(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4925852号
(P4925852)

(45)発行日　平成24年5月9日(2012.5.9)　(24)登録日　平成24年2月17日(2012.2.17)

(51)Int.Cl.		F I		
E05B 49/00	(2006.01)	E05B	49/00	R
H04L 9/32	(2006.01)	H04L	9/00	675A
G09C 1/00	(2006.01)	G09C	1/00	640E
G06F 21/20	(2006.01)	G06F	21/20	131A
G06K 17/00	(2006.01)	G06K	17/00	V

請求項の数 12　(全 20 頁)　最終頁に続く

(21)出願番号　特願2007-33075(P2007-33075)
(22)出願日　平成19年2月14日(2007.2.14)
(65)公開番号　特開2008-196217(P2008-196217A)
(43)公開日　平成20年8月28日(2008.8.28)
審査請求日　平成21年12月28日(2009.12.28)

(73)特許権者　000139780
株式会社イトーキ
大阪府大阪市城東区今福東１丁目４番１２号
(74)代理人　100088672
弁理士　吉竹　英俊
(74)代理人　100088845
弁理士　有田　貴弘
(72)発明者　大谷　和史
大阪府大阪市城東区今福東１丁目４番１２号　株式会社イトーキ内

審査官　深田　高義

最終頁に続く

(54)【発明の名称】認証システム、端末装置、権限書込装置及び認証ロック装置

(57)【特許請求の範囲】
【請求項１】
ロック対象物の認証を行う認証システムであって、
利用権限情報と利用可能条件情報とを記憶可能な端末側記憶部と、人体を通信経路とした人体通信を行う端末側人体通信部と、前記端末側人体通信部を通じた通信結果に応じて、前記端末側人体通信部を通じて受信した利用権限情報と利用可能条件情報とを前記端末記憶部に書込み、又は、前記端末側記憶部に記憶された利用権限情報と利用可能条件情報とを前記端末側人体通信部を通じて外部に送信する端末側制御部とを有する端末装置と、
個人認証情報を取得する個人認証部と、人体を通信経路とした人体通信を行う権限書込側人体通信部と、個人認証情報と前記ロック対象物の利用権限情報とを対応づけた利用権限書込情報を記憶した権限書込側記憶部と、前記個人認証部で取得された個人認証情報と前記権限書込記憶部側に記憶された利用権限書込情報とに基づいて決定される利用権限情報を利用可能条件情報と共に書込む指令を、前記権限書込側人体通信部を介して外部に送信する権限書込制御部とを有する権限書込装置と、
前記ロック対象物に設けられ、人体を通信経路とした人体通信を行う認証ロック側人体通信部と、前記ロック対象物をロック状態又はアンロック状態にするロック部と、前記端末装置から前記認証ロック側人体通信部を通じて受信される利用権限情報と利用可能条件情報とに基づいて利用の可否を判断し、利用可と判断された場合に前記ロック部をロック状態からアンロック状態に切替えるように制御するロック制御部とを有する認証ロック装置と、

を備えた認証システム。
【請求項２】
請求項１記載の認証システムであって、
前記権限書込装置は、前記権限書込側記憶部に予め記憶された利用可能回数情報と、計時回路からの計時信号に基づいて決定される書込時間情報とのうち少なくとも一方を含む利用可能条件情報を決定し、
前記ロック制御部は、前記端末装置から前記認証ロック側人体通信部を通じて受信される利用可能条件情報に基づいて、利用可能回数情報と書込時間情報とのうち少なくとも一方に基づいて規定される条件を満たすか否かを判断し、その条件を満たさない場合に利用不可と判断する、認証システム。
【請求項３】
請求項１又は請求項２記載の認証システムであって、
前記利用権限情報は、識別符号であり、
前記認証ロック装置は、識別符号と前記ロック対象物の利用諾否とを対応づけた利用諾否情報を記憶した認証ロック側記憶部を有し、
前記ロック制御部は、前記端末装置から前記認証ロック側人体通信部を通じて受信される識別符号と前記認証ロック側記憶部に記憶された利用諾否情報とに基づいて利用の可否を判断する、認証システム。
【請求項４】
請求項１～請求項３のいずれかに記載の認証システムであって、
個人認証部は、生体に固有の情報を取得する生体認証装置である、認証システム。
【請求項５】
請求項４記載の認証システムであって、
前記個人認証部は、生体が接触することで認証を行う生体認証装置であり、
前記権限書込側人体通信部は、生体が前記生体認証装置に接触する際に、その生体に接触可能な人体通信用電極を有する、認証システム。
【請求項６】
請求項１～請求項３のいずれかに記載の認証システムであって、
前記個人認証部は、利用者に付与された個人認証端末との間で近接通信を行う個人認証通信部を有し、
前記権限書込側人体通信部は、前記個人認証端末を前記個人認証通信部に近接させようとする手と接触可能な位置に配設された人体通信用電極を有する、認証システム。
【請求項７】
請求項１～請求項６のいずれかに記載の認証システムであって、
前記権限書込装置は、前記ロック対象物が存在するエリアの入口に設置された、認証システム。
【請求項８】
請求項１～請求項７のいずれかに記載の認証システムであって、
前記認証ロック装置は、
前記ロック部として、
前記ロック対象物としての格納手段に取付けられた開閉部をロック及びアンロックする格納ロック部と、
部屋の出入口扉をロック及びアンロックする出入口扉ロック部と、
電気機器を使用不能にロック及び使用可能にアンロックする制御ロック部と、
とのうち少なくとも１つを含む、認証システム。
【請求項９】
請求項１～請求項８のいずれかに記載の認証システムであって、
前記認証ロック側人体通信部は、前記ロック対象物を利用するにあたって人体が直接的に又は間接的に接触する接触部を人体通信用電極として有する、認証システム。
【請求項１０】

ロック対象物の認証を行うための端末装置であって、
利用権限情報と利用可能条件情報とを記憶可能な端末側記憶部と、
人体を通信経路とした人体通信を行う端末側人体通信部と、
前記端末側人体通信部を通じた通信結果に応じて、前記端末側人体通信部を通じて受信した利用権限情報と利用可能条件情報とを前記端末記憶部に書込み、又は、前記端末側記憶部に記憶された利用権限情報と利用可能条件情報とを前記端末側人体通信部を通じて外部に送信する端末側制御部と、
を備えた端末装置。
【請求項１１】
ロック対象物の認証を行うための端末装置に情報書込み可能な権限書込装置であって、
個人認証情報を取得する個人認証部と、
人体を通信経路とした人体通信を行う権限書込側人体通信部と、
個人認証情報と前記ロック対象物の利用権限情報とを対応づけた利用権限書込情報を記憶した権限書込側記憶部と、
前記個人認証部で取得された個人認証情報と前記権限書込記憶部側に記憶された利用権限書込情報とに基づいて決定される利用権限情報を利用可能条件情報と共に書込む指令を、前記権限書込側人体通信部を介して外部に送信する権限書込制御部と、
を備えた権限書込装置。
【請求項１２】
ロック対象物に設けられ、端末装置との間で通信してロック対象物の認証を行う認証ロック装置であって、
人体を通信経路とした人体通信を行う認証ロック側人体通信部と、
前記ロック対象物をロック状態又はアンロック状態にするロック部と、
前記端末装置から前記認証ロック側人体通信部を通じて受信される利用権限情報と利用可能条件情報とに基づいて利用の可否を判断し、利用可と判断された場合に前記ロック部をロック状態からアンロック状態に切替えるように制御するロック制御部と、
を備えた認証ロック装置。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、人体通信を利用して、キャビネット等の利用権限を認証する技術に関する。
【背景技術】
【０００２】
キャビネット等の利用権限を認証する技術として、各利用者に無線端末装置を付与すると共に、キャビネット側に前記無線端末装置と通信可能な錠装置を取付けたシステムである。
【０００３】
このシステムでは、無線端末装置を所持する利用者が、所定のキャビネットを利用しようとする場合に、無線端末装置と錠装置とが無線通信を行って、当該キャビネットを利用できるか否かの認証動作を行うようになっている。そして、利用可と判断された場合に、錠装置は解錠動作を行い、利用者は当該キャビネットを利用できるようになる。一方、利用不可と判断された場合には、錠装置は施錠状態を維持し、利用者は当該キャビネットを利用できない。
【０００４】
このような技術は、例えば、特許文献１に開示されている。
【０００５】
【特許文献１】特開２００６－２５７８２２号公報
【発明の開示】
【発明が解決しようとする課題】

