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

特許第4510392号
(P4510392)

(45)発行日　平成22年7月21日(2010.7.21)　(24)登録日　平成22年5月14日(2010.5.14)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675B
G09C 1/00 (2006.01)　H04L 9/00 675D
G09C 1/00 640E

請求項の数 3　(全 22 頁)

(21)出願番号　特願2003-70403(P2003-70403)
(22)出願日　平成15年3月14日(2003.3.14)
(65)公開番号　特開2003-338816(P2003-338816A)
(43)公開日　平成15年11月28日(2003.11.28)
審査請求日　平成18年1月11日(2006.1.11)
(31)優先権主張番号　特願2002-71862(P2002-71862)
(32)優先日　平成14年3月15日(2002.3.15)
(33)優先権主張国　日本国(JP)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100090446
弁理士　中島　司朗
(72)発明者　横田　薫
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　大森　基司
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　館林　誠
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】個人情報認証を行うサービス提供システム

(57)【特許請求の範囲】
【請求項１】
個人情報認証装置が認証した利用者の個人情報に基づいて、サービス提供装置からサービス利用装置へネットワーク経由でサービスが提供される、というサービス提供システムであって、
前記個人情報認証装置は、
前記サービス利用装置から受け付けた利用者の個人情報の正当性を確認する個人情報認証手段と、
前記個人情報認証手段によって正当性が確認された個人情報に対して電子署名を付加することで生成した署名付き個人情報を前記サービス利用装置に送る署名付き情報生成手段と、を有し、
前記サービス利用装置は、
前記個人情報認証装置に利用者個人情報を送り、署名付き個人情報を得る署名付き情報取得手段と、
前記署名付き情報取得手段が取得した前記署名付き個人情報を記憶し、管理する情報記憶管理手段と、
前記情報記憶管理手段から前記署名付き個人情報を読み出し、サービス提供要求と共に前記サービス提供装置に送付するサービス要求手段と、
前記サービス要求手段が送付したサービス提供要求に対して前記サービス提供装置からサービスの提供をうけるサービス取得手段と、を有し、

前記サービス提供装置は、
前記サービス利用装置からサービス提供要求及び署名付き個人情報を受け付ける受付手段と、
前記受付手段が受け付けた署名付き個人情報が正当か否かを、付加された電子署名に基づいて判定する検証手段と、
前記検証手段が正当と判定した場合に、前記サービス利用装置にサービスを提供するサービス提供手段とを有し、
前記情報記憶管理手段は、前記署名付き個人情報を暗号化するための暗号鍵、及び、暗号化された署名付き個人情報を復号するための復号鍵を生成する鍵生成手段と、前記復号鍵を格納する鍵格納手段と、前記署名付き個人情報を、前記暗号鍵を用いて暗号化する暗号化手段と、前記暗号化手段によって暗号化された署名付き個人情報を格納する情報格納手段と、前記情報格納手段から前記暗号化された署名付き個人情報を、前記鍵格納手段から読み出した前記復号鍵を用いて復号する復号手段と、からなること
を特徴とするサービス提供システム。
【請求項２】
前記情報記憶管理手段は、外部からのアクセスから保護された保護記憶領域と、外部からのアクセスが可能な一般記憶領域と、プログラムを実行する演算装置とを有する、ＩＣメモリカードで成り、
前記暗号化手段及び前記復号化手段はそれぞれ、前記保護記憶領域に格納されたプログラムが前記演算装置によって実行されることで実現されるものであり、
前記鍵格納手段は前記保護記憶領域内に前記復号鍵を格納し、
前記情報格納手段は前記一般記憶領域内に前記暗号化された署名付き個人情報を格納すること、
を特徴とする請求項１に記載のサービス提供システム。
【請求項３】
個人情報認証装置が認証した利用者の個人情報に基づいて、サービス提供装置からサービス利用装置へネットワーク経由でサービスが提供される、というサービス提供システムにおいて、サービス利用装置が認証後の個人情報を保持するための情報管理装置であって、
前記署名付き個人情報を暗号化するための暗号鍵、及び、暗号化された署名付き個人情報を復号するための復号鍵を生成する鍵生成手段と、
前記復号鍵を格納する鍵格納手段と、
前記署名付き個人情報を、前記暗号鍵を用いて暗号化する暗号化手段と、
前記暗号化手段によって暗号化された署名付き個人情報を格納する情報格納手段と、
前記情報格納手段から前記暗号化された署名付き個人情報を読み出して、前記鍵格納手段から読み出した前記復号鍵を用いて復号する復号手段と、を有し、
前記情報記憶管理手段は、外部からのアクセスから保護された保護記憶領域と、外部からのアクセスが可能な一般記憶領域と、プログラムを実行する演算装置とを有する、ＩＣメモリカードで成り、
前記暗号化手段及び前記復号化手段はそれぞれ、前記保護記憶領域に格納されたプログラムが前記演算装置によって実行されることで実現されるものであり、
前記鍵格納手段は前記保護記憶領域内に前記復号鍵を格納し、
前記情報格納手段は前記一般記憶領域内に前記暗号化された署名付き個人情報を格納すること、
を特徴とする情報管理装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、インターネットなどのネットワークを介して各種サービス（例えば、商品の販売、音楽や映像などのデジタルコンテンツの有料配信）が業者から利用者へ提供される、

というサービス提供システムに関し、特に、サービス提供に当たって利用者の個人情報の機密性を保証するようなサービス提供システムに関する。また、同様のサービス提供方法に関する。

【０００２】

【従来の技術】

近年、一般家庭へのインターネット普及に伴い、ネットワークを介した各種サービス（商品の販売、デジタルコンテンツ（音楽や映像）の配信）を有料で提供するビジネスが盛んになっている。こうしたサービスの提供にあたって、サービス利用者は、商品の発送や代金の決済を行うために必要な個人情報をサービス提供業者に送信する必要がある。こうした個人情報としては氏名、住所、電話番号クレジットカード番号などが一般的である。サービス提供業者は、送信されてきた個人情報の正当性を検証し、正当性を認証した上でサービスの提供を行う。

【０００３】

だが、サービス利用者が同じサービス提供業者から繰り返しサービス提供を受ける場合、毎回個人情報を送信するのは利用者にとって不便である。また、サービス提供業者の側でも、数多い利用者の個人情報の正当性を、サービス提供のたびに認証するのは負荷が重い。

そこで、サービス利用者の利便性を高め、サービス提供業者の負荷を軽減することのできるサービス提供システムが必要とされる。

【０００４】

そうしたシステムの基本的な様態として、以下のようなものがある。サービス利用者は、あるサービス提供業者を１回目に利用する時にのみ個人情報を送信し、その正当性がサービス提供業者によって認証されると、この個人情報を自身が設定したユーザＩＤ及びパスワードと共に当該サービス提供業者に登録する。それ以降、サービス提供を受ける際、サービス利用者は前記登録したユーザＩＤ及びパスワードのみをサービス提供業者に送信する。サービス提供業者は、パスワードによってサービス利用者の正当性を認証し、ユーザＩＤを元に登録済み個人情報の中から当該サービス利用者の個人情報を得る。このシステムでは、サービス利用者はサービスを利用する度に個人情報を送信する必要はない。また、サービス提供業者は、個人情報の正当性認証を１人のサービス利用者につき１回行うだけでよい。

【０００５】

ただし、上記システムでは、複数のサービス提供業者を利用するサービス利用者は、サービス提供業者毎に別個のユーザＩＤ及びパスワードを登録し、これらを記憶しておく必要があり、ユーザＩＤ及びパスワードの管理が煩雑になる。一方、サービス提供業者の側でも、サービス利用者の数が増えれば、１人１回でも個人情報の正当性認証の処理負荷は重い。

【０００６】

そこで、個人情報の正当性認証と、認証済み個人情報の管理とを専門的に行う管理センターを含めたサービス提供システムが考案された。その代表的なものとして「．ＮＥＴ Ｐａｓｓｐｏｒｔ」方式（インターネット上の文書“Ｍｉｃｒｏｓｏｆｔ ．ＮＥＴ Ｐａｓｓｐｏｒｔ Ｔｅｃｈｎｉｃａｌ Ｏｖｅｒｖｉｅｗ（２００１年９月時点）（非特許文献１）”に記載）を採用したシステムがある。

【０００７】

このシステムでは、サービス利用者は予め、自身の個人情報をユーザＩＤ及びパスワードと共に管理センターに登録しておく。管理センターは個人情報の登録にあたって、上記のシステムではサービス提供業者が行っていた正当性確認を行う。そして、いったん個人情報を登録したサービス利用者は、サービス提供業者からサービスを受ける際に、管理センターにユーザＩＤ及びパスワードを送信して登録個人情報を取得し、取得した個人情報をサービス提供業者に送信する。なお、管理センターは、各サービス提供業者とユニークな秘密鍵暗号の鍵を共有しており、サービス利用者に個人情報を送信する際は、相手のサー

ビス提供業者と共有する鍵で暗号化した上で送信する。サービス利用者は暗号化された個人情報をサービス提供業者に送信し、サービス提供業者はこの共有する鍵を用いてサービス利用者から送信されてくる個人情報を復号する。

【０００８】

このシステムでは、サービス利用者は１種類のユーザＩＤ及びパスワードを管理センターにのみ登録すればよい。また、サービス提供業者は個人情報認証処理の負荷から解放される。

