通信情報保護學會論文誌
第 9 券 第 3 號, 1999. 09

메타정보체계를 위한 정보보호속성의 설계

이 요 섭*, 전 문 석**

A Design Information Security Attributes of for Meta-Information System

Yo-seob Lee, Moon-seog Jun

요 약

인터넷의 고속 성장은 많은 유용한 정보를 공유할 수 있는 토대를 제공하고 있다. 방대한 양의 정보는 빠른 시간안에 정보를 처리할 수 있는 능력을 요구하게 되었고, 이러한 요구에 부응하여 메타 정보체계가 나타나게 되었다. 메타 정보 체계는 원하는 정보를 정확하게 빠르게 검색하는 기능을 제공하고 있으나 그 반면에 정보보호 측면에서 대책을 제공하고 있지 않으므로 심각한 문제를 발생시킬 수 있다. 본 논문에서는 이러한 문제점을 해결하기 위해 메타 정보 체계를 위한 사용자 접속 제어에 관한 정보보호 속성을 제안한다.

ABSTRACT

The rapid growth of Internet supports a base that share useful information. It needs for mass of information that requires a fast processing capability. It needs a meta-information system. Meta-information system supports fast search service but occurs a problem in case of information security. In this paper, we propose a information security attribute that are user access control for meta-information system to solve the problem.

I. 서 론

인터넷의 보편화와 그에 따르는 정보 검색 엔진의 발전으로 인해서 사용자들에게 정보 검색에 대한 편의를 제공하고 있지만, 새로운 정보의 생성과 기존 정보의 사멸의 방대화로 인해, 사용자들이 인터넷의 정보를 검색할 때 다음의 단점을 가지고 있다. 첫째로는 유사한 정보가 많아서 인터넷상의 정보를 모두 검색하는 것이 불가능하고, 검색된 정보 중에는 원하지 않는 정보가 있을 수 있으며, 가져오지 않은 페이지 중에 원하는 정보가 있을 수 있다는 것이다. 이러한 문제점들의 해결 방안으로 메타 정보를 구축함으로써 정보의 인덱스 역할을 하면서 해당 정보에 대한 정확한 정보를 가지고 여러 사이트에서 제공하는 정보들을 쉽게 분류할 수 있도록 구성할 수 있다. 메타 정보 체계는 정보보호 측면에서 사용자 정의에 의해 정보 체계를 구축하기 때문에 정보를 보호하지 못하고 노출시키는 문제점을 유발할 수 있기 때문에 본 논문에서는 메타 정보 체계를 위한 정보보호 속성을 설계하고자 한다.

* 숭실대학교 컴퓨터학부 통신연구실(yslee@eve.soongsil.ac.kr), ** 숭실대학교 컴퓨터학부 통신연구실(mjun@computing.soongsil.ac.kr)

2장에서는 기본의 메타 정보 체계들에 대해 분석하고, 3장에서는 메타 정보 체계를 구축하는데 좋은 도구로 각광을 받고 있는 XML에 대해 알아본다. 4장에서는 메타 정보 체계를 위한 정보 보호 속성을 설계하고 5장에서는 결론 및 향후 연구 방향에 대해 논한다.

II. 기존의 메타 정보 체계 분석

넓은 범위의 전자 오브젝트들을 간결하게 설명하기 위해 간단한 메타데이타 레코드가 1995년 3월 더블린의 Online Computer Library Center(OCLC)와 National Center for Supercomputing Application(NCSA)의 메타데이터 워크숍에서 정의되었다[2]. SGML 위원회에서 문제의 범위를 규정하고, 넓은 주제 분야에서 데이터의 간단한 설명을 생성할 수 있는 메타데이터의 리스트를 생성하였으며, 전자 정보를 설명할 수 있는 메타데이터 구성요소의 정의를 진전시키기 위한 토대를 준비하였다[3][4].

Dublin Core를 비롯한 기존의 메타 정보 체계에 대한 조사와 분석은 정보보호를 위한 메타 정보 체계의 설계에 도움을 줄 수 있고, 기존 메타 정보체계가 원하는 정보를 정확하고 빠르게 검색하는 것에 반해 정보보호 측면에서 많은 문제점이 발생할 수 있기 때문에 이러한 문제점을 해결할 수 있다.

