(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년03월04일
(11) 등록번호 10-1599740
(24) 등록일자 2016년02월26일

(51) 국제특허분류(Int. Cl.)
*G06F 21/60* (2013.01) *G06F 21/30* (2013.01)
*G06F 21/62* (2013.01)
(21) 출원번호 10-2014-0090128
(22) 출원일자 2014년07월17일
심사청구일자 2014년07월17일
(65) 공개번호 10-2016-0009825
(43) 공개일자 2016년01월27일
(56) 선행기술조사문헌
KR101315482 B1*
KR1020060058427 A*
정재호, 지란지교소프트, 금융권-대기업용 '보안 파일전송결재 시스템' 제시, 이데일리, 2013.6.14.*
*는 심사관에 의하여 인용된 문헌
기술이전 희망 : **기술양도**, **실시권허여**, **기술지도**

(73) 특허권자
**한국전자통신연구원**
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
**김민식**
대전광역시 유성구 온천로 51, 사서함 1호
**류승진**
대전광역시 유성구 온천로 51, 사서함 1호
*(뒷면에 계속)*
(74) 대리인
**한양특허법인**

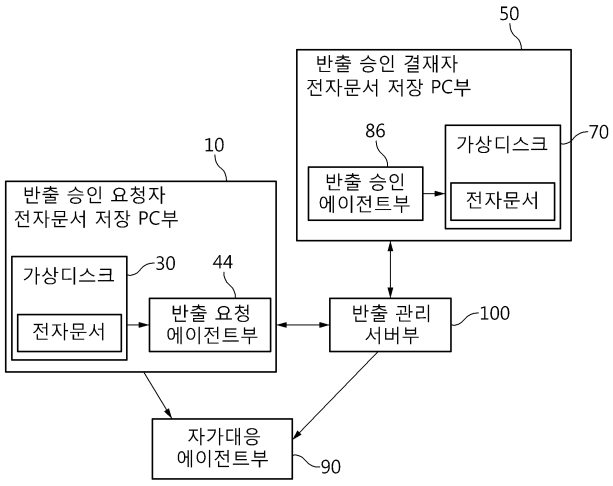
전체 청구항 수 : 총 12 항 심사관 : 서광훈

(54) 발명의 명칭 **전자문서 불법 유출 방지 방법 및 장치**

## (57) 요 약

불법 유출시 자가 대응할 수 있고 불법 유출 근원지를 추적할 수 있는 기능을, 보호하고자 하는 정보에 탑재하여 전자문서 불법 유출을 원천 차단할 수 있도록 하는 전자문서 불법 유출 방지 방법 및 장치를 제시한다. 제시된 장치는 통제대상이 되는 전자문서를 저장하기 위한 가상디스크를 생성하고 전자문서의 외부 반출을 통제하는 반출 통제부, 전자문서의 외부 반출이 합법한 반출인지를 인증하는 반출 관리 서버부, 및 반출 관리 서버부로부터 불법 반출을 알리는 결과를 수신하게 되면 자기소멸을 행하는 자가 대응 에이전트부를 포함한다.

*대 표 도* - 도3



(72) 발명자

**김기헌**

대전광역시 유성구 온천로 51, 사서함 1호

**윤한준**

대전광역시 유성구 온천로 51, 사서함 1호

**이도훈**

대전광역시 유성구 온천로 51, 사서함 1호

이 발명을 지원한 국가연구개발사업

| | |
|---|---|
| 과제고유번호 | 10048592 |
| 부처명 | 산업통상자원부 |
| 연구관리전문기관 | 한국산업기술평가관리원(KEIT) |
| 연구사업명 | 산업기술혁신사업 기술료지원사업 |
| 연구과제명 | 기술유출 방지를 위한 융복합 원천기술 연구개발 |
| 기 여 율 | 1/1 |
| 주관기관 | ETRI부설 국가보안기술연구소 |
| 연구기간 | 2014.05.01 ~ 2015.04.30 |

# 명 세 서

## 청구범위

### 청구항 1

통제대상이 되는 전자문서를 저장하기 위한 가상디스크를 생성하고, 상기 전자문서의 외부 반출을 통제하는 반출 통제부;

상기 전자문서의 정보, 상기 전자문서의 반출을 요청하는 단말기의 정보, 상기 전자문서의 반출을 승인하는 단말기의 정보, 상기 전자문서를 수신한 반출 대상의 정보 중에서 적어도 하나를 이용하여 상기 전자문서의 외부 반출이 합법한 반출인지를 인증하는 반출 관리 서버부; 및

상기 반출 관리 서버부로부터 불법 반출을 알리는 결과를 수신하게 되면 상기 전자문서를 삭제하여 자기소멸을 행하는 자가 대응 에이전트부;를 포함하며,

상기 반출 통제부는,

상기 외부 반출이 합법한 반출인 경우, 상기 전자문서를 수신한 상기 반출 대상이 가상디스크 상에서 상기 전자문서를 실행하도록 제어하고,

상기 자가 대응 에이전트부는 상기 반출 관리 서버부에서의 인증을 위해 단말의 호스트명, MAC 주소, IP 주소, 및 네트워크 정보 중에서 하나 이상을 포함하는 상기 반출 대상의 정보와 상기 전자문서를 상기 반출 관리 서버부에게 제공하는 것을 특징으로 하는 전자문서 불법 유출 방지 장치.

