

(19)日本国特許庁(JP)

(12)特許公報(B1)

(11)特許番号
特許第7403705号
(P7403705)

(45)発行日 令和5年12月22日(2023.12.22)

(24)登録日 令和5年12月14日(2023.12.14)

(51)国際特許分類

FI

G 0 6 F 21/44 (2013.01)

G 0 6 F 21/44

請求項の数 10 (全18頁)

(21)出願番号	特願2023-179090(P2023-179090)	(73)特許権者	519110124
(22)出願日	令和5年10月17日(2023.10.17)		P a y P a y 株式会社
審査請求日	令和5年10月17日(2023.10.17)		東京都千代田区紀尾井町1番3号
早期審査対象出願		(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 P a y P a y 株式会社内
		審査官	平井 誠
最終頁に続く			

(54)【発明の名称】 認証装置、認証方法、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 S M S (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 S M S 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、

10

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、

20

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 Q R 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、

30

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、

40

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

50

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】

【文献】特許第7247416号公報

【文献】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

10

20

30

40

50

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。

10

【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。

20

【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もよい。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。

30

【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

50

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。

10

【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。

20

【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。

30

【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

40

50

、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まれて決済サーバ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

10

20

30

40

50

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。

10

【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。

20

【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。

30

40

【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

50

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。

10

【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】

20

〔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なく、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】

30

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。

40

【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

50

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している。

【 0 0 3 7 】

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。

【 0 0 3 8 】

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。

【 0 0 3 9 】

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。

【 0 0 4 0 】

[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。

【 0 0 4 1 】

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。

【 0 0 4 2 】

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

10

20

30

40

50

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

10

20

30

40

50

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

10

20

30

40

50

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。

10

【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。

20

【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。

30

【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

40

50

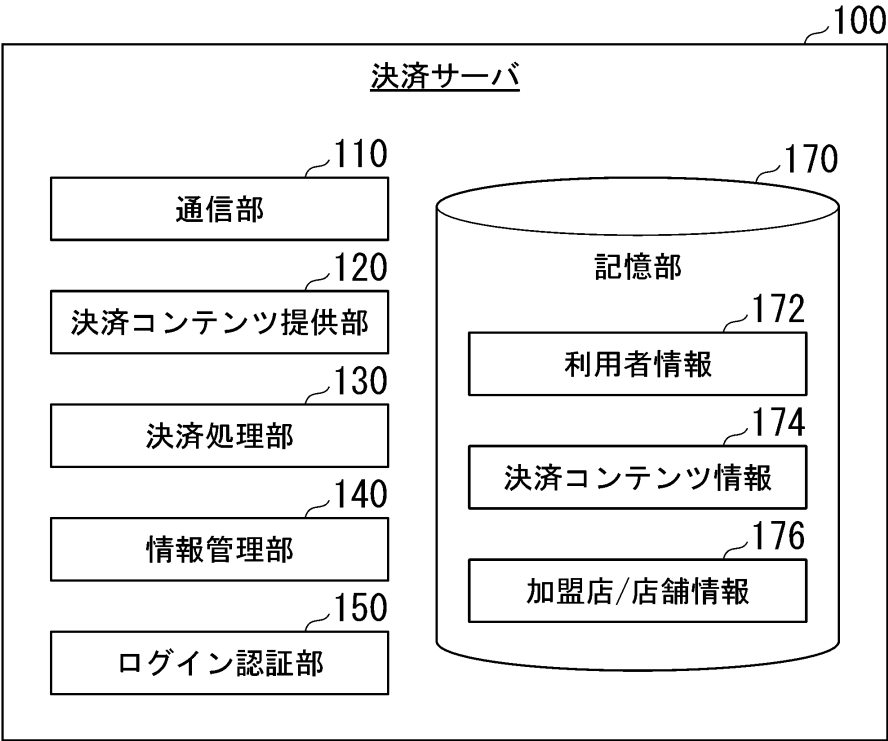
- 1 4 0 情報管理部
- 1 5 0 ログイン認証部
- 1 7 0 記憶部
- 1 7 2 利用者情報
- 1 7 4 決済コンテンツ情報
- 1 7 6 加盟店／店舗情報

