P1.1)" Specification", 2006.

[32] A list of privacy surveys, Available at http://www.w3.org/P3P/p3pfaq.html.

[33] 개인정보보호정책 설정 및 협상 기술 분석, 한국정보보호진흥원, 2006.

[34] Judith Winter and Oswald Drobnik, "An Architecture for XML Information Retrieval in a Peer-to-Peer Environment", Lisbon, Portugal, PIKM'07, Pages 17-24, November 9, 2007.

[35] Jae-Gil Lee, Kyu-Young Whang, Wook-Shin Han and Il-Yeol Song, "integrating access control with query processing in XML databases", The VLDB Journal, Volume 16 Issue 3, July, 2007.

[36] 김갑중 외 2명, “e-Business for Managers", 2002.

[37] 김성식, 유인선, "e-비즈니스 : 기술과 전략", 2007.

[38] Seng-Phil Hong, Sungmin Kang and Jaehyun Kim, "Privacy Protection Model in Customer Relationship Management Systems", Volume 9 Number 6, November 2006.

[39] 한국정보보호진흥원, "개인정보보호 기술 및 표준화 동향", 2006.

[40] 김종승, 조진호, "CRM 최신 트렌드 및 도입 전략", 2001.

[41] 이동훈, "e-비즈니스 원론", 2004.

[42] 홍승필, "유비쿼터스 컴퓨팅 보안", 2006.

[43] 한국정보보호진흥원, "정보보호 실태조사", 2006.

[44] 한국전산원, "개인정보보호법제의 현황과 그 발전전망", 2005.

[45] 정보통신부, 한국정보보호진흥원, "개인정보보호지침 해설서", 2005.

[46] 한국전산원, "우리나라의 개인정보보호체계와 제도적 이슈", 2004.

[47] 한국정보사회진흥원, "개인정보보호를 위한 기술개발 및 기술정책에 관한연구", 2004.

[48] 권현영, "전자정부시대 개인정보보호법제의 쟁점", 정보화정책 제11권 제3호, 2004.

[49] 한국정보보호진흥원, "개인정보보호 기술, 제품 및 활용사례 분석", 2007.

ABSTRACT

Applied to method of the Privacy Information Access Control Mechanism in e-business environment

Jang, Hyun Mi

Major in Computer Science

Graduate School

Sungshin Women's University

The development of IT and spread of internet rapidly have an effect on each field of information progress and economic activity in our society. This trend which is merged with e-business environment and economic activity neglected time and space is increased by geometric progression. Accordingly, the companies which want to secure the competence for turning of new business paradigm are trying to maximize their effective management, and attempting systemic revolutions. However, from the view of information re-engineering, protecting privacy information is important because inadequate usage of privacy information can be the decisive factor reducing positive effects from e-business environment.

This research analyzes the risk or privacy issues in e-business environment, CRM(Customer Relationship Management), then I suggest to the reliable privacy model which I call to TPM(Trusted Privacy Policy Model) to solve

above mentioned privacy issues or problems. The TPM is consists of the four major mechanism which are CAM(Consolidated Authentication Mechanism), SPM(Security Privacy Policy Mechanism), ACM(Access Controller Mechanism) and OCM(Output Control Mechanism). These Mechanisms emphasize on how to build the trust privacy information system in CRM with secure manner, and I also focus on trust access control methods or well defined to privacy information management in distributed sharing information system environment.

Finally, this research applies the analysis, design and prototyping in part of TPM model such as CAM, and ACM for feasible my thesis approach.