(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)公開番号
特開2025-68954
(P2025-68954A)
(43)公開日　令和7年4月30日(2025.4.30)

(51)国際特許分類　FI
G06F 21/31 (2013.01)　G06F 21/31

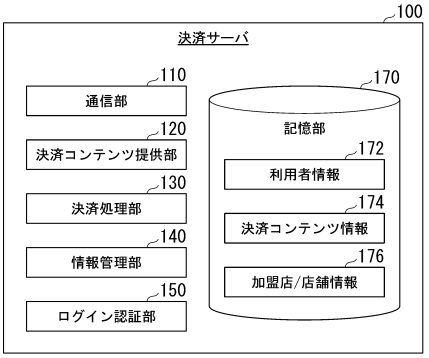
審査請求　有　請求項の数　10　OL　（全16頁）

(21)出願番号　特願2023-179090(P2023-179090)
(22)出願日　令和5年10月17日(2023.10.17)
(11)特許番号　特許第7403705号(P7403705)
(45)特許公報発行日　令和5年12月22日(2023.12.22)

(71)出願人　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　亀山 直起
東京都千代田区紀尾井町１番３号 ＰａｙＰａｙ株式会社内

(54)【発明の名称】　認証装置、認証方法、およびプログラム

(57)【要約】
【課題】規定の認証手段に対する追加の認証手段として提供されるワンタイムパスワードのセキュリティを向上させること。
【解決手段】利用者の端末装置で動作する第１アプリの要求に応じて利用者を認証するための処理を実行する認証装置であって、第１アプリの識別情報であって、前記要求の際に第１アプリから受信される第１識別情報と、前記要求の際に前記端末装置に通知されるアドレスにアクセスした第２アプリの識別情報である第２識別情報とが一致する場合に利用者を認証する認証部を備え、前記アドレスは、第１アプリを前記アドレスへのアクセス主体として指定する態様で記載されたものであり、認証部は、第１識別情報と第２識別情報が一致しない場合、前記アドレスを表示させるための表示情報を第２アプリに供給し、その供給後に前記アドレスにアクセスしたアプリの識別情報である第３識別情報が第１識別情報と一致する場合に利用者を認証する、認証装置。
【選択図】図４



【特許請求の範囲】
【請求項１】
利用者の端末装置で動作する第１アプリケーションプログラムの要求に応じて前記利用者を認証するための認証処理を実行する認証装置であって、
前記第１アプリケーションプログラムの識別情報であって、前記要求の際に前記第１アプリケーションプログラムから受信される第１識別情報と、前記要求の際に前記端末装置に通知される所定のネットワークアドレスにアクセスした第２アプリケーションプログラムの識別情報である第２識別情報とが一致する場合に前記利用者を認証する認証部を備え、
前記ネットワークアドレスは、前記第１アプリケーションプログラムを前記ネットワークアドレスへのアクセス主体として指定する態様で記載されたものであり、
前記認証部は、前記第１識別情報と前記第２識別情報が一致しない場合、前記ネットワークアドレスを表示させるための表示情報を前記第２アプリケーションプログラムに供給し、前記表示情報の供給後に前記ネットワークアドレスにアクセスしたアプリケーションプログラムの識別情報である第３識別情報が前記第１識別情報と一致する場合に前記利用者を認証する、
認証装置。
【請求項２】
前記認証部は、前記第３識別情報が前記第１識別情報と一致しない場合、パスワードによる認証手段を提供するものであり、前記パスワードによる認証手段が使用された場合、前記利用者について登録されている連絡先、または前記認証装置の管理者に通知する、
請求項１に記載の認証装置。
【請求項３】
前記認証部は、前記要求の際、前記ネットワークアドレスをＳＭＳ（Short Message Service）によって前記端末装置に通知する、
請求項１に記載の認証装置。
【請求項４】
前記ＳＭＳで通知された前記ネットワークアドレスがタップ操作によって選択された場合、前記第１アプリケーションプログラムが前記ネットワークアドレスにアクセスし、前記ネットワークアドレスが長押し操作によって選択された場合、前記第２アプリケーションプログラムが前記ネットワークアドレスにアクセスする、
請求項３に記載の認証装置。
【請求項５】
前記第２アプリケーションプログラムはウェブブラウザであり、
前記ウェブブラウザが有する前記第２識別情報は前記第１識別情報と異なる識別情報である、
請求項４に記載の認証装置。
【請求項６】
前記第１アプリケーションプログラムは決済管理装置と協働して前記利用者に電子決済サービスを提供するものであり、
前記第１アプリケーションプログラムは、前記電子決済サービスにログインする利用者の認証を前記決済管理装置に要求し、前記認証に成功した利用者に対して前記電子決済サービスを提供する、
請求項１に記載の認証装置。
【請求項７】
前記認証部は、前記第３識別情報が前記第１識別情報と一致しない場合、パスワードによる認証手段を提供するものであり、前記パスワードによる認証手段が使用された場合、前記利用者について、前記電子決済サービスが提供する機能の一部を制限する、
請求項６に記載の認証装置。
【請求項８】

