기밀문서 유통체계 설계에 관한 탐색적 연구

A Exploratory Study of Confidential Document Circulation System Design

장항배*, 김흥국**

Hang-Bae Chang*, Heung-Gook Kim**

요 약

1991년 Davis 가 '정보기술수용모형(TAM, Technology Acceptance Model)'을 제시하여 조직의 정보통신기술 도입이 이것을 사용하는 사용자의 편이성과 기술 도입에 따른 업무의 효용성 및 효과의 정도에 따라 결정되어 진다는 정보화 추진의 이론적 배경을 제공한 이래로, 최근에는 인터넷, 전자우편, 전자문서교환, 그룹웨어 등의 급격한 기술 발전이 진행되면서 공공기관 및 일반 기업의 업무 조직에 많은 변화를 가져오고 있다. 하지만 정보기술의 순기능과 함께 정보기술의 발전은 업무 조직에게 다양한 혜택을 가져다주었으나, 치명적인 역기능도 부가적으로 발생하게 되었다. 통합적인 업무환경에 따라 비 권한자가 정보를 조회하거나 중요 정보의 전산화로 인해 정보관리가 한층 어려워졌으며, 통신 기술의 발달로 인하여 외부로부터의 해킹이나, 내부자에 의한 정보유출이 용이해졌다. 본 연구에서는 조직에서 취급하는 기밀문서의 전자적 처리를 위한 보안 규정과 지침개선안을 마련하여 기밀문서의 세부적 절차 및 구현 방법을 개발하고자 한다.

Abstract

Since, Davis(1991) has proposed the TAM(Technology Acceptance Model) through a literature review of informatization promotion, which insists that a user conveniency is judged by the degree of effectiveness caused by IT, the advancement of IT such as the Internet, e-mail, electronic data exchange, and groupware have brought into various changes in ordinary corporations and public institutions. However, with the right function, the advancement of IT has provided various benefits including additional reverse functions. Based on an integrated environment of business process, unauthorized user could access to information and a management of information becomes more difficult than before due to informatization of critical information. Furthermore, external hacking or information leakage by insider becomes easier owing to advancement in communication technology. This study has tried to develop a specified management procedure and implementation method for confidential documents.

Key words : Confidential Document, Circulation System, Security

I. 서 론

1-1 연구 목적

오늘날 전 세계는 문호개방과 함께 무한경쟁시대로 접어들면서 공공기관 및 일반기업의 지속적인 생존과 경쟁 우위를 확보하기 위한 정보기술의 역할이

* 대진대학교 경영학과 (Department of Business Administration, Daejin University)
** 대진대학교 경영학과 (Department of Business Administration, Daejin University)
· 제1저자 (First Author) : 장항배
· 투고일자 : 2011년 6월 8일
· 심사(수정)일자 : 2011년 6월 10일 (수정일자 : 2011년 6월 22일)
· 게재일자 : 2011년 6월 30일

그 어느 때 보다도 중요시되고 있다. 점차 확산되고 있는 이러한 정보화의 흐름은 기존 업무에 단순히 컴퓨터를 도입하던 초기수준의 전산화 단계를 지나서 이제는 개인 업무의 정보화는 물론, 조직의 모든 자원과 프로세스를 전사적으로 유지관리 및 개선하고, 전자거래를 통한 조직간 통합 및 동시공학을 가능하게하며, 자료를 수집 및 가공 처리하여 유의미한 정보를 생성하고, 이를 전달하고 활용하여 새로운 지식의 창출에 이르기까지 그 기능이 무제한적으로 확산되고 있다.

그러나 앞서 설명한 정보기술의 순기능과 함께 정보기술의 발전은 업무 조직에게 다양한 혜택을 가져다주었으나, 치명적인 역기능도 부가적으로 발생하게 되었다. 개인의 정보 및 사생활이 노출되어 악용되는 사례가 발생하고 있으며, 자유로운 통신의 비밀이 보장되지 않는 등 기본적인 인권 침해의 원인을 제공하고 있다. 또한 조직의 업무에 있어서도 통합적인 업무환경에 따라 비 권한자가 정보를 조회하거나 중요 정보의 전산화로 인해 정보관리가 한층 어려워졌으며, 통신 기술의 발달로 인하여 외부로부터의 해킹이나, 내부자에 의한 정보유출이 용이해졌다.

본 연구를 통하여 조직 내 전자결재체계가 일반문서 위주로 되어있어 기밀문서 처리가 체계적으로 정립하지 못하는 단점을 보완기위해서 조직의 기밀문서 처리 기능 구현 범위를 설정하고 기밀문서의 전자적 처리를 위한 보안 규정과 지침개선안을 마련하여 기밀문서의 세부적 절차 및 구현 방법을 개발하고자 한다.

