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

特許第4511684号
(P4511684)

(45)発行日　平成22年7月28日(2010.7.28)　(24)登録日　平成22年5月14日(2010.5.14)

(51)Int.Cl.		F I		
G06Q 20/00	(2006.01)	G06F	17/60	414
G06Q 10/00	(2006.01)	G06F	17/60	512
G06Q 50/00	(2006.01)	G06F	17/60	ZEC
G06F 21/20	(2006.01)	G06F	15/00	330F

請求項の数 20　(全 28 頁)

(21)出願番号　特願2000-142617(P2000-142617)
(22)出願日　平成12年5月16日(2000.5.16)
(65)公開番号　特開2001-325549(P2001-325549A)
(43)公開日　平成13年11月22日(2001.11.22)
審査請求日　平成16年10月14日(2004.10.14)
審判番号　不服2007-11133(P2007-11133/J1)
審判請求日　平成19年4月18日(2007.4.18)

(73)特許権者　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　100121290
弁理士　木村　明隆
(74)代理人　100160554
弁理士　浅井　俊雄
(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

最終頁に続く

(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)【特許請求の範囲】
【請求項１】
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、前記電子商取引提供装置を経由せず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し、前記バイオメトリクス照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とするバイオメトリクス本人確認サービス提供システム。
【請求項２】
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請求項１記載のバイオメトリクス本人確認サービス提供システム。
【請求項３】

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請求項２記載のバイオメトリクス本人確認サービス提供システム。

【請求項４】

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請求項１記載のバイオメトリクス本人確認サービス提供システム。

【請求項５】

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請求項３記載のバイオメトリクス本人確認サービス提供システム。

【請求項６】

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請求項３記載のバイオメトリクス本人確認サービス提供システム。

【請求項７】

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請求項３記載のバイオメトリクス本人確認サービス提供システム。

【請求項８】

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請求項１記載のバイオメトリクス本人確認サービス提供システム。

【請求項９】

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前記電子商取引提供装置を経由せずに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し、前記バイオメトリクス照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とするバイオメトリクス本人確認サービス提供システム。

【請求項１０】

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請求項９記載のバイオメトリクス本人確認サービス提供システム。

【請求項１１】

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前記電子商取引提供装置を経由せずに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し、前記バイオメトリクス照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とするバイオメトリクス本人確認サービス提供システム。

【請求項１２】

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前記電子商取引提供装置を経由せずに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し、前記バイオメトリクス照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とするバイオメトリクス本人確認サービス提供システム。

【請求項１３】

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、前記共用サービス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前記電子商取引提供装置を経由せずに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し、前記バイオメトリクス照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とするバイオメトリクス本人確認サービス提供システム。

【請求項１４】

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前記電子商取引提供装置を経由せずに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し、前記バイオメトリクス照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とするバイオメトリクス本人確認サービス提供システム。

【請求項１５】

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つでなる請求項１ないし１４記載のバイオメトリクス本人確認サービス提供システム。

【請求項１６】

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請求項１ないし１４記載のバイオメトリクス本人確認サービス提供システム。

【請求項１７】

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前記電子商取引提供装置を経由せずに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し、前記指紋照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とする指紋本人確認サービス提供システム。

【請求項１８】

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前記電子商取引提供装置を経由せずに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し、前記指紋照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とする指紋本人確認サービス提供システム。

【請求項１９】

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、前記共用サービス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前記電子商取引提供装置を経由せずに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し、前記指紋照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とする指紋本人確認サービス提供システム。

【請求項２０】

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前記電子商取引提供装置を経由せずに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し、前記指紋照合サービス提供装置と前記電子商取引提供装置とは異なる組織で使用され、前記バイオメトリクスデータが前記電子商取引提供装置に通信されず使用されないことを特徴とする指紋本人確認サービス提供システム。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は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。
【０００２】
【従来の技術】
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】
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「電子商取引提供業者」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業者に決済方法などを含めてユーザ登録し、電子商取引提供業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う問題点があった。
【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。
【０００６】
【発明が解決しようとする課題】
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、
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。
【０００７】
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。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。
【０００８】
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業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。
【０００９】
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業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。
【００１０】
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業者が、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。
【００１１】
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。
【００１２】
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と、そのそれぞれに対して指紋などを登録する必要があり煩雑である、
（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。
【００１３】
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。
【００１４】
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。
【００１５】
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。
【００１６】
【課題を解決するための手段】
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。

