e-Business 환경 내 개인정보 보호 메커니즘적용 방안☆

Applied Method of Privacy Information Protection Mechanism in e-business environments

홍 승 필* 장 현 미**
Seng-phil Hong Hyun-me Jang

요 약

e-business 환경 내 정보기술이 혁신적으로 발전하면서 기업들 사이에서는 고객정보 보유량이 기업의 핵심 경쟁력임을 인지하게 되었고, 이때 민감한 개인정보들까지도 무작위로 오남용·도용 되면서 개인정보에 대한 적절한 대안이 절실히 필요한 실정이다. 본 논문에서는 e-business 환경 내 노출되어질 수 있는 개인정보 위험을 분석하고, 이를 해결하기 위해 신뢰를 기반으로 한 개인정보정책 모델(TPM-Trusted Privacy Policy Model)을 제시하였고, 정보보호 관점에서 4가지 주요 메커니즘(CAM, SPM, RBAC Controller, OCM)을 제안하였다. 이는 e-business 환경에서 개인정보 정책 및 절차를 기반으로 사용자별 권한부여를 통한 접근제어 및 통제가 가능하도록 분석·설계하였다. 또한 TPM 모델의 활용성을 제안하고자 실제 e-business 환경의 CRM(Customer Relationship Management)에 적용하여 보았다.

Abstract

As the innovative IT are being developed and applied in the e-business environment, firms are recognizing the fact that amount of customer information is providing core competitive edge. However, sensitive privacy information are abused and misused, and it is affecting the firms to require appropriate measures to protect privacy information and implement security techniques to safeguard corporate resources. This research analyzes the threat of privacy information exposure in the e-business environment, suggests the TPM-Trusted Privacy Policy Model in order to resolve the related problems, and examines 4 key mechanisms (CAM, SPM, RBAC Controller, OCM) focused on privacy protection. The model is analyzed and designed to enable access management and control by assigning user access rights based on privacy information policy and procedures in the e-business environment. Further, this research suggests practical use areas by applying TPM to CRM in e-business environment.

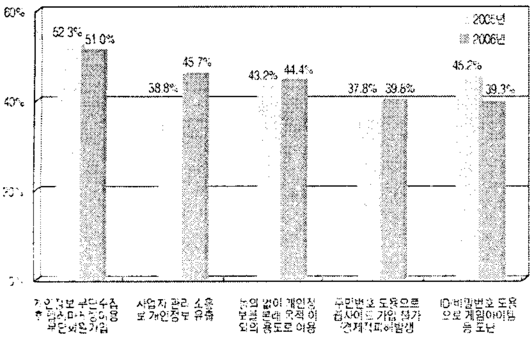
☞ keyword : Privacy, Security, Policy, Access Control, Security Architecture

1. 서 론

개인정보란 "생존하는 개인에 관한 정보로서 성명·생년월일·주민등록번호 등에 의하여 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)"를 말한다[1][3][4]. 이러한 개인정보는 급변하는 경제 환경 및 신기술의 등장으로 가공 및 활용이 용의해졌다는 것이다. 그에 따라 정부나 민간단체로부터 정보주체의 어떠한 동의 없이 무한대로 수집·축적·처리·가공을 이용한 개인정보 통합 관리시스템의 구축이 가능해지면서 개인정보 도용 및 유출에 따른 피해가 끊임없이 발생하고 있다[2][3].

아래 그림 1은 2005~06년 동안 개인 인터넷 사용자를 대상으로 실시한 설문 조사 결과이다.

* 종신회원 : 성신여자대학교 미디어학부 전임교수
philhong@sungshin.ac.kr(제1저자)
** 준 회 원 : 성신여자대학교 전산학과 박사 과정 중
nicemiya@sungshin.ac.kr(교신저자)
[2007/06/04 투고 - 2007/06/05 심사 - 2007/08/02 심사완료]
☆ 이 논문은 2007년도 성신여자대학교 학술연구조성비 지원에 의하여 연구되었습니다.



(그림 1) 유형별 개인정보/프라이버시 침해 경험률

아래 표 1는 개인정보 피해구제 · 상담 현황을 제시해주는 표로서, 2006년 한 해 동안 총 23,333 건이 접수되었으며, 이는 2005년에 접수된 18,206 건에 비해 약 28% 증가한 수치이다[4][5].

