情 報 保 護 學 會 誌
第 14 卷 第 6 號, 2004. 12

ID관리시스템에서의 프라이버시 보호†

최 향 창*, 이 용 훈*, 노 봉 남*, 이 형 효**, 조 상 래***, 진 승 헌***

요 약

웹 기반환경에서는 수많은 개인정보 자원이 산재되어 있으며, 이들 개인정보는 마땅히 보호되어야 함에도 불구하고 서비스 혹은 개인의 편의성을 강조한다는 명목으로 여러 시스템들로부터 개인의 동의 없이 무분별하게 수집, 이용되고 있다. 개인 정보에 대한 이상적인 프라이버시 보호는 정보의 생성 단계부터 폐기 단계까지 전 과정 동안 개인정보가 보호되어야 하며, 활용단계에서 정보의 주체인 개인에게 정보의 사용에 대한 통보와 개인이 허가하는 범위 내에서만 사용하도록 하는 것은 프라이버시 보호측면에서 매우 중요하다.

본 논문에서는 개인정보를 저장하고 관리하는 ID 관리시스템에서의 프라이버시 보호 기술에 대해 기술한다. 특히 ID 관리시스템에서의 정보의 생성부터 폐기까지의 개인정보 보호 생명주기(Life-cycle)를 제안하고, ID 관리시스템에서 프라이버시 보호를 위한 요구사항과 보안구조를 제시한다.

Ⅰ. 서 론

정보화 물결 속에서 수많은 개인정보는 정보의 주체가 허가하지 않은 사용자나 그룹에게 유포되어 사용되고 있지만, 대부분 개인들은 자신의 개인정보가 유포되고 있는 사실조차 인식하지 못한다. 더욱이 개인정보를 가공하고 처리하는 기업이나 제 3자도 개인의 프라이버시를 꼭 지켜야 한다는 법률적인 지침보다는, 정보를 사용하는데 있어서 발생하는 이점 측면에 더욱더 관심을 갖는다. 따라서 개인정보를 사용하는 시스템들 대부분이 개인의 프라이버시를 고려하지 않고 시스템을 설계하고 운용한다.

일반적으로 프라이버시 침해의 한 유형으로는 데이터 마이닝 기술에 의한 프라이버시 침해이다. 데이터 마이닝 기술은 정보화의 가속화나 개인의 편리성을 제공하는 반면에 개인정보의 일괄적인 수집과 가공이라는 면 때문에 수많은 개인정보를 수집하여, 개인에게 민감한 정보를 노출 시킬 수 있는 위험성을 내포하고 있다. 또 다른 프라이버시 침해 유형은 개인이 인터넷을 통해 웹 서핑이나, 기타 정보 통신 기술로 수행될 수 있는 일련의 업무를 수행하는 과정에서 프라이버시 침해가 발생할 수 있다. 예를 들면, 특정 개인이 '어떤 사이트에 방문했으며, 어떤 날짜 및 시간에 어떤 물품을 얼마만큼 구매했는가?' 등의 정보가 이용하는 정보 시스템에 기록되고 결과적으로 개인의 취향과 개인이 감추고 싶은 기록들까지 노출될 수 있다.

본 논문의 2장에서는 프라이버시 및 ID 관리시스템에 대해 살펴보고 3장에서는 프라이버시관련 연구 동향을 고찰하기 위해 프라이버시 보호 관련 프로젝트인 RAPID[1], PRIME[2], P3P[4], IBM의 E-P3P[5] 및 EPAL[3]을 살펴본다. 4장에서는 OECD가이드라인[6]을 기반으로 한 개인정보 생명주기를 제안하고 5장은 제안된 개인정보 생명주기를 반영하는 ID 관리시스템에 대해 기술한다. 끝으로 결론 및 향후 연구방향을 제시한다.

Ⅱ. 프라이버시 및 ID 관리시스템

1. 프라이버시

1.1 프라이버시 정의

프라이버시의 사전적 정의는 "통제되어야 하는 개인이나 조직의 권리, 개인이나 조직이 소유하는 자료, 개인이

† 본 연구는 한국전자통신연구원 연구과제(0801-2004-0031) 지원으로 수행하였습니다.
* 전남대학교 정보보호협동과정 ({hcchoi, yhyi, bongnam} @athena.jnu.ac.kr)
** 원광대학교 정보·전자상거래학부 (hlee@wonkwang.ac.kr)
*** 한국전자통신연구원(ETRI) 정보보호연구본부 인증기반연구팀 ({jinsh, sangrae} @etri.re.kr)

나 조직에 관한 정보는 허가 없이 수집되어 사용되어서는 안 되며, 조직에 속하는 개인 신상 정보는 인사나 고용, 작업, 서비스 등과 관련이 없는 다른 개인이나 조직 사이에서 부당하게 수집·배포하거나 사용될 수 없다."로 정의된다[16]. 즉, 개인과 관련된 일련의 정보데이터가 정보의 주체의 의지대로 보호되는 의미이다. 정보사회의 프라이버시는 "개인, 집단, 단체 스스로 자신이 소유한 정보를 다른 사람에게 언제, 어떻게, 얼마나 공개할 것인가를 결정하고 그렇게 하도록 요구하는 것"이라고 Alan Westin은 정의했다. 또한 Samuel Waren과 Louis Brandesis는 "개인의 프라이버시는 상대방에게 절대적으로 침해 받아서는 안 된다"고 정의하고 있다[17].

1.2 OECD 프라이버시 보호지침

1980년에 경제개발 협력기구(OECD)는 '사생활 정보 보호와 개인정보의 국제적 유통에 관한 개인정보보호의 8원칙'을 규정했다[13]. 모든 개인정보는 적법하고 정당한 절차에 의해서만 수집되고 데이터 소유자에게 정보의 수집을 통지하여 접근과 사용에 대한 동의를 얻도록 하는 정보수집(Collection Information)제한의 원칙, 개인정보를 사용할 때 사용목적에 일치될 때 사용되고 필요한 범위에서 정확하고 완전한 최신의 정보가 유지 되도록 하는 데이터 정확성(Data Quality)의 원칙, 개인정보의 수집 목적은 반드시 특정하고 명확하게 기술 하도록 하는 목적명확화(Purpose Specification)의 원칙, 개인 정보가 정보주체의 동의나 법률에 의해 정해진 것 외에는 다른 목적으로 사용되지 않도록 하는 이용제한(Use Limitation)의 원칙, 개인정보의 분실이나 불법적인 접근, 파괴와 불법사용, 변조, 공개 등의 위험으로부터 적절하게 보호되도록 하는 안전보호(Security Safeguards)의 원칙, 개인 정보처리를 위한 정보시스템의 활용정책을 일반인에게 공개(Openness)하도록 하는 원칙, 정보의 소유자가 개인정보를 확인할 권리를 가지며 정보의 접근을 통지 받을 수 있고 필요에 따라서 정보를 파기, 정정, 수정을 요구가 가능하도록 하는 개인 참가(Individual Participation)의 원칙, 정보 관리자가 원칙을 이행할 책임(Accountability)을 갖도록 하는 원칙들을 제공한다[23].