【００１７】

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。

【００１８】

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。

【００１９】

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。

【００２０】

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。

【００２１】

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。

【００２２】

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。

【００２３】

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。

【００２４】

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。

【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、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。

【００２６】

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。

【００２７】

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。

【００２８】

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。

【００２９】

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。

【００３０】

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。

【００３１】

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。

【００３２】

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。

【００３３】

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。

【００３４】

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。

【００３５】

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。

【００３６】

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提供装置とを有することを特徴とする。

【００３７】

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。

【００３８】

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され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。

【００３９】

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。

【００４０】

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。

【００４１】

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。

【００４２】

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。

【００４３】

【発明の実施の形態】

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。

【００４４】

（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。

【００４５】

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（ＰＣ），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。

【００４６】

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。

【００４７】

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。

【００４８】

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。

【００４９】

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。

【００５０】

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。

【００５１】

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。

【００５２】

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と、指紋特徴データ復号化部２１と、指紋特徴照合部２３とを含んで構成されており、電子商取引提供装置１５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２４の生成する復号鍵を用い、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。

【００５３】

この復号処理は、ユーザ側端末１０の暗号鍵発生部１４および指紋特徴データ暗号化部１３の処理内容に対応したものを用いる。例えば、指紋特徴データ暗号化部１３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１４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。

【００５４】

登録ユーザ情報テーブル２６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。

【００５５】

指紋特徴照合部２３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２６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。

【００５６】

以上の指紋センサ１１，指紋特徴抽出部１２，指紋特徴照合部２３を含む指紋照合装置の実現例としては、特開昭５６－２４６７５号公報や特開平４－３３０６５号公報に記載された「指紋照合装置」がある。

【００５７】

特開昭５６－２４６７５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個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。

【００５８】

また、特開平４－３３０６５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。

【００５９】

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。

【００６０】

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２０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１０（あるいはそのうちの１１，１２，１３，１４の部分）を指定しておく。指紋照合サービス提供装置２０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業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１０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。

【００６１】
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、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１５に要求するとともに、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。
【００６２】
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を抽出し、この指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。
【００６３】
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。
【００６４】
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。
【００６５】
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）。
【００６６】
　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（１０３）。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）。
【００６７】
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）。
【００６８】
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）。

【００６９】

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）。

【００７０】

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。

【００７１】

（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の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。

【００７２】

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で使用することである。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。

【００７３】

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。

【００７４】

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。

【００７５】

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。

【００７６】

指紋照合サービス提供装置２０Ａは、ユーザ端末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。

【００７７】

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。ユーザ側端末１０Ａ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２０Ａに送る。

【００７８】

指紋照合サービス提供装置２０Ａは、ユーザ側端末１０Ａ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２６に登録する。前述のように、暗号鍵対発生部２４Ａ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１３で暗号化された指紋特徴データは、暗号鍵対発生部２４Ａ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。

【００７９】

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１０Ａ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１５Ａに通知する（２０１）。

【００８０】

電子商取引提供装置１５Ａ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２０Ａに送る（２０２）。

【００８１】

指紋照合サービス提供装置２０Ａ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２４Ａ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１０Ａに送る（２０３）。

【００８２】

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。ユーザが指紋センサ１１に指を当てて指紋を入力すると（２０４）、指紋センサ１１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１３で暗号化される。ユーザ側端末１０Ａは、指紋特徴データ暗号化部１３から出力された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２０Ａに送信する（２０５）。

【００８３】

指紋照合サービス提供装置２０Ａは、ユーザ側端末１０Ａ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２４Ａ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２１により指紋特徴データに復号する。

【００８４】

次に、指紋照合サービス提供装置２０Ａ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２３で行う。

【００８５】

続いて、指紋照合サービス提供装置２０Ａ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に通知する（２０６）。