### 청구항 2

삭제

### 청구항 3

삭제

### 청구항 4

청구항 1에 있어서,

상기 반출 통제부는 반출 승인 요청자의 PC부 및 반출 승인 결재자의 PC부에 각각 포함되되,

상기 반출 승인 요청자의 PC부의 반출 통제부가 상기 전자문서의 외부 반출 요청 기안을 작성하여 상기 반출 관리 서버부를 통해 상기 반출 승인 결재자의 PC부에게로 전달하면 상기 반출 승인 결재자의 PC부의 반출 통제부는 상기 전자문서의 외부 반출을 승인하여 상기 반출 관리 서버부를 통해 상기 반출 승인 요청자의 PC부의 반출 통제부에게로 보내는 것을 특징으로 하는 전자문서 불법 유출 방지 장치.

### 청구항 5

청구항 4에 있어서,

상기 반출 승인 요청자의 PC부의 반출 통제부는,

상기 가상디스크를 생성하고 관리하는 가상디스크 생성 및 관리부; 및

상기 전자문서의 외부로의 반출을 요청하는 반출 요청 에이전트부;를 포함하는 것을 특징으로 하는 전자문서 불법 유출 방지 장치.

### 청구항 6

청구항 4에 있어서,

상기 반출 승인 결재자의 PC부의 반출 통제부는,

상기 가상디스크를 생성하고 관리하는 가상디스크 생성 및 관리부; 및

상기 전자문서의 외부로의 반출을 승인하는 반출 승인 에이전트부;를 포함하는 것을 특징으로 하는 전자문서 불법 유출 방지 장치.

**청구항 7**

청구항 1에 있어서,

상기 반출 통제부는 상기 전자문서의 해쉬 값, 상기 전자문서의 제목, 상기 전자문서의 수신자 단말기의 MAC, IP 주소 및 호스트명 정보, 기안자 또는 결재자의 정보를 이용하여 상기 전자문서의 외부 반출을 통제하는 것을 특징으로 하는 전자문서 불법 유출 방지 장치.

**청구항 8**

청구항 1에 있어서,

상기 반출 통제부는 상기 생성된 가상디스크의 영역에 접근할 수 있는 어플리케이션을 제한하고, 상기 가상디스크의 영역을 암호화하는 것을 특징으로 하는 전자문서 불법 유출 방지 장치.

**청구항 9**

청구항 1에 있어서,

상기 반출 관리 서버부는 미리 설정된 합법 반출 인증 요청 기간내에 상기 전자문서의 외부 반출이 합법한 반출인지를 인증하는 것을 특징으로 하는 전자문서 불법 유출 방지 장치.

**청구항 10**

반출 승인 요청자의 PC부 및 반출 승인 결재자의 PC부의 반출 통제부가, 통제대상이 되는 전자문서를 저장하기 위한 가상디스크를 각각 생성하고 관리하는 단계;

상기 반출 승인 요청자의 PC부 및 반출 승인 결재자의 PC부의 반출 통제부가, 반출 관리 서버부를 통해 상기 전자문서의 정보, 상기 전자문서의 반출을 요청하는 단말기의 정보, 상기 전자문서의 반출을 승인하는 단말기의 정보, 상기 전자문서를 수신한 반출 대상의 정보 중에서 적어도 하나를 이용하여 상기 전자문서의 외부 반출을 통제하는 단계;

상기 반출 관리 서버부가, 상기 전자문서의 외부 반출이 합법한 반출인지를 인증하는 단계; 및

자가 대응 에이전트부가, 상기 인증하는 단계에 의해 불법 반출을 알리는 결과를 수신함에 따라 상기 자가 대응 에이전트부에 포함된 상기 전자문서를 삭제하여 자기소멸을 행하는 단계;를 포함하며,

상기 외부 반출이 합법한 반출인 경우, 상기 전자문서를 수신한 상기 반출 대상이 가상디스크 상에서 상기 전자문서를 실행하도록 제어하는 단계를 더 포함하고,

상기 인증하는 단계는,

상기 전자문서를 수신한 단말의 호스트명, MAC 주소, IP 주소, 및 네트워크 정보 중에서 하나 이상을 포함하는 상기 반출 대상의 정보를 근거로 상기 전자문서의 외부 반출이 합법한 반출인지를 인증하는 것을 특징으로 하는 전자문서 불법 유출 방지 방법.

**청구항 11**

삭제

**청구항 12**

삭제

**청구항 13**

청구항 10에 있어서,

상기 전자문서의 외부 반출을 통제하는 단계는,

상기 반출 승인 요청자의 PC부의 반출 통제부가, 상기 전자문서의 외부 반출 요청 기안을 작성하여 상기 반출 관리 서버부를 통해 상기 반출 승인 결재자의 PC부에게로 전달하는 단계; 및

상기 반출 승인 결재자의 PC부의 반출 통제부가, 상기 전자문서의 외부 반출을 승인하여 상기 반출 관리 서버부를 통해 상기 반출 승인 요청자의 PC부의 반출 통제부에게로 보내는 단계;를 포함하는 것을 특징으로 하는 전자문서 불법 유출 방지 방법.

**청구항 14**

청구항 10에 있어서,

상기 전자문서의 외부 반출을 통제하는 단계는, 상기 전자문서의 해쉬 값, 상기 전자문서의 제목, 상기 전자문서의 수신자 단말기의 MAC, IP 주소 및 호스트명 정보, 기안자 또는 결재자의 정보를 이용하여 상기 전자문서의 외부 반출을 통제하는 것을 특징으로 하는 전자문서 불법 유출 방지 방법.

**청구항 15**

청구항 10에 있어서,

상기 가상디스크를 각각 생성하고 관리하는 단계는 상기 생성된 가상디스크의 영역에 접근할 수 있는 어플리케이션을 제한하고 상기 가상디스크의 영역을 암호화하는 것을 특징으로 하는 전자문서 불법 유출 방지 방법.

