情報保護學會論文誌
第16卷 第6號, 2006. 12

인터넷 환경용 정책 기반 프라이버시 인가 시스템*

최 향 창[1†], 박 희 만[1], 이 승 용[1], 노 봉 남[1], 이 형 효[2‡]

[1]전남대학교, [2]원광대학교

A Policy-based Privacy Authorization System in the Internet Environment

Hyang-chang Choi[1†], Hee-man Park[1], Seung-yong Lee[1],
Bong-nam Noh[1], Hyung-hyo Lee[2‡]

[1]Chonnam University, [2]Wonkwang University

요 약

인터넷에서 기업의 정보시스템은 기업이 보유하고 있는 개인정보와 다른 기업에 저장 유지되는 개인정보를 개인이나 기업의 이익을 위해 사용한다.

본 논문은 개인정보 제공자인 사용자와 개인정보 활용자인 기업의 프라이버시 정책을 기반으로 개인정보에 대한 접근을 통제하는 프라이버시 인가 시스템을 설계하고 구현한다. 제안된 프라이버시 인가 시스템은 OASIS에서 제정한 인가정책 기술언어 표준인 XACML을 이용하여 프라이버시 보호 정책을 기술한다. 프라이버시 인가시스템은 XACML 1.0 스펙과 일부 XACML 2.0 스펙을 구현한 Sun사의 SUNXACML 1.2 패키지를 수정 및 확장하여 프라이버시 인가 시스템은 구현되었으며 프라이버시 보호 정책 설정과 점검을 위한 GUI 개발 도구 및 시험 도구도 함께 개발되었다.

ABSTRACT

In the Internet era, enterprises want to use personal information of their own or other enterprises' subscribers, and even provide it to other enterprises for their profit.

In this paper, a privacy authorization system for personal information based on privacy policies of users and enterprises is designed and implemented. Privacy policies of users and enterprises are described in XACML. Also, components of policy in XACML 2.0 such as Purpose, Obligation are suitable for expressing privacy policy. A prototype of privacy authorization system is implemented by modifying and extending the SUNXACML 1.2, a Sun's implementation of XACML 1.0 and some features of XACML 2.0, and GUI tools for composing and verifying are also developed.

Keywords : *Privacy Protection, Access Control, Authorization System*

Ⅰ. 서 론

인터넷을 기반으로 비즈니스를 수행하는 기업의 정보 시스템들은 가입자들의 사용 편의를 위해 개인정보(personal information)를 기업의 정보 시스템에 저장·운용한다. 이 개인정보는 정보 소유자

접수일: 2006년 7월 26일 ; 채택일: 2006년 10월 2일
* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (IITA-2006-C1090-0603-0027).
† 주저자, hcchoi@lsrc.chonnam.ac.kr
‡ 교신저자, hlee@wonkwang.ac.kr

가 허용하는 목적에 의해서만 수집·사용됨이 원칙이다. 하지만 기업과 개인의 입장 차로 기업에 의해 개인의 프라이버시가 무시되는 사례가 발생한다[1,2]. 따라서 개인에게 많은 편리와 장점을 제공하는 정보 시스템이라도 프라이버시(privacy)가 보호되지 않는다면 개인의 정보 시스템 이용률은 하락될 수 있다.

개인정보 보호를 위해 전통적인 보안 기술만을 이용하면 개인의 프라이버시가 지켜질 수 없다. 왜냐하면, 보안은 개인의 입장보다는 정보 시스템 자체의 보호를 최우선으로 하기 때문이다. 하지만 프라이버시는 개인정보에 대한 접근 여부를 결정하는 과정(authorization)에서 개인정보 소유자가 주도권을 가지고 결정하는 점에서 전통적인 보안과 차이점이 있다[3,-6]. 이 때문에 개인과 기업들은 개인정보 인가 결정을 수행하는 과정에서 충돌할 수 있다. 예를 들어 전자 상거래 시스템이 광고 목적으로 사용자의 거래 내역을 분석하여 사용자의 물품 선호 패턴을 분석한다면 기업(enterprise)의 입장에서는 효과적이나 개인(personal user)의 입장에서는 프라이버시 침해로 느낄 수 있다[4,6].

본 논문은 위와 같은 문제를 해결하기 위해 정보 시스템을 운용하는 기업의 입장과 개인정보를 제공하는 개인의 입장을 모두 참조하여 효과적으로 개인정보의 인가를 제공할 수 있는 프라이버시 인가 시스템을 설계하고 구현한다. 제안하는 프라이버시 인가 시스템은 PIMS(Privacy-enhanced model for Identity Management System)[7] 모델에 기반을 둔다. 특히, XACML 1.0 스펙[8]과 일부 XACML 2.0 스펙[9]을 구현한 SUN사의 SUNXACML 1.2 패키지[10]를 수정 및 확장하여 프라이버시 보호 시스템을 구현하였으며 프라이버시 보호 정책 설정과 점검을 위한 GUI 개발 도구 및 시험 도구도 함께 개발되었다.

본 논문의 2장에서는 인터넷 환경을 위한 프라이버시 보호 시스템을 제안하기 위해 개인정보의 프라이버시를 정의하고 관련된 프로젝트와 관련 기술들을 고찰한다. 3장에서는 PIMS[7] 모델을 소개한다. 또한, 제안된 모델을 XACML 관련 기술[8,9]에 기반을 두어 프라이버시 보호 시스템을 설계한다. 4장은 설계된 내용에 기반을 두어 SUNXACML 1.2 패키지[10]를 확장하여 인터넷 환경에서 개인의 프라이버시를 보장하는 프라이버시 인가 시스템(privacy authorization system)을 구현한다. 끝으로 5장에서는 결론과 향후 연구 계획을 제시한다.

II. 관련연구

1. 프라이버시 정의 및 원칙

일반적으로 정보화 사회에서 프라이버시 위반은 디지털 식별 데이터의 사용으로 발생한다[4,6]. 이 디지털 식별 데이터들은 개인의 기본 정보를 담고 있으며 정보 시스템 서비스에서 이용된다. 따라서 정보 시스템을 사용하는 과정에서 개인정보를 프라이버시 의무 없이 허가한다면 개인의 프라이버시는 침해될 수 있다. 이 문제를 해결하기 위해서는 개인정보 인가에 있어서 프라이버시 보호 원칙을 준수하도록 해야 한다[1,11].

프라이버시는 어떤 특정 개인이나 단체와 관련된 정보가 누출되었을 때 개인이나 단체가 감수해야 할 물질적인 손실뿐만 아니라 정신적인 피해가 발생되지 않아야 함을 권고하고 있다[3]. 또한 이를 기반으로 지켜야 할 프라이버시 원칙들도 제공한다[11]. 1980년에 경제개발 협력 기구(OECD)는 "사생활 정보 보호와 개인정보의 국제적 유통에 관한 개인정보 보호의 8원칙"을 규정했다. 모든 개인정보는 적법하고 정당한 절차에 의해서만 수집되고 데이터 소유자에게 정보의 수집을 통지하여 접근과 사용에 대한 동의를 얻도록 하는 정보 수집(collection information)의 원칙, 개인정보를 사용할 때 사용 목적에 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 목적 명확화(purpose specification)의 원칙, 개인정보가 정보 주체의 동의나 법률에 의해 정해진 것 외에는 다른 목적으로 사용되지 않도록 하는 이용 제한(use limitation)의 원칙, 개인정보의 분실이나 불법적인 접근, 파괴와 불법 사용, 변조, 공개 등의 위협으로부터 적절하게 보호되도록 하는 안전 보호(security safeguards)의 원칙, 개인 정보 처리를 위한 정보 시스템의 활용 정책을 일반인에게 공개(openness)하도록 하는 원칙, 정보의 소유자가 개인정보를 확인할 권리를 가지며 정보의 접근을 통지 받을 수 있고 필요에 따라서 정보를 파기, 정정, 수정 요구가 가능하도록 하는 개인 참여(individual participation)의 원칙, 정보 관리자가 원칙을 이행할 책임(accountability)을 갖도록 하는 원칙들을 제공한다[1,11].

