Journal of Digital Contents Society Vol. 9 No. 4 Dec. 2008(pp. 697-705)

# 웹 2.0 환경에서 사용되는 디지털 컨텐츠의 사용자 프라이버시 보호를 위한 RCBAC 모델

조은애*, 문창주**, 박대하***, 김정동****, 강동수****, 백두권*****


## 요 약

최근 웹 기술은 통합화, 가상화, 사회화의 세 가지 원동력에 의해 발전해왔다. 그러나 웹 기술은 소셜 네트워킹 능력의 증가를 제공하는 반면에 개인의 디지털 컨텐츠에 대한 프라이버시의 노출을 더욱 복잡하고 해결하기 어려운 문제로 심화시키고 있다. 대표적으로 세부적인 관계의 정의나 관리가 불가능하여 컨텐츠의 수집, 요약으로부터 개인의 정보 및 관심사가 추론될 수 있고, 정보 소유자만의 소셜 네트워크 구축이 어려운 문제점이 있다. 따라서 본 논문에서는 웹 2.0 환경에서 사용자만의 디지털 컨텐츠를 보호하기 위해 기존의 접근 통제 방법에 관계(Relationship)와 컨텐트 시맨틱(Content Semantic)의 개념을 적용한 RCBAC(Relationship-Content based Access Control) 모델을 제안한다. 이 방법은 개인적인 성향 등의 프라이버시가 노출되지 않고 세부적인 관계의 정의나 관리가 가능하도록 하여 정보 소유자가 자신의 소셜 네트워크를 구축할 수 있고, 이것을 웹 컨텐츠로 적용 및 확장할 수 있다.


# RCBAC(Relationship-Content based Access Control) Model for User Privacy Protection of Digital Contents in Web 2.0 Environment

Eun-Ae Cho*, Chang-Joo Moon**, Dae-Ha Park***, Jeong-Dong Kim****, Dong-Su Kang****, Doo-Kwon Baik*****


## Abstract

The recent web technology has been developed by three mainsprings which include integration, virtualization, and socialization. The web technology provides the increment of the social networking ability. However it deepens the exposure of privacy about personal information as more complicating and difficult problems. Representatively, it is impossible to define and manage the specific relation, so the personal information and interest can be inferred from collecting and summarizing the contents. Also, there are some problems that it is hard to construct the information owner's own social network. Thus this paper proposes the RCBAC(Relationship-Content based Access Control) Model which applies both the concepts of Relationship and Content Semantic to the existing access control methods to protect the user's own digital contents in web 2.0 environment. This method prevents privacy such as personal inclination from being exposed and enables to define and manage the specific relation. By doing this the information owners can construct their social network. This social network can be applied and extended to web contents.


Keywords : Web Contents, Social Network, Privacy, Access Control

## 1. 서론

1990년대 이후로 웹 기술은 통합화(integration), 가상화(virtualization), 사회화(socialization)

※ 제일저자(First Author) : 조은애
접수일:2008년 10월 16일, 완료일:2008년 12월 22일
* 고려대학교 정보통신대학
each@korea.ac.kr
** 건국대학교 항공우주정보시스템공학과
*** 한국디지털대학교 디지털정보학과
**** 고려대학교 정보통신대학
***** 고려대학교(교신저자)
▣ 이 연구에 참여한 연구자는 '2단계 BK21사업'의 지원을 받았음

의 3 가지 원동력에 의해 발전해 왔다[1]. 특히 2000년대에 등장한 웹 2.0에서는 이와 같은 현상이 가속화되고 있는데, 먼저 통합화는 태깅(tagging)과 RSS(Really Simple Syndication)[2] 및 SOA(Service-oriented Architecture)[3]와 SaaS(Software as a Service)[4] 기술을 기반으로 하는 매쉬업(mash-up)으로 이루어지고 있다. 또 AJAX(Asynchronous JavaScript and XML) 기술을 바탕으로 하여 온라인 개인 데이터와 애플리케이션의 가상화가 발달하고 있고, 블로깅(blogging), 소셜 네트워킹(social networking - 예: del.icio.us, www.flickr.com), 협력적 지식 창출(예: wikipedia) 등으로 대표되는 사회화가 급속한 진전을 이루고 있는 중이다. 뿐만 아니라 앞으로 웹 2.0은 기존의 웹 2.0 서비스와 그동안 부족했던 의미론적 통합의 결합을 통해서 가상화와 사회화를 더욱 가속화하게 만들 것이고, 온톨로지(ontology), 지능형 에이전트(intelligent agent), 의미 지식 관리(semantic knowledge management) 등의 기술들은 시맨틱 웹의 구현을 가능하게 할 것으로 예상된다.

