(19)日本国特許庁(JP)

(12)特許公報(B1)

(11)特許番号
特許第7247416号
(P7247416)

(45)発行日　令和5年3月28日(2023.3.28)

(24)登録日　令和5年3月17日(2023.3.17)

(51)国際特許分類

Ｇ０６Ｆ　21/45　(2013.01)		Ｇ０６Ｆ	21/45
Ｇ０６Ｆ　21/31　(2013.01)		Ｇ０６Ｆ	21/31

ＦＩ

請求項の数　13　（全17頁）

(21)出願番号　特願2022-205656(P2022-205656)
(22)出願日　令和4年12月22日(2022.12.22)
(62)分割の表示　特願2022-136645(P2022-136645)の分割
原出願日　令和4年8月30日(2022.8.30)
審査請求日　令和4年12月22日(2022.12.22)
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　岸野 徹

最終頁に続く

(54)【発明の名称】　情報処理装置、情報処理方法、およびプログラム

(57)【特許請求の範囲】

【請求項１】

利用者の第１端末装置から、前記第１端末装置を一意に識別可能な第１識別情報を少なくとも含む、アプリ又はＷｅｂサービスへのログイン要求を受信する受信部と、

受信した前記ログイン要求に含まれる前記第１識別情報と、記憶部に事前に記憶された、前記アプリ又は前記Ｗｅｂサービスに過去にログインした端末装置を一意に識別可能な識別情報とが一致しない場合、前記第１端末装置から、前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有しているか否かを示す情報を受信し、受信した前記情報に応じて、前記第１端末装置に対する前記アプリ又は前記Ｗｅｂサービスへのログイン認証方法を切り替える認証部と、を備える、

情報処理装置。

【請求項２】

前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有しているか否かを示す情報は、前記利用者が現在利用する利用端末の台数が１台のみでないか否かを示す情報である、

請求項１に記載の情報処理装置。

【請求項３】

前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有しているか否かを示す情報は、前記利用者が前記アプリ又は前記Ｗｅｂサービスを過去に利用した端末装置を保有しているか否かを示す情報である、

請求項１に記載の情報処理装置。
【請求項４】
前記認証部は、前記第１識別情報と前記識別情報とが一致しない場合、前記第１端末装置に、前記利用者が利用する前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有しているか否かを問い合わせ、前記問いあわせの結果として、前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有しているか否かを示す情報を受信する、
請求項２又は３に記載の情報処理装置。
【請求項５】
前記アプリ又は前記Ｗｅｂサービスは、前記利用者の端末装置を用いた電子決済を実現するアプリはＷｅｂサービスである、
請求項１に記載の情報処理装置。
【請求項６】
前記第１端末装置から、前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有していないことを示す情報を受信した場合、前記アプリ又は前記Ｗｅｂサービスにアクセスするためのアドレスが記載されたＳＭＳ（Short Message Service）通知を、前記記憶部に事前に記憶された前記識別情報に紐づく前記利用者の第２端末装置に通知する通知部を更に備える、
請求項１に記載の情報処理装置。
【請求項７】
前記認証部は、前記第２端末装置が前記アドレスを介して前記アプリ又は前記Ｗｅｂサービスへのアクセスを試みた際に、前記第２端末装置を一意に識別可能な第２識別情報を前記第２端末装置から受信して、前記第１識別情報と前記第２識別情報とが一致するか否かを判定し、前記第１識別情報と前記第２識別情報とが一致すると判定された場合、前記第１端末装置に前記アプリ又は前記Ｗｅｂサービスへのログインを許可する、
請求項６に記載の情報処理装置。
【請求項８】
前記第１端末装置から、前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有していることを示す情報を受信した場合、前記認証部は、前記第１端末装置と、前記記憶部に事前に記憶された前記識別情報に紐づく前記利用者の第２端末装置との間での情報授受を必要とする認証処理を実行する、
請求項１に記載の情報処理装置。
【請求項９】
前記認証部は、前記情報授受を必要とする認証処理として、認証情報がコード化されたコード情報を生成して、前記第２端末装置に送信し、前記第１端末装置が前記コード情報を撮影してデコードすることによって得られた前記認証情報を、前記第１端末装置から受信し、受信した前記認証情報と送信した前記認証情報とが一致する場合、前記第１端末装置に前記アプリ又は前記Ｗｅｂサービスへのログインを許可する、
請求項８に記載の情報処理装置。
【請求項１０】
前記認証部は、前記情報授受を必要とする認証処理として、認証情報を前記第２端末装置に送信し、前記利用者が前記第１端末装置に入力した前記認証情報を、前記第１端末装置から受信し、受信した前記認証情報と送信した前記認証情報とが一致する場合、前記第１端末装置に前記アプリ又は前記Ｗｅｂサービスへのログインを許可する、
請求項８に記載の情報処理装置。
【請求項１１】
前記認証部は、前記第１識別情報と前記第２識別情報とが一致しないと判定された場合、前記第１端末装置と、前記記憶部に事前に記憶された前記識別情報に紐づく前記利用者の第２端末装置との間での情報授受を必要とする認証処理を実行する、
請求項７に記載の情報処理装置。

【請求項１２】
コンピュータが、
利用者の第１端末装置から、前記第１端末装置を一意に識別可能な第１識別情報を少なくとも含む、アプリ又はＷｅｂサービスへのログイン要求を受信し、
受信した前記ログイン要求に含まれる前記第１識別情報と、記憶部に事前に記憶された、前記アプリ又は前記Ｗｅｂサービスに過去にログインした端末装置を一意に識別可能な識別情報とが一致しない場合、前記第１端末装置から、前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有しているか否かを示す情報を受信し、受信した前記情報に応じて、前記第１端末装置に対する前記アプリ又は前記Ｗｅｂサービスへのログイン認証方法を切り替える、
情報処理方法。
【請求項１３】
コンピュータに、
利用者の第１端末装置から、前記第１端末装置を一意に識別可能な第１識別情報を少なくとも含む、アプリ又はＷｅｂサービスへのログイン要求を受信させ、
受信した前記ログイン要求に含まれる前記第１識別情報と、記憶部に事前に記憶された、前記アプリ又は前記Ｗｅｂサービスに過去にログインした端末装置を一意に識別可能な識別情報とが一致しない場合、前記第１端末装置から、前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有しているか否かを示す情報を受信し、受信した前記情報に応じて、前記第１端末装置に対する前記アプリ又は前記Ｗｅｂサービスへのログイン認証方法を切り替えさせる、
プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報処理方法、およびプログラムに関する。
【背景技術】
【０００２】
従来、利用者が端末装置を用いてＷｅｂサービスやアプリケーションプログラムを利用する際に、当該利用者の本人認証を行う技術が知られている。例えば、特許文献１には、情報処理装置が予め端末識別情報を登録している場合には端末識別情報のみで本人認証を行い、端末識別情報を登録していない場合にはパスワード認証を行った後に端末識別情報を登録する技術が開示されている。
【先行技術文献】
【特許文献】
【０００３】
【文献】特表２０１９－５１７０８７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、従来技術では、利用者が端末装置の機種変更を行った際に、当該利用者にとって本人認証の利便性が低い場合があった。
【０００５】
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、利用者が端末装置の機種変更を行った際に、当該利用者にとって本人認証の利便性を向上させることができる情報処理装置、情報処理方法、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】
【０００６】
本発明の一態様は、利用者の第１端末装置から、前記第１端末装置を一意に識別可能な第１識別情報を少なくとも含む、アプリ又はＷｅｂサービスへのログイン要求を受信する

