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

特許第4727065号
(P4727065)

(45)発行日　平成23年7月20日(2011.7.20)　(24)登録日　平成23年4月22日(2011.4.22)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330F
G06F 1/00	(2006.01)	G06F	1/00	370E
H04L 9/32	(2006.01)	H04L	9/00	673D

請求項の数 17　(全 24 頁)

(21)出願番号　特願2001-139024(P2001-139024)
(22)出願日　平成13年5月9日(2001.5.9)
(65)公開番号　特開2002-32343(P2002-32343A)
(43)公開日　平成14年1月31日(2002.1.31)
審査請求日　平成20年3月3日(2008.3.3)
(31)優先権主張番号　特願2000-138095(P2000-138095)
(32)優先日　平成12年5月11日(2000.5.11)
(33)優先権主張国　日本国(JP)

(73)特許権者　000153878
株式会社半導体エネルギー研究所
神奈川県厚木市長谷３９８番地
(72)発明者　山崎　舜平
神奈川県厚木市長谷３９８番地　株式会社半導体エネルギー研究所内
(72)発明者　小山　潤
神奈川県厚木市長谷３９８番地　株式会社半導体エネルギー研究所内

審査官　深沢　正志

最終頁に続く

(54)【発明の名称】認証装置および通信システム

(57)【特許請求の範囲】

【請求項１】

使用者の識別を行う認証装置であって、

基準用生体情報を記憶する手段と、

前記使用者の照会用生体情報を読み取る手段と、

前記照会用生体情報を、前記基準用生体情報と照合する手段と、

前記照合が合致した場合、合致した旨をデータとして送信する手段と、

前記データの送信によって通信が許可された後でパスワードを送信し、前記パスワードによって、前記基準用生体情報の書き換えが許可された場合に、前記記憶する手段に記憶された前記基準用生体情報の書き換えを行う手段とを有することを特長とする認証装置。

【請求項２】

使用者の識別を行う認証装置であって、

ｎ（ｎは自然数）個の基準用生体情報を記憶する手段と、

前記使用者のｎ個の照会用生体情報を読み取る手段と、

前記ｎ個の照会用生体情報を、前記ｎ個の基準用生体情報と照合する手段と、

前記照合において、前記ｎ個の照会用生体情報の少なくとも一と、前記ｎ個の基準用生体情報の少なくとも一とが合致した場合、合致した旨をデータとして送信する手段と、

前記データの送信によって通信が許可された後でパスワードを送信し、前記パスワードによって、前記ｎ個の基準用生体情報の書き換えが許可された場合に、前記記憶する手段に記憶された前記ｎ個の基準用生体情報の少なくとも一の書き換えを行う手段とを有する

ことを特長とする認証装置。
【請求項３】
使用者の識別を行う認証装置であって、
ｎ（ｎは自然数）個の基準用生体情報を記憶する手段と、
前記使用者のｍ（ｍは自然数）個の照会用生体情報を読み取る手段と、
前記ｍ個の照会用生体情報を、前記ｎ個の基準用生体情報と照合する手段と、
前記照合において、前記ｍ個の照会用生体情報の少なくとも一と、前記ｎ個の基準用生体情報の少なくとも一とが合致した場合、合致した旨をデータとして送信する手段と、
前記データの送信によって通信が許可された後でパスワードを送信し、前記パスワードによって、前記ｎ個の基準用生体情報の書き換えが許可された場合に、前記記憶する手段に記憶された前記ｎ個の基準用生体情報の少なくとも一の書き換えを行う手段とを有することを特長とする認証装置。
【請求項４】
使用者の識別を行う認証装置であって、
ｎ（ｎは自然数）個の、複数の種類の基準用生体情報を記憶する手段と、
前記使用者のｍ（ｍは自然数）個の、複数の種類の照会用生体情報を読み取る手段と、
前記ｍ個の、複数の種類の照会用生体情報を、前記ｎ個の、複数の種類の基準用生体情報と照合する手段と、
前記照合において、前記複数の種類の内、各種類の照会用生体情報の少なくとも一と、前記複数の種類の内、各種類の基準用生体情報の少なくとも一とが合致した場合、合致した旨をデータとして送信する手段と、
前記データの送信によって通信が許可された後でパスワードを送信し、前記パスワードによって、前記ｎ個の、複数の種類の基準用生体情報の書き換えが許可された場合に、前記記憶する手段に記憶された前記ｎ個の、複数の種類の基準用生体情報の少なくとも一の書き換えを行う手段とを有することを特長とする認証装置。
【請求項５】
請求項１乃至請求項４のいずれか一において、
前記基準用生体情報とは、指紋、掌紋、または声紋であることを特長とする認証装置。
【請求項６】
請求項１乃至請求項５のいずれか一において、
前記照会用生体情報とは、指紋、掌紋、または声紋であることを特長とする認証装置。
【請求項７】
請求項５または請求項６において、
前記掌紋とは、手のひらの全体の掌紋、または前記手のひらの一部の掌紋であることを特長とする認証装置。
【請求項８】
請求項１乃至請求項７のいずれか一において、
前記記憶する手段とは、フラッシュメモリであることを特長とする認証装置。
【請求項９】
請求項１乃至請求項８のいずれか一において、
前記読み取る手段とは、フォトダイオード、ＣＣＤ、またはマイクであることを特長とする認証装置。
【請求項１０】
請求項１乃至請求項９に記載の認証装置と、前記パスワードの入力用のキーとを有することを特長とする携帯情報端末。
【請求項１１】
請求項１乃至請求項９のいずれか一に記載の認証装置と、前記パスワードの入力用のキーとを有することを特長とする携帯電話。
【請求項１２】
請求項１乃至請求項９のいずれか一に記載の認証装置と、前記パスワードの入力用のキ

ーボードとを有することを特長とするパーソナルコンピュータ。
【請求項１３】
請求項１乃至請求項１２のいずれか一において、
前記データが相手先によって受信された後、前記認証装置と前記相手先との間で直接通信が開始されることを特長とする通信システム。
【請求項１４】
請求項１乃至請求項１２のいずれか一において、
前記データが管理者によって受信された後、前記管理者を間に介して前記認証装置と相手先との間で通信が開始されることを特長とする通信システム。
【請求項１５】
請求項１乃至請求項１２のいずれか一において、
前記データが管理者によって受信された後、前記管理者は、前記照合が合致した旨をデータとして相手先に送信し、前記管理者を間に介して前記認証装置と前記相手先との間で通信が開始されることを特長とする通信システム。
【請求項１６】
請求項１乃至請求項１２のいずれか一において、
前記データが管理者によって受信された後、前記管理者は、前記照合が合致した旨をデータとして相手先に送信し、前記認証装置と前記相手先との間で直接通信が開始されることを特長とする通信システム。
【請求項１７】
請求項１乃至請求項１６のいずれか一において、
前記認証装置と相手先との間で取引が行われ、前記使用者の識別は、前記相手先において設定された条件を満たす場合に限定して要求されることを特長とする通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は通信システムに関する。特に、生体情報を用いて認証を行うことを特徴とした通信システムである。
【０００２】
【従来の技術】
近年、携帯電話、パソコン、携帯情報端末などの認証装置を使用してインターネットに接続する通信技術が急速に発展しつつある。企業、家庭でのインターネット等への接続は、据え置き型のパソコンに電話回線を接続することで行われている。特に近年では、インターネットが簡単に出来るiモードなどの携帯電話が普及し、さまざまな情報交換が簡便に行われるようになった。
【０００３】
さらに近頃では、居ながらにして取引を成立させることが可能であるという利便性の面から、インターネット等の通信網を用いた通信販売や株取引などが注目をあびている。しかし認証装置を用いて相手先と取引を行う場合、通信を行っている相手が本人であることの確認（認証作業）が難しい。そのため、本人以外の第三者が本人になりすまし、使用者として相手先と通信する可能性がある。
【０００４】
上述したことに鑑み、認証作業において使用者が本人であることの確実性を高めることが求められている。
【０００５】
図１４に従来の認証作業のフローを示す。まず使用者は、携帯電話等の認証装置を用いてインターネットに接続し、指定された条件下で、認証のための暗証番号等のパスワードをデータとして相手先に送信する。認証のためのパスワードをデータとして受信した相手先は、自分のところにあらかじめ登録された本人のパスワードと、使用者から送られてきたパスワードとの照合を行い、合致するかどうかを確認する。ここで合致が見られれば、使