그러나 사회화를 원동력으로 하여 발전한 웹 기술은 소셜 네트워킹 능력의 증가를 제공하는 반면에 개인 정보에 대한 프라이버시의 노출 문제를 더욱 복잡하고 해결하기 어렵게 만들고 있다. 웹 2.0에서 대표적인 개인 미디어로 각광받고 있는 블로그(blog 또는 web log)는 개인출판, 개인방송, 커뮤니티 등의 역할을 수행하고 있으며 주민등록번호, 전화번호, 금융정보, 의료정보 등 법적으로 보호되고 있는 개인정보를 노출하고 있지는 않지만 특정한 사람 또는 그룹에게만 공개하고자 하는 개인적인 성향 정보가 나타난다. 예를 들면, 가치관, 집안 또는 직장 상황, 정치적 또는 종교적 성향 등이 여기에 포함된다. 이러한 후자의 정보는 분명한 개인 프라이버시이며, 보호해야만 한다. 그러나 현재의 블로그에서는 이것들이 만족스럽게 보호되지 못하고 있다. 그에 대한 예로, 1)자신의 블로그에 회사에 대한 불만을 올렸다가 고용자에게 그 내용이 발견되어 직장에서 해고된 경우, 2)변태성욕자가 소셜 네트워크를 통해 공격 대상자를 찾는 경우, 3)정치적 성향이 다른 지도자를 추종하는 내용을 블로그에서 찾아내어 테러의 대상으로 만드는 경우 등의 프라이버시 노출에 따른 위협과 공격이 존재했던 경우를 들 수 있다[5].

이와 같이 웹 2.0에서뿐만 아니라, 차세대 웹 환경에서는 자신이 직접 생성한 콘텐츠와 더불어 링크 또는 검색으로 접근한 정보에 대한 의미(semantic)를 제3자가 쉽게 파악할 수 있다. 따라서 개인적인 관심사에 대한 노출이 문제가 되므로 블로그 게시자의 프라이버시 보호에 대한 중요성이 더욱 증가하고 있다. 이와 더불어 현재는 세부적인 관계의 정의나 관리가 불가능하기 때문에 컨텐츠의 수집, 요약으로부터 개인의 정보 및 관심사가 추론될 수 있고, 정보 소유자만의 소셜 네트워크 구축이 어렵다.

따라서 본 논문에서는 나(I)를 중심으로 관계를 정의하고, 프라이버시를 보호하는 동시에 소셜 네트워크를 웹 컨텐츠로 적용 및 확장할 수 있도록 하기 위해 관계-내용 기반 접근 통제 방법(Relationship-Content Based Access Control, RCBAC)을 제안하도록 한다.

본 논문의 나머지 부분은 다음과 같다. 2장에서는 관련 연구에 대해서 살펴보고, 3장에서는 제안한 방법인 RCBAC(Relationship-Content based Access Control)에 대해서 설명한다. 4장에서는 기존의 방법들과 비교 평가한 다음, 5장에서 결론을 맺는다.

## 2. 관련 연구

기존 웹 2.0환경에서 컨텐츠 사용자의 프라이버시를 보호하기 위한 방법은 여러 가지가 있다.

먼저, 익명(anonymous)[6] 혹은 가명(pseudonymous)[6]의 방법은 필명을 사용하는 것과 같은 방법으로 개인 미디어에 소유자 자신의 신원을 노출할 수 있는 정보를 올리지 않는 방법이다. 그러나 이것은 추론에 의한 신원 파악이 가능하고 소셜 네트워킹이 단절되는 단점이 있다.

패스워드 보호(password protection)[7]는 소유자가 설정한 패스워드를 공유한 주체만 접근할 수 있도록 설정하는 방법이다. 패스워드를 가진 사람은 정보를 모두 공유할 수 있고 패스워드가 없는 사람은 어떤 정보도 볼 수 없기 때문에 정보의 소유자가 권한을 부여할 주체를 세밀하게 나누거나 관리할 수 없다는 단점이 있다.

전통적인 접근 통제 모델[8]은 MAC (Mandat

ory Access Control), DAC (Discretionary Access Control), MLS(Multi Level Security), RBAC (Role-based Access Control) 등의 방법이 있으며, MAC 또는 MLS는 개인의 자율에 의한 프라이버시 통제에 적용하기 어려우며, DAC은 개인 미디어에 접근하려는 개별적인 주체와 대상이 되는 객체를 일일이 직접 연결하는데 노력이 너무 많이 소모되는 단점이 있다. 또한 RBAC 모델[9]은 대규모의 사용자와 컴퓨터 자원이 존재하는 컴퓨팅 환경에서 역할을 기반으로 하여 최적의 권한 부여와 자원공유를 위한 모델이지만 개인의 관점인 소셜 네트워크에 속한 접근 주체를 기업에서 직무에 해당하는 역할로 할당하는데 어려움이 존재한다.

P3P(Platform for Privacy Preference)[10]는 사용자가 브라우저에 설정한 preference와 특정 사이트의 프라이버시 정책에 따라 개인 정보의 제공 여부를 결정하는 것으로 한 사이트에 다양한 정보 객체가 제공되는 경우에는 세부적인 통제(fine-grained control)가 어렵다.

