(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년05월27일
(11) 등록번호 10-2403127
(24) 등록일자 2022년05월24일

(51) 국제특허분류(Int. Cl.)
G06F 21/60 (2013.01) *G06F 11/07* (2006.01)
G06F 21/52 (2013.01)
(52) CPC특허분류
G06F 21/60 (2013.01)
G06F 11/0757 (2013.01)
(21) 출원번호 10-2020-0155057
(22) 출원일자 2020년11월19일
심사청구일자 2020년11월19일
(65) 공개번호 10-2022-0068355
(43) 공개일자 2022년05월26일
(56) 선행기술조사문헌
KR1020190030864 A
KR1020190029501 A
KR1020180116035 A

(73) 특허권자
주식회사 올리브텍
경기도 성남시 수정구 창업로 42,경기기업성장센타 530,531호(시흥동, 판교제2테크노밸리)
(72) 발명자
임장식
경기도 용인시 수지구 대지로 139 용인죽전동부센트레빌 107동 1401호
이덕원
경기도 용인시 수지구 동천로 64 동천마을동문굿모닝힐5차아파트 513동 2201호
(74) 대리인
김익수

전체 청구항 수 : 총 10 항 심사관 : 구대성

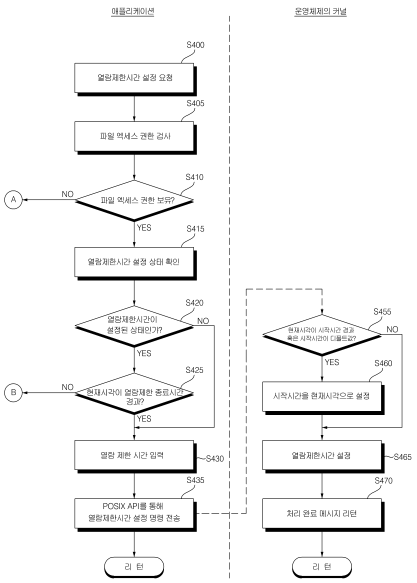
(54) 발명의 명칭 **스토리지 운영체제의 커널 수준에서 파일에 지정된 열람제한시간 동안 파일 내용 읽기 및 쓰기를 원천적으로 방지하는 데이터 보호 방법**

(57) 요 약

본 발명은 열람제한시간이 설정된 파일의 내용을 어떠한 권한으로도 열람하거나 수정하는 것을 원천적으로 방지할 수 있는 데이터 보호 방법에 관한 것이다. 본 데이터 보호 방법은, 사용자의 명령을 통해 스토리지 장치에 저장된 파일 중에서 제1 파일에 대해 설정된 제한 시간 동안 읽기 및 쓰기를 차단하는 열람제한시간 설정을 요청

(뒷면에 계속)

대 표 도 - 도4



받는 과정, 사용자가 제1 파일에 대한 파일 엑세스 권한이 있고, 제1 파일에 열람제한시간이 설정된 상태가 아니며, 열람제한을 시작하는 시작시간과, 열람제한을 종료하는 종료시간을 입력받는 과정, POSIX API를 통해 시작시간과 종료시간을 포함하는 제1 파일에 대한 열람제한시간 설정 명령을 스토리지 장치에 파일시스템 서비스를 제공하는 운영체제의 커널에 전송하는 과정, 커널에서 제1 파일의 메타데이터에 열람제한시간 설정 상태를 나타내는 열람제한 플래그와, 시작시간의 속성 및 종료시간의 속성을 추가로 생성하는 과정, 및 커널에서 시작시간의 속성에 시작시간을 저장하고, 종료시간의 속성에는 종료시간을 저장하며, 열람제한 플래그를 열람제한시간 설정 상태로 셋팅하여, 시작시간부터 종료시간까지 제1 파일에 대해 읽기 및 쓰기를 차단하는 열람제한시간 설정 상태로 만드는 과정을 포함한다.

(52) CPC특허분류
G06F 21/52 (2013.01)
G06F 2221/2137 (2013.01)
G06F 2221/2141 (2013.01)
G06F 2221/2147 (2013.01)

명 세 서

청구범위

청구항 1

사용자의 명령을 통해 스토리지 장치에 저장된 파일 중에서 제1 파일에 대해 설정된 제한 시간 동안 읽기 및 쓰기를 차단하는 열람제한시간 설정을 요청받는 단계;

상기 사용자가 상기 제1 파일에 대한 파일 엑세스 권한이 있고, 상기 제1 파일에 열람제한시간이 설정된 상태가 아니며, 열람제한을 시작하는 시작시간과, 열람제한을 종료하는 종료시간을 입력받는 단계;

POSIX API를 통해 상기 시작시간과 상기 종료시간을 포함하는 상기 제1 파일에 대한 열람제한시간 설정 명령을 상기 스토리지 장치에 파일시스템 서비스를 제공하는 운영체제의 커널에 전송하는 단계;

상기 커널에서 상기 제1 파일의 메타데이터에 열람제한시간 설정 상태를 나타내는 열람제한 플래그와, 상기 시작시간의 저장을 위한 제1 속성 항목 및 상기 종료시간의 저장을 위한 제2 속성 항목을 추가로 생성하는 단계; 및

상기 커널에서 상기 제1 속성 항목에 상기 시작시간을 저장하고, 상기 제2 속성 항목에는 상기 종료시간을 저장하며, 상기 열람제한 플래그를 열람제한시간 설정 상태로 셋팅하여, 상기 시작시간부터 상기 종료시간까지 상기 제1 파일에 대해 읽기 및 쓰기를 차단하는 열람제한시간 설정 상태로 만드는 단계를 포함하는 데이터 보호 방법.

청구항 2

제1항에 있어서,

상기 제1 파일에 대한 읽기나 쓰기 명령이 있는 경우, 상기 커널에서 상기 제1 파일의 열람제한 플래그를 검사하여 열람제한시간이 설정된 상태이고, 현재 시각이 상기 시작시간과 상기 종료시간 사이의 제한 시간 범위에 있으면, 상기 읽기나 쓰기 명령의 수행을 차단하는 것을 특징으로 하는 데이터 보호 방법.

청구항 3

제1항에 있어서,

특정 파일에 대한 열람제한시간 설정 요청이 있는 경우, 상기 POSIX API를 통해 상기 커널로부터 상기 특정 파일의 열람제한 플래그 설정값을 가져와서 열람제한시간 설정 상태를 확인하는 단계;

상기 특정 파일에 열람제한시간이 설정된 상태이고, 현재시각이 상기 시작시간과 상기 종료시간 사이의 제한 시간 범위에 있으면, 에러 메시지를 리턴하는 단계; 및

상기 특정 파일에 열람제한시간이 설정된 상태이지만, 현재시각이 상기 종료시간을 경과한 경우에는, 상기 특정 파일에 대한 열람제한시간 설정 과정을 수행하는 단계를 더 포함하는 데이터 보호 방법.

청구항 4

제3항에 있어서,

상기 현재 시각은 시스템 시간에 독립적인 독립 시간을 기준으로 판단하는 것을 특징으로 하는 데이터 보호 방법.

청구항 5

제4항에 있어서,

상기 독립 시간은, 미리 설정된 특수 사용자 아이디의 사용 권한을 통해서만 수정되며, 소정 단위 주기로 동작하는 타이머 프로세스의 신호에 따라, 상기 소정 단위 주기마다 사용 권한이 상기 특수 사용자 아이디로 전환되어 업데이트되는 것을 특징으로 하는 데이터 보호 방법.