受信部と、受信した前記ログイン要求に含まれる前記第１識別情報と、記憶部に事前に記憶された、前記アプリ又は前記Ｗｅｂサービスに過去にログインした端末装置を一意に識別可能な識別情報とが一致しない場合、前記第１端末装置から、前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有しているか否かを示す情報を受信し、受信した前記情報に応じて、前記第１端末装置に対する前記アプリ又は前記Ｗｅｂサービスへのログイン認証方法を切り替える認証部と、を備える、情報処理装置である。

【発明の効果】

【０００７】

本発明の一態様によれば、利用者が端末装置の機種変更を行った際に、当該利用者にとって本人認証の利便性を向上させることができる。

【図面の簡単な説明】

【０００８】

【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】決済アプリ２０を用いた電子決済の大まかな流れを例示した図である。

【図３】決済サーバ１００の構成図である。

【図４】利用者情報１７２の内容の一例を示す図である。

【図５】ログイン認証処理の一例を示すフローチャートである。

【図６】利用者端末装置１０への問い合わせ処理の一例を示す図である。

【図７】ＳＭＳ認証処理の一例を示すフローチャートである。

【図８】ＱＲ認証処理の一例を示すシーケンス図である。

【図９】ＱＲコードが表示された第２利用者端末装置１０Ｂの表示画面の一例を示す図である。

【発明を実施するための形態】

【０００９】

以下、図面を参照し、本発明の情報処理装置、情報処理方法、およびプログラムについて説明する。情報処理装置は、一以上のプロセッサにより実現される。以下の説明では、情報処理装置は、電子決済サービスを提供するものとし、「決済サーバ」と称して説明するが、情報処理装置は、ショッピング、オークション、チャット、ミニブログ、その他の、ログインを伴う任意のサービスを提供するものであってもよい。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。

【００１０】

＜第１実施形態＞

［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、および一以上の店舗端末装置５０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。

【００１１】

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を含む。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。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、カメラ、通信装置、タッチパネルなどを制御する。

【００１２】

利用者端末装置１０では、さらに、ＣＰＵ等のプロセッサによりＷｅｂブラウザ３０が実行されることで、決済サーバ１００が提供するＷｅｂ決済サービスにアクセスするように動作する。決済アプリ２０による電子決済と、Ｗｅｂブラウザ３０による電子決済とは、後述するチャージ残高を共通に用いて実行することができる。

【００１３】

利用者端末装置１０では、さらに、例えば、デスクトップパソコンなどの非可搬型端末装置をも含む。非可搬型端末装置である利用者端末装置１０は、少なくとも、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。非可搬型端末装置である利用者端末装置１０は、光学読取機能を必ずしも有さないため（換言すると、決済アプリ２０を必ずしも実行可能とは限らないため）、少なくともＷｅｂブラウザ３０を含み、Ｗｅｂブラウザ３０を介した電子決済を少なくとも実行する。これら可搬型端末装置と非可搬型端末装置とを含む利用者端末装置１０は、「第１端末装置」および「第２端末装置」の一例である。

【００１４】

店舗端末装置５０は、例えば、店舗に設置される。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。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によって表示されてもよい。

【００１５】

決済サーバ１００は、利用者端末装置１０または店舗端末装置５０から受信した決済情報に基づいて、決済アプリ２０を用いた電子決済を実現する。決済サーバ１００は、例えば、利用者ＩＤに対応付けて管理しているチャージ残高を増減させる（換言すると、電子マネーを入出金する）ことで、電子決済を行う。電子決済は、リボ払いやクレジット払い等の方法によって、購買時点のチャージ残高よりも多額の購買を可能にするものが含まれてよい。

【００１６】

決済サーバ１００は、さらに、上述した通り、Ｗｅｂブラウザ３０を用いて利用可能なＷｅｂ決済サービスを提供する。Ｗｅｂ決済サービスにおいても、利用者ＩＤに対応付けて管理しているチャージ残高を増減させることで電子決済が行われ、さらに、Ｗｅｂ決済サービスにおける電子決済は、リボ払いやクレジット払い等の方法によって、購買時点のチャージ残高よりも多額の購買を可能にするものが含まれてよい。なお、本実施形態では、説明の簡潔性のため、決済アプリ２０を介した電子決済サービスを提供する決済サーバ１００と、Ｗｅｂブラウザ３０を介したＷｅｂ決済サービスを提供する決済サーバ１００とを共通のサーバとして説明しているが、これら２つのサービスを提供するサーバは別個のものであってもよい。

【００１７】

図２は、決済アプリ２０を用いた電子決済の大まかな流れを例示した図である。決済アプリ２０を用いた電子決済には、パターン１とパターン２の二つが存在してよい。パターン１の場合、まず利用者端末装置１０において決済アプリ２０が起動し、ＱＲコードやバーコード等のコード画像を表示する。利用者は利用者端末装置１０の表示面を店舗端末装置５０に翳す（提示する）。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、アカウントＩＤ等の情報を取得する。そして、店舗端末装置５０は、アカウントＩＤ、決済金額、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。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、ユーザの電子決済口座から店舗の電子決済口座に決済金額を移動させて決済処理を完了させる。

