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

特許第5130420号
(P5130420)

(45)発行日　平成25年1月30日(2013.1.30)　(24)登録日　平成24年11月16日(2012.11.16)

(51)Int.Cl.　F I
A61B 5/117 (2006.01)　A61B 5/10 320Z
A61B 5/00 (2006.01)　A61B 5/10 320C
A61B 5/00 G

請求項の数 1　(全 46 頁)

(21)出願番号　特願2006-26401 (P2006-26401)
(22)出願日　平成18年2月2日 (2006.2.2)
(65)公開番号　特開2007-202869 (P2007-202869A)
(43)公開日　平成19年8月16日 (2007.8.16)
審査請求日　平成21年1月30日 (2009.1.30)

(73)特許権者　706000296
田中　雅英
大阪府豊中市小曽根１－１７－９
(73)特許権者　508278745
ＮＬ技研株式会社
大阪府豊中市小曽根１丁目１７番９号
(72)発明者　田中　雅英
大阪府豊中市小曽根１丁目１７番９号
(72)発明者　松井　徹
奈良県奈良市登美ヶ丘６丁目１０番１３号

審査官　冨永　昌彦

最終頁に続く

(54)【発明の名称】個人認証兼健康管理システム

(57)【特許請求の範囲】
【請求項１】
複数の人間によって共通に使用される場所に設置され人体の生体情報を取得する生体情報取得部と、前記生体情報取得部によって取得された生体情報を生体認証情報として処理する生体認証部と、前記生体情報取得部によって取得された生体情報を健康管理情報として処理する健康管理情報処理部と、前記生体情報取得部からの生体情報が生体認証に充分か否かおよび健康管理情報として充分か否かをそれぞれ互いに異なる判定レベルにて判定する判定部とを有し、生体認証情報と健康管理情報のうちの一方として不充分と判定されても他方として充分であると判定されたときは他方の生体情報として処理することを特徴とする生体情報利用システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、個人認証システムに関し、特に個人認証の際に併せて健康管理情報を取得するを行う個人認証兼健康管理システムに関するものである。
【背景技術】
【０００２】
この分野においては、個人認証の際のなりすましの防止、および認証の簡便性のために種々の生体認証システムが提案されている。また、認証のために取得される生体情報を健康管理に利用することも提案されている。

【０００３】
しかしながら、個人認証と健康管理の関連付けやその活用については検討が充分とはいえない。
【特許文献１】特開２００４－３４４３７５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
本発明が解決しようとする課題は、個人認証と健康管理との関係により配慮した個人認証兼健康管理システムを提供することにある。
【課題を解決するための手段】
【０００５】
上記の課題を解決するため、本発明は、複数の人間によって共通に使用される場所に設置され人体の生体情報を取得する生体情報取得部と、前記生体情報取得部によって取得された生体情報を生体認証情報として処理する生体認証部と、前記生体情報取得部によって取得された生体情報を健康管理情報として処理する健康管理情報処理部と、前記生体情報取得部からの生体情報が生体認証に充分か否かおよび健康管理情報として充分か否かをそれぞれ互いに異なる判定レベルにて判定する判定部とを有し、生体認証情報と健康管理情報のうちの一方として不充分と判定されても他方として充分であると判定されたときは他方の生体情報として処理することを特徴とする生体情報利用システムを提供する。
【発明を実施するための最良の形態】
【０００９】
本発明は、多数の家族が入居するマンションや多数の組織が雑居するビルなど、複数の人間が出入りする共通の入口のロック制御システムを第一部分として実施するのに好適である。また、銀行の個人認証システムを第一部分として実施するのにも適している。
一方、第二部分としては、共通の入口を出入りする特定の人間によってプライベートに管理される各居室などとして実施するのが好適である。また、第二部分は、個人が管理する携帯電話として実施するのにも適している。
【実施例１】
【００１０】
図１は、本発明の生体認証兼健康管理システムの実施例１のブロック図であり、複数の家族が入居しているマンションにおける実施を例示している。
マンション１には複数の家庭が入居しているが、図１では、Ａ家族が入居しているＡ居室２、Ｂ家族が入居しているＢ居室３、およびＣ家族が入居しているＣ居室４のみ図示し、他の居室は省略している。Ａ居室２内のシステムはＡパソコン５が制御しているが、居室内の構成については後述する。なお、Ｂ居室３およびＣ居室４はそれぞれＡ居室２と同様の構成をもつが、それぞれの居室内のシステムを制御しているＢパソコン６およびＣパソコン７を除いて図示を省略し、その説明も重複を避けるために省略する。
また、実施例１のシステムにおいて、各居室２、３、４はマンション入口ロック制御システム８および医療機関９とも連携しており、その詳細については後述する。
なお、以後の説明において、居室内の制御手段はAパソコン５のようなパソコンとするが、本発明の実施に当たっては、汎用のパソコンに代えてシステム専用に居室に備えられたコンピュータを用いてもよく、その他同等の機能を有するものであれば、種々の制御手段を用いることが可能である。
【００１１】
Ａ居室２において、玄関ドア１０にはドアロック１１が設けられているが、玄関ドア１０を閉じる度にオートロックされ、外部からの開錠の可否の制御はＡパソコン５が行っている。Ａパソコン５の制御部１２は、玄関ドア１０の開錠を望む人の生体認証を行う家庭用開錠認証センサ１３からの情報を受け、これを認証照合データ保持部１４にあらかじめ登録しておいた認証照合データと照合する。そして、照合の結果、Ａ居室にへの入室資格がある人であることが認証されるとドアロック１１に開錠信号を送る。

家庭用開錠認証センサ１３は、所定位置に挿入された人の指の血管の情報を光学的に検出する血管センサを持っている。この血管センサから得られる血液の情報を受けた制御部１２はそこから血管パターンを抽出し、これが認証照合データ保持部１４に登録された家族内の誰かの血管パターンと同一であるかどうか判定する。そして、同一であれば入室資格のある家族の一員であると認証してドアロック１１に開錠信号を送る。

【００１２】

家庭用開錠認証センサ１３によって検出された指の血管の情報には、血管パターンだけでなく、人の指における血液の脈動をしめす脈波の情報も含まれている。制御部１２は、この脈波信号から例えば酸素飽和度などの血液の成分情報や血管の若さの情報を得る。この血液の成分情報や血管の若さなどの情報は個人の健康管理データとなるので、制御部１２はこれらの情報を認証できた個人別に個人健康データベース１５に送って蓄積させる。

【００１３】

制御部１２はさらに血液の成分情報や血管の若さなどの健康管理データを健康照合データ保持部１６に登録されている個人別の健康照合データと照合する。健康照合データ保持部１６には、健康指標となる値そのものだけでなく、その値の経時変化についての照合用経時変化データも登録されている。従って、制御部１２は、家庭用開錠認証センサ１３から送られてくるその時々の健康管理データを健康照合データと照合するとともに、個人健康データベース１５に蓄積されたデータに基づく健康指標の経時変化を健康照合データ保持部１６に登録された照合用経時変化データと比較し、健康指標となる値の経時変化の速さなどの観点からも照合を行う。健康指標の値の照合結果および健康指標の経時変化の照合結果は、テレビ１７に表示される。この表示については、例えば照合の結果、異常と認められるときにはテレビ１７のスイッチを入れたとき自動的に「健康異常」の警告が行われるようにする。

なお、健康照合結果の表示については、家族といえどもプライバシーがあるので、各家族構成員が持っている携帯電話に個別にその情報を送るよう構成してもよい。この場合、自分の携帯電話の表示部を見ることによって、例えば入室の度毎に健康状態を自分だけで確認できる。携帯電話を利用した実施については、後出の実施例２でも詳述する。

【００１４】

以上のように、本発明の家庭用開錠認証センサ１３は、ドアロック開錠のための生体個人認証と健康管理データ取得の二重の機能を持っている。従って、通常は、この両者に成功したとき、Ａパソコン５はドアロック１１に開錠信号を送る。

ただ、本来はドアロック開錠のための個人認証ができれば入室管理という当座の目的は達成できるので、個人認証には成功したが健康管理データ取得の観点からは充分な情報が取得できなかった場合であっても、Ａパソコン５はドアロック１１に開錠信号を送る。しかし利用者はドアロック開錠の際に同時に健康管理データの取得もできていることを期待しているので、この場合は玄関ドア１０において健康管理データ取得失敗の旨とその原因について警告表示を行う。この警告を見た利用者は、健康管理データの取得を重視する場合には、再度家庭用開錠承認センサ１３に指を挿入してチェックを行うことができるし、急いでいるときは、失敗の原因だけを理解してとりあえずＡ居室５に入室し、次回の入室時からは失敗の原因を除去するよう指の挿入の仕方を改めるよう心がける。

【００１５】

家庭用開錠認証センサ１３には、血管情報を光学的に検出する血管センサの代わりに、人の眼を撮影することによって眼底情報を得るセンサを採用してもよい。眼底情報も、網膜パターンが生体認証データとなるとともに眼底画像が健康情報を持っているので、上記において指の血管情報について説明したのと同様、ドア開錠のための生体認証とその人の健康管理を同時に行うことができる。また、声紋センサも生体認証データと健康管理情報の取得が可能なので家庭用開錠認証センサ１３に採用できる。さらに声紋センサの場合、合わせて吐息成分のセンサを設ければ、アルコール濃度のチェックもでき、飲酒と健康状態との因果関係のチェックも行うことができる。

家庭用開錠認証センサ１３としては、以上例示したものに限らず、生体認証とその人の

健康管理のデータを同時に得ることができる種々のセンサが採用可能である。例えば、非接触のタイプには限らず皮膚に接触するタイプのものが可能であり、光や音を利用するものに限らず微弱な電流を生体に流してその反応信号を検出するものも可能である。また、いずれかのセンサを単独で採用するのだけではなく、複数のセンサを組み合わせて生体認証の精度を上げるとともに健康管理データをより豊富に得ることもできる。

【００１６】

さらに、それぞれ生体認証とその人の健康管理のデータを同時に得ることができるセンサ同士を組み合わせる場合だけでなく、このような両機能を持つセンサと単に生体認証または健康管理のいずれか一方のデータのみが得られるセンサとの組み合わせも可能である。例えば、健康管理のみのセンサとして、画像処理により体温を検知するセンサと両機能をもつ他のセンサとを組み合わせてもよい。また、生体認証のみのセンサとなる指紋センサと両機能をもつ他のセンサとを組み合わせてもよい。

なお、家庭用開錠認証センサ１３全体として生体認証および健康管理の機能を持てばいいので、生体認証の機能のみを持つセンサと健康管理データ取得の機能のみを持つセンサとを組み合わせて家庭用開錠認証センサ１３とすることも可能である。さらには、認証動作の際に自然に健康管理データの取得も行われるよう構成する場合には、認証機能に関しては生体認証に限らず、暗証番号やＩＣカードなど、在来の認証手段を採用してもよい。

【００１７】

Ａパソコン５は、さらに、パソコン使用時にアクセス権があるかどうかを認証するためのユーザ認証センサ１８を持っている。ユーザ認証センサ１８も生体認証機能を持っており、すでに説明したのと同様の指血管情報取得機能の他、マウスを持つ掌の血管情報などパソコンの使用特有の事情に合致した生体認証機能を持っている。マウスに生体認証機能を持たせた場合には、パソコンの使用開示時点だけでなく、使用途中においても常に生体認証を繰り返すことができるとともに、継続して健康管理データを取得することができる。このようにしてパソコン使用におけるユーザ認証の際にも、生体認証データと健康管理データの取得とを同時に行うことができる。

ユーザ認証センサ１８からの信号の取り扱い、認証照合データ保持部１４に登録された認証照合データとの照合、健康照合データ保持部１６に登録された健康照合データとの照合、および健康管理データの個人健康データベース１５への蓄積については、家庭用開錠認証センサ１３に関連して説明したのと同様なので、重複を避けるため説明を省略する。但し、ユーザ認証センサ１８の場合、認証照合データ保持部１４の認証照合データとの照合によりユーザとして認証されたときは、制御部１２がＡパソコンの使用を許可する点だけは異なる。

【００１８】

Ａパソコン５は、以上説明した玄関ドア１０のドアロック１１の開錠管理機能とＡパソコン５のユーザ認証機能の他に、マンション１の入口ロック制御システム８に用いられる管理パソコン１９との連携機能も有している。

マンション入口ロック制御システム８には入口ロック２０が設けられているが、マンション入口を閉じる度にオートロックされ、外部からの開錠の制御は管理パソコン１９が行う。管理Ａパソコン１９は、マンション入口の開錠を望む人に対して生体認証を行う業務用開錠認証センサ２１からの情報を受け、これをマンション入口ロック制御システム８に参加しているすべての居室のパソコンに送る。図１ではＡ居室２のＡパソコン５、Ｂ居室３のＢパソコン６、Ｃ居室４のＣパソコン７に業務用開錠認証センサ２１からの情報が送られるが、図示していない居室がマンション入口ロック制御システム８に加入していれば、それらの居室のパソコンにも同様の情報が送られる。なお、業務用開錠認証センサ２１は家庭用開錠認証センサ１３と共通の機能も持つが、それより高度のセンシング機能も備えたハイスペックのものとなっている。

【００１９】

以上の構成において、例えばＡ居室２のＡパソコン５に送られた業務用開錠認証センサ２１からの情報は、制御部１２によって認証照合データ保持部１４にあらかじめ登録して

おいた認証照合データと照合される。そして、照合の結果、マンションへの入館資格がある人であることが認証されると管理パソコン１９にその結果を通知し、管理パソコン１９はこの通知に応じて入口ロック２０に開錠信号を送る。一方、認証照合データと一致しなければ管理パソコン１９に不一致の旨通知する。この場合、管理パソコン１９は少なくともＡ居室２からの指示によっては入口ロック２０に開錠信号を送らない。

同様のことが、Ｂ居室３、Ｃ居室４などマンション入口ロック制御システム８に参加しているすべての居室のパソコンと管理パソコン１９との間で行われる。そして、管理パソコン１９はいずれかの居室のパソコンからマンションへの入館資格がある人である旨の認証結果が通知された場合、入口ロック２０に開錠信号を送る。一方、すべての居室から認証照合データと不一致の旨の通知があった場合は、管理パソコン１９は入口ロック２０に開錠信号を送らない。そして、入館拒否の表示がマンション入口において行われる。

【００２０】

なお、いずれかの居室から管理パソコンへの通知がなかった場合でも、その他の居室すべてから認証照合データと不一致の旨の通知があれば、管理パソコン１９は入口ロック２０に開錠信号を送らない。この場合も、入館拒否の表示がマンション入口において行われる。もしこの表示を見た人自身がマンションへの入館資格を持った住人なら、自分の居室になんらかのシステム障害が起こっていると判断できるので、別途の暗証番号入力またはＩＣカード挿入等の手段によって入口ロック２０を開錠し、当座の入館を行うことができる。また、その後のシステム復旧の手を打つこともできる。

なお、入館拒否の表示においては、すべての居室から認証照合データ不一致の通知があったのか、それともシステム障害があったのかの情報は一切明らかにされない。また、管理パソコン１９自体も認証照合結果の通知がどの居室のものか分からないように配慮されている。

【００２１】

以上のように、マンション入口ロック制御システム８の管理パソコン１９自体には各居室の住人の認証照合データの記録や照合機能はなく、単に照合結果が各居室から通知されるだけである。このような配慮により、血管パターンや眼底パターンなどプライバシーにかかわる生体認証用の認証照合データは各居室内に留められる。また、管理パソコン１９自体に照合機能がなく、かつ照合結果がどの居室から来たものか分からないので、業務用開錠センサ２１によって取得されるデータも誰のものかわからず、プライバシーが保護される。

【００２２】

業務用開錠認証センサ２１は、家庭用開錠認証センサ１３と同様、認証用の情報だけでなく、健康管理情報も取得できる。従って、家庭用開錠センサ１３について説明したのと同様の健康管理が業務用開錠認証センサ２１によっても可能となる。業務用開錠認証センサ２１からの信号の取り扱い、健康照合データ保持部１６に登録された健康照合データとの照合、および健康管理データの個人健康データベース１５への蓄積については、家庭用開錠認証センサ１３の場合と同様なので、これ以上の説明は省略する。

【００２３】

先に述べたように、業務用開錠認証センサ２１は、家庭用開錠認証センサ１３と共通の機能を備えるとともに、それより高度のセンシング機能を備えたハイスペックのものである。認証照合データ保持部１４および健康照合データ保持部１６に保持される照合データおよびこれらの情報を取り扱う個人健康データベース１５は、このような業務用開錠認証センサ２１の高度のセンシング機能にも対応するものとなっている。

【００２４】

また、業務用開錠認証センサ２１と家庭用開錠認証センサ１３との間で共通の機能については、同一の健康指標についてダブルチェックが行われる。つまり、Ａ居室に向かう住人に対しては、まずマンション入口にて業務用開錠認証センサ２１によって健康指標を取得し、次いでＡ居室２の玄関ドア１０において家庭用開錠認証センサ１３によって同一の健康指標を取得することができる。これによって同一の健康指標の検知精度を向上させる

ことができる。
さらにマンション入口での検出結果と玄関ドアでの検出結果との間で同一の健康指標における因果関係をチェックすることもできる。具体的にはマンション入口にて平静状態の健康管理データを取得した後、階段を上ってＡ居室２の玄関ドアに到達した場合、その運動負荷がかかっている状態で同一の健康管理データを取得することができるので、両者の比較により平静状態と運動負荷状態における因果関係のチェックが可能となる。運動負荷の違いは、検知される脈拍数などによって把握できる。
逆に、坂道を登ってマンションに帰宅した場合は、その運動負荷がかかっている状態でマンション入口にて康管理データが取得され、その後エレベータ内で平静状態に戻ってＡ居室２に到達したときは、玄関ドアにて運動負荷から回復後の同一の健康管理データの取得ができる。
このように、各個人の生活パターンやマンションと居室の居住条件などを利用し、マンション入口で取得される健康管理データと玄関ドアで取得される健康管理データとを組み合わせれば、各人に合わせた豊富な健康管理データの取得が可能となる。
【００２５】
さらに、健康状態は、季節や、気温、湿度、風速などの気象条件にも依存する可能性があるので、家庭用開錠認証センサ１３および業務用開錠認証センサ２１には、健康管理データ取得時の日付時刻データを合わせて記録する機能を持たせるとともに、季節や気象条件のセンサを設ける。これらの機能との組み合わせによって、さらに豊富な健康管理データの取得が可能となる。特に、業務用開錠認証センサ２１は屋外に面しているのでより豊富な情報の取得が可能である。また、気温、湿度などは、マンション入口と各居室の玄関ドア部分では条件が異なるので、これらの条件変化について同一の健康管理データの比較を行うこともできる。
【００２６】
先に述べたように、Ａ居室２とマンション入口ロック制御システム８との連携は、Ｂ居室３やＣ居室４とマンション入口ロック制御システム８との間でも同様に行われる。このため、各居室のシステムは少なくともマンション内において相互に連携可能な規格によって運営されている。従ってマンション入居の際には、システムチェックが行われるとともに、マンション入口ロック制御システムのバージョンアップの際には、各居室のシステムも連動してバージョンアップされる。
なお、引越しの際には、開錠認証はともかくとして、個人健康データベースや健康照合データについては転居先でも引き続き使用することが望まれる。従って、少なくとも健康管理システムについてはマンションなどの住居が変わっても引き続き使用できるような一般性のある規格によって運営される。
【００２７】
次に、Ａ居室２を例にとって医療機関との連携について説明する。Ａパソコン５はインターネットによって医療機関９の大型コンピュータ２２と情報交換している。セキュリティの維持のため、交換される情報は暗号化されているとともに、患者の認証についてもＡパソコン５のユーザ認証センサ１８を活用した生体認証システムによって万全が期されている。
【００２８】
健康照合データ保持部１６の健康照合データは、医療機関９の健康照合データ登録部２３によって登録される。これは、医療機関９を訪れた患者が自動化装置を用い、健康照合ソフト２４の指示に基づいて自身の健康管理データを検査して自動的に登録することが可能である。また、同じ数値であっても個人によって健康度の判断が異なるので、必要に応じ医師２５が実際に診察を行った上で健康照合データの登録を行う。その際、自動登録された健康管理データなのか、医師の判断が入った上で登録された健康照合データなのかを区別する情報を入れておき、後に照合する際に反映する。
このようにして登録された患者の健康照合データは制御部２６の制御によって患者自宅のＡパソコン５に送信され、健康照合データ保持部１６に保存される。また、健康照合デ