(표 1) 2006년 유형별 피해구제현황 · 상담 신청현황

침해유형	2005년		2006년		증감율
	건수	비율	건수	비율	
이용자 동의없는 개인정보 수집	1,140	6.2	2,565	10.9	▲125
개인정보 수집시 고지 또는 명시의무 불이행	15	0.1	27	0.1	▲80
과도한 개인정보 수집	33	0.2	61	0.3	▲85
고지 · 명시한 범위를 초과한 목적외 이용 또는 제3자 제공	916	5.0	917	3.9	▲0.1
개인정보 취급자에 의한 훼손 · 침해 또는 누설	186	1.0	206	0.9	▲11
개인정보 처리 위탁 시 고지의무 불이행	4	0.1	5	0.1	▲25
영업의 양수 등의 통지의무 불이행	7	0.1	11	0.1	▲57
개인정보관리책임자 미지정	25	0.1	23	0.1	▼8
개인정보보호 기술적 · 관리적 조치 미비	390	2.1	632	2.7	▲62
수집 또는 제공받은 목적 달성 후 개인정보 미파기	152	0.8	266	1.1	▲75
동의철회 · 열람 또는 정정 요구 등 불응	771	4.2	923	4.0	▲20
동의철회, 열람 · 정정을 수집방법보다 쉽게 해야 할 조치 미이행	285	1.6	484	2.1	▲69
법정대리인의 동의없는 아동의 개인정보 수집	71	0.4	23	0.1	▼67
타인 정보의 훼손 · 침해 · 도용	9,810	53.9	10,835	46.4	▲10
정보통신망법 적용대상 이외의 개인정보침해	4,401	24.2	6,355	27.2	▲44
합 계	18,206	100	23,333	100	▲28

본 논문에서는 다양하고 나날이 치밀해지고 있는 위험으로부터 개인정보를 신뢰적으로 관리하고 통제할 수 있는 방안에 대해 제시하였다.

본 논문의 구성은 다음과 같다. 1장에서는 논문의 개요 및 프라이버시 침해 유형에 대해 간략히 소개하고, 2장에서는 사례연구를 통해 e-business 환경 내에서 발생할 수 있는 개인정보 침해에 대한 문제점과 대응방안을 연구하였다. 3장에서는 개인정보보호 관련 기술 및 표준화에 대하여 설명하였으며, 4장에서는 신뢰할 수 있는 개인정보보호정책모델 TPM(Trusted Privacy Policy Model)과 4가지 주요 관련 메커니즘에 대하여 제안하였다. 5장에서는 TPM모델의 프로토타이핑을 통한 구현 방안을 제시하였다. 6장에서는 기대효과와, 마지막으로, 7장에서는 결론 및 향후 연구 방향을 기술하였다.

2. 사례연구 - CRM

CRM(Customer Relationship Management)이란 기업 전반에 걸쳐 고객의 정보와 기업 내 · 외부의 고객관련 데이터를 DB에 통합 및 분석하여, 고객의 요구사항(needs)을 적절히 파악하고, 원하는 제품과 서비스를 지속적으로 제공함으로써 고객과 상호작용 하는데 활용하도록 하는 비즈니스 프로세스를 말한다[6].

글로벌 시대의 도래, 고객 욕구의 다양화, 디지털 환경 기술의 발달 등의 여러 변화로 인해 고객지향 적인 "일대일 마케팅"이라는 새로운 전략적 패러다임을 맞이하고 있다. 이런 환경에서 기업들은 타 기업과의 차별된 서비스를 제공하기 위하여 필요이상의 개인정보 수집 및 활용, 더 나아가 개인정보의 오남용 · 도용의 문제가 점점 대두되고 있는 실정이다.

예를 들면 기업들은 업무 효율은 물론 경영효과를 극대화시키기 위해 아웃소싱 마케팅을 활용하여 고객의 정보처리업무를 처리하도록 행하고 있다. 하지만 이러한 개인정보는 기술적/법적인 제한 없이 제공됨에 따라 사용자의 정보가 필요이상으로 사용되어지고 있다. 뿐만 아니라 홈쇼핑이나 콜센터로부터 제공되었던 민감한 개인정보들도 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 있다.