2.1 Dublin Core

Dublin Core(또는 Dublin Core Metadata Element Set)는 인터넷과 같은 네트워크 환경에서 document-like objects(DLOs)를 찾는 기능을 요구하는 최소한의 메타데이터 구성요소들을 제공한다. 표 1은 Dublin Core의 구성요소들을 나타낸다.

2.2 Warwick Framework

Warwick Framework는 메타데이터의 다양한 패키지들을 논리적, 물리적으로 통합하는 메커니즘을 말한다. Warwick Framework는 container와 package의 두 개의 구성요소를 가지고 있다[5]. container는 타입이 있는 메타데이터 집합을 통합하

표 1. Dublic Core의 구성요소들
Table 1. The Components of Dublin Core

구성요소	설명
Subject	작업의 주체를 나타낸다.
Title	객체의 이름을 나타낸다.
Author	객체의 담당자를 나타낸다.
Publisher	이용가능한 객체를 만드는 에이전트를 나타낸다.
Other Agent	편집자나 복사자를 나타낸다.
Date	작성일자를 나타낸다.
Object Type	객체의 장르를 나타낸다.(예: 소설, 시, 사전 등)
Form	객체의 파일 형태를 나타낸다. (예: postscript 파일, 윈도 실행 파일 등)
Identifier	객체를 규정하는 데 유일하게 사용된 스트링이나 이름을 나타낸다.
Relation	다른 객체와의 관계를 나타낸다.
Source	객체의 소스를 나타낸다.(예: print 또는 electronic)
Language	내용을 작성한 언어를 나타낸다.
Coverage	객체의 공간적 위치와 시간적 지속 기간의 특성을 나타낸다.

고 package는 이 메타데이터 집합들을 나타낸다. 각각의 package는 타입을 가진 object이며 클라이언트나 에이전트에 접속된 이후에 참조된다.

2.3 USMARC 포맷

USMARC(US MAchine Readable Catalogue) 포맷은 machine-readable한 형태의 도서목록, 관련된 정보의 표현과 통신 표준이다[6]. USMARC 레코드는 다음과 같이 세 개의 구성요소들로 이루어져 있다:

1) structure : USMARC 레코드의 구조는 국제 표준인 *Information Interchange Format*(ANSI Z39.2)과 *Format for Information Exchange*(ISO 2709)를 구현한 것이다.

2) content designation : 레코드안에서 데이터 구성요소들을 규정하고 특성화하고 이 데이터들을 지원하기 위한 코드와 컨벤션은 USMARC 포맷에서 정의된다.

3) content : 외부의 표준에 의해 정의된 대부분의 데이터 구성요소들의 내용은 USMARC 포맷에서 정의된다.

USMARC 포맷은 machine-readable한 레코드들을 인코딩하기 위해 정의된 코드와 content designator 들의 집합이다. 포맷은 다음과 같이 다섯 가지의 데이터 타입을 정의한다: bibliographic, holding, authority, classification, community information.

2.4 CSDGM(Content Standards for Digital Geospatial Metadata)

이 표준은 digital geospatial 데이터 집합을 위한 메타데이터의 information content를 나타낸다[7]. 이 표준의 목적은 이러한 메타데이터와 관련된 용어와 정의들을 제공한다. 메타데이터는 데이터의 내용, 질, 조건, 다른 특성에 관한 데이터를 나타낸다.

III. XML

3.1 XML의 등장

웹상에서 홈페이지를 만들 때 가장 많이 쓰이는 언어가 HTML이다. 하지만 많은 사용자들은 HTML의 문제가 되는 확장성, 구조성, 데이터 검사 기능의 단점에 많은 어려움을 느끼고 있었다. 또한 일부 사용자들에 의해 사용되는 SGML의 문서는 일반 사용자가 사용하기에는 너무 복잡하고 어렵다.

