

明 細 書

発明の名称：

セキュリティデバイス、情報管理システムおよび情報管理プログラム

技術分野

[0001] 本発明の実施形態は、セキュリティデバイス、情報管理システムおよび情報管理プログラムに関する。

背景技術

[0002] 近年、スマートフォン、タブレットＰＣおよび携帯電話機などの携帯端末には、個人情報などのセキュリティ対策が必要な情報が保持されている。例えば、近年、運転免許証を含む身分証明機能をスマートフォン等のモバイル機器に持たせるための取り組みが進行している。

[0003] 一例としては、スマートフォン等の携帯端末を運転免許証として利用するモバイル運転免許証がある。モバイル運転免許証は、携帯端末が実行可能な運転免許証として利用されるアプリケーションプログラムとして提供される。携帯端末に搭載するモバイル運転免許証は、個人情報を含む免許証の情報をセキュアに管理する必要がある。しかしながら、携帯端末だけでは、セキュリティ対策に限界があるという問題がある。

先行技術文献

特許文献

[0004] 特許文献１：日本国特開２０１９－０４７３２５号公報

発明の概要

発明が解決しようとする課題

[0005] 上記の課題を解決するために、本発明は、情報をセキュアに管理できるセキュリティデバイス、情報管理システムおよび情報管理プログラムを提供することを目的とする。

課題を解決するための手段

[0006] 実施形態によれば、セキュリティデバイスは、インターフェースとセキュアメモリとプロセッサとを有する。インターフェースは、情報を開示する機能を有する携帯端末と通信する。セキュアメモリは、認証に用いる情報を記憶する。プロセッサは、インターフェースにより携帯端末におけるセキュリティ管理すべき情報の開示指示に伴う認証要求を受信し、認証要求の内容に応じてセキュアメモリが記憶する情報を用いて実行すべき認証処理を特定し、特定した認証処理を実行した認証結果を携帯端末へ通知する。

図面の簡単な説明

- [0007] [図1]図1は、第1実施形態に係るセキュリティデバイスとしてのスマートウォッチを含む情報管理システムの構成例を概略的に示す図である。
- [図2]図2は、第1実施形態に係るセキュリティデバイスの構成例を示すブロック図である。
- [図3]図3は、第1実施形態に係る情報管理システムにおける携帯端末の構成例を示すブロック図である。
- [図4]図4は、第1実施形態に係る情報管理システムにおけるサーバの構成例を示すブロック図である。
- [図5]図5は、第1実施形態に係る情報管理システムにおける携帯端末の動作例を説明するためのフローチャートである。
- [図6]図6は、第1実施形態に係る情報管理システムにおけるセキュリティデバイスの動作例を説明するためのフローチャートである。
- [図7]図7は、第1実施形態に係る情報管理システムのセキュリティデバイスにおける認証状態のアンロック処理を説明するためのフローチャートである。
- [図8]図8は、第2実施形態に係る情報管理システムを実現する装置の構成例を概略的に示す図である。
- [図9]図9は、第2実施形態に係る情報管理システムにおけるセキュリティデバイスの構成例を示すブロック図である。
- [図10]図10は、第2実施形態に係る情報管理システムにおける携帯端末の

構成例を示すブロック図である。

[図11]図 1 1 は、第 2 実施形態に係る情報管理システムにおけるサーバの構成例を示すブロック図である。

[図12]図 1 2 は、第 2 実施形態に係る情報管理システムにおける携帯端末による保存設定の動作例を説明するためのフローチャートである。

[図13]図 1 3 は、第 2 実施形態に係る情報管理システムにおける携帯端末による免許情報の表示処理の動作例を説明するためのフローチャートである。

[図14]図 1 4 は、第 2 実施形態に係る情報管理システムにおけるサーバの動作例を説明するためのフローチャートである。

実施形態

[0008] 以下、第 1 および第 2 実施形態について、図面を参照しつつ説明する。

(第 1 実施形態)

まず、第 1 実施形態に係るセキュリティデバイスを含む情報管理システム 1 について説明する。

図 1 は、第 1 実施形態に係るセキュリティデバイスを含む情報管理システム 1 の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 1 は、セキュリティデバイス 2、携帯端末 3 およびサーバ 4 を有する。セキュリティデバイス 2 とサーバ 4 とは、インターネットなどのネットワーク 5 を介して通信接続される。

[0009] セキュリティデバイス 2 は、ユーザが保持する電子デバイスである。セキュリティデバイス 2 は、例えば、スマートウォッチなどのウェアラブルデバイスである。セキュリティデバイス 2 は、携帯端末 3 と通信する通信インターフェース、サーバ 4 と通信する通信インターフェース、生体センサ（指紋センサ、静脈センサ、カメラなど）、セキュアメモリ、内部時計（クロック）などを有する。

[0010] また、セキュリティデバイス 2 としてのウェアラブルデバイスは、図 1 に示すように、各部を備える本体 2 a と本体 2 a をユーザが保持（装着）するための装着部 2 b とを備える。例えば、セキュリティデバイス 2 としてのス

スマートウォッチは、ユーザが本体 2 a を装着するための装着部 2 b としてのベルトを備える。

[0011] 第 1 実施形態において、セキュリティデバイス 2 は、主として、生体情報としての指紋を用いて生体認証を行う機能を有するスマートウォッチであることを想定して説明するものとする。ただし、第 1 実施形態に係るセキュリティデバイス 2 は、スマートウォッチに限定されるものではなく、ユーザが携帯端末 3 とともに所持するデバイスであれば良い。また、第 1 実施形態に係るセキュリティデバイス 2 は、生体情報として指紋による指紋（生体）認証を行うものに限定されるものではない。

[0012] 携帯端末 3 は、ユーザが所持する情報処理装置である。携帯端末 3 は、例えば、スマートフォン、携帯電話機、タブレット PC などである。携帯端末 3 は、身分証明書で示される個人情報を含む証明書情報などの各種の情報を表示するためのアプリケーションプログラム（以下、アプリとも称する）がロードされる。第 1 実施形態において、携帯端末 3 は、運転免許証として利用可能なモバイル運転免許証（以下、mDLとも称する）を実現するためのアプリがロードされるものとする。携帯端末 3 は、ユーザ自身が操作するものであって、mDLとしての運転免許証で証明される各種の情報を表示する。

[0013] 携帯端末 3 は、セキュリティデバイス 2 と通信する機能、および、ネットワーク 5 を介してサーバ 4 と通信する機能を備える。また、携帯端末 3 は、生体センサ（指紋センサ、静脈センサ、カメラなど）を備え、生体センサで取り込んだ生体情報による生体認証を行う機能も有するものとする。

[0014] サーバ 4 は、セキュリティデバイス 2 および携帯端末 3 と通信する機能を有する。サーバ 4 は、セキュリティデバイス 2 の識別情報およびオンライン認証に必要な情報を保存するデータベースを備える。オンライン認証に必要な情報としては、セキュリティデバイス 2 に保持する秘密情報を検証できる情報（例えば、セキュリティデバイス 2 が保持する秘密鍵に対応する公開鍵）などである。

[0015] 次に、第1実施形態に係る情報管理システム1におけるセキュリティデバイス2の構成について説明する。

図2は、第1実施形態に係るセキュリティデバイス2における制御系の構成例を示すブロック図である。

図2に示す構成例において、セキュリティデバイス2は、プロセッサ11、ROM12、RAM13、データメモリ14、セキュアメモリ15、インターフェース(I/F)16、通信部17、表示部18、入力部19、生体センサ20、および、クロック21などを有する。

[0016] なお、セキュリティデバイス2としてのウェアラブルデバイスは、図2に示す構成を備える本体2aとユーザが装着するための装着部2bとを備える。例えば、セキュリティデバイス2としてのスマートウォッチは、図2に示す構成を備える本体2aとユーザが腕などに装着するための装着部2bとしてのベルトなどを備える。

