(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년09월28일
(11) 등록번호 10-2448341
(24) 등록일자 2022년09월23일

(51) 국제특허분류(Int. Cl.)
G06F 21/12 (2013.01) *G06F 21/16* (2018.01)
G06F 21/30 (2013.01) *G06F 21/60* (2013.01)
(52) CPC특허분류
G06F 21/125 (2013.01)
G06F 21/16 (2019.02)
(21) 출원번호 10-2020-0187184
(22) 출원일자 2020년12월30일
심사청구일자 2020년12월30일
(65) 공개번호 10-2022-0095554
(43) 공개일자 2022년07월07일
(56) 선행기술조사문헌
KR1020030084798 A*
KR1020080105970 A*
KR1020160121248 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
소프트캠프 주식회사
경기도 과천시 삼부골로 26 ,2층(주암동,GTMotors)
(72) 발명자
배환국
서울특별시 관악구 은천로37길 42-3 (봉천동)
(74) 대리인
이상문, 박천도

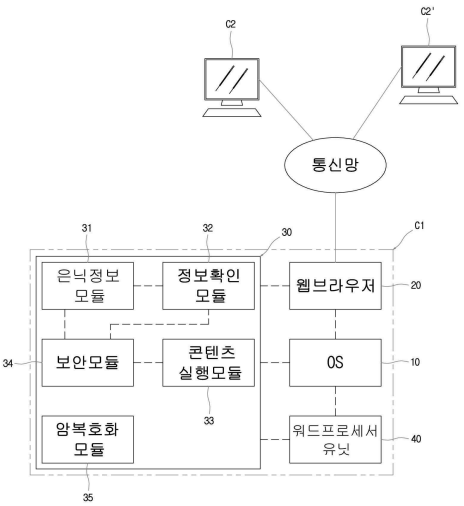
전체 청구항 수 : 총 4 항 심사관 : 문남두

(54) 발명의 명칭 **전자문서 보안을 위한 은닉정보 기반의 보안시스템**

(57) 요 약

본 발명은 전자문서의 데이터 변형에도 보안등급과 로그 관련 정보를 유지하며 정책에 따른 보안 프로세스를 지속할 수 있는 전자문서 보안을 위한 은닉정보 기반의 보안시스템에 관한 것으로, OS(Operating System) 기반 워드프로세서 유닛에 의해 실행된 전자문서 데이터의 소스코드를 분석해서 fmtID(format identifier)를 식별값으로 하는 은닉정보인 custom.xml을 탐색해서 권한정보를 확인하는 은닉정보 모듈; 보안모듈의 제어에 따라 상기 워드프로세서 유닛에 의한 전자문서 데이터의 콘텐츠 실행을 조정하는 콘텐츠 실행모듈; 전자문서 데이터의 보안을 위한 권한정보가 구성된 custom.xml를 해당 전자문서 데이터의 소스코드의 특정 위치에 스테가노그래피 기법으로 은닉하여 보안에이전트 전용 fmtID가 지정된 은닉정보로 생성하고, 상기 은닉정보 모듈에서 확인된 권한정보를 기준정보와 비교해서 콘텐츠의 허용범위를 제한하는 보안모듈;을 갖춘 보안에이전트가 포함된 것이다.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/30 (2013.01)
G06F 21/60 (2013.01)
G06F 2221/0748 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711116181
과제번호	2018-0-01799-003
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	대학ICT연구센터지원사업
연구과제명	블록체인 비즈니스 서비스 기술 개발 및 인력양성
기 여 율	1/1
과제수행기관명	중앙대학교 산학협력단
연구기간	2020.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

OS(Operating System) 기반 워드프로세서 유닛에 의해 실행된 전자문서 데이터의 소스코드를 분석해서 fmtID(format identifier)를 식별값으로 하는 은닉정보인 custom.xml을 탐색해서 권한정보를 확인하는 은닉정보 모듈;

보안모듈의 제어에 따라 상기 워드프로세서 유닛에 의한 전자문서 데이터의 콘텐츠 실행을 조정하는 콘텐츠 실행모듈; 및

전자문서 데이터의 보안을 위한 권한정보가 구성된 custom.xml를 해당 전자문서 데이터의 소스코드의 특정 위치에 스테가노그래피 기법으로 은닉하여 보안에이전트 전용 fmtID가 지정된 은닉정보로 생성하고, 상기 은닉정보 모듈에서 확인된 권한정보를 기준정보와 비교해서 콘텐츠의 허용범위를 제한하는 보안모듈;

을 갖춘 보안에이전트가 포함된 것을 특징으로 하는 전자문서 보안을 위한 은닉정보 기반의 보안시스템.

청구항 2

제 1 항에 있어서,

상기 보안모듈은 전자문서 데이터의 실행 이력에 관한 로그정보를 custom.xml의 내용을 구성하고. 상기 은닉정보 모듈은 전자문서 데이터에서 탐색된 은닉정보에서 로그정보를 확인하며;

상기 은닉정보 모듈에 의해 확인된 로그정보에서 전자문서 데이터의 실행 이력을 파악하여 출력시키는 정보확인모듈을 더 포함하는 한편;

상기 정보확인모듈에서 확인된 실행 이력을 유해한 URL 또는 사용자의 경로가 등록된 기준정보와 비교해서, 상기 전자문서 데이터가 기준정보의 경로를 경유한 경우 해당 전자문서 데이터의 실행을 제한하는 것;

을 특징으로 하는 전자문서 보안을 위한 은닉정보 기반의 보안시스템.

