(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2007년11월23일
(11) 등록번호 10-0778749
(24) 등록일자 2007년11월16일

(51) Int. Cl.
G06F 21/20 (2006.01)
(21) 출원번호 10-2006-0004895
(22) 출원일자 2006년01월17일
심사청구일자 2006년01월17일
(65) 공개번호 10-2007-0076010
공개일자 2007년07월24일
(56) 선행기술조사문헌
KR1020050051210 A
전체 청구항 수 : 총 7 항

(73) 특허권자
주식회사 팬택
서울특별시 마포구 상암동 디엠씨구역 아이2블럭 팬택계열알앤디센터
(72) 발명자
최정락
서울시 동작구 노량진2동 298-9번지 1층 좌
(74) 대리인
이창훈

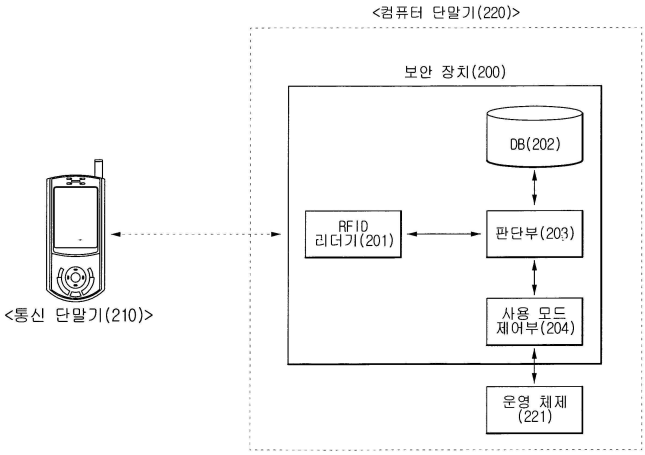
심사관 : 김견수

(54) 컴퓨터 단말기의 보안 장치 및 상기 보안 장치의 동작 방법

(57) 요 약

본 발명은 컴퓨터 단말기의 보안 장치에 관한 것으로, 통신 단말기의 RFID 태그로부터 RFID 식별정보를 수집하고, 상기 RFID 식별정보에 따라서, 상기 컴퓨터 단말기의 사용 모드를 제어하는 보안 장치 및 상기 보안 장치의 동작 방법에 관한 것이다. 본 발명에 따르면, 통신 단말기를 통해 컴퓨터 단말기의 사용을 제어하거나, 특정 데이터에 대한 사용을 제어함으로써, 사생활 보호 및 그룹 내의 중요한 정보에 대하여 보안을 강화할 수 있다.

대표도 - 도2



특허청구의 범위

청구항 1

통신 단말기에 대한 RFID 식별정보를 기록하는 데이터베이스;

상기 통신 단말기에 탑재된 RFID 태그로부터 상기 RFID 식별정보를 수집하는 RFID 리더기;

상기 데이터베이스 내에 상기 수집된 RFID 식별정보와 대응하는 RFID 식별정보가 존재하는 경우, 상기 RFID 식별정보를 인증하는 판단부; 및

상기 판단 결과, 상기 수집된 RFID 식별정보가 인증되는 경우, 상기 컴퓨터 단말기를 사용 가능 모드로 제어하는 사용 모드 제어부

를 포함하는 것을 특징으로 하는 컴퓨터 단말기의 보안 장치.

청구항 2

제1항에 있어서,

상기 판단부는,

상기 데이터베이스 내에 상기 수집된 RFID 식별정보와 대응하는 RFID 식별정보가 존재하지 않는 경우, 상기 RFID 식별정보를 인증하지 않고,

상기 사용 모드 제어부는,

상기 RFID 식별정보가 인증되지 않는 경우, 화면 보호 기능을 구동하여 상기 컴퓨터 단말기를 사용 불가능 모드로 제어하는 것을 특징으로 하는 컴퓨터 단말기의 보안 장치.

청구항 3

제1항에 있어서,

상기 데이터베이스는,

상기 RFID 식별정보에 대응하는 제어 권한을 더 기록하고,

상기 사용 모드 제어부는,

상기 수집된 RFID 식별정보가 인증되는 경우, 상기 RFID 식별정보에 대응하는 통신 단말기의 사용자에게 선정된 제어 권한을 부여하고, 상기 부여된 제어 권한에 기초하여 상기 컴퓨터 단말기를 제어하는 것을 특징으로 하는 컴퓨터 단말기의 보안 장치.

청구항 4

제1항에 있어서,

상기 통신 단말기는 컴퓨터 단말기, 통신 단말기, PSTN(Public Switched Telephone Network) 단말기, VoIP, SIP(Session Initiation Protocol), Megaco, PDA(Personal Digital Assistant), 셀룰러폰, PCS(Personal Communication Service)폰, 핸드 헬드 PC(Hand-Held PC), CDMA-2000(1X, 3X)폰, WCDMA(Wideband CDMA)폰, 듀얼 밴드/듀얼 모드(Dual Band/Dual Mode)폰, GSM(Global Standard for Mobile)폰, MBS(Mobile Broadband System)폰, 또는 위성/지상파 DMB(Digital Multimedia Broadcasting)폰 중 어느 하나인 것을 특징으로 하는 컴퓨터 단말기의 보안 장치.

