

(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2007-200367

(P2007-200367A)

(43) 公開日 平成19年8月9日(2007.8.9)

(51) Int. Cl.

G06Q 40/00 (2006.01)
H04L 9/32 (2006.01)

F I

G06F 17/60 222
H04L 9/00 673D

テーマコード (参考)

5J104

審査請求 有 請求項の数 5 O L (全 25 頁)

(21) 出願番号 特願2007-127545 (P2007-127545)
(22) 出願日 平成19年5月14日 (2007.5.14)
(62) 分割の表示 特願2000-142617 (P2000-142617)
の分割
原出願日 平成12年5月16日 (2000.5.16)

(71) 出願人 000004237
日本電気株式会社
東京都港区芝五丁目7番1号
(74) 代理人 100109313
弁理士 机 昌彦
(74) 代理人 100124154
弁理士 下坂 直樹
(74) 代理人 100111637
弁理士 谷澤 靖久
(72) 発明者 内田 薫
東京都港区芝五丁目7番1号 日本電気株
式会社内
Fターム(参考) 5J104 AA07 KA01 KA16 PA07 PA10

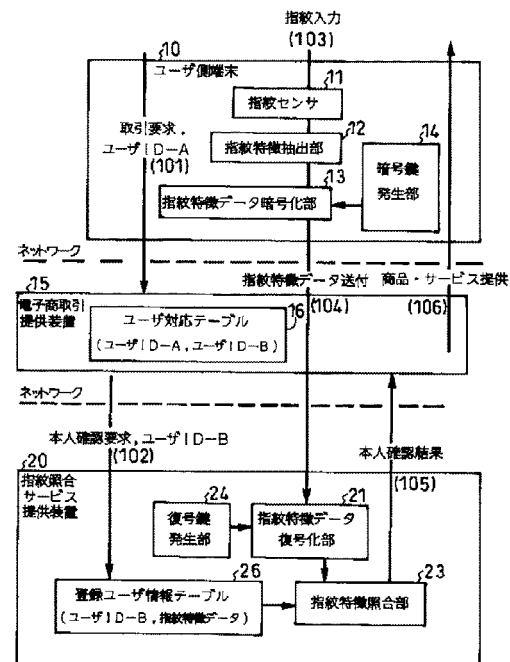
(54) 【発明の名称】 バイオメトリクス本人確認サービス提供システム

(57) 【要約】

【課題】 ユーザのバイオメトリクスデータのセキュリティを損なうことなく、バイオメトリクスを用いた本人確認技術を利用した電子商取引に複数の電子商取引提供業者が参加するためのバイオメトリクス本人確認サービスを提供する。

【解決手段】 電子商取引提供装置15は専用のユーザ識別子を使用して指紋照合サービス提供装置20にバイオメトリクスを利用した本人確認を要求する。指紋照合サービス提供装置20は、ユーザ側端末10と合意したメッセージの暗号鍵を用い、ユーザがユーザ側端末10で入力した指紋特徴データを受信し、それを用いて本人確認を行う。電子商取引提供装置15は、知らされた本人確認結果に基づいて電子商取引の可否を判断する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

ユーザ端末からユーザのバイオメトリクスデータを受信する受信部と
複数の電子商取引提供装置のうちの一つの電子商取引提供装置から前記ユーザのユーザ識別情報を受信する受信部と
照合用の登録バイオメトリクスデータを記憶する記憶部と、
前記バイオメトリクスデータと前記ユーザ識別情報で特定される前記登録バイオメトリクスデータを照合し前記ユーザの本人確認を行う照合部と、
前記本人確認の結果を該一つの電子商取引提供装置に送信する送信部、とから構成されることを特徴とするバイオメトリクス照合サービス提供装置。

10

【請求項 2】

請求項 1 記載のバイオメトリクス照合サービス提供装置のためのユーザ端末であって、ユーザがバイオメトリクスデータを入力した後に該入力になされたことを前記一つの電子商取引提供装置に通信することを特徴とするユーザ端末。

【請求項 3】

請求項 1 記載のバイオメトリクス照合サービス提供装置のためのユーザ端末であって、前記電子商取引提供装置を経由しないネットワークを介してユーザが入力したバイオメトリクスデータを前記バイオメトリクス照合サービス提供装置に送信することを特徴とするユーザ端末。

【請求項 4】

バイオメトリクス照合サービス提供装置のためのユーザ端末用通信方法であって、受信部が、ユーザ端末からユーザのバイオメトリクスデータを受信する手順と
受信部が、複数の電子商取引提供装置のうちの一つの電子商取引提供装置から前記ユーザのユーザ識別情報を受信する手順と
記憶部が、照合用の登録バイオメトリクスデータを記憶する手順と、
照合部が、前記バイオメトリクスデータと前記ユーザ識別情報で特定される前記登録バイオメトリクスデータを照合し前記ユーザの本人確認を行う手順と、
送信部が前記本人確認の結果を該一つの電子商取引提供装置に送信する手順とを有し、前記ユーザ端末にてユーザが入力したバイオメトリクスデータを前記電子商取引提供装置を経由せずに前記バイオメトリクス照合サービス提供装置に送信することを特徴とするユーザ端末用通信方法。

20

30

【請求項 5】

請求項 4 記載のバイオメトリクス照合サービス提供装置のためのユーザ端末用通信方法であって、
前記ユーザ端末にてユーザがバイオメトリクスデータを入力した後に入力になされたことを前記一つの電子商取引提供装置に通信することを特徴とするユーザ端末用通信方法。

【発明の詳細な説明】**【技術分野】****【0001】**

本発明はバイオメトリクス本人確認サービス提供システムに関し、特にネットワークを介した情報提供や電子商取引（EC = Electronic Commerce）に際してユーザの本人確認を行うサービスを提供するバイオメトリクス本人確認サービス提供システムに関する。

40

【背景技術】**【0002】**

ネットワークを通じての情報提供や電子商取引において、データの盗聴や改竄、「なりすまし」といった不正や犯罪などに対抗するセキュリティの確保のためには、取引にアクセスする人間が正当な権限を持つユーザであるか、また価値の交換の相手が自分の望むユーザであるかを確認するための本人確認の実現が必須の条件となる。

【0003】

50

具体的な例として、ネットワークを介した電子商取引において、提供する商品やサービスを持つ「電子商取引提供者」がネットワークを通じて顧客である「ユーザ」と取り引きを行う場合を考える。通常、取り引きを希望するユーザは予めその電子商取引提供者に決済方法などを含めてユーザ登録し、電子商取引提供者は確実に決済可能であることを前提としてユーザの取引要求に応じる。電子商取引において商取引を要求しているユーザが登録したユーザ本人であることを確認するのが本人確認である。現在、本人確認には磁気カードやパスワードが利用されているが、例えば磁気カードをなくしたりパスワードを忘れたりしてしまうと本人でも使えないという不便さがあることはもちろん、いずれの場合も盗難、偽造、盗み見、推量等により容易に他人がなりすませるといった問題点があった。

10

【0004】

そこで、これらの問題点を解決するためにバイオメトリクスが用いられる。バイオメトリクスとは、たとえば指紋のような個人に特有な生体特徴を利用するものである。人間の指先の皮膚紋様である指紋は、「万人不同」かつ「終生不変」という特徴を持つとされ、表皮が損傷を受けてもその奥の不変な真皮から同じ指紋が復元されるため、精密な個人の同定を可能にするバイオメトリクスとして広く知られている。

【0005】

バイオメトリクスによって個人を確認するシステムは、基本的に、1. ユーザが提示したバイオメトリクスデータをシステム側で取得する「バイオメトリクス入力装置」と、2. 入力されたバイオメトリクスデータを処理し照合に用いる特徴を求める「バイオメトリクス特徴抽出部」と、3. あらかじめ求めて記憶しておく正規ユーザについての登録バイオメトリクス特徴データ（「テンプレート」）と、4. 登録バイオメトリクスデータと入力バイオメトリクスデータと（の特徴同士）を比較し同一人物であるか否かを決定する「照合判定部」と、から構成される。照合の結果、特徴が十分類似し、バイオメトリクスデータの提示者が登録ユーザであると判定されれば、確認成功ということでバイオメトリクスデータの提示者は取引に参加できる。以下、バイオメトリクスの例として指紋を挙げて説明する。

20

【0006】

【特許文献1】特国際公開第98/50875号（特表2002-501700号公報に対応）

30

【特許文献2】特開平11-98252号公報

【特許文献3】特開平5-347617号公報

【特許文献4】特開平10-117173号公報

【特許文献5】特開平11-338947号公報

【特許文献6】特開2000-92046号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

上記のような、指紋を例とするバイオメトリクスによる本人確認を電子商取引において利用することを考える。まず、例えばインターネットバンキングサービスを提供する銀行Aと取り引きする場合、

40

1. 銀行Aが登録ユーザに指紋入力装置を配布し（あるいは銀行Aが認めた指紋入力装置をユーザが購入して設置し）、

2. ユーザはそれを用いて銀行Aに指紋データを登録し、

3. インターネットバンキングサービスの利用時には指紋データを入力して銀行Aの登録指紋データと照合する、

4. 一致すれば銀行Aのサービスを受けるという手順を踏むことになる。

【0008】

別のインターネット対応書店Bと取り引きする場合も同様に、書店Bが配布する（あるいは書店Bが認めた）指紋入力装置を通して書店Bに指紋データを登録する必要がある。

50

さらに、このような登録は、電子商取引の決済を実際に行う、例えばクレジットカード会社Cに対しても必要となりうる。

【0009】

このように、銀行、書店、クレジットカード会社等の電子商取引提供者ごとに指紋データを登録しなければならないのはユーザにとってかなり煩雑である。

【0010】

さらに重大な問題としては、悪質あるいはセキュリティレベルの低い電子商取引提供者に指紋データを登録した場合、極めて重要性の高い個人情報である指紋データが悪用され、あるいは技術的な要因で漏洩や盗用につながる可能性がある。

【0011】

本発明の目的は、大小さまざまな、また技術レベルの異なる幅広い電子商取引提供者が、バイオメトリクスを用いた本人確認技術を利用した電子商取引に参加するためのバイオメトリクス本人確認サービス提供システムを提供することにある。

【0012】

なお、先行技術文献としては、特開平11 96363号公報、特表平11 511882号公報等がある。

【0013】

特開平11 96363号公報に開示された「指紋認証による決済方法」は、「決済を行う業者が指紋を用いて利用者を認証する」ものである。このように決済を行う業者が指紋を扱う際の問題点としては、(1)複数の決済業者と取り引きしようとする、そのそれぞれに対して指紋などを登録する必要がある煩雑である、(2)指紋データ管理などの技術的制度的なセキュリティレベルが低い業者がいた場合に、そこから指紋データの漏洩などの問題が生じる恐れがある、ことは、すでに述べた通りである。

【0014】

本発明は、まさしく特開平11 96363号公報に開示された発明の課題を解決するためのものであり、決済業者とは独立した、指紋認証の第三者機関を置くことを特徴としたものであり、全く異なるものである。

【0015】

また、特表平11 511882号公報に開示された「電子取引および電子送信の承認のためのトークンレス識別システム」は、上記と同様の枠組みで、決済に参加する機関が直接ユーザのバイオメトリクスサンプルの同一性確認を行うことを基本としているものである。