1.3 미국, EU의 프라이버시 관련지침

미국과 유럽의 경우, 온라인 고객정보 보호 정책과 관련한 규정들은 고객정보 FIPP(Fair Information Practice Principles)와 OPA(Online Privacy Alliance)의 내용에 부합해야 한다. FIPP에는 고객정보 수집방법, 수집된 정보에 대한 고지 의무, 고객정보의 올바른 사용을 보장하는 기업의 보안 의무 등이 명시되어 있으며, OPA는 기업의 고객정보보호 정책을 개발하고 이 정책을 공개하기 위한 필요조건에 대한 지침을 제공한다. 정보 소유자는 자신과 관련된 정보가 요청되고 수집되는 것을 통보(Notice) 받아야 하며 또한 그것을 인지(Awareness)해야 한다. 정보는 정보사용자로부터 선택(Choice)될 수 있고 수집될 때 그 정보는 정보 소유자로부터 사용해도 좋다는 동의(Consent)를 받아야 한다. 또한 정보소유자는 자신의 정보에 접근(Access)권한을 가져야 하며 필요에 따라서 정보를 정정할 수 있어야 한다. 개인 정보는 불법적이고 악의 적인 행위로부터 변조돼서는 안 되고 개인 정보에 대한 공개에 대해 불법적인 사용자로부터 보호되어야 한다. 개인의 프라이버시를 보호하기 위한 정책은 수행되어 개인의 정보를 보호하고 프라이버시 침해가 발생되면 적절하게 보상받아야 한다.

EU는 개인정보를 보호하기 위해서 표 1과 같은 개인정보 보호 원칙[9,13]을 제정하였고, 또한 기본적으로 개인정보 보호가 미흡한 제 3국에 대한 개인정보 이전을 금하고 있다.

〔표 1〕 EU의 개인정보보호지침

원 칙	의 미
목적제한 (Purpose Limitation)	개인정보는 특정 목적에 의해서만 사용되고 목적에 일치될 때만 사용
정보의 품질과 균형성 (Data Quality and Proportionality)	정보는 정확하게 구축되고 필요에 따라서 갱신되어야 함. 정보사용 목적과 관련하여 적절하고 과도하지 않아야 함
투명성 (Transparency)	개인은 정보를 처리하는 제3의 기관에서 자신의 정보를 사용하는 목적과 정보를 보호하는 정책을 확인할 수 있어야 함
안전성 (Security)	정보를 관리하는 자는 정보를 보호하는데 있어서 안전한 기술적, 관리적 대응
접근·정정·거부 (Access, Rectification, Opposition)	정보의 주체는 자신의 모든 정보에 접근 가능해야 하고 필요에 따라서 자신의 정보를 정정하거나 정보의 요청을 거부할 수 있음
정보 이전의 제한 (Restriction on Onward Transfers)	개인의 정보를 수령한자가 다른 곳으로 정보를 전송하고자 할 때 적절한 수준의 개인정보 보호 규정을 따를 때에만 전송이 가능

2. ID 관리 시스템

2.1 ID 관리, Federated ID 관리

ID 관리란 사용자, 서비스, 정보통신기기 등 네트워크에 연결되는 개체의 신원의 속성, 신원증명서(credential), 정보이용 자격(entitlement) 등을 전체 생명주기 동안 통합 관리해주는 플랫폼 기반구조이다[22]. 이것은 또한 조직의 내부 통신망이나 외부 통신망으로부터 접속해오는 사용자 또는 단말기를 인증하고 해당하는 권한을 확인하여 정보자원에 대한 적절한 접근권한을 인가해주는 과정이다. 따라서 신원 관리(Identity Management) 시스템은 AAA(Authentication, Authorization, Audit/Account)기술, P3P기술, 패스워드 reset 기술, 패스워드 동기화 기술, 계정관리 셀프 서비스, 관리권한 위임, SSO(Single Sign On), 메타 디렉터리, LDAP (Lightweight Directory Access Protocol) 등 여러 기술을 종합하여 구현된 복잡한 시스템으로 구성되어 있다.

Federated Identity 관리는 신원 관리의 단위를 확대하여 사용자·통신기기가 네트워크에 한번 로그인하면 다른 조직의 네트워크에 접속할 때 별도의 로그인이 필요 없는 환경을 제공해준다[10]. 이러한 기술의 대표적인 것으로는 Liberty Alliance[7]와 MS사의 .NET Passport[19]가 있다.

2.2 Liberty Alliance Project

Liberty Alliance는 분산·협업형 네트워크 환경에 적합한 싱글사인온(SSO: Single Sign-On) 표준마련과 고객 신원 정보의 프라이버시 및 안전성 보장을 목적으로 "Federated Identity"의 표준화 단계를 단계별로 추진하고 있다[7,13]. 또한 ID-FF(Liberty Identity Federation Framework) 버전 1.2, ID-SIS(Liberty Identity Services Specification) 버전 1.0, ID-WSF (Liberty Identity Web Service Framework) 버전 1.0등을 개발하여 발표했으며 구현에 필요한 가이드라인, 신원 통합관리와, 상호인증 및 세션의 관리 등의 솔루션을 제공하는 Liberty 프로토콜 및 스키마의 표준 규격을 발표했다. 현재 Liberty 프로토콜의 요청 및 응답 메시지의 송수신에 SOAP을 적용하여 가능한 방법을 정의하고 통신 메시지 규격 및 전송메커니즘을 규정한 바인딩 및 프로파일의 표준규격을 발표하는 등의 연구가 진행되고 있다. Liberty의 주요목표는 분산네트워크 환경에서 고객의 정보에 대한 보안타협을 배제하고 중요정보를 잘 보존하여 정보의 프라이버시 및 안전성을 보장하는 SSO 표준의 제정이다.

Liberty Alliance 연구에서 ID연합 프레임워크 (ID-FF : Federation Framework)는 기업의 시스템들 간에 서로 연합이 가능하도록 한다. 또한 이것은 상호 이질적인 컴퓨터나 이동단말기 등의 환경에서 현재의 모든 장치들을 지원할 수 있도록 설계하고 연합체간에 연결을 맺기 위해서 기업 간 신뢰체제 구축에 대해 제안했다. 서비스 인터페이스명세 (ID-SIS : Services Interface Specification)는 각각의 이질적인 서비스가 서로 간에 이질적인 장치에서 제공되더라도 하나의 공통적인 인터페이스에서 조작될 수 있도록 각각의 인터페이스를 정의하여 명세 한다. 그리고 웹 서비스 구조(ID-WSF : Web Service Framework)는 데이터 규격 및 스키마, 웹 주소 전환 이동에 관한 구조를 제시한다. Liberty Alliance는 관련기술의 표준화와 관련하여 새로운 기술을 개발하지 않고 이미 제공되고 있는 관련된 기술인 WSS, WSDL, SAML, XML, HTTP, WAP, SOAP, SSL/TLS들의 기본적인 부분을 이용한다.

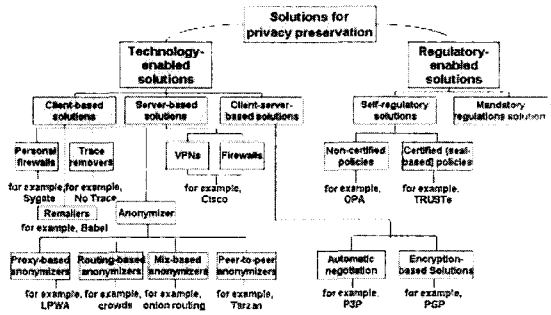
Liberty Alliance의 기본 모델을 따르면 기본동작에서 신원의 제공자 및 서비스 제공자의 신원정보는 연합시스템들과 공유되므로 하나의 이용자 신원에 연관된 모든 서비스 제공자에게 세션이 성립되고 종료되었음을 알려야 하고 이용자에 대한 사생활 정보를 위해 익명성을 보장해 줄 필요가 있다. 또한 이용자 SSO 과정에서 제공되는 전송메시지에 대한 무결성, 기밀성, 인증 기능이 제공되어야 한다.

