내부정보 유출 방지를 위한 정보보호 기술구조 설계 및 구현에 관한 연구

문진규*
*국방과학연구소
e-mail:jingue@add.re.kr

A Study on Information Security Architecture for Prevention of Proprietary Information Leakage

Jin-Gue Moon*
*Agency for Defense Development

요 약

내부 정보 유출 방지체계는 침입탐지시스템이나 방화벽 같은 외부 공격자에 대한 방어 대책으로는 한계가 있어 새로운 정보보호 체계가 필요하다. 본 논문은 내부정보 유통 구조에 내재되어 있는 내부 정보 유출 취약점을 분석하고 이에 대한 대책으로서 새로운 정보보호 모델을 제안하며, 제안된 정보보호 모델을 구현하는 한 방법으로서 DRM 기술을 적용한 정보보호 기술구조를 제안한다.

1. 서론

그 동안 정보보호 대책은 외부 침입자나 바이러스에 대한 방어 대책이 주를 이루었고 내부자의 고의적 또는 관리 소홀에 의한 정보 유출에 대한 대책은 미비한 실정이었다.

전자문서의 안전한 유통 환경을 위한 기존의 정보보호 대책[1]은 비 인가자로부터 기간시스템 보유 자료의 기밀성 보호와 서비스의 가용성 확보에 초점을 두고 있으며, 실제로 내부 인가자 간 비공식 유통 경로는 등한시하고 있다.

최근 정보화 수준이 고도화되고 대외 기술 교류가 활발해짐에 따라 내부자의 기업 정보 유출에 의한 피해 사례가 급증하고 있어 이에 대한 체계적인 연구와 실용적인 시스템 개발이 매우 절실히 요구되고 있다[2,3].

2장에서는 관련 연구를 살펴보고, 3장에서는 내부정보 유통 구조의 취약점을 분석하며, 4장에서는 DRM 기술을 이용한 보안 기술구조를 제안하고 구현 시 고려사항을 설명하며, 마지막으로 5장에서 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

초기 DRM은 콘텐츠의 상거래시 콘텐츠 보호가 주목적이었지만 현재는 여러 방면에서 응용되고 있다. 상거래 시 콘텐츠의 저작권 보호를 위한 DRM을 Commerce DRM, 문서 보안용 DRM을 Enterprise DRM이라고 부른다[4,5]. Enterprise DRM은 기업 내부의 또는 외부의 합법적 사용자의 고의나 부주의로 인한 정보의 유출을 막을 수 있고 정보보호 대상이 주로 PC나 PDA상의 다양한 프로그램이 작성하는 문서를 대상으로 하고 있다.

3. 내부정보 유출 취약점 분석

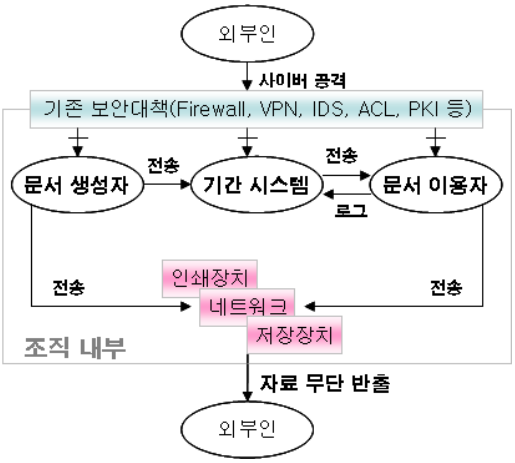

그림 1 내부 자료 유통 구조의 취약점

내부자에 의한 정보 유출의 원인은 조직 내 인가자에 대해 조직 내 자료의 무원칙하고 무제한적인 접근권한 부여와 내부자료 유출 방지를 위한 체계적인 정보보호 대책 미흡을 들 수 있다.

그림1에서 기간 시스템에 올려진 문서 생성자의 사본은 생성자 PC에 남아 있어 보안 관리는 전적으로 사용자 책임이다. 또한 문서 생성자는 기간 시스템 외 ftp, P2P 등 다른 관리되지 않는 수단으로 제3의 문서 이용자에게 전송할 수도 있다.

