

비밀문서관리시스템 요구사항 분석

이지영*, 박진섭*, 신영선*, 강성기*,
대전대학교 컴퓨터 공학과

The Analysis of the classified document management system requirements

Ji-Young Lee*, Jin-Sub Park*, Young-Sun Shin*, Sung-Gi Kang**,
Dept. of Computer Engineering, Daejeon University*,
Dept. of Internet, Hyecheon University*

요 약

본 논문에서는 비밀문서를 전자화하여 유통 시킬 수 있도록 하기 위해 현재일반문서관리시스템을 분석하여 문서의 기안단계, 송·수신단계, 결재단계, 문서의 보관/저장 단계, 열람단계, 심사단계, 발송단계, 파기단계 까지를 포함한 전 과정에 수반되는 위험요소가 무엇인지를 파악하고, 각각의 보안 위험요소가 도출되고 나면 그에 상응하는 적절한 보안대책을 마련하는 방식으로 접근하여 비밀문서관리체계의 안전한 구축을 위한 보안 가이드라인을 제시한다.

1. 서론

각 정부/공공기관 및 기업들에서 정보통신망을 이용한 문서정보 및 금융정보의 유통이 활발해짐에 따라 정부는 정보기술을 활용한 정부 업무의 재설계 및 국가 자원의 효율 극대화를 위하여 전자결재 및 전자 문서 유통 정책 사업을 추진하고 있다.

이러한 전자문서 유통이 추진되면서 처리시간의 단축 및 인건비 절감과 신속하고 정확한 자료의 수집 및 활용에 의한 의사 결정 지원, 행정 운영의 과학화, 행정 정보의 효율적인 관리를 통해 국민 편의 증진과 행정 능률 향상을 추진하고 있으나 현재의 문서유통 시스템이나 그룹웨어 시스템은 저장정보 및 유통정보의 위조, 변조, 도난, 유출 등의 문제와 시스템의 의도적 운영방해, 불법접근(물리적, 논리적)등의 치명적인 역기능이 부가적으로 발생하게 되었다. 더욱이 조직의 중요 정보를 담고 있는 비밀문서에 대한 정보보호 기술 개발 및 적용, 표준 정립에 대한 연구가 이루어지지 않아 비밀문서 유통에 대한 업무는 배제된 상황으로써 이러한 정보의 역기능을 억제하여 일반문서 뿐만 아니라 비밀문서의 유통까지 모든 문서에 전자화를 실현하기 위해서는 체계적인 보안 정책 수립이 필요하게 되었다.

즉, 본 논문에서는 이러한 보안의 문제점을 해소하

고 비밀문서를 전자화하여 유통 시킬 수 있도록 전 과정에 수반되는 위험요소가 무엇인지를 파악하여, 각각의 보안 위험요소가 도출되고 나면 그에 상응하는 적절한 보안대책을 마련한다. 본 논문의 구성은 다음과 같다. 2장에서는 그룹웨어의 문서관리 일반적 기능 및 연구배경을 제시하고 3장에서는 전자문서시스템을 분석하여 위험요소를 파악한 후 4장에서 그에 대한 대책을 제시한다. 마지막으로 5장의 결론에서는 현 논문에 중요성 및 활용방안을 제시한다.

2. 그룹웨어의 문서관리 일반 및 연구배경

그룹웨어란 구내 정보 통신망(LAN)등으로 연결된 컴퓨터로 공동의 업무를 수행하는 구성원들이 원활하게 정보를 공유하도록 하고, 신속하고 정확한 의사결정을 내릴 수 있도록 지원함으로써 공동으로 수행하는 업무의 생산성을 높이기 위한 집합 소프트웨어를 말한다. 그룹웨어의 기능은 다음과 같다.

1) 전자결재 및 유통 기능

전자결재 및 유통 기능은 그룹 내에서 신속한 의사 결정을 내릴 수 있도록 지원하는 역할을 하며, 이는 문서 작성·기안, 결재, 발송, 접수, 문서합관리, 환경 설정 등의 기능을 포함한다.

2) 전자우편 기능

사용자들 사이의 정보유통을 효율적으로 할 수 있도록 지원하는 기능이다.

3) 전자계시판 기능

시간에 관계없이 정보를 저장하고 검색할 수 있는 수단을 제공하여 정보를 공유하고 전달할 수 있도록 하는 기능이다.

4) 시스템 운영/관리기능

관리자가 전자문서시스템을 관리하는 데 공통적으로 필요한 기능으로서, 사용자·그룹 및 사용자현황관리, 시스템감시·제어, 문서수발관리, 감사 등의 기능을 포함한다.