[0017] プロセッサ11は、種々の処理を実行する回路を含む。プロセッサ11は、例えば、CPU(Central Processing Unit)である。プロセッサ11は、セキュリティデバイス2全体の制御を司る。プロセッサ11は、ROM12あるいはデータメモリ14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11が実行する各種の機能のうちの一部又は全部は、ハードウェア回路により実現されるようにしても良い。

[0018] ROM12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。ROM12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。ROM12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セキュリティデバイス2の筐体内に組み込まれる。ROM12に記憶される制御プログラムや制御データは、予め当該セキュリティデバイス2の仕様等に応じて組み込まれる。

[0019] RAM13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、RAM13は、プロセッサ11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 13は、通信部17を介してサーバ4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。

[0020] データメモリ14は、データの書き込みおよび書き換えが可能な不揮発性のメモリである。データメモリ14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14には、当該セキュリティデバイス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。

[0021] セキュアメモリ15は、セキュアにデータが格納できる耐タンパー性を有するメモリである。セキュアメモリ15は、セキュリティデバイス2が認証処理を行うための情報を記憶する。例えば、セキュアメモリ15は、後述するサーバ4を用いたオンライン認証に用いる秘密情報としての秘密鍵を記憶する。

[0022] また、セキュアメモリ15は、当該セキュリティデバイス2の所有者（登録者）であるユーザを認証するための認証情報を記憶する。セキュアメモリ15に記憶する認証情報は、セキュリティデバイス2が備える認証処理方式に対応する各種の認証情報を記憶する。例えば、認証情報としては、生体認証に用いる生体情報、および、暗証番号（PIN）による認証に用いる暗証番号などがある。また、生体情報としては、セキュリティデバイス2が備える生体センサ20が取得する生体情報に対応する登録者の生体情報を記憶する。例えば、セキュリティデバイス2が生体認証として指紋認証を行う機能を有する場合、セキュアメモリ15は、登録者の生体情報として指紋情報を記憶する。

[0023] インターフェース16は、携帯端末3と通信接続するためのインターフェースである。インターフェース16は、当該セキュリティデバイス2をユー

ザが保持した状態（例えば、腕に装着した状態）で携帯端末3と通信接続できるものであれば良く、例えば、ブルートゥース（登録商標）などの無線通信を行うインターフェースである。

[0024] 通信部17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17は、ネットワーク5を介してサーバ4と通信するものであれば良い。通信部17は、3G、LTE（登録商標）あるいは5Gなどの携帯電話通信網で通信するものであっても良い、Wifiなどの無線LANによりサーバ4と通信するものであっても良い。

[0025] 表示部18は、液晶パネル等の表示デバイスである。入力部19は、携帯端末3に対して操作指示を入力する操作デバイスである。入力部19は、例えば、タッチパネルを含む。表示部18と入力部19とは、タッチパネル付き表示装置（以下、タッチスクリーンと称する）で構成しても良い。また、入力部19は、ボタンスイッチで構成する操作キー、静電容量の変化に基づいて操作者の手指が触れたことを検出するタッチセンサなどを含むものであっても良い。

[0026] 生体センサ20は、生体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。生体センサ20は、例えば、指紋センサ、静脈センサ、あるいは、カメラなどである。生体センサ20としての指紋センサは、ユーザの指紋を読み取るものであり、例えば、表示部18に設けたタッチパネルで実現するようにしても良い。生体センサ20としての静脈センサは、セキュリティデバイス2としてのスマートウォッチを腕に装着した状態で装着部位にある静脈パターンを読み取る。また、生体センサ20としてのカメラは、顔認証に用いる顔画像あるいは虹彩認証に用いる虹彩などの光学的に撮影可能な生体情報を取得する。

[0027] クロック21は、日時を計時するものである。クロック21は、セキュリティデバイス2の内部クロックであり、独立して日時を計時できるものである。ただし、クロック21は、通信部17によりネットワーク5を介して接続する外部機器あるいはインターフェース16を介して接続する携帯端末3

から日時情報に基づいて内部クロックを補正（設定）するようにしても良い。

[0028] 次に、第1実施形態に係る情報管理システム1における携帯端末3の構成について説明する。

図3は、第1実施形態に係る情報管理システム1における携帯端末3の構成例を示すブロック図である。

図3に示す構成例において、携帯端末3は、プロセッサ31、ROM32、RAM33、データメモリ34、通信部35、カードリーダーライタ（RW）36、表示部37、および、入力部38などを有する。

[0029] 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携帯端末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と協働して携帯端末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。例えば、プロセッサ31は、ROM32あるいはデータメモリ34に記憶されているアプリケーション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31が実行する各種の機能のうちの一部又は全部は、ハードウェア回路により実現されるようにしても良い。

[0030] ROM（Read Only Memory）32は、携帯端末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。例えば、ROM32は、オペレーティングシステム（OS）などの基本動作を司るプログラムを記憶する。また、ROM32は、携帯端末3が具備する機能を実現するためのアプリケーションプログラムなどを記憶しても良い。ROM32は、書き換え可能な不揮発性のメモリで構成しても良い。例えば、書き換え可能なROM32としては、EEPROM（Electrically Erasable Programmable ROM）又はフラッシュROMなどで実現される。

- [0031] 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。RAM 33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。
- [0032] 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、フラッシュROM、SSD (Solid State Drive) などの半導体素子メモリ、あるいは、HDD (Hard Disc Drive) などの記憶装置が用いられる。データメモリ 34は、アプリケーションプログラム、動作設定値、個人情報などを記憶する。また、データメモリ 34は、OSプログラムを記憶するようにしても良い。
- [0033] 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、インターフェースを介してサーバ4と通信するものである。通信部 35は、3G、LTEあるいは5Gなどの携帯電話通信網（移動体通信）で通信するものであっても良いし、Wifiなどの無線LANによりサーバ4と通信するものであっても良い。
- [0034] セキュリティデバイスインターフェース (I/F) 36は、セキュリティデバイス2と通信接続するためのインターフェースである。セキュリティデバイスインターフェース 36は、ユーザが保持した状態のセキュリティデバイス2と通信接続できるものであれば良く、例えば、ブルートゥースなどの無線通信を行うインターフェースである。
- [0035] 表示部 37は、液晶パネル等の表示デバイスである。入力部 38は、携帯端末3に対して操作指示を入力する操作デバイスである。入力部 38は、例えば、タッチパネルを含む。表示部 37と入力部 38とは、タッチパネル付き表示装置（以下、タッチスクリーンと称する）で構成しても良い。また、入力部 38は、ボタンスイッチで構成する操作キー、静電容量の変化に基づいて操作者の手指が触れたことを検出するタッチセンサなどを含むものであっても良い。
- [0036] 生体センサ 39は、生体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。生体センサ39は、例えば、指紋センサ、静脈センサ、あるいは、カメラなどである。生体センサ39は、セキュリティデバイス2が備える生体センサ20と同じものであっても良いし、異なるものであっても良い。また、携帯端末3は、複数種類の生体センサを備えるものであっても良い。

[0037] 次に、第1実施形態に係る情報管理システム1におけるサーバ4の構成について説明する。

図4は、第1実施形態に係る情報管理システム1におけるサーバ4の構成例を示すブロック図である。

図4に示すように、サーバ4は、プロセッサ41、ROM42、RAM43、データメモリ44、インターフェース45、通信部46、および、データベース47を有する。

[0038] プロセッサ41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41は、例えば、CPU (Central Processing Unit) である。プロセッサ41は、システムバスを介してサーバ4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41は、ROM42およびRAM43と協働してサーバ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。

[0039] ROM (Read Only Memory) 42は、サーバ4として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。