위의 사례를 기반으로, 개인정보에 대한 침해

유형은 크게 다음 6가지로 구분해 볼 수 있다. 1) 접근과 수집, 2) 모니터링, 3) 분석, 4) 이전, 5) 원하지 않은 영업행위, 6) 저장 등이 있으며, 이는 지식정보사회의 발달과 더불어 점점 증가하는 웹 시스템 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[3][5][7].

이러한 위험으로부터 개인정보 보호 측면에서 고려하여야 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 되어 지면서, 한번 입력 된 개인정보가 필요한 곳에 효과적으로 사용되어지는 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.

3. 관련 연구

3.1 정보보호 및 개인정보 관련 기술

PKI (X.509 V. 3.0)

PKI(공개키 기반구조-Public Key Infrastructure)란 사이버 증권거래와 같이 고객과 은행 또는 증권사가 인터넷이라는 가상공간을 통해 개인정보와 금융 거래정보에 대해 인증서를 활용하여 상대방의 신원확인과 송수신되는 금융거래 내용의 무결성을 전자적으로 보장해 주는 표준화된 보안 인프라 구조이다[9].

RBAC (Role Based Access Control)

RBAC(역할기반접근통제 - Role Based Access Control)은 사용자가 기업이나 조직의 정보 자원을 임의로 접근할 수 없도록 제한하는 모델이다. 이는 접근 권한이 역할(role)에 부여되고 사용자는 적절한 역할에 소속됨으로서 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 이러한 아이디어는 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다. 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되며 접근 구조의 변경이 없이도 역할의 변경을 쉽게 할 수 있다[10].

XML(Extensible Markup Language)

XML은 W3C(World Wide Web Consortium)에서 제안된 국제전자문서를 위한 확장성 마크업 언어의 표준으로 본래 1986년에 문서작성을 위한 국제 표준으로 제안된 SGML(Standard Generalized Markup Language)에 그 기반을 두고 있다. SGML

은 문법의 복잡함 때문에 문서 제작을 위해서 막대한 시간과 비용을 감수해야 한다. XML은 SGML에서 잘 쓰이지 않는 복잡한 문법을 제외시키고 웹상에서의 이용을 위하여 단순화시킨 형태이며, HTML보다는 보다 정교한 문서의 형식과 내용의 표현이 가능하다[13].

P3P(Platform for Privacy Preferences)

P3P(Platform for Privacy Preferences)는 지난 2002년 국제 웹 표준화 기구인 W3C(World Wide Web Consortium)가 웹사이트 이용 시 프라이버시를 보호하기 위해 정한 표준 기술 플랫폼으로, 개인 사용자는 자신의 개인정보 보호 내역을 주어진 프로그램이나 에디터 등을 통해 명시하고 브라우저에서, 이 보호정책과 맞지 않는 외부 사이트를 차단하여 개인정보유출을 사전에 방지하는 기술이다[12].

APPEL(A P3P Preference Exchange Language)

W3C(World Wide Web Consortium)는 웹 사이트 이용 시 사용자 개인정보보호 내역을 APPEL(A P3P Preference Exchange Language)언어를 통해 명시할 수 있도록 제공하고 있다. 현재 APPEL은 W3C에서 XML언어를 기반으로 개인정보보호 정책을 web 기반에 적용이 용이하도록 문법과 규칙에 맞게 인코딩하는 가이드라인을 제시하고 있다[8].

3.2 개인정보 관련 표준화 연구

국내- 관련 법규

정보통신망을 이용한 대량의 개인정보의 수집, 취급 등이 용이해지면서 정보통신 서비스 이용자의 자기정보통제권이 보장될 수 있도록 개인정보보호 법안의 제정이 추진되고 있다. 다음 아래 표 2은 국내 개인정보보호 법령을 설명한다[5].