DRM(Digital Rights Management)[11]은 컨텐츠 제공자의 권리와 이익을 보호하며 불법복제를 막고 적법한 사용자만 컨텐츠를 사용할 수 있도록 정책을 작성할 수 있다. 사용료 부과와 결제대행 등 컨텐츠의 생성에서 유통·관리까지를 일괄적으로 지원하는 기술이다. 그러나, 열람 횟수, 출력 횟수 등을 정책으로 정의하여 각 컨텐츠별로 적용하는 것이므로 관계 구성, 소셜 네트워크 형성 및 확장을 적용할 수 없다.

ReBAC(Relationship-based Access Control)[12]는 데이터 소유자가 관계를 기반으로 개인적인 정보들의 접근 여부를 관리할 수 있다. 또, 한 개인은 여러 개의 관계(relationship)를 가질 수 있다. 그러나 나타낼 수 있는 관계가 제한적이라는 단점이 있다. 'FaceBook'과 같이, 서비스를 제공하는 사이트에서 미리 정의해 놓은 항목들만 사용할 수 있고, 자신이 직접 원하는 관계를 정의하는 데에는 어려움이 있다[12].

CBAC(Content-based Access Control)[13]은 컨텐츠를 분류(categorization)하여 대상이 되는 컨텐츠 자체에 권한을 부여한다. 그래서 접근 대상이 되는 컨텐츠를 중심으로 하는 모델이고, 이것 역시 기존 모델에서 쓰이던 역할(role)을 부여하게 되는 것이기 때문에 개인 중심으로 된 소셜 네트워크를 반영한 관계(relationship)를 반영하는데 어려움이 있다[13].

# 3. RCBAC 모델

본 절에서는 기존의 접근 통제에 방법에 관계(relationship)와 컨텐트 시맨틱(content semantic)의 개념을 적용한 RCBAC (Relationship-Content based Access Control) 모델을 제안한다.

## 3.1 RCBAC 모델을 위한 요구사항 및 제약조건

웹 2.0 환경에서 컨텐츠와 사용자 프라이버시를 보호하고 소셜 네트워크를 구축하기 위해서 요구사항과 제약조건이 필요하다. 먼저, 요구사항은 다음과 같이 정리할 수 있다.

- 요구사항 1: 웹 상에서의 보안이 보장되어야 한다.
- 요구사항 2: 세부적인 관계의 정의나 관리가 가능하도록 해야 한다.
- 요구사항 3: 정보 소유자가 자신의 소셜 네트워크를 구축할 수 있도록 해야 한다.

먼저, 웹 2.0 기술은 대화형 웹 응용프로그램을 구현하기 위해 자바스크립트의 사용량이 많다. 또한 사용자 참여 등 개방성을 지향하고 있는 AJAX와 같은 웹 2.0 기술들도 기존 웹과 같은 보안상 문제점이 여전히 존재하고 있다. 따라서 본 논문에서는 '요구사항 1'을 만족하기 위해 웹 보안에 대한 연구인 WS-Security(Web Service Security), XML security 등을 적용하여 웹 보안을 보장하도록 한다. '요구사항 2'는 개인적인 성향 및 관심사에 대한 노출을 막기 위한 것으로, 현재 블로그 및 커뮤니티에서 지원하는 회원관리와는 달리, 나(I)를 중심으로 사용자가 직접 세부적인 관계를 정의할 수 있도록 한다. 또, '요구사항 3'을 위해, 세부적으로 정의된 관계를 이용할 수 있다. 각각의 사용자들이 관계들을 결합 및 적용할 수 있도록 하여 각각의 정보에 대한 소유자가 자신의 소셜 네트워크로 확장할 수 있도록 한다.

이와 같은 요구사항을 바탕으로, RCBAC 모델의 설계 시 필요한 제약조건은 다음과 같다.

- 제약조건 1: 각각의 관계 그룹이 하나의 주체로 취급받을 수 있도록 한다.

- 제약조건 2: 권한의 계층을 정의하도록 한다.
- 제약조건 3: 두 개 이상의 그룹에 속해있는 관계의 경우, 각각의 그룹이 가지고 있는 권한이 상이할 때, 그룹 중 가장 낮은 레벨을 가진 권한을 가지게 된다.
- 제약조건 4: 일반 웹 사용자는 나(웹 컨텐츠 관리자)에 의해 두 개 이상의 관계에 배정되지 않아야 한다.

위의 제약조건들에서 권한에는 계층이 있지만 관계에는 계층이 없는 것을 가정하며, 추후 관계에 계층의 개념을 도입할 경우, '제약조건 3'과 '제약조건 4'는 변경의 가능성이 생길 수 있다. 왜냐하면, 계층이 서로 다른 두 개의 관계가 어떠한 권한을 상속받았는지의 여부에 따라 이로 인한 권한의 충돌이 발생할 수 있기 때문이다.