청구항 5

통신 단말기에 대한 RFID 식별정보를 데이터베이스에 기록하는 단계;

상기 통신 단말기에 탑재된 RFID 태그로부터 상기 RFID 식별정보를 수집하는 단계;

상기 데이터베이스 내에 상기 수집된 RFID 식별정보와 대응하는 RFID 식별정보가 존재하는 경우, 상기 RFID 식별정보를 인증하는 단계; 및

상기 판단 결과, 상기 수집된 RFID 식별정보가 인증되는 경우, 상기 컴퓨터 단말기를 사용 가능 모드로 제어하는 단계

를 포함하는 것을 특징으로 하는 컴퓨터 단말기의 보안 장치의 동작 방법.

청구항 6

제5항에 있어서,

상기 판단 결과, 상기 수집된 RFID 식별정보가 인증되지 않는 경우, 화면 보호 기능을 구동하여 상기 컴퓨터 단말기를 사용 불가능 모드로 제어하는 단계

를 더 포함하는 것을 특징으로 하는 컴퓨터 단말기의 보안 장치의 동작 방법.

청구항 7

제5항에 있어서,

상기 데이터베이스는 상기 컴퓨터 단말기가 사용 불가능 모드로 전환된 경우, 사용자의 접근이 차단되는 소정의 데이터 목록을 더 기록하는 것을 특징으로 하는 컴퓨터 단말기의 보안 장치의 동작 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<11> 본 발명은 컴퓨터 단말기의 보안 장치에 관한 것으로, 통신 단말기의 RFID 태그로부터 RFID 식별정보를 수집하고, 상기 RFID 식별정보에 따라서, 상기 컴퓨터 단말기의 사용 모드를 제어하는 보안 장치 및 상기 보안 장치의 동작 방법에 관한 것이다.

<12> 컴퓨터 단말기는 인류의 역사상 가장 위대한 발명품이라는 수식어와 함께 사용될 만큼 인간에게 없어서는 안될 중요한 도구이다. 최근에는 반도체의 비약적인 발전과 더불어 통신 단말기의 처리 속도가 현저하게 향상되었다. 이로 인해, 인간에게 컴퓨터의 중요성은 두말할 필요 없는 당연한 사상으로 받아 들여지고 있다. 컴퓨터 단말기를 통해 인간은 여러 가지 데이터 처리, 인터넷 사용, 전화, 뱅킹, 및 쇼핑 등의 다양한 기능을 사용하고 있다. 이러한 다양한 기능의 사용에 따라 사용자는 자신의 신상 정보 등에 대한 중요한 데이터를 컴퓨터 단말기에 저장하거나, 기업의 경우에 상기 컴퓨터 단말기는 사업의 성패여부를 결정지을 수도 있는 중요한 업무 데이터를 저장한다.

<13> 현재 이러한 중요 데이터를 기록하고 처리하는 컴퓨터 단말기에 보안 기능을 제공하기 위하여, 소정의 비밀번호가 사용된다. 사용자는 사전에 입력한 숫자 또는 문자의 조합을 통해 비밀번호를 설정하고, 컴퓨터 단말기의 부팅 또는 특정 데이터의 접근 시 상기 비밀번호를 입력하여 사용을 인증 받는다. 그러나 이러한 비밀번호를 통한 인증은 간단한 장비를 통해 해킹이 가능하며, 또한, 상기 비밀번호가 인증되지 않은 제2 사용자로 노출된 경우에 중요 데이터가 외부로 유출되는 심각한 문제를 야기할 수 있다. 따라서, 보다 강화된 인증 기능을 제공하는 보안 장치의 개발이 절실히 필요한 실정이다.

발명이 이루고자 하는 기술적 과제

<14> 본 발명은 상기와 같은 종래기술을 개선하기 위해 안출된 것으로서, 통신 단말기를 통해 컴퓨터 단말기의 사용을 제어함으로써, 보안을 강화하는 것을 목적으로 한다.

<15> 본 발명의 목적은 통신 단말기를 통해 컴퓨터 단말기의 특정 데이터에 대한 사용을 제어함으로써, 사생활 보호 및 그룹 내의 중요한 정보에 대하여 보안을 강화하는 것이다.