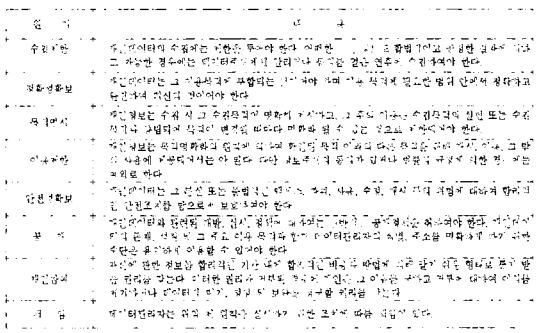
(표 2) 국내의 개인정보보호 관련법령

개인정보보호 국내법	주요 내용
통신비밀보호법	통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.
공공기관의 개인정보보호에 관한법률	컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다.
금융실명거래 및 비밀보장에 관한법률	실지명의에 의한 금융거래를 실시하고 그 비밀을 보장하여 금융거래의 정상화를 기함으로써 경제정의를 실현하고 국민경제의 건전한 발전을 도모함을 목적으로 한다.
정보통신망 이용촉진 등에 관한법률	정보통신망의 이용 활성화, 개인정보의 보호, 정보통신망에서의 청소년 보호, 정보통신망의 안정성 확보뿐만 아니라 광고성 정보 등 스팸에 관한 규제와 정보통신망에서의 명예훼손 등에 대한 법적 등을 규정한다.
정보통신망기반 보호법	2006.1 제정되었으며, 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다

국외- OECD

프라이버시에 대한 논의는 OECD에서 이미 1978년대부터 시작하여왔다. 그리고 이러한 논의의 결과 1980년 "프라이버시 보호와 개인 데이터의 국제유통에 관한 가이드라인에 관한 이사회 권고"라는 가이드라인을 채택하였고, 개인정보의 사생활권 보호, 정보의 자유로운 유통 장려, 국내 사생활보호입법에 의한 자유로운 정보유통에 대한 부당한 제한방지, 관련국내법규정과의 조화를 주목적으로 하고 있는 가이드라인의 8대원칙 아래 표 3과 같다[11].

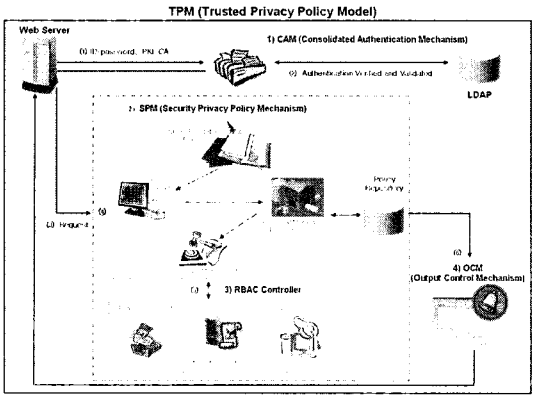
(표 3) OECD의 개인정보 보호원칙



4. TPM(Trusted Privacy Policy Model)

e-business 환경 내에서 신뢰할 수 있는 개인정보 모델(TPM-Trusted Privacy Policy Model)을 구

현하기 위해 본 논문에서는 4가지 주요메커니즘 (1. 통합사용자 인증 메커니즘-CAM, 2. 개인정보 정책 메커니즘-SPM 3. 역할기반접근통제메커니즘 -RBAC Controller 4. 안전한 개인정보 분배 메커니즘-OCM)을 제시하였으며, 그 기본 구조는 아래 그림 2와 같다.



(그림 2) TPM Architecture

사용자가 웹사이트로부터 원하는 서비스를 제공받고자 접근을 시도할 때, 가장먼저 ① ID/Password 또는 PKI를 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 RBAC Controller를 활용하여 사용자 정보와 서비스 제공자의 정책을 비교, 분석하여 적절한 역할대비 권한을 부여한 뒤, ⑥ XML기반의 OCM메커니즘을 활용하여 안전한 정보배분 및 Notice 기능을 제공 받는다.