【００８６】

電子商取引提供装置１５Ａ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。

【００８７】

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。

【００８８】

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。

【００８９】

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。

【００９０】

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。

【００９１】

（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、ユーザの管理下に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。

【００９２】

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。

【００９３】

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，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。

【００９４】

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。

【００９５】

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。

【００９６】

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。

【００９７】

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。

【００９８】

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。

【００９９】

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。

【０１００】

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。

【０１０１】
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。
【０１０２】
電子商取引提供業者と実際に取引を行う際、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１５Ａに通知する（３０１）。
【０１０３】
電子商取引提供装置１５Ａ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２０Ａに送信する（３０２）。
【０１０４】
指紋照合サービス提供装置２０Ａ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２４Ａ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１０Ｂの指紋特徴データ暗号化部１３に送る（３０３）。
【０１０５】
ユーザが指紋入力要求に対してユーザ携帯ユニット１０Ｂ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２４Ａ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業装置１５を介して指紋照合サービス提供装置２０Ａに送られる（３０５）。
【０１０６】
指紋照合サービス提供装置２０Ａ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２４Ａ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。
【０１０７】
次に、指紋照合サービス提供装置２０Ａ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。
【０１０８】
続いて、指紋照合サービス提供装置２０Ａ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１５Ａに通知する（３０６）。
【０１０９】
電子商取引提供装置１５Ａ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。
【０１１０】
（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で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。

【０１１１】

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置２０Ｂが、指紋特徴照合部２３の代わりに、指紋特徴１対多照合部２３Ａを持っている。指紋特徴照合部２３が登録ユーザ情報テーブル２６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２１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２３Ａは登録ユーザ情報テーブル２６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２１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。

【０１１２】

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。

【０１１３】

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。

【０１１４】

ユーザが行う指紋照合サービス提供装置２０Ｂ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２６が保持される。なお、登録ユーザ情報テーブル２６は、指紋照合サービス提供装置２０Ｂ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。

【０１１５】

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１０Ａ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１５Ａに取引を要求する（４０１）。

【０１１６】

電子商取引提供装置１５Ａは、指紋照合サービス提供装置２０Ｂ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（４０２）。

【０１１７】

指紋照合サービス提供装置２０Ｂは、電子商取引提供装置１５Ａからユーザ識別要求を受けると、暗号鍵対発生部２４Ａで暗号鍵および復号鍵を生成し、電子商取引提供装置１５Ａを通じてユーザ側端末１０Ａの指紋特徴データ暗号化部１３に送り（４０３）、ユーザに指紋の入力を要求する。

【０１１８】

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。ユーザが指紋センサ１１に指を当てて指紋を入力すると（４０４）、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１３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２０Ｂに送られる（４０５）。

【０１１９】

指紋照合サービス提供装置２０Ｂ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２４Ａ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。

【０１２０】

指紋特徴１対多照合部２３Ａは、登録ユーザ情報テーブル２６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２１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２０Ｂは、このユーザ識別結果としてのユーザＩＤを電子商取引提供装置１５に通知する（４０６）。

【０１２１】

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。

【０１２２】

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。

【０１２３】

（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。

【０１２４】

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。

【０１２５】

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。

【０１２６】

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。

【０１２７】

（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。

【０１２８】

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。

【０１２９】

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。

【０１３０】

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。

【０１３１】

（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。

【０１３２】

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。

【０１３３】

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。

【０１３４】

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。

【０１３５】

（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。

【０１３６】

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。

【０１３７】

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。

【０１３８】

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。

【０１３９】

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、より本人確認の確実性を高めることも可能である。

【０１４０】

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。

【０１４１】

【発明の効果】

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業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業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業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業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。

【０１４２】

また、バイオメトリクスデータは電子商取引提供業者を通過するが電子商取引提供業者には解読できない方法で暗号化されているため、電子商取引提供業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業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業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。