【要約】

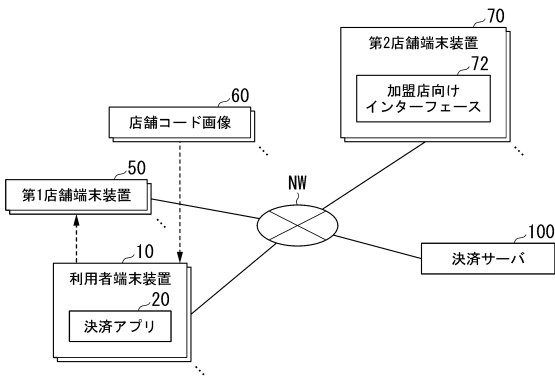
【課題】規定の認証手段に対する追加の認証手段として提供されるワンタイムパスワードのセキュリティを向上させること。

【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

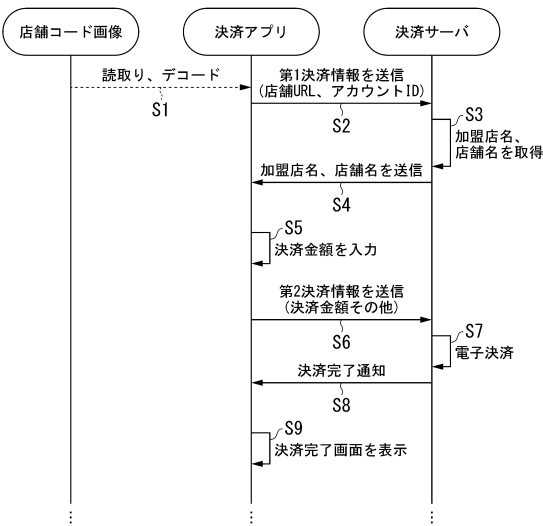


【図面】
【図 1】



【図 2】

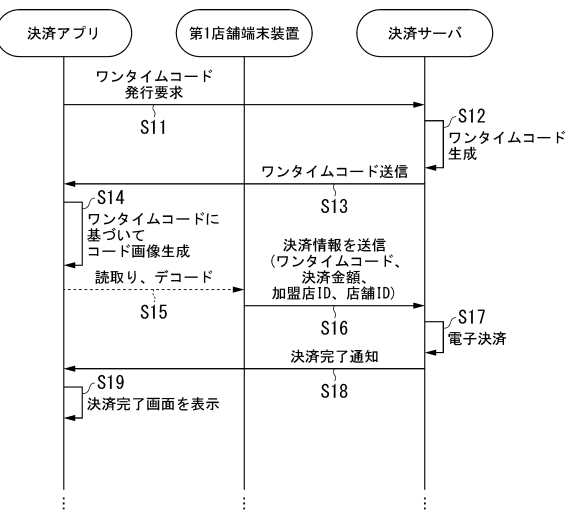
ユーザスキャン



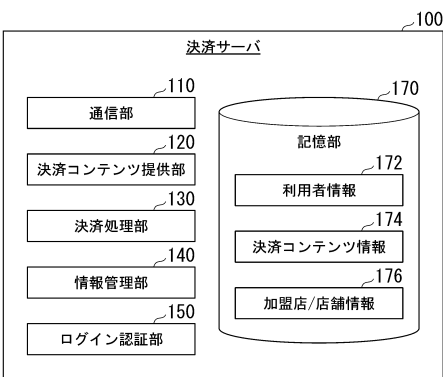
10

【図 3】

ストアスキャン



【図 4】



20

30

40

50

【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
https://...	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	決済履歴情報	ログイン状態情報	登録済み端末情報
チャージ履歴1	決済履歴1	ログイン中	XXX
...	...	ログアウト中	YYY
...	...	...	...
...	...	...	...

【図 6】

176

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
...	...	...

