韓國 컴퓨터情報 學會誌
第10卷 第2號, 2003. 6

누출차단과 식별을 위한 다큐먼트 보안 디자인

장 덕 성

요 약

최근, 기업은 급변하는 비즈니스 환경 속에서 업무 효율성 극대화가 비즈니스를 수행하는데 필요로 한다고 인식하고, 이를 위한 해결책이 조직원간 정보공유를 활성화하기 위한 지식경영 시스템을 도입하고 있다. 지식경영 시스템의 근간이 되는 디지털 문서들은 복사 및 전달이 쉽고 빠르게 이루어 질 수 있다는 문제점이 있다. 이에 따라, 기업은 업무 효율성을 높이면서 동시에 기밀정보의 유출을 방지하기 위한 정보보안 정책을 세우고 있는 실정이다.

대부분 기업들의 초창기 정보화 과정에서는 네트웍 보안에 치중하여 방화벽이나 침입탐지 시스템 혹은 침입방지 시스템을 설치하여 외부 침입자를 차단하기 위한 노력에 집중하였으나 대다수의 기업 내부 정보 유출 사례가 내부자의 소행이라는 것이 밝혀지면서 업무의 효율성이라는 측면과 기업 내부 정보 보안을 위한 보안 기술을 채택하고 있다. 이에, 본 논문에서는 누출차단과 식별을 위한 다큐먼트 보안을 디자인함으로써, 디지털 정보보안 체계 확립과 더불어, 디지털 정보자산을 안정적으로 관리할 수 있게 되었다. 또한, 발생할 수 도 있는 디지털 정보자산의 불법유출을 사전에 차단함으로써 기업/기관의 노하우 및 정보자산을 안정적인 보호로 피해를 방지할 수 있게 되었다.

Ⅰ. 서론

최근, 산업전반에 확산되고 있는 디지털화와 전자거래의 활성화는 기업 운영에 많은 순 기능적인 역할과 함께 적지 않은 역기능적인 역할을 하여 왔다. 기업의 지식 자산인 디지털 정보 중 50% 이상은 재사용 되거나 참조될 것으로 예상되고 있으며, 웹 업무환경의 확산으로 전자거래가 촉진되어 전자문서의 생성과 배포 등의 프로세스는 이제 일상적인 업무가 되었다. 기업 내부·외부에서는 중요한 핵심정보를 구하기 위하여 이러한 환경을 이용하여 부단히 기업에 침투를 하고 있다. 이에 기업은 기업의 중요한 정보가 담긴 문서가 비인가자가 보거나 경쟁자에게 넘겨지지 않도록 예전보다 더 높은 경각심을 갖고 이를 방지하기 위한 대책 마련에 많은 자금, 시간, 노력을 투입하고 있는 실정이다. 기업 문서정보 유출은 크게 외부자의 침입과 내부자에 의한 유출로 나누어 볼 수 있다. 금년도 초 국내 인터넷 대란과, 4월경의 정보보호 사이트의 접근권한 노출은 바로 외부자의 침입에 의한 유출로서, 해커들은 가상사설망 등을 이용하여 흔적도 없이 다른 시스템의 정보를 가져가거나, 도청, 그리고 바이러스 침입 등으로 그 기업의 정보를 파괴시키기도 한다. 해커들의 기업정보 해킹공격과 이를 방지하기 위한 기업의 노력은 마치 창과 방패 같아서 상호간 공방이 치열하여

새로운 방지기술이 등장하면, 곧 얼마안가 새로운 해킹 기술이 나타나기도 한다. 스파이들의 기밀문서 유출, 1997년 반도체 사 직원의 기업기밀 외국 유출, 연구원들의 중요 설계도 유출, 개인신용 정보유출, 그리고 개인신용카드 정보 유출 등은 퇴직한 후에도 발생되어 기업뿐만 아니라 국가경제에도 큰 손실을 입히고 있다. 미국 FBI/CSI는 내부자에 의한 문서정보 유출이 70%나 된다고 하는데, 이는 종신고용이라는 고정관념이 사라지고, 또, 이직이 빈번이 일어나기 때문으로 본다. 유출되는 경로도 전자메일, 내부망 해킹, 대량출력, CD/디스켓, USB 등으로 다양하다.

