ID관리시스템의 접근통제기반 프라이버시 보안모델☆

An Access Control Based Privacy Protection Model in ID Management System

최 향 창* 노 봉 남** 이 형 효***
Hyang-Chang Choi Bong-Nam Noh Hyung-Hyo Lee

요 약

사용자의 개인정보를 통합 관리하는 ID관리시스템에서 프라이버시 문제는 일반 사용자들에게 매우 주요한 관심사이다. 따라서 ID관리 환경에서 개인의 프라이버시가 보호되지 않는다면 ID관리시스템의 활용도는 낮아질 수밖에 없다. 본 논문에서는 단일 COT(Circle of Trust)안에서 프라이버시 정책을 이용하여 개인프라이버시를 보호하는 접근통제기반의 프라이버시 보안모델을 제안한다. 또한 프라이버시 보안모델 구성요소와 특성들을 정형적으로 기술하고, 프라이버시 보안 아키텍처와 프라이버시 정책들을 위한 XML기반의 스키마를 보인다.

Abstract

The vulnerability of privacy in the Identity Management System (IMS) is the most pressing concern of ordinary users. Uncertainty about privacy keeps many users away from utilization of IMS. Therefore, this paper proposes an access-control oriented privacy model for IMS. The proposed model protects privacy using access control techniques with privacy policies in a single circle of trust. We address characteristics of the components of for the proposed model and describe access control procedures. After that, we show the architecture of privacy enforcement and XML-based schema for privacy policies.

☞ Keyword : privacy protection model, ID management system, access control model

1. 서 론

ID관리 기술은 디지털식별(digital identity) 데이터들을 효율적으로 관리하기 위한 원천 메커니즘(mechanism)을 연구하고 개발한다[1]. 이것은 디지털식별들을 관리함으로 이와 연루된 제반 문제에 대한 안전한 보장을 위해 인증(authentication), 인가(authorization), 프라이버시(privacy) 보호 기술 등을 요구한다. 프라이버시 보호 기술은 현재까지 미약하며 확실한 기술적 대안이 존재하지 않고 있어 매우 심각한 문제로 남고 있다[4,5]. 더욱이 정보통신기술의 발전과 유비쿼터스(ubiquitous) 컴퓨팅 환경이 도래하고 표준화된 웹(web) 지원 서비스 플랫폼, 시만텍(semantic) 웹과 결부된 정보검색 서비스 등 새로운 형태의 서비스가 창출됨에 따라 서비스를 위해 공유해야 할 디지털식별(digital identity) 데이터가 증가되어 개인의 정보시스템 의존도와 개인의 프라이버시 보호 욕구가 지속적으로 증가되고 있다. 이와 비슷한 이유로 프라이버시 보호가 정보시스템의 개인 참여율에 영향을 미칠 수 있다고 여러 연구기관에 의해 조사된바 있다[4,13]. 이러한 중요성을 인식하고 현재에는 여러 프라이버시 보호 프로젝트가 수행 중이다. 그 중 ID관리 시스템을 위한 주요한 프라이버시 보호 프로젝트는 RAPID와 PRIME을 중심으로 프라이버

* 정 회 원 : 전남대학교 리눅스시스템보안연구센터 연구원
hcchoi@lsrc.jnu.ac.kr(제1저자)
** 종신회원 : 전남대학교 컴퓨터정보학부 교수
bongnam@chonnam.ac.kr
*** 정 회 원 : 원광대학교 정보·전자상거래학부 교수
hlee@lsrc.jnu.ac.kr(교신저자)
[2005/03/18 투고 - 2005/04/19 심사 - 2005/10/18 심사완료]
☆ 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 육성지원 사업의 결과로 수행되었음.

시 보호 프레임워크의 개발을 목표로 연구가 진행 중이다[7,8].

기업이나 공공기관은 프라이버시 관련 법률의 권고로부터 개인의 프라이버시를 제공하기 위해서 P3P[15]나 E-P3P[19]의 기술적 대안을 제시하지만 P3P는 기업 내부에서 그 약관이 집행(enforcement)되는 실제적인 기술을 의미하지는 않는다[13]. 또한 E-P3P는 기업에 저장 유지되는 개인의 프라이버시를 위해 탄생한 기술임에도 불구하고 정보소유자가 집행해야 할 프라이버시 정책이 기업 관리자에게 위임됨으로써 각 사용자를 위한 정책보다는 기업의 측면에서 개인의 프라이버시가 제공될 수 있는 근본적인 문제점을 안고 있다[19,20]. 이러한 상황에서 개인의 프라이버시 보안을 위한 기술적 대안을 개발하기 위해서는 프라이버시 보안 모델의 개발이 요구된다.

본 논문에서는 ID관리 시스템에서 프라이버시 측면을 강화할 수 있도록 ID관리 환경에 적용 가능한 프라이버시 보안모델을 제안한다. 이는 접근제어 기술을 이용하여 개인정보 이용자와 허가자의 정책에 기반을 두어 접근제어를 수행한다. 2장에서는 제안하는 모델의 관련연구를 위해 프라이버시의 정의를 살핀 후 프라이버시보안 프로젝트에 대해 조사하고 웹 프라이버시 보호 관련기술에 대해 살펴보고 대표적인 P3P, EP3P, EPAL 기술들을 분석하며 ID관리 시스템에 대해 연구한다. 3장에서는 ID관리시스템의 접근통제기반 프라이버시 보안 모델을 제안하고 접근통제 절차를 살펴본다. 4장에서 본 모델을 적용한 시스템 구조(system architecture)에 대해 제시하고 5장에서 접근통제 처리 예를 보인다. 끝으로 6장은 결론 및 향후 연구주제를 논의한다.

2. 관련 연구

정보사회의 프라이버시는 Alan Westin에서 "개인, 집단, 단체 스스로 자신이 소유한 정보를 다른 사람에게 언제, 어떻게, 얼마나 공개할 것인가를 결정하고 그렇게 하도록 요구하는 것"이라고 정의했다. Samuel Waren과 Louis Brandesis는 "개인의 프라이버시는 상대방에게 절대적으로 침해 받아서는 안 된다"고 정의하고 있다[21].

정보시스템을 사용하는 대부분의 사용자가 개인의 프라이버시에 관심을 가지고 이와 동시에 편리함을 추구하여 정보시스템을 운영하는 기업은 개인의 프라이버시 측면보다는 기업의 이익을 위해 개인정보를 운용하는 사례가 존재한다[11,13].

2.1 프라이버시 보안 프로젝트

ID관리 시스템을 보호하기 위해 ID관련 개인 프라이버시 보호 프로젝트는 프라이버시 및 ID 관리 연구를 위한 로드맵인 RAPID와 ID관리 환경의 프라이버시 프레임워크를 목표로 하는 PRIME이 있다.

RAPID(Roadmap for Advanced research in Privacy and Identity management)는 PIM (Privacy and Identity Management)분야의 연구주제를 결정하고 개인의 프라이버시를 보호하는 것을 목표로 하는 프로젝트이다. 이 프로젝트는 프라이버시 강화 기술과 ID 관리 방법을 기술적 측면과 사회-경제-법률적 측면에서 다룬다. 특히 ID관리 영역에서 프라이시를 위한 전략적인 로드맵을 개발하고 PIM 분야의 다양한 워크숍을 통해 다양한 정보를 교환하고 다른 로드맵 프로젝트와 협력하는 것을 목표로 한다. 기술적 측면은 개인 정보 보호에 사용되는 보안 메커니즘을 활용하는 인증, 접근 통제, 암호, 보안관리, 익명의 웹 서핑, 프로비저닝(provisioning) 등이다. 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[7]. RAPID는 목표들을 지원하기 위해서 다양하고 신뢰할 수 있는 신원관리, 적법한 PIM 이슈들, 사회 경제

적인 PIM 등의 테마들을 연구한다.

