(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년05월06일
(11) 등록번호 10-2107277
(24) 등록일자 2020년04월27일

(51) 국제특허분류(Int. Cl.)
G06F 21/62 (2013.01) *G06F 21/31* (2013.01)
G06F 21/60 (2013.01) *H04L 29/06* (2006.01)
(52) CPC특허분류
G06F 21/6209 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2017-0089456
(22) 출원일자 2017년07월14일
심사청구일자 2017년07월14일
(65) 공개번호 10-2018-0016937
(43) 공개일자 2018년02월20일
(30) 우선권주장
1020160100945 2016년08월08일 대한민국(KR)
(56) 선행기술조사문헌
JP2005534104 A*
KR100985073 B1*
KR1020120128412 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
(주)나무소프트
서울특별시 금천구 디지털로 130, 남성프라자 에이스9차 1308호 (가산동)
(72) 발명자
우종현
서울특별시 영등포구 도신로29길 28, 108동 2001호 (영등포동, 영등포푸르지오)
(74) 대리인
강경돈

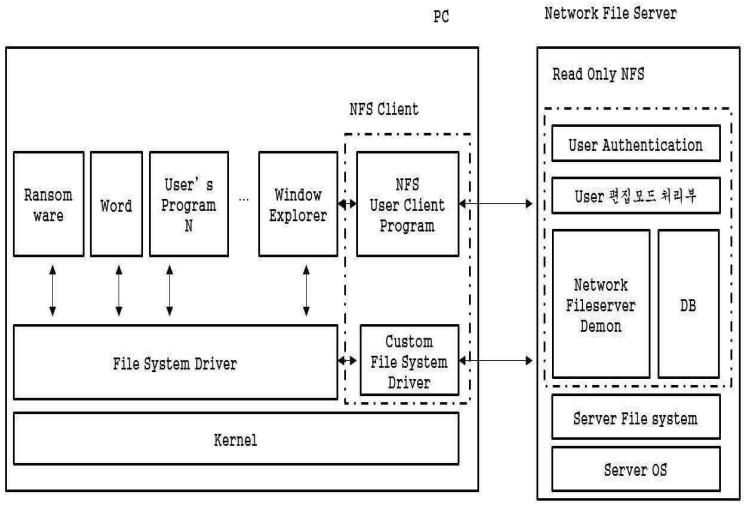
전체 청구항 수 : 총 2 항 심사관 : 구대성

(54) 발명의 명칭 **피싱 또는 랜섬웨어 공격을 차단하는 방법 및 시스템**

(57) 요 약

외부 공격 차단 시스템으로서, 네트워크 파일서버; 및 사용자 단말기 또는 서비스 서버에 설치되며 원격에 위치한 상기 네트워크 파일서버와 통신 연결되는 NFS 클라이언트(Network File Server Client)를 포함하고, 상기 네트워크 파일서버는, 상기 사용자 단말기 또는 서비스 서버에 네트워크 드라이브 형태로 마운트되는 상기 네트워크 파일서버 내의 보관 파일에 관한 상기 NFS 클라이언트로부터의 접근 또는 열기 요청이 있는 경우, 접근 또는 열기 요청을 한 사용자 정보 및 프로그램 정보 중 적어도 하나에 관하여 적격 여부를 판정하고, 판정 결과에 따라 부적격 판정이 이루어지는 경우 상기 접근 요청된 파일에 관한 접근을 차단하거나 또는 상기 열기 요청된 파일을 읽기 전용 모드로만 상기 NFS 클라이언트로 제공하는, 외부 공격 차단 시스템이 제공된다.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/604 (2013.01)
H04L 63/1466 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 S2369524
부처명 중소기업청
연구관리전문기관 중소기업기술정보진흥원
연구사업명 상거래 정보유출 방지를 위한 POS용 보안클라우드 서비스 개발 사업
연구과제명 기업서비스연구개발사업
기 여 율 1/1
주관기관 (주)나무소프트
연구기간 2016.04.05 ~ 2017.04.04

명 세 서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

외부 공격 차단 시스템으로서,

네트워크 파일서버; 및 사용자 단말기 또는 서비스 서버에 설치되며 원격에 위치한 상기 네트워크 파일서버와 통신 연결되는 NFS 클라이언트(Network File Server Client)를 포함하고,

상기 NFS 클라이언트는,

상기 사용자 단말기 또는 서비스 서버에 네트워크 드라이브 형태로 마운트되는 상기 네트워크 파일서버 내의 보관 파일에 관한 접근 또는 열기 요청이 어떤 프로그램을 통한 요청인지를 확인하고, 상기 요청에 프로그램 정보를 추가하여 상기 네트워크 파일서버로 전달하고,

상기 네트워크 파일서버는,

수신된 프로그램 정보에 근거하여 해당 프로그램이 사전 지정된 프로그램에 해당하는지 여부를 확인하여, 해당 프로그램이 사전 지정된 프로그램에 해당하지 않는 경우에는 상기 요청된 파일을 읽기 전용 모드로만 상기 NFS 클라이언트로 제공하되,

상기 NFS 클라이언트는,

상기 사용자 단말기 또는 상기 서비스 서버에 네트워크 드라이브 형태로 마운트된 상기 네트워크 파일서버 내의

보관 폴더 또는 파일에 관하여 사용자가 편집모드로 열기 또는 편집모드로의 전환을 선택 조작할 수 있도록, 편집 모드로 전환된 폴더 또는 파일이 편집모드로 실행되고 있음을 시각적으로 구별할 수 있는 아이콘을 해당 파일의 아이콘에 함께 표출하는 선택 정보를 제공하고,

상기 네트워크 파일서버는,

상기 편집모드로 열기 또는 상기 편집모드로의 전환이 선택된 상태에서 상기 NFS 클라이언트로부터의 파일 열기 또는 파일 변경 요청이 있는 경우, 파일 열기 또는 파일 변경을 허가하고, 상기 편집모드로 열기 또는 상기 편집모드로의 전환이 선택된 상태에서 이루어진 요청이 아닌 경우라면, 상기 열기 요청된 파일을 읽기 전용 모드로만 상기 NFS 클라이언트로 제공하거나 또는 상기 파일 변경 요청을 불허하는, 외부 공격 차단 시스템.

청구항 11

삭제

청구항 12

제10항에 있어서,

응용프로그램의 속성에 따라 특정 파일의 동작을 위해서는 해당 파일과 연관된 참조 파일들을 함께 동작시켜야 하는 경우,

상기 네트워크 파일서버는, 상기 특정 파일에 관한 편집모드로의 전환 또는 종료를 실행할 때 상기 참조 파일 또는 상기 참조 파일이 속한 폴더도 편집모드로의 전환 또는 종료를 함께 실행하는, 외부 공격 차단 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 피싱(fishing) 또는 랜섬웨어(ransomware) 공격을 차단하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 해커들이 배포하는 피싱과 랜섬웨어가 갈수록 다양화되면서 점점 더 사용자들의 데이터가 위협받고 있다. 일반적으로 피싱이란 사용자의 단말기에 저장된 데이터를 유출하는 공격으로 사용자 단말기에 존재하는 계정정보나 전자인증서, 주요 데이터 등을 탈취하는 공격을 의미한다. 또한, 랜섬웨어란 사용자의 단말기에 저장되었거나 연결된 네트워크 저장소에 보관된 데이터를 사용자가 접근할 수 없도록 암호화한 후, 금전을 요구하는 공격 기법을 말한다. 최근에는 데이터를 유출한 후 사용자가 사용하지 못하게 하는 것에서부터 단말기의 디스크 파티션을 조작하여 아예 PC 단말기를 사용하지 못하게 하는 것까지 그 방법과 형식이 다양해지고 있다.

[0003] 이러한 피싱 공격에 대응하는 기존 방법으로는 PC내 저장공간을 암호화하고 해당특정 저장공간에 접근하는 프로세스가 사전에 지정된 프로세스인지 아닌지를 확인하는 기술이 사용되었으나, 해당 저장공간을 암호화하였더라도 암호화된 저장공간을 구성한 파일을 탈취하여 복호화하는 경우가 발생하고 있다.