발명의 구성 및 작용

<16> 상기의 목적을 달성하고, 상술한 종래기술의 문제점을 해결하기 위하여, 본 발명에 따른 컴퓨터 단말기의 보안

장치는 하나 이상의 고유 식별정보를 유지하는 데이터베이스 - 상기 고유 식별정보는 상기 통신 단말기의 CTN(Customer Telephone Number), ESN(Electronic Serial Number), 또는 MIN(Mobile Identification Number) 중에서 어느 하나를 포함하거나 사용자가 입력한 비밀번호 정보를 포함함 -, 상기 통신 단말기의 고유 식별정보를 기록한 RFID 태그로부터 RFID 식별정보를 수집하는 RFID 리더기, 상기 데이터베이스를 참조하여, 상기 수집된 RFID 식별정보의 인증 여부를 판단하는 판단부, 및 상기 판단부의 판단 결과, 상기 수집된 RFID 식별정보가 인증되는 경우, 상기 컴퓨터 단말기를 사용 가능 모드로 제어하는 사용 모드 제어부를 포함하는 것을 특징으로 한다.

<17> 또한, 본 발명의 일실시예에 따른 컴퓨터 단말기의 보안 장치의 동작 방법은 소정의 데이터베이스에 하나 이상의 고유 식별정보를 유지하는 단계 - 상기 고유 식별정보는 상기 통신 단말기의 CTN(Customer Telephone Number), ESN(Electronic Serial Number), 또는 MIN(Mobile Identification Number) 중에서 어느 하나를 포함하거나 사용자가 입력한 비밀번호 정보를 포함함 -, RFID 리더기를 통해 상기 통신 단말기의 고유 식별정보를 기록한 RFID 태그로부터 RFID 식별정보를 수집하는 단계, 상기 데이터베이스를 참조하여, 상기 수집된 RFID 식별정보의 인증 여부를 판단하는 단계, 및 상기 판단 결과, 상기 수집된 RFID 식별정보가 인증되는 경우, 상기 컴퓨터 단말기를 사용 가능 모드로 제어하는 단계를 포함하는 것을 특징으로 한다.

<18> 또한, 본 명세서에서 상기 통신 단말기는 컴퓨터 단말기, 통신 단말기, PSTN(Public Switched Telephone Network) 단말기, VoIP, SIP(Session Initiation Protocol), Megaco, PDA(Personal Digital Assistant), 셀룰러폰, PCS(Personal Communication Service)폰, 핸드 헬드 PC(Hand-Held PC), CDMA-2000(1X, 3X)폰, WCDMA(Wideband CDMA)폰, 듀얼 밴드/듀얼 모드(Dual Band/Dual Mode)폰, GSM(Global Standard for Mobile)폰, MBS(Mobile Broadband System)폰, 또는 위성/지상파 DMB(Digital Multimedia Broadcasting)폰 중 어느 하나인 것을 특징으로 한다.

<19> 이하 첨부된 도면을 참조하여, 본 발명에 따른 보안 장치 및 상기 보안 장치의 동작 방법에 대하여 상세히 설명한다.

<20> 도 1은 본 발명에 따른 컴퓨터 단말기의 보안 방법을 제공하기 위한 통신 단말기를 도시한 도면이다.

<21> 도 1을 참조하면, 본 발명에 따른 컴퓨터 단말기(110)는 통신 단말기(100)가 소정 반경의 범위(120)로 접근하는 경우에 상기 사용 가능 모드로 전환된다. 이를 위하여, 통신 단말기(100)는 RFID 식별정보를 기록한 RFID 태그를 유지하고, 컴퓨터 단말기(110)는 상기 RFID 식별정보를 판독할 수 있는 RFID 리더기를 유지한다. 이에, 컴퓨터 단말기(110)는 통신 단말기(100)가 소정 반경의 범위(120)이내로 접근하는 경우, 통신 단말기(100)가 유지하는 상기 RFID 태그로부터 상기 RFID 식별정보를 수집한다.

<22> 상기 컴퓨터 단말기(110)는 사전에 통신 단말기(100)로부터 RFID 식별정보를 수집하고, 데이터베이스에 기록한다. 이에, RFID 리더기를 통해 수집되는 상기 RFID 식별정보와 상기 데이터베이스에 기록된 상기 RFID 식별정보와의 대응여부를 판단한다. 상기 판단 결과, RFID 리더기를 통해 수집되는 상기 RFID 식별정보와 상기 데이터베이스에 기록된 상기 RFID 식별정보가 대응되는 경우에 컴퓨터 단말기(110)는 사용 가능 모드로 전환된다. 상기 사용 가능 모드라 함은 컴퓨터 단말기(110)의 특정 프로그램의 사용 가능 모드, 특정 데이터의 사용 가능 모드, 또는 컴퓨터 단말기(110)의 운영 체제의 사용 가능 모드 등을 모두 포함한다. 즉, 상기 RFID 식별정보를 통해 인증되지 않은 사용자는 컴퓨터 단말기(110)의 일부 또는 전체 기능을 모두 사용할 수 없게 된다. 일예로, 컴퓨터 단말기(110)는 소정의 범위 이내로 근접한 통신 단말기(100)로부터 RFID 식별정보를 수집하지 못하는 경우, 화면 보호기 등을 구동함으로써, 사용자의 조작을 원천적으로 거부한다. 이에, 통신 단말기(110)는 인증된 RFID 식별정보를 수집하는 경우에만 상기 화면 보호기 등을 해제하고, 정상적인 동작 모드로 전환될 수 있다.

