저작권연구 2009-01

2009 워킹그룹 최종보고서

SW 역분석과 기술적 보호조치

[법적·기술적 재해석]

한국저작권위원회
KOREA COPYRIGHT COMMISSION

참여연구원

- **손승우** 교수 | 단국대 법과대학 |
- **정진근** 교수 | 강원대 법학전문대학원 |
- **이강석** 계장 | 금융결제원 |
- **강기봉** 선임연구원 | 한국소프트웨어저작권협회 |
- **김석훈** 팀장 | 저작권보호센터 |
- **정재곤** 저작권정보센터장 | 한국저작권위원회 |
- **김혜창** 법정책연구팀장 | 한국저작권위원회 |
- **이진태** 연구원 | 한국저작권위원회 |

Contents

Contents

6장 SW 역분석과 기술적보호조치의 관계 분석

7장 역분석과 기술적 보호조치 관련 법제도 개선방안

제1장 연구의 목적과 범위

Ⅰ. 연구의 목적

Ⅱ. 연구의 범위

제 1 장 연구의 목적과 범위

Ⅰ. 연구의 목적

정보통신기술의 발달로 인해 SW는 우리 일상에서 매우 중요한 역할을 하고 있다. 전화기, 냉장고, 세탁기에서 시작해서 항공기, 인공위성에 이르기까지 우리주변의 모든 기기에는 SW가 없는 것이 없을 정도로 그 중요성은 더욱 커지고 있다. 이렇게 SW의 중요성이 커지는 만큼 SW에 대한 저작권 보호와 이를 위한 기술적보호조치의 대한 관심도 매우 커져가고 있다.

특히 SW의 경우에는 거금의 자금을 들여 수많은 기술적보호조치를 취함에도 불구하고 그것을 우회하거나 무력화하는데 걸리는 시간은 빠르면 몇시간 늦어도 몇 달 밖에 걸리지 않는다. 실제로 2008년 2월 26일날 개최된 '캔섹웨스트 시큐리티 컨퍼런스' 해킹대회에서 애플의 맥 OS X 레퍼트에 대한 해킹 공격이 있은 후 2분 만에 맥 OS X의 시스템을 장악했고, 윈도우 비스타는 3일째 되던 날에 해킹이 되었다. 물론 주최측에서 하루가 지날때마다 난이도를 낮추긴 했지만 기술적 보호조치를 무력화하는데 걸리는 시간을 감안한다면 SW를 보호하는데 있어서 가장 핵심기술이라고 할 수 있는 기술적 보호조치에 대한 관심이 커질 수 밖에 없는 것이다.[1)]

또한 해외에서는 역분석이 하나의 학문이나 문화로 형성되어 이와 관련된 블로그나 카페, 동호회 등이 많이 개설되어 있어 서로의 정보를 공유하며 다양한 기술적 보호조치들의 기술을 향상시키고 있다. 더 나아가서는 정부의 정보기관이 이러한 환경이나 문화조성에 앞장서서 이들의 컨퍼런스에 참여하여 정보를 공유하고 어떤 경우에는 아예 컨퍼런스를 지원해주기도 한다. 그러나 우리나라에서는 이러한 역분석에 대한 논의가 외국과 같이 활발히 이루어지고 있지 않다. 특히 기술적 보호조치와 관련해서는 이것이 하나의 범죄행위처럼 여겨지는 문화에서 이와 관련된 연구나 자료를 공유한다는 것은 너무나 험난한 길이 아닐 수 없다.

1) http://www.asiae.co.kr/news/view.htm?idxno=2008033016372583429&nvr=y

법적으로 들어가면 우리나라 저작권법에서는 역분석에 대해서 정당한 권한에 의하여 프로그램을 이용하는 자 또는 저작권자의 허락을 받은 자에 한해 호환 목적으로만 역분석을 인정하고 있다.[2] 그러나 이와는 약간 모순되게도 프로그램의 역분석이 요구되는 프로그램의 기능 조사 · 연구 · 시험 목적인 경우는 복제를 허용해주고 있다. 즉, 프로그램의 저작재산권의 제한 사유에는 프로그램의 기초를 우리는 아이디어 및 원리를 확인하기 위하여 프로그램의 기능을 조사 · 연구 · 시험 목적으로 복제할 수 있도록 규정하고 있다.[3]

이러한 문제점들을 해결하기 위해 금년도 워킹그룹에서는 역분석과 기술적 보호조치에 대한 전문가분들과 함께 이에 대한 발표와 토론을 5회 개최하였다. 그리고 이러한 논의의 최종결과물로써 이 보고서가 작성되었다. 이보고서에는 역분석과 기술적 보호조치에 대한 기술적인 이해와 현재 SW 산업의 실태를 살펴보았고 이를 통해 현행 법제도의 문제점과 이에 대한 개선방안을 도출해보고자 하였다.

Ⅱ. 연구의 범위

이번 연구의 범위는 기본적으로 SW의 역분석과 기술적보호조치에 대한 기술적인 이해와 현행 법제도에 대한 이해를 기반으로 이에 대한 문제점을 살펴보고 이에 대한 개선방안을 도출하는데 그 목적이 있다.

이를 위해서 크게 역분석 부분과 기술적보호조치에 대한 부분으로 나누고 마지막에서 이 둘의 상관관계에 대해서 검토하였다.

이를 위해 제2장에서는 역분석에 대한 기술적 이해를 돕기 위해 역분석이 무엇이고 역분석이 어떻게 이루어지는를 살펴보았다. 그리고 역분석의 유형에는 어떤 것이 있는지에 대해서 살펴보았다.

2) 저작권법 제101조의4
제101조의4(프로그램코드역분석) ① 정당한 권한에 의하여 프로그램을 이용하는 자 또는 그의 허락을 받은 자는 호환에 필요한 정보를 쉽게 얻을 수 없고 그 획득이 불가피한 경우에는 해당 프로그램의 호환에 필요한 부분에 한하여 프로그램의 저작재산권자의 허락을 받지 아니하고 프로그램코드역분석을 할 수 있다.
② 제1항에 따른 프로그램코드역분석을 통하여 얻은 정보는 다음 각 호의 어느 하나에 해당하는 경우에는 이를 이용할 수 없다.
1. 호환 목적 외의 다른 목적을 위하여 이용하거나 제3자에게 제공하는 경우
2. 프로그램코드역분석의 대상이 되는 프로그램과 표현이 실질적으로 유사한 프로그램을 개발 · 제작 · 판매하거나 그 밖에 프로그램의 저작권을 침해하는 행위에 이용하는 경우

3) 저작권법 제101조의3 제1항 제6호
제101조의3(프로그램의 저작재산권의 제한) 6. 프로그램의 기초를 이루는 아이디어 및 원리를 확인하기 위하여 프로그램의 기능을 조사 · 연구 · 시험할 목적으로 복제하는 경우(정당한 권한에 의하여 프로그램을 이용하는 자가 해당 프로그램을 이용 중인 때에 한한다)

제3장에서는 이러한 역분석에 대한 이해를 바탕으로 현행 역분석의 법적 이해를 위해 저작권법상 역분석에 대한 정의와 이를 적용하기 위한 요건들을 살펴보았다. 그리고 이 조항이 가지는 저작권법에서 가지는 법적 의미에 대해서 검토해보고 역분석과 불가분에 관계에 있는 기술적보호조치 예외 사유의 관계와 국내외의 판례에서는 어떻게 역분석 사례를 다루고 있지는 살펴보았다.

제4장에서부터는 기술적보호조치로 넘어가서 기술적보호조치의 기술적 이해를 돕기 위해 먼저 기술적보호조치의 의의와 유형에 대해서 살펴보고 기술적보호조치의 기술현황 및 어떻게 기술적보호조치가 적용되는지에 대해서 검토해보았다.

제5장에서는 역분석과 같이 기술적보호조치가 가지는 법적 성격을 살펴보기 위해서 기술적보호조치의 법적 의의와 저작권법상 기술적보호조치가 어떻게 규정되고 적용되는지를 살펴보았다. 또한 국내외 판례를 통해서 기술적보호조치에 대한 해외 사례 및 국내 사례를 살펴보았다.

제6장에서는 창과 방패와도 같은 역분석과 기술적 보호조치와의 관계에 대해서 분석을 해 보았다. 이를 위해 저작권과 기술적보호조치로 저작물을 이중으로 보호하게 된 배경과 기술적보호조치 저작물에 대한 저작권 제한 규정의 적용가능성, 그리고 저작권법상 이 두 규정간의 상관관계에 대해서 살펴보았다. 그리고 해외 법률과 해외지침 등을 통해 현재 역분석 조항과 기술적보호조치 조항의 입법배경에 대해서도 살펴보았다.

마지막으로 제7장에서는 지금까지 논의된 기술적이고 법적인 논의들을 바탕으로 우리나라의 역분석 및 기술적보호조치를 위한 법적 · 정책적 개선방안들을 정리해보았다.

그리고 여기서 사용되는 용어 중 역분석과 리버스 엔지니어링이 혼동되어 사용되고 있는데 이것은 실제 개발자들 사이에서는 리버스 엔지니어링이라는 용어가 법적으로는 역분석이라고 사용되고 있기 때문에 생겨나는 용어상의 차이로 이 보고서에서는 동일한 의미로 사용된다.

제2장 역분석의 기술적 이해

제 2장 연구의 목적과 범위

이강석 계장(금융결제원)

Ⅰ. 역분석의 의의

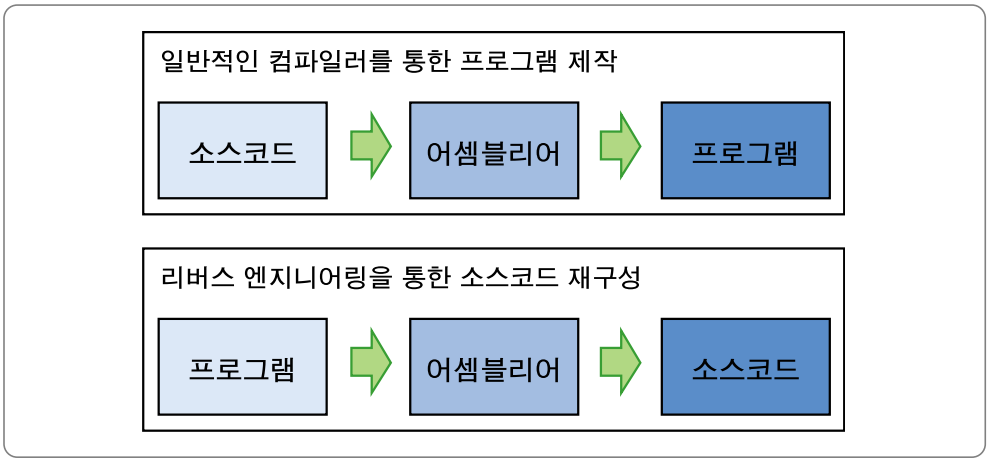
1. 리버스 엔지니어링이란 무엇인가

소프트웨어 관점에서의 엔지니어링이란 알고리즘을 설계하고 이를 소스코드 형태의 프로그램 언어로 제작하고 컴파일러에 의해 기계 언어 형태의 프로그램이 완성되는 일련의 과정을 의미한다.

개발환경에 따라 32bit, 64bit 또는 다양한 운영체제 환경에서 실행되는 프로그램을 만들 수도 있으며 이렇게 만들어진 프로그램들은 소스코드를 보지 않는 이상 구현된 기능과 알고리즘을 확인할 수가 없어 실행에 따른 동작만 볼 수 있게 된다.

리버스 엔지니어링이란 소프트웨어에 대한 디버깅, 디컴파일 등의 분석을 통해 원래의 제품에 구현된 구조, 원리, 기술, 방법, 기능, 알고리즘, 노하우 등을 역으로 분석하여 재구성하는 과정을 말하며 역공학, 역분석, 리버싱, 리버스 엔지니어링, RCE, RE 등의 이름을 갖고 있다.

리버스 엔지니어링을 그림으로 나타내면 다음과 같으며 흔히 소스코드 제작 후 컴파일을 하여 만들어지는 프로그램 과정을 정공학이라고 하고 프로그램에서 역으로 분석하여 소스코드를 추출하는 과정을 역공학이라고 이해할 수 있다.



초기 리버스 엔지니어링은 기계, 부품, 하드웨어의 설계, 제조방법, 노하우 등을 분석하여 그대로 복제하여 만들거나 기존 제품보다 더 나은 제품으로 발전해 나아가는데 쓰였다. 잘 만들어진 제품은 나사, 형태, 크기까지 그대로 모방하여 만들기도 했으며 하드웨어 제작자 입장에서는 중요 부품의 분해와 복제를 막기 위해 다양한 방법을 이용하여 제작하기도 하였다.

현재의 소프트웨어 또한 하드웨어 복제, 모방과 같이 소스코드를 복제하거나 리버스 엔지니어링을 이용하여 만들어 지기도 하며 어떤 경우는 타사 제품의 중요코드와 알고리즘을 분석하여 얻어낸 코드와 아이디어를 GUI[4]만 변경한 채 출시하기도 한다. 이런 제품들은 사용자들의 의심과 분석을 통해 밝혀지고 기업의 신뢰도와 이미지는 추락하게 된다.

자사가 개발하려는 프로그램에 다른 오픈소스 또는 공개된 모듈을 사용한다고 했을 때 해당 모듈이 갖고 있는 라이선스를 정확히 파악하고 이를 준수해서 사용해야 하지만 이를 숨기고 그대로 사용하거나 약간만 코드를 수정하여 모든 것을 개발했다고 하는 프로그램도 있을 수 있다.

리버스 엔지니어링의 기본적인 목적은 컴퓨터 프로그램이 내부적으로 어떤 과정을 거쳐 실행되는지에 대한 선의의 행동패턴 연구에서 출발한다. 이를 통해 상호 호환되는 소프트웨어 개발을 할 수 있고 분석 과정에서 얻은 아이디어를 통해 새로운 소프트웨어를 개발하고 설계상의 오류로 인한 취약점을 찾아 패치하는 일들과 악성코드 분석을 통해 사용자의 안전한 컴퓨터 환경을 지키는 일들도 할 수 있다.

그러나 이러한 분석과정에 앞서 중요한 점은 분석하려는 대상 소프트웨어에 대한 정당한 사용권한이 있는지 확인해야 하며 정당한 권한으로 지불하거나 허락을 받지 않은 불법 소프트웨어, 불법 복제물 등은 이에 해당되지 않는다.

리버스 엔지니어링은 창과 방패의 속성을 모두 갖고 있어, 좋은 목적으로 쓰일 경우 소프트웨어 발전과 기술발전에 선의의 영향을 끼칠 수 있는 반면 악의적인 목적으로 쓰일 경우 저작권 침해, 온라인 게임 데이터 변조, DRM 우회, 프로그램 인증 우회 등 악영향을 끼치게 된다.

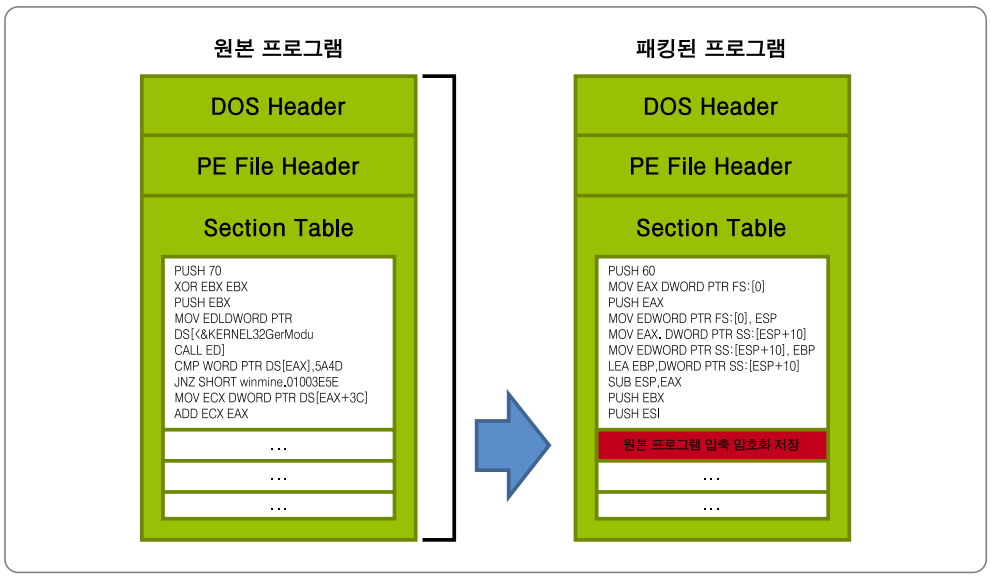
이런 악의적인 리버스 엔지니어링을 막고자 실행 파일에 안티 리버스 엔지니어링 기법을 적용하기도 하는데 가장 대표적인 것이 실행파일(Windows 운영체제 환경에서의 PE파일[5])을 패킹하는 것이다. 패킹은 일반적으로 많이 생각하고 있는 여러 파일을 하나의 압축파일로 만드는 과정을 말하는 것이 아닌 실행파일을 실행 압축하는 것이며 패커의 암호화 및 압축 알고리즘에 의해 패커 프로그램의 섹션 내부에 원본 프로그램을 저장하는 것을 말한다.

4) GUI(Graphical User Interface) : 마우스나 메뉴 등의 인터페이스로 구성된 프로그램의 외적인 모습을 말한다.
5) PE파일 : Windows 운영체제 환경에서의 실행파일로써 EXE, DLL, OCX 등의 확장자

이렇게 패킹된 프로그램이 실행되면 패킹 프로그램의 알고리즘이 우선 시작되고 복호화, 압축 해제 알고리즘이 수행된 후 메모리에 원본 프로그램 실행코드가 저장되며 이 때 원본 프로그램이 메모리에서 실행하게 된다. 이 과정을 언패킹 이라고 하며 언패킹된 지점이 원본 프로그램의 시작점인 OEP[6]가 된다.

다음 그림과 같이 원본 프로그램은 패킹된 프로그램의 하나의 섹션 안에 존재하기 때문에 패킹된 프로그램을 디스어셈블러나 디버깅을 하게 되면 원본 프로그램을 분석하는 것이 아닌 패킹된 프로그램을 분석하게 되는 것이다.

중요 프로그램을 보호하려고 실행파일에 패킹을 하지만 악성코드도 자신을 보호하고 분석을 방해하려는 목적으로 패킹을 하는 경우도 많다. 실제 악성코드를 분석하려면 패킹된 상태가 아닌 원본 프로그램인 상태에서 분석을 해야 원활한 분석이 가능하므로 언패킹을 하는 시간이 추가로 소요된다.



실행파일에 패킹을 적용하면 패킹 프로그램의 알고리즘, 기능에 따라 원본 프로그램의 안전을 기대할 수 있는데 패커의 대표적인 오픈소스 프로그램에는 UPX[7]가 있고 상용 패킹 프로그램에는 Themida[8], ASProtect[9] 등이 있다.

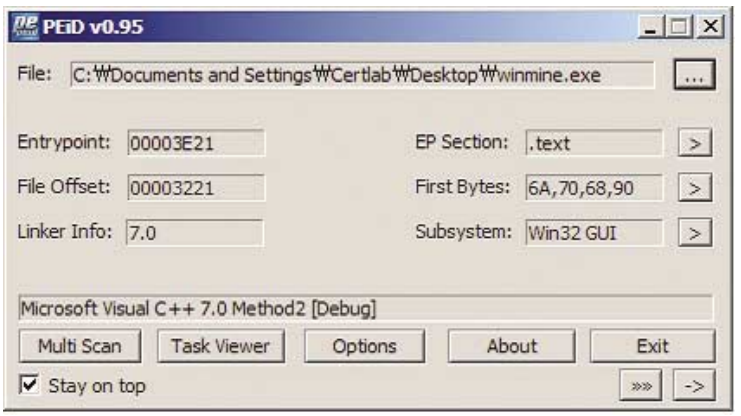
6) OEP : Original Entry Point (원본 프로그램의 시작 지점)
7) UPX : upx.sourceforge.net
8) Themida : www.oreans.com/themida.php
9) ASProtect : www.aspack.com/asprotect.aspx

2. 리버스 엔지니어링의 기본 분석

리버스 엔지니어링의 기본적인 분석 과정을 통해 각 단계별로 어떤 정보들을 확인 할 수 있는지 알아본다. 기본적으로 파일의 기본정보를 파악하여 분석 방향을 정하고 디스어셈블러, 디버거 프로그램을 이용하여 세부 분석을 한다. 실행파일에서 원본 소스로의 변환이 필요하다면 디컴파일 프로그램을 이용하여 변환하여 분석한다.

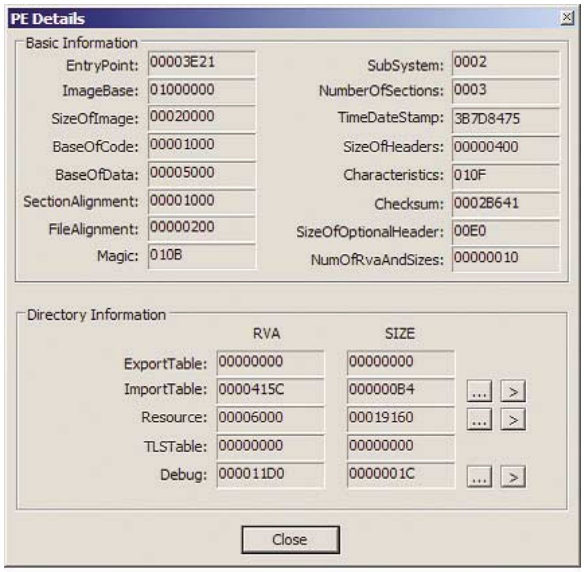
가. 파일의 기본정보 확인

분석의 시작은 분석 대상에 대한 기본 정보 등을 파악하는 것으로 PEID[10]를 통해 어떤 개발 프로그램으로 컴파일 되어 있는지에 대한 정보를 확인할 수 있다. 아래 이미지는 윈도우 운영체제에서 기본으로 제공하는 지뢰찾기 게임이고 "Microsoft Visual C++ 7.0"으로 컴파일된 것으로 확인 되지만 이 정보는 100% 정확한 것은 아니다.

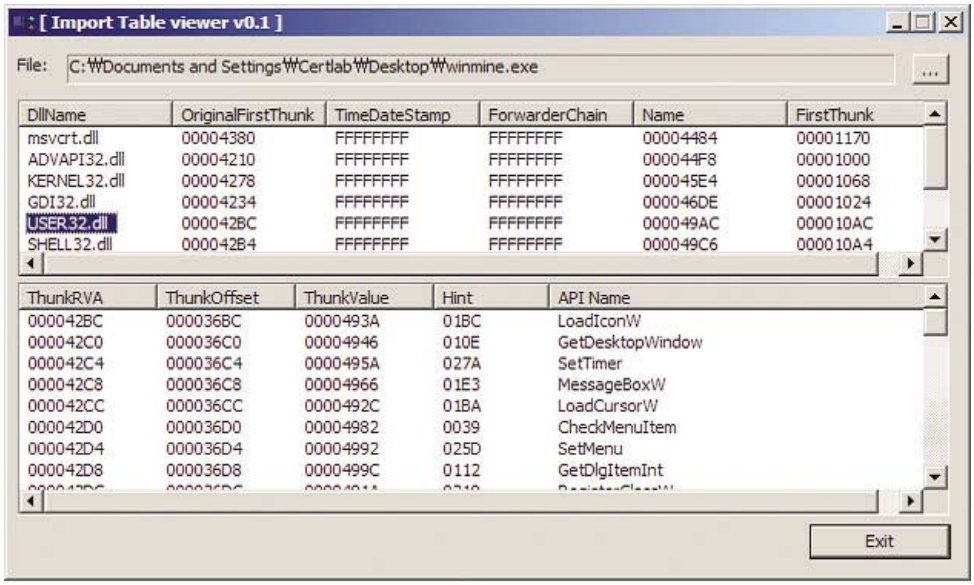


PEiD 프로그램은 PE 파일의 구조를 볼 수 있는 기능도 제공하는데 프로그램의 시작 지점(Entry Point), 섹션 정보(NumberOfSections), RVA 계산시 이용되는 시작지점(Image Base), 사용되는 외부함수 정보가 담긴 테이블(Import Table) 정보 등을 확인 할 수 있다.

10) PEID : www.peid.info



Import Table은 프로그램에서 사용하고 있는 외부 API함수의 경로와 이름을 저장하는 테이블이며 Import Table Viewer[11] 프로그램을 이용하여 이런 정보들을 쉽게 확인 할 수 있다.

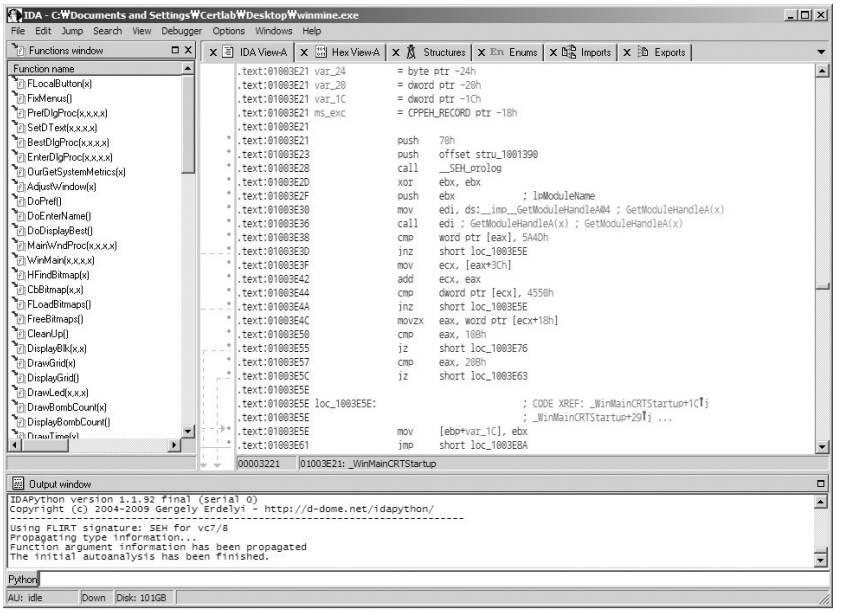


11) Import Table Viewer : www.ntcore.com

나. 디스어셈블러

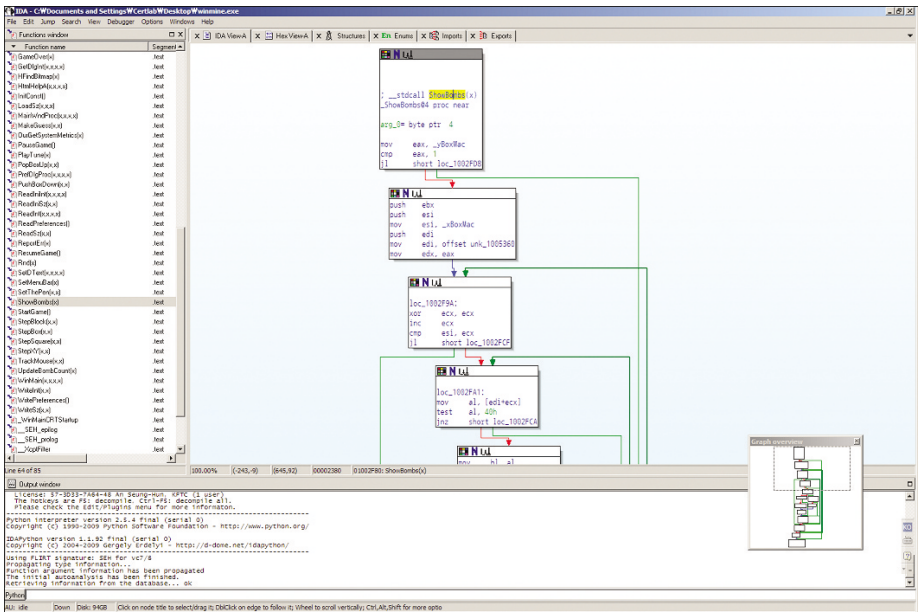
어셈블리어는 기계어와 1:1 매핑이 되며 이를 이용한 디스어셈블러는 기계어를 번역하여 어셈블리어로 변환해준다. 이런 디스어셈블러 프로그램들에는 IDA[12], BDASM[13], PVDasm[14], DisasmViewer[15] 등이 있으며 상용 소프트웨어인 IDA 같은 경우 다양한 플랫폼, 아키텍처, 파일 포맷을 지원하고 어셈블리어 명령들을 그래프 형태로도 출력해주는 기능을 갖고 있기 때문에 가독성이 뛰어나 분석하는데 효율적인 장점이 있다.

다음은 IDA 뿐만 아니라 대부분의 디스어셈블러 프로그램의 일반적인 형태이며 기계어를 어셈블리어로 변환한 화면과 해당 .text 섹션의 주소값, 변수선언 부분, 해당 프로그램에 쓰인 API 명령, 함수정보들을 볼 수 있다.



다음은 IDA 프로그램을 이용하여 지뢰찾기 게임에서 게임오버시 지뢰들이 모두 보이게 하는 ShowBombs 함수의 디스어셈블된 화면이다. 그래프 형태로 볼 수 있고 각 분기문 마다 참, 거짓으로 이동되는 위치를 쉽게 표시해 준다.

12) IDA : www.datarescue.com
13) BDASM : www.bdasm.com
14) PVDasm : pvdasm.reverse-engineering.net
15) DisasmViewer : naggingmachine.tistory.com/430



다. 디버거

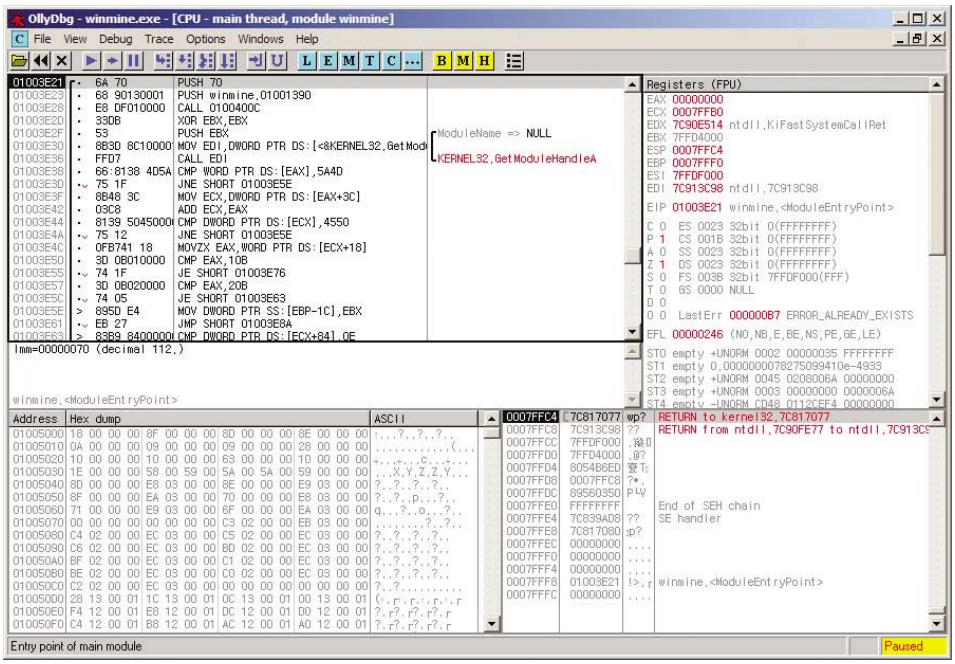
소프트웨어 개발 시 소스코드 레벨에서 개발 프로그램이 제공해주는 디버거 프로그램을 이용하여 특정 변수의 상태와 프로그램 실행흐름을 확인 할 수 있다. 디버거의 큰 장점은 버그가 있을만한 소스코드 라인에 브레이크 포인트를 걸고 프로그램을 실행하면 브레이크 포인트가 걸린 라인에서 실행이 멈추고 이후 소스코드 한 라인씩 순차적으로 실행하며 프로그램의 예외상황 및 행동패턴을 분석하여 버그를 찾아낼 수 있다.

소스코드 레벨에서의 디버깅처럼 기계어 레벨에서도 디버깅을 할 수 있는데 대표적으로 OllyDebugger[16], Immunity Debugger[17], BinNavi, GDB[18] 등이 있다.

기계어에서 어셈블리어로 디스어셈블된 화면 상태에서 버그가 있을만한 어셈블리어 라인에 소스코드 레벨에서의 디버깅과 마찬가지로 브레이크 포인트를 걸고 프로그램 실행을 하면 해당 라인까지 실행되고 멈추며 그 부분부터 한줄 한줄 어셈블리어 명령을 순차적으로 실행이 가능하다.

다음은 OllyDebugger 프로그램을 이용하여 지뢰찾기 프로그램을 오픈한 화면이다.

16) OllyDebugger : www.ollydbg.de
17) Immunity Debugger : www.immunityinc.com/products-immdbg.shtml
18) GDB : www.gnu.org/software/gdb



디버거와 디스어셈블러는 서로 중복되는 기능들이 많은데 이것은 어떤 기능에 더 특화되었는지에 따라 분류되며 IDA 같은 경우 디버깅 기능도 막강하지만 FLIRT(Fast Library Identification and Recognition Technology)[19]기능과 다양한 플랫폼, 아키텍처, 파일포맷을 지원하는 등의 특징 때문에 디스어셈블러로 분류된다. OllyDebugger 같은 경우 유저모드[20] 기반에서 실행되는 프로그램이며 수많은 사용자가 만든 다양한 플러그인과 스크립트들이 있으며 디버깅에 특화된 기능들이 많기 때문에 디버거로 분류된다.

라. 디컴파일러

기계어에서 어셈블리언어로 변환된 상태에서 하이레벨 언어 형태로 변환해주는 프로그램을 말하며 종류로는 자바 디컴파일러, 플래시 디컴파일러, 실행파일 디컴파일러, 델파이 디컴파일러, 닷넷 디컴파일러 등이 있으며 어떤 개발도구로 컴파일 되었는지에 따라 디컴파일러의 종류는 다양하며 모든 파일이 디컴파일 되는 것은 아니다.

19) FLIRT(Fast Library Identification and Recognition Technology) : 기계어의 코드로부터 컴파일러 특유의 Library 함수를 산출해 낼 수 있는 기능
20) 유저모드 : 인텔 프로세서에서는 Ring0(커널모드), Ring3(유저모드)가 있으며 프로그램이 실행될 때 운영체제의 중요한 데이터가 손상되지 않도록 별개의 모드로 나누어서 실행되는 것을 말한다. 일반적인 프로그램은 대부분 유저모드에서 실행된다.

다음은 Hexray[21] 디컴파일러 프로그램을 이용하여 ShowBombs 함수를 C언어로 변환한 일부 화면이다.

```
.text:01002F80 ; _stdcall ShowBombs(X)
.text:01002F80 _ShowBombs04  proc near               ; CODE XREF: GameOver(x)+2F?D
.text:01002F80
.text:01002F80 arg_0         = byte ptr  4
.text:01002F80
.text:01002F80               mov     eax, _yBOXMac
.text:01002F85               cmp     eax, 1
.text:01002F88               jl      short loc_1002FDB
.text:01002F8A               push    ebx
.text:01002F8B               push    esi
.text:01002F8C               mov     esi, _xBoxMac
.text:01002F92               push    edi
.text:01002F93               mov     edi, offset unk_1005360
.text:01002F98               mov     edx, eax
.text:01002F9A
.text:01002F9A loc_1002F9A:                          ; CODE XREF: ShowBombs(x)+53?j
.text:01002F9A               xor     ecx, ecx
.text:01002F9C               inc     ecx
.text:01002F9D               cmp     esi, ecx
.text:01002F9F               jl      short loc_1002FCF
.text:01002FA1
```

```
int __stdcall ShowBombs(char a1)
{
  int v1; // edx@2
  _UNKNOWN *v2; // edi@2
  signed int v3; // esi@2
  signed int v4; // ecx@3
  char v5; // al@4
  char v6; // bl@5
  char v7; // al@7

  if ( yBoxMac >= 1 )
  {
    v3 = xBoxMac;
    v2 = &unk_1005360;
    v1 = yBoxMac;

  ... 생략 ...

LABEL_11:
      ++v4;
      if ( v4 > v3 )
        goto LABEL_12;
    }
  }
  return DisplayGrid();
}
```

21) Hexray : www.hex-rays.com

다음은 Sothink SWF Decompiler[22] 프로그램을 이용하여 SWF 파일의 이미지, 버튼, 심벌정보, ActionScript 정보들을 추출할 수 있다.

추출된 이미지, 버튼, 심벌정보

3. 안티 리버스 엔지니어링

리버스 엔지니어링을 막기 위한 다양한 방법 중 안티 리버스 엔지니어링 분야도 크게 발전하고 있다.

프로그램 내부 알고리즘과 중요 데이터들을 분석 하지 못하도록 실행파일을 패킹하거나 안티 디버깅을 적용함으로써 디버깅[23]을 방지하고 분석을 어렵게 하는데 큰 목적이 있다.

프로그램 실행과 상관이 없는 의미 없는 코드들을 무작위로 삽입하거나 패킹, 코드 난독화, 암호화, 리버스엔지니어링 관련 프로그램 실행시 강제 프로그램 종료, 프로그램 실행 시 다른 프로세스가 접근 하지 못하도록 하는 등의 방법으로 프로그램을 보호하며 분석을 방해하고 지연시킨다.

22) Sothink SWF Decompiler : www.sothink.com/product/flashdecompiler

23) 디버깅 : 프로그램의 오류를 찾아 수정하는 것으로 프로그램 제작과정의 마지막에 수행하는 작업이다. 프로그램의 특정 부분에 브레이크 포인트를 설정한 후 실행을 하면 그 위치에 프로그램이 멈추게 되며 메모리에 값이 제대로 들어가 있는지 확인하고 코딩한 흐름 데로 프로그램이 진행되는지 단계적으로 실행할 수 있다. 오류를 찾아 수정하는 것으로 디버깅이라고 하며 디버깅을 해주는 프로그램을 디버거라 한다. [역분석구조와원리 – 안티디버깅] 참고

리버스 엔지니어링을 막기 위한 원천적인 방법은 아직까지 존재하지 않으며 얼마나 분석을 어렵게 하느냐에 따라 프로그램의 보호되는 시간이 늘어나게 된다.

돈과 관련된 상용 소프트웨어 같은 경우 기능 구현이 완료되면 끝이 아니라 프로그램을 보호 할 안티 리버스 엔지니어링 까지 적용해야 한다. 그렇지 않을 경우 시간과 노력을 들여 개발한 소프트웨어가 크랙이 되어 P2P, 웹하드에 유포 될 수 있는 문제가 있으며 특히 라이선스 인증 부분은 소프트웨어를 개발하는데 들어간 시간과 노력만큼 신경을 써야 하는 부분이다.

라이선스 인증방식의 종류로는 크게 클라이언트인증, 서버인증 방식 등이 있으며 인증방식에 취약점이 있을 경우 이를 우회하는데 시간이 소요되지만 불가능 하지는 않는다.

라이선스 인증 방식으로 USB 메모리로 만들어진 하드웨어기반 복제 방지키도 사용되고 있는데 소프트웨어를 실행하려면 이 키를 컴퓨터에 인식시켜야 실행이 되는 구조이며 현재로써는 안전하다고 판단되지만 소프트웨어적으로 에뮬레이션 시켜주는 프로그램도 존재하고 발전되는 컴퓨터 환경과 리버스 엔지니어링을 통하여 언젠가 하드웨어 인증방식 또한 우회하는데 시간이 소요되지만 불가능 하지는 않을 거라고 바라본다.

안티 리버스엔지니어링에는 수많은 방법들이 존재하고 계속 발전하고 있으며 이를 우회하는 방법 또한 계속적으로 발전되고 있다. 방지방법이 개발되면 이를 우회하는 방법 또한 언젠가 나오게 되어있다.

소프트웨어의 실행파일을 보호하기 위해 안티 리버스 엔지니어링 솔루션을 도입하기도 하는데 소프트웨어가 안전하게 보호가 되는 대신 단점도 존재한다.

안티 리버스 엔지니어링 솔루션을 우회하게 되면 해당 솔루션을 적용한 모든 소프트웨어가 우회되는 것을 뜻하며 해당 솔루션을 적용한 모든 실행파일의 원본파일을 얻을 수 있고 이를 이용하여 해당 소프트웨어의 인증 알고리즘, 취약점 등을 찾아 낼 수 있는 단점이 존재한다.

그렇다면 제일 안전한 방법은 무엇일까

그것은 안티 리버스 엔지니어링 솔루션에 의지하지 않고 소스코드 레벨에서 보안 코딩을 하는 것이며 모든 입,출력값에 대한 검증을 하고 예외처리를 확실하게 구현을 해야 한다. 특히 서버, 클라이언트 구조의 프로그램이면 서버에서 중요 입력 값들의 확실한 검증이 필요하다.

Ⅱ. 역분석의 유형

1. 파일 비교분석

파일 비교분석은 소프트웨어의 업데이트 또는 패치버전이 릴리즈 되었을 경우 업데이트 이전 파일과 이후 파일을 비교분석하여 어떤 부분이 바뀌었는지 확인이 필요할 경우에 쓰인다.

바뀐 부분이 확인되면 취약했던 코드와 이를 보완한 코드를 확인 할 수 있고 이를 응용하면 취약점에 대한 패치를 만들 수 있고 악용하면 악성코드도 만들 수 있다.

