(19)日本国特許庁(JP)　(12)特許公報(B1)　(11)特許番号
特許第7390519号
(P7390519)
(45)発行日　令和5年12月1日(2023.12.1)　(24)登録日　令和5年11月22日(2023.11.22)

(51)国際特許分類　ＦＩ
*Ｇ０６Ｑ　20/40　(2012.01)*　Ｇ０６Ｑ　20/40
*Ｇ０６Ｆ　21/31　(2013.01)*　Ｇ０６Ｆ　21/31

請求項の数　13　（全20頁）

(21)出願番号　特願2023-142221(P2023-142221)
(22)出願日　令和5年9月1日(2023.9.1)
審査請求日　令和5年9月1日(2023.9.1)
早期審査対象出願

(73)特許権者　519110124
ＰａｙＰａｙ株式会社
東京都千代田区紀尾井町１番３号
(74)代理人　100149548
弁理士　松沼 泰史
(74)代理人　100154852
弁理士　酒井 太一
(74)代理人　100181124
弁理士　沖田 壮男
(74)代理人　100194087
弁理士　渡辺 伸一
(72)発明者　大西 朋史
東京都千代田区紀尾井町１番３号 ＰａｙＰａｙ株式会社内
審査官　平井 嗣人

最終頁に続く

(54)【発明の名称】　サービス提供装置、サービス提供方法、およびプログラム

(57)【特許請求の範囲】

【請求項１】

電子決済サービスを提供するサービス提供装置であって、

少なくとも電話番号を必須の登録事項として利用者のアカウント設定を行い、前記利用者の電話番号を含む登録情報を管理する情報管理部と、

前記利用者から、前記登録情報に登録された第１電話番号であって第１端末装置に対応付けられた第１電話番号とは異なる第２電話番号が対応付けられた第２端末装置を通じて電話番号の変更が申し込まれたとき、複数の質問を含むコンテンツを前記第２端末装置に提供し、前記第２端末装置により利用者に提示された複数の質問に対して前記利用者が前記第２端末装置に入力した、複数の回答を含む複数の確認情報を前記第２端末装置から取得し、前記複数の確認情報に基づくスコアを計算する番号変更時認証部と、

を備え、

前記情報管理部は、前記スコアが第１閾値以上である場合、および前記スコアが前記第１閾値よりも小さい第２閾値以上である場合に、前記申し込みに係る新しい電話番号で前記登録情報を更新し、前記スコアが前記第１閾値未満かつ前記第２閾値以上である場合には、前記登録情報に含まれる情報の一部を削除または隠蔽する、

サービス提供装置。

【請求項２】

電子決済サービスを提供するサービス提供装置であって、

少なくとも電話番号を必須の登録事項として利用者のアカウント設定を行い、前記利用

者の電話番号を含む登録情報を管理する情報管理部と、
前記利用者から、前記登録情報に登録された第１電話番号であって第１端末装置に対応付けられた第１電話番号とは異なる第２電話番号が対応付けられた第２端末装置を通じて電話番号の変更が申し込まれたとき、前記第２端末装置にインストールされているアプリケーションプログラムが予め保持している複数の質問に基づいて前記第２端末装置により前記利用者に提示された、複数の質問に対して前記利用者が前記第２端末装置に入力した、複数の回答を含む複数の確認情報を前記第２端末装置から取得し、前記複数の確認情報に基づくスコアを計算する番号変更時認証部と、
を備え、
前記情報管理部は、前記スコアが第１閾値以上である場合、および前記スコアが前記第１閾値よりも小さい第２閾値以上である場合に、前記申し込みに係る新しい電話番号で前記登録情報を更新し、前記スコアが前記第１閾値未満かつ前記第２閾値以上である場合には、前記登録情報に含まれる情報の一部を削除または隠蔽する、
サービス提供装置。
【請求項３】
前記情報管理部は、前記スコアが前記第１閾値以上である場合には、前記登録情報に含まれる情報の一部を削除または隠蔽しない、
請求項１または２記載のサービス提供装置。
【請求項４】
前記情報管理部は、前記スコアが前記第１閾値以上である場合には、前記登録情報に含まれる情報の一部であって、前記スコアが前記第１閾値未満かつ前記第２閾値以上である場合に比して少ない情報を削除または隠蔽する、
請求項１または２記載のサービス提供装置。
【請求項５】
前記情報管理部は、前記登録情報に含まれる情報の一部を削除または隠蔽する場合、前記電子決済サービスを運営する事業者とは異なる事業者の金融サービスに関する情報を削除または隠蔽する、
請求項１または２記載のサービス提供装置。
【請求項６】
前記情報管理部は、前記登録情報に含まれる情報の一部を削除または隠蔽する場合、前記複数の質問に対する利用者の正解状況に応じて削除または隠蔽する情報を決定する、
請求項１または２記載のサービス提供装置。
【請求項７】
前記複数の質問のそれぞれは、前記登録情報に登録された情報の内容に関する質問であり、
前記番号変更時認証部は、前記登録情報に登録されていない情報に関する質問を除外した一以上の質問を含むコンテンツを前記第２端末装置に提供する、
請求項１記載のサービス提供装置。
【請求項８】
前記複数の質問のそれぞれは、前記登録情報に登録された情報の内容に関する質問であり、
前記番号変更時認証部は、前記登録情報に登録されていない情報に関する質問を除外した一以上の質問を前記利用者に提示するように前記アプリケーションプログラムに通知する、
請求項２記載のサービス提供装置。
【請求項９】
前記番号変更時認証部は、前記複数の確認情報のそれぞれに対して予め設定された点数を用いて前記スコアを計算する、
請求項１または２記載のサービス提供装置。
【請求項１０】

電子決済サービスを提供するサービス提供装置が、
少なくとも電話番号を必須の登録事項として利用者のアカウント設定を行い、前記利用者の電話番号を含む登録情報を管理する処理と、
前記利用者から、前記登録情報に登録された第１電話番号であって第１端末装置に対応付けられた第１電話番号とは異なる第２電話番号が対応付けられた第２端末装置を通じて電話番号の変更が申し込まれたとき、複数の質問を含むコンテンツを前記第２端末装置に提供し、前記第２端末装置により利用者に提示された複数の質問に対して前記利用者が前記第２端末装置に入力した、複数の回答を含む複数の確認情報を前記第２端末装置から取得し、前記複数の確認情報に基づくスコアを計算する処理と、
前記スコアが第１閾値以上である場合、および前記スコアが前記第１閾値よりも小さい第２閾値以上である場合に、前記申し込みに係る新しい電話番号で前記登録情報を更新し、前記スコアが前記第１閾値未満かつ前記第２閾値以上である場合には、前記登録情報に含まれる情報の一部を削除または隠蔽する処理と、
を実行するサービス提供方法。
【請求項１１】
電子決済サービスを提供するサービス提供装置が、
少なくとも電話番号を必須の登録事項として利用者のアカウント設定を行い、前記利用者の電話番号を含む登録情報を管理する処理と、
前記利用者から、前記登録情報に登録された第１電話番号であって第１端末装置に対応付けられた第１電話番号とは異なる第２電話番号が対応付けられた第２端末装置を通じて電話番号の変更が申し込まれたとき、前記第２端末装置にインストールされているアプリケーションプログラムが予め保持している複数の質問に基づいて前記第２端末装置により前記利用者に提示された、複数の質問に対して前記利用者が前記第２端末装置に入力した、複数の回答を含む複数の確認情報を前記第２端末装置から取得し、前記複数の確認情報に基づくスコアを計算する処理と、
前記スコアが第１閾値以上である場合、および前記スコアが前記第１閾値よりも小さい第２閾値以上である場合に、前記申し込みに係る新しい電話番号で前記登録情報を更新し、前記スコアが前記第１閾値未満かつ前記第２閾値以上である場合には、前記登録情報に含まれる情報の一部を削除または隠蔽する処理と、
を実行するサービス提供方法。
【請求項１２】
電子決済サービスを提供するサービス提供装置に、
少なくとも電話番号を必須の登録事項として利用者のアカウント設定を行い、前記利用者の電話番号を含む登録情報を管理する処理と、
前記利用者から、前記登録情報に登録された第１電話番号であって第１端末装置に対応付けられた第１電話番号とは異なる第２電話番号が対応付けられた第２端末装置を通じて電話番号の変更が申し込まれたとき、複数の質問を含むコンテンツを前記第２端末装置に提供し、前記第２端末装置により利用者に提示された複数の質問に対して前記利用者が前記第２端末装置に入力した、複数の回答を含む複数の確認情報を前記第２端末装置から取得し、前記複数の確認情報に基づくスコアを計算する処理と、
前記スコアが第１閾値以上である場合、および前記スコアが前記第１閾値よりも小さい第２閾値以上である場合に、前記申し込みに係る新しい電話番号で前記登録情報を更新し、前記スコアが前記第１閾値未満かつ前記第２閾値以上である場合には、前記登録情報に含まれる情報の一部を削除または隠蔽する処理と、
を実行させるためのプログラム。
【請求項１３】
電子決済サービスを提供するサービス提供装置に、
少なくとも電話番号を必須の登録事項として利用者のアカウント設定を行い、前記利用者の電話番号を含む登録情報を管理する処理と、
前記利用者から、前記登録情報に登録された第１電話番号であって第１端末装置に対応

