韓國 컴퓨터情報學會 論文誌
第14卷 第1號, 2009. 1.

2009-14-1-1-4

MCL: 메타데이터 레지스트리 접근제어를 위한 질의어

황 선 홍*, 김 진 형*, 정 동 원**, 백 두 권***

MCL: Query Language for Metadata Registry Access Control

Sunhong Hwang*, Jinhyung Kim*, Dongwon Jeong**, Doo-Kwon Baik***

요 약

다양한 분야에서 ISO/IEC 11179 기반의 MDR(Metadata Registry) 시스템들이 개발되었다. 그러나 현재 구축된 MDR시스템들은 표준을 엄격하게 준수하고 있지 않기 때문에 메타데이터 간 불일치 문제가 발생한다. 무엇보다 ISO/IEC 11179는 표준적인 접근 방법을 제공하지 않아 여러 가지 문제점을 초래한다. 이러한 문제점들을 해결하기 위해 SQL/MDR이 제안되었다. 그러나 현재의 SQL/MDR은 검색 기능만 지원할 뿐, MDR의 유효한 생성 및 안전한 접근을 위한 연산을 제공하지 않는다. 이 논문에서는 앞서 언급한 SQL/MDR 문제점 중에서, 안전하고 쉬운 접근제어를 보장할 수 있는 방법으로 MCL(Metadata Control Language)을 제안한다. MCL은 ISO/IEC 11179 Part 6에 정의되어 있는 사용자 그룹의 역할과 권한을 미리 정의하여 사용자를 사용자 그룹에 할당한다. 이러한 방법으로 MDL은 편이성과 보안성을 증대시킨다.

Abstract

In various fields, ISO/IEC 11179-based MDR (Metadata Registry) systems have been developed. However, the current systems do not observe the standard, so inconsistency issue between metadata arises. Most of all, there exist several problems because ISO/IEC 11179 provides no standardized access method. SQL/MDR has been suggested to resolve those problems. SQL/MDR supports search operations, but it does not provide operations for vaild building and safe access for MDR. This paper, in the aforementioned issues, suggests MCL(Metadata Control Language) to guarantee safe and easy access control. MCL offers predefined roles and authority of user groups defined in ISO/IEC 11179 Part 6, and users are assigned to a proper user group. With such a way, MCL increases usability and security.

▸ Keyword : 메타데이터 레지스트리(Metadata Registry), ISO/IEC 11179, 보안(Security), 접근 제어(Access control), SQL/MDR, RBAC, 메타데이터 제어언어(Metadata control language)

• 제1저자 : 황선홍 교신저자 : 백두권
• 투고일 : 2008. 11. 9, 심사일 : 2008. 11. 28, 게재확정일 : 2008. 12. 27.
* 고려대학교 컴퓨터·전파통신공학과, ** 군산대학교 정보통계학과 교수, *** 고려대학교 컴퓨터·전파통신공학과 교수
"이 논문은 2007년도 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임" (KRF-2007-331-D00448)

Ⅰ. 서 론

ISO/IEC 11179는 메타데이터 간 불일치에 의한 상호 운용성 문제 해결과 정보공유 및 교환의 용이성을 위하여 개발되었다[1]. 하지만, ISO/IEC 11179는 MDR 시스템 구현에 대한 표준적인 방법은 포함하고 있지 않으며 이로 인해 ISO/IEC 11179를 통해 개발된 MDR 시스템 간에 구조적, 의미적 이질성 문제가 다시 발생한다. 따라서 이러한 문제를 해결하기 위해 MDR에 대한 표준화된 접근 방법 (SQL/MDR)에 대한 연구가 진행되었으며, ISO/IEC 표준으로도 제안되어 현재 표준화가 진행 중이다[2-3]. 그러나 SQL/MDR에서도 MDR 시스템에 대한 접근 권한 관리 및 부여에 대해서는 고려하지 않고 있어 보안 측면에서 취약하다[4-6].

ISO/IEC 11179 표준에 따라 개발된 MDR 시스템은 크게 두 가지 특징을 갖는다. 첫째, MDR 접근 시 일정한 형태의 질의 연산 패턴을 갖는다. 다시 말해, 표준에서 요구하는 필수 기능을 제공해야 하므로 모든 MDR 시스템들은 일정한 질의 패턴을 지니게 된다. 둘째, MDR 시스템은 필수적인 구성요소를 제공한다. 현재까지 구축된 MDR들은 MDR 시스템 접근 시 사용되는 연산 패턴들에 대한 일관성 있는 접근방법을 고려하지 않았다. 이는 MDR 시스템 개발 시 ISO/IEC 11179를 준수하기 위해 매번 동일한 접근 연산 패턴을 다른 방법으로 개발함으로써 시간과 비용의 낭비를 초래한다. 또한 표준접근 방법을 제공하지 않기 때문에 MDR 접근 시 반드시 요구되는 제약조건이 고려되지 않는 경우가 발생한다. 이는 MDR간의 이질성 문제를 야기하고 표준화된 MDR 구축을 어렵게 한다. 그리고 ISO/IEC 11179에서는 기능에 대한 개략적인 설명만 있을 뿐 구체적인 스키마를 제공하지 않는다. 따라서 개발된 MDR 시스템마다 다른 구조와 명칭을 갖는 스키마를 사용하게 되며 이는 결국 MDR간의 이질성을 유발한다. 이러한 문제점 해결을 위해 ISO/IEC 11179에서 요구하고 있는 테이블과 속성을 정의하고 동일한 패턴을 지니는 접근연산들을 분석하여 일관성 있는 접근을 위한 SQL/MDR을 정의하였다. SQL/MDR은 국제표준 질의어인 SQL[7]을 기반으로 확장된 메타데이터 레지스트리 질의 언어로써 MDR 시스템에 대한 일관적인 접근 방법을 제공한다.