자료 유출 취약점을 정리하면 다음과 같다.

- 공식 문서: 기간 시스템에서 다운로드한 문서의 무제한적 활용 가능성

- 비공식 문서: 본인 또는 제3자가 생성한 비공식 문서의 무제한적 활용 가능성

4. 정보보호 기술구조 제안

4.1 내부정보 유출 방지 정보보호 모델

PC는 기간시스템의 사용자 인터페이스, 문서 생성자, 그리고 이용자 역할을 함과 동시에 비공식 유통경로를 통해 자료유출 포털 역할을 하기도 한다. 기간시스템은 사용자 역할에 따라 접근권한 부여는 엄격한 반면 일단 접근이 허용된 자료에 대해 내부자에 한하여는 그 이용이 관대한 정보보호 정책으로 운용되기 쉽다.

본 논문에서 제안하는 내부정보 유출 방지 정보보호 모델은 조직의 전산자원이 관리영역과 비관리영역으로 명확히 구분되도록 관리영역을 정의하고, 관리영역 내의 정보체계나 정보기기에서 비관리영역으로의 정보체계나 정보기기로 자료흐름을 통제하는 구조로 기존 자료 유통 구조를 전환하도록 하는 것이다.

4.2 정보보호 기술구조 설계

4.2.1 정 의

전자문서 저장 및 관리의 주체를 기준으로 Enterprise DRM[4] 기술을 아래와 같이 2가지로 세분화 정의한다.

- PC DRM

PC DRM은 패키징의 시점이 PC 내에서 이루어진다. 문서 생성자가 PC 내에서 문서를 처음 생성하여 저장하거나 기존 PC 내 자료를 수정하여 저장하거나, 또는 정보체계 서버로부터 문서를 다운로드 받아 PC에 저장하는 시점에 패키징이 이루어진다. 문서 관리의 주체는 PC 관리자이다.

- Server DRM

Server DRM은 패키징의 시점이 정보체계 서버 내에서 이루어지며, 자료 유통 시 자료의 열람, 인쇄, 저장 등 다운로드 후 이용의 권한을 통제하는데 사용된다. 문서 관리의 주체는 서버 관리자이다.

4.2.2 정보보호 기술구조

내부정보 유출 방지 정보보호 모델의 핵심은 조직의 전산자원을 관리영역과 비관리영역으로 명확히 구분하고 관리영역에서 비관리영역으로의 자료흐름을 통제하는 것이다. 본 논문은 PC DRM과 Server DRM을 이용하여 표1과 같이 정보보호 기술구조를 제안한다.

Server DRM의 보호대상은 조직의 기간시스템인 각종 정보체계에 저장된 자료이다. 정보체계에는 통상 화면별로 ACL이 정의되어 있는데 여기에 자료 이용에 관한 권한 속성을 추가하여 자료 이용 권한을 관리하는 것이며 화면별로 관리영역을 구분하여 비관리영역으로의 자료 유출을 통제하는 것이다.

PC DRM의 보호대상은 PC에 저장되는 전자문서이다. PC의 애플리케이션 종류를 기준으로 관리영역을 구분하며 ACL과 통제유형을 조직 내 공통 보안정책에 따라 설정하여 비관리영역으로의 자료 유출을 통제하는 것이다.

구 분	Server DRM	PC DRM
보호대상	정보체계 (공식문서)	PC (비공식 문서)
문서특징	열람 위주	편집, 재생산 위주
자료유형	문서, 웹페이지 등	문서
패키징 시점	다운로드 이전	- 편집 문서 저장 시 - 다운로드 시
ACL	정보체계별 정책	조직 공통 정책
통제유형	열람, 인쇄, 저장 등	열람, 인쇄, 저장 등
자료반출	정보체계별 정책	조직 공통 정책
인증	조직의 SSO 연동	조직의 SSO 연동

표 1 내부정보 유출 방지를 위한 정보보호 기술구조

4.3 정보보호 기술구조의 적용 방법

4.3.1 기간시스템 보유 자료의 관리영역 구분

Server DRM의 경우는 응용프로그램마다 화면별로 사용자의 역할에 따라 관리영역을 정의한다. 관리영역은 응용프로그램의 화면별로 ACL이 정의되고 해당 화면에 첨부되는 문서 파일에도 그대로 ACL을 적용하며, 추가로 Server DRM이 제공하는 자료의 이용권한을 R(열람전용), R+P(열람 및 인쇄전용) 등으로 세분화하여 ACL에 추가한다.

