

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2022年7月28日(28.07.2022)



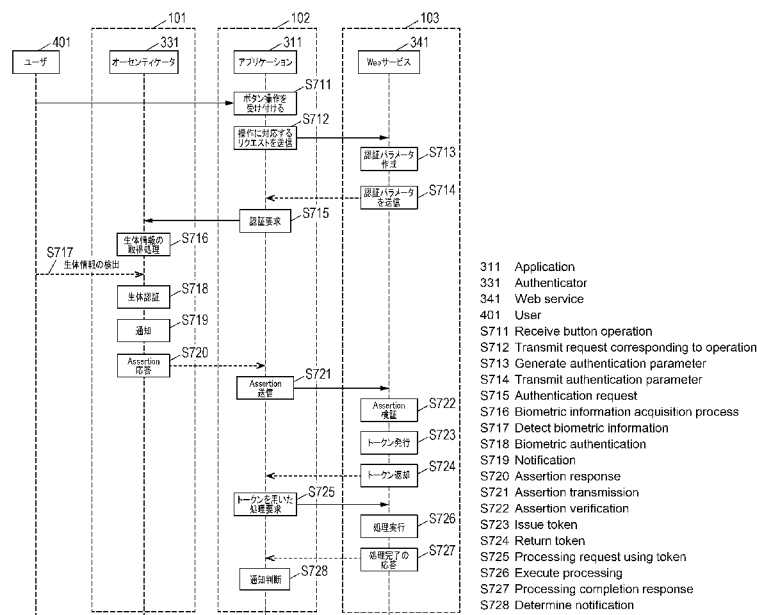
(10) 国際公開番号

WO 2022/158241 A1

- (51) 国際特許分類:
G06F 21/32 (2013.01) G06F 3/01 (2006.01)
G06F 21/33 (2013.01)
- (21) 国際出願番号: PCT/JP2021/047909
- (22) 国際出願日: 2021年12月23日(23.12.2021)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2021-009130 2021年1月22日(22.01.2021) JP
- (71) 出願人: キヤノン株式会社 (CANON KABUSHIKI KAISHA) [JP/JP]; 〒1468501 東京都大田区下丸子3丁目30番2号 Tokyo (JP).
- (72) 発明者: 白河 祐貴 (SHIRAKAWA Yuki); 〒1468501 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内 Tokyo (JP).
- (74) 代理人: 阿部 琢磨, 外 (ABE Takuma et al.); 〒1468501 東京都大田区下丸子3丁目30番2号 キヤノン株式会社内 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): 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, IT, JO, 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,

(54) Title: INFORMATION PROCESSING DEVICE, AUTHENTICATOR AND METHOD AND PROGRAM THEREFOR

(54) 発明の名称: 情報処理装置、認証器、それら方法およびプログラム



(57) Abstract: A verification mechanism in which an information processing device, which executes an application which can control an authentication process using an external authenticator worn by a user, transmits received signature data to a system upon successful authentication by the external authenticator, said mechanism being characterised in that, in response to a result of a biometric authentication and/or to a request transmitted from the information processing device to the external authenticator, a notification is issued to the user by the external authenticator.

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告(条約第21条(3))
-

(57) 要約: ユーザに装着された外部認証器を用いた認証処理を制御できるアプリケーションを実行する情報処理装置が前記外部認証器で認証に成功した場合に受信する署名データをシステムに対して送信して検証する仕組みにおいて、前記外部認証器が、前記生体認証の結果、および、前記情報処理装置から前記外部認証器に対して送信される要求、のすくなくとも何れかに応答して、前記外部認証器により前記ユーザに対して通知が行われることを特徴とする。

明 細 書

発明の名称：

情報処理装置、認証器、それら方法およびプログラム

技術分野

[0001] 本発明は、認証器を利用した認証技術に関する。

背景技術

[0002] ウェブ上のサービスにログインしたり、サービス利用の承認をしたり、するための認証方法が多数存在する。例えば、近年、F I D O (F a s t I d e n t i t y O n l i n e) と呼ばれる認証方法が注目されている。F I D O では、生体情報などの認証情報がネットワーク上を流れることがないため、情報漏洩のリスクが少ない認証方法と言われている。

[0003] 生体情報の入力方法として、指紋認証リーダを利用した指紋認証や、カメラを利用した顔認証などが広く普及している。特許文献1では、スマートフォンをF I D O 認証の外部オーセンティケータ（認証器）として利用している。近年では、スマートウォッチやスマートリング、イヤホンなどのウェアラブル端末に生体情報を読み取るセンサが備えられ、静脈認証や皮膚認証、耳音響認証などで個人認証を実現している。このようなウェアラブル端末であっても、F I D O などの認証方法における、認証器としても利用されることが可能である。

先行技術文献

特許文献

[0004] 特許文献1：特開2020-95687号公報

発明の概要

発明が解決しようとする課題

[0005] ウェアラブル端末を、外部認証器として利用して、静脈認証や皮膚認証、耳音響認証などの認証方法を採用した場合、指をスマートフォンの所定位置にかざすなど、といった特定の操作入力なしに認証がスムーズに行える可能

性がある。

[0006] その一方で、装着しているだけでユーザの操作なしに認証が行えるがゆえに、ユーザからすると認証処理の結果や、成功したタイミングが把握しづらくなる懸念がある。イヤホンなどウェアラブル端末は、スマートフォンなどとは異なり、ディスプレイをもっていない場合もあり、その場合はそのような懸念が顕著になる。とくに、前述のFIDOでサービス利用（商品購入など）の承認を行う際に、外部認証器としてウェアラブル端末を利用している場合には、ユーザが認証処理の結果などをリアルタイムに把握したいと考えるかもしれない。

[0007] 本発明は、ウェアラブル端末を認証器として利用する場合においても、認証処理に伴う通知をユーザに適切に行うことができる仕組みの提供を目的とする。

課題を解決するための手段

[0008] 外部認証器を用いた認証処理を制御できるアプリケーションを実行する情報処理装置であって、ネットワークを介して通信するシステムに対してリクエストを送信する第1送信手段と、検証用のデータを前記システムから受信する第1受信手段と、前記検証用のデータを含む認証要求を外部認証器に送信する要求手段と、前記外部認証器から、前記外部認証器が生成した署名データを受信する第2受信手段と、前記署名データを前記システムに対して送信する第2送信手段と、前記システムに登録済みの公開鍵を用いた前記署名データの検証処理の結果に基づくデータを受信する第3受信手段と、を有し、前記外部認証器は、前記情報処理装置のユーザに装着され、前記認証要求に応じた生体認証の結果、および、前記第3受信手段によるデータの受信に応じて前記情報処理装置から前記外部認証器に対して送信される要求、の少なくとも何れかに応答して、前記外部認証器により前記ユーザに対して通知が行われることを特徴とする。

