

# DRM 사용자간 재배포를 위한 라이선스관리 모델 설계☆

## Design of License Management Model for super-distribution between DRM Consumers

이 병 옥\*                      유 중 화\*\*  
Byung-wook Lee              Zong-Hua Liu

### 요 약

DRM 시스템의 재배포 기능은 디지털 콘텐츠 산업 활성화에 필수적이다. 기존의 DRM은 지적재산권의 안전에 치중하였기 때문에 배포에 대한 제약과 소비자 권리를 억제하는 요소가 된다. 본 연구는 사용자간 재배포를 강화할 수 있는 라이선스관리 모델을 제시한다. 배포 시에 콘텐츠 헤더에 사용자의 식별정보를 넣어서 배포함으로써 배포 이력을 관리한다. 라이선스 발급 후에는 클라이언트가 헤더와 라이선스의 식별정보를 비교하여 안전을 확인한다. 배포 형식과 라이선스를 유형별로 분류하여 적합한 배포 방식을 적용하고 적합한 라이선스를 발급함으로써 배포를 활성화할 수 있다.

### Abstract

Super-distribution is essential for revitalization of digital contents industry in DRM system. Since existing DRM systems emphasize on security for intellectual property rights, it became restrictions to content distribution and the consumer rights. This paper suggests license management mechanism which strengthen super-distribution between consumers. It is to manage distribution history for each content by inserting consumer's identification information in content head. Client can verify security by comparing header and license after issuing license. It classifies the type of distribution and license, and then applies adaptive distribution methods. It can revitalize contents distribution by releasing proper license for super-distribution.

키워드 : Digital right management, distribution, license, right expression language

## 1. 개요

인터넷과 미디어 기술의 발전으로 인하여 디지털 콘텐츠 시장이 급속하게 증대되고 있다. 다양한 분야와 형태의 콘텐츠를 공급하고 수요가 요구되는 콘텐츠 시장에서는 유통 수단의 안전이 중요하다. DRM은 콘텐츠 유통의 전체 과정에서 불법 복제와 불법 유통으로부터 콘텐츠를 안전하게 보호하고 체계적으로 관리함으로써 콘텐츠 산업의 발전에 기여하고 있다.

미국 저작권법의 Fair Use Doctrine에 의하면 소비자가 콘텐츠 구매하면 개인적인 용도로 예비 저장할 수 있고, 남에게 빌려줄 수도 있고, 다시 판매할 수도 있다. 그러나 DRM은 자신이 구매한 콘텐츠라도 사용을 엄격히 제한함으로써 소비자 권리를 침해하는 요소가 있다. DRM은 콘텐츠를 안전하게 보호하는 기능과 함께 콘텐츠를 원활하게 배포하는 이중 기능을 제공해야 한다[1].

콘텐츠의 원활한 재배포를 위해서는 라이선스 소유자가 여러 사용자들에게 라이선스를 제공할 수 있는 재배포 기능이 필요하고, 라이선스를 재배포 받은 사용자가 다시 다른 사용자에게 재배포할 수 있는 이월전달(passover) 기능이 필요하다. 이를 위해 사용자가 라이선스를 다른 사용자에게 원활하게 재배포할 수 있는 새로운 라이선

\* 중신회원 : 경원대학교 소프트웨어학부 교수  
leebw@kyungwon.ac.kr(교신저자)

\*\* 준회원 : 경원대학교 전자계산학과 석사과정  
lzh5333@hotmail.com

[2006/12/15 투고 - 2007/01/04 심사 - 2007/03/09 심사완료]

☆ 이 논문은 경기도 차세대성장동력기술개발사업과 BK21에 의하여 연구되었음

스관리 모델이 요구된다.

라이선스관리란 DRM의 핵심 요소이다. 콘텐츠가 배포되는 형태를 분류하고 이를 분석하여 재배포에 적합한 라이선스관리 모델을 제안한다. 본 연구에서는 재배포 트랜잭션의 처리율과 적용 범위가 대규모가 아닌 업무에 적용하도록 권리 표현 언어 REL의 일종인 ODRL을 이용하여 재배포 권리를 표현하는 기법을 제시한다[2].

