

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-63077

(P2005-63077A)

(43) 公開日 平成17年3月10日(2005.3.10)

(51) Int. Cl.⁷

G06T 7/00
A61B 5/117
H04Q 7/38

F I

G06T 7/00 510A
H04B 7/26 109R
A61B 5/10 320B
A61B 5/10 320C
A61B 5/10 320Z

テーマコード(参考)

4C038
5B043
5K067

審査請求 未請求 請求項の数 22 O L (全 64 頁) 最終頁に続く

(21) 出願番号 特願2003-290979(P2003-290979)
(22) 出願日 平成15年8月8日(2003.8.8)

(71) 出願人 500103384
株式会社アール・アンド・デー・アソシエイツ
大阪府大阪市中央区淡路町3丁目2番8号
トーア紡第2ビル501号
(71) 出願人 503128021
株式会社新興機材
東京都中央区入船3-5-10藤和入船ビル3階
(71) 出願人 397025314
明光産業株式会社
東京都中央区八重洲一丁目5番3号

最終頁に続く

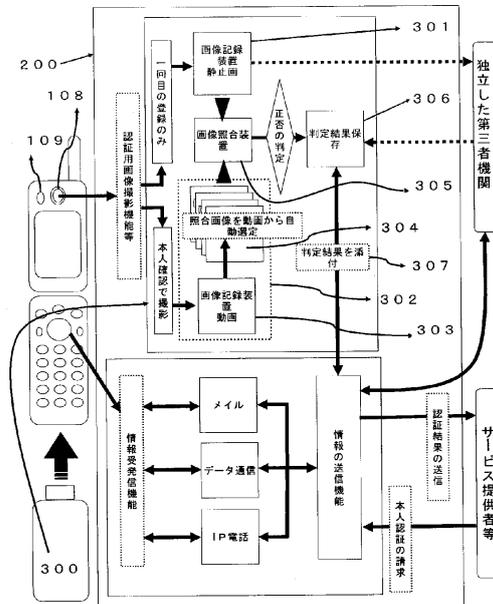
(54) 【発明の名称】 個人認証方法、個人認証装置及びコネクタ

(57) 【要約】

【課題】カメラ付携帯電話機等通信端末機器に搭載し、同機器の中だけで個人の認証を行い、個人情報やプライバシー情報をみだりに公開しないような良好な情報社会の建設に資する個人認証方法、装置及びシステムを提供すること。

【解決手段】カメラ108及び撮像フラッシュ装置109とを備えるカメラ付携帯電話機200の認証部タグ300は、原本画像記録装置301、認証時の顔画像データ処理部302、画像照合装置305、照合判定結果保存装置306、照合判定結果添付・送出装置307を持つ。認証時の顔画像データ処理部302は、撮像動画像記録装置303と静止画像選別装置304を有し、原本画像記録装置301は、カメラ付携帯電話機の所有者または占有使用者が携帯電話機を占有した時最初に撮影した自己の顔画像を記録し、認証要求がある通信の相手先に対して、照合判定結果を相手先に送付する照合判定結果添付・送出装置307を備える。

【選択図】 図2



【特許請求の範囲】**【請求項 1】**

個人の特徴原本データを取得するステップと、
前記特徴原本データを記憶するステップと、
前記特徴原本データを符号化するステップと、
前記符号化した特徴原本データを送信するステップと、
個人の特徴データを取得するステップと、
前記特徴データを符号化するステップと、
前記符号化した特徴原本データと前記符号化した特徴データとを照合するステップと、
該照合結果を送信するステップと
を備えることを特徴とする個人認証方法。

10

【請求項 2】

前記個人の特徴原本データが、生体情報に基づくものであることを特徴とする請求項 1 記載の個人認証方法。

【請求項 3】

前記生体情報が、顔画像、虹彩情報、網膜情報、耳介情報、指紋情報、掌紋情報、静脈パターン情報、声紋情報および遺伝子情報の少なくともいずれか 1 つであることを特徴とする請求項 2 記載の個人認証方法。

【請求項 4】

前記符号化した特徴原本データを記憶するステップを更に有することを特徴とする請求項 1 記載の個人認証方法。

20

【請求項 5】

前記符号化した特徴原本データが改竄されていないことを証明するための改竄防止情報を獲得するステップと、該改竄防止情報を通信手段によって第三者機関に保存するステップと、前記照合時に保存された情報から得られる改竄防止照合情報を前記第三者機関に送信するステップとをさらに備えることを特徴とする請求項 1 記載の個人認証方法。

【請求項 6】

前記個人の特徴原本データを取得するステップおよび前記個人の特徴データを取得するステップが、携帯電話、公衆電話、コンピュータ、自動販売機および無人サービス提供機であって、個人情報を入力する手段と、外部の公衆通信網を使って通信のやり取りが出来る通信手段とを備える装置によって行われることを特徴とする請求項 1 記載の個人認証方法。

30

【請求項 7】

前記携帯電話が、カメラ付携帯電話であることを特徴とする請求項 6 記載の個人認証方法。

【請求項 8】

前記自動販売機が、酒類、タバコまたは飲料の自動販売機であることを特徴とする請求項 6 記載の個人認証方法。

【請求項 9】

前記自動販売機が、交通機関または娯楽施設の自動券売機、有価証券類または住民票の自動発行機のいずれかであることを特徴とする請求項 6 記載の個人認証方法。

40

【請求項 10】

前記無人サービス提供機が、クレジットカードのキャッシュディスペンサーまたは金融機関の A T M 装置のいずれかであることを特徴とする請求項 6 記載の個人認証方法。

【請求項 11】

前記個人の特徴原本データを取得するステップおよび前記個人の特徴データを取得するステップが、
前記特徴原本データを記憶する手段と、
前記特徴原本データを符号化する手段と、
前記特徴データを符号化する手段と、

50

前記符号化した特徴原本データと前記符号化した特徴データとを照合する手段とを備えたコネクタを前記装置に挿入することにより行われることを特徴とする請求項 6 記載の個人認証方法。

【請求項 1 2】

前記特徴原本データおよび前記特徴データが、顔画像から抽出された顔特徴に基づくものであって、該顔画像は動画画像であることを特徴とする請求項 1 記載の個人認証方法。

【請求項 1 3】

前記動画画像から顔特徴を抽出するステップは、複数枚の画像から正面を向いた顔画像を選択するステップと、正面顔を検出するステップと、特徴を抽出するステップとを備えることを特徴とする請求項 1 2 記載の個人認証方法。

10

【請求項 1 4】

前記特徴原本データおよび前記特徴データが、顔画像から抽出された顔特徴に基づくものであって、前記記憶された符号化特徴原本データが、該顔特徴抽出に使用した顔画像の任意の 1 本の横線上の画素の濃度を加算したものであることを特徴とする請求項 4 記載の個人認証方法。

【請求項 1 5】

前記特徴原本データおよび前記特徴データが、顔画像から抽出された顔特徴に基づくものであって、前記改竄防止情報は、前記特徴原本データに係る画像の任意の 1 本の横線もしくは縦線上の画素、もしくは前記特徴原本データに係るデータのビット数の少なくともいずれか 1 つであることを特徴とする請求項 5 記載の個人認証方法。

20

【請求項 1 6】

前記個人の特徴原本データを取得するステップおよび前記個人の特徴データを取得するステップが、個人情報を入力する手段と、外部の公衆通信網を使って通信のやり取りが出来る通信手段とを備える装置によって行われ、前記改竄防止情報を通信手段によって第三者機関に保存するステップにおいて、該装置の登録 ID 番号も送信して、該番号を前記符号化した特徴原本データと同時に登録するステップとを、さらに備えることを特徴とする請求項 5 記載の個人認証方法。

【請求項 1 7】

前記個人の特徴原本データを取得するステップおよび前記個人の特徴データを取得するステップが、個人情報を入力する手段と、外部の公衆通信網を使って通信のやり取りが出来る通信手段とを備える装置によって行われ、前記改竄防止照合情報を第三者機関に送信するステップにおいて、該装置の登録 ID 番号も送信して、該番号を前記符号化した特徴原本データと同時に照合するステップとを、さらに備えることを特徴とする請求項 5 記載の個人認証方法。

30

【請求項 1 8】

個人の特徴原本データを取得するステップと、
前記特徴原本データを記憶するステップと、
動画画像から個人の特徴データを取得するステップと、
前記特徴原本データと前記特徴データとを照合するステップと、
該照合結果を送信するステップと
を備えることを特徴とする個人認証方法。

40

【請求項 1 9】

個人の特徴原本データを取得する手段と、
前記特徴原本データを記憶する手段と、
前記特徴原本データを符号化する手段と、
前記符号化した特徴原本データを送信する手段と、
個人の特徴データを取得する手段と、
前記特徴データを符号化する手段と、
前記符号化した特徴原本データと前記符号化した特徴データとを照合する手段と、
該照合結果を送信する手段と

50

を備えることを特徴とする個人認証装置。

【請求項 20】

個人の特徴原本データを取得する手段と、
前記特徴原本データを記憶する手段と、
動画像から個人の特徴データを取得する手段と、
前記特徴原本データと前記特徴データとを照合する手段と、
該照合結果を送信する手段と

を備えることを特徴とする個人認証装置。

【請求項 21】

個人の特徴原本データを記憶する手段と、
前記特徴原本データを符号化する手段と、
個人の特徴データを符号化する手段と、
前記符号化した特徴原本データと前記符号化した特徴データとを照合する手段と
を備え、前記個人の特徴原本データまたは前記個人の特徴データを取得する手段と情報受
発信手段とを有する装置に供されることを特徴とするコネクタ。

10

【請求項 22】

前記コネクタが、ICタグチップであることを特徴とする請求項 21 記載のコネクタ。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、予め個人が占有または所有する記録媒体に記録した照合用の個人情報を使っ
て公衆通信回線網を介してサービス提供者から要求された個人認証を行う場合に、照合に
必要な個人情報である生体情報である顔画像情報の他、虹彩情報、指紋情報、声紋情報、
遺伝子情報等を外部に送信しないで、すなわち個人情報やプライバシー情報をみだりに公
開しない個人認証が可能になる、よって良好な情報社会の建設に資する個人認証方法、個人
認証装置及びコネクタに関する。

20

【背景技術】

【0002】

携帯電話や情報端末がメールの送受信やテレショッピング、振り込みなどの金融操作や
社会的な契約手続きに利用されるようになり、実際に端末装置を操作しているのが間違い
なく本人かどうかを認証することが重要になっている。

30

【0003】

これまで一般に端末ユーザを認識する方法は、個人の認証を必要とするサービス提供者
が、個人の認証を請求する相手を識別する情報、例えばID番号、パスワード、指紋等を
予め自己のデータベースとして蓄積するか、もしくは相手から独立して情報を管理する第
三者機関に蓄積し、取引決済を必要とする要求時に相手から通信を介して送られてくる個人
識別情報と照合して本人の同一性を確認する方法を前提としている。

【0004】

そのために従前の認証システムでは、具体的な取引が発生する前に本人確認に必要な個人
を識別する情報をサービス提供者である相手側に提供しておく必要がある。

40

【0005】

従来、キー入力によってキーワードやID(Identifier)番号を入力して本人確認を行う
ケースが多かったが、昨今は生体情報による認証方法に移り始めている。パスワードやID
番号で行う認証方式に対して、指紋や虹彩、顔写真や遺伝子情報等、最もプライバシー
に係わる情報である生体情報をネットで相手側に送付することに対する国民の抵抗感がま
だまだ強い。また、電子決済等、ネットワークを介して認証する手続きで、一定の目的が
相互に確認されている商取引もしくは行政手続きを除いて、相手に事前に認証するための
個人識別情報を提供させることは個人情報保護法、もしくは全国の自治体で成立している
個人情報保護条例に抵触するという指摘がある一方で、運営体制上未知な部分がまだ多く
個人情報漏洩する危険性は少なくない。

50

【0006】

一方これまで実用化している生体情報を使用した認証方式としては、情報端末機器に本人の生体情報を登録して該機器の動作を制限する方式がこれまで提案されており、情報端末の操作そのものを制御する方式の他、外部へのアクセス制限を行うことで擬似的な認証を行っているものが多い。この認証方式は情報端末機器を操作する本人が取引きの決済責任を負うことを前提にしたものである。

【0007】

【特許文献1】特開2000-259828号公報

【特許文献2】特開2001-273498号公報

【非特許文献1】小杉 信、"個人識別のための多重ピラミッドを用いたシーン中の顔の探索・位置決め"、電子情報通信学会論文誌、Vol.J77-D-II, No.4, pp.672-681, April 1994 10

【非特許文献2】M.H.Yang et al "Detecting Faces in Images: A Survey" IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol.24, No.1, Jan. 2002.

【発明の開示】

【発明が解決しようとする課題】

【0008】

従前の認証方式の内、単純にID番号やパスワードによる本人確認と個人認証方式は、人間の記憶力に依存して設定するため、解読、漏洩の危険性が避けられない。その上、伝言や行為代行を他人に依頼することによって簡単に第三者の成り済ましが可能であり、情報端末を操作している人間が正当な利用者であるという決済手続きを、本人だけが記憶しているとは仮定したパスワード等で成立させようとする擬似的に認証する方法にすぎない。 20

【0009】

外部に個人情報や個人情報を予め提供する方法による認証方式では、個人を識別する生体情報を認証要求者である企業や行政機関に登録することは国民の側に抵抗が強い上、企業や行政機関が通信回線を通じてサービスを提供する前提条件で相手方に対して個人情報の提供を要求することが、個人のプライバシーや基本的人権の侵害にあたることとして避けるべきだとする意見がある。

【0010】

電子決済を個人が行うことを前提に、ネットワークを通じて個人に対して事前に個人識別情報の提供を要求することは、取引上の優越的地位を利用した要求と看做されても仕方が無い。個人が通信を介して相手から取引手続きに必要であるとして個人情報の登録を要求された場合、自ら提供した個人情報が相手側から開示された目的以外に利用された場合には、本人の意向に沿ってその事実を確認する方法が確立されていないため、個人情報を提供した相手側に他の目的で個人識別情報が利用される危険性を回避できないためである。 30

【0011】

個人情報保護法の観点から、利用者側の情報端末内に個人情報を登録して本人を認証する方法は、個人情報が外部に漏洩する危険性がない点で利用者側から見れば安心である。一方で認証要求者からみれば、情報端末内もしくは接続端子内で行われる本人確認手続きだけではあくまで自己申告であり、情報端末機器の認証手続きの延長にすぎない。社会的な認証として第三者に対する対抗要件になるかどうか疑問である。 40

【0012】

顔、虹彩、網膜、指紋、掌紋、声紋、遺伝子等、人間一人ひとりに固有の生体情報を使って本人確認をする技術はすでに世界各国で実用化されている。しかし、生体情報を使う本人確認や個人認証においては、事前に本人を特定しようとする側が相手から照合用の生体情報を取得したうえでデータベースとして保存しておく必要があること、また実際に本人確認を行う場合には、本人が通信網に接続された何等かの情報端末本に指定された個人情報を入力し、相手先にそのデータを送信しなければならないこと、この二つの必要要件によって、個人情報保護に対する安全性が完全に確保されることは難しい。

【0013】

問題の一つは、個人情報を提供して登録した相手先が、本人の意志に反して他の目的に利用することを防げないことである。一旦、本人を永久に特定出来る生体情報を外部に登録してしまえば、相手側から、盗難、改竄、処理ミス、管理ミス、不正な持ち出しなど、意図する意図しないに係わらず第三者に個人情報の漏洩事故の被害、犯罪の被害が発生して、拡散した個人情報を社会的に取り消すことは事実上不可能になる。また相手先が勝手に他の目的に利用した場合に、その事実を本人が確認し中止させる手立てが本人に確保されていないことがある。

【 0 0 1 4 】

問題のもう一つは、本人確認を要求された場合に本人が個人情報を送信せざるを得ないとすると、その要求を出した相手側が 1) 不正なアクセス、 2) 他人へのなりすまし、 3) パスワードの盗用、 4) 認定条件の虚偽と違反行為、 5) システム突破と破壊行為、 6) 第三者による通信データのピックアップ、 7) 第三者による通信データの改竄、 8) アクセス妨害、 9) アクセス否認、のような不正な行為を行っていないこと、相手側に成り済まし等がないこと、通信網の安全性を完全に担保されない限り、要求に応じて送信した個人情報が不正に利用される危険性が避けられないことである。

10

【 0 0 1 5 】

高度情報化社会では通信手段を使って様々な契約行為が行われるため、これまで対面によって成立していた認証方式に代わって、非対面を前提とする通信手段を介した認証方式の確立が急務となっている。対面を前提とした本人確認は、対面している相手に本人の特定が可能な資料（例えば運転免許証、パスポートなど）の提示を要求して本人を目視で見

20

【 0 0 1 6 】

これまで通信手段を介して本人を確認しようとする場合は、予め登録されたパスワードやICカードなどのデバイスを利用していた。ただしあくまでデバイスを鍵とするアクセス権限の認証にとどまっております、意図的な成り済ましや犯罪を完全に防止することは難しかった。最近ではその欠陥を補うためにパスワードやICカードより確実な認証手段として生体（バイオメトリクス）情報を活用することが推奨され、我が国では一部の企業や官庁でも採用されている。

【 0 0 1 7 】

情報端末間の情報通信で完結する情報システムは、情報端末を操作する人間ではなく情報端末機器の特定までがシステム技術の責任範囲である。現在、情報システムにアクセスした情報端末機器を操作する人間特定をしたい時に生体情報を使う場合、世界で通性となっている生体情報を使った個人認証方式では、相手先が入力する生体情報を照合するために、本人の特定を要求するサービス提供者側は要求した相手の生体情報を予め取得し登録しておかなければならないことになっている。

30

【 0 0 1 8 】

しかしOECDが取り決めた個人情報保護のガイドライン、また我が国で成立した個人情報保護法、さらに我が国の自治体の半数近くが制定している個人情報保護条例など、各々の条項では取得した個人情報は本人の確認なしに他目的に使用することが明確に禁止されていることから、将来生じうる可能性がある契約行為のために、近い将来、我々が高度

40

【 0 0 1 9 】

仮に、通信手段を介して決済を求められる都度、サービス提供者である相手側に本人確認の個人情報の利用について承諾を与えるという条件を設定した場合にも、相手側には「承諾を与えたのが本人である」という認証のために事前に本人の個人情報を提供しておかなければならないという矛盾が発生してしまう。

【 0 0 2 0 】

ほとんどの国民の感覚では、個人情報を他目的に使われることに抵抗があるのは事実で

50

あり、世界的に見て収集した個人情報の他目的利用が犯罪行為とされるのもその背景がある。そのために、我が国も含めて世界各国では、個人情報の取扱いに一定の制限を加えているが、高度情報化社会が現在、一般化している本人確認や個人認証方式のままであれば、電子決済における本人確認、個人認証においては、その規制や制限が根本から成立しなくならざるをえない。

【0021】

本発明は、このような根本的な矛盾を解決する個人認証方法とプログラム実行システムを確立させたものである。

【0022】

一般的に我々が身分を証明するにはIDカードを提示する方法と、第三者機関や人物に保証をもらう方法がある。相手側は提示されたIDや保証の内容を自ら定めた方法で確認した上で、自らの判断基準に基づいて認証する。この本人証明を受け入れる側は、もし提示された物や保証する者に対して不十分であると判断した場合は、相手に対してさらに確実な保証を求めて可能な限り認証の確実性を確保しようとする。

10

【0023】

この手続きを非対面による認証方式で考えれば、我々はできるだけ本人であることを証する材料を相手に提示することに努め、その材料の正当性を保証する手段を用意すること、相手は可能な限りリスクを回避する手続きを踏んでその提示を自ら判断すること、お互いの行為の中に必ずバランスの取れた解決方法を見出す他ないのである。これまでの社会における通常の見取りや契約行為で相手の指紋や掌紋を要求することは反社会的な行為であり、その反社会的なルールを前提とした個人認証方法は淘汰されなければならない。

20

【0024】

本発明は、このような過った前提で作られている現在の認証方式の矛盾を解決する個人認証方法とプログラム実行システムを実現させたものである。

【0025】

本人を正確に特定できる生体情報を利用した照合方式は、厳密な認証結果を要求する側にとっては極めて有効な認証手段であるが、認証される本人にとっては心理的に使って欲しくない、もしくは人権保護の立場からは使用を拒否すべきものであるとする人も少なくない。

30

【0026】

生体情報はあくまでも自己の意志で相手に提示すべき情報であって、安易に相手方のコントロール下に委ねるものではなくましてや認証を要求する側のデータベースとすることは間違いである。

【0027】

様々な契約関係が発生する社会で生活している我々は、その局面ごとに生体情報を提供することで、一部の組織や団体に個人の行動や思想を正確に把握される可能性を生じさせてしまう。その結果、一方的にある個人の行動や活動が掌握される可能性を感じるだけで人間は恐らく極めて不平等な人間関係を強要されたことと同じように感じる不安がどんどん膨らんでいくだろう。

40

【0028】

本発明は、個人の識別が可能な生体情報（顔、虹彩、網膜、指紋、掌紋、声紋、遺伝子等）による個人認証を要求する相手先に生体情報である個人情報の登録を不要にする認証方式を実現する個人認証方法、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッドを提供することを目的とする。個人が利用する情報通信端末に本人確認のために予め記録した照合用個人情報を使って、本人を識別することができる個人情報を外部に送信せずに、本人確認と個人認証を可能とするシステムであり、情報通信ネットワークを介して本人確認を要求する電子的な決済手続きにおいて、個人の識別が可能なバイOMETRICS個人情報（顔

50

、虹彩、指紋、声紋、遺伝子等)を、インターネットなどの通信システムで送受信する危険性を回避する個人認証方法、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッドを提供することを目的とする。

【0029】

ユビキタス時代を迎え私たちが利用する情報端末は私たちの生活の身の回りで増えて行くことは間違いなく、個人情報や外部に発信することなく相互に認証が可能な情報通信環境を実現する本発明は、情報化社会の健全化には不可欠な技術である。

【0030】

本発明は、顔画像データを外部送信せずにカメラ付携帯電話などの画像照合装置、方法、システムの開発を通して、通信網を介する契約行為に不可欠な本人確認手段として顔画像などの生体情報を利用し、個人の占有下にある情報端末内で照合手続きを完結させ照合結果だけを送信することで個人情報の漏洩など国民の不安を解消することを目的とする。

