(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6906809号
(P6906809)
(45)発行日　令和3年7月21日(2021.7.21)　(24)登録日　令和3年7月2日(2021.7.2)

(51)Int.Cl.　　F I
G06Q 20/34 (2012.01)　　G06Q 20/34 430
G06Q 20/40 (2012.01)　　G06Q 20/40

請求項の数 11　(全 29 頁)

(21)出願番号　特願2019-200873(P2019-200873)
(22)出願日　令和1年11月5日(2019.11.5)
(62)分割の表示　特願2016-103411(P2016-103411)の分割
原出願日　平成27年9月3日(2015.9.3)
(65)公開番号　特開2020-17323(P2020-17323A)
(43)公開日　令和2年1月30日(2020.1.30)
審査請求日　令和1年11月5日(2019.11.5)

(73)特許権者　515349548
ブレイニー株式会社
沖縄県那覇市おもろまち一丁目１番２５－５１２号
(74)代理人　110001737
特許業務法人スズエ国際特許事務所
(72)発明者　田中　雅史
沖縄県那覇市おもろまち１丁目１番２５－５１２号

審査官　竹下　翔平

最終頁に続く

(54)【発明の名称】集積回路

(57)【特許請求の範囲】
【請求項１】
メモリとプロセッサとを具備し、
前記メモリは、決済のための第１の機能で用いられる第１のデータと、前記第１の機能を利用可能な第１の利用者の第１の生体データと、前記第１の利用者を示す第１の利用者識別情報と、前記第１の機能と異なる第２の機能で用いられる第２のデータと、前記第２の機能を利用可能であり前記第１の利用者と異なる第２の利用者の第２の生体データと、前記第２の利用者を示す第２の利用者識別情報と、前記第１の機能と前記第２の機能とに関する履歴情報と、を記憶し、
前記プロセッサは、
前記第１の利用者が前記第１の機能を用いる場合に、第１の外部装置へ前記第１のデータと前記第１の生体データとを無線により送信し、前記第１の外部装置から前記第１の生体データに基づく第１の生体認証の第１の結果データを無線により受信し、前記履歴情報に、前記第１の利用者識別情報と、前記第１の機能を示す第１の識別情報と、前記第１の結果データと、第１の時間情報とを関連付けた第１の情報を加え、
前記第２の利用者が前記第２の機能を用いる場合に、前記第１の外部装置又は前記第１の外部装置とは異なる第２の外部装置へ前記第２のデータと前記第２の生体データとを無線により送信し、前記第１の外部装置又は前記第２の外部装置から前記第２の生体データに基づく第２の生体認証の第２の結果データを無線により受信し、前記履歴情報に、前記第２の利用者情報と、前記第２の機能を示す第２の識別情報と、前記第２の結果データと

、第２の時間情報とを関連付けた第２の情報を加える、
集積回路。
【請求項２】
前記メモリは、設定情報をさらに記憶しており、
前記設定情報は、前記第１の識別情報と前記第１の利用者識別情報とを関連付けており、前記第２の識別情報と前記第２の利用者識別情報とを関連付けている、
請求項１の集積回路。
【請求項３】
メモリとプロセッサとを具備し、
前記メモリは、決済のための第１の機能で用いられる第１のデータと、前記第１の機能を利用可能な第１の利用者の第１の生体データと、前記第１の利用者を示す第１の利用者識別情報と、前記第１の機能と異なる第２の機能で用いられる第２のデータと、前記第２の機能を利用可能であり前記第１の利用者と異なる第２の利用者の第２の生体データと、前記第２の利用者を示す第２の利用者識別情報と、前記第２の機能を利用可能であり前記第１の利用者及び前記第２の利用者と異なる第３の利用者の第３の生体データと、前記第３の利用者を示す第３の利用者識別情報と、前記第１の機能と前記第２の機能とに関する履歴情報と、を記憶し、
前記プロセッサは、
前記第１の利用者が前記第１の機能を用いる場合に、第１の外部装置へ前記第１のデータと前記第１の生体データとを無線により送信し、前記第１の外部装置から前記第１の生体データに基づく第１の生体認証の第１の結果データを無線により受信し、前記履歴情報に、前記第１の利用者識別情報と、前記第１の機能を示す第１の識別情報と、前記第１の結果データと、第１の時間情報とを関連付けた第１の情報を加え、
前記第２の利用者又は前記第３の利用者が前記第２の機能を用いる場合に、前記第１の外部装置又は前記第１の外部装置とは異なる第２の外部装置へ、前記第２のデータと、前記第２の生体データと前記第３の生体データとのうちの生体認証候補データとを無線により送信し、前記第１の外部装置又は前記第２の外部装置から前記生体認証候補データに基づく第２の生体認証の第２の結果データを無線により受信し、前記第２の結果データが前記第２の生体認証の成功を示す場合に、前記履歴情報に、前記生体認証候補データに対応する利用者識別情報と、前記第２の機能を示す第２の識別情報と、前記第２の結果データと、第２の時間情報とを関連付けた第２の情報を加える、
集積回路。
【請求項４】
前記メモリは、設定情報をさらに記憶しており、
前記設定情報は、前記第１の識別情報と、前記第１の利用者識別情報とを関連付けており、前記第２の識別情報と、前記第２の利用者識別情報及び前記第３の利用者識別情報とを関連付けている、
請求項３の集積回路。
【請求項５】
メモリとプロセッサとを具備し、
前記メモリは、決済のための第１の機能で用いられる第１のデータと、前記第１の機能を利用可能な第１の利用者の第１の生体データと、前記第１の利用者を示す第１の利用者識別情報と、前記第１の機能と異なる第２の機能で用いられる第２のデータと、前記第２の機能を利用可能であり前記第１の利用者と異なる第２の利用者の第２の生体データと、前記第２の利用者を示す第２の利用者識別情報と、複数の利用者に対して利用を許可する第３の機能で用いられる第３のデータと、前記第１の機能乃至前記第３の機能に関する履歴情報と、を記憶し、
前記プロセッサは、
前記第１の利用者が前記第１の機能を用いる場合に、第１の外部装置へ前記第１のデータと前記第１の生体データとを無線により送信し、前記第１の外部装置から前記第１の生

体データに基づく第１の生体認証の第１の結果データを無線により受信し、前記履歴情報に、前記第１の利用者識別情報と、前記第１の機能を示す第１の識別情報と、前記第１の結果データと、第１の時間情報とを関連付けた第１の情報を加え、
前記第２の利用者が前記第２の機能を用いる場合に、前記第１の外部装置又は前記第１の外部装置とは異なる第２の外部装置へ前記第２のデータと前記第２の生体データとを無線により送信し、前記第１の外部装置又は前記第２の外部装置から前記第２の生体データに基づく第２の生体認証の第２の結果データを無線により受信し、前記履歴情報に、前記第２の利用者情報と、前記第２の機能を示す第２の識別情報と、前記第２の結果データと、第２の時間情報とを関連付けた第２の情報を加え、
前記複数の利用者のうちのいずれかが前記第３の機能を用いる場合に、前記第１の外部装置、前記第２の外部装置、又は、前記第１の外部装置及び前記第２の外部装置とは異なる第３の外部装置へ前記第３のデータを無線により送信し、前記履歴情報に、前記第３の機能を示す第３の識別情報と、第３の時間情報とを関連付けた第３の情報を加える、
集積回路。
【請求項６】
前記メモリは、設定情報をさらに記憶しており、
前記設定情報は、前記第１の識別情報と前記第１の利用者識別情報とを関連付けており、前記第２の識別情報と前記第２の利用者識別情報とを関連付けており、前記第３の識別情報には利用者識別情報を関連付けていない、
請求項５の集積回路。
【請求項７】
メモリとプロセッサとを具備し、
前記メモリは、決済のための第１の機能で用いられる第１のデータと、前記第１の機能を利用可能な第１の利用者の第１の生体データと、前記第１の利用者を示す第１の利用者識別情報と、前記第１の機能と異なる第２の機能で用いられる第２のデータと、前記第２の機能を利用可能であり前記第１の利用者と異なる第２の利用者の第２の生体データと、前記第２の利用者を示す第２の利用者識別情報と、前記第２の機能を利用可能であり前記第１の利用者及び前記第２の利用者と異なる第３の利用者の第３の生体データと、前記第３の利用者を示す第３の利用者識別情報と、複数の利用者に対して利用を許可する第３の機能で用いられる第３のデータと、前記第１の機能乃至前記第３の機能に関する履歴情報と、を記憶し、
前記プロセッサは、
前記第１の利用者が前記第１の機能を用いる場合に、第１の外部装置へ前記第１のデータと前記第１の生体データとを無線により送信し、前記第１の外部装置から前記第１の生体データに基づく第１の生体認証の第１の結果データを無線により受信し、前記履歴情報に、前記第１の利用者識別情報と、前記第１の機能を示す第１の識別情報と、前記第１の結果データと、第１の時間情報とを関連付けた第１の情報を加え、
前記第２の利用者又は前記第３の利用者が前記第２の機能を用いる場合に、前記第１の外部装置又は前記第１の外部装置とは異なる第２の外部装置へ、前記第２のデータと、前記第２の生体データと前記第３の生体データとのうちの生体認証候補データとを無線により送信し、前記第１の外部装置又は前記第２の外部装置から前記生体認証候補データに基づく第２の生体認証の第２の結果データを無線により受信し、前記第２の結果データが前記第２の生体認証の成功を示す場合に、前記履歴情報に、前記生体認証候補データに対応する利用者識別情報と、前記第２の機能を示す第２の識別情報と、前記第２の結果データと、第２の時間情報とを関連付けた第２の情報を加え、
前記複数の利用者のうちのいずれかが前記第３の機能を用いる場合に、前記第１の外部装置、前記第２の外部装置、又は、前記第１の外部装置及び前記第２の外部装置とは異なる第３の外部装置へ前記第３のデータを無線により送信し、前記履歴情報に、前記第３の機能を示す第３の識別情報と、第３の時間情報とを関連付けた第３の情報を加える、
集積回路。

【請求項８】
前記メモリは、設定情報をさらに記憶しており、
前記設定情報は、前記第１の識別情報と、前記第１の利用者識別情報とを関連付けており、前記第２の識別情報と、前記第２の利用者識別情報及び前記第３の利用者識別情報とを関連付けており、前記第３の識別情報には利用者識別情報を関連付けていない、
請求項７の集積回路。
【請求項９】
前記メモリは、新たなソフトウェアを記憶し、
前記プロセッサは、新たな機能として前記メモリの前記新たなソフトウェアを実行する、
請求項１乃至請求項８のうちのいずれか１項の集積回路。
【請求項１０】
前記第２の機能は、キー機能であり、
前記第３の機能は、ポイントカード機能である、
請求項５乃至請求項８のうちのいずれか1項の集積回路。
【請求項１１】
前記プロセッサは、前記第１の生体認証と前記第２の生体認証のうちの少なくとも１つが失敗である場合に、失敗と判断された機能、又は、全機能を、使用禁止状態へ変更する、
請求項１乃至請求項１０のうちのいずれか１項の集積回路。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、集積回路に関する。
【背景技術】
【０００２】
偽のサイン、暗証番号の解析、スキミング、カード偽造、親族による無断利用などのようなクレジットカードの不正利用は、増加している。
【０００３】
カード決済の不正利用を防止するため、近年ではセキュリティの高い生体認証が用いられる場合がある。
【０００４】
生体認証に基づいて利用者を確認するシステムの一例として、銀行の預貯金の残高照会、入出金、振込処理を行う現金自動預け払い機（ＡＴＭ）などがある。このような銀行システムにおいて、ＡＴＭは、利用者の生体データを取得して銀行のサーバに送信する。サーバは、ＡＴＭから受信した利用者の生体データと、データベースに記憶されている生体データとを照合する生体認証を実行する。
【０００５】
また、クレジットカードに指紋センサが取り付けられており、クレジットカード内部でクレジットカードに記憶されている指紋データと指紋センサによって取得された利用者の指紋データとを照合する技術がある。
【０００６】
さらに、カード決済端末がクレジットカードに記憶されている生体データを取得し、当該カード決済端末に備えられているセンサによって利用者の生体データを取得し、カード決済端末が取得された生体データを照合する技術が、特許第５７１３５１６号に開示されている。
【先行技術文献】
【特許文献】
【０００７】
【特許文献１】特許第５７１３５１６号公報

