Enterprise DRM 구축 방안

파수닷컴 조규곤

1. Enterprise DRM 개요

Digital Rights Management(DRM) 기술은 디지털 콘텐츠의 저작권 보호를 목적으로 1990년대 중반부터 개발이 시작되었으며, 국내에는 2000년부터 소개되기 시작하였다[1][2]. 초기 DRM은 콘텐츠의 상거래 시 콘텐츠 보호가 주목적이었지만 현재는 여러 방면에서 응용되고 있다. 기업들은 자신들의 중요한 자산인 문서의 기밀을 효과적으로 지키기기 위하여 DRM의 활용을 연구해 왔다. 상거래 시 콘텐츠의 저작권 보호를 위한 DRM을 Commerce DRM, 기업 문서 보안용 DRM을 Enterprise DRM이라고 구분하여 부른다. 혹은 Enterprise Rights Management(ERM)이라고 부르기도 한다. Enterprise DRM과 Commerce DRM은 표 1에서와 같이 서로 다른 특성을 가지고 있다.

방화벽, VPN, IDS, IPS, 서버보안, PC보안 등 기존의 보안 솔루션들은 기업의 자산을 외부의 침입자로부터 보호하기 위한 것이었다. 반면에 Enterprise DRM은 기업 내부의 혹은 외부의 합법적 사용자의 고의나 부주의로 인한 정보의 유출을 막을 수 있는 특징이 있다. Commerce DRM이 표준 문제, 사용자들의 fair-use 권리의 보장 문제 등 때문에 본격적인 확산이 늦어지고 있는 사이 Enterprise DRM 기술은 2001년부터 기업의 문서 보안에 적용되기 시작하였고, 그 시장은 성장기로 접어들어 2008년 미국 시장 규모가 2억7천4백만 달러 규모에 이를 것으로 예상되고 있다[3]. 초기 Enterprise DRM 기술의 적용에는 문서 저작 프로그램 제어 기술이 문제가 되었었다. Application plug-in, OS level hooking, application hooking, 등 여러 다른 시도가 있었으며 최근 들어서는 application hooking 기술이 주류를 이루고 있으며, 일반 문서뿐만 아니라 CAD, 그래픽 디자인 관련 저작 프로그램들도 제어하고 있다[4]. 저작 프로그램을 개발하는 Microsoft나 Adobe 같은 회사는 소스코드를 고쳐 DRM 기능을 제공하고 있으나 각 회사의 DRM 방식에 상이하고 채택하려는 기업 입장에서 보면 해당 회사의 저작 프로그램 만 사용하는 것이 아니라서 아직은 실제 적용에 제약이 따른다.

기업마다 Enterprise DRM 솔루션의 도입이 늘어나면서 겪는 어려움은 DRM의 기능을 충분히 활용한 문서 보안 정책의 수립이 쉽지 않다는 것이다. 중 규모 이상의 기업에서 본격적인 DRM 적용을 계획할 경우 고려해야 할 사항들이 많아져 보안 정책을 정하는데 많은 시간을 허비하게 된다. 아직은 많은 기업들이 보안 사고 후 다급히 DRM 솔루션을 도입하거나 특정 시스템에 국한하여 구축하는 경우가 많아 체계적인 접근이 이루어지지 못하는 경우가 많다. 이런 경우, 향후 DRM 적용을 확산하려 할 때 어려움에 처하게 된다. 본 논문에서는 그런 문제를 피할 수 있는 Enterprise DRM 구축 방안을 제시하고자 한다.

표 1 Commerce DRM과 Enterprise DRM 비교

	Commerce DRM	Enterprise DRM
사용 환경	다양한 디지털 기기에서 특정 프로그램	주로 PC, PDA 상의 다양한 프로그램
정책	콘텐츠 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 발생 시 조사를 위하여 필요

2. 기존의 문서 보안 정책

DRM이 문서 보안에 적용되기 이전의 문서 보안 정책은 어떠하였는지 살펴보자. 문서들이 전자화되기 전에는 기업들은 대체로 다음과 같은 문서 관리 체계를 가지고 있었다.