【課題を解決するための手段】

【0031】

本発明は、個人が特定できる生体情報を情報端末に入力することにより、端末に予め登録されている個人が特定できる原本情報と照合して本人確認を行い、その結果と、照合の根拠となる原本情報が改竄もしくは入れ換えられていないことを確認した結果を相手に送信するシステム、及びその装置、方法を実現する個人認証方法と個人認証方法とプログラム実行システムである。

【0032】

本発明に係る個人認証システムは、まず顔画像とカメラ付き携帯電話を使った個人認証方式で説明されるが、生体情報を外部に送信しないというシステムは、顔、虹彩、網膜、指紋、掌紋、声紋、遺伝子等、人間一人ひとりに固有の情報においても、個人情報の入力デバイスの違いはあっても、全く同じ認証方式で成立する。根本的な原理は、採用された生体情報を、本人が占有または所有する情報端末機器もしくはその機器に接続して使用する拡張端子内に保存し、外部に送信しないこと、保存された生体情報の原本性を証明する改竄防止照合情報のみを、外部の第三者に登録し、情報端末を使って本人確認をした結果と非改竄の証明データのみを相手先に送信する、となる。

【0033】

顔画像を利用したカメラ付き携帯電話による本人確認と個人認証方式は、所有者または占有使用者が特定できるカメラ付き携帯電話の内部、もしくはカメラ付き携帯電話の外部接続端子で携帯電話機本体に接続されたコネクタもしくはコンピュータの内部に、個人照合のための特徴原本データとして撮像した顔特徴を記憶する記憶部と、該カメラ付き携帯電話のカメラで顔画像を撮像する撮像部と、該顔画像から照合要求時顔特徴を抽出する抽出部と、前記特徴原本データと照合要求時顔特徴とを照合する照合部と、該顔情報照合結果をサービス提供先に送信する第1送信部と、前記特徴原本データを作成するために使用した初使用時顔画像を符号化したデータを、前記特徴原本データが改竄されていないことを証明する改竄防止符号原本データとして第三者機関に送信する第2送信部と、前記照合要求時顔特徴を符号化したデータを改竄防止符号照合データとして前記第三者機関に送信する第3送信部とを備えるカメラ付き携帯電話機と、前記送信された改竄防止符号原本データを保存する改竄防止符号原本保存部と、該改竄防止符号原本データと前記送信された改竄防止符号照合データとを照合する改竄防止用照合部と、該照合結果である改竄防止用照合結果を前記サービス提供先に送信する改竄防止用照合結果送信部とを備える第三者機関と、前記送信された顔情報照合結果を受信する第1受信部と、前記送信された改竄防止用照合結果を受信する第2受信部と、該顔情報照合結果及び改竄防止用照合結果をもって前記照合要求者の真正を判断する判断部とを備えるサービス提供先とを具備している。

【0034】

前記の顔画像とカメラ付き携帯電話による認証方式に用いた生体情報は、虹彩、網膜、

10

20

30

40

50

静脈パターン、指紋、掌紋、声紋、遺伝子、いずれかの情報であっても本発明にかかる個人認証方法とプログラム実行システムは変わらない。

【0035】

すなわち、上記課題は、以下の本発明により解決される。

【0036】

カメラ付き携帯電話内、あるいは携帯電話機の外部接続端子に接続されるコネクタもしくはコンピュータに内装され、カメラ付き携帯電話機の使用者の顔特徴を、個人照合のための特徴原本データとして記憶するステップと、カメラ付き携帯電話のカメラで動画を撮像するステップと、該動画から顔特徴を抽出するステップと、前期特徴原本データと顔特徴とを照合するステップと、該照合結果を相手方に送信するステップとを備えることを特徴とするカメラ付き携帯電話機に接続して本人確認を行う個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

10

【0037】

該特徴原本データを作成するために使用した顔画像データを符号化するステップと、符号化したデータを、特徴原本データが改竄されていないことを証明する改竄防止符号原本として保存するステップとをさらに備えることを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

20

【0038】

該特徴原本画像情報(特徴原本データ)を符号化し、該特徴原本情報が改竄されていないことを証明するための改竄防止情報を獲得するステップと、該改竄防止情報を通信手段によって第三者機関に保存するステップと、前記照合時に保存された情報から得られる改竄防止照合情報を前記第三者機関に送信するステップとをさらに備えることを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

30

【0039】

該特徴原本データを記憶するステップは、カメラ付き携帯電話、もしくは携帯電話機に接続する個人認証用のコネクタもしくはコンピュータの使用開始時に、カメラ付き携帯電話のカメラ機能によりコネクタの所有者または占有使用者の顔を撮像するステップと、撮像した顔画像から顔特徴を抽出するステップと、顔特徴を記憶するステップとを備えることを特徴とするコネクタもしくはコンピュータに搭載される個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

40

【0040】

該動画から顔特徴を抽出するステップは、複数枚の画像から正面を向いた顔画像を選択するステップと、正面顔を検出するステップと、特徴を抽出するステップとを備えることを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0041】

該改竄防止符号原本データは、照合用の前記特徴原本作成に使用した顔画像の任意の1本の横線上の画素の濃度を加算したものであることを特徴とする個人認証方法、プログラ

50

ム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0042】

カメラ付き携帯電話機の外部接続端子に接続されるコネクタもしくは接続したコンピュータに内装されている本人確認認証プログラムと携帯電話機を中継して外部にデータの送信を行う装置と、同装置から送るデータによって携帯型電話機の機能を可能にすることを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

10

【0043】

該コネクタのプログラムは、カメラ付き携帯電話機の電源によって動作し、携帯電話機の操作ボタンを使ってプログラムを起動することを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0044】

該コネクタをカメラ付き携帯電話に最初に差し込んだ段階で撮影装置を起動して撮像した画像は、コネクタ内蔵の記録装置に原本画像として登録することを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

20

【0045】

該コネクタ内の記録装置に保存した改竄防止符号原本データが、本体の携帯電話を中継して外部の第三者機関に送信され、認証保証センターの専用サーバに記録されるようにプログラムされていることを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

30

【0046】

該改竄防止符号原本データは、前記特徴原本画像情報（特徴原本データ）に係る画像の任意の1本の横線もしくは縦線上の画素、もしくは前記特徴原本情報に係るデータのビット数の少なくともいずれか1つであることを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

40

【0047】

該改竄防止符号原本データを送信する装置には、外部の第三者機関の通信先が予め指定されており、カメラ付き携帯電話のデータ通信機能によって送信することを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0048】

該コネクタ内に保存される改竄防止符号原本データは自動的に複数のデータを保存しており、第三者機関に登録する改竄防止符号原本データは本人確認手続きを行う度に、保存

50

してある複数の原本の非改竄を証明するデータを入れ替える機能を有する個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0049】

該第三者機関に改竄防止符号原本データを登録する時、使用するカメラ付き携帯電話、もしくはコネクタやコンピュータの登録ID番号を送信して該番号を改竄防止符号原本データと同時に登録する機能をもつ個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

10

【0050】

該第三者機関に登録した改竄防止符号原本データを参照する場合、使用するカメラ付き携帯電話、もしくはコネクタやコンピュータの登録ID番号を送信して該番号を改竄防止符号原本データと同時に照合する機能をもつ個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0051】

該原本画像改竄防止用データが、カメラ付き携帯電話から最初にコネクタに画像を送信して登録された場合に前項のプログラム実行装置で抽出された改竄防止符号原本データを、カメラ付き携帯電話の通信機能を使って外部の認証機関に自動的に送信する個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

20

【0052】

携帯電話機の通信をオフすることなく、外部の第三者から受信した原本画像の非改竄を証明するデータと、コネクタ内で照合した結果を含む記憶装置に記憶されている各種の情報を一緒に通信中の相手先に送信する個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

30

【0053】

該携帯電話機を使った通信で、通信の相手先から本人確認と個人認証を請求された際に、携帯電話機の電話通信を維持したまま、外部の第三者から受信した原本画像の非改竄を証明するデータと、コネクタ内で照合した結果を一緒にして相手先に該データの PACKET 通信が可能な個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

40

【0054】

該携帯電話機を使った通信で、本人確認と個人認証を請求された際に、携帯電話機のメール通信機能を使って、外部の第三者から受信した原本画像の非改竄を証明するデータと、コネクタ内で照合した結果を添付して、カメラ付き携帯電話で作成したメール本文と一緒に相手先に送信可能な個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

50

【0055】

本人確認認証プログラム実行装置を内装したコネクタが外部接続端子に差し込まれている状態で、本体のカメラ付き携帯電話の操作機能を使ってコネクタ内の各種プログラムを有効とするモードが設定されている個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0056】

本人確認認証プログラムを実行するプログラム実行装置に外部からのデータを受信させる個人認証方法とプログラム実行システムにおいて、前記プログラム実行装置とカメラ付き携帯電話が接続され、携帯電話機が受信したデータを変換して前記プログラム実行装置に送る中継装置を有することを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

10

【0057】

該中継装置は、前記カメラ付き携帯電話から送られる動画像データから静止画像を抽出して記憶する装置と、原本画像と照合可能なコネクタ対応のデータに変換する装置を含むことを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

20

【0058】

照合の実行を可能とするプログラムによって、カメラ付き携帯電話で撮像された顔画像を読み取って原本として記録された記録媒体と、本人確認用に撮像された動画像から照合顔画像データを抽出するステップと具体的に照合して正解率を計算するステップを一体的に処理できるプログラムを搭載したチップを内装することを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

30

【0059】

カメラ付き携帯電話の使用者の顔特徴を、個人照合のための特徴原本データとして記憶する記憶部と、該カメラ付き携帯電話のカメラで顔画像を撮像する撮像部から送られた画像データと、該顔画像から照合要求時に顔特徴を抽出する抽出部と、前記特徴原本データと照合要求時の顔特徴とを照合する照合部と、該顔情報の照合結果をサービス提供先に送信する第1送信部と、前記特徴原本データを作成するために使用した初使用時の顔画像を符号化したデータを、前記特徴原本データが改竄されていないことを証明する改竄防止符号原本データとして第三者機関に送信する第2送信部と、前記照合要求時の顔特徴を符号化したデータを改竄防止符号照合データとして前記第三者機関に送信する第3送信部とを備えるカメラ付き携帯電話機、コネクタもしくはコンピュータと、前記送信された改竄防止符号原本データを保存する改竄防止符号原本保存部と、該改竄防止符号原本データと前記送信された改竄防止符号照合データとを照合する改竄防止用照合部と、該照合結果である改竄防止用照合結果を前記サービス提供先に送信する改竄防止用照合結果送信部とを備える第三者機関と、前記送信された顔情報照合結果を受信する第1受信部と、前記送信された改竄防止用照合結果を受信する第2受信部と、該顔情報照合結果及び改竄防止用照合結果をもって前記照合要求者の真正を判断する判断部とを備えるサービス提供先とを具備することを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、（各種）コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、か

40

50

かる認証の仕組みを実現したビジネス・メソッド。

【0060】

該個人照合用の情報が、顔画像だけではなく、他の生体情報である、虹彩情報、網膜情報、耳介情報、指紋情報、掌紋情報、静脈パターン情報、声紋情報、遺伝子情報の少なくともいずれか1つであることで代換可能なシステムであることを特徴とする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0061】

該個人照合用の生体情報の読み取りについて、上記に記載されたカメラ付き携帯電話のカメラによる顔画像の撮像機能を使った入力方式の他に、指紋や掌紋情報を取り込む光学方式、静電方式、感熱方式、電界方式、圧力方式などのセンサー機能をもつ入力デバイス、声紋情報を取り込むマイクロフォン、遺伝子情報をスキャニングするセンサー機能をもつ入力デバイスを使用して取り込んだ生体情報を使って本人確認を行う個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0062】

該通信手段を持つカメラ付き携帯電話に代えて、顔特徴情報の他、情報、網膜情報、耳介情報、指紋情報、掌紋情報、静脈パターン情報、声紋情報、遺伝子情報などを読み取ることの出来るカメラ、センサー、テンキー等の個人情報を入力する装置と、外部の通信網を使って通信のやり取りが出来る通信手段とを備えた情報処理装置に対して有効となる個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0063】

該個人情報を入力する装置と、外部の公衆通信網を使って通信のやり取りが出来る通信手段とを備えて第三者機関による個人認証用の生体情報の原本性を証明が可能な情報処理装置が取り付けられた、酒類、タバコ、飲料等の自動販売機、交通機関、娯楽施設の自動券売機、有価証券類、住民票等の自動発行機、クレジットカードのキャッシュディスプレイ、金融機関のATM装置、公衆電話機など事業者のサービス提供用の機器において、自動的に本人確認を行うことを可能にする個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【0064】

該動画像から抽出する静止画像を使って照合する認証方式、及び前述の個人認証方法とプログラム実行システムは、サービス提供者もしくは利用者本人が簡易な認証で構わないと判断した場合は、顔画像を静止画として撮像して照合することも可能な発明であり、カメラ付き携帯電話やその外部接続端子に接続する様々な認証機能を備えて情報端末機器の情報処理能力(主に処理速度及び記録容量)を勘案して、静止画による照合も可能な機能を包含するものとして設計された個人認証方法、プログラム実行システム、個人認証装置、コネクタ、個人認証システム、認証タグ、及び、該認証タグを搭載した車輛、(各種)コンピュータ、機械、電化製品、自動販売機、チップ、専用機、工作機械、その他機械、並びに、かかる認証の仕組みを実現したビジネス・メソッド。

【発明の効果】

【0065】

10

20

30

40

50

本発明によって、通信手段を介して相手側から本人確認を求められた場合でも、プライバシー情報である個人情報、特に永久に個人を特定できる生体情報を自ら管理する情報端末機器、あるいは該機器に接続する拡張端子や記録装置から、外部に個人情報を提供しないで精度の高い本人確認を成立させることができると同時に、認証を要求するサービス提供者もリスクの大きい個人情報を預かることをしないで、電子決済に不可欠である本人確認を行うことができるようになる。

【0066】

すなわち、本発明によれば、下記の成果が達成される。

【0067】

生体情報を外部送信しないで本人確認を行う。

10

【0068】

今回の技術開発は、本人の確認手段として保有する情報端末内で生体情報を使った本人を特定する照合手続きを完結させその照合結果だけを相手に提示するものである。情報端末に登録された照合用の原本情報は書換えもしくは改竄ができないような機構で保護されているが、さらに通信の相手が本人確認をより確実に行えるように、その照合に必要な視認もしくは確認する代わりに通信手段を通じて照合の原本になったデータの正当性を第三者に保証してもらう方式の採用を前提としている。

【0069】

第三者による個人情報の他目的利用を防止する。

【0070】

前項の方式によって照合に不可欠な生体情報を一切相手方もしくは第三者に提供しないため、相手側は要求した本人確認の結果の正当性を自ら判断し認証した後は個人情報を保管する必要は全くなく、本人確認情報を提供した個人は、個人情報保護法でも禁止されている個人情報を他目的に利用される心配がなくなることになる。

20

【0071】

認証用のデータを相手に渡さない。

【0072】

個人の生体情報は、個人の本人認証にとって有効な手段であることは否定しないが、本人を特定できる生体情報の活用の前提はあくまで本人の意志と判断でコントロールできる範囲で止めておくべきである。認証に必要なだという理由で本人確認手段である生体情報を相手に登録してはならない、ということは国民感情からいっても当然であろう。

30

【0073】

これまで本人確認の際に運転免許証やパスポートは常時本人の管理下にあり、相手の求めに応じて必要な部分（封印された顔写真もしくは署名）を相手方に提示するだけである。それらを相手に預けることはなく、ましてや発行者以外の人間が、照合用に運転免許証やパスポートの原本を保管するなどということはいない。

【0074】

1948年の世界人権宣言を契機に、国際社会では人類共通の価値として基本的な人権を擁護する思想がすでに世界で確立しており、高度情報化社会に向けた動きは世界的規模で加速する一方、社会的な関心事として個人情報保護をさらに強化して法制化する流れは世界的な規模で定着しつつある。

40

【0075】

本発明は、高度に情報化された社会において通信手段を介して日常的な決済や契約手続きを行うことが急速に増加することは確かななか、通信手段を介した電子決済手続きで、もっとも大事な個人の識別情報である生体情報を、第三者が個人に対して事前に登録することを求めることなしに、かつ、個人情報そのものを本人の管理下でない情報システムに提供しないで、個人認証を可能にする技術を提案している。

【0076】

これまでの社会では、何等かの社会的な契約行為を決済する場合に、当事者がお互いに面談することによって相互に相手方を契約行為の正当な当事者として承認する、また第三

50

者による当事者の正当性の保証もしくは証明行為とそれを証する証書、あるいは公的機関による証明行為とそれを証する証書によって客観的に成立していたが、情報化社会ではそのような決済行為に代わる具体的な手続きの確立が必要になる。

【0077】

実際に、これまで我が国だけではなく世界各国では様々な技術が提案され、数多くの認証に必要な技術が使われて電子的決済が一般的に行われるようになってきている。しかし数多くの企業、団体、個人によって様々なサービスが提供されることで、サービスを利用しその利益を享受する利用者のアクセス先とアクセス数が増え、それに従って本人の生活や仕事に係わって蓄積された個人情報、幾何級数的にサービス提供者のデータファイルやサーバーシステム、さらには個々のサービス提供者が意図しない形でネットワーク上に蓄積されることは避けられなくない。そのため情報通信システムを利用している個人の意志や、サービスを提供している個々の企業や行政組織の意に反して、個人情報の漏洩の危険性が極めて大きくなっている。

10

【0078】

本発明は、個人を識別できる生体情報を一切外部に登録せずに、通信手段を介して電子決済が可能な認証の構造を実現させるものである。個人が自ら管理する認証用の個人情報の原本性を保証するサービス提供者である第三者機関によるデータ照合によって実現する。本発明は、ユビキタス時代の到来で予想されている日常生活のあらゆる場面で接することになる情報端末機器（コンピュータ、電話機、モバイル端末、情報家電、車両制御システム、自販機、券売機、発券機など）や情報デバイス（ICカード、メモリーカード、ICタグ、など）もしくはその両方の機能を兼ね備えた複合的な情報アクセスインターフェイスをもった情報装置や設置管理者に対して、個人情報を提供しないで自己を証明して情報化社会の利便性を徹底的に追求すると同時に、個人情報保護を徹底し個人情報の自己管理権を確立させるものである。

20

【発明の概要】

【0079】

A. カメラ付き携帯電話と第三者認証機関を使った本人確認の決済システムに必要な装置とその方法について

- 1) カメラ付き携帯電話を使った個人認証装置と本人確認の方法
- 2) カメラ付き携帯電話用の個人認証タグと本人確認の方法
- 3) 携帯電話を使う成り済みが不可能なクレジットカード決済(1)
- 4) 携帯電話を使う成り済みが不可能なクレジットカード決済(2)

30

上記のカメラ付き携帯電話および個人認証タグに関する発明において、本人確認に使う個人を特定する生体情報である顔画像を使った「原本画像」「照合画像」は各々、個人を識別する生体情報である「指紋」「掌紋」「静脈パターン」「声紋」「虹彩」「遺伝子」「耳介形状」「署名形状」「筆圧データ」などに置き換えるて記述することが出来る。その場合、本発明に記述しているカメラ付き携帯電話の撮像装置は、上記の各生体情報を入力する装置と読み替えることを前提としている。またカメラ付き携帯電話の撮像装置並びに照合装置、通信装置などは、コンピュータとデジタルカメラ、PDA、スマートテレホンでも同じ機構で本発明を完全に再現し全く同じ機能を実現できる。

40

- 1) カメラ付き携帯電話を使った個人認証装置と本人確認の方法
- < 携帯電話の所有者と利用者が同一であることを証明するシステム >

原本画像 = 携帯電話に保存する原本となる顔画像情報

照合画像 = 携帯電話で入力した照合するための顔画像情報

< 本発明の技術的課題を実現する構成 >

携帯電話に顔画像情報を入力する撮像装置

撮像した動画像から複数の照合画像を抽出する装置

原本画像と照合画像を照合する装置

原本画像と照合画像の正解率を算出した照合結果を指定したアドレス先に送信する通信装置

50

原本画像の改竄、取替、修正、消去が出来ない保存装置
 原本画像の非改竄を証明するデータを保存した原本画像から抽出する装置
 原本画像から抽出した非改竄を証明するデータを指定したアドレス先に送信する通信装置
 原本画像の非改竄を証明するデータを送信する際に同データを暗号化する装置
 電話会社に携帯電話の電話番号と所有者を登録した後、最初の撮像操作で入力された画像
 情報を携帯電話の保存装置に登録して原本画像とするプログラム
 携帯電話から送信された原本画像の非改竄証明データを携帯電話番号と関連付けて保存す
 る装置。
 携帯電話から送信された原本画像の非改竄データを照合してその結果を送信された携帯電
 話、または指定された相手先に自動的に返信する装置。

10

< 提案方法 >

本人確認の手順；原本非改竄証明付 = 証明添付型
 携帯電話を操作して本人確認の画像照合プログラムを起動し、携帯電話の撮像装置で撮像
 した照合画像と保存してある原本画像と照合し、正解率を算出して一時保存し、原本保存
 装置から非改竄証明データを抽出し、通信装置を介して同データを第三者機関に送信し、
 第三者機関に登録してある非改竄データと照合した結果を受信し、一時的に携帯電話に保
 存してあった正解率と受信した非改竄の証明データを相手先に送信する。

本人確認の手順；非改竄証明付き = 第三者証明型

携帯電話を操作して本人確認の画像照合プログラムを起動し、携帯電話の撮像装置で撮像
 した照合画像と保存してある原本画像と照合し、正解率を算出して相手先に送信する。一
 方、携帯電話を操作して原本非改竄証明データを抽出し、第三者機関に非改竄証明データ
 を送信する。第三者機関は送信された非改竄証明データを登録してある非改竄データと照
 合してその結果を指定された相手先に送信する。

20

本人確認の手順；非改竄証明なし = 簡易型

携帯電話を操作して本人確認の画像照合プログラムを起動し、携帯電話の撮像装置で撮像
 した照合画像と保存してある原本画像と照合し、正解率を算出して相手先に送信する。

2) カメラ付き携帯電話用の個人認証タグと本人確認の方法

< 個人認証タグの登録者と利用者が同一であることを証明するシステム >

個人認証タグ = カメラ付き携帯電話の外部接続端子に差し込んで利用する本人確認専用の
 装置

30

原本画像 = 個人認証タグに保存する原本となる顔画像情報

照合画像 = 携帯電話で入力した照合するための顔画像情報

< 本発明の技術的課題を実現する構成 >

個人認証タグに顔画像情報を入力する携帯電話の撮像装置

携帯電話で撮像した動画像から原本画像と照合する複数の照合画像を抽出する装置

原本画像と照合画像を照合する個人認証タグに搭載する装置

個人認証タグで照合して正解率を算出した結果を指定したアドレス先に送信する通信シス
 テム

原本画像の改竄、取替、修正、消去が出来ない保存装置

原本画像の非改竄を証明するデータを保存した原本画像から抽出する装置

40

原本画像から抽出した非改竄を証明するデータを指定したアドレス先に送信する通信シス
 テム

原本画像が非改竄であることを証明するデータを送信する際に同データを暗号化する装置
 携帯電話の外部接続端子に差し込んで最初の撮像操作で入力された画像情報を個人認証タ
 グの保存装置に登録して原本画像とするプログラム

