



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0006309
(43) 공개일자 2010년01월19일

(51) Int. Cl.

H04L 9/32 (2006.01) H04L 9/08 (2006.01)

(21) 출원번호 10-2008-0066497

(22) 출원일자 2008년07월09일

심사청구일자 2008년07월09일

(71) 출원인

고려대학교 산학협력단

서울 성북구 안암동5가1 고려대학교 내

(72) 발명자

이동훈

서울특별시 종로구 내수동 72 경희궁의아침3단지 아파트 1404호

임종인

서울 종로구 내수동 95 삼성파크팰리스 101-901

김범한

서울 송파구 방이1동 130-16호 201호

(74) 대리인

현중철

전체 청구항 수 : 총 15 항

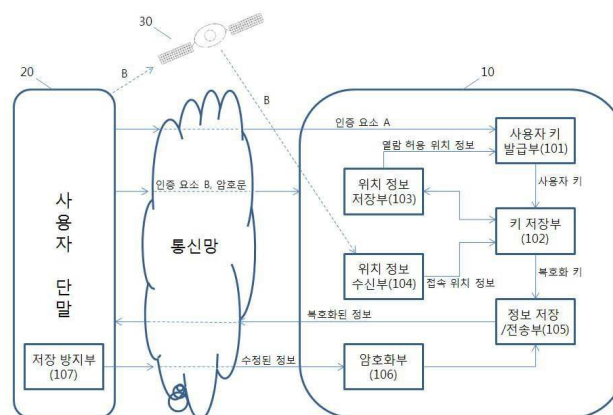
(54) 위치 기반 정보 보호 시스템 및 그 방법

(57) 요약

본 발명은 기업 등 단체 내부의 정보(기밀)가 디지털 문서화(전자 문서화)된 경우, 문서의 복사, 외부 유출, 문서에 대한 정당한 권한을 가진 사용자의 비밀키(패스워드)의 임의적 노출 등으로 인해 발생할 수 있는 정보의 유출을 위치 기반으로 방지할 수 있는 시스템에 관한 것이다.

본 명세서에서 개시하는 정보 보호 시스템은 전자 문서화(암호화)된 정보의 열람이 허용되는 위치 정보(열람 허용 위치 정보)가 반영된 사용자 키를 생성하여 사용자에게 발급하는 사용자 키 발급부; 상기 사용자가 상기 정보에 대한 정당한 권한을 가진 사용자임을 인증하는 인증 요소를 이용하여 상기 정보의 열람을 신청하는 경우, 상기 열람을 신청한 시점의 사용자의 위치 정보(접속 위치 정보)를 수신하는 위치 정보 수신부; 및 상기 발급된 사용자 키를 저장하고, 상기 접속 위치 정보가 상기 열람 허용 위치 정보에 포함하는지 판단하여, 포함되는 경우에만 상기 열람 신청된 정보가 상기 사용자에게 제공가능토록 하는 키 저장부를 포함하여 본 발명이 해결하고자 하는 과제를 해결한다.

대표도 - 도1a



특허청구의 범위

청구항 1

전자 문서화(암호화)된 정보의 열람이 허용되는 위치 정보(열람 허용 위치 정보)가 반영된 사용자 키를 생성하여 사용자에게 발급하는 사용자 키 발급부;

상기 사용자가 상기 정보에 대한 정당한 권한을 가진 사용자임을 인증하는 인증 요소를 이용하여 상기 정보의 열람을 신청하는 경우, 상기 열람을 신청한 시점의 사용자의 위치 정보(접속 위치 정보)를 수신하는 위치 정보 수신부; 및

상기 발급된 사용자 키를 저장하고, 상기 접속 위치 정보가 상기 열람 허용 위치 정보에 포함되는지 판단하여 포함되는 경우에만 상기 열람 신청된 정보가 상기 사용자에게 제공가능토록 하는 키 저장부를 포함하는 위치 기반 정보 보호 시스템.