1. 문서를 등록(문서 번호 부여 및 문서 대장에 기록)
2. 보안 등급, 보존 연한 설정

3. 등급 별로 문서 캐비닛에 보관
4. 열람 관리
5. 폐기 관리

여기서 보안 등급이라는 것은 기밀, 사내한, 일반 등의 등급으로서 각 등급별로 열람할 수 있는 범위 등 상세 관리 규정이 사전에 정해져 있다. 이런 방식에서 보안의 핵심은 문서 캐비닛의 키 관리와 열람 권한을 가지고 있는 사람이 정해진 보안 범위 내에서 만 열람하는지 여부이다. 그러나 이런 보안 정책은 다분히 선언적인 의미만을 가지고 있지 허점이 많을 수밖에 없었다.

근래에는 모든 문서들이 전자화 되면서 변화가 생기게 되었다. 위와 같이 단순한 보안 등급 외에 문서 별로 구체적인 사용자나 그룹을 지정할 수 있게 된 것이다. EDMS 같은 시스템들은 문서 별로 단순 열람 권한뿐만 아니라 편집할 수 있는 권한 등을 Access Control List(ACL) 를 통하여 관리하도록 하였다. 이런 문서 전용 시스템 외에도 문서를 첨부할 수 있도록 한 응용 프로그램에서는 화면 별로 ACL이 있어 해당 화면에 첨부되는 문서 파일에도 그대로 ACL이 적용되고 있다.

종이 문서를 사용할 때의 보안 방식 보다 진일보 한 것으로 보이지만 오히려 보안성은 떨어졌다. 문서 파일은 사용자 PC로 다운로드된 후에 ACL에 없는 여러 다른 사람에게 재 배포될 수 있다. ACL은 해당 서버에서만 효력이 있지 사용자 PC에서는 아무런 소용이 없다. 전자파일의 유통이 종이 문서의 유통보다 편한 만큼 보안도 취약해 졌다고 보아야 한다.

3. DRM을 활용한 문서 보안 정책

DRM을 적용하면 각 문서 별로 다음과 같은 점을 통제 할 수 있게 된다.

- 사용자, 사용 PC, 사용 기간, 사용 회수, 오프라인 사용 허용 여부, 사용 이력 수집 주기
- 보기, 편집, 인쇄, 암호화 저장, 원본 저장 허용 여부

이제는 ACL이 가지고 있던 원래의 의미가 사용자 PC에 까지 기술적으로 구현 할 수 있게 된 것이다. 그러나 통제할 수 있는 항목들이 늘어나면서 정책적으로 결정해야 할 사항들은 기하급수적으로 늘어나게 된다. 위와 같은 문서 별 보안을 어떻게 설정 할 수 있도록 할 것인가에 대한 정책 외에도 패키징 시점, 사용자 인증 방식에 대한 정책의 선택도 Enterprise DRM의 구현에는 매우 중요하며 문서 보안 정책은 더욱 복잡해 질 수밖에 없다.

3.1 문서별 보안 설정

보안 설정을 누가 하도록 할 것인가가 우선 매우 중요한 보안 정책이다.

A. 기존 시스템의 ACL에 의한 자동 설정
B. 관리자가 설정
C. 문서를 작성하는 혹은 서버에 문서를 업로드 하는 사용자가 설정
D. 혼합형, A+C 혹은 B+C

사용자가 정하는 것 보다는 관리자나 시스템에 의한 자동 설정이 간편할 수는 있으나 유연성 면에서는 떨어진다. 사용자에게 모든 것을 결정하게 할 경우 유연성은 있으나 사용자들이 적극적으로 DRM을 적용할 것인가가 관건이다. 그래서 위의 D와 같이 혼합형이 많이 채택되고 있다.

관리자나 사용자가 문서의 보안 설정을 할 때 DRM의 각 보안 기능의 사용 여부를 직접 설정하게 할 수도 있지만 문서 별로는 보안 등급 만을 설정하게 할 수도 있다. 보안 등급을 기밀, 사내한, 일반 등으로 혹은 1등급, 2등급, 3등급 등으로 나눈 다음 각 보안 등급에 관하여 관리자가 상세한 DRM 보안 기능을, 예를 들어, 다음과 같이 설정해 놓는다.