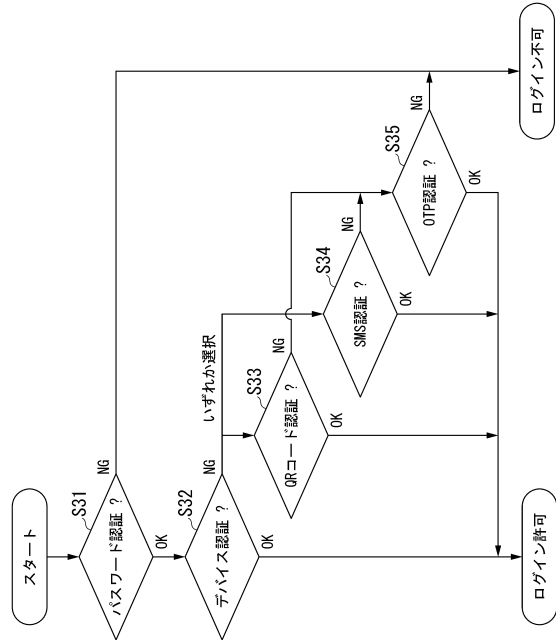
176C

店舗ID	店舗名
651874	大井町店
2495782	目黒店
...	...

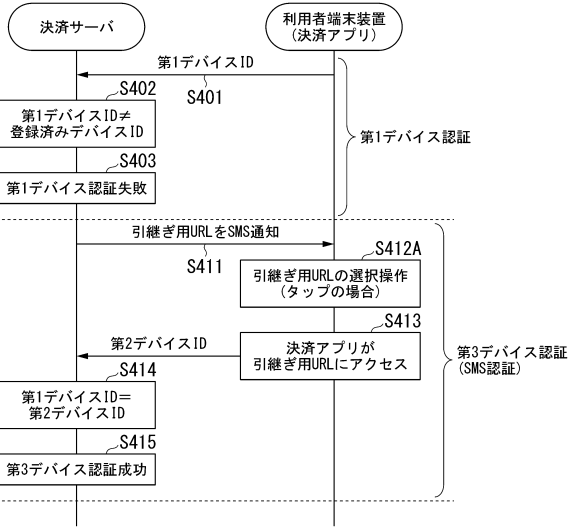
10

20

【図 7】



【図 8】

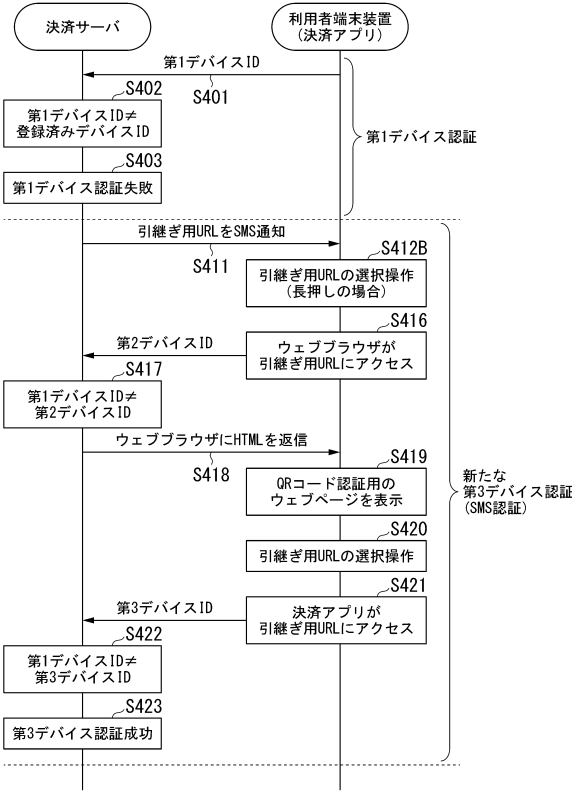


30

40

50

【図 9】



【図 10】



10

20

30

40

50

フロントページの続き

(56)参考文献 特許第7202500(JP, B1)
(58)調査した分野 (Int.Cl., DB名)
G06F21/00-88