PRIME(Privacy and Identity Management for Europe) 프로젝트는 유럽의 주요한 연구단체들을 중심으로 W3C등 주요 표준화 기관과 연계된 개인의 프라이버시 보호를 위한 프로젝트이다. PRIME 프로젝트는 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 프로젝트를 수행하고 있다. 이것은 개인들이 정보화 사회에서 그들의 행위와 무관하게 스스로 개인정보를 제어하여 그들의 프라이버시 보호를 제공받고 정부, 경제, 전문분야 등 정보화 사회의 전반에 걸쳐 프라이버시를 제공을 위해 연구를 수행 중이다. 또한 편리한 컴퓨터 사용자 인터페이스, 온톨로지(ontology), 인증, 암호화 기술을 기초로 하고 최신의 ID관리 기술과도 상호동작하고 프로그램 개발자나, 서비스제공자, 애플리케이션 운영자 등 특정 산업과도 잘 적응되도록 표준 기술을 개발한다. 즉 사용자 자신이 그들의 ID를 관리하고 개인 프라이버시를 통제할 수 있는 기술을 개발하고 또한 이 프라이버시가 강화된 ID관리 기술을 퍼베이시브 컴퓨팅(pervasive computing)까지 확대시키는 것이다. 이를 위해서는 현재의 컴퓨팅 환경뿐만 아니라 미래 환경의 다양한 컴퓨팅 시나리오, 프라이버시와 보안을 통한 통신과 검증뿐만 아니라 프라이버시를 위한 다양한 기능을 제공해야 한다[8].

2.2 웹 프라이버시와 보호 관련 기술

웹은 온라인상에서 정부와 기업이 제공하는 서비스를 개인과 연결시켜주는 편리함을 제공한다. 하지만 개인의 데이터에 쉽게 접근할 수 있는 편리함은 프라이버시를 침해할 수 있는 보다 폭 넓은 길을 열어주었다[14,16]. 웹에서 개인정보에 대한 프라이버시의 침해는 정보의 주체가 허가하지 않는 정보의 전송, 시스템과 네트워크 보안의 취약성, 허가 받지 않은 개인정보데이터의 무분별한 수집 등으로 발생한다. ID관리시스템은 하나의 웹 시스템으로 구성할 수 있다. 웹 시스템은 서비스 제공자와 개인을 연결시켜주는 편리함을 제공하는 반면에 개인의 프라이버시를 침해할 수 있는 길로 활용될 수 있다. 일반적으로 웹에서 개인의 프라이버시 침해는 정보의 주체가 허가하지 않은 정보의 전송, 개인 정보 보호의 취약함, 개인정보 데이터의 무분별한 수집 등으로 발생된다. 웹 프라이버시를 위해서는 정보의 수집, 정보의 사용목적, 수집된 정보의 저장, 수집된 정보의 배포, 개인 정보 보호를 위한 정책과 도구들, 정보의 접근 제어, 개인정보 접근과 사용의 모니터링, 정보보호 정책의 변경을 위한 규정이 필요하다.

개인의 프라이버시를 보호하기 위한 방법들은 크게 기술적인 방법(technology-enabled solution)과 규범적인 방법(regulatory-enabled solution)으로 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 가상사설망(virtual private network) 이나 방화벽(firewall)을 이용할 수 있다. 셋째 클라이언트 서버에 기반을 둔 방법은 서버와 클라이언트가 서로 협력하여 개인의 프라이버시를 보호한다. 암호화에 의한 방법과, P3P[15,17,18]와 같이 협상에 의한 방법으로 프라이버시를 제공한다. 규범적인 방법은 사적인 규범과 강제적인 규범에 의한 방법으로 분류 된다. 사적인 규범은 공인되지 않은 정책과, 공인

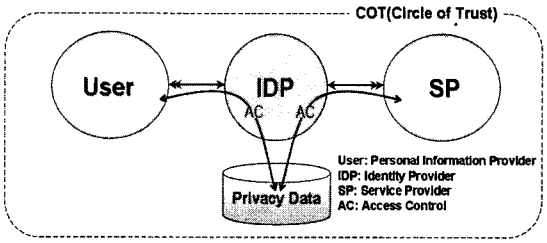
된 정책이며 이들은 개인의 사생활을 보호하기 위해 사용된다. 다른 하나인 강제적인 규범은 국가나 정부에 의해 제정된 권고적인 프라이버시 보호 법률이다.

대표적인 프라이버시 보호관련 기술은 P3P, E-P3P, EPAL이 있다. P3P(Platform for Privacy Preference Project)는 웹 사이트에서 프라이버시를 보호하기 위해 W3C(the World Wide Web Consortium)에서 제정한 표준이다. 이것은 사용자가 방문하는 웹 사이트에서 정보를 소유자가 개인정보를 제어할 수 있도록 개인정보보호정책(Privacy statement)을 기술하는 산업 표준으로 웹 사이트에서 프라이버시 보호를 위한 관리방법 등을 기술하기 위한 표준 용어집과 문법 및 기본 프로토콜을 정의하고 있다[15,20]. P3P를 이용하는 응용들은 마이크로소프트사의 IE6.0(Internet Explorer 6.0)이상이나 AT&T Privacy Bird[12,17]가 있다. IE 6.0에서는 P3P를 구현하지만 제안된 프라이버시 기능만을 제공하는 콤팩트 정책(Compact Policy)만을 제공한다[12]. 콤팩트 정책은 데이터양이 적고 구조가 간단해서 브라우저에서 바로 정책을 해석하여 판단을 내릴 수 있다. 일반적으로 개인정보보호 정책의 생성은 IBM Policy Editor와 같은 자동화된 GUI(Graphic User Interface)를 이용하면 쉽게 생성할 수 있다[18]. E-P3P(The Platform for Enterprise Privacy Practice)는 현재 IBM의 프라이버시 연구소에서 활발하게 연구를 진행하고 있는 기술이다. P3P는 기업의 프라이버시 정책을 기술하는데 사용되지만, 기업내부에서 그 정책이 제대로 집행되도록 하는 세부적인 기술을 의미하지 않기 때문에 IBM은 기업 내부에서 고객들의 프라이버시 정보를 신뢰할 수 있는 방법으로 관리할 수 있도록 하는 프레임워크를 개발했다[19]. EPAL(Enterprise Privacy Authorization Language)은 인터넷 환경에 개인정보를 제공하는데 있어서 개인이 인가(authorization)하는 범위 내에서만 개인정보를 제공하도록 하기 위해 기업에 저장된 개인정보에 대한 개인정보 정책들을 기술하기 용이하도록 제작된 정책기술언어이다. EPAL정책의 구성요소는 Data-category, User-category, Purpose, Actions, Obligations, Condition이다[20].