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。

- [0040] 通信部４６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４６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。本第１実施形態において、通信部４６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保持するセキュリティデバイス２および携帯端末３と通信するものであれば良い。
- [0041] データベース４７は、セキュリティデバイス２とのオンライン認証を行うためのデータを記憶するメモリである。データベース４７は、例えば、セキュリティデバイス２の識別情報（ＩＤ）とオンライン認証に必要な情報としてセキュリティデバイスの秘密情報を検証できる情報（例えば、秘密鍵に対応する公開鍵など）と対応づけて記憶する。
- [0042] 次に、第１実施形態に係る情報管理システム１において携帯端末３がモバイル運転免許証の情報を利用するための動作例について説明する。
- まず、第１実施形態に係る情報管理システム１における携帯端末３の動作例について説明する。
- 図５は、第１実施形態に係る情報管理システムにおける携帯端末の動作例を説明するためのフローチャートである。
- [0043] まず、ユーザは、携帯端末３においてｍＤＬを起動させた後、開示を要求する情報を示す指示を入力部３８を用いて入力する。携帯端末３のプロセッサ３１は、ユーザが入力部３８に用いて入力する開示を要求する情報を指定する操作指示を受け付ける（ＳＴ１０）。例えば、ユーザは、携帯端末３の表示部３７に表示させたいｍＤＬの情報（免許証情報）を入力部３８により指示する。ここで、ユーザは、使用用途あるいは使用用途に応じて表示することが必要な情報などを指示するものとする。
- [0044] プロセッサ３１は、ｍＤＬの使用指示が入力されると、指示内容に応じて携帯端末３での生体認証が必要であるか否かを判断する（ＳＴ１１）。例えば、データメモリ３４は、ユーザが指定する指示内容に応じて実施すべき認証などの処理内容を示す設定情報を記憶しているものとする。プロセッサ３１は、データメモリ３４に記憶する設定情報に基づいて、ユーザが指定した

指示内容に応じて携帯端末3での生体認証が必要であるか否かを判断する。

- [0045] 携帯端末3での生体認証が必要であると判断すると（ST11、YES）、プロセッサ31は、携帯端末3において生体認証を実行する（ST12）。携帯端末3での生体認証として、プロセッサ31は、生体センサ39を取得し、生体センサ39が取得する生体情報とデータメモリ34に保存している登録者としてのユーザの生体情報とを照合することにより生体認証を行う。なお、ST12の携帯端末3における生体認証は、生体認証以外のユーザ認証に置き換えても良い。例えば、携帯端末3における生体認証は、暗証番号によるユーザ認証に置き換えても良い。
- [0046] 携帯端末3における生体認証が成功した場合（ST13、YES）、プロセッサ31は、ST14へ進む。また、携帯端末3での生体認証が必要でないと判断した場合（ST11、NO）、プロセッサ31は、携帯端末3での生体認証を省略し、ST14へ進む。
- [0047] ST14において、プロセッサ31は、指示内容に応じてセキュリティデバイス2での認証が必要であるか否かを判断する（ST14）。プロセッサ31は、データメモリ34に記憶する設定情報に基づいて、ユーザが指定した指示内容に応じてセキュリティデバイス2での認証が必要であるか否かを判断する。
- [0048] セキュリティデバイス2での認証が不要であると判断した場合（ST14、NO）、プロセッサ31は、ユーザが指定した内容に応じてmDLの情報を提示する（ST18）。例えば、プロセッサ31は、ユーザが免許証情報の一部の表示を指示した場合、ユーザが指定した情報をmDLによって読み出して表示部37に表示させる。
- [0049] セキュリティデバイス2での認証が必要であると判断した場合（ST14、YES）、プロセッサ31は、ユーザが指定した指示内容に応じてセキュリティデバイス2において実行することが必要となる認証処理をセキュリティデバイス2に要求する（ST15）。プロセッサ31は、セキュリティデバイスインターフェース36を介して通信接続するセキュリティデバイス2

に対して認証要求を送信する。

- [0050] 例えば、プロセッサ31は、セキュリティデバイス2で実行すべき認証処理の内容を示す情報として、セキュリティデバイス2に要求するセキュリティレベル（認証レベル）を通知するようにしても良い。また、プロセッサ31は、セキュリティデバイス2で実行すべき認証処理の具体的な内容を判断し、セキュリティデバイス2に実行すべき認証処理の内容を認証要求とともに通知する。また、プロセッサ31は、ユーザが指定する指示内容をセキュリティデバイス2に通知することによりセキュリティデバイス2に実行すべき認証処理の内容を判断させるようにしても良い。
- [0051] セキュリティデバイス2に認証要求を送信した後、プロセッサ31は、セキュリティデバイス2からの認証結果の受信待ちとなる（ST16）。セキュリティデバイス2から認証結果を取得した場合、プロセッサ31は、指示内容に応じたセキュリティデバイス2での認証処理が成功したか否かを判断する（ST17）。
- [0052] セキュリティデバイス2での認証が成功した場合（ST17、YES）、プロセッサ31は、ユーザが指定した内容に応じてmDLの情報を提示する（ST18）。例えば、プロセッサ31は、ユーザが表示を要求した免許証情報をmDLによって読み出して表示部37に表示させる。
- [0053] セキュリティデバイス2での認証が失敗した場合（ST17、NO）、又は、携帯端末3における生体認証が失敗した場合（ST17、NO）、プロセッサ31は、mDLの使用不可を報知する（ST19）。例えば、プロセッサ31は、表示部37に指定された生体認証が失敗したためmDLが使用できない旨の警告を表示部37に表示する。
- [0054] 以上のような処理によれば、第1実施形態に係る情報処理システムは、携帯端末でユーザが提示を要求する指示内容に応じて携帯端末およびセキュリティデバイスで実施すべき認証処理を実行し、携帯端末およびセキュリティデバイスにおける認証が成功した場合に、ユーザが指示した内容の情報を提示する。

[0055] これにより、第1実施形態に係る情報処理システムによれば、携帯端末だけでなく、携帯端末と連携するセキュリティデバイスを用いた認証を前提して携帯端末が保持する情報を提示するようにできる。この結果として、第1実施形態に係る情報処理システムは、利便性の高いmDLなどの携帯端末で実現する身分証明書機能が提示可能とする情報に対しても強固な情報セキュリティを実現できる。

[0056] 次に、第1実施形態に係る情報管理システム1におけるセキュリティデバイス2の動作について説明する。

図6は、第1実施形態に係る情報管理システムにおけるセキュリティデバイスの動作例を説明するためのフローチャートである。

セキュリティデバイス2のプロセッサ11は、携帯端末3とインターフェース16を介して通信接続した状態で稼働しているものとする。この状態において、プロセッサ11は、携帯端末3から情報の開示に伴う認証要求を取得する(ST21)。

[0057] 認証要求を受けた場合、プロセッサ11は、携帯端末3又は携帯端末3のアプリ(ここでは、mDLとする)からの認証要求が有効であるか否かを判断する(ST22)。例えば、セキュリティデバイス2は、接続設定されている携帯端末3又は携帯端末3のmDLに対して認証要求を受け付け可能とする有効期限を設けても良い。この場合、プロセッサ11は、有効期限内であれば携帯端末3又はmDLからの認証要求を実行し、有効期限外(失効期間)であれば携帯端末3又はmDLからの認証要求を実行不可とする。

[0058] 認証要求が有効であると判断した場合(ST22、YES)、プロセッサ11は、携帯端末3から認証要求とともに取得する情報に基づいて実行すべき認証処理の内容を特定する。ここでは、図6に示すように3段階で設定された認証レベルに応じて認証処理を行う動作例について説明する。

[0059] すなわち、プロセッサ11は、携帯端末3から取得した認証要求が有効である場合、認証要求に応じて実行すべき認証処理の認証レベル(又は認証処理内容)を特定する。例えば、携帯端末3から認証レベルが指定された場合