【0016】

本発明は、上述のような(決済機関が本人確認を行うという)枠組みにある問題点を指摘し、それを解決するモデルを提供するものである。

【課題を解決するための手段】

【0017】

本発明のバイオメトリクス照合サービス提供装置は、ユーザ端末からユーザのバイオメトリクスデータを受信する受信部と、複数の電子商取引提供装置のうちの一つの電子商取引提供装置から前記ユーザのユーザ識別情報を受信する受信部と、照合用の登録バイオメトリクスデータを記憶する記憶部と、前記バイオメトリクスデータと前記ユーザ識別情報で特定される前記登録バイオメトリクスデータを照合し前記ユーザの本人確認を行う照合部と、前記本人確認の結果を該一つの電子商取引提供装置に送信する送信部、とから構成されることを特徴とする。

本発明のユーザ端末は、本発明のバイオメトリクス照合サービス提供装置のためのユーザ端末であって、ユーザがバイオメトリクスデータを入力した後に該入力になされたことを前記一つの電子商取引提供装置に通信することを特徴とする。

本発明のユーザ端末用通信方法は、バイオメトリクス照合サービス提供装置のためのユーザ端末用通信方法であって、受信部が、ユーザ端末からユーザのバイオメトリクスデータを受信する手順と、受信部が、複数の電子商取引提供装置のうちの一つの電子商取引提

10

20

30

40

50

供装置から前記ユーザのユーザ識別情報を受信する手順と、記憶部が、照合用の登録バイオメトリクスデータを記憶する手順と、照合部が、前記バイオメトリクスデータと前記ユーザ識別情報で特定される前記登録バイオメトリクスデータを照合し前記ユーザの本人確認を行う手順と、送信部が前記本人確認の結果を該一つの電子商取引提供装置に送信する手順とを有し、前記ユーザ端末にてユーザが入力したバイオメトリクスデータを前記電子商取引提供装置を経由せずに前記バイオメトリクス照合サービス提供装置に送信することを特徴とする。

【0018】

本発明のバイオメトリクス本人確認サービス提供システムは、ユーザからの取引要求を電子商取引提供装置に発行するとともに、該ユーザが入力したバイオメトリクスデータをバイオメトリクス照合サービス提供装置に送付するユーザ側端末と、前記電子商取引提供装置からユーザ識別情報を伴う本人確認要求を受けるとともに、前記ユーザ側端末から受け取ったバイオメトリクスデータが前記電子商取引提供装置から受け取ったユーザ識別情報に対応する登録バイオメトリクスデータと類似しているか否かを評価することにより本人確認を行う前記バイオメトリクス照合サービス提供装置と、前記ユーザ側端末からの取引要求を受けて前記バイオメトリクス照合サービス提供装置に本人確認要求を発行するとともに、前記バイオメトリクス照合サービス提供装置による本人確認結果に基づいて該ユーザとの電子商取引の可否を決定する前記電子商取引提供装置とを有することを特徴とする。

10

【0019】

また、本発明のバイオメトリクス本人確認サービス提供システムは、前記電子商取引提供装置が前記バイオメトリクス照合サービス提供装置に渡すユーザ識別情報が、前記電子商取引提供装置がユーザとの取引に使用するユーザに関する識別情報とは別のものであることを特徴とする。

20

【0020】

さらに、本発明のバイオメトリクス本人確認サービス提供システムは、前記電子商取引提供装置がユーザとの取引に使用するユーザに関する識別情報と、前記電子商取引提供装置が前記バイオメトリクス照合サービス提供装置に渡すユーザ識別情報との変換を前記電子商取引提供装置が行うことを特徴とする。

30

【0021】

さらにまた、本発明のバイオメトリクス本人確認サービス提供システムは、前記バイオメトリクス照合サービス提供装置は前記ユーザ側端末との間でメッセージ内容秘匿の方法を合意し、前記ユーザ側端末は合意した方法でバイオメトリクスデータの内容を秘匿して前記バイオメトリクス照合サービス提供装置に送付し、前記バイオメトリクス照合サービス提供装置は受け取ったバイオメトリクスデータを合意した方法に従って復元した後に類似度を評価することを特徴とする。

【0022】

また、本発明のバイオメトリクス本人確認サービス提供システムは、前記ユーザ側端末が暗号鍵発生手段およびバイオメトリクスデータ暗号化手段を持ち、前記バイオメトリクス照合サービス提供装置が前記暗号鍵発生手段および前記バイオメトリクスデータ暗号化手段に対応する復号鍵発生手段およびバイオメトリクスデータ復号化手段を持つことで内容秘匿を実現することを特徴とする。

40

【0023】

さらに、本発明のバイオメトリクス本人確認サービス提供システムは、前記ユーザ側端末がバイオメトリクスデータ暗号化手段を持ち、前記バイオメトリクス照合サービス提供装置が暗号鍵対発生手段およびバイオメトリクスデータ復号化手段を持ち、前記暗号鍵対発生手段で発生した暗号鍵を元に前記ユーザ側端末が暗号化を行い、前記暗号鍵対発生手段で発生した復号鍵を元に前記バイオメトリクス照合サービス提供装置が復号化を行うことで内容秘匿を行うことを特徴とする。

【0024】

50

さらにまた、本発明のバイオメトリクス本人確認サービス提供システムは、前記ユーザ側端末が暗号鍵対発生手段およびバイオメトリクスデータ暗号化手段を持ち、前記バイオメトリクス照合サービス提供装置がバイオメトリクスデータ復号化手段を持ち、前記暗号鍵対発生手段で発生した暗号鍵を元に前記ユーザ側端末が暗号化を行い、前記暗号鍵対発生手段で発生した復号鍵を元に前記バイオメトリクス照合サービス提供装置が復号化を行うことで内容秘匿を行うことを特徴とする。

【0025】

また、本発明のバイオメトリクス本人確認サービス提供システムは、前記電子商取引提供装置が、バイオメトリクスデータを内容秘匿された形で扱うことを特徴とする。

【0026】

さらにまた、本発明のバイオメトリクス本人確認サービス提供システムは、前記ユーザ側端末は共用サービス端末とそれに接続するユーザ携帯ユニットとから構成され、前記ユーザ携帯ユニットはバイオメトリクスデータ入力手段およびデータ内容秘匿手段を備え、前記共用サービス端末はバイオメトリクスデータを内容秘匿された形で扱うことを特徴とする。

【0027】

また、本発明のバイオメトリクス本人確認サービス提供システムは、ユーザからの取引要求を電子商取引提供装置に発行するとともに、該ユーザが入力したバイオメトリクスデータを前記バイオメトリクス照合サービス提供装置に送付するユーザ側端末と、前記電子商取引提供装置からユーザ識別要求を受けるとともに、前記ユーザ側端末から受け取ったバイオメトリクスデータがあらかじめ登録してある登録ユーザのバイオメトリクスデータ群の中のどのバイオメトリクスデータと一致しているかを求める前記バイオメトリクス照合サービス提供装置と、前記ユーザ側端末からの取引要求を受けて前記バイオメトリクス照合サービス提供装置にユーザ識別要求を発行するとともに、前記バイオメトリクス照合サービス提供装置からのユーザ識別結果に基づいて該ユーザとの電子商取引の可否を決定する前記電子商取引提供装置とを有することを特徴とする。

【0028】

さらに、本発明のバイオメトリクス本人確認サービス提供システムは、前記バイオメトリクス照合サービス提供装置は前記ユーザ側端末との間でメッセージ内容秘匿の方法を合意し、前記ユーザ側端末は合意した方法でバイオメトリクスデータの内容を秘匿して前記バイオメトリクス照合サービス提供装置に送付し、前記バイオメトリクス照合サービス提供装置は受け取ったデータを合意した方法に従って復元した後に登録ユーザのバイオメトリクスデータ群の中のどのバイオメトリクスデータと一致しているかを求めることを特徴とする。

【0029】

さらにまた、本発明のバイオメトリクス本人確認サービス提供システムは、前記電子商取引提供装置が、バイオメトリクスデータを内容秘匿された形で扱うことを特徴とする。

【0030】

また、本発明のバイオメトリクス本人確認サービス提供システムは、バイオメトリクスデータを読み取るバイオメトリクスセンサ、このバイオメトリクスセンサにより読み取られたバイオメトリクスデータからバイオメトリクス特徴データを抽出するバイオメトリクス特徴抽出部、このバイオメトリクス特徴抽出部により抽出されたバイオメトリクス特徴データを暗号化するバイオメトリクス特徴データ暗号化部、およびこのバイオメトリクス特徴データ暗号化部で使用される暗号鍵を生成する暗号鍵発生部を含むユーザ側端末と、前記ユーザ側端末からの第1のユーザ識別情報を第2のユーザ識別情報に変換するためのユーザ対応テーブルを含む電子商取引提供装置と、前記第2のユーザ識別情報とバイオメトリクス特徴データとを対にして登録する登録ユーザ情報テーブル、前記暗号鍵発生部で生成される暗号鍵と対応する復号鍵を生成する復号鍵発生部、この復号鍵発生部で生成された復号鍵を用いて前記ユーザ側端末から送信されてきた暗号化バイオメトリクス特徴データを復号化するバイオメトリクス特徴データ復号化部、およびこのバイオメトリクス特

10

20

30

40

50

徴データ復号化部で復号化されたバイオメトリクス特徴データと前記登録ユーザ情報テーブルから検索されたバイオメトリクス特徴データとを照合して本人確認結果を出力するバイオメトリクス特徴照合部を含むバイオメトリクス照合サービス提供装置とを有することを特徴とする。

【0031】

さらに、本発明のバイオメトリクス本人確認サービス提供システムは、バイオメトリクスデータを読み取るバイオメトリクスセンサ、このバイオメトリクスセンサにより読み取られたバイオメトリクスデータからバイオメトリクス特徴データを抽出するバイオメトリクス特徴抽出部、およびこのバイオメトリクス特徴抽出部により抽出されたバイオメトリクス特徴データを暗号化するバイオメトリクス特徴データ暗号化部を含むユーザ側端末と、前記ユーザ側端末からの取引要求に基づいて本人確認要求を発行する電子商取引提供装置と、前記ユーザ識別情報とバイオメトリクス特徴データとを対にして登録する登録ユーザ情報テーブル、暗号鍵と復号鍵との対を生成し前記ユーザ側端末に暗号鍵を送付してバイオメトリクスの入力を要求する暗号鍵対発生部、この暗号鍵対発生部で生成された復号鍵を用いて前記ユーザ側端末から送信されてきた暗号化バイオメトリクス特徴データを復号化するバイオメトリクス特徴データ復号化部、およびこのバイオメトリクス特徴データ復号化部で復号化されたバイオメトリクス特徴データと前記登録ユーザ情報テーブルから検索されたバイオメトリクス特徴データとを照合して本人確認結果を出力するバイオメトリクス特徴照合部を含むバイオメトリクス照合サービス提供装置とを有することを特徴とする。