用者は本人であるということが認証され、合致しない場合は認証されない。
【０００６】
照合が終了した後、相手先は認証の是非を情報として有する照合終了信号を、使用者にデータとして送信する。使用者が本人として認証されなかった場合は、使用者は再びパスワードをデータとして相手先に送信する。また認証された場合は、照合終了信号を受信した時点で認証作業が終了し、次に通信が開始される。
【０００７】
なお本明細書において通信とは、認証作業が終了した後に行われる、目的とする情報の送受信を意味する。
【０００８】
このように従来の認証作業では、本人以外の第三者が本人になりすまし、使用者として相手先と通信することを防止するために、使用者が相手先に送信した番号と、あらかじめ相手先に登録されている本人のパスワードとを照合することで、使用者が本人であることの確認が行われていた。
【０００９】
【発明が解決しようとする課題】
上述したような従来の認証装置を用いた通信システムでは以下の問題があった。
【００１０】
まず、パスワードが第三者に漏洩する可能性のあることは否めない。第三者にパスワードが漏洩した場合、従来の認証作業では使用者が本人であるという確認をすることが不可能になる。
【００１１】
またパスワードは本人が忘れてしまう可能性がある。その場合、本人が相手先にパスワードを問い合わせたり、パスワードを頻繁に書き換えたりする必要が生じ、非常に煩わしい。
【００１２】
また、従来の認証作業では、使用者は、パスワードをデータとして相手先へ送り、照合終了信号を相手先から受信する必要がある。そして、使用者が間違ったパスワードを相手先に送った場合、正しいパスワードを再び相手先に送る必要がある。このため、相手先と使用者との間で少なくとも２回はデータの送受信を行うことになる。
【００１３】
使用者と相手先との間でデータを送受信する回数が多いと、認証作業に必要なコストが上昇する。またデータを送受信する回数が多いと、何らかのエラーによりデータの送受信中に使用者と相手先の間の回線が途切れる可能性が高くなる。データの送受信中に回線が途切れると、認証作業を最初から再び行う必要が生じ、作業が繁雑である。
【００１４】
本発明は、上記問題を解決することを課題とする。
【００１５】
【課題を解決するための手段】
本発明では認証作業を使用者の側のみにおいて行い、相手先には認証が終了したことをデータとして送信する。そして本人かどうかの確認（識別）は、使用者の生体情報（照合用生体情報）と本人の生体情報（基準用生体情報）とを照合することで行う。
【００１６】
本明細書において生体情報とは、人間が生まれつき持っている身体的な特徴で、なおかつ人間の個体識別が可能な情報を意味する。代表的な生体情報としては、指紋、掌紋、声紋等が挙げられる。なお本発明で用いられる生体情報は指紋、掌紋、声紋に限定されない。人間が生まれつき持っている身体的な特徴で、なおかつ人間の個体識別が可能な情報であれば、生体情報として本発明の認証作業に用いることが可能である。
【００１７】
照合の結果、使用者と本人の生体情報が合致しない場合、使用者は再び使用者と本人の生

体情報の照合を行う。使用者と本人の生体情報が合致した場合、認証が終了したことを相手先にデータとして送信し、認証作業が完了する。

【００１８】

認証作業が終了し、使用者が本人であることを相手先が確認したら、相手先との目的とする通信が開始される。

【００１９】

上述した認証作業において、使用者の生体情報が本人の生体情報と合致しない場合、再び使用者の生体情報と本人の生体情報とを照合することができる。そして繰り返し照合を行おうとしたとき、連続してｎ回以上（ｎは自然数）合致しない場合は相手先に自動的にｎ回以上合致しなかったことを通知するようにしても良い。

【００２０】

また、本人の生体情報（基準用生体情報）は複数あっても良く、例えば、指紋と声紋の両方を用いて認証作業を行う構成にしても良い。または、複数の指紋を本人の生体情報（基準用生体情報）として用いることも可能である。

【００２１】

そして使用者の生体情報（照合用生体情報）も複数用いることが可能であり、同じ種類の複数の生体情報を用いたり、種類の異なる複数の生体情報を用いたりすることが可能である。

【００２２】

そして基準用生体情報を書き換える場合、本人であることを確認できるものを相手先に提示することが必要である。または、一度認証作業を行った後、相手先に生体情報を書き換える際に必要なパスワードをデータとして送り、相手先においてパスワードが合致したら、基準用生体情報を書き換えることができるようにしても良い。

【００２３】

なお上述した認証作業は、使用者と相手先との二者間で行われる場合に限られない。例えば使用者と相手先との間の通信を管理する管理者が存在する場合、使用者が本人であるという認証が終了したことを管理者に通知することで、使用者と相手先との間の通信が開始されるようにしても良い。

【００２４】

なお、本明細書において相手先または管理者とは、認証装置の使用者と相手先の間で行なわれる通信の、管理をするものに相当する。具体的には、プロバイダー等が含まれるが、本明細書における相手先または管理者はこれに限定されず、使用者と相手先の間で行なわれる通信を管理する者であれば良い。

【００２５】

使用者と相手先との間の通信を管理する管理者が存在する場合、使用者の生体情報と本人の生体情報の照合が連続してｎ回以上（ｎは自然数）合致しないと、管理者にｎ回以上合致しなかったことを自動的に通知するようにしても良い。

【００２６】

またこの場合、基準用生体情報を書き換える時、本人であることを確認できるものを管理者に提示することが必要である。または、一度認証作業を行った後、管理者に生体情報を書き換える際に必要なパスワードをデータとして送り、管理者側においてパスワードが合致したら、基準用生体情報を書き換えることができるようにしても良い。

【００２７】

上述したように、本発明は生体情報を用いて認証作業を行うため、パスワードが本人以外の第三者に漏洩して、本人であることの確認が行われなくなる可能性がなくなる。よって、認証作業によって使用者が本人であることの確実性を高くすることができる。

【００２８】

そして、認証作業の際に、使用者と相手先（または管理者）との間においてデータをやりとりする回数が抑えられるため、データの送受信に必要なコストを抑えることができ、何らかのエラーにより通信が途絶えて認証作業を再び最初から行うという繁雑さを回避する

ことができる。
【００２９】
さらに、使用者の生体情報を用いて認証作業を行うため、使用者がパスワードを忘れて相手先に問い合わせたり、パスワードを頻繁に書き換えたりする必要がなくなる。
【００３０】
また一般的に生体情報は、パスワードに比べて情報量が大きい。しかし本発明では、本人または使用者の生体情報を、データとして相手先（または管理者）に直接送信する必要がないので、相手先（または管理者）とのデータの送受信に必要な時間の長さを抑えることができ、コストも抑えることができる。
【００３１】
また本発明では、認証作業を行う全ての人の基準用生体情報を、相手先（または管理者）が保存しておく必要がないので、生体情報の情報量がパスワードに比べて大きくても、相手先（または管理者）の負担が重くなることがない。そして、個人で基準用生体情報を保存しているので、セキュリティが破られたときに漏洩する基準用生体情報の数（この場合、同一の人が有する全ての生体情報を一と数える）を、認証作業を行う全ての人の基準用生体情報を相手先（または管理者）に保存しておく場合に比べて、抑えることが可能である。
【００３２】
以下に本発明の構成を示す。
【００３３】
本発明は使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。
【００３４】
本発明は使用者を識別する通信システムであって、
ｎ個の基準用生体情報を記憶する手段と、
前記使用者のｎ個の照会用生体情報を読み取る手段と、
前記ｎ個の照会用生体情報を前記ｎ個の基準用生体情報と照合する手段と、
前記照合が全て合致した場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。
【００３５】
本発明は使用者を識別する通信システムであって、
ｎ個の基準用生体情報を記憶する手段と、
前記使用者のｍ個の照会用生体情報を読み取る手段と、
前記ｍ個の照会用生体情報を前記ｎ個の基準用生体情報と照合する手段と、
前記照合において、前記ｍ個の照会用生体情報の少なくとも１つが、前記ｎ個の基準用生体情報の少なくとも１つと合致している場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。
【００３６】
本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報を記憶する手段と、
前記使用者の複数の種類の照会用生体情報を読み取る手段と、
前記複数の照会用生体情報と前記複数の基準用生体情報とを照合する手段と、
前記照合において、前記複数の種類の照会用生体情報と、前記複数の種類の基準用生体情報と全て合致している場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。

