

(19) 日本国特許庁(JP)

再公表特許(A1)

(11) 国際公開番号

W02018/096772

発行日 令和1年10月17日 (2019.10.17)

(43) 国際公開日 平成30年5月31日 (2018.5.31)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/32 (2013.01)	G06F 21/32	
G06F 21/44 (2013.01)	G06F 21/44	

審査請求 未請求 予備審査請求 未請求 (全 29 頁)

<p>出願番号 特願2018-552429 (P2018-552429)</p> <p>(21) 国際出願番号 PCT/JP2017/033754</p> <p>(22) 国際出願日 平成29年9月19日 (2017.9.19)</p> <p>(31) 優先権主張番号 特願2016-226581 (P2016-226581)</p> <p>(32) 優先日 平成28年11月22日 (2016.11.22)</p> <p>(33) 優先権主張国・地域又は機関 日本国 (JP)</p>	<p>(71) 出願人 000002185 ソニー株式会社 東京都港区港南1丁目7番1号</p> <p>(74) 代理人 110002147 特許業務法人酒井国際特許事務所</p> <p>(72) 発明者 王 啓宏 東京都港区港南1丁目7番1号 ソニー株式会社内</p> <p>(72) 発明者 倉田 雅友 東京都港区港南1丁目7番1号 ソニー株式会社内</p> <p>(72) 発明者 白井 太三 東京都港区港南1丁目7番1号 ソニー株式会社内</p>
---	---

最終頁に続く

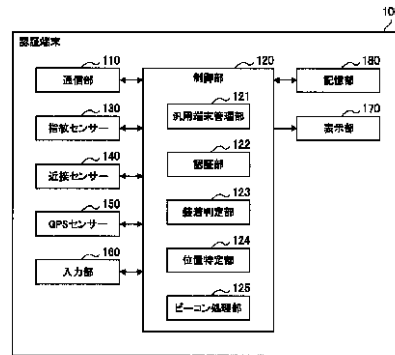
(54) 【発明の名称】 情報処理端末、情報処理装置、情報処理方法、情報処理システムおよびプログラム

(57) 【要約】

【課題】 生体認証に用いられる生体情報を一元化することを可能にする。

【解決手段】 生体認証のための生体情報および、サービスが提供される装置の識別情報を取得する取得部と、前記生体認証の成功に応じて、前記識別情報を送信する送信部と、を備える、情報処理端末が提供される。

【選択図】 図3



- 100 Authentication terminal
- 110 Communication unit
- 120 Control unit
- 121 General terminal management unit
- 122 Authentication unit
- 123 Mounting assessment unit
- 124 Position identification unit
- 125 Beacon processing unit
- 130 Fingerprint sensor
- 140 Proximity sensor
- 150 GPS sensor
- 160 Input unit
- 170 Display unit
- 180 Storage unit

- 【特許請求の範囲】
- 【請求項 1】
生体認証のための生体情報および、サービスが提供される装置の識別情報を取得する取得部と、
前記生体認証の成功に応じて、前記識別情報を送信する送信部と、を備える、
情報処理端末。
- 【請求項 2】
前記送信部は、前記生体認証の成功に応じて、前記情報処理端末の識別情報も送信する、
請求項 1 に記載の情報処理端末。 10
- 【請求項 3】
前記取得部が、前記装置からの入力に基づく承認要求を取得した場合、
前記送信部は、前記生体認証の対象ユーザの承認に関する操作に基づいて承認結果を送信する、
請求項 2 に記載の情報処理端末。
- 【請求項 4】
前記情報処理端末は、前記生体認証の対象ユーザに装着される端末である、
請求項 1 に記載の情報処理端末。
- 【請求項 5】
前記取得部は、前記情報処理端末が前記対象ユーザに装着される際に、前記生体情報を取得する、
請求項 4 に記載の情報処理端末。 20
- 【請求項 6】
前記生体情報は、指紋情報である、
請求項 1 に記載の情報処理端末。
- 【請求項 7】
前記生体認証を行う認証部をさらに備える、
請求項 1 に記載の情報処理端末。
- 【請求項 8】
生体認証のための生体情報および、サービスが提供される装置の識別情報を取得することと、
前記生体認証の成功に応じて、前記識別情報を送信することと、を有する、
コンピュータにより実行される情報処理方法。 30
- 【請求項 9】
生体認証のための生体情報および、サービスが提供される装置の識別情報を取得することと、
前記生体認証の成功に応じて、前記識別情報を送信することと、
をコンピュータに実現させるためのプログラム。
- 【請求項 10】
生体認証の成功に応じて、前記生体認証のための生体情報を取得した第 1 の装置から提供される、第 2 の装置の識別情報を取得する取得部と、
前記第 2 の装置の識別情報に基づいて前記第 2 の装置へサービスを提供するサービス提供部と、を備える、
情報処理装置。 40
- 【請求項 11】
前記取得部は、前記生体認証の成功に応じて、前記第 1 の装置の識別情報も取得し、
前記第 1 の装置の識別情報および前記第 2 の装置の識別情報に対応付けて記憶する記憶部をさらに備える、
請求項 10 に記載の情報処理装置。
- 【請求項 12】 50

前記取得部が、前記第 2 の装置からの入力情報を取得した場合、
前記サービス提供部は、前記第 2 の装置と識別情報が相互に対応付けられている前記第 1 の装置からの承認結果に基づいて前記第 2 の装置へサービスを提供する、
請求項 1 1 に記載の情報処理装置。

【請求項 1 3】

前記取得部は、前記第 1 の装置の位置情報を取得し、
前記サービス提供部は、前記位置情報に基づいて、前記第 1 の装置と識別情報が相互に対応付けられている前記第 2 の装置へサービスを提供する、
請求項 1 1 に記載の情報処理装置。

【請求項 1 4】

前記取得部は、複数の第 1 の装置の位置関係情報を取得し、
前記サービス提供部は、前記位置関係情報に基づいて、前記複数の第 1 の装置と識別情報が相互に対応付けられている前記第 2 の装置へサービスを提供する、
請求項 1 3 に記載の情報処理装置。

【請求項 1 5】

前記取得部が、前記第 2 の装置から入力された、他の第 2 の装置への権限付与に関する入力情報を取得した場合、
前記サービス提供部は、前記他の第 2 の装置への権限付与に関する処理を行う、
請求項 1 0 に記載の情報処理装置。

【請求項 1 6】

前記サービス提供部は、ショッピングに関するサービス、決済に関するサービス、商品の受取人変更に関するサービスまたは、クーポンに関するサービスを提供する、
請求項 1 0 に記載の情報処理装置。

【請求項 1 7】

サービスを提供する情報処理装置と、生体認証に関する処理を行う第 1 の装置と、前記サービスが提供される第 2 の装置と、を備え、

前記第 1 の装置は、

前記生体認証のための生体情報および、前記第 2 の装置の識別情報を取得する取得部と

、

前記生体認証の成功に応じて、前記識別情報を送信する送信部と、を備え、

前記情報処理装置は、

前記生体認証の成功に応じて、前記第 1 の装置から提供される前記識別情報を取得する識別情報取得部と、

前記識別情報に基づいて前記第 2 の装置へサービスを提供するサービス提供部と、を備える、

情報処理システム。

【発明の詳細な説明】

【技術分野】

【0001】

本開示は、情報処理端末、情報処理装置、情報処理方法、情報処理システムおよびプログラムに関する。

【背景技術】

【0002】

近年、生体認証の技術が様々な装置またはシステム等に活用されている。例えば、特許文献 1 には、指紋認証機能を各種装置に付加させる技術が開示されている。

【0003】

また、ユーザがサービス等を利用する際にも生体認証の技術が活用されるケースが増加している。例えば、ユーザが PC (Personal Computer) またはスマートフォンを用いて所望のアプリケーションサービスを利用する際、生体認証によって当該アプリケーションサービスへのログインが行われるケース等が挙げられる。

10

20

30

40

50

【先行技術文献】

【特許文献】

【0004】

【特許文献1】特許第3951920号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかし、上記のケースにおいて、生体認証に用いられる生体情報を一元化することができなかつた。例えば、ユーザは、生体認証に用いられる生体情報を含むユーザに関する情報（以降、便宜的に「ユーザ情報」とも呼称する）をサービス毎に登録し、サービスを利用する度に生体認証によるログインを行わなければならない場合がある。この場合、ユーザに対して、ユーザ情報の登録および認証等の負荷がかかる。他方、サービス運営者に対しては、ユーザ情報の管理等の負荷がかかる。さらに、サービス毎にユーザ情報が散在することによって、ユーザ情報が漏洩するリスクも発生する。

10

【0006】

そこで、本開示は、上記に鑑みてなされたものであり、本開示は、生体認証に用いられる生体情報を一元化することが可能な、新規かつ改良された情報処理端末、情報処理装置、情報処理方法、情報処理システムおよびプログラムを提供する。

【課題を解決するための手段】

【0007】

本開示によれば、生体認証のための生体情報および、サービスが提供される装置の識別情報を取得する取得部と、前記生体認証の成功に応じて、前記識別情報を送信する送信部と、を備える、情報処理端末が提供される。

20

【0008】

また、本開示によれば、生体認証のための生体情報および、サービスが提供される装置の識別情報を取得することと、前記生体認証の成功に応じて、前記識別情報を送信することと、を有する、コンピュータにより実行される情報処理方法が提供される。

【0009】

また、本開示によれば、生体認証のための生体情報および、サービスが提供される装置の識別情報を取得することと、前記生体認証の成功に応じて、前記識別情報を送信することと、をコンピュータに実現させるためのプログラムが提供される。

30

【0010】

また、本開示によれば、生体認証の成功に応じて、前記生体認証のための生体情報を取得した第1の装置から提供される、第2の装置の識別情報を取得する取得部と、前記第2の装置の識別情報に基づいて前記第2の装置へサービスを提供するサービス提供部と、を備える、情報処理装置が提供される。

【0011】

また、本開示によれば、サービスを提供する情報処理装置と、生体認証に関する処理を行う第1の装置と、前記サービスが提供される第2の装置と、を備え、前記第1の装置は、前記生体認証のための生体情報および、前記第2の装置の識別情報を取得する取得部と、前記生体認証の成功に応じて、前記識別情報を送信する送信部と、を備え、前記情報処理装置は、前記生体認証の成功に応じて、前記第1の装置から提供される前記識別情報を取得する識別情報取得部と、前記識別情報に基づいて前記第2の装置へサービスを提供するサービス提供部と、を備える、情報処理システムが提供される。

40

【発明の効果】

【0012】

以上説明したように本開示によれば、生体認証に用いられる生体情報を一元化することができる。

【0013】

なお、上記の効果は必ずしも限定的なものではなく、上記の効果とともに、または上記

50

の効果に代えて、本明細書に示されたいずれかの効果、または本明細書から把握され得る他の効果が奏されてもよい。

【図面の簡単な説明】

【0014】

【図1】本開示の背景について説明するための情報システムの構成図である。

【図2】本実施形態に係る情報処理システムの構成を示す図である。

【図3】本実施形態に係る認証端末の機能構成を示す図である。

【図4】本実施形態に係る汎用端末の機能構成を示す図である。

【図5】本実施形態に係る店舗サーバの機能構成を示す図である。

【図6】本実施形態に係るアカウント決済サーバの機能構成を示す図である。

10

【図7】認証端末による認証動作を示すフローチャートである。

【図8】本実施形態に係る情報処理システムを用いて商品を注文する場合の動作を示すシーケンス図である。

【図9】本実施形態に係る情報処理システムを用いて商品の受取人を変更する場合の動作を示すシーケンス図である。

【図10】本実施形態に係る情報処理システムを用いてクーポンを発行する場合の動作を示すシーケンス図である。

【図11】本実施形態に係る装置のハードウェア構成を示す図である。

【発明を実施するための形態】

【0015】

20

以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

【0016】

なお、説明は以下の順序で行うものとする。

1. 背景
2. 情報処理システムの概要
3. 装置の機能構成
4. 装置の動作
5. ハードウェア構成
6. むすび

30

【0017】

< 1. 背景 >

まず、図1を参照して、本開示の背景について説明する。図1は、本開示の背景について説明するための情報システムの構成図である。ここでは、一例として、当該情報処理システムがショッピングサービスシステムであるケースについて説明する。