하지만, SQL/MDR은 MDR 시스템에 대한 검색기능 만을 정의하고 있으며, 접근 권한의 관리에 대해서는 고려하지 않는다. MDR 시스템에 대한 접근 권한 관리는 기존 SQL에 정의된 DCL을 이용하여 관리 가능하다. 하지만, MDR간의 메타데이터 공유 및 교환을 위하여 SQL 기반의 DCL을 사용할 경우 구현하는 과정이 복잡하여 사용성이 떨어지고, 사용자 권한 부여시 복잡한 과정을 거치다 보면 접근 보안상의 오류가 발생할 가능성이 크다.

따라서 이 논문에서는 SQL/MDR중 MDR접근제어에 대한 문제점을 해결하여 MDR 시스템 개발과 사용성 및 보안성을 높이기 위해 MDR 시스템 접근 권한 관리 언어 MCL(Metadata Control Language)을 제안한다. 구현된 MDR 접근제어 시스템은 ISO/IEC 11179의 규칙을 준수하고 활용을 위한 필수적인 기능들을 포함하고 있어 시스템 개발 프로세스 및 MDR 접근제어 구축을 위한 가이드로서 활용 가능하다. 또한 컴포넌트를 기반으로 설계 및 구현되었기 때문에 다양한 분야의 메타데이터 레지스트리 관리 시스템 개발을 위한 재사용이 용이하며 시스템 개발 시간과 비용을 감소시키고 일관적이고 정형화된 접근방법을 제공함으로써 편이성과 보안성 측면에서 우수하다.

이 논문의 구성은 다음과 같다. 제2장에서는 관련연구로서 ISO/IEC 11179의 개념과 SQL/MDR에 대해 기술한다. 제3장에서는 MCL 개념 및 연산자 그리고 규칙을 정의한다. 제4장에서는 구현 및 평가에 대하여 기술한다. 제5장에서는 결론에 대하여 기술한다.

Ⅱ. 관련 연구

2.1 ISO/IEC 11179 소개

ISO/IEC 11179는 데이터를 쉽게 이해하고 상호운용성을 높이기 위해 국제표준 기구인 ISO/IEC에서 제안된 표준이다. 이는 MDR간 데이터 공유 및 교환을 극대화하여 일관성 있는 데이터를 표현하고 구축하기 위한 국제 표준이다. MDR은 데이터 요소들의 집합이고, 데이터 요소는 정의, 식별, 표현 및 허용 가능한 값들의 속성 집합으로 데이터를 명세하기 위한 최소단위이다. 국내에서 구축된 MDR은 한국전자통신연구원의 컴포넌트의 원활한 사용을 위해 구축한 컴포넌트 메타데이터 레지스트리[8], 한국과학기술정보 연구원의 서지정보 메타데이터 레지스트리[9]가 있다. 해외에서 구축된 메타데이터 레지스트리는 미국 환경청의 환경 정보를 위한 EDR(Environmental Data Registry)[10-11], 호주 건강복지기간의 NHIK(Australian National Health Information Knowledgebase)[12-13] 등이 있다. 이들은 모두 국제 표준인 ISO/IEC 11179를 기반으로 구축되었으나 일관성과

표준화가 결여된 MDR 접근 방법을 사용하고 있기 때문에 MDR 간 이질성을 야기함으로써 국제표준인 ISO/IEC 11179의 혼란을 발생시킨다. 이는 결국 MDR간 메타데이터의 불일치를 야기하게 된다.

2.2 SQL/MDR

앞서 언급한 문제점을 해결하기 위해 SQL/MDR이 개발되었다. 즉, SQL/MDR의 목적은 메타데이터 간의 불일치를 해결하기 위해 메타데이터 레지스트리에 대한 표준 인터페이스를 제공하여 일관성 있는 접근 방법을 제공하는데 있다. 즉, MDR시스템 구현 시 연산패턴을 다른 방법으로 개발함으로써 시간과 비용의 낭비를 초래하고 제약조건이 고려되지 않고 개발되어 발생하는 MDR간의 이질성 문제를 해결하기 위해 SQL/MDR을 제안하여 현재 표준화가 진행 중이다. 이미 SQL/MDR과 유사한 접근방법들이 많은 데이터베이스 분야에서 이루어져 왔다. 공간 데이터의 표준 접근을 위한 공간 질의어(Spatial Query Language) 연구[14-15], 시간 데이터를 위한 시간 질의어(Temporal Query Language) 연구[15-16], 멀티미디어 데이터를 위한 SQL/MM[17]등이 그 예이며, 이들은 모두 국제 표준 질의 언어인 SQL을 기반으로 확장된 질의 언어들이다.

이와 같은 연구들은 각각 다른 구조를 지니는 데이터베이스를 상이한 구조에 무관하게 표준화된 접근을 위한 것이다. 즉 표준화된 접근 방법으로 다양한 데이터베이스를 일관성 있게 접근할 수 있게 해 준다. 따라서 각 구조에 독립적이고 일관성 있는 질의 모델링이 가능하며 질의 모델링 비용 및 분산된 다양한 데이터베이스로부터의 분산 처리 비용의 효율성을 제공한다.

