공학석사 학위논문

단일 인증을 통한 기업내 정보유출 방지 DRM 시스템

2011년 2월

부 경 대 학 교 산 업 대 학 원

컴 퓨 터 공 학 과

황 진 희

공학석사 학위논문

단일 인증을 통한 기업내 정보유출 방지 DRM 시스템

지도교수 정 목 동

이 論文을 工學碩士 學位論文으로 提出함

2011년 2월

부 경 대 학 교 산 업 대 학 원

컴 퓨 터 공 학 과

황 진 희

이 논문을 황진희의 공학석사 학위논문으로 인준함

2011년 2월 23일

주 심 공학박사 윤 성 대 (인)

위 원 공학박사 조 우 현 (인)

위 원 공학박사 정 목 동 (인)

목 차

그 림 목 차

표 목 차

단일 인증을 통한 기업내 정보유출

방지 DRM 시스템

황 진 희

부 경 대 학 교 산 업 대 학 원 컴 퓨 터 공 학 과

요약

정보화시대를 맞이해 사무실이나 가정에서의 컴퓨터 사용은 일상화되고 있으며, 의존도 또한 높아져 가고 있다. 그리고 디지털 융합에 의해 다양한 형태의 장치와 함께 통신이 결합된 새로운 기능의 디바이스들을 속속 선보이고 있어 생활의 편리함이 커지고 있다. 이러한 편리함과 유용성에 비례하여 역기능도 매우 커지고 있다. 심각한 역기능중의 하나가 정보유출이며, 컴퓨터내의 데이터나 파일들의 보관이나 전송에 대해 보안이 중요한 요소가 되었다. 컴퓨터에 저장된 자료나 파일을 국가적인 중요한 보안자료가 될 수 있으며, 기업에서는 기업의 성패가 좌우될 수 있는 기술, 영업, 경영 등

의 기업 보안자료일 수 있고, 개인의 보안자료가 될 수도 있다.

온라인 상에서의 정보 교환이 활발히 이루어져 있으며 그에 따라 기업내의 정보 유출 및 단말기 해킹에 대한 위험요소도 빠르게 증대되고 있다. 보안 위험 요소를 보완하기 위해 새로운 패러다임의 발전과 더불어 네트워크, 시스템, DB 등의 보안 및 관리 통합의 기술들이 개발되고 있지만 여전히 주요 기업에서 기업 기밀정보가 유출되는 보안 사고가 빈번히 발생한다.

이를 해결하기 위해서 본 논문에서는 기업유출에 대한 심각성에 대해서 살펴보고 이를 정보유출 보호를 위하여 단일 인증을 통한 데이터보호 기술을 제공한다. 단일 인증을 통해 서버를 통합해서 관리해줌으로써 데이터 흐름에 대해서 체계적으로 관리가 가능하며 별도 인증 절차 없이 이용이 가능하게 설계하였다. 별도 존재했던 DRM서버를 AD와 연동시켜 업데이트되는 유틸리티간의 상호호환 및 재설치도 용이 하게 되었다.

기존 DRM 솔루션 종류의 문제점에 대해서 분석 하고, 정보유출 및 문서보안을 위한 주요정책에 대해서도 살펴본다. 이를 통하여 기밀성, 무결성, 가용성, 인증, 권한부여 서비스를 제공한다.

라이센스 전송 및 변환 기술을 적용하여 이기종 단말과의 DRM 연동이 가능하도록 구현이 되어야 하고, 모바일 DRM 기술 개발이 필요하다. 타 분야 간 DRM 호환성 미비로 인한 사용자, 기기제조 기업의 불편 및 비효율성 부분도 해결해 나가야 할 부분이다. 또한 전반적인 콘텐츠 유통 환경을 고려한 DRM에 대한 인식도 갖추어야 한다.

DRM System for Prevention of Industry Information Leakage using SSO

Jin Hee Hwang

Department of Computer Engineering, Graduate School,

Pukyong National University

Abstract

The information society, no Office or at home, the use of the computer and doesn't, dependence also. And Digital Fusion by various forms of communication with the device, the combined new features being introduced to the devices of this convenience is growing. These convenience and usability features very station in proportion to the growing. Serious dysfunction of any of the information disclosure, and the data within the computer or the file's archive or transport for security was

an important element. Data stored on your computer, or a file, a critical national security can be material, the success of the enterprise, companies can be influenced by the technology, sales, management, and enterprise security materials, and personal security could be material.

Online actively exchange of information that consists of companies according to the information disclosure and handset hacking for risk factors increase quickly. Security risks to compensate for a new paradigm of development and with the network, system, DB, such as security and management integration of the technologies being developed, but still the major corporations in the business confidential information being leaked security accident occurs frequently. In order to resolve this, this thesis, corporate disclosure, for a look at this for the seriousness, information disclosure, to protect data over a single authentication protection technology. Through a single authentication server consolidation and management for data flow well-organized management without a separate authentication procedures available to the design. Separate DRM server was present AD and linked update utility is a cross between compatible and reinstall was also facilitates.

Existing DRM solution types of issues and for analysis, information disclosure, and document security for major policy scans for. This throughout the confidentiality, integrity, availability, authentication, authorization, provides the service.

License transfer and transformation techniques applied to the heterogeneous devices, the implementation of the DRM to enable communication and be, mobile DRM technology development is needed. DRM compatibility between other areas due to the user, appliance manufacturing companies, uncomfortable and inefficiencies part should resolve. In addition, considering the overall content distribution environment, and recognition for the DRM also should have.

1. 서론

인터넷의 급속한 보급 및 기업 내 네트워크 환경의 발달로 인하여 회사내의 모든 업무들이 컴퓨터를 떼놓고는 일을 할 수가 없게 되었다. 그러다 보니 이러한 많은 기술들과 정보들이 디지털화된 데이터들로 저장되고 처리되는 이 시대에 있어서 각 기업들도 몇 년간 계발되어온 정보나 회사의 기밀사항들을 디지털 정보로 저장하고 유지하고 있다. 이렇게 저장된 디지털 컨텐츠는 인터넷을 통하여 접근이 용이하게 되었고, 디지털 데이터의 특성상 데이터의 삭제 및 복제가 쉬어, 삭제할 경우 데이터의 무결성을 손상시킬 뿐 아니라 기업의 신뢰성 하락을 이야기 할 수 있고, 또한 원본과 동일한 디지털 데이터를 재사용하고 재가공 함으로써 그동안의 투자 회사에 대하여 치명타를 줄 수가 있다. 이렇게 복제된 데이터는 e-mail 이나 웹 하드 등의 네트워크나 usb메모리 및 하드 디스크 등의 저장매체를 통해서 쉽고 빠르게 배포되어 데이터의 불법 복사 및 배포가 가능하게 되었다.

온라인 상에서의 정보 교환이 활발히 이루어져 있으며 그에 따라 기업내의 정보 유출 및 단말기 해킹에 대한 위험요소도 빠르게 증대되고 있다. 보안 위험 요소를 보완하기 위해 새로운 패러다임의 발전과 더불어 네트워크, 시스템, DB 등의 보안 및 관리 통합의 기술들이 개발되고 있지만 여전히 주요 기업에서 기업 기밀정보가 유출되는 보안 사고가 빈번히 발생한다. 취약점 및 위험요소에 대한 대응은 상대적으로 취약한 상황이다.

이러한 기업 비밀정보 유출에 따른 피해는 해당 기업에 그치지 않고 국가 경제에 막대한 손실은 초래할 수 있어 심각한 문제를 가지고 있다. 이와 같

은 문제를 해결하기 위하여, 각 기업에서는 보호구역의 설정, 기업 내에서 활용되는 기밀문서에 대해서는 DRM(Digital Right Management)을 기반으로 한 시스템을 구축하여 문서유출을 방지하고자 노력하고 있으며, 네트워크망 분리 및 중요 네트워크 트래픽 필터링을 통해 기밀 정보의 유출을 차단하는 등 다양한 보안 대책을 적용하고 있다.

이들 중에는 정보유출 방지 기술인 DLP(Data Loss Prevention), 데이터 보호기술인 DRM, 바이오 정보를 이용한 사용자 인증 등 내부 유출을 막기 위해 보호하는 기술이 널리 활용되고 있다.

각 기업에서는 보호구역의 설정 기준을 정확하게 설정하기 위해서 엑티브 디렉토리(Active Directory)를 구성하여 작업그룹들에게는 마치 웹 사이트처럼 도메인 이름이 부여되고, 클라이언트(윈도우, 매킨토시, 유닉스 등)라도 여기에 액세스 할 수 있게 된다[3]. 엑티브 디렉토리가 구성되지 않은 클라이언트에서 문서를 열고자 할 경우 DRM 기술이 적용되어 문서를 열고자 할 경우 암호화 적용되는 방법에 대해서 제안하고 구현시 고려사항을 기술한다.

1.1 연구의 목적

기업의 단말기에 대한 지침은 국가사이버안전센터의 국가사이버 안전메뉴얼을 통해 제시하고 있다. 국가사이버메뉴얼에서 제시하는 PC 보안 관리 부분은 공유폴더, 비인가자의 접근제어, OS 통제(비밀번호, 화면보호기, 부팅통제), 바이러스 통제, 문서 보호를 위한 암호화, 노트북의 반출제어의 간단

한 지침만을 제공하고 있어 실제 PC 보안을 위해 갖추어야 할 기업의 보안 지침과는 거리가 있다.

기업마다 중요 정보에 대한 차이가 있을 수 있으며, 이번 연구에서 제시하고 하는 것은 정보유출 기능에 대해 기존의 DRM, PC보안의 매체제어 기능의 문제점을 분석하고 정보유출 기능의 효과적인 방법에 대해 연구한다.

1.2 연구의 방법 및 범위

최근 들어 기업정보 유출사고는 내부직원의 소행인 사고가 대부분이다. 이와 같은 정보유출을 막기 위해 많은 보안 솔루션이 존재하지만 내부통제에 대한 정보유출을 막기에는 한계가 있다. 본 논문에서는 기업이 보유하고 있는 정보를 안전하게 외부로부터 보호 할 수 있는 방안을 연구 하고자 한다. 기업의 정보유출에 대한 심각성을 조사하고 장치 매체를 통한 유출방지 기능의 현황을 파악하고 문서보안에 대한 취약성 및 위협요소를 분석하여 기업의 프로세스에 맞는 DRM을 분석하고 기업의 현실에 맞는 개선방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 다루고, 관련연구에서는 기업정보유출, 엑티브 디렉토리, DRM에 대해서 살펴보고, 3장에서는 단일인증 기반 DRM 시스템 설계 및 구현, 마지막 장에는 결론 및 향후 연구 방향을 논한다.

2. 관련 연구

2.1 기업 정보 유출 기술

정보화시대를 맞이해 사무실이나 가정에서의 컴퓨터 사용은 일상화되고 있으며, 의존도 또한 높아져 가고 있다. 그리고 디지털 융합에 의해 다양한 형태의 장치와 함께 통신이 결합된 새로운 기능의 디바이스들을 속속 선보이고 있어 생활의 편리함이 커지고 있다. 이러한 편리함과 유용성에 비례하여 역기능도 매우 커지고 있다. 심각한 역기능중의 하나가 정보유출이며, 컴퓨터내의 데이터나 파일들의 보관이나 전송에 대해 보안이 중요한 요소가 되었다. 컴퓨터에 저장된 자료나 파일을 국가적인 중요한 보안자료가 될 수 있으며, 기업에서는 기업의 성패가 좌우될 수 있는 기술, 영업, 경영 등의 기업 보안자료일 수 있고, 개인의 보안자료가 될 수도 있다

미국의 CSI(Crime Scene Investigator)/FBI(Federal Bureau of Investigation)가 2001년 실시한 기업의 기밀정보 유출 실태 조사에 따르면 내부자에 의한 정보유출의 경우가 외부 해커에 의한 경우보다 9배나 높은 것으로 나타나 내부자에 의한 정보 유출 정도가 더 심각하다는 것을 알 수 있다.

2.1.1 정보보호의 개요

정보를 보호한다는 것은 어떤 정보가 어떻게 악용·오용될 수 있는지를 살

펴보고 이를 방지하기 위한 모든 노력 및 대책들을 강구하는 것을 말한다. 정보를 보호하기 위해서는 그 정보가 어떠한 위험에 노출되어 있는지에 대해 고려하고 조사하는 것이 선행되어야 한다. 일반적으로, 가장 먼저 생각할 수 있는 위험은 어떤 정보에 대하여 그 정보에 접근할 수 있는 권한이 없는 사람이 조회를 통해 그 내용을 노출, 변경, 파괴할 수 있다는 것이다.