Ⅲ. 프라이버시 보호 관련연구 동향

1. 웹 프라이버시

웹은 온라인상에서 정부와 기업 등 서비스를 제공하는 업체와 개인을 연결시켜주는 편리성을 제공하는 반면에 개인의 데이터를 침해할 수 있는 문제점이 있다. 웹의 개인정보의 프라이버시 침해는 정보의 주체가 허가하지 않은 정보의 전송, 개인 정보 보호의 취약함, 개인정보 데이터의 무분별한 수집 등으로 발생된다.

웹 프라이버시가 지켜지려면 웹 프라이버시의 위반사항을 설정하고 그 사항에 위배되지 않는 범위 내에서 개인정보 데이터를 사용한다. 또한 개인에게 민감한 정보에 대해서는 보다 높은 프라이버시보호 정책을 적용하여 프라이버시를 보호하도록 하고 개인정보를 유형별로 분류하여 웹 프라이버시가 위반사항을 위한 규정을 보다 용이하게 할 수 있도록 한다. 즉 웹 프라이버시를 위해서는 정보의 수집, 정보의 사용목적, 수집된 정보의 저장, 수집된



〔그림 1〕 웹에서 프라이버시 보호 방법의 분류

정보의 배포, 개인 정보 보호를 위한 정책과 도구들, 정보의 접근 제어, 개인정보 접근과 사용의 모니터링, 정보 보호 정책의 변경을 위한 규정이 필요하다.

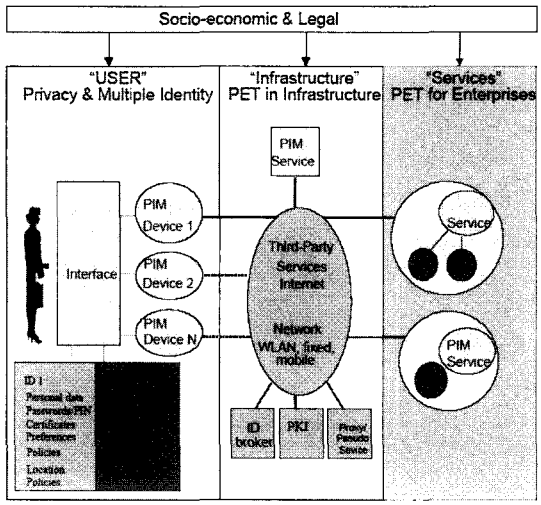
개인의 프라이버시를 보호하기 위한 방법들은 그림 1과 같이 기술적인 방법(Technology-enabled solutions)과 규범적인 방법(Regulatory-enabled solutions)으로 크게 분류될 수 있다[12].

기술적인 방법으로 첫째 클라이언트에 의한 방법이 있다. 이 방법은 개인의 프라이버시 보호 기준에 의해서 개인방화벽에 의한 개인PC 보호, 전자우편주소보호, 웹 접근 기록삭제, 웹 서핑 사용자의 익명성 제공 등이다. 둘째 서버에 의한 방법은 기업이나 단체 등 대규모에 적절한 개인의 프라이버시 보호를 위한 기술로서 가상 사설망 이나 방화벽을 이용할 수 있다. 셋째 클라이언트 서버에 기반을 둔 방법은 서버와 클라이언트가 서로 협력하여 개인의 프라이버시를 보호한다. 암호화에 의한 방법과, P3P와 같이 협상에 의한 방법으로 프라이버시를 보호한다.

규범적인 방법은 사적인 규범과 강제적인 규범에 의한 방법으로 분류 된다. 사적인 규범은 공인되지 않은 정책과, 공인된 정책이며 이들은 개인의 사생활을 보호하기 위해 사용된다. 다른 하나인 강제적인 규범은 국가나 정부에 의해 제정된 권고적인 프라이버시 보호 법률이다[12].

2. RAPID

RAPID(Roadmap for Advanced research in Privacy and Identity management)는 PIM(Privacy and Identity Management)분야의 연구주제를 결정하고 이 분야의 연구 주제들을 확인함으로써 EU 연구 커뮤니티를 활성화하는 것을 목표로 하는 프로젝트이다. RAPID의 목표들을 지원하기 위하여, 기반 구조들에서의



〔그림 2〕 RAPID 개념도

프라이버시 강화 기술들, 그림 2와 같은 기업 시스템들에서의 PIM, 다양하고 신뢰할 수 있는 신원 관리, 적법한 PIM 이슈들, 사회 경제적인 PIM 이슈들 등 5개의 세부적인 PIM 테마들로 연구되었다[1].

RAPID의 프라이버시 강화 기술과 ID 관리 방법에는 기술적 측면과 사회-경제-법률적 측면을 모두 고려하고 있다. 기술적 측면에는 개인 정보 보호에 사용되는 보안 메커니즘을 활용하는 인증, 접근 통제, 암호, 보안관리 기술 등이 가능하며, 서비스 제공자에 의한 ID 보호 기술로 익명의 웹 서핑, 계정과 가명의 프로비저닝(Provisioning)이 있다[12]. 그리고 원격 서비스 사용에 대한 무결성(Integrity)의 서비스 제공을 위해 사용자를 대신하여 디지털 ID를 관리하는 Liberty Alliance, MS Passport가 있으며, 공급자, 고객, 직원, 사업 파트너 간의 온라인 거래를 촉진하기 위해 Enterprise-IM 시스템들이 개발 중이다. 사회-경제-법률적 측면으로 우수한 개인 정보 보호를 실행하여 개인 정보 보호 규정을 준수하고, 불필요한 개인 정보의 수집이나 관리 비용을 절감하고 부정확하거나 오래된 정보와 연관된 위험 요소 제거에 목표를 두고 있다. 이를 통해, 개인 정보 처리에 대한 고객의 신뢰도가 향상됨으로써 기업의 높은 고객이 유지될 수 있게 된다.