[0004] 또한 랜섬웨어 공격에 대응하는 기존 방법으로는 PC 내 자료를 안전한 저장 영역으로 주기적으로 백업하여 PC가 랜섬웨어에 걸려도 백업된 자료를 가져와 사용하는 방법이 있다. 그러나 이 방식에 의하더라도 최근 작업했던 파일에 대한 손실은 피할 수 없는 문제점이 있다. 다른 기존 방법으로는 파일 서버에 접근하는 프로세스를 사전에 등록해놓고 PC 내에서 인가된 프로세스만 자료에 접근 가능하도록 함으로써, 사전에 등록되지 않은 프로세스가 데이터 접근시 이를 차단하여 랜섬웨어 프로세스가 자료에 접근하지 못하도록 하는 방법이 있다. 그러나 이 방식은 인가된 프로세스를 사전에 등록해야 하는 불편함이 발생하고, 수시로 프로그램이 설치되는 경우 프로세스를 매번 번잡하게 등록할 수 없는 한계점도 있다.

[0005] 또한 최근에는 랜섬웨어 자체가 PC 내 보관된 데이터만을 암호화 하는 것이 아니라 PC 전체를 암호화하거나, PC에 마운트된 디스크 전체를 암호화하여 랜섬머니를 요구하는 사례까지 발생하고 있는 바, 데이터 암호화를 방지하는 것만으로는 더 이상 충분하지 않는 상황이 발생하고 있다

[0006] 게다가 PC뿐만 아니라 리눅스나 유닉스 서비스 서버에 놓여있는 전체 데이터까지 한번에 암호화하는 공격까지 발생하고 있어 근본적인 대안이 필요한 상황이다. 따라서 피싱을 예방하기 위하여 PC나 서비스서버에 생성한 암

호화된 저장공간이 탈취되지 않도록 하면서, 랜섬웨어가 PC나 서비스서버에서 구동된다 하더라도 이에 따른 공격을 차단할 수 있는 새로운 기술이 필요하다.

발명의 내용

해결하려는 과제

[0007] 본 발명은 PC나 서비스서버에서 네트워크 파일서버가 연결될 수 있도록 하는 드라이브와 클라이언트 프로그램을 제공하여 사전에 지정된 프로그램만이 해당 저장공간 내 파일에 엑세스할 경우 파일서버가 접근을 허용하고 그 이외에 경우는 접근을 차단하여 효과적으로 피싱을 차단하는 것과 일반적인 PC나 서비스서버 내 프로그램들이 네트워크 드라이브에 없던 파일을 생성할 수는 있지만, 사전에 지정된 프로그램의 파일 쓰기 요청을 제외하고 모든 프로그램이 네트워크 파일서버내 보관하던 데이터를 암호화하거나 변경, 삭제하지 못하도록 읽기 전용 모드로만 네트워크 파일서버가 PC나 서비스 서버에 파일을 제공하여 효과적으로 랜섬웨어를 차단하는 방법 및 시스템을 제공한다. 보다 구체적으로 PC나 서비스서버에 커스텀 파일시스템 드라이버가 설치되어 네트워크 파일서버 내 보관중인 파일 및 폴더가 드라이브나 파티션으로 마운트되어 사용될 수 있게 하고,

[0008] 사전에 지정된 프로그램을 통해서 네트워크 파일서버내에 존재하는 특정 파일이나 폴더에 접근하지 않는 한, 네트워크 파일서버는 파일에 접근할 수 없게 하는 방법 및 시스템을 제공하며, 사전에 지정된 네트워크 파일서버 사용자 클라이언트 프로그램을 통해서 특정 파일이나 폴더에 쓰기가 가능하도록 편집모드로 설정하지 않는 한, PC나 서비스서버에 마운트된 드라이브 내에서 파일열기 요청이 발생하면 네트워크 파일서버는 읽기 모드로만 파일을 PC에게 열수 있게 하는 방법 및 시스템을 제공한다.

과제의 해결 수단

[0009] 본 발명의 일 측면에 따르면, 피싱 또는 랜섬웨어 공격 차단 시스템으로서, 네트워크 파일서버; 및 사용자 단말기 또는 서비스 서버에 설치되며 원격에 위치한 상기 네트워크 파일서버와 통신 연결되는 NFS 클라이언트(Network File Server Client)를 포함하고, 상기 네트워크 파일서버는, 상기 사용자 단말기 또는 서비스 서버에 네트워크 드라이브 형태로 마운트되는 상기 네트워크 파일서버 내의 보관 파일에 관한 상기 NFS 클라이언트로부터의 접근 또는 열기 요청이 있는 경우, 접근 또는 열기 요청을 한 사용자 정보 및 프로그램 정보 중 적어도 하나에 관하여 적격 여부를 판정하고, 판정 결과에 따라 부적격 판정이 이루어지는 경우 상기 접근 요청된 파일에 관한 접근을 차단하거나 또는 상기 열기 요청된 파일을 읽기 전용 모드로만 상기 NFS 클라이언트로 제공하는, 피싱 또는 랜섬웨어 공격 차단 시스템이 제공된다.

[0010] 본 발명의 다른 측면에 따르면, 랜섬웨어 공격 차단 시스템으로서, 네트워크 파일서버; 및 사용자 단말기 또는 서비스 서버에 설치되며 원격에 위치한 상기 네트워크 파일서버와 통신 연결되는 NFS 클라이언트(Network File Server Client)를 포함하고, 상기 네트워크 파일서버는, 상기 사용자 단말기 또는 상기 서비스 서버에 네트워크 드라이브 형태로 마운트되는 상기 네트워크 파일서버 내의 보관 파일에 관한 상기 NFS 클라이언트로부터의 파일 변경 요청이 있는 경우, 변경 요청을 한 사용자 정보 및 프로그램 정보 중 적어도 하나에 관하여 적격 여부를 판정하고, 판정 결과에 따라 부적격 판정이 이루어지는 경우 상기 파일 변경 요청을 불허하는, 피싱 또는 랜섬웨어 공격 차단 시스템이 제공된다.

[0011] 본 발명의 또 다른 측면에 따르면, 랜섬웨어 공격 차단 시스템으로서, 네트워크 파일서버; 및 사용자 단말기 또는 서비스 서버에 설치되며 원격에 위치한 상기 네트워크 파일서버와 통신 연결되는 NFS 클라이언트(Network File Server Client)를 포함하고, 상기 NFS 클라이언트는, 상기 사용자 단말기 또는 상기 서비스 서버에 네트워크 드라이브 형태로 마운트되는 상기 네트워크 파일서버 내의 보관 파일에 관하여 사용자가 편집모드로의 전환 및 종료를 선택할 수 있도록 하는 선택 정보를 제공할 수 있다. 또한, 상기 네트워크 파일서버는, 상기 NFS 클라이언트로부터의 파일 열기 또는 변경 요청이 있는 경우, 상기 열기 또는 변경 요청이 상기 편집모드로의 전환이 선택된 상태에 따른 요청이 아닌 경우, 상기 열기 요청된 파일을 읽기 전용 모드로만 상기 NFS 클라이언트로 제공하거나 또는 상기 파일 변경 요청을 불허하는, 피싱 또는 랜섬웨어 공격 차단 시스템이 제공된다.

[0012] 본 발명의 실시예에 따라 랜섬웨어 공격 방지 시스템은 아래와 같이 동작할 수 있다.

[0013] 일 실시예에서, 네트워크 파일서버는, 윈도우 탐색기의 파일접근 요청에 대해서는 Read/Write로 파일을 사용할 수 있다. 반면, 윈도우 탐색기이외에 파일요청에 대해서는 Read Only로 파일을 제공할 수 있다.

[0014] 다른 실시예에서, 네트워크 파일서버는, 사전에 지정된 프로그램의 파일접근 요청에 대해서는 Read/Wirte로 파

일을 제공할 수 있고, 그 이외의 경우에 대해서는 Read Only로만 파일을 제공할 수 있다.

[0015] 또 다른 실시예에서, 네트워크 파일서버는, 사전에 지정된 프로그램의 파일 접근 요청에 대해서만 Read로 파일을 제공할 수 있고, 그 이외의 경우에 대해서는 접근을 거부(Access deny)할 수 있다.