## 2. 라이선스 배포와 REL

### 2.1 라이선스 배포

콘텐츠의 합법적인 유통 수단으로 DRM이 발전되었으나 번거로운 절차로 인식되어 콘텐츠 유통에 걸림돌이 될 수 있다. 콘텐츠 유통이 활성화 되려면 사용자들 사이에 라이선스가 안전하고 쉽게 재배포 되어야 한다. 현재 사용자들은 공급자로부터 콘텐츠를 사용할 수 있는 라이선스를 직접 구매해야 한다. 유통의 편리를 위해서는 사용자 간에 라이선스를 배포시킬 수 있는 안전한 배포 모델이 필요하다.

기존의 라이선스는 그룹 배포도 쉽지 않고, 사용자가 라이선스를 다른 사용자에게 인도하기도 어렵다. 그러나 소비자의 권리 측면에서는 사용자가 자신의 재산을 일정 부분 권리 행사할 수 있어야 한다. 따라서 콘텐츠 구매 조건에 따라서 콘텐츠를 한정된 수의 사용자에게 양도할 수 있는 그룹 배포 기능과 사용자간 재배포 기능이 필요하다[1]. 라이선스를 구매하는 사용자와 재배포 받는 사용자에게 따라서 상이한 라이선스를 생성하고 관리할 수 있는 새로운 모델이 요구된다.

### 2.2 REL

REL(Right Expression Language)은 사용자/장치 가 허용 받은 권리인 콘텐츠의 사용 조건을 잘 표현하기 위해 정의된 언어이다. 가장 관련 있는

REL은 XrML을 기반으로 하는 MPEG-21과 Renato Iannela가 제안한 ODRL이다. 이들은 모두 구조적으로 권리 모델링의 자명한 원리에 일치하며, XML에 기반하고 있다[2].

XrML은 DRM을 위한 XML 기반의 범용 언어로서, 웹 서비스 접근에 필요한 권리와 조건을 구축해주는 수치 권리 언어의 능력을 확충하였다. 또한 MPEG 표준에서도 XrML을 도입하였다[5]. MPEG-21 REL은 ISO/IEC의 공식 표준이고, ODRL은 OMA가 채택한 실제 산업계의 주역이다. MPEG21은 보다 완벽하지만 복잡하고, ODRL은 보다 융통성이 있다. ODRL은 수치 자원들을 지원하기 위하여 상호 운용할 수 있는 메커니즘을 제공하기 위해 고안되었다[3].

기존 메커니즘에서는 하나의 라이선스에 여러 허가를 포함하거나, 하나의 허가에 여러 주체(party)들에 대한 권리를 표현하는 것이 가능하다. 그러나 하나의 주체가 다수의 다른 주체들에게 자신의 권리를 공유하게 하지는 못한다. 따라서 부주체(subparty) 등을 추가하여 다양한 권리를 부주체가 공유하는 새로운 모델이 필요하다[8].

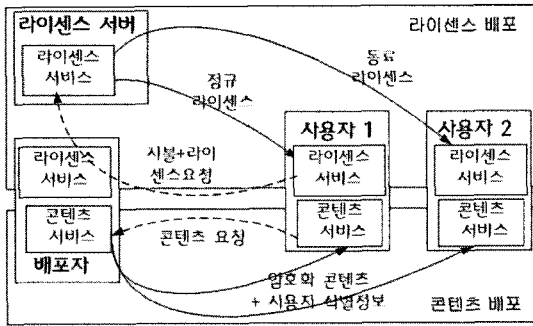
## 3. 재배포를 위한 소프트웨어 서비스

### 3.1 배포 서비스의 이원 구조

재배포에 직접 관련된 개체는 배포자(distributor), 라이선스 서버, 사용자 등으로 구성된다. 설계의 1차적인 관점은 콘텐츠 헤더에 사용자 식별정보를 기억하여 배포 이력을 관리하는 것이며, 2차적으로 사용자 간에 라이선스를 재배포하고, 3차적으로 사용자 프로그램이 콘텐츠 헤더와 라이선스의 식별정보를 비교하여 라이선스의 안전을 확인하는 것이다[3].

콘텐츠와 라이선스를 별도로 재배포하는 기능을 중심으로 소프트웨어 구조를 설계한다. 공통되는 기능들은 서비스를 공용으로 작성하여 각 개체에서 운영한다. <그림 1>은 콘텐츠와 라이선스

배포가 2원화된 서비스 모델이다.[4][6]. 다음은 <그림 1>의 각 개체를 구성하고 있는 서비스들의 기능이다.



<그림 1> 재배포 서비스 모델

(1) 배포자 : 콘텐츠를 배포하고, 라이선스 발급을 요청하는 개체.