【0018】

図1に示すように、当該情報処理システムは、汎用端末1と、店舗サーバ2と、決済サーバ3と、を備える。汎用端末1は、サービスの提供が行われる端末である。より具体的に説明すると、ユーザは、汎用端末1にインストールされている所定のアプリケーションを用いて店舗サーバ2にアクセスしサービスを利用することができる。その際、ユーザは、生体認証によるログインを行うこととする。店舗サーバ2は、店舗等に設置される装置であり、汎用端末1がアクセスするショッピングサイト等のアプリケーションを制御している。決済サーバ3は、ショッピングサービスの決済処理等を行う装置である。決済サーバ3は、ユーザのクレジットカード情報等を保持しており、ユーザがショッピングサービスにて商品を注文した場合、当該クレジットカード情報等を用いて決済処理を行う。

40

【0019】

ここで、図1の情報処理システムにおいては、生体認証に用いられる生体情報を一元化することができないため、ユーザは、店舗毎（「サービス毎」と等価）に生体情報を含むユーザ情報を登録しなければならない。より具体的に説明すると、ユーザは、ショッピン

50

グを行う店舗毎にユーザの属性情報（氏名、年齢、連絡先、住所等）、クレジットカード情報（種類、番号、有効期限等）および生体情報等を登録しなければならない。これらの登録作業は、相当量の時間を要し煩雑であるため、登録作業がユーザに与える負荷は小さくない。また、各店舗での登録内容が同一または類似である場合が多く、ユーザは同一または類似の内容を複数回登録することになるため、登録作業がユーザに与える心理的負荷も小さくない。また、登録されたユーザ情報は各店舗の店舗サーバ2で管理されることになるため、セキュリティレベルが低い店舗が存在する場合、ユーザ情報が漏洩する可能性がある。さらに、ユーザが店舗毎にユーザ情報を登録する際に、ユーザ情報が第三者によって不正に取得されたり、ウイルスによって拡散されたりする危険性もある。また、ユーザがサービスを利用するとき、店舗毎に認証によるログイン操作を行わなければならない。

10

【0020】

また、商品の注文後に、ユーザが店舗に来店し商品を受け取るケースにおいては、店舗サーバ2は、商品の受け渡しの際に使用される各種番号（問い合わせ番号、認証番号等）を、メール等を用いて汎用端末1へ提供することになる。このとき、上記と同様に、各種番号が第三者によって不正に取得されたり、ウイルスによって拡散されたりする危険性がある。

【0021】

そこで、本件の開示者は、上記事情に着眼して本開示を創作するに至った。本開示の一実施形態に係る情報処理システムは、生体認証を行う装置とサービスが提供される装置を分けることで、生体認証に用いられる生体情報を一元化することができる。これにより、本実施形態に係る情報処理システムは、ユーザが店舗毎にユーザ情報を登録したりログイン操作を行ったりすることなくサービスを提供することができる。したがって、各店舗はユーザ情報を管理しなくてもよいため、本実施形態に係る情報処理システムは、ユーザ情報が漏洩するリスクを低減させることができる。さらに、本実施形態に係る情報処理システムは、商品の受取人権限を付与する機能を有することにより、商品を受取るための各種番号を用いることなく商品の受け渡しを実現できる。以下に、本開示の一実施形態に係る情報処理システムの概要、装置の機能構成、装置の動作およびハードウェア構成等について説明する。

20

【0022】

< 2 . 情報処理システムの概要 >

上記では、本開示の背景について説明した。続いて、図2を参照して、本開示の一実施形態に係る情報処理システムの概要について説明する。

30

【0023】

（ 2 - 1 . 情報処理システムの概要 ）

図2は、本実施形態に係る情報処理システムの構成を示す図である。図2に示すように、本実施形態に係る情報処理システムは、認証端末100と、汎用端末200と、店舗サーバ300と、アカウント決済サーバ400と、を備える。図2に示すように、認証端末100と汎用端末200、認証端末100とアカウント決済サーバ400、汎用端末200と店舗サーバ300は、互いに無線通信を行う。また、店舗サーバ300とアカウント決済サーバ400は、ネットワーク500によって接続されている。ここで、上記の通信接続形態はあくまで一例であり、各装置の通信接続形態は任意である。また、本明細書では、情報処理システムが上記の構成を備える例について説明するが、店舗サーバ300とアカウント決済サーバ400の機能は、1台の装置に集約されてもよいし、3台以上の装置に分散されてもよい。

40

【0024】

本実施形態に係る情報処理システムは、様々であり得る。例えば、本実施形態に係る情報処理システムは、ユーザが商品を注文できるショッピングサービス、予約サービス（ホテルの予約、レンタカーの予約等）、シェアリング・エコノミーに関するサービス（カーシェアリング、民泊等）等のシステムであってもよい。ここで、本明細書では、主に、本

50

実施形態に係る情報処理システムがショッピングサービスシステムである場合の例について説明する。

【0025】

(2-2. 認証端末100の概要)

本実施形態に係る認証端末100は、生体認証を行う情報処理端末(第1の装置とも呼称する)である。より具体的に説明すると、認証端末100は、生体情報を取得するための構成を備えており、取得した生体情報と予め登録されている生体情報を比較することで生体認証を行う。

【0026】

認証端末100の種類は任意であるが、本明細書では、認証端末100が、生体認証の対象ユーザが装着するブレスレット型のウェアラブル端末である場合の例について説明する。ここで、認証端末100がウェアラブル端末であることによって、セキュリティを向上させることができる。より具体的に説明すると、認証端末100がウェアラブル端末であることによって、ユーザが認証端末100を外すと、認証状態を、認証が行われた状態から認証が行われていない状態へ変化させることができる。これによって、認証端末100は、第三者が認証後の認証端末100を不正に取得し、悪用することを防ぐことができる。

10

【0027】

なお、本明細書では、生体認証が認証端末100によって行われる例について説明するが、生体認証は、認証端末100以外の端末によって行われてもよい。例えば、認証端末100は、生体情報を取得し当該情報をアカウント決済サーバ400へ送信することで、アカウント決済サーバ400が生体認証を行ってもよい。

20

【0028】

上記のとおり、認証端末100がブレスレット型のウェアラブル端末であることはあくまで一例であり、認証端末100は、メガネ型の装置、時計型の装置、指輪型の装置、衣服型の装置でもよく、ウェアラブル端末でなくてもよい。

【0029】

また、本明細書では、生体認証として指紋認証が用いられる例を主に説明するが、生体認証の種類は任意である。例えば、生体認証として、静脈認証、虹彩認証、声紋認証、顔認証等が用いられてもよい。

30

【0030】

また、認証端末100は、サービス利用に用いられる汎用端末200の識別情報を取得する。例えば、サービスの利用開始時に汎用端末200の所定のアプリケーションが起動されたことをトリガに、認証端末100は、汎用端末200との無線通信によって、汎用端末200の識別情報を含む接続要求情報を取得し、接続処理を行う。そして、認証端末100は、認証端末100の識別情報および汎用端末200の識別情報をアカウント決済サーバ400へ送信する。

【0031】

これによって、サービス提供を行うアカウント決済サーバ400は、指紋認証を行う認証端末100とサービス提供先の端末である汎用端末200とを対応付けて記憶することができ、ユーザは、サービスを利用するときにログインを行わなくてもよくなる。より具体的に説明すると、本実施形態に係る情報処理システムは、指紋認証の成功後に、指紋認証を行った認証端末100と汎用端末200が対応付けられた状態でアカウント決済サーバ400に記憶されていることに基づいて、ログインと等価な処理が行われたと判断し、ユーザが汎用端末200を用いてサービスを利用することを可能にすることができる。

40

【0032】

なお、認証端末100は上記以外の機能を有していてもよい。例えば、認証端末100は、決済機能(クレジットカード型決済、プリペイド型決済等)、ユーザの行動計測機能(歩数、移動距離、消費カロリーの計測機能等)、時計機能、メール機能等を有していてもよい。

50

【 0 0 3 3 】

(2 - 3 . 汎用端末 2 0 0 の概要)

本実施形態に係る汎用端末 2 0 0 は、ユーザがサービスを利用する際に使用する端末（第 2 の装置とも呼称する）である。より具体的に説明すると、ユーザは、汎用端末 2 0 0 にインストールされている所定のアプリケーションを用いて店舗サーバ 3 0 0 にアクセスし、サービスを利用することができる。例えば、ユーザは、汎用端末 2 0 0 を用いて商品の注文、商品の受取人の変更等を行うことができる。なお、汎用端末 2 0 0 の種類は任意である。例えば、汎用端末 2 0 0 は、ノート PC、タブレット PC、スマートフォン、携帯型ゲーム端末またはデジタルカメラ等、通信機能を有している装置であれば任意の装置でよい。

10

【 0 0 3 4 】

(2 - 4 . 店舗サーバ 3 0 0 の概要)

本実施形態に係る店舗サーバ 3 0 0 は、店舗等に設置される装置であり、商品の注文等に関する処理、受取人変更に関する処理等を行う。商品の注文等に関する処理について具体的に説明すると、ユーザが汎用端末 2 0 0 を用いて商品を注文した場合、店舗サーバ 3 0 0 は、注文情報を汎用端末 2 0 0 から受信し、当該注文情報をアカウント決済サーバ 4 0 0 へ送信する。アカウント決済サーバ 4 0 0 による処理が行われた後、店舗サーバ 3 0 0 は、注文の成否に関する情報を汎用端末 2 0 0 へ送信することで、当該ユーザへ通知する。

20

【 0 0 3 5 】

続いて、受取人変更に関する処理について具体的に説明すると、ユーザが商品を注文した際、店舗サーバ 3 0 0 は、アカウント決済サーバ 4 0 0 からユーザの家族情報を取得し、家族が登録されている場合、受取人変更の有無を確認する。ユーザによって受取人が変更された場合、店舗サーバ 3 0 0 は、受取人変更情報（受取人変更の有無情報、受取人として設定されたユーザの識別番号等）をアカウント決済サーバ 4 0 0 へ送信する。これによって、アカウント決済サーバ 4 0 0 は、受取人に指定されたユーザを把握し当該ユーザの認証端末 1 0 0 に対して受取人権限情報を提供することができる。

【 0 0 3 6 】

そして、受取人が来店し、所定の装置に認証端末 1 0 0 を接近または接触させた場合、店舗サーバ 3 0 0 は、当該装置を介して認証端末 1 0 0 から受取人権限情報（商品の識別情報、購入日時、購入者属性、受取人属性、認証端末 1 0 0 の識別情報等）を取得する。その後、店舗サーバ 3 0 0 は、アカウント決済サーバ 4 0 0 に対して受取人権限情報を送信することで、アカウント決済サーバ 4 0 0 によって当該ユーザが事前に設定された受取人であるか否かの判定が行われる。これにより、ユーザは、各種番号（問い合わせ番号、認証番号等）を用いることなく、受取人であることの証明を行うことができる。すなわち、各種番号が第三者によって不正に取得されたり、ウィルスによって拡散されたりする危険性を低減させることができる。