2. 프라이버시 프로젝트 및 보호 기술

개인정보 프라이버시 보호를 제공하는 대표적인 프로젝트는 RAPID(Roadmap for Adv anced research in Privacy and Identity management)[12], PRIME(Privacy an d Identity Management for Europe) [13]이 있다. RAPID 는 PIM (Privacy and Identity Management)분야의 연구 주제를 결정하고 이 분야의 연구 주제들을 결정함으로써 EU 연구 커뮤니티를 활성화하는 것을 목표로 하는 프로젝트이다. 또한 현재 수행 중인 PRIME 프로젝트는 유럽의 주요한 연구 단체들을 중심으로 W3C등 주요 표준화 기관과 연계된 개인의 프라이버시 보호를 위한 프로젝트다[13].

〔표 1〕 프라이버시 보호 기술의 분류

분류		기술 예
클라이언트 기반	개인 컴퓨터용 방화벽	Sygate
	사용자 자취 제거	No Trace
	익명 E-mail 발송 시스템	Babel
	익명 시스템	Crowds, Onion Routing, Tarzan
서버 기반	가상사설망	Cisco VPN
	서버용 방화벽	Cisco Firewall
클라이언트 서버기반	프라이버시 자동 협상 시스템	P3P, E-P3P
	암호 기반 솔루션	PGP

프라이버시 보호 기술들은 〔표 1〕과 같이 분류될 수 있다[2]. 이중 클라이언트 기반 기술들은 개인 사용자가 자신의 프라이버시를 보호하기 위해 사용할 수 있는 기술들이며 서버 기반 기술들은 서버 시스템에 속해있는 보안 관리자나 프라이버시 관리자가 운용하는 기술들이다. 이들을 병합한 기술이 클라이언트 서버 기반 기술이다. 이중 프라이버시 보호 원칙을 따르는 대표적인 기술에는 P3P(Platform for Privacy Preferences)[15-17] 와 E-P3P(The Platform for Enterprise Privacy Practices)[18]가 있다. E-P3P는 기업의 입장에서 개인정보의 프라이버시를 보호하기 위한 모델을 정의하고 있으며 기업의 정보시스템에 저장된 개인정보의 프라이버시를 보장하기 위해 프라이버시 보호 정책에 따라 인가를 수행한다. 이 프라이버시 정책은 프라이버시 원칙을 반영한 EPAL[14]로 기술된다.

3. 정책기반 프라이버시 보호 해결방안

인터넷 환경의 정보 시스템에서 개인들의 프라이버시 보호를 보장하기 위해서는 개인정보 보호가 요구된다. P3P와 E-P3P는 사용자 참여를 최소화하면서 개인의 프라이버시를 보호하기 위해 프라이버시 자동 협상 기능을 제공하는 좋은 해법이다. 이 기술들은 개인정보 보호를 제공하기 위해 프라이버시 정책 기반 접근 제어 기술을 사용한다[14,15,18].

프라이버시 개념이 포함되지 않은 시스템 정책들은 P3P와 E-P3P에 의해 생성된 프라이버시 정책과는 서로 다르다[1,15,18]. 일반적으로 보안 관리자에 의해 생성된 시스템 정책이 시스템에 보안 기능은 제공하지만 프라이버시 정의와 원칙에 기반을 두어 설정되지 않아서 프라이버시를 위반할 수 있다[4,6]. 왜냐하면, 프라이버시는 정보 소유자 각자의 프라이버시 민감도를 고려하여 집행해야 프라이버시가 보장되나 정보 시스템의 보안 관리자가 기업의 안전과 경영 효과 측면에 우선하여 집행하기 때문이다[1-3]. 따라서 기업의 정보 시스템에 접속하는 인가되지 않은 접근으로부터 정보 시스템에 저장 유지되는 개인정보 자원을 방어할 수는 있지만 정보 시스템 내부적으로 기업의 이득을 위해서 허용된 개인정보의 사용은 허가될 수 있다. 하지만 이는 기업의 입장에서 개인정보가 인가될 수 있는 근본적인 위협을 가지며 개인의 프라이버시를 침해하는 사례들로 나타난다[4,6].

이런 프라이버시 문제를 근본적으로 해결하기 위해 제안하는 시스템은 개인과 기업들 간에 서로 독립적인 프라이버시 정책을 유지하도록 한다. 인가를 위해 사용되는 프라이버시 보호 정책은 P3P와 E-P3P와 같이 프라이버시 정의와 OECD 가이드라인을 정책에 반영할 수 있도록 개인정보 사용 목적과 의무 등이 제공된다. 즉 정책을 수립할 때 프라이버시를 고려해서 작성해야 하기 때문에 프라이버시의 근본 측면이 고려될 수 있다. 예를 들어 P3P는 웹사이트에 의해 개인정보가 기업의 정보 시스템으로 임의로 제공되는 것을 막기 위해 프라이버시 선호(preference)를 설정할 수 있다[16]. 또한, E-P3P는 기업에 저장 유지되는 개인정보의 사용 동안 안전함을 제공하기 위해 EPAL로 프라이버시 보호 정책을 기술하여 프라이버시를 보호한다[14]. 그리고 개인정보가 인가되는 상황에 기반을 두어 정보제공자와 정보소유자간에 정책을 조율하고, 만약 정책이 충돌한다면 해결 규칙(resolution rules)에 의해 프

라이버시 정책들 간에 충돌을 해결한다.

Ⅲ. 프라이버시 인가시스템 설계

1. PIMS 모델(7)

PIMS 모델은 개인정보를 사용하는 측면과 제공하는 측면의 서로 다른 입장을 고려해 ID관리 시스템의 프라이버시 보호 모델이다. PIMS 모델의 모든 관련 구성 요소는 SSO(Single Sign-On) 환경을 지원하도록 제안되었다[7].

인터넷 환경은 다양한 웹 정보 시스템들과 다양한 인터넷 프로토콜을 사용하는 응용들로 구성되며, 대표적인 응용들로는 WWW(World Wide Web), FTP(File Transfer Protocol), Telnet, E-mail 등이 있다.

〔그림 1〕 정보 관리에 기반을 둔 인터넷 환경

인터넷 환경은 다양한 서비스들을 이용하는 가운데에서 〔그림 1〕과 같이 개인 정보를 이용한다. 이 정보들은 정보들의 제공자(Information Provider)임을 의미하는 개인정보 소유자와 정보 사용자(Information Consumer)임을 의미하는 개인정보 소비자가 존재한다. 이러한 정보 자원들은 다양한 인터넷 프로토콜로부터 이동된다. 본 논문에서는 PIMS 모델의 환경을 통합 ID관리 환경으로 한정시키지 않고 인터넷 환경에 적용할 수 있는 구성요소들을 제안한다.