ータを取り扱うための健康照合ソフト中、Ａパソコン５に必要な部分もあわせて送信され、制御部１２にインストールされる。

【００２９】

家庭用開錠認証センサ１３、業務用開錠認証センサ２１およびユーザ認証センサ１８から得られた生データ、およびそれらが蓄積された個人健康データベース１５のデータはリアルタイムで医療機関９の大型コンピュータ２２に送信され、総合健康データベース２７に蓄積される。

また、健康照合データ保持部１６との照合結果も補助的に医療機関９の大型コンピュータ２２に送信される。健康照合データとの照合は医療機関の健康照合ソフト２４でも可能であるが、すでにＡパソコン５内で行われた照合の結果通知を受ける方が効率的であるからである。もちろん、Ａパソコン５で取り扱うことのできない高度の健康管理データの照合は大型コンピュータ２２の健康照合ソフト２４で初めて取り扱われる。その結果も総合健康データベース２７に蓄積される。

【００３０】

また、総合健康データベース２７に蓄積された各患者のデータは定期的に医師２５の診断を得るために医師２５の手元にある診断入出力部２８に出力される。医師２５の診断結果は診断入出力部２８に入力され、総合健康データベース２７に蓄積される。

【００３１】

総合健康データベース２７に蓄積された健康照合ソフト２４の照合結果および医師２５による診断結果は定期的にＡパソコン５に送られ、患者は自宅のＡパソコン５の表示部又はテレビ１７により診断結果を見ることができる。

なお、健康照合ソフト２４の照合結果または医師２５による診断結果に基づき、緊急を要する異常が認められたときは、その都度、大型コンピュータ２２からＡパソコン５にその旨の通知が行われる。

【００３２】

以上の医療機関９とＡ居室２との連携は、Ｂ居室３、Ｃ居室４でも共通である。このようなシステムを維持するため、各居室は、マンション入口ロック制御システムだけでなく、医療機関９とも相互に連携可能な規格によって運営されている。

【００３３】

医療機関９の総合健康データベース２７には多数の患者の健康管理データが蓄積されているので、その統計処理に基づき、特定の患者の健康管理データが平均値や分布に照らしてどの位置にいるかの参考情報を提供することができる。また、統計処理の観点から特定の患者の健康管理データが正常範囲にあるのか異常範囲にあるのかの診断をより客観的に行うことも可能となる。医療機関９はこのようなサービス情報の配信もＡパソコン５に対して行う。なお、統計処理に当たっては、各患者のプライバシー情報保護について万全の処置がとられる。

【００３４】

医療機関の健康照合ソフト２４は、家庭用開錠認証センサ１３、業務用開錠認証センサ２１およびユーザ認証センサ１８の健康管理データ取得機能と深く関連している。従って、これらのセンサが変更されたときや新しい機能のセンサが導入されたときは、その都度、医療機関９の健康照合ソフト２４がこれらのセンサに対応できるよう機能のメンテンスを行う必要がある。このため、医療機関９の大型コンピュータ２２と各居室のＡパソコン、Ｂパソコン、Ｃパソコンなど、および医療機関９の大型コンピュータ２２とマンション入口ロック制御システムの管理パソコン１９とは常にソフトウエア更新の連携を保っている。

また、逆に、医療機関９側からの提案により、家庭用開錠認証センサ１３、業務用開錠認証センサ２１およびユーザ認証センサ１８を、より高性能、高機能のものに変更する事も行われる。その場合は、医療機関９から各センサとそのセンサのドライバーソフトが有償で提供される。また、医療機関９とその旨のメンテナンス契約をしておけば、センサとそのドライバーソフトについて改良が行われる度に、それらの無償提供を受けることも可

能である。

【００３５】

各患者は、その意思または引越しなどの事情によって、医療機関を変えることがある。その場合、患者は総合健康データベース２７に保存された自分の健康管理データベースを新しい医療機関でも引き続き使用することを望む。従って、従って、総合健康データベース２７を取り扱うシステムについては医療機関９が変わっても引き続き使用できるような一般性のある規格によって運営される。

【００３６】

図２は、生体認証および健康管理データ取得のために、家庭用開錠認証センサ１３、業務用開錠認証センサ２１およびユーザ認証センサ１８で用いられる血管センサシステムを示すシステムブロック図である。図2では家庭用開錠認証センサ１３にの場合に基づいて説明し、図１と共通のブロックには同一番号を付す。

【００３７】

図２において、血管センサ３１は、家庭用開錠認証センサ１３に設けられているもので、生体認証を求める人の指が挿入される部分にあり、血液と血管に対する吸収特性が異なる複数波長の光源と受光部を持つ。血管センサ３１の出力はＡパソコン５に送られ、制御部１２における画像処理部３２で処理される。以下、制御部１２における機能は実際にはソフトウエアによって実行されるが、図２では、このようなソフトウエアで実行される機能をブロックとして「画像処理部３２」のように表記して説明する。

なお、当然ながら制御部１２における機能の実行をハードウエアで行うことも可能であり、ハードウエアとソフトウエアの組合せにより実行することも可能である。

【００３８】

血管パターン抽出部３３は、画像処理部３２で処理された画像に基づいて血管パターンを抽出する。抽出された血管パターンは、制御部１２の照合/本人判定部３４により認証照合データ保持部１４に保持される登録パターン３５と照合され、両者が同一かどうかで認証を求めた人が本人かどうか判定する。本人であると判定されたときは制御部１２はドアロック１１に開錠信号を送る。

照合/本人判定部３４による個人特定情報は個人健康データベース１５にも送られ、後述する健康管理データが誰のものであるかの管理に用いられる。

【００３９】

一方、制御部１２の脈波検出部３６は、画像処理部３２で処理された画像に基づき、動脈血の脈波を検出する。検出された脈波は、制御部１２の波形分析部３７により分析され、第１健康判定部３８により認証照合データ保持部１４に保持されている参照波形３９と比較される。そして、比較結果に基づく血管若さの情報が照合/本人判定部３４からの個人特定情報とともに個人健康データベース１５に蓄積される。なお、先に述べたように、この判定結果は、テレビ１７にも表示される。

【００４０】

さらに、脈波検出部３６によって検出された脈波は、制御部１２の成分分析部４０により分析されて酸素飽和度などの動脈血の成分が検出される。検出された動脈血の成分は、第２健康判定部４１により認証照合データ保持部１４に保持されている参照成分４２と比較される。そして、比較結果に基づく血液成分情報が照合/本人判定部３４からの個人特定情報とともに個人健康データベース１５に蓄積される。なお、第２健康判定部４１の判定結果についても、テレビ１７に表示される。

【００４１】

個人健康データベース１５に蓄積された第１健康判定部３８の判定結果および第２健康判定部４１の判定結果は、制御部１２により医療機関９に送信される。なお、先に述べたように、第１健康判定部３８の判定結果および第２健康判定部４１の判定結果そのものもリアルタイムで医療機関９に送信される。

【００４２】

なお、照合/本人判定部３４には、脈波検出部３６からの脈波信号も補助的に入力され

る。そして照合/本人判定部３４は、血管パターン抽出部３３で抽出した血管パターンと認証照合データ保持部１４に保持される登録パターン３５とが一致したとしても、脈波検出部３６からの脈波信号の入力がなければ本人との判定を行わず、制御部１２はドアロック１１に開錠信号を送らない。これは、生体反応のない物質で偽造した血管パターンによりドアロックが開錠されてしまうのを防ぐためである。

【００４３】

図３は、開錠認証センサの詳細構成を示すブロックである。図３では業務用開錠認証センサ２１の場合に基づいて説明し、図１と共通のブロックには同一番号を付し、必要がない場合は説明を省略する。

業務用開錠認証センサ２１では、構成部品が交換可能にユニット化されており、センサユニット５１は、故障時の交換が可能なようにユニット化されている。またバージョンアップ時の交換にも対応できるよう、外形および電気接続部が規格化されている。また、認証を求める人の指が挿入される部分は、外部からの汚れからセンサユニット５１を保護するための透明カバーなどの保護ユニット５２として構成されており、これも損傷時やバージョンアップ時のために交換可能なユニットになっている。センサユニット５１および保護ユニット５２は、それぞれ独立に交換可能である。

【００４４】

管理パソコン１９の制御部５３は、センサユニット５１と接続されており、センサユニット５１の機能を制御するとともに検知された信号を受ける。また、センサユニット５１が正常に機能しているかどうかのチェックも行う。。

管理パソコン１９の制御部５３は、さらに保護ユニット５２とも接続されており、保護ユニット５２に汚れや破損がないかチェックする。これによって、戸外に露出させられた環境下における性能劣化に対応するとともにいたずらによる破損等についても迅速に対応する。

なお、保護ユニット５２の汚れや破損のチェックは、上記のように直接保護ユニット５２と制御部５３を接続して行ってもよいが、これに代えてセンサユニット５１からの出力を制御部５３で分析し、その出力低下の様子から間接的に保護ユニットの汚れや破損を推定するようにしてもよい。

管理パソコンの制御部は、さらには、センサユニット５１または保護ユニット５２が交換されたときの初期動作確認も行う。具体的にはセンサユニット５１や保護ユニット５２の性能や動作のバラツキ等を補償するため、所定の初期動作を行わせて確認を行うとともにその結果に応じて出力のキャリブレーション等の調整を行う。

【００４５】

入館拒否表示部５４は、すでに説明したように、すべての居室から認証照合データ不一致の通知があるか、またはシステム障害によりいずれの居室からも認証できた旨の通知がなかったとき、その旨の表示を行う。補助認証部５５は、暗証番号入力部またはＩＣカード挿入部等として構成され、入館資格のあるマンションの住人がシステム障害によりマンションに入館できない場合に対応する。

【００４６】

健康データ取得失敗表示部５６は、個人認証には成功したが健康管理データ取得の観点からは充分な情報が取得できなかった場合にその旨およびその原因について警告表示を行う。すでに説明したように、この表示によって、健康管理データの取得期待している使用者は、その失敗に気づくことができる。

このように、健康データ取得失敗表示部６は、生体情報が健康管理情報として不充分であるときこれを報知する報知部となっている。報知の手段としては、視覚的な表示の他、警告音なども採用することができる。

【００４７】

マンション入口ロック制御システム８は、健康管理情報を含む生体情報を業務用開錠認証センサ２１によって取得するものの、その利用は専らA居室２側で行われる。したがって、健康データ取得失敗表示部６によって表示を行うべきかどうかの判断自体は、A居室

２のAパソコン側で行い、その結果のみをマンション入口ロック制御システム８に通知して、健康データ取得失敗表示部５６にこれを表示させる。

しかしながら、業務用開錠認証センサ２１によって取得される生体情報が健康管理情報として充分かどうかはその出力レベル等により、マンション入口ロック制御システム８側で判断することも可能である。従って、健康データ取得失敗表示部５６の表示を行わせるかどうかの制御を管理パソコン１９独自の判断で行うよう構成してもよい。なお、管理パソコン１９独自の判断とAパソコン５からの指示を併用して健康データ取得失敗表示部５６の表示の制御を行わせるようにしてもよい。

【００４８】

外部条件センサ５７は、さらに、気温、湿度、風速などの気象条件を検出するもので、制御部５３はこの外部条件センサの出力をセンサユニットからの情報と関連付け、健康管理データ取得時の日付時刻データとともにＡパソコン５に送る。

【００４９】

また、人センサ５８は、マンション入口の所定のエリア内に人が立ったときこれを検知して認証センサの動作にトリガーをかけるものである。

【００５０】

図３の業務用開錠認証センサ２１におけるセンサユニット５１および保護ユニット５２の構成は、家庭用開錠認証センサ１３にも採用できる。また、図３の入館拒否表示部５４、補助認証部５５、健康データ取得失敗表示部５６、外部条件センサ５７、人センサ５８と同様の構成は、A居室２などの各居室における玄関ドア１０にも設けられる。

【００５１】

図４は、Ａ居室２のＡパソコンにおける制御部１２の機能を示す基本フローチャートである。この基本フローチャートはAパソコンのＯＳの制御に従って、適宜繰り返し実行される。

基本フローチャートの機能がスタートすると、ステップＳ１で業務用開錠認証センサ２１が変更されていないかどうかチェックする。変更があるとステップＳ２で管理パソコン１９から新たなソフトの提供を受け、業務用開錠認証センサ２１の情報を処理できるようＡパソコン５のソフトを自動書き換えしてステップＳ３に移行する。業務用開錠認証センサ２１に変更がなければ、直接ステップＳ３に移行する。

【００５２】

ステップＳ３では、管理パソコン１９の処理ソフトがバージョンアップされていないかどうかチェックする。バージョンアップがあると、ステップＳ４で管理パソコン１９からバージョンアップに関する新たなソフトの提供を受け、Ａパソコン５のソフトを自動書き換えしてステップＳ５に移行する。バージョンアップがなければ、直接ステップＳ５に移行する。

【００５３】

ステップＳ５では、医療機関９の健康照合データ登録部２３において登録された新たな健康照合データがないかどうかチェックする。新たな健康照合データがあると、ステップＳ６でそのデータを健康照合データ保持部１６に自動入力してステップＳ７に移行する。新たに登録された健康照合データがなければ、直接ステップＳ７に移行する。

【００５４】

ステップＳ７では、医療機関９の健康照合ソフト２４がバージョンアップされていないかどうかチェックする。バージョンアップがあると、ステップＳ８で医療機関９の大型コンピュータ２２からバージョンアップに関する新たなソフトの提供を受け、Ａパソコン５のソフトを自動書き換えしてステップＳ９に移行する。バージョンアップがなければ、直接ステップＳ９に移行する。

なお、ステップＳ７では、具体的には医療機関９の最新の健康照合ソフト２４がＡパソコン５のソフトと比較され、両者が異なっていれば、健康照合ソフトのバージョンアップがあったと判断される。このようにバージョンアップの有無とは、医療機関９側でいつバージョンアップがあったかの問題ではなく、Ａパソコン５側に現在どんなソフトが入って

いるかによって決まる。従って、Ａ居室２が家庭内健康管理システムに新規加入してＡパソコンには健康照合ソフトがまだ何もインストールされていない場合には、バージョンアップがあったと判断され、ステップＳ８では、その時点での医療機関９の最新の健康照合ソフトがＡパソコン５に提供されて自動インストールされる。

【００５５】

ステップＳ９は、家庭用開錠認証センサ１３が変更されていないかどうかチェックする。変更があるとステップＳ１０で家庭用開錠認証センサのドライバソフトをインストールする処理を行い、ステップＳ１１に移行する。家庭用開錠認証センサ１３に変更がなければ、直接ステップＳ１１に移行する。

【００５６】

ステップＳ１１では、Ａパソコン５の認証照合データ保持部１４に開錠認証照合データを新たに登録する処理を行う。この処理は、家族のマンション入居のときや、新たに登録を必要と家族が増えたときや、業務用開錠認証センサ２１または家庭用開錠認証センサ１３が変更されて新たな機能が追加されたときなどに生じる。認証照合データを新たに登録する際、家庭用開錠認証センサ１３のために登録を行う場合と、業務用開錠認証センサ２１のために登録を行う場合では手続きが異なるので、その詳細については後述する。

【００５７】

次いでステップＳ１２においてセンサチェック処理を行う。ステップＳ１２は、ステップＳ１やステップＳ９において開錠認証センサが変更されたときにその初期状態においてセンサが正常に動作することをチェックする他、センサに故障や劣化がないかどうか常にチェックするために必要なものである。その詳細については後述する。

【００５８】

ステップ１２に続くステップＳ１３では、システムスタート処理が行われるがその詳細は後述する。ステップＳ１３の処理が終わるとステップＳ１４に移行し、認証トリガーを待機状態とする。認証トリガー待機状態では、具体的には、玄関ドアの前に人が立ったときこれを自動的に検知してトリガーがかかり認証機能がスタートできるようＡパソコン５を待機させる。認証トリガー待機状態では、さらに、マンション入口に人が立ったときこれを管理パソコン１９が認識してその旨をＡパソコン５に通知した際にもトリガーがかかり認証機能がスタートするようＡパソコン５を待機させる。

認証トリガー待機状態においてトリガーがかかると、Ａパソコン５は、家庭用開錠センサ１３での認証が求められたのか、または管理パソコン１９からの通知があったのかを識別してそれぞれ別に認証フローに入る。その詳細は後述するが、このようなトリガーがかかったときにＡパソコン５が使用中である場合、トリガーがかかった旨の表示がＡパソコン５のディスプレー上において行われる。

【００５９】

図５は、図４のＡ居室２のＡパソコンにおける制御部１２の機能におけるステップＳ１２のシステムスタート処理の詳細を示す

システムスタート処理が始まると、ステップＳ２１で認証照合データ保持部１４になんらかの開錠認証照合データが登録されているかどうかをチェックする。開錠認証照合データが登録されていれば、ステップＳ２２で、その開錠認証照合データに対応した個人別に玄関ドア開錠の待機状態となる。

【００６０】

次にステップＳ２３に進み、Ａ居室２がマンション入口ロック制御システム８に加入済みかどうかチェックする。加入済みであればステップＳ２４で、照合認証データ保持部１４に登録された認証照合データに対応した個人別にマンション入口開錠の待機状態としてステップＳ２５に移行する。ステップＳ２３でＡ居室２がマンション入口ロック制御システム８に加入済みでなければ、直接ステップＳ２５に移行する。この場合、生体認証による開錠はＡ居室２の玄関ドア１０だけとなり、生体認証によるマンション入口開錠の資格はない。

【００６１】

ステップＳ２５では、医療機関９が管理する家庭内健康管理システムにＡ居室２が加入しているかどうかチェックする。加入済みであれば、ステップＳ２６で、照合認証データ保持部１４に登録された認証照合データに対応した個人別に、まず健康管理データの健康管理データを個人別健康データベース１５に蓄積させる機能を待機状態とする。

次いで、ステップＳ２７で、個人別健康管理データ保持部１５に蓄積されたセンサ出力の経時変化をテレビ表示する機能も待機状態とする。ここまでの機能は、健康照合データがなくても可能だからである。

【００６２】

次いでステップＳ２８で、医療機関９の健康照合データ登録部２３にて登録された健康照合データが健康照合データ保持部１６に保持されているかどうかチェックする。健康照合データがあれば、ステップＳ２９に至り、照合認証データ保持部１４に登録された認証照合データに対応した個人別に、センサ出力または個人別健康管理データ保持部１５に蓄積されたセンサ出力と健康照合データとを照合する機能を待機状態とする。

次いで、ステップＳ３０で、照合結果をテレビ表示する機能も待機状態とし、ステップＳ３１に移行する。

【００６３】

なお、ステップＳ２１において認証照合データ保持部１４に開錠認証照合データが全く登録されていない場合は、開錠システムの以降の機能ができないので、直接ステップＳ３１に飛ぶ。