【０１４３】

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。

【０１４４】

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。

【０１４５】

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。

【図面の簡単な説明】

【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。

【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。

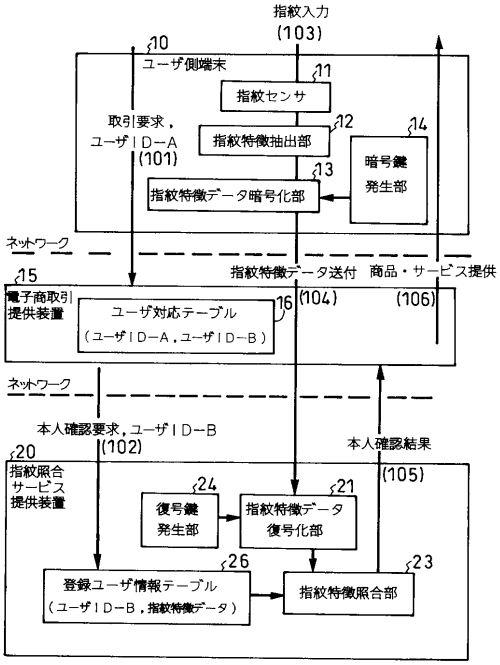
【図７】本発明の第７の実施の形態に係るバイオメトリクス本人確認サービス提供システムとしての指紋本人確認サービス提供システムを示すブロック図である。

【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。

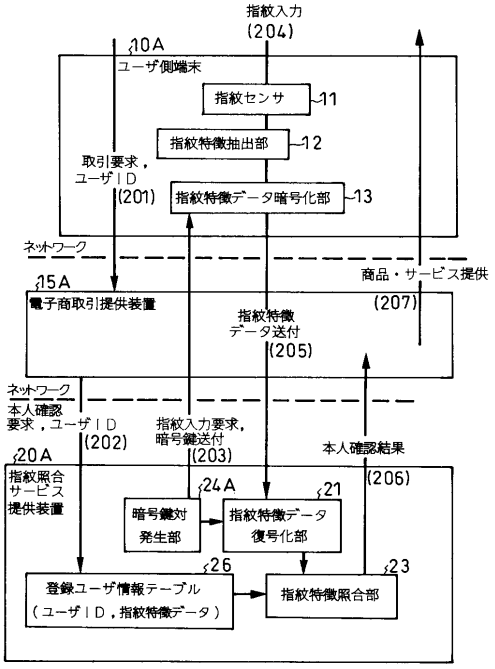
【符号の説明】

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
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

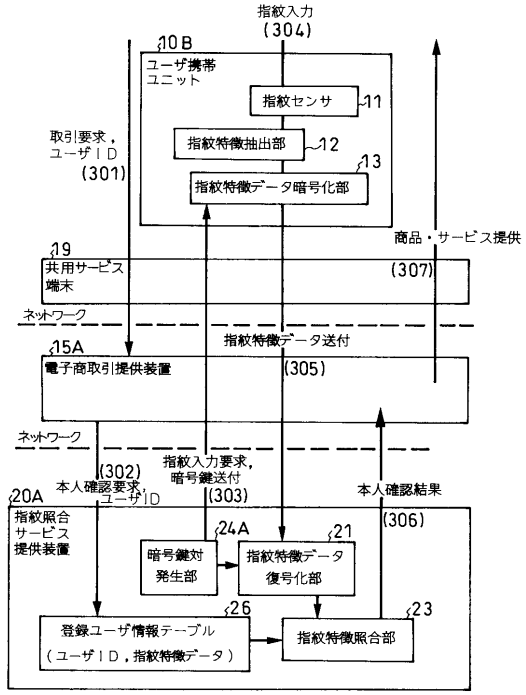
【図１】


指紋入力
(103)
10
ユーザ側端末
11
指紋センサ
取引要求，
ユーザＩＤ−Ａ
(101)
12
指紋特徴抽出部
14
暗号鍵
発生部
13
指紋特徴データ暗号化部
ネットワーク
15
電子商取引
提供装置
指紋特徴データ送付
(104)
商品・サービス提供
(106)
16
ユーザ対応テーブル
（ユーザＩＤ−Ａ，ユーザＩＤ−Ｂ）
ネットワーク
本人確認要求，ユーザＩＤ−Ｂ
(102)
本人確認結果
(105)
20
指紋照合
サービス
提供装置
24
復号鍵
発生部
21
指紋特徴データ
復号化部
26
23
登録ユーザ情報テーブル
（ユーザＩＤ−Ｂ，指紋特徴データ）
指紋特徴照合部