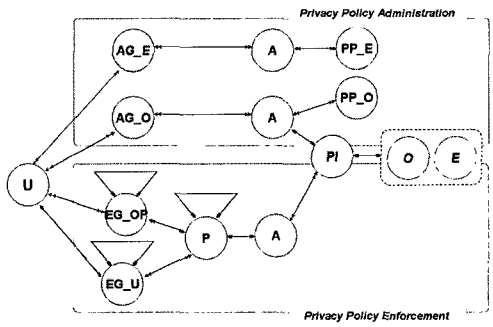
〔그림 2〕에서 구성 요소들간에 데카르트의 곱 관계는 "↔" 기호의 화살표로 표현된다. 구성 요소들의 계층 관계를 표현할 때 데카르트 곱 관계 표시인 "↔" 기호를 재귀적으로 표현한다. 예를 들어 〔그림 2〕에서 계층 관계를 갖는 구성 요소는 EG_OP, EG_U이다. 또한 O는 P3P나 E-P3P에서 정의된 의무(Obligation)를 의미하며 E는 XACML에서의 결과(Effect)를 의미한다.

〔그림 2〕에서 프라이버시 보호 정책을 설정하고 관리하는 측면은 프라이버시 정책 관리(privacy policy administration)모델 부분이고, 정책에 기반을 두어 개인정보를 인가하는 측면은 프라이버시 정책 수

〔표 2〕 프라이버시 보호 모델의 주요 구성요소

구성요소	정의 및 의미
U (Users)	개인정보에 접근을 원하는 모든 사용자들의 집합, 즉 접근통제 구성요소 중 개인정보에 접근하려는 주체들을 의미함
G (Groups)	U가 속할 수 있는 그룹들의 집합을 의미함 G = *AG_E ∪ AG_O ∪ EG_OP ∪ EG_U*
AG_E	정보시스템에서 프라이버시 보호 역할을 수행중인 도메인 프라이버시 관리자
AG_O	정보시스템에 개인정보를 제공하는 실체이며 개인정보의 소유권을 가지는 사용자의 집합을 의미함. 즉 AG_O는 기업의 정보시스템에 가입하여 개인정보를 제공하는 주체들을 의미함
EG_OP	정보시스템에 관련된 내부적인 개인정보 운영자들의 집합. 단 EG_OP는 개인정보를 내부적으로 운영하거나 가공 관리 목적으로 사용하는 주체
EG_U	인터넷 환경에서 기업 정보시스템이 제공하는 서비스를 소비하는 주체이며 이들은 정보시스템을 이용하는 개인사용자에서부터 기업들까지 다양하게 분류될 수 있음. PI_U가 서비스를 소비하는 과정에서 개인정보의 사용이 발생됨
PI(Personal Information)	PI_U가 제공한 개인정보의 집합을 의미함, PI_U는 개인정보 자원으로써 U 또는 G에 의해서 사용됨.
P (Purposes)	PI를 사용하는 이용 목적들의 집합. 예) P = *{Credit_inquiry, Marketing, Advertising}*
A(Access modes)	PI에 대한 접근 연산들의 집합. 예) A = *{r, w, c, d}*, *r: read, w: write, c: create, d: delete*
E (Effects)	프라이버시 정책에 따른 개인정보 요청처리 결과 E = *{ permit, deny, indeterminate, not applicable }*
O (Obligations)	P에 의해 PI가 U나 G에 의해 사용될 때 만족해야 할 의무들의 집합을 의미함

행(privacy policy enforcement)모델 부분이다[21]. 이 모델은 개인의 서로 다른 선호(preference)를 반영한 프라이버시 보호 정책을 이용하여 개인정보 보호를 수행하기 위해 접근 제어를 수행한다. 본 모델에서는 하나이상의 COT(circle of trust)를 수용하기 위해 정보제공자를 기준으로 하나로 묶일 수 있는 단일한 COT영역을 도메인으로 표현 한다.



〔그림 2〕 웹 환경을 위한 프라이버시 보호 모델

프라이버시 보호 모델 구성 요소의 세부 정의 및 의미는 〔표 2〕와 같다.

제안된 모델은 관리의 효율성을 위해 그룹(G) 개념을 도입한다. G는 관리 그룹(AG_E, AG_O)과 실행 그룹(EG_OP, EG_U)으로 구성된다. 이중 AG_E와 AG_O는 개인정보를 관리하는 주체들이 속할 수 있는 그룹이며 EG_OP와 EG_U는 개인정보를 사용하는 주체들이 속할 수 있는 그룹이다. 개인정보 소유자의 필요에 따라서 G는 U를 그룹 단위로 관리하고 개인정보를 사용하는 특정 개체의 표현도 동시에 제공할 수 있어야 한다. 본 논문은 이러한 점을 고려하여 구현 부분에서 G를 URN(Uniform Resource Names)[20]으로 표기하여 이를 해결한다.

〔그림 2〕 모델에서 프라이버시 인가를 수행할 때 사용되는 개인정보 보호 정책은 〔표 3〕과 같다. PP_E는 기업의 정보 시스템에서 개인정보를 관리하는 기업의 프라이버시 보안 관리자가 설정한 프라이버시 정책이며 PP_O는 개인정보 소유자가 설정한 프라이버시 정책이다. PP_E와 PP_O의 차이점은 기업과 개인이라는 입장이 다르므로 프라이버시 정책의 집행자가 다르다. PP_E는 기업의 정보 시스템에 유지되는 다양한 개인정보를 통합 관리해야 하므로 기업의 정보 시스템에 속해있는 다양한 개인들의 세부적인 선호(preference)를 반영하기 어렵다. 따라서 PP_E는 개인의 특성을 일괄적으로 고려하여 설정된 프라이버시 정책으로 기업에 의해 집행되는 E-P3P의 정책 구조와 유사하다[18]. 이와 반해서 PP_O는 정보 소유주인 주체가 개인의 선호에 기반을 두어 집행하는 P3P의 정책 구조와 유사하다[15].

본 논문에서 프라이버시 보호정책은 〔표 3〕과 같은 구조를 따르면서 〔표 4〕와 같이 구분된다. 정책 중 PP_E에 해당하는 정책은 도메인 정책, 도메인 예외정책이며 PP_O에 해당되는 정책은 디폴트 사용자 정책, 사용자 정책이다. 이들의 분류기준은 개인정보를 관리하는 정보시스템과 개인정보 소유자 측면이 반영되었다.