**청구항 16**

청구항 10에 있어서,

상기 전자문서의 외부 반출이 합법한 반출인지를 인증하는 단계는 미리 설정된 합법 반출 인증 요청 기간내에 상기 전자문서의 외부 반출이 합법한 반출인지를 인증하는 것을 특징으로 하는 전자문서 불법 유출 방지 방법.

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 전자문서 불법 유출 방지 방법 및 장치에 관한 것으로, 보다 상세하게는 외부로의 전자문서 유출시 인증과정을 통해 불법 유출 여부를 판단하여 전자문서 자가대응(자기소멸) 및 불법 유출 근원지 추적을 통해 전자문서 불법 유출을 방지하는 방법 및 장치에 관한 것이다.

### *배 경 기 술*

[0002] 기업들의 기술력이 높아지면서 첨단 산업기술의 유출사건이 지속적으로 증가하고 있다.

[0003] 기술유출은 지능화된 해킹기법 또는 기존에 구축된 보안체계의 허점을 지능적으로 악용하는 내부자에 의해 주로 발생한다. 이에 따라, 전자문서의 외부 유출을 방지하기 위한 기술이 필요하다.

[0004] 전자문서의 유출을 방지하기 위한 기존의 기술로는 DRM(Digital Rights Management), DLP(Data Loss Prevention) 등의 정보 보호 기술들이 제안 및 개발되어 운영되고 있다.

[0005] 그러나, 해킹 기법이 나날이 지능화되고 있고 내부자가 지능적으로 전자문서를 유출하고 있어서, 전자문서 유출에 완벽히 대응하기가 쉽지 않다.

[0006] 특히, 기존 방법들은 정보를 저장하고 있는 시스템을 위협으로부터 보호하는데 집중하거나 또는 보호하고자 하는 데이터를 단순 암호화하여 저장 및 관리하는 것이어서, 보호대상이 되는 전자문서의 유출시 완벽한 대응에 한계점을 갖는다.

[0007] 관련 선행기술로는, 2010년 4월에 한국인터넷정보학회 11권 2호에 개재된 "내부 사용자에 의한 불법 데이터 유출방지를 위한 안전한 지식관리 시스템"이라는 논문 내용이 있다. 그 논문 내용은 내부 사용자들에 대한 명시적 인증을 수행하고 이를 기반해 데이터를 제공하고 2MAC을 이용하여 악의적인 내부 사용자에 의한 불법적 데이터

유출을 방지한다.

[0008] 다른 관련 선행기술로는, 기밀문서 유출 방지 시스템에서 기계 학습(언어 기반) 및 핑거 프린팅(비언어 기반)을 이용하여 기밀문서의 유출을 방지하는 내용이, 대한민국공개특허 제2008-0029602호에 제시되었다.

## *발명의 내용*

### *해결하려는 과제*

[0009] 본 발명은 상기한 종래의 문제점을 해결하기 위해 제안된 것으로, 불법 유출시 자가 대응할 수 있고 불법 유출 근원지를 추적하여 전자문서 불법 유출을 원천 차단할 수 있도록 하는 전자문서 불법 유출 방지 방법 및 장치를 제공함에 그 목적이 있다.

### *과제의 해결 수단*

[0010] 상기와 같은 목적을 달성하기 위하여 본 발명의 바람직한 실시양태에 따른 전자문서 불법 유출 방지 장치는, 통제대상이 되는 전자문서를 저장하기 위한 가상디스크를 생성하고, 상기 전자문서의 외부 반출을 통제하는 반출 통제부; 상기 전자문서의 외부 반출이 합법한 반출인지를 인증하는 반출 관리 서버부; 및 상기 반출 관리 서버부로부터 불법 반출을 알리는 결과를 수신하게 되면 자기소멸을 행하는 자가 대응 에이전트부;를 포함한다.

[0011] 상기 자가 대응 에이전트부는 상기 반출 관리 서버부에서의 인증을 위해 반출 대상의 정보를 상기 반출 관리 서버부에게 제공할 수 있다.

[0012] 상기 반출 대상의 정보는 단말의 호스트명, MAC 주소, IP 주소, 및 네트워크 정보 중에서 하나 이상을 포함할 수 있다.

[0013] 상기 반출 통제부는 반출 승인 요청자의 PC부 및 반출 승인 결재자의 PC부에 각각 포함되되, 상기 반출 승인 요청자의 PC부의 반출 통제부가 상기 전자문서의 외부 반출 요청 기안을 작성하여 상기 반출 관리 서버부를 통해 상기 반출 승인 결재자의 PC부에게로 전달하면 상기 반출 승인 결재자의 PC부의 반출 통제부는 상기 전자문서의 외부 반출을 승인하여 상기 반출 관리 서버부를 통해 상기 반출 승인 요청자의 PC부의 반출 통제부에게로 보낼 수 있다.

[0014] 상기 반출 승인 요청자의 PC부의 반출 통제부는, 상기 가상디스크를 생성하고 관리하는 가상디스크 생성 및 관리부; 및 상기 전자문서의 외부로의 반출을 요청하는 반출 요청 에이전트부;를 포함할 수 있다.

[0015] 상기 반출 승인 결재자의 PC부의 반출 통제부는, 상기 가상디스크를 생성하고 관리하는 가상디스크 생성 및 관리부; 및 상기 전자문서의 외부로의 반출을 승인하는 반출 승인 에이전트부;를 포함할 수 있다.