、プロセッサ 11 は、携帯端末 3 から指定される認証レベルに応じて実行すべき認証処理の内容を特定する。また、プロセッサ 11 は、携帯端末 3 から提示が要求された内容を示す情報を取得し、取得した情報に基づいて認証レベルを特定するようにして良い。なお、各認証レベルに応じた認証処理の内容については、データメモリ 14 等に記憶しておくようにすれば良い。

- [0060] 高レベルの認証処理が必要であると判断した場合（S T 23、Y E S）、プロセッサ 11 は、高レベルの認証処理を実行する（S T 24）。例えば、各種の手続き（例えば、銀行カード、クレジットカードの発行、役所等での公的な手続き）を行うための個人の証明として m D L が示す情報が必要である場合、セキュリティデバイス 2 における高レベルの認証処理が必要であるものとする。
- [0061] 高レベルの認証処理としては、例えば、サーバ 4 と連携したオンライン認証、および、生体認証との両方を実行すべき認証処理であるものとする。この場合、セキュリティデバイス 2 は、オンライン認証および生体認証の成功を認証成功の条件とすることで、高度なセキュリティ性を持つ認証結果を携帯端末 3 へ提供できる。
- [0062] また、サーバ 4 と連携したオンライン認証としては、例えば、P K I（公開鍵暗号基板：P u b l i c K e y I n t r a s t r u c t u r e）に基づくチャレンジレスポンス認証がある。具体例としては、セキュリティデバイス 2 には公開鍵ペアのうち秘密鍵が保存され、サーバ 4 には公開鍵が保存される構成とする。セキュリティデバイス 2 は、サーバ 4 からのチャレンジを秘密鍵で暗号化しレスポンスする。サーバ 4 は、セキュリティデバイス 2 からのレスポンスを対応する公開鍵で検証する。
- [0063] また、認証処理のレベル（認証処理の内容）は、内部時計としてのクロック 21 が計時する日時に基づいて特定するようにしても良い。セキュリティデバイス 2 の内部時計としてのクロックが計時する日時を用いて認証処理のレベルや認証処理の内容を特定することにより、情報管理システム 1 としては、外部のデバイスに依存せずにセキュリティデバイス 2 内だけで時間経過

等に応じた認証方法の制御が実現できる。

- [0064] 例えば、前回オンライン認証を行ってから（前回オンライン認証が成功してから）の経過した期間に応じて認証処理のレベルを特定するようにしても良い。具体的には、セキュリティデバイス2は、オンライン認証が成功した日時をデータメモリ14に保持しておき、前回オンライン認証が成功してから経過時間が所定基準値を超えた場合、高レベルの認証処理が必要であると判断するようにしても良い。
- [0065] また、前回オンライン認証を行ってから（前回オンライン認証が成功してから）オフラインで実施された認証処理（生体認証又はPIN認証）の回数（又は、認証情報としての生体情報又はPINの読み出し回数）に応じて認証処理のレベルを特定するようにしても良い。具体的には、セキュリティデバイス2は、オンライン認証が成功してからオフラインで実施された認証処理の回数をデータメモリ14に保持しておき、前回オンライン認証が成功してからオフラインで実施された認証処理の回数が所定基準値を超えた場合、高レベルの認証処理が必要であると判断するようにしても良い。
- [0066] また、認証処理に要求されるセキュリティレベルが高レベルでないと判断した場合（ST23、NO）、プロセッサ11は、携帯端末3から要求された認証処理の認証レベルが中レベルである否かを判断する（ST25）。
- [0067] 中レベルの認証処理が必要であると判断した場合（ST25、YES）、プロセッサ11は、中レベルの認証処理を実行する（ST26）。例えば、個人を確認（例えば、警察からの任意聴取、又は、チケットと個人の紐付けの確認など）を行うためにmDLが示す個人を証明する情報を提示することが必要である場合、セキュリティデバイス2における中レベルの認証処理が必要であるものとする。
- [0068] 中レベルの認証処理としては、例えば、セキュリティデバイス2におけるオフラインでの生体認証が実行すべき認証処理であるものとする。この場合、セキュリティデバイス2は、サーバ4と連携したオンライン認証が要求されずに、セキュリティデバイス2におけるオフラインでの生体認証の成功を

条件とすることで、利便性を確保しつつ生体認証によるセキュリティ性を維持できる認証結果を携帯端末3へ提供することができる。

[0069] また、認証処理に要求されるセキュリティレベルが中レベルでないと判断した場合（ST25、NO）、プロセッサ11は、携帯端末3から要求された認証処理の認証レベルが低レベルであると判断する。例えば、低レベルの認証処理としては、一部の個人情報の確認（例えば、たばこ、又は、酒類を購入するための年齢確認）を行うためにmDLが示す個人情報の一部だけを提示することが必要である場合、セキュリティデバイス2においては、低レベルの認証処理が必要であるものとする。

[0070] 低レベルの認証処理としては、例えば、セキュリティデバイス2においてオフラインでのPIN認証が実行すべき認証処理であるものとする。この場合、セキュリティデバイス2は、サーバ4と連携したオンライン認証および生体認証が要求されずに、セキュリティデバイス2におけるオフラインでのPIN認証の成功を条件とすることで、利便性を確保しつつ一定のセキュリティ性を維持できる認証結果を携帯端末3へ提供することができる。

[0071] 認証要求に応じて特定したレベルの認証処理を行うと、プロセッサ11は、セキュリティデバイス2としての認証が成功したか否かを判定する（ST28）。

認証要求に応じたセキュリティデバイス2における認証が成功した場合（ST28、YES）、プロセッサ11は、セキュリティデバイス2における認証が成功した旨を認証要求元の携帯端末3へ通知する（ST31）。

[0072] また、認証要求に応じたセキュリティデバイス2における認証が失敗した場合（ST28、NO）、プロセッサ11は、認証処理がリトライ可能な状態であるか否かを判断する（ST29）。リトライ可能な状態である場合（ST29、YES）、プロセッサ11は、ST23へ戻り、上述した認証処理を再度実行する。

[0073] リトライ不可の状態となった場合（ST29、NO）、プロセッサ11は、当該セキュリティデバイス2における認証要求元の携帯端末3又は携帯端

末3のmDLに対する認証状態をロック状態にする（ST30）。認証状態をロック状態とした場合、プロセッサ11は、認証要求に応じた認証が失敗した旨と認証状態がロック状態となった旨とを示す認証結果を携帯端末3へ送信する（ST31）。

[0074] 以上のような処理によれば、第1実施形態に係る情報処理システムにおいて、セキュリティデバイスは、mDLを実行する携帯端末からの認証要求の内容に応じた内容の認証処理を特定し、認証要求の内容に応じた認証処理の結果を認証結果として携帯端末へ通知する。これにより、第1実施形態に係る情報処理システムによれば、mDLを実行する携帯端末とは別の機器であるセキュリティデバイスにおける認証結果に基づいてmDLの情報を提供することができ、mDLの情報に対するセキュリティ性を向上できる。

[0075] また、上述した動作例によれば、第1実施形態に係る情報処理システムにおいて、セキュリティデバイスは、mDLを実行する携帯端末からの認証要求に応じて内部クロックが計時する計時情報などに応じた実行すべき認証処理の内容を特定する。これにより、セキュリティデバイスは、外部のデバイスに依存せずにセキュリティデバイス自身が時間経過等に伴って必要とされる認証方法で認証処理を実行することでき、強固なセキュリティ性を維持できる。

[0076] 次に、第1実施形態に係るセキュリティデバイス2における認証状態のロック状態をアンロックするアンロック処理について説明する。

図7は、第1実施形態に係るセキュリティデバイス2における認証ロック状態をアンロック状態にするためのアンロック処理を説明するためのフローチャートである。

上述した図6に示す動作例によれば、セキュリティデバイス2は、所定のリトライ中に認証処理が成功しなければ認証状態をロック状態とする。ロック状態となった場合、セキュリティデバイス2がアンロック処理によってロック状態を解除しなければ、携帯端末3のmDLが使用不可となる。