【００３７】
本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報をｎ個記憶する手段と、
前記使用者の複数の種類の照会用生体情報をｍ個読み取る手段と、
前記ｍ個の複数の種類の照会用生体情報を前記ｎ個の複数の種類の基準用生体情報と照合する手段と、
前記照合において、前記複数の種類の内、各種類の照会用生体情報の少なくとも１つが、前記複数の種類の内、各種類の基準用生体情報の少なくとも１つと合致している場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。
【００３８】
本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報をｎ個記憶する手段と、
前記使用者の複数の種類の照会用生体情報をｍ個読み取る手段と、
前記ｍ個の、複数の種類の照会用生体情報を、前記ｎ個の、複数の種類の基準用生体情報と照合する手段と、
前記照合において、前記ｍ個の、複数の種類の照会用生体情報が、前記ｎ個の、複数の種類の基準用生体情報と合致している場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。
【００３９】
本発明は使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記相手先が前記照合が合致したことをデータとして受け取った後に、前記管理者を間に介して前記使用者と前記相手先との間で通信が開始されることを特長とする。
【００４０】
本発明は使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
前記管理者は前記照合が合致したことをデータとして相手先に送る手段と、
を有する通信システムであって、
前記相手先が前記照合が合致したことをデータとして受け取った後に、前記管理者を間に介して前記使用者と前記相手先との間で通信が開始されることを特長とする。
【００４１】
本発明は使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
前記管理者は前記照合が合致したことをデータとして相手先に送る手段と、
を有する通信システムであって、
前記相手先が前記照合が合致したことをデータとして受け取った後に、前記使用者と前記相手先との間で直接通信が開始されることを特長とする。
【００４２】

前記使用者と前記相手先との間で取引が行われ、前記相手先に設定された条件を満たす場合のみ、前記使用者の識別を要求することを特長としていても良い。

【００４３】

本発明は使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、相手先に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記基準用生体情報を書き換えられることを特長とする。

【００４４】

本発明は使用者を識別する通信システムであって、
ｎ個の基準用生体情報を記憶する手段と、
前記使用者のｎ個の照会用生体情報を読み取る手段と、
前記ｎ個の照会用生体情報を前記ｎ個の基準用生体情報と照合する手段と、
前記照合が全て合致した場合、相手先に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記ｎ個の基準用生体情報を書き換えられることを特長とする。

【００４５】

本発明は使用者を識別する通信システムであって、
ｎ個の基準用生体情報を記憶する手段と、
前記使用者のｍ個の照会用生体情報を読み取る手段と、
前記ｍ個の照会用生体情報を前記ｎ個の基準用生体情報と照合する手段と、
前記照合において、前記ｎ個の基準用生体情報の少なくとも１つが、前記ｍ個の照会用生体情報の少なくとも１つと合致している場合、相手先に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記ｎ個の基準用生体情報を書き換えられることを特長とする。

【００４６】

本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報を記憶する手段と、
前記使用者の複数の種類の照会用生体情報を読み取る手段と、
前記複数の照会用生体情報と前記複数の基準用生体情報とを照合する手段と、
前記照合において、前記複数の種類の照会用生体情報と、前記複数の種類の基準用生体情報と全て合致している場合、相手先に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記複数の種類の基準用生体情報を書き換えられることを特長とする。

【００４７】

本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報をｎ個記憶する手段と、
前記使用者の複数の種類の照会用生体情報をｍ個読み取る手段と、
前記ｍ個の、複数の種類の照会用生体情報を、前記ｎ個の、複数の種類の基準用生体情

報と照合する手段と、
前記照合において、前記複数の種類の内、各種類の照会用生体情報の少なくとも１つが、前記複数の種類の内、各種類の基準用生体情報の少なくとも１つと合致している場合、相手先に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記複数の種類の基準用生体情報を書き換えられることを特長とする。
【００４８】
本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報をｎ個記憶する手段と、
前記使用者の複数の種類の照会用生体情報をｍ個読み取る手段と、
前記ｍ個の、複数の種類の照会用生体情報を、前記ｎ個の、複数の種類の基準用生体情報と照合する手段と、
前記照合において、前記ｍ個の、複数の種類の照会用生体情報が、前記ｎ個の、複数の種類の基準用生体情報と合致している場合、相手先に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記複数の種類の基準用生体情報を書き換えられることを特長とする。
【００４９】
本発明は使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記管理者に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記管理者に送り、前記管理者において前記パスワードが正しいと認証された場合、前記基準用生体情報を書き換えられることを特長とする通信システム。
【００５０】
前記基準用生体情報が、指紋、掌紋または声紋であることを特長としていても良い。
【００５１】
前記照合用生体情報が、指紋、掌紋または声紋であることを特長としていても良い。
【００５２】
前記掌紋は手ひらの全体の掌紋、もしくは前記手のひらの一部の掌紋であることを特徴としていても良い。
【００５３】
前記記憶する手段が、フラッシュメモリであることを特長としていても良い。
【００５４】
前記読み取る手段が、フォトダイオードまたはＣＣＤであることを特長としていても良い。
【００５５】
本発明は、携帯情報端末、携帯電話またはパーソナルコンピューターを用いることを特長としていても良い。
【００５６】
【発明の実施の形態】
図１に本発明の通信システムのフローを示す。認証作業が開始されると、認証作業を行う装置（認証装置）によって使用者の生体情報が採取される。生体情報の採取は、使用者が

認証装置を制御することで開始される。あらかじめプログラムされていれば、１つの操作用のキー（操作キー）を押すことによって生体情報の採取が開始されるようにすることも可能である。また、認証装置の電源投入時に自動的に生体情報の採取がはじめられるようにすることも可能である。

【００５７】

生体情報の採取は、例えば、ＣＣＤやフォトダイオードを用いたラインセンサーやエリアセンサー、マイク等によって行われる。

【００５８】

認証装置には、あらかじめ本人の生体情報（基準用生体情報）が記憶されている。基準用生体情報は、例えば認証装置が有する、不揮発性メモリなどで形成されている内蔵メモリに蓄えられている。

【００５９】

採取された使用者の生体情報（照合用生体情報）は、あらかじめ認証装置に記憶されている本人の生体情報（基準用生体情報）と照合される。ここで、照合用生体情報と基準用生体情報の２つの生体情報が合致すると判断されれば、使用者は目的とする通信を行う本人であることが認証される。

【００６０】

ここで照合が合致しないと判断された場合、認証装置によって再び使用者の生体情報を採取し、採取した照合用生体情報と基準用生体情報を再度照合することが可能である。

【００６１】

なお使用者が生体情報の照合をやり直す回数は、実施者が任意に設定することができる。例えば一度の認証作業中にｎ回（ｎは任意の自然数）より多く繰り返して照合を行うことができないようにしても良い。また、ｎ回連続して照合が合致しなかった場合、認証装置がアラームを発するようにしても良い。また、ｎ回連続して照合が合致しなかったことを、使用者以外の人間または該認証装置以外の装置に、自動的に通知する様にしても良い。

【００６２】

認証完了後、認証が完了したという情報を有する信号（認証完了信号）を、目的とする通信を行う相手先に送信する。このとき、認証はすでに完了しているので、新たに相手先との間で生体情報のやりとりを行う必要がなく、相手先は認証装置から認証完了信号を受信するだけでよい。

【００６３】

相手先が認証完了信号を受信した時点で、認証作業が終了する。認証作業が終了した後、使用者と相手先との間で、目的とする通信が行われる。なお目的とする通信は、取引等の営利のためになす経済行為に用いられることに限定されない。使用者と相手先との間で行われる通信は、あらゆる意志や情報の伝達が可能である。

【００６４】

なお、本発明において認証装置は、使用者の生体情報の採取と、生体情報の照合と、認証完了信号の送信といった、３つの機能を有していることが必要である。１つの認証装置が上記３つの機能を併せ持っていても良い。また複数の装置を用いて上記３つの機能を果たすようにしても良い。この場合、複数の装置を全て合わせて認証装置と呼ぶ。

【００６５】

次に、本発明の通信システムに用いられる生体情報のうち、指紋及び掌紋について説明する。

【００６６】

図２に人間の右手の図を示す。生体情報として認証装置に読み取られるのは、手のひらの一部である掌紋１、手のひら全体である掌紋２、親指の指紋、人差し指の指紋、中指の指紋、薬指の指紋または小指の指紋である。また右手ではなく左手の掌紋を用いても良く、右手と左手を両方用いても良い。

【００６７】

手のひらの一部である掌紋１、手のひら全体である掌紋２、親指の指紋、人差し指の指紋

、中指の指紋、薬指の指紋及び小指の指紋は、個々の人間に特有のものであるため、第３者による認証装置の悪用を防ぐことができる。

【００６８】

なお生体情報のうち、１種類だけ本発明の通信システムに用いても良いし、複数種類用いても良い。また、同じ種類の生体情報を単数または複数用いることもできる。例えば同じ親指の指紋を複数生体情報として用いることが可能である。また、異なる種類の生体情報を複数用いることができる。例えば同じ小指の指紋を複数と、声紋とを共に生体情報として用いることが可能である。