30

【 0 0 3 7 】

(2 - 5 . アカウント決済サーバ 4 0 0 の概要)

本実施形態に係るアカウント決済サーバ 4 0 0 は、各種情報の管理、商品の注文等に関する処理、受取人変更に関する処理、クーポン発行に関する処理等を行う情報処理装置である。各種情報の管理について具体的に説明すると、アカウント決済サーバ 4 0 0 は、ユーザの属性情報（氏名、年齢、連絡先、住所等）、クレジットカード情報（カード番号情報、履歴情報等）、家族情報（家族構成、家族の属性情報、家族の認証端末 1 0 0 の識別情報等）、友人情報（友人の属性情報、友人の認証端末 1 0 0 の識別情報等）、行動履歴情報、購買履歴情報等を管理する。また、上記のとおり、アカウント決済サーバ 4 0 0 は、認証端末 1 0 0 から受信した、認証端末 1 0 0 の識別情報と汎用端末 2 0 0 の識別情報に対応付けて管理する。さらに、アカウント決済サーバ 4 0 0 は、認証端末 1 0 0 から受信した認証状態に関する情報を管理する。

40

【 0 0 3 8 】

50

本実施形態に係る情報処理システムにおいては、各店舗サーバ300がユーザ情報を含む各種情報を個別に管理するのではなく、アカウント決済サーバ400がこれらの情報を一元管理する。これによって、本実施形態に係る情報処理システムは、ユーザ情報等の漏洩のリスクを低減させることができる。

【0039】

また、商品の注文等に関する処理について具体的に説明すると、ユーザが商品を注文した場合、アカウント決済サーバ400は、店舗サーバ300から注文情報（商品、価格、注文日時、注文を行った汎用端末200の識別情報等）を受信する。そして、アカウント決済サーバ400は、指紋認証が成功した認証端末100と対応付けて管理している汎用端末200の識別情報の中から、注文を行った汎用端末200の識別情報と一致する識別番号を探す。

10

【0040】

注文を行った汎用端末200の識別情報と一致する識別番号が存在する場合には、アカウント決済サーバ400は、当該識別情報に対応付けられている認証端末100に対して承認要求を送信する。これによって、アカウント決済サーバ400は、ユーザに対して注文への承認を要求する。ユーザが注文を承認した場合、アカウント決済サーバ400は、当該注文を確定し決済処理等を行う。ユーザが注文を承認しない場合、アカウント決済サーバ400は当該注文を受け付けない。これによって、アカウント決済サーバ400は、第三者による不正な注文が確定すること等を防ぐことができる。より具体的に説明すると、指紋認証が成功した後に、第三者が汎用端末200を不正に取得し注文を行ったとしても、ユーザは、認証端末100を用いて当該注文を承認しないことで注文の確定を防ぐことができる。

20

【0041】

なお、アカウント決済サーバ400は、認証端末100と汎用端末200が所定の距離以上離れた場合、汎用端末200からの注文を受け付けない等の制御を行うことで、第三者による不正注文へ対応してもよい。これによって、アカウント決済サーバ400は、ユーザが非承認操作を行わなくても不正注文へ対応することができる。

【0042】

続いて、受取人変更に関する処理について具体的に説明すると、アカウント決済サーバ400は、ユーザが汎用端末200を用いて商品を注文したとき、当該ユーザの家族情報を店舗サーバ300へ送信する。これによって、店舗サーバ300がユーザに対して受取人の変更有無を確認することができる。受取人が変更された場合、アカウント決済サーバ400は、店舗サーバ300から受取人変更情報を受信し、受取人として指定されたユーザの認証端末100へ受取人の権限情報を送信する。これによって、受取人の権限情報が受取人の認証端末100に記憶される。そして、受取人として指定されたユーザが来店し商品を受取る際には、アカウント決済サーバ400は、来店したユーザの認証端末100から取得された受取人権限情報に基づいて、当該ユーザが事前に設定された受取人であるか否かの判定を行い、判定結果情報を店舗サーバ300に対して送信する。これによって、本実施形態に係る情報処理システムは、受取人の変更を誤りなく適切に行うことができる。

30

40

【0043】

続いて、クーポン発行に関する処理について具体的に説明すると、アカウント決済サーバ400は、店舗に来店したユーザとその同伴者の情報を取得する。例えば、店舗にビーコン端末が設置されており、当該ビーコン端末は定期的にビーコンを発信するとする。そして、来店していたユーザおよびその同伴者の認証端末100がビーコンを受信した場合、これらの認証端末100は、ビーコン受信情報（ビーコン端末の識別情報、受信電波強度、受信時刻等）をアカウント決済サーバ400へ送信する。そして、アカウント決済サーバ400は、ビーコン受信情報と、自装置が管理している家族情報または友人情報に基づいて、ユーザがその家族または友人を同伴させて来店したことを把握することができる。

50

【 0 0 4 4 】

その後、例えば、ユーザが店舗にて商品を購入した場合、アカウント決済サーバ400は、当該情報を取得し、商品を購入したユーザおよび同伴者の認証端末100に対してクーポンを発行する。アカウント決済サーバ400は、認証端末100に対してクーポンを発行することで、発行対象者以外がクーポンを使用することを防ぐことができる。より具体的に説明すると、認証端末100は、ユーザに装着されることによって本人を認証することができるため、アカウント決済サーバ400は、認証なしに第三者が認証端末100のクーポンを利用することを防ぐことができる。なお、クーポンが発行される条件は任意である。例えば、ユーザが来店して商品を購入するのではなく、任意の場所で汎用端末200を用いて商品を購入した場合においても、アカウント決済サーバ400はクーポンを

10

【 0 0 4 5 】

< 3 . 装置の機能構成 >

上記では、本実施形態に係る情報処理システムの概要について説明した。続いて、図3～図6を参照して、本実施形態に係る各装置の機能構成について説明する。

【 0 0 4 6 】

(3 - 1 . 認証端末100の機能構成)

まず、図3を参照して、認証端末100の機能について説明する。図3は、本実施形態に係る認証端末100の機能構成を示す図である。図3に示すように、本実施形態に係る認証端末100は、通信部110と、制御部120と、指紋センサー130と、近接センサー140と、GPS (Global Positioning System) センサー150と、入力部160と、表示部170と、記憶部180と、を備える。また、制御部120は、汎用端末管理部121と、認証部122と、装着判定部123と、位置特定部124と、ビーコン処理部125と、を備える。通信部110は送信部としても機能し、制御部120は取得部としても機能する。

20

【 0 0 4 7 】

(通信部110)

通信部110は、汎用端末200およびアカウント決済サーバ400との通信を行う。汎用端末200との通信について具体的に説明すると、通信部110は、汎用端末200から接続要求情報を受信すると、当該情報を制御部120へ提供する。制御部120による接続処理が完了した後、通信部110は、接続完了情報を汎用端末200へ送信する。

30

【 0 0 4 8 】

また、アカウント決済サーバ400との通信について具体的に説明すると、指紋認証が成功し、自装置と汎用端末200の接続処理が完了した場合に、通信部110は、汎用端末200および自装置の識別情報をアカウント決済サーバ400へ送信する。

【 0 0 4 9 】

その後、ユーザが汎用端末200を用いて商品の注文を行った場合には、通信部110は、アカウント決済サーバ400から当該注文に対する承認要求を受信する。そして、通信部110は、ユーザによって承認または否認が行われた後に、これらの承認結果情報をアカウント決済サーバ400へ送信する。また、通信部110は、上記以外にも例えば、受取人の変更、クーポン発行等に関する通信をアカウント決済サーバ400に対して行う。また、通信部110は、ビーコン端末から送信されたビーコンを受信することも可能である。

40

【 0 0 5 0 】

(制御部120)

制御部120は、認証端末100の各種処理を制御する。以下に、制御部120が備える汎用端末管理部121、認証部122、装着判定部123および位置特定部124に関

50

する機能について説明する。なお、制御部 120 が有する機能は、以下に説明する機能に限定されない。例えば、制御部 120 は、ユーザの行動計測機能（歩数、移動距離、消費カロリーの計測機能等）、時計機能、メール機能等を制御してもよい。

【0051】

（汎用端末管理部 121）

汎用端末管理部 121 は、汎用端末 200 の情報を管理する。より具体的に説明すると、汎用端末管理部 121 は、汎用端末 200 によって送信された、汎用端末 200 の識別情報を含む接続要求情報を取得した場合、汎用端末 200 の識別情報を管理する。なお、汎用端末管理部 121 は、複数の汎用端末 200 を管理してもよい。すなわち、ユーザが、複数の汎用端末 200 を並行して使用する場合、汎用端末管理部 121 は、当該複数の汎用端末 200 の識別情報を管理してもよい。

10

【0052】

（認証部 122）

認証部 122 は、指紋認証を行う。より具体的に説明すると、ユーザが認証端末 100 を装着する際、指紋センサー 130 が当該ユーザの指紋情報を取得し、当該情報を認証部 122 へ提供する。そして、認証部 122 は、取得した指紋情報と予め登録されているユーザの指紋情報を用いてパターンマッチングを行う。認証部 122 は、パターンマッチングによって算出された類似度が所定の値よりも高い場合、認証部 122 は、指紋認証が成功したと判定する。なお、指紋センサー 130 によって指紋情報が取得されるタイミングは任意である。また、指紋認証の方式は任意である。例えば、認証部 122 は、パターン

20

【0053】

認証部 122 は、アカウント決済サーバ 400 に対して指紋認証の成否に関する情報を送信する処理を制御する。なお、認証部 122 は、発光部（図示なし）または鳴動部（図示なし）等を制御することで、光または音等によってユーザに対して指紋認証の成否を通知してもよい。

【0054】

（装着判定部 123）

装着判定部 123 は、ユーザによる認証端末 100 の装着状態を判定する。より具体的に説明すると、装着判定部 123 は、近接センサー 140 からユーザと認証端末 100 の離隔距離に関する情報を取得し、当該情報に基づいてユーザが認証端末 100 を装着しているか否か、または、ユーザが認証端末 100 を装着しようとしているか否かを判定する。これによって、ユーザが認証端末 100 を装着する際に、指紋センサー 130 が指紋情報を取得することができる。また、装着判定部 123 は、ユーザが認証端末 100 を装着していないと判定した場合、その旨をアカウント決済サーバ 400 へ通知するための処理を行う。これによって、アカウント決済サーバ 400 は、認証状態を、認証が行われた状態から認証が行われていない状態へ変化させることができる。

30

【0055】

（位置特定部 124）

位置特定部 124 は、認証端末 100 の位置を特定する。より具体的に説明すると、位置特定部 124 は、GPS センサー 150 から GPS 信号の情報を取得し、当該情報に基づいて位置を特定する。位置特定部 124 は、特定した位置情報をアカウント決済サーバ 400 へ通知するための処理を行う。これにより、アカウント決済サーバ 400 は、ユーザが移動したルートを特定したり、店舗に来店したか否かの判定等を行ったりすることができる。

40

【0056】

（ビーコン処理部 125）

ビーコン処理部 125 は、ビーコンに関する処理を行う。より具体的に説明すると、通信部 110 がビーコン端末から送信されたビーコンを受信した場合、ビーコン処理部 12

50

5 は、ビーコン受信情報（ビーコン端末の識別情報、受信電波強度、受信時刻等）をアカウント決済サーバ400へ送信する処理を制御する。これによって、アカウント決済サーバ400は、認証端末100とビーコン端末との位置関係を把握することができる。したがって、ビーコン端末が店舗に設置されている場合、アカウント決済サーバ400は、ビーコン受信情報に基づいて認証端末100を装着したユーザが店舗に来店したか否かを推定することができる。