Ⅱ. 관련연구

2-1 미국

2011년도 발표한 미국 Computer Emergency Response Team(CERT)의 보고서에 따르면, 전체응답기관 607개중 직원 수 5000명이상 기업 38% 직원 수 500명이하의 기업 37%가 내부자에 의한 정보유출을 경형한 것으로 나타났다.

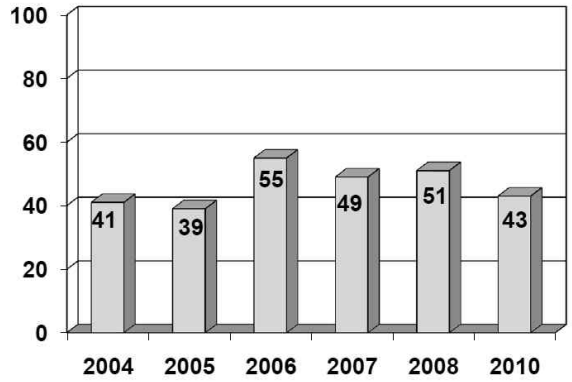


그림 1. 내부자 사고를 경험한 기업 비율
Fig. 1.Percentage of participants who experienced an insider incident

또한 내부자에 의한 범죄 조사결과 비 인가된 정보에 접근 및 사용이 63%로 가장 높았으며 그다음으로는 비의도적 개인 및 민감 정보가 노출이 57%로 그다음 순위를 차지하였다.

표 1. 내부자 범죄 유형
Table 1.Case of insider incident

정보 유출 유형	비 율
비인가된 정보에 접근 및 사용	63%
비의도적 개인 및 민감 정보가 노출	57%
바이러스, 웜 등 악성코드	37%
지적재산의 절도	32%

2-2 한국

기술집약적 산업 형태인 국내에서는 공공기관 및 일반기업의 내부자에 의한 정보유출은 매우 심각한 상태이다. 국정원 통계에 따르면 2006년에서 2010년까지 조직의 내부의 기밀정보가 내부자에 의해 유출된 비율이 전직직원 60% 및 현직직원의 비율을 합쳐 합계 77%로 많은 보안사고가 나타나고 있는 것으로 나타났다.

Ⅲ. 기밀문서 유통체계 설계

3-1 연구 범위

본 연구에서는 조직 내 전자결제시스템 분석하여 기밀문서 보안을 위한 정책 및 설계를 개발하고자 한다.

- 기밀문서의 전자적 처리를 위한 보안 규정 및 지침 개선 안 작성
- 기밀문서처리의 세부적 절차 및 구현 방법 설계

3-2 연구 방법

비밀정보 유통체계 개념 및 설계를 개발하기 위한 방법론으로는 향후 구축된 시스템과 소프트웨어 도입을 고려하여 이에 맞는 관리기법을 수행한다. 특히 소프트웨어 개발방법에 있어서 객체지향 소프트웨어 개발방법론을 적용한다. 그 이유는 본 방법론이 개발 절차 및 산출물 변형이 용이하며 다양한 자동화 도구와의 인터페이스가 가능하기 때문이며, 컴포넌트(component) 단위의 개발방법론이기 때문에 한번 개발한 소프트웨어는 객체 단위로 존재하여 다시 사용될 수 있는 형태로 존재하게 된다.

일반적으로 소프트웨어 개발 주기에서 노력의 분포는 개발노력의 절반을 개발자체에서 발생하는 오류를 해결하는데 소모하고, 전 개발 주기의 절반을 유지 보수하는 데에 투입되고 있다. 이는 구현하고자 하는 기능의 불명확성 등 시스템 분석과 설계의 미흡에 그 원인이 있다고 볼 수 있다. 따라서 이러한 불합리성을 해결하려면, 소프트웨어 품질향상과 소프트웨어의 개발주기의 전 과정에 걸쳐 사용자의요구사항을 명확히 분석하고, 비용과 일정 등에 관한 치밀한 계획을 수립하는 시스템 분석과 제약 환경 하에서 요구되는 기능을 효과적으로 구현할 수 있는 설계가 선행되어야 한다. 따라서 본 연구를 통하여 얻어진 결과물이 별다른 수정 없이 그대로 시스템 구축 및 소프트웨어 도입에 사용될 수 있도록 그림 2와 같은 일련의 작업 절차를 고려하여 연구를 진행한다.