個人認証タグの非改竄証明データを携帯電話番号と関連付けて送信する装置。

携帯電話から送信された原本画像の非改竄データを照合してその結果を送信された携帯電
 話、または指定された相手先に自動的に返信する装置。

< 提案方法 >

本人確認の手順；非改竄証明付き = 証明添付型

50

携帯電話を操作して同外部接続端子に差し込まれた個人認証タグの本人確認の画像照合プログラムを起動し、携帯電話の撮像装置で撮像した照合画像と個人認証タグの原本画像と照合し、正解率を算出して一時保存し、個人認証タグから原本非改竄証明データを抽出し、携帯電話の通信装置を介して同データを第三者機関に送信し、第三者機関に登録してある非改竄データと照合した結果を受信し、一時的に携帯電話に保存してあった正解率と受信した非改竄の証明データを相手先に送信する。

本人確認の手順；非改竄証明付き = 第三者証明型

携帯電話を操作して同外部接続端子に差し込まれた個人認証タグの本人確認の画像照合プログラムを起動し、携帯電話の撮像装置で撮像した照合画像と個人認証タグの原本画像と照合し、正解率を算出して相手先に送信する。一方、携帯電話を操作して個人認証タグから原本非改竄証明データを抽出し、第三者機関に非改竄証明データを送信する。第三者機関は送信された非改竄証明データを登録してある非改竄データと照合してその結果を指定された相手先に送信する。

10

本人確認の手順；非改竄証明なし = 簡易型

携帯電話を操作して同外部接続端子に差し込まれた個人認証タグの本人確認の画像照合プログラムを起動し、携帯電話の撮像装置で撮像した照合画像と個人認証タグの原本画像と照合し、正解率を算出して相手先に送信する。

3) 携帯電話を使う成り済ましが不可能なクレジットカード決済(1)

<クレジットカードで所有者(登録者)と利用者の同一性を保証する携帯電話>

20

携帯電話 = 動画撮像が可能なカメラ付き携帯電話

原本画像 = 携帯電話に保存する原本となる顔画像情報

照合画像 = 携帯電話で入力した照合するための顔画像情報

カード利用者 = クレジットカード決済でサービスを提供する営業者

カード所有者 = クレジットカードの所有名義人

カード発行者 = クレジットカードを発行して請求金額の決済を行う者

第三者認証機関 = 携帯電話所有者が本人確認機能付きの携帯電話を購入または占有して本人確認用の機能を申込んだ場合、原本画像の非改竄証明を得るために非改竄データを登録する機関。

(携帯電話会社、クレジット会社、保険会社、認証專業会社、その他独立の会社または公的団体が運営する)

30

<本発明の技術的課題を実現する構成>

カード利用者サイド

クレジットカードの番号の読取り機能を備えたカード所有者に対する請求金額を入力できる機能と、カード所有者の携帯番号入力が可能で、請求金額のデータといっしょにカード発行者に送信できる機能を有する装置

カード所有者がカード発行者に登録済の携帯電話番号を携帯電話器から直接入力できる装置

カード所有者が提示する電話番号をテンキーから入力できる装置

カード所有者サイド/クレジットカード決済を代用できる携帯電話

40

携帯電話に顔画像情報を入力する撮像装置

撮像した動画像から複数の照合画像を抽出する装置

原本画像と照合画像を照合する装置

原本画像と照合画像の正解率を算出した照合結果をカード発行者が指定するメールアドレスに自動的に送信する通信装置

原本画像の改竄、取替、修正、消去が出来ない保存装置

原本画像の非改竄を証明するデータを保存した原本画像から抽出する装置

原本画像から抽出した非改竄を証明するデータをカード発行者が指定したアドレス先に自動的に送信する通信装置

原本画像の非改竄を証明するデータを送信する際に同データを暗号化する装置

50

カード所有者が電話会社に携帯電話の電話番号と所有者の個人情報を登録した後、最初の撮像操作で入力された画像情報を携帯電話の保存装置に登録して原本画像とするプログラム

カード所有者が携帯電話から送信された原本画像の非改竄証明データを携帯電話番号と関連付けて保存する装置。

カード発行者サイド

カード所有を希望する者から送られてきた申込書に記載してある携帯番号を登録するサーバ装置

同上の携帯電話番号の所有者の個人情報（氏名、生別、住所、生年月日）名が、電話会社に登録された所有者の個人情報と同じであることを自動的に確認する装置

10

携帯電話によるクレジット決済を開始するパスワードを記入した秘匿性のあるハガキを同上の所有者の住所地に送付する装置

カード利用者から送信された請求金額とカード利用者名をカード所有者の携帯電話に転送する装置

カード所有者が登録してある携帯電話番号から、請求金額の承認と本人確認の照合結果を受信する装置。

カード所有者が原本画像の非改竄証明データを登録してある第三者認証機関から送信された原本証明結果を受けて、前項の請求金額の承認結果をカード利用者へ送信する装置

第三者認証機関サイド

携帯電話から送信された原本画像の非改竄データを照合してその結果を送信された携帯電話、またはカード発行者から指定されたアドレス先に自動的に返信する装置。

20

< 提案方法 >

クレジット決済の手順；本人確認と第三者認証を行う場合

カード利用者へ携帯電話番号を提示し、カード利用者は店頭で決済端末で携帯電話番号と請求金額を入力し、カード発行者が指定するセンターのデータを送信し、カードセンターはそのデータとカード利用者の店舗名等を携帯電話にメール送信する。

同データを受信したカード所有者は請求金額、店舗名、請求年月日を確認し、携帯電話を操作して本人確認の画像照合プログラムを起動し、携帯電話の撮像装置で撮像した照合画像と保存してある原本画像と照合し、正解率を算出して相手先に送信する。

カード所有者は、携帯電話を操作して原本非改竄証明データを抽出し、第三者機関に非改竄証明データを送信する。第三者機関は送信された非改竄証明データを登録してある非改竄データと照合してその結果をカード発行者へ指定された相手先に送信する。

30

カード発行者は第三者認証機関から送信された原本非改竄証明を確認したうえで、カード所有者から送信された決済承認データを元に、カード利用者へ決済完了の通知を送信し、カード利用者はそのデータを確認して全ての手続きを完了する。

本人確認の手順；非改竄証明なし＝簡易型

カード利用者へ携帯電話番号を提示し、カード利用者は店頭で決済端末で携帯電話番号と請求金額を入力し、カード発行者が指定するセンターのデータを送信し、カードセンターはそのデータとカード利用者の店舗名等を携帯電話にメール送信する。

同データを受信したカード所有者は請求金額、店舗名、請求年月日を確認し、携帯電話を操作して承認済の証としてメールをカード発行者が指定するセンターへ返信する。

40

カード発行者は、カード所有者から送信された決済承認データを元に、カード利用者へ決済完了の通知を送信し、カード利用者はそのデータを確認して全ての手続きを完了する。

4) 携帯電話を使う成り済みが不可能なクレジットカード決済(2)

< クレジット決済で所有者(登録者)と利用者の同一性を保証する認証タグ >

携帯電話 = 動画撮像が可能なカメラ付き携帯電話

認証タグ = 携帯電話の外部接続端子に差し込んで使用する本人確認専用の認証タグ

原本画像 = 携帯電話に保存する原本となる顔画像情報

照合画像 = 携帯電話で入力した照合するための顔画像情報

50

- カード利用者 = クレジットカード決済でサービスを提供する営業者
 カード所有者 = クレジットカードの所有名義人
 カード発行者 = クレジットカードを発行して請求金額の決済を行う者
 認証機関 = クレジット会社または独立した機関が認証タグに保存されている原本画像の非改竄性証明を行う機関
 (携帯電話会社、クレジット会社、保険会社、認証専業会社、その他独立の会社または公的団体が運営することも可能である)
 <本発明の技術的課題を実現する構成>
 カード利用者サイド
 クレジットカードの番号の読取り機能を備えたカード所有者に対する請求金額を入力できる機能と、カード所有者の携帯番号入力が可能で、請求金額のデータといっしょにカード発行者に送信できる機能を有する装置 10
 カード所有者がカード発行者に登録済の携帯電話番号を携帯電話器から直接入力できる装置
 カード所有者が提示する電話番号をテンキーから入力できる装置
 カード所有者サイド/クレジットカード決済を代用できる個人認証タグと携帯電話
 個人認証タグに顔画像情報を入力する携帯電話の撮像装置
 携帯電話で撮像した動画像から原本画像と照合する複数の照合画像を抽出する装置
 原本画像と照合画像を照合する個人認証タグに搭載する装置
 個人認証タグで照合して正解率を算出した結果を指定したカード発行者のアドレス先に送信する通信システム 20
 原本画像の改竄、取替、修正、消去が出来ない保存装置
 原本画像の非改竄を証明するデータを保存した原本画像から抽出する装置
 原本画像から抽出した非改竄を証明するデータをカード発行者が指定したアドレス先に自動的に送信する通信装置
 原本画像が非改竄であることを証明するデータを送信する際に同データを暗号化する装置
 カード所有者がカード発行者から送られた電話会社に携帯電話の電話番号と所有者の個人情報登録した後、最初の撮像操作で入力された画像情報を携帯電話の保存装置に登録して原本画像とするプログラム
 携帯電話の外部接続端子に差し込んで最初の撮像操作で入力された画像情報を個人認証タグの保存装置に登録して原本画像とするプログラム 30
 個人認証タグの非改竄証明データを携帯電話番号と関連付けて送信する装置。
 カード所有者が携帯電話から送信された個人認証タグの原本画像の非改竄証明データを携帯電話番号と関連付けて保存する装置。
 カード発行者サイド
 カード所有を希望する者から送られてきた申込書に記載してある携帯番号とカード所有者に発行した個人認証タグのID番号を関連づけて登録するサーバ装置
 同上の携帯電話番号の所有者の個人情報(氏名、生別、住所、生年月日)名が、電話会社に登録された所有者の個人情報と同じであることを自動的に確認する装置
 携帯電話によるクレジット決済を開始するパスワードを記入した秘匿性のあるハガキを同上の所有者の住所地に送付する装置 40
 カード利用者から送信された請求金額とカード利用者名をカード所有者の携帯電話に転送する装置
 カード所有者が登録してある携帯電話番号から、請求金額の承認と本人確認の照合結果を受信する装置。
 カード所有者が原本画像の非改竄証明データを登録してある第三者またはカード発行者が指定する認証機関から送信された原本証明結果を受けて、前項の請求金額の承認結果をカード利用者に送信する装置
 認証機関サイド
 携帯電話から送信された原本画像の非改竄データを照合してその結果を送信された携帯電 50

話、またはカード発行者から指定されたアドレス先に自動的に返信する装置。

< 提案方法 >

クレジット決済の手順；本人確認と第三者認証を行う場合

カード利用者に携帯電話番号を提示し、カード利用者は店頭での決済端末で携帯電話番号と請求金額を入力し、カード発行者が指定するセンターのデータを送信し、カードセンターはそのデータとカード利用者の店舗名等を携帯電話にメール送信する。

同データを受信したカード所有者は請求金額、店舗名、請求年月日を確認し、携帯電話を操作して本人確認の画像照合プログラムを起動し、携帯電話の撮像装置で撮像した照合画像と保存してある原本画像と照合し、正解率を算出して相手先に送信する。

カード所有者は携帯電話の外部接続端子に個人認証タグを差し込んで携帯電話を操作して原本非改竄証明データを抽出し、第三者またはカード発行者指定の認証機関に非改竄証明データを送信する。認証機関は送信された非改竄証明データを登録してある非改竄データと照合してその結果をカード発行者に指定された相手先に送信する。

カード発行者は第三者認証機関から送信された原本非改竄証明を確認したうえで、カード所有者から送信された決済承認データを元に、カード利用者に決済完了の通知を送信し、カード利用者はそのデータを確認して全ての手続きを完了する。

本人確認の手順；非改竄証明なし = 簡易型

カード利用者に携帯電話番号を提示し、カード利用者は店頭での決済端末で携帯電話番号と請求金額を入力し、カード発行者が指定するセンターのデータを送信し、カードセンターはそのデータとカード利用者の店舗名等を携帯電話にメール送信する。

同データを受信したカード所有者は請求金額、店舗名、請求年月日を確認し、携帯電話を操作して承認済の証としてメールをカード発行者が指定するセンターに返信する。

カード発行者は、カード所有者から送信された決済承認データを元に、カード利用者に決済完了の通知を送信し、カード利用者はそのデータを確認して全ての手続きを完了する。

B. クレジットカード決済を一変させるセキュリティと認証システム

B-1 携帯電話を使う分散型セキュリティ構造をもつクレジットカード決済システム

この発明は、携帯電話とネットワークを利用したクレジットカード決済における新しい体系的なセキュリティシステムを実現する。カード発行者によるカードホルダーの社会的信用確認と、本人の署名の視認に基づくサービス提供者の本人確認を背景にしたカード決済には、インターネット時代に対応するクレジット創造機能は全く期待出来なくなっている。

【0080】

クレジットカード決済に用いられているカード発行者の認証システムは極めて巨大な集中管理型のシステムである。ネットワーク時代が本格化しIT技術が一般社会に浸透するにつれ、カード偽造や成り済ましによる犯罪が急増しており、犯罪被害に対するセキュリティ管理は際限のない膨大な設備投資と損害保険で維持されている。

【0081】

今後は、これまでの対面によるカード決済だけではなく、通信手段を介した非対面の電子決済手続きの大幅な増加が避けられない。本発明は、その流れを背景にして肥大化するクレジットカード会社のセキュリティ管理システムに変わる新たな個人認証方式を前提にしたクレジット決済システムを実現するものである。

(1) クレジットセキュリティの基本的な概念と対策、処理、機能の整理

(2) クレジットセキュリティで用いられる主な通信技術と認証システム

(3) クレジットカードシステムに導入する分散型の決済システム

発明者は1998年から2002年にかけて、大阪市において展開した多用途ICカードを活用した地域情報システムの運用実証事業において、個人情報保護と活用を両立させる第三者認証構造を実現している。

【0082】

これまで、我々の社会的行為における日常的な認証の構造は、多用途、多目的、多段階が一般的である。しかし、クレジットカードのように巨大な顧客データベースを背景にす

る情報システムと通信手段を介した決済システムは、多段階の認証決済を管理責任上一極に集中せざるをえなくなってしまう。

このような情報セキュリティシステムでは、情報漏洩やクラッシュのリスクが飛躍的に大きくなると同時に、個々のカードホルダーとサービス提供者の間の決済手続きの形骸化が一挙にすすみ、計画的な犯罪による被害の急激な拡大が続いている。

【0083】

本発明は、クレジットカードを使用する現場で、多段階の認証構造とサービス提供者とカードホルダーが独立した複数の通信ルートを使うことにより、カードデータの改竄、盗聴、成り済ましの犯罪を完全に封じ込めることが可能になった。同時に、カードホルダーの本人確認を行うにあたって、カード発行者と第三者機関とに分散して構築するデータベースを使うことによってインターネットや一般回線を経由する通信環境の元で安全で安定的な認証システムの提供を実現したものである。

(1) 情報セキュリティの基本的な概念の整理

クレジットカードのセキュリティシステムは通信セキュリティとコンピュータセキュリティから成る。通信セキュリティは、一方の情報システムから他方のシステムに通信される間の保護であり、コンピュータセキュリティはコンピュータシステム中の情報の保護である。コンピュータセキュリティにはOSのセキュリティやデータベース管理ソフトのセキュリティ、カードに搭載しているデータのセキュリティも含まれている。

クレジットカード決済において情報セキュリティの対象となるリスク一覧。

不正なアクセス

他人へのなりすまし

パスワード・暗証番号の盗用

認定条件の虚偽と違反行為

システム突破と破壊行為

第三者による通信データのピックアップ

第三者による通信データの改竄

アクセス妨害

アクセス否認

クレジットカードのセキュリティ対策の4つの基本目標

1) 守秘性；

情報が見られないあるいは認められていない人によって引き出されることがないことを保証する。

【0084】

2) 完全性；

データの一貫性の保証、特に非認定者によるデータの創作、変更または破壊の防止を行う。

【0085】

3) 可用性；

正当な使用者が情報源、コンピュータ資源や通信資源などの供給源へのアクセスを不当に拒否されることがないことを保証する。

【0086】

4) 承認された使用；

情報源が非認定者あるいは非認定の方法によって使われないことを保証する。

情報セキュリティ基本目標の実現に必要なシステム処理と機能

システム処理の内容

1) アクセス資格同一性 (ID) の保証：

名前等の同一性を確認できること。ID確認は現状ではパスワードが一般的であり、ICカードが注目を集め始めている。

2) アクセス制御：

不正使用、不正開示、不正修正、不正廃棄、不正命令発令等による情報源への不正アクセ

10

20

30

40

50

スを防止する。

3) 暗号化：(註1)

データを暗号によって隠す。

4) データ完全(同一)性の保証：

データの追加、削除、変更などデータの値が変えられるのを防止する。

5) 行為者の否認防止：

取引や通信を行った当事者が後でその行為を否定することを防ぐ。

【0087】

電子的処理機能について。

1) デジタル暗号化処理；(註1)

デジタルデータに暗号処理を施し通常では判読できない形にする。

2) 自己証拠処理：

自己のバイOMETRICS(生体科学的特徴)情報を用いて自己を証明する。

3) 自己証明処理：

自己のIDを自身で証明するために電子的な署名を施す(電子署名)。

4) 他者証明処理：

公的機関などにより電子的に認証証明を行う(電子認証)。

(2) 情報セキュリティの管理技術を前提とした認証機構

認証機構とは、情報システムによってアクセスされた情報に対して、情報発信者の正当性を確認し保証する仕組みのことである。通信された情報に関する正当性は情報セキュリティによって担保されていることが前提である。

情報システムを経由したアクセスの目的と資格を相手方、もしくは第三者が確認するためには一般に次のような行為者による手続きが必要である。

1) パスワード、生年月日、電話番号等の固有の知識を示す。

2) 物理的な鍵やカード等の所有物を示す。(ICカードなど電子媒体では自己証明可能な電子的署名を含むことが可能)

3) バイOMETRICS情報(指紋等)の固有不変な特性を示す。(バイOMETRICS情報は生体科学的特徴情報；註2)

4) 特定の時間に情報が存在した証拠として第三者によるアクセス履歴を示す。(公的機関などによる電子的なタイムスタンプなど)

5) 相手方が信頼する同一性を保証する電子認証証明書などを示す。

問題の所在と解決の方向/集中処理から分散処理へ

従来のインターネットを使った一般的な認証システム

インターネットでの代表的なセキュリティ処理システムは、クレジットカードでの資金移動(トランザクション)を行うために開発されたSET(Secure Electronic Transaction)と呼ばれる世界規模の公開鍵型セキュリティシステム(一般的に公開鍵基盤(PKI)と呼ばれるシステム)が主流である。

【0088】

SETはインターネットに基づく販売での銀行カード支払を処理するためVISAとMasterCardなど主要なクレジットカード会社が共同で開発したものである。SETの環境は、カード発行者、カード保有者、店舗、確認者(銀行カード処理で店舗を支援する金融機関)、支払ゲートウェイ(支払処理のために運営されるシステム)、認証を主に行う認証局から成っている。

【0089】

ここでは公開鍵技術が全ての取引当事者の認証と全ての守秘取引データの暗号化のために使われている。暗号化には盗聴の危険がある店舗に銀行カード番号を見せないようにしてカード保有者を保護している。SETのPKIには次のような数種の認証局が使われる。

1) ルート認証局

主に信頼された第三者機関に委託され、クレジットカード会社を管轄する認証局(ブラン

10

20

30

40

50

ド認証局) に対して証明書を発行。

2) ブランド認証局

VISAやMasterCard等のブランドの所有者が、この階層の認証局を運用する。各ブランドは彼らが管轄している証明書の管理については責任を負う。

3) 地域認証局

ブランドが異なる地域を越えて処理を分散させるものである。

4) カード保有者認証局

カード保有者に他社証明としての電子証明書を発行する。

5) 店舗認証局

店舗に証明書を発行する電子認証局である。

10

【0090】

このSETのように業界共同の決済システムを情報セキュリティによって安全に処理するためには、世界規模での広範で大規模なシステムを構築する必要が生じてしまう。問題点は次の二点である。

- ・認証が行われる毎に個人情報が一ヶ所の認証システムに集積するため、個人情報がインターネットなどのオープンネットワークを通して通信され、情報搾取の危険にさらされる。
- ・これらのリスクを防ぎながら世界的規模の大量の決済と認証の処理を実行するために、全体システムは大規模、高価なシステムになっており、クラッシュの危険性もまた肥大化している。

20

(3) 情報システム上で信頼される多段階の認証システムの構築

情報システムがユビキタス時代の多用途、多目的なデバイスや端末に対応して、多段階な認証要求に応えていくためには、誰でも何処でも何時でも利用できるシステムを構築する必要がある。その前提にはユーザーやサービス提供者が誰でも安心してアクセスできる安全かつ安定して安価な情報システムである必要があり、SETで生じている二つの大きな問題を解決する必要がある。

【0091】

以下は、本発明で開発の前提としている認証システムの基本的な要件定義である。

- ・認証の基本責任はユーザに帰属し、進行は全てユーザの意思、指示による。
- ・認証は階層かつ分離分散された認証システムとし、確認証明者は認証に伴う他の認証責任を負う必要がないものとする。
- ・サービス提供者及び確認証明者のなりすましや不正処理を防ぐために、認証要求は同時に複数の確認証明者に複数のルートから依頼する同時多発要求処理を行う。
- ・認証要求者は認証の結果のみを受領し、原本情報など他の情報を扱うことはないような安全対策を行う。
- ・各関連者間の情報は認証の指示のための基本情報と確認結果のみとすることで、信頼性を確保し、問題を生じたときの追跡機能を確保するとともに新規情報の発生と蓄積を回避する。
- ・認証に伴う新たな個人用及びシステム用の情報を発生させない。
- ・各認証は独立に進行し、認証レベルは分離させる。

