

明 細 書

発明の名称：

情報管理システム、認証デバイスおよび個人情報サーバ

技術分野

[0001] 本発明の実施形態は、情報管理システム、認証デバイスおよび個人情報サーバに関する。

背景技術

[0002] 近年、自己主権型アイデンティティのシステムが検討されている。自己主権型アイデンティティのシステムは、従来の中央集権型のデータ管理から個人がデータを管理する概念に基づくシステムである。自己主権型アイデンティティのシステムは、スマートフォンのようなモバイルデバイスあるいはパーソナルコンピュータ（PC）などを利用して、個人の資格情報を受け取り提供したりすることを想定している。

[0003] 従来の中央集権型のシステムでは、データをプラットフォーム提供者が一括管理するため、一括管理するデータに対するセキュリティ攻撃が発生した場合の大人数の個人情報漏洩したり第三者による大規模なデータの不正利用が発生したりするなどのプライバシーおよびデータ保護の観点で大きなリスクを持つ。これに対して、自己主権型アイデンティティのシステムでは、情報を分散管理し、個人がデータの取り扱いを行い、かつ、信頼できる相手との1対1でのデータの受け渡しなどを行うことによりデータの保護に関するリスクを低減することが期待される。

[0004] しかしながら、高齢者などの個人は、スマートフォンやPCなどの情報機器の操作に不慣れなことが多い。このような情報機器の利用に不慣れな個人は、自己主権型アイデンティティのシステムを用いて自分のデータを管理することは難しいと考えられる。このため、自己主権型アイデンティティのシステムを実現するには、わかりやすいユーザインターフェースなどを用いた運用が必要であると考えられる。さらに、自己主権型アイデンティティのシ

ステムでは、秘密鍵などの情報を利用者自身が安全に管理および保管する必要がある。利用者自身が安全に情報を保管する運用を想定すると、利用者自身が所持するスマートフォンやPCでは、コンピュータウイルスなどの攻撃による鍵の漏洩などが懸念されるという問題がある。

先行技術文献

特許文献

[0005] 特許文献1：日本国特開2001-312477号公報

発明の概要

発明が解決しようとする課題

[0006] 上記した課題を解決するために、個人ごとに管理する情報を複雑な操作なしで安全に運用することができる情報管理システム、認証デバイスおよび個人情報サーバを提供する。

課題を解決するための手段

[0007] 実施形態によれば、情報管理システムは、認証デバイスと個人情報サーバとを有する。認証デバイスは、センサとメモリとインターフェースと第1プロセッサとを有する。個人情報サーバは、通信部とデータメモリと第2プロセッサとを有する。センサは、人物の生体情報を取得する。メモリは、所持者の生体情報を記憶する。インターフェースは、端末装置と接続する。第1プロセッサは、センサが取得する生体情報とメモリが記憶する生体情報との生体照合が成功した場合に個人情報サーバの場所を示す情報を端末装置へ出力する。通信部は、端末装置と通信する。データメモリは、認証デバイスの所持者の個人情報を保管する。第2プロセッサは、認証デバイスが接続された端末装置からの要求に応じてデータメモリが保管する認証デバイスの所持者の個人情報を端末装置へ供給する。

図面の簡単な説明

[0008] [図1]図1は、実施形態に係る情報管理システムで利用する認証デバイスとしてのICカードを発行するためのシステム構成例を示す図である。

[図2]図2は、実施形態に係る情報管理システムで利用する認証デバイスとしてのICカードの構成例を示すブロック図である。

[図3]図3は、実施形態に係る情報管理システムで利用する認証デバイスとしてのICカードを発行するための登録装置の構成例を示すブロック図である。

[図4]図4は、実施形態に係る情報管理システムで利用する認証デバイスとしてのICカードを発行する発行処理を説明するためのシーケンスである。

[図5]図5は、実施形態に係る情報管理システムが認証デバイスとしてのICカードの所持者の情報を提供するためのシステム構成例を示す図である。

[図6]図6は、実施形態に係る情報管理システムにおけるICカードの所持者のリポジトリである個人情報サーバの構成例を示すブロック図である。

[図7]図7は、実施形態に係る情報管理システムにおいてICカードと個人情報サーバと窓口端末との認証手続きを説明するためのシーケンスである。

[図8]図8は、実施形態に係る情報管理システムが窓口端末に個人情報サーバが保管するICカードの所持者の情報を提供する処理を説明するためのシーケンスである。

[図9]図9は、実施形態に係る情報管理システムが窓口端末からの情報をICカードの所持者のリポジトリである個人情報サーバに保管する処理を説明するためのシーケンスである。

実施形態

[0009] 以下、実施形態について、図面を参照しつつ説明する。

まず、実施形態に係る情報管理システムに用いる認証デバイスの発行（登録）手続きについて説明する。

図1は、実施形態に係る情報管理システムに利用可能な認証デバイスとしてのICカード2を発行（登録）するためのシステム構成例を模式的に示す図である。

図1に示す構成例において、情報管理システムは、端末（ユーザ端末）1、ICカード2、登録装置3、および、個人情報サーバ4などを有する。

- [0010] ICカード2は、生体認証を実行する機能を有する認証デバイスの一例である。認証デバイスとしてのICカード2は、個々の個人ごとに発行され、所持者本人であることを生体情報によって認証する機能を有する。
- [0011] 認証デバイスとしてのICカード2は、人物から取得する認証情報としての生体情報を取得するための生体センサ20を備える。本実施形態において、認証デバイスとしてのICカード2は、生体センサ20として、生体情報の一例である指紋を読み取る指紋センサを備える指紋認証カード（指紋センサカード）であるものとして説明する。ICカード2は、指紋センサ（生体センサ）20が読み取る指紋とICカード2内のメモリに予め登録されている所持者（登録者）の指紋とを照合することにより本人確認としての指紋認証（生体認証）を実行する。
- [0012] なお、実施形態に係る認証デバイスは、指紋センサを備えるICカードである指紋センサカードに限定されるものではない。例えば、認証デバイスは、指紋以外の生体情報によって生体認証を行う携帯可能電子装置であっても良いし、スマートフォンなどのハードウェアであっても良い。
- [0013] 本実施形態において、ICカード2を所持する所持者は、本人の個人情報および資格情報などの情報を管理する個人情報サーバ4を持っているものとする。個人情報サーバ4は、リポジトリと呼ばれる。個人情報サーバ4は、個人ごとに情報を分散管理し、各個人がデータの取り扱いを行う自己主権型アイデンティティのシステムを構成するものである。自己主権型アイデンティティのシステムは、データをプラットフォーム提供者が一括管理する中央集権型のデータ管理システムとは異なり、個人ごとの個人情報サーバ4が分散管理する個人の資格情報などのデータを認証デバイスによる個人認証を利用してセキュアに受け渡しすることによりデータのプライバシー保護を向上させる。
- [0014] 個人情報サーバ4は、資格情報などの個人情報を管理する対象者となるICカード2の所持者ごとに設けられる。個人情報サーバ4は、ICカード2の所持者に関する情報として資格情報などの個人情報を保管する。個人情報