[0016] 상기 반출 통제부는 상기 전자문서의 해쉬 값, 상기 전자문서의 제목, 상기 전자문서의 수신자 단말기의 MAC, IP 주소 및 호스트명 정보, 기안자 또는 결재자의 정보를 이용하여 상기 전자문서의 외부 반출을 통제할 수 있다.

[0017] 상기 반출 통제부는 상기 생성된 가상디스크의 영역에 접근할 수 있는 어플리케이션을 제한할 수 있고, 상기 전자문서를 상기 가상디스크에서 실행할 수 있도록 실행 통제할 수 있고, 상기 가상디스크의 영역을 암호화할 수 있다.

[0018] 상기 반출 관리 서버부는 미리 설정된 합법 반출 인증 요청 기간내에 상기 전자문서의 외부 반출이 합법한 반출인지를 인증할 수 있다.

[0019] 한편, 본 발명의 바람직한 실시양태에 따른 전자문서 불법 유출 방지 방법은, 반출 승인 요청자의 PC부 및 반출 승인 결재자의 PC부의 반출 통제부가, 통제대상이 되는 전자문서를 저장하기 위한 가상디스크를 각각 생성하고 관리하는 단계; 상기 반출 승인 요청자의 PC부 및 반출 승인 결재자의 PC부의 반출 통제부가, 반출 관리 서버부를 통해 상기 전자문서의 외부 반출을 통제하는 단계; 상기 반출 관리 서버부가, 상기 전자문서의 외부 반출이 합법한 반출인지를 인증하는 단계; 및 자가 대응 에이전트부가, 상기 인증하는 단계에 의해 불법 반출을 알리는 결과를 수신함에 따라 자기소멸을 행하는 단계;를 포함한다.

[0020] 상기 인증하는 단계는 반출 대상의 정보를 근거로 상기 전자문서의 외부 반출이 합법한 반출인지를 인증할 수 있다.

[0021] 상기 반출 대상의 정보는 단말의 호스트명, MAC 주소, IP 주소, 및 네트워크 정보 중에서 하나 이상을 포함할

수 있다.

[0022] 상기 전자문서의 외부 반출을 통제하는 단계는, 상기 반출 승인 요청자의 PC부의 반출 통제부가, 상기 전자문서의 외부 반출 요청 기안을 작성하여 상기 반출 관리 서버부를 통해 상기 반출 승인 결재자의 PC부에게로 전달하는 단계; 및 상기 반출 승인 결재자의 PC부의 반출 통제부가, 상기 전자문서의 외부 반출을 승인하여 상기 반출 관리 서버부를 통해 상기 반출 승인 요청자의 PC부의 반출 통제부에게로 보내는 단계;를 포함할 수 있다.

[0023] 상기 전자문서의 외부 반출을 통제하는 단계는, 상기 전자문서의 해쉬 값, 상기 전자문서의 제목, 상기 전자문서의 수신자 단말기의 MAC, IP 주소 및 호스트명 정보, 기안자 또는 결재자의 정보를 이용하여 상기 전자문서의 외부 반출을 통제할 수 있다.

[0024] 상기 가상디스크를 각각 생성하고 관리하는 단계는 상기 생성된 가상디스크의 영역에 접근할 수 있는 어플리케이션을 제한할 수 있고, 상기 전자문서를 상기 가상디스크에서 실행할 수 있도록 실행 통제할 수 있고, 상기 가상디스크의 영역을 암호화할 수 있다.

[0025] 상기 전자문서의 외부 반출이 합법한 반출인지를 인증하는 단계는 미리 설정된 합법 반출 인증 요청 기간내에 상기 전자문서의 외부 반출이 합법한 반출인지를 인증할 수 있다.

## *발명의 효과*

[0026] 이러한 구성의 본 발명에 따르면, 불법 유출시 자가 대응(자가 소멸)할 수 있고 불법 유출 근원지를 추적할 수 있으므로 전자문서의 불법 유출을 원천 차단할 수 있다.

[0027] 이에 따라 지능화된 해킹 기법 및 내부자에 의한 첨단 산업 기밀의 불법 유출을 차단하여 기업 및 국가의 경제적 손실을 예방할 수 있다.

## *도면의 간단한 설명*

[0028] 도 1은 본 발명의 실시예에 채용되는 전자문서 저장 PC부의 구성도이다.

도 2는 도 1에 도시된 반출 통제부의 내부 구성도이다.

도 3은 본 발명의 실시예에 따른 전자문서 불법 유출 방지 시스템의 구성도이다.

도 4는 본 발명의 실시예에 따른 전자문서 불법 유출 방지 방법을 설명하는 플로우차트이다.

## *발명을 실시하기 위한 구체적인 내용*

[0029] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시 예들을 도면에 예시하고 상세하게 설명하고자 한다.

[0030] 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0031] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0032] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0033] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0034] 도 1은 본 발명의 실시예에 채용되는 전자문서 저장 PC부의 구성도이고, 도 2는 도 1에 도시된 반출 통제부의

내부 구성도이고, 도 3은 본 발명의 실시예에 따른 전자문서 불법 유출 방지 시스템의 구성도이다.

[0035] 전자문서 저장 PC부(10, 50)는 반출 승인 요청자 및 반출 승인 결재자의 것으로 대별된다.