10

20

【0032】

さらにまた、本発明のバイオメトリクス本人確認サービス提供システムは、バイオメトリクスデータを読み取るバイオメトリクスセンサ、このバイオメトリクスセンサにより読み取られたバイオメトリクスデータからバイオメトリクス特徴データを抽出するバイオメトリクス特徴抽出部、およびこのバイオメトリクス特徴抽出部により抽出されたバイオメトリクス特徴データを暗号化するバイオメトリクス特徴データ暗号化部を含むユーザ携帯ユニットと、前記ユーザ携帯ユニットを着脱可能に装着する共用サービス端末と、前記ユーザ携帯ユニットからの取引要求に基づいて本人確認要求を発行する電子商取引提供装置と、前記ユーザ識別情報と前記バイオメトリクス特徴データとを対にして登録する登録ユーザ情報テーブル、暗号鍵と復号鍵との対を生成し前記ユーザ携帯ユニットに暗号鍵を送付してバイオメトリクスの入力を要求する暗号鍵対発生部、この暗号鍵対発生部で生成された復号鍵を用いて前記ユーザ携帯ユニットから送信されてきた暗号化バイオメトリクス特徴データを復号化するバイオメトリクス特徴データ復号化部、およびこのバイオメトリクス特徴データ復号化部で復号化されたバイオメトリクス特徴データと前記登録ユーザ情報テーブルから検索されたバイオメトリクス特徴データとを照合して本人確認結果を出力するバイオメトリクス特徴照合部を含むバイオメトリクス照合サービス提供装置とを有することを特徴とする。

30

【0033】

また、本発明のバイオメトリクス本人確認サービス提供システムは、バイオメトリクスデータを読み取るバイオメトリクスセンサ、このバイオメトリクスセンサにより読み取られたバイオメトリクスデータからバイオメトリクス特徴データを抽出するバイオメトリクス特徴抽出部、およびこのバイオメトリクス特徴抽出部により抽出されたバイオメトリクス特徴データを暗号化するバイオメトリクス特徴データ暗号化部を含むユーザ側端末と、前記ユーザ側端末からの取引要求に基づいてユーザ識別要求を発行する電子商取引提供装置と、前記ユーザ識別情報とバイオメトリクス特徴データとを対にして登録する登録ユーザ情報テーブル、暗号鍵と復号鍵との対を生成し前記ユーザ側端末に暗号鍵を送付してバイオメトリクスの入力を要求する暗号鍵対発生部、この暗号鍵対発生部で生成された復号鍵を用いて前記ユーザ側端末から送信されてきた暗号化バイオメトリクス特徴データを復号化するバイオメトリクス特徴データ復号化部、およびこのバイオメトリクス特徴データ復号化部で復号化されたバイオメトリクス特徴データと前記登録ユーザ情報テーブルのバ

40

50

イオメトリクス特徴データとを照合してユーザ識別結果を出力するバイオメトリクス特徴照合部を含むバイオメトリクス照合サービス提供装置とを有することを特徴とする。

【0034】

さらに、本発明のバイオメトリクス本人確認サービス提供システムは、前記バイオメトリクスデータが、指紋、掌紋、顔、虹彩、網膜血管パターン、掌形、筆跡、声紋のうちの1つでなることを特徴とする。

【0035】

さらにまた、本発明のバイオメトリクス本人確認サービス提供システムは、前記バイオメトリクスデータが、指紋、掌紋、顔、虹彩、網膜血管パターン、掌形、筆跡、声紋のうちの任意の組み合わせでなることを特徴とする。

【0036】

一方、本発明の指紋本人確認サービス提供システムは、指紋画像データを読み取る指紋センサ、この指紋センサにより読み取られた指紋画像データから指紋特徴データを抽出する指紋特徴抽出部、この指紋特徴抽出部により抽出された指紋特徴データを暗号化する指紋特徴データ暗号化部、およびこの指紋特徴データ暗号化部で使用される暗号鍵を生成する暗号鍵発生部を含むユーザ側端末と、前記ユーザ側端末からの第1のユーザ識別情報を第2のユーザ識別情報に変換するためのユーザ対応テーブルを含む電子商取引提供装置と、前記第2のユーザ識別情報と指紋特徴データとを対にして登録する登録ユーザ情報テーブル、前記暗号鍵発生部で生成される暗号鍵と対応する復号鍵を生成する復号鍵発生部、この復号鍵発生部で生成された復号鍵を用いて前記ユーザ側端末から送信されてきた暗号化指紋特徴データを復号化する指紋特徴データ復号化部、およびこの指紋特徴データ復号化部で復号化された指紋特徴データと前記登録ユーザ情報テーブルから検索された指紋特徴データとを照合して本人確認結果を出力する指紋特徴照合部を含む指紋照合サービス提供装置とを有することを特徴とする。

【0037】

また、本発明の指紋本人確認サービス提供システムは、指紋画像データを読み取る指紋センサ、この指紋センサにより読み取られた指紋画像データから指紋特徴データを抽出する指紋特徴抽出部、およびこの指紋特徴抽出部により抽出された指紋特徴データを暗号化する指紋特徴データ暗号化部を含むユーザ側端末と、前記ユーザ側端末からの取引要求に基づいて本人確認要求を発行する電子商取引提供装置と、前記ユーザ識別情報と指紋特徴データとを対にして登録する登録ユーザ情報テーブル、暗号鍵と復号鍵との対を生成し前記ユーザ側端末に暗号鍵を送付して指紋の入力を要求する暗号鍵対発生部、この暗号鍵対発生部で生成された復号鍵を用いて前記ユーザ側端末から送信されてきた暗号化指紋特徴データを復号化する指紋特徴データ復号化部、およびこの指紋特徴データ復号化部で復号化された指紋特徴データと前記登録ユーザ情報テーブルから検索された指紋特徴データとを照合して本人確認結果を出力する指紋特徴照合部を含む指紋照合サービス提供装置とを有することを特徴とする。

【0038】

さらに、本発明の指紋本人確認サービス提供システムは、指紋画像データを読み取る指紋センサ、この指紋センサにより読み取られた指紋画像データから指紋特徴データを抽出する指紋特徴抽出部、およびこの指紋特徴抽出部により抽出された指紋特徴データを暗号化する指紋特徴データ暗号化部を含むユーザ携帯ユニットと、前記ユーザ携帯ユニットを着脱可能に装着する共用サービス端末と、前記ユーザ携帯ユニットからの取引要求に基づいて本人確認要求を発行する電子商取引提供装置と、前記ユーザ識別情報と前記指紋特徴データとを対にして登録する登録ユーザ情報テーブル、暗号鍵と復号鍵との対を生成し前記ユーザ携帯ユニットに暗号鍵を送付して指紋の入力を要求する暗号鍵対発生部、この暗号鍵対発生部で生成された復号鍵を用いて前記ユーザ携帯ユニットから送信されてきた暗号化指紋特徴データを復号化する指紋特徴データ復号化部、およびこの指紋特徴データ復号化部で復号化された指紋特徴データと前記登録ユーザ情報テーブルから検索された指紋特徴データとを照合して本人確認結果を出力する指紋特徴照合部を含む指紋照合サービス

10

20

30

40

50

提供装置とを有することを特徴とする。

【0039】

さらにまた、本発明の指紋本人確認サービス提供システムは、指紋画像データを読み取る指紋センサ、この指紋センサにより読み取られた指紋画像データから指紋特徴データを抽出する指紋特徴抽出部、およびこの指紋特徴抽出部により抽出された指紋特徴データを暗号化する指紋特徴データ暗号化部を含むユーザ側端末と、前記ユーザ側端末からの取引要求に基づいてユーザ識別要求を発行する電子商取引提供装置と、前記ユーザ識別情報と指紋特徴データとを対にして登録する登録ユーザ情報テーブル、暗号鍵と復号鍵との対を生成し前記ユーザ側端末に暗号鍵を送付して指紋の入力を要求する暗号鍵対発生部、この暗号鍵対発生部で生成された復号鍵を用いて前記ユーザ側端末から送信されてきた暗号化指紋特徴データを復号化する指紋特徴データ復号化部、およびこの指紋特徴データ復号化部で復号化された指紋特徴データと前記登録ユーザ情報テーブルの指紋特徴データとを照合してユーザ識別結果を出力する指紋特徴照合部を含む指紋照合サービス提供装置とを有することを特徴とする。

10

【0040】

他方、本発明の記録媒体は、コンピュータを、バイオメトリクスデータを読み取るバイオメトリクスセンサ手段、このバイオメトリクスセンサ手段により読み取られたバイオメトリクスデータからバイオメトリクス特徴データを抽出するバイオメトリクス特徴抽出手段、このバイオメトリクス特徴抽出手段により抽出されたバイオメトリクス特徴データを暗号化するバイオメトリクス特徴データ暗号化手段、およびこのバイオメトリクス特徴データ暗号化手段で使用する暗号鍵を生成する暗号鍵発生手段として機能させるためのプログラムを記録する。

20

【0041】

また、本発明の記録媒体は、コンピュータを、ユーザ識別情報とバイオメトリクス特徴データとを対にして登録する登録ユーザ情報テーブル手段、暗号鍵発生手段で生成される暗号鍵と対応する復号鍵を生成する復号鍵発生手段、この復号鍵発生手段で生成された復号鍵を用いて送信されてきた暗号化バイオメトリクス特徴データを復号化するバイオメトリクス特徴データ復号化手段、およびこのバイオメトリクス特徴データ復号化手段で復号化されたバイオメトリクス特徴データと前記登録ユーザ情報テーブル手段から検索されたバイオメトリクス特徴データとを照合して本人確認結果を出力するバイオメトリクス特徴照合手段として機能させるためのプログラムを記録する。

30

【0042】

さらに、本発明の記録媒体は、コンピュータを、バイオメトリクスデータを読み取るバイオメトリクスセンサ手段、このバイオメトリクスセンサ手段により読み取られたバイオメトリクスデータからバイオメトリクス特徴データを抽出するバイオメトリクス特徴抽出手段、およびこのバイオメトリクス特徴抽出手段により抽出されたバイオメトリクス特徴データを暗号化するバイオメトリクス特徴データ暗号化手段として機能させるためのプログラムを記録する。

【0043】

さらにまた、本発明の記録媒体は、コンピュータを、ユーザ識別情報とバイオメトリクス特徴データとを対にして登録する登録ユーザ情報テーブル手段、暗号鍵と復号鍵との対を生成し暗号鍵を送付してバイオメトリクスの入力を要求する暗号鍵対発生手段、この暗号鍵対発生手段で生成された復号鍵を用いて送信されてきた暗号化バイオメトリクス特徴データを復号化するバイオメトリクス特徴データ復号化手段、およびこのバイオメトリクス特徴データ復号化手段で復号化されたバイオメトリクス特徴データと前記登録ユーザ情報テーブル手段から検索されたバイオメトリクス特徴データとを照合して本人確認結果を出力するバイオメトリクス特徴照合手段として機能させるためのプログラムを記録する。

40

【0044】

また、本発明の記録媒体は、コンピュータを、ユーザ識別情報とバイオメトリクス特徴データとを対にして登録する登録ユーザ情報テーブル手段、暗号鍵と復号鍵との対を生成

50

しユーザ側端末に暗号鍵を送付してバイオメトリクスの入力を要求する暗号鍵対発生手段、この暗号鍵対発生手段で生成された復号鍵を用いて送信されてきた暗号化バイオメトリクス特徴データを復号化するバイオメトリクス特徴データ復号化手段、およびこのバイオメトリクス特徴データ復号化手段で復号化されたバイオメトリクス特徴データと前記登録ユーザ情報テーブル手段のバイオメトリクス特徴データとを照合してユーザ識別結果を出力するバイオメトリクス特徴照合手段として機能させるためのプログラムを記録する。