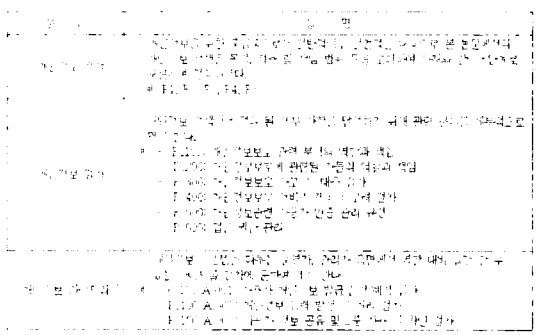
4.1 CAM(Consolidated Authentication Mechanism)

CAM은 TPM에 접속할 때 사용자 신분확인을 위해 기본 속성을 저장하고 검증할 수 있는 모델이다. 즉, X.509 V3.0 인증서를 통한 암호화 기반의 강한 신분확인(Strong Authentication) 후 개인정보 정책에 준한 사용자의 적합한 속성을 PKI의 확장 필드를 응용하여 적용 하는 메커니즘이다. 이러한 구조는 향후 프라이버시에 관련해서 익명성과 아호에 따른 문제를 해결하기 위해 SPM에서 미리 할당된 개인정보 정책을 보여주고, 그에 준한 사용자 속성 및 검증하는 기능을 수행할 수 있다.

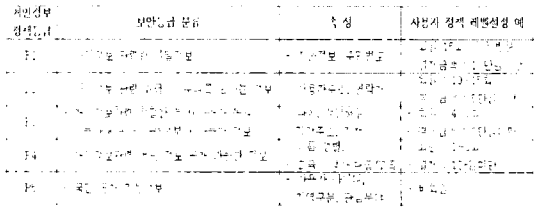
4.2 SPM(Security Privacy Policy Mechanism)

SPM은 e-business 환경 내 개인정보 관련하여 비즈니스의 중요도와 사용자 정보의 활용, 공개, 보안정도의 여부에 따라 적절한 개인정보 정책, 절차 가이드라인을 제공하는 메커니즘으로써 아래 표 4과 같이 보여 진다. 표 5는 실제 시스템 환경 내에서 사용자 속성이 주워졌을 때 정책의 등급을 설정 및 분류할 수 있도록 제시하였다.

(표 4) 개인정보 정책, 절차, 가이드라인 생성 표



(표 5) 정책을 기반으로 사용자 등급 설정표



(표 6) APPEL를 활용한 개인정보정책 설정

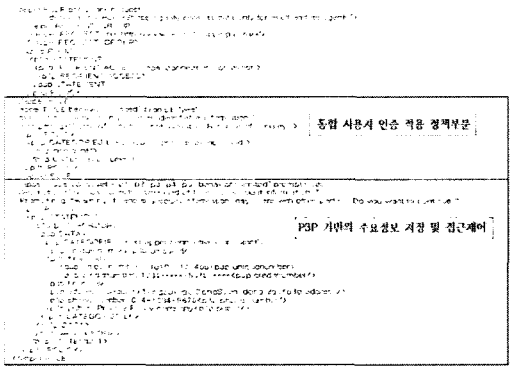


표6은 APPEL을 이용한 개인정보 정책 적용 방안의 예시를 보여 주고 있다.

4.3 RBAC Controller

RBAC은 사용자가 기업이나 조직의 정보자원을 임의로 접근할 수 없도록 접근 권한의 역할을 부여하여, 적절할 역할에 소속됨으로서 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 제공하는 메커니즘이다. 제시된 개인 정보의 중요도 및 등급별 또는 역할 기반의 접근 통제가 시스템 관리자로부터 가능하도록 설계되어졌다. 아래 표 7은 관리자 측면에서 개인정보의 역할기반에 따른 권한부여에 대한 가이드라인을 보여주고 있다.