청구항 2

제 1 항에 있어서, 상기 사용자 키 발급부는

상기 전자 문서화(암호화)된 정보의 복호화 키를 생성하고, 상기 인증 요소와 열람 허용 위치 정보를 이용하여 상기 생성된 복호화 키를 암호화하여 상기 사용자 키를 생성하는 것을 특징으로 하는 위치 기반 정보 보호 시스템.

청구항 3

제 1 항에 있어서, 상기 위치 정보 수신부는

GPS(Global Positioning System)를 이용하여 상기 접속 위치 정보를 수신하는 것을 특징으로 하는 위치 기반 정보 보호 시스템.

청구항 4

제 2 항에 있어서, 상기 키 저장부는

상기 접속 위치 정보가 상기 열람 허용 위치 정보에 포함되는 경우에만 상기 사용자 키로부터 상기 복호화 키를 추출하여, 상기 열람 신청된 정보의 복호화가 가능하게 하는 것을 특징으로 하는 위치 기반 정보 보호 시스템.

청구항 5

제 4 항에 있어서, 상기 키 저장부는

상기 인증 요소와 상기 접속 위치 정보를 트랩도어(trapdoor)로 하는 트랩도어 일방향 함수를 이용하여 상기 복호화 키를 추출하는 것을 특징으로 하는 위치 기반 정보 보호 시스템.

청구항 6

제 1 항에 있어서,

상기 열람 신청된 정보가 상기 사용자에게 제공된 후 상기 사용자가 상기 제공된 정보를 수정하면, 상기 수정된 정보를 암호화하여 상기 위치 기반 정보 보호 시스템에 저장시키는 암호화부를 더 포함하는 것을 특징으로 하는 위치 기반 정보 보호 시스템.

청구항 7

제 6 항에 있어서,

상기 수정된 정보에 대하여 상기 사용자가 저장을 시도하는 경우, 상기 수정된 정보에 대한 더 이상의 수정은 없는 것으로 간주하여 상기 수정된 정보를 상기 암호화부로 즉시 전송함으로써 상기 저장 시도를 방지하는 저장 방지부를 더 포함하는 것을 특징으로 하는 위치 기반 정보 보호 시스템.

청구항 8

(a)전자 문서화(암호화)된 정보의 열람이 허용되는 위치 정보(열람 허용 위치 정보)가 반영된 사용자 키를 생성하여 사용자에게 발급하는 단계;

(b)상기 사용자가 상기 정보에 대한 정당한 권한을 가진 사용자임을 인증하는 인증 요소를 이용하여 상기 정보의 열람을 신청하는 경우, 상기 열람을 신청한 시점의 사용자의 위치 정보(접속 위치 정보)를 수신하는 단계; 및

(c)상기 발급된 사용자 키를 저장하고, 상기 접속 위치 정보가 상기 열람 허용 위치 정보에 포함되는지 판단하여 포함되는 경우에만 상기 열람 신청된 정보가 상기 사용자에게 제공가능토록 하는 단계를 포함하는 위치 기반 정보 보호 방법.

청구항 9

제 8 항에 있어서, 상기 (a)단계는

(a1)상기 전자 문서화(암호화)된 정보의 복호화 키를 생성하는 단계; 및

(a2)상기 인증 요소와 열람 허용 위치 정보를 이용하여 상기 생성된 복호화 키를 암호화하여 상기 사용자 키를 생성하는 단계를 포함하는 것을 특징으로 하는 위치 기반 정보 보호 방법.

청구항 10

제 8 항에 있어서, 상기 (b)단계에 의한 위치 정보 수신은

GPS(Global Positioning System)를 이용하여 구현되는 것을 특징으로 하는 위치 기반 정보 보호 시스템.

청구항 11

제 9 항에 있어서, 상기 (c)단계는

상기 접속 위치 정보가 상기 열람 허용 위치 정보에 포함되는 경우에만 상기 사용자 키로부터 상기 복호화 키를 추출하여, 상기 열람 신청된 정보의 복호화가 가능하게 하여 구현되는 것을 특징으로 하는 위치 기반 정보 보호 방법.

