인터넷 Identity 관리 시스템을 위한 프라이버시 인가

정회원 노 종 혁*, 진 승 헌*, 종신회원 이 균 하**

Privacy Authorization for Internet Identity Management System

Jong-Hyuk Roh*, Seung-Hun Jin* *Regular Members*, Kyoon-Ha Lee** *Lifelong Member*

요 약

인터넷에 산재되어 있는 사용자 개인정보의 오남용은 더 이상 간과할 수 없는 문제이다. 개인정보의 유통은 반드시 소유자의 허가 하에서만 이루어져야 하고, 개인정보를 관리하는 사이트는 인터넷에 익숙하지 않은 사용자들에게 개인정보 유출에 관한 두려움을 없애줄 수 있는 환경을 제공하여야 한다. 본 논문은 인터넷 Identity 관리 시스템에서 개인정보를 안전하게 관리하고 유통할 수 있는 기술을 소개한다. 개인정보의 소유자가 자신의 정보를 관리하는 방법, 정보 관리 시스템 차원에서 사용자 정보를 관리하기 위한 정책, 개인정보 접근을 제어하는 Privacy Controller 등 여러 관점에서의 프라이버시 인가 기술을 제안한다. 그리고, 정책 기반의 프라이버시 인가 기술을 인터넷 Identity 관리 시스템에 적용하기 위한 다양한 모델을 제시한다.

Key Words : Privacy, Privacy Authorization, Digital Identity, Identity Management

ABSTRACT

One's identity on the Internet has been disclosed and abused without his consent. Personal information must be protected by appropriate security safeguard. An Individual should have the right to know whether his personal details have been collected and stored. This paper proposes various conceptual models for designing privacy enabling service architecture in the Internet identity management system. For the restriction of access to personal information, we introduce the owner's policy and the management policy. The owner's policy should provide the user with enough information to manage easily and securely his data. To control precisely and effectively all personal information in the Identity provider, we propose the privacy management policy and the privacy authorization model.

Ⅰ. 서 론

프라이버시의 중요성에 대해서는 오래 전부터 많은 사람들이 인식하고 있었지만, 컴퓨터가 발명되기 이전에는 프라이버시 문제가 크게 복잡하지 않았다. 그 당시에는 개인의 정보를 보관하는 곳은 학교, 직장, 공공기관, 금융기관과 같은 신뢰할 수 있는 곳이 전부였고, 정보의 유통 또한 대화에 의하거나 주로 문서의 전달로 이루어지는 형태였다. 그러므로 타인의 개인 정보를 얻기란 쉬운 작업이 아니었다. 하지만, 컴퓨터가 사람들에게 익숙해지고 인터넷이 실생활의 큰 부분을 차지하면서 프라이버시의 중요성이 새롭게 대두되었다.

인터넷에서 많은 사이트들은 사용자들에게 서비스를 제공하면서 사용자들에게 등록을 요구하고 있다. 사용자들은 서비스를 이용하기 위해 새로운 사이트에 가입할 때마다 주소, 전화번호, 주민등록번호 등 자신의 중요한 개인정보를 입력한다. 사용자들은 너무 많은 사이트에 가입을 하다 보니, 사용자 스스로 어느 사이트에 가입을 했는지 어떤 정보를

* 한국전자통신연구원 정보보호연구단(jhroh@etri.re.kr),
** 인하대학교 컴퓨터정보공학과
논문번호 : KICS2005-04-154, 접수일자 : 2005년 4월 13일

등록했는지 기억하기 쉽지 않다. 그리고 인터넷의 수많은 영세 사이트들은 고객의 정보를 관리함에 있어 정보보호 및 프라이버시 보호 문제들은 전혀 고려하고 있지 않다. 심지어 고객의 정보를 불법으로 판매하는 일도 벌어지고 있다. 최근에 들어 사용자들은 자신의 정보가 유출되고 있음을 점차 두려워하고 있다. 이는 곧 전자거래 활성화의 큰 저해요인으로 작용할 수 있다.

인터넷 Identity 관리 시스템은 사용자가 인터넷을 사용함에 있어 보다 편하고 안전한 환경을 제공하는 것을 목표로 한다. 즉, 한번의 로그인 과정으로 인터넷의 많은 사이트들을 자유롭게 사용할 수 있는 SSO(Single Sign On) 서비스를 제공하고, 사용자의 정보를 안전한 사이트에 저장함으로써 자신의 정보를 최신의 상태로 유지하고 안전하게 관리할 수 있게 해준다.

본 논문은 인터넷 Identity 관리 시스템에서 개인정보를 안전하게 관리하고 유통할 수 있는 기술을 소개한다. 개인정보의 소유자가 자신의 정보를 관리하는 방법, 관리 시스템 차원에서 개인정보를 관리하기 위한 정책, 개인정보 접근을 제어하는 Privacy Controller 등 다양한 관점에서의 프라이버시 인가 기술을 설명한다.

본 논문의 2장에서는 프라이버시에 대한 정의 및 관련 지침을 살펴보고 Identity 관리 시스템과 관련된 표준 및 기술을 소개한다. 3장에서는 프라이버시 인가의 정의를 내리고 Identity 관리 시스템에서의 개인정보 유통 시나리오 및 프라이버시 제어 주체에 따른 다양한 정보 제어 방법을 소개한다. 4장에서는 개인정보 소유자 정책과 관리 정책에 따른 다양한 모델을 제시하고 각각의 특징을 살펴본 후, 5장에서 결론을 맺는다.

Ⅱ. 프라이버시 및 Identity 관리 시스템

본 논문은 인터넷 환경의 Identity 관리 시스템에서 개인정보 보호를 어떻게 제공하는 가에 관한 것이다. 본 장에서는 프라이버시에 대한 정의 및 관련 지침 등에 대해서 간단하게 살펴본 후, 논문의 배경이 되는 Identity 관리 시스템과 관련 표준 및 기술을 소개한다. 또한, 프라이버시 보호 관련 연구 동향 및 표준 기술을 설명한다.

2.1 프라이버시

2.1.1 프라이버시 정의

프라이버시라는 용어는 주관적이고 가변적이며, 포괄적인 성격을 가지고 있어서, 시간의 흐름, 지역, 개인의 사정에 따라 그 개념이 다양하다. 원래 프라이버시라는 용어는 "사람의 눈을 피한다"라는 뜻의 라틴어 privatue에서 유래한 말이다. 프라이버시에 대한 본격적인 논의는 19세기말 개인의 사적인 일을 본인의 의사에 반하여 공개 당함으로써 발생하는 감정, 지성의 침해를 보호해야 한다는 견해가 대두되면서 시작되어 1890년 미국의 Warren과 Brandeis의 논문 "프라이버시 권리(The Right to Privacy)"에서 독립된 권리로서 주장하였다. 여기서 프라이버시 권리란 "혼자 있을 권리(Right to be let alone)"라는 개념이었다. 사생활에 대하여 타인으로부터 간섭 받지 않을 권리, 사생활의 비밀이 공개 당하지 않을 권리이다[1, 12].

정보 사회가 급속히 진행되면서 프라이버시 개념은 보다 적극적인 개념인 "자기 정보 통제권(Self-control on personal)"으로 바뀌었다. 이 개념은 개인, 집단 또는 기관이 자기에 관한 정보를 언제, 어떻게, 어느 정도 타인에게 유통시키느냐를 스스로 결정하는 권리라고 까지 파악 되었다. C. Fried 교수는 프라이버시란 단지 자기에 관한 정보가 타인에게 알려져 있지 않음을 의미하는 것이 아니라, 오히려 자기에 관한 정보를 스스로 통제할 수 있음을 의미한다고 하여 프라이버시 권리의 현대적 개념을 구체적으로 표현하였다[12].