콘텐츠 서비스 : 콘텐츠 헤더에 사용자 식별 정보를 삽입하여 배포한다. 구매 사용자의 요청에 의하여 비 구매 사용자에게도 같은 방식으로 콘텐츠를 제공한다.

라이선스 서비스 : 라이선스 서버에게 라이선스 발급을 요청한다.

(2) 라이선스 서버 : 사용자에게 라이선스를 제공하고, 관리하는 개체.

라이선스 서비스 : 구매자에게 정규 라이선스(official license)를 제공하고, 비 구매자에게 동료 라이선스(peer license)를 제공한다[11].

(3) 사용자 1 : 정규 라이선스로 콘텐츠를 소비하는 개체.

라이선스 서비스 : 콘텐츠 헤더와 라이선스의 사용자 식별정보를 비교하여 해독 키를 추출한다.

콘텐츠 서비스 : 배포자로부터 콘텐츠를 받고, 라이선스 서비스로부터 해독 키를 받아서 콘텐츠를 해독한다. 배포자에게 다른 사용자의 식별정보를 주고 콘텐츠 재배포를 요청한다.

(4) 사용자 2 : 동료 라이선스로 콘텐츠를 소비하는 개체.

라이선스 서비스 : 동료 라이선스와 콘텐츠의 식별정보와 비교하여 해독 키를 추출한다.

콘텐츠 서비스 : 라이선스 서비스로부터 해독 키를 받아 콘텐츠를 해독한다.

### 3.2 라이선스 관리

배포자는 사용자 식별정보를 헤더에 삽입하여 콘텐츠를 제공하고, 라이선스에는 사용자의 장치 식별자, URL 등의 식별정보와 해독 키가 사용자의 공개키로 암호화되어 있다. 라이선스는 구매 여부에 따라서 라이선스를 정규 라이선스와 동료 라이선스로 나누어 관리한다.

#### (1) 정규 라이선스

정규 라이선스는 기존 DRM의 라이선스 개념과 동일하며, 부가적으로 다른 사용자에게 동료 라이선스를 제공하여 권리를 양도할 수 있으므로 이월전달이 가능하다[5][9]. 구매자는 자신과 다른 사용자의 식별정보를 제공하고 라이선스에 배포 이력을 반영하여 해당 사용자만 사용하도록 한다.

#### (2) 동료 라이선스

동료 라이선스는 라이선스 소유자가 요청하여 라이선스 서버에 의하여 다른 사용자에게 발급되며, 정규 라이선스의 계약 조건 내에서 계약이 성립된다. 동료 라이선스 발급 요청 시 다른 사용자의 식별정보와 URL 등을 요청하는 사용자가 제공해야 한다.

#### (3) 사용자 라이선스 서비스

사용자의 라이선스 서비스는 콘텐츠 헤더의 사용자 식별정보와 라이선스 내의 식별정보를 확인하여 일치하면 해독 키를 추출하여 사용자의 콘텐츠 서비스에게 제공한다.

(4) 라이선스 갱신

라이선스 서버는 동료 라이선스 발급 시에 정규 계약서에서 동료 계약서의 권리조건을 제외하고 라이선스를 갱신한다. 기존의 계약자들도 계약을 변경하면 라이선스를 갱신한다. 갱신 결과는 사용자의 라이선스 서비스에게 전송한다.

(5) 라이선스의 폐기

라이선스 서버는 계약조건이 만료되면 라이선스를 폐기하고, 폐기 내용을 각 사용자들의 라이선스 서비스에게 제공한다. 사용자 라이선스 서비스는 해독 키를 제거하여 콘텐츠 서비스의 기능을 정지시킨다.

대한 사용자 Q의 사용 규칙을 정의한다. 사용 규칙은 사용 횟수, 사용 시간, 사용 일자의 조건과 이 조건에 충족될 때 주어지는 인쇄, 실행, 보기 등의 구체적인 권한이다[5].

[정의 2] 사용자간 재배포

사용자간 재배포는  $\langle r, n, po \rangle$ 로 정의한다. 한 사용자가 다른 사용자에게 자원  $r$ 을  $n$ 명에게 재배포할 수 있고,  $po$ 번 이월전달할 수 있다.