サーバ4は、認証デバイスとしてのICカード2との相互認証によって当該ICカード2とセキュアに通信する機能を有する。ICカード2の所持者のリポジトリである個人情報サーバ4は、ネットワークに接続される。個人情報サーバは、URLなどのネットワーク上におけるアドレスによって場所（サーバの場所）が示される。

[0015] 端末1は、認証デバイスとしてのICカード2と通信するカードインターフェースと登録装置3と通信するネットワークインターフェースとを備える情報処理装置である。端末1は、ICカードと登録装置3との通信を仲介できるものであれば良い。また、端末1は、ICカード2と通信するカードインターフェース（カードリーダライタ）を備える装置に限定されるものではなく、外部機器としてのカードリーダライタに接続するためのインターフェースを備えるものであっても良い。端末1は、例えば、ユーザ自身が操作するスマートフォン、タブレットPC、パーソナルコンピュータ（PC）などのユーザ端末であるものとする。

[0016] 登録装置3は、ネットワークを介して外部装置と通信する機能を有し、個人の情報が登録されたHSM（ハードウェアセキュリティモジュール：Hardware Security Module）3Aを管理する装置である。登録装置3は、例えば、公的機関が運用するサーバであり、公的機関で管理する各個人の生体（指紋）情報とリポジトリのURL（アドレスなどのサーバの場所）とを含む個人情報を保存するHSM3Aを管理する。

[0017] HSM3Aは、セキュアに情報を保存するデバイスである。また、本実施形態において、HSM3Aは、保存している登録済みの指紋情報と端末1および登録装置3を介して与えられるICカード2が取得する指紋情報との指紋照合（生体認証）を行う機能を有する。さらに、HSM3Aは、秘密鍵と公開鍵との鍵ペアを生成し、秘密鍵をセキュアに保存する機能を有する。

[0018] 次に、実施形態に係る認証デバイスとしてのICカード2における制御系の構成について説明する。

図2は、実施形態に係る認証デバイスとしてのICカード2の構成例を示

すブロック図である。

ＩＣカード２は、外部装置から供給される電力により活性化する（動作可能な状態になる）認証デバイスである。ＩＣカード２は、スマートカードとも称される。図２に示すように、ＩＣカード２は、本体Ｃを有する。本体Ｃは、プラスチックなどによりカード状に形成される。ＩＣカード２の本体Ｃ内には、制御モジュールＭが埋設される。制御モジュールＭは、１つ又は複数のＩＣチップに通信インターフェースが接続された状態で一体的に形成される。

[0019] 図２に示す構成例において、制御モジュールＭは、プロセッサ２１、ＲＯＭ２２、ＲＡＭ２３、データメモリ２４および通信インターフェース２５を有する。また、ＩＣカード２の本体Ｃ内において、制御モジュールＭには、表示器２６および生体センサとしての指紋センサ２０が接続される。

[0020] プロセッサ２１は、種々の処理を実行する回路を含む。プロセッサ２１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。プロセッサ２１は、ＩＣカード２全体の制御を司る。プロセッサ２１は、ＲＯＭ２２あるいはデータメモリ２４に記憶されているプログラムを実行することにより、種々の処理機能を実現する。ただし、後述するプロセッサ２１が実行する各種の機能のうち一部又は全部は、ハードウェア回路により実現されるようにしても良い。

[0021] ＲＯＭ２２は、プログラムメモリとして機能する不揮発性のメモリである。ＲＯＭ２２は、予め制御用のプログラムおよび制御データなどが記憶される。ＲＯＭ２２は、製造段階で制御プログラムや制御データなどが記憶された状態でＩＣカード２内に組み込まれるものである。ＲＯＭ２２に記憶される制御プログラムや制御データは、予め当該ＩＣカード２の仕様に応じて組み込まれる。例えば、ＲＯＭ２２には、外部装置（カードリーダーライター）から受信するコマンドに応じた処理をプロセッサ２１が実行するためのプログラムが記憶される。

[0022] ＲＡＭ２３は、ワーキングメモリとして機能する揮発性のメモリである。

また、RAM 23は、プロセッサ21が処理中のデータなどを一時保管するバッファとしても機能する。例えば、RAM 23は、通信インターフェース25を介して外部装置との間で送受信するデータを一時保管する通信バッファとして機能する。

[0023] データメモリ24は、データの書き込みおよび書換えが可能な不揮発性のメモリである。データメモリ24は、例えば、EEPROM（登録商標）（Electrically Erasable Programmable Read Only Memory）などで構成する。データメモリ24には、当該ICカード2の運用用途に応じたプログラムや種々のデータが書き込まれる。データメモリ24には、プログラムファイルあるいはデータファイルなどが定義され、それらのファイルに制御プログラムや種々のデータが書き込まれる。データメモリ24は、一部又は全部の領域が耐タンパ性を有し、セキュアにデータが格納できる。例えば、データメモリ24におけるセキュアにデータを記憶できる記憶領域には、鍵情報などの情報が記憶される。

[0024] データメモリ24は、当該ICカード2の所持者の生体情報を記憶する記憶領域24aを有する。ICカード2が指紋を用いた生体情報を行う指紋センサカードである場合、ICカード2の記憶領域24aには、所持者であるユーザの生体情報としての指紋情報が書き込まれる。以下に説明する本実施形態では、ICカード2は、データメモリ24の記憶領域24aに所持者本人の生体情報としての指紋情報が書き込まれた状態でユーザが所持しているものであることを前提とする。

[0025] 通信インターフェース25は、通信制御部とインターフェース部とを有し、通信部を構成する。通信インターフェース25は、端末1および窓口端末5（図5参照）などの端末装置が備えるカードインターフェース（カードリーダーライター）又は端末装置とインターフェースを介して接続されるカードリーダーライターと通信接続するためのインターフェースである。通信インターフェース25は、端末装置（端末1および窓口端末5）が備えるカードインタ

ーフェースに対応した通信方式による通信機能を実現する。また、通信インターフェース 25 は、複数の通信方式（例えば、接触通信と非接触通信）をサポートするものとして構成しても良い。

[0026] 当該 IC カード 2 が非接触型の IC カードとして実現される場合、通信インターフェース 25 は、端末装置が備えるカードインターフェース又は端末装置とインターフェースを介して接続されるカードリーダーライター（RW）と非接触（無線）で通信する通信部を構成する。この場合、通信インターフェース 25 は、電波の送受信を行うアンテナを備え、アンテナから送信する電波を生成するための変調回路およびアンテナが受信した電波から信号を生成するための復調回路などにより構成される。

[0027] また、当該 IC カード 2 が接触型の IC カードとして実現される場合、通信インターフェース 25 は、端末装置が備えるカードインターフェース又は端末装置とインターフェースを介して接続されるカード RW と接触して通信する通信部を構成する。この場合、通信インターフェース 25 は、カード RW に設けられたコンタクト部と物理的かつ電氣的に接触するコンタクト部を備え、コンタクト部を介した信号の送受信を制御する通信制御回路などにより構成される。