【００１８】

パターン２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。店舗コード画像６０には、店舗名等の情報が含まれている。利用者は、店舗名等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。そして、利用者端末装置１０は、アカウントＩＤ、決済金額、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。決済サーバ１００は、受信した情報に基づいて決済処理を行う。なお、上記のいずれかのパターンでのみ電子決済が行われてもよい。また、図２で説明する「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。

【００１９】

一方、Ｗｅｂブラウザ３０を介したＷｅｂ決済サービスの場合、例えば、利用者は、Ｗｅｂブラウザ３０を用いてオンラインショッピングサイトにアクセスして購入商品を選択した後に、Ｗｅｂ決済サービスにログインし、ログイン後に表示された支払い画面において支払い金額を入力することによって電子決済を実行する。決済サーバ１００は、入力された支払い金額に基づいて決済処理を行う。

【００２０】

［決済サーバ］

図３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、決済コンテンツ提供部１２０と、決済処理部１２２と、通知部１２４と、認証部１２６と、情報管理部１２８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インターフェースカードである。通信部１１０は、ネットワークＮＷを介して情報を送信する送信部としての機能と、ネットワークＮＷを介して情報を受信する受信部としての機能を備える。

【００２３】

決済コンテンツ提供部１２０は、例えば、Ｗｅｂサーバの機能を有し、決済アプリ２０を介した電子決済サービス、又はＷｅｂブラウザ３０を介したＷｅｂ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１２０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又はＷｅｂブラウザ３０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、前述した電子決済サービスの決済情報や、Ｗｅｂ決済サービスの決済情報などを決済サーバ１００に送信する。

【００２４】

決済処理部１２２は、利用者端末装置１０または店舗端末装置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１２２は、利用者情報１７２を参照しながら決済処理を行う。

【００２５】

［利用者情報］

図４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、デバイスＩＤ、チャージ残高、銀行口座、クレジットカード番号、チャージ履歴情報、および決済履歴情報などの情報が対応付けられたものである。電話番号、パスワード、デバイスＩＤ、チャージ残高、チャージ履歴情報、決済履歴情報以外の情報は任意設定情報である。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。電話番号は、電子決済サービスのログインＩＤとして使用されてもよい。

【００２６】

利用者ＩＤは、決済サーバ１００が利用者を識別するための利用者識別情報の一例であり、利用者のニックネームなど、利用者が任意に設定できる情報である。デバイスＩＤは、決済サーバ１００が利用者端末装置１０を識別するための情報である。デバイスＩＤは、例えば、利用者端末装置１０上で動作するＯＳ（Operating System）が、利用者端末装置１０を一意に識別可能に割り当てるＩＤ情報である。また、例えば、デバイスＩＤは、ＩＭＥＩ（International Mobile Equipment Identifier）、利用者端末装置１０の製造業者に関する情報、ＯＳのＩＤなどの情報を組み合わせて生成された情報であってよい。デバイスＩＤは、「第１識別情報」および「第２識別情報」の一例である。また、取得できるデバイスＩＤは利用者が利用する利用者端末装置１０のアプリによって異なる場合がある。例えば、決済アプリ２０を介して電子決済サービスを利用する場合と、Ｗｅｂブラウザ３０を介してＷｅｂ決済サービスを利用する場合とでは、決済サービスを提供する決済サーバ１００が取得するデバイスＩＤは、利用者端末装置１０が同じであっても異なる場合がある。後述する通り、本発明は、単一の利用者端末装置１０が決済サービスへのアクセス経路ごとに異なるデバイスＩＤを付与される場合であっても、利用者端末装置１０の認証を可能にするものである。

【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。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。

【００２８】

［フィッシングの手口］

利用者は、スマートフォンの機種変更を行った場合等、利用者によって使用される端末装置であるとして既に認証されている端末装置以外の端末装置を用いて電子決済サービスにログインしようとする場合がある。この場合、一般的に、利用者は、既存の端末装置又は新規の端末装置から認証情報を入力することで、当該新規の端末装置の認証処理が行われる。しかしながら、他人によって認証情報が不正に取得されてしまうと、他人の端末装置から電子決済サービスに不正ログインされてしまう可能性がある。このため、本実施形態は、他人（例えば、フィッシング犯）によって不正ログインが行われることを防止することを目的としている。そこで、本実施形態の処理の詳細を説明する前に、フィッシングの手口について説明する。

【００２９】

フィッシングとは、利用者のログインＩＤ、パスワード、および認証コード等の情報を、インターネットを介して取得するために行われる詐欺行為である。近年、フィッシングサイトの数が急増し、ログインＩＤ、パスワード、および認証コード等の情報を奪われる被害者が後を絶たない。本実施形態は、ログイン強度を高めることで、フィッシング犯のログイン試行自体を削減させるとともに、フィッシング犯に対してフィッシングサイトの立ち上げ意欲自体を失わせることを目的とする。

【００３０】

フィッシング犯は、以下の流れで利用者のログインＩＤ（電話番号など）およびパスワードを取得する。

（１）フィッシング犯は、利用者に対して偽のログインサイトにアクセスさせ、ログインＩＤおよびパスワードを入力させる。

（２）フィッシング犯は、入力されたログインＩＤおよびパスワードを利用して、フィッシング犯の端末装置から正規のログインサイトへのログインを試みる。このとき、利用者の端末装置以外からのアクセスであるため、不正アクセスを防止するべく、認証コードを記載したメッセージがＳＭＳ（Short Message Service）等で利用者の端末装置に送信される。

（３）フィッシング犯は、偽のログインサイトにおいてＳＭＳで通知された認証コードを入力させる画面を表示させる。

（４）フィッシング犯は、利用者によって偽のログインサイトに入力された認証コードを、フィッシング犯の端末装置を用いて正規のログインサイトに入力してログインを完了する。

【００３１】

上記のフィッシング犯の手口においては、利用者が偽のログインサイトにおいて認証コードを誤って入力し、フィッシング犯が、利用者端末装置１０とは異なる自身の端末装置と、窃取した認証コードとを用いてログインを完了してしまうことが問題である。そこで、本実施形態では、利用者端末装置１０が、決済アプリ２０又はＷｅｂ決済サービスのログイン画面にアクセスした際に決済サーバ１００に送信したデバイスＩＤと、ＳＭＳ（Short Message Service）通知に記載されたＵＲＬ（Uniform Resource Locator）をクリックした際に決済サーバ１００に送信したデバイスＩＤとを照合することによって、利用者端末装置１０の認証を行う。これにより、フィッシング犯の端末装置がログイン画面にアクセスした際に送信するデバイスＩＤと、利用者端末装置１０がＳＭＳ通知に記載されたＵＲＬをクリックした際に送信するデバイスＩＤとは異なることとなり、フィッシングを防ぐことができる。さらに、本実施形態の認証は、一台の端末装置のみを用いて実行可能なため、例えば、機種変更等によって、端末装置を新環境の一台のみしか保有していない利用者にとっての利便性を向上させることもできる。以下、本実施形態の詳細を説明する。

