

디지털 저작권관리(DRM)와 Rights Language

박정희

주식회사 마하넷 기술이사
재능대학 컴퓨터 정보계열 겸임교수
jpark@mail.jnc.ac.kr

성평식

재능대학 컴퓨터 정보계열 교수
sps@mail.jnc.ac.kr

Junghee Park, Pyungshik Sung

요 약

인터넷의 발달은 전통적인 자연 발생적인 시장에 의한 상거래를, 기술에 의한 안전하면서 세계 시장을 쉽게 접근할 수 있는 전자상거래 구조를 제공하고 있다. 현재 전자상거래의 대상은 실물에 대한 상거래와 디지털 콘텐츠에 대한 상거래로 크게 분류할 수 있으며, 실물에 대한 상거래는 전통적 상거래 방식이 컴퓨터로 바뀐 상황이라고 볼 때, 디지털 콘텐츠에 대한 상거래 즉, D-Commerce에 대한 상거래의 개념이 도래하고 있다. 디지털 콘텐츠의 상거래에 필요한 요소 기술에 대한 연구, 그리고 특히 새로운 유통 비즈니스 모델에 대한 연구가 필요하다.

디지털 콘텐츠는 생성, 가공, 유통, 분배 등의 측면에서 많은 장점을 갖는 반면, 복사를 여러 번해도 원본의 품질에 손상 없이 쉽게 복사 될 수 있다는 것이 디지털 저작권 보호에 커다란 문제점으로 대두되고 있다. 디지털 저작권관리(Digital Rights Management: DRM)은 디지털 콘텐츠의 보호와 적절한 유통체계를 설립하여 안전하게 상거래를 할 수 있게 하기 위한 새로운 기술이다.

XrML은 권리(Right)을 명시하는 언어로써 디지털 콘텐츠와 그에 따른 서비스들을 사용할 수 있는 권리와 조건들을 명시해준다. XrML은 현재 디지털 저작권관리(Digital Rights Management: DRM)에 가장 많이 쓰이고 있는 Rights Language이다. XrML은 ContentGuard가 개발한 DRM 서술 언어로 전 세계 산업계 표준으로 추진하기 위하여 파트너 회사 확대, 기능 확장, 무료 / 공개 형식으로 보급을 추진하고 있다.

Key Word(키워드) : 디지털 저작권관리(Digital Rights Management: DRM), XrML, 디지털 콘텐츠
DCC(Data Clearing Center), Rights Language

1. 연구배경

디지털 저작권관리(Digital Rights Management: DRM)는 디지털 콘텐츠 보호 기술, 디지털 콘텐츠 불법사용 금지 기술등으로 표현할 수 있다. ContentGuard(<http://www.contentguard.com>)에 따르면 DRM은 신뢰성 있는 라이선스, 안전한 저작권과 인증, 신뢰성 있는 환경과 인프라를 가능하게 하는 H/W, S/W를 포함하는 저작권 관리를 위한 넓은 의미의 기술, 절차, 처리, 알고리즘이라고 정의한다[1]. 점차 인터넷의 보급이 확산됨에 따라 아날로그 형태의 데이터들로부터 콘텐츠를 포함한 디지털 정보들이 데이터의 주요 형태로 바뀌어 가고 있다. 이런 디지털 콘텐츠들은 어느 장소에서나 언

제든지 쉽게 얻을 수 있으나 저작권 관리, 콘텐츠의 배포 등에 문제점을 안고있다. 원본의 불법 복사가 쉽고 외부로부터 내용의 불허가된 변경 등의 전통적인 방법의 상거래와는 다른 양상을 띠고 있다. 이러한 인터넷 환경 하에서는 디지털 콘텐츠의 안전한 보호와 적절한 유통체계의 설립이 새로운 전자 상거래 모델의 확립을 위한 필요 불가결한 요건이다.

DRM은 인터넷과 네트워크들을 사용하여 안전하게 상거래를 할 수 있게 하는 새로운 기술이다. 본 연구는 현재 불법 복제 또는 불법 도용의 위험이 있는 디지털 콘텐츠를 보호하기 위해 많이 언급되고 있는 대표적 기술인 디지털 저작권관리(Digital Rights Management: DRM)와 DRM 언어인 XrML을 논하고자 한다.