4.3.2 PC 보유 자료의 관리영역 구분

PC DRM과 Server DRM을 적용한 후 PC내에 저장된 문서는 그림2와 같이 관리영역과 비관리영역이 구분되고 관리영역내 문서는 비관리영역으로의 이동이 통제된다.

PC DRM에서 관리영역에 편성시킬 애플리케이션의 종류는 전자문서가 유통되는 각 정보체계별 파일형식, 문서의 종류, 문서저작 프로그램, 사용빈도 등 조직 내 문서의 유통환경을 고려하여 선정한다.

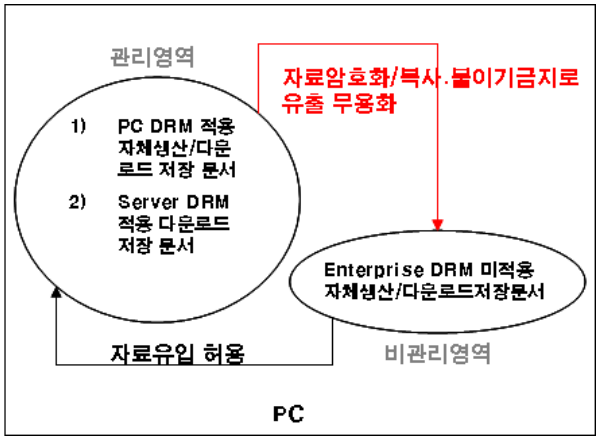

그림 2 PC내 저장된 문서의 관리영역 구분

Server DRM의 ACL 정의가 운용되는 정보체계 특성에

따라 여러 가지로 정의될 수 있는 반면 PC DRM의 ACL 정의는 조직 내 유통되는 비공식 전자문서에 관한 보안정책이므로 조직 공통 ACL로서 정의한다.

4.3.3 PC 내 패키징된 자료의 업로드 및 다운로드

제안된 정보보호 기술구조를 구현할 때 고려해야 할 사항을 설명한다.

PC DRM에 의하여 PC내에 패키징되어 보관중인 자료를 정보체계 서버에 업로드시 다음과 같은 선택이 가능하다.

1. PC내 암호화된 자료를 서버에 그대로 업로드
2. PC내 암호화된 자료를 복호화한 후 업로드
3. PC내 암호화된 자료를 그대로 업로드하고 추후 서버에서 복호화

서버에 암호화된 자료를 그대로 가지고 있는 경우는 가장 단순한 구조이며 보안성도 유리하다. 그러나 다음과 같이 서버가 암호화된 자료를 별도 가공 처리하고자 할 때는 문제가 발생할 수 있어 상황에 따라 PC DRM에 의하여 PC내 패키징된 자료의 처리가 달라진다.