【００３２】

［ログイン認証処理］

図５は、ログイン認証処理の一例を示すフローチャートである。本フローチャートによる処理は、決済サーバ１００によって実行される。まず、決済サーバ１００の通信部１１０は、利用者端末装置１０から決済アプリ２０又はＷｅｂ決済サービスへのログイン要求を受信する（Ｓ１１）。ログイン要求には、ログインＩＤ（電話番号など）、パスワード、およびデバイスＩＤなどの情報が含まれている。以下、ログイン要求を送信した利用者端末装置１０を、「第１利用者端末装置１０Ａ」と称する。

【００３３】

次に、認証部１２６は、ログイン要求に含まれるログインＩＤ（電話番号など）およびパスワードと、利用者情報１７２とを比較して、ログイン認証が成功したか否かを判定する（Ｓ１２）。具体的に、認証部１２６は、ログイン要求に含まれるログインＩＤ（電話番号など）が利用者情報１７２に登録されており、ログイン要求に含まれるパスワードが、利用者情報１７２に含まれるパスワードと一致する場合には、ログイン認証が成功した

と判定する。一方、認証部１２６は、ログイン要求に含まれるログインＩＤ（電話番号など）が利用者情報１７２に登録されていない、またはログイン要求に含まれるパスワードが、利用者情報１７２に含まれるパスワードと一致しない場合には、ログイン認証が失敗したと判定する。

【００３４】

認証部１２６は、ログイン認証が失敗したと判定した場合、ログイン失敗通知を第１利用者端末装置１０Ａに送信し（Ｓ１３）、本フローチャートによる処理を終了する。

【００３５】

一方、認証部１２６は、ログイン認証が成功したと判定した場合、ログイン要求に含まれるデバイスＩＤと、利用者情報１７２とを比較して、新環境からのログインであるか否かを判定する（Ｓ１４）。ここで、新環境とは、利用者によって使用される端末装置であるとして認証されていない端末装置を意味する。また、既存環境とは、利用者によって使用される端末装置であるとして既に認証されている端末装置を意味する。

【００３６】

具体的に、認証部１２６は、ログイン要求に含まれるデバイスＩＤと、利用者情報１７２に含まれるデバイスＩＤとが一致しない場合には、新環境からのログインであると判定する。一方、認証部１２６は、ログイン要求に含まれるデバイスＩＤと、利用者情報１７２に含まれるデバイスＩＤとが一致する場合には、既存環境からのログインであると判定する。

【００３７】

認証部１２６は、新環境からのログインではないと判定した場合（すなわち、既存環境からのログインであると判定した場合）、ログイン成功通知を第１利用者端末装置１０Ａに送信し（Ｓ１５）、本フローチャートによる処理を終了する。

【００３８】

一方、認証部１２６が新環境からのログインであると判定した場合、認証部１２６は、第１利用者端末装置１０Ａに、決済アプリ２０又はＷｅｂ決済サービスを利用する利用端末の台数が１台のみであるか否かを問い合わせる（Ｓ１６）。ステップＳ１６において、決済アプリ２０又はＷｅｂ決済サービスを利用する利用端末の台数が１台のみであるとする情報を第１利用者端末装置１０Ａから受信した場合、認証部１２６は、後述するＳＭＳ認証処理を実行する（Ｓ１７）。一方、ステップＳ１６において、決済アプリ２０又はＷｅｂ決済サービスを利用する利用端末の台数が１台のみではないと判定された場合、認証部１２６は、後述するＱＲ認証処理を実行する（Ｓ１８）。これにより、本フローチャートの処理が終了する。

【００３９】

なお、上記のステップＳ１６において、認証部１２６は、第１利用者端末装置１０Ａに、決済アプリ２０又はＷｅｂ決済サービスを利用する利用端末の台数が１台のみであるか否かを問い合わせている。これは、利用者が電子決済サービスの利用登録（利用者情報１７２）に紐づけている電話番号の端末を保有しているか確認するための処理である（すなわち、１台のみである場合、これは利用者が、利用登録に紐づけている電話番号の端末を保有していないことを意味する）。そのため、より直接的に、認証部１２６は、電子決済サービスを過去に利用した古い端末が利用者の手元にあるか否かを問い合わせてもよい。

【００４０】

図６は、第１利用者端末装置１０Ａへの問い合わせ処理の一例を示す図である。図６に示す通り、認証部１２６は、新環境からのログインであると判定した場合、例えば、第１利用者端末装置１０Ａに、利用端末の台数が一台のみであるか否かを選択するための問い合わせ画面を送信する。図６において、ボタンＢ１は、利用端末の台数が一台のみであることを選択するためのボタンを表し、ボタンＢ２は、利用端末の台数が複数台存在することを選択するためのボタンを表す。第１利用者端末装置１０Ａは、例えば、利用者が、第１利用者端末装置１０Ａ上でボタンＢ１をクリックすることによって、利用端末の台数が一台のみであることを示す情報を決済サーバ１００に送信する一方、利用者が、第１利用

者端末装置１０Ａ上でボタンＢ２をクリックすることによって、利用端末の台数が複数台存在することを示す情報を決済サーバ１００に送信する。これにより、認証部１２６は、図５のフローチャートのステップＳ１６において、利用端末の台数が一台のみであるか否かを判定することができる。

【００４１】

［ＳＭＳ認証処理］

図７は、ＳＭＳ認証処理の一例を示すフローチャートである。本フローチャートによる処理は、図５のフローチャートのステップＳ１６において利用端末の台数が一台のみであると判定された場合に決済サーバ１００によって実行される。