II. 본론

1. 문서보안 개념

기업은 기업활동을 영위하기 위하여 기업의 중요핵심 도면, 제조설계서, 영업비밀, 입찰서, 기업전략, 사업계획 등 모두 기업의 흥망과 관련이 있는 정보가 담겨있는 전자문서를 생산하고 있다. 전자 문서는 사용자 자신이 갖고 있는 지식을 표현한다고 볼 수가 있는데, 이는 개인 정보 시스템을 보다 구체화 한 것으로써, 전자문서 기술은 조직의 핵심 역량을 비즈니스화 하기 위한 인프라인 것뿐만 아니라 조직원의 능력을 향상시키는 소스라고 볼 수 있다. 그러나, 정보 기술의 급격한 발전과 라이프 싸이클의 단축, 그리고 유연한 사용자 인터페이스 등으로 정보 사용자들은 전자문서를 손쉽게 획득할 수 있게 되었다. 이에, 조직내외에서는 허가자만 문서에 접근할 수 있는 보안관리를 고려하게 되었다. 따라서, 초기에는 중요한 문서의 보안을 위하여 다양한 문서접근 권한을 부여할 수 있도록 하였다. 문서 작성자는 문서를 작성 완료한 후, 사용자별, 그룹별 등으로 문서접근 권한을 다르게 할 수 있는 기능과 함께, 조직 내의 부서별, 직급별, 프로젝트별로 문서의 접근 권한을 사전에 지정할 수 있는 기능을 포함하였다.

그러나, 이들 전자문서들은 집중 관리되지 못하고 있는 실정이며 안전한 보안체계로 보호되지도 못하는 상황이다. 이에 따라, 기업은 기업의 업무경험과 기술이 조직원들간 공유되지 못한 상태가 진행되어 담당자가 퇴사 시, 또는 신규 구성원을 충원할 때, 업무 인수인계가 이루어지지 못하여 업무가 단절되는 경우가 종종 발생되고 있다. 더욱 문제가 되고 있는 것은 개인 컴퓨터에 보관된 중요한 전자문서인 설계도면, 기술 보고서 등이 무단 복사, e-mail 전송 등에 의하여 외부로 불법 유출될 수 있는 통로가 상시 열려 있어 기업자산을 더 이상 지킬 수 없게도 만든다.

2. 관련기술

문서정보의 불법 배포 및 위하여 변조 방지, 그리고 저작권 보호를 위하여 사용되는 기술은 DRM(Digital Right Management), 워터마킹(Watermarking), 2차원 바코드 기술, 인증, 암호화, 사용권한 관리, 템퍼 푸르핑(Temper Proofing), 업퓨스케이션(Obfuscation), 응용 소프트웨어 지원 커널수준 디지털 자산보호 소프트웨어 모듈, 추적, PKI 기반의 문서보안, 다양한 포맷의 문서의 PDF 파일 자동 변환 등이 있다.

① DRM(Digital Rights Management)

DRM은 콘텐츠 권리에 대한 명시와 콘텐츠 사용에 대한 허가, 그리고 콘텐츠 거래를 투명하게 해주 솔루션(Mark Baugher, 2001) 이라고 할 수 있다. 즉, 기업의 내부 정보 보호 목적보다는 멀티미디어 콘텐츠의 유료서비스를 효과적으로 지원하고, 수익원천이 되는 멀티미디어 콘텐츠를 보호하기 위해서 개발된 기술이다. DRM 기술은 재배포와 투명한 거래구조, 그리고 사용규칙이라는 특징을 갖고 있다(이창열), DRM은 일반적으로 다음의 〈그림 1〉과 같은 체제를 같고 구동한다.