프라이버시 정책 중 사용자 정책 (UP: User Privacy Policy)은 개인정보 소유자가 자신의 개인정보(PI)에 대한 사용허가 조건들로 구성된다. 디폴트 사용자 정책 (DUP: Default User Privacy Policy)은 도메인 프라이버시 관리자가 미리 설정해 놓은 프라이버시 정책으로, 사용자 정책이 설정되지 않은 개인정보에 대해 적용되는 정책이다. 개인정보 소유자는 Very High(VH), High(H), Medium(M), Low(L) 보안수준의 디폴트 사용자 정책을 선택함으로써 보안정책이 설정되지 않은 자신의 개인정보를 보호할 수 있는 장점이 있다. 도메인 정책 (DP: Domain Privacy Policy)은 도메인 또는 COT에 포함된 개인정보 사용자들이

〔표 3〕 프라이버시 보호 정책 구성요소

정책 유형		정 의
PP		PP = *PP_E* ∪ *PP_O*, 프라이버시 정책의 집합
	PP_E	*AG_ E*가 생성한 프라이버시 보호 정책의 집합 PP_E = *(U* ∪ *G)* × *PI* × *P* × *A* × *E* × *O*, *subject* × *resource* × *purpose* × *access_mode* × *effect* × *obligation*
	PP_O	*AG_ O*가 생성한 프라이버시 보호 정책 집합 PP_O = *(U* ∪ *G)* × *PI* × *P* × *A* × *E* × *O* *subject* × *resource* × *purpose* × *access_mode* × *effect* ×*obligation*

〔표 4〕 프라이버시 정책 유형

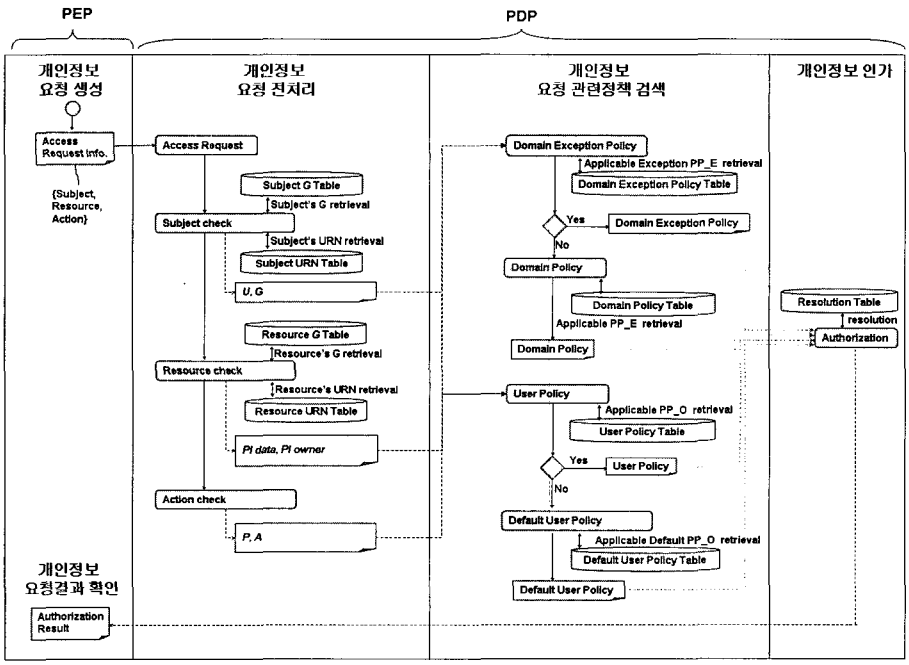
명칭	디폴트 사용자정책	도메인정책	도메인 예외정책	사용자정책
정의	DUP: User의 Default PP_O	DP: Domain의 PP_E	DEP: Domain의 Exception PP_E	UP: User의 PP_O
정의주체	도메인 프라이버시 관리자	도메인 프라이버시 관리자	도메인 프라이버시 관리자	개인정보 소유자
설정주체	개인정보 소유자	도메인 프라이버시 관리자	도메인 프라이버시 관리자	개인정보 소유자
정책 내 Subject	모든 Subject	단일 Subject 또는 Subject 그룹	단일 Subject 또는 Subject 그룹	단일 Subject 또는 Subject 그룹
표현방법	XACML	XACML	XACML	XACML

개인정보를 사용할 수 있는 조건들로 구성되며 도메인 프라이버시 관리자에 의해 정의된다. 도메인 예외정책 (DEP: Domain Exception Privacy Policy)은 다른 프라이버시 정책에 우선하여 적용되는 정책으로 도메인에 포함된 특정 개인정보 사용자의 개인정보 접근금지 등이 긴급히 필요한 예외적인 경우에 사용된다.

2. 프라이버시 인가 시스템

제안된 시스템은 〔그림 2〕에서 정의한 프라이버시 인가 모델을 따르며 주요 구성 모듈 및 인가 흐름은 〔그림 3〕과 같다. 프라이버시 인가 시스템은 〔그림 2〕에서 제안한 모델과 같이 프라이버시 관련 정책을 관리하는 부분과 프라이버시 관련 정책을 인가하는 부분으로 나뉜다. 프라이버시 인가를 위해서는 프라이버시 정책 설정 및 관리가 요구된다. 이 프라이버시 관련 정책은 〔표 3〕에서 정의된 정책 구조를 따라서 XACML을 이용하여 작성된다.

〔그림 3〕에 나타난 프라이버시 인가시스템의 PEP (Policy Enforcement Point)는 개인정보 요청생성과 개인정보 요청 결과 확인으로 이루어