청구항 3

제 1 항에 있어서,

상기 보안모듈의 제어에 따란 전자문서 데이터 전체 또는 콘텐츠를 암복호화하는 암복화모듈을 더 포함하고;

상기 보안모듈은 워드프로세서 유닛과 연동하며 암복화모듈을 제어하는 것;

을 특징으로 하는 전자문서 보안을 위한 은닉정보 기반의 보안시스템.

청구항 4

제 1 항에 있어서,

상기 보안모듈은 입력된 명령값에 대응한 권한정보를 생성하는 것;

을 특징으로 하는 전자문서 보안을 위한 은닉정보 기반의 보안시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 전자문서의 데이터 변형에도 보안등급과 로그 관련 정보를 유지하며 정책에 따른 보안 프로세스를 지속할 수 있는 전자문서 보안을 위한 은닉정보 기반의 보안시스템에 관한 것이다.

배 경 기 술

[0002] 일반적으로 전자문서를 보안하기 위해서 해당 전자문서를 저장한 보안시스템에 대해 사용자의 로그인을 제한하거나, 전자문서 자체에 보안등급을 설정해서 사용자에 따라 접근을 제한했다. 전자(前者)의 보안 방식은 수많은 전자문서를 등급별로 분류해서 일괄적으로 보안하므로 전자문서의 등급별 보안에 효율적이나 전자문서 하나하나에 대한 세밀한 권한 제한에 한계가 있었고, 후자(後者)의 방식은 전자문서 단위의 세밀한 권한 제한이 가능하나 전자문서 하나하나에 보안에 관한 접근권한을 설정해야 하므로 전자문서별 보안시스템의 보안 처리에 부담이 있었다.

[0003] 따라서 상기의 보안 기술들은 전자문서의 보안 목적에 따라 병행해 사용되었다.

[0004] 한편, 전자문서 자체의 보안등급 설정을 위해서 종래에는 해당 전자문서를 암호화하고, 접근권한 등의 보안등급과 접근 이력에 대한 로그가 기록된 헤더를 추가 생성했다. 결국 보안시스템은 헤더를 확인해서 해당 전자문서의 보안등급과 로그를 확인하고, 확인된 보안등급과 로그에 따라 전자문서에 대한 타인의 접근을 제한하며 보안성을 강화했다.

[0005] 그런데 전술한 종래 기술의 전자문서가 보안등급과 로그가 기록된 헤더에 대한 인식 불능인 레가시 시스템(Legacy System)에서 리딩이 시도될 경우, 상기 레가시 시스템이 전자문서의 헤더를 인식할 수 없어서 실행 오류가 발생하는 문제가 있었다. 즉, 보안 전용 워드 프로그램에서 보안성을 갖춘 전자문서는 보안 기능이 없는 저 버전의 기존 워드 프로그램에서 오류가 발생되어 실행 자체가 이루어질 수 없는 것이다.

[0006] 또한 보안등급과 로그 관련 정보가 저장된 헤더가 악성 사용자에 의해 제 기능을 상실하면 전자문서 자체가 보안성을 상실할 수 있으므로, 종래 보안시스템은 해당 전자문서를 보호하지 못하며 보안 내용을 그대로 노출시키는 문제 또한 있었다.

[0007] 따라서 보안등급이 설정된 상태에서도 레가시 시스템의 오류없이 지원되어 실행이 가능하고, 복호화 이후에도 보안시스템이 해당 전자문서의 보안등급을 인식하며 사용자에 따라 접근 권한을 제한할 수 있는 기술이 요구되었다.

선행기술문헌

[0008] 대한민국 공개특허공보 제10-2016-0121248호

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 문제를 해결하기 위해 안출된 것으로, 전자문서의 데이터 변형에도 보안등급과 로그 관련 정보를 유지하며 정책에 따른 보안 프로세스를 지속할 수 있도록 하는 전자문서 보안을 위한 은닉정보 기반의 보안시스템을 제공함에 그 목적이 있다.

과제의 해결 수단

[0010] 이와 같은 본 발명에 따른 목적을 달성하기 위해,

[0011] OS(Operating System) 기반 워드프로세서 유닛에 의해 실행된 전자문서 데이터의 소스코드를 분석해서 fmtID(format identifier)를 식별값으로 하는 은닉정보인 custom.xml을 탐색해서 권한정보를 확인하는 은닉정보 모듈;

[0012] 보안모듈의 제어에 따라 상기 워드프로세서 유닛에 의한 전자문서 데이터의 콘텐츠 실행을 조정하는 콘텐츠 실행모듈; 및

[0013] 전자문서 데이터의 보안을 위한 권한정보가 구성된 custom.xml를 해당 전자문서 데이터의 소스코드의 특정 위치에 스테가노그래피 기법으로 은닉하여 보안에이전트 전용 fmtID가 지정된 은닉정보로 생성하고, 상기 은닉정보 모듈에서 확인된 권한정보를 기준정보와 비교해서 콘텐츠의 허용범위를 제한하는 보안모듈;

[0014] 을 갖춘 보안에이전트가 포함된 전자문서 보안을 위한 은닉정보 기반의 보안시스템이다.