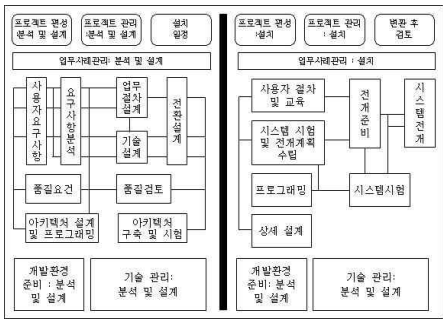


그림 2. 연구 수행 절차 경로
Fig. 2. Research Execution Procedures

3-3 기밀문서 처리 환경

기밀문서의 생성은 초기 작성자가 문서를 만든 다음 개인용 컴퓨터나 기타 저장장치에 저장하며, 작성된 문서는 필요에 따라 전자메일이나 출력을 통하여 내부자나 외부자에게 전달되게 된다. 최근에서는 정보공유시스템을 통하여 문서를 업로드(upload)하여 필요한 사람마다 자유롭게 다운로드(download)하여 사용하고 있다.

3-4 보호 위협 요소

정보공유시스템을 통한 기밀문서의 사용은 다음과 같은 보안 위협 요소를 내재하게 된다.

① 기밀문서의 부분별한 접근
② 기밀문서의 무분별한 전달 및 외부 유출
③ 기밀문서의 무단 변조 및 내용의 도용
④ 문서 저장 및 전달 수단의 다양화 및 편리화
⑤ 정보공유시스템 상의 기밀문서 관리의 취약성
⑥ 기밀문서 유출시 감사 및 사후처리 수단의 미비

3-5 보안 목적

앞서 살펴본 보안 위협 요소에 대응하기 위하여 다음과 같은 보안 목적을 설정한다.

① 기밀문서의 접근체계 적용
② 기밀문서의 유출경로 차단
③ 업무상 전자메일을 통하여 외부로 전달되는 기밀문서 보안

④ 정보공유시스템과 연동을 통한 공유 문서 보안
⑤ 기밀문서의 활용기록에 대한 감사

3-6 기본적인 시스템 보안 정책의 수립

기밀문서 보안 정책은 기밀문서의 생성, 사용, 처리, 관리를 위한 기본적인 보안의 방향을 전체적인 차원에서 명시하는 것이다. 보안 정책은 일반적인 사항을 추상적인 형태로 기술하여 시스템의 사양이 변하더라도 변함없이 적용될 수 있는 포괄적인 의미를 지닌 언어들로 구성된다.

① 문서의 실시간 암호화
② 문서의 권한 정책
③ 문서의 사용통제
④ 문서의 출력
⑤ 보안문서 외부 열람

3-7 세부적인 시스템 보안 정책의 수립

① 보안객체(Object): 접근의 대상이 되는 수동적 존재(문서, 개인용 컴퓨터PC).
② 보안주체(Subject): 보안객체에 접근하는 능동적인 존재(개인, 그룹).
③ 소유자(Owner): 보안객체를 소유하거나 생성하는 주체(개인, Service Linker를 호출하는 서버).
④ 능력 테이블(CT, Capability Table): 보안주체에 부여되는 권한(능력) 테이블
⑤ 접근제어 목록(ACL, Access Control List): 보안객체에 부여되는 보안주체 별 권한을 의미하며 임의적 접근제어 모델에서 소유자가 자신이 생성한 보안객체에 부여한다.
⑥ 접근제어모델

- 임의적 접근 제어(DAC, Discretionary Access Control)

사용자가 파일을 작성하면 그 사용자를 그 파일의 소유자라 한다. 임의적 접근 통제를 사용하는 시스템은 그 자원의 소유자로 하여금 특정 자원에 접근할 수 있는 주체를 결정할 수 있게 해 준다. 이 모델은 접근의 통제가 소유자의 재량에 근거하여 이루어지므로 임의적이라고 불리 운다. 가장 일반적인 구현방법은 접근제어목록을 통해서 이루어진다. 접근제어목록은 소유자에 의해서 지시되고 운영 시스템에 의하여 구동된다. 접근제어목록은 중앙 집중적으로 통제되는 환경에는 적합하지 않으며 강제적 접근 통제의 고정적인 역할에 비하여 정보에 접근하는 사용자의 권한을 보다 유동적으로 만들어 준다.

- 강제적 접근 제어(MAC, Mandatory Access Control, MAC)

강제적 접근 제어 모델에서 사용자들과 데이터의 소유자들은 사실상 그들의 파일들에 접근할 수 있는 사람들을 결정할 수 있는 권한을 갖지 못한다. 데이터 소유자는 다른 사람들이 자신의 파일들에 접근하도록 허용할 수는 있지만, 운영 시스템이 최종 결정을 내리고 데이터 소유자의 설정을 무효로 만들 수 있다. 이 모델은 보다 체계적이고 엄격한 보안 레이블 시스템(Security Label System)에 의해 이루어진다. 사용자는 비밀 취급허가(비밀, 최고 기밀, 대외비 및 기타)를 부여 받고 데이터도 그에 따라 분류된다. 그 분류는 자원의 보안 레이블에 저장되며 사용자가 파일에 접근할 수 있는 신뢰의 수준을 결정한다.