30

40

以上の処理を前提としたシステムが構築されると、従来我々の社会で実際に行われて来た人間関係を基礎においた認証方式に近い認証の構造がネットワーク上に実現する。

- a) 流通性 (Interoperability) の確保によりあらゆる応用へ適用可能である
- b) 小規模機能や構造の組合せ (クラスター構造) により小規模 ~ 大規模までシステム規模を柔軟に構築できる
- c) 運用手順を変えるだけで任意のシステムへ適用できる
- d) 危険分散化により個人情報の漏洩などのセキュリティ崩壊を効果的に防止できる
- e) 責任分散により責任、賠償範囲の簡素化、明確化が実現できる
- f) 各種のセキュリティサービス及びその関連製品を導入あるいは付加することが容易と

50

なる

- g) ポータビリティ（何時でも何処でも使える融通性や運用性）が確保できる
- h) 公的機関と民間任意機関との連携や融合が容易性に確保できる
- i) 公的機関の究極系である電子公証局への適用が容易となる
- j) 各種国家的及び公的認証系との連携が容易となる
- k) 金融系の認証機構との連携が容易となる
- l) その他各種のコンピュータシステムとの組合せが柔軟にできる
- m) 処理ログ保存によるトレーサビリティ（追跡性）確保に処理の動作保証と犯罪・不正の抑止効果など多くのメリットが実現し、極めて効率的に情報セキュリティが確保されるとともに個人情報の保護も行うことが可能となる。

10

（註1）暗号技術の種類について

暗号化処理やデジタル署名等はいわゆる暗号技術を用いて行われ、セキュリティ対策を行う際の重要な構成要素である。

最も基本的な構成要素は暗号アルゴリズムと呼ばれ、暗号化および復号化のデータ変形を行うものである。暗号化は情報を構成する言葉や数字等を直接読める平文から暗号文と呼ばれる判読できないデータに変形する。復号化は暗号文を元の平文に再現することをいう。暗号化には平文データと暗号鍵の2つの入力を持ち、復号化には暗号文データと復号鍵が必要である。

【0092】

暗号の典型的な使い方は守秘性用である。平文は無防備な秘密データであるが、その暗号文は信用できない環境でも伝送できる。なぜなら、その暗号が良質なら復号鍵を知らない限り暗号文から平文を導き出すことが不可能だからである。

20

【0093】

暗号には対称型暗号と公開鍵暗号の2つの種類がある。この2つは異なった特徴を持ち、異なったセキュリティ処理で使われる。

（1）対称型暗号

1970年代初頭から商用ネットワークで用いられている対称型暗号システムは暗号化と復号化に同じ鍵を用いるために対称型の名前が付いた。別名、秘密鍵型暗号とも言う。最も一般的な対称型暗号は1977年に米国連邦標準に採用され、日本でも金融情報を保護するために使用されているDESと呼ばれる暗号アルゴリズムである。DESはその暗号解読の危険をさけるために新たにAESと呼ばれる暗号アルゴリズムを2001年に米国政府暗号として採用し、世界中に広がることを期待されている。

30

（2）公開鍵暗号

公開鍵暗号技術は2個の相関する鍵ペアを使用し、1つの鍵を暗号化用に、もう1つの鍵を復号用に用いる。一方の鍵はシステムにより極秘裡に保管されるため私有鍵と呼ばれ、もう一方の鍵は一般に公開されるため公開鍵と呼ばれる。このように鍵の一方を公開するので公開鍵暗号と呼ばれる。

【0094】

公開鍵暗号は公開鍵が暗号鍵として用いられるか、復号鍵として用いられるかにより2つの基本モードが存在する。

40

一つは公開鍵を暗号鍵として使うもので通常の暗号処理と同様である。しかし、通信する人同士で各々異なる鍵を持つ必要がない。もう一つは私有鍵を暗号鍵として使うもので私有鍵を知り得るのはその所有者のみであることからデータ発信者の認証とメッセージの完全性の保証を行うことができるもので、認証処理と呼ばれる。

【0095】

このような公開鍵暗号での認証処理を行うことで、電子的な署名処理いわゆる電子署名を行うことが可能となる。

【0096】

公開鍵暗号は数学的に解くことが難しいという想定に基づいたものであり、代表的なアルゴリズムはマサチューセッツ工科大学（MIT）で発明されたRSAアルゴリズムである。

50

【0097】

公開鍵に基づく署名では復号鍵（発信者の公開鍵）は、セキュリティを考慮することなく受取人が保有でき、受取人はそれを用いていかなるメッセージの署名も確認できるという重要な特性を持っている。

（註2）バイオメトリクス（生体科学的特徴）による本人確認について

バイオメトリクス認証は電氣的に個人を認証するために、生体科学的特徴や個人の動作上の特徴を使う。バイオメトリクス読取機は物理的特徴を測り、特定の値と比較する。多くのバイオメトリクス技術が開発されている。

- （1）指紋認識
- （2）音声認識
- （3）手書き署名認識
- （4）顔形認証
- （5）虹彩認識
- （6）掌形認識
- （7）DNA認識

10

他であり、インターネットでの情報交換や電子商取引を安全に行うために複数端末、家庭及びオフィスの端末あるいはショッピングモールでの公衆インターネットキオスクなどで実際に操作している人を特定するために重要である。

バイオメトリクス情報はICカードなどの個人保有のメディアに格納することも可能である。

20

【発明を実施するための最良の形態】

【0098】

本発明に係る技術の構成要素は、一実現形態として、1．個人が占有している情報端末に生体情報を入力する装置、2．照合の根拠となる原本情報を登録する記録装置と、原本として登録された生体情報が改ざんされるとき、入れ換えられていないことを照合する機能、3．本人確認が必要になった時に入力する生体情報と登録済みの原本情報を照合して判定する機能、4．第三者機関によって本人確認時に登録済み原本が非改竄であることを証明する機能、5．本人確認を要求している相手方に照合の判定結果を送信する機能を具備している。

【0099】

30

以下、本発明の実施の形態につき説明する。

【0100】

（A）システム全体

図1は、本発明の実施の形態に係る個人認証装置の構成を示すブロック図である。同図に示すように、本発明の一実施形態に係る個人認証装置100は、カメラ付携帯電話機200に内包されている。個人認証装置100は、原本画像記録装置101と、認証時の顔画像データ処理部102と、画像照合装置105と、照合判定結果保存装置106と、照合判定結果添付・送出装置107と、カメラ108と、撮像フラッシュ装置109とを具備して構成される。

【0101】

40

カメラ108および撮像フラッシュ109は、装置使用開始時に、当該装置の所有者または占有使用者の本人確認のための照合用原本情報を取得したり、照合用の新たな個人情報取得するのに用いられる。もちろん、個人認証用の情報を取得する以外にも、通常の撮影のために用いることができる。フラッシュ109は、保存する画像としてはっきりとした画像を確保する上で照度がかかなり大きなポイントになることから、重要である。太陽光や照明が逆光になった場合は照合精度が落ちてしまう。

【0102】

原本画像記録装置101は、カメラ付携帯電話機の所有者または占有使用者が携帯電話機を占有した時最初に撮影した自己の顔画像を記録するものであり、一度だけ書き込み必要に応じて読み出しが可能であるが映像の改変または再撮影は出来ない構造である。また

50

この原本画像記録装置101は、原本画像記録装置101に記録された映像のデータに関するバイト数を映像データと別途保存し、必要に応じて第三者に、できれば自動的に送信して保存することが可能な機構を備えていてもよい。カメラ付携帯電話機200の工場出荷段階で決められる製造番号が出荷時に第三者に登録されている場合、この製造番号と最初に撮像した画像のデータ容量(バイト数)と併せて第三者に保存することにより、本発明の装置および方法に係る個人認証が極めて正確になるとともに、社会的な信頼性を確保することも可能となる。利用者が情報端末に登録した照合用の生体情報の原本性確認は、利用者が情報端末の使用開始時に登録した生体情報のデータ容量の照合によって行うことができる。

【0103】

本発明では、個人情報となる生体情報を個人が占有する端末機器から外部に出さないために、外部すなわち第三者に送信可能なのは、原本画像記録装置101に記録された原本情報のデータ容量のみである。

【0104】

認証時の顔画像データ処理部102は、撮像動画像記録装置103と、静止画像選別装置104で構成されている。

【0105】

認証時に映像照合装置105で照合される映像は、ダミーの静止画の撮像による照合を避けるため、カメラ108で撮像され照合される映像は動画像から顔画像データ処理部102で選択された複数枚の映像によるものである。所有者の写真を撮影することで成りすましの恐れがあるので、動画像を選択するようにすること、動画像から任意に選択した複数枚を選択して照合することによって照合の精度を上げることができる。

【0106】

照合時に所有者の顔をカメラ108で撮像すると、顔画像データ処理部102が撮像動画像から複数画像と原本画像記憶装置101に登録されている原本画像とを照合し、双方の画像から同一人と判定されればその結果を照合判定結果保存装置106に保存するようになっている。照合時に使用される画像照合については次項に詳説する。

【0107】

所有者は認証要求がある、通信の相手先に対して必要な情報を通信する際に、保存しているカメラ付携帯電話機の照合判定結果添付・送出装置107を経由して相手先に送付する。繰り返しになるが、本発明では、認証要求のある通信の相手先には、照合の判定結果のみを送付するのであって、生体情報そのものについては個人が占有する端末機器からは外部に出さない。

【0108】

カメラ付携帯電話機200は、認証部100に備わった認証に必要な各装置・処理部を使い、その照合結果を用いて最終的に、本人であるか否か確認を行うものである。これらの認証に応える動作は、カメラ付携帯電話機200全体もしくはその一部の操作を制御するものではなく、画像照合の判定結果を送信するものであり、このような動作は照合の結果に係わらない。

【0109】

上記説明においては、顔画像を動画像として撮影し、これから抽出する静止画像を使って照合する認証方式を用いたが、無論静止画として撮像して照合することも可能であり、本発明では、静止画による照合も可能な機能を備えている。さらに、上記説明においては、個人情報として生体情報のうち、顔画像を採用したが、顔画像に替えて、または顔画像に加えて、新たに虹彩、指紋、掌紋、網膜情報、耳介情報、静脈パターン、声紋および遺伝子情報のいずれかを用いてもよい。すなわち、カメラによる顔画像の撮像機能を使った入力方式の他に、指紋や掌紋情報を取り込む光学方式、静電方式、感熱方式、電界方式、圧力方式などのセンサー機能を持つ入力デバイス、声紋情報を取り込むマイクロフォン、遺伝子情報をスキャンするセンサー機能を持つ入力デバイスを使用して生体情報を取り込むことも可能である。前記情報は2つ以上組み合わせるよう設定することも

10

20

30

40

50

可能である。さらにパスワードやID番号認証機能を加えて、本人確認の精度をあげることも可能である。

【0110】

複数の生体情報である、たとえば個人の顔画像、音声、指紋、或いは特定のパスワード又はID番号の認証結果のうち何れかを組み合わせ用いられた、本人確認の判定結果は必ずカメラ付携帯電話機等、情報端末内の照合装置で処理され、照合に使われた生体情報は一切外部に通信されない構造を保持する。

【0111】

虹彩情報を取得する装置は、たとえば、特開平11-146507号、特開2002-307715号および特開2002-330318号に記載のものが使用できる。指紋情報を取得する装置は、たとえば、特開2001-344544号に記載のものが使用できる。声紋情報を取得する装置は、たとえば、特開2000-259828号記載のものが使用できる。その他、公知の技術を用いて個人情報を取得することができ、取得した生体情報を認証装置の外には出さず、照合結果のみを出力する本発明に供することができる。

【0112】

図1では便宜的にカメラ付携帯電話機に搭載された個人認証装置で本発明の装置および方法の説明を行ったが、本発明に係る装置および方法の認証機能である本人確認の仕組みは、家庭用のTV電話機、パーソナルコンピュータなど、家族が共有で使うことになる通信機能をもつ端末や移動用のパソコンなどを始め、酒類、タバコ、飲料等の自動販売機、交通機関、娯楽施設の自動券売機、有価証券類、住民票等の自動発行機、クレジットカードのキャッシュディスペンサー、金融機関のATM装置、公衆電話機など事業者のサービス提供用の機器など社会的なサービスを提供している装置（無人サービス提供機）にも広く利用することができる。更に、外国人および/または日本人の入出国管理、不動産売買/賃貸契約に伴う本人確認、病院での本人確認など、本人確認が必要とされる社会のあらゆる場面に応用可能である。簡便かつ正確な個人認証/本人確認を行うことができる。

【0113】

カメラ付携帯電話機等、情報端末内の原本画像記録装置101に記録された画像情報の他、その他の生体情報を用いる原本情報記憶装置に記録されている情報を外部機関によって認証を受ける場合に必要な情報は、顔画像情報等の個人認識可能な情報ではない。照合用に撮影された画像として特徴原本データに登録した画像の指定された1ライン（図6のライン1）上の画素の濃度を加算器にて加算し結果をnビットレジスタに累積し、オーバーフローする上位ビットは無視し、下位nビットを改竄防止符号として登録する。

【0114】

カメラ付携帯電話機を含み、テレビ電話機又は携帯テレビ電話機に備えられ特定個人であると認証する機構が、認証の結果によって各々の端末の動作を制御する機能ではなく、操作した本人と登録済みの本人を画像もしくはその他の生体情報によって照合しその結果だけを外部送信して相手先の認証に資するデータを提供することを実現しているのは、前記の改竄防止符号を使って特徴原本データの非改竄、言い換えれば原本性保証を第三者機関によって証明されるからである。

【0115】

(B) システム全体/カメラ付き携帯電話の外部接続端子利用型

【0116】

図2は、本発明の別の実施の形態に係る個人認証装置の構成を示すブロック図である。同図に示すように、本発明の一実施形態に係る個人認証装置300は、カメラ付携帯電話機200の外部接続端子に取り付けられて使用される。個人認証装置300は、原本画像記録装置301と、認証時の顔画像データ処理部302と、画像照合装置305と、照合判定結果保存装置306と、照合判定結果添付・送付装置307と、カメラ308と、撮像フラッシュ装置309とを具備して構成される。

【0117】

カメラ108および撮像フラッシュ109は、個人認証装置300の使用開始時に、該

10

20

30

40

50

装置の所有者または占有使用者の本人確認のための照合用原本情報取得し、また照合用の新たな個人情報として本人の顔画像を取得するために用いられる。もちろん、個人認証用の情報を取得する以外にも、通常の撮影のために用いることができる。フラッシュ109は、保存する画像としてはっきりとした画像を確保する上で照度がかかなり大きなポイントになることから、重要である。太陽光や照明が逆光になった場合は照合精度が落ちてしまう。

【0118】

原本画像記録装置301は、カメラ付携帯電話機の所有者または占有使用者が携帯電話機を占有した時最初に撮影した自己の顔画像を記録するものであり、一度だけ書き込み必要に応じて読み出しが可能であるが映像の改変または再撮影は出来ない構造である。またこの原本画像記録装置301は、原本画像記録装置301に記録された映像のデータに関するバイト数を映像データと別途保存し、必要に応じて第三者に自動的に送信して保存することが可能な機構を備えている。個人認証装置300の工場の製造段階で決められる製造番号を、生産者の管理下で製品の工場出荷時に第三者機関に登録しておくことによって、製品を購入または確保した本人がこの個人認証装置300の製造番号を、最初に撮像した画像のデータ容量(バイト数)と併せて第三者機関に送信して保存することにより、本発明の個人認証方法とプログラム実行システムに係る個人認証が極めて正確になるとともに、社会的な信頼性を確保することも可能になる。利用者が自ら占有する情報端末機器に登録した照合用の生体情報の原本性確認を行う場合は、利用者が情報端末機器の使用開始時に登録した生体情報のデータ容量の照合する他、すでに登録してある製造番号と原本性証明の要求時に、改めて製造番号の照合することで証明の確度を高めることができる。

10

20

【0119】

本発明の特徴は、個人情報である生体情報を個人が占有する情報端末機器から外部に出さないことであり、外部すなわち第三者機関に送信可能なのは、原本画像記録装置301に記録された改竄防止符号原本データのデータ容量のみである。

【0120】

認証時の顔画像データ処理部302は、撮像動画像記録装置303と、静止画像選別装置304で構成されている。

【0121】

認証時に映像照合装置305で照合される映像は、所有者の顔写真を撮影するダミーによる成り済ましを可能にする静止画の撮像による照合を避け、携帯電話機のカメラ108で撮像され照合される映像は動画像から顔画像データ処理部302で予め設定されたプログラムによって選択された複数枚の映像である。所有者の写真を撮影することで成り済ましの恐れがあるので、動画像から静止画像を選択、複数枚を使って照合することによって照合の精度を上げることができる。

30

【0122】

照合時に所有者の顔をカメラ108で撮像すると、顔画像データ処理部302が、撮像動画像から選択した複数画像と原本画像記憶装置301に登録されている原本画像とを照合し、双方の画像から同一人と判定されればその結果を照合判定結果を正解率という数値データで保存装置306に保存するようになっている。照合時に使用される画像照合については次項に詳説する。

40

【0123】

所有者は認証要求がある、通信の相手先に対して必要な情報を通信する際に、保存している照合判定結果を照合判定結果添付・送出装置307を経由して相手先に送付する。前記の繰り返しになるが、本発明では、認証要求のある通信の相手先には、照合の判定結果のみの数値データを送付するのであって、生体情報そのものについては個人が占有する端末機器機からは外部に出さないことが重要である個人認証方法とプログラム実行システムである。

【0124】

カメラ付携帯電話機200において、その外部接続端子に差し込まれたコネクタもしくは

50

は接続されたコンピュータ、さらにはICカードやメモリーカードなど個人情報情報を保存し読み出しができるデバイスから情報を読み取ることが可能な情報端末装置の認証部300に備わった認証に必要な各装置・処理部を使い、その照合結果を用いて最終的に、本人であるか否か確認を行うこれらの認証に応える動作は、カメラ付携帯電話機200全体もしくはその一部の操作を制御するものではなく、カメラ付携帯電話機200をコントロールして画像照合の判定結果を相手先に送信するものであり、このような動作は照合の結果に係わらないものである。

【0125】

前記コネクタもしくは接続されたコンピュータなど、カメラ付携帯電話機200の外部接続端子に差し込まれる情報端末認証部300には、本人確認認証プログラムが内装されている。このプログラムは、カメラ付携帯電話機の電源によって動作し、携帯電話機の操作ボタンによって起動するのが好ましい。また、情報端末認証部300に内装されている本人確認認証プログラムと携帯電話機200とを中継して外部にデータの送信を行う装置を介在させ、同装置から送るデータによって携帯電話機の機能を可能にするようにしてもよい。

10

【0126】

情報端末認証部300をカメラ付携帯電話機200に最初に差し込んだ段階で、撮影装置を起動して撮像した画像は、コネクタなど情報端末認証部300の記録装置303に原本画像として登録されることが望ましい。

【0127】

前記情報端末認証部内の記録装置に保存した原本画像が符号化され、改竄防止符号原本データとして、接続した携帯電話機を中継して外部の第三者機関に送信され、認証保証センターの専用サーバーに記録されるようなプログラムが内装されていることが望ましい。この際、外部の第三者機関の通信先が予め指定されており、カメラ付携帯電話のデータ通信機能によって送信されることが望ましい。また、カメラ付携帯電話から最初にコネクタなど情報端末認証部に画像を送信して、改竄防止のための原本画像情報が登録された場合に、改竄防止符号原本データを、カメラ付携帯電話の通信機能を使って外部の認証機関に自動的に送信するようにしておいてもよい。

20

【0128】

この改竄防止符号原本データは、前記原本画像情報(特徴原本画像情報、特徴原本データ)に係る画像の任意の1本の横線もしくは縦線上の画素、もしくは前記特徴原本情報にかかるデータのビット数の少なくともいずれか1つであることが好ましい。また、改竄防止符号原本データとして自動的に複数のデータを保存しており、第三者機関に登録する改竄防止符号原本データは本人確認手続きを行うたびに、保存してある複数の原本の非改竄を証明するデータを入れ替える機能を有していることが好ましい。

30

【0129】

第三者機関に改竄防止符号原本データを登録するとき、使用するカメラ付携帯電話、もしくはコネクタやコンピュータなどの情報端末認証部の登録ID番号を送信して、該番号を改竄防止符号原本データと同時に登録する機能を有してもよい。また、第三者機関に登録した改竄防止符号原本データを参照する場合、使用するカメラ付携帯電話、もしくはコネクタやコンピュータなどの情報端末認証部の登録ID番号を送信して該番号を改竄防止符号原本データと同時に照合する機能を有してもよい。

40

【0130】

認証時には、携帯電話機の通信をオフすることなく、外部の第三者から受信した原本画像の非改竄を証明するデータと、コネクタなど情報端末認証部内で照合した結果を含む記憶装置に記憶されている各種の情報を一緒に通信中の相手先に送信するようにしてもいい。通信の相手先から本人確認と個人認証を請求された際に、携帯電話機の電話通信を維持したまま、外部の第三者から受信した原本画像の非改竄を証明するデータと、コネクタなど情報端末認証部内で照合した結果と一緒に相手先に該データの packets 通信が可能ないようにしてもいい。また、通信の相手先から本人確認と個人認証を請求された際に、携

50

携帯電話のメール通信機能を使って、外部の第三者から受信した原本画像の非改竄を証明するデータと、コネクタなど情報端末認証部内で照合した結果を添付して、カメラ付携帯電話で作成したメール本文と一緒に相手先に送信可能なようにしてもいい。

【0131】

本人確認認証プログラムを内装したコネクタなど情報端末認証部が外部接続端子に差し込まれている状態で、本体のカメラ付携帯電話の操作機能を使ってコネクタなど情報端末認証部内の各種プログラムを有効とするモードが設定されていてもよい。

【0132】

本人確認認証プログラムを内装したコネクタなど情報端末認証部（本人確認認証プログラム実行装置）に外部からのデータを受信させるようにしてもよく、この実行装置とカメラ付携帯電話が接続され、携帯電話機が受信したデータを変換して実行装置に送る中継装置を更に有してもいい。この中継装置には、カメラ付携帯電話から送られる動画像データから静止画像を抽出して記憶する装置と、原本画像と照合可能なコネクタなど情報端末認証部対応のデータに変換する装置を含んでもよい。

【0133】

照合の実行を可能とするプログラムによって、カメラ付携帯電話で撮像された顔画像を読み取って原本として記録された記録媒体と、本人確認用に撮像された動画像から照合用顔画像データを抽出するステップと具体的に照合して正解率を計算するステップを一体的に処理できるプログラムを搭載したチップとを内装してもよい。

【0134】

個人情報の種類、本発明に係る装置および方法の認証機能である本人確認の仕組みの利用範囲などは、図2においても、図1と同様であることはいうまでもない。

【0135】

本発明は、カメラ付携帯電話もしくは携帯電話に取り付けられて機能拡張端子を使ってこれらの通信端末機器の機能自体を写真付きの身分証明書の機能と、契約行為に必要なハンコの機能の二つを同時にしたものと解釈すべきものである。

【0136】

現在、運転免許証、パスポートなどの公的証明書、また学生証、社員証、一部のクレジットカード、キャッシュカード、その他の会員カードなど、身分証明書には「顔写真」が添付されている。さらに身分証明書は学生証、社員証、免許証、パスポートなどは、本人が所属する組織が学校印、社印、公安委員会印、外務省印など印判を使う形式で必ず第三者が見て明らかな視認確認が可能な発行者の存在が不可欠である。また、特に免許証やパスポートなど重要な証明書は本人の成り済ましを防ぐために顔写真が改竄できないような工夫がこらされている。

【0137】

これら身分証明書の形式は全て、目の前の人間が本人の顔と証明書を見比べながら本人確認を行うためのものである。最近では、コピーやファクスでも認証用の手続きとして認められるケースが増えて来ているが、基本的にはフェースツーフェイスを前提とする認証方式である。

【0138】

本発明が目標としている具体的な目的の内、身分証明書の機能は次の二点である。

【0139】

(1) 本人の所属の有無に係わらないで身分証明に代わる認証行為の設定を可能にする。

【0140】

(2) 通信手段を用いて直接の面談を伴わない本人確認の方式を実現する。

【0141】

ハンコには、本人が所有し本人を特定する印判を使って本人の契約行為の意志を証する印影を、相手方が受取る紙媒体に捺印することで、相互の意志を認証する割付方式の保証書の役割をもっている。印判は本人が所有し、印影は相手方が保存することで後日に契約行為の存在を証明することが可能になる。

10

20

30

40

50

【0142】

もうひとつ本発明の目標としている具体的な目的の内、ハンコの機能は次の二点である。

【0143】

(1)所有者本人の原本登録顔写真のデータ容量(印判に彫込んだ名前)を、相手側に送ることによって(捺印して)契約行為の意志確認の証書となる。

【0144】

(2)同上の原本登録顔写真のデータ容量を第三者機関に登録し(印鑑登録)、第三者機関経由で同データ容量を送信することで一般にいう印鑑証明書付きの契約行為となる。

【0145】

上記の二つの機能を満足できるように、たとえば本発明を適用したカメラ付携帯電話端末は工場出荷後、撮像機構が未使用の場合に限り、初回に撮像しCD-R方式(一度だけ書込み可能。読出し自由)で記録する本人の顔画像データを原本写真とデータ容量に分けて端末内に保存できる装置を備えていることには重要な意義があるのである。またデータ容量については端末側に保存すると同時に外部に送信して指定の第三者機関が保存する機能が付加されている。

10

【0146】

この機能を、実際の手続きの流れで説明してみる。

【0147】

以下は本発明に係る装置の機能説明の一例であり、携帯電話販売の店頭という設定である。

20

【0148】

お客;ハンコの代わりになるっていう携帯電話ありますか?