【発明の概要】
【発明が解決しようとする課題】
【０００８】
しかしながら、クレジットカードに記憶されている生体データをカード決済ではない他の機能に利用することについては上記の技術で検討されていない。
【０００９】
本発明は上記実情を考慮してなされたものであり、ユーザに決済機能を含む多機能を提供可能であり、利用履歴を記憶する集積回路に関する。
【課題を解決するための手段】
【００１０】
本実施形態によれば、集積回路は、メモリとプロセッサとを具備する。メモリは、決済のための第１の機能で用いられる第１のデータと、第１の機能を利用可能な第１の利用者の第１の生体データと、第１の利用者を示す第１の利用者識別情報と、第１の機能と異なる第２の機能で用いられる第２のデータと、第２の機能を利用可能であり第１の利用者と異なる第２の利用者の第２の生体データと、第２の利用者を示す第２の利用者識別情報と、第１の機能と第２の機能とに関する履歴情報と、を記憶する。プロセッサは、第１の利用者が第１の機能を用いる場合に、第１の外部装置へ第１のデータと第１の生体データとを無線により送信し、第１の外部装置から第１の生体データに基づく第１の生体認証の第１の結果データを無線により受信し、履歴情報に、第１の利用者識別情報と、第１の機能を示す第１の識別情報と、第１の結果データと、第１の時間情報とを関連付けた第１の情報を加え、第２の利用者が第２の機能を用いる場合に、第１の外部装置又は第１の外部装置とは異なる第２の外部装置へ第２のデータと第２の生体データとを無線により送信し、第１の外部装置又は第２の外部装置から第２の生体データに基づく第２の生体認証の第２の結果データを無線により受信し、履歴情報に、第２の利用者情報と、第２の機能を示す第２の識別情報と、第２の結果データと、第２の時間情報とを関連付けた第２の情報を加える。
【発明の効果】
【００１１】
本発明によれば、決済機能を含む多機能カードの利用履歴を記録することができる。
【図面の簡単な説明】
【００１２】
【図１】第１の実施形態に多機能カードの構成の一例を示すブロック図。
【図２】第１の実施形態に係る多機能カードに備えられる機複数の能を例示するブロック図。
【図３】第１の実施形態に係る設定情報の一例を示すデータ構造図。
【図４】第１の実施形態に係る履歴情報の一例を示すデータ構造図。
【図５】第１の実施形態に係る多機能カードの設定処理の一例を示すフローチャート。
【図６】第１の実施形態に係る多機能カードの利用処理の一例を示すフローチャート。
【図７】第２の実施形態に係るカード決済端末と周辺機器の構成の一例を示すブロック図。
【図８】第２の実施形態に係る決済データの第１の例を示すデータ構造図。
【図９】第２の実施形態に係る決済データの第２の例を示すデータ構造図。
【図１０】第２の実施形態に係る決済データの第３の例を示すデータ構造図。
【図１１】第２の実施形態に係る与信結果データの一例を示すデータ構造図。
【図１２】第２の実施形態に係るカード決済端末の処理を例示するフローチャート。
【図１３】第２の実施形態に係るサインデータ照合処理を例示するフローチャート。
【図１４】第３の実施形態に係るカード決済システムの構成の一例を示すブロック図。
【図１５】第３の実施形態に係る個人情報の設定処理を例示するフローチャート。
【図１６】第３の実施形態に係るセキュリティサービスにおける処理を例示するフローチャート。

【発明を実施するための形態】
【００１３】
以下、本発明の実施形態を、図面を参照して説明する。なお、以下の説明において、略又は実質的に同一の機能及び構成要素については、同一符号を付し、必要な場合にのみ説明を行う。
【００１４】
［第１の実施形態］
本実施形態においては、カード決済機能に加えて他の機能を含む多機能カードについて説明する。多機能カードは、生体データを記憶する。
【００１５】
本実施形態において、識別情報はＩＤと称する。
【００１６】
図１は、本実施形態に係る多機能カードの構成の一例を示すブロック図である。
【００１７】
多機能カード１は、例えば、カード形状のカード本体１Ａと、カード本体１Ａに備えられる集積回路２とを含む。集積回路２は、例えば、ＩＣ（Integrated Circuit）チップでもよい。この集積回路２は、通信部３、プロセッサ４、メモリ５Ａ～５Ｃを含む。
【００１８】
多機能カード１は、情報処理装置８又は生体認証装置９と連携して動作する。
【００１９】
情報処理装置８は、例えば、カード・ライタ８Ａにより、信号、コマンド、ソフトウェア、プログラム、データ、設定情報、利用者ＩＤ、ソフトウェアＩＤ、データＩＤ、その他の各種情報、などを送信する。
【００２０】
生体認証装置９は、カード・リーダ／ライタ９Ａ、生体センサ９Ｂ、照合部９Ｃを含む。カード・リーダ／ライタ９Ａは、多機能カード１から信号、コマンド、データ、情報などを受信し、又は、多機能カード１へ信号、コマンド、データ、情報などを送信する。生体センサ９Ｂは、多機能カード１の利用者の生体データを取得する。照合部９Ｃは、生体センサ９Ｂによって取得された生体データと、多機能カード１からカード・リーダ／ライタ９Ａ経由で受信された生体データとを照合し、生体認証を実行する。そして、照合部９Ｃは、生体認証結果を、カード・リーダ／ライタ９Ａ経由で、多機能カード１へ送信する。
【００２１】
生体認証装置９は、例えば、店舗に備えられるカード決済端末でもよく、各種の情報処理装置でもよい。情報処理装置としては、例えば、パーソナルコンピュータ、スマートフォンなどの携帯電話、タブレット型コンピュータなどでもよい。
【００２２】
多機能カード１は、例えば、クレジットカードとしての機能、デビッドカードとしての機能、プリペイトカードとしての機能のうちの、少なくとも１つのカード決済機能６１を含むとしてもよい。本実施形態では、説明を簡略化するため、カード決済機能６１はクレジットカードとしての機能である場合を例として説明する。
【００２３】
本実施形態において、多機能カード１は、複数の利用者のそれぞれに対応する複数の生体データ７１～７Ｎを含むとする。このように、多機能カード１に複数の生体データ７１～７Ｎが含まれている場合、例えば、家族、社員などの任意のグループに所属する複数の利用者で多機能カード１を共用することが可能になる。しかしながら、本実施形態において、多機能カード１をクレジットカードとして用いることが許可される利用者は一人であるとする。なお、複数の利用者が多機能カード１をクレジットカードとして利用可能でもよい。
【００２４】

多機能カード１が一人の利用者にのみ専属的に使用されることを前提とする場合、多機能カード１に含まれる生体データは一人の利用者に対応するとしてもよい。多機能カード１に含まれるカード決済機能６１ではない他の機能６２～６Ｍは、例えば、ポイントカード、乗車券（定期券）、社会保障カード、住民カード、印鑑カード、開錠カード、免許証、保険証、パスポート、自動車のキー、マイナンバーカード、ソーシャルセキュリティカード、又は、診察カードなどとしての機能でもよい。本実施形態において、例えば、カード決済機能６１では特定の一人の利用者について生体認証が成功した場合に多機能カード１を利用可能とする。ポイントカードなどのような第２の機能では生体認証を行うことなく多機能カード１を利用可能とする。自動車のキー又は開錠カードなどのような第３の機能では多機能カード１に記憶されている複数の生体データのうちのいずれかについて生体認証が成功した場合に多機能カード１を利用可能とする。

【００２５】

多機能カード１は、カード・ライタ８Ａ又はカード・リーダ／ライタ９Ａなどの装置から発せられる電波（電磁界）を通信部３のアンテナ回路３Ａで受け、この受けた電波を電気に変換し、集積回路２の電力として用いる。しかしながら、多機能カード１は、電源を備えるとしてもよい。

【００２６】

通信部３は、多機能カード１の設定時に、情報処理装置８に備えられるカード・ライタ８Ａから、接触又は非接触で、又は、有線又は無線で、信号、コマンド、ソフトウェア、プログラム、データ、設定情報、利用者ＩＤ、ソフトウェアＩＤ、データＩＤ、その他の各種情報、などを受信する。

【００２７】

通信部３は、多機能カード１の利用時に、カード・リーダ／ライタ９Ａと、接触又は非接触で、又は、有線又は無線で、信号、コマンド、データ、情報などを送信、又は、受信する。

【００２８】

プロセッサ４は、通信部３を制御し、メモリ５Ａ～５Ｃをアクセスする。より具体的には、プロセッサ４は、メモリ５Ａに記憶されている制御ソフトウェア１０を実行する。また、プロセッサ４は、メモリ５Ｂに記憶されている各種機能を実現するためのソフトウェア１１１～１１Ｋを実行可能である。プロセッサ４は、メモリ５Ｃを作業メモリとして利用可能である。プロセッサ４は、メモリ５Ａに記憶されている制御ソフトウェア１０を実行し、制御ソフトウェア１０に基づく制御にしたがって、メモリ５Ｂに記憶されている複数のソフトウェア１１１～１１Ｋのそれぞれを実行可能である。また、プロセッサ４は、メモリ５Ｂに新規のソフトウェアが追加された場合に、新規のソフトウェアを実行可能である。例えば、制御ソフトウェア１０はオペレーティング・システム（ＯＳ）としてもよい。例えば、ソフトウェア１１１～１１Ｋはアプリケーションとしてもよい。

【００２９】

例えば、メモリ５Ａ，５Ｂは、不揮発性メモリである。より具体的には、例えば、メモリ５Ａはリード・オンリー・メモリ（ＲＯＭ）としてもよく、メモリ５ＢはＥＰＲＯＭ（Erasable Programmable Read-Only Memory）又はＥＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory）としてもよい。

【００３０】

メモリ５Ｂは、ソフトウェアＩＤと関連付けられているソフトウェア１１１～１１Ｋ、利用者ＩＤと関連付けられている生体データ７１～７Ｎ、設定情報１２、履歴情報１３を記憶する。

【００３１】

ソフトウェア１１１～１１Ｋは、それぞれ各種の機能を実現するためのプログラムと当該プログラムに関する情報を含む。ソフトウェア１１１～１１Ｋを実行可能とすることにより、多機能カード１は、カード決済機能６１に加えて他の機能６２～６Ｍを実現可能である。例えば、ソフトウェア１１１はクレジットカードとしてのカード決済機能６１を実

現し、ソフトウェア１１２～１１Ｋはカード決済機能６１ではない他の機能６２～６Ｍを実現可能とする。

【００３２】

生体データ７１～７Ｎは、例えば指紋データ、静脈データ、動脈データ、掌形データ、網膜データ、虹彩データ、顔データ、血管データ、音声データ、声紋データ、又は、耳型データでもよい。