【0057】

なお、本明細書では、ビーコンが用いられる例を中心に説明するが、ビーコン以外の信号を用いて、信号の送信装置と認証端末100との位置関係が把握されてもよい。例えば、Bluetooth（登録商標）、赤外線または音波等の任意の信号が用いられてもよい。また、ビーコン端末が店舗等に設置されていない場合には、ビーコン処理部125がビーコンの送信処理を行ってもよい。これによって、認証端末100間でビーコンの送受信を行うことで認証端末100同士の位置関係が把握されてもよい。

10

【0058】

（指紋センサー130）

指紋センサー130は、認証端末100を装着するユーザの指紋情報を取得する。より具体的に説明すると、ユーザが認証端末100を装着する際、ユーザの指が指紋センサー130に触れることによって、指紋センサー130は、ユーザの指紋情報を取得する。指紋センサー130は、取得した指紋情報を認証部122へ提供する。ここで、指紋センサー130は、認証端末100の装着動作においてユーザの指が接触し易い箇所に位置することで、指紋認証のための準備作業を行っているという感覚をユーザの意識から除外させることができる。なお、指紋センサー130によって指紋情報が取得されるタイミングは任意である。また、指紋センサー130の種類は任意である。例えば、指紋センサー130は、光学式、静電容量方式、電解強度測定方式、感圧式または感熱式等のセンサーであってもよい。

20

【0059】

（近接センサー140）

近接センサー140は、ユーザと認証端末100の離隔距離に関する情報を取得する。より具体的に説明すると、近接センサー140は、電磁波等を放出し、ユーザが認証端末100を把持したり装着したりすること等によって生じる電磁波等の変化に基づいてユーザと認証端末100の離隔距離に関する情報を取得する。近接センサー140は、取得した離隔距離に関する情報を装着判定部123へ提供する。これにより、装着判定部123は、ユーザが認証端末100を装着しているか否か、または、ユーザが認証端末100を装着しようとしているか否かを判定することができる。なお、近接センサー140の種類は任意である。例えば、近接センサー140は、誘導式、静電容量式、超音波式または赤外線式等のセンサーであってもよい。

30

【0060】

（GPSセンサー150）

GPSセンサー150は、認証端末100の位置を特定するためのGPS信号情報を取得する。より具体的に説明すると、GPSセンサー150は、GPS衛星からのGPS信号を受信し、GPS信号情報を位置特定部124へ提供する。これにより、位置特定部124は、認証端末100の位置を判定することができる。

40

【0061】

（入力部160）

入力部160は、ユーザによる入力情報を取得する。より具体的に説明すると、入力部160はボタンまたはタッチパネル等を備えることができ、ユーザが当該ボタンまたはタッチパネル等を操作したとき、入力部160は当該操作に基づいて入力情報を生成し、制御部120に対して入力情報を提供する。これにより、制御部120は各種処理を行うことができる。

【0062】

50

(表示部 170)

表示部 170 は、各種情報を表示する。より具体的に説明すると、表示部 170 は、制御部 120 に制御されることによって、各種情報を画像、テキスト、グラフなどの多様な形式で表示することで、ユーザに対して当該情報を視覚的に通知する。当該各種の情報には多様なコンテンツが含まれ得る。

【0063】

(記憶部 180)

記憶部 180 は、各種情報を記憶する。より具体的に説明すると、記憶部 180 は、上記で説明した、自装置および汎用端末 200 の識別情報、指紋情報、GPS 信号情報、位置情報、ユーザと認証端末 100 の離隔距離に関する情報、入力情報等を記憶する。

10

【0064】

(3-2. 汎用端末 200 の機能構成)

続いて、図 4 を参照して、汎用端末 200 の機能について説明する。図 4 は、本実施形態に係る汎用端末 200 の機能構成を示す図である。図 4 に示すように、本実施形態に係る汎用端末 200 は、通信部 210 と、制御部 220 と、入力部 230 と、表示部 240 と、記憶部 250 と、を備える。

【0065】

(通信部 210)

通信部 210 は、認証端末 100 および店舗サーバ 300 との通信を行う。認証端末 100 との通信について具体的に説明すると、通信部 210 は、ユーザ操作によって自装置の所定のアプリケーションが起動されたことをトリガに、認証端末 100 に対して接続要求情報を送信する。そして、認証端末 100 と自装置の接続処理が完了した後に、通信部 210 は、認証端末 100 から接続完了情報を受信する。ここで、通信部 210 は、認証端末 100 から接続完了情報を受信できない場合、所定の回数、接続要求情報を送信してもよいし、接続完了情報を受信するまで、接続要求情報を送信してもよい。なお、通信部 210 が接続要求情報を送信するトリガは任意である。

20

【0066】

店舗サーバ 300 との通信について具体的に説明すると、通信部 210 は、ユーザによって商品等の注文が行われると、店舗サーバ 300 に対して注文情報(商品、価格、注文日時、注文を行った汎用端末 200 の識別情報等)を送信する。その後、通信部 210 は、店舗サーバ 300 から当該注文の成否に関する注文成否情報を受信する。また、通信部 110 は、上記以外にも例えば、受取人の変更に伴う各種情報等を店舗サーバ 300 と通信する。

30

【0067】

(制御部 220)

制御部 220 は、汎用端末 200 の各種処理を制御する。以下では、商品の注文に関する処理、受取人変更に関する処理について具体的に説明する。まず、商品の注文に関する処理について具体的に説明すると、制御部 220 は、店舗サーバ 300 へアクセスを行う所定のアプリケーションを制御する。また、制御部 220 は、自装置と認証端末 100 の接続のために、認証端末 100 に対して接続要求情報を送信する処理を制御する。また、ユーザが商品の注文を行った場合、店舗サーバ 300 に対して注文情報を送信する処理を制御する。

40

【0068】

受取人変更に関する処理について具体的に説明すると、制御部 220 は、ユーザが商品の注文操作を行った後に、受取人変更の有無をユーザに確認する処理を制御する。受取人が変更される場合、制御部 220 は、受取人変更情報を店舗サーバ 300 へ送信する処理を制御する。

【0069】

(入力部 230)

入力部 230 は、認証端末 100 の入力部 160 と同様に、ユーザによる入力情報を取

50

得する。入力部 230 は入力情報を生成し、制御部 220 に対して入力情報を提供する。これにより、制御部 220 は各種処理を行うことができる。

【0070】

(表示部 240)

表示部 240 は、認証端末 100 の入力部 160 と同様に、各種情報を表示する。

【0071】

(記憶部 250)

記憶部 250 は、各種情報を記憶する。より具体的に説明すると、記憶部 250 は、上記で説明した、注文情報、注文成否情報、入力情報等を記憶する。

【0072】

(3-3. 店舗サーバ 300 の機能構成)

続いて、図 5 を参照して、店舗サーバ 300 の機能について説明する。図 5 は、本実施形態に係る店舗サーバ 300 の機能構成を示す図である。図 5 に示すように、本実施形態に係る店舗サーバ 300 は、通信部 310 と、制御部 320 と、記憶部 330 と、を備える。

【0073】

(通信部 310)

通信部 310 は、汎用端末 200 およびアカウント決済サーバ 400 との通信を行う。汎用端末 200 との通信について具体的に説明すると、通信部 310 は、商品の注文に伴って注文情報および注文成否情報を汎用端末 200 と通信する。また、通信部 310 は、受取人の変更に伴って受取人変更情報等を汎用端末 200 と通信する。

【0074】

アカウント決済サーバ 400 との通信について具体的に説明すると、通信部 310 は、商品の注文に伴って注文情報および注文に対するユーザの承認結果情報等をアカウント決済サーバ 400 と通信する。また、通信部 310 は、受取人の変更に伴って受取人変更情報等をアカウント決済サーバ 400 と通信する。

【0075】

(制御部 320)

制御部 320 は、店舗サーバ 300 の各種処理を制御する。以下では、商品の注文に関する処理、受取人変更に関する処理について具体的に説明する。まず、商品の注文に関する処理について具体的に説明すると、ユーザが商品の注文を行った場合、制御部 320 は、アカウント決済サーバ 400 に対して注文情報を送信する処理を制御する。また、制御部 320 は、アカウント決済サーバ 400 から注文成否情報を取得すると、当該情報を汎用端末 200 へ送信する処理を制御する。

【0076】

受取人変更に関する処理について具体的に説明すると、制御部 320 は、ユーザが商品の注文操作を行ったときに、家族情報をアカウント決済サーバ 400 から取得し、当該情報を汎用端末 200 に対して送信する処理を制御する。汎用端末 200 から受取人変更情報を取得すると、当該情報をアカウント決済サーバ 400 に対して送信する処理を制御する。

【0077】

(記憶部 330)

記憶部 330 は、各種情報を記憶する。より具体的に説明すると、記憶部 330 は、上記で説明した、注文情報、注文成否情報、受取人変更情報、承認結果情報等を記憶する。

【0078】

(3-4. アカウント決済サーバ 400 の機能構成)

続いて、図 6 を参照して、アカウント決済サーバ 400 の機能について説明する。図 6 は、本実施形態に係るアカウント決済サーバ 400 の機能構成を示す図である。図 6 に示すように、本実施形態に係るアカウント決済サーバ 400 は、通信部 410 と、制御部 420 と、記憶部 430 と、を備える。また、制御部 420 は、ユーザ管理部 421 と、端

10

20

30

40

50

未管理部 4 2 2 と、認証状態管理部 4 2 3 と、注文処理部 4 2 4 と、決済処理部 4 2 5 と、クーポン処理部 4 2 6 と、受取人変更処理部 4 2 7 と、を備える。制御部 4 2 0 は、取得部およびサービス提供部としても機能する。

【 0 0 7 9 】

(通信部 4 1 0)

通信部 4 1 0 は、認証端末 1 0 0 および店舗サーバ 3 0 0 との通信を行う。認証端末 1 0 0 との通信について具体的に説明すると、指紋認証が成功し、認証端末 1 0 0 および汎用端末 2 0 0 の接続が完了した後に、通信部 4 1 0 は、認証端末 1 0 0 および汎用端末 2 0 0 の識別情報を認証端末 1 0 0 から受信する。また、ユーザが汎用端末 2 0 0 を用いて商品の注文を行った場合には、通信部 4 1 0 は、認証端末 1 0 0 に対して当該注文に対する承認要求を送信する。そして、通信部 4 1 0 は、ユーザによって承認または否認が行われた場合には、承認結果を認証端末 1 0 0 から受信する。また、通信部 4 1 0 は、上記以外にも例えば、受取人の権限情報、クーポン情報を認証端末 1 0 0 に対して送信する。

10

【 0 0 8 0 】

店舗サーバ 3 0 0 との通信について具体的に説明すると、通信部 4 1 0 は、商品の注文に伴って注文情報および注文成否情報等を店舗サーバ 3 0 0 と通信する。また、通信部 4 1 0 は、受取人の変更に伴って家族情報および受取人変更情報等を店舗サーバ 3 0 0 と通信する。

【 0 0 8 1 】

(制御部 4 2 0)

制御部 4 2 0 は、アカウント決済サーバ 4 0 0 の各種処理を制御する。以下に、制御部 4 2 0 が備えるユーザ管理部 4 2 1、端末管理部 4 2 2、認証状態管理部 4 2 3、注文処理部 4 2 4、決済処理部 4 2 5、クーポン処理部 4 2 6、受取人変更処理部 4 2 7 に関する機能について説明する。なお、制御部 4 2 0 が有する機能は、以下に説明する機能に限定されない。

20

【 0 0 8 2 】

(ユーザ管理部 4 2 1)