정보보호의 목적은 정보가 생성되어 소멸되기까지 그 처리 및 유통의 생명 주기 전반에 걸쳐 기밀성(Secrecy, Confidentiality), 무결성(Accuracy, Integrity), 가용성(Availability)을 확보하는 데에 있다. 조직이 필요로 하는 정보보호의 유형에 따라 그로부터 도출되는 보안 관련 요구사항을 만족시키기 위해서 필요한 보안 기술 및 제품 선택이 달라질 수 있다.

(1) 기밀성

안정한 정보 시스템을 구축하기 위해서는 허가되지 않은 사용자에게 정보를 공개해서는 안 된다. 신뢰할 수 있는 안전이 확보된 정부 시스템에서는, 사용자가 자신의 비밀 정보 취급 허가의 특성에 따라 접근할 수 있도록 허가된 정보에만 접근할 수 있음을 보증해 줌으로써 기밀성을 유지한다. 기업의 경우에는 기업 내부용 메모나 경쟁 전략 문서와 같은 민감한 기업 데이터뿐만 아니라 고용 정보와 같은 개인 정보의 보호를 위해서 기밀성은 반드시 지켜줘야 한다. 시스템의 기밀성을 강화하기 위해서는 누가 시스템에 접근하는지, 또 각각의 사용자가 시스템에서 어떠한 작업을 수행할 수 있는지에 대해 제어할 수 있어야 한다. 이를 위한 보안 대책으로는 접근통제 방법을 사용한다. 뿐만 아니라 비록 정보가 누출되더라도 그 내용을 허가받지 않은 사용자가 해독할 수 없도록 암호화 기법을 사용할 수도 있다.

(2) 무결성

안전한 컴퓨터 시스템은 저장하고 있는 정보의 무결성을 영구적으로 유지할 수 있어야 한다. 무결성은 시스템이 정보를 변조하거나 비인가된 사용자가 악의적인 또는 의도하지 않은 변화를 유발시키는 것을 방지해야 한다. 네트워크 통신에서는 데이터 무결성과 관련하여 인증성(Authenticity)이 보장되어야 한다. 인증성은 누가 네트워크에 접근하여 정보를 제공하였는지를 결정하고, 데이터의 전송 및 수신 시점을 기록함으로써 데이터의 출처를 확증하는 방법을 제공한다. 메세지가 위조 혹은 변조되지 않았는지 확인한다.

(3) 가용성

안전한 컴퓨터 시스템은 사용자가 필요로 할 때에는 언제든지 정보를 이용할 수 있도록 유지 관리되어야 한다. 가용성이란 컴퓨터 시스템의 하드웨어와 소프트웨어가 효율적으로 작업을 수행하며, 사고 및 재앙이 발생하더라도 신속하고 완전하게 복구 할 수 있는 특성을 의미한다.

가용성의 반대 개념은 서비스 거부(Denial of Service)이다. 서비스 거부는 시스템 사용자가 자신이 필요로 하는 자원 얻을 수 없는 상태를 의미한다.

가용성을 유지하기 위해서는 주의 깊게 시스템을 관리하고 시스템 디자인에 완벽을 기해야 한다. 모든 정보는 주기적으로 백업을 수행해야 하며, 시스템의 변경과 관련하여 형상 관리 및 변경 관리, 시스템에 이상이 발생한 경우에 대비하여 업무절차에 지장을 주지 않도록 사업 연속성 계획과 재난 복구 계획을 수립해 두어야 한다.

2.1.2 정보유출의 정의

정보유출이란 개인 및 기업이 가지고 있는 정보, 개인의 경우 개인에 대

한 신체적, 경제적, 사회적 사실·판단·평가 및 도용이 가능한 개인에 관한 고유정보(성명, 주민등록번호 등), 기업의 경우 기업에 대한 경제적, 사회적 가치를 가지고 있는 물리적(핵심장비, 결과물 등), 논리적(핵심기술, 기업기밀 등) 정보를 다양한 이익을 위해 정보의 주체가 동의하지 않은 상태로 무단으로 가져가는 행위를 말한다.

2.1.3 정보유출의 특징

내부정보유출의 특징은 첫째 발생횟수는 적지만 발생하게 되면 미치는 영향이 매우 크다는 것이다. 둘째 위험요소가 매우 구체적이지만 통제가 매우 어렵다. 셋째 매우 다양한 유출경로가 존재한다. 넷째 한번에 대용량의 정보유출이 가능하다. 다섯째 내부정보 유출되는 것을 인지하기 어렵다. 마지막으로 대부분 사람에 의해서 유출된다.

2.1.4 정보유출 실태

기술유출 적발현황은 연도별로 살펴보면 기술유출 적발현황은 연도별로 살펴보면 2003년 6건에 불과하던 것이, 2004년에는 26건, 2005년 29건, 2007년에는 32건으로 지속적으로 증가하고 있다.[3]

응답 중소기업의 17.8%가 최근 3년간 산업기밀의 외부 유출로 인한 피해를 입은 것으로 나타났으며, 이중 52.6%가 2회 이상의 기밀유출 경험이 있는 것으로 나타났다. 산업기밀 유출경험이 있는 기업의 건당 피해금액은 '1억 ~ 이상 5억 미만'이 37.1% 가장 높게 나타났으며, 1건당 5억 이상의 피

해를 입었다는 기업도 26.7%로 조사되었다.

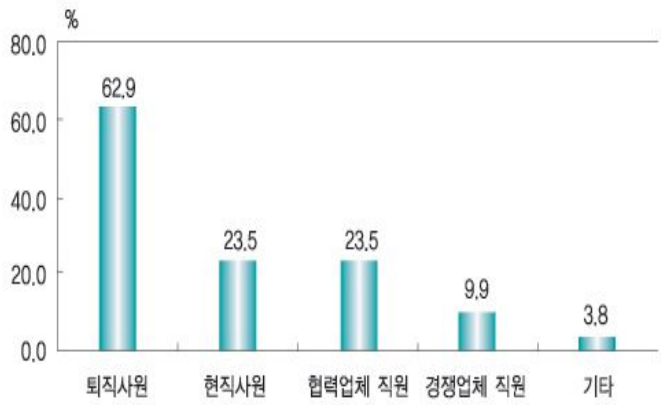

그림 1. 산업기밀 유출 관련자 (출처:[2])

그림 1처럼 산업기밀 유출 관련자로는 퇴직사원이 62.9%로 가장 많았으며, 현직 사원(23.5%), 협력업체 직원(23.5%), 경쟁업체 직원(9.9%) 들에 의해 기밀 유출이 발생한 것으로 나타내고 있다.

2.1.5 내부 정보 유출 위협 요소

내부 정보가 저장되어 있는 장소를 주체로 보면 서버(Server)나 호스트(Host) 또는 PC가 정보 유출의 보호 대상이 되고, 내부 정보가 유출되는 목적지를 개체로 보면 이에 해당하는 외부 저장장치, 통신장지, 출력장치 등으로 구분할 수 있다.

첫째, 저장장치를 이용한 정보 유출 위협 요소

PC에 내장되어 있는 저장장치에는 플로피 디스크(FDD), 하드 디스크(HDD), CD-R/W, DVD-R/W 등이 있고, USB또는 IEEE-1394 포트를 이

용한 USB 저장장치, 외장형 HDD, 디지털카메라 및 캠코더, MP3 플레이어 등이 있다. 국가기관 및 공공기관, 대기업 등에서 일반적으로 사용하는 노트북을 외부로 무단 반출하여 대용량의 정보를 한꺼번에 유출할 수도 있다. 또한 패러럴 통신이나 시리얼 통신, 랜(LAN) 환경에서 네트워크 공유 및 가상 드라이브를 설정하여 내부 정보를 유출하기도 한다.

둘째, 통신장지를 이용한 정보 유출 위협 요소

유선통신의 경우에는 랜카드 또는 모뎀 등, 무선통신의 경우에는 무선랜, 이동통신 서비스, 근거리 무선통신 등이 해당 된다.

무선랜은 사용자 컴퓨터에서 AP(Access Point) 구간까지 무선으로 운영되고, 근거리 무선통신은 블루투스 및 적외선 통신 등이 있다. 또한 이동통신 서비스는 최근 와이브로(Wibro), HSDPA 방식과 PDA 및 휴대폰을 통하여 정보를 유출할 수 있는 위협 요소이다. 통신장치의 위협은 대용량 웹메일 및 웹 하드 서비스와 결합하여 더욱 커다란 문제점을 발행시킬 수 있다.

셋째, 출력장치를 이용한 정보 유출 위협 요소

PC 로컬 프린터와 네트워크 프린터를 연결하여 이용하거나, 최근 보편화된 복합기를 이용하여 내부 정보를 손쉽게 유출 할 수도 있다.

초고속 인터넷에 연결되어 있는 외부 프린터 또는 복합기에 내부 기밀정보를 출력할 수 있는 것은 물론 파일 박스에 저장할 수도 있는 심각한 위협이 있다.

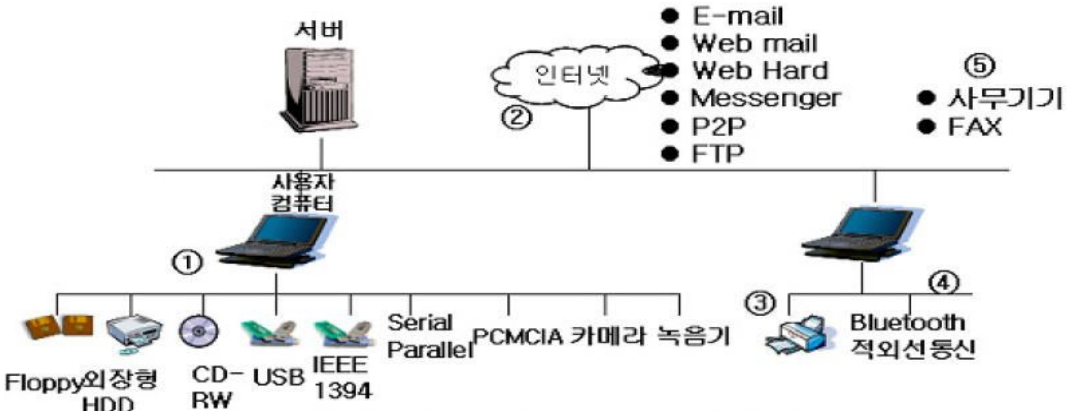

그림 2. 컴퓨터 내 저장된 파일의 유출경로 (출처:[1])

내부 사용자에 의해 컴퓨터내에 저장된 파일이 외부로 유출되는 형태는 그림 2과 같이 구분할 수 있다.

2.1.6 정보유출의 대응과 기본요소

내부정보 유출에 대응하는 방법으로는 크게 3가지 측면 관리적, 물리적, 기술적 측면에서 협동으로 대응이 이루어져야 한다.

가. 관리적 보안

관리적 측면에서는 정보유출 대응에 대해서 어떤 정책을 사용할 것인지, 관리방법을 어떻게 할 것인지 등을 관리하게 된다. 내부 인원에 대한 보안관리, 외부 인원에 대한 보안관리, 중요 자료에 대한 보안관리로 나누어진다 [4].

내부 인원에 대한 보안관리는 기업 내에서 근무하게 되는 인원에 대한 관리를 말한다. 직원의 채용, 재직, 퇴직 등의 단계별로 관리하며 채용시 정보

사용에 대한 기업에 맞는 보안 서약서를 작성하는 것이 좋다.

외부 인원에 대한 보안관리는 업무상 정기적으로 출입하는 협력업체 직원 등에 관한 관리이다. 외부에서 출입하는 직원에 대해서는 최소한으로 제한하고 출입지역도 일정한 한계를 두어 핵심시설에는 일체 접근하지 못하도록 엄격하게 통제해야 한다.

중요 자료에 대한 보안관리는 기업의 핵심이 되는 정보·자료의 관리에 관한 것이다. 제품의 설계도·소스 코드 등 핵심기술 자료는 영업비밀로 분류하고 비인가자는 접근하지 못하도록 물리적·기술적 보안대책을 강구해야 한다.

나. 물리적 보안

물리적 측면에서는 실제 정보에 대해 직접적으로 보안을 적용하는 방법을 말한다. 정보를 관리하는 구역, 장소, 방법 등에 대해서 관리하게 된다.

물리적 보안은 표 1와 같이 두 가지로 크게 나눌 수 있다.