## 3.2 RCBAC 모델의 정의

RCBAC은 앞에서 언급한 바와 같이, 관계 기반 접근 통제와 내용 기반 접근 통제의 개념을 모두 적용한 접근 통제 모델이다.

먼저, 최근에 인기가 있었던 ReBAC의 일종인 친구 기반 접근 통제(Friend-based access control)(예: 미국-MySpace.com, 한국-Cyworld.com)는 관계를 private, friend, public으로 구분하며 비교적 쉽게 관계를 정의할 수 있다. 그러나 이러한 방식은 실세계의 친구와 가상세계의 친구에 대한 구분을 하지 못하고 친밀함의 단계를 세분화하지 못한다.

또, CBAC은 이미 분류가 되어 있는 컨텐츠에 대해서는 다시 분류할 필요가 없다. 그래서 사용자의 작업을 줄여줄 수 있고, 사용자가 정보를 이해하거나 변경하기 쉽다. 그러나 CBAC은 접근 대상을 중심으로 하는 모델이기 때문에 웹 2.0의 화두인 소셜 네트워크와 관련성이 많지 않다. 또한 기존에는 엔터프라이즈 환경이나 관리자 중심으로 관계가 정의되었지만, 웹 2.0에서는 개인 사용자를 중심으로 컨텐츠가 모아지고 재생산되므로 이에 맞게 변경할 필요가 있다.

따라서 사용자가 나(I)를 중심으로 하는 관계(예: family, friend, colleague 등)를 정의할 수 있다면, 접근 주체에 대한 자연스럽고 다양한 표현을 할 수 있으며, 여러 사람들이 각자 소유한 관계들을 결합하면 소셜 네트워크의 확장도 가능하도록 할 수 있다.

제안하는 RCBAC 모델은 컨텐츠를 주제별로 분류하여 관계를 주체(subject)로 하고 주제별 분류를 객체(object)로 하여 이 둘을 연산(operation)으로 매핑한 권한(permission)을 정의한다. 그 종류와 예는 다음 표 1과 같다.

<표 1> 주체, 객체, 권한의 기호와 종류의 예

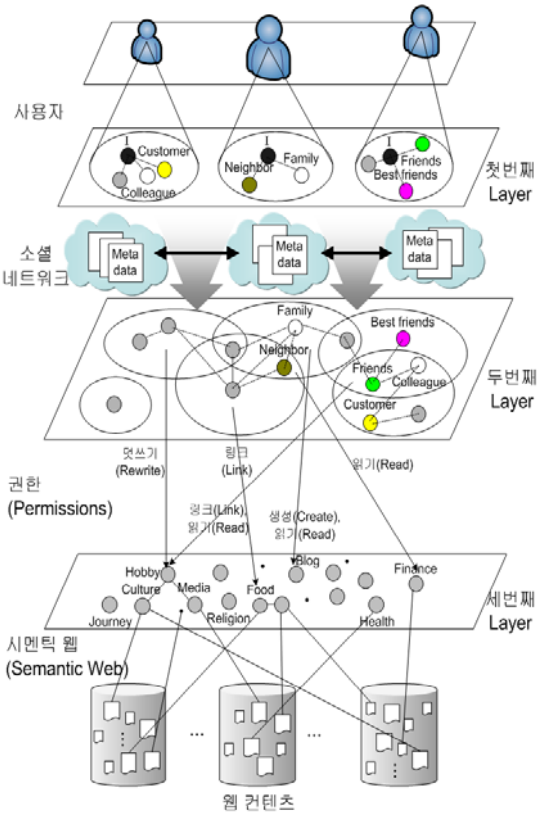
| | 기호 | 종류의 예 | 대상 |
|---|---|---|---|
| 주체 | S | I, family, friend, guest, public 등 | 블로그 사용자 네트워크 |
| 객체 | O | hobby, food, trip, finance, consumer 등 | 분류된 컨텐츠 |
| 권한 | P | 읽기(read), 덧쓰기(rewrite), 링크(link), 생성(create) 등 | 주체와 객체 |

먼저, 주체는 인간관계(personal relationship)를 의미한다. 이것은 블로그의 접속자들을 네트워크 형식으로 정의할 수 있다. 다음으로, 객체는 주체가 접근할 수 있는 웹 컨텐츠와 이미 분류된 데이터들을 의미한다. 여기서 객체의 타입과 객체에 대한 연산을 정의할 수 있다. 마지막으로 객체에 대한 연산과 객체 타입 등을 포함한 접근 권한(permission)을 정의하여 주체가 접근하고자 하는 객체에 대한 내용 의미(content semantic)를 표현할 수 있도록 한다. 예를 들어, '가족' 관계에 할당되어 있는 사용자는 블로그 게시자의 '여행' 분류의 컨텐츠를 생성(create) 혹은 링크(link)할 수 있도록 권한을 정의할 수 있는 것이다. 이렇게 하면, 소셜 네트워크의 구축 및 확장이 용이할 뿐만 아니라 사용자 편의성과 프라이버시도 보장할 수 있다.