2.1.2 프라이버시 원칙

1980년 OECD는 프라이버시 보호와 개인정보의 유통에 관한 가이드라인 8 원칙을 만들어 각국들로 하여금 이를 준수하도록 권고해 왔다. 개인 정보는 적법하고, 공정한 방법으로 필요한 경우에 당사자의 동의를 얻어서 수집해야 한다는 수집제한의 원칙(Collection Limitation), 개인 정보는 사용목적과 그 목적에 필요한 범위 안에서 정확하고, 최신의 정보가 유지되어야 한다는 데이터 정확성의 원칙(Data Quality), 개인 정보의 수집 목적은 반드시 명확하게 기술 되어야 한다는 목적 명확화 원칙(Purpose Specification), 개인 정보는 주체의 동의와 법률에 의한 경우를 제외하고, 공개되거나, 특정한 목적 이외 다른 용도로 사용되지 않도록 하는 이용 제한의 원칙(Use Limitation), 개인 정보는 불법적인 접근이나 파괴, 불법 사용, 데이터 수정, 공개 등의 위험에 대비하여 적합하게 보호되어야 한다는 정보보호의 원칙(Security Safeguards), 개인 정보를 처리하는 시스템은 자신의 개인정보에 관한 개발, 준칙, 정책

등을 일반에게 공개하도록 하는 원칙(Openness), 개인 정보의 소유자는 자신의 정보를 확인할 수 있고, 정보에 대한 접근을 통지 받을 수 있고, 상기의 요청을 거부할 수 있으며, 정당한 경우에는 자신의 정보를 삭제, 수정할 수 있는 개인 참가 원칙(Individual Participation), 정보 관리자는 상기의 원칙을 이해할 책임이 있다는 책임 원칙(Accountability)을 규정하였다.

2.2 Identity 관리 시스템

2.2.1 인터넷 Identity

인터넷의 여러 웹 사이트들은 사용자들에게 수많은 서비스를 제공하고 있다. 사용자들은 서비스를 제공받기 위하여 각 사이트에 개인 정보를 등록하고 로그인 과정을 수행한다. ID, 패스워드를 등록하고 개인의 주소, 전화번호, e-mail, 관심분야 그리고 주민등록번호까지 많은 정보를 사이트에 보관한다. 이러한 개인 정보들을 인터넷 Identity 혹은 네트워크 Identity라고 한다[3]. 각 사이트들은 개인의 Identity 정보를 불법적인 접근으로부터 안전하게 보호해야 하며, 소유자의 허가 범위 내에서만 개인정보를 사용해야 한다[2].

Identity가 독자적으로 흩어져서 관리되고 있는 현재 상황에서, 개인이 네트워크 Identity를 관리하기에는 많은 어려움이 있다. 각각의 Identity를 증명하기 위해서는 해당 사이트에 설정해둔 ID와 패스워드의 조합을 기억해야 하고, 계정마다 관리되고 있는 개인 정보를 최신의 정보로 유지해야 한다. 보통의 경우, 개인은 동일한 ID와 패스워드를 사용하거나, 혹은 여러 개의 ID, 패스워드를 사용하고 어딘가에 이 정보를 기록하는 식으로 문제를 해결하려고 한다. 하지만 이 방법들은 사용자를 번거롭게 할 뿐만 아니라, 악의적인 사용자에게 노출되기 쉬운 문제가 있다. 노출된 ID와 패스워드는 해당 사이트뿐만 아니라 사용자가 가진 모든 계정에도 악영향을 미칠 수 있다[13].

또 다른 문제는 번거로운 Identity 등록 과정이다. 사용자가 개인 정보를 손으로 일일이 입력하는 불편함이 있기 때문에, 대부분의 사용자들은 이런 입력 과정에 지쳐 있다. 그리고 자신이 가입한 계정의 Identity를 최신 상태로 유지시키는 것은 불편할 뿐만 아니라 현실적으로 불가능하다.

2.2.2 인터넷 Identity 관리 시스템

인터넷 Identity 관리는 네트워크 Identity 관리 문제점들을 해결하기 위하여 등장하였다. 네트워크 Identity를 시스템 레벨에서 관리해주기 때문에, 개인이 관리하는 부담을 없애고 현재와는 차원이 틀린 인터넷 환경을 제공해줄 수 있게 된다.

Identity 관리 시스템은 사용자, 서비스, 정보통신 기기 등 네트워크에 연결되는 개체의 Identity 속성, 신원 증명서(Credential), 정보 이용 자격(Entitlement) 등을 포함한 네트워크 Identity의 생명주기를 전체적으로 관리해주는 플랫폼 기반 구조이다. Identity 관리를 통하여 조직의 내부 통신망이나 외부 통신망으로부터 접속해오는 사용자 또는 단말기를 인증하고 해당하는 권한을 확인하며 정보 자원에 대한 적절한 접근 권한을 인가해주는 과정을 처리할 수 있게 된다. 즉, 기존의 AAA(Authentication, Authorization, Audit/ Account) 기술, P3P 기술, 패스워드 재설정 기술, 패스워드 동기화 기술, 계정관리 셀프 서비스, 관리 권한 위임, SSO, 메타 디렉터리, LDAP(Lightweight Directory Access Protocol) 등 여러 기술을 망라하여 구현된 복잡한 시스템이 바로 Identity 관리 시스템이다.

Identity 관리는 기업 내부와 계열사 전체를 관리하는 단계를 넘어서, 인터넷 차원에서 Identity 관리를 제공하려는 시도가 외국에서 진행되고 있다. 이러한 움직임은 Identity를 관리하는 방식에 따라서 크게 중앙화된 방식과 Federated 방식으로 나누어 볼 수 있다.

중앙화된 Identity 관리는 모든 기관들이 각자 보유하고 있던 Identity 관련 정보를 하나의 데이터 저장소에 집중화하는 방식이다. 모든 정보가 한곳에 있기 때문에 엄격한 모니터링 및 추적이 가능하며, 데이터의 접근, 이용, 저장, 가공, 처리 방법을 통제할 수 있다. 하지만 이 방식은 중앙 서버에 문제가 발생하면 모든 작업이 중단되는 문제를 갖고 있다.

Federated Identity 관리는 중앙화된 Identity 관리 문제를 해결하기 위하여 나온 개념이다. Federated Identity 관리 방식은 기관에게 독자적인 보안 정책들을 지원하면서, 다른 기관과는 표준화된 절차로 Identity 정보를 주고 받도록 도와준다. 네트워크에 한번 로그인하여, 여러 영역에서 관리되는 Identity를 사용한다는 생각이 들지 않도록 자연스럽게 네트워크 간을 이동하는 것이 Federated Identity 관리의 특징이다[13, 14].

2.2.3 인터넷 Identity 관리 표준 및 기술

인터넷 레벨의 Identity 관리 서비스를 제공하기

위하여 여러 단체에서 기술을 제안하고 솔루션을 만들었다. 그러한 시도는 인터넷 레벨의 Identity 관리를 위한 표준화의 필요성을 공감하도록 하였다.

대표적으로 OASIS의 SAML(Security Assertion Markup Language)은 도메인 간에 사용자 정보를 안전하게 교환하기 위해 만들어진 확장 언어로, SOAP 프로토콜을 통하여 제공된다. SAML은 보안 토큰의 형식을 정의하고, 프로파일에서는 인증, 속성 정보, 인가 정보에 관한 3가지 종류의 assertion과 이들 assertion을 사용하여 웹 SSO를 제공할 수 있는 방법을 정의하였다[6].