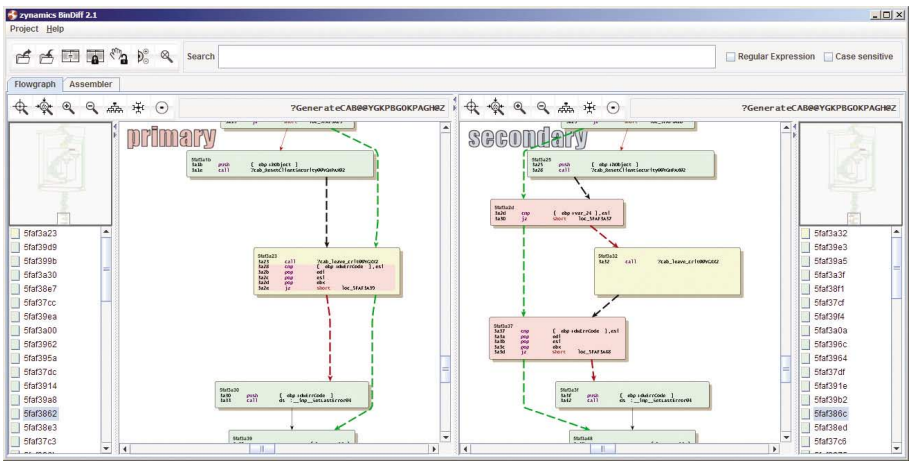
운영체제를 공격하는 대부분의 악성코드는 이런 취약점들을 악용하며 패치가 되어있지 않은 운영체제를 공격하도록 만들고 스스로 전파하도록 제작된다.

그래서 운영체제 및 소프트웨어 패치가 릴리즈 되었을 경우 바로 패치하는 것이 좋으며 안티바이러스 패턴 업데이트도 주기적으로 해주어야 한다.

프리웨어 프로그램으로는 다른그림[24], 상용 소프트웨어에는 BinDiff[25]가 유명하다.

다음은 BinDiff 프로그램을 이용하여 소프트웨어 패치 전의 원본파일과 패치 후의 변경된 파일을 비교한 화면이며 좌측이 패치 전, 우측이 패치 후의 모습이다. 변경되고 추가 또는 삭제된 코드들을 쉽게 확인 할 수 있으며 패치의 목적과 이유를 알 수 있다.

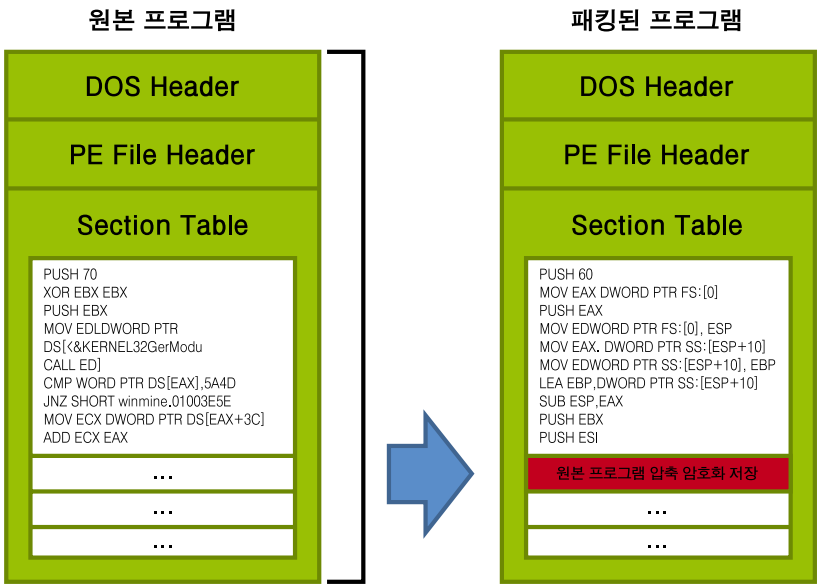
보통 입력값 체크를 하지 않았거나 잘못된 입/출력 알고리즘으로 발생되는 문제가 많으며 여러번 패치가 적용된 안전한 소프트웨어라고 할지라도 취약점이 존재 할 수도 있다.



24) 다른그림 : www.darungrim.org
25) BinDiff : www.zynamics.com/bindiff.html

2. 실행파일 언패킹

다음 그림과 같이 원본 프로그램은 패킹된 프로그램의 하나의 섹션 안에 존재하기 때문에 패킹된 프로그램을 디스어셈블러나 디버깅을 하게 되면 원본 프로그램을 분석하는 것이 아닌 패킹된 프로그램을 분석하게 되는 것이다. 그래서 패킹된 프로그램을 분석하려면 우선 언패킹(실행파일 압축해제)을 해야 한다.



패킹된 프로그램이 실행되면 패킹 프로그램의 알고리즘이 우선 시작되고 복호화, 압축 해제 알고리즘이 수행된 후 메모리에 원본 프로그램 실행코드가 저장되며 이 때 원본 프로그램이 메모리에서 실행하게 된다. 이 과정을 언패킹 이라고 하며 언패킹된 지점이 원본 프로그램의 시작점인 OEP[26]가 된다.

디버깅 프로그램을 이용하여 패킹된 프로그램의 알고리즘을 분석하고 동적으로 생성되는 메모리, 호출되는 API 등을 분석하여 OEP를 찾게 되면 메모리 덤프 과정을 거쳐 원본 프로그램을 파일로 저장을 하는데 이 과정이 언패킹이다.

유명한 패킹 프로그램일 경우 분석을 하는 사람이 그만큼 많고 분석이 어느정도 되어있기 때문에 전용 언패킹 프로그램도 만들어 배포하기도 한다. 그래서 유명한 패킹 프로그램을 이용하여 적용을 해도 소용이 없는 경우도 있다.

3. 악성코드 분석

90년대에 발견되었던 대부분의 컴퓨터 바이러스들은 파일을 손상시키고 전파하며 업무를 마비시키는 것을 주목적으로 만들어 졌지만 현재의 바이러스들은 사용자PC의 공인인증서, 주민등록번호, 카드번호, 중요파일들을 KeyLog[27], Bot[28] 등을 이용하여 개인정보, 온라인게임 계정정보, 금융거래 정보 등을 획득하고 이를 바탕으로 보이스 피싱[29], 자신의 PC가 공격자의 좀비PC[30]가 된지도 모른채 특정 웹사이트를 DoS[31] 공격을 하고, 획득한 개인정보 및 공인인증서, 패스워드를 이용하여 공격자의 계좌에 불법이체를 하는 공격 등의 사고로 이어지게 된다.

이런 사고들을 보았을 때 악성코드의 감염목적과 대상이 시대에 따라 바뀐다고 볼 수 있으며 앞으로도 사용자PC를 주 대상으로 발전 될 것이다.

사용자PC를 주로 공격하는 악성코드들에는 무엇이 있을까
- 신뢰되지 않은 사이트에서의 ActiveX 설치로 인한 해킹공격
- USB 메모리에 상주하는 악성코드로 인해 USB 메모리를 여러 PC에 사용할 때 마다 악성코드 전파
- P2P, 웹하드 또는 신뢰되지 않은 사이트에서의 파일 다운로드
- PDF, Word등의 문서파일을 열람할 때 문서파일 안에 존재하는 악성코드가 실행되어 중요정보 노출

이런 종류들이 있으며 안티바이러스, 운영체제 패치 미설치 등의 상대적으로 보안이 되어있지 않은 사용자PC가 주 공격대상이 된다.

최근 이슈가 되고 있는 악성코드들은 무엇이 있고 이런 악성코드들은 누가 어떤 방식으로 분석을 할까
- DoS 프로그램을 이용한 특정 사이트 서비스 거부 공격
- IRC Bot 악성코드를 이용한 사용자PC의 중요 데이터 파일 유출
- 악성코드가 포함된 문서파일
- 운영체제 취약점으로 인한 관리자 권한 획득

26) OEP : Original Entry Point, 원본 프로그램의 시작 지점
27) 키로깅 : 키보드로 입력한 값을 획득하는 것을 말하며 크래커에게 전달하거나 파일로 저장을 할 수도 있다.
28) Bot : 보통 IRC Bot을 말하며 감염이 되면 크래커가 원격으로 사용자PC를 조정할 수 있다.
29) 보이스 피싱 : 획득한 개인정보를 바탕으로 전화를 하여 사기를 치는 행위
30) 좀비PC : 악성코드에 감염이 된 PC를 말하며 악의적인 공격자가 조정을 하여 특정 사이트에 공격을 하도록 명령을 내릴 수도 있다.
31) DoS(Denial of Serivce) : 특정 서버에 엄청난 패킷을 보냄으로써 네트워크가 과부화 되어 사이트 접속을 차단시키는 공격을 말한다.

- 키로깅을 통한 게임 계정 유출
- 악성코드 치료 프로그램을 위장한 악성코드

일반적으로 국, 내외 안티바이러스 회사에서 샘플을 수집하거나 사용자가 신고한 의심이 가는 파일들을 분석하여 악성코드의 행동패턴과 감염경로를 분석하고 안티바이러스에서 탐지 되도록 패턴에 넣으면 사용자는 패턴 업데이트를 함으로써 악성코드가 탐지되고 치료가 된다.

평균적으로 하루에 15,000~20,000개의 샘플이 안티바이러스 회사에 접수되며 자체적으로 구축한 분석 프로그램에 의해 자동으로 패턴이 만들어 지며 이 과정에서 탐지가 되지 않은 샘플들은 악성코드 분석 전문가가 직접 수동으로 분석을 하여 패턴을 만들게 된다.

안티바이러스가 설치되어 있으면 안전할까

이에 대한 대답은 아쉽게도 그렇지 않다. 악성코드 탐지 벤치마킹에서 점수가 제일 높은 안티바이러스라고 할지라도 모든 악성코드를 탐지해내지는 못한다. 이는 제품의 성능이 떨어져서가 아니라 안티바이러스의 탐지기술이 발전되는 만큼 악성코드도 발전하기 때문이다.

안티바이러스의 패턴이 업데이트되기 전에는 악성코드에 무방비 상태이기 때문에 주기적인 패턴 업데이트와 주기적으로 운영체제 보안 업데이트를 해야 하며 웹하드, P2P, 신뢰할 수 없는 사이트에서의 파일 다운로드, ActiveX 설치는 되도록 피하는 것이 좋다.

4. 소프트웨어 취약점 점검

안전한 소프트웨어를 개발하려면 계발단계에서부터 보안상의 취약점이 발생되지 않도록 내부 개발보안정책 또는 가이드라인을 적용하여 개발해야 하지만 이 과정들은 그야말로 이상이며 현실적으로 볼 때 시간에 기거나 기타 다른 이유로 일정에 쫓겨 심각한 취약점이 내제된 소프트웨어가 개발 될 수 있다.

취약점의 존재를 떠나 프리웨어, 셰어웨어, 오픈소스 등의 소프트웨어들은 사용자가 사용하면서 취약점들을 발견하고 제작자에게 말하면 해당부분을 보완한 패치버전을 만들어서 재배포 한다.

만약 위험도 높은 취약점을 크래커[32]가 발견했을 경우 제로데이[33] 취약점이 되어 해당 소프트웨어를 사용 중인 사용자PC 또는 서버를 공격하여 권한 획득 및 중요정보를 획득하거나 범죄로 이어질 수도 있다. 이런 취약점들의 발생을 최소화하기 위해 소프트웨어 배포 전 취약점 점검을 하여 소프트웨어의 안전성을 확인해야 하며 점검의 종류로는 화이트박스, 블랙박스 점검이 있다.

32) 크래커 : 악의적인 공격자를 지칭

33) 제로데이 : 취약점이 있는 프로그램의 패치가 아직 발표되지 않은 상태를 가리키거나 당일 배포되는 불법 소프트웨어를 가리키기도 한다.

가. 화이트박스 점검

프로그램의 소스코드를 직접 보면서 프로그래밍의 오류와 잘못된 알고리즘의 구현, 버퍼 오버플로우, 포맷스트링 등의 취약점이 존재하는지 분석 하는 것을 말한다.

자동화된 소스코드 점검도구를 이용하기도 하지만 사용되지 않는 변수, 포인터의 잘못된 참조 등의 실제 취약점으로 분류되지 않는 항목들도 같이 분석되기 때문에 발견된 취약점들에 대해 점검자가 다시 분석을 해서 실제 취약점 유무를 확인해야 한다.

화이트박스 점검의 단점으로는 소스코드 상태에서 보이지 않는 실제 위협이 되는 취약점은 찾기가 힘들다.

나. 블랙박스 점검

소스코드가 없는 상태의 소프트웨어를 점검하는 것이며 구현된 기능들이 오류 없이 정상적으로 작동하는 것을 포함하여 구현된 모든 입, 출력 값을 테스트 하면서 소프트웨어의 동작 상태를 확인한다.

화이트 박스 점검에서 발견되지 않았던 취약점, 예외 상황 등을 찾을 수 있으며 디스어셈블러, 디컴파일러, 디버깅 등의 분석과정을 거치고 입력 값에 대한 네트워크, 프로세스, 파일 등의 다양한 분석을 통해 점검을 한다.

다양한 입, 출력 테스트를 위해 파일포멧, 네트워크, 프로토콜 등의 Fuzzer[34] 프로그램을 사용하기도 한다. 무작위로 값을 테스트 하는 것 이므로 실제 취약점을 찾는 경우는 드물지만 Fuzzer도 계속 발전해 나가기 때문에 성능도 많이 좋아지고 있다.

이런 블랙박스의 단점으로는 화이트박스 점검은 소스코드를 점검 하는 것이기 때문에 어디까지 분석이 되었는지 확인하기 쉽지만 블랙박스 점검은 어디까지 분석이 되었는지 확실하지 않기 때문에 소프트웨어가 전체적으로 모두 점검 되었는지 알 수 없는 단점이 있다.

그 외 점검방식으로는 화이트박스 점검과 블랙박스 점검을 조합하여 각 점검방식의 단점을 보완한 그레이박스 점검이 있다.

5. 소프트웨어 호환성

개발이 완료된 소프트웨어를 유지보수 해야 하지만 개발자가 퇴사하였거나 소스코드가 분실되었을 경우 리버스 엔지니어링을 이용하여 분석 및 개발이 가능하다. 이 과정에서 소프트웨어 복제

34) Fuzzer : 무작위로 입력 값을 테스트 하는 프로그램

가 일어나기 때문에 저작권 침해문제가 발생 되지만 이러한 경우에는 리버스 엔지니어링이 허용된다.[35] 그렇지만 모든 상황에서 허용되는 것은 아니다.

소프트웨어 호환성을 위한 개발을 할 때 중요한 점은 개발자는 원 소프트웨어 저작자에게 호환성과 관련된 정보를 획득하기 위한 노력을 해야 하며 호환에 필요한 정보를 못 얻었을 때는 불가피한 경우 리버스 엔지니어링이 허용된다. 또한 개발된 프로그램은 원 프로그램을 대체하는 것이 아닌 확장되고 특징적인 기능을 포함하고 있어야 하고 원 프로그램에 포함된 코드가 포함되어져 있지 않아야 한다.

참고로 A업체가 소프트웨어 호환성을 위해 시간과 노력을 들여 리버스 엔지니어링을 하여 얻은 자료를 제3자인 B업체가 정보를 요청할 경우 국내 현행법에서는 배포 할 수 없음을 규정하고 있다.[36]

소프트웨어 호환성 개발의 대표적인 소프트웨어로는 ReactOS[37]가 있으며 윈도우와 리눅스 운영체제의 호환성을 위해 1996년부터 지금까지 개발되고 있는 오픈소스 프로그램이고 소스가 공개되어 있지 않은 윈도우 운영체제를 리버스 엔지니어링 분석을 통해 윈도우 운영체제와 거의 흡사하게 만들었다는 것에 큰 의미가 있다.

ReactOS 목적 자체가 윈도우와 똑같은 운영체제를 만드는 것이 목적이 아닌 Win32 API 호환 운영체제를 만드는 것이기 때문에 윈도우와 비교했을 때 많은 부족함이 보일지 모르지만 공개되어 있지 않은 정보를 바탕으로 이 정도까지 호환되게 만든다는 것은 많은 어려움이 따랐을 것이다.

라이선스는 GNU General Public License (GPL)[38]을 적용하고 있으며 수많은 개발자가 참여하고 있고 업데이트 될 때마다 호환성 및 기능들이 많이 개선되고 있다.

35) 저작권법 제13조 제2항 각호, 제101조의3 제1항 제6호, 제101조의4에서 리버스엔지니어링 관련 규정을 두고 있음

36) 저작권법 제101조의4.

37) RectOS : www.reactos.org

38) GNU General Public License (GPL) : www.gnu.org/licenses/licenses.html

6. 기술적 보호조치 우회 검증

악의적인 리버스 엔지니어링을 통해 안티바이러스, 키보드보안 프로그램 등의 보안솔루션을 우회하고 소프트웨어에 구현된 기술적 보호조치 및 알고리즘을 우회하는 악성코드나 프로그램이 있을 경우 이런 우회 방법들을 검증하고 분석을 할 때에도 리버스 엔지니어링이 쓰인다.

해당 프로그램이 구현된 기술적 보호조치를 우회하고 무력화 했는지를 검증하여 컴퓨터프로그램보호법에 위배 되었는지 검증을 하며 이것을 통해 실제 소프트웨어의 취약점을 찾을 수도 있다.

대부분의 상용 소프트웨어의 Keygen[39], Crack[40] 등이 이에 속하며 온라인 게임일 경우 자동사냥 봇, 스피드 핵, 게임 리소스 추출, 논 클라이언트 제작 등 온라인 게임을 금전적, 정책적으로 위협하는 프로그램이 상당히 많으며 기술적 보호조치 우회를 검증하는 것과 법률적으로 해결해야 되는 사항이 많은 부분이다.

39)) KeyGen : 상용 소프트웨어의 라이선스 등록번호를 불법으로 생성하는 프로그램
40)) Crack : 기간제한 또는 일부 기능이 제한된 상용 소프트웨어를 무력화하여 제한이 없도록 하는 변조된 파일

7. 소프트웨어 불법 복제

가. 소프트웨어 인증 우회

소프트웨어의 인증 알고리즘을 우회하고 이를 배포하고 재판매하는 행위로 인한 손실은 해마다 증가하고 있다. 이를 방지하기 위한 다양한 안티 리버스 엔지니어링을 적용하고 방지대책을 세우지만 한계가 있다.

나. 경쟁회사의 소프트웨어 복제

경쟁회사에서 만든 소프트웨어를 개발하기 위해 리버스 엔지니어링을 통해 일부 코드를 복제하여 유사한 소프트웨어를 개발 및 판매하는 것은 저작권 침해행위에 해당된다. 이러한 사건이 발생될 경우 원 소프트웨어와 유사 소프트웨어의 코드를 비교 분석하여 코드를 복제했는지의 여부를 검증한다.

다. 라이선스를 무시한 소스코드 복제

소스코드가 공개된 소프트웨어의 경우 저작자가 정한 라이선스 정책을 무시하고 이를 무단 복제하여 사용할 경우에도 저작권 침해에 해당된다.

제3장 SW 역분석의 법적 이해

제 3장 SW 역분석의 법적 이해

정진근 교수(강원대 법학전문대학원)

Ⅰ. 저작권법상 SW 역분석 조항

1. SW 역분석의 의의

SW 역분석(software reverse analysis)이란 SW 역공정(software reverse engineering)이란 용어로 이용되기도 한다.[41] 이러한 견해는 대체로 타당한 것으로 평가된다. SW 역분석이란 용어는 우리나라만이 사용하고 있는 용어이기 때문이다. 이에 반해 미국과 일본은 역공정이란 용어를, 유럽연합은 역컴파일이란 용어를 쓰고 있다.

역공정이란 용어는 주로 공업분야에서 널리 이용되어 왔는데, 일반적으로 타사가 개발한 공업제품을 조사, 해석, 연구하여 그 안에 포함된 기술적 아이디어나 정보 또는 그 제품제조에 유익한 노하우 등을 제품으로부터 역 과정을 통하여 유출하는 것을 말한다.[42] 역공정은 공업제품을 분해하여 기술사상을 알아내는 것이 핵심이므로, 표현이 공개되어 있는 저작물에는 역공정이 필요하지 않았다. 즉, 저작권법은 아이디어가 아닌 표현을 보호하기 위한 법이기 때문에 표현은 이미 공개되어 있었고 표현으로부터 추출한 아이디어를 이용하는 것은 적법한 일이었다. 따라서 저작권법은 본질적으로 역공정을 금지하지 않고 있고, 역공정을 허용하기 위한 규정이 필요하지도 않았다.

그러나 컴퓨터프로그램은 목적프로그램(object code)이라는 형태로 유통되기 때문에 표현을 볼 수 없었고, 이와 같은 프로그램의 특징으로 인해 역공정이 필요하게 되었다. 이 때 컴퓨터프로그램의 목적프로그램과 대응되는 동등한 수준의 원시프로그램(source code)을 추출하기 위해서는 역어셈블이나 역컴파일을 통하는 방법이 이용되고 있다. 이러한 이유로 유럽연합의 "컴퓨터프로그램의 법적 보호에 관한 EU지침"에서는 역컴파일(decompilation)이란 용어를 이용하고 있다. 이 때 역컴파일(decomplilation)이란 목적프로그램을 원시프로그램으로 변환하는 그 방법 자체를 의미하는 용어이다.

41) SW 역분석을 SW 역공정과 동일시하는 국내의 견해는 안효질, "프로그램코드역분석 규정의 비교법적 분석", 창작과 권리(제47호), 2007; 김두환 · 문준우, "Reverse Engineering(역분석)에 대한 법적 고찰", 경영법률(제18권 제4호), 2008; 강기봉 · 정봉현, "컴퓨터프로그램보호법상 S/W 리버스 엔지니어링 규정에 관한 소고", 창작과 권리(제42호), 2006 등에서 쉽게 찾아볼 수 있다.

42) 中山信弘, ソフトウェアの法 的 保 護(新版), 127頁 (有斐閣, 昭63).

이에 반해 역공정 또는 역분석이란 용어는 목적프로그램을 역컴파일, 실행, 조사하는 행위로부터 원시프로그램을 추출하여 분석하는 일련의 과정을 의미한다.

2. 저작권법의 역분석의 정의

저작권법 제2조 제34호는 역분석을 "프로그램코드역분석"이란 용어로 새롭게 정의하고 있다. 이 정의 규정에 따르면 "프로그램코드역분석"은 독립적으로 창작된 컴퓨터프로그램저작물과 다른 컴퓨터프로그램과의 호환에 필요한 정보를 얻기 위하여 컴퓨터프로그램저작물코드를 복제 또는 변환하는 것을 말한다.

이 규정에 따르면 프로그램코드역분석이 되기 위해서는 두 가지 요건을 만족시켜야 할 것인데, 첫째는 호환에 필요한 정보를 얻기 위한 행위이어야 하며 둘째로 컴퓨터프로그램저작물코드를 복제 또는 변환하는 행위이어야 한다.

이 중 첫째 요건은 행위의 목적이므로 주관적 요건인데 반해, 둘째 요건이 행위의 태양을 의미하는 요건으로서 객관적 요건에 해당한다. 일반적인 역공정 또는 역분석이란 용어는 둘째 요건인 객관적 요건과 부합한다. 이러한 정의는 EU 지침에서와 같은 것인데, 객관적 요건에 대해 EU 지침 제6조는 프로그램코드의 복제(reproduction)와 형태의 변환(translation)을 의미한다고 규정한다. 우리 규정과 다른 점은 EU 지침이 복제와 변환을 앤드(and) 요건으로 기술하고 있는데 반해, 우리 규정은 복제와 변환을 오어(or) 요건으로 기술하고 있다는 점이다.

일반적으로 역분석은 원시프로그램으로의 변환과 변환된 프로그램의 복제에 의해 이루어진다는 점을 고려할 때, EU 지침과 같은 앤드(and) 요건으로 기술하는 것이 바람직해 보인다.

뿐만 아니라 첫째 요건으로 기술되고 있는 행위의 목적으로서의 주관적 요건이 프로그램코드역분석의 정의의 요건으로서 적합한지에 대해서도 의문의 여지가 있다. 일반적으로 정의조항은 객관적 행위 또는 성질을 기술하고 있는 것인데 반해, 프로그램코드역분석은 주관적 요건을 요구함으로써 행위자의 주관적 의사에 따라 프로그램코드역분석에 해당될 수도 있고 그렇지 않을 수도 있기 때문이다. 이에 대해서는 호환성 확보 외의 정보를 얻을 목적으로 프로그램코드를 복제 및 변환하는 행위가 프로그램코드역분석에 해당하지 않게 되는 불합리한 결과가 도출될 수 있으며, 행위자의 주관적 의사를 입증하는 것은 소송법적으로 용이하지 아니할 것이므로 저작권법의 정의 규정은 재검토할 필요가 있다.

어쨌든, 일반적인 프로그램코드역분석은 디컴파일, 실행, 조사하는 행위로부터 원시프로그램을 추출하여 분석하는 일련의 과정으로 이해되는데 반해, 우리 저작권법상의 프로그램코드역분석이

란 이 중 호환성 확보를 위한 목적으로 디컴파일 또는 디어셈블리의 방법을 통해 목적프로그램에서 원시프로그램 또는 어셈블리어 등 인간이 인식가능한 코드를 추출하는 행위를 의미하는 것으로 이해된다. 이러한 점을 고려할 때, 프로그램코드 역분석을 허용하는 제101조의4 규정을 종합적으로 고려할 때, 프로그램역분석의 정의 중 호환성 확보의 목적이라는 주관적 요건은 프로그램역분석 과정 중에 발생하는 저작권 침해 주장에 대해 저작권을 제한하기 위한 요건으로 이해된다.

3. SW 역분석에 관한 저작권법의 규정

가. 역분석 규정을 적용하기 위한 요건

저작권법 제101조의4는 프로그램역분석에 관하여 규정하고 있다. 이 규정은 컴퓨터프로그램보호법과 저작권법이 통합하기 전에는 프로그램보호법 제12조의2에 있던 규정이다.

본 규정은 프로그램코드역분석을 할 수 있는 허용범위를 정하고 있는데, 이 규정에 의하면 프로그램코드역분석을 할 수 있는 요건은 다음과 같다.

우선 역분석을 하기 위한 전제 조건은 다음과 같다.

첫째, 역분석을 할 수 있는 자는 정당한 권원에 의하여 프로그램을 사용하는 자 또는 그의 허락을 받은 자에 한한다.

둘째, 역분석을 하려는 자는 호환에 필요한 정보를 쉽게 얻을 수 없을 뿐만 아니라 호환성의 획득이 불가피한 경우에만 역분석을 할 수 있다.

셋째, 당해 프로그램의 호환에 필요한 부분에 한하여 허락 없이 역분석을 할 수 있다.

다음으로 역분석을 통하여 얻은 정보는 다음 사항에 따라 이용이 제한된다.

첫째, 호환 목적 외의 다른 목적을 위하여 이용하거나 제3자에게 제공해서는 아니된다.

둘째, 역분석 대상 프로그램과 실질적으로 유사한 프로그램을 개발, 제작, 판매하거나 기타의 프로그램저작권을 침해하는 행위에 이용하여서는 아니된다.

나. 역분석 규정의 법적 성격

역분석 조항의 법적 지위에 대해서는 역분석조항을 강행규정으로 보아 부정하는 견해, 계약자유원칙을 인정하면서 독점규제법에 위반한다고 보아 부정하는 견해, 역분석 금지 특약의 내용에 따라 판단해야 한다는 절충적 견해와 계약자유가 역분석 조항에 우선한다는 긍정설로 나누어볼 수 있다.

첫째, 역분석조항을 강행규정으로 보아 부정하는 견해에 따르면 컴퓨터 산업발전의 생명이라고 할 수 있는 호환성 있는 프로그램의 개발을 제도적으로 보장하는 강행규정에 속하며, 법조항의 구조도 제101조의3[43]의 자유이용에 연결되어 있다는 점을 생각할 때 계약으로 파기할 수 없는 성질

을 가진다는 것이다. 이에 대해서는 어떤 법률규정이 강행규정이 되기 위해서는 이 점을 법률에 명시하는 것이 통례인데, 한국 법에서는 이 점에 관한 규정이 없어 옳지 않다고 비판하는 견해가 있다.[44] 그러나 모든 강행규정을 법률에 명시한다고 보기는 힘들기 때문에 강행규정인지의 여부는 입법자의 입법의도와 학설 및 판례를 통해 좀 더 논의가 필요할 것으로 생각된다.

둘째, 계약자유원칙을 인정하면서 독점규제법에 위반한다고 보아 부정하는 견해[45]에 따르면, 역분석을 금지하는 특약은 계약자유의 원칙에서 볼 때 원칙적으로 허용될 수 있는 것이긴 하지만, 역분석의 제한은 경쟁을 크게 저해하는 것이고, 이와 같은 조항은 독점금지법에서 규정하는 불공정한 거래방법(독점규제법 제19조, 제2조 제9항)에 해당한다고 본다. 이 견해에 의하면 역분석에 의해 복제가 일어나더라도 저작권 침해는 되지 않는다고 보는데, 그 이유로는 ①역분석은 기술발전에 필수적인 것이며 끊임없는 기술혁신의 원천이므로 이를 적극적으로 인정할 필요가 있다. ②역분석을 금지하는 것은 저작권보호의 대상 밖인 아이디어의 독점을 사실상 인정하는 것이 된다. ③기술성이 강한 프로그램 저작물과 특허의 대상인 발명 사이에서 후자에서 허용되는 역분석이 전자에서는 인정되지 않는 것은 해석의 합리성이 없다. ④역분석을 금지하면 동종의 기능을 가진 경쟁 프로그램의 개발이 크게 저해된다. ⑤저작권법의 보호대상이 아닌 인터페이스나 프로토콜 또는 바이오스(BIOS) 등에 대하여 역분석이 금지되면 당해 기종을 이용한 다른 프로그램이나 다른 기종과의 접속이 되지 않아 호환기의 개발을 불가능하게 한다는 점을 들고 있으며, 이에 따라 저작권법에서 볼 때 이와 같은 범위까지 보호할 필요는 없다고 본다.

또한, 포장형 사용허락계약의 효력에 대해서는 의문이 많을 뿐만 아니라 프로그램의 구매자가 역분석을 못하도록 금지하는 내용의 계약은 부당한 모방, 무임승차 방지의 범위를 넘는 것이며, 독점규제법의 관점에서 보아도 특약의 내용은 공정한 경쟁질서를 저해하는 것이 되어 저작권의 권리행사로 인정할 수 없고 구속조건부 계약으로서 위법무효라고 한다.

43) 컴퓨터프로그램보호법에서는 제12조가 자유이용 규정이었으며, 프로그램코드역분석은 제12조의2로 규정하고 있었다.

44) 김동진, "컴퓨터 프로그램 코드의 역분석", CLIS Monthly(2003-11호), KISDI, 2003, 13쪽.

45) 이혜광, 전게논문, 114쪽 이하; 정상조, "Reverse engineering의 법적 문제점", 인권과 정의(제254호), available at http://jus.snu.ac.kr/~sjjong/classroom/thesis/jungsj042.htm.

46) 김동진, "컴퓨터 프로그램 코드의 역분석", CLIS Monthly(2003-11호), KISDI, 2003, 13-14쪽.

셋째, 역분석 금지 특약의 내용에 따라 판단해야 한다는 절충적 견해[46]에 따르면 역분석 금지특약이 있다고 하여 곧바로 강행규정 위반이나 독점규제법상 불공정거래가 된다고 단정할 수는 없고, 계약을 이루고 있는 구체적인 약정사항, 역분석 금지에 대하여 특별한 대가가 있는지, 계약을 축으로 한 전체적인 이해관계 등을 종합적으로 고려하여 위 법규정 소정의 구속조건부 계약인지 여부에 대하여 신중히 판단하여야 할 것이라고 한다. 또한 이 견해는 역분석조항이 임의규정이라고 하더라도 일반시장형 사용허락계약에서 정한 역분석 금지 특약은 약관 내용의 부당성 심사의 대상이 되는 것이고, 이 판단은 사업자의 이익과 고객의 이익을 종합적으로 비교 형량하여 판단하여야 하고, 나아가 컴퓨터프로그램보호법에서 최소한의 범위에서 허용한 프로그램 코드 역분석을 사업자가 약관으로 금지하는 것은 그와 같은 금지의 대가로 고객에게 특별한 대가를 부여하는 등 특단의 사정이 없는 이상 고객에게 부당하게 불리한 약관조항으로 해석될 수 있다고 본다.

넷째, 계약자유가 역분석 조항에 우선한다는 긍정설은 문언 그대로 역분석 조항은 임의 규정에 불과하므로, 계약에 의해 제한할 수 있으며, 계약은 역분석 조항에 우선하여 적용된다는 견해이다.

이와 같은 견해 중에서 다수의 학자들은 강행규정설을 지지하는 것으로 생각된다.[47]

Ⅱ. SW 역분석에 대한 법적 재해석

1. 문제의 소재

앞서 살펴본 바와 같이 프로그램코드역분석은 프로그램저작권의 제한을 규정한 저작권법 제101조의3에 뒤이어 제101조의4로 규정하고 있다. 이와 같은 구조는 컴퓨터프로그램보호법의 태도를 그대로 이어받은 것이다. 컴퓨터프로그램보호법은 제12조에서 프로그램저작재산권을 제한하고, 제12조의2에서 프로그램코드역분석을 규정하고 있었다.

프로그램코드역분석이 프로그램저작권을 제한하는 규정이라는 점은 프로그램코드역분석의 조문을 통해서도 쉽게 알 수 있다. 프로그램코드역분석 규정은 일정한 조건에 한해 프로그램코드역분석을 할 수 있다고 규정함으로써, 일정한 조건 하에서 프로그램저작권이 제한되고 있음을 간접적으로 명시하고 있기 때문이다.

47) 자세한 사항은 정진근, "프로그램코드역분석에 관한 비교법적 고찰", 비교사법(제13권 2호(통권 33호)), 2006, 545쪽 이하 참조; 강행규정설을 지지하는 견해로는 김두환 · 문준우, 앞의 글 및 강기봉 · 정봉현, 앞의 글 참조.

이러한 규정은 프로그램코드역분석이 프로그램저작권을 침해하고 있다는 점을 전제로 하는 것이다. 즉, 프로그램코드역분석은 필연적으로 역분석의 과정에서 프로그램을 복제, 변환하는 과정이 존재하게 되므로, 이러한 행위로 인해 발생한 복제권 및 개작권(또는 번역권)을 침해할 가능성이 있다. 이에 대해서는 원시프로그램과 역분석에 의해 추출한 프로그램 간에 실질적 유사성이 인정되므로 복제가 이루어지며, 변환에 의한 번역권 침해는 이루어지지 않는다는 견해가 유력하다.[48] 일본에서도 마이크로소프트사의 프로그램을 역어셈블한 사건에서 역어셈블은 기계적 변환에 불과하므로 창작성이 가미되지 않았으므로 원시프로그램과 변환된 프로그램 간에는 실질적 유사성이 인정되므로 복제권 침해를 인정한 바 있다.[49]

그렇다면 프로그램코드역분석은 제101조의4가 전제하는 바와 같이 저작권 침해를 반드시 수반하는가? 그리고 제101조의4에서 규정한 요건을 충족하지 않는 프로그램코드역분석은 프로그램저작권을 반드시 침해하는가? 이에 대한 검토가 필요할 것으로 생각된다.

2. 프로그램코드역분석의 침해영역

프로그램코드역분석의 침해를 판단하는데 있어 일반적으로 혼동하는 것 중 대표적인 것은 프로그램코드역분석과 기술적보호조치무력화를 구별하지 않는 것이다. 물론, 프로그램코드를 역분석하기 위해서는 기술적보호조치를 무력화해야 하는 경우가 일반적이다. 그러나 기술적보호조치무력화는 그 자체가 간접침해에 해당되므로, 프로그램코드역분석이 없더라도 침해에 대한 구제가 가능하다. 따라서 프로그램코드역분석의 권리침해영역을 판단하기 위해서는 프로그램코드를 역분석하는 행위 영역에 한정하여 고찰해야 할 것이다.

이러한 태도는 미국 저작권법에서도 발견할 수 있다. 미국의 판례는 프로그램코드역분석을 공정사용의 원칙에 따라 판단하고 있는 한편, 미국은 1998년의 새천년저작권법(The Digital Millennium Copyright Act: DMCA)을 통해 연방저작권법 제117조의 일부 조항을 개정하고, 연방저작권법에 저작권보호와 관리시스템(copyright protection and management systems)이라는 별도의 장을 신설함으로써, 역공정(reverse engineering)을 기술적 보호조치를 회피할 수 있는 예외의 하나로 인정하고 있다.

48) 정진근, "프로그램코드역분석에 관한 비교법적 고찰", 비교사법(제13권 2호(통권 33호)), 2006, 528쪽.
49) 東京地判昭和62年1月30日判示1219号.

제1201조 (f)를 보면 컴퓨터프로그램의 복제본을 사용할 권리를 적법하게 취득한 자는 독립적으로 창작된 컴퓨터프로그램과 다른 프로그램의 호환성 달성에 필요하고, 종전에 쉽게 이용할 수 없었던 프로그램의 요소를 확인, 분석하기 위한 목적으로만 그리고 그와 같은 확인, 분석이 이 법에 의하여 권리침해가 되지 않는 한도 내에서 프로그램의 특정부분의 접근을 효과적으로 통제하는 기술적 보호조치를 회피할 수 있다고 규정한다. 이 규정은 일반적 역공정 규정이 아니라 역공정에 의해 기술적 보호조치의 회피 가능성만을 규정한 것이므로 적용의 한계를 갖는다는 점에서 우리법의 태도와 다른 것이다.

일반적으로 프로그램코드역분석은 기술적보호장치가 해제되어 있는 목적프로그램을 역컴파일 또는 역어셈블이라는 행위를 통해 목적프로그램과 대응되는 원시프로그램을 추출하는 행위이다. 이 때 추출된 원시프로그램은 목적프로그램의 원래의 원시프로그램과는 표현이 매우 상이한 것이 일반적이나, 이들 원시프로그램 간에는 실질적 유사성이 인정되고 있다. 따라서 프로그램코드역분석으로 인한 침해의 영역은 무단으로 원시프로그램을 추출하는 행위가 아니라, 추출된 원시프로그램을 무단으로 복제하는데 있다.

복제된 원시프로그램은 개작, 아이디어만의 습득, 호환성을 갖는 연계프로그램의 창작에 이용되는가 하면, 이용하지 않고 방치 또는 폐기될 수도 있다. 이 중 아이디어만의 습득은 별도의 저작권 침해를 수반하지는 않는다. 이용하지 않고 방치 또는 폐기될 경우에도 동일하게 저작권 침해를 수반하지는 않는다. 그러나 원시프로그램을 임의로 개작하여 동일성 유지권을 침해하거나 2차적저작물작성권을 침해하는 경우에는 추가적인 저작권 침해가 발생할 수 있다. 호환성을 갖는 연계프로그램의 창작에 이용하는 경우에도 저작권 침해가 발생할 소지가 있으나, 이 때에는 제101조의4를 적용함으로써 저작권 침해주장을 제한할 수 있을 것이다.

이상과 같은 분석에 따르면 프로그램코드역분석으로 인한 침해영역은 다음과 같이 정리된다.

첫째, 목적프로그램에서 원시프로그램을 역컴파일 또는 역어셈블의 방법에 의해 추출하여 저장하는 행위는 복제권 침해에 해당될 수 있다.

둘째, 추출된 원시프로그램을 호환성 확보 외의 목적으로 개작한 경우 동일성유지권 또는 2차적저작물작성권 침해에 해당될 수 있다.

셋째, 추출된 원시프로그램을 이용하여 아이디어를 습득하던지, 방치 또는 폐기하던지, 또는 호환성을 갖는 연계프로그램을 창작하는 경우에는 추가적인 침해를 발생시키지 아니한다.

3. 저작권법 제101조의3 제1항 제6호 규정과 프로그램코드역분석

저작권법 제101조의4에서 규정한 컴퓨터프로그램코드역분석 규정과 제101조의3 제1항 제6호에서 규정하고 있는 일반적인 역공정 규정과의 관계도 의문의 여지가 있다. 제101조의3 제1항 제6호는 "정당한 권한에 의하여 프로그램을 이용하는 자가 해당 프로그램을 이용 중인 때에 한하여, 프로그램의 기초를 이루는 아이디어 및 원리를 확인하기 위하여 프로그램의 기능을 조사, 연구, 시험할 목적으로 복제하는 경우, 프로그램저작재산권을 제한한다"는 취지를 규정하고 있기 때문이다.

본 규정에서 정한 프로그램역공정의 방법은 역컴파일이나 역어셈블에 한정되어 있지 아니하므로, 다양한 방법에 의한 역공정을 허용한다. 다만, 본 규정에 의한 역공정은 프로그램의 기능에 관한 아이디어를 얻는데 그친다는 한계가 있다.

이러한 점을 감안할 때, 제101조의4는 제101조의3 제1항 제6호의 특별규정으로 이해하는 것이 자연스러운 해석일 것으로 생각한다.

즉, 제101조의3 제1항 제6호는 일반적인 프로그램역공정 규정으로서, 아이디어를 습득하기 위하여 프로그램저작권을 침해하는 경우에 저작재산권을 제한하는 규정으로서의 성격을 갖는다. 이때 습득된 아이디어를 이용하는데 그치지 않고 실질적으로 유사한 프로그램 또는 개작프로그램을 만드는 행위는 허용되지 아니한다.

다만, 제101조의4 프로그램코드역분석 규정에 따라 호환성 확보에 필요한 범위 내에서는 프로그램의 개작을 허용한다.

이러한 전제 위에서 판단할 때, 프로그램코드역분석에 의한 프로그램저작권 침해영역은 다시 다음과 같이 정리된다.