2. 디지털 저작권관리(Digital Rights Management : DRM)란?

2.1 DRM의 정의

DRM이란 다양한 경로로 유통되고 있는 디지털 형태의 모든 정보를 암호 화한 후 유통시킴으로써 불법 복사와 도용을 막고 인증된 사용자만이 해독키를 가지고 해독함으로써 디지털 콘텐츠를 보호하는 디지털 콘텐츠 저작권 보호 기술이다. 넓은 의미에서의 DRM은 디지털 콘텐츠를 인터넷상에서 안전하게 거래 할 수 있도록 하는 표준 기술들을 포함한 통괄 적인 모든 과정을 포함한다. 즉 디지털 콘텐츠의 생성(Creation), 거래(Transaction), 변경(Modification), 사용(Usage), 소비(Consumption)등의 라이프 사이클을 통해 전 과정을 안전하고 투명하게 유통시키는 콘텐츠 기술이다.

2.2 DRM의 역할

D-commerce 에서 디지털 콘텐츠들의 안전한 상거래를 위해 DRM은 여러 장점들을 가지고 있는데 그중 에서도 디지털 콘텐츠의 보호, 콘텐츠의 불법 변경 방지, 거래 내역 정보와 사용자 정보의 제공이 가장 중요한 역할이다.

1. 디지털 콘텐츠의 보호

DRM은 디지털 콘텐츠를 보호하기 위해 암호화 기술을 사용한다. 암호화는 특별한 키(Key)을 사용하여 이루어진다. 일단 암호화되어 진 콘텐츠는 키를 가진 사용자만이 해독할 수 있다. 그러므로 디지털 콘텐츠를 암호, 해독하는데 쓰이는 키들을 다루는 문제는 DRM에 있어서 중요한 역할을 한다.

2. 디지털 콘텐츠의 불법 변경 방지

DRM은 또한 콘텐츠 내용의 불법 변경을 방지함으로써 콘텐츠의 본래 내용을 그대로 유지할수 있게 한다. 그중 하나가 일 방향 해쉬 함수(one-way hash function)의 사용이다. 예를 들어서 해쉬 함수가 전자책의 내용을 입력 값(input)으로 받아 들인 다면 결과(output)는 메시지 다이제스트(message digest)라고 불리는 작은 고정 길이의 메시지가 되며 이 결과가 사용자에게 보내지게 된다. 만약 콘텐츠 내용이 변경되었다면 변경된 콘텐츠를 입력 값으로 받아들인 해쉬 함수는 원본의 메시지 다이제스트와는 다른 메시지 다이제스트를 값을 생산한다. 그러므로 사용자는 거래 과정 중 콘텐츠의 변경 여부를 알수 있다.

콘텐츠의 수신자와 송신자 사이에 데이터를 보호하고 서명자를 확인하는 전자 서명은 비공개 비밀키(private key)

를 사용해서 서명하고 공개키(public key)를 사용해서 검증하는 것으로 e-commerce에서 손을 사용해서 서명하는 것을 대체한다. 오직 이문서의 창작자만이 서명을 할 수 있고 이 서명의 확인은 적절한 키 혹은 판독 소프트웨어를 가진 사람은 모두 할 수 있다.

디지털 콘텐츠의 원본을 보호하기 위한 또 다른 방법은 워터마킹(watermarking)의 사용이다. 사용되는 워터마킹은 원본의 디지털 콘텐츠에 저작권(copyright), 소유자(owner), 발행일(production date), 아이디(ID)등의 저작권 정보를 삽입한다. 이것은 콘텐츠의 보호가 목적이고 원본에는 아무런 영향이 없다. 그러므로 사용자는 워터마크의 삽입 여부를 인식하지 못하고 특정 프로그램에 의해서만 판독될수 있다.