付けられた第１電話番号とは異なる第２電話番号が対応付けられた第２端末装置を通じて電話番号の変更が申し込まれたとき、前記第２端末装置にインストールされているアプリケーションプログラムが予め保持している複数の質問に基づいて前記第２端末装置により前記利用者に提示された、複数の質問に対して前記利用者が前記第２端末装置に入力した、複数の回答を含む複数の確認情報を前記第２端末装置から取得し、前記複数の確認情報に基づくスコアを計算する処理と、

前記スコアが第１閾値以上である場合、および前記スコアが前記第１閾値よりも小さい第２閾値以上である場合に、前記申し込みに係る新しい電話番号で前記登録情報を更新し、前記スコアが前記第１閾値未満かつ前記第２閾値以上である場合には、前記登録情報に含まれる情報の一部を削除または隠蔽する処理と、

を実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、サービス提供装置、サービス提供方法、およびプログラムに関する。

【背景技術】

【０００２】

従来、少なくとも部分的にネットワークを介して提供されるサービスでは、利用者がアカウントにログインをすることでサービスを受けられるようになるのが通常である。ログインに際しては、電話番号やログインＩＤ、パスワード等を入力することが要求される（ブラウザやアプリが情報を記憶して自動入力する場合も含まれる）。特に電子決済サービスなどの金銭を扱うサービスにおいては認証処理の重要度が高く、ＳＭＳ認証などの比較的セキュリティ性が高い認証方法が採用されている。

【０００３】

ところで、利用者がスマートフォンやタブレット端末などの端末装置を買い替えた場合などにおいて、サービスに登録されている電話番号を変更する必要が生じる。従来の技術では、オンラインで電話番号を変更する場合、電話番号を変更する前の端末装置を用いてアカウントにログインした状態で電話番号の変更を申し込まなければならない場合があった。これに対し、特許文献１に記載の発明では、既存と異なる端末装置から電話番号の変更が申し込まれた場合に、複数の質問を利用者に送信し、回答状況に応じて電話番号の変更を承諾するようにしている。

【先行技術文献】

【特許文献】

【０００４】

【文献】特許第７１９５４７３号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

従来の技術では、利用者の特定に関してある程度の確証を得たものの、異なる利用者である可能性を十分に払拭できない場合においてどのように対応するのかについて言及されておらず、利便性と安全性の両立を実現することができない場合があった。

【０００６】

本発明は、このような事情を考慮してなされたものであり、利便性と安全性の両立を実現することができるサービス提供装置、サービス提供方法、およびプログラムを提供することを目的の一つとする。

【課題を解決するための手段】

【０００７】

本発明の一態様は、電子決済サービスを提供するサービス提供装置であって、少なくとも電話番号を必須の登録事項として利用者のアカウント設定を行い、前記利用者の電話番号を含む登録情報を管理する情報管理部と、前記利用者から、前記登録情報に登録された

第１電話番号であって第１端末装置に対応付けられた第１電話番号とは異なる第２電話番号が対応付けられた第２端末装置を通じて電話番号の変更が申し込まれたとき、複数の質問を含むコンテンツを前記第２端末装置に提供し、前記第２端末装置により利用者に提示された複数の質問に対して前記利用者が前記第２端末装置に入力した、複数の回答を含む複数の確認情報を前記第２端末装置から取得し、前記複数の確認情報に基づくスコアと第１閾値、および前記スコアと前記第１閾値よりも小さい第２閾値を、それぞれ比較する番号変更時認証部と、を備え、前記情報管理部は、前記スコアが前記第１閾値以上である場合、および前記スコアが前記第２閾値以上である場合に、前記申し込みに係る新しい電話番号で前記登録情報を更新し、前記スコアが前記第１閾値未満かつ前記第２閾値以上である場合には、前記登録情報に含まれる情報の一部を削除または隠蔽する、サービス提供装置である。

【発明の効果】

【０００８】

本発明の一態様によれば、利便性と安全性の両立を実現することができる。

【図面の簡単な説明】

【０００９】

【図１】電子決済サービスが実現されるための構成の一例を示す図である。

【図２】電子決済の大まかな流れを例示したシーケンス図（その１）である。

【図３】電子決済の大まかな流れを例示したシーケンス図（その２）である。

【図４】第１実施形態に係る決済サーバ１００の構成図である。

【図５】利用者情報１７２の内容の一例を示す図である。

【図６】加盟店／店舗情報１７６の内容の一例を示す図である。

【図７】利用者が第１端末装置を手元に保持しておらず、第２端末装置のみ手元に保持している場合の、電話番号変更の流れを示す図である。

【図８】第２端末装置の決済アプリ２０、番号変更時認証部１２８および情報管理部１３０により実行される処理の内容の一例を示すフローチャートである。

【図９】第２端末装置の決済アプリ２０、番号変更時認証部１２８および情報管理部１３０により実行される処理の内容の一例を示すフローチャートである。

【図１０】質問リスト１７８から質問が抽出される様子を示す図である。

【図１１】決済アプリ２０が第２端末装置に表示させる質問提示画面ＩＭ１の一例を示す図である。

【発明を実施するための形態】

【００１０】

以下、図面を参照し、本発明のサービス提供装置、サービス提供方法、およびプログラムの実施形態について説明する。以下に登場する「サーバ」、「管理装置」「情報提供装置」などの、利用者にサービスを提供したり内部解析を行ったりするための各種装置は、分散化された装置群によって実現されてよく、それぞれの装置を運用する事業者は異なってもよい。また装置のハードウェアの保有者（クラウドサーバの提供者）と実質的な運用を行う事業者も異なってよい。サービス提供装置は、電子決済サービスを提供する。電子決済サービスは、アプリケーションプログラムと決済サーバ（サービス提供装置の一例）が協働して提供される。以下の説明ではアプリケーションプログラムを決済アプリと称する。電子決済サービスは、店舗における商品やサービスの購買に係る決済をサポートするサービスである。店舗とは、例えば、現実空間に存在する物理的な店舗（実店舗）であるが、電子商取引の仮想店舗を含んでもよい。仮想店舗は、電子決済サービスの運営者とは異なる主体によって提供されるものを含んでもよい。その場合、仮想店舗における買い物の決済の際に、電子決済サービスのインターフェース画面に遷移するように制御される。電子決済サービスにおいて、店舗は、例えば加盟店（ブランド）に属するものとして扱われ、店舗において購買行動が行われた際の決済などの処理は、主として利用者と加盟店の間で行われる。これに代えて、決済などの処理が利用者と店舗との間で行われてもよい。

【００１１】

［電子決済サービス］

図１は、電子決済サービスが実現されるための構成の一例を示す図である。電子決済サービスは、決済サーバ１００を中心として実現される。決済サーバ１００は、例えば、一以上の利用者端末装置１０、一以上の第１店舗端末装置５０、及び一以上の第２店舗端末装置７０のそれぞれとネットワークＮＷを介して通信する。ネットワークＮＷは、例えば、インターネット、ＬＡＮ（Local Area Network）、無線基地局、プロバイダ装置などを含む。

【００１２】

利用者端末装置１０は、例えば、スマートフォンやタブレット端末等の可搬型端末装置である。利用者端末装置１０は、少なくとも、光学読取機能、通信機能、表示機能、入力受付機能、プログラム実行機能を有するコンピュータ装置である。以下の説明では、これらの機能を実現するための構成をそれぞれカメラ、通信装置、タッチパネル、ＣＰＵ（Central Processing Unit）等と称する。利用者端末装置１０では、ＣＰＵ等のプロセッサにより決済アプリ２０が実行されることで、決済サーバ１００と連携して電子決済サービスを利用者に提供するように動作する。決済アプリ２０は、例えば、アプリケーションストアから利用者端末装置１０にインストールされ、カメラ、通信装置、タッチパネルなどを制御する。

【００１３】

第１店舗端末装置５０は、例えば、店舗に設置される。第１店舗端末装置５０は、少なくとも、商品価格取得機能、光学読取機能、プログラム実行機能、通信機能を有するコンピュータ装置である。第１店舗端末装置５０は、いわゆるＰＯＳ（Point of Sale）装置を含み、ＰＯＳ装置によって商品価格取得機能や光学読取機能を実現してもよい。店舗コード画像６０は、店舗に置かれ、ＱＲコード（登録商標）等のコード画像が紙やプラスチックの媒体に印刷されたものである。なお、店舗コード画像６０は、店舗に置かれたディスプレイ（スマートフォンなどの端末装置のディスプレイでもよい）によって表示されてもよい。

【００１４】

第２店舗端末装置７０は、加盟店の運営者によって使用される。第２店舗端末装置７０は、スマートフォンやタブレット端末、パーソナルコンピュータ等である。第２店舗端末装置７０では、加盟店向けインターフェース７２が動作する。加盟店向けインターフェース７２は、加盟店向けアプリであってもよいし、ブラウザであってもよい。加盟店向けインターフェース７２は、加盟店の運営者によるクーポンの設定等を受け付け、決済サーバ１００に送信する。スマートフォンである第２店舗端末装置７０は、加盟店向けアプリを実行することで、店舗コード画像に相当するコード画像を表示したり、利用者端末装置１０が表示するコード画像を読み取ったりする機能を有する。

【００１５】

決済サーバ１００は、利用者端末装置１０または第１店舗端末装置５０から受信した決済情報に基づいて電子決済を実現する。第１店舗端末装置５０は、ＰＯＳ装置と加盟店サーバを含む場合があり、その場合、ＰＯＳ装置から加盟店サーバを介して決済情報が決済サーバ１００に送信される。以下の説明では、これを特に区別せず、第１店舗端末装置５０から決済情報が送信されるものとする。