【００６９】

以下に、同じ種類の複数の生体情報を用いて照合を行う場合について、具体的に説明する。

【００７０】

図３に複数の基準用生体情報を用いた場合の照合の関係図を示す。図３（Ａ）では、４つの基準用生体情報（Ａ１、Ａ２、Ａ３、Ａ４）と、同じく４つの照合用生体情報（Ａ１’、Ａ２’、Ａ３’、Ａ４’）とが全て合致した場合に認証される例を示す。

【００７１】

図３（Ａ）に示すように、Ａ１とＡ１’、Ａ２とＡ２’、Ａ３とＡ３’、Ａ４とＡ４’がそれぞれ合致している。このように、複数の基準用生体情報と複数の照合用生体情報とが全て合致してはじめて認証されるようにすることで、使用者が本人であることの確実性を高めることができる。

【００７２】

なお基準用生体情報と照合用生体情報の数は４つに限定されず、生体情報の数は任意である。

【００７３】

図３（Ｂ）では、４つの基準用生体情報（Ａ１、Ａ２、Ａ３、Ａ４）のいずれか１つと、照合用生体情報（Ａ５’、Ａ６’、Ａ７’、Ａ２’）のいずれか１つとが合致した場合に認証される例を示す。

【００７４】

図３（Ｂ）に示すように、Ａ２とＡ２’が合致しているが、Ａ１、Ａ３、Ａ４と、Ａ５’、Ａ６’、Ａ７’とは合致していない。このように、複数の基準用生体情報のいずれか１つと、複数の照合用生体情報のいずれか１つとが合致してはじめて認証されるようにすることで、照合用生体情報を採取する回数を抑えることができ、認証作業が容易になる。

【００７５】

なお基準用生体情報と照合用生体情報の数は４つに限定されず、生体情報の数は任意である。また図３（Ｂ）では、複数の基準用生体情報のいずれか１つと、複数の照合用生体情報のいずれか１つとが合致してはじめて認証される様にしているが、合致する数は１つに限定されない。合致するべき数は実施者が任意に設定することが可能である。

【００７６】

図４に複数種類の基準用生体情報を用いた場合の照合の関係図を示す。図４（Ａ）では、２種類の基準用生体情報（Ａ１、Ａ２、Ａ３、Ｂ１、Ｂ２）と、同じく２種類の照合用生体情報（Ａ１’、Ａ２’、Ａ３’、Ｂ１’、Ｂ２’）とが全て合致した場合に認証される例を示す。

【００７７】

図４（Ａ）に示すように、Ａ１とＡ１’、Ａ２とＡ２’、Ａ３とＡ３’、Ｂ１とＢ１’、Ｂ２とＢ２’がそれぞれ合致している。このように、複数種類の基準用生体情報と複数種類の照合用生体情報とが全て合致して、はじめて認証されるようにすることで、使用者が本人であることの確実性を高めることができる。

【００７８】

なお基準用生体情報と照合用生体情報の種類は２つに限定されず、生体情報の種類の数は任意である。また基準用生体情報と照合用生体情報の各種類の数も任意である。

【００７９】
図４（Ｂ）では、３つの基準用生体情報（Ａ１、Ａ２、Ａ３）のいずれか１つと、照合用生体情報（Ａ４’、Ａ５’、Ａ２’）のいずれか１つとが合致し、２つの基準用生体情報（Ｂ１、Ｂ２）のどちらか１つと、照合用生体情報（Ｂ３’、Ｂ１’）のどちらか１つとが合致した場合に認証される例を示す。
【００８０】
図４（Ｂ）に示すように、Ａ２とＡ２’、Ｂ１とＢ１’が合致しているが、Ａ１、Ａ３、Ｂ２と、Ａ４’、Ａ５’、Ｂ３’は合致していない。このように複数種の基準用生体情報を用い、各種類ごとに、基準用生体情報のいずれか１つと、照合用生体情報のいずれか１つとが合致して、はじめて認証されるようにすることで、使用者が本人であることの確実性を高めることができる。
【００８１】
なお基準用生体情報と照合用生体情報の種類は２つに限定されず、生体情報の種類の数は任意である。また基準用生体情報と照合用生体情報の各種類の数も任意である。また図４（Ｂ）では、各種類ごとに基準用生体情報のいずれか１つと、複数の照合用生体情報のいずれか１つとが合致してはじめて認証される様にしているが、合致する数は１つに限定されない。生体情報の各種類毎に合致するべき数は実施者が任意に設定することが可能である。
【００８２】
次に、上述した認証作業において、認証が完了した後のフローについて、図５を用いて詳しく説明する。
【００８３】
図５（Ａ）は、認証作業と通信とが、使用者と相手先との二者間でのみ行われる場合の関係図である。認証が完了した後、使用者側（具体的には使用者が用いる認証装置）から相手先に、認証終了信号が送信される。そして使用者と、相手先との間で目的とする通信が開始される。
【００８４】
図５（Ｂ）は、認証作業と通信が、使用者と相手先との二者間でのみ行われるのではなく、使用者と、相手先と、管理者との三者間で行われる場合の関係図である。管理者は、使用者と相手先との間の通信を管理する役目を担っている。
【００８５】
認証が完了するまでのフローは、使用者と相手先との二者間で行われる場合と同じなので省略する。使用者が本人であるという認証が完了したら、使用者側（具体的には使用者が用いる認証装置）から管理者に、認証終了信号が送信される。そして管理者を介して、使用者と相手先との間で目的とする通信が開始される。
【００８６】
図５（Ｃ）は、図５（Ｂ）と同じく認証作業と通信が使用者と、相手先と、管理者との三者間で行われる場合の関係図である。
【００８７】
認証が完了するまでのフローは、使用者と相手先との二者間で行われる場合と同じなので省略する。使用者が本人であるという認証が完了したら、使用者側（具体的には使用者が用いる認証装置）から管理者に認証終了信号が送信される。管理者は、使用者側からの認証終了信号を受信したら、相手先にも認証終了信号を送信する。そして管理者を介して、使用者と相手先との間で目的とする通信が開始される。
【００８８】
図５（Ｄ）は、図５（Ｂ）、図５（Ｃ）と同じく、認証作業と通信が使用者と、相手先と、管理者との三者間で行われる場合の関係図である。
【００８９】
認証が完了するまでのフローは、使用者と相手先との二者間で行われる場合と同じなので省略する。使用者が本人であるという認証が完了したら、使用者側（具体的には使用者が

用いる認証装置）から管理者に認証終了信号が送信される。管理者は、使用者側からの認証終了信号を受信したら、相手先にも認証終了信号を送信する。そして使用者と相手先との間で、管理者を介さずに直接、目的とする通信が開始される。

【００９０】

なお本発明の通信システムにおいて、使用者と相手先以外にも認証作業と通信に関与しているもの（例えば管理者）が存在する場合、認証が完了したあとのフローは、さまざまな組み合わせが考えられる。本発明は図５に示した関係図に限定されない。使用者が認証完了信号を他者に送信することで、使用者と相手先との通信を開始することが可能であるならば、どのような組み合わせでも良い。

【００９１】

また本発明の通信システムにおいて、相手先と管理者の数は１つに限定されない、相手先が複数存在していても良いし、管理者が複数存在していても良い。

【００９２】

上述したように、本発明は生体情報を用いて認証作業を行うため、パスワードが本人以外の第三者に漏洩して、本人であることの確認が行われなくなる可能性がなくなる。よって、認証作業によって使用者が本人であることの確実性を高くすることができる。

【００９３】

そして、認証作業の際に、使用者と相手先（または管理者）との間においてデータをやりとりする回数が抑えられるため、データの送受信に必要なコストを抑えることができ、何らかのエラーにより通信が途絶えて認証作業を再び最初から行うという繁雑さを回避することができる。

【００９４】

さらに、使用者の生体情報を用いて認証作業を行うため、使用者がパスワードを忘れて相手先に問い合わせたり、パスワードを頻繁に書き換えたりする必要がなくなる。

【００９５】

また一般的に生体情報は、パスワードに比べて情報量が大きい。しかし本発明では、本人または使用者の生体情報を、データとして相手先（または管理者）に直接送信する必要がないので、相手先（または管理者）とのデータの送受信に必要な時間の長さを抑えることができ、コストも抑えることができる。

【００９６】

また本発明では、認証作業を行う全ての人の基準用生体情報を、相手先（または管理者）が保存しておく必要がないので、生体情報の情報量がパスワードに比べて大きくても、相手先（または管理者）の負担が重くなることがない。そして、個人で基準用生体情報を保存しているので、セキュリティが破られたときに漏洩する基準用生体情報の数（この場合、同一の人が有する全ての生体情報を一と数える）を、認証作業を行う全ての人の基準用生体情報を相手先（または管理者）に保存しておく場合に比べて、抑えることが可能である。