5) 기타 선택기능

기본기능 이외에 작업 시에 보다 편리하고 효율적인 작업을 가능하게 하기 위한 보조 기능을 말한다.

◆ 일반문서관리시스템의 문제제시

일반문서관리시스템은 업무의 효율성과 편의성에 주요안점을 두고 개발되다 보니 기밀성 보장이 가장 우선되어야 할 비밀문서에 대해서는 위협사항이 존재한다. 그로인하여 관리소홀 및 실수, 접근통제의 허술, 통제 없이 무분별한 문서의 복사/삭제/수정 등을 통한 문서의 유출, 장비(저장매체, 프린트, 휴대장비)를 통한 유출, 사고발생 후 사후감사를 위한 로그기록의 관리 미비 등 일반문서관리시스템에서 제공하는 기능들 중에 문서의 유출 및 변조의 가능성을 발생시킬 수 있는 요인들이 존재한다. 즉, 이러한 일반문서관리시스템에서의 기능들 중 비밀문서를 관리하기 위하여 발생할 수 있는 위협을 분석하고 그에 대한 보안대책 및 추가사항을 제시하여 보안할 필요가 있다.

3. 전자문서관리시스템 위험분석

일반전자문서관리시스템에서 나타날 수 있는 위협요소는 다음과 같다.

1) 전자결재 기능

① 문서 작성·기안

- 비취급인가자에게 공개되었을 경우 그 비밀의 내용이 누설될 위험이 있다.
- 비밀문서일 경우 제목으로 인하여 내용이 누출될 수 있다.
- 기안 내용 작성 또는 변경 시 비밀내용을 다른 편집기에 복사해 놓은 후 유출 시키거나 삭제 또는 수정의 기능 등을 통하여 문서의 내용이 불법으로 변조되거나 훼손될 수 있다.
- 기안자가 악의적인 목적으로 문서를 인쇄하여 인쇄물을 통해 유출시킬 수 있다.
- 비밀문서는 비밀의 표지와 첨부물로 구성되어 되며 비밀내용은 첨부물에 수록 되어 첨부하게 됨으로 첨부물에 대한 관리

소홀로 인해 기안자 및 다른 비인가자에 의해서 비밀 내용이 유출될 수 있다.

-기안도중 임시 저장 되었을 경우 그 문서에 대해 접근하여 변조시키거나 이동식 저장 매체 등을 통하여 외부로 유출시킬 위험이 있다.

-패스워드 방법은 제 3자가 도청하거나 위장하기 쉬우며 사용자의 패스워드 관리의 번거로움과 잊었을 경우 문제가 된다.

-부가설명 및 요약문에 비밀내용이 수록될 수 있다.

-비밀문서는 기안문 앞에 보안 등급 및 보호기간 등을 적은 비밀문서 표지를 붙인다.

-비밀문서는 비밀의 복제·복사를 제한하고 배포선을 명확히 함으로써 비밀의 누출을 예방하기 위하여 사본의 일련번호인 사본번호를 부여한다.

-비밀문서는 정보 기록물관리법에 의하면 비밀기록물을 생산 시에는 그 원본에 비밀보호기간 및 보존기간을 함께 정하여 보존기간이 만료될 때까지 보존토록 되어 있으며 비밀기록물에 대한 기록물 분류기준표를 별도로 작성하여야 한다.

② 결재 및 분류, 편철

-결재선상에 있는 자의 전자이미지 서명을 다른 비인가자에 의해서 도용할 수 있다.

-결재자가 잠시 자리를 비웠을 경우 문서의 도난 및 변조될 수 있다.

-결재의견 첨부 내용에 비밀내용이 포함되는 내용이 있을 경우 암호화하거나 조회 권한 확인 절차가 필요하다.

-첨부물은 비밀내용이 포함된 것으로서 비인가자가 첨부물을 열람/인쇄/복사/삭제/수정을 통하여 비밀문서의 내용이 외부로 유출될 수 있다.

-비밀문서의 경우 비밀관리번호를 부여하여 관리한다.

-사후감사를 위하여 결재선상에 있는 결재자의 검토 시 수정/반려된 내용에 대한 정보 및 결재 시 수정된 내역에 대한 정보 및 이력 관리가 필요하다.

③ 문서 발송

-비밀이 발송하였을 경우 수신부서 또는 수신자가 수신 사실을 부인할 수 있다.

-잔여정보를 통한 외부 유출 및 관리상의 문제가 발생한다.