【発明の効果】

【0045】

本発明によれば、ネットワークを介した電子商取引において、商品・サービスなどの電子商取引提供者ごとに本人確認のためのバイオメトリクスデータを登録する必要がなく
10 なり、ユーザにとっての煩雑性が軽減される。さらには、大小さまざまな、また技術レベルの異なる幅広い電子商取引提供者に各ユーザが本人確認のためのバイオメトリクスデータを登録し、またそれぞれの電子商取引提供者がその本人確認処理を実行する場合、悪質なあるいはセキュリティ面での技術レベルが低い電子商取引提供者によって極めて重要性の高い個人情報であるバイオメトリクスデータが悪用され、あるいは技術的な要因で漏洩・盗用につながることで、バイオメトリクスデータのプライバシーが危険にさらされるというセキュリティ上の問題があったが、本発明はバイオメトリクス本人確認サービスをより信頼できる業者や公的機関などのバイオメトリクス照合サービス提供機関に営業・受託することで、これを解決することができる。

【0046】

また、バイオメトリクスデータは電子商取引提供者を通過するが電子商取引提供者には解読できない方法で暗号化されているため、電子商取引提供者がバイオメトリクスデータの中身を知り悪用することはできない。一方、バイオメトリクス照合サービス提供機関は、ユーザと電子商取引提供者と間の取引の内容を知ることはないので、複数の電子商取引提供者での購買状況などの個人情報が蓄積されたり、悪用されたりすることはない。

【0047】

さらに、第2の実施の形態の構成をとることにより、ネットワークを介したバイオメトリクスデータ通信におけるセキュリティをさらに高めることができる。

【0048】

さらにまた、第3の実施の形態の構成をとることにより、店舗店頭の共用サービス端末などを用いて電子商取引を提供する際も、共用サービス端末におけるバイオメトリクスデータの遺漏の可能性を回避し、システム・サービス全体のセキュリティをさらに高めることができる。

【0049】

また、第4の実施の形態のようにユーザが取引要求に際してIDの提示・入力を不要とすることにより、ユーザの利便性を増大することができる。

【発明を実施するための最良の形態】

【0050】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0051】

(1) 第1の実施の形態図1は、本発明の第1の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムの構成を示すブロック図である。これは、ユーザが電子商取引提供者との電子商取引を行う際に、本人確認を指紋で行う場合の構成の一例およびそこでのデータの流れを示すものである。図1を参照すると、第1の実施の形態に係る指紋本人確認サービス提供システムは、ユーザ側端末10と、電子商取引提供装置15と、指紋照合サービス提供装置20とがネットワークを介して接続されて構成されている。

【0052】

ユーザ側端末10は、ネットワークに接続される、例えばパーソナルコンピュータ(P

10

20

30

40

50

C)、テレビゲーム機、情報端末機、通信端末機などの、情報処理機能および通信機能を持つデジタル家電あるいは情報家電と呼ばれるものの一種である。ユーザ側端末10には、指紋センサ11、指紋特徴抽出部12、指紋特徴データ暗号化部13、および暗号鍵発生部14が装備されている。

【0053】

指紋センサ11は、ユーザの指が接触した際にその指紋画像を撮影する。撮影された指紋画像はデジタル形式の指紋画像データに変換され、指紋特徴抽出部12に送られる。

【0054】

指紋特徴抽出部12は、指紋画像データから指紋照合に用いるための指紋特徴データを抽出する。

【0055】

暗号鍵発生部14は、一般ユーザなどに知られない秘密情報としてデータの暗号化に用いる暗号鍵を発生する。これは、例えば256ビットのビット列などである。もちろん、秘密データを用いて固定的な値を発生してもよいが、より安全性を高めるにはある秘密のアルゴリズムに従い、毎回異なる暗号鍵を発生することが望ましい。また、多数の同様なユーザ側端末10をネットワークを介して接続して使用することになるので、そのユーザ側端末10固有の秘密の発生元を元にするることにより、ユーザ側端末10毎に異なる暗号鍵の列を発生することが望ましい。

【0056】

指紋特徴データ暗号化部13は、暗号鍵発生部14から暗号鍵を受け取り、これを鍵として指紋特徴抽出部12から受け取った指紋特徴データの暗号化処理を行う。この暗号化処理としては、DES(Data Encryption Standard)を例とするような共通秘密鍵方式の暗号化方法を用いることができるが、また一方、RSA(Rivest, Shamir, Adleman)を例とするような公開鍵方式(非対称暗号系)の暗号化方法を利用することも可能である。この場合、指紋照合サービス提供装置20内の復号用秘密鍵に対応する公開鍵を暗号化に用いることになる。暗号化された指紋特徴データ(以下、暗号化指紋特徴データという)は、ネットワーク経由で電子商取引提供装置15に送られる。

【0057】

なお、ユーザ側端末10の構成法としては、指紋センサ11、指紋特徴抽出部12、指紋特徴データ暗号化部13、および暗号鍵発生部14を不可分な方法で構成することが望ましい。不可分であるとは、ここの部分の解読や改造を図る不当な第三者が、指紋センサ11から指紋特徴データ暗号化部13への内部信号、あるいは暗号鍵発生部14から指紋特徴データ暗号化部13への内部信号を解読したり、それらの信号を外部からの信号で置き換えたり、あるいはそれぞれの構成要素の中身を解読したり改造したりできないように構成する、ということである。

【0058】

ユーザ側端末10とネットワーク接続により結ばれた電子商取引提供装置15のユーザ確認部(図示せず)では、その内部のユーザ対応テーブル16に、電子商取引提供装置15が登録ユーザの識別に用いるユーザ識別子(ユーザID-A)を、指紋照合サービス提供装置20が電子商取引提供装置15から委託を受けた本人確認を行う際に登録ユーザの識別に用いるユーザ識別子(ユーザID-B)と対にして記憶しておく。このようにユーザ識別子を分離しているのは、指紋照合サービス提供装置20に実際に電子商取引提供装置15が取り引きする登録ユーザの情報を知られないようにするためである。電子商取引提供装置15は、ユーザがそのユーザ識別子(ユーザID-A)を提示して商取引を要求すると、対応するユーザID-Bを指紋照合サービス提供装置20に送り、またユーザ側端末10から暗号化指紋特徴データを受け取ると、そのまま指紋照合サービス提供装置20に送る。

【0059】

指紋照合サービス提供装置20は、登録ユーザ情報テーブル26と、復号鍵発生部24

10

20

30

40

50

と、指紋特徴データ復号化部 2 1 と、指紋特徴照合部 2 3 とを含んで構成されており、電子商取引提供装置 1 5 を通じて暗号化指紋特徴データを受け取り、復号鍵発生部 2 4 の生成する復号鍵を用い、指紋特徴データ復号化部 2 1 において、暗号化指紋特徴データを指紋特徴データに復号する。

【 0 0 6 0 】

この復号処理は、ユーザ側端末 1 0 の暗号鍵発生部 1 4 および指紋特徴データ暗号化部 1 3 の処理内容に対応したものをを用いる。例えば、指紋特徴データ暗号化部 1 3 が共通秘密鍵方式の暗号化方法を用いていれば、暗号鍵発生部 1 4 が生成するものと同一の鍵を用いた復号処理を用いる。また、公開鍵方式（非対称暗号系）の暗号化方法であれば、暗号化に用いた公開鍵に対応する秘密鍵を用いて復号する。

10

【 0 0 6 1 】

登録ユーザ情報テーブル 2 6 は、本人確認用のユーザ識別子であるユーザ ID - B と、そのユーザの指紋照合に用いる指紋特徴データとを対にして保持している。

【 0 0 6 2 】

指紋特徴照合部 2 3 は、復号化された指紋特徴データと登録ユーザ情報テーブル 2 6 に登録されたそのユーザの指紋特徴データとの照合を行う。

【 0 0 6 3 】

以上の指紋センサ 1 1 , 指紋特徴抽出部 1 2 , 指紋特徴照合部 2 3 を含む指紋照合装置の実現例としては、特開昭 5 6 - 2 4 6 7 5 号公報や特開平 4 - 3 3 0 6 5 号公報に記載された「指紋照合装置」がある。

20

【 0 0 6 4 】

特開昭 5 6 - 2 4 6 7 5 号公報に記載された「指紋照合装置」では、指紋等の照合に際して、指紋紋様を特徴付ける各特徴点の位置 X , Y および方向 D とともに各特徴点により固有に決定される局所座標系を複数の扇形領域に分割した近傍における最近傍点と上記特徴点との隆線数、すなわちリレーションを検査することによって、安定で、かつ精度の高い照合を可能にしている。

【 0 0 6 5 】

また、特開平 4 - 3 3 0 6 5 号公報に記載された「指紋照合装置」では、登録されている 1 つの指もしくは複数の指の全てと入力指紋との照合を行うことによって、暗証番号の盗難や忘却に関与しない、操作性が優れかつ信頼性の高い同定を可能としている。

30

【 0 0 6 6 】

次に、このように構成された第 1 の実施の形態に係る指紋本人確認サービス提供システムの動作について説明する。

【 0 0 6 7 】

まず、指紋照合サービス提供機関は、あらかじめ自機関の指紋照合サービス提供装置 2 0 において指紋照合サービスの提供を受けることができるユーザ側端末 1 0 (あるいはそのうちの 1 1 , 1 2 , 1 3 , 1 4 の部分)を指定しておく。指紋照合サービス提供装置 2 0 による指紋本人確認サービスを利用する電子商取引提供者と取り引きしようとするユーザは、このような指定されたユーザ側端末 1 0 を、指紋照合サービス提供機関から配布を受けたり、あるいは認定された機種を購入するなどして、商取引を行う場所(例えば自宅など)に設置しておく。

40

【 0 0 6 8 】

電子商取引提供者と電子商取引を行おうとするユーザは、電子商取引用のユーザ識別子であるユーザ ID - A , ユーザの住所, 氏名などの個人情報, クレジットカード使用や銀行口座引き落としなどの決済方法を指定した決済情報などを含むユーザ情報を登録することを電子商取引提供装置 1 5 に要求するとともに、ユーザ側端末 1 0 の指紋センサ 1 1 に指を当てて指紋を入力する。

【 0 0 6 9 】

ユーザ側端末 1 0 は、指紋センサ 1 1 により指紋画像データを読み取り、読み取られた指紋画像データから指紋特徴抽出部 1 2 により照合用の指紋特徴データを抽出し、この指

50

紋特徴データを暗号鍵発生部 14 から生成される暗号鍵に基づいて指紋特徴データ暗号化部 13 により暗号化する。

【0070】

電子商取引提供装置 15 は、登録のためのユーザ情報と、指紋特徴データ暗号化部 13 から出力される暗号化指紋特徴データとを受け取ると、ユーザ情報中のユーザ ID - A に対応するユーザ ID - B を決定し、ユーザ ID - A とユーザ ID - B との対をユーザ対応テーブル 16 に登録するとともに、ユーザ ID - B と暗号化指紋特徴データとをそのまま指紋照合サービス提供装置 20 に送り、指紋特徴データの登録を要求する。なお、電子商取引提供装置 15 を通過する暗号化指紋特徴データは暗号化されているため、電子商取引提供装置 15 が指紋特徴データを盗用、流用、あるいは偽造することはできない。

