

(19)日本国特許庁(JP)

(12)特許公報(B1)

(11)特許番号
特許第7453458号
(P7453458)

(45)発行日 令和6年3月19日(2024.3.19)

(24)登録日 令和6年3月11日(2024.3.11)

(51)国際特許分類

F I

G 0 6 F 21/36 (2013.01)

G 0 6 F 21/36

G 0 6 Q 20/40 (2012.01)

G 0 6 Q 20/40

請求項の数 14 (全19頁)

(21)出願番号	特願2023-144663(P2023-144663)	(73)特許権者	519110124
(22)出願日	令和5年9月6日(2023.9.6)		P a y P a y 株式会社
審査請求日	令和5年9月6日(2023.9.6)		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	田中 啓介

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】

利用者の端末装置で動作するアプリケーションプログラムと協働して前記利用者に所定のサービスを提供するサービス提供装置であって、

前記アプリケーションプログラムによりコード画像を提示した利用者に対して前記サービスを提供するサービス提供部と、

前記コード画像の有効性を管理する管理部と、

前記利用者が提示したコード画像から読み取られたコード情報に基づいて前記サービスの不正利用を検知する検知部と、

を備え、

前記管理部は、前記端末装置において前記コード画像を画面キャプチャにより複製する操作が行われたことを示す複製通知が前記アプリケーションプログラムから受信された場合、前記操作による複製の対象となったコード画像を無効化し、

前記検知部は、前記サービスの利用に際して受信されたコード情報が無効化されている場合、前記サービスの利用が不正利用であると判定する、

サービス提供装置。

【請求項2】

前記コード画像は、前記アプリケーションプログラムを介して前記サービスにログインする際の二要素認証において、二要素目の認証情報として使用されるものである、

請求項1に記載のサービス提供装置。

【請求項 3】

前記検知部は、前記サービスの不正利用を検知した場合、前記不正利用に係るコード情報の送信元に関する情報を記録する、

請求項 1 に記載のサービス提供装置。

【請求項 4】

前記管理部は、前記コード画像の有効期限を前倒して強制的に満了させることにより前記コード情報を無効化する、

請求項 1 に記載のサービス提供装置。

【請求項 5】

前記管理部は、前記コード画像を更新することにより、更新前のコード画像を無効化する、

請求項 1 に記載のサービス提供装置。

【請求項 6】

前記サービスは、前記利用者に電子決済サービスを提供するものであり、

前記コード画像は、前記電子決済サービスにおいて、決済に必要な決済情報を前記サービス提供装置に供給する手段として使用されるものである、

請求項 1 に記載のサービス提供装置。

【請求項 7】

前記コード画像は、前記電子決済サービスの加盟店の店舗に設置された店舗端末によって読み取られるものであり、

前記店舗端末は、前記コード画像から読み取ったコード情報を前記決済情報に含めて前記サービス提供装置に送信する、

請求項 6 に記載のサービス提供装置。

【請求項 8】

前記管理部は、前記コード画像を無効化した場合、前記複製通知の送信元に対して通知を行う、

請求項 1 に記載のサービス提供装置。

【請求項 9】

前記検知部は、前記サービスの不正利用を検知した場合、前記不正利用に係るコード情報の送信元に対して通知を行う、

請求項 1 に記載のサービス提供装置。

【請求項 10】

前記検知部は、前記サービスの不正利用を検知した場合、前記不正利用に係るコード情報の用途に応じた処理を行う、

請求項 1 に記載のサービス提供装置。

【請求項 11】

前記管理部は、前記複製通知に基づいて複製の対象となったコード画像を特定し、前記コード画像の用途に応じた処理を実行する、

請求項 1 に記載のサービス提供装置。

【請求項 12】

前記サービス提供部は、前記アプリケーションプログラムにより提示された前記コード画像を読み取る読取装置から前記コード画像から読み取られた情報を取得し、取得した前記情報に基づいて前記サービスを提供するものである、

請求項 1 に記載のサービス提供装置。

【請求項 13】

利用者の端末装置で動作するアプリケーションプログラムと協働して前記利用者に所定のサービスを提供するサービス提供装置が、

前記アプリケーションプログラムによりコード画像を提示した利用者に対して前記サービスを提供するためのサービス提供処理と、

前記コード画像の有効性を管理するための管理処理と、

10

20

30

40

50

前記利用者が提示したコード画像から読み取られたコード情報に基づいて前記サービスの不正利用を検知するための検知処理と、

を実行するサービス提供方法であって、

前記管理処理は、前記端末装置において前記コード画像を画面キャプチャにより複製する操作が行われたことが前記アプリケーションプログラムから通知された場合、前記操作による複製の対象となったコード画像を無効化するものであり、

前記検知処理では、前記サービスの利用に際して受信されたコード情報が無効化されている場合、前記サービスの利用が不正利用であると判定する、

サービス提供方法。

【請求項 1 4】

利用者の端末装置で動作するアプリケーションプログラムと協働して前記利用者に所定のサービスを提供するサービス提供装置に、

前記アプリケーションプログラムによりコード画像を提示した利用者に対して前記サービスを提供するためのサービス提供処理と、

前記コード画像の有効性を管理するための管理処理と、

前記利用者が提示したコード画像から読み取られたコード情報に基づいて前記サービスの不正利用を検知するための検知処理と、

を実行させるためのプログラムであって、

前記管理処理は、前記端末装置において前記コード画像を画面キャプチャにより複製する操作が行われたことが前記アプリケーションプログラムから通知された場合、前記操作による複製の対象となったコード画像を無効化するものであり、