발명의 효과

[0015] 상기의 본 발명은, 전자문서의 데이터 변형에도 보안등급과 로그 관련 정보를 유지하며 정책에 따른 보안 프로

세스를 지속할 수 있는 효과가 있다. 또한, 전자문서의 은닉정보가 데이터 파일의 형식 변형에도 유지되므로 전자문서에 대한 권한정보와 로그정보를 지속해 확인해서 보안에 활용할 수 있는 효과가 있다.

도면의 간단한 설명

[0016] 도 1은 본 발명에 따른 바람직한 실시예로서 전자문서 보안을 위한 은닉정보 기반의 보안시스템을 도시한 블록도이며,

도 2는 본 발명에 따른 바람직한 실시예로서 보안시스템을 기반으로 전자문서 데이터를 보안 처리하고 사용자를 인증해서 전자문서 데이터의 콘텐츠를 출력하는 과정을 순차로 보인 플로차트이고,

도 3은 보안 처리된 전자문서 데이터의 은닉정보를 일실시 예로 보인 이미지 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 다양한 "일 실시예" 또는 "실시예"가 이하에서 논의되는 세부사항을 참조하여 설명되며, 첨부된 도면은 다양한 실시예를 도시한다. 이하의 설명 및 도면은 예시적인 것이며, 제한적인 것으로 해석되어서는 안된다. 본 발명의 다양한 실시예에 대한 완전한 이해를 제공하기 위해 다수의 구체적인 세부사항이 설명된다. 그러나, 특정 실시예에서, 본 발명의 실시예에 대한 간결한 설명을 제공하기 위해 널리 알려진 또는 종래의 세부사항은 설명되지 않는다.

[0018] 명세서에서 "일 실시예" 또는 "실시예"라는 언급은 실시예와 함께 설명된 특정 특징, 구조 또는 특성이 적어도 하나의 실시예에 포함될 수 있음을 의미한다. 명세서의 다양한 곳에서 "일 실시예에서"라는 문구의 출현은 모두 반드시 동일한 실시예를 지칭할 필요는 없다.

[0019] 본 발명의 실시예들은, 하기의 보다 상세히 기술되어 있는 바와 같이, 다양한 컴퓨터 하드웨어를 포함하는 특수 목적의 또는 범용 컴퓨터를 포함할 수 있다. 도 1은 본 발명의 특징을 구현하는 데 사용될 수 있는 예시적 컴퓨팅 시스템의 개략도를 도시한 것으로 클라이언트로 지칭된다. 기술된 클라이언트는 이러한 적합한 컴퓨팅 환경의 일례에 불과하며, 본 발명의 용도 또는 기능성의 범위에 관해 어떤 제한을 암시하고자 하는 것이 아니다. 본 발명은 도 1에 도시된 컴포넌트들 중 임의의 하나 또는 그 컴포넌트들의 임의의 조합과 관련하여 어떤 의존성 또는 요구사항을 갖는 것으로 해석되어서는 안된다.

[0020] 본 발명에 따른 "전자문서 보안을 위한 은닉정보 기반의 보안시스템"을 설명하기 위해 사용하는 용어를 정의한다. 본 발명에 따른 "전자문서 보안을 위한 은닉정보 기반의 보안시스템"은 전자문서의 콘텐츠 읽기, 읽기 횟수, 편집, 암호화 해제, 반출, 출력, 프린트마킹, 유효기간, 자동파기, 권한변경, 콘텐츠 복제 등을 사용자 또는 실행 PC 등에 따라 제한하는 소프트웨어 또는 장치를 지칭한다. "전자문서 보안을 위한 은닉정보 기반의 보안시스템"은 클라이언트에 설치되며 전자문서을 실행하는 소프트웨어와 연계되어 동작하도록 된다. 이하에서는 "전자문서 보안을 위한 은닉정보 기반의 보안시스템"을 "보안시스템"으로 칭한다.

[0021] 본 발명에 따른 "전자문서"는 영문으로 'Electronic document'이며, 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태(electronic form)로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것이며, 상기 자료는 텍스트, 이미지, 그래표 등의 콘텐츠가 포함될 수 있다. 컴퓨터에서의 실행을 위한 전자문서 관련 소프트웨어의 지원 확장자는 MS Office에서 지원하는 doc, 틴, ppt, dock, xlsx, pptx 등의 버전과, HWP, PDF 등의 버전이 예시될 수 있으며, 이외에도 다양한 확장자가 예시될 수 있다. 또한 "워드프로세서 유닛"은 전자문서를 읽고 고치거나 작성할 수 있는 사무용 소프트웨어를 지칭한다. 본 발명에 따른 "보안에이전트"는 전자문서에 은닉정보를 생성해 입력하고, 전자문서에 구성된 은닉정보를 탐색해 확인해서 전자문서의 보안 등급과 로그정보를 리딩하는 소프트웨어를 지칭한다. 또한, "권한정보"는 전자문서에 대한 콘텐츠 읽기, 읽기 횟수, 편집, 암호화 해제, 반출, 출력, 프린트마킹, 유효기간, 자동파기, 권한변경, 콘텐츠 복제 등을 사용자 또는 실행 PC 등에 부여한 권리를 칭한다. 따라서 사용자가 누구인지, 실행 PC가 무엇인지에 따라 전자문서에 대한 사용 범위에 차이가 있다.

[0023] 본 발명에 따른 실시예로서 전자문서 보안을 위한 은닉정보 기반의 보안시스템을 설명한다.