청구항 12

제 12 항에 있어서, 상기 복호화 키는

상기 인증 요소와 상기 접속 위치 정보를 트랩도어(trapdoor)로 하는 트랩도어 일방향 함수를 이용하여 추출되는 것을 특징으로 하는 위치 기반 정보 보호 방법.

청구항 13

제 8 항에 있어서,

(d)상기 열람 신청된 정보가 상기 사용자에게 제공된 후 상기 사용자가 상기 정보를 수정하면, 상기 수정된 정보를 암호화하여 상기 전자 문서화(암호화)된 정보가 저장되었던 단말에 저장시키는 단계를 더 포함하는 것을 특징으로 하는 위치 기반 정보 보호 방법.

청구항 14

제 13 항에 있어서,

(e)상기 수정된 정보에 대하여 상기 사용자가 저장을 시도하는 경우, 상기 수정된 정보에 대한 더 이상의 수정은 없는 것으로 간주하여 상기 수정된 정보를 상기 (d)단계에 의해 즉시 암호화함으로써 상기 사용자의 저장 시도를 방지하는 단계를 더 포함하는 것을 특징으로 하는 위치 기반 정보 보호 방법.

청구항 15

제 8 항 내지 제 14 항의 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록 매체.

명세서

발명의 상세한 설명

기술 분야

- <1> 본 발명은 정보 보호 시스템 및 그 방법에 관한 것으로, 보다 상세하게는 기업 등 단체 내부의 정보(기밀)가 디지털 문서화(전자 문서화)된 경우, 문서의 복사, 외부 유출, 문서에 대한 정당한 권한을 가진 사용자의 비밀번호(패스워드)의 임의적 노출 등으로 인해 발생할 수 있는 정보의 유출을 위치 기반으로 방지할 수 있는 시스템 및 그 방법에 관한 것이다.

배경 기술

- <2> 디지털화의 과급 효과는 일상적으로 접하는 문서에 까지 미치고 있으며, 기업 등의 대부분의 단체들은 관리해야 할 업무 관련 문서의 양이 많아지고 문서의 결제처리 과정을 신속하게 진행하기 위해 전자문서 관리시스템을 구축하여 문서를 디지털화(전자화)하여 관리하고 있다. 이러한 전자 문서의 경우 복사가 쉬우며 대량의 복제본을 빠른 시간 내에 생성할 수 있는 특성으로 인해 특히 중요 기밀 사항을 담고 있는 문서가 외부로 노출되었을 경우 해당 단체에 매우 큰 손해가 발생할 수 있다.
- <3> 전자 문서화된 정보(기밀)의 노출을 방지하기 위해 대부분의 단체는 DRM(Digital Right Management) 시스템을 문서 보안에 적용하고 있다. DRM 시스템에서는 사전 발급된 라이선스를 통해서 정당한 권한을 가진 사용자(the authorized, 이하 '정당 사용자')만이 전자 문서화된 정보(기밀)를 열람, 수정 및 복사를 할 수 있게 해준다. 일반적으로 DRM에 의해 보호되는 전자 문서화된 정보(기밀)는 대칭키로 암호화되며 전자 문서화된 정보(기밀)를 암호화 한 대칭키는 정당 사용자의 공개키로 암호화되어 라이선스를 통해 배포된다. DRM 시스템에서는 정당한 개인키를 소유한 자가 정당한 패스워드를 입력한 경우에만 전자 문서화된 정보(기밀)를 복호하도록 하여 문서화된 기밀의 보호를 꾀한다.
- <4> 그러나 상기한 방식으로 보호된 전자 문서화된 정보(기밀)라 할지라도 정당 사용자가 자신의 개인키와 패스워드를 제3자에게 임의적으로 제공하는 경우 등 개인키와 패스워드가 외부에 임의적으로 노출되는 경우에는 제3자도 전자 문서화된 정보(기밀)를 열람할 수 있어, 특히 단체 내부의 정당 사용자의 악의적인 의도에 의해 단체 내부의 기밀이 무방비적으로 노출되는 문제점이 있다.