RAPID의 기술적 연구들은 3개의 영역들로 구분된다. 첫 번째 영역은 다수(multiple)의 신뢰적인 ID 관리와 관련된 것으로서, 다양한 사회적, 기술적 상황에서 서로 다른 온라인 역할(employee, partner, customer)을 제시하고 상호 연관된 비즈니스 프로세스(commerce, health, government)를 사용하는 사용자들에 대한 다

수의 신뢰적인 ID 관리를 제안한다. 연구 주제로는, ID 프로비저닝 철회, 프로파일(profile) 관리, ID 급증 방지와 IM에 대한 사용자측 아키텍처, 인터페이스 및 개인정보 보호 기호(preference) 관리 개발, 서버 측에 다양한 아키텍처 및 자원에 대한 접근통제 기능 통합, 사용자 프로파일과 기호(preference) 기반과 개인 정보 보호에 적합한 접근통제 사용자 장치 개발, ID 도용 방지를 위한 신뢰할 수 있는 ID 보호 기술, 부분 ID의 연결이나 2차 사용(secondary use)을 통제할 수 있는 도구 개발 등이 있다. 기술적 연구의 두 번째 영역은 기반 구조와 관련된 것이다. 익명성은 개인 보호에 있어서 매우 중요한 역할을 담당하는 것으로, RAPID에서는 다양한 통신 계층에서 익명성을 제공한다. 총 5가지 계층에서 서로 다른 익명성을 제공하는데, address privacy, location privacy, service-level privacy, authorization privacy가 바로 그것이다. 마지막으로 기술적 연구의 세 번째 영역은 기업 ID 관리와 관련된 주제들이다. EIM (Enterprise Identity Management) 기능은 필요에 따라 사용자 식별이 불가능한 방식으로 사용자 인증을 하고 사용자 권한 부여를 하며 기업 정보의 보호와 기업 정보의 침해 발생 시 경보 발생 기능을 한다. 이 분야에서의 연구 주제들은 기업 정보시스템 PET(Privacy Enhanced Technology) 기능, 실행 기술, 온톨로지(Ontology), 접근통제 정책 등이다.

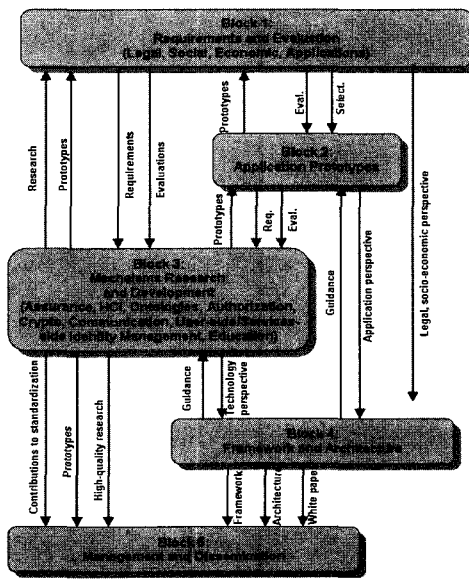
RAPID의 비 기술적 연구들은 2개의 영역들로 구분된다. 비 기술적 연구의 첫 번째 영역은 사회-경제적 영역들이다. 개인의 정보보호는 정치적인 의사 결정에 있어서 다른 사회적 가치와 충돌하는 사회적 개념으로 볼 수 있다. 이 영역에서의 주요 연구 주제들은, 서로 다른 당사자 간 다양한 관계에서 사람들의 신뢰가 무엇인지에 대해 분석하고, 이러한 관계에서 개인정보보호와 ID 관리가 어떻게 효과적으로 다루어질 수 있는지에 대해 분석한다. 또한 디지털식별(identification) 설계에 대해 정부가 독점적 위치가 필요한 사례 및 환경에 대한 분석과 개인 회사가 우선권을 갖는 사례 및 환경 분석, 디지털 ID 서비스와 PIM 관련성 분석, PIM 개발자와 PIM 비즈니스 모델을 지원하는 방법이나 조건에 대해 분석한다. 비 기술적 연구의 두 번째 영역은 법적 영역들이다. 개인정보보호 기술에 대한 연구 등의 결론은 기술과 규정만으로는 불충분하며 둘 간의 격차를 좁힐 수 있는 메커니즘을 연구한다. 이 영역에서의 주요 연구 주제들은 프라이버시 온톨로지, 디지털 ID의 다수성, 온라인 익명, 가명 사용의 법적 의미, 개인정보보호에 적합한 PKI의 법적 한계, 개인 정보 보호에 적합한 DRM[18]의 법적 한계, 개인 정보 보호 요구 사항과 전자 정부의 기능 요구와의 대비, 국가 보안, 법 집행이다.

3. PRIME

PRIME(Privacy and Identity Management for Europe)[2] 프로젝트는 유럽의 주요한 연구단체들을 중심으로 W3C등 주요 표준화 기관과 연계된 개인의 프라이버시 보호를 위한 프로젝트이다[2]. 이것은 개인들이 정보화 사회에서 그들의 행위와 무관하게 스스로 개인정보를 제어하여 그들의 자치를 보호하는데 목적이 있다. 정부, 사회, 경제, 전문적인 분야를 총괄하는 정보화 사회 전반에 걸쳐 프라이버시를 제공하도록 하고 최종 사용자에게 프라이버시를 제공하는 ID 관리에 초점을 맞추고 ID 관리의 프라이버시를 위한 프레임워크를 제안하기 위해 2004년에 시작해서 그림 3과 같이 향후 4년 동안 5단계로 나누어 프로젝트를 수행하고 있다.

또한 편리한 컴퓨터 사용자 인터페이스, 온톨로지, 인가(Authentication), 암호화(Encryption)기술을 기초로 하고 최신의 ID 관리 기술과도 상호 동작하고 프로그램 개발자나, 서비스 제공자, 애플리케이션 운용자 등 특정 산업과 연루되는 여러 응용들과 관련된 전문가들을 위한 프라이버시 보호 지침에 해당하는 표준 기술의 제공을 목표로 한다.

PRIME 연구의 핵심부분인 그림 3의 Block 3에서는 프라이버시 보호를 위한 온톨로지 개발, 프라이버시 보호



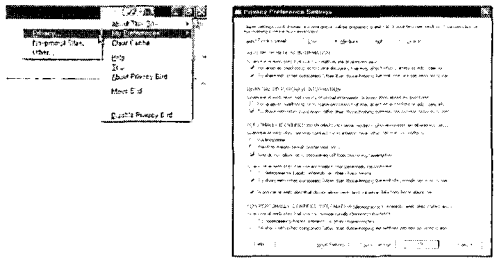
〔그림 3〕 PRIME 프로젝트 구조 및 연관성

를 위한 속성(위치, nym 등)기반 인가정책 및 모델의 개발, 개인정보의 암호를 위한 암호기술 및 프로토콜 개발, 단대단(end-to-end) 안전한 통신과 익명성 보장을 위한 통신 인프라기술 개발, 사용자측 및 서버측 신원관리를 위한 도구 개발, 프라이버시 보호기술의 보증을 위한 평가방법 개발 등을 진행한다.

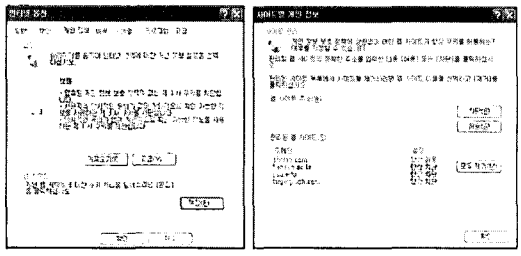
4. P3P

P3P(Platform for Privacy Preferences Project)[4,14,15]는 웹사이트에서 사용자 프라이버시를 보호하기 위한 개인정보 정책을 기술하는 W3C(the World Wide Web Consortium)에서 제정한 표준이다. 사용자가 방문하는 웹사이트에서 사용자가 자신의 개인정보를 제어할 수 있도록 개인정보보호정책(Privacy statement)을 기술하는 산업 표준으로 웹사이트에서 프라이버시 보호를 위한 관리방법 등을 기술하기 위한 표준 용어집과 문법을 정의하고 있다. 개인정보보호정책은 웹 사이트 방문객들과 신뢰받는 관계를 만들어내는데 사용되는 주요한 컴포넌트로 기업이나 개인이 수집한 데이터, 특정 목적에 의해 수집된 데이터의 사용, 특정 사람에게 데이터의 사용허가 등을 기술한다. P3P는 사이트에서 사용자의 정보를 어떻게 다룰지에 대한 정책이 정의되어 있으며 P3P를 지원하는 사용자의 브라우저는 이 정책을 사용자가 볼 수 있어서 그 정책과 사용자 브라우저 사이의 정책에 따라 동작을 제한하기도 한다. 개인정보보호정책과 관련해서 P3P가 제공하는 기능은 사용자 개인정보정책을 생성하고 다양한 자원들로부터 정보를 수집해서 유지하며 정보 사용자를 인증하고 정보데이터를 제공할 타입으로 변형하고 제공된 개인정보가 정책에 따라서 올바르게 사용되었음을 정보의 주체에게 증명한다.