[0024] 본 발명에 따른 실시예로서, 전자문서 보안을 위한 은닉정보 기반의 보안시스템은, OS(Operating System) 기반 워드프로세서 유닛에 의해 실행된 전자문서 데이터의 소스코드를 분석해서 fmtID(format identifier)를 식별값으로 하는 custom.xml을 탐색하고, custom.xml에 구성된 권한정보와 로그정보를 확인하는 은닉정보 모듈; 상기 은닉정보 모듈에 의해 확인된 로그정보에서 전자문서의 실행 이력을 파악하여 출력시키는 정보확인모듈; 보안모

듈의 제어에 따라 상기 워드프로세서 유닛에 의한 전자문서의 콘텐츠 실행을 조정하는 콘텐츠 실행모듈; 전자문서의 보안을 위한 권한정보와, 전자문서의 실행 이력에 관한 로그정보를 내용으로 한 custom.xml를 해당 전자문서의 소스코드에 스테가노그래피 기법으로 생성하여 보안에이전트 전용 fmtID를 지정하고, 상기 은닉정보 모듈에서 확인된 권한정보와, 상기 정보확인모듈에서 확인된 실행 이력을 기준정보와 비교해서 콘텐츠의 허용범위를 제한하는 보안모듈;을 갖춘다. 또한, 본 발명에 따른 보안시스템은, 상기 보안모듈의 제어에 따란 전자문서 데이터 전체 또는 콘텐츠를 암복호화하는 암복화모듈을 더 포함하고; 상기 보안모듈은 워드프로세서 유닛과 연동하며 암복화모듈을 제어하는 것이다. 여기서 상기 보안모듈은 입력된 명령값에 대응한 권한정보를 생성하는 것일 수 있다.

[0026] 이하 본 발명에 따른 바람직한 실시예로서 보안시스템을 첨부된 도면을 참조하여 보다 자세히 설명한다.

[0028] 도 1은 본 발명에 따른 바람직한 실시예로서 전자문서 보안을 위한 은닉정보 기반의 보안시스템을 도시한 블록도이다.

[0030] 도 1을 참조하면, 본 발명에 따른 바람직한 일실시예로서 보안시스템은, OS(Operating System; 10) 기반 워드프로세서 유닛(40)에 의해 실행된 전자문서 데이터의 소스코드를 분석해서 fmtID(format identifier)를 식별값으로 하는 custom.xml을 탐색하고, custom.xml에 구성된 권한정보와 로그정보를 확인하는 은닉정보 모듈(31); 은닉정보 모듈(31)에 의해 확인된 로그정보에서 전자문서의 실행 이력을 파악하여 출력시키는 정보확인모듈(32); 보안모듈(34)의 제어에 따라 워드프로세서 유닛(40)에 의한 전자문서의 콘텐츠 실행을 조정하는 콘텐츠 실행모듈(33); 전자문서의 보안을 위한 권한정보와, 전자문서의 실행 이력에 관한 로그정보를 내용으로 한 custom.xml를 해당 전자문서의 소스코드의 특정 위치에 스테가노그래피 기법으로 생성하여 보안에이전트(30) 전용 fmtID를 지정하고, 은닉정보 모듈(31)에서 확인된 권한정보와, 정보확인모듈(32)에서 확인된 실행 이력을 기준정보와 비교해서 콘텐츠의 허용범위를 제한하는 보안모듈(34);을 갖춘 보안에이전트(30)가 포함된다.

[0031] 은닉정보 모듈(31)은 OS 기반 워드프로세서 유닛(40)에 의해 실행된 전자문서 데이터의 소스코드를 분석해서 fmtID를 식별값으로 하는 custom.xml을 탐색하고, custom.xml에 구성된 권한정보와 로그정보를 확인한다. 전술한 바와 같이 보안모듈(34)은 전자문서에 권한정보와 로그정보가 구성된 은닉정보를 생성하므로, 은닉정보 모듈(31)은 은닉정보의 식별값으로 생성된 fmtID를 탐색해서 custom.xml 형식의 은닉정보를 확인한다. 본 발명에 따른 은닉정보는 스테가노그래피 기법을 통해 생성되므로, 워드프로세서 유닛(40)는 custom.xml 형식의 은닉정보를 인지할 수 없고 은닉정보 모듈(31)만이 fmtID를 확인해서 인식한다. 한편, 상기 로그정보는 전자문서의 데이터 복제, 이름변경 등을 통한 저장 과정에서 갱신된다. 로그정보에 구성된 이력은 전자문서의 열기시간, 닫기시간, 저장시간, 저장위치, 저장 과정에서 신생된 현버전의 ID와 이전버전의 ID 등의 정보일 수 있다.

[0032] 정보확인모듈(32)은 은닉정보 모듈(31)에 의해 확인된 로그정보에서 전자문서의 실행 이력을 파악한다. 이를 좀 더 구체적으로 설명하면, 은닉정보에 구성된 로그정보의 이력은 앞서 예시된 바와 같이, 전자문서의 열기시간, 닫기시간, 저장시간, 저장위치, 저장 과정에서 신생된 현버전의 ID와 이전버전의 ID 등의 정보일 수 있으며, 정보확인모듈(32)은 상기 이력을 파악해서 전자문서의 실행 이력과 유통경로를 파악할 수 있도록 한다.