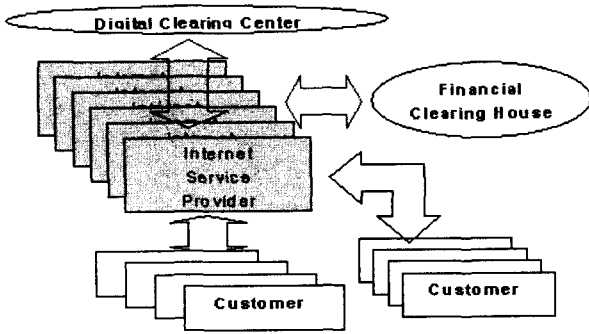
3. 거래내역 정보와 사용자 정보의 제공

디지털 정보의 거래가 성공적으로 이루어지고 나면 그 거래에 관한 모든 정보는 전자 인증서(digital certificates)에 저장되어 지고 이 정보들은 후에 다시 쓰이게 된다.

앞에서도 언급한 바와 같이 신뢰와 보안은 모든 인터넷 상에서 이루어지는 거래들의 필수 요건이다. 많은 DRM 업체들은 디지털 정보들의 저작권 보호를 위해 e-commerce 상의 거래에 있어 디지털 정보들을 보호하여 안전한 상거래를 이루려 노력하고 있다. 반면에 여러 종류의 저작권 보호 기술들이 공존하고 있는 현재의 시스템에 있어서는 DRM 시장에 있어서 시스템간의 호환성과 표준화가 필요하다.

3. DCC(Data Clearing Center)의 구조

DRM은 디지털 권리 관리에 관한 사항이다. 디지털 콘텐츠에 대한 상거래 증가는 저작권자, 소비자, 유통업자가 모든 만족하는 기술이 필요하게 되었으며 이 만족은 기술의 신뢰성, 유통 구조의 신뢰성 회복에서 비롯된다. DRM은 신뢰성을 만족시키는 기술로 정의될 수 있으며, 그 방법은 WIPO 저작권 법에서 언급한 바와 같이 RMI(Rights Management Information)에 의해 비롯된다고 할 수 있다. 즉 콘텐츠의 상거래 내역과 저작권자 관련 정보가 RMI 속에 들어가 있으며, 이 RMI는 콘텐츠와 함께 영원히 같이 있게 하는 것이다. 이 방법은 RMI를 콘텐츠와 같이 합쳐서(패키지화) 판매, 저장, 관리하는 것이고, 이 RMI 정보를 이용하여 모든 상거래 내역과 소비자 권리를 운영할 수 있게 하는 것이다. ContentGuard에서는 이 RMI를 Rights-label[1]이라고 정의하고 있다.



<그림 1> Data Clearing Center 구조

이러한 Rights-label 또는 RMI 정보의 유통 관리는 상거래업자(Internet Service Provider)가 관리하는 것이 아니다. <그림 1>에 기술된 것 같이 모든 상거래는 Data Clearing Center(DCC)에서 통제하는 것이고, 상거래업자는 판매만 할 뿐 판매에 대한 내역과 판매 허가 등이 DCC에서 일어난다. Rights-label 정보가 콘텐츠에 추가되지만 이 정보는 DCC의 내부 DBMS에서 primary key의 역할을 하고, 추후에 본 콘텐츠에 대하여 계속 추적할 수 있는 근거를 제공한다. 이 DCC는 ContentGuard에서는 Back-Office로 InterTrust에서는 Data Center로, MS Reader에서는 DAS로, MS Media Player에서는 Rights Manger Provider라고 불리워진다.

DRM의 기능에는 사용 규칙(Usage Rules)에 관한 사항이 있다. 사용 규칙은 콘텐츠와 관련된 명령어인 Play, View, Copy, Delete, Edit, Embed, Transfer, Print 등과 같은 명령에 대하여 저작권자, 유통업자, 또는 소비자가 선택한 권리만 동작되도록 가능하게 한다.

4. XrML

XrML은 Xerox DPRL 2.0의 확장으로, ContentGuard에 의해 관리 유지되는 DRM 기술 언어이다. DPRL은 Xerox PARC의 Mark Stefik에 의해 1996년 개발되었고, 인증과 메시지의 무결성을 가진 디지털 콘텐츠 사용을 위한 권리(rights), 요금(fees), 조건(conditions)을 기술할 수 있다.