前記検知処理は、前記サービスの利用に際して受信されたコード情報が無効化されている場合、前記サービスの利用が不正利用であると判定するものである、

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、サービスにログインする際に使用する端末装置を変更しようとする利用者を、QRコード（登録商標、以下同様）を用いて認証する仕組みを備えた電子決済サービスが開発されている（例えば、特許文献1参照）。より具体的には、変更前の端末装置に認証用のQRコードを送信し、当該QRコードを変更後の端末装置で読み取らせることにより端末装置の変更を認証するというものである。

【先行技術文献】

【特許文献】

【0003】

【文献】特許第7104259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、認証用のQRコードが画面キャプチャによって複製されてしまう可能性があった。そのため、複製されたQRコードを取得した第3者が正当な利用者になりすまして不正に認証に成功してしまう可能性があった。

【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、コード情報を用いた認証処理のセキュリティを向上させ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】

10

20

30

40

50

【0006】

本発明の一態様は、利用者の端末装置で動作するアプリケーションプログラムと協働して前記利用者に所定のサービスを提供するサービス提供装置であって、前記アプリケーションプログラムによりコード画像を提示した利用者に対して前記サービスを提供するサービス提供部と、前記コード画像の有効性を管理する管理部と、前記利用者が提示したコード画像から読み取られたコード情報に基づいて前記サービスの不正利用を検知する検知部と、を備え、前記管理部は、前記端末装置において前記コード画像を複製する操作が行われたことを示す複製通知が前記アプリケーションプログラムから受信された場合、前記操作による複製の対象となったコード画像を無効化し、前記検知部は、前記サービスの利用に際して受信されたコード情報が無効化されている場合、前記サービスの利用が不正利用であると判定する、サービス提供装置である。

10

【発明の効果】

【0007】

本発明の一態様によれば、コード情報を用いた認証処理のセキュリティを向上させ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。

20

【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】コード関連情報178の内容の一例を示す図である。

【図8】第2の情報連携に係る端末操作の一例を示す図である。

【図9】なりすまし防止処理における第1処理の流れの一例を説明するシーケンスチャートである。

【図10】なりすまし防止処理における第2処理の流れの一例を説明するシーケンスチャートである。

30

【図11】なりすまし防止処理における第2処理が実行される状況を説明するイメージ図である。

【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。

40

50

【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。

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。

30

【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。

40

【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

50

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

10

20

30

40

50

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、コード関連情報178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。送金的手段としては、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

10

20

30

40

50

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】

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

【0027】

図7は、コード関連情報178の内容の一例を示す図である。コード関連情報178は、例えば、利用者IDに対してコード情報と、有効期限と、コード画像とが対応付けられた第1テーブル178Aと、送信元利用者IDに対して受信時刻と、コード情報と、コード画像と、送信元情報とが対応付けられた178Bとを含む。第1テーブル178Aは、各利用者について生成したコード画像を管理するための情報である。コード情報は、コード画像として符号化された情報である。“[画像データ]”は、コード画像の画像データが項目の値として保持されることを表している。第2テーブル178Bは、利用者端末装置10から受信されたコード情報を管理するための情報である。コード画像は、決済アプリ20と決済サーバ100との間において直接的または間接的にコード情報を連携するための手段であり、コード情報の符号化によって得られる画像である。コード情報には、少なくとも決済サーバ100において対象の利用者および用途を特定できるようにするための情報が含まれるものである。本実施形態では、コード情報による情報連携の用途として、決済用途と、端末変更時のログイン用途とを想定する。

20

【0028】

送信元利用者IDは、受信されたコード情報の送信元の利用者を示す利用者IDである。送信元利用者IDは、例えば、送信元の利用者端末装置10において読み取られるコード画像に含まれており、送信元の利用者端末装置10が決済サーバ100に送信するコード情報に含まれる。受信時刻は、決済サーバ100が送信元の利用者端末装置10からコード情報を受信した時刻である。受信コード情報は、送信元の利用者端末装置10から受信されたコード情報である。受信コード画像は、送信元の利用者端末装置10において受信コード情報の取得のために読み取られたコード画像である。送信元情報は、受信コード情報の送信元の利用者端末装置10に関する情報である。送信元情報には、例えば、IPアドレスやMACアドレス、端末機種、電話番号等の情報が含まれる。なお、コード画像はコード情報を符号化したものであるため、コード関連情報178において、コード画像およびコード情報のいずれか一方は省略されてもよい。

30

【0029】

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、加盟店／店舗情報176、およびコード関連情報178を管理する。情報管理部140は、利用者情報172、加盟店／店舗情報176、およびコード関連情報178について新規レコードの追加、編集、削除などを行う。また、情報管理部140は、コード情報からコード画像を生成する機能と、コード画像からコード情報を読み取る機能とを有する。また、情報管理部140は、コード情報を更新する機能を有する。情報管理部140は、コード情報を更新した場合、更新後のコード情報によりコード画像も更新する。