[0016] 본 발명의 실시예에 따라 피싱 공격 방지 시스템은 아래와 같이 동작할 수 있다.

[0017] 일 실시에에서, 사전에 네트워크 파일시스템 클라이언트 프로그램이 설치될 때 접근을 허용하려고 하는 프로그램을 선택하고, 선택된 프로그램의 바이너리 파일의 해쉬값을 추출하여 서버에 전달하여, 추후 서버에 파일을 요청하는 프로그램이 어떤 프로그램인지를 검증할 수 있도록 준비할 수 있다.

[0018] 여기서, 네트워크 파일시스템 내에 파일요청이 발생하게 되면, 네트워크 파일시스템 커스텀 드라이브가 요청하는 프로그램을 확인하고, 해당 프로그램의 해쉬값을 생성하여 서버에 전달할 수 있다. 또한, 네트워크 파일서버는 사전에 등록되어 있던 프로그램인지 아닌지 확인하여, 사전에 등록되어 있던 프로그램이라면 파일을 제공하지만 그 이외의 경우는 파일을 제공하지 않을 수 있다.

발명의 효과

[0019] 본 발명의 실시예에 의하면, 사용자가 PC 단말기를 조작하여 다양한 프로그램을 사용하는데 있어서, 해커의 속임수에 의해 악성코드를 실행하여 랜섬웨어가 PC 내 단말기에 작동된다 하더라도 PC 단말기와 연결된 네트워크 드라이브 내의 사용자 데이터를 보호할 수 있도록 하는 효과가 있다. 이를 통해 랜섬웨어 대비를 위하여 수시로 백업 작업을 수행하지 않아도 되고, 인가된 프로세스만 접근하도록 설정하기 위하여 별도의 프로세스를 등록하는 번잡함도 극복할 수 있게 된다.

도면의 간단한 설명

[0020] 도 1은 읽기 전용으로 작동하는 네트워크 파일서버 및 클라이언트 프로그램이 설치된 PC를 포함하는 전체 시스템 블록도.

도 2는 본 발명의 실시예예 따라, 읽기 전용으로 파일을 열었을 때 타이틀 바에 읽기 전용이 표시되는 화면 예시.

도 3은 윈도우 탐색기가 아닌 DOS 커맨드 창에서 네트워크 파일시스템 드라이브 내에 있는 파일의 이름을 명령어로 변경하려고 한 경우에 대해서 거절하는 화면 예시.

도 4는 윈도우 탐색기에서 네트워크 파일서버의 저장공간이 드라이브로 마운트된 후에, 사용자가 윈도우 탐색기에 부가적으로 설치된 네트워크 파일서버 클라이언트 프로그램을 이용하여 네트워크 파일서버내 저장공간에 있는 파일을 '편집모드 전환'하려는 경우에 대한 화면 예시.

도 5는 특정 사용자 ID에 의해서 편집 모드로 열린 파일이 윈도우 탐색기에 표시될 때 자물쇠 모양의 아이콘이 파일 아이콘 위에 함께 표시되도록 하는 화면 예시.

도 6은 특정 사용자 ID에 의해서 잠겨있는 파일을 네트워크 파일서버에서 해제되도록 할 때 편집 모드 종료 명령을 전송할 수 있게 하는 네트워크 파일서버 클라이언트 프로그램 실시 화면 예시.

발명을 실시하기 위한 구체적인 내용

[0021] 본 발명은 다양한 변환을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변환, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0022] 본 발명을 설명함에 있어서, 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 본 명세서의 설명 과정에서 이용되는 숫자(예를 들어, 제1, 제2 등)는 하나의 구성요소를 다른 구성요소와 구분하기 위한 식별기호에 불과하다.

[0023] 또한, 명세서 전체에서, 일 구성요소가 다른 구성요소와 "연결된다" 거나 "접속된다" 등으로 언급된 때에는, 상기 일 구성요소가 상기 다른 구성요소와 직접 연결되거나 또는 직접 접속될 수도 있지만, 특별히 반대되는 기재가 존재하지 않는 이상, 중간에 또 다른 구성요소를 매개하여 연결되거나 또는 접속될 수도 있다고 이해되어야

할 것이다.

[0024] 또한, 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "부", "모듈" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하나 이상의 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 조합으로 구현될 수 있음을 의미한다.

[0025] 도 1은 읽기 전용으로 작동하는 네트워크 파일서버 및 클라이언트 프로그램이 설치된 PC를 포함하는 전체 시스템 블록도이다. 이하, 본 발명의 실시예에 따른 랜섬웨어 공격을 차단하는 방법 및 시스템에 관하여, 도 1의 시스템 블록도를 중심으로, 도 2 ~ 도 6을 함께 참조하여 본 발명을 설명하기로 한다. 본 명세서에서는 PC와 같은 사용자 단말기가 네트워크 파일서버에 세션 연결되는 경우를 중심으로 설명하지만, 서비스 서버가 네트워크 파일서버에 세션 연결되는 경우에도 이하의 설명에서와 동일 유사하게 구현될 수 있음은 자명하다.

[0026] 도 1을 참조하면, 사용자의 PC(Personal Computer)에는 네트워크 파일서버 클라이언트(NFS Client)가 설치된다. 사용자의 PC는 네트워크 파일서버 클라이언트를 통해서 원격의 네트워크 파일서버(Network File Server, 이하 NFS)와 통신 연결된다.

[0027] 본 발명의 실시예에서, 정상적인 사용자인지 확인하기 위하여 네트워크 파일서버클라이언트 프로그램(도 1의 NFS User Client Program)을 구동하여 사용자 인증을 정상적으로 끝마치면, PC에 설치된 커스텀 파일시스템 드라이버(Custom File System Driver)를 통해서 네트워크 파일서버(NFS)의 저장공간이 PC의 드라이브로 마운트될 수 있다. 즉, 이때 PC에 마운트되는 드라이브는 가상 드라이브(virtual drive)이다.

[0028] 이후, 사용자가 네트워크 파일서버에 맵핑된 드라이브에 보관중인 파일에 대해 윈도우 탐색기 또는 기타 일반 응용프로그램으로 열기를 시도하면, 커스텀 파일시스템 드라이버는 시도된 파일 열기 요청이 어떤 프로그램을 통한 요청인지를 확인하여, 파일 열기 요청에 사용자 정보 및 프로그램명 중 적어도 하나를 추가하여 네트워크 파일서버에 보낸다. 본 명세서에서는 설명의 편의 및 집중을 위해, 상기 사용자 정보로서 사용자 ID가 활용되는 것으로 가정하여 설명하기로 한다. 다만, 해당 사용자를 식별할 수 있는 정보라면 사용자 ID 이외에도 다양한 사용자 정보가 활용될 수 있음은 물론이다.

[0029] 다만, 구현 방식에 따라서 PC에서 네트워크 파일서버 클라이언트가 구동될 때 네트워크 파일서버에서 사용자 아이디와 암호를 인증했다면, 해당 접속 세션에 대해서는 해당 아이디로 간주하고 별도의 아이디값을 전달하지 않게 구성할 수 있음은 자명하다.

[0030] 일반적인 파일서버는 파일을 요청하는 단말기의 사용자 계정이 인증되어 상호간의 세션 연결이 이루어진 이후에는 데이터를 요청하는 프로그램을 검토하지 않는다. 즉, 종래 기술에 의할 때, 네트워크 파일서버 클라이언트 드라이버는 파일 서버에게 파일을 요청하였을 뿐, 어떤 프로그램이 어떤 파일을 요청했는지를 정보를 서버에게 제공하지 않았다.

[0031] 그러나 랜섬웨어를 파일 서버 중심에서 막기 위해서는 현재 파일을 요청하는 주체가 어떤 단말기인지, 어떤 사용자인지를 넘어서 어떤 프로그램인지까지 함께 전달해야 파일서버 관점에서 판단하여, 사전에 지정한 프로그램인 경우에 한하여 파일을 제공할 필요가 있다.