Liberty Alliance는 Federated 네트워크 Identity 관리와 Identity 기반의 서비스를 위한 공개 표준을 개발할 목적으로 2001년 9월에 결성되었고, 2005년 현재 150개의 멤버를 가진 조직으로 성장하였다. ID-FF(IDentity Federation Framework)는 Liberty 표준 스펙의 1 단계로서, Federated 네트워크 Identity 관리를 시작하기 위한 작업을 담당한다. 여러 기능 중에서, 신뢰 관계를 맺은 CoT(Circle of Trust) 내의 서비스 제공자들이 보유하고 있는 ID들을 연결해주고 SSO를 지원한다. 추가로 Identity 연동, Identity 제공자 알림 서비스, 익명 Identity 매핑과 글로벌 로그 아웃 서비스도 지원한다. 현재 Liberty는 ID-FF 기술을 OASIS의 SAML 2.0으로 대체하였다[3,6].

Liberty ID-WSF(IDentity Web Service Framework)는 웹 서비스 환경에서 Identity 정보 공유를 위한 표준이다. 사용자의 Identity 정보 위치를 제공해주는 디스커버리 서비스, Ideneity 정보를 공유하는 데이터 서비스, 정보 제공 시 소유자의 동의를 얻을 수 있는 인터액션 서비스 등을 지원한다[4]. ID-SIS(IDentity Service Interface Specifications)는 기업들에게 표준화된 방법을 제공하여, Identity를 기반으로 하는 서비스를 구축할 수 있도록 도와준다. ID-SIS로 작성되는 서비스는 ID-WSF 위에서 제공된다. 시범 서비스로 기본 프로파일 정보를 제공해주는 ID-Personal/Employee 프로파일 서비스가 있으며, 사용자의 등록 과정에 사용된다. 이름, 주소, 회사 주소, e-mail 같은 정보를 보유하고 있으면서, 필요할 때 해당 정보를 알려주고 다른 서비스와 상호 동작할 수 있다[5].

WS-Security는 보안 토큰을 이용한 무결성과 신뢰성을 웹 서비스 메시지(SOAP)에 적용하기 위한 메커니즘을 정의한다. 메시지의 무결성, 신뢰성, 인증을 포함하는 메시지 보호 수준을 제공하기 위한 SOAP 메시지의 활용 방안이 기술되어 있다. X.509 인증서나 Kerberos 티켓 등을 사용하여 보안 토큰들을 인코딩 할 수 있으며, 인증서의 특성들을 설명하는 확장 메커니즘이 추가되어 있다. WS-Security는 보안 토큰에 사용할 수 있는 여러 범용 기술을 제공하기 때문에, 다양한 종류의 보안 모델과 암호화 기술에 적용될 수 있다.

2.3 프라이버시 보호 관련 연구

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 프라이버시 강화 기술, 기업 시스템들에서의 PIM, 다양하고 신뢰할 수 있는 신원 관리, 적법한 PIM 이슈들, 사회 경제적인 PIM 이슈들 등 5개의 세부적인 PIM 테마들로 연구되었다.

PRIME(PRivacy and Identity Management for Europe) 프로젝트는 유럽의 주요한 연구단체들을 중심으로 W3C 등 주요 표준화 기관과 연계된 개인의 프라이버시 보호를 위한 프로젝트이다. 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 Identity 관리에 초점을 맞추고 Identity 관리의 프라이버시를 위한 프레임워크를 제안하기 위해 2004년에 시작해서 향후 4년 동안 5단계로 나누어 프로젝트를 수행하고 있다.

P3P(Platform for Privacy Preference Project)는 W3C(World Wide Web Consortium)에서 개발한 프라이버시 보호 표준기술 플랫폼으로서 웹사이트에서 이루어지는 데이터 처리에 관한 일련의 표준을 제시하고 있다. 웹브라우저나 다른 사용자 도구를 이용하여 자동적으로 해당 웹사이트의 프라이버시에 관한 정보를 읽고 사용자가 이미 설정해 놓은 정보 공개 수준과 비교하여 정보를 선별적으로 제공하는 것을 목표로 한다[8].

XML 기반 접근제어 기술은 OASIS에서 표준화가 진행되고 있으며, 현재 XACML V2.0에 대한 표준화가 진행되고 있는 상태이다. 그 밖에 XACML (eXtensible Access Control Markup Language)과

관련된 여러 프로파일들도 표준화가 진행되고 있다[7]. XACML은 XML 정보보호기술 중의 하나로써 자원들 혹은 접근 요청 개체들에 권한부여(authorization)를 통해 자원들에 대한 접근 제어(access control)를 하는 XML 기반의 언어이다. 또한, 다양한 접근제어 제품들에게 일관되게 적용될 수 있는 권한부여 정책들을 위한 통합 언어를 제공함으로써 광범위한 관리 및 권한부여 제품들에게 상호 운영성을 제공한다.

IBM과 ZKS(Zero Knowledge Systems)는 프라이버시 인가 기술을 개발하기 위하여 서로 협약을 맺고 ZKS의 PRML(Privacy Rights Markup Language)을 공유하여 XML 기반 기업용 프라이버시 기술 규격인 EPML(Enterprise Privacy Markup Language)을 개발하였다. 후에 IBM은 EPML을 기반으로 하여 EPAL(Enterprise Privacy Authorization Language)를 개발하였고 현재는 W3C에 등록되어 있다. EPAL은 프라이버시와 관련된 데이터를 다루는 정책 및 준칙 등을 표현하는 언어를 제공한다[9].

Ⅲ. 프라이버시 인가 및 정책

인터넷 Identity 관리 시스템에서 개인정보 보호를 위한 방법은 다양하게 존재한다. 사용자의 Identity 정보를 안전하게 보관하는 방법, Identity 정보 수집 시 사용자에게 사용 목적을 명시하는 방법, 사용자가 자신의 정보를 최신의 상태로 유지할 수 있게 지원하는 방법 등이 있다. 본 논문은 이러한 방법들 중에서 프라이버시 인가에 관한 것이다. 프라이버시 인가란 개인 정보에 대한 접근이 발생하였을 때, 사용자가 정해 놓은 규칙과 정보 관리자의 정책에 따라 접근 허가를 판단하고, 필요시에는 사용자의 동의를 구하는 기술이다. 본 장에서는 프라이버시 인가를 설명하고 인터넷 Identity 관리 시스템에서의 개인정보 유통에 대하여 살펴본다. 그리고 개인정보를 제어하는 주체를 구분하고 각각의 제어 방법을 제시한다.

3.1 프라이버시 인가

프라이버시 인가는 개인 정보에 대한 접근을 사용자의 규칙과 정보 관리자의 정책에 따라 제어하는 것이다. 특정 주체의 특정 자원에 대한 특정 행위를 제어한다는 특징은 접근 제어와 유사하다고 볼 수 있다. 하지만, 프라이버시 인가는 특정 자원이 개인정보에 국한된다는 점과 자원에 대한 접근 허가 판단을 개인 정보의 소유자가 직접 제어할 수 있다는 점에서 다른 기술이라고 할 수 있다[10, 11].

앞에서 언급하였듯이, XACML은 접근 제어를 위해 생성된 XML 기반 언어이다. 그러나, 최근에 제안된 XACML 2.0은 프라이버시 보호를 위한 부분이 추가 되었고, 기업 내부 고객의 프라이버시 보호를 위해 생성된 EPAL과 흡사한 기능을 많은 부분에서 엿볼 수 있다. 두 언어를 기준으로 하여 인가와 개인정보와의 차이점을 살펴보면 다음과 같다. 정보 요청자가 요청 메시지를 생성할 때, 정보 사용의 목적(Purpose)을 표현할 수 있다는 점, 정보 제공자가 정보 제공 시, 그 사용에 대한 제약사항을 명시할 수 있다는 점, 그리고, 모든 정보가 개인 정보에 한정을 두고 있다는 점 등이다.