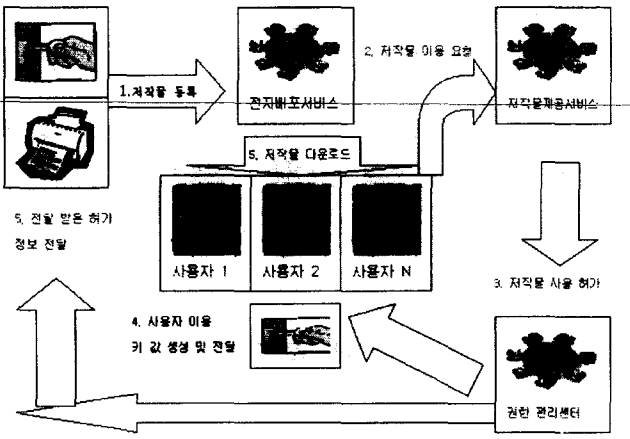

그림 1. 일반적 DRM 구성체제, 이경수

DRM 시스템은 콘텐츠 서버, 라이센스 서버, 클라이언트 어플리케이션, 키 분배 서버로 구성되어 있다(웹 비즈니스, 2002.6~9). 콘텐츠 서버는 콘텐츠 리파지터리로써 파일과 메타데이터들을 포함하고 있다. 즉, 이 서버는 콘텐츠를 암호화하고 사용자에 대한 제반 규칙(사용 횟수 및 기간, 출력 및 전송 권한 등)을 정의하여 콘텐츠와 함께 또는 분리(규칙의 캡슐화와 라이센스를 통한 전송)하여 사용자에게 전달한다. 라이센스 서버는 사용권한과 관련된 서버로써 콘텐츠를 사용할 수 있는 자와 장치 식별, 권한이 부여된 콘텐츠 인지, 권한과 관련된 세부사항 등을 포함하고 있다. 또한, 결제 시스템을 PG를 통해 연동시켜서 사용자의 대금 납입을 확인하여 라이센스의 전송여부를 판단하며, 사용자의 콘텐츠에 대한 반응 정보를 포함하고 있다. 클라이언트 어플리케이션은 콘텐츠 사용자의 컴퓨터에 설치되어 콘텐츠를 복호화 한다. 즉, 사용자의 콘텐츠 이용 요청에 따라 사용자나 장치를 식별하고,, 라이센스 서버로부터 실행시킬 콘텐츠의 라이센스를 받는다. 그리고 콘텐츠 구동을 위한 어플리케이션 인증획득과 함께 복호화 키를 넘겨받아 콘텐츠 복호화를 한다. 키 분배 서버는 키를 배포하기 위한 서버로써 콘텐츠는 대칭방식으로 암호화하고 라이센스 키는 비대칭 암호화 방식을 사용하여 공개키로 암호화한 후 전송을 하고, 사용자는 개인의 비밀키로 복호화를 한다.