〔그림 3〕 프라이버시 인가시스템 구조

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Request xmlns="urn:oasis:names:tc:xacml:2.0:context" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  - <Subject>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authn-locality:dns-name"
        DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>urn:IDSP-ETRI:Highly_Trusted_Group:www.nhic.or.kr</AttributeValue>
      </Attribute>
    </Subject>
  - <Resource>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>urn:ETRI-PP:General_Identity:Name</AttributeValue>
      </Attribute>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:resource:resource-owner-id"
        DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>alice@lsrc.jnu.ac.kr</AttributeValue>
      </Attribute>
    </Resource>
  - <Action>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>read</AttributeValue>
      </Attribute>
    - <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:action:purpose" DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>marketing</AttributeValue>
      </Attribute>
    </Action>
  </Request>
```

〔그림 4〕 개인정보 요청 구조

지며 PDP(Policy Decision Point)는 개인정보 요청 전처리, 개인정보 요청 관련정책 검색, 개인정보 요청 인가과정으로 구성된다.

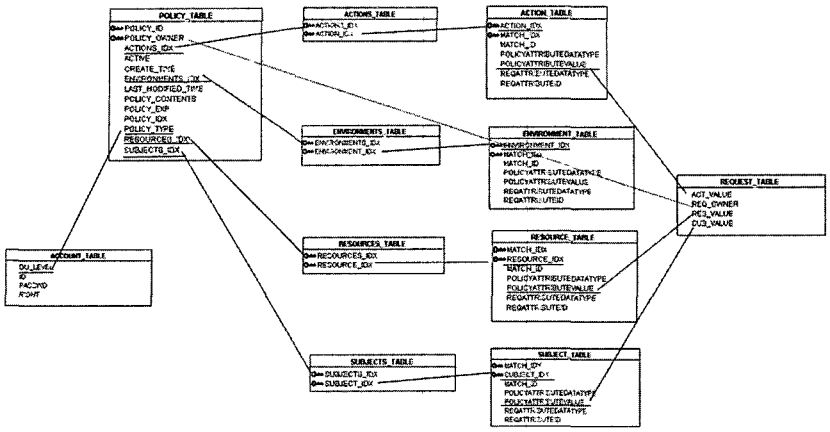
개인정보 요청 생성 단계(Step 1)는 개인정보를 필요로 하는 응용으로부터 접근 요청 정보(Access Request)를 생성한다. 이때 생성되는 접근 요청은 개인정보를 요청하는 주체(Subject: S)와 이 주체가 필요로 하는 개인정보 자원(Resource: R)과 이 자원을 어떻게 이용(Action: A)하겠다는 정보들로 구성된다.

〔그림 3〕의 S는 개인정보를 요청하는 사용자인 프라이버시 보호 모델의 U ∪ G를 의미한다. 또한 R는 주체가 접근하려는 PI를 의미한다. 이 PI는 개인정보인 자원 자체를 의미하는 {PI data}와 이 자원의 소유주를 나타내는 {PI owner}로 구성된다. 〔그림 4〕는 PEP에서 생성한 XACML로 표현된 개인정보 요청을 나타내고 있다. 개인정보 접근 주체인 S와 개인정보 R은 URN 표기법을 이용하여 표현되며 단일 정보뿐만 아니라 그룹 단위도 주체와 자원을 지정할 수 있는 장점을 제공한다[22].

개인정보 요청 처리 전처리 단계 (Step 2)는 접근요청 구성요소 중 〈Subject〉 엘리먼트와 주체 그룹 테이블(Subject G Table), 주체 URN 테이블(Subject URN Table)을 비교하여 개인정보 요청주체인 U를 찾아내고 〈Resource〉 엘리먼트와 자원 그룹 테이블(Resource G Table), 자원 URN 테이블(Resource URN Table)을 비교하여 PI data를 얻어낸다. PI owner는 〈Resource〉 엘리먼트의 속성에서, 접근연산 A와 접근목적 P는 〈Action〉 엘리먼트에서 각각 추출한다.

개인정보 요청 관련정책 검색 단계 (Step 3)는 U, PI data, PI owner, P, A로 구성된 개인정보 요청 허가여부를 결정하는 데 필요한 프라이버시 정책인 PP_E, PP_O를 추출한다. PP_E는 〔표 4〕에서 DEP와 DP를 의미하고 PP_O는 UP와 DUP를 의미한다. 기업에 저장 유지되는 개인정보를 기업의 입장에서 어떻게 사용하겠다는 것을 나타낸 정책인 도메인 정책인 DP와 이러한 도메인 정책 중 사용자 정책인 UP를 추출한다. DP는 기업의 정책 집합을 의미하는 PP_E로부터 추출되고 개인정보 요청 정보 관련 정책인 DP와 개인정보 소유자의 개인정보 보호 정책인 UP를 검색한다. 동작 절차를 요약하면 step 3은 단계 2에서 처리된 정보를 기초로 관련된 프라이버시 정책을 검색한다. 기업의 정책 검색 처리는 DEP Retrieval과 DP Retrieval 모듈에 의해서 수행된다. UP는 step 2에서 요청하는 개인정보에 대한 소유자에 관한 정책만을 검색한다. DUP가 필요한 이유는 사용자 정책 검색 처리에서 해당되는 UP가 존재하지 않을 때 DUP가 UP를 대신하기 위해서다. 정책 검색에서 개인정보 요청과 관련된 정책이라면 Step 2에서 얻은 〔그림 3〕의 S, R, A가 일치하는 정책을 의미한다.

개인정보 인가 단계 (Step 4)는 Step3에서 검색된 정책을 기반으로 인가를 결정하는 단계이다. 이 단계 중 첫 번째는 동일 정책 간에 충돌 해결 규칙을 통해 충돌을 해결한다. 두 번째는 정책의 종류별로 얻은 각각에 결과에서 충돌을 해결하여 하나의 결과로 조율한다. 인가 결정은 검색된 개인과 기업의 프



〔그림 6〕 개인정보와 프라이버시 정책 데이터베이스 구조

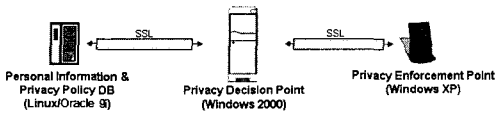
라이버시 정책을 조율한다. 만약 검색된 정책들 간에 충돌이 발생된다면 이 정책들은 충돌 해결 규칙(Resolution Rule Table)에 의해서 충돌은 해결된다. 충돌 해결 규칙에는 도메인 정책 우선, 소유자 정책 우선, 금지 우선, 허용 우선이 있다. 이중 도메인 정책 우선, 사용자 정책 우선은 도메인 정책을 의미하는 정보 시스템의 프라이버시 정책과 소유자 정책을 의미하는 사용자간에 정책 충돌을 해결할 목적으로 존재한다. 또한 다른 유형인 금지 우선 허가 우선 규칙은 두 정책들이 충돌할 때 정보 시스템과 소유자간에 관계없이 금지와 허가 측면의 정책의 요소에서 어떤 결과(Effect)를 더 우선시 할 것인가를 위해 존재한다. 예를 들어 금지 우선이면 Effect의 값이 'Deny'인 것을 우선하며 허가 우선이면 'Permit'을 우선하여 정책 충돌을 해결한다.

Ⅳ. 프라이버시 인가시스템 구현

1. 프라이버시 인가시스템 모듈구현 및 수행환경

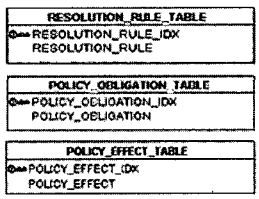