청구항 6

제1항에 있어서,

상기 커널은, 설정된 제한 시간 동안 열람제한시간이 설정된 파일에 대해 읽기나 쓰기 명령의 수행은 차단하지만, 상기 열람제한시간이 설정된 파일의 메타데이터에 대한 엑세스는 허용하는 것을 특징으로 하는 데이터 보호 방법.

청구항 7

제1항에 있어서,

상기 커널은, 상기 열람제한 플래그, 상기 제1 속성 항목, 및 상기 제2 속성 항목 중 적어도 어느 하나를 변경하는 독립적인 명령의 수행을 차단하는 것을 특징으로 하는 데이터 보호 방법.

청구항 8

제1항 내지 제7항 중 어느 한 항의 데이터 보호 방법을 프로세서에서 실행시키기 위한 프로그램을 기록한 프로세서가 읽을 수 있는 기록매체.

청구항 9

스토리지 장치;

메모리;

제어부; 및

상기 메모리에 저장되어 상기 제어부에 의해 실행되는 하나 이상의 모듈을 포함하며, 상기 모듈은,

사용자의 명령을 통해 스토리지 장치에 저장된 파일 중에서 제1 파일에 대해 설정된 제한 시간 동안 읽기 및 쓰기를 차단하는 열람제한시간 설정을 요청받는 과정;

상기 사용자가 상기 제1 파일에 대한 파일 엑세스 권한이 있고, 상기 제1 파일에 열람제한시간이 설정된 상태가 아니며, 열람제한을 시작하는 시작시간과, 열람제한을 종료하는 종료시간을 입력받는 과정;

POSIX API를 통해 상기 시작시간과 상기 종료시간을 포함하는 상기 제1 파일에 대한 열람제한시간 설정 명령을 상기 스토리지 장치에 파일시스템 서비스를 제공하는 운영체제의 커널에 전송하는 과정;

상기 커널에서 상기 제1 파일의 메타데이터에 열람제한시간 설정 상태를 나타내는 열람제한 플래그와, 상기 시작시간의 저장을 위한 제1 속성 항목 및 상기 종료시간의 저장을 위한 제2 속성 항목을 추가로 생성하는 과정; 및

상기 커널에서 상기 제1 속성 항목에 상기 시작시간을 저장하고, 상기 제2 속성 항목에는 상기 종료시간을 저장하며, 상기 열람제한 플래그를 열람제한시간 설정 상태로 셋팅하여, 상기 시작시간부터 상기 종료시간까지 상기 제1 파일에 대해 읽기 및 쓰기를 차단하는 열람제한시간 설정 상태로 만드는 과정을 수행하는 것을 특징으로 하는 데이터 저장 시스템.

청구항 10

제9항에 있어서,

상기 모듈은,

상기 제1 파일에 대한 읽기나 쓰기 명령이 있는 경우, 상기 커널에서 상기 제1 파일의 열람제한 플래그를 검사하여 열람제한시간 설정 상태이고, 현재 시각이 상기 시작시간과 상기 종료시간 사이의 제한 시간 범위에 있으면, 상기 읽기나 쓰기 명령의 수행을 차단하는 과정을 더 포함하는 것을 특징으로 하는 데이터 저장 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 파일시스템 서비스를 제공하는 운영체제에서 특정 파일에 대해 설정된 제한 시간 동안 파일의 내용을 읽고 쓰는 것을 제한할 수 있는 열람제한시간 설정 기능을 제공함으로써, 열람제한시간이 설정된 파일의 내용을 어떠한 권한으로도 열람하거나 수정하는 것을 원천적으로 방지할 수 있는 데이터 보호 방법에 관한 것이다.

배 경 기 술

[0002] 파일의 보안은 크게 파일의 훼손 방지와, 파일 내용의 열람 및 유출 방지로 나눌 수 있다. 일반적으로 파일의 훼손 방지는 파일의 무단 삭제 및 위·변조를 커널 수준에서의 권한 관리를 통해 원천 봉쇄하는 WORM(Write Once Read Many) 스토리지 기술을 통해 이루어진다. WORM 스토리지 기술은 일반적으로 파일에 지정된 보존기간 동안 어떠한 권한으로도 파일을 수정하거나 삭제할 수 없도록 커널 내부에 하드코딩된 모듈을 통해 관리자의 권한을 통제하는 것이다.

[0003] 파일 내용의 열람 및 유출에 대한 방지 기능은 파일시스템에서 제공하는 접근 권한 통제 기능인 ACL(Access Control List)를 통해 사용자 별로 접근할 수 있는 권한을 통제하는 방법 등에 의해 이루어질 수 있다.

[0004] 그러나, 관리자 권한이나 슈퍼 유저 권한을 가진 사용자는 이러한 제한을 모두 해제할 수 있다. 또한, 파일 내용의 열람에 대해서는 스토리지 차원에서 어떠한 권한으로도 열람이 불가능하게 차단하는 기능은 존재하고 있지 않다.

[0005] 따라서, 어떠한 권한으로도 파일 내용의 열람, 유출 및 훼손을 원천적으로 방지할 수 있도록 하는 기술이 필요하다.

발명의 내용

해결하려는 과제

[0006] 따라서, 본 발명의 목적은, 파일시스템 서비스를 제공하는 운영체제에서 특정 파일 내용에 대해 설정된 제한 시간 동안 읽기 및 쓰기를 제한할 수 있는 열람제한시간 기능을 제공하여, 어떠한 권한으로도 파일의 내용을 무단으로 열람, 유출 및 훼손하는 것을 원천적으로 방지할 수 있는 데이터 보호 방법을 제공함에 있다.

과제의 해결 수단

[0007] 상기 목적을 달성하기 위한 본 발명에 따른 데이터 보호 방법은, 사용자의 명령을 통해 스토리지 장치에 저장된 파일 중에서 제1 파일에 대해 설정된 제한 시간 동안 읽기 및 쓰기를 차단하는 열람제한시간 설정을 요청받는 단계, 상기 사용자가 상기 제1 파일에 대한 파일 엑세스 권한이 있고, 상기 제1 파일에 열람제한시간이 설정된 상태가 아니며, 열람제한을 시작하는 시작시간과, 열람제한을 종료하는 종료시간을 입력받는 단계, POSIX API를 통해 상기 시작시간과 상기 종료시간을 포함하는 상기 제1 파일에 대한 열람제한시간 설정 명령을 상기 스토리지 장치에 파일시스템 서비스를 제공하는 운영체제의 커널에 전송하는 단계, 상기 커널에서 상기 제1 파일의 메타데이터에 열람제한시간 설정 상태를 나타내는 열람제한 플래그와, 상기 시작시간의 속성 및 상기 종료시간의 속성을 추가로 생성하는 단계, 및 상기 커널에서 상기 시작시간의 속성에 상기 시작시간을 저장하고, 상기 종료시간의 속성에는 상기 종료시간을 저장하며, 상기 열람제한 플래그를 열람제한시간 설정 상태로 셋팅하여, 상기 시작시간부터 상기 종료시간까지 상기 제1 파일에 대해 읽기 및 쓰기를 차단하는 열람제한시간 설정 상태로 만드는 단계를 포함한다.

[0008] 상기 제1 파일에 대한 읽기나 쓰기 명령이 있는 경우, 상기 커널에서 상기 제1 파일의 열람제한 플래그를 검사하여 열람제한시간이 설정된 상태이고, 현재 시각이 상기 시작시간과 상기 종료시간 사이의 제한 시간 범위에 있으면, 상기 읽기나 쓰기 명령의 수행을 차단할 수 있다.