[0077] 第1実施形態に係る情報管理システムにおけるセキュリティデバイス2は

、所定の手続きによるロック状態を解除するアンロック処理を実行する機能を有するものとする。図7に示す動作例においては、セキュリティデバイス2は、サーバ4との連携によるオンライン認証が成功すればロック状態を解除できるものとする。

[0078] まず、セキュリティデバイス2のプロセッサ11は、インターフェース16を介して通信接続する携帯端末3からアンロックのための認証要求（アンロック要求）を取得する（ST41）。

[0079] アンロック要求を受けると、プロセッサ11は、ロック状態を解除するための所定の手続きとしてオンライン認証を行うために、サーバ4と通信接続する（ST42）。プロセッサ11は、サーバ4との通信接続が確立すると、オンライン認証を実行する（ST43）。オンライン認証としては、例えば、上述したようなPKIに基づくセキュリティデバイス2が保持する秘密鍵とサーバ4が保持する公開鍵とを用いた認証が適用できる。

[0080] オンライン認証が成功した場合（ST44、YES）、プロセッサ11は、携帯端末3又は携帯端末3のmDLに対する認証状態のロック状態をアンロックする（ST45）。オンライン認証の成功に伴ってロック状態を解除した場合、プロセッサ11は、認証状態のロックを解除した旨の処理結果を携帯端末3へ送信する（ST47）。

また、オンライン認証が成功しなかった場合（ST44、NO）、プロセッサ11は、携帯端末3又は携帯端末3のmDLに対する認証状態のロック状態を維持し（ST46）、認証状態のロック状態のままである旨の処理結果を携帯端末3へ送信する（ST47）。

[0081] 以上の処理によれば、第1実施形態に係るセキュリティデバイスは、サーバとのオンライン認証などの所定の手続きによって携帯端末又はmDLに対する認証のロック状態を解除する。これにより、セキュリティデバイスにおいて有効期限切れなど含む様々な要因で認証状態がロックされた場合であっても所定の手続きによるロック状態を解除することができ、セキュリティ性を保持しながら安定した運用が可能となる。

[0082] (第2実施形態)

以下、第2実施形態について、図面を参照しつつ説明する。

まず、第2実施形態に係るセキュリティデバイス202を含む情報管理システム201について説明する。

図8は、第2実施形態に係るセキュリティデバイス202を含む情報管理システム201の構成例を模式的に示す図である。

図8に示す構成例において、情報管理システム201は、セキュリティデバイス202、携帯端末203およびサーバ204を有する。携帯端末203とサーバ204とは、インターネットなどのネットワーク205を介して通信接続される。また、セキュリティデバイス202とサーバ204とがネットワークを介して通信するようにしても良い。

[0083] セキュリティデバイス202は、携帯端末203と接続する通信インターフェースおよびセキュアに情報を記憶するセキュアメモリを備える電子デバイスである。セキュリティデバイス202は、携帯端末203内にセットされるものであっても良いし、携帯端末203と通信接続するデバイスであっても良い。また、情報管理システム201において、携帯端末203に接続するセキュリティデバイスは、複数あっても良い。

[0084] 携帯端末203内にセットされるセキュリティデバイス202の例としては、SIM (Subscriber Identification Module) カード、sSIM (Embedded SIM)、メモリカードなどがある。また、携帯端末203に通信接続するセキュリティデバイス202の例としては、スマートウォッチなどのウェアラブルデバイス、ICカード、外部セキュリティデバイスなどがある。

[0085] 携帯端末203は、ユーザが携帯する情報処理装置である。携帯端末203は、例えば、スマートフォン、携帯電話機、タブレットPCなどである。携帯端末203は、ユーザインターフェースとしての表示部および入力部などを備え、セキュリティデバイス202と接続する機能、および、ネットワーク205を介してサーバ204と通信する機能などを備える。

[0086] 携帯端末２０３は、身分証明書で示される個人情報を含む証明書情報などの各種の情報を表示するためのアプリケーションプログラム（以下、アプリとも称する）がロードされる。第２実施形態では、携帯端末２０３は、身分証明証の一例である運転免許証として利用可能なモバイル運転免許証（以下、mDLとも称する）を実現するためのアプリがロードされるものとする。また、携帯端末２０３は、ユーザ自身が操作するものであって、モバイル運転免許証の機能として運転免許証で証明される各種の情報を表示部に表示する。

[0087] サーバ２０４は、セキュリティデバイス２０２および携帯端末２０３と通信する機能を有する。また、サーバ２０４は、セキュリティデバイス２０２と通信する機能を有する。サーバ２０４は、携帯端末２０３を介してセキュリティデバイス２０２と通信する機能を備えるものであっても良いし、携帯端末２０３を介さずにネットワーク２０５を介してセキュリティデバイス２０２と通信する機能を備えるものであっても良いし、両者の機能を備えるものであっても良い。

[0088] サーバ２０４は、携帯端末２０３がモバイル運転免許証の機能として表示する免許証情報を保持するデータベースを有する。サーバ２０４は、各ユーザの携帯端末２０３にインストールされるモバイル運転免許証に対する秘密鍵の保管場所を示す情報（保管場所情報）を携帯端末２０３から取得する。サーバ２０４は、携帯端末２０３から取得する保管場所情報を示すセキュリティデバイス２０２などの保管場所から秘密鍵を取得し、取得した秘密鍵を用いて各ユーザの免許証情報を携帯端末２０３に表示させる制御を行う。

[0089] 次に、第２実施形態に係る情報管理システム２０１におけるセキュリティデバイス２０２の構成について説明する。

図９は、第２実施形態に係るセキュリティデバイス２０２における制御系の構成例を示すブロック図である。

図９に示す構成例において、セキュリティデバイス２０２は、プロセッサ２１１、ROM２１２、RAM２１３、データメモリ２１４、セキュアメモ

リ 2 1 5、インターフェース (I/F) 2 1 6、および、通信部 2 1 7 などを有する。

[0090] プロセッサ 2 1 1 は、種々の処理を実行する回路を含む。プロセッサ 2 1 1 は、例えば、CPU (Central Processing Unit) である。プロセッサ 2 1 1 は、セキュリティデバイス 2 0 2 全体の制御を司る。プロセッサ 2 1 1 は、ROM 2 1 2 あるいはデータメモリ 2 1 4 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 2 1 1 が実行する各種の機能のうちの一部又は全部は、ハードウェア回路により実現されるようにしても良い。

[0091] ROM 2 1 2 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。ROM 2 1 2 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。ROM 2 1 2 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セキュリティデバイス 2 0 2 の筐体内に組み込まれる。ROM 2 1 2 に記憶される制御プログラムや制御データは、予め当該セキュリティデバイス 2 0 2 の仕様等に応じて組み込まれる。

[0092] RAM 2 1 3 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 2 1 3 は、プロセッサ 2 1 1 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 2 1 3 は、通信部 2 1 7 を介してサーバ 2 0 4 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。

[0093] データメモリ 2 1 4 は、データの書き込みおよび書き換えが可能な不揮発性のメモリである。データメモリ 2 1 4 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 2 1 4 には、当該セキュリティデバイス 2 0 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 2 4 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。

[0094] セキュアメモリ 215 は、セキュアにデータが格納できる耐タンパー性を有するメモリである。セキュアメモリ 215 は、接続された携帯端末 203 のモバイル運転免許証に対応する秘密鍵を保管する。

[0095] インターフェース 216 は、携帯端末 203 と接続するためのインターフェースである。インターフェース 216 は、携帯端末 203 が備えるインターフェースと物理的に接触して接続されるものであっても良いし、携帯端末 203 と通信接続できるものであっても良い。例えば、携帯端末 203 と通信接続するインターフェースとしては、ブルートゥース（登録商標）などの近距離無線通信、非接触 IC カードと非接触で通信するための非接触通信、あるいは、W i f i （登録商標）などの無線通信などのインターフェースである。