표 1. 조직의 정보자산 유형

구분		저장 매체	저장 형태	정보 유형	보안 영역
정보자산	일반문서	공장 또는 사무실	출력물	주요문서, 보고서 및 제안서 등 과 같은 단위 정보가 가공된 물리적 정보	물리적 보안
	전자문서	서버	문서 및 DB	보고서 및 제안서 등과 같이 단위정보가 가공된 전자적 정보 및 트랜잭션 및 파일 형태의 정보	기술적 보안
		개인용 컴퓨터	문서 파일	보고서 및 제안서 등과 같이 단위정보가 가공된 전자적 정보	
		네트워크	전송 패킷	표준화된 형태의 전송 단위 정보	

다. 기술적 보안

정보의 유출을 방지할 수 있는 기술적인 보안방법으로는 정보에 대한 접근을 제한하거나 차단하는 방법, 데이터나 파일을 암호화하여 권한이 없는 사용자는 파일 내용을 열어볼 수 없도록 하여 정보의 노출을 방지하는 방법, 데이터나 파일이 유출되는 경우에 로그를 남겨 유출되는 내용을 모니터링 하는 방법이 있으며, 유출경로에 대해 복사를 제한하거나 파일 전송을 차단하는 방법, 데이터나 파일이 저장된 장치를 파괴하는 방법 등 이 있다.

그림 3처럼 문서에 대한 위협과 보안 취약점은 정보의 생성부터 파기까지의 흐름을 살펴볼 수 있다. 정보는 생성·저장, 정보열람, 정보편집, 정보 반출, 정보공유, 정보파기 단계의 과정을 거칠 수 있다.

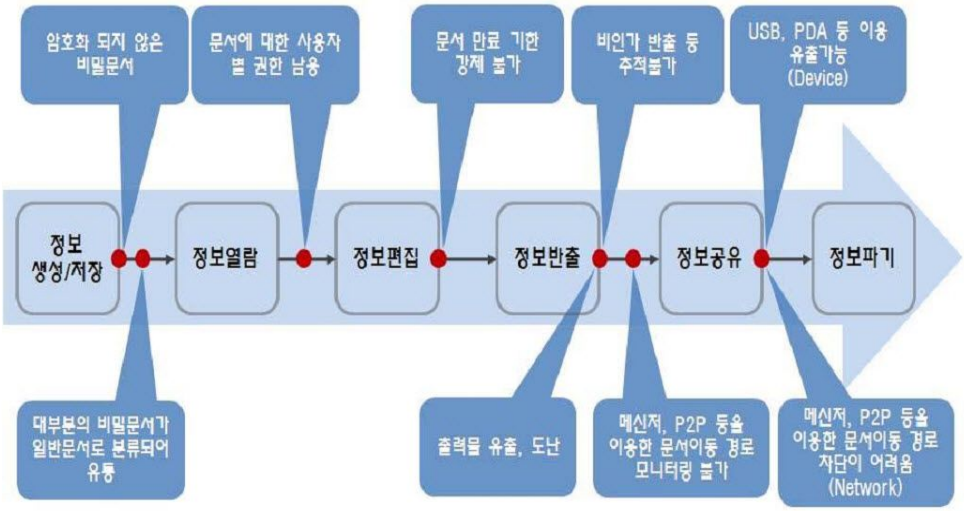

그림 3. 문서에 대한 위협·보안 취약점 (출처:[4])

2.1.7 내부 정보유출 방지 관련 국내 상용 제품

최근 국내·외에서 심각하게 부각되고 있는 조직의 내부 정보 유출 사고를 예방하기 위한 다양한 방법과 기술이 연구되고 있으며, 상용 제품이 계속 출시되고 있다. 현재 상용 제품으로 출신 된 내부 정보 유출을 방지 기술은 크게 세 가지가 주류를 형성하고 있다. 첫째 내부 정보가 이동하는 경로를 차단하고 관리하술 기술, 둘째 내부 정보 자체에 암호를 걸어 비인가자가 볼 수 없도록 하는 기술, 셋째 정보 유출 방지 도구들이 제대로 동작하는지 등을 점검·관리 하는 기술로 나눌 수 있다[5].

표 2는 내부 정보 유출 방지 기술 및 상용 제품 현황을 나타내고 있다.

표 2. 내부 정보 유출 방지 기술 및 사용 제품 현황

구 분	업체명	제품명	특 징
데이터 손실 방지 (DLP)	컴트루테크놀로지	넷센터	내부정보 유출 방지와 매체 제어
	와이즈허브시스템즈	그라디우스	여러 유출 경로에 대한 통합된 시스템 제공
	소만사	DB-i	유출 경로 관리
	지란지교소프트	스팸스나이퍼	토털 유해 메일 방지
문서 보안	마크애니	다큐먼트 세이퍼 e페이지세이버	문서 유출 방지, 위·변조 방지
	파수닷컴	파수 엔터프라이스 DRM 스위트	유연한 대응
	소프트캠프	다큐먼트 시큐리티	비인가자의 부적절한 접근 금지
DB 보안	바넷정보기술	미들만	DB 하이더 기능, SQL 인젝션 탐지 차단 기능
	펜타시큐리티시스템	디아모	정보만을 선택해 암호화
네트워크 접근 제어 (NAC)	유넷시스템	애니클릭	안전성이 검증된 단말기만이 네트워크에 접속 할 수 있도록 하는 보안 플랫폼
	지니네트웍스	지니인 NAC	네트워크 구성 변경 없이 손쉽게 적용 가능
	시만텍	SEP-SNAC	네트워크 접근 제어 동시 제공하는 통합 엔드포인트 보안 솔루션
통합 PC 보안	닉스테크	세이프PC패키지	중앙집중적인 관리로 통합적으로 PC 보호
	뉴테크웨이브	PCMS + VC6.0	프로그램 차단 기능 및 방화벽 기능 인가되지 않은 포트 차단

2.2 Active Directory 이론적 고찰

2.2.1 Active Directory 개념

Active Directory는 디렉터리에 정보를 생성하고, 유지, 관리하며 이 디렉터리에 존재하는 다양한 정보들을 사용할 수 있도록 해주는 서비스를 말한다. 네트워크와 관련된 모든 개체(사용자와 그룹, 컴퓨터, 프린터, 응용 프로그램과 서비스, 공유 자원 등)의 정보를 저장하고 사용자와 응용프로그램이 이 정보를 사용하기 위한 기능을 제공하는 디렉터Active Directory 설치시 도메인이라는 관리 단위를 만들게 되면 네트워크상의 컴퓨터들을 이 도메인에 합류시킴으로써 도메인의 구성원으로 만들게 된다. 도메인에 합류된 컴퓨터들은 사용자 인증을 위해 자신의 로컬 데이터베이스 대신 Active Directory를 이용하게 된다.

Active Directory에는 사용자 계정, 컴퓨터 계정뿐 아니라, 그룹, 시스템 구성 정보, 공유 폴더, 프린터와 같은 모든 네트워크 구성 요소들이 저장된다[6].

Active Directory의 목적은 사용자, 공유 자원, 프린트, 애플리케이션(application) 등 실제 네트워크 정보를 사용자가 필요할 때 쉽게 찾을 수 있도록 질서정연하게 조직화 하는데 있다.

(1) Active Directory 개체 및 특성

개체(object)는 Active Directory 내의 사용자, 프린터, 그룹, 응용 프로그램 같은 네트워크 자원을 말하며 구체적인 무엇인가를 나태는 특성

(attribute)의 집합이다.

특성은 디렉토리 개체가 식별할 수 있는 주제를 설명하는 데이터를 가지고 있다. 한 사용자의 특성에는 성, 이름, 전자 메일 주소 등이 포함될 수 있다.

(2) Active Directory 스키마

Active Directory 스키마(schema)에는 Active Directory에 저장된 컴퓨터, 사용자, 프린터 등 모든 개체에 대한 설명이 들어있다.

스키마에는 개체 클래스(class)와 특성(attribute)이라는 두가지 유형이 있다. 개체 클래스는 만들 수 있는 디렉토리 개체를 설명한다. 각 개체 클래스는 특성의 모음이다. 특성은 개체 클래스와 별도로 정의된다. 각 특성은 한 번만 정의하여 여러 개체 클래스에서 사용할 수 있다.

(3) Lightweight Directory Access Protocol(LDAP)

Lightweight Directory Access Protocol(LDAP)은 Active Directory를 쿼리하고 업데이트하는 데 사용하는 디렉토리 서비스 프로토콜이다. LDAP의 프로토콜 사양은 Active Directory 개체가 Active Directory내에 LDAP 명명 경로를 만드는 일련의 도메인 구성요소, 조직 단위, 일반 이름으로 표현되도록 지정한다.

Active Directory의 각 개체에는 고유이름(distinguished names)이 있다. 고유 이름은 개체가 있는 도메인과 개체의 전제 경로를 식별한다. 일반적인 고유 이름의 예는 다음과 같다.

CN=Jin Hee Hwang, OU=myunit, DC=A, DC=com

개체의 상대 고유 이름(relative distinguished names : RDN)은 개체의 특

성인 이름의 일부이다. 이전 예에서 보면 "Jin Hee Hwang" 사용자 개체의 RDN은 CN=Jin Hee Hwang이고, 부모 개체의 RDN은 OU=myinit 이다.

2.2.2 Active Directory 논리적 구조

(1) 도메인

도메인(domain)은 조직 단위를 하나의 논리적인 그룹단위로 구성하여 계정과 자원을 관리할 수 있다. 대규모 네트워크 환경의 경우 다중 도메인을 구성하여 Active Directory를 구성할 수 있다. 보안, 자원에 대한 액세스, 구성 및 사용방법을 도메인 단위로 정의할 수 있으며 단일 관리 계정을 이용하여 모든 작업을 수행할 수 있다.

(2) 조직단위

조직 단위(organizational units : OU)는 도메인 내에서 개체를 구성할 때 사용하는 컨테이너 개체다. OU에는 사용자 계정, 그룹, 컴퓨터, 프린터, 다른 OU 개체가 포함될 수 있다. 그리고 OU는 관리 제어 위임 및 그룹 정책(group policy)의 적용 단위가 된다.

(3) 도메인 트리

도메인 트리는 공통 루트 이름을 가지는 도메인들의 계층적인 배열로 연속된 이름 공간을 사용한다. 네트워크에 첫 번째 도메인을 자식 도메인이라고 하며 자식 도메인의 상위 도메인을 부모 도메인이라고 한다. 도메인 트리의 가장 최상위 도메인을 트리 루트 도메인이라고 한다.

도메인 트리를 구성하면 부모 도메인과 자식 도메인 사이에는 양방향 전이 트러스트가 자동으로 만들어진다. 트리 내의 모든 도메인들은 양방향 전

이 트러스트를 통해 각 도메인에 있는 네트워크 자원들을 서로 공유할 수 있게 된다.

(4) 포리스트(Forests)

포리스트는 하나 이상의 도메인 트리 집합이다. 포리스트의 트리는 안전한 이름 공간을 공유하지 않는다. 그러나 포리스트의 트리는 공통 스키마와 글로벌 카탈로그를 공유한다. 다른 트리에 연결되지 않은 단일 트리는 하나의 트리로 구성된 포리스트를 형성한다. 따라서 모든 트리 루트 도메인은 포리스트 루트 도메인과 이행성 트러스트 관계를 갖는다. 포리스트 루트 도메인의 이름은 특정 포리스트를 참고하는 데 사용한다.

(5) 글로벌 카탈로그

포리스트 내의 모든 도메인에 있는 개채에 대한 일부 정보만을 모아 놓은 데이터베이스이며 포리스트에 있는 개체에 대한 빠른 검색을 위해 사용된다. 글로벌 카탈로그에 저장되는 개체 정보는 사용자 이름, 성, 로그온 이름과 같이 검색에 자주 사용되는 속성들만이 저장된다. 글로벌 카탈로그는 포리스트 루트 도메인에 컨트롤러에 만들어지며 글로벌 카탈로그를 관리하는 도메인 컨트롤러를 글로벌 카탈로그(Global Catalog) 서버라고 한다.

그림 4에서는 Active Directory의 논리적 구조인 도메인, 조직 단위, 트리, 포르스트에 대해 잘 보여 주는 그림이다.