[0028] 生体センサ 20 は、認証情報を取得する認証情報取得部の一例である。生体センサ 20 は、認証処理に用いる認証情報として人物の生体情報を取得するセンサである。本実施形態において、生体センサ 20 は、利用者の指紋情報（指紋画像）を読み取る指紋センサであるものとする。生体センサとしての指紋センサ 20 は、指紋を読み取るセンサがカード本体 C の表面に露出するように設けられ、露出したセンサ部分に翳された人物の指の指紋を読み取る。指紋センサ 20 が読み取る指紋情報が、データメモリ 24 の記憶領域 24a に記憶されている指紋情報と照合されることで指紋照合が実行される。

[0029] なお、生体センサ 20 は、指紋センサに限定されるものではなく、指紋以外の生体情報（例えば、掌紋、静脈、虹彩等）を取得するセンサであっても良い。指紋以外の生体情報を取得するセンサを備える場合、IC カード 2 は

、センサが取得する生体情報に対応した生体認証を行う機能（例えば、掌紋照合、静脈照合、虹彩照合等を実行するＩＣチップ）を備えるようにすれば良い。

[0030] 次に、実施形態に係る情報管理システムに利用する認証デバイスとしてのＩＣカード２を発行（登録）するための登録装置３の構成について説明する。

図３は、実施形態に係る発行システムにおける登録装置３の構成例を示すブロック図である。

図３に示すように、登録装置３は、プロセッサ３１、ＲＯＭ３２、ＲＡＭ３３、データメモリ３４、通信部３５、および、インターフェース３６を有する。

[0031] プロセッサ３１は、プログラムを実行することにより各種の処理を実行する。プロセッサ３１は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）である。プロセッサ３１は、システムバスを介して登録装置３内の各部と接続され、各部との間でデータを送受信する。プロセッサ３１は、ＲＯＭ３２およびＲＡＭ３３と協働して登録装置３における制御およびデータ処理などの動作を実行する。

[0032] ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）３２は、登録装置３の基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）３３は、データを一時的に記憶する揮発性のメモリである。ＲＡＭ３３は、プロセッサ３１がプログラムを実行する場合にワーキングメモリとして機能する。

[0033] データメモリ３４は、各種のデータを記憶する記憶部である。データメモリ３４は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ３４は、ＯＳプログラム、アプリケーションプログラム、動作設定情報などを記憶する。

[0034] 通信部３５は、外部装置と通信するための通信インターフェースである。

通信部 35 は、無線で通信を行うものであって良いし、有線で通信を行うものであって良い。本実施形態において、通信部 35 は、インターネットなどの広域のネットワークを介して、ユーザが使用する端末 1 と通信する。プロセッサ 31 は、通信部 35 により端末 1 を介して IC カード 2 とのセキュアな通信を実行する。

[0035] インターフェース 36 は、HSM 3A にアクセスするためのインターフェースである。インターフェース 36 は、HSM 3A が備えるインターフェース規格に対応したものであれば良い。ここで、HSM 3A は、インターフェース 36 を介して接続される登録装置 3 に接続される装置であっても良い。

[0036] HSM 3A は、IC カード 2 の所持者の生体情報としての指紋情報とリボジトリのアドレス (URL) とを含む情報をセキュアに保存する。また、HSM 3A は、登録装置 3 から入力される生体情報と保存している生体情報との生体照合を実行し、その生体照合結果を出力する機能を有する。HSM 3A は、保存している生体情報を外部に出力することなく生体照合を行えるためセキュアに生体照合を実現できる。

[0037] 次に、本実施形態に係る情報管理システムで利用する IC カード 2 を発行 (登録) するための発行処理について説明する。

図 4 は、認証デバイスとしての IC カード 2 を情報管理システムで利用可能な IC カード 2 として発行 (登録) する発行処理の動作例を説明するためのシーケンスである。図 4 に示す動作例では、前提条件として、IC カード 2 が所持者本人の指紋情報を記憶し、HSM 3A が IC カード 2 の所持者に関する指紋情報とリボジトリの URL とを保管しているものとする。また、IC カード 2 と HSM 3A とは、端末 1 および登録装置 3 を介してセキュアに通信する機能を有するものとする。

[0038] IC カード 2 のプロセッサ 21 は、通信 I/F 25 により端末 1 に接続し、端末 1 のネットワーク通信機能により登録装置 3 と通信する。IC カード 2 のプロセッサ 21 は、端末 1 を介して登録装置 3 との通信状態が確立すると、IC カード 2 と HSM 3A との相互認証を実行する (ST11)。

- [0039] ICカード2とHSM3Aとの相互認証が成功すると、ICカード2のプロセッサ21は、データメモリ24の記憶領域24aに保存している当該ICカード2の所持者の指紋情報を登録装置3のHSM3Aへ送信する(ST12)。HSM3Aは、ICカード2から取得した指紋情報と保管している登録済みの指紋情報との指紋照合を実行する(ST13)。ICカード2から取得した指紋情報と登録済みの指紋情報との照合が成功した場合、HSM3Aは、登録装置3および端末1を介してICカード2に照合成功を通知する(ST14)。
- [0040] HSM3Aは、ICカード2から取得した指紋情報に対する指紋照合が成功した後、秘密鍵と公開鍵との鍵ペアを生成する(ST15)。鍵ペアを生成すると、HSM3Aは、生成した秘密鍵をセキュアに保存(登録)する(ST16)。秘密鍵を登録した後、HSM3Aは、公開鍵をICカード2へ送信する(ST19)。
- [0041] 一方、ICカード2のプロセッサ21は、指紋センサ20で読み取った指紋に対するHSM3Aにおける指紋照合が成功した旨の通知を受けた場合、秘密鍵と公開鍵との鍵ペアを生成する(ST17)。鍵ペアを生成すると、プロセッサ21は、生成した秘密鍵をデータメモリ24におけるセキュアな記憶領域に保存(登録)する(ST18)。秘密鍵を保存した後、プロセッサ21は、保存した秘密鍵に対応する公開鍵をHSM3Aへ送信する(ST19)。
- [0042] すなわち、相互認証が成功したICカード2とHSM3Aとは、ICカード2が取得する指紋情報とHSM3Aが保管する指紋情報との照合が成功した場合、それぞれが秘密鍵と公開鍵との鍵ペアを生成する。ICカード2とHSM3Aとは、自身が生成した秘密鍵を自身で保存し、それらの秘密鍵に対応する公開鍵を交換する。ICカード2とHSM3Aとは、それぞれが生成した鍵ペアを使用することによりデータの暗号化および検証が可能となる。
- [0043] HSM3Aは、ICカード2が生成した公開鍵を取得すると、秘密鍵を用

いてICカード2が生成した公開鍵と当該ICカード2の所持者のリポジトリのURLとに対して電子署名を行う(ST20)。電子署名付きの公開鍵とURLとを生成すると、HSM3Aは、生成した電子署名付きの公開鍵とURLとをICカード2へ送信する(ST21)。

[0044] ICカード2は、通信インターフェース25によりHSM3Aが生成した電子署名付きの公開鍵とURLとを受信する。ICカード2のプロセッサ21は、HSM3Aからの電子署名付きの公開鍵とURLとを受信した場合、HSM3Aによる電子署名付きの公開鍵とURLとをデータメモリ24に記憶する(ST22)。ICカード2のプロセッサ21は、HSM3Aが電子署名した当該ICカード2が生成した公開鍵を確認することにより自身が生成した公開鍵と共に受信したURL(所持者のリポジトリのURL)が正しいことを確認する。