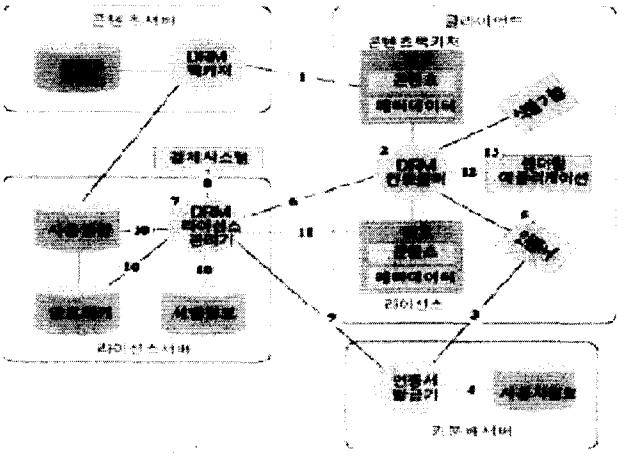

그림 2. DRM 시스템의 기술적 구성도, WebBusiness, 2002.6~9

② 워터마킹

DRM은 저작권이 침해되는 것을 막고자 암호화 기술을 적용하여 불법 사용을 방지하는 기술로써, 생성된 문서가 생성자의 시스템에서 암호화되면, 사용자는 ID 및 패스워드로 디지털 서명을 한 후 사용하여야 하므로, 문서가 외부로 유출되더라도 비인가자에게는 문서가 공개되지 않는다. 그러나, DRM은 콘텐츠 접근이 제한되며, 복호화가 된 콘텐츠는 보호하기가 어렵다는 문제점이 있다. 이를 보완하기 위한 워터마킹은 불법으로 복제되고 배포된 문서에 대한 추적이 가능한 기술로써, 디지털 콘텐츠 내부에 쉽게 알아볼 수 없는 디지털 코드를 삽입한 것이다. 즉, 워터마킹은 멀티미디어 데이터 자체에 사람의 지각으로 구분 할 수 있거나, 없도록 정보를 저장하는 행위(영상처리연구실, 경기대) 이다. 이 기술을 이용하면, 콘텐츠내에 저작권 정보인 워터마크를 삽입하여 저작권 보호가 가능하다. 복사 관련된 정보내에 워터마크를 삽입하면, 복사권한 부여, 복사회수 제한, 그리고 복사 방지 등의 사용권한 제어가 가능하다. 불법 유통되고 있는 콘텐츠를 발견시 누가 불법 배포하였는지를 추적하기 위하여 최종 사용자의 ID 정보 등을 삽입(핑거 프린트)할 수도 있다. 만일 위조나 변조를 하고자 한다면, 워터마크가 쉽게 손상되도록 하여 쉽게 알 수 있도록 한다. 또한, 과금과 모니터링을 할 수 있게 한다.

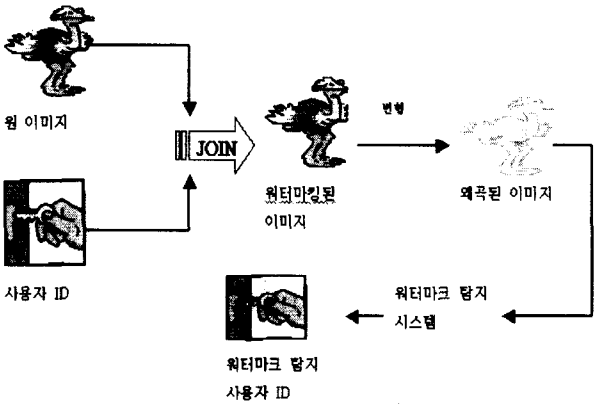

그림 3. 워터마킹 시스템 개념도

표 1. Watermarking 기술 분류, 영상처리연구실, 경기대

대 분류	중 분류	하위 분류	조 건
Invisible (워터마크를 보이지 않게 삽입)	Fragile		1. 원 이미지와 워터마크된 이미지간 차이 미 감지성 2. 워터마크 된 이미지에 대한 필터링, 압축 등에 대한 내구성 3. 워터마크의 보안성
	robust	Spatial/time domain (이미지 구성 픽셀 값 변경에 의한 워터마크 삽입)	
		Frequency domain (영상을 주파수로 변환하여 워터마크 삽입)	
Visible (워터마크를 보이게 삽입)			

③ 정부 민원 서류 위·변조방지

인터넷 민원발급시스템에서는 온·오프라인 연결 과정상 출력물인 문서의 보안성을 유지하는 것이 중요하다. 그러므로, 인증자가 인터넷으로 민원서류를 신청할 수 있는 기능, 신청한 민원서류에 대하여 신청자가 출력할 매수를 제한할 수 있는 기능, 그리고 출력한 민원 서류에 대한 복사 및 위·변조를 방지할 수 있는 보안성 유지 기능 등이 필요로 한다. 이를 위하여, 전자서명 인증, PKI, 프린터 제어, 2차원 바코드, 3차원 화상암호시스템, 워터마킹 등의 기술이 사용된다. G4C 인터넷 민원발급시스템에서는 정부 민원 서류를 온라인으로 발급 받을 때, 전자문서의 위·변조방지를 위하여 2차원 바코드 기술을 적용할 예정이라고 한다(황치규 delight@inews24.com).