前記表示情報は、第１の認証手段として認証用のＱＲコードを表示するとともに、第２の認証手段として前記ネットワークアドレスにアクセスさせるためのリンクを表示する、
請求項１に記載の認証装置。
【請求項９】
利用者の端末装置で動作する第１アプリケーションプログラムの要求に応じて前記利用者を認証するための認証処理を実行する認証装置が、
前記第１アプリケーションプログラムの識別情報であって、前記要求の際に前記第１アプリケーションプログラムから受信される第１識別情報と、前記要求の際に前記端末装置に通知される所定のネットワークアドレスにアクセスした第２アプリケーションプログラムの識別情報である第２識別情報とが一致する場合に前記利用者を認証する認証方法であって、
前記ネットワークアドレスは、前記第１アプリケーションプログラムを前記ネットワークアドレスへのアクセス主体として指定する態様で記載されたものであり、
前記認証装置は、前記第１識別情報と前記第２識別情報が一致しない場合、前記ネットワークアドレスを表示させるための表示情報を前記第２アプリケーションプログラムに供給し、前記表示情報の供給後に前記ネットワークアドレスにアクセスしたアプリケーションプログラムの識別情報である第３識別情報が前記第１識別情報と一致する場合に前記利用者を認証する、
認証方法。
【請求項１０】
利用者の端末装置で動作する第１アプリケーションプログラムの要求に応じて前記利用者を認証するための認証処理を実行する認証装置に、
前記第１アプリケーションプログラムの識別情報であって、前記要求の際に前記第１アプリケーションプログラムから受信される第１識別情報と、前記要求の際に前記端末装置に通知される所定のネットワークアドレスにアクセスした第２アプリケーションプログラムの識別情報である第２識別情報とが一致する場合に前記利用者を認証する認証処理を実行させるためのプログラムであって、
前記ネットワークアドレスは、前記第１アプリケーションプログラムを前記ネットワークアドレスへのアクセス主体として指定する態様で記載されたものであり、
前記第１識別情報と前記第２識別情報が一致しない場合、前記認証装置に、
前記ネットワークアドレスを表示させるための表示情報を前記第２アプリケーションプログラムに供給させ、
前記表示情報の供給後に前記ネットワークアドレスにアクセスしたアプリケーションプログラムの識別情報である第３識別情報が前記第１識別情報と一致する場合に前記利用者を認証させる、
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、認証装置、認証方法、およびプログラムに関する。
【背景技術】
【０００２】
従来、サービスにログインするユーザの認証において、規定の認証手段に加え、ログイン要求元の端末装置が登録済みの端末装置であるか否かを確認し、ログイン要求元の端末装置が登録済みの端末装置でない場合、ＱＲコード（登録商標、以下同様）やＳＭＳ（Short Message Service）などを利用した追加の認証を実施する場合があった（例えば特許文献１、２参照）。
【先行技術文献】
【特許文献】
【０００３】

【特許文献１】特許第７２４７４１６号公報
【特許文献２】特許第７２０２５００号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
従来の技術では、追加の認証方法の一例としてワンタイムパスワードによる認証が挙げられるが、この場合、フィッシングなどの手口によりワンタイムパスワードを不正に取得したユーザが正当なユーザのアカウントが悪用される可能性があった。
【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、規定の認証手段に対する追加の認証手段として提供されるワンタイムパスワードのセキュリティを向上させることができる認証装置、認証方法、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、利用者の端末装置で動作する第１アプリケーションプログラムの要求に応じて前記利用者を認証するための認証処理を実行する認証装置であって、前記第１アプリケーションプログラムの識別情報であって、前記要求の際に前記第１アプリケーションプログラムから受信される第１識別情報と、前記要求の際に前記端末装置に通知される所定のネットワークアドレスにアクセスした第２アプリケーションプログラムの識別情報である第２識別情報とが一致する場合に前記利用者を認証する認証部を備え、前記ネットワークアドレスは、前記第１アプリケーションプログラムを前記ネットワークアドレスへのアクセス主体として指定する態様で記載されたものであり、前記認証部は、前記第１識別情報と前記第２識別情報が一致しない場合、前記ネットワークアドレスを表示させるための表示情報を前記第２アプリケーションプログラムに供給し、前記表示情報の供給後に前記ネットワークアドレスにアクセスしたアプリケーションプログラムの識別情報である第３識別情報が前記第１識別情報と一致する場合に前記利用者を認証する、認証装置である。
【発明の効果】
【０００７】
本発明の一態様によれば、規定の認証手段に対する追加の認証手段として提供されるワンタイムパスワードのセキュリティを向上させることができる認証装置、認証方法、およびプログラムを提供することができる。
【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】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】電子決済サービスにおけるログイン認証の流れの概略を示すフローチャートである。
【図８】新たな第３デバイス認証に係る処理の流れの一例を示すシーケンスチャート（その１）である。
【図９】新たな第３デバイス認証に係る処理の流れの一例を示すシーケンスチャート（その２）である。
【図１０】引継ぎ用ＵＲＬが記載されたウェブページ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、本発明の認証装置、認証方法、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。アプリケーションプログラムと決済サーバは、協働して電子決済サービスを提供する。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。

【００１０】

［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。

【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。

【００１２】

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。

【００１３】

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。

【００１４】
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。
【００１５】
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。
【００１６】
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ＩＤ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。
【００１７】
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）。
【００１８】
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。

【００１９】

［決済サーバ］

図４は、第１実施形態に係る決済サーバ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１３０と、情報管理部１４０と、ログイン認証部１５０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。

【００２０】

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、加盟店／店舗情報１７６などの情報が格納される。

【００２１】

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。

【００２２】

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、電子決済サービスの各種機能を提供する画面を表示するための情報（決済コンテンツ）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。

【００２３】

決済処理部１３０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１３０は、利用者情報１７２を参照しながら決済処理を行う。