⑦ 보안 레이블(Security Label)

보안주체별 분류(classification)와 보안객체별 범주(category)에 대하여 그 권한을 정의한 각 항목을 의미한다. 강제적 접근 제어 모델에서 사용되며 관리자가 관리자 프로그램을 통하여 정의한다.

⑧ 권한의 내용

- 문서보안: 읽기, 편집, 해제, 반출, 출력, 유효기간, 자동파기, 권한 변경
- 개인용 컴퓨터 보안: 플로피, 이동 저장장치, CD-ROM, 프린터, 모뎀, 통신

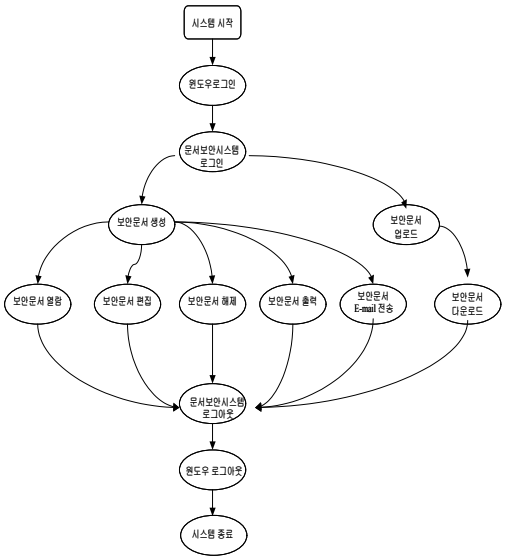


그림 3. 기밀문서 보안 흐름도
Fig. 3. Confidential Document Security Flowchart

3-8 기밀문서보안 기능 명세

기밀문서 보안을 위한 시스템은 내부 정보공유시스템에 축적되어있는 핵심정보를 보호하고, 송신하고자 하는 기밀정보를 안전하게 외부로 반출할 뿐만 아니라, 무분별한 불법유출을 방지하는 기능을 수행한다. 즉, 조직 내 기밀문서의 생성과 보관, 내부유통 및 외부반출의 전체적인 흐름을 통합적인 보안 정책을 통해서 체계적으로 관리할 수 있도록 지원하는 기능이다.

① 문서보안의 정책 관리

문서보안 정책관리서버는 다양한 조직의 전산 업무 환경에 적합하나 보안 정책을 수립, 관리하는 기능을 제공한다. 조직의 특성에 따라 다양한 보안 수준과 정책을 수행할 수 있으며, 디지털자료저작권관리(DRM, Digital Right Management)와 같은 단순한 규칙에서부터 다중등급보안(Multilevel Security)정책까지 지원함으로써 직책과 직무에 따라 보안 정책이 엄격히 요구되는 조직의 요구까지 모두 지원이 가능해야 한다.

② 인증 및 키 관리 체계

인증 및 키 관리 서버는 다양한 방법의 사용자 인증 및 사용자별 문서 보안 키 관리를 수행한다. 사용자 인증을 위해서 기존 인사관리 데이터베이스와 연동함으로써, 잦은 인사인동에 따른 사용자 및 부서 정보를 자동으로 유지하고 고객의 요구에 따라 다양한 인증 장치를 통하여 인증을 수행한다. 키의 안전한 관리를 위하여 'Pseudo Random Number Generator'로 키를 생성하고 'SSL(Secure Socket Layer)' 통신을 이용하여 키를 클라이언트(일반 개인용 컴퓨터)에 안전하게 전송하고 클라이언트 프로그램(client agent)에서는 시스템 메모리 영역에 키를 저장하여 키의 유출을 원천적으로 방지하게 된다.

③ 서버연동방안

기밀문서 보안은 기본적으로 지금 현재 구축되어 있는 각종 문서관련 서버와 연동이 되어야 한다. 조직내에 문서처리와 관련한 지식경영시스템(KMS), 전자문서처리시스템(EDMS), 그룹웨어 등과 유연하게 연결되어야하며, 기존 업무환경을 그대로 유지하는 것이 필수적이다. 기존 환경의 서버연동을 위한 서비스링커(Service Linker)는 현재 가장 먼저 구축되어있는 사무자동화시스템과 연동하여 보안 문서의 암호화 및 권한을 부여하는 기능을 제공한다. 향후 증가되는 다양한 서비스와 환경에 대해 최소한의 노력으로 유연한 연동을 보장하여야 하며, 완벽한 문서보안 기능을 구현하여야 한다.