2.3 ID관리 시스템

ID 관리란 사용자, 서비스, 정보통신기기 등 네트워크에 연결되는 개체들에 해당하는 신원의 속성(identity attribute), 신원증명서(credential), 정보이용 자격(entitlement) 등을 전체 생명주기 동안 디지털 신원(Identity)들을 통합 관리해주는 플랫폼 기반구조이다[1]. ID관리 시스템은 조직의 내부 통신망이나 외부 통신망으로부터 접속해오는 사용자나 단말기를 인증하고 해당하는 권한을 확인하여 정보자원에 대한 적절한 접근권한을 인가해주는 과정을 수행한다. 따라서 ID관리(Identity Management)시스템은 AAA(Authentication, Authorization, Audit/Account)기술, P3P기술, 패스워드 초기화/동기화 기술, 관리권한 위임, SSO (Single Sign On), LDAP(Light-weight Directory Access Protocol)등의 여러 기술을 종합하여 구현된 복잡한 시스템이다. 이러한 기술을 이용한 대표적인 ID관리시스템으로는 ID 통합(Federated Identity)을 제공하는 Liberty Alliance[2,3]와 PingIdentity의 SourceID[9], MS사의 .NET Passport[10]가 있다.

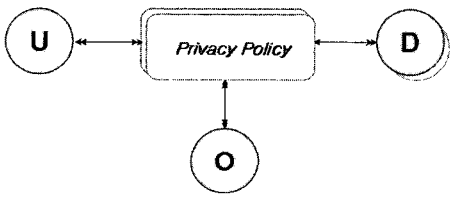
그림 1은 ID관리시스템을 나타낸다. 사용자(User)는 SSO서비스를 사용하는 주체이며, IDP는 사용자의 식별들을 고유하게 유지하고 관리하는 시스템이며, SP는 IDP와 연합관계에 있으면서 IDP를 신뢰한다. IDP는 사용자를 인증하고 사용자와 관계된 개인정보 데이터를 유지 관리하고 필요에 의해서 SP에게 제공한다. SP들은 IDP로부터 받은 정보데이터를 이용하여 SP에게 서비스를 제공한다. 이러한 환경에서 사용자의 개인 프라이버시는 매우 중요하다. 하나의 동일



〈그림 1〉 ID관리시스템

신원정보를 이용하여 서로 다르지만 연합관계에 있는 여러 웹사이트의 서비스를 활용하는 과정에서 사용자의 개인 행위가 감시되고 개인정보를 기반으로 새롭게 생성되는 개인의 의료정보, 금융정보, 구매 정보, 신용정보 등의 다양한 정보들이 생성될 수 있다[5]. 이렇게 생성된 개인정보 데이터들은 사용자가 허가한 개인정보의 생성 및 사용 목적에 의해서 통제 되어야 개인의 프라이버시가 지켜질 수 있다[21].

대부분의 ID관리 환경에서는 다양한 사용자들에게 서비스를 제공하기 위해서 IDP의 접근 메커니즘에 사용되기 위한 보안정책을 제공한다. 이 보안정책의 용도는 서비스를 필요로 하는 사용자를 인증하고 서비스와 데이터를 인가하며 IDP입장에서 개인정보와 서비스를 관리한다. 이것은 IDP운영자인 기업의 입장에서 서비스를 운영할 목적으로 생성되기 때문에 IDP에 개인정보를 제공하고 이용하는데 있어서 기업의 입장에서 정보소유자인 개인에게 허락 받지 않고 개인의 정보를 사용할 수 있는 프라이버시적인 문제가 발생한다. 개인의 프라이버시가 보호되기 위해서는 프라이버시 보호 원칙과 정의를 고수하기 위해서 그림 1의 프라이버시 데이터와 직접



〈그림 2〉 기본 개념모델

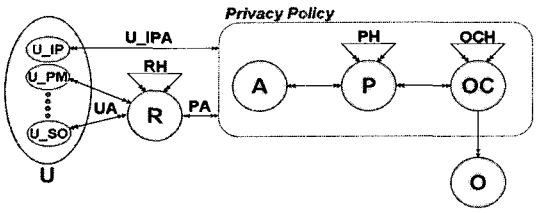
적인 관련이 있는 개인이 직접 자신의 정보의 이용에 대한 권한을 행사하는 것이 필요하다.

3. ID관리시스템의 접근통제기반 프라이버시 보안모델

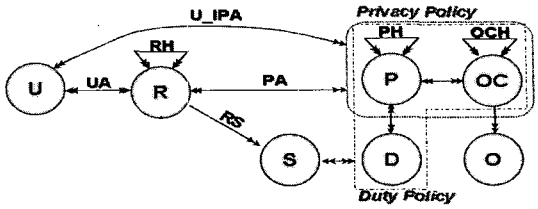
ID관리 환경은 SSO 메커니즘을 제공해서 디지털식별(digital identity)들이 미치는 범위가 COT 영역으로 확장됨에 따라 프라이버시의 영향범위가 증가되어 개인의 프라이버시 문제가 가중되는 악영향을 안고 있다[4]. 본 장은 ID관리시스템의 접근통제기반 개인 프라이버시 보안모델을 제안한다. 이 모델은 그림 1과 같은 ID관리 환경을 기반으로 하고 프라이버시데이터(Privacy Data)를 사용자(User)가 허가하는 목적으로만 사용하도록 하여 개인의 프라이버시를 안전하게 보호하는 ID관리 프라이버시 보안모델이다. 또한 정보소유자인 개인이 직접 개인정보에 대한 프라이버시 보호를 수행할 수 있도록 하며 P3P와 E-P3P와 유사한 프라이버시정책(Privacy Policy)에 기반을 둔 접근제어(Access Control)로 프라이버시데이터를 통제하고 P3P의 근본개념[15]과 EPAL의 프라이버시 보안을 위한 기본 개념[20]을 확장하여 ID관리 환경에 적합한 하나의 모델을 제안한다.

3.1 ID관리 프라이버시 보안모델(Identity Management Privacy Protection Model)

그림 2는 사용자가 프라이버시 데이터에 접근하기 위해 모태가 되는 기본 개념모델이다. 기본 개념 모델은 모든 사용자(U)들이 프라이버시정책(Privacy Policy)에 기반하여 ID관리 시스템에 저장되어있는 개인정보데이터(O)에 접근한다. 이후 우리는 그림 3과 같은 구체적인 모델을 보인다. U는 개인정보 제공자와 사용자를 의미하며 Privacy Policy는 U로부터 생성되는 프라이버시 정책들이다. D는 EPAL에서 Obligation의 개념



〈그림 3〉 IDMP 모델



〈그림 4〉 D를 적용한 IDMP 모델

과 같은 개인정보 데이터의 사용에 따른 의무이다 [6,20]. D(Duty)는 U가 O에 접근하는 시점에서 D가 프라이버시 정책에 관여하여 이미 획득한 개인정보데이터에 대한 재사용을 제한한다[16,20]. 제안된 모델을 통해 인가된 개인정보의 재사용을 다루기 위해 D를 고려한 모델은 그림 4와 같이 표현될 수 있다. 이때 S(Session)는 RBAC (Role-based access control) 모델에서 Session과 같은 개념이며 해당세션 동안 Duty Policy를 계산 하고 만족하는 동안에만 개인정보에 접근할 수 있다. 이 모델은 그림 3의 IDMP 모델에 그림 2의 D의 개념을 도입하여 객체를 제공받기 이전에 D를 제공받고 D에 만족하는 동안만 해당 P동안 OC를 얻어내서 O에 접근할 수 있다. Privacy Policy는 개인정보를 어떤 경우에 허가할 것인가를 결정하며 Duty Policy는 허가된 개인정보를 얼마 동안 사용할 것인가를 다룬다.