[0009] 또한, 특정 파일에 대한 열람제한시간 설정 요청이 있는 경우, 상기 POSIX API를 통해 상기 커널로부터 상기 특정 파일의 열람제한 플래그 설정값을 가져와서 열람제한시간 설정 상태를 확인하는 단계, 상기 특정 파일에 열람제한시간이 설정된 상태이고, 현재시각이 상기 시작시간과 상기 종료시간 사이의 제한 시간 범위에 있으면, 에러 메시지를 리턴하는 단계, 및 상기 특정 파일에 열람제한시간이 설정된 상태이지만, 현재시각이 상기 종료시간을 경과한 경우에는, 상기 특정 파일에 대한 열람제한시간 설정 과정을 수행하는 단계를 더 포함할 수 있다.

[0010] 또한, 상기 현재 시각은 시스템 시간에 독립적인 독립 시간을 기준으로 판단할 수 있으며, 상기 독립 시간은, 미리 설정된 특수 사용자 아이디의 사용 권한을 통해서만 수정되며, 소정 단위 주기로 동작하는 타이머 프로세스의 신호에 따라, 상기 소정 단위 주기마다 사용 권한이 상기 특수 사용자 아이디로 전환되어 업데이트될 수 있다.

[0011] 또한, 상기 목적을 달성하기 위한 본 발명에 따른 데이터 저장 시스템은, 스토리지 장치, 메모리, 제어부, 및 상기 메모리에 저장되어 상기 제어부에 의해 실행되는 하나 이상의 모듈을 포함하며, 상기 모듈은, 사용자의 명령을 통해 스토리지 장치에 저장된 파일 중에서 제1 파일에 대해 설정된 제한 시간 동안 읽기 및 쓰기를 차단하는 열람제한시간 설정을 요청받는 과정, 상기 사용자가 상기 제1 파일에 대한 파일 엑세스 권한이 있고, 상기 제1 파일에 열람제한시간이 설정된 상태가 아니며, 열람제한을 시작하는 시작시간과, 열람제한을 종료하는 종료시간을 입력받는 과정, POSIX API를 통해 상기 시작시간과 상기 종료시간을 포함하는 상기 제1 파일에 대한 열람제한시간 설정 명령을 상기 스토리지 장치에 파일시스템 서비스를 제공하는 운영체제의 커널에 전송하는 과정, 상기 커널에서 상기 제1 파일의 메타데이터에 열람제한시간 설정 상태를 나타내는 열람제한 플래그와, 시작시간의 속성 및 종료시간의 속성을 추가로 생성하는 과정, 및 상기 커널에서 상기 시작시간의 속성에 상기 시작시간을 저장하고, 상기 종료시간의 속성에는 상기 종료시간을 저장하며, 상기 열람제한 플래그를 열람제한시간 설정 상태로 셋팅하여, 상기 시작시간부터 상기 종료시간까지 상기 제1 파일에 대해 읽기 및 쓰기를 차단하는 열람제한시간 설정 상태로 만드는 과정을 수행할 수 있다.

[0012] 그리고, 상기 목적을 달성하기 위하여 본 발명에서는, 상기 데이터 보호 방법을 프로세서에서 실행시키기 위한 프로그램을 기록한 프로세서로 읽을 수 있는 기록매체를 제공한다.

발명의 효과

[0013] 본 발명에 따르면, 파일시스템 서비스를 제공하는 스토리지 운영체제에서 특정 파일 내용에 대해 설정된 제한 시간 동안 읽기 및 쓰기를 제한할 수 있는 열람제한시간 기능을 제공하여, 설정된 제한 시간 동안 어떠한 권한으로도 파일 내용의 열람, 유출 및 훼손을 원천적으로 방지할 수 있다. 이와 같은 열람제한시간 설정 기능은, 특정 기간동안 열람이 금지된 데이터나, 비밀 해제 기간이 설정된 데이터 등을 보존하는 용도로 유용하게 사용할 수 있으며, 온라인 전자투표 시스템의 경우투표 결과 개봉을 위한 암호키 등을 투표 기간 동안 투표를 주관하는 기관도 열람할 수 없게 하는 것 등과 같이 다양한 분야에서 활용이 가능하다. 또한, 제한 시간 동안 부수적으로 파일 열람뿐만 아니라 파일의 내용을 수정하는 것도 방지함으로써 악성 소프트웨어나 악의적인 변조로부터 파일의 내용을 보호하는 기능도 제공할 수 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명에 따른 데이터 보호 방법이 적용되는 데이터 저장 시스템의 일 예를 나타낸 도면,

도 2 및 도 3은 본 발명에서 사용하는 독립 시간의 설정 및 업데이트 과정에 대한 설명에 제공되는 흐름도,

도 4 및 도 5는 본 발명의 일실시예에 따른 데이터 보호 방법에서 열람제한시간 설정 과정에 대한 설명에 제공되는 흐름도, 그리고

도 6은 본 발명의 일실시예에 따른 데이터 보호 방법에서 운영체제의 커널에서 동작 과정에 대한 설명에 제공되는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 본 명세서에서, 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 경우, 어떤 구성요소에 다른 구성요소에 직접적으로 연결되어 있거나 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 또한, 구성요소들 간의 관계를 설명하는 다른 표현들, 즉 "~사이에" 또는 "~에 이웃하는" 등과, 어떤 구성요소가 다른 구성요소로 신호를 "전송한다" 와 같은 표현도 마찬가지로 해석되어야 한다.

[0016] 이하에서는 도면을 참조하여 본 발명을 보다 상세하게 설명한다.

[0017] 도 1은 본 발명에 따른 데이터 보호 방법이 적용되는 데이터 저장 시스템의 일 예를 나타낸 것이다.

[0018] 도 1을 참조하면, 본 데이터 저장 시스템(100)은, 통신부(110), 메모리(120), 스토리지 인터페이스부(130), 스토리지 장치(140), 및 제어부(150)를 포함할 수 있다. 이와 같은 구성요소들은 실제 응용에서 구현될 때 필요

에 따라 2 이상의 구성요소가 하나의 구성요소로 합쳐지거나, 혹은 하나의 구성요소가 2 이상의 구성요소로 세분되어 구성될 수 있다.

[0019] 통신부(110)는 네트워크를 통해 클라이언트 기기(200)나 기타 다른 기기와 데이터 송수신이 가능하도록 한다. 클라이언트 기기(200)나 기타 외부 기기를 통해 사용자는 스토리지 장치(140)에 파일을 저장하거나 저장된 파일을 읽거나 수정할 수 있다.

[0020] 메모리(120)는 제어부(150)의 처리 및 제어를 위한 프로그램 코드가 저장될 수 있으며, 입력되거나 출력되는 데이터들을 임시 저장하는 기능을 수행할 수도 있다. 메모리(120)에는 스토리지 장치(140)에 디렉토리 및 파일을 계층적 구조로서 논리적으로 구성하는 파일 시스템 서비스 등을 제공하는 스토리지 운영체제(125)가 설치될 수 있다.

[0021] 스토리지 인터페이스부(130)는 스토리지 장치(140)와 데이터 송수신을 위한 인터페이스 역할을 수행한다.

[0022] 스토리지 장치(140)는 제어부(150)나 기타 컴퓨터 프로세서 등이 접근할 수 있도록 전자기적인 형태로 데이터를 저장하는 장치이며, 하드디스크나 SSD(Solid State Disk) 등으로 구성할 수 있다.