【００２４】

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、利用者ＵＲＬ、アカウントＩＤ、電話番号、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、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、チャージ履歴情報、決済履歴情報、ログイン状態情報、登録済み端末情報などの情報が対応付けられたものである。利用者ＵＲＬは、利用者間の送金処理に使用される。電子決済サービスへの新規登録時には、電話番号およびパスワードの登録が必須となる。アカウントＩＤは、決済サーバ１００によって利用者に発行されるものであり、利用者ＩＤは、利用者が任意に設定できる（設定しなくてもよい）ＩＤである。メールアドレス、および氏名・住所・生年月日も同様に、利用者が任意に設定できる（設定しなくてもよい）情報である。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。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。
【００２５】
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。後払い設定は、後払いによる電子決済を可能とするための設定が済んでいるか否かを示す情報であり、「済」と「未」のいずれかに設定される。後払い枠は月ごとに利用可能な後払いの限度額であり、後払い利用額は、当月に既に利用された後払いの金額であり、後払い利用可能額は、後払い枠から後払い利用額を差し引いて求められる、当月に利用可能な後払いの金額である。図では後払い枠を一つだけ示しているが、実際には更に日ごとの上限額などが存在し、それらの低い方が後払い枠に設定されてよい。後払いの更なる詳細については後述する。決済方法設定は、その時点において利用者がチャージ残高による電子決済を行うのか、後払いによる決済を行うのかを示す設定情報である。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、決済方法など）を、決済ごとに示す情報である。
【００２６】
ログイン状態情報は、電子決済サービスにおける各利用者のログイン状態を表す情報である。例えば、ログイン状態情報には、電子決済サービスにおいて利用者がログイン中の状態であるか、またはログアウトした状態であるかの情報が含まれる。また、ログイン状態情報には、利用者が電子決済サービスにログインした日時や、ログアウトした日時などの情報が含まれてもよい。登録済み端末情報は、後述する「登録済み端末」の識別情報である。登録済み端末情報は、利用者が決済サーバ１００に予め登録しておくものである。
【００２７】
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に対して店舗名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。
【００２８】
情報管理部１４０は、利用者端末装置１０や第２店舗端末装置７０から取得した情報に基づいて、利用者情報１７２および加盟店／店舗情報１７６を管理する。情報管理部１４０は、利用者情報１７２および加盟店／店舗情報１７６について新規レコードの追加、編集、削除などを行う。
【００２９】
ログイン認証部１５０は、決済アプリ２０からの要求に応じて、電子決済サービスにログインしようとしている利用者について認証処理を行う。ログイン認証部１５０は、認証結果に応じて利用者のログイン状態を更新する。
【００３０】
［電子決済］
決済処理部１３０は、利用者端末装置１０または第１店舗端末装置５０から決済情報が取得されると、利用者情報１７２を参照して当該利用者の「決済方法設定」を取得する。決済処理部１３０は、「決済方法設定」が「チャージ残高」に設定されている利用者に関して、以下のように電子決済を行う。決済処理部１３０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減少させ、加盟店の売上金の項目値を増加させることで、電子決済を行う。加盟店の売上金の項目値は、例えば、それ自体が電子マネーとして使用されるものでは無く、加盟店と電子決済サービスとの取り決めに応じたサイクルで、売

上金の項目値に対応する金額が銀行口座に送金される。
【００３１】
決済処理部１３０は、「設定情報」が「後払い」に設定されている利用者に関して、以下のように電子決済を行う。後払いとは、電子決済サービスの運営者とは別主体であるクレジットカード会社との連携による「クレジット払い」とは別枠で設定されるものであり、電子決済サービスの運営者が与信者となって、後払い枠の範囲内でチャージ残高に依存しない電子決済を許容するものである。なお後払いサービスを受けるために、電子決済サービスの運営者が提供するクレジットカードの取得が要求されてよい。後払いで利用された金額は、一か月分まとめて翌月の支払日に、例えば銀行口座からの引き落としによって決済される。この場合、決済処理部１３０は、後払い利用額に決済金額を加算し、後払い利用可能額から同額を差し引くことで暫定決済を行い、締め日になると上記のように当月分の決済を翌月の支払い日に引き落とすための処理を行う、或いはクレジットカード会社の運営者に当該処理を依頼する。なお暫定決済の時点で決済金額が後払い利用可能額を超える場合は、エラー通知が決済アプリ２０に返信される。
【００３２】
［電子決済サービスへのログイン］
本実施形態において、電子決済サービスの各種機能は、電子決済サービスにログイン済みの利用者に対して提供されるものである。より具体的には、決済コンテンツ提供部１２０は、電子決済サービスへのログイン状態がログイン済みの利用者に対して決済コンテンツを提供し、未ログインの利用者に対して決済コンテンツを提供しないように構成される。例えば、利用者が電子決済サービスにログインしていない場合（例えばアプリ起動時など）、決済アプリ２０は、ログイン画面を表示して認証情報（利用者ＩＤおよびパスワード）の入力を受け付け、入力された認証情報をもとに、決済サーバ１００に対してログイン要求を行う。このログイン要求に応じて、決済サーバ１００では、ログイン認証部１５０が認証処理を実行する。ログイン認証部１５０は、利用者の認証に成功した場合、利用者のログイン状態を未ログインからログイン済みに変更する。決済コンテンツ提供部１２０は、利用者のログイン状態がログイン済みに変更された後、利用者の利用者端末装置１０に決済コンテンツを提供する。
【００３３】
しかしながら、従来のログイン認証の方法では、フィッシング等の手口によってパスワード（パスコードを含む）が不正に取得され、正当な利用者のアカウントが第三者によって不正利用されてしまう場合があった。本実施形態におけるログイン認証の方法は、このようなパスワードの流出によって不正利用が発生する可能性が従来方法よりも低減するように構成されたものである。より具体的には、従来のログイン認証では、デバイス認証に失敗した利用者がワンタイムパスワード認証に移行した際にパスワードが盗まれてしまうことが懸念されていた。本実施形態は、デバイス認証の失敗に起因して発生するワンタイムパスワード認証の方法を改善することにより、不正利用の可能性の低減を図るものである。
【００３４】
図７は、電子決済サービスにおけるログイン認証の流れの概略を示すフローチャートである。本実施形態において、電子決済サービスにログインする利用者の認証は、パスワード認証（利用者ＩＤおよびパスワードによる認証）（Ｓ３１）とデバイス認証（Ｓ３２）とを組み合わせて実施されるものである。すなわち、利用者はパスワード認証とデバイス認証の両方に成功した場合に電子決済サービスにログインすることができる（ログイン許可）。一方、パスワード認証に失敗した利用者は、ログインが拒絶される（ログイン不可）。また、デバイス認証に失敗した利用者は、ＱＲコード認証（Ｓ３３）およびＳＭＳ認証（Ｓ３４）のいずれかを選択して認証に成功した場合にログインが許可される。一方、ＱＲコード認証（Ｓ３３）およびＳＭＳ認証（Ｓ３４）のうちいずれかを選択して認証に失敗した利用者は、ワンタイムパスワード認証（Ｓ３５：ＯＴＰ認証）を実施することができる。ワンタイムパスワード認証に成功した場合にはログインが許可され、失敗した場