[0033] 콘텐츠 실행모듈(33)은 보안모듈(34)의 제어에 따라 워드프로세서 유닛(40)에 의한 전자문서의 콘텐츠 실행을 조정한다. 이를 좀 더 구체적으로 설명하면, 상기 은닉정보는 전자문서에 대한 권한정보를 포함하므로, 해당 전자문서는 권한정보에 따라 전자문서의 실행 범위가 제한되어야 한다. 따라서 보안모듈(34)이 권한정보를 확인해서 허용범위를 지정하면, 콘텐츠 실행모듈(33)은 워드프로세서 유닛(40)과 연동하며 허용범위 이내로만 전자문서가 실행되도록 강제로 제한시킨다. 즉, 전자문서의 허용범위가 콘텐츠 읽기로만 제한되면, 콘텐츠 실행모듈(33)은 전자문서에 대한 워드프로세서 유닛(40)의 접근 내용을 확인하면서 편집이 시도될 경우 이를 강제로 정지시키는 것이다.

[0034] 보안모듈(34)은, 워드프로세서 유닛(40)이 인식하지 못하는 은닉정보를 전자문서에 생성시켜서 보안에이전트(30)만이 인식할 수 있도록 한다. 이를 위한 은닉정보는 전자문서의 소스코드의 특정 위치에 스테가노그래피 기법으로 은닉정보를 생성해 삽입한다. 상기 은닉정보는 custom.xml 형식으로 전자문서에 구성되고, fmtID(format identifier)를 custom.xml의 식별값으로 설정한다. custom.xml은 해당 전자문서에 대한 권한정보와 로그정보가 구성되며, 은닉정보 모듈(31)이 전자문서의 소스코드에서 특정 위치에 독립되도록 위치하게 할 수 있다. 결국, 은닉정보는 스테가노그래피 기법과 같이 워드프로세서 유닛(40)가 인식할 수 없거나 무시하는 데이터로 전자문서에 구성되고, 은닉정보 모듈(31)만이 지정된 fmtID을 인식해서 은닉정보를 확인하고 권한정보와 로그정보를 리딩할 수 있다. 또한, 전자문서에 구성된 은닉정보는 전자문서와는 독립된 객체이므로, 전자문서의 콘텐츠 또는 속성을 변경하거나 전자문서의 확장자를 변경하여도 은닉정보는 제 형식을 유지하며 은닉정보 모듈(31)이 탐

색해서 권한정보와 로그정보를 인식할 수 있다. 참고로, 스테가노그래피(Steganography)는 데이터 은폐 기술 중 하나이며, 데이터를 다른 데이터에 삽입하는 기술 혹은 그 연구를 가리킨다. 첨언하면 크립토그래피(cryptography)가 메시지의 내용을 읽을 수 없게 하는 수단인 반면, 스테가노그래피는 존재 자체를 숨긴다.

[0035] 계속해서 보안모듈(34)은 은닉정보 모듈(31)에서 확인된 권한정보와, 정보확인모듈(32)에서 확인된 실행 이력을 기준정보와 비교해서 콘텐츠의 허용범위를 제한한다. 전술한 바와 같이, 권한정보는 해당 전자문서 실행에 대한 허용범위에 관한 것이므로, 은닉정보에 구성된 권한정보에서 허용범위를 파악하여 허용된 실행 내용에 대해서만 워드프로세서 유닛(40)이 해당 전자문서를 실행하도록 콘텐츠 실행모듈(33)을 통해 제한한다.

[0036] 상기 권한정보와 실행 이력을 기준정보와 비교하는 기술에 대해서는 아래에서 다시 설명한다.

[0037] 한편, 보안에이전트(30)가 설치된 클라이언트(C1)는 웹브라우저(20)를 이용해 통신망에 접속하여 다른 클라이언트(C2)와 데이터 통신을 할 수 있다. 상기 데이터 통신 중에 보안이 설정된 전자문서가 웹브라우저(20)에 수신되면 보안에이전트(30)는 해당 전자문서에서 은닉정보를 탐색하고, 탐색된 은닉정보에서 로그정보를 확인하여 갱신한다. 전술한 바와 같이 로그정보는 전자문서의 저장시간과 버전 등을 포함할 수 있으므로, 보안모듈(34)은 해당 전자문서가 수신 및 저장되면 해당 전자문서의 저장시간과 버전 등 로그정보에 보강한다.

[0038] 또한 본 발명에 따른 보안에이전트(30)는 보안모듈(34)의 제어에 따란 전자문서 데이터 전체 또는 콘텐츠를 암복호화하는 암복화모듈(35)을 더 포함하고, 보안모듈(34)은 워드프로세서 유닛(40)과 연동하며 암복화모듈(35)을 제어한다. 좀 더 구체적으로 설명하면, 전자문서의 보안성을 강화하기 위해서 보안에이전트(30)는 실행이 종료되는 전자문서의 데이터를 암호화해서 클라이언트(C1)에 저장할 수 있다. 이를 위해 보안모듈(34)은 워드프로세서 유닛(40)에서 전자문서의 종료 프로세스를 인식하면, 워드프로세서 유닛(40)에 의해 저장된 전자문서 데이터를 암복호화모듈(35)이 암호화하도록 제어한다. 암복호화모듈(35)은 워드프로세서 유닛(40)이 암호화된 전자문서 데이터를 인식해 로딩할 수 있도록 암호화된 전자문서 데이터의 저장경로에 해당 전자문서 데이터의 이름과 확장자가 일치하는 임시파일을 생성해 위치시키고, 콘텐츠를 갖는 실제 전자문서 데이터는 암호화파일로 저장할 수 있다. 하지만, 해당 암호화 절차는 본 발명의 일실시 예에 불과하며, 보안모듈(34)이 전자문서 데이터를 암호화할 수 있도록 워드프로세서 유닛(40)의 저장 프로세스가 보안모듈(34)과 연계해 이루어지도록 할 수도 있다.