3.2 인터넷 Identity 관리 시스템에서의 개인정보 유통

Liberty Alliance 표준을 수용하는 인터넷 환경의 Identity 관리 시스템은 다음과 같은 구성 요소로 이루어진다[2].

- Principal - 인터넷을 이용하는 사용자이다. Identity Provider로부터 Federated Identity를 보유하고 있고, 인터넷 SSO를 위하여 Identity Provider를 통한 인증 과정을 거친다. 개인 정보는 Identity Provider에 저장한다.
- Service Provider(SP) - Principal에게 서비스를 제공하는 개체이다. 사용자가 서비스를 요청하면, Identity Provider에게 사용자의 인증 확인을 요청한다. 사용자가 요청한 서비스를 제공하기 위해 사용자의 정보가 필요하게 되면, Attribute Provider에게 정보를 요청한다. 이때, 획득하려는 정보가 무엇인지, 획득한 정보는 어떻게 사용할 것인지에 대하여 사용자에게 통지하여야 한다.
- Identity Provider(IdP) - 사용자의 Identity 정보를 생성하고 관리하는 개체이다. 사용자에게 인증 서비스를 제공한다.
- Attribute Provider - 사용자의 정보를 제공하는 개체이다. 정보의 제공은 자체 정책과 사용자의 허가에 따라 제어된다. 일반적으로, Identity Provider가 본 기능을 겸한다.
- Discovery Service - 특정 사용자의 정보를 어느 Attribute Provider가 관리하고 제공하는지

알려주는 개체이다.

Liberty Alliance의 구성 요소에서 IdP와 Attribute Provider는 독립적으로 구분되어 있다. 두 Provider는 기능상의 특징으로 보면 다소 다른 기능을 수행하지만, Principal의 Identity 정보를 관리한다는 측면은 서로 같다. 기능적인 측면에 따라 두 Provider가 독립적인 서버 형태로 구성되더라도, 개인정보의 소유자인 Principal에게는 단일 인터페이스로 자신의 정보를 관리할 수 있게 하여야 한다. 또한, Attribute Provider는 Principal에게 노출되지 않는 것이 좋다. 본 연구에서는 IdP가 Attribute Provider의 기능을 포함하는 하나의 시스템으로 가정한다. Discovery Service는 사용자 정보의 위치를 알려주는 서비스로 독립적인 서버 형태로 존재하거나 IdP의 서비스 모듈이 될 수 있다.

인터넷 Identity 관리 시스템에서 개인정보가 유통되는 간단한 시나리오를 생각해 보자. Airline은 사용자에게 항공 관련 서비스를 제공하는 회사이고, 사용자에게 SSO 서비스를 제공하는 IdP이다. 그리고, 사용자의 개인정보인 이름, 주소, 자주 사용하는 항공편 정보 등을 저장 관리하고 있으며, Discovery Service를 제공한다. Hotel은 Airline과 Identity가 연계되어 있으며 호텔 예약 서비스를 제공한다. Bank는 Hotel, Airline과 Identity가 연계되어 있으며 은행 업무 서비스를 제공한다. 그리고, Bank는 사용자의 전자 지갑, 계좌번호, 신용카드 정보 등을 관리하며, Airline의 Discovery Server에게 자신이 관리하는 사용자의 정보가 무엇인지 통지한다[2].

사용자는 Airline 홈페이지에 로그인한 후(1), Hotel 홈페이지로 이동하여 호텔 예약을 하려고 한다(2). Hotel은 예약 서비스를 제공하기 위해 사용자의 이름, 주소, 신용카드 정보가 필요하다. Hotel은 Airline에 이 정보들을 요청한다(3). Airline은 사용자의 규칙(preference)과 프라이버시 정책에 따라 정보 제공이 허가되는지 판단을 하고, 허가된다면 Hotel에게 사용자의 이름과 주소 정보를 제공한다(4). 신용카드 정보는 Bank가 제공하고 있음을 Hotel에게 알려준다(5). Hotel은 Bank에게 신용카드 정보를 요청한다(6). Bank는 사용자의 규칙과 프라이버시 정책에 따라 정보 제공이 허가되는지 판단을 하고, 허가된다면 Hotel에게 사용자의 신용카드 정보를 제공한다(7). Hotel은 획득한 정보가 무엇이며 어떤 용도만으로 사용할 것인지를 사용자에게 통지한 후, 호텔 예약 서비스를 제공한다.

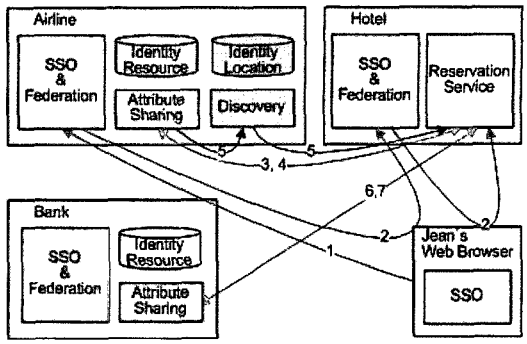

그림 1. 인터넷 Identity 관리 시스템에서의 개인정보 유통

이러한 일련의 작업들은 사용자가 전혀 모르게 진행되거나, 또는 반대로 정보 제공에 대하여 일일이 사용자의 동의를 요구할 수도 있다. 또한, Bank는 정보 획득에 앞서 서비스를 제공하기 위하여 어떠한 정보가 필요한지 사용자에게 통지를 하거나, 허가를 얻을 수 있다. 정보 획득에 대한 사용자의 허가를 assertion 형태로 획득하여, Airline과 Bank에게 정보를 요청할 때, 허가 assertion을 제공하는 방법도 있다.

위 시나리오에서는 각 IdP에 저장되어 있는 사용자의 규칙과 프라이버시 정책을 기준으로 정보 제공 여부를 판단한다. Liberty Alliance에서는 프라이버시 정책을 생성하고 판단하는 개체를 독립적으로 표현하지 않지만, 본 논문에서는 이를 Privacy Controller라고 표현한다.

- Privacy Controller - 개인정보 보호 정책을 설정하고 관리하며, 정보 유통에 대한 판단을 내리는 개체이다.

Identity 관리 시스템에 Privacy Controller가 배치될 수 있는 형태는 개인정보 정책의 속성 및 개인정보 정책 도메인 관점에 따라 다양한 형태로 구성될 수 있다. 자세한 사항은 4장에서 다룬다.

3.3 프라이버시 제어 주체 및 방법

3.3.1 제어 주체

인터넷 Identity 관리 시스템에서 개인정보를 제어할 수 있는 주체는 개인 정보의 소유자와 개인정보를 관리하는 시스템이다. 직관적으로 개인 정보의 모든 권한은 소유자에게 있으므로 개인정보의 유통은 소유자의 의지대로 수행되어야 한다. 그러나, 인터넷 사용자들은 대부분 프라이버시에 대한 문제는 어느 정도 인식하고 있지만, 실제로 자신의 정보

가 어떠한 위협에 놓여 있으며 자신의 정보를 어떻게 관리하여야 하는 가에 대한 것은 사용자에게는 귀찮고 어려운 문제로 다가선다. 인터넷 Identity 관리 시스템은 이러한 사용자들이 자신의 정보를 관리할 수 있도록 직관적이고 편리한 인터페이스를 제공하여야 한다. 또한, 자신의 정보를 적절히 관리하지 못하는 사용자들을 위하여, 소유자의 직접적인 제어 외에 관리 시스템 입장에서 개인 정보를 제어할 수 있는 방법이 필요하다.