【０００６】
しかしながら、上記のように、無線通信によって認証を行う技術では、利用権限を持つ人が利用対象物近くに存在する状況で、他の利用権限の無い人が当該利用対象物を利用しようとすると、利用権限を持つ人が所持する誤った無線端末装置との間で無線通信が成立し、誤った認証がなされてしまう恐れがある。
【０００７】
また、正規の所有者でなくとも、無線端末装置を所有さえしていれば、認証装置で利用可と判断され、利用対象物を利用できてしまう。このため、無線通信端末装置を無くしてしまうと、正規の利用者が利用できないだけでなく、悪用されてしまう恐れがある。
【０００８】
ここで、各利用者に与えられた端末装置と、利用対象物に設けられた認証装置との間で、人体通信を行って認証を行うようにすると、誤った通信成立が抑制され、誤った認証を防止して、前者の問題を解決し得る。
【０００９】
しかしながら、この場合でも、端末装置さえ所有していれば、認証装置で利用可と判断されてしまうため、その端末装置を拾得した者に悪用されてしまうという問題は残る。
【００１０】
ここで、正規の利用者が紛失に気付けば、認証装置側で、当該個人識別ＩＤ情報を無効化することで、その後の不正使用を防止することができる。しかしながら、人体通信を行う端末装置では、その性質上、普段あまり意識しない形態、例えば、リストバンドの形態や名札の形態で利用されるため、その紛失に気付かないことが多く、悪用される可能性は高まる。
【００１１】
そこで、本発明は、誤った認証及び悪用を有効に防止しうる技術を提供することを目的とする。
【課題を解決するための手段】
【００１２】
上記課題を解決するため、この認証システムは、ロック対象物の認証を行う認証システムであって、利用権限情報と利用可能条件情報とを記憶可能な端末側記憶部と、人体を通信経路とした人体通信を行う端末側人体通信部と、前記端末側人体通信部を通じた通信結果に応じて、前記端末側人体通信部を通じて受信した利用権限情報と利用可能条件情報とを前記端末記憶部に書込み、又は、前記端末側記憶部に記憶された利用権限情報と利用可能条件情報とを前記端末側人体通信部を通じて外部に送信する端末側制御部とを有する端末装置と、個人認証情報を取得する個人認証部と、人体を通信経路とした人体通信を行う権限書込側人体通信部と、個人認証情報と前記ロック対象物の利用権限情報とを対応づけた利用権限書込情報を記憶した権限書込側記憶部と、前記個人認証部で取得された個人認証情報と前記権限書込記憶部側に記憶された利用権限書込情報とに基づいて決定される利用権限情報を利用可能条件情報と共に書込む指令を、前記権限書込側人体通信部を介して外部に送信する権限書込制御部とを有する権限書込装置と、前記ロック対象物に設けられ、人体を通信経路とした人体通信を行う認証ロック側人体通信部と、前記ロック対象物をロック状態又はアンロック状態にするロック部と、前記端末装置から前記認証ロック側人体通信部を通じて受信される利用権限情報と利用可能条件情報とに基づいて利用の可否を判断し、利用可と判断された場合に前記ロック部をロック状態からアンロック状態に切替えるように制御するロック制御部とを有する認証ロック装置とを備えたものである。ここで、人体通信を行う人体通信部とは、人体を通信経路として通信を行う構成をいう。
【００１３】
この場合に、前記権限書込装置は、前記権限書込側記憶部に予め記憶された利用可能回数情報と、計時回路からの計時信号に基づいて決定される書込時間情報とのうち少なくとも一方を含む利用可能条件情報を決定し、前記ロック制御部は、前記端末装置から前記認証ロック側人体通信部を通じて受信される利用可能条件情報に基づいて、利用可能回数情

報と書込時間情報とのうち少なくとも一方に基づいて規定される条件を満たすか否かを判断し、その条件を満たさない場合に利用不可と判断してもよい。

【００１４】

また、前記利用権限情報は、識別符号であり、前記認証ロック装置は、識別符号と前記ロック対象物の利用諾否とを対応づけた利用諾否情報を記憶した認証ロック側記憶部を有し、前記ロック制御部は、前記端末装置から前記認証ロック側人体通信部を通じて受信される識別符号と前記認証ロック側記憶部に記憶された利用諾否情報とに基づいて利用の可否を判断してもよい。

【００１５】

また、個人認証部は、生体に固有の情報を取得する生体認証装置であってもよい。

【００１６】

この場合に、前記個人認証部は、生体が接触することで認証を行う生体認証装置であり、前記権限書込側人体通信部は、生体が前記生体認証装置に接触する際に、その生体に接触可能な人体通信用電極を有していてもよい。

【００１７】

また、前記個人認証部は、利用者に付与された個人認証端末との間で近接通信を行う個人認証通信部を有し、前記権限書込側人体通信部は、前記個人認証端末を前記個人認証通信部に近接させようとする手と接触可能な位置に配設された人体通信用電極を有していてもよい。

【００１８】

また、前記権限書込装置は、前記ロック対象物が存在するエリアの入口に設置されていてもよい。

【００１９】

また、前記認証ロック装置は、前記ロック部として、前記ロック対象物としての格納手段に取付けられた開閉部をロック及びアンロックする格納ロック部と、部屋の出入口扉をロック及びアンロックする出入口扉ロック部と、電気機器を使用不能にロック及び使用可能にアンロックする制御ロック部と、とのうち少なくとも１つを含んでいてもよい。

【００２０】

また、前記認証ロック側人体通信部は、前記ロック対象物を利用するにあたって人体が直接的に又は間接的に接触する接触部を人体通信用電極として有していてもよい。

【００２１】

また、この端末装置は、ロック対象物の認証を行うための端末装置であって、利用権限情報と利用可能条件情報とを記憶可能な端末側記憶部と、人体を通信経路とした人体通信を行う端末側人体通信部と、前記端末側人体通信部を通じた通信結果に応じて、前記端末側人体通信部を通じて受信した利用権限情報と利用可能条件情報とを前記端末記憶部に書込み、又は、前記端末側記憶部に記憶された利用権限情報と利用可能条件情報とを前記端末側人体通信部を通じて外部に送信する端末側制御部とを備えたものである。

【００２２】

また、この権限書込装置は、ロック対象物の認証を行うための端末装置に情報書込み可能な権限書込装置であって、個人認証情報を取得する個人認証部と、人体を通信経路とした人体通信を行う権限書込側人体通信部と、個人認証情報と前記ロック対象物の利用権限情報とを対応づけた利用権限書込情報を記憶した権限書込側記憶部と、前記個人認証部で取得された個人認証情報と前記権限書込記憶部側に記憶された利用権限書込情報とに基づいて決定される利用権限情報を利用可能条件情報と共に書込む指令を、前記権限書込側人体通信部を介して外部に送信する権限書込制御部とを備えたものである。