10

【0071】

指紋照合サービス提供装置 20 は、ユーザ ID - B および暗号化指紋特徴データを伴う登録要求を受信すると、暗号化指紋特徴データを復号鍵発生部 24 により生成された復号鍵を元に指紋特徴データ復号化部 21 により指紋特徴データに復号した後、ユーザ ID - B と指紋特徴データとを対にして登録ユーザ情報テーブル 26 に登録する。前述のように、暗号鍵発生部 14 の暗号鍵に基づいて指紋特徴データ暗号化部 13 により暗号化された指紋特徴データは、復号鍵発生部 24 の生成する復号鍵を用いて指紋特徴データ復号化部 21 において正しく復号される。これが正しく復号されることをもって、ユーザ側端末 10 の指紋処理部分 (11, 12, 13, 14 の部分) が純正でかつ正しく駆動されていることが確認できる。

20

【0072】

実際にユーザが電子商取引提供業者と電子商取引を行う際、ユーザは、ユーザが取引を希望する商品・サービスの指定等の取引情報および自分のユーザ ID - A をユーザ側端末 10 に入力して取引を要求する。すると、ユーザ側端末 10 は、取引情報およびユーザ ID - A を伴う取引要求をネットワーク経由で電子商取引提供装置 15 に送信する (101)。

【0073】

また、ユーザは、手順に従ってユーザ側端末 10 の指紋センサ 11 に指を当てて指紋を入力する (130)。すると、ユーザ側端末 10 は、指紋センサ 11 により指紋画像データを読み取り、読み取られた指紋画像データから指紋特徴抽出部 12 により照合用の指紋特徴データが抽出され、この指紋特徴データが暗号鍵発生部 14 から生成される暗号鍵に基づいて指紋特徴データ暗号化部 13 により暗号化され、この暗号化指紋特徴データがネットワーク経由で電子商取引提供装置 15 に送信される (104)。

30

【0074】

電子商取引提供装置 15 は、ユーザ ID - A および取引情報とともに、指紋特徴データ暗号化部 13 から出力される暗号化指紋特徴データを受け取ると、ユーザ対応テーブル 16 を参照してユーザ ID - A に対応するユーザ ID - B を求め、ユーザ ID - B と暗号化指紋特徴データとをそのままネットワーク経由で指紋照合サービス提供装置 20 に送り、ユーザの本人確認を要求する (102)。

【0075】

指紋照合サービス提供装置 20 は、ユーザ ID - B を伴う本人確認要求および暗号化指紋特徴データを受けると、復号鍵発生部 24 により生成された復号鍵を元に指紋特徴データ復号化部 21 において暗号化指紋特徴データを指紋特徴データに復号する。また、登録ユーザ情報テーブル 26 の登録ユーザ情報 (ユーザ ID - B, 指紋特徴データ) からユーザ ID - B に対応する登録指紋特徴データを求め、これと復号された入力指紋特徴データとの照合を指紋特徴照合部 23 で行う。その結果としての、それら 2 つの指紋特徴データが十分一致しており同一指紋であると判定できる、あるいはそうでないという本人確認結果をネットワーク経由で電子商取引提供装置 15 に通知する (105)。

40

【0076】

電子商取引提供装置 15 は、指紋照合サービス提供装置 20 からの本人確認結果が一致

50

であれば真の登録ユーザであり、なりすましではないと判断して、商品・サービスをユーザID - Aのユーザに提供する(106)。

【0077】

ここで注目すべきことは、ユーザID - Bは、電子商取引提供装置15と指紋照合サービス提供装置20との間でユーザの識別子として用いることができれば任意に決定可能であり、必ずしもユーザのプライバシーを含む個別情報とリンクする必要がないことである。すなわち、電子商取引提供装置15が使用するユーザの決済情報などの個人情報とは分離され、指紋照合サービス提供装置20は個人情報に接する可能性がなくなり、プライバシーがより高度に保たれることになる。

【0078】

(2) 第2の実施の形態図2は、本発明の第2の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムの構成を示すブロック図である。第2の実施の形態に係る指紋本人確認サービス提供システムは、第1の実施の形態に係る指紋本人確認サービス提供システムと同様に、ユーザが電子商取引提供業者との電子商取引を行う際に、本人確認を指紋で行う場合の構成の一例およびそこでデータの流れを示すものである。ここでは、データ交換の安全性を増すために、別の実施方法をとっている。

【0079】

第2の実施の形態に係る指紋本人確認サービス提供システムと、第1の実施の形態に係る指紋本人確認サービス提供システムとの違いとしては、指紋照合サービス提供装置20Aが暗号鍵対発生部24Aを持ち、ここで1回の本人確認にのみ使用する暗号鍵と復号鍵との対を生成し、前者をユーザ側端末10Aに送ったものを指紋特徴データ暗号化部13で使用するものである。また、電子商取引提供装置15Aが、ユーザ対応テーブルを備えておらず、ユーザ側端末10Aで入力するユーザIDと指紋照合サービス提供装置20Aが使用するユーザIDとが同じものであることである。なお、その他の特に言及しない部分は、第1の実施の形態に係る指紋本人確認サービス提供システムと同様に構成されているので、対応する部分には同一符号を付してそれらの詳しい説明を割愛する。

【0080】

このように構成された第2の実施の形態に係る指紋本人確認サービス提供システムの動作を、第1の実施の形態に係る指紋本人確認サービス提供システムとの違いを中心に説明する。

【0081】

指紋照合サービス提供機関の指紋照合サービスを利用する電子商取引提供業者と取り引きしようとするユーザは、指紋照合サービス提供機関により指定されたユーザ側端末10Aを、指紋照合サービス提供機関から配布を受ける、あるいは認定された機種を購入するなどして電子商取引を行う場所(自分の手元など)に設置しておく。

【0082】

電子商取引提供業者と電子商取引を行おうとするユーザは、まず、指紋照合サービス提供機関の指紋照合サービス提供装置20Aに対してネットワーク経由で指紋の登録を要求する。

【0083】

指紋照合サービス提供装置20Aは、ユーザ側端末10Aからの指紋登録要求を受けると、このユーザの識別子であるユーザIDを決定するとともに、暗号鍵対発生部24Aで暗号鍵および復号鍵の対を生成し、暗号鍵を伴う指紋入力要求をネットワーク経由でユーザ側端末10Aの指紋特徴データ暗号化部13に送り、ユーザに指紋の入力を要求する。この通信は、電子商取引提供装置15Aを介する必要はない。

【0084】

ユーザ側端末10Aは、暗号鍵を伴う指紋入力要求を受けると、ユーザに指紋の入力を促す。ユーザが指紋入力要求に対してユーザ側端末10Aの指紋センサ11に指を当てて指紋を入力すると、指紋センサ11により指紋画像データが読み取られ、読み取られた指

10

20

30

40

50

紋画像データから指紋特徴抽出部 1 2 により照合用の指紋特徴データが抽出され、この指紋特徴データが暗号鍵対発生部 2 4 A から送られた暗号鍵に基づいて指紋特徴データ暗号化部 1 3 で暗号化される。ユーザ側端末 1 0 A は、暗号化指紋特徴データをネットワーク経由で指紋照合サービス提供装置 2 0 A に送る。

【 0 0 8 5 】

指紋照合サービス提供装置 2 0 A は、ユーザ側端末 1 0 A から受け取った暗号化指紋特徴データを指紋特徴データ復号化部 2 1 により指紋特徴データに復号した後、ユーザ ID と指紋特徴データとを対にして登録ユーザ情報テーブル 2 6 に登録する。前述のように、暗号鍵対発生部 2 4 A により生成された暗号鍵に従って指紋特徴データ暗号化部 1 3 で暗号化された指紋特徴データは、暗号鍵対発生部 2 4 A の生成する復号鍵を用いて指紋特徴データ復号化部 2 1 において正しく復号される。 10

【 0 0 8 6 】

実際にユーザが電子商取引提供業者と電子商取引を行う際、ユーザは、ユーザ側端末 1 0 A を使用してユーザ ID を含む取引要求をネットワーク経由で電子商取引提供装置 1 5 A に通知する (2 0 1) 。

【 0 0 8 7 】

電子商取引提供装置 1 5 A は、ユーザ ID を含む取引要求を受けると、ユーザ ID を含む本人確認要求をネットワーク経由で指紋照合サービス提供装置 2 0 A に送る (2 0 2) 。

【 0 0 8 8 】

指紋照合サービス提供装置 2 0 A は、ユーザ ID を含む本人確認要求を受けると、暗号鍵対発生部 2 4 A で暗号鍵と復号鍵との対を生成し、暗号鍵を伴う指紋入力要求をネットワーク経由でユーザ側端末 1 0 A に送る (2 0 3) 。

【 0 0 8 9 】

ユーザ側端末 1 0 A は、暗号鍵を伴う指紋入力要求を受けると、ユーザに指紋の入力を促す。ユーザが指紋センサ 1 1 に指を当てて指紋を入力すると (2 0 4) 、指紋センサ 1 1 で指紋画像データが読み取られ、読み取られた指紋画像データから指紋特徴抽出部 1 2 で照合用の指紋特徴データが抽出され、この指紋特徴データが暗号鍵対発生部 2 4 A で生成された暗号鍵に基づいて指紋特徴データ暗号化部 1 3 で暗号化される。ユーザ側端末 1 0 A は、指紋特徴データ暗号化部 1 3 から出力された暗号化指紋特徴データをネットワーク 30 経由で指紋照合サービス提供装置 2 0 A に送信する (2 0 5) 。

【 0 0 9 0 】

指紋照合サービス提供装置 2 0 A は、ユーザ側端末 1 0 A から暗号化指紋特徴データを受信すると、この暗号化指紋特徴データを前述のように暗号鍵対発生部 2 4 A で先の暗号鍵と対で生成された復号鍵を使用して指紋特徴データ復号化部 2 1 により指紋特徴データに復号する。

【 0 0 9 1 】

次に、指紋照合サービス提供装置 2 0 A は、登録ユーザ情報テーブル 2 6 の登録ユーザ情報 (ユーザ ID , 指紋特徴データ) からユーザ ID に対応する登録指紋特徴データを求め、この登録指紋特徴データと復号された入力指紋特徴データとの照合を指紋特徴照合部 2 3 で行う。 40

【 0 0 9 2 】

続いて、指紋照合サービス提供装置 2 0 A は、指紋特徴照合部 2 3 での照合結果として、登録指紋特徴データと入力指紋特徴データとが十分一致しており同一指紋であると判定できる場合には一致を、登録指紋特徴データと入力指紋特徴データとが十分一致しておらず同一指紋であると判定できない場合には不一致を、本人確認結果としてネットワーク経由で電子商取引提供装置 1 5 に通知する (2 0 6) 。

【 0 0 9 3 】

電子商取引提供装置 1 5 A は、本人確認結果を受けると、本人確認結果が一致であれば登録済みのユーザであり、なりすましではないとして、商品・サービスを要求ユーザに提 50

供する(207)。一方、本人確認結果が不一致であれば、登録済みのユーザではないとして、商品・サービスの提供を行わない。

【0094】

第2の実施の形態の場合も、第1の実施の形態の場合と同様に、ユーザIDはユーザと指紋照合サービス提供装置20Aとの間でユーザの識別子として用いることができれば任意に決定可能であり、必ずしもユーザのプライバシーを含む個別情報とリンクする必要がない。すなわち、電子商取引提供装置15Aが使用するユーザの決済情報などの個人情報とは分離され、指紋照合サービス提供装置20Aは、個人情報に接する可能性がなくなり、プライバシーがより高度に保たれることになる。