첫째, 목적프로그램에서 원시프로그램을 역컴파일 또는 역어셈블의 방법에 의해 추출하여 저장하는 행위는 복제권 침해에 해당될 수 있으나, 프로그램의 기능을 조사, 연구, 시험할 목적인 경우 즉 아이디어만을 확보하는 경우에는 제101조의3 제1항 제6호에 따라 저작재산권이 제한된다.

둘째, 추출된 원시프로그램을 호환성 확보의 목적으로 개작한 경우 제101조의4에 의거하여 동일성유지권 또는 2차적저작물작성권 침해에 해당되지 아니한다.

따라서, 프로그램역분석에 의하여 프로그램저작권이 침해되는 경우는 역분석에 의하여 추출된 원시프로그램을 이용하여 호환성 확보 외의 목적으로 프로그램을 개작하는 때에만 발생한다.

이와 관련하여 일본의 일부 학설은 우리 저작권법 제101조의3 제1항 제6호가 없더라도 아이디어를 습득하기 위한 역공정은 여전히 저작권을 침해하지 않는다고까지 주장한다. 이 견해는 특허법의 규정을 유추적용하는 것이다. 일본 특허법 제69조는 특허발명을 시험연구할 목적에서 실시하는 것에 대해서는 특허권 침해에 해당하지 않는다는 규정을 가지고 있는데, 이 제도는 특허제도에 내재되어

있는 공공적인 관점으로부터의 제한을 정한 것이어서 일종의 공서양속으로 보아야 하고, 이에 따라 이 규정은 독점금지법 이전의 문제로서 강행규정이므로, 이에 반한 역공정 금지계약조항은 무효라고 설명하면서, 이러한 논리구조를 저작권에도 그대로 적용할 수 있을지에 대해 조심스럽게 긍정한다.[50]

생각건대, 저작권법은 표현을 보호하고 아이디어는 보호하지 않는다는 점과 호환성확보는 컴퓨터정보재를 이용하는데 불가피하다는 점을 고려할 때, 이와 같이 역분석을 최대한 자유롭게 할 수 있도록 해석하는 것이 바람직할 것으로 생각된다.

Ⅲ. SW 역분석 관련 국내외 판례

1. 개요

프로그램코드역분석은 컴퓨터프로그램산업계의 주요 이슈로 인식되고 있다. 특히, 호환성 확보를 위한 연구는 물론 해킹에 대한 백신프로그램의 개발 등 특수 분야에 있어서 프로그램코드역분석의 필요성이 널리 인식되고 있다. 그럼에도 불구하고 구 컴퓨터프로그램보호법 제12조의2와 현행 저작권법 제101조의4 규정에 대해 관련 업계종사자들은 사실상 프로그램코드역분석이 불가능한 것으로 인식되어 있는 실정이다.

이러한 상황에 따라 프로그램코드역분석과 관련된 판례는 발견하기 어렵다. 다만, 소수의 판례를 통해 프로그램코드역분석이 복제권을 침해한다는 판례와 프로그램코드역분석을 제한하는 계약의 유효성과 관련된 판례를 찾아볼 수 있다.

2. 프로그램코드역분석이 복제권을 침해한다는 판례

가. 프로그램코드역분석이 복제권 침해에 해당된다는 일본의 판례

일본에서는 피고가 마이크로소프트사의 베이직 인터프리터 목적프로그램을 16진수의 코드로 치환한 후, 역어셈블하여 라벨과 코멘트를 더하여 해설서를 출한한 사건이 이었다. 이에 대해 법원은 "양 저작물의 차이가 대부분 라벨표시의 차이에 불과하다"고 하여 복제권침해를 인정하였다.[51]

이 판결에서 법원은 마이크로소프트사의 프로그램을 역어셈블한 행위가 기계적 변환에 불과하여 창작성이 가미되지 않았다는 이유로 번역권이 아닌 복제권 침해를 인정한 것이다. 결국, 컴파일

50) 大澤恒夫, IT事業競爭法 –獨禁法 · 知的財産法 · 消費者契約法今日的課題–, 76-77頁 (日本評論社, 2001) 참조.
51) 東京地判昭和62年1月30日判示1219号.

러 또는 역컴파일러에 의한 기계적 치환에는 인간의 정신활동인 창작성이 가미될 여지가 없으므로, 역어셈블한 변환프로그램과 원시프로그램 간에는 실질적 유사성(substantial similarity)이 인정된다는 것이다.

이 사건에서는 역어셈블에 의한 복제권 침해가 공정사용에 해당하는지에 대해서는 판단하고 있지 아니하다.

나. 프로그램코드역분석이 공정사용에 해당될 가능성에 관한 미국의 판례[52]

미국에서 지금까지 나온 판례 중에서 역공정에 대한 지도적 판례로 드는 것이 Sega Enterprises Ltd. v. Accolade, Inc. 사건[53], Atari Games Corp. v. Nintendo of America Inc. 사건[54] 그리고 DSC v. DGI사건[55]이다. 이 사건들에서 법원은 역공정이 공정사용에 해당하느냐와 관련하여 목적프로그램을 역공정하는 것이 ①프로그램에 내재된 사상(idea)이나 기능적 요소(functional elements)에 접근할 수 있는 유일한 방법이고, ②복제를 하는 자가 이러한 접근에 대해 정당한 이유가 있다면, 저작물의 공정사용에 해당한다고 판단하였다. 이때도 저작권법 제107조에서 열거한 네 가지 요건을 만족하여야 한다.

역공정이 저작권법 제107조에서 규정한 공정사용 요건에 해당하는지에 대해서 판례는 첫째, 이용의 목적과 성질에 대해서 임시적인 중간복제는 상업적 중요성이 최소한도에 그칠 뿐만 아니라 역공정에 의한 호환성 증대로 인하여 일반 공중의 이익이 증가되고 있다는 점에서 상업적 복제도 공정사용에 해당된다고 하고, 둘째 잠재적인 시장이나 가치에 미치는 영향에 대해서도 역공정된 프로그램과 역공정에 의해 새로 창작된 프로그램이 실질적으로 유사하지 않은 이상 대체재로 볼 수 없을 뿐만 아니라 저작권에 의해 경쟁이 불가능해져서는 아니된다는 취지에서 공정사용에 해당된다고 하고, 셋째 컴퓨터프로그램의 특징을 볼 때 목적프로그램을 역공정할 수 없다면 프로그램 저작자는 프로그램의 기능적 면에 대해 사실상 독점권을 행사하게 되어 불합리하며, 넷째 역공정의 대상이 저작물 전체일지라도 최종적인 사용에 저작물 전체가 이용되지 않았으므로 중요하지 않다고 하면서 최종적으로 공정사용에 해당된다고 판시하였다.

이 판결에서 중요한 정책적 고려사항은 만일 역공정이 공정사용에 해당되지 않아 불법적인 행위라면 Sega사에게 아이디어와 기능적 개념에 대한 사실상의 독점(de facto monopoly)을 허용하는 것이고, 그러한 독점권을 얻기 위해서는 특허법적 보호방법을 찾아볼 필요가 있다고 판단한 데

52) 정진근, "프로그램코드역분석에 관한 비교법적 고찰", 비교사법(제13권 2호(통권 33호)), 2006, 531-532쪽.
53) 977 F.2d 1510 (9th Cir. 1992).
54) 975 F.2d 832 (Fed. Cir. 1992).
55) DSC Communications Corp. v. DGI Techs., 81 F3d 597 (5th Cir. 1996).

있다.[56] Altari 사건에는 역공정을 공정사용으로 인정하면서도, 피고가 저작권국을 기망하고 원시 프로그램을 입수하였다는 특수한 사정이 있었으므로, '깨끗한 손의 원칙(clean hand doctrine)'에 의하여 공정사용의 원칙이 적용되지 않았다.[57]

역공정이 적법하다는 근거가 되는 공정사용의 원칙이란 형평법(equitable rule of reason)으로부터 발전하여 온 것인데, 이러한 이유로 공정사용인지를 판단하기 위한 제107조의 요건은 배타적인 요건이 아니므로, 법원은 공정사용으로 볼 것인지에 대해서 각 사건에 따라(case by case) 판단해야 한다. 이 때 공정사용의 원칙을 인용하는 궁극적인 정당성은 당연히 "과학기술과 유용한 예술의 진보를 촉진하려는" 저작권법의 목적으로부터 나온다고 한다.[58]

뿐만 아니라 Sony Computer Entertainment, Inc. v. Connectix Corp. 사건[59]에서 미국법원은 리버스 엔지니어링 과정에서의 중간복제는 창조적 변형이 아닌 비보호요소와 보호요소를 모두 포함한 단순한 복제에 불과했지만, 법원은 보호요소를 포함한 복제가 이루어지는 것이 리버스 엔지니어링에 반드시 필요한 것으로서 공정이용을 인정했는데, 이는 호환성을 목적으로 한 리버스 엔지니어링의 필요성에 대한 요구가 정책적으로 너무나 강하기 때문에 변형적 성격을 띤 창작 활동을 가능케 해주는 필수적 역할을 해오고 있는 중간복제를 통한 저작권 침해가 정당화된다고 본다.[60]

이상과 같이, 미국 법원은 공정사용의 원칙(fair use doctrine)[61]을 통해 역공정을 허용하고 있다. 따라서 공정사용에 의하여 허용되는 역공정은 유럽연합과 같이 일정한 허용범위나 원리를 정한 명시적 규정으로 존재하는 것은 아니며, 법원의 판례에 따라서 결정된다고 할 수 있다.

다. 프로그램역분석을 제한하는 계약의 유효성을 인정한 미국의 판례

역공정의 법적 지위와 관련하여 중요한 판례 중 하나가 미국의 Bowers v. Baystate Technologies, Inc. 사건[62]이다. 이 사건에서 Bowers는 CAD(Computer Aided Design) 소프트웨어를 위한 템플릿(template)을 개발하여 1990년 미국에서 특허 등록을 받았으며, Bowers는 자신의 템플릿을 Cadkey사의 CAD 프로그램인 CADKEY tool과 함께 묶어 판매하는 배급계약을

56) Pamela Samuelson & Suzanne Scotchmer, The law & economics of reverse engineering, Yale Law Journal (April 2002) at 33.

57) 椙山敬士, 著作権・特許権, 31頁 (日本評論社, 1999).

58) Seungwoo Son, supra note 8, at 79.

59) 203 F.3d 596 (9th Cir. 2000).

60) 강기봉 · 정봉현, "컴퓨터프로그램보호법상 S/W 리버스 엔지니어링 규정에 관한 소고", 창작과 권리(제42호), 2006, 82쪽; 손승우 · 임길환, "소프트웨어 Reverse Engineering의 침해와 공정이용", IT관련법제도연구, 프로그램심의조정위원회, 2004, 84 · 85쪽.

61) 17 U.S.C.A §107. Limitation on exclusive rights: fair use

62) 320 F.3d 1317 (Fed.Cir.(Mass.) 2003); 320 F.3d 1316, 65 U.S.P.Q.2d 1746 (Fed.Cir. 2003).

Cadkey사와 체결하였다. Baystate사는 이 CADKEY tool을 구입하여 Bowers의 제품특징들을 통합한 템플릿과 소프트웨어를 개발하였는데, 이 과정에서 Baystate사는 CADKEY 제품 안에 있던 역공정을 금지하는 포장형 사용허락계약의 내용을 위반하였다는 것이다.

이에 대해 Bowers는 Baystate사를 대상으로 특허권 침해, 저작권 침해, 계약 위반으로 소송을 제기하였으며, 연방항소법원은 이 중에서 계약위반과 저작권침해를 인정하였다.

법원의 판결은 여러 가지 이슈(issue)들을 논하고 있으나 이 중 역공정의 법적지위와 관련하여 중요한 점은 "저작권법이 계약에 의한 역공정 제한내용에 우선하거나 범위를 좁히지 않는다"고 판시한 점이다.

이 판결은 계약에 의해, 그것도 포장형(shrink wrap)과 같은 일반시장형 사용허락(mass market license)계약에 의해 일방적으로, 역분석을 허용하는 연방법과 공정사용의 원칙이 제한될 수 있는지에 대해 우려를 낳게 되었다.

이번 판결의 의미를 평가하기 위하여, 첫째로 Bowers 판결이 "연방법이 주의 계약법에 우선한다"는 영미법의 일반원칙의 변경을 의미하는 지와, 둘째로 계약에 의해 공정사용마저 제한될 수 있는지의 문제로 나누어 살펴보기로 한다.

첫째 문제와 관련하여, Baystate사는 저작권법이 역공정을 금지하는 Bowers의 포장형 사용허락계약의 내용에 우선한다고 주장하였으나, 법원은 이를 부정하면서 계약자유의 원칙의 중요성을 강조하면서 계약의 내용은 쉽게 배제되지 않는다는 점을 강조한 후, 그럼에도 불구하고 연방의 규범은 경우에 따라 사적 계약내용에 우선될 수 있다고 판시하였다.

생각건대, 이 문제와 관련하여 법원은 모든 연방법이 계약의 내용에 우선하는 것은 아니나 연방법의 목적에 따라 우선 적용되는지의 여부를 판단하여야 한다는 일반원칙을 설명한 것으로 보인다.

이러한 원칙을 이번 사건에 적용할 경우 저작권법에 일반적 역공정을 허용하는 규정이 없고, 단지 호환성 확보를 위한 기술보호조치 우회만을 허용할 뿐이므로 연방법이 계약내용에 의해 배제되거나 저작권법의 목적이 형해화 되었다고 볼 여지도 없으므로 법원의 판단은 "계약의 내용이 연방법인 저작권법의 어느 특정 조항을 위반하고 있지 않으므로, 연방법이 계약의 내용에 우선될 여지가 없다"고 이해하는 것이 옳다.

둘째 문제와 관련하여 법원은 "이번 결정을 함에 있어, 법원은 역공정이 저작권을 침해하는 예외로서 Atari Games v. Nintendo 사건에서와 같은 공정사용에 간주될 것인지에 대해 결론을 유보한다"고 하고, "컴퓨터프로그램에 내재된 보호되지 않는 사상을 알아내기 위한 목적프로그램의

역공정은 공정사용에 해당한다"는 설시를 하고 있으므로, 이번 판결이 공정사용을 무조건 배제하는 것으로 보는 것은 옳지 않다.

또한, 이번 사례의 역공정이 공정사용의 요건에 해당되는지 살펴보더라도 Baystate사는 경쟁사이고, 이를 이용하여 경쟁제품인 템플릿과 소프트웨어를 개발하였다는 점, 이러한 행위가 시장에 미치는 영향이 작지 않다는 점과 함께 기업 간 거래에 의해 계약조건에 대한 협상이 일방적으로 불리하였다고 볼 근거가 없다는 점 등을 고려할 때, 형평법적 원칙을 기반으로 한 공정사용의 원칙이 형해화 되었다고 볼 근거는 없다.

따라서 이번 판결은 공정사용을 형평법적 견지에서 바라보는 미국의 법원칙상 그리 놀랄만한 판결로 보이지는 않는다. 즉 미국의 법원의 판단은 공정사용의 원칙이라는 잣대를 들이대기 위해서는 그것이 저작권법적 목적에 적합한지를 음미하여야 하고, 이 때 공정사용은 형평법적 원리에서 도출된 것이므로 각 당사자 간의 계약내용을 살펴서 공정사용의 강제 여부를 판단하여야 한다는 것으로 이해된다. 이러한 이유로 Alcatel USA v. DGI Technologies, Inc., 사건[63]에서 법원은 사용허락계약의 내용으로 역공정을 금지하는 조항이 특허권이나 저작권에 의해 보호되지 않는 시스템의 부분에 대해 독점을 야기하는 때에 한해 저작권 남용으로 보아야 한다고 한 바 있으며, DSC Communications Corp. v. Pulse communications, Inc., 사건[64]에서도 공정사용의 원칙에 따른 역공정 조항은 그 원리가 형평법적 개념(equitable concepts)에 기반하고 있기 때문에 역공정을 배제하는 계약의 내용에 의해 영향을 받게 된다고 판단하였다.

따라서 Bowers v. Baystate Technologies, Inc. 사건도 계약에 의해 형평법적 원칙이 침해되었는지의 견지에서 판단하여야 하는데, 이 사건에서 법원은 형평이 깨지지 않았다고 판단하여 계약의 유효성을 지지하는 것으로 이해해야 할 것이다.

그러나 계약의 내용이 양 당사자의 지위를 현저하게 불공정하게 만들지 않더라도, 만일 연방저작권법이 역공정에 대해 광범위하고 명확한 규정을 가지고 있거나, 앞에서 살펴본 바와 같이 UCITA in 2002의 채택으로 인해 역공정을 금지하지 못 하도록 계약법의 수정이 이루어진다면, 역공정을 제한하는 계약자유원칙에 따른 계약내용은 연방법 또는 주 계약법에 의해 효력이 부정될 수 있을 것이다.[65]

63) 166 F.3d 772, 49 U.S.P.Q.d (BNA) 1641 (5th Cir. 1999).

64) 170 F.3d 1354, 50 U.S.P.Q.2d (BNA) 1001 (Fed. Cir. 1999).

65) 본 사건에 관한 자세한 사항은 정진근, "프로그램코드역분석에 관한 비교법적 고찰", 비교사법(제13권 2호(통권 33호)), 2006, 534쪽 이하 참조.

Ⅳ. 한 · 미 FTA 이행법안 검토

1. 한 · 미 FTA의 프로그램코드 역분석 조항

한 · 미 FTA 제18.4조 제7호 라목에서는 프로그램역분석에 관하여 규정하고 있다. 그러나 제7호는 원칙적으로 기술적보호조치의 무력화에 관한 규정으로서 라목은 기술적보호조치의 우회에 관한 예외 및 제한에 관하여 프로그램역분석을 규정하고 있다.

제7호는 "저작자 · 실연자 및 음반제작자가 자신의 권리 행사와 관련하여 사용하고 그의 저작물 · 실연 및 음반과 관련한 허락받지 아니한 행위를 제한하는 효과적인 기술조치의 우회에 대하여 충분한 법적 보호와 효과적인 법적 구제를 제공하기 위하여, 각 당사국은 구제에 대하여 책임이 있고 그 적용대상이 되도록 규정한다"고 한 후, 동호 라목에서 "독립적으로 창작된 컴퓨터프로그램의 다른 프로그램과의 호환성을 얻는 목적으로만 비침해 리버스 엔지니어링 행위에 관여한 인에게 쉽게 이용가능하지 아니하였던 컴퓨터프로그램의 특정요소에 대하여 선의로 수행된, 적법하게 획득된 컴퓨터프로그램에 대한 비침해 리버스 엔지니어링 행위", "복제물, 고정되지 아니한 실연, 또는 저작물 · 실연 또는 음반의 현시물을 적법하게 획득하였고 선의의 비침해 행위에 대한 허락을 얻기 위하여 선의의노력을 하였고, 적절한 자격을 갖춘 연구자에 의하여 정보의 스크램블 및 디스크램블을 위한 기술의 흠결 및 취약성을 확인하고 분석하는 것으로 구성된 연구 목적을 위하여서만 필요한 한도에서 수행된 선의의 비침해 행위", "부적절한 온라인 콘텐츠에 미성년자가 접근하는 것을 방지하는 것을 유일한 목적으로, 그 자체로 금지되지 아니하는 기술, 상품, 서비스 또는 장치에 구성요소나 부품을 포함하는 것" 등을 기술적보호조치의 구제 행위에 대한 예외 및 제한 행위로 규정하고 있다.

이러한 태도는 미국 새천년저작권법 제1201조 (f)와 유사한 것이다.

2. 우리 저작권법 규정과 한 · 미 FTA 규정의 비교

한 · 미 FTA 규정과 미국 저작권법의 규정 및 판례는 다음과 같이 설명될 수 있다.

첫째, 프로그램코드역분석은 공정사용의 원칙에 따라 허용될 수 있는 행위이다. 이 과정에서 발생하는 중간적인 복제는 역분석에 반드시 필요한 것으로서 공정이용에 해당된다.

둘째, 역분석의 과정에 기술적보호조치의 우회, 무력화 또는 회피가 발생한 경우에는 프로그램의 복제본을 적법하게 취득한 자일 것, 호환성 목적 달성에 필요할 것 등의 일정 요건에 따라 기술적보호조치의 무력화에 대한 구제가 제한된다는 것이다.

이는 우리 저작권법이 기술적보호조치와 프로그램코드역분석을 서로 독립적으로 규정하고 있는 것과는 다른 태도이다.

이러한 점을 고려할 때, 우리 저작권법은 미국의 저작권법 및 판례, 그리고 한 · 미 FTA에서 규정하고 있는 것보다 더 광범위하게 프로그램코드역분석을 제한하고 있다고 평가할 수 있다.

따라서 프로그램코드역분석 그 자체는 좀 더 넓게 허용하고, 기술적보호조치를 무력화를 수반하는 프로그램코드역분석에 한해 엄격한 요건을 충족시키는 방향으로의 개선이 필요한 것으로 생각된다.

제4장 기술적보호조치의 기술적 이해

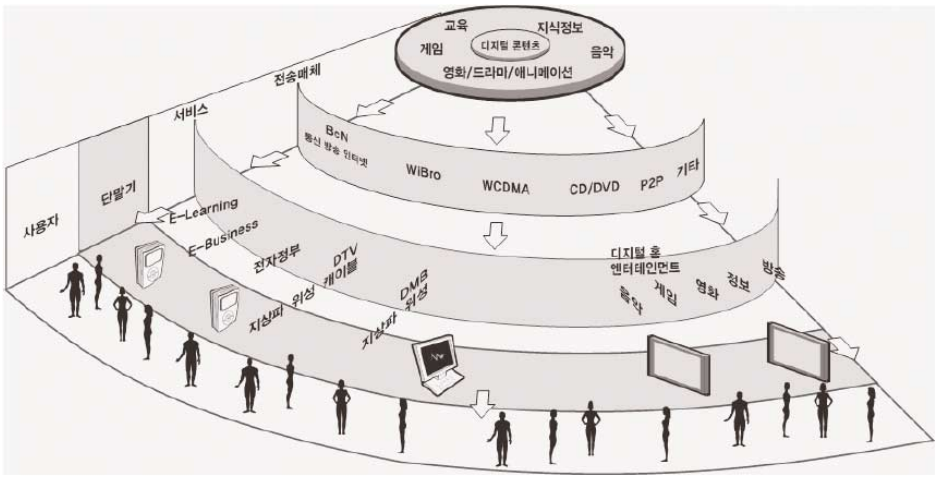


제4장 기술적보호조치의 기술적 이해

김석훈 팀장(저작권보호센터)

Ⅰ. 기술적보호조치의 의의

콘텐츠 산업의 성장과 함께 저작권 보호를 위한 기술적보호조치의 중요성은 더욱 증가하고 있다. 기술적보호조치란 저작권을 보호하기 위하여 멀티미디어, 문서 등의 디지털화된 저작물의 불법 복제를 방지하고 지정된 사용자에게 허가된 범위 내에서 사용할 수 있게 하는 기술로서 콘텐츠 유통산업의 성장에 핵심이 되는 기술이라고 할 수 있다. 또한, 콘텐츠 중심의 산업구조 발전은 세계적인 추세이며, 이러한 추세 속에서 기술적보호조치의 중요성은 점점 커지고 있다.



그러나 P2P, Web Hard 서비스를 이용한 사용자들의 무분별한 콘텐츠 불법 공유 등의 사례는 디지털 콘텐츠 산업의 장기적인 정체만이 아니라 기존의 오프라인 및 아날로그 콘텐츠 산업의 존립 기반마저 위협하고 있는 실정이다. 이에 따라 단순한 법적인 규제만으로 디지털 콘텐츠의 불법복제 문제를 통제하는 것이 아니라 DRM 등의 보다 능동적인 저작권 보호기술 및 디지털 핑거프린팅, 워터마킹 , 콘텐츠 인식 및 추적 기술 등이 요구되고 실제 산업 환경에서 적용되고 있는 상황이다.

인터넷과 방송, 모바일 등 다양한 형태로 서비스 될 디지털 콘텐츠의 유통 인프라 구축 및 유통 활성화를 위해서는 기술적보호조치의 표준화가 필수적이며, 비표준화로 인해 발생하는 기술적, 제도적 산업 환경의 불확실성을 증가시키기 때문에 디지털 콘텐츠 산업 자체의 성장에도 악영향을 미침. 때문에 상호호환성을 보장할 수 있는 기술적보호조치의 개발 및 보급노력이 무엇보다 중요하다.

기술적보호조치의 가장 핵심이 되는 DRM 기술의 표준화가 급속하게 이루어지고 있는 모바일 분야와 차세대 디지털케이블 방송분야 등 특정 산업군을 대표하는 업체들에 대한 여타 회사들의 지지도가 높게 나타나고 있는 것을 보면 알 수 있다.

저작권자를 보호하고, 투명하고 상호 호환성 있는 유통 환경을 제공하여 콘텐츠 유료화 및 콘텐츠 유통을 활성화를 위한 기술적보호조치는 다양한 응용(음악, 게임, 모바일, 전자책 등)에 DRM 체계를 확산시켜 일관성 있는 콘텐츠 유통 서비스 체계를 구축하는 기반이 되며 디지털 디바이스, 콘텐츠 저장매체 산업, 전달 매체 산업, 정보 단말기 산업 등 관련 산업의 발전 촉진에 기여한다는 의의가 있다.

Ⅱ. 기술적보호조치의 유형

1. 디지털 저작물 확인 · 증명

최근 디지털 신호는 오디오, 비디오, 정지 영상 등에서 아날로그 신호를 대체하고 있다. 아날로그 신호는 원래의 신호를 정확하게 표현할 수 있다는 장점이 있는 반면, 미세한 잡음에도 쉽게 영향을 받아 원래의 신호가 변경되기가 쉽다는 단점을 지니고 있다. 이에 반해 디지털 신호는 잡음에 대해서 강인할 뿐만 아니라 복제 후에도 원본과 완전히 동일한 신호를 갖는 특성을 지니고 있다. 그러나 복제된 신호가 원본과 동일하기 때문에 불법적으로 복제된 복사본들이 원본의 가치를 떨어뜨리고 지적 재산권(Intellectual Property Right, IPR)을 침해할 수 있다는 특성 또한 지니고 있다. 디지털로 저장, 전송되는 비중이 커지면서 디지털 저작물에 대한 저작권(copyright) 보호는 중요한 문제로 현재 제기되고 있다. 이를 위한 효율적인 보호방법으로 디지털 워터마킹과 같은 은닉된 저작권 정보에 의해서 저작권을 확인하고 증명하는 기술이 사용되고 있다.

저작권 확인 · 증명의 가장 대표적인 기술을 디지털 워터마킹이라 할 수 있는데 디지털 워터마킹의 과정은 워터마크의 생성, 삽입(embedding), 검출(decoding)의 세 가지 과정으로 이루어져 있다. 워터마크의 생성은 삽입하고자 하는 정보를 생성자만이 알고 있는 비밀키에 의해 변조하여 사용하

는데 m-sequence[66], Gaussian random sequence 등이 많이 사용되고 있다. 초기연구에는 생성된 워터마크를 주로 인간 지각에 잘 띄지 않는 고주파 영역이나 디지털 데이터에서 덜 중요한 부분에 삽입하였으나 워터마크 삽입된 데이터가 전송 과정에서 부호화 방법, 디지털/아날로그-아날로그/디지털 변환, 기하학적 또는 시간 축 변형, 신호 처리 등의 여러 과정을 거치기 때문에 저작권 확인 및 증명을 위한 강인한 워터마킹의 경우 이러한 과정 후에도 삽입된 워터마크가 살아남도록 디지털 데이터의 중요 부분에 워터마크를 삽입하는 방법이 사용되고 있다. 삽입된 워터마크(watermark)는 디지털 신호 파일 뒤에 첨가되는(append) 것이 아니라 파일의 내용 안에 뒤섞이게 되며, 따라서 원래 파일보다 크기가 늘어나지는 않는다는 특징을 가지고 있다. 입력 단계에서는 가능한 삽입된 워터마크를 복잡하게 삽입하여 이를 지우려는 의도에도 강하게 해야 한다. 삽입된 저작권 정보는 검출 소프트웨어로 다시 추출이 가능하여야 하며, 때로는 특별한 키(key)가 추가로 필요하다.

삽입 및 검출 일련의 과정은 통신 시스템에 비유되어 설명되기도 하는데, 저작권 정보를 입력 신호에, 워터마크가 삽입될 저작물 신호를 통신 채널에, 그리고, 예측하지 못한 공격이나 신호처리 과정은 추가 잡음으로 각각 비유된다. 따라서 채널 정보량(capacity)은 얼마나 많은 양의 워터마크를 원 저작물 신호를 손상시키지 않고 삽입할 수 있는지에 비유될 수 있을 것이다.

이밖에도 원 신호를 사용하는 경우와 사용하지 않는 경우의 고려, 안전성을 위한 키의 고려 등 여러 요건들이 필요하며 이들 요건들은 서로 상충되는 성질을 가지고 있는 경우가 많아서 디지털 워터마킹을 사용하는 활용 경우에 따라 적절한 조절이 필요하다.

보통 워터마킹은 DRM[67] 기술과 함께 사용되거나, 일부에서는 DRM 시스템의 한 부분으로 보기도 한다. 즉, 암호화를 이용한 DRM 기술은 디지털 저작물의 유통 과정에 있어서 주로 사전 제어의 역할을 담당하며 단독으로는 저작물 보호에 한계가 있기 때문에 워터마킹을 이용한 사후 관리 기능을 함께 사용하여 전체 시스템의 안전성을 향상시킬 수 있다. 예를 들어, 실수나 공격에 의해 암호화가 풀린 저작물을 얻게 되는 경우, 무차별적인 복사가 가능하며 복사된 저작물은 원본과 구별할 수 없기 때문에 더 이상 디지털 저작물의 소유권은 보호받을 수 없다. 그러나, 워터마크는 디지털 저작물 자체에 삽입되는 정보로써 이를 이용하여 불법적으로 유통되는 저작물의 저작권을 지속적으로 확인 및 증명해 줄 수 있으며, 유통 경로를 워터마크 정보로 가지고 있는 경우에는 불법 복사의 경로 추적 및 유통 사후 관리에 사용될 수 있다. 이밖에도 디지털 워터마킹은 디지털 신호의 원본의 진위 및 무결성 확인, 광역 모니터링, 인증, 복사 방지 등의 활용에 사용되기도 한다.

66) M-sequence는 최대장계열 또는 최대주기열로 불린다. M-sequence는 간단한 규칙에 의해 만들어지는 확정적 계열이지만, 외관상은 불규칙한 계열로 보인다. 그리고 통신이나 암호 의 분야에서도, 그 규칙성을 모르는 사람에게 있어서는 암호가 되어, 규칙성을 아는 사람에게만 의미가 있는 부호가 된다.

67) 웹을 통해 유통되는 각종 디지털 콘텐츠의 안전 분배와 불법 복제 방지를 위한 보호 방식. 파일 교환 프로그램을 통해 전파되는 상업적 자료의 온라인 불법 복제로부터 디지털 콘텐츠를 보호하기 위한 것으로, 관련 법령이나 위반자 단속으로는 예방이 어렵기 때문에 사후 단속 보다 사전에 문제점을 파악해 첫 단계에서 내용 복제를 못하도록 한 것이다. 이 보호 방식을 적용한 제품들은 서버 소프트웨어와 사용자 플러그인 운용에 필요한 패키지 제품들이 대부분이다.

2. 디지털 저작물 위 · 변조 방지

디지털 저작물의 불법적인 위조나 변조를 검사하여 무결성을 증명하는 기술이다. 디지털 저작물 위변조 방지를 위하여 다양한 기술 방식이 존재한다. 이러한 위변조 방지 기술 방식에는 Built-in 방식 · Plug-in 삽입 방식 · OLE 제어 방식 · File System Filter 제어 방식 · VBA 제어 방식 등이 존재한다.

가. Built-in 방식

초기의 DRM 제품은 DRM Controller를 전용뷰어에 built-in 방식으로 내장하는 방식을 사용하였다. 따라서 built-in 방식으로 응용 프로그램에 DRM Controller를 내장하기 위해선 응용 프로그램의 소스 변경이 불가피하게 요구되는데, DRM업체로선 저작물 포맷별로 응용 애플리케이션의 개발이 용이하지 않을 뿐만 아니라 상용 뷰어 제공업체의 협력을 끌어내기가 어렵기 때문에 지원하는 저작물 포맷에 한계가 있을 수 밖에 없다. 또한 어렵게 전용뷰어를 개발한다고 하더라도 이미 상용화된 애플리케이션 정도의 품질을 제공하지 못하기 때문에 최근에는 전용뷰어 방식을 거의 사용하지 않고 있다.

나. Plug-in 삽입 방식

Acrobat Reader, WinAmp와 같은 일부 애플리케이션들은 3rd party들의 의도에 맞게끔 커스터마이징 할 수 있도록 plug-in ADK를 제공하고 있다. DRM 벤더들은 이러한 애플리케이션 제공업체가 제공하는 plug-in ADK를 이용하여 DRM Controller를 개발하고, 이를 애플리케이션에 plug-in 형태로 제공함으로써 사용권한에 따른 애플리케이션 제어를 하게 된다.

다. OLE 제어 방식

MS Office, AutoCAD, 훈민정음, 아래한글2002 등과 같이 Active Document Server를 지원하는 애플리케이션들은 OLE 인터페이스를 이용하여 애플리케이션을 제어할 수 있다. OLE는 Microsoft의 Windows 플랫폼에서 응용 프로그램간 정보의 전송 및 공유를 가능케 하는 기술로, DRM Controller는 OLE를 통해 Active Document Sever의 각종 기능들을 통제할 수 있게 된다.

라. API Hooking 제어 방식

API hooking 제어 방식은 응용 프로그램에서 사용하는 커널 레벨의 system API를 hooking하여 DRM Controller에서 애플리케이션의 기능을 통제하는 방식이다. 이 방식은 사용권한의 통제가 system API 레벨에서 통제가 이루어지기 때문에 애플리케이션을 수정할 필요가 없을 뿐만 아니라 모든 애플리케이션에 범용적으로 적용이 가능하다.

마. File System Filter 제어 방식

File System Filter 제어 방식은 File System Filter를 이용하여 파일시스템의 I/O를 hooking 하여 암/복호화 처리를 수행하는 방식이다. 이 방식은 암/복호화 처리가 커널 레벨의 File System Filter를 통해 이루어지기 때문에 모든 애플리케이션에 범용적으로 적용이 가능하다.

바. VBA 제어 방식

VBA(Visual Basic for Applications)는 애플리케이션의 신속한 커스터마이징과 통합을 위해 Microsoft에서 제공하는 개발툴이다. VBA를 지원하는 애플리케이션은 VBA IDE를 통해 그 애플리케이션을 제어할 수 있기 때문에 DRM Controller와 연동이 가능하게 된다. VBA를 이용한 애플리케이션은 구현이 간단하기 때문에 쉽게 적용할 수 있지만 불법 사용자가 개발한 VBA 코드 삽입을 통해서 저작물의 임의 조작이 가능하기 때문에 보안성이 떨어지는 취약점을 안고 있다.

3. 핑거프린팅

디지털 저작물의 사용자 정보를 핑거프린팅 데이터로 삽입하여 유통함으로써, 불법 복제/배포자를 추적하는 기술이다. 현재까지의 핑거프린팅 기술은 워터마킹 기술을 바탕으로 위에서 언급한 공모공격에 강인하도록 연구가 진행되어 왔지만 아직까지는 초보적인 단계이다. 핑거프린팅 기술은 크게 대칭성과 익명성을 지원하는 암호학적 기법과 Malvar 등에 의해 제안된 듀얼(dual) 워터마킹/핑거프린팅 기법, 삽입코드 자체를 공모공격이 불가능하도록 설계하는 공모보안코드(collusion secure code) 개발 기법 등으로 나누어진다.

암호학을 이용한 핑거프린팅 기술은 판매자와 구매자 사이에서 향후 불법저작물에서 구매자 추적을 어떻게 할 것인가에 초점을 둔 암호프로토콜을 의미하며 저작물을 판매하는 판매자가 핑거프린팅된 저작물을 접근할 수 있는지 없는지에 따라 대칭형과 비대칭형으로 구분된다. 암호학적 방식을 이용한 핑거프린팅 기술은 주로 핑거프린팅의 비대칭성과 익명성을 효율적으로 충족시킨다.

대칭형 핑거프린팅은 초기의 연구기법으로 핑거프린팅 프로토콜, 구매자 판별 프로토콜의 두 가지 알고리듬과 구매기록을 위한 데이터베이스로 구성된다. 앞의 두 알고리듬은 모두 판매자에 의해 수행되므로 판매자가 핑거프린팅된 저작물을 생성할 수 있다. 먼저 핑거프린팅 할 저작물과 구매한 사용자의 식별자, 현재까지 판매된 리스트를 입력으로 하여 핑거프린팅을 수행한다. 그에 대한 결과물로 핑거프린팅된 저작물과 구매레코드가 생성된다. 만약 핑거프린팅된 저작물이 어떤 구매자에 의해서 불법 복제되고 배포되었다면 판매자는 발견된 복사본과 핑거프린팅 되기 전의 저작물, 그리고 구매기록을 입력으로 발견된 복사본의 원구매자를 찾아내게 된다. 하지만 이 방법의 문제점은 판매자와 구매자 모두 핑거프린팅된 저작물을 접근할 수 있으므로 불법 복제되어 유통된

저작물이 발견된 경우 이를 유통시킨 주체가 구매자인지 혹은 판매자인지를 판단하기가 모호하다. 따라서 책임 규명이 분명치 않다는 문제점을 갖는다.

대칭형 핑거프린팅 방식의 문제점을 보완하기 위하여 비대칭형 핑거프린팅 방식이 제안되었다. 이 방식은 판매자와 구매자가 2-party 프로토콜에 참여함으로써 구매자만이 핑거프린팅된 저작물을 접근할 수 있도록 한다. 이는 판매자가 불법 복사된 저작물을 찾은 후에 불법배포자의 잘못을 신뢰된 제3자를 통하여 증명함으로써 책임 규명을 분명히 한다.

4. 공격 · 평가

디지털 저작물 보호기술의 강인성 및 안정성을 확인할 수 있는 공격기법과 평가기법으로 구분할 수 있다.

1995년 최초로 디지털워터마킹이라는 개념이 소개된 이후 이러한 기술을 이용하여 저작권자 확인, 불법유통 추적, 방송 모니터링, 접근 제어 등 다양한 응용분야에의 활용가능성이 제기되어 실제로 점차 많은 분야에서 저작권자의 권리를 보호하기 위하여 사용되고 있다. 그러나 이와 동시에 이러한 기술을 무력화시키는 기술들도 또한 다양한 방법으로 제기되고 있다. 디지털워터마킹 기술을 개발하는 연구기관이나 개인들이 이러한 기술을 이용하여 디지털워터마킹 기술을 무력화시키는 기술을 선보이기도 한다. 또한 보다 심오한 이론연구를 위하여 디지털워터마크를 제거하거나 검출이 불가능하게 하는 연구들을 수행하고 있다. 현재 정지영상, 동영상, 오디오등의 매체에 대한 저작권을 보호하기 위한 기술들이 가장 활발하게 연구되고 활용되고 있으며 공격기술도 역시 이러한 매체에 집중되고 있다.

5. 디지털 저작물 패키징

디지털 저작물 및 저작권을 보호할 수 있는 형태로 구성하는 기술, DRM용 저작물 제작 기술로 정의한다.

Pre-packaging은 사용자의 요청이 있기 전에 미리 저작물을 Secure Container로 패키징하는 방식을 말한다. 이렇게 미리 패키징된 Secure Container는 특정 사용자와 무관하게 패키징되기 때문에 동시에 많은 사용자가 저작물을 이용하더라도 패키징의 부하 부담을 피할 수 있게 된다.

Pre-packaging은 EDMS[68], KMS[69], Groupware[70] 등에 문서가 저장되기 전에 패키징함으로써 사용자의 요청이 있기 전에 미리 저작물을 Secure Container로 패키징하는 방식이다. 이렇게 미리 패키징된 Secure Container는 특정 사용자와 무관하게 패키징되기 때문에 동시에 많은 사용자가 저작물을 이용하더라도 패키징의 부하 부담을 피할 수 있게 된다. 그러나 이 방식으로 패키징된 지식정보들은 암호화되어 있기 때문에 기존 index 서버와의 연동이 어렵다는 제약점을 안고 있다.

On-the-fly packaging은 사용자의 요청에 의해 다이나믹하게 저작물을 생성해서 배포해야 되는 저작물을 패키징 할 때 사용하는 방식이다. 이 방식은 동시 사용자가 많을 경우에 암호화로 인해 시스템의 부하가 급속하게 증가하고, 결국 이로 인해 전체적인 시스템의 성능을 현격하게 떨어뜨리는 현상을 야기하게 된다. 따라서 이 방식을 이용해서 저작물을 패키징하기 위해서는 사용자의 증가에 따른 시스템의 부하 부담을 최소화 할 수 있는 기술적 구조를 우선적으로 고려해서 시스템을 구현되어야 한다.

6. 라이선스 처리

라이선스는 저작물의 이용에 대한 권한을 담고 있는 정보 단위로, 저작물에 대한 사용 권한을 부여하기 위해 사용된다. DRM에서의 라이선스 처리는 [그림 3]과 같은 프로세스를 통해 처리되어진다.

저작물의 이용을 위해선 사용규칙 및 조건을 포함하고 있는 라이선스가 필요하다. 라이선스가 사용자의 PC에 존재하고 있으면 사용자는 저작물을 바로 이용할 수 있도록 한다. 만일 사용자의 PC에 라이선스가 없다면 저작물 제공업자의 시스템으로 라이선스 발급을 요청하게 된다. 라이선스 발급 요청 시 사용자가 이용할 저작물의 식별번호와 사용자 정보 등이 저작물 제공업자의 시스템으로 전달된다. 저작물 제공업자의 시스템은 사용자로부터 전송된 정보를 이용하여 라이선스 발급 여부를 결정하게 된다. 만일 라이선스 발급요청을 한 사용자가 이미 해당 저작물에 대한 권한을 획득한 것으로 확인되면 새로운 라이선스를 발급하도록 한다.