관리 시스템의 프라이버시 방법의 필요성을 정리하면 다음과 같다. 첫째, 사용자에게 편의를 제공하여야 한다. 사용자가 자신의 정보를 관리할 수 있는 예제를 제시하거나, 자신의 정보를 관리하지 않는 사용자를 대신할 수 있는 방법이 필요하다. 둘째, 사용자가 정보를 관리하더라도 스스로 예측하지 못하는 문제가 발생할 수 있으므로 이를 방지할 수 있는 방법이 필요하다. 셋째, 정보 공유 주체간의 협약 관계, 정보 사용의 다양한 목적 및 이에 따른 협상, 그리고 정보 사용의 제한 사항 등과 같은 문제는 개인정보의 소유자가 직접 제어하기는 무리가 따른다. 넷째, 개인정보에는 소유자가 직접 생성한 정보 외에 다른 정보들이 존재한다. 예를 들면, 고객이 자주 사용하는 교통편 정보, 학교에서 관리하는 학생의 성적과 같은 정보이다. 분명 소유자의 정보임에는 틀림없지만, 소유자 마음대로 변경하거나 삭제할 수 없는 정보이다. 이러한 정보들을 관리할 수 있는 방법이 필요하다.

3.3.2 제어 방법

개인정보를 제어하는 방법은 다양하게 존재한다. 접근 제어에서 주로 사용되는 ACL(Access Control List), RBAC(Role-based Access Control)을 사용하는 방법, 프라이버시에 어느 정도 특화되어 있는 XACML, EPAL을 사용하는 방법 등이 있다. 그리고, 미리 정의해 놓은 규칙 및 정책에 의해 정보를 제어하는 방법이 아닌, 개인정보 접근이 발생하는 시점에 소유자의 허락을 얻는 방법이 있다. 이러한 제어 방법들은 사용되는 환경에 따라 적절하게 선택 또는 취합하여 사용된다. 앞 절에서 언급한 개인정보 제어 주체에 따라 프라이버시 제어 방법을 구분하고 각 특징에 대하여 설명하도록 한다.

우선, 소유자 중심의 제어 방법은 무엇보다도 편의성에 초점을 맞추어야 한다. 소유자가 직관적으로 이해할 수 있게 하여야 하고, 제어 규칙을 생성하는데 적은 시간을 소요하도록 해야 한다. 이를 위한 첫 번째 방법은 개인 정보의 속성에 따라 각 항목별로 제어하도록 하는 것이다. 예를 들어, 주민번호와 같은 정보는 정보 공유를 못하게 하고, e-mail 또는 주소와 같은 정보는 정보 공유를 허용한다. 소유자는 각 항목 별로 중요도를 판단하고 제어할 수 있게 한다.

두 번째 방법은 개인정보를 요청하는 주체에 따라 제어한다. 예를 들면, 국가 기관, 금융 기관과 같은 주체에게는 정보 공유를 허용하고, 쇼핑몰 또는 개인 등에게는 정보 공유를 금지한다. 즉, 정보 사용 주체의 신뢰 정도에 따라 정보 공유를 제어한다. 각각의 주체 별로 제어할 수도 있지만, 소유자에게 편의성을 제공하기 위해 주체들을 그룹화하여 제어하는 방법도 가능하다. 이 두 방법은 같이 사용될 수 있다. 이러한 방법을 어려워하는 소유자를 위해서는 이미 정의되어 있는 정책을 적절하게 조합하여, 개인정보 보호 수준 낮음, 보통, 높음 등의 세팅을 구성하고 소유자에게 간단히 선택하게 할 수도 있다. 이와 반대로 고급 사용자를 위해 정보 사용의 목적, 사용의 제한과 같은 정밀한 부분도 제어할 수 있게 한다.

관리자 중심의 제어 방법에서는 각각의 소유자 정책 보다는 시스템 전체적인 관점에서 발생할 수 있는 문제를 대비하여야 한다. 또한, 사용자가 자신의 정보를 정밀하게 관리하지 못함을 염두에 두어야 한다. 그러므로, 보다 정교하게 제어할 수 있는 방법이 요구된다. 그리고, 인터넷 Identity 관리 시스템이 자신의 도메인을 벗어나 타 도메인과의 정보 유통이 가능 하려면, 프라이버시 정책이 상호간에 교환되고 상대 도메인의 정책을 시스템에 적용시킬 수 있어야 한다. 이를 위해서 관리자 중심 제어 방법은 표준을 따르는 것이 바람직하다. 이러한 요구사항을 만족하기 위해서 관리자 중심의 제어 방법은 XACML, EPAL과 같은 프라이버시 정책 언어를 사용하는 것이 바람직하다.

프라이버시 정책 표현 언어는 아래와 같이 대상(Target), 규칙(Rule), 정책(Policy)으로 이루어져 있다.

특정 주체의 특정 자원에 대한 특정 행위를 대상이라고 한다. 대상은 주체, 자원, 행위로 구성된 집합이다. (s, r, a)로 표현한다. 여기서, 주체를 표현하는 방법에 있어, 행위를 하고자 하는 실체를 직접 표현하거나, RBAC과 같은 기법을 이용하여 역할(Role)로 표현할 수 있다.

Target T = {(s, r, a)|s∈Subject,

$r \in Resource,\ a \in Action\}$

$Rule\ R = \{(T,\ c,\ p,\ e) | c \in Condition,$

$p \in Purpose,\ e \in Effect\}$

$Policy\ P = \{(R,\ o) | o \in Obligation\}$

규칙이란 대상에 목적(Purpose), 조건(Condition), 판단(Effect) 등을 추가한 것이다. 목적은 대상을 수행하고자 하는 주체의 사용 목적을 표현하고, 조건은 대상이 성립되거나 발생하는 데 갖추어야 하는 요소를 말한다. 판단은 규칙에 대한 허가, 거부를 말한다. 정책은 하나 이상의 규칙으로 이루어지고, 정보 사용시 반드시 지켜야 할 의무사항(Obligation)이 추가되어 있다.

개인정보 제어 방법은 미리 정의해 놓은 정책에 따라 정보의 접근을 제어하는 방법 외에, 개인정보 접근이 발생하는 시점에 소유자의 허락을 얻는 방법이 있다. 이 방법은, 소유자가 접근에 대하여 직접 판단할 수 있다는 장점이 있다. 문제 발생시 책임 소재 또한 명확하다. 하지만, 너무 잦은 질의는 소유자에게 부담으로 다가오며, 소유자의 부담은 잘못된 판단으로 이끌 여지를 갖고 있다. 이를 해결하기 위한 방법으로는 개인정보 접근이 발생할 때마다, 질의를 하는 것이 아니라 소유자가 로그온 상태인 경우에만 질의가 이루어지게 하거나, 실시간 질의는 아니지만 사용자의 e-mail 등을 이용하여 질의하도록 한다. 또는 3.2절의 시나리오처럼 소유자가 요청한 작업에 의해 개인정보 접근이 발생할 때에만 질의가 이루어지도록 한다면, 소유자의 질의에 따른 부담을 줄일 수 있다.