【0095】

また、指紋特徴データの送付毎に暗号鍵と復号鍵との対を生成して使用することにより、指紋特徴データの内容秘匿の確実性を増すことができる。

【0096】

なお、第2の実施の形態では、暗号鍵対発生部24Aを指紋照合サービス提供装置20A側に設けるようにしたが、これと同様な機能をユーザ側端末10A側に置き、指紋特徴データ暗号化部13で使用した暗号鍵と対となる復号鍵を指紋照合サービス提供装置20A側の指紋特徴データ復号化部21に送って復号するという構成も、同様にして容易に実現することができる。

【0097】

また、第2の実施の形態では、指紋特徴データ暗号化部13および指紋特徴データ復号化部21は受け取った暗号鍵および復号鍵をそのまま暗号処理および復号処理に使用しているが、その前に秘密の関数機能を設け、受け取った暗号鍵および復号鍵をあるルールに従って一度別の値に変換し、それらを暗号処理および復号処理に使用するという構成を実現することもできる。

【0098】

(3) 第3の実施の形態図3は、本発明の第3の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムの構成を示すブロック図である。第3の実施の形態に係る指紋本人確認サービス提供システムは、例えばコンビニエンスストアなどの店頭に設置されている共用の電子商取引サービス端末(以下、共用サービス端末という)19を使用してユーザが取引を行う場合についてのものである。このような共用サービス端末19についても、第1および第2の実施の形態に係る指紋本人確認サービス提供システムにおけるユーザ側端末10および10Aと同様に、そこに指紋センサなどを設置し、それらを同様に動作させて本人確認を行うことができる。しかし、ユーザは、そのような他の人間も使用した共用サービス端末19の指紋センサに指を置くことをいやがる可能性がある。また、ユーザの管理下でないそのような店舗の共用サービス端末19では、例えばその共用サービス端末19の管理者に指紋特徴データを盗まれるなどの可能性をおそれることが考えられる。このような不安感は電子商取引における指紋を用いた確実な本人確認の普及の妨げになりうるので、なくすような処置を講ずることが望ましい。

【0099】

そこで、第3の実施の形態に係る指紋本人確認サービス提供システムでは、ユーザは自分の証明を行うユーザ携帯ユニット10Bを自分で所有し、携帯して本人確認に用いることとする。ユーザ携帯ユニット10Bは、第2の実施の形態におけるユーザ側端末10Aと同様に、指紋センサ11、指紋特徴抽出部12、および指紋特徴データ暗号化部13を備え、ユーザが指紋センサ11に指を当てて指紋を入力すると、指紋センサ11により指紋画像データが読み取られ、読み取られた指紋画像データから指紋特徴抽出部12で照合用の指紋特徴データが抽出され、以下に述べるようにして暗号鍵対発生部24Aから送られた暗号鍵に基づいて指紋特徴データ暗号化部13でそれが暗号化される。

【0100】

ユーザ携帯ユニット10Bは、電子手帳、携帯情報端末、携帯通信端末、携帯電話機、

10

20

30

40

50

あるいは情報処理機能を持つカード形式のものがあり得る。

【0101】

共用サービス端末19は、ネットワークを介して電子商取引提供装置15と接続されて、物品の購入・サービスの申込みなどの電子商取引を仲介する機能を持つものであり、さらに第3の実施の形態では、ユーザ携帯ユニット10Bと何らかの形で情報交換を行う機能を持つ。例えば、共用サービス端末19は、ユーザ携帯ユニット10Bを内部に一部挿入する、ユーザ携帯ユニット10Bとケーブルで接続する、あるいはユーザ携帯ユニット10Bと無線あるいは赤外線などの非接触通信によって通信する機能を持つものである。共用サービス端末19は、ユーザに対しさまざまな情報サービスや電子商取引の提供端末として働くが、ユーザの本人確認に関しては、ユーザ携帯ユニット10Bと電子商取引提供装置15との通信を、中身を変えずに橋渡しする透明な仲介者として機能する。 10

【0102】

なお、その他の部分は、第1および第2の実施の形態に係る指紋本人確認サービス提供システムにおける対応部分と同様に構成されているので、対応部分には同一符号を付してそれらの詳しい説明を割愛する。

【0103】

次に、このように構成された第3の実施の形態に係る指紋本人確認サービス提供システムの動作について、第1および第2の実施の形態に係る指紋本人確認サービス提供システムの動作との違いを中心に説明する。

【0104】

指紋照合サービス提供機関の指紋照合サービスを利用する電子商取引提供業者と取り引きしようとするユーザは、指紋照合サービス提供機関によって指定されたユーザ携帯ユニット10Bを、指紋照合サービス提供機関から配布を受ける、あるいは認定された機種を購入するなどして入手し、共用サービス端末19の設置されている店頭などに持参する。 20

【0105】

電子商取引提供業者と取引を行おうとするユーザは、まず、共用サービス端末19にユーザ携帯ユニット10Bをセットし、共用サービス端末19を使用して指紋照合サービス提供装置20Aに対してネットワーク経由で指紋の登録を要求する。

【0106】

指紋照合サービス提供装置20Aは、共用サービス端末19からの指紋登録要求を受けると、このユーザの識別子であるユーザIDを決定するとともに、暗号鍵対発生部24Aで暗号鍵および復号鍵を生成し、暗号鍵を伴う指紋入力要求を共用サービス端末19を通じてユーザ携帯ユニット10Bに送信する。この通信は、電子商取引提供装置15Aや共用サービス端末19を介する必要はかならずしもない。 30

【0107】

ユーザ携帯ユニット10Bは、暗号鍵を伴う指紋入力要求を受けると、ユーザに指紋の入力を促す。ユーザが指紋入力要求に対して指紋センサ11に指を当てて指紋を入力すると、指紋センサ11により指紋画像データが読み取られ、読み取られた指紋画像データから指紋特徴抽出部12で照合用の指紋特徴データが抽出され、この指紋特徴データが暗号鍵対発生部24Aから送られた暗号鍵に基づいて指紋特徴データ暗号化部13で暗号化される。ユーザ携帯ユニット10Bは、暗号化指紋特徴データを共用サービス端末19を通じてネットワーク経由で指紋照合サービス提供装置20Aに送信する。 40

【0108】

指紋照合サービス提供装置20Aは、共用サービス端末19から受け取った暗号化指紋特徴データを指紋特徴データ復号化部21で指紋特徴データに復号した後、ユーザIDと指紋特徴データとを対にして登録ユーザ情報として登録ユーザ情報テーブル26に登録する。前述のように、暗号鍵対発生部24Aで生成された暗号鍵に従って指紋特徴データ暗号化部13で暗号化された指紋特徴データは、暗号鍵対発生部24Aで発生された復号鍵を用いて指紋特徴データ復号化部21において正しく復号される。

【0109】

電子商取引提供業者と実際取引を行う際、ユーザは、共用サービス端末 19 の操作などによりユーザ ID を含む取引要求をネットワーク経由で電子商取引提供装置 15 A に通知する (301)。

【0110】

電子商取引提供装置 15 A は、共用サービス端末 19 からユーザ ID を含む取引要求を受けると、ユーザ ID を含む本人確認要求をネットワーク経由で指紋照合サービス提供装置 20 A に送信する (302)。

【0111】

指紋照合サービス提供装置 20 A は、ユーザ ID を含む本人確認要求を受信すると、暗号鍵対発生部 24 A で暗号鍵と復号鍵との対を生成し、暗号鍵を含む指紋入力要求を共用サービス端末 19 を介してユーザ携帯ユニット 10 B の指紋特徴データ暗号化部 13 に送る (303)。

10

【0112】

ユーザが指紋入力要求に対してユーザ携帯ユニット 10 B の指紋センサ 11 に指を当てて指紋を入力すると (304)、指紋センサ 11 により指紋画像データが読み取られ、読み取られた指紋画像データから指紋特徴抽出部 12 により照合用の指紋特徴データが抽出され、この指紋特徴データが暗号鍵対発生部 24 A から送信されてきた暗号鍵に基づいて指紋特徴データ暗号化部 13 で暗号化される。指紋特徴データ暗号化部 13 から出力される暗号化指紋特徴データは、共用サービス端末 19 および電子商取引提供装置 15 を介して指紋照合サービス提供装置 20 A に送られる (305)。

20

【0113】

指紋照合サービス提供装置 20 A は、受け取った暗号化指紋特徴データを前述のように暗号鍵対発生部 24 A で先の暗号鍵と対で生成された復号鍵によって指紋特徴データ復号化部 21 により指紋特徴データに復号する。

【0114】

次に、指紋照合サービス提供装置 20 A は、登録ユーザ情報テーブル 26 の登録ユーザ情報 (ユーザ ID、指紋特徴データ) からユーザ ID に対応する登録指紋特徴データを求め、これと復号された入力指紋特徴データとの照合を指紋特徴照合部 23 で行う。

【0115】

続いて、指紋照合サービス提供装置 20 A は、指紋特徴照合部 23 での照合結果として、登録指紋特徴データと入力指紋特徴データとが十分一致しており同一指紋であると判定できる場合には一致を、登録指紋特徴データと入力指紋特徴データとが十分一致しておらず同一指紋であると判定できない場合には不一致を、本人確認結果としてネットワーク経由で電子商取引提供装置 15 A に通知する (306)。

30

【0116】

電子商取引提供装置 15 A は、本人確認結果を受けると、本人確認結果が一致であれば登録済みのユーザであり、なりすましではないとして、共用サービス端末 19 を介するなどして商品・サービスを要求ユーザに提供する (307)。一方、本人確認結果が不一致であれば、登録済みのユーザではないとして、商品・サービスの提供を行わない。

【0117】

(4) 第 4 の実施の形態図 4 は、本発明の第 4 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムの構成を示すブロック図である。第 4 の実施の形態に係る指紋本人確認サービス提供システムは、第 2 の実施の形態に係る指紋本人確認サービス提供システムと同様に、ユーザが電子商取引提供業者との電子商取引を行う際に、本人確認を指紋で行う場合の構成の一例およびそこのデータの流れを示すものである。ここでは、ユーザの利便性を増すために、別の実施方法をとっている。

40

【0118】

第 4 の実施の形態に係る指紋本人確認サービス提供システムは、第 2 の実施の形態に係る指紋本人確認サービス提供システムとの構成上の違いとして、指紋照合サービス提供装

50

置 2 0 B が、指紋特徴照合部 2 3 の代わりに、指紋特徴 1 対多照合部 2 3 A を持っている。指紋特徴照合部 2 3 が登録ユーザ情報テーブル 2 6 で参照されたある 1 人の登録指紋特徴データと指紋特徴データ復号部 2 1 で復号された入力指紋特徴データとの 1 対 1 照合を行うのに対し、指紋特徴 1 対多照合部 2 3 A は登録ユーザ情報テーブル 2 6 に登録された全ての登録指紋特徴データと指紋特徴データ復号部 2 1 で復号された入力指紋特徴データとの照合を順次行い、最も類似度の高い、すなわち、一致するただ 1 つの指紋特徴データを発見してその指紋特徴データに対応するユーザ ID をユーザ識別結果として出力する。

【 0 1 1 9 】

なお、その他の部分は、第 1 ないし第 3 の実施の形態に係る指紋本人確認サービス提供システムにおける対応部分と同様に構成されているので、対応部分には同一符号を付してそれらの詳しい説明を割愛する。