- 기밀: 보기만 허용, 편집, 인쇄, 저장, 오프라인 사용 불허, 유효기간 1년
- 사내한: 보기, 편집, 인쇄 허용 저장 불허, 오프라인 사용 허용, 유효기간 무제한
- 일반: 제한 없음

이런 보안 등급에 의한 간접적인 설정은 문서별 보안 설정 상 사용자의 편의를 도모하기 위한 것이다.

3.2 사용자 인증 방식

문서 유통을 위하여 기업 내에서는 어떤 방법이던 사용자 인증 방법이 있을 것이다. DRM 시스템은 그 인증 방법을 활용하는 것이 가장 좋다. 특정 DRM 시스템은 별도 인증 기능을 가지고 있어서 사용자들이 문서 유통 시스템의 인증과 함께 이중으로 인증 절차를 거쳐야 하는 경우도 있다. 별도의 추가 인증을 하는 경우 인증의 신뢰성은 높힐 수 있지만 이로 인한 사용자의 불편, 관리의 어려움이 늘어난다.

SSO(Single Sign On)가 구축되어 있다면 문제는 간단해지지만 SSO로 통합되지 않은 영역도 있고 아직도 많은 기업들이 복수의 인증 시스템을 가지고 있는 경우가 많다. 이 경우에도 DRM을 위하여 별도의 통합 인증 시스템을 구축하는 것은 바람직하지 않다.

기업의 문서는 기업 내에서만 유통 되는 것이 아니라 기업 외부에도 업무 상 유통 될 필요가 있다. 이 경우 외부인 인증하기 위한 방법이 필요하다. 다음과 같은 방법들이 사용되고 있다.

- 기존 인증 시스템을 활용할 수 있다. 기존 시스템을 확장하여 외부인에게도 미리 등록을 하도록 하여 새로운 ID를 발급하는 것이다. 이 방법은 문서를 주고 받을 외부인의 범위가 한정적일 때 효과적인 방법이다.
- 다른 방법은 외부의 인증 서비스를 활용하는 방법이다[5]. 널리 퍼진 인증기관이 있다면 편리한 방법이 될 수도 있으나 보내는 사람이 받는 사람의 ID를 알기 쉽지 않다는 문제가 있다. PKI(Public Key Infrastructure) 기반의 공인 인증서를 활용하는 방법이 그런 예 중에 하나이다.
- 송신자와 수신자 간에 서로 공개키를 교환하는 방법이 있다. PGP 같은 방법이 그 예이다[6].
- 이메일 주소를 ID로 활용하고 수신자가 해당 ID의 실 소유자임을 확인 하는 이메일 기반의 인증 방식을 활용한다[7].

이메일 기반의 인증 방식이 가장 간편하고 널리 쓰일 수 있는 방법이나 각 기업이 처해 있는 환경에 따라 다른 방식을 선택할 수 있다.

3.3 패키징 시점

문서를 암호화 하는, 즉 패키징하는 시점은 문서가 작성되어 서버에 저장 되었다가 다시 열람자의 PC까지 내려오는 과정에서 보면 다음과 같은 선택의 여지가 있다.

1. 생성과 동시
2. 서버로 업로드 될 때 사용자 PC에서
3. 서버로 업로드 될 때 서버에서
4. 서버에 등록 된 후 일괄 작업으로
5. 사용자에게 다운로드 될 때 서버에서
6. 사용자에게 다운로드 될 때 사용자 PC에서

패키징 하는 시점을 늦출수록 원본 상태의 파일이 존재하는 시간이 길어져 보안성은 떨어지지만 DRM의 적용이 기존시스템에 미치는 영향은 그만큼 적어진다. 서버에 DRM을 적용한 암호화된 문서가 존재할 때 기존 시스템에 미치는 문제를 고려하여야 한다. 예를 들어 문서의 검색을 위하여 본문 내용에 대하여 자동 인덱싱을 할 경우 언패키징을 했다가 다시 패키징을 해야 하는 번거로움이 있을 수 있다.