【０００９】

【非特許文献１】

Ｍｉｃｒｏｓｏｆｔ　．ＮＥＴ　Ｐａｓｓｐｏｒｔ　Ｔｅｃｈｎｉｃａｌ　Ｏｖｅｒｖｉｅｗ（２００１年９月）

【００１０】

【発明が解決しようとする課題】

しかしながら、管理センターを含むサービス提供システムには、以下のような問題がある。

先ず、管理センターは、システム内のサービス提供業者のいずれか一つでも利用したことのあるサービス利用者全てについて、個人情報を管理することになる。すなわち、管理センターには膨大な数のサービス利用者の個人情報が集中する。個人情報が集中することで、管理センターは、個人情報の不正入手を企むハッカーなどの標的にされ易い。そして、万が一、個人情報のデータベースが不正アクセスされた場合、流出する個人情報も大量となる。このことは、サービス利用者がシステムの安全性に不安を抱く原因となり、ネットワークを介してサービスの提供を受けることをためらわせる可能性がある。即ち、上記の安全性上の不安は、ネットワークを介してのサービス提供ビジネスの普及・促進の妨げになりかねない。

【００１１】

また、サービス利用者は、サービスを利用する際には必ず管理センターにアクセスすることになるので、管理センターの処理負荷は大きい。同時に多数のサービス利用者が管理センターにアクセスした場合、管理センターは許容限度を超えた負荷によってダウンしてしまう可能性もある。

本発明は、上記課題に鑑み、管理センターを含むサービス提供システムであって、個人情報管理の安全性、並びに、稼動中の安定性及び信頼性がより高い、というサービス提供システム、および、このようなサービス提供方法を提供することを目的とする。

【００１２】

【課題を解決するための手段】

上記の目的を達成するために、本発明は、個人情報認証装置が認証した利用者の個人情報に基づいて、サービス提供装置からサービス利用装置へネットワーク経由でサービスが提供される、というサービス提供システムであって、前記個人情報認証装置は、前記サービス利用装置から受け付けた利用者の個人情報の正当性を確認する個人情報認証手段と、前記個人情報認証手段によって正当性が確認された個人情報に対して電子署名を付加することで生成した署名付き個人情報を前記サービス利用装置に送る署名付き情報生成手段と、を有し、前記サービス利用装置は、前記個人情報認証装置に利用者個人情報を送り、署名付き個人情報を得る署名付き情報取得手段と、前記署名付き情報取得手段が取得した前記署名付き個人情報を記憶し、管理する情報記憶管理手段と、前記情報記憶管理手段から前記署名付き個人情報を読み出し、サービス提供要求と共に前記サービス提供装置に送付するサービス要求手段と、前記サービス要求手段が送付したサービス提供要求に対して前記サービス提供装置からサービスの提供をうけるサービス取得手段と、を有し、前記サービス提供装置は、前記サービス利用装置からサービス提供要求及び署名付き個人情報を受け付ける受付手段と、前記受付手段が受け付けた署名付き個人情報が正当か否かを、付加された電子署名に基づいて判定する検証手段と、前記検証手段が正当と判定した場合に、前記サービス利用装置にサービスを提供するサービス提供手段とを有すること、を特徴とす

るサービス提供装置、を提供する。

【００１３】

この構成によれば、正当性を認証された個人情報（署名付き個人情報）は、管理センター内の個人情報認証装置によって一元的に保持されるのでなく、各サービス利用者の手元にあるサービス利用装置に保存される。そのため、一度の不正アクセスで大量の個人情報が個人情報認証装置から流出するという事態を防ぐことができる。よって、システムの安全性は向上する。また、サービス利用の際は、サービス利用装置から個人情報認証装置にアクセスする必要がないので、サービス提供システム内で同時に大勢の利用者がサービス提供を求めることがあっても、個人情報認証装置に過大な負荷がかかることはない。よって、稼働中のサービス提供システムの安定性及び信頼性は向上する。

【００１４】

更に言えば、従来のサービス提供システムでは、サービス利用装置はサービス提供を受ける度に認証センターにアクセスするため、認証センターは、どの利用者がどのサービス提供装置をどの程度の頻度で利用しているかなど（サービス利用者の嗜好、サービス提供業者の売上実績など）の情報を収集できる立場にある。本実施の形態のサービス提供システムでは、サービス提供を受けようとするサービス利用装置は認証センターにアクセスする必要がないので、利用者や業者は、これら情報が認証センター経由で外部に漏れるのではという不安がなくなる。

【００１５】

また、上記の目的を達成するために、本発明のサービス提供方法は、個人情報認証装置が認証した利用者の個人情報に基づいて、サービス提供装置からサービス利用装置へネットワーク経由でサービスが提供される、というサービス提供システムにおけるサービス提供方法であって、前記個人情報認証装置において、前記サービス利用装置から受け付けた利用者の個人情報の正当性を確認する個人情報認証ステップと、前記個人情報認証装置において、前記個人情報認証ステップで正当性が確認された個人情報に対して電子署名を付加することで生成した署名付き個人情報を前記サービス利用装置に送る署名付き情報生成ステップと、前記サービス利用装置において、前記個人情報認証装置に利用者個人情報を送り、署名付き個人情報を得る署名付き情報取得ステップと、前記サービス利用装置において、前記署名付き情報取得ステップで取得した前記署名付き個人情報を記憶し、管理する情報記憶管理ステップと、前記サービス利用装置において、前記署名付き個人情報を読み出し、サービス提供要求と共に前記サービス提供装置に送付するサービス要求ステップと、前記サービス利用装置において、前記サービス提供要求に対して前記サービス提供装置から提供されるサービスを受け取るサービス取得ステップと、前記サービス提供装置において、前記サービス利用装置から前記サービス提供要求及び署名付き個人情報を受け付ける受付ステップと、前記サービス提供装置において、受け付けた前記署名付き個人情報が正当か否かを、付加された電子署名に基づいて判定する検証ステップと、前記サービス提供装置において、前記署名付き個人情報が正当と判定された場合に、前記サービス利用装置にサービスを提供するサービス提供ステップとを有すること、を特徴とするサービス提供方法とする。

【００１６】

【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ながら詳細に説明する。

（実施の形態１）

（概要）

図１は、本発明に関わるサービス提供システムの第１の実施の形態における大まかな構成を示す図である。本実施の形態におけるサービス提供システム１は、サービス提供業者がサービス利用者に対して有償サービスを提供するシステムであり、サービス利用者はサービスの提供を受ける際に、事前に認証センターによって正当性が認証された署名付き個人情報をサービス提供業者に提示する。

【００１７】

サービス提供システム１は、その装置構成として、サービス利用者の個人情報の認証業務を行う認証センター内にある個人情報認証装置１１、サービス利用者が使用するサービス利用装置１２、サービス提供業者がサービス提供のために用いるサービス提供装置１３がネットワークＮで接続されて成る。サービス利用装置、及び、サービス提供装置は複数存在するが、説明の便宜上、１つのみ図示してある。

【００１８】

個人情報認証装置１１は、具体例には、個人認証のためのプログラムを実行するコンピュータ又はサーバとする。また、サービス利用装置１２は、ネットワークＮと接続されたパーソナルコンピュータ又は通信機能を有する携帯端末とし、予め認証センターから提供され、インストールされているプログラムを実行することでサービス利用装置１２として動作する（前記プログラムは、例えば、認証センターが管理するホームページからダウンロードによってインストールされる）。サービス提供装置１３はサービス提供のためのプログラムを実行するコンピュータ又はサーバとする。

【００１９】

個人情報認証装置１１は、サービス利用装置１２から送信されてくる利用者の個人情報を認証する。個人情報認証装置１１は、認証した個人情報に電子署名を付加してサービス利用装置１２に返送する。電子署名は、これが付加された個人情報に関し、「誤りや虚偽がなく信頼できるものである」ことを、サービス提供業者に対して保証するものである。そして、個人情報認証装置１１は個人情報を保持しない。

【００２０】

サービス利用装置１２は、利用者が入力した利用者個人情報を個人情報認証装置１１に送って認証を受け、認証後の署名付き個人情報を内部に保存する。署名付き個人情報の保存場所は、外部からの参照が制限されたメモリカード内である。その後は、利用者からのサービス取得の指示を受けると、前記署名付き個人情報をサービス提供要求と共にサービス提供装置１３に送信し、サービス提供装置１３からサービスコンテンツを受信する。ただし、この署名付き個人情報が有効なのは、あらかじめ認証センタと契約してサービス提供システム１に参加しているサービス提供業者が管理するサービス提供装置１３に対してのみである。

【００２１】

サービス提供装置１３は、サービス提供を求める利用者がサービス利用装置１２を用いて送信してくる署名付き個人情報に応じてサービスを提供する。サービス提供装置１３は、サービス提供に当たって、署名付き個人情報に付加された電子署名の正当性のみを確認し、個人情報の正当性確認は行わない。電子署名の正当性確認には予め個人情報認証装置１１から得た署名確認用データ（例えば、公開鍵）を用いる。この確認用データは、例えば、サービス提供装置１３を管理するサービス提供業者が認証センターと契約を結んだ時点で、個人情報認証装置１１からサービス提供装置１３に送信されてくるものとすればよい。

【００２２】

上記のように、本実施の形態におけるサービス提供システム１では、認証後の署名付き個人情報は、認証センター内の個人情報認証装置１１に保持されるのでなく、各利用者それぞれの手元にあるサービス利用装置１２に保持される。また、サービス提供を受けようとするサービス利用装置１２も個人情報認証装置１１にはアクセスしない。そのため、認証センターへの個人情報の集中やアクセスの集中によって、システムの安全性や運用上の安定性が悪影響を受けることはない。

【００２３】

さらに、サービス利用装置１２における署名付き個人情報の管理におけるセキュリティを強化することで、署名付き個人情報の漏えいや改ざんの危険性が従来に比べ増大することを防止している。