④ 문서의 접수

-비밀문서는 신속한 처리를 위하여 등급별로 분리 관리되어야 하며 등급에 따라 비밀문서를 취급할 수 있도록 문서 또한 등급별로 보관할 수 있는 기능이 필요하다.

-문서접수 시 문서의 내용이 변조될 수 있다.

2) 전자문서관리기능

① 전자문서관리

-기록물을 등록하는 기록물철 또한 등급별로 나누어 등급에

맞는 관리가 필요하다

-비밀문서를 열람할 경우 비밀문서의 내용이 외부로 유출될 수 있으며 권한이 부여된 사용자(내부자)가 의도적으로 문서를 유출 시킬 수 있다.

-인쇄/저장 기능을 통해 외부로 유출될 위험이 있다.

3) 전자우편 기능

① 전자우편 작성

-본문내용에 비밀내용을 수록하게 되면 내용의 유출되기 쉽다.

-첨부파일은 비밀내용이 수록되는 것으로써 비인가자의 접근 및 유실 될 경우를 대비해야 한다.

② 전자우편 송·수신

-송·수신하는 도중 통신망 사이에서의 거래 자료 유실 및 위조·변조될 위험이 있다.

-운영상의 실수 및 장비의 장애 등으로 인한 거래 자료의 전송 지연 및 우편함에서의 메시지 인출 지연으로 비밀내용 유출 및 변조 될 수 있다.

-메시지를 송·수신하는 당사자들 간에 메시지의 송·수신 사실을 부인할 수 있다.

4) 사용자 운영·관리기능

① 시스템 감시 및 제어

-문서의 중요도에 따라 보안등급을 부여하여 사용자를 구분하여 접근권한을 제한할 수 있어야 한다.

② 정보 관리 기능

-비밀내용 정보의 등록은 그에 권한이 주어진 자만이 가능해야 한다.

-비밀문서의 경우 해당 정보를 등록한 사람이라도 정보가 비밀내용으로 판정된 이상 비밀내용을 임의로 삭제되어서는 안 된다.

4. 비밀문서 관리를 위한 보안 요구사항

앞에서 살펴본 위험분석을 통한 보안요구사항을 다음과 같이 제시한다.

1) 전자결재 기능

분류	기능	
문서작성·기안	서식풀러요기	등급별로 지정서식을 풀러오는 기능
	구분표시	공개구분을 '비공개'로 기본 지정
	제목작성	제목을 '가제'로 입력
	본문작성문서 인쇄	기안문의 새로 작성 시 복사기능 제한, 기존 문서의 경우 수정, 삭제, 복사의 기능 제한하며 복사, 수정, 삭제의 경우 모든 로그를 기록하는 기능
문서인쇄	인쇄 기능을 제한	
	출력이 필요할 경우 인쇄자, 인쇄일, 인쇄 사유 등의 로그 기록	
문서첨부	첨부물 지정 시 미리 지정된 비밀디렉토리에 저장된 파일 여부 확인 및 재지정 기능	
	첨부물 선택 시 공개키 자동 지정 및 암호화	