예를 들어  $\langle r_3, 5, 2 \rangle$ 는 자원  $r$ 을 5명에게 재배포 가능하고, 이월전달은 2번 가능하다.  $\langle r_3, 4, 0 \rangle$ 는 자원  $r$ 을 4명의 사용자에게 재배포 가능하고, 이월전달은 불가능한 경우이다.  $\langle r_3, 0, 0 \rangle$ 는 재배포가 불가능한 라이선스이다.

4. 재배포를 위한 라이선스 모델

4.1 사용자간 재배포 요소 정의

재배포 기법의 각 요소 작업에 대한 정의를 정확하게 기술하기 위해 명제논리와 술어논리를 이용하여 술어 해석식으로 주요 기능을 논증한다.

[정의 1] 라이선스 발급

라이선스 발급은 튜플  $\langle P, R, U \rangle$ 의 3 가지 요소로 정의한다.  $P$ 는 라이선스 배포를 요청하는 사용자와 라이선스를 수령하는 사용자 주체들의 튜플이다.  $R$ 은 특정한 자원  $r$ 의 재배포 조건을 표현하는 튜플이다.  $U$ 는 사용 규칙을 표현하는 논리식 명제이다.

사용자  $P$ 는 라이선스를 요청하며,  $Q$ 는 라이선스를 수령하는 사용자이다.  $P$ 가  $Q$ 와 같으면 자신의 라이선스를 구매 요청하는 것이고, 다르다면 다른 사용자의 라이선스 재배포를 요청하는 것이다.  $R$ 은 라이선스 대상 자원을 지정하고, 재배포를 받는 사용자의 수와 사용자가 다시 재배포할 수 있는 이월전달의 수를 지정한다.  $U$ 는 자원  $R$ 에

[정의 3] 라이선스 그룹 재배포

그룹 라이선스 재배포란 라이선스를 가진 사용자가 다른 사용자들에게 동일한 라이선스를 인도하는 것으로 튜플  $\langle p, \{q_1, q_2, \dots, q_n\} \rangle$ 로 정의한다.  $p$ 는 라이선스 발급 요청자이고  $q_i$ 는 라이선스 발급 대상자 집합이다.

$q$ 가  $p$ 와 같다면 요청자가 직접 라이선스 구매를 요청하는 것이고, 다르다면 사용자간 재배포하는 것이다.  $q$ 의 수는 그룹 대상자의 수이다. 라이선스를 가진 사용자  $p_1$ 이 사용자  $q_1, q_2, q_3$ 에게 그룹 라이선스 재배포를 요청하는 형식은  $\langle p_1, \{q_1, q_2, q_3\} \rangle$ 으로 표현한다.

[정의 4] 사용 규칙

사용 규칙은 조건식  $c$ 의 진위에 따라 행위  $e$ 가 결정되는 술어식  $c \rightarrow e$ 로 정의한다.  $c$ 와  $e$ 는 각각 논리식인 명제로서 술어를 형성한다.  $c$ 와  $e$ 는 논리합, 논리곱, 부정 등의 논리 연산자로 구성된 논리식이다.

$c$ 는 실행 횟수, 시간, 일자 등의 조건 함수가 가능하고,  $e$ 는 조건이 충족되면 실행할 수 있는

권리이다. 조건식은  $\max(m)$ ,  $\text{time}(n)$ ,  $\text{date}(yymmdd)$  등으로서 최대  $m$ 번, 라이선스 시간으로부터  $n$  시간동안 또는  $yymmdd$  일자까지 조건이 참이면 함수  $\text{print}$ ,  $\text{view}$  등이 허용되는 술어식이다.

이상의 정의들을 이용하여 재배포를 위한 라이선스 발급을 아래와 같이 표현한다.

구매자  $p_1$ 이 사용자  $q_1$ 과  $q_2$ 에게는 영화  $r_1$ 을 48 시간 볼 수 있고, 인쇄도 할 수 있는 10명에게 재배포할 수 있고 이월전달이 2번 가능한 라이선스를 재배포 허용한다면, 그룹 재배포 형태의 type 1로서 다음과 같이 표현할 수 있다.

$\langle\langle p_1, \{q_1, q_2\}, \langle r_1, 10, 2 \rangle, (\text{time}(48) \rightarrow (\text{view}, \text{print})) \rangle\rangle$

취득자  $q_2$ 가 사용자  $q_5$ 에게 영화  $r_1$ 을 72시간 볼 수 있고 인쇄할 수 있는 5명에게 재배포할 수 있으며 이월전달이 불가능한 라이선스를 허용하도록 요청한다면, type 2의 재배포 형태로서 다음과 같이 표현한다.