프라이버시 인가 시스템의 동작 및 시험환경은 〔그림 5〕와 같다. 각 시스템들 간의 통신은 도청자(eavesdropper)로부터의 스니핑 공격(sniffing attack)에 대응하기 위해 SSL(Secure Sockets Layer) 프로토콜에 기반을 둔다.

이 시스템 환경 중 개인정보와 프라이버시 정책 데이터베이스(Personal Information & Privacy Policy DB)는 개인정보와 개인정보 보호 정책을 〔그림 6〕과 같은 구조로 유지 관리한다.

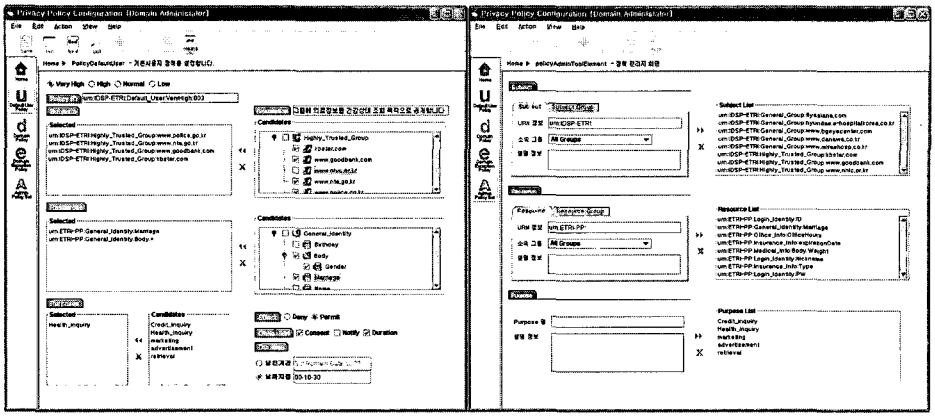


〔그림 5〕 프라이버시 인가 시스템 구축도

〔그림 5〕에서 프라이버시 결정점(Privacy Decision Point: PDP)은 개인정보의 인가를 결정하는 기능을 담당하는 모듈을 제공한다. 프라이버시 실행점(Privacy Enforcement Point: PEP)은 개인정보를 이용하는 사용자로부터의 개인정보 요청을 받아 PDP로 접근허가 여부를 묻고 그 결과에 따라 개인정보에 대한 연산을 실행하는 기능을 담당한다. 이 시스템들에서 사용되는 각 모듈들은 Sun사의 XACML 1.2 패키지를 수정하여 Java언어로 구현되었다. PDP는 PEP로 받은 개인정보 요청을 처리하기 위해 다양한 기능들을 수행하며 이를 위해 정책 충돌 해결 규칙(policy resolution rule)과 정책에 대한 권고적인 의무(obligation), 결과(effect) 관련 정보들을 각각 그림 7의 Resolution rule, Obligation, Effect 테이블에 각각 유지된다.



〔그림 7〕 Resolution, Obligation, Effect 구조

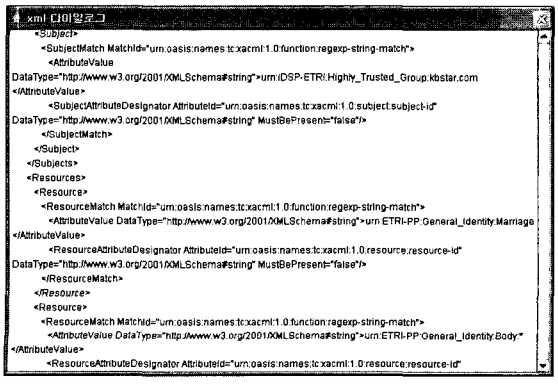


〔그림 8〕 프라이버시 정책관리자 GUI

PEP에서는 개인정보 소유자와 프라이버시 정책 관리자가 프라이버시 보호 정책, 개인정보 데이터를 입력, 수정, 삭제, 조회할 수 있는 GUI화면 인터페이스를 제공한다.

이것은 정책간 충돌 해결, 인가 결과를 개인정보 인가를 요청한 PEP에게 전달하기 위한 모듈도 제공된다. 〔그림 8〕은 프라이버시 정책 관리자를 위한 정책 설정 GUI와 각 정책 구성 요소의 관리 화면의 일부를 보인다. 즉 도메인 예외 정책을 설정할 때 도메인 관리자는 정책 설정 GUI만을 통해 정책을 설정할 수 있다.

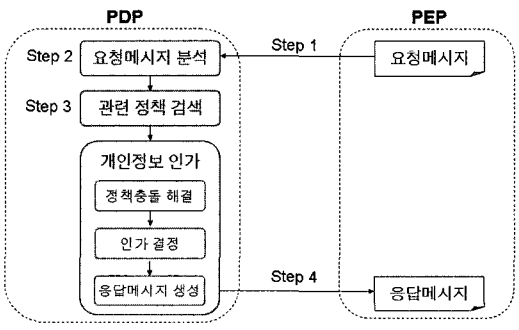
이 정책 설정 GUI 도구는 도메인 관리자가 도메인 예외 정책으로 설정할 수 있는 최대한의 정책들을 기준으로 하여 한정된 설정 범위를 초과하지 않도록 하는 기능을 제공한다. 이렇게 설정된 정책은 〔그림 9〕의 XACML형태로 생성되며 각 요소는 개인정보와 프라이버시 정책 데이터베이스에 저장 유지된다.



〔그림 9〕 프라이버시 정책관리자 GUI 정책 예

2. 프라이버시 인가시험

프라이버시 인가 절차 동작 순서는 〔그림 10〕과 같다. 〔그림 10〕은 〔그림 5〕의 시스템 환경에서 〔그림 3〕을 구현한 동작 절차를 의미한다. 이중 PEP는 요청된 개인정보를 XACML형태의 요청 메시지를 생성하여 PDP에게 개인정보 인가를 요청한다. 이후 프라이버시 컨트롤러는 요청 받은 메시지를 분석해서 관련된 정책을 〔그림 6〕의 개인정보와 프라이버시 정책 데이터베이스가 구축된 시스템과의 접속을 수행해서 요청 정보에 상응하는 정책을 검색하고 검색된 정책에 기반을 두어 〔그림 3〕의 흐름으로 정책 충돌 해결 및 인가 결정, 응답 메시지의 생성을 절차적으로 수행한다. 수행된 개인정보 인가 결과는 응답 메시지로 변환되어 프라이버시 인가를 요청한 주체인 PEP에게 전송된다.



〔그림 10〕 개인정보 인가절차

〔표 5〕 도메인 정책 예

Privacy Policy	Subject	Resource	Purpose	Effect	Obligation
D1	ALL	GI:Name, GI:ID, LI:Nickname	ALL	P	
D2	HTG	GI, CI, LI	ALL	P	
D3	HTG	FI, II	CI	P	C, N
D4	HTG	MI	HI	P	C
D5	TG	GI, CI	ALL	P	N
D6	TG	FI, II	CI	P	C
D7	GG	FI, II, MI	ALL	D	N
D8	flyasiana.com	II	HI	P	C, N
DE1	TG	FI	ALL	D	N

〔표 6〕 디폴트 사용자 정책 예

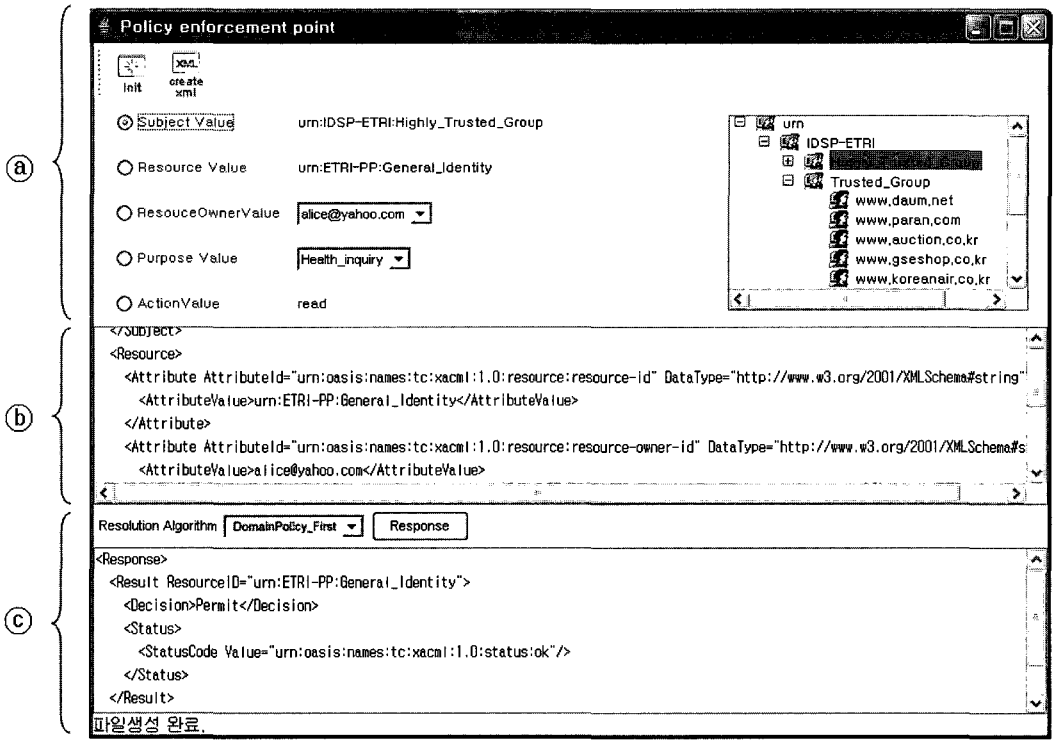
Privacy Policy	Subject	Resource	Purpose	Effect	Obligation
DU_VH1	HTG	GI, CI, LI	ALL	P	N
DU_VH2	HTG	FI, II	CI	P	C, N
DU_VH3	HTG	MI	HI	P	C, N
DU_H1	TG	GI, CI, LI	ALL	P	N
DU_H2	TG	FI, II	CI	P	C, N
DU_H3	TG	MI	HI	P	C, N
DU_M1	GG	GI, CI, LI	ALL	P	N
DU_M2	GG	FI, II	CI	P	C
DU_M3	GG	MI	HI	P	C
DU_L1	GG	GI, CI, LI	ALL	P	
DU_L2	GG	FI, II	CI	P	N
DU_L3	GG	MI	HI	P	N

〔표 7〕 Alice의 사용자 정책 예

Privacy Policy	Subject	Resource	Purpose	Effect	Obligation
U_Alice1	HTG	MI	ALL	D	C, N
U_Alice2	TG	MI, FI	ALL	D	C, N
U_Alice3	GG	GI	ALL	P	N

※ 범례(〔표 5〕 ~ 〔표 9〕)

- o Privacy Policy: 프라이버시 정책의 종류 = {D, DE, DU, U}, 각각의 정의는 〔표 4〕의 정의와 같고 정책의 종류 뒤에 오는 숫자는 정책에 고유하게 부여된 식별 번호를 의미한다.
- o Subject: 개인정보를 요청하는 주체들로 구성된다. 각 주체는 그룹이나 특정 개체일 수 있음, 표에서 각각의 의미는 ALL= 누구나 상관없음, HTG, TG, GG는 신뢰의 정도에 따라 정량화된 값을 의미한다. 예를 들어 Subject가 될 수 있는 각 개체는 HTG, TG, GG에 속할 수 있다. 신뢰단계는 HTG가 가장 높고 다음으로 TG, 가장 낮은 신뢰를 갖는 GG순이다. 그룹이 아닌 특정 개체의 지정은 특정 개체 식별이 가능한 URL로 표현된다.
- o Resource: 개인정보를 의미하며 각각은 URN으로 표현된다. GI = General_Identity, LI = Login_Identity, CI = Contact_Info., FI = Financial_Info., II = Insurance_Info., MI = Medical_Info.
- o Purpose: 개인정보 사용목적을 의미한다. ALL = 어떤 목적이나 가능, CI = Credit_inquiry, HI = Health_Info_Inquiry, M = Marketing
- o Effect: 〔표 2〕의 E를 의미한다. P = Permit, D= Deny, I = Indeterminate, N = Not applicable