【００２３】

さらに、この認証ロック装置は、ロック対象物に設けられ、端末装置との間で通信してロック対象物の認証を行う認証ロック装置であって、人体を通信経路とした人体通信を行う認証ロック側人体通信部と、前記ロック対象物をロック状態又はアンロック状態にするロック部と、前記端末装置から前記認証ロック側人体通信部を通じて受信される利用権限

情報と利用可能条件情報とに基づいて利用の可否を判断し、利用可と判断された場合に前記ロック部をロック状態からアンロック状態に切替えるように制御するロック制御部とを備えたものである。

【発明の効果】

【００２４】

この認証システムによると、端末装置と認証ロック装置との間で人体通信を行うため、利用者が所持する端末装置と認証ロック装置との間で人体通信が行われて、利用の可否が判断される。このため、非利用者が所持する誤った端末装置との通信が抑制され、誤った認証を防止し得る。

【００２５】

また、権限書込装置で個人認証情報を取得し、この個人認証情報と利用権限書込情報とに基づいて決定される利用権限情報と利用可能条件情報とを端末装置に書込むようにしている。そして、認証ロック装置では、前記端末装置から前記認証ロック側人体通信部を通じて受信される利用権限情報と利用可能条件情報とに基づいて利用の可否を判断し、利用可と判断された場合に前記ロック部をアンロック状態にするように制御している。このため、利用可能条件を満たす場合にロック部をアンロック状態にできるので、悪用を有効に防止しうる。

【００２６】

また、前記権限書込装置は、前記権限書込側記憶部に予め記憶された利用可能回数情報と、計時回路からの計時信号に基づいて決定される書込時間情報とのうち少なくとも一方を含む利用可能条件情報を決定し、前記ロック制御部は、前記端末装置から前記認証ロック側人体通信部を通じて受信される利用可能条件情報に基づいて、利用可能回数情報と書込時間情報とのうち少なくとも一方に基づいて規定される条件を満たすか否かを判断し、その条件を満たさない場合に利用不可と判断すると、例えば、端末装置紛失後、所定時間経過したり、また、利用可能回数を満たさなくなれば、ロック対象物を利用できないようになる。

【００２７】

さらに、前記ロック制御部は、前記端末装置から前記認証ロック側人体通信部を通じて受信される識別符号と前記認証ロック側記憶部に記憶された利用諾否情報とに基づいて利用の可否を判断することで、認証ロック装置側で各利用の可否を変更等できる。

【００２８】

また、個人認証部が、生体に固有の情報を取得する生体認証装置であると、利用者は手ぶらで個人認証を行えるので便利である。

【００２９】

また、前記個人認証部は、生体が接触することで認証を行う生体認証装置であり、前記権限書込側人体通信部は、生体が前記生体認証装置に接触する際に、その生体に接触可能な人体通信用電極を有すると、利用者による認証動作の際に端末装置に書込みを行うことができる。

【００３０】

また、前記個人認証部は、利用者に付与された個人認証端末との間で近接通信を行う個人認証通信部を有し、前記権限書込側人体通信部は、前記個人認証端末を前記個人認証通信部に近接させようとする手と接触可能な位置に配設された人体通信用電極を有すると、利用者が認証させようとして個人認証端末を個人認証通信部に近接させる際に、人体通信を行って利用権限情報の書込みを行うことができる。

【００３１】

また、前記権限書込装置は、前記ロック対象物が存在するエリアの入口に設置されていると、利用者が入口を通過する際に、端末装置に利用権限情報を書込むことができる。

【００３２】

また、前記認証ロック装置は、前記ロック部として、前記ロック対象物としての格納手段に取付けられた開閉部をロック及びアンロックする格納ロック部と、部屋の出入口扉を

ロック及びアンロックする出入口扉ロック部と、電気機器を使用不能にロック及び使用可能にアンロックする制御ロック部と、とのうち少なくとも１つを含むと、格納手段の利用や入室、パソコンの利用等を制限できる。

【００３３】

また、前記認証ロック側人体通信部は、前記ロック対象物を利用するにあたって人体が直接的に又は間接的に接触する接触部を人体通信用電極として有すると、利用者がロック対象物を利用するにあたって接触部に接触することで、認証が行われるため、特別な動作操作が不要となる。

【００３４】

また、この端末装置によると、人体通信を行うため、誤った認証を防止できる。また、端末側記憶部に、利用権限情報と利用可能条件情報とが記憶可能であり、端末制御部は、前記端末側人体通信部を通じた通信結果に応じて、前記端末側人体通信部を通じて受信した利用権限情報と利用可能条件情報とを前記端末記憶部に書込み、又は、前記端末側記憶部に記憶された利用権限情報と利用可能条件情報とを前記端末側人体通信部を通じて外部に送信するため、利用可能条件情報を利用可否の判断材料として提供することができ、悪用を有効に防止しうる。

【００３５】

また、この権限書込装置によると、個人認証情報を行って利用権限情報等の書込みを行うため、正当権限ある者が所持する端末装置に、利用権限情報と利用可能条件情報とを書込むことができる。そして、ロック対象物の利用可否判断材料として、この利用権限情報と利用可能条件情報とを提供することができるため、悪用を有効に防止しうる。

【００３６】

また、この認証ロック装置によると、端末装置と人体通信を行うため、誤った認証を防止できる。また、ロック制御部は、前記端末装置から前記認証ロック側人体通信部を通じて受信される前記利用権限情報と前記利用可能条件情報とに基づいて利用の可否を判断し、利用可と判断された場合に前記ロック部をアンロック状態にするため、悪用を有効に防止しうる。

【発明を実施するための最良の形態】

【００３７】

以下、実施形態にかかる認証システムについて説明する。

【００３８】

＜１．全体構成＞

まず、認証システムの全体構成について説明する。図１は認証システムの全体構成を示す説明図である。

【００３９】

この認証システムは、ロック対象物の認証を行うシステムであり、端末装置２０と、権限書込装置４０と、認証ロック装置６０とを備えている。

【００４０】

ロック対象物は、利用不能なロック状態と利用可能なアンロック状態とで切替えて管理される物である。このようなロック対象物としては、格納手段に取付けられた開閉部や、部屋の出入口扉、電気機器等が想定される。ここでは、ロック対象物が、格納手段としての開閉部であるキャビネット１０の扉１２や引出部１３である場合（図８参照）、部屋Ｒの出入口扉１６である場合、電気機器としてのパーソナルコンピュータ１８である場合について説明する。

【００４１】

上記端末装置２０は、本システムの利用者に付与される。権限書込装置４０は、各端末装置２０に対して共通に用いられる装置であり、好ましくは、利用者が本システムを利用するにあたって通過する場所、例えば、本システムの出入口等に設置される。認証ロック装置６０は、各利用対象物に設けられる装置であり、当該利用対象物をロック状態又はアンロック状態に切替える装置である。