그러나, 이러한 기술의 발전과 노력에도 불구하고 기업은 기업생존과 밀접하게 관련되어 있는 사업계획서, 입찰서, 제품개발서, 소프트웨어 개발서 등의 문서 정보들을 누출하고 있다. 이에 따라, 기업은 기업소유권과 기업 문서정보 유출자가 누구인지 확인하고 추적할 수 있는 사후증거 확보차원의 워터마킹 기술 이용이 요구되고 있다. 이뿐만 아니라, 적극적인 차원에서의 문서유출을 사전에 차단하는 것이 요구되고 있다. 이에 문서정보 보안 시스템은 다음과 같은 디자인을 고려하여 구현할 필요가 있다. 첫째, 조직 구성원 각자의 컴퓨터에 보관하고 있는 전자문서를 문서관리시스템데이터베이스에 저장한 후, 이를 상호간 공유하여 조직원들 간에 공유할 수 있는 지식경영 체재의 근간이 되도록 한다. 둘째, 데이터베이스에 보관된 전자문서들은 문서보안시스템으로 보호하여 기업 자산이 외부로 불법유출되는 것을 사전에 차단한다.

III. 제안 시스템

컴퓨터와 네트워크의 지속적인 발전으로 다양한 디지털 정보들이 널리 활용되고 있는 가운데 체계적인 보호 및 관리가 이루어지지 않아 기밀 정보의 유출, 무분별한 활용, 복제 및 보안에 대한 문제점이 점차 심각해지고 있다. 디지털로 된 중요/기밀 정보의 유출로 인하여 매년 각종 산업분야에서 피해가 증가하고 있으며, G/W, KMS, EDMS, ERP 등의 사무자동화시스템들의 확산으로 인하여 안정적인 문서 보안 및 유출방지 솔루션이 요구되고 있다.

본 논문에서 제안하는 통합문서보안 솔루션은 기존의 사무자동화시스템과 연계하여 저장되는 원천 문서에 대해 암호화 알고리즘을 이용하여 보안상태를 유지하고자 한다. 사용자가 다운로드를 받는 시점에서 해당 사용자만이 열람할 수 있는 권한을 부여하면 디지털 문서의 외부유출을 원천적으로 방지할 수 있다. 또한 암호화된 문서는 저장 및 출력, 전송 등을 제어, 불법유출을 예방하며, 온라인 및 오프라인 모두를 통제/감시할 수 있는 문서보안 솔루션을 제공한다.

내부의 기밀정보는 내부망 해킹 정보유출, 대량 출력으로 인한 정보유출, 전자메일 등으로 정보유출, CD/Diskette, USB등의 경로가 있다. 이에 내부 기물문서에 대한 유출방지와 저장, 편집, 전송, 무단 유출방지 및 사후추적 등을 위한 통제가 필요로 한다. 이를 위하여 통합문서 보안 솔루션으로 중앙 통제 및 감시를 통한 디지털 정보자산의 안정적 활용이 요구된다. 이에 사용자의 불법사용 시도 체크 및 각종 통계정보 기능, 문서의 Copy, Capture 및 편집방지 기능, 사용자별, 문서별 사용권한 부여 기능, 사용자와 시스템의 인증 기능, 권한 부여 출력 문서의 추적 기능, 복제, 해킹, e-Mail에 의한 유출시 사용 불가능 기능 등이 포함되어야 한다. 따라서, 본 논문에서는 다음의 〈그림 4〉와 같이 문서보호 및 관리시스템을 디자인 하고자 한다. 시스템은POMS(Policy Management Server), SECS(Service Control Server), CS(Contents Server), Contents-DB로 구성된다. SECS내에는 AKMS, lots, DOSS, LIUS를 포함한다. AKMS(Authentication & Key Management Service)는 사용자의 고유 ID 및 키를 관리하는 서비스이

며, 고유 ID는 사용자 PC의 시스템 정보를 바탕으로 자동 생성된다. DOSS(Document Supply Service)는 사용자 권한을 포함한 암호화된 문서를 만들며, Up/Down-Load를 수행한다. LTS(Log & Tracking Service)는 사용자가 사용하는 문서에 대한 전반적인 이력 관리를 해주며, 각종 통계정보를 제공한다. LUS(Live Update Service)는 사용자 PC에 설치된 AI Robot과 통신하고 실시간으로 업데이트를 수행한다.