発明の効果

[0009] 本発明によれば、ウェアラブル端末を認証器として利用する場合において

も、認証処理に伴う通知をユーザに適切に行うことができる仕組みを提供できる。

図面の簡単な説明

[0010] [図1]システム構成およびネットワーク構成の例を示す図

[図2A]サーバシステムを構築する情報処理装置のハードウェア構成の例を示す図

[図2B]ウェアラブル端末のハードウェア構成の例を示す図

[図2C]クライアント端末のハードウェア構成の例を示す図

[図3A]クライアント端末のソフトウェアのモジュール構成の例を示す図

[図3B]ウェアラブル端末のソフトウェアのモジュール構成の例を示す図

[図3C]サーバシステムのソフトウェアのモジュール構成の例を示す図

[図4]オーセンティケータの登録時のシーケンスの例を示す図

[図5A]登録パラメータ 5 1 0 のデータ構造の例を示す図

[図5B]登録要求データ 5 2 0 のデータ構造の例を示す図

[図5C]クレデンシャル 5 3 0 のデータ構造の例を示す図

[図5D]登録データ 5 4 0 のデータ構造の例を示す図

[図6A]アプリケーションが提供する認証設定画面の例を示す図

[図6B]クライアント端末で表示される登録画面の例を示す図

[図6C]クライアント端末でのオーセンティケータの検索中を示す画面の例を示す図

[図6D]クライアント端末 1 0 2 で表示されるオーセンティケータの登録確認のための画面の例を示す図

[図6E]クライアント端末でのオーセンティケータの登録中を示す画面の例を示す図

[図6F]クライアント端末で表示される登録完了の画面の例を示す図

[図7]認証を含むサービス利用時のシーケンスの例を示す図

[図8A]認証パラメータ 8 1 0 の例を示す図

[図8B]認証要求パラメータ 8 2 0 の例を示す図

[図8C]アサーション情報830の例を示す図

[図9A]Webサービスが提供する画面の例を示す図

[図9B]サービス利用時の認証中を示す画面の例を示す図

[図9C]認証完了を示す画面の例を示す図

[図9D]サービス利用の受諾を示す画面の例を示す図

[図10]実施例3における認証を含むサービス利用時のシーケンスの例を示す図

[図11A]オーセンティケータの登録確認のための画面の変形例1を示す図

[図11B]オーセンティケータの登録確認のための画面の変形例2を示す図

発明を実施するための形態

[0011] 以下、本発明を実施するための最良の形態について図面を用いて説明する。以降の説明では、ウェブ上のサービス利用に際して、ユーザが所有し、装着するウェアラブル端末で生体認証を行っている。その認証が成功したことを証明できるデータ（署名データ）をウェブ上のサービスに提供し、サービスにおいてそのデータの検証に成功することでサービスを提供する仕組みに関するものである。なお、以降の実施例では、その仕組みとしてFIDOを利用する例を説明しているが、同様の認証の仕組みであれば、FIDO以外の技術を採用することも可能である。

[0012] （実施例1）

<ネットワーク構成>

図1は、本実施例のネットワーク構成例を示す図である。本システムは、ウェアラブル端末101と、クライアント端末102、サーバシステム103から構成される。

[0013] クライアント端末102、サーバシステム103はネットワーク105を介して接続される。ネットワーク105は、例えば、インターネット等のLAN、WAN、電話回線、専用デジタル回線、ATMやフレームリレー回線、ケーブルテレビ回線、データ放送用無線回線等のいずれであり。またはこれらの組み合わせにより実現される、いわゆる通信ネットワークである。ま

た、ウェアラブル端末101は、クライアント端末102ともネットワーク106を介して接続される。ネットワーク106は、例えば、NFC (Near Field Communication) やBluetooth等の近距離の無線通信や、USBケーブル接続による通信などによって実現される。ネットワーク106はWi-Fiでの通信によって実現されてもよい。また、ウェアラブル端末101は、ネットワーク105に接続されてもよい。

[0014] <サーバシステム103の内部構成>

図2Aは、サーバシステム103の情報処理機能を有するハードウェアの構成例を示す図である。サーバシステム103は、少なくとも1以上の情報処理装置により構築され、以下で説明する、それら装置が具備するハードウェアを用いて、ウェブサイトやウェブサービス、認証サービスを提供する。

[0015] 201はCPUであり、RAM202、ROM203、記憶装置210などから読み込んだプログラムを実行する。キーボードコントローラ204は、キーボード208や図示しないポインティングデバイス（マウス、タッチパッド、タッチパネル、トラックボールなど）からの操作入力を制御する。ディスプレイコントローラ205は、ディスプレイ209の表示を制御する。ディスクコントローラ206は、各種データを記憶するハードディスクドライブ（HD）、ソリッドステートドライブ（SSD）等の記憶装置210へのデータアクセスを制御する。ネットワークインターフェース207は、LANなどのネットワークに接続されて、ネットワークに接続された他の機器と通信する。201～207などハードウェアを構成する各部は内部バス211を介して接続されている。

[0016] <ウェアラブル端末101の内部構成>

図2Bは、ウェアラブル端末101の内部構成を示す図である。

[0017] CPU221はROM223に格納されているプログラム（後述する各処理を実現するプログラムも含む）を備え、内部バス233を介して各デバイスを総括的に制御する。RAM222は、CPU221のメモリやワークエ

リアとして機能する。記憶装置 224 は、各種データを記憶するハードディスクドライブ（HD）、ソリッドステートドライブ（SSD）などである。ネットワーク I/F 225 は、外部のネットワーク機器と片方向または双方向にデータをやり取りする。生体情報センサ 226 は、静脈認証や皮膚認証、耳音響認証などの生体情報を読み取るセンサである。Trusted Platform Module（TPM）227 は、機密情報を処理したり格納したりする目的で、格納したデータを外部から読み取られることを防ぐ耐タンパー性を備えた記憶手段である。TPM 227 は、生体情報センサ 226 で入力した生体情報やウェアラブル端末 101 内で生成した秘密鍵を記憶すると共に、記憶している生体情報と入力された生体情報とを検証する機能を有する。耐タンパー性を備えた記憶手段としては、ウェアラブル端末 101 の OS などのプラットフォームが独自に定義するセキュアに構築された信頼環境を代用することが可能である。

[0018] 近接通信 I/F 228 は NFC や Bluetooth などの近接通信用のネットワーク I/F である。近接通信 I/F 228 を利用することでクライアント端末 102 等とデータのやり取りや、クライアント端末 102 等からウェアラブル端末 101 に対して認証指示を出すことが可能である。タッチパネル 229 はディスプレイ機能とポインティング機能の両方を備えた装置であり、ディスプレイに表示されたオブジェクトをユーザが指やタッチペンなどで操作することができる。バイブレータ 230 は、ウェアラブル端末 101 を振動させるための装置であり、ユーザの操作や外部からのイベント等に呼応して振動する。スピーカ 231 は、音声メッセージやメロディなどの音を出力するための装置である。