40

【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。

50

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】

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】

〔コード情報による情報連携〕

コード情報による第 1 の情報連携は、ストアスキャン方式（図 3）の決済時における情報連携である。上述のとおり、ストアスキャン方式の決済では、決済アプリ 20 が決済サーバ 100 から受信されたワнтаイムコードに基づいてコード画像を生成し、生成したコード画像を第 1 店舗端末装置 50 に読み取らせる。第 1 店舗端末装置 50 は、コード画像から読み取ったワнтаイムコードをもとに決済情報を生成して決済サーバ 100 に送信する。

【0033】

コード情報による第 2 の情報連携は、決済アプリ 20 の使用端末を変更する手続き（以下「端末変更手続き」という。）において変更先端末での二要素認証に必要な認証情報の連携である。図 8 は、第 2 の情報連携に係る端末操作の一例を示す図である。より具体的には、図 8 は、変更先の利用者端末装置 10 A で動作する決済アプリ 20 にログインする際の二要素目の認証として、変更元の利用者端末装置 10 B に表示されたコード画像 CD1 を、変更先の利用者端末装置 10 B で読み取ることを要求する認証方法を例示するものである。なお、変更先の利用者端末装置 10 B における一要素目の認証は、ユーザ ID およびパスワードによる認証であってもよいし、その他の認証方法によるものであってもよい。

【0034】

第 1 の情報連携および第 2 の情報連携のいずれにおいても、コード情報が不正に取得されてしまった場合、正当な利用者の決済アプリ 20 が他の利用者によって使用されてしまう可能性がある。例えば、第 1 の情報連携の場合、或る利用者 A1 のコード画像を不正に取得した利用者 B1 が利用者 A1 のコード画像を第 1 店舗端末装置 50 に読み取らせて決済を行うことが考えられる。この場合、利用者 A1 の支払い手段が利用者 B1 によって不正に利用されてしまうことになる。

【0035】

また、例えば、第 2 の情報連携の場合、変更先の利用者端末装置 10 の利用者 A2 が、変更元の利用者端末装置 10 の利用者 B2 のユーザ ID およびパスワードを不正に取得し、変更先の利用者端末装置 10 において利用者 B2 のユーザ ID およびパスワードを用いて一要素目の認証を突破したとする。この場合、利用者 A2 が利用者 B2 のコード画像をさらに取得したとすると、利用者 A2 は、利用者 B2 のコード画像を変更先の利用者端末

10

20

30

40

50

装置 10 で読み取ることにより二要素目の認証を突破することができてしまう。この場合、利用者 A 2 が変更先の利用者端末装置 10 において利用者 B 2 としてログインすることが可能になってしまう。

【0036】

このようなコード画像の不正入手を可能にする方法の一例として、電子決済サービスの利用者をフィッシングサイトに誘導してコード画像の画面キャプチャ（スクリーンショットともいう）を取得させ、取得したキャプチャ画像をフィッシングサイトに送信させるという手口が想定される。本実施形態におけるログイン認証部 150 は、決済アプリ 20 と協働して、このようなコード画像の不正利用によるなりすましを抑制するための処理（以下「なりすまし防止処理」という。）を実行するものである。

10

【0037】

図 9 は、なりすまし防止処理における第 1 処理の流れの一例を説明するシーケンスチャートである。第 1 処理は、コード情報の複製を検知するとともに、複製が検知されたコード情報を無効化する処理である。図 9 において、利用者端末装置 10 は、正当な利用者が操作する利用者端末装置 10 である。第 1 処理が実行される状況として、例えばフィッシングサイトに誘導された正当な利用者が、当該フィッシングサイトの指示に従ってコード画像の画面キャプチャを取得しようとしている状況が想定される。この場合、まず利用者は、利用者端末装置 10 を操作して決済アプリ 20 にコード画像を表示させる（S201）。

【0038】

続いて、利用者は決済アプリ 20 がコード画像を表示している状態で、利用者端末装置 10 に対して画面キャプチャを取得するための操作（以下「画面キャプチャ操作」という。）を行う（S202）。決済アプリ 20 は、画面キャプチャ操作が行われたことを検知すると（S203）、その旨を決済サーバ 100 に通知する（S204：キャプチャ検知通知）。なお、本実施形態において、利用者端末装置 10 は、OS（Operating System）の機能によって画面キャプチャを取得することができるよう構成されているものとする。また、利用者端末装置 10 の OS は、画面キャプチャ操作を認識した際、フォアグラウンドで動作しているアプリケーションプログラムに対して画面キャプチャ操作が行われた旨の通知（キャプチャ操作通知）を送信するように構成されているものとする。本実施形態の決済アプリ 20 は、コード画像の表示中にキャプチャ操作通知が受信された場合、コード画像が複製されたと認識してキャプチャ検知通知を決済サーバ 100 に送信するように構成されるものである。