合にはログインが拒絶される。
【００３５】
［デバイス認証］
デバイス認証とは、利用者端末装置１０から取得されたデバイスＩＤが、当該利用者端末装置１０の利用者の利用者が予め登録したデバイスＩＤ、または当該利用者端末装置１０に関して別の手段で確認されたデバイスＩＤに一致する場合に、当該利用者端末装置１０を認証するものである。より具体的には、本実施形態におけるデバイス認証には、最初に実施される第１デバイス認証と、第１デバイス認証が失敗した場合に実施され得る第２デバイス認証および第３デバイス認証とがある。第１デバイス認証は、ログイン要求の際に利用者端末装置１０から取得されるデバイスＩＤが、要求元の利用者によって予め登録されているデバイスＩＤに一致する場合に当該利用者端末装置１０を認証してログインを許可するものである。以下、利用者によって予め登録されたデバイスＩＤを有する利用者端末装置１０を「登録済み端末」という。第１デバイス認証によれば、登録済み端末でない利用者端末装置１０からのログイン要求が拒絶されるので、第三者によるなりすましを防止することができる。
【００３６】
一方で、正当な利用者であっても、機種変更の場合など、ログインに使用する利用者端末装置１０（以下「ログイン端末」という。）が登録済み端末と異なる場合がある。そこで、本実施形態の電子決済サービスでは、第１デバイス認証に失敗した場合であっても、利用者は、第２デバイス認証または第３デバイス認証を実施することにより、登録済み端末と異なるログイン端末から電子決済サービスにログインすることができるようになっている。
【００３７】
第２デバイス認証は、ログイン端末（以下「新端末」ともいう。）と登録済み端末（以下「旧端末」ともいう。）の両方を操作可能な利用者（すなわち新端末と旧端末の両方が手元にある利用者）に向けたデバイス認証である。第２デバイス認証では、利用者は、旧端末の決済アプリ２０を操作して引継ぎ用のＱＲコードを表示させた後、旧端末に表示されているＱＲコードを新端末の決済アプリ２０で読み取ることで、新端末から電子決済サービスにログインすることができる。
【００３８】
第３デバイス認証は、新端末は操作できるが旧端末を操作できない利用者（すなわち新端末のみ手元にある利用者）に向けたデバイス認証である。第３デバイス認証は、引継ぎ用のＵＲＬをＳＭＳで新端末に送信し、当該ＵＲＬにアクセスした利用者端末装置１０のデバイスＩＤが、第１デバイス認証で認識された新端末のデバイスＩＤに一致する場合に新端末を認証するものである。第３デバイス認証では、利用者は、新端末を操作してＳＭＳで通知されたＵＲＬにアクセスすることにより、新端末から電子決済サービスにログインすることができる。引継ぎ用ＵＲＬは、一時的に有効なＵＲＬ（ワンタイムリンク）として生成されるものである。
【００３９】
第２デバイス認証および第３デバイス認証のいずれにおいても、認証が成功した場合、登録済み端末が旧端末から新端末に変更される。これにより、以後、新端末を用いたログインでは第１デバイス認証が成功するので、利用者は、第２デバイス認証または第３デバイス認証を行うことなく、パスワード認証のみで電子決済サービスにログインすることが可能となる。
【００４０】
［第３デバイス認証に対するフィッシングの懸念］
しかしながら、従来の第３デバイス認証には、決済アプリ２０の側では回避することができない理由（不可避理由）によって引継ぎ処理が想定通りに実施されない場合があった。このような理由によって認証に失敗した利用者を救済するために、従来の第３デバイス認証には、認証失敗時に使用可能な認証手段としてワンタイムパスワード認証が提供され

ていた。このため、従来の第３デバイス認証では、フィッシング等の手口によってワンタイムパスワードが第三者によって不正に取得されてしまう可能性があった。ワンタイムパスワード認証は、登録済み端末（旧端末）にワンタイムパスワードを表示させ、それを新端末に入力させることで認証する方法である。

【００４１】

より具体的には、上記の不可避理由とは、利用者がＳＭＳで通知されたＵＲＬにアクセスする際に行う操作によっては、新端末の決済アプリ２０のデバイスＩＤとは異なるデバイスＩＤが決済サーバ１００に通知されてしまうことである。第３デバイス認証において、決済アプリ２０のデバイスＩＤを決済サーバ１００に取得させるためには、決済アプリ２０を引継ぎ用ＵＲＬにアクセスさせる必要がある。このため、従来の第３デバイス認証において、決済サーバ１００は、新端末側で引継ぎ用ＵＲＬが選択された場合に、決済アプリ２０が当該ＵＲＬにアクセスする動作を行うように、引継ぎ用ＵＲＬをディープリンクの態様で記載していた。これにより、ＳＭＳを受信した新端末において引継ぎ用ＵＲＬを選択する操作が行われた場合、決済アプリ２０が当該ＵＲＬにアクセスすることにより、決済サーバ１００が決済アプリ２０のデバイスＩＤを認識することができる想定であった。

【００４２】

しかしながら、引継ぎ用ＵＲＬがタップ操作によって選択された場合には決済アプリ２０が当該ＵＲＬにアクセスする一方で、引継ぎ用ＵＲＬが長押し操作によって選択された場合は決済アプリ２０ではなく、ウェブブラウザが当該ＵＲＬにアクセスする場合があった。そして、ウェブブラウザが引継ぎ用ＵＲＬにアクセスした場合、決済サーバ１００の側では決済アプリ２０のデバイスＩＤとは異なるデバイスＩＤが認識され、第３デバイス認証が失敗することとなった。そして、ＳＭＳメッセージに含まれるＵＲＬの選択操作に対して、当該ＵＲＬをどのアプリケーションプログラムに引き渡すかの制御は、一般にオペレーティングシステムによるところが大きく、オペレーティングシステムの配下で動作するアプリケーションプログラムの側から制御することは困難である。例えば、ＳＭＳの受信メッセージ上で引継ぎ用ＵＲＬが長押し操作によって選択された場合、オペレーティングシステムによっては、ウェブブラウザのプレビュー機能が呼び出される場合がある。この場合、ディープリンクによる決済アプリ２０の呼び出しがうまく機能せず、プレビュー機能によってウェブブラウザが引継ぎ用ＵＲＬにアクセスしてしまい、ウェブブラウザのデバイスＩＤが決済サーバ１００に連携されてしまう場合がある。