[0019] 本発明におけるウェアラブル端末 101 は、ユーザが装着したまま認証可能な静脈認証や皮膚認証、耳音響認証などの機能を有するスマートウォッチやイヤホン、スマートリングなどを想定しているが、特定のデバイスに限定しているわけではない。また、図 2B ではタッチパネル 229 のような表示出力装置を備えているが、本発明では必ずしも必要ではない。さらに、ウェ

アラブル端末１０１のバイブレータ２３０やスピーカ２３１は、本実施例においてはユーザへ処理の完了を通知するために用いるが、通知するための装置はこれに限らない。例えば、スマートウォッチであればベルトを締め付けるための装置を、スマートリングであれば点滅するライトを有することも可能である。

[0020] <クライアント端末の内部構成>

図２Ｃは、クライアント端末１０２である情報処理装置のハードウェアの構成例を示す図である。

[0021] 内部バス２４１、ＣＰＵ２４２、ＲＡＭ２４３、ＲＯＭ２４４は、内部バス２１１、ＣＰＵ２０１、ＲＡＭ２０２、ＲＯＭ２０３と同様の機能を有する。記憶装置２４５は、ソリッドステートドライブ（ＳＳＤ）やＳＤメモリカードなどの記憶装置であり、記憶装置２１０と同様に各種データを記憶する。ネットワークインターフェース２４７はネットワークに接続された他の機器と通信する無線通信機能を備えた通信モジュールである。タッチパネル２４９はタッチパネル２２９と同様に、ディスプレイ機能とポインティング機能の両方を備えた装置であり、ディスプレイに表示されたオブジェクトをユーザが指やタッチペンなどで操作することができる。近接通信ＩＦ２５０、バイブレータ２５１、スピーカ２５２は、それぞれ近接通信Ｉ／Ｆ２２８、バイブレータ２３０、スピーカ２３１と同様の機能を有する。

[0022] 本発明におけるクライアント端末１０２は、スマートフォンやＰＣ、タブレットコンピュータなどの情報処理端末を想定しているが、特定のデバイスに限定しているわけではない。例えば、ディスプレイやタッチパネルを持たないスマートスピーカや、スマートグラスなどのデバイスであってもよい。

[0023] <クライアント端末１０２のソフトウェア構成>

図３Ａは、クライアント端末１０２のソフトウェアの構成例を示す図である。

[0024] アプリケーション３１１は、サーバシステム１０３のＷｅｂサービス３４１が提供するサービスを利用するためのアプリケーションである。アプリケ

ーション311は、表示部(UI)312と通信部313、オーセンティケータ登録制御部314、オーセンティケータ認証制御部315、通知制御部316から成る。

[0025] アプリケーション311は、WebブラウザあるいはWebサービス341の使用に特化したネイティブアプリケーションである。312は表示部であり、Webサービス341から取得したWebコンテンツ等を実行・表示するソフトウェアモジュールである。通信部313は、サーバシステム103やウェアラブル端末101と通信するためのソフトウェアモジュールである。オーセンティケータ登録制御部314は、オーセンティケータ(認証器)331に対して後述するクレデンシャルの作成要求を行ったり、オーセンティケータの登録時にWebサービス341に対して送信するリクエストを生成したりするソフトウェアモジュールである。オーセンティケータ認証制御部315はオーセンティケータ331に対して認証処理を要求したり、認証時にWebサービス341に対して送信するリクエストを生成したりする。通知制御部316は、本発明の特徴である認証時にユーザに認証結果を通知・制御するためのソフトウェアモジュールである。通知制御部316が通知する条件またはタイミング、パターンについては後述する。ユーザが表示部312を操作し、通信部313がサーバシステム103と通信を行うことで、Webサービス341が提供するサービスを利用することができる。

[0026] なお、オーセンティケータの登録やユーザの認証などの具体的な処理シーケンスに関しては後述する。

[0027] <ウェアラブル端末101のソフトウェア構成>

図3Bは、ウェアラブル端末101のソフトウェアの構成例を示す図である。

[0028] 表示部325はタッチパネル229を介してユーザにGUIを提供するためのソフトウェアモジュールである。通信部326はネットワークインターフェース225を介してクライアント端末102などの外部の機器と通信するためのソフトウェアモジュールである。

[0029] オーセンティケータ 331 は、生体情報センサ 226 を用いた生体認証に係る処理を実行する認証モジュール群である。本実施例におけるウェアラブル端末 101 は、オーセンティケータ 331 が実行されることで、クライアント端末 102 の外部オーセンティケータ（外部認証器）として機能することが可能となる。

[0030] オーセンティケータ登録処理部 332 はオーセンティケータ登録制御部 314 などからクレデンシャルの作成要求を受け付け、ペアの鍵（秘密鍵および公開鍵）の作成やクレデンシャルの作成を行うソフトウェアモジュールである。生体認証処理部 333 は、オーセンティケータ認証制御部 315 から生体認証要求を受け付けて、生体情報センサ 226 を用いて、生体認証を行うソフトウェアモジュールである。認証情報格納部 334 は、認証情報管理テーブル（表 1）に示す認証情報などを、TPM 227 に対して格納するソフトウェアモジュールである。生体情報要求部 335 は、ユーザに生体情報の入力を受け付けるための UI をタッチパネル 229 に表示するソフトウェアモジュールである。なお、ウェアラブル端末 101 の種類によってはタッチパネル 229 などの UI を表示するための表示出力装置を備えていないデバイスも存在するため、タッチパネル 229 と同様に表示部 325 は本発明の必要構成要素ではない。通知制御部 336 は、本発明の特徴である認証時にユーザに認証結果を通知・制御するためのソフトウェアモジュールである。通知制御部 336 が通知するタイミングやパターンについては後述する。

[0031] <ウェアラブル端末 101 のオーセンティケータ 331 が管理するテーブルの例>

表 1 の認証情報管理テーブルでは、1 つのレコードが 1 つの認証情報のエントリを示している。

[0032]

[表1]

認証情報管理テーブル

認証情報 ID	サービス ID	ユーザ ID	秘密鍵	生体情報 ID
407c-8841-79d	xxxmarket.com	user001	1faea2da-a269-4fa7-812a-509470d9a0cb	d493a744
4c04-428b-a7a2	xxxmarket.com	user001	d7ae30c8-3775-4706-8597-aaf681bc30f5	dcc97daa
92b2-498d-bea6	xxxmarket.com	user001	36ae5eed-732b-4b05-aa7b-4dddb4be3267	51caacaa
...	...	...	...	...