(표 7) 개인정보 역할기반 권한부여 가이드라인

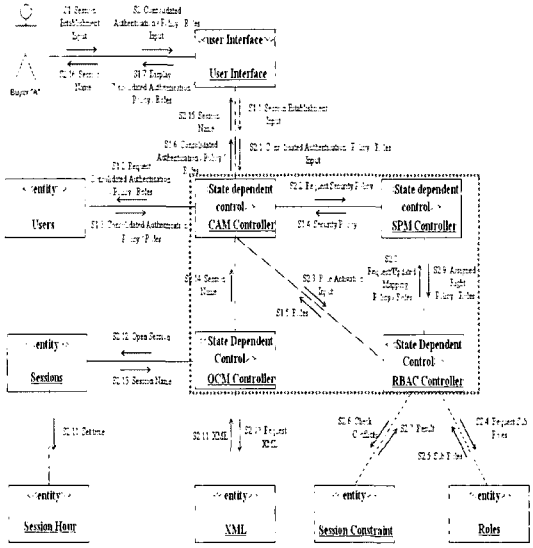
역할 정립 (Role Assignment)	조직 내 업무에 대하여, 수행가능한 권한과 책임을 기반으로 조성 된 구성원들에 대한 관련 업무를 정립 한다 예) 사용자, 관리자, 개발자, 운영자 등
역할 부여 Role Fermission)	- 조직 내 업무에 대하여, 관리자 또는 감독자가 필요한 자격을 갖춘 사람에게 그에 적합한 역할권한을 허가한다.
역할 제한 (Role Constraint)	- 조직 내 업무에 대하여, 관리자 또는 감독자가 필요한 자격을 갖춘 사람에게 필요 이상의 역할에 대한 접근을 제한한다.
역할기반 접근제어	관리자, 운영자 측면에서 사용자 개인정보에 대하여 누가, 언제, 어디에서, 어떤 행동에 대하여 개인정보 이용 관련 사용자 배정, 역할 할당, 권한 배정, 세션 (Session)등에 따른 제한 및 접근 가능한 지에 대한 규정을 제시 한다 예) 제약(Constraint)적 기능 - R_100_C_001 : 사용자 주민번호 저장기능 제한 - R_100_C_002 : 사용자 신용정보 제공기능 제한 - R_100_C_003 : 사용자 기밀정보 제공기능 제한 - R_100_C_004 : 개인정보보호 오류시 세션 종적 기능 - R_100_C_005 : 개인정보 저장시 역할별 차관 서비스 제공 - R_100_C_006 : 개인정보 중요도에 따른 저장 서비스 제한 기능 예) 허락(Fermission) 기능 - R_100_P_001 : 개인정보보호 요청시 사용자 정보 제공 허가 기능 - R_100_P_002 : 개인정보보호 사용자 사전통보 기능 - R_100_P_003 : 개인정보보호 사용자 사후통지 기능

4.4 OCM (Output Control Mechanism)

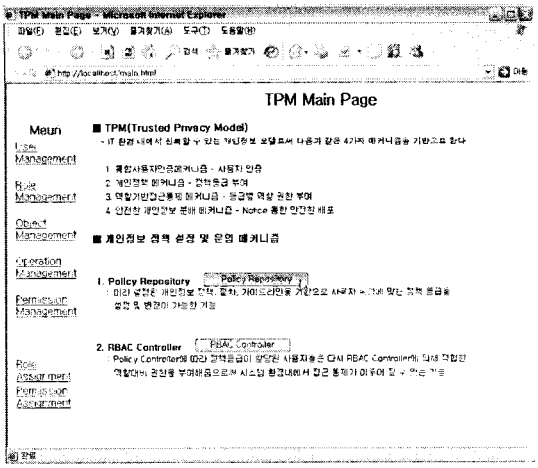
OCM은 SPM으로부터의 할당 받은 개인정보 정책 기반의 접근제어를 수행하고 잘 정의된 XML(Extensible Markup Language) 문서들이나 XSL과 같은 기술들을 이용하여, 타 기관시스템과의 커뮤니케이션을 수행하는 메커니즘이다. 사용자 입장에서는 타 개인정보 시스템에서 자기 정보의 공개 정도를 이해하고, 필요시 직·간접적인 통제 방안을 원활히 수행 할 수 있도록 P3P를 적용하였다. 특히 개인정보의 오남용문제에 관련해서, 개인정보 사용 시 그 사용 범위와 목적 등을 고려한 개인정보 알림("Notice")기능을 수행한다.

5. TPM 구현방안

아래 그림 3은 e-business 환경 내에 개인정보 보호 및 접근통제가 적용 되어질 수 있는 4가지 주요 메커니즘(CAM, SPM, OCM, RBAC Controller)인 TPM모델이 UML을 통해 활용되어졌을 때 보여질 수 있는 분석 설계도이다.