<23> 본 발명의 일실시예에 따른 컴퓨터 단말기(110)의 데이터베이스는 하나 이상의 RFID 식별정보에 대응하는 제어 권한을 더 기록한다. 즉, 컴퓨터 단말기(110)를 사용하는 사용자가 복수인 경우에 제1 사용자의 통신 단말기(100)에 대한 제1 RFID 식별정보를 관리자로서 등록할 수 있다. 즉, 컴퓨터 단말기(110)는 상기 제1 RFID 식별정보를 판독하는 경우, 모든 데이터에 대하여, 읽기, 쓰기, 및 삭제 권한이 부여되고, 하드웨어 또는 소프트웨어의 조작이 가능한 제어 권한에 따라 사용 모드가 설정될 수 있다. 이와는 달리, 상기 데이터베이스는 제2 사용자의 통신 단말기(100)에 대한 제2 RFID 식별정보에 특정 기능만을 제어할 수 있는 권리를 부여할 수 있다. 즉, 상기 제2 RFID 식별정보를 수집한 컴퓨터 단말기(110)는 읽기, 쓰기, 삭제, 또는 관리 중에서 어느 하나의 권한만을 제공할 수 있다. 다른 일예로, 컴퓨터 단말기(110)는 특정 데이터에 대하여, 제3 RFID 식별정보에 대응되는 통신 단말기(100)의 사용자로 상기 특정 데이터에 대한 상기 권한을 차별적으로 부여할 수 있다.

<24> 도 2는 본 발명의 일실시예에 따른 보안 장치의 내부 구성을 도시한 블록도이다.

<25> 도 2를 참고하면, 본 발명의 일실시예에 따른 보안 장치(200)는 RFID 리더기(201), 데이터베이스(202), 판단부(203), 및 사용 모드 제어부(204)를 포함한다.

<26> RFID 리더기(201)는 통신 단말기(210)의 RFID 식별정보를 기록한 RFID 태그로부터 RFID 식별정보를 수집한다. 상기 RFID 식별정보는 컴퓨터 단말기(220)가 통신 단말기(210)의 사용자에 대한 사용 권한을 제공하기 위해 참조되는 정보이다.

<27> 데이터베이스(202)는 하나 이상의 RFID 식별정보를 유지한다. 상기 RFID 식별정보는 상기 통신 단말기의 CTN(Customer Telephone Number), ESN(Electronic Serial Number), 또는 MIN(Mobile Identification Number) 등을 포함할 수 있다. 또한, 상기 RFID 식별정보는 사용자가 입력한 비밀번호 정보를 포함할 수 있다. 상기 RFID 식별정보는 사전에 통신 단말기(210)로부터 수신하여 데이터베이스(202)에 등록된다. 데이터베이스(202)는 도 3에서 상세히 설명한다.

<28> 도 3은 본 발명의 일실시예에 따른 데이터베이스의 내부 구성을 도시한 도면이다.

<29> 도 3을 참조하면, 데이터베이스(300)는 RFID 식별정보 필드, 제어 권한 필드, 및 데이터 목록 필드를 포함한다.

<30> RFID 식별정보 필드는 하나 이상의 RFID 식별정보를 기록한다. 도 3에서는 '식별정보 #1', '식별정보 #2', 및 '식별정보 #3' 등이 RFID 식별정보 필드에 기록되어 있다.

<31> 제어 권한 필드는 상기 RFID 식별정보에 대응되는 사용자의 컴퓨터 단말기에 대한 제어 권한을 기록한다. 도 3을 참조하면, '식별정보 #1'에 대응되는 통신 단말기의 사용자는 상기 컴퓨터 단말기에 기록된 데이터에 '읽기' 제어 권한으로만 접근할 수 있다. 또한, '식별정보 #2'에 대응되는 통신 단말기의 사용자는 상기 데이터에 '읽기' 제어 권한뿐만 아니라, '쓰기' 및 '삭제' 제어 권한으로 접근할 수 있다. 이와 더불어, '식별정보 #3'에 대응되는 통신 단말기의 사용자는 '관리자' 제어 권한으로 상기 데이터뿐만 아니라, 상기 컴퓨터 단말기의 하드웨어 및 소프트웨어를 제어할 수 있다.

<32> 본 발명의 일실시예에 따른 데이터베이스(300)는 사용자의 접근의 차단 여부를 결정하는 소정의 데이터 목록 필드를 더 유지한다. 도 3을 참고하면, 상기 데이터 목록 필드는 '식별정보 #3'에 대응되는 사용자가 '읽기', '쓰기', 및 '삭제' 등을 수행하기 위한 제어 권한을 제공하기 위한 정보이다. 즉, 상기 컴퓨터 단말기가 소정의 통신 단말기로부터 상기 '식별정보 #3'의 RFID 식별정보를 수집하는 경우, 상기 사용자로 상기 '데이터 #1.doc' 및 상기 '데이터 #2'에 대하여 '읽기', '쓰기', 및 '삭제' 등의 제어 권한을 부여한다. 다른 일예로 상기 컴퓨터 단말기는 특정 데이터에 대하여, 특정 RFID 식별정보에 대응되는 통신 단말기의 사용자가 접근할 수 없도록 설정할 수 있다.