[0032] 따라서, 본 발명에서는 파일에 접근하려는 프로그램의 식별값을 커스텀 파일시스템 드라이버가 함께 네트워크 파일서버에 요청하고, 네트워크 파일서버 데몬은 수신한 프로그램 식별값이 사전에 지정된 프로그램 식별값과 다른 경우 읽기 전용으로만 데이터를 제공하는 것으로 구동된다.

[0033] 구성에 따라서는 네트워크 파일서버 데몬은 파일을 요청하는 프로그램뿐만 아니라 사용자 ID를 사전에 지정하여 사전에 지정한 ID가 아닌 경우, 해당 파일 열기 요청에 대한 열람이 읽기 전용 모드로 이루어질 수 있도록 커스텀 파일시스템 드라이버에게 제공할 수 있다. 이에 따라, 사전에 지정한 프로그램이 OS의 기본 파일탐색기가 아닌 경우 네트워크 파일서버로부터 제공된 파일은 PC에서 읽기 전용으로만 접근될 수 있게 작동될 수 있다.

[0034] 또한 구성을 바꾸어, 네트워크 파일서버 클라이언트 드라이버가 구동될 때 서버로부터 서버에 요청 가능한 프로그램 목록을 사전에 내려 받은 후, 파일을 요청하는 프로그램이 사전에 지정된 프로그램이 아니라면 클라이언트 프로그램 모듈에서 커널 수준에서 "접근권한이 없습니다."라는 메시지를 파일을 요청한 프로그램에게 회신을 줄 수도 있을 것이다.

[0035] 도 2는 본 발명의 실시예예 따라, 읽기 전용으로 파일을 열었을 때 타이틀 바에 읽기 전용이 표시되는 화면 예

시이다.

[0036] 또한 본 발명의 실시예에 의할 때, 특정 사용자 프로그램이 읽기/쓰기 모드로 드라이브 내 파일을 열도록 작동하는 경우, 커스텀 파일시스템 드라이버가 현재 요청이 어떤 프로그램에 의한 요청인지를 확인하여, 읽기/쓰기 모드로 파일 열기를 요청하면서 사용자 ID 및 프로그램명 중 적어도 하나를 추가하여 네트워크 파일서버에 보낼 수 있다.

[0037] 이 경우, 본 발명의 실시예에 따른 네트워크 파일서버 데몬은 읽기/쓰기 모드로 들어온 파일 접근 요청을 거부 메시지를 커스텀 파일시스템 드라이버로 전송할 수 있다. 이에 따라, 커스텀 파일시스템 드라이버는 다시 이를 수신하여 프로그램에 전송할 수 있다.

[0038] 또한, 또다른 작동 방법으로는 일반적인 프로그램이 읽기/쓰기 모드로 파일서버 내 파일 열기를 시도하는 경우, 커스텀 파일시스템 드라이버는 현재 요청이 어떤 프로그램에 의한 요청한 것인지 확인하고, 읽기/쓰기 모드로 파일 열기를 요청하면서 프로그램명을 추가하여 네트워크 파일서버에 보낼 수 있다. 이 경우, 네트워크 파일서버 데몬은 해당 파일 열기 요청에 대해 사전에 지정된 프로그램이 아닌 경우 읽기 전용 파일열기 모드로 해당 파일을 커스텀 파일시스템 드라이버에게 제공한다. 이에 따라, 사전에 지정된 프로그램이 아닌 경우 네트워크 파일서버로부터 제공된 파일은 PC에서 읽기 전용으로만 제공 된다.

[0039] 이와 같이 작동하는 프로그램들은 대체로 워드나 파워포인트와 같은 일반 프로그램들로서 오피스 프로그램 자체가 파일시스템에서 파일을 열려고 할 때, 읽기/쓰기모드로 열려고 하는데 파일 시스템으로부터 읽기 전용 파일 속성으로 파일이 제공되면 자동으로 읽기 전용 모드로 파일을 열람시킨다.

[0040] 또한 본 발명의 실시예에 의할 때, 사용자가 네트워크 파일서버와 맵핑된 드라이브에 윈도우 탐색기나 일반 응용프로그램을 이용하여 파일을 최초 생성하는 경우, 네트워크 파일서버 클라이언트 내 커스텀 파일시스템 드라이버는 프로그램, 쓰기 파일 정보를 추가하여 파일 생성 요청을 네트워크 파일서버에게 전달할 수 있다.

[0041] 이 경우, 네트워크 파일서버 데몬은 네트워크 파일서버 내의 파일시스템이 허용하는 범위내에서 해당 파일을 생성할 수 있다. 여기서, 서버 내 파일시스템이 허용하는 범위를 예로 들면 동일한 파일명이 서버의 파일시스템에 존재하지 않거나, 서버의 파일시스템에 추가로 저장할 용량이 남아있는 경우이거나, 생성을 시도하는 파일명 규칙이 서버의 파일시스템의 제한을 초과하지 않는 경우 등일 수 있다.

[0042] 네트워크 파일서버에 파일이 생성된 경우, 네트워크 파일서버 데몬은 해당 사용자ID가 해당 파일에 대해서 쓰기 권한을 갖고 있는 것을 쓰기 권한 DB(도 1의 DB 참조)에 갱신시켜 놓고서, 커스텀 파일시스템 드라이버에게 해당 파일이 읽기/쓰기 모드로 열람될 수 있도록 전달한다.

[0043] 이 경우, 커스텀 파일시스템 드라이버는 프로그램에게 파일에 대한 읽기/쓰기 모드로 문서가 열려있음을 전달하고, 프로그램이 종료되기 전까지 해당 파일에 대한 수정을 할 수 있게 한다.

[0044] 이후, 프로그램이 종료될 때, 파일을 닫는 것이 커스텀 파일시스템 드라이버에 의해 감지되는 경우, 커스텀 파일시스템 드라이버는 파일 닫힘 이벤트를 네트워크 파일서버 데몬에 전달하고, 이를 수신한 네트워크 파일서버 데몬은 해당 파일에 대한 쓰기 권한정보를 갖고 있는 쓰기 권한 DB에서 해당 사용자 ID를 제거할 수 있다.

[0045] 여기서, 운영체제 파일시스템 마다 다양한 파일 생성 및 닫기 함수가 존재할 수 있다. 예를 들어, 윈도우 운영체제만 하더라도 파일을 생성을 할 때 Openfile(), Createfile()로 생성할 수도 있고, 파일을 닫을때도 Close(), Closefile()로 닫을 수 있어서 명령 하나 하나에 충실하기 보다는 전체적인 동작 절차를 중심으로 본 명세서를 기술한다.

[0046] 또한 여기서, 네트워크 파일서버 클라이언트는 윈도우 탐색기에 확장하여 컨텍스트 메뉴로 구현된 프로그램일 수 있고, 별도의 프로그램으로 구동될 수 있는 등 그 구현 형식의 제한은 없다.

[0047] 또한 본 발명의 실시예에 의할 때, 사용자가 네트워크 파일서버와 맵핑된 드라이브에 윈도우 탐색기나 일반 응용프로그램을 이용하여 파일을 변경을 요청하는 경우, 커스텀 파일시스템 드라이버는 네트워크 파일서버내에 위치한 파일에 대해서 파일변경 명령을 감지하고, 해당 파일정보에 파일변경 명령정보, 현재 명령이 어떤 프로그램에 의해서 생성되었는지에 대한 프로그램 정보 및 사용자 ID 중 적어도 하나를 추가하여 네트워크 파일서버로 보낼 수 있다.

[0048] 여기서, 파일 변경 요청은 예를 들어 파일 암호화, 파일 삭제, 파일 이름 변경, 파일 이동, 파일 시간 변경, 파일 본문내용 변경, 파일 바이너리값 변경 등에 관한 요청을 의미한다.

[0049] 네트워크 파일서버 데몬은 해당 사용자 세션에 해당 작업대상 파일에 쓰기 권한을 갖는 ID인지여부를 쓰기 권한 DB를 통해서 확인할 수 있다. 확인 결과에 따라, 네트워크 파일서버 데몬은 해당 작업대상 파일에 쓰기 권한이 부여된 사용자 ID로부터의 파일변경 요청인 경우에만 파일변경 명령을 허용할 수 있다.