ユーザ管理部 4 2 1 は、各種情報を管理する。より具体的に説明すると、ユーザ管理部 4 2 1 は、ユーザの属性情報（氏名、年齢、連絡先、住所等）、クレジットカード情報（カード番号情報、履歴情報等）、家族情報（家族構成、家族の属性情報、家族の認証端末 1 0 0 の識別情報等）、友人情報（友人の属性情報、友人の認証端末 1 0 0 の識別情報等）、行動履歴情報、購買履歴情報等を管理する。なお、上記の行動履歴情報には、ユーザの位置情報が含まれる。ユーザ管理部 4 2 1 は、GPS 信号に基づいて特定されたユーザの位置情報を認証端末 1 0 0 から取得し、管理する。

30

【 0 0 8 3 】

また、ユーザ管理部 4 2 1 は、ビーコン受信情報を認証端末 1 0 0 から取得し、当該情報に基づいてビーコン端末と認証端末 1 0 0 の位置関係を予測し、位置関係情報として管理する。また、ユーザ管理部 4 2 1 は、複数の認証端末 1 0 0 から送信されたビーコン受信情報に基づいて、複数の認証端末 1 0 0 の位置関係を予測し、位置関係情報として管理する。

40

【 0 0 8 4 】

(端末管理部 4 2 2)

端末管理部 4 2 2 は、認証端末 1 0 0 および汎用端末 2 0 0 に関する情報を管理する。より具体的に説明すると、端末管理部 4 2 2 は、指紋認証が成功した後に認証端末 1 0 0 から送信される認証端末 1 0 0 の識別情報と汎用端末 2 0 0 の識別情報を互いに対応付けて管理する。また、端末管理部 4 2 2 は、認証端末 1 0 0 の識別情報と複数の汎用端末 2 0 0 の識別情報に対応付けて管理してもよい。すなわち、ユーザが複数の汎用端末 2 0 0 を並行して使用する場合、端末管理部 4 2 2 は、当該複数の汎用端末 2 0 0 の識別情報と認証端末 1 0 0 の識別情報に対応付けて管理してもよい。

【 0 0 8 5 】

50

(認証状態管理部 4 2 3)

認証状態管理部 4 2 3 は、認証端末 1 0 0 によるユーザの認証状態を管理する。より具体的に説明すると、認証状態管理部 4 2 3 は、認証端末 1 0 0 によって送信される指紋認証の成否に関する情報に基づいてユーザの認証状態を管理する。また、認証状態管理部 4 2 3 は、ユーザが認証端末 1 0 0 を装着していない旨の情報を取得した場合、認証状態を、認証が行われた状態から認証が行われていない状態へ変化させる。

【 0 0 8 6 】

(注文処理部 4 2 4)

注文処理部 4 2 4 は、ユーザによる商品等の注文に関する処理を行う。より具体的に説明すると、ユーザが汎用端末 2 0 0 を用いて商品等を注文した場合、注文処理部 4 2 4 は、店舗サーバ 3 0 0 から注文情報 (商品、価格、注文日時、注文を行った汎用端末 2 0 0 の識別情報等) を取得する。その後、注文処理部 4 2 4 は、当該注文に対する承認要求をユーザから得るために、認証端末 1 0 0 に対して承認要求を送信する処理を行う。そして、注文処理部 4 2 4 は、認証端末 1 0 0 から送信された承認結果に基づいて、注文の確定等を行う。そして、注文処理部 4 2 4 は、注文成否情報を生成し当該情報を汎用端末 2 0 0 へ送信する処理を制御する。

10

【 0 0 8 7 】

(決済処理部 4 2 5)

決済処理部 4 2 5 は、注文等に対する決済処理を行う。より具体的に説明すると、ユーザが商品の注文を承認した場合、決済処理部 4 2 5 はクレジットカード型決済処理を行う。なお、決済処理部 4 2 5 は、プリペイド型決済処理を行ってもよい。

20

【 0 0 8 8 】

(クーポン処理部 4 2 6)

クーポン処理部 4 2 6 は、クーポンの発行に関する処理を行う。より具体的に説明すると、クーポン処理部 4 2 6 は、ユーザの購買履歴情報を参照して、何らかの商品またはサービスに対して支払いを行ったユーザ、または何らかの行動を行ったユーザに対してクーポンを発行する。また、クーポン処理部 4 2 6 は、複数の認証端末 1 0 0 の位置関係に基づいてクーポンを発行する。例えば、クーポン処理部 4 2 6 は、ユーザ管理部 4 2 1 によって管理されている位置関係情報、家族情報および友人情報を取得し、これらの情報に基づいて、店舗にて商品を購入したユーザに同伴者がいるか否かを判定する。そして、クーポン処理部 4 2 6 は、商品を購入したユーザに同伴者がいる場合は、商品を購入したユーザおよび同伴者に対してクーポンを発行する。

30

【 0 0 8 9 】

また、クーポン処理部 4 2 6 は、一定期間にわたるユーザの行動履歴情報に基づいてユーザの行動パターンを学習することで、未来の行動を予想しクーポンを発行してもよい。例えば、ユーザが定期的にある店舗である商品を購入している場合には、クーポン処理部 4 2 6 は、今後もユーザが同様の行動をとると予想して当該店舗の当該商品に関するクーポンを発行してもよい。また、クーポン処理部 4 2 6 は、ユーザの行動履歴情報に基づいて、ユーザに対してある店舗を推薦し、当該店舗に関するクーポンを発行してもよい。例えば、ユーザがレストランにて昼食をとった場合、クーポン処理部 4 2 6 は、近隣のデザート店を推薦する情報を認証端末 1 0 0 に対して送信する処理を行い、ユーザがデザート店を予約する等の行動をとった場合には、クーポン処理部 4 2 6 は、デザート店に関するクーポンを発行してもよい。

40

【 0 0 9 0 】

クーポン処理部 4 2 6 は、クーポン情報 (割引額、有効期限等) を含む信号を生成し、対象ユーザの認証端末 1 0 0 に対して当該信号を送信するための処理を行う。なお、クーポン情報の送信先は、対象ユーザの認証端末 1 0 0 ではなく、汎用端末 2 0 0 でもよい。

【 0 0 9 1 】

(受取人変更処理部 4 2 7)

受取人変更処理部 4 2 7 は、商品の受取人の変更に関する処理を行う。より具体的に説

50

明すると、受取人変更処理部 4 2 7 は、店舗サーバ 3 0 0 から送信された受取人変更情報を取得すると、受取人の認証端末 1 0 0 に対して受取人の権限情報を送信するための処理を行う。これによって、受取人は、店舗の所定の装置に認証端末 1 0 0 を接近または接触させること等によって、自らが受取人であることを証明することができる。なお、受取人の権限情報の送信先は、認証端末 1 0 0 ではなく、汎用端末 2 0 0 でもよい。

【 0 0 9 2 】

そして、商品の受取りの際には、受取人変更処理部 4 2 7 は、来店したユーザの認証端末 1 0 0 から取得された受取人の権限情報に基づいて、当該ユーザが事前に設定された受取人であるか否かの判定を行い、判定結果情報を店舗サーバ 3 0 0 に対して送信する処理を制御する。

【 0 0 9 3 】

(記憶部 4 3 0)

記憶部 4 3 0 は、各種情報を記憶する。より具体的に説明すると、記憶部 4 3 0 は、上記で説明した、ユーザの属性情報、クレジットカード情報、家族情報、友人情報、行動履歴情報、購買履歴情報、位置関係情報、認証端末 1 0 0 および汎用端末 2 0 0 の識別情報、指紋認証の成否に関する情報、受取人変更情報、受取人の権限情報、クーポン情報、注文情報、注文成否情報、判定結果情報等を記憶する。

【 0 0 9 4 】

< 4 . 装置の動作 >

上記では、本実施形態に係る各装置の機能構成について説明した。続いて、図 7 ~ 図 1 0 を参照して、本実施形態に係る各装置の動作について説明する。

【 0 0 9 5 】

(4 - 1 . 指紋認証動作)

まず、図 7 を参照して、認証端末 1 0 0 による認証動作について説明する。図 7 は、認証端末 1 0 0 による認証動作を示すフローチャートである。

【 0 0 9 6 】

ステップ S 1 0 0 0 では、認証端末 1 0 0 の装着判定部 1 2 3 が、ユーザによる自装置の装着状態を判定する。装着判定部 1 2 3 が、ユーザが自装置を装着する動作を行っている途中であると判定した場合 (ステップ S 1 0 0 4 / Y e s)、ステップ S 1 0 0 8 にて、指紋センサー 1 3 0 がユーザの指紋情報を取得し、ステップ S 1 0 1 2 にて、認証部 1 2 2 が当該指紋情報を用いて指紋認証を行う。

【 0 0 9 7 】

指紋認証が成功した場合 (ステップ S 1 0 1 6 / Y e s)、ステップ S 1 0 2 0 にて、認証部 1 2 2 は、アカウント決済サーバ 4 0 0 に対して認証が成功した旨を通知し、処理が終了する。指紋認証が成功しなかった場合 (ステップ S 1 0 1 6 / N o)、ステップ S 1 0 2 4 にて、認証部 1 2 2 は、アカウント決済サーバ 4 0 0 に対して認証が失敗した旨を通知し、処理が終了する。

【 0 0 9 8 】

ステップ S 1 0 0 4 にて、装着判定部 1 2 3 が、ユーザが自装置を装着する動作を行っている途中ではないと判定した場合 (ステップ S 1 0 0 4 / N o)、かつ、ユーザが自装置を装着していない状態であると判定した場合 (ステップ S 1 0 2 8 / Y e s)、ステップ S 1 0 3 2 にて、装着判定部 1 2 3 は、アカウント決済サーバ 4 0 0 に対してその旨を通知し、処理が終了する。ステップ S 1 0 2 8 にて、装着判定部 1 2 3 が、ユーザが自装置を装着していると判定した場合 (ステップ S 1 0 2 8 / N o)、処理が終了する。なお、認証端末 1 0 0 は、図 7 のフローチャートの動作を定期的に行ったり、所定のタイミングで行ったり、何らかのトリガに基づいて実行することとする。

【 0 0 9 9 】

(4 - 2 . 商品の注文動作)

続いて、図 8 を参照して、商品の注文動作について説明する。図 8 は、本実施形態に係る情報処理システムを用いて商品を注文する場合の動作を示すシーケンス図である。なお

10

20

30

40

50

、図8のシーケンス図は、図7で示した指紋認証が成功した状態で行われることとする。

【0100】

まず、ステップS1100にて、ユーザが汎用端末200の所定のアプリケーションを起動する。ステップS1104では、汎用端末200の通信部210が認証端末100に対して、汎用端末200の識別情報を含む接続要求情報を送信する。ステップS1108では、認証端末100の汎用端末管理部121が、汎用端末200の識別情報を取得することに基づいて認証端末100と汎用端末200の接続が行われる。ステップS1112では、通信部110が汎用端末200に対して接続完了情報を送信する。ステップS1116では、通信部110がアカウント決済サーバ400に対して認証端末100および汎用端末200の識別情報を送信する。ステップS1120では、アカウント決済サーバ400の端末管理部422が認証端末100および汎用端末200の識別情報を対応付けて管理する。

10

【0101】

ステップS1124では、ユーザが汎用端末200の所定のアプリケーションを用いて商品の注文操作を行うことで、ステップS1128にて、汎用端末200の通信部210が店舗サーバ300に対して注文情報を送信する。ステップS1132では、店舗サーバ300の制御部320が注文情報の登録処理を行い、ステップS1136では、通信部310がアカウント決済サーバ400に対して注文情報を送信する。ステップS1140では、アカウント決済サーバ400の注文処理部424が注文情報の登録処理を行い、ステップS1144では、通信部410が認証端末100に対して承認要求情報を送信する。ステップS1148にて、ユーザが認証端末100を用いて承認操作を行った場合、ステップS1152にて、認証端末100の通信部110は、アカウント決済サーバ400に対して承認結果情報を送信する。