그래서 1996년 중반에, 대략 80명의 SGML 전문가 그룹이 모여 SGML의 강력한 power와 일반적인 내용을 유지하면서 웹상에서 보다 사용하기에 쉬운 Markup Language를 개발하고자 하였다. 이 Markup Language는 다음과 같은 기능을 유지해야 한다.

- 웹상에서 개괄적인 Markup 지원
- 이상적으로는 SGML의 규칙에 따라 유효하게 할 수 있는 문서들의 생성
- URL 접근시에도 이상적으로 사용할 수 있는 하이퍼링크 지원
- 강력한 스타일 시트 메카니즘 제공

위의 목적에 부합하는 최초 Markup Language로 제안된 것이 바로 XML(eXtensible Markup language)이다[9]. 이 은 웹에서 구조화된 문서를 전송 가능하도록 설계된 표준화된 텍스트 형식으로, XML 표준에서의 기본 문자집합은 8-bit ASCII와 Unicode를 사용하여 문자 집합의 차이에서 오는 문서 구성의 한계를 극복하였다. 또한, 웹상에서 기존에 사용하던 HTML의 한계를 극복하고 SGML의 복잡함을 해결하기 위해 HTML에 사용자가 새로운 태그(tag)를 가변적으로 정의할 수 있는 기능을 추가하였다.

3.2 HTML, SGML, XML과의 비교

XML은 위에서 언급한 HTML과 SGML의 장점을 유지하면서 단점을 극복하는 Markup Language이다. SGML은 XML로 변환이 용이하고, XML을 모두 수정없이 SGML의 응용에 사용할 수 있다.

또한 HTML과의 관계에 대해 살펴보면, 웹상에서 HTML 문서를 사용할 때 두드러지게 나타나는 단점이라면 고정 태그를 사용한다는 점이다. 표준으로 발표된 태그 또는 각각의 브라우저에서 표현 가능한 태그를 사용해 홈페이지를 만들고, 브라우저는 홈페이지의 태그 중에서 자신이 인식할 수 있는 태그만을 표현할 뿐 인식하지 못하는 태그에 대해서는 무시한다.

사용자가 임의로 태그를 만들 수 있으려면 태그

정의 기능이 있어야 하며, 브라우저에서는 DTD를 읽고, 또 DTD를 이용해 만든 문서를 DTD에 맞게 해석할 수 있고, 또 브라우저에 보여줄 수 있어야 한다. 이같은 기능이 있지 않는한 기존의 웹 브라우저에서는 임의의 태그를 사용할 수 없다. 즉, 웹이 지금까지 발전하는 데에는 누구나 사용할 수 있는 HTML의 단순함이 큰 역할을 했지만, 현재 시점에서는 사용자의 다양한 요구가 발생하게 됐고, 그러한 요구를 수용하려는 시도가 바로 XML인 것이다.

그렇다고 XML의 등장으로 현재 웹에서 사용하고 있는 HTML이 완전하게 사라지는 것은 아니다. 각각을 SGML과의 관계에서 살펴보면, HTML은 SGML의 어플리케이션 - 즉, 온라인 상에서 하이퍼링크를 제공하여 웹 문서를 나타내려는 목적으로 원소들의 유형의 정의된 셋으로 제공한다는 의미 - 인 반면, XML은 SGML의 프로파일(*profile*) - 무제한의 어플리케이션을 제공할 수 있다는 의미 - 이라는 차이가 있다.

XML은 하이퍼링크와 스타일 시트를 제공하며, 사용자의 엘리먼트와 속성을 정의할 수 있고 구조를 확장하여 사용할 수 있다.

3.3 XLL (XML Linking Language)

다음은 XLL의 구성요소와 속성들을 나타낸다. XLL의 링크는 종류에 따라 단순 링크, 확장 링크, 확장 링크의 그룹 등으로 분류된다.

단순 링크는 HTML 링크의 기능과 유사한 목적으로 사용되지만, 링크 엘리먼트의 기능과 한 엘리먼트의 로케이터를 결합하는 기능을 갖는다. 결합의 결과로 단순 링크 엘리먼트는 로케이터의 속성과 모든 링크와 자원 의미 속성 등을 제공한다.