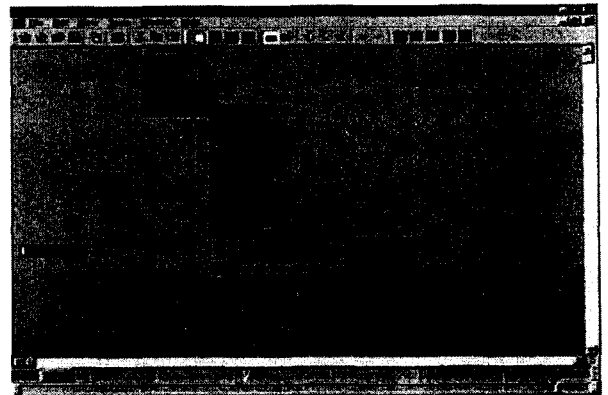
디지털 콘텐츠의 사용 권리(usage rights)를 위한 XrML의 사용은 신뢰 체계(trusted system)가 디지털 콘텐츠를 교환하고 상호운용할 수 있게 하는 확신을 제공한다. 신뢰 체계 또는 저장소(repositories)는 디지털 콘텐츠와 디지털 콘텐츠에 기술된 권리(rights), 조건(conditions), 그리고 요금(fee)에 신뢰를 제공할 수 있는 시스템이다. 문서 상거

래에서 신뢰 체계는 디지털 작업의 저작, 플레이, 그리고 판매를 위한 것이다. 그들은 개인적 시스템, 온라인 시스템, 도서 시스템 등을 포함한다.

XrML 문서는 하나의 작업, 작업과 구성 부분, 작업 모임의 형태로 임의의 디지털 콘텐츠에 적용된다. 디지털 콘텐츠는 객체를 사용하여 식별된다. 다양한 사용 권리가 콘텐츠를 위해 기술된다. 메타데이터를 가진 콘텐츠 식별과 권리 사용은 무결성을 확신하기 위하여 암호화하여 서명된다. XrML 문서는 <그림 2>과 같은 DTD 구조를 가진 XrML 원소로 표현된다.

<그림 2>에서 루트 원소 XrML 안에 하나의 필수 요소 BODY와 선택적 요소 SIGNATURE가 있으며 후자는 무결성을 확신하는데 사용하는 전자의 디지털 서명이다. BODY 원소는 디지털 작업의 선택적 기술과 XrML 문서에서 선택적 메타 정보로 구성된다. TIME 원소는 XrML 문서가 유효한 시간 기간을 나타낸다. 원소 ISSUED는 이 문서가 만들어진 순간을 나타낸다. 원소 ISSUER는 이 문서를 만든 주체(principal)를 원소 ISSUEDPRINCIPALS은 이 문서를 만든 주체 리스트를 원소 WORK는 디지털 작업과 사용 권리를 정의한다. 마지막으로, 원소 AUTHENTICATEDDATA는 XrML 문서를 처리하는 응용에 제공되는 자료를 나타낸다.

상위 레벨 구조는 ISSUER, ISSUEDPRINCIPALS, WORK 사이 관계를 정의하는데 유통적 레벨을 제공한다. 만약 3가지 원소가 모두 나타나면, ISSUER는 WORK의 사용 권리에 대하여 ISSUEDPRINCIPALS에게 XrML 문서를 발행하게 한다. 만약 ISSUER와 WORK만 나타나면, ISSUER는 WORK의 사용 권리를 가진 XrML 문서를 만든 것을 확정한다. 이런 형태의 관계는 만든 주체가 알려지기 전에 사용 권리를 정의하는데 유용하다.



<그림 2> XrML DTD

XrML에서 디지털 콘텐츠에 제공되는 권리는 다음 DTD에 기술된 것과 같다.

```
DTD:
<!ELEMENT RIGHTSLIST ((COPY | TRANSFER | LOAN
| PLAY | PRINT |
EXPORT | VIEW | EDIT |
EXTRACT | EMBED |
BACKUP | RESTORE |
VERIFY | FOLDER |
DIRECTORY | DELETE |
INSTALL | UNINSTALL)+>
```

이름에 의해 식별되는 각 권리는 선택적 요소로 COMMENT, TIME, ACCESS, FEE, TERRITORY, TRACK 을 가진다. 권리는 여러 가지 범주 중에 하나에 속한다. XrML에서 권리는 다음 사용을 기술한다.