- o Obligation: 〔표 2〕의 O를 의미한다. 즉 개인정보 인가를 수행하는 동안 수반될 의무를 의미한다. C = Consent, N = Notify



〔그림 11〕 개인정보 인가 처리 결과 GUI

〔표 8〕 Alice의 개인정보 인가 시험 시나리오

No.	Subject	Resource Owner(Policy Level)/Resource	Purpose	Access mode
1	TG:www.paran1.com	alice(H)/General_Identity:SSN	M	read
2	GG:flyasiana.com	bob(M)/Financial_Info:CreditCard:expirationDate	CI	read
3	GG:flyasiana.com	bob(M)/Insurance_Info	HI	read
4	HTG:www.nhic.go.kr	alice(H)/Medical_Info:BloodPressure	HI	read
5	GG:www.flyasiana.com	alice(H)/Insurance_Info	M	read
6	GG:www.flyasiana.com	alice(H)/Insurance_Info	HI	read
7	TG:www.auction.co.kr	alice(VH)/Financial_Info:Bank:AccountNumber	CI	read

※ 범례(〔표 8〕)

- Access mode: 〔표 2〕의 A를 의미한다.

2.1 프라이버시 정책

프라이버시 인가 시험을 위해 사용된 프라이버시 정책들의 일부는 〔표 5〕, 〔표 6〕, 〔표 7〕과 같다.

〔표 5〕는 도메인 프라이버시 관리자가 설정한 DP와 DEP이다. 〔표 6〕은 도메인 프라이버시 관리자에 의해 설정된 디폴트 사용자 정책이다. 〔표 7〕은 개인정보의 소유자인 Alice가 설정한 Alice의 UP이다. 이들 각 정책은 〔그림 8〕처럼 제공되는 정책 관리 GUI를 통해 설정되었다.

2.2 개인정보 접근요청

개인정보 요청자는 개인정보 요청의 각 구성 요소를 지정하여 개인정보를 〔그림 11〕의 a의 세부 요소를 설정하여 요청한 후 XML 생성 버튼(Create xml)을 클릭하면 PEP는 XACML 형태의 개인정보 요청 구조를 생성한다. 이렇게 생성된 예는 〔그림 11〕의 b와 같다. 이 요청 정보는 〔그림 5〕의 PDP로 전달되고 PDP는 〔그림 3〕의 인가 결정 시나리오를 따르는 모듈의 수행으로 프라이버시 인가

〔표 9〕 Alice의 개인정보 인가 테스트 결과

No.	Result			Applicable Policy
	D(Obligation)	DE(Obligation)	U(Obligation)	
1	P(N)		P(N)	D5, DU_H1
2	D(N)		P(C)	D7,DU_M2
3	I(N)		N	D7, D8
4	P(C)		D(C, N)	D4, DU_H3, Alice1
5	I(N, C)		N	D7, D8
6	I(N, C)		N	D7, D8
7	P(C)	Deny(N)	D(C, N)	D6, DE1, Alice2

여부가 결정된다. 결정된 결과는 〔그림 11〕의 c의 XACML형태로 개인정보 요청자에게 반환된다.

본 논문에서 〔그림 11〕의 GUI도구를 이용하여 〔표 8〕의 개인정보 요청 시나리오에 대한 테스트를 수행했다. 〔표 8〕에서 Policy Level은 사용자가 설정한 디폴트 사용자 정책 보안수준을 의미한다.

2.3 프라이버시 인가 절차 및 결과

〔표 9〕는 〔표 8〕의 개인정보 인가 시험 시나리오들을 본 논문에서 제안된 프라이버시 인가 절차에 따라 수행한 결과를 나타내고 있다. 〔표 9〕의 적용가능 정책(applicable policy)은 개인정보 요청을 구성하는 주체(Subject), 개인정보(Resource), 이용연산(Action) 정보를 사용자/사용자 디폴트 사용자 정책, 도메인/도메인 예외 정책들과 비교하여 일치하는 프라이버시 정책들을 의미한다. 예를 들어 〔표 8〕의 1번 시나리오는 Subject인 TG:www.paran1.com 사이트가 개인정보 소유자인 Alice의 개인정보 General_Identity:SSN을 Marketing 목적으로 Read 연산을 요청한 경우이다. 프라이버시 인가 시스템은 Subject, Resource, Action 정보를 추출하여 〔표 5〕, 〔표 6〕, 〔표 7〕에 각각 정의된 도메인/도메인예외 정책, 디폴트 사용자 정책, Alice의 사용자 정책과 〔그림 3〕의 절차에 따라 비교 과정을 거친다.

비교 결과 도메인 예외 정책 중에는 적용가능 정책은 존재하지 않으며 도메인 정책 D5가 1번 시나리오 개인요청에 적용가능 정책으로 선택되었다. 이 때 정책적용 결과는 P(Permit)이며 수반되는 의무사항은 N(Notification)이다. 사용자 정책의 경우 Subject, Resource, Action 정보와 일치하는 정책이 존재하지 않으므로 사용자 디폴트 정책을 참조하게 된다. 이 때 Alice가 설정한 보안 수준이 H(High)이므로 DU_H1, DU_H2, DU_H3 중에서 적용가능 정책을 찾게 되는데 DU_H1이 선택되고 정책적용 결과는 P(Permit), 수반되는 의무사항은 N(Notification)으로 결정됨을 알 수 있다.

주어진 개인정보 접근요청에 대해 하나 이상의 적절한 정책들이 검색되는 경우 도메인정책우선, 사용자정책우선, Permit 우선, Deny 우선 등의 정책 충돌해결 규칙에 의해 인가여부가 결정된다.

V. 결 론

본 논문은 사용자로부터 제공된 개인정보를 저장, 활용, 관리하는 환경에서 발생할 수 있는 개인정보 침해 문제의 해결을 위한 개인정보 보호 모델을 제안하고 정책 기반의 개인정보 보호 시스템을 구현했다. 개인정보 보호 모델은 OECD와 미국 등 개인정보 보호 선진국에서 제정한 개인정보 보호에 관한 가이드라인과 원칙들을 반영하여 설계되었으며, 제안된 개인정보 보호 모델에는 보안 모델의 일반적인 구성 요소인 주체, 객체 외에 개인정보 보호에 필요한 구성 요소인 목적이나 의무 사항 등이 추가되어 개인정보 보호 원칙을 반영할 수 있는 특징을 가지고 있다.

또한 개인정보의 프라이버시 측면을 강화하기 위해 개인정보의 제공자와 개인정보를 관리하는 개인정보 관리자 별로 서로 다른 정책을 유지하도록 하는데 초점을 맞추어 개인정보 보호 정책을 도메인, 도메인 예외, 디폴트 사용자, 사용자 정책으로 세분화하였다. 도메인, 도메인 예외, 디폴트 사용자 정책은 개인정보가 저장된 정보 시스템의 개인정보 관리자가 작성하며, 사용자 정책은 개인정보를 제공했던 개인

정보의 소유자가 작성하게 된다. 이와 같이 작성된 개인정보 보호 정책들은 개인정보 접근 요청 허가 여부를 결정할 때 판단 근거로 활용된다. 본 연구에서 정의한 개인정보 보호 정책의 기술 형식은 OASIS 기구에서 접근 통제 정책 및 개인정보 접근 요청/응답 기술 언어의 표준으로 제정한 XACML을 이용하였다.