【００４２】
本システムの概略的な使用方法を説明しておくと、この認証システムを利用する利用者は、端末装置２０を所持して権限書込装置４０前に移動する。そして、権限書込装置４０が、当該利用者が正規の利用者であるか否かを個人認証し、正規の利用者である場合に、当該利用者が所持する端末装置２０に利用権限情報と利用可能条件情報とを書込む。
【００４３】
この後、利用者は、当該端末装置２０を所持して扉１２や出入口扉１６、パーソナルコンピュータ１８前に移動する。そして、認証ロック装置６０は、当該利用者が所持する当該端末装置２０と人体通信を行って、利用の可否を判断し、利用可と判断された場合に、アンロック状態に切替える。これにより、利用者は当該扉１２や出入口扉１６を開いたり、パーソナルコンピュータ１８を利用できるようになる。
【００４４】
以下、各部構成についてより詳細に説明する。
【００４５】
＜２．端末装置＞
図２は端末装置と権限書込装置とを示すブロック図であり、図３は端末装置と認証ロック装置とを示すブロック図である。
【００４６】
端末装置２０は、端末側の記憶部２２と、端末側の人体通信部としての人体通信回路部２４ａ及び人体通信用電極２４ｂと、端末側制御部２６とを有している。
【００４７】
端末側制御部２６は、ＣＰＵ、ＲＯＭおよびＲＡＭ等を備える一般的なマイクロコンピュータにより構成され、予め格納されたソフトウェアプログラムによって演算動作を行い後述する処理を実行する。
【００４８】
記憶部２２は、フラッシュメモリ等の書換え可能な不揮発性メモリによって構成されており、利用権限情報としての個人識別ＩＤと、利用可能条件情報としての書込時間とを記憶可能に構成されている。
【００４９】
人体通信回路部２４ａは、変調回路及び復調回路、増幅回路等を有しており、端末側制御部２６より与えられる信号を変調等して人体通信用電極２４ｂに出力し、或は、当該人体通信用電極２４ｂを通じて受信された信号を復調等して端末側制御部２６に与える。また、人体通信用電極２４ｂは、人体に対して直接的に又は衣服等を介して間接的に接触可能に設けられている。これにより、人体通信回路部２４ａは、人体を通信経路とした人体通信を行う。なお、人体通信部としては、人体に電流信号を流して通信する構成の他、人体に電圧信号を印加して静電結合を利用して通信する構成等を含む。
【００５０】
図４は端末装置の動作を示すフローチャートである。
【００５１】
まず、端末装置２０は、後述する処理終了後の通常状態ではより電力消費量の少ない休止モードとなっており、権限書込装置４０又は認証ロック装置６０から人体を経由した信号を受信する等、人体通信用電極２４ｂを経由して所定電圧レベル以上の電気信号を受信することで起動して動作モードに移行する。これにより、端末装置２０の省電力化が図られる。
【００５２】
そして、端末装置２０の起動後、まず、ステップＳ１において、人体通信の成立の有無が判定される。ここで、人体通信の成立が否定されると、ステップＳ１に戻り、人体通信が成立したと判断されると、ステップＳ２に進む。
【００５３】
ステップＳ２では、人体通信によって受信された信号に書込み要求が含まれているか、

読出し要求が含まれているかを判断する。
【００５４】
ここで、書込み要求が含まれていると判断された場合には、ステップＳ３に進む。ステップＳ３では、人体通信によって受信された信号に含まれている個人識別ＩＤと書込時間とを記憶部２２に書込み、処理を終了する。
【００５５】
一方、ステップＳ２で、読出し要求が含まれていると判断された場合には、ステップＳ４に進む。ステップＳ４では、記憶部２２に記憶されている個人識別ＩＤと書込時間とを読出して、人体通信回路部２４ａ及び人体通信用電極２４ｂを介して外部に向けて送信し、処理を終了する。
【００５６】
このような端末装置２０は、各利用者に付与される。付与形態としては、各利用者に永続的又は継続的に付与される形態（つまり、専用品として付与される形態）であっても、各利用者に本システムの利用の度に付与される形態（つまり、共有品として利用される形態）であってもよい。
【００５７】
また、端末装置２０は、各利用者に常時身につける形態として構成されることが好ましい。例えば、端末装置２０は、利用者の手首に装着されるリストバンドとしての形態（図７参照）や、首からぶら下げられるネックストラップとしての形態、ピン等で衣服に装着される名札状の形態として構成される。その他、端末装置２０は衣服のポケット等に収納可能なカード形状に構成されていてもよく、また、携帯電話に組込まれていてもよい。
【００５８】
＜３．権限書込装置＞
図７は権限書込装置を示す斜視図である。図２及び図７に示すように、権限書込装置４０は、権限書込側の記憶部４２と、権限書込側の人体通信部としての人体通信回路部４４ａ及び人体通信用電極４４ｂと、権限書込制御部４６と、個人認証部としての個人認証部４８とを有している。
【００５９】
権限書込制御部４６は、ＣＰＵ、ＲＯＭおよびＲＡＭ等を備える一般的なマイクロコンピュータにより構成され、予め格納されたソフトウェアプログラムによって演算動作を行い後述する処理を実行する。なお、この権限書込制御部４６は、計時回路４６ａを内蔵している。
【００６０】
記憶部４２は、フラッシュメモリ等の書換え可能な不揮発性メモリによって構成されており、個人認証情報とロック対象物の利用権限情報である個人識別ＩＤとを対応づけた利用権限書込情報を記憶可能に構成されている。ここでは、個人認証情報として、予め登録された各利用者の指紋データを記憶している。また、利用権限書込情報は本システムの管理者によって予め設定登録されている。
【００６１】
人体通信回路部４４ａ及び人体通信用電極４４ｂは、上記人体通信回路部２４ａ及び人体通信用電極２４ｂと同様構成とされており、人体を通信経路とした人体通信を行う。
【００６２】
個人認証部４８は、個人認証情報を取得可能に構成されている。ここでは、個人認証部４８は、本装置４０のケース４０ａに露出するように設けられたタッチ部４０ｂに利用者の指先が接触すると、当該指先の指紋を個人認証情報として取得し、権限書込制御部４６に与える（図７参照）。
【００６３】
なお、上記人体通信用電極４４ｂは、タッチ部４０ｂに設置されており、指先をタッチ部４０ｂに接触させると、その指紋データが個人認証情報として取得されると共に、人体通信回路部４４ａ及び人体通信用電極４４ｂから人体を通じた通信が成立するようになっ

ている。
【００６４】
このように個人認証部４８として、生体が接触することで認容を行う生体認証装置である場合には、個人認証部４８のうち指等の生体の一部が接触する部分に人体通信用電極４４ｂを設置しておき、個人認証と同時に人体通信が成立し得るようにしておくとよい。これにより、生体接触による個人認証の際に端末装置２０に対する書込みを行うことができ、便利である。
【００６５】
なお、個人認証部４８としては、上記の例に限らず、静脈、網膜、声紋等各人に固有の認証情報を取得する構成であってもよい。これらのように、個人認証部４８として、生体に固有の情報を取得する生体認証装置を用いれば、利用者は手ぶらで個人認証を行えるので便利である。
【００６６】
また、個人認証部は、上記のように、生体に固有の認証情報を取得するだけでなく、各人に認証用端末装置として付与されたＩＤカードを読取るカードリーダによって、ＩＤカードに記憶された識別ＩＤを個人認証情報として読取る構成や、入力された暗証番号によって個人認証情報を取得する構成であってもよい。カードリーダを用いた変形例については後述する。
【００６７】
図５は権限書込装置の動作を示すフローチャートである。
【００６８】
処理開始後、権限書込装置４０は、ステップＳ１１において、個人認証情報の取得の有無を判断する。ここで、個人認証情報の取得が否定されると、ステップＳ１１に戻る。一方、個人認証部４８で個人認証情報が取得されるとステップＳ１２に進む。
【００６９】
ステップＳ１２では、人体通信の成立の有無が判定される。ここで、人体通信の成立が否定されると、ステップＳ１１に戻る。一方、人体通信が成立したと判断されると、ステップＳ１３に進む。
【００７０】
ステップＳ１３では、取得された個人認証情報と記憶部４２に記憶された利用権限書込情報とに基づいて、利用権限情報としての個人識別ＩＤを決定する。すなわち、取得された個人認証情報としての指紋データと記憶部４２に予め記憶された各指紋データとのパターンマッチング等を行って、個人識別ＩＤを特定し、その後、ステップＳ１４に進む。
【００７１】
ステップＳ１４では、ステップＳ１３で決定された個人識別ＩＤを、書込時間と共に書込む指令を含む信号を、人体通信回路部４４ａ及び人体通信用電極４４ｂを介して外部に向けて送信する。なお、書込時間は、計時回路４６ａからの計時信号に基づいて決定される。
【００７２】
これにより、端末装置２０において、個人識別ＩＤと書込時間とが書込まれ、権限書込装置４０の処理を終了する。
【００７３】
このような権限書込装置４０は、利用者が本システムを利用するにあたって通過する場所、ここでは、本システムが設置される建物Ｂの入口に設置してある。この権限書込装置４０は、本システム全体において、１つだけ設置されてもよいし、複数設置されてもよい。
【００７４】
＜４．認証ロック装置＞
図８は認証ロック装置を組込んだキャビネットの一例を示す図であり、図９はキャビネットの利用状態を示す図である。