D를 적용한 IDMP 모델에서 D의 기능은 접근제어 함수와 인가 규칙에 의해 개인정보가 허가된 이후에 이정보를 얼마 동안 사용할 것인가를 다루고 반드시 정해진 목적으로만 재사용해야 할 것을 감시한다. D가 단순히 허가된 개인정보의 사용에 있어서 얼마 동안 유지되어야 한다는 기능적인 면만을 제공해서는 안 된다. D는 반드시 허가된 개인정보에 대한 이용에 따른 책임도 제공돼야 한다. D에 책임성을 부여하기 위해 세션 ID(Session ID)와 암호화 기술을 이용한다. 세션 ID는 암호화 키를 생성하는 주요한 키 변수로 쓰여서 획득한 객체에 대한 암호화를 수행하여 복호화 키를 갖는 유효한 세션 동안만 가능하도록 제안한다. 이에 대한 자세한 논의와 연구는 향후의 연구에서 다룰 계획이다. 본 논문에서는 D를 제외한 그림 3의 모델만을 다룬다.

3.2 IDMP모델의 주요 구성요소

제안한 IDMP 모델의 구성요소는 표 1을 따른다.

정의 1. IDMP(Identity Management Privacy Protection) 모델

3.2.1 U(User): ID관리 시스템 사용자

ID관리 시스템의 사용자(U)는 U_IP(U_Identity Provider), U_PM(U_Privacy Manager), U_SM (U_Service Manager), U_SU(U_Service User), U_SO(U_Special Operator)의 모임으로 정의한다. U_IP는 개인정보허가정책을, U_PM은 개인정보요청정책을 설정하는 실체이다. U_SM은 서비스 운영자이며 이들은 개인정보의 조회, 통계, 백업 목적으로 개인정보를 운영한다. 이러한 U_SM은 위탁으로도 운영될 수 있다. U_SU는 하나의 단일 COT내에 속해있고 IDP에 의해 인증 받은 모든 사용자들의 집합이다. 프라이버시 관점에서 U_IP는 개인정보 제공자이며 U_SP는 개인정보 요청자로 나뉜다. U_SO는 개인정보를 법률이 정한 특수 목적으로 사용할 수 있는 특권 사용자들의 모임이다.

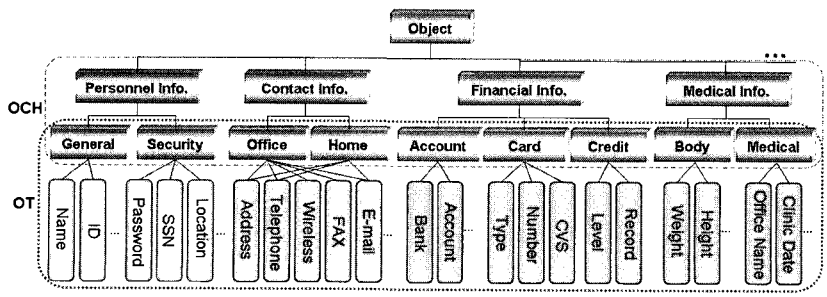
3.2.2 O(Object): ID관리 시스템의 개인정보

객체(O)는 O_IP, O_SM의 집합들로 구성된

〈표 1〉 IDMP 모델의 구성요소

이 름	의 미
U(User)	$U = U\_IP \cup U\_PM \cup U\_SM \cup U\_SU \cup U\_SO$
O(Object)	$O = O\_IP \cup O\_SM$
OCH(Object Category Hierarchy)	$OCH \subseteq OC \times OC$
OT(Object Tree)	$OT \subseteq OC \times 2O$
A(Access Mode)	$A = \{Create, Delete, Update, Retrieve\}$
R(Role)	$R = R\_IP \cup R\_PM \cup R\_SM \cup R\_SU \cup R\_SO$
RH(Role Hierarchy)	$RH \subseteq R \times R$
P(Purpose)	$P = P\_IP \cup P\_PM$
PH(Purpose Hierarchy)	$PH \subseteq P \times P$
PP(Privacy Policy)	$PP = PP\_IP \cup PP\_PM$
PP_IP(PP_Identity Provider)	$PP\_IP=P\_IP \times R \times A \times 2^{Object} \times OC$
PP_PM(PP_Privacy Manager)	$PP\_PM=P\_PM \times R \times A \times 2^{Object} \times OC$
U_IPA(U_IP Association)	$U\_IPA \subseteq U\_IP \times PP\_IP$
UA(User Assignment)	$UA \subseteq U \times R$
PA(Purpose Association)	$PA \subseteq R \times PP\_PM$

다. O_IP는 IDP나 SP에 U_IP를 통해 저장되는 모든 개인정보 데이터의 집합이며 O_SM은 IDP나 SP에 저장된 개인정보를 U_SM이 운영정보로 변형하여 새롭게 생성 및 유지하는 모든 데이터의 집합이다. O_SM은 개인정보를 통계 및 백업처리 목적으로 개인정보를 가공하고 유지한다. 이렇게 생성된 O_SM은 외부의 침입으로부터 발생할 수 있는 제반 문제점들이나 시스템 운영에 관련된 업무를 융통성 있게 해결한다. 객체의범주의집합(OC)은 O_IP로부터 생성되는 개인정보를 의미하는데 이러한 개인정보는 신상정보, 연락정보, 금융정보, 의료정보 등 여러 객체 범주의 집합으로 나뉜다. 그림 5와 같이 이들 객체 범주들 간에는 계층관계(OCH)를 가진다. O의 범주의 집합이 OC이며 이 범주들은 OCH로 표현된다. OC는 O의 단위를 객체의 범주의 집합으로 그룹화 함으로써 객체를 관리하는데 효율성을 제공하여 정책을 설정하는데 있어서 정책이 OC단위로 설정됨으로 정책을 간소화 시킬 수 있는 이점이 있지만 객체범주 단위로 인가를 제공하므로 개인정보가 객체범주만큼 늘어나는 단점이 있다. OT는 객체의범주의집합과 각 데이터 집합의 릴레이션으로 구성되는 OCH를 이루는 단말의 OC에 속하는 각 구성 요소의 집합을 의미한다. 사용자는 객체에 대해 접근할 수 있는데 이때 가능한 단위가 OT이며 이에 따른 접근모드(A)는 객체의 생성(Create), 삭제(Delete), 수정(Update), 조회(Retrieve)이다. 즉 A는 개인정보를 어떻게 사용, 허용할 것인가를 의미하며 이에 따라서 다양한 정책이 기술된다.