20

30

【0039】

続いて、決済サーバ 100 では、情報管理部 140 が、S204 のキャプチャ検知通知を受けて、画面キャプチャの対象となったコード画像を無効化する（S205）。コード画像の無効化は、例えば、コード画像の更新によって実現されてもよいし、コード画像の有効期限を前倒して強制的に満了させることによって実現されてもよいし、コード画像に無効化のフラグを立てることによって実現されてもよい。情報管理部 140 は、コード画像を無効化した旨を利用者端末装置 10 に通知する（S206：無効化通知）。ここで、情報管理部 140 は「検知部」の一例であり、キャプチャ検知通知は「複製通知」の一例である。

40

【0040】

続いて、利用者端末装置 10 では、決済アプリ 20 が S206 の無効化通知を受けてエラー情報を表示する（S207）。例えば、エラー情報は、コード画像がキャプチャされた場合、キャプチャされたコード画像が第三者に送信され不正利用される可能性がある旨を通知するものであってもよい。また、例えば、エラー情報は、決済アプリ 20 では画面キャプチャによるコード画像の複製が禁止されている旨を通知するものであってもよいし、複製されたコード画像が無効化された旨を通知するものであってもよい。このような第 1 処理が行われることによって、複製されたコード画像の悪用により第三者が正当な利用者になりすまして電子決済サービスを利用することを防止することができる。

50

【0041】

図10は、なりすまし防止処理における第2処理の流れの一例を説明するシーケンスチャートである。第2処理は、複製されたコード画像による電子決済サービスの不正利用を検知する処理である。図10において、第1の利用者端末装置10および第2の利用者端末装置30は、正当な利用者のコード画像の画面キャプチャを不正に取得した利用者（不正利用者）の端末装置である。図11は、図10で説明する第2処理が実行される状況を説明するイメージ図である。ここでは第2処理が実行される状況として、端末変更手続きの際の二要素目の認証において、変更先端末において不正なコード画像が読み込まれた状況を想定する。図11の例において、第1の利用者端末装置10は変更先の端末装置であり、第2の利用者端末装置30は、不正に取得されたキャプチャ画像IM1を表示させるための端末装置である。図10のシーケンス開始時点において、第1の利用者端末装置10は、決済アプリ20へのログインについて一要素目の認証を突破した状態であり、二要素目の認証情報としてコード画像を読み取ろうとしている。

10

【0042】

このような状況において、まず、不正利用者は、第1の利用者端末装置10に読み取らせるべきコード画像CD2を含んでいるキャプチャ画像IM1を第2の利用者端末装置30に表示させる（S301）。上述のとおり、キャプチャ画像IM1は不正に取得されたものである。次に、不正利用者は、第2の利用者端末装置30に表示されたキャプチャ画像IM1に含まれるコード画像CD2を第1の利用者端末装置10で撮像することにより、第1の利用者端末装置10で動作する決済アプリ20にコード情報を読み取らせる（S302）。以下、コード画像CD2から読み取られたコード情報をコード情報CD2と称する。決済アプリ20は、読み取ったコード情報CD2を二要素目の認証情報として決済サーバ100に送信する（S303）。

20

【0043】

続いて、決済サーバ100では、ログイン認証部150がS303で受信されたコード情報CD2に基づいて、送信元の利用者が正当な利用者であるか否かを判定する（S304）。より具体的には、ログイン認証部150は、コード関連情報178を参照し、受信されたコード情報の有効性を認識する。ログイン認証部150は、コード情報が有効化されている場合には、送信元の利用者は正当な利用者であると判定して決済アプリ20へのログインを許可する（S305）。ここでは、送信元の利用者が不正利用者である場合を想定しているのでログインが許可されることはないが、仮に正当な利用者によって端末変更手続きが実施された場合には、ここで手続きが完了する。

30

【0044】

一方、コード情報が無効化されている場合、ログイン認証部150は、送信元の利用者は不正な利用者であると判定して決済アプリ20へのログインを許可しない。上述のとおり、ここでは送信元の利用者が不正利用者である場合を想定しているが、この場合、キャプチャ画像IM1から読み取られたコード情報CD2については、キャプチャ画像IM1が取得された際の第1処理によって既に無効化されているので、S304において不正利用者によるなりすましの試みが検知される。この場合、ログイン認証部150は、不正利用に関する情報をコード関連情報178（第2テーブル）として記録する（S306）とともに、不正利用者に対して警告を通知するための情報（警告情報）をコード情報CD2の送信元である第1の利用者端末装置10に送信する（S307）。警告情報は、S306で記録された不正利用に関する情報を含んでもよい。第1の利用者端末装置10の決済アプリ20は、決済サーバ100から受信された警告情報を表示する（S308）。

40

【0045】

ここでは、コード画像がキャプチャされたことに応じてコード情報が無効される場合について説明したが、コード情報はコード画像の画面キャプチャ以外の要因で無効化されるものであってもよい。この場合、決済サーバ100は、無効化されたコード情報についてその理由とともに管理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は、コード情報が無効化されている場合、且つ、その無効化の理由がコード画像の画面キャ