[0045] 次に、実施形態に係る情報管理システムにおいてICカード2の所持者のリポジトリである個人情報サーバ4が保存する資格情報を提供する処理および個人情報サーバ4に資格情報を登録する処理について説明する。

図5は、実施形態に係る情報管理システムにおいてICカード2を用いて個人情報サーバ4が保持する情報を提供するためのシステム構成例を模式的に示す図である。

図5に示す構成例において、情報管理システムは、ICカード2、個人情報サーバ4および窓口端末5などを有する。

[0046] ICカード2は、図2に示すように、生体センサとしての指紋センサ20を備える構成を有する。図5に示すICカード2は、登録装置3による発行手続きによって発行された認証デバイスの一例であるものとする。ICカード2は、所持者本人であることが確認する生体認証としての指紋認証(指紋照合)機能を有し、所持者本人のリポジトリである個人情報サーバ4を示す情報を保持する認証デバイスである。

[0047] 窓口端末5は、認証デバイスとしてのICカード2と通信するカードインターフェースとネットワークを経由して個人情報サーバ4と通信するネット

ワークインターフェースとを備える情報処理装置である。窓口端末5は、ＩＣカード2と個人情報サーバ4との通信を仲介する機能を有する。窓口端末5は、利用者が提示するＩＣカード2をカードインターフェースに接続し、個人情報サーバ4が保持する当該ＩＣカード2の所持者に関する資格情報などの情報を取得する。例えば、窓口端末5は、個人情報サーバ4が保持するＩＣカード2の所持者の資格情報を取得し、所得した資格情報に基づいて当該人物に対する各種サービスの手続きを行う。また、窓口端末5は、ＩＣカード2の所持者に関する資格情報などの情報を個人情報サーバ4に登録する（書き込む）手続きを行うものであっても良い。例えば、窓口端末5は、ＩＣカード2の所持者に関する資格情報を当該人物のリポジトリである個人情報サーバ4に書き込むことを依頼する。

[0048] 個人情報サーバ4は、ＩＣカード2の所持者のリポジトリである。個人情報サーバ4は上述したように、ＩＣカード2を所持する所持者本人に関する情報（例えば、資格情報などの個人情報）の情報を管理する。個人情報サーバ4は、ＩＣカード2が接続された端末装置からの要求に応じて保管している当該ＩＣカード2の所持者の情報を提供する。また、個人情報サーバ4は、ＩＣカード2が接続された端末装置からの依頼に応じて新たな資格情報などの情報を当該ＩＣカード2の所持者の情報として登録（保存）する。

[0049] 図6は、実施形態に係る情報管理システムにおける個人情報サーバ4の構成例を示すブロック図である。

図6に示すように、個人情報サーバ4は、プロセッサ41、ＲＯＭ42、ＲＡＭ43、データメモリ44、および、通信部45を有する。

[0050] プロセッサ31は、プログラムを実行することにより各種の処理を実行する。プロセッサ31は、例えば、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓ　ｉｎｇ　Ｕｎｉｔ）である。プロセッサ31は、システムバスを介して個人情報サーバ4の各部との間でデータを送受信する。プロセッサ41は、ＲＯＭ42およびＲＡＭ43と協働して個人情報サーバ4における制御およびデータ処理などの動作を実行する。

[0051] ROM (Read Only Memory) 42は、個人情報サーバ4の基本的な動作を実現するためのプログラムおよび制御データなどを記憶する不揮発性のメモリである。

RAM (Random Access Memory) 43は、データを一時的に記憶する揮発性のメモリである。RAM43は、プロセッサ41がプログラムを実行する場合にワーキングメモリとして機能する。

[0052] データメモリ44は、各種のデータを記憶する記憶部である。データメモリ44は、データの書き換えが可能な不揮発性のメモリで構成される。例えば、データメモリ44は、OSプログラム、アプリケーションプログラム、動作設定情報などを記憶する。

[0053] 通信部45は、外部装置と通信するための通信インターフェースである。通信部45は、無線で通信を行うものであって良いし、有線で通信を行うものであっても良い。本実施形態において、通信部45は、インターネットなどの広域のネットワークを介して、窓口端末5と通信する。プロセッサ41は、通信部45により窓口端末5を介したICカード2とのセキュアな通信を実行する。

[0054] 次に、本実施形態に係る情報管理システムにおいてICカード2を用いて個人情報サーバ4が保持する情報を提供する情報提供処理について説明する。

図7および図8は、個人情報サーバ4が保持するICカード2の所持者の資格情報を窓口端末5へ提供する情報提供処理（読取処理）の動作例を説明するためのシーケンスである。

図7および図8に示す動作例の説明としては、ICカード2の所持者がサービス開始に必要な個人情報サーバ4が保管する資格情報をサービス提供者の窓口で係員が操作する窓口端末5に提示することを想定する。具体例としては、ICカード2の所持者が金融機関で口座を開設する場合に、口座開設に必要な個人情報サーバ4が保管する資格情報を金融機関の係員が操作する窓口端末5に提示することを想定する。

- [0055] サービスの開始手続きを受け付ける窓口の係員は、利用者から要求に応じてサービス開始の手続き開始を窓口端末5の操作部（図示しない）に指示入力し、利用者が所持する認証デバイスとしてのＩＣカード2を窓口端末5のＩＣカード用のインターフェース（図示しない）に提示させる。利用者がＩＣカード2を窓口端末5に提示すると、窓口端末5は、指紋照合コマンドをＩＣカード2に供給する（ＳＴ３１）。
- [0056] ＩＣカード2は、通信インターフェース25により窓口端末5からの指紋照合コマンドを受信する。指紋照合コマンドを受信すると、ＩＣカード2のプロセッサ21は、指紋センサ20により指紋を読み取り、指紋センサ20により読み取る指紋と記憶領域24aに保持している所持者本人の指紋とを照合する指紋照合を実行する（ＳＴ３２）。
- [0057] ＩＣカード2のプロセッサ21は、指紋照合コマンドに応じた指紋照合を実行すると、その指紋照合の結果を窓口端末5へ送信する。ここでは、ＩＣカード2における指紋照合が成功したものとする。指紋照合が成功すると、プロセッサ21は、指紋照合コマンドに対する応答として指紋照合が成功したことを窓口端末5へ通知する（ＳＴ３３）。
- [0058] 窓口端末5は、ＩＣカード2から指紋照合が成功した旨の通知を受信すると、指紋照合が成功したことを窓口端末5の表示部（図示しない）に表示する。これにより、窓口端末5を操作する係員は、ＩＣカード2を提示した人物がＩＣカード2の所持者本人であると確認する。係員は、ＩＣカード2の所持者本人であることを確認した後、窓口端末5の操作部によりＩＣカード2の所持者本人に関する情報の格納場所（リポジトリ）を示す情報の取得を指示する。窓口端末5は、操作指示に応じて当該ＩＣカード2に対して所持者本人のリポジトリを示す情報（ここでは、リポジトリのＵＲＬとする）の読み出しを要求する読み出しコマンドを供給する（ＳＴ３４）。
- [0059] ＩＣカード2は、通信インターフェース25により窓口端末5からのリポジトリのＵＲＬの読み出しを要求する読み出しコマンドを受信する。読み出しコマンドを受信すると、ＩＣカード2のプロセッサ21は、当該コマンド