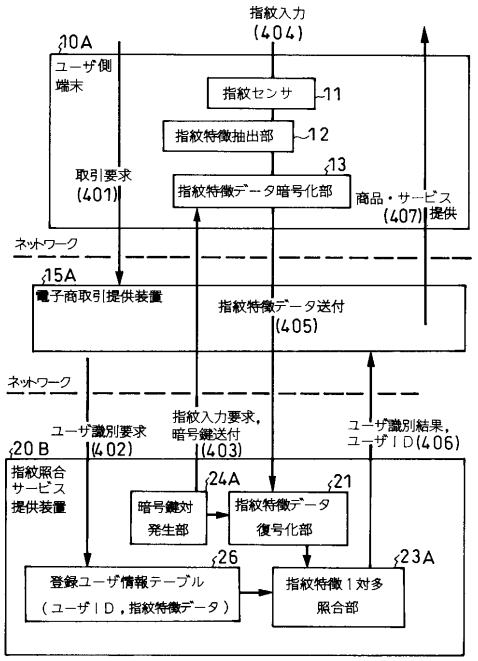
【図２】


指紋入力
(204)
10A
ユーザ側端末
11
指紋センサ
12
指紋特徴抽出部
取引要求，
ユーザＩＤ
(201)
13
指紋特徴データ暗号化部
ネットワーク
15A
電子商取引提供装置
商品・サービス提供
(207)
指紋特徴
データ送付
(205)
ネットワーク
本人確認
要求，ユーザＩＤ
(202)
指紋入力要求，
暗号鍵送付
(203)
本人確認結果
(206)
20A
指紋照合
サービス
提供装置
24A
暗号鍵対
発生部
21
指紋特徴データ
復号化部
26
23
登録ユーザ情報テーブル
（ユーザＩＤ，指紋特徴データ）
指紋特徴照合部

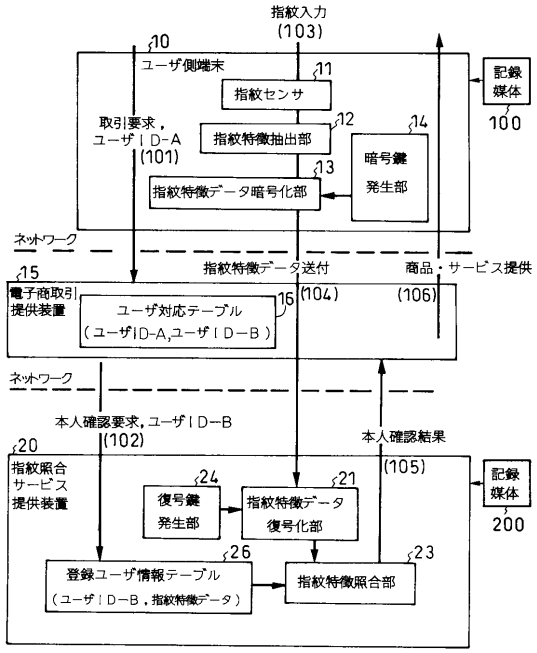
【図３】


指紋入力
(304)
10B
ユーザ携帯
ユニット
11
指紋センサ
取引要求，
ユーザＩＤ
(301)
12
指紋特徴抽出部
13
指紋特徴データ暗号化部
商品・サービス提供
(307)
19
共用サービス
端末
ネットワーク
指紋特徴データ送付
15A
電子商取引提供装置
(305)
ネットワーク
(302)
本人確認要求，
ユーザＩＤ
指紋入力要求，
暗号鍵送付
(303)
本人確認結果
(306)
20A
指紋照合
サービス
提供装置
24A
暗号鍵対
発生部
21
指紋特徴データ
復号化部
26
23
登録ユーザ情報テーブル
（ユーザＩＤ，指紋特徴データ）
指紋特徴照合部