[0039] 이후, 사용자가 워드프로세서 유닛(40)을 통해 암호화된 전자문서 데이터의 실행을 시도하면, 보안모듈(34)은 워드프로세서 유닛(40)의 실행 프로세스를 인식해서 암복호화모듈(35)이 암호화된 전자문서 데이터를 복호화하도록 제어한다. 물론 암복호화모듈(35)은 보안모듈(34)의 제어에 따라 지정된 데이터를 복호화하고, 보안모듈(34)은 복호화를 확인하면 해당 전자문서 데이터가 워드프로세서 유닛(40)에 의해 실행되도록 처리한다.

[0041] 도 2는 본 발명에 따른 바람직한 실시예로서 보안시스템을 기반으로 전자문서 데이터를 보안 처리하고 사용자를 인증해서 전자문서 데이터의 콘텐츠를 출력하는 과정을 순차로 보인 플로차트이고, 도 3은 보안 처리된 전자문서 데이터의 은닉정보를 일실시 예로 보인 이미지 도면이다.

[0043] 도 1 내지 도 3을 참조하면, 본 발명에 따른 보안시스템 기반 보안방법은 하기와 같다.

[0045] S10; 은닉정보 설정 단계

[0046] 워드프로세서 유닛(40)이 전자문서의 데이터 파일을 생성해 저장하면, 보안에이전트(30)의 보안모듈(34)은 전자문서를 저작한 저작자 또는 전자문서의 권리를 갖는 권리자(이하 '설정자')가 전자문서의 권한정보를 설정한다. 이를 위해 보안에이전트(30)는 워드프로세서 유닛(40)의 메뉴에 보안설정 메뉴키(미도시함)를 GUI(Graphical User Interface) 또는 일반 UI를 생성하고, 설정자가 보안설정 메뉴키를 클릭하면 보안에이전트(30)의 보안모듈(34)이 실행되며 실행 허용범위를 입력할 수 있는 설정레이어(미도시함)를 출력한다.

[0047] 설정자는 출력된 설정레이어에 실행 허용범위를 입력하고, 보안모듈(34)은 입력된 명령값에 따라 실행 허용범위에 대한 권한정보를 은닉정보로 생성한다. 상기 은닉정보는 스테가노그래피 기법에 따라 custom.xml 형식으로 생성되고, 보안모듈(34)은 전자문서의 소스코드의 특정 위치에 배치된다. 또한, 은닉정보인 custom.xml은 은닉정보 모듈(31)이 인식할 수 있는 fmtID가 식별값으로 지정된다.

[0048] 보안모듈(34)은 은닉정보에 전자문서의 실행 이력에 대한 정보를 저장하는 로그정보를 더 포함할 수 있다. 로그정보에 구성된 이력은 전자문서의 열기시간, 닫기시간, 저장시간, 저장위치, 저장 과정에서 신생된 현버전의 ID와 이전버전의 ID 등의 정보일 수 있다.

[0050] S20; 은닉정보 탐색 단계

[0051] 워드프로세서 유닛(40)이 사용자의 조작에 따라 특정 전자문서 실행을 시도하면, 보안에이전트(30)의 은닉정보 모듈(31)이 해당 전자문서에서 은닉정보를 탐색하고 권한정보와 로그정보를 확인한다.

[0052] 은닉정보 모듈(31)이 권한정보를 확인하면 보안모듈(34)을 호출하고, 로그정보를 확인하면 정보확인모듈(32)을 호출한다.

[0054] S30; 전자문서의 실행 이력 확인 단계

[0055] 은닉정보 모듈(31)의 호출로 정보확인모듈(32)이 은닉정보의 로그정보를 확인해서 전자문서의 실행 이력을 파악한다. 전술한 바와 같이 실행 이력은 전자문서의 열기시간, 닫기시간, 저장시간, 저장위치, 저장 과정에서 신생된 현버전의 ID와 이전버전의 ID 등의 정보일 수 있으며, 정보확인모듈(32)은 상기 이력을 통해 전자문서의 실행 이력과 유통경로를 파악할 수 있도록 한다.

[0056] 참고로, 정보확인모듈(32)에 의해 파악된 전자문서의 실행 이력은 별도의 설정창(미도시함)을 통해 출력될 수 있고, 이를 통해 해당 전자문서의 유통경로를 추적할 수 있다.