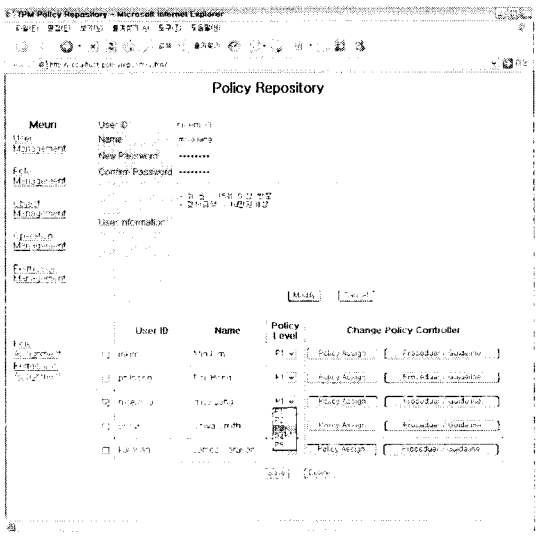


(그림 3) 개인정보정책 분석설계도



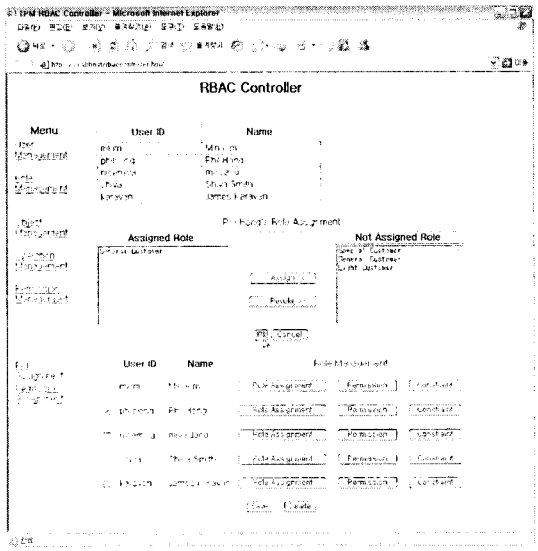
(그림 4) TPM Main 화면

위 그림 4는 TPM 모델을 활용하기 위한 초기 Main 화면으로, 개인정보 정책 설정 및 운영을 위한 주요 기능은 크게 정책저장 설정기능과 접근통제 설정기능으로 구분할 수 있다. 아래 그림 5는 비즈니스 관리자 측면에서의 정책 저장 및 변경관리(Policy Repository)부분을 보여주고 있다. 즉, 사용자별 보안 등급을 할당할 수 있도록 속성정보를 통하여 개인정보 정책을 할당하고, 관리되어질 수 있도록 제시하는 화면이다.



(그림 5) Policy Repository

아래 그림 6은 그림 5에서 부여된 개인정보 정책등급을 기반으로 접근제어 통제 기능을 제공할 수 있도록 RBAC Controller에서 사용자의 역할에 맞는 권한을 부여하고, 통제되어 질 수 있도록 보여주는 화면이다.



(그림 6) RBAC Controller

6. 기대효과

e-business 환경 내에 TPM모델을 적용했을 때 3가지 기대효과는 다음과 같다.

1) 시스템 측면

- 개인정보 정책설정 및 개인정보 교환 시 유연하고 독립적인 표준기반 형식의 XML을 활용함으로써, 다양한 어플리케이션 환경에서의 뛰어난 상호운용성을 확보할 수 있다.
- 관리자·운영자 측면에서 개인정보통합 시tm템을 통하여, 일괄적으로 개인정보가 관리되어짐에 따라 개인정보의 신뢰성을 높일 수 있다.

2) 사용자 측면

- 사용자측면에서 선택적/분별적 개인정보를 제공함으로써 기업으로부터 불필요한 개인정보 활용 및 오남용을 방어할 수 있다.
- 타 기관으로부터 개인정보 사용에 대한 Notice 기능을 제공해줌으로써, 타인 또는 허가 받지 않은 기관으로부터의 악용을 방지하고, 사용자들로부터 개인정보의 중요성에 대한 인식 수준을 향상 시킬 수 있다.