【００１６】

図２および図３は、電子決済の大まかな流れを例示したシーケンス図である。電子決済には、パターン１とパターン２の二つが存在してよい。

【００１７】

図２に示すパターン１（以下、ユーザスキャンと称する）の場合、決済アプリ２０が起動した状態の利用者端末装置１０が、光学読取機能によって店舗コード画像６０をデコードする（Ｓ１）。店舗コード画像６０には、店舗ＵＲＬ（Uniform Resource Locator）の情報が含まれている。この店舗ＵＲＬは、電子決済サービスのドメインに対して店舗を識別可能な情報が付加されたものであり、決済サーバ１００において加盟店ＩＤや店舗Ｉ

Ｄ等との対応付けがなされている（後述）。決済アプリ２０は、店舗ＵＲＬとアカウントＩＤを含む第１決済情報を決済サーバ１００に送信する（Ｓ２）。決済サーバ１００は、店舗ＵＲＬに対応する加盟店ＩＤ、店舗ＩＤから、店舗情報（後述）を検索して加盟店名と店舗名の情報を取得し（Ｓ３）、決済アプリ２０に送信する（Ｓ４）。利用者は、加盟店名や店舗名が表示された画面において、決済金額を利用者端末装置１０に入力する（Ｓ５）。そして、利用者端末装置１０は、少なくとも決済金額を含む第２決済情報を生成し、決済サーバ１００に送信する（Ｓ６）。決済サーバ１００は、受信した第２決済情報に基づいて電子決済を行う（Ｓ７）。そして、決済サーバ１００は、決済完了通知（決済完了画面を表示するための情報）を決済アプリ２０に送信し（Ｓ８）、決済アプリ２０は決済完了画面を表示する（Ｓ９）。なお、店舗コード画像６０が店舗に置かれたディスプレイによって表示される場合、店舗コード画像６０には、店舗ＵＲＬだけでなく決済金額の情報が含まれる場合がある。この場合、利用者が決済金額を入力する手順が省略され、第１決済情報に決済金額の情報が含められて決済サーバ１００に送信される。加盟店名や店舗名の情報は、決済完了画面に含めて表示されてよい。

【００１８】

図３に示すパターン２（以下、ストアスキャンと称する）の場合、決済アプリ２０の起動時、決済アプリ２０において支払う操作が行われたとき、自動更新のタイミング（例えば１分おき）になったとき、およびその他のタイミングで、決済アプリ２０はワンタイムコードの発行要求を決済サーバ１００に送信する（Ｓ１１）。決済サーバ１００はワンタイムコードを生成し（Ｓ１２）、決済アプリ２０に送信する（Ｓ１３）。決済アプリ２０は、ワンタイムコードに基づいて生成した、ＱＲコードやバーコード等のコード画像を表示する（Ｓ１４）。利用者は利用者端末装置１０の表示面を第１店舗端末装置５０に翳し（提示し）、第１店舗端末装置５０は、光学読取機能によってコード画像をデコードし、ワンタイムコード等を取得する（Ｓ１５）。そして、第１店舗端末装置５０は、ワンタイムコード、決済金額、加盟店ＩＤ、店舗ＩＤ等を含む決済情報を生成し、決済サーバ１００に送信する（Ｓ１６）。決済金額の情報は、予めバーコード読み取りや手入力等によって取得されている。決済サーバ１００は、受信した情報に基づいて、ワンタイムコードに対応する利用者を特定し、電子決済を行う（Ｓ１７）。そして、決済サーバ１００は、決済完了通知を決済アプリ２０に送信し（Ｓ１８）、決済アプリ２０は決済完了画面を表示する（Ｓ１９）。

【００１９】

なお、上記のいずれか一方のみのパターンで電子決済が行われてもよい。また、図２で説明した「アカウントＩＤ」は、利用者の識別情報として用いられ得る他の情報（例えば電話番号）であってもよい。また、ストアスキャンにおいてワンタイムコードの発行が省略され、決済アプリ２０は、利用者のアカウントＩＤに基づいて生成したコード画像を表示してもよい。その場合、決済サーバ１００は、ワンタイムコードに対応する利用者を特定するのに代えて、アカウントＩＤに対応する利用者を特定する。

【００２０】

［決済サーバ］

図４は、決済サーバ１００の構成図である。決済サーバ１００は、例えば、通信部１１０と、ログイン状態管理部１２０と、決済コンテンツ提供部１２２と、決済処理部１２４と、ＳＭＳ認証部１２６と、番号変更時認証部１２８と、情報管理部１３０と、記憶部１７０とを備える。通信部１１０および記憶部１７０以外の構成要素は、例えば、ＣＰＵなどのハードウェアプロセッサがプログラム（ソフトウェア）を実行することにより実現される。これらの構成要素のうち一部または全部は、ＬＳＩ（Large Scale Integration）やＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field-Programmable Gate Array）、ＧＰＵ（Graphics Processing Unit）などのハードウェア（回路部；circuitryを含む）によって実現されてもよいし、ソフトウェアとハードウェアの協働によって実現されてもよい。プログラムは、予めＨＤＤ（Hard Disk Drive）やフラッシュメモリなどの記憶装置（非一過性の記憶媒体を備える記憶装置）に格納されていても

よいし、ＤＶＤやＣＤ－ＲＯＭなどの着脱可能な記憶媒体（非一過性の記憶媒体）に格納されており、記憶媒体がドライブ装置に装着されることで記憶装置にインストールされてもよい。

【００２１】

記憶部１７０は、ＨＤＤやフラッシュメモリ、ＲＡＭ（Random Access Memory）などである。記憶部１７０は、決済サーバ１００がネットワークを介してアクセス可能なＮＡＳ（Network Attached Storage）装置であってもよい。記憶部１７０には、利用者情報１７２、決済コンテンツ情報１７４、店舗情報１７６などの情報が格納される。

【００２２】

通信部１１０は、ネットワークＮＷに接続するための通信インターフェースである。通信部１１０は、例えばネットワークカードである。

【００２３】

ログイン状態管理部１２０は、各利用者のログイン状態を管理する。ログイン状態管理部１２０は、利用者が新規に決済アプリ２０をインストールし、各種情報を登録した時点で（新規登録した時点で）、その利用者がログインしたものとする。その後、ログイン状態管理部１２０は、同一の利用者端末装置１０からアクセスがあり、ログアウト操作がされていない限り、その利用者のログイン状態を維持する。新規登録において、利用者は少なくとも電話番号とパスワードを入力する。利用者が利用者端末装置１０を用いてログアウト操作を行い、その後で再度ログイン操作をした場合、ログイン状態管理部１２０は、利用者に電話番号とパスワードの入力を要求する。このとき、ログイン状態管理部１２０は、ＯＳの識別情報のハッシュ値などに基づいて利用者端末装置１０が以前のものと同一であるか否かを判別し、同一の利用者端末装置１０で無いと判定した場合、ＳＭＳ認証部１２６にＳＭＳ認証を行わせる。ＳＭＳ認証については後述する。

【００２４】

決済コンテンツ提供部１２２は、例えば、Ｗｅｂサーバの機能を有し、前述した決済完了画面を含む、電子決済サービスの各種画面を表示するための情報（コンテンツ）を利用者端末装置１０に提供する。決済コンテンツ提供部１２２は、決済コンテンツ情報１７４から適宜、必要なコンテンツを読み出して利用者端末装置１０に提供する。利用者端末装置１０は、決済アプリ２０によってコンテンツが再生された状態で利用者による各種入力を受け付け、前述した決済情報などを決済サーバ１００に送信する。なお、決済コンテンツ情報１７４に基づくコンテンツには、ログイン状態で提供されるコンテンツと、非ログイン状態で提供されるコンテンツがある。非ログイン状態のコンテンツにおいて、決済サーバ１００は、各種案内情報を提供したり、新規登録や電話番号の変更申し込みを受け付けたりする。

【００２５】

決済処理部１２４は、利用者端末装置１０または第１店舗端末装置５０により送信された決済情報に基づいて、決済処理を行う。決済処理部１２４は、利用者情報１７２を参照しながら決済処理を行う。

【００２６】

図５は、利用者情報１７２の内容の一例を示す図である。利用者情報１７２は、利用者の登録情報の一例である。利用者情報１７２は、例えば、アカウントＩＤ（省略されてもよい）に対して、新規登録時に最低限必要な電話番号およびパスワードの他、メールアドレス、利用者ＩＤ、氏名・住所・生年月日、登録日、チャージ残高、銀行口座、クレジットカード番号、他サービス連携情報、電波認証設定、キャリア決済設定、チャット友達リスト、チャージ履歴情報、決済履歴情報、チャット履歴情報、本人確認情報、ＩＳＰ（インターネットサービスプロバイダ）情報、位置情報履歴、端末言語設定などの情報が対応付けられたものである。以下、これらの情報が対応付けられた利用者のインスタンス（電子決済口座）のことをアカウントと称する。なお登録日とは利用者が電子決済サービスに登録した日（アカウントを作成した日）である。