[0033] 認証情報 ID 列は、各認証情報に対して一意な識別情報（ID）を格納する列である。サービス ID 列は、Web サービス 341 など、対象となるサービスを識別するための識別情報（サービス ID）の列である。認証情報管理テーブルでは、サービス ID として各 Web サービスのドメイン名が格納されている。ユーザ ID 列には、レガシー認証などで使用する Web サービスがユーザを一意に識別するためのユーザ識別情報（ユーザ ID）が格納されている。レガシー認証とは、ユーザ ID とパスワードの一致を検証する認証のことであり、生体認証と区別してレガシー認証と記載する。秘密鍵列は、オーセンティケータ登録処理部 332 が作成した秘密鍵の識別子を格納している。なお、秘密鍵列の各識別子で管理されるそれぞれの秘密鍵に対応する公開鍵は、サービス ID 列で示されるサービス ID に対応するネットワーク上のサービスに登録、管理されることになる。生体情報 ID 列は、生体情報の特徴量に対応する識別情報（ID）を格納する。

[0034] 認証情報管理テーブルの各列で管理されるデータを格納する手順、および公開鍵を Web サービス 341 に送信、格納する手順については後述する。

[0035] <サーバのソフトウェア構成>

図 3C は、サーバシステム 103 のソフトウェアの構成例を示す図である。

[0036] Web サービス 341 は、HTTP などの通信プロトコルを利用してサービスを提供するユーザ認証を必要とする Web サービスである。Web サービスは、提供するサービスごとに用意される。具体例として、Web サービスは、ソーシャル・ネットワーキング・サービス（social netw

orking service) やEコマース (Electric Commerce) サービス、金融サービスと、それらのサービスのためのウェブサイトを提供する。

[0037] サーバシステム103が有するROM203に記憶されているWebサービスを提供するためのプログラムを、CPU201がRAM202に読み出して実行することでWebサービスを実現している。レガシー認証処理部342は、通信部348が受信したレガシー認証要求に含まれるユーザID、パスワードとユーザ情報格納部344に格納されているユーザID、パスワードが一致するかを検証するソフトウェアモジュールである。オーセンティケータ情報処理部343は、通信部348が受信したクレデンシャルを用いて、オーセンティケータに関する情報をオーセンティケータ情報格納部345に格納するソフトウェアモジュールである。また、オーセンティケータ情報処理部343は、通信部348が受信した後述するアサーション情報 (Assertion) を検証する。ユーザ情報格納部344は、ユーザ情報管理テーブルを用いて後述するユーザ情報を格納するソフトウェアモジュールである。オーセンティケータ情報格納部345は、オーセンティケータ情報管理テーブルを用いて後述するオーセンティケータ情報を格納するソフトウェアモジュールである。プレゼンテーション部346は、通信部348がクライアント端末102などから受信したWebサービス341の各種画面の取得要求に応じて、HTMLやCSS、JavaScriptなどを作成するソフトウェアモジュールである。トークン管理部347は、トークン管理テーブルを用いて後述するトークンの発行や検証を行うソフトウェアモジュールである。通信部348は、クライアント端末102と通信して、要求を受け付けるソフトウェアモジュールである。

[0038] <サーバシステム103が管理するテーブルの例>

表2は、ユーザ情報管理テーブルであり、Webサービス341のユーザ情報格納部344が管理する。ユーザ情報管理テーブルは、1つのレコードが登録済みの1ユーザのアカウント情報を示している。

[0039] [表2]

ユーザ情報管理テーブル		
ユーザID	パスワード	メールアドレス
user001	*****	user001@xxx.co.jp
user002	*****	user002@xxx.co.jp
...	...	...

[0040] ユーザID列は、Webサービス341のユーザを一意に識別するためのユーザ識別子（ユーザID）である。パスワード列は、ユーザを認証するためのパスワードを格納する。このパスワードはレガシー認証で使用するパスワードであり、通常ハッシュ化されて格納されている。メールアドレス列は、ユーザのメールアドレスを格納する。メールアドレス以外にもユーザの住所、プロフィールなど、ユーザに関する属性情報をユーザ情報管理テーブルのテーブルに格納するようにしてもよい。

[0041] 表3は、attestationチャレンジ管理テーブルであり、Webサービス341のユーザ情報格納部344が管理する。

[0042] [表3]

attestationチャレンジ管理テーブル		
attestationチャレンジ	ユーザID	有効期限
65C9B063-9C33	user001	2017-05-02T12:00:34Z
7317EFBA-4E63	user002	2017-05-02T12:03:12Z
...	...	...

[0043] 表3で示すattestationチャレンジ管理テーブルは、1つのレコードが1つのattestationチャレンジの情報を示している。attestationチャレンジは、ユーザのクレデンシャル登録の際に発行されるデータで、チャレンジレスポンス認証のための検証用データとして利用するパラメータである。attestationチャレンジの発行処理については後述する。attestationチャレンジ列は、attestation

t a t i o n チャレンジを格納する。ユーザ I D 列は、発行された a t t e s t a t i o n チャレンジが紐づけられたユーザ I D を表す。有効期限列は、a t t e s t a t i o n チャレンジの有効期限を表す。

[0044] 表 4 は、オーセンティケータ情報管理テーブルであり、W e b サービス 3 4 1 のオーセンティケータ情報格納部 3 4 5 が管理する。

[0045] [表4]

オーセンティケータ情報管理テーブル

認証情報 I D	公開鍵	ユーザ I D	通知能力
407c-8841-79d	AC43C5FB-BFA2-48D1-A71B-FB04ACDA347A	user001	有
4c04-428b-a7a2	8143CA9F-35C9-4333-948F-BFCE66A74310	uesr001	無
...	...	...	...

[0046] 表 4 で示すオーセンティケータ情報管理テーブルは、1 つのレコードが 1 つのオーセンティケータ情報を示している。認証情報 I D 列は、認証情報管理テーブル（表 1）における認証情報 I D 列の値が格納される。公開鍵列は、オーセンティケータからクレデンシャルとして登録要求された公開鍵の情報を管理する。この公開鍵は、認証情報 I D に紐づく秘密鍵のペアとなる公開鍵となる。すなわち、同一認証情報 I D で管理される鍵ペアでは、オーセンティケータ側の秘密鍵で暗号化したデータは、W e b サービス 3 4 1 側のオーセンティケータ情報管理テーブルで管理される公開鍵で復号できるということになる。

[0047] ユーザ I D 列は、W e b サービス 3 4 1 を利用するユーザを一意に識別するためのユーザ I D を格納する。通知能力列は、ウェアラブル端末 1 0 1 に通知制御部 3 3 6 が備わっているかどうか（本実施例に係る通知機能をサポートしているかどうか）を示す能力情報である。この情報は、本発明の特徴でもある通知判断時に用いられる情報である。

[0048] 表 5 は、トークン管理テーブルであり、W e b サービス 3 4 1 のトークン管理部 3 4 7 が管理する。

[0049]

[表5]

トークン管理テーブル		
トークン	ユーザID	有効期限
3FD4FA-AA4-56DC-B45F-45BCD65AC45D	user001	2017-05-02T13:14:31Z
EC51DC-36C4-4BC3-54CF-31ECE6CACBF0	user002	2017-05-02T13:31:32Z
...	...	...