【００７５】
このキャビネット１０は、上半部に扉式収納部１０ａを有すると共に、下半部に複数段（ここでは３段）の引出式収納部１０ｂとを有している。
【００７６】
扉式収納部１０ａは、開閉自在な両開き式の扉１２を有しており、扉１２を開くことによって内部に収納された物品を利用できるようになり、扉１２を閉状態に維持することで内部に収容された物品を利用できない状態が維持される。
【００７７】
扉１２の合せ目部分は、重なり合って配設されており、一方の扉１２を閉じた状態では、他方の扉１２を開くことができない構成となっている。また、一方の扉１２には、操作部としての取っ手部１２ａと、ラッチ機構部１２ｂとが取付けられている。ラッチ機構部１２ｂは、扉１２に組込まれ、扉１２を閉状態に保つようにロックする機構である。このような機構としては、爪部をキャビネット本体１１側に係脱自在に係合させるような周知の機構を含む各種構成を採用できる。取っ手部１２ａは、扉１２の外面側に姿勢変更自在に取付けられている。この取っ手部１２ａの姿勢変更に連動して、上記ラッチ機構部１２ｂがロック及びロック解除動作を行うようになっている。このラッチ機構部１２ｂに、後述するロック部６８が組込まれることで、ラッチ機構部１２ｂがロック状態に維持され、又は、アンロック状態になる。
【００７８】
引出式収納部１０ｂは、開閉自在、換言すれば、引出し及び押込自在な複数段の引出部１３を有しており、各引出部１３を引出すことで内部に収容された物品を利用でき、各引出部１３を押込んだ状態に維持することで内部に収容された物品を利用できない状態が維持される。
【００７９】
引出部１３は、上方に開口する筐状に形成されており、その前面に操作部としての取っ手部１３ａと、ラッチ機構部１３ｂとが取付けられている。
【００８０】
ラッチ機構部１３ｂは、引出部１３の前面側の部分に組込まれ、引出部１３を閉じた状態に保つようにロックする機構である。このような機構としては、上記ラッチ機構部１２ｂと同様に周知の機構を含む各種構成を採用できる。取っ手部１３ａは、引出部１３の前面に姿勢変更自在に取付けられており、この取っ手部１３ａの姿勢変更に連動して、上記ラッチ機構部１３ｂがロック及びロック解除動作を行うようになっている。このラッチ機構部１３ｂに、後述するロック部６８が組込まれることで、ラッチ機構部１３ｂがロック状態に維持され、又はアンロック状態になる。
【００８１】
なお、格納手段は、上記構成に限られない。格納手段の全体が扉にて開閉される構成であってもよいし、また、複数の引出部のみを有する構成であってもよい。また、格納手段は、上記のようなキャビネット１０に限らず、ロッカーや机や脇机の引出部等であってもよい。
【００８２】
本認証ロック装置６０は、上記のようなキャビネット１０における扉１２，引出部１３の外面側に取付けられる。
【００８３】
認証ロック装置６０は、図３に示すように、認証ロック側の記憶部６２と、認証ロック側の人体通信部としての人体通信回路部６４ａ及び人体通信用電極６４ｂと、ロック制御部６６と、ロック部６８とを有している。
【００８４】
ロック制御部６６は、ＣＰＵ、ＲＯＭおよびＲＡＭ等を備える一般的なマイクロコンピュータにより構成され、予め格納されたソフトウェアプログラムによって演算動作を行い後述する処理を実行する。なお、このロック制御部６６は、計時回路６６ａを内蔵してい

る。
【００８５】
記憶部６２は、フラッシュメモリ等の書換え可能な不揮発性メモリによって構成されており、識別符号としての個人識別ＩＤとロック対象物との利用諾否とを対応づけた利用諾否情報を記憶している。利用諾否情報は、例えば、個人識別ＩＤである”０００１”に対して、利用諾否として”利用許可”又は”利用不許可”を対応づけた情報等を含んでおり、本システムの管理者によって予め設定登録されている。
【００８６】
人体通信回路部６４ａ及び人体通信用電極６４ｂの基本的構成は、上記人体通信回路部２４ａ及び人体通信用電極２４ｂと同様である。ここでは、取っ手部１２ａ，１３ａは、金属等の導電性材料によって形成されており、人体通信用電極２４ｂとして用いられている（図９参照）。従って、利用者が本取っ手部１２ａ，１３ａに触れることで、当該利用者が所持する端末装置２０と本認証ロック装置６０との間で人体通信が成立するようになっている。もっとも、人体通信用電極２４ｂは、人体通信専用の電力として扉１２や引出部１３の外部に露出する構成であってもよい。
【００８７】
ロック部６８は、上記ロック制御部６６の制御下、ロック対象物をロック状態又はアンロック状態に切替え可能に構成されている。ここでは、ロック部６８は、上記ラッチ機構部１２ｂ，１３ｂの動作を規制することで、ロック対象物である扉１２又は引出部１３をロック状態又はアンロック状態に維持する。このようなロック部６８としては、例えば、ラッチ機構部１２ｂ，１３ｂのロック及びロック解除動作を規制又は許容するように動作する電磁プランジャー等のアクチュエータと、当該アクチュエータを駆動する駆動回路との組合わせ等、種々の電子式の錠装置に適用されている周知技術を含む種々の構成によって実現可能であるので、ここではその説明を省略する。
【００８８】
図６は認証ロック装置の動作を示すフローチャートである。
【００８９】
まず、初期状態では、ロック部６８は、扉１２や引出部１３を閉状態に維持するロック状態となっている。
【００９０】
この初期状態からの処理開始後、まず、ステップＳ２１において、人体通信の成立の有無が判定される。ここで、人体通信の成立が否定されると、ステップＳ２１の処理を繰返す。一方、端末装置２０を所持した利用者が取っ手部１２ａ，１３ａに触れることにより、人体通信が成立したと判断されると、ステップＳ２２に進む。
【００９１】
ステップＳ２２では、個人識別ＩＤ及び書込時間を要求する信号を、人体通信回路部６４ａ及び人体通信用電極６４ｂを介して外部に向けて送信する。これにより、端末装置２０から個人識別ＩＤ及び書込時間が送信され、人体通信を介して、個人識別ＩＤ及び書込時間が受信される。
【００９２】
次ステップＳ２３では、人体通信を通じて受信された個人識別ＩＤと記憶部６２に記憶された利用諾否情報とに基づいて利用権限の有無を判断する。例えば、受信された個人識別ＩＤに”利用許可”が対応づけられている場合には、利用権限有りと判断し、”利用不許可”が対応づけられている場合には、利用権限無しと判断する。ここで、利用権限無しと判断された場合には、ステップＳ２１に戻る。一方、利用権限有りと判断された場合には、次ステップＳ２４に進む。
【００９３】
ステップＳ２４では、人体通信を通じて受信された書込時間と内蔵された計時回路６６ａからの計時信号に基づいて利用可能条件を満たすか否かが判断される。利用可能条件としては、例えば、書込時間から予め設定された所定時間（例えば、１２時間）以内である