유료 저작물인 경우, 저작물 제공업자는 저작물의 가격 및 이용 조건 등 저작물의 판매 정보를 사용자에게 제시하고 이를 수락하는 사용자에게 라이선스 발급을 허락한다. 저작물 제공업자는 허

68) EDMS(Electronic Document Management System)는 업무의 효율화 등을 위해 다양한 형태의 문서와 자료를 그 생성부터 폐기에 이르기까지 전체 생명 주기에 걸쳐 일관성 있게 전자적으로 통합 관리하기 위한 시스템. 각종 전자 문서의 등록, 저장, 관리, 송수신, 조회 등을 지원하는 시스템이다.

69) KMS(Knowledge Management System)는 조직이나 기업의 인적 자원이 축적하고 있는 개별적인 지식을 체계화하여 공유함으로써 경쟁력을 향상시키기 위한 기업 정보 시스템. 기업이나 조직의 지식을 이용하기 쉽게 축적하여 해당 지식을 기업의 전략이나 정책 수립, 의사 결정에 사용할 수 있도록 적절한 시간에, 적절한 사람에게, 적절한 지식을 제공하기 위한 시스템을 말한다.

70) 여러 사람이 함께 쓸 수 있는 소프트웨어. 집단으로서의 작업을 지원하기 위해 만들어진 소프트웨어라는 의미에서 그룹웨어라고 한다.

가된 사용자에 한하여 적절한 사용권리 정보를 담고 있는 라이선스를 발급하게 된다. 라이선스에 포함되는 사용권리 정보는 사용권한(permission)과 사용조건(condition), 그리고 암호화된 저작물을 풀어볼 수 있는 암호화 키 정보 등이 포함되어 있다. 사용권한은 view/play, print, edit, extract, embed 등과 같은 저작물의 사용권한을 제어하는 정보를 담고 있으며, 사용조건은 저작물의 이용 회수 및 이용기간 등의 정보가 담겨지게 된다.

7. 유통 메타데이터 처리

유럽을 중심으로 한 저작권 단체들이 주도하는 디지털 저작물의 메타데이터 표준화 작업은 저작물정보, 저작자 정보, 저작권자 정보, 권리운용 정보로 구별하여 저작물의 메타데이터를 정의하였다. INDECS는 DOI를 지원하며, 현재 표준화 작업 중인 MPEG-21은 DOI와 INDECS를 모두 수용할 것으로 보인다.

디지털 저작물 유통을 위한 메타데이터 요소는 크게 지불관리, 저작권관리, 저작물 유통보호, 저작물 관리용 메타데이터로 구분할 수 있다.

- 지불관리용 메타데이터 : 다양한 지불 방식을 제공하며 정확한 정산이 이루어져야 한다.
- 저작권관리용 메타데이터 : 저작권의 등록, 관리 및 검색 서비스를 제공하여 유통업자와 저작권자간 계약이 이루어져야 한다.
- 유통보호용 메타데이터 : 저작물이 불법으로 복사되어 사용되는 것을 통제하며 저작권자가 인지하지 못하는 사용에 있어서도 지불 처리가 가능해야 한다.
- 저작물 관리용 메타데이터 : 저작권 관리로부터 받은 계약 사항에 의하여 저작물과 정보를 안전하게 저작권자로부터 수집하고 유통업자에게 전달되어야 한다.

아래 표는 디지털 저작물 유통에 필요한 메타데이터를 범주에 맞게 카테고리화한 것이다.

〈표 2〉 디지털 제작물 유통에 필요한 메타데이터

범주	카테고리
지불관리	Mall 정보, Program사 정보, 수수료, 관리자, 결제내역, 정산내역, 신용카드 결제내역, 휴대폰 결제내역, 700 결제내역, 계좌이체 결제내역, 사이버패스 결제내역, 무통장입금 결제내역
저작권관리	사용자정보, 계약정보, 관리정보, 생성문서정보, 시스템I/F 정보, 저작물 장르, 저작물 분류, Set, 시리즈물, 저작물제목, 버전에디션, 저자, 키워드정보, 제작물 컴퍼넌트, 제작사정보, 제작, 용적, 자원링크
유통보호	사용자정보, 계약정보-유통업체, 구매사용정책, 계약인증정보, 계약인증사용자정보
저작물 관리	저작물정보, 저작물수집관련정보, 저작물 유통관련정보, 사용자정보

8. 디지털 저작물 식별체계

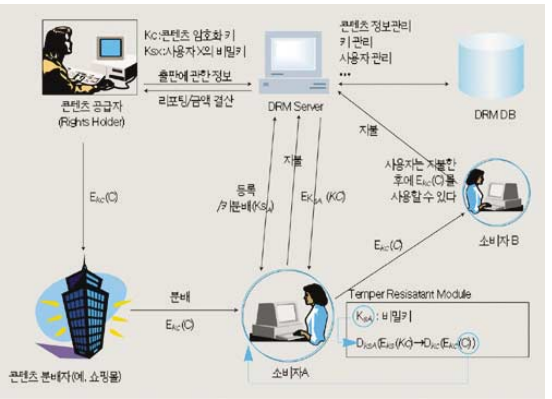
인터넷을 통한 디지털 저작물 유통이 활성화되면서 다양한 분야에서 식별체계에 대한 관심과 연구들이 진행되고 있다. 식별체계란 물류의 유통현황, 통계 등의 목적으로 또는 특정분야인 도서출판, 음악, 방송(미디어), 이미지 등에서 활용성과 개념들이 적용되어왔다. 일반적으로 식별체계를 구성하기 위해서는 식별체계 코드체계인 구문구조(Syntax Structure)형식, 운영주체, 어떻게 운영을 할 것인가에 관한 운영정책(Management Policy), 어떻게 서비스를 제공해야 하는 서비스 모델(Business Model), 마지막으로 어디서 어떻게 활용될 것인가를 다루는 유통시스템(Service Framework) 등을 통해 식별체계 개념과 기능을 정의 할 수 있다.

식별체계의 대표적인 예를 들면, 디지털 저작물 분야 식별체계는 미국 전자출판분야의 DOI(Digital Object Identifier)와 일본의 멀티미디어 저작물을 대상으로 한 CID(Content Id) 등이 있고, 오프라인 식별체계로는 도서 단행본을 대상으로 하는 ISBN(International Standard Book Number)과 음악 산업분야에서 활용되고 있는 ISRC(International Standard Recording Code) 등이 있다. 최근 문화체육관광부 산하 한국콘텐츠진흥원의 UCI(Universal Content Identifier) 등이 독자적으로 개발되어 콘텐츠 분야별로 적용하고 있는 상황이다.

디지털 저작물 식별체계란 인터넷 정보자원의 유일한 식별을 목적으로 다양한 서비스 모델을 근거로 저작물의 유통을 지원하기 위한 하나의 관리체계이다. 디지털 저작물 체계적인 관리 및 유통을 위해 디지털 저작물에 바코드 같은 기호를 붙이는 효과이며 이러한 식별기호를 통해 창작자(혹은 저작권자), 소유권자 즉 저작물의 책임과 권리소재를 명확히 해줄 수 있다. 따라서 식별체계를 따르는 디지털 저작물을 공식적으로 유통될 수 있다는 신뢰성을 부여한다는 의미를 갖는다.

9. 키 생성 관리

디지털 저작물 보호를 위해 사용되는 암호기술의 안전성을 보장하기 위해서는 안전한 키 관리 및 분배 메커니즘이 필요하다. DRM에서의 키 관리가 다른 암호시스템의 키 관리와 구별되는 가장 큰 특징은 저작물 전달과정에 참여하는 유통업자, 분배자, 이용자 등 모든 사용자 자신도 자신의 키를 알 수 없도록 관리되어야 한다는 점이다. 만약 자신의 키에 접근할 수 있다면 알고리즘의 비밀성이 보장되지 않는 한 저작물 원본을 뽑아내서 복제할 수 있기 때문이다. DRM 키 분배 방법은 대칭키 방식과 공개키 방식으로 구별될 수 있다.



〈그림 6〉 DRM 키 분배 방법

대칭키 방식은 하나의 키 분배 서버로 모든 부하가 집중되고 모든 저작물 거래에 키 분배 서버가 관여해야 한다. 반면 공개키 방식을 사용할 경우 분산성, 확장성, 상호운용성 등에서 많은 장점을 갖게 되나, 공개키 기반구조(PKI)가 필요하다는 부담을 지니고 있다.

그러므로, 저작물의 특성 및 적용 환경에 따라 적절한 키 관리 메커니즘을 선택하는 것이 바람직하다. 예를 들어 전자책, 음악 등과 같이 저작물 유통 범위가 광범위하고 저작물 유통 흐름에 많은 역할 개체들이 참여하는 경우, 하나의 키 분배 서버로 부하가 집중되는 키 관리 메커니즘의 경우는 적절하지 못하다.

10. 사용자 인증

저작물에 대한 사용 권리를 사용자별로 지정하고 통제하기 위해서 사용자 인증을 할 필요가 있다. 일반적으로 사용자의 인증처리를 위해 사용되는 기술은 ID/Password, Digital Certificate, SSO(Single-Sign-On), 생체인식 등이 있다. 이외에도 특정한 컴퓨터 또는 디바이스에서만 사용권한을 제어하기 위해 디바이스 인증 기술이 사용된다. 디바이스 인증 기술은 CPU 일련번호나 통신카드의 MAC Address, 그리고 HDD 일련번호 등과 같이 컴퓨터 또는 단말기의 고유한 식별정보를 바탕으로 사용자 정보와 결합하여 사용된다.

DRM은 특정한 인증기술에 종속될 필요는 없지만 적용 도메인 및 애플리케이션에 따라 적절한 인증기술과의 연동이 중요한 고려 사항이 된다. 따라서 DRM이 적용되는 응용 애플리케이션이나 적용 도메인에 따라 상이한 인증체계와 인증기술을 사용하고 있기 때문에, 이러한 기존 인증 체계와의 연동이나 통합을 손쉽게 수행할 수 있는 아키텍처의 설계 및 구현이 필요하다.

11. Tamper Resistance

DRM은 크게 서버군과 클라이언트군 소프트웨어로 나누어 구성된다. 서버는 이해관계가 동일한 집단 및 조직에 의해서 운영되기 때문에 그리 큰 문제점은 없다. 그러나 클라이언트 소프트웨어는 워낙 다양한 사용자들에 의해서 이용될 수 있도록 노출되어 있기 때문에 많은 위험 요소들을 안고 있으며, 그 중 가장 위협적인 부분이 악의적인 사용자에 의해서 소프트웨어의 구조 및 코드를 크래킹하는 것이다.

컴퓨터 기술이 발전함에 따라 소프트웨어 개발 기술도 발전하여 이의 생산성 개선을 위해 Reverse Engineering Tool, Debugging Tool, reassembling Tool들이 많이 개발되었다. 그러나 이러한 툴들은 개발자의 생산성을 높이는 데에만 사용되는 것이 아니라 소프트웨어를 크래킹하는 데에도 사용되고 있다. 따라서 Tamper Resistance는 이러한 크래킹 위협으로부터 소프트웨어를 안전하게 보호하는 것이 목적이라 할 수 있다.

크래킹을 통해서 위협이 될 수 있는 예는 다음과 같다.

- 소프트웨어 내부의 구조적인 분석 및 변경을 통해 임의의 조작을 취하는 행위
- 암호화 메커니즘의 무력화 행위
- 시간 등의 임의 조작
- 메모리 덤프 등을 통한 중요 데이터의 캡처링
- 하드디스크에 저장 관리되는 각종 데이터의 I/O 메커니즘 해독 및 임의 조작
- 소프트웨어의 여러 모듈 중 한 모듈로 가장하여 다른 모듈의 통신을 통한 임의 조작 및 데이터 갈취
- 기타

저작물 보호를 어렵게 하는 요인은 저작물이 사용되는 어떤 순간에 반드시 복호화 되어야 한다는 점이다. 저작물을 가공하거나 사용하는 과정에서 저작물 복호화키 또는 복호화된 저작물이 사용자에게 노출될 수 있다면, 암호기술을 깨지 않고도 보호되지 않은 저작물을 얻어낼 수 있게 된다. TRM은 마치 블랙박스와 같이 세부동작 과정이 드러나지 않도록 숨기고, 변형을 가하면 동작하지 않도록 제작된 소프트웨어 또는 하드웨어 모듈을 의미한다. DRM에서는 저작물의 권리 정보, 키 정보, 복호화된 저작물 등을 다루는 모듈에 TRM 기술을 적용하여, 디버깅 도구를 사용한 소프트웨어 역분석을 방지한다.

Tamper Resistance는 DRM에 있어서 저작물의 안전한 배포 및 이용을 위해서 가장 중요한 기술 중 하나이다. 이를 위해 크게 두 가지 방식이 적용되고 있다.

· 소스레벨에서 Scramble code의 삽입 : 가장 손쉬운 방식으로서, 소스레벨의 작업을 필요로 함
· 운영환경에서 크래킹 시도의 탐지 및 억제 : 소스레벨에서 대응하지 않고 운영체제 레벨에서 Specific cracking 기법에 대응하는 adhoc 방식의 방지 기법

국내 DRM 업체 중에서 Tamper Resistance의 두 가지 방식을 모두 지원하는 곳은 거의 없는 상태로 비록 지원을 하더라도 가장 간단한 방식인 Scramble code 삽입만 지원하는 정도이다. TRM 기술은 향후 DRM 시스템의 안전성을 결정하는 중요한 요소기술로 자리 잡을 것으로 예상된다.

저작물의 보안성을 보장함에 있어서 가장 우선적으로 고려해야 하는 분야는 암호화 기술의 견고성과 클라이언트 프로그램의 탬퍼링 방지 대책이다. 클라이언트 프로그램은 DRM이 적용된 저작물을 사용하기 위해서 사용자의 컴퓨터 또는 단말기에 설치되는 프로그램으로, 일부 악의적인 사용자에 의해 소프트웨어의 구조 변경이나 기술적 보호조치의 무력화 등 다양한 크래킹 위협에 노출되어 있다.

Ⅲ. 기술적보호조치 현황 및 다양한 활용

저작권을 보호하기 위한 업무는 거시적 관점에서는 저작권자의 권리 보호와 공정한 이용활성화로 구분되어지고, 단속과 예방업무로 나눌 수 있다. 단속 업무는 저작권을 위반한 불법 저작물에 대해 직접 수거 및 폐기, 또는 형사 고발을 통해서 법적인 조치를 취하는 것을 말한다. 반면, 예방업무는 불법물의 복제, 전송 등 불법물의 유통이나 소비가 이루어지는 것을 교육이나 홍보 및 기술적보호조치 등을 통해 사전에 불법 유통이 되지 않게 하는 것을 말할 수 있다.

온라인 서비스 제공자의 자율적 권리 구제의 틀 속에서 권리자가 서비스 관리 · 운영자에게 침해의 중단을 요청할 수 있도록 하고, 온라인 서비스 제공자가 기술적 조치의 적극적인 조치가 수행된다면 저작권 보호환경이 올바르게 정착될 수 있다. 하지만 디지털화된 저작물들을 개인과 개인 간 쉽게 배포하고 서로 공유할 수 있게 되었다는 긍정적인 측면이 부각되고 있지만, 이에 못지않게 저작권의 측면에서는 부정적인 면도 증가하고 있는게 오늘날의 현실이다.

따라서, 자신의 노력에 대한 정당한 대가를 받을 수 있으면서 허가되지 않은 사용, 저작권 침해를 방지할 수 있는 기술적, 제도적 환경이 요구되고 있으며, 이러한 환경의 조성은 고급 콘텐츠 생산을 유도하기 위해 필수적이다. 그러므로 불법 유통 및 복제에 대한 기술적인 문제가 해결되지 않는다면 개방형 네트워크를 통해 디지털 저작물 유통시장은 아주 제한적일 수밖에 없게 된다.

현재 저작권보호를 위해 사용되는 기술은 크게 DRM, 워터마크, 핑거프린팅, 필터링 등이 대표적이다. 기술적보호조치에 해당되는 이러한 기술들의 기능적인 측면과 활용될 수 있는 분야를 간략히 기술한다.

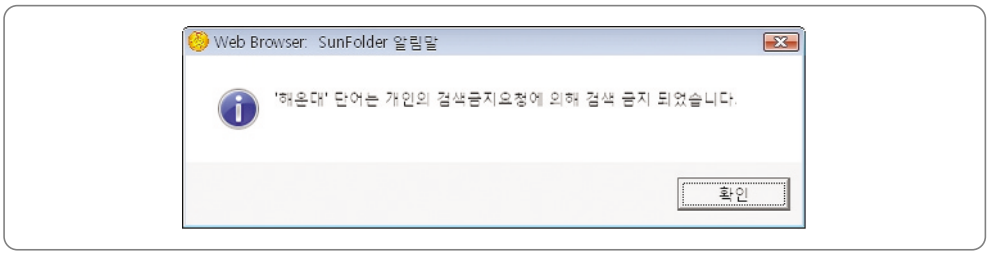
1. 기술적보호조치 현황

가. 필터링(Filtering)

저작권 보호기술에서의 필터링이란, 불법저작물의 유통을 막기 위해 이용자들의 불법 저작물 접근을 제한하거나 온라인 서비스에서 불법 저작물을 걸러내는 여러 방법들을 통칭한다. OSP들이 자체적인 모니터링 인력을 활용하여 불법 콘텐츠를 삭제하는 것도 일종의 필터링에 해당한다 볼 수 있으며, P2P · 웹스토리지 서비스에서 검색에 대한 금칙어를 설정하여 이용자들이 불법콘텐츠를 검색하지 못하게 하는 것도 필터링이다. 즉, 필터링 방법에는 여러 가지가 존재하며, 그 중에서 각 OSP에서 현재 널리 기술적 조치로서 사용되고 있는 필터링 기술들은 아래와 같다.

1) 저작물 제호 필터링

제목 제호 필터링이란, 저작물들의 제호 등을 DB화하여, 이용자가 파일의 제목을 이용하여 해당 저작물의 제호를 검색하여 해당 저작물의 제호가 검색이 되지 않도록 하는 방법이다. 아래 그림은 대표적인 웹스토리지 파일 송수신 전용 프로그램에서 특정 영화의 제호를 입력하여 검색을 시도할 때 보이는 금칙어 설정의 예이다.

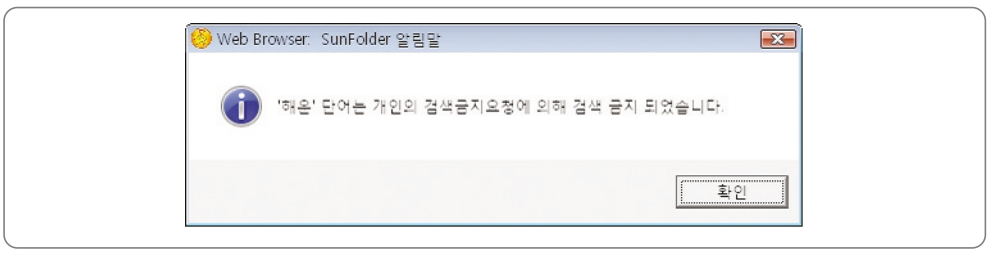


〈그림〉 저작물 제호 필터링

이러한 저작물 제호 필터링은 단순히 이용자가 입력한 검색어와 금칙어(콘텐츠 제목) 데이터베이스를 비교하면 되므로 제목 필터링 서비스 구축에 별다른 비용이 소요되지 않지만, 검색할 제목을 조금만 변경하여도 아주 쉽게 필터링을 피해갈 수 있다는 단점이 있다. 따라서 가장 간단하고 낮은 수준의 필터링 방법이라 할 수 있다. 현재 대부분의 P2P, 웹스토리지 업체에서 적용하고 있으며, 음악 · 영화 · 출판 · 게임 · 방송 · SW 등 저작물 종류에 관계없이 저작물마다 쉽게 적용이 가능하다.

2) 제호 문자열 확장 비교방식의 필터링

앞서 살펴본 저작물 제호를 이용한 필터링과 유사한 방법으로, 저작물을 검색하기 위한 단어들의 조합을 금칙어로 지정하는 방식이다. 예를 들어, 최신 개봉작인 '해운대'라는 영화 제목에서 '해운' + '운대'를 함께 금칙어로 설정하여, 두 단어의 조합이 검색어로 입력되면 검색이 제한 되도록 하는 방식이다. 아래 그림은 제호의 문자열을 확장한 비교방식의 필터링의 예로써, 웹스토리지 전용 프로그램에서 영화 제호의 일부 단어를 입력했을 때 확인할 수 있는 화면이다.



〈그림〉 저작물 제호 필터링

문자열 비교방식의 필터링 또한, 단순히 이용자가 입력한 검색어와 금칙어(단어 조합) DB만 비교하면 되므로 이러한 서비스 구축에 별다른 비용이 소요되지 않는다. 하지만 문자열 비교방식의 필터링 역시 검색할 단어를 조금만 변경하여도 쉽게 필터링을 피해갈 수 있다는 단점과 정작 찾고자 하는 검색어가 금칙어로 설정이 되어 검색의 혼선을 줄 수 있다는 단점을 가지고 있다.

3) 파일 확장자에 따른 필터링

파일 확장자에 따른 필터링이란, 파일의 특정 확장자를 차단하여 필터링하는 방법이다. 즉, mp3, mpg, mpeg, avi, wmv등과 같은 확장자를 가진 파일들을 모두 검색 결과에서 제외하는 방식이다.

파일 확장자에 따른 필터링은 파일의 확장자에 따라 검색결과만 제외시키면 되므로 제목필터링이나 문자열 비교방식의 필터링과 같이 서비스 구축이 간단하고 별다른 비용이 들지 않는다. 하지만 저작물들이 개별적으로 필터링 되는 것이 아니라 확장자 별로 필터링 되므로 실제 서비스에서 활용하기가 어려운 면이 많다. 또한 파일의 확장자명을 바꿔 파일을 유통시킬 경우 이러한 필터링 방법을 쉽게 우회할 수 있다는 단점을 가지고 있다. 일부 P2P 및 웹스토리지 서비스 업체에서는 음악파일의 확장자를 모두 필터링하여 음악파일의 유통을 모두 차단하고 있다.

4) 해시값 비교를 통한 필터링

해시값(Hash Value)이란 해시함수(Hash Function)에 의해 만들어진 결과 값이다. 해시함수는 특정한 크기의 데이터를 입력 값으로 하고 고정된 길이(대략 160bits)의 정수 값을 출력으로 하는 함수이다. 이 함수의 특징은 데이터의 입력 값이 다르면 그 출력 값도 거의 다르다. 따라서 출력 값이 다른 두 입력 데이터는 다르다고 판단하면 된다. 예를 들어, 두 개의 음악파일의 해시 값이 다르면 두 음악파일은 서로 다른 것으로 간주할 수 있다.

해시값 비교를 통한 필터링이란, 이러한 파일의 고유한 해시값을 이용하여 저작물의 동일성 여부를 인식하도록 하여 콘텐츠의 불법유통을 차단하는 방법이다. 해시함수를 만드는 방법은 무수히 많이 존재하고 구현 또한 어렵지 않으므로, 이러한 필터링 서비스의 구축이 간단하고 큰 비용이 소요되지 않는다. 하지만 해시함수의 특성상 데이터가 단 1비트만 달라도 전혀 다른 해시값이 나오게 되므로, 간단한 파일 변형을 통해서도 해시값 비교를 통한 필터링을 손쉽게 피할 수 있다. 즉, 동일한 노래라 할지라도 음질이나 인코딩 방식이 다르다면 입력 데이터가 다르므로, 해시값을 통해 필터링을 하려면 모든 변형에 대한 해시값을 가지고 있어야 한다. 하지만 이것은 불가능에 가까우므로 해시값을 통한 필터링에는 한계가 존재한다.

해시값을 통한 필터링이 위와 같은 한계를 가지고 있지만, 실제 온라인상에서 유통되는 동일한 저작물에 대한 파일의 종류는 일반적으로 제한되어 있으므로, 이러한 제한된 수의 파일들에 대한 해시값을 이용하여 필터링을 하는 것이 효과적인 방법이 될 수 있다. 예를 들어, 입력값이 쉽게 변하지 않는 SW나 패키지 게임 저작물의 경우 해시값을 이용한 필터링이 주요할 수 있다.

해시값 비교를 통한 필터링은 위의 문자열 비교방식이나 파일 확장자에 따른 필터링 방식보다 높은 수준의 저작권 보호 기술이자 더욱 효과적인 저작권 보호 기술 이다.

현재 일부 P2P업체에서 해시값을 통한 필터링 방식을 적용하고 있다.

나. 워터마킹 (Watermarking)

최근 오디오, 정지영상, 동영상과 같은 디지털 콘텐츠의 저작권 보호의 필요성이 대두됨에 따라 디지털 저작물에 "워터마킹"을 삽입하는 데에 대한 관심이 고조되고 있다. 디지털 저작물은 다양한 이점들을 제공해주지만, 원본과 동일한 대량의 복사본이 불법적으로 배포될 수 있다는 사실은 저작권 보호에 심각한 위협이 되고 있다.

워터마킹은 소유자 확인(Owner Identification), 특허권 사용료 지불(Royalty Payment), 원본 조작 여부 인증(Authentication)에 사용된다. 일단 워터마킹 된 데이터는 권한이 없는 이용자에게 통계적으로 소유권 정보의 검출이 불가능해야 하며, 신호처리 필터링이나 정보압축 동작에 의해 신호가 변형되더라도 소유자에 의해서는 소유권 정보의 검출이 가능해야 한다.

〈그림 19〉 워터마킹 활용 영역

디지털 워터마킹은 오디오, 비디오, 이미지, 그리고 텍스트 등의 멀티미디어 콘텐츠에 저작권 정보 등 소유권을 주장하고자 하는 특정의 데이터를 사람의 육안이나 청각으로는 구별할 수 없게

삽입하는 기술로 다양한 영역에 활용 될 수 있다. 만약, 유통 과정에서 소유권의 분쟁 등 원 소유자를 확인해야 하는 경우 이를 다시 검색, 추출하여 소유권, 저작권 등을 인증하여 권리를 행사할 수 있는 근거를 마련할 수 있도록 해주는 기술이다.

워터마킹은 여러 가지 특성에 따라 다양하게 분류 할 수 있다. 즉 물리적인 특성에 따라, 워터마크의 삽입 및 검출과정의 적용영역에 따라, 워터마크 검출 시 원본 데이터의 사용유무에 따라, 혹은 사용되는 저작물의 종류에 따라, 그리고 사용되는 기술에 따라 구분할 수가 있다. 여기서는 저작물 종류에 따른 워터마크의 분류에 대하여 살펴보기로 한다.

1) 오디오 워터마킹

오디오 워터마킹은 음악, 효과음, 교육용 음성파일과 같은 파일(wav, mp3, wma 등)에 대해서 저작권 정보를 파일 내에 삽입하는 기술을 말하며 워터마킹 후에도 음질에는 영향을 받지 않는다. 워터마킹 기술은 원본과 동일성을 유지하는 것에 기본을 두고 있기 때문이다. 또한 워터마크의 삽입이 후 Pressing, AD/DA변환 등 SDMI(Secure Digital Music Initiative)요건에 명시된 모든 변형에 강한 내성을 지닌다. 최근 인터넷의 활성화와 압축 코덱(Codec)이 발달함에 따라 음원의 유통이 활발해지고 파일의 사이즈가 작아져서 오디오 워터마킹에 대한 관심이 커지고 있다.

〈그림 20〉 오디오 워터마킹 삽입과정

또한 미국의 넵스터의 사례를 통해 저작권의 보호문제도 함께 나타나고 있다. 이러한 요구조건을 충분히 만족하는 오디오 워터마킹 기술은 보통 마스킹 현상(음원 내에 큰소리가 있을 때 작은 소리는 큰소리에 묻혀서 들리지 않게 되는 현상)을 이용하여 인간의 청각으로는 느낄 수 없는 신호부에 워터마킹 정보를 삽입하게 된다. 워터마킹을 삽입/추출할 시 원본 Playing Time의 30% 정도의 시간이 소요되며 삽입 할 수 있는 정보는 72bit/sec의 국제표준을 따르고 있다. 삽입정보량은 대상 오디오의 음질, 검출율과 상관관계가 있다. 이러한 조건을 감안하여 지원하도록 맞추어져 있다. 또한 짧은 특수 음향에도 적용을 할 수 있는데 Standalone 제품에는 검출율 및 공격에 대한 내성을 고려하여 10초 이상의 음원에 대해서만 워터마킹이 되도록 조절되어 있지만, 고객의 요청에 따라 1초미만의 음원에도 워터마킹을 할 수 있으며 워터마크 된 음악을 아날로그로 녹음하여 다시 디지털화한 음악에서도 검출이 가능하다. 아날로그로 녹음하여 디지털화하는 것은 가장 강한 종류의 공격이지만 실트로닉의 워터마킹 기술은 이러한 공격에도 강한 내성을 갖도록 설계되어 있다.

디지털 오디오 워터마킹 기술은 여러 응용 분야에 활용될 수 있는 연구 분야이며 디지털 방송의 경우도 콘텐츠에 대한 저작권 보호 필요성이 요구됨에 따라 오디오 워터마킹에 대한 관심이 고조되고 있다. 대표적인 오디오 워터마킹 방법에는 대역확산 기반의 워터마킹, 반향 워터마킹, 위상부호화 워터마킹, 패치워크 워터마킹 등이 있으며, 계속해서 새로운 워터마킹 기법들이 개발되고 있다. 지금까지 주요 음반업체들은 오디오 워터마킹 기술만 사용해왔다. 또 음반업체 · 전자 · 정보통신 관련 175개 업체가 디지털음악보호구상(SDMI)협의회를 조직, 표준화 작업을 추진해왔다. 오디오 워터마크 기술의 성능 평가는 SDMI, STEP 2001과 같은 표준화 기구에서 제시한 여러 가지 공격 유형을 설정하여 기술을 평가한다.

2) 이미지 워터마킹

디지털 이미지파일(gif, bmp, jpeg, pdf등)에 워터마킹을 삽입한 형태를 말한다. 즉, 이미지에 저작자나 배포자의 정보, 혹은 생성 날짜 등과 같은 정보나 고유번호 등을 삽입하는 방법이다. 이 방법은 삽입 방법에 따라 이미지 공간상의 미세한 변화를 주는 공간영역방법, 이미지 데이터를 주파수 변환하여 워터마크를 삽입하는 주파수 변환방법, 주파수 변환 시 워터마크를 데이터에 확산시켜 삽입하는 확산 스펙트럼 방법 등이 잘 알려져 있다. 이미지 워터마킹방법은 이미지에 저작자의 마크를 삽입한다면 JPEG이나 기타 필터링을 통해 변환된 이미지가 자신의 창작품임을 증명하기 위해서 자신이 삽입한 마크를 명확하게 인지가 가능한 수준으로 추출할 수 있어야 한다.

〈그림 21〉 이미지 워터마킹 적용

이미지 워터마킹은 응용시장이 무한한 것도 오디오 워터마킹에 비하면 큰 장점 중 하나다. 인터넷을 통한 문서 · 티켓 발급, 인터넷 우표 사업, 중요 문서 보안 및 관공서 · 은행 · 경찰 등의 문서 원본 증명 등은 모두 이미지 워터마킹 응용시장 분야다. 실 응용 예로 여권이나 신분증 등에는 아주 강력한 워터마크를 다량 삽입하여 아날로그 환경에서도 살아남도록 한다. 검출은 스캐너 등을 이용하여 디지털화 한 뒤 검출 프로그램을 통해 확인하며, 검출된 정보와 신분증에 적힌 정보를 비교하여 위조여부를 알 수 있다. 현재 이미지 워터마킹 솔루션을 출시한 곳은 미국의 디지마크 등 5개 업체가 있으며 이중 국내에서도 몇 개의 업체가 주목 받고 있다. 이러한 이미지 워터마크 기술의 성능 평가를 위해서 그 견고성에 대한 실험 또한 필요하다. 그러므로 워터마크가 삽입된 이미지가 공격을 받았을 경우에 워터마크가 얼마나 강하게 남아있는지 판단하기 위해 JPEG손실 압축, 필터링, 크로핑(cropping) 및 리샘플링(resampling)에 대해 확인을 해야 한다. 여기에는 워터마크 된 이미지에 다양한 공격을 할 수 있는 프로그램인 Stirmark, Checkmark 라는 Tool을 일반적으로 많이 사용한다. 이 프로그램을 이용하여 워터마크가 삽입된 이미지에 대해서 여러 가지 해킹을 시도하게 된다. Stirmark는 약 280 가지, Check mark는 약 380 가지의 해킹방법이 있다.

3) 비디오 워터마킹

동영상 파일(mpg, avi, rm 등)에 대해서 워터마킹을 삽입하는 형태이다. 이미지 워터마킹과 다른 점은 삽입 및 검출시간을 최적화하기 위하여 압축 후에 삽입하는 기술도 가지고 있다. 기본적으로 프레임에 삽입하는 원리는 같다. 공간영역법이나 주파수영역에서 특정함수에 의해 변환된 계수에 워터마크를 삽입하는 기술을 많이 사용하며 특정함수로는 DCT, Wavelet Transform, DFT등을 많이 사용한다. 삽입이 가능한 포맷은 MPEG1, MPEG2의 포맷이 삽입 가능하며 원본 Playing Time의 70% 정도의 시간이 소요된다. Raw data에 삽입하는 경우는 이미지 워터마킹과 같은 방식으로 프레임마다 삽입되며, 워터마크의 내성과 검출율은 상당히 높아지지만 삽입 시간이

엄청나게 길어지는 단점이 있다. 또한 기본적으로 64bit(숫자 16, 영문 8자)까지 삽입 할 수 있도록 지원하며 삽입정보량은 대상 이미지의 화질, 검출율과 상관관계가 있다. 그리고 비디오 워터마킹으로 모니터링이 가능하다. 즉 파일에 고유한 워터마크를 삽입하여 유통한 후, 방송 수신기 등에 검출기를 탑재하여 검출된 내용으로 모니터링 할 수 있다는 의미이다. 방송물 레코더나 카메라를 통한 캡처에도 워터마킹의 추출이 가능하며 이것은 실트로닉의 워터마킹 기술이 스트리밍 캡처나 아날로그 전환 시에도 워터마크가 생존할 수 있도록 설계되어 있다.

비디오 워터마크 기술의 성능 평가는 일반적으로 디지털에서 아날로그로 변환되고 아날로그가 다시 디지털로 변화되었을 때 워터마크가 살아남는지에 대한 여부와 디지털 방송에서의 깨끗한 화질을 보장할 수 있는 지의 여부를 기준으로 하고 있다.

〈그림 22〉 동영상 워터마킹 예

4) 벡터 워터마킹

벡터 이미지 파일(Digital Map Data, 및 기타 벡터기반의 2차원 혹은 3차원 이미지)에 보이지 않게 저작권 정보를 숨길 수 있도록 워터마킹하는 기술이 바로 벡터 워터마킹이다. 벡터 이미지라는 용어는 우리에게 생소한데 어도브사의 acrobat프로그램을 통한 파일 등과 같은 형태나 게임의 개발 등을 위한 오브젝트 파일, CAD 파일등 (pdf, dxf, bak 등)이 대표적인 형태이다.

저작자의 저작권정보나, 소유자만 알고 있는 어떤 정보를 바이너리형태로 변환하여 삽입하는데 벡터 이미지의 구조의 서술에 삽입하는 방법, 벡터 이미지의 구조에 삽입하는 방법, 좌표 값 자체

5) 텍스트 워터마킹

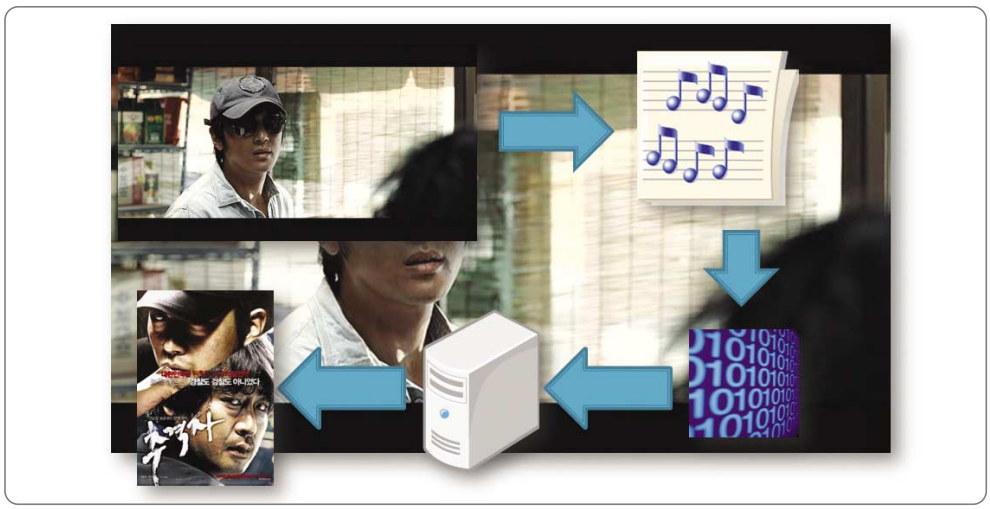
문서화된 데이터(hwp, doc)에 자신의 소유권 주장을 위한 저작권 정보를 삽입하는 기술이다. 글자간의 줄 간격을 미세하게 변화시키는 방법(line-shift coding method)이 있는데 이것은 단어와 뒤에 붙는 스페이스의 수는 변경 가능하며, 의미의 변화는 없는 방법이다. 글자의 폰트를 마찬가지로 변화시키는 방법(font coding method)등이 있다. 또한 문장 구성을 이용한 방법이 있으나 활용할 수 있는 기회가 제한되어있으며 단어의 의미를 조작하는 방법은 텍스트 데이터에 기밀 정보를 삽입하는 또 다른 방법으로 단어 자체를 변경하는 방법이다.에 삽입하는 방법, 위상영역에 삽입하는 방법 등이 있다.

다. 핑거프린팅 (Fingerprinting)

핑거프린팅은 두 가지가 존재하며, 하나는 '특징점 기반의 핑거프린팅' 이고 다른 하나는 '워터마킹 기반의 핑거프린팅(식별정보 삽입 방식의 핑거프린팅)' 이다. 국내에서 '핑거프린팅' 이라는 용어는 두 가지 의미로 모두 혼용하여 쓰고 있기 때문에 이를 잘 구분하여야 한다.

1) 특징점 기반의 핑거프린팅(Feature Based Fingerprinting)

음악, 영상 등의 콘텐츠에서 특징점을 찾아내어 이것을 DB에 보관하고, 후에 이를 다른 콘텐츠에서 추출된 특징점과 비교하여 두 콘텐츠가 일치 혹은 유사한지 알아내는 방법을 특징점 기반의 핑거프린팅이라고 한다. 여기서 특징점이란, 음악이나 영상파일이 가지고 있는 고유한 특성인 음원의 주파수나 화면전환정보, 위치정보, 컬러정보 등을 말하며, 이것을 음원DNA, 영상물DNA라고 부르기도 한다. 지문을 통해 사람의 신원을 확인하듯이, 콘텐츠의 특징점을 통해 해당 콘텐츠를 올바르게 인식할 수 있다.



〈그림 23〉 특징점 기반의 핑거프린팅 예

파일이 복제되거나 편집되더라도 특징점은 쉽게 변하지 않으므로 데이터베이스가 충분하다면 높은 확률로 사본을 찾아낼 수 있다. 업체마다 특징점을 추출하는 알고리즘이 다르므로 필터링 정확도에는 차이가 있지만, 유명한 업체나 연구소의 필터링 정확도는 대개 95% 이상이라고 알려져 있다. 하지만 합법적으로 만들어진 2차 저작물을 필터링에서 제외시켜야 하는 등의 기술적인 쟁점도 존재한다.

특징점 기반의 핑거프린팅 중 오디오 기반의 핑거프린팅(Audio Fingerprinting)에서는 다음과 같은 5가지의 요소들이 고려되어야 한다.

- 견고성(Robustness): 오디오 클립이 심한 신호 손상을 받은 경우에도 올바르게 인식될 수 있는지를 나타낸다. 강인한 견고성을 지니기 위해서 핑거프린트는 신호 손상과 관련하여 적어도 어느 정도는 변하지 않는 인지적 특성들을 가져야 한다. 심하게 손상된 오디오파일 역시 매우 유사한 핑거프린트를 가져야 한다. False-Negative rate가 보통 이러한 견고성을 나타내기 위해 사용된다. False-Negative는 인지적으로 비슷한 오디오 클립의 핑거프린트들이 서로 크게 상이한 경우에 발생한다.

- 신뢰성(Reliability): 노래가 잘못 인식되는 정도와 관련이 있다. 예를 들어 롤링스톤즈의 "Angie"라는 노래는 비틀즈의 "Yesterday"로 인식될 수도 있다. 이렇게 잘못 인식되는 비율을 False-negative rate로 나타낼 수 있다.

- 핑거프린트 크기(Fingerprint Size): 핑거프린트를 위해 얼마나 많은 용량과 대역폭이 필요한지와 관련이 있다. 핑거프린트는 빠른 검색을 하기 위해서 보통 RAM에 저장된다. 따라서 보통 초당 비트 수 또는 곡당 비트 수로 나타내어지는 핑거프린트 크기는 핑거프린트 데이터베이스 서버에 필요한 메모리와 대역폭을 결정짓는데 큰 역할을 한다.