【００４３】

上述のワンタイムパスワード認証は、このような不可避理由により第３デバイス認証に失敗した利用者を救済するために設けられた認証手段であるが、パスワード認証の類はフィッシングの対象とされやすい傾向にあるので、このような認証手段を設けることは電子決済サービスのセキュリティを低下させる要因となり得る。本実施形態は、このようなセキュリティの低下を抑制するために、従来の第３デバイス認証の一部を変更して、新たな第３デバイス認証を行うようにしたものである。

【００４４】

［新たな第３デバイス認証］

図８および図９は、新たな第３デバイス認証に係る処理の流れの一例を示すシーケンスチャートである。図８は、利用者端末装置１０において、ＳＭＳで受信された引継ぎ用ＵＲＬがタップ操作によって選択された場合のシーケンスを表しており、図９は、利用者端末装置１０において、ＳＭＳで受信された引継ぎ用ＵＲＬが長押し操作によって選択された場合のシーケンスを表している。なお、図８および図９において、Ｓ４０１～Ｓ４０３は、ログイン要求時に決済アプリ２０から取得されたデバイスＩＤ（Ｓ４０１：第１デバイスＩＤ）が登録済み端末のデバイスＩＤに一致しなかったことにより（Ｓ４０２）、第１デバイス認証が失敗した状況を表している（Ｓ４０３）。

【００４５】

（タップ操作の場合）

図８において、まずＳ４１１は、決済サーバ１００が第１デバイス認証に失敗し、第３デバイス認証を選択した利用者の利用者端末装置１０に対して引継ぎ用ＵＲＬをＳＭＳで通知する処理である。次にＳ４１２Ａでは、利用者が通知された引継ぎ用ＵＲＬをタップ操作により選択する。上述のとおり、タップ操作の場合は引継ぎ用ＵＲＬが決済アプリ２０に渡されて、決済アプリ２０が当該ＵＲＬにアクセスすることとなるので（Ｓ４１３）、第１デバイス認証で認識されたデバイスＩＤ（第１デバイスＩＤ）が引継ぎ用ＵＲＬにアクセスした決済アプリ２０のデバイスＩＤ（第２デバイスＩＤ）と一致し（Ｓ４１４）、第３デバイス認証が成功する（Ｓ４１５）。なお、タップ操作の場合は、決済アプリ２０のデバイスＩＤが想定通りに決済サーバ１００に連携されるので、この場合の処理の流れは従来の第３デバイス認証と同様である。

【００４６】

一方、利用者が通知された引継ぎ用ＵＲＬを長押し操作によって選択した場合、上述のとおり、当該ＵＲＬが決済アプリ２０向けのディープリンクの態様で記載されていたとしても、引継ぎ用ＵＲＬが決済アプリ２０以外のアプリケーションプログラム（典型的にはウェブブラウザである）に引き渡される場合がある。ここでは、長押し操作により、引継ぎ用ＵＲＬがウェブブラウザに引き渡される場合を想定して説明する。この場合（Ｓ４１２Ｂ）、利用者端末装置１０では、ウェブブラウザが起動して引継ぎ用ＵＲＬにアクセスすることになる（Ｓ４１６）。ここでは、決済サーバ１００のログイン認証部１５０が引継ぎ用ＵＲＬを公開するウェブサーバの機能を有するものとする。

【００４７】

次に、決済サーバ１００では、ログイン認証部１５０が引継ぎ用ＵＲＬに対する利用者端末装置１０のアクセスを受け付け、アクセス元のデバイスＩＤが第１デバイス認証において認識されたデバイスＩＤに一致しないことを認識する（Ｓ４１７）。ログイン認証部１５０は、デバイスＩＤの不一致を認識した場合、認証用のＱＲコードと、引継ぎ用ＵＲＬとの両方を含むウェブページを表示させるためのＨＴＭＬ（Hyper-Text Markup Language）データを利用者端末装置１０のウェブブラウザに返信する（Ｓ４１８）。ここで、ログイン認証部１５０は、Ｓ４１１においてＳＭＳで通知した引継ぎ用ＵＲＬと同様に、決済アプリ２０に向けたディープリンクの態様で記載した引継ぎ用ＵＲＬをＨＴＭＬデータに含めて利用者端末装置１０に送信する。

【００４８】

続いて、利用者端末装置１０において、ウェブブラウザがＳ４１８で受信されたＨＴＭＬデータをもとに、引継ぎ用ＵＲＬが記載された、ＱＲコード認証用のウェブページを表示する（Ｓ４１９）。図１０は、引継ぎ用ＵＲＬが記載されたウェブページＷＰの一例を示す図である。ウェブページＷＰには、認証用のＱＲコードＣＤと、引継ぎ用ＵＲＬをリンク先とするハイパーリンクＬＫとが表示される。図１０に示すウェブページＷＰは、ＱＲコード認証をメインの認証手段として提示しつつ、ＱＲコードをスキャンできない利用者に対して引継ぎ用ＵＲＬによるデバイス認証を代替手段として提供する方法の一例である。

【００４９】

ここで、例えば、電子決済サービスに登録されている利用者の電話番号が旧端末に紐づけられているとする。すなわち、登録済みの電話番号を有するＳＩＭ（Subscriber Identity Module）カードが旧端末に挿入されている状況である。この場合、Ｓ４１１の通知先が旧端末となるので、認証用のＱＲコードが旧端末のウェブブラウザに表示される。利用者は、旧端末に表示されたＱＲコードを新端末の決済アプリ２０で読み取ることにより、読み取られた情報が決済サーバ１００に連携されてログインが許可される。