[0050] 表5で管理されるトークンは、各種認証処理を終えた後に、Webサービス341のトークン管理部347が発行する。アプリケーション311は、Webサービス341を利用する際に、発行されたトークンを付与してリクエストを送信することで、Webサービス341が提供するサービスを利用することができる。

[0051] トークン管理テーブルは、1つのレコードが1つのトークンの情報を示している。トークン列は、トークンの情報を格納する。ユーザID列は、Webサービス341のユーザを一意に識別するためのユーザIDを格納する。有効期限列は、トークンの有効期限を示す。

[0052] Webサービス341は、リクエストに付与されたトークンが、トークン管理テーブルのトークン列に存在し、有効期限列の有効期限を過ぎていない場合に、リクエストを受け付ける。

[0053] <オーセンティケータ登録処理>

図4で示すオーセンティケータ登録処理について、図5A～D、図6A～Fも用いて説明する。図4で示す処理は、各装置で対応するプログラムを実行することで実現される処理ステップを示している。ここでは、ウェアラブル端末101のオーセンティケータ331が作成する情報を登録する例について説明する。以降、オーセンティケータ331が作成する情報をWebサービス341に登録することを、単にオーセンティケータ（認証器）の登録と呼ぶ。

[0054] 図5A～Dは、ウェアラブル端末101、クライアント端末102、サーバシステム103間での通信に含まれるパラメータの例を示す図である。図

6 A～Fは、オーセンティケータの登録処理中にアプリケーション311の表示部312で表示制御されるUIの例を示した図である。

[0055] まず、図6Aは、アプリケーション311が提供する認証設定画面であり、ユーザは、Webサービス341の利用時にレガシー認証（パスワード認証）以外の認証方法を利用したい場合にボタン611を押下する。なお、認証設定画面は、レガシー認証などでWebサービス341に対してユーザ401を認証済み場合に提供される。

[0056] S411では、アプリケーション311が、ユーザによるボタン611の選択に応じた登録指示を受け付ける。

[0057] S412では、アプリケーション311のオーセンティケータ登録制御部314が、通信部313を介して、Webサービス341に対してオーセンティケータ登録画面の要求を行う。

[0058] S413では、Webサービス341のオーセンティケータ情報処理部343が、登録パラメータ510の作成を行う。

[0059] ここで、図5Aを用いて登録パラメータ510について説明する。登録パラメータ510は、アカウント情報511、暗号化パラメータ512、`attestation`チャレンジ513、登録ポリシー514、拡張領域515から構成される。アカウント情報511は、Webサービス341における、認証時に特定したユーザIDと、そのユーザIDと紐付くメールアドレスなどの属性情報を表す。暗号化パラメータ512は、Webサービス341がサポートしている暗号化アルゴリズムなど、登録する認証情報に関する属性情報を示す。`attestation`チャレンジ513はチャレンジレスポンス認証をするために利用する検証用データとしてのパラメータである。`attestation`チャレンジは、S413の登録パラメータ作成時に作成して、`attestation`チャレンジ管理テーブル（表3）にユーザIDや有効期限などと紐付けて格納される。登録ポリシー514は、Webサービス341に登録できるオーセンティケータの種別を指定するためのオプションパラメータである。ポリシーとは、例えば、認証器となるウェアラブ

ル端末１０１がＷｅｂサービス３４１の指定する認証方法に対応しているか、特定の能力を有しているか、などである。拡張領域５１５は、Ｗｅｂサービス３４１がオーセンティケータ３３１やアプリケーション３１１の動作を制御するために、Ｗｅｂサービス３４１が指定可能な拡張パラメータが格納される。

[0060] Ｓ４１４で、Ｗｅｂサービス３４１のオーセンティケータ情報処理部３４３は、Ｓ４１２の要求に対するレスポンスとして、オーセンティケータ登録画面の情報をアプリケーション３１１に送信する。送信されるレスポンスには、登録パラメータ５１０も含まれている。

[0061] 図６Ｂは、Ｓ４１４でのレスポンスに応じてアプリケーション３１１により、クライアント端末１０２のタッチパネル２４９に対して表示制御される登録画面の例である。ボタン６２１がユーザに操作されるとＳ４１５で検索処理を実行し、ボタン６２２が操作されると図６Ａの画面に戻る。

[0062] 図６Ｃは、Ｓ４１５～Ｓ４１６の処理が実行されている際に、タッチパネル２４９で表示される画面である。

[0063] Ｓ４１５で、オーセンティケータ登録制御部３１４は、クライアント端末１０２にオーセンティケータ（外部認証器）として利用できるデバイスが接続されているかを検索する。具体的には接続デバイスであるウェアラブル端末にオーセンティケータ情報を取得するためのリクエストを送信する。ウェアラブル端末でオーセンティケータのプログラムが実行されている場合には、このリクエストに応答することが可能である。本実施例では、オーセンティケータ登録制御部３１４がアプリケーション３１１の通信部３１３を介して、ウェアラブル端末１０１の通信部３２６に対してこのリクエストを送信することになる。

[0064] なお、リクエストされるオーセンティケータ情報には、オーセンティケータ情報管理テーブルで説明したオーセンティケータの通知能力も含まれている。

[0065] Ｓ４１６では、ウェアラブル端末１０１の通信部３２６を介してオーセン

ティケータ登録処理部332がリクエストを受信して、さらに、オーセンティケータ情報をアプリケーション311に応答する。

[0066] S417で、オーセンティケータ登録制御部314は、S416で取得したオーセンティケータ情報が、S414でのレスポンスに含まれる登録ポリシ514の条件を満たし、Webサービス341のオーセンティケータとして使用できるか否かを確認する。

[0067] 図6Dは、S417の処理でWebサービス341のオーセンティケータとして使用できることが確認できた場合に、タッチパネル249に対して表示される画面である。ユーザによりボタン641が選択操作されると、S418を実行すると共に、図6Eで示す画面に遷移する。また、ボタン642が選択されると、図6Aの画面に戻る。