## 3.3 RCBAC 모델의 설계

RCBAC 모델은 앞의 '3.1 RCBAC을 위한 요구사항 및 제약조건'에서 언급한 관련 연구들의 문제점 및 취약점들을 보완한다. RCBAC 개념을 적용하여 프라이버시를 보호한 접근 통제의 구성과 관계 통합을 위한 전체 구성은 다음 (그림 1)과 같다.

RCBAC은 크게 주체(Subject), 객체(Object), 권한(Permission)으로 구성한다. 먼저, 주체는 웹 사용자와 그의 소셜 네트워크로 구성되고, 그 둘 사이의 웹 보안을 위해 WS-Security, XML 보안 등을 적용하여 사용자와 웹 서버간의 보안을 보장하도록 한다.




(그림 1) 관계-내용 기반 접근 통제 방법

사용자가 정의하는 소셜 네트워크는 앞에서 언급한 바와 같이 나(I)를 중심으로 구성할 수 있다. 예를 들어, 기존에 사용하던 'guest, level1, level2, level3' 혹은 'guest, manager, admin'와 같이 구성된 회원 관리의 형태가 아니라 사용자 자신의 개성에 따라 그룹의 종류와 이름, 구성원 등을 설정할 수 있는 것이다.

다음으로 객체는 웹 컨텐츠와 그것들을 분류하여 정리한 시맨틱 웹으로 구성한다. 객체의 타입은 url, title, image, text, voice와 같이 정의하고, 그에 대한 연산은 앞에서 언급한 <표 1>과 같이 생성(create), 읽기(read), 연결(link), 덧쓰기(rewrite) 등과 같이 정의한다.

그런 다음 주체와 객체 사이의 연산(operation)을 매핑한 접근 권한(permission)을 정의하여 객체에 대한 내용 의미(content semantic)를 네트워크 형식으로 표현할 수 있도록 한다. 이 모델은 컨텐츠를 설명하고 분류한 태그들을 협력적으로 생성하고 관리하는 방법인 '폭소노미(Folksonomy)'[16][17]를 사용한다. 폭소노미는 정보를 분류하는 방법 중에 하나로, 여러 사람들이 각 데이터에 대해 키워드(태그 혹은 메타데이터)를 입력해 두고, 태그를 공유하여 전체를 분류하는 방식이다. 앞서 언급했던, 북마크 공유 사이트(예:del.icio.us)나 사진 공유사이트(예:flickr)에서도 폭소노미를 사용하고 있다.

권한에 대한 표현은 user $X$가 소셜 네트워크 그룹 $G$에 포함될 때, 분류 $C$에 대한 접근 권한 $P$에 대하여 연산 집합 $O$는 다음과 같이 표현될 수 있다.

$$P(C) = \{G, (O)\}$$

예를 들어, 'alice'가 'family'에 포함되고, 'alice'의 'journey'에 대한 권한을 표현하고자 할 때,

$G$(family) $\ni$ alice 이고,

$P$(journey) = { family, (read, link)}이면,

$$\text{alice} \xrightarrow{read,link} G(\text{ journey })$$

와 같이 나타낼 수 있다.

이러한 구조는 평면이 아니라 멀티레이어(multi-layer)로 구성한다. 먼저 맨 상위의 레이어에서는 사용자가 나(I) 중심의 소셜 네트워크를 정의하고, 두 번째 레이어에서는 사용자들의 정의들을 수집하고 정리하여 자동적인 통합 뷰가 만들어지도록 한다. 이때, 통합 뷰를 만들고 타인과의 소셜 네트워크를 공유 및 확장하기 위해서 각각의 그룹은 메타데이터를 정의하도록 한다. 사용자들은 소셜 네트워크 공유 시, 사전에 동의를 얻은 다른 사용자들 그룹(group)의 메타정보를 확인 한 뒤 자신의 그룹과 상대방의 그룹을 매핑시켜 네트워크를 확장시킬 수 있다. 이렇게 하면, 여러 사용자들의 관계를 그룹으로 통합한 통합 뷰에 대해 전체적인 보안 정책을 적용할 수 있다. 이때, 사용자들 간의 관계를 정의하기 위해서 중앙집중식 데이터베이스 없이도 소셜 네트워크를 구성할 수 있도록 해주는 FOAF(Friend of a Friend)[14]를 이용한다.

FOAF는 사람에 대한 기계가독형 온톨로지이며 웹 온톨로지 언어인 OWL[15]을 사용해 표현할 수 있다. 실제로 제안한 모델에서 FOAF를

사용한 예는 아래의 (그림 2)와 같이 나타난다.