[0096] また、通信部 217 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 217 は、ネットワーク 205 を介してサーバ 204 と通信する。通信部 217 は、3 G、L T E （登録商標）あるいは 5 G などの携帯電話通信網で通信するものであっても良いし、W i f i などの無線 LAN によりサーバ 204 と通信するものであっても良い。なお、セキュリティデバイス 202 が携帯端末 203 を介してサーバ 204 と通信する形態とする場合、セキュリティデバイス 202 の構成としては通信部 217 を省略しても良い。

[0097] 次に、第 2 実施形態に係る情報管理システム 201 における携帯端末 203 の構成について説明する。

図 10 は、第 2 実施形態に係る情報管理システム 201 における携帯端末 203 の構成例を示すブロック図である。

図 10 に示す構成例において、携帯端末 203 は、プロセッサ 231、R O M 232、R A M 233、データメモリ 234、通信部 235、インターフェース（I / F）236、表示部 237、および、入力部 238などを有する。

[0098] プロセッサ 231 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231は、例えば、CPU (Central Processing Unit) である。プロセッサ231は、システムバスを介して携帯端末203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231は、ROM232およびRAM233と協働して携帯端末203における制御およびデータ処理などの動作を実行する。例えば、プロセッサ231は、ROM232あるいはデータメモリ234に記憶されているアプリケーション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231が実行する各種の機能のうちの一部又は全部は、ハードウェア回路により実現されるようにしても良い。

[0099] ROM (Read Only Memory) 232は、携帯端末203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。例えば、ROM232は、オペレーティングシステム (OS) などの基本動作を司るプログラムを記憶する。また、ROM232は、携帯端末203が具備する機能を実現するためのアプリケーションプログラムなどを記憶しても良い。ROM232は、書き換え可能な不揮発性のメモリで構成しても良い。例えば、書き換え可能なROM232としては、EEPROM (Electrically Erasable Programmable ROM) 又はフラッシュROMなどで実現される。

[0100] RAM (Random Access Memory) 233は、データを一時的に記憶する揮発性のメモリである。RAM233は、プロセッサ231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。

[0101] データメモリ234は、各種のデータを記憶する記憶部である。データメモリ234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234は、フラッシュROM、SSD (Solid State Drive) などの半導体素子メモリ、あるいは、HDD (Hard Disc Drive) などの記憶装置が用いられる。データメモリ234は、アプリケーションプログラム、動作設定値、個人情報などを記憶する。また、データメモリ234は、OSプログラムを記憶するようにし

ても良い。

[0102] 通信部235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235は、インターフェースを介してサーバ204と通信するものである。通信部235は、3G、LTEあるいは5Gなどの携帯電話通信網（移動体通信）で通信するものであっても良いし、Wifiなどの無線LANによりサーバ204と通信するものであっても良い。

[0103] インターフェース(I/F)236(236a、236b、…)は、セキュリティデバイス202と通信接続するためのセキュリティデバイスインターフェースである。インターフェース236は、少なくとも1つのセキュリティデバイス202と接続できるように構成される。図10では、インターフェース236は、第1のインターフェース236aおよび第2のインターフェース236bを含むことを例示する。各インターフェース236は、それぞれが各種のセキュリティデバイス202に対応するインターフェースで構成する。

[0104] 例えば、第1のインターフェース236aは、携帯端末203の所定位置にセット（携帯端末203の装着）されるセキュリティデバイス（例えば、SIMカード、eSIM、メモリカード等）202aに対応するインターフェースである。第2のインターフェース236bは、携帯端末203と通信接続する外部デバイスとしてのセキュリティデバイス（例えば、スマートウォッチ等のウェアラブルデバイス、ICカード、外部セキュリティデバイスなど）202bに対応するインターフェースである。第2のインターフェース236bとしては、ブルートゥースなどの無線通信を行うインターフェース、あるいは、ICカードリーダーライタなどがある。

[0105] 表示部237は、液晶パネル等の表示装置（表示デバイス）である。入力部238は、携帯端末203に対して操作指示を入力する入力デバイスである。入力部238は、例えば、タッチパネルを含む。表示部237と入力部238とは、タッチパネル付き表示装置（以下、タッチスクリーンと称する）で構成しても良い。また、入力部238は、ボタンスイッチで構成する操

作キー、静電容量の変化に基づいて操作者の手指が触れたことを検出するタッチセンサなどを含むものであっても良い。

[0106] 次に、第2実施形態に係る情報管理システム201におけるサーバ204の構成について説明する。

図11は、第2実施形態に係る情報管理システム201におけるサーバ204の構成例を示すブロック図である。

図11に示すように、サーバ204は、プロセッサ241、ROM242、RAM243、データメモリ244、通信部246、および、データベース247を有する。

[0107] プロセッサ241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241は、例えば、CPU (Central Processing Unit) である。プロセッサ241は、システムバスを介してサーバ204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241は、ROM242およびRAM243と協働してサーバ204における制御およびデータ処理などの動作を実行する。

[0108] ROM (Read Only Memory) 242は、サーバ204として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) 243は、データを一時的に記憶する揮発性のメモリである。RAM243は、プロセッサ241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。

データメモリ244は、各種のデータを記憶する記憶部である。データメモリ244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244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。

[0109] 通信部246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246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。本第2実施形態において、通信部246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保持するセキュリティデバイス202および携帯端末203と通信するものであれば良い。

[0110] データベース247は、モバイル運転免許証の情報として携帯端末203に表示可能な免許証情報を保存する。例えば、データベース247には、ユーザの携帯端末203にモバイル運転免許証としてのアプリがインストールされると、当該モバイル運転免許証によって表示する免許証情報が登録される。

[0111] 次に、第2実施形態に係る情報管理システム201において携帯端末203がモバイル運転免許証としての免許証情報を表示するための動作について説明する。

まず、第2実施形態に係る情報管理システム201における携帯端末203におけるモバイル運転免許証に対応する秘密鍵の保管設定の動作例について説明する。

図12は、第2実施形態に係る情報管理システム201の携帯端末203におけるモバイル運転免許証に対応する秘密鍵の保管設定の動作例を説明するためのフローチャートである。

[0112] まず、ユーザは、携帯端末203のインターフェース236にセキュリティデバイス202を接続させる操作を行う。プロセッサ231は、ユーザ操作などに応じてインターフェース236を介したセキュリティデバイス202との接続を確立させる(ST211)。例えば、ユーザは、SIMカードなどのセキュリティデバイス202aを携帯端末203における所定位置にセットする。所定位置にセットされたセキュリティデバイス202aがインターフェース236aのコンタクト部に接触すると、プロセッサ231は、インターフェース236aを介してセキュリティデバイス202aとの通信状態を確立させる。

[0113] また、外部デバイスとしてのセキュリティデバイス202bを接続する場合、プロセッサ231は、ユーザ操作などに応じてインターフェース236bによりセキュリティデバイス202bとの通信接続を試行することにより

インターフェース236bを介してセキュリティデバイス202bとの通信状態を確立させる。

[0114] インターフェース236にセキュリティデバイス202が接続されると、プロセッサ231は、通信部235によりサーバ204にアクセスする(ST212)。さらに、プロセッサ231は、インターフェース236に接続されているセキュリティデバイス202から鍵の保管場所が選択可能であるかを判断する(ST213)。例えば、プロセッサ231は、インターフェース236に接続されているセキュリティデバイス202が秘密鍵を保管可能なセキュアメモリを備えているか否かなどにより鍵の保管場所として選択可能であるか否かを判断する。