- 입자성(Granularity): 오디오 클립을 인식하기 위해 필요한 시간 단위를 의미한다. 인식에 필요한 시간은 어플리케이션에 따라 달라진다. 어떤 어플리케이션들은 노래를 올바르게 인식하기 위해 노래 전체를 이용하며, 다른 어플리케이션들은 노래의 일부만을 이용하기도 한다.

- 검색 속도와 확장성(Search speed and scalability): 핑거프린트 데이터베이스에서 일치하는 핑거프린트를 찾아내는데 얼마나 오랜 시간이 걸리는가와 관련된 요소이다. 데이터베이스의 크기와 검색시간은 서로 반비례한다. 오디오 핑거프린트 시스템의 상용화를 위해서는, 검색 속도와 확장성이 중요 요소가 된다. 제한된 양의 고사양 컴퓨터를 이용하였을 때, 10만 곡에 대한 핑거프린트 데이터베이스를 검색하는데 수 천분의 일초 정도가 소요되어야 한다.

이러한 다섯 요소는 서로 밀접하게 관련이 되어있다. 예를 들어, 입자성이 낮아지는 것은(노래 인식에 필요한 시간이 줄어드는 것) false-positive 및 false-negative 에러율과 관련하여 신뢰성이 낮아진다는 것을 의미한다. 또한, 일반적으로 검색 속도는 견고성과 관련이 있다. 더 높은 견고성은 줄어든 검색 공간, 즉 검색하기 더 쉽다는 것을 의미한다.

국외의 경우 Audible Magic사의 핑거프린팅 기술이 YouTube와 미국의 유명한 SNS(Social Network Service)인 MySpace에 제공되었고, 국내의 경우에는 ETRI에서 개발한 Audio Fingerprint기술이 소리바다5 서비스에 적용되었다. 미국의 미디어 리서치 전문 업체인 닐슨(Nielsen)사와 정보보호기술 개발 업체인 디지마크(Digimark)사는 공동으로 올해 하반기 이전에 Watermarking과 특징점 기반의 핑거프린팅 기술을 모두 적용한 저작권 보호 서비스를 시작할 예정이라고 발표하였다.

2) 워터마킹 기반의 핑거프린팅

워터마킹 기반의 핑거프린팅(식별정보 삽입 방식의 핑거프린팅)이란 쉽게 말해서, 콘텐츠 구매자의 정보를 콘텐츠 내에 삽입하여 콘텐츠 불법 배포자를 추적할 수 있게 하는 기술이다. 디지털 워터마킹과 매우 유사하지만 삽입되는 정보에 차이가 있다(디지털 워터마킹은 저작권자 정보만 삽입된다).

아래 그림은 워터마킹 기반의 핑거프린트의 활용을 보여준다. 콘텐츠에 삽입된 핑거프린트(구매자정보)를 이용해 콘텐츠의 불법 배포자를 추적한다.

〈그림〉 워터마킹 기반의 핑거프린팅의 활용

이러한 워터마킹 기반의 핑거프린팅 기술은 소유권에 대한 인증뿐만 아니라 개인 식별 기능까지 제공해야 하므로 기존의 워터마킹이 갖추어야 할 요구사항인 비가시성, 견고성, 유일성과 더불어 공모 허용, 비대칭성, 익명성, 조건부 추적성 등이 부가적으로 필요하다.

- 비가시성(Imperceptibility): 콘텐츠의 가치를 그대로 유지함과 동시에 삽입 정보가 인간의 시각이나 감각에 의해 감지될 수 없어야 한다.

- 견고성(Robustness): 콘텐츠에 대해 필터링, 압축, 재샘플링 등 일반적인 신호 처리 및 포맷 변환, 기하학적 영상 변환 등을 가한 후에도 삽입 정보가 유지되어야 한다.

- 유일성(Uniqueness): 검출된 삽입 정보는 저작권자 · 구매자를 명확하게 특정할 수 있어야 한다.

- 공모 허용(Collusion Tolerance): 핑거프린팅 된 콘텐츠는 삽입되는 내용이 구매자마다 다르므로 다수의 구매자들이 자신의 콘텐츠를 비교하여 삽입 정보를 삭제하거나 다른 이용자의 정보를 삽입한 콘텐츠로 위조하여 배포할 수 있으므로, 이와 같은 공격에 견고해야 한다.

- 비대칭성(Asymmetry): 핑거프린팅 된 콘텐츠는 판매자는 알지 못하고, 구매자만이 알아야 한다.

- 익명성(Anonymity): 구매자의 익명성을 보장해야 한다.

- 조건부 추적성(Conditional traceability): 정직한 구매자는 익명으로 유지되는 반면, 불법 배포한 부정자는 반드시 추적할 수 있어야 한다.

불법배포자의 정보가 파일 내에 고스란히 담겨 있기 때문에 후에 책임을 추궁할 수 있지만, 구매자 정보를 삽입하는 알고리즘이 유출되면 정보조작의 가능성이 있다는 단점이 존재한다. 또한 원본의 변형을 피하기 위하여 많은 정보를 삽입할 수 없다는 단점도 존재한다.

라. DRM(Digital Rights Management)

DRM (Digital Rights Management : 저작권 관리 시스템)은 네트워크에서의 다양한 저작물 제공자 (Content Provider : CP) 로부터 고객(Client)로 안전하게 전달하고 이 고객이 불법적으로 콘텐츠를 유통하지 못하도록 하는 시스템 기술이다. 이러한 DRM은 오디오, 텍스트, 이미지, 비디오, eBook, 문서, AoD, 사진, 만화, VoD, 영화, 플래시 등의 콘텐츠에서부터 인터넷TV, 기

업정보관리, 전자도서관, 사이버대학, 인터넷 신문, 인터넷 라디오, 교육서비스, 디지털 이미징 서비스, 인터넷 만화방, 웹진 등의 애플리케이션 서비스에까지 광범위하게 적용 될 수 있다.

콘텐츠 산업발전적인 측면에서 필수 기술로서 인식되어 세계 시장의 선점[71] 및 표준화에 대한 각국의 경쟁이 치열한 상태이며, 현재까지 설립되어 활동 하고 있는 디지털 콘텐츠 보호 기술의 표준화 관련 분야는 다음과 같이 세 개로 구분할 수 있다.

저작권보호기술분야	디지털 방송&셋탑박스 분야	복제방지기술분야
MPEG-21, OMA, DVB-CPCM, DHWG, TV-Anytime, IDRM, SDMI, OeBF, xrML,ODRL	OpenCable POD Copy Protection(케이블 방송), ATSC CA(지상파), DVB-CA, ISMACryp	CPWG, CSS, CPSA,CPPM,CPRM, DTCP, HDCP, SmartRigt

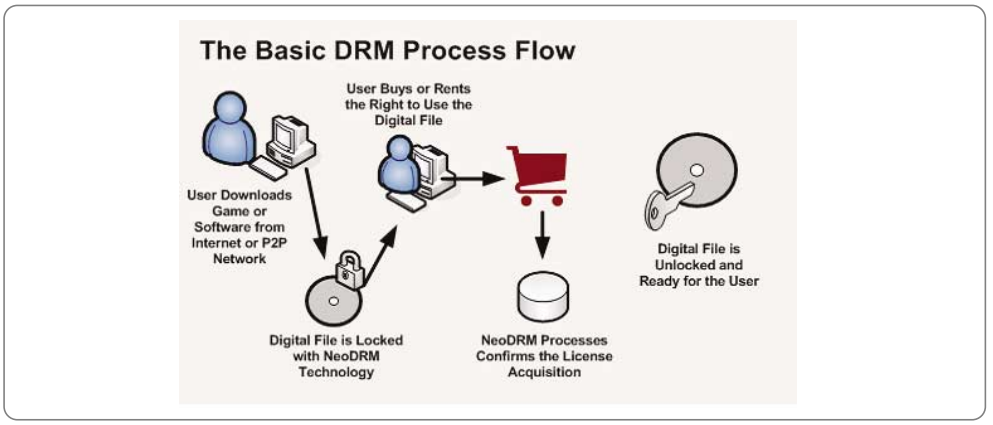
〈표〉 저작권 보호 기술 분야

DRM 시스템에서 있어 가장 중요한 기술은 암호화 기술로서 고객의 비밀 번호 혹은 고객 컴퓨터의 고유번호를 암호 키로 사용하여 콘텐츠를 암호화하여 전달하기 때문에 이를 복사하여 제3자에게 전달하여도 풀리지 않도록 하는 점이 가장 중요하며 암복호화 기술은 멀티미디어 콘텐츠의 유통에 있어서 불법유통이나 불법복제를 방지하기 위한 핵심 기술로서, 콘텐츠를 특정한 암호키를 이용하여 암호화시킴으로써 적법한 이용자만이 복호화하여 콘텐츠를 사용할 수 있도록 하는 기술이다.

기존의 콘텐츠 보호 시스템은 이용자 ID와 비밀번호만을 사용하고 있는데 이런 경우 ID와 비밀번호를 공유함으로써 쉽게 컨텐츠를 불법으로 사용할 수 있다는 문제가 있고 이것을 해결하기 위하여 고객 컴퓨터의 고유 ID[72]를 변형하여 사용하는 방법 고객의 PKI키나 은닉된 개인 키를 사용하는 방법이 있다.

71) Digital Millennium Copyright Act
미국의 '디지털 밀레니엄 저작권법'(DMCA)은 1996년 채택된 'WIPO저작권조약'과 'WIPO실연 및 음반조약'의 이행, 그리고 디지털시대의 새로운 저작권 보호를 모색하기 위해 1998년 10월에 제정되었으며, 온라인저작권을 강화하고 이를 방해하는 기술개발을 불법화하는 것을 주 내용으로 하고 있다. 이 법은 제1부에서 WIPO저작권 조약 및 실연 · 음반조약의 이행에 대해, 제2부에서 온라인서비스제공업자의 책임제한에 대해, 제3부에서 컴퓨터 유지보수 목적의 복제에 대한 면책에 대해, 제4부에서 기타 규정으로 저작권청의 기능 및 원격교육, 도서관 및 기록보관소, 일시적 기록물에 대한 면책 및 영상저작물의 권리이전에 관한 계약상 의무의 추정 규정에 대해, 제5부에서 선박디자인에 대한 보호에 대해 규정하고 있다.

72) 고객 컴퓨터의 고유번호, 예를 들면 HardDisk 번호 라든가 혹은 CPU번호를 이용하여 컨텐츠를 암호화시키는 경우가 있지만 컴퓨터의 고유번호는 누구나 쉽게 접근할 수 있기 때문에 보안성이 떨어진다는 단점이 있다.



〈그림 24〉 DRM 기본 흐름도

다음으로 중요한 DRM의 부품기술은 콘텐츠 사용 규칙 제어기술이다. 이는 고객의 지불(Payment) 형태에 따라 콘텐츠의 사용 횟수와 형태, 사용기간, 제3자 양도 등을 제어하는 기술이다.

그 외에도 지불 시스템과 고객 관리 시스템과의 연동, 고객 과금 처리 등의 요소 기술이 DRM을 구성하는 중요한 요소이다. DRM을 이용한 저작물 유통 서비스의 한 예로, 저작물을 가진 공급자(CP)와 지불 시스템을 연결하여 저작물을 제공하며 이용자에게는 암호화하여 저작물을 전달한다.

순서상으로 본다면 이용자가 네트워크에서 이미지나 오디오, 비디오 등의 저작물을 신청하고 지불을 하게 되면 지불시스템에서는 지불 승인을 통보 하게 되고, 정당한 이용자인 경우에 한해 저작물을 암호화하여 네트워크상 에서 이용자에게 전송하게 된다.

이미지, 오디오, 비디오 등의 저작물은 다운로드 되는 경우와 스트리밍으로 전송 받는 경우가 있으며 이용자 측에서 이미지를 보거나 오디오를 듣거나 비디오를 감상하는 경우 저작자(CP)측이 제공하는 브라우저(Browser)가 PC, PDA등에 설치되어야 한다. 이용자의 불법복제나 Play 횟수를 제한하는 사용규칙 제어 기능은 대체로 이 브라우저를 통해서 이루어진다. 그런데 이 브라우저에는 이용자의 비밀번호 관리프로그램이 들어있기 때문에 이 브라우저의 보안성이 대단히 높아야 한다는 점이 DRM시스템의 성공의 관건이다.

DRM은 디지털 콘텐츠의 정상적인 인터넷 상거래를 가능하게 하는 매우 확실한 기술이다. 불법 유통의 여지가 매우 적다. 그에 대한 대가로 DRM이 걸려있는 콘텐츠의 사용은 매우 불편하다. MP3 파일의 경우 매번 들을 때마다. 또한 실행시키는 기구를 변경할 때에도 패스워드를 넣거나 인증 절차를 거쳐야 하는데, 기구에 따라서는 실행을 전혀 못 하는 경우도 있다. 따라서 세계적인 콘텐츠 제공자인 세계 4대 음반사와 애플의 아이튠즈 등은 DRM 기술을 쓰지 않겠다고 선언을 하고 있다.

2. 기술적보호조치의 활용

1) 저작권 권리 보호 주장(Copyright Protection)

기술적보호조치의 목적은 디지털 저작물과 저작권 소유자의 정보를 삽입하여 다른 이들이 함부로 저작권 주장을 하지 못하도록 하거나 불법 저작물의 송 · 수신을 제한하여 궁극적으로 권리자를 보호하고 공정한 디지털 저작물 이용 활성화에 있다. 그러므로, 워터마크나 핑거프린팅과 같은 저작권 보호 기술은 올바른 저작권 소유자를 결정하는데 사용되며, 요구되는 강인성의 중요도가 매우 높다. 예를 들면, 웹상에 쉽게 이용 가능한 영상에 대해 그 소유자가 저작권을 보호받기 원하는 경우 이러한 기술적 응용이 적용될 수 있다. 강인성과 더불어 다른 이들이 부가적으로 워터마크나 핑거프린팅 정보를 삽입하는 경우에 대해서도 저작권 보호를 할 수 있도록 고려하여 활용되어야 할 것이다.

앞에서도 언급했듯이 디지털 저작물의 소유 관계를 주장하기 위해 활용되는 방법으로 저작물의 관련 정보를 삽입하거나 추출하는 것이다. 워터마크의 경우를 살펴보면, 먼저 디지털 저작물을 만드는 자가 프로그램을 사용해서 워터마크를 생성한 뒤 그것을 원본 저작물에 삽입을 한다. 그런 뒤 워터마크가 삽입된 이미지를 공개하여 워터마크가 가시적으로 나타난 경우는 다른 사람들이 이것을 보고 복사하지 않을 것이고 비가시적인 경우는 다른 사람이 저작물의 소유를 주장하면 원래 저작물을 생성한 작가는 소유를 주장하는 다른 사람의 이미지에 자신이 삽입한 워터마크가 있음을 보여주면 되는 것이다.

활용분야를 보면 텍스트, 오디오 파일, 비디오 파일, 이미지 파일, 벡터 파일 등의 저작권 주장을 하는데 이용된다.

2) 온라인 상 저작물 위변조 판별의 활용

기술적보호조치를 위한 기술은 온라인 상 저작물 위변조 판별에 활용될 수 있을 것이다. 동영상의 경우, 한편의 동영상이 압축율, 크기, 파일 용량, 코덱 등에 따라 여러 버전의 같은 동영상이 존재 할 수 있다. 위와 같은 경우, 해시(Hash) 값을 추출하여 인식할 수 있겠지만 각 생성되는 파일마다 다른 해시값 DB를 구성을 해야 하기 때문에 위변조 판별에는 취약할 수 있는 단점이 존재한다.

하지만, 동영상을 비롯한 디지털 저작물에는 고유의 특징값을 추출 할 수 있기 때문에 동영상의 왜곡이나 변환에도 동일한 특징값을 얻도록 하여 위변조 판별에도 활용할 수 있다. 특수한유형의 OSP 경우, 실제 최근 영화라 할지라도 다양한 형태의 영화가 유통되고 있고, 무한 복제가 이루어지고 있는 실정임을 감안한다면 핑거프린팅과 같은 특징값을 DB화하여 보유하고 있다면 동일 저작물에 대한 송 · 수신 차단에 활용될 수 있을 것이다.

뿐만 아니라, 활용 분야를 보면 온라인 티켓, 보험증서, 성적증명서, 의료기록 등 온라인 혹은 오프라인 상으로 전송되는 파일들의 위?변조 확인 시에도 활용될 수 있다.

3) 복사 제어(Copy Control)

앞으로의 멀티미디어 배포 시스템은 미디어의 불법적인 복사를 막을 수 있는 복사 제어 메커니즘을 보유하여 활용될 수 있다. 복사 제어는 개방된 시스템에 대해 매우 힘들지만, 밀폐된 또는 개인적으로 관리되는 시스템에 대해 가능하다. 그러한 시스템에 대해 데이터의 복사 여부를 나타내는 워터마크를 이용할 수 있다. 예를 들면, DVD의 경우 데이터에 복사정보가 삽입되어 있다. 그에 순응하는 DVD 재생기는 "복사 불가" 라는 정보를 담고 있는 복사 데이터에 대해 재생할 수 없다. "일회 복사" 라는 워터마크를 담고 있는 데이터는 일회의 복사가 가능하며 더 이상의 복사를 할 수 없다. 또한 워터마킹 기술을 사용해서 저작물에 대한 추가적인 정보를 제공하는 것이라고도 할 수 있다.

한 예로 이미지를 만드는 경우 이 이미지가 만들어진 시간, 창작자 등과 같은 정보나 복사된 것이라는 표시를 워터마크로 만들어서 이미지에 삽입하는 것이다. 활용분야를 보면 각종 서류나 문서, 유가증권 등의 복사기를 통한 복사방지 등에 활용된다.

4) 이용자 제어(User Control)

멀티미디어 저작물을 복사하거나 재생하는데 특별한 하드웨어 장치가 필요한 경우, 디지털 워터마크가 저작물에 삽입되어 저작물을 복사할 수 있는 횟수 등을 제어하는데 활용하는 것이다. 이 방법의 경우 복사를 할 때마다 하드웨어가 워터마크나 핑거프린팅 정보를 수정하게 되므로 더 이상 카피하지 않게 될 것이다. 활용분야를 보면 온라인 티켓, 성적증명서, 주민등록 등본 등의 전자문서 발급 시 횟수제한 등에 활용된다.

5) 불법 배포자 추적을 위한 특징점 DB 활용

핑거프린팅은 저작물 정보가 아닌 합법적 이용자에 대한 정보를 전달할 목적으로, 주로 저작물의 초본 복사 진의를 입증한다. 다시 말해 디지털 미디어의 무단 복제와 무단 배포를 막기 위한 방법이다. 이러한 응용은 불법적으로 배포되고 있는 저작물의 복사본을 감시하거나 추적하는데 유용하며, 소프트웨어 제품의 일련 번호(Serial Number)와도 흡사하다. 배포되는 각 복사본에 개별적으로 삽입된다. 이러한 배포는 각 초본 복사본을 비교하여 삽입된 마크를 쉽게 검출할 수 있으므로 그러한 공모에 안전하도록 (Collusion-Secure) 설계되어야 한다. 또한, 예를 들면, 특정 웹 Crawler가 저작권이 침해된 워터마크가 삽입된 영상을 검색하는 WWW(World Wide Web) 응용에 대해 쉽고 복잡하지 않도록 워터마크가 검출되어야 한다. 이러한 응용은 불법적인 공격뿐 만 아니라, 신호의 압축 처리에 대해 매우 강인해야 한다.

제5장 기술적 보호조치의 법적 이해



제5장 기술적 보호조치의 법적 이해

손승우 교수(단국대 법과대학)

Ⅰ. 법적 보호의 필요성과 의의

콘텐츠 산업의 성장과 함께 저작권 보호를 위한 기술적보호조치의 중요성은 더욱 증가하고 있다. 기술적보호조치란 저작권을 보호하기 위하여 멀티미디어, 문서 등의 디지털화된 저작물의 불법 복제를 방지하고 지정된 사용자에게 허가된 범위 내에서 사용할 수 있게 하는 기술로서 콘텐츠 유통산업의 성장에 핵심이 되는 기술이라고 할 수 있다. 또한, 콘텐츠 중심의 산업구조 발전은 세계적인 추세이며, 이러한 추세 속에서 기술적보호조치의 중요성은 점점 커지고 있다.

1. 보호의 필요성

디지털 기술의 발전과 인터넷의 보급은 복제물을 원본과 차이 없이 쉽고 빠르게 재생할 수 있게 되었고, 복제된 저작물이 네트워크를 통해 한번 전송되고 나면 이어진 동시 다발적인 복제로 인해 저작권자의 피해는 막을 수 없는 수준에 다다르게 된다. 이에 저작권자는 스스로 침해를 방지하고 저작물을 보호하기 위하여 다양한 기술적 조치를 강구하게 되었다. 그러나 이러한 기술적 보호조치(technological protection measures)도 오래되지 않아 다른 전문가들에 의해 무력화되어졌다.[73]

또한 기술적 보호조치가 복잡하고 정교하게 만들어 질수록 저작물의 이용자들은 불편과 번거로움을 감수해야만 했다. 저작권자들은 이러한 불편함을 최소화하기 위해 기술적 조치를 단순화시켜 빠르게 작동될 수 있도록 설계할 필요가 있었다.[74] 이러한 문제들에 직면한 권리자들은 정부에 기술적 보호조치를 무력화하는 행위를 법으로 금지해 줄 것을 요구하였다. 1996년 12월 제네바회의에서 각국 대표들은 기술적 보호조치에 대한 법적 보호의 필요성에 합의하였고, WIPO 저작권조약(WIPO Copyright Treaty)과 WIPO 실연 · 음반조약(WIPO Performance and Phonograms Treaty)에서는 기술적 보호조치의 무력화에 대한 효과적인 보호를 의무화하였다.

73) 손승우, "디지털 저작권보호의 확대경향과 공정한 경쟁", 「상사판례연구」제19집 제1권 (2006), 34면.
74) 임원선, 실무자를 위한 저작권법, 「한국저작권위원회」, 2007, 292면.

미국은 1998년 'Digital Millennium Copyright Act(이하 'DMCA'라 한다)'[75] 제1201조에 기술적 보호조치에 관한 규정을 두었고, EU는 2001년 저작권지침에 기술적 보호조치를 규정하게 되었다. 우리나라도 2001년에 컴퓨터프로그램보호법에, 2003년에 저작권법에 기술적 보호조치의 법적 보호에 관한 규정을 신설하였다.[76] 최근 타결된 한미 · FTA 협약에서는 기술적 보호조치에 대한 법적 보호를 한층 강화시켰다.

2. 법적 의의

기술적 보호조치에 대한 법적 규율은 크게 저작물에 대한 '접근통제(access control)'와 '복제에 대한 통제(copy control)'로 구분할 수 있다. 전자는 저작물에 대한 접근 자체를 통제하는 기술로서 저작권 침해와는 관계없이 저작물에 대한 접근을 통제하기 위한 기술을 말한다. 저작물에 접근을 할 수 없다면 저작물을 이용할 수도 없는 것이므로 접근을 통제한다는 것은 정보를 전반적으로 이용하는 것을 통제하는 것이 된다. 대표적인 방법으로서 온라인을 통해 저작물에 접근하는 과정에서 비밀번호 등에 의해 인증절차를 거치도록 하는 기술적 통제장치가 있다.[77]

한편, 복제통제형(Copy Control) 기술적 보호조치는 일단 저작물에 대한 접근은 통제하지 않지만 해당 저작물에 대한 복제 등 이용을 통제하는 기술이다. 여기서 '이용'이란 저작권자의 허락을 필요로 하는 저작물의 이용행위, 즉 저작권을 구성하는 복제, 공연, 방송, 배포, 전송하는 행위 등을 말한다. 이 유형은 다시 세 가지 경우로 나눌 수 있다.

첫째, 주로 소프트웨어에 많이 사용되는 '시간제한 방식'은 시간, 장소 이용자 등에 대한 일정한 조건을 만족하는 경우에만 작동하도록 하는 장치이다. 일반적으로 소프트웨어를 정해진 사용기한 후에는 이용할 수 없게 하는 장치로 셰어웨어나 베타버전 등이 있으며 대표적인 기술로서 '타임락(Time lock)' 등을 예로 들 수 있다.

둘째, '장소제한 방식'으로 특정한 시스템 또는 매체에서만 작동되도록 하거나 한 번에 단 하나의 시스템에서만 작동되도록 하는 '오리지널신호 대조방식' 등이 있다. 이는 특정한 시스템의 시리얼번호와 소프트웨어에 내장된 시리얼 번호를 상호 비교하여 다른 번호를 가진 시스템에서는 작동되지 않도록 하는 장치이다. 예를 들면, 컴퓨터프로그램이 무단 복제되어도 컴퓨터의 고유번호와 프로그램내의 번호가 일치하지 않으면 실행되지 않는 경우이다. 최근에는 MP3등에 사용되고 있으며, 특수한 경우로 DVD지역코드의 경우도 이에 해당한다고 볼 수 있다.

75) Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

76) 미국과 우리나라는 1996년 12월에 합의된 WIPO 저작권조약(WIPO Copyright Treaty) 제11조와 WIPO 실연 · 음반조약(WIPO Performance and Phonograms Treaty) 제18조에 명문화 된 기술적 보호조치의 법적보호(adequate legal protection and effective legal remedies)를 이행하기 위해 이를 명문화하였다.

77) 접근통제형 기술적 보호조치의 핵심기술로서 기업의 최종사업자의 권한을 규명하는 사용권한 제어기술(ACL)이 있으며, 또한 방송 서비스 가입자를 인식하여 허가된 가입자에 대해서만 서비스 제공이 가능하도록 하는 CAS 기술 등이 있다.

셋째, '이용자제한 방식'은 추가적인 권리처리를 한 이용자에게 할당된 고유의 시리얼 넘버나 패스워드가 아니면 작동되지 않도록 하는 방식으로 접근 통제형의 기능도 가지고 있다. 최근 음악 CD에 이러한 기술이 적용되어 시리얼 넘버가 부착된 CD를 삽입하고 해당사이트로 로그인하면 뮤직비디오 등을 부가적으로 이용할 수 있다.[78]

저작권법에서는 기술적 보호조치를 "저작권 그 밖에 이 법에 따라 보호되는 권리에 대한 침해행위를 효과적으로 방지 또는 억제하기 위하여 그 권리자나 권리자의 동의를 얻은 자가 적용하는 기술적 조치"로 정의하고 있다.[79] 따라서 저작권법에서 보호받는 기술적 보호조치는 이법에서 부여하고 있는 권리를 보호하기 위한 것으로 한정되므로 복제통제형 기술적 보호조치만이 그 대상이 된다. 저작권법은 저작권자에게 '접근'을 통제할 권한을 부여하고 있지 않으므로 접근통제형 기술적 보호조치는 이법의 보호대상에 포함되지 않는다.

2009년 7월 통합 저작권법의 시행으로 폐지된 컴퓨터프로그램보호법에서는 기술적 보호조치를 "프로그램에 관한 식별번호 · 고유번호 입력, 암호화 기타 이 법에 의한 권리를 효과적으로 보호하는 핵심기술 또는 장치 등을 통하여 프로그램저작권을 보호하는 조치"라고 정의하였다.[80] 이법의 보호대상이 되는 기술적보호치는 '이 법에 의한 권리를 효과적으로 보호하는 기술'에 한정되므로 저작권법과 같이 복제통제형 기술적 보호조치를 대상으로 하고 있다.

그 밖에도 온라인디지털 저작물산업발전법에서도 기술적 보호조치에 관한 정의규정을 두고 있는데, 즉 기술적 보호조치란 "온라인디지털 저작물제작자가 이 법에 의하여 보호되는 이익의 침해를 효과적으로 방지하기 위하여 적용하는 기술 또는 장치"를 말한다.[81]

위에서 살펴본 바와 같이, 저작권법과 컴퓨터프로그램보호법이 모두 복제통제형 기술적 보호조치만을 보호하고 접근통제형 기술적 보호조치를 보호하지 않는 것은 후자를 보호하게 되면 전통적으로 인정해 온 저작물에 대한 일반인의 접근을 과도하게 차단하게 되어 저작권법의 근본적인 입법취지인 문화발전을 저해할 우려가 있기 때문이다.

우리나라와 달리, 미국은 1998년에 DMCA(Digital Millennium Copyright Act of 1998)를 제정하여 저작권자에게 저작물에 대한 접근통제권을 부여하고 있는데, 이는 전통적인 저작권과는

78) 이성우, "기술적 보호조치에 있어서 접근통제조치의 문제점에 관한 소고", 「경성법학」제16집 제2호, 경성대학교 법학연구소 (2007.12), 220-221면.

79) 저작권법 제2조 제9호.

80) 컴퓨터프로그램보호법 제2조 제9호. 기술적 보호조치란 프로그램에 관한 식별번호 · 고유번호 입력, 암호화 및 기타 법에 의한 권리를 보호하는 핵심기술 또는 장치 등을 통하여 프로그램저작자에게 부여된 공표권, 성명표시권, 동일성유지권과 프로그램을 복제 · 개작 · 번역 · 배포 · 발행 및 전송할 권리 등 프로그램저작권에 대한 침해를 효과적으로 방지하는 조치를 의미하였다. 대법원 2006.2.24. 선고 2004도2743 판결.

81) 온라인디지털콘텐츠산업발전법 제2조 제10호.

별도로 저작물에 대한 접근을 통제할 수 있는 새로운 권리를 부여한 것이라 할 수 있다.[82] 즉 DMCA 제1201조 (a)(1)에서 "누구든지 본 법에 의하여 보호되는 저작물에 대한 접근을 효과적으로 통제하는 기술적 조치를 우회해서는 안 된다"고 규정하여 접근통제를 위한 기술적 보호조치를 보호하고 있다.[83] 한편 EU는 정보사회 지침 제6조(Obligations as to technological measures)에서 복제통제 및 접근통제의 무력화를 금지하고 있다.

일본의 경우는 기술적 보호조치에 대해 저작권법과 부정경쟁방지법이 역할을 나누어 보호하고 있는 것이 특징이다. 우선 '복제통제형' 기술적 보호조치에 대하여는 저작권법에서 보호하고 있으며, 부정경쟁방지법에서는 '접근을 통제형' 기술적 보호조치를 무력화시키는 장치, 도구 등을 거래행위를 금지하고 있다. 저작권법에서는 접근통제에 대해서는 규율하지 않고 복제통제형 기술적 보호조치의 무력화 도구의 거래행위를 규제하고, 또한 업(業)으로서 복제통제형 기술적보호조치를 무력화하는 행위를 금지하고 있다.

이와 같이 기술적 보호조치에 관한 각국의 입법이 상이한 것은 WCT 제11조에서 "체약국은 이 조약 또는 베른협약에 따라 저작자가 자신의 권리를 행사하는 것과 관련하여 사용하는 효과적인 기술적 보호조치와 저작물에 관하여 저작자가 허락하지 아니하거나 법에서 허용하지 아니하는 행위를 제한하는 효과적인 기술적 보호조치를 무력화시키는 것에 대하여 적절한 법적 보호와 효과적인 법적 구제수단을 제공하여야 한다"[84]고 규정하고 있을 뿐 접근통제에 관해서는 명시적인 규정을 두지 않고 이행국의 재량에 맡기고 있기 때문이다.

82) DMCA 이외에 기술적 보호조치에 관한 미국의 입법으로 1992년의 Audio Home Recording Act와 1996년의 Telecommunication Act 등이 있다.

83) 이 규정은 "저작물에 대한 접근을 통제하기 위하여" 사용되는 기술적 보호조치를 우회하는 것을 금지하는 권리를 규정한 것으로 미국의 연방저작권법상 인정되는 "저작권자의 권리(예컨대, 복제, 2차적 저작물, 배포, 공연, 전시 등을 허락하거난 금지할 저작자의 권리)를 보호하기 위하여" 사용되는 기술적 보호조치를 우회하는 것과는 별도로 규정된 것이다. 접근을 저작자의 권리와 분리시킨 이유는 (i) 저작물에 대한 접근은 저작권자가 제시하는 가격이나 조건에 의해 제한받는 한도에서 일반인에게 제공되는지 여부나, (ii) 일단 접근이 합법적으로 획득된 이후에 일반인들이 저작물을 복제, 개작, 배포, 공연, 전시하고자 하는지 여부에 따른 균형에 대응하기 위한 것이다. Jane C. Ginsburg, "Copyright Legislation for the "Digital Millennium",", 23 Colum. -VLA J.L. & Arts 137, 139 (1999).

84) WIPO Copyright Treaty Article 11 (Obligations concerning Technological Measures) "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."

Ⅱ. 저작권법상 기술적 보호조치 규정

1. 통합 저작권법에 의한 규제

최근 정부조직법 개정으로 컴퓨터프로그램에 대한 보호업무가 문화체육관광부로 이관되면서 컴퓨터프로그램보호법이 저작권법으로 흡수 · 통합되었다. 개정 저작권법에서는 기술적 보호에 관하여 개정 전 저작권법과 동일한 규정을 두고 있다. 즉 이법 제124조제2항에서 "정당한 권리 없이 저작권 그 밖에 이 법에 따라 보호되는 권리의 기술적 보호조치를 제거 · 변경 · 우회하는 등 무력화하는 것을 주된 목적으로 하는 기술 · 서비스 · 제품 · 장치 또는 그 주요 부품을 제공 · 제조 · 수입 · 양도 · 대여 또는 전송하는 행위는 저작권 그 밖에 이 법에 따라 보호되는 권리의 침해로 본다"고 규정하여 기술적 보호조치의 무력화 행위 자체를 금지하지 않고 무력화에 사용되는 도구의 거래행위를 금지하고 있다.

미국 DMCA의 경우 접근통제를 무력화하는 행위를 금지하면서도 복제통제를 무력화하는 행위를 별도로 금지하지 않고 있다. 그 이유는 복제통제를 무력화할 경우 바로 복제로 이어지게 되므로 저작재산권의 하나인 복제권에 대한 침해로서 이를 충분히 규율할 수 있기 때문이다.[85] 반면, EU 정보사회 지침에서는 접근통제뿐만 아니라 복제통제의 무력화도 금지하고 있으며, 기존 컴법에서도 복제통제형 기술적 보호조치의 무력화를 금지하고 있다. 생각건대, 비록 복제에 대해 권한이 있는 자라 하더라도 복제통제형 기술적 보호조치를 무력화할 경우 컴법과 EU 지침에 따르면 처벌이 가능하게 되는데, 이를 규제할 실익이 있는지는 의문이다.

그리고 저작권법과 DMCA와 같이 복제통제를 무력화하는 행위를 금지하지 않을 경우에는 이용자가 저작권법상 저작권제한 사유에 해당하는 행위를 위해 당해 기술적 보호조치를 무력화할 수 있게 된다. 반대로 복제통제의 무력화를 금지하게 되면 저작권제한 사유에 해당하는 행위를 위해 무력화를 하더라도 민 · 형사적 책임을 지게 되는 문제가 생긴다. 물론 아래에서 설명하는 바와 같이, 폐지된 컴퓨터프로그램보호법에서는 무력화 금지의 예외를 자세하게 규정하고 있다.

한편, 저작권법상의 기술적 보호조치는 그 '주된 목적'이 무력화에 있는 조치에 한정하고 있으므로 CD-RW와 같이 사용에 따라 기술적 보호조치의 무력화가 가능한 장치라도 그 주된 목적이 무력화에 있지 않으므로 동법의 보호 대상에서 제외된다.[86] 또한 개정 저작권법은 동 조항의 위반행위를 저작권 침해행위로 간주하는 방식으로 규제하고 있으므로 기술적 보호조치 침해에 대해 민 · 형사적 구제가 가능하다. 다만, 실무적으로 저작권 침해 전에 발생하는 기술적 보호조치의 무

85) Roger E. Schechter & John R. Thomas, Intellectual Property: The Law of Copyrights, Patents and Trademarks (2003), 143.
86) 이해완, 저작권법, 박영사, 2007, 741면.

력화 행위 또는 무력화 도구의 거래행위로 인한 손해액의 입증은 쉽지 않은 일이다.[87] 또한 무력화할 수 있는 기술, 장치 등을 제작한 행위에 대해 손해배상을 청구할 경우 그 무력화 대상이 되는 저작물과 저작권자를 특정하는 일도 쉽지 않을 것이다. 한편 저작권법 제136조 제2항 제5호에서 "업으로 또는 영리를 목적으로 제124조제2항의 규정에 따라 침해행위로 보는 행위를 한 자"에게 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 규정하고 있다.

2. 컴퓨터프로그램보호법에 의한 규제

컴법 제30조 제1항에서 "누구든지 정당한 권원없이 기술적보호조치를 회피, 제거, 손괴 등의 방법으로 무력화하여서는 아니된다"고 규정하여 저작권법과 달리 복제통제형 기술적 보호조치의 무력화행위를 금지하고 있다. 또한 동조 제2항에서 "누구든지 상당히 기술적보호조치를 무력화하는 기기 · 장치 · 부품 등을 제조 · 수입하거나 공중에 양도 · 대여 또는 유통하여서는 아니되며, 기술적보호조치를 무력화하는 프로그램을 전송 · 배포하거나 기술적보호조치를 무력화하는 기술을 제공하여서는 아니된다"고 규정하여 저작법과 같이 기술적 보호조치에 사용되는 도구의 거래행위를 금지하고 있다.

더불어 동조 제1항 각호에서는 기술적 보호조치의 무력화 금지의 예외를 규정하고 있는데, 즉 제10조의 규정에 의한 프로그램의 동일성을 변경하는 경우(제1호), 제12조 각호의 1에 해당되어 복제 사용하는 경우(제2호), 제14조의 규정에 의한 프로그램 사용자가 필요한 범위안에서 복제하는 경우(제3호), 정당한 권원에 의하여 사용하는 자가 다른 프로그램과 호환성을 유지하기 위하여 필요한 경우(제4호), 정당한 권원에 의한 최종사용자로부터 프로그램의 수정 · 보완을 요청받은 경우(제5호), 정당한 권원에 의하여 사용하는 자가 연구 · 교육 등의 목적으로 프로그램과 관련된 암호화 분석을 하기 위하여 필요한 경우(제6호) 등이다. 이와 같이 복제통제의 무력화를 금지하면서도 이에 대한 예외를 둔 것은 저작권제한 사유 등 일정한 공정한 목적을 위해 무력화를 할 수 있도록 허용함으로써 저작권자의 이익과 이용자의 이익간의 균형을 유지하기 위한 것으로 해석된다.

2009년 7월 23일 통합 저작권법이 시행되면서 컴퓨터프로그램보호법상의 복제통제형 기술적 보호조치의 무력화행위 금지 조항은 삭제되었고, 저작권법에 따라 무력화 도구의 거래행위만을 규율하게 되었다.

87) 오승종, 저작권법, 박영사, 2007, 1343면.

〈기술적 보호조치에 대한 입법 비교〉

국 가 / 행 위	한국		미국	한미 FTA 법안
	저작권법	컴 법	DMCA	
접근통제의 무력화	X	X	§1201(a)(1)	§104의2①
접근통제의 무력화 도구 거래	X	X	§1201(a)(2)	§104의2③
복제통제의 무력화	X	§30①	X	X
복제통제의 무력화 도구 거래	§124②	§30②	§1201(b)	§104의2③

Ⅲ. 기술적 보호조치 관련 국내외 판례

1. P2P 모드칩 사건[88)]

피고인은 소니 엔터테인먼트사가 제작한 플레이스테이션 2라는 게임기본체(이하 'PS2'라 한다)에서 복제 게임CD가 구동될 수 있도록 지역코드를 해제하기 위한 모드칩을 고객들의 요청에 따라 PS2에 장착한 사건에서 대법원은 모드칩 장착행위가 기술적 보호조치의 무력화에 해당하는지의 여부를 판단하였다.

대법원에 따르면, "컴퓨터프로그램 보호법 제30조 제1항 및 제2항은 누구든지 상당히 기술적 보호조치를 회피, 제거, 손괴 등의 방법으로 무력화하는 기기 · 장치 · 부품 등을 제조 · 수입하거나 공중에 양도 · 대여 또는 유통하여서는 아니 되며, 기술적 보호조치를 무력화하는 프로그램을 전송 · 배포하거나 기술적 보호조치를 무력화하는 기술을 제공하여서는 아니 된다고 규정하고 있고, … '기술적 보호조치'란 프로그램에 관한 식별번호 · 고유번호 입력, 암호화 및 기타 법에 의한 권리를 보호하는 핵심기술 또는 장치 등을 통하여 프로그램저작권에 대한 침해를 효과적으로 방지하는 조치를 의미하는 것으로 봄이 상당하다(제2조 제9호, 제7조).

대법원은 엑세스 코드나 부트롬만으로 게임프로그램의 물리적인 복제자체를 막을 수는 없지만, 통상적인 장치나 프로그램만으로는 엑세스 코드의 복제가 불가능하여 게임프로그램을 복제해도 PS2를 통한 프로그램의 실행을 할 수 없으므로 엑세스 코드는 게임프로그램의 물리적인 복제를 막는 것과 동등한 효과의 기술적 보호조치에 해당한다고 판단하였다. 또한 피고인이 고객들의 요청으로 이 사건 모드칩을 PS2에 장착해 주는 행위는 게임기의 엑세스 코드를 무력화시켜 복제CD가 구동할 수 있게 하는 것으로 기술적 보호조치를 무력화하는 기기 · 장치 · 부품 등을 유통시키는 행위에 해당한다고 하였다.[89)]

88) 대법원 2006.2.24. 선고 2004도2743 판결.

89) 부산지법 2004.4.22. 선고 2004노307 판결(P2P 모드칩 사건의 원심에 해당한다).