위에서 살펴 본 문서 별 보안 설정 방법, 사용자 인증 방법, 패키징 시점에 관한 정책을 결정한 예를 살펴보자. 표 2는 KMS(Key Management Server)와 file-server에 DRM을 적용하기 위한 보안 정책의 실례이다. 예에서 볼 수 있듯이 서로 다른 시스템에서는 다른 보안 정책을 유지 하는 것이 합리적이다. 한 가지 보안 정책으로 모든 것을 처리하기에는 무리이다. 어떤 경우에 서로 다른 보안 정책을 유지하는 것이 적절한지, 서로 다른 보안 정책을 유지하면 전체적으로 문제가 없는지 등, 보안 정책 수립 방안에 대한 연구가 필요하다.

표 2 보안 정책 실례

	인증	패키징 시점	설정 설정
KMS	KMS의 인증	KMS에서 문서를 다운로드 할 때 서버에서	관리자에 의한 ACL 자동연동
File-server	Windows log on	File-server에 업로드 시 서버에서	File-server의 ACL에 따라 자동 설정, 폴더 관리자가 변경 가능

4. Document Security Domain(DSD)

본 논문에서는 기업의 문서 보안 문제를 여러 개의 DSD로 나누어 접근하는 방안을 제시한다. DSD로 나누게 되면 각 DSD 별로 일관 된 보안 정책을 정할 수 있고 이에 가장 적합한 DRM 시스템의 구축도 용이하게 된다.

4.1 DSD의 정의

DSD는 "문서 보안 정책과 시스템이 일관되게 유지될 수 있는 범위" 라고 정의 할 수 있다. DSD는 다음과 같은 특성을 갖는다.

- 한 문서는 한 DSD에 속한다. 복수의 DSD에 속한다면 보안 정책의 혼선이 생길 것이고 어디에도 속하지 않으면 보안의 공백이 생긴 것이다.
- 한 DSD에서는 동일한 사용자 인증 방법을 사용하여야 한다.
- 한 DSD는 동일한 보안 관리자가 관리하여야 한다.
- 문서는 다른 DSD로 이관될 수 있다. 이 경우 문서 이관 정책이 분명하여야 하며, 문서의 재패키징이 필요하다.

DSD 개념을 기업 문서 보안에 적용하여 보면 다음과 같은 유형의 DSD로 구분 될 수 있으며 그 대상 문서들은 다음과 같다.

- Server DSD: 특정 서버에서 관리하고 있는 문서

- Ad-hoc DSD: 불특정 다수에게 전달되는 문서
- PC DSD: 특정 서버에서 관리하지 않는 PC에 있는 문서
- File-server DSD: file-server에 있는 문서

4.2 Server DSD

기업의 기간 시스템들인 KMS, EDMS, ERP, PDM 등에 저장된 문서들을 그 대상으로 한다. ACL이 잘 정비되어 있어도 문서들이 사용자 PC로 다운로드 된 후에 ACL 범위를 벗어나도 통제할 수단이 없다. DRM의 적용이 시급히 고려되어야 하는 영역이다.

기존 시스템의 인증 시스템과 연동이 필요하며 보안 정책도 ACL과 연동하는 것이 필요하다. 패키징은 사용자들이 문서를 PC로 다운로드 받을 때 서버에서 하는 것이 기존 시스템에 영향을 덜 주고 간편하다. 다만 다운로드 시 패키징으로 인한 성능 저하가 문제가 되지 않도록 주의 할 필요가 있다. 각 응용 시스템 별로 별도의 DSD로 구분하여도 되고 만약 사용자 인증 방식, 관리자, 사용자 그룹이 같다면 같은 DSD로 통합하는 것도 적극 고려할 수 있다.

4.3 Ad-hoc DSD

기업의 업무 목적 상 문서는 기업 외부로 전달 될 필요가 있으며 주로 이메일을 통하여 전달되고 있지만, 메신저, ftp, Web disk 등을 통하여 전달되기도 한다. 이 경우 문서가 전달 된 후에 받은 사람이 문서의 관리를 어떻게 할지는 전적으로 받은 사람의 선택이다. 이것은 보안상 매우 부적절하며 보내는 사람이 좀 더 명확히 보내는 문서의 활용 범위를 설정할 수 있는 방법이 있어야 한다. DRM의 적용이 적극적으로 고려되어야 하는 이유이다.