[0023] 제어부(150)는 통상적으로 상기 각부의 동작을 제어하여 데이터 저장 시스템(100)의 전반적인 동작을 제어한다. 예를 들어, 제어부(150)는 스토리지 장치(140)에서 디스크의 어레이를 포함하는 하나 이상의 볼륨을 관리하고, 클라이언트 기기(200)나 기타 외부 기기의 요청에 따라, 스토리지 장치(140)에 데이터를 기록하거나 수정, 또는 추가하거나 삭제하는 것과 같은 동작을 수행할 수 있다.

[0024] 이와 같은 데이터 저장 시스템에서, 관리자 권한을 가진 사용자는 스토리지 장치(140)에 저장된 어떠한 데이터든지 변경하거나 삭제할 수 있는 권한을 가진다. 그런데, 정상적으로 관리자 권한을 부여받은 관리자가 실수 혹은 의도적으로 데이터를 손상시키는 경우나, 불법적으로 관리자 권한을 획득한 침입자가 데이터를 파괴하는 경우 등이 발생할 수 있다.

[0025] 이를 방지하기 위해 WORM(Write Once Read Many) 기능을 부가할 수 있는데, WORM 기능이 구현된 데이터 저장 시스템은 어떠한 경로로 관리자 권한을 획득하더라도 데이터를 변조하거나 삭제하는 것을 허용되지 않는 구조를 가진다.

[0026] 그리고, WORM 기능을 구현한 데이터 저장 시스템에서 보존 기간을 설정하여, 미리 설정된 보존 기간이 경과된 경우에만 저장된 파일을 삭제거나 수정할 수 있도록 구성할 수 있다. 이때. 보존 기간의 경과 여부는 하드웨어적인 리얼 타임 클럭(RTC)이 제공하는 시간을 기준으로 바이오스(BIOS)나 시스템에 설치된 운영 체제(OS)가 제공하는 시스템 시간을 기준으로 판단할 수 있다.

[0027] 또한, 본 발명에서는 특정 파일에 대해 설정된 제한 시간 동안 읽기 및 쓰기를 방지할 수 있는 열람제한시간을 설정할 수 있고, 열람제한시간이 설정된 파일에 대해서는 제한 시간 동안에는 열람제한시간 기능을 설정한 사용자를 포함해서 어떠한 권한으로도 파일의 내용을 읽거나 수정할 수 없도록 차단하는 기능을 커널 내부에 구현한다. 이때, 이러한 기능을 제공하는 소프트웨어는 스토리지 운영체제(125)안에 고정된 코드로 구현이 되거나 펌웨어로 구현되어 외부에서 이를 변경할 방법을 원천적으로 차단하여, 제한 시간이 경과하기 전까지는 어떤 권한으로도 데이터를 열람하거나, 위변조하는 것을 방지할 수 있다.

[0028] 그런데, 합법적인 절차 혹은 해킹을 통해 관리자 권한을 획득하면, 시스템 시간을 기준으로 특정 파일에 설정된 제한 시간을 시스템 시간의 변경을 통해 무력화 하고 데이터를 삭제하거나 위변조하는 것이 가능해 질 수 있다. 기준 시간을 제공해 주는 네트워크 상의 타임서버와 연결된 시스템의 경우에는 외부로부터 기준시간을 받아서 시스템 시간을 최신으로 보정할 수 있어서 이러한 위협을 최소화할 수도 있지만, 타임서버에 접속할 수 없는 폐쇄된 환경에서 독립적으로 운영되는 시스템의 경우에는 이러한 방법을 사용할 수 없다.

[0029] 따라서, 본 발명에서는 시스템 시간과 독립적으로 운영되며 임의로 변경할 수 없는 독립 시간을 이용하여 이러한 위협을 방지한다. 즉, 저장 시스템(100)의 바이오스(BIOS)나 운영 체제(OS) 등이 제공하는 시스템 시간과 독립적으로 운영되는 독립 시간을 설정하고, 소정 주기마다 독립 시간을 업데이트한다. 독립 시간은 소프트웨어적으로 설정할 수 있으며, 미리 설정되고 비밀이 보장되는 특수 사용자 아이디의 사용 권한을 통해서만 업데이트되도록 구성된다.

[0030] 도 2는 본 발명에서 사용하는 독립 시간의 설정 과정에 대한 설명에 제공되는 흐름도이다.

[0031] 도 2를 참조하면, 먼저, 초기 독립 시간을 현재 시스템 시간으로 설정한다(S300). 그리고, 독립적으로 운영되

는 독립 시간을 소정 주기로 업데이트 하는 단위 주기 시간과, 상황에 따라 독립 시간을 미세 보정할 수 있는 추가 보정 시간을 설정한다(S310). 예컨대, 단위 주기 시간은 60초, 추가 보정 시간은 1초와 같이 설정할 수 있다.

[0032] 다음으로 소정 단위 주기로 신호를 발생하여 소정 단위 주기가 도래하였음을 알려주는 타이머 프로세스를 설정하고(S320), 설정된 타이머 프로세스를 실행한다, (S330).

[0033] 그리고, 타이머 프로세스를 통해 전달된 신호에 따라 소정 단위 주기가 도래한 것으로 인식되면(S340), 독립 시간의 업데이트 과정을 수행한다(S350).

[0034] 이와 같은 과정에 의해, 시스템 시간과 독립적으로 운영되는 독립 시간을 설정하여 운영할 수 있다. 독립 시간의 업데이트는 미리 설정되고 비밀이 보장되는특수 사용자 아이디의 사용 권한을 통해서만 실행되도록 구성된다.

[0035] 도 3은 본 발명에 사용하는 독립 시간의 업데이트 과정에 대한 설명에 제공되는 흐름도이다.

[0036] 도 3을 참조하면, 독립 시간의 업데이트 과정이 시작되면, 독립 시간을 업데이트할 수 있는 권한을 가진 특수 사용자 아이디(ID)로 사용자 권한을 전환한다(S351). 이 특수 사용자 아이디는 사전에 정의된 비밀 아이디이며, 독립 시간을 운영 관리하는 프로세스 및 업데이트를 수행하는 운영체제 등의 내부 코드에 내장되어 있어, 외부에서 이를 변경할 방법을 원천적으로 차단하도록 구성된다.

[0037] 특수 사용자 아이디로 전환한 후, 일단 현재 독립 시간과 단위 주기 시간을 합산한 시간을 잠정 업데이트 시간으로 설정한다(S352).

[0038] 그리고, 잠정 업데이트 시간과 현재 시스템 시간을 비교하여, 잠정 업데이트 시간이 현재 시스템 시간보다 큰 경우(S353), 잠정 업데이트 시간은, '현재 독립 시간 + 단위 주기 시간 - 추가 보정 시간'으로 설정한다(S354).

[0039] 잠정 업데이트 시간이 현재 시스템 시간보다 작은 경우(S355), 잠정 업데이트 시간은, '현재 독립 시간 + 단위 주기 시간 + 추가 보정 시간'으로 설정한다(S356).

[0040] 그리고, 업데이트 할 새로운 독립 시간은 잠정 업데이트 시간으로 설정한다(S338). 즉, 잠정 업데이트 시간이 현재 시스템 시간과 같은 경우에는 새로운 독립 시간은 기존 독립 시간에 단위 주기 시간을 합산한 시간으로 설정하고, 잠정 업데이트 시간이 현재 시스템 시간보다 크거나 작은 경우에는 새로운 독립 시간은 기존 독립 시간에 단위 주기 시간을 합산한 시간에 추가 보정 시간을 가감한 시간으로 설정한다.