2. Universal City Studios, Inc. v. Reimerdes[90]

원고는 영화를 DVD 형태로 제작하여 배포하면서 영화를 복제하는 것을 막기 위해 CSS 시스템을 이용한 기술적 조치를 하였다. 인터넷을 통해 만난 피고들은 DVD 플레이어를 역분석하여 CSS를 해독할 수 있는 방법인 DeCSS를 제작하였고 이를 이용해 영화파일을 컴퓨터의 하드 드라이버에 복제할 수 있도록 하였다. 피고는 이 프로그램을 자신의 웹사이트에 게시하고 이러한 사실을 공개하였다.

2000년 1월 원고는 DMCA를 근거로 소를 제기하였다. 이에 피고는 그들의 행위가 DMCA를 위반하는 것이 아니라 오히려 컴퓨터 프로그램 또는 암호에 적용되는 DMCA가 수정헌법 제1조를 위반하는 것이라고 주장하였다.

피고는 원고의 CSS 기술은 너무 쉽게 해독되기 때문에 저작물에 대한 접근을 '효과적으로 통제할 수 있는 조치'에 해당하지 않으므로 DMCA가 적용되지 않는다고 주장하였다. 그러나 Kaplan 판사는 이용자가 암호화 키 없이는 CSS기술로 보호되는 영화를 볼 수 없으며, 그러한 암호화 키를 얻으려면 정당한 라이선스에 근거한 DVD 플레이어 또는 컴퓨터 드라이버를 구입해야 한다면서 피고의 주장을 받아들이지 않았다.[91]

그러나 이 판결에서 CSS기술이 접근통제에 해당한다는 법원의 분석에는 문제점이 있다. 즉 영화 스튜디오가 궁극적으로 CSS기술적 조치를 취한 이유는 허락받지 않은 접근을 통제하기보다는 복제를 통제하기 위한 것이기 때문이다.[92]

3. Coupons, Inc. v. Stottlemire[93]

원고 Coupons사는 자사가 제공한 소프트웨어를 이용하여 이용자들이 온라인으로 접속하여 할인 쿠폰을 다운 받을 수 있는 서비스를 제공하였는데, 이 소프트웨어는 개별 이용자가 쿠폰을 출력할 수 있는 회수를 제한하는 기능을 가진다. 원고는 피고 Stottlemire가 이용자들이 회수의 제한 없이 쿠폰을 출력할 수 있도록 원고의 소프트웨어에 적용된 기술적 조치를 우회하는 프로그램을 개발하여 배포한 것을 이유로 캘리포니아 북부지방법원에 소를 제기하였다.

90) 111 F.Supp.2d 294 (S.D.N.Y. 2000)(이하 'DeCSS 사건'이라 한다). Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

91) 한편, 'DeCSS 사건'과 유사한 사실관계를 가진 DVD Copy Control Ass'n Inc. v. Bunner 사건에서 원고는 피고가 DeCss를 포스팅한 행위는 원고의 영업비밀을 침해한다는 이유로 캘리포니아 지방법원에 소를 제기하였다. 법원은 원고의 CSS 기술이 더 이상 영업비밀에 해당한다고 볼 수 없고, 피고의 DeCSS 소프트웨어를 포스팅한 행위를 금지하는 것은 피고의 표현의 자유에 대한 사전억제(prior restraint)에 해당한다고 판결하였다. DVD Copy Control Ass'n Inc. v. Bunner, 116 Cal.App.4th 241, 255-6(Cal.App. 6 Dist. 2004).

92) Roger E. Schechter & John R. Thomas, Intellectual Property: The Law of Copyrights, Patents and Trademarks (2003), 146.

93) 588 F.Supp.2d 1069 (N.D.Cal., 2008); F.Supp.2d, 2008 WL 3245006 (N.D.Cal., 2008).

원고는 DMCA 제1201조(b)의 기술적 보호조치 우회금지 조항을 근거로 피고가 개발한 프로그램이 쿠폰의 이용을 제한하는 기술적 보호조치를 우회하였다고 주장하였다. 또한 피고의 프로그램은 제1201조(a) 조항에 따라 쿠폰에 대한 접근을 제한하는 기술적 보호조치도 우회하였다고 주장하였다.

동 법원은 기술적 보호조치 우회 프로그램의 사용 여부와 상관없이 이용자들은 쿠폰에 대한 접근이 가능하므로 이 사건에서 제1201조(a) 규정에 따른 쿠폰에 대한 접근을 제한하는 기술적 보호조치 우회 주장은 타당하지 않다고 판단하였다. 그리고 원고의 주장은 저작권자의 저작권과 이용자들의 정보 접근권간의 권리의 경계를 설정한 저작권법의 체계에 반하는 주장이라고 판결하였다.

4. Edelman v. N2H2 사건[94)]

피고 N2H2사는 인터넷 필터링 프로그램을 개발하는 전문업체로서 피고가 개발한 필터링프로그램(Bess)은 음란물, 마약, 경매, 도박, 주류, 인종차별 등 유해성 웹사이트를 식별하여 청소년들이 이러한 웹사이트에 접근하지 못하도록 제작된 컴퓨터프로그램이다. 미국 전역에서 약 40%의 학교가 이 프로그램을 사용하고 있으며 공공 도서관 등에서도 사용하고 있다.

원고 Edelman은 컴퓨터 연구자로서 하버드 법대에서 일을 하고 있었는데, 피고가 개발한 Bess 프로그램이 전혀 유해하지 않는 웹사이트까지도 필터링한다는 중대한 오류를 발견하고 그 사실을 입증하고자 하였다. 이를 위해서 Edelman은 문제의 프로그램을 구입한 뒤 이 프로그램에 장착되어 있는 기술적 보호조치를 무력화하고 역분석(reverse engineering)을 통하여 프로그램상의 오류를 분석하였다. Edelman의 분석결과에 따르면, Bess 프로그램에 의해 잘못 식별된 웹사이트의 예로서 비영리단체인 IRIS Center Romania 웹사이트, Wales지역의 소방서 웹사이트, 국제 열기구 축제 웹사이트, 전국자원봉사자센터 웹사이트 등이 포함되어 있었다. Edelman의 연구는 이 프로그램의 문제점을 분석하는데 머물지 않고 Bess에 의해 접근 금지된 웹사이트에 접근할 수 있는 무력화 도구로서 소프트웨어를 개발하여 온라인을 통해 배포하였다.

그런데 Bess 프로그램의 라이선스에서는 기술적 보호조치의 무력화와 역분석을 금지하고 있었다. 이에 대하여, Edelman은 연구의 일환으로 수행된 자신의 행위는 공정이용(fair-use)으로서 DMCA 규정을 위반하지 않았다고 주장하였다. 또한 기술적 보호조치를 무력화할 수 있는 도구를 배포한 행위로 인하여 피고의 경제적 이익을 침해하지 않았으며, 오히려 이 도구를 사용함으로써 필터링프로그램이 보다 정확하게 작동될 수 있게 되었으므로 DMCA의 기술적 보호조치에 관한 규정을 위반하지 않았다고 주장하였다.

94) No. 02-CV-11503 (D. Mass. filed July 25, 2002). 손승우, 앞의 논문, 43-48면 참조.

이 소송은 Edelman을 대리한 ACLU(American Civil Liberties Union)가 기술적 보호조치를 무력화한 Edelamn의 법적 책임의 부존재를 확인(declaratory relief)하고 피고에 의한 잠재적 제소를 예방하기 위하여 제기한 것이다. 이에 대하여 N2H2사는 Edelman이 필터링프로그램에 관한 연구를 더 이상 진행하지 않는다면 향후 책임을 묻지 않겠다고 제안하였다. 법원은 피고의 잠재적 제소를 막기위한 Edelman 측의 신청은 추측에 근거한 것으로 소익이 없다고 하면서 N2H2사의 신청(motion to dismiss)을 받아들였고 원고의 신청을 기각하였다. 이 판결이후 Edelman은 Bess 프로그램에 관한 연구를 더 이상 진행할 수 없었다.

이 사건에서 법원은 비록 Edelman의 기술적 보호조치를 무력화할 수 있는 도구를 배포한 행위에 관한 위법성 여부를 가리지는 않았지만, 이 사례는 과거의 사례들과는 중요한 점에서 차이를 보이고 있다. 기존의 DMCA를 위반한 기술적 보호조치의 무력화 도구들은 단순히 저작물을 무단복제하기 위해서 고안된 것들이지만 이 사안에서 문제가 된 Edelman의 무력화 도구는 필터링 소프트웨어의 오류를 수정할 뿐만 아니라 사용자에게 이익을 줄 수 있다는 점에서 차이가 있다.

Ⅳ. 한 · 미 FTA 이행법안 검토

1. 접근통제의 수용

한 · 미 FTA와 그 이전의 통상협상에서 미국이 끊임없이 제기해왔고, 또 금번 협상에서 미국 측이 한 치의 양보도 않겠다는 사안이 바로 접근통제권의 인정이다. 한국 측은 접근통제형 기술적 보호조치에 대한 법적 보호를 하기로 합의하였는데, 그 이유로서 최근 온라인을 통한 불법 복제물 등의 유통이 급격하게 증가하여 저작권산업에 미치는 영향이 심각함에 따라 이에 대한 방안 마련이 필요하였고, 복제통제형 기술적 보호조치만으로는 이러한 불법복제의 확산을 규제하기에 한계가 이었기 때문이다. 접근통제적 기술조치를 추가함으로써 불법복제를 원천적으로 억제 · 방지할 수 있는 길이 열렸고, 나아가 거래비용의 감소와 자동화된 권리관리체계와의 결합을 통해 저작물 이용을 더욱 용이하게 할 수 있게 되었다.[95]

그러나 지나친 접근통제 조치는 공정하게 저작물을 이용하려는 사람들까지 접근을 제한하게 되어 저작물의 공정한 이용을 저해할 우려가 있으므로 접근통제권에 대한 예외조항을 구체적으로 열거할 필요가 있다. 저작권법은 문화의 발전이라는 근본적인 목적을 달성하기 위하여 창작물의 표

95) 김현철, 한미 FTA 이행을 위한 저작권법 개정 방안 연구, 저작권위원회, 2007, 109-110면.

현은 보호하고 아이디어는 창작활동의 기초도구로서 누구나 활용할 수 있도록 만인의 공유(public domain)로 두었다.[96] 그런데 이러한 저작물의 접근통제권은 저작물에 녹아 있는 아이디어에 대한 접근 자체를 제한하게 되므로 저작권법상 보호하지 않는 아이디어까지 보호하게 되는 문제점이 있다.[97] 실제 이 문제는 한 · 미 FTA 협정문을 이행하기 위한 저작권법 개정안과 직접 관련된 것으로서 합리적인 예외조항의 도출이 이슈가 되고 있다.

2. 예외규정

접근통제에 관한 한 · 미 FTA 협상안은 미국의 DMCA를 모델로 하고 있는데, DMCA에서는 접근통제에 대한 예외를 저작권 침해에 대한 예외로서 공정이용(fair-use)과 별로도 규정하고 있다. 즉 DMCA는 접근통제를 무력화할 수 있는 법적 근거로서 미국 저작권법상 공정이용법리(fair-use doctrine)를 적용하지 못하도록 하고 있다. 금번 협상안에서도 아래 표에서 보는 바와 같이 기술적 보호조치에 대한 예외를 저작권제한사유와 구별하여 규정함으로써 저작권제한사유와 기술적 보호조치를 연계시키지 않고 있다.

그런데 이러한 접근방법에 대해 미국 내에서도 공정이용을 과도하게 위축시킨다는 비판이 강력히 제기되고 있다. 한 · 미 FTA 이행법안에서도 동일한 문제에 직면하고 있으며 저작권제한사유와의 연계 또는 추가적인 예외규정에 대한 논의가 필요한 때라고 본다.

〈한 · 미 FTA의 기술적 보호조치에 대한 예외〉

	접근통제 무력화 금지	접근통제 도구의 거래행위 금지	복제통제 무력화 도구의 거래금지
역분석[§ 18.4.7(d)(i)]	O	O	O
암호화연구[§ 18.4.7(d)(ii)]	O	O	X
청소년 보호[§ 18.4.7(d)(iii)]	O	O	X
안전성 검사[§ 18.4.7(d)(iv)]	O	O	X
개인정보보호[18.4.7(d)(v)]	O	X	X
법집행[§ 18.4.7(d)(vi)]	O	O	O
비영리 도서관 등[§ 18.4.7(d)(vii)]	O	X	X
규칙제정의 의한 예외[§ 18.4.7(d)(viii)]	O	X	X

96) 이를 표현과 아이디어의 이분법(expression-idea dichotomy)이라고 한다. 저작권법에 의해 보호받는 저작물은 인간의 사상 또는 감정을 창작적으로 표현한 것이며, 그 표현의 기초가 되는 아이디어는 창작활동을 위해 누구나 이용할 수 있는 공중의 영역(public domain)에 놓여 있다.

97) 손승우, 한미 FTA와 지적재산권의 미래 -저작권 협상을 중심으로-, 「국제거래법연구」제15집제2호 (2006), 79면.

한 · 미 FTA 협상에서 합의한 기술적 보호조치에 대한 예외와 이를 이행하기 위해 마련한 저작권법 개정안의 내용이 다소 상이하여 문제의 소지가 있다. 예컨대, 암호화연구를 위한 접근통제의 무력화 예외로서 개정안에서는 한미 FTA 협정문에서 규정하고 있는 '권리자로부터 사전 허락을 얻기 위한 노력', '연구자의 자격', '선의' 등에 관한 요건을 규정하고 있지 않다. 즉 협정문에서는 "복제물, 고정되지 아니한 실연, 또는 저작물 · 실연 또는 음반의 현시물을 적법하게 획득하였고 선의의 비침해 행위에 대한 허락을 얻기 위하여 선의의 노력을 하였고, 적절한 자격을 갖춘 연구자에 의하여 정보의 스크램블 및 디스크램블을 위한 기술의 흠결 및 취약성을 확인하고 분석하는 것으로 구성된 연구 목적을 위해서만 필요한 한도에서 수행된 선의의 비침해 행위"를 예외로서 규정하고 있는 반면, 이행법안에서는 "저작물등의 복제물을 정당하게 이용하는 자가 저작물등에 적용된 암호 기술의 결함이나 취약점을 조사 · 연구하기 위하여 필요한 범위에서 행하는 경우"로만 규정하고 있다.

또한 한미 FTA 협정문상의 '안전성 검사'에 관한 규정[98]은 이행법안에 포함되어 있지 않아 협정문의 충실한 이행을 담보하지 못하고 있다. 협정문에서는 기술적 보호조치의 무력화의 예외로서 "컴퓨터, 컴퓨터 시스템 또는 컴퓨터 네트워크의 보안성을 검사 · 조사 또는 보정하는 것을 유일한 목적으로 컴퓨터, 컴퓨터시스템 또는 컴퓨터 네트워크의 소유자에 의해서 승인된 선의의 비침해 행위"로 규정하고 있다.

한편 프로그램코드 역분석(SW Reverse Engineering)과 관련해서는 보다 큰 문제를 지니고 있다. 통합 저작권법 제101조의4에서 "정당한 권한에 의하여 프로그램을 이용하는 자 또는 그의 허락을 받은 자는 호환에 필요한 정보를 쉽게 얻을 수 없고 그 획득이 불가피한 경우에는 해당 프로그램의 호환에 필요한 부분에 한하여 프로그램의 저작재산권자의 허락을 받지 아니하고 프로그램코드역분석을 할 수 있다."라고 규정하고 있는데, 이는 기존 컴퓨터프로그램보호법 제12의2에 있는 규정이 그대로 저작권법 제5장의2 프로그램에 관한 특례에 신설된 것이다.

그런데 역분석에 관한 이 규정은 DMCA 제1201조(f)(reverse engineering)와 유럽연합 지침 제6조(Decompilation)의 영향을 받은 것인데, 흥미로운 것은 미국 DMCA에서는 접근통제를 위한 기술적 보호조치를 무력화할 수 있는 근거로서 '호환성 목적'의 역분석을 예외로서 인정하고 있다. 그런데 현행 저작권법의 호환목적의 역분석에 관한 규정(제101조의4)은 기술적 보호조치와는 관계없이 일정한 역분석만을 인정하고 있어 DMCA와는 상이함을 알 수 있다.

98) 한 · 미 FTA 협정문 §18.4.7(d)(iv) "컴퓨터, 컴퓨터 시스템 또는 컴퓨터 네트워크의 보안성을 검사 · 조사 또는 보정하는 것을 유일한 목적으로 컴퓨터, 컴퓨터 시스템 또는 컴퓨터 네트워크의 소유자에 의하여 승인된 선의의 비침해 행위"

또한 이와 같이 DMCA가 기술적 보호조치를 회피할 수 있는 근거로서 호환성 목적의 일정한 역분석만을 인정하고 있는 반면 일반적인 역분석 행위는 공정이용법리(fair-use doctrine)에 의해 허용되고 있다. 반면 우리나라 저작권법에서는 프로그램 저작재산권의 제한에 관한 규정(제101조의3)과 호환목적의 역분석에 관한 규정(제101조의4)을 분리하여 규정함으로써 역분석 행위에 대해서는 제101조의3은 적용되지 않고 후자만이 적용되도록 하였다. 따라서 미국에서 일반적으로 인정될 수 있는 역분석 행위라도 우리나라에서는 허용되지 않을 수 있다. 현행 저작권법 제101조의4는 접근통제와는 무관하게 역분석을 호환목적으로만 허용하고 있어 산업전반에서 유용하게 활용되고 있는 일반적인 역분석을 제한할 여지를 가지고 있다.

따라서 프로그램저작권 제한에 관한 제101조의3 제1항 제6호에서 "프로그램의 기초를 이루는 아이디어 및 원리를 확인하기 위하여 프로그램의 기능을 조사?연구?시험할 목적으로 복제하는 경우"를 규정하고 있는데, 이는 향후 접근통제에 관한 규정이 도입되었을 때 일반적인 역분석 행위에 적용될 수 있도록 하고 제101조의4를 기술적 보호조치의 무력화의 예외로서 규정하는 것이 바람직하다고 본다.[99]

한편 협정문에서 청소년 보호와 관련된 예외로서는 부적절한 온라인 콘텐츠에 미성년자가 접근하는 것을 방지하는 것을 유일한 목적으로 하는 무력화 행위를 인정하고 있다. 이는 음란물 등 청소년 유해물에 대한 접근을 차단하기 위해 시민단체나 도서관 그룹 등에 의해 이루어질 수 있는 무력화 활동을 정책적으로 뒷받침하기 위해 인정하였다. 또한 개인의 온라인상의 행위를 파악할 수 있는 개인 식별 정보를 비공개적으로 수집하거나 배포하는 기능을 확인하고 이를 방지하기 위하여 필요한 경우 무력화를 허용하고 있다. 청소년 보호와 마찬가지로 이 경우에도 무력화 도구의 유포, 전송 등 행위는 인정되지 않는다.

그 밖에 정부가 법 집행, 정보수집 또는 안전보장 등을 위하여 필요한 경우, 그리고 교육기관, 비영리도서관, 기록보관소 등이 기술적 보호조치를 무력화하지 아니하고는 접근할 수 없는 저작물 등의 구입 여부를 결정하기 위하여 필요한 경우에 무력화를 인정하고 있다. 전자의 목적을 위해서는 무력화뿐만 아니라 무력화 도구의 거래행위도 인정하고 있다.

앞서 언급한 바와 같이, 기술적 보호조치의 무력화금지에 대해서는 저작권제한 사유에 해당하는 정도의 예외 규정이 필요한데,[100] 현재 협정문에서 열거하고 있는 8가지 예외만으로는 접근통제권에 대한 충분한 안정장치가 될 수 없다고 본다. 이러한 측면에서 협상안에서는 3년 마다 기술적 보호조

99) 손승우, "인터넷상의 저작물 불법유통에 대한 규제방안"[발제: 김병일]에 대한 토론문, 개인정보 및 웹사이트 규제의 법적문제, 한국정보보호진흥원 · 단국대학교 법학연구소 공동개최 학술세미나, 2009.7.16., 155면 참조.

100) 김병일 외 3인, 위조 및 불법복제방지조약(ACTA) 협상 대응방안, 문화체육관광부, 2009.4., 249-250면.

치에 대한 예외를 검토하고 미국에 통보도록 규정하고 있다. 현실적으로 협상의 이행초기라는 점을 감안하면 접근통제권의 제공으로부터 이용자의 권익이 위축되지 않도록 예외조항을 점차로 확대해 나가도록 하되 장기적으로는 저작권 제한사유와의 연계를 모색하고 아울러 저작권 제한 사유로서 포괄적인 공정이용(fair-use) 규정의 도입을 적극적으로 검토하는 것이 바람직하다고 본다.

제6장

SW 역분석과 기술적보호조치의 관계 분석

제6장 SW 역분석과 기술적보호조치의 관계 분석

강기봉 선임연구원(한국소프트웨어저작권협회)

Ⅰ. 기본적 관계

저작권의 보호와 기술적 보호조치의 무력화의 금지는 독립적인 것으로 저작권법상 중첩적인 보호 체계라고 할 수 있다.[101] 따라서 기술적 보호조치의 무력화가 금지되어 있다고 가정하는 경우에 기술적 보호조치를 무력화할 수 있는 권한이 있는 경우나 기술적 보호조치 규정에 예외 규정이 존재하는 경우가 아니라면, 원칙적으로 저작재산권이 제한되는 경우 등 이용자가 저작권을 침해하지 않고 저작물을 이용할 수 있는 경우에도 기술적 보호조치를 무력화할 수 없다. 이러한 관계는 한국, 미국,[102] EU 등의 법률에서 동일하게 적용된다.

1. 저작권과 기술적 보호조치의 중첩적 보호의 배경

저작권법은 저작자의 저작인격권과 저작재산권을 보호한다. 즉, 저작권법의 보호의 객체는 기본적으로 저작자가 저작한 저작물에 대한 권리이다. 그러나 인터넷 및 컴퓨터 기술의 발전에 따라 저작물이 디지털 형태로 복제되는 것이 용이해지고, 이에 따른 저작권 침해가 범람했다. 이러한 배경에서 저작권자들은 저작권법의 개정을 통한 저작권 강화를 요구하면서, 저작물에 기술적 보호조치를 함에 의해 자구적인 노력을 도모하였다.

그러나 이러한 노력에도 불구하고 기술적 보호조치에 대한 무력화 내지 우회 기술 또한 개발되었고, 이에 따라 기술적 보호조치가 무력화될 수 있게 되었다. 그리고 기술적 보호조치에 관한 기술이 발전하는 속도만큼이나 이를 우회하는 기술의 개발 속도도 빨라졌다. 따라서 단순히 기술적 보호조치의 개발에만 의존하지 않고, 저작권법에 기술적 보호조치의 우회를 금지하도록 규정하여 저작권의 침해를 방지하기 위한 조치를 취하게 되었다.

101) 저작권자가 저작권법에 의한 보호, 기술적 보호조치에 의한 보호(곧 기술적 보호조치 자체에 의한 저작권의 보호, 기술적 보호조치의 우회금지의 3중의 보호를 받을 수 있게 된다는 견해(이대희, "기술적 보호조치의 범위 설정 – 대법원 2004도2743 컴퓨터프로그램보호법위반–", 계간 저작권 제74호(2006 여름호), 저작권심의조정위원회, 2006,6, 46-47면)가 있다.

102) THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 : U.S. Copyright Office Summary, Copyright Office, 1998.12, 4면. 〈http://www.copyright.gov/legislation/dmca.pdf〉 : This distinction was employed to assure that the public will have the continued ability to make fair use of copyrighted works. Since copying of a work may be a fair use under appropriate circumstances, section 1201 does not prohibit the act of circumventing a technological measure that prevents copying. By contrast, since the fair use doctrine is not a defense to the act of gaining unauthorized access to a work, the act of circumventing a technological measure in order to gain access is prohibited.

이것이 명시적으로 저작권법에 반영된 것은 미국의 DMCA(The Digital Millennium Copyright Act of 1998)의 제정을 통한 저작권법의 개정, EU의 관련 EU 지침의 제정, 한국, 일본 등의 법률에의 관련 규정의 도입 등을 들 수 있다.

그런데 복제통제 기술적 보호조치가 필연적으로 복제와 관련이 있는 것과 달리 접근통제 기술적 보호조치의 경우에는 저작재산권과는 직접적인 관련성이 없다. 접근통제 기술적 보호조치는 저작물의 이용자들이 저작물에 접근하는 것을 통제하는 것이고, 이는 곧 접근권(access right)[103]이라는 개념과 연결된다. 즉, 복제, 배포 등의 저작재산권의 개념과는 다른 새로운 개념이 저작권법 체계에 편입된 것이다.[104] 이러한 접근권에 대한 논의는 미국 DMCA에 접근통제 기술적 보호조치 규정이 도입되면서 지속적으로 화두가 되어 왔다. 그리고 우리나라도 한 · 미 FTA가 비준이 되면 개정법에서 이러한 접근통제 기술적 보호조치가 도입될 예정이다.

따라서 기술적 보호조치는 법률 규정에 따라 별도로 보호가 가능하다. 다만, 현행 저작권법이 복제통제 기술적 보호조치와 관련한 규정을 두면서도 그 무력화 행위 자체를 규제하지 않고, 한 · 미 FTA 이행을 위한 저작권법 개정안(이하 "한 · 미 FTA 저법 이행법안"이라 한다)과 한 · 미 FTA 이행을 위한 컴퓨터프로그램 보호법 개정안(이하 "한 · 미 FTA 컴법 이행법안"이라 한다)[105]에도 복제통제 기술적 보호조치의 무력화 행위는 규정되어 있지 않은데, 이러한 복제통제 기술적 보호조치의 무력화 행위는 복제를 수반하므로 복제권 침해 여부로써 규제될 수 있을 것이다.

2. 기술적 보호조치 저작물에 대한 저작권 제한 규정의 적용 가능성

기술적 보호조치가 되어 있는 저작물에 대해 저작권자의 저작재산권이 제한되는 것은 우선 기술적 보호조치의 무력화 행위가 선행될 것을 전제로 한다. 그리고 이후에 복제, 배포 등의 행위가 저작재산권의 제한 대상이 된다.

103) 접근권(access right)이라는 개념은 디지털환경에서 기술적 보호조치에 관한 입법이 이루어지기 전과는 달리, 디지털 환경으로 변화하여 저작물의 이용행태도 소유보다는 이용으로 변화하고 출판자나 저작자들이 경제적 이익을 지키기 위해 기술적 보호조치로 접근을 통제하게 되면서 저작권자가 '복제물의 접근을 통제하고 제한하는 권리'로 의미가 바뀌게 되었다. 즉, 과거에는 복제나 배포 등의 이용행위만을 저작권법의 대상으로 삼았지만 디지털 시대로 변화하면서 최종소비자인 일반인이 저작물을 읽거나 듣고 보는 행위까지 통제하는 권리를 저작자에게 부여하게 된 것이다.: 최진원 · 남형두, 매체기술의 변화와 저작권법: 그 도전과 응전의 역사, 커뮤니케이션 이론 제2권-제2호(2006년 겨울), 한국언론학회, 2006, 157-158면.

104) 전자 담장과 같이 접근통제를 위한 기술적 보호조치에 의하여 저작권이 포기되거나 저작권의 보호범위를 벗어나거나 저작권의 존속기간이 만료된 자료 등 일반인의 공유영역에 있는 자료를 봉쇄할 수 있게 된다. 곧 접근권의 인정에 의하여 존속기간의 제한이 있는 저작권이 영구적인 권리가 될 수 있으며, 미국 법원이 해석하는 바와 같이 기술적 보호조치에 대하여 공정이용의 예외가 인정되지 않음으로써 저작권을 특허권과 같은 권리가 되도록 할 수 있다. 따라서 접근권에 의하여 저작권자가 하나의 배타적인 권리를 부여받는 것에 한정되는 것이 아니라 저작권이 확대 · 강화되고, 저작권법이 설정해 놓은 공유영역(publice domain)은 저작권자 개인에 의하여 무용지물이 될 수 있으며, 공기와 같이 누구나 이용할 수 있는 정보 및 자료에 대하여 저작권자를 위한 재산권이 창조된다.: 이대희, "디지털환경에서의 접근권의 인정에 관한 연구", 창작과권리 제34호(2004년 봄호), 2004.3, 114면.

105) 현행 저작권법의 시행 이전에 저작권법 및 컴퓨터프로그램 보호법의 개정 법률이 국회에 제출되어 있는 상태인데, 이 법률안들에는 공히 한 · 미 FTA 협정문의 내용이 그대로 반영되어 기술적 보호조치 관련한 규정이 미국의 저작권법 체계에 따라 규정되어 있다.

그런데, 만약 기술적 보호조치의 무력화 내지 우회를 금지하는 내용이 저작권법에 규정되어 있다면, 기술적 보호조치를 무력화하고 저작물에 접근하거나 저작물을 복제하는 것은 저작권 제한 여부와 관계없이 금지가 된다. 왜냐하면 상기한 바와 같이 저작권 보호와 기술적 보호조치에 대한 보호는 각각 독립적으로 이뤄지기 때문이다.

그러므로 기술적 보호조치의 무력화 내지 우회 규정에 저작권 제한에 관한 예외 규정이 없다면, 원칙적으로는 저작권 제한 규정이 적용될 수 있는 여지는 없게 된다. 따라서 이와 관련하여 저작권자의 권리에 대한 중첩적 보호가 이뤄지게 된다.

그리고 이와 관련하여 2009년 7월 23일 폐지된 컴퓨터프로그램 보호법(이하 "구컴퓨터프로그램 보호법"이라 한다) 제30조에 기술적 보호조치 규정에는 복제통제 기술적 보호조치의 무력화 금지에 대한 예외로써 저작재산권 제한을 포함하여 규정하고 있었다. 그러나 한 · 미 FTA 저법 이행법안 및 한 · 미 FTA 컴법 이행법안에는 접근통제 기술적 보호조치의 무력화 금지에 대한 예외를 규정하고 있으면서도, 저작재산권 제한과 관련하여서는 예외로써 규정하고 있지는 않다.

3. 저작권법상 두 규정의 관계

구컴퓨터프로그램보호법은 복제통제 기술적 보호조치의 무력화에 대해 금지 규정이 존재하였지만, 현행 저작권법의 경우에는 해당 규정은 존재하지 않는다.[106]

따라서 직접적으로 저작권과 기술적 보호조치를 중첩적으로 보호함에 따른 문제는 현재로써는 없다고 할 수 있다. 다만, 기술적 보호조치를 제거 · 변경 · 우회하는 등 무력화하는 것을 주된 목적으로 하는 기술 · 서비스 · 제품 · 장치 또는 그 주요 부품을 제공 · 제조 · 수입 · 양도 · 대여 또는 전송하는 행위를 침해로 보고 이를 규제하고 있을 뿐이다(제124조제2항).

그러나 향후 한 · 미 FTA 이행법안들[107]이 국회를 통과하면 이야기가 달라진다. 비록 복제통제 기술적 보호조치의 무력화에 대한 금지 규정은 없지만, 접근통제 보호조치의 무력화에 대한 금지 규정이 신설되기 때문이다.

106) 복제통제 기술적 보호조치의 무력화에 대한 금지 규정이 존재하지 않기 때문에 해당 무력화에 대한 규제가 직접적으로 이뤄지지 않지만, 이것의 무력화에는 복제가 수반되기 때문에 문제는 결국 복제권 침해 여부로 귀결된다.

107) 컴퓨터프로그램 보호법과 저작권법의 통합에 따라 한 · 미 FTA 이행을 위한 법률안에 있어서도 향후 컴퓨터프로그램 보호법이 저작권법에 통합된 새로운 개정법률안이 국회에 제출될 것으로 보인다.

4. 기술적 보호조치 규정과 프로그램코드역분석에 대한 예외

현행 저작권법에는 복제통제든 접근통제든 기술적 보호조치의 무력화를 금지하는 규정이 없다. 따라서 두 규정의 관계를 논하는 것은 사실상 의미가 없다고도 할 수 있다.

그런데 구컴퓨터프로그램보호법과 한 · 미 FTA 협정에서는 기술적 보호조치 규정에 예외 규정을 두고 있었다. 전자의 경우 제30조[108]에 복제통제 기술적 보호조치의 무력화를 금지하는 규정을 두면서, 해당 규정에 프로그램의 동일성 변경, 저작재산권의 제한, 프로그램 사용자의 필요한 범위 안에서의 복제, 프로그램코드역분석, 프로그램의 수정 · 보완, 암호화 분석 등 이용자의 정당한 이용을 보장하도록 예외 사항들을 함께 규정하고 있었다.

그리고 한 · 미 FTA 협정의 기술적 보호조치 관련 규정은 미국과 같은 구조를 하고 있고, 접근통제 기술적 보호조치의 무력화의 금지 및 그 예외가 규정되어 있다. 그리고 그 예외로써 프로그램코드역분석, 암호화 기술의 조사 · 연구, 보안성의 검사 · 조사 또는 보정 등 여러 가지 이유로 필요한 사항들에 대해 기술적 보호조치를 우회할 수 있는 몇 가지를 규정한다. 따라서 해당 예외의 몇 가지만을 제외한 기타의 무력화 행위는 금지된다. 그리고 이 협정 내용은 한 · 미 FTA 저법 이행법안 및 한 · 미 FTA 컴법 이행법안에 반영되었다.

5. 온라인 디지털콘텐츠산업 발전법의 기술적 보호조치 규정

가. 온라인 디지털콘텐츠산업 발전법의 보호 범위

온라인 디지털콘센츠산업 발전법은 온라인디지털콘텐츠산업의 발전에 필요한 사항을 정함으로써 온라인디지털콘텐츠산업의 기반을 조성하고 그 경쟁력을 강화하여 국민생활의 향상과 국민경제의 건전한 발전에 이바지함을 목적으로 한다.[109]

108) 폐지된 컴퓨터프로그램 보호법 제30조 (기술적보호조치의 침해 등의 금지)
① 누구든지 정당한 권원없이 기술적보호조치를 회피, 제거, 손괴 등의 방법으로 무력화(이하 "기술적보호조치무력화"라 한다)하여서는 아니된다. 다만, 다음 각호의 1에 해당하는 경우에는 그러하지 아니하다. 〈개정 2001.1.16〉
1. 제10조의 규정에 의한 프로그램의 동일성을 변경하는 경우
2. 제12조 각호의 1에 해당되어 복제 사용하는 경우
3. 제14조의 규정에 의한 프로그램 사용자가 필요한 범위안에서 복제하는 경우
4. 정당한 권원에 의하여 사용하는 자가 다른 프로그램과 호환성을 유지하기 위하여 필요한 경우
5. 정당한 권원에 의한 최종사용자로부터 프로그램의 수정 · 보완을 요청받은 경우
6. 정당한 권원에 의하여 사용하는 자가 연구 · 교육 등의 목적으로 프로그램과 관련된 암호화 분석을 하기 위하여 필요한 경우
② 누구든지 상당히 기술적보호조치를 무력화하는 기기 · 장치 · 부품 등을 제조 · 수입하거나 공중에 양도 · 대여 또는 유통하여서는 아니되며, 기술적보호조치를 무력화하는 프로그램을 전송 · 배포 기술적보호조치를 무력화하는 기술을 제공하여서는 아니된다.

109) 온라인 디지털콘텐츠산업 발전법
제1조 (목적) 이 법은 온라인디지털콘텐츠산업의 발전에 필요한 사항을 정함으로써 온라인디지털콘텐츠산업의 기반을 조성하고 그 경쟁력을 강화하여 국민생활의 향상과 국민경제의 건전한 발전에 이바지함을 목적으로 한다.

그리고 디지털콘텐츠는 부호 · 문자 · 음성 · 음향 · 이미지 또는 영상 등으로 표현된 자료 또는 정보로서 그 보존 및 이용에 있어서 효용을 높일 수 있도록 전자적 형태로 제작 또는 처리된 것을 말하는데, 자료 또는 정보는 저작권법상 저작물일 필요는 없다.

또한 온라인디지털콘텐츠산업[110]은 정보통신망이용촉진및정보보호등에관한법률 제2조제1항제1호[111]의 규정에 의한 정보통신망에서 사용되는 디지털콘텐츠의 수집 · 가공 · 제작 · 저장 · 검색 · 송신 등과 이와 관련된 서비스를 행하는 산업이다.

따라서 이 법률은 정보통신망을 통해 디지털콘텐츠와 관련된 서비스를 행하는 자들을 보호하는 것이고, 따라서 보호대상이 저작물에 한정되어 있지 않다. 그러나 이런 이유로 이 법률에 의한 저작물 관련 보호의 범위도 정보통신망 관련 디지털콘텐츠에 한정되어 있다.

나. 저작권법과의 관계

제21조에는 다른 법률과의 관계를 규정하여 "온라인콘텐츠제작자[112]가 「저작권법」의 보호를 받는 경우에는 「저작권법」이 이 법에 우선하여 적용된다."고 규정하고 있다. 따라서 저작권법이 적용되는 사항에 대해서는 이 법은 적용되지 않는다. 즉, 온라인디지털콘텐츠제작자가 곧 저작권자인 경우에는 그는 그의 저작권을 근거로 저작권법에 의한 보호를 받게 된다.

그러나 디지털콘텐츠의 제작자가 저작권자일 필요도 없고, 디지털콘텐츠가 저작물이어야 할 필요도 없다. 따라서 이런 경우에는 저작권법이 개입되지 않을 것이고 온라인디지털콘텐츠을 발전법은 그 독자적인 지위를 갖게 된다.

---

110) 온라인 디지털콘텐츠산업 발전법
제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. "디지털콘텐츠"라 함은 부호 · 문자 · 음성 · 음향 · 이미지 또는 영상 등으로 표현된 자료 또는 정보로서 그 보존 및 이용에 있어서 효용을 높일 수 있도록 전자적 형태로 제작 또는 처리된 것을 말한다.
2. "온라인디지털콘텐츠"라 함은 정보통신망이용촉진및정보보호등에관한법률 제2조제1항제1호의 규정에 의한 정보통신망(이하 "정보통신망"이라 한다)에서 사용되는 디지털콘텐츠를 말한다.
3. "온라인디지털콘텐츠산업"이라 함은 온라인디지털콘텐츠를 수집 · 가공 · 제작 · 저장 · 검색 · 송신 등과 이와 관련된 서비스를 행하는 산업을 말한다.

111) 정보통신망 이용촉진 및 정보보호 등에 관한 법률
제2조 (정의)① 이 법에서 사용하는 용어의 뜻은 다음과 같다.
1. "정보통신망"이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집 · 가공 · 저장 · 검색 · 송신 또는 수신하는 정보통신체제를 말한다.
전기통신기본법
제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. "전기통신"이라 함은 유선 · 무선 · 광선 및 기타의 전자적 방식에 의하여 부호 · 문언 · 음향 또는 영상을 송신하거나 수신하는 것을 말한다.
2. "전기통신설비"라 함은 전기통신을 하기 위한 기계 · 기구 · 선로 기타 전기통신에 필요한 설비를 말한다.

112) 제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
5. "온라인디지털콘텐츠제작"이라 함은 정보통신망에서 사용하기 위하여 디지털형태의 원정보를 가공하거나 디지털형태외의 원정보를 디지털방식으로 전환 또는 가공하는 것을 말한다.
6. "온라인디지털콘텐츠제작자"라 함은 온라인디지털콘텐츠 제작에 있어 그 전체를 기획하고 책임을 지는 자를 말하며 이들로부터 적법하게 그 지위를 양수한 자를 포함한다.

그런데 저작권법의 경우에는 기술적 보호조치를 "저작권 그 밖에 이 법에 따라 보호되는 권리에 대한 침해 행위를 효과적으로 방지 또는 억제하기 위하여 그 권리자나 권리자의 동의를 얻은 자가 적용하는 기술적 조치를 말한다"고 정의하고 있다. 즉, 기술적 보호조치의 적용 주체가 저작권자나 저작권자의 동의를 얻은 자이다.

그리고 온라인 디지털콘텐츠산업 발전법에는 기술적보호조치를 "온라인디지털콘텐츠제작자가 이 법에 의하여 보호되는 이익의 침해를 효과적으로 방지하기 위하여 적용하는 기술 또는 장치를 말한다"고 정의되어 있다. 즉, 기술적 보호조치을 적용하는 주체가 온라인디지털콘텐츠제작자이다.

따라서 기술적 보호조치의 주체가 같은 경우에는 저작권법, 다른 경우에는 각각 저작권법 및 온라인 디지털콘텐츠산업 발전법을 적용하면 된다.

다. 금지규정 및 기술적 보호조치 규정

제18조에는 금지규정등을 규정하고 있는데, 제1항에 "누구든지 정당한 권한없이 타인이 상당한 노력으로 제작하여 표시한 온라인콘텐츠의 전부 또는 상당한 부분을 복제 또는 전송하는 방법으로 경쟁사업자의 영업에 관한 이익을 침해하여서는 아니된다. 다만, 온라인콘텐츠를 최초로 제작하여 표시한 날부터 5년이 경과한 때에는 그러하지 아니하다."라고 규정되어 있다. 이에 따라, 온라인콘텐츠의 전부 또는 상당한 부분을 최초로 제작하여 표시한 날부터 5년이 경과하기 전에는 복제 또는 전송에 의해 경쟁사업자의 영업에 관한 이익을 침해해서는 안 된다. 그런데 이 규정은 "경쟁사업자의 영업에 관한 이익"을 침해하는 것을 금지하고 있기 때문에, 사업자간 부정경쟁을 금지하는 것으로 해석할 수 있기 때문에 제1항의 적용 대상은 사업자에 한정된다고 볼 수 있다.