【００３３】

設定情報１２は、多機能カード１の制御ソフトウェア１０及びソフトウェア１１１～１１Ｋの動作で必要になる各種の情報を含む。例えば、設定情報１２は、多機能カード１のメモリ５Ｂに記憶されたソフトウェア１１１～１１Ｋを示すソフトウェアＩＤと、生体認証候補（対象）の利用者を示す利用者ＩＤとを関連付けて管理する情報である。これにより、例えば、多機能カード１は、一人の利用者に対してカード決済機能６１を許可し、例えば、ポイントカード機能を誰でも利用可能（生体認証不要）とし、例えば、複数の利用者に対して自動車のキーとしての機能を許可するなど、多機能カード１の機能に応じてセキュリティのレベルを設定可能である。

【００３４】

なお、多機能カード１が共用されることなく、特定の一人の利用者のみに利用されることを想定している場合、設定情報１２は、ソフトウェアＩＤと、生体認証が必要か否かを示す情報とを関連付けて管理するとしてもよい。

【００３５】

履歴情報１３は、例えば、多機能カード１が利用されるごとに、時間情報、利用対象のソフトウェアを示すソフトウェアＩＤ、生体認証が成功したか否かを示す情報、生体認証が成功した場合の認証された利用者を示す利用者ＩＤ、を関連付けて管理する情報である。

【００３６】

なお、多機能カード１が共用されることなく、特定の一人の利用者のみに利用されることを想定している場合、履歴情報１３に含まれる情報のうち、利用者ＩＤを省略してもよい。

【００３７】

各ソフトウェア１１１～１１Ｋは、制御ソフトウェア１０による制御にしたがって実行される。

【００３８】

ソフトウェア１１１は、例えば、プロセッサ４によって実行されることにより、カード側におけるカード決済機能６１を実現する。

【００３９】

ソフトウェア１１２は、例えば、プロセッサ４によって実行されることにより、カード側におけるポイントカード機能６２を実現する。

【００４０】

ソフトウェア１１３は、例えば、プロセッサ４によって実行されることにより、カード側における自動車キーの機能６３を実現する。

【００４１】

制御部４１は、プロセッサ４が制御ソフトウェア１０を実行することにより実現される。

【００４２】

制御部４１は、多機能カード１の設定時に、カード・ライタ８Ａから通信部３経由でソフトウェア１１１～１１Ｋ、ソフトウェアＩＤ、生体認証候補（対象）の利用者を示す利用者ＩＤ、生体データ７１～７Ｎ、生体データ７１～７Ｎに対応する利用者を示す利用者ＩＤを受信する。そして、制御部４１は、受信されたソフトウェアとソフトウェアＩＤとを関連付けてメモリ５Ｂに記憶する。制御部４１は、受信されたソフトウェアＩＤと生体認証候補の利用者を示す利用者ＩＤとを関連付けて設定情報１２を更新する。制御部４１

は、受信された生体データ７１～７Ｎと対応する利用者ＩＤとを関連付けてメモリ５Ｂに記憶する。

【００４３】

制御ソフトウェア１０は、例えば、ＯＳに含まれるとしてもよい。より具体的な例として、制御ソフトウェア１０は、マルチアプリケーションＯＳに含まれるとしてもよく、又は、仮想マシン（Virtual Machine）と呼ばれる汎用ＯＳに含まれるとしてもよい。しかしながら、制御ソフトウェア１０は、ＯＳに含まれるのではなく、ＯＳの制御にしたがって動作するソフトウェアでもよい。

【００４４】

制御部４１は、通信部３経由で受けたコマンドに基づいて、複数のソフトウェア１１１～１１Ｋのうちのどのソフトウェアを実行するか決定する。

【００４５】

制御部４１は、設定情報１２に基づいて、決定されたソフトウェアが生体認証を必要とするか否か判断する。

【００４６】

制御部４１は、決定されたソフトウェアが生体認証を必要としない場合に、決定されたソフトウェアを実行する。

【００４７】

制御部４１は、決定されたソフトウェアが生体認証を必要とする場合に、認証成功を示す認証結果を受けるまで、又は、設定情報１２において、決定されたソフトウェアに対して生体認証候補として設定されている全ての生体データに対する生体認証が終了するまで、順次、生体データを通信部３経由で、生体認証装置９へ送信する。そして、制御部４１は、生体認証装置９に備えられるカード・リーダ／ライタ９Ａから、通信部３経由で、認証結果を受信する。

【００４８】

制御部４１は、受信された認証結果が認証成功を示す場合に、決定されたソフトウェアを実行し、時間情報と、決定されたソフトウェアを示すソフトウェアＩＤと生体認証が成功であったことを示す認証結果と、生体認証の成功した利用者を示す利用者ＩＤとを関連付けてメモリ５Ｂの履歴情報１３を更新する。

【００４９】

制御部４１は、設定情報１２において、決定されたソフトウェアに対して生体認証候補として設定されている全ての生体データに対する生体認証が終了し、当該全ての生体認証候補の生体データに対する受信された認証結果が認証失敗を示す場合に、時間情報と、決定されたソフトウェアを示すソフトウェアＩＤと、生体認証が失敗であったことを示す認証結果とを関連付けてメモリ５Ｂの履歴情報１３を更新する。

【００５０】

制御部４１は、設定情報１２において、決定されたソフトウェアに対して生体認証候補として設定されている全ての生体データに対する生体認証が終了し、受信された認証結果の全てが認証失敗を示す場合に、多機能カード１のメモリ５Ｂの各種データを読み出し不可とし、これにより多機能カード１を保護してもよい。

【００５１】

制御部４１は、設定情報１２に基づいて、生体認証が失敗であると判断されたソフトウェアに基づく用途において、多機能カード１を使用可能状態から使用禁止状態へ変更してもよい。または、制御部４１は、設定情報１２に基づいて、生体認証が失敗であると判断されたソフトウェアが１つ以上存在する場合は、多機能カード１の全ての機能について使用可能状態から使用禁止状態へ変更してもよい。

【００５２】

図２は、本実施形態に係る多機能カード１に備えられる複数の機能を例示するブロック図である。

【００５３】

多機能カード１は、上述のように、カード決済機能６１、ポイントカード機能６２、自動車キーの機能６３、免許証の機能６４などを実現するためのソフトウェア１１１～１１Ｋを記憶する。ソフトウェア１１１～１１Ｋは、対応する機能を実現するために必要とされるデータを含む。

【００５４】

また、多機能カード１は、生体データ７１を記憶する。生体データ７１は、複数の機能で共有されてもよい。

【００５５】

例えば、生体センサ９Ｂを含むカード決済端末などのような生体認証装置９は、多機能カード１から生体データ７１を受信し、生体データ７１と生体センサ９Ｂによって取得された生体データとを照合し、認証結果を多機能カード１に送信する。

【００５６】

多機能カード１は、生体認証に成功した場合に、機能に対応するデータを生体認証装置９へ送信する。

【００５７】

図３は、本実施形態に係る設定情報１２の一例を示すデータ構造図である。

【００５８】

設定情報１２は、多機能カード１にインストールされたソフトウェアを示すソフトウェアＩＤと、生体認証が成功の場合に当該ソフトウェアの利用を許可する利用者を示す利用者ＩＤとを関連付ける。例えば、設定情報１２において、ソフトウェアＩＤに対して利用者ＩＤが関連付けられていない場合、当該ソフトウェアＩＤで示されるソフトウェアは、誰でも利用可能であり、生体認証が不要であることを示す。

【００５９】

図４は、本実施形態に係る履歴情報１３の一例を示すデータ構造図である。

【００６０】

履歴情報１３は、コマンドを受信した時間情報と、コマンドに対応するソフトウェアを示すソフトウェアＩＤと、生体認証結果と、生体認証が成功した場合の認証された利用者を示す利用者ＩＤと、を関連付けている。

【００６１】

図５は、本実施形態に係る多機能カード１の設定処理の一例を示すフローチャートである。

【００６２】

ステップＳ１において、通信部３は、情報処理装置８のカード・リーダ８Ａから、ソフトウェア、ソフトウェアＩＤ、生体認証候補の利用者を示す利用者ＩＤ、生体認証候補の利用者の生体データを受信する。このステップＳ１で受信されるソフトウェア、情報、データは、複数回に分けて受信されてもよい。

【００６３】

ステップＳ２において、制御部４１は、受信されたソフトウェアとソフトウェアＩＤとを関連付けてメモリ５Ｂに記憶する。

【００６４】

ステップＳ３において、制御部４１は、受信されたソフトウェアＩＤと生体認証候補の利用者を示す利用者ＩＤとを関連付けて設定情報１２を更新する。

【００６５】

ステップＳ４において、制御部４１は、受信された生体データと利用者ＩＤとを関連付けてメモリ５Ｂに記憶する。

【００６６】

なお、上記のステップＳ２からステップＳ４までに関しては、順序を自由に入れ替えてもよく、同時に実行されてもよい。

【００６７】

図６は、本実施形態に係る多機能カード１の利用処理の一例を示すフローチャートであ

る。
【００６８】
ステップＴ１において、通信部３は、生体認証装置９のカード・リーダ／ライタ９Ａから、コマンドを受信する。
【００６９】
ステップＴ２において、制御部４１は、生体認証が必要か否か判断する。具体的には、制御部４１は、設定情報４１において、コマンドの示すソフトウェアＩＤが利用者ＩＤと関係付けられているか否か判断する。
【００７０】
生体認証が不要な場合、処理はステップＴ８Ａに移る。
【００７１】
生体認証が必要な場合、ステップＴ３において、制御部４１は、生体認証候補の生体データをメモリ５Ｂから読み出す。具体的には、制御部４１は、設定情報１２において、コマンドの示すソフトウェアＩＤと関連付けられている利用者ＩＤを選択し、当該選択された利用者ＩＤと関連付けられている生体データをメモリ５Ｂから読み出す。
【００７２】
ステップＴ４において、通信部３は、読み出された生体データを、生体認証装置９へ送信する。
【００７３】
ステップＴ５において、通信部３は、生体認証装置９から生体認証結果を受信する。
【００７４】
ステップＴ６において、制御部４１は、生体認証結果が成功か又は失敗かを判断する。
【００７５】
生体認証結果が成功の場合、処理はステップＴ８Ｂに移る。
【００７６】
生体認証結果が失敗の場合、ステップＴ７において、制御部４１は、全ての生体認証候補の生体データに対して生体認証が実行されたか否か判断する。具体的には、制御部４１は、設定情報１２において、コマンドの示すソフトウェアＩＤと関連付けられている利用者ＩＤを生体認証候補の利用者ＩＤとし、生体認証候補の利用者ＩＤと関連付けられている生体データを生体認証候補の生体データとし、全ての生体認証候補の生体データに対して生体認証が実行されたか否か判断する。
【００７７】
全ての生体認証候補の生体データに対して生体認証が実行されたが、生体認証結果が成功ではない場合、処理はステップＴ８Ｃに移る。
【００７８】
全ての生体認証候補の生体データに対して生体認証が実行されていない場合、処理は、ステップＴ３に戻り、次の生体認証候補の生体データに対して同様の処理を実行する。
【００７９】
上記ステップＴ２において生体認証が不要と判断された場合、ステップＴ８Ａにおいて、制御部４１は、履歴情報１３に、時間情報とコマンドの示すソフトウェアＩＤとを関連付けて記憶する。
【００８０】
そして、ステップＴ９Ａにおいて、制御部４１は、コマンドの示すソフトウェアＩＤに関連付けられているソフトウェアを実行し、外部の装置で使用されるデータを通信部３経由で送信する。これにより、生体認証の必要ない用途に対して、多機能カード１を利用することができる。
【００８１】
上記ステップＴ６において生体認証が成功の場合、ステップＴ８Ｂにおいて、制御部４１は、履歴情報１３に、時間情報、ソフトウェアＩＤ、生体認証が成功であることを示す認証結果、認証された利用者ＩＤを関連付けて記憶する。

【００８２】
そして、ステップＴ９Ｂにおいて、制御部４１は、上記ステップＴ９Ａと同様に、コマンドの示すソフトウェアＩＤに関連付けられているソフトウェアを実行し、外部の装置で使用されるデータを通信部３経由で送信する。例えば、コマンドが決済コマンドの場合、制御部４１は、カード決済機能６１を実行し、カード決済端末のカード・リーダ／ライタ９Ａへ、生体認証の成功した利用者を示す利用者ＩＤと、当該利用者ＩＤに対応するカード番号、有効期限、氏名、住所、電話番号などを含む決済のためのデータを送信する。
【００８３】
上記ステップＴ７において全ての生体認証候補の生体データに対して生体認証が実行されたが生体認証結果が成功ではない場合、ステップＴ８Ｃにおいて、制御部４１は、履歴情報１３に、時間情報、ソフトウェアＩＤ、生体認証が失敗であることを示す認証結果を関連付けて記憶する。そして、ステップＴ８Ｃの後、処理は終了する。
【００８４】
以上説明した本実施形態においては、生体データ７１～７Ｎを含む多機能カード１を、様々な目的、機能、用途、又は、サービスで利用することができる。生体データ７１～７Ｎは、カード決済機能６１のみではなく、他の機能でも生体認証のために利用可能である。
【００８５】
本実施形態においては、多機能カード１の目的、機能、用途、又は、サービスに応じて、生体認証を行うか否かを設定することができる。
【００８６】
本実施形態においては、設定情報１２を用いることで、少なくとも一人の特定の利用者に対して生体認証が成功した場合に、例えば多機能カード１から生体認証装置９へデータの送信などの各種のサービスを提供することができる。
【００８７】
本実施形態においては、履歴情報１３に基づいて、多機能カード１の利用履歴を管理することができ、不正な使用を抑制することができる。
【００８８】
本実施形態においては、複数のカードの機能を１枚の多機能カード１に集約することができ、利用者のカードの管理負担を軽減することができ、利用者の利便性を増すことができ、利用者の不正使用を防止することができる。
【００８９】
本実施形態においては、例えば多機能カード１をカード決済に用いる場合には１人の利用者のみが利用可能とし、例えば多機能カード１を自動車のキーとして用いる場合には複数の利用者で共用可能とすることができる。
【００９０】
本実施形態において、例えば、パスワードに代えて生体データを用いることで、利用者はパスワードの管理及び変更の負担を解消することができる。
【００９１】
本実施形態において、生体認証が失敗した場合に、生体認証が失敗であると判断された機能または多機能カード１の全ての機能についてカードを使用禁止状態とすることで、多機能カード１のセキュリティを高めることができる。
【００９２】
［第２の実施形態］
以下、第２の実施形態に係るカード決済端末の実施形態を、図面を用いて説明する。
【００９３】
本実施形態においては、生体認証に用いられる生体データを記憶しているカードがクレジットカードの場合を例として説明する。しかしながら、生体データを記憶しているカードとしては、決済に用いられるものであれば、例えばデビッドカード、電子マネーカードなど各種のカードであってもよい。例えば、生体認証に用いられる生体データを記憶して

いるカードは、上記第１の実施形態に係る多機能カード１でもよい。

【００９４】

図７は、本実施形態に係るカード決済端末と周辺機器の構成の一例を示すブロック図である。

【００９５】

本実施形態において、利用者Ｕのカード Ｃは、カード形状のカード本体Ｃ１と、カード本体Ｃ１に備えられる集積回路Ｔとを含む。集積回路Ｔは、例えば、カードＩＤの一例であるカード番号２０１、有効期限２０２、利用者ＩＤの一例である氏名２０３、生体認証結果の一例である認証失敗フラグ２０４、生体データ２０５などを含むカードデータＤを記憶する。カードデータＤは、例えばカード発行時に既にカード Ｃに記憶されている。生体データ２０５としては、例えば、上記の生体データ７１～７Ｎと同様に、指紋パターン、虹彩パターン、静脈パターンなどが用いられ、生体認証において決済時に取得された利用者Ｕの生体データ２０６と照合される。また、１枚のカードを複数の契約者で利用することができるようにするため、生体データ２０５及び氏名２０３には複数の契約者のデータを含むことができる。利用者の識別方法については、後述する。

【００９６】

カード決済端末２００は、サイン入力装置２０７、生体センサ９Ｂの一例である生体データ取得装置２０８、カード端末２０９を備える。カード端末２０９は、カード・リーダ／ライタ９Ａの一例であるカードデータ読み書き装置２１０、決済受付装置２１１、照合部９Ｃの一例である処理装置２１２、通信装置２１３を備える。

【００９７】

カードデータ読み書き装置２１０は、利用者Ｕのカード Ｃに記憶されているカードデータＤを読み取り、カードデータＤを処理装置２１２に送る。また、カードデータ読み書き装置２１０は、処理装置２１２の指示により、カード Ｃに記憶されているカードデータＤを書き換えることができる。

【００９８】

さらに、カードデータ読み書き装置２１０は、カード Ｃに備えられている磁気記憶媒体Ｔ１に記憶されているカードデータＤ１を読み出し可能である。例えば、カードデータＤ１は、利用者ＩＤとカードＩＤとのうちの少なくとも一方の情報を含む。

【００９９】

決済受付装置２１１は、例えば加盟店の店員の操作に基づいて支払金額、支払方法（例えば一括払い、分割払い）などを受け付け、支払金額、支払方法を処理装置２１２に送る。

【０１００】

サイン入力装置２０７は、利用者Ｕのカード決済時のサインデータ２１４を取得し、サインデータ２１４をカード端末２０９の処理装置２１２に送る。なお、サイン入力装置２０７は、利用者Ｕが手書きでサインを入力でき、それを電子データとして処理装置２１２へ送ることができるものであればよい。例えば、サイン入力装置２０７はタッチペンによる電子サインが可能な装置であってもよいし、利用者Ｕによる紙媒体に対するサインを電子化する例えばスキャナまたはカメラなどのような装置であってもよい。

【０１０１】

さらにサイン入力装置２０７は、カード Ｃ裏面のサイン領域Ａに記載されている利用者ＵのサインＤ３を、電子データ（カード Ｃ上のサインデータ２２７）として取得可能である。サインＤ３の読み取り方法は、例えば利用者Ｕがサイン入力装置２０７に備えられているスキャナまたはカメラを用いてカード Ｃをスキャンするとしてもよい。

【０１０２】

サイン入力装置２０７は、カード Ｃ上のサインデータ２２７を処理装置２１２へ送る。

【０１０３】

生体データ取得装置２０８は、利用者Ｕのカード決済時の生体データ２０６を電子データとして取得し、生体データ２０６をカード端末２０９の処理装置２１２に送る。

【０１０４】
なお、本実施形態において、サイン入力装置２０７と生体データ取得装置２０８は別々の装置である必要はなく、一つの装置として実現されてもよい。この場合、処理装置２１２に送るデータは、生体データであるかサインデータであるかが区別されていなくてもよい。
【０１０５】
処理装置２１２は、生体データ取得装置２０８によって決済時の利用者Ｕの生体データ２０６が読み取られたか否か、さらにサイン入力装置２０７によって利用者Ｕのサインデータ２１４が読み取られたか否かを自動で判別する。
【０１０６】
処理装置２１２は、決済データ２１５を作成し、決済データ２１５を通信装置２１３へ送る。決済データ２１５については、図８乃至図１０を用いて後述する。
【０１０７】
なお、処理装置２１２はカード端末２０９における一連のカード認証処理を制御する。処理装置２１２によって実行される各種認証処理の詳細については、図１２を用いて後述する。
【０１０８】
処理装置２１２は、生体データ取得装置２０８によって生体データ２０６が取得されない場合に、カードＣの磁気記憶媒体Ｔ１から読み取られた利用者ＩＤとカードＩＤとのうちの少なくとも一方の情報と、サインデータ２１４と、支払金額とを関連付けてデータベースＤＢに格納してもよい。
【０１０９】
通信装置２１３は、ネットワーク経由で、アクワイアラのサーバ２１６に決済データ２１５を送信する。その後、決済データ２１５は、例えば、アクワイアラのサーバ２１６からカードブランドのサーバ２１７へ送信され、カードブランドのサーバ２１７からイシュアのサーバ２１８へ送信される。例えば、通信装置２１３は、決済データ２１５を、イシュアのサーバを宛先として送信する。なお、通信装置２１３は、アクワイアラのサーバ２１６とカードブランドのサーバ２１７とのうちの一方を経由して、イシュアのサーバ２１８へ決済データ２１５を送信してもよい。
【０１１０】
また、通信装置２１３は、イシュアのサーバ２１８から、カードブランドのサーバ２１７、アクワイアラ２１６を経由して、与信結果データ２１９を受信し、受信した与信結果データ２１９を処理装置２１２へ送る。例えば、イシュアのサーバ２１８は、与信結果データ２１９を、カード決済端末２００を宛先として送信する。なお、イシュアのサーバ２１８は、アクワイアラのサーバ２１６とカードブランドのサーバ２１７とのうちの一方を経由して、カード決済端末２００へ与信結果データ２１９を送信してもよい。処理装置２１２は、与信結果データ２１９に基づいて、決済完了または決済不成立を判定する。与信結果データ２１９の詳細については、図１１を用いて後述する。
【０１１１】
データベースＤＢは、例えば加盟店に設置される端末に含まれており、加盟店が顧客との過去の取引の際に使用したデータを記憶する。このデータは、例えば顧客との取引毎に、取引ＩＤ２２０を付して記憶され、顧客ＩＤ２２１、品物名と金額となどを含む取引データ２２２、品物の発送先と日時などを含む発送データ２２３、カードに関する情報と支払金額などを含む決済・認証データ２２４、などを含む。決済・認証データ２２４は、カード情報２２５、支払金額２２６、生体認証の場合であれば被認証者（認証対象の利用者）ＩＤ２２８を含む。
【０１１２】
カード情報２２５は、カードデータ読み書き装置２１０によって取得されたカードデータＤに含まれる各データのうち、加盟店側で必要な情報が記憶される。
【０１１３】

なお、決済・認証データ２２４は、被認証者ＩＤ２２８を除く部分については、カード端末２０９からサーバ２１６へ送信される決済データ２１５と同等の内容を含むが、両者は一致しなくともよい。また、取引データ２２２、発送データ２２３、決済・認証データ２２４は、上記で説明した情報と異なる他の情報を含んでいてもよい。

【０１１４】

データベースＤＢは、カード端末２０９と接続されており、例えばカード端末２０９の処理装置２１２に設けられたデータベースインタフェースを介してカード端末２０９との間でデータの送受信を行うことができる。

【０１１５】

図８は、本実施形態に係る決済データ２１５の第１の例を示すデータ構造図である。決済データ２１５ａは、カード端末２０９とサーバ２１６との間で通信が行われる際に作成される。決済データ２１５ａは、図８の決済データ２１５ａを基本とするが、状況に応じて図９の決済データ２１５ｂ、図１０の決済データ２１５ｃのいずれかとなる場合もある。

【０１１６】

決済データ２１５ａは、カード番号２０１、有効期限２０２、氏名２０３、支払金額２２６、支払方法２２９、加盟店情報２３０などを含むが、他の情報を含むとしてもよい。

【０１１７】

加盟店情報２３０は、加盟店の名称、住所、又は、業態など、加盟店を特定する情報を含む。

【０１１８】

図９は、本実施形態に係る決済データ２１５の第２の例を示すデータ構造図である。

【０１１９】

利用者Ｕの生体データ２０６の取得は完了したがカードデータＤに生体データ２０５が含まれていない場合は、サーバ２１６～２１８のいずれかで生体認証を実行するために、カード端末２０９は、決済データ２１５ａに生体データ２０６を加えた決済データ２１５ｂを作成し、決済データ５ｂをサーバ２１６へ送信する。

【０１２０】

サーバ２１６又はサーバ２１７が決済データ２１５ｂを受信すると、サーバ２１６又はサーバ２１７は、生体データ２０６と照合するための生体データを記憶しているか否か判断する。サーバ２１６又はサーバ２１７が生体データ２０６と照合するための生体データを記憶している場合、サーバ２１６又はサーバ２１７は、決済データ２１５ｂに含まれる生体データ２１５ｂと記憶している生体データとに基づいて照合を行う。サーバ２１６又はサーバ２１７が生体データ２０６と照合するための生体データを記憶していない場合、サーバ２１６又はサーバ２１７は、決済データ２１５ｂをサーバ２１７又はサーバ２１８へ送信する。

【０１２１】

図１０は、本実施形態に係る決済データ２１５の第３の例を示すデータ構造図である。

【０１２２】

カード端末２０９、サーバ２１６、又は、サーバ２１７は、カードＣに記憶されている生体データ２０５、サーバ２１６に記憶されている生体データ、又は、サーバ２１７に記憶されている生体データと、生体データ２０６とを照合し、生体認証成功の場合に、上記図９の決済データ２１５ｂの生体データ２０６に代えて、認証成功通知２３１を含む決済データ２１５ｃを作成する。そして、カード端末２０９、サーバ２１６、又は、サーバ２１７は、決済データ２１５ｃを、サーバ２１６、サーバ２１７、又は、サーバ２１８に送信する。

【０１２３】

認証成功通知２３１は、生体認証を実行した者を特定する認証実行者ＩＤ２３２と、生体認証された者を特定する被認証者ＩＤ２３３を含む。

【０１２４】

処理装置２１２で生体認証が成功した場合、認証実行者ＩＤ２３２は、例えば、カード決済端末２００を利用する加盟店のＩＤ、カード決済端末２００のＩＤ、加盟店の口座情報などとしてもよい。

【０１２５】

サーバ２１６又はサーバ２１７で生体認証が成功した場合、認証実行者ＩＤ２３２は、例えば、サーバ２１６を管理・運営するアクワイアラＩＤ又はサーバ２１７を管理・運営するカードブランドＩＤでもよい。

【０１２６】

被認証者ＩＤ２３３は、認証された人物を特定可能であれば、例えば固有のＩＤであってもよいし、氏名でもよい。

【０１２７】

なお、カード決済端末２００で、生体データ２０６と生体データ２０５との照合による生体認証が失敗した場合は、この時点で決済不成立となり、サーバ２１６、サーバ２１７、又は、サーバ２１８との通信が不要であり、決済データ２１５は作成されなくてもよい。

【０１２８】

図１１は、本実施形態に係る与信結果データ２１９の一例を示す図である。

【０１２９】

与信結果データ２１９は、与信結果２３４、生体認証実行フラグ２３５を含む。与信結果データ２１９は、生体認証が実行され、生体認証が成功した場合に、さらに被認証者ＩＤ２３６を含む。

【０１３０】

与信結果２３４は、与信結果がＯＫであるかＮＧであるかを示し、例えば１ビットのフラグで表現されていてもよい。

【０１３１】

生体認証実行フラグ２３５は、生体認証が行われたか否かを示し、例えば１ビットのフラグで表現されてもよい。

【０１３２】

被認証者ＩＤ２３６は、与信結果データ２１９がどの被認証者に対応する情報であるかを示す。また、被認証者ＩＤ２３６により、与信結果データ２１９がどの決済データ２１５に対応するか関連付けることが可能である。

【０１３３】

図１２は、カード決済端末２００の処理を例示するフローチャートである。

【０１３４】

ステップＳ１２０１において、加盟店でカード決済端末２００の電源がＯＮされ、生体データ取得装置２０８、サイン入力装置２０７及びカード端末２０９が入力待ちとなる。

【０１３５】

ステップＳ１２０２において、カード端末２０９は、決済受付装置２１１を用いた決済受付処理を実行する。例えば、決済受付処理では、商品又はサービスの支払金額と支払方法とが受け付けられる。

【０１３６】

ステップＳ１２０３において、カード端末２０９は、カードデータ読み書き装置２１０を用い、カードデータ読み取り処理を実行する。例えば、カードデータ読み取り処理では、カードデータＤ用のデータ記憶領域が初期化され、カードデータＤの読み取りが実行される。カードデータＤが読み取られた場合には、カードデータＤがカードデータＤ用のデータ記憶領域に記憶される。例えば３回などの所定の回数、カードデータＤの読み取りが失敗した場合には、エラーが表示される。

【０１３７】

ステップＳ１２０４において、カード端末２０９は、サイン入力装置２０７または生体データ取得装置２０８を用いてサインデータ２１４または生体データ２０６の取得処理を

実行する。例えば、サインデータ２１４または生体データ２０６用に確保されているデータ記憶領域が初期化され、データ記憶領域に取得したデータが記憶される。

【０１３８】

ステップＳ１２０５において、カード端末２０９は、取得データがサインデータであるか生体データであるかの自動判別処理を行う。判別処理は、例えば各データの特徴またはパターンを認識することにより行われてもよい。例えば、指紋データであれば、取得データは画像データであり、画像上に層状の線が多数存在する特徴を有する。例えば、指静脈データであれば、時間と振幅に関する２次元データが取得され、振幅は一定間隔で拍動を示す特徴を有する。また、例えばサインデータであれば、取得データは画像データであり、線状の文字または図形で表現される特徴を有する。

【０１３９】

上記のステップＳ１２０５において、取得データがサインデータであると判定された場合、ステップＳ１２０６において、カード端末２０９は、サインデータ照合処理を行う。サインデータ照合処理の詳細については、図１３を用いて後述する。

【０１４０】

上記のステップＳ１２０５において、取得データが生体データであると判定された場合、ステップＳ１２０７においてカード端末２０９は生体認証処理を行う。

【０１４１】

ステップＳ１２０８において、カード端末２０９は、決済データ２１５の作成、サーバ２１６への決済データ２１５の送信、およびサーバ２１６からの与信結果データ２１９の受信を行う。与信結果データ２１９により、決済不成立と判断された場合は、取引の中止が実行される。

【０１４２】

なお、上記のステップＳ１２０７にて生体認証を行う際、カード端末２０９は、取得済のカードデータＤに生体データ２０５が含まれているかどうかをチェックする。

【０１４３】

カードデータＤに生体データ２０５が含まれていない場合には、カード端末２０９での生体認証を行うことができない。この場合は、上記のステップＳ１２０８においてサーバ２１６に生体データ取得装置２０８が取得した生体データ２０６を含んだ決済データ２１５ｂを送付した後、上述のようにサーバ２１６乃至サーバ２１８のいずれかのサーバにおいて生体認証が実行される。

【０１４４】

カードデータＤに生体データ２０５が含まれている場合、カード端末２０９は、生体認証を実行する。カード端末２０９における生体認証が失敗となった場合は、この時点で決済不成立となる。従って、この場合は上記のステップＳ１２０８において決済データ２１５の作成、サーバ２１６に対する決済データ２１５の送信、およびサーバ２１６からの与信結果データ２１９の受信は行われなくてもよい。

【０１４５】

カードデータＤに記憶されている生体データ２０５が複数人数分である場合には、カード端末２０９またはサーバ２１６乃至サーバ２１８のいずれかのサーバは、生体データ取得装置２０８が取得した生体データ２０６と照合完了するか、又は、複数人数分の生体データの全てに対して照合が実行されるまで、複数人数分の生体データのうちの照合候補の生体データについて順番に照合を行う。照合完了した場合には、カード端末２０９またはサーバ２１６乃至サーバ２１８のいずれかのサーバは、照合被認証者ＩＤを得る。

【０１４６】

ステップ１２０９において、カード端末２０９は、取引ＩＤ２２０、取引データ２２２、発送データ２２３、決済・認証データ２２４をデータベースＤＢへ登録する。

【０１４７】

上記のステップＳ１２０７またはステップＳ１２０８において生体認証が行われた場合は、カード端末２０９は、カード端末２０９またはサーバ２１６乃至サーバ２１８のいず

れかのサーバで生体認証が成功となった場合に、処理装置２１２を経由してデータベースＤＢに被認証者ＩＤを格納する。

【０１４８】

なお、サーバ２１６乃至サーバ２１８のいずれかのサーバにおける生体認証結果は、処理装置２１２が与信結果データ２１９に基づいて判定することができる。処理装置２１２は、生体認証が実行済であるか否かを、与信結果データ２１９に含まれる生体認証実行フラグ２３５により判定する。処理装置２１２は、生体認証が実行済であると判定した場合は、被認証者ＩＤの有無を確認する。被認証者ＩＤがない場合は、生体認証が失敗したと判定し、被認証者ＩＤがある場合は、生体認証が成功したと判定する。

【０１４９】

ステップ１２１０において、カード端末２０９は、生体認証またはサインデータ照合が失敗した場合、その旨を通知する。例えば、カード端末２０９は、カード決済端末２００が備えるディスプレイまたはスピーカより、生体認証失敗またはサインデータ照合失敗を表示又は音声出力してもよい。

【０１５０】

また、カード端末２０９は、通信手段を用いて利用者Ｕへ通知してもよい。例えば予めデータベースＤＢに利用者Ｕのメールアドレスを登録しておき、処理装置２３は、データベースＤＢにおけるメールアドレスを参照し、通信装置２１３を用いて利用者Ｕ宛のメールを送信してもよい。

【０１５１】

サーバ２１６乃至サーバ２１８のいずれかのサーバで生体認証が行われ、生体認証が失敗となった場合は、利用者Ｕへの通知は、生体認証が失敗となったサーバにより行われてもよい。

【０１５２】

また、カード端末２０９は、生体認証またはサインデータ照合が成功した場合においても、成功の旨を表示又は音声出力するとしてもよい。

【０１５３】

ステップ１２１１において、カード端末２０９は、生体認証が失敗であると判定した場合、処理装置２１２によりカードデータ読み書き装置２１０に対して認証失敗フラグ２０４の書き込み指示を送信する。カードデータ読み書き装置２１０は、カードＣに対して認証失敗フラグ２０４を書き込む。

【０１５４】

生体認証に失敗した場合、第三者がカードを不正利用している可能性が高い。そのため、本実施形態においてカード端末２０９は、例えば認証失敗フラグ２０４を書き込まれたカードＣは次回カード端末２０９で読み込まれる際に使用不可と判定することで、カードのセキュリティを高めることができる。

【０１５５】

ステップＳ１２１２において、カード端末２０９は、継続使用の場合にステップＳ１２０２に戻る。継続使用されない場合、ステップＳ１２１３において、カード決済端末２００は、電源をＯＦＦする。

【０１５６】

図１３は、サインデータ照合処理を例示するフローチャートである。

【０１５７】

ステップＳ１３０１において、サイン入力装置２０７は、カードＣのサインＤ３を読み取り、読み取りに成功した場合、カードＣ上のサインデータ２２７として保持する。

【０１５８】

サイン入力装置２０７はサインＤ３の読み取りに失敗した場合（ステップＳ１３０２）、ステップ１３０１に戻り再度カードＣ上のサインデータ２２７の読み取りを行う。規定回数以上サインＤ３の読み取りに失敗した場合は（ステップＳ１３０３）、サインデータの照合失敗となり、処理を終了するとしてもよい。サインＤ３の読み取り失敗および成功

の判定は、例えばカードＣ上のサイン領域Ａを画像処理等により自動判別し、サイン領域Ａが正常に取得できているか否かを判定基準としてもよい。なお、カードＣ上のサインデータ２２７の読み取り失敗および成功の判定は、処理装置２１２が行うとしてもよい。

【０１５９】

ステップＳ１３０２において、カードＣ上のサインデータ２２７の読み取りが成功した場合、処理装置２１２は、カードＣ上のサインデータ２２７と、ユーザＵが入力したサインデータ２１４を照合する（ステップＳ１３０４）。

【０１６０】

カードＣ上のサインデータ２２７と、ユーザＵが入力したサインデータ２１４とが類似していると判定され、照合成功の場合は、本人確認が行われたことになり、照合処理は完了する。カードＣ上のサインデータ２２７と、ユーザＵが入力したサインデータ２１４とが非類似と判定された場合、またはステップＳ１３０２においてカードＣ上のサインデータ２２７が取得できなかった場合は、照合失敗となり、上述のステップＳ１２１０において、利用者への通知が行われる。

【０１６１】

なお、サインデータの照合処理は、例えばパターンマッチング等の画像照合技術により自動的に行われることが望ましいが、カード決済端末２００を操作している店員などの目視による確認などのように、その他の方法により行われてもよい。

【０１６２】

複数人の生体データを記憶したカード、すなわち複数人が使用可能なカードでは、複数人がサイン入力を使用するとサインデータは毎回変化することとなる。このため、複数人のうちの特定の一人のみが、サイン入力を許可されるとしてもよい。また、複数人が使用可能なカードでは、サイン入力は使用不可としてもよい。例えば、複数人が使用可能なカードでは、上記図１２のステップＳ１２０５において取得データがサインデータであると判定された時点で、取引を停止してもよく、カード決済端末２００を操作している店員へ取引不可を通知してもよく、利用者Ｕへの通知または警告を行ってもよい。

【０１６３】

なお、サインデータを生体データと同様にカード内に記憶しておくことが可能であれば、サインデータ入力の場合でも、後述する生体データ認証の場合と同様に認証を行うことができ、複数人によって使用可能なカードであってもサイン照合を適用可能である。

【０１６４】

本実施形態において、カード決済端末２００は、カード決済サービスの加盟店に設置される場合を例として説明したが、カード決済端末２００は利用者Ｕの生体データ２０６もしくはサインデータ２１４、カードＣのカードデータＤを取得可能な他の装置でもよい。例えば、カード決済端末２００は、生体データ取得機能、カードデータ読み取り機能、決済受付機能、生体認証機能、通信機能を備えた情報処理装置でもよい。情報処理装置の各機能は、ソフトウェアで実現されてもよく、ハードウェアで実現されてもよく、ソフトウェアとハードウェアとの協働により実現されてもよい。情報処理装置の各機能を実現するために必要なハードウェアは、情報処理装置に内蔵されていてもよく、情報処理装置に外付けされてもよい。本実施形態に係る商品又はサービスの購入は、店舗で行われてもよく、ネットワーク上の電子商取引サイト又はサービス提供サイトで行われてもよい。情報処理装置としては、例えば、携帯電話機、パーソナルコンピュータ、タブレット型コンピュータなどが用いられる。

【０１６５】

本実施形態において、データベースＤＢに格納されているデータは顧客毎のデータであるとして説明したが、格納されているデータが取引毎のデータであってもよい。この場合、取引毎に例えば顧客の氏名又は顧客ＩＤ等、顧客を特定する情報の格納も必要となる。

【０１６６】

本実施形態において、カード決済時に利用者Ｕより取得するデータがサインデータもしくは生体データのみである場合を例として説明したが、これに加え、カード決済の一般的

な認証方法である暗証番号入力が選択可能であってもよい。
【０１６７】
上記の図１２及び図１３のフローチャートにおいて、各ステップの順序は、処理結果に影響を及ぼさない範囲で適宜変更されてもよい。
【０１６８】
本実施形態において、決済データ２１５，２１５ａ～２１５ｃは、複数に分割されてもよい。
【０１６９】
以下、具体的に本実施形態の効果について説明する。
【０１７０】
本実施形態において、カード決済端末２００は、複数のカード認証方法に対応する。例えば、利用者Ｕより取得するデータがサインデータであるか、生体データであるかを自動的に判別する。これにより、決済端末２０９の操作者である加盟店の店員は、取得するデータの種類を意識することなく、自動的にカード決済処理を進めることが可能となるため、カード決済者側の利便性を向上させることができる。
【０１７１】
また、第１の実施形態に示すように、１枚のカードを複数人で利用する場合が想定される。本実施形態において、カード端末２０９またはサーバ２１６乃至サーバ２１８のいずれかのサーバで生体認証が実行される場合で、カードデータＤに含まれる生体データ２０５が複数存在する場合には、取得データと照合完了するまで各生体データについて順番に照合が行われる。照合完了した場合は、照合結果をデータベースＤＢに保存する。これにより、カードを複数人で共有して使用しても、カードを使用した人物を特定することが可能となる。さらに、認証失敗時には、利用者への通知を行い、かつカードへの認証失敗情報の書き込みによりカードを使用不可とすることで、カード決済の不正利用を予防することができる。
【０１７２】
また、カードＣが第三者により不正に利用された場合、生体認証であれば契約者本人以外のカード使用により認証成功することは考えにくいが、それ以外の暗証番号認証またはサイン入力の場合であれば、本人以外によりカードが不正利用される可能性がある。または不正利用でなくとも、詐欺等により、本人の意図しないカード利用がされる可能性がある。本実施形態において、カード決済端末２００は、利用者Ｕよりサインデータ２１４を取得した場合、サインデータ２１４とカードＣ上のサインデータ２２７が類似するかどうかの照合を行うことにより、取得したサインデータ２１４の有効性を判定する。さらに、照合失敗時には、利用者Ｕへその旨を通知することにより、カードＣの不正利用を通知する。これにより、サイン認証が行われる場合でも、カードＣのセキュリティを高めることができる。
【０１７３】
本実施形態において、カード決済端末２００によりサインデータの照合が行われる場合、サイン入力装置２０７がカードＣ上のサインデータ２２７を読み取るとした。しかしながら、カードデータ読み書き装置２１０がカードＣ上のサインデータ２２７を読み取る機能を備えている場合は、カードデータ読み書き装置２１０がカードＣ上のサインデータ２２７を読み取るとしてもよい。
【０１７４】
本実施形態においては、カード決済に関するデータがデータベースＤＢに蓄えられる。これにより、店舗は、対面で顧客がサインした紙媒体のカード決済書類を長期間管理する必要がなく、店舗の管理コスト及び労力を大幅に低減することができる。
【０１７５】
［第３の実施形態］
第３の実施形態においては、第２の実施形態に示したカード決済端末２００およびサーバ２１８を用いてカード決済システムを構成する。本カード決済システムでは、例えば高

齢者、障碍者、未成年者といったユーザに対して、意図しないカード決済を未然に防ぐセキュリティサービスを提供することを目的とする。

【０１７６】

第３の実施形態は、上記第１の実施形態で説明された多機能カード１を利用する場合にも適用可能である。

【０１７７】

以下、第３の実施形態に係るカード決済システムの実施形態を、図面を用いて説明する。

【０１７８】

図１４は、本実施形態に係るカード決済システムの構成の一例を示すブロック図である。本実施形態においては、第２の実施形態に示したカード決済端末２００およびサーバ２１８に加え、さらにオペレータ３０１、サーバ２１８に接続されるデータベース３０２を備えるカード決済システム３００を構成する。サーバ２１８は、以下ではイシュアのサーバ２１８であるとして説明するが、アクワイアラのサーバ２１６、またはカードブランドのサーバ２１７であってもよい。

【０１７９】

カード決済端末２００とサーバ２１８との通信には、決済データ２１５と与信結果データ２１９が用いられ、これらの動作および構成は第２の実施形態で示した通りである。

【０１８０】

サーバ２１８は、データベース３０２に記憶されたデータの読み出し、およびデータの書き込みが可能である。

【０１８１】

データベース３０２は、カード決済に必要なユーザＵの個人情報３０２ａ、過去の異常な決済データのパターンを示す異常パターン情報３０２ｂ、およびユーザＵの過去のカード決済に用いられた決済データ２１５に含まれる任意の情報を記憶する。

【０１８２】

オペレータ３０１は、ユーザＵがデータベース３０２に対して個人情報３０２ａを設定する際に利用するインタフェースであり、例えば設定を代行するイシュア側の電話口のオペレータであってもよいし、イシュアのサーバ２１８上に設けられたユーザＵ専用の登録フォームであってもよい。

【０１８３】

なお、オペレータ３０１はサーバ２１８に含まれていてもよいし、ユーザＵがデータベース３０２に直接アクセスできる手段がある場合は、オペレータ３０１はなくてもよい。

【０１８４】

図１５は、本実施形態に係る個人情報３０２ａの設定処理を例示するフローチャートである。

【０１８５】

ユーザＵは、カード決済に関する利用限度額、決済地域といった個人情報（カード利用条件情報）３０２ａをあらかじめデータベース３０２に登録しておくことで、サーバ２１８はカード決済があった際、ユーザＵの意図したカード決済であるかどうかを登録された個人情報３０２ａを用いて判定することが可能となる。

【０１８６】

ユーザＵは、オペレータ３０１に対し、カード決済の利用回数、利用限度額、または決済地域といった個人情報３０２ａの設定を依頼する（ステップＳ１５０１）。決済地域の設定は、生活圏外でのカード利用を防ぐことを目的とする。例えば、不正請求、消費者被害、詐欺被害等（以下、詐欺被害等と称する）の課金会社は一部の地域に偏る傾向がある。したがって、決済地域を監視することは、詐欺被害等を防ぐために有効である。

【０１８７】

なお、ユーザＵは、オペレータ３０１に対し、必要に応じてさらに追加の個人情報３０２ａの設定を依頼してもよい。

【０１８８】
オペレータ３０１は、ユーザＵによる個人情報３０２ａの設定依頼を受信すると、サーバ２１８に対し、ユーザ情報の設定指令を送信する（ステップＳ１５０２）。
【０１８９】
サーバ２１８は、オペレータ３０１よりユーザ情報の設定指令を受信すると、データベース３０２にユーザ情報を設定する（ステップＳ１５０３）。
【０１９０】
図１６は、本実施形態に係るセキュリティサービスにおける処理を例示するフローチャートである。なお、ユーザＵの個人情報３０２ａは、図１５の手順によりデータベース３０２に設定されているとする。
【０１９１】
ユーザＵは、加盟店に設置されているカード決済端末２００を使用してカード決済による物品またはサービスの購入を行うと（ステップＳ１６０１）、カード決済端末２００は、決済データ２１５を作成し、決済データ２１５をサーバ２１８へ送信する（ステップＳ１６０２）。
【０１９２】
サーバ２１８は、データベース３０２に設定されたユーザＵの個人情報３０２ａである利用回数を参照し、データベース３０２内部を検索することにより得られたユーザＵの実際の利用回数と比較する（ステップＳ１６０３）。サーバ２１８は、ユーザＵの利用回数が設定された回数を超えている場合、カードは利用不可すなわち与信結果をＮＧと判定し、ステップＳ１６０８の処理に移る。そうでない場合は、ステップＳ１６０４の処理に移る。
【０１９３】
サーバ２１８は、データベース３０２に設定されたユーザＵの個人情報３０２ａである決済地域を参照し、決済データ２１５に含まれる加盟店情報２３０の住所と比較する（ステップＳ１６０４）。
【０１９４】
サーバ２１８は、加盟店情報２３０の住所がデータベース３０２に設定された決済地域に含まれてない場合、詐欺被害等の疑いがあるか否かを判定する（ステップＳ１６０５）。例えば、データベース３０２に過去の詐欺被害等の決済データが記憶されている場合は、異常パターン情報３０２ｂとしての過去の詐欺被害等の決済データを読み出し、決済データ２１５の加盟店情報２３０および支払金額２２６と比較することにより詐欺被害等の疑いがあるか否かを判定してもよい。また、例えば支払金額２２６とユーザＵによりデータベース３０２に設定された利用限度額とを比較し、支払金額２２６が一定基準以上の高額であれば、詐欺被害等の疑いがあると判定してもよい。
【０１９５】
ステップＳ１６０５において、詐欺被害等の疑いがないと判定された場合は、ステップＳ１６０８の処理に移る。詐欺被害等の疑いがあると判定された場合は、サーバ２１８は、ユーザの安否確認を実施する（ステップＳ１６０６）。ユーザＵは、安否確認サービスを受信する（ステップＳ１６０７）。安否確認サービスの受信方法は、ユーザがデータベース３０２に事前に設定した連絡先へ自動音声連絡を行うとしてもよく、自動でメールを送信してもよく、または、その他の手段による連絡でもよい。さらに、安否確認が取れない場合は、サーバ２１８は、例えばデータベース３０２において記憶されているユーザＵの緊急連絡先、成年後見人、または警察警備会社等へ、自動音声連絡、自動メール送信、またはその他の手段による連絡を行ってもよい。
【０１９６】
ステップＳ１６０８において、サーバ２１８は、与信結果をＮＧとする与信結果データ７を作成し、カード決済端末２００へ送信する。また、ステップＳ１６０５において詐欺被害等であると判定された場合は、決済データ２１５のうちその取引に関する情報、すなわち支払金額２２６、加盟店情報２３０、およびこれらに加えて他に必要な情報をデータ

ベース３０２に記憶する。カード決済端末２００は、与信結果ＮＧデータを受信し、決済不成立となる（ステップＳ１６０９）。

【０１９７】

ステップＳ１６０４において、サーバ２１８により加盟店情報２３０の住所がデータベース３０２に設定された決済地域内であると判定された場合、サーバ２１８は、現在の決済データ２１５のユーザＵの支払金額２２６を足し合わせた、データベース３０２に保存されているユーザＵの過去一定期間の支払金額の累積額と、ユーザＵによりデータベース３０２に設定された利用限度額とを比較する（ステップＳ１６１０）。累積額が利用限度額内である場合、与信結果をＯＫと判定し、ステップＳ１６１５の処理に移る。累積額が利用限度額内ではない場合は、サーバ２１８は、ユーザＵに対し、利用限度額制限を解除するか否か確認を行う（ステップＳ１６１１）。

【０１９８】

ユーザＵは、利用限度額制限を解除の通知を受け取った場合、オペレータ３０１に対し利用限度額制限の解除可否の設定を依頼する（ステップＳ１６１２）。

【０１９９】

ステップＳ１６１３において、オペレータ３０１は、ユーザＵより利用限度額制限を解除する旨の設定依頼を受信した場合、かつユーザＵの利用限度額が支払金額２２６を超えるよう設定可能であると判定した場合、サーバ２１８に対しユーザＵの利用限度額制限の解除を行うよう指示する。利用限度額制限を解除する旨の設定依頼を受信しない場合、または、利用限度額が支払金額２２６を超えるよう設定不可の場合、オペレータ３０１は、与信結果はＮＧと判定し、サーバ２１８に対し上述のステップＳ１６０８の処理に移るよう指示する。

【０２００】

サーバ２１８は、オペレータ３０１より利用限度額制限の解除指令を受信すると、ユーザＵの利用限度額を、設定可能な金額かつ支払金額２２６を超える金額になるように設定する（ステップＳ１６１４）。

【０２０１】

ステップＳ１６１５において、サーバ２１８は、与信結果をＯＫとする与信結果データ２１９を作成し、カード決済端末２００へ送信する。また、決済データ２１５のうちユーザＵの取引であることおよびその金額を特定する情報、すなわちカード番号２０１、氏名２０３、支払金額２２６、支払方法およびこれらに加えて他に必要な情報をデータベース３０２に記憶する。カード決済端末２００は、与信結果ＯＫデータを受信し、決済成立となる（ステップＳ１６１６）。

【０２０２】

本実施形態においては、データベース３０２に対し、利用回数、限度額、決済地域といった個人情報３０２ａを設定し、サーバ２１８において、データベース３０２に記憶されている個人情報３０２ａまたは過去のカード決済情報と現在の決済データ２１５とを比較照合して与信可否を決定することにより、ユーザＵの意図しないカード利用や、詐欺被害等のようなカード被害を防ぐことができる。

【０２０３】

本実施形態において、ユーザ毎に行うカードの利用回数の設定は、月単位であってもよいし、日単位であってもよい。また、従来一般のクレジットカードの利用限度額は利用枠全体に対してのみ設定でき、またデビットカードまたはキャッシュカードでの利用限度額は銀行口座残高全部となっているが、本実施形態においては、利用限度額をカードの使用目的に応じて細かく設定できるとしてもよい。例えば、現金払い戻しは２万円以下で１日１回まで、振り込みは３万円以下で１日２回まで、通常買い物は１万円以下で３回までといった設定が可能であるとしてもよい。

【０２０４】

本実施形態において、データベース３０２に設定される利用回数、限度額、決済地域といったユーザＵの個人情報３０２ａは、サーバ２１８によるユーザＵのカード利用内容の

パターン化に基づいて、または、サーバ２１８によるユーザＵのカードの利用回数、利用間隔、利用店舗、利用目的、与信残高などに基づくスコアリングにより、サーバ２１８が自動的に設定してもよい。

【０２０５】

上記の図１６のフローチャートにおいて、各ステップの順序は、例えばサーバ２１８においてデータベース３０２に記憶されている個人情報３０２ａまたは過去のカード決済情報と現在の決済データ２１５との比較照合処理が実現できる範囲であれば、適宜変更されてもよいし、１つの処理モジュールで一括して複数ステップの処理が行われてもよい。

【０２０６】

本実施形態においては、ユーザＵが事前に設定した利用限度額以上の金額を決済しようとした場合、サーバ２１８はユーザＵに対し、利用限度額制限の解除確認を行う。これにより、ユーザＵ本人ではない他人による利用限度枠の解除を禁止するとともに、ユーザＵの意図しない高額なカード決済を防ぐことができる。

【０２０７】

さらに、本実施形態において、詐欺被害等の疑いがあると判定された場合は、本人の安否確認を行うことにより、例えば高齢者、障碍者、未成年者といったユーザＵの保護を強化することができる。

【０２０８】

上記の各実施形態は、例示であり、発明の範囲を限定することは意図していない。上記の各実施形態は、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。上記の各実施形態やその変形は、発明の範囲や要旨に含まれると同様に、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ものである。

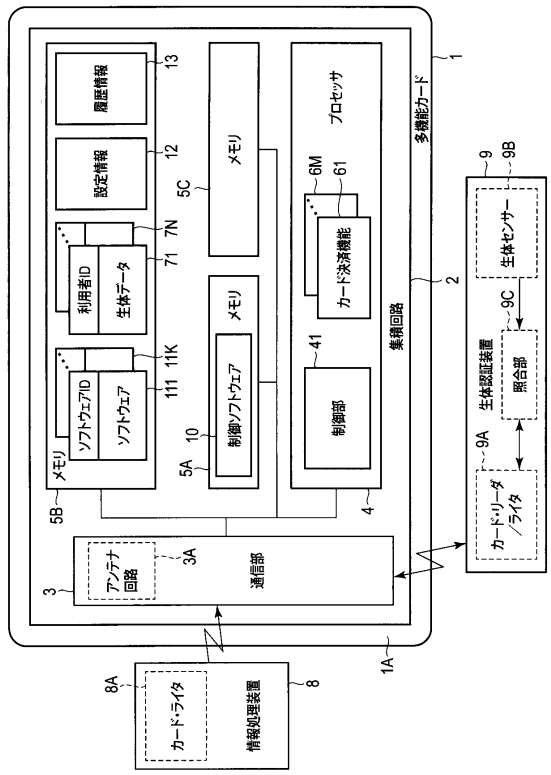
【符号の説明】

【０２０９】

１…多機能カード、１Ａ…カード本体、２…集積回路、３…通信部、３Ａ…アンテナ回路、４…プロセッサ、５Ａ，５Ｂ，５Ｃ…メモリ、８…情報処理装置、８Ａ…カード・ライタ、９…生体認証装置、９Ａ…カード・リーダ／ライタ、９Ｂ…生体センサ、９Ｃ…照合部、１０…制御ソフトウェア、１２…設定情報、１３…履歴情報、４１…制御部、６１…カード決済機能、７１～７Ｎ…生体データ、１１１～１１Ｋ…ソフトウェア。

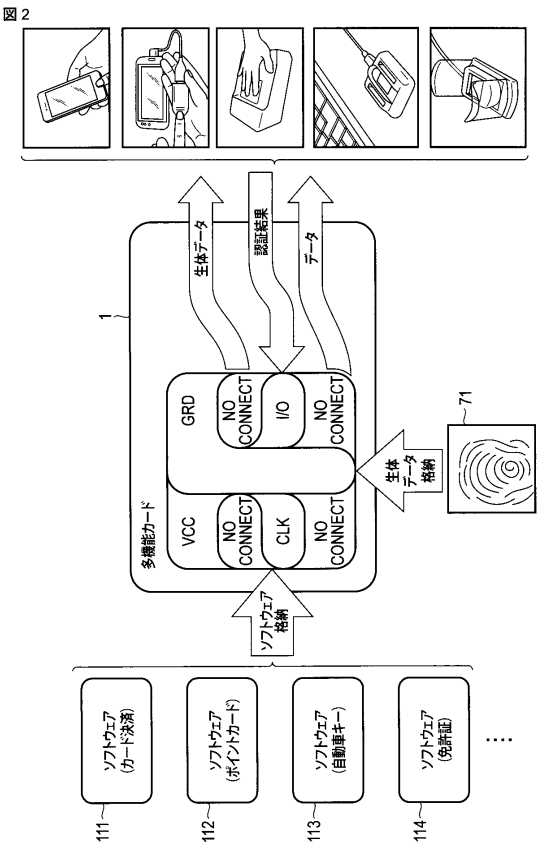
【図１】

図1



【図２】

図2



【図３】

図3

ソフトウェアID	利用者ID
クレジットカード	U1
ポイントカード	
自動車キー	U1,U2,U3
⋮	⋮

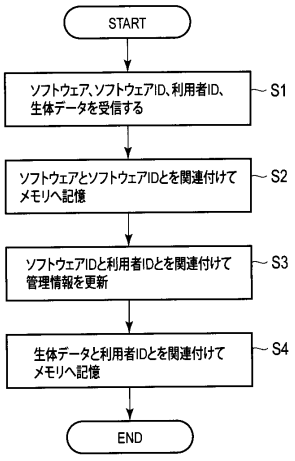
【図４】

図4

時間情報	ソフトウェアID	認証結果	認証された利用者ID
2017/1/2	自動車キー	○	U2
2017/1/10	クレジットカード	○	U1
2017/1/12	ポイントカード		
⋮	⋮	⋮	⋮