で読み出しが指定されたりポジトリのURLをデータメモリ24から読み出す。プロセッサ21は、データメモリ24から読み出したリポジトリのURLをセットした読み出しコマンドに対するレスポンスデータを生成し、生成したレスポンスデータを窓口端末5へ送信する(ST35)。

[0060] 窓口端末5は、ICカード2からリポジトリのURLを含むレスポンスデータを受信すると、ICカード2から取得したリポジトリのURLにアクセスする。これにより、ICカード2の所持者のリポジトリである個人情報サーバ4と窓口端末5とはネットワークを介した通信を開始する。

[0061] 個人情報サーバ4のプロセッサ41は、通信部45により窓口端末5からのアクセスを受けて当該窓口端末5とのセッションを確立させる(ST36)。個人情報サーバ4のプロセッサ41は、窓口端末5とのセッションが確立すると、窓口端末5を識別する端末識別情報を窓口端末5から受信する(ST37)。

[0062] 窓口端末5の端末識別情報を受信すると、個人情報サーバ4のプロセッサ41は、受信した端末識別情報で指定される窓口端末5に接続されているICカード2との相互認証を実行する(ST38)。個人情報サーバ4とICカード2とは、ネットワークおよび窓口端末5を介して通信することによりお互いを認証する相互認証を行う。相互認証が成功すると、個人情報サーバ4のプロセッサ41とICカード2のプロセッサ21とは、窓口端末5を介したセキュアチャネルを確立させる(ST39)。

[0063] 個人情報サーバ4のプロセッサ41は、ICカード2とのセキュアチャネルが確立すると、窓口端末5の公開鍵を示す公開鍵IDを窓口端末5から取得する(ST40)。個人情報サーバ4のプロセッサ41は、窓口端末5の公開鍵IDを取得すると、公開鍵IDが示す窓口端末5の公開鍵を取得する(ST41)。窓口端末5の公開鍵を取得すると、個人情報サーバ4のプロセッサ41は、ICカード2に対して鍵ペアの生成を要求するコマンドを送信する(ST42)。

[0064] ICカード2は、窓口端末5を介して通信インターフェース25により個

個人情報サーバ4からの鍵ペアの生成を要求するコマンドを受信する。個人情報サーバ4からの鍵ペアの生成を要求するコマンドを受信した場合、ＩＣカード2のプロセッサ21は、秘密鍵と公開鍵との鍵ペアを生成する（ＳＴ43）。鍵ペアを生成すると、プロセッサ21は、生成した秘密鍵と公開鍵を示す公開鍵ＩＤとをデータメモリ24に記憶する（ＳＴ44）。

[0065] プロセッサ21は、少なくとも秘密鍵をデータメモリ24におけるセキュアなメモリ領域に保存する。秘密鍵と公開鍵ＩＤとを記憶した後、ＩＣカード2のプロセッサ41は、窓口端末5を介した個人情報サーバ4とのセキュアな通信によって公開鍵と公開鍵ＩＤとを個人情報サーバ4へ送信する（ＳＴ45）。

[0066] 個人情報サーバ4は、窓口端末5を介してＩＣカード2からの公開鍵と公開鍵ＩＤとを受信する。個人情報サーバ4のプロセッサ41は、ＩＣカード2から受信した公開鍵をデータメモリ44に記憶する（ＳＴ46）。ＩＣカード2の公開鍵を保存すると、個人情報サーバ4のプロセッサ41は、ＩＣカード2の公開鍵を示す公開鍵ＩＤを通信部45によりネットワークを経由して窓口端末5へ送信する（ＳＴ47）。

[0067] 窓口端末5は、個人情報サーバ4からＩＣカード2の公開鍵を示す公開鍵ＩＤを取得する（ＳＴ48）。これにより、窓口端末5は、個人情報サーバ4が公開するＩＣカード2の公開鍵を取得することができる。この状態において、窓口端末5は、個人情報サーバ4が管理する当該ＩＣカード2の所持者に関する情報が取得可能となる。

[0068] すなわち、ＩＣカードの公開鍵ＩＤを取得した後、窓口端末5は、当該ＩＣカード2の所持者に対して口座開設などのサービスの提供を開始するため、に当該人物に関する情報として取得すべき情報（資格情報）を特定する（ＳＴ51）。例えば、窓口端末5は、取得すべき資格情報を表示部に表示する。窓口の係員は、表示部に表示した取得すべき資格情報を確認して当該資格情報の取得を操作部によって指示する。窓口端末5は、取得すべき資格情報が特定されると、取得すべき資格情報を示す識別情報（資格情報識別子）を

含む読出し要求を個人情報サーバ4へ送信する（ST52）。

[0069] 個人情報サーバ4は、通信部45によりICカード2の所持者の資格情報の読出し要求を窓口端末5から受信する（ST53）。個人情報サーバ4のプロセッサ41は、窓口端末5から資格情報の読出し要求を受信すると、読出しが要求された資格情報を取得する（ST53）。

[0070] 個人情報サーバ4のプロセッサ41は、読出し要求に含まれる資格情報識別子によって読み出すべき資格情報を特定し、データメモリ44に保存しているICカード2の所持者に関する情報から特定した資格情報を読み出す。読出しが要求された資格情報を読み出すと、プロセッサ41は、セキュアチャネルが確立しているICカード2に対してデータメモリ44から読み出した資格情報を送信する（ST54）。

[0071] ICカード2は、個人情報サーバ4とのセキュアな通信によって個人情報サーバ4がデータメモリ44から読み出した当該ICカード2の所持者本人の資格情報を受信する。ICカード2のプロセッサ21は、個人情報サーバ4から資格情報を受信すると、受信した資格情報に対して電子署名を付与する（ST55）。ここで、プロセッサ21は、上述したST44でデータメモリ24に保存した秘密鍵を用いて個人情報サーバ4から受信した資格情報に対して電子署名を付与する。個人情報サーバ4からの資格情報に署名を付与した後、プロセッサ21は、電子署名を付与した署名済みの資格情報を個人情報サーバ4へ送信する（ST56）。

[0072] 個人情報サーバ4は、ICカード2とのセキュアな通信によってICカード2が署名した資格情報を受信する。個人情報サーバ4のプロセッサ41は、ICカード2から署名済みの資格情報を受信すると、受信した署名済みの資格情報をRAM43又はデータメモリ44に保持する。

[0073] 個人情報サーバ4のプロセッサ41は、ICカード2が署名した資格情報を保持した状態でワンタイムトークンを発行する（ST56）。ワンタイムトークンを発行すると、プロセッサ41は、ICカード2とのセキュアメッセージングによってワンタイムトークンを暗号化してICカード2へ送信す