Ⅳ. 프라이버시 인가 모델

본 장에서는 인터넷 Identity 관리 시스템에서 프라이버시 인가 서비스를 제공하기 위한 다양한 모델을 제시하고 설명한다. 그림 2는 프라이버시 인가 서비스를 추상화된 개체로 표현하고 있다. 정보 요청자(Data Requester)는 개인정보를 요청하는 개체로 개인정보를 보관하고 있는 정보 제공자(Data Provider, PEP: Policy Enforcement Point)를 찾기 위하여 Discovery Service를 이용한다. 정보 요청자로부터 개인정보를 요청 받은 정보 제공자는 정보제공에 대한 허가를 PDP(Policy Decision Point)에게 질의한다. PDP는 개인정보 소유자 정책(Owner Policy)과 개인정보 관리 정책(Mgt Policy)에 따라 질의를 판단하고 정보 제공자에게 그 결정을 통보한다. 결정이 허가이면, 정보 제공자는 정보 요청자에게 개인정보와 정보 사용에 대한 제한사항을 전달하고, 결정이 금지이면 거부되었다는 메시지를 전달한다. 결정에서 정보 소유자의 동의를 요구한다면 정보 제공자는 정보 제공의 대한 허가를 정보 소유자에게 질의한다. PAP(Policy Administration Point)는 소유자 정책과 관리 정책을 설정하고 관리한다.

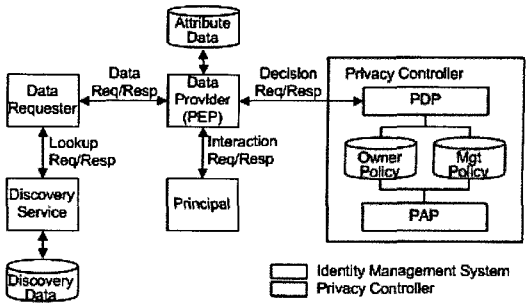

그림 2. 프라이버시 인가 개체

프라이버시 인가 서비스를 위한 개체들이 인터넷 Identity 관리 시스템에서 배치될 수 있는 모든 형태를 살펴보고 각각의 특징을 설명한다. 개인정보의 주체에 따른 모델의 특징, 프라이버시 도메인의 확장, PEP, PDP, PAP의 위치, 독립적인 Privacy Controller 등에 대하여 자세히 살펴본다.

4.1 개인정보 소유자 정책 모델

개인정보 소유자의 정책을 관리하는 모델이다. 우선, 개인정보 소유자가 자신의 정보를 저장할 때, 즉 IdP에서 사이트 등록과정을 거칠 때, 자신의 정보가 어떤 방식으로 저장되고 관리되는지 통보 받는다. 그리고, 소유자는 자신의 정보 노출에 대한 방침을 설정한다. 설정할 수 있는 인터페이스는 IdP로부터 제공 받는다. 정책은 개인정보 항목 및 정보 요청 주체로 구분하여 설정한다. 필요에 따라 소유자 자신에게 질의하도록 설정한다.

그림 3은 개인정보 소유자 정책 모델이다. 3장에서의 시나리오처럼 SP는 IdP에게 사용자의 정보를 요청하고 IdP는 사용자가 정의해 놓은 정책에 따라 정보를 제공한다. 정책에 따라 소유자에게 정보 제공에 대한 동의를 얻을 수 있다. 그림에서 PAP는 표현되어 있지 않으나 IdP는 사용자에게 정책을 관리할 수 있는 인터페이스를 제공한다.

소유자는 자신의 정보를 금지, 질의, 허용, 이렇게 세 단계로 구분하여 통제한다. 금지는 자신의 정보를 제공하지 않음을 의미하고, 질의는 정보 요청시 소유자에게 질의하도록 하는 것이며, 허용은 정

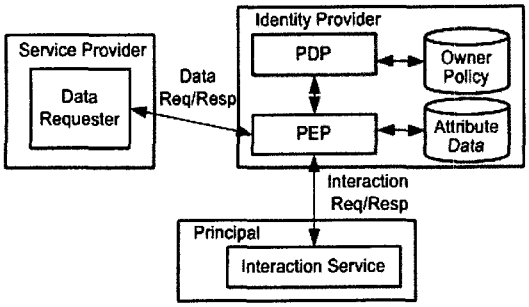

그림 3. 소유자 정책 모델

보를 제공함을 말한다. 개인정보 각 필드마다 금지, 질의, 허용 중 하나를 선택하게 한다. 예를 들어, 주민번호는 금지, 집주소는 질의, 취미사항은 허용 등이다. 그리고, 개인정보를 요청하는 대상에 따라 통제 방법을 다르게 정의할 수 있다. 예를 들어, 정보 요청 대상이 금융기관일 경우에는 주민번호, 집주소는 허용, 대상이 쇼핑몰일 경우에는 주민번호는 금지, 집주소는 질의 등 이와 같이 다양한 통제 방법이 가능하다. 그리고, 보다 정밀하게 제어하게는 사용의 목적에 따른 통제, 정보 사용에 대한 제한 등을 추가할 수 있다.

이와 같이 소유자가 자신의 정보를 자세하게 통제할 수 있지만, 사용자의 프라이버시에 대한 지식 수준과 편의성을 제공하기 위해서는 앞에서 설명한 세세한 부분을 적절하게 통합하여 간단하게 통제할 수 있는 방안을 마련해 두어야 한다.

4.2 개인정보 관리 정책 모델

개인정보 관리 정책은 소유자가 자신의 정보를 관리하지 않더라도 개인정보가 안전하게 관리될 수 있도록 해야 한다. 또한, 관리 정책은 반드시 소유자에게 통지되어야 한다. 기본적으로 관리 정책은 소유자의 의도보다 강하게 통제되거나 소유자에게 질의하는 방식으로 구성되어야 한다.

Identity 관리 시스템은 CoT라는 신뢰 도메인 개념을 가지고 있다. CoT는 다수의 SP와 IdP로 구성된 도메인으로, 각자 관리되고 있는 사용자의 ID들을 연계하여 SSO 서비스를 제공한다. 이는 사업자들의 협약에 의해 이루어진 추상적인 신뢰 관계이다. 이외에 IdP 도메인이란 개념이 있다. IdP 도메인이란 하나의 IdP와 다수의 SP로 구성된다. IdP는 사용자에게 SSO 서비스를 제공하고, 사용자의 개인정보를 저장하고 관리한다. 이 또한 사업자들의 협약에 의해 이루어지며, 하나의 작은 CoT로 보아도 무방하다.

Identity 관리 시스템에 개인정보 보호를 제공하는 본 연구에서는 프라이버시 도메인이라는 개념을 도입한다. 프라이버시 도메인이란 일관된 프라이버시 정책으로 개인정보가 관리되는 영역을 의미한다. 크게는 여러 사업자들이 단일한 프라이버시 정책을 구성하여 개인정보를 관리한다. 이 경우에는 도메인 내에 정책을 설정하고 정보 요청에 대한 결정을 내릴 수 있는 중앙 집중적인 Privacy Controller가 필요하다. 이와는 다르게, 개인정보를 관리하고 프라이버시 정책을 설정하고 판단하는 모든 작업이 하나의 IdP에서 수행되는, 작은 규모의 프라이버시 도메인 또한 존재할 수 있다.

프라이버시 도메인과 IdP 도메인에 따른 개인정보 모델을 정의하고 각각의 특징을 설명한다.