그러나 비록 SQL/MDR이 일관성 있는 접근방법을 제공한다 해도 단순한 검색을 위한 방법만을 제공하며 이는 MDR에 대한 수정 연산과 구조 정의는 물론 접근 제어를 위한 추가적인 오버헤드를 요구하게 된다.

III. MCL 개념 및 정의

이 장에서는 ISO/IEC 11179의 명세를 바탕으로 MDR 접근에 대한 인터페이스로 MCL을 정의하고, MCL 세부 연산자인 MGRANT와 MREVOKE에 대하여 정의한다.

3.1 MCL(Metadata Control Language)

ISO/IEC 11179 Part6에는 사용자 그룹 및 각 사용자 그룹의 Role이 정의되어 있다. 이러한 정보를 기준으로 하여 개별 사용자에게 정확하고 편리하게 부여할 수 있도록 하는 언어를 제안하고 이를 MCL이라고 명명한다. 이러한 MCL은 SQL/MDR이 가지고 있는 사용성과 보안성 부분의 취약점을 개선한다. MCL은 MGRANT(GRANT FOR MDR)와 MREVOKE (REVOKE FOR MDR)가 있다.

MDR에서 사용자 그룹에 대한 역할과 권한에 대하여 정의하고 있으므로, 기 정의되어 있는 사용자 그룹과 권한을 DBMS상에서 구현하여 MCL 연산자로 사용자가 사용자 그룹의 권한을 주는 시스템을 구현한다. 구현된 MDR 접근제어 시스템은 ISO/IEC 11179의 규칙을 준수하고 활용을 위한 필수적인 기능들을 포함하고 있어 시스템 개발 프로세스 및 MDR 접근제어 구축을 위한 지침서로서 이용될 수 있다. 또한 컴포넌트를 기반으로 설계 및 구현되었기 때문에 다양한 분야의 메타데이터 레지스트리 관리 시스템 개발을 위한 재사용이 용이하며 시스템 개발 시간과 비용을 감소시키고 일관되고 정형화된 접근방법을 제공함으로써 사용의 편이성과 보안성을 향상시킨다. DCL을 이용한 MDR 보안모델의 구현도 가능하지만 DCL 기반으로 구현하기 위해서는 MDR에 대한 이해에 많은 시간이 들어가고, 구축 시에도 MDR 표준을 명확히 구현해야 하는 문제점이 있다.

3.2 MDR 사용자 그룹 Role정의

ISO/IEC 11179 Part 6 '데이터 요소의 등록'에서는 사용자, 제출자, 책임자, 등록자, 통제위원회, 집행위원회의 6개의 사용자 그룹으로 분류한다. 일반 사용자(Read- only user)는 메타데이터 내용을 검색(검토)하는 역할을 하고, 제출자(Submitter)는 새로운 메타데이터 관리항목을 제출하는 역할을 하고, 전문가(Stewards)는 메타데이터 관리항목의 품질을 검토 및 보장하고, 등록자(registrar)는 데이터 요소를 등록하고 관리하고 유지하는 역할을 하고, 통제위원회는 기술적 문제의 해결방향을 제시하고, 집행위원회는 MDR 전체정책과 방향을 결정하는 역할을 한다. 메타데이터 등록 프로세스와 관련된 등록 활동주체(RAB, Registration Acting Body)의 구성은 <그림 1>과 같다.

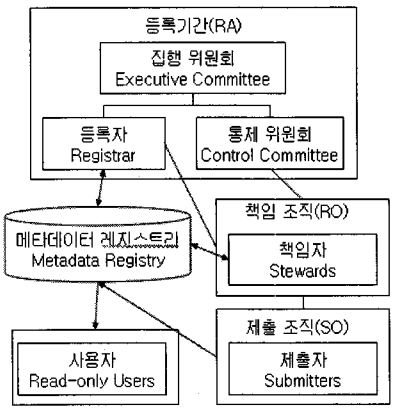


그림 1. MDR에 대한 조직별 Role과 관계
Fig. 1. Organizational roles to the Metadata Registry and their relationships

사용자 그룹별 세부 역할과 권한은 〈표 1〉과 같다.

표 1. 사용자 그룹의 역할과 권한
Table 1. Roles and privileges of user groups

User Group	Role	Privilege
Registrar	Monitoring and manualing the Metadata Registry contents Proposing procedures and standard formats for the MDR Recording current registration status for Administered Items Ensuring access for authorized users Assisting in the progression of Administered Items Enforcing data registration procedures Adding new users or organizational entities	Alter, Insert, Delete, Select
Executive Committee	Establishing overall Metadata Registry policies Resolution of all business management issues Ensuring the long-term success and performance of the Metadata Registry Establishing and updating the Metadata Registry charter and strategic plans Meeting periodically in face-to-face	Alter, Insert, Delete, Select
Control Committee	Overall conduct of registration operations. Promoting the reuse and sharing of data in the metadata register Progressing Administered Items Approving updates to Administered Items Proposing Metadata Registry policies to the Executive Committee for approval Approving authorized Submitters, Read-only Users Approving Metadata Registry content, procedures, and formats, Acting on directions from the Executive Committee	Alter, Insert, Delete, Select
Steward	Ensuring that appropriate Administered Items Reviewing all Administered Items once they are in the "Recorded" status Ensuring the quality of metadata attribute values for Administered Items Proposing "Standard" registration status level Administered Items. Proposing "Preferred Standard" registration status level Administered Items. Recommending Submitters to the Registration Authority	Select, Insert
Submitter	Submitting Administered Items to the metadata registry Ensuring the completeness of mandatory metadata attributes	Insert, delete, select
Read-only user	Retrieval(review) the contents of the metadata register	Select