- 저작권법에 기술된 사용과 관계된다.
- 디지털 작업의 상거래 목적에서 일반적 면허에 적절한 사용의 구별을 한다.
- 실제적인 신뢰 체계에 의해 강화될 수 있다.
- 저장소에서 내의 실제 상거래를 수행함으로써 행사된다.

논리적으로 권리들은 전송(Transport)권, 제공(Render)권, 파생 작업(Derivative work)권, 파일 관리(File Management) 권, 그리고 인접(Configuration)권으로 나누어진다. 전송 권리는 한 저장소에서 다른 곳으로 작업의 이동을 관리한다. 제공 권리는 작업의 외부 매체로 전달하는 작업의 인쇄, 보기를 나타낸다. 이것은 명확히 복사가 될 수 있는 수출(Export)권을 포함한다. 파생 작업 권리는 새 작업을 만드는 것으로 작업의 재사용을 관리한다. 파일 관리 권리는 백업 복사본을 만들고 재생하는 것을 관리한다. 마지막으로 인접 권리는 저장소에 소프트웨어 설치를 나타낸다.

5. 결론

인터넷과 함께 전자상거래가 발전함에 따라 디지털 기술의 급격한 발달은 많은 분야에서 상거래의 변모를 가져오고 있다. 그중 특히 중요성이 부각되고 있는 것 중의 하나가 디지털 콘텐츠 산업이다. 디지털 콘텐츠는 생성, 가공, 유통, 분배 등의 측면에서 많은 장점을 갖는 반면, 복사를 여러 번해도 원본의 품질에 손상 없이 쉽게 복사될 수 있다는 것이 디지털 저작권 보호에 커다란 문제점

으로 대두되고 있다.

디지털 저작권관리(Digital Rights Management: DRM)는 디지털 콘텐츠의 보호와 적절한 유통체계를 설립하여 안전하게 상거래를 할 수 있게 하기 위한 기술이다. 다양한 경로로 유통되고 있는 디지털 정보의 불법 복사와 도용을 막고 허가된 사용자만이 사용할 수 있도록 하는 디지털 콘텐츠 저작 보호를 위한 기술이다. DRM은 새로운 기술로써 세계의 여러 비영리 단체 기구들과 상업적인 회사들이 각각의 기술들을 내놓고 있으나 아직 호환성이나 표준화가 이루어지고 있지 않다. 디지털 콘텐츠를 생산자, 거래처, 시간, 장소등에 구매 받지 않고 필요한 곳으로 안전하게 거래하기 위해서는 DRM의 표준화 연구가 요구된다.

XrML은 권리(Rights)을 명시하는 언어로써 디지털 콘텐츠와 그에 따른 서비스들을 사용할 수 있는 권리와 조건들을 명시해준다. XrML은 현재 디지털 저작권관리(Digital Rights Management: DRM)에 가장 많이 쓰이고 있는 Rights Language이다. 이 언어는 여러 시스템들의 권리와 조건들을 잘 명시해주므로 시스템들간의 호환이 이루어지도록 개발되고 발달되고 있다. 개발회사인 ContentGuard는 전 세계 산업을 표준으로 추진하기 위하여 파트너 회사 확대, 기능 확장, 무료 / 공개 형식으로 보급을 추진하고 있다.

참고 문헌

- [1] ContentGuard, ContentGuard DRM Solution, October 2000, 3-7
- [2] Dennis M. Davis & Tim Lafferty, Digital rights management, Managing Library Finances, 2002, Vol15(1) 8-23
- [3] Digital Rights Management Architecture, D-Lib Magazine, June 2001, Vol7(6)
- [4] The Need for a Rights Language, Technical White Paper, Version 1.0
- [5] Boley, H., Rule Markup Language, <http://www.dfki.uni-kl.de/ruleml>, 2002
- [6] Coverpages:XrML and Digital Rights Management, www.coverpages.org