발명의 내용

해결 하고자하는 과제

- <5> 본 발명은 상기와 같은 문제를 해결하기 위해 창안된 것으로, 본 발명이 해결하고자 하는 과제는 단체 내부의 전자 문서화된 정보(기밀)를 열람(접근)할 수 있는 정당 사용자의 개인키와 패스워드가 제3자(외부)에게 임의적으로 노출되었더라도, 전자 문서화된 정보(기밀)의 보호를 꾀할 수 있는 정보 보호 시스템 및 그 방법을 제공하는 것에 있다.

과제 해결수단

- <6> 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 정보 보호 시스템은
- <7> 전자 문서화(암호화)된 정보의 열람이 허용되는 위치 정보(열람 허용 위치 정보)가 반영된 사용자 키를 생성하여 사용자에게 발급하는 사용자 키 발급부; 상기 사용자가 상기 정보에 대한 정당한 권한을 가진 사용자임을 인증하는 인증 요소를 이용하여 상기 정보의 열람을 신청하는 경우, 상기 열람을 신청한 시점의 사용자의 위치 정보(접속 위치 정보)를 수신하는 위치 정보 수신부; 및 상기 발급된 사용자 키를 저장하고, 상기 접속 위치 정보가 상기 열람 허용 위치 정보에 포함하는지 판단하여, 포함되는 경우에만 상기 열람 신청된 정보가 상기 사용자에게 제공가능도록 하는 키 저장부를 포함하여 본 시스템 발명이 해결하고자 하는 과제를 해결한다.
- <8> 상기와 같은 과제를 해결하기 위해 본 명세서에서 개시하는 정보 보호 방법은
- <9> (a)전자 문서화(암호화)된 정보의 열람이 허용되는 위치 정보(열람 허용 위치 정보)가 반영된 사용자 키를 생성하여 사용자에게 발급하는 단계; (b)상기 사용자가 상기 정보에 대한 정당한 권한을 가진 사용자임을 인증하는 인증 요소를 이용하여 상기 정보의 열람을 신청하는 경우, 상기 열람을 신청한 시점의 사용자의 위치 정보(접속

위치 정보)를 수신하는 단계; 및 (c)상기 발급된 사용자 키를 저장하고, 상기 접속 위치 정보가 상기 열람 허용 위치 정보에 포함하는지 판단하여, 포함되는 경우에만 상기 열람 신청된 정보가 상기 사용자에게 제공가능토록 하는 단계를 포함하여 본 방법 발명이 해결하고자 하는 과제를 해결한다.

효 과

- <10> 본 발명에 의할 경우, 단체 내부의 전자 문서화된 정보(기밀)에 대한 정당 사용자의 개인키와 패스워드가 임의적으로 외부에 노출되더라도, 상기 정보에 대한 접근(열람) 시도의 위치가 특정 위치 즉, 열람 허용 위치가 아닌 경우에는 접근(열람) 자체가 차단되므로 단체 내부의 전자 문서화된 정보(기밀) 보호의 확실성을 담보할 수 있다.