【００５０】

しかしながら、利用者は、手元に旧端末がない場合、新端末で旧端末に表示されたＱＲコードを読み取るのは不可能である。このような場合、利用者は、代替の認証手段として、新端末から引継ぎ用ＵＲＬにアクセスすることにより、デバイス認証を受けることができる。より具体的には、利用者が新端末のウェブブラウザに表示された引継ぎ用ＵＲＬを

選択する操作を行う（Ｓ４２０）。例えば、図１０の例では、利用者は、ハイパーリンクＬＫをタップ操作や長押し操作によって選択する。ここでの選択操作では、引継ぎ用ＵＲＬの表示主体がＳＭＳ機能ではなくウェブブラウザとなるため、タップ操作および長押し操作のいずれであってもディープリンクが想定どおりに認識される。その結果、引継ぎ用ＵＲＬが決済アプリ２０に引き渡され、決済アプリ２０が引継ぎ用ＵＲＬにアクセスすることとなる（Ｓ４２１）。

【００５１】

すなわち、新たな第３デバイス認証において、Ｓ４２０において引継ぎ用ＵＲＬを選択する操作は、タップ操作であってもよいし、長押し操作であってもよいということである。この場合、決済サーバ１００では、ログイン認証部１５０が、引継ぎ用ＵＲＬにアクセスした決済アプリ２０のデバイスＩＤが第１デバイス認証で認識されたデバイスＩＤと一致することを認識することになるので（Ｓ４２２）、第３デバイス認証が成功する（Ｓ４２３）。

【００５２】

このように、新たな第３デバイス認証において、決済サーバ１００は、決済アプリ２０ではないアプリケーションプログラムから引継ぎ用ＵＲＬにアクセスした利用者に対して（デバイスＩＤの不一致により）即座にワンタイムパスワード認証を実施させるのではなく、決済アプリ２０から引継ぎ用ＵＲＬにアクセスさせるための手段をより確実な方法で提供するものである。この結果、正当な利用者によるＳＭＳ認証が失敗する頻度が減少し、ワンタイムパスワード認証が必要になる状況そのものが発生しにくくなるので、必然的にワンタイムパスワードが流出する可能性も低下する。すなわち、本実施形態における新たな第３デバイス認証によれば、第３デバイス認証に対する追加の認証手段としてのワンタイムパスワード認証のセキュリティを向上させることができる。

【００５３】

また、新たな第３デバイス認証において正当な利用者によるＳＭＳ認証が失敗する頻度が減少することは、裏返せば、ＳＭＳ認証に失敗してワンタイムパスワード認証を実施する者は悪意をもってＳＭＳ認証に失敗したと考えられることの蓋然性が高くなるということである。なぜなら、正当な利用者であれば、機種変更でもしない限り、デバイス認証に失敗する可能性が低いからである。また、正当な利用者であれば、機種変更の場合であっても、ＱＲコード認証またはＳＭＳ認証によって認証に成功するはずである。また、正当な利用者であれば、ＳＭＳ認証において、ＳＭＳ受信メッセージに記載された引継ぎ用ＵＲＬを長押し操作によって選択した場合であっても、ウェブブラウザに表示された引継ぎ用ＵＲＬを選択（タップ操作でも長押し操作でもよい）して認証に成功するはずである。その上でなお、正当な利用者がＳＭＳ認証に失敗してワンタイムパスワード認証を実施すること想定し難いものである。さらに、ＱＲコード認証とＳＭＳ認証とでは、一般にＳＭＳ認証の方がフィッシングを成功させやすいと考えられるので、フィッシングを行う者はＱＲコード認証よりもＳＭＳ認証を選択する可能性が高いと考えられる。

【００５４】

このため、ログイン認証部１５０は、ＳＭＳ認証に失敗した利用者がワンタイムパスワード認証を実施したことを検知した場合、その旨を通知する。ここで、ログイン認証部１５０は、電子決済サービスの管理者に通知してもよいし、当該利用者について登録されている連絡先（電話番号やメールアドレスなど）に通知してもよい。また、ログイン認証部１５０は、ＳＭＳ認証に失敗した利用者がワンタイムパスワード認証を実施したことを検知した場合、上記通知に代えて、または上記通知に加えて、当該利用者について、電子決済サービスが提供する機能の一部を制限するように構成されてもよい。

【００５５】

以上説明した実施形態によれば、規定の認証手段に対する追加の認証手段として提供されるワンタイムパスワードのセキュリティを向上させることができる。

【００５６】

なお、上記の実施形態では、本発明の認証装置が決済サーバ１００として構成された場

合について説明したが、認証装置は、決済サーバ１００が有する電子決済サービスの機能とは分離した別体の装置として構成されてもよい。この場合、認証装置は決済サーバ１００との通信により、必要に応じて必要な情報を決済サーバ１００との間でやり取りするように構成されてもよい。また、この場合、決済サーバ１００が記憶部１７０に記憶する情報のうち、ログイン認証に必要な情報の一部または全部は認証装置の記憶部に保持されてもよい。