[0036] 즉, 반출 승인 요청자의 전자문서 저장 PC부(10)와 반출 승인 결재자의 전자문서 저장 PC부(50)는 각각 로컬디스크(20, 60), 가상디스크(30, 70), 및 반출 통제부(40, 80)를 포함한다. 다시 말해서, 반출 승인 요청자의 전자문서 저장 PC부(10)와 반출 승인 결재자의 전자문서 저장 PC부(50)의 내부 구성요소는 서로 동일하다고 볼 수 있다. 여기서, 반출 승인 요청자의 전자문서 저장 PC부(10)는 본 발명의 특허청구범위에 기재된 반출 승인 요청자의 PC부가 될 수 있고, 반출 승인 결재자의 전자문서 저장 PC부(50)는 본 발명의 특허청구범위에 기재된 반출 승인 결재자의 PC부가 될 수 있다.

[0037] 그리고, 상술한 전자문서 저장 PC부(10, 50)를 전자문서 저장 서버부라고 하여도 무방하다.

[0038] 로컬디스크(20, 60)는 해당 전자문서 저장 PC부(10, 50)의 HDD(Hard Disk Drive)/SSD(Solid State Drive)에서 제공하는 데이터 저장공간이다. 로컬디스크(20, 60)는 비 통제대상 파일이 저장되는 공간이라고 할 수 있다.

[0039] 가상디스크(30, 70)는 통제대상이 되는 전자문서를 저장하는 공간이다. 가상디스크(30, 70)의 영역은 블록단위로 암호화될 수 있다. 자가 대응 에이전트부(90)는 전자문서 반출 요청 프로세스 단계에서 생성되며, 반출 승인 요청자의 전자문서 저장 PC부(10)는 반출 승인을 획득한 후에 반출 관리 서버부(100)로부터 자가 대응 에이전트부(90)를 다운로드 받을 수 있다.

[0040] 반출 통제부(40, 80)는 전자문서의 외부 반출을 통제한다. 반출 통제부(40, 80)는 디바이스 드라이버 기반의 에이전트 프로그램이라고 할 수 있다. 반출 통제부(40, 80)는 전자문서 저장 PC부(10, 50)에 설치시 가상디스크(30, 70) 영역을 생성시켜 그 가상디스크(30, 70) 영역에 통제하고자 하는 전자문서를 강제로 모두 저장하고 외부 반출을 통제한다. 여기서, 에이전트는 특정 목적(본 발명의 실시예에서는 전자문서의 외부 반출 통제)에 대해 사용자를 대신하여 작업을 수행하는 자율적 프로세스라고 할 수 있다.

[0041] 예를 들어, 반출 통제부(40)는 가상디스크(30)에 저장된 통제 전자문서(즉, 통제대상인 전자문서)를 외부에 반출하고자 할 경우, 반출 승인 요청자의 전자문서 저장 PC부(10)(즉, 기안자 PC)에서 반출 승인 결재자의 전자문서 저장 PC부(50)(즉, 결재자 PC)에게로 외부 반출 승인 요청(반출대상자 PC 정보(PC의 MAC/IP 주소/Hostname 정보) 포함)을 할 수 있도록 지원한다. 이 경우, 반출 승인 결재자의 전자문서 저장PC부(50)의 반출 통제부(80)는 기안자의 통제 전자문서 외부 반출 승인 요청 기안문을 결재 승인해 줌으로써 전자문서의 외부 반출을 허용할 수 있도록 하는 기능을 한다.

[0042] 전자문서의 외부반출 결재 요청이 이루어지는 동안 외부에 전달하고자 하는 전자문서는 전자문서를 포함한 자가 대응 에이전트부(90)의 형태로 교환된다. 외부반출이 승인된 경우 기안자는 외부로 전달하고자 하는 전자문서를 반출 관리 서버부(100)로부터 자가 대응 에이전트부의 형태로 다운로드받아 외부(사내망 포함, 기안자 PC가 아닌 모든 PC)에 전달하게 된다.

[0043] 한편, 반출 통제부(40)의 내부 구성을 살펴보면, 도 2에서와 같이 가상디스크 생성 및 관리부(42), 반출 요청 에이전트부(44), 및 반출 승인 에이전트부(46)를 포함한다.

[0044] 가상디스크 생성 및 관리부(42)는 가상디스크(30)의 생성, 접근제어 및 실행 통제 등을 담당한다.

[0045] 반출 요청 에이전트부(44)는 반출용 전자문서와 자가대응 에이전트 결합 및 반출 승인 신청을 담당한다.

[0046] 반출 승인 에이전트부(46)는 반출 승인 결재를 담당한다.

[0047] 도 2에 도시된 반출 통제부(40)의 내부 구성은 반출 승인 요청자의 전자문서 저장 PC부(10) 및 반출 승인 결재자의 전자문서 저장 PC부(50)에 포함되는 반출 통제부의 내부 구성을 총괄하여 표현하였다고 볼 수 있다. 실제로는, 반출 승인 요청자의 전자문서 저장 PC부(10)의 반출 통제부(40)는 상술한 가상디스크 생성 및 관리부(42) 및 반출 요청 에이전트부(44)를 포함할 것이다. 한편, 반출 승인 결재자의 전자문서 저장 PC부(50)의 반출 통제부(80)는 가상디스크 생성 및 관리부(42) 및 반출 승인 에이전트부(46)(도 3에서는 반출 승인 에이전트부(86)로 표시됨)를 포함할 것이다.

[0048] 이와 같이 반출 통제부(40)는 생성된 가상디스크(30) 영역에 접근할 수 있는 어플리케이션을 제한할 수 있으며, 전자문서를 가상디스크(30)에서만 실행할 수 있도록 실행 통제할 수 있으며, 가상디스크(30) 영역을 암호화할 수 있다. 그리고, 반출 통제부(40)는 전자문서의 외부 반출을 통제하기 위해, 해당 전자문서의 해쉬(hash) 값, 해당 전자문서의 제목, 해당 전자문서의 수신자 단말기의 MAC(Media Access Control), IP(Internet Protocol)

주소 및 호스트명(hostname) 정보, 기안자/결재자의 정보(예컨대, 안면 이미지, 홍채, 지문 등의 정보)를 이용할 수 있다.