발명의 실시를 위한 구체적인 내용

- <11> 본 발명에 관한 구체적인 내용의 설명에 앞서 이해의 편의를 위해 본 발명이 해결하고자 하는 과제의 해결 방안의 개요를 우선 제시한다.
- <12> 본 발명에 의해 기업 등의 단체 내부의 전자 문서화된 정보(기밀)를 보호하는 방안의 핵심은, 전자 문서화된 정보(기밀)를 열람하거나 복사 등이 가능하게 하기 위해서는 정당 사용자의 개인키와 패스워드 등의 인증 요소를 요구하는 것뿐만이 아니라, 여기에 더해 전자 문서화된 정보(기밀)에 대해 특정 위치에서만 접근(열람) 가능하게 하는 것이다.
- <13> 즉, 정당 사용자의 개인키와 패스워드 등이 제3자에게 임의적으로 노출되더라도 전자 문서화된 정보(기밀)에의 접근 위치가 미리 정해진 위치 즉, 열람(접근) 허용 위치(access-admitted location)가 아닌 경우에는 정당 사용자의 개인키와 패스워드만으로는 정당 사용자에게조차도 접근(열람) 자체를 불허하여 단체 내부의 전자 문서화된 정보(기밀) 보호의 만전을 기하는 것이 본 발명이 해결하고자 하는 과제의 해결 방안의 개요이다.
- <14> 이하, 본 발명이 해결하고자 하는 과제의 해결 방안을 명확하게 하기 위한 발명의 구성을 본 발명의 바람직한 실시예에 근거하여 첨부 도면을 참조하여 상세히 설명하되, 도면의 구성요소들에 참조번호를 부여함에 있어서 동일 구성요소에 대해서는 비록 다른 도면에 있더라도 동일 참조번호를 부여하였으며 당해 도면에 대한 설명 시 필요한 경우 다른 도면의 구성요소를 인용할 수 있음을 미리 밝혀둔다.
- <15> 도 1a와 도 1b는 본 시스템 발명의 바람직한 일 구성을 제시한 도면이고, 도 2는 본 방법 발명의 바람직한 일 흐름을 제시한 도면이다.
- <16> 전자 문서화된 정보(기밀)를 저장한 단말(10)은 사용자 단말(PC, 노트북, UMPC, 휴대폰 등 컴퓨팅과 디스플레이 기능을 가지는 기기, 20)과 원격으로 분리되어 있거나(도 1a의 경우), 사용자 단말(20)에 일 모듈로 구비하여 일체형(통합형)으로 구현될 수 있다(도 1b의 경우). 분리형인 경우 본 시스템 발명의 일부 구성은 전자 문서화된 정보(기밀)를 저장한 단말(10)에, 일부 구성은 사용자 단말(20)에 구현된다. 일체형인 경우, 본 시스템 발명의 전 구성은 사용자 단말(20)에 구현된다.
- <17> 사용자 키 발급부(101)는 사용자가 기업 등 단체에 가입시에 자신이 정당 사용자임을 인증(authentication)받기 위한 인증 요소(authentication factor) A와 단체의 제반 업무에 관련된 문서에 접근(열람)이 허용되는 위치 정보(열람 허용 위치 정보)를 입력받아 상기 문서의 복호화 키를 생성하고(s111), 인증 요소와 열람 허용 위치 정보를 이용하여 복호화 키를 암호화한 사용자 키를 생성하여(s112) 사용자에게 발급하는 기능을 수행하는 부분이다. 사용자 키의 발급(s11)은 구체적으로 전자 문서화된 정보(기밀)를 저장한 단말(10)의 키 저장부(102)에 사용자 키를 저장하는 것으로 이루어진다.
- <18> 여기서 A는 '발급'을 위한 것임을 나타내는데, 이는 하기에서 언급할 B와의 구별을 위한 것이다. 인증 요소는 그 대표적인 예로 사용자 패스워드를 들 수 있는데, 만일 단말(10)로 패스워드를 전송하는 구간이 안전하지 아니하면(unsecure) 암호화적으로 보호된 형태의 다른 데이터일 수 있으며 이하의 인증 요소에서도 같다.
- <19> 복호화 키는 문서의 암호화 알고리즘에 따라 공개키 암호화 알고리즘인 경우에는 개인키, 대칭키 암호화 알고리즘인 경우에는 비밀키를 나타낸다. 한편 열람 허용 위치 정보는 전자 문서화된 정보(기밀)를 저장한 단말(10)의 열람 허용 위치 정보 저장부(103)에 저장되며, 사용자 키 발급 이벤트가 발생하면 사용자 키 발급부(101)에 전달된다. 열람 허용 위치 정보의 지정 및 저장은 단체에 의한 정보 보호 정책에 의해 이루어지겠으나, 기밀 보호의 완전성을 기하기 위해서는 가급적 최소 개수의 위치를 지정 및 저장하는 것이 타당하며, 그 위치도 단체의 관리에 의해 엄격하게 통제가능한 곳인 만이 타당할 것이다. 위치 정보의 지정 및 저장의 구체적 방식은 본 발