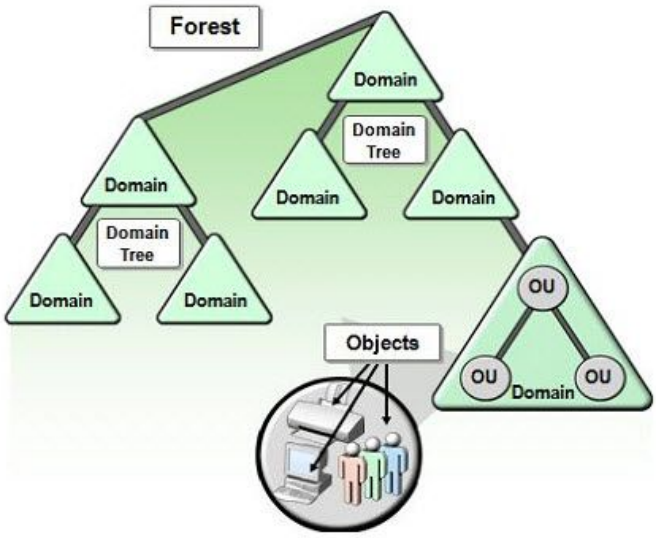

그림 4. Active Directory의 논리적 구조 (출처:[7])

2.2.3 Active Directory 물리적 구조

Active Directory에서 논리적 구조는 물리적 구조(physical structure)와 확실히 구별된다. 논리적 구조를 사용하여 네트워크 리소스를 구성하고, 물리적 구조를 사용하여 네트워크 트래픽을 구성하고 관리한다. Active Directory에서는 도메인 컨트롤러(domain controllers)와 사이트(site)를 통해 그림 5와 같이 물리적 구조를 형성한다.

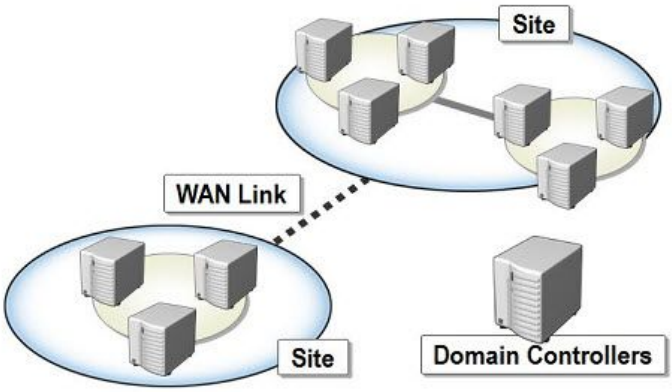

그림 5. Active Directory의 물리적 구조 (출처:[7])

(1) 도메인 컨트롤러

도메인 컨트롤러(domain controller)란, 디렉토리 복제를 저장하는 컴퓨터이다. 도메인 컨트롤러는 또한 디렉토리 정보의 변경 내용을 관리하고 변경 내용을 같은 도메인에 있는 다른 도메인 컨트롤러를 복제한다. 도메인 컨트롤러는 디렉토리 데이터를 저장하고, 사용자 로그온 프로세스를 확인하고, 인증하고, 디렉토리 검색을 제공한다.

(2) 사이트

사이트는 Active Directory에 저장되는 하나의 개체이다.Active Directory 서버들을 포함하는 네트워크 내의 물리적인 위치를 말하며 10Mbps 이상의 속도로 연결된 하나의 네트워크를 사이트로 정의한다. 하나의 도메인이 여러 물리적인 네트워크 구조를 포함하고 있을 때 사용자 로그온 프로세스 및 도메인 컨트롤러간의 복제를 효과적으로 구성하기 위해서 사용된다

2.3 데이터보호기술

2.3.1 DRM(Digital Rights Management) 정의

인터넷 등 통신수단의 발달은 디지털 컨텐츠의 불법복제, 저작권 침해, 비밀보호유지 곤란 등의 많은 문제점을 가져왔으며, 컨텐츠를 복제할 때 누구나 자신의 PC를 이용하여 쉽고 빠르게 복제가 가능하고 복제물도 원본과 동일하다[10]. 이런 정보화의 발전과 함께 정보화의 역기능도 함께 발생하고 있다.

DRM기술은 디지털 컨텐츠 유통에 안정성, 유통성, 재사용을 지원하며 저작권자, 유통업, 소비자에 이르는 컨텐츠 라이프 사이클에 관계된 모든 에이전트를 만족시켜줄 수 있는 신뢰구조를 제공하는 기술이다. 즉 DRM은 암호화 기술을 이용하여 허가되지 않은 사용자로부터 디지털 컨텐츠를 안전하게 보호함으로써 당사자의 권리 및 이익을 제공하는 기술이다. DRM의 범위가 한마디로 정의하기는 매우 힘들다. Commerce DRM(디지털 컨텐츠를 상업적으로 가치 보호) 허가된 사용자가 디지털 컨텐츠를 이용 가능하게 통제하며, 저작권 보호 및 복제방지를 한다. Enterprise DRM(문서보안) 기업 내부의 문서자원에 대한 보호를 하면 기업기밀 문서에 대한 보호, 인간된 사용자 접근허용, 인간되지 않은 사용자의 통제, 사용자별 권한에 따른 정보의 활용 등으로 구분할 수 있다. 표 3는 Commerce DRM과 Enterprise DRM 비교를 나타냈다[13].

표 3. Commerce DRM과 Enterprise DRM 비교

	Commerce DRM	Enterprise DRM
사용 환경	다양한 디지털 기기에서 특정 프로그램	주로 PC, PAD 상의 다양한 프로그램
정책	컨텐츠 판매 정책, fair-use	보안 정책, ACL 연동
표준, 상호호환	시장 확대를 위하여 필수적	표준의 필요성이 상대적으로 적음
사용 내역 관리	사생활 침해 논란이 있음	사고 예방 및 발생시 조사를 위하여 필요

문서보안은 문서의 소유자(생성자)에 의해 생성된 문서를 암호화하고 해당 문서를 사용할 수 있는 사용자(그룹)와 사용자(그룹)의 권한을 서럊ㅇ하여 문서의 유출을 방지하는 시스템을 말한다. 문서보안에서 제공되어야 할 기본적인 기능은 다음과 같다[14].

(1) 외부전송 보안 파일

외부전송 보안파일은 문서보안 프로그램을 사용하지 않는 외부 사용자가 보안문서의 열람이 가능하도록, 권한을 부여하여 특정 문서를 실행 파일의 형태로 만드는 것을 말한다.

(2) 보안문서 권한 변경

보안문서 권한 변경은 이미 생성되어 있는 보안문서의 접근대상과 해당 접근대상의 권한을 변경하는 것을 말한다. 권한을 변경하기 전에 해당 접근대상의 권한정보를 확인 후 어떤 정보를 변경할 것인지를 결정한다.

(3) 복사 및 붙여넣기 방지

일반문서 보안 문서 상이의 편집을 방지하여 중요 정보 유출을 차단하는 기능을 말한다.

(4) 프린터 출력물에 대한 보안 방안

문서 출력시 해당 문서 생성자와 정보를 문서 배경에 마킹하여 문서에 대한 책임 및 외부 유출에 대한 보안성을 강화하는 것을 말한다. 출력 권한을 설정은 물론 출력시 출력한 사용자의 정보를 담을 수 있게 지원해 출력물에 대한 감사를 제공한다. 출력한 사용자의 사번이나 시간 등의 이력이 문서에 찍히게 되는 프린터 마킹 기술과 언제 누가 어떤 문서를 출력했는지에 대한 로그정보를 서버로 전송해 사후 감사와 추억을 진행 하여야 한다.

(5) 이동장치 이용한 전자문서 유통 시 보안 방안

기업에서 생성되는 문서는 외부로 전달되는 경우가 많으며, 전달 수단은 이메일, USB저장매체, CD-R등의 매체를 통해 외부로 반출하고 있다. 이러한 이동장치를 통한 전자문서 유통 시 보안 방안을 제공하기 문서보안 시스템은 이동장치를 사용할 수 있는 권한에 대한 통제를 제공해야 한다. 또한 전자문서가 이동하더라도 사용자 고유 정보가 일치 않는다면 해당 문서를 열어보는 것을 불가능하게 만들어 정보유출을 막게 된다.

2.3.2 DRM의 특징

첫째, 컨텐츠의 유통성을 기존의 저작권 보호방식에 비하여 획적으로 높은 슈퍼디스트리뷰션(superdistribution) 기능을 제공한다. 슈퍼디스트리뷰션은 암호화된 컨텐츠를 소비자가 자유롭게 복사 또는 배포하는 것으로써, 이렇게 배포된 컨텐츠를 소지하더라도 별도의 인증 또는 검증 과정 없이는 컨텐츠에 접근이 불가능하다.

둘째, 저작권자와 컨텐츠 판매자 사이의 거래구조의 투명성을 높인다. 인

증기관, 권한 등 컨텐츠의 소비과정에 개입하고, 모든 소비구조과 전자적으로 이루어짐으로써 당사자 간의 간적접인 거래보다 안정적으로 이루어진다.

셋째, DRM은 컨텐츠의 사용성을 높이는 기능을 하는데, 이는 DRM 자차에 횟수, 유효기간, 컴퓨터 환경 등을 사용규칙(usage rule) 내장함으로써 컨텐츠 소비의 형태의 세분화 및 통제가 가능하기 때문에 소비자의 다양한 요구에 적합한 컨텐츠 모델을 구현할 수 있다.

DRM이 저작권 보호하는 기술적 보호처치의 하나라는 점에서 다른 기술적 보호 조치인 복제방지기술, 수신제한시스템과의 특성을 비교하면 다음 표 4와 같다[11].

표 4. 다양한 기술 보호조치의 비교

기 술	장 점	단 점
복제 방지	- 디바이스간 전송중의 불법복제 방지 - 기록장치에 저장되는 컨텐츠의 불법복제방지	- 제한된 사용범위 - 권한제어 불가 - 다양한 컨텐츠 유통모델 지원 불가
수신제한시스템	- 허가된 시청자에게만 수신허용 - 구체적이고 세부적인 기술규격 - 성공적인 시장적용 사례	- 방송컨텐츠 적용분야 제한 - 다양한 권한제어 불가 - MEPG-2, MPEPG-4 등 일부 포맷만 지원 - 디지털 버서를 통해 재전송되는 컨텐츠 사용불가
디지털 저작권 관리	- 다양한 권한 제어 - 다양한 포맷지원 - 컨텐츠의 유통모델이 풍부 - 슈퍼디스트리뷰션 가능	- 표준 기술 규격 부재 - 상호호환성의 결여

2.3.3 DRM시스템의 구조

DRM 시스템은 그림 6과 같이 클라이언트 서버 구조를 구성되어 운영된다. 서버는 클라이언트에 에이전트를 파견한 후, 네트워크를 통하여 클라이언트 에이전트와 실시간으로 클라이언트의 저작물 사용상황 등을 보고 받고 디지털 저작권에 대한 보호 및 감시기능을 수행한다.

DRM 시스템구성은 다음과 같이 컨텐츠 제공자모듈, 컨텐츠 분리모듈 및 사용자 모듈 등으로 구성되며 외부 연계모듈로 클리어링하우스 모듈과 컨텐츠 암호화 모듈과 라이센스 암호화 모듈로 구성된다[12].

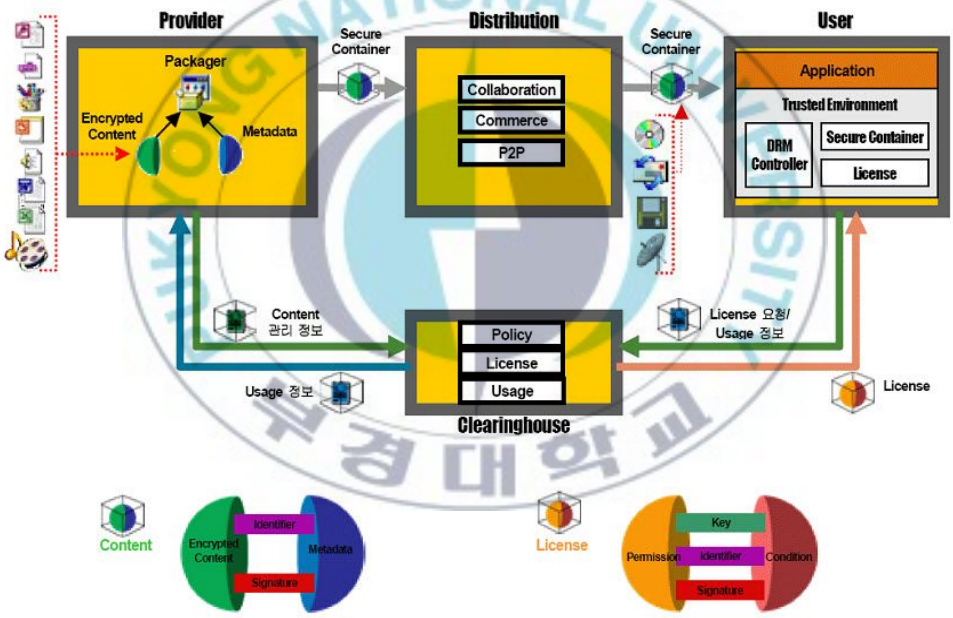

그림 6. DRM 시스템 일반적인 구조 (출처:[8])

가. 컨텐츠 제공자 모듈

서버 외부로부터 제작된 저작물을 안전하게 제공하기 위하여 보호 조건을 입력 받기 위한 인터페이스로 컨텐츠와 메타데이터를 포함하는 패키지로 구성되어 있다. 컨텐츠 제공자 모듈에서는 저작물을 받아 등록에서 보안까지 안전하게 지원하기 위한 전처리 작업을 지원한다.