(그림 2)는 FOAF를 작성한 한 예로 나(I) 'Alice Cho'의 별명, 사진, 연락처, 학교, 소속 등의 정보를 필요에 따라 정의하고, 점선으로 된 부분과 같이 친구를 추가할 수 있다. 이 중 메일 주소는 스팸 메일을 막기 위해 암호화 하여 표현할 수도 있다[14].

```
<rdf:RDF
 xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
 xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
 xmlns:foaf="http://xmlns.com/foaf/0.1/">
<foaf:PersonalProfileDocument rdf:about="">
    <foaf:maker rdf:resource="#me"/>
    <foaf:primaryTopic rdf:resource="#me"/>
</foaf:PersonalProfileDocument>
<foaf:Person rdf:ID="me">
    <foaf:name>Alice Cho</foaf:name>
    <foaf:title>Mrs</foaf:title>
    <foaf:givenname>Alice</foaf:givenname>
    <foaf:family_name>Cho</foaf:family_name>
    <foaf:mbox
      rdf:resource="mailto:alice@software.korea.ac.kr"/>
    <foaf:workplaceHomepage
      rdf:resource="http://software.korea.ac.kr"/>
   <foaf:friendOf>
        <foaf:Person>
          <foaf:name> Bob </foaf:name>
          <foaf:mbox
            rdf:resource="mailto:bob@software.korea.ac.kr"/>
        </foaf:Person>
   </foaf:friendOf>
</foaf:Person>
</rdf:RDF>
```

(그림 2) FOAF의 관계 정의의 예

또한, FOAF에서 정의된 사용자들의 그룹은 아래와 같이 간단히 표현할 수 있다.

```
<foaf:Group>
   <foaf:name> Best-friends </foaf:name>
   <foaf:member>
      <foaf:Person>
          <foaf:name>Bob</foaf:name>
      </foaf:Person>
   </foaf:member>
</foaf:Group>
```

(그림 3) FOAF 그룹 정의의 예

(그림 3)과 같이 'Best-friends' 그룹을 정의하여 'member'를 넣을 수도 있고 'Person'의 속성(property)을 통해서 'member'에 대한 설명을 추가할 수 있다. 이와 같은 FOAF 명세를 통하여 소셜 네트워크를 표현하면, 개인 관계에 대한 게시(publish) 및 다른 사람의 FOAF와 링크(link)가 가능하다.

따라서 이와 같이 설계를 하면, 제안한 RCBAC 모델은 요구사항에서 언급한 내용인 웹 보안 보장, 개인 프라이버시 보호 및 세부 관계 정의, 소셜 네트워크 확장 등을 모두 만족할 수 있다.

## 4. 비교 평가

제안하는 RCBAC 모델은 웹 컨텐츠에 관계(relationship)와 분류(categorization)의 개념 을 모두 활용하여 정형화된 새로운 개념의 접근 통제 기법이다. 기존에는 세부적인 관계의 정의나 관리가 불가능하여 컨텐츠의 수집, 요약으로부터 개인의 정보 및 관심사가 추론될 수 있었고, 정보의 소유자만의 소셜 네트워크 구축이 어려웠다. 그러나 RCBAC 모델을 사용한 접근 통제 기법으로 이러한 문제점들을 해결하고 프라이버시 등을 보호할 수 있다. 즉, 자신에 관한 정보를 보호받기 위하여 자신에 관한 정보를 자율적으로 결정하고 관리할 수 있는 권리인 자기정보통제권을 보장받을 수 있게 되는 것이다.

다음 <표 2>는 기존의 모델과 제안한 모델을 여러 항목에서 비교하여 나타낸 것이다.

<표 2> 기존 모델과 제안 모델의 비교

| | RCBAC | ReBAC | CBAC |
|---|---|---|---|
| 사용자 프라이버시 노출 가능성 | 낮음 | 높음 | 높음 |
| 관계 정의 시 사용자 편의성 | 높음 | 높음 | 낮음 |
| 컨텐츠 상세 분류 지원 | 가능 | 불가능 | 가능 |
| 사용자 중심의 관계 정의 | 가능 | 불가능 | 불가능 |
| 소셜 네트워크 구조 및 그룹의 확장 | 가능 | 가능 | 불가능 |

앞에서 언급한 바와 같이 ReBAC은 관계를 기반으로 한 접근 통제이고, CBAC은 컨텐츠를 기반으로 한 접근 통제이므로, 각각의 초점에 맞게 장단점이 있다.