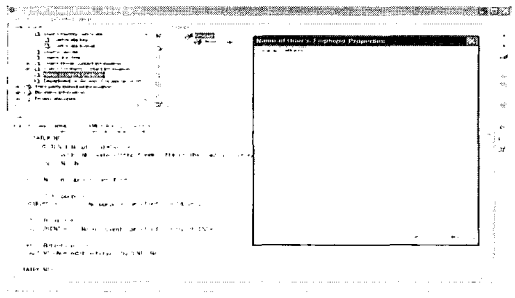
P3P는 사용자 스스로 자신의 정보 관리와 권한을 부여하도록 해서 사용자 정보가 잘못된 방법으로 사용되는 것을 미연에 방지한다. 사용자가 웹 사이트를 방문할 때, 사용자측 에이전트는 방문할 사이트의 프라이버시 정책 파일을 획득하고 이를 방문자가 이미 설정해 놓은 사용자 정보 공개 수준과 비교하여 정보를 선별적으로 제공할 수 있다. 웹 사이트는 XML 문서형식으로 자신의 프라이버시 정책을 게시하며 사용자는 자신의 웹 브라우저(또는 P3P 에이전트)에 자신의 정보에 대한 정보 공개 수준을 설정한다. 일반적으로 P3P는 마이크로소프트사의 IE 6.0 (Internet Explorer 6.0)이상 이나 그림 4의 AT &T Privacy Bird[21]에서 사용된다. IE 6.0에서는 P3P를 구현하지만, Compact Policy와 사용자 설정에 따라 쿠키를 필터링하는 기능만을 제공한다. P3P는 XML문서로 정의되며 이를 생성하기 위해서는 전용 에디터를 사용하거나, 관련 업체에 의뢰 받아 생성하도록 해야 하지만 그림 5의 익스플로러의 Compact Policy는 익스플로러의 옵션의 개인정보에서 개인의 선호도에 맞는 설정을 함으로써 프라이버시 정책을 사용한다. Compact Policy는 XML문서로 정의되는 일반적인 P3P와는 다르게 데이터 양이 적고 구조가 간단해서 브라우저에서 바로 정책을 해석하여 판단을 내릴 수 있다.



〔그림 4〕 AT&T Privacy Bird



〔그림 5〕 익스플로러의 Compact Policy



〔그림 6〕 IBM Policy Editor

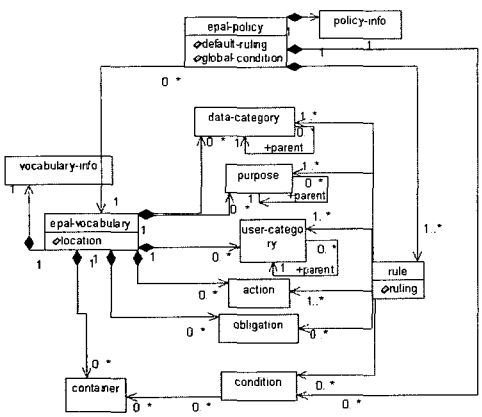
일반적으로 개인정보보호정책의 생성은 그림 6과 IBM Policy Editor[20]와 같은 자동화된 GUI 도구를 이용한다. P3P의 개인정책을 자연어로 확인하고 선택문에 대답하여 개인정보보호정책을 설정한다. GUI 도구는 P3P의 어휘와 문법에 의해 사용자가 설정한 프라이버시 정책을 XML포맷으로 변환하여 개인정보보호 정책을 생성한다.

5. IBM의 E-P3P와 EPAL

E-P3P는 IBM의 프라이버시 연구소에서 개발한 기술로서, 대표적인 프라이버시 보호 기술로 알려진 P3P의 한계를 인지하고 기업 내부에서 고객들의 프라이버시 정보를 신뢰할 수 있는 방법으로 관리할 수 있도록 하는 프레임워크라 할 수 있다[5].

E-P3P나 EPAL(Enterprise Privacy Authorization Language)은 기업입장에서 사용자가 제공한 개인정보데이터를 사용자가 원하는 범위 내에서 안전하게 사용하도록 한다. EPAL은 응용들과 기업들 사이의 구조화된 포맷에서 프라이버시 정책을 교환하기 위한 상호 운용적인 언어이다. 이것은 인증 권한에 따라 IT 시스템들에서 데이터 조작 실무들을 관리하기 위한 기업 프라이버시 정책들을 기술한다. EPAL은 그림 7과 같이 Data-category, User-category, purpose, sets of privacy actions, Obligations, Conditions의 계층들의 리스트들을 정의한다[3]. User-category는 수집된 데이터를 사용하는 객체들 즉 사용자들과 그룹들을 의미하고, Data-category는 프라이버시 관점으로부터 다르게 조작되는 수집된 데이터의 다양한 카테고리들이다.

Purpose란 임의의 데이터가 사용되는 의도된 목적이며, Action은 어떻게 데이터가 사용되는지 기술한다. Obligation은 EPAL 환경에 의해 발생되어야만 하는 행동들을 나타내고, Condition은 context를 평가하는 Boolean 표현들이다. 어떤 프라이버시를 유지하기 위한 규칙들이 요구되는 동안 어떤 조건들 하에서 어떤 목적들을 위한 사용자-카테고리들에 의해 데이터-카테고리들 상의 행동들을 허용하거나 거부하는 프라이버시 인증 규칙들을 생성하는데 사용된다. EPAL 정책들은 기업이 가지고 있는 데이터와 각 카테고리의 데이터의 사용을 관리하는 규칙들을 목록화하며 각 정책기술 요소들이 프라이버시 정책들을 반영하도록 설계되어 있다. 정책을 생성할 때 사용되는 요소들의 정의를 위한 메커니즘도 제공한다.



〔그림 7〕 EPAL 정책의 UML 표현

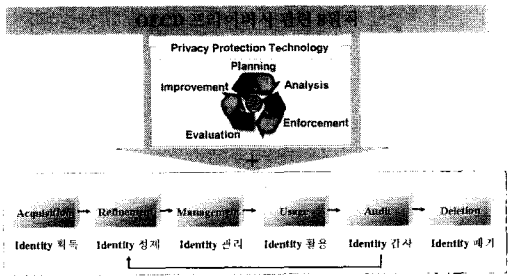
Ⅳ. 개인정보 생명주기

개인의 프라이버시 보호를 위해서는 개인이 허용하는 범위 내에서만 개인정보가 사용돼야 하므로 개인정보의 생성부터 활용, 폐기까지의 단계에서 프라이버시를 고찰할 수 있는 기본 모형이 필요하다. 따라서 우리들은 프라이버시 보호를 위해 개인정보의 흐름을 관리할 수 있는 개인정보의 생명주기를 제안한다.