$\langle\langle q_2, \{q_5\}, \langle r_1, 5, 0 \rangle, (\text{time}(48) \rightarrow (\text{view}, \text{print})) \rangle\rangle$

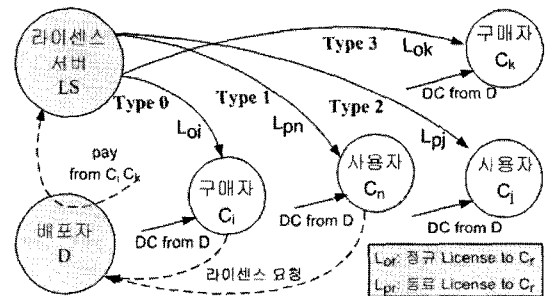
취득자  $q_2$ 가 사용자  $q_6$ 에게 영화  $r_1$ 을 98시간 볼 수 있고 인쇄할 수 있는 6명에게 재배포할 수 있고 1번 이월전달할 수 있는 라이선스를 구매하도록 요청한다면, type 3의 재배포 형태로서 다음과 같이 표현한다.

$\langle\langle q_2, \{q_6\}, \langle r_1, 6, 1 \rangle, (\text{time}(98) \rightarrow (\text{view}, \text{print})) \rangle\rangle$

결과적으로 type3 형태에서 사용자가 취득한 라이선스를 구매하지 않으면 영화를 볼 수 없고, 라이선스를 구매하면 type0과 유사한 형태가 된다.

## 4.2 배포 및 재배포 모델

디지털 콘텐츠의 배포를 활성화하기 위하여 배포 형태를 라이선스 취득 방식에 따라서 분류하면 <그림 2>과 같이 4가지로 구분할 수 있으며, 라이선스를 소유하고 그룹 배포하는 형태로 구분하면 <표 1>과 같다. Type0은 사용자가 배포자를 통하여 라이선스 서버로부터 정규 라이선스를 구매한다. Type1은 라이선스 구매 사용자가 다른 사용자에게 동료 라이선스를 발급해준다. Type2는 동료 라이선스 사용자가 다른 사용자에게 동료 라이선스를 발급하는 경우이다. Type3은 동료 라이선스 사용자가 정규 라이선스를 구매하는 경우이다. 결과적으로 type3은 type0과 동일하지만 재배포가 활성화된 결과이다[8]. 현재 시장에서는 type0이 주로 사용되고 있다. 콘텐츠 보급의 활성화를 위해서는 재배포 모델인 type1, type2, type3이 적극적으로 활용되어야 한다.



<그림 2> 라이선스 재배포 모델

<표 4> 라이선스 형태 및 그룹 배포 구분

구분	라이선스 요청자	라이선스 형태	그룹 배포
type0	구매자 자신	정규 라이선스	가능
type1	구매자	동료 라이선스	가능
type2	사용자	동료 라이선스	보류
type3	사용자	정규 라이선스	가능

<그림 2> 재배포 모델의 사용자  $C_i$ 가 콘텐츠의 해독 키를 취득하는 절차를 <그림 3>으로 표현하였다. 디지털 콘텐츠 DC와 라이선스  $L_{oi}$ 를 배포하고 인증하는 절차는 다음과 같이 네 단계로 구성된다.

**단계 0: 사용자(구매자)  $C_i$**

- $C_i$ 는  $C_i$ 의 식별정보  $CID_i$ 를 암호화한  $E_{D\_pub}CID_i$ 를 배포자 D에게 전송

**단계 1: 배포자 D**

- D는  $E_{C_i\_pub}CID_i$ 를 DC의 헤더 H에 삽입하고, DC를  $C_i$ 에게 전송
- D는  $CID_i$ 를 암호화한  $E_{LS\_pub}(KeyID, CID_i)$ 를 LS에게 전송

**단계 2: 라이선스 서버 LS**

- LS는  $D_{LS\_pri}$ 로 KeyID와  $CID_i$ 를 생성하고, seed를 이용하여 key를 생성.
- LS는  $E_{C_i\_pub}(key, CID_i)$ 를  $L_{oi}$ 에 삽입하여  $C_i$ 에게 전송