【００４２】

まず、認証部１２６は、図５のフローチャートのステップＳ１１において受信したログイン要求が決済アプリ２０を介して受信したものであるか、Ｗｅｂブラウザ３０を介して受信したものであるかを判定する（Ｓ２１）。受信したログイン要求が決済アプリ２０を介して受信したものであると判定された場合、通知部１２４は、決済アプリ２０にアクセスするためのＵＲＬ、すなわち決済アプリ２０を介して決済サーバにアクセスまたは情報送信するためのＵＲＬが記載されたＳＭＳ通知を、利用者情報１７２に登録された電話番号に紐づく利用者端末装置１０に送信する（Ｓ２２）。一方、受信したログイン要求が、Ｗｅｂブラウザ３０を介して受信したものであると判定された場合、通知部１２４は、Ｗｅｂ決済サービスにアクセスするためのＵＲＬ、すなわちＷｅｂブラウザを介して決済サーバにアクセスまたは情報送信するためのＵＲＬが記載されたＳＭＳ通知を、利用者情報１７２に登録された電話番号に紐づく利用者端末装置１０に送信する（Ｓ２３）。以下、利用者情報１７２に登録された電話番号に紐づく利用者端末装置１０を「第２利用者端末装置１０Ｂ」と称する。このような構成とすることで、利用者がステップＳ１１においてログイン要求を送信した際のアプリと同じアプリで決済サービスにアクセスさせることができる。換言すると、単一の利用者端末装置１０が決済サービスへのアクセス経路ごとに異なるデバイスＩＤを付与される場合であっても、利用者端末装置１０の認証を可能にすることができる。

【００４３】

次に、認証部１２６は、利用者が、第２利用者端末装置１０Ｂに送信されたＳＭＳ通知に記載されたＵＲＬをクリックすると、当該クリックに応じて、第２利用者端末装置１０Ｂからデバイスを受信する（Ｓ２４）。次に、認証部１２６は、第１利用者端末装置１０Ａのデバイスと第２利用者端末装置１０Ｂのデバイスが一致するか否かを判定する（Ｓ２５）。第１利用者端末装置１０Ａのデバイスと第２利用者端末装置１０Ｂのデバイスが一致すると判定された場合、認証部１２６は、第１利用者端末装置１０Ａに、決済アプリ２０又はＷｅｂ決済サービスへのログインを許可する（Ｓ２６）。次に、情報管理部１２８は、利用者情報１７２の更新処理を行う（Ｓ２７）。具体的に、情報管理部１２８は、第１利用者端末装置１０Ａから送信されたログイン要求に含まれるデバイスＩＤ（すなわち、第１利用者端末装置１０Ａのデバイス）を、ログイン要求に含まれるログインＩＤ（電話番号など）に関連付けて利用者情報１７２に書き込む。一方、第１利用者端末装置１０Ａのデバイスと第２利用者端末装置１０Ｂのデバイスが一致しないと判定された場合、認証部１２６は、後述するＱＲ認証処理を実行する（Ｓ２７）。これにより、本フローチャートの処理が終了する。

【００４４】

なお、ステップＳ２５において、認証部１２６は、ログイン要求時に取得されるデバイスＩＤと、ＳＭＳ通知に記載されたＵＲＬをクリックした際に取得されるデバイスＩＤとが一致しているか否かを判定している。このとき、認証部１２６は、ログイン要求時には決済アプリ２０からデバイスＩＤを受信する一方、ＳＭＳ通知に記載されたＵＲＬのクリック時には、Ｗｅｂブラウザ３０からデバイスＩＤを受信することがあり得る。これは、換言すると、第１利用者端末装置１０Ａには決済アプリ２０がインストールされている一方、第２利用者端末装置１０Ｂには決済アプリ２０がインストールされておらず、ＵＲＬ

のクリックに応じてＷｅｂブラウザ３０が立ち上がったことを意味する。すなわち、これは第１利用者端末装置１０Ａと第２利用者端末装置１０Ｂとが異なることを意味するため、認証部１２６は、このとき、デバイスＩＤを照合することなく、第１利用者端末装置１０Ａと第２利用者端末装置１０ＢとのＱＲ認証処理に移行しても良い。

【００４５】

［ＱＲ認証処理］

図８は、ＱＲ認証処理の一例を示すシーケンス図である。図８に示すシーケンス図の処理は、図５のフローチャートのステップＳ１６において利用者端末装置が複数台存在すると判定されたか、又は、図７のフローチャートのステップＳ２５においてデバイスＩＤが一致しないと判定された場合に実行されるものである。

【００４６】

まず、決済サーバ１００の通信部１１０は、第２利用者端末装置１０ＢにＳＭＳ通知を送信する（Ｓ３１）。ＳＭＳ通知は、利用者の電話番号を利用したショートメッセージによる通知である。ＳＭＳ通知には、決済アプリ２０又はＷｅｂ決済サービスにアクセスするためのＵＲＬ（Uniform Resource Locator）が含まれている。代替的に、決済サーバ１００の通信部１１０は、第２利用者端末装置１０Ｂの決済アプリ２０に、当該ＵＲＬが記載されたプッシュ通知を送信してもよい。

【００４７】

第２利用者端末装置１０Ｂは、決済サーバ１００からＳＭＳ通知を受信すると、利用者がＳＭＳ通知に記載されたＵＲＬをクリックしたことを示す情報を決済サーバ１００に送信する（Ｓ３２）。次に、決済サーバ１００の認証部１２６は、認証情報がコード化されたＱＲコードを生成する（Ｓ３３）。例えば、認証情報は、ワンタイムパスワード等の時限的な情報であってよい。また、認証部１２６は、生成されたＱＲコードを通信部１１０から第２利用者端末装置１０Ｂに送信する（Ｓ３４）。第２利用者端末装置１０Ｂは、決済サーバ１００からＱＲコードを受信すると、決済アプリ２０の画面にＱＲコードを表示する（Ｓ３５）。

【００４８】

図９は、ＱＲコードが表示された第２利用者端末装置１０Ｂの表示画面の一例を示す図である。図９に示されるように、第２利用者端末装置１０Ｂの表示画面には、ＱＲコードＣと、「新しい端末でＱＲコードを読み取ってください」というメッセージ等が表示される。

【００４９】

次に、新環境である第１利用者端末装置１０Ａは、第２利用者端末装置１０Ｂに表示されたＱＲコードを撮影する（Ｓ３６）。具体的に、利用者は、第１利用者端末装置１０Ａのカメラを用いて、第２利用者端末装置１０Ｂに表示されたＱＲコードを撮影する。