그리고 "누구든지 정당한 권한없이 제1항 본문의 행위를 효과적으로 방지하기 위하여 온라인콘텐츠제작자나 그로부터 허락을 받은 자가 디지털콘텐츠에 적용한 기술적보호조치의 회피 · 제거 또는 변경(이하 "무력화"라 한다)을 주된 목적으로 하는 기술 · 서비스 · 장치 또는 그 주요부품을 제공 · 수입 · 제조 · 양도 · 대여 또는 전송하 기술양도 · 대여를 위하여 전시하는 행위를 하여서는 아니된다. 다만, 기술적보호조치의 연구 · 개발을 위하여 기술적보호조치를 무력화하는 장치 또는 부품을 제조하는 경우에는 그러하지 아니하다."라고 규정되어 있다. 이에 따라 기술적보호조치의 무력화를 주된 목적으로 하는 기술 · 서비스 · 장치 또는 그 주요부품을 제조, 유통 등을 해서는 안 된다. 그리고 그 행위의 주체를 "누구든지"로 규정하고 있어 제2항의 적용대상은 사업자가 아니고 누구라도 상관이 없다.

그런데, 제10호의 기술적 보호조치 정의 규정은 "기술적보호조치라 함은 온라인디지털콘텐츠제작자가 이 법에 의하여 보호되는 이익의 침해를 효과적으로 방지하기 위하여 적용하는 기술 또는

장치를 말한다."라고 규정되어 있다. 저작권법의 정의 규정과 그다지 차이가 없어 보이지만,[113] 이 규정은 복제통제 뿐만 아니라 접근통제 기술적 보호조치도 포함하는 것으로 보거나 규정을 보다 명확하게 개정하는 것이 바람직할 것으로 보인다. 왜냐하면 제18조제1항의 금지행위는 복제와 전송 행위밖에 없는데, 이와 관련하여 경쟁사업자의 이익을 침해하는 방법에는 접근통제를 무력화하고 디지털콘텐츠의 온라인 주소를 복제하여 제공하는 등 접근통제 기술적 보호조치와 관련된 문제들이 있을 수 있기 때문이다.

라. 기술적 보호조치와 프로그램코드역분석

온라인디지털콘텐츠산업발전법에는 기술적 보호조치의 무력화 금지 및 프로그램코드역분석 규정은 존재하지 않는다. 따라서 프로코드역분석과 기술적 보호조치 규정의 상관관계를 논할 수 있는 근거는 없다. 게다가 이것의 경우에는 프로그램코드역분석 규정이 있다고 하더라도 소프트웨어 저작자의 저작권을 침해하는 것으로써 결국 저작권법의 규제를 받게 되므로 의미가 없었을 것이다.

다만, 온라인디지털콘텐츠산업발전법에 의해서 1차적으로 보호되고, 2차적으로 저작권법 침해 여부를 논한다고 했을 때에는 저작권법 차원에서 이를 논할 수는 있을 것이다.

Ⅱ. 저작권법상의 관계

저작권법의 기술적 보호조치 규정은 복제통제 기술적 보호조치를 제거 · 변경 · 우회하는 등 무력화하는 것을 주된 목적으로 하는 기술 · 서비스 · 제품 · 장치 또는 그 주요 부품을 제공 · 제조 · 수입 · 양도 · 대여 또는 전송하는 행위를 침해로 보는 행위로써 금지하는 규정만 존재한다. 그리고 호환성에 필요한 정보를 얻기 위한 프로그램코드역분석을 별도의 규정으로 허용하고 있다. 따라서 우리 현행 저작권법상 기술적 보호조치 규정과 프로그램코드역분석 규정이 충돌할 수 있는 여지는 사실상 없다.

113) 온라인디지털콘텐츠산업발전법상의 정의
제2조 10. "기술적보호조치"라 함은 온라인디지털콘텐츠제작자가 이 법에 의하여 보호되는 이익의 침해를 효과적으로 방지하기 위하여 적용하는 기술 또는 장치를 말한다.
저작권법상 정의
제2조 28. "기술적보호조치"는 저작권 그 밖에 이 법에 따라 보호되는 권리에 대한 침해 행위를 효과적으로 방지 또는 억제하기 위하여 그 권리자나 권리자의 동의를 얻은 자가 적용하는 기술적 조치를 말한다.
구컴퓨터프로그램보호법상의 정의
제2조 9. "기술적보호조치"라 함은 프로그램에 관한 식별번호 · 고유번호 입력, 암호화 기타 이 법에 의한 권리를 효과적으로 보호하는 핵심기술 또는 장치 등을 통하여 프로그램저작권을 보호하는 조치를 말한다.

1. 기술적 보호조치 관련 규정

저작권법상 기술적 보호조치의 정의는 복제통제 기술적 보호조치만을 의미한다.[114] 법 제2조 정의 규정은 "기술적보호조치는 저작권 그 밖에 이 법에 따라 보호되는 권리에 대한 침해 행위를 효과적으로 방지 또는 억제하기 위하여 그 권리자나 권리자의 동의를 얻은 자가 적용하는 기술적 조치를 말한다."라고 되어 있다. 그런데 이 규정에는 '저작권 그 밖에 이 법에 따라 보호되는 권리에 대한 침해 행위'를 그 대상으로 하고 있어서(복제통제 기술적 보호조치) '저작물에 대한 접근'을 대상으로 하고 있는 접근통제 기술적 보호조치를 포함하고 있지 않는다고 해석된다.[115]

그리고 기술적 보호조치의 무력화를 직접 금지하는 규정은 존재하지 않고 간접적으로 "기술적 보호조치"를 제거 · 변경 · 우회하는 등 무력화하는 것을 주된 목적으로 하는 기술 · 서비스 · 제품 · 장치 또는 그 주요 부품을 제공 · 제조 · 수입 · 양도 · 대여 또는 전송하는 행위를 침해로 간주하는 규정만 존재한다(법 제124조 제2항).

이외에 불법 복제물의 수거 · 폐기 및 삭제에 관한 규정인 제133조[116]와 정보통신망을 통한 불법복제물등의 삭제명령 등을 규정한 제133조의2 제1항[117]에도 기술적 보호조치와 관련된 규정이 있다. 이들은 침해로 간주되는 사항들에 대해 수거 · 폐기 및 삭제를 하도록 하거나 행정적 조치를 취하도록 하는 것으로 침해의 내용을 규정하는 것은 아니다.

2. 프로그램코드역분석 규정

가. 규정 내용

프로그램코드역분석에 대한 규정은 제2조 제34호의 정의 규정과 제101조의4의 프로그램코드역분석 규정만 존재한다. 프로그램코드역분석은 EU의 COUNCIL DIRECTIVE of 14 May 1991 on

114) 정상조 편, 「저작권법 주해」, 박영사, 2007.12, 170-171면.

115) 구컴퓨터프로그램보호법의 기술적 보호조치 규정도 일반적으로는 복제통제 기술적 보호조치만을 의미한다고 보고 있음. 다만, 모드칩 사건(대법원 2006.2.24. 선고 2004도2743 판결)을 통해 이에 대한 논란이 있었는데, 구컴퓨터프로그램보호법의 기술적 보호조치 규정에 대해 복제통제 기술적 보호조치로 보면서도 기술적 보호조치의 범위를 법률상의 그것보다 확대하는 견해, 접근통제조치에 대한 보호를 규정한 것인지 여부가 모호한 것으로 보는 견해 등이 있었다고 한다.: 이규홍, "기술적 보호조치에 관한 소고", 정보법학 제11권 제1호, 한국정보법학회, 2007, 173면.

116) 제133조 (불법 복제물의 수거 · 폐기 및 삭제)㈜화체육관광부장관, 특별시장 · 광역시장 · 도지사 · 특별자치도지사 또는 시장 · 군수 · 구청장(자치구의 구청장을 말한다)은 저작권 그 밖에 이 법에 따라 보호되는 권리를 침해하는 복제물(정보통신망을 통하여 전송되는 복제물은 제외한다) 또는 저작물등의 기술적 보호조치를 무력하게 하기 위하여 제작된 기기 · 장치 · 정보 및 프로그램을 발견한 때에는 대통령령으로 정한 절차 및 방법에 따라 관계공무원으로 하여금 이를 수거 · 폐기 또는 삭제하게 할 수 있다.

117) 제133조의2 (정보통신망을 통한 불법복제물등의 삭제명령 등)① 문화체육관광부장관은 정보통신망을 통하여 저작권이나 그 밖에 이 법에 따라 보호되는 권리를 침해하는 복제물 또는 정보, 기술적 보호조치를 무력하게 하는 프로그램 또는 정보(이하 "불법복제물등"이라 한다)가 전송되는 경우에 위원회의 심의를 거쳐 대통령령으로 정하는 바에 따라 온라인서비스제공자에게 다음 각 호의 조치를 할 것을 명할 수 있다.
1. 불법복제물등의 복제 · 전송자에 대한 경고
2. 불법복제물등의 삭제 또는 전송 중단

the legal protection of computer programs (91/250/EEC)(이하 "EU 컴퓨터프로그램 지침[118]"이라 함)을 기초로 하여 마련된 것이다.[119] 이에 따라 법률의 구조도 EU 컴퓨터프로그램 지침의 것과 같다고 할 수 있을 것이다. 그리고 규정의 해석에 있어서도 EU 컴퓨터프로그램 지침을 참조할 수 있을 것이다.

우리 현행 저작권법 제2조 제34호의 정의 규정에는 "프로그램코드역분석은 독립적으로 창작된 컴퓨터프로그램저작물과 다른 컴퓨터프로그램과의 호환에 필요한 정보를 얻기 위하여 컴퓨터프로그램저작물코드를 복제 또는 변환하는 것을 말한다."라고 규정되어 있다.

그리고 법 제101조의4에는 제1항에 "정당한 권한에 의하여 프로그램을 이용하는 자 또는 그의 허락을 받은 자는 호환에 필요한 정보를 쉽게 얻을 수 없고 그 획득이 불가피한 경우에는 해당 프로그램의 호환에 필요한 부분에 한하여 프로그램의 저작재산권자의 허락을 받지 아니하고 프로그램코드역분석을 할 수 있다."라고 규정하여 프로그램코드역분석이 허용되는 사항을 규정하고 있고, 제2항에는 "제1항에 따른 프로그램코드역분석을 통하여 얻은 정보는 다음 각 호의 어느 하나에 해당하는 경우에는 이를 이용할 수 없다. 1. 호환 목적 외의 다른 목적을 위하여 이용하거나 제3자에게 제공하는 경우, 2. 프로그램코드역분석의 대상이 되는 프로그램과 표현이 실질적으로 유사한 프로그램을 개발 · 제작 · 판매하거나 그 밖에 프로그램의 저작권을 침해하는 행위에 이용하는 경우"라고 규정하여 프로그램코드역분석의 결과로써 얻은 정보의 이용 및 제3자에의 양도를 규제하고 있다.

일반적인 즉, 넓은 의미에서의 리버스 엔지니어링에 대해서는 정의규정을 두고 있지는 않지만, 일반적으로 제101조의3 제1항 제6호가 이러한 리버스 엔지니어링에 대한 규정으로 해석하고 있다. 이 규정에서 "프로그램의 기초를 이루는 아이디어 및 원리를 확인하기 위하여 프로그램의 기능을 조사 · 연구 · 시험할 목적으로 복제하는 경우"에 저작재산권을 제한하고 있는데, 이러한 행위를 일반적인 리버스 엔지니어링 의미하는 것으로 볼 수 있다. 즉 현행 저작권법상 리버스 엔지니어링이란 프로그램의 존재형태를 변경시키지 않고, 단지 이를 실행시킴으로써 그 아이디어나 원리를 파악하는 것을 의미한다.[120]

118) 본 지침은 EU 지침, EU 컴퓨터프로그램 지침, EU 프로그램 지침, EU 소프트웨어지침 등으로 칭해지고 있으나 원래 명칭에서 컴퓨터프로그램이 사용되고 있으므로, 여기에서는 EU 컴퓨터프로그램 지침으로 한다.

119) 안효질, "프로그램코드역분석 규정의 비교법적 분석-EU 소프트웨어지침을 중심으로-", 창작과권리 제47호(2007년 여름호), 세창출판사, 2007.6, 89면.

120) 안효질, "프로그램코드역분석 규정의 비교법적 분석-EU 소프트웨어지침을 중심으로-", 창작과권리 제47호(2007년 여름호), 세창출판사, 2007.6, 93면.

나. 규정의 문제점

현행 저작권법 제2조 제34호에서 프로그램코드역분석을 하는 것은 "복제" 또는 "변환"하는 행위와 관련되어 있다는 것을 알 수 있다. 그런데 프로그램코드역분석 과정에서 "복제"가 필연적으로 일어난다고 하더라도 "변환"은 저작권법상 어떤 권리로 인정해야 할 것인지는 명확하지 않다.

"변환"의 개념을 구컴퓨터프로그램보호법상 "개작" 내지 현행 저작권법상 "2차적저작물작성"으로 보기에는 무리가 있다.[121] 즉, 변환에 대해서 명시적인 규정 없이 2차적저작물작성[122]으로 보아 "번역 · 편곡 · 변형 · 각색 · 영상제작 그 밖의 방법으로 작성"한 경우에 해당한다고 할 수는 없다.

그런데 이것은 EU 컴퓨터프로그램 지침에서 저작권자의 권리에 변환을 포함하는 컴퓨터프로그램의 포괄적인 변경을 포함시키고 프로그램코드역분석 과정에서 일어나는 복제 및 변환을 모두 저작권을 침해하는 행위로 명확히 규정했다는 점과 대비되는 점이다.

그리고 "변환"을 불완전한 복제 또는 창작성 없는 코드의 변환으로 보아야 한다는 견해가 있는데,[123] 이는 "변환"을 "복제"로 보고자 한 것으로 보인다. 이는 "변환"의 속성을 고려해 보았을 때 원래의 원시코드와 기능적 측면이나 구조적인 측면에서 동일할 것이므로 타당해 보이는 것 같다. 더군다나 "변환" 과정에서 "복제"가 수반된다는 점에서는 "변환"을 "복제"로 보더라도 문제가 없는 것처럼 보인다.

그러나 프로그램코드역분석 과정에서 목적코드(object code)를 원시코드(source code)로 "변환"하는 것은 개발자에 의한 복제와 직접 수정이 수반된다. 즉, 관련 소프트웨어에 의해 자동으로 변환된 원시코드라고 하더라도 완전한 변환이 이뤄지기 위해서는 개발자의 개입이 필요할 수 있다는 것이다. 따라서 그 결과는 원래의 원시코드와 그 표현에 있어서 다소 다를 수 있다. 그렇다면 이러한 경우에는 이를 단순히 복제로 보는 것이 타당한지 의문이다.

또한 제101조의4의 "변환"을 복제에 해당하는 것으로 해석하는 경우에는 제101조의3 제1항 제6호에 따라서도 프로그램코드역분석이 허용될 수 있을 것으로 보인다. 왜냐하면 제101조의4의 프로그램코드역분석 행위는 결국 복제 행위로 귀결되고 저작재산권의 제한 사유에 해당하는 복제의 경우에는 저작재산권이 제한되어 자유롭게 복제가 가능하기 때문이다. 즉, 제101조의3 제1항 제6호에는 "프로그램의 기초를 이루는 아이디어 및 원리를 확인하기 위하여 프로그램의 기능을 조사 · 연

121) 안효질, "프로그램코드역분석 규정의 비교법적 분석-EU 소프트웨어지침을 중심으로-", 창작과권리 제47호(2007년 여름호), 세창출판사, 2007.6, 93-94면.

122) 제5조 (2차적저작물)① 원저작물을 번역 · 편곡 · 변형 · 각색 · 영상제작 그 밖의 방법으로 작성한 창작물(이하 "2차적저작물"이라 한다)은 독자적인 저작물로서 보호된다.
② 2차적저작물의 보호는 그 원저작물의 저작자의 권리에 영향을 미치지 아니한다.

123) 안효질, "프로그램코드역분석 규정의 비교법적 분석-EU 소프트웨어지침을 중심으로-", 창작과권리 제47호(2007년 여름호), 세창출판사, 2007.6, 94면.

구 · 시험할 목적으로 복제하는 경우(정당한 권한에 의하여 프로그램을 이용하는 자가 해당 프로그램을 이용 중인 때에 한한다)"라고 규정하고 있고, 본조 제1항 본문 규정에 따라 이러한 경우에 필요한 범위에서 해당 프로그램을 복제할 수 있게 되는 것이다. 물론, 이러한 복제는 해당 프로그램을 이용중인 때에 한하고 있기는 하지만, 해당 조문의 해석상 이용중에 일어나는 우연한 복제 외에 조사 · 연구 · 시험을 위한 컴퓨터프로그램의 의도적인 복제를 포함하여 규정하고 있어 상기의 복제가 허용된다.

더군다나 프로그램코드역분석 자체를 별도로 처벌하는 규정은 존재하지 않는다.[124] 따라서 프로그램코드역분석 행위가 복제 행위로 한정된다면, 결국 제101조의3 제1항 제6호에 해당된다고 해석해도 큰 문제는 없다.

이에 더해 프로그램코드역분석이 결국 복제와 다름 아니라면, 굳이 프로그램코드역분석이 제12조와 별개인 것처럼 해석할 이유도 없다고 생각된다. 왜냐하면 프로그램코드역분석 행위 자체를 금지하는 규정도 없으려니와 프로그램코드역분석이 복제라면 제12조의 저작재산권 제한 사유에 해당되는 경우 어떤 경우라도 복제, 즉 프로그램코드역분석이 가능한 것으로 귀결되기 때문이다. 물론, 이와 같은 해석이 다소 극단적일 수는 있지만, 법률의 입법의도를 고려하지 않고 순수하게 문리해석을 하는 경우 이러한 해석도 가능하게 된다.

이에 따라 "변환"을 복제로 해당하는 것으로 보게 되면, 프로그램코드역분석의 범위가 프로그램코드역분석 규정의 입법의도와는 달리 상당히 넓어질 수 있게 된다.

그러나 이것은 프로그램코드역분석 규정이 EU 컴퓨터프로그램 지침을 모델로 하여 입법되었다는 점과 해당 규정이 미국의 통상 문제에 따라 제101조의3 제1항 제6호와 구분되어 규정되었다는 점에서도 원래 입법 시 의도했던 내용과도 차이가 있어 보인다. 더군다나 법문을 문리해석하면 그 범위가 극단적으로 넓어질 수도 있게 되므로 바람직하지도 않다.

이러한 점들을 고려한다면, "변환"을 EU 컴퓨터프로그램 지침과 같이 별도로 저작재산권의 하나로 규정하거나 우리 법의 현실을 감안하여 "2차적저작물작성"의 하나로 규정하는 것을 고려할 수 있을 것이다. 이렇게 규정하는 것이 제12조와 어느정도 구분이 되고, 원래 EU 컴퓨터프로그램 지침을 참조하였던 입법의도에 맞는 것으로 생각된다.

124) 프로그램코드역분석 행위 자체에 대한 처벌 규정은 EU 컴퓨터프로그램 지침이나 미국 저작권법에도 직접적으로 존재하지 않는다. EU 컴퓨터프로그램 지침은 프로그램코드역분석이 복제 및 변환에 해당하는 것으로 저작재산권의 제한을 하면서 계약으로도 이를 금지할 수 없도록 하고 있고, 미국 저작권법은 원칙적으로 제107조 공정이용 규정에 따라 판단하고 있어 프로그램코드역분석을 저작재산권의 침해와 결부하고 있다. 그리고 미국 저작권법 제1201조 (f)에 기술적 보호조치에 관한 규정을 두고 있는데, 이는 접근통제 기술적 보호조치 우회 금지의 예외로써 규정한 것이고 이를 위반했을 때에는 기본적으로 기술적 보호조치에 관한 처벌 규정(미국 저작권법 제1204조)에 따라 처벌을 받게 된다.

다. 계약과의 관계

미국 저작권법에는 저작재산권을 제한하는 프로그램코드역분석 규정은 명시적으로는 존재하지 않는다. 다만, 기술적 보호조치 규정 내에 접근통제 기술적 보호조치 우회 금지의 예외로써 해당 규정이 존재한다. 따라서 프로그램코드역분석에 있어서 미국 저작권법의 허용범위와 우리 저작권법상의 허용범위는 다를 수가 있다. 물론, 한 · 미 FTA 이행 법률이 시행된다면, 접근통제 기술적 보호조치 무력화 금지의 예외 규정으로써는 거의 같은 의미를 가질 것이다.

이런 전제에서 라이선스의 계약으로써의 효력을 생각해 보면, 명시적인 규정이 있는 것과 없는 것에서 계약의 효력에 있어서 차이가 있을 것으로 보인다. 즉, 미국 저작권법상에 명시적인 규정이 없고 공정이용의 법리에 그 판단을 맡기고 있다는 점에서 계약으로 프로그램코드역분석을 제한 할 수 있는 가능성이 있지만, 우리 저작권법에 있어서 프로그램코드역분석은 명시적으로 규정되어 자유이용을 허용하는 강제규정의 의미를 가지기 때문이다. 따라서 우리나라에서는 계약을 통한 프로그램코드역분석의 제한은 무효이다.[125]

3. 규정간 상호 관계

저작권법의 기술적 보호조치 규정은 복제통제 기술적 보호조치의 무력화 행위 자체는 규정하고 있지 않고 무력화를 주된 목적으로 하는 기술 · 서비스 · 제품 · 장치 또는 그 주요 부품을 제공 · 제조 · 수입 · 양도 · 대여 또는 전송하는 행위만을 규제하고 있다. 그리고 접근통제 기술적 보호조치의 무력화와 관련된 규정은 존재하지 않는다. 따라서 기술적 보호조치의 무력화와 프로그램코드역분석과는 직접 관련이 있게 되는 경우는 없다고 볼 수 있다. 즉, 무력화 금지 규정 자체가 없기 때문에 기술적 보호조치를 무력화 여부와 관계없이 프로그램코드역분석을 할 수 있다.

이것은 구컴퓨터프로그램보호법에서 제30조 제1항에서 복제통제 기술적 보호조치를 무력화하는 것을 금지하고 프로그램코드역분석를 그 예외로써 인정한 것과는 대조적이다. 또한 미국 저작권법에서 접근통제 기술적 보호조치를 우회하는 것을 금지하고 프로그램코드역분석을 그 예외로써 인정한 것과도 대조적이다.

그렇지만 복제통제 기술적 보호조치를 무력화하는 행위의 경우 기본적으로 복제를 수반하게 된다. 복제통제 기술적 보호조치의 무력화의 이유가 복제를 하기 위한 것임을 상기해 보았을 때 이는 당연한 귀결일 것이다. 따라서 해당 무력화 행위의 경우에는 복제 행위와 결부시켜 판단해야 할 것이다. 그리고 이후의 프로그램코드역분석도 이러한 복제권 침해 여부와 연관시켜야 할 것으로 보인다.

125) 정진근, "프로그램코드역분석에 관한 비교법적 고찰", 비교사법 제13법적2호 (통권33호), 한국비교사법학회, 2006.6, 547-549면.

Ⅲ. EU 지침상의 관계

EU는 프로그램코드역분석과 기술적 보호조치에 관련하여서는 COUNCIL DIRECTIVE of 14 May 1991 on the legal protection of computer programs (91/250/EEC)(EU 컴퓨터프로그램 지침, 본 지침의 최신 개정은 Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs[126]) 및 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society(이하 "EU 정보사회 지침[127]"이라 함)에 각각 규정을 두고 있다. 프로그램코드역분석에 대해서는 EU 컴퓨터프로그램 지침이 우선 적용된다는 점에서 두 지침이 상호 배치되지 않고, 기술적 보호조치는 복제통제 및 접근통제 기술적 보호조치의 우회 및 우회 장치 등의 유통을 모두 금지하고 있다.

1. EU 정보사회 지침

기술적 보호조치에 관하여는 EU 정보사회 지침 제6조에 기술적 보호조치에 관한 의무로써 규정되어 있다. 제1항에는 회원국들이 효과적인 기술적 보호조치들의 우회에 대응하는 적절한 법적 보호를 제공해야 함을 규정하고 있고,[128] 제2항에는 기술적 보호조치들의 우회 장치 등의 유통에 대응하는 적절한 법적 보호를 제공해야 함을 규정하고 있다.[129] 그리고 제3항에는 기술적 보호조치의 의미 등에 대해 규정하고 있는데, 이것에서 기술적 보호조치가 복제통제 및 접근통제를 모두 포함하고 있음을 알 수 있다.[130] 또한 제4조에는 제5조에 규정된 내용 중에서 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a),

126) EU 컴퓨터프로그램 지침은 1991년에 제정된 이후로 개정이 있었으며, 2009년의 개정이 최신 개정이다. 그러나 여기에서 다루는 내용에 대해서는 특별한 변화가 없기 때문에 여기에서는 1991년의 지침을 기초로 하였다.

127) 본 지침은 EU 저작권 지침으로도 불려지나 여기에서는 본 지침의 명칭에 정보사회가 사용되므로 EU 정보사회 지침으로 한다.

128) Article 6 Obligations as to technological measures
1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

129) Article 6 Obligations as to technological measures
2. Member States shall provide adequate legal protection against the manufacture, ie ort, distribution, sale, rental, advertise salefor sale or rental, oal ossession for atemercn,l pur ose pur devices, produ,l puruate onenl pur the provision of services which:
(a) are promoted, advertised or marketed for the purpose of circumvention of, or
(b) have only a limited commercially significant purpose or use other than to circumvent, or
(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

130) Article 6 Obligations as to technological measures
3. For the purposes of this Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

(3)(b) 및 (3)(e) 저작권 제한 규정에 대해서 기술적 보호조치 규정이 적용되지 않도록 의무로써 규정하고 있고 5(2)(b)의 사적복제에 대해서는 기술적 보호조치에 대해서는 각 국가의 정책에 맡기고 있다.[131]

2. EU 컴퓨터프로그램 지침

EU 컴퓨터프로그램 지침은 제5조에 저작권 제한 규정을 두고 있고, 제6조에 프로그램코드역분석에 관한 규정을 두고 있다. 즉, 우리나라가 제101조의3과 제101조의4에 저작권 제한 규정과 프로그램코드역분석 규정을 두고 있는 것과 같은 구조를 취하고 있다.

가. 제5조 저작권 제한 규정

제5조 제1항[132]에서는 에러 수정을 포함하는 사용 과정에서의 복제, 일시적 복제, 변환 등 제4조 (a)와 (b)에서 규정된 행위를 허용하고 있고, 제5조 제2항에서는 사용자에 의한 백업을 위한 복제를 허용하고 있으며, 제5조 제3항에서는 프로그램을 적재(loading), 디스플레이(displaying), 실행(running), 전송(transmitting) 및 저장(storing)하는 동안 해당 프로그램의 모든 요소에 존재하는 아이디어와 원칙들을 알기 위해 해당 프로그램의 기능을 관찰, 연구 및 시험할 수 있도록 규정했다.

131) Article 6 Obligations as to technological measures
4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.
A Member State may also take such measures in respect of a beneficiary of an exception or limitation provided for in accordance with Article 5(2)(b), unless reproduction for private use has already been made possible by rightholders to the extent necessary to benefit from the exception or limitation concerned and in accordance with the provisions of Article 5(2)(b) and (5), without preventing rightholders from adopting adequate measures regarding the number of reproductions in accordance with these provisions.
The technological measures applied voluntarily by rightholders, including those applied in implementation of voluntary agreements, and technological measures applied in implementation of the measures taken by Member States, shall enjoy the legal protection provided for in paragraph 1.
The provisions of the first and second subparagraphs shall not apply to works or other subject-matter made available to the public on agreed contractual terms in such a way that members of the public may access them from a place and at a time individually chosen by them.
When this Article is applied in the context of Directives 92/100/EEC and 96/9/EC, this paragraph shall apply mutatis mutandis.

132) Article 5 Exceptions to the restricted acts
1. In the absence of specific contractual provisions, the acts referred to in Article 4 (a) and (b) shall not require authorization by the rightholder where they are necessary for the use of the computer program by the lawful acquirer in accordance with its intended purpose, including for error correction.
2. The making of a back-up copy by a person having a right to use the computer program may not be prevented by contract insofar as it is necessary for that use.
3. The person having a right to use a copy of a computer program shall be entitled, without the authorization of the rightholder, to observe, study or test the functioning of the program in order to determine the ideas and principles which underlie any element of the program if he does so while performing any of the acts of loading, displaying, running, transmitting or storing the program which he is entitled to do.

그런데 제5조 제3항의 경우는 특히 제4조 (a)의 복제와 관련이 있다고 보여진다. 이러한 이용 과정에서 기술적으로 일시적 또는 영구적 복제가 일어나게 되는데, 제5조 제3호에 의해 이러한 제4조 (a)에 규정된 복제가 허용될 수 있을 것이다.[133] 따라서 이 규정은 상기한 바와 같이 우리 저작권법 제101조의3 제1항 제6호[134]에 해당한다고 볼 수 있다. 여기에서 EU 컴퓨터프로그램 지침에 있어서 일시적 저장이 복제로 인정되고 있다는 점에서 이 규정은 더욱 의미가 있다. 그리고 이는 넓은 의미의 리버스 엔지니어링(reverse engineering) 행위로써 프로그램코드역분석 행위는 포함되지 않는 것으로 볼 수 있다.[135]

그리고 이 규정은 Recital[136]에서 프로그램의 저작권을 침해하지 않는 경우에 프로그램의 기능을 관찰, 연구 및 시험하기 위한 행위를 수행하는 것을 금지할 수 없도록 한다고 기술하고 있고, 제5조 제3항에 컴퓨터프로그램의 이용자에게 해당 행위에 대한 권리를 부여하고 있으며, 제9조 제1항에서 명시적으로 계약에 의해 금지할 수 없도록 한 것으로 보아 계약에 의해 이러한 행위들이 제한될 수도 없게 된다.[137]

사실 제4조 (a)에는 일시적 저장을 복제로 규정하고 있고 이러한 복제를 저작권자의 권리로써 보고 있기 때문에 이 규정은 더 의미가 있다고도 볼 수 있을 것이다.

133) EU 컴퓨터프로그램 지침 Recital
Whereas the exclusive rights of the author to prevent the unauthorized reproduction of his work have to be subject to a limited exception in the case of a computer program to allow the reproduction technically necessary for the use of that program by the lawful acquirer;

134) 제101조의3(프로그램의 저작재산권의 제한)① 다음 각 호의 어느 하나에 해당하는 경우에는 그 목적상 필요한 범위에서 공표된 프로그램을 복제 또는 배포할 수 있다. 다만, 프로그램의 종류·용도 및 프로그램에서 복제된 부분이 차지하는 비중 및 복제의 부수 등에 비추어 프로그램의 저작재산권자의 이익을 부당하게 해치는 경우에는 그러하지 아니하다.
6. 프로그램의 기초를 이루는 아이디어 및 원리를 확인하기 위하여 프로그램의 기능을 조사·연구·시험할 목적으로 복제하는 경우(정당한 권한에 의하여 프로그램을 이용하는 자가 해당 프로그램을 이용 중인 때에 한한다)

135) 그러나 EU 컴퓨터프로그램 지침 제5조는 우리 저작권법과 비교하여 조금 더 세심한 고찰이 필요해 보인다.

136) Whereas a person having a right to use a computer program should not be prevented from performing acts necessary to observe, study or test the functioning of the program, provided that these acts do not infringe the copyright in the program;

137) Article 9 Continued application of other legal provisions
1. The provisions of this Directive shall be without prejudice to any other legal provisions such as those concerning patent rights, trade-marks, unfair competition, trade secrets, protection of semi-conductor products or the law of contract. Any contractual provisions contrary to Article 6 or to the exceptions provided for in Article 5 (2) and (3) shall be null and void.

나. 제6조 프로그램코드역분석 규정

제6조[138]에는 디컴파일(Decompilation) 규정을 두고 있다. 이 규정은 우리 저작권법 제101조의4에 해당되는 규정으로 우리 저작권법상 프로그램코드역분석 규정이, 구컴퓨터프로그램보호법에 신설될 때 모델이 된 규정이다.[139] 따라서 EU 컴퓨터프로그램 지침 제6조의 규정은 우리 저작권법상 프로그램코드역분석 규정과 같은 구조와 내용을 가지고 있다고 볼 수 있다.

그런데, EU 컴퓨터프로그램 지침의 경우 제4조에 행위 제한 규정을 두어 제1항에 일시적 복제를 포함하는 저작권자의 복제권에 관하여 규정하고, 제2항에 변환을 번역, 개작 및 모든 변환 및 그 결과물의 복제에 대한 저작권자의 권리를 규정하고 있다. 그리고 제4조 본문에 제5조와 제6조에 있는 (a), (b) 및 (c)의 내용이 제2조의 저작권자의 배타적 권리에 포함됨을 기술하고 있다. 또한 EU 컴퓨터프로그램 지침의 Recital에서도 컴퓨터프로그램의 복제물이 이용가능한 코드 형태를 허락받지 않고 복제, 번역, 개작 및 변환하는 것은 저작권자의 배타적 권리를 침해하는 것으로 설명하고 있다.[140]

그래서 제6조에서 프로그램코드역분석에 의한 코드의 복제 및 변환 행위는 원래는 제4조 (a) 및 (b)의 금지 행위에 해당한다. 그러나 제6조 제1항에 호환성을 얻기 위해 불가피한 경우에 제4조 (a) 및 (b)의 의미내에서의 코드의 복제 및 형태의 변환을 허용하고 있다. 즉, 프로그램코드역분석 행위는 지침상 원칙적으로 금지된 행위이지만 예외적으로 허용되는 것이 된다.[141]

---

138) Article 6 Decompilation
1. The authorization of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of Article 4 (a) and (b) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:
(a) these acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to to so;
(b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in subparagraph (a); and (c) these acts are confined to the parts of the original program which are necessary to achieve interoperability.
2. The provisions of paragraph 1 shall not permit the information obtained through its application:
(a) to be used for goals other than to achieve the interoperability of the independently created computer program;
(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or (c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.
3. In accordance with the provisions of the Berne Convention for the protection of Literary and Artistic Works, the provisions of this Article may not be interpreted in such a way as to allow its application to be used in a manner which unreasonably prejudices the right holder's legitimate interests or conflicts with a normal exploitation of the computer program.

139) 안효질, "프로그램코드역분석 규정의 비교법적 분석-EU 소프트웨어지침을 중심으로-", 창작과권리 제47호(2007년 여름호), 세창출판사, 2007.6, 89면.

140) EU 컴퓨터프로그램 지침 Recital
Whereas the unauthorized reproduction, translation, adaptation or transformation of the form of the code in which a copy of a computer program has been made avcolable constitutes an infringement of the exclusive rights of the author;

141) 미국의 경우 프로그램코드 역분석은 복제(reproduction)과 2차적 저작물에 해당하는 "derivative work"에 해당될 수 있을 것으로 보인다.

그리고 프로그램코드역분석 행위 자체에 대한 처벌 규정은 EU 컴퓨터프로그램 지침에는 직접적으로 존재하지 않는다. EU 컴퓨터프로그램 지침은 프로그램코드역분석이 복제 및 변환에 해당하는 것으로 저작재산권의 제한을 하고 있다. 따라서 규정을 위반하여 프로그램코드역분석을 하는 경우에는 제4조 (a) 및 (b)의 저작재산권 침해를 이유로 처벌을 받게 될 것으로 보인다.

그리고 제9조 제1항에서 제5조 제2항 및 제3항과 제6조를 계약에 의해 금지하지 못함을 명시적으로 규정하고 있는데, 이러한 점에서 제6조의 프로그램코드역분석은 저작권을 제한하는 규정이기도 하지만, 계약에 의한 프로그램코드역분석의 제한을 방지하는 기능도 하고 있다고 할 수 있을 것이다.

3. 지침 및 규정 간 관계

EU 정보사회 지침과 EU 컴퓨터프로그램 지침과의 관계는 해당 지침의 규정들이나 Recital[142]의 내용에 따라 판단해야 한다. 그런데 EU 정보사회 지침 Recital (50)에는 EU 컴퓨터프로그램 지침과의 관계를 기술하고 있다. Recital (50)[143]에는 "그런 조화된 법적 보호(기술적 보호조치[144]의 법적 보호)는 EU 컴퓨터프로그램 지침에 의해 규정된 보호에 관한 특정한 규정들에 영향을 미치지 않는다. 특히 그것은 해당 지침에 배타적으로 규정된 컴퓨터 프로그램에 관하여 이용된 기술적 보호조치의 보호에 적용하지 말아야 한다. 그것이 EU 컴퓨터 프로그램 지침의 제5조 제3항 또는 제6조의 규정에 합치하는 행위들이 수행되는 것이 가능케 하기 위해 필요한 기술적 보호조치의 우회의 모든 방법들의 개발 또는 이용을 금지하거나 방지하지 말아야 한다. 그 지침의 제5조와 제6조는 컴퓨터 프로그램에 적용 가능한 배타적 권리들에 대한 예외들을 배타적으로 결정한다."고 규정되어 있다.

그러므로 Recital (50)에 따라 EU 정보사회 지침의 기술적 보호조치에 대한 규정은 EU 컴퓨터프로그램 지침 제5조 제3항 및 제6조에는 적용되지 않는다. 즉, 프로그램코드역분석에는 적용되지 않는다.

따라서 미국 저작권법이 접근통제 기술적 보호조치의 우회 금지의 예외로써만 프로그램코드역분석이 규정되어 있는 것과 달리, EU 지침에서는 프로그램코드역분석을 위해 복제통제 기술적 보호조치 및 이용통제 기술적 보호조치 모두에 대해 우회의 방법을 개발하거나 이용하는 것이 허용된다.

142) Recial은 지침의 해석을 위한 기초가 되기 때문에 본문과 동일한 효력을 가진다고 볼 수 있다.

143) (50) Such a harmonised legal protection does not affect the specific provisions on protection provided for by Directive 91/250/EEC. In particular, it should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive. It should neither inhibit nor prevent the development or use of any means of circumventing a technological measure that is ne developto enable acts to be undertakt tin accordance with the terms of Article 5(3) or Article 6 of Directive 91/250/EEC. Articles 5 and 6 of that Directive exclusively determine exceptions to the exclusive rights applicable to computer programs.

144) EU 정보사회 지침에는 기술적 조치(technological measures)로 기술되어 있으나, 기술적 보호조치와 같은 의미로 보이므로 여기에서는 기술적 보호조치로 기술하도록 한다.

Ⅳ. DMCA상의 관계

미국 저작권법상에서도 저작권과 기술적 보호조치는 각각 독립적으로 보호한다. 미국법상 프로그램코드역분석(Reverse Engineering)에 관한 규제는 판례로써 정립되어 왔는데, 법 제107조의 공정이용 규정으로 그 적법성을 판단해 왔다. 그리고 DMCA는 1998년에 입법되어 미국 저작권법에 반영되었는데, 이 법에는 기술적 보호조치에 관한 규정이 포함되어 있으나 복제통제 기술적 보호조치의 우회 금지 규정은 제외되어 있다. 또한 해당 규정 내에 기술적 보호조치의 우회를 허용하는 예외 규정으로써 프로그램코드역분석 규정이 포함되어 있다. 그러나 미국 저작권법상 기술적 보호조치 규정에 대해 공정이용 내지 저작권 제한 규정으로 그 예외를 인정하지는 않는다.

1. 미국법상 프로그램코드역분석의 허용

미국 저작작권법에는 프로그램코드역분석에 대한 독립된 규정이 존재하지 않는다. 그러나 프로그램코드역분석에 대해 원칙적으로 미국 저작권법 제107조의 공정이용 규정에 따라 허용 여부를 판단하게 된다. 그리고 이와 같이 저작권법상에 명시적인 근거 규정이 없기 때문에 계약에 의한 프로그램코드역분석의 금지에 관하여는 판례에서 다소 이견이 있어 왔다. 따라서 결과적으로 프로그램코드역분석의 허용에 대해서는 판례의 해석이 중요한 기준이 된다. 그러나 판례의 이러한 경향에도 불구하고 제107조의 공정이용 규정은 프로그램코드역분석의 허용에 대한 기본적인 근거가 되고 있다.[145]

2. DMCA의 기술적 보호조치 규정과 프로그램코드역분석 규정

DMCA는 접근통제 기술적 보호조치의 우회를 금지하고 있는 것에 반하여, 복제통제 기술적 보호조치를 우회하는 것은 기본적으로 복제를 수반하고 공정 이용인 경우도 있을 수 있기 때문에 금지하지 않는다.[146] 그러나 우회 기술의 유통과 관련해서는 복제통제 및 접근통제 기술적 보호조치를 모두 금지하고 있다.[147]

145) 정진근, "프로그램코드역분석에 관한 비교법적 고찰", 비교사법 제13권 2호 (통권33호), 한국비교사법학회, 2006.6, 535-537면.

146) THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 : U.S. Copyright Office Summary, Copyright Office, 1998.12, 4면. 〈http://www.copyright.gov/legislation/dmca.pdf〉

147) 이대희, "디지털기술의 발전에 따른 S/W보호제도의 개선방향 – S/W 불법복제방지 기술의 법적 대응", 컴퓨터프로그램보호위원회 세미나 자료, 2003.11, 3면.

그리고 접근통제 기술적 보호조치의 우회 금지의 예외 중의 하나로써 프로그램코드역분석이 규정되어 있다. 그러나 저작재산권의 제한이나 자유이용의 의미의 프로그램코드역분석에 대한 별도의 규정은 존재하지 않는다. 즉, 기본적으로 프로그램코드역분석에 대해서는 미국 저작권법 제107조의 공정이용의 법리에 따라 그 허용 여부를 판단하고 있지만, 접근통제 기술적 보호조치에 관하여서는 프로그램코드역분석의 허용 범위를 명문화시켜서 그 허용범위를 좁게 규정하였다.