また、ステップＳ２５において家庭内健康管理システムにＡ居室２が加入していなかった場合、以降の健康管理機能の実行ができないので、直接ステップＳ３１に飛ぶ。

さらに、ステップＳ２８で、医療機関９の健康照合データ登録部２３にて登録された健康照合データが健康照合データ保持部１６に保持されていない場合は、以降の照合機能の実行ができないので、直接ステップＳ３１に飛ぶ。

【００６４】

ステップＳ３１からは、パソコンユーザ認証機能に入る。ステップＳ３１では、認証照合データ保持部１４にパソコンユーザ認証のための照合データが登録されているかどうかをチェックする。パソコンユーザ認証照合データが登録されていれば、ステップＳ３２で、そのパソコンユーザ認証照合データに対応した個人別に、パソコンへのアクセス認証を待機状態とし、ステップＳ３３に移行する。一方、ステップＳ３１において認証照合データ保持部１４にパソコンユーザ認証のための照合データが登録されていない場合は、それ以降の機能は不要なので直ちにシステムスタート機能を終了し、図４のステップＳ１４に移行する。

【００６５】

ステップＳ３３では、医療機関９が管理する家庭内健康管理システムにＡパソコン５のユーザ認証機能が加入しているかどうかをチェックする。加入済みであれば、ステップＳ３４で、照合認証データ保持部１４に登録された認証照合データに対応した個人別に、健康管理データの個人別健康データベース１５への蓄積および照合認証データ保持部１４に登録された認証照合データとの照合などの健康管理機能を待機状態とし、システムスタート機能を終了する。一方、ステップＳ３３においてＡパソコン５のユーザ認証機能が家庭内健康管理システムに加入していなければ、直ちにシステムスタート機能を終了する。

【００６６】

図５では、健康管理データの蓄積と照合への待機をまとめてステップＳ３４として記載している。しかし詳細には、ステップＳ３４においても、まずはステップＳ２６のように健康管理データの蓄積機能および経時変化表示機能を待機状態とし、その後、ステップＳ２８のように健康照合データ保持部１６における健康照合データの有無をチェックしたうえで照合機能を待機状態とする。

【００６７】

図６は、玄関ドアの前に人が立って認証トリガーがかかった場合のＡ居室２のＡパソコンにおける制御部１２の機能を示すフローチャートである。

このトリガーがかかった場合、ステップＳ４１において、まず玄関ドアの前に人が立ってから所定時間経過したかどうかのチェックをおこなう。所定時間経過していなければステップＳ４２に進み、家庭用開錠認証センサ１３への指の挿入が行われたがどうかをチェックする。指の挿入がなければステップＳ４１に戻り、以下、所定時間が経過するまで指の挿入を待つ。

【００６８】

ステップＳ４２において指の挿入があるとステップＳ４３に進み、認証照合データ保持部１４に保持されている開錠認証照合データのいずれかと一致するかどうかがチェックされる。一致があればステップＳ４４に進み、家庭用開錠認証センサ１３が健康管理データ取得に成功したかどうかがチェックされる。成功しない場合とは、家庭用開錠認証センサ１３で得られた情報が開錠照合には充分であるが、健康管理データとするには不十分である場合である。このように、家庭用開錠認証センサ１３で得られた情報については開錠照合に充分なレベルと健康管理データとして充分なレベルには差があり、通常、充分なレベルの情報を得るには後者の方がより高い精度が要求され、また情報の取得にはより時間がかかる。従って、指の挿入時間が短いと、ステップＳ４３で開錠認証照合データが一致した旨の判断が行われても、ステップＳ４４に至って、家庭用開錠認証センサ１３が健康管理データ取得に失敗した旨の判断が行われる可能性がある。

ステップＳ４４で健康管理データ取得が成功したことが確認されるとステップＳ４５に進み、取得したデータを個人健康データベース１５に蓄積する。個人健康データベース１５に蓄積されたデータは医療機関９との契約により、ステップＳ４５の段階でリアルタイムに大型コンピュータ２２にも送信され、総合健康データベースに２７にも蓄積される。これによって、個人健康データベースの内容がバックアップされるとともに、引越し等への対応も可能となる。

【００６９】

次いで、ステップＳ４６において、健康照合データ保持部１６に照合データがあるかどうかをチェックし、データがあればステップＳ４７に進んで、取得したデータとの照合処理を行う。そしてステップＳ４８に進み、照合の結果健康管理データに異常があるかどうかをチェックする。異常があればステップＳ４９に進み、テレビ１７のスイッチを入れたとき自動的に「健康異常」の警告が行われるよう準備し、ステップＳ５０に進む。ステップＳ４８において異常がなければ、直接ステップＳ５０に進む。上記の「健康異常」の表示にあたっては、ステップＳ４３において誰のデータであるか判明しているので、「誰が健康異常であるか」の表示を行うことができる。

【００７０】

テレビでの表示においては、以上のように構成する場合の他、ステップＳ４８において異常ではなくても注意を喚起すべき新しいデータがあるときはこれをステップＳ４９で表示するよう構成することができる。

また、ステップＳ４９において、テレビ１７のスイッチを入れたとき自動的に「健康異常」の警告が行われるよう準備する代わりに、緊急性の高いときはテレビ１７のスイッチを強制的にオンにして即座に表示を開始するよう構成してもよい。

また、ステップＳ４９の表示を行うか行わないかをA居室２の各個人毎に予め希望通りに選択しておくことができるよう構成することも可能である。

【００７１】

ステップＳ５０では、ステップＳ４７の照合結果を個人健康データベースに蓄積する。個人健康データベース１５に蓄積された照合結果のデータについても、医療機関９との契約により、ステップＳ５０の段階でリアルタイムに大型コンピュータ２２に送信され、総合健康データベースに２７にも蓄積される。ステップＳ４８で異常を検出した旨の情報も同時に大型コンピュータ２２に送信され、総合健康データベースに２７に蓄積される。

以上の処理を経てステップＳ５１に至り、ドアロック１１に開錠を指示する。ドアロック１１は、その指示に応じて開錠を実行する。ドアロック１１の開錠指示後、ステップＳ５２で玄関ドアの前に人が立ってから所定時間経過したかどうかのチェックを再度行い、

所定時間経過していれば玄関ドア開錠処理を終了する。ステップＳ５２の意味は後述する。

なお、ステップＳ４６において、健康照合データ保持部１６に照合データがなければ、照合関連の処理は不要なので、直接ステップＳ５１に至り、ドアロック１１に開錠を指示する。

【００７２】

一方、ステップＳ４４において、健康管理データの取得に失敗した場合は、ステップＳ５３においてデータ取得失敗の旨の表示およびステップＳ５４においてその理由の表示をし、ステップＳ５１に至る。このように健康管理データの取得に失敗した場合であっても、ドアロック開錠の指示自体は行う。

玄関ドアから入室しようとしてデータ取得失敗表示およびその理由を見た利用者は、健康管理データの取得を重視する場合には、再度家庭用開錠承認センサ１３に指を挿入してチェックを行うことを望む。ステップＳ５２はこのために設けられているものであり、ドアの前に人が立ってから所定時間経過していない場合はステップＳ４１からステップＳ４２に戻り、指の挿入からやり直すことを可能とする。所定時間が経過してしまった場合は開錠処理を終了するが、どうしても健康管理データの取得をやり直したい場合は、一度玄関ドアから離れ、再度玄関ドアに近づいて、図６のトリガーをかけ直せばよい。

なお、ステップＳ５３でデータ取得失敗表示を見た利用者は、急いでいる場合、そのままＡ居室５に入室して差し支えない。この場合、ステップＳ５４で表示される失敗理由を理解しておき、次回の入室時からはその失敗の理由を除去するよう気をつけて指の挿入を行えばよい。

【００７３】

ステップＳ４１において、ドアの前に人が立ってから指を挿入しないまま所定時間が経過した場合はステップＳ５５に移行し、入室拒否表示を行う。次いで、ステップＳ５６において指が挿入されていない旨の拒否理由の表示を行った後、ステップＳ57に進む。

ステップＳ５７では暗証番号入力やＩＣカード挿入などを行う補助認証を可能とし、補助認証が成功すればステップＳ５１に移行してドアロック開錠を指示する。但し、ステップＳ５７経由でステップＳ５１に至るときは、ステップＳ５０またはステップＳ５４経由の場合と区別できる信号とする。ステップＳ５７はあくまで補助手段であり、セキュリティの観点からは危険が大きいので、上記区別できる信号に基づいて開錠記録を残すとともに必要に応じて警告を行うためである。

補助認証が行われないかまたは補助認証が失敗したときは、ステップＳ５２を経て開錠処理を終了するので、ドアロックの開錠は行われない。

【００７４】

また、ステップＳ４３において、開錠認証照合データが一致しないか、または指が挿入されるが照合に必要なデータが取得されなかった場合も、ステップＳ５５に移行し、入室拒否表示を行う。次いで、ステップＳ５６において開錠認証照合データが一致しない旨の理由表示または照合に必要なデータが取得されない理由の表示を行う。

その後、ステップＳ５７に進み、暗証番号入力やＩＣカード挿入などを行う補助認証を可能とし、補助認証が成功すればステップＳ５１に移行してドアロックの開錠を指示する。補助認証が行われないかまたは補助認証が失敗したときは、ステップＳ５２に進む。

この場合、ステップＳ５２において所定時間が経過していなければステップＳ４１を経てステップＳ４２に戻るので、指の挿入が不適切であった場合、ステップＳ５６の理由表示を参考に指の挿入をやり直せばステップＳ４３からステップＳ４４に進むことも可能となる。

【００７５】

ここで、ステップＳ４３がステップＳ４４以前に設けられていて、開錠認証照合データが一致しないと健康管理データ取得のフローに入れないよう構成していることの意義について補足する。その第一義は、開錠認証照合データが一致しない場合、それは健康管理データを取得する意味のな他人であるからである。

しかし、より重要なのは、正しく指を挿入しておれば本来開錠認証照合データと一致するはずの個人について、開錠認証照合データとの一致がない場合に健康管理データを取得しないようにしている点である。つまり、開錠認証照合データとの一致は指が正しく挿入されたことの保障の意味を持っており、この場合だけ健康管理データを取得するよう構成することによって、指が誤って挿入された状態で不正確な健康管理データが取得されることを防いでいることに意義がある。

換言すれば、取得した生体情報に基づいて生体認証を行うとともに健康管理情報処理を行うことが可能な場合において、生体認証ができないときは健康管理情報処理部を無効とし、これによって健康管理情報の信頼性を保障している。

【００７６】

図７は、マンション入口にの前に人が立ったことを管理パソコン１９が検出し、この通知を受けたAパソコン５に認証トリガーがかかった場合の制御部１２の機能を示すフローチャートである。その動作は図６とほぼ同一なので、説明の大半は省略し、異なっている部分のみコメントする。

図６のステップＳ４２では、指の挿入のチェックを行っていたが、図７の場合は管理パソコン１９がこのチェックを行う。従って、図７のステップＳ６２では管理パソコン１９の業務用開錠認証センサ２１からの指データの受信があったかどうかをチェックする。

【００７７】

ステップＳ６４は図７において加えられたもので、ステップＳ６３で開錠認証データが一致した場合、マンション入口にＡ居室２の住人が帰宅したことを意味するので、このことをＡ居室２内に報知するための信号を発生する。この帰宅報知信号の利用法としては、例えば夫の帰宅をＡ居室２内の妻に事前報知するよう構成する。また独居の場合は、帰宅報知信号によりＡ居室２内のエアコンおよび照明のスイッチを入れるよう構成する。

【００７８】

図７では、図６のステップＳ５３、ステップＳ５４、ステップＳ５５、ステップＳ５６で行われるのと同様の表示に関連するステップがあるが、図７の場合、これらの表示の実行は管理パソコン１９が行うので、Aパソコン５は、ステップＳ７４、ステップＳ７５、ステップＳ７６、ステップＳ７７において、管理パソコン１９による表示のための情報送信のみを行う。

なお、図６ではステップＳ５６における入館拒否理由表示の後、補助認証一致によるドアロック開錠のためのステップＳ５７を置いている。これに対し、マンション入口ロック制御システムでは、補助認証一致による開錠制御は専ら管理パソコン１９のよって行われるので、図７では、ステップＳ７７において入館拒否の情報送信を行った後、直接ステップＳ７３に移行する。

【００７９】

さらに、図６のステップＳ５１と同様の開錠処理が、図７でも行われるが、図７の場合、開錠の指示は管理パソコン１９が行うので、Aパソコン５は、ステップＳ７２において、管理パソコン１９への入口ロック開錠信号の送信処理を行う。

ステップＳ７２において送信される信号は、マンション入口ドアロック開錠指示に直結するセキュリティ上非常に重要な信号なので、ステップＳ７２では、ステップＳ６２において指データとともに受信する管理パソコン１９からの指示に基づいて慎重な送信処理が行われる。まず、管理パソコン１９の指示する暗号コードによって入口ロック開錠信号が暗号化される。さらにその送信タイミングも管理パソコン１９の指示する極短時間幅内に行われる。これらの点については、図１０でさらに詳しく説明する。

以上コメントした部分以外の図７における機能は基本的には図６と同様であるので、説明を省略する。

【００８０】

図８は、図６のステップＳ４７または図７のステップＳ６８において制御部１２によって行われる照合処理の詳細を示すを示すフローチャートである。

照合処理がスタートすると、まずステップＳ８１において個人健康データベース１５に

過去の蓄積データがあるかどうかがチェックされる。過去の蓄積データがあればステップＳ８２に進み、所定の蓄積期間が経過しているかどうかのチェックが行われる。これは、蓄積データの分析照合を行う意味のある期間が経過しているかどうかを見るためのものである。

蓄積データの分析照合を行うのに意味がある充分な蓄積期間が経過していればステップＳ８３に進み、個人健康データベース１５から必要な蓄積データを呼出す。呼出された蓄積データは、ステップＳ８４において蓄積データ照合処理される。この蓄積データ照合処置においては、今回取得したデータも含めて処理する。以上で蓄積データに関する照合を終了し、ステップＳ８５に移行する。ステップＳ８４の蓄積データ処理については経時変化や季節変化など種々の照合があるのでその詳細は後述する。

なお、ステップＳ８１において過去の蓄積データがなければ、直接ステップＳ８５に移行する。また、ステップＳ８２において所定期間が経過してない場合も直接ステップＳ８５に移行する。いずれの場合も、蓄積データ照合処理をする意味がないからである。

【００８１】

ステップＳ８５では今回取得したデータを個人健康データベース１５に蓄積し、ステップＳ８６に進む。ステップＳ８６では、今回取得した健康照合データと保持部１６に保持されている照合データとの単純な照合を行い、ステップＳ８７に進む。ステップＳ８７以下では、状況にあわせてより高度の照合が可能かどうかチェックされ、可能であればそれらの照合が実行される。

【００８２】

まず、ステップＳ８７では、今回取得された健康管理データが業務用開錠認証センサ２１に特有のセンシング機能に由来する項目であるかどうかチェックする。この答えがノーであるということは、取得されたデータが業務用開錠認証センサ２１および家庭用開錠認証センサ１３の両者で共通に取得可能な項目であることを意味する。従って、この場合はステップＳ８８に進み、所定時間内に取得された同一項目のデータがあるかどうかをチェックする。

所定時間内に取得された同一個目のデータがある場合、通常は、A居室２の住人がまずマンション入口にて業務用開錠認証センサ２１による認証を行ってこれを通過し、次いで所定時間内にA居室の玄関ドアに至って家庭用開錠認証センサ１３による認証を行ったことが想定される。

【００８３】

ステップＳ８８で所定時間内に取得された同一個目のデータがある場合はステップＳ８９に進み、データ取得条件が同一かどうかをチェックする。条件が同一である場合は、ステップＳ９０に進む。この場合、データが大きく異なっている場合は一方がエラーである可能性が高いので、ステップＳ９０では両者のデータが近似しているかどうかのクロスチェックを行う。クロスチェックの結果両方のデータが近似しており、両者とも信頼できるときはステップＳ９１に進んで両者の平均化処理を行い、照合処理を終了する。

【００８４】

一方、ステップＳ９０のクロスチェックの結果、両者が大きく食い違っている場合は、いずれかのセンサが異常である可能性があるのでステップＳ９２に進み、過去のデータを参考にして信頼できない方のデータを出したセンサを異常状態にあると判断し警告を行う。あわせてステップＳ９３でそのセンサからのデータをエラーと見做し、破棄する。

以上のように、ステップＳ８９においてデータ取得条件が同一の場合、業務用開錠認証センサ２１によって取得されたデータと家庭用開錠認証センサ１３によって取得されたデータにより同一項目をダブルチェックし、データの信頼性を高める。

【００８５】

一方、ステップＳ８９において、データ取得条件が異なっていた場合、データ取得条件に依存する健康管理データの変化の因果関係を含めた照合が可能となる。データ取得条件が異なる場合とは、すでに述べたように、業務用開錠認証センサ２１によるチェックを行ったときと家庭用開錠認証センサ１３によるチェックを行ったときとで同一人物自身の運

動負荷が異なっていた場合などが該当する。さらに、通常は戸外にある業務用開錠認証センサ２１でチェックを行ったときと通常は館内にある家庭用開錠認証センサ１３でチェックを行ったときとで、気温などの気象条件が異なり、これが健康管理データに影響を与えている場合もこれに該当する。

ステップＳ８９でこのようなデータ取得条件の違いが検知されたときには、ステップＳ９４に進み、運動負荷が異なる場合には脈拍数などのデータ、気象条件が異なっている場合には、気温、湿度、風速などのデータを健康管理データ取得の条件として付加し、このような因果関係を含めて照合を行う。

【００８６】

ステップＳ８７において、取得された健康管理データが業務用開錠認証センサ２１に特有のセンシング機能に由来する項目である場合には、同一の項目が家庭用開錠認証センサ１３によって検出されることはないので、ステップＳ８６の単純照合だけで直ちに照合処理を終了する。

また、ステップＳ８９において所定時間内に取得された同一項目のデータがない場合も、後の処理は意味がないので直ちに照合処理を終了する。

なお、以上の機能において、何か特別な事情で業務用開錠認証センサ２１のみによる認証または家庭用開錠認証センサ１３のみによる認証を所定時間内に続けて行った結果ステップＳ８８の答えがイエスになった場合でもステップＳ８９に進むことがあるが、その場合でも効果は有効である。

【００８７】

図９は、マンション入口ロック制御システム８の管理パソコン１９における制御部５３の機能を示す基本フローチャートである。この基本フローチャートはAパソコンのＯＳの制御に従って、適宜繰り返し実行される。

図９のフローがスタートすると、ステップＳ１０１で業務用開錠認証センサ２１のセンサユニット５１が変更されていないかどうかチェックする。変更があるとステップＳ１０２で新たなセンサユニットのドライバソフトをインストールする処理を行う。このとき、新たなセンサユニット５１が医療機関９から提供されたものである場合は、制御部５３は医療機関９の大型コンピュータから通信によりドライバソフトの提供を受け、自動インストールを行う。イ

ンストール処理が終了すれば、ステップＳ１０３に移行する。なお、センサユニット５１に変更がなければ、直接ステップＳ３に移行する。

【００８８】

ステップＳ１０３では、医療機関９の健康照合ソフト２４がバージョンアップされていないかどうかチェックする。バージョンアップがあると、ステップＳ１０４で医療機関９の大型コンピュータ２２からバージョンアップに関する新たなソフトの提供を受け、管理パソコンにおける健康管理データ取り扱いソフトを自動書き換えしてステップＳ１０５に移行する。バージョンアップがなければ、直接ステップＳ１０５に移行する。