50

プチャによるものである場合にログインの不許可および警告情報の通知を行うように構成されてもよい。また、決済サーバ100は、コード情報が無効化されている場合にログインを許可せず、さらに、無効化の理由がコード画像の画面キャプチャによるものである場合に警告情報を通知するように構成されてもよい。

【0046】

また、不正利用に関する情報には、図7で説明したもののほか、不正に得たキャプチャ画像（すなわち無効化されたコード情報）でログインを試行した端末装置の識別情報が含まれてもよいし、当該ログインを試行したアプリケーションプログラムの識別情報が含まれてもよい。

【0047】

また、S304において不正利用者によるなりすましの試みが検知された場合、決済サーバ100は、不正利用者の第1の利用者端末装置10に対して警告情報を通知する（S307、S308）ことに代えて／加えて、正当な利用者の第2の利用者端末装置30に対して「あなたのアカウントに対して不正な方法によるログインが試行されました。」といったような注意喚起のメッセージを通知するように構成されてもよい。

【0048】

このような第2処理によれば、画面キャプチャによって複製されたコード画像が不正に利用されることを防止することができる。また、実施形態の第2処理によれば、不正に取得されたコード画像によるなりすましの試みが検知された場合、不正利用に関する情報が記録される。このため、電子決済サービスの運営者は、記録された情報をもとに不正利用者を特定したり、不正利用の防止策を検討したりするといったことが可能となり、不正利用に対してより適切な対応をとることができる。

【0049】

以上説明した実施形態によれば、コード情報を用いた認証処理のセキュリティを向上させることができる。なお、実施形態では、端末変更手続きにおけるなりすましを検知または防止する方法について説明したが、この方法は、端末変更手続きにおけるなりすましに限らず、利用者端末装置10での画面キャプチャによるコード画像の複製を伴うものであればどのような態様のなりすましにも適用可能なものである。例えば、ストアスキャン方式（図3参照）での決済においてやりとりされるコード画像についても適用可能である。ストアスキャン方式への適用によれば、不正利用者がコード画像の画面キャプチャを取得した時点では当該コード画像が無効化されているので、不正利用者が正当な利用者の電子決済口座を悪用して決済を行うことを防止することができる。

【0050】

<変形例>

決済サーバ100は、決済アプリ20からキャプチャ検知通知が受信された場合、キャプチャ対象のコード画像を無効化する際に、当該コード画像の用途に応じた処理を行うように構成されてもよい。例えば、コード画像の用途は、当該コード画像から読み取られるコード情報に含まれるものであってもよいし、決済サーバ100において、コード情報に対応づけて管理されるものであってもよい。この場合、決済アプリ20がキャプチャされたコード画像からコード情報を読み取り、キャプチャ検知通知とともに決済サーバ100に送信することにより、決済サーバ100側で当該コード情報（コード画像）の用途を認識することができる。

【0051】

例えば、情報管理部140は、キャプチャ検知通知を受けた場合であっても、コード画像の用途が特定の用途である場合、コード情報を無効化しないように構成されてもよい。例えば、情報管理部140は、キャプチャ検知通知を受けた場合であっても、コード画像の用途が端末変更手続きであることが認識された場合には、まず、変更先端末が手元にあることの確認を利用者に対して行い、確認がとれた場合にはコード情報を無効化せず、確認がとれなかった場合にコード情報を無効化するように構成されてもよい。なお、変更先端末が利用者の手元にあることの確認は、例えば以下のようにして実施されてもよい。ま

ず、決済サーバ１００は、キャプチャ検知通知を受けた際に、変更元端末の決済アプリ２０と変更先端末の決済アプリ２０の両方に位置情報の送信許可を求める画面を表示させる。決済サーバ１００は、両端末において位置情報の送信が許可されて位置情報が提供された場合、且つ、両者の位置情報が一定の範囲内を示す場合に、変更先端末が手元にあると判定してもよい。

【００５２】

情報管理部１４０は、ストアスキャン方式（図３参照）の決済において、第１店舗端末装置５０を介して決済アプリ２０から無効化されたコード情報が受信された場合、当該第１店舗端末装置５０の設置店舗を特定し、不正利用に関して記録するコード関連情報１７８に当該設置店舗に関する情報を含めるように構成されてもよい。なお、設置店舗は、決済情報に含まれる店舗ＩＤによって特定可能である。さらに、情報管理部１４０は、キャプチャ検知通知を受けた場合、対象のコード画像についてその旨を記録する（例えばフラグを立てるなど）にとどめ、コード情報の無効化までは行わないように構成されてもよい。また、情報管理部１４０は、過去にキャプチャ検知通知を受けたことが記録されているコード画像が利用者によって使用された場合、当該コード画像は画面キャプチャによって複製された可能性がある旨を、決済アプリ２０を介して当該利用者に通知するように構成されてもよい。また、情報管理部１４０は、コード画像の用途が決済である場合、当該決済の対象の加盟店の情報や決済金額などを当該コード情報に紐づけて記録するように構成されてもよい。この場合、情報管理部１４０は、コード画像が画面キャプチャによって複製された可能性がある旨を利用者に通知する際、当該コード画像を用いて過去に実施された決済に関する情報（例えば決済が実施された加盟店や決済金額など）を利用者に提示するように構成されてもよい。