	기안자 및 기안자의 결재선과 수신자 및 수신자의 결재선 또는 협조서명이 필요한 인원만 복호화
	첨부행위가 끝나면 하드디스크에 남아있는 해당비밀은 자동 소거
문서인쇄보관·호출	인쇄 저장할 경우에는 자동 암호화 하여 지정된 PC의 하드디스크 내에서만 가능
사용자인증	생체인식/지문인식/스마트카드 등의 방법으로 보다 강력한 보안 및 사용자 인증 가능
요약문첨부	요약문은 암호화하여 첨부
기안문 표시	기안문서에는 문서의 취급방법을 표시 하는 기능
	기안문 표시에는 비밀내용이 수록되어서는 안됨 표지는 암호화 하지 않음
비밀관리정보 추가기능	사본번호, 원본/사본 예고문 기록 기능
	예고문 도래 15일전 경고문을 제시
	기안문서에 비밀패포션을 포함한다.
직위에의한 결재표시	결재자가 결재 암호를 입력하거나 생체인식 시스템을 도입하여 결재선상에 있는 사람의 입증
	전자이미지 서명은 개인 PC에 저장 할 수 없음
	전자이미지 서명은 보안관리 서버에서 안전하게 관리하고 전송 시 암호화되어 전송
결재및분류·편철	문서회수 및 처리
	회수 및 반송 처리된 문서는 모든 곳에서 완전소거 되어야 하며 회수, 반송된 문서에 대해 기록
	결재문서 수정
	결재문서 수정 시 그에 해당하는 (등급)권한이 있는지의 재차 확인 절차가 필요하며 인증이 되었을 경우에는 수정에 대한 이력관리 수정 전 문서는 결재 문서 수정한 결재권자가 가지고 있는 것이 아니라 문서 보관 서버에 별도로 저장하여야 하며 수정본과 수정 후 문서를 함께 보관
의견첨부	암호화 후 첨부
결재의견 조회	인증 절차를 걸친 후 권한 부여에 따라 조회
첨부문서보기	열람만 가능해야 하며 저장 및 인쇄기능을 제한
	출력이 불가피한 경우에는 출력 시 출력근거(이유, 수신, 업무 참고 등)를 자동 기록
	첨부파일의 열람 가능 시간과 열람 횟수를 제한하며 열람 행위에 대해 로그 기록
관리번호	비밀 관리번호 부여 가능
이력관리	결재선상에 있는 결재자의 검토 및 결재 시 수정된 내용(수정 부서, 인쇄, 수정자 등)에 대한 정보 및 이력을 관리
문서발송	내용의 무결성
	메시지에 대해서 전자서명을 적용
	인증이 되지 못한 비밀자료는 기록에 남기고 즉시 확인하여 조치 기능
	모든 문서는 암호화 후 저장
	관인 및 서명
	결재자는 생체인식 시스템을 도입하여 인증 절차를 거쳐 서명 표시
비밀관리기록부	모든 비밀의 발송(회송, 이첩, 배부)은 발송용 비밀관리 기록부에 수발부서, 접수자 등 근거 자료를 남긴
전송 후 삭제	비밀자료를 송·수신한 경우에는 즉시 정상적으로 수신되었는가를 확인하고, 전송즉시 컴퓨터에 수록되었던 비밀자료는 삭제
예고문 표시	시행문 사본의 예고문을 표시
로그파일 기록	모든 전송내역(송·수신 일시, 송·수신자, 파일명, 파일 크기)을 로그 파일에 자동 기록
문서접수	도착알림
	알림 내용에는 비밀내용이 포함되어서는 안됨.
	접수문서 편철 기능
문서는 그 중요도에 따라 등급(권한)이 부여되어야 하며 접수 문서에 대해서도 그 등급(권한)에 따라 별도로 보관	
비밀문서 접수 시 접수자(소속/성명)의 정보를 자동표시 후 정보 발송	
접수문서 보호	접수문서의 본문 및 결문 내용 중 그 일부를 추출하거나 편집할 수 없도록 하는 기능
	접수 문서는 자동 암호화
	접수 문서의 접근 시 패스워드 및 생체인식, 지문인식 등

	의 방법을 통하여 인증 모든 로그(접수문서 접근자, 접근일시, 작업의 종류, 이유 등)를 기록
--	---

2) 전자문서 관리기능

분류	기능
대 중	
등록정보입력	등급별로 나누어 기록물을 기록물철 등록대장에 입력/지정
기록물등 록대장 관리 및 수정	기록물철 등록대장은 등급별로 분류하여 관리 열람 시 열람 횟수 및 열람 시간 등을 제한하고 열람에 대한 로그를 기록 출력/지장 기능은 제공하지 않으며 불가피하게 출력해야 할 경우에는 별도의 승인 절차를 통하여 출력에 대한 출력자, 출력일, 출력 사유, 출력문서 등의 로그를 기록
첨부문서 관리	첨부파일은 열람만 가능해야 하며 지장 및 인쇄기능을 제한 출력이 불가피한 경우에는 출력 시 출력근거(이유, 수신, 업무 참고 등)를 자동 기록하고 보존·관리
계시판	첨부파일의 열람 가능 시간과 열람 횟수를 제한 기능 제한
열람처리	인증절차를 거쳐야 하며 열람 시 열람 횟수 및 열람 시간 등을 제한하고 열람에 대한 로그를 기록 출력/지장 기능은 제공하지 않으며 불가피하게 출력해야 할 경우에는 별도의 승인 절차를 통하여 출력에 대한 출력자, 출력일, 출력 사유, 출력문서 등의 로그를 기록
기록물정 리기능	일반사용자는 임의변경을 불가능하도록 함
이관목록 작성 및 검색	인쇄 기능 제한 출력해야 할 경우에는 별도의 승인 절차를 통하여 출력에 대한 출력자, 출력일, 출력 사유, 출력내용 등의 로그를 기록
문서 PC 저장	이미지 서명 및 비밀공문서는 PC 저장 할 수 없음