이 경우 제일 큰 문제는 어떻게 외부 사람을 인증할 수 있는 방법이 있느냐 하는 것이다. 그 범위를 미리 한정할 수 없는 ad-hoc 사용자 그룹을 대상으로 하는 인증 방법이 필요하다. 특정 응용에서는 3.2절에서 설명한 여러 방법들이 쓰일 수 있으나 장기적으로 보면 외부인 인증은 기업의 중요한 IT 기반이므로 확장성이 좋은 인증 방식을 사용하는 것이 바람직하다. 외부의 인증 서버를 쓰지 않고 기업에서 직접 인증 서버를 운영할 경우에는 인증 서버를 DMZ 지역에 두어야 한다.

Ad-hoc DSD에서 보안의 설정은 보내는 사람이 할 수 있도록 하는 것이 일반적이다. 패키징 시점은 보내기 전 사용자 PC에서, 하는 것이 보안성이나 성능 면에서 유리하다. 만약 회사의 문서 전달이 특정 서버를 통하여 이루어진다면 해당 서버에서 업로드 되는 순간 패키징 할 수도 있다. 대부분 문서는 외부로 전달되기 전 다른 DSD에서 Ad-hoc DSD로 넘어가게 되므로 다른 DSD에서 Ad-hoc DSD로 문서가 이관 되는 절차나 정책에 대하여서는 필수적으로 고려되어야 한다.

4.4 PC DSD

PC에는 서버에 아직 등록 전인 작성 중인 문서도 있고, 완성된 문서라도 특정 서버에 등록될 계획이 없는 중요한 문서도 있다. 이런 문서들이 서버에 있는 문서들 보다 상대적으로 접근이 쉬우므로 해커의 표적이 될 수도 있다. PC를 잃어 버렸을 경우에 대비할 필요도 있다. 물론 사용자 자신에 의한 부주의나 고의성 유출에도 대비하여야 한다. 또한 한 PC를 여러 사람 공유하는 경우도 있다. 그런 경우에 한 PC에 여러 다른 사용자가 작성한 문서가 공존할 수 있으며 이 경우 보안에 특별히 주의가 필요하다. PC DSD도 여러 위험을 내포하고 있음을 알 수 있다.

PC DSD에서 사용자 인증 방식은 회사의 SSO가 있다면 SSO를 우선 고려하여야 할 것이고 그렇지 않다면 Windows log-on, 혹은 PC 보안이 적용되어 있다면 PC 보안 시스템의 인증과 연동을 고려하여야 한다. PC DSD의 경우 문서는 생성과 동시에 암호화 할 필요가 있으며 이때 보안 설정은 관리자가 정한 기본값으로 설정되고 후에 사용자가 변경할 수 있도록 하는 것이 일반적이다. 모든 파일을 생성과 동시에 암호화 할 필요는 없으며 그 범위를 정하는 것도 필요하다.

4.5 File-server DSD

기업에서 문서를 보관하고 공유하기 위한 가장 간단한 시스템이 file-server이다. 사용도 간편하고 관리도 쉽기 때문이다. 많은 기업들이 체계적인 관리를 하고 있지 않으며 그 결과 문서 유출의 흔한 근원지이기도 하다.

여기에 DRM을 적용하기 위해서는 우선 사용자 인증은 file-server의 인증과 연동할 필요가 있다. File-server는 폴더 별로 사용자의 접근 제어를 하고 있기 때문에 이 폴더 별 사용 권한과 DRM 권한과 연동하는 것이 필요하다. 패키징 시점은 사용자가 문서를 특정 폴더에 업로드하는 순간이 적절하다. 한번 패키징 된 문서는 해당 폴더의 문서 보안 설정을 지속적으로 따르도록 해야 한다. 만약 패키징 한 파일을 다른 폴더로 이동했을 때 자동으로 해당 폴더의 보안 설정으로 바뀌게 되면 쉽게 보안 허점이 생긴다.

위에서 살펴 본 것들이 일반적인 기업 환경에서 흔히 나오는 DSD 유형이다. 각 DSD 유형 별로 많이 선택할 수 있는 보안 정책을 정리하면 표 3과 같다.