[0041] 이와 같은 과정에 의해, 특수 사용자 아이디의 사용자 권한을 통해 독립 시간이 업데이트되며, 추가 보정 시간을 통해 미세 조정도 가능하게 된다.

[0042] 그리고, 시스템 시간과 현재 시스템 시간의 차이가 미리 설정된 기준을 벗어나는 경우에는, 시스템 시간이 변조된 것으로 파악하여, 경고 메시지를 표시하거나 미리 설정된 사용자에게 통보하도록 구성할 수도 있다.

[0043] 도 4 및 도 5는 본 발명의 일실시예에 따른 데이터 보호 방법에서 열람제한 시간 설정 과정에 대한 설명에 제공되는 흐름도이다.

[0044] 도 4를 참조하면, 사용자의 명령 등에 따라, 스토리지 장치(140)에 저장된 파일 중에서 선택한 제1 파일에 대해 설정된 제한 시간 동안 읽기 및 쓰기를 차단하는 열람제한시간 설정 요청이 있으면(S400), 제어부(150)는 사용자가 선택한 제1 파일에 대해 파일 엑세스 권한이 있는지 검사한다(S405).

[0045] S405 단계의 검사 결과, 사용자가 제1 파일에 대해 파일 엑세스 권한을 보유하고 있으면, 제1 파일의 열람제한 시간 설정 상태를 확인한다(S415).

[0046] 열람제한시간 설정 여부의 확인은 POSIX API를 통해 운영체제의 커널로부터 제1 파일의 열람제한시간 설정 상태를 나타내는 열람제한 플래그인 xread-flag 등을 가져와서 확인할 수 있다. 열람제한 플래그를 가져오는 명령은 다음과 같은 형식으로 나타낼 수 있다.

[0047] getxattr file-path xread-flag

[0048] 그리고, POSIX는 Portable Operating System Interface의 약자로써 운영체제의 공통적인 규약을 규정하고 있는 표준으로, 애플리케이션이 운영체제들과 통신하기 위한 API 규격들을 제공한다. 이 규격의 내용은 커널로의 C 언어 인터페이스인 시스템 콜뿐만 아니라, 프로세스 환경, 파일과 디렉토리, 시스템 데이터베이스, 압축 포맷

등 다양한 분야를 포함한다.

[0049] 열람제한 플래그 설정값으로부터 제1 파일에 열람제한시간이 설정되어 있지 않은 상태로 확인되면(S420), 제어부(150)는 사용자 명령 등에 의해 열람 제한 시간을 입력받는다(S430).

[0050] 제1 파일에 열람제한시간이 설정되어 있는 상태라고 하더라도, 독립 시간을 기준으로 하는 현재 시각이 설정된 열람제한 종료시간을 경과한 경우에도(S425), 제어부(150)는 사용자 명령 등에 의해 열람 제한 시간을 입력받는다(S430). 즉, 제1 파일에 열람제한시간이 설정되어 있더라도, 제한 시간이 경과한 후의 기간에 대해서 다시 열람제한시간을 설정할 수 있다.

[0051] 열람 제한 시간은 열람제한을 시작하는 시작시간(xread-start)과 열람제한을 종료하는 종료시간(xread-end)로 구성할 수 있으며, 시작시간(xread-start)을 입력하지 않는 경우에는 미리 설정된 디폴트 값으로 시작시간(xread-start)을 설정할 수 있다.

[0052] 다음으로 제어부(150)는 POSIX API를 통해 시작시간(xread-start)과 종료시간(xread-end)을 포함하는 제1 파일에 대한 열람제한시간 설정 명령을 운영체제의 커널로 전송한다(S435). 열람제한시간 설정 명령은 다음과 같은 형식으로 나타낼 수 있다.

[0053] setxattr file-path xread-start xread-end

[0054] 열람제한시간 설정 명령을 전달받은 커널은, 독립 시간을 기준으로 하는 현재 시각이 이미 전달받은 시작시간(xread-start)을 경과한 경우나, 시작시간(xread-start)이 디폴트 값으로 설정되어 있는 경우(S455), 시작시간(xread-start)을 현재 시각으로 설정한다(S460).

[0055] 그리고, 열람제한시간 설정 상태를 나타내는 열람제한 플래그인 xread-flag와, 시작시간의 속성인 xread-start-time과, 종료시간의 속성인 xread-end-time 이라는 세 개의 파일 확장 속성을 제1 파일의 메타데이터에 추가로 생성하여, 시작시간의 속성인 xread-start-time에 시작시간(xread-start)을 저장하고, 종료시간의 속성인 xread-end-time에는 종료시간(xread-end)을 저장하며, 열람제한 플래그인 xread-flag를 1로 설정하여 열람제한시간 설정 상태로 만든다(S465). 그리고 처리 완료 메시지를 리턴한다(S470).

[0056] 도 5를 참조하면, S410 단계에서 사용자에게 파일 엑세스 권한이 없는 경우, 제어부(150)는 제1 파일에 대해 파일 엑세스 권한이 없음을 표시하고(S440), 에러 메시지를 리턴한다(S450).

[0057] 그리고, S425 단계에서 제1 파일이 이미 열람제한시간이 설정된 상태이고, 현재 시각이 아직 열람제한 종료시간을 경과하지 않은 경우, 제어부(150)는 제1 파일에 이미 열람제한시간이 설정되어 있는 상태임을 표시하고(S445), 에러 메시지를 리턴한다(S450).

[0058] 이와 같은 과정에 의해, 사용자 선택한 파일에 대해 설정한 제한 시간 동안 읽기 및 쓰기를 차단할 수 있는 열람제한시간 상태를 설정할 수 있다.

[0059] 도 6은 본 발명의 일실시예에 따른 데이터 보호 방법에서 운영체제의 커널에서 동작 과정에 대한 설명에 제공되는 흐름도이다.

[0060] 도 6을 참조하면, 운영체제의 커널에서는 애플리케이션 등으로부터 요청 받은 파일 관련 동작을 분류해서(S500), 파일에 대한 메타데이터를 처리하는 것과 관련된 동작인지, 파일의 내용을 읽거나 쓰는 것과 관련된 동작인지 등을 구분한다.

[0061] 요청받은 파일 관련 동작이 열람제한시간을 처리하는 동작인 경우(S535), 전술한 열람제한시간 설정 과정을 수행한다(S550).

[0062] 기타 메타데이터와 관련된 동작의 요청에 대해서는 일반적인 절차에 따라 요청된 동작이 수행되도록 하고(S540), 동작 수행이 완료되면, 요청된 동작이 성공적으로 처리 완료되었음을 나타내는 처리 완료 메시지를 리턴한다(S545).

[0063] 요청 받은 파일 관련 동작이, 파일의 내용을 읽거나 쓰는 것과 관련된 동작인 경우(S510), 해당 파일에 열람제한 플래그가 1로 설정되어, 열람제한시간 설정된 상태이고(S515), 현재시각이 제한시간의 시작시간과 종료시간의 사이인 제한 시간의 범위에 속하는 경우(S520), 요청된 동작의 수행을 차단하고(S525), 에러 메시지를 리턴한다(S530)

[0064] 요청받은 파일 관련 동작이 파일 내용의 읽거나 쓰는 것과 관련된 명령이 아닌 경우에는(S510), 일반적인 절차

에 따라 요청된 동작이 수행되도록 하고(S540), 동작 수행이 완료되면, 요청된 동작이 성공적으로 처리 완료되었음을 나타내는 처리 완료 메시지를 리턴한다(S545).