나. 컨텐츠 분리모듈

컨텐츠를 제공받는 주체별로 구분하여 안정된 서비스를 제공할 수 있도록 구분한 분리 모듈이다. 데이터를 안전하게 제공받을 수 있도록 클라이언트 측의 에이전트와의 통신을 처리하는 모듈이다.

다. 사용자 모듈

외부 인터페이스로부터 입력 받은 저작물의 복호화를 수행하며 디지털 저작권 감시와 보호를 위하여 클라이언트 측에 에이전트를 파견하고 에이전트로부터 보고받은 사용행위나 불법행위에 대한 감시결과를 처리하는 모듈이다. 또한, 저작권 정보관리, 사용내역 관리, 불법 접근 기록 관리와 각종 통계 관리를 위한 데이터 베이시들이 내부 모듈을 통하여 관리된다. 클라이언트 측의 에이전트는 클라이언트 컴퓨터 시스템에 파견되어 사용자의 저작물을 보호하고 감시를 수행하면서 사용자의 요구에 의하여 저작물에 대한 복호화를 수행하여 실행하는 기능을 수행한다.

라. 클리어링하우스 모듈

사용자 정보를 입력받아 사용자가 요청한 컨텐츠를 제공할 수 있도록 사용권한을 제공하는 정책을 맡고 있으며, 허가된 사용자에게 라이센스를 부여하여 컨텐츠를 안전하게 제공하는 역할을 한다.

마. 컨텐츠 및 라이센스 암호화 모듈

클리어링 하우스모듈과 연계하여 컨텐츠 제공자는 컨테츠를 암호화하여

컨텐츠를 요구하는 사용자에게 제공할 수 있도록 하는 역학을 수행하며, 이때 라이센스 암호화 모듈은 사용자가 인가된 사용자임을 확인한 후 라이센스를 제공할 수 있도록 구성되어 있다.

2.3.4 DRM 기술 요소 및 내용

DRM은 협의적 의미로 단순히 컨텐츠의 불법복제를 방지하는 요소기술로 정의되기도 하지만 광의적 의미로 디지털 컨텐츠 전제 라이프사이클에 걸쳐 투명하고 신뢰성을 보장해주기 위한 기술과 서비스체계를 통틀어 말할 수 있다. 표 5는 DRM의 기술 요소 및 내용을 개괄적으로 보여주고 있다[9].

표 5. DRM의 기술 요소 및 내용

요소기술	세부 요소 기술	내 용
컨텐츠 패키징 기술	컨텐츠 패키징 구조 선언 기술	패키징된 컨텐츠의 내부 구조를 표현하는 기술
	컨텐츠 파일포맷 설계기술	패키징된 컨텐츠의 포맷에 대한 기술 규격 설계
	복합컨텐츠의 패키징 기술	여러 개의 컨텐츠를 묶어서 패키징하는 기술
	컨텐츠 암호화 기술	컨텐츠의 기밀성, 무결성 보장을 위한 기술
	암호화키관리기술	컨텐츠의 암호화를 위해 사용된 키의 안전한 관리
권리표현 기술	권리 데이터 사전	권리요소에 대한 정의
	범용 REL 파서 설계 및 구현 기술	라이센스에서 권리정보 추출 및 정확한 해석 처리
	권리정보 저장 및 관리	권리정보의 DB 보관을 위한 처리 기술
워터마킹 / 핑커프린팅 기술	공모공격에 강인한 워터마킹 기술	다양한 공격에도 충분한 강인성을 유지하는 기술
	공모허용 핑커프린팅 기술	불법추적을 위한 핑거프린팅 정보의 삽입 및 추출 기술
	실시간 핑커프린팅 삽입기술	핑거프린팅 정보의 실시간 처리 기술
복제방지 기술	디바이스 인증 기술	컨텐츠 전송단과 수신단 간의 상호 인증처리 기술
	디바이스 폐기/ 회복 기술	훼손된 디바이시의 폐기 및 회복 기술
	암호화 기술	컨텐츠 전송단과 수신단 간의 안전한 컨텐츠 전송을 위해 암호화하는 기술
컨텐츠 식별체계	식별자 변환 기술	식별자의 실시간 변환기술
	식별 메타데이터 관리 기술	공통으로 사용되는 기본 메타데이터 구조 설계

(1) 암호화 기술(Cryptography)

DRM은 컨텐츠의 컨텐츠 이용과 관련된 라이센스 내용과 기밀성의 유치, 비허가자에 대한 컨텐츠의 접근을 제한하기 위해 암호화기술을 사용한다. 이를 위해 기밀성보호를 위해서는 아래의 대칭키(Symmetric Key)방식의 암호화 알고리즘이 사용되며, 무결성 인증처리를 위해 PKI 인증서 기반의 전자서명 기술을 이용한다.

암호화 기술의 강도는 암호화 알고리즘 자체의 강인성측면과 키 길이에 따른 강인성으로 구분하여 생각할 수도 있다. 암호화를 위해 사용되는 키 길이의 증가는 암호화된 컨텐츠의 보안성을 증가시키게 되며, 설명 해독할 수 있다고 하더라도 해독하기 위한 비용의 정보의 가치보다 높게 만듦으로써 불법적인 공격을 무력화시키는 효과를 누릴 수 있다. 암호화알고리즘으로 최근에는 AES(Advanced Encryption Standard)알고리즘이 많이 사용되고 있다. 표 6은 암호화 대상 목적별 적용 암호화 기술에 대해 나타내고 있다[8].

표 6. 암호화 대상 목적별 적용 암호화 기술

대상 / 목적	디지털컨텐츠	라이센스	트랜잭션
기밀성	DES, 3-DES, AES-128	DES, 3-DES, AES-128	SSL
무결성	RSA with MD5/SHA-1	RSA with MD5/ SHA-1	RSA with MD5/ SHA-1
인증		PKI	DH, PKI
부인방지			RSA with MD5/ SHA-1

나. 키 관리 기술(Key Management)

일반적으로 DRM은 허가되지 않은 사용자로부터 디지털컨텐츠를 보호하고자 컨텐츠를 암호화하고, 허가된 사용자에 복호화를 위한 키정보를 전달함으로써 컨텐츠의 보호가 이루어진다. 컨텐츠의 암호화는 무작위로 선택된 암호 대칭키를 통해서 이루어지며, 이 같은 암호화 대칭키는 라이센스에 권리정보와 함께 컨텐츠의 이용자에게 전달, 컨텐츠를 복호화할 때 사용된다. 따라서 본 기술의 가장 핵심은 암호화 대칭키(CEK)이며 이는 안전이 확보된 상태에서 관리 배포되어야 한다. CEK의 관리방식에 따라서, 중앙의 키관리서버에 저장되는 방식이 KMS(Key Management Server)과 컨텐츠 DRM Packaging시에 사용되는 Secure Container 내부에 저장하는 장식은 Envelope 방식이 존재한다.

(3) DRM 패키징 포맷(Secure Container)

DRM패키징은 DC의 유통을 위해 DC를 암호화하고 메타데이터를 추가하여 하나의 전자적 정보구조체 형태(Secure Container)로 구성하는 기술이다. 컨텐츠의 패키징은 컨텐츠별 무작위로 생성된 CEK를 이용하여 암호화하며, 생성된 Secure Container를 전자서명 함으로써 유통되는 컨텐츠의 동일성 유지와 저작권 소유관계에 대한 인증처리를 한다.

디지털컨텐츠의 패키징을 위해 암호화된 컨텐츠와 메타데이터, 유통관리 정보들이 하나의 Secure Container파일로 구성되며 Secure Container의 포맷은 이러한 구조체 정보들이 삽입 될 수 있는 전자적 정보구조체를 제공한다. Secure Container의 예로는 MPEG-21에서 개발하고 있는 DID(Digital Item Declaration)와 FF(File Format), OMA DRM의 DCF(Digital Content Format)등이 다양하게 존재하고 있으나, 상용화된 DRM 제품은 개별업체별

로 자신의 독자적 형태를 사용하고 있다.

(4) 디지털컨텐츠식별체계

디지털컨텐츠 식별체계는 디지털컨텐츠의 글로벌한 식별을 가능하게 하고 유통과정에서 DC 관리 및 가치사슬(value chain)에서 DC의 정보교환이 쉽게 이루어지게 하는 기술이다. 미국출판인협회(Association of American Publisher)에서 개발한 DOI(Digital Object Identifier)가 있으며, 그 외 URI(Uniform Resource Identifier), 그리고 한국정보사회진흥원에서 개발한 UCI(Universal Content Identifier)등이 있다.

(5) 메타데이터(Metadata)

메타데이터는 디지털컨텐츠에 대한 식별정보, 내용정보, 그리고 특성정보 등을 표현하는 기술로, 디지털컨텐츠의 체계적인 관리 및 원활한 검색에 활용됨으로써 디지털컨텐츠 이용의 효율성을 가져온다. 현재까지 메타데이터에 대해 범용적인 사용을 목적으로 표준화된 기술은 없는 상태이다.

(6) 권리표현기술(Right Expression)

디지털컨텐츠의 사용권한은 일반적으로 디지털컨텐츠 배포자로부터 허가된 사용자에게 제공되는 라이센스에 의해 전달되며, 이 라이센스는 식별장치가 해독할 수 있는 형태의 권리표현기술을 이용하여, 생성, 전달된다. 즉 권리표현기술은 디지털컨텐츠에 대한 사용권한(Permission)과 조건(Condition)을 표현한다. 디지털컨텐츠에 대한 사용 권리는 사용한 비즈니스 환경에 따라 표현이 달라 질 수 있는데, 이를 위해 호환성을 위해 구현되는 기술이 요구된다. 호환성이 보장되는 대표적인 기술은 MPEG-21 REL과 OMA의 ODRL등이 있다.

(7) 권한통제기술(Right Enforcement)

권한통제기술은 디지털컨텐츠를 계약에 따른 사용권한과 조건 내에서 사용될 수 있도록 통제가능 기술이다. 컨텐츠에 대한 사용통제는 컨텐츠처리 응용프로그램에 대한 직접적인 제어가 요구된다. 이때 사용되는 권한통제기술의 구현방식은 표 7와 같은 방식들이 사용되고 있다[8].

표 7. 권한통제기술의 구현방식

구현방식	설 명
Built-In	제어 기능을 응용 프로그램의 소스에 추가하고 재컴파일 하는 방식
Application plug-in 방식	응용 프로그램에서 제공하는 ADK를 사용하여 extension 기능으로 추가하는 방식
Hosted 방식	외보로 공개된 표준 인터페이스를 사용하여 제어하는 방식
Application rewriting 방식	응용 프로그램의 실행코드를 수정하는 방식
OS add-on 방식	OS 커널을 수정하는 방식

(8) 탬퍼링 방지기술(Tamper Resistance)

사용권한 범위 이외의 행위를 기술적으로 차단하는 기술인 DRM에 대해서 무력화 및 다양한 해킹위협으로부터 안전하게 DRM 소프트웨어를 보호하는 기술이다.

(9) 사용자/디바이스인증기술(Authentication)

사용 권한이 허가된 사용자 및 디바이스에만 실행될 수 있도록 통제하는 기술로서 사용자 인증기술은 ID/Password, 공인인증서, E-mail 인증, SSO,

ID-Federation, 생체인식 등이 있다.

(10) 도메인 권한관리기술(Domain Rights Management)

현재 상용화된 대부분의 DRM제품은 DC별로 특정 단말기(device)에서 그 이용이 가능하고 다른 기기에서의 이용은 허락되지 않았다. 허나 다른 선진국에서 디지털컨텐츠의 사적본제 보장을 통한 컨텐츠의 이용편리성보자(Fair Use)에 대한 요구가 증가하고 있어 DRM에서도 이에 대한 여구가 이루어지고 있는 실정이다. 도메인 권한관리기술은 사적본제권이 인정되는 장비에 한해 컨텐츠의 자유로운 전송 및 편집 작업이 가능하도록 DRM이 지원할 것을 목표로 하고 있으며, OMA, DVB 등 국제표준단체에서는 'domain authority' 또는 'virtual device'라는 개념의 도입을 시도하고 있다.