る（ST57）。

[0074] ICカード2は、セキュアメッセージングによって窓口端末5を経由して個人情報サーバ4から暗号化されたワンタイムトークンを受信する。ICカード2のプロセッサ21は、個人情報サーバ4からセキュアメッセージングによる暗号化されたトークンを受信すると、受信したデータを復号することによりワンタイムトークンを取得する（ST58）。また、プロセッサ21は、個人情報サーバからのセキュアメッセージングの認証子を確認する（ST59）。

[0075] ICカード2のプロセッサ21は、個人情報サーバ4からのセキュアメッセージングの認証子を確認した後、個人情報サーバ4から取得したトークン（ワンタイムトークン）を窓口端末5へ供給する（ST60）。

[0076] 窓口端末5は、カードインターフェースに接続されたICカード2から当該ICカード2が復号したワンタイムトークンを取得する。窓口端末5は、ICカード2から取得したワンタイムトークンを個人情報サーバ4へ送信する（ST61）。このワンタイムトークンは、個人情報サーバ4が発行し、暗号化してICカード2に送信したデータである。窓口端末5は、個人情報サーバ4が暗号化したワンタイムトークンをICカード2で復号化した後に取得する。従って、個人情報サーバ4による暗号化とICカード2による復号化とが正常に実行されていれば、窓口端末5が個人情報サーバ4へ送信するワンタイムトークンは、元々個人情報サーバ4が生成したワンタイムトークンと一致するものとなる。

[0077] 個人情報サーバ4は、セキュアメッセージングにより暗号化したワンタイムトークンをICカード2へ送信した後、窓口端末5からワンタイムトークン（ワンタイムトークンのチャレンジデータ）を受信する。個人情報サーバ4のプロセッサ41は、窓口端末5からワンタイムトークンを受信すると、窓口端末5から受信したワンタイムトークンが当該個人情報サーバ4が発行してセキュアメッセージングでICカード2へ送信したワンタイムトークンと一致するかを確認する（ST62）。

- [0078] 窓口端末5から受信したトークンと自身が発行したワンタイムトークンとが一致する場合、個人情報サーバ4のプロセッサ41は、窓口端末5に資格情報を提供することを示す履歴情報をデータメモリ44に保存し（ST63）、RAM等の保持しているICカード2が署名した署名済みの資格情報を窓口端末5へ送信する（ST64）。
- [0079] 窓口端末5は、ICカード2から受信したワンタイムトークンを個人情報サーバ4へ送信した後、個人情報サーバ4からICカード2が署名した署名済みの資格情報を受信する。窓口端末5は、個人情報サーバ4からICカード2による署名済みの資格情報を受信すると、ST48で個人情報サーバ4から取得した公開鍵IDによってICカード2の公開鍵を取得する。窓口端末5は、ICカード2の公開鍵によってICカード2が署名した資格情報を復号化することによりICカード2の所持者本人の資格情報を取得する（ST65）。
- [0080] 以上の処理によれば、利用者が所持するICカードを窓口端末に接続させて指紋認証することで、個人情報サーバが保管している当該ICカードの所持者の情報を窓口端末に提供できる。これにより、利用者は、ICカードで指紋認証するだけで複雑な操作を行うことなく、個人情報サーバが保存する本人の資格情報などの情報を窓口端末に提供でき、窓口端末の表示部に本人の資格情報を表示などの運用ができる。
- [0081] また、上述した実施形態によれば、個人情報サーバは、指紋認証でICカードの所持者であることが確認された後、窓口端末から要求されるICカードの所持者の資格情報をICカードへ送信する。ICカードは、個人情報サーバから受信する資格情報に電子署名した署名済みの資格情報を個人情報サーバへ送信する。個人情報サーバは、ICカードから取得するICカードによる署名済みの資格情報を窓口端末へ提供する。窓口端末は、個人情報サーバからICカードによる署名済みの資格情報を受信し、ICカードの公開鍵を用いて資格情報を取得する。すなわち、実施形態に係る情報管理システムは、個人情報サーバが保管する資格情報を生体認証で本人確認したICカー

ドで電子署名した後で窓口端末に提供でき、個人情報サーバが保管する資格情報を安全に窓口端末に提供できる。

[0082] また、上述した実施形態によれば、個人情報サーバは、ワンタイムトークンを発行し、発行したワンタイムトークンをセキュアメッセージングによってＩＣカードへ送信する。ＩＣカードは、個人情報サーバからセキュアメッセージングで受信するワンタイムトークンを復号し、復号したワンタイムトークンを窓口端末へ送信する。窓口端末は、ＩＣカードが復号化したワンタイムトークンを個人情報サーバへ送信する。個人情報サーバは、窓口端末から受信するワンタイムトークンが正しければＩＣカードの所持者の情報を窓口端末へ提供する。これにより、窓口端末が送信するワンタイムトークンが生体認証で本人確認したＩＣカードを経由して得られる正当なワンタイムトークンであることを確認した後個人情報サーバが保管する情報を窓口端末に提供することができる。

[0083] 次に、本実施形態に係る情報管理システムにおいてＩＣカード２を用いて個人情報サーバ４が保持する情報を提供する情報提供処理について説明する。

図９は、窓口端末５からの資格情報を個人情報サーバ４が保持するＩＣカード２の所持者の資格情報として保存する保存処理の動作例を説明するためのシーケンスである。図９に示す動作例は、ＩＣカード２の所持者に関する新たな情報を窓口端末５を用いて個人情報サーバ４に登録する処理（書き込む処理）を想定する。具体例としては、窓口端末５を用いてＩＣカード２の所持者が新たに取得した資格情報をＩＣカード２の所持者のリポジトリとしての個人情報サーバ４に登録する処理が想定される。

[0084] 図９に示す処理は、上述した図７に示す処理の後に実行されるものとする。すなわち、個人情報サーバ４に資格情報を登録する利用者が所持するＩＣカード２が窓口端末５に接続される。窓口端末５とＩＣカード２は、図７に示すＳＴ３１～３５と同様な処理を実行する。これにより、窓口端末５は、ＩＣカード２が指紋照合によって所持者本人であることを確認した後に当該

所持者のリポジトリのURLを取得する。

[0085] 窓口端末5とリポジトリのURLで示される個人情報サーバ4とは、図7に示すST36と同様な処理によって通信用のセッションを確立し、個人情報サーバ4は、図7に示すST36と同様な処理によって窓口端末5の端末識別情報を取得する。

[0086] さらに、ICカード2と個人情報サーバ4とは、図7に示すST38-37と同様な処理によって相互認証を行ってセキュアチャネルを確立する。これにより、ICカード2と個人情報サーバ4とは、窓口端末5を含む外部装置に解読されないデータの送受信が可能なセキュアメッセージングを実行できる状態となる。

[0087] また、個人情報サーバ4は、図7に示すST40-41と同様な処理によって窓口端末5の公開鍵を取得する。

さらに、図7に示すST40-41と同様な処理によって、個人情報サーバ4とのセキュアチャネルが確立したICカード2は、個人情報サーバ4から要求に応じて鍵ペアを生成し、秘密鍵を保存する。ICカード2の公開鍵は、個人情報サーバ4および窓口端末5に登録される。