【００２７】

チャージ残高は、利用者が予めアカウントに送金することで設定された電子マネーの残高を示す情報である。送金の手段としては、指定業者（銀行）のＡＴＭ（Automatic Teller Machine）からの送金、登録された銀行口座からの送金などがある。銀行口座とクレジットカード番号のそれぞれは、電子決済サービスに入金可能な銀行口座またはクレジットカード番号の情報（口座番号、カード番号）である。他サービス連携情報は、電子決済サービスと連携する（例えば同じ事業グループに属する運営者により運営されている）他のサービスのログインＩＤ等である。電波認証設定は、特定の通信キャリアとの通信によって認証を行う場合の設定情報である。キャリア決済設定は、電子決済サービスを利用した支払いの少なくとも一部を通信キャリアへの支払いに振り替えるための設定情報である。チャット友達リストは、電子決済サービスが提供するチャット機能においてチャットの相手先となる他の利用者のリストである。チャージ履歴情報は、利用者が予め電子決済サービスに送金してチャージ残高を増加させた履歴である。決済履歴情報は、利用者が行った決済の内訳（日時、購買行動が行われた店舗の店舗ＩＤ、決済金額等）を、決済ごとに示す情報である。チャット履歴情報は、利用者が行ったチャットの内容の履歴である。

【００２８】

本人確認情報は、利用者端末装置１０の近距離無線通信機能を用いて、ＩＣチップを内蔵する利用者の身分証明書から得られた電子情報である（第２電子情報の一例）。ＩＣチップを内蔵する身分証明書とは、例えば、マイナンバーカード、運転免許証などである。本人確認情報は、例えば、生年月日、郵便番号、氏名などを含み、身分証明書から電子的に取得されたことを示すフラグが付与されてよい。なお、広義の本人確認情報は、他の方法で取得された情報を含んでもよいが、本発明において本人確認情報は、ＩＣチップを内蔵する利用者の身分証明書から得られた電子情報に限るものとする。

【００２９】

ＩＳＰ情報は、利用者が使用するインターネットプロバイダ（以下、ＩＳＰと称する）の名称あるいはコード情報である。ＩＳＰ情報は、第１端末装置１０との通信で認識されるＩＰアドレスと、ＩＰアドレスとＩＳＰとの対応関係を規定したテーブルとを用いて情報管理部１３０により導出される。なお、公衆Ｗｉ－Ｆｉを使用した場合など、一人の利用者に複数のＩＳＰが対応付けられる場合があるが、最も頻度の高いＩＳＰが抽出されてＩＳＰ情報として格納されてもよい。また、頻度が一定以上の複数のＩＳＰがＩＳＰ情報として格納されてもよい。

【００３０】

端末言語設定は、利用者端末装置１０において利用者が設定している言語の情報である。日本語、英語、スペイン語などといった設定が端末言語設定として登録されている。

【００３１】

店舗の情報は、加盟店／店舗情報１７６として管理されている。図６は、加盟店／店舗情報１７６の内容の一例を示す図である。加盟店／店舗情報１７６は、例えば、店舗ＵＲＬに対して加盟店ＩＤと店舗ＩＤが対応付けられた第１テーブル１７６Ａと、加盟店ＩＤに対して加盟店名と売上金（前述）が対応付けられた第２テーブル１７６Ｂと、店舗ＩＤに対して店舗ＩＤが対応付けられた第３テーブル１７６Ｃとを含む。加盟店／店舗情報１７６には、これらの情報の他、加盟店または店舗のカテゴリ、店舗の所在地、決済パターン等の情報が含まれてもよい。

【００３２】

ＳＭＳ認証部１２６は、ＳＭＳ認証を行う。ＳＭＳ認証とは、電話番号を利用したショートメッセージにワンタイムパスワードを含めて利用者端末装置１０に送信し、利用者にワンタイムパスワードを利用者端末装置１０に入力させ、決済アプリ２０を介して決済サーバ１００に送信されたワンタイムパスワードが正しいかどうかを確認することで、電話番号が利用者のものであることを確認する認証方法である。前述したように、ＳＭＳ認証部１２６は、既に認識されている利用者端末装置１０とは異なる利用者端末装置１０から、同一の電話番号を使用したログイン要求がなされた場合、ＳＭＳ認証を行う。なおＳＭＳ認証は、ショートメッセージ内に貼り付けられたＵＲＬを操作することで完了するもの

であってもよい。以下について同様である。
【００３３】
番号変更時認証部１２８は、利用者から、利用者情報１７２に登録された電話番号とは異なる電話番号が対応付けられた利用者端末装置１０を通じて電話番号の変更が申し込まれたとき、電話番号変更時の認証処理を行う。なお、利用者情報１７２に登録された電話番号が対応付けられた利用者端末装置１０（つまり番号変更前の古い利用者端末装置１０）を通じて電話番号の変更が申し込まれた場合、ＳＭＳ認証のみで電話番号の変更が受け付けられる。
【００３４】
情報管理部１３０は、利用者端末装置１０から取得した情報に基づいて、利用者情報１７２の新たなレコードを作成したり、作成済みのレコードにおける各データ項目を更新したりする。
【００３５】
［電話番号変更］
以下、利用者が利用者情報１７２における電話番号を変更しようとする際の決済サーバ１００の動作について説明する。以下、変更前の電話番号（第１電話番号）が対応付けられた利用者端末装置１０を「第１端末装置」、変更後の電話番号（第２電話番号）が対応付けられた利用者端末装置１０を「第２端末装置」と略称する。
【００３６】
利用者情報１７２に登録された第１電話番号とは異なる第２電話番号が対応付けられた第２端末装置を通じて電話番号の変更が申し込まれた場合、従来の手法では、フォームの入力を利用者に要求してオペレータのオフライン処理などを経て電話番号の変更が承認されていた。係る手法は時間を要し、また利用者にとって煩雑に感じられる場合がある。
【００３７】
そこで、本発明の番号変更時認証部１２８は、電子決済サービスの利便性を高めるため、以下に説明するように、非ログイン状態でオンライン電話番号変更を可能とする処理を行う。なお「非ログイン状態」と称するのは、電話番号の変更前に第２端末装置でログインすることは不可であるため、必然的に非ログイン状態となるからである。
【００３８】
図７は、利用者が第１端末装置を手元に保持しておらず、第２端末装置のみ手元に保持している場合の、電話番号変更の流れを示す図である。まず、利用者が、非ログイン状態の第２端末装置に対して、第１電話番号および第２電話番号を入力して電話番号の変更の申し込みを行う（Ｓ２１）。第２端末装置の決済アプリ２０は、入力された情報を決済サーバ１００に送信する（Ｓ２２）。番号変更時認証部１２８は、第１電話番号が利用者情報１７２に登録されていることを確認する（Ｓ２３）。第１電話番号が利用者情報１７２に登録されていない場合、以降の処理が停止される。その場合、エラーメッセージを決済アプリ２０に表示させて最初から申し込みのやり直しを要求するなどの措置が取られる。
【００３９】
第１電話番号が利用者情報１７２に登録されていることが確認されると、ＳＭＳ認証部１２６がＳＭＳ認証を行う。なお、ＳＭＳ認証と以下に説明する確認シーケンスの順序は逆でもよい。まず、ＳＭＳ認証部１２６がＳＭＳ認証コードを生成して、申し込みに係る第２電話番号を用いたショートメッセージに含めて送信する（Ｓ２４）。利用者は、ショートメッセ―ジに記載されているＳＭＳ認証コードを決済アプリ２０に入力する（Ｓ２５）。決済アプリ２０は、入力されたＳＭＳ認証コードを決済サーバ１００に送信する（Ｓ２６）。ＳＭＳ認証部１２６は、返信されたＳＭＳ認証コードが正しいことを確認する（Ｓ２７）。返信されたＳＭＳ認証コードが正しくない場合、以降の処理が停止される。その場合、Ｓ２３の処理に戻る、或いはエラーメッセージを決済アプリ２０に表示させて最初から申し込みのやり直しを要求するなどの措置が取られる。
【００４０】
次に、番号変更時認証部１２８および情報管理部１３０による確認シーケンスが実施さ

れる。確認シーケンスの結果、確認処理が成功すると、情報管理部１３０が、利用者情報１７２における当該アカウントの電話番号を、申し込みに係る第２電話番号に変更し（Ｓ６０）、情報管理部１３０（或いは決済コンテンツ提供部１２２）が、電話番号の変更が完了したことを示す変更完了通知を決済アプリ２０に送信する（Ｓ６１）。これによって、第２電話番号を用いたアカウントへのログインが可能となる。

【００４１】

［確認シーケンス］

以下、番号変更時認証部１２８および情報管理部１３０による確認シーケンスの詳細について説明する。図８～図９は、第２端末装置の決済アプリ２０、番号変更時認証部１２８および情報管理部１３０により実行される処理の内容の一例を示すフローチャートである。

【００４２】

まず、決済アプリ２０は、決済サーバ１００からの確認シーケンス開始の通知を受けて、第２端末装置において位置情報がオンになっており、更に決済アプリ２０が位置情報の使用を許可されているか否かを判定する（Ｓ３０）。位置情報がオフになっている、または決済アプリ２０が位置情報の使用を許可されていない場合、決済アプリ２０は、位置情報をオンにし決済アプリ２０に位置情報の使用を許可するように促す通知を利用者に表示する（Ｓ３１）。

【００４３】

決済アプリ２０は、位置情報がオンであり、且つ決済アプリ２０が位置情報の使用を許可されている状態である場合は、位置情報と端末言語設定の情報を決済サーバ１００に送信する（Ｓ３２）。このとき、送信されるデータにはＩＰアドレスが含まれるため、決済サーバ１００は位置情報、端末言語設定、およびＩＰアドレスから認識可能なＩＳＰの情報を取得することになる。

【００４４】

一方、位置情報がオフになっている、または決済アプリ２０が位置情報の使用を許可されていない状態でタイムアウトした場合、決済アプリ２０は、端末言語設定の情報を決済サーバ１００に送信する（Ｓ３３）。このとき、送信されるデータにもＩＰアドレスが含まれるため、決済サーバ１００は端末言語設定、およびＩＰアドレスから認識可能なＩＳＰの情報を取得することになる。