すなわち、本実施の形態におけるサービス提供システム１は、署名付き個人情報を各々の利用者の手元にあるサービス利用装置に保持させることで従来の問題を解決する一方で、

サービス利用装置において署名付き個人情報を厳重管理させることで、署名付き個人情報の信頼性の低下を防いでいる。
（処理の流れ）
以下、本実施の形態のサービス提供システム１において実行される処理の流れについて説明する。
【００２４】
上記の概要説明から分かるように、本サービス提供システム１において行われる処理は、大きく２種類に分かれる。１つは、個人情報認証装置１１とサービス利用装置１２とが、サービス利用者の個人情報認証に関連して行う処理（以下、「個人情報認証手続き」）であり、もう１つは、サービス利用装置１２とサービス提供装置１３とが、サービス提供業者からサービス利用者へのサービス提供に関連して行う処理（以下、「サービス利用手続き」）である。以下、それぞれの手続きの流れについて、図面を参照しながら説明する。
・個人情報認証手続きの流れ
先ず、個人情報登録手続きの流れを、図面を参照しながら説明する。
【００２５】
図２は、個人情報認証装置１１とサービス利用装置１２とによって実行される個人情報登録手続きの流れを示す図である。
（１）利用者個人情報の入力
まず、サービス利用装置１２はサービス利用者から個人情報の入力を受け付ける。サービス利用装置１２は、入力された個人情報を認証センター内の個人情報認証装置１１に送信する。
【００２６】
図３は、サービス利用装置１２が個人情報認証装置１１に送信する利用者個人情報の構成を示す模式図である。同図に示す利用者個人情報は、「氏名」、「電話番号」、「住所」、「生年月日」、「クレジットカード番号」、「身長・体重」、「血液型」という項目からなる。同図に示すのは一例であり、利用者個人情報の項目は、システム内の各サービス提供装置において必要とされる項目を網羅したものとする必要がある。
【００２７】
（２）利用者個人情報の確認
次いで、個人情報認証装置１１は、サービス利用装置１２から受信した利用者個人情報を、外部の信頼できる情報源から得られた当該サービス利用者に関する情報（予め、個人情報認証装置１１に入力されているもの）に照会することで、利用者個人情報の正当性をチェックする。
【００２８】
（３）ＩＤ番号・署名の付与
個人情報認証装置１１は、正当性を認証できる利用者個人情報の各項目に対して、利用者固有の利用者ＩＤ番号と電子署名とを付加して、署名付き個人情報を生成する。
図４は、署名付き利用者個人情報４００の構成の一例を示す模式図である。署名付き個人情報は複数の項目から成り、各項目は、サービス利用装置１２から送信されてきた個人情報である本体部４１０に利用者ＩＤ部４２０、署名部４３０が付加された構成である。
【００２９】
個人情報認証装置１１は、先ず、利用者ＩＤ番号を１つ生成して利用者個人情報の各項目に付加する。その後、利用者ＩＤ番号付加後の各項目に対して公開鍵暗号方式を用いた電子署名を生成して付加する。電子署名の値は各項目毎に異なるようにする。署名データを生成する方法としては、例えばＥｌＧａｍａｌ署名方式を用いればよい。ＥｌＧａｍａｌ署名方式については例えば、岡本龍明、山本博資著「現代暗号」（産業図書）に記載されている。
【００３０】
そして、個人情報認証装置１１は、生成した署名付き利用者個人情報を、暗号化してサービス利用装置１２に送信する。具体的には、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａ

ｙｅｒ）プロトコルによる秘匿通信を行う。
なお、（２）の処理において、個人情報の正当性が認証できなかった場合、個人情報認証装置１１は、正しい個人情報の送信を求めるメッセージをサービス利用装置１２に送信し、手続きは（１）に戻る。
【００３１】
（４）署名付き個人情報の格納
サービス利用装置１２は、個人情報認証装置１１から送信されてきた署名付き個人情報を受信すると、先ずこれを復号する。さらに、いったん復号した署名付き個人情報を固有の格納用暗号鍵で暗号化し、内蔵するメモリカードに格納する。
【００３２】
（サービス利用手続き）
次いで、サービス利用者の要求に応じてサービス利用装置１２がサービス提供装置１３からサービスの提供を受ける手続き（サービス利用手続き）について説明する。
図５は、サービス利用手続きの手順を示す図である。
【００３３】
（１）サービス提供要求の発行
まず、利用者から指示を受けたサービス利用装置１２が、ネットワークＮを介してサービス提供装置１３にサービス提供要求を送信する。
（２）個人情報要求の発行
サービス提供要求を受信したサービス提供装置１３は、サービス提供のために必要な個人情報の項目を指定する個人情報要求をサービス利用装置１２に送信する。個人情報要求は所定のフォーマット（予め個人情報認証装置１１によって定められているもの）で記述され、必要な項目を項目の通番（例えば、図４の例では、「氏名」の通番は「１」、「住所」は「３」などとなる）で指定する。
【００３４】
（３）部分個人情報の送付
個人情報要求を受信したサービス利用装置１２は、暗号化して保持している署名付き個人情報を復号し、その中から個人情報要求によって指定された項目のみ抽出したもの（部分個人情報）をサービス提供装置１３に送信する。そして、送信の際は、ＳＳＬプロトコルに基づいた秘匿通信を行う。なお、この時、サービス利用装置１２は、個人情報要求の記述フォーマットをチェックして、正しいサービス提供装置１３からの要求であるか否か判定し、要求のフォーマットが正しくなければ、業者に成りすました第３者からの不正な要求と判断して個人情報の送信は行わない。フォーマットは予め個人情報認証装置１１から通知されているものとする。また、この判定は、フォーマットではなく、要求に付加された電子署名を元に行うこととしてもよい。その場合、サービス提供業者は、予め個人情報認証装置１１によって認証の上電子署名を付加された記述内容の要求を使用し、サービス利用装置１２は当該署名チェック用の公開鍵を予め個人情報認証装置１１から与えられているものとする。
【００３５】
図６は、部分個人情報６００の一例を示す模式図である。同図に示すのは、署名付き個人情報のうち、「氏名」、「電話番号」、「住所」、「クレジットカード番号」の４項目が要求された場合の内容である。
（４）利用者ＩＤ番号・署名の確認
部分個人情報を受信したサービス提供装置１３は、これを復号した上で、利用者ＩＤ番号と署名とを元に当該部分個人情報の正当性を判定する。判定処理の詳細については後で述べる。
【００３６】
（５）サービスの提供
上記判定の結果、部分個人情報が正当であると確認されると、サービス提供装置１３は、サービス利用装置１２に対してサービス提供を行う。提供されるサービスは、デジタル音

楽コンテンツのネットワーク配信などである。
（各装置の構成）
次いで、上記のような処理を実現する各装置（個人情報認証装置１１、サービス利用装置１２、サービス提供装置１３）の構成について、詳細な説明を述べる。
【００３７】
（個人情報認証装置１１の構成）
個人情報認証装置１１は、個人情報認証手続きに関する処理のみを行う。
図７は、個人情報認証装置１１の構成を示すブロック図である。個人情報認証装置１１は、サービス利用装置１２との間でデータ（認証前の利用者個人情報、認証後の署名付き個人情報など）の送受信を行う認証装置送受信部１１１、サービス利用装置１２から受け取った認証前の個人情報の正当性チェックを行う個人情報確認部１１２、正当性が確認された個人情報に認証証明である署名データを付加して署名付き個人情報を生成する署名生成部１１３を有する。
【００３８】
・認証装置送受信部１１１
認証装置送受信部１１１は、外部装置とのデータ送受信を行い、特に、サービス利用装置１２から個人情報を受信し、認証後の署名付き個人情報をサービス利用装置１２に送信する。個人情報（認証前後）の送受信においては、データを暗号化して秘匿する。具体的には、ＳＳＬプロトコルによる秘匿通信を行う。
【００３９】
・個人情報確認部１１２
個人情報確認部１１２は、認証装置送受信部１１１が受信した認証対象の個人情報の正当性を確認する（すなわち、認証してよい個人情報か否か判定する）。正当性確認は、利用者が送信してきた個人情報の内容を、認証センターに所属する管理者が予め他の信頼できる情報源から取得して個人情報確認部１１２に入力しておいた同種情報と比較するかたちで行われる。比較対象の情報は、具体的には、利用者に郵送させた住民票に記載された情報や、利用者の許可を得た上でクレジットカード会社から取得した利用者情報（クレジットカード番号を含む）などである。
【００４０】
・署名生成部１１３
署名生成部１１３は、個人情報確認部１１２によって正当性が確認された個人情報に電子署名を付加する。署名生成部１１３は、個人情報確認部１１２から個人情報を受け取る。そして、当該個人情報に対して、利用者毎にユニークな利用者ＩＤ番号を１つ生成し、これを個人情報の各項目の冒頭に付加する。
【００４１】
そして、利用者ＩＤ番号を付加した個人情報の項目の各々に対して、デジタル署名を生成して付加する。デジタル署名の生成方法は、公開鍵暗号方式とする（具体的には、ＥｌＧａｍａｌ署名方式を用いることができる）。すなわち、予め外部からの参照を禁じた形で保持している署名用秘密鍵を用い、利用者ＩＤ番号と対象項目とを連結したデータを元に電子署名を生成する。なお、この署名用秘密鍵に対応する署名用公開鍵は、サービス提供システム１内の各サービス提供装置１３に予め配布されている。
【００４２】
上記の手順で生成される電子署名は、各利用者で値の異なる個人情報及び利用者ＩＤ番号の内容をもとに生成されるので、当然、その値は利用者毎に異なり、さらには、１人の利用者の署名付き個人情報においても項目毎に値が異なる。
（サービス利用装置１２の構成）
サービス利用装置１２は、個人情報認証手続き、及びサービス利用手続きに関する処理を行う。
【００４３】
図８は、サービス利用装置１２の構成を示す。