[0058] S40; 전자문서 실행 결정 단계

[0059] 보안모듈(34)은 전자문서의 보안을 위한 권한정보와, 로그정보의 실행 이력을 기준정보와 비교해서 콘텐츠의 허용범위를 제한한다. 이를 좀 더 구체적으로 설명하면, 상기 권한정보는 전자문서의 실행에 관한 허용범위로서 보안등급 코드로 입력된다. 즉, 전자문서에 대한 보안 설정 시 설정자가 해당 전자문서에 대해 콘텐츠 읽기만 허용범위로 설정했다면 권한정보에는 콘텐츠 읽기에 대한 보안등급 코드만 세팅되는 것이다. 한편 보안모듈(34)은 보안등급 코드별 허용범위 내용이 기준정보로 저장된다. 따라서 보안모듈(34)은 권한정보에 세팅된 보안등급 코드를 확인하고, 해당 보안등급 코드의 허용범위 내용을 기준정보에서 검색하여 전자문서에 허가된 허용범위가 무엇인지를 파악한다. 이후, 허용범위가 확인되면, 보안모듈(34)은 관련 데이터를 콘텐츠 실행모듈(33)에 전달한다.

[0060] 또한, 상기 로그정보는 전자문서의 실행 이력에 관한 것으로서 유해한 URL 또는 사용자 등의 경로가 등록된 기준정보와 전자문서의 실행 이력을 비교해서 전자문서의 실행 이력 중 기준정보의 경로를 경유한 경우 해당 전자문서의 실행을 제한한다.

[0062] S50; 전자문서 실행 단계

[0063] 워드프로세서 유닛(40)은 사용자의 조작에 따라 해당 전자문서를 실행시키고, 보안모듈(34)의 제어를 받는 콘텐츠 실행모듈(33)은 워드프로세서 유닛(40)과 연동하며 해당 전자문서의 실행을 조정한다. 즉, 보안모듈(34)이 권한정보로부터 전자문서의 허용범위가 콘텐츠 읽기로 제한되면, 보안모듈(34)로부터 콘텐츠 읽기의 신호를 받은 콘텐츠 실행모듈(33)은 워드프로세서 유닛(40)이 전자문서에 대한 사용자의 콘텐츠 읽기 이외에 다른 기능은 실행하지 않도록 프로세스의 실행을 제한하는 것이다.

[0064] 또한, 보안모듈(34)이 로그정보로부터 전자문서의 실행 이력을 확인하고 실행 이력에서 기준정보에 등록된 유해한 경로와 동일한 경로를 확인하면, 보안모듈(34)로부터 실행 제한 신호를 받은 콘텐츠 실행모듈(33)은 워드프로세서 유닛(40)이 전자문서를 실행하지 않도록 정지신호를 전달한다.

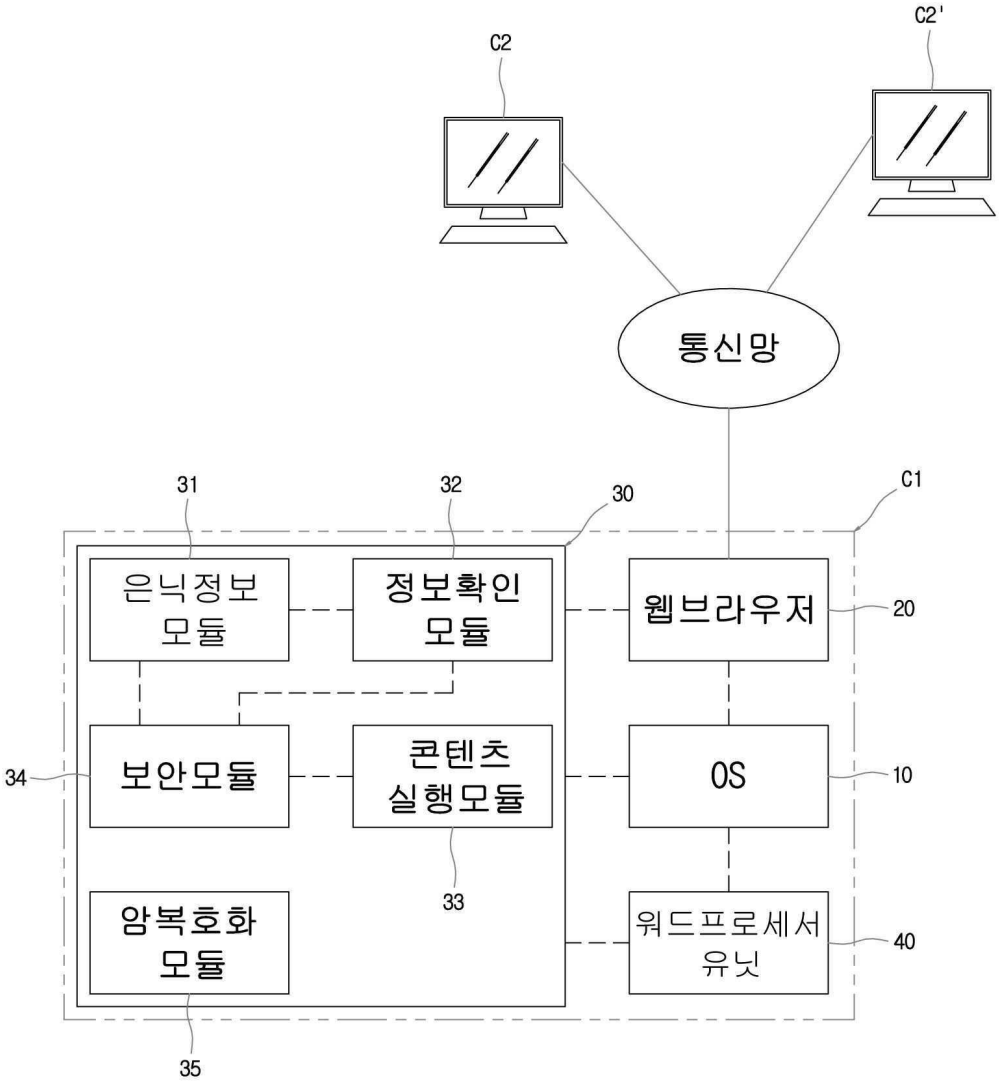
[0066] S60; 전자문서 저장 단계

[0067] 보안모듈(34)이 워드프로세서 유닛(40)에서 전자문서의 종료 프로세스를 확인하면, 은닉정보에 구성된 권한정보와 로그정보 중 선택된 하나 이상을 갱신하고 해당 클라이언트(C1)의 저장수단에 저장한다.