【００４５】

決済サーバ１００において、番号変更時認証部１２８は、まず、利用者の回答に依らずに取得される、ＩＳＰ、位置情報、および端末言語設定に基づいてスコアＳＣを計算する（Ｓ３４）。例えば、番号変更時認証部１２８は、スコアＳＣの初期値をゼロに設定し、以下のようにスコアを加算または減算する。スコアＳＣは例えば１００点を十分な合格点として計算されるものである。なお、Ｓ３４においてスコアＳＣを算定するための情報としてＩＳＰ、位置情報、および端末言語設定のうち一部が省略されてもよい。

【００４６】

（１）：番号変更時認証部１２８は、第１端末装置との通信によって得られたＩＰアドレスから導出されるＩＳＰ名と、第２端末装置との通信によって得られたＩＰアドレスから導出されるＩＳＰ名とが一致し、且つ当該一致したＩＳＰ名がシェア上位の数社（特定のＩＳＰ）の名称でない場合、スコアＳＣにα１を加算する。α１は、５～３０程度の値である。ＩＳＰ名が一致しない場合、或いは一致したＩＳＰ名がシェア上位の数社の名称である場合、番号変更時認証部１２８は、ＩＳＰに基づくスコアＳＣへの加算を行わない。多くの利用者が利用するＩＳＰは、利用者を特定するには十分な情報ではないと考えられるからである。

【００４７】

（２）：番号変更時認証部１２８は、第２端末装置から取得した位置情報が、電話番号の変更の申し込み以前に取得された位置情報（第１端末装置から取得した位置情報でもよいし、それよりも前の端末装置から取得した位置情報でもよい）と合致している場合、ス

コアＳＣにα２を加算する。α２は、５～３０程度の値である。電話番号の変更の申し込み以前に取得された位置情報は、決済アプリ２０からアップロードされる位置情報でもよいし、電子決済が行われた店舗の場所から導出された位置情報でもよい。「位置情報が合致する」とは、最頻値や平均値などの代表値が所定範囲内であることを意味してもよいし、就寝時（夜間）に限定した代表値が所定範囲内であることを意味してもよいし、過去に取得された位置情報のいずれかと比較して所定範囲内であることを意味してもよいし、その他の基準で判断されるものであってもよい。位置情報が合致しない場合、または第２端末装置から位置情報が取得されていない場合、番号変更時認証部１２８は、位置情報に基づくスコアＳＣへの加算を行わない。なお、番号変更時認証部１２８は、固定値であるα２をスコアＳＣに加算するのに代えて、第２端末装置から取得した位置情報と、電話番号の変更の申し込み以前に取得された位置情報との距離が短いほど大きい値をスコアＳＣに加算するようにしてもよいし、第２端末装置から取得した位置情報と、電話番号の変更の申し込み以前に取得された位置情報との距離の大多数が非常に遠い場合にマイナスの値をスコアＳＣに加算する（正の値を減算するようにしてもよい。

【００４８】

（３）：第２端末装置から取得した端末言語設定が、第１装置から取得していた（利用者情報１７２に登録されている）端末言語設定と一致しない場合、番号変更時認証部１２８は、スコアＳＣからα３を減算する。α３は、３０～７０程度の値である。端末言語設定が一致する場合、番号変更時認証部１２８は、端末言語設定に基づくスコアＳＣからの減算を行わない、或いは任意の値をスコアＳＣに加算してもよい。

【００４９】

このように、番号変更時認証部１２８は、ＩＳＰ情報や端末言語設定といった、利用者を特定する上で十分な効力があり、且つ利用者の手を煩わせることなく自動的に取得可能な情報に基づいて電話番号の変更のための判断を行う。これによって、より適切かつ簡便に電話番号の変更を承諾することができる。

【００５０】

次に、番号変更時認証部１２８は、申し込みに係る利用者の本人確認情報が利用者情報１７２に登録されているか否かを判定する（Ｓ３５）。登録されている場合、番号変更時認証部１２８は、第２端末装置の決済アプリ２０に、本人確認情報の送信を促す情報を送信する（Ｓ３６）。第２端末装置の決済アプリ２０は、以前に利用者端末装置１０で読み取ったのと同じ本人確認情報を読み込むように促す画像を表示する（Ｓ３７）。本人確認情報が読み込まれると、決済アプリ２０は読み取った本人確認情報（第１電子情報の一例）を決済サーバ１００に送信する（Ｓ３８、Ｓ３９）。番号変更時認証部１２８は、本人確認情報が取得され、且つ利用者情報１７２に登録されたものと一致するか否かを判定し（Ｓ４０）、一致する場合は電話番号の変更を承諾する旨を情報管理部１３０に通知する（Ｓ４１）。これを受けて情報管理部１３０は、第２電話番号に変更し（図７のＳ６０）、変更完了通知を行う（Ｓ６１）。身分証明書から得られた本人確認情報は、利用者の身分を証明するために十分な信頼度があると考えらえるため、係る処理を行うことで、利用者が質問に回答する手間を省いて、より簡易な手続きで適切に電話番号の変更を承諾することができる。

【００５１】

本人確認情報が取得されなかった（利用者が読み取りを行わなかった）、或いは利用者情報１７２に登録されたものと一致しなかった場合、図９の処理に進む。

【００５２】

なお、Ｓ３５～Ｓ４１の処理で示したように、本人確認情報が一致した場合に直ちに電話番号の変更が承諾されるのではなく、本人確認情報が一致した場合にスコアＳＣに値が加算され、仮に端末言語設定の不一致によるマイナスがあった場合には後続の質問でプラス評価が無ければ電話番号の変更が承諾されないようにしてもよい。また、本人確認情報の読み取りを促す表示は、以下に説明する質問の一つとして利用者に提示されてもよい。

【００５３】

ここで、本人確認情報が部分一致するケースも想定される。例えば、身分証明書において住所変更や婚姻等による姓の変更があったが、電子決済サービスにおいて変更登録をしていないケースが該当する。この場合、生年月日と氏名が一致するが住所が一致しない、生年月日、住所、および名が一致するが姓が一致しないといったことが生じ得る。本人確認情報が部分一致する場合は直ちに電話番号の変更が承諾されるのではなく、ある程度の値をスコアに加算した上で後続の質問取得に進んでもよい。また、そもそも本人確認情報が完全一致した場合に直ちに電話番号の変更が承諾されるのではない場合であっても、本人確認が部分一致した場合は、本人確認情報が完全一致した場合に与える値よりも低い値をスコアに加算するようにしてもよい。

【００５４】

そして、番号変更時認証部１２８は、本人確認情報が部分一致する場合、電話番号の変更処理が完了した後に、利用者情報１７２における本人確認情報の更新を促す情報を決済アプリ２０に表示させるようにしてもよいし、本人確認情報の更新を必須とする（更新しなければ電話番号の変更を承諾しない、或いは取り消す）ようにしてもよい。本人確認情報が部分一致する場合とは、本人確認情報が「合致しない」場合の一例である。なお、本人確認情報のうち姓のみが異なる場合、本人確認情報が「合致する」とみなして、完全一致する場合と同様の処理を行ってもよい。

【００５５】

図９に進み、番号変更時認証部１２８は、予め用意され記憶部１７０に記憶された質問リスト１７８を参照し、利用者に提示する質問への回答事項のそれぞれが利用者情報１７２に登録されているか否かを確認し、回答事項が登録されている質問のみを抽出する（Ｓ４２）。

【００５６】

図１０は、質問リスト１７８から質問が抽出される様子を示す図である。質問リスト１７８として、例えば、生年月日、郵便番号、氏名、パスワード、他サービスログインＩＤ、メールアドレスに送信されたメール認証コード、銀行口座、現在の残高（チャージ残高）、１年以内の支払い履歴、１年以内のチャージ履歴といったものが用意されている。１年以内の支払い履歴、および１年以内のチャージ履歴は、電子決済サービスの利用履歴の一例である。電子決済サービスの利用履歴は、更に、利用者間送金の履歴を含んでもよい。これらのうち、利用者情報１７２に正解（メール認証コードに関してはメールアドレス）が登録されていないものは質問から省かれる。なお、パスワードと現在のチャージ残高に関しては必ず利用者情報１７２に登録されているものであるため、全ての利用者に提示される質問として抽出される。図１０の例では、生年月日、郵便番号、氏名、メールアドレス、銀行口座、１年以内の支払い履歴が利用者情報１７２に登録されていないため、残りのパスワード、他サービスログインＩＤ、現在の残高、１年以内のチャージ履歴が質問として抽出される。質問リスト１７８に登録された各質問ｋには、スコアＳＣに加算される点数βｋ（ｋ＝１～ｍ、ｍは質問の数）が予め設定されている。βｋのそれぞれは、５～５０程度の値である。なお、Ｓ３６で取得される本人確認情報は、生年月日、郵便番号、および氏名を含むものであるが、質問に対する回答として生年月日、郵便番号、および氏名が得られた場合のプラス評価は、Ｃチップを内蔵する利用者の身分証明書から得られた電子情報が一致した場合よりも低く設定される。これは、手入力によって入力された情報の信頼度が身分証明書からの情報よりも低いからである。