3.3 MCL Operator정의

앞서 분석한 메타데이터 레지스트리에서 사용되는 연산 패턴 중 접근제어에 대해 표준 SQL을 확장하여 MCL로 정의하였다. MCL은 사용자에 대하여 객체에 대한 접근 권한을 다루는 MGRANT와 MREVOKE 라는 두 가지의 주요 연산자를 가진다. 권한을 부여하는 연산자를 MGRANT(GRANT FOR MDR)라고 정의하고, 권한을 회수하는 연산자를 MREVOKE (REVOKE FOR MDR)라고 정의하고 사용문법은 다음과 같다.

```
MGRANT USER_GROUP (ROLE) TO USER
MREVOKE USER_GROUP (ROLE) TO USER
```

3.4 MCL 사용 예제

이 절에서는 〈표 2〉, 〈표 3〉, 〈표 4〉에 기술되어 있듯이, 사용자와 사용자 그룹, 사용자 그룹과 역할, 역할과 권한의 관계를 표준 SQL문을 이용한 방법과 이미 정의된 MCL을 이용한 방법으로 비교한다.

표 2. 사용자와 사용자 그룹간의 관계
Table 2. The relationships between users and user groups

사용자	사용자 그룹
KIM	Read-only-users
SAM	Stewards

표 3. 사용자 그룹과 역할관계
Table 3. The relationships between user groups and roles

사용자그룹	Role
Read-only-users	데이터요소검색
Submitters	데이터요소검색
	데이터요소제출

표 4. 역할과 권한관계
Table 4. The Relationships roles and privileges

Role	Privileges	Tables
데이터요소검색	Select	Data_elements
데이터요소제출	Select,Insert,Update, DeleteData_elements	Data_elements

예제 1은 데이터요소 검색 Role을 Read_only_users 사용자 그룹에 부여하고 개별 사용자에게 권한을 부여하는 예이다. 예제 2는 데이터요소 검색 Role, 데이터요소 제출 Role을 Submitter 사용자 그룹에게 부여하고 개별 사용자에게 권한을 부여하는 예이다.

예제 1. Kim에게 Read_only_users 권한 부여

〈SQL의 DCL방식〉

(데이터요소검색)
create role 데이터요소검색
grant select on data_elements(table) to 데이터요소검색
(Read_only_users) Kim
create role Read_only_users
grant 데이터요소검색 to Read_only_users
grant Read_only_users to Kim

〈 MCL방식〉
MGRANT read_only_users TO Kim

예제 2. Sam에게 Submitters 권한 부여

〈SQL의 DCL방식〉
(데이터요소검색)
create role 데이터요소검색
grant select data_elements(table) to 데이터요소검색
(데이터요소제출)
create role 데이터요소제출
grant insert, update data_elements(table) to 데이터요소제출
(Submitters) sam
create role submitters
grant 데이터요소검색, 데이터요소제출 to submitters
grant submitters to sam

〈SQL/MDR의 MCL방식〉
MGRANT submitters TO sam

SQL의 DCL방식 사용시 개별 Role들을 순차적으로 부여하는 복잡성과 이로 인한 잘못된 권한 부여로 접근 시 문제가 있을 수 있다. 예제 1과 예제2 의 MCL을 사용하면 개별 사용자에게 사용자 그룹Role을 바로 부여하는 방법을 사용하기 때문에 사용상의 편이성과 접근제어의 일관성을 유지할 수 있게 해준다.

IV. 평 가

MCL Operator를 구현하는 방법으로는 Grant처럼 DBMS에 MCL Operator를 구현하는 방법과 ISO/IEC 11179 Part7의 SQL/MM처럼 User Define Type으로 구현하는 방법이 있다. 2007년 11월 ISO/IEC JTC1/SC32 WG4 회의에서 신규기능 추가 시 User Define Type으로 하기를 권장하고 있어 이 논문에서 구현은 User Define Type으로 한다.

4.1 사용자 그룹 정보

〈그림 2〉는 ISO/IEC 11179 Part 6 '데이터 요소의 등록'에서 분류한 사용자 그룹 중 사용자(Read only user)와 제출자(Submitters) 그룹의 역할, 역할의 데이터 요소에 대한 권한에 관한 내용이다. 즉, 사용자 SAM은 데이터 요소 테이블에 대하여 입력, 갱신, 삭제의 권한을 가지는 데이터요소 제출 역할과 데이터 요소 테이블에 대하여 검색의 권한을 가지는 데이터요소검색 역할을 가진다. 사용자 그룹 기준정보인 〈그림 2〉의 실선 부분을 미리 구축하여 MCL 연산자로 사용자에게 사용자그룹을 쉽게 부여 할 수 있도록 한다.

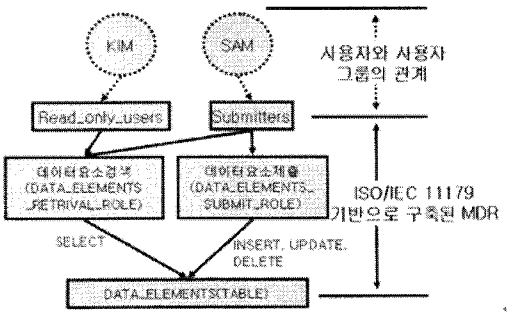


그림 2. ISO/IEC 11179에 기준한 사용자 그룹정보
Fig. 2. ISO/IEC 11179 based user group's information

4.2 ISO/IEC 11179 Part 6에 기반한 사전정보 구축

사전 정의된 Role과 권한과의 관계를 테이블로 구성하면 〈표 4〉와 같고, 사전 정의된 정보를 구성하는 과정은 아래와 같은 순서로 진행된다.