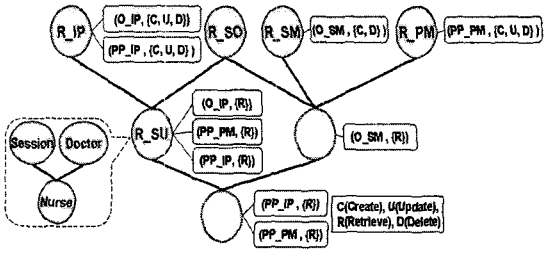


〔그림 5〕 객체의 예

3.2.3 R(Role): ID관리 시스템의 역할

역할(R)은 R_IP, R_PM, R_SM, R_SU, R_SO의 집합으로 구성된다. R_IP는 IDP나 SP에 개인정보를 제공하는 U_IP와 관련된 역할들의 집합이며, R_PM은 U_PM이 행사할 수 있는 프라이버시 정책관련 역할들의 집합이다. 또한 R_SM은 U_SM이 행사할 수 있는 운영 관련 역할들의 집합이고 R_SU는 U_SU들이 행사할 수 있는 서비스 이용 역할들의 집합이며 R_SO는 U_SO가 개인정보를 특수 목적으로 접근할 수 있는 특수 사용 역할들의 집합이다. 이들 역할들은 계층에 의해 관리되며 부분순서(partial order)관계를 갖는다. U_IP의 R_IP가 존재하면 개인에 대한 프라이버시 영향력은 감소될 수 있지만 IDP나 SP측에 저장된 개인정보를 관리하거나 처리하는데 있어서 효율성을 높일 수 있다. 따라서 U_PM과 U_SM이 U_IP와 사전협의 하에 R_IP에 사용을 결정해야 한다. 이때 R_IP에 사용이 확정되면 U_PM과 U_SM이 IDP나 SP들에 서비스운영에 적합한 R_IP들을 결정한다. 반면에 R_IP가 없다면 개인의 프라이버시 영향력이 증가되지만 개인정보 관리의 효율성은 낮아진다. 이때는 개인의 식별 ID와 연결되는 고유한 PP_IP가 생성된다. R_IP와 개인의 식별 ID는 서로 이질적이므로 PP에 의해서 병행적으로 사용될 수 있으므로 개인의 식별 ID가 R_IP 등급의 역할로 사용 될 수 있다. UA는 사용자들이 다대다 관계로 그에 맞는 역할로 사상된다. 역할 계층분류의 예는 그림 6과 같다.

그림 6에서 R_SU에서 Doctor가 Nurse보다



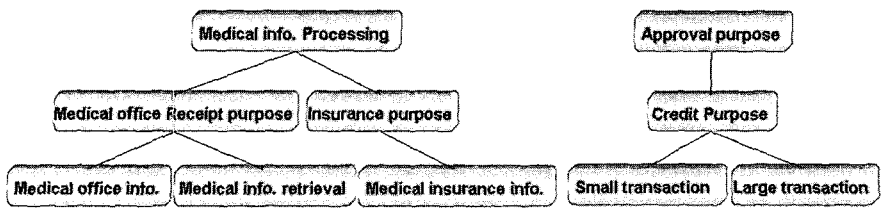
〔그림 6〕 역할 계층분류 예

높은 계층을 가지며 이둘 간의 계층 간의 관계는 '>'기호를 사용하여 Doctor > Nurse로 표기한다. R_IP와 R_SO와 같이 계층이 같은 경우는 '='기호를 이용한다. 예를 들어 R_IP = R_SO로 표현된다. '>'기호와 '='기호를 모두 의미하는 경우는 '≥'기호로 쓰인다.

3.2.4 P(Purpose): 정보사용 목적

목적(P)은 개인정보를 어떠한 의도로 허가하고 사용하는 것을 규정한다. P_IP는 U_IP의 개인정보 사용을 위한 허가목적이며, P_PM은 U_PM의 개인정보 사용을 위한 요청목적이다. P_IP와 P_PM은 같은 의미이며 단 생성한 주체가 U_IP, U_PM인지에 따라서 서로 다른 정보사용 목적이 된다. 또한 P_IP와 P_PM들 간에는 계층이 존재하며 부분순서(partial order)관계를 갖는다. 그림 7은 목적 계층의 예를 나타낸다.

P간의 계층 간의 관계는 역할계층의 관계와 같게 '>', '<', '=', '≥', '≤'기호로 표현된다. 예를 들어 그림 6에서 Medical Office Receipt purpose와 Medical office info.의 계층 간의 표



〔그림 7〕 Purpose 계층 예

〈표 2〉 접근 정책의 구분

구분	생성 주체	단위	대상	용도
PP_IP	정보소유주 개인	개인	개인정보 소유자	프라이버시 인가정책
PP_PM	시스템 정책 관리자	그룹	개인정보 이용자	프라이버시 요청정책

현은 Medical Office Receipt purpose가 Medical office info.보다 상위 계층이므로 Medical Office Receipt purpose > Medical office info. 의 관계를 갖는다.

3.2.5 PP(Privacy Policy): 프라이버시 정책

프라이버시정책은 표 2와 같은 PP_IP), PP_PM으로 구성된다. PP_IP는 개인정보 제공자가 설정하는 프라이버시 정책이며 개인정보를 어떠한 P_IP에 의해, 얼마 동안, 어떤 정보를 허가하겠다는 것을 명시한다. PP_PM은 개인정보 요청자가 요청하는 정책으로 해당 개인정보를 사용할 U_PM에 의해서 개인정보를 어떠한 P_PM에 의해, 얼마 동안, 어떤 정보를 사용하겠다는 것을 명시한다. U_IPA는 U_IP와 PP_IP간에 다대다 관계로 사상된다. 따라서 제공한 개인정보를 허가할 정책을 정보소유자인 U_IP가 설정할 수 있음을 의미 하므로 개인정보제공자의 프라이버시를 강화할 수 있다. PA는 역할들이 각 정책들에 해당하는 PP_PM에 다 대다 관계로 사상된다. 따라서 정보 이용자는 자신이 속해있는 역할에 의해 정책을 부여 받는다. 이렇게 함으로써 정보사용자의 관리가 역할 단위로써 수행됨으로 이용자의 관리가 용이하다.

PP_IP는 U_IP가 O_IP를 제공하는 처리과정에서 생성된다. 이때 개인들은 개인정보를 제공할 때 자신의 개인정보가 어떠한 P_IP, A를 따를 것인가에 대한 PP_IP를 설정한다. 따라서 PP_IP는 U_IP에 해당하는 각 사용자에 따라서 다른 정책이 유지될 수 있다. PP_PM은 U_PM이 생성하며 U_SU가 서비스를 이용하는 과정에서 필요로 하는 O_IP가 발생할 때 어떻게 O_IP를 요구할 것인가에 대한 정책이다. O_IP는 관리상의 효율성을 위해서 OC로 나뉜다. OC는 범주에 의해서 PP를 설정하게 함으로써 PP_IP와 PP_PM을 설정하는 U_IP와 U_PM에 PP설정을 돕는다. PP를 설정하는데 있어서 O_IP의 크기만큼 고려될 필요 없이 OC에 의해서만 고려하면 된다. 즉 $R \times A \times 2O \times O$를 $R \times A \times 2O \times OC$로 줄이는 효과가 있다. 하지만 개인 프라이버시 보호를 위해 U_IP와 U_PM이 PP를 설정하는 대상이 O가 아니라 OC이므로 개인프라이버시에서 개인의 영향력은 줄어들 수 있다.

3.3 접근 제어 처리

제안된 모델은 ID관리시스템에서 프라이버시를 제공하기 위해 접근허가정책과 접근요청정책을 이용하여 접근 제어를 수행한다. 여기서는 제안된 모델의 접근 제어 처리를 정의한다. 정의 2는 개인정보 사용자가 접근 제어를 요청할 때 필요한 정보구조를 정의한다.

정의 2. 접근 요청 정보 구조

○ Access Request =(u, r, a, o, p) where u ∈U, r∈R, a∈A, o∈O, p∈P

정의 3, 4는 정의 2의 u, r, o에 대응되는 정보요청정책과 정보허가정책을 이용하여 접근제어를 처리하는 함수들과 인가 규칙을 정의한다.

정의 3. 제안된 모델의 사용함수

표 3은 접근 요청을 수행하는데 있어서 필요로 하는 함수들을 정의한다.