【００５７】

ここで、「現在の残高」に関しては正確な金額ではなくレンジ（例えば「０～１０００円、１０００円～５０００円、５０００円～１００００円」）のどれに該当するかを選択させる形で質問が提示されてもよい。また、「支払い履歴」に関しては加盟店または店舗も併せて質問されてもよい。更に、日時、加盟店、金額のうち一部について正解を示しつつ、他の一部を回答させるようにしてもよい。また、「チャージ履歴」に関しては日時と金額を入力させるのに加えて、チャージ手段（コンビニエンスストア端末、銀行口座など）も併せて回答させるようにしてもよい。これについても「支払い履歴」と同様に、一部

について正解を示しつつ、他の一部を回答させるようにしてもよい。更に、図１０に示した質問に加えて、利用者間送金の履歴を質問してもよい。この場合、送金先や受金元のアカウント（電話番号から検索して選択させてもよい）を回答させるようにしてもよい。

【００５８】

更に、質問の内容として、利用者の過去の電子決済サービスの利用履歴の中で出現頻度が高い内容を質問するようにしてもよい。例えば、決済頻度が高い加盟店、送金頻度が高い送金元または送金先、利用頻度が高いチャージ手段などを質問するようにしてもよい。

【００５９】

番号変更時認証部１２８は、Ｓ４２で抽出した質問を提示（表示）するように第２端末装置の決済アプリ２０に指示する（Ｓ４３）。このとき、質問を提示する形式は、質問が含まれるコンテンツを決済サーバ１００から決済アプリ２０に提供する形であってもよいし、質問自体は予め決済アプリ２０に埋め込まれており、決済サーバ１００は提示する質問を指定する情報を決済アプリ２０に送信する形であってもよい。

【００６０】

第２端末装置の決済アプリ２０は、決済サーバ１００により指示された質問を利用者に提示する（Ｓ４４）。図１１は、決済アプリ２０が第２端末装置に表示させる質問提示画面ＩＭ１の一例を示す図である。質問提示画面ＩＭ１には、一以上の質問に回答するための領域Ａ１～Ａｎが含まれる。それぞれの領域には、質問展開スイッチＳＷ１が設けられており、展開スイッチＳＷを操作することで質問の詳細が表示されるようになっている。

【００６１】

利用者の回答を取得すると（Ｓ４５）、決済アプリ２０は回答を決済サーバ１００に送信する（Ｓ４６）。決済サーバ１００の番号変更時認証部１２８は、回答に基づいてスコアを計算する（Ｓ４７）。番号変更時認証部１２８は、正解した質問に対して設定された点数βｋを合計して、Ｓ３４で計算されたスコアＳＣに加算することで、最終的なスコアＳＣを計算する。

【００６２】

番号変更時認証部１２８は、最終的なスコアＳＣが閾値Ｔｈ１以上であるか否かを判定する（Ｓ４８）。閾値Ｔｈ１は、前述したように１００程度の値である。スコアＳＣが閾値Ｔｈ１以上である場合、電話番号の変更を承諾する旨を情報管理部１３０に通知する（Ｓ４９）。これを受けて情報管理部１３０は、第２電話番号に変更し（図７のＳ６０）、変更完了通知を行う（Ｓ６１）。

【００６３】

最終的なスコアＳＣが閾値Ｔｈ１未満である場合、番号変更時認証部１２８は、最終的なスコアＳＣが閾値Ｔｈ２以上であるか否かを判定する（Ｓ５０）。閾値Ｔｈ２は閾値Ｔｈ１よりも小さい値であり、例えば７０程度の値である。最終的なスコアＳＣが閾値Ｔｈ１未満かつが閾値Ｔｈ２以上である場合、番号変更時認証部１２８は、電話番号の変更を承諾するが、利用者情報１７２における一部の情報を削除すべきである旨を情報管理部１３０に通知する（Ｓ５１）。これを受けて情報管理部１３０は、利用者情報１７２のうち一部の情報を削除（または隠蔽）し（Ｓ５２）、第２電話番号に変更し（図７のＳ６０）、変更完了通知を行う（Ｓ６１）。Ｓ５２において情報管理部１３０が削除または隠蔽する情報は、例えば、銀行口座、クレジットカード番号、および後払いに関する各種情報に加えて、利用者間で送金する相手の情報、利用者間送金履歴の情報など、仮に第２端末装置を用いて電話番号変更を試みているのが不正な利用者であった場合に、正当な利用者への被害が大きくなる可能性がある情報である。銀行口座、クレジットカード番号、および後払いに関する各種情報は、「電子決済サービスを運営する事業者とは異なる事業者の金融サービスに関する情報」の一例である。隠蔽するとは、データ自体は残しつつアクセスを禁止することである。最終的なスコアＳＣが閾値Ｔｈ１未満かつが閾値Ｔｈ２以上であるということは、正当な利用者である可能性が高いものの、不正な利用者である疑いが十分に払拭できないことを示している。そのような場合に利用者情報１７２の全てを第２端末装置に対応付けてしまうと予期せぬ被害が生じることがあり得るため、一部情報を削除

して電話番号の変更を承諾することで、利便性と安全性の両立を実現することができる。情報管理部１３０は、最終的なスコアＳＣが閾値Ｔｈ１以上である場合、利用者情報１７２のうち一部の情報を削除（または隠蔽）しない。これに代えて、情報管理部１３０は、最終的なスコアＳＣが閾値Ｔｈ１以上である場合にも、念のため一部の情報を削除または隠蔽するようにしてもよく、その場合、削除または隠蔽する情報を、スコアＳＣが閾値Ｔｈ１未満かつ閾値Ｔｈ２以上である場合よりも少なくすればよい。また、最終的なスコアＳＣが閾値Ｔｈ１未満かつが閾値Ｔｈ２以上である場合、番号変更時認証部１２８は、電話番号の変更を承諾する上で、本人確認情報の更新を必須とする（更新しなければ電話番号の変更を承諾しない、或いは取り消す）ようにしてもよい。

【００６４】

また、最終的なスコアＳＣが閾値Ｔｈ１未満かつが閾値Ｔｈ２以上である場合、情報管理部１３０は、回答が正解であった事項については削除しないようにしてもよい。例えば、銀行口座を問う質問について回答が正解であった場合、利用者情報１７２から銀行口座の情報を削除または隠蔽しないようにしてもよい。このように、情報管理部１３０は、最終的なスコアＳＣが閾値Ｔｈ１未満かつが閾値Ｔｈ２以上である場合に削除または隠蔽する情報を、利用者の正解状況に応じて決定してもよい。

【００６５】

最終的なスコアＳＣが閾値Ｔｈ２未満である場合、番号変更時認証部１２８は、電話番号の変更を承諾しない旨を情報管理部１３０に通知する（Ｓ５３）。この場合、決済アプリ２０は、電話番号の変更に失敗した旨の情報を第２端末装置に表示させる。

【００６６】

以上説明した実施形態によれば、より適切かつ簡便に電話番号の変更を承諾することができる。また、より簡易な手続きで適切に電話番号の変更を承諾することができる。また、利便性と安全性の両立を実現することができる。

【００６７】

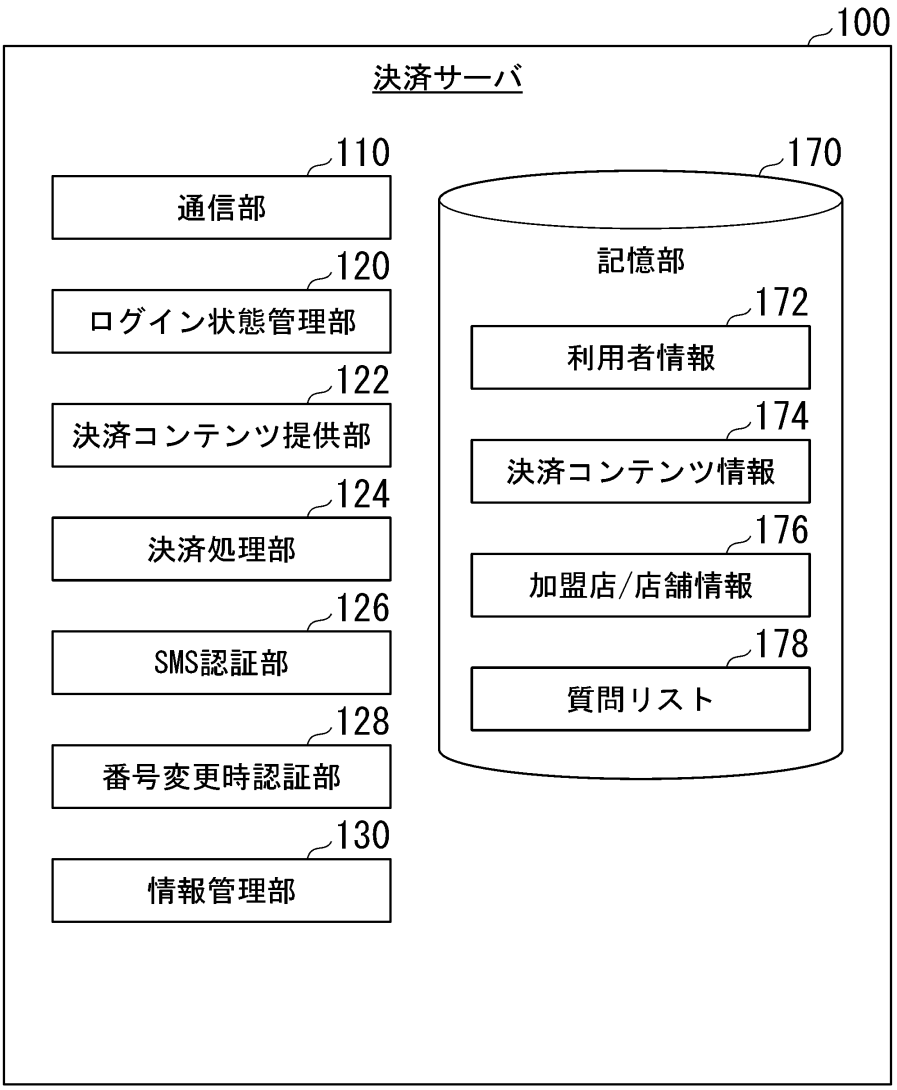
以上、本発明を実施するための形態について実施形態を用いて説明したが、本発明はこうした実施形態に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々の変形及び置換を加えることができる。