か否かといった条件であり、その所定時間は予め本システムの管理者等によって設定された時間である。

【００９４】

そして、ステップＳ２４で利用可能条件を満たさないと判断されると、ステップＳ２１に戻る。この際、ロック部６８のロック状態が維持されるので、扉１２や引出部１３を開いて利用できない。一方、ステップＳ２４で利用可能条件を満たすと判断されると、ステップＳ２５に進む。このように、ステップＳ２３及びステップＳ２５で利用の可否が判断される。

【００９５】

ステップＳ２５では、ロック部６８にアンロック動作を行わせる。これにより、ラッチ機構部１２ｂ，１３ｂがアンロック状態になり、扉１２や引出部１３を開いて利用できるようになる。これにより、処理を終了する。

【００９６】

なお、利用可能条件情報は上記の例に限られない。例えば、端末装置２０に利用可能条件情報として書込日付を記憶させておいてもよい。この場合、認証ロック装置６０において書込日と同日であると判断した場合に利用可能条件を満たすと判断するとよい。

【００９７】

また、利用可能条件情報として、権限書込装置４０に予め利用可能回数情報（例えば、１回のみ使用可能といった内容）を設定しておいて、権限書込装置４０から端末装置２０にその利用可能回数情報を書込むようにしてもよい。この場合、認証ロック装置６０において、当該利用可能回数情報で規定される上限回数内での使用であると判断された場合に利用可能条件を満たすと判断するとよい。また、この場合、端末装置２０を利用する度に、端末装置２０において利用回数をカウントしてもよいし、または、個別の認証ロック装置６０毎に利用回数をカウントしてもよいし、または、全ての認証ロック装置６０で相互通信することで利用対象物全体の利用回数をカウントしてもよい。そして、このカウントされた利用回数と利用可能回数とに基づいて、所定の上限回数内での使用であるか否かを判断するとよい。

【００９８】

また、利用可能条件情報として、書込時間及び書込日付のうちの少なくとも一方を含む書込時間情報と、利用可能回数情報とを採用し、上記両条件を満たす場合に利用可能条件を満たすと判断してもよい。

【００９９】

なお、ここでは、認証ロック装置６０がキャビネット１０に組込まれた場合を例にして説明したが、部屋Ｒの出入口扉１６についても同様構成にて適用できる。

【０１００】

また、利用対象物がパーソナルコンピュータ１８である場合には、上記ロック部６８として、パーソナルコンピュータ１８のＵＳＢポート等の入出力端子に接続され、利用権限が有りかつ利用可能条件を満たす場合に、当該パーソナルコンピュータ１８を利用可能にする利用許可信号を出力して、アンロック状態、つまり、パーソナルコンピュータ１８を利用可能にする構成とすればよい。この場合、人体通信用電極６４ｂは、人体通信専用の電極として外部に露出する構成であってもよい。もっとも、机や椅子、マウスやキーボード等、パーソナルコンピュータ１８を利用するにあたって人体が直接的又は間接的に触れる接触部に人体通信用電極６４ｂを設置することが好ましい。

【０１０１】

＜５．全体動作＞

このように構成された認証システムの全体動作を、利用者の動作を踏まえつつ説明する。

【０１０２】

まず、利用者は、端末装置２０を所持して本システムが設置された建物Ｂ内に入る。建物Ｂの入口には、権限書込装置４０が設置されているので、利用者は指を権限書込装置４

０のタッチ部４０ｂに接触させる。すると、権限書込装置４０は、指紋認証を行い、利用者を特定し、人体通信を介して当該利用者が所持する端末装置２０に個人識別ＩＤ及び書込時間を書込む。

【０１０３】

なお、権限書込装置４０は、必ずしも建物Ｂの入口に設置する必要はない。権限書込装置４０は、例えば、建物Ｂ内でセキュリティエリアと開放エリアとが設定されている場合に、セキュリティエリアの入口にあってもよく、また、所定の部屋の入口にあってもよい。もっとも、権限書込装置４０をロック対象物としてのキャビネット１０やパーソナルコンピュータ１８、出入口扉１６等が設置されるエリアの入口に設置しておくことで、利用者が当該入口を利用する際に、端末装置２０に利用権限情報を書込むことができて便利である。

【０１０４】

次に、利用者は、通路を通って本システムが設置された所定の部屋Ｒ内に入る。この部屋Ｒの出入口扉１６には、認証ロック装置６０が設置されている。利用者、当該出入口扉１６の取っ手部を掴んで、出入口扉１６を開こうとする。この際、認証ロック装置６０と、当該利用者が所持する端末装置２０との間で人体通信が行われ、端末装置２０から認証ロック装置６０に向けて個人識別ＩＤ及び書込時間が送信される。これにより、認証ロック装置６０は、利用権限の有無を判断すると共に利用可能条件を満たすか否かを判断する。ここで、利用権限が有りかつ利用可能条件を満たす場合には、認証ロック装置６０は出入口扉１６をロック状態からアンロック状態に切替える。これにより、利用者は、出入口扉１６を開いて部屋Ｒ内に入ることができる。一方、個人識別ＩＤに対して”利用不許可”と登録されている場合には利用権限無しと判断され入室できない。また、個人識別ＩＤに対して”利用許可”と登録されている場合（利用権限有り）であっても、書込時間から所定時間以上経過している場合には、利用可能条件を満たさないので、出入口扉１６のロック状態が維持され、入室できない。

【０１０５】

なお、利用者が部屋Ｒに入り、出入口扉１６を閉じると再度ロック状態に切替えられる。

【０１０６】

また、利用者が部屋Ｒ内に入り、各キャビネット１０やパーソナルコンピュータ１８を利用するにあたっては、各キャビネット１０やパーソナルコンピュータ１８に設けられた各認証ロック装置６０と利用者が所持する端末装置２０との間で、上記と同様に、利用権限の有無及び利用可能条件を満たすか否かの判断がされる。そして、利用権限が有りかつ利用可能条件を満たす場合にだけ、各キャビネット１０やパーソナルコンピュータ１８を利用できる。そして、利用を終了すると、各キャビネット１０やパーソナルコンピュータ１８は利用不能なロック状態に切替る。

【０１０７】

このように構成された認証システムによると、実際に利用しようとする利用者が所持する端末装置２０と認証ロック装置６０との間で人体通信が行われて、利用の可否が判断される。このため、無線通信方式による認証のように、近傍にある誤った端末装置との間で認証が行われることを防止でき、誤った認証を有効に防止できる。

【０１０８】

また、権限書込装置４０で個人認証情報を取得し、この個人認証情報と利用権限書込情報とに基づいて決定される利用権限情報（個人識別ＩＤ）と、利用可能条件情報（書込時間）とを端末装置２０に書込むようにしている。そして、認証ロック装置６０では、端末装置２０から人体通信を通じて受信される利用権限情報（個人識別ＩＤ）と、利用可能条件情報（書込時間）とに基づいて利用の可否を判断し、利用可と判断された場合にロック部６８をアンロック状態にしている。このため、利用可能条件を満たす場合、即ち、書込時間から所定時間経過前である場合に限ってロック部６８をアンロック状態にできる。このため、正規の利用者が端末装置２０を紛失しそれに気が付かない場合に、不正な他人が