[0049] 도 1에서, 참조부호 10을 반출 승인 요청자의 전자문서 저장 PC부라고 하고, 참조부호 50을 반출 승인 결재자의 전자문서 저장 PC부라고 하였는데, 이는 설명의 편의를 위해 그리한 것으로서 상황에 따라 바뀔 수도 있다.

[0050] 한편, 도 3에 도시된 자가 대응 에이전트부(90)는 실행파일(EXE) 형태의 에이전트로서 외부에 반출하고자 하는 전자문서를 포함하고 있는 형태이다. 자가 대응 에이전트부(90)는 외부에 반출하고자 하는 전자문서의 해쉬(Hash) 값 및 해당 전자문서의 파일명 등을 메타정보로서 포함하고 있다.

[0051] 이와 같이 전자문서를 포함하고 있는 자가 대응 에이전트부(90)를 실행할 경우, 자가 대응 에이전트부(90)는 해당 전자문서를 실행할 PC의 정보를 반출 관리 서버부(100)에 전송한다. 이는 실행 PC가 적법한 대상인지를 확인(인증)하기 위한 것으로서, 인증 요청시 해당 실행 PC의 정보를 반출 관리 서버부(100)에게로 전송한다.

[0052] 그리고, 자가 대응 에이전트부(90)는 반출 관리 서버부(100)로부터 불법 반출을 알리는 결과를 수신하게 되면 전자문서 생성없이 자가소멸을 행할 수 있다. 한편, 자가 대응 에이전트부(90)는 반출 관리 서버부(100)로부터 적법한 반출임을 알리는 결과를 수신하게 되면 전자문서 생성후 자가소멸을 행할 수 있다.

[0053] 그에 따라, 자가 대응 에이전트부(90)는 전자문서의 불법적인 외부 반출이 있게 되면 사용자를 대신하여 전자문서의 생성없이 자가소멸의 작업을 능동적으로 수행하는 자율적 프로세스라고 할 수 있다.

[0054] 반출 관리 서버부(100)는 반출 요청 에이전트부(44)와 반출 승인 에이전트부(86)의 모든 이력을 저장 및 관리한다. 즉, 반출 관리 서버부(100)는 반출 허용된 전자문서 및 외부 수신자 정보를 저장하고 관리한다.

[0055] 또한, 반출 관리 서버부(100)는 자가 대응 에이전트부(90)를 저장 및 관리한다.

[0056] 또한, 반출 관리 서버부(100)는 외부에서 자가 대응 에이전트부(90)가 실행될 때 반출 대상의 적법성 여부 확인을 위해 수신되는 인증 요청(실행PC의 MAC/IP 주소/Hostname 정보 수신)에 대해 관리 목록을 확인한 후에 적법성 여부 결과(즉, 인증 결과)를 자가 대응 에이전트부(90)에게로 통보해 준다.

[0057] 상술한 도 3에서, 반출 관리 서버부(100)는 전자문서 저장 PC부(10, 50)의 외부에 구성되는 것으로 하였는데, 필요에 따라서는 전자문서 저장 PC부(10) 또는 전자문서 저장 PC부(50)의 내부에 갖추어지는 것으로 하여도 무방하다.

[0058] 도 4는 본 발명의 실시예에 따른 전자문서 불법 유출 방지 방법을 설명하는 플로우차트이다.

[0059] 먼저, 전자문서 유출 통제를 위해 전자문서 저장 PC부(10, 50)에서 통제대상이 되는 전자문서를 강제로 저장하기 위한 가상디스크(30, 70)를 생성하고 관리한다. 이때, 생성된 가상디스크(30, 70)에 접근할 수 있는 어플리케이션은 제한할 수 있으며 가상디스크 영역은 블록단위로 암호화할 수 있다.

[0060] 이후, 반출통제용 전자문서는 반출 승인 요청자의 전자문서 저장 PC부(10) 및 반출 승인 결재자의 전자문서 저장 PC부(50) 내의 가상디스크(30, 70) 영역에 강제로 저장 및 보관된다(S10).

[0061] 이어, 반출 승인 요청자의 전자문서 저장 PC부(10)의 반출 요청 에이전트부(44)는 전자문서의 합법적인 반출을 위해 전자문서 반출 요청 기안을 작성한다(S12). 이러한 전자문서 반출 요청 기안 작성시 반출용 전자문서는 자가 대응 에이전트부(90)에 탑재된 형태로 첨부된다. 한편, 전자문서 반출 요청 기안 작성시 반출 대상자의 PC정보(예컨대, PC의 MAC/IP 주소, 호스트명(hostname) 정보, 네트워크 정보 등)를 함께 기입하게 된다.

[0062] 반출 관리 서버부(100)는 반출 요청 에이전트부(44)와 반출 승인 에이전트부(86)간의 모든 이력을 저장 및 관리(예컨대, 목록 형태로 관리)하고 있으므로, 반출 관리 서버부(100)는 S12에서 작성된 전자문서 반출 요청 기안을 반출 승인 결재자의 전자문서 저장 PC부(50)의 반출 승인 에이전트부(86)에게로 전송한다. 이어, 반출 승인 에이전트부(86)는 전자문서 반출 승인을 해주고 그 결과를 반출 관리 서버부(100)를 통해 반출 요청 에이전트부(44)에게로 보낸다. 그에 따라, 반출 요청 에이전트부(44)는 전자문서 반출 승인을 얻게 된다(S14).