【００５０】

また、第１利用者端末装置１０Ａは、撮影したＱＲコードをデコードすることにより、認証情報を取得する（Ｓ３７）。そして、第１利用者端末装置１０Ａは、取得した認証情報を決済サーバ１００に送信する（Ｓ３８）。

【００５１】

決済サーバ１００の通信部１１０が第１利用者端末装置１０Ａから認証情報を受信すると、決済サーバ１００の認証部１２６は、認証情報の照合処理を行う（Ｓ３９）。具体的に、認証部１２６は、第２利用者端末装置１０Ｂに送信したＱＲコードに含まれる認証情報と、第１利用者端末装置１０Ａから受信した認証情報とが一致するか否かを判定する。認証部１２６は、第２利用者端末装置１０Ｂに送信したＱＲコードに含まれる認証情報と、第１利用者端末装置１０Ａから受信した認証情報とが一致しない場合、ログイン不許可通知を通信部１１０から第１利用者端末装置１０Ａに送信する。

【００５２】

一方、認証部１２６は、第２利用者端末装置１０Ｂに送信したＱＲコードに含まれる認証情報と、第１利用者端末装置１０Ａから受信した認証情報とが一致する場合、ログイン

許可通知を通信部１１０から第１利用者端末装置１０Ａに送信する（Ｓ１１０）。これによって、新環境である第１利用者端末装置１０Ａからのログインが許可されることとなる。

【００５３】

その後、情報管理部１２８は、利用者情報１７２の更新処理を行う（Ｓ１１１）。具体的に、情報管理部１２８は、第１利用者端末装置１０Ａから送信されたログイン要求に含まれるデバイスＩＤ（すなわち、第１利用者端末装置１０Ａのデバイスｉｄ）を、ログイン要求に含まれるログインＩＤ（電話番号など）に関連付けて利用者情報１７２に書き込む。これにより、本フローチャートの処理が終了する。

【００５４】

なお、本実施形態において、利用端末の台数が複数台存在する場合や、ＳＭＳ認証に失敗した場合、認証部１２６はＱＲ認証処理を実行している。しかし、本発明はそのような構成に限定されず、利用端末の台数が複数台存在する場合や、ＳＭＳ認証に失敗した場合、認証コード（例えば、４桁ＰＩＮコード）を記載したＳＭＳ通知を第２利用者端末装置１０Ｂに送信し、利用者は、第１利用者端末装置１０Ａ上で当該認証コードを入力して決済サーバ１００に送信することによって、認証を行ってもよい。これにより、第１利用者端末装置１０Ａがカメラ撮影機能を有しない場合であっても、認証処理を実行することができる。ＱＲ認証処理が失敗した場合に、上述の認証コードでの認証処理を実行しても良い。例えば、図９のＱＲコードが表示された画面に、ＱＲコードを別の端末で読み取れない場合の遷移ボタンを表示し、認証コードを表示する構成にしても良い。

【００５５】

さらに、図５のステップＳ１４において新環境からのログインであると判定された場合には、決済サーバ１００は、ステップＳ１６の処理を省略してそのままステップＳ１８に進み、図８のシーケンス図の処理に移行しても良い。その場合、図８のシーケンス図のステップＳ３２にて、決済サーバ１００の認証部１２６は、第２利用者端末装置１０Ｂのデバイスｉｄを取得し、図５のステップＳ１１にて取得したデバイスＩＤと照合する。認証部１２６は、これら２つのデバイスＩＤが一致する場合、第１利用者端末装置１０Ａからのログインを許可しても良い。このような構成により、利用者がステップＳ１６の問い合わせに対応する手間を省くことができる。

【００５６】

以上説明した本実施形態によれば、機種変更等によって、利用者が端末装置を新環境の一台のみしか保有していない場合であっても、ログイン要求時に取得されるデバイスＩＤと、ＳＭＳ通知に記載されたＵＲＬをクリックした際に取得されるデバイスＩＤとが一致する場合には、当該利用者の本人認証を完了させる。これにより、利用者が端末装置の機種変更を行った際に、当該利用者にとって本人認証の利便性を向上させることができる。

【００５７】

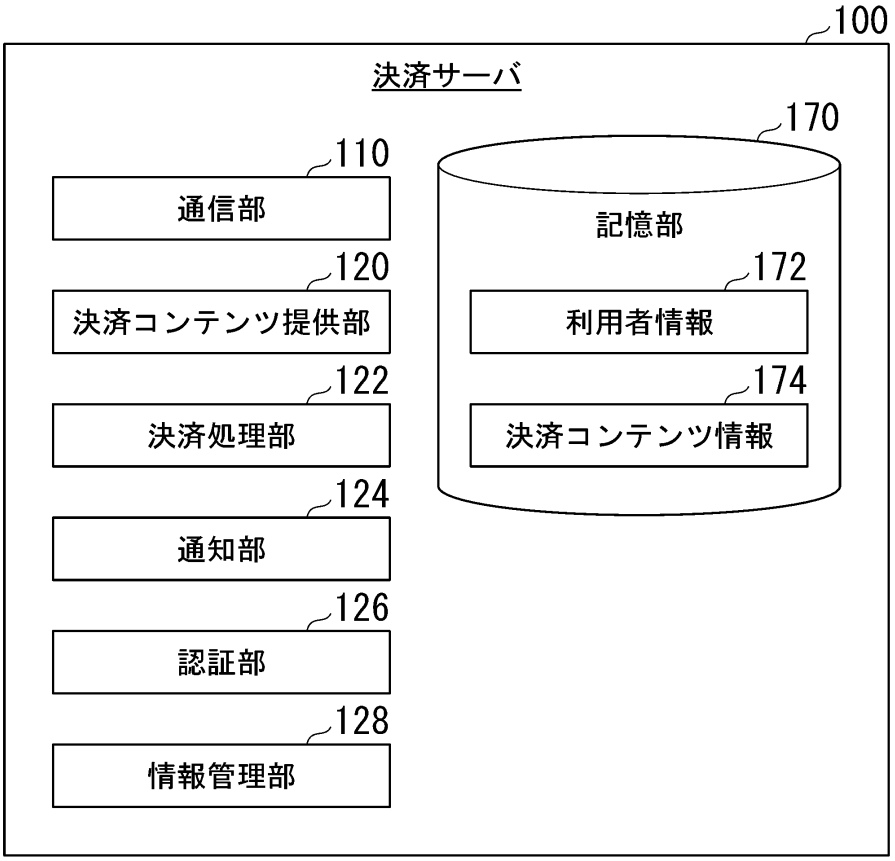
以上、本発明を実施するための形態について実施形態を用いて説明したが、本発明はこうした実施形態に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々の変形及び置換を加えることができる。