다음은 단순 링크의 간단한 선언 부분을 나타낸다. 선언 부분중에 다양한 속성들을 나타낸다. 단순 링크의 xml:link 속성은 simple이다.

```
<!ELEMENT simple ANY>
<!ATTLIST simple
        xml:link CDATA #FIXED "simple"
        %locator.att;
        %remote-resource-semantics.att;
        %local-resource-semantics.att;
        %simple-link-semantics.att;
        %protection-semantics.att;
>
```

다음은 단순 링크의 예를 나타낸다.

```
<mylink xml:link="simple" title="Citation"
href="http://www.xyz.com/xml/foo.xml"
show="new" content-role="Reference">as discussed
in Smith(1997)
</mylink>
```

mylink는 다음과 같은 구성요소와 속성 리스트 선언부분을 가진다.

```
<!ELEMENT mylink (#PCDATA)>
<!ATTLIST mylink
      xml:link   CDATA   #FIXED "simple"
      href       CDATA   #REQUIRED
>
```

3.3.1 Locators

locator 스트링은 참여한 자원을 규정한다. 링크는 각각의 원격 자원에 대한 로케이터를 제공해야 하며, 로케이터는 href 속성의 형태를 가진다. 다음은 이 속성의 간단한 선언 부분으로 locator.att라는 파라미터 객체로 표현된다.

```
<!ENTITY % locator.att
    "href    CDATA    #REQUIRED"
>
```

3.3.2 Link Semantics

링크를 위해 다음과 같은 시맨틱 정보를 제공한다.

- 링크가 inline인지의 여부

  링크가 inline인 경우에 내용은 링크의 로컬 자원으로 간주하고, out-of-line인 경우에는 로컬 자원으로 간주하지 않는다.

- 링크의 역할

  링크의 역할은 링크의 의미를 응용 소프트웨어에 규정하는 것이다.

다음은 이 속성의 간단한 선언 부분으로 link-semantics.att라는 파라미터 개체로 표현된다.

```
<!ENTITY % link-semantics.att
```

```
    "inline     (true|false)     'true'
     role       CDATA            #IMPLIED"
>
```

단순 링크 구성요소를 사용하는 경우에는 simple-link-semantics.att라는 파라미터 개체로 표현된다.

```
<!ENTITY % simple-link-semantics.att
    "inline          (true|false)          'true'"
>
```

3.3.3

링크의 원격 자원을 위해 다음과 같은 시멘틱 정보가 제공된다.

- 자원의 역할

  자원의 역할은 링크상에서 동작하는 부분을 응용 소프트웨어에 규정하는 것이다.

- 자원의 타이틀

  자원에 대한 타이틀은 링크상에서 자원이 동작하는 부분을 사용자에데 설명하는 캡션을 나타낸다.

- 행위 정책은 자원을 검색하는데 사용된다.

다음은 이 속성의 간단한 선언 부분으로 remote-resource-semantics.att라는 파라미터 객체로 표현된다.

```
<!ENTITY % remote-resource-semantics.att
    "role       CDATA                  #IMPLIED
     title      CDATA                  #IMPLIED
     show       (embed|replace|new)    #IMPLIED
     actuate    (auto|user)            #IMPLIED
     behavior   CDATA                  #IMPLIED"
>
```

3.3.4 Local Resource Semantics

링크가 inline인 경우 링크의 로컬 자원을 위해 다음과 같은 시멘틱 정보가 제공된다.

- 자원의 역할

  자원의 역할은 링크상에서 동작하는 부분을 응용 소프트웨어에 규정하는 것이다.

- 자원의 타이틀

  자원에 대한 타이틀은 링크상에서 자원이 동작하는 부분을 사용자에게 설명하는 캡션을 나타낸다.

다음은 이 속성의 간단한 선언 부분으로 local-resource-semantics.att라는 파라미터 객체로 표현된다.

```
<!ENTITY % local-resource-semantics.att
    "content-role   CDATA      #IMPLIED
     content-title  CDATA      #IMPLIED"
>
```

3.3.5 링크의 행위

링크 행위는 링크 형태, 자원의 역할, 사용자 환경에 근거한 규칙에 의해 결정된다.