3. 단일인증 기반 DRM 시스템 설계 및 구현

3.1 DRM시스템의 보안 요소

DRM 시스템을 안전하게 유지하기 위하여 컨텐츠를 암호화하여 서버에 등록하고, 컨텐츠를 제공자는 인증된 사용자에게 컨텐츠를 제공할 수 있도록 사용자는 사용자 인증시스템을 갖추고 있어야 한다. 또한 인간된 사용자에게 복호화키를 제공하며, 복호화 키 전송시 안전한 키 전송 기법이 제공되어야 함으로 DRM 시스템에서 보안 요소는 다음과 같이 컨텐츠 암호 방식과 사용자 인증 및 키 분배, 복호화 방법 등이 있다.

가. 암호화 방식

DRM 시스템 암호 방식은 표 8과 같이 블록 암호 방식과 스트리밍 암호 방식이 있다.

블록 암호 방식은 저작물을 패키지화 할 때 같은 비밀기로 암호화를 수행하는 방식으로 한 사용자가 다른 사용자에게 저작물을 전달하여 사용자가 저작물에 대한 라이센스를 서버로부터 새로 발급받아서 저작물을 사용할 수 있는 저작물 재분배가 가능하다. 그러나 저작물을 하나의 비밀키로 암호화하면 임의의 사용자에 의한 키의 노출이 일어날 경우 해당 저작물에 대한 안전을 보장받지 못하며, 키를 노출시킨 사용자를 추적할 수 있는 방법도 없다. 일반적인 대용량의 디지털컨텐츠에 대한 DRM시스템에서는 블록암호화 방식을 사용한다.

스트리밍 암호 방식은 사용자의 다운로드 요청이 있을 경우 암호화를 수

행하면서 저작물을 다운로드 할 수 있는 방식으로 서로 다른 사용자에게 서로 다른 키를 가지고 암호화된 저작물을 배포하므로 키의 노출이 일어날 경우 해당 사용자를 찾아낼 수 있다. 그러나 다운로드를 수행하면서 동시에 암호화를 수행하므로 대용량의 디지털컨텐츠 파일의 경우 암호화에 많은 시간이 소용되는 단점이 있다. 그리고 사용자에 대하여 별도의 키를 부여하므로 한 사용자가 다운로드 받은 저작물을 다른 사용자에게 재분배 할 수 없으며 모든 디지털컨텐츠에 적용할 수 없고 스트리밍 방식의 파일에만 적용가능하다.

표 8. DRM 시스템에서 블록암호와 스트리밍 암호화의 비교

구 분	블록 암호화	스트리밍 암호화
암호화 시점	패키지 시	다운로드 시
재분배	가능	불가능
키의 노출 추적	취약	안전
적용 파일	모든 동영상 파일	스트리밍 파일

나. 키의 분배

공개키 암호 방식은 속도가 느린 단점이 있고 사용자의 공개키가 해당 사용자의 공개키가 맞는지에 대한 인증이 필요하므로 인증센터를 통하여 사용자의 공개키에 대한 인증을 해야 한다. 그리고 비밀키 암호 방식은 공개키의 단점인 속도문제를 해결할 수 있는 기법으로 암호화 속도가 공개키에 비하여 빠르고 또한 암호화를 미리 해 놓을 수 있는 장점이 있으나 데이터를 암호화한 그 비밀키를 네트워크상으로 전달할 수 있는 방법이 없다. 그러므로 대부분의 DRM시스템에서는 보호하는 데이터에 대한 암호기술로는 비밀키 암호방식을 사용하고 해당 비밀키를 보호하기 위한 방법으로는 공캐키

암호 방식을 사용한다.

다. 복호화 방식

디지털컨텐츠는 사용자의 컴퓨터에 암호화되어 저장되므로 사용자가 해당 파일을 실행하면 사용자 에이전트는 서버에 라이센스를 확인하고, 해당 파일을 복호화한 후에 실행하게 된다. 그러나 대용량의 멀티미디어 파일인 경우 복호화에 많은 시간이 소요되는 단점이 있다.

3.2 DRM 솔루션 종류

가. Server DRM

Server DRM에 의해 보안이 형성된 문서 파일은 사내에서 자유롭게 사용가능하지만 외부 유출될 경우 강력한 암호화 기능을 통한 비밀성 유지기능을 통해 열람이 불가능 하도록 만든다. 그림 7은 Server DRM 시스템 구조를 나타냈다.

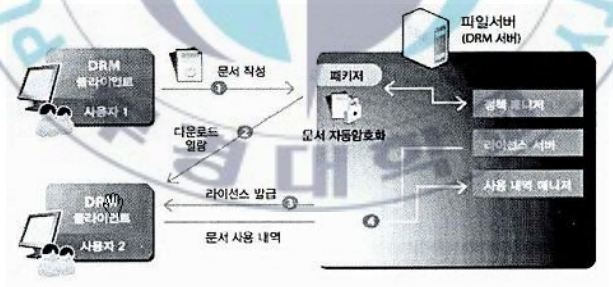

그림 7. Server DRM 시스템 구조 (출처:[15])

나. PC DRM

개인 PC의 문서를 자동 암호화하고 문서 사용 권한을 통제함으로써 내부

임직원이 주요 문서를 외부로 전송하거나 PC를 무단 반출하여 내부 정보의 유출을 시도하더라도 문서의 사용이 불가능하여 소중한 정보자산을 원천적으로 보호할 수 있다. 그림 8은 PC DRM 시스템 구조를 나타냈다.

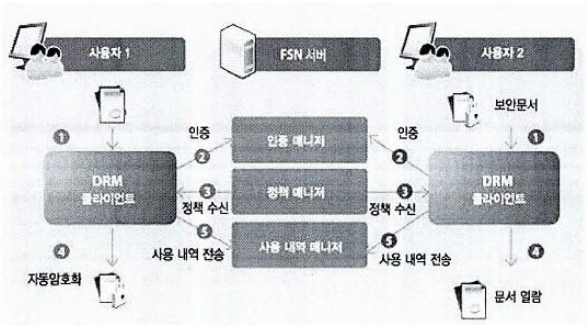

그림 8. PC DRM 시스템 구조 (출처:[15])

다. Web DRM

웹으로 제공되는 웹 컨텐츠의 복사, 저장, 인쇄 등의 기능을 제어하고 HTML 페이지를 암호화 하여 중요한 정보의 유출을 방지함으로 유료컨텐츠의 외부 유출 및 무단 도용을 방지하도록 컨텐츠 방어 기능을 제공한다. 그림 9는 Web DRM 시스템 구조를 나타냈다.

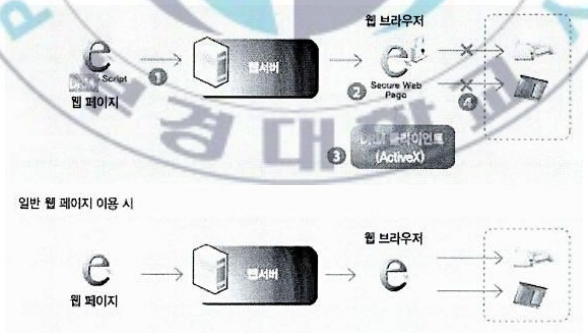

그림 9. Web DRM 시스템 구조 (출처:[15])

라. File Server DRM

파일서버의 특정 폴더가 보안 폴더로 설정되면 허가되지 않은 사용자의 사용권한을 제어함으로 중요한 기업 문서의 불법 사용 및 외부 유출을 차단한다. 그림 10는 File Server DRM 시스템 구조를 나타냈다.

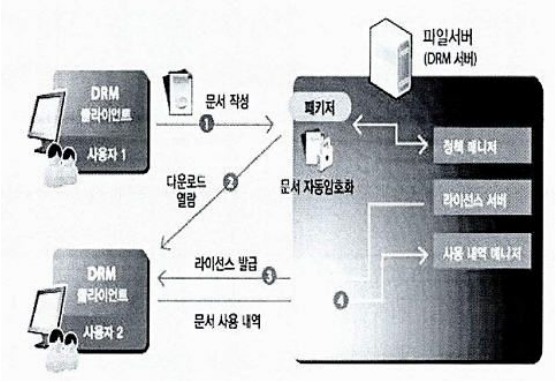

그림 10. File Server 시스템 구조 (출처:[15])

마. PRINT DRM

문서 출력시, 출력자 정보, 출력일시, 회사 정보 등의 출력 정보를 프린트 워터마킹 기술을 이용하여 사용자 의자와 상관없이 강제로 삽입하는 방식으로 출력물의 보안성을 강화한다. 그림 11은 PRINT DRM 시스템 구조를 나타냈다.

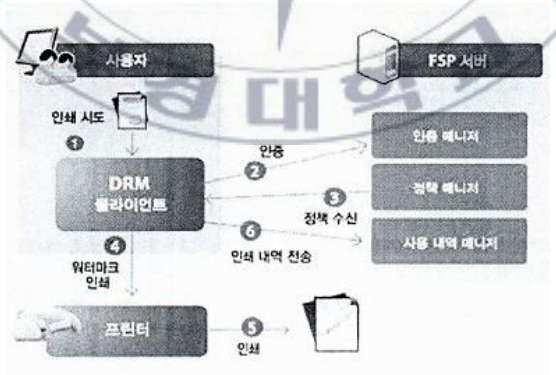

그림 11. PRINT DRM 시스템 구조 (출처:[15])

3.3 DRM 문제점

컨텐츠에 대한 저작권을 보호하고 디지털 환경에서의 컨텐츠의 유통을 촉진하게 되는데, 기술적 특성상 다음과 같은 한계가 존재한다.

첫째, DRM의 보안성은 시스템이 채택하고 있는 암호기술에 근거하고 있는 근본적으로 어떠한 암호기술도 완벽하지 않으며 그 보완성이 지속될 수 없다는 제한성이 있다.

둘째, 문서 보안의 시스템은 사내의 사용자 인증을 통하여 비로소 보안문서의 사용허가를 받게 된다. 개별 사용자 pc에 에이전트로 설치가 되어 사용자 확인 할 수 있지만 기업에서는 개별사용자의 관리가 쉽지 않은 설정이다. 휴가자나 퇴직자 또는 프로젝트를 통한 외부업체에 대한 관리가 명확하게 이루어지지 않은 실정이다.

셋째, DRM 에이전트를 별도로 설치하게 되는데 특정 프로세스를 찾아 kill 해주는 프로그램이 있다. 이러한 방법을 이용하여 사용자 pc의 모든 프로세스를 확인하고 다운시키게 되면 DRM 에이전트가 제대로 동작하지 않게 된다.

넷째, DRM솔루션간의 호환이 안 되서 서로 충돌하거나 같은 기능을 하는 솔루션일지라도 두 솔루션간의 연동이 안됨에 다라서 잦은 에러가 발생함으로서 한 회서에서 구축하여 사용 중인 솔루션이 있을 경우 CNN 더 나은 솔루션이 개발이 되거나, 회사의 부도 등으로 타 솔루션을 도입해야 하는 경우 더 나은 DRM솔루션을 구입하여 사용할 수가 없고 변경하기 위해서는 기존에 구성된 문서들의 변환의 문제점으로 인하여 폐기해야할 경우까지도

생긴다.

다섯째, 라이센스 관리의 문제가 대두된다. 예를 들어 정당한 절차에 의하여 컨텐츠에 대한 라이센스를 획득한 후, 컨텐츠를 저장한 하드웨어를 교체할 경우 이를 어떠한 방식으로 지원 또는 해결할 것인가를 DRM의 라이센스 관리정책이 풀어야 할 숙제이다.

3.4 정보유출 및 문서보안을 위한 주요정책

3.4.1 정보보호 기본원칙

정보보호 기본원칙은 적정 등급 및 표시의 원칙, 최소인원 참가의 원칙, 최적보관의 원칙, 기록보존의 원칙, 책임한계 명확화의 원칙으로 구분되어진다[16].

가. 적정 등급 분류 및 표시의 원칙(객체의 접근 통제 기준)

- 비밀의 중요도와 가치를 평가하여 분류기준에 따라 적정한 등급으로 분류하여 보호객체를 분명히 하고 그 등급에 맞는 취급절차에 의하여 보호하여야 한다.
- 비밀보호는 등급분류에서 시작되므로 분류기준을 설정하여 적정등급으로 분류하고 그 등급을 표시와 내면의 각장마다 상·하단 중앙에 쉽게 식별할 수 있도록 적색으로 표시하는 것이 보편화되어 있다.