当該端末装置２０利用しようとしても、書込時間から所定時間経過すると、当該端末装置２０を利用して、扉１２や引出部１３、出入口扉１６を開いて利用したり、パーソナルコンピュータ１８を利用することはできない。従って、端末装置２０の悪用を有効に防止できる。

【０１０９】

特に、ロック制御部６６は、利用可能条件情報としての書込時間に基づき当該書込時間から所定時間経過したときに、利用可能条件を満たさず利用不可と判断するため、端末装置２０紛失後、所定時間経過後に確実に当該端末装置２０の悪用を防止できる。

【０１１０】

なお、利用可能条件情報としては、書込時間では無く、上記したように書込日付とし、書込みと同日における端末装置２０の使用に限って利用可能条件を満たすと判断してもよい。これにより、書込みと同日における端末装置２０の使用に限って、利用できるようにすることができ、翌日における悪用を有効に防止できる。

【０１１１】

また、利用可能条件情報として、上記したように利用可能回数情報を用い、所定の上限回数内での使用である場合に利用可能条件を満たすと判断してもよい。これにより、所定の上限回数を超すと、端末装置２０の悪用を防止できる。

【０１１２】

また、端末装置２０に利用権限情報として個人識別ＩＤを書込み、認証ロック装置６０は、当該個人識別ＩＤとロック対象物との利用諾否を対応づけた利用諾否情報を記憶しており、人体通信を介して受信された個人識別ＩＤと利用諾否情報とに基づいて利用の可否を判断するため、認証ロック装置６０側の利用諾否を変更することで、各端末装置２０の利用の可否を判断できる。例えば、端末装置２０に個人識別ＩＤ等を書込んだ後、利用者が当該端末装置２０を紛失したことを早期に気付けば、認証ロック装置６０側の利用諾否情報において、当該個人識別ＩＤへの対応付けを”利用不許可”に設定することで、その後、即座に、端末装置２０を利用できなくすることができる。

【０１１３】

もっとも、利用権限情報として単に”利用許可”又は”利用不許可”の情報を端末装置２０に書込むようにしてもよい。この場合、認証ロック装置６０は、端末装置２０から人体通信を通じて当該”利用許可”又は”利用不許可”の情報を受信して、利用権限の有無を判断すればよい。

【０１１４】

また、権限書込装置４０で個人認証情報を取得しているため、そのための個人認証動作を１回行うだけでよいことになる。

【０１１５】

このため、個人認証部４８として生体認証装置等を用いている場合は、比較的高価な生体認証装置を各利用対象物に設置せずに、権限書込装置４０だけに設置するだけで比較的少数の設置で済むため、システムの全体コストを低減できる。

【０１１６】

また、個人認証部４８として、カードリーダを用いている場合を想定すると、利用者に、ＩＤカードを用いた比較的面倒な認証動作を行わせる動作を、権限書込装置４０で行わせるだけで済むため、利用者に対する負担を小さくできる。

【０１１７】

特に、認証ロック装置６０の人体通信用電極６４ｂが、前記ロック対象物を利用するにあたって人体が直接的に又は間接的に接触する接触部、中でも、ロック対象物としてのキャビネット１０を利用するにあたって操作される操作部である取っ手部１２ａ，１３ａに人体通信用電極２４ｂが設けられているため、利用者がロック対象物を利用するにあたって取っ手部１２ａ，１３ａを操作すると、認証が行われるため、個人認証部４８以外で特別な認証操作を不要にできる。

【０１１８】

＜６．変形例＞

図１０は権限書込装置に係る変形例を示す図である。この権限書込装置１６０は、個人認証部として、利用者に付与された個人認証端末１７０との間で近接通信を行う個人認証通信部１６８ａを有している。このような個人認証端末１７０は、例えば、ＩＤカード（例えばfelica）であり、また、個人認証通信部１６８ａは、例えば、それを読込むカードリーダ（例えばパソリ）等である。また、個人認証通信部１６８ａは、前記個人認証端末１７０を個人認証通信部１６８ａに近接させようとする手と接触可能な位置に配設され人体通信用電極１６４ｂを有している。ここでは、個人認証通信部１６８ａの表面に、網目状の人体通信用電極１６４ｂを配設している。

【０１１９】

この変形例では、利用者が個人認証端末１７０を個人認証通信部１６８ａに近接させようとすると、手と人体通信用電極１６４ｂとが接触し、人体通信が成立する。従って、個人認証端末１７０により個人認証を行う際に、人体通信による端末装置２０への利用権限等の書込みを行うことができる。

【０１２０】

図１１は取っ手部の変形例を示す図である。この変形例では、扉１１２は、回転可能なレバー式の取っ手部１１２ａを有している。この取っ手部１１２ａは、金属等の導電性材料で形成されており、人体通信用電極６４ｂとして用いられている。このように、利用対象物の利用に先立って操作される操作部としては種々の形態が考えられる。

【０１２１】

また、上記建物Ｂの入口に設置される権限書込装置４０にロック部を組込んでおき、個人認証が許可された場合にのみ当該建物Ｂの入口のゲートをアンロック状態にして入館可能にしてもよい。この場合に、権限書込装置４０にも上記認証ロック装置６０を組込んでおき、利用者が再度建物Ｂ内に入る際には、当該認証ロック装置６０による利用可否判断及びロック状態の解除を行うようにしてもよい。

【図面の簡単な説明】

【０１２２】

【図１】実施形態に係る認証システムの全体構成を示す説明図である。
【図２】端末装置と権限書込装置とを示すブロック図である。
【図３】端末装置と認証ロック装置とを示すブロック図である。
【図４】端末装置の動作を示すフローチャートである。
【図５】権限書込装置の動作を示すフローチャートである。
【図６】認証ロック装置の動作を示すフローチャートである。
【図７】権限書込装置を示す斜視図である。
【図８】認証ロック装置を組込んだキャビネットの一例を示す図である。
【図９】キャビネットの利用状態を示す図である。
【図１０】権限書込装置に係る変形例を示す図である。
【図１１】取っ手部の変形例を示す図である。

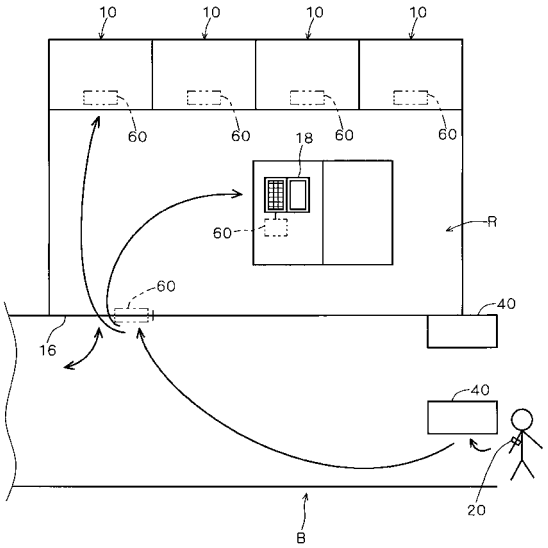
【符号の説明】

【０１２３】

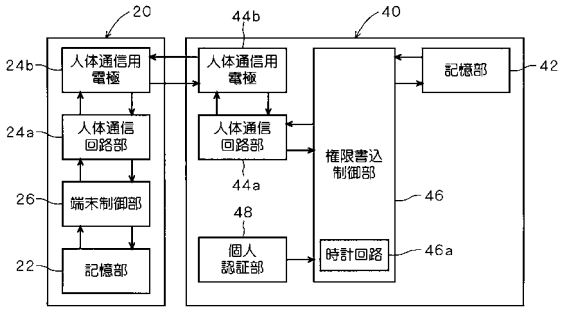
１０　キャビネット
１２，１１２　扉
１２ａ，１３ａ，１１２ａ　取っ手部
１３　引出部
１６　出入口扉
１８　パーソナルコンピュータ
２０　端末装置
２２　記憶部
２４ａ　人体通信回路部
２４ｂ　人体通信用電極