- show 속성

  show 속성은 나타내거나 처리해야 하는 자원에서 문맥으로 정책을 나타내는데 사용된다.

표 2. 정보 보호 속성

Table 2. Information security attribute

```
<!ENTITY % protection-semantics.att
  "role                    CDATA                    #IMPLIED
   title                   CDATA                    #IMPLIED
   group                   (group1|group2|...)      #IMPLIED
   access-control-group    (group1|group2|...)      #IMPLIED
   access-control-ipaddr   (ip-addr1|ip-addr2|...)  #IMPLIED
   access-control-time     ([time1,time2]|...)      #IMPLIED"
>
```

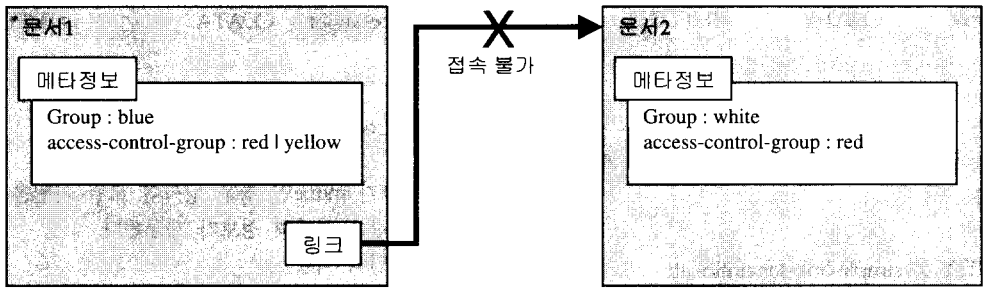

그림 1. 그룹별 접속제어 기능

Figure 1. Access control function for Groups

embed
링크가 시작되는 위치의 자원의 body안에서 지정한 자원이 embed된 것을 나타낸다.

replace
지정한 자원이 링크가 시작된 자원을 대체하는 것을 나타낸다.

new
지정한 자원이 링크가 시작된 자원에 영향을 주지 않고 새로운 문맥안에 있는 것을 나타낸다.

- atuate 속성

actuate 속성은 링크가 실행될 때의 정책을 나타내는데 사용된다. 이 속성은 다음과 같은 값들을 가진다.

auto 같은 링크의 다른 자원이 발생할 때 문제의 자원이 검색되는 것을 나타낸다. 모든 auto 자원은 주어진 순서대로 검색된다.

user 외부의 요구가 있을 때까지 자원이 표현되지 않는 것을 나타낸다.

IV. 메타 정보 체계를 위한 정보 보호 속성의 설계

4.1 정보 보호 기능

다음은 메타정보에서 정보보호를 위해 제공하는 기능들을 나타낸다.

- 사용자 정의 그룹 기능

사용자가 원하는 그룹을 설정할 수 있도록 한다.

- 사용자 접속 제한 기능

사용자의 조건이 만족하지 않는 경우 접속을 제한한다. 다음은 접속을 제한하는 경우를 나타낸다.

1) 사용자가 원하는 정보의 그룹에 속하지 않은 경우

표 3. 그룹들과 그룹별 접속 제어 정책

Table 3. Groups and Access control poloices for Groups

출 발 지	목 적 지				
	로컬 네트워크	인터넷	로컬 인트라넷	신뢰 사이트	제한 사이트
로컬 네트워크	접속 허용	접속 허용	접속 허용	접속 허용	접속 거부
인터넷	접속 거부	접속 허용	접속 거부	접속 거부	접속 거부
로컬 인트라넷	접속 거부	접속 허용	접속 허용	접속 거부	접속 거부
신뢰 사이트	접속 거부	접속 거부	접속 거부	접속 허용	접속 거부
제한 사이트	접속 거부	접속 거부	접속 거부	접속 거부	접속 거부