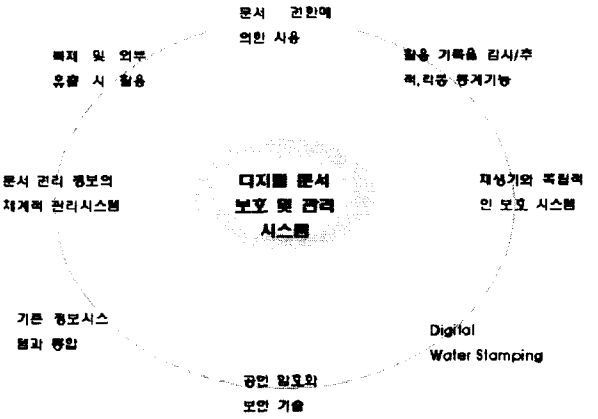

그림 4. 디지털 문서보호 및 관리시스템 도

1. 불법 유출방지 기능

암호화된 문서를 정상적으로 열 경우에는 다음의 〈그림 5〉와 같이 문서를 열람할 수가 있다. 그러나 불법적인 문서 유출(전송, 프린트, 화면캡쳐, 잘라내기 & 붙이기) 시도는 차단된다. 또한, 불법시도 행위 및 시간, 장소 등을 관리자가 모니터링 할 수 있기 때문에 보안 관련 통계정보를 이용하여 보안대책을 사전에 수립할 수가 있다. 만일 암호화된 문서를 비정상적인 경로를 통하여 강제적으로 열었을 경우에는 〈그림 6〉과 같이 문서의 내용을 알아볼 수 없는 상태로 나타나서 문서의 내용을 식별할 수가 없게된다. 물론, 암호화된 문서의 포맷을 임의로 변경한 경우에도 문서를 열람하여 볼 수가 없다.

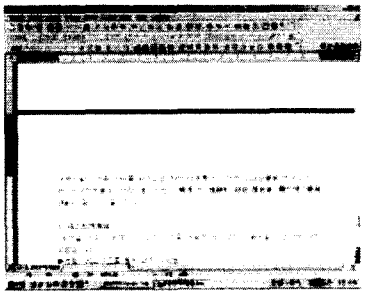

그림 5. 암호화 문서 정상오픈 화면

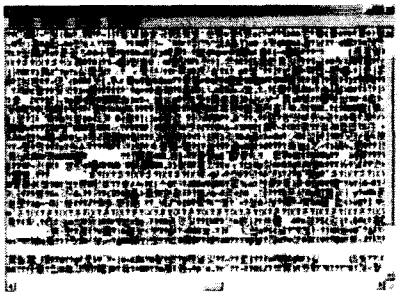

그림 6. 암호화 문서 비정상오픈화면

2. 보안정책 설정 기능

〈그림 7〉은 조직내의 보안정책에 따라 사용자에게 적합한 권한을 설정하기 위한 기능 화면이다. 이이에도 블록설정 권한, 편집권한, 문서유효기간, 문서출력권한, 로그설정 권한 등에 대해서 설정할 수가 있다.