[0088] ICカード2の公開鍵を取得した後、窓口端末5は、当該ICカード2の所持者のリポジトリである個人情報サーバ4に登録（保管）すべき資格情報（書き込む情報）が指定される（ST71）。ここで、窓口端末5は、個人情報サーバ4に登録すべきICカード2の所持者の新たな資格情報を保持した状態であるものとする。

[0089] 例えば、窓口端末5は、ICカード2の所持者のリポジトリである個人情報サーバ4に登録（保管）すべき資格情報を表示部に表示する。窓口の係員は、表示部に表示したリポジトリに登録すべき資格情報を確認して当該資格情報の保存を操作部によって指示する。窓口端末5は、リポジトリに登録すべき資格情報が指定されると、登録すべき資格情報（書き込み情報）の書き込み依頼を個人情報サーバ4へ送信する（ST72）。

[0090] 個人情報サーバ4は、通信部45によりICカード2の所持者に関する情

報としての資格情報の書き込み要求を窓口端末5から受信する。個人情報サーバ4のプロセッサ41は、窓口端末5から資格情報の書き込み依頼を受信すると、ワンタイムトークンを発行する（ST73）。ワンタイムトークンを発行すると、プロセッサ41は、ICカード2とのセキュアメッセージングによってワンタイムトークンを暗号化してICカード2へ送信する（ST74）。

[0091] ICカード2は、セキュアメッセージングによって個人情報サーバ4から暗号化されたワンタイムトークンを受信する。ICカード2のプロセッサ21は、個人情報サーバ4からセキュアメッセージングによる暗号化されたワンタイムトークンを含むデータを受信すると、受信したデータに含まれる暗号化されたワンタイムトークンを復号する（ST75）。また、プロセッサ21は、個人情報サーバ4からのセキュアメッセージングの認証子を確認する（ST76）。

[0092] ICカード2のプロセッサ21は、個人情報サーバ4からのセキュアメッセージングの認証子を確認した後、個人情報サーバ4から受信したデータに含まれる復号化したワンタイムトークンを窓口端末5へ供給する（ST77）。

[0093] 窓口端末5は、カードインターフェースに接続されるICカード2から当該ICカード2が復号したワンタイムトークンを受信する。窓口端末5は、ICカード2からワンタイムトークンを受信すると、ICカード2の所有者に関する情報としてリポジトリとしての個人情報サーバ4に登録（保存）すべき資格情報に署名を付与する（ST78）。窓口端末5は、個人情報サーバ4に通知した公開鍵に対応する秘密鍵を保持しており、その秘密鍵を用いて個人情報サーバ4に保存すべき資格情報に電子署名を付与する。

[0094] 窓口端末5は、自身の秘密鍵を用いて登録すべき資格情報に電子署名した場合、ICカード2から取得したワンタイムトークン（ワンタイムトークンのチャレンジデータ）と当該資格情報を識別する資格情報識別子と署名済みの資格情報を含むデータを個人情報サーバ4へ送信する（ST79）。

- [0095] 個人情報サーバ4は、セキュアメッセージングによりICカード2へワンタイムトークンを送信した後、窓口端末5からワンタイムトークン、署名情報識別子および署名済みの資格情報を含むデータを受信する。個人情報サーバ4のプロセッサ41は、窓口端末5からワンタイムトークンを含むデータを受信すると、窓口端末5から受信したワンタイムトークンと当該個人情報サーバ4自身が発行したセキュアメッセージングでICカード2へ送信したワンタイムトークンとが一致するかを確認する（ST80）。
- [0096] 窓口端末5から受信したワンタイムトークンと自身が発行したワンタイムトークンとが一致する場合、個人情報サーバ4のプロセッサ41は、窓口端末5から登録が要求された資格情報を書き込みすることを示す履歴情報をデータメモリ44に保存する（ST81）。プロセッサ41は、窓口端末5から受信した署名済みの資格情報を当該窓口端末5の公開鍵で復号し、当該ICカード2の所持者の資格情報としてデータメモリ44に書き込む（ST82）。資格情報（書き込み情報）を書き込んだ後、プロセッサ41は、窓口端末5に対して登録が依頼された資格情報を正常に書き込んだ旨を通知する（ST83）。
- [0097] 以上の処理によれば、利用者が所持するICカードを窓口端末に接続させて指紋認証することで、窓口端末がICカードの所持者の新たな情報を個人情報サーバに書き込むことができる。これにより、利用者は、ICカードで指紋認証するだけで複雑な操作を行うことなく、窓口端末が表示部に表示する本人の新たな資格情報などの情報を個人情報サーバに保存することができる。
- [0098] また、上述した実施形態によれば、窓口端末は、指紋認証でICカードの所持者であることが確認された後、ICカードから取得したリポジトリのURLが示す個人情報サーバにICカードの所持者の新たな資格情報（書き込み情報）の書き込みを依頼する。窓口端末は、個人情報サーバに登録する資格情報を自身の秘密鍵を用いて電子署名し、電子署名した署名済みの資格情報を個人情報サーバに送信する。個人情報サーバは、窓口端末の公開鍵を用

いて窓口端末から受信した署名済みの資格情報に基づく資格情報をＩＣカードの所持者の情報として書き込む。これにより、実施形態に係る情報管理システムは、生体認証で本人確認したＩＣカードを接続した窓口端末がＩＣカードの所持者の情報として保管すべき新たな資格情報などの情報を安全に個人情報サーバへ供給でき、個人情報サーバに安全に保管できる。

[0099] また、上述した実施形態によれば、窓口端末から情報書き込み依頼を受けた個人情報サーバは、ワンタイムトークンを発行し、発行したワンタイムトークンをセキュアメッセージングによってＩＣカードへ送信する。ＩＣカードは、個人情報サーバからセキュアメッセージングで受信するワンタイムトークンを復号し、復号したワンタイムトークンを窓口端末へ送信する。窓口端末は、ＩＣカードからのワンタイムトークンと登録すべき資格情報（書き込み情報）とを個人情報サーバへ送信する。個人情報サーバは、窓口端末から受信するワンタイムトークンが正しければ窓口端末が書き込みを要求する資格情報を当該ＩＣカードの所持者の情報として書き込む。これにより、個人情報サーバは、窓口端末からのワンタイムトークンが生体認証で本人確認したＩＣカードを経由して得られる正当なワンタイムトークンであることを確認した後に窓口端末が書き込みを依頼する書き込み情報を個人情報サーバに書き込んで保管できる。