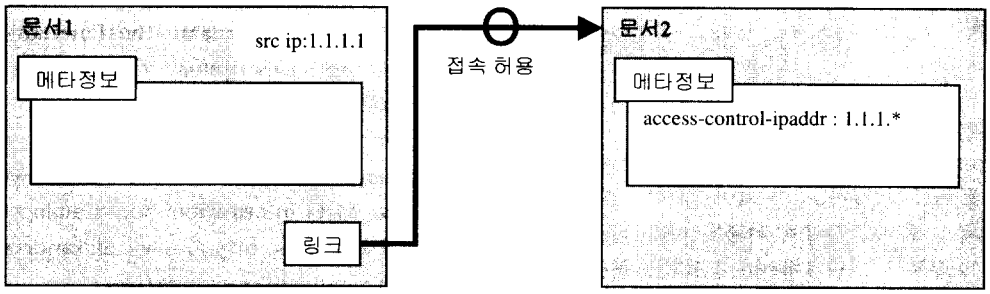

그림 2. ip 주소별 접속 제어 기능
Figure 2. Access control function for IP addresses

2) 사용자의 source IP주소가 등록되어 있지 않은 경우
3) 사용자가 등록된 시간외에 접속하는 경우

4.2 메타 정보 체계의 정보보호 기능들의 구조

다음은 메타 정보에서 제공하는 정보 보호 기능들의 구조를 XLL(XML Linking Language)로 표현한 형태를 나타낸다. 정보보호 기능들은 XLL에서 제공하는 링크의 종류에 따라 단순 링크, 확장 링크, 확장 링크의 그룹 등으로 표현된다.

정보 보호 속성을 제공하기 위해 Link Semantics, Remote Resource Semantcis, Local Remote Sematics 외에 Protection Semantics를 추가한다.

4.2.1 Protection Semantics

Protection Semantics는 정보 보호 속성을 선언하는 부분으로 protection-semantics.att라는 파라미터 객체로 표현된다. Protection Semantics는 표 2와 같다.

- role : 링크시 작동하는 응용 소프트웨어를 규정한다.
- title : 정보 보호 속성의 타이들을 나타낸다.

4.2.2 정보보호를 위한 링크의 형태

- group 속성

group 속성은 그룹의 속성을 지정한다. 그룹의 속성은 다음과 같이 나누어진다.

- 로컬 네트워크 : 인트라넷에 포함되지 않은 내부 네트워크를 말한다.
- 인터넷
- 로컬 인트라넷
- 신뢰 사이트 : 접속을 허용할 수 있는 사이트를 말

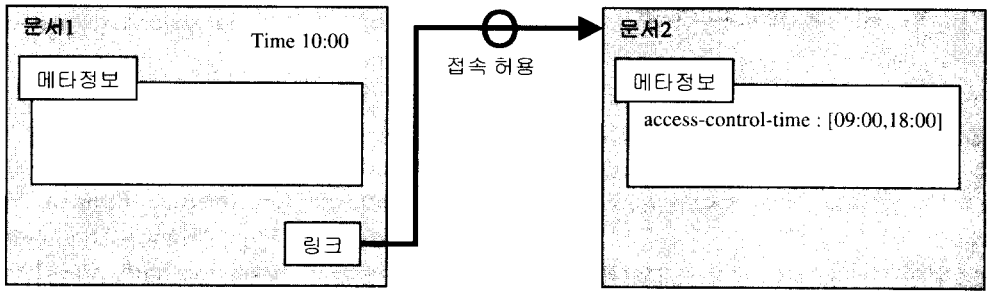

그림 3. 시간별 접속 제어 기능
Figure 3. Access control function for Time units

한다.
- 제한 사이트: 접속을 허용하지 않는 사이트를 말한다.

● access-control-group 속성

access-control-group 속성은 주어진 그룹만 접속을 허용하게 한다. 그룹별 접속 제어 정책은 표3과 같다. 출발지와 목적지 사이의 관계에 따라 접속을 허용하거나 거부한다. 그림 1에서는 링크되는 문서의 그룹에 자신이 속해있지 않은 경우 접속 불가되는 것을 나타낸다. 자신의 문서 그룹은 blue이고, 링크되는 문서는 red만 허용하기 때문에 접속이 허용되지 않는다.