- create role 데이터요소검색
- grant select on data_elements (table) to 데이터요소검색
- create role 데이터요소제출
- grant insert, update, delete on data_elements (table) to 데이터요소제출

사용자 그룹과 Role과의 관계도 사전 정의된 내용을 테이블로 구성하면 〈표 3〉과 같이 되고 사전 정의된 정보를 구성하는 과정은 아래와 같은 순서로 진행된다.

- create role read_only_users
- grant 데이터요소검색 to Read_only_users
- create role submitters
- grant 데이터요소검색, 데이터요소제출 to Submitters

4.3 사용자 권한 부여 및 검증

ISO/IEC 11179에서 정의된 사용자 그룹과 역할관계를 DBMS로 미리 구성한 후 〈그림 3〉과 같이 MCL 연산자로 실제 사용자에게 사용자 그룹에 대한 권한을 부여한다.

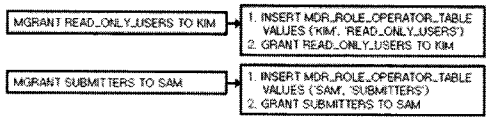


그림 3. MCL과 DCL관계
Fig. 3. The relationships between MCL and DCL

검증단계에서는 부여한 권한에 대한 정확성에 대하여 확인하도록 하겠다. 앞에서 부여한 권한을 보면 KIM은 DATA_ELEMENTS 테이블에 대하여 SELECT 권한만을 가지고 SAM은 DATA_ELEMENTS 테이블에 대하여 SELECT, INSERT, UPDATE, DELETE 권한을 가진다. 〈그림 4〉, 〈그림 5〉와 같이 DBMS상에 부여된 권한을 확인하면 KIM은 READ_ONLY_USERS 사용자 그룹에 속하고 DATA_ELEMENTS 테이블에 대하여 Select 권한을 가지고, SAM은 SUBMITTERS 사용자 그룹에 속하고 DATA_ELEMENTS 테이블에 대하여 SELECT, DELETE, INSERT, UPDATE 권한을 가진다.

```
select USERNAME, y.USER_GROUP, GRANTED_ROLE, PRIVILEGE, TABLE_NAME
from
    (select TABLE_NAME, PRIVILEGE, a.GRANTED_ROLE, USER_GROUP
    from
        (select ROLE GRANTED_ROLE, TABLE_NAME, PRIVILEGE from ROLE_TAB_PRIVS) a,
        (select ROLE USER_GROUP, GRANTED_ROLE from ROLE_ROLE_PRIVS) b
    where a.GRANTED_ROLE=b.GRANTED_ROLE) x,
    (select USERNAME, GRANTED_ROLE USER_GROUP from USER_ROLE_PRIVS) y
where x.USER_GROUP=y.USER_GROUP;
```

USERNAME	USER_GROUP	GRANTED_ROLE	PRIVILEGE	TABLE_NAME
KIM	READ_ONLY_USERS	DATA_ELEMENTS_RETRIVAL_ROLE	SELECT	DATA_ELEMENTS

그림 4. KIM의 권한 확인
Fig. 4. Confirmation of Kim's privileges

```
select USERNAME, y.USER_GROUP, GRANTED_ROLE, PRIVILEGE, TABLE_NAME
from
    (select TABLE_NAME, PRIVILEGE, a.GRANTED_ROLE, USER_GROUP
    from
        (select ROLE GRANTED_ROLE, TABLE_NAME, PRIVILEGE from ROLE_TAB_PRIVS) a,
        (select ROLE USER_GROUP, GRANTED_ROLE from ROLE_ROLE_PRIVS) b
    where a.GRANTED_ROLE=b.GRANTED_ROLE) x,
    (select USERNAME, GRANTED_ROLE USER_GROUP from USER_ROLE_PRIVS) y
where x.USER_GROUP=y.USER_GROUP;
```

USERNAME	USER_GROUP	GRANTED_ROLE	PRIVILEGE	TABLE_NAME
SAM	SUBMITTERS	DATA_ELEMENTS_RETRIVAL_ROLE	SELECT	DATA_ELEMENTS
SAM	SUBMITTERS	DATA_ELEMENTS_SUBMIT_ROLE	DELETE	DATA_ELEMENTS
SAM	SUBMITTERS	DATA_ELEMENTS_SUBMIT_ROLE	INSERT	DATA_ELEMENTS
SAM	SUBMITTERS	DATA_ELEMENTS_SUBMIT_ROLE	UPDATE	DATA_ELEMENTS