【００９７】

【実施例】

以下に、本発明の実施例について説明する。

【００９８】

（実施例１）

本実施例では、認証装置に記憶されている基準用生体情報を、認証装置を用いて書き換える場合について詳しく説明する。

【００９９】

図６に本実施例の、基準用生体情報の書き換えのフローを示す。まず、認証作業を行い、使用者が本人であることを認証する。なお認証作業の詳しい説明については実施の形態において既に示したので、ここでは説明を省略する。

【０１００】

認証作業が終了し使用者と相手先（または管理者）との通信が開始されたら、書き換え作

業が開始され、生体情報を書き換える際に必要なパスワードを、使用者が相手先にデータとして送信する。

【０１０１】

このパスワードの照合において合致しない場合は、基準用生体情報の書き換えができない。この場合、相手先（管理者）から使用者に、パスワードが合致しなかったことが通知される。そして使用者は再びパスワードをデータとして送信し直すことが可能である。

【０１０２】

なおこの場合も認証作業の照合の場合と同じく、パスワードを送信し直す回数は、実施者が任意に設定することができる。例えば一度の書き換え作業中にｎ回（ｎは任意の自然数）より多く繰り返して照合を行うことができないようにしても良い。また、ｎ回連続して照合が合致しなかった場合、認証装置がアラームを発するようにしても良い。また、ｎ回連続して照合が合致しなかったことを、使用者以外の人間または該認証装置以外の装置に、自動的に通知する様にしても良い。

【０１０３】

相手先においてパスワードを照合して合致したら、基準用生体情報の書き換えが承諾される。相手先（管理者）から基準用生体情報の書き換えが承諾されたことを情報として有する、書き換え承諾信号が使用者に送信される。

【０１０４】

使用者は、書き換え承諾信号を受信したら、認証装置に新たに生体情報を読み込む。そして新しい基準用生体情報が認証装置に記憶され、基準用生体情報の書き換え作業が完了する。

【０１０５】

上述したフローに従って基準用生体情報を書き換えることで、本人以外の第三者に基準用生体情報を勝手に書き換えられてしまう可能性を低くすることができる。

【０１０６】

また書き換え作業の全てを、認証装置を用いて行うことができるので、基準用生体情報の書き換えの煩雑さを抑えることができる。

【０１０７】

（実施例２）

以下に本発明において用いられる認証装置の構成と、その動作について説明する。

【０１０８】

図７は本実施例の認証装置のブロック図である。本実施例の認証装置はアンテナ６０１、送信受信回路６０２、信号を圧縮伸張化、符号化する信号処理回路６０３、制御用マイコン６０４、フラッシュメモリ６０５、操作キー６０６などを有している。そしてさらに、センサー６１１、照合回路部６１２などを有している。

【０１０９】

操作キー６０６を操作することによって、制御用マイコン６０４がセンサー６１１を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として掌紋または指紋を用いる例について説明する。センサー６１１で読み取った使用者の生体情報は、照合回路部６１２に入力される。

【０１１０】

照合回路部６１２に入力された使用者の生体情報（照合用生体情報）は、Ａ／Ｄコンバータ６１３においてデジタル信号に変換される。デジタル信号に変換された使用者の生体情報は、ＤＳＰ（デジタルシグナルプロセッサ）６１４に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、微分フィルタなどを用い映像の濃淡が変わるところを際立たせることである。得られた照合用生体情報はＤＳＰ６１４内部で数値化され、比較回路６１５に入力される。

【０１１１】

比較回路６１５はフラッシュメモリ６０５に記憶されている基準用生体情報と、ＤＳＰ６１４内部で数値化され比較回路６１５に入力された照合用生体情報とを比較し照合する。

【０１１２】
生体情報を照合する方法としては、基準用生体情報と照合用生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報を直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準用生体情報は１つだけではなく、手の向きを多少変えるなどして、複数備えたほうがより確実な認証が可能となる。
【０１１３】
ここで合致が見られれば、制御用マイコン６０４は認証完了信号を出力し、該認証完了信号は、信号処理回路６０３、送受信回路６０２、アンテナ６０１を介して認証装置から出力される。認証装置から出力された認証完了信号は、インターネットなどを通じて相手先（または管理者）に送信される。なお、認証装置から出力された認証完了信号を、インターネットを介さず直接相手先（または管理者）に送信に送信しても良い。
【０１１４】
（実施例３）
以下に本発明において用いられる認証装置の構成と、その動作の、実施例１とは異なる例について説明する。
【０１１５】
図８は本実施例の認証装置のブロック図である。この認証装置はアンテナ５０１、送信受信回路５０２、信号を圧縮伸張化、符号化する信号処理回路５０３、制御用マイコン５０４、フラッシュメモリ５０５、操作キー５０６などを有している。そしてさらに、マイク５１１、アンプ５１６、照合回路部５１２などを有している。
【０１１６】
操作キー５０６を操作することによって、制御用マイコン５０４がマイク５１１を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、声紋を用いる例について説明する。マイク５１１で読み取った使用者の生体情報は、アンプ５１６によって増幅され、照合回路部５１２に入力される。
【０１１７】
照合回路部５１２に入力された使用者の生体情報（照合用生体情報）は、Ａ／Ｄコンバータ５１３においてデジタル信号に変換される。デジタル信号に変換された照合用生体情報は、ＤＳＰ（デジタルシグナルプロセッサ）５１４に入力され、信号処理される。信号処理とは、具体的には、生体情報をより判別しやすくするため、帯域フィルタなどを用い、周波数ごとの音の強さを数値化することである。ＤＳＰ５１４により数値化された基準用生体情報は比較回路５１５に入力される。
【０１１８】
比較回路５１５はフラッシュメモリ５０５に記憶されている基準用生体情報と、ＤＳＰ５１４内部で数値化され比較回路５１５に入力された照合用生体情報とを比較し照合する。
【０１１９】
生体情報を照合する方法としては、基準用生体情報と照合用生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報が有するスペクトルを直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準用生体情報は１つだけではなく、発音を多少変えるなどして、複数備えたほうがより確実な認証が可能となる。
【０１２０】
ここで合致が見られれば、制御用マイコン５０４は認証完了信号を出力し、該認証完了信号は、信号処理回路５０３、送受信回路５０２、アンテナ５０１を介して認証装置から出力される。認証装置から出力された認証完了信号は、インターネットなどを通じて伝達される。なお、認証装置から出力された認証完了信号を、インターネットを介さず直接相手先に送信しても良い。
【０１２１】
本実施例の構成は、実施例１または２と組み合わせて実施することが可能である。
【０１２２】

（実施例４）
次に本発明で用いられる認証装置の１つである、携帯情報端末について述べる。図９に示すのは本実施例の携帯情報端末であり、２７０１は表示用パネル、２７０２は操作用パネルである。表示用パネル２７０１と操作用パネル２７０２は接続部２７０３において接続されている。そして接続部２７０３における、表示用パネル２７０１のセンサー内蔵ディスプレイ２７０４が設けられている面と操作用パネル２７０２の音声入力部２７０８が設けられている面との角度θは、任意に変えることができる。
【０１２３】
表示用パネル２７０１はセンサー内蔵ディスプレイ２７０４を有している。センサー内蔵ディスプレイ２７０４は画像の読み取りと、画像の表示との、２つの機能を併せ持っている。本実施例ではセンサー内蔵ディスプレイ２７０４にはＥＬディスプレイが用いられている。
【０１２４】
また図９に示した携帯情報端末は電話としての機能を有しており、表示用パネル２７０１は音声出力部２７０５を有しており、音声が音声出力部２７０５から出力される。
【０１２５】
操作用パネル２７０２は操作キー２７０６、電源スイッチ２７０７、音声入力部２７０８を有している。なお図９では操作キー２７０６と電源スイッチ２７０７とを別個に設けたが、操作キー２７０６の中に電源スイッチ２７０７が含まれる構成にしても良い。音声入力部２７０８において、音声が入力される。
【０１２６】
なお図９では表示用パネル２７０１が音声出力部２７０５を有し、操作用パネル２７０２が音声入力部２７０８を有しているが、本実施例はこの構成に限定されない。表示用パネル２７０１が音声入力部２７０８を有し、操作用パネルが音声出力部２７０５を有していても良い。また音声出力部２７０５と音声入力部２７０８とが共に表示用パネル２７０１に設けられていても良いし、音声出力部２７０５と音声入力部２７０８とが共に操作用パネル２７０２に設けられていても良い。
【０１２７】
なおセンサー内蔵ディスプレイ２７０４は、携帯情報端末の周りの明るさ（照度）を測定し、自動的に輝度を調整する機能を有していても良い。また図９に示した本実施例の携帯情報端末は、センサー内蔵ディスプレイ２７０４において周りの明るさ（照度）を測定することができるが、センサー内蔵ディスプレイ２７０４とは別個にＣＣＤ等のセンサ部を設けて、該センサ部において周りの照度を測定し、センサー内蔵ディスプレイ２７０４の輝度を調整するようにしても良い。
【０１２８】
また、携帯情報端末のセンサー内蔵ディスプレイ２７０４は、電源投入時、操作キー２７０６を操作している時、または電話の着信があった時に、自動的に輝度が高くなるようにし、通話している時、操作キー２７０６を操作し終わってから一定の時間が過ぎた時に、自動的に輝度を下げるようにしても良い。これによって、携帯情報端末自体の消費電力を抑えることが可能になる。
【０１２９】
またある一定の時間以上、操作キー２７０６を操作しなかったり、電話が着信しなかったりすると、自動的にセンサー内蔵ディスプレイ２７０４のみがオフの状態になって画像が表示されないようにすることも可能である。これによって、携帯情報端末自体の消費電力を抑えることが可能になる。
【０１３０】
図１０、図１１を用いて、図９で示した携帯情報端末の使用方法について説明する。図１０に示すように、図９で示した携帯情報端末によって認証を行う場合には、手のひら２７１０をセンサー内蔵ディスプレイ２７０４に覆いかぶせるようにして使用する。認証は操作キー２７０６でキー操作を行うとともに、使用者の手相をセンサー内蔵ディスプレイ２