명의 본질적 측면과는 상관이 없으므로 더 이상의 상세한 설명은 생략한다.

- <20> 사용자가 전자 문서화된 정보(기밀)를 열람하고자 인증 요소 B(패스워드)를 자신의 단말(20)을 통해 단말(10)에 전송하여 열람을 신청하는 경우(s121), 열람을 신청한 사용자 단말(20)의 위치 정보(접속 위치 정보)가 위치 정보 수신부(104)에 수신된다(s122). 여기서 'B'는 상기의 'A'와 구별되는 것으로 정보(기밀)의 '열람(접속) 요청'을 위한 것임을 나타내는 것이다.
- <21> 한편 접속 위치 정보의 수신은, 특히 도 1a에서처럼 사용자 단말(20)이 전자 문서화된 정보(기밀)를 저장한 단말(10)과 원격으로 떨어져 있는 경우에는, 최근 많이 활성화되고 있는 GPS(Global Positioning System)에 의해 이루어지는 것이 바람직하다. 즉, 사용자가 자신의 단말(20)을 통해 단말(10)에 정보(기밀)의 열람 요청을 하면 GPS 서비스를 제공하는 인공위성(satellite, 30)에 열람(접속) 요청이 발생한 지점의 위치 정보(접속 위치 정보)가 전송되고, 위성(30)은 전송받은 접속 위치 정보를 위치 정보 수신부(104)에 전송하게 된다. 또는 사용자 단말(20)로부터 단말(10)에 열람 요청이 오면 위치 정보 수신부(104)가 열람 요청을 감지하여 직접 위성(30)에 사용자 단말(20)의 접속 위치 정보를 요구할 수 있도록 구현하는 것도 가능하다.
- <22> 위치 정보 수신부(104)는 키 저장부(102)에 접속 위치 정보를 전달하고(s123), 키 저장부(102)는 열람 허용 위치 정보 저장부(103)의 위치 정보를 조회하여 위치 정보 수신부(104)로부터 전달받은 접속 위치 정보가 열람 허용 위치 정보 저장부(103)에 저장된 열람 허용 위치 정보들 중의 하나에 포함되는지 판단한다(s124). 판단 결과 포함되지 아니하면 사용자 단말(20)에 '열람 불가(access denied)'를 통보하며, 포함되면 열람을 요청한 사용자 단말(20)의 열람에 관한 정당한 권한이 인정되는 것이므로 사용자 키로부터 열람 대상 문서의 복호화 키를 추출하여(s125) 정보 저장/전송부(105)에 전달한다. 이때, 복호화 키의 추출은 다음과 같이 이루어진다.
- <23> 복호화 키 = F(인증 요소, 접속 위치 정보, 사용자 키).