【0149】

店員;カメラ付で画像保存のできる携帯電話ですね。身分証明書でも使えますよ。

【0150】

お客;それもらいます。

【0151】

店員;わかりました。ご希望の電話機をセンターに登録しますのでまず機種を選んでください。それからこの申込書にお名前、生年月日、ご住所、電話番号をご記入ください。免許証か保険証、それとハンコはお持ちですか。

30

【0152】

お客;免許証はありますが、ハンコは持ってません。

【0153】

店員;向いの文具店でも売っていますがどうされます。300円ですが・・・

【0154】

お客;じゃ、買って来ますわ。

【0155】

店員;申し訳ありません。この携帯電話なら次からハンコも免許証もいらないんですが・・・

40

【0156】

・・・

【0157】

店員;今までお使いの電話番号になさいますか。

【0158】

お客;はい。

【0159】

店員;料金の払込みは銀行引落しで構いませんか。今お使いの銀行口座のままでしたらお手続きは簡単に済みますので、できたらそれでお願いしたいのですが。

【0160】

50

お客；口座を代えたいけど、難しいの？

【0161】

店員；銀行口座を新たに開設していただく場合は、開設後に販売させていただくことになります。他にお使いの銀行口座ですとその銀行に対して信用紹介が必要になりますので少しお時間がかかってしまいますが・・・

【0162】

お客；仕方がないか、そのままでいいや。

【0163】

店員；申し訳ありません。最近は成り済ましによる被害が増えていまして、銀行口座の名義人がご当人であるかどうか確認が非常に厳しくなっていますので、否認されるケースも結構あります。

【0164】

お客；でも、このカメラ付携帯電話を持っていたら銀行口座はすぐに開設できると聞いたけど。

【0165】

店員；その通りです。私どもの販売しているカメラ付携帯電話は製造者番号と電話番号、それとご購入された方を確認できるデータをセンターで保管しますので、本人確認が簡単にできるようになっています。銀行の窓口でも本人確認にこの携帯電話を使うようになって、インターネットでも同じことができるようになりました。

【0166】

お客；早くお願いします。

【0167】

店員；はい。少しお待ち下さい。

【0168】

携帯電話の登録が終わって；

【0169】

店員；センターの手続きは全て終わりました。ご本人のお顔を取り込んでからお使いになれるように成ります。後からご自身でも出来ますが、取込みに失敗したらこの電話を廃棄しなければ成りませんのでこちらでやっておきましょうか。

【0170】

お客；難しいんですか。

【0171】

店員；いいえ。画面の上に付いているレンズをご自身のお顔に向けてからこのボタンを押して下さい。フラッシュが光ったあと保存用の画像が画面に表示されますので、それでよければこの通話ボタンを押してください。それで終わりです。画像がお気に召さなければ右側の赤いマークのボタンを押していただければもう一度撮影できます。後は繰り返します。

【0172】

お客；わかりました簡単ですね。後で自分でやります。

【0173】

店員；うっかりして他のボタンに触れたり、それ以外の操作をされますと画像の保存が出来なくなりますので注意してください。その場合は一切認証の機能が使えなくなります。もちろん普通のカメラ付携帯電話としてお使いになれるのですが・・・よく失敗されて取り替えて欲しいといわれる方がありますが、失敗されてもお取替えは出来ないことになっています。その場合は新たにお買い求めいただくしかありません。ご購入の翌日までなら10%引きになります。

【0174】

それと、購入から30分以内にこの作業をしていただかないとセンター登録が出来なくなります。その場合は電話だけの認証になりますので、センターや外部からの認証が受けられません。

10

20

30

40

50

【0175】

お客；それだったら、ここでやって行くわ。

【0176】

店員；それでは、この電話の内側に付いているレンズをお客さんの顔に向けてシャッターを押してください。

【0177】

お客；はい。こうですか。バシャッ。

【0178】

店員；その顔の写真で良いですか。

【0179】

お客；はい。

【0180】

店員；それでは、左側の緑の通話ボタンを押してください。

【0181】

お客；はい・・・・・・・・・・画面に登録完了と出ましたが。

【0182】

店員；それで終わりです。これで保存した画像のデータ容量とこの電話番号をセンターに登録できましたので、今から認証機能をお使いになれます。試しに当社の会員登録をされてみますか。会員になりますと盗まれたり無くされたときに割引きでお買い求めになれたり、他で使われた時の認証保証サービスが受けられます。

【0183】

お客；その認証保証サービスって何？

【0184】

店員；例えば、お客さまがどこかのローン会社から急にお金を借る必要が出て来た場合、それまで取引が全くなかったとしても、このカメラ付携帯電話で認証して申込をされますと、ご本人の確認は当社が保証しますので、そのローン会社が当社のシステムをご存じだったら比較的簡単にローンの決済が受けられるはずですよ。お借入には当然いろいろな条件がありますが、おのカメラ付携帯電話端末であれば、他の銀行との取引情報や勤務先の会社が公開している個人情報を見てももらうことも出来ます。普通なら個人情報保護法の関係で出来ませんが、この電話では本人確認の保証が付いていますので相手先が安心して個人情報を見ても大丈夫です。

【0185】

お客；なるほど、なるほど。ではどうやるの。

【0186】

店員；まずこの電話番号にそのカメラ付携帯電話で電話をしてください。

【0187】

お客；はい・・・・・・・・・・もしもし。

【0188】

センター；ありがとうございます。認証センターです。様、当社のサービスをご利用いただきありがとうございます。どのようなサービスをご希望ですか？

【0189】

お客；会員の登録をしたいのですが。

【0190】

センター；はい解りました。お使いの電話はご本人さんのものですね。

【0191】

お客；はい。

【0192】

センター；それでは、電話の内側のレンズでお客さまの顔を撮影していただきます。メニューボタンから顔のマークの認証アイコンを選んでください。「さつえいOK」の表示が出ますから上のボタンを押してください。2、3秒間はそのまま、ピッと音が鳴るま

10

20

30

40

50

で撮影を続けて下さい。

【0193】

お客；はい・・・バシャッ、ジー・・・ピッ。

【0194】

センター；ありがとうございます。顔が写っていましたら、そのまま同じボタンを押してください。もし写っていなかったり、ぶれていましたら、「やりなおし」にスクロールしてからボタンを押してください。「さつえいOK」の表示が出ましたら、もう一度同じボタンを押して撮影しなおしてください。

【0195】

お客；大丈夫だと思います。

10

【0196】

センター；ありがとうございます。では、上のボタンを押してください。

【0197】

お客；押しました。

【0198】

センター；画面には何と出ていますか？

【0199】

お客；「正しい」と出ています。

【0200】

センター；それでお客さまの電話をご本人を確認しましたので、もう一度同じボタンを押してください。それで確認結果が電話機に保存されます。

20

【0201】

お客；押しましたが。

【0202】

センター；はい。画面にメニューが出ていますが、スクロールして会員登録・確認のアイコンをクリックしてください。

【0203】

お客；はい。

【0204】

センター；これで、当センターの会員として登録されました。それでは確認しますが、お名前は 夫様ですね。生年月日は1968年8月24日ですね。よろしいですか。

30

【0205】

お客；はい。

【0206】

センター；わたしどもが保存しているお客さまのデータは、お客さまが今お使いいただいている携帯電話の製造者登録番号と電話番号、お客さまのお名前と生年月日、それとお客さまの携帯電話に保存されている画像データの容量です。お客さまがお買い求めになったお店の名前と登録番号です。お店は ショップの大阪市の心齋橋東店で間違いありませんね。

40

【0207】

お客；はい。

【0208】

センター；あと、お客さまが電話を無くされた場合に、ご本人を確認する情報を登録しなければなりません。お客さまだけがご存知でお忘れにならない自信がある情報を教えてくださいませんか。

【0209】

お客；どんな情報がいいんですか。

【0210】

センター；はい。数字でも文字でも構いません。よくあるのはご家族の誕生日や結婚記

50

念日、奥様がお出身の町、家族のだれかのお名前、ペットの名前を登録される方もございます。お客さまが卒業された学校名や初恋の方のお名前をおっしゃった方もおられます。別に電話番号をダブって登録されても構いません。

【0211】

お客；結婚記念日にしておきます。1987年5月3日です。

【0212】

センター；わかりました。めったにありませんがご確認の意味でご質問させていただくことがありますのでその時は年月日だけおっしゃっていただければ結構です。最後になりましたが、画面にメニューが表示されていると思いますが、スクロールして送信のアイコンをクリックしていただだけませんか。その後で送信完了とできれば手続きは全て完了です。どうもありがとうございました。

10

【0213】

お客；いいえ。

【0214】

店員；それで終わりましたね。お客さまがこれからこの携帯電話を使って電子ショッピングをしたり、銀行の振り込みや振替えをするとき、また旅行の申込やコンサートの申込みなどをする場合に、相手先から本人確認を求められたら、今と同じような手続きで画面に「正しい」と表示させて、保存してください。電話でしたらそのままお話を続けて終わりましたら、最後にメニューの送信アイコンをクリックすれば認証が終わっています。

【0215】

お客；ホームページやメールの場合はどうしたらいいのですか。

20

【0216】

店員；ホームページの場合か、必要な書き込みをしていくと、本人確認をお願いしますと、というような表示が出てきます。その場合は、先程と同じようにメニューボタンから認証のアイコンを選んでクリックして同じように「正しい」という表示を保存して、メニューボタンの送信アイコンを選んで送信します。ホームページ画面に「認証（確認）できました」とでたら後は、ホームページの誘導にそって手続きをしてください。

【0217】

メールを送る場合は、メールを一旦保存してから、メニューから認証アイコンをクリック、同じように画面に「正しい」と表示させるところまで行ってから、そのまま送信アイコンをクリックしてください。カメラ付携帯電話内に保存してあるメールに添付されて認証結果を送信します。

30

【0218】

お客；了解です。

【0219】

店員；もしお判りにならなければいつでもお電話ください。いろんな裏技をお教えしますよ。ただし、本人確認はキチンと要求しますよ。他の人に教えたくないですからね。

【0220】

このように、本発明に係る一実施形態においては、上述の説明にあるように、バイオメトリクス情報そのものという秘密情報を直接送受信の対象としない。原データを自己装置内に購入時に撮像・登録し、照合の必要な際に撮像した照合必要時撮像データを原データと比較した結果（おそらく数バイト程度のデータ）をサービス提供者側に送信する。それと共に、かかる原データが改竄されていない保証として、やはり装置購入時に原データの撮像画像から（詳細について後述する）一定の符号化した改竄防止用原符号化データを作成、第3者機関に送信・保存させ、照合必要時に撮像した照合必要時撮像データから当該符号化を施した改竄防止用照合用符号化データを作成、当該第3者機関に送信し、当該第3者機関ではこの送られた改竄防止用照合用符号化データを先に保存されている改竄防止用原符号化データと比較して改竄がなされているかを判定し、その結果を先のサービス提供者側に送信する。当該サービス提供者側では、サービス要求者側から上記の送られた照合結果データを、第3者機関から改竄がされていないかどうかの判定データを受け取るこ

40

50

とになり、このダブルの認証をもって本人確認を行うことができる。そしてこのときに、サービス要求者にとっては、バイオメトリクス情報という極めて個人的な秘密性の高い情報を他に委ねる危険を冒すことなく、本人認証を受けることが可能となる。

【0221】

上記の説明では、認証に用いる比較データとして例えば顔写真を例にとって説明したが、これは本人の認証に用いることが可能なデータであれば原理的に何でも可能である。したがって、バイオメトリクス情報、本人しか知り得ず（持ち得ない）常時（或いは照合要求時）身につけている情報であればよい。具体的には、顔写真のほか、声紋、指紋、虹彩、遺伝子情報等であっても原理的に同様の効果を奏することが可能である。

【0222】

また、第三者認証を使ってクレジットカード機能をたとえばカメラ付き携帯電話にもたせることが可能になる。以下は、クレジットフォンの申込みから利用の実態の一例を解説したものである。

【0223】

カード会社；「お客さま、今、私どものクレジットカードをお使いいただいておりますが、クレジットフォンを申し込まれませんか。」

【0224】

お客；「?????」

【0225】

カード会社；「カードの代わりにカメラ付き携帯電話で直接カード決済ができるシステムです。ふた通りの方法がお選びいただけます」

【0226】

お客；「ちょっと待ってください。そのクレジットフォンに代えるとどんなメリットがあるんですか」

【0227】

カード会社；「まず第一が安全性です。このクレジットフォンをお使いになられるときに、私たちのセンターが、直接電話でお客さまを確認しますので、他人が使うことはできません。カードの偽造や盗難による被害がほとんどなくなるので、これまでの被害額を、お客さまに還元することが出来るようになりました。会費が安くなりますし、お使いいただいた額によってポイントが大きくなります。お店側も色々なサービスをご用意しています。」

【0228】

お客；「クレジットフォンの看板があるお店ですね」

【0229】

カード会社；「はいそうです。」

【0230】

お客；「どうやって使うんですか」

【0231】

カード会社；「お店やレストランで使う場合、まずこのカメラ付き携帯電話からVISAのコールセンターを呼び出します。『本人確認をお願いします』という案内が流れますので、ご自身の顔正面からこのカメラで撮影してください。画面に『確認できました』か『もう一度』と表示されます。『確認できました』と表示されたらそのまま送信ボタンを押していただいたら本人確認は終わります。そのままこのクレジットフォンをレジにお持ちいただいて、このボタンを押してお店の機械に近づけますと機械が電話番号を読み込みます。それを確認してお店の方がご利用金額を打ち込めば終わりです。後はこれまでと同じように打ち出された伝票にサインしていただければ結構です。」

【0232】

お客；「なんべんやっても確認できなかつたらどうなるの」

【0233】

カード会社；「本人確認のときに『もう一度』が3回表示されると認証が出来なくなっ

10

20

30

40

50

てしまいますので、その場合は、申し訳ありませんがカードをお持ちでないクレジットカードがお使いになれません。暗い場所や逆光がきつい場合にご本人を確認できない場合がありますが、頻繁に『もう一度』と表示される場合は登録してある顔写真を変更する必要がありますので、当社の方までご連絡いただくことになります。」

【0234】

お客；「この電話に代えたらどこの店でも使えるの。海外でも？」

【0235】

カード会社；「申し訳ありませんが、今はお店側の機械をこのカメラ付き携帯電話対応型に代えているところです。世界中に約500万ヶ所以上ありますので、暫くはカードと一緒にをお持ちいただく方が安全かと思えます。現在、世界各国にあるサービスセンターと銀行窓口では、このクレジットフォンがご使用になれますのでキャッシュサービスはご利用になれます。」

10

【0236】

お客；「しばらくは両方いるのか。でも、海外に行っていきなり使えなくなったら困るなあ。いじわるな質問をするだけで、現地で怪我をして顔をカメラで確認できなくなったらどうするの。ハワイで日焼けしたとか、八チにさされて顔が歪んだとか」

【0237】

カード会社；「おっしゃるようなケースは考えられます。クレジットフォンには指紋照合用のタイプもあります。本当のことを申し上げますと、こちらのタイプの方が本人確認もが容易で実際のトラブルも少ないのですが、お客さまのなかには『指紋はかなわんな、指紋はいやだ』という人が結構おられます。そのせいか顔写真対応のカメラ付き携帯電話を選ばれる方が多いですね。顔写真と指紋、声紋と顔写真のどちらも使える機種もご用意してありますがそこまでされる方はほとんどおられません。」

20

【0238】

お客；「だいたい分かった。で、申込むにはどうしたらいいの」

【0239】

カード会社；「こちらの申込書に必要事項をご記入いただいて、このカメラでお顔の撮影をさせていただきます。ご本人の確認はお顔でよかったんですね。」

【0240】

お客；「指紋の方が確実だといってもやっぱり指紋はかなわないね。でもここで撮影された顔写真はどうなるの。他の目的に使われたらかなわんなあ。最近、商店街の角かどにビデオカメラは付いているは、会社の入り口や郵便局にも付いている。万引き防止とかいって、スーパーからコンビニまでいつでも買い物のときに顔を撮影されているでしょう。そのカメラのデータと付き合わせたら、私の行動を監視するのは簡単じゃないの？警察ならすでにやっていると思うよ。」

30

【0241】

カード会社；「その通りです。もちろんVISAとしてはそんなことはしておりませんし、日本の個人情報保護法だけではなく、世界中の国々で決められている規則で最も厳しいものに合わせて厳重に管理していますのでご安心ください」

【0242】

お客；「ちょっと待って。ご安心くださいっていっても、もう少し詳しく説明してもらわないと心配は心配だ。」

40

【0243】

カード会社；「ここで撮影した写真は、お申し込みされたお客さんの名前や住所等とは別々に送ります。書類は最終的に郵送でVISAセンターに送られます。途中でデジタルデータに加工することはありません。写真の方は、画像のデータを申込書の番号といっしょにお客さんの個人情報（生体情報）を登録するセンターに送って、カメラ付き携帯電話と生のICカードのチップに直接登録します。カードの表面にもプリントします。このプリントは上塗り部分だけではなく、プラスチック素材の中心まで書込むのでカードが削られても消えることはありません。もちろん指紋の場合はカードにプリントはしません。電話と

50

カードの製造段階ではこの写真の画像データと申込み用紙の番号を記録しますので、実際どなたの写真かだれにも分かりません。ですからデータを送信中、またはカメラ付き携帯電話を製造して本部まで届けてもらうまでに、途中でだれかにデータを盗まれても心配はいりません。それから、登録センターにはお客さんがご希望のカメラ付き携帯電話の品番が送られています。」

【0244】

お客；「なぜ？」

【0245】

カード会社；「登録センターはどのメーカーのどのタイプの電話機に登録したらいいか分からないと困るからです。」

【0246】

お客；「カメラ付き携帯電話やカードに登録した顔のデータはどう処理するの？」

【0247】

カード会社；「そのデータは、また別のコールセンターに送られ、画像登録センターの写真データは完全に消去されます」

【0248】

お客；「コールセンターは何をするところなの？」

【0249】

カード会社；「お客さんが、クレジットフォンやクレジットカードを無くされたときに、申し出られた方がご本人かどうか確認する役割があります。コールセンターにまとめられた顔画像データと申込書の番号を保存するサーバーは、データ保存しておくためだけのサーバーであり基本的にオフラインと考えてください。常時外部に接続することはありません。連絡のあった方の元の画像を検索し、照合用のサーバーに送り出します。」

【0250】

お客；「専門的なことはよくわからないが、顔写真や指紋をカメラ付き携帯電話とカードに入れる場所と、私の名前や住所等知っている場所が違うということだよな。」

【0251】

カード会社；「そうです。お客さんの顔写真や指紋を登録した電話機とカードが発行センターに届けられますと、書込まれている申込書の番号を確認してお客さんに届けられます。発行センターではお客さんに届けた電話機とカードの製造者番号を記録して、お客さんのデータベースに入力します。ここから先の管理の仕方はこれまでと同じシステムです」

【0252】

お客；「送られた電話機にはどんな情報が入っているの？」

【0253】

カード会社；「本人確認用の情報は、顔画像（指紋）データとそのデータから抽出した改竄防止データです。申込書の番号も入っています。」

【0254】

お客；「届いたそのクレジットフォンを使えばクレジットカードと同じように使えるんだよね？」

【0255】

カード会社；「そうです。ただし、最初はお受け取りになったお客さんが申込まれた方と同一であるという照合をしないとお店では使えません。」

【0256】

お客；「え？」

【0257】

カード会社；「送られてきたクレジットフォンでコールセンターを呼び出していただきます。さっき説明したように『本人確認をお願いします』という音声ながれますので同じように顔か指紋を照合してください。そこでご本人であると確認されれば、あとはクレジットカードと同じようにお使いになれます。それまでは、コールセンターはどのお店で