サービス利用装置１２は、個人情報認証装置１１及びサービス提供装置１３とのデータ送受信を行う利用装置送受信部１２１、署名付き個人情報を格納するためのメモリカード１２３、メモリカード１２３を制御するメモリカード制御部１２２を有し、このうちメモリカード１２３は、着脱可能な様態でサービス利用装置１２のスロットに挿入されている。

【００４４】

・利用装置送受信部１２１

利用装置送受信部１２１は、個人情報認証手続きにおいては個人情報認証装置１１との間で認証前後の個人情報の送受信を行い、サービス利用手続きにおいてはサービス提供装置１３との間で各種情報（個人情報要求、部分個人情報、サービスコンテンツ）の送受信を行う。いずれの場合も、ＳＳＬプロトコルに基づく秘匿通信で送受信を行う。

【００４５】

・メモリカード制御部１２２

メモリカード制御部１２２は、メモリカード１２３への署名付き個人情報の入出力を管理する。個人情報認証手続きにおいては署名付き個人情報のメモリカード１２３への格納を行う。具体的には、暗号化された状態で受信された署名付き個人情報を復号した上で、格納命令と共にメモリカード１２３に出力する。

【００４６】

また、メモリカード制御部１２２は、サービス利用手続きにおいてはメモリカード１２３からの個人情報の読み出しを行う。具体的には、先ず、サービス利用要求に応じてサービス提供装置１３から送信されてきた個人情報要求を利用装置送受信部１２１経由で取得する。そして、この個人情報要求を解析して、サービス提供装置１３が求めている項目を特定する。そして、前記項目を示す情報と共に、個人情報出力命令をメモリカード１２３に対して発行する。

【００４７】

・メモリカード１２３

メモリカード１２３は、内部でのプログラム実行が可能なＩＣカードチップを有する。署名付き個人情報を格納するだけでなく、その入出力に関連して、メモリカード制御部１２２からの命令に従い、内部で処理を実行する。

図９は、メモリカード１２３の構造を示すブロック図である。メモリカード１２３の実体は、耐タンパ性の（外部からの不正アクセスから保護されている）ＩＣカードチップを有するメモリカードである。ＩＣカードチップはプログラムの格納及び実行、機能を有する。メモリカード１２３は耐タンパ性を有する保護記憶領域１２４（ＩＣカードチップ）、大容量データの格納が可能な一般記憶領域１２５を有する。保護記憶領域１２４には、署名付き個人情報の暗号化／復号処理を行う暗号化／復号部１２６、前記暗号化／復号処理に用いられる鍵の生成を行う鍵生成部１２７が格納されている。また、保護記憶領域１２４には、鍵を格納するための鍵記憶領域１２８が含まれている。なお、暗号化／復号部１２６、鍵生成部１２７の実体は保護記憶領域１２４に格納されたプログラムであり、これらプログラムは内蔵の演算装置（図示せず）によって実行されることで暗号化／復号部１２６、鍵生成部１２７として動作する。以下、主要構成部の処理内容を、「個人情報認証手続き」の場合と「サービス利用手続き」の場合とに分けて説明する。

【００４８】

・暗号化／復号部１２６

個人情報認証手続きに関連して、暗号化／復号部１２６は、メモリカード制御部１２２から転送されてくる署名付き個人情報を暗号化して一般記憶領域１２５に保存する。具体的には、暗号化／復号部１２６は、メモリカード制御部１２２から転送されてくる署名付き利用者個人情報を受け取ったタイミングで鍵生成部１２７に鍵生成を指示する。そして、鍵生成部１２７から暗号鍵を受け取ると、この暗号鍵を用いて署名付き利用者個人情報を暗号化し、一般記憶領域１２５に格納する。

【００４９】

サービス利用手続きに関連して、暗号化／復号部１２６は、メモリカード制御部１２２か

らの要求に応じ、保存されている署名付き個人情報を復号、出力する処理を行う。具体的には、暗号化／復号部１２６は、メモリカード制御部１２２から要求を受け取ると、鍵記憶領域１２８からは復号鍵を、一般記憶領域１２５からは暗号化された署名付き個人情報を、それぞれ読み出し、復号鍵を用いて署名付き個人情報を復号する。この時、読み出し及び復号の対象となるのは、個人情報のうちメモリカード制御部１２２から指定された項目のみである。そして、暗号化／復号部１２６は、復号した署名付き個人情報をメモリカード制御部１２２に送出する。

【００５０】

・鍵生成部１２７

鍵生成部１２７は、個人情報認証手続きにおいてのみ処理を行う。鍵生成部１２７は、暗号化／復号部１２６からの指示に応じて署名付き個人情報用に、暗号鍵及び復号鍵を生成する。そして、暗号鍵を暗号化／復号部１２６に送る一方、復号鍵は鍵記憶領域１２８に格納する。鍵記憶領域１２８は保護記憶領域１２４の内部にあるので、復号鍵はカード外部から直接読み出すことのできない状態で保持される。なお、ここで用いられるデータ暗号化方式については、公開鍵暗号方式でも秘密鍵暗号方式でもよい。例えば、秘密鍵暗号方式の一つであるＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）暗号方式を用いることができる。秘密鍵暗号方式の場合には、前記暗号鍵と復号鍵は同一のものとなる。なお、ＤＥＳ暗号方式については、例えば、「現代暗号」（岡本龍明、山本博資著、産業図書）に記載されている。

（サービス提供装置１３の構成）

サービス提供装置１３は、サービス利用手続きにおいて処理を行う。

【００５１】

図１０は、サービス提供装置１３の構成を示す。サービス提供装置１３は、サービス利用装置１２との間でデータ送受信を行う提供装置送受信部１３１、サービス提供要求と共にサービス利用装置１２から送信されてくる署名付き個人情報の正当性を確認する署名確認部１３２、提供すべきサービスコンテンツが格納されているメモリ装置１３３を有する。

【００５２】

提供装置送受信部１３１は、サービス利用装置１２からサービス提供要求を受信し、これに対して個人情報要求を送信する。そして、サービス利用装置１２から部分個人情報を受信すると、これを署名確認部１３２に送る。署名確認部１３２が個人情報の正当性を確認した場合、提供装置送受信部１３１は、メモリ装置１３３から要求されたサービスコンテンツを読み出してサービス利用装置１２に送信する。正当性が確認されなかった場合、提供装置送受信部１３１は、サービス利用装置１２にエラーメッセージを送信する。なお、サービスコンテンツをサービス利用装置１２に送信した際には、提供装置送受信部１３１は、サービス料の課金に必要な情報（利用者氏名、クレジットカード番号、提供されたコンテンツの内容など）を、図外の履歴データベースに保存しておく。この情報は、別途、サービス料の決済の際に参照される。

【００５３】

署名確認部１３２は、提供装置送受信部１３１がサービス利用装置１２から受信したサービス提供要求の内容を解析して、要求されたサービスの利用に必要な個人情報の項目を判定する。そして、その項目の送信を要求する個人情報要求を生成して提供装置送受信部１３１に送り、サービス利用装置１２に送信するよう指示する。

【００５４】

その後、サービス利用装置１２から送信されてきた部分個人情報を提供装置送受信部１３１から取得すると、署名確認部１３２は、付加された署名及び利用者ＩＤを元にその正当性を確認する。

先ず、署名確認部１３２は、署名を元に、当該個人情報の各項目が個人情報認証装置１１によって認証された情報であるか否かを確認する。署名確認の方法は、予め個人情報認証装置１１から通知されていた署名用公開鍵を用いる公知のものである。具体的には、署名用公開鍵、項目に付加された署名部４３０（図４参照）、及び、当該署名の元になったデ

ータ（利用者ＩＤ部４１０と個人情報部４２０とを連結したデータ）の３種類のデータの間に署名検証式と呼ばれる所定の関係が成り立つか否かチェックする。

【００５５】

次に、署名確認部１３２は、部分個人情報の各項目に付加されている利用者ＩＤ番号が全項目で共通か否か確認する。これは、署名で確認できるのが項目単位の正当性のみであり、例えば、複数の利用者の署名付き個人情報から、一部項目のみを抽出した上でこれらをまとめ、存在しない人物の署名付き個人情報を生成する、という形の偽造を検出できないからである。そこで、利用者ＩＤが全項目で一致するか否かをチェックし、一致しなかった場合は、複数の利用者の署名付き個人情報が混在しており、偽造された情報だと判定する。

【００５６】

利用者ＩＤ又は電子署名によるチェックの結果、両方で正当性が確認できなかった場合、署名確認部１３２は不正検出を提供装置送受信部１３１に送って、エラーメッセージをサービス利用装置１２に送信するよう指示する。

（まとめ）

上記の説明から分かる通り、本実施の形態におけるサービス提供システム１で、個人情報認証装置１１は、個人情報の正当性を確認後、署名を付加してサービス利用装置１２に返送し、従来のような署名付き個人情報の一括管理は行わない。すなわち、署名付き個人情報は各利用者の手元のサービス利用装置１２内に保存される。よって、従来のシステムのように、認証センターから多人数分の個人情報がまとめて流出するという安全性の面での問題はなく、また、サービスを利用の際にサービス利用装置１２が認証センターにアクセスすることもないので、システムの安定性も向上する。

