

# DRM(Digital Rights Management)

이창열 · 동의대학교 컴퓨터공학과

## I. 개요

DRM(Digital Rights Management) 기술은 디지털 콘텐츠 유통에 안전성, 유통성, 재사용을 지원하며 저작권자, 유통업자, 소비자에 이르는 콘텐츠 라이프 사이클에 관계된 모든 에이전트를 만족시켜줄 수 있는 신뢰 구조를 제공하는 기술이다. DRM 자체가 신뢰를 제공하는 비즈니스 모델 구조를 간직하고 있기 때문에 기술이라기보다 모델이나 틀(Framework)이라고 말할 수도 있다.

이러한 DRM 기술(또는 틀) (이하 'DRM 기술'이라고 언급하겠음)은 인터넷이 등장하고, 콘텐츠 유통의 증가와 PKI 기반 암호화 기술의 등장에 따라 유통업자나 저작권자의 요구가 증가하면서 자연스럽게 제시된 유통체계인 것이다.

## II. DRM 기술의 탄생과 표준화

1996년 12월 국제저작권기구인 WIPO(World Intellectual Property Organization; www.wipo.

org)는 6년 간 이끌어오던 저작권법을 마무리하면서 3가지 사항을 발표하였는데, 그 중에 1개가 WCT(WIPO Copyright Treaty)와 WPPT(WIPO Performance and Phonogram Treaty)이며, 본 조항이 디지털 콘텐츠 유통과 관련된 법안인 것이다. WCT와 WPPT의 대표적인 내용은 콘텐츠에 삽입된 권리 관리정보(RMI; Rights Management Information)를 보호하는 것으로, 권리 관리정보에 기술조치(Technical Measures)를 취하는 것이고, 본 기술조치를 파괴하거나, 우회(기술조치에 쓰여진 정보를 사용하지 않고 콘텐츠를 사용하는 경우), 변경하는 어떠한 소프트웨어나 장치를 제조 또는 판매하는 기관에 대해 처벌하는 것이 주요 내용인 것이다.

WPPT는 WCT의 내용과 동일하며, 단지 실연·음반에 관한 조항인 것이다. WCT와 WPPT에서 언급한 기술이 구체적으로 어떤 것인가에 모호성이 있지만 보편적으로 DRM이라는 기술이 WCT와 WPPT를 만족시키는 기술이라고 인식하고 있다.

그러므로 DRM이라는 기술은 법적으로 보호받을

수 있으면서, 콘텐츠 라이프 사이클인 제작, 유통, 판매, 작동, 재판매 전 과정에 관여하는 디지털 콘텐츠의 구조체계를 가지는 것이다.

DRM 기술의 초기는 1995년부터 1998년까지 진행된 유럽의 IMPRIMATUR 프로젝트에 기초하고 있다. IMPRIMATUR 프로젝트에서는 디지털 콘텐츠 유통에 관한 전형적인 비즈니스 모델 정의(후에 MPEG-21의 초기 비즈니스 모델이 되었음), RMI 정보에 대한 유럽과 미국의 시각차이 분석, 워터마킹 기술 등에 관한 연구가 진행되었으며, 본 연구를 바탕으로 유럽의 CISAC, SUISA 등에서는 그동안 별도로 진행되어오던 디지털 콘텐츠 유통에서 확실한 저작권을 받을 수 있는 체계를 구성하여야 한다는 원칙에 따라 INDECS라는 단일 프로젝트를 1998년 10월부터 진행하기 시작하였지만, 본 프로젝트는 새로운 프레임워크인 MPEG-21을 주도하기 위하여 2000년 3월 3차 회의를 끝으로 종료하였다. 그러나 INDECS 프로젝트는 디지털 콘텐츠를 IFLA 모델에 기초하여 Work, Performance, Manifestation, 그리고 Item으로 분류하고 이들 각 콘텐츠 유형에 따른 저작권 정보를 체계적으로 분류 제시하였으며, Event 중심의 거래정보 표현 등으로 인하여 DRM 체계의 기본적 틀을 제시한 것으로 평가받고 있다. INDECS 프로젝트에 참여하였던 Keith Hill, Godfrey Rusty, Chris Barlas는 Rightscom이라는 자문회사를 만들고, 현재 진행중인 MPEG-21을 주도하고 있기 때문에 그동안 작업을 표준화라는 이름 하에서 재탄생시킨 것으로 해석하고 있다.