정의4. 인가 규칙

· Authorization = inclusive_purpose(p of pp_pm, p of pp_ip)

^ inclusive_role(r of pp_pm, r of pp_ip)

〈표 3〉 접근제어 처리절차 함수

함수 정의	의미
get_oc_set(o) = ∪oc∈OT (oc) where o ∈ oc	O → 2OC
get_purpose_set(r, oc_set) = ∪oc ⊆ oc_setget_oc_purpose(r, oc)	R × 2OC → 2P
get_oc_purpose(r, oc) = p ∃(r, a, oc', p) ∈ PP, oc = oc' ∪oc' get_oc_purpose(r, oc') where (oc', oc) ∈ OCH	R × OC → 2P
get_pm_policy(u, r, oc) = ∪pp_pm ∈ PP_PMpp_pm (ri, ai, oci, ui, di) where (ui=u, ri=r, oci=oc)∀1≤i≤n	U × R × 2OC → PP_PM
get_ip_policy(u, r, oc) = ∪pp_ip ∈ PP_IPpp_ip (ri, ai, oci, ui, di) where (ui=u, ri=r, oci=oc)∀1≤i≤n	U × R × 2OC → PP_IP
inclusive_purpose(p, p') = TRUE p ≤ p' FALSE otherwise	P × P → Boolean
inclusive_role(r, r') = TRUE r ≥ r' FALSE otherwise	R × R → Boolean

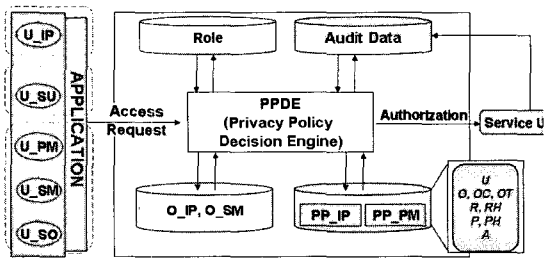
인가 규칙은 접근 요청을 받아 표 3에서 정의한 함수를 이용해 접근 허가와 거부를 결정한다. 이것은 인가가 일어나는 시점에 입력 값으로 정보요청정책과 정보허가 정책을 받아서 inclusive_purpose, inclusive_role에 입력 값으로 제공되고 이를 수행하여 결과 같이 모두 TRUE인 경우에만 개인정보의 접근을 허용한다. 예를 들어 inclusive_role은 개인정보허가정책의 r과 개인정보요청정책의 r'을 입력 값으로 처리하여 그 결과가 r≤r'인 경우에만 TRUE를 반환한다. 즉 정보요청자의 r'이 정보 허가자의 r의 계층과 같거나 그보다 높은 경우에만 TRUE임을 의미한다.

4. ID관리 프라이버시 보안모델의 시스템 구조와 정책 스키마

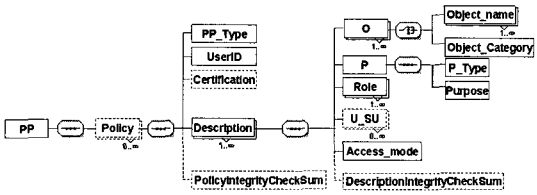
본 장에서는 제안된 모델을 수행하기 위한 시스템 구조와 프라이버시 정책스키마를 정의한다. 시스템 구조는 ID관리 환경의 다양한 사용자들이 다양한 서비스를 제공받기 위해 필요로 하는 개인정보를 이용하는데 있어서 제안한 모델을 적용하여 개인의 프라이버시를 보호하는데 있다. 프라이버시 정책스키마는 시스템의 동작에 필요한 정책을 제안한 모델에 기반을 두고 제안한다.

4.1 시스템 구조

IDMP모델을 따르는 시스템 아키텍처는 그림 8에서 보인다. 단 개인정보 처리의 안전함을 위해서 전송간 암호화 기법에 의해 안전함을 제공하는 프로토콜을 사용한다. ID관리 시스템에 통합 유지되는 개인정보에 접근하는 사용자들은 크게 3개의 그룹을 갖는다. 이것은 정보제공자, 정보사용자, 이외에 서비스를 운용하거나 안전하게 관리하는 사용자 그룹이다. 이 그룹들은 응용(APPLICATION)을 통해 제공되는 모든 서비스의 이용(Service Usage)이 가능하다. 제안하는 시스템구조의 가장 큰 특징은 서비스의 사용 전에 반드시 PPDE를 거쳐 인가를 받아야 한다. PPDE(Privacy Policy Design Engine)는 표 3의 접근 처리절차 함수와 접근요청(Access Request)



〔그림 8〕 ID관리시스템 구조



〔그림 9〕 정책 스키마

과 관련된 프라이버시 정책인 PP_IP, PP_PM를 참조하여 3장에서 정의한 접근제어 처리절차와 인가 규칙에 의거하여 개인정보데이터인 O_IP, O_SM를 인가한다. 인가된 데이터는 서비스 사용(Service Usage)동안만 사용가능 하며 인가된 개인정보에 대한 정확한 수행을 보장하기 위해 감사 데이터(Audit Data)를 유지하고 PPDE가 이를 점검한다.

4.2 제안한 모델의 정책 스키마

본 논문에서 제안하는 모델은 ID관리 시스템에 저장된 프라이버시 정보에 대해서 정보 소유주가 허가하는 목적을 따르는 경우에만 개인의 프라이버시 데이터에 접근이 가능하도록 제한된다. 따라서 프라이버시데이터의 사용에 있어서 프라이버시 데이터의 소유자가 허가하는 목적에 의해서만 인가를 제공하기 위해 프라이버시 정책이 설정되고 정책에 기반을 두고 접근제어를 수행한다. 이 프라이버시 정책은 P3P나 E-P3P, EPAL과 유사하지만 ID관리 환경을 지원하기 위해 개인정보 허가 정책이나 요청 정책들을 위한 스키마가 필요하다. 본 논문에서 제안한 ID관리시스템은 그림 9와 같은 PP 정책 스키마를 따른다.

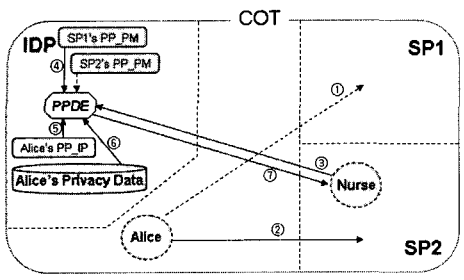
개인정보허가정책을 예로 들면 'Alice'란 사용자가 자신의 의료정보인 'Medical record'에 대해 'Doctor'이상의 역할이 'Alice'의 개인 정보를 'Medical office Receipt'의 용도로만 접근하거나 사용할 때만 개인정보를 허가하는 정책을 선택한다면 'Alice'의 개인정보 허가정책인 PP_IP는 그림 10과 같은 XML 형태로 생성되어 그림 8의 정책 데이터베이스인 PP_IP에 자동 저장된다.

그림 10에서 ①은 개인정보 허가정책의 헤더 정보이다. 여기에서 <PP_Type>은 정책의 유형을 결정한다. 여기서는 허가 정책이므로 'PP_IP'이다. <UserID>는 사용자의 ID를 의미하며 <Certification>은 사용자를 증명하는 개인정보 사용 인증서를 해시(hash) 값으로 유지한다.