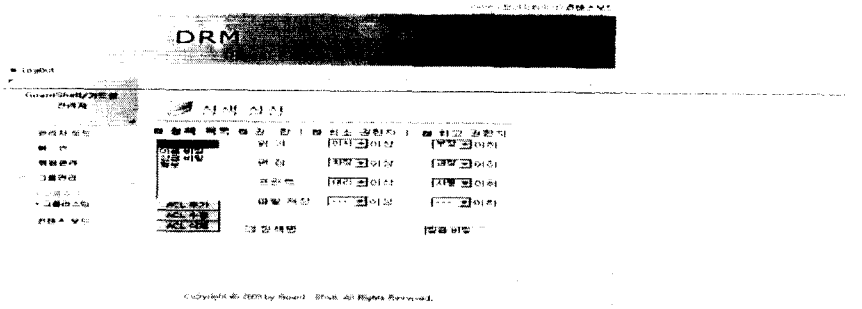

그림 7. 사용자 권한설정 화면

3. 문서저장 방지 기능

저장권한이 없는 사용자가 암호화된 문서를 저장하고자 한다면, 〈그림 8〉 과 같이 경고 창에 저장할 수 없다는 메시지 출력과 함께 저장화면이 나타나지 않는다. 물론, 메뉴, 아이콘 등도 동일하게 적용된다. 권한이 없는 행위는 모두 서버에 보고되어 보안관리자나 책임자가 그 내용을 모니터링 할 수 있게 된다.

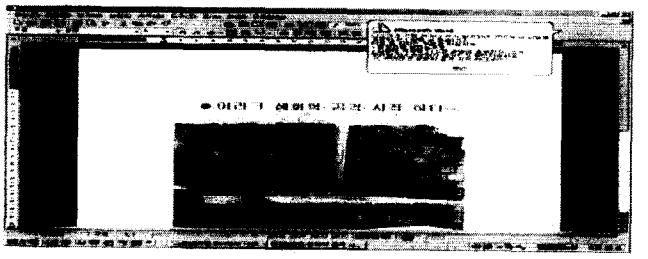

그림 8. 저장 권한이 없는 사용자의 저장 시도 시 나타나는 화면

4. 문서양도 제어 기능

사용자가 문서를 다운로드받을 때, 문서와 사용자의 고유한 시스템 키가 함께 묶어서 사용 권한이 없는 자의 열람을 원천적으로 방지한다. 또한, 타 시스템으로 문서를 양도하려고 시도할 때, 클라이언트에 설치된 AI Robot이 작동되어 양도를 차단한다. 또한, 〈그림 9〉와 같이 권한 없는 사용자에게 양도된 문서는 경고 메시지 창과 함께 문서가 자동 파기된다.

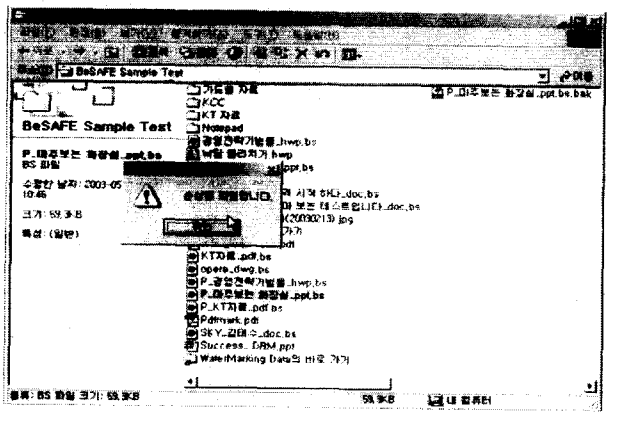

그림 9. 비권한 사용자에게 양도된 문서에 대한 경고 메시지 화면

• 워터 스탬핑 기능

출력되는 모든 자료에는 워터마크 처리를 함으로써 사후 추적 및 위·변조를 방지할 수가 있다. 워터스탬핑을 하는 정보는 고유 프린터 정보, 프린터 출력일시, 출력부서 및 출력자 정보가 들어간다. 고유 프린터정보는 관리자가 직접 지정하여, 사용자 신상정보 DB와 연동하여 사용자 신상정보 및 부가정보를 삽입하고 편집한다.

Ⅳ. 결론

이제 까지, 문서 보안 관련 기술을 살펴본 후 문서유출을 사전에 차단할 수 있는 디자인을 제시하였다. 대부분 기업들이 네트웍 보안만을 고려하여 방화벽, 침입탐지 및 침입방지 시스템을 설치하여 외부 침입자를 차단하기 위한 노력으로부터, 기업 내부정보의 유출 대부분이 내부자의 소행임을 인지하고 업무의 효율성이라는 측면과 기업 내부 정보 보안을 위한 보안 기술을 채택하고 있다. 그러므로, 방화벽이나 사용자 인증과 같은 절차가 기존의 1차적인 기업내의 디지털 정보를 지키기 위한 수단이었다면 디지털 정보에 대한 권한 관리와 암호화 등을 통해서 불법 사용자의 의지를 무력화시키는 보안기술은 차세대 디지털 정보보호 기술이라 하겠다.