위의 <표 2>에서 먼저, 기존의 방법인 ReBAC과 CBAC 방법들은 상세한 관계의 정의가 어렵기 때문에 사용자 프라이버시가 노출될 가능성을 배제할 수 없다. 예를 들어, 익명의 사용자가 목표자를 정한 뒤 그에 대한 성별, 출신학교, 취미와 같은 프라이버시에 해당하는 정보를 알기를 원할 경우, ReBAC 기반 방법에서는 목표자의 블로그에 접근하거나 답글을 남긴 사용자들의 블로그를 통하여 정보의 파악이 가능하며, CBAC 기반 방법에서는 컨텐츠의 분류 방법이나 분류의 이름을 통해서 정보의 파악이 가능하기 때문이다. 그러나 본 논문에서 제안한 RCBAC은 사용자 중심의 상세한 접근 통제의 정의가 가능하므로 각각의 사용자는 자신의 정의에 따라 구분하여 컨텐츠를 공개할 수 있다. 따라서 익명의 사용자에 의해 컨텐츠 게시자가 원하지 않는 개인의 프라이버시 정보가 열람되거나 분류 항목들이 노출되는 것은 불가능하다.

또한, ReBAC은 사용자가 관계를 정의할 때, 오퍼레이터(operator)가 제공하는 관계의 종류에 따라 비교적 편리하게 수행이 가능하고, CBAC은 사용자가 컨텐츠를 분류할 때 사용자의 의도에 따라 태깅 등의 분류방법을 적용할 수 있다. 그러나 반대로 ReBAC은 관계 정의 시 오퍼레이터가 제공하는 관계로만 설정을 할 수 있고, 컨텐츠의 분류가 1차원적이다. 게다가 CBAC은 사용자의 관계 정의는 고려하고 있지 않다. 그러나 제안하는 방법은 컨텐츠 분류를 바탕으로 한 사용자 간의 권한 부여가 가능하기 때문에 사용자가 자유롭게 관계를 정의할 수 있도록 편의성을 제공해주는 동시에 사용자의 의도를 충분히 반영한 관계의 정의가 가능하고, 폭사노미를 사용한 컨텐츠에 대한 상세 분류도 가능하다.

마지막으로, 소셜 네트워크의 그룹 혹은 분류의 확장면에서 ReBAC과 CBAC 방법은 오퍼레이터나 서비스 제공자가 제시한 구조와 그룹만을 사용할 수 있어 확장이 쉽지 않다. 그러나 제안한 방법은 사용자가 본인의 의도에 따라 메타데이터를 만들어 그룹을 생성하고 구성할 수 있으므로 다른 사용자나 서비스로의 소셜 네트워크 확장이 가능하다.

## 5. 결론

본 연구는 웹 2.0에서 쓰이고 있는 AJAX, RSS, SOA, SaaS, 태깅 등의 기술을 기반으로 하고 있다. 이들 중 대부분이 오픈 소스이거나 오픈 API를 사용하고 있어 다양한 서비스 및 제품과의 결합과 지원이 가능하다.

본 연구의 프라이버시 보호 접근 정책은 이를 바탕으로 확장될 수 있는 소셜 네트워크를 통해서 더욱 다양한 형태로 제공될 수 있으며, 온라인 서비스 뿐만 아니라 오프라인 모임 및 서비스로 확장 및 발전하여 산업적 가치 창출을 높일 수 있다. 또한, 기존의 DRM 기술과 접목하여 P2P 환경을 통해 공유되는 콘텐츠(영상, 음반, e-book 등) 또는 UCC에 대한 저작권 보호 정책으로 사용 가능하다. 뿐만 아니라 방송, 게임, 출판 산업에도 새로운 비즈니스 모델이 창출될 수 있다.

결국 본 논문은 기존 연구 및 모델들이 만족하지 못하고 있는 프라이버시 보호를 위한 접근 통제 기술들을 적용하여 차후 가치의 중요성이 더 높아질 개인 정보 및 개인 관계들을 보호하는 모델들의 가이드라인을 제시해 줄 수 있으며 유비쿼터스 컴퓨팅 환경에서의 접근 통제 및 프라이버시 보호로 확장을 도울 수 있을 것이다.

향후 연구로는 RCBAC 모델의 정형적인 정의와 발생할 수 있는 관계의 충돌 검출 및 해결 방안, 정의된 관계들의 관리 방법 등이 있으며, 제안한 방법들을 더욱 향상시킬 수 있도록 관련 제약 조건의 계층화 및 발전된 사용자 인터페이스 모델을 제시하고자 한다.

## 참 고 문 헌

[1] Udi h Bauman, "Web 2.0 and the Semantic Web: A New World of Integration," 2006.

[2] RSS Advisory Board, Really Simple Syndication: RSS 2.0.1 Specification (revision 6), http://www.rssboard.org/rss-2-0-1-rv-6, 2008.

[3] SOA(Service Oriented Architecture), http://en.wikipedia.org/wiki/Service-oriented architecture/, 2008.