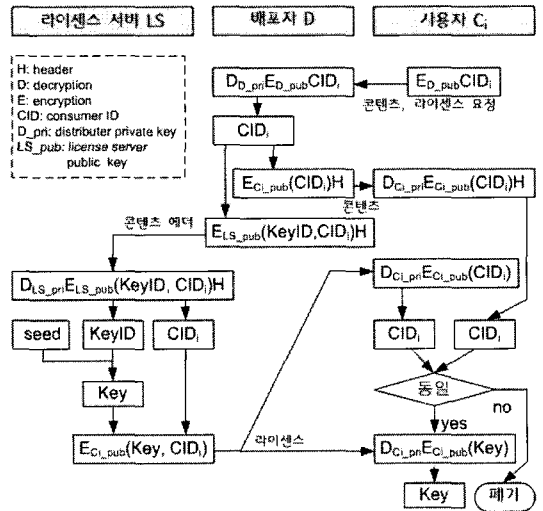
**단계 3: 사용자  $C_i$**

- $C_i$ 의 라이선스 서비스 LS는  $D_{C_i\_pri}$ 로 라이선스와 H에 있는 두 개의  $CID_i$ 를 추출.
- $C_i$ 의 LS는 두 개의  $CID_i$ 가 같으면  $D_{C_i\_pri}E_{C_i\_pub}(key)$ 로 key를 추출하고, 다르 면 폐기.

단계 3에서  $C_i$ 의 LS는 배포자와 라이선스 서버가 제공한 식별정보를 확인하고 해독 키를  $C_i$ 의 비밀키로 추출하므로 키관리는 안전하다.

재배포는 배포와 동일한 방식으로 실행된다.  $C_i$ 의 LS는 H와  $L_{pm}$ 에 있는 두 식별정보  $E_{C_i\_pub}CID_i$ 를  $C_i$ 의 비밀키로 해독하여 일치하면 암호화된 key를 추출하고, 콘텐츠 서비스가 사용한다. 배포 모델 type0의 key 전달이 안전하므로

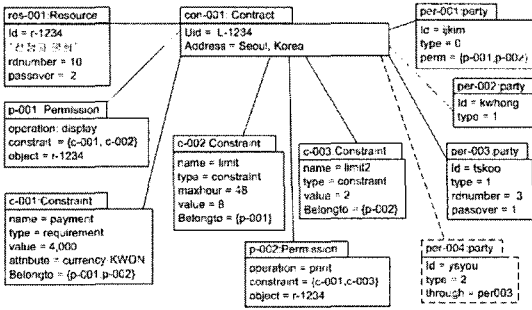
재배포 모델 type1의 key도 안전하다. H와  $L_{pm}$ 은  $C_n$ 의 공개키로 암호화하므로 키 전달 과정의 안전은 공개키의 안전만큼 안전하다. 재배포 모델 type2와 type3은 type1과 같은 방식으로 처리되므로 동일하게 안전이 유지된다.



<그림 3> 배포를 위한 키관리 절차

**4.3 재배포를 위한 권리 표현**

<그림 4>는 재배포를 강화하기 위하여 ODRL의 라이선스구조를 개선한 재배포 계약의 실례이다. 원천 라이선스는 “김일진”이 가지고 있으며, 자원은 영화 ‘전쟁과 평화’이고, 48시간 후까지 8번 시청할 수 있고, 텍스트를 2번 인쇄할 수 있으며, 비용은 4,000원이다. ”김일진“은 10명에게 재배포하고, 2번의 이월전달할 권리가 있다. “김일진”은 “홍길원”과 “구태수”에게 라이선스를 재배포하였으며, 홍길원은 재배포 권리가 전혀 없으나, “구태수”는 3번의 재배포와 1번의 이월전달 권리를 가지고 있다. 현재 상태에서 ”구태수“가 ”유윤식“에게 라이선스를 취득하게 하면 라이선스는 점선 부분과 같이 개정된다[2][7].