표 3 전형적인 DSD

DSD	사용자 인증	패키징 시점	보안설정 방법
Server	기존 시스템 연동	다운로드 시	ACL에 의한 자동 설정
Ad-hoc	PKI 기반 인증, 이메일 기반 인증	보내기 전 PC에서	사용자 설정
PC	Windows log-on, SSO	문서 생성 시	관리자 설정, 사용자 변경
File-server	File-server 인증	해당 폴더로 이동 시	관리자 설정

4.6 DSD 간 문서 이관

이론적으로는 DSD 간 문서 이관은 해당 문서에 대한 권한의 범위가 이관 후의 것이 이관 전의 것의 부분집합일 때는 모두 허용할 수 있다. 즉 문서 권한이 이관하여 더 넓혀지지만 않으면 가능 한 것이다. 그러나 현실적으로는 문서가 이관된 후의 권한 허용 범위가 원래 것의 부분집합이 될 지 미리 알 수 없는 경우가 많다. DSD의 보안 정책에 따라 권한 허용 범위가 동적으로 변할 수도 있기 때문이다. 보안 정책이 정적이어서 미리 알 수 있다고 하더라도 그 범위 간의 관계를 파악하기는 기술적으로 어렵다. 현실적인 간편한 문서 이관 정책은 사용자가 원본 저장 권한이 있는 경우에만 허용하는 것이다. 원본 저장 권한을 가지고 있다는 것은 원본 문서를 추출한 후 어떤 새로운 권한의 부여도 가능하기 때문이다.

DSD 간 문서 이관은 기술적으로는 문서의 원본 추출 후 재패키징을 의미한다. 문서의 유통 과정을 고려하여 보면 그림 1과 같은 경우의 문서 이관이 가장 일반적으로 빈번하게 일어난다. 사용자의 편의를 위하여 이와 같이 빈번히 일어나는 DSD간 문서 이관을 자동화 하는 방안을 고려 해 볼 필요가 있다. 이 경우에도 사용자가 해당 문서에 대하여 원본 저장 권한이 있는지를 확인하는 것은 필수적이다. 사용자가 수동으로 원본 추출을 하고 그 원본을 다른 DSD로 넘긴 경우 원본

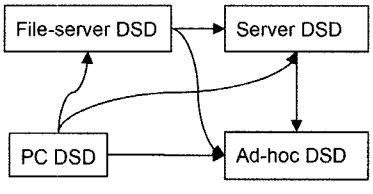

그림 1 자주 발생하는 DSD 간 문서 이관

추출 이력이 남게 되는데 자동 이관을 하게 되는 경우에도 사용자가 원본 추출을 하였다는 이력을 남기도록 하는 것이 바람직하다.

4.7 DSD의 공존

한 PC에는 여러 DSD에 속하는 문서들이 공존할 수 있다. ERP에서 내려 받은 문서, 작성 중인 보고서, 결재 중인 문서 등 여러 다른 DSD에 속한 문서들이 공존할 수 있다.

DSD 별로 다른 DRM 솔루션을 사용한다면 이로 인한 문제가 발생할 수 있다. 그렇다고 PC의 문서를 모두 PC DSD에 속하도록 하는 것은 일견 문제를 간단하게 할 수 있는 방법으로 보이지만 다음과 같은 보안상 중대한 결함을 갖게 된다.

예를 들어 PC DSD의 보안 정책은 DRM이 적용되는 순간 자동으로 결정되며 그 때 보안 설정은 같은 팀 내의 모든 사용자에게 모든 권한을 부여하기로 한다. 그런데 KMS에서의 보안 정책은 각 화면 별로 다른 보안 정책을 가지고 있다. 팀장인 사용자가 KMS에서 팀장 이상 모든 권한이 부여된 문서를 자신의 PC로 다운로드하게 되는 경우 자동 이관을 하게 되면 자신도 모르는 사이 팀원 전원이 해당 문서에 대하여 모든 권한을 갖게 된다. 이는 보안상 큰 허점이다. 원본 저장 권한이 있는 사용자가 수동으로 문서를 이관 할 수 있음에도 불구하고, KMS에서 다운로드 받은 문서는 여전히 KMS의 보안 정책을 따르는 것이 바람직하다.

5. Enterprise DRM 구축 전략

DSD에 근간을 둔 Enterprise DRM 구축 절차는 다음과 같다.