７０４が読み取り、認証作業を行う。
【０１３１】
なお図１０では操作キー２７０６を人差し指で操作している例について示したが、図１１に示すように、親指で操作キー２７０６を操作することも可能である。なお操作キー２７０６は操作用パネル２７０２の側面に設けても良い。操作は片手（きき手）の人差し指のみ、または親指のみでも可能である。
【０１３２】
以下に図９に示した携帯情報端末の構成と、その動作について説明する。
【０１３３】
図１２は本実施例の携帯情報端末のブロック図である。この携帯情報端末はアンテナ９０１、送信受信回路９０２、信号を圧縮伸張化、符号化する信号処理回路９０３、制御用マイコン９０４、フラッシュメモリ９０５、操作キー９０６、音声入力回路９０７、音声出力回路９０８、マイク９０９、スピーカ９１０などを有している。そしてさらに、センサー９１１、照合回路部９１２などを有している。
【０１３４】
音声入力部２７０８から入力された音声は、マイク９０９に入力され、アナログ信号として音声入力回路９０７に入力される。音声入力回路９０７に入力されたアナログ信号は増幅された後デジタル信号に変換され、信号処理部９０３に入力される。信号処理部９０３において圧縮伸張化、符号化されたデジタル信号は、送受信回路９０２において周波数を変えられて、場合によっては増幅されて、アンテナ９０１から送信される。
【０１３５】
またアンテナ９０１において受信した音声情報を有するデジタル信号は、送受信回路９０２において周波数を変えられて、場合によっては増幅されて、信号処理部９０３に入力される。信号処理部９０３に入力されたデジタル信号は圧縮伸張化、符号化され、音声出力回路９０８に入力される。音声出力回路９０８に入力されたデジタル信号はアナログ信号に変換された後増幅され、スピーカー９１０から出力され、音声出力部２７０８から音声として使用者の耳に入力される。
【０１３６】
操作キー９０６を操作することによって、制御用マイコン９０４がセンサー９１１を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、掌紋または指紋を用いる例について説明する。センサー９１１で読み取った使用者の生体情報（照合用生体情報）は、照合回路部９１２に入力される。
【０１３７】
照合回路部９１２に入力された照合用生体情報は、Ａ／Ｄコンバータ９１３においてデジタル信号に変換される。デジタル信号に変換された照合用生体情報は、ＤＳＰ（デジタルシグナルプロセッサ）９１４に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、微分フィルタなどを用い映像の濃淡が変わるところを際立たせることである。得られた照合用生体情報はＤＳＰ９１４内部で数値化され、比較回路９１５に入力される。
【０１３８】
比較回路９１５はフラッシュメモリ９０５に記憶されている基準用生体情報と、ＤＳＰ９１４内部で数値化され比較回路９１５に入力された照合用生体情報とを比較し照合する。
【０１３９】
生体情報を照合する方法としては、基準用生体情報と照合用生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報を直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準用生体情報は１つだけではなく、手の向きを多少変えるなどして、複数備えたほうがより確実な認証が可能となる。
【０１４０】
ここで合致が見られれば、制御用マイコン９０４は認証完了信号を出力し、該認証完了信号は、信号処理回路９０３、送受信回路９０２、アンテナ９０１を介して携帯情報端末か

ら出力される。携帯情報端末から出力された認証完了信号は、インターネットなどを通じて伝達される。なお、携帯情報端末から出力された認証完了信号を、インターネットを介さず直接相手先に送信しても良い。

【０１４１】

なお本発明で用いられる認証装置は、本実施例で示した構成の携帯情報端末に限定されない。また本実施例で示した携帯情報端末は、指紋または掌紋を生体情報として利用しているが、声紋を生体情報として利用する構成を有していても良い。

【０１４２】

なお、本実施例は、実施例１～３を組み合わせて実施することが可能である。

【０１４３】

（実施例５）

本実施例は本発明を使用する状況を述べるものである。目的とする通信が取引などの営利のためになす経済行為に用いられる場合において、認証が生体情報までの高度な認証が不要な場合は本発明を使用しないこともありえる。小額の金銭移動などの場合は必ずしも必要ではない。

【０１４４】

このため、認証の有無が選択できること、たとえば金銭が高額な移動が伴う場合のみに選択的に認証が出来るようにすることも可能である。相手先の状況に合わせ使用することや、あらかじめ認証装置の制御マイコン上に判定基準を設定しておき、数値が一定値を超えた場合のみ使用することが可能である。また、認証結果が必要な場合のみ、認証完了信号をインターネットで相手先（または管理者）伝達することも可能である。

【０１４５】

なお、本実施例は、実施例１～実施例４と組み合わせて実施することが可能である。

【０１４６】

（実施例６）

本発明に用いられる認証装置として、様々な電子機器を用いることができる。

【０１４７】

図１３（Ａ）はパーソナルコンピューター（パソコン）であり、本体２５０１、筐体２５０２、表示部２５０３、キーボード２５０４、センサー２５０５等を含む。本発明では、センサー２５０５を用い、パーソナルコンピューター内に生体情報を取り込むことができる。

【０１４８】

なお本実施例では、指紋または掌紋を生体情報として利用する例について示したが、音声入力部を設けて声紋を生体情報として利用する構成にしても良い。またセンサー２５０５と音声入力部を両方設けて、指紋または掌紋と、声紋とを共に利用する構成にしても良い。

【０１４９】

図１３（Ｂ）は携帯電話であり、本体２６０１、音声出力部２６０２、音声入力部２６０３、表示部２６０４、操作キー２６０５、アンテナ２６０６を含んでいる。通常の電話をかける場合は表示部２６０４に相手先の電話番号や、電波の受信状態などが表示される。また、インターネットを使用する場合には、相手先の必要情報が表示されることになる。そして表示部２６０４はセンサーとしても機能し、表示部２６０４において生体情報を取り込むことが可能である。

【０１５０】

また、図１３（Ｂ）に示した携帯電話は、表示部２６０４がセンサーとしての機能とディスプレイとしての機能を併せ持っていたが、表示部２６０４をディスプレイとしてのみ利用し、センサーを別個に設ける構成にしても良い。

【０１５１】

なお本発明で用いられる認証装置は本実施例で示した電子機器に限定されない。生体情報を取り込み、該生体情報をあらかじめ記憶されている生体情報と照合し、照合が合致した

ら相手先に認証が終了したことを知らせる機能を有していればよい。

【０１５２】

【発明の効果】

上述したように、本発明は生体情報を用いて認証作業を行うため、パスワードが本人以外の第三者に漏洩して、本人であることの確認が行われなくなる可能性がなくなる。よって、認証作業によって使用者が本人であることの確実性を高くすることができる。

【０１５３】

そして、認証作業の際に、使用者と相手先（または管理者）との間においてデータをやりとりする回数が抑えられるため、データの送受信に必要なコストを抑えることができ、何らかのエラーにより通信が途絶えて認証作業を再び最初から行うという繁雑さを回避することができる。

【０１５４】

さらに、使用者の生体情報を用いて認証作業を行うため、使用者がパスワードを忘れて相手先に問い合わせたり、パスワードを頻繁に書き換えたりする必要がなくなる。

【０１５５】

また一般的に生体情報は、パスワードに比べて情報量が大きい。しかし本発明では、本人または使用者の生体情報を、データとして相手先（または管理者）に直接送信する必要がないので、相手先（または管理者）とのデータの送受信に必要な時間の長さを抑えることができ、コストも抑えることができる。