MPEG-21의 목표는 멀티미디어 콘텐츠 유통 프레임워크라고 정의하고 있으며, DRM 또한 디지털 콘텐츠에 대한 신뢰 프레임워크라고 정의할 수 있기 때문에 DRM과 MPEG-21 사이의 관계는 유사하면서도 다르다고 언급할 수 있다. 그것은 MPEG-21은 명확한 주도 그룹에 의하여 콘텐츠 유통구조

를 정하여 가는 것이라면, DRM 자체는 개념구조에 가깝기 때문이다. 실제로 전자책에서는 EBX DRM과 AAP의 DRM 표준화 방향 제안서, 영화분야에서 ISMA-DRM, 방송에서는 DVB-CPCM, TVAnyTime의 RMP, IRTF/IETF에서는 IDRM 등 DRM 개념이 적용되는 응용분야별로 표준화가 별도로 진행되고 있는 것이다. 그러나 이런 DRM 표준화를 자세히 살펴보면, MPEG-21을 제외한 DRM은 각기 응용분야를 가지고 있기 때문에 MPEG-21은 특정 응용분야에 의존하지 않는 프레임워크라고 할 수 있다.

특정 DRM 표준화 영역에서도 MPEG-21에서 제시하는 모델을 수용하면서 DRM 표준화 작업을 진행하는 것이 특별한 문제를 야기시키지 않기 때문에 MPEG-21은 DRM 표준화를 선도하고 있다.

그러면 우선 DRM이 어떤 것인지 살펴본 후, 표준화 동향을 좀 더 자세히 살펴보기로 하겠다.

### III. DRM 기술의 특징

DRM 기술의 특징은 Superdistribution(재배포)과 투명한 거래구조, 그리고 사용규칙이라는 3가지 특징을 가지고 있다.

재배포는 기존 콘텐츠 유통이 사용자의 공개키로 암호화하고, 사용자의 비밀키로 콘텐츠의 암호화를 푼다면, DRM에서는 콘텐츠마다 키를 생성하여 사용한다. 즉 콘텐츠의 공개키로 암호화하고, 콘텐츠의 비밀키를 판매(또는 허가받은 사람에게 배포)하는 것이다. 그러므로 누구나 허가를 받은 사람은 사용할 수 있는 것이고, 이러한 방식은 콘텐츠를 재유통할 수 있게 하는 것이다. 물론 이러한 방식에는 기

본적으로 고려할 사항이 좀 더 있다. 즉 어디에서 키를 받을 것인가, 그리고 비밀키는 무한정 유용한가가 의문시될 수 있으나, 이 또한 간단한 방법으로 해결방법을 제공하고 있다.

두 번째 투명한 거래구조는 기본적으로 라이선스를 제공하는 기관과 콘텐츠를 배포하는 기관(쇼핑몰)을 분리함으로써 해결될 수 있다. DRM 환경하에서 콘텐츠는 반드시 라이선스 파일이 있어야 동작하게 되어있다. 이 라이선스 파일에는 해당 콘텐츠의 비밀키와 사용규칙 정보 등이 들어있기 때문에 콘텐츠의 암호를 풀기 위하여 라이선스 파일이 필수적인 것이다.

그러므로 콘텐츠 판매의 마지막 단계로 라이선스 제공기관에 라이선스를 요청하면, 이러한 요청에 대하여 라이선스 제공기관은 해당 소비자에게 라이선스를 제공하고, 해당 내역(거래내역)을 보관하는 것이다. 이것은 일반 상가에서 카드로 물건을 살 경우 카드로 사용허가를 받는 과정과 동일한 것이다. 이러한 메커니즘은 해당 쇼핑몰이 판매내역을 감출 수 없으며, 저작권자와 계약을 투명하게 준수할 수 있는 환경을 제공한다. Adobe DRM인 ACS의 경우 또 다른 방법의 투명성을 제공하기도 한다. 즉 애초에 콘텐츠 제작시 해당 콘텐츠에 발급할 수 있는 라이선스의 최대량을 고정시키는 것이다. 이 개념은 종이 책 뒷면에 ‘인지’를 붙이고, 작가가 출판사에게 ‘인지’ 개수를 제어함으로써 책 판매량을 확인하고, 그리고 판매량에 해당하는 로열티를 받는 구조와 일치한다.

마지막 특정한 사용규칙(Usage Rules)은 콘텐츠를 소비자가 사용하는데 있어서 횟수, 날짜수, 장비 환경 등을 통제하는 것이다. 예를 들어 특정 콘텐츠를 ‘1일 무제한’, ‘1주일에 10번’, ‘1달간 무제한’,

‘1일 1회’ 등 볼 수 있는 횟수를 제한하는 것으로, 이러한 횟수에 따라서 해당 콘텐츠의 가격을 차별화할 수 있기 때문이다. 이때 소비자가 컴퓨터 날짜를 조작함으로써 실제로 사용을 연장하려는 시도를 할 수 있는데 이러한 변조를 Tampering이라고 하며, Tamper Resistance 기능이 반드시 DRM에 포함되어야 한다.

지금까지 언급한 3가지 사항이 반드시 있어야만 DRM 제품이라고 할 수 있다. 즉, 유통성(콘텐츠의 공개키/비밀키 사용하여 제작), 투명성(저작권자와 유통업자 사이 메커니즘), 사용성(다양한 비즈니스 모델 적용하여)이 보장되는 것이 DRM 기술인 것이다.