[0063] 상술한 전자문서에 대한 합법 반출 요청 및 승인하는 단계(S12, S14)에서, 합법 반출 요청/승인/목록 관리를 위해 해당 전자문서의 해쉬(hash) 값, 해당 전자문서의 제목, 해당 전자문서의 수신자 단말기의 MAC(Media Access Control) 및 IP(Internet Protocol) 주소 정보, 기안자/결재자의 안면 이미지 또는 홍채 또는 지문 등의 정보를 이용할 수 있다.

[0064] 이와 같이 전자문서 반출 승인을 얻은 후에는, 전자문서 반출 요청 기안자(즉, 반출 승인 요청자의 전자문서 저

장 PC부(10))는 반출 관리 서버부(100)를 통해 전자문서를 포함하고 있는 자가 대응 에이전트부(90)를 다운로드 한 후 반출하고자 하는 대상에게 해당 에이전트부(90)를 전달한다(S16, S18).

[0065] 자가 대응 에이전트부(90)가 반출하고자 하는 대상에게 전달됨에 따라, 자가 대응 에이전트부(90)는 반출하고자 하는 대상(예컨대, PC)에서 실행된다. 이때, 자가 대응 에이전트부(90)는 해당 반출 대상(또는 반출 대상자)의 PC 정보를 반출 관리 서버부(100)에게로 전송하여 실행 PC의 적법 대상 여부(즉, 반출 대상이 적법한 대상인지의 여부)를 확인하기 위해 인증을 요청한다. 이때, 자가 대응 에이전트부(90)가 반출 관리 서버부(100)에게로 전송하는 해당 PC 정보는 해당 PC의 MAC(Media Access Control)/IP(Internet Protocol) 주소, 호스트명(hostname) 정보, 네트워크 정보 등을 포함할 수 있다. 그에 따라, 반출 관리 서버부(100)는 수신한 해당 PC 정보를 근거로 인증을 행한 후에 그 결과를 자가 대응 에이전트부(90)에게로 보낸다(S20). 예를 들어, 반출 관리 서버부(100)가 반출 대상자 A, B에 대한 PC 정보를 관리 목록에 미리 가지고 있는 것으로 가정한다. 반출 대상자 A에게 전자문서를 보내고자 할 경우 반출 관리 서버부(100)는 미리 저장되어 있는 정보를 근거로 반출 대상자 A가 적법한 자인지를 인증할 수 있게 된다. 여기서, 인증 기능을 강화하기 위해 사전에 합법 반출 인증 요청 기간을 설정해 두어도 무방하다. 즉, 지속적인 인증 요청이 있게 되면 시스템적으로도 부하가 많이 걸리고 후속 단계로의 전환이 늦어지므로, 미리 설정된 합법 반출 인증 요청 기간동안에만 인증 요청 및 인증이 이루어지도록 할 수 있다. 이러한 인증 단계(S20)에서 해당 기능을 무력화하거나 우회할 수 없도록 안티리버싱, 난독화, 안티디버깅 등의 보안 기능을 적용하여도 된다.

[0066] 즉, 인증 결과, 적법한 대상인 경우(S22에서 "Yes")에는, 반출 관리 서버부(100)는 적법한 대상임을 알리는 신호를 자가 대응 에이전트부(90)에게로 보낸다. 그에 따라, 자가 대응 에이전트부(90)는 전자문서를 생성하게 된다(S24).

[0067] 반대로, 부적합한 대상인 경우(S22에서 "NO")에는, 반출 관리 서버부(100)는 부적합한 대상임을 알리는 신호(즉, 불법 반출임을 알리는 신호)를 자가 대응 에이전트부(90)에게로 보낸다. 물론, 반출 관리 서버부(100)는 인증하고자 하는 해당 반출 대상에 대한 정보를 가지고 있지 않을 경우에는 인증을 할 수 없어서 인증 실패가 되어 부적합한 대상으로 간주할 것이다. 그에 따라, 자가 대응 에이전트부(90)는 전자문서의 생성없이 자기소멸하게 된다(S26). 한편, 이와 같이 불법 반출을 행하는 근원지 정보 획득 및 자가 대응(자가 소멸)하는 단계에서, 해당 기능을 무력화하거나 우회할 수 없도록 안티리버싱, 난독화, 안티디버깅 등의 보안 기능을 적용하여도 된다.

[0068] 이상에서와 같이 도면과 명세서에서 최적의 실시예가 개시되었다. 여기서 특정한 용어들이 사용되었으나, 이는 단지 본 발명을 설명하기 위한 목적에서 사용된 것이지 의미 한정이나 특허청구범위에 기재된 본 발명의 범위를 제한하기 위하여 사용된 것은 아니다. 그러므로, 본 기술 분야의 통상의 지식을 가진자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호범위는 첨부된 특허청구범위의 기술적 사상에 의해 정해져야 할 것이다.