<33> 도 2에서, 판단부(203)는 데이터베이스(202)를 참조하여, 상기 수집된 RFID 식별정보의 인증 여부를 판단한다.

<34> 상기 인증 여부의 판단의 일예로, 판단부(203)는 통신 단말기(210)로부터 수신된 상기 RFID 식별정보가 데이터베이스(202)에 기록된 RFID 식별정보와 대응되는지를 판단한다.

<35> 사용 모드 제어부(204)는 판단부(203)의 판단 결과, 통신 단말기(210)로부터 수집된 RFID 식별정보가 인증되는 경우에 컴퓨터 단말기(220)를 사용 가능 모드로 제어한다. 즉, 사용 모드 제어부(204)는 상기 RFID 식별정보를 수집하는 경우, 화면 보호기 기능 등을 통해 사용 불가능 모드로 동작하던 컴퓨터 단말기(220)의 운영 체제(221)를 사용 가능 모드로 전환한다. 또한, 데이터베이스(202)를 참조 후 상기 RFID 식별정보에 대응되는 상기 제어 권한을 확인하고, 상기 RFID 식별정보에 대응되는 소정의 제어 권한을 부여할 수 있다. 따라서, 본 발명에 따른 보안 장치(200)를 구비한 컴퓨터 단말기(220)는 소정의 RFID 태그를 유지하는 통신 단말기(210)가 소정 범위 이내로 근접한 경우에 사용이 가능하다. 뿐만 아니라, 컴퓨터 단말기(220)의 사용자가 복수인 경우에 각각의 사용자의 통신 단말기(210)에 대한 RFID 식별정보 및 상기 RFID 식별정보에 대응되는 제어 권한을 통해 각각의 사용자로 차별된 제어 권한을 부여할 수 있다. 또한, 상기 컴퓨터 단말기에 기록된 데이터에 대하여, 상기 각각의 사용자가 접근할 수 있는 제어 권한을 다르게 설정할 수 있다. 이로 인하여, 통신 단말기를 통해 컴퓨터 단말기의 사용을 제어함으로써, 사생활 보호 및 그룹 내의 중요한 정보에 대하여 보안을 강화할 수 있다.

<36> 도 4는 본 발명의 일실시예에 따른 보안 장치의 동작 방법을 도시한 흐름도이다.

<37> 도 4를 참조하면, 컴퓨터 단말기의 보안 장치는 단계(401)에서, 데이터베이스에 하나 이상의 RFID 식별정보를 유지한다. 상기 RFID 식별정보는 소정의 통신 단말기에 구비된 RFID 태그에 기록된 RFID 식별정보에 대응되며,

상기 RFID 식별정보는 상기 통신 단말기의 CTN(Customer Telephone Number), ESN(Electronic Serial Number), 또는 MIN(Mobile Identification Number) 중에서 어느 하나를 포함할 수 있다. 또한, 상기 RFID 식별정보는 상기 통신 단말기의 사용자로부터 입력된 숫자 또는 문자를 포함하는 비밀번호 정보를 포함할 수 있다.

<38> 다음으로, 단계(402)에서, 상기 보안 장치는 RFID 리더기를 통해 상기 통신 단말기로부터 RFID 식별정보를 수집한다. 상기 RFID 리더기는 통신 단말기의 수동형 또는 능동형 방식의 RFID 태그로부터 RFID 식별정보를 수집할 수 있다.

<39> 이에, 상기 보안 장치는 상기 수집된 RFID 식별정보가 등록된 RFID 식별정보 인지 여부를 판단하기 위하여, 데이터베이스를 참조한다. 등록 여부에 따라, 보안 장치는 단계(403)에서 상기 RFID 식별정보가 인증된 것인지 여부를 판단한다. 판단 결과 상기 RFID 식별정보가 인증된 RFID 식별정보인 경우에 상기 보안 장치는 컴퓨터 단말기의 운영 체제로 사용 가능 모드로 전환될 것을 요청함으로써, 상기 RFID 식별정보에 대응되는 사용자로 소정의 제어 권한을 부여한다. 이에, 상기 컴퓨터 단말기는 사용 가능 모드로 전환한다.

<40> 만약, 단계(403)에서, 상기 수집된 RFID 식별정보가 인증되지 않은 정보인 경우, 상기 보안 장치는 상기 컴퓨터 단말기를 사용 불가능 모드로 전환한다. 즉, 상기 RFID 식별정보에 대응되는 사용자에게 상기 컴퓨터 단말기의 사용에 대한 어떠한 권한도 부여하지 않는다.