본 논문에서 개발된 개인정보 보호 시스템은 프라이버시의 새로운 특징인 개인정보 소유자의 자기 정보 통제권을 반영하는 프라이버시 보호 정책의 도입, 개인정보 제공자 및 개인정보 사용자 프라이버시 보호 정책 분류 방안 제시, DBMS 기술을 이용한 적용 대상 개인정보 보호 정책의 인덱스 기반 검색 기능 등 개인정보를 저장, 관리, 활용하는 기업의 정보 시스템에 필수 요소 기술들을 포함하고 있다. 따라서 대량의 개인정보를 수집, 활용, 관리하면서 인터넷 비즈니스를 수행하고 있는 포털 사이트, 기업 정보 시스템 등의 개인정보 보호 시스템에 적용되어 활용될 수 있을 것으로 기대된다.

참 고 문 헌

[1] Christine Varney, Hogan & Hartson, "Privacy and Security Best Prac tices," Liberty Alliance Project, November 12, 2003.

[2] Abdelmounaam Rezgui, Athman Bouguettaya, Mohamed Y. Eltowe issy, Virginia Tech, "Privacy on the Web: Facts, Challenges, and Solu tions," IEEE Security and Privacy (Vol. 1, No. 6), 2003.

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

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

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

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

[7] Hyang-Chang Choi, Seung-Yong Lee, Hyung-Hyo Lee, "PIMS: An Access-Control based Privacy Model for Identity Management Systems," GESTS International Transaction on Computer Science and Engineering, Vol.9 and No.1(ISSN 1738-6438), 2005.

[8] OASIS, "eXtensible Access Control Markup Language (XACML) Version 1.0," OASIS Committee Specification (T. Simon Godik, editor), 2003.

[9] OASIS, "eXtensible Access Control Markup Language (XACML) Version 2.0," OASIS Committee Specification (T. Moses,editor), 2005.

[10] Sun, "Sun's XACML Implementation," January 7, 2005. http:// sunxac ml.sourceforge.net/

[11] "OECD: Guidelines on the Prote ction of Privacy and Transborder Flows of Personal Data," Orga nisation for Economic Co-Operation and Development, 1981.

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

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

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

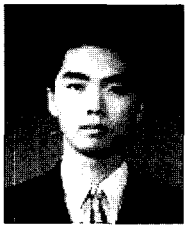
[15] Lorrie Faith Cranor, "Web Privacy

with P3P," AT&T, 2002.
[16] "P3P 1.0: The Platform for Privacy Preferences 1.0 Specification," W3C, 2002, http://www.w3.org/TR/P3P/
[17] G. Karjoth, M. Schunter, E. Van Herreweghen, and M. Waidner, "Amending P3P for Clearer Privacy Promises," 14th International Work shop on Database and Expert Sys tems Applications, 2003.
[18] P. Ashley, S. Hada, G. Karjoth, M. Schunter, "E-P3P: Privacy Policies and Privacy Authorization," WPES, November 2002.
[19] Anne Anderson, Sun Microsystems, "XACML Profile for Role Based Access Control (RBAC)," OASIS, February 2004.
[20] M. Mealing, R. Denenberg, Uniform Resource Identifiers(URIs), URLs, and Uniform Resource Names(URN s): Clarifications and Recommen dations, http://www.ietf.org/rfc/rfc33 05.txt, RFC 3305, August 2002.
[21] 최향창, 이형효, 노종혁, 진승헌 "정책 기반 프라이버시 보호시스템 설계 및 구현," 한국정보과학회 정보보호 연구회지, 2005.
[22] 최향창, 이용훈, 노봉남, 이형효, 조상래, 진승헌," ID관리시스템에서의 프라이버시 보호," 한국정보보호학회지 1598-3978 제14권6호, pp.82-93, 2004.

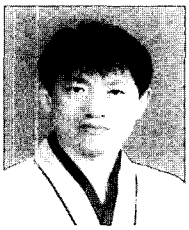
〈著者紹介〉

최 향 창 (Hyang-chang Choi) 정회원
2002년 8월 : 전남대학교 전산학과 졸업(석사)
2005년 8월 : 전남대학교 정보보호 협동과정(박사)
2005년 9월 ~ 현재: 전남대학교 시스템 보안 연구센터 Post-doc
<관심분야> 컴퓨터와 네트워크 보안, 전자상거래 보안, 유비쿼터스 보안

박 희 만 (Hee-man Park) 학생회원
2003년 2월: 전남대학교 전기공학과 졸업
2006년 2월: 전남대학교 정보보호학과 석사
2006년 3월~현재: 전남대학교 정보보호학과 박사과정
<관심분야>네트워크 보안, 유비쿼터스 보안



이 승 용 (Seung-yong Lee) 정회원
1995년 : 전남대학교 전산학과 졸업
1997년 : 전남대학교 전산통계학과 석사
2004년 : 전남대학교 정보보호협동과정 박사
1997년 1월~1998년 4월 : 금호정보통신연구소
1998년 5월~2002년 10월 : 핸디소프트 기술연구소
2005년~현재 : 전남대학교 객원교수
<관심분야> 보안운영체제, 유비쿼터스 컴퓨팅 보안



노 봉 남 (Bong-nam Noh) 종신회원
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~전남대학교 시스템 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