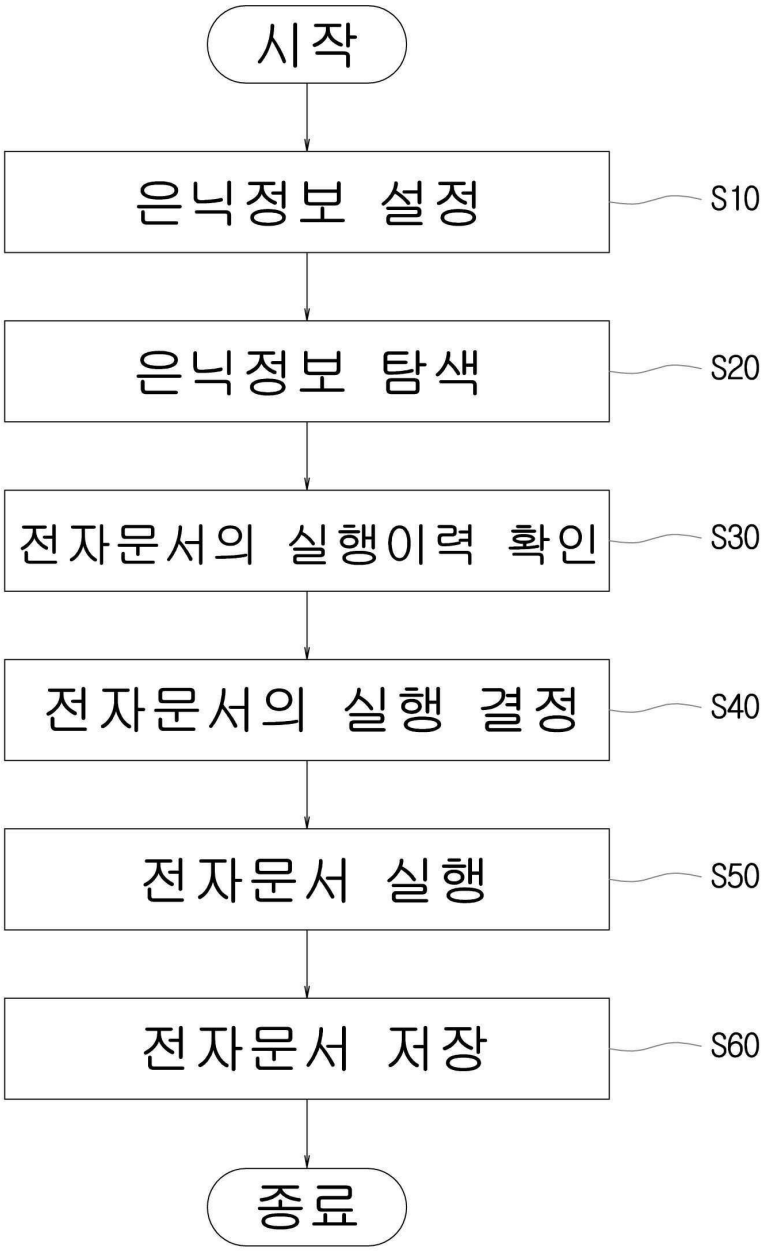
[0069] 이상과 같이, 본 발명에 따른 보안시스템을 보다 자세히 설명하고 도시하였으나, 이는 본 발명에 따른 보안시스템의 설명과 이해의 편의를 위한 것으로 이해되어야 하며, 상술된 실시 예의 구성과 데이터의 저장 위치 등에 한정하여 권리가 제한적으로 해석되어서는 안되고, 본 발명의 설명에 반하여 다른 문헌을 이용하여 제한하여 해석되어서도 안되며, 본 발명에 따른 보안시스템의 권리범위는 첨부된 특허청구범위에 의해 정해져야 한다.

도면

도면1


C2
C2'
통신망
C1
30
31
32
은닉정보 모듈
정보확인 모듈
웹브라우저
20
34
보안모듈
콘텐츠 실행모듈
OS
10
33
암복호화 모듈
워드프로세서 유닛
40
35

도면2


시작
은닉정보 설정
S10
은닉정보 탐색
S20
전자문서의 실행이력 확인
S30
전자문서의 실행 결정
S40
전자문서 실행
S50
전자문서 저장
S60
종료

도면3

상략
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Properties xmlns="http://schemas.openxmlformats.org/officeDocument/2006/custom-properties"
xmlns:vt="http://schemas.openxmlformats.org/officeDocument/2006/docPropsVTypes">
<property fmtid="{11CD0505-2E9C-101B-9397-08002B2CF9AE}" pid="2" name="_Version">
<vt:lpwstr>Softcamp</vt:lpwstr>
</property>
</Properties>
하략