【００５７】

しかも、サービス利用装置１２において、署名付き個人情報は、暗号化された上でメモリカードに保存され、その復号鍵は外部からの参照ができない領域に格納されている。このように、厳重に保存されるため、署名付き個人情報の管理主体が認証センターから利用者に代わることで、署名付き個人情報の信頼性が従来のシステムに比べて劣る、ということにはならない。

【００５８】

また、利用者に発行される署名付き個人情報の各項には利用者ごとにユニークな利用者ＩＤ番号が付加されているので、例えば、利用者Ａの氏名と利用者Ｂの住所をつなぎあわせて、存在しない人物の署名付き個人情報を偽造して、これを用いてサービス提供を受けようとしても、項目間で利用者ＩＤ番号が不一致となり、偽造は検出される。これによって、サービス提供業者から見た署名付き個人情報の信頼性は高まる。

【００５９】

また、署名付き個人情報は、着脱可能なメモリカードに記憶されているので、故障などの理由でサービス利用装置を交換する必要が生じた場合、メモリカードを移動するだけで、直ちに新しい装置でサービス提供を受けることができる。

なお、従来のサービス提供システムでは、サービス利用装置はサービス提供を受ける度に認証センターにアクセスする必要があったため、認証センターは、どの利用者がどのサービス提供装置をどの程度の頻度で利用しているかなど（言いかえれば、サービス利用者の嗜好、サービス提供業者の売上実績など）、サービス利用状況に関する情報を知りうる立場にあった。本実施の形態のサービス提供システムでは、サービス提供を受けようとするサービス利用装置は認証センターにアクセスする必要がないので、認証センターにこれら情報が知られる可能性はない。よって、サービス利用者やサービス提供業者としては、他者に知られたくない情報が認証センター経由で漏えいするのでは、という不安がなくなり、システムに対する提供業者の信頼は高くなる。

【００６０】

（変形例）

上述した実施の形態におけるサービス提供システム１では、署名付き個人情報はサービス

利用装置１２内に厳重に保管されているが、それでも、通信盗聴などの不正な手段で署名付き個人情報が盗まれた場合、盗んだ人物は、その情報をサービス提供装置に提示することによって利用者になりすますことが可能となる。そこで、本変形例は、署名付き個人情報が万が一盗まれても、成りすましには使用できないように、公開鍵暗号方式を用いた認証方式によって、サービス提供業者が個人情報送信元の身元認証を行える、というサービス提供システムを示す。

【００６１】

本変形例におけるサービス提供システムの特徴は以下の通りである。サービス利用装置が、サービス提供を受ける際に必要な身元認証用の公開鍵・秘密鍵の組を予め作成して、身元認証用公開鍵は、個人情報の一部として個人情報認証装置による認証を受けておく。サービス提供を受ける際、サービス利用装置は、身元認証用公開鍵を含めた署名付き個人情報をサービス提供業者に送信して、サービス提供業者は、これを元に送信もとのサービス利用装置の身元を確認した上でサービスを提供する。

【００６２】

本変形例に特有の構成として、サービス利用装置に、利用者から認証対象の個人情報が入力されたタイミングで、身元認証用の公開鍵・秘密鍵を生成する身元認証鍵生成部が追加される。また、サービス提供装置における署名確認部は、上述の実施の形態における処理に加え、身元認証用公開鍵を用いて個人情報送信元の身元を認証する処理を行う。

【００６３】

以下、本変形例における「個人情報登録手続き」、「サービス利用手続き」について図面を参照しながら説明する。実施の形態と同一の部分については説明を省略する。

図１１は本変形例ににおける個人情報登録手続きの手順を示す図である。

本変形例に固有の処理は、「（１ａ）身元認証用鍵の生成」である。ここでは、利用者からの個人情報入力を受け付けた身元認証鍵生成部が、公開鍵暗号方式に基づく、身元認証用の公開鍵・秘密鍵ペアを作成する。そして、身元認証用公開鍵については、入力された個人情報と共に利用装置送受信装置１２１（図８参照）に送出して、これらを個人情報認証装置に送信するよう指示する。一方、身元認証用秘密鍵については、メモリカード１２３内の保護記憶領域１２４内にある鍵記憶領域１２８（図９参照）に格納する。ここで利用される公開鍵暗号方式の種類は問わないが、例えばＥｌＧａｍａｌ暗号方式が使用できる。

【００６４】

これ以降の、個人情報認証装置１１における処理（２）、（３）は、実施の形態における処理と同じである。身元認証用公開鍵も、他の項目と同様に扱われる。

図１２は、本変形例における個人情報の構成の例を示したものである。同図（ａ）は認証及び署名付加前の個人情報を示し、同図（ｂ）は認証後の署名付き個人情報を示す。実施の形態における個人情報とは、項目の１つとして身元認証用公開鍵１２０１が追加されている点のみ異なる。当然、身元認証用公開鍵に対しても利用者ＩＤ番号が付加されたうえで、電子署名が付加される。

【００６５】

署名付き個人情報がサービス利用装置に送付されてからの処理（４）も、実施の形態におけるものと同じである。

図１３は、本変形例ににおけるサービス利用手続きの手順を示す図である。本変形例に固有の処理は、「（４ａ）公開鍵暗号を用いた身元確認」である。

「（１）サービス要求」から「（４）ＩＤ番号・署名の確認」までの処理は、実施の形態における処理とほぼ同一である。但し、（２）においてサービス提供装置からサービス利用装置に送付される個人情報要求には、対象の個人情報項目として必ず身元認証用公開鍵を含むこととする。

【００６６】

（４ａ）の処理を行うのはサービス提供装置の署名確認部（図１０参照）である。署名確認部は、（４）の処理（署名付き部分個人情報の利用者ＩＤ番号と署名とによるチェック

）の後、前記署名付き部分個人情報に含まれる身元認証用公開鍵を用いて、送信元が正当なサービス利用装置（対応する身持ち身元認証用秘密鍵を保持している装置）か否かの検証を行う。この検証の方式としては、公開鍵暗号方式に基づくものであれば種類は問わない。例えば、「現代暗号」（岡本龍明、山本博資著、産業図書）の「９．４　公開鍵暗号／ディジタル署名を利用した方式」に記載の方式を用いることができる。

【００６７】

本変形例では、サービス利用手続きの実行にあたって、公開鍵暗号方式による個人情報送信者の身元認証を行う。そのため、署名付き個人部分に含まれる身元認証用公開鍵に対応する身元認証用秘密鍵を保持していない装置を用いてサービスを受けることはできない。よって不正に署名付き個人情報を取得した者が正当なサービス利用者に成りすましてサービスを受けることはできない。サービス提供システムにおける署名付き個人情報の信頼度はさらに高くなる。身元認証用秘密鍵については、一度作成して保存した後は、メモリカードの保護記憶領域から外部に出力されないようにすることで、高い安全性を実現することができる。

（備考）

なお、署名付き個人情報については有効期限を定めておいてもよい。具体的には、個人情報認証装置が署名付き個人情報の中に有効期限情報を付加する。サービス提供業者はサービス提供の際に有効期限を参照し、有効期限切れであれば、署名付き個人情報を送信してきたサービス利用装置に対して最新の個人情報に基づく署名付き個人情報の再取得を要求する。このようにすれば、署名付き個人情報の信頼性は向上する。

【００６８】

また、サービス利用手続きの際にメモリカード内部で実行される暗号化署名付き個人情報の復号処理については、サービス利用者が予め設定したパスワードが入力されない限り実行されないこと、としてもよい。こうすれば、たとえメモリカードが挿入されたままでサービス利用装置が盗まれた場合でも、窃盗者がパスワードを知らない限りメモリカード内の個人情報を利用してサービスを受けることはできないので、安全性が向上する。また、パスワード以外にも、サービス利用者の生体情報（指紋、虹彩、声紋など）が利用可能である。

【００６９】

また、個人情報認証装置とサービス利用装置との間の通信、及び、サービス利用装置とサービス提供装置との間の通信における通信について、本実施の形態では、ＳＳＬプロトコルに基づく秘匿通信としているが、秘匿通信の実現手段はこれに限られるものではない。また、上記の実施の形態では、個人情報登録手続きにおける個人情報認証装置１１とサービス利用装置１２間の個人情報のやり取りは、ネットワークを介しての通信によって行われることになっているが、やり取りの方法はこれに限定されない。サービス利用者がサービス利用装置１２を携帯して認証センター１を訪れ、サービス利用装置１２と個人情報認証装置１１とを操作して直接的にデータ入出力を行う、という形も考えられる。または、メモリカードに個人情報を記録し、これを郵送でやり取りしてもよい。このようにすれば、通信経路での盗聴によって個人情報が漏えいする事態は防止できる。すなわち、個人情報認証装置とサービス利用装置とがネットワーク接続されていない形でのサービス提供システムも可能である。

【００７０】

また、サービス利用装置がサービス提供装置の要求に応じて個人部分情報を送信する際、サービス利用者による要求内容チェックが行われるようにしてもよい。具体的には、要求内容を画面表示させた上で、サービス利用者からの指示を受け付けるインタフェース部をサービス利用装置に備えさせてもよい。あるいは、予め、インタフェース部がサービス利用者からサービス提供業者に提示してもよい個人情報の項目の設定を受け付けておくこととしてもよい。

【００７１】

また、サービス提供時、サービス提供装置がサービス利用装置に送信する個人情報要求の

内容については、サービス利用者の個人情報と同様に、予め個人情報認証装置が妥当性や正当性を確認し、正当性の認証できる個人情報要求のデータに署名を付加してサービス提供装置に返送すること、としてもよい。そして、サービス利用装置は、個人情報要求の受信時に、前記署名によって内容の正当性を確認できる個人情報要求にのみ応答する。署名チェックのための公開鍵は、予め個人情報認証装置からサービス利用装置に送信しておく。このようにすれば、サービス提供装置へのなりすましによる個人情報の不正要求を防止でき、システム内における個人情報の安全性が高まる。