- <24> 여기서 F는 트랩도어 일방향 함수(trapdoor one-way function)로서, 트랩도어 일방향 함수는 주어진 입력에 대해 일방향성(one-way)의 성질을 가지는 출력을 생성하는 함수의 일종이며, RSA(Rivest-Shamir-Adleman) 타원곡선, ID 기반, 속성 기반 등의 암호시스템에 적용될 수 있다. 트랩도어 일방향 함수는 함수의 출력값이 주어지더라도 입력값을 알아낼 수 없는 함수이며, 보통 일방향 함수처럼 함수의 역을 구하는 것은 어렵지만 트랩도어라고 부르는 특수한 정보가 있으면 쉽게 역을 구할 수 있는 함수이다. 트랩도어 일방향 함수는 암호학 분야에서 널리 사용하는데, 트랩도어 일방향 함수를 수학적으로 정의하면 다음과 같다.
- <25> 어떤 비밀값 y가 있어서, 어떤 x에 대해서 y가 없을 때는 f(x)를 구하기 어렵지만 y가 주어진다면 f(x)에서 x값을 쉽게 찾을 수 있다면 그 함수 f는 트랩도어 일방향 함수이다. 본 발명에서 트랩도어에 해당되는 특수한 정보는 인증 요소와 접속 위치 정보이다.
- <26> 정보 저장/전송부(105)는 전자 문서화(암호화)된 정보(기밀)를 저장하고 있다가, 키 저장부(102)로부터 복호화 키를 전달받아 암호화된 정보(기밀)를 복호화하여 복호화된 정보를 사용자 단말(20)로 전송한다(s13).
- <27> 한편, 본 시스템 발명은 암호화부(106)를 더 포함하여, 만일 열람된 정보에 수정(변경)이 발생한 경우 수정된 정보에 대해서도 상기와 같은 보호 방안이 구현될 수 있도록 한다(s14). 즉, 사용자가 열람한 정보를 수정한 경우 암호화부(106)는 수정된 정보를 암호화하여 정보 저장/전송부(105)에 저장한다. 정보 저장/전송부(105)에 저장된 수정된 정보는 상기와 동일한 복호화 과정을 통해 수정전 정보와 역시 동일하게 보호를 받을 수 있다.
- <28> 한편 수정된 정보에 대하여 사용자가 악의적 의도 등으로, 특히 도 1a의 경우, 자신의 단말(20) 내지는 단말(10) 이외의 다른 단말에 임의적으로 저장을 시도하는 수가 있다. 이를 방지하기 위해 저장 방지부(107)는 사용자가 수정된 정보를 자신의 단말(20) 내지는 단말(10) 이외의 다른 단말에 저장하고자하는 경우 이를 수정이 완료된 것으로 판단하여(s141), 수정된 정보를 암호화부(106)로 바로 전달하여 암호화시키고 정보 저장/전송부(105)에 저장하는 조치를 취한다(s142). 이는 도 1b의 경우, 전자 문서화된 정보(기밀)를 저장한 단말(10)이 사용자 단말(20)과 일체형으로 구비되어 사용자가 정보 저장/전송부(105)가 아닌 단말(20)의 다른 로컬 저장 디스크에 저장을 시도하고자 하는 경우에도 마찬가지이다.
- <29> 본 방법발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.
- <30> 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 유무선 네트워크를 통한 전송)의 형태로 구현되는 것도 포함한다.