【符号の説明】

【００５８】

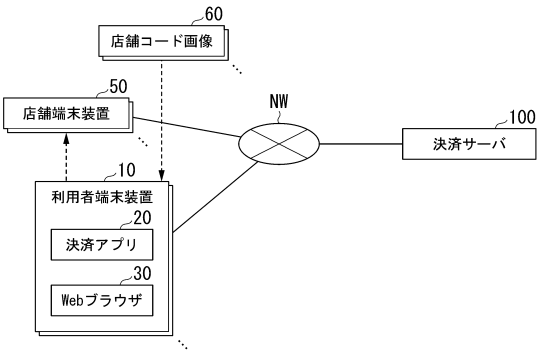
１０　利用者端末装置
２０　決済アプリ
３０　Ｗｅｂブラウザ
５０　店舗端末装置
６０　店舗コード画像
１００　決済サーバ
１１０　通信部
１２０　決済コンテンツ提供部
１２２　決済処理部
１２４　通知部

１２６　認証部
１２８　情報管理部
１７０　記憶部
【要約】
【課題】利用者が端末装置の機種変更を行った際に、当該利用者にとって本人認証の利便性を向上させること。
【解決手段】利用者の第１端末装置から、前記第１端末装置を一意に識別可能な第１識別情報を少なくとも含む、アプリ又はＷｅｂサービスへのログイン要求を受信する受信部と、受信した前記ログイン要求に含まれる前記第１識別情報と、記憶部に事前に記憶された、前記アプリ又は前記Ｗｅｂサービスに過去にログインした端末装置を一意に識別可能な識別情報とが一致しない場合、前記第１端末装置から、前記アプリ又は前記Ｗｅｂサービスの利用登録に過去に紐づけた電話番号の端末装置を保有しているか否かを示す情報を受信し、受信した前記情報に応じて、前記第１端末装置に対する前記アプリ又は前記Ｗｅｂサービスへのログイン認証方法を切り替える認証部と、を備える、情報処理装置。
【選択図】図３

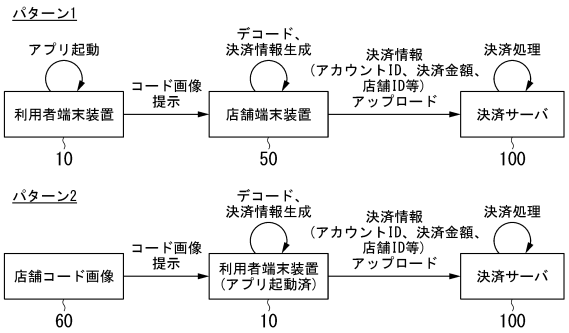


【図面】

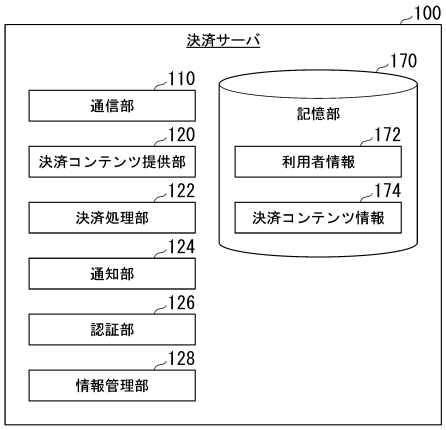
【図１】


60
店舗コード画像
50
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
30
Webブラウザ

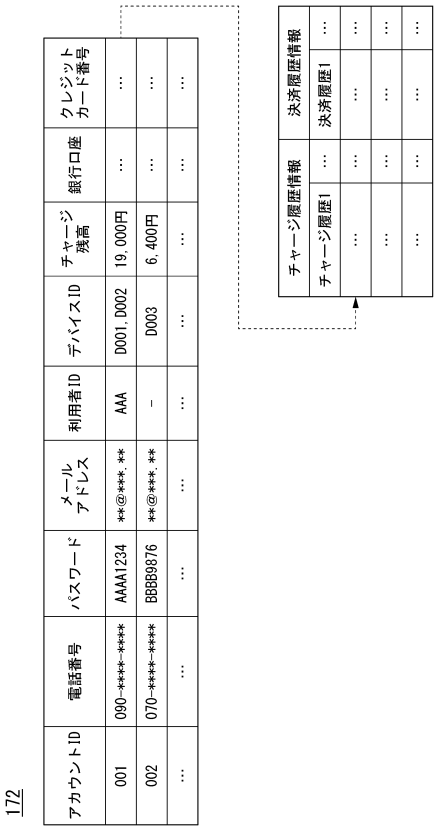
【図２】


パターン1
アプリ起動
利用者端末装置
10
コード画像
提示
デコード、
決済情報生成
店舗端末装置
50
決済情報
（アカウントID、決済金額、
店舗ID等）
アップロード
決済サーバ
100
決済処理
パターン2
店舗コード画像
60
コード画像
提示
デコード、
決済情報生成
利用者端末装置
（アプリ起動済）
10
決済情報
（アカウントID、決済金額、
店舗ID等）
アップロード
決済サーバ
100
決済処理

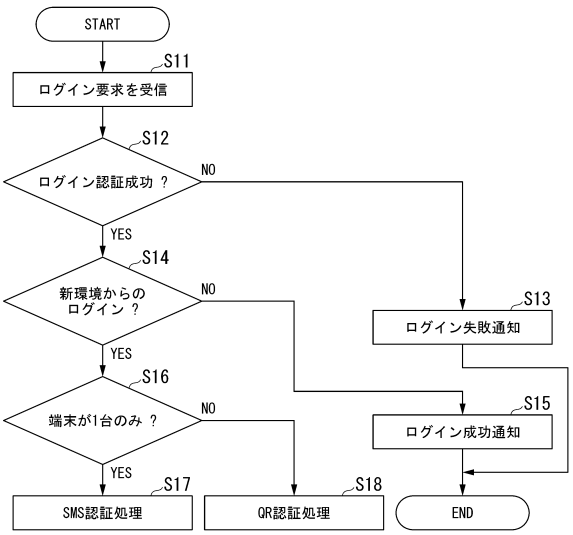
【図３】


100
決済サーバ
110
通信部
120
決済コンテンツ提供部
122
決済処理部
124
通知部
126
認証部
128
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