[0115] 鍵の保管場所として選択不可能である場合(ST213、NO)、プロセッサ231は、秘密鍵の保管設定処理を終了する。

鍵の保管場所として選択可能である場合(ST213、YES)、プロセッサ231は、鍵の保管場所をユーザに選択させるための選択画面を表示部237に表示する(ST214)。例えば、プロセッサ231は、鍵の保管場所とすることが可能なセキュリティデバイス202の一覧を選択画面に表示する。ユーザは、表示部237に表示された選択画面において選択肢として示されるセキュリティデバイス202のいずれかを秘密鍵を保管する保管場所として入力部238を用いて選択指示する。

[0116] 例えば、インターフェース236aに第1のセキュリティデバイス202aとしてのSIMカードが接続され、インターフェース236bに第2のセキュリティデバイス202bとしてのスマートウォッチが接続されている場合、プロセッサ231は、SIMカード又はスマートウォッチのいずれかを鍵の保管場所として選択させる選択画面を表示部237に表示する。この場合、ユーザは、入力部238を用いてSIMカードもしくはスマートウォッチを秘密鍵の保管場所として選択する。

[0117] 選択画面に表示した選択肢から鍵の保管場所が選択された場合(ST215、YES)、プロセッサ231は、ユーザにより選択された保管場所とし

てのセキュリティデバイス202に秘密鍵を保存する(ST216)。例えば、プロセッサ231は、選択されたセキュリティデバイス202のセキュアメモリに当該携帯端末203にインストールされてるモバイル運転免許証に対応する秘密鍵を書き込む。

[0118] ユーザが選択した保管場所に秘密鍵を保存すると、プロセッサ231は、秘密鍵を保管した保管場所としてのセキュリティデバイス202を示す保管場所情報を生成し、生成した保管場所情報をデータメモリ234に保存する(ST217)。

[0119] 以上のような処理によれば、第2実施形態に係る情報処理システムにおける携帯端末は、ユーザが選択するセキュリティデバイスを秘密鍵の保管場所として登録することができる。携帯端末は、ユーザが指定する秘密鍵の保管場所としてのセキュリティデバイスを示す保管場所情報を生成し、生体した保管場所情報をメモリに保存おくことができる。

[0120] 次に、第2実施形態に係る情報管理システム201における携帯端末203に免許情報を表示させる表示処理の動作について説明する。

図13は、第2実施形態に係る情報管理システム201における携帯端末203に免許情報を表示させる処理の動作例を説明するためのフローチャートである。

ユーザは、携帯端末203においてモバイル運転免許証のアプリを起動させ、入力部238を用いて表示させたい免許情報を指定する。プロセッサ231は、ユーザ操作に応じてモバイル運転免許証のアプリを起動させ、入力部238を用いて指定される免許情報の表示指示を受け付ける。

[0121] 携帯端末203のプロセッサ231は、入力部238により免許情報の表示指示が入力された場合(ST231、YES)、通信部235によりサーバ204と通信する(ST232)。サーバ204との通信が確立した後、プロセッサ231は、入力部238を用いて表示指示された免許情報の開示をサーバ204に要求する(ST233)。

[0122] 携帯端末203のプロセッサ231は、サーバ204に免許情報の開示要

求を送信した後、サーバ204からの要求に応じて鍵（秘密鍵）の保管場所（セキュリティデバイス）を示す保管場所情報をサーバ204へ送信する（ST234）。保管場所情報は、上述したように保管設定によって登録される情報であり、ユーザのモバイル運転免許証に対応する秘密鍵の保管場所を示す情報である。

[0123] 鍵の保管場所を示す保管場所情報を送信した後、プロセッサ231は、サーバ204から開示を要求した表示部237に表示させるための免許情報を取得する（ST235）。サーバ204から免許情報を取得すると、プロセッサ231は、取得した免許情報を表示部237に表示する（ST236）。

[0124] 以上のような処理によれば、第2実施形態に係る情報処理システムにおいて、携帯端末は、入力部により入力される免許情報の表示指示に応じてサーバに免許情報の開示要求を送信する。携帯端末は、免許情報の開示要求を送信したサーバから要求に応じてモバイル運転免許証に対応する秘密鍵の保管場所を示す保管場所情報をサーバに通知する。保管場所情報した後、携帯端末は、サーバから取得する免許情報を表示部に表示する。これにより、携帯端末とは別のセキュアメモリを有するセキュリティデバイスにモバイル運転免許証を利用するための秘密鍵を保存しておくことができ、その秘密鍵の保管場所をサーバに通知することが可能となる。

[0125] 次に、第2実施形態に係る情報管理システム201におけるサーバ204の動作について説明する。

図14は、第2実施形態に係る情報管理システム201におけるサーバ204の動作例を説明するためのフローチャートである。

携帯端末203は、図13に示すような動作により、ユーザ操作に応じてモバイル運転免許証として表示する免許情報をサーバ204へ要求する。サーバ204は、通信部246にネットワーク205を介して携帯端末203と通信する。サーバ204のプロセッサ241は、通信部246により携帯端末203からの免許情報の開示要求を取得する（ST251）。

- [0126] 携帯端末203の免許情報の開示要求を取得すると、プロセッサ241は、当該携帯端末203にユーザの免許情報を表示させるために、当該携帯端末203にインストールされているモバイル運転免許証に対応する秘密鍵を取得する処理を行う。サーバ204のプロセッサ241は、秘密鍵を取得するため、携帯端末203に対して保管場所情報を要求する（ST252）。サーバ204のプロセッサ241は、保管場所情報を要求した後、通信部246により携帯端末203から保管場所情報を取得する（ST253）。
- [0127] 保管場所情報を取得すると、プロセッサ241は、取得した保管場所情報が示す保管場所から秘密鍵を取得する（ST254）。ここで、保管場所としてのセキュリティデバイス202が携帯端末203を介さずに当該サーバ204と通信する機能を有するものであれば、プロセッサ241は、携帯端末203を経由することなく通信部246により通信するセキュリティデバイス202から秘密鍵を取得する。また、保管場所としてのセキュリティデバイス202が携帯端末203を介して当該サーバ204と通信するものであれば、プロセッサ241は、携帯端末203を介して保管場所としてのセキュリティデバイス202から秘密鍵を取得する。
- [0128] 秘密鍵を取得すると、プロセッサ241は、取得した秘密鍵を利用して携帯端末203の表示部237に表示させるためのユーザの免許情報を携帯端末203へ出力する（ST255）。
- [0129] 以上のような処理によれば、第2実施形態に係る情報処理システムにおいて、サーバは、携帯端末からの免許情報の開示要求を受けた場合に携帯端末から秘密鍵の保管場所を示す保管場所情報を取得し、保管場所情報が示す保管場所から取得する秘密鍵を利用してユーザの免許情報を携帯端末に表示させる。これにより、第2実施形態によれば、情報管理システムは、携帯端末とは別のユーザが指定するセキュアメモリを有するセキュリティデバイスに秘密鍵を用いてユーザの免許情報を携帯端末に表示させることができる。これにより、秘密鍵をセキュアに管理することができ、秘密鍵を用いて提供される情報のセキュリティを向上することができる。