3) e-business 측면

- 관리자측면에서 각 사용자별 속성대비 정책 및 권한을 부여함으로써 등급별 고객 관리를 통한 차별화된 서비스 및 효과적인 마케팅을 제공할 수 있다.
- 신뢰할 수 있는 기관은 민감한 개인정보 수집을 필요로 하는 업체를 분별하고, 선택적 개인정보를 제공함으로써 서비스업체 내부로부터 발생되어질 수 있는 개인정보의 불법적 오·남용/도용으로부터 방어할 수 있다.

7. 결론 및 향후 연구과제

정보통신기술의 급격한 발전으로 e-business 환경에서는 다양한 시스템과의 통합으로 인해 대량의 정보가 처리되어지고 있다. 그에 따라 개인정보의 불법이용과 유통이 날로 증가하는 추세에서 개인정보보호에 대한 대책이 시급한 실정이다. 본 논문에서는 e-business 환경 내에서 신뢰할 수 있는 개인정보정책모델 TPM(Trusted Privacy Policy Model)를 제안하였다. 이 모델은 강한 사용자통합인증과 정책을 기반으로 역할기반통제시스템을 통해 사용자별 등급할당 및 접근통제가 원활히 이루어질 수 있는 개인정보정책 엔진을 개발하였고, UML설계, 프로토타이핑을 통한 구현 방안도 제시하였다. 향후에는 본 TPM 모델을 응용하여 유비쿼터스 환경 내에서 개인정보를 보다 안정적이고 신뢰할 수 있도록 시스템 기반의 개인정보 정책 설정 및 관리, 안전한 개인정보 배포 방안에 대한 연구를 주력할 예정이다.

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

[5] 2007년 국가정보보호백서, NIS 국가정보원, MIC 정보통신부, 2007.

[6] Kevin B. Hendricks, Vinod R. Singhal and Jeff K. Stratman, "The impact of enterprise systems on corporate performance: A study of ERP, SCM, and CRM system implementations", Journal of Operations Management, Volume 25, Issue 1, Pages 65-82, January, 2007.

[7] 조화순, "IT혁명과 개인정보보호", 한국전산원, 5월, 2004.

[8] Lorrie Cranor, Marc Langheinrich, A P3P Preference Exchange Language 1.0(APPEL 1.0), W3C Working Draft, 15, April, 2002.

[9] 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, Feb., 2007.

[10] Tsung-Yi Chen, Yuh-Min Chen, Hui-Chuan Chu and Chin-Bin Wang, "Development of an access control model, system architecture and approaches for resource sharing in virtual enterprise Computers in Industry", Volume 58, Issue 1, Pages 57-73, January, 2007.

[11] Jean-Philippe Cotis, "Economic PolicyReforms : Going for Growth 2006", OECD Publishing, 7, February, 2006.

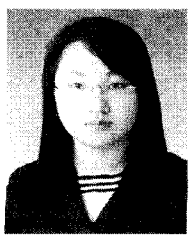
[12] A list of privacy surveys, Available at http:// www. w3.org/P3P/p3pfaq.html.

[13] Huaxin Zhang, Ning Zhang, Kenneth Salem and Donghui Zhuo, "Compact access control labeling for efficient secure XML query evaluation", Data & Knowledge Engineering, Volume 60, Issue 2, Pages 326-344, February, 2007.

◐ 저 자 소 개 ◑

홍 승 필(Seng-Phil Hong)

1993년 Indiana State University (학사)
1994년 Ball State University (석사)
1997년 Illinois Institute of Technology(박사수료)
2002년 한국정보통신대학교 (박사)
1997년 ~ 2004년 LG CNS Systems, Inc.
2005년~현재 성신여자대학교 미디어학부 전임교수
관심분야 : 접근제어, 통합인증, 정보보호 아키텍처, 유비쿼터스 보안, 프라이버시 보호
E-mail : philhong@sungshin.ac.kr



장 현 미(Hyun-me Jang)

2006년 서울산업대학교 산업정보 시스템학과 졸업(학사)
2008년 성신여자대학교 대학원 전산학과 (석사)
2008년 현재 성신여자대학교 전산학과 박사 과정 중
관심분야 : 프라이버시 보호, 유비쿼터스 보안, 접근제어
E-mail : nicemiya@sungshin.ac.kr