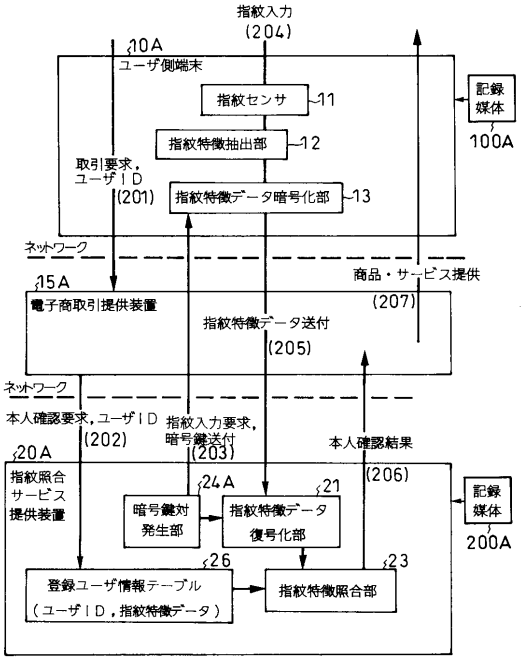
【図４】


指紋入力
(404)
10A
ユーザ側
端末
11
指紋センサ
12
指紋特徴抽出部
取引要求
(401)
13
指紋特徴データ暗号化部
商品・サービス
(407)提供
ネットワーク
15A
電子商取引提供装置
指紋特徴データ送付
(405)
ネットワーク
ユーザ識別要求
(402)
指紋入力要求，
暗号鍵送付
(403)
ユーザ識別結果，
ユーザＩＤ(406)
20B
指紋照合
サービス
提供装置
24A
暗号鍵対
発生部
21
指紋特徴データ
復号化部
26
23A
登録ユーザ情報テーブル
（ユーザＩＤ，指紋特徴データ）
指紋特徴１対多
照合部

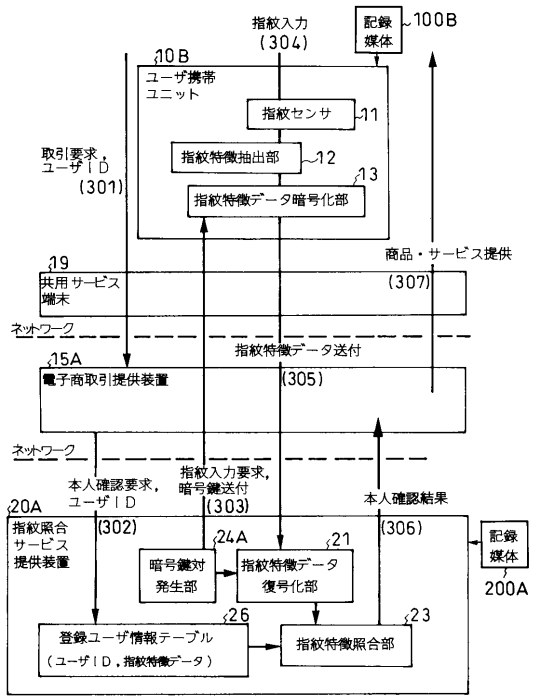
【図５】


指紋入力
(103)
10
ユーザ側端末
11
指紋センサ
記録媒体
100
取引要求，
ユーザＩＤ-A
(101)
12
指紋特徴抽出部
14
暗号鍵
発生部
13
指紋特徴データ暗号化部
ネットワーク
指紋特徴データ送付
(104)
商品・サービス提供
(106)
15
電子商取引
提供装置
16
ユーザ対応テーブル
（ユーザID-A,ユーザＩＤ－Ｂ）
本人確認要求，ユーザＩＤ－Ｂ
(102)
本人確認結果
(105)
20
指紋照合
サービス
提供装置
24
復号鍵
発生部
21
指紋特徴データ
復号化部
記録媒体
200
26
登録ユーザ情報テーブル
（ユーザＩＤ－Ｂ，指紋特徴データ）
23
指紋特徴照合部