● access-control-ipaddr 속성

access-control-ipaddr 속성은 주어진 IP 주소만 접속을 허용한다. 그림 2에서는 링크되는 문서의 ip 주소에 자신의 주소가 속해있는 경우 접속이 허용되는 것을 나타낸다. 링크되는 문서는 1.1.1.*에서 오는 문서만 접속이 허용되는데 현재 링크하려는 문서의 ip 주소가 1.1.1.1이기 때문에 접속이 허용된다.

● access-control-time 속성

access-control-time 속성은 주어진 시간만 접속을 허용한다. 그림 3에서는 링크되는 문서의 시간 범위에 자신이 접속하는 시간이 그 범위에 속해있는 경우 접속이 허용되는 것을 나타낸다. 링크되는 문서의 접속이 허용되는 시간 범위는 09:00에서 18:00인데 링크하는 문서의 접속 시간이 10:00이기 때문에 접속이 허용된다.

V. 결론 및 향후 연구방향

본 논문은 기존 메타 정보 체계의 보안을 강화하는 기능을 XLL의 링크 속성으로 제공하므로써, 정확하고, 효율적인 정보 검색을 수행하며 노출되기 쉬운 메타 정보 체계에서 메타 정보의 보호가 가능하게 된다.

앞으로의 연구 방향으로는 확장 링크와 확장 링크의 그룹에 대해 정보보호 기능을 제공하는 구조를 설계한다.

참 고 문 헌

[1] Stuart Weibel, Metadata: The Foundations of Resource Description, *D-Lib Magazine*, July 1995

[2] Terence R. Smith, Steven Geffner, and Jonathan Gottsegen, A General Framework for the Meta-Information and Catalogs in Digital Libraries, http://www.alexandria.ucsb.edu/public-documents/ieee/

[3] Terence R. Smith, The Meta-Information Environment of Digital Libraries, http://www.alexandria.ucsb.edu/public-documents/dlib/

[4] Michael F. Goodchild, Alexandria Digital Library: Report on a Workshop on Metadata,http://www.alexandria.ucsb.edu/public-documents/metadata/metadata_ws.hml, November 1995

[5] Lagoze, Carl and Lynch, Clifford and Daniel, Ron, Jr. The Warwick Framework: A Container Architecture for Aggregating Sets of Metadata. Cornell Computer Science Technical Report TR96-1593, June, 1996,http://cs-tr.cs.cornell.edu:80/Dienst/UI/2.0/Describe/ncstrl.cornell%2fTR96-1593.

[6] The Library of Congress. Machine-Readable Cataloging.http://lcweb.loc.gov/marc/marc.html.

[7] Federal Geographic Data Committee, Content Standards for Digital Geospatial Metadata, http://geochange.er.usgs.gov/pub/tools/metadata/standard/metadata.html.

[8] Miller, Jim and Resnick, Paul and Singer, David, Rating Services and Rating Systems (and their Machine Readable Descriptions), Platform for Internet Content Selection Version 1.1,http://www.w3.org/pub/WWW/PICS/services.html, May 1996

[9] XML Linking Language (XLink), World Wide Web Consortium Working Draft 3-March-1998,http://www.oasis-open.org/cover/WD-xlink980303.html

著者紹介

이 요 섭 **[Yo-seob Lee]** 정회원

1990년 2월 : 숭실대학교 전자계산학과 졸업

1992년 2월 : 숭실대학교 컴퓨터공학과 석사

1999년 2월 : 숭실대학교 컴퓨터공학과 박사

1999년 3월 ~ 현재 : 숭실대학교 강사

〈관심분야〉 정보보안, 인터넷보안, 침입탐지

전 문 석 **[Moon-seog Jun]** 종신회원

1980년 2월 : 숭실대학교 전자계산학과 졸업

1986년 2월 : University of Maryland, Computer Science 석사

1988년 2월 : University of Maryland, Computer Science 박사

1991년 3월 ~ 현재 : 숭실대학교 컴퓨터학부 부교수

〈관심분야〉 정보보안, 인터넷보안, 침입탐지, 방화벽, 암호화 알고리즘