제안된 개인정보 생명주기에서 프라이버시 적용대상은 개인이 제공하는 신원 정보이며 이들 정보는 일정한 순환단계를 반복한다. 개인이 제공하는 여러 신원 정보들은 생명주기관점에서 표 2와 같은 단계로 나눌 수 있

〔표 2〕 개인정보 생명주기 단계별 수행과제

구 분	내 용
1단계: 획득 (Acquisition)	· 데이터 생성 및 데이터의 사용목적에 일치하는 데이터를 수집 · 데이터 획득과정에 발생하는 과정을 정보 소유자에게 보고 · 정보수집 및 인가확인(개인정보 모니터링 도구이용)
2단계: 정제 (Refinement)	· 시스템에 필요한 정보 데이터 형으로 변환 · 데이터 온톨로지 수행(수집된 데이터의 온톨로지를 위해 표준 용어로 변환) · 수집된 데이터 사용자 및 그룹 분류 · 수집된 데이터의 다양한 프라이버시 카테고리 분류(Ex. 데이터 민감도에 따른 분류)
3단계: 관리 (Management)	· 데이터 사용목적 동안 유효한 정책을 적용하여 데이터를 시스템 데이터베이스나 기타 위치에 저장 및 유지 · 데이터 저장유지 및 폐기를 정보소유자에게 보고
4단계: 활용 (Usage)	· 개인정보 사용목적에 의거하여 사용 · 각 사용목적에 따른 활용과정을 정보소유자에게 보고 · 데이터 정보사용 보고(확인 및 감사 목적)
5단계: 감사 (Audit)	· 데이터의 무결성 확인 · 프라이버시 침해 점검 · 프라이버시 위험도와 손해분석(개인정보 모니터링 도구이용)
6단계: 폐기 (Deletion)	· 수집된 데이터를 주기적으로 확인하여 데이터 보존정책에 어긋나는 데이터 폐기 · 보존정책에 어긋나는 데이터 분류규정 · 사용자 요청에 의한 개인정보 폐기



〔그림 8〕 개인정보 생명주기

다. 이러한 개인정보의 생명주기를 이용하여 개인정보를 단계별로 분석하면 단계별로 프라이버시측면이 강화될 수 있으므로 보다 완벽한 정보의 프라이버시가 제공될 수 있다.

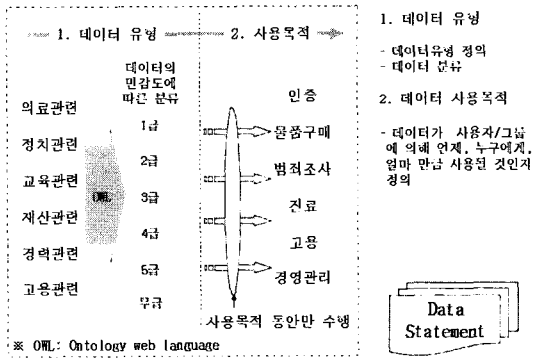
개인정보의 생명주기는 신원 정보 데이터의 획득, 정제, 관리, 활용, 감사, 폐기 등 6단계로 구성된다. 또한 이와 같은 각 단계는 프라이버시 보호를 위한 정책들을 계획(Planning), 분석(Analysis), 수행(Enforcement), 평가(Evaluation), 개선(Improvement) 과정을 그림 8과 같이 수행한다.

1. 1단계: 획득

획득 단계는 정보사용자가 정보를 요청하면 정보의 주체는 정보사용자가 요청하는 개인정보의 사용목적을 확인해서 어떠한 목적에 의해 정보데이터가 수집되고 사용될 것인지 확인한다. 정보의 주체가 허용하는 범위 내에서 개인정보를 정보를 요청한 사용자에게 제공한다.

2. 2단계: 정제

정제 단계는 수집된 정보데이터를 일련의 과정을 거쳐 정보데이터를 수집한 서비스 기관에 맞게 필요한 데이터 타입으로 가공하는 역할을 수행한다. 수집된 정보데이터는 개인정보 사용 목적에 기반 하여 그림 9과 같이 프라이버시 보호를 위한 정보데이터 구문(Data Statement)으로 변환된다. 예를 들면 그림 9와 같이 데이터 유형은 수집된 정보데이터가 어떤 정보관련 데이터(의료, 정치, 교육, 재산, 경력, 고용)인지 확인하고 데이터의 민감도에 따라서 1급~무급까지 데이터를 분류한다. 데이터 유형별로 분류된 데이터는 사용목적(인증, 물품구매, 범죄조사, 진료, 고용, 경영관리)으로 분류된다. 생성된 데이터 구문들은 혼합(Mixing), 분리(Disjunction), 감축(Reduction)되어 개인정보 프라이버시를 위한 유용한 데이터 타입으로 가공된다.



〔그림 9〕 개인정보 생명주기 2단계

3. 3단계: 관리

관리 단계는 정제단계를 거쳐서 데이터의 유형에 따라 구분되고 사용목적에 따라 세분화되어 생성된 데이터 구문(Data statement)이 유지 및 관리되는 단계이다. 2단계에서 생성된 데이터 구문의 유지 기간을 설정하고 데이터의 민감도나 정보의 사용자에 따라 분류되어 저장된다.

4. 4단계: 활용

활용 단계는 단계 3에서 생성된 데이터구문을 사용자의 개인정보보호 정책이 허용하는 목적동안만 사용될 수 있도록 한다. 데이터를 사용할 사용자가 특정 정보를 요청하고, 요청된 정보가 어떤 데이터구문에 포함되어있을 때 그 구문의 접근을 허가하기 이전에 개인정보의 사용목적을 확인하고 해당 데이터구문에 설정된 개인정보보호 정책과 비교하여 접근을 허용한다. 접근이 허용된 데이터 구문은 정보 요청자의 정보사용 목적, 사용자유형, 데이터의 민감도에 따라 사용될 정책을 설정한다.

5. 5단계: 감사

감사 단계는 관리 단계에서 획득한 데이터구문의 활용(Usage)과 폐기(Deletion)가 정확하게 수행되는지 점검한다. 정보의 획득, 관리 활용단계에서 정보데이터의 접근과 사용을 모니터링(Monitoring)하고 정보데이터의 활용과 폐기를 검사한다. 데이터구문의 무결성(Integrity), 사용목적(Purpose), 데이터구문의 유지(Retention) 정책 등을 확인한다.

6. 6단계: 폐기

폐기 단계는 데이터구문의 정책에 따라서 데이터를 삭

제하거나 감사과정에서 확인된 오용되거나 정책에 위배되는 데이터모듈을 폐기하고 폐기 과정이 정확하게 수행되었음을 확인하고 정보의 주체에게 알린다.

