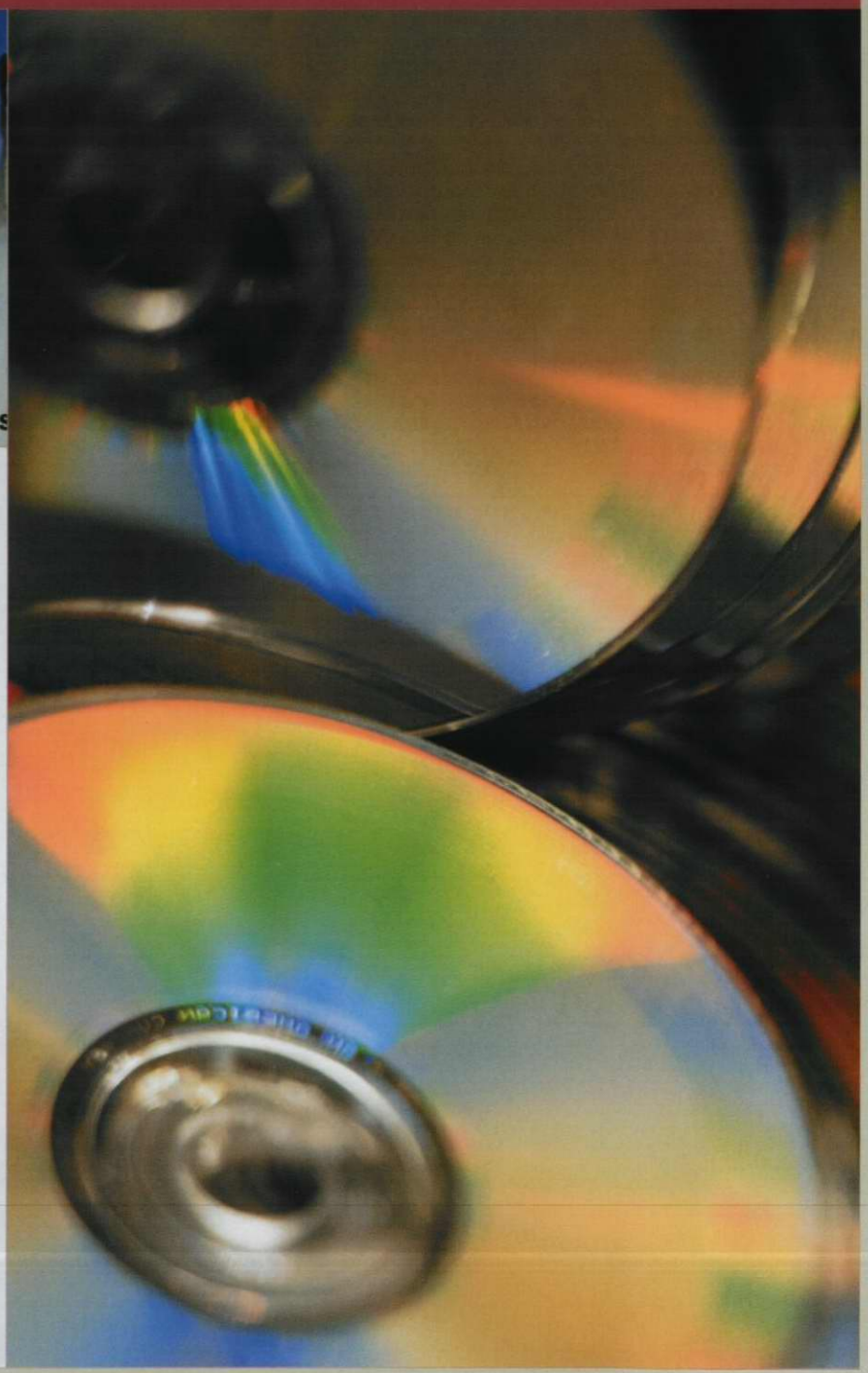
콘텐츠 비즈니스는 저작권 관리가 핵심

사용자의 인식부족이 DRM의 발전 저해

김진영 실트로닉테크놀로지 전략기획팀장



연재순서

지난 2회의 연재를 통해 살펴본 콘텐츠비즈니스의 속성과 DRM의 특징에 대해 상기하며 금번 연재를 시작해보자. 콘텐츠비즈니스가 성공하기 위해서는 우선적으로 거래(Transaction)가 많이 발생해야 한다. 그래야 계속적으로 부가 가치가 높아지면서 수익을 창출해낼 수 있다. 이런 활발한 유통 구조를 만들어 내기 위해서는 법, 제도, 사회적인 인식, 문화 등의 환경적 요소가 중요하다. 물론 DRM과 같은 저작권과 관련된 기술 역시 빼놓을 수는 없다.