20

【0102】

ステップS1156にて、アカウント決済サーバ400の注文処理部424は、認証端末100から送信された承認結果情報を取得すると注文の確定等の処理を行う。ユーザが注文を承認した場合、ステップS1160にて、決済処理部425が決済処理を行う。ステップS1164では、通信部410が店舗サーバ300に対して注文成否情報を送信し、ステップS1168では、店舗サーバ300の制御部320は注文の確定等の処理を行う。ステップS1172では、通信部310が、汎用端末200に対して注文成否情報を送信する。ステップS1176では、汎用端末200の表示部240が、注文成否情報を表示することで、ユーザに対して注文の成否を通知し、処理が終了する。

30

【0103】

(4-3. 受取人の変更動作)

続いて、図9を参照して、受取人の変更動作について説明する。図9は、本実施形態に係る情報処理システムを用いて商品の受取人を変更する場合の動作を示すシーケンス図である。より具体的に説明すると、図9には、図8の動作によって商品の注文が完了した後に、その商品の受取人を変更する動作が示されている。なお、以下では、ユーザが汎用端末200を用いて商品を注文した後に、続けて、受取人の変更を行うケースを想定して説明するが、受取人の変更が行われるタイミングおよび用いられる装置は任意である。例えば、ユーザは、商品を注文した後に、改めて受取人の変更を行ってもよい。また、ユーザは、汎用端末200ではなく認証端末100を用いて受取人の変更を行ってもよい。

40

【0104】

まず、ステップS1200では、店舗サーバ300の通信部310がアカウント決済サーバ400に対して、ユーザの家族情報を要求するための情報を送信する。ステップS1204では、アカウント決済サーバ400のユーザ管理部421がユーザの家族情報を取得し、ステップS1208では、通信部410が店舗サーバ300に対して家族情報を送信する。なお、ユーザの家族情報が登録されていない場合には、通信部410はその旨の情報を送信する。ユーザの家族情報が登録されている場合、ステップS1212にて、店舗サーバ300の通信部310は、所定のアプリケーションを介して汎用端末200へ家

50

族情報を提供することで、受取人の変更の有無を確認する。ユーザは、商品の受取人を変更する場合、ステップS 1 2 1 6にて、当該アプリケーションを用いて受取人の変更操作を行う。例えば、ユーザは、家族情報に基づいて表示された家族リストの中から、受取人として指定したいユーザを選択する。その後、ステップS 1 2 2 0にて、受取人変更情報は当該アプリケーションを介して店舗サーバ3 0 0へ提供される。

【0 1 0 5】

ステップS 1 2 2 4では、店舗サーバ3 0 0の通信部3 1 0が、アカウント決済サーバ4 0 0に対して受取人変更情報を送信する。ステップS 1 2 2 8では、アカウント決済サーバ4 0 0の受取人変更処理部4 2 7が、受取人変更情報を登録する。ステップS 1 2 3 2では、受取人変更処理部4 2 7が、受取人として設定されたユーザの認証端末1 0 0に対して、受取人の権限情報を送信する。ステップS 1 2 3 6では、受取人として設定されたユーザの認証端末1 0 0の制御部1 2 0が受取人の権限情報を取得し、処理が終了する。

10

【0 1 0 6】

なお、ステップS 1 2 3 6では、受取人の権限情報が、受取人として設定されたユーザの認証端末1 0 0に送信される旨を説明したが、上記のとおり、受取人の権限情報は汎用端末2 0 0へ送信されてもよい。

【0 1 0 7】

(4 - 4 . クーポン発行動作)

続いて、図1 0を参照して、クーポン発行動作について説明する。図1 0は、本実施形態に係る情報処理システムを用いてクーポンを発行する場合の動作を示すシーケンス図である。図1 0は、ユーザAが家族または友人であるユーザBと店舗へ来店し、店舗にて商品を購入した場合において、ユーザAおよびユーザBに対してクーポンが発行される動作を説明する図である。なお、店舗にはビーコンを送信するビーコン端末が設置されていることとする。

20

【0 1 0 8】

まずステップS 1 3 0 0にて、ユーザAの認証端末1 0 0 Aの通信部1 1 0がビーコン端末によって送信されたビーコンを受信する。ステップS 1 3 0 4では、認証端末1 0 0 Aの通信部1 1 0がアカウント決済サーバ4 0 0に対してビーコン受信情報を送信する。ステップS 1 3 0 8およびステップS 1 3 1 2では、認証端末1 0 0 Bの通信部1 1 0が、認証端末1 0 0 Aと同様に、ビーコンを受信し、アカウント決済サーバ4 0 0に対してビーコン受信情報を送信する。

30

【0 1 0 9】

ステップS 1 3 1 6では、アカウント決済サーバ4 0 0のユーザ管理部4 2 1が認証端末1 0 0 Aおよび認証端末1 0 0 Bの位置関係を算出する。ステップS 1 3 2 0では、ユーザ管理部4 2 1が、ユーザAおよびユーザBの家族情報および友人情報を取得する。そして、ステップS 1 3 2 4にて、ユーザ管理部4 2 1は、ユーザAおよびユーザBが互いの家族または友人として登録されているか否かを確認し、ユーザAおよびユーザBが互いの家族または友人として登録されている場合、ユーザAおよびユーザBが共に店舗へ来店した旨の情報を登録する。

40

【0 1 1 0】

その後、ステップS 1 3 2 8にて、ユーザAまたはユーザBが店舗にて商品を購入したとする。ここで、当該購入に伴う決済方法は任意である。例えば、ユーザAまたはユーザBは、認証端末1 0 0または汎用端末2 0 0を店舗に設置されている所定の装置に接近または接触させることで決済を行ってもよい。

【0 1 1 1】

ステップS 1 3 3 2では、当該決済が行われたことを把握したアカウント決済サーバ4 0 0のクーポン処理部4 2 6が、認証端末1 0 0 Aおよび認証端末1 0 0 Bに対してクーポンを発行する。すなわち、ステップS 1 3 3 6およびステップS 1 3 4 0にて、クーポン情報が認証端末1 0 0 Aおよび認証端末1 0 0 Bに対して送信される。これによって、

50

アカウント決済サーバ400は、店舗にて商品を購入したユーザだけでなく、同伴者として来店したユーザに対してもクーポンを発行することができる。また、アカウント決済サーバ400は、ユーザ同士の関係性（家族関係、友人関係等）を踏まえて、クーポンを発行することができる。

【0112】

なお、ステップS1336およびステップS1340では、クーポン情報が、認証端末100に送信される旨を説明したが、上記のとおり、クーポン情報は汎用端末200へ送信されてもよい。

【0113】

<5. ハードウェア構成>

以上、本開示の実施形態を説明した。上記の各種処理は、ソフトウェアと、以下に説明する、認証端末100、汎用端末200、店舗サーバ300およびアカウント決済サーバ400を実現する情報処理装置900のハードウェアとの協働により実現される。

【0114】

図11は、本実施形態に係る認証端末100、汎用端末200、店舗サーバ300およびアカウント決済サーバ400を実現する情報処理装置900のハードウェア構成を示す図である。情報処理装置900は、CPU(Central Processing Unit)901と、ROM(Read Only Memory)902と、RAM(Random Access Memory)903と、ホストバス904と、を備える。また、情報処理装置900は、ブリッジ905と、外部バス906と、インタフェース907と、入力装置908と、出力装置909と、ストレージ装置(HDD)910と、ドライブ911と、通信装置912とを備える。

【0115】

CPU901は、演算処理装置および制御装置として機能し、各種プログラムに従って情報処理装置900内の動作全般を制御する。また、CPU901は、マイクロプロセッサであってもよい。ROM902は、CPU901が使用するプログラムや演算パラメータ等を記憶する。RAM903は、CPU901の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を一時記憶する。これらはCPUバスなどから構成されるホストバス904により相互に接続されている。当該CPU901、ROM902およびRAM903の協働により、各制御部の機能が実現され得る。

【0116】

ホストバス904は、ブリッジ905を介して、PCI(Peripheral Component Interconnect/Interface)バスなどの外部バス906に接続されている。なお、必ずしもホストバス904、ブリッジ905および外部バス906を分離構成する必要はなく、1つのバスにこれらの機能を実装してもよい。

【0117】

入力装置908は、タッチパネル、ボタン、マイクロフォンおよびスイッチなどユーザが情報を入力するための入力手段と、ユーザによる入力に基づいて入力信号を生成し、CPU901に出力する入力制御回路などから構成されている。情報処理装置900のユーザは、該入力装置908を操作することにより、情報処理装置900に対して各種のデータを入力したり処理動作を指示したりすることができる。入力装置908により、各入力部の機能が実現され得る。

【0118】

出力装置909は、例えば、CRT(Cathode Ray Tube)ディスプレイ装置、液晶ディスプレイ(LCD)装置、OLED(Organic Light Emitting Diode)装置およびランプなどの表示装置を含む。さらに、出力装置909は、スピーカおよびヘッドホンなどの音声出力装置を含む。出力装置909は、例えば、再生されたコンテンツを出力する。具体的には、表示装置は再生された映像データ等の各種情報をテキストまたはイメージで表示する。一方、音声出力装置は、再生された音声データを音声に変換して出力する。出力装置909により、各表示部の機能が実

10

20

30

40

50

現され得る。

【0119】

ストレージ装置910は、データ格納用の装置である。ストレージ装置910は、記憶媒体、記憶媒体にデータを記録する記録装置、記憶媒体からデータを読み出す読出し装置および記憶媒体に記録されたデータを削除する削除装置などを含んでもよい。ストレージ装置910は、例えば、HDD(Hard Disk Drive)で構成される。このストレージ装置910は、ハードディスクを駆動し、CPU901が実行するプログラムや各種データを格納する。ストレージ装置910により、各記憶部が実現され得る。

【0120】

ドライブ911は、記憶媒体用リーダライタであり、情報処理装置900に外付けされる。ドライブ911は、装着されている磁気ディスク、光ディスク、光磁気ディスク、または半導体メモリ等のリムーバブル記憶媒体913に記録されている情報を読み出して、RAM903に出力する。また、ドライブ911は、リムーバブル記憶媒体913に情報を書き込むこともできる。

10

【0121】

通信装置912は、例えば、通信網914に接続するための通信デバイス等で構成された通信インターフェースである。当該通信装置912により、各通信部の機能が実現され得る。

【0122】

<6.むすび>

20

以上で説明したように、本開示の一実施形態に係る情報処理システムは、生体認証を行う装置とサービスが提供される装置を分けることで、生体認証に用いられる生体情報を一元化することができる。これにより、本実施形態に係る情報処理システムは、ユーザがサービス毎にユーザ情報を登録したりログイン操作を行ったりすることなくサービスを提供することができる。したがって、各店舗はユーザ情報を管理しなくてもよいため、本実施形態に係る情報処理システムは、ユーザ情報が漏洩するリスクを低減させることができる。さらに、本実施形態に係る情報処理システムは、商品の受取人権限を付与する機能を有しているため、商品を受取るための各種番号を用いることなく商品の受け渡しを実現できる。

【0123】

30

以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本開示の技術的範囲に属するものと了解される。

【0124】

例えば、本実施形態に係る各装置の動作における各ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はない。例えば、図7~図10に記載された各ステップは、適宜、図に記載された順序と異なる順序で処理されても、並列的に処理されてもよい。

40

【0125】

また、認証端末100、汎用端末200、店舗サーバ300またはアカウント決済サーバ400の構成の一部は、適宜外部装置に設けられ得る。例えば、認証端末100のGPSセンサー150および位置特定部124が外部装置に設けられ、ユーザの位置情報が当該外部装置から認証端末100に対して提供されてもよい。