[0065] 이와 같이, 커널 내부에서는 파일 관련 동작 요청이 있는 경우마다, 해당 파일이 열람제한시간이 설정된 상태인지 확인하며, 열람제한시간이 설정된 파일에 대해서는 파일의 메타데이터 엑세스는 허용하지만 파일 내용에 대한 읽기 및 쓰기는 허용하지 않도록 한다.

[0066] 또한, 열람제한 플래그, 열람제한 시작시간, 열람제한 종료시간을 표시하는 속성도 독립적인 명령을 통해 변경할 수 없도록 구성한다.

[0067] 이와 같은 과정에 의해, 사용자는 특정 파일에 대해 열람제한시간을 설정 과정을 수행하여, 열람제한시간이 설정된 파일에 대해서 설정된 제한 시간 동안 파일 읽기 및 쓰기를 차단할 수 있다.

[0068] 한편, 본 발명에 따른 데이터 보호 방법은 상기한 바와 같이 설명된 실시예들의 구성에 한정되게 적용될 수 있는 것이 아니라, 상기한 실시예들은 다양한 변형이 이루어질 수 있도록 각 실시예들의 전부 또는 일부가 선택적으로 조합되어 구성될 수도 있다.

[0069] 또한, 본 발명은 프로그램 가능한 컴퓨터상에서 컴퓨터 프로그램으로 구현 가능하다. 이러한 컴퓨터는 프로세서, 저장장치, 입력장치, 출력 장치를 포함할 수 있다. 본 발명에서 설명한 내용을 구현하기 위해 프로그램 코드는 마우스 또는 키보드 입력장치로 입력될 수 있다. 이러한 프로그램들은 고차원적인 언어나, 객체지향적인 언어로 구현될 수 있다. 또한 어셈블리나 기계어 코드로 구현된 컴퓨터 시스템으로도 구현될 수 있다.

[0070] 또한, 본 발명의 내용은 하드웨어나 소프트웨어 사용에만 국한되지는 않으며, 다른 어떤 컴퓨팅 또는 처리 환경에 대해서도 적용 가능하다. 본 발명에서 설명하는 하드웨어, 소프트웨어, 또는 하드웨어와 소프트웨어의 조합으로 구현될 수 있다. 본 발명은 회로를 사용하여 구현될 수 있다. 즉, 한 개 이상의 프로그램 가능한 논리회로, 즉 ASIC(application specific integrated circuit) 또는 논리회로(AND, OR NAND gates) 또는 프로세싱 장치(예컨대, 마이크로 프로세서, 콘트롤러)로 구현가능하다.

[0071] 본 발명은 프로세서가 읽을 수 있는 기록매체에 프로세서가 읽을 수 있는 코드로서 구현하는 것도 가능하다. 프로세서가 읽을 수 있는 기록매체는 프로세서에 의해 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 프로세서가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있다. 또한 프로세서가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 프로세서가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0072] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어서는 안될 것이다.

부호의 설명

[0073]