[0068] なお、図4のシーケンスには示していないが、固定の外部認証器を常に利用するなどユーザに登録確認を要求しない設定の場合には、図6Dの画面をスキップし、S418を実行してもよい。また、使用できるオーセンティケータが見つからない、外部認証器を利用しない設定などであった場合には、S417以降の処理を実行しないといった実装も可能である。

[0069] S418で、アプリケーション311のオーセンティケータ登録制御部314は通信部313を介して、ウェアラブル端末101に対してクレデンシャルの作成要求を行う。そして、このクレデンシャル作成要求はウェアラブル端末101の通信部326が受信し、オーセンティケータ登録処理部332に送信される。このS418のクレデンシャル作成要求には登録要求データ520を含める。

[0070] ここで図5Bを用いて、登録要求データ520について説明する。登録要求データ520は、Webサービス341から受信した登録パラメータ510と、認証情報管理テーブル(表1)で説明したWebサービス341のサービスID521と、WebOrigin522を含む。WebOrigin522はWebサービス341のオリジンを示す情報である。

[0071] S419で、オーセンティケータ登録処理部332は、ユーザの生体情報

の取得処理を実行する。具体的には、内部的に生体情報センサ 226 に生体情報の読み取りを指示する。S 420 では、ウェアラブル端末 101 を装着するユーザ 401 の生体情報が、生体情報センサ 226 を介して検出される。本発明においては、ユーザ 401 はウェアラブル端末 101 を装着しているだけで、ウェアラブル端末 101 に対する操作なしに生体情報の検出が実行されることを想定している。

[0072] S 421 で、オーセンティケータ 331 のオーセンティケータ登録処理部 332 は読み取った生体情報の特徴量と生体情報を一意に識別する生体情報 ID を作成する。S 422 で、オーセンティケータ 331 のオーセンティケータ登録処理部 332 は、秘密鍵と公開鍵のペアを作成し、認証情報 ID を発行する。そして、オーセンティケータ登録処理部 332 は認証情報格納部 334 に S 421、S 422 で作成した認証情報 ID、秘密鍵、生体情報 ID および登録要求データ 520 に含まれるサービス ID 521 と登録パラメータ 510 に含まれるユーザ ID を格納する。

[0073] S 423 で、オーセンティケータ 331 のオーセンティケータ登録処理部 332 は、図 5C で示すクレデンシャル 530 を作成する。クレデンシャル 530 は、認証情報 ID 531 とアルゴリズム 532 と公開鍵 533 と `attestation` 534 とオーセンティケータ名 535 から構成される。

[0074] 認証情報 ID 531、公開鍵 533 は S 422 の処理で作成した公開鍵である。アルゴリズム 532 は S 422 における秘密鍵と公開鍵のペアの作成に利用したアルゴリズムにそれぞれ対応する。また、`attestation` 534 は `attestation` チャレンジ 513 を、S 422 にて作成した秘密鍵を用いて暗号化したものである。

[0075] S 424 では、通知制御部 336 が、ウェアラブル端末 101 が備えるバイブレータ 230 やスピーカ 231 の少なくとも何れかを利用して、生体情報の入力完了した旨をユーザ 401 に通知する。ユーザ 401 は、ウェアラブル端末 101 から伝わる振動や、特定の音で通知を認識できる。

[0076] なお、S 424 の処理で利用される通知手段は、ウェアラブル端末 101

の種類によって異なり、例えば、スマートウォッチであれば振動やベルトの締め付け、イヤホンであれば音、スマートリングであればライトを点滅させる等の方法を用いることができる。

[0077] また、ウェアラブル端末101が通知制御部329やバイブレータ230やスピーカ231などの装置を備えていない場合は、S424の処理をスキップし、後述するS429で、アプリケーション311が代替となり生体情報の入力完了した旨をユーザ401に通知することも可能である。

[0078] S425で、オーセンティケータ331のオーセンティケータ登録処理部332は、クライアント端末102のアプリケーション311に対して、S423で作成したクレデンシャル530を応答する。

[0079] S426で、オーセンティケータ登録制御部314は、通信部313を介して、Webサービス341に対して、登録データ540を含む登録処理要求を送信する。

[0080] ここで、図5Dを用いて登録データ540について説明する。540は登録データであり、クレデンシャル530と能力情報541から構成される。クレデンシャル530はS423で作成したクレデンシャルである。能力情報541は、S415～S416で取得したウェアラブル端末101のオーセンティケータ情報である。

[0081] S427では、Webサービス341のオーセンティケータ情報処理部343は、S426の登録処理要求で受信した登録データ540を用いて、オーセンティケータの登録処理を行う。登録処理には、登録データ540のクレデンシャル530に含まれる`attestation534`を、同じクレデンシャル530に含まれる公開鍵533で復号することによる検証処理が含まれる。さらに、Webサービス341のオーセンティケータ情報処理部343は、`attestation534`を公開鍵533で復号した値と、`attestation`チャレンジ管理テーブル（表3）における`attestation`チャレンジ列の値とが同一のものを特定する。そして、特定した`attestation`チャレンジ列の値と同一のレコードのユーザ1

Dをクレデンシャル530と紐付けるIDとして特定する。Webサービス341のオーセンティケータ情報処理部343は、クレデンシャル530に含まれる認証情報ID531、公開鍵533と、特定されたユーザIDと能力情報541を、オーセンティケータ情報管理テーブルに登録する。S428で、Webサービス341のオーセンティケータ情報処理部343は、通信部348を介して、アプリケーション311に対して正常にオーセンティケータの登録処理が完了した旨を応答する。

[0082] S429では、Webサービス341のオーセンティケータ登録制御部314がS415～S416で取得したウェアラブル端末101のオーセンティケータ情報に含まれている通知能力に応じて通知判断を行う。オーセンティケータ登録制御部314は、ウェアラブル端末101が通知能力“無”であると判断した場合に通知制御部316を呼び出し、S424のステップに代わり、ユーザ401に生体情報の入力および登録処理が完了した旨の通知を行う。

[0083] 例えば、図6Fは、オーセンティケータ登録制御部314によりS429で示す処理が実行された際に表示される画面である。クライアント端末102がタッチパネル249やバイブレータ251のような出力装置を有する場合は、図6Fのような画面表示やクライアント端末102を振動させることで登録処理が完了したことが分かる通知を行う。

[0084] なお、クライアント端末102がスマートスピーカのように音声のみで入出力を行うデバイスの場合は、図6A～Fで示した表示内容を音声によって実現することになる。

[0085] <図6Dに関する処理の変形例>

図11Aは、図6Dに示す画面の変形例を示している。具体的には、Webサービス341のオーセンティケータとして使用できる機器として複数のウェアラブル端末が見つかった場合の例である。図11Bは、さらに、複数のウェアラブル端末に加え、クライアント端末102自身が備える内部オーセンティケータがWebサービス341のオーセンティケータとして使用で