그림 5. SAM의 권한 확인
Fig. 5. Confirmation of Sam's Privileges

사용자 KIM과 SAM의 권한에 대하여 검증하기 위해 질의문 Q1, Q2, Q3, Q4를 다음과 같이 만들었다.

```
Q1) SELECT REG_AUTH_IDENTIFIER, DATA_IDENTIFIER,
    VERSION, CREATION_USER FROM
    MDR.DATA_ELEMENTS;

Q2) UPDATE MDR.DATA_ELEMENTS SET
    CREATION_USER='KIM' WHERE
    REG_AUTH_IDENTIFIER=200800001
    AND DATA_IDENTIFIER=200804001 AND VERSION=1 ;

Q3) INSERT INTO MDR. DATA_ELEMENTS(
    REG_AUTH_IDENTIFIER, DATA_IDENTIFIER,VERSION,
    RESPONSIBILITY_NAME,  CREATION_USER)
    VALUES(200800002, 200804002, 2, 'DEFAULT', 'SAM');

Q4) DELETE FROM MDR.DATA_ELEMENTS WHERE
    REG_AUTH_IDENTIFIER=200800002 AND
    DATA_IDENTIFIER=200804002 AND VERSION=2;
```

```
SQL> CONN KIM/KIM
연결되었습니다.
SQL> SELECT REG_AUTH_IDENTIFIER, DATA_IDENTIFIER, VERSION, CREATION_USER
  2  FROM MDR.DATA_ELEMENTS;

REG_AUTH_IDENTIFIER DATA_IDENTIFIER    VERSION CREATION_USER
------------------- ------------------ ------- ------------
          200800001          200804001       2 KIM

SQL> UPDATE MDR.DATA_ELEMENTS SET CREATION_USER='KIM'
  2  WHERE REG_AUTH_IDENTIFIER=200800001
  3        AND DATA_IDENTIFIER=200804001 AND VERSION=1;
UPDATE MDR.DATA_ELEMENTS SET CREATION_USER='KIM'
                *
1행에 오류:
ORA-01031: 권한이 불충분합니다

SQL> INSERT INTO MDR.DATA_ELEMENTS(REG_AUTH_IDENTIFIER, DATA_IDENTIFIER,
  2                    VERSION, RESPONSIBILITY_NAME, CREATION_USER)
  3  VALUES(200800002, 200804002, 2, 'DEFAULT', 'SAM');
INSERT INTO MDR.DATA_ELEMENTS(REG_AUTH_IDENTIFIER, DATA_IDENTIFIER,
            *
1행에 오류:
ORA-01031: 권한이 불충분합니다

SQL> DELETE FROM MDR.DATA_ELEMENTS
  2  WHERE REG_AUTH_IDENTIFIER=200800002
  3        AND DATA_IDENTIFIER=200804002 AND VERSION=2;
DELETE FROM MDR.DATA_ELEMENTS
            *
1행에 오류:
ORA-01031: 권한이 불충분합니다
```

그림 6. KIM의 권한 검증
Fig. 6. Verification of Kim's privileges

DATA_ELEMENTS 테이블에 대하여 SELECT 권한만 가지는 사용자 KIM에 대한 Q1, Q2, Q3, Q4의 실행 결과 〈그림 6〉과 같이 Q1은 정상 실행이 되고, Q2, Q3, Q4는 권한 오류가 정상적으로 발생하였다.

```
SQL> CONN SAM/SAM
연결되었습니다.
SQL> SELECT REG_AUTH_IDENTIFIER, DATA_IDENTIFIER, VERSION, CREATION_USER
  2  FROM MDR.DATA_ELEMENTS;

REG_AUTH_IDENTIFIER DATA_IDENTIFIER    VERSION CREATION_USER
------------------- ------------------ ------- ------------
          200800001          200804001       1 KIM

SQL> UPDATE MDR.DATA_ELEMENTS SET CREATION_USER='KIM'
  2  WHERE REG_AUTH_IDENTIFIER=200800001
  3        AND DATA_IDENTIFIER=200804001 AND VERSION=1;

1 행이 갱신되었습니다.

SQL> INSERT INTO MDR.DATA_ELEMENTS(REG_AUTH_IDENTIFIER, DATA_IDENTIFIER,
  2                    VERSION, RESPONSIBILITY_NAME, CREATION_USER)
  3  VALUES(200800002, 200804002, 2, 'DEFAULT', 'SAM');

1 개의 행이 만들어졌습니다.

SQL> DELETE FROM MDR.DATA_ELEMENTS
  2  WHERE REG_AUTH_IDENTIFIER=200800002
  3        AND DATA_IDENTIFIER=200804002 AND VERSION=2;

1 행이 삭제되었습니다.
```

그림 7. SAM의 권한 검증
Fig. 7. Verification of Sam's privileges

DATA_ELEMENTS 테이블에 SELECT, UPDATE, INSERT, DELETE을 가지는 사용자 SAM에 대하여 Q1, Q2, Q3, Q4 실행 결과는 〈그림 7〉과 같이 Q1, Q2, Q3, Q4가 권한 오류 없이 정상적으로 실행되었다.

4.4 비용 평가

〈그림 8〉과 같이 MDR 접근제어를 DCL을 사용하여 개별적으로 구현하는 방법과 〈그림 9〉와 같이 ISO/IEC 11179에 정의된 사용자별 공통된 접근제어를 MCL 사용하여 구현하는 방법을 시간 비용측면에서 비교하기 위한 계산 모델은 다음과 같다.

먼저, DCL 접근방식의 경우 개발비용은 다음과 같다.

$$Cost(DEV_{PREV}) = [n] \times [\, AnalMDR_T + (MDRAC_{PREV})_T \,] \quad \cdots\cdots (2.1)$$

. $AnalMDR_T$: MDR의 사용자별 권한과 역할 분석 시간
. $(MDRAC_{PREV})_T$: DCL을 이용한 MDR접근제어 개발 시간

계산 모델에서 $AnalMDR_T$는 MDR의 사용자별 권한과 역할 분석 시간을 의미하며, $(MDRAC_{PREV})_T$는 DCL을 이용한 MDR 접근제어 개발 시간을 나타낸다.