10

20

30

40

50

使われても決済ができないような仕組みになっています」

【0258】

お客；「ちょっと待って、少し混乱してきた。私なりに解釈した中身を説明するから、それで正しいか教えて欲しい。まず私の写真をとってお店から登録センターに送る。それは電話機とカードに私の顔を登録する所ですね。登録してしまえばそこには私の写真はなくなる。そのデータはなくすとか盗まれた場合など万が一の時だけ使うデータとしてコールセンターに保管される。そのデータはオフラインで決済には使わない。そうでしたね」

【0259】

カード会社；「その通りです」

【0260】

お客；「私の顔写真が登録された電話機が本部に届けられてから、私が書いた申込書と照らし合わせて電話機を私に送ってくる。申込書に書かれた内容はお宅の会社のデータベースに登録して保管される。そうすると私が電話機をなくし、自分からコールセンターに連絡して登録した画像を照合して欲しいというまで、クレジット会社は私の顔画像を使うことはない。そうですよね」

【0261】

カード会社；「その通りです」

【0262】

お客；「そうすると、私に送られたカメラ付き携帯電話のデータを他人の顔写真に代えてしまっても分からないんじゃないの」

【0263】

カード会社；「お客さんのようにお考えになる方からそのご指摘はよくあります。そのために私たちはふたつの対策をしています。ひとつは、修正が出来ないようにする仕組みです。電話機やカードに登録した画像を取り替えるとか修正することが簡単には出来ないようにしてあります。しかし、正直申しますと、ITに詳しい人や実際にこの電話の製造に参加した人がやれば不可能ではありません。もうひとつは、改竄防止データを第三者機関に登録できるようになっています。この第三者機関は私どもの会社と経営的には全く分離した認証を専業とする組織です。」

【0264】

お客；「それって面倒臭くない？」

【0265】

カード会社；「さっき、クレジットフォンが最初に届いたときに本人確認をしていただくようになっていると説明しましたが、そのときクレジットフォンに登録されていた改竄防止データが自動的に第三者機関に送信されて登録されるようになっています。もちろんクレジットフォンを申込んでいただいた時に、改竄防止データを第三者認証機関にご登録いただきますという決まりは説明させていただいてご了承いただきます。もちろん義務付けられているわけではありませんので、ご承認されなくても構いませんが、会費の割引やその他の特典を得られなくなってしまいます。」

【0266】

お客；「でもそれって、その第三者機関で悪用されませんか？」

【0267】

カード会社；「顔写真や指紋のデータは一切送信しません。改竄防止データと電話番号、その機器やカードの製造者番号だけを登録しますのでご心配はいらないと思います。」

【0268】

お客；「すると、この電話を使って本人を確認するのは、電話の中だけのデータだけを使うということだね。その元のデータが修正されていないということだけを、私が私の責任で第三者に連絡して確認してもらっていることと理解すべきということだね。」

【0269】

カード会社；「全くその通りです。お客さんご自身がお客さんのお使いいただいている電話機で本人確認をしていただいた結果は、私どものコールセンターとお客さまの電話機

10

20

30

40

50

が一旦保存しますので、その電話機のデータと電話番号がお店やレストランの端末を経由してコールセンターに送信されれば、そのデータ同志が照合されて同時に送られたそのお店でのご利用金額の決済が承認されたこととなります。」

【0270】

お客；「なるほど、それなら私の個人データは電話番号以外一切クレジット決済では使われていないということになるね。」

【0271】

カード会社；「そこまで神経質にならなくてもは、とも思いますが、実はその電話番号を送る場合も暗号化されていますので、一般的な電話の番号通知とはシステムは違ってきます。電話番号がコールセンター内で突き合わせられるまで全く別の通信ラインで送信されますのでそれだけで安全は確保されていると思います。もちろん、これまで電話各社で採用されている番号通知方式も利用できますが・・・その辺りはセキュリティにはあまり影響はないと思います。」

10

【0272】

お客；「やっと、この電話が安全なのかわかった。安心感が全然違うね」

【0273】

カード会社；「最初に説明しようとして、出来ませんでした。実はこのクレジットフォンにはふたつの方法があってお客さまにお選びいただけるようになっています。」

【0274】

お客；「すみません。そう言えば、最初におっしゃってましたね。」

20

【0275】

カード会社；「ひとつは、これまでご説明してきましたVISA（登録商標）決済が可能な電話機をご購入いただくことです。これはお申し込みいただいたときにVISA（登録商標）対応の電話機から選んでいただいてこちらからお送りする方法です。もうひとつは、今お使いいただいている携帯電話の外部拡張端子に取り付けられる決済専用のタグをお使いになる方法です。どちらもシステムは同じです。VISA（登録商標）対応のカメラ付き携帯電話では個人情報の保存と照合システムが電話機に内蔵されたチップをいめますが、専用のタグは同じシステムがタグ内にあります。通信やカメラ、ボタン操作はカメラ付き携帯電話本体を使うことは同じです。専用タグをお使いになれる場合は、ご自分の携帯電話だけではなく他の携帯電話や個人情報を取り込める装置、例えばカメラとか指紋入力装置ですが、その機能さえ満足すれば通信を介して決済が可能になります。その場合は、先ほどから説明させていただいている電話番号をコールセンターとの確認に使わずに、専用タグのIPアドレスを利用することになっています。」

30

【0276】

お客；「そっちの方が便利じゃないの？」

【0277】

カード会社；「色々な方がおられます。どちらも同じようにお使いいただけますが、タグは確かに便利ですね。ただ、皆様携帯電話はまず間違いなくいつでもお持ちいただいておりますが、専用タグはしょっちゅう使わないので忘れられたり無くされる方が比較的多いのが実態です。電話なら探すことは容易ですが専用タグは無くしても通話機能がありませんので、なくされと見付かるケースはほとんどありません。」

40

【0278】

お客；「それでは申し込もう。で申込書は？」

【0279】

カード会社；「こちらにございます。書式はこれまでとほとんどいっしょです。一番下の覧に、クレジットフォンまたはクレジットタグどちらかを選んでいただく欄がありますのでそちらにご記入ください。上の部分は、ご住所や勤務先、ご同居の家族など変更があればご記入ください。それ以外はご不要です。今お使いのカメラ付き携帯電話をそのままお使いになれるのでしたら、クレジットタグをお申し込みいただくほうがいいでしょう。今、お使いの携帯電話の機種と電話番号をご記入下さい。全部ご記入いただいたら、こ

50

の切取線から端の部分を切り離してください。」

【0280】

お客；「これが、さっきから言っていた申込書の番号だね。」

【0281】

カード会社；「そうです。切取線の上下に同じ番号が書かれていますね。その番号は、万が一、途中でデータが消えたり、電話機が届かなかったりした場合、申込書の審査にあたってこちらからご連絡した場合には、必ず申込書の番号をお聞きすることになりますのでキチンと保管しておいて下さい。」

【0282】

(C) 特徴原本データの登録、改竄防止符号の登録の詳細手順

10

【0283】

図3は、特徴原本データの登録、改竄防止符号の登録の詳細手順を説明するためのフローチャートである。

【0284】

動画像を撮影し、正面顔が撮影された画像を選択し、選択された画像を個別に処理して各画像の特徴量を算出し、特徴量を統計的に処理して最終結果を得る。この結果を、特徴原本データとして登録する。特徴原本データとして登録するデータの一部を符号化し、改竄防止符号として登録し、第三者機関に送信する。

【0285】

この一連の動作を同図に沿って下記に説明する。

20

【0286】

(ステップS-1) 動画像撮影、取り込み

【0287】

顔を連続的に撮影し動画像を得る。カラー画像でもモノクロ画像でもよい。

【0288】

(ステップS-2) 正面顔の検出

【0289】

多数の顔のデータベースなどから、図4のようなマスク画像を作成し、原画像を左上から右下に走査して両眼を含む部分を検出する。具体的には、両眼を含んだマスク画像で、図5のように、原画像上にマスク画像を置き、画素ごとに濃度を比較して類似度を計算し、スコアとする。この操作を原画像の左上から1画素ずつ右方向へずらせて繰り返す。右端に達したら1画素下へ移動し左端から右方向へ繰り返す。この操作を右下へ到達するまで繰り返す、最大スコアを閾値と比較し、閾値以上であれば、正面顔と判断する。顔の大きさは、個人差、撮影距離などにより一定ではないため、マスクのサイズを数段階に変化させて以上の処理を繰り返す。顔が回転している可能性がある場合には、たとえばマスクを時計回り、反時計回りに数度ずつ回転し、以上の処理を繰り返す。

30

【0290】

この探索は、1画素ずつずらして走査する方法のほかに、はじめに10画素程度ずつずらせて大域的に探索しスコアを計算し、次にスコアの大きな場所を重点的に探索することもできる。画像ピラミッドを利用して粗い画像を作成し、大域的に探索することもできる。文献(小杉 信、“個人識別のための多重ピラミッドを用いたシーン中の顔の探索・位置決め”、電子情報通信学会論文誌、Vol.J77-D-II, No.4, pp.672-681, April 1994)。ずらせ方は1画素に限定されない。原画像の左上から右下まですべて探索することなく、顔のある確率の高い部分だけ探索することもできる。画像そのままでもウェーブレット変換などの変換をしたのち係数の類似度を計算することもできる。その他さまざまな方法が、文献(M.H.Yang et al “Detecting Faces in Images: A Survey” IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol.24, No.1, Jan. 2002.)に紹介されている。

40

【0291】

(ステップS-3) 正面顔画像の選択

50

【0292】

以上の処理を画像ごとに行い、スコアの大きい順に複数枚の画像を選択する。

【0293】

(ステップS-4) 顔画像正規化

【0294】

選択した画像ごとに、眼及び口の位置を検出する。眼の位置、口の位置にもとづいて、画像を拡大縮小し、正規化する。明るさ、コントラストも、調節する。

【0295】

(ステップS-5) 特徴原本データの登録

【0296】

複数枚の画像を重ね合わせ、図6に示すように、眼およびその周囲、鼻およびその周囲、口およびその周囲の画素について、画素ごとに、濃度の平均値、分散を計算してこれを顔特徴として画素ごとに記録し、特徴原本データとする。また顔の幅なども特徴として特徴原本データに記録する。

【0297】

以上のように画像データそのものを顔特徴として記録する方法のほかに、画像そのままではなくウェーブレット変換などの変換をしたのち係数を顔特徴とし特徴原本データとして記録することもできる。

【0298】

(ステップS-6) 改竄防止符号の登録

【0299】

特徴原本データに登録した画像の指定された1ライン(図6のライン1)上の画素の濃度を加算器にて加算し結果をnビットレジスタに累積し、オーバフローする上位ビットは無視し、下位nビットを改竄防止符号として登録する。

【0300】

(ステップS-7) 改竄防止符号を第3者機関に送信する。

【0301】

(D) 認証機能

【0302】

次に、認証機能の詳細について説明する。動画像を撮影し、正面顔が撮影された画像を選択し、選択された画像を個別に処理して各画像の特徴量を算出し、特徴量を統計的に処理して最終結果を得る。

【0303】

この結果を、特徴原本データと照合し、判定結果と改竄防止符号とを送信する。

【0304】

図8は、これを説明するためのフローチャートである。この一連の動作を同図に沿って下記に説明する。

【0305】

・動画像撮影、取り込み

【0306】

上記ステップS-1 と同様。

【0307】

・正面顔の検出

【0308】

上記ステップS-2 と同様。

【0309】

・正面顔画像の選択

【0310】

上記ステップS-3 と同様。

【0311】

10

20

30

40

50

- ・顔画像正規化

【0312】

上記ステップS-4 と同様。

【0313】

- ・個別顔画像の照合

【0314】

正規化した複数枚の原画像の1枚を特徴原本データと最適に重ね合わせ、眼およびその周囲、鼻およびその周囲、口およびその周囲を特徴原本データと比較し、スコアを計算する。特徴原本データとの比較は画素ごとに濃淡を比較して類似度を計算し、スコアとする。

10

【0315】

原画像と特徴原本データとの比較方法としては、画素ごとの差の2乗の累積値を比較したり、画素配列を特徴ベクトルと考え、特徴ベクトルの内積を求める方法、あるいは画像をウェーブレット変換などの変換をした時の係数を比較する方法等がある。

【0316】

- ・顔認証

【0317】

複数の画像で照合した結果のスコアの平均値を最終結果とする。最終結果としては、中央値、最大値、最大値と分散などを考えることもできる。最終結果が設定した閾値より大きければ、本人と判定する。

20

【0318】

結果の送信

【0319】

判定結果と、改竄防止符号とを送信する。判定結果が否であれば、改竄防止符号は送信する必要はない。

【0320】

改竄防止符号は、記憶装置に記録されたデータをそのまま送信してもよいが、ステップS-6 改竄防止符号の登録と同様の処理をして、ここで新たに得られた改竄防止符号を送信してもよい。

【実施例】

30

【0321】

(実施例1)

次に、上記の実施形態の一実施例について詳細に説明する。

【0322】

本人確認に利用する生体情報を顔画像とし、情報端末側に必要な照合装置と照合に使う原本情報の原本性保証機能を備えた通信システムを開発する。

【0323】

その他の生体情報(指紋、掌紋、声紋、虹彩、遺伝子)については、情報端末の入力機構が異なるだけで、登録された情報や照合するシステムについてはほとんど同じ機構で対応可能であると考えられる。

40

【0324】

本実施例で実現する顔画像認識装置による認証システムは、一般のモバイル端末である携帯端末機器/PDAやノートブック型パソコンで機動するシステムを前提にしているが、市場性のあるカメラ付き携帯電話に搭載することも、また、カメラ付き携帯電話の外部接続端子に差し込んで使う専用の情報処理機能をもつ情報端末装置をも想定した開発である。

【0325】

また、個人用ゲーム用端末やゲームセンター、他の娯楽施設で使われるゲーム機器、また酒類、タバコ、飲料等の自動販売機、交通機関、娯楽施設の自動券売機、有価証券類、住民票等の自動発行機、クレジットカードのキャッシュディスプレイ、金融機関のATM装置、公衆電話機など事業者のサービス提供用の機器など社会的なサービスを提供してい

50

る装置などに、公衆通信網に接続して通信が可能な装置を持たせた場合にも、本発明による認証システムが有効である。

【0326】

以下に、カメラ付き携帯電話を使って本人確認用のための顔画像の特徴原本データを登録する手続きと同画像を用いた個人認証手続きを説明し、この手続きを有効とする技術開発の詳細を概説する。

【0327】

システムの利用手続き

【0328】

(A) 原本情報の登録

10

【0329】

通信手段と撮像装置を備える情報端末で、本人照合用の特徴原本データが未登録の場合、最初に撮像されて登録される画像は自動的に情報端末内の記憶装置に登録され、照合用の原本情報となる。

【0330】

1. 情報端末機器を起動し、画面メニューから「本人確認」を選択する。

【0331】

2. レンズを自分の顔に向けて、画面一杯の顔画像を撮像する。

【0332】

3. 撮像後、画面に表示された画像を確認し、画面上の「登録する」「やりなおし」を選択して登録、もしくは撮影をやり直す。

20

【0333】

4. 前項の記録装置は、最初に登録された画像の書換えもしくは改竄ができない機構を採用する。

【0334】

5. 前項の登録された画像の原本性確認のため、画像データから特定の情報(改竄防止データ)を抽出して記録装置内に保存する。

【0335】

6. 前項の特徴原本データと改竄防止データの登録と同時に、情報端末機器の通信機能を起動し予め設定している第三者機関に接続し、端末機器の情報(IPアドレス、登録済み電話番号)、5.記載の画像照合データを同機関に送信して登録する。

30

【0336】

7. 上記5.から6.までの操作は自動的に行われ、登録が完了した段階で情報端末機器の画面に「登録されました」と表示する。

【0337】

8. 本項目記載のプログラムは、上記記載の撮像装置を、接触センサー読取り装置、音声収録装置、タブレット装置等の入力装置に置き換えて、各々に対応する具体的な生体情報の採録を可能にすることによって、顔画像以外の個人識別情報の場合も同じように動作するプログラムである。

【0338】

(B) 本人確認の手続き－電子メール型

40

【0339】

メール機能を使って、本人確認の結果と第三者(認証センター)の原本保証を添付して個人認証を要求する相手先に情報を送信する場合

【0340】

1. 情報端末機器の認証に関するメニュー表示から「本人確認」を選択する。

【0341】

2. 表示された「電話」「メール」の内「メール」を選択する。

【0342】

3. 撮像機能が立ち上がる。

50

【0343】

4. 表示画面一杯に顔画像を写して、シャッターを押して撮像する。

【0344】

5. 撮像した画像と情報端末に保存されている原本情報が自動的に照合され、正解率が算出され判定結果は一旦保存される。

【0345】

6. 前項の原本情報と照合する撮像画像は、動画像から選定した複数枚の顔画像を使う(顔写真など静止画データを利用した成り済ましを防ぐための機能だが、簡易型の認証では静止画;静止画の照合も可能である)。

【0346】

7. 情報端末機器内で前項の処理を行うと同時に通信機能を起動し、予め設定されているプログラムで特徴原本データから原本の改竄防止データを抽出して、改竄防止データを登録してある第三者機関と交信して原本性を保証したデータ(16ビットの暗号)を取得する。

【0347】

8. 1.から7.までの手続きによって本人確認と原本性確認の処理が完了した段階で、表示画面には「照合しました」もしくは「もう一度撮影してください」のどちらかが表示される。(「もう一度・・・」が表示された場合はくり返す)

【0348】

9. 「照合しました」という表示は「送信する・保存する」に切り替わり、「送信する」を選択すると自動的に新規メール作成画面が立ち上がる。(自動的に判定結果と原本性保証のデータが添付される)

【0349】

10. 必要な項目を入力してからメール画面の「送信」ボタンをクリックすれば相手方に作成した本文と一緒に照合結果原本性の証明データが相手先に送信される。

【0350】

11. 本人確認を要求しているメールに返信する場合は、受信メールから「返信」を選択してから、メニューボタンで「本人確認」を選んで上記の2.から10.まで記載した一連の操作を行い、表示された「照合しました/送信する・保存する」から「送信する」を選択すれば自動的に相手に送信される。

【0351】

12. メール操作の前に、本人確認操作を行うことも可能である。その場合、「照合しました」の後から表示される「送信する・保存する」の「保存する」を選択してから、メール作成を行い編集メニューの「本人確認添付」を選択して送信する。

【0352】

註; この保存機能は、電話による通話でも利用できる。事前に登録してある照合結果を送信することで、簡単に本人確認を行えるようにすることも可能である。

【0353】

註; 保存機能には時間的制約を前提に原本性保証データ取得から送信までの時間を制限する機能を搭載している。当該発明の目的は本人確認については通話もしくはデータ送信行為の当事者を行為と同時に認証することだからである。

【0354】

(C) 本人確認の手続きーカメラ付き携帯電話または電話型

【0355】

電話機能を使って通話中、相手から本人確認を求められた場合。

【0356】

1. 通話を中断しないで、メニューから「本人確認」を選ぶ。

【0357】

2. 表示された「電話」「メール」の内「電話」を選択する。

【0358】

10

20

30

40

50

3. 画面の指示に従って、カメラ機能を使って、表示画面一杯に顔画像を撮像する。

【0359】

4. 画面には「照合しました」もしくは「もう一度撮影してください」のどちらかが表示される。（「もう一度・・・」が表示された場合は1. から4. までの操作をくり返す）

【0360】

5. 「照合しました」の表示に続いて「送信する・認証する」が表示され、「送信する」を選べばそのまま相手に原本照合の結果を送信、「認証する」を選択すると、第三者機関に改竄防止データが送信される。

【0361】

6. 記録されている情報端末内の原本と照合した判定結果（正当率）と第三者機関から送られる改竄防止データの照合結果は暗号化する。 10

【0362】

註；電話機を使った個人認証では、ここで、「照合しました」と表示された後で、第三者機関に対して原本性の照合を要求するか否かの選択メニューが表示されるプログラムとなる。第三者機関は、予め登録された改竄防止データを照合して非改竄証明を行うことが役割であるが、実際に非改竄証明を請求するのはカメラ付き携帯電話はその他の情報端末機器を使用している利用者である。電話による個人認証は利用者の使っている情報端末内で完結する簡易型の本人確認手続きと、第三者機関による個人の情報端末機器内の本人確認の特徴原本データの非改竄証明書を添付する「保証人付」の個人認証に分けられる。

【0363】

20

技術開発の説明

【0364】

本機能を実現するために以下の技術の開発を行うが、これにつき、順次説明する。

【0365】

(1) 本人の顔の認証機能の開発

【0366】

(2) 登録画像データ原本保証用暗号化機能の開発

【0367】

(3) 認証を行うための通信機能の開発

30

【0368】

(4) 携帯端末GUI機能および、初期登録データの改竄防止機能の開発

【0369】

(5) 携帯端末（PDA）へのソフトの移植

【0370】

(1) 本人の顔の認証機能の開発実施例

【0371】

ここでは、本人成りすましを防ぐため、正面顔のみでなく、左右上下の動きのあるビデオ画像を用いて顔の認証を行う技術を開発する。ただし、前記に記述したが、サービス提供者もしくは利用者本人が簡易な認証で構わないと判断した場合は、顔画像を静止画として撮像して照合することも可能である。カメラ付き携帯電話やその外部接続端子に接続する様々な認証機能を備えて情報端末機器の情報処理能力（主に処理速度及び記録容量）を勘案して、静止画による照合も可能な機能を包含するものとして設計されている。

40

【0372】

基本的には、例えばヘブライ大学アムノン・シャシュア（Amnon Shashua）教授の「ビデオ画像を用いたカーネルプリンシプルアングル法による認証技術」を利用して開発を行う。

【0373】

< 技術の概要 >

【0374】

50

画像を用いる顔の認証方法として、スチール写真を用いる方法と、ビデオ画像を用いる方法の2つがあるが、現時点では殆どの認証システムがスチール写真認証法を用いている。

【0375】

スチール写真を用いる顔の認証法では、1枚の写真で認証するため写真を用いた成りすましに対しては、これを防ぐのが困難である。また、この方法では登録時の顔の撮影アングルと、実際に認証するための顔のアングルが殆ど同じでないと認証精度が大幅に低下する。このため殆どの認証方法は、登録時と同一カメラで、同一の場所で、同じ顔のアングルで撮影することを要する。