【００７２】

また、サービス利用装置が署名付き個人情報を保存するための構成は、必ずしもメモリカードでなくてもよい。サービス利用装置に内蔵された記憶装置内部に不正アクセスから保護された記憶領域を設けて、そこに記憶するようにしてもよい。

【００７３】

【発明の効果】

以上の説明から明らかなように、本発明のサービス提供システムは、個人情報認証装置が認証した利用者の個人情報に基づいて、サービス提供装置からサービス利用装置へネットワーク経由でサービスが提供される、というサービス提供システムであって、前記個人情報認証装置は、前記サービス利用装置から受け付けた利用者の個人情報の正当性を確認する個人情報認証手段と、前記個人情報認証手段によって正当性が確認された個人情報に対して電子署名を付加することで生成した署名付き個人情報を前記サービス利用装置に送る署名付き情報生成手段と、を有し、前記サービス利用装置は、前記個人情報認証装置に利用者個人情報を送り、署名付き個人情報を得る署名付き情報取得手段と、前記署名付き情報取得手段が取得した前記署名付き個人情報を記憶し、管理する情報記憶管理手段と、前記情報記憶管理手段から前記署名付き個人情報を読み出し、サービス提供要求と共に前記サービス提供装置に送付するサービス要求手段と、前記サービス要求手段が送付したサービス提供要求に対して前記サービス提供装置からサービスの提供をうけるサービス取得手段と、を有し、前記サービス提供装置は、前記サービス利用装置からサービス提供要求及び署名付き個人情報を受け付ける受付手段と、前記受付手段が受け付けた署名付き個人情報が正当か否かを、付加された電子署名に基づいて判定する検証手段と、前記検証手段が正当と判定した場合に、前記サービス利用装置にサービスを提供するサービス提供手段とを有する、という構成を特徴とする。

【００７４】

この構成によれば、正当性を認証された個人情報（署名付き個人情報）は、管理センター内の個人情報認証装置によって一元的に保持されるのでなく、各サービス利用者の手元にあるサービス利用装置に保存される。そのため、一度の不正アクセスで大量の個人情報が個人情報認証装置から流出するという事態を防ぐことができる。よって、システムの安全性は向上する。また、サービス利用の際は、サービス利用装置から個人情報認証装置にアクセスする必要がないので、サービス提供システム内で同時に大勢の利用者がサービス提供を求めることがあっても、個人情報認証装置に過大な負荷がかかることはない。よって、稼働中のサービス提供システムの安定性及び信頼性は向上する。

【００７５】

更に言えば、従来のサービス提供システムでは、サービス利用装置はサービス提供を受ける度に認証センターにアクセスするため、認証センターは、どの利用者がどのサービス提供装置をどの程度の頻度で利用しているかなど（サービス利用者の嗜好、サービス提供業者の売上実績など）の情報を収集できる立場にある。本実施の形態のサービス提供システムでは、サービス提供を受けようとするサービス利用装置は認証センターにアクセスする必要がないので、利用者や業者は、これら情報が認証センター経由で外部に漏れるのではという不安がなくなる。

【００７６】

また、ここで前記情報記憶管理手段は、前記署名付き個人情報を外部からのアクセスから保護された状態で記憶し、予め設定されたキー情報が入力された場合に限り前記署名付き

個人情報の読み出しを許すこと、としてもよい。
この構成によれば、サービス利用者の手元にあるサービス利用装置に保存された署名付き個人情報を、サービス利用者以外の者が外部から不正に読み出し悪用することは困難である。よって、署名付き個人情報の信頼性は従来に劣らない。なお、具体的には、前記キー情報は、パスワードまたは生体情報である、とすることができる。

【００７７】
さらに、前記情報記憶管理手段は、前記署名付き個人情報を暗号化するための暗号鍵、及び、暗号化された署名付き個人情報を復号するための復号鍵を生成する鍵生成手段と、前記復号鍵を格納する鍵格納手段と、前記署名付き個人情報を、前記暗号鍵を用いて暗号化する暗号化手段と、前記暗号化手段によって暗号化された署名付き個人情報を格納する情報格納手段と、前記情報格納手段から前記暗号化された署名付き個人情報を、前記鍵格納手段から読み出した前記復号鍵を用いて復号する復号手段と、からなることとしてもよい。

【００７８】
この構成によれば、サービス利用装置に保存された署名付き個人情報の信頼性は更に高まる。署名付き個人情報は暗号化されており、しかも復号のための鍵は保護領域に格納されているためである。加えて、保護領域にはデータ量の小さい鍵のみが格納されるので、本発明における記憶媒体は、記憶領域全体における保護領域の占める割合が小さい安価な媒体によって実現できる。具体的には、前記情報記憶管理手段は、外部からのアクセスから保護された保護記憶領域と、外部からのアクセスが可能な一般記憶領域と、プログラムを実行する演算装置とを有する、ＩＣメモリカードで成り、前記暗号化手段及び前記復号化手段はそれぞれ、前記保護記憶領域に格納されたプログラムが前記演算装置によって実行されることで実現されるものであり、前記鍵格納手段は前記保護記憶領域内に前記復号鍵を格納し、前記情報格納手段は前記一般記憶領域内に前記暗号化された署名付き個人情報を格納すること、とすればよい。

【００７９】
また、署名付き個人情報の信頼性を保証するためには、前記サービス提供装置における前記受付手段が、前記サービス利用装置から署名付き個人情報を受信するのに先立って、個人情報要求を前記サービス利用装置に送信し、前記サービス利用装置における前記サービス要求手段は、署名付き個人情報の送信開始に先立って前記個人情報要求を受信し、受信した前記個人情報要求が所定の条件を満たす場合にのみ前記サービス提供装置に署名付き個人情報を送信すること、とすることもできる。

【００８０】
この構成によれば、署名付き個人情報が、サービス提供業者に送信される場面で、サービス提供業者に成りすました悪意の第三者に不正取得されることを防止できる。よって、システム内での署名付き個人情報の信頼性は高まる。なお、具体的には、前記個人情報要求は予め定められた形式で生成され、前記個人情報認証装置によって認証のうえ専用の要求用電子署名が付加されており、前記サービス要求手段は、前記要求用電子署名を予め前記個人情報認証装置から配布された要求署名用公開鍵を用いて検証し、要求用電子署名が正当なものであった場合に、前記個人情報要求が前記所定の条件を満たすと判断することとする。すなわち、予め個人情報が認証されるのと同様に、個人情報要求の内容も予め個人情報認証装置による認証を受けておく。

【００８１】
また、電子署名については、前記利用者個人情報は複数の項目データからなり、前記個人情報認証装置における前記署名付き情報生成手段は、項目データの各々に対して電子署名を付加し、前記サービス提供装置における前記検証手段は、前記項目データの各々について署名の検証を行うこと、としてもよい。これによれば、項目単位で厳密な署名チェックが可能となる。

【００８２】
また、前記利用者個人情報は複数の項目データからなり、前記個人情報認証装置におけ

る前記署名付き情報生成手段は、項目データの各々に対して利用者毎にユニークな利用者ＩＤを付加したうえで、前記利用者個人情報に電子署名を付加し、前記サービス提供装置における前記検証手段は、前記受付手段が受け付けた署名付き個人情報の項目データの各々に付加された利用者ＩＤが同一であるか検証し、同一でない場合は、前記署名付き個人情報は正当でないと判定すること、としてもよい。

【００８３】

この構成は、悪意のあるサービス利用者が、自身に関する署名付き個人情報を改ざんして不正にサービスを受ける、といった事態を防止する。例えば、２人のサービス利用者がそれぞれの署名付き個人情報の一部ずつをつなぎあわせて、存在しない人物の署名付き個人情報を生成する場合などである。この場合、作られた個人情報の各項目には正しい署名が付加されているが、項目間でＩＤの不統一があるため、サービス提供業者は不正な情報であることを認識できる。さらに、具体的には、前記個人情報認証装置における前記署名付き情報生成手段は、前記利用者ＩＤを付加した項目データの各々に対して、各項目データの内容と前記利用者ＩＤ番号とから生成した電子署名を付加し、前記サービス提供装置における前記検証手段は、項目データ毎に電子署名に基づく正当性の判定を行うこと、としてもよい。

【００８４】

また、前記サービス利用装置は、身元認証用の公開鍵及び秘密鍵のペアを生成する身元認証用鍵生成手段と、前記身元認証用鍵生成手段が生成した前記身元認証用秘密鍵を、外部からのアクセスを制限した形で保持する秘密鍵保持手段と、を更に有し、前記署名付き情報取得手段は、前記身元認証用鍵生成手段が生成した前記身元認証用秘密鍵を前記個人情報認証装置に送信する利用者個人情報に含め、前記サービス要求手段は、前記サービス提供装置に送信する署名付き個人情報に、前記身元認証用秘密鍵を含め、前記サービス提供装置における検証手段は、前記前記サービス要求手段から送信されてくる署名付き個人情報の前記身元認証用秘密鍵を参照しながら、公開鍵暗号方式による身元認証を行い、身元の正当性が認証された場合に当該署名付き個人情報を正当と判定すること、としてもよい。