２６　端末側制御部
４０　権限書込装置
４０ｂ　タッチ部
４２　記憶部
４４ａ　人体通信回路部
４４ｂ　人体通信用電極
４６　権限書込制御部
４６ａ　計時回路
４８　個人認証部
６０，１６０　認証ロック装置
６２　記憶部
６４ａ　人体通信回路部
６４ｂ，１６４ｂ　人体通信用電極
６６　ロック制御部
６６ａ　計時回路
６８　ロック部
１６８ａ　個人認証通信部
１７０　個人認証端末

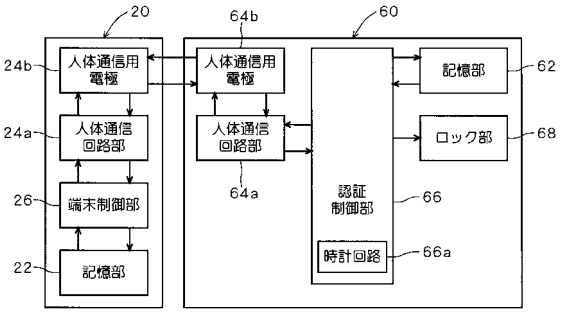
【図１】



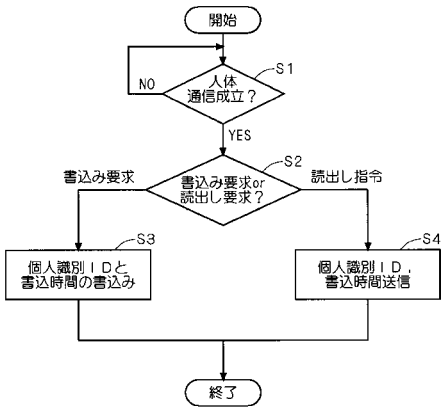
【図２】



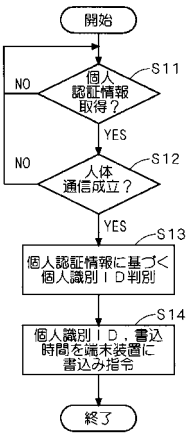
【図３】



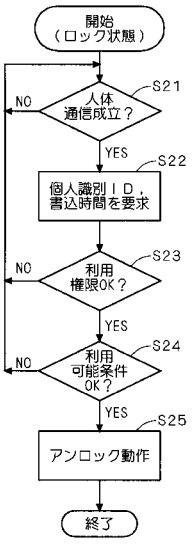
【図４】


開始
S1
NO
人体
通信成立？
YES
S2
書込み要求
書込み要求or
読出し要求？
読出し指令
S3
個人識別ＩＤと
書込時間の書込み
S4
個人識別ＩＤ，
書込時間送信
終了

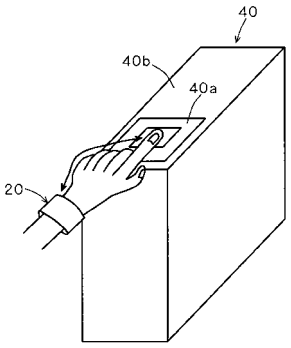
【図５】


開始
S11
NO
個人
認証情報
取得？
YES
S12
NO
人体
通信成立？
YES
S13
個人認証情報に基づく
個人識別ＩＤ判別
S14
個人識別ＩＤ，書込
時間を端末装置に
書込み指令
終了

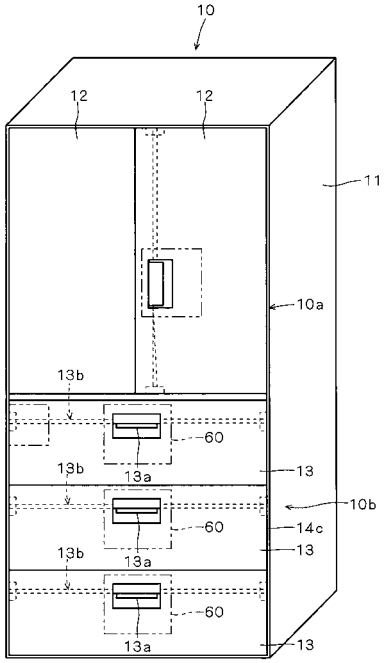
【図６】


開始
（ロック状態）
S21
NO
人体
通信成立？
YES
S22
個人識別ＩＤ，
書込時間を要求
S23
NO
利用
権限OK？
YES
S24
NO
利用
可能条件
OK？
YES
S25
アンロック動作
終了

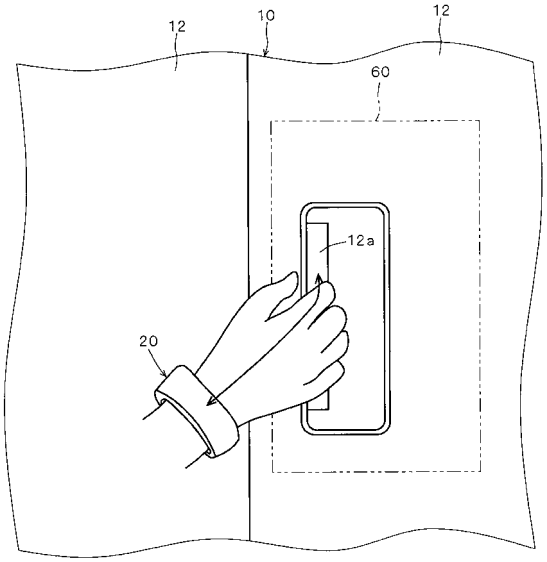
【図７】


40
40b
40a
20

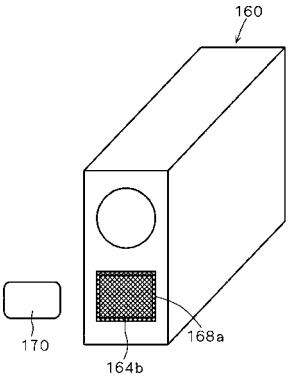
【図８】


10
12
12
11
10a
13b
60
13a
13
13b
60
13a
10b
14c
13
13b
60
13a
13

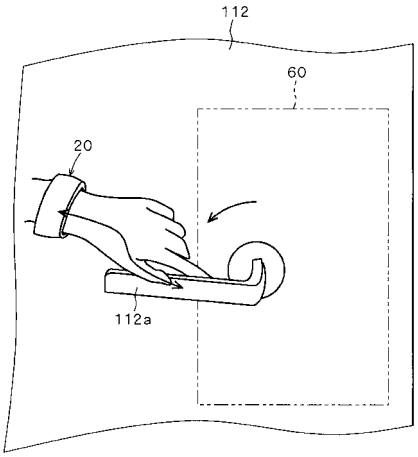
【図９】


12
10
12
60
12a
20

【図１０】


160
170
168a
164b

【図１１】


112
60
20
112a

フロントページの続き

(51)Int.Cl. F I
G06K 19/10 (2006.01) G06K 19/00 S

(56)参考文献 特開２００６－２８３３８３（ＪＰ，Ａ）
特開２００６－１１２０８３（ＪＰ，Ａ）
特開２００１－２４１２３７（ＪＰ，Ａ）
特開２００５－１３９８２４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｅ０５Ｂ ４９／００
Ｇ０６Ｆ ２１／２０
Ｇ０６Ｋ １７／００
Ｇ０６Ｋ １９／１０
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／３２