V. ID 관리시스템에서의 프라이버시

1. ID 관리시스템에서 프라이버시 관리 영역

개인의 신원정보를 저장, 관리하는 ID 관리시스템과 연관된 구성요소들로는 개인정보를 제공하는 일반사용자인 개인정보 제공자, 사용자의 신원을 확인하고 인가된 사용자에 한해 서비스를 제공하는 서비스 제공자 (SP: Service Provider) 등이 있다. 개인정보 제공자는 IDSP (Identity Service Provider)에 자신의 신원정보를 제공하고, SP들은 서비스 제공을 위해 필요한 사용자의 신원정보를 IDSP에 요구한다. IDSP는 SP가 요구하는 사용자의 신원정보를 개인정보 제공자가 지정한 사용목적 등을 참조하여 제공여부를 결정하고 필요에 따라 사용자에게 동의를 구한 후 SP에게 개인정보를 전송한다.

이러한 환경에서 개인의 정보를 보호하기 위한 영역들로는 개인정보 제공자가 IDSP에 제공하는 개인정보, IDSP가 SP에 제공하는 개인정보, IDSP나 SP에 의해 새롭게 생성되는 개인과 관련된 정보들이 있다. 개인정보 제공자들이 IDSP에 제공하는 정보의 대부분은 사용자가 IDSP 서비스에 가입할 때 생성되며, IDSP가 SP에 제공하는 정보는 SP가 IDSP에 개인정보를 요구할 때 SP로 전달되고 당초 SP가 IDSP에 제시한 사용목적에 부합되게 사용되어야 한다. IDSP나 SP에 의해 새롭게 생성되는 정보는 사용자의 접근기록이나 행위로부터 발생되는 개인정보 데이터이다.

개인정보의 프라이버시를 위해서 이들 영역들은 개인정보 생명주기에 따라 안전하게 관리되어야 한다.

2. 프라이버시 생명주기를 적용한 ID 관리

개인정보 제공자가 IDSP에 제공하는 정보는 가입과정에서 생성된다. IDSP에 가입되지 않은 사용자인 개인정보 제공자가 IDSP에 가입하려할 때 IDSP는 개인정보를 요청하게 되고, 이때 IDSP는 정보 제공자에게 정보의 수집 목적을 알리고 동의를 받은 후 개인 정보를 획득한다. 획득된 개인정보는 IDSP가 정보수집 목적에 부합하도록 정제단계를 거쳐서 그림 9와 같이 데이터구문을 생성한다. 저장된 정보는 정보제공자에 의해서 수정되거나 삭제될 수 있으며 새로운 프라이버시 보호정책에 의해 관리될 수 있다.

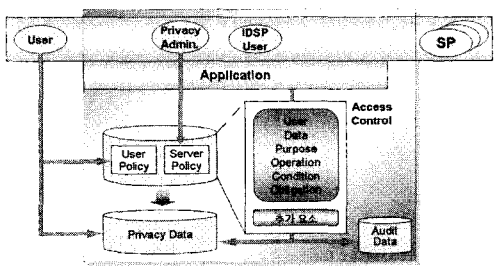
IDSP가 SP에 제공하는 정보의 이동은 SP가 IDSP에게 개인정보를 요청함으로써 발생된다. IDSP는 SP의 정보사용 목적을 개인정보 제공자에게 알리고 동의를 받거나 IDSP는 SP의 정보 사용목적을 당초 정보 제공자가 설정한 프라이버시 보호정책과 비교해서 정보사용 여부를 결정한다. 요청된 개인정보 사용이 허가되면 IDSP는 정제단계를 거쳐서 개인정보데이터를 가공하고 이후 관리단계에서 사용목적에 부합하도록 제한사항을 설정한 후에 SP가 요청한 개인정보는 전송된다. SP에 전송된 개인정보는 생명주기의 활용단계를 거치며, 이때 감사단계가 수행되어 개인정보의 정확한 사용 여부가 기록된다.

IDSP나 SP에 의해 새롭게 생성되는 개인과 관련된 정보들은 수집될 때 개인정보의 주체인 개인정보 제공자에게 정보의 수집을 알려서 정보수집에 대한 동의를 얻거나, IDSP에 유지된 당초 정보제공자의 개인 기호(preference)를 정보수집 목적과 비교해서 정보허용 여부를 판단한다. 사용이 허용되는 정보데이터는 IDSP나 SP로 전송되어 정제단계를 거쳐 프라이버시를 위한 유용한 구문으로 변경되고, 생명주기의 관리단계를 거쳐 정보 사용목적 동안 시스템의 특정위치에 저장되거나 사용된다.

ID 관리시스템에서 정보의 폐기는 정보의 주체인 정보제공자의 정보폐기 요청이나 관리단계에서 정보사용 목적에 부합하도록 설정된 기간 동안만 유지된다.

3. ID 관리 환경에서 프라이버시 보호 실행 구조

본 논문에서는 IDSP에서 저장, 관리되는 개인정보에 대한 프라이버시를 보호하기 위해 사용할 수 있는 주요 기술로 접근통제기술을 제시한다. 그림 10과 같이 IDSP에 의해 관리되는 개인정보는 개인정보 제공자에 의해 생성되고, IDSP의 프라이버시 관리자와 사용자, SP들에 의해 사용, 관리된다. 따라서 IDSP에 저장된 개인정보에 대한 접근을 개인정보 제공자나 IDSP의 프라이버시 관리자에 의해 설정된 보안정책에 의해 통제하면 프라이버시 보호를 위한 주요 보안기능을 수행할 수 있다.



〔그림 10〕 프라이버시 보호 실행 구조

3.1 정보사용자

ID 관리 환경에서 개인정보 사용자로는 개인정보 제공자 (User), 개인정보 관리하는 IDSP 사용자 (IDSP User), 서비스 제공자(SP) 등이 있다. 이들은 인증과정을 통과한 후 프라이버시 보호 정책에 기반을 둔 정해진 응용을 통해서만 개인정보에 접근할 수 있다.

3.2 접근통제 정책

ID 관리 환경에서 접근통제 정책으로는 개인정보 제공자의 개인정보 보호정책(User Policy)과 IDSP 사용자나 SP들의 개인정보 보호 정책(Server Policy)이 있다. 개인정보 제공자의 접근통제 정책은 정보주체와 관련된 개인정보데이터를 통제할 수 있도록 정보의 사용목적, 정보 접근의 제한사항, 의무사항 등을 정보제공자의 기호(preference)에 의해 정보제공자가 설정하고 IDSP 사용자나 SP들에 대한 개인정보 보호 정책은 개인정보에 접근·사용할 수 있는 조건, 연산의 종류, 의무사항 등을 명시한 정책이며 프라이버시 관리자에 의해 설정된다.

Ⅵ. 결 론

프라이버시는 정보의 주체가 그들 스스로 자신이 소유한 정보를 다른 사람에게 언제, 어떻게, 얼마나 공개할 것인가를 결정하도록 하고 결정된 범위 내에서만 정보가 사용될 수 있도록 하면 보호될 수 있다. 개인들은 정보화 사회에서 행정, 의료, 정보, 금융 등의 여러 서비스를 제공받기 위해서 개인정보를 제공해야 되고, 개인이 제공하는 여러 정보들은 개인과 깊은 관련이 있어서 프라이버시를 침해할 수 있는 원인이 된다. 따라서 프라이버시를 위해서는 개인정보는 주체의 의지대로 생성, 사용, 수정, 폐기 될 수 있어야 한다.

본 논문은 프라이버시 보호를 위한 국외의 주요 프로젝트와 관련기술 및 법, 제도들을 조사하고 ID 관리 시스템에서의 프라이버시 보호 측면에 대해 살펴보았다. 또한, ID 관리시스템에서 개인정보에 대한 체계적 보안정책 수립과 실행을 위해 필요한 개인정보 생명주기를 제안하고, 접근통제기술에 기반을 둔 프라이버시보호 실행구조를 제시하였다.