【0376】

ここでは個人の認証を主要用途とするため、成りすましが最大の問題であり、その問題を回避するため顔の認証方法としてビデオ画像方式を用いる。ビデオ画像を用いると、顔の3次元的画像を得ることが可能であり、成りすましは非常に難しい。

【0377】

本実施例では、ビデオ画像を用いた認証方式として、「カーネルプリンシプルアングル法」を用いた認証法を用いる。この方法は、画像データを高次元ベクトル化し、この画像ベクトルの類似性をカーネルプリンシプルアングル法（類似性をベクトルの内積で計る。）により、その類似性を検証し、ある閾値以上の類似性を示した場合本人であると認証する方法である。

【0378】

具体的には、携帯電話のカメラで顔のビデオ画像を撮影し、この画像データを用いて、登録してあるビデオ画像を数値化した登録データ値（ベクトル値）と比較し、カーネルプリンシプルアングル値を算出し、類似度を測定し、その類似度を、例えばパーセンテージ（<80%>等）で出力し認証を行う。

【0379】

本実施例に係る機能を実現するために以下の技術の開発を行う必要があるが、この詳細については上述したことを参考に、ここでは割愛する。

【0380】

- ・画像の多次元ベクトル化法の開発

【0381】

- ・多次元ベクトル間のカーネルプリンシプルアングル算出法の開発

【0382】

- ・サポートベクターマシン法を用いた学習法の開発

【0383】

- ・照明変化に対してロバストな認証法の開発

【0384】

- ・本人認証結果送受信フォーマットの開発

【0385】

（2）登録画像データ原本保証用暗号化機能の開発の実施例

登録された認証用画像データが改竄されて悪用されることを防ぐため、携帯端末に登録されている認証用画像データが改竄されていないことを保証する原本情報（認証用画像データ）の原本性保証機能を備えた通信システムを開発する。

【0386】

<技術の概要：2>

【0387】

登録された複数枚の認証用画像データのある特定のエリア（例えば各画像の100番目の走査線から110番目の走査線のエリア：特に認証に用いられるエリアが好ましい）の輝度デジタルデータの和を算出し、その和のうちデジタルで下16ビット（例えば宝くじの下5桁の数字）を登録する。もし一部でも改竄されるとこの数字が変化するため、原本性を検証することが可能となる。この下16ビットのデータを原本保証センターに登録す

10

20

30

40

50

る。本人認証を行う時に携帯端末の原本データの該当する16ビットデータを送信して、センターにて登録データと照合して原本性を確認し、その旨の証明を原本保証センターから送受信する機能。

【0388】

本実施例に係る機能を実現するために以下の技術の開発を行う必要があるが、この詳細については上述したことを参考に、ここでは割愛する。

【0389】

- ・複数毎の輝度データの最適抽出エリアの自動抽出法の開発

【0390】

- ・輝度データの下16ビット化法の開発

10

【0391】

- ・原本保証登録方式と照合方式の開発

【0392】

- ・原本保証結果送受信フォーマットの開発

【0393】

(3) 認証を行うための通信機能の開発の実施例

【0394】

上記(1)、(2)では顔認証機能および原本保証機能の個々の機能の開発を行うが、ここでは、システム全体の通信機能の開発を行う。特に、携帯端末を紛失した場合の対応方式、同時に多数のタスクが来た場合の対応、データの修正、改訂に関してのシステムとしての堅牢性等を実現するための開発を行う。

20

【0395】

本実施例に係る機能を実現するために以下の技術の開発を行う必要があるが、この詳細については上述したことを参考に、ここでは割愛する。

【0396】

- ・認証結果送受信、原本保証結果の送受信に関する通信システムの開発

【0397】

- ・携帯端末紛失等の処理システムの開発

【0398】

- ・データの改訂、修正システムの開発

30

【0399】

- ・通信の堅牢性を保持するための開発

【0400】

(4) 携帯端末GUI機能の開発及び初期登録データ改竄防止機能の開発の実施例

【0401】

携帯端末は、直接ユーザとコンタクトする機器であり、その使い勝手が本システムの普及率を左右する可能性が大きい。ここでは、ユーザが使い易いGUIを開発し、簡単に、何時でも何処でも使えるシステムとする。また、初期登録データ改竄防止機能の開発も行う。

40

【0402】

本実施例に係る機能を実現するために以下の技術の開発を行う必要があるが、この詳細については上述したことを参考に、ここでは割愛する。

【0403】

- ・認証登録操作GUIの開発

【0404】

- ・原本保証操作GUIの開発

【0405】

- ・本人認証操作GUIの開発

【0406】

50

- ・初期登録データ改竄防止機能の開発

【0407】

- (5) 携帯端末(PDA)へのソフトの移植の実施

【0408】

本実施例は、最終的には本機能の携帯電話への搭載を目的とするが、ここでは本機能の有効性の検証を主眼とするため、携帯端末としてはPDAを用いて実証を行い、その有効性を確認する。ここでは、上記開発されたソフトをPDAに移植し、その機能を確認する。その目的は、今後考えられる高度情報化社会における電子決済機能を通信手段を介して求めるサービス提供者とサービス享受者との間での契約行為で、通信手段を使って何等かの決済が必要となった場合で、既存のサービス提供装置の認証手段として移植可能なプログラムであることが前提になっているからである。

10

【0409】

本実施例に係る機能を実現するために以下の技術の開発を、行っているが、この詳細については上述したことを可能にすることを前提に、ここでは詳細の記述を割愛する。

【0410】

- ・本人登録機能の移植

【0411】

- ・顔認証機能の移植

【0412】

- ・原本性保証機能の移植

20

【0413】

- ・GUI機能の移植

【0414】

- ・通信機能の移植

【0415】

最後に、本人確認を行うタグの利用パターン例を挙げておく。この中には、一部カメラ付携帯電話やその他の情報端末を使う事例も含まれる。

【0416】

金融機関の窓口で口座開設をする。

【0417】

通信手段を介して出金と送金を行う。

30

【0418】

・銀行口座の預金出金と口座振替時には、銀行は口座開設者が手続きを行っていることを必ず認証しなければならない。

【0419】

・認証の基本は、銀行側が手続きをしようとする口座開設者が本人であることを確認することである。

【0420】

・本人確認の方法には、窓口の行員が本人の顔や持参した通帳とハンコの印影または署名を確認する方法と、ATMや通信を介する場合の、登録済の暗証番号かパスワードを確認する方法がある。

40

【0421】

- ・本人確認の実際は、厳密な意味での本人を直接確認しているわけではない。

【0422】

・本人が確保している前提の通帳とハンコ、本人以外が知らないという前提の番号やパスワードを使い、結果として本人確認をしたことにしているのである。

【0423】

・ただし、通帳とハンコでは手続きをした人間を銀行側が視認していること、ATMでは手続きをした人間をビデオカメラで撮影して認証のバックアップをしている。

【0424】

50

・通信を介した銀行口座の預金出金と口座振替では、ATMと同じように暗証番号もしくはパスワードを使うが実際にはだれが端末を操作したかを後から確認する方法はない。

【0425】

・本発明では、通信機能をもつ情報端末を操作して銀行口座にアクセスしている人間が口座を登録した本人であることを確認することを可能にしている。

【0426】

・本発明では、口座の決済に使う情報端末内、もしくは情報端末の拡張端子に予め登録された口座開設者本人の生体情報を、本人確認に利用する。

【0427】

・本発明では、本人確認に使う予め登録した生体情報が改竄されていないことを第三者が証明するため、改竄防止情報を当該第三者に登録しておく必要がある。

【0428】

具体的な使用方法を以下に説明する。

【0429】

・口座開設者が、預金出金と口座振替をする目的で銀行またはその他の金融機関にアクセスし、銀行から本人確認を要求された場合は、その通信を維持したまま本人の生体情報を保存してある拡張端子を携帯電話の外部端子に差し込む。

【0430】

・顔画像を使う場合は、カメラ付き携帯電話や情報端末に取り付けられているデジタルカメラで自分の顔画像を撮像し、本人確認の操作を行う。

【0431】

・本人確認用に撮像された画像は情報端末内の記録装置に登録済みの原本と照合され、その正解確率が算出される。

【0432】

・「本人確認されました」という表示を本人が確認した上で、第三者機関に非改竄の証明を要求し、証明した結果を情報端末で受信する。

【0433】

・証明データの受信を確認して、必要な口座手続きの端末操作を行った上で、本人確認の結果、証明データといっしょに送信して手続きを完了する。

【0434】

・上記の手続きは、指紋、掌紋、静脈パターン、声紋、虹彩、網膜パターン、遺伝子を使う場合も、生体情報を入力する装置を除いて手続きは同じである。

【0435】

・同時に、記録装置に保存してある改竄防止情報を第三者機関に送信して原本が非改竄であることを証明するデータを受信した上で、本人確認の照合結果と合わせて本人確認データとして、口座手続き操作データと一緒に銀行に送信して手続きを完了する。

【0436】

・生体情報が顔画像の場合は、カメラ付き携帯電話もしくは情報端末に接続したデジタルカメラで撮像した顔画像を使って照合を行う。

【0437】

・生体情報が指紋、掌紋、静脈パターンの場合は、センサ、声紋はマイク、遺伝子の場合は専用のセンサを使って情報を入力して原本と照合する。改竄防止データを第三者機関に送って非改竄を証明してもらう方法は同一である。

【0438】

カメラ付き携帯電話をつかった口座取引

【0439】

金融機関 / 銀行・証券会社の本人確認

【0440】

口座開設者 ; 「もしもし。口座振り替えをしますのでお願いします」

【0441】

10

20

30

40

50

- 金融機関；「わかりました。お客様の口座ですね」
- 【0442】
- 口座開設者；「はい」
- 【0443】
- 金融機関；「ご本人の確認をいたします。登録はお済みですね」
- 【0444】
- 口座開設者；「はい」
- 【0445】
- 金融機関；「顔画像認証？指紋認証？どちらをお使いですか」
- 【0446】 10
- 口座開設者；「顔画像です」
- 【0447】
- 金融機関；「お使いのお電話はご本人のものですか」
- 【0448】
- 口座開設者；「いいえ。私のものではありません」
- 【0449】
- 金融機関；「ご本人確認にお使いになるのは認証タグですね。認証センターに登録はお済みですか」
- 【0450】 20
- 口座開設者；「はい」
- 【0451】
- 金融機関；「それではお客様のお名前、店番号と口座番号をお願いします」
- 【0452】
- 口座開設者；「コヤマユウジ。店番号は432。口座番号は普通口座202033459276です」
- 【0453】
- 金融機関；「いくつか質問をさせていただきます。生年月日は1952年7月7日ですね」
- 【0454】
- 口座開設者；「いいえ。1949年8月24日です」 30
- 【0455】
- 金融機関；「わかりました。最後に送金された日付はいつでしょうか」口座開設者「確か、先月末です。」
- 【0456】
- 金融機関；「わかりました。それでは認証タグを今お使いのカメラ付き携帯電話の外部接続端子に差し込んで、ご本人を確認してください」
- 【0457】
- ・・・・・・・・・・・・・・・・
- 【0458】
- 口座開設者；「これでいいですか」 40
- 【0459】
- 金融機関；「確認しました。それでは振替え先の口座番号をお願いします」
- 【0460】
- ここから先は、事務的手続きである。
- 【0461】
- インターネット、iモードを使ってメールで口座振り替えなどの手続きをする場合は次の通りである。
- 【0462】
- ・口座振り替え用の入力画面を呼び出して、本人の個人情報、口座番号などのデータ、振替先の口座番号と氏名など、金融機関が要求する項目に記入する。 50

【0463】

・「送信する」ボタンを選択して相手方のセンターに接続すると、本人確認が必要な場合は、「本人確認手続きをして下さい」と応答して来る。

【0464】

・「本人確認をする」ボタンを選択して、カメラ付き携帯電話で自分の顔を撮像し電話機内で本人照合、第三者機関から非改竄証明データを受け取って、「本人確認が終了」の状況を確認して、振替用の入力画面に戻り改めて送信し手続きを完了する。

【0465】

証券会社、保険会社、クレジットカード会社、消費者金融機関等、電子決済を行う場合は同じ方法で本人確認をすることが可能である。カメラ付き携帯電話もしくはその他の通信機能をもつ情報端末にセットして使用する認証タグは、金融機関が直接発行し管理している認証機能ではないため、全ての組織で本人確認を行う個人認証手続きに利用可能である。

10

【0466】

優良顧客のプライベートバンキングに活用

【0467】

銀行が取引きを重視する資産家に対するプライベートバンキングの営業の考え方が、外資系銀行からわが国の金融機関に広がっている。

【0468】

資産運用のコンサルティングを含んで、クレジットカード利用額の無制限、テレフォンバンキング、ネットバンキング口座の活用など、便利さとともに銀行、顧客とも金融決済事務手続きや資産に係わる個人情報漏洩など事故や犯罪防止の必要性が非常に大きくなっている。

20

【0469】

通信手段を介して金融機関とやり取りする情報の安全性を高めるために本発明である認証タグを口座開設者に配付することによって、常時、本人確認による個人認証手続きが容易になる。

【0470】

プライベートバンキングの口座開設と手続き

【0471】

口座開設者；「口座を開設して下さい」

30

【0472】

外資系銀行；「わかりました。こちらの申込書に必要事項を記入して、住民票を添付して後日、提出して下さい。申し込みはご本人にお出でいただくことになっております、当日は事前にご連絡いただいで、運転免許証かパスポートをお持ちください」

【0473】

・・・出直しである。

【0474】

口座開設者；「全部揃えてきました」

【0475】

外資系銀行；「わかりました。しばらくお待ちください」

40

【0476】

外資系銀行；「当銀行では通帳は発行しておりません。取引実績は毎月ご指定の住所に送付します。日々のお取引は電話またはインターネットで決済できますので、お電話かパソコンからお願いします。ただし、ご本人の確認が必要ですので、顔写真か指紋を登録いただいた認証タグをお送りしますので、カメラ付き携帯電話か、指紋照合ができるパソコンなどをお使いください。もちろん窓口にお出でいただいてもいいですが御本人をご確認できるものをお持ちください。」

【0477】

口座開設者；「便利そうだけど、面倒くさそうですね」

50

【0478】

外資系銀行；「これまでのように暗証番号やパスワードだけでは、悪質な成り済ましに対する対抗が出来ませんでした。この方法ですと、当行がお渡しした認証タグをカメラ付き携帯電話の外部接続端子に差し込むだけで、その電話をされている方がご本人かどうか確認できますので事故が防ぐことができます。指紋でも同様です」

【0479】

口座開設者；「いちいち顔写真や指紋をやり取りしてたら、その情報自体が盗まれる恐れがないですか」

【0480】

外資系銀行；「登録いただいた個人情報通信では一切送受信しません。お持ちのカメラ付き携帯電話やパソコンとその認証タグとの間のやり取りだけですのでご心配いりません」 10

【0481】

口座開設者；「その認証タグとやらを、取引の時に常に用意していただければいいんですね」

【0482】

外資系銀行；「はいそうです。それだけではありません。お客さんは今クレジットカードやお使いですね」

【0483】

口座開設者；「はい。V I S A（登録商標）。M A S T E R S（登録商標）。J C B（登録商標）です。」 20

【0484】

外資系銀行；「この認証タグをお使いいただくと、利用額の制限のないV I S A（登録商標）カードを発行させていただきます」

【0485】

口座開設者；「海外旅行をするときは便利ですね」

【0486】

外資系銀行；「預金の範囲内の買い物がいつでも出来ますので、高額になっても安心してしょう。ポイントサービスなどが桁違いに貯まりますよ」

【0487】

口座開設者；「お願いします」 30

【0488】

外資系銀行；「それでは、こちらの書類にもご記入下さい。口座開設用のお写真をV I S A（登録商標）カードの決済用に利用する承諾書です。後からお送りするV I S A（登録商標）カードにはその写真が記録されています。身分証明書の写真がブラインドになっていると思って下さい。そのカードは専用の読取り装置と照合用のデータ読取り装置を備えた端末をおいてあるお店でお使いになるか、I Cカード対応型の認証タグをご用意いただくこととなります。銀行決済用の認証タグは、口座を開設されたお客さま全員にお渡ししますが、I Cカード対応のタグは有料となります」

【0489】

口座開設者；「その認証タグを使わなかったら不便やね」 40

【0490】

外資系銀行；「認証タグやデータを読取る装置がない場合は、普通のクレジットカードとしてどの店でもご利用になれます。ただし、その場合は安全性を考慮して通常の利用金額の制限がかかります」

【0491】

口座開設者；「わかりました」

【0492】

外資系銀行；「それでは、これで口座開設の手続きは終わります。最後にこのカメラでお写真を撮らせていただきます」 50

【0493】

航空券の予約と回数券

【0494】

関西空港の日本航空（登録商標）のカウンターで

【0495】

係員；「どちらまでご利用ですか」

【0496】

乗客；「羽田です」

【0497】

係員；「次のフライトは328便になりますが。どのような航空券をお持ちですか」

【0498】

乗客；「インターネットで登録した回数券ですが、まだ残っているはずですが」

【0499】

係員；「お名前とお電話番号か生年月日を頂戴できますか」

【0500】

乗客；「コヤマユウジ。0662299185です」

【0501】

係員；「（発券センターにアクセス）・・・・・・・・。後1枚だけご利用できますね。全日空（登録商標）さんの航空券ですが、こちらをお使いになりますか」

【0502】

乗客；「はい」

【0503】

係員；「この券ですと、ご本人しかご利用になれません（註1）。失礼ですが携帯電話でご購入された時にお使いになった認証タグをお持ちでしょうか（註2）」

【0504】

乗客；「このタグでいいですか」

【0505】

係員；「結構です。このタグはお顔の確認（註3）ですね。こちらの端末に差し込んでいただけますか」

【0506】

乗客；「これでいいですか」

【0507】

係員；「はい。そのままこちらのカメラのレンズを見ていただけますか・・・・・・・・はい結構です。こちらが搭乗券になります。搭乗口は67番です。いってらっしゃいませ」

【0508】

（註1）本人確認には次のような方法がある。ただし、1と2のケースは、利用者が航空券を所持してカウンターで搭乗を申込みの場合に限られる。有価証券として扱われる航空券に記載された個人データは利用者の権利と責任の所在を証明するものであり、利用者が限定される航空券では本人確認が必要になるが、航空券を所持していない場合は、航空券の購入者と利用者の特定が問題になる。本発明は、インターネットや電話を使って申込みされた利用者限定の航空券の本人確認が可能なシステムを提供するものである。

【0509】

1；運転免許証、パスポート、航空会社によっては社員証、学生証など写真が添付されているIDカードの視認。

【0510】

2；本人の写真がプリントされているクレジットカード（磁気カードとICカード）の視認と通信を介した発行者に対する有効確認。

【0511】

3；本人の生体情報の原本情報が記録されている情報媒体（認証用タグ、ICカード、

10

20

30

40

50

携帯電話、PDAなど)と、窓口で入力する原本に対応する個人情報の照合と、第三者に対する改竄防止データの確認。

【0512】

(註2)回数券や年齢制限、家族割引など利用者を特定する必要がある航空券を電話またはインターネットの電子決済で購入する場合は、本人確認用の認証用タグを使って利用者名と認証で使用した装置の認識番号(または電話番号、メールアドレス)を登録する。

【0513】

(註3)指紋照合の場合も手続きは同じ手続きを踏襲する。航空会社のカウンターに設置された専用端末に備えられた指紋入力装置に指紋の形状を認識させて、登録済みの原本データと照合して本人を確認する。

10

【0514】

カメラ付き携帯電話で回数券を購入する

【0515】

乗客;「もしもし。東京大阪のネット回数券をお願いします」

【0516】

発券センター;「わかりました。携帯電話でお掛けですね。ご本人の確認ができる携帯電話ですか」

【0517】

乗客;「はい」

【0518】

発券センター;「ご本人だけしかお使いできませんが構いませんか。」

20

【0519】

乗客;「はい」

【0520】

発券センター;「今電話をお掛けのお客様がお使いになれますか。お名前と生年月日をお願いします」

【0521】

乗客;「コヤマユウジ。1949年8月24日です」

【0522】

発券センター;「いつからお使いになりますか。その日から90日間有効になります」

30

【0523】

乗客;「8月1日からお願いします」

【0524】

発券センター;「それではご本人確認をいたしますので、お願いします」

【0525】

乗客;「・・・・・・・・・・・・・・・・これでもいいですか(註4)」

【0526】

発券センター;「結構です。それではご搭乗の時もこの携帯電話をお持ちいただくようお願いします」

【0527】

乗客;「はい」

40

【0528】

発券センター;「いつも日本航空(登録商標)をご利用いただきありがとうございました」

【0529】

(註4)乗客は、発券センターとの通話を維持したまま、カメラ付き携帯電話で自分の顔を撮像して、電話機または拡張端子に登録されている原本画像と照合した結果と、同時に改竄防止データを使って第三者機関から取得した非改竄証明結果を。発券センターに送信して、本人確認を終える。

50

【0530】

自治体の戸籍掛で住民票と印鑑証明をもらう

【0531】

住民；「印鑑証明書と住民票をお願いします」

【0532】

戸籍掛；「住基カードとご本人をご確認するものが必要になります」

【0533】

住民；「どんなものいるのですか」

【0534】

戸籍掛；「運転免許証、パスポートです。健康保険証は写真がないため今年から使えなくなりました。住基カードで本人確認用の登録をされている場合は住基カードだけでも構いません。後は認証タグがお使いになれます」 10

【0535】

住民；「私は主人の代わりに来たので、これは主人の住基カードです。確か本人確認の登録はしてあるはずですが」

【0536】

戸籍掛；「その場合はご主人しかお使いになれません」

【0537】

住民；「どうしてですか」

【0538】

戸籍掛；「ご主人の住基カードをその専用の端末機に入れて、ご本人の顔をこのカメラで撮影して、カードに登録してあるご本人の顔と照合して、申請者を認証するからです」 20

【0539】

住民；「主人は忙しくて来られませんので、なんとかなりませんか」

【0540】

戸籍掛；「電話かインターネットでもご本人の確認ができれば、住民票と印鑑証明書の発行は可能です。ご主人は本人確認用のカメラ付き携帯電話か認証タグをお持ちですか」

【0541】

住民；「はい。持っているはずですが」

【0542】

戸籍掛；「それでは、今ご主人に連絡していただいて戸籍掛のこの電話番号に、お持ちのカメラ付き携帯電話で番号通知にして電話を掛けてもらってください」 30

【0543】

.....