100 : 데이터 저장 시스템 110 : 통신부

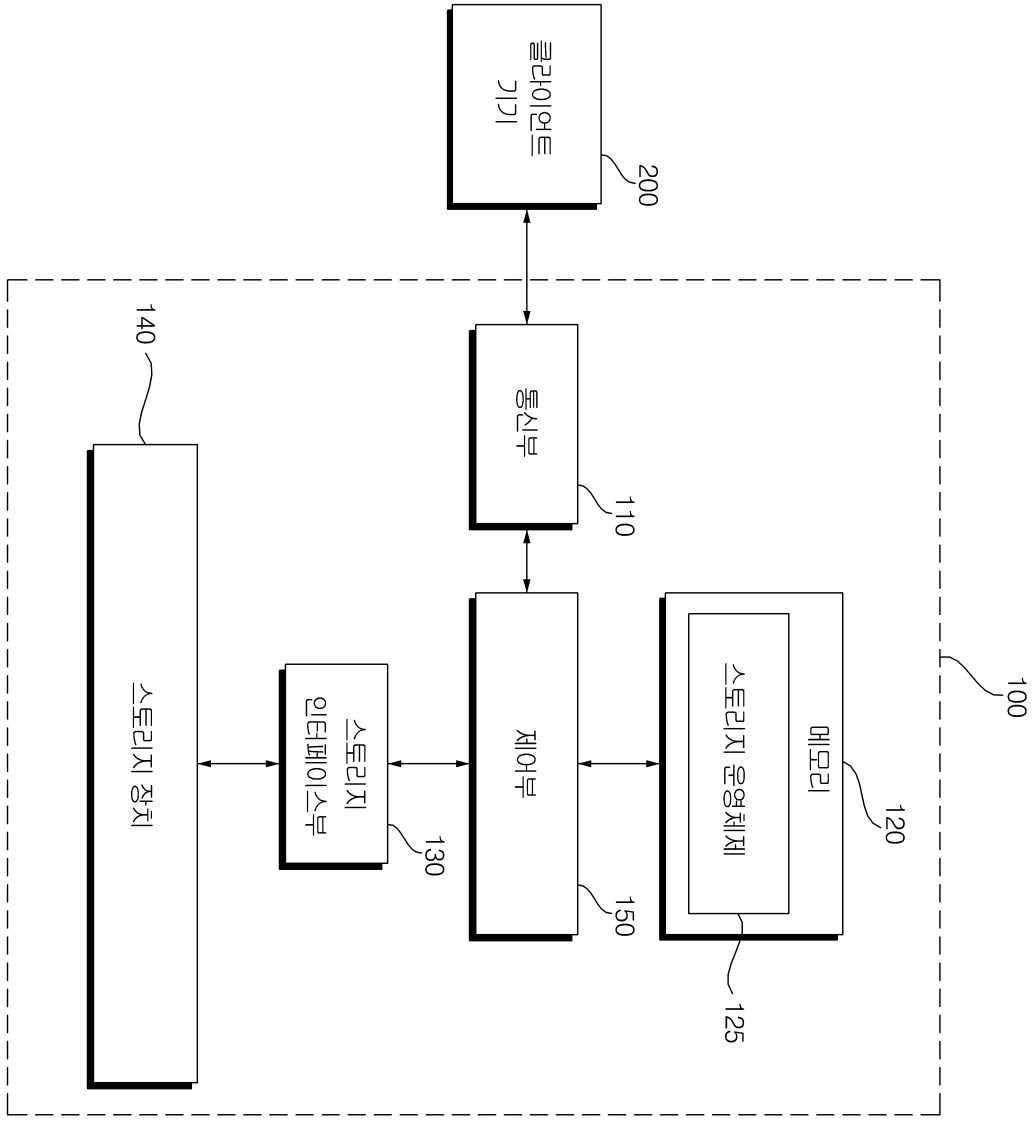
120 : 메모리 130 : 스토리지 인터페이스부

140 : 스토리지 장치 150 : 제어부

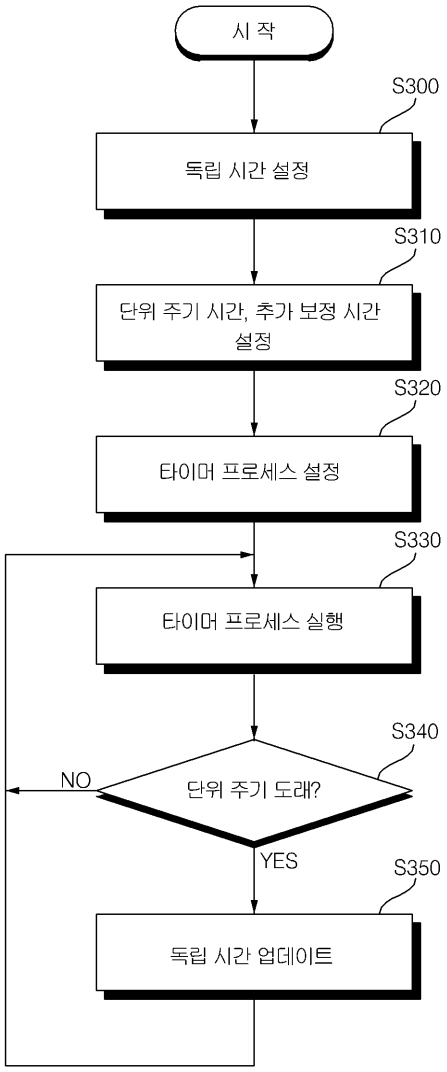
200 : 클라이언트 기기

도면

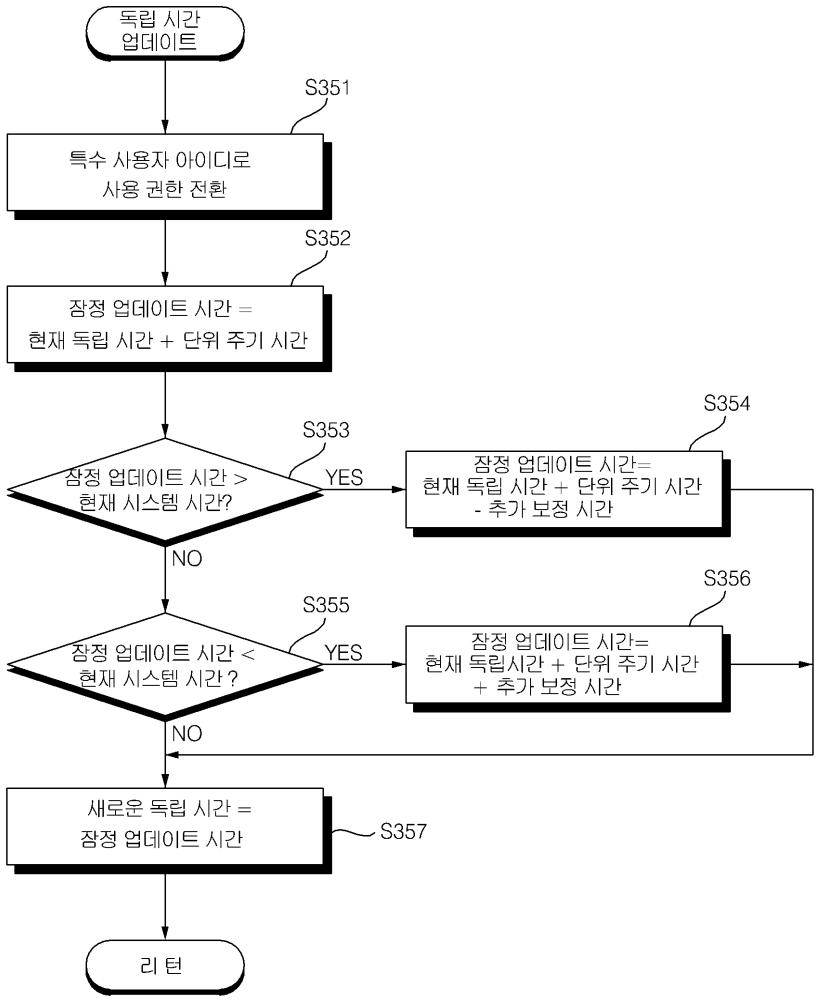
도면1


클라이언트 기기
200
통신부
110
제어부
150
메모리
120
스토리지 운영체제
125
스토리지 인터페이스부
130
스토리지 장치
140
100

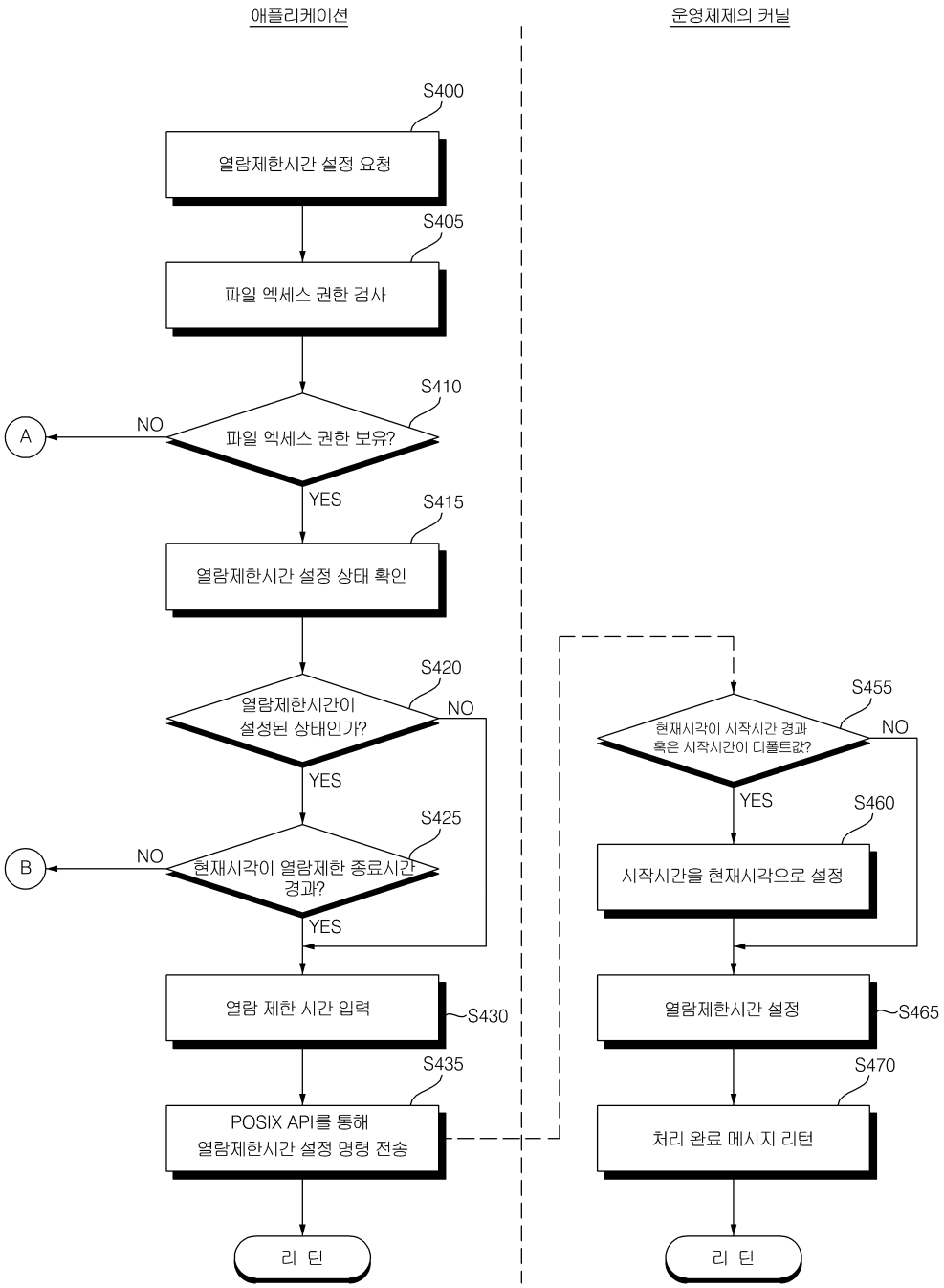
도면2


시 작
S300
독립 시간 설정
S310
단위 주기 시간, 추가 보정 시간 설정
S320
타이머 프로세스 설정
S330
타이머 프로세스 실행
S340
단위 주기 도래?
NO
YES
S350
독립 시간 업데이트