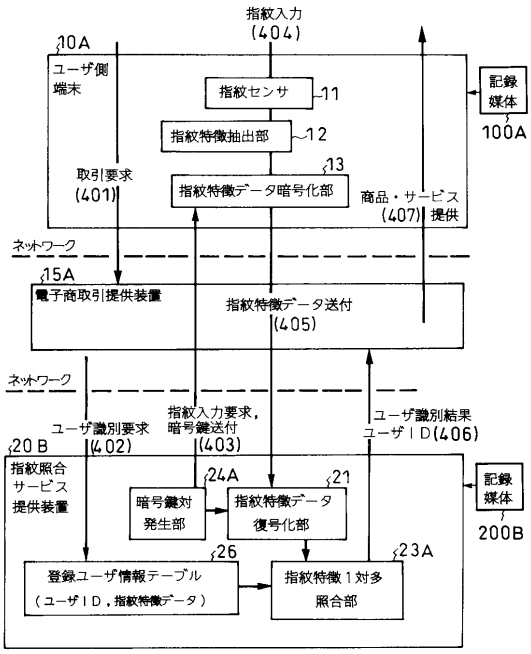
【図６】


指紋入力
(204)
10A
ユーザ側端末
11
指紋センサ
記録媒体
100A
12
指紋特徴抽出部
取引要求，
ユーザＩＤ
(201)
13
指紋特徴データ暗号化部
ネットワーク
商品・サービス提供
15A
電子商取引提供装置
(207)
指紋特徴データ送付
(205)
本人確認要求，ユーザＩＤ
(202)
指紋入力要求，
暗号鍵送付
(203)
本人確認結果
(206)
20A
指紋照合
サービス
提供装置
24A
暗号鍵対
発生部
21
指紋特徴データ
復号化部
記録媒体
200A
26
登録ユーザ情報テーブル
（ユーザＩＤ，指紋特徴データ）
23
指紋特徴照合部

【図７】


指紋入力
(304)
記録媒体
100B
10B
ユーザ携帯
ユニット
11
指紋センサ
取引要求，
ユーザＩＤ
(301)
12
指紋特徴抽出部
13
指紋特徴データ暗号化部
商品・サービス提供
(307)
19
共用サービス
端末
ネットワーク
指紋特徴データ送付
15A
電子商取引提供装置
(305)
ネットワーク
本人確認要求，
ユーザＩＤ
(302)
指紋入力要求，
暗号鍵送付
(303)
本人確認結果
(306)
20A
指紋照合
サービス
提供装置
24A
暗号鍵対
発生部
21
指紋特徴データ
復号化部
記録媒体
200A
26
登録ユーザ情報テーブル
（ユーザＩＤ，指紋特徴データ）
23
指紋特徴照合部

【図８】


指紋入力
(404)
10A
ユーザ側
端末
11
指紋センサ
記録媒体
100A
12
指紋特徴抽出部
13
指紋特徴データ暗号化部
取引要求
(401)
商品・サービス
(407)
提供
ネットワーク
15A
電子商取引提供装置
指紋特徴データ送付
(405)
ネットワーク
ユーザ識別要求
(402)
指紋入力要求，
暗号鍵送付
(403)
ユーザ識別結果
ユーザＩＤ(406)
20B
指紋照合
サービス
提供装置
24A
暗号鍵対
発生部
21
指紋特徴データ
復号化部
記録媒体
200B
26
登録ユーザ情報テーブル
（ユーザＩＤ，指紋特徴データ）
23A
指紋特徴１対多
照合部

フロントページの続き

合議体
審判長　清田　健一
審判官　須田　勝巳
審判官　山本　穂積

(56)参考文献　国際公開第９８／５０８７５（WO，Ａ１）
特開平１１－９８２５２（ＪＰ，Ａ）
特開平０５－３４７６１７（ＪＰ，Ａ）
特開平１０－１１７１７３（ＪＰ，Ａ）
特開平１１－３３８９４７（ＪＰ，Ａ）
特開２０００－９２０４６（ＪＰ，Ａ）
特開平１１－３１６７２９（ＪＰ，Ａ）
特開平１１－９６３６３（ＪＰ，Ａ）
特表平１１－５１１８８２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06Q10/00-50/00