【００５３】

決済サーバ１００は、コード画像の画面キャプチャ不正利用の試みが検知された場合、当該試みが実施された利用者端末装置１０の決済アプリ２０と協働して、当該利用者端末装置１０に関する情報を取得するように構成されてもよい。例えば、利用者端末装置１０がＧＰＳ（Global Positioning System）等の位置情報取得機能を有している場合、決済サーバ１００は決済アプリ２０と協働して、利用者端末装置１０の位置情報を取得するように構成されてもよい。また、例えば、利用者端末装置１０がカメラを有している場合、決済サーバ１００は決済アプリ２０と協働してカメラを作動させることにより、利用者端末装置１０の周辺が撮像された画像データを取得するように構成されてもよい。また、例えば、利用者端末装置１０がマイクを有している場合、決済サーバ１００は決済アプリ２０と協働して録音機能を作動させることにより、利用者端末装置１０の周辺の音声録音された音声データを取得するように構成されてもよい。

【００５４】

実施形態では、決済アプリ２０がコード画像をデコードしてコード情報を読み取るものとしたが、コード画像のデコードは決済サーバ１００が実施してもよい。この場合、決済アプリ２０はコード画像からコード情報を読み取る代わりにコード画像を撮像し、撮像したコード画像を決済サーバ１００に送信してもよい。

【００５５】

決済アプリ２０が表示する画面の制御（表示内容の切替えのための判定処理およびレンダリング）は、専ら決済アプリ２０が行うものであってもよいし、決済アプリ２０と決済サーバ１００が協働して行うものであってもよいし、専ら決済サーバ１００が行うものであってもよい。

【００５６】

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】

【００５７】

1 0 利用者端末装置
2 0 決済アプリ
3 0 第2の利用者端末装置
5 0 第1店舗端末装置
6 0 店舗コード画像
7 0 第2店舗端末装置
7 2 加盟店向けインターフェース
1 0 0 決済サーバ
1 1 0 通信部
1 2 0 決済コンテンツ提供部
1 3 0 決済処理部
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 店舗情報
1 7 8 コード関連情報

【要約】

【課題】コード情報を用いた認証処理のセキュリティを向上させ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。

【解決手段】利用者の端末装置で動作するアプリと協働して利用者にサービスを提供する装置であって、アプリによりコード画像を提示した利用者に対して前記サービスを提供するサービス提供部と、前記コード画像の有効性を管理する管理部と、利用者が提示したコード画像から読み取られたコード情報に基づいて前記サービスの不正利用を検知する検知部と、を備え、前記管理部は、前記端末装置において前記コード画像を複製する操作が行われたことを示す複製通知がアプリから受信された場合、前記操作による複製の対象となったコード画像を無効化し、前記検知部は、前記サービスの利用に際して受信されたコード情報が無効化されている場合、前記サービスの利用が不正利用であると判定する、サービス提供装置。