1. 문서 유통 환경 분석: 문서가 유통되는 각 시스템의 사용 빈도, 문서의 종류, 파일 형식, 문서 저작 프로그램, 사용자 인증 방법, 사용자 수 등 문서의 유통 환경에 대한 전반적인 조사 분석을 한다.
2. DSD로 구분: 문서 유통 환경을 몇 개의 DSD로 구분하고 서로 통합할 수 있는 것은 없는지 검토한다.
3. DSD 별 문서 보안 정책 수립: 도출된 DSD별로 구체적인 보안 정책을 수립한다.
4. DSD간 문서 보안 우선순위 결정: DSD 별로 종합 위험도를 평가한다. 종합 위험도를 측정하는 데는 여러 가지 분석 기법을 활용할 수 있으나 사용자들의 경험에 의한 우선순위 판단도 효과적일 수 있다[8].
5. 우선순위에 따른 순차적 구현: 운영의 효율성과 시스템의 종합적인 성능을 고려하여 구현한다.

한 번에 기업의 모든 문서 보안 시스템을 구축하는 것 보다는, DSD로 영역을 구분하고 보안이 시급한 영

역부터 우선적으로 단계적 DRM 구축을 하는 것이 새로운 보안 기술의 적용에 따르는 구축 및 운영 시 발생할 수 있는 시행착오와 사용자의 거부감을 최소화 할 수 있는 효과적인 전략이다.

DRM은 간단히 인하우스 개발로 할 수 있는 기술은 아니기 때문에 DRM 솔루션을 도입하는 것이 바람직하다. 솔루션 선택의 기준은 필요한 보안 정책을 제대로 구현할 수 있느냐, 운영 단계에서 일상적 운영 관리 및 변화 관리의 편의성, 시스템의 통합 성능이 주요 결정 요인이어야 한다. 물론 솔루션의 보안성, 안정성, 솔루션 벤더의 기술 지원 능력, 가격 등도 종합적으로 고려되어야 함은 물론이다. Enterprise DRM 회사 중에는 위의 DSD 중 특정 DSD 용 제품만 공급하는 회사, 한 제품으로 여러 다른 DSD를 지원하려는 회사, DSD별로 별도의 제품을 가지고 있는 회사도 있다[9][10][11].

6. 결 론

DRM을 문서 보안에 적용하면서 기업의 문서 보안 정책은 결정할 요소가 많은 어려운 문제가 되었다. 본 논문에서는 이 문제를 여러 개의 DSD로 나누어 독립적으로 수행하는 것이 효과적임을 보여주었다. DSD는 Server, Ad-hoc, PC, File-server 등의 유형으로 나눌 수 있으며 각기 다른 보안 정책이 필요하다. Enterprise DRM 구축 시, 문서 유통 환경을 분석, DSD로 구분하고, 도출된 DSD간 우선순위를 정하여 단계적으로 접근하는 것이 바람직하다.

참고문헌

[1] B. Rosenblatt, B. Trippe and S. Mooney, Digital Rights Management: Business and Technology, John Wiley & Sons, 2001.

[2] 배민오, 조규곤, 디지털 콘텐츠 저작권 보호 기술 동향, 정보과학회지, 18(7), 통권 제 134호, 2000.

[3] JupiterResearch, Digital Rights Management for the Enterprise, Analysis Report, 2004.

[4] Fasoo.com, Implementing Enterprise DRM for PDM Systems, White Paper, 2004.

[5] B. Rosenblatt, Integrating DRM with Peer-to-Peer Networks, White Paper, 2003.

[6] http://www.wrapsody.co.kr

[7] S. Garfinkel, PGP: Pretty Good Privacy, O'Reilly & Associates, 1994.

[8] Fasoo.com, FCM ONE: 문서보안 컨설팅 방법론, 보고서, 2004.

[9] http://www.fasoo.com.

[10] http://www.authentica.com.

[11] http://www.sealedmedia.com.

조 규 곤

1981 서울대학교 전기공학(학사)
1983 서울대학교 전기공학(석사)
1983~1986 삼성전자 종합연구소
1992 Rutgers University 컴퓨터공학(박사)
1992~2000 삼성SDS 정보기술연구소
2000 현재 Fasoo.com 대표이사
관심분야 : DRM, Information Security, Software Architecture, Machine Learning, Computer Vision

E-mail : kcho@fasoo.com