10

【 0 1 2 0 】

このように構成された第 4 の実施の形態に係る指紋本人確認サービス提供システムの動作を、第 2 の実施の形態に係る指紋本人確認サービス提供システムとの違いを中心に説明する。

【 0 1 2 1 】

ユーザが行う指紋照合サービス提供装置 2 0 B への指紋の登録は同様であり、登録したユーザ全ての登録ユーザ情報（ユーザ ID、指紋特徴データ）を含む登録ユーザ情報テーブル 2 6 が保持される。なお、登録ユーザ情報テーブル 2 6 は、指紋照合サービス提供装置 2 0 B を利用する電子商取引提供業者ごとにそのユーザのみを含む形で管理されることが望ましい。

20

【 0 1 2 2 】

実際に電子商取引提供業者と取引を行う際、ユーザは、ユーザ側端末 1 0 A を使用してユーザ ID を用いずにネットワーク経由で電子商取引提供装置 1 5 A に取引を要求する（4 0 1）。

【 0 1 2 3 】

電子商取引提供装置 1 5 A は、指紋照合サービス提供装置 2 0 B に対して、本人確認要求の代わりにユーザ識別要求を行う（4 0 2）。

【 0 1 2 4 】

指紋照合サービス提供装置 2 0 B は、電子商取引提供装置 1 5 A からユーザ識別要求を受けると、暗号鍵対発生部 2 4 A で暗号鍵および復号鍵を生成し、電子商取引提供装置 1 5 A を通じてユーザ側端末 1 0 A の指紋特徴データ暗号化部 1 3 に送り（4 0 3）、ユーザに指紋の入力を要求する。

30

【 0 1 2 5 】

ユーザ側端末 1 0 A は、暗号鍵を伴う指紋入力要求を受けると、ユーザに指紋の入力を促す。ユーザが指紋センサ 1 1 に指を当てて指紋を入力すると（4 0 4）、指紋センサ 1 1 により指紋画像データが読み取られ、読み取られた指紋画像データから指紋特徴抽出部 1 2 により指紋特徴データが抽出され、この指紋特徴データが指紋特徴データ暗号化部 1 3 により同様に暗号化され、暗号化指紋特徴データがネットワーク経由で指紋照合サービス提供装置 2 0 B に送られる（4 0 5）。

40

【 0 1 2 6 】

指紋照合サービス提供装置 2 0 B は、受け取った暗号化指紋特徴データを前述のように暗号鍵対発生部 2 4 A で先の暗号鍵と対で生成された復号鍵によって指紋特徴データ復号化部 2 1 により指紋特徴データに復号する。

【 0 1 2 7 】

指紋特徴 1 対多照合部 2 3 A は、登録ユーザ情報テーブル 2 6 に登録された全ての指紋特徴データと指紋特徴データ復号部 2 1 から得られた入力指紋特徴データとの照合を順次行い、最も類似度の高い、すなわち一致するただ 1 つの指紋特徴データを発見してその指紋特徴データに対応するユーザ ID を出力する。なお、類似する指紋特徴データがなければ、その旨を出力する。指紋照合サービス提供装置 2 0 B は、このユーザ識別結果として

50

のユーザIDを電子商取引提供装置15に通知する(406)。

【0128】

電子商取引提供装置15Aは、指紋照合サービス提供装置20Bから通知されたユーザIDに基づいてそのユーザ情報に基づいた商品・サービスを要求ユーザに提供する(407)。ユーザが特定されるので、決済・支払いもこのユーザに対して行えばよい。

【0129】

このように、ユーザが取引を要求するに際してユーザIDの提示・入力を不要とすることにより、ユーザの利便性が増すことになる。

【0130】

(5) 第5の実施の形態図5は、本発明の第5の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムの構成を示すブロック図である。

【0131】

図5を参照すると、第5の実施の形態に係る指紋本人確認サービスシステムは、図1に示した第1の実施の形態に係る指紋本人確認サービスシステムにおけるユーザ側端末10に対して指紋処理プログラムを記録した記録媒体100を、指紋照合サービス提供装置20に対して指紋照合サービスプログラムを記録した記録媒体200をそれぞれ備える点が異なっている。これら記録媒体100および200は、磁気ディスク、半導体メモリ、その他の記録媒体であってよい。

【0132】

指紋処理プログラムは、記録媒体100からコンピュータでなるユーザ側端末10に読み込まれ、当該ユーザ側端末10の動作を指紋センサ11、指紋特徴抽出部12、指紋特徴データ暗号化部13、および暗号鍵発生部14として制御する。指紋処理プログラムの制御によるユーザ側端末10の動作は、第1の実施の形態における場合と全く同様になるので、その詳しい説明を割愛する。

【0133】

また、指紋照合サービスプログラムは、記録媒体200からコンピュータでなる指紋照合サービス提供装置20に読み込まれ、当該指紋照合サービス提供装置20の動作を登録ユーザ情報テーブル26、復号鍵発生部24、指紋特徴データ復号化部21、および指紋特徴照合部23として制御する。指紋照合サービスプログラムの制御による指紋照合サービス提供装置20の動作は、第1の実施の形態における場合と全く同様になるので、その詳しい説明を割愛する。

【0134】

(6) 第6の実施の形態図6は、本発明の第6の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムの構成を示すブロック図である。

【0135】

図6を参照すると、第6の実施の形態に係る指紋本人確認サービスシステムは、図2に示した第2の実施の形態に係る指紋本人確認サービスシステムにおけるユーザ側端末10Aに対して指紋処理プログラムを記録した記録媒体100Aを、指紋照合サービス提供装置20Aに対して指紋照合サービスプログラムを記録した記録媒体200Aをそれぞれ備える点が異なっている。これら記録媒体100Aおよび200Aは、磁気ディスク、半導体メモリ、その他の記録媒体であってよい。

【0136】

指紋処理プログラムは、記録媒体100Aからコンピュータでなるユーザ側端末10Aに読み込まれ、当該ユーザ側端末10Aの動作を指紋センサ11、指紋特徴抽出部12、および指紋特徴データ暗号化部13として制御する。指紋処理プログラムの制御によるユーザ側端末10Aの動作は、第2の実施の形態における場合と全く同様になるので、その詳しい説明を割愛する。

【0137】

10

20

30

40

50

また、指紋照合サービスプログラムは、記録媒体 200A からコンピュータでなる指紋照合サービス提供装置 20A に読み込まれ、当該指紋照合サービス提供装置 20A の動作を登録ユーザ情報テーブル 26，暗号鍵対発生部 24A，指紋特徴データ復号化部 21，および指紋特徴照合部 23 として制御する。指紋照合サービスプログラムの制御による指紋照合サービス提供装置 20A の動作は、第 2 の実施の形態における場合と全く同様になるので、その詳しい説明を割愛する。

【0138】

(7) 第 7 の実施の形態図 7 は、本発明の第 7 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムの構成を示すブロック図である。

10

【0139】

図 7 を参照すると、第 7 の実施の形態に係る指紋本人確認サービスシステムは、図 3 に示した第 3 の実施の形態に係る指紋本人確認サービスシステムにおけるユーザ携帯ユニット 10B に対して指紋処理プログラムを記録した記録媒体 100B を、指紋照合サービス提供装置 20A に対して指紋照合サービスプログラムを記録した記録媒体 200A をそれぞれ備える点が異なっている。これら記録媒体 100B および 200A は、磁気ディスク，半導体メモリ，その他の記録媒体であってよい。

【0140】

指紋処理プログラムは、記録媒体 100B からコンピュータでなるユーザ携帯ユニット 10B に読み込まれ、当該ユーザ携帯ユニット 10B の動作を指紋センサ 11，指紋特徴抽出部 12，および指紋特徴データ暗号化部 13 として制御する。指紋処理プログラムの制御によるユーザ携帯ユニット 10B の動作は、第 3 の実施の形態における場合と全く同様になるので、その詳しい説明を割愛する。

20

【0141】

また、指紋照合サービスプログラムは、記録媒体 200A からコンピュータでなる指紋照合サービス提供装置 20A に読み込まれ、当該指紋照合サービス提供装置 20A の動作を登録ユーザ情報テーブル 26，暗号鍵対発生部 24A，指紋特徴データ復号化部 21，および指紋特徴照合部 23 として制御する。指紋照合サービスプログラムの制御による指紋照合サービス提供装置 20A の動作は、第 3 の実施の形態における場合と全く同様になるので、その詳しい説明を割愛する。

30

【0142】

(8) 第 8 の実施の形態図 8 は、本発明の第 8 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムの構成を示すブロック図である。

【0143】

図 8 を参照すると、第 8 の実施の形態に係る指紋本人確認サービスシステムは、図 4 に示した第 4 の実施の形態に係る指紋本人確認サービスシステムにおけるユーザ側端末 10A に対して指紋処理プログラムを記録した記録媒体 100A を、指紋照合サービス提供装置 20B に対して指紋照合サービスプログラムを記録した記録媒体 200B をそれぞれ備える点が異なっている。これら記録媒体 100A および 200B は、磁気ディスク，半導体メモリ，その他の記録媒体であってよい。

40

【0144】

指紋処理プログラムは、記録媒体 100A からコンピュータでなるユーザ側端末 10A に読み込まれ、当該ユーザ側端末 10A の動作を指紋センサ 11，指紋特徴抽出部 12，および指紋特徴データ暗号化部 13 として制御する。指紋処理プログラムの制御によるユーザ側端末 10A の動作は、第 4 の実施の形態における場合と全く同様になるので、その詳しい説明を割愛する。

【0145】

また、指紋照合サービスプログラムは、記録媒体 200B からコンピュータでなる指紋照合サービス提供装置 20B に読み込まれ、当該指紋照合サービス提供装置 20B の動作

50

を登録ユーザ情報テーブル 26, 暗号鍵対発生部 24A, 指紋特徴データ復号化部 21, および指紋特徴 1 対多照合部 23A として制御する。指紋照合サービスプログラムの制御による指紋照合サービス提供装置 20B の動作は、第 4 の実施の形態における場合と全く同様になるので、その詳しい説明を割愛する。

【0146】

ところで、バイオメトリクスとして指紋を採用した場合を例に挙げて説明したが、指紋センサ, 指紋特徴抽出部, および指紋特徴照合部の部分を別のバイオメトリクスを入力し、特徴を抽出して照合する手段で置換すれば、掌紋, 顔, 虹彩, 網膜血管パターン, 掌形, 筆跡, 声紋など他のバイオメトリクスを使用することも可能である。さらには、複数のバイオメトリクスを併用し、バイオメトリクス複合による確認によって、より本人確認の

10

【0147】

また、上記各実施の形態では、指紋画像データから指紋特徴データを特徴抽出して用いるようにしたが、バイオメトリクスデータによっては特徴抽出することは必須ではなく、バイオメトリクスデータそのものを用いることも可能である。

【産業上の利用可能性】

【0148】

本発明はバイオメトリクス本人確認サービス提供システムに関し、特にネットワークを介した情報提供や電子商取引 (EC = Electronic Commerce) に際してユーザの本人確認を行うサービスを提供するバイオメトリクス本人確認サービス提供システムに関する。