<41> 본 발명의 일실시예에 따른 상기 데이터베이스는 각각의 데이터에 대한 차별된 제어 권한 및 상기 제어 권한과 연관된 RFID 식별정보를 유지한다. 즉, 상기 RFID 식별정보를 수집하는 상기 보안 장치는 상기 데이터에 상기 차별된 제어 권한을 부여할 수 있다. 만약, 상기 데이터베이스에 'RFID 식별정보 #1'과 상기 'RFID 식별정보 #1'과 연관된 제어 권한으로서, '읽기'가 연관지어 기록된 경우, 상기 보안 장치는 상기 'RFID 식별정보 #1'를 수집하는 경우 컴퓨터 단말기로 모든 정보의 읽기만을 제공하도록 요청할 수 있다.

<42> 본 발명의 다른 일실시예에 따른 보안 장치는 복수의 사용자에 대한 각각의 제어 권한을 차별적으로 제공할 수 있다. 즉, 데이터베이스는 각각의 사용자에 대응되는 RFID 식별정보와 상기 RFID 식별정보에 대응되는 제어 권한을 유지하고, 특정 RFID 식별정보를 수집하는 경우, 상기 사용자에게 연관된 제어 권한을 부여할 수 있다.

<43> 본 발명에 따르면, 통신 단말기를 통해 컴퓨터 단말기의 사용을 제어함으로써, 사생활 보호 및 그룹 내의 중요한 정보에 대하여 보안을 강화할 수 있다.

<44> 도 5는 본 발명에 따른 보안 장치의 동작 방법을 수행하는데 채용될 수 있는 범용 컴퓨터 장치의 내부 블록도이다.

<45> 본 발명의 실시예들은 다양한 컴퓨터로 구현되는 동작을 수행하기 위한 프로그램 명령을 포함하는 컴퓨터 판독 가능 매체를 포함한다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 상기 매체는 프로그램 명령, 데이터 구조 등을 지정하는 신호를 전송하는 반송파를 포함하는 광 또는 금속선, 도파관 등의 전송 매체일 수도 있다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

<46> 컴퓨터 장치(500)는 램(RAM: Random Access Memory)(520)과 롬(ROM: Read Only Memory)(530)을 포함하는 주기억장치와 연결되는 하나 이상의 프로세서(510)를 포함한다. 프로세서(510)는 중앙처리장치(CPU)로 불리기도 한다. 본 기술분야에서 널리 알려져 있는 바와 같이, 롬(530)은 데이터(data)와 명령(instruction)을 단방향성으로 CPU에 전송하는 역할을 하며, 램(520)은 통상적으로 데이터와 명령을 양방향성으로 전송하는 데 사용된다. 램(520) 및 롬(530)은 컴퓨터 판독 가능 매체의 어떠한 적절한 형태를 포함할 수 있다. 대용량 기억장치(Mass Storage)(540)는 양방향성으로 프로세서(510)와 연결되어 추가적인 데이터 저장 능력을 제공하며, 상기된 컴퓨터 판독 가능 기록 매체 중 어떠한 것일 수 있다. 대용량 기억장치(540)는 프로그램, 데이터 등을 저장하는데 사용되며, 통상적으로 주기억장치보다 속도가 느린 하드 디스크와 같은 보조기억장치이다. CD 롬(560)과 같은 특정 대용량 기억장치가 사용될 수도 있다. 프로세서(510)는 비디오 모니터, 트랙볼, 마우스, 키보드, 마이크로폰, 터치스크린 형 디스플레이, 카드 판독기, 자기 또는 종이 테이프 판독기, 음성 또는 필기 인식기, 조이스틱, 또는 기타 공지된 컴퓨터 입출력장치와 같은 하나 이상의 입출력 인터페이스(550)와 연결된다.

마지막으로, 프로세서(510)는 네트워크 인터페이스(570)를 통하여 유선 또는 무선 통신 네트워크에 연결될 수 있다. 이러한 네트워크 연결을 통하여 상기된 방법의 절차를 수행할 수 있다. 상기된 장치 및 도구는 컴퓨터 하드웨어 및 소프트웨어 기술 분야의 당업자에게 잘 알려져 있다.

<47> 지금까지 본 발명에 따른 구체적인 실시예에 관하여 설명하였으나, 본 발명의 범위에서 벗어나지 않는 한도 내에서는 여러 가지 변형이 가능함은 물론이다.

<48> 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 안되며, 후술하는 특허청구의 범위뿐만 아니라 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

발명의 효과

<49> 본 발명에 따르면, 통신 단말기를 통해 컴퓨터 단말기의 사용을 제어함으로써, 보안을 강화할 수 있다.

<50> 본 발명에 따르면, 통신 단말기를 통해 컴퓨터 단말기의 특정 데이터에 대한 사용을 제어함으로써, 사생활 보호 및 그룹 내의 중요한 정보에 대하여 보안을 강화할 수 있다.