〈그림1〉 소리바다 웹사이트

온라인의 뜨거운 감자 : 소리바다

소리바다에 대한 법원의 사이트 폐쇄 가처분 결정이 내려지면서 점점 논란이 거듭되고 있다. 네티즌들과 음반협회의 대립은 이제 극단적으로까지 치닫고 있는 양상이다. 혹자들은 이런 상황의 탈출구로서 디지털 저작권 문제를 기술적으로 어떻게 해결할 수 있을지 관심을 표명하면서 필자에게 소리바다와 같은 사이트에서 DRM 기술 적용 가능 여부를 물어 왔었다. 내심 이제 좋은 시절 온 것 아니냐는 부러움과 함께.

사실 DRM이 가장 먼저 목표로 한 콘텐츠는 음악과 영상 콘텐츠였다. 사실 콘텐츠비즈니스 초창기에 가장 주목을 받았으며, 시장 크기나 성장 가능성이 높을 것으로 예상했던 콘텐츠들이었다. 하지만 그 예상은 여지없이 빗나가 현재는 대안 모색에 골머리를 썩이고 있음은 주지의 사실이다.

기술은 어떻게 본다면 큰 문제가 아닐 수 있다. 실제적으로 mp3 사이트들이 요구하는 기술적 스펙은 현재의 솔루션 수준으로 커버가 가능하기 때문이다. 정작 문제는 기술 이외의 문제들이다.

하지만 기술적 측면에서 보다 진보된 발전은 필요로 한다. 한번 팔린 콘텐츠는 아무도 제어하지 않고 온라인에서 떠돌기 때문에 해킹과 같은 위법 행위에 그대로 노출돼 있기 때문이다. 또한 비즈니스가 확장되고 변모하는 과정에서 기술적인 뒷받침이 없다면 제대로 된 비즈니스 모델을 창출하기 힘들 것이다.

DRM의 기술적 구성 모듈과 작동 Flow

DRM의 요소 기술을 알기 위해서는 우선 DRM 시스템의 컴포넌트에 대해 먼저 살펴 볼 필요가 있다. 기본적으로 다음과 같이 네 가지 요소로 구성돼 있다.

콘텐츠 서버

일반적으로 콘텐츠 제공업자(이하 CP)는 콘텐츠를 담아둔 저장소(이하 DB서버)를 가지고 있다. DB서버는 실질적으로 파일 서버이거나 콘텐츠에 대한 정보를 가지고 있는 메타데이터이다. 콘텐츠 서버에서 주 역할을 하는 부분은 콘텐츠 암호화를 담당하는 팩키저이다. 단순히 콘텐츠 암호화만 진행하는 것이 아니라 다양한 사용자 규칙(Usage rule), 사용 회수, 기간, 프린팅 권한, 재전송 권한, 여타 디바이스 지원 등을 정의한 메타데이터 역시 포함한다.

라이센스 서버

라이센스는 일반적으로 콘텐츠에 대한 권리를 행사하는 사용자와 디바이스를 식별하거나, 권한이 적용되는 콘텐츠에 대한 인지 및 권한에 관한 세부 사항을 담고 있다. 일반적으로 라이센스는 팩키저에서 사용 권한을 설정할 때 생성돼 라이센스 서버에 전달돼 보관/관리된다. 추가적으로 DRM 암호화 과정은 암호 키(사용자를 인증하고 콘텐츠를 복호화 하는데 쓰이는)를 생성한다. 세부적인 권장 사항과 키 값은 다른 DB에 저장되는데 물론 키 값에 보안성이 높아야 한다.

클라이언트

클라이언트 프로그램은 기본적으로 콘텐츠를 사용하는 사용자의 PC에 장착돼 암호화된 콘텐츠를 복호화 하는 기능을 담당한다. 세부적으로 살펴보면 사용자의 콘텐츠 이용 요구를 받아들여 사용자 또는 디바이스를 식별하는 정보를 모으고, 라이센스 서버로부터 해당 콘텐츠의 라이센스를 획득한다. 그런 후에는 적절한 권리 행사를 위해 콘텐츠와 관련한 애플리케이션 구동을 인증하며, 라이센스로부터 복호화 키를 받아 복호화 작업을 수행한다.