④ 문서의 외부 유출 및 백업(backup) 방안

내부 문서보안 프로그램이 설치되어 있지 않은 수신자에게도 안전하게 문서를 보낼 수 있어야 하며, 이를 위하여 실행 파일 형태로 암호화된 문서와 인증 프로그램을 캡슐화(encapsulation)하여 전송한다.

또한 예측할 수 없는 재난과 장애에 대비하여 각각의 기능 서버는 이중화 구조(Active, Standby)에 의한 높은 가용성을 보장하도록 한다.

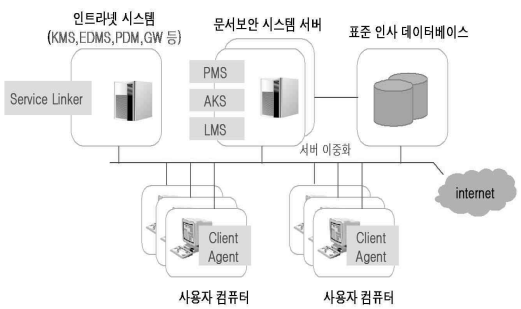


그림 4. 전체적인 기밀문서 보안 구성도
Fig. 4. Comprehensive Confidential Document Security Structure

⑤ 관리자 프로그램 기능 명세

표 2. 관리자 프로그램 기능
Table 2. Function of administrator program

기능 항목	내 용
정책 관리	보안정책
	로그정책
	감사정책
보안 감사	추적
	해독
	경고
로그 관리	보안 로그
	시스템 로그
	백업 로그
	로그 삭제
업그레이드 관리	서버 목록
	패치파일 업로드
관리자 관리	관리자 등록
	중간 관리자 권한 설정
환경 설정	서버 프로파일
	백업
통 계	통계 항목 추가/변경/삭제
기 타	관리자 로그 전송

⑥ 사용자 프로그램 기능 명세

표 3. 사용자 프로그램 기능
Table 3. Function of user program

기능 항목	내 용
설치	서버와의 통신 없이 설치
	보안 서약
삭제	삭제 허용/차단(사용자 프로파일)
로그인	최초 로그인 시 PC 등록
	PC의 IP/MAC 정보를 서버로 전송
	업그레이드 버전 확인 및 업그레이드
	서버와 PC 시간 정보 동기화
	오프라인 로그인 허용/차단(사용자 프로파일)
	다중 로그인 허용/차단(사용자 프로파일)
환경설정	서버 주소(IP, Port) 설정
	아이디/패스워드 저장 후 자동 로그인
	보안문서 생성 창이 나타나지 않도록 설정
사용자 정보	기본정보 및 사용자 프로파일
	문서 권한 / PC 권한
버전 정보	문서보안 버전 확인
사용자 권한 변경	소속 부서의 구성원들에 대한 권한 변경(사용자 프로파일)
문서보안	보안문서 열람 횟수 제한
	보안문서 생성(MAC/DAC/Hybrid)
	강제 암호화(사용자 프로파일)
	보안문서 편집(편집 시 정보 유출 방지)
	보안문서 해제
	보안문서 출력 시 프린트 마킹
	보안문서/일반문서 출력 시 페이지 단위 이미지/텍스트 추출
	보안문서 출력 횟수 제한
	보안문서/일반문서 반출(외부전송 파일 생성 및 권한 설정)
	보안문서 유효기간 설정
	보안문서 자동파기(읽기 횟수/프린트 횟수/유효기간)
	보안문서 권한 변경
	폴더 단위 암/복호화
개인용 컴퓨터 보안	플로피 제어
	이동 드라이브 제어
	CD-RW 제어
	프린터 제어
	모뎀 제어
	통신 제어(프로토콜, IP, Port 단위)
기 타	SSL/Non-SSL 옵션 설정(INI 수정 프로그램을 통하여)
	로그전송 옵션에 따른 선택적 로그 전송
	오프라인 사용 시 로그 저장
	오프라인 사용 시 서버 시간 유지
	업그레이드 시 다중 서버
	프로그램 강제 실행/종료 방지

⑦ 서버프로그램 기능 명세

표 4. 서버 프로그램 기능
Table 4. Function of server program

기능 항목	내 용
Fail Over	L4 Switch를 통한 Fail Over
모니터링	성능 및 시스템 로그 실시간 모니터링
DB 백업	파일 백업, 2차 저장소 백업
보안 통신	SSL / Non-SSL 통신 모두 가능

3-9 주요 정보 암호화 설계

① 주요 정보 암호화의 개념

- 모든 문서의 생성자는 그 문서의 소유주가 된다.
- 소유주는 법적 규제, 또는 회사의 정책 및 사업적 요구에 따라 보안문서를 생성하며 그 보안문서를 보호할 책임이 있다.
- 소유주는 보안문서 생성 시 접근 대상 및 접근 권한을 지정해야 한다.
- 소유주는 생성된 보안문서에 대해 책임이 있고 문서 유통 시 이를 직접 보호하거나 보안정책에 의해 보호되도록 해야 한다.