<그림 4> 재배포를 위한 계약 구조

```

<o-ex:party>
<o-ex:context>
  <o-dd:uid> ijkim </o-dd:uid> //type0
  <o-dd:name> Kim iljin </o-dd:name>
</o-ex:context>
<o-ex:passover>
<o-ex:context>
  <o-dd:uid> kwhong </o-dd:uid> //type1
  <o-dd:name> Hong kilwon </o-dd:name>
</o-ex:context>
<o-ex:context>
  <o-dd:uid> tskoo </o-dd:uid> //type2
  <o-dd:name> Koo taesoo </o-dd:name>
  <o-dd:dnumber> 3 </o-dd:dnumber>
  <o-dd:passover> 1 </o-dd:passover>
</o-ex:context>
<o-ex:passover>
<o-ex:context>
  <o-dd:uid> ysyoo </o-dd:uid> //type3
  <o-dd:name> You yoonsik </o-dd:name>
</o-ex:context>
</o-ex:passover>
</o-ex:passover>
</o-ex:party>
    
```

<그림 5> 재배포를 위한 ODRL 라이선스

<그림 5>는 사용자간 라이선스 재배포를 보여주는 <그림 4>를 정의한 ODRL의 한 부분이다. 사용자 “김일진”이 “구태수”에게 3명의 사용자에게 라이선스 재배포를 허가하고, 1번의 이월전달을 허가한 것이 코드에 반영되었다. ”구태수”가 ”유윤식”에게 라이선스를 제공하면 ”구태수”의 <o-ex:context> 다음에 <o-ex:passover>를 추가하고 ”유윤식”의 <o-ex:context>를 추가한다.

#### 4.4 평가

Microsoft사의 WMRM과 OMA 규격은 현재 DRM 기술 중에서 대표적이다. WMRM은 Windows의 보급과 연계되어 DRM 시장에 많이 보급된 상태이고, OMA는 DRM 표준화를 위한 대표적인 수단으로 인정받고 있다. WMRM은 DRM의 핵심 기능을 제공하고 있으나 구현을 위한 모든 기능을 제공하지는 않는다. 단지 SDK를 제공하여 핵심 기능을 활용하도록 지원하고 있다. 이들 시스템들은 서비스 기반의 소프트웨어 시스템을 설계하였으므로 서비스 기능을 비교하였다 [4][8].

<표 2> 재배포 서비스 비교

DRM 기술	기능적 특징	메타 자료	라이선스 형식	그룹 배포	재배포	이월 전달	헤더 조작
WMRM	핵심만 제공	콘텐츠 내	콘텐츠와 분리	부분적	소극적	없음	보통
OMA	규격만 제공	콘텐츠 내	복합 방식	부분적	소극적	없음	소극적
제안	서비스 기반	콘텐츠 내	콘텐츠와 분리	적극적	적극적	있음	적극적

<표 2>에서와 같이 WMRM은 시스템의 일부 핵심 기능만 제공하고 나머지는 개발하여 사용하고, OMA는 설계 규격만 제공하는데 반하여 제안 모델은 서비스 기반의 프로그램 전체를 제공한다. 세 시스템의 공통적 특징은 메타 자료를 모두 콘텐츠 안에 가지고 있다. 기존의 DRM 시스템들과 달리 OMA는 키를 콘텐츠와 분리하여 배포하기도 하고 함께 배포하기도 한다. WMRM과 OMA는 그룹 배포 기능과 재배포 기능을 가지고 있으나 부분적이며 이월전달과 같은 적극적인 기능은 없다. 제안 모델의 특징은 재배포를 강화하여 사용자가 이월전달과 함께 그룹 배포를 지원한다 [9][10]. WMRM은 재배포 시에 콘텐츠 헤더에 배포자의 ID를 여러 방식으로 삽입하여 관리한다.

즉, 콘텐츠 소유자와 배포자가 헤더에 배포자 ID를 삽입할 수 있으며, 소유자가 동적으로 삽입하여 배포자를 관리할 수 있다. 제안 모델에서는 여기에 부가하여 배포자가 사용자의 ID를 헤더에 삽입하여 배포 정보를 관리한다[12].

본 연구는 모바일 VOD용 DRM 기술을 개발하여 e-Learning 등의 분야에서 활용하고자 하므로 재배포 기능을 강화하는 DRM 시스템을 구축하고 있다. 따라서 그룹 배포 기능과 함께 재배포 기능을 강화하는 라이선스관리 모델을 제안한다. 콘텐츠의 재배포 라이선스를 명확하게 관리하기 위하여 배포되는 경로를 누적하여 헤더에 기록함으로써 추적 서비스를 강화한다.