【選択図】図4

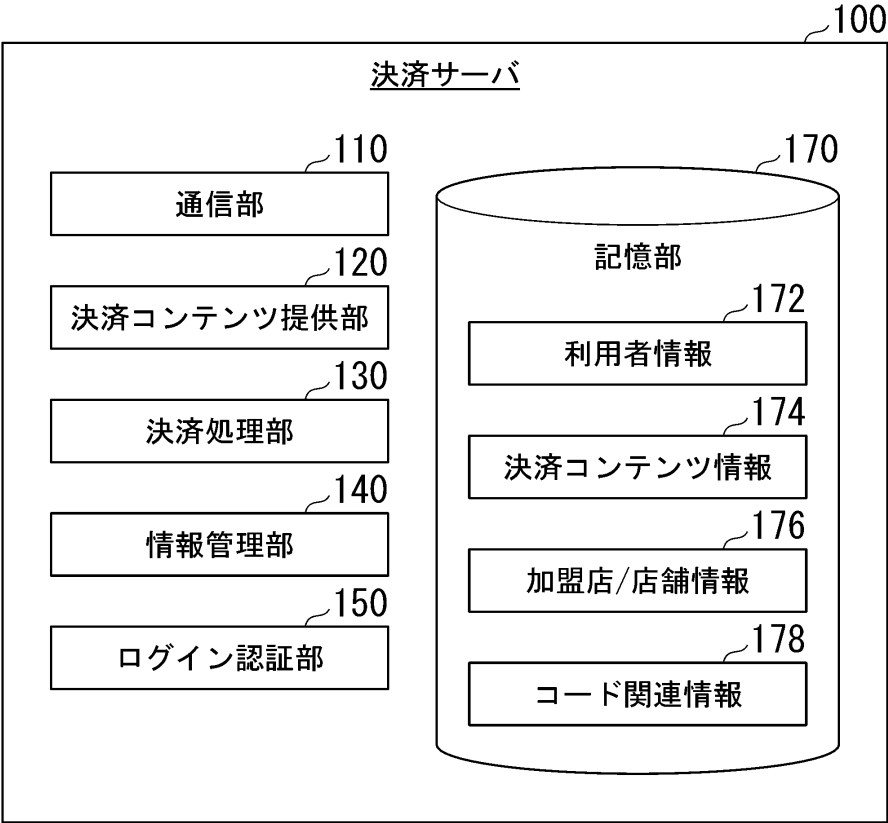
10

20

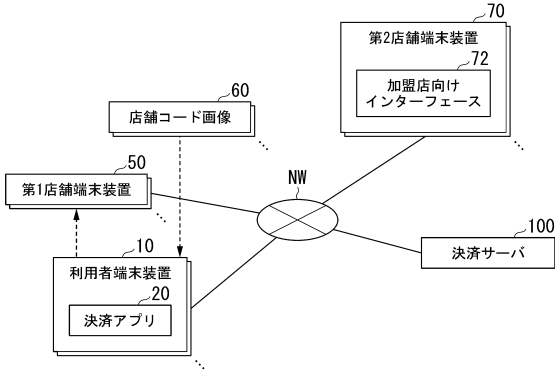
30

40

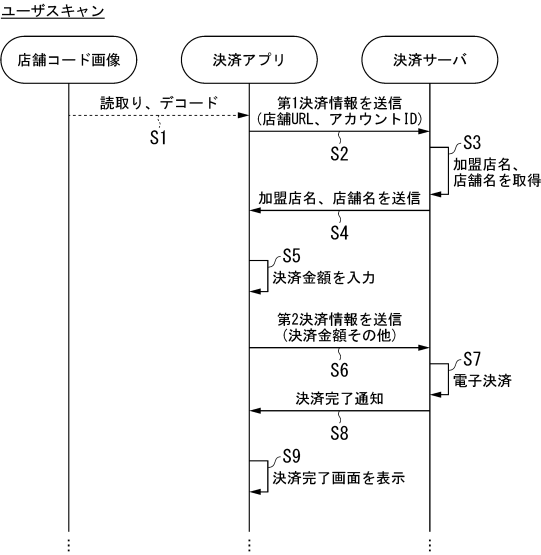
50



【図面】
【図 1】



【図 2】



10

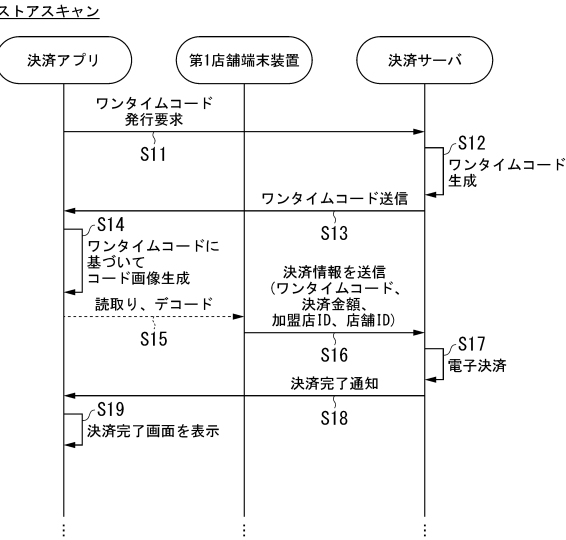
20

30

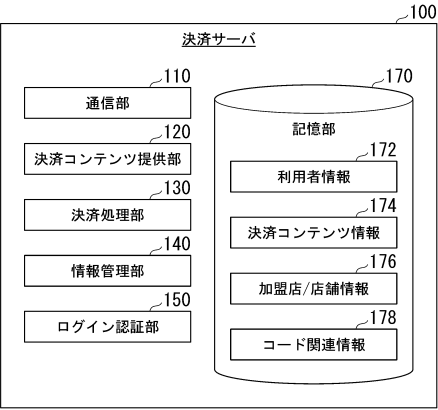
40

50

【図 3】



【図 4】



10

【図 5】

172	加盟店URL	利用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	チャージ残高
	https://...	https://...	001	090-****-****	AAA1234	**@****.***	AAA	...	2020/6/4	19000
	https://...	https://...	002	070-****-****	BBB8976	**@****.***	-	...	2015/7/11	6400
	...	...	...	...	...	...	...	...	...	...

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 チャージ履歴1	決済履歴情報 決済履歴1	...	...	...	...
済	20000	5600	14400	後払い	...	...	...	...	...	...	...	...
済	15000	3200	11800	チャージ残高	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...	...	...	...

【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	
	...	...	