きる場合の例である。

[0086] 図 1 1 A と図 1 1 B では、複数のウェアラブル端末として、「〇〇スマートウォッチ」と「△△ワイヤレスイヤホン」とを例示している。ユーザによってボタン 1 1 0 1、1 1 0 2 の何れかが選択された場合には、ボタンに対応するウェアラブル端末に対してクレデンシャルの作成要求を実行して、S 4 1 8 以降の処理が実行されることになる。

[0087] 図 1 1 A と図 1 1 B で、キャンセルボタン 1 1 0 4 が選択された場合には、図 6 A の画面に戻る。

[0088] 図 1 1 B で、ボタン 1 1 0 3 が選択操作された場合には、クライアント端末 1 0 2 に実装された内部オーセンティケータに対して、クレデンシャルの作成要求が実行される。その場合には、S 4 1 9 ～S 4 2 5 までの処理が、クライアント端末 1 0 2 が有する生体情報センサを用いて取得された生体情報を用いて内部オーセンティケータにより実行されることになる。

[0089] <認証処理>

図 7 は、ユーザ 4 0 1 がアプリケーション 3 1 1 から、認証を必要とする Web サービス 3 4 1 を利用する際のシーケンスを示す図である。図 7 で示す処理は、各装置で対応するプログラムを実行することで実現される処理ステップを示している。

[0090] 図 8 A ～C は、認証で使用するパラメータの例を示す図である。図 9 A ～D は、図 7 で示す処理に伴って、アプリケーション 3 1 1 の表示部 3 1 2 が表示制御する画面例を示している。

[0091] 本実施例では、オーセンティケータの登録処理と同様に認証処理においても生体情報の入力後に、ユーザ 4 0 1 に完了を示す旨を通知する仕組みを提供する。ここでは、図 7、図 8 A ～C、図 9 A ～D を用いて、Web サービス 3 4 1（E コマースサイト）で、商品の購入手続きを行う際の認証処理の例を説明する。

[0092] まず、図 9 A は、Web サービス 3 4 1 のプレゼンテーション部 3 4 6 が提供するコンテンツをアプリケーション 3 1 1 の表示部 3 1 2 によって表示

した際の画面である。

- [0093] S 7 1 1 で、アプリケーション 3 1 1 は、ユーザ 4 0 1 によるボタン 9 1 1 への選択操作に応じた指示を受け付ける。S 7 1 2 では、アプリケーション 3 1 1 のオーセンティケータ認証制御部 3 1 5 が Web サービス 3 4 1 に対して商品購入に係るリクエストを送信する。
- [0094] S 7 1 3 で、Web サービス 3 4 1 のオーセンティケータ情報処理部 3 4 3 は、利用者の認証のために、認証パラメータ 8 1 0 を作成する。S 7 1 4 で、Web サービス 3 4 1 のオーセンティケータ情報処理部 3 4 3 は、S 7 1 3 で作成した認証パラメータ 8 1 0 をアプリケーション 3 1 1 に対して送信する。
- [0095] 図 8 A は、認証パラメータ 8 1 0 を示す。認証パラメータ 8 1 0 は、Assertion チャレンジ 8 1 1、Assertion 拡張領域 8 1 2 で構成される。Assertion チャレンジ 8 1 1 は、チャレンジレスポンス認証をするために利用する検証用データとしてのパラメータである。Assertion 拡張領域 8 1 2 は、Web サービス 3 4 1 がオーセンティケータ 3 3 1 やアプリケーション 3 1 1 の動作を制御するために、Web サービス 3 4 1 が指定可能な拡張パラメータが格納される。今回、この Assertion 拡張領域 8 1 2 に、S 4 2 6 で付与したオーセンティケータの能力情報 5 4 1 を含める。
- [0096] S 7 1 5 で、アプリケーション 3 1 1 のオーセンティケータ認証制御部 3 1 5 は、オーセンティケータ 3 3 1 の生体認証処理部 3 3 3 に対して、認証要求パラメータを用いて認証要求を行う。このとき、表示部 3 1 2 により、図 9 B に示す画面が表示される。
- [0097] 図 8 B は、認証要求パラメータ 8 2 0 を示す。認証要求パラメータ 8 2 0 は、認証パラメータ 8 1 0、サービス ID 8 2 1、Web Origin 8 2 2 で構成される。サービス ID 8 2 1 と Web Origin 8 2 2 は図 5 B で説明したものと同一である。
- [0098] S 7 1 6 で、オーセンティケータ 3 3 1 の生体情報要求部 3 3 5 は、ユー

ザの生体情報の取得処理を実行する。ここでは、S 4 1 9 の処理と同様の処理が実行される。S 7 1 7 で、ウェアラブル端末 1 0 1 を装着するユーザ 4 0 1 の生体情報が、生体情報センサ 2 2 6 を介して検出される。本発明においては、ユーザ 4 0 1 はウェアラブル端末 1 0 1 を装着しているだけで、ウェアラブル端末 1 0 1 に対する操作なしに生体情報の検出が実行されることを想定している。

[0099] S 7 1 8 で、オーセンティケータ 3 3 1 の生体認証処理部 3 3 3 が、生体情報センサ 2 2 6 を介して検出した生体情報と、T P M 2 2 7 に格納された生体情報との照合を行い、ユーザ認証を行う。照合アルゴリズムとして、特徴点抽出法やパターンマッチング法などが一般的に知られているが、本発明において照合アルゴリズムは特に限定しない。その後、認証情報格納部 3 3 4 が T P M 2 2 7 に格納された生体情報をもとに認証情報管理テーブルから、対応する秘密鍵を特定する。そして、認証パラメータ 8 1 0 に含まれる `attestation` チャレンジ 8 1 1 と、特定した秘密鍵とから、署名 (8 3 2) データを作成する。さらに、生体認証処理部 3 3 3 は、認証情報管理テーブル (表 1) から特定した認証情報 I D 8 3 1 と署名 8 3 2 を含んだアサーション情報 8 3 0 を作成する。

[0100] S 7 1 9 で、オーセンティケータ 3 3 1 の通知制御部 3 3 6 が通知を行う処理である。S 7 1 8 で生体認証が行われた結果を通知制御部 3 3 6 がバイブレータ 2 3 0 やスピーカ 2 3 1 などによりユーザ 4 0 1 に通知を行う。S 7 1 9 において、通知制御部 3 3 6 は S 7 1 8 の認証結果に応じて通知パターンを変えることができる。例えば、外部認証器として利用するウェアラブル端末 1 0 1 がイヤホンの場合、装着したまま自動で行われた認証に成功した場合は「認証に成功しました」等の音声を、失敗した場合は「認証に失敗しました」等の音声を流す制御を行う。また、S 7 1 9 において、オーセンティケータの登録時同様、ウェアラブル端末 1 0 1 が通知制御部 3 2 9 やバイブレータ 2 3 0 やスピーカ 2 3 1 などの装置を備えていないこともある。その場合は、同様に S 7 1 9 の通知処理をスキップし、後述する S 7 2 8 で