반면, MCL 접근방식의 경우 개발 비용은 다음과 계산 모델에 의해 산출된다.

$$Cost(DEV_{MCL}) = [\, AnalMDR_T + (MDRAC_{MCL})_T \,] \quad \cdots\cdots (2.2)$$

. $AnalMDR_T$: MDR의 사용자별 권한과 역할 분석 시간
. $(MDRAC_{PREV})_T$: MCL을 이용한 MDR접근제어 개발 시간

접근제어를 개발하는 시간은 유사하다고 가정하면, 시스템 개수에 따른 DCL을 이용한 접근제어를 개발하는 시간비용과 MCL을 이용한 접근제어를 개발하는 시간비용은 다음과 같은 계산 모델에 의해 측정된다.

$$\begin{aligned} Cost(DEV_{PREV}) &= [n] \times [\, AnalMDR_T + (MDRAC_{MCL})_T \,] \\ &= n \cdot Cost(DEV_{MCL}) \\ &= n \cdot C \end{aligned} \quad \cdots\cdots (2.3)$$

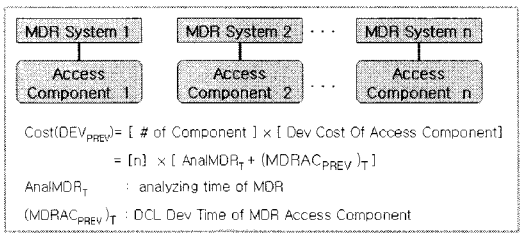


그림 8. DCL을 이용한 접근제어
Fig. 8. Access control using DCL

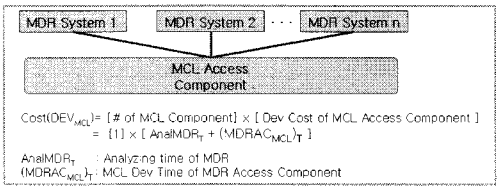


그림 9. MCL을 이용한 접근제어
Fig. 9. Access control using MCL

즉, 〈그림 10〉과 같이 기존의 DCL을 사용하여 개발하는 경우가 MCL을 이용하여 개발하는 경우보다 시스템의 개수만큼의 비율로 개발 비용이 증가한다. 다수의 MDR시스템 구현시는 제안하는 시스템이 우수하다.

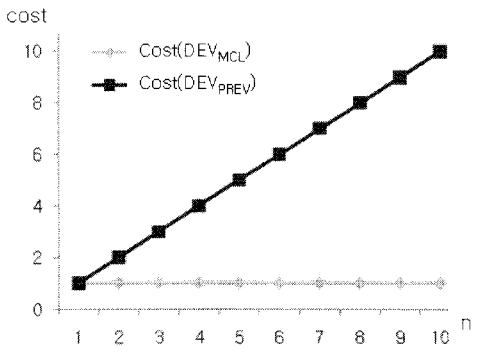


그림 10. 개발 시간 비용 그래프
Fig. 10. The cost graph of development time

4.5 특성비교

DCL과 MCL의 특성을 비교해 보면 〈표 5〉와 같이 MCL은 처리구조가 간단하여 사용이 편하고 미리 정의된 구조를 사용하므로 보안성이 우수하다.

표 5. DCL과 MCL비교
Table 5. Compare DCL with MCL

항목	DCL	MCL
활용성	낮음	높은
정확성 유지비용	높음	낮음
보안 정책 생성 용이성/보안성	복잡/낮음	단순/높음
정책 규칙의 일관성 유지	어려움	용이함

V. 결론 및 향후 연구

MDR은 메타데이터의 관리 및 상호 운용성 향상을 위하여 개발된 ISO/IEC 11179의 핵심요소이며, 다양한 분야에서 MDR 시스템들이 개발되었다. 그러나 시스템들이 MDR표준을 따르지 않고 개발되거나 구축되어 MDR 간 메타데이터 불일치가 발생하고 MDR 간에 데이터를 공유하고 교환할 수 있는 표준화된 연산자가 없어 개발비용 및 시간이 많이 드는 문제가 있다.

이러한 문제를 해결하기 위해 SQL/MDR이 제안되었으나 SQL/MDR은 검색을 위한 연산만을 지원하고 있다. 즉, 메타데이터에 대한 수정, 삭제, 추가는 물론 구조의 일관성 있는 정의 및 접근제어를 위한 연산은 제공하지 않는다. 특히 접근제어는 안전하고 정형화 된 MDR에 대한 보안을 위해 필수적으로 지원되어야 한다.

이 논문에서는 ISO/IEC 11179 Part 6에서 제안하는 사용자 그룹별 권한과 역할을 미리 구축하고 MCL이라는 연산자를 제공하여 시스템 관리자가 표준 및 저장 구조에 대한 명확한 이해와 사용자 권한에 대한 이해 없이도 접근 시스템을 쉽고 안전하게 개발할 수 있도록 했다. 먼저 MCL의 개념 및 정의에 대해서 기술하고 MDR사용자 그룹의 Role을 검토하여 MCL Operator를 정의하였다. 또한 DCL과 MCL방법을 비교하고 MCL Operator를 구현하고 검증을 하였다.

향후 연구 과제로 MDR 구축시 메타데이터간 불일치 해결을 위한 MDR 조작 언어와 MDR 구조를 생성하는 언어에 대한 연구가 필요하다.

참고문헌

[1] ISO/IEC JTC 1/SC 32, "ISO/IEC 11179: Specification and standardization of data elements, Part 1~6," 2003.

[2] 신동길, 김영갑, 정동원, 박수현, 백두권, "메타데이타 레지스트리의 일관성 있는 접근을 위한 질의 언어," 정보과학회 논문지, 데이타베이스 제 31권, 제6호, 609~623쪽, 2004년 12월.