4.2.1 단일 프라이버시 도메인

단일 프라이버시 도메인에서는 하나의 프라이버시 정책을 책정하고 이에 따라 도메인 내의 모든 개인정보 유통이 제어된다. 사용자는 IdP에 가입을 하면서 자신의 정보를 등록한다. 등록된 정보는 도메인 프라이버시 정책에 따라 제어된다. 사용자가 직접 입력하지 않았음에도 생성되는 개인정보, 즉 사이트 방문 횟수, 자주 사용하는 항공편과 같은 정보들이 있다. 이 정보들은 사용자가 의식하지 못하는 상태에서 생성되기도 하고, 생성된 정보가 사용자의 소유임에도 불구하고 자신이 직접 변경하지 못한다. 이러한 정보들은 도메인 내의 일관된 관리 정책으로 안전하게 제어하여야 한다.

그림 4는 하나의 IdP 도메인과 하나의 프라이버시 도메인에 적합한 모델이다. SP가 IdP에게 정보를 요청하고 IdP는 정보 유통에 대한 결정을 Privacy Controller가 질의한다. Privacy Controller는 질의에 대한 결정을 내리며, 도메인 내의 프라이버시 관리 정책을 설정하고 관리한다. 그림에는 표

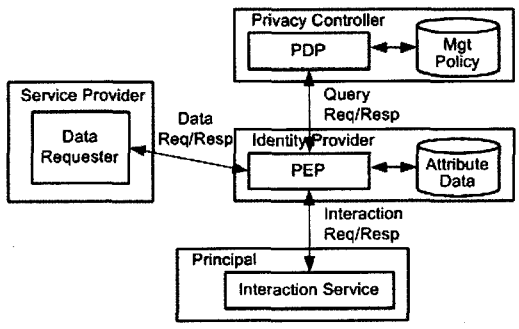

그림 4. 단일 프라이버시 도메인/단일 IdP 도메인

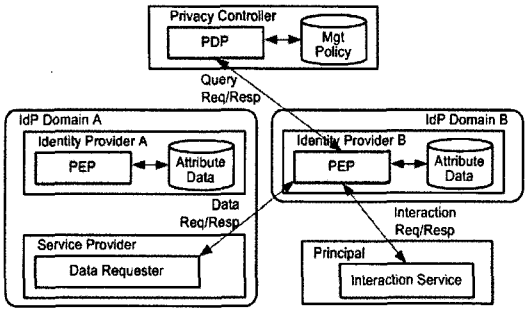

그림 5. 단일 프라이버시 도메인/다수의 IdP 도메인

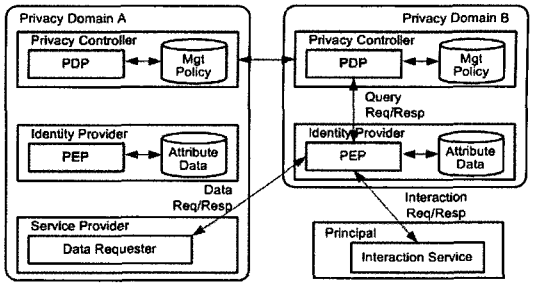

그림 6. 다수의 프라이버시 도메인

현되어 있지 않지만, SP에도 개인 정보가 저장되어 있을 수 있으며 이 정보에 대한 제어도 Privacy Controller가 수행한다.

그림 5는 하나의 프라이버시 도메인 내에 다수의 IdP 도메인이 포함된 모델을 표현한다. IdP 도메인 A의 SP가 도메인 B의 IdP에게 정보를 요청하고, IdP는 정보 유통에 대한 결정을 Privacy Controller에게 질의한다. Privacy Controller는 도메인 내의 모든 개인정보들에 대한 유통을 제어한다. IdP 도메인간에 개인정보 유통에 관한 협약, 프라이버시 인가 정책 등이 하나의 규칙으로 정의되고 중앙집중적으로 관리된다면, 앞에서 설명한 단일 프라이버시 도메인과 단일 IdP 도메인 모델과 같은 개념이다.

앞서 설명한 모델에서 Privacy Controller는 두 가지 일을 수행한다. 프라이버시 정책을 설정하는 PAP 작업과 정보 사용에 대한 요청에 대하여 결정을 내리는 PDP 작업을 수행한다. 그림 5와 같이 다수의 PEP가 하나의 Privacy Controller에게 결정을 요청하는 환경에서는 병목 현상이 발생할 수 있다. 이를 해결하기 위해서 Privacy Controller는 PAP 작업만 수행하고 생성된 프라이버시 정책과 PDP는 PEP로 내려 보낸다. Privacy Controller는 새로이 정책이 설정될 때마다 PDP로 전송하여야 한다. 이 방법은 병목 현상은 제거할 수 있지만, 정책이 여러 곳으로 분산되므로 저장 공간의 낭비를 초래하고 최신 정책 유지를 위한 오버헤드가 발생한다.

4.2.2 다중 프라이버시 도메인

인터넷 규모의 Identity 관리 시스템에서는 하나의 프라이버시 도메인을 벗어나 타 도메인의 개인정보를 요청하는 경우가 발생한다. 그림 6에서 프라이버시 도메인 A의 SP가 도메인 B의 IdP에게 정보를 요청하고, IdP는 도메인 B의 Privacy Controller에게 질의한다. Privacy Controller는 도메인 B의 프라이버시 정책으로 질의를 판단한다. 여기서 해결해야 하는 문제는 도메인 B의 프라이버시 정책으로 도메인 A의 SP를 어떻게 인식하는 가이다.

Privacy Controller는 상대 도메인의 개체들을 자신의 프라이버시 정책의 주체들로 인식할 수 있는 주체 매핑 테이블(Subject Mapping Table)을 사용한다. 매핑 테이블은 양쪽 도메인 간에 프라이버시 정책 협약 시에 생성한다. 매핑 테이블은 도메인간에 주체를 직접 사상하는 방법과 중간 매체를 두어 사상하는 방법이 있다. 주체 매핑 테이블 방법 외에 상호간에 프라이버시 정책을 통합할 수 있는 방안도 있다. 이는 곧 하나의 프라이버시 도메인으로 간주할 수 있다.

다중 프라이버시 도메인에서 해결해야 하는 또 다른 문제로는 정보 사용에 대하여 제한을 두는 것이 용이하지 않다는 것이다. 프라이버시 정책에서 Obligation으로 표현되는 정보 사용의 제한은 같은 도메인에서도 해결하기 어려운데, 이것이 타 도메인의 주체에게 사용 제한을 강요하는 것은 결코 쉽지 않은 문제이다. 인터넷 규모의 개인정보 보호를 위해서는 향후 반드시 해결해야 할 문제이다.

4.3 소유자 정책과 관리 정책

앞 절에서 개인정보 소유자 정책과 관리 정책에 적합한 모델들을 설명하였다. 소유자 정책 모델에서는 개인 정보를 보관하는 시스템에 소유자 정책을 함께 저장하여 관리하고, 관리 정책 모델에서는 프라이버시 정책을 관리하고 도메인에서 발생하는 개인정보 접근에 대하여 판단을 내릴 수 있는 Privacy Controller를 이용한다. 두 정책은 서로 다른 특성을 갖고 있지만, 보다 안전한 개인정보 보호 시스템을 구축하기 위해서는 두 정책을 모두 수용할 수 있는 모델이 필요하다.