【００８５】

この構成によれば、サービス利用装置からサービス提供装置へ署名付き個人情報が送信される際には送信元の身元認証が行われる。そのため、送信サービス利用装置からサービス提供装置へ送信された署名付き個人情報送信が盗聴されても、この盗聴を行ったものが盗聴した個人情報を用いて不正にサービスを受けることはできない。よって、署名付き個人情報の信頼性はさらに高くなる。さらに、具体的には、前記秘密鍵保持手段は外部からのアクセスが制限される保護記憶領域を有する記憶媒体であり、前記身元認証用秘密鍵を前記保護記憶領域に格納すること、としてもよい。

【００８６】

また、上に述べた効果は、上記サービス提供システムで順次実行される処理に相当するステップを有するサービス提供方法、並びに、当該サービス提供方法をコンピュータシステムに実行させるプログラムによっても達成できる。また、サービス提供システムを構成する個人情報認証装置、サービス提供装置、サービス利用装置（及び、これが有する情報管理装置）単独でも、一部の効果を達成できる。

【図面の簡単な説明】

【図１】本発明に関わるサービス提供システムの実施の形態における全体的な構成を示すブロック図である。

【図２】同実施の形態における個人情報認証手続きの流れを示す図である。

【図３】同実施の形態における認証前の個人情報の構成例を示す図である。

【図４】同実施の形態における署名付き個人情報の構成例を示す図である。

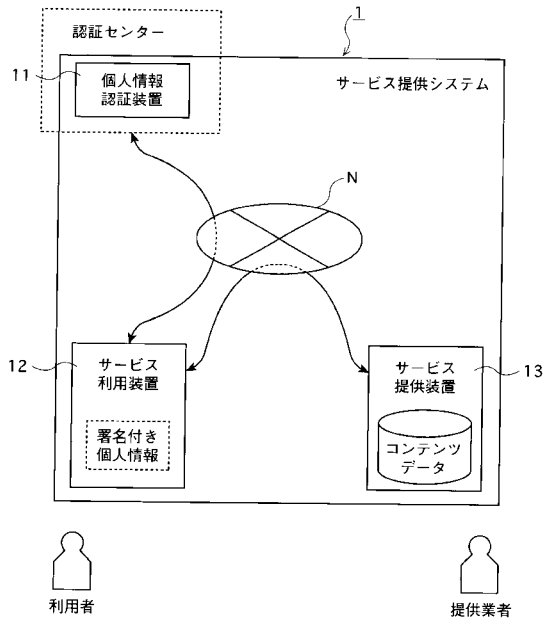
【図５】同実施の形態におけるサービス利用手続きの流れを示す図である。

【図６】同実施の形態における部分個人情報の構成例を示す図である。

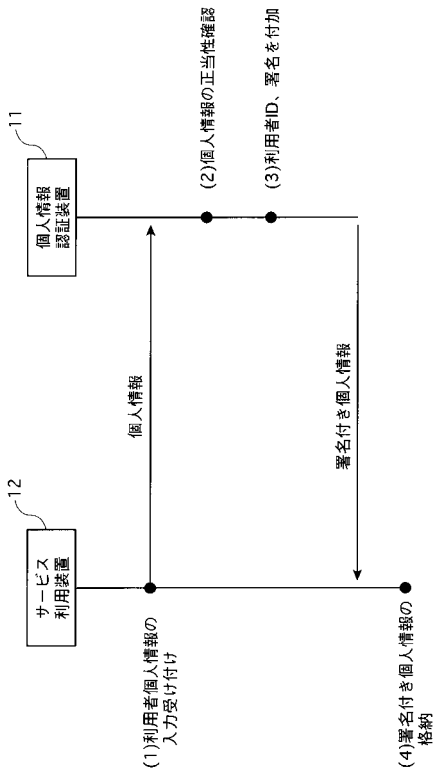
【図７】同実施の形態における個人情報認証装置の構成を示すブロック図である。

【図８】同実施の形態におけるサービス利用装置の構成を示すブロック図である。
【図９】同実施の形態においてサービス利用装置が有するメモリカードの構成を示すブロック図である。
【図１０】同実施の形態におけるサービス提供装置の構成を示すブロック図である。
【図１１】同実施の形態の変形例における個人情報認証手続きの流れを示す図である。
【図１２】同変形例における認証前後の個人情報を示す図である。
【図１３】同変形例におけるサービス利用手続きの流れを示す図である。
【符号の説明】
１　サービス提供システム
１１　個人情報認証装置
１１１　認証装置送受信部
１１２　個人情報確認部
１１３　署名生成部
１２　サービス利用装置
１２１　利用装置送受信部
１２２　メモリカード制御部
１２３　メモリカード
１２４　保護記憶領域
１２５　一般記憶領域
１２６　暗号化／復号部
１２７　鍵生成部
１２８　鍵記憶領域
１３　サービス提供装置
１３１　提供装置送受信部
１３２　署名確認部

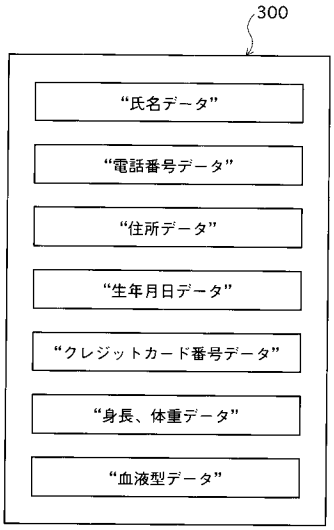
【図１】



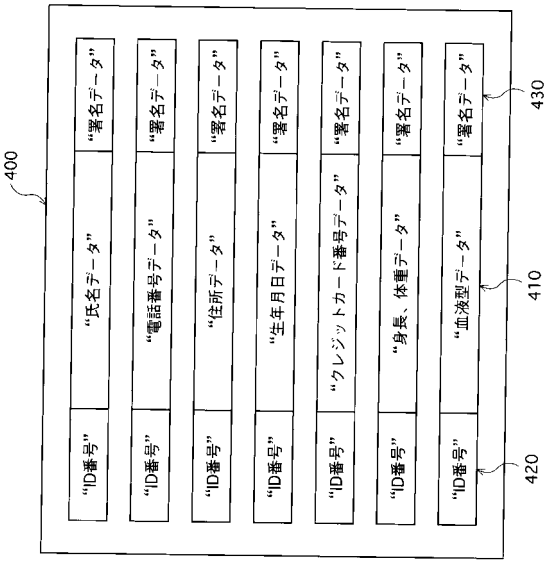
【図２】



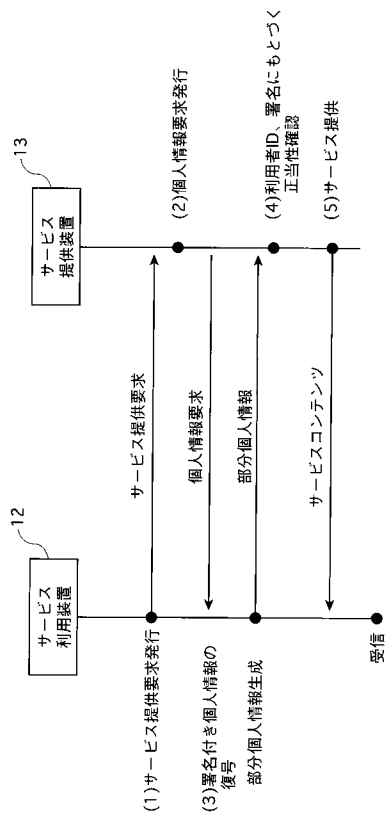
【図３】


300
“氏名データ”
“電話番号データ”
“住所データ”
“生年月日データ”
“クレジットカード番号データ”
“身長、体重データ”
“血液型データ”

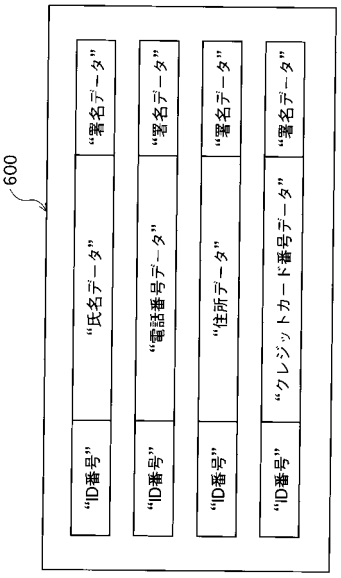
【図４】


400
“ID番号”
“氏名データ”
“署名データ”
“電話番号データ”
“住所データ”
“生年月日データ”
“クレジットカード番号データ”
“身長、体重データ”
“血液型データ”
410
420
430

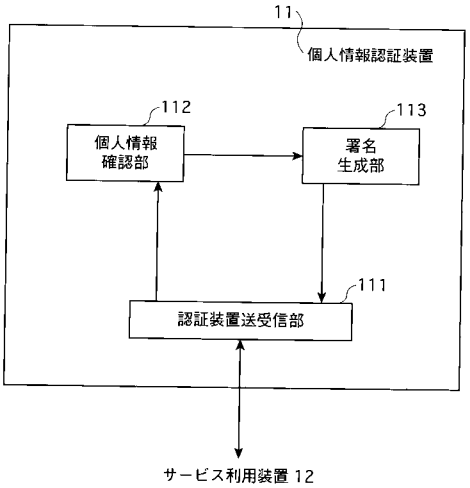
【図５】


12
サービス利用装置
13
サービス提供装置
(1)サービス提供要求発行
(2)個人情報要求発行
(3)署名付き個人情報の復号
部分個人情報生成
(4)利用者ID、署名にもとづく正当性確認
(5)サービス提供
サービス提供要求
個人情報要求
部分個人情報
サービスコンテンツ
受信