그리고 프로그램코드역분석 행위 자체에 대한 처벌 규정은 미국 저작권법에 직접적으로 존재하지 않는다. 미국 저작권법은 원칙적으로 제107조 공정이용 규정에 따라 판단하고 있어 프로그램코드역분석을 저작재산권의 침해와 결부하고 있다. 그리고 미국 저작권법은 접근통제 기술적 보호조치 우회 금지의 예외로써 제1201조 (f)에 기술적 보호조치에 관한 규정을 두고 있는데, 이를 위반했을 때에는 기본적으로 기술적 보호조치에 관한 처벌 규정[148]에 따라 처벌을 받게 된다.

3. 두 규정의 상관관계

상기한 바와 같이 미국 저작권법에서 기술적 보호조치의 우회를 금지하는 것은 접근통제 기술적 보호조치에 한정되어 있다. 따라서 프로그램코드역분석은 기본적으로 공정이용에 해당하면면면면이 된다. 다 기술복제통제 기술적 보호조치를 우회하고 프로그램코드역분석을 하는 것은 "호환성(interoperability)"[149]을 위해서만 가능하다.

그리고 기술적 보호조치 규정의 예외에는 공정이용과 관련된 내용은 없다. 다만, 예외로 규정되어야 할 사항들이 나열되어 있어서 해당 사항들에 대해서만 예외로 인정된다. 제1201조 (c)에 공정이용을 포함하여 구제, 제한, 저작권 침해에 대한 항변에 대해 영향을 미치지 않음을 규정하고 있으나, 이것은 기술적 보호조치에 관한 규정이 기존의 저작재산권자 및 이용자들의 권리에 영향을 주지 않는다는 선언적인 규정으로 보여진다.[150]

148) 미국 저작권법 §1204 Criminal offenses and penalties
(a) In General.–Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain–
(1) shall be fined not more than $500,000 or imprisoned for not more than 5 years, or both, for the first offense; and
(2) shall be fined not more than $1,000,000 or imprisoned for not more than 10 years, or both, for any subsequent offense.
(b) Limitation for Nonprofit Library, Archives, Educational Institution, or Public Broadcasting Entity.–Subsection (a) shall not apply to a nonprofit library, archives, educational institution, or public broadcasting entity(as defined under section 118(g)).
(c) Statute of Limitations.–No criminal proceeding shall be brought under this section unless such proceeding is commenced within five years after the cause of action arose.

149) interoperability는 상호운영성이라고 번역되기도 한다. 호환성과 상호운영성은 그 의미에서 구분이 될 수도 있겠으나 여기에서는 호환성이라고 번역했다.

150) 이에 대해 Nimmer 교수는 기술적 보호조치 규정의 우회에 대해 공정이용의 원칙이 항변이 되지 않음을 지적하면서도, 이용의 공정한 이용의 성격이 1201조 그 자체가 위반되었는지 여부의 분석에 개입될 가능성을 언급하고 있다.: Melville B. Nimmer · David Nimmer, 「Nimmer on Copyright」, Mattew Bender & Company, inc., 2007, §13.05[G], 13-271면.

이에 대하여 전통적인 저작권 침해에 대해서만 공정이용이 적용된다는 것은 제1201조 (c)를 완전히 쓸모없게 만드는 것이고, 공정이용의 원리가 법원이 독자적으로 형성시켜 온 판례법이라는 사실에 기초한다면 DMCA에 대해서도 공정이용이 적용될 수 있다고 해석하는 것이 가능하다는 등 접근통제에 대하여 공정이용의 원리가 적용되어야 한다는 소비자입장에서의 긍정론도 있으나, Corley 사건[151]을 비롯한 판례는 접근통제조치에 대하여 공정이용이 적용될 수 없다는 부정론을 취하고 있어 그 논란은 어느 정도 정리된 것으로 보인다.[152]

접근통제 기술적 보호조치에 대해서는 프로그램코드역분석의 행위가 예외 규정에 부합하는지를 가지고 판단한다. 그러나 복제통제 기술적 보호조치에 관하여서는 프로그램코드역분석 행위는 복제권 침해의 문제로써 이에 대해 공정이용 규정에 기초하여 침해 문제를 판단해야 한다.

Ⅴ. 한 · 미 FTA 관련 개정법률안상의 관계

한 · 미 FTA 저법 이행법안에서 기술적 보호조치 규정은 기본적으로 미국 저작권법의 형태를 취한다. 따라서 복제통제 기술적 보호조치의 무력화 금지 규정은 존재하지 않는다. 그리고 프로그램코드역분석 규정은 한 · 미 FTA 저법 이행법안에는 존재하지 않고 한 · 미 FTA 컴법 이행법안에 기존의 규정이 그대로 규정되어 있는 상태에서 접근통제 기술적 보호조치의 무력화 금지의 예외 중의 하나로 규정되어 있다.

1. 기술적 보호조치 규정

가. 규정 개요

한 · 미 FTA 이행을 위한 저작권법 및 컴퓨터프로그램 보호법 개정법률안은 복제통제 무력화 금지 규정이 존재하지 않고, 접근통제 기술적 보호조치 무력화 금지와 접근통제 및 복제통제 기술적 보호조치의 무력화를 주된 목적으로 하는 기술 · 서비스 · 제품 · 장치 또는 그 주요 부품을 제공 · 제조 · 수입 · 양도 · 대여 또는 전송하는 행위를 금지하는 규정들을 두고 있다.[153]

151) Universal City Studios, Inc. v. Corley [273 F.3d 429(2d Cir. 2001)].

152) 이규홍, "기술적 보호조치에 관한 소고", 정보법학 제11권 제1호, 한국정보법학회, 2007, 179-180면.

153) 저작권법 개정안 제2조 28. "기술적 보호조치"란 다음 각 목의 어느 하나에 해당하는 조치를 말한다.
가. 저작권, 그 밖에 이 법에 따라 보호되는 권리에 의하여 보호되는 저작물등에 대한 접근을 통제하기 위하여 그 권리자나 권리자의 동의를 받은 자가 적용하는 기술 · 장치 또는 부품
나. 저작권, 그 밖에 이 법에 따라 보호되는 권리에 대한 침해 행위를 방지 또는 억제하기 위하여 그 권리자나 권리자의 동의를 받은 자가 적용하는 기술 · 장치 또는 부품

상술한 바와 같이 기술적 보호조치의 보호는 저작권의 보호와는 독립적인 것이어서, 해당 기술적 보호조치의 무력화 행위는 저작권의 제한 규정의 영향을 받지 않는다. 따라서 접근통제 기술적 보호조치 무력화 금지의 예외 규정을 마련하여 개별적인 사항에 대해 무력화를 허용하고 있다.[154] 즉, 접근통제 기술적 보호조치 규정에는 미국과 마찬가지로 프로그램코드역분석을 포함하는 예외 사항들이 규정되어 있다. 그리고 그 외의 제한 사항들에 대해서는 문화체육관광부에서 대통령령으로 정하는 절차에 따라 기술적보호조치 무력화의 금지에 대한 예외를 고시하는 것에 의해 추가적인 예외를 규정하는 것이 가능하다.

나. 기술적보호조치 무력화 기기 등의 양도 등의 금지 규정

한 · 미 FTA 저법 및 컴법 이행법안에서 기술적보호조치 무력화 기기 등의 제공 · 제조 · 수입 · 양도 · 대여 등에 대해 금지하고 있다.

우선 한 · 미 FTA 컴법 이행법안에는 제34조의10 제1항에 "누구든지 대통령령으로 정하는 기술적 보호조치를 무력화하는 장치 · 부품을 제조 · 수입하거나 공중에 양도 · 대여 또는 유통하여서는 아니 되며, 기술적보호조치를 무력화하는 프로그램을 전송 · 배포하거나 그 기술을 제공하여서는 아니 된다."라고 규정하고 있다.

그리고 한 · 미 FTA 저법 이행법안에는 제104조의2 제3항에 "누구든지 정당한 권한 없이 기술적 보호조치를 무력화하는 것으로서 대통령령으로 정하는 장치 등이나 그 주요부품을 제공 · 제조 · 수입 · 양도 · 대여하거나 그 밖의 방법으로 배포 또는 전송하여서는 아니 된다."라고 규정하고 있다.

154) 저작권법 개정안 제104조의2(기술적 보호조치의 무력화 금지)① 누구든지 정당한 권한 없이 고의 또는 과실로 제2조제28호가목에 따른 기술적 보호조치를 제거 · 변경하거나 우회하는 등의 방법으로 무력화하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
1. 저작물등의 복제물을 정당하게 이용하는 자가 저작물등에 적용된 암호 기술의 결함이나 취약점을 조사 · 연구하기 위하여 필요한 범위에서 행하는 경우
2. 미성년자에게 유해한 온라인상 저작물등에 미성년자가 접근하는 것을 방지하기 위하여 그 자체로는 제2조제28호가목에 따른 기술적 보호조치를 무력화시키는 기술 · 제품 · 서비스 또는 장치(이하 "장치등"이라 한다)에 해당하지 아니하는 것에 기술적 보호조치를 무력화시키는 구성요소나 부품을 포함시키는 경우
3. 개인의 온라인상의 행위를 파악할 수 있는 개인 식별 정보를 비공개적으로 수집하거나 배포하는 기능을 확인하고 이를 방지하기 위하여 필요한 경우. 다만, 다른 사람들이 저작물등에 접근하는 것에 영향을 미치는 경우는 제외한다.
4. 국가의 법 집행, 정보수집 또는 안전보장 등을 위하여 필요한 경우
5. 제25조제2항에 따른 교육기관, 제31조제1항에 따른 도서관(비영리인 경우로 한정한다) 또는 「공공기록물 관리에 관한 법률」에 따른 기록물관리기관 등 대통령령으로 정하는 시설이 기술적 보호조치를 무력화하지 아니하고는 접근할 수 없는 저작물등의 구입 여부를 결정하기 위하여 필요한 경우
6. 문화체육관광부장관이 기술적 보호조치의 무력화 금지에 의하여 특정 종류의 저작물등을 정당하게 이용하는 것이 부당하게 영향을 받거나 받을 가능성이 있다고 인정하여 고시한 경우
② 문화체육관광부장관은 제1항제6호에 따라 고시하는 경우에는 제112조에 따른 저작권위원회의 심의를 거쳐야 한다. 이 경우 그 예외의 효력은 3년 이내로 한다.
③ 누구든지 정당한 권한 없이 기술적 보호조치를 무력화하는 것으로서 대통령령으로 정하는 장치 등이나 그 주요부품을 제공 · 제조 · 수입 · 양도 · 대여하거나 그 밖의 방법으로 배포 또는 전송하여서는 아니 된다. 다만, 제2조제28호가목에 따른 기술적 보호조치와 관련하여서는 제1항제1호 · 제2호 및 제4호에 해당하는 경우에는 그러하지 아니하며, 제2조제28호나목에 따른 기술적 보호조치와 관련하여서는 제1항제4호에 해당하는 경우에는 그러하지 아니하다.

두 이행법안의 규정은 모두 "기술적보호조치를 무력화하는 장치 · 부품"을 대통령령에 규정하도록 되어 있다. 따라서 이것들이 어떤 것들인지는 개정에 따른 새로운 저작권법 시행령이 마련된 이후에 나 알 수 있을 것이다.

이러한 입법은 EU 정보사회 지침 제6조 제2항[155]과 미국 저작권법 제1201조 (a)(2)[156] 및 (b)(1)[157]에서 비교적 요건을 상세하게 규정한 것과는 대비되는 것이다. 아마도 이와 관련하여서는 대통령령으로 상세한 내용을 규정할 것으로 보인다.

그런데, 두 규정에서 한 · 미 FTA 컴법 이행법안이 "장치 · 부품"으로 기술한 것에 대해 한 · 미 FTA 저법 이행법안은 "장치 등이나 그 주요부품"이라고 기술한 것으로 봐서는 후자의 규제 범위가 다소 좁다고 할 수 있다. 그러나 어차피 대통령령으로 세부적인 사항을 정할 것이라면 굳이 후자와 같이 규정할 필요는 없을 것 같다. 게다가 "그 주요부품"이라는 의미도 불분명하므로 이것의 해석에 있어서 논란이 있을 수 있다. 다만, 무력화 기기등과 관련된 부품이라고 해서 해당 기기등에만 사용되는 것은 아니므로, 대통령령으로 규정하는 것보다는 애초에 법률에 한정을 하는 것도 의미가 있어 보인다.

155) Article 6 Obligations as to technological measures
2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:
(a) are promoted, advertised or marketed for the purpose of circumvention of, or
(b) have only a limited commercially significant purpose or use other than to circumvent, or
(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

156) § 1201 Circumvention of copyright protection systems
(a)(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that–
(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

157) (b) Additional Violations.?(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that?
(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;
(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or
(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

2. 프로그램코드역분석 규정

프로그램코드역분석에 대하여는 한 · 미 FTA 컴법 이행법안에 기존의 제12조의2를 그대로 규정하였다. 따라서 해석상 차이는 없다고 할 것이다.

또한 한 · 미 FTA 컴법 이행법안 제34조의9 제2항 제1호[158]에는 접근통제 기술적 보호조치 무력화 금지의 예외로써 "정당한 권원을 가지고 사용하는 자가 호환에 필요한 정보를 쉽게 얻을 수 없는 경우에 다른 프로그램과의 호환을 목적으로 프로그램코드역분석을 하기 위하여 필요한 경우"를 규정하고 있다. 이 규정은 단순히 프로그램코드역분석에 관하여 기본적인 요건을 정하여 예외를 규정하고 있을 뿐이므로, 프로그램코드역분석에 대한 보다 세부적인 내용은 제12조의2를 기초로 판단해야 할 것으로 보인다.

그런데 현재 프로그램코드역분석 규정은 법률 통합 과정에서 저작권법에 제101조의4로 신설 규정되었으므로, 향후 한 · 미 FTA 이행을 위한 저작권법 개정안이 재차 국회에 제출되는 경우에는 프로그램코드역분석 규정이 해당 법률에 포함될 것이다. 그렇지만 이때에도 상기의 내용과 별다른 차이는 없을 것으로 보인다.

3. 상관관계에 대한 고찰

가. 두 규정의 구조

기술적 보호조치 관련 규정은 미국 저작권법과 그 구조적인 면에서 차이가 없다. 한 · 미 FTA 협상 시에 미국 저작권법을 기초하여 협상이 진행되었기 때문인 것으로 보인다. 다만 내용면에서 미국 저작권법과 비교해 본다면, 미국 저작권법상 접근통제 기술적 보호조치 우회 금지의 예외 규정이 상세한 내용을 담고 있는 것과 달리 우리나라 저작권법상에는 다소 간략한 내용만을 담고 있다. 결국, 우리나라 저작권법의 해당 규정의 구체적인 해석 및 적용은 학설 및 법원판결에 맡겨졌다고 볼 수 있을 것이다. 이에 대해 프로그램코드역분석 규정은 별도 규정이 있으므로 다른 규정들에 비해서는 구체적인 법적 기준이 존재한다고 볼 수 있다.

나. 공정이용 규정과의 관계

그런데 한 · 미 FTA 컴법 개정안에는 미국 저작권법과는 달리 프로그램코드역분석 규정이 별도로 존재하고, 공정이용에 관한 규정은 제12조, 제12조의2 및 제12조의3의 경우 외에 적용하는 것으로

158) ② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
1. 정당한 권원을 가지고 사용하는 자가 호환에 필요한 정보를 쉽게 얻을 수 없는 경우에 다른 프로그램과의 호환을 목적으로 프로그램코드역분석을 하기 위하여 필요한 경우

규정하여 프로그램코드역분석 규정에는 영향을 미치지 않도록 별도로 규정되어 있다. 즉, 공정이용 규정의 적용 범위에서 프로그램코드역분석 규정은 배제되어 있다.

이 공정이용 규정의 적용 범위는 다소 불분명한 부분이 있다. 우선 이 규정이 제12조, 제12조의2 및 제12조의3의 경우를 제외한다는 의미가 이 규정에 의해 프로그램저작권이 제한되지 않는 경우까지 포함한다고 하는 것인지 아니면 해당 규정들에 규정된 사항들을 제외한 사항들에만 공정이용 규정을 적용한다는 것인지 불분명하다. 만약 전자의 경우라면 제12조의3의 프로그램코드역분석 규정에 제시된 프로그램코드역분석의 허용 외에 다른 경우에도 공정한 이용인 경우라면 프로그램코드역분석이 가능하다는 의미가 될 수도 있을 것이다. 그러나 후자와 같다고 보는 경우에는 제12조의4가 프로그램코드역분석과 관련하여 개입될 여지는 없다.

그런데, 미국의 저작권법의 공정이용 규정을 국내 법률에 도입하면서 기존의 저작재산권의 제한 규정에 포함되지 못하는 사항들에 대해서도 저작재산권자의 이익을 부당하게 해치지 않는 정당한 이용을 허용하도록 해당 규정을 마련했다는 점에서 원래의 입법의도[159]는 전자에 가까울 것으로 생각된다. 더군다나 프로그램코드역분석 규정은 금지 규정이 아니라 허용 규정으로 해석된다. 즉, 다른 이유로도 프로그램코드역분석의 가능성은 열려 있다고 보여진다.

따라서 접근통제 기술적 보호조치와 관련하여서는 그 허용범위를 제12조의2에 한정하되, 경우에 따라서는 제12조의4에 의한 프로그램코드역분석을 허용하는 것으로 해석하는 것도 의미가 있어 보인다.

[기술적 보호조치와 프로그램코드 역분석 관련 규정의 존재 여부]

	폐지된 컴법	현행 저작권법	FTA 컴법 이행법안	FTA 저법 이행법안	미국 저작권법	EU 컴퓨터 프로그램 지침	EU 정보사회 지침
복제통제무력화금지	O	X	X	X	X	X	O
접근통제무력화금지	X	X	O	O	O	X	O
복제통제무력화 장치유통금지	O	O (침해간주)	O	O	O	X	O
접근통제무력화 장치유통금지	X	X	O	O	O	X	O
무력화금지 예외: 역분석 규정	O	X	O	X	O	X	X
프로그램코드역분석 규정	O	O	O	X	△ (공정이용)	O	X
공정이용 규정	X (저작권 제한)	X (저작권 제한)	O (역분석 배제)	O	O	X (저작권 제한)	X (저작권 제한)
계약을 통한 역분석 금지 가능성 여부	X (강행규정)	X (강행규정)	X (강행규정)	– (규정없음)	△ (판례)	X (명시규정)	X (명시규정)

159) 정부, 프로그램 보호법 일부개정법률안, 2008.10.10, 2-3면.

제7장

역분석과 기술적 보호조치 관련 법제도 개선방안

제7장 역분석과 기술적 보호조치 관련 법제도 개선방안

Ⅰ. SW 역분석 관련 법제도 개선방안

1. SW 역분석 조항 개선방안

가. 저작권법 상 프로그램코드역분석 조항의 성격과 문제점

저작권법 상 프로그램코드역분석 조항은 유럽연합의 "컴퓨터프로그램의 법적 보호에 관한 EU지침(European Communities Council Directive on the Legal Protection of Computer Programs) 제6조의 규정을 계수한 것이다.

그러나 우리 저작권법에 이 규정을 모델로 프로그램코드역분석 조항을 규정하면서 제101조의3 제1항 제6호와의 관계가 불명확해지게 되었다.

뿐만 아니라 미국의 판례와 저작권법과는 달리 프로그램코드역분석 조항이 기술적보호조치와 독립적으로 규정되면서, 기술적보호조치를 무력화시키지 않는 프로그램코드역분석마저 호환성 확보의 목적 하에서만 가능한 것으로 오해를 일으키는 부작용이 노출되고 있다.

이로 인해 우리 저작권법은 프로그램코드역분석을 미국 저작권법은 물론 한·미 FTA에서 정한 것보다 더 좁게 인정할 가능성이 있다. 아울러 EU지침 제9조 제2문의 규정을 두지 않음으로써 계약에 의해 프로그램코드역분석을 제한하는 것이 가능한지에 대한 의문도 여전히 제시되고 있다.

그러나 컴퓨터프로그램은 일반적 저작물이나 산업재산권과는 달리 역분석과 관련하여 다음과 같은 특징이 있다는 점을 유념하여야 한다.

첫째는 컴퓨터프로그램은 일반 저작물과는 달리 컴퓨터프로그램에 내재된 아이디어나 기능적 요소에 접근할 수 있는 유일한 방법이 역공정이라는 것이다.

둘째는 임시적인 중간복제(intermediate copying)가 저작권에서 정한 복제권의 침해인 듯 보이지만, 실제로는 그 변환의 단계에 불과할 뿐 직접적 침해와는 달리 간접적 연관성만을 갖는다는 점이다.

셋째는 프로그램시장은 네트워크 효과에 따라 시장의 과점은 곧바로 독점으로 연결되고, 이는 신규시장진입을 사실상 불가능하게 만들고 있으므로 저작권에 의한 보호가 경쟁을 불가능하게 하는 경우가 비일비재하고 이는 저작권 본래의 목적인 문화의 향상발전에 반하기 때문에 시장에 미치는 다소의 잠재적 영향만으로 저작권의 칼을 함부로 들이대서는 아니된다는 점이다.

넷째는 저작권은 저작물의 형태에 따라 보호의 정도를 달리하고 있으므로, 산업적 성격이 강한 컴퓨터프로그램은 일반 저작물과는 달리 산업상 영향력을 고려하여 보호하여야 한다는 점이다. 특히, 목적프로그램이 보여주는 기능 외에 아이디어나 기능적 요소에 대해 독점배타적 보호를 받고자 한다면 특허법이 요구하는 엄격한 요건을 충족시켜야 한다고 본다.

이러한 요소들을 종합해볼 때 프로그램역분석은 좀 더 넓게 허용되는 방향으로 해석되어야 하며, 해석의 혼란을 방지하기 위하여 미국 저작권법의 태도와 같은 방향으로 개정되어야 할 것이다.

나. 개선방향

프로그램코드역분석은 원칙적으로 허용되어야 하며, 저작권법 제101조의3 제1항 제6호의 규정에 따라 허용되어야 할 것이다. 이러한 태도는 프로그램코드역분석을 공정사용의 원칙에 따라 기술적보호조치무력화와 독립적으로 허용하는 미국 저작권법의 태도와 일치하는 것이다.

아울러, 제101조의4는 기술적보호조치의 무력화가 수반되는 경우에 한하여 적용된다는 점을 명확하게 할 것이 요망된다. 이와 같은 태도는 미국의 판례와 저작권법의 규정과도 같은 것이며, 한 · 미 FTA 협정에서 정한 바와도 일치하는 것이다.

이와 같이 프로그램코드역분석은 2단계의 법적 구조를 통해 허용하는 것이 바람직하다. 즉, 기술적보호조치무력화를 수반하지 않는 프로그램코드역분석은 제101조의3 제1항 제6호의 규정에 따라 가급적 넓게 인정함으로써, 아이디어의 독점을 불허하는 저작권법의 이념에 부합하도록 해석하는 것이다. 아울러, 기술적보호조치무력화를 수반하는 프로그램코드역분석은 호환성 확보를 위한 목적에서만 허용함으로써, 상대적으로 제한적인 허용을 하는 방안이다.

따라서, 현행 저작권법은 제101조의3 제1항 제6호의 규정과 제101조의4 규정이 모두 기술적보호조치무력화와 무관하게 기술되어 있음으로 인하여 양 규정의 해석상 충돌이 발생할 여지가 있었음을 고려하여, 제101조의4 규정은 기술적보호조치무력화를 수반하는 경우에 한하여 적용한다는 점을 명시적으로 규정할 것이 요망된다.

2. 프로그램코드역분석의 변환의 개념

EU 컴퓨터프로그램 지침 제6조는 상기한 바와 같이 우리 저작권법의 태도와는 차이가 난다. 우리 저작권법 제2조 제34호에는 프로그램코드역분석을 "독립적으로 창작된 컴퓨터프로그램저작물과 다른 컴퓨터프로그램과의 호환에 필요한 정보를 얻기 위하여 컴퓨터프로그램저작물코드를 복제 또는 변환하는 것"으로 규정하고 있다. 즉 프로그램코드역분석 행위는 코드의 복제 또는 변환 행위라고 할 수 있다. 우리 저작권법상 변환의 의미는 다소 불분명하지만, 상기한 바와 같이 우리 저작권법상 프로그램역분석 행위는 "변환"을 불완전한 복제 또는 창작성 없는 코드의 변환으로 보아야 한다는 견해가 있다.[160]

그런데 이와 같이 해석하게 되면 저작권법상 프로그램코드역분석은 단순히 복제 행위라고 밖 볼 수 없게 된다. 그리고 이 경우 제101조의3 제1항 제6호에서 저작재산권의 제한으로써 복제를 허용하고 있으므로, 이 규정에 의해서도 프로그램코드역분석이 가능하게 된다. 그러나 이것은 프로그램코드역분석 규정을 제101조의3 제1항 제6호와 구분하고자 했던 입법취지[161]에 배치되는 결과이다. 또한 상기한 바와 같이 프로그램코드역분석이 복제로만 해석이 제한되면, 문언해석상 제101조의3의 어떤 경우에도 허용이 되므로 그 범위가 상당히 넓어진다.

그리고 변환에 대해서는 규제 규정이 없다는 점에서 복제와 변환을 별도로 보게 되는 경우에도 입법의 불비로 인한 문제가 발생한다. 즉, 정작 허용 범위를 벗어나는 프로그램코드역분석을 행했을 때에도 제103조의3 제6호의 행위이기만 하면 상관이 없고 설사 변환 행위로 보더라도 법적으로 아무런 문제가 없는 것이다.

따라서 EU 컴퓨터프로그램 지침에서와 같이 변환을 별도로 또는 2차적저작물의 하나로써 규정하는 것이 저작권법 내에서의 의미가 보다 명확해 질 것으로 보인다.

160) 안효질, "프로그램코드역분석 규정의 비교법적 분석-EU 소프트웨어지침을 중심으로-", 창작과권리 제47호(2007년 여름호), 세창출판사, 2007.6, 94면.

161) 과학기술정보통신위원회 수석전문위원, "컴퓨터프로그램보호법중개정법률안 검토보고서", 과학기술정보통신위원회, 2000.12, 2-4면에 다음과 같은 검토 의견이 있다.:
"현행 컴퓨터프로그램보호법에서는 프로그램코드 역분석에 대하여 아무런 정의 규정이나 구체적 허용기준을 두지 않고, 다만 제12조 제6호에 프로그램저작권이 제한되는 사유로 "프로그램의 해법 기타 특정요소를 확인하고 분석 · 연구 · 교육하기 위하여 필요한 경우" 그 목적에 필요한 범위내에서 공표된 프로그램을 복제 또는 사용할 수 있도록 하는 규정을 두어 제12조 제6호의 규정이 역분석에 관한 정의인지의 여부가 불명확할 뿐만 아니라 프로그램저작권자의 권리를 지나치게 제한하여 컴퓨터프로그램보호법의 입법 목적에 위배될 소지가 있었음."
"따라서 법해석의 명확화와 신설된 코드역분석의 판단기준을 제공하고자 프로그램코드역분석에 대한 정의규정을 명확히 두고자 하는 개정안의 취지는 적절한 것으로 봄."
"개정안 제12조 제6호에서는 공표된 프로그램을 복제 또는 사용할 수 있는 경우의 유형으로서 "프로그램 기초를 이루는 아이디어 및 원리를 확인하기 위하여 프로그램의 기능을 조사 · 연구 · 시험하는 경우(정당한 권원에 의하여 당해 프로그램을 사용하는 자가 당해 프로그램을 사용 중인 때에 한한다)"로 재설정 하고 있음."
"개정안의 취지는 프로그램 사용의 주체를 '정당한 권원 있는 자'로 한정하고, 사용의 방법을 '프로그램사용중인 때'로 제한함으로써 역분석에 의해 프로그램 저작권자의 지나친 권리침해를 막기 위한 것으로, 선진외국의 동향을 반영한 것임."

이에 따라 현행 저작권법 제101조의4에 규정된 프로그램코드역분석은 제101조의3 제6호의 규정과는 구분하여 이용자에게 별도의 자유이용의 권한을 부여하는 규정임이 분명해질 것이다. 즉, 저작권자가 이용에 관한 구체적인 허락의 내용을 라이선스에 규정하였다고 해도, 제101조의4 규정에 따라 제48조의 이용허락 규정에 저촉되지 않고 계약에서 자유로울 수 있는 것이다.

3. 민사 및 형사 구제 측면에서의 고찰

처벌규정에는 기술적 보호조치 관련 규정과는 달리 프로그램코드역분석 관련하여 직접 규정한 것은 없다. 따라서 프로그램코드역분석에 대해서는 그 행위의 저작권 침해성을 가지고 처벌 여부를 판단해야 한다. 즉, 복제 및 변환에 따른 저작권 침해 여부가 문제가 된다. 즉, 우리 저작권법상 프로그램코드역분석 규정에 위반하여 프로그램코드역분석을 한 경우에도 이 규정에 따라 직접 형사처벌을 받는 것이 아니라 이것이 복제권 침해가 있는지 또는 변환과 관련된 권리의 침해가 있는지 여부에 따라 형사처벌이 가능하다.

또한 이러한 이유로 이 규정은 복제권 침해나 변환과 관련된 권리의 침해 시에 프로그램코드역분석 규정의 조건에 따르는 경우에는 저작권이 제한되게 된다. 즉, 해당 규정에 따라 저작물의 자유이용이 가능한 것이다.

만약 해당 규정에 따른 형사처벌이 불가한 경우라고 하더라도 이 규정은 쓸모가 없게 되지는 않을 것으로 생각된다. 적어도 이 규정은 계약에 의해 프로그램코드역분석을 금지한 경우에 계약의 내용을 무효화하는 근거가 되는 규정은 될 수 있을 것이다. 즉, 해당 규정을 강행규정이라고 본다면, 적어도 계약에 의한 프로그램코드역분석의 제한은 막을 수 있다는 것이다. 또한 반대로 말하면 계약에 의해 프로그램코드역분석을 제한하지 않았다면, "변환"의 권리의 존재여부 및 제12조의3 제6호에 의한 복제 가능성 여부를 판단하는 것만 남아 있게 된다.

그런데 이것은 EU 컴퓨터프로그램 지침 제6조도 저작재산권의 제한에 해당하는 규정이고, 결국 우리나라의 저작권법의 규정과 별다른 차이는 없다. 다만, 상기한 바와 같이 제6조의 허용범위를 벗어나는 프로그램코드역분석은 "복제" 또는 "변환" 행위에 대해서 관련 저작재산권의 침해로써 규제해야 한다. 따라서 이 경우에도 결국 "변환"을 어떻게 규정하느냐가 중요한 사안으로 남게 된다.

162) EU 컴퓨터프로그램 지침 Recital
Whereas this means that the acts of loading and running necessary for the use of a copy of a program which has been lawfully acquired, and the act of correction of its errors, may not be prohibited by contract; whereas, in the absence of specific contractual provisions, including when a copy of the program has been sold, any other act necessary for the use of the copy of a program may be performed in accordance with its intended purpose by a lawful acquirer of that copy;

4. 오류 수정을 위한 프로그램코드역분석

EU 컴퓨터프로그램 지침 제5조 제1항에는 오류수정(error correction)에 대해 제4조 (a)와 (b)의 적용이 배제되며, 이는 계약으로도 금지하지 못한다.[162] 그리고 이 규정에 따라 자연스럽게 제6조의 프로그램코드역분석도 허용이 된다. 이것은 상기한 바와 같이 제6조의 프로그램코드역분석이 제4조 (a)와 (b)의 의미 내에서의 행위에 대한 규정이기 때문이다. 즉, 제4조 (a)와 (b)의 저작재산권이 이미 제한되어 적용이 되지 않는 상태에서, 이들 권리를 근거로 하고 있는 프로그램코드역분석의 허용 여부를 논한다는 것은 의미가 없는 것이다.

EU 정보사회 지침 Recital (50)[163]에서 EU 컴퓨터프로그램 지침 제5조 제3호 및 제6조에 적용되지 않음을 규정하고 있다. 따라서 프로그램코드역분석의 경우 기술적 보호조치 규정의 우회가 가능하다. 다만, 해당 Recital에는 제5조 및 제6조가 컴퓨터프로그램에 대한 배타적 권리에 대한 예외를 배타적으로 규정할 수 있음을 규정하고 있을 뿐인데, 이러한 점에서는 문언해석상 오류수정을 위한 프로그램코드역분석의 경우에는 기술적 보호조치 규정의 우회가 가능할 것으로 보이지는 않는다.

우리 저작권법의 경우 EU와 같이 프로그램코드역분석에 대한 명시적인 규정을 두고 있다는 점에서 미국 저작권법과 다르다. 따라서 이러한 점에서는 프로그램코드역분석의 허용 범위에 오류수정에 관한 규정을 두는 것도 필요하지 않나 싶다.[164] 물론, 향후 한 · 미 FTA 이행을 위해 법률이 개정되는 경우에는 공정이용 규정이 저작권법에 포함되게 될 것이지만, 프로그램코드역분석은 공정이용 규정에서 배제되어 있으므로 오류수정을 위한 프로그램코드역분석도 배제된다.

이외에 한 · 미 FTA 이행을 위해 법률이 개정되는 경우에 컴퓨터프로그램의 오류수정과 관련하여 컴퓨터의 유지 · 보수를 위하여 그 컴퓨터를 사용하는 과정에서 일시적 복제가 발생하는 경우에 저작재산권이 제한되고, 현행 저작권법상 컴퓨터의 유지 · 보수는 동일성유지권에 관한 규정인 제13조 제2항에 따라 해당 규정이 허용하는 범위 내에서 허용될 수 있다. 그러나 프로그램코드역분석과 관련하여 관련 내용이 존재하지 않는다.

따라서 한 · 미 FTA 이행을 위해 법률이 개정되는 경우에도 EU가 EU 컴퓨터프로그램 지침 제5조에 따라, 미국이 저작권법상 공정이용 법리에 따라 허용하는 것으로 판단할 수 있는 것에 비해 프로그램코드역분석의 허용범위가 좁아진다.

163) (50) Such a harmonised legal protection does not affect the specific provisions on protection provided for by Directive 91/250/EEC. In particular, it should not apply to the protection of technological measures used in connection with computer programs, which is exclusively addressed in that Directive. It should neither inhibit nor prevent the development or use of any means of circumventing a technological measure that is necessary to enable acts to be undertaken in accordance with the terms of Article 5(3) or Article 6 of Directive 91/250/EEC. Articles 5 and 6 of that Directive exclusively determine exceptions to the exclusive rights applicable to computer programs.

164) 강기봉 · 정봉현, "컴퓨터프로그램보호법상 S/W 리버스 엔지니어링 규정에 관한 소고", 창작과 권리 제42호(2006년 봄호), 2006. 98면; 안효질, "프로그램코드역분석 규정의 비교법적 분석: EU 소프트웨어지침을 중심으로", 창작과권리 통권47호(2007년 여름), 세창출판사, 2007, 104면.

이와 관련하여 저작권법에 오류수정을 위한 프로그램코드역분석을 허용하도록 개정하는 방법, 공정이용의 원칙을 적용하여 이러한 경우에도 프로그램코드역분석이 허용되도록 해석하는 방법 등이 있을 것이다.

Ⅱ. 기술적 보호조치 관련 법제도 개선방안

1. 한 · 미 FTA 협상안과 이행법안의 정합성

한 · 미 FTA 협약을 통해 우리나라는 접근통제형(Access control) 기술적 보호조치의 개념을 도입하였고, 이를 이행하기 위한 한 · 미 FTA 이행법안에 대한 논의를 전개하고 있다. 이러한 논의에서 가장 큰 쟁점은 접근통제에 대한 예외를 규정하고 있는 협정문을 얼마만큼 정확히 이행법안에 담아낼 것인지에 관한 문제와 3년 마다 미국에 통보하도록 되어 있는 기술적 보호조치에 대한 추가적 예외로서 고려될 수 있는 사항에 관한 문제이다. 즉 전자는 한 · 미 FTA 협정문과 이행법안과의 정합성의 문제이고, 후자는 일종의 접근통제권의 도입에 따른 공정이용의 축소를 방지하기 위한 문제이다.

우선 첫 번째와 관련하여, 이행법안의 내용과 FTA 협정문의 내용이 다소 일치하지 않는 문제점이 있으므로 검토 및 개선이 요구된다. 첫째, 접근통제의 무력화에 대한 예외로서 허용되는 "암호화연구"의 요건과 관련하여, 이행법안에서는 "저작물등의 복제물을 정당하게 이용하는 자가 저작물등에 적용된 암호 기술의 결함이나 취약점을 조사 · 연구하기 위하여 필요한 범위에서 행하는 경우" 접근통제형 기술적 보호조치를 무력화할 수 있도록 규정하고 있다. 그러나 FTA 협정문에서는 위 이행법안에서 규정하고 있는 내용 외에도 '권리자로부터 사전 허락을 얻기 위한 노력', '연구자의 자격', '선의' 등에 관해 규정하고 있다. 따라서 결과적으로 이행법안이 협정문의 규정보다 완화된 요건을 규정하게 되므로 향후 미국으로부터 정합성의 문제 제기될 수 있으며, 이에 대한 검토와 보완이 필요하다고 본다.

둘째, 한 · 미 FTA 협정문상의 '안전성 검사'에 관한 규정(§18.4.7(d)(iv))은 개정안에 아예 포함되어 있지 않으므로 역시 협정문의 충실한 이행을 하였는지에 대한 이의제기를 받을 수 있으며, 또한 이를 규정하지 않음으로 인하여 컴퓨터 시스템에 대한 보안성 검사 및 조사를 위한 공정한 사용이 뜻하지 않게 처벌받을 수 있다. 따라서 이에 대한 보완도 필요하다.

셋째, 프로그램코드 역분석과 관련해서는 현행 저작권법과 이행법안 및 협정문 사이의 관계를 명확히 정립할 필요가 있다. 협정문 §18.4.7(d)(i)에서 기술적 보호조치의 무력화에 대한 예외로서 프로그램 역분석을 허용하고 있다. 이는 협정문이 미국의 DMCA 제1201조(f)에 기초하고 있기 때문이다. 그러나 현행 저작권법 제101조의4에서 규정하고 있는 호환 목적의 프로그램코드 역분석은 기술

적 보호조치와는 무관한 것으로 일정한 역분석만을 허용하고 있다. 따라서 향후 접근통제에 관한 규정이 도입될 경우 이 조항은 기술적 보호조치의 예외에 대한 근거로서 규정될 필요가 있다. 그렇게 함으로써 저작권법 제101조의3에서 규정하고 있는 저작권 제한사유는 일반적인 역분석에 대한 근거로서 활용될 수 있을 것이다. 미국에서도 기술적 보호조치의 회피 목적이 없는 일반적인 역분석 행위의 저작권 침해 판단은 공정사용 법리에 따라 해결하고 있다.

2. 공정사용 개념의 도입과 추가적 예외

한 · 미 FTA 협정문을 이행하기 위한 개정 법률안에서 규정하고 있는 접근통제의 예외사유들은 현행 저작권법상의 저작권제한사유와는 독립된 것이다. 이는 미국의 DMCA에서 접근통제에 대한 예외를 공정이용(fair-use) 법리와는 결부시키지 않는 것과 동일한 접근방식이다. 즉 접근통제형 기술적 보호조치를 무력화하는 어떤 행위가 저작권법상 공정이용에 해당한다고 하더라도 DMCA에서 별도로 정한 예외에 해당되지 않는다면 여전히 위법한 행위가 될 수 있다. 이러한 접근방법에 대해 미국 내에서도 기술적 보호조치의 무력화에 대한 엄격한 예외를 별도로 규정하는 것은 공정이용을 지나치게 축소시키고 장기적으로 문화발전을 저해할 수 있다는 비판이 제기되고 있다.

따라서 협정문에서 열거하고 있는 8가지 예외만으로는 접근통제권에 대한 충분한 안정장치가 될 수 없으므로 장기적으로는 저작권제한 사유에 해당하는 정도의 예외가 필요하며, 이러한 측면에서 저작권제한 사유와의 연계를 모색할 필요가 있다. 아울러 접근통제권을 권리자에게 부여함으로써 상대적으로 위축될 수 있는 이용자의 권익을 보완하기 위한 조치로서 포괄적인 공정이용(fair-use)에 관한 규정을 적극적으로 도입할 필요가 있다. 그러나 현실적으로 저작권법상의 공정이용에 관한 규정과 접근통제권의 예외를 연계시키는 문제는 미국 DMCA의 수정을 전제로 하는 것이므로 매우 어려운 과제라고 할 수 있다.

한편 앞서 Edelman 사건에서 본 바와 같이, 프로그램상의 오류를 분석하기 위하여 기술적 보호조치를 무력화하는 행위도 예외로서 고려해 볼 수 있는데, 협정문상의 허용되는 '안전성 검사'가 되기 위해서는 시스템의 소유자나 운영자의 허락이 전제되어야 하고, 또한 이러한 예외는 기술적 보호조치의 무력화 행위 자체에만 한정되는 것으로 무력화 도구를 배포 · 전송하는 행위는 인정되지 않는다. 그러나 기술적 보호조치의 무력화 도구가 연구목적의 일환으로 행하여지고, 또 그 도구의 배포 · 전송 행위로 인하여 저작권자와 일반 공중이 일정한 이익을 얻는 경우라면 제재에 대한 예외로서 규정해 볼 수 있다고 본다.

SW 역분석과 기술적보호조치

2009년 12월 4일 인쇄
2009년 12월 4일 발행

발 행 인 이보경
발 행 처 한국저작권위원회
서울특별시 강남구 개포동길 619
서울강남우체국 6~7층 (135-240)
TEL. 02-2660-0000(代)
FAX. 02-2660-0079
http://www.copyright.or.kr
인 쇄 처 호정씨앤피(☎ 02-2277-4718)
I S B N 978-89-6120-048-6 94010
978-89-6120-047-9(세트)