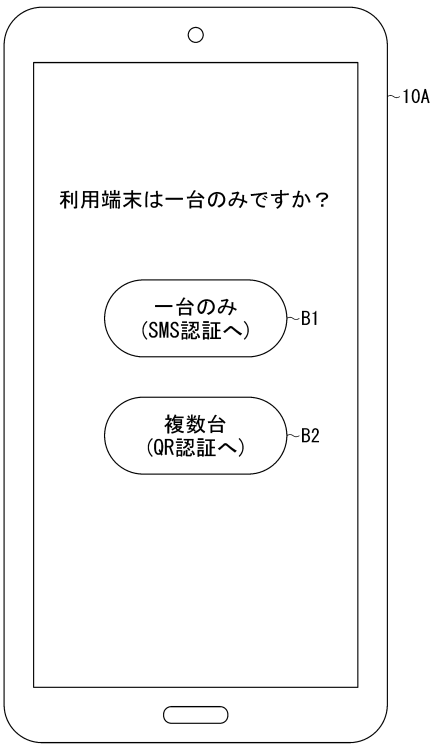
【図４】


172
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
デバイスID
チャージ残高
銀行口座
クレジットカード番号
001
090-****-****
AAAA1234
@*.**
AAA
D001, D002
19,000円
002
070-****-****
BBBB9876
@*.**
–
D003
6,400円
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

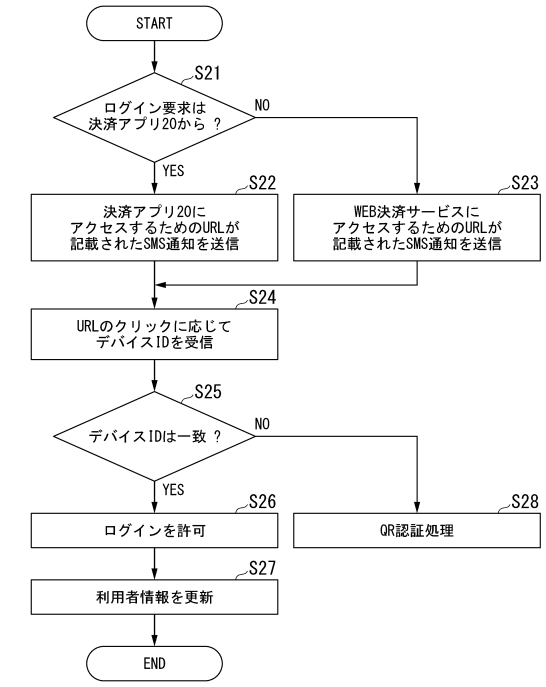
【図５】


START
S11
ログイン要求を受信
S12
ログイン認証成功 ？
NO
YES
S14
新環境からの
ログイン ？
NO
YES
S16
端末が1台のみ ？
NO
YES
S13
ログイン失敗通知
S15
ログイン成功通知
S17
SMS認証処理
S18
QR認証処理
END

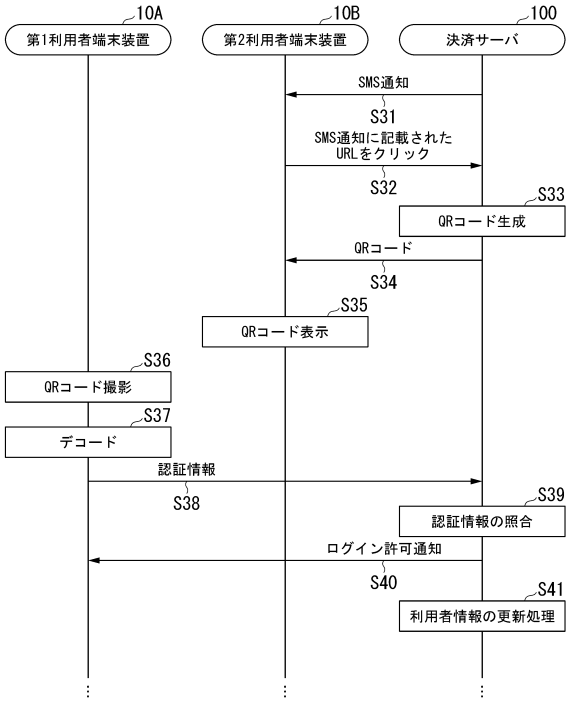
【図６】


10A
利用端末は一台のみですか？
一台のみ
(SMS認証へ)
B1
複数台
(QR認証へ)
B2

【図７】


START
S21
ログイン要求は
決済アプリ20から ？
NO
YES
S22
決済アプリ20に
アクセスするためのURLが
記載されたSMS通知を送信
S23
WEB決済サービスに
アクセスするためのURLが
記載されたSMS通知を送信
S24
URLのクリックに応じて
デバイスIDを受信
S25
デバイスIDは一致 ？
NO
YES
S26
ログインを許可
S28
QR認証処理
S27
利用者情報を更新
END

【図８】


10A
第1利用者端末装置
10B
第2利用者端末装置
100
決済サーバ
SMS通知
S31
SMS通知に記載された
URLをクリック
S32
S33
QRコード生成
QRコード
S34
S35
QRコード表示
S36
QRコード撮影
S37
デコード
認証情報
S38
S39
認証情報の照合
ログイン許可通知
S40
S41
利用者情報の更新処理

【図９】


10B
C
新しい端末でQRコードを
読み取ってください
ログインを完了するには
QRコードによる認証が必要です

フロントページの続き

(56)参考文献 特許第７０７２１１１（ＪＰ，Ｂ１）
国際公開第２０１６／１４３０２７（WO，Ａ１）
米国特許第７５２３０６７（ＵＳ，Ｂ１）
特開２０２１－１１１１０６（ＪＰ，Ａ）
特開２０１８－１２１０９９（ＪＰ，Ａ）
Ｐａｒｔ＿２ ＬＩＮＥ ＨＯＷ ＴＯ これさえ読めば使い方はバッチリ！！ ＬＩＮＥの使い方＆設定方法，５０００万人のためのＬＩＮＥ便利帳，日本，株式会社▲▼出版社，2014年03月10日，第１６頁－第５５頁

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／４５
Ｇ０６Ｆ ２１／３１