나. 최소인원 참가의 원칙(주체의 접근통제)

- 비밀은 업무수행을 위하여 꼭 필요한 사람과 알아야 최소 인원만 취급

또는 열람하게 하고 업무수행에 참고가 될 사람은 가능한 접근을 제한하여야 하며, 비밀에 접근하는 사람이 많으면 그만큼 누설과 유출의 위험성이 높아진다.

◆ 최소 인원 참가의 원칙은 열람자의 적정성과 배포처의 적절성 및 관리의 적절성을 확보하고 유출을 방지하기 위하여 생산단계에서 부터 접근 자를 모두 기록한다.

다. 최적 보관의 원칙(객체의 보호)

◆ 최소 관리자에게만 접근권한을 부여하고, 비밀업무를 할 때에는 일반직원이 접근할 수 없는 장소에서 하는 것이 원칙이다.

◆ 일상 활용하는 비밀은 부서별로 보관하는 방법과 자주 활용하지 않는 비밀과 최종 연구보고서 등을 집중 보관하여야 한다.

라. 기록보존의 원칙(접근자의 통제)

◆ 비밀의 생산결재에 참여한 자, 보관 취급하거나 열람, 대출, 반출자 등과 비밀에 준하는 핵심시설에 접근 출입자 등 모든 관련자는 반드시 인적사항을 기록 유지하여야 한다.

마. 책임한계 명확화의 원칙(비밀취급 통제)

◆ 비밀은 비밀보호규정에 그 취급절차를 규정하고 있으므로 그에 따라 비밀의 취급 과정별로 담당자를 지정하여 그 과정에 대한 책임 있는 업무수행을 할 수 있도록 명확히 하여야 한다.

3.4.2 기업비밀보호 조직과 기능

가. 대표이사

기업의 대표자는 그 기업의 대표자로서 기업 비밀의 총책임을 지며 대내외적인 비밀보호 문제에 기업을 대표한다.

나. 비밀관리 위원회

부사장 또는 전무급이 위원장이 된다. 연구소, 사업장의 장과 본사의 각 분야별 임원이 비밀관리원이 되며 그 기능을 다음 사항을 심의한다.

- 비밀번호규정제정, 주요계획, 주요정책과 상벌 등
- 특허와 보호방법과 처분 및 보상금 지급결정
- 핵심비밀 취급자 및 퇴직자의 관리정책

다. 각 부서 비밀관리자

각 부서의 부서장이 임명과 동시에 당연직으로 소관 비밀에 대한 총괄 책임자로서 비밀을 관리하며, 비밀업무를 담당할 수 없는 부적격자를 비밀보호 업무에서 제외케 하는 정책을 유지하는 것이 필요하다.

3.4.3 비밀보호 객체에 대한 접근정책

가. 보호 객체의 접근통제

비밀을 보호하기 위한 비밀등급과 등급별 접근자를 엄격히 구분하여 비밀유출을 방지하며, 보호객체를 엄격히 분류하여 중요도에 따라 보호의 방법과 절차의 강도를 달리하는 접근통제를 하여야 한다.

나. 문서의 중요도 구분

국가비밀은 그 중요도에 따라 1급비밀, 2급비밀, 3급비밀 및 대외비 등 4

단계로 구분하고 있지만 기업비밀은 2~3단계로 단순화할 필요가 있다. 비밀의 등급별 명칭도 기업이 임의로 결정한다.

다. 시설의 중요도 구분

기업이 관리하는 사업장별 또는 시설과 장비 및 설비 중에 그 기업만이 보유한 특수시설 및 장비는 그 자체가 영업비밀과 동일하므로 차단시설을 설치하여 접근을 물론 관망을 차단하여야 한다.

3.4.4 보호주체 등에 대한 접근정책

접근자의 통제는 업무상의 접근 필요성 여부와 접근의 권한여부를 정해진 기준과 절차에 따라 실시하며, 접근 권한이 있는 자라도 중요한 비밀에 접근할 경우에는 반드시 접근 자의 인적사항, 접근목적, 일시, 접근방법 등을 기록 또는 모니터링하게 하여야 한다.

가. 비밀별 접근자 통제

비밀등급 및 개개의 비밀별로 접근 자를 지정 통제하고 그 이외에는 접근의 필요성에 의해 일정한 절차를 거쳐 정당한 이유가 있을 때에 접근을 가능하게 한다.

나. 접근자 별 통제

비밀 취급자, 관리자, 업무수행자 등 접근이 필요한 임직원별로 접근할 수 있는 비밀 또는 등급을 지정하여 접근을 통제하며, 비밀 접근자는 그 비밀에 접근할 권한이 있는지 그리고 업무수행에 꼭 필요한 접근이지를 확인하여야 하고 사후에 정보의 유출 또는 접근의 정당성을 확인할 수 있도록 반

드시 기록과정을 거쳐야 한다.

3.4.5 보호할 비밀의 등급 분류정책

가. 등급 분류의 원칙

◆ 적정 등급 분류의 원칙, 기업비밀은 내용의 가치에 따라 분류하되 고대평가나 과소평가 분류를 하여서는 안 되며, 과대분류는 필요이상의 제한으로 업무의 지장을 초래하고, 과소 분류는 비밀보호의 관리소홀로 비밀의 주요 내용이 유출될 수 있다.

◆ 비밀분류 독립의 원칙, 각각의 비밀 내용과 가치에 따라 분류하여야 하므로 다른 부서의 협조 및 자료요청 문서는 일반문서로 왔어도 회신하는 문서의 내용의 가치에 따라 독립된 등급으로 분류하여야 한다.

◆ 동일한 업무의 문서라도 각각 다른 문서인 경우 그 내용에 따라 독립적으로 분류하여야 한다.

나. 등급의 분류

기업별로 등급을 정할 수 있으며 가능한 등급은 2등급 또는 3등급으로 분류한다.

◆ 최상위 등급(극비, 1급 비밀)

그 기업의 경쟁력이 있는 최신의 기술, 최점단의 기술, 다른 기업이 보유하지 하지 못한 유일한 기술과 주요한 경영관리 정보들이 유출도면 경영에 많은 영향을 미치고 공개되면 경쟁업체에 큰 이익이 되는 정보, 침해되었을 때 법적으로 구제청구가 가능한 내용의 정보를 최상위 등급으로 한다.

◆ 중간 등급(비밀, 2급 비밀)

기업이 대외적으로 공개할 수 없는 정보로서 기업의 이익에 많은 기여를 할 수 있는 기술상의 정보 및 경영상의 정보로서 공개될 시에 경쟁업체의 대응책이 예상되는 정보이며, 침해시에는 침해의 유형, 형태, 피해정도에 따라 선별적으로 법에 의한 구제를 청구할 수 있는 정도의 비밀을 중간등급으로 분류한다.

◆ 하위급 등급(대외비, 사내한)

기업 내에서는 업무상 필요에 따라 보관자의 승인 후 열람 등 취급이 가능하며, 대외적으로 공개 시에 기업의 업무혼란, 경영상의 지장, 대외저인 이미지 손상 등에 예상되는 기술상·경영상의 정보와 기타공개를 전제로 일정기간 동안 보호할 필요가 있는 정보를 하위등급으로 분류한다.

3.5 AD기반 설계

기존에 각각의 DRM솔루션 Server DRM, PC DRM, File Server DRM 등으로 존재했던 DRM솔루션 형태를 Active Directory로 구성하여 도메인이라는 관리 단위를 만들어 통합적으로 관리하는 방법을 제안한다.

기존에 별도로 구성되었던 서버들도 도메인이라는 단위로 연동시킨다. 도메인에 합류된 컴퓨터들은 사용자 인증을 위해 자신의 로컬 데이터베이스 대신 AD를 이용할 수 있게 된다. AD가 설치된 서버를 도메인컨트롤러(Domain Controller)라고 한다. DC는 Active Directory에 개체를 저장, 사용자 로그온 프로세스, 인증, 디렉터리 검색 등 서비스를 제공한다.

그림 12. Active Directory 사용자 인증 과정

그림 12처럼 클라이언트가 사용자 계정을 이용하여 로그인하게 되면 도메인 컨트롤러에서 사용자 인증 요청을 하게 되고 AD 에서 사용자 확인 작업을 하게 된다. 데이터 보호기술인 DRM 기술을 이용하여 사용자 허가 방법을 AD서버를 통하여 도메인 간 인증 및 상호 연동 방안을 제공한다. 도메인 서버는 도메인 내 응용 서버들의 서비스를 제공받는 사용자 정보를 중앙 집중적으로 관리하여 사용자 인증 기능을 제공한다. 사용자 인증 기능은 사용자의 응용서비스 요청에 앞서 각 사용자들은 인증 하는 것이다. 인증 과정은 사용자의 ID/PW를 기반으로 인증 하는 방법이다. 도메인컨트롤러(DC)에서 알맞은 권한을 부여하고 각 응용 서버에 대한 사용자의 접근 권한은 관리한다.

기존 DRM을 문제점으로 인식되었던 별도의 프로그램을 설치하여 기존의 컨텐츠를 이용하는 인터페이스 자체를 변경하게 되는 경우 사용자는 이

로 인하여 상당한 이용의 불편함을 느끼게 되었는데 이러한 문제점도 자동으로 해결할 수 있게 된다.

사용자는 응용 서버를 제공받는 주체로서 인증 과정에서 필요한 ID/PW 정보를 도메인 인증에서 사용한다. 내부 자원의 보호를 위하여 비인가 된 사용자의 불법적인 접근을 차단하고 인간된 사용자들에게 부가적인 인증 과정 없이 서버스를 제공하기 위한 기능을 제공한다. 도메인 인증을 통하여 사내임을 인식하게 되고, 별도 인증 없이 문서내 파일 접근이 가능하다. 그림 13은 AD서버를 이용한 DRM설계 화면에 대한 설명이다.

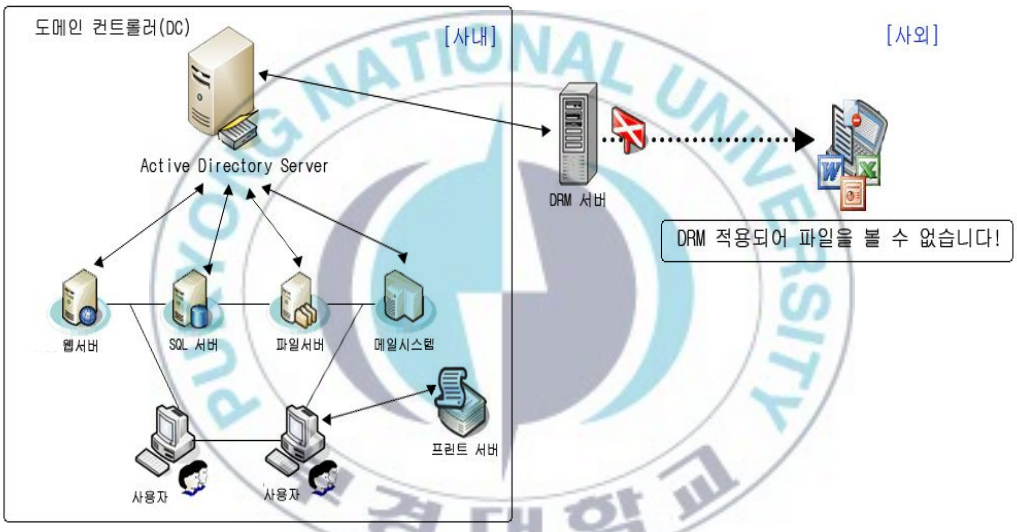

그림 13. AD서버를 이용한 DRM설계

도메인컨트롤러(DC)와 DRM서버를 연동시켜 도메인 인증이 없는 경우 외부로 인식하게 되고 DRM서버에서 데이터 암호화기술이 적용된다. 암호화 기술이 적용 되면 데이터를 열고자 할 경우 내용이 표시되지 않는다. 도메인컨트롤러(DC)와 DRM서버를 상호연동을 통하여 정보 유출 방지 효과

를 최대 활용할 수 있게 된다.

도메인간 상호 인증 기능을 검증하기 위하여 사용자는 자신이 속한 도메인(도메인 A)을 통해 사용자 인증을 요청한다. 도메인컨트롤러(DC)에서 사용자가 리스트에 포함되어 있는지 확인한다. 확인 과정 끝나면 그림 12 처럼 사용자 ID/PW를 도메인A에 인증하게 되고 로그인 과정을 걸치게 된다. 사용자는 도메인 A의 도메인 서버를 통해 ID/PW를 입력하게 되고 최초의 인증과정을 수행한다.

전체 시스템의 흐름을 순서대로 살펴보면 다음과 같다.

① 사용자는 AD서버에 인증 서비스를 요청한다.