따라서, 디지털 정보자산을 안정적으로 관리할 수 있는 디지털 정보보안 체계 확립과 더불어, 본 논문에서 제안한 시스템을 활용하면, 발생할 수 도 있는 디지털 정보자산의 불법유출을 사전에 차단할 수 있게 되어, 기업 및 기관은 자신들의 노하우 및 정보자산을 안정적으로 보호할 수 있게될 것이다. 이에 다음 사항들을 고려하면, 최근 나타나고 있는 정보유출에 의한 피해를 최소화할 수 있을 것이다.

첫째, 보안시스템을 구축 및 가동하기 전에 우선, 기업 내 문서 정보보안 정책을 수립하고 내부자가 수행할 절차를 규정하여야 한다. 기업에서 생성된 문서는 이동이 뒤따르기 때문에 문서정보 보호를 위하여 인위적으로 문서 이동을 원천 봉쇄한다면, 문서 생성자는 물론 열람자는 문서접근을 꺼려할 것이고, 이는 곧 근무자의 사기와도 연결되어 기업 생산성은 현저히 떨어질 수도 있기 때문에 각 기업상황에 적합한 정보보안 정책 수립이 요구된다. 그러므로, 각 문서에 대한 보안 수준에 따른 접근과 이용방법에 대한 정책결정이 결정된 후 적용되는 것이 중요하다.

둘째, 문서정보 보안 시스템은 높은 보안성 확보와 함께 사용자의 편의성이 동시에 제공되어야 한다. 만일, 강조된 보안의 중요성 때문에 기업 구성원이 시스템 사용을 함에 있어서 어려움이 있다면, 이는 문서정보를 올바르게 생성하는 것이 어려워지게 되어 기업경쟁력을 약화시키게 되므로, 사용자 편의성을 고려한 보안 시스템이 디자인되어야 한다.

셋째, 파일시스템, 네트워크시스템, 주변기기에 모두 보안기능을 부여할 수 있도록, 운영체제 레이어 기반의 커널링 0 수준에서 어플리케이션을 제어할 수 있어야 한다. 가상 드라이버 기술이나, 메시지 후킹기술은 복호화시 흔적을 남기지 않으나, 고의 정전이나 높은 기술의 디버거 사용자는 흔적을 발견할 가능성이 높다. 메시지를 먼저 후킹 당하면 보안이 뚫리게 되며, 레지스트리를 방어하지 못하게 되고, 또한, 메시지를 계속 트래킹하기 때문에 메시지가 오버플로우 되면 시스템에 치명적 오류가 발생되어 이때, 해킹되거나 크래킹될 가능성이 상존하므로, 하드웨어 API 후킹 기술과 RAM을 이용하여 하드웨어 드라이버를 제어하여야 한다.

V. 참고문헌

[1] 이창열, DRM, 동의대학교 컴퓨터공학과, 제82호 TTA저널, 이경수, 에이전트 기반의 DRM 솔루션, DRM 워킹그룹 워크샵, 2001.4.30

[2] 영상처리 연구실, Digital Watermarking,
http://www.kyonggi.ac.kr/~jcchun/gip/web%20page/ lecture/multimedia2002/Digital.ppt

[3] 조성호, guardshell paper

[4] 장덕성, 기업자산인 문서정보 유출방지를 위한 제언, SPC, 2003.6

[5] 황치규, delight@inews24.com

[6] Mark baugher, Digital Rights Management on Internet Protocol Networks, cisco systems, DRM 워킹그룹 워크샵, 2001.4.30,

[7] WebBusiness, DRM 비즈니스와 기술, 2002.06~09월호