[0050] 다만, 경우에 따라서는, 본 발명의 다른 실시예에 의할 때, 해당 사용자 ID에 쓰기 권한이 부여되지 않은 경우라 하더라도, 해당 작업요청을 요청한 프로그램이 윈도우 탐색기일 경우에는 파일삭제 명령을 허용할 수도 있다. 여기서, 파일삭제 명령을 생성한 것이 윈도우 탐색기인 경우는 사용자의 직접적인 조작으로 간주하고, 파일삭제 명령을 정상적으로 처리해주어도 무방할 수 있기 때문이다. 이에 관한 일 예시로서, 도 3은 윈도우 탐색기가 아닌 DOS 커맨드 창에서 네트워크 파일시스템 드라이브 내에 있는 파일의 이름을 명령어로 삭제하려고 한 경우에 대해서 거절하는 화면을 예시하고 있다. 즉, 도 3은 윈도우 탐색기가 아닌 다른 응용프로그램을 통해서 쓰기 권한이 부여되지 않은 ID의 사용자가 파일삭제를 시도한 경우 이를 허용하지 않는 경우를 보여주고 있다.

[0051] 위와 비슷한 취지로, 구현 방식에 따라서, 사전에 지정한 프로그램에 의한 읽기 명령인 경우에는 해당 파일에 관한 열람을 허용하지만, 그 외의 프로그램에 의한 읽기 명령은 네트워크 파일서버 측(보다 구체적으로는 네트워크 파일서버 데몬)에서 이를 불허(읽기 금지)할 수도 있다.

[0052] 실제로 공인인증서를 일반적인 네트워크 파일서버에 저장하고 운영체제에 마운트되어 있다면 운영체제 상에서 작동하는 모든 프로그램이 접근(읽기)이 가능하지만, 공인인증서 클라이언트 프로그램만 접근되도록 사전에 설정되었다면 공인인증서 클라이언트 프로그램에 의한 파일 열기 요청에 의해서만 파일을 제공하고 그 이외에 모든 프로그램에 의한 파일 열람 요청을 차단할 수 있다. 또한 구성에 따라서 공인인증서 생성 프로그램만이 해당 네트워크 드라이브에 접근하여 파일을 생성할 수 있도록 제한 한다면 사전에 지정된 공인인증서 생성 프로그램만이 파일을 쓸 수 있음도 자명하다.

[0053] 네트워크 파일서버 데몬은 파일변경 명령을 수행한 후 커스텀 파일시스템 드라이버에게 결과를 전달할 수 있다. 이때, 최종적으로 작업요청에 대한 결과는 커스텀 파일시스템 드라이버를 통해 해당 작업요청 프로그램에게 전달되어 사용자에게 결과가 표시된다.

[0054] 이상에서는 사전에 지정된 프로그램이 윈도우 탐색기를 예로 들었지만, 이와 같이 예외 처리되는 프로그램의 종류 또는/및 프로그램명은 운영체제에 따라서 상이할 수 있다. 일 예로 MS 윈도우에서는 사용자가 직접 파일을 조작할 수 있는 프로그램 명이 윈도우 탐색기이지만, Apple Mac OS에서는 Finder로 작동하며 Linux의 X윈도우에서는 파일탐색기 임이 바로 그러하다.

[0055] 또한, 네트워크 파일서버가 처리를 완료한 이후 향후 처리 절차에 대해서는, 운영체제 작동방식에 따라서 상이해질 수 있다. 네트워크 파일서버가 최종 동작을 마친 후에 커스텀 파일시스템 드라이버에 처리된 것을 알려줄 수도 있지만, 커스텀 파일시스템 드라이버가 네트워크 파일서버에 작업요청이 어떻게 이행되었는지를 확인할 수도 있을 것이다.

[0056] 또한, 이상에서는 해당 프로그램 또는 사용자 ID가 해당 작업파일에 쓰기 권한이 부여되고 있는지 여부에 따라 파일변경 처리의 허용여부를 결정하는 경우를 주로 설명하고 있지만, 이외에도 다양한 변형이 가능하다. 예를 들어, 해당 사용자로 쓰기 권한이 부여되어 있는지에 관한 대조 절차는 생략될 수도 있다.

[0057] 일 예로, 도 4에 도시된 바와 같이, 해당 사용자가 의도적인 조작을 통해서 사전에 지정된 프로그램이 아니라 일반 프로그램으로 파일을 열람하더라도 편집이 가능하게 파일을 '편집모드 전환'하여 여는 경우에는 사전에 지정된 프로그램이 아니라 하더라도 파일서버가 해당 파일에 대해 읽기/쓰기 속성으로 파일을 제공하게 구현될 수 있다. 경우에 따라서, 랜섬웨어 공격이 아님이 명확히 구별될 수 있는 사용자의 의도적 조작 행위임이 인정되는 경우라면, 파일변경 요청을 허용하도록 구현할 수도 있기 때문이다. 여기서, 도 4는 윈도우 탐색기에서 네트워크 파일서버의 저장공간이 드라이브로 마운트된 후에, 사용자가 윈도우 탐색기에 부가적으로 설치된 네트워크 파일서버 클라이언트 프로그램을 이용하여 네트워크 파일서버내 저장공간에 있는 파일을 '편집모드 전환'하려는 경우에 대한 화면 예시이다.

[0058] 이에 대한 구체적 구현 방식은 다음과 같을 수 있다. 네트워크 파일서버 클라이언트가 정상 인증된 사용자 ID로 특정 경로의 파일에 대해 편집모드로 전환을 선택하면, 네트워크 파일서버 상의 편집모드 처리부(도 1의 User 편집모드 처리부 참조)가 특정 경로의 파일이 이미 다른 사용자 ID에 의해서 쓰기가 되어있는지 확인할 수 있다. 이때, 다른 사용자 ID가 등록되어 있지 않은 경우, 편집모드 처리부는 쓰기 권한 DB 해당 파일에 사용자 ID를 쓰기 권한을 부여하여, 해당 사용자ID에 한하여 읽기/쓰기가 가능하도록 설정을 변경하고, 네트워크 파일서버 클라이언트에게 변경 완료를 알려줄 수 있으며, 읽기/쓰기로 전환된 문서에 대해서 해당 사용자가 사전에

지정되지 않은 프로그램으로 파일을 접근한다 하더라도 파일에 대해서 읽기/쓰기 모드로 네트워크 파일 서버가 파일을 제공한다.

[0059] 또한 구현 방식에 따라서 네트워크 파일서버 내의 파일이 편집모드로 전환될 때마다 강제로 네트워크 파일서버에 리비젼을 남기도록 구성될 수 있음은 자명하다. 이와 별개로 도 6에 도시된 바와 같이 사용자가 직접 '리비젼 생성'을 선택함으로써 리비젼 파일을 남길 수도 있음은 물론이다.

[0060] 상술한 바와 같이, 편집 모드롤 파일이 열린 경우, 도 5에 도시된 바와 같이 해당 파일이 편집 모드로 실행되고 있음을 시각적으로 구별시킬 수 있는 아이콘이 함께 표시될 수도 있다. 여기서, 도 5는 특정 사용자 ID에 의해서 편집 모드로 열린 파일이 윈도우 탐색기에 표시될 때 자물쇠 모양의 아이콘이 파일 아이콘 위에 함께 표시되도록 하는 화면 예시이다.

[0061] 또한 상술한 편집 모드는 사용자의 조작을 통해서 편집 모드 종료 처리될 수도 있다. 이에 관한 예시가 도 6에 도시되고 있으며, 여기서 도 6은 특정 사용자 ID에 의해서 잠겨있는 파일을 네트워크 파일서버에서 해제되도록 할 때 편집 모드 종료 명령을 전송할 수 있게 하는 네트워크 파일서버 클라이언트 프로그램 실시 화면 예시이다. 이때, 편집 모드 종료가 선택되는 경우, 네트워크 파일서버의 편집모드 처리부는, 해당 사용자가 더 이상 쓰기 모드로 해당 파일을 열지 못하도록 쓰기 권한 DB에서 해당 경로의 파일에 대한 해당 사용자 ID를 삭제할 수 있다.