②의 <Description>에는 ①에 해당하는 개인에 대한 정책이 기술된다. <O>는 객체이며, <P>는 목적이다. <Role>은 객체에 접근할 수 있는 역할들이며, <U_SU>는 특정 사용자를 나타내는 식별자가 올 수 있다. 여기서는 <Role>이 'Doctor'이상인 경우에만 허가를 받을 수 있다. 만약 <U_SU> 태그가 사용되었다면 이것은 <Role> 태그와 '&' 연산 조건으로 수행된다. <Access_mode>는 객체에 대한 접근 유형을 지

```
<?xml version="1.0" encoding="UTF-8"?>
<PP xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
" xsi:noNamespaceSchemaLocation="http://x.x.x.x/pixml/pp_schema.xsd">
<Policy>
   <PP_Type>PP_IP</PP_Type>  <UserID>Alice's ID</UserID>  <Certification>0e0c95d2caca1d</Certification> ——①
 <Description>
   <O> <Object_Category>Medical record</Object_Category> </O>
   <P>  <P_Type> P_IP </P_Type> <Purpose> Medical office Receipt </Purpose> </P>
   <Role> Doctor</Role>
   <Access_mode>Retrieve</Access_mode>
   <DescriptionIntegrityCheckSum>c748f4df00d698ad2c98ac61b0ebc746f4c800dc98a12cb0fcc74af49500d398ff2cc
   </DescriptionIntegrityCheckSum>                                                              ②
 </Description>
 <PolicyIntegrityCheckSum>a36b0fcc71df49400d298a42c92ac31b0aac71ff494008298f12cc4ac35b0aec798f7
 </PolicyIntegrityCheckSum>                                                                   ③
</Policy>
</PP>
```

〔그림 10〕 Alice의 개인정보 허가정책 예



(그림 11) Alice의 의료정보 접근 예

정하고 <Description IntegrityCheckSum>은 <Description>의 내용에 대한 무결성(integrity)을 검사한다.

③의 <PolicyIntegrityCheckSum>은 설정된 PP에 대한 무결성을 검사한다. <DescriptionIntegrity CheckSum>과 <PolicyIntegrityCheckSum>은 U_PM에 의해 옵션으로 선택 될 수 있다.

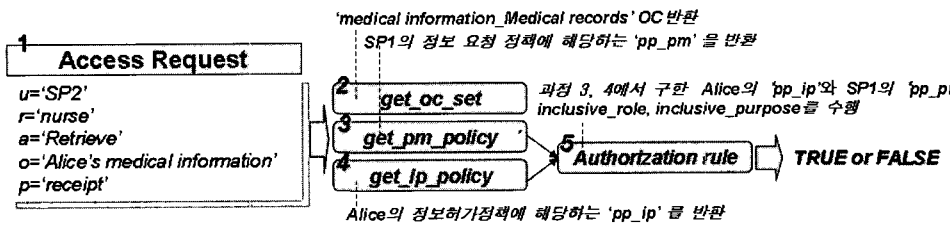
정의된 XML스키마로부터 생성된 정책은 그림 10의 정책데이터베이스인 PP_IP이나 PP_PM의 데이터베이스에 저장된다. 이후 PPDE의 처리를 위해 사용되고 정보제공자에 의해 수정되거나 삭제될 수 있다.

5. 제안된 모델 적용 및 수행

의료정보에는 개인이 민감함을 느껴서 보호받기를 원하는 프라이버시 데이터 정보가 존재한다. 본 장은 제안된 모델을 적용하여 정보의 소유주인 환자가 자신이 민감하게 여기는 정보에 대하여 접근제어를 위한 정책을 설정하고 이 정책에 의해 개인정보가 관리됨에 따라 개인의 프라이버시를 지키는 경우를 보인다. 예를 들어 어떤 환자가 특정 병명으로 어떠한 치료를 받아왔다는 기록을 진찰하고 처방할 담당의사에게만 공개하고 진료를 돕는 간호사나 접수를 담당하는 접수자에게는 이 정보의 조회나 이용을 거부할 수 있어야 한다.

앞에서 제안한 개인 정보의 접근제어를 위한 함수와 인가규칙의 실행을 보이기 위해서 그림 11과 같은 ID관리 환경의 의료정보시스템을 위한 상황을 가정하고 이 가정된 시나리오를 이용하여 해결한다. Alice는 ID관리시스템에 가입되어 있는 상황이며 COT내에는 두 개의 의료 사이트인 SP1, SP2가 있다. 이 두 사이트와 관련된 Alice의 PP_IP는 ID관리시스템 가입으로부터 생성되는데 본 예제에서 다루는 Alice의 PP_IP 는 그림 10과 같다. 또한 PP_PM은 U_PM으로부터 생성되어 유지된다. 생성된 정책들은 그림 5와 같은 개인정보 구조와 그림 6의 역할 구조, 그림 7의 정보요청목적을 따른다. ①은 사전에 Alice가 SP1에 방문해서 Alice와 관련된 진료기록을 남겼음을 의미한다. Alice의 진료정보를 조회하기 위해 ③~⑦의 단계를 수행하는 접근인가를 위한 단계는 그림 12와 같다.

그림 12는 5단계로 구성되며 1단계는 접근요청을 위한 기본정보를 얻어낸다. 2~4단계는 1단계의 기본정보를 정의된 표 3의 함수를 이용해서 Authorization rule에 적용할 정책들을 추출한다. 이렇게 추출된 정책은 5단계를 거쳐 Boolean 값을 결과 값으로 리턴하고 TRUE일 때만 요청된 개인정보에 대한 접근을 허가한다.



(그림 12) 접근제어 함수에 각 단계별 흐름

```
<?xml version="1.0" encoding="UTF-8"?>
<PP xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance
" xsi:noNamespaceSchemaLocation="http://x.x.x.x/pixml/pp_schema.xsd">
<Policy>
   <PP_Type>PP_PM</PP_Type>  <UserID>SP1's ID</UserID>  <Certification>5d2b0aac71df2c</Certification> ——①
<Description>
   <O>  <Object_Category>Medical record</Object_Category> </O>
   <P>  <P_Type> P_PM </P_Type> <Purpose> Medical info. Retrieval </Purpose> </P>
   <Role> Nurse </Role>
   <Access_mode>Retrieve</Access_mode>
   <DescriptionIntegrityCheckSum>4c800494008298f12cc4ac35b0aec79ac61b0ebc747a42c92ac3c4ac35b1b0aac71ff
   </DescriptionIntegrityCheckSum>                                                          ②
</Description>
<PolicyIntegrityCheckSum>98a42c992ac31b0aac7ad2c986f4c800dc98a12cb0fcc74af4950ac31b0aac70d398f
</PolicyIntegrityCheckSum>                                                                  ③
</Policy>
</PP>
```

〔그림 13〕 SP1의 개인정보 요청정책 예

· 상황: SP2의 Nurse가 특정 병을 가진 환자에게 E-mail을 보낼 목적으로 동일한 COT범위에 있는 의료기관들에서 개인들의 의료정보를 수집하는 과정에서 SP1 으로부터 생성된 Alice의 진료기록을 요청하는 ③~⑦의 단계를 수행하는 경우를 보인다. 단 SP1의 개인정보 요청 목적은 그림 13과 같다.

[단계 1] SP2가 Alice's medical information을 요청하는 단계를 수행한다. 이 단계에서는 현재의 상황을 고려하여 접근 요구 정보인 u, r, a, o, p인 Access Request 정보를 계산해서 채운다.