<51> 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 이는 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명 사상은 아래에 기재된 특허청구범위에 의해서만 파악되어야 하고, 이의 균등 또는 등가적 변형 모두는 본 발명 사상의 범주에 속한다고 할 것이다.

도면의 간단한 설명

<1> 도 1은 본 발명에 따른 컴퓨터 단말기의 보안 방법을 제공하기 위한 통신 단말기를 도시한 도면이다.

<2> 도 2는 본 발명의 일실시예에 따른 보안 장치의 내부 구성을 도시한 블록도이다.

<3> 도 3은 본 발명의 일실시예에 따른 데이터베이스의 내부 구성을 도시한 도면이다.

<4> 도 4는 본 발명의 일실시예에 따른 보안 장치의 동작 방법을 도시한 흐름도이다.

<5> 도 5는 본 발명에 따른 보안 장치의 동작 방법을 수행하는데 채용될 수 있는 범용 컴퓨터 장치의 내부 블록도이다.

<6> <도면의 주요 부분에 대한 부호의 설명>

<7> 200: 보안 장치 201: RFID 리더기

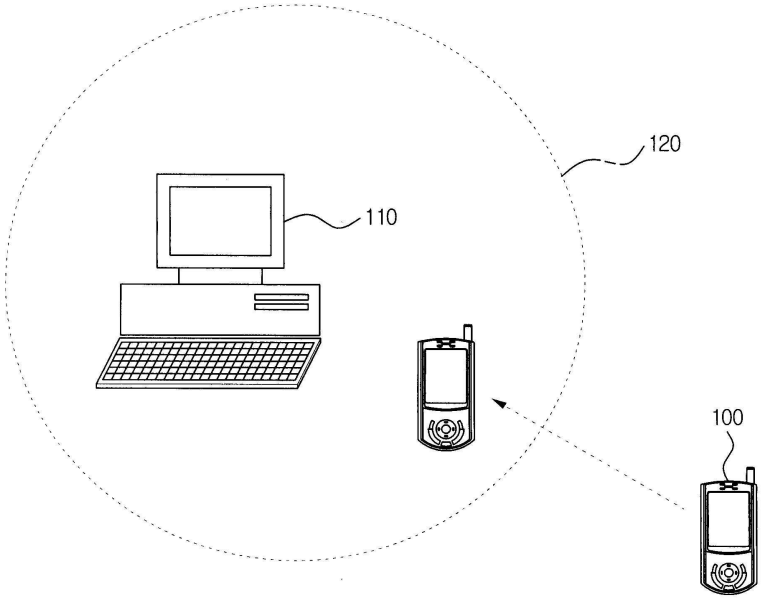