[0062] 또한 상술한 편집 모드로의 전환 또는/및 편집 모드 종료의 처리는 단위 파일 단위로 이루어질 수도 있지만, 경우에 따라서는 파일 구동 상 필요한 범위 내에서 혹은 설정된 범위 내에서 복수의 파일에서 동시에 이루어질 수도 있다. 일 예로, 캐드나 소프트웨어 개발툴의 경우에서처럼 하위 폴더를 갖고 있는 참조 파일을 동시에 접근해서 사용해야 할 필요가 있는 경우에는 어느 하나의 파일에 관한 편집 모드로의 전환/종료 조작에 의하더라도, 이와 연관되는 해당 하위 폴더 전체 또는 하위 폴더 내의 참조 파일들을 함께 편집 모드로 전환/종료 처리할 수도 있을 것이다.

[0063] 또한 네트워크 파일서버 클라이언트가 해당 파일의 확장자와 연결된 PC 내 설치된 프로그램을 구동하여 상기 경로에 있는 파일 열기를 시도하는데 있어서도 운영체제마다 그 구현 방식이 다소 차이가 있을 수 있다. 예를 들어, MS 윈도우에서 구동되는 경우는 Shell command가 지원하는 ShellExecute로 "Open 파일경로 및 파일명"을 통하여 해당 문서의 열람을 시도하면, 운영체제가 해당 파일의 확장자를 보고 디폴트 연결프로그램을 실행시키면서 해당 파일 경로를 디폴트 연결 프로그램에게 전달하여 문서를 열람시킬 수도 있다.

[0064] 또한 이상에서는 파일 열람, 생성, 변경 등에 관한 요청이 있을 때마다, 커스텀 파일시스템 드라이버가 파일을 요청한 프로그램의 고유값(해쉬)과 사용자 ID를 네트워크 파일서버 데몬에게 전달하는 경우를 주로 설명하였지만, 경우에 따라서 다른 변형이 가능하다. 즉, 구현 방식에 따라서, 최초 사용자 인증이 이루어진 이후 네트워크 파일서버가 해당 접속 세션에 대한 사용자 ID를 기록하고 있는 경우라면, 그 이후의 파일 열람, 생성, 변경 등의 요청 과정에서 커스텀 파일시스템 드라이버가 사용자 ID 첨부하지 않고 네트워크 파일서버 데몬에게 전달할 수도 있을 것이다.

[0065] 또한 본 발명은 사용자 PC OS뿐만 아니라 리눅스나 유닉스 시스템에 기반한 서비스 서버가 네트워크 파일서버의 특정 저장공간을 마운트하여 데이터를 사용하는 경우도 동일하게 적용될 수 있음은 자명하다.

[0066] 보다 구체적으로 리눅스나 유닉스 서비스 서버에서 네트워크 파일서버의 저장공간을 해당 시스템의 저장 파티션으로 구성하여 데이터에 접근하려고 하는 경우, 서비스 서버에서 네트워크 파일서버내 보관된 파일에 대해서 파일 열람 또는 수정 요청을 전송한다 하더라도 파일서버가 사전에 지정된 프로세스에 의해서 파일 접근 요청이 생성된 경우가 아니라면 파일 접근을 차단 할 수 있고, 사전에 지정된 프로세스인 경우 읽기 전용으로만 파일을 제공할 수 있게 구동될 수 있음도 자명하다.

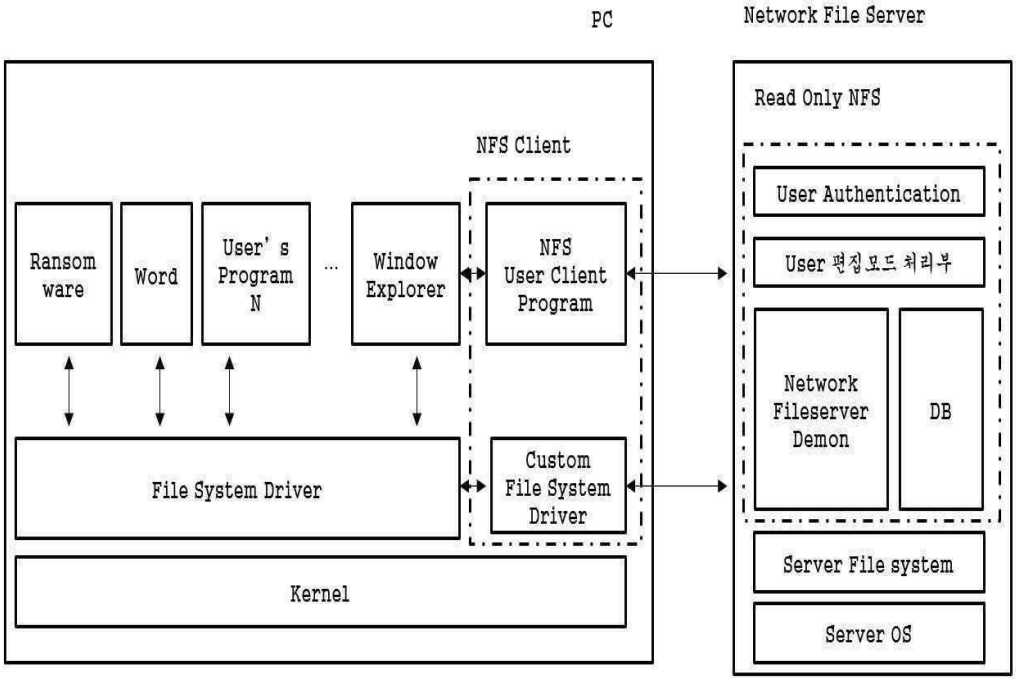
[0067] 상술한 본 발명의 실시예에 따른 랜섬웨어 공격을 차단하는 방법은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로서 구현되는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체로는 컴퓨터 시스템에 의하여 해독될 수 있는 데이터가 저장된 모든 종류의 기록 매체를 포함한다. 예를 들어, ROM(Read Only Memory), RAM(Random Access Memory), 자기 테이프, 자기 디스크, 플래쉬 메모리, 광 데이터 저장장치 등이 있을 수 있다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 통신망으로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 읽을 수 있는 코드로서 저장되고 실행될 수 있다.

[0068] 이상에서는 본 발명의 실시예를 참조하여 설명하였지만, 해당 기술 분야에서 통상의 지식을 가진 자라면 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수

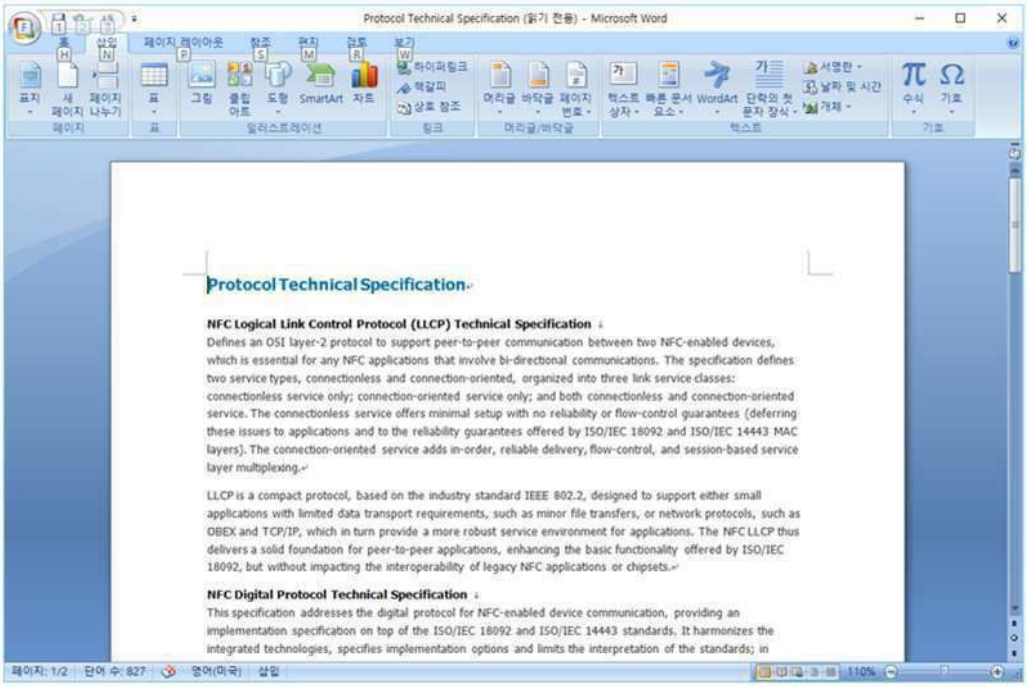
정 및 변경시킬 수 있음을 쉽게 이해할 수 있을 것이다.