Access Request = ('SP2', 'nurse', 'Retrieve', 'Alice's medical information', 'receipt')

[단계 2] SP2가 요청한 개인정보에 대해 객체의 범주를 검색하는 단계이다. SP2가 요청한 Alice의 의료정보를 입력 값으로 받아 계산한다. 그림 5와 같으므로 Alice의 의료정보 카테고리는 'medical information_medical records' 이다.

get_oc_set('Alice's medical information')

→ {medical information-Medical records}

[단계 3] Nurse의 요청에 맞는 정책을 검색하는 단계이다. 단계1의 입력 값과 단계2의 출력 값을 입력 값으로 받아 수행한다. 이 경우는 SP2의 Nurse가 SP1 으로부터 생성된 Alice의 진료기록을 요청하는 상황이므로 SP1의 개인정보요청정책을 검색한다.

get_pm_policy('SP1', 'nurse', {medical information_Medical records})

→ PP_PM(R: nurse, A: r, OC: Medical record, P_PM: Medical info Retrieval)

[단계 4] 개인정보의 소유자인 Alice의 정책을 가져오는 단계이다. 단계 1의 입력 값과 단계2의 출력 값을 입력 값으로 받아 수행한다.

get_ip_policy('Alice', 'doctor', {medical information-Medical records})

→ PP_IP(R: doctor, A: r, OC: Medical record, P_IP: Medical office Receipt)

[단계 5] 인가 규칙을 이용해서 개인정보에 허가에 대해 결정하는 단계이다.

Authorization

→ Step 3의 purpose & role

p: get_purpose_set('nurse', 'medical information-Medical records')

= {'Medical info. Retrieval'}

r: nurse

Step 4의 purpose & role

p′: get_purpose_set('doctor', 'medical information-Medical records')

= {'Medical office Receipt', 'Medical office info., 'Medical info. Retrieval'}

r′: doctor

→ inclusive_purpose({'Medical info. Retrieval'}, {'Medical office Receipt', 'Medical office info., 'Medical info. Retrieval'})= {'Medical

info. Retrieval'} < {'Medical office Receipt', 'Medical office info., 'Medical info. Retrieval'})

^ inclusive_role('nurse', 'doctor')= nurse < doctor

= TRUE ^ FALSE → FALSE

단계 5의 결과가 FALSE이므로 SP2의 Nurse는 Alice의 의료정보를 획득하지 못한다. 즉 제안된 모델은 프라이버시 허가와 거부여부를 정책으로 기술하고 정책에 의해 정보의 소유자가 프라이버시 데이터를 인가함으로써 개인의 프라이버시를 보호한다.

6. 결 론

ID관리 시스템에서 개인정보 프라이버시란 통합 관리되는 개인 정보를 사용하기 이전에 정보의 소유자에게 허가 받아야 하며 반드시 허가된 범위 안에서만 개인정보를 사용하도록 제한해야 한다. 본 논문은 접근제어 처리를 이용하여 ID 관리시스템에서의 프라이버시 보안 모델을 제안하고 특성을 논의했다. 이후 모델을 위한 접근통제 절차를 제안하고 모델을 적용하기 위한 IDMP의 시스템 구조를 보이고 모델을 따르는 정책 스키마를 제안했다. 끝으로 접근 통제 처리 과정을 설명하기 위해 ID관리 환경을 지원하는 의료관리 시스템에서의 접근통제 처리를 보였다.

제안된 프라이버시 보안 모델은 ID관리시스템 환경과 다양한 프라이버시 보호 기술이 필요한 개인정보보호 프레임워크에서 개인정보를 저장, 관리하는 정보 시스템의 개인정보보호 모델의 설계에 활용될 수 있을 것이다. 향후에는 모델에 D를 지원하도록 확장하고 제안된 모델이 단일 신뢰서클에 기반을 둔 동작만 규정하고 있으므로 다중 신뢰서클[3]을 수용할 수 있도록 확장한다. 또한 ID 관리 공간상에 노출될 수 있는 개인의 사생활 기록에 익명성[12]을 보장하도록 하고, 제안된 프라이버시 정책언어를 지속적으로 발전시켜 ID관리 환경의 다양한 개인정보 보호를 위한 표준화된 프라이버시 정책 기술언어로 발전시킬 계획이다.

참 고 문 헌

[1] "Identity Management Systems (IMS): Identification and Comparison Study," PRIME Project, 2003, http://www.daten-schutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Stu dy.pdf

[2] "Liberty Alliance: Introduction to the Liberty Alliance Identity Architecture," Liberty Alliance Project, 2003.

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

[4] Magnuson, G., Reid, P., "Privacy and Identity Management Survey," IAPP Conference, 2004.

[5] "Privacy and Security Best Practices," Liberty Alliance Project, 2003.

[6] J. Park and R. Sandhu, "The UCON(Usage Control Model)," ACM Transactions on Information and Systems Security, 2004.

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

[8] "PRIME: Privacy and Identity Management for Europe Date of preparation," PRIME Project, 2004, http://www.prime- projec-t.eu.org/

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

[10] "Microsoft .NET Passport,"Microsoft,

2004, http://www.microsoft.com/net/services/ passport/

[11] R. Agrawal and R. Srikant, "Privacy-preserving data mining," Proc. of the ACM SIGMOD Conference on Management of Data, 2000.

[12] Abdelmounaam Rezgui, Athman Bouguettaya, Mohamed Y. Eltoweissy, Virginia Tech, "Privacy on the Web: Facts, Challenges, and Solutions," IEEE Security and Privacy (Vol. 1, No. 6), 2003.

[13] Computer Science and Telecommunications Board (CSTB), "Who Goes There?: Authentication Through the Lens of Privacy," The National Academies, 2003. http://www.nap.edu/catalog/10656.html

[14] Lorrie Faith Cranor, "Web Privacy with P3P," AT&T, 2002.

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

[16] 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, 2003.

[17] "AT&T Privacy Bird," AT&T, 2004, http://www.privacybird.com

[18] "IBM Policy Editor," IBM, 2004, http://www.alphaworks.ibm.com/tech/p3peditor

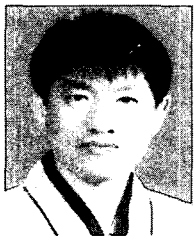
[19] P. Ashley, S. Hada, G. Karjoth, M. Schunter, E-P3P, "Privacy Policies and Privacy Authorization," WPES, November 2002.

[20] 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/

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

◐ 저 자 소 개 ◑

최 향 창 (Hyang-Chang Choi)
2002년 전남대학교 대학원 전산학과 졸업(석사)
2005년 전남대학교 대학원 정보보호협동과정 졸업(박사)
2001년~현재 전남대학교 리눅스시스템보안연구센터 연구원
관심분야 : 침입탐지 시스템, 유비쿼터스 보안, 프라이버시 보호
E-mail : hcchoi@lsrc.jnu..ac.kr



노 봉 남 (Bong-Nam Noh)
1978년 전남대학교 수학교육과 졸업(학사)
1982년 KAIST 대학원 전산학과 졸업(석사)
1994년 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
E-mail : bongnam@chonnam.ac.kr

이 형 효 (Lee, Hyung Hyo)
1987년 전남대학교 전산학과 졸업(학사)
1989년 한국과학기술원 전산학과 졸업(석사)
2000년 전남대학교 대학원 전산학과 졸업(박사)
2001년~현재 원광대학교 정보·전자상거래학부 교수
관심분야 : 보안정책 및 보안모델, 유비쿼터스 보안, 프라이버시 보호기술
E-mail : hlee@wonkwang.ac.kr