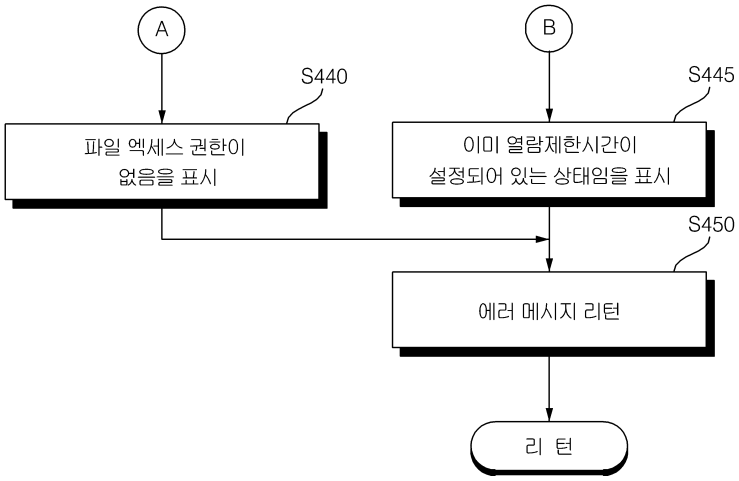
도면3


독립 시간
업데이트
S351
특수 사용자 아이디로
사용 권한 전환
S352
잠정 업데이트 시간 =
현재 독립 시간 + 단위 주기 시간
S353
잠정 업데이트 시간 >
현재 시스템 시간?
YES
S354
잠정 업데이트 시간=
현재 독립 시간 + 단위 주기 시간
- 추가 보정 시간
NO
S355
잠정 업데이트 시간 <
현재 시스템 시간 ?
YES
S356
잠정 업데이트 시간=
현재 독립시간 + 단위 주기 시간
+ 추가 보정 시간
NO
새로운 독립 시간 =
잠정 업데이트 시간
S357
리 턴

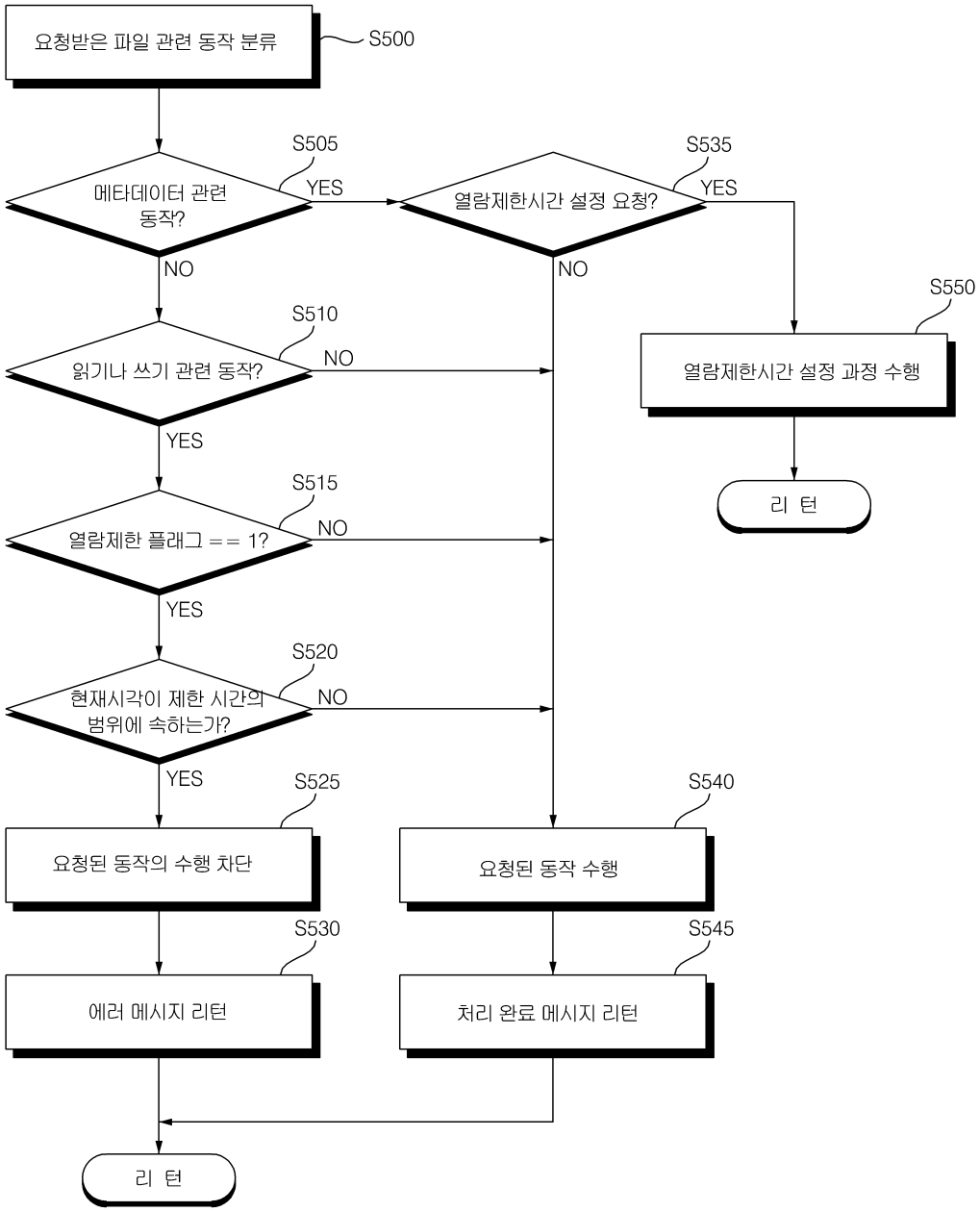
도면4


애플리케이션
운영체제의 커널
S400
열람제한시간 설정 요청
S405
파일 엑세스 권한 검사
S410
A
NO
파일 엑세스 권한 보유?
YES
S415
열람제한시간 설정 상태 확인
S420
열람제한시간이
설정된 상태인가?
NO
YES
S425
B
NO
현재시각이 열람제한 종료시간
경과?
YES
열람 제한 시간 입력
S430
S435
POSIX API를 통해
열람제한시간 설정 명령 전송
리 턴
S455
현재시각이 시작시간 경과
혹은 시작시간이 디폴트값?
NO
YES
S460
시작시간을 현재시각으로 설정
열람제한시간 설정
S465
S470
처리 완료 메시지 리턴
리 턴

도면5


A
B
S440
S445
파일 엑세스 권한이
없음을 표시
이미 열람제한시간이
설정되어 있는 상태임을 표시
S450
에러 메시지 리턴
리 턴

도면6


요청받은 파일 관련 동작 분류
S500
메타데이터 관련 동작?
S505
YES
NO
열람제한시간 설정 요청?
S535
YES
NO
S550
열람제한시간 설정 과정 수행
리 턴
읽기나 쓰기 관련 동작?
S510
NO
YES
열람제한 플래그 == 1?
S515
NO
YES
현재시각이 제한 시간의 범위에 속하는가?
S520
NO
YES
요청된 동작의 수행 차단
S525
요청된 동작 수행
S540
에러 메시지 리턴
S530
처리 완료 메시지 리턴
S545
리 턴