키 분배 서버

일반적으로 DRM 시스템에서 콘텐츠 암호화는 대칭키 방식을 사용해왔다. 대칭키 방식이란 콘텐츠를 암호화하는 키와 다시 복호화하는 키가 동일한 것이다. 구조가 단순하고 암호화 속도가 뛰어난 장점이 있었지만 하나의 키 값을 사용자가 알아낸다고 하면 다른 PC에서도 콘텐츠를 실행시킬 수 있으며, 키 값과 콘텐츠를 묶어 배

포한다면 광범위한 불법 유통/사용이 가능해질 수 있는 보안상의 큰 허점이 있다(불행히도 아직까지 이런 키 분배 구조를 가지고 있는 솔루션이 현존한다).

이런 점에서 착안해 DRM 벤더들은 보다 안정성 높은 암호화 체계를 탐색한 결과 100% 만족할 만하지는 않지만 비대칭 방식의 공개키(PKI 방식)가 그 대안이 될 수 있음을 깨닫기 시작했다. RSA가 대표적인 비대칭 암호화 알고리즘이다. 콘텐츠는 기존의 대칭키로 암호화하되 콘텐츠의 라이센스 키를 공개키로 암호화하고, 개인의 비밀키로 복호화를 수행하게 함으로써 적용의 효율성과 보안성을 모두 일정 수준 이상으로 끌어올릴 수 있게 되었다.

이와 같은 네 가지 컴포넌트는 〈그림2〉와 같은 순서로 기술적인 작용을 하게 된다.

① 우선 사용자는 콘텐츠를 받는다.

② 사용자는 더블 클릭으로 파일을 실행하려고 하면 클라이언트의 DRM 컨트롤러를 활성화하게 된다. 물론 처음 사용자라면 클라이언트 프로그램부터 다운로드받아 설치하게 된다.

③ 활성화가 되면 컨트롤러는 우선 PC내 인증서가 있는지 확인한 후 없으면 키 분배 서버에 인증서를 요청한다.

④ 간단한 등록 사용자 절차를 거친다.

⑤ 사용자 정보와 사용자 공개키를 포함한 인증서를 내려보낸다.

⑥ DRM 컨트롤러는 라이센스 서버에 라이센스를 요청한다(공개키 전송).

⑦ 라이센스 관리기는 라이센스를 확인한다.

⑧ 아직 미결제 상태임을 확인하고 결제 프로세스를 거친다.

⑨ 결제 완결 정보가 통보되고 라이센스 서버는 인증서 확인을 키 관리 서버에 요청하고 확인 받는다.