【0126】

また、認証端末100の機能の一部が、制御部120によって具現されてもよい。すなわち、制御部120が、通信部110、指紋センサー130、近接センサー140、GPSセンサー150、入力部160または表示部170の機能の一部を具現してもよい。認証端末100と同様に、汎用端末200、店舗サーバ300またはアカウント決済サーバ4

50

00の各制御部が、他の構成の機能の一部を具現してもよい。

【0127】

また、本明細書に記載された効果は、あくまで説明的または例示的なものであって限定的ではない。つまり、本開示に係る技術は、上記の効果とともに、または上記の効果に代えて、本明細書の記載から当業者には明らかな他の効果を奏しうる。

【0128】

なお、以下のような構成も本開示の技術的範囲に属する。

(1)

生体認証のための生体情報および、サービスが提供される装置の識別情報を取得する取得部と、

10

前記生体認証の成功に応じて、前記識別情報を送信する送信部と、を備える、
情報処理端末。

(2)

前記送信部は、前記生体認証の成功に応じて、前記情報処理端末の識別情報も送信する

、
前記(1)に記載の情報処理端末。

(3)

前記取得部が、前記装置からの入力に基づく承認要求を取得した場合、

前記送信部は、前記生体認証の対象ユーザの承認に関する操作に基づいて承認結果を送信する、

20

前記(2)に記載の情報処理端末。

(4)

前記情報処理端末は、前記生体認証の対象ユーザに装着される端末である、

前記(1)から(3)のいずれか1項に記載の情報処理端末。

(5)

前記取得部は、前記情報処理端末が前記対象ユーザに装着される際に、前記生体情報を取得する、

前記(4)に記載の情報処理端末。

(6)

前記生体情報は、指紋情報である、

前記(1)から(5)のいずれか1項に記載の情報処理端末。

30

(7)

前記生体認証を行う認証部をさらに備える、

前記(1)から(6)のいずれか1項に記載の情報処理端末。

(8)

生体認証のための生体情報および、サービスが提供される装置の識別情報を取得することと、

前記生体認証の成功に応じて、前記識別情報を送信することと、を有する、
コンピュータにより実行される情報処理方法。

(9)

生体認証のための生体情報および、サービスが提供される装置の識別情報を取得することと、

40

前記生体認証の成功に応じて、前記識別情報を送信することと、
をコンピュータに実現させるためのプログラム。

(10)

生体認証の成功に応じて、前記生体認証のための生体情報を取得した第1の装置から提供される、第2の装置の識別情報を取得する取得部と、

前記第2の装置の識別情報に基づいて前記第2の装置へサービスを提供するサービス提供部と、を備える、

情報処理装置。

50

(1 1)

前記取得部は、前記生体認証の成功に応じて、前記第 1 の装置の識別情報も取得し、前記第 1 の装置の識別情報および前記第 2 の装置の識別情報を対応付けて記憶する記憶部をさらに備える、

前記 (1 0) に記載の情報処理装置。

(1 2)

前記取得部が、前記第 2 の装置からの入力情報を取得した場合、

前記サービス提供部は、前記第 2 の装置と識別情報が相互に対応付けられている前記第 1 の装置からの承認結果に基づいて前記第 2 の装置へサービスを提供する、

前記 (1 1) に記載の情報処理装置。

10

(1 3)

前記取得部は、前記第 1 の装置の位置情報を取得し、

前記サービス提供部は、前記位置情報に基づいて、前記第 1 の装置と識別情報が相互に対応付けられている前記第 2 の装置へサービスを提供する、

前記 (1 1) から (1 2) のいずれか 1 項に記載の情報処理装置。

(1 4)

前記取得部は、複数の第 1 の装置の位置関係情報を取得し、

前記サービス提供部は、前記位置関係情報に基づいて、前記複数の第 1 の装置と識別情報が相互に対応付けられている前記第 2 の装置へサービスを提供する、

前記 (1 3) に記載の情報処理装置。

20

(1 5)

前記取得部が、前記第 2 の装置から入力された、他の第 2 の装置への権限付与に関する入力情報を取得した場合、

前記サービス提供部は、前記他の第 2 の装置への権限付与に関する処理を行う、

前記 (1 0) から (1 4) のいずれか 1 項に記載の情報処理装置。

(1 6)

前記サービス提供部は、ショッピングに関するサービス、決済に関するサービス、商品の受取人変更に関するサービスまたは、クーポンに関するサービスを提供する、

前記 (1 0) から (1 5) のいずれか 1 項に記載の情報処理装置。

(1 7)

サービスを提供する情報処理装置と、生体認証に関する処理を行う第 1 の装置と、前記サービスが提供される第 2 の装置と、を備え、

前記第 1 の装置は、

前記生体認証のための生体情報および、前記第 2 の装置の識別情報を取得する取得部と

30

、前記生体認証の成功に応じて、前記識別情報を送信する送信部と、を備え、

前記情報処理装置は、

前記生体認証の成功に応じて、前記第 1 の装置から提供される前記識別情報を取得する識別情報取得部と、

前記識別情報に基づいて前記第 2 の装置へサービスを提供するサービス提供部と、を備える、

40

情報処理システム。

【符号の説明】

【 0 1 2 9 】

1 0 0 認証端末

1 1 0、2 1 0、3 1 0、4 1 0 通信部

1 2 0、2 2 0、3 2 0、4 2 0 制御部

1 3 0 指紋センサー

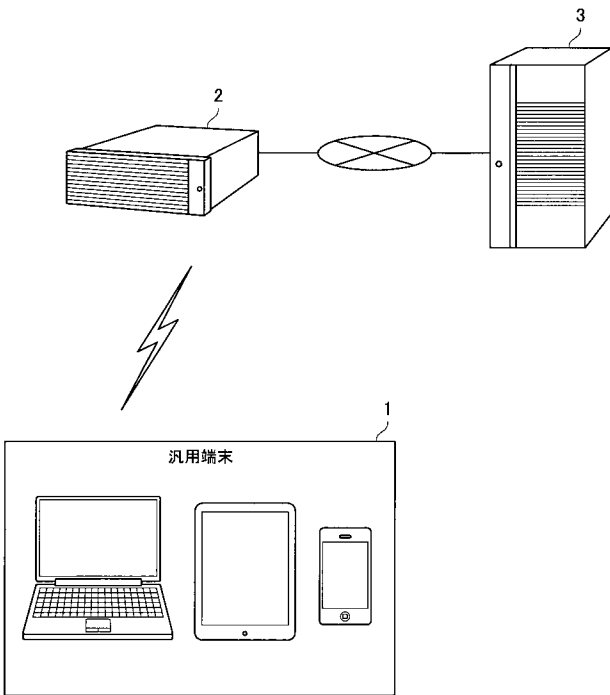
1 4 0 近接センサー

1 5 0 G P S センサー

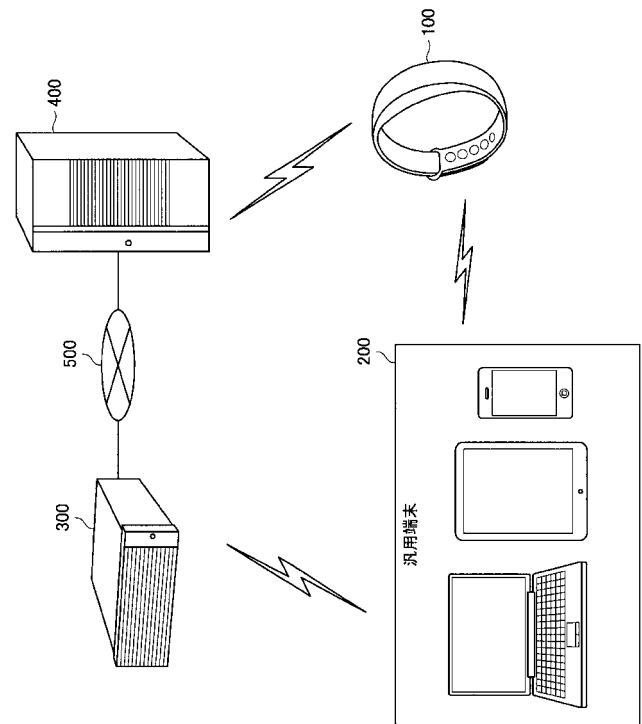
50

- 160、230 入力部
- 170、240 表示部
- 180、250、330、430 記憶部
- 200 汎用端末
- 300 店舗サーバ
- 400 アカウント決済サーバ