【００８９】

なお、健康照合ソフト２４のバージョンアップの通知は医療機関９側のサービスとしてビジネス上大きな意味を持っている。従って、医療機関９はステップＳ１０３の過程を利用してその他の医療機関９側のサービス情報を提供することができる。例えば、次回受信日のリマインダ、定期健康診断の案内さらには花粉情報などを契約している個人のニーズに合わせて送信する。

ステップＳ１０４では、これら健康管理データ取り扱いソフト変更に直接関係のない情報を受け取ったときでも、これを記録し、次回にテレビ１７がつけられたときにそのサービス情報が表示されるよう準備を行う。

【００９０】

ステップＳ１０５では、業務用開錠認証センサ２１の保護ユニット５２が外部環境に曝されることによる劣化や破損またはいたずらによる破壊などにより損傷していないかどうかチェックする。損傷があり、センサユニット５１が正常に動作しないと判断されたとき

は、ステップＳ１０６で保護ユニット交換を促す警告を行ってステップＳ１０７に移行する。なお、保護ユニット５２に損傷がなければ、直接ステップＳ１０７に移行する。

【００９１】

ステップＳ１０７では、マンション入口ロック制御システム８に新たな居室が加入したかどうかまたは加入済みの居室が脱退したかどうかをチェックする。加入または脱退があるとステップＳ１０８でその旨の処理を行う。

これによって、新規加入の居室の住人に対するマンション入口の開錠を可能にするとともに、常に全居室からの認証結果受信の有無を把握できるようにする。加入または脱退の処理が終わるとステップＳ１０９に移行する。なお、居室の加入または脱退がないときは、直接ステップＳ１０９に移行する。

【００９２】

ステップＳ１０９では、マンション入口ロック制御システム８において認証照合データの新規登録が求められたかどうかをチェックする。新規登録が求められた場合にはステップＳ１１０に進んで登録処理を行い、ステップＳ１１１に移行する。なお、新規登録が求められていないときは、直接ステップＳ１１１に移行する。ステップＳ１１０の登録処理の詳細については後述する。

【００９３】

ステップＳ１１１では、センサチェック処理を行う。これは図４のステップＳ１２と同様のものであるが、管理パソコン１９の場合、業務用開錠認証センサ２１のチェックを担当し、その変更の際の初期状態での動作チェックを行う他、その後の故障や劣化がないかどうかのチェックを行う。その詳細については後述する。

【００９４】

次いでステップＳ１１２に移行し、マンション入口での認証トリガーを待機状態とする。具体的には、マンション入口に人が立ったときこれを管理パソコン１９が認識して認証機能がスタートするよう管理パソコン１９を待機させる。

【００９５】

図１０は、マンション入口にの前に人が立ったことを管理パソコン１９が検出し、認証トリガーがかかった場合の制御部５３の機能を示すフローチャートである。

このトリガーがかかった場合、ステップＳ１15において、まずマンション入口の前に人が立ってから所定時間経過したかどうかのチェックをおこなう。所定時間経過していなければステップＳ１16に進み、業務用開錠認証センサ２１への指の挿入が行われたがどうかをチェックする。指の挿入がなければステップＳ１15に戻り、以下、所定時間が経過するまで指の挿入を待つ。

【００９６】

ステップＳ１16において指の挿入があって生体情報が取得できるとステップＳ１17に進み、マンション入口ロック制御システムに加入している全居室に取得データを送信する。次いで、ステップＳ１18において、送信した取得データと開錠認証照合データが一致したことを示す認証データが受信されたかどうかがチェックする。なお、この認証データは偽造防止や誤信号との混同防止のため、暗号化されている。この暗号化コードは乱数表によってその都度変更され、ステップＳ１１７の取得データ送信時に各居室に伝えられる。ステップＳ１１８において、いずれかの居室から認証データの受信があればステップＳ１19に進む。

【００９７】

ステップＳ１１９では、ステップＳ１１８における受信がステップＳ１１７における送信に関連して決められる所定の極短時間幅内にあったのかどうかチェックする。後述のようにステップＳ１１８において受信する信号は、入口ドアロック開錠指示に直結する非常に重要な信号なので、ステップＳ１１９を置いて、さらに誤信号による誤動作防止と偽造認証データ信号発信によるロック破りに対抗する。特に認証データの偽造に対抗するため、ステップＳ１１９における極短時間幅は乱数表に基づいてその都度変更され、ステップＳ１１７によるデータ送信を受けた居室のパソコンだけにその時間幅が指定される。居室

のパソコンは指定された時間幅の間に認証データを管理パソコン１９に送信するので、この時間幅以外に受信された認証データ信号は偽造信号または誤信号と判断される。
ステップＳ１１９において認証データが指定どおりの極短時間幅に受信されたことが確認されるとステップＳ１２０に進む。

【００９８】

ステップＳ１２０では、いずれかの居室から健康管理データ取得失敗の旨の通知が入信されたかどうかチェックする。失敗した場合とは、送信した取得データが開錠照合には充分であるが、健康管理データとするには不十分であるといずれかの居室にて判断された場合である。
ステップＳ１２０で健康管理データ取得失敗の旨の通知がいずれの居室からも受信されないことが確認されるとステップＳ１２１に進み、入口ロック２０に開錠を指示する。入口ロック２０はその指示に応じて開錠を実行する。
以上のステップＳ１１８およびステップＳ１２０における居室から管理パソコンへの認証データの送信および健康管理データ所得失敗の送信においては、これらの送信がいずれの居室から行われたか管理パソコン１９側ではわからないようにし、プライバシー保護に配慮する。

【００９９】

入口ロック２０開錠指示後、ステップＳ１２２に進み、ステップＳ１１６で取得した生体情報を消去する。これは、プライバシー保護の万全を期するためである。その後ステップＳ１２３に進み、再度マンション入口の前に人が立ってから所定時間経過したかどうかのチェックをおこなう。所定時間が経過していれば、開錠処理を終了する。

【０１００】

一方、ステップＳ１２０において、健康管理データの取得に失敗した旨の通知を受信したことが確認された場合は、ステップＳ１２４においてデータ取得失敗の旨の表示を行うとともに、ステップＳ１２５においてその理由の表示をし、ステップＳ１２１に至る。このように、健康管理データの取得に失敗した場合であっても、入口ロック開錠の指示を行うことは、マンション入口開錠制御システム８でも同様である。

【０１０１】

ステップＳ１１５において、ドアの前に人が立ってから指を挿入しないまま所定時間が経過した場合はステップＳ１２６に移行し、入館拒否表示を行う。次いで、ステップＳ１２７において指が挿入されていない旨の拒否理由の表示を行った後、ステップＳ１２８に進む。
ステップＳ１２８では暗証番号入力やＩＣカード挿入などを行う補助認証を可能とし、補助認証が成功すればステップＳ１２１に移行して入口ロック開錠を指示する。このときステップＳ１２０またはステップＳ１２５経由でステップＳ１２１に至る場合と区別できる信号とするのは、図６の５７と同様である。得にステップＳ１２８の場合はマンション入口という公共の場所なのでより高いセキュリティが求められる。従ってステップＳ１２８の補助認証の際には誰がこれを求めたのかの個人IDを取得して記録に残す。
補助認証が行われないかまたは補助認証が失敗したときは、ステップＳ１２２およびステップＳ１２３を経て開錠処理を終了するので、入口ロック２０の開錠は行われない。なおこの場合、元々消去すべき生体情報の取得がないのでステップＳ１２２では結果的に何もしないのと同じことになるが、次に述べる事情のためにステップＳ１２２を経由するようにしている。

【０１０２】

ステップＳ１１６を経由して生体情報を得ている場合であって、ステップＳ１１８においていずれの居室からも認証データを受信しない場合、ステップＳ１２６に移行し、入館拒否表示を行う。次いで、ステップＳ１２７において入室拒否表示の理由表示を行う。
また、ステップＳ１１９において認証データが指示通りの極短時間幅内に受信されなかった場合も、同様にステップＳ１２６に移行して入館拒否表示を行うとともにステップＳ１２７において入室拒否表示の理由表示を行う。

表示すべき理由に関する情報は、管理パソコン１９だけでは分からない場合もあるので、そのときは認証機能を担当している各居室のパソコンから入手する。ただし、どの居室からの情報であるかは管理パソコン１９が検知できないようにし、各居室のプライバシーを守っている。

その後、ステップＳ１２８に進み、暗証番号入力やＩＣカード挿入などを行う補助認証を可能とし、補助認証が成功すればステップＳ１２１に移行してドアロックの開錠を指示する。補助認証が行われないかまたは補助認証が失敗したときは、ステップＳ１２２に進み、ステップＳ１１６で取得した生体情報を消去する。このように、認証ができなかった場合であっても取得した生体情報は消去し、プライバシーの保護を万全とする。

次にステップＳ１２３に進むが、ここで所定時間が経過していなければステップＳ１１５を経てステップＳ１１６に戻るので、指の挿入が不適切であった場合、ステップＳ１２７の理由表示を参考に指の挿入をやり直せばステップＳ１１６からステップＳ１１７に進むことも可能となる。

【０１０３】

図１１は、医療機関９の大型コンピュータ２２における制御部２６の機能を示す基本フローチャートである。機能がスタートすると、ステップＳ１３１において業務用開錠認証センサ２１の新規登録または既登録センサの抹消または更新がないかどうかチェックする。更新にはセンサのバージョンアップによる機能変更も含まれる。業務用開錠認証センサ２１に登録、抹消、更新のいずれかがあればステップＳ１３２に進み、大型コンピュータのデータまたはソフトにその旨の変更を行った上でＳ１３３に移行する。これによって医療機関９がカバーする業務用開錠センサの変更に対応することができる。なお、業務用開錠認証センサ２１に変更がなければ直接ステップＳ１３３に移行する。

【０１０４】

ステップＳ１３３とステップＳ１３６では、家庭用錠認証センサ１３の新規登録または既登録センサの抹消または更新がないかどうかチェックする。更新にはセンサのバージョンアップによる機能変更も含まれる。家庭用認証センサ１３に登録、抹消、更新のいずれかがあればステップＳ１３４に進み、大型コンピュータによって引越し処理が行って、ステップＳ１３５に移行する。

家庭用開錠認証センサの登録、抹消、更新は、単なるセンサーのバージョンアップによることもあるが、多くの場合、家族の引越しによるマンションへの入退居を伴い、居室内パソコン内のデータ処理も必要なので、引越し処理にはいくつかの手続きが伴う。その詳細については後述する。なお、家庭用開錠認証センサ１３に変更がなければ直接ステップＳ１３５に移行する。

【０１０５】

ステップＳ１３５では、医療機関９における個人の新規登録または既登録個人についての抹消または更新がないかどうかチェックする。変更があればステップＳ１３６に進み、大型コンピュータにその旨の登録、抹消、更新を行う。

また、個人の新規登録または既登録個人についての抹消は、多くの場合、医療機関の変更により生じるので、ステップＳ１３７で変更先の他の医療機関との個人データの引継ぎを行う。

つまり、他の医療機関から医療機関９に転入した結果新規登録となった場合には、元の医療機関の大型コンピュータに記録されていた個人の健康照合データおよび健康管理データを、転入した医療機関９の健康照合データ登録部２３および総合健康データベース２７にそれぞれ移管する。逆に、他の医療機関に転出した際には、医療機関９の健康照合データ登録部２３および総合健康データベース２７に保持されていた個人の健康照合データおよび健康管理データをそれぞれ転出先の医療機関に転送するとともに、医療機関９の大型コンピュータ２２からは消去する。

なお、個人の誕生、死亡、または結婚による姓の変更など、健康管理の登録、抹消、更新の手続きが複数の医療機関にまたがらない場合、ステップＳ１３７の処理は省略される。

以上の処理の後、ステップＳ１３８に移行する。なお、ステップＳ１３５において個人の登録、抹消、更新がなければ直接ステップＳ１３３に移行する。

【０１０６】

ステップＳ１３８では、登録されている個人の健康照合データについて登録、抹消、更新がないかチェックする。健康照合データに異動があれば、ステップＳ１３９に進み、大型コンピュータ２２の健康照合データ登録部２３のデータを変更してステップＳ１４０に移行する。なお、健康照合データに異動がなければ、直接ステップＳ１４０に移行する。

【０１０７】

ステップＳ１４０では、登録されている個人による統計処理データ配信希望について登録、抹消、更新がないかチェックする。統計処理希望に異動があれば、ステップＳ１４１に進み、大型コンピュータ２２の希望データを変更してステップＳ１４２に移行する。なお、統計処理希望に異動がなければ、直接ステップＳ１４２に移行する。

【０１０８】

ステップＳ１４２では、契約している個人のパソコンから医療機関９に送られる健康センサのデータまたは健康照合結果のデータを受信するための待機処理を行う。また、ステップＳ１４２では、契約している個人のパソコンに、健康照合データ、診断結果、統計処理情報など、種々の情報を送信する処理の待機を行う。以上で基本フローを終了する。

【０１０９】

図１２は、医療機関９の大型コンピュータ２２の制御部２６における送信処理の詳細を示すフローチャートである。この送信処理は、図１１のステップＳ１４３によって制御部２６が待機状態なっているとき種々のトリガーによってスタートする。

送信処理がスタートすると、ステップＳ１５１で、健康照合データ登録部２３においてある個人に対する健康照合データが新規登録されたことによってトリガーがかかったのかどうかがチェックされる。答えがイエスならステップＳ１５２に進み、その個人の使用しているパソコンに健康照合データの送信を行ってステップＳ１５３に移行する。例えば、健康照合データを新規登録したのがA居室２に入居している家族の一員なら、Aパソコン５に健康照合データを送信し、Aパソコン５は受信した健康照合データを健康照合データ保持部１６に収納する。なお、健康照合データの新規登録によってトリガーがかかったのではないときは、直接ステップＳ１５３に移行する。

【０１１０】

ステップＳ１５３では、総合健康データベース２７に保持されているデータに基づき、ある個人について健康照合ソフトよって新規に自動診断結果が出されたことによってトリガーがかかったのかどうかがチェックされる。答えがイエスならステップＳ１５４に進み、その個人の使用しているパソコンに自動診断結果の送信を行ってステップＳ１５５に移行する。なお、自動診断結果が出されたことによってトリガーがかかったのではないときは、直接ステップＳ１５５に移行する。

【０１１１】

ステップＳ１５５では、総合健康データベース２７に保持されているデータに基づき、ある個人について医師２５が診断入出力部２８に診断結果を入力したことによってトリガーがかかったのかどうかがチェックされる。答えがイエスならステップＳ１５６に進み、その個人の使用しているパソコンに医師の診断結果を送信する。

【０１１２】

次いでステップＳ１５７に進み、自動診断結果と異なる医師の所見があるかどうかがチェックされる。医師の異所見があった場合はステップＳ１５８に進み、その旨の警告を個人のパソコンに併せて送信し、医師の所見が自動診断結果と異なることについて注意を喚起する。所見が異なるときは医師の所見が優先される。

次いで、ステップＳ１５９に進み、所見が異なった理由に基づいて健康照合ソフトを改変するための処理を開始させた後、ステップＳ１６０に移行する。

【０１１３】

ステップＳ１５５において医師の診断結果がない場合は、直接ステップＳ１６０に移行

する。また、ステップＳ１５７において自動診断結果と異なる医師の所見がない場合も、直接ステップＳ１６０に移行する。

【０１１４】

ステップＳ１６０では、統計処理の希望を登録している個人に配信すべき統計データが作成されたことによってトリガーがかかったのかどうかがチェックされる。答えがイエスならステップＳ１６１に進み、その個人の使用しているパソコンに、統計データおよびその統計データ中でその個人がどんな位置にいるかの情報を送信して送信処理を終了する。なお、統計データの作成によりトリガーがかかったのではないときは、直ちに送信処理を終了する。

【０１１５】

図１３は、図１１のステップＳ１３４における引越し処理の詳細を示すフローチャートである。

引越し処理がスタートすると、まずステップＳ１７１で、家庭用開錠認証センサの新規登録であるかどうかをチェックする。新規登録であればステップＳ１７２に進んで新規の家庭用開錠認証センサを医療機関９の大型コンピュータ２２に登録する。する。これによって登録された家庭用開錠センサ１３が大型コンピュータ２２の管理下に入り、家庭用開錠センサ１３がで取得された健康管理データが大型コンピュータ２２で処理されるようになる。

【０１１６】

次いで、ステップＳ１７３に進み、新規登録された家庭用開錠認証センサが設置されている居室に入居した家族に医療機関９に登録済の個人が含まれていないかどうかをチェックする。そして登録済みの個人が含まれていればステップＳ１７４に進む。この場合は、例えば、別の住居において医療機関９にすでに登録されていた個人が転居し、マンション１のA居室２に入居してAパソコン５から家庭用開錠認証センサ１３の登録をしてきた場合に相当する。

そのような場合は、その個人の健康照合データが大型コンピュータ２２の健康照合データ登録部２３に既に登録されている可能性があるので、ステップＳ１７４でその有無をチェックする。そして、健康照合データが登録されていた場合はステップＳ１７５でその健康照合データをAパソコン５に送信してステップＳ１７６に移行する。Aパソコン５は受信した健康照合データを健康照合データ保持部１６に保持させる。なお、ステップＳ１７４において健康照合データの登録がなければ、直接ステップＳ１７６に移行する。

【０１１７】

医療機関９に登録済みの個人であれば、その個人の健康管理データが大型コンピュータ２２の総合健康データベース２７に保持されている可能性があるので、ステップＳ１７６でこれをチェックする。そして、登録があればステップＳ１７７でその個人の健康管理データをAパソコン５に送信してステップＳ１７８に移行する。Aパソコン５は受信した個人健康管理データを個人健康データベース１５に保持させる。このような過去の個人健康管理データは経時変化をAパソコン５にてローカルにチェックする際有用となる。なお、ステップＳ１７６において個人健康管理データの保持がなければ、直接ステップＳ１７８に移行する。

【０１１８】

ステップＳ１７１において、家庭用開錠認証センサの新規登録でなかったときは、直接ステップＳ１７８に移行する。また、ステップＳ１７３において、新規登録された家庭用開錠認証センサに関する家族中に医療機関９に登録済の個人が含まれていなかった場合も、直接ステップＳ１７８に移行する。

【０１１９】

ステップＳ１７８では、家庭用開錠認証センサ１３の抹消であるかどうかをチェックする。抹消の必要性は、例えば、A居室２に居住していた家族が転居する場合に生じる。家庭用開錠認証センサ１３の抹消であればステップＳ１７９に進み、家庭用開錠認証センサ１３の登録を医療機関９の大型コンピュータ２２から抹消する。登録されていた家庭用開

錠認証センサ１３は大型コンピュータ２２の管理外となる。

【０１２０】

次いで、ステップＳ１８０に進み、Aパソコン５に認証照合データ消去信号を送る。Aパソコン５は、この消去信号に応答し、認証照合データ保持部１４から転居する家族全員の認証照合データを消去する。本来、開錠認証は医療機関９の管理する領分ではないが、開錠認証データは個人のプライバシーに関する生体データであり、同じ家庭用開錠認証センサ１３に関連しているので、転居の際に医療機関９はこのようなプライバシー保護のサービスも行う。