[4] SaaS(Software as a Service), http://en.wikipedia.org /wiki/Software as a Service/, 2008.
[5] Wikipedia - http://en.wikipedia.org/wiki/Blog, 2008.
[6] Alfred Kobsa, "A Component Architecture for Dynamically Managing Privacy Constraints in Personalized Web-Based Systems," 3rd International Workshop Privacy Enhancing Technologies (PET2003), LNCS 2760/2003, pp.177-188, 2004.
[7] D. Balfanz, "Usable Access Control for the World Wide Web," 19th Annual Computer Security Applications Conference, pp.406- 415, 2003.
[8] D. F. Ferraiolo, D. R. Kuhn, R. Chandramouli, Role-based Access Control, Artech House, 2003.
[9] R. S. Sandhu, E. J. Coynek, H. L. Feinsteink , C. E. Youmank, "Role-Based Access Control Models," IEEE Computer, Vol.29, No.2, pp.38-47, 1996.
[10] I. K. Reay, P. Beatty, S. Dick, "A Survey and Analysis of the P3P Protocol's Agents, Adoption, Maintenance, and Future," IEEE Transactions on Dependable and Secure Computing, Vol. 4, No. 2, pp.151-164, 2007.
[11] Roberto García González, "A Semantic Web approach to Digital Rights Management," Ph.D. Thesis in University at Pompeu Fabra, 2005.
[12] C. E. Gates, "Access Control Requirements for Web 2.0 Security and Privacy," 2007 IEEE Symposium on Security and Privacy (W2SP2007), 2007.
[13] M. Hart, R.Johnson, A. Stent, "More Content - Less Control: Access Control in the Web 2.0," 2007 IEEE Symposium on Security and Privacy(W2SP2007), 2007.
[14] Dan Brickley and Libby Miller, "FOAF Vocabulary Specification 0.9," http://xmlns.com/foaf/0.1/, 2007..
[15] OWL Web Ontology Language Overview, W3C Candidate Recommendation, 2003.
[16] J. Breslin, S. Decker, "Semantic Web 2.0: Creating Social Semantic Information Spaces," 15th International World Wide Web Conference (WWW2006), 2006.
[17] Folksonomy, http://en.wikipedia.org/wiki/Folksonomy/, 2008.

**조 은 애**

2003년 : 고려대학교 컴퓨터학과(학사)
2005년 : 고려대학교 컴퓨터학과(석사)
2005년~현 재 : 고려대학교 컴퓨터학과 (박사과정)
관심분야 : 접근제어(Access Control), 프라이버시, 권한부여(Authorization), RBAC(Role-based Access Control)

**문 창 주**

1997년 : 고려대학교 컴퓨터학과 (학사)
1999년 : 고려대학교 컴퓨터학과 (석사)
2004년 : 고려대학교 컴퓨터학과 (박사)
2004년~2005년 : 고려대학교 정보보호대학원 연구교수
2005년~2006년 : 건국대학교 컴퓨터응용과학부 컴퓨터시스템전공 조교수
2006년~현 재 : 건국대학교 공과대학 항공우주정보시스템공학과 조교수
관심분야 : 접근제어, 권한부여, RBAC, 프라이버시, 유비쿼터스 보안, 임베디드 시스템

**박 대 하**

1992년 : 고려대학교 컴퓨터학과(학사)
1994년 : 고려대학교 컴퓨터학과(석사)
2004년 : 고려대학교 컴퓨터학과(박사)
1999년~2003년 : (주)시큐리티테크놀로지스연구소장
2003년~현 재 : 한국디지털대학교 디지털정보학과 교수
관심분야 : XML 보안, 보안프로토콜, 이동코드보안, 임베디드 시스템보안

**김 정 동**

2005년 : 선문대학교 컴퓨터정보학부(학사)
2008년 : 고려대학교 컴퓨터학과(석사)
2008~현 재 : 고려대학교 컴퓨터학과 (박사과정)
관심분야 : 데이터 통합, 유비쿼터스 컴퓨팅, 메타데이터 레지스트리, 온톨로지, 시멘틱 웹

**강 동 수**

1997년 : 해군사관학교 전기공학(학사)
2006년 : 국방대학교 전산학(석사)
2008년~현 재 : 고려대학교 컴퓨터전파통신학과(박사과정)
1997년~1999년 : 암호관
관심분야 : SOC(Service-Oriented Computing), 시스템공학, 소프트웨어공학

**백 두 권**

1974년 : 고려대학교 수학과(학사)
1977년 : 고려대학교 산업공학과(석사)
1983년 : Wayne State Univ. 전산학과(석사)
1985년 : Wayne State Univ. 전산학과(박사)
1986년~현 재 : 고려대학교 컴퓨터학과 (교수)
1989년~현 재 : (사)한국정보과학회(이사/평의원/부회장)
1991년~현 재 : (사)한국시뮬레이션학회 (이사/부회장/감사/회장/고문)
1991년~현 재 : ISO/IEC JTC1/SC32 전문위원회(위원장)
2001년~현 재 : (사)도산아카데미 (원장)
2002년~2004년 : 고려대학교 정보통신대학(초대학장)
2004년~2005년 : (사)한국정보처리학회 (부회장)
관심분야 : 메타데이터, 소프트웨어공학, 데이터공학, 컴포넌트기반 시스템, 메타데이터 레지스트리, 프로젝트 매니지먼트 등