【０１５６】

また本発明では、認証作業を行う全ての人の基準用生体情報を、相手先（または管理者）が保存しておく必要がないので、生体情報の情報量がパスワードに比べて大きくても、相手先（または管理者）の負担が重くなることがない。そして、個人で基準用生体情報を保存しているので、セキュリティが破られたときに漏洩する基準用生体情報の数（この場合、同一の人が有する全ての生体情報を一と数える）を、認証作業を行う全ての人の基準用生体情報を相手先（または管理者）に保存しておく場合に比べて、抑えることが可能である。

【図面の簡単な説明】

【図１】　本発明の通信システムのフロー。

【図２】　読み取る掌紋または指紋の位置を示す図。

【図３】　生体情報の照合の関係図。

【図４】　生体情報の照合の関係図。

【図５】　認証が完了した後のフロー。

【図６】　基準用生体情報を書き換える際の書き換え作業のフロー。

【図７】　認証装置の構造を示すブロック図。

【図８】　認証装置の構造を示すブロック図。

【図９】　認証装置の一例である携帯情報端末の外観図。

【図１０】　認証装置の一例である携帯情報端末の使用例。

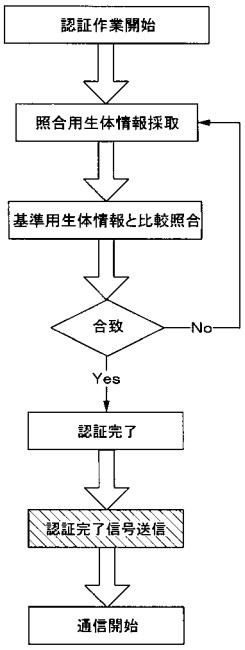
【図１１】　認証装置の一例である携帯情報端末の使用例。

【図１２】　認証装置の一例である携帯情報端末の構造を示すブロック図。

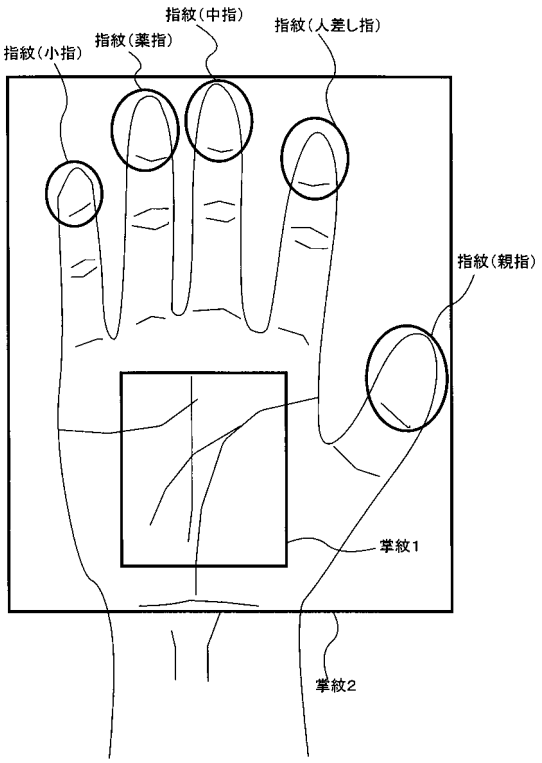
【図１３】　認証装置の一例である電子機器の図。

【図１４】　従来の認証のフロー。

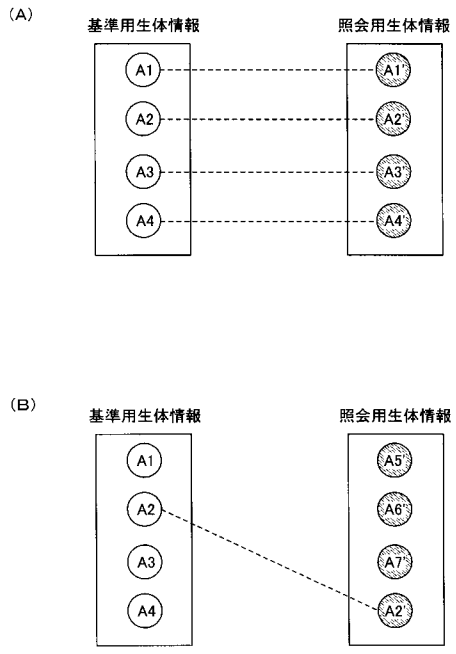
【図１】


認証作業開始
照合用生体情報採取
基準用生体情報と比較照合
合致
No
Yes
認証完了
認証完了信号送信
通信開始

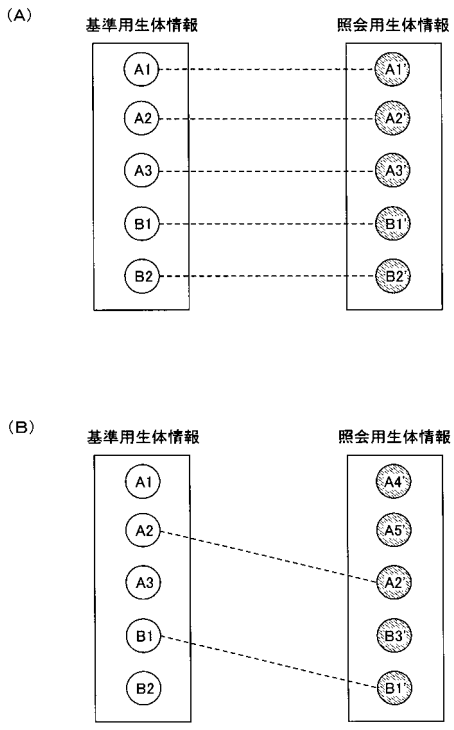
【図２】


指紋(小指)
指紋(薬指)
指紋(中指)
指紋(人差し指)
指紋(親指)
掌紋1
掌紋2

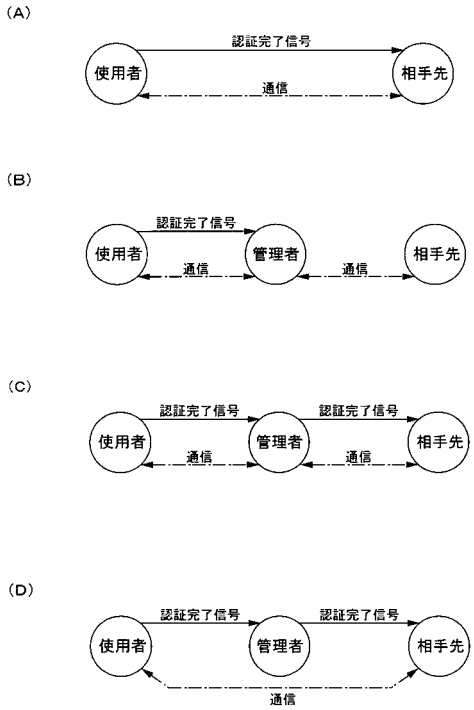
【図３】


(A)
基準用生体情報
照会用生体情報
A1
A2
A3
A4
A1'
A2'
A3'
A4'
(B)
基準用生体情報
照会用生体情報
A1
A2
A3
A4
A5'
A6'
A7'
A2'

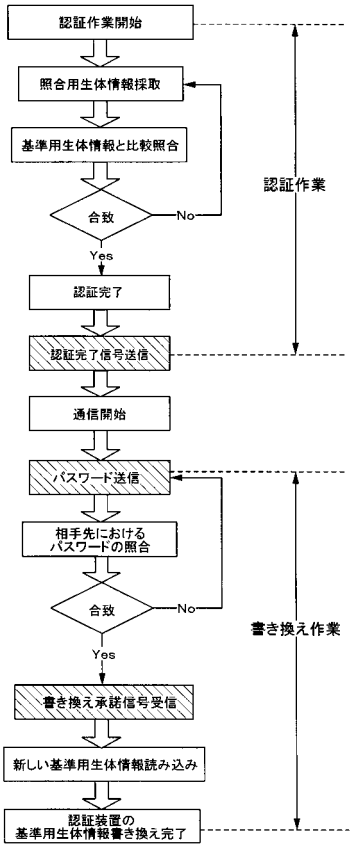
【図４】


(A)
基準用生体情報
照会用生体情報
A1
A2
A3
B1
B2
A1'
A2'
A3'
B1'
B2'
(B)
基準用生体情報
照会用生体情報
A1
A2
A3
B1
B2
A4'
A5'
A2'
B3'
B1'