【０１２１】

次いでステップＳ１８１に移行し、医療機関９の健康照合データ登録部２３に転居する家族中の個人の健康照合データが登録されているかどうかをチェックする。登録があれば、その健康照合データは医療機関期間９でそのまま保持する。そしてステップＳ１８２に進み、Aパソコン５に健康照合データ消去信号を送ってステップＳ１８３に移行する。Aパソコン５は、この消去信号に応答し、健康照合データ保持部１６から転居する家族全員の健康照合データを消去する。なお、ステップＳ１８１において健康照合データの登録がなければ、直接ステップＳ１８３に移行する。

【０１２２】

ステップＳ１８３では、医療機関９の総合健康データベース２７に転居する家族中の個人の健康管理データがバックアップされているかどうかをチェックする。バックアップがあれば、その健康管理データは医療機関期間９側でそのまま保持する。そしてステップＳ１８４に進み、Aパソコン５に健康管理データ消去信号を送って引越し処理を終了する。Aパソコン５は、この消去信号に応答し、個人健康データベース１５から転居する家族全員の健康管理データを消去する。なお、ステップＳ１８３において健康管理データのバックアップがなければ、直ちに引越し処理を終了する。

【０１２３】

ステップＳ１７８において、家庭用開錠認証センサ１３の抹消でなかったときはステップＳ１８５に進む。この場合は、家庭用開錠認証センサの新規登録でも抹消でもなかったことを意味し、引越しを伴わない家庭用開錠センサの更新であるので、ステップＳ１８５で更新処理を行い、引越し処理を終了する。

【０１２４】

以上の実施例１では、複数の家族が入居しているマンションにおける実施を例に説明してきた。しかしながら実施例１ようなシステムの実施は、これに限られるものではなく、複数の会社が入居している雑居ビルであって共通の入口を有するケース、または複数の部署が入居している事業所であって共通の入口を有するケースなどでも実施可能である。

【実施例２】

【０１２５】

図１４は、本発明の生体認証兼健康管理システムの実施例２のブロック図である。複数の家族が入居しているマンションの入口およびその各居室ドアの開錠システムに関する点は実施例１と共通するが、携帯電話１０１を利用した点が実施例１と異なる。なお、マンション入口ロック制御システム８および医療機関９の構成は実施例１と共通する点が多いので、図１と共通のブロックには同一番号を付し、必要がない場合は説明を省略する。

また、実施例２の場合、各居室の玄関ドアにおけるロック制御システムは、マンション入口ロック制御システム８と同様の構成なので、図１４における図示と説明を省略する。

【０１２６】

マンション入口ロック制御システム８の構成は、Ａ近距離無線通信部１０２を有する。このＡ近距離無線通信部１０２としては、例えばブルートゥース（商標）、無線LAN、無線USBなどの通信システムが採用可能である。

実施例２の管理パソコン１９は、実施例１と同様、マンション１のA居室２におけるAパソコン５などと通信可能であるが、さらに入口ロック２０の開錠および健康管理データ処理のためにＡ近距離無線通信部１０２によって携帯電話１０１と通信可能となっている。

マンション入口ロック制御システムのその他の構成は実施例１と共通である。

【０１２７】

医療機関９は、Ｂ近距離通信部１０３およびＢ電話通信部１０４を有する。Ｂ近距離通信部１０３は、Ａ近距離通信部と共通の通信システムにより構成される。また、Ｂ電話通信部は携帯電話通信システムに従ったものである。

実施例２の医療機関９の大型コンピュータは、実施例１と同様、マンション入口ロック管理システム８やマンション１のA居室２におけるAパソコン５などと通信可能であるが、さらに健康管理データ処理のためにＢ近距離無線通信部１０３またはＢ電話通信部によって携帯電話１０１と通信可能となっている。医療機関９のその他の構成は実施例１と共通である。

【０１２８】

実施例２において、マンション入口の開錠を望む人は、携帯電話１０１を持ってマンション入口に近づく。管理パソコン１９の認証トリガーは、実施例１と同様の人センサ５８が人の接近を検知したことによっても可能であるが、併せて、Ａ近距離無線通信部１０２の通信圏内に携帯電話１０１が入ったことをＡ近距離無線通信部１０２自体が検知することによってもトリガーがかかるようになっており、これらのいずれか早い方の検知によってトリガーがかかる。

業務用開錠認証センサ２１に指が挿入されて情報が取得されると、管理パソコン１９はその情報をＡ近距離無線通信部１０２から携帯電話１０１に送信する。携帯電話１０１には、Ａ近距離無線通信部１０２と共通の通信システムに基づくＣ近距離無線通信部１０５が設けられている。

【０１２９】

Ａ業務用開錠認証センサ２１が取得した情報を近距離無線通信部１０２から受信したＣ近距離無線通信部１０５は、これを制御部１０６に送る。制御部１０６に送られた業務用開錠認証センサ２１からの情報は、認証照合データ保持部１０７にあらかじめ登録しておいた認証照合データと照合される。そして、照合の結果、マンションへの入館資格がある人であることが認証されると、制御部１０６はその旨をＣ近距離無線通信部１０５からＡ近距離無線通信部１０２を経由して管理パソコン１９に通知する。

管理パソコン１９はこの通知に応じて入口ロック２０に開錠信号を送る。一方、認証照合データと一致しなければ制御部１０６は同様のルートで管理パソコン１９に不一致の旨通知する。この場合、管理パソコン１９は入口ロック２０に開錠信号を送らない。

【０１３０】

以上のように、実施例２においても、マンション入口ロック制御システム８の管理パソコン１９自体には認証照合データの記録や照合機能はなく、単に照合結果が携帯電話１０１から通知されるだけである。このような配慮により、血管パターンや眼底パターンなどプライバシーにかかわる生体認証用の認証照合データは携帯電話１０１内に留められる。また、管理パソコン１９自体に照合機能がなく、かつ照合結果が誰の携帯電話から来たものか分からないので、業務用開錠センサ２１によって取得されるデータも誰のものかわからず、実施例１と同様にしてプライバシーが保護される。

【０１３１】

業務用開錠認証センサ２１は、実施例１と同様、認証用の情報だけでなく、健康管理情報も取得できる。従って、業務用開錠認証センサ２１による健康管理も可能となる。

つまり、Ａ業務用開錠認証センサ２１によって取得され、近距離無線通信部１０２からＣ近距離無線通信部１０５を経て制御部１０６に送られた情報は血液の成分情報や血管の若さなどの健康管理データを含んでいる。そこで、制御部１０６は、これらの健康管理データーを健康照合データ保持部１０８に登録されている携帯電話所有者本人の健康照合データと照合する。

実施例１と同様、健康管理データ保持部１０８には、健康指標となる値そのものだけでなく、その値の経時変化についての照合用経時変化データも登録されている。従って、制御部１０６は、業務用開錠認証センサ２１から送られてくるその時々の健康管理データを

健康照合データと照合するとともに、本人健康データベース１０９に蓄積されたデータに基づく健康指標の経時変化を健康照合データ保持部１０８に登録された照合用経時変化データと比較し、健康指標となる値の経時変化の速さなどの観点からも照合を行う。健康指標の値の照合結果および健康指標の経時変化の照合結果は、携帯電話の表示部１１０に表示される。この表示については、例えば照合の結果、異常と認められるときには警告音を発して携帯電話１０１の所有者が表示部１１0に注目するようにする。

【０１３２】

携帯電話１０１は、さらに実施例１のユーザ認証センサ１８と同様の生体認証機能をもったユーザ認証センサ１１１を持っている。従って、携帯電話使用におけるユーザ認証の際にも、生体認証データと健康管理データの取得とを同時に行うことができる。

【０１３３】

携帯電話１０１は、また、電話中に健康情報を検知できる健康センサ１１２を有しており、ここから得られた情報についても業務用開錠認証センサ２１やユーザ認証センサ１１１からの情報と同様、健康管理のために活用される。健康センサの例としてはマイク近辺に設けられる息成分センサや、スピーカ近辺またはイヤホンに設けられる耳式体温計などがある。健康センサ１１２は健康情報収集専用の機能をもっていればよく、必ずしも生体認証情報は得られなくてもよい。

【０１３４】

携帯電話１０１は、さらに、腕時計、ベルト、眼鏡、靴など、日常的な装身具に設けられた健康センサからの情報をＣ近距離無線通信部１０５で受信し、これらから得られた情報についても健康センサ１１２などからの情報と同様、健康管理のために活用する。

また、常に携帯電話の近辺にあるアイテムだけではなく、例えばマッサージ機などに設けた健康センサからの情報をＣ近距離無線通信部１０５で受信することによって、健康センサ１１２などからの情報と同様、健康管理のために活用することができる。

【０１３５】

図１４における携帯電話１０１におけるＣ近距離無線通信部１０５は、以上のような元々他の用途のために提供されるアイテムに付加的に設けた健康センサからの情報を受け取って本人健康データベース１０９に記録する場合だけでなく、例えば医療機関９の待合室などに設置されている専用の血圧計によって得られた血圧データを血圧計に設けられたＢ近距離無線通信部１０３から受信し、本人健康データベース１０９に記録することもできる。

【０１３６】

また、Ｃ近距離無線通信部１０５を経て得られた情報や、ユーザ認証センサ１１１、健康センサ１１２から得られた情報については、健康照合データと照合した上で表示部１１０に表示する場合の他、照合なしに利用することもできる。例えば、単に本人健康データベース１０９に蓄積していき、蓄積された経時変化情報をそのままグラフにして表示部１１０に表示することも可能である。さらには、得られた情報をリアルタイムでそのまま表示部１１０に表示することも可能である。

このような、蓄積された経時変化情報をそのままグラフにして表示することは、図１の実施例１におけるテレビ１７による表示でも可能である。また、得られた情報をリアルタイムでそのままテレビ１７に表示することも可能である。

【０１３７】

携帯電話１０１は、当然のこととして、携帯電話本来の電話機能部１１３およびＣ電話通信部１１４を持っている。これらについては従来技術のとおりであるので説明は省略する。

説明の順序が逆になったが、Ｃ電話通信部１１４は医療機関９のＣ電話通信部と共通の携帯電話通信システムに準拠している。従って、携帯電話回線を通じたインターネットによって遠隔地においても携帯電話１０１と医療機関９は情報のやり取りが可能である。例えば、本人健康データベース１０９の内容をリアルタイムで送信して医療機関９にバックアップさせるとともに、医療機関９から自分自身の健康照合データや健康管理データ、診

断結果などの配信を受けることができる。このように携帯電話１０１は、実施例１のＡパソコンとほぼ同等の機能を持つとともに、さらに個人単位のプライバシーの保護が可能なものとなっている。

【０１３８】

携帯電話１０１と医療機関９との情報交換は、以上のように遠隔地においてＢ電話通信部１０４とＣ電話通信部１１４との間で行う他、健康照合データ登録のためなどで携帯電話１０１の使用者が医療機関９を実際に訪れたときには、医療機関９の通信スポットにおいてＢ近距離無線通信部１０３とＣ近距離無線通信部１０５との間で行うこともできる。

【０１３９】

図１４の携帯電話１０１における制御部１０６の動作フローは、図７とほぼ同じである。但し、図７のステップＳ６９におけるテレビ警告準備の代わりに、携帯電話１０１の表示部１１０での警告の準備を行う。これによって、その後表示部１１０がオンとなったとき自動的に「健康異常」の警告が行われる。

また、図１４におけるマンション入口ロック制御システム８における管理パソコン１９の制御部の動作フローも図１０とほぼ同一である。但し、図１０のステップＳ１１７における全居室への取得データ送信の代わりに、携帯電話１０１のＣ近距離無線通信部１０５へのデータ送信を行う。

【０１４０】

図１４のような携帯電話１０１を利用したシステムの実施は、マンションや会社入口の開錠システムだけでなく、銀行における預金引き出しの本人確認など、お金や情報へのアクセスにおける個人認証に生体認証システムを導入している機関においても実施できる。

例えば、銀行における実施の場合、図１４に「マンション入口ロック制御システム８」とあるのを「現金自動預け払い機」と読替えるとともに、図１４に「業務用開錠認証センサ２１」とあるのを「預金口座本人確認センサ」と読替え、さらに図１４に「入口ロック２０」とあるのを「預金引出し入力許可部」と読替えればよい。

上記の読み替えを行った図１４において、携帯電話１０１を持った本人が「現金自動預け払い機」８に接近するとA近距離無線通信部１０２とC近距離無線通信部の交信が始まる。そして、「預金口座本人確認センサ」２１に指を差し入れるとその情報が携帯電話１０１に送られて制御部１０６によって認証照合データ保持部１０７の照合データと比較され、一致していればその結果が管理パソコン１９に送られてれ「預金引き出し入力許可部」２０への預金引出し金額入力や預金引出し実行入力が可能となる。このように、生体認証における照合データの保持および照合は銀行側では行われないのでプライバシーが保護される。

また、「預金口座本人確認センサ」２１から携帯電話１０１に送られてた情報には健康管理データも含まれているので携帯電話側でこれを表示したり、蓄積したり、健康初号データと比較したりすることができる。利用者に対するこのような利便は、銀行側のサービスとして捉えることができる。

【０１４１】

次に、開錠認証照合データの登録処理の詳細について説明する。

まず、実施例１の場合について説明すると、図１５は、図４のステップＳ１１における開錠認証照合データ登録処理の詳細を示すフローチャートである。フローがスタートすると、ステップＳ１９１でA居室２における玄関ドア１０の開錠のための照合データを新規に登録する要求があるかどうかがチェックされる。要求があればステップＳ１９２に進み、
マンション入力照合データが既に認証照合データ保持部に登録済みかどうかチェックする。

登録済みでなければステップＳ１９３に進み、家庭用開錠認証センサ１３からのセンサ出力の受信を待つ。この出力は、照合データ作成のために本人確認された個人の指を家庭用開錠認証センサ１３に挿入することによって行われる。センサ出力の受信があればステ

ップＳ１９４に進み、センサ出力に基づく照合データを仮登録する。
【０１４２】
一方、ステップＳ１９２においてマンション入力照合データが既に認証照合データ保持部に登録済みであれば、玄関ドア照合データとして共通に流用できる可能性があるのでス直接ステップＳ１９４に移行し、登録済みのマンション入力照合データをコピーしてこれを玄関ドア照合データとして仮登録する。
【０１４３】
次にステップＳ１９５に進み、家庭用開錠認証センサ１３に再び指を挿入して同一である旨の照合が正常に行われるかどうかの確認を行う。ステップＳ１９５でこのような正常動作の確認ができればステップＳ１９６に進み、仮登録しておいた照合データを認証照合データ保持部１４に本登録する。一方、正常動作の確認ができなければ、ステップＳ１９３に戻り、指を挿入し直して再度家庭用開錠認証センサ１３からのセンサ出力を受信し照合データの仮登録をやり直す。登録済みのマンション入力照合データをコピーしてこれを玄関ドア照合データとして仮登録していた場合でも同様である。
ステップＳ１９５で正常動作の確認ができ、ステップＳ１９６で玄関ドア照合データの本登録が終わればステップＳ１９７に移行する。また、ステップＳ１９１で、玄関ドア照合データの新規登録が要求されていなければ、直接ステップＳ１９７に移行する。
【０１４４】
ステップＳ１９７では、マンション入口開錠のための認証照合データ新規登録が管理パソコン１９によって要求されているかどうかがチェックされる。要求があればステップＳ１９８に進み、マンション入口ロック制御システム８において認証照合データ作成のために業務用開錠認証センサ２１に指が挿入され、得られたセンサ出力に基づくデータが管理パソコン１９から送信されるのを待つ。この管理パソコン１９からのデータは、マンション入口ロック制御システム８において既に正常動作の確認が済んでいるものである。管理パソコン１９からのデータが受信されるとステップＳ１９９に進み、管理パソコン１９からのデータを仮登録する。
次いでステップＳ２００に進み、管理パソコン１９側の認証照合データを消去させるための信号を送信する。そして、ステップＳ２０１で認証照合データ消去済みの確認信号が管理パソコン１９から送られてきたかどうかをチェックする。ステップＳ２０１において管理パソコン１９側での認証照合データの消去が確認できれば、ステップＳ２０２に進み、ステップＳ１９９で仮登録しておいた認証照合データを認証照合データ保持部１４に本登録して開錠認証照合データ登録処理を終了する。一方ステップＳ２０１において管理パソコン１９側での照合データ消去が確認できない場合は、ステップＳ１９９に戻って管理パソコン１９への消去信号送信からやり直す。
【０１４５】
以上のように、管理パソコン１９から受信した認証照合データを認証照合データ保持部１４に本登録することと管理パソコン１９で用済みの認証照合データを消去することとはワンセットになっており、マンション入口ロック制御システム側で取得した認証照合データがそのまま残ってプライバシー侵害に悪用されることがないよう配慮している。このことは言い換えれば、管理パソコン１９から受信した認証照合データが認証照合データ保持部１４に確実に本登録しない限り、マンション入口ロック制御システム側で取得した認証照合データの消去はしないということを意味する。
なお、ステップＳ１９７で、マンション入口の開錠のための照合データの新規登録が管理パソコンによって要求されていなければ、直ちに開錠認証照合データ登録処理を終了する。
【０１４６】
なお、図１５のフローでは、まず玄関ドア照合データの新規登録であるかどうかを問い、その後、マンション入口照合データの新規登録であるかどうかを問うているが、この順序は逆でもよい。つまり、ステップＳ１９７からステップＳ２０２のフローをステップＳ１９１の前においてもよい。

【０１４７】
図１におけるユーザ認証センサ１８のための認証照合データを登録する際の制御部１２のフローは、図１５のステップＳ１９１から１９６と同様である。但し、ステップＳ１９１で「玄関ドア」とあるのを「ユーザ認証」と読替え、ステップＳ１９３において「家庭用開錠認証センサ」とあるのを「ユーザ認証センサ」と読替える。
また図１４の実施例２における携帯電話１０１の認証照合データ保持部１０７に認証照合データを登録する際の制御部１０６の動作フローは、上記のような読替えを行った場合の図１５のフローと同じである。
【０１４８】
図１６は、図９のステップＳ１１０における開錠認証照合データ登録処理の詳細を示すフローチャートである。フローがスタートすると、ステップＳ２１１において、業務用開錠認証センサ２１からのセンサ出力の受信を待つ。この出力は、照合データ作成のために本人確認された個人の指を業務用開錠認証センサ２１に挿入することによって行われる。センサ出力の受信があればステップＳ２１２に進み、センサ出力に基づく照合データを管理パソコンで保持する。
次にステップＳ２１３に進み、業務用開錠認証センサ２１に再び指を挿入して同一である旨の照合が正常に行われるかどうかの確認を行う。ステップＳ２１３でこのような正常動作の確認ができればステップＳ２１４に進み、ステップＳ２１２で保持しておいた照合データをAパソコン５に送信する。一方正常動作の確認ができなければ、ステップＳ２１１に戻り、指を挿入し直して再度業務用開錠認証センサ２１からのセンサ出力を受信し照合データの保持をやり直す。
【０１４９】
ステップＳ２１４において照合データを送信するとステップＳ２１５に移行し、管理パソコン側の照合データを消去せよとの旨の信号がAパソコン５から受信されたかどうかをチェックする。この信号の受信は、Aパソコンが照合データを正しく受信したことの確認の意味も持つ。
ステップＳ２１５で消去信号を受信するとステップＳ２１６に進み、管理パソコン１９に保持していた照合データを消去するとともに、ステップＳ２１７で消去確認信号をAパソコン５に送信し、認証照合データ登録処理を終了する。一方、ステップＳ２１５で消去信号が受信できない場合、ステップＳ２１４に戻ってAパソコン５への照合データ送信からやり直す。
【０１５０】
以上のように、マンション入口ロック制御システムにおける照合データの登録にあたっては、個人のプライバシーを保護するため、最終的な認証照合データの保持はA居室２に任せる。しかしながら、その登録行為については管理を行い、個別に勝手な登録が行われてマンション入口ロックのセキュリティが損なわれるのを防止する。
なお、玄関ドアの開錠管理のために認証照合データの登録を行う場合は、家庭用開錠認証センサ１３によって取得した認証照合データがA居室２の外に出ることはないので、その登録処理は簡便となっている。
【０１５１】
図１４の実施例２における携帯電話１０１の認証照合データ保持部１０７に認証照合データを登録する際の管理パソコン１９の動作フローは、図１６と同様である。但し、上記の説明で「Aパソコン５」とあるのを「携帯電話１０１」と読替える。
【０１５２】
以上、図１５、図１６では、マンション入口ロック制御システム８用の認証照合データの登録は業務用開錠認証センサ２１によって取得されたデータによって行っている。しかしながら、開錠認証の機能について業務用開錠認証センサ２１が家庭用開錠認証センサ１３またはユーザ認証センサ１１１など共通の場合は、家庭用開錠認証センサ１３またはユーザ認証センサ１１１によって取得されたデータに基づいてマンション入口ロック制御システム８用の認証照合データの登録を行うよう構成してもよい。