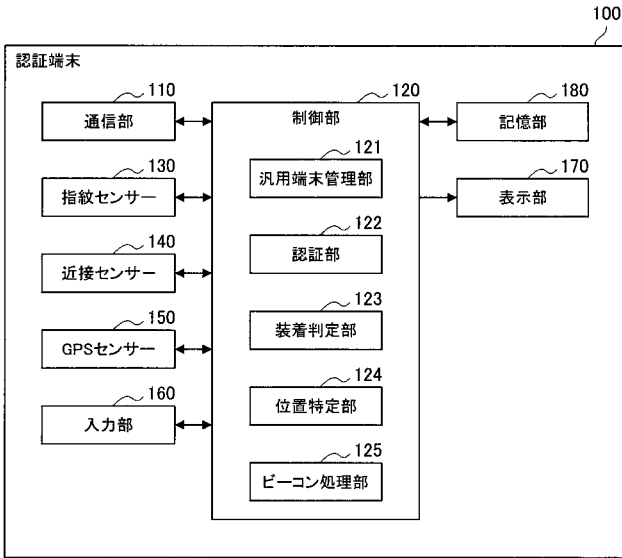
【図1】



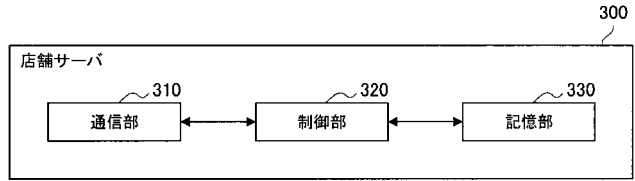
【図2】



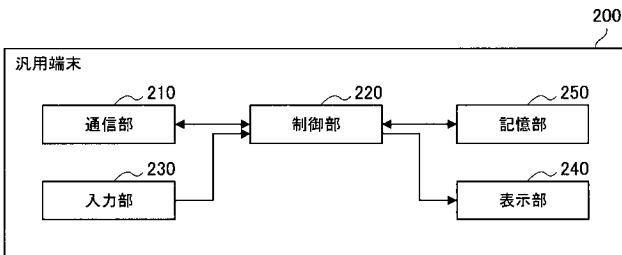
【 図 3 】



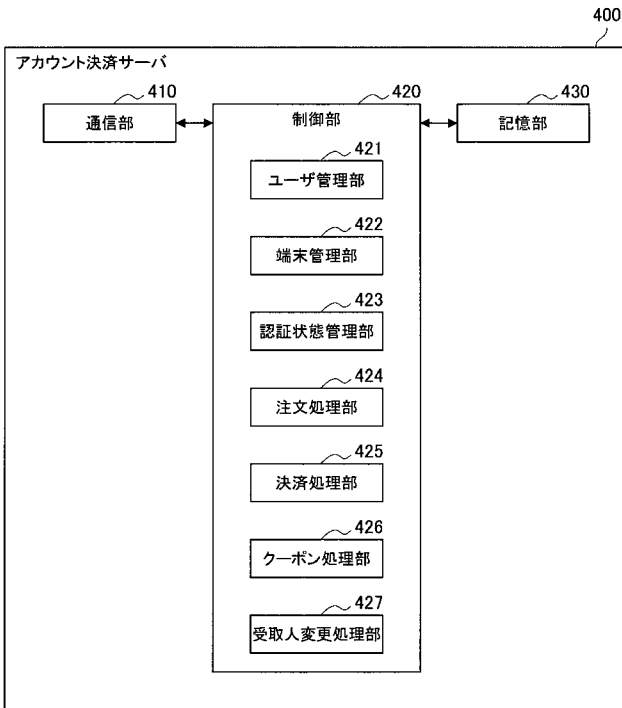
【 図 5 】



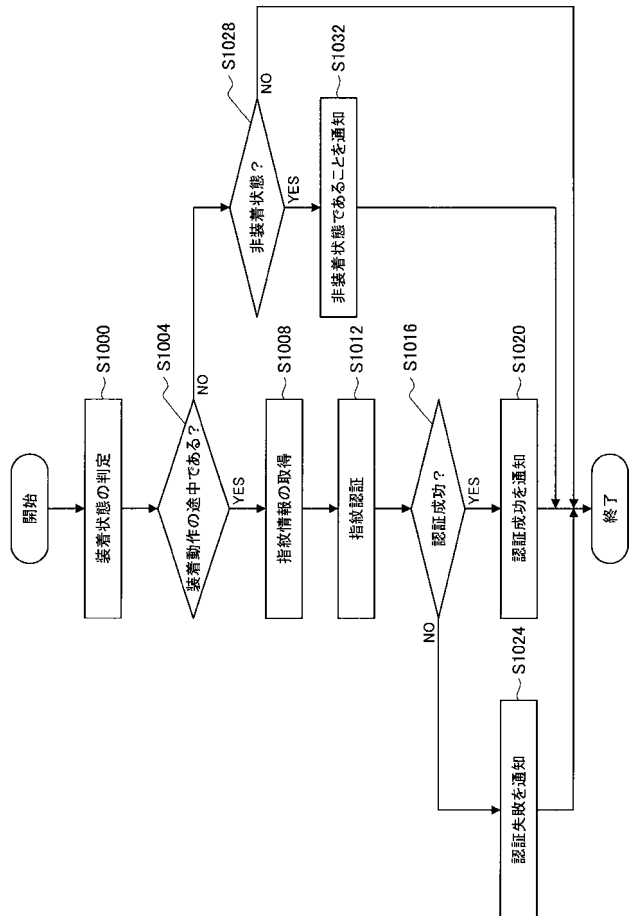
【 図 4 】



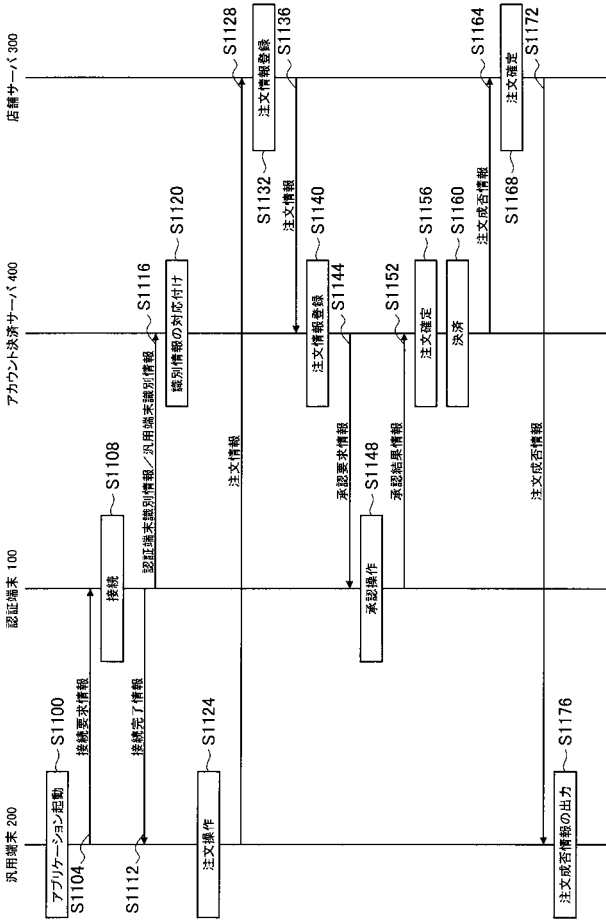
【 図 6 】



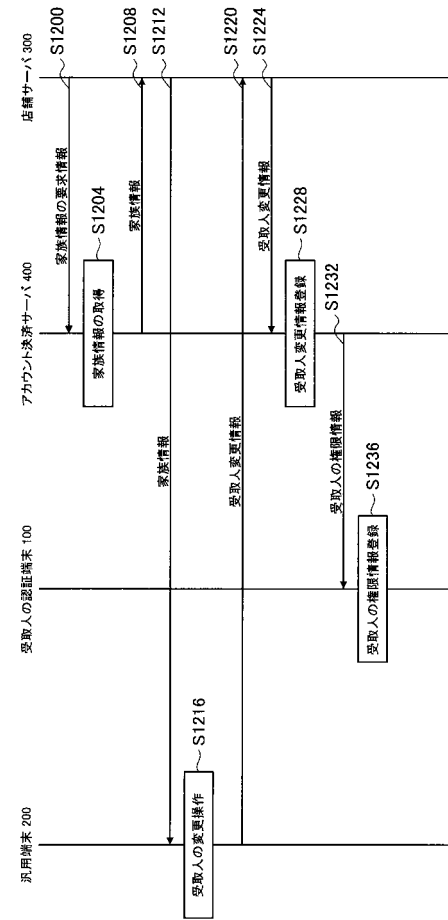
【 図 7 】



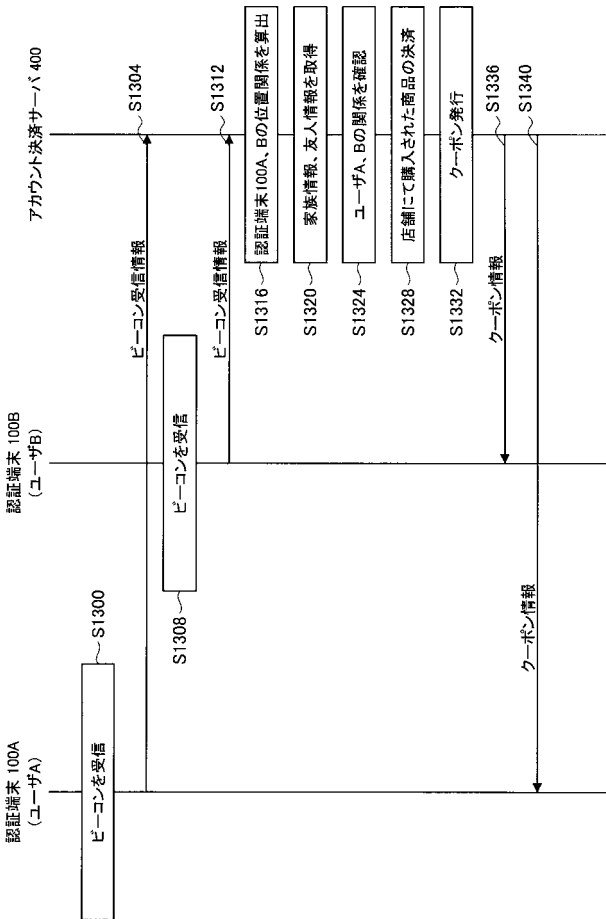
【 8 】



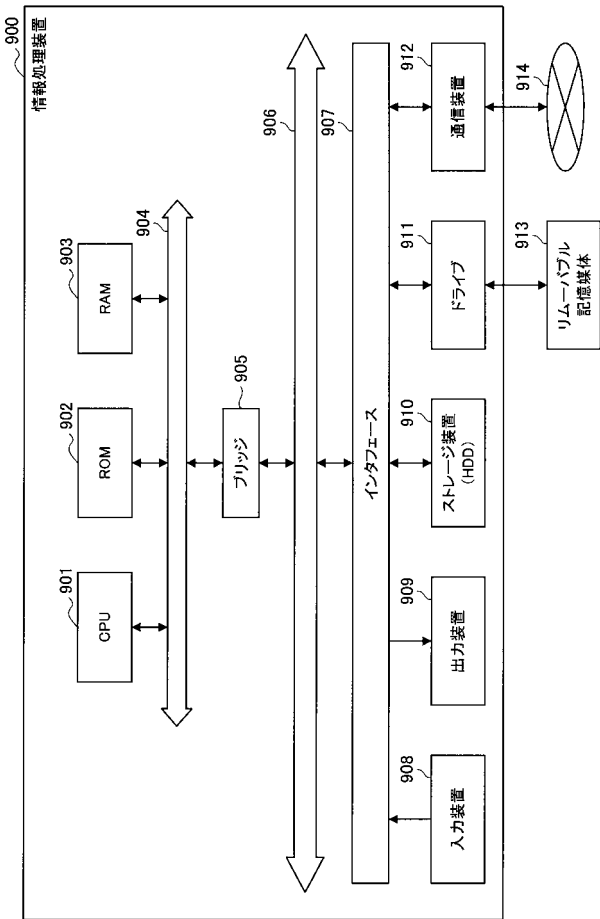
【 9 】



【 10 】



【 11 】



【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2017/033754
A. CLASSIFICATION OF SUBJECT MATTER Int.Cl. G06F21/32 (2013.01) i, G06F21/44 (2013.01) i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Int.Cl. G06F21/32, G06F21/44 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Published examined utility model applications of Japan 1922-1996 Published unexamined utility model applications of Japan 1971-2017 Registered utility model specifications of Japan 1996-2017 Published registered utility model applications of Japan 1994-2017 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2005-323070 A (NIPPON TELEGRAPH AND TELEPHONE) 17 November 2005, paragraphs [0039]-[0043], [0067], fig. 5 (Family: none)	1-17
X	JP 2008-47022 A (OKI ELECTRIC IND CO., LTD.) 28 February 2008, paragraphs [0010], [0039], [0062] (Family: none)	1-17
A	JP 2003-58509 A (SONY CORPORATION) 28 February 2003, fig. 9, 10 & US 2003/0037264 A1, fig. 9, 10	1-17
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 21 November 2017		Date of mailing of the international search report 28 November 2017
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		Authorized officer Telephone No.

国際調査報告		国際出願番号 PCT/J P 2 0 1 7 / 0 3 3 7 5 4	
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. G06F21/32(2013.01)i, G06F21/44(2013.01)i			
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. G06F21/32, G06F21/44			
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2017年 日本国実用新案登録公報 1996-2017年 日本国登録実用新案公報 1994-2017年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号	
X	JP 2005-323070 A (日本電信電話株式会社) 2005.11.17, 段落 [0039] - [0043], [0067], 図5 (ファミリーなし)	1-17	
X	JP 2008-47022 A (沖電気工業株式会社) 2008.02.28, 段落 [0010], [0039], [0062] (ファミリーなし)	1-17	
A	JP 2003-58509 A (ソニー株式会社) 2003.02.28, 図9-10 & US 2003/0037264 A1, figures 9-10	1-17	
☐ C欄の続きにも文献が列挙されている。		☐ パテントファミリーに関する別紙を参照。	
* 引用文献のカテゴリー 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す) 「O」 口頭による開示、使用、展示等に言及する文献 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願		の日の後に公表された文献 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの 「&」 同一パテントファミリー文献	
国際調査を完了した日 21.11.2017		国際調査報告の発送日 28.11.2017	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 平井 誠	5 S 9 0 7 1
		電話番号 03-3581-1101 内線 3546	

フロントページの続き

(81)指定国・地域 AP(BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), EA(AM, AZ, BY, KG, KZ, RU, TJ, TM), EP(AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT

(注) この公表は、国際事務局(WIPO)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。