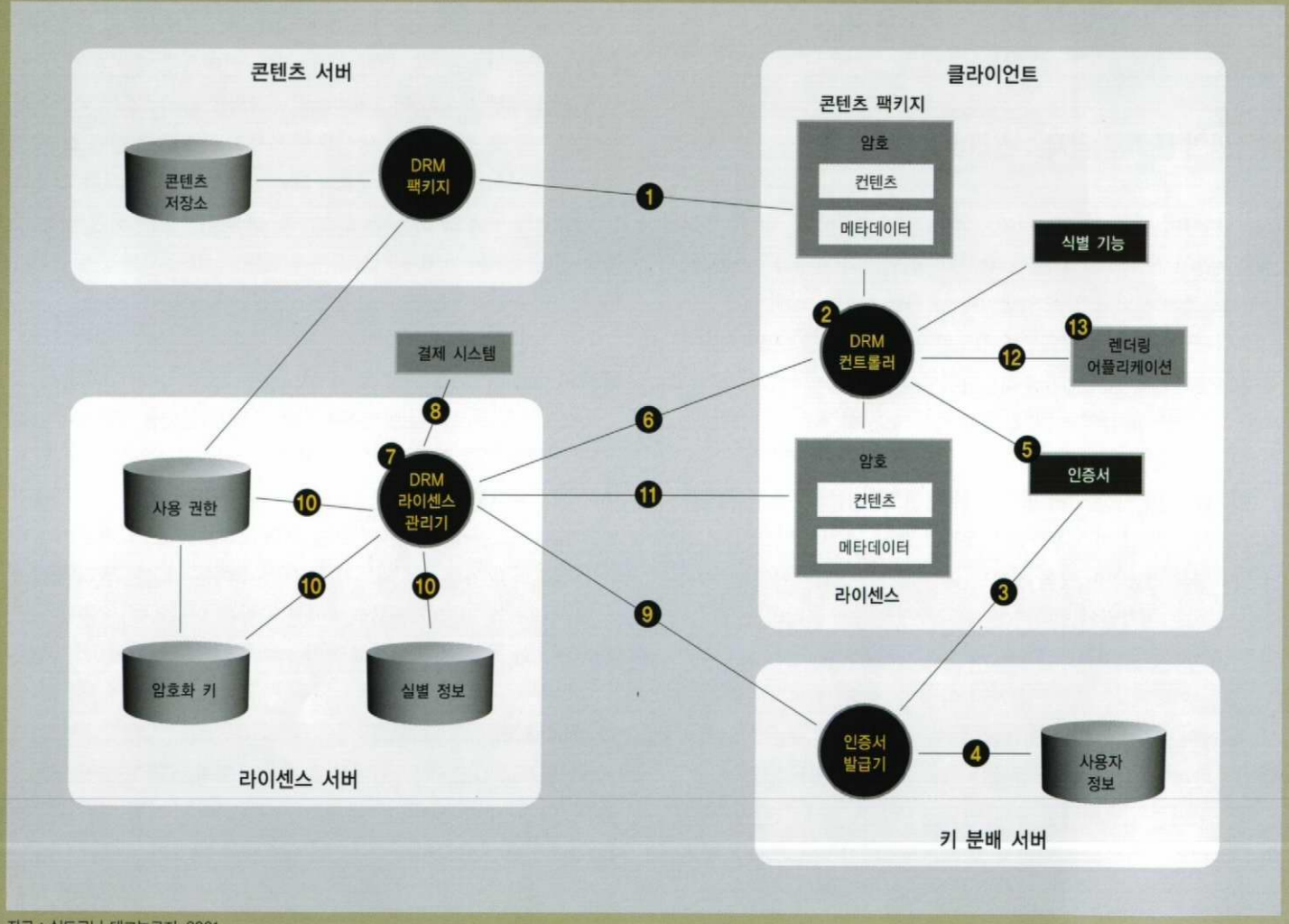
⑩ 식별 정보, 암호 키, 클라이언트 식별 정보 등을 모아 라이센스를 만든다(공개키).

⑪ 클라이언트에 라이센스를 발급한다.

⑫ 클라이언트에서 복호화를 실행하고,

⑬ 콘텐츠에 맞는 애플리케이션이 구동돼 서비스된다.

〈그림2〉 DRM 시스템의 기술적 구조도

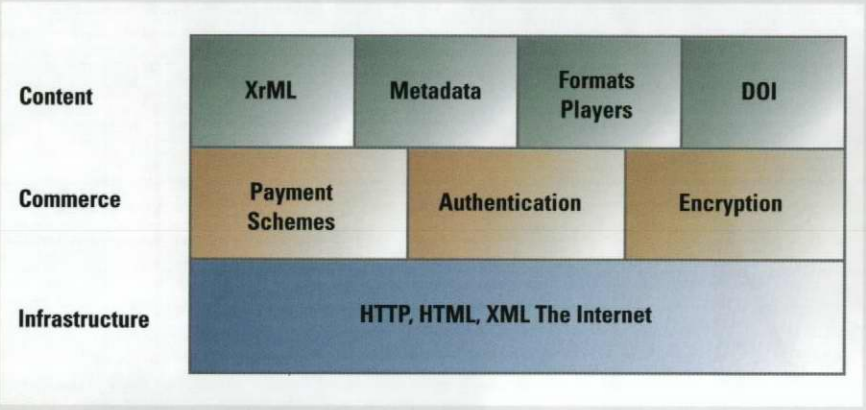


자료 : 실트로닉 테크놀로지, 2001

DRM 솔루션의 요소 기술과 표준화 동향

DRM 각 요소 기술별로 표준화 상황과 MPEG-21에 대해 간략하게 살펴보고자 한다. 〈그림3〉에서 나타난 인프라 부분과 전자상거래 부분은 DRM 기술이 얹어질 근간이므로 본 연재에서는 언급하지 않기로 한다.

〈그림3〉 DRM 표준 체계



자료 : GiantSteps Media Technology Strategies

XrML

Extensible Rights Markup Language의 약자로 콘텐츠에 대한 권리 관리 정보를 정의하기 위해 쓰인 XML 언어이다. 이 권리 관리 정보라는 것은 해당 콘텐츠의 소유권, 권리, 사용규칙(횟수, 기간, 직급별 등)을 정의해 콘텐츠 이용 시에 정의된 규칙대로 적용시켜, 콘텐츠를 원활히 사용하도록 하기 위한 일종의 명세이다.