但し、この場合は偽造を防ぐため、マンション入口ロック制御システム８との間で暗号キーをやり取りするなど、マンション入口ロック制御システム８における管理パソコン１９の厳しい管理下でしか登録ができないようにする。

【実施例３】

【０１５３】

図１７は、本発明の生体認証兼健康管理システムの実施例３に関するフローチャートである。実施例３のブロック図は図１と同様なので説明に当たってはこれを流用する。但し、Ａパソコン５および管理パソコン１９の機能が異なっている。具体的には、実施例１では開錠認証の照合をAパソコン５側で行い、照合結果に基づいてドアロック開錠信号を管理パソコン１９に送信していた。これに対し、実施例３では、認証照合データをAパソコン５側から受け取った管理パソコン１９自体で開錠認証の照合を行う。以下図１７および図１８に基づいて、その機能の詳細を説明する。

【０１５４】

実施例３のAパソコン５における制御部１２は、マンション入口ロック制御システム８の制御にあたり、図７ではなく、図１７のフローチャートに従って機能する。

マンション入口にの前に人が立ったことを管理パソコン１９が検出し、この通知を受けたAパソコン５に認証トリガーがかかると図１７のフローがスタートし、ステップＳ２２１において、まず玄関ドアの前に人が立ってから所定時間経過したかどうかのチェックをおこなう。所定時間経過していなければステップＳ２２２に進み、業務用開錠認証センサ２１への指の挿入が行われたがどうかをチェックする。指の挿入がなければステップＳ２２１に戻り、以下、所定時間が経過するまで指の挿入を待つ。

【０１５５】

ステップＳ２２２において指の挿入があるとステップＳ２２３に進み、認証照合データ保持部１４に保持されている開錠認証照合データのいずれかと一致するかどうかがチェックされる。この一致確認は、受信した指データがA居室２の住人のものかどうかを確認するためであり、マンション入口のロック開錠のためではない。ステップＳ２２３で認証照合データとの一致があればステップＳ２２４に進み、管理パソコン１９に認証照合データを送信する。以下、マンション入口のロック開錠制御は管理パソコン１９に任される。

以上のように、ステップＳ２２２における指データの受信のチェックは、生体認証の際に認証照合データ保持部１４に保持されている開錠認証照合データを管理パソコン１９に送信する旨の要求の検知の意味を持っている。

なお、ステップＳ２２４における開錠認証照合データの送信では、これがAパソコンから送られたことを伏せる処置をとり、管理パソコン１９側ではどこから開錠認証照合データが送られたかわからないようにする。

【０１５６】

次いでステップＳ２２５に進み、業務用開錠認証センサ１９が健康管理データ取得に成功したかどうか、換言すれば、管理パソコンから受信した指データが健康管理データとして充分かどうかがチェックされる。成功しない場合とは、管理パソコン１９から受信した指データが開錠照合には充分であるが、健康管理データとするには不十分である場合である。

ステップＳ２２５で健康管理データ取得が成功したことが確認されるとステップＳ２２６に進み、取得したデータを個人健康データベース１５に蓄積する。個人健康データベース１５に蓄積されたデータは医療機関９との契約により、ステップＳ２２６の段階でリアルタイムに大型コンピュータ２２にも送信され、総合健康データベースに２７にも蓄積される。これによって、個人健康データベースの内容がバックアップされるとともに、引越し等への対応も可能となる。

【０１５７】

また、このような個人健康データベース１５のデータをリアルタイムで医療機関９に送信する契約は、例えば独居老人のケアシステムとしても機能する。健康管理データの取得はドアの出入りと連動して自動的に行われるので、健康データベース１５の情報が医療機

関９に何も送信されない日が続くということは、その期間ドアの出入りがなかったことを意味する。従って、このような場合、独居老人になんらかの事故があったと考えられるので医療機関９は即座にその対応をとる。

【０１５８】

次いで、ステップＳ２２７において、健康照合データ保持部１６に照合データがあるかどうかをチェックし、データがあればステップＳ２２８に進んで、取得したデータとの照合処理を行う。そしてステップＳ２２９に進み、照合の結果健康管理データに異常があるかどうかをチェックする。異常があればステップＳ２３０に進み、テレビ１７のスイッチを入れたとき自動的に「健康異常」の警告が行われるよう準備し、ステップＳ２３１に進む。ステップＳ２２９において異常がなければ、直接ステップＳ２３１に進む。

【０１５９】

ステップＳ２３１では、ステップＳ２２８の照合結果を個人健康データベースに蓄積する。個人健康データベース１５に蓄積された照合結果のデータについても、医療機関９との契約により、ステップＳ２３１の段階でリアルタイムに大型コンピュータ２２に送信され、総合健康データベースに２７にも蓄積される。ステップＳ２２９で異常を検出した旨の情報も同時に大型コンピュータ２２に送信され、総合健康データベースに２７に蓄積される。

以上の処理を経てステップＳ２３２に至り、玄関ドアの前に人が立ってから所定時間経過したかどうかのチェックを再度行い、所定時間経過していればステップＳ２３３に進む。ステップＳ２３２の意味は図７のステップＳ７２と同様である。

なお、ステップＳ２２７において、健康照合データ保持部１６に照合データがなければ、照合関連の処理は不要なので、直接ステップＳ２３２に進む。

ステップＳ２３３では、ステップＳ２２４で管理パソコン１９に送信した開錠認証照合データを消去した旨の管理パソコン１９からの報告を待ち、報告があればマンション入口開錠処理を終了する。ステップＳ２３３の意味は管理パソコン１９に開錠認証照合データが残り、プライバシーが侵害されるのを防止することにある。

【０１６０】

一方、ステップＳ２２５において、健康管理データの取得に失敗した場合は、ステップＳ２３４においてデータ取得失敗の旨の表示およびステップＳ２３５においてその理由の表示をし、ステップＳ２３２に至る。

また、ステップＳ２２１において、ドアの前に人が立ってから指を挿入しないまま所定時間が経過した場合は直ちにマンション入口開錠処理を終了する。

【０１６１】

さらに、ステップＳ２２３において開錠認証照合データが認証照合データ保持部１４に保持されている開錠認証照合データのいずれかと一致しない場合は、受信した指データがA居室２の住人のものではないので、直ちにマンション入口開錠処理を終了する。換言すれば、指データは赤の他人のものなので、当然ながらステップＳ２２５以降の健康管理データとしての取り扱いは行わない。また、マンション入口開錠そのものは管理パソコン１９に任されるので、開錠認証照合データ不一致の旨を管理パソコン１９に通知することもない。

【０１６２】

実施例３の管理パソコン１９における制御部５３（図３参照）は、マンション入口ロック制御システム８の制御にあたり、図１０ではなく、図１８のフローチャートに従って機能する。

図１８において、マンション入口にの前に人が立ったことを管理パソコン１９が検出し、認証トリガーがかかるとフローがスタートし、ステップＳ２４１において、まずマンション入口の前に人が立ってから所定時間経過したかどうかのチェックをおこなう。所定時間経過していなければステップＳ２４２に進み、業務用開錠認証センサ２１への指の挿入が行われたがどうかをチェックする。指の挿入がなければステップＳ２４１に戻り、以下、所定時間が経過するまで指の挿入を待つ。

【０１６３】
ステップＳ２４２において指の挿入があって生体情報が取得できるとステップＳ２４３に進み、マンション入口ロック制御システムに加入している全居室に取得データを送信する。次いで、ステップＳ２４４において、いずれかの居室から開錠認証照合データを受信したかどうかチェックする。いずれかの居室から開錠認証照合データを受信すればステップＳ２４５に進む。
【０１６４】
実施例３では開錠認証の照合は管理パソコン１９側で行うので、ステップＳ２４５では、ステップＳ２４４で受信した開錠認証照合データと業務用開錠認証センサ２１が取得した指データとの照合を行い両者が一致するかどうかをチェックする。そして、両者が一致していればステップＳ２４６に進む。
【０１６５】
ステップＳ２４６では、いずれかの居室から健康管理データ取得失敗の旨の通知が入信されたかどうかチェックする。
ステップＳ２４６で健康管理データ取得失敗の旨の通知がいずれの居室からも受信されないことが確認されるとステップＳ２４７に進み、入口ロック２０に開錠を指示する。入口ロック２０はその指示に応じて開錠を実行する。
以上のステップＳ２４４およびステップＳ２４６における居室から管理パソコンへの開錠認証照合データの送信および健康管理データ所得失敗の送信においては、これらの送信がいずれの居室から行われたか管理パソコン１９側ではわからないようにし、プライバシー保護に配慮する。
【０１６６】
入口ロック２０開錠指示後、ステップＳ２４８に進み、ステップＳ２４２で取得した生体情報を消去する。これは、プライバシー保護の万全を期するためである。その後ステップＳ２４９に進み、再度マンション入口の前に人が立ってから所定時間経過したかどうかのチェックをおこなう。所定時間が経過していれば、ステップＳ２５０に進み、ステップＳ２４４で居室のいずれかから受信した開錠認証照合データを消去するとともに、その旨全居室に報告してマンション入口開錠処理を終了する。
【０１６７】
一方、ステップＳ２４６において、健康管理データの取得に失敗した旨の通知を受信したことが確認された場合は、ステップＳ２５１においてデータ取得失敗の旨の表示を行うとともに、ステップＳ２５２においてその理由の表示をし、ステップＳ２４７に至る。このように、健康管理データの取得に失敗した場合であっても、ステップＳ２４５で開錠印象照合結果が一致していれば、入口ロック開錠の指示を行う。
【０１６８】
ステップＳ２４１において、ドアの前に人が立ってから指を挿入しないまま所定時間が経過した場合はステップＳ２５３に移行し、入館拒否表示を行う。次いで、ステップＳ２５４において指が挿入されていない旨の拒否理由の表示を行った後、ステップＳ２５５に進む。
ステップＳ２５５では暗証番号入力やＩＣカード挿入などを行う補助認証を可能とし、補助認証が成功すればステップＳ２４７に移行して入口ロック開錠を指示する。補助認証が行われないかまたは補助認証が失敗したときは、ステップＳ２４８からステップＳ２５０を経て開錠処理を終了するので、入口ロック２０の開錠は行われない。なおこの場合、元々消去すべき生体情報の取得がないのでステップＳ２４８では実質的になにもしないのと同様の処理となるが、次にのべる事情および想定外の事故に対応して確実に消去を実行し、プライバシーを保護するため、ステップＳ２４８をこの位置に置いている。
【０１６９】
生体情報を得ている場合であって、ステップＳ２４４においていずれの居室からも開錠認証照合データを受信しない場合も、ステップＳ２５３に移行し、入館拒否表示を行とともに、ステップＳ２５４において入室拒否表示の理由表示を行う。

同様に、ステップＳ２４５において開錠認証照合データの照合結果が一致しない場合も、ステップＳ２５３に移行し、入館拒否表示を行とともに、ステップＳ２５４において入室拒否表示の理由表示を行う。

これらの場合も、その後、ステップＳ２５５に進み、暗証番号入力やＩＣカード挿入などを行う補助認証を可能とし、補助認証が成功すればステップＳ２４７に移行してドアロックの開錠を指示する。補助認証が行われないかまたは補助認証が失敗したときは、ステップＳ２４８に進み、ステップＳ２４２で取得した生体情報を消去する。このように、認証ができなかった場合であっても取得した生体情報は消去し、プライバシーの保護を万全とする。

この場合、次のステップＳ２４９に進んで所定時間が経過していなければステップＳ２４１を経てステップＳ２４２に戻るので、指の挿入が不適切であった場合、ステップＳ２５４の理由表示を参考に指の挿入をやり直せばステップＳ２４３からステップＳ２４３に進むことも可能となる。

【０１７０】

以上、いずれの場合であっても、ステップＳ２４９を経由してステップＳ２５０に至るが、ステップＳ２４１またはステップＳ２４４を経由してステップＳ２５３に至っていた場合は受信した開錠認証照合データはないので、ステップＳ２５０では実質的に何も行われないのと等しい結果となる。しかし、プライバシー保護は重要な問題なので、想定外の事故にも備えるため、いずれの場合もマンション入口開錠処理を終了する前に必ず開錠認証照合データを消去するステップを通るようにしている。

【実施例４】

【０１７１】

実施例４は、図１４の携帯電話１０１を利用した実施例において、実施例３のように、管理パソコン１９側で開錠認証の照合を行うよう構成したものである。実施例４のブロック図は図１４と同様であるのでこれを流用する。また、携帯電話１０１における制御部１０６の機能および管理パソコン１９における制御部５３の機能は、それぞれ図１７および図１８とほぼ共通なのでこれを流用するとともに大半の説明は省略し、異なっている部分のみコメントする。

【０１７２】

実施例４では、図１７のステップＳ２２３を省略することが可能である。つまり、実施例３では送信されてくる指データが他の居室に居住する無関係の人のものである可能性があり、その場合は開錠認証照合データを送信する必要がないので、ステップＳ２２３でその確認を行っていた。これに対し、実施例４の場合、管理パソコン１９から携帯電話１０１に送信される指データは現にマンション入口に立って業務用開錠認証センサに指を入れた本人のものなので、すぐステップＳ２２４に移行して開錠人諸照合データを送信してよいからである。

また、実施例４では、実施例２と同様、図１７のステップＳ２３０におけるテレビ警告準備の代わりに、携帯電話１０１の表示部１１０での警告の準備を行う。これによって、その後表示部１１０がオンとなったとき自動的に「健康異常」の警告が行われる。

【０１７３】

図１８の管理パソコンのフローにおいても、実施例４では、実施例２と同様、ステップＳ２４３における全居室への取得データ送信の代わりに、携帯電話１０１のＣ近距離無線通信部１０５へのデータ送信を行う。

さらに、ステップＳ２４２とステップＳ２４３の間に「健康管理データ供給契約ユーザ？」を問うステップを挿入し、契約ユーザのときにステップＳ２４３に進むとともに、契約ユーザでなければ「開錠認証照合データ送信要求」のステップを経てステップＳ２４４に進むようにする。このように実施例４の場合、管理パソコン１９は相手の携帯電話との契約に従って指データを送信するかどうかの決定を行う。

なお、健康管理データ供給契約ユーザでない携帯電話における処理は非常に簡単なので、図１７を流用して異なる点のみコメントする。まず、ステップＳ２２２は「開錠認証照

合データ送信要求？」と読代える。そして、ステップＳ２２３、ステップＳ２２５からステップＳ２３１、ステップＳ２３４、およびステップＳ２３５を省略する。つまり、契約ユーザでない携帯電話では、開錠認証照合データの送信とその消去報告の確認のみが行われる。

【０１７４】

次に、センサチェック処理の詳細について説明する。これは、上記の実施例１から実施例４まで共通なので、実施例１を例にとって説明する。

図１９は図４のステップＳ１２におけるセンサチェック処理の詳細を示すものであり、フローがスタートするとステップＳ２６１で、家庭用開錠認証センサ１３に変更があったかどうかをチェックする。変更があった場合、ステップＳ２６２に進み、まず、家庭用開錠認証センサ１３に指が挿入されていない状態での出力信号を取得する。次いでステップＳ２６３でテスト的に指が挿入されるのを待ち、指挿入があってその状態での信号が取得されるとステップＳ２６４に進む。

ステップＳ２６４では、基本信号に異常がないかどうかをチェックしており、具体的には、指を入れない状態での出力をベースにしたときに指を入れた状態で所定の出力が得られるかをチェックする。もし異常があればステップＳ２６５において基本調整処理を行い、ステップＳ２６６に移行する。異常がなければ直接ステップＳ２６６に移行する。

【０１７５】

ステップＳ２６６ではクロスチェック信号の送信が行われる。具体的には、共通の生体情報取得項目について、指を入れない状態において家庭用開錠認証センサ１３と業務用開錠認証センサ２１にチェック信号を送り、業務用開錠認証センサ２１の応答信号をベースにしたときに家庭用開錠センサ１３から所定の出力が得られるかをチェックする。もしこのようなクロスチェックの結果に異常があればステップＳ２６８において業務用開錠認証センサ２１を基準に家庭用開錠センサ１３の出力が所定の範囲になるようクロス調整処理を行い、ステップＳ２６９に移行する。異常がなければ直接ステップＳ２６９に移行する。なお、ステップＳ２６１において家庭用開錠認証センサに変更がなければ直接ステップＳ２６９に移行する。

【０１７６】

ステップＳ２６９では、前回の定期チェック後所定時間が経過して定期チェックの時期に来ているかどうかを確認する。なおこの定期チェックは短時間間隔で頻繁に行ってもよい。ステップＳ２６９で定期チェック時期に来ていると判断された場合、ステップＳ２７０で所定の定期チェックを行う。具体的にはステップＳ２６６と同様、指を入れない状態において家庭用開錠認証センサ１３と業務用開錠認証センサ２１にチェック信号を送り、その結果を見る。そして定期チェックの結果に異常があればステップＳ２７１に移行して定期調整処理を行い、ステップＳ２７２に移行する。異常がなければ直接ステップＳ２７２に移行する。なお、ステップＳ２６９においてまだ定期チェック時期ではないと判断された場合も直接ステップＳ２７２に移行する。

【０１７７】

ステップＳ２７２では、ステップＳ２６５、ステップＳ２６８、およびステップＳ２７１において必要に応じ行われた自動調整処理がすべて成功したかどうかを確認し、自動調整処理ができなかった場合はステップＳ２７３に移行してその旨のテレビでの警告を準備する。ステップＳ２７３におけるテレビ警告のやり方は、図７のステップＳ７０と同様なのでこれに関して先に行った説明はステップＳ２７３においても流用することとし、ここでは繰り返さない。

【０１７８】

図９のステップＳ１１１における管理パソコン１９によるセンサチェック処理の詳細は基本的には図１９と同様である。但し、ステップＳ２６６からステップＳ２６８におけるクロスチェックは省略される。因みに、ステップＳ２７０からステップＳ２７１における定期チェックは業務用開錠認証センサ２１のみを対照に実施する。また、ステップＳ２７３のテレビ警告に代え、自動調整処理ができなかったときは管理パソコン１９のモニタで