도면

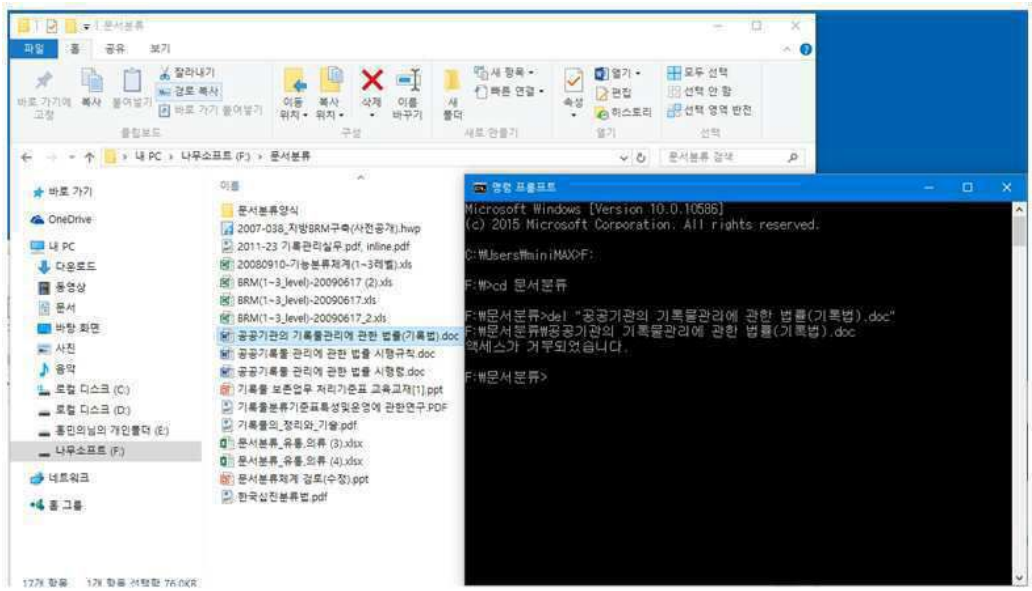
도면1



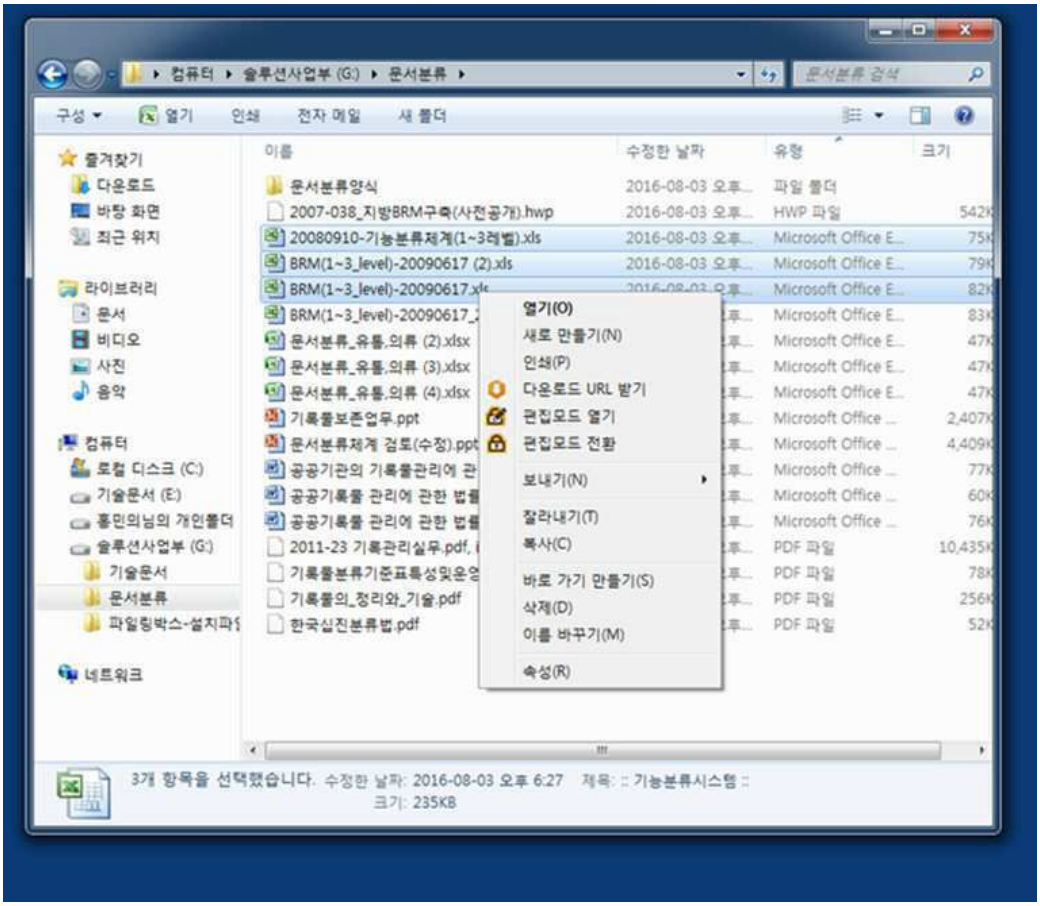
도면2



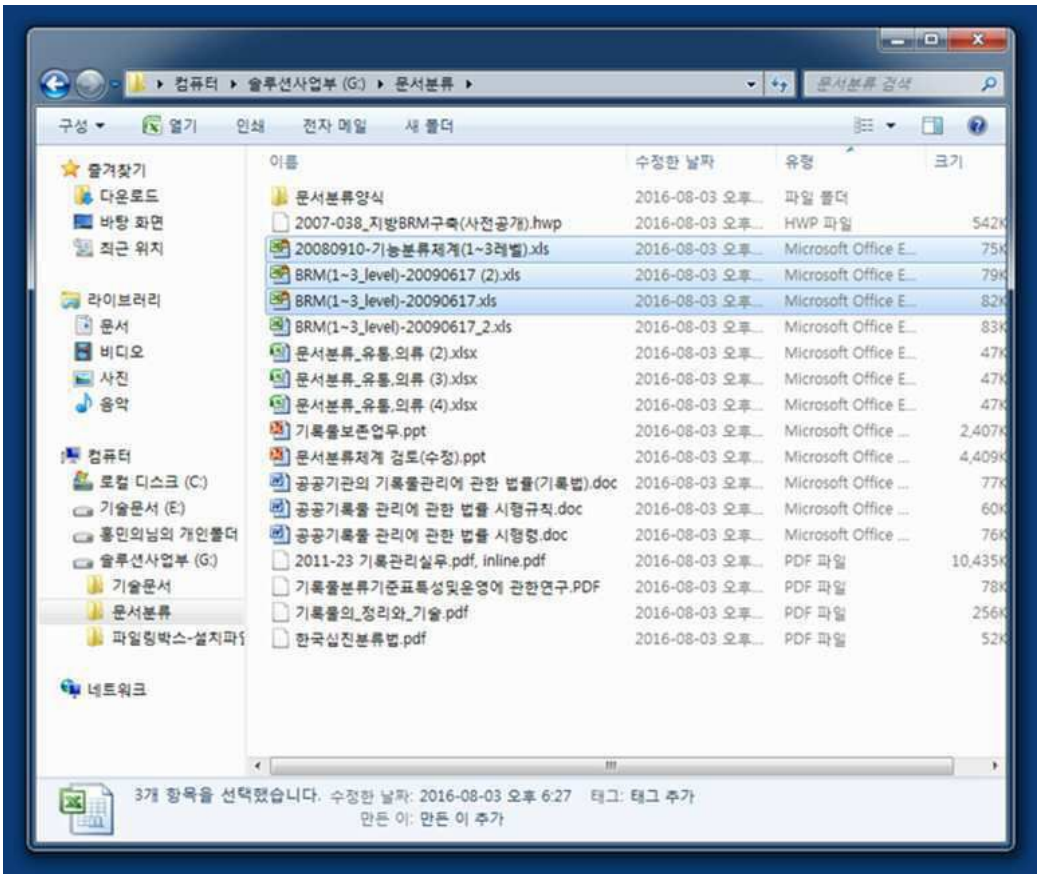
도면3


Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.
F:₩>cd 문서분류
F:₩문서분류>del "공공기관의 기록물관리에 관한 법률(기록법).doc"
액세스가 거부되었습니다.
F:₩문서분류>