## 5. 결론

콘텐츠 유통을 활성화하기 위한 수단으로 재배포 기능을 강화한 라이선스관리 모델을 설계하였다. 콘텐츠를 구매한 소비자는 계약에 의하여 콘텐츠를 사용하는 라이선스를 여러 사람들에게 그룹으로 재배포할 수 있고, 사용자간 재배포가 가능하다. 사용자간 라이선스 재배포는 콘텐츠의 원활한 유통을 촉진하여 콘텐츠 공급자의 수익을 증대시켜주며, 소비자의 저작물 사용 권한을 확대하여 소비자 권리를 보호할 수 있으므로 원활한 유통과 소비자권리를 함께 달성할 수 있는 효과적인 수단이다. 사용자간 재배포 모델의 목적이 달성되기 위해서는 콘텐츠 배포의 유형을 세밀하게 분류하고 각 유형에 적합한 안전한 키관리 기법을 적용하였다. 즉, 라이선스를 정규 라이선스와 동료 라이선스로 구분하여 재배포 기능을 확대하였다. 재배포를 위한 권리를 명확하게 표현하기 위하여 ODRL을 이용하고 재배포 권리를 표현하는 기법을 제시하였다.

향후 연구로는 제안한 모델을 위하여 재배포와 그룹 배포를 위한 라이선스들의 관계를 명확하게 정의하고, 라이선스 종류별로 라이선스와 콘텐츠 헤더에 포함되어 있는 정보를 효과적으로 관리하

는 기술을 개발하고, 이동환경에 ODRL로 적용하여 구체적인 문제점들을 찾아서 해결하고자 한다.

## 참고 문헌

- [1] Qiong Liu, Reihaneh Safavi-Naini, Nicholas Paul Sheppard, "Digital Right Management for Content Distribution", Australian Information Security Workshop 2003 (AISW2003), Adelaide, Australia, Vol., 21. C., 2003.
- [2] Brenton Cooper, Montague, "Translation of Rights Expression", 4th Australasian Information Security Workshop (AISW), 2005.
- [3] Naini, Sheppard, Uehara, "Import/Export in Digital Rights Management", DRM'04, October 25, 2004.
- [4] Sam Michiels, Kristof Verslype, Wouter Joosen and Bart De Decker, "Towards a Software Architecture for DRM", Proceedings of the 5th ACM Workshop on DRM '05, pp. 65-74, Nov. 2005.
- [5] 장혜진, "DRM 기술로 보호된 콘텐츠의 유통성 있는 공유를 위한 멤버/그룹 라이선스 메커니즘", 정보처리학회논문지 C 제11-C권 제 6호, 12. 2004.
- [6] 정연정, 윤기송, 류재철, "라이선스 기반 디지털 저작권 보호 시스템 설계 및 구현", 정보처리학회논문지 C 제11-C권 제1호, 2004.
- [7] Guth, Neumann, Strembeck, "Experiences with the Enforcement of Access Rights Extracted from ODRL-based Digital Contracts", DRM'03, Oct. 27, 2003.
- [8] Microsoft, "Windows Media Rights Manager 10.1 SDK", Microsoft Corporation, 2005.
- [9] 박복녕, 김태윤, "디지털 저작권 관리에서 사용자의 프라이버시 보호를 제공하는 라이선스 관리 프로토콜", 정보과학회논문지: 정보통신 제30권 제2호, 2003



- [10] 김정재, 박재표, 전문석, “동영상 데이터 보호를 위한 공유 키 풀 기반의 DRM 시스템”, 정보처리학회논문지 C 제12-C권 제2호, 2005.
- [11] S.H.Kwok, S.M. Lui, “A License Management Model to Support B2C and C2C Music Sharing”, Proceedings of the International WWW Conference, Hong-Kong, 2001,
- [12] Microsoft Corporation, Windows Media Rights Manager 10.1 SDK, 2005.
- [13] Byungwook Lee, “Group License Management using Super-Distribution in DRM”, The 2007 International Conference on Ubiquitous City Technology”, Korea Society for, internet Information, 2007.

## ○ 저자 소개 ○



### 이 병 옥(Byung-wook Lee)

1973 연세대학교 공과대학 공학사  
1984 George Washington University 전자계산학과 공학석사  
1994 중앙대학교 전자계산학과 공학박사  
1985.3.1 - 현재 경원대학교 소프트웨어학부 교수  
관심분야 : 분산 시스템, 데이터베이스, 저작권관리 Digital Rights Management  
E-mail : leebw@kyungwon.ac.kr



### 유 종 화(Zong-Hua Liu)

2004년: 중국 산둥이공대학교 전자공학과 공학사  
2005 - 현재 경원대학교 전자계산학과 석사과정  
관심분야: 데이터베이스, 저작권관리  
E-mail : lzh5333@hotmail.com