その旨警告する。
以上のように、業務用開錠認証センサ２１のチェックおよび調整は管理パソコン１９が行い、その結果を信頼することを前提に、Aパソコン５による図１９のステップＳ２６６からステップＳ２６８におけるクロスチェックでは、業務用開錠認証センサ２１を基準に家庭用開錠認証センサ１３のチェックおよび調整を行う。
【０１７９】
次に、蓄積データ照合処理の詳細について説明する。これは、上記の実施例１から実施例４まで共通なので、実施例１を例にとって説明する。
図２０は図８のステップＳ８４における蓄積データ照合処理の詳細を示すものであり、フローがスタートするとステップＳ２８１で、組合せ可能な異種の複数の生体認証センサ情報が蓄積されているかどうかをチェックし、蓄積されていればステップＳ２８２でこれらを組み合わせて照合する準備をしてステップＳ２８３に移行する。組合せ可能な情報が蓄積されていなければ直接ステップＳ２８３に移行する。
組合せ可能な生体認証センサ情報とは例えば、血管センサ情報、眼底センサ情報、声紋センサ情報などであり、あわせて健康管理情報の取得も可能なセンサ情報である。複数の生体認証センサ情報の組合せは、生体認証のエラーを減少させるとともに、より高度の健康管理を実現する意義がある。
【０１８０】
ステップＳ２８３では、それ自身生体認証のための情報は持たないが、生体認証データを取得する生体自身の条件に関する情報が蓄積されているかどうかをチェックし、蓄積されていればステップＳ２８４でこれらを組み合わせて照合する準備をしてステップＳ２８５に移行する。生体条件の情報が蓄積されていなければ直接ステップＳ２８５に移行する。生体認証データを取得する時点での生体条件の情報としては例えば、体温、血圧、脈拍数などの情報がある。
【０１８１】
なお、生体認証データを取得する生体自身の条件に関する情報としては、上記のものの他、次のようなものが有用である。
まず、実施例２の携帯電話１０１のように、本人健康データベース１０９が常に持ち歩かれる場合、携帯電話１０１に歩数計を設ければ、生体認証データを取得する時点での生体自身の条件だけでなく、生体認証データを取得する時点までの運動量の履歴も本人健康データベース１０９に蓄積することができる。このような場合、例えば生体認証データを取得する時点での脈拍数が同じであっても、それが過去一ヶ月間ウオーキングを続けてきた結果なのかそれとも特に運動に努めなかった結果なのかで健康照合データとの照合や健康判断が異なって来る。このように生体認証データを取得する生体自身の条件については、生体自身の運動負荷の履歴などの情報も有用である。
また、生体認証データを取得する生体自身の条件としては、本人だけでなく家族の病歴などに関する情報も有用である。例えば、生体認証データを取得する時点での本人の血圧が同じであっても、親や祖父母などの高血圧病歴がある人とない人では、危険因子が異なり、健康照合データとの照合や健康判断が異なって来るからである。
医療機関９における健康照合データ登録にあたっては、健康照合ソフト２４または医師２５の判断により上記の種々に因子が加味され、このようにして登録された健康照合データがどのようなものであるかによって、要求される照合の仕方も異なってくる。
【０１８２】
ステップＳ２８５では、生体認証データや生体自身の条件を取得する際の外部の条件に関する情報が蓄積されているかどうかをチェックし、蓄積されていればステップＳ２８６でこれらを組み合わせて照合する準備をしてステップＳ２８７に移行する。外部条件の情報が蓄積されていなければ直接ステップＳ２８７に移行する。
外部条件の情報とは図３の外部条件センサ５７によって取得される情報であって、例えば気温、湿度、風速などの気象条件である。
【０１８３】

ステップＳ２８７では、生体認証データ、生体自身の条件、外部条件を取得した時刻の情報が蓄積されているかどうかをチェックする。蓄積されていればステップＳ２８８において異なる日付の同時刻における生体認証データ、生体自身の条件、外部条件を抽出し、同時刻同士の情報を照合する準備をする。特に開錠センサにより健康管理データを取得した場合、出勤時刻などに合わせて規則正しいデータが日々抜けなく蓄積されるのでデータ収集の効率が高い。

さらに、ステップＳ２８９においては、同じ日の時刻情報に基づき、生体認証データ、生体自身の条件、外部条件が朝から昼、そして夜への日周変化に応じてどのように変わるかを照合する。

ステップＳ２８８およびステップＳ２８９の処理を終わると、ステップＳ２９０に移行する。時刻情報が蓄積されていなければ、直接ステップＳ２９０に移行する。

【０１８４】

ステップＳ２９０では、生体認証データ、生体自身の条件、外部条件を取得した日付の情報が所定期間分蓄積されているかどうかをチェックする。蓄積されていればステップＳ２９１において大きな季節変化に応じて生体認証データ、生体自身の条件、外部条件がどのように変化するかを照合する準備をし、ステップＳ２９２に移行する。春夏秋冬の季節の流れの中で生体情報もこれに影響されて変化する可能性があるので、ステップＳ２９１によってその因果関係を把握することが可能となる。日付情報が意味のある照合に充分な期間分蓄積されていなければ、直接ステップＳ２９２に移行する。

【０１８５】

ステップＳ２９２では、生体認証データ、生体自身の条件、外部条件の経時変化を見る場合において、前回の経時変化照合以降、所定の蓄積期間分蓄積されているかどうかチェックする。蓄積されていればステップＳ２９３において生体認証データおよび生体自身の条件の経時変化を照合する準備をし、ステップＳ２９４に移行する。経時変化のチェックは特に変化の早さに意味があり、病状の急変の発見にもつながる意義がある。経時変化を見るのに意味のある期間のデータの蓄積がなければ、直接ステップＳ２９４に移行する。

【０１８６】

ステップＳ２９５では、ステップＳ２８２、ステップＳ２８４、ステップＳ２８６、ステップＳ２８８、ステップＳ２８９、ステップＳ２９１、およびステップＳ２９３における準備に基づき、得られた生体情報同士の照合、対応する健康照合データとの照合、およびそれらの組合せとして実行する。

【０１８７】

図２１は、実施例１から実施例４において共通に実施できる玄関ドアの詳細模式図である。図２１において玄関ドア１０はその断面が図示されており、玄関ドア１０の左側がＡ居室外側、右側がＡ居室内側である。また、玄関ドアに関連するその他の構成は、図１のドアロック１１、家庭用開錠認証センサ１３、および入室拒否、健康データ取得失敗などの報知部にほぼ対応している。

各構成を具体的に説明すると、まず、玄関ドア１０の外側には電子ペーパーなどからなる電子表札２０１が配置されている。この電子表札２０１は、通常は表札を表示しているが、玄関ドア１０の内側に配置された回路部２０２を通じたＡパソコン５の制御を受けており、必要に応じ入室拒否表示、健康データ取得失敗表示などを行う報知部を兼ねている。

回路部２０２は、共通光源部２０３および共通受光部２０４とともに家庭用開錠認証センサ１３を構成しており、Ａパソコン５の制御を受ける。また、ノブ／ロック機構２０５は回路部２０２とともにドアロック１１を構成しており、Ａパソコン５の制御を受ける。

なお回路部２０２から出ている各制御ラインは、図２１では模式的に玄関ドアの内側に露出しているように図示しているが、実際には玄関ドア１０の内部に配線される。

【０１８８】

ノブ／ロック機構２０５は、玄関ドア１０の開閉の際に操作するドアノブとロック機構を備えたもので、玄関ドア１０の外側および内側のいずれからも操作可能となっている。

なお、ノブ／ロック機構２０５は、外側からはロックが開錠されない限りドアノブを操作しても玄関ドア１０を開けることができないが、内側からはドアノブを操作すれば玄関ドア１０を開けることができるよう構成される。

共通光源部２０３および共通受光部２０４は玄関ドア１０の外側および内側で生体情報を取得するとることができるように構成されており、ノブ／ロック機構２０５を挟んで配置されている。これによって玄関ドア１０の外側および内側のいずれからノブ／ロック機構２０５を操作する場合でも、その操作に伴って指が自然に共通光源部２０３および共通受光部２０４の間に入り、生体情報が取得できるようになっている。

【０１８９】

そして、玄関ドア１０の外側からノブ／ロック機構２０５を操作した場合、その操作に伴って生体情報が取得され、これが認証されて正当な住人であることが確認されるとドアロックが自動開錠されるので、そのままドアを開けることができる。この一連の処理は高速で行われるので、正当な住人の場合、ノブ／ロック機構２０５の操作により何の抵抗もなく玄関ドア１０が開くような感覚でＡ居室２に入ることができる。

なお、玄関ドア１０の内側からノブ／ロック機構２０５を操作した場合は、生体認証なしにロックが開錠されるので生体認証の必要はないが、玄関ドア１０を出る際にも健康データを取得する目的で、玄関ドア１０の内側でも生体情報を取得することができるように構成している。これは、特に朝の出勤時などに規則正しく健康管理データを取得するためである。

【０１９０】

次に共通光源部２０３と共通受光部２０４の構成の詳細について説明する。共通光源部２０３の光源２０６は玄関ドア１０の内側に配置されており、生体情報取得のための光を内側のドアノブに向けて照射する。一方、光源２０６の光は玄関ドア１０の外側に向けても照射され、これが導光部２０７によって下方に屈曲されて外側のドアノブに向けて照射される。以上の構成によって、玄関ドア１０の外側に光源２０６を配置することなく、生体情報取得のための光を外側のドアノブに向けて照射することができる。

共通光源部２０４のセンサ２０８は玄関ドア１０の内側に配置されており、光源２０６から照射されて内側のドアノブを操作する指を透過した光を受光することができる。一方、導光部２０７から照射されて外側のドアノブを操作する指を透過した光は、導光部２０９に入射するとともに玄関ドア１０の内側に向けて屈曲され、これがセンサ２０８により受光される。以上の構成によって、玄関ドア１０の外側にセンサ２０８を配置することなく、玄関ドア１０の外部で取得された生体情報取得のための光を受光することができる。

【０１９１】

以上の共通光源部２０３および共通受光部２０４の構成は、既に述べたように共通の光源２０６とセンサ２０８によって玄関ドア１０の内側および外側の両方で生体情報を取得することができる利点があるが、他にも利点がある。

つまり、光源２０６とセンサ２０８が回路部２０２とともに玄関ドア１０の内側に設けられる構成は、比較的高価なこれらの部品が、気候の変化やいたずらなどによって外部から損傷をうけることを防止できる利点がある。このように、導光部２０７および導光部２０９は、図３の保護ユニット５２としての意味もある。図３の保護ユニット５２と同様、導光部２０７および導光部２０９も光源２０６やセンサ２０８と独立に交換や調整ができるよう構成される。

なお、生体認証センサにおいて、ドアの外側に露出する部分を極力減らし、構成の主要部をドアの内側に設けることによる上記の利点は、図２１においてドアの内側で生体認証する機能を省略する場合でも同様に享受できるものである。

【０１９２】

生体認証センサは外部環境に曝されるので光源部の光照射口やセンサの受光口に付着する汚れやゴミ、また検出光路を妨害する異物の挿入によって検出が不可能になったり検出性能が劣化したりする問題がある。これに対しては、光照射口、受光口、検出光路の清掃などのメンテナンスで対応する必要がある。

図２１では、生体認証を求める際にノブ／ロック機構２０５を機械的に操作するので、光照射口と受光口に機械的なワイパーを設けておき、ノブ／ロック機構２０５の操作に連動してこれらのワイパーを作動させるようにする。また、検出光路の妨害異物の除去については、ドアノブを操作する指が光路を横切って挿入されるので、指自体によって除去される。

なお、上記のような人力による清掃に代え、ワイパーを定期的に電動で動作させることも可能である。

【実施例５】

【０１９３】

図２２は、実施例5における個人認証データおよび健康管理データのデータ構造図である。実施例１から実施例４においては、個人認証データおよび健康管理データが、健康照合データ保持部、個人または本人健康データベース、認証照合データ保持部などに分かれて保持される姿を示したが、実施例５ではこれらのデータが統一したデータ形式に従って保持される。図２２はそのデータ形式のデータ構造図を示したものであって、実施例１から実施例４は、このような実施例５によるデータ保持のしかたで実施することが可能である。

【０１９４】

実施例５の統一データ形式では、基本的には各データが一つの統合されたデータファイルとして管理される。統一データファイルは図２２に示すように、個人認証データ３０１、健康管理データ３０２、参考条件データ３０３、医療機関管理データ３０４に分かれているが、共通の関連付けコード３０５、３０６、３０７、３０８によって全体的に一つのファイルのように関連付けられている。

【０１９５】

実施例５の統一データ形式では、基本的には各データが一つの統合されたデータファイルにまとめられて管理される。統一データファイルは、図２２に示すように、個人認証データファイル３０１、健康管理データファイル３０２、参考条件データファイル３０３、医療機関管理データファイル３０４に分かれており、必要に応じそれぞれ独立したファイルとして扱うこともできるが、共通の関連付けコード３０５、３０６、３０７、３０８によって通常は全体的に一つのファイルとして扱うことができるよう関連付けられている。ファイル内の各データへのアクセス権は目的に応じ異なっているがそれについては以下で詳述する。

【０１９６】

個人認証データファイル３０１には、氏名、住所、電話番号など個人を特定するための基本データ３０９、性別、生年月日などその他の個人属性が含まれる個人属性データ３１０、各居室の玄関ドア照合データなどのローカル生体認証照合データ３１１、およびマンション入口照合データなどの共用生体認証照合データ３１２などが含まれる。

共用生体認証照合データ３１２以外は使用者本人による登録ができるが、共用生体認証照合データ３１２は、マンション入口ロック制御システム８の管理パソコン１９など共用システムの管理下でしか登録できない。また、ローカル生体認証照合データ３１１、共用生体認証照合データ３１２については医療機関９からのアクセスはできない。

なお、認証照合の際に共用生体認証照合データ３１２がマンション入口ロック制御システム８などに送信されるときは、氏名、住所、電話番号など個人を特定するための基本データ３０９、性別、生年月日などその他の個人属性が含まれる個人属性データ３１０、各居室の玄関ドア照合データなどのローカル生体認証照合データ３１１については一切伏せられ、共用生体認証照合データ３１２が誰のものなのかわからないようにされる。

【０１９７】

健康管理データファイル３０２には、日付時刻つきで取得した健康管理データを格納する日付時刻つき個人健康データベース３１３、データ取得時生体条件データベース３１４データ取得時外部条件データベース、３１５、および照合結果データベース３１６がなど含まれる。

これらの健康管理データに関しては、マンション入口ロック制御システム８などの生体認証を目的とするシステムはアクセスすることができない。なお、本人がこれらのデータを利用するときは、ローカル生体認証照合データ３１１との照合結果が一致した場合のみアクセスが可能となるので、他人が見ることはできない。

【０１９８】

参考条件データファイル３０３には、歩数計によるウオーキング実施状況などの健康維持活動履歴データ３１７、家族病歴データ３１８などが含まれる。

これらのデータも個人の健康管理が目的なので、マンション入口ロック制御システム８などの生体認証を目的とするシステムはアクセスすることができない。これらの参考条件データについても、プライバシーを守るため、本人が利用するときは、ローカル生体認証照合データ３１１との照合結果が一致した場合のみアクセスが可能となる。

【０１９９】

医療機関管理データファイル３０４には、医療機関９の管理下で取り扱うべきデータがまとめられている。医療機関９は生体認証に関するローカル生体認証照合データ３１１や共用生体認証照合データ３１２に関与しないし、本人でもないので、これらのデータによって健康管理データにアクセスすることもできない。従って、本人の了解の下に健康管理用暗証番号３１９を決めておき、これを医療機関管理データファイル３０４に保持させる。従って、医師などが健康管理データにアクセスするときはこの健康管理用暗証番号を入力する。

医療機関管理データファイル３０４には、さらに、医療機関IDコード３２０、健康照合データ３２１、医師診断データが含まれる。これらのデータは医療機関９によって管理され、本人といえども勝手に書き換えることはできない。

また、健康照合データ３２１は登録後Aパソコンや携帯電話に提供されるが、医師診断データ３２２は基本的には告知の問題もあるので所定の手続きを経なければ本人のアクセスはできない。

【図面の簡単な説明】

【０２００】

【図１】生体認証兼健康管理システムのブロック図を示した図面代用写真である。（実施例１）

【図２】血管センサシステムのブロック図を示した図面代用写真である。（実施例１）

【図３】開錠認証センサの詳細構成のブロックを示した図面代用写真である。（実施例１）

【図４】居室内パソコンの基本フローチャートを示した図面代用写真である。（実施例１）

【図５】図４のステップＳ１２の詳細フローチャートを示した図面代用写真である。（実施例１）

【図６】居室ドアにて認証トリガーがかかった場合の居室内パソコンフローチャートを示した図面代用写真である。（実施例１）

【図７】マンション入口にて認証トリガーがかかった場合の居室内パソコンフローチャートを示した図面代用写真である。（実施例１）

【図８】図６のステップＳ４７または図７のステップＳ６８の詳細フローチャートを示した図面代用写真である。（実施例１）

【図９】マンション側管理パソコンの基本フローチャートを示した図面代用写真である。（実施例１）

【図１０】マンション入口にて認証トリガーがかかった場合のマンション側管理パソコンフローチャートを示した図面代用写真である。（実施例１）

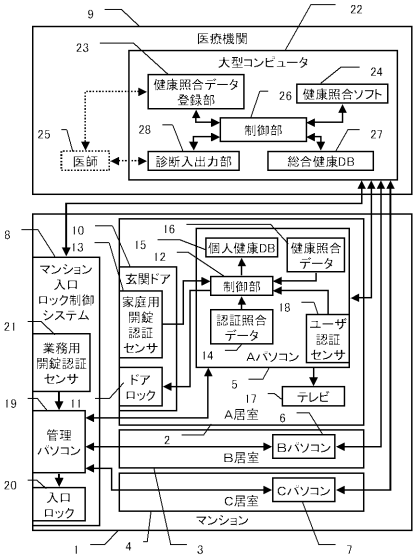
【図１１】医療機関側コンピュータの基本フローチャートを示した図面代用写真である。（実施例１）

【図１２】医療機関側コンピュータの送信処理フローチャートを示した図面代用写真である。（実施例１）

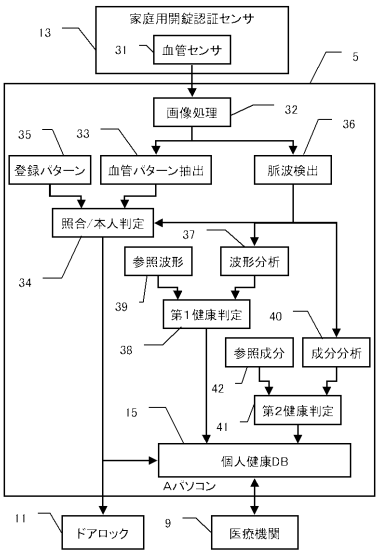
【図１３】図１１のステップＳ１３４の詳細フローチャートを示した図面代用写真である。（実施例１）
【図１４】生体認証兼健康管理システムのブロック図を示した図面代用写真である。（実施例２）
【図１５】図４のステップＳ１１の詳細フローチャートを示した図面代用写真である。（実施例１）
【図１６】図９のステップＳ１１０の詳細フローチャートを示した図面代用写真である。（実施例１）
【図１７】マンション入口にて認証トリガーがかかった場合の居室内パソコンフローチャートを示した図面代用写真である。（実施例３）
【図１８】マンション入口にて認証トリガーがかかった場合のマンション側管理パソコンフローチャートを示した図面代用写真である。（実施例３）
【図１９】図４のステップＳ１２の詳細フローチャートを示した図面代用写真である。（実施例１）
【図２０】図８のステップＳ８４の詳細フローチャートを示した図面代用写真である。（実施例１）
【図２１】玄関ドアの詳細模式図を示した図面代用写真である。（実施例１～４）
【図２２】個人認証データおよび健康管理データのデータ構造図を示した図面代用写真である。（実施例５）
【符号の説明】
【０２０１】