② 이때 도메인컨트롤러는 서비스를 원하는 사용자에 대한 인증 요청을 수행하게 된다.

③ 사용자는 ID/PW를 AD서버내에 응답요청하고, 도메인컨트롤러에서는 정보과 일치하는 경우 인증을 실행한다.

④ 도메인 A의 사용자 정보가 변경되었을 경우 관련 사용자 정보를 보냈다.

⑤ 도메인A가 도메인 컨트롤러에 각종 서버(파일서버, SQL 서버, 웹서버 등)들이 연결되어 있다.

⑥ 프린트 서버는 네트워크 프린터를 이용하여 도메인 컨트롤러에 대해 서비스를 요청한다.

⑦ 사용자들은 도메인 컨트롤러에 연결되어 있는 서버 및 프린트 사용이 별도 인증 절차 없이 사용 가능하다.

⑧ 도메인 컨트롤러가 DRM 서버와 연결되어 도메인간의 상호 인증은 도

메인 A를 통해 인증된 도메인임을 확인하게 된다.

⑨ 도메인A 인증이 없는 경우 외부로 인식하게 되고, 각종 파일에 대해서 DRM서버에서 암호화기술이 동작하게 된다.

⑩ DRM서버에서 암호화기술이 동작하게 되면 파일을 열람할 수 없게 된다.

전체 시스템의 흐름동작의 순서를 추상 데이터 타입(DAT) 표현하면 다음과 같다.

```
BOOLEAN data                          //변수선언
data=connect(ip넘버, 포트번호)          //연결성공시 true, 실패시 false
if(data==true)                        //메시지박스(연결성공)
else                                  //메시지박스(연결실패)
open(ip넘버, 포트번호)                  //포트를 열고 대기
if( Accept(소켓) )                     //메시지박스(연결성공)
STRING ID="hjh"                       //변수선언 및 데이터입력
STRING PW="1234"                      //변수선언 및 데이터입력
STRING DATA=ID+PW
Send(DATA)                            //데이터 전송
STRING DATA                           //변수선언
STRING ID                             //변수선언
STRING PW                             //변수선언
Receive(DATA)                         //받은 문자를 DATA에 담는다.
ID=DATA.LEFT(3)                       //ID를 분리
```

```
PW=DATA.RIGHT(4)                    //PW를 분리
STRING DB_ID=DB_READ(ID)            //DB에서 ID읽어옴
STRING DB_PW=DB_READ(PW)            //DB에서 PW읽어옴
if(ID==DB_ID && PW==DB_PW)          //ID와 PW가 맞을 때 메시지박스
                                      (인증성공)
else if(ID==DB_ID)                  //ID만 맞고 PW가 다를때
{
        if(PW!=DB_PW)
        {
         Send("패스워드가맞지않습니다.")
        }
}
else if(ID!=DB_ID)                      //ID가 다를때
        Send("등록된ID가없습니다.")      //데이터 전송
```

3.6 단일인증을 통한 설계 구현

AD서버를 이용한 DRM 설계를 구현하게 되면 전체 구성도는 그림 14처럼 적용되게 된다.

기존 DRM 솔루션(Server DRM, PC DRM, File Server DRM 등) 여러 종류에 따라 각각 다르게 적용되었던 솔루션 방법을 엑티브 디렉토리를 통해 인증을 받게 되고, 별도로 존재했던 서버들도 엑티브 디렉토리(AD)와 연

동 시켜 사용자 인증 관리 및 정책 관리 위주로 설계했다.

기존 DRM방법은 AD도메인간 인증 절차를 걸치게 되더라도 각종 서버는 별도로 연결이 이루어지지 않게 되었다. 하지만 이 논문에서는 AD서버와 각종 서버들을 연동시켜 구성하게 되었다.

사용자 인증과 동시에 각종 서버에도 접근이 가능하게 된다. 또한 AD 서버와 DRM서버가 연동이 되게 구성하였다. AD서버를 중심으로 사용자 인증 과정이 걸치게 되게 각종 서버와 DRM서버와도 사용자와 연동이 되게 설계하였다.

사용자 pc에 에이전트로 설치가 되어 사용자 확인 할 수 있지만 기업에서는 개별사용자의 관리가 쉽지 않았던 문제를 AD와 연동해줌으로써 정책을 이용해서 바로 업데이트가 가능하다. 또한 휴가자나 퇴직자 또는 프로젝트를 통한 외부업체에 대한 관리가 명확하게 이루어지지 부분도 AD를 통해서 각종 서버와 연동이 되어 있어 실시간 정보를 수정가능하다.

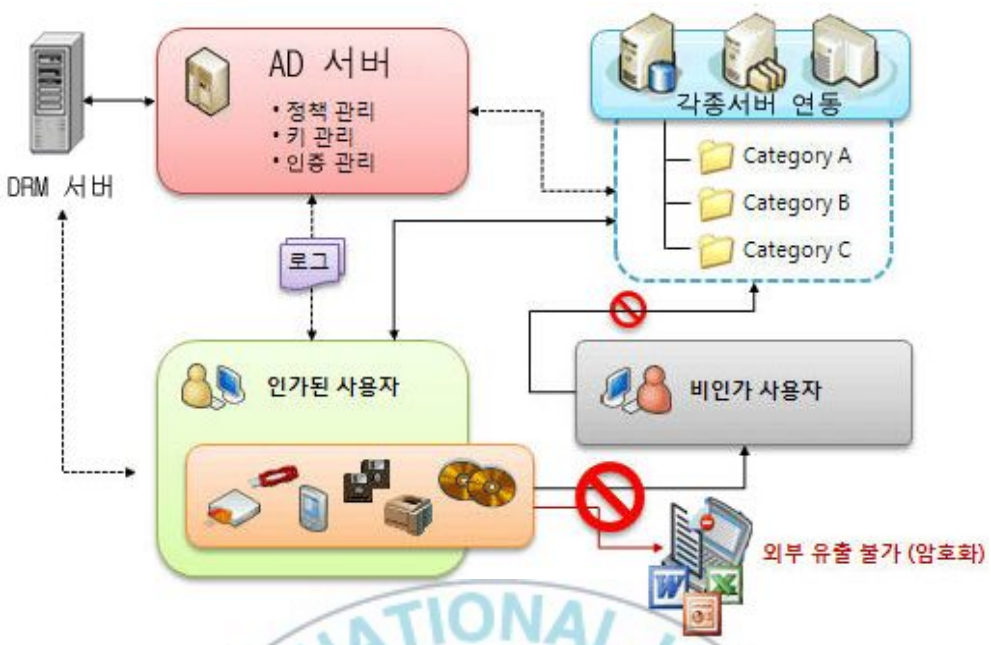

그림 14. AD서버를 이용한 DRM설계 전체 구성도

4. 결론 및 향후 연구

AD를 통한 사용자 인증을 통한 시스템 구조로 내부 정보 유통 구조의 취약점 식별 및 정보 보호 기술구조를 제안하였다. DRM 기술을 이용하면 단순 암호화하는 방법보다는 열람, 인쇄, 저장, 재배포 제한 등 이용 권한을 세분화 관리할 수 있게 되었다. 도메인 컨트롤러(DC)와 DRM서버를 상호 연동을 통하여 정보유출 방지 효과를 최대 활용할 수 있게 되었다.

각종 분산된 서버(인사서버, 파일서버 등)를 단일 인증을 통해서 한번에 상호연동이 가능하게 되어, 각종 서버에 연결되는 번거로움을 최소화 할 수 있으며, 새로운 유틸리티 버전에 대한 클라이언트와 호환성 관련 문제점이 있었으나 단일인증을 통해 새로운 유틸리티에 대해 쉽게 배포가 가능하며, DRM파일서버, 프린터 서버 등 여러 종류에 따라 정보유출에 대한 보호가 이루어졌지만, 통합해서 관리 가능하게 되었다.

기업보안 정보유출 방지기술은 개인 PC, 네트워크, 물리적 보안 등 이상 행위를 탐지하기 위한 유형, 무형의 보안 장치가 필요하다.

라이센스 전송 및 변환 기술을 적용하여 이기종 단말과의 DRM 연동이 가능하도록 구현이 되어야 하고, 모바일 DRM 기술 개발이 필요하다. 타 분야 간 DRM 호환성 미비로 인한 사용자, 기기제조 기업의 불편 및 비효율성 부분도 해결해 나가야 할 부분이다. 또한 전반적인 콘텐츠 유통 환경을 고려한 DRM에 대한 인식도 갖추어야 한다.

하나의 기술로 모든 취약점을 대응할 수 있었으며 DRM 기술이 한계를 갖는 영역은 다른 기술로 보안하여 대응하여야 한다. 통합 정보보보 기술

구조, DRM 외 다른 기술을 적용하는 방법, 등 내부 정보 유출 방지를 위한 활발한 연구가 필요하다.

참고문헌

[1] 최주호, “기획특집: 정보유출방지를 위한 방안의 실제”,

[2] 보안뉴스, http://www.boannews.com/plan/plan_view.asp?idx=6997,

[3] 송지훈, 이시진, 장향배, “내부정보유출 방지를 위한 데이터베이스 보안 솔루션 보안성 평가,” 2009. 06, pp. 179~187.

[4] 송지훈(2009), “내부정보유출 방지 솔루션 보안성 평가”, 대진대학교.

[5] 최옥현(2009), “내부자에 의한 정보 유출 위협과 대응방안 수립에 관한 연구”, 한남대학교.

[6] 이동희, “실습을 겸한 Server 2003,” 정일, 2008.

[7] 김지운(2008), “Active Directory를 이용한 디렉토리 서비스 개발에 관한 연구”, 부경대학교.

[8] 강호갑, “최신 DRM 기술동향”, 전자공학회지, 대한전자공학회, 2005, pp.18~22.

[9] 전용호(2005), “DRM 구조적 모델을 통한 기술요소 분석 및 국제 표준화 시장에 관한 연구”, 성균관대학교.

[10] 박재천, “DRM 시장 확대 및 공공부문도입에 관한 연구”, 한국정보사회진흥원, 2006.

[11] 황준석, 서덕록 “DRM 기술표준의 정책적 과제”, 서울대학교.

[12] 박찬길(2006), “디지털컨텐츠 보호를 위한 상호인증 프로토콜과 암호화 기법 설계”, 숭실대학교.

[13] 조규곤, “Enterprise DRM 구축 방안”, 정보과학회지. 23권 제8호. 2005, pp. 31~36.

[14] 이윤호(2008), “기업의 정보 유출방지를 위한 개인정보 전송시스템에 대한 연구”, 동국대학교.

[15] 양성은(2008), “DRM 솔루션을 이용한 문서보안에 관한 연구”, 동국대학교.

[16] IT기술 해외 유출 방지를 위한 메뉴얼, 정보통신부, 한국정보통신수출진흥센터, 2004. 02.

감사의 글

시작과 끝이 공존하는 12월 입니다.

2년전 공부를 하기 위해 원서를 넣고, 면접 보던 기억이 엊그제 같은데 벌써 석사학위를 졸업하게 되었습니다. 졸업을 앞두고 보니 교정 곳곳에서의 추억과 향기가 더 아름다운 그림이 있는 풍경으로, 추억으로 새겨집니다.

2년 동안 많은 가르침과 도움을 주신 많은 분들께 감사드리고 싶습니다. 특히 바쁘신 와중에도 시간 내어주시고 지도 및 교훈으로 따듯한 배려와 함께 항상 먼저 챙겨주셔서 석사학위를 무사히 마칠 수 있도록 도와주신 지도교수님이신 정목동 교수님께 진심으로 감사드립니다. 부족한 저희 논문을 심사 및 지도·조언을 해 주신 윤성대 교수님과 조우현 교수님께도 감사의 마음을 전합니다. 또한 많은 가르침과 격려를 주신 학과의 여러 교수님들께 감사를 드립니다.

연구실 생활을 함께하면서 많은 도움을 받았던 영민, 호식, 징스다, 재천 선배, 현동선배의 의 행복한 동행에도 감사드립니다.

교정에서의 짧은 2년은 마무리 되지만 따뜻한 어울림으로 향기를 주신 모든 분들의 고마움은 가슴속 따스한 햇살처럼 오래 기억 될 것 같습니다.

끝으로 한걸음 더 나아갈 수 있도록 도와준 사랑하는 가족들에도 고마움을 전하고 싶습니다.

대학원 생활을 마치면서 좀 더 열심히 생활할 수 있었는데 후회와 아쉬움이 남습니다. 그 후회와 아쉬움을 뒤로하고 이제 끝이 아닌 또 다른 시작을 향한 설레임으로 한걸음 더 나아가려 합니다. 감사합니다.

2011년 2월

황 진 희 올림