또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<31> 이제까지 본 발명에 대하여 그 바람직한 실시예를 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다.

<32> 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 균등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

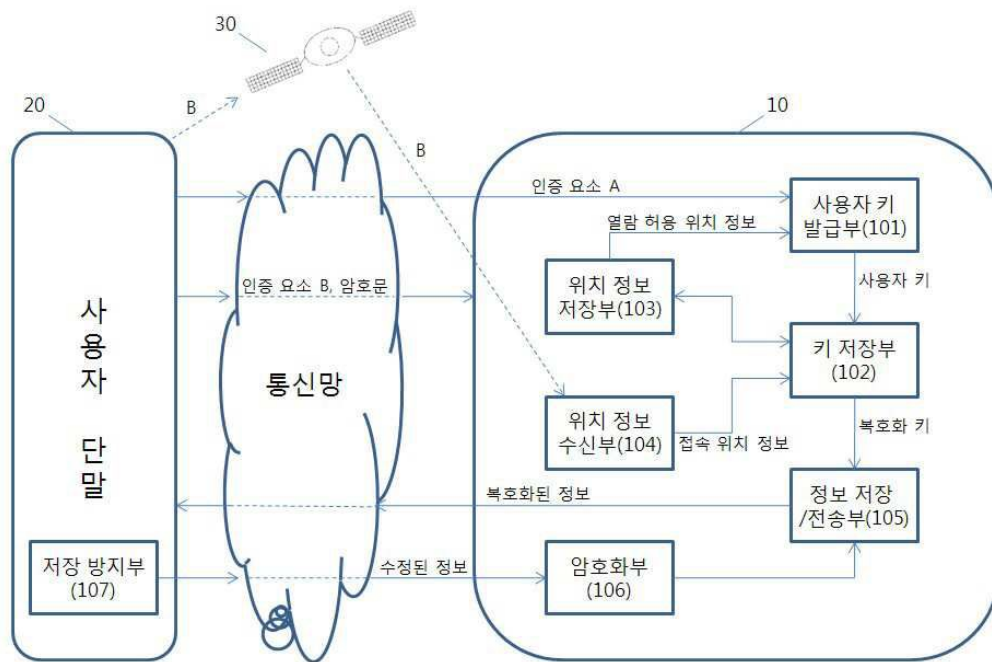
도면의 간단한 설명

<33> 도 1a와 도 1b는 본 시스템 발명의 바람직한 일 구성을 제시한 도면이다.

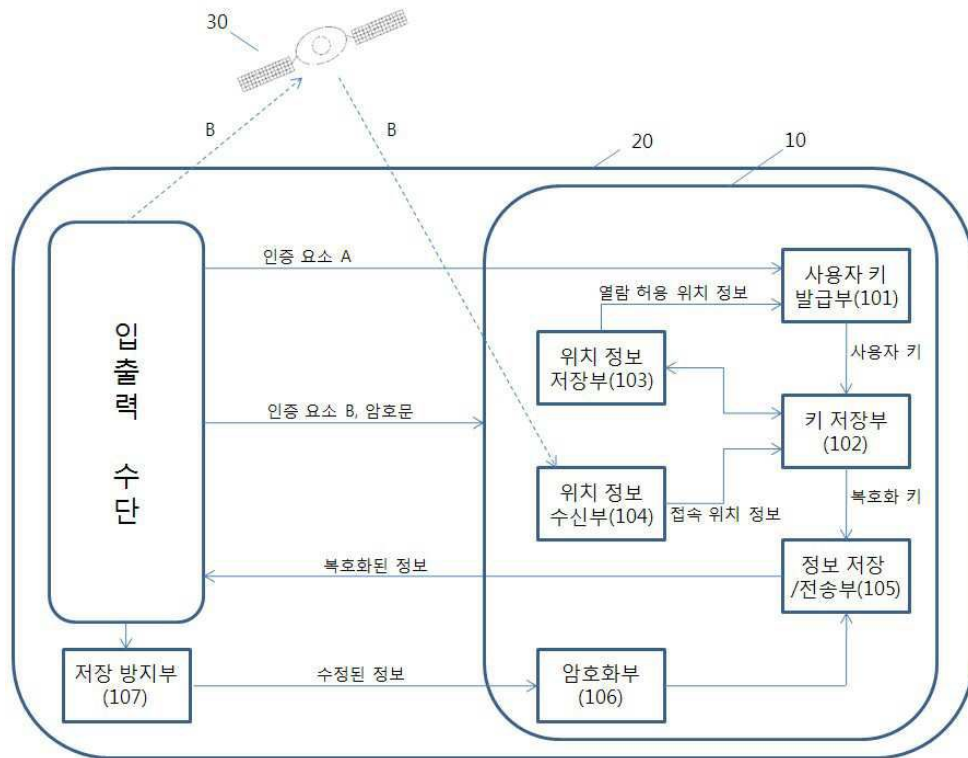
<34> 도 2는 본 방법 발명의 바람직한 일 흐름을 제시한 도면이다.

도면

도면1a



도면1b



도면2