② 암호화 대상

표 5. 암호화 파일 형식 및 대상
Table 5. Objective and Format of Encrypted File

파일 형식	응용 프로그램
DOC	Microsoft Word
XLS	Microsoft Excel
PPT	Microsoft Power Point
MPP	Microsoft Project
HWP	한글
GUL	훈민정음
PDF	Adobe Acrobat
TXT	메모장, Word Pad
BMP, GIF, JPG, TIF	그림판

안전하게 외부로 반출할 뿐만 아니라, 무분별한 불법유출을 방지하는 기능을 수행한다. 즉, 조직 내 기밀문서의 생성과 보관, 내부유통 및 외부반출의 전체적인 흐름을 통합적인 보안 정책을 통해서 체계적으로 관리할 수 있도록 지원하는 기능이다.

③ 사용자 암호화

주요정보 암호화 시스템의 사용자 프로그램은 개인이 작성한 중요문서에 대하여 선택적 암호화를 수행할 수 있는 기능을 제공한다. 이 때 생성된 보안문서는 헤더에 정의된 접근 대상과 접근 권한 정보에 의해 열람 또는 편집, 해제, 파기가 허용된다. 또한 주요 기능으로는 보안문서 전자메일, 프로그램 업그레이드 기능 등이 있다.

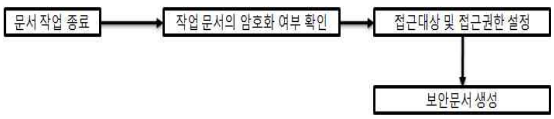


그림 5. 사용자 암호화 과정
Fig. 5. Function of User Program

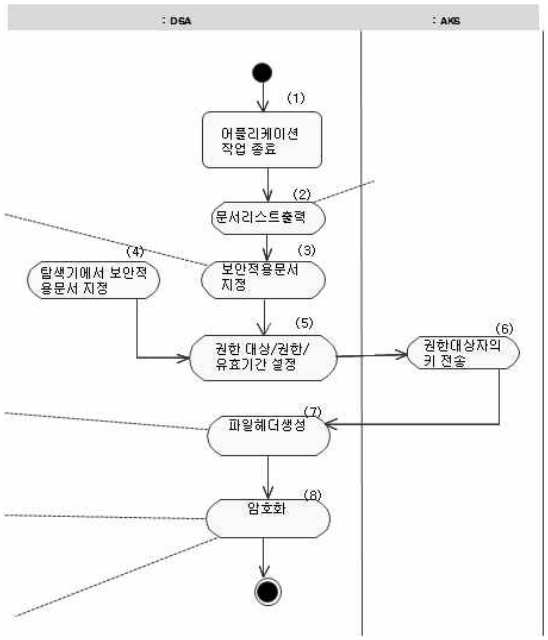


그림 6. 보안문서 생성 과정
Fig. 6. Security Document Generation Process

- 보안문서 생성 : 보안이 적용될 문서를 선택한 후 권한대상/권한/유효기간을 설정한다. AKS로부터 권한대상에 따른 암호화 키를 전송 받아 파일 헤더 정보를 생성한다. 키로 원본문서를 AES(Rijndael 알고리즘) 사용 암호화 한다. 생성된 암호화된 원본문서에 헤더를 부착하여 보안문서를 생성한다.

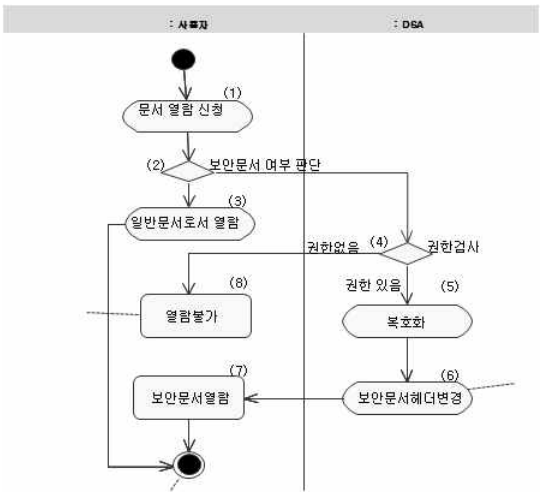


그림 7. 보안문서 열람 과정
Fig. 7. Security Document Access Process

- 보안문서 열람 : 보안문서 열람을 실행한다. 보안문서여부를 판단하여 보안문서가 아닌 경우 일반문

서로서 열람하고, 보안 문서인 경우 권한여부를 확인한다. 개인/그룹키를 이용하여 보안문서 암호키를 이용하여 암호화된 원본문서를 복호화 한다. 보안문서 헤더정보를 변경하고, 보안문서를 열람한다.