８	第一部分
５、１０１	第二部分
２１	生体情報取得部
２０	利用部
１９	伝達部
１２、１０６	健康管理情報処理部
５，１０１	受領部
１９	決定部
８	共通の入口
１０	個別の入口
２１	第一の生体情報取得部
１３	第二の生体情報取得部
１６、１０９	蓄積部
１４、１０８	健康照合情報保持部

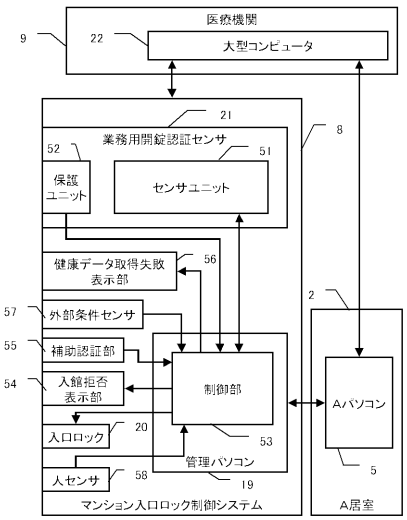
【図１】


医療機関
大型コンピュータ
健康照合データ登録部
健康照合ソフト
制御部
医師
診断入出力部
総合健康DB
マンション入口ロック制御システム
玄関ドア
家庭用開錠認証センサ
業務用開錠認証センサ
ドアロック
管理パソコン
入口ロック
個人健康DB
健康照合データ
制御部
認証照合データ
ユーザ認証センサ
Aパソコン
テレビ
A居室
B居室
Bパソコン
C居室
Cパソコン
マンション

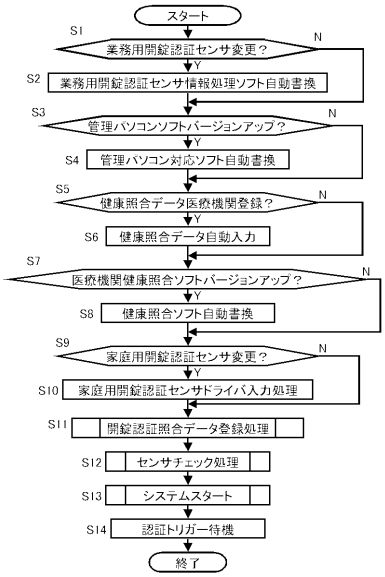
【図２】


家庭用開錠認証センサ
血管センサ
画像処理
登録パターン
血管パターン抽出
脈波検出
照合/本人判定
参照波形
波形分析
第1健康判定
参照成分
成分分析
第2健康判定
個人健康DB
Aパソコン
ドアロック
医療機関

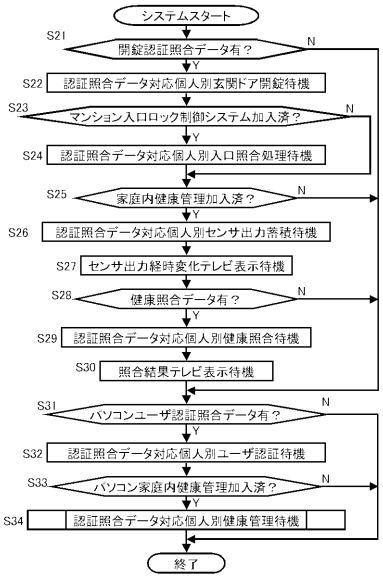
【図３】


医療機関
大型コンピュータ
業務用開錠認証センサ
保護ユニット
センサユニット
健康データ取得失敗表示部
外部条件センサ
補助認証部
入館拒否表示部
入口ロック
人センサ
制御部
管理パソコン
マンション入口ロック制御システム
Aパソコン
A居室

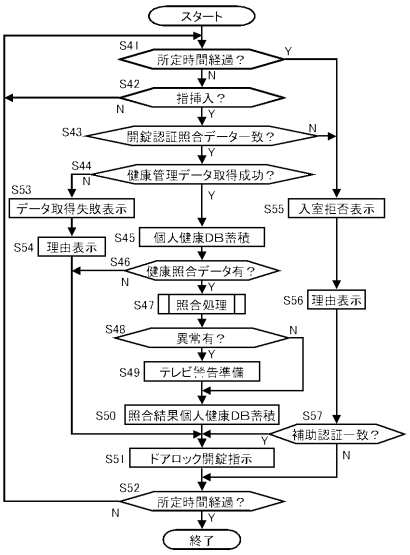
【図４】


スタート
S1
業務用開錠認証センサ変更？
N
Y
S2
業務用開錠認証センサ情報処理ソフト自動書換
S3
管理パソコンソフトバージョンアップ？
S4
管理パソコン対応ソフト自動書換
S5
健康照合データ医療機関登録？
S6
健康照合データ自動入力
S7
医療機関健康照合ソフトバージョンアップ？
S8
健康照合ソフト自動書換
S9
家庭用開錠認証センサ変更？
S10
家庭用開錠認証センサドライバ入力処理
S11
開錠認証照合データ登録処理
S12
センサチェック処理
S13
システムスタート
S14
認証トリガー待機
終了

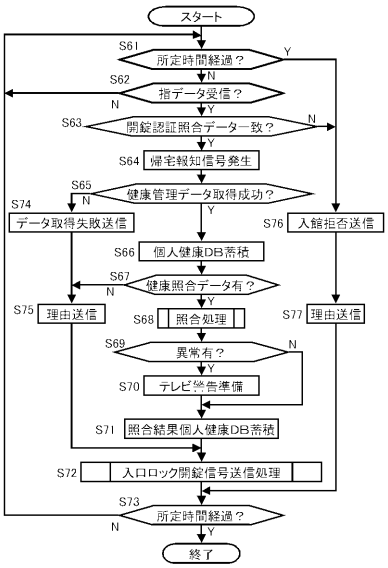
【図５】


システムスタート
S21
開錠認証照合データ有？
N
Y
S22
認証照合データ対応個人別玄関ドア開錠待機
S23
マンション入口ロック制御システム加入済？
N
Y
S24
認証照合データ対応個人別入口照合処理待機
S25
家庭内健康管理加入済？
N
Y
S26
認証照合データ対応個人別センサ出力蓄積待機
S27
センサ出力経時変化テレビ表示待機
S28
健康照合データ有？
N
Y
S29
認証照合データ対応個人別健康照合待機
S30
照合結果テレビ表示待機
S31
パソコンユーザ認証照合データ有？
N
Y
S32
認証照合データ対応個人別ユーザ認証待機
S33
パソコン家庭内健康管理加入済？
N
Y
S34
認証照合データ対応個人別健康管理待機
終了

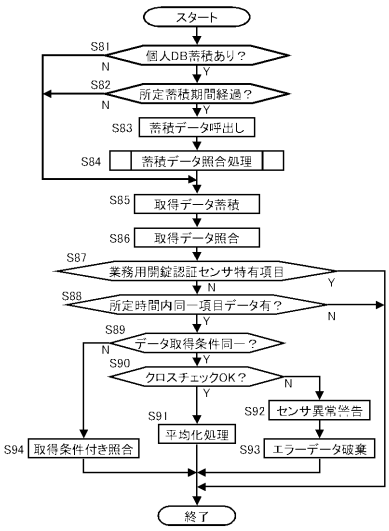
【図６】


スタート
S41
所定時間経過？
Y
N
S42
指挿入？
N
Y
S43
開錠認証照合データ一致？
N
Y
S44
健康管理データ取得成功？
N
Y
S53
データ取得失敗表示
S55
入室拒否表示
S54
理由表示
S45
個人健康DB蓄積
S46
健康照合データ有？
N
Y
S47
照合処理
S56
理由表示
S48
異常有？
N
Y
S49
テレビ警告準備
S50
照合結果個人健康DB蓄積
S57
補助認証一致？
Y
N
S51
ドアロック開錠指示
S52
所定時間経過？
N
Y
終了

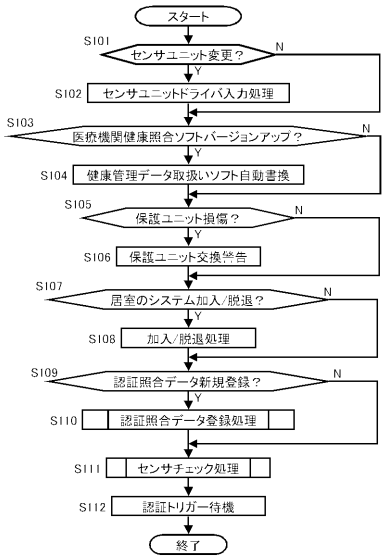
【図７】


スタート
S61
所定時間経過？
Y
N
S62
指データ受信？
N
Y
S63
開錠認証照合データ一致？
N
Y
S64
帰宅報知信号発生
S65
健康管理データ取得成功？
N
Y
S74
データ取得失敗送信
S76
入館拒否送信
S66
個人健康DB蓄積
S67
健康照合データ有？
N
Y
S75
理由送信
S68
照合処理
S77
理由送信
S69
異常有？
N
Y
S70
テレビ警告準備
S71
照合結果個人健康DB蓄積
S72
入口ロック開錠信号送信処理
S73
所定時間経過？
N
Y
終了

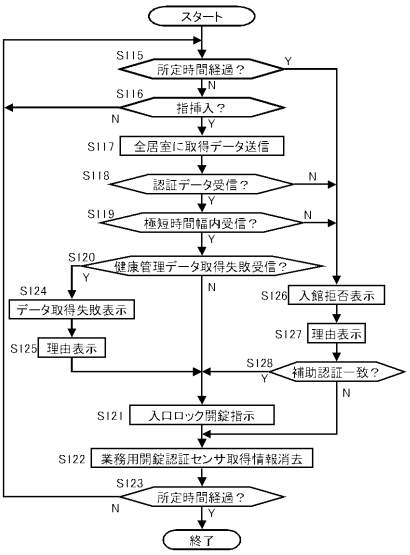
【図８】


スタート
S81
個人DB蓄積あり？
N
Y
S82
所定蓄積期間経過？
N
Y
S83
蓄積データ呼出し
S84
蓄積データ照合処理
S85
取得データ蓄積
S86
取得データ照合
S87
業務用開錠認証センサ特有項目
Y
N
S88
所定時間内同一項目データ有？
N
Y
S89
データ取得条件同一？
N
Y
S90
クロスチェックOK？
N
Y
S91
平均化処理
S92
センサ異常警告
S94
取得条件付き照合
S93
エラーデータ破棄
終了

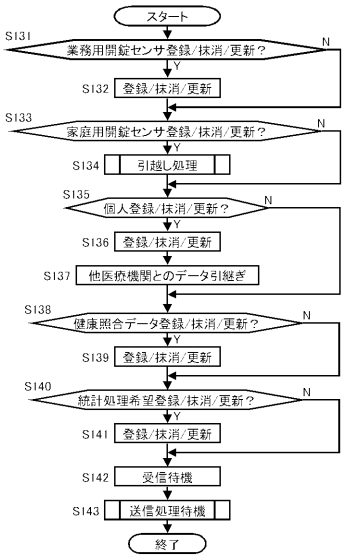
【図９】



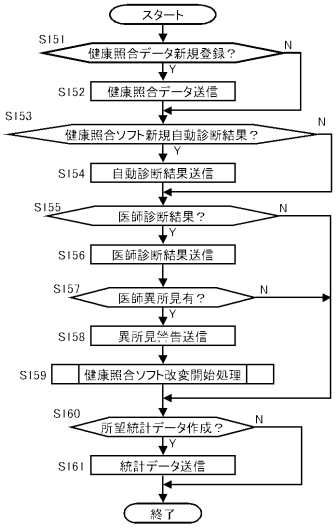
【図１０】



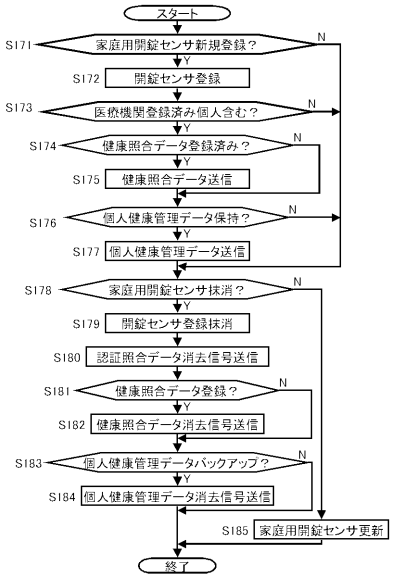
【図１１】



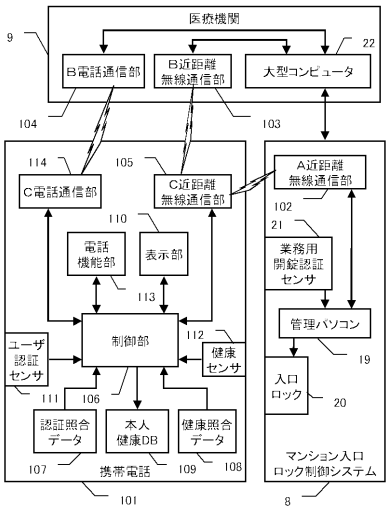
【図１２】



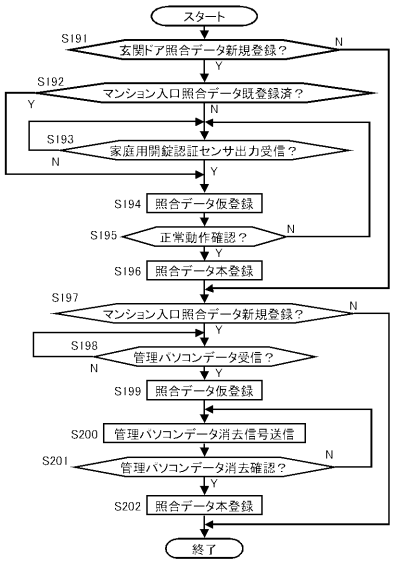
【図１３】



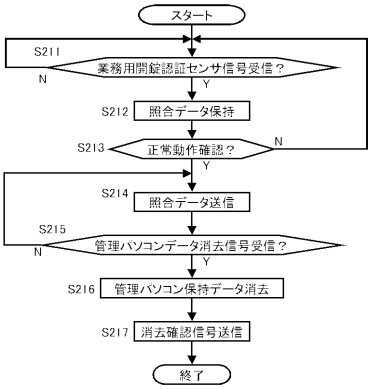
【図１４】



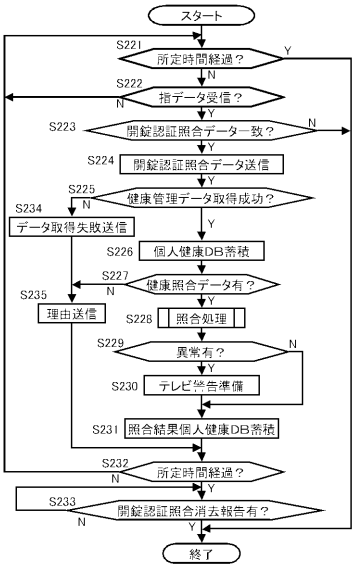
【図１５】



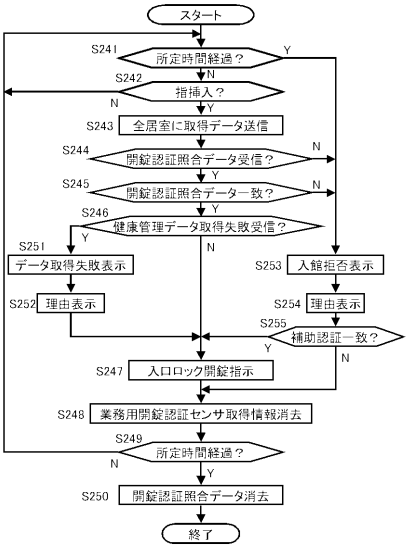
【図１６】



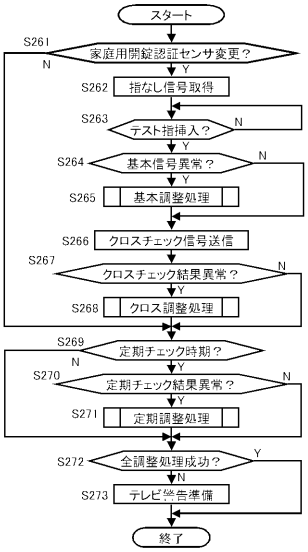
【図１７】



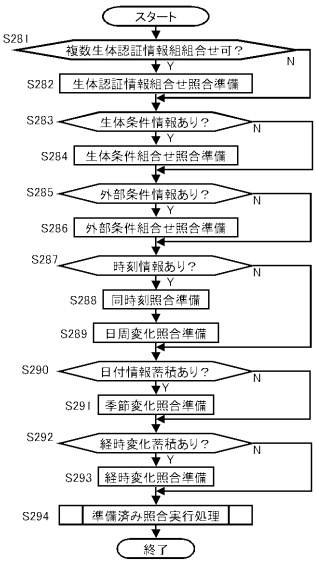
【図１８】



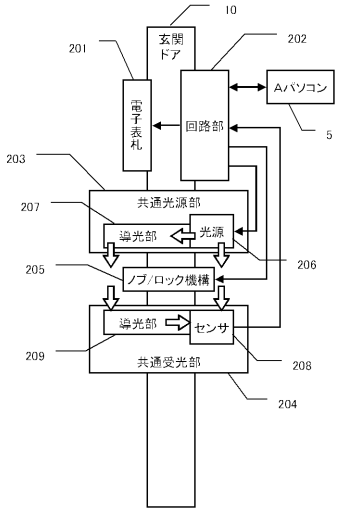
【図１９】



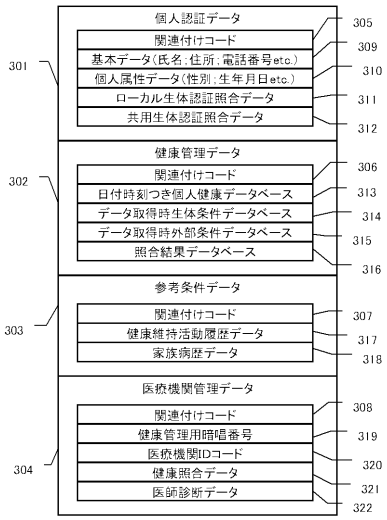
【図２０】



【図２１】


10
玄関ドア
201
202
Aパソコン
5
電子表札
回路部
203
共通光源部
207
導光部
光源
206
205
ノブ/ロック機構
導光部
センサ
209
208
共通受光部
204

【図２２】


個人認証データ
関連付けコード
基本データ(氏名;住所;電話番号etc.)
個人属性データ(性別;生年月日etc.)
ローカル生体認証照合データ
共用生体認証照合データ
301
305
309
310
311
312
健康管理データ
関連付けコード
日付時刻つき個人健康データベース
データ取得時生体条件データベース
データ取得時外部条件データベース
照合結果データベース
302
306
313
314
315
316
参考条件データ
関連付けコード
健康維持活動履歴データ
家族病歴データ
303
307
317
318
医療機関管理データ
関連付けコード
健康管理用暗唱番号
医療機関IDコード
健康照合データ
医師診断データ
304
308
319
320
321
322

フロントページの続き

(56)参考文献 特開２００４－３４４３７５（ＪＰ，Ａ）
特開２００２－０８３０５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ａ６１Ｂ　　５／１１７
Ａ６１Ｂ　　５／００
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩ）