

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7190816号
(P7190816)

(45)発行日 令和4年12月16日(2022.12.16)

(24)登録日 令和4年12月8日(2022.12.8)

(51)国際特許分類 F I
G 0 6 Q 20/40 (2012.01) G 0 6 Q 20/40 3 0 0

請求項の数 10 (全35頁)

(21)出願番号	特願2018-32593(P2018-32593)	(73)特許権者	302064762
(22)出願日	平成30年2月26日(2018.2.26)		株式会社日本総合研究所
(65)公開番号	特開2019-148939(P2019-148939 A)	(74)代理人	100104190
			弁理士 酒井 昭徳
(43)公開日	令和1年9月5日(2019.9.5)	(72)発明者	高橋 康子
審査請求日	令和3年1月27日(2021.1.27)		東京都品川区東五反田2丁目18番1号
			株式会社日本総合研究所内
		審査官	加内 慎也

最終頁に続く

(54)【発明の名称】 認証情報生成装置、認証情報生成方法、および認証情報生成プログラム

(57)【特許請求の範囲】

【請求項1】

利用者が閲覧可能な取引に関する、カード会社が決済に関する通知を発行した場合に、当該通知に記載される情報を含む履歴を取得する取得手段と、

前記取得手段によって取得された前記履歴に基づいて、前記カード会社が発行したクレジットカードを用いた以降の取引において用いられる認証情報を生成する生成手段と、
を有することを特徴とする認証情報生成装置。

【請求項2】

利用者が閲覧可能な取引に関する履歴を取得する取得手段と、

前記取得手段によって取得された前記履歴のうち、金融機関が預金通帳を発行した場合に、当該預金通帳に記帳される出金額または入金額に関する情報に基づいて、以降の取引において用いられる認証情報を生成する生成手段と、
を有することを特徴とする認証情報生成装置。

【請求項3】

利用者が閲覧可能な取引に関する履歴を取得する取得手段と、

前記取得手段によって取得された前記履歴のうち、金融機関が預金通帳を発行した場合に、当該預金通帳に記載される、特定の支払先が定められており、かつ、定期的に引き落とされる記帳情報に基づいて、以降の取引において用いられる認証情報を生成する生成手段と、

を有することを特徴とする認証情報生成装置。

【請求項 4】

前記記帳情報は、公共料金の支払いに関する記帳情報であることを特徴とする請求項 3 に記載の認証情報生成装置。

【請求項 5】

利用者が閲覧可能な取引に関する、カード会社が決済に関する通知を発行した場合に、当該通知に記載される情報を含む履歴を取得し、

取得した前記履歴に基づいて、前記カード会社が発行したクレジットカードを用いた以降の取引において用いられる認証情報を生成し、

生成した認証情報を記憶部に記憶させる、

処理をコンピュータが実行することを特徴とする認証情報生成方法。

10

【請求項 6】

利用者が閲覧可能な取引に関する履歴を取得し、

取得した前記履歴のうち、金融機関が預金通帳を発行した場合に、当該預金通帳に記載される出金額または入金額に関する情報に基づいて、以降の取引において用いられる認証情報を生成し、

生成した認証情報を記憶部に記憶させる、

処理をコンピュータが実行することを特徴とする認証情報生成方法。

【請求項 7】

利用者が閲覧可能な取引に関する履歴を取得し、

取得した前記履歴のうち、金融機関が預金通帳を発行した場合に、当該預金通帳に記載される、特定の支払先が定められており、かつ、定期的に引き落とされる記帳情報に基づいて、以降の取引において用いられる認証情報を生成し、

生成した認証情報を記憶部に記憶させる、

処理をコンピュータが実行することを特徴とする認証情報生成方法。

20

【請求項 8】

利用者が閲覧可能な取引に関する、カード会社が決済に関する通知を発行した場合に、当該通知に記載される情報を含む履歴を取得し、

取得した前記履歴に基づいて、前記カード会社が発行したクレジットカードを用いた以降の取引において用いられる認証情報を生成し、

生成した認証情報を記憶部に記憶させる、

処理をコンピュータに実行させることを特徴とする認証情報生成プログラム。

30

【請求項 9】

利用者が閲覧可能な取引に関する履歴を取得し、

取得した前記履歴のうち、金融機関が預金通帳を発行した場合に、当該預金通帳に記載される出金額または入金額に関する情報に基づいて、以降の取引において用いられる認証情報を生成し、

生成した認証情報を記憶部に記憶させる、

処理をコンピュータに実行させることを特徴とする認証情報生成プログラム。

【請求項 10】

利用者が閲覧可能な取引に関する履歴を取得し、

取得した前記履歴のうち、金融機関が預金通帳を発行した場合に、当該預金通帳に記載される、特定の支払先が定められており、かつ、定期的に引き落とされる記帳情報に基づいて、以降の取引において用いられる認証情報を生成し、

生成した認証情報を記憶部に記憶させる、

処理をコンピュータに実行させることを特徴とする認証情報生成プログラム。

40

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、クレジットカードやキャッシュカードなどの各種カードに用いられる認証情報を生成する、認証情報生成装置、認証情報生成方法、および認証情報生成プログラム

50

に関する。

【背景技術】

【0002】

従来、クレジットカードやキャッシュカードなど各種カードを用いて、取引がおこなわれている。各種カードを用いて取引をおこなう際には、暗証番号やパスワードといった認証情報が用いられる。たとえば、クレジットカードを用いて、利用者が商品を購入した場合やサービスの提供を受けた際に、暗証番号を入力して支払がおこなわれる。また、たとえば、キャッシュカードを用いて、利用者が銀行の口座から所望の額を引き出す際に、暗証番号を入力して出金がおこなわれる。

【0003】

関連する技術として、たとえば、プリペイドカードに付与された識別コードと、取引ごとに使用される認証情報と、残高情報と、を対応付けて記憶するデータベースを参照し、取引の際に利用者から識別コードとともに受け付けた認証情報がデータベースに記憶される認証情報に合致する場合、当該識別コードに対応する残高情報を取引金額に基づいて更新する、取引方法が開示されている（たとえば、下記特許文献1参照。）。

【先行技術文献】

【特許文献】

【0004】

【文献】特開2002-163583号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、従来におけるキャッシュカードやクレジットカードの認証情報は固定化されることが多く、セキュリティが高いとは言えなかった。ここで、セキュリティを高めるために認証情報を変更する場合、利用者が銀行の窓口に出向いたり、利用者とカード会社との間で各種書類や各種情報をやり取りしたりするため、利用者や各社のスタッフにとって手間がかかるという問題があった。

【0006】

また、セキュリティを高めるために認証情報を適宜変更したとすると、利用者が認証情報を失念する可能性が高くなり、認証情報を失念した場合には、取引をおこなうことができず、取引にかかる利便性が低下するといった問題があった。特に、高齢化社会において、高齢な利用者ほど、認証情報を失念する可能性は高くなるため、認証情報を適宜変更したとすると、このような問題が生じやすくなる。

【0007】

この発明は、上述した従来技術による問題点を解消するため、取引の利便性が低下することを抑えつつ、セキュリティを簡単に向上させることができる、認証情報生成装置、認証情報生成方法、および認証情報生成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】

【0008】

上述した課題を解決し、目的を達成するため、この発明にかかる認証情報生成装置は、利用者が閲覧可能な取引に関する履歴を取得する取得手段と、前記取得手段によって取得された履歴に基づいて、以降の取引において用いられる認証情報を生成する生成手段と、を有することを特徴とする。

【0009】

また、この発明にかかる認証情報生成装置は、上記発明において、前記履歴は、金融機関が発行する預金通帳に印字された情報を含み、前記生成手段は、前記預金通帳に印字された情報に基づいて、前記金融機関における以降の取引において用いられる認証情報を生成することを特徴とする。

【0010】

また、この発明にかかる認証情報生成装置は、上記発明において、前記取得手段は、前

10

20

30

40

50

記預金通帳に印字された直近の情報を取得し、前記生成手段は、前記取得手段によって取得された前記直近の情報に基づいて、前記認証情報を生成することを特徴とする。

【0011】

また、この発明にかかる認証情報生成装置は、上記発明において、前記生成手段は、前記預金通帳に印字された情報が示す金額の中から、予め設定された複数の桁に該当する数字をそれぞれ選択して前記認証情報を生成することを特徴とする。

【0012】

また、この発明にかかる認証情報生成装置は、上記発明において、前記履歴は、前記預金通帳に印字されていない情報を含み、前記預金通帳に印字された情報と、前記預金通帳に印字されていない情報とを区別させる付加情報を、前記履歴とともに所定の端末に表示可能にするための制御をおこなう出力制御手段を有することを特徴とする。

10

【0013】

また、この発明にかかる認証情報生成装置は、上記発明において、前記生成手段は、前記利用者による設定に応じて、前記履歴に基づく認証情報の生成をおこなうことを特徴とする。

【0014】

また、この発明にかかる認証情報生成装置は、上記発明において、前記履歴は、カード会社が発行した決済に関する通知に印字された情報を含み、前記生成手段は、前記通知に印字された情報に基づいて、前記カード会社が発行したクレジットカードを用いた以降の取引において用いられる認証情報を生成することを特徴とする。

20

【0015】

また、この発明にかかる認証情報生成方法は、利用者が閲覧可能な取引に関する履歴を取得し、取得した前記履歴に基づいて、以降の取引において用いられる認証情報を生成し、生成した認証情報を記憶部に記憶させる処理をコンピュータが実行することを特徴とする。

【0016】

また、この発明にかかる認証情報生成プログラムは、利用者が閲覧可能な取引に関する履歴を取得し、取得した前記履歴に基づいて、以降の取引において用いられる認証情報を生成し、生成した認証情報を記憶部に記憶させる処理をコンピュータに実行させることを特徴とする。

30

【発明の効果】

【0017】

この発明にかかる認証情報生成装置、認証情報生成方法、および認証情報生成プログラムによれば、取引の利便性が低下することを抑えつつ、セキュリティを簡単に向上させることができる、という効果を奏する。

【図面の簡単な説明】

【0018】

【図1】図1は、実施の形態1にかかる認証情報生成システム100のシステム構成例を示す説明図である。

【図2A】図2Aは、銀行サーバ111のハードウェア構成の一例を示すブロック図である。

40

【図2B】図2Bは、利用者端末121およびATM131のハードウェア構成の一例を示すブロック図である。

【図3A】図3Aは、口座情報データベース(DB)112の記憶内容の一例を示す説明図である。

【図3B】図3Bは、実施の形態1にかかる取引情報データベース(DB)113の記憶内容の一例を示す説明図である。

【図4】図4は、実施の形態1にかかる認証情報の生成例を示す図である。

【図5】図5は、実施の形態1にかかる認証情報生成システム100の機能的構成を示す説明図である。

50

【図 6 A】図 6 A は、利用者端末 1 2 1 に表示される取引履歴の表示例を示す説明図である。

【図 6 B】図 6 B は、利用者端末 1 2 1 が SNS により取得した直近の記帳情報の表示例を示す説明図である。

【図 7】図 7 は、銀行サーバ 1 1 1 がおこなう認証情報生成処理手順の一例を示すフローチャートである。

【図 8】図 8 は、銀行サーバ 1 1 1 がおこなう取引履歴の出力処理手順の一例を示すフローチャートである。

【図 9 A】図 9 A は、認証情報の生成の他の例を示す図（その 1）である。

【図 9 B】図 9 B は、認証情報の生成の他の例を示す図（その 2）である。

【図 1 0】図 1 0 は、実施の形態 2 にかかる認証情報生成システム 1 0 0 0 のシステム構成例を示す説明図である。

【図 1 1 A】図 1 1 A は、カード情報データベース（DB）1 0 1 2 の記憶内容の一例を示す説明図である。

【図 1 1 B】図 1 1 B は、実施の形態 2 にかかる取引情報データベース（DB）1 0 1 3 の記憶内容の一例を示す説明図である。

【図 1 2】図 1 2 は、実施の形態 2 にかかる認証情報の生成例を示す図である。

【図 1 3】図 1 3 は、実施の形態 2 にかかる認証情報生成システム 1 0 0 0 の機能的構成を示す説明図である。

【図 1 4】図 1 4 は、カード会社サーバ 1 0 1 1 がおこなう認証情報生成処理手順の一例を示すフローチャートである。

【発明を実施するための形態】

【0 0 1 9】

以下に添付図面を参照して、この発明にかかる認証情報生成装置、認証情報生成方法、および認証情報生成プログラムの好適な実施の形態（実施の形態 1 および実施の形態 2）を詳細に説明する。

【0 0 2 0】

（実施の形態 1）

（認証情報生成システムのシステム構成）

まず、実施の形態 1 にかかる認証情報生成システム 1 0 0 のシステム構成例について説明する。図 1 は、実施の形態 1 にかかる認証情報生成システム 1 0 0 のシステム構成例を示す説明図である。図 1 において、認証情報生成システム 1 0 0 は、銀行サーバ 1 1 1 と、利用者端末 1 2 1 と、カード 1 2 2 と、預金通帳 1 2 3 と、ATM（Automated Teller Machine：現金自動預け払い機）1 3 1 と、を有する。

【0 0 2 1】

銀行サーバ 1 1 1 は、この発明にかかる認証情報生成装置の一例である。銀行サーバ 1 1 1 は、銀行 1 1 0 に設けられるサーバである。具体的には、銀行サーバ 1 1 1 は、利用者ごとの口座の預金額等を管理する汎用的なコンピュータ装置である。銀行サーバ 1 1 1 は、たとえば、CPU（Central Processing Unit）やメモリやインタフェースなどを有するパーソナルコンピュータである。また、銀行サーバ 1 1 1 は、口座情報データベース（DB）1 1 2 と、取引情報 DB 1 1 3 とを有する。各種 DB 1 1 2、1 1 3 の記憶内容については、図 3 A および図 3 B を用いて後述する。

【0 0 2 2】

利用者端末 1 2 1 は、たとえば、カード 1 2 2 の利用者が有するコンピュータ装置である。利用者端末 1 2 1 には、たとえば、スマートフォンやタブレット型 PC（Personal Computer）といったコンピュータ装置が用いられる。利用者端末 1 2 1 は、CPU やメモリやインタフェースなどを有する。

【0 0 2 3】

ただし、利用者端末 1 2 1 は、スマートフォンやタブレット型 PC に限らず、デスクトップ型 PC、ノート型 PC などの各種 PC、携帯電話機、PHS（Personal H

10

20

30

40

50

andyphone System) とすることも可能である。

【0024】

カード122は、銀行110が発行したキャッシュカードである。預金通帳123は、利用者の預金口座に対応する、銀行110が発行した冊子であり、預金の受け入れ額や、払い戻し額が記帳される。

【0025】

ATM131は、銀行110の店舗やコンビニエンスストアなどに設けられ、インターネットなどのネットワーク140に接続されている。ATM131は、カード122や預金通帳123が挿入されて、利用者によって所定の取引情報が入力されることにより、入出金や振込などにかかる各種の処理をおこなう。ATM131は、入出金や振込などにかかる各種の処理の実行に際して、銀行サーバ111との間で通信をおこなう。

10

【0026】

また、ATM131は、利用者と銀行サーバ111とのインタフェースをつかさどり、出金や振込などにかかる取引情報を利用者に通知する。また、ATM131は、預金通帳123が挿入されて、取引をおこなった場合、預金通帳123に取引の内容を記帳（印字）する。また、ATM131は、預金通帳123が挿入されずに、カード122のみが挿入されて、取引をおこなった場合、取引情報を示す利用明細書を印字出力する。

【0027】

認証情報生成システム100において、銀行サーバ111と、利用者端末121と、ATM131とは、有線または無線のネットワーク140を介して接続される。ネットワーク140は、たとえば、インターネット、移動体通信網などである。ただし、ネットワーク140は、LAN（Local Area Network）、WAN（Wide Area Network）などであってもよい。

20

【0028】

（銀行サーバ111のハードウェア構成の一例）

つぎに、銀行サーバ111について、その具体的な構成の一例を説明する。図2Aは、銀行サーバ111のハードウェア構成の一例を示すブロック図である。

【0029】

図2Aにおいて、銀行サーバ111を実現するコンピュータ装置は、CPU211と、メモリ212と、通信IF（Interface）213と、を備える。コンピュータ装置が備える各部211～213は、バス210によってそれぞれ接続されている。CPU211は、コンピュータ装置の全体の制御をつかさどる。

30

【0030】

メモリ212は、ブートプログラムなどのプログラムや、各種のデータベースのデータなどを記憶する。また、メモリ212は、認証情報生成プログラムや各種データベースの一部のデータなど、実施の形態1の認証情報生成方法にかかる各種のプログラムやデータを記憶する。

【0031】

また、メモリ212は、CPU211のワークエリアとして使用される。メモリ212は、たとえば、ROM（Read-Only Memory）、RAM（Random Access Memory）、HDD（Hard Disc Drive）およびHD（Hard Disc）などによって実現することができる。

40

【0032】

通信IF213は、ネットワーク140に接続され、コンピュータ装置の内部と、利用者端末121やATM131などの外部装置とのインタフェースをつかさどる。具体的には、通信IF213は、コンピュータ装置の内部と外部装置との間におけるデータの入出力を制御する。

【0033】

（利用者端末121およびATM131のハードウェア構成の一例）

つぎに、利用者端末121およびATM131について、その具体的な構成の一例を説

50

明する。図 2 B は、利用者端末 1 2 1 および A T M 1 3 1 のハードウェア構成の一例を示すブロック図である。なお、以下においては、利用者端末 1 2 1 について説明することとし、A T M 1 3 1 については適宜補足して説明することとする。

【0034】

図 2 B において、利用者端末 1 2 1 を実現するコンピュータ装置は、C P U 2 2 1 と、メモリ 2 2 2 と、出力デバイス 2 2 3 と、入力デバイス 2 2 4 と、通信 I F 2 2 5 と、を備える。コンピュータ装置が備える各部 2 2 1 ~ 2 2 5 は、バス 2 2 0 によってそれぞれ接続されている。C P U 2 2 1 は、コンピュータ装置の全体の制御をつかさどる。

【0035】

メモリ 2 2 2 は、ブートプログラムなどのプログラムや、各種のデータベースのデータなどを記憶する。また、メモリ 2 2 2 は、C P U 2 2 1 のワークエリアとして使用される。メモリ 2 2 2 は、たとえば、R O M、R A M、H D D、および H D などによって実現することができる。

10

【0036】

出力デバイス 2 2 3 は、たとえば、ディスプレイ、スピーカ、音声出力端子などを含む。ディスプレイは、操作内容や、利用者に対する案内情報などを表示する。ディスプレイは、認証サービスにかかる各種の操作画面を表示する。ディスプレイは、たとえば、主に液晶ディスプレイや有機 E L (E l e c t r o - L u m i n e s c e n c e) ディスプレイなどによって実現することができる。

【0037】

また、スピーカは、音声、アラーム音などを出力する。音声出力端子は、ヘッドフォンなどを接続する端子であり、スピーカと同様に、音声、アラーム音などを接続されたヘッドフォンなどに出力する。

20

【0038】

入力デバイス 2 2 4 は、文字、数値、各種指示などの入力のためのキーを備え、データ入力をおこなう。入力デバイス 2 2 4 は、たとえば、タッチパネルやキーボードなどを含む。タッチパネルやキーボードは、入力操作に応じた信号を C P U 2 2 1 に対して出力する。

【0039】

タッチパネルは、ディスプレイの表示面側に積層される。タッチパネルは、指やペンなどの筆記部材が接触したことを検出した場合に、タッチパネルに対する筆記部材の接触位置に応じた電気信号を出力する。タッチパネルは、たとえば抵抗膜方式や静電容量方式、音響パルス認識方式、超音波表面弾性波方式、赤外遮光方式、画像認識方式など公知の各種の方式のものをを用いることができる。

30

【0040】

また、入力デバイス 2 2 4 は、カメラなどの撮像装置を含む。カメラは、静止画や動画を撮像する。具体的には、たとえば、カメラは、C P U 2 2 1 によって制御されて撮像対象を撮像し、画像データを生成する。また、カメラは、バーコードや Q R コード（登録商標）といった二次元コードを撮影して入力する。また、カメラは、O C R (O p t i c a l C h a r a c t e r R e a d e r) 機能を用いて撮影した文字をデータ化して入力する。

40

【0041】

また、入力デバイス 2 2 4 は、マイクなどの録音装置を含む。マイクは、アナログデータとして入力された話者の声をアナログ／デジタル変換し、デジタル形式の音声データを生成する。入力デバイス 2 2 4 としてマイクを用いることによって、利用者は、利用者端末 1 2 1 を介して、タッチパネルやキーボードを用いる代わりに、文字などのテキスト入力をおこなうことができる。したがって、マイクは、いわゆる「A I (A r t i f i c i a l I n t e l l i g e n c e 人工知能) スピーカー」などを含めるようにしてもよい。この「A I スピーカー」を用いることによって、対話型の音声操作に対応した A I アシスタントが利用可能となる。

50

【0042】

通信IF225は、ネットワーク140に接続され、コンピュータ装置の内部と、銀行サーバ111や、ATM131などの外部装置とのインタフェースをつかさどる。具体的には、通信IF225は、コンピュータ装置の内部と外部装置との間におけるデータの入出力を制御する。

【0043】

ここで、ATM131の場合、上述した出力デバイス223や入力デバイス224には、以下のデバイスを含む。

【0044】

たとえば、ATM131の場合、出力デバイス223は、プリンタを含む。プリンタは、取引結果を印字する。たとえば、プリンタは、預金通帳123の記帳や、利用明細書の印字をおこなう。ATM131の場合、入力デバイス224は、カードリーダを含む。カードリーダは、カード122の識別情報などのカード情報を読み取る。

【0045】

(各種DB112, 113の記憶内容)

つぎに、図3Aおよび図3Bを用いて、図1に示した銀行サーバ111が有する口座情報データベース(DB)112および取引情報データベース(DB)113の記憶内容について説明する。各種DB112, 113は、たとえば、メモリ212などの記憶部により実現される。

【0046】

図3Aは、口座情報データベース(DB)112の記憶内容の一例を示す説明図である。図3Aにおいて、口座情報データベース112は、口座ID(Identification)、氏名、住所、端末情報、金融機関コード、支店番号、口座番号、および残額のフィールドを有する。各フィールドに情報を設定することで、口座情報(たとえば、口座情報300-1, 300-2)のレコードが記憶される。

【0047】

口座IDは、口座情報300を識別する識別情報を示す。氏名は、銀行口座の名義人(利用者)の氏名を示す。住所は、銀行口座の名義人の住所を示す。端末情報は、銀行口座の名義人が有する端末装置(利用者端末121)のアドレスである。金融機関コードは、金融機関ごとに割り当てられたコードである。支店番号は、金融機関の支店に割り当てられた番号である。口座番号は、口座に割り当てられた番号である。残額は、口座内の残額である。

【0048】

たとえば、口座情報300-1は、口座ID「U001」、氏名「総研総太郎」、住所「東京都…」、端末情報「aaa・・・@xxx」、金融機関コード「0000」、支店番号「345」、口座番号「123…」、残額「¥96,390」を示す。また、口座情報300-2についても、同様に、口座情報DB112に記憶される。

【0049】

図3Bは、実施の形態1にかかる取引情報データベース(DB)113の記憶内容の一例を示す説明図である。図3Bにおいて、取引情報DB113は、取引ID、口座ID、氏名、取引日時、取引内容、取引金額、残額、記帳の有無、認証情報の生成方式、および認証情報のフィールドを有する。各フィールドに情報を設定することで、取引情報(たとえば、取引情報310-1~310-6)のレコードが記憶される。

【0050】

取引IDは、取引を識別する識別情報を示す。口座IDは、口座を識別する識別情報を示し、口座情報DB112(図3Aを参照)に記憶される口座IDと同一である。このため、口座情報DB112の口座情報300と取引情報310とは、口座IDによって対応付けられている。

【0051】

また、取引情報DB113において、氏名は、口座情報DB112の口座情報300に

10

20

30

40

50

含まれる氏名と同一である。取引日時は、取引をおこなった日付を示す。取引内容は、出金、入金、振込といった取引の種別を示す。取引金額は、取引をおこなった金額を示す。残額は、取引後の口座の預金額である。記帳の有無は、預金通帳 1 2 3 に取引内容や残額等の記帳をおこなったか否かを示す。

【0052】

認証情報の生成方式は、残額を用いて4桁の認証情報（暗証番号）を生成する際の方式を示す。認証情報の生成方式は、たとえば、残額の「下4桁」や「上4桁」などを設定することが可能である。

【0053】

認証情報は、残額と、認証情報の生成方式とに基づいて生成される。認証情報の生成について、取引情報 310-1 を例に挙げて説明すると、認証情報は、残額が「¥101,000」であり、認証情報の生成方式が「下4桁」であるため、残額「¥101,000」の「下4桁」である「1000」となる。すなわち、次の取引において用いられる認証情報は、「1000」となる。

10

【0054】

認証情報の生成方式は、利用者によって、残額に応じた認証情報の生成を設定することが可能であり、残額に応じた認証情報の生成をおこなわない設定（認証情報が固定の設定）を「-」で示す。また、残額の「下4桁」とするか、「上4桁」とするかについても、利用者によって設定される。利用者による各設定は、たとえば、預金口座の初期登録時におこなわれてもよいし、預金口座が利用可能になってから利用者からの登録操作に応じておこなわれてもよい。認証情報は、次の取引において用いられる認証情報（暗証番号）を示す。

20

【0055】

ここで、たとえば、取引情報 310-1 は、取引ID「T001」、口座ID「K001」、氏名「総研総太郎」、取引日時「2017年12月1日」、取引内容「入金」、残額「¥101,000」、記帳の有無「有り」、認証情報の生成方式「下4桁」、認証情報「1000」を示す。また、取引情報 310-1 以外の取引情報 310-2～310-6 についても、同様に、取引情報 DB 113 に記憶される。

【0056】

（実施の形態1にかかる認証情報の生成例）

30

つぎに、図4を用いて、実施の形態1にかかる認証情報の生成例について説明する。図4は、実施の形態1にかかる認証情報の生成例を示す図である。以下に示す括弧書きの番号は、図4に示す括弧書きの番号と対応する。

【0057】

図4に示すように、（1）2017年12月1日に、利用者がATM131に預金通帳123を挿入し、所定の暗証番号を入力し、¥10,000の入金をおこなったことにより、残額が¥101,000となったとする。この場合、預金通帳123には、その旨を示す取引履歴が印字される。そして、残額が¥101,000であることから、たとえば、下4桁の認証情報である「1000」が次の認証情報（暗証番号）となる。

【0058】

40

また、（2）2017年12月11日に、利用者がATM131に預金通帳123を挿入し、前回の取引で更新された暗証番号「1000」を入力し、¥4,500の出金をおこなったことにより、残額が¥96,500となったとする。この場合、預金通帳123には、その旨を示す取引履歴が印字される。そして、残額が¥96,500であることから、たとえば、下4桁の認証情報である「6500」が次の認証情報（暗証番号）となる。

【0059】

さらに（3）2017年12月22日に、利用者がATM131に預金通帳123を挿入し、前回の取引で更新された暗証番号「6500」を入力し、¥10の出金をおこなったことにより、残額が¥96,490となったとする。この場合、預金通帳123には、

50

その旨を示す取引履歴が印字される。そして、残額が¥ 96, 490であることから、たとえば、下4桁の認証情報である「6490」が次の認証情報（暗証番号）となる。

【0060】

そして、(4) 2017年12月25日に、利用者がATM131に預金通帳123を挿入せずに、カード122を挿入し、前回の取引で更新された暗証番号「6490」を入力し、¥100の出金をおこなったことにより、残額が¥96, 390となったとする。この場合、利用明細書400に、その旨を示す取引履歴が印字される。そして、残額が¥96, 390であるものの、預金通帳123に記帳された残額は¥96, 490であることから、認証情報に変更はなく、すなわち、認証情報である「6490」を保持する。

【0061】

なお、(4)においては、カード122のみで取引をおこなっていることから、利用者が預金通帳123を所持していないこともある。この場合、利用者は、前回の取引で更新された暗証番号「6490」がわからないことがある。そこで、詳細については図6Aおよび図6Bを用いて後述するが、利用者端末121には、取引履歴を表示することが可能となっている。

【0062】

図4に説明したように、実施の形態1では、預金通帳123に記帳された残額と、所定の認証情報の生成方式とに基づいて、以降の取引に用いられる認証情報が生成される。このため、認証情報を随時更新することができるとともに、利用者が認証情報を覚えていなくても、預金通帳123を見るだけで、認証情報を容易に把握することができる。したがって、取引の利便性が低下することを抑えつつ、カード122を用いた取引のセキュリティを簡単に高めることができる。

【0063】

(実施の形態1にかかる認証情報生成システム100の機能的構成)

図5は、実施の形態1にかかる認証情報生成システム100の機能的構成を示す説明図である。図5において、認証情報生成システム100は、銀行サーバ111と、利用者端末121と、ATM131とを備える。

【0064】

銀行サーバ111は、取引情報受信部501と、取引制御部502と、取引結果送信部503と、取引履歴受信部504と、取引履歴記憶部505と、取引履歴取得部506と、認証情報生成部507と、生成方式記憶部508と、認証情報記憶部509と、口座情報記憶部510と、出力制御部511と、端末通信部512と、記憶制御部513とを備える。

【0065】

ATM131は、取引情報入力部521と、取引情報送信部522と、取引結果受信部523と、取引処理部524と、処理結果出力部525とを備える。

【0066】

ここで、利用者が、ATM131を介して、各種取引を開始させる場合について説明する。ATM131の取引情報入力部521は、取引情報を入力する。取引情報は、挿入されたカード122から読み取ったカード情報や、挿入された預金通帳123に記載される内容や、利用者から入力される認証情報（暗証番号）や取引内容である。認証情報は、たとえば、4桁の数字であるが、これに限らず、4桁以外の数字であってもよいし、また、文字や記号を含んでもよい。

【0067】

ここで、詳細については、後述するが、認証情報は、たとえば、預金通帳123に記載された、前回の取引における残額に基づいて生成される。このため、利用者は、預金通帳123に記載された、前回の取引における残額を閲覧して、所定の生成方式で生成される認証情報を確認してから、今回の取引における認証情報を入力する。取引情報入力部521は、ATM131の入力デバイス224によって実現される。

【0068】

10

20

30

40

50

取引情報送信部 5 2 2 は、取引情報入力部 5 2 1 に入力された取引情報を銀行サーバ 1 1 1 へ送信する。取引情報送信部 5 2 2 は、A T M 1 3 1 の通信 I F 2 2 5 によって実現される。

【 0 0 6 9 】

取引情報送信部 5 2 2 から取引情報が銀行サーバ 1 1 1 へ送信されると、銀行サーバ 1 1 1 の取引情報受信部 5 0 1 は、取引情報を受信する。取引情報受信部 5 0 1 は、A T M 1 3 1 から受信した取引情報を取引制御部 5 0 2 へ出力する。取引情報受信部 5 0 1 は、銀行サーバ 1 1 1 の通信 I F 2 1 3 によって実現される。

【 0 0 7 0 】

取引制御部 5 0 2 は、取引情報受信部 5 0 1 から取引情報が入力されると、当該取引情報に含まれる、利用者から受け付けた認証情報が、各利用者の認証情報を記憶する認証情報記憶部 5 0 9 に記憶されているか否かの一致判定（認証）をおこなう。当該一致判定において、否定の判定結果が得られた場合（認証に失敗した場合）、取引制御部 5 0 2 は、認証に失敗した旨を示す取引結果を取引結果送信部 5 0 3 へ出力する。

【 0 0 7 1 】

一方、一致判定において、肯定の判定結果が得られた場合（認証に成功した場合）、取引制御部 5 0 2 は、取引情報に含まれる、利用者から受け付けた取引内容での取引を可能にする。具体的には、たとえば、取引内容が出金や振込である場合、取引制御部 5 0 2 は、預金額等を記憶する口座情報記憶部 5 1 0 を参照し、利用者から受け付けた金額分の残額が口座情報記憶部 5 1 0 に記憶されているか否かの金額判定をおこなう。

【 0 0 7 2 】

当該金額判定において、否定の判定結果が得られた場合（残金がない場合）、取引制御部 5 0 2 は、その旨を示す取引結果を取引結果送信部 5 0 3 へ出力する。一方、当該金額判定において、肯定の判定結果が得られた場合（残金がある場合）、取引制御部 5 0 2 は、取引情報に含まれる、利用者から受け付けた取引内容の取引をおこなうとともに、その旨を示す取引結果を取引結果送信部 5 0 3 へ出力する。

【 0 0 7 3 】

取引制御部 5 0 2 は、銀行サーバ 1 1 1 のメモリ 2 1 2 に記憶されたプログラムを C P U 2 1 1 に実行させることにより、その機能を実現する。認証情報記憶部 5 0 9 および口座情報記憶部 5 1 0 は、銀行サーバ 1 1 1 のメモリ 2 1 2 によって実現される。具体的には、認証情報記憶部 5 0 9 は、取引情報 D B 1 1 3 （図 3 B を参照）によって実現される。また、口座情報記憶部 5 1 0 は、口座情報 D B 1 1 2 （図 3 A を参照）によって実現される。ただし、認証情報記憶部 5 0 9 および口座情報記憶部 5 1 0 は、銀行サーバ 1 1 1 に設けられずに、外部の他の装置に設けられていてもよい。

【 0 0 7 4 】

取引結果送信部 5 0 3 は、取引制御部 5 0 2 から取引結果が入力されると、入力された取引結果を A T M 1 3 1 へ送信する。取引結果送信部 5 0 3 から取引結果が A T M 1 3 1 へ送信されると、A T M 1 3 1 の取引結果受信部 5 2 3 は、取引結果を受信する。取引結果受信部 5 2 3 は、銀行サーバ 1 1 1 から受信した取引結果を取引処理部 5 2 4 へ出力する。取引結果受信部 5 2 3 は、A T M 1 3 1 の通信 I F 2 2 5 によって実現される。

【 0 0 7 5 】

取引処理部 5 2 4 は、取引結果受信部 5 2 3 から受信した取引結果に応じた取引処理をおこなう。具体的には、たとえば、取引内容が出金である場合には、取引結果に応じて、所定の払出口から所定の金額を払い出したり、取引結果を示す通知を音声や表示によりおこなったりする。また、たとえば、認証に失敗した場合や取引をおこなえない旨を示す取引結果である場合、取引処理部 5 2 4 は、その旨を示す通知を音声や表示によりおこなう。

【 0 0 7 6 】

また、取引処理部 5 2 4 は、取引結果に応じた取引処理をおこなうと、取引処理の処理結果を処理結果出力部 5 2 5 へ出力する。取引処理部 5 2 4 は、A T M 1 3 1 のメモリ 2 2 2 に記憶されたプログラムを C P U 2 2 1 に実行させることにより、その機能を実現す

10

20

30

40

50

る。

【0077】

処理結果出力部525は、取引処理部524から取引処理の処理結果が入力されると、処理結果を銀行サーバ111へ送信する。また、処理結果出力部525は、取引がおこなわれた場合であり、且つ預金通帳123が挿入されている場合には、処理結果を預金通帳123に記帳（印字）する。さらに、処理結果出力部525は、預金通帳123に記帳すると、記帳したことを示す記帳情報を含む取引履歴を銀行サーバ111へ送信する。処理結果出力部525は、ATM131の出力デバイス223（プリンタ）や通信IF225によって実現される。

【0078】

処理結果出力部525から取引履歴が銀行サーバ111へ送信されると、銀行サーバ111の取引履歴受信部504は、取引履歴を受信する。取引履歴受信部504は、ATM131から受信した取引履歴を取引履歴記憶部505へ出力する。取引履歴記憶部505は、取引履歴受信部504から入力した取引履歴を記憶する。上述したように、取引履歴には、記帳したことを示す記帳情報が含まれているため、取引履歴記憶部505は、取引ごとに記帳されているか否かを記憶することができる。

【0079】

取引履歴受信部504は、銀行サーバ111の通信IF213によって実現される。取引履歴記憶部505は、銀行サーバ111のメモリ212によって実現される。具体的には、取引履歴記憶部505は、取引情報DB113（図3Bを参照）によって実現される。

【0080】

取引履歴取得部506は、取引履歴記憶部505から、取引履歴を取得する。取引履歴は、利用者が閲覧可能な取引に関する履歴である。利用者が閲覧可能とは、預金通帳123に記載されることによって閲覧可能であることや、利用者端末121に表示されることによって閲覧可能であることである。

【0081】

取引履歴は、金融機関が発行する預金通帳123に印字された情報（以下「記帳情報」という）や、印字されていない情報を含む。金融機関は、たとえば銀行110であるが、郵便局や信用金庫などであってもよい。記帳情報は、たとえば、日付、出金額や入金額といった取引の額、残額、振込先、といった情報を含む。

【0082】

認証情報生成部507は、取引履歴取得部506によって取得された取引履歴に基づいて、以降の取引において用いられる認証情報を生成する。取引履歴に基づく認証情報の生成は、利用者によって設定される。利用者による設定は、利用者が自らおこなう設定でもよいし、利用者の申告に基づいて銀行110のスタッフがおこなう設定でもよい。

【0083】

取引履歴に基づく認証情報の生成をおこなわない設定となっている場合、認証情報は、固定されたままとなる。一方で、取引履歴に基づく認証情報の生成をおこなう設定となっている場合、認証情報は、取引履歴に基づいて更新される。

【0084】

認証情報の生成について具体的に説明すると、認証情報生成部507は、預金通帳123に印字された記帳情報に基づいて、金融機関における以降の取引において用いられる認証情報を生成する。特に、記帳情報は、直近の記帳情報である。この場合、取引履歴取得部506は、預金通帳123に印字された直近の記帳情報を取得する。直近の記帳情報は、預金通帳に最後に記帳された情報である。認証情報生成部507は、取引履歴取得部506によって取得された直近の記帳情報に基づいて、認証情報を生成する。

【0085】

認証情報生成部507は、生成方式記憶部508に記憶される、予め設定される生成方式により認証情報を生成する。具体的には、認証情報生成部507は、預金通帳123に印字された記帳情報が示す金額（たとえば残額）の中から、予め設定された複数の桁に該

10

20

30

40

50

当する数字をそれぞれ選択して認証情報を生成する。

【0086】

具体的には、認証情報生成部507は、最後に記帳された残額のうち、予め設定された複数の桁（認証情報の桁）に該当する数字をそれぞれ選択して認証情報を生成する。たとえば、認証情報が4桁の数字であれば、認証情報生成部507は、下4桁や上4桁といった数字を選択して認証情報を生成する。

【0087】

ただし、認証情報生成部507は、下4桁や上4桁といった数字を選択することに限らず、たとえば、5桁目と、4桁目と、2桁目と、1桁目などのように、特定の桁の数字を選択してもよい。また、下4桁とするか、上4桁とするかといった、選択の対象となる桁は、利用者によって設定されてもよい。

10

【0088】

たとえば、認証情報生成部507は、最後に記帳された残額が「¥96,490」であり、下4桁を選択する設定となっている場合には、下4桁に該当する「6」、「4」、「9」、「0」を選択する。認証情報生成部507は、選択した数字を、予め設定した所定の並べ方で並べて認証情報を生成する。

【0089】

所定の並べ方は、たとえば、左から並べる並べ方であり、この場合、上記の例では「6490」が認証情報となる。ただし、所定の並べ方は、これに限らず、たとえば、右から並べる並べ方としてもよく、この場合、上記の例では「0946」が認証情報となる。また、所定の並べ方は、利用者によって設定されてもよい。

20

【0090】

同様に、たとえば、上4桁を選択する設定となっており、最後に記帳された残額が「¥96,490」である場合には、認証情報生成部507は、上4桁に該当する「9」、「6」、「4」、「9」を選択し、所定の並べ方で並べて認証情報を生成すればよい。

【0091】

なお、預金通帳123に記帳された残額が、認証情報に該当する複数の桁（4桁）に満たない場合、具体的には、たとえば、認証情報が4桁であるものの、残額が「¥1,000」未満（たとえば「¥512」）の場合、記帳のない位（千の位）については、所定の数字（たとえば「0」）を補って、認証情報を「0512」とすればよい。記帳のない桁がある場合に補う所定の数字は、利用者によって設定されてもよい。

30

【0092】

また、詳細については図9Aを用いて後述するが、認証情報生成部507は、預金通帳123に記帳された数字を、横方向に選択して認証情報を生成するのではなく、縦方向に選択して認証情報を生成してもよい。たとえば、預金通帳123に4回以上の取引をおこなったことにより、記帳された段数が4段以上ある場合、特定の桁（たとえば1桁目）に該当する数字を縦方向に選択して認証情報とすることも可能である。

【0093】

また、認証情報生成部507は、預金通帳123に記載された残額の中から数字を選択することに限らず、たとえば、預金通帳123に記帳された、入金額や出金額の中から数字を選択して、認証情報を生成してもよい。

40

【0094】

さらに、認証情報生成部507は、預金通帳123に記載された金額の中から数字を選択することに限らない。詳細については、図9Bを用いて後述するが、認証情報生成部507は、たとえば、預金通帳123に記帳された日付の情報を選択して、認証情報を生成してもよい。

【0095】

また、認証情報生成部507は、ガス料金、電気料金、水道料金などの公共料金の支払のように、特定の支払先が定められており、且つ、定期的に引き落とされる記帳情報が得られる場合には、当該引き落としの額を用いて認証情報を生成してもよい。具体的には、

50

たとえば、引き落としの対象がガス料金に設定されているとすると、認証情報生成部 507 は、ガス料金の引き落としがある都度、その引き落としの額に応じて、認証情報を生成してもよい。

【0096】

これにより、予め設定された特定の引き落としがあった場合に、認証情報を更新することができる。また、特定の引き落としをいずれにするかの指定は、利用者によって設定されてもよい。これにより、第三者に預金通帳 123 が盗まれたり、紛失したりしたとしても、第三者が認証情報の生成方式を把握することをより困難にすることができるため、認証情報生成システム 100 にかかるセキュリティをより向上させることができる。

【0097】

また、認証情報は、直近の記帳情報に基づいて生成されることに限らず、予め設定した特定の時期の記帳情報に基づいて生成されてもよい。たとえば、特定の時期を年末としたとすると、年末の最後に記帳された記帳情報に基づいて生成された認証情報を、翌年の 1 年間の認証情報とすることも可能である。このように、特定の時期を設定することにより、認証情報を更新する期間を定めることができる。

【0098】

記憶制御部 513 は、認証情報生成部 507 によって生成された認証情報を認証情報記憶部 509 に記憶させる。認証情報生成部 507 および記憶制御部 513 は、銀行サーバ 111 のメモリ 212 に記憶されたプログラムを CPU 211 に実行させることにより、その機能を実現する。生成方式記憶部 508 は、銀行サーバ 111 のメモリ 212 によって実現される。具体的には、生成方式記憶部 508 は、取引情報 DB 113（図 3B を参照）によって実現される。ただし、生成方式記憶部 508 は、銀行サーバ 111 に設けられずに、外部の他の装置に設けられていてもよい。

【0099】

このように、認証情報は、認証情報生成部 507 が、予め生成しておいて、記憶制御部 513 が、認証情報生成部 507 によって生成された認証情報を認証情報記憶部 509 に記憶させておく。そして、認証要求を受信した際には、認証情報記憶部 509 に記憶されている認証情報を抽出して、抽出された認証情報に基づいて認証をおこなうようにする。このようにすることによって、認証要求があるごとに、認証情報を生成しておく必要がない。

【0100】

あるいは、認証情報生成部 507 は、認証情報を予め生成しない。したがって、記憶制御部 513 は、認証情報を認証情報記憶部 509 に記憶させない。そして、認証要求を受信した際には、はじめて、認証情報の生成方式に基づいて認証情報を生成して、生成した認証情報に基づいて認証をおこなうようにしてもよい。

【0101】

このように、認証情報は、予め生成して記憶手段に記憶させておいても良いが、認証要求を受信したときに定められた認証情報の生成方式に基づいて認証情報を生成する（予め記憶しない）ようにしてもよい。したがって、そのように構成する場合には、認証情報記憶部 509 は設けなくてもよい。

【0102】

つぎに、利用者によっては、取引の際に、預金通帳 123 を所持しないことが想定される。このようなことに鑑み、取引において預金通帳 123 を用いたか否かにかかわらず、取引履歴を利用者端末 121 に記憶可能にすることについて説明する。

【0103】

具体的には、ATM 131 において、利用者が取引を終える際に、出力制御部 511 は、預金通帳 123 に印字された情報と、預金通帳 123 に印字されていない情報とを区別させるための付加情報を、取引履歴とともに所定の端末に表示可能にするための制御をおこなえばよい。

【0104】

10

20

30

40

50

付加情報は、預金通帳 1 2 3 に印字された情報に対して、「記帳済」の文字を付す旨の情報や、記帳済を示すマークを付す旨の情報であってもよい。また、付加情報は、預金通帳 1 2 3 に印字された情報と、預金通帳 1 2 3 に印字されていない情報とを異なる表示態様とする旨の情報であってもよい。所定の端末は、たとえば、利用者端末 1 2 1 である。

【0105】

出力制御部 5 1 1 は、付加情報と取引履歴とを、たとえば、利用者端末 1 2 1 が読取可能な QR コードによって出力してもよい。利用者端末 1 2 1 は、ディスプレイに表示された QR コードを、利用者端末 1 2 1 が備えるリーダ（カメラ）で読み取ることにより、付加情報と取引履歴とを、利用者端末 1 2 1 のメモリ 2 2 2 に記憶すればよい。そして、利用者端末 1 2 1 は、メモリ 2 2 2 に記憶した付加情報と取引履歴とを用いて、預金通帳 1 2 3 に印字された情報と、預金通帳 1 2 3 に印字されていない情報とを区別して表示すればよい。

10

【0106】

これにより、利用者は、ATM 1 3 1 において取引をおこなった際に、取引履歴を利用者端末 1 2 1 に記憶させることができる。このため、利用者は、以降に取引をおこなう際に、預金通帳 1 2 3 を所持していなくても、利用者端末 1 2 1 に記憶された取引履歴を閲覧して、認証情報を容易に把握することができる。

【0107】

また、出力制御部 5 1 1 は、付加情報と取引履歴とを、QR コードによって出力することに限らず、予め登録された利用者端末 1 2 1 へ電子メールや SNS（Social Networking Service）等で送信してもよい。具体的には、出力制御部 5 1 1 は、端末通信部 5 1 2 を制御して、予め登録された利用者端末 1 2 1 へ付加情報と取引履歴とを送信させる制御をおこなえばよい。

20

【0108】

この場合、利用者端末 1 2 1 は、銀行サーバ 1 1 1 から受信した付加情報と取引履歴とをメモリ 2 2 2 に記憶すればよい。また、利用者端末 1 2 1 は、メモリ 2 2 2 に記憶した付加情報と取引履歴とを用いて、預金通帳 1 2 3 に印字された情報と、預金通帳 1 2 3 に印字されていない情報とを区別して表示すればよい。

【0109】

これにより、利用者は、ATM 1 3 1 において取引をおこなった際に、取引履歴を利用者端末 1 2 1 に記憶させることができる。このため、利用者は、以降に取引をおこなう際に、預金通帳 1 2 3 を所持していなくても、利用者端末 1 2 1 に記憶された取引履歴を閲覧して、認証情報を容易に把握することができる。

30

【0110】

つぎに、銀行サーバ 1 1 1 は、利用者端末 1 2 1 から送信要求に応じて取引履歴を利用者端末 1 2 1 へ送信する場合について説明する。まず、利用者の操作により、利用者端末 1 2 1 が、銀行サーバ 1 1 1 へ取引履歴の送信要求をおこなう。送信要求は、たとえば、SNS でおこなわれる。この SNS は、たとえば、本認証情報生成システム 1 0 0 の利用にかかる登録時に、利用者端末 1 2 1 および銀行サーバ 1 1 1 の双方の認証がおこなわれている。このため、利用者は、SNS を利用する際に、ログインやパスワードの入力などを要しない。

40

【0111】

端末通信部 5 1 2 は、利用者端末 1 2 1 から取引履歴の送信要求を受信する。出力制御部 5 1 1 は、端末通信部 5 1 2 によって取引履歴の送信要求を受信された場合に、取引履歴を利用者端末 1 2 1 に送信する制御をおこなう。利用者端末 1 2 1 に送信する取引履歴は、直近の記帳情報を含む。

【0112】

また、利用者端末 1 2 1 に送信する取引履歴は、直近の記帳情報のほかに、他の記帳情報を含んでもよいし、預金通帳 1 2 3 に印字されていない情報を含んでもよい。ただし、取引履歴に、預金通帳 1 2 3 に印字されていない情報が含まれる場合、出力制御部 5 1 1

50

は、取引履歴と付加情報とを利用者端末 1 2 1 に送信すればよい。

【0 1 1 3】

出力制御部 5 1 1 の制御により、端末通信部 5 1 2 は、取引履歴を利用者端末 1 2 1 へ送信する。端末通信部 5 1 2 は、たとえば、SNS で取引履歴を利用者端末 1 2 1 へ送信する。利用者端末 1 2 1 は、銀行サーバ 1 1 1 から受信した取引履歴を表示する。取引履歴に、預金通帳 1 2 3 に印字されていない情報が含まれる場合、利用者端末 1 2 1 は、預金通帳 1 2 3 に印字された情報と、預金通帳 1 2 3 に印字されていない情報とを区別して表示すればよい。

【0 1 1 4】

これにより、利用者は、預金通帳 1 2 3 を所持していなくても、銀行サーバ 1 1 1 から受信した取引履歴を閲覧して、認証情報を容易に把握することができる。

10

【0 1 1 5】

なお、SNS に限らず、利用者が銀行サーバ 1 1 1 の所定のサイトにアクセスすることにより、取引履歴を閲覧することも可能である。具体的には、利用者端末 1 2 1 は、所定のサイトにアクセスし、利用者から受け付けたログイン ID やログインパスワードを銀行サーバ 1 1 1 に送信し、銀行サーバ 1 1 1 における認証に成功することにより、取引履歴を受信することができる。これにより、利用者端末 1 2 1 は、銀行サーバ 1 1 1 から受信した取引履歴を、利用者端末 1 2 1 のメモリ 2 2 2 に記憶させることも可能である。

【0 1 1 6】

端末通信部 5 1 2 は、銀行サーバ 1 1 1 の通信 IF 2 1 3 によって実現される。出力制御部 5 1 1 は、銀行サーバ 1 1 1 のメモリ 2 1 2 に記憶されたプログラムを CPU 2 1 1 に実行させることにより、その機能を実現する。

20

【0 1 1 7】

(利用者端末 1 2 1 に記憶される取引履歴の表示例)

つぎに、図 6 A を用いて、利用者端末 1 2 1 に表示される取引履歴の表示例について説明する。図 6 A は、利用者端末 1 2 1 に表示される取引履歴の表示例を示す説明図である。図 6 A の表示画面 6 0 0 は、取引履歴 6 0 1 ~ 6 0 4 の一覧を示す。各取引履歴 6 0 1 ~ 6 0 4 は、それぞれ、取引をおこなった日時と、取引の内容と、記帳の有無と、取引額と、残額とを示す。

【0 1 1 8】

取引履歴 6 0 1 ~ 6 0 4 は、たとえば、利用者端末 1 2 1 のメモリ 2 1 2 に記憶された情報である。取引履歴 6 0 1 ~ 6 0 4 は、たとえば、取引終了時に ATM 1 3 1 のディスプレイに表示される QR コードを利用者端末 1 2 1 に読み取られたり、取引終了時に銀行サーバ 1 1 1 から利用者端末 1 2 1 に送信されたりすることにより、利用者端末 1 2 1 のメモリ 2 1 2 に記憶された情報である。

30

【0 1 1 9】

認証情報を残額の下 4 桁とする設定となっていたとすると、利用者は、直近に記帳した内容である取引履歴 6 0 3 を閲覧することにより、残額「¥ 9 6 , 4 9 0」の下 4 桁「6 4 9 0」が認証情報であることを把握することができる。

【0 1 2 0】

(利用者端末 1 2 1 が SNS により取得した直近の記帳情報の表示例)

つぎに、図 6 B を用いて、利用者端末 1 2 1 が SNS により取得した直近の記帳情報の表示例について説明する。図 6 B は、利用者端末 1 2 1 が SNS により取得した直近の記帳情報の表示例を示す説明図である。図 6 B の表示画面 6 1 0 は、SNS のメッセージを示す。

40

【0 1 2 1】

メッセージ 6 1 1 は、利用者から銀行サーバ 1 1 1 への、記帳情報の送信要求を示す。メッセージ 6 1 1 は、たとえば、予め複数の定型文が用意されており、利用者がいずれか一つを選択可能であってもよい。メッセージ 6 1 2 は、メッセージ 6 1 1 に対する銀行サーバ 1 1 1 の回答である。メッセージ 6 1 1 を定型文とした場合、銀行サーバ 1 1 1 は、

50

受信した定型文に応じた回答を利用者ごとにおこなえばよい。

【0122】

認証情報を残額の下4桁とする設定となっていたとすると、利用者は、メッセージ612を閲覧することにより、残額「¥96,490」の下4桁「6490」が認証情報であることを把握することができる。

【0123】

(銀行サーバ111がおこなう認証情報生成処理手順の一例)

つぎに、図7を用いて、銀行サーバ111がおこなう認証情報生成処理手順の一例について説明する。図7は、銀行サーバ111がおこなう認証情報生成処理手順の一例を示すフローチャートである。

【0124】

図7において、銀行サーバ111は、預金通帳123が記帳されたか否かを判断する(ステップS701)。預金通帳123が記帳されたとは、ATM131において預金通帳123への記帳がおこなわれて、記帳したことを示す記帳情報を、ATM131から受信することである。銀行サーバ111は、預金通帳123が記帳されるまで待つ(ステップS701:No)。

【0125】

銀行サーバ111は、預金通帳123が記帳された場合(ステップS701:Yes)、取引情報DB113(図3Bを参照)に記憶される、認証情報の生成方式を参照する(ステップS702)。そして、銀行サーバ111は認証情報を生成する設定となっているか否かを判断する(ステップS703)。

【0126】

銀行サーバ111は、認証情報を生成する設定となっていない場合(ステップS703:No)、具体的には、取引情報DB113に記憶される「認証情報の生成方式」が記憶されていない場合、そのまま一連の処理を終了する。

【0127】

一方、銀行サーバ111は、認証情報を生成する設定となっている場合(ステップS703:Yes)、具体的には、取引情報DB113の「認証情報の生成方式」のフィールドに「下4桁」や「上4桁」等が記憶されている場合、記帳された残額と、参照した生成方式とに基づいて、以降の取引に用いられる認証情報を生成する(ステップS704)。

【0128】

つぎに、銀行サーバ111は、取引情報DB113に、生成した認証情報を記憶し(ステップS705)、一連の処理を終了する。取引情報DB113に記憶された認証情報は、次回以降の取引において用いられる。

【0129】

上述した処理によれば、預金通帳123が記帳されるたびに、残額に応じた認証情報に、認証情報を更新することができる。これにより、カード122を用いた取引のセキュリティを向上させることができる。

【0130】

(銀行サーバ111がおこなう取引履歴の出力処理手順の一例)

つぎに、図8を用いて、銀行サーバ111がおこなう取引履歴の出力処理手順の一例について説明する。図8は、銀行サーバ111がおこなう取引履歴の出力処理手順の一例を示すフローチャートである。

【0131】

図8において、銀行サーバ111は、取引履歴を出力するタイミングであるか否かを判断する(ステップS801)。取引履歴を出力するタイミングとは、たとえば、利用者端末121からの取引履歴の送信要求を受信したタイミングである。ただし、取引履歴を出力するタイミングとは、これに限らず、取引終了時に取引履歴をQRコードで出力するタイミングや、取引終了時に利用者端末121に取引履歴を送信するタイミングなどであってもよい。

10

20

30

40

50

【0132】

銀行サーバ111は、取引履歴を出力するタイミングとなるまで待つ（ステップS801：No）。銀行サーバ111は、取引履歴を出力するタイミングとなった場合（ステップS801：Yes）、取引情報DB113（図3Bを参照）に記憶される、取引日時、取引内容、取引金額、残額を含む、取引履歴を取得する（ステップS802）。

【0133】

そして、銀行サーバ111は、取引履歴を出力し（ステップS803）、一連の処理を終了する。取引履歴の出力は、利用者端末121へ取引履歴を送信することである。ただし、取引履歴の出力は、これに限らず、取引終了時においてQRコードで取引履歴を出力することとしてもよいし、取引終了時に利用者端末121に取引履歴を送信することとしてもよい。

10

【0134】

（認証情報の生成の他の例）

つぎに、図9Aおよび図9Bを用いて、認証情報の生成の他の例について説明する。図9Aは、認証情報の生成の他の例を示す図（その1）である。

【0135】

図9Aに示すように、取引一覧900は、預金通帳123に記帳された取引履歴901～905を示す。取引履歴901～905は、5回の取引があったことを示す。取引一覧900は、記帳された段数が4段以上ある。このため、たとえば、特定の桁に該当する数字を縦方向に選択して認証情報とすることも可能である。

20

【0136】

具体的には、たとえば、4段の取引履歴902～905について説明すると、上段から下段にかけて「¥86,079」、「¥82,811」、「¥77,811」、「¥75,380」の残額の記帳がある。また、たとえば、1桁目を下段から上段に向けて選択するものとする。この場合、認証情報は、各残額の1桁目を下段から上段に向けて選択した「0119」とすればよい。

【0137】

また、特定の桁に該当する数字を縦方向に選択して認証情報とする場合、預金通帳123において、最後に記帳が埋まったページ（改ページをおこなう前のページ）の最下段から下4段目までに記載された数字を用いることとしてもよい。これにより、数字を縦方向に選択することとする場合、利用者が参照するページが複数のページに跨ることがないため、利用者にとって、認証情報が把握しにくくなることを抑えることができる。

30

【0138】

また、認証情報の更新の頻度を、改ページとなる頻度に応じた頻度とすることができ、具体的には、1ページ内の段数（たとえば20段）に相当する取引回数（20回）に応じた頻度（20回に1回）とすることができ。

【0139】

図9Bは、認証情報の生成の他の例を示す図（その2）である。なお、図9Bにおいて、図9Aと同様の内容については同様の符号を付し、説明を省略する。図9Bにおいては、預金通帳123に記帳された日付の情報を選択して、認証情報を生成する場合について説明する。

40

【0140】

具体的には、預金通帳123に記帳された直近の取引履歴905が示すように、日付が「17年12月29日」である場合には、月に該当する数字「12」と、日に該当する数字「29」とを選択し、「1229」を認証情報としてもよい。また、取引履歴905の日付から生成される認証情報は、これに限らず、年に該当する数字「17」と、月に該当する数字「12」とを選択し、「1712」としてもよい。また、選択した数字の並べ方は予め設定した任意の並べ方としてもよい。

【0141】

以上説明したように、実施の形態1にかかる銀行サーバ111によれば、利用者が閲覧

50

可能な取引履歴に基づいて、以降の取引において用いられる認証情報を生成して、記憶するため、取引履歴に応じて認証情報を更新することができる。これにより、利用者は、認証情報を覚えていなくても、取引履歴を見るだけで、認証情報を容易に把握することができる。

【0142】

ここで、セキュリティを向上させる手法として、生体情報を用いて認証をおこなう手法もある。生体情報を用いた認証をおこなう場合には、ATM131が生体情報に対応している必要がある。仮に、ATM131が生体情報に対応していない場合には、ATM131に生体情報を読み取る機能を付加させたり、ATM131自体を取り替えたりする必要があるため、手間やコストがかかる。また、生体情報が盗まれてしまうと、第三者による不正な取引がおこなわれる懸念もある。

10

【0143】

これに対して、実施の形態1にかかる銀行サーバ111によれば、生体情報を用いないため、生体情報が盗まれるおそれがなく、また、生体情報に対応していないATM131を用いることができる。また、実施の形態1にかかる銀行サーバ111によれば、利用者が銀行110の店舗に出向かずに、認証情報を随時更新することができるため、利用者や銀行110のスタッフの手間を抑え、迅速且つ簡単に、認証情報を変更することができる。

【0144】

したがって、実施の形態1にかかる銀行サーバ111によれば、取引の利便性が低下することを抑えつつ、カード122を用いた取引のセキュリティを簡単に向上させることができる。特に、実施の形態1にかかる銀行サーバ111によれば、利用者が認証情報を覚える必要がないため、認証情報を失念しやすい高齢者などの利用者に効果的である。

20

【0145】

また、実施の形態1にかかる銀行サーバ111は、預金通帳123に印字された情報に基づいて、銀行110における以降の取引において用いられる認証情報を生成することとした。

【0146】

これにより、利用者は、認証情報を覚えていなくても、利用者が所持する預金通帳123を見るだけで、認証情報を容易に把握することができる。たとえば高齢者など、利用者端末121を所有していない利用者や、利用者端末121に取引履歴を表示させることが煩雑であると感じる利用者でも、預金通帳123を見るだけで、認証情報を容易に把握することができる。

30

【0147】

また、実施の形態1にかかる銀行サーバ111は、預金通帳123に印字された直近の記帳情報に基づいて、認証情報を生成することとした。これにより、銀行サーバ111は、預金通帳123への記帳がおこなわれるごとに認証情報を更新することができる。したがって、利用者は、直近の記帳情報だけを閲覧すればよいと、認証情報を容易に把握することができる。また、認証情報の更新の頻度を高めることができるため、セキュリティをより向上させることができる。

【0148】

また、実施の形態1にかかる銀行サーバ111は、預金通帳123に印字された記帳情報が示す金額の中から、予め設定された複数の桁に該当する数字をそれぞれ選択して認証情報を生成することとした。これにより、銀行サーバ111は、たとえば、下4桁や上4桁といった利用者にとって把握しやすい数字の列を認証情報とすることができる。このため、利用者は、認証情報を容易に把握することができる。

40

【0149】

また、実施の形態1にかかる銀行サーバ111は、利用者による設定に応じて、取引履歴に基づく認証情報の生成をおこなうこととした。このため、銀行サーバ111は、利用者ごとに、取引履歴に基づく認証情報の生成をおこなったり、おこなわないようにしたりすることができる。

50

【0150】

また、実施の形態1にかかる銀行サーバ111は、利用者による設定に応じた認証情報の生成方式とした。このため、利用者が所望する生成方式を設定することができるため、預金通帳123やカード122が盗まれたり、紛失したりしたとしても、第三者が認証情報の生成方式を把握することをより困難にすることができる。したがって、銀行サーバ111によれば、セキュリティをより向上させることができる。

【0151】

また、実施の形態1にかかる銀行サーバ111は、預金通帳123に印字された記帳情報と、預金通帳123に印字されていない情報とを区別させるための付加情報を、取引履歴とともに利用者端末121に表示可能にするための制御をおこなうこととした。これにより、利用者は、預金通帳123を所持していなくても、利用者端末121に表示される取引履歴を閲覧することができる。また、利用者は、どこまでの取引が記帳されているのかを容易に把握することができるため、認証情報を覚えていなくても、認証情報を容易に把握することができる。

【0152】

(実施の形態2)

つぎに、この発明にかかる認証情報生成装置、認証情報生成方法、および認証情報生成プログラムの実施の形態2について、説明する。実施の形態1では、銀行のキャッシュカードの認証情報(暗証番号)を生成する場合について説明した。実施の形態2では、クレジットカードの認証情報(暗証番号)を生成する場合について説明する。なお、以下の説明において、実施の形態1で説明した内容と同様の内容については同様の符号を付し、説明を省略する。

【0153】

(認証情報生成システムのシステム構成)

実施の形態2にかかる認証情報生成システム1000のシステム構成例について説明する。図10は、実施の形態2にかかる認証情報生成システム1000のシステム構成例を示す説明図である。図10において、認証情報生成システム1000は、カード会社サーバ1011と、利用者端末121と、カード1022と、利用明細書1023と、店舗端末1031と、を有する。

【0154】

カード会社サーバ1011は、この発明にかかる認証情報生成装置の一例である。カード会社サーバ1011は、カード会社1010に設けられるサーバである。具体的には、カード会社サーバ1011は、利用者ごとのクレジットカードの利用限度額や現在の利用額等を管理する汎用的なコンピュータ装置である。カード会社サーバ1011は、たとえば、CPUやメモリやインタフェースなどを有するパーソナルコンピュータである。また、カード会社サーバ1011は、カード情報DB1012と、取引情報DB1013とを有する。各種DB1012、1013の記憶内容については、図11Aおよび図11Bを用いて後述する。

【0155】

カード1022は、カード会社1010が発行したクレジットカードである。利用明細書1023は、所定期間(たとえば1ヶ月)に1回、カード会社1010によって発行される。利用明細書1023は、クレジットカードを用いた決済(以下「カード決済」という)がおこなわれた1ヶ月の明細書である。

【0156】

店舗端末1031は、クレジットカードの決済機能を備え、決済用のネットワークを介して、インターネットなどのネットワーク140に接続されている。店舗端末1031は、カード決済にかかる各種の処理をおこなう。店舗端末1031は、カード決済にかかる各種の処理の実行に際して、カード会社サーバ1011との間で通信をおこなう。

【0157】

また、店舗端末1031は、利用者とカード会社サーバ1011とのインタフェースを

つかさどり、カード１０２２の利用状況を利用者に通知する。また、たとえば、店舗端末１０３１は、カード決済をおこなうごとにカード１０２２の利用状況を利用者に通知する。

【０１５８】

店舗端末１０３１は、購入する商品についての会計をおこなうレジスタや、カード１０２２のカード情報を読み取るカードリーダーや、カード会社サーバ１０１１に対してカード情報等を送受信する通信部などを備える。店舗端末１０３１は、具体的には、たとえばＣＡＴ（Credit Authorization Terminal）端末やＰＯＳ（Point Of Sales system）端末などのクレジットカードの信用照会端末などによって実現することができる。

【０１５９】

認証情報生成システム１０００において、カード会社サーバ１０１１と、利用者端末１２１と、店舗端末１０３１とは、有線または無線のネットワーク１４０を介して接続される。

【０１６０】

（各種ＤＢ１０１２，１０１３の記憶内容）

つぎに、図１１Ａおよび図１１Ｂを用いて、図１０に示したカード会社サーバ１０１１が有するカード情報ＤＢ１０１２および取引情報ＤＢ１０１３の記憶内容について説明する。各種ＤＢ１０１２，１０１３は、たとえば、メモリなどの記憶部により実現される。

【０１６１】

図１１Ａは、カード情報データベース（ＤＢ）１０１２の記憶内容の一例を示す説明図である。図１１Ａにおいて、カード情報ＤＢ１０１２は、カード番号、名義人、利用者端末情報、有効期限、セキュリティコード、限度額、および現在までの利用額のフィールドを有する。各フィールドに情報を設定することで、カード情報（たとえば、カード情報１１００－１，１１００－２）のレコードが記憶される。

【０１６２】

カード番号は、カード１０２２に記載される、たとえば１６桁の数字である。名義人は、カード１０２２の名義人を示す。利用者端末情報は、たとえば、名義人が有する利用者端末１２１のアドレス情報である。有効期限は、カード１０２２の利用可能な期限を示す。セキュリティコードは、たとえば、カード１０２２の裏面に記載される３桁の数字である。

【０１６３】

限度額は、一定期間内（たとえば１ヶ月間）においてカード１０２２を用いて支払をおこなうことのできる上限額を示す。また、現在までの利用額は、一定期間の開始（たとえば月初）から現在までの間にカード１０２２を用いて支払をおこなった額の総額を示す。現在までの利用額は、カード１０２２を用いて支払をおこなうたびに更新される。

【０１６４】

たとえば、カード情報１１００－１は、カード番号「１２３４…」、名義人「総研総太郎」、利用者端末情報「ＸＸＸ・・・＠ｘｘｘ」、有効期限「〇〇年〇〇月」、セキュリティコード「〇〇〇」、限度額「¥〇〇万」、現在までの利用額「¥〇〇〇〇」を示す。なお、不図示であるが、現金を融資するキャッシングの利用が可能である場合には、キャッシングについての情報（限度額や現在までの利用額）もカード情報ＤＢ１０１２に記憶される。

【０１６５】

カード情報ＤＢ１０１２に示す、カード番号、名義人、利用者端末情報、有効期限、セキュリティコード、および限度額については、カード１０２２を新規に作成する際に、利用者の申告やカード会社の審査結果に応じて設定される。なお、カード情報ＤＢ１０１２において、図示したフィールドのほかにも、名義人の住所、電話番号、生年月日等のフィールドを設けてもよい。

【０１６６】

図１１Ｂは、実施の形態２にかかる取引情報データベース（ＤＢ）１０１３の記憶内容

10

20

30

40

50

の一例を示す説明図である。図 1 1 B において、取引情報 DB 1 0 1 3 は、カード番号、氏名、取引日時、前年度の請求金額、認証情報の生成方式、および翌月の認証情報のフィールドを有する。各フィールドに情報を設定することで、取引情報（たとえば、取引情報 1 1 1 0 - 1 ~ 1 1 1 0 - 4）のレコードが記憶される。

【0 1 6 7】

カード番号は、カード 1 0 2 2 に記載される、たとえば 1 6 桁の数字であり、カード情報 DB 1 0 1 2（図 1 1 A を参照）に記憶されるカード番号と同一である。このため、カード情報 DB 1 0 1 2 のカード情報 1 1 0 0 と取引情報 1 1 1 0 とは、カード番号によって対応付けられている。

【0 1 6 8】

また、取引情報 DB 1 0 1 3 において、氏名は、カード情報 DB 1 0 1 2 のカード情報 1 1 0 0 に含まれる名義人と同一である。取引日時は、カード 1 0 2 2 を用いてカード決済をおこなった日付を示す。前年度の請求金額は、前年度にカード決済をおこなった金額を示す。

【0 1 6 9】

認証情報の生成方式は、前年度の請求金額を用いて 4 桁の認証情報（暗証番号）を生成する際の方式を示す。認証情報の生成方式は、たとえば、前年度の請求金額の「下 4 桁」や「上 4 桁」などを設定することが可能である。翌月の認証情報は、翌月の取引において用いられる認証情報（暗証番号）を示す。

【0 1 7 0】

翌月の認証情報は、前年度の請求金額と、認証情報の生成方式とに基づいて生成される。翌月の認証情報の生成について、取引情報 1 1 1 0 - 1 を例に挙げて説明すると、翌月の認証情報は、前年度の請求金額が「¥ 1 1 3 , 4 3 1」であり、認証情報の生成方式が「下 4 桁」であるため、前年度の請求金額「¥ 1 1 3 , 4 3 1」の「下 4 桁」である「3 4 3 1」となる。すなわち、翌月の取引において用いられる認証情報は、「3 4 3 1」となる。

【0 1 7 1】

ここで、たとえば、取引情報 1 1 1 0 - 1 は、カード番号「1 2 3 4 …」、氏名「総研総太郎」、取引日時「2 0 1 7 年 9 月」、前年度の請求金額「¥ 1 1 3 , 4 3 1」、認証情報の生成方式「下 4 桁」、認証情報「3 4 3 1」を示す。また、取引情報 1 1 1 0 - 1 以外の取引情報 1 1 1 0 - 2 ~ 1 1 1 0 - 4 についても、同様に、取引情報 DB 1 0 1 3 に記憶される。

【0 1 7 2】

（実施の形態 2 にかかる認証情報の生成例）

つぎに、図 1 2 を用いて、実施の形態 2 にかかる認証情報の生成例について説明する。図 1 2 は、実施の形態 2 にかかる認証情報の生成例を示す図である。以下に示す括弧書きの番号は、図 1 2 に示す括弧書きの番号と対応する。

【0 1 7 3】

図 1 2 に示すように、（1）2 0 1 7 年 1 0 月のカード決済による請求金額が ¥ 8 4 , 5 0 2 であったとする。このため、利用明細書 1 0 2 3 には、¥ 8 4 , 5 0 2 が印字されている。請求金額が ¥ 8 4 , 5 0 2 であることから、たとえば、下 4 桁の認証情報である「4 5 0 2」が翌月の認証情報（暗証番号）となる。

【0 1 7 4】

また、（2）2 0 1 7 年 1 1 月のカード決済による請求金額が ¥ 9 0 , 6 8 3 であったとする。このため、利用明細書 1 0 2 3 には、¥ 9 0 , 6 8 3 が印字されている。請求金額が ¥ 9 0 , 6 8 3 であることから、たとえば、下 4 桁の認証情報である「0 6 8 3」が翌月の認証情報（暗証番号）となる。

【0 1 7 5】

図 1 2 に説明したように、実施の形態 2 では、利用明細書 1 0 2 3 に印字された請求金額と、所定の認証情報の生成方式とに基づいて、翌月の取引に用いられる認証情報が生成

10

20

30

40

50

される。このため、認証情報を随時更新することができるとともに、利用者が認証情報を覚えていなくても、利用明細書 1023 を見るだけで、認証情報を容易に把握することができる。したがって、取引の利便性が低下することを抑えつつ、カード 1022 を用いた取引のセキュリティを簡単に高めることができる。

【0176】

(認証情報生成システム 1000 の機能的構成)

図 13 は、実施の形態 2 にかかる認証情報生成システム 1000 の機能的構成を示す説明図である。図 13 において、認証情報生成システム 1000 は、カード会社サーバ 1011 と、利用者端末 121 と、店舗端末 1031 とを備える。

【0177】

カード会社サーバ 1011 は、取引情報通信部 1301 と、取引制御部 1302 と、認証情報記憶部 1303 と、カード情報記憶部 1304 と、取引履歴記憶部 1305 と、取引履歴取得部 1306 と、認証情報生成部 1307 と、生成方式記憶部 1308 と、出力制御部 1309 と、端末通信部 1310 と、記憶制御部 1311 とを備える。

【0178】

店舗端末 1031 は、取引情報入力部 1321 と、取引情報通信部 1322 とを備える。ここで、利用者が、店舗において、カード 1022 を用いてカード決済をおこなう場合について説明する。店舗端末 1031 の取引情報入力部 1321 は、取引情報を入力する。取引情報は、挿入されたカード 1022 から読み取ったカード情報や、店員から入力される支払額の情報および支払方法に関する情報や、利用者から入力される認証情報（暗証番号）などである。

【0179】

ここで、詳細については、後述するが、認証情報は、たとえば、利用明細書 1023 に記載された、前月度の請求金額に基づいて生成される。このため、利用者は、利用明細書 1023 に記載された、前月度の請求金額を閲覧して、所定の生成方式で生成される認証情報を確認してから、今回の取引における認証情報を入力する。

【0180】

ここで、図示を省略するが、店舗端末 1031 のハードウェア構成は、図 2B に示した ATM 131 のハードウェア構成と同様である。ただし、店舗端末 1031 の場合、上述した入力デバイス 224 は、バーコードリーダを含む。バーコードリーダは、商品名や商品番号や価格などの商品に関する情報がコード化されたバーコードを読み取る。上述した取引情報入力部 1321 は、店舗端末 1031 の入力デバイスによって実現される。

【0181】

取引情報通信部 1322 は、取引情報入力部 1321 に入力された取引情報をカード会社サーバ 1011 へ送信する。取引情報通信部 1322 は、店舗端末 1031 の通信 IF によって実現される。

【0182】

取引情報通信部 1322 から取引情報がカード会社サーバ 1011 へ送信されると、カード会社サーバ 1011 の取引情報通信部 1301 は、取引情報を受信する。取引情報通信部 1301 は、店舗端末 1031 から受信した取引情報を取引制御部 1302 へ出力する。

【0183】

ここで、図示を省略するが、カード会社サーバ 1011 のハードウェア構成は、図 2A に示した銀行サーバ 111 のハードウェア構成と同様である。取引情報通信部 1301 は、カード会社サーバ 1011 の通信 IF によって実現される。

【0184】

取引制御部 1302 は、取引情報通信部 1301 から取引情報が入力されると、当該取引情報に含まれる、利用者から受け付けた認証情報が、各利用者の認証情報を記憶する認証情報記憶部 1303 に記憶されているか否かの一致判定（認証）をおこなう。当該一致判定において、否定の判定結果が得られた場合（認証に失敗した場合）、取引制御部 13

10

20

30

40

50

02は、認証に失敗した旨を示す取引結果を取引情報通信部1301へ出力する。

【0185】

一方、一致判定において、肯定の判定結果が得られた場合（認証に成功した場合）、取引制御部1302は、与信照会をおこなう。与信照会は、カード情報記憶部1304に記憶されるカード情報を参照して、クレジットカードの月々の利用可能な金額を示す与信枠のうち、支払額分の空きがあるか否かの照会である。

【0186】

与信照会において、与信枠に支払額分の空きがない場合、取引制御部1302は、その旨を示す取引結果を取引情報通信部1301へ出力する。一方、与信照会において、与信枠に支払額分の空きがある場合、取引制御部1302は、支払額分を確保して、支払方法に関する情報が示す支払方法により、カード決済を完了させる。そして、取引制御部1302は、カード決済を完了させた旨を示す取引結果を取引情報通信部1301へ出力する。

【0187】

取引制御部1302は、カード会社サーバ1011のメモリに記憶されたプログラムをCPUに実行させることにより、その機能を実現する。認証情報記憶部1303およびカード情報記憶部1304は、カード会社サーバ1011のメモリによって実現される。具体的には、認証情報記憶部1303は、取引情報DB1013（図11Bを参照）によって実現される。また、カード情報記憶部1304は、カード情報DB1012（図11Aを参照）によって実現される。ただし、認証情報記憶部1303およびカード情報記憶部1304は、カード会社サーバ1000に設けられずに、外部の他の装置に設けられていてもよい。

【0188】

取引情報通信部1301は、取引制御部1302から取引結果が入力されると、入力された取引結果を店舗端末1031へ送信する。取引情報通信部1301から取引結果が店舗端末1031へ送信されると、店舗端末1031の取引情報通信部1322は、取引結果を受信する。取引情報通信部1322によって取引結果を受信されると、店舗端末1031は、当該取引結果をディスプレイに表示したり、印字出力をおこなったりする。

【0189】

また、取引制御部1302は、カード情報記憶部1304を参照して、毎月のクレジットカードの利用金額（請求金額）を取引履歴記憶部1305に記憶させる。取引履歴記憶部1305は、カード会社サーバ1011のメモリによって実現される。具体的には、取引履歴記憶部1305は、取引情報DB1013（図11Bを参照）によって実現される。

【0190】

取引履歴取得部1306は、取引履歴記憶部1305から、取引履歴を取得する。取引履歴は、利用者が閲覧可能な取引に関する履歴である。利用者が閲覧可能とは、利用明細書1023に記載されることによって閲覧可能であることや、利用者端末121に表示されることによって閲覧可能であることである。取引履歴は、利用明細書1023に印字された情報を含む。具体的には、取引履歴は、たとえば、日付、前月度の請求金額、購入先、といった情報を含む。

【0191】

認証情報生成部1307は、取引履歴取得部1306によって取得された取引履歴に基づいて、翌月の取引において用いられる認証情報を生成する。取引履歴取得部1306によって取得された取引履歴は、たとえば、利用明細書1023に印字された情報（以下「記載情報」という）である。特に、記載情報は、前月度の利用明細書1023に印字された記載情報である。

【0192】

この場合、取引履歴取得部1306は、前月度の記載情報を取得する。たとえば、取引履歴取得部1306は、利用者が前月度の利用明細書1023を受領した以降の、予め設定した所定の期日（認証情報を変更する期日）に取引履歴を取得してもよい。認証情報生成部1307は、取引履歴取得部1306によって取得された前月度の記載情報に基づい

10

20

30

40

50

て、認証情報を生成する。

【0193】

認証情報生成部1307は、生成方式記憶部1308に記憶される、予め設定された生成方式により認証情報を生成する。具体的には、認証情報生成部1307は、利用明細書1023に印字された記載情報が示す請求金額の中から、予め設定された複数の桁に該当する数字をそれぞれ選択して認証情報を生成する。

【0194】

具体的には、認証情報生成部1307は、請求金額のうち、予め設定された複数の桁（認証情報の桁）に該当する数字をそれぞれ選択して認証情報を生成する。たとえば、認証情報が4桁の数字であれば、認証情報生成部1307は、下4桁や上4桁といった数字を選択して認証情報を生成する。

10

【0195】

記憶制御部1311は、認証情報生成部1307によって生成された認証情報を認証情報記憶部1303に記憶させる。また、ある月において利用者がカード決済を一度もおこなわず、請求金額がない場合、認証情報生成部1307は、認証情報を生成しなくてもよい。この場合、認証情報記憶部1303に記憶される認証情報が変更されないため、翌月も前月の認証情報を引き継ぐこととしてもよい。

【0196】

また、認証情報生成部1307によって生成された認証情報に切り替える時期は、利用者が取引履歴を閲覧可能となった後であり、たとえば、利用明細書1023を受領した後とすればよい。具体的には、たとえば、認証情報を切り替える時期は、利用者が利用明細書1023を受領することが想定される日以降の、任意の日を設定しておけばよい。また、カード会社サーバ1011は、認証情報を切り替える時期を、利用者に通知してもよく、たとえば、利用明細書1023へ記載したり、利用者端末121へ送信したりしてもよい。

20

【0197】

認証情報生成部1307および記憶制御部1311は、カード会社サーバ1011のメモリに記憶されたプログラムをCPUに実行させることにより、その機能を実現する。生成方式記憶部1308は、カード会社サーバ1011のメモリによって実現される。具体的には、生成方式記憶部1308は、取引情報DB1013（図11Bを参照）によって実現される。ただし、生成方式記憶部1308は、カード会社サーバ1000に設けられずに、外部の他の装置に設けられていてもよい。

30

【0198】

このように、認証情報は、認証情報生成部1307が、予め生成しておいて、記憶制御部1311が、認証情報生成部1307によって生成された認証情報を認証情報記憶部1303に記憶させておく。そして、認証要求を受信した際には、認証情報記憶部1303に記憶されている認証情報を抽出して、抽出された認証情報に基づいて認証をおこなうようにする。このようにすることによって、認証要求があるごとに、認証情報を生成しておく必要がない。

【0199】

あるいは、認証情報生成部1307は、認証情報を予め生成しない。したがって、記憶制御部1311は、認証情報を認証情報記憶部1303に記憶させない。そして、認証要求を受信した際に、はじめて、認証情報の生成方式に基づいて認証情報を生成して、生成した認証情報に基づいて認証をおこなうようにしてもよい。

40

【0200】

このように、認証情報は、予め生成して記憶手段に記憶させておいても良いが、認証要求を受信したときに定められた認証情報の生成方式に基づいて認証情報を生成する（予め記憶しない）ようにしてもよい。したがって、そのように構成する場合には、認証情報記憶部1303は設けなくてもよい。

【0201】

50

つぎに、利用者によっては、カード１０２２を利用する際に、利用明細書１０２３を所持しないことが想定される。このようなことに鑑み、利用明細書１０２３に記載される取引履歴を利用者端末１２１に記憶可能にすることについて説明する。

【０２０２】

たとえば、出力制御部１３０９は、カード会社１０１０から利用者に毎月の利用明細書１０２３を送信する時期などの所定の期日に、予め登録された利用者端末１２１へ電子メールやSNS（Social Networking Service）等で、利用明細書１０２３に記載される内容の取引履歴を送信してもよい。具体的には、出力制御部１３０９は、所定の期日に、端末通信部１３１０を制御して、予め登録された利用者端末１２１へ、１ヶ月分の取引履歴を送信させる制御をおこなえばよい。

10

【０２０３】

この場合、利用者端末１２１は、カード会社サーバ１０１１から受信した取引履歴をメモリに記憶すればよい。また、利用者端末１２１は、メモリに記憶した取引履歴を表示すればよい。

【０２０４】

これにより、利用者は、利用明細書１０２３に記載される取引履歴を利用者端末１２１に記憶させることができる。このため、利用者は、取引をおこなう際に、利用明細書１０２３を所持していなくても、利用者端末１２１に記憶された取引履歴を閲覧して、認証情報を容易に把握することができる。

【０２０５】

20

端末通信部１３１０は、カード会社サーバ１０１１の通信ＩＦによって実現される。出力制御部１３０９は、カード会社サーバ１０１１のメモリに記憶されたプログラムをＣＰＵに実行させることにより、その機能を実現する。

【０２０６】

（カード会社サーバ１０１１がおこなう認証情報生成処理手順の一例）

つぎに、図１４を用いて、カード会社サーバ１０１１がおこなう認証情報生成処理手順の一例について説明する。図１４は、カード会社サーバ１０１１がおこなう認証情報生成処理手順の一例を示すフローチャートである。

【０２０７】

図１４において、カード会社サーバ１０１１は、認証情報を変更可能なタイミングであるか否かを判断する（ステップＳ１４０１）。認証情報を変更可能なタイミングは、利用者が利用明細書１０２３を閲覧可能となった後のタイミングであり、たとえば、予め定めた所定の期日である。カード会社サーバ１０１１は、認証情報を変更可能なタイミングとなるまで待つ（ステップＳ１４０１：Ｎｏ）。

30

【０２０８】

カード会社サーバ１０１１は、認証情報を変更可能なタイミングになった場合（ステップＳ１４０１：Ｙｅｓ）、取引情報ＤＢ１０１３（図１１Ｂを参照）に記憶される、認証情報の生成方式を参照する（ステップＳ１４０２）。そして、カード会社サーバ１０１１は、認証情報を生成する設定となっているか否かを判断する（ステップＳ１４０３）。

【０２０９】

40

カード会社サーバ１０１１は、認証情報を生成する設定となっていない場合（ステップＳ１４０３：Ｎｏ）、具体的には、取引情報ＤＢ１０１３の「認証情報の生成方式」のフィールドに情報が記憶されていない場合、そのまま一連の処理を終了する。

【０２１０】

一方、カード会社サーバ１０１１は、認証情報を生成する設定となっている場合（ステップＳ１４０３：Ｙｅｓ）、具体的には、取引情報ＤＢ１０１３の「認証情報の生成方式」のフィールドに「下４桁」や「上４桁」等が記憶されている場合、請求金額と、参照した生成方式とに基づいて、翌月の取引に用いられる認証情報を生成する（ステップＳ１４０４）。

【０２１１】

50

つぎに、カード会社サーバ１０１１は、取引情報ＤＢ１０１３に、生成した認証情報を記憶し（ステップＳ１４０５）、一連の処理を終了する。取引情報ＤＢ１０１３に記憶された認証情報は、たとえば、翌月の取引において用いられる。

【０２１２】

上述した処理によれば、毎月、カード決済の請求をおこなう際に、請求金額に応じた認証情報に、認証情報を更新することができる。これにより、カード１０２２を用いた取引のセキュリティを向上させることができる。

【０２１３】

以上説明したように、実施の形態２にかかるカード会社サーバ１０１１によれば、実施の形態１と同様の効果を奏する。特に、実施の形態２にかかるカード会社サーバ１０１１は、利用明細書１０２３に印字された情報に基づいて、クレジットカード（カード１０２２）を用いた翌月の取引において用いられる認証情報を生成することとした。

【０２１４】

これにより、利用者は、認証情報を覚えていなくても、利用明細書１０２３を見るだけで、認証情報を容易に把握することができる。たとえば高齢者など、利用者端末１２１を所有していない利用者や、利用者端末１２１に取引履歴を表示させることが煩雑であると感じる利用者でも、利用明細書１０２３を見るだけで、認証情報を容易に把握することができる。

【０２１５】

また、実施の形態２にかかるカード会社サーバ１０１１は、利用明細書１０２３に記載される内容の取引履歴を利用者端末１２１に送信することとした。これにより、利用者は、預金通帳１２３を所持していなくても、利用者端末１２１に表示される取引履歴を閲覧することができる。これにより、利用者は、認証情報を覚えていなくても、認証情報を容易に把握することができる。

【０２１６】

また、実施の形態２にかかるカード会社サーバ１０１１によれば、利用者がカード会社１０１０と書類や情報のやり取りをせずに、認証情報を随時更新することができるため、利用者やカード会社１０１０のスタッフの手間を抑え、迅速且つ簡単に、認証情報を変更することができる。

【０２１７】

したがって、実施の形態２にかかるカード会社サーバ１０１１は、クレジットカードの取引にかかる利便性が低下することを抑えつつ、クレジットカードを用いた取引のセキュリティを簡単に向上させることができる。特に、実施の形態２にかかるカード会社サーバ１０１１によれば、利用者が認証情報を覚える必要がないため、認証情報を失念しやすい高齢者などの利用者に効果的である。

【０２１８】

また、実施の形態１，２では、この発明の認証情報生成装置を、銀行サーバ１１１やカード会社サーバ１０１１によって実現した場合について説明したが、これに限らない。たとえば、銀行サーバ１１１やカード会社サーバ１０１１以外の他の会社のサーバによっても、この発明の認証情報生成装置を実現することが可能である。また、各種カード１２２，１０２２のＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ Ｐｒｏｇｒａｍｍｉｎｇ Ｉｎｔｅｒｆａｃｅ）を用いて、異業種間でも各種情報を共有することが可能となる場合には、たとえば、保険会社のサーバによっても、この発明の認証情報生成装置を実現することが可能である。

【０２１９】

なお、実施の形態１，２で説明した認証情報生成方法は、予め用意されたプログラムをパーソナルコンピュータやワークステーション等のコンピュータで実行することにより実現することができる。

【０２２０】

また、実施の形態１，２で説明した認証情報生成プログラムは、ハードディスク、フレ

10

20

30

40

50

キシブルディスク、CD (Compact Disc) -ROM、MO (Magnetooptical disk)、DVD (Digital Versatile Disk)、USB (Universal Serial Bus) メモリ等のコンピュータで読み取り可能な記憶媒体に記憶され、コンピュータによって記憶媒体から読み出されることによって実行される。また、認証情報生成プログラムは、インターネット等のネットワークを介して配布されてもよい。

【産業上の利用可能性】

【0221】

以上のように、この発明にかかる認証情報生成装置、認証情報生成方法、および認証情報生成プログラムは、各種カードに用いられる認証情報を生成する、認証情報生成装置、
認証情報生成方法、および認証情報生成プログラムに有用であり、特に、取引の利便性が
低下することを抑えつつ、簡単にセキュリティを向上させる、認証情報生成装置、認証情
報生成方法、および認証情報生成プログラムに適している。

10

【符号の説明】

【0222】

100, 1000 認証情報生成システム

110 銀行

111 銀行サーバ

112 口座情報DB

113, 1013 取引情報DB

20

121 利用者端末

122, 1022 カード

123 預金通帳

131 ATM

140 ネットワーク

210, 220 バス

211, 221 CPU

212, 222 メモリ

213, 225 通信IF

223 出力デバイス

30

224 入力デバイス

400, 1023 利用明細書

501 取引情報受信部

502, 1302 取引制御部

503 取引結果送信部

504 取引履歴受信部

505, 1305 取引履歴記憶部

506, 1306 取引履歴取得部

507, 1307 認証情報生成部

508, 1308 生成方式記憶部

40

509, 1303 認証情報記憶部

510 口座情報記憶部

511, 1309 出力制御部

512, 1310 端末通信部

513, 1311 記憶制御部

521, 1321 取引情報入力部

522 取引情報送信部

523 取引結果受信部

524 取引処理部

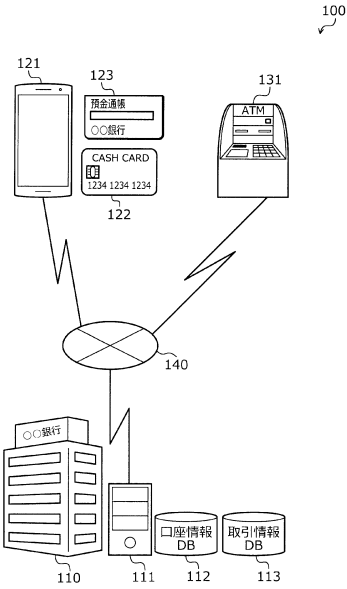
525 処理結果出力部

50

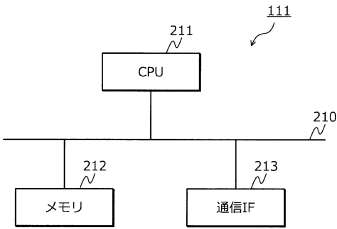
- 1 0 1 0 カード会社
- 1 0 1 1 カード会社サーバ
- 1 0 1 2 カード情報 D B
- 1 0 3 1 店舗端末
- 1 3 0 1 取引情報通信部
- 1 3 0 4 カード情報記憶部
- 1 3 2 2 取引情報通信部

【図面】

【図 1】



【図 2 A】



10

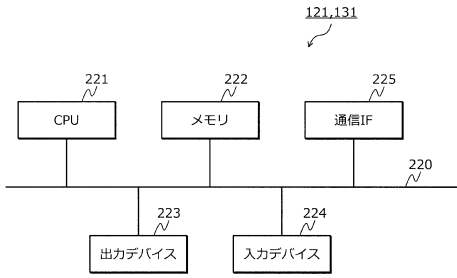
20

30

40

50

【図 2 B】



【図 3 A】

口座ID	氏名	住所	端末情報	金融機関コード	支店番号	口座番号	残高
K001	総研総太郎	東京都...	aaa-@xxx	0000	345	123...	¥96,390
K002	総山花子	神奈川県...	bbb-@xxx	0000	789	456...	¥37,520
...	...	...	...	...	...	...	...

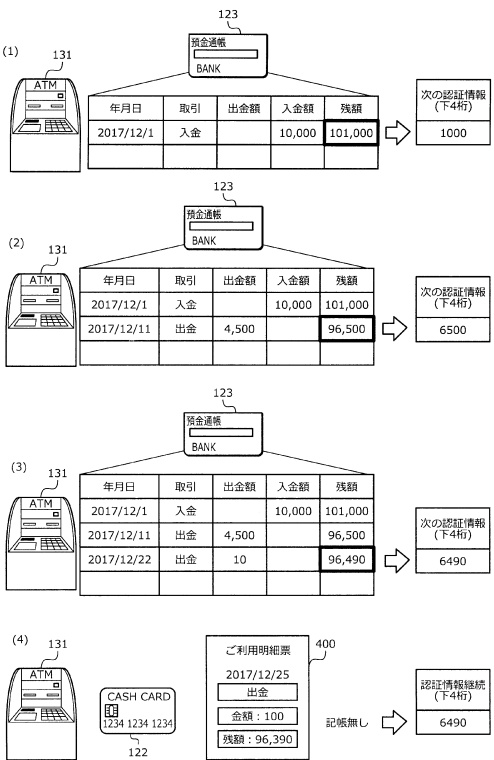
10

20

【図 3 B】

口座ID	氏名	取引日付	取引内容	取引金額	残高	記帳の有無	認証情報の生成方式	認証情報
T001	総研総太郎	2017/12/1	入金	¥10,000	¥101,000	有り	下4桁	1000
T002	総研総太郎	2017/12/11	出金	¥4,500	¥96,500	有り	下4桁	6500
T003	総研総太郎	2017/12/22	出金	¥10	¥96,490	有り	下4桁	6490
T004	総研総太郎	2017/12/23	出金	¥100	¥96,390	無し	下4桁	6490
T005	総山花子	2017/12/25	入金	¥10,000	¥37,520	有り	上4桁	3752
T006	総田総太	2017/12/25	入金	¥10,000	¥345,928	有り	-	0417(固定)
...	...	...	...	...	...	...	...	...

【図 4】

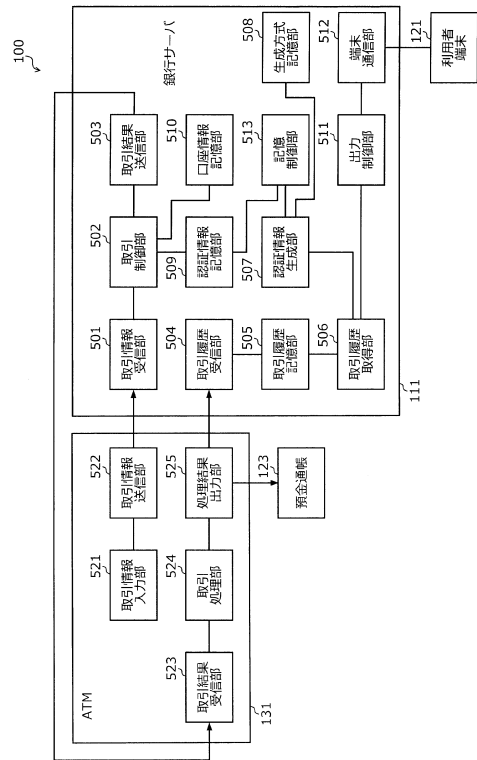


30

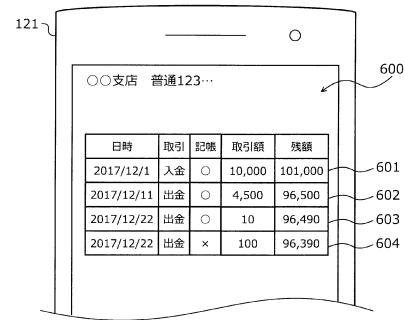
40

50

【図 5】



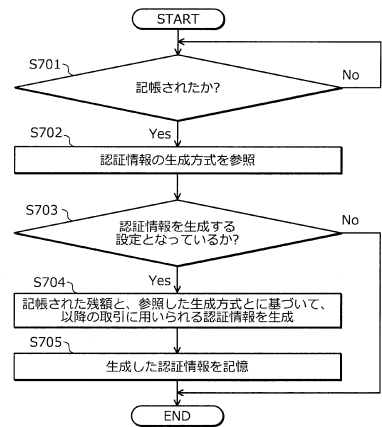
【図 6 A】



【図 6 B】



【図 7】



10

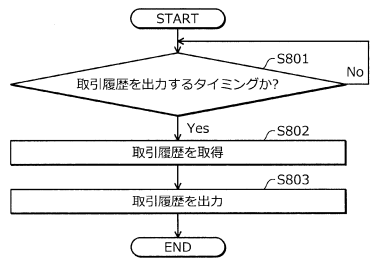
20

30

40

50

【図 8】



【図 9 A】

123					
現金通帳					
BANK					
年月日	取引	出金額	入金額	残高	
2017/12/24	入金		10,000	90,631	
2017/12/25	振込	4,552		86,079	
2017/12/27	振込	3,268		82,811	
2017/12/28	出金	5,000		77,811	
2017/12/29	振込	2,431		75,380	

900

901

902

903

904

905

認証情報
(下1桁を4段)

0119

10

【図 9 B】

123					
現金通帳					
BANK					
年月日	取引	出金額	入金額	残高	
2017/12/24	入金		10,000	90,631	
2017/12/25	振込	4,552		86,079	
2017/12/27	振込	3,268		82,811	
2017/12/28	出金	5,000		77,811	
2017/12/29	振込	2,431		75,380	

900

901

902

903

904

905

認証情報
(月日)

1229

【図 10】

1000

121

1023

ご利用明細

CREDIT CARD

1234 1234 1234

1022

1031

140

カード会社

1010

1011

カード情報DB

1012

取引情報DB

1013

20

30

40

50

【図 1 1 A】

カード情報DB 1012

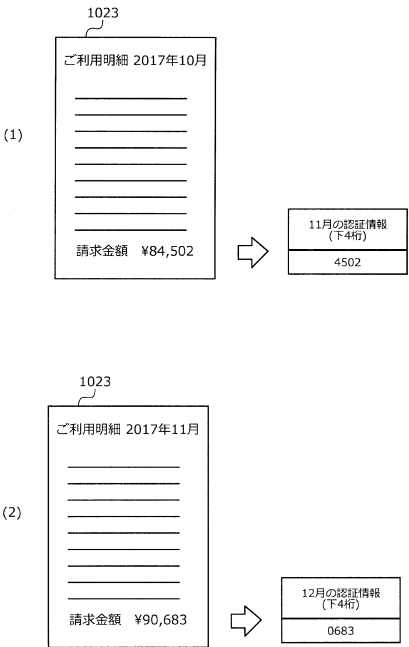
カード番号	名義人	利用者端末情報	有効期限	セキュリティコード	残高額	現在までの利用額
1100-1 1234...	総研総太郎	XXx-@xx	〇〇年〇〇月	〇〇〇	¥〇〇万	¥〇〇〇〇
1100-2 2345...	総研二郎	YYy-@xx	〇x年x月	〇x〇	¥x〇万	¥〇x〇〇
...	...	...	...	...	...	...

【図 1 1 B】

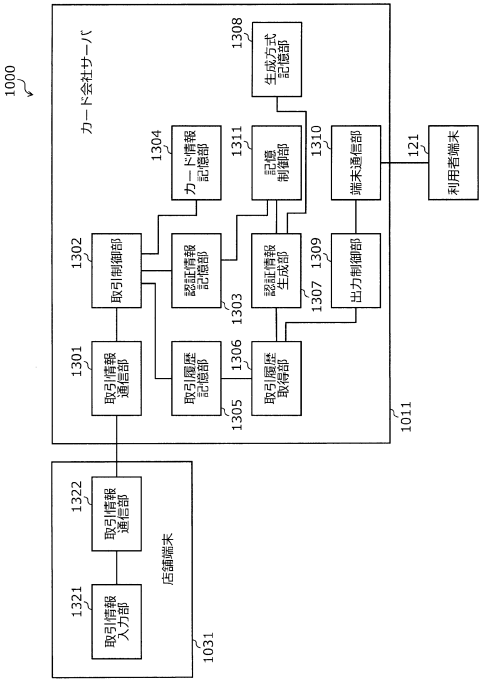
取引情報DB 1013

カード番号	氏名	取引日時	前月後の請求金額	認証情報の生成方式	翌月の認証情報
1110-1 1234...	総研総太郎	2017年9月	¥113,431	下4桁	3431
1110-2 1234...	総研総太郎	2017年10月	¥84,502	下4桁	4502
1110-3 1234...	総研総太郎	2017年11月	¥90,683	下4桁	0683
1110-4 3456...	総研二郎	2017年11月	¥30,544	-	1201(固定)
...	...	...	...	...	...

【図 1 2】



【図 1 3】



10

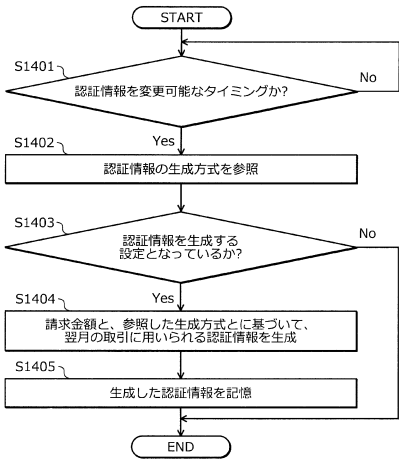
20

30

40

50

【図 14】



10

20

30

40

50

フロントページの続き

- (56)参考文献 特開２００１－３３７９２９（ＪＰ，Ａ）
 特開２００９－１６９５２０（ＪＰ，Ａ）
 特開２００２－２７９４９１（ＪＰ，Ａ）
 特開２００７－２９９１０９（ＪＰ，Ａ）
 特開２００４－１８５３７１（ＪＰ，Ａ）
- (58)調査した分野 (Int.Cl., DB名)
 G 0 6 Q 1 0 / 0 0 - 9 9 / 0 0