【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。

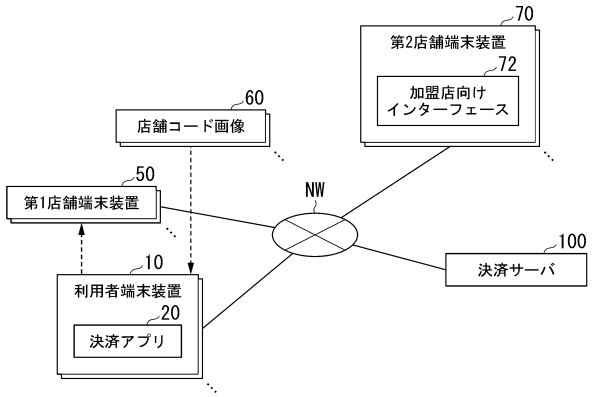
【符号の説明】

【００５８】

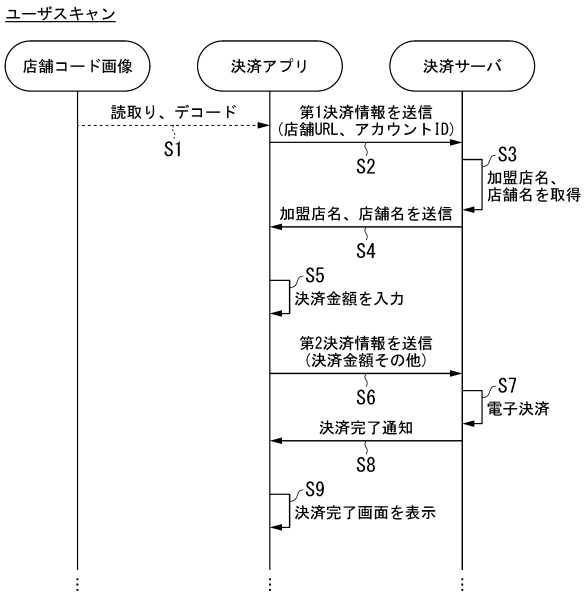
１０　利用者端末装置
２０　決済アプリ
５０　第１店舗端末装置
６０　店舗コード画像
７０　第２店舗端末装置
７２　加盟店向けインターフェース
１００　決済サーバ
１１０　通信部
１２０　決済コンテンツ提供部
１３０　決済処理部
１４０　情報管理部
１５０　ログイン認証部
１７０　記憶部
１７２　利用者情報
１７４　決済コンテンツ情報
１７６　加盟店／店舗情報