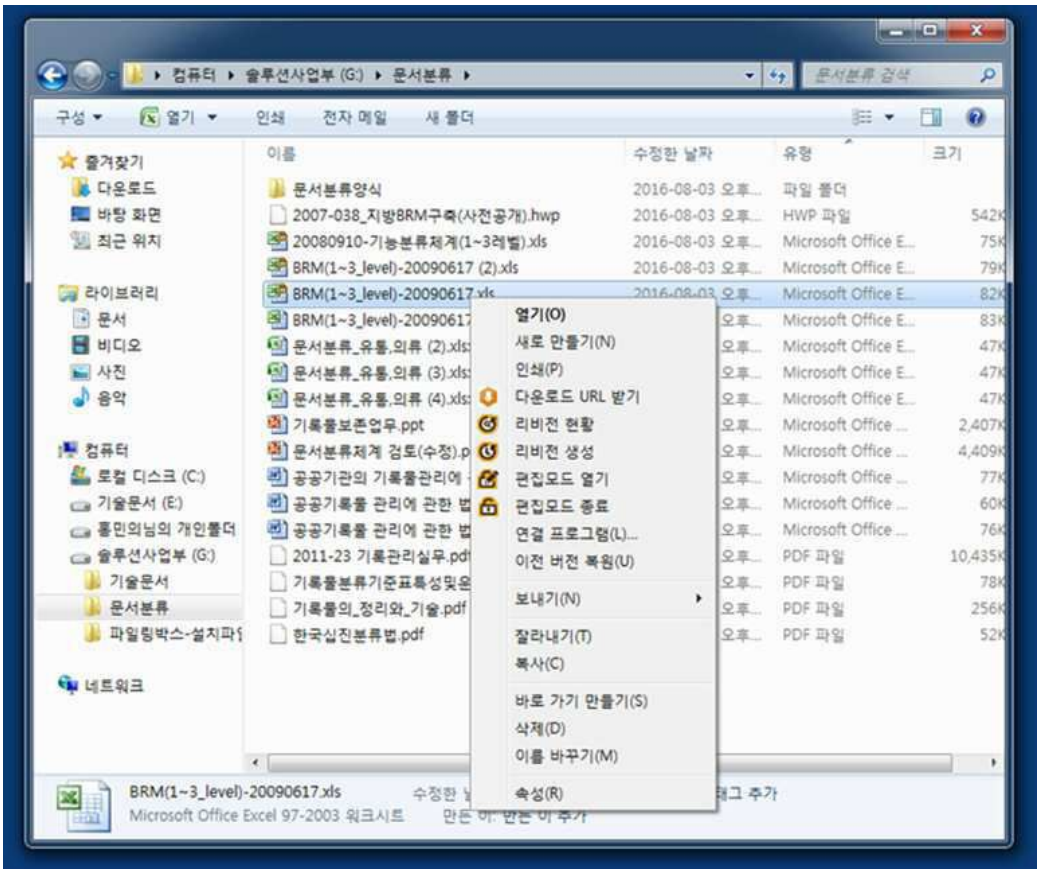
도면4


열기(O)
새로 만들기(N)
인쇄(P)
다운로드 URL 받기
편집모드 열기
편집모드 전환
보내기(N)
잘라내기(T)
복사(C)
바로 가기 만들기(S)
삭제(D)
이름 바꾸기(M)
속성(R)

도면5


컴퓨터 ▸ 솔루션사업부 (G:) ▸ 문서분류 ▸
문서분류 검색
구성
열기
인쇄
전자 메일
새 폴더
즐겨찾기
다운로드
바탕 화면
최근 위치
라이브러리
문서
비디오
사진
음악
컴퓨터
로컬 디스크 (C:)
기술문서 (E:)
홍민의님의 개인폴더
솔루션사업부 (G:)
기술문서
문서분류
네트워크
이름
수정한 날짜
유형
크기
문서분류양식 2016-08-03 오후... 파일 폴더
2007-038_지방BRM구축(사전공개).hwp 2016-08-03 오후... HWP 파일 542K
20080910-기능분류체계(1~3레벨).xls 2016-08-03 오후... Microsoft Office E... 75K
BRM(1~3_level)-20090617 (2).xls 2016-08-03 오후... Microsoft Office E... 79K
BRM(1~3_level)-20090617.xls 2016-08-03 오후... Microsoft Office E... 82K
BRM(1~3_level)-20090617_2.xls 2016-08-03 오후... Microsoft Office E... 83K
문서분류_유통.의류 (2).xlsx 2016-08-03 오후... Microsoft Office E... 47K
문서분류_유통.의류 (3).xlsx 2016-08-03 오후... Microsoft Office E... 47K
문서분류_유통.의류 (4).xlsx 2016-08-03 오후... Microsoft Office E... 47K
기록물보존업무.ppt 2016-08-03 오후... Microsoft Office ... 2,407K
문서분류체계 검토(수정).ppt 2016-08-03 오후... Microsoft Office ... 4,409K
공공기관의 기록물관리에 관한 법률(기록법).doc 2016-08-03 오후... Microsoft Office ... 77K
공공기록물 관리에 관한 법률 시행규칙.doc 2016-08-03 오후... Microsoft Office ... 60K
공공기록물 관리에 관한 법률 시행령.doc 2016-08-03 오후... Microsoft Office ... 76K
2011-23 기록관리실무.pdf, inline.pdf 2016-08-03 오후... PDF 파일 10,435K
기록물분류기준표특성및운영에 관한연구.PDF 2016-08-03 오후... PDF 파일 78K
기록물의_정리와_기술.pdf 2016-08-03 오후... PDF 파일 256K
한국십진분류법.pdf 2016-08-03 오후... PDF 파일 52K
3개 항목을 선택했습니다. 수정한 날짜: 2016-08-03 오후 6:27 태그: 태그 추가
만든 이: 만든 이 추가

도면6


컴퓨터 ▸ 솔루션사업부 (G:) ▸ 문서분류 ▸
문서분류 검색
구성
열기
인쇄
전자 메일
새 폴더
즐겨찾기
다운로드
바탕 화면
최근 위치
라이브러리
문서
비디오
사진
음악
컴퓨터
로컬 디스크 (C:)
기술문서 (E:)
홍민의님의 개인폴더
솔루션사업부 (G:)
기술문서
문서분류
파일링박스-설치파일
네트워크
이름
수정한 날짜
유형
크기
문서분류양식
2007-038_지방BRM구축(사전공개).hwp
20080910-기능분류체계(1~3레벨).xls
BRM(1~3_level)-20090617 (2).xls
BRM(1~3_level)-20090617.xls
문서분류_유통.의류 (2).xls
문서분류_유통.의류 (3).xls
문서분류_유통.의류 (4).xls
기록물보존업무.ppt
2011-23 기록관리실무.pdf
기록물의_정리와_기술.pdf
한국십진분류법.pdf
열기(O)
새로 만들기(N)
인쇄(P)
다운로드 URL 받기
리비전 현황
리비전 생성
편집모드 열기
편집모드 종료
연결 프로그램(L)...
이전 버전 복원(U)
보내기(N)
잘라내기(T)
복사(C)
바로 가기 만들기(S)
삭제(D)
이름 바꾸기(M)
속성(R)
BRM(1~3_level)-20090617.xls
Microsoft Office Excel 97-2003 워크시트