3) 전자우편 기능

분류	기능
대 중	
우편작성	본문내용에는 기밀내용이 포함되어서는 안 되며 비 밀내용은 첨부파일을 통하여 수록
내용인쇄	인쇄 기능 제한
파일첨부	첨부파일은 암호화되어야 하며 열람 시 확인
전자우편 송·수신	비밀문서 파일 접근에 대비한 사용자별 비밀문서 파일에 대한 접근 권한 설정 전송내용은 모두 암호화 또는 PGP, PEM 사용하여 전송 전송내용 제한 및 승인절차 수행 전자우편의 수·발신자 신원, 발신 시간, 발신 위치 등의 정보를 로그 기록
접근제어	통신망에서 접속을 요구하는 모든 사용자에 대해 그 정당 성을 확인 후 접속을 허용 인증절차에 통과하지 못한 사용자가 있을 경우에는 즉시 이에 대한 확인 및 조치를 취함 수신 확인 시 스마트카드, 생체인식, 지문인식을 통한 방 법으로 확인 메시지의 수신 확인은 특정컴퓨터에서만 보안 전자메일을 볼 수 있도록 함 수신 메시지 인쇄 기능 제한 수신메시지 우편함 또는 파일로 저장 할 수 없도록 기능
장애복구	장애 발생시에 대비한 통신망 및 컴퓨터 장비에 대한 복 구 절차 및 장애 방지 조치
전자우편보안함	비밀문서 파일 접근에 대비한 사용자별 비밀문서저장 파 일에 대한 접근 권한 설정 통신망에서 접속을 요구하는 모든 사용자에 대해 그 정당 성을 확인 후 접속을 허용 인증절차에 통과하지 못한 사용자가 있을 경우에는 즉시 이에 대한 확인 및 조치를 취함

	스마트카드, 생체인식, 지문인식을 통한 방법으로 확인 직원의 우편함에 대한 접근 수준 및 방법의 규정 등에 관 한 공식적 절차를 마련하여 접근 통제 전송내용 제한 및 승인절차 수행
--	---

4) 사용자 운영·관리기능

분류	기능
대 중	
사용자 감시 및 제어	계층별 보안등급 별 또는 담당 업무별, 직급별 보안등급 을 부여하여 사용자들을 구분하여 접근권한을 제한 하도록 지정함
정보관리	정보의 등록 비밀문서의 경우 등록 절차를 밟음 정보의 삭제 정보관리자만이 해당 정보를 삭제함

5. 결론

일반전자문서유통 시스템에서의 보안위험요소를 분석한 결과 비밀문서의 접근 권한문제, 내부자에 의한 비밀문서의 유출 통제 문제, 비밀문서의 기록관리 및 사후감사 기능 등의 보안에 문제점이 있는 것으로 판단되었다. 이러한 문제점을 보완하기 위하여 비밀문서 유통 단계별/기능별로 보안대책으로써 강력한 인증방법, 암호화의 의무화, 내부자에 의한 유출을 막기 위한 방법, 비밀문서 사용에 대한 모든 로그 관리를 통한 사후 대책 등을 제시하였으며 이러한 보안대책을 보완함으로써 정보통신망을 이용한 전자비밀문서의 기간/결재/유통 과정에서 야기될 수 있는 정보의 변조, 위조, 도난, 누설 등의 제반 정보보호가 가능하여 보안체계를 강화할 수 있을 것으로 사료된다. 즉, 유통/보관 관리되는 정보의 대부분이 비밀사항인 국방 관련 조직 및 외교 문서 또는 개인 간·기업간의 비밀문서관리시스템의 설계 시 참고자료로 쓰일 수 있을 것으로 보인다.

[참고문헌]

- [1] 김경식, “보안통제를 고려한 전자결재 시스템 구현”, 석사학위논문, 고려대학교 경영정보대학원, 1997,
- [2] 김재향, “전자정부 문서 유통 표준을 지원하는 전자문서시스템 설계 및 구현에 관한 연구”, 석사학위 논문, 연세대학교 공학대학원, 2001
- [3] 김정희·김태운, “전자식 문서 교환(EDI)의 보안과 통제관리”, 「산업경제」 12, 경상대학교 경영경제연구소, 1991
- [4] 한국전산원, “공문서 전자 유통 방안”, 1996
- [5] 한국전산원, “그룹웨어 시스템 구성 연구”, 1997
- [6] 한국정보통신기술협회, “인터넷 구축 지침서”, 1998
- [7] 행정자치부, “행정기관의 전자문서시스템 규격”, 2002