【符号の説明】

【００６８】

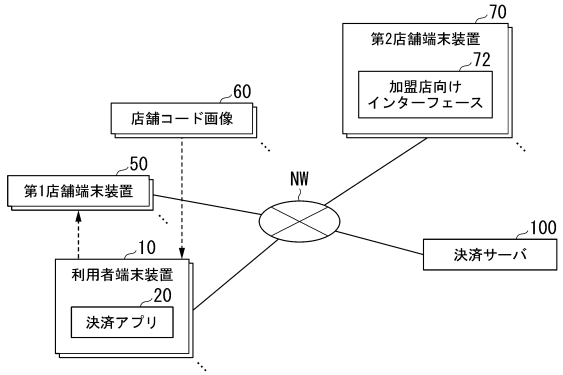
１０　利用者端末装置
２０　決済アプリ
５０　店舗端末装置
６０　店舗コード画像
１００　決済サーバ
１２０　ログイン状態管理部
１２２　決済コンテンツ提供部
１２４　決済処理部
１２６　ＳＭＳ認証部
１２８　番号変更時認証部
１３０　情報管理部
１７０　記憶部
１７２　利用者情報
１７４　決済コンテンツ情報
１７６　加盟店／店舗情報
１７８　質問リスト

【要約】
【課題】利便性と安全性の両立を実現すること。
【解決手段】利用者から、登録情報に登録された第１電話番号であって第１端末装置に対応付けられた第１電話番号とは異なる第２電話番号が対応付けられた第２端末装置を通じて電話番号の変更が申し込まれたとき、複数の質問を含むコンテンツを第２端末装置に提供し、利用者の回答を第２端末装置から取得し、複数の確認情報に基づくスコアと第１閾値、およびスコアと第１閾値よりも小さい第２閾値を、それぞれ比較し、スコアが第１閾値以上である場合、およびスコアが第２閾値以上である場合に、申し込みに係る新しい電話番号で登録情報を更新し、スコアが第１閾値未満かつ第２閾値以上である場合には、登録情報に含まれる情報の一部を削除または隠蔽する、サービス提供装置。
【選択図】図４

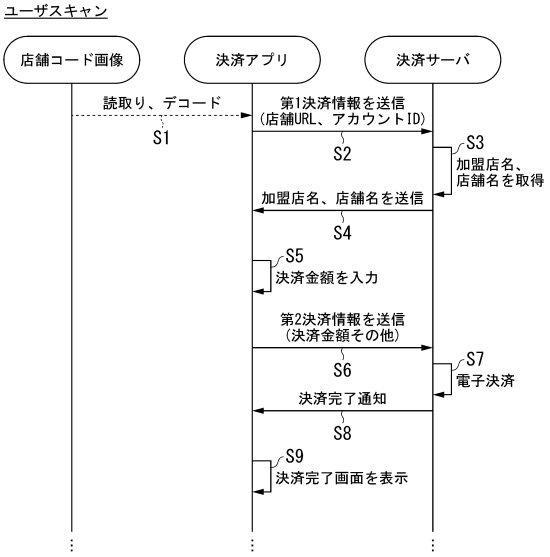


【図面】

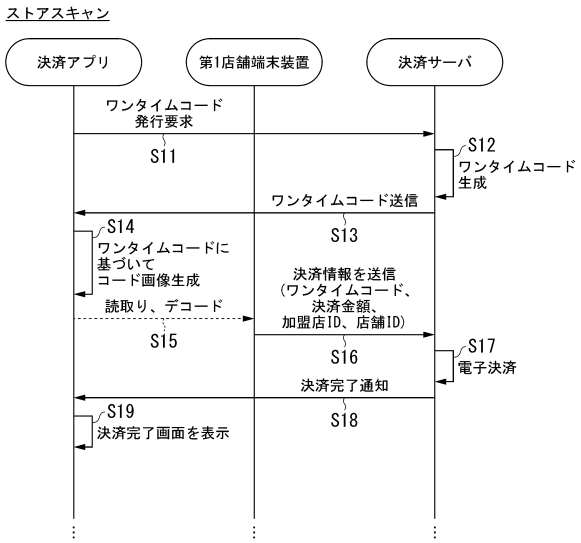
【図１】


70
第2店舗端末装置
72
加盟店向け
インターフェース
60
店舗コード画像
50
第1店舗端末装置
NW
100
決済サーバ
10
利用者端末装置
20
決済アプリ

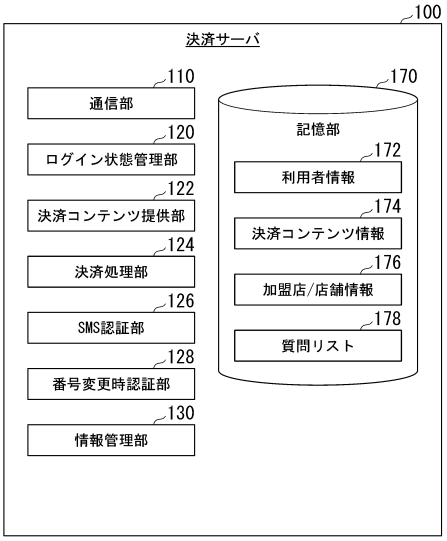
【図２】


ユーザスキャン
店舗コード画像
決済アプリ
決済サーバ
読取り、デコード
S1
第1決済情報を送信
(店舗URL、アカウントID)
S2
S3
加盟店名、
店舗名を取得
加盟店名、店舗名を送信
S4
S5
決済金額を入力
第2決済情報を送信
(決済金額その他)
S6
S7
電子決済
決済完了通知
S8
S9
決済完了画面を表示

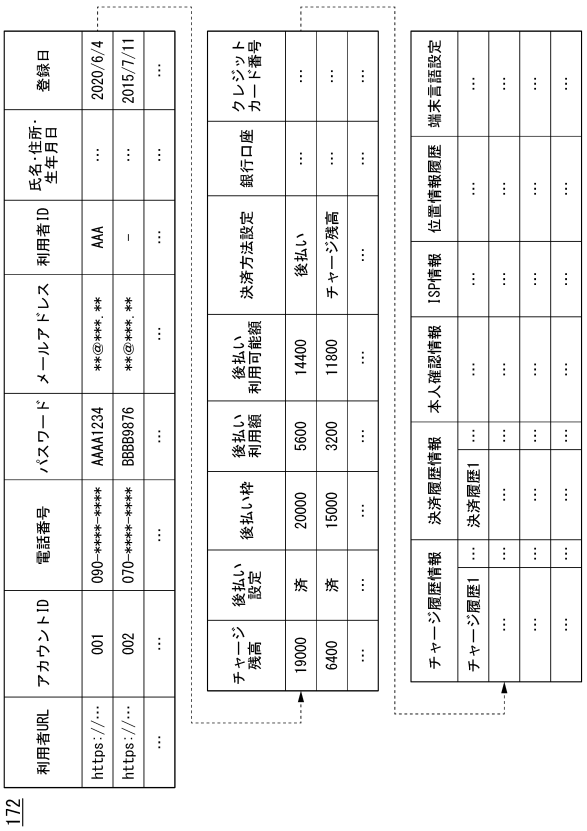
【図３】


ストアスキャン
決済アプリ
第1店舗端末装置
決済サーバ
ワンタイムコード
発行要求
S11
S12
ワンタイムコード
生成
ワンタイムコード送信
S13
S14
ワンタイムコードに
基づいて
コード画像生成
決済情報を送信
(ワンタイムコード、
決済金額、
加盟店ID、店舗ID)
読取り、デコード
S15
S16
S17
電子決済
決済完了通知
S18
S19
決済完了画面を表示

【図４】


100
決済サーバ
110
通信部
120
ログイン状態管理部
122
決済コンテンツ提供部
124
決済処理部
126
SMS認証部
128
番号変更時認証部
130
情報管理部
170
記憶部
172
利用者情報
174
決済コンテンツ情報
176
加盟店/店舗情報
178
質問リスト