#### IV. 표준화 전망 및 국내 대응방안

이러한 DRM 기술은 응용분야에 따라 모습이 다를 수 있어도 기본구조는 같으며, 이러한 원칙에 따라 표준화가 진행되어 왔다.

IETF/IRTF에서 제시하는 IDRM(Internet DRM)인 경우, 기존의 DRM과 약간 다른 형태로 진행되고 있다. CDN과 같은 환경에서 네트워크 사이 URI(URL, URN, URC)를 사용하여 콘텐츠에 접근할 경우, 해당 콘텐츠를 해석할 수 있는 키 구조를 제공하는 것으로 전형적인 Broadcasting Encryption 기반으로 콘텐츠에 접근하는 것을 통제하는 것이다. 즉, 특정 콘텐츠의 Revocation List를 만들고 이 Revocation List에 해당하는 사람(또는 장치)은 콘텐츠에 접근할 수 있지만, 콘텐츠의 암호를 풀 수 없게 제약하는 것이다.

DRM 기술의 표준화는 MPEG-21 기반으로 진행

되고 있으며, 장르나 영역에 따라 MPEG-21에 추가적인, 아니면 보완적인 기능으로 표준화가 진행되고 있다.

de facto 표준이라는 분야는 초기 Intertrust를 선두로 해서, Contentguard가 DRM의 대표적인 업체라고 한다면, Reciprocal은 DRM 서비스 업체로 선두를 이루었었다. Intertrust는 업계의 선두로, ContentGuard는 XrML이라는 권리표현 언어를, 그리고 Reciprocal은 다양한 서비스 모델을 기반으로 DRM 시장을 점령하여 나갔었는데, Reciprocal은 서비스 모델 자체는 매우 훌륭하였지만 경영적 잘못으로 문을 닫았고, Intertrust는 판매부실로 매우 어려운 상황에 처하여졌으며, Contentguard 역시 특별한 성과를 거두지 못하고 있는 실정이다.

이러한 선두 DRM 업체의 쇠퇴는 후발 DRM 업체인 Microsoft와 Adobe의 약진과 대비된다. 그것은 Vendor DRM이라 불리는 후발 DRM 업체의 제품이 기존 플레이어/뷰어 시장점령과 매우 관계가 깊기 때문이다. Microsoft와 Adobe는 DRM 시장진출 이전에 Media Player와 Acrobat Reader라는 세계적으로 일반화된 플레이어 시장에서의 성공과 직결하기 때문이다. DRM 제품의 특징상 Player 부분에 DRM 정보가 들어가 있어야 하고, 특정 회사가 자신의 DRM 제품을 제작할 경우 자기의 플레이어가 있어야 하기 때문이다. 그것은 자연스럽게 소비자에게 DRM 제품을 선택할 경우 Plug-in이나 아니면 특정 (Proprietary) 플레이어를 설치하는 부담이 주어지기 때문이다.

이러한 관점에서 Media Player나 Acrobat Reader에 DRM 정보를 삽입하여 제공하는 Microsoft나 Adobe는 DRM 시장에서 매우 독보적인 위치를 차지하게 되었다. 현재 Video/Audio인 경

우 Microsoft의 DRM이 de facto 표준이라고 이야기하는데 전 세계적으로 무리가 없다. 그러나 Adobe DRM인 ACS의 경우, 미국 시장에서는 Microsoft의 또 다른 DRM(전자책용 DRM)인 DAS와 경쟁관계에 있기 때문에 de facto 표준이라고 할 수 없다. 물론 국내에는 아직 DAS가 서비스되고 있지 않기 때문에 국내 시장에서는 ACS가 우월한 상태에 있다.

국내 DRM 업체는 이러한 세계적인 추세에 대하여 매우 늦은 대응을 하고 있다. 그것은 DRM이 무엇인가에 대한 정확한 정의를 알고 있는지부터 짚고 넘어가야 한다. DRM은 복합적인 기술이며 어떤 방식을 제공하여도 유통성, 투명성, 사용성을 제공하여야 하나, 기존의 PKI 기술의 안정성과 워터마킹의 추적성이 DRM인 것처럼 포장하는 것으로 인하여 진정한 DRM 기술진보에 늦은 대응을 하고 있는 것이다.

물론 현재 ETRI를 중심으로 우리의 DRM 기술개발을 시작하였으며, 이러한 기술개발이 우리의 독창성과 MPEG-21 등에서 제시하는 표준화를 바탕으로 개발을 진행하여야만 앞으로 상품화된 시장에서 경쟁력을 확보할 것이다.

DRM에 대한 EU의 2002년 2월 보고서 등에서 우리는 DRM이 선택적인 기술이 아니라는 것을 확신할 수 있다. DRM은 WCT와 WPPT에서 제시하는 법적 기술이며, 콘텐츠 라이프 사이클의 맨 끝 쪽에 있는 유통기술이고, 또한 미래 인터넷 거래에 대한 인증을 제공할 수 있기 때문에 반드시 확보하여야 하고, 추가적으로 시장에서 경쟁력을 갖추어야 할 것이다. 