<8> 202: 데이터베이스 203: 판단부

<9> 204: 사용 모드 제어부 210: 통신 단말기

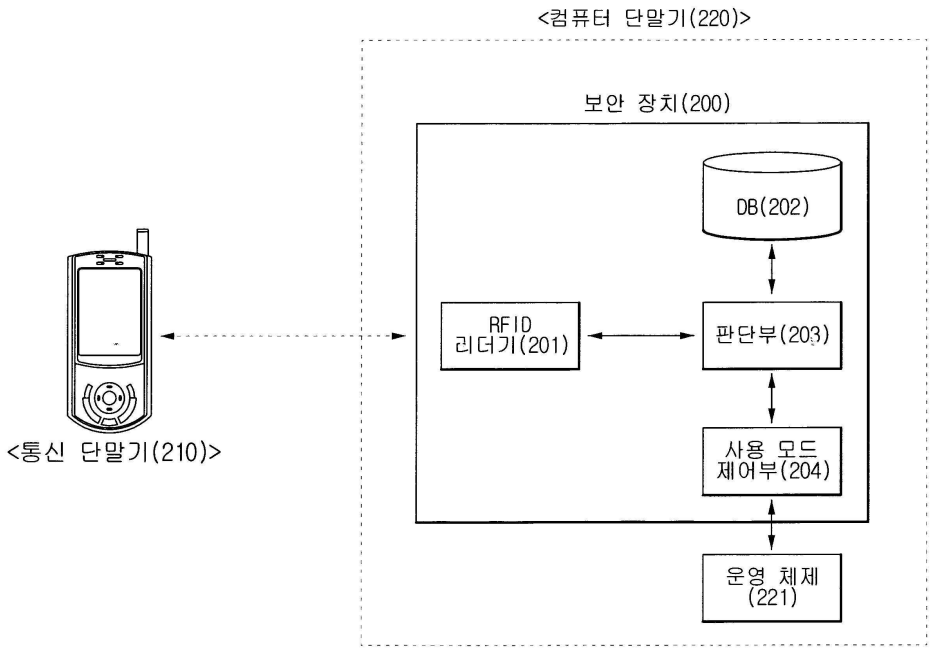
<10> 220: 컴퓨터 단말기 221: 운영 체제

도면

도면1


120
110
100

도면2

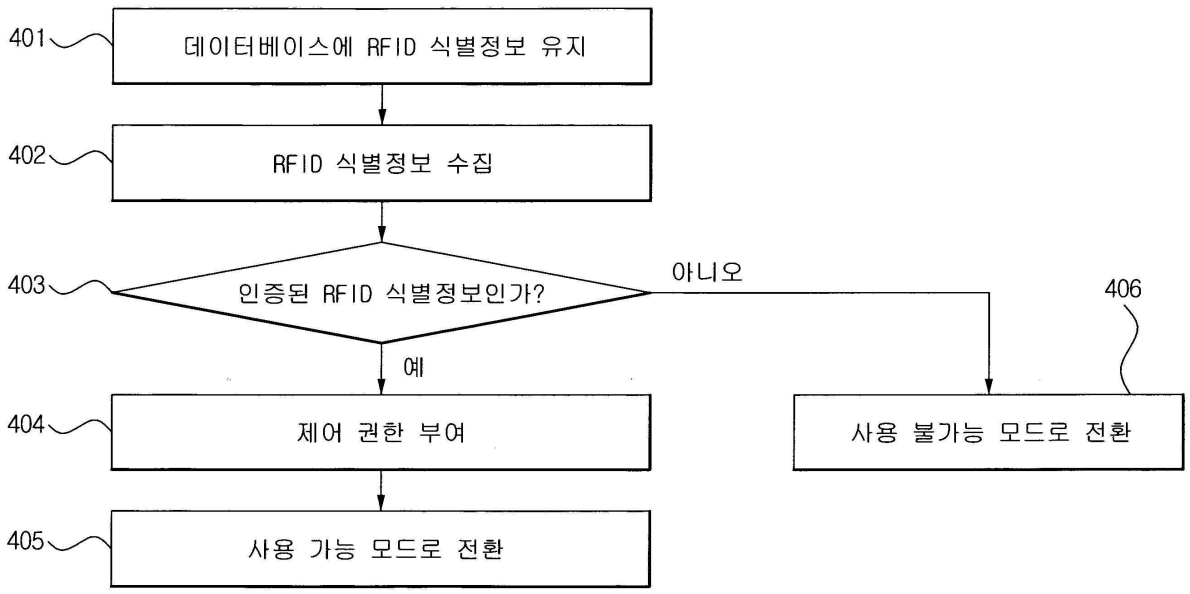

<컴퓨터 단말기(220)>
보안 장치(200)
DB(202)
RFID 리더기(201)
판단부(203)
사용 모드 제어부(204)
운영 체제 (221)
<통신 단말기(210)>

도면3

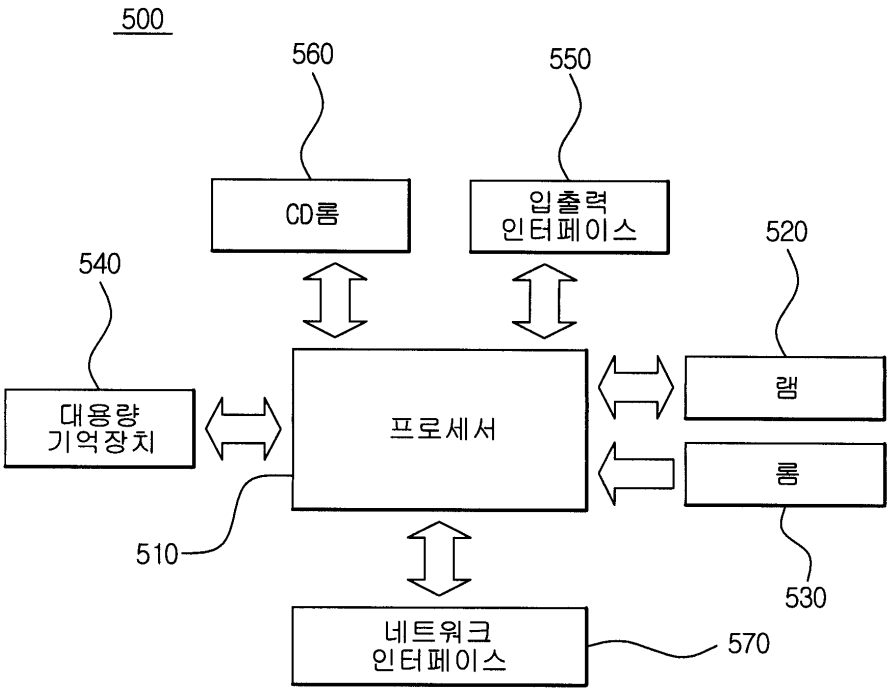
<데이터베이스(300)>

RFID 식별정보	제어 권한	데이터 목록
식별정보 #1	읽기	—
식별정보 #2	읽기, 쓰기, 삭제	—
식별정보 #3	관리자	데이터 #1.doc
• • •	• • •	데이터 #2.wmv
		• • •

도면4



도면5


500
560
550
CD롬
입출력
인터페이스
520
540
대용량
기억장치
프로세서
램
롬
510
530
네트워크
인터페이스
570