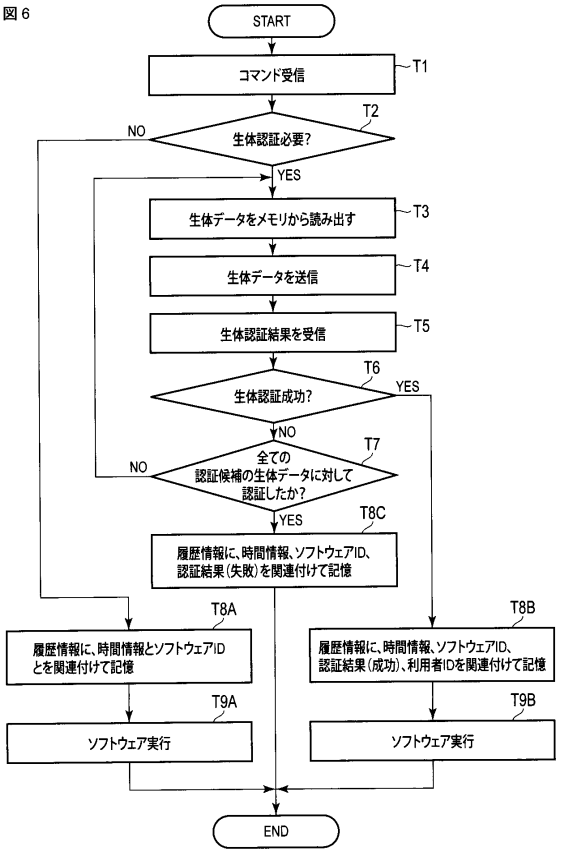
【図５】

図5



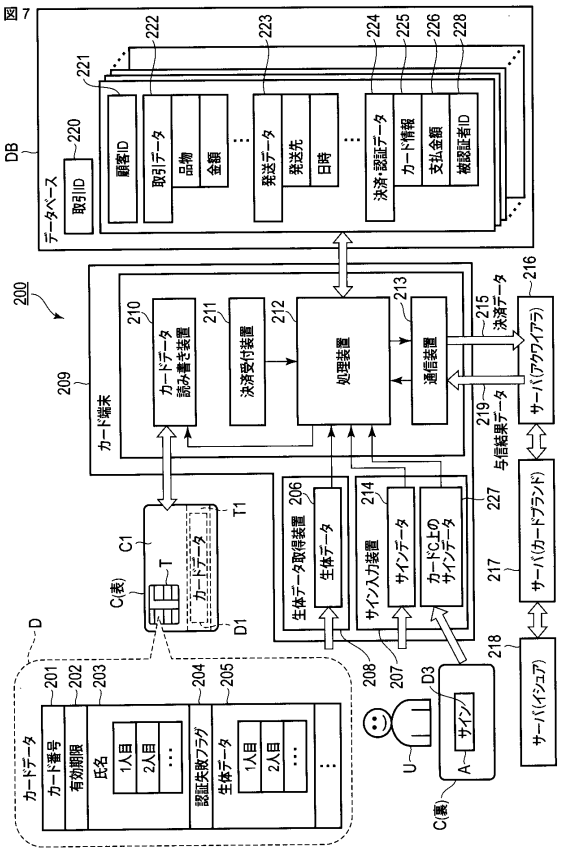
【図６】

図６



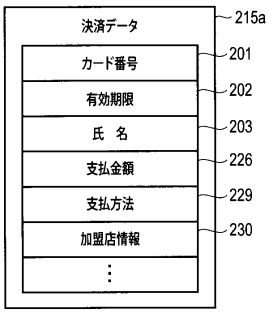
【図７】

図７



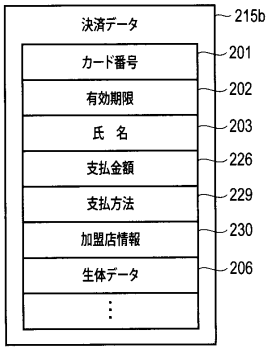
【図８】

図８



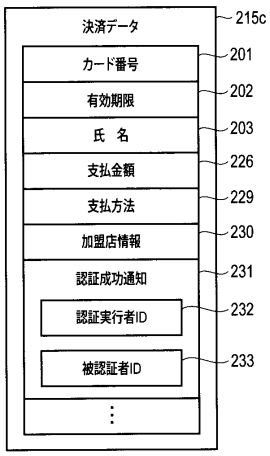
【図９】

図９



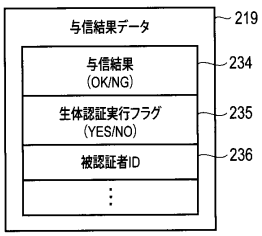
【図１０】

図10

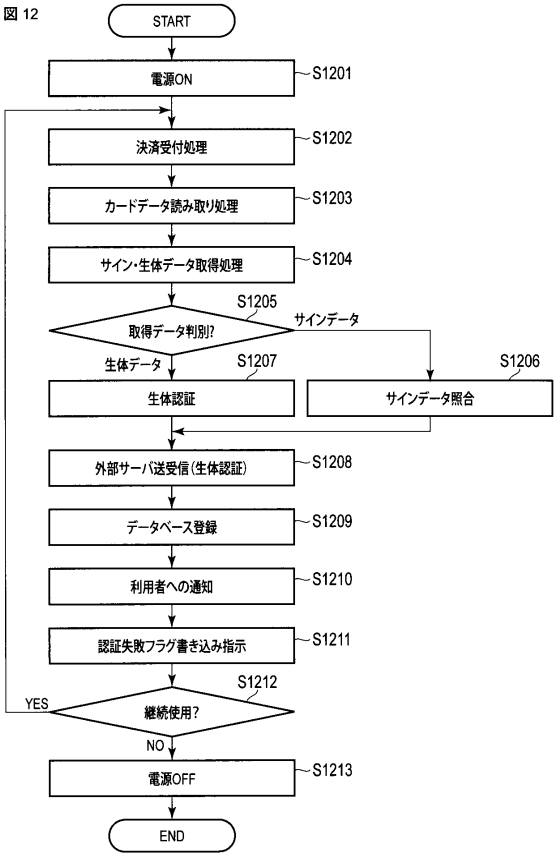


【図１１】

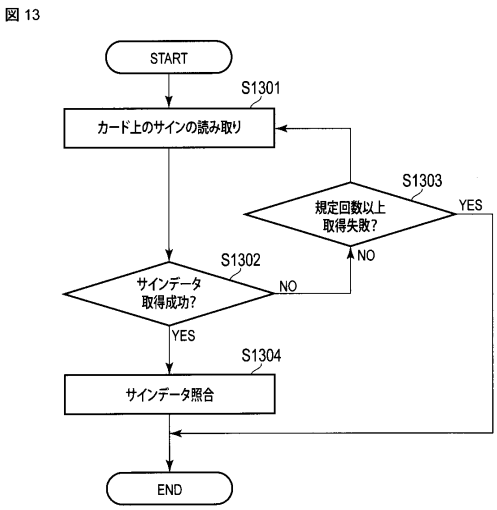
図11



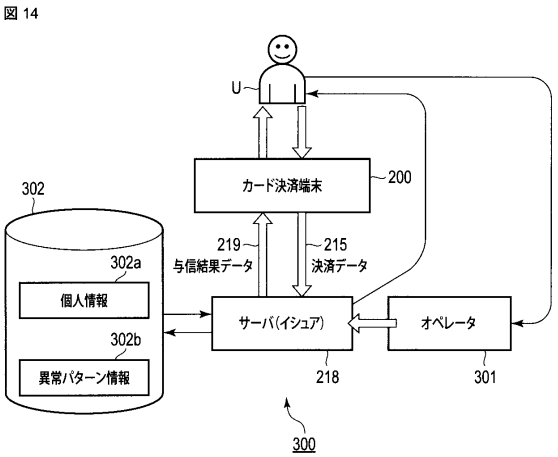
【図１２】



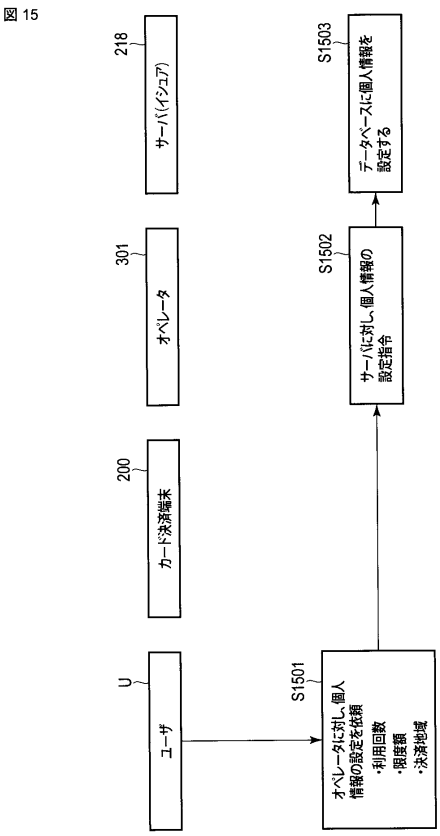
【図１３】



【図１４】



【図１５】



【図１６】

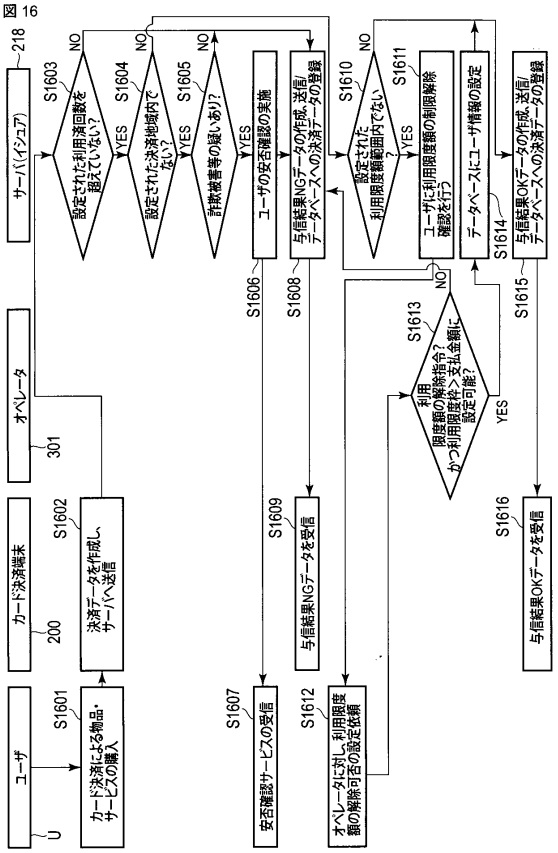


図16
ユーザ
U
カード決済端末
200
オペレータ
301
サーバ(イシュア)
218
カード決済による物品・サービスの購入
S1601
決済データを作成し、サーバへ送信
S1602
設定された利用済回数を超えていない?
S1603
設定された決済地域内でない?
S1604
詐欺被害等の疑いあり?
S1605
ユーザの安否確認の実施
S1606
安否確認サービスの受信
S1607
与信結果NGデータを受信
S1609
与信結果NGデータの作成、送信/データベースへの決済データの登録
S1608
オペレータに対し、利用限度額の解除可否の設定依頼
S1612
設定された利用限度額範囲内でない?
S1610
ユーザに利用限度額の制限解除確認を行う
S1611
利用限度額の解除指令?かつ利用限度枠>支払金額に設定可能?
S1613
データベースにユーザ情報の設定
S1614
与信結果OKデータの作成、送信/データベースへの決済データの登録
S1615
与信結果OKデータを受信
S1616
NO
YES

フロントページの続き

(56)参考文献 特開２００２－１３３３８４（ＪＰ，Ａ）
特開２００４－００５１３３（ＪＰ，Ａ）
特開２００６－０６５４５５（ＪＰ，Ａ）
特開２００５－０８５０７２（ＪＰ，Ａ）
特開平０９－２５９２３９（ＪＰ，Ａ）
特開２０１１－００２８８３（ＪＰ，Ａ）
特開２００９－０３１８７７（ＪＰ，Ａ）
特開平０１－０９３８７７（ＪＰ，Ａ）
特開２００７－０２６１１８（ＪＰ，Ａ）
特開２０１１－０８１７５６（ＪＰ，Ａ）
特表２００７－５２８０３５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００