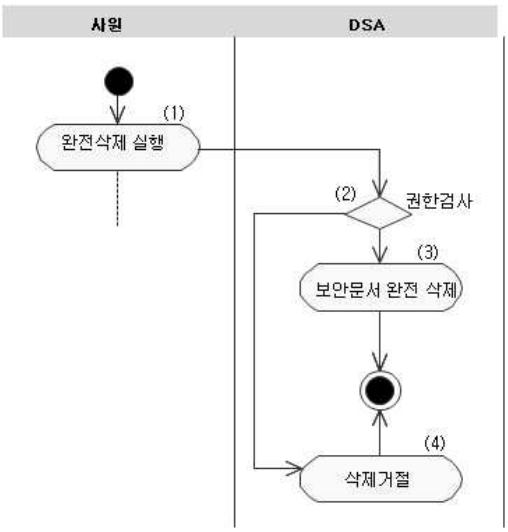


그림 8 보안문서 파기 과정
Fig. 8. Security Document Destruction Process

- 보안문서 파기 : 보안문서 파기를 실행하여 권한 여부를 확인한다. 해당문서에 대한 “열람권한”이 있는지 검사하여 권한이 없으면 삭제 거절하고, 권한이 있으면, 복구가 불가능하도록 원래 파일이 있던 자리에 복구 불가능하게 쓰레기 값을 채워 넣는다.

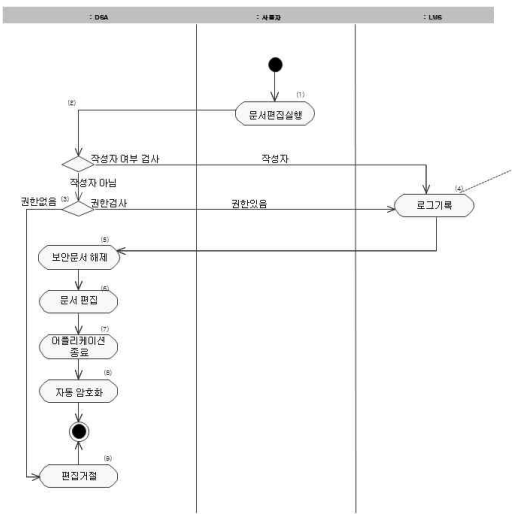


그림 9 보안문서 편집 과정
Fig. 9. Security Document Modify process

- 보안문서 편집 : 문서를 편집을 실행가호, 현재 사용자가 해당 보안문서의 작성자인지 검사한다. 복호화에 성공하면 권한검사의 접근권한부분과 기한부분과 관계없이 편집을 실행 할 수 있다. 작성자가 아니면 대상 문서에 대한 “편집권한”이 있는가 검사한다. 권한이 없으면 편집이 거절된다. 단, 보안문서의 작성자인 경우 위/변조부분만 검사한다. LMS에 로그기록을 남긴다. 보안해제 한다. 개인/그룹키를 이용하여 대상문서를 복호화 한다. 편집을 위한 어플리케이션을 실행한다. 편집 종료 후 어플리케이션을 종료한다. 편집한 문서를 암호화 한다.

④ 그룹웨어 서버 암호화

- 그룹웨어에 저장된 문서(첨부 파일)는 암호화 되어 보호된다.
- 그룹웨어에 저장된 보안문서의 접근 대상은 회사의 모든 개인이며 접근 권한은 열람(Read)이다.
- 그룹웨어로부터 전송 받은 보안문서를 직접 열람할 경우 편집이 불가능하다.
- 그룹웨어로부터 전송 받은 보안문서에 대하여 편집을 원할 경우 마우스 오른쪽 버튼의 "보안문서 편집" 메뉴를 실행하며 이 때 주요정보 암호화 로그 서버에 그 내역이 기록된다.
- 그룹웨어로부터 전송 받은 보안문서가 회사 외부로 유출 될 경우 열람이 불가능 하며 최초 작성자, 최근 열람자, 원본 파일명, 생성 시간 등의 정보를 분석하여 유출 경로를 추적할 수 있다.