20

【図面の簡単な説明】

【0149】

【図 1】本発明の第 1 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムを示すブロック図である。

【図 2】本発明の第 2 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムを示すブロック図である。

【図 3】本発明の第 3 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムを示すブロック図である。

【図 4】本発明の第 4 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムを示すブロック図である。

30

【図 5】本発明の第 5 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムを示すブロック図である。

【図 6】本発明の第 6 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムを示すブロック図である。

【図 7】本発明の第 7 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムを示すブロック図である。

【図 8】本発明の第 8 の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムを示すブロック図である。

【符号の説明】

40

【0150】

10, 10A ユーザ側端末

10B ユーザ携帯ユニット

11 指紋センサ

12 指紋特徴抽出部

13 指紋特徴データ暗号化部

14 暗号鍵発生部

15, 15A 電子商取引提供装置

16 ユーザ対応テーブル

19 共用サービス端末

50

20, 20A, 20B 指紋照合サービス提供装置

21 指紋特徴データ復号化部

23 指紋特徴照合部

23A 指紋特徴1対多照合部

24 復号鍵発生部

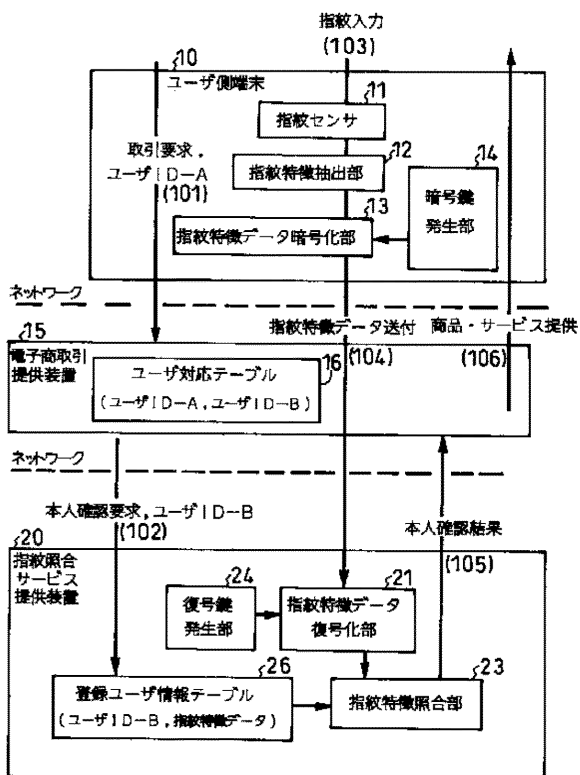
24A 暗号鍵対発生部

26 登録ユーザ情報テーブル

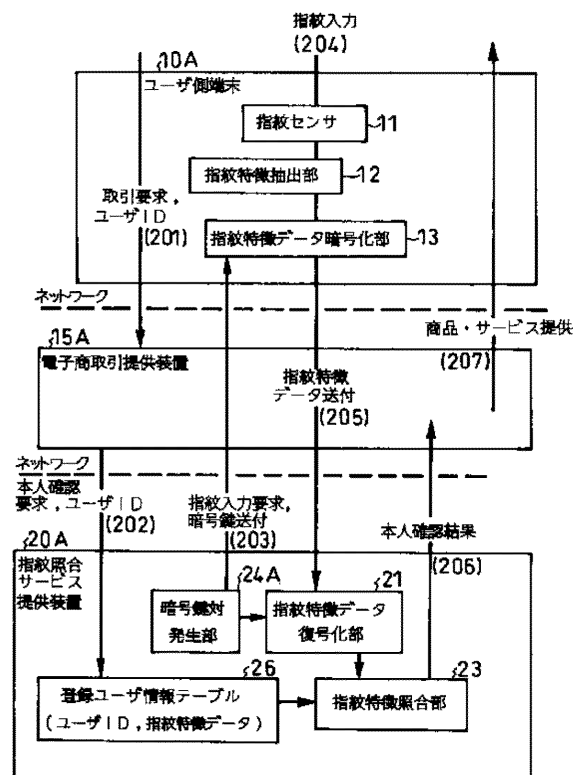
100, 100A, 100B 記録媒体

200, 200A, 200B 記録媒体

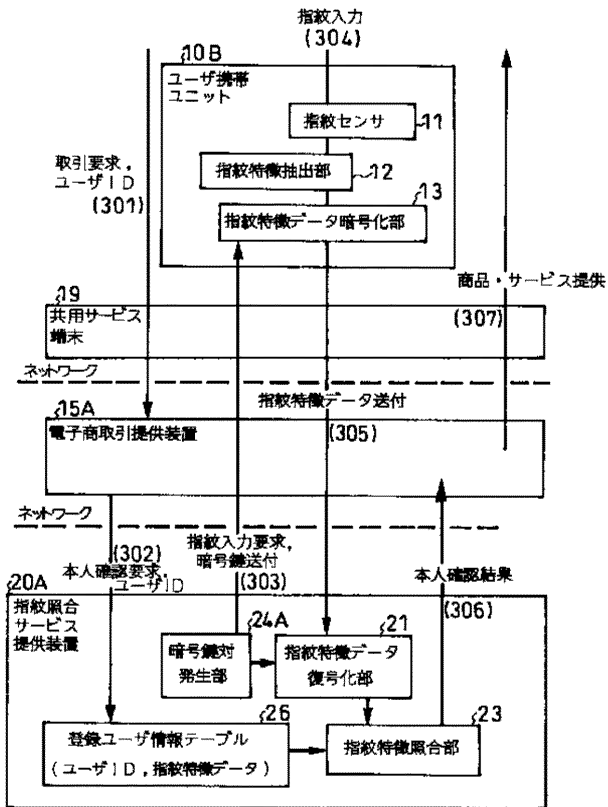
【図1】



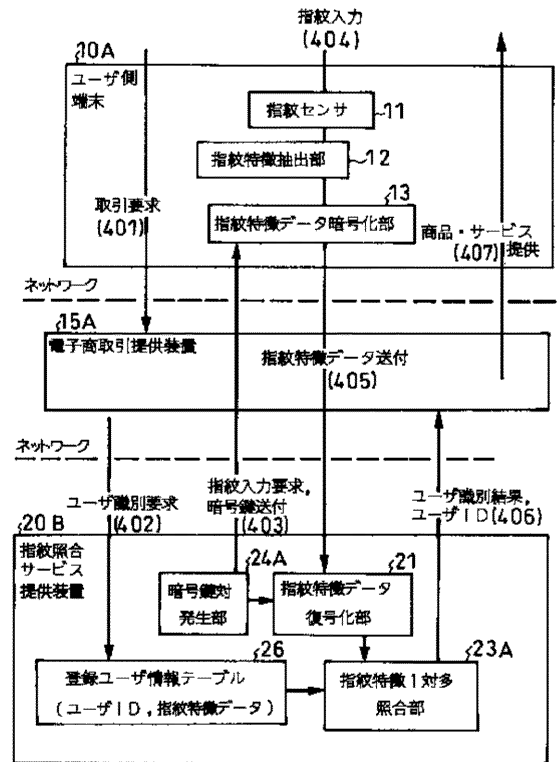
【図2】



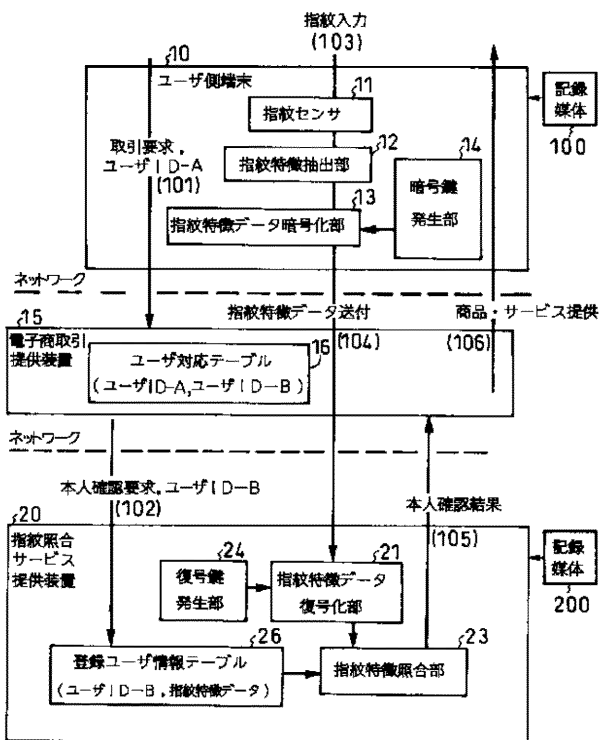
【図 3】



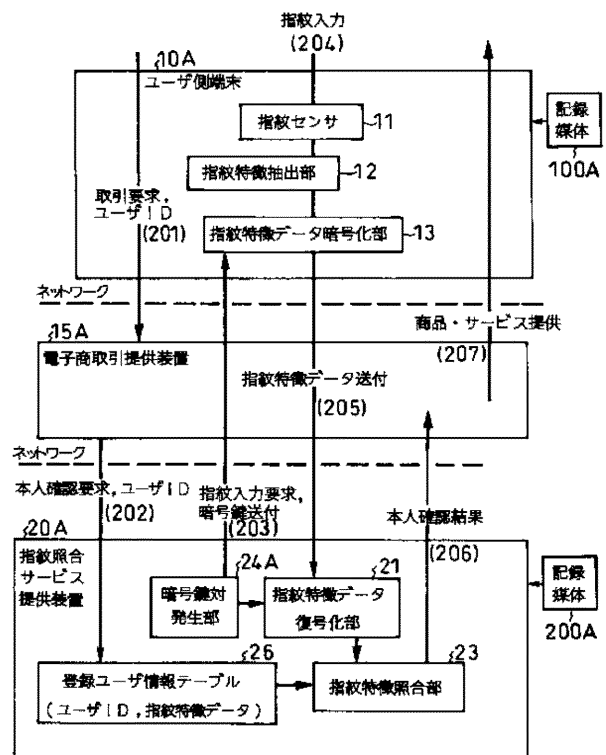
【図 4】



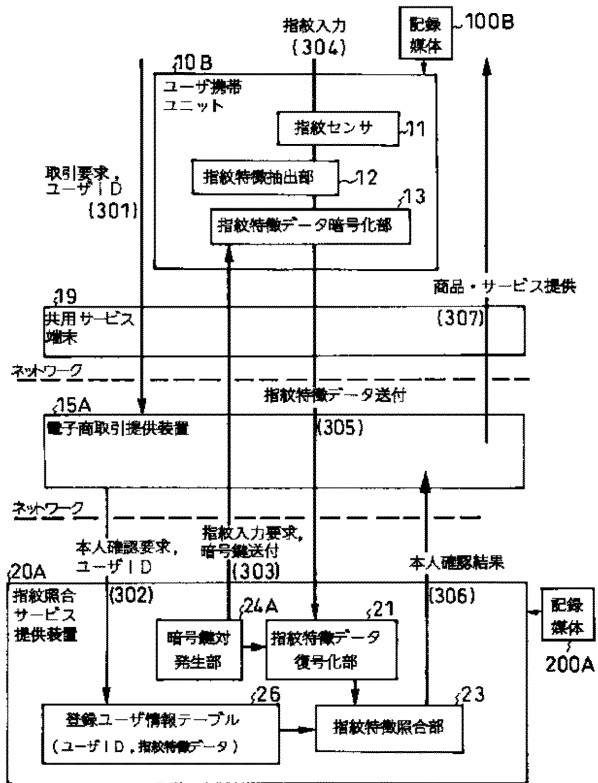
【図 5】



【図 6】



【図 7】



【図 8】