이런 관리 정보를 표기하는 방법으로는 DRM 전문 업체인 콘텐츠가드(ContentGuard)에서 개발한 XrML이 가장 대표적이다. 이 외에도 ODRL(Open Digital Rights Language) 등 여러 언어들이 있으나 XrML이 MPEG-21의 REL(Rights Expression Language)로 채택됨으로써 현재 가장 표준으로 유력한 상태이다.

메타데이터

'데이터의 데이터'란 뜻인 메타데이터는 점점 확장돼 복잡성을 띠게 될 콘텐츠 비즈니스를 원활하게 지원하기 위해 유럽연합의 지적재산권 관련 기관에서 시작된 INDECS(Interoperability of Data in E-Commerce System)를 중심으로 논의가 진행 중에 있다. XrML이나 후술하게 될 DOI 역시 메타데이터의 구조를 띄고 있으며, 궁극적으로는 전자상거래에서 투명한 상거래와 저작권료를 받을 수 있는 자료 기술 프레임워크와 호환구조를 창출하는 것이 목적이다.

DOI

Digital Object Identifier의 약자로 1994년 미국출판인협회(Association of American Publishers)가 온라인 식별 체계를 제기하면서 시작됐다. DOI는 현재 웹 자원에 대한 Unique Identifier와 URL을 보완한 URN(Uniform Resource Name) 체계를 만족시키는 방향으로 전개되고 있다.

DOI 구조상 글로벌 핸들링을 맞는 미국의 CNRI(Corporation for National Research Initiatives)와 각 지역별로 결국 URL로 변환 서비스를 담당하는 RA(Registration Agency)가 필요하다. 이처럼 국제적인 콘텐츠의 고유한 코드를 부여하는 기술인 관계로 아직 표준화 단계까지는 다소 시간이 필요해 보인다. 이에 따라 대다수의 DRM 솔루션들은 DOI 체계를 미적용 상태에 있다.

이밖에 DRM 기술 표준을 위해서 연구활동 중인 여러 단체들이 있지만 그 중에서 MPEG-21의 활동이 가장 활발하다. MPEG-21은 2000년 초에 멀티미디어 콘텐츠 유통 프레임워크를 구성하기 위해 설립된 표준화 기구다. 멀티미디어 콘텐츠를 유통하기 위해서는 많은 부분의 기술 요소가 필요한데 이전에는 이러한 요소들이 서로 연계되지 않고 단편적인 하나의 요소 기술에 불과했다. 하지만 MPEG-21에서는 전체적인 큰 그림을 갖추고 이런 기술적 요소들을 적절하게 구성해 프레임워크를 형성하는 것을 목적으로 하고 있다.

이것으로 전자상거래 환경 하에서 다양한 디지털 콘텐츠를 다양한 네트워크와 단말기를 이용해 사용자가 상호 호환적으로 쉽고, 편리하게 생성, 배급할 수 있는 방법을 정의, 구현할 수 있는 하나의 유통체계의 기반을 만들고 있다.

세부적으로 콘텐츠 제작에서 시작해 생산, 유통, 소비, 사용 패키징, IPMP, 콘텐츠 식별 및 기술, 재정관리, 사용자 보호, 터미널과 네트워크 자원 추상화, 그리고 콘텐츠 표현 및 사건 보고를 포함하고 있다. 이 중 DRM은 MPEG-21의 주요 7가지 원소 중 콘텐츠를 신뢰성 있게 관리하고 보호하는 수단인 IPMP(Intellectual Property Management and Protection)을 주로 구성하고 있다.

지금까지 DRM의 구성 요소와 요소 기술, 그리고 솔루션 선택시 고려 사항들을 살펴보았다. 지난 10여년 동안 DRM 기술이 상당 부분 발전을 거듭해온 것이 사실이다. 하지만 정작 저작권 주된 문제점은 기술 외적인 문제인 비즈니스 모델, 구사업 체계의 문제점, 법적인 근거 미비, 사용자의 인식 부족 등에 있었다.

여기에 요소 기술 개발에 많은 집중을 해온 나머지 제대로 된 솔루션을 만들지 못한 부분도 있었다. 솔루션 벤더들은 비즈니스 모델과 함께 나가는 기술을 고민하고 콘텐츠 비즈니스 사업자들은 과감하게 솔루션을 적용해 필드에서 검증 받는 것이 현시점에서 DRM 관련 기술의 발전의 가장 효과적인 돌파구로 작용할 것이다.