4.3.1 개별 관리

개별 관리 모델은 소유자 정책 모델과 관리 정책 모델을 단순하게 결합한 형태이다. 개별 관리 모델

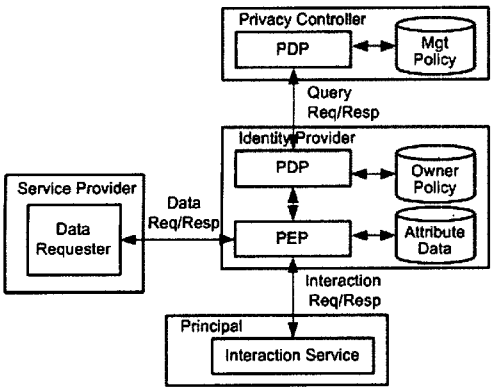

그림 7. 개별 관리

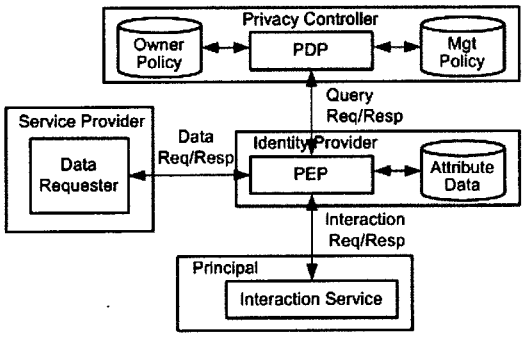

그림 8. 통합 관리

은 두 모델의 특성을 그대로 소유하고 있다. 소유자는 자신의 개인정보를 등록한 곳에서 자신의 정보를 제어하고, 타 도메인간의 관계 또는 도메인 내에 소유자가 제어할 수 없는 정보들을 보호하기 위해 Privacy Controller를 사용한다.

그림 7처럼 사용자 정책과 사용자 정책에 따른 PDP는 IdP에 위치하고, 관리 정책과 관리 정책에 따른 PDP는 Privacy Controller에 위치한다. 사용자는 Privacy Controller에 대한 인식 없이 자신의 정책만을 IdP에서 관리하면 된다.

소유자 정책과 관리 정책은 서로 상반된 결정을 내릴 수 있으므로, 이를 해결할 메커니즘이 필요하게 된다. 대부분 소유자 정책을 우선으로 하지만, 결정이 상충되는 경우에는 소유자에게 실시간 질의를 하거나, 어느 정책이 우선인가를 떠나서 접근을 거부하는 방향으로 결정을 내린다.

4.3.2 통합 관리

통합 관리는 소유자 정책과 관리 정책 모두를 Privacy Controller에서 관리하는 모델이다. 통합 관리 모델은 프라이버시에 대한 모든 부분을 Privacy Controller에 집중시킨 모델로 IdP나 SP들은 프라이버시를 지원하기 위해서는 질의/응답 프로토콜만 소유하면 된다. Privacy Controller는 사용자들이 소유자 정책을 관리할 수 있도록 인터페이스를 제공하여야 한다. Privacy Controller에 혼란과 부담을 느끼는 사용자들을 위해서, 소유자 정책 관리에 대한 인터페이스를 IdP에서 제공토록 할 수도 있다.

V. 결 론

인터넷에 산재되어 있는 Identity를 효과적으로 관리하고 인터넷을 보다 편리하게 사용할 수 있도록 해주는 인터넷 Identity 관리 서비스는 머지않아 사용자들과 대면할 것이다. 그때는 현재 인터넷에서 발생하고 있는 개인정보 유출 및 오남용에 따른 문제들이 발생하지 않도록 인터넷 Identity 관리 시스템에서 개인정보를 안전하게 관리하고 유통할 수 있는 방법과 모델이 필요하다.

본 논문은 사용자의 개인정보를 안전하게 관리하기 위한 수많은 방법 중 개인정보에 대한 접근이 발생하였을 때, 사용자 및 관리 주체가 정의해 놓은 프라이버시 정책에 따라 접근 허가를 판단하고, 필요시에는 사용자의 동의를 구하는 프라이버시 인가에 관한 것이다. 사용자의 개인정보를 제어하는 정책은, 개인정보의 실소유자가 참여하여 자신의 정보를 제어하는 소유자 정책과 관리 입장에서 개인정보에 따른 문제를 해결하기 위한 관리 정책으로 구분하였다. 그리고 각 정책에 따른 제어 방법을 설명하고 이를 인터넷 Identity 관리 시스템에 적용하기 위한 모델을 제시하고 각각의 특징을 설명하였다.

본 논문에서 제안하고 있는 프라이버시 모델은 인터넷 Identity 관리 시스템뿐만 아니라, 환자의 병력정보와 같이 민감한 개인정보를 다루는 의료정보 시스템, 개인정보를 바탕으로 온라인 행정서비스를 제공하는 전자정부 시스템과 같은 환경에 적용될 수 있다.

향후, 개인정보를 얻은 주체가 정보사용에 대한 제약 사항을 지키도록 하기 위한 메커니즘 및 유비쿼터스 환경에서의 프라이버시 문제를 해결할 수 있는 모델에 관한 연구가 필요하다.

참 고 문 헌

[1] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*, 1980.

[2] Liberty Alliance Project, *Privacy and Security Best Practices*, Nov. 2003.
[3] Liberty Alliance Project, *Liberty ID-FF Architecture Overview*, Nov. 2003.
[4] Liberty Alliance Project, *Liberty ID-WSF Web Services Framework Overview*, 2003.
[5] Liberty Alliance Project, *Liberty ID-SIS Personal Profile Service Specification*, 2003.
[6] OASIS, *Assertion and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*, 2005.
[7] OASIS, *eXtensible Access Control Markup Language(XACML) Version 2.0*, Committee draft 04, 2004.
[8] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall, and J. Reagle, *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, W3C 2002.
[9] P. Ashley, S. Hada, G. Karjoth, M. Schunter, *Enterprise Privacy Authorization Language (EPAL 1.2)*, W3C, 2003.
[10] G.Karjoth, M.Schunter, and M.Waidner, "Platform for Enterprise Privacy Practices: Privacy-enbaled Management of Customer Data," *LNCS 2482*, 2002.
[11] P. Ashley, "Authorization For A Large Heterogeneous Multi-Domain System," *Australian Unix and Open Systems Group National Conference*, 1997.
[12] 류종현, "사이버공간에서의 프라이버시 침해에 관한 사례연구," *코리아크립토*, 2002.
[13] 김승현, 진승헌, 정교일, "인터넷 ID 관리 서비스 기술 동향," *주간기술동향*, 2004.
[14] 최대선, 조상래, 김승현, 진승헌, 정교일, "인터넷 ID 관리 서비스," *정보보호학회지*, 제 14권 5호, 2004.

노 종 혁(Jong-Hyuk Roh) 정회원

1996년 2월 인하대학교 전자계산공학과 졸업
1998년 2월 인하대학교 전자계산공학과 석사
1998년~현재 인하대학교 컴퓨터정보공학과 박사과정
2000년 12월~현재 한국전자통신연구원 정보보호연구단 디지털ID보안연구팀 선임연구원
<관심분야> 정보보호(프라이버시, PKI), 컴퓨터네트워크, 네트워크 보안

진 승 헌(Seunghun Jin) 정회원

1993년 2월 숭실대학교 전자계산공학과 졸업
1995년 2월 숭실대학교 전자계산공학과 석사
2004년 2월 충남대학교 컴퓨터과학과 박사
1994년 12월~1996년 4월 대우통신 종합연구소
1996년 5월~1999년 5월 삼성전자 통신연구소
1999년 6월~현재 한국전자통신연구원 정보보호연구단 디지털ID보안연구팀장/선임연구원
<관심분야> 컴퓨터/네트워크 보안, 정보보호(PKI), Digital Identity Management

이 균 하(Kyoon-Ha Lee) 종신회원

1970년 인하대학교 전기공학과 졸업
1976년 인하대학교 전자공학과 석사
1981년 인하대학교 전자공학과 박사
1977년~1981년 광운대학교 교수
1981년~현재 인하대학교 컴퓨터정보공학과 교수
<관심분야> 지능통신망, 이동통신, 패턴인식