1. 정보검색을 위하여 색인하고자 할 때
2. 타 기관으로 전자문서를 송부할 때
3. 정보체계 자체 ACL과 연동하고자 할 때

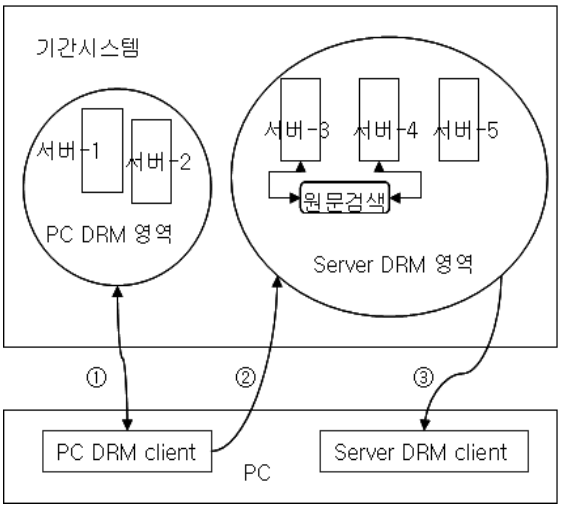

그림 3 PC와 서버 간 자료 연동 고려사항

그림3에서 ①은 PC DRM에 의해 자동으로 암호화 저장된 문서를 정보체계 서버-1과 서버-2에 암호화된 상태 그대로 업로드 및 다운로드하는 상황이다. PC에서 문서가 최초로 저장될 때 지정된 ACL 규칙이 자료유통 경로 상 이용자에게 그대로 유지된다. 암호화된 자료를 서버에서 별도 가공하거나 정보체계 간 연동이 별도로 필요 없기 때문에 구조가 단순하여 쉽게 구현된다.

②는 PC 내에 패키징된 자료가 서버에 복호화 되어 저장되는 상황을 나타낸다. 서버-4와 서버-5는 자료에 대한 원문검색(Full-Text Search) 기능을 위해 서버 내 저장된 자료를 사전에 복호화 저장한다. 이 외에도 서버 내에서 별도 가공 처리가 필요할 수 있다. 또한 외부 기관과 전자문서의 유통이 이루어진다면 동일한 정보보호 체계인 경우는 관계없지만 외부 기관 서버에 자료를 전송하기 전 복호화된 자료가 저장되어 있어야 한다.

복호화 주체는 PC이거나 서버가 될 수 있다. 서버가 복호화를 수행하는 구조에서는 업로드 시 바로 복호화가 필요한 경우는 정보체계의 업로드 S/W모듈이 PC DRM client를 호출하도록 수정되어야 한다. 그렇지 않다면 서버의 내부 배치프로그램이 수행하게 할 수도 있다. PC가 복호화를 수행하는 구조에서는 PC-DRM의 복호화 기능이 담당한다.

③은 복호화된 자료에 대하여 ACL정의가 서버의 애플리케이션 프로그램이 정의하고 있는 ACL에 따라 Server DRM이 적용되는 상황을 나타낸다.

5. 결 론

본 논문은 내부자 정보 유출의 방지 대책으로서 내부정보 유통구조의 취약점 식별 및 정보보호 모델을 제안하였다. 제안된 모델을 구현하기 위하여 DRM 기술을 이용하여 정보보호 기술구조를 제안하였고 제안된 기술구조를 기간시스템과 PC에 적용할 때 고려해야 할 사항을 설명하였다.

제안된 기술구조는 조직 내 정보체계와 정보기기를 자료 유통의 통제가 가능한 관리영역으로 구분하고 외부로의 무단 유출을 통제하는 장점이 있다.

실제 적용은 조직 내 자료유통 환경 분석 및 우선순위에 의해 이루어져야 하며, 순차적 적용이 바람직하다고 판단된다[5,6]. 하나의 기술로 모든 취약점을 대응할 수는 없으며 DRM 기술이 한계를 갖는 영역은 다른 기술로 보완하여 대응하여야 한다. 앞으로 내부정보 유출 방지체계가 기존 정보보호 대책과 함께 정보보호의 한 분야로 자리매김할 수 있도록 통합 정보보호 기술 구조와 DRM 외 다른 기술의 도입 시 장.단점 분석 등 활발한 연구 및 시스템 개발이 지속적으로 이루어져야 한다.

참고문헌

[1] William Stallings, "Network and Internetwork Security," Prentice Hall, 1995.
[2] 국정원, 정통부, “정보보호 수준”, 2005 국가정보보호 백서, pp.7-21, 2005.6.
[3] 허현회, “기업의 산업기밀 관리실태 및 시사점”, 기술과 경영, 통권 제275호, pp.9-13, 2006.7.
[4] 윤기송, “DRM 기술 현황 및 콘텐츠 유통 인프라 구축 방안”, 정보과학회지 23(8), 통권 제195호, pp.8-14, 2005.8.
[5] 조규곤, "Enterprise DRM 국축 방안", 정보과학회지, 23(8), 통권 제195호, pp.31-36, 2005.8.
[6] 한영구, 최명길, 김세헌, 정보보호정책 도입에 영향을 미치는 요인에 관한 연구, 한국경영과학회, 2004년 추계 학술대회논문집, pp.636-639, 2004.11.