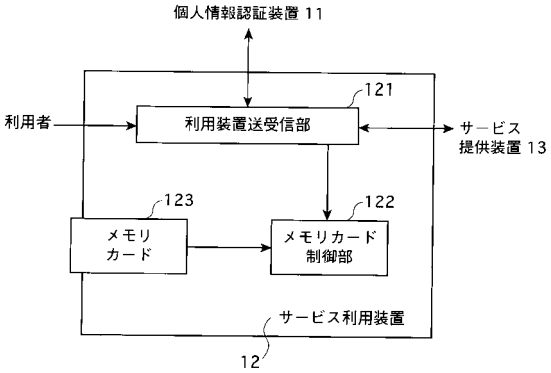
【図６】


600
“ID番号”
“氏名データ”
“署名データ”
“電話番号データ”
“住所データ”
“クレジットカード番号データ”

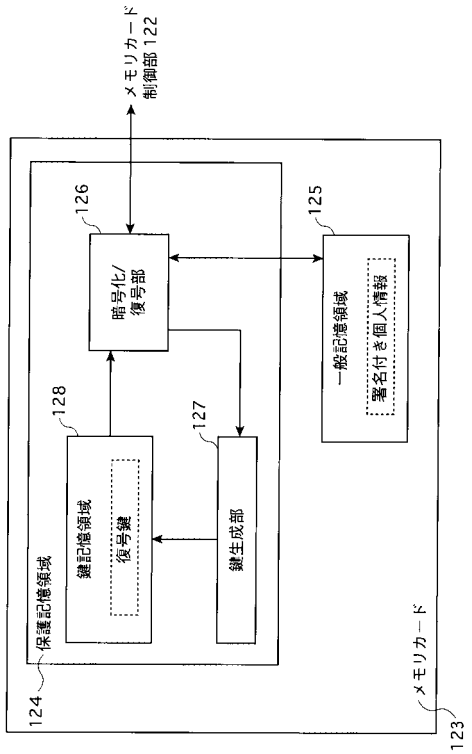
【図７】


11
個人情報認証装置
112
個人情報
確認部
113
署名
生成部
111
認証装置送受信部
サービス利用装置 12

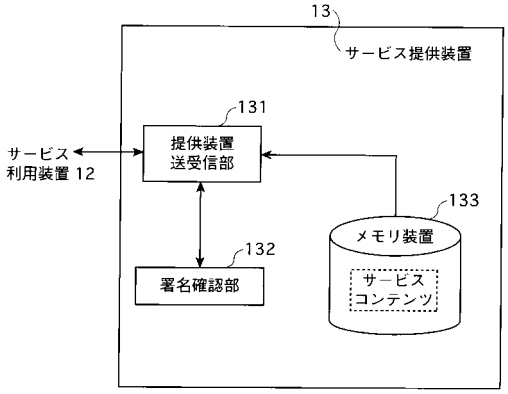
【図８】


個人情報認証装置 11
121
利用者
利用装置送受信部
サービス
提供装置 13
123
122
メモリ
カード
メモリカード
制御部
サービス利用装置
12

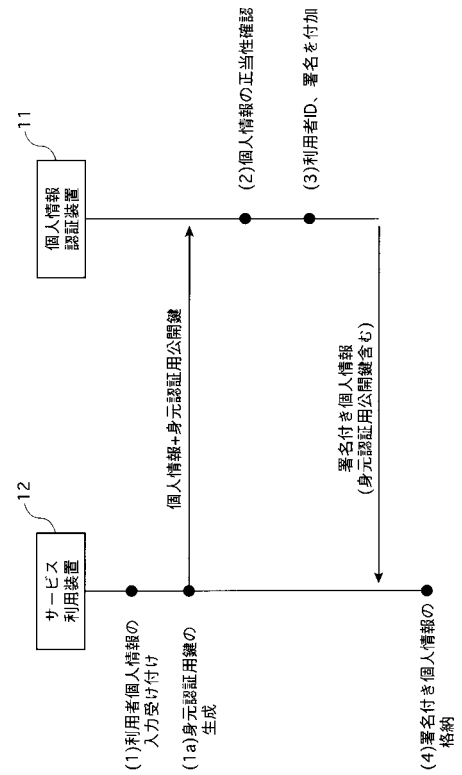
【図９】


メモリカード
制御部 122
126
125
暗号化/
復号部
一般記憶領域
署名付き個人情報
128
127
鍵記憶領域
復号鍵
鍵生成部
保護記憶領域
124
メモリカード
123

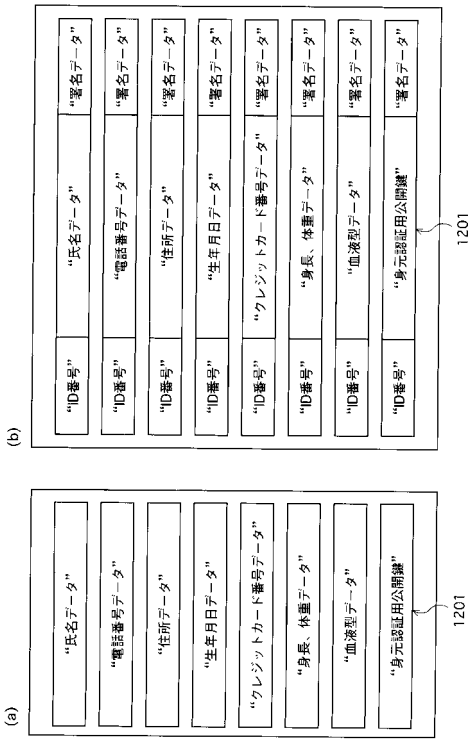
【図１０】


13
サービス提供装置
131
サービス
利用装置 12
提供装置
送受信部
133
メモリ装置
132
署名確認部
サービス
コンテンツ

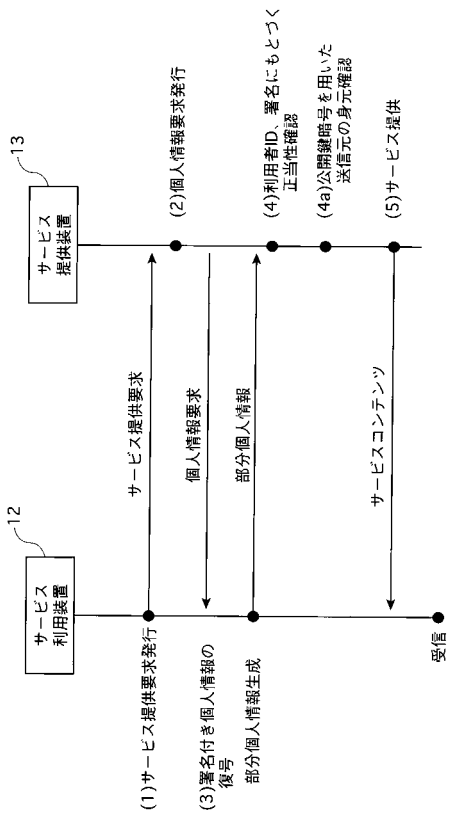
【図１１】


11
個人情報
認証装置
12
サービス
利用装置
(1)利用者個人情報の
入力受け付け
(1a)身元認証用鍵の
生成
個人情報+身元認証用公開鍵
(2)個人情報の正当性確認
(3)利用者ID、署名を付加
署名付き個人情報
(身元認証用公開鍵含む)
(4)署名付き個人情報の
格納

【図１２】


(a)
"氏名データ"
"電話番号データ"
"住所データ"
"生年月日データ"
"クレジットカード番号データ"
"身長、体重データ"
"血液型データ"
"身元認証用公開鍵"
1201
(b)
"ID番号"
"氏名データ"
"署名データ"
"電話番号データ"
"生年月日データ"
"クレジットカード番号データ"
"身長、体重データ"
"血液型データ"
"身元認証用公開鍵"
1201

【図１３】


12
サービス
利用装置
13
サービス
提供装置
(1)サービス提供要求発行
(3)署名付き個人情報の
復号
部分個人情報生成
サービス提供要求
個人情報要求
部分個人情報
(2)個人情報要求発行
(4)利用者ID、署名にもとづく
正当性確認
(4a)公開鍵暗号を用いた
送信元の身元確認
(5)サービス提供
サービスコンテンツ
受信

フロントページの続き

審査官　松平　英

(56)参考文献　特開平１０－１３５９４３（ＪＰ，Ａ）
特開平１０－２７４９２７（ＪＰ，Ａ）
特開２００１－２５６４１３（ＪＰ，Ａ）
特開２００１－２４９９０１（ＪＰ，Ａ）
特開平１０－０５６４４７（ＪＰ，Ａ）
特開平１１－０２４９１６（ＪＰ，Ａ）
特開平１１－０３１１３０（ＪＰ，Ａ）
特開２００１－１１７８２３（ＪＰ，Ａ）
特開２００３－２１８８６４（ＪＰ，Ａ）
特開平０３－０７３０６５（ＪＰ，Ａ）
櫻井　三子他，インターネットにおける認証技術，ＮＥＣ技報，日本，株式会社ＮＥＣクリエイティブ，１９９８年　9月２５日，第５１巻，第9号，ｐ．１０５～１１２
ウォーウィック・フォード他，ディジタル署名と暗号技術　第２版　安全な電子商取引のためのＰＫＩ（公開鍵基盤），セキュリティシステム，法律基盤，日本，株式会社ピアソン・エデュケーション，２００１年１０月１０日，第2版，ｐ．１６２～１６３，１８５～１８６

(58)調査した分野(Int.Cl.，ＤＢ名)
G09C　1/00
H04L　9/00
G06F　12/14
G06F　15/00