- [0130] 上述の各実施形態で説明した機能は、ハードウェアを用いて構成するに留まらず、ソフトウェアを用いて各機能を記載したプログラムをコンピュータに読み込ませて実現することもできる。また、各機能は、適宜ソフトウェア、ハードウェアのいずれかを選択して構成するものであっても良い。
- [0131] 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] 情報を開示する機能を有する携帯端末と通信するインターフェースと、
- 認証に用いる情報を記憶するセキュアメモリと、
- 前記インターフェースにより前記携帯端末におけるセキュリティ管理すべき情報の開示指示に伴う認証要求を受信し、前記認証要求の内容に応じて前記セキュアメモリが記憶する情報を用いて実行すべき認証処理を特定し、特定した認証処理を実行した認証結果を携帯端末へ通知するプロセッサと、
- を有するセキュリティデバイス。
- [請求項2] さらに、前記インターフェース、前記セキュアメモリおよび前記プロセッサを備える本体と、
- 前記本体をユーザに装着させる装着部と、を備える、
- 請求項1に記載のセキュリティデバイス。
- [請求項3] 生体情報を取得する生体センサを有し、
- 前記セキュアメモリは、生体情報を含む認証情報を記憶し、
- 前記プロセッサは、前記セキュアメモリが記憶する生体情報を用いた生体認証を含む複数の認証処理の中から前記認証要求の内容に応じて実行すべき認証処理を特定する、
- 請求項1又は2のいずれか1項に記載のセキュリティデバイス。
- [請求項4] サーバと通信する通信部を有し、
- 前記セキュアメモリは、前記サーバが保持する鍵に対応する鍵を記憶し、
- 前記プロセッサは、前記セキュアメモリが記憶する鍵と前記サーバが保持する鍵とを用いたオンライン認証を含む複数の認証処理の中から前記認証要求の内容に応じて実行すべき認証処理を特定する、
- 請求項1乃至3のいずれか1項に記載のセキュリティデバイス。
- [請求項5] 前記プロセッサは、前記認証要求の内容に基づいて認証レベルを特

定し、認証レベルに応じた認証処理を特定する、

請求項 1 乃至 4 のいずれか 1 項に記載のセキュリティデバイス。

[請求項6]

日時を計時するクロックを有し、

前記プロセッサは、前記クロックが計時する日時に基づいて実行すべき認証処理を特定する、

請求項 1 乃至 5 のいずれか 1 項に記載のセキュリティデバイス。

[請求項7]

さらに、日時を計時するクロックと、

前記オンライン認証が成功した日時を記憶するメモリと、を有し、

前記プロセッサは、前記クロックが計時する日時と前記メモリが記憶する情報とに基づく前回オンライン認証が成功してから経過した時間が基準値を超えた場合に実行すべき認証処理として前記オンライン認証を含む認証処理を特定する、

請求項 4 に記載のセキュリティデバイス。

[請求項8]

さらに、日時を計時するクロックと、

前記オンライン認証が成功してから実施した認証処理の回数を示す情報を記憶するメモリと、を有し、

前記プロセッサは、前記メモリが記憶する情報に基づく前回オンライン認証が成功してから実施した認証処理の実行回数が基準値を超えた場合に実行すべき認証処理として前記オンライン認証を含む認証処理を特定する、

請求項 4 に記載のセキュリティデバイス。

[請求項9]

携帯端末とセキュリティデバイスとを有する情報管理システムにおいて、

前記携帯端末は、

前記セキュリティデバイスと通信するセキュリティデバイスインターフェースと、

ユーザが情報の開示を指示するための入力部と、

前記入力部で指示された情報を開示するために前記セキュリティデ

バイスでの認証が必要である場合、前記セキュリティデバイスに認証要求を送り、前記セキュリティデバイスにおける認証が成功した場合に前記情報を開示する第1のプロセッサと、を有し、

前記セキュリティデバイスは、

前記携帯端末と通信するインターフェースと、

認証に用いる情報を記憶するセキュアメモリと、

前記インターフェースにより前記携帯端末が情報を開始するための認証要求を受信した場合、前記認証要求の内容に応じて前記セキュアメモリが記憶する情報を用いて実行すべき認証処理を特定し、特定した認証処理を実行した認証結果を携帯端末へ通知する第2のプロセッサと、

を有する情報管理システム。

[請求項10]

サーバと通信する通信部を有し、

前記セキュアメモリは、前記サーバが保持する鍵に対応する鍵を記憶し、

前記第2のプロセッサは、前記セキュアメモリが記憶する鍵と前記サーバが保持する鍵とを用いたオンライン認証を含む複数の認証処理の中から前記認証要求の内容に応じて実行すべき認証処理を特定する、

請求項9に記載の情報管理システム。

[請求項11]

日時を計時するクロックを有し、

前記第2のプロセッサは、前記クロックが計時する日時に基づいて実行すべき認証処理の内容を特定する、

請求項9又は10のいずれか1項に記載の情報管理システム。

[請求項12]

日時を計時するクロックと、

前記オンライン認証が成功した日時を記憶するメモリと、を有し、

前記第2のプロセッサは、前記クロックを計時する日時と前記メモリが記憶する情報とに基づく前回オンライン認証が成功してから経過

した時間が基準値を超えた場合に実行すべき認証処理として前記オンライン認証を含む認証処理を特定する、

請求項 10 に記載の情報管理システム。

[請求項13]

日時を計時するクロックと、

前記オンライン認証が成功してから実施した認証処理の回数を示す情報を記憶するメモリと、を有し、

前記第2のプロセッサは、前記メモリが記憶する情報に基づく前回オンライン認証が成功してから実施した認証処理の回数が基準値を超えた場合に実行すべき認証処理として前記オンライン認証を含む認証処理を特定する、

請求項 10 に記載の情報管理システム。

[請求項14]

携帯端末とサーバとを有する情報管理システムであって、

前記携帯端末は、

メモリと、

表示装置と、

ユーザ操作を受け付ける入力デバイスと、

セキュリティデバイスを接続する少なくとも1つのインターフェースと、

前記サーバと通信する第1通信部と、

前記インターフェースに接続されるセキュリティデバイスから秘密鍵の保管場所をユーザに選択させるための選択画面を前記表示装置に表示し、

前記選択画面を表示した場合に前記入力デバイスを用いてユーザが秘密鍵の保管場所として指定したセキュリティデバイスを示す保管場所情報を前記メモリに記憶し、

前記第1通信部により通信する前記サーバに前記保管場所情報を送信し、

前記保管場所情報を送信した前記サーバからの情報を前記表示装

置に表示させる、第1のプロセッサと、を有し、

前記サーバは、

前記携帯端末と通信する第2通信部と、

前記第2通信部により前記携帯端末から前記保管場所情報を取得し、前記保管場所情報が示すセキュリティデバイスから取得する秘密鍵を用いて前記携帯端末の表示装置に表示させる前記ユーザに関する情報を前記携帯端末に出力する、第2のプロセッサと、を有する、情報管理システム。

[請求項15] 前記携帯端末の前記インターフェースは、前記携帯端末に装着するセキュリティデバイスに接続するためのインターフェースを含む、請求項14に記載の情報管理システム。

[請求項16] 前記携帯端末の前記インターフェースは、前記携帯端末の外部デバイスとしてのセキュリティデバイスと通信するインターフェースを含む、請求項14に記載の情報管理システム。

[請求項17] 前記サーバは、前記秘密鍵を用いて前記携帯端末の表示装置に表示させる前記ユーザに関する情報として前記ユーザの免許情報を保持するデータベースを有する、請求項14に記載の情報管理システム。

[請求項18] メモリと、表示装置と、入力デバイスと、セキュリティデバイスを接続する少なくとも1つのインターフェースと、サーバと通信する通信部と、プロセッサと、を備える携帯端末において、前記プロセッサに、前記インターフェースに接続されるセキュリティデバイスから秘密鍵の保管場所をユーザに選択させるための選択画面を前記表示装置に表示させ、

前記選択画面を表示した場合に前記入力デバイスを用いてユーザが秘密鍵の保管場所として指定するセキュリティデバイスを示す保管場

所情報を前記メモリに記憶させ、

前記通信部により前記サーバに保管場所情報を送信させ、

前記保管場所情報を送信した前記サーバからの情報を前記表示装置
に表示させる、

ことを実行させるための情報管理プログラム。

[請求項19] 前記インターフェースは、前記携帯端末に装着するセキュリティデ
バイスに接続するためのインターフェースを含む、

請求項18に記載の情報管理プログラム。

[請求項20] 前記インターフェースは、前記携帯端末の外部デバイスとしてのセ
キュリティデバイスと通信するインターフェースを含む、

請求項18に記載の情報管理プログラム。