[3] Dongwon Jeong, Young-Gab Kim, and Hoh Peter In, "Quantitative Evaluations on the Query Modeling and System Integrating Cost of SQL/MDR," ETRI Journal, Volume, Number 4, pp. 367~376, August 2005.

[4] 황선홍, 김진형, 정동원, 김희석, 백두권, "RBAC기반의 메타데이타 레지스트리 접근제어 모델," 한국정보과학회 2008 종합학술대회 논문집 제35권 제1호(C), 165~170쪽, 2008년 6월.

[5] 이유리, 박동규, "모바일 환경에 적합한 헬스 케어 정보 시스템에서의 역할기반 접근제어," 한국컴퓨터정보학회 논문지 제10권, 제3호, 119~132쪽, 2005년 7월.

[6] 문형진, 서정석, "역할기반 접근제어시스템에 적용 가능한 민감한 개인정보 보호모델," 한국컴퓨터정보학회논문지 제13권, 제5호, 103~110쪽, 2008년 9월.

[7] ISO/IEC JTC 1/SC 32/WG 3, "ISO/IEC 9075, Database Language SQL3, Part1~10," 1999.

[8] ETRI, *"Research on the Registration and Search System of Component,"* Research Report, 2002.

[9] KISTI, *"A Study on The Development of Standardization and Management Model for Science and Technology Information,"* Research Report, 2002.

[10] EPA, Environmental Data Registry, *http://www.epa.gov/edr/*

[11] EPA, *"Data Standards Publications and Guidances,"* 2003.

[12] AIHW, Australian National Health Information Knowledgebase, *http://www.aihw.gov.au/*

[13] Australian National Health Data Committee, *"National Health Data Dictionary,"* 2003.

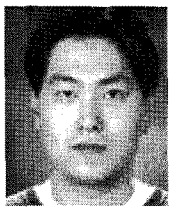
[14] Egenhofer, M. "Spatial SQL: A query and presentation

language," IEEE Transactions on Knowledge and Data Engineering, Vol. 6, No. 1, pp. 86~95, 1994.
[15] Lee, J.-Y., "Integrating Spatial and Temporal Relationship Operators into SQL3 for Historical Data Management," ETRI Journal, Vol. 24, No. 3, pp. 226~238, 2002.
[16] Pissinou, N., Snodgrass, R., Elmasri, R., Mumick, I., Ozsu, T., Pernici, B., Segev, A., Theodoulidis, B., and Dayal, U., "Towards an Infrastructure for Temporal Databases: Report of An Invitational ARPA/NSF Workshop," Vol. 23, No. 1, pp. 35-51, In SIGMOD Record, 1994.
[17] ISO/IEC JTC 1/SC 32, "ISO/IEC 13249: Information Technology-Database Languages-SQL Multimedia and Application Packages," 2003.

저 자 소 개

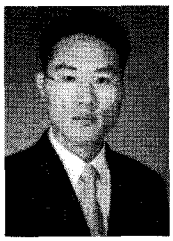
황 선 홍

1998: 부산대학교 전자공학과 공학사
현재: 삼성전자 반도체총괄 책임연구원, 고려대학교 컴퓨터·전파통신 공학과 석사과정
관심분야: 메타데이터 레지스트리, 정보보안, 접근제어



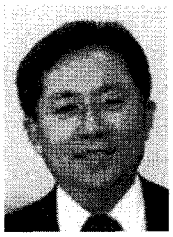
김 진 형

2004: 홍익대학교 컴퓨터공학과 공학사
2006: 고려대학교 컴퓨터학과 이학석사
현재: 고려대학교 컴퓨터학과 박사과정, 고려대학교 컴퓨터정보통신연구소 연구원
관심분야: 데이타베이스, XML, 유비쿼터스 컴퓨팅, 시맨틱웹, 온톨로지



정 동 원

1997: 군산대학교 컴퓨터과학과 이학사
1999: 충북대학교 전산과 이학석사
2004: 고려대학교 컴퓨터학과 이학박사
1998: 전자통신연구원 위촉연구원
1999~2000: ICU 부설 한국정보통신교육원 GIS 분원 전임강사,
2000~2001:지구넷 부설 연구소 선임연구원, 2002~2005:라임디미디어 테크놀로지 연구원
2004~2005:고려대학교 정보통신기술연구소 연구조교수
2005: Pennsylvania State University PostDoc
2002~2004: TTA 표준화위원회-데이터연구회 (SG08.02) 특별위원
현재: 군산대학교 정보통계학과 교수, TTA 표준화위원회-메타데이타 표준화 프로젝트 그룹(PG406) 위원, ISO/IEC JTC1/SC32 국내위원회 위원, ISO/TC211 국내위원회 위원
관심분야: 데이타베이스, 시맨틱 웹, 시맨틱 GIS, 유비쿼터스 컴퓨팅, 정보보안



백 두 권

1974: 고려대학교 수학과 학사
1977: 고려대학교 산업공학과 석사
1983: Wayne State Univ. 전산학과 석사
1985: Wayne State Univ. 전산학과 박사
현재: 고려대학교 컴퓨터학과 교수, ISO/IEC JTC1/SC32 국내위원회 위원장, 정보통신진흥협회 데이터기술위원회 의장, 한국 시뮬레이션학회 고문
관심분야:데이터베이스, 소프트웨어공학, 데이터 공학, 컴포넌트 기반 시스템, 메타데이터 레지스트리, 정보 통합, 프로젝트 매니지먼트