## *부호의 설명*

[0069] 10 : 반출 승인 요청자의 전자문서 저장 PC부

20, 60 : 로컬디스크 30, 70 : 가상디스크

40, 80 : 반출 통제부

42 : 가상디스크 생성 및 관리부 44 : 반출 요청 에이전트부

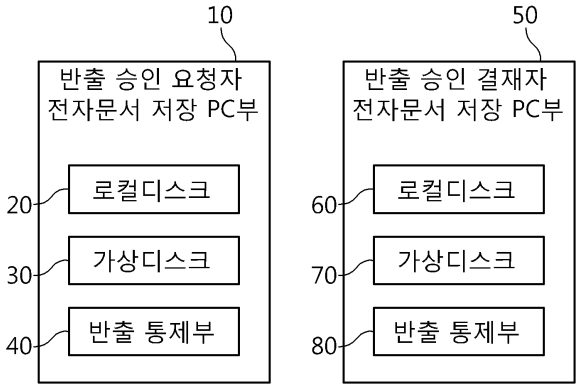
46, 86 : 반출 승인 에이전트부

50 : 반출 승인 결재자의 전자문서 저장 PC부

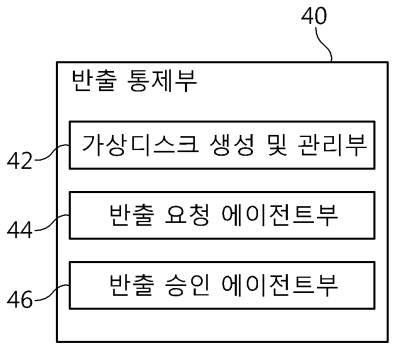
90 : 자가 대응 에이전트부 100 : 반출 관리 서버부

## 도면

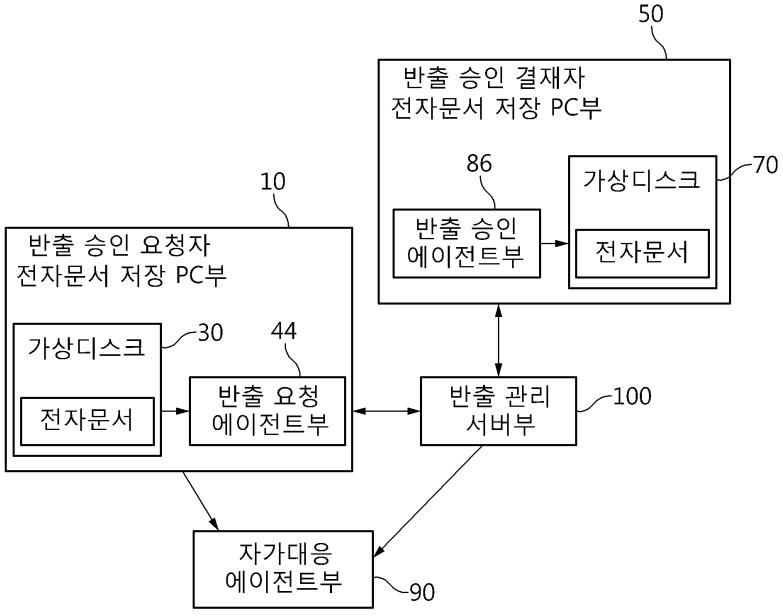
### 도면1



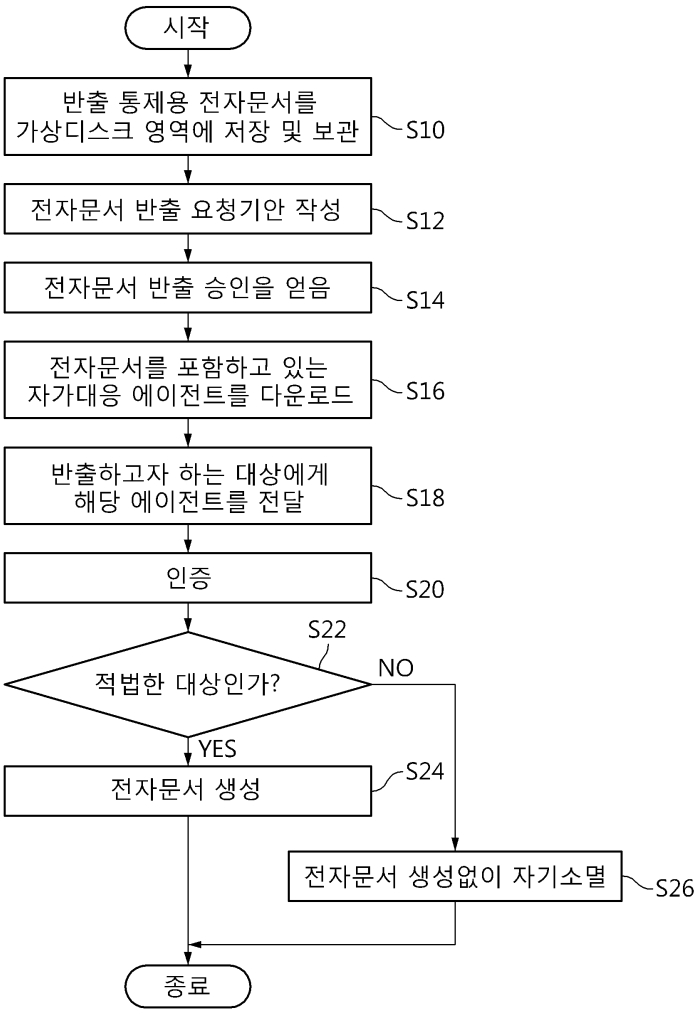

### 도면2




### 도면3



도면4


시작
반출 통제용 전자문서를 가상디스크 영역에 저장 및 보관
S10
전자문서 반출 요청기안 작성
S12
전자문서 반출 승인을 얻음
S14
전자문서를 포함하고 있는 자가대응 에이전트를 다운로드
S16
반출하고자 하는 대상에게 해당 에이전트를 전달
S18
인증
S20
S22
적법한 대상인가?
NO
YES
전자문서 생성
S24
전자문서 생성없이 자기소멸
S26
종료