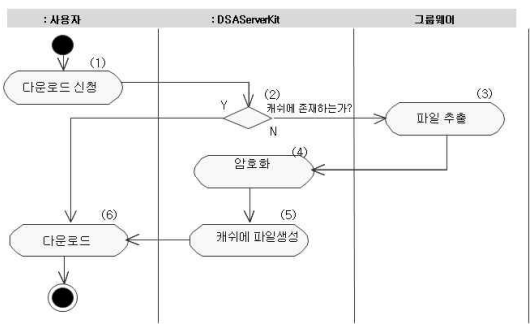


그림 10. 다운로드 파일 암호화 과정
Fig. 10. Download File Encryption Process

- 다운로드 파일 암호화 : 브라우저에서 다운로드 선택한다. 캐쉬에 해당파일이 존재 하는가 검사한다.

존재하면 해당 파일의 URL정보를 클라이언트에게 넘긴다. 캐쉬에 존재하지 않으면 그룹웨어DB에서 해당 파일을 추출한 후 Extract폴더에 저장한다. 저장도니 파일을 모든 사내 직원이 접근할 수 있는 전체키로 " 편집 해제 허용" 권한으로 암호화한다. 캐쉬에 파일을 생성한다. 파일을 생성한 후 URL정보를 클라이언트에게 넘긴다. 향후 동일한 파일을 다시 다운로드 받을 때 속도의 향상을 기대할 수 있다. DSA Server Kit로부터 받은 URL 정보로 다운로드 받는다.

Ⅳ. 결 론

본 연구에서는 조직에서 취급하는 기밀문서의 전자적 처리를 위한 보안 규정과 지침개선안을 마련하여 기밀문서의 세부적 절차 및 구현 방법을 개발하였다. 본 연구를 통하여 기술적 측면에서는 한정된 자원에서 조직 내부 정보를 용이하게 볼 수 있는 기술 개발 기반 구축하였으며 디지털저작권 보안을 기술의 고도화 설계 및 기밀문서 보안 인증 기술의 표준 확립하였다는데 의의가 있다. 또한 일반 기업의 전자상거래 사이트 개발에 필요한 응용 기술 이전 기회 마련 및 이동 컴퓨터 업무환경에 적합한 기밀문서보안을 위한 기반 기술 제공 가능하게 되었다. 업무적 측면에서는 전자 문서의 보안 및 보호 강화, 조직 내에 전자결재체계의 기밀문서처리 기능 개발 시 직접 참조가능, 사용자 편리성 제고 및 보안성 유지를 동시에 고려한 기밀문서 유통체계 개발 방향 제시, 중요도 높은 기밀문서의 전산화 촉진 가능하게 만들었다. 경제 및 산업적 측면에서는 우수한 정보 보안 전문 인력 창출이 가능하게 되었으며, 조직 경쟁력 강화 및 정보화 강국으로의 국가 이미지 상승이 기대된다.

감사의 글

이 논문은 2011년도 대진대학교 학술연구비 지원에 의한 것임

참 고 문 헌

[1] Arzi. Z., "Integrating a Key Cryptosystem into the Digital Signature Standard", *Electronic Letters,* Vol. 29, 1994.

[2] Farley, M., T. Stearns, and J. Hsu, Data Integrity and Security, *Triangle*, 1997.

[3] Garfingel, S., Spafford, G., Practical Unix and Internet Security, 2nd Ed., *Initech*, 1996.

[4] Whilliam, S., Internet Securities, B&C Press, 1995.

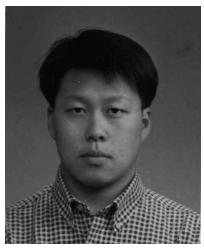
[5] Howard JD. "An Analysis of Security Incidents on the Internet", *Ph. D Thesis, Carnegie Mellon University*, 1997.

[6] Jan-Martin Lowendahl, "Case Study: How to Use a Security Incident to Your Advantage (Lesions Learned at Goteborg University)", *Gartner Industry Research*, 2007

[7] Kristen Noakers-Fry, Richard Hunter, "Case Study: Information Security Governance at TeliaSonera", *Gartner Research,* 2006.

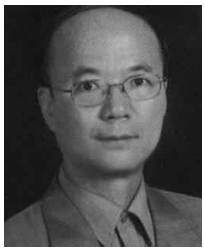
[8] Mark Nicolett, Jeffrey Wheatman, "DAM Technology Provides Monitoring and Analytics With Less Overhead", *Gartner Research*, 2007.

장 항 배 (洪吉憧)



2006년 : 연세대학교 정보시스템 관리전공(정보시스템 박사)
2007년~현재 : 대진대학교 경영학과 교수
관심분야 : 정보화 수준평가, 정보보호, 유비쿼터스 컴퓨팅

김 흥 국 (金興國)



1988년 : University of Michigan(박사)
1993년~현재 : 대진대학교 경영학과 교수
관심분야 : 비즈니스 서비스 모델, 조직관리 전략, 인간과 컴퓨터 상호작용