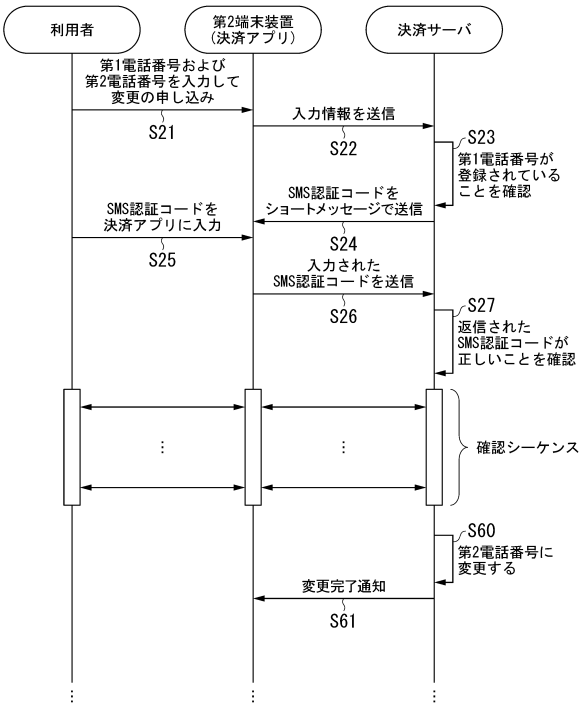
【図５】


172
利用者URL
アカウントID
電話番号
パスワード
メールアドレス
利用者ID
氏名・住所・生年月日
登録日
https://…
001
090-****-****
AAAA1234
**@***.**
AAA
2020/6/4
002
070-****-****
BBBB9876
**@***.**
–
2015/7/11
チャージ残高
後払い設定
後払い枠
後払い利用額
後払い利用可能額
決済方法設定
銀行口座
クレジットカード番号
19000
済
20000
5600
14400
後払い
6400
済
15000
3200
11800
チャージ残高
チャージ履歴情報
チャージ履歴1
決済履歴情報
決済履歴1
本人確認情報
ISP情報
位置情報履歴
端末言語設定

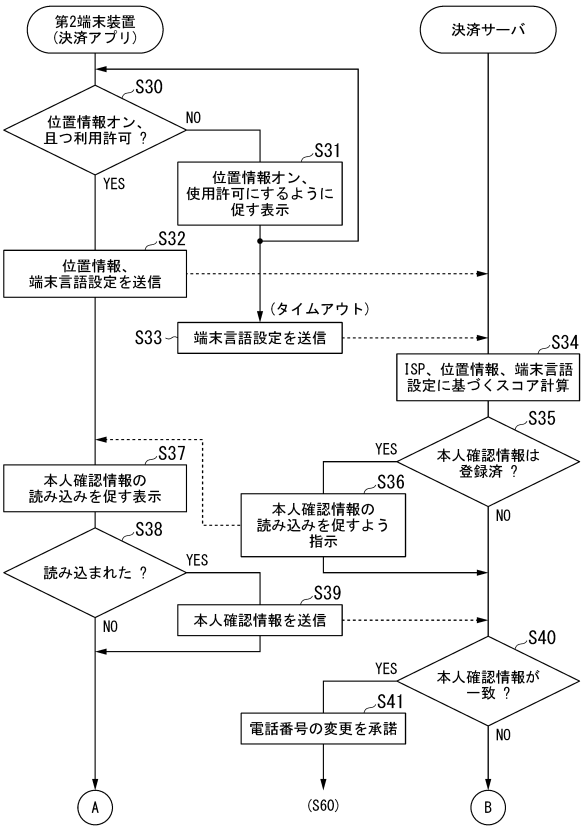
【図６】


176
176A
店舗URL
加盟店ID
店舗ID
https://…
13579
651874
https://…
24685
2495782
176B
加盟店ID
加盟店名
売上金
13579
〇〇珈琲
557420
24685
△△寿司
1257400
176C
店舗ID
店舗名
651874
大井町店
2495782
目黒店

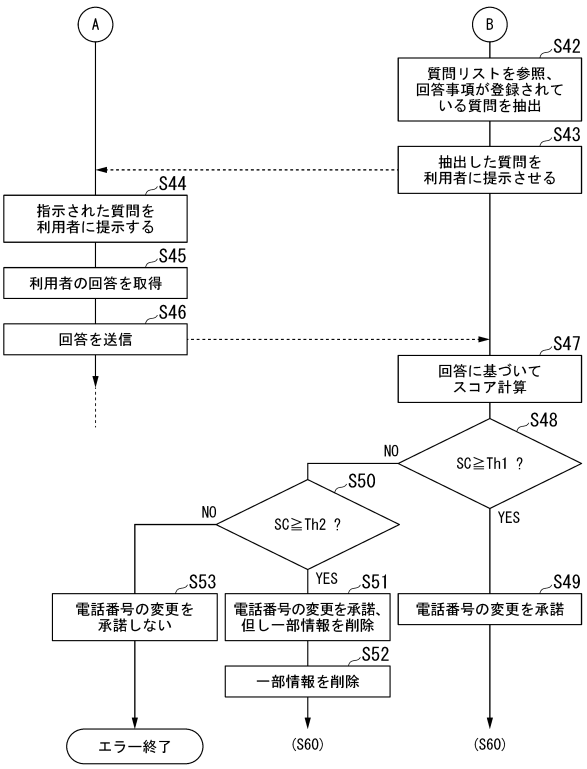
【図７】


利用者
第2端末装置（決済アプリ）
決済サーバ
第1電話番号および第2電話番号を入力して変更の申し込み
S21
入力情報を送信
S22
S23
第1電話番号が登録されていることを確認
SMS認証コードをショートメッセージで送信
S24
SMS認証コードを決済アプリに入力
S25
入力されたSMS認証コードを送信
S26
S27
返信されたSMS認証コードが正しいことを確認
確認シーケンス
S60
第2電話番号に変更する
変更完了通知
S61

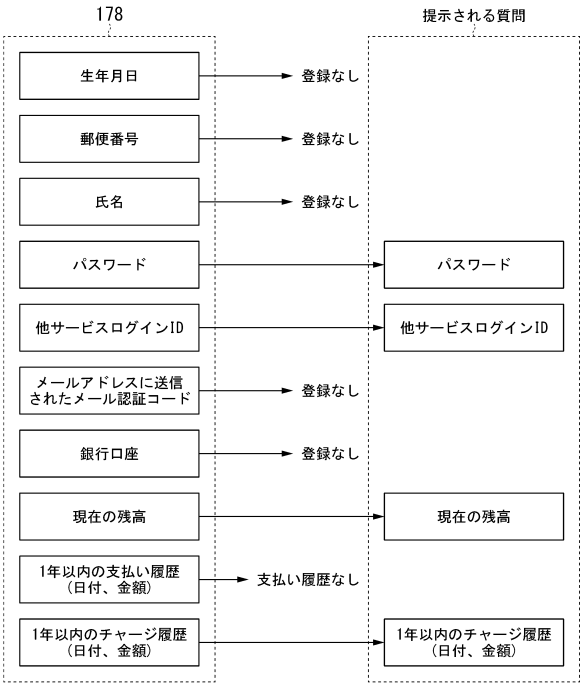
【図８】


第2端末装置（決済アプリ）
決済サーバ
S30
位置情報オン、且つ利用許可 ？
NO
YES
S31
位置情報オン、使用許可にするように促す表示
S32
位置情報、端末言語設定を送信
（タイムアウト）
S33
端末言語設定を送信
S34
ISP、位置情報、端末言語設定に基づくスコア計算
S35
本人確認情報は登録済 ？
YES
NO
S36
本人確認情報の読み込みを促すよう指示
S37
本人確認情報の読み込みを促す表示
S38
読み込まれた ？
YES
NO
S39
本人確認情報を送信
S40
本人確認情報が一致 ？
YES
NO
S41
電話番号の変更を承諾
A
(S60)
B

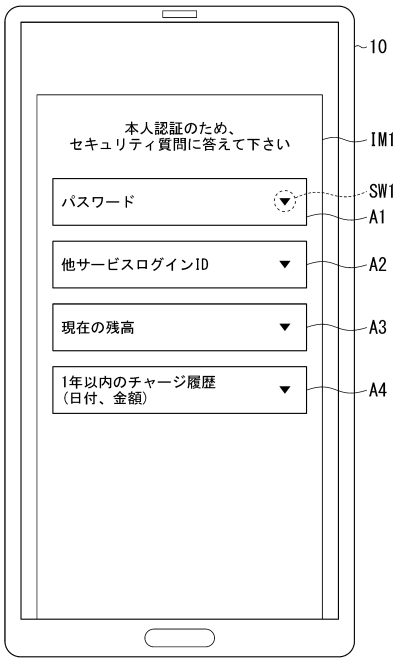
【図９】


A
B
S42
質問リストを参照、
回答事項が登録されて
いる質問を抽出
S43
抽出した質問を
利用者に提示させる
S44
指示された質問を
利用者に提示する
S45
利用者の回答を取得
S46
回答を送信
S47
回答に基づいて
スコア計算
S48
SC≧Th1 ？
NO
YES
S50
SC≧Th2 ？
NO
YES
S53
電話番号の変更を
承諾しない
S51
電話番号の変更を承諾、
但し一部情報を削除
S49
電話番号の変更を承諾
S52
一部情報を削除
エラー終了
(S60)
(S60)

【図１０】


178
提示される質問
生年月日
登録なし
郵便番号
登録なし
氏名
登録なし
パスワード
パスワード
他サービスログインID
他サービスログインID
メールアドレスに送信
されたメール認証コード
登録なし
銀行口座
登録なし
現在の残高
現在の残高
1年以内の支払い履歴
（日付、金額）
支払い履歴なし
1年以内のチャージ履歴
（日付、金額）
1年以内のチャージ履歴
（日付、金額）

【図１１】


10
本人認証のため、
セキュリティ質問に答えて下さい
IM1
パスワード
SW1
A1
他サービスログインID
A2
現在の残高
A3
1年以内のチャージ履歴
（日付、金額）
A4

フロントページの続き

(56)参考文献　　特許第７１９５４７３（ＪＰ，Ｂ１）
特開２０２３－６２４３４（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００
Ｇ０６Ｆ　２１／３１－２１／４３