【図面】

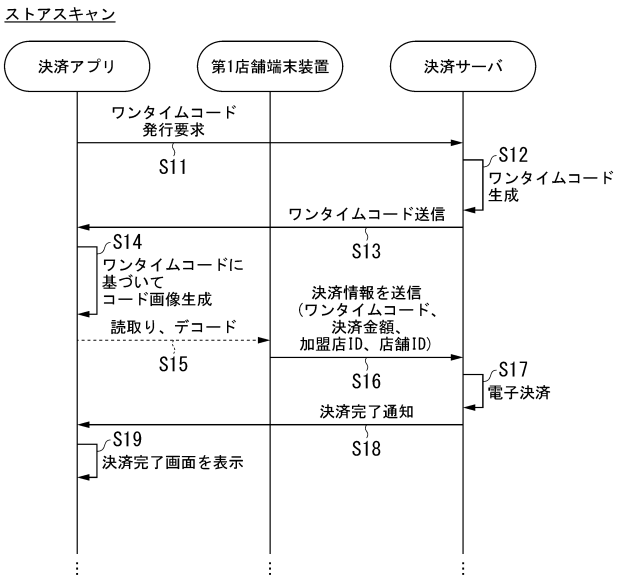
【図１】



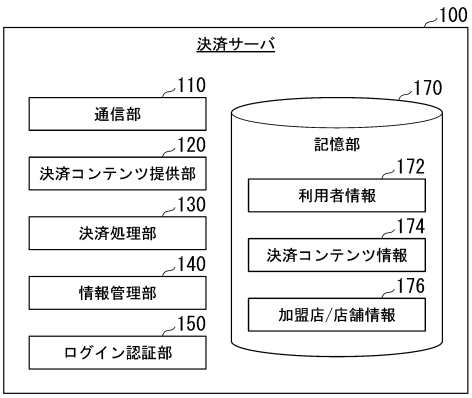
【図２】



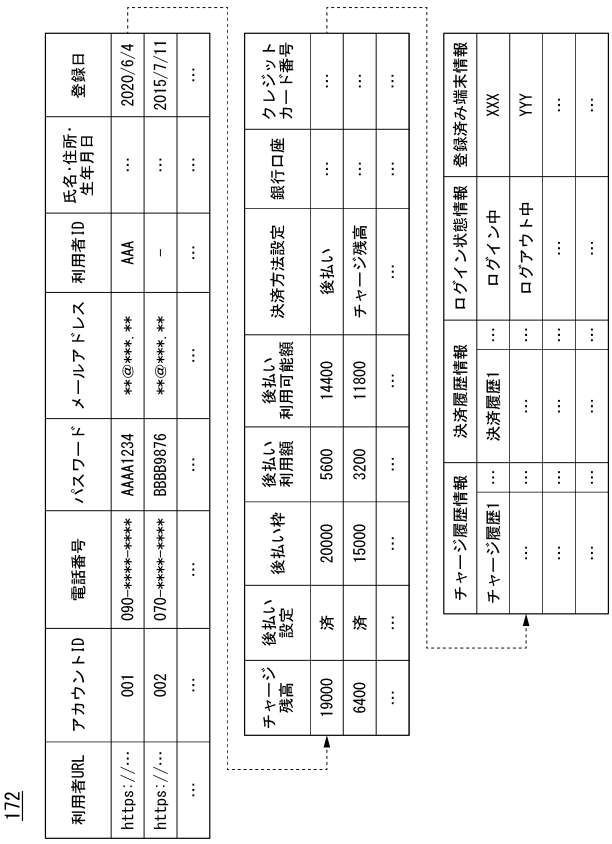
【図３】



【図４】



【図５】



【図６】

176

176A

店舗URL	加盟店ID	店舗ID
https://…	13579	651874
https://…	24685	2495782
…	…	…

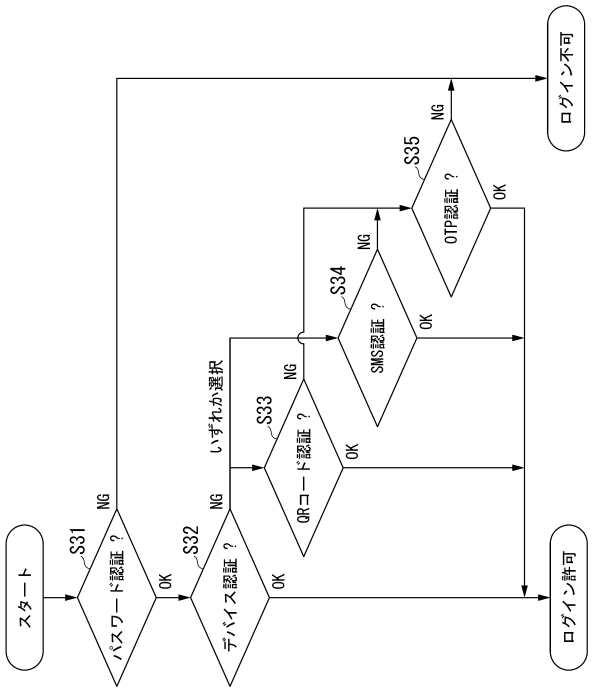
176B

加盟店ID	加盟店名	売上金
13579	○○珈琲	557420
24685	△△寿司	1257400
…	…	…

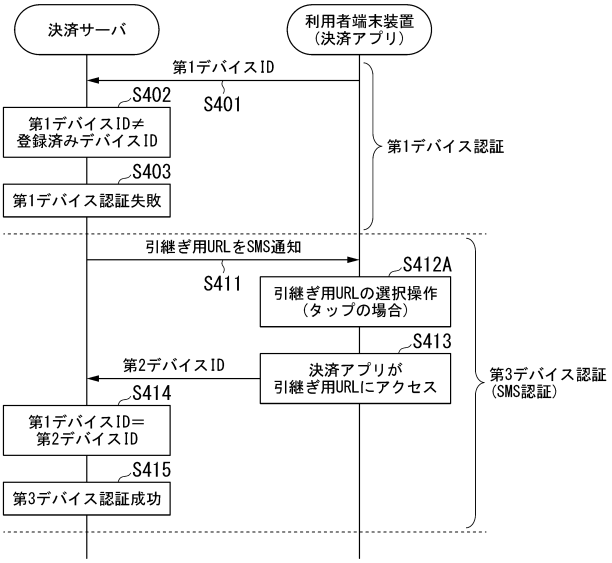
176C

店舗ID	店舗名
651874	大井町店
2495782	目黒店
…	…

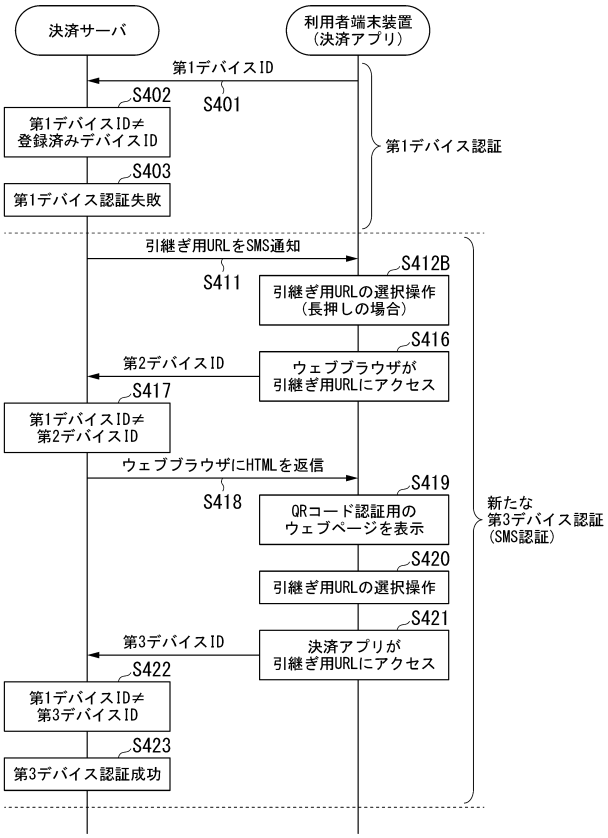
【図７】


スタート
S31
パスワード認証 ？
NG
OK
S32
デバイス認証 ？
NG
OK
いずれか選択
S33
QRコード認証 ？
NG
OK
S34
SMS認証 ？
NG
OK
S35
OTP認証 ？
NG
OK
ログイン不可
ログイン許可

【図８】


決済サーバ
利用者端末装置
（決済アプリ）
第1デバイスID
S401
S402
第1デバイスID≠
登録済みデバイスID
S403
第1デバイス認証失敗
第1デバイス認証
引継ぎ用URLをSMS通知
S411
S412A
引継ぎ用URLの選択操作
（タップの場合）
S413
第2デバイスID
決済アプリが
引継ぎ用URLにアクセス
S414
第1デバイスID＝
第2デバイスID
S415
第3デバイス認証成功
第3デバイス認証
（SMS認証）

【図９】


決済サーバ
利用者端末装置
（決済アプリ）
第1デバイスID
S401
S402
第1デバイスID≠
登録済みデバイスID
S403
第1デバイス認証失敗
第1デバイス認証
引継ぎ用URLをSMS通知
S411
S412B
引継ぎ用URLの選択操作
（長押しの場合）
S416
第2デバイスID
ウェブブラウザが
引継ぎ用URLにアクセス
S417
第1デバイスID≠
第2デバイスID
ウェブブラウザにHTMLを返信
S418
S419
QRコード認証用の
ウェブページを表示
新たな
第3デバイス認証
（SMS認証）
S420
引継ぎ用URLの選択操作
S421
第3デバイスID
決済アプリが
引継ぎ用URLにアクセス
S422
第1デバイスID≠
第3デバイスID
S423
第3デバイス認証成功

【図１０】


10
ログイン認証
ログイン認証用QRコード
CD
有効期限：10:00
新しい端末で上のQRコードを
スキャンしてください
QRコードをスキャンできない場合は
こちらから認証してください。
LK