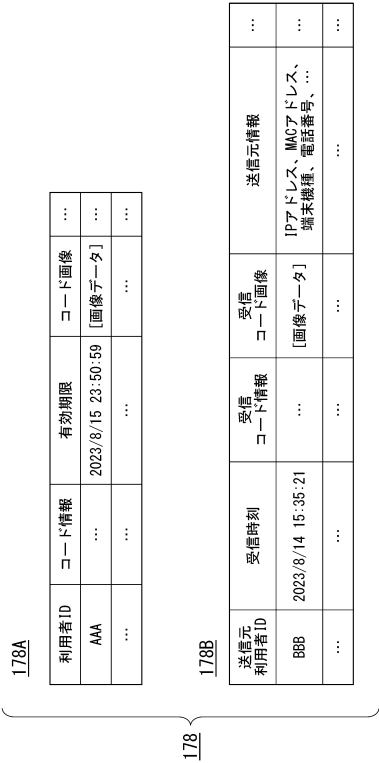
20

30

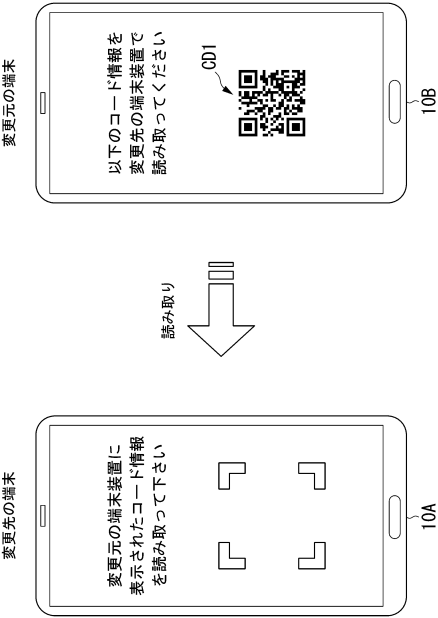
40

50

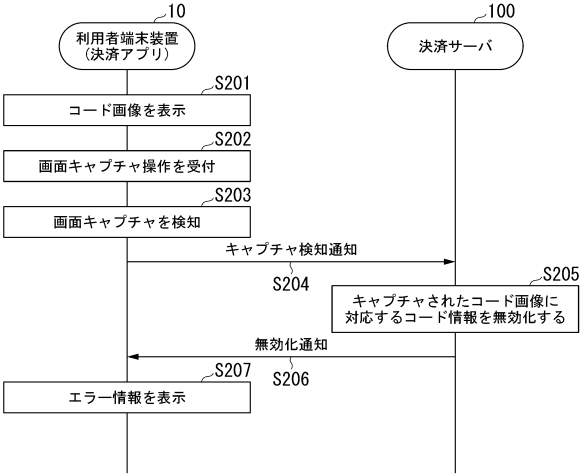
【図 7】



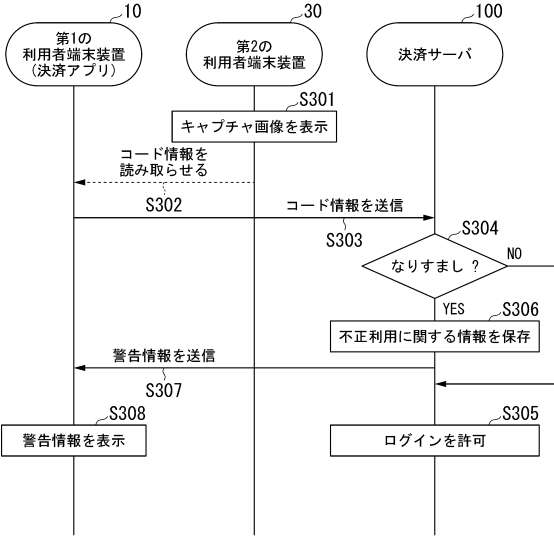
【図 8】



【図 9】



【図 10】



10

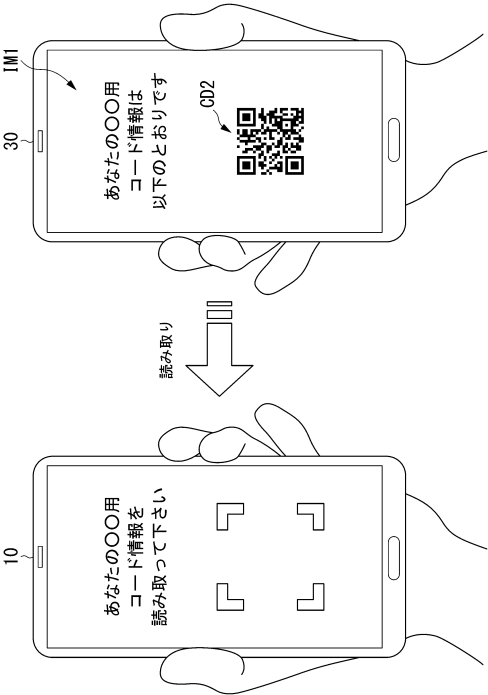
20

30

40

50

【図 1 1】



10

20

30

40

50

フロントページの続き

- (56)参考文献 中国特許出願公開第112948869 (CN, A)
特開2022-072446 (JP, A)
米国特許出願公開第2015/0052065 (US, A1)
特開2022-099434 (JP, A)
特開2018-045418 (JP, A)
中国特許出願公開第115222002 (CN, A)
中国特許出願公開第113860094 (CN, A)

- (58)調査した分野 (Int.Cl., DB名)
G06F12/14、21/00-21/88
G06K7/00-7/14
G06K19/00-19/18
G06Q10/00-99/00
G09C1/00-5/00
H04K1/00-3/00
H04L9/00-9/40
H04M3/00、3/16-3/20
H04M3/38-3/58
H04M7/00-7/16
H04M11/00-11/10
H04N7/10、7/14-7/173
H04N7/20-7/56
H04N21/00-21/858