앞으로는 제안된 개인정보 생명주기와 ID 관리시스템의 개인정보 보호 실행구조를 보완하고, 접근통제기술과 함께 프라이버시 보호에 활용될 수 있는 기술을 연구한다.

참 고 문 헌

[1] "RAPID : Roadmap for Advanced Research in Privacy and Identity Management," 2001. http://www.ra-pid.org

[2] "PRIME : Privacy and Identity Management for Europe Date of preparation," February 2004, http://www.prime-project.eu.org/

[3] Paul Ashley, Satoshi Hada, Günter Karjoth, Calvin Powers, Matthias Schunter, "Enterprise Privacy Authorization Language (EPAL 1.2)," W3C, 2003. http://www.w3.org/Submission/2003/SUBM-EPAL-20031110/

[4] "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification,"W3C, April 2002. http://www.w3.org/TR/P3P/

[5] P. Ashley, S. Hada, G. Karjoth, M. Schunter, E-P3P, "Privacy Policies and Privacy Authorization," WPES, November 2002.

[6] "Privacy Online OECD Guidance on Policy and Practice," OECD, 2003. http://www1.oecd.org/publications/e-book/9303051E.PDF

[7] "Liberty Alliance: Introduction to the Liberty Alliance Identity Architecture," Revision 1.0 Liberty Alliance Project, March 2003.

[8] Maler, Eve, Mishra, Prateek, Philpott, Rob, "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1," OASIS, May 2003.

[9] P. Ashley, M. Schunter, "The Platform for Enterprise Privacy Architectures," Information Security Solutions Europe, 2002.

[10] Cantor, Scott, Kemp, John, "Liberty ID-FF Protocols and Schema Specification," Version 1.2 Liberty Alliance Project, January 2004.

[11] "Sourceid: Open Source Federated Identity Management," Ping Identity, 2004. http://www.sourceid.org/

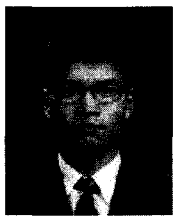
[12] Abdelmounaam Rezgui, Athman Bouguet-

taya, Mohamed Y. Eltoweissy, Virginia Tech, "Privacy on the Web: Facts, Challenges, and Solutions", IEEE Security and Privacy (Vol. 1, No. 6), 2003.
[13] "Privacy and Security Best Practices," Liberty Alliance project, November 12, 2003.
[14] G. Karjoth, M. Schunter, E. Van Herreweghen, and M. Waidner, "Amending P3P for Clearer Privacy Promises", 14th International Workshop on Database and Expert Systems Applications (DEXA'03), September 01 - 05, 2003.
[15] Lorrie Faith Cranor, "P3P: Making Privacy Policies More Useful", IEEE Security and Privacy,November - December 2003 (Vol. 1, No. 6), pp. 50-55, 2003.
[16] 두산대백과 용어사전, 두산, 2004. http://www.encyber.com/infocomdic/content.php?IDNO=45885&pagenum=1&key=프라이버시
[17] Samuel D. Warren/Louis D. Brandeis, The Right to Privacy, Harvard Law Review, 1980.
[18] Claudine Conrado, Frank Kamperman, Geert Jan Schrijen, Willem Jonker, "Privacy in an Identity-based DRM System," 14th International Workshop on Database and Expert Systems Applications, 2003.
[19] "Microsoft .NET Passport," Microsoft, 2004, http://www.microsoft.com/net/services/passport/
[20] "IBM Policy Editor," IBM, 2004. http://www.alphaworks.ibm.com/tech/p3peditor
[21] "AT&T Privacy Bird," AT&T, 2004. http://www.privacybird.com
[22] "정보보호 뉴스," KISA(한국 정보보호 진흥원), 2004. 3, http://www.kisa.or.kr
[23] "APEC Privacy Principles," APPCC, May 2003. http://www.bakercyberlawcentre.org/appcc/apec_redraft_v2.htm

〈著 者 紹 介〉

최 향 창(Hyang-Chang Choi)
학생회원

2002년 8월 : 전남대학교 대학원 전산학과 졸업(이학석사)
2003년 2월~현재 : 전남대학교 대학원 정보보호 협동과정(박사과정)
〈관심분야〉 컴퓨터와 네트워크 보안, 전자상거래 보안, 유비쿼터스 보안



이 용 훈 (Yong-Hoon Lee)
정회원

1994년 2월 : 전남대학교 전산통계학과 석사(이학석사)
2003년 8월 : 전남대학교 전산통계학과 박사(이학박사)
1994년~1997년 : Hewlett Packard Korea.
1997년~2000년 : 한국교육학술정보원
2003년~현재 : 전남대학교 리눅스보안 연구센터 선임연구원
〈관심분야〉 정보보호(보안모델, 인증/인가 기술, 보안명세), 컴퓨터/네트워크 보안

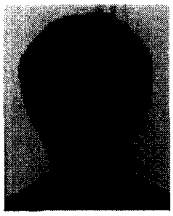
노 봉 남(Bong-Nam Noh)
정회원

1978년 2월 : 전남대학교 수학교육과 졸업(학사)
1982년 2월 : KAIST 대학원 전산학과 졸업(석사)
1994년 2월 : 전북대학교 대학원 전산과 졸업(박사)
1983년~현재 : 전남대학교 컴퓨터정보학부 교수
2000년~현재 : 리눅스 보안 연구센터 소장
〈관심분야〉 컴퓨터와 네트워크 보안, 정보보호시스템, 전자상거래 보안, 사이버사회와 윤리

이 형 효 (Hyung-Hyo Lee)
정회원

1987년 2월 : 전남대학교 계산통계학과 졸업(학사)
1989년 2월 : 한국과학기술원 전산학과 졸업(석사)

2000년 2월 : 전남대학교 대학원 전산학과 졸업(박사)
1990년~1997년: 삼보컴퓨터 기술연구소, 한국통신 연구개발원
2001년 3월~현재: 원광대학교 정보·전자상거래학부 조교수
〈관심분야〉 보안모델, 네트워크보안, 전자상거래보안



조 상 래 (Sang-Rae Cho)
정회원

1996년 2월 : Imperial College of Science, Technology and Medicine, 전산과 (학사)
1997년 2월 : Royal Holloway, University of London, 정보보호 (석사)
1997년~1999년 : LG 종합기술원 연구원
1999년~현재 : 한국전자통신연구원 연구원
〈관심분야〉 정보보호(PKI, 인증/인가 기술, 프라이버시 보호기술), 컴퓨터/네트워크 보안

진 승 헌 (Seung-Hun Jin)
정회원

1995년 2월 : 숭실대학교 전자계산공학과 졸업(석사)
2004년 2월 : 충남대학교 컴퓨터과학과 졸업(이학박사)
1996년 4월 : (주)대우통신 종합연구소 연구원
1999년 5월 : (주)삼성전자 통신연구소 전임연구원
1999년 6월~현재 : 한국전자통신연구원 정보보호연구본부 인증기반연구팀 팀장
〈관심분야〉 정보보호(PKI, 인증/인가 기술, 프라이버시 보호기술), 컴퓨터/네트워크 보안