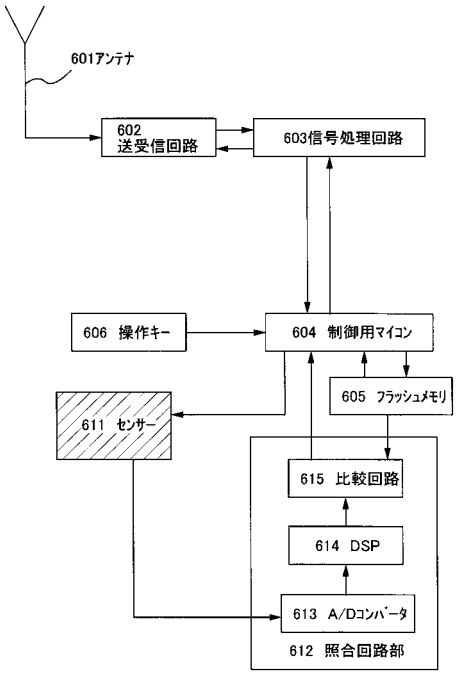
【図５】


(A)
認証完了信号
使用者
相手先
通信
(B)
認証完了信号
使用者
管理者
相手先
通信
通信
(C)
認証完了信号
認証完了信号
使用者
管理者
相手先
通信
通信
(D)
認証完了信号
認証完了信号
使用者
管理者
相手先
通信

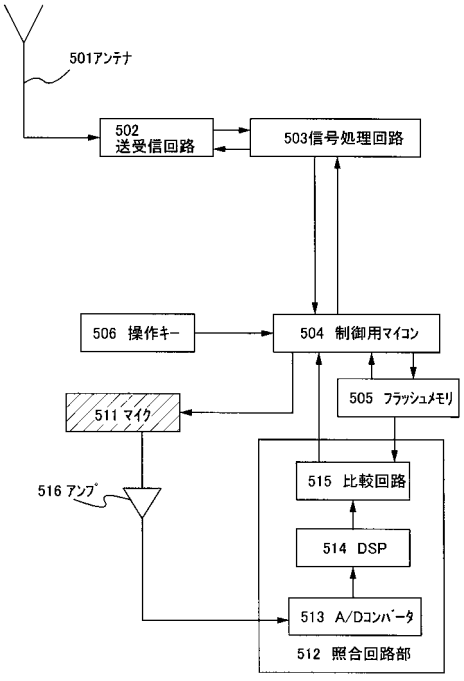
【図６】


認証作業開始
照合用生体情報採取
基準用生体情報と比較照合
合致
No
Yes
認証作業
認証完了
認証完了信号送信
通信開始
パスワード送信
相手先における
パスワードの照合
合致
No
Yes
書き換え作業
書き換え承諾信号受信
新しい基準用生体情報読み込み
認証装置の
基準用生体情報書き換え完了

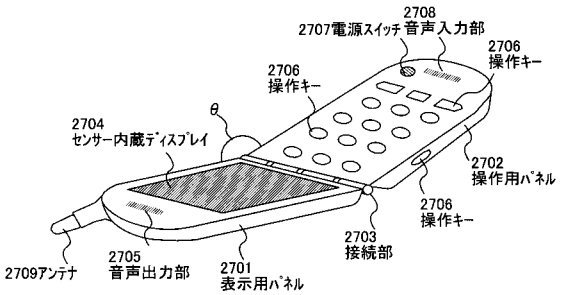
【図７】


601アンテナ
602
送受信回路
603信号処理回路
606 操作キー
604 制御用マイコン
605 フラッシュメモリ
611 センサー
615 比較回路
614 DSP
613 A/Dコンバータ
612 照合回路部

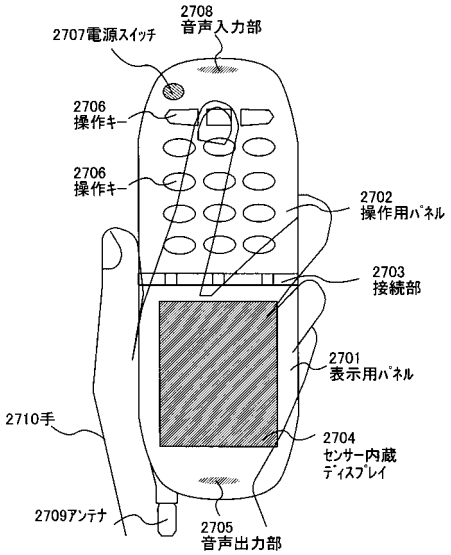
【図８】


501アンテナ
502
送受信回路
503信号処理回路
506 操作キー
504 制御用マイコン
505 フラッシュメモリ
511 マイク
516 アンプ
515 比較回路
514 DSP
513 A/Dコンバータ
512 照合回路部

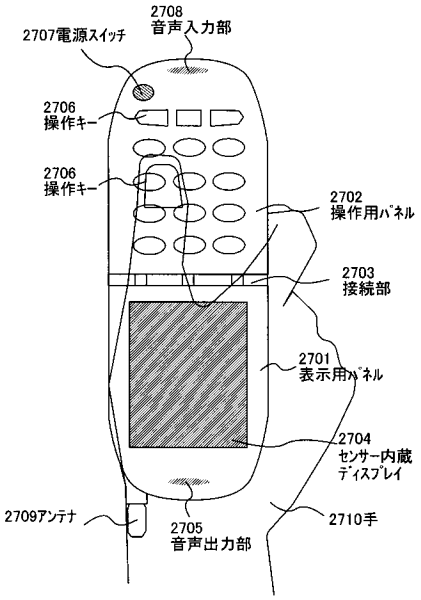
【図９】



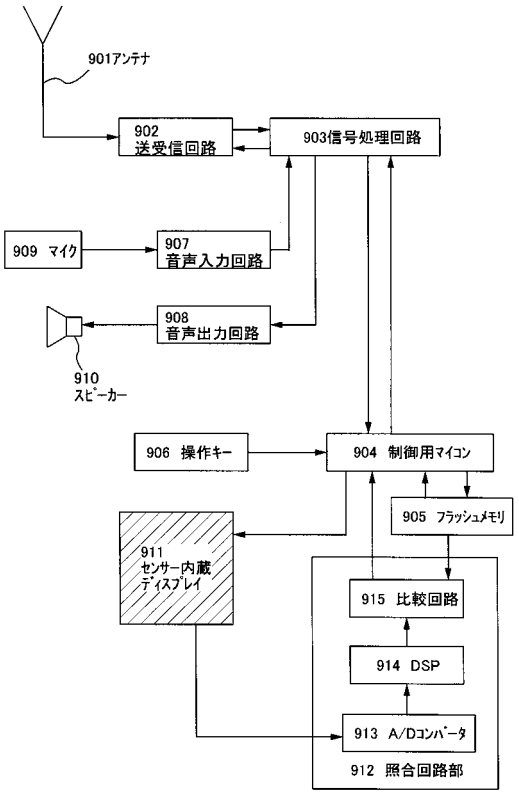
【図１０】



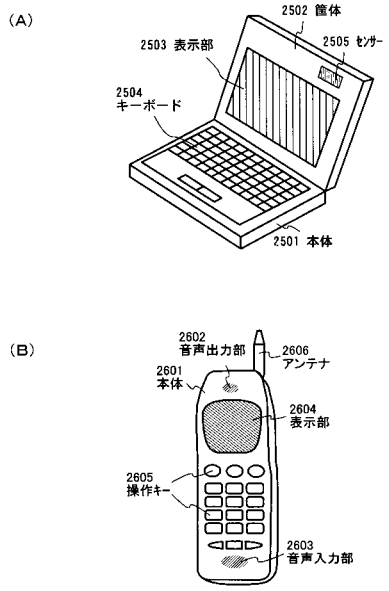
【図１１】



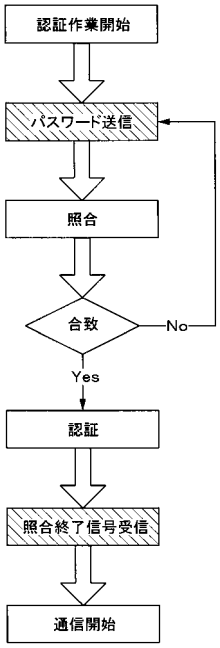
【図１２】



【図１３】


(A)
2502 筐体
2503 表示部
2505 ｾﾝｻｰ
2504
キーボード
2501 本体
(B)
2602
音声出力部
2606
アンテナ
2601
本体
2604
表示部
2605
操作キー
2603
音声入力部

【図１４】


認証作業開始
パスワード送信
照合
合致
No
Yes
認証
照合終了信号受信
通信開始

フロントページの続き

(56)参考文献 特表２０００－５１６７４６（ＪＰ，Ａ）
特開平１１－０８５７０５（ＪＰ，Ａ）
特開２００１－２４４９２６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/00 - 21/24