【0544】

戸籍掛；「はい。天王寺区役所戸籍掛です。小山さんですか」

【0545】

主人；「はい。」

【0546】

戸籍掛；「奥さんが見えられてご主人の印鑑証明書と住民票をご請求になっていますが、ご存知ですね」 40

【0547】

主人；「はい。知っています」

【0548】

戸籍掛；「それでは、いくつかご質問させていただきます」

【0549】

主人；「はい。」

【0550】

戸籍掛；「まずご主人の生年月日をどうぞ。」

【0551】

主人；「1949年8月24日です」

【0552】

戸籍掛；「天王寺区に転居されていますが、いつ頃ですか。それと前住所はどちらですか」

【0553】

主人；「確か。5年前の2月頃です。登録した日はしりません。前は阿倍野区の北畠1丁目です」

【0554】

戸籍掛；「結構です。ではご本人の確認をしていただきます。方法をご存知ですね」

【0555】

主人；「はい」

【0556】

戸籍掛；「それではお願いします」

【0557】

・・・カメラ付き携帯電話を使った認証は前掲と同じ・・・

【0558】

主人；「・・・これでいいですか」

【0559】

戸籍掛；「はい結構です。それでは奥様に・・・でよろしかったでしょうか、おいでいただいている女性の方に住民票と印鑑証明書をお渡ししておきます」

【0560】

主人；「わかりました。ありがとうございました」

【0561】

住基カードなどICカードで本人確認をする方法

【0562】

住基カードに生体情報を登録して本人確認をする方法は次の通りである。

【0563】

1．住基カード搭載の記憶媒体で、住民が自由に書込み読み出して利用できる記録部分に、本人確認用に生体情報を登録する。

【0564】

2．同情報から抽出した改竄防止データもチップに登録すると同時に、第三者機関に改竄防止データだけを送信し登録を行う。

【0565】

3．住民の本人確認が必要な場合は、窓口に備えられた専用端末にカードを挿入し、同端末に内蔵または接続された生体情報読取り装置で入力した申請者の生体情報とカードに登録した情報を使って、カード持参者とカード登録者を照合する。

【0566】

4．住基カードに生体情報を登録して本人確認手続きを提供するサービスと、同情報の改竄防止データを使って非改竄証明を行うサービスの提供は、自治体もしくは民間事業者どちらが行うことも可能である。

【0567】

5．1から4に記載される生体情報は、顔写真だけではなく、指紋、掌紋、静脈パターン、虹彩、声紋、遺伝子などについても有効である。

【0568】

クレジットカードの決済に本人確認を使う

【0569】

クレジットカードの不正利用が急増している。クレジットカードはカードを所持している人間が、正当の利用者と想定して成立する信用決済手続きである。基本的に、従来の通帳とハンコまたはサイン（自署署名）の組み合わせによる決済手段が通信手段を介して行われると解釈して成立している決済システムである。

10

20

30

40

50

【0570】

そのシステムの信用秩序が成立し、信用供与機能が成立したのは、クレジットカードを申込んだ人物の事前審査が厳密だったからである。しかし市場競争が激化して入り口での信用調査はほとんど機能しなくなっている。サインについても決済に対する物証能力は乏しく、成り済ましやデータ改竄、スキミングなどの被害は保険でまかなっているのが現実である。

【0571】

本発明である本人確認装置である認証タグは、カードの所持者とカード名義人を同一人物であると確認することを可能にする装置である。具体的な流れを以下に説明する。

【0572】

・クレジットカードの発行時に、顔画像データをクレジットカード本体の記録媒体に記録する。

【0573】

・同時に原本とする同画像データから抽出した改竄防止データも登録しておく。

【0574】

・カードが本人に送られた段階で、カードから改竄防止データを認証タグに備えられたICチップ読取り装置で読取って第三者機関に送信、カードを特定する番号といっしょに登録する。同第三者機関は、カード発行機関が認証サービスを行う場合も考えられるが、仕組みは同じである。

【0575】

・カードを利用する場合は、所有しているカメラ付き携帯電話にICチップに登録してある顔画像データを読取る装置を備えた認証タグをカメラ付き携帯電話の外部接続端子に差し込んで、カメラ付き携帯電話のカメラで撮像した顔画像と照合して本人を確認する。

【0576】

・本人確認を実行すると同時に、改竄防止データを使って非改竄の証明データを取得する。

【0577】

この非改竄証明は、カード会社が定める期間内にバッチシステムで証明して、その結果をクレジットカード本体の記録装置に登録して本人確認の結果のバックアップに利用することも可能である。

【0578】

また、クレジット会社または第三者機関から受けた非改竄証明データがカードの記録部分登録されていない限り、サービス提供者が使用する決済センターにデータを送信する専用の端末装置とカードのデータチップが情報の通信を行うことが出来ないようにすることによって、クレジットカードから個人情報やカード決済情報が読み取れないようにすることが出来る。

【0579】

この方式は、クレジットカードのセキュリティを解読し、決済データを盗んで成り済ましの犯罪に悪用されることを防ぐ目的がある。通信を介して決済直前に個人が占有する専用端末でアクセスした結果を暗号化してクレジットカードに登録し、各店舗やサービス拠点の情報端末で読取ってカードセンターに接続することで、カードからのデータ読み出しとデータの改竄を防ぐことが容易になる。

【0580】

カードの発行会社は、カード発行時に個人情報を登録した申込者に不正被害が発生することがなくなるアドバンテージを提供しサービスの向上に利用することが可能である。

(実施例2)

次に、上記の実施形態の別の一実施例について詳細に説明する。

<クレジットカードの決済システムの問題点と解決手段>

成り済ましによる被害が多発するクレジットカード決済の問題点は、カードのクレジットラインがリニアであること、閉じることで責任をカード発行者に一元化していることに

10

20

30

40

50

ある。カードの発行からカードの使用、カードの決済まで相当な時間が要するため、カード発行会社とカード所有者がその事実を確認する段階ではすでに被害が発生した後にならざるを得ないからである。この模様を図9に示す。

【0581】

カード所有者のカードデータのスキミングと、カード利用者が通信を使ってカードデータを送信する際にデータを盗まれるケースが被害のほとんどである。

カード利用者によるカード所有者の本人確認は署名によるためカードが偽造されている場合は成り済ましの防ぎようがない。

犯罪者は、世界中に散らばっている数百万軒のカード利用ポイントをカード発行者と所有者のラインから切り離すことによって、そのポイントから商品やサービスを盗み出すことが簡単に出来る。

クレジットカードシステムの決済構造の改革

R & Dが設計したクレジットカード決済システムは、これまでリニアに閉じていた発行者と所有者、利用者のクレジットラインを各々独立させ、かつカード使用時の決済をリアルタイムで平行なダブルラインで行うようにするものである。最も難しいカード所有者とカード利用者の中で発生していた本人確認手続きを止めてデータ盗聴の可能性を完全に排除したことである。

【0582】

図10に示すように、カード所有者はカードを使用する場合は、カード決済機能をもつ携帯電話を使って本人確認を行いカード発行者のカード認証センター（仮称）にその結果を送信する。カード利用者は本人確認の結果を待ってその携帯番号と請求金額を店舗の決済端末に入力してカード認証センターに送信する。カード認証センターはそれらの手続きを確認してカード所有者の携帯電話に結果を送信し、カード所有者は送られて来たメール記載の決済データを確認した上でカード認証センターに送信して全ての手続きを終えることになる。

【0583】

この方式による決済方式では、カード所有者を認証する携帯電話や携帯番号が盗まれた場合でも、カード決済に手続きでの成り済ましが成立しない。

盗んだ電話で本人認証をする場合は、携帯番号に登録してある生体情報と所有者を照合するために携帯電話だけではカードセンターに本人確認データが送信できない。携帯番号は既知の情報として扱われているため、仮にその番号で第三者がカードセンターにアクセスしても携帯電話を使った本人確認通知がない限り、センターはその第三者に正当性を通知できないことになる。

【0584】

本人が自分の携帯電話でセンターに本人確認通知を行い、その携帯番号を知った第三者が他の決済端末（成り済ましの端末）から、センターにアクセスしその携帯番号を入力すれば正当性確認の通知が来て請求金額を送信することによって決済は可能である。ただしその場合でも本人の携帯電話には請求金額と店舗名が送信されるためその段階で決済しても本人の被害は発生しないことになる。言い換えれば、購入した商品やサービスは本人に占有または消費されており、決済端末に成り済ましても犯罪が成立しないのである。

【0585】

携帯番号を搾取しても、生体情報の改竄をしない限りカード決済に必要な本人確認が不可能である。携帯電話に搭載する原本の非改竄データを第三者の認証機関が保有することで原本の非改竄証明が可能となる。カード決済時には、第三者の認証機関経由で非改竄証明書がカード認証センターに送られる。

【0586】

カードの成り済ましは、カードの正当性と決済確認の時間ギャップを利用したものであるが、本人確認をカード所有者が行うことによって犯罪に使われる。この模様を図11に示す。

クレジット決済のパターン

10

20

30

40

50

クレジット決済の前に事前に本人確認を行う場合

カード利用者（サービス提供者）の請求額の入力前に本人確認を行う。レストランで着席したまま決済する場合に有効である。携帯電話の所有者の正当性確認を素早く行うことが出来る。またクレジット会社の規定によって、毎回の決済時に本人確認を行わず、一定の間隔（例えば、8時間、24時間、または1週間など）で本人確認を有効とする方法も考えられる。

1；決済前の本人確認パターン

図12に示す。

2；決済要求データ入力後の本人確認パターン

図13に示す。

【0587】

以上詳細に説明したように、本発明によれば、昨今増加の一途を辿っているクレジットカードの（組織的）犯罪を有効に防止することにも十分資することができる。

【産業上の利用可能性】

【0588】

本発明にかかる個人認証方法とプログラム実行システムは、たとえば携帯電話機などの情報端末機器の利用者は、自己が購入もしくは自己が所属する組織から支給され自己の管理下となった情報端末機器に、利用者本人の個人認証を目的として、本人確認が可能な生体情報を入力して本人確認の照合に使用することを目的としている。本発明では、利用者が個人認証を目的として情報端末に最初に登録した照合用の生体情報は、登録後の改竄ができない記録方式である。その記録装置自体に施された技術的な対策である改竄防止の仕組みと、最初に登録した原本情報から抽出した改竄防止情報が通信回線を通じて第三者機関に登録されることによっている。従って、個人情報データを外部に送信しない本発明の認証方式が社会的に成立する根拠は、利用者個人の識別が可能な個人情報である顔画像等の生体情報の改竄防止情報を、認証要求者が客観的に評価する第三者に登録され、該機関が非改竄を証明することによる。

【図面の簡単な説明】

【0589】

【図1】本発明の実施形態に係る個人認証装置の構成の一例を示すブロック図である。

【図2】本発明の実施形態に係る個人認証装置の構成の別の一例を示すブロック図である

。 【図3】本発明の実施形態に係る個人認証のための特徴原本データの登録、改竄防止符号の登録の詳細手順を説明するためのフローチャートである。

【図4】本発明の実施形態に係る個人認証のための特徴原本データの登録、改竄防止符号の登録の詳細手順の説明するためのイメージ図である。

【図5】本発明の実施形態に係る個人認証のための特徴原本データの登録、改竄防止符号の登録の詳細手順の説明するためのイメージ図である。

【図6】本発明の実施形態に係る個人認証のための特徴原本データの登録、改竄防止符号の登録の詳細手順の説明するためのイメージ図である。

【図7】本発明の実施形態に係る個人認証のための特徴原本データの登録、改竄防止符号の登録の詳細手順の説明するためのイメージ図である。

【図8】本発明の実施形態に係る個人認証のための認証機能の詳細手順を説明するためのフローチャートである。

【図9】クレジットカードについての暗証番号の盗用・成りすましのシステムの原理を説明するための概念図である。

【図10】クレジットカードについての暗証番号の盗用・成りすましをシステム的に防止する本発明の考え方を説明するための概念図である。

【図11】本発明の本人認証付き携帯電話、クレジットカード携帯電話申込の考え方を示すためのタイミング・フローチャートである。

【図12】本発明に係る決済前の本人確認パターンの考え方を説明するための概念図であ

10

20

30

40

50

る。

【図13】本発明に係る決済要求データ入力後の本人確認パターンの考え方を説明するための概念図である。

【符号の説明】

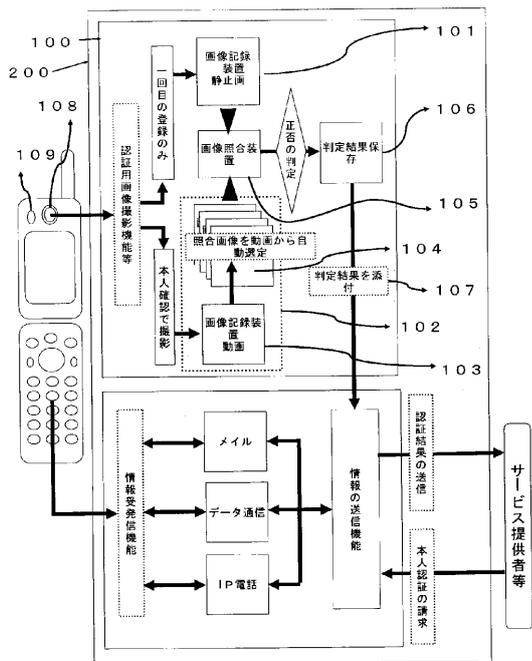
【0590】

- 100 ... 個人認証装置
- 101 ... 原本画像記録装置
- 102 ... 認証時の顔画像データ処理部
- 103 ... 撮像動画像記録装置
- 104 ... 静止画像選別装置
- 105 ... 画像照合装置
- 106 ... 照合判定結果保存装置
- 107 ... 照合判定結果添付・送装置
- 108 ... カメラ
- 109 ... 撮像フラッシュ装置
- 200 ... カメラ付携帯電話機
- 300 ... 個人認証装置 / 個人認証部
- 301 ... 原本画像記録装置
- 302 ... 認証時の顔画像データ処理部
- 303 ... 撮像動画像記録装置
- 304 ... 静止画像選別装置
- 305 ... 画像照合装置
- 306 ... 照合判定結果保存装置
- 307 ... 照合判定結果添付・送装置

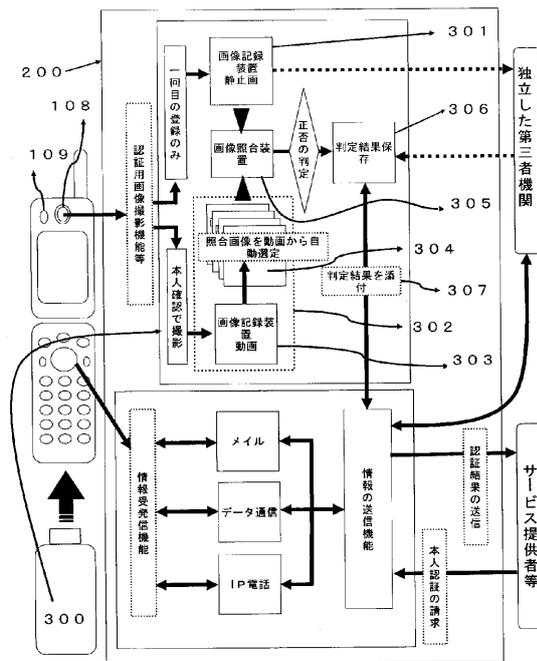
10

20

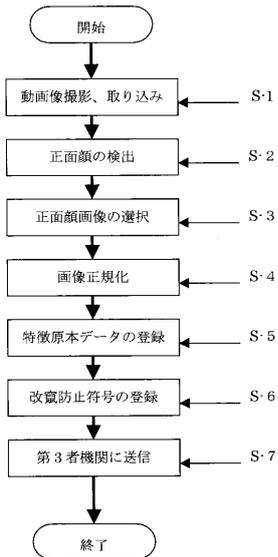
【図1】



【図2】



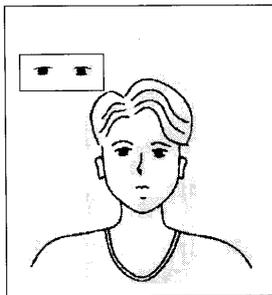
【図3】



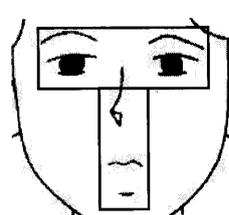
【図4】



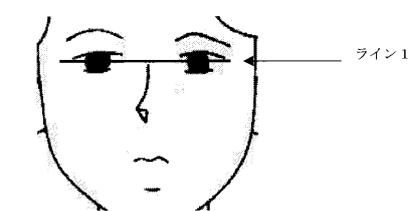
【図5】



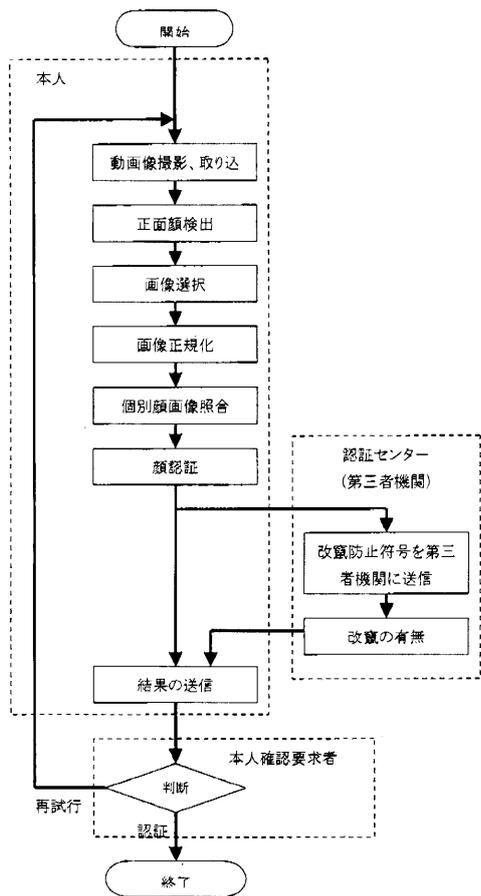
【図6】



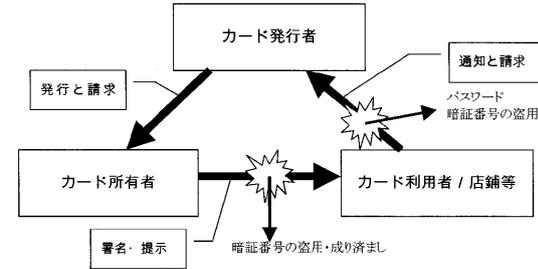
【図7】



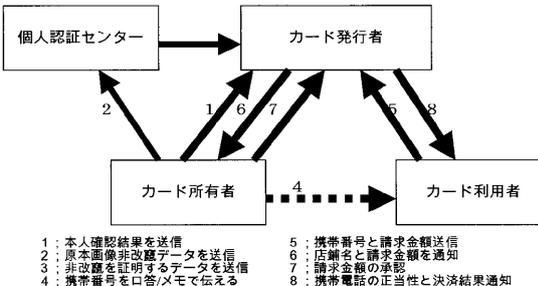
【図8】



【図9】

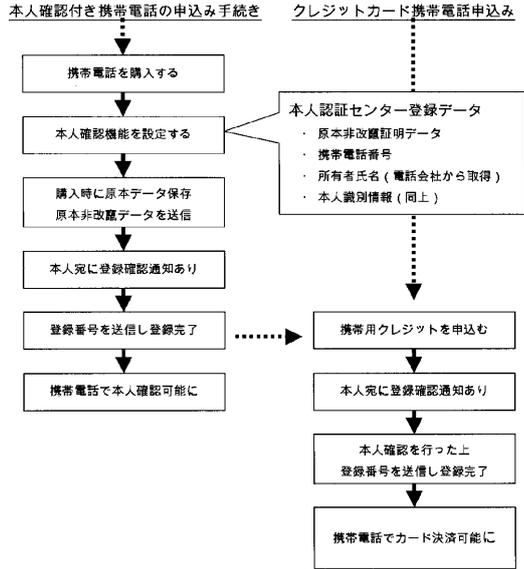


【図10】

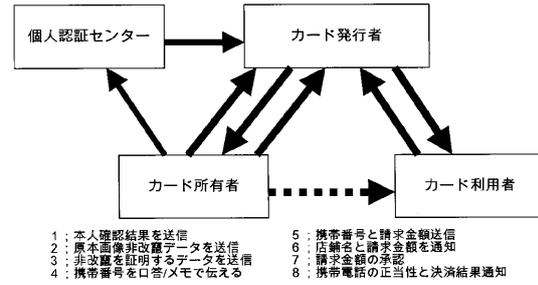


- 1: 本人確認結果を送信
- 2: 原本画像非改竄データを送信
- 3: 非改竄を証明するデータを送信
- 4: 携帯番号を口答/メッセで伝える
- 5: 携帯番号と請求金額送信
- 6: 店舗名と請求金額を通知
- 7: 請求金額の承認
- 8: 携帯電話の正当性と決済結果通知

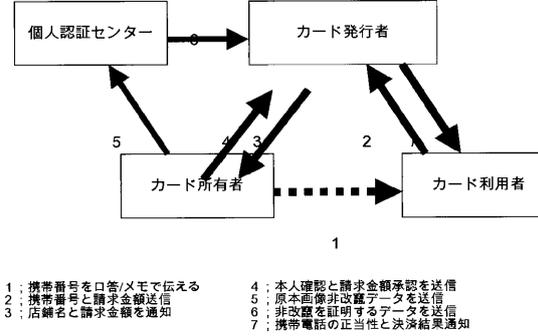
【 図 1 1 】



【 図 1 2 】



【 図 1 3 】



フロントページの続き

(51)Int.Cl.⁷ F I テーマコード(参考)
A 6 1 B 5/10 3 2 2

(71)出願人 596085612

株式会社ゲン・テック

東京都渋谷区広尾5 - 1 9 - 9 広尾ONビル

(74)代理人 100110559

弁理士 友野 英三

(72)発明者 小山 雄二

大阪府大阪市中央区淡路町3丁目2番8号 トーア紡第2ビル501号 株式会社アール・アンド
・デー・アソシエイツ内

Fターム(参考) 4C038 VA07 VB03 VB12

5B043 AA01 AA02 AA09 BA04 CA03 CA10 DA05 EA02 EA11 EA12

EA13 FA02 FA03 FA04 FA07 FA08 GA04 GA05 GA17 GA18

HA20

5K067 AA30 BB04 DD17 DD51 DD52 EE02 EE10 EE16 HH22 HH23

HH36