[0100] 本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

請求の範囲

- [請求項1] 認証デバイスと個人情報サーバとを有する情報管理システムであって、
- 前記認証デバイスは、
- 人物の生体情報を取得するセンサと、
- 所持者の生体情報を記憶するメモリと、
- 端末装置と接続するインターフェースと、
- 前記センサが取得する生体情報と前記メモリが記憶する生体情報との生体照合が成功した場合に前記個人情報サーバの場所を示す情報を前記端末装置へ出力する第1プロセッサと、を有し、
- 前記個人情報サーバは、
- 前記端末装置と通信する通信部と、
- 前記認証デバイスの所持者の個人情報を保管するデータメモリと、
- 前記認証デバイスが接続された前記端末装置からの要求に応じて前記データメモリが保管する前記認証デバイスの所持者の個人情報を前記端末装置へ供給する第2プロセッサと、を有する、
- 情報管理システム。
- [請求項2] 前記個人情報サーバの前記第2プロセッサは、ワンタイムトークンを発行し、前記認証デバイスにセキュアメッセージングによって前記ワンタイムトークンを送信した後に前記端末装置から受信するデータが前記発行したワンタイムトークンと一致すれば、前記個人情報を前記端末装置へ送信し、
- 前記認証デバイスの前記第1プロセッサは、前記個人情報サーバからのセキュアメッセージングによって受信するデータを復号することで得られる前記個人情報サーバが発行したワンタイムトークンを前記端末装置へ送信する、
- 請求項1に記載の情報管理システム。
- [請求項3] 前記認証デバイスの前記第1プロセッサは、前記個人情報サーバか

ら受信する前記所持者の個人情報に電子署名した署名済み個人情報を前記個人情報サーバへ送信し、

前記個人情報サーバの前記第2プロセッサは、前記認証デバイスから取得する前記認証デバイスの公開鍵を前記端末装置に開示し、前記端末装置からの要求に応じて前記データメモリが保管する前記認証デバイスの所持者の個人情報を前記認証デバイスに送信した後に前記認証デバイスが電子署名した署名済み個人情報を前記端末装置へ供給する、

請求項1に記載の情報管理システム。

[請求項4]

前記認証デバイスの前記第1プロセッサは、前記個人情報サーバからのセキュアメッセージングによって受信するデータを復号することで得られる前記個人情報サーバが発行するワンタイムトークンを前記端末装置へ送信し、

前記個人情報サーバの前記第2プロセッサは、前記ワンタイムトークンを発行し、前記認証デバイスにセキュアメッセージングによって前記ワンタイムトークンを送信した後に、前記端末装置から受信するワンタイムトークンのチャレンジデータが前記発行したワンタイムトークンと一致すれば、前記署名済み個人情報を前記端末装置へ送信する、

請求項3に記載の情報管理システム。

[請求項5]

前記認証デバイスは、カード状の本体を有し、

前記認証デバイスの前記センサは、生体情報として指紋を読み取る指紋センサであり、前記認証デバイスの前記第1プロセッサは、前記指紋センサが取得する指紋情報と前記メモリが記憶する指紋情報との指紋照合が成功した場合に前記個人情報サーバの場所を示す情報を前記端末装置へ出力する、

請求項1乃至4の何れか1項に記載の情報管理システム。

[請求項6]

人物の生体情報を取得するセンサと、

所持者の生体情報を記憶するメモリと、
端末装置と接続するインターフェースと、
前記センサが取得する生体情報と前記メモリが記憶する生体情報との生体照合が成功した場合に前記所持者の個人情報を保管する個人情報サーバの場所を示す情報を前記端末装置へ出力するプロセッサと、
を有する認証デバイス。

[請求項7] センサが取得する生体情報と登録済みの所持者の生体情報に対する生体照合を行う認証デバイスが接続される端末装置と通信する通信部と、

前記認証デバイスの所持者の個人情報を保管するデータメモリと、
前記端末装置に接続された前記認証デバイスにおける所持者の生体照合が成功した場合に前記端末装置からの要求に応じて前記データメモリが保管する前記認証デバイスの所持者の個人情報を前記端末装置へ供給するプロセッサと、
を有する個人情報サーバ。

[請求項8] 認証デバイスと個人情報サーバとを有する情報管理システムであって、

前記認証デバイスは、
人物の生体情報を取得するセンサと、
所持者の生体情報を記憶するメモリと、
端末装置と接続するインターフェースと、
前記センサが取得する生体情報と前記メモリが記憶する生体情報との生体照合が成功した場合に前記個人情報サーバの場所を示す情報を前記端末装置へ出力する第1プロセッサと、を有し、
前記個人情報サーバは、
前記端末装置と通信する通信部と、
前記認証デバイスの所持者の個人情報を保管するデータメモリと、
前記認証デバイスが接続された前記端末装置からの書き込み依頼に

応じて前記端末装置から供給される書き込み情報を前記認証デバイスの所持者の個人情報として前記データメモリに書き込む第2プロセッサと、を有する、

情報管理システム。

[請求項9] 前記認証デバイスの前記第1プロセッサは、前記個人情報サーバからのセキュアメッセージングによって受信するデータを復号することで得られる前記個人情報サーバが発行するワンタイムトークンを前記端末装置へ送信し、

前記個人情報サーバの前記第2プロセッサは、前記ワンタイムトークンを発行し、前記認証デバイスにセキュアメッセージングによって前記ワンタイムトークンを送信した後に、前記端末装置から受信するワンタイムトークンのチャレンジデータが前記発行したワンタイムトークンと一致すれば、前記端末装置からの前記書き込み情報を前記データメモリに書き込む、

請求項8に記載の情報管理システム。

[請求項10] 前記個人情報サーバの前記第2プロセッサは、前記端末装置が前記書き込み情報に電子署名した署名済み書き込み情報を前記端末装置から取得し、前記署名済み書き込み情報を前記端末装置の公開鍵を用いて確認した後に前記書き込み情報を前記データメモリに書き込む、

請求項8に記載の情報管理システム。

[請求項11] 前記認証デバイスの前記第1プロセッサは、前記個人情報サーバからのセキュアメッセージングによって受信するデータを復号することで得られる前記個人情報サーバが発行するワンタイムトークンを前記端末装置へ送信し、

前記個人情報サーバの前記第2プロセッサは、前記ワンタイムトークンを発行し、前記認証デバイスにセキュアメッセージングによって前記ワンタイムトークンを送信した後に、前記端末装置から受信するワンタイムトークンのチャレンジデータが前記発行したワンタイムト

ークンと一致すれば、前記端末装置からの前記署名済み書き込み情報を前記端末装置の公開鍵を用いて確認した後に前記書き込み情報を前記データメモリに書き込む、請求項10に記載の情報管理システム。

[請求項12] 前記認証デバイスは、カード状の本体を有し、
前記認証デバイスの前記センサは、生体情報として指紋を読み取る指紋センサであり、前記認証デバイスの前記第1プロセッサは、前記指紋センサが取得する指紋情報と前記メモリが記憶する指紋情報との指紋照合が成功した場合に前記個人情報サーバの場所を示す情報を前記端末装置へ出力する、

請求項8乃至11の何れか1項に記載の情報管理システム。

[請求項13] センサが取得する生体情報と登録済みの所持者の生体情報に対する生体照合を行う認証デバイスが接続される端末装置と通信する通信部と、

前記認証デバイスの所持者の個人情報を保管するデータメモリと、
前記端末装置に接続された前記認証デバイスにおける所持者の生体照合が成功した場合に前記端末装置からの書き込み依頼に応じて前記端末装置から供給される書き込み情報を前記認証デバイスの所持者の個人情報として前記データメモリに書き込むプロセッサと、を有する個人情報サーバ。