アプリケーション311が代替となり生体情報の入力および認証が完了した旨をユーザ401に通知する。

[0101] S720で、オーセンティケータ331の生体認証処理部333は、S718で作成したアサーション情報830を、アプリケーション311に返却する。

[0102] S721で、アプリケーション311のオーセンティケータ認証制御部315は、生体認証処理部333から受け取ったアサーション情報830をWebサービス341に送信する。

[0103] S722では、Webサービス341のオーセンティケータ情報処理部343は、アプリケーション311から受け取ったアサーション情報830の検証を行う。オーセンティケータ情報処理部343はアサーション情報830の署名832を認証情報ID831で特定される公開鍵を用いて復号し、S713で作成した認証パラメータ810に含まれるattestationチャレンジ811と一致するか判定することで署名を検証する。公開鍵の特定にはオーセンティケータ情報管理テーブルを用いる。検証が成功した場合には、S723で、Webサービス341のトークン管理部347は、トークンを発行して、そのトークンに関する情報をトークン管理テーブルで管理する。S724で、Webサービス341のトークン管理部347が、S723で発行したトークンを、アプリケーション311に返却する。

[0104] S725で、オーセンティケータ認証制御部315は、S724で受信したトークンを用いて、商品購入のためのリクエストをWebサービス341に送信する。

[0105] S726で、トークン管理部347は、S725のリクエストに付与されたトークンを検証し、県庁が成功した場合に、リクエストに応じた購入処理を実行する。S727で、Webサービス341は、購入処理が完了した旨のレスポンスをアプリケーション311に返却する。

[0106] S728では、Webサービス341のオーセンティケータ認証制御部315が、S714で返却された認証パラメータ810のAssertion

拡張領域 8 1 2 に含まれていた能力情報 5 4 1 をもとに認証結果を通知するかどうかを判断する。

[0107] オーセンティケータの登録時と同様に、オーセンティケータ認証制御部 3 1 5 はウェアラブル端末 1 0 1 が通知能力“無”であると判断した場合に、通知制御部 3 1 6 を呼び出す。そして、S 7 1 9 の処理に代わりユーザ 4 0 1 に認証処理および S 7 2 6 の購入処理が完了した旨の通知を行う。

[0108] 例えば、図 9 C は、オーセンティケータ認証制御部 3 1 5 により S 7 2 8 が実行された際に表示される画面である。S 7 2 8 での通知パターンもオーセンティケータの登録時同様、UI 表示や音声、振動など、クライアント端末 1 0 2 が備える装置によって異なるため、特に限定しない。S 7 2 8 でオーセンティケータ認証制御部 3 1 5 が、ウェアラブル端末 1 0 1 の通知能力が“有”であると判断した場合は、図 9 C のように認証が完了した旨の通知を行う必要は無く、図 9 D の画面に遷移する。

[0109] 以上、実施例 1 では、ウェアラブル端末 1 0 1 のオーセンティケータ 3 3 1 に通知制御部 3 3 6 を備えることで、生体情報を入力されオーセンティケータの登録・認証処理が実行されたことをユーザ 4 0 1 が気付けるように、通知を行った。また、ウェアラブル端末 1 0 1 が通知制御部 3 3 6 を備えない場合であってもクライアント端末 1 0 2 側の通知制御部 3 1 6 が代替としてユーザ 4 0 1 に通知する方法についても説明した。このシステムにより、認証のためにユーザによる操作を必要としないウェアラブル端末をオーセンティケータとして使用した場合でも、ユーザが生体情報を入力し、オーセンティケータの登録や認証処理が確かに実行されたということを、ユーザが適切なタイミングで把握することができる。

[0110] (実施例 2)

実施例 1 では、オーセンティケータ 3 3 1 のオーセンティケータ登録処理部 3 3 2 と生体認証処理部 3 3 3 が、単に S 4 2 3、S 7 1 8 の処理を終えた後に通知制御部 3 3 6 を呼び出すことでユーザ 4 0 1 に通知を行うように制御していた。しかし、ユーザ 4 0 1 が利用する Web サービス 3 4 1 の提

供サービスによっては、通知の有無や通知パターンを制御したい場合がある。

[0111] 例えば、サービスの利用中に頻繁に認証を要求されるようなシステムにおいて、その都度、認証が完了したことを通知されると煩わしいと感じるユーザもいる。また、同じ認証処理でも、Webサービス341上の操作に応じて通知パターンを変化させたい場合もある。

[0112] 上記のケースを鑑み、オーセンティケータの登録時には登録パラメータ510の拡張領域515に、認証時には認証パラメータ810のAssertion拡張領域812に、それぞれ通知に関する制御情報を追加で格納するよう実装可能である。この制御情報は、ウェアラブル端末101の通知制御部336が解釈可能な情報であり、S424およびS719において、通知制御部336はこの制御情報の値に応じた通知の有無を判断する。より具体的には、制御情報の値が、通知が必要なことを示す場合にのみ通知するよう制御することができる。また、制御情報の値によって、通知パターン（メッセージの内容、LED点灯パターンなど）を変化させるように実装することも可能である。

[0113] なお、拡張領域515、Assertion拡張領域812に制御情報が含まれない場合に、実施例1に示す処理を行ってもよい。

[0114] 本実施例による拡張により、Webサービス341側から、ウェアラブル端末101の通知の制御を行うことが可能となる。

[0115] （実施例3）

実施例1では、通知制御部336が、S424、S719など、ウェアラブル端末101での外部認証器としての生体認証が成功したタイミングで通知を行っていた。

[0116] 実施例3では、Webサービス341の処理が完了したことを以て、通知する方法について説明する。本実施例では、上述した実施例1、2との重複となる説明を避け、差分について詳細に説明する。

[0117] 図10は、実施例1の認証時のシーケンスにおいて、通知タイミングを変

えたシーケンス図である。差分としては、S 7 1 9 の通知処理が無い代わりに、S 1 0 2 9、S 1 0 3 0 の処理が追加されている。

[0118] S 7 2 8 では、ウェアラブル端末 1 0 1 の通知能力の有無と、通知の要否と、が同時に確認される。ウェアラブル端末 1 0 1 での通知が必要と判断した場合、S 1 0 2 9 で、オーセンティケータ認証制御部 3 1 5 はオーセンティケータ 3 1 1 に対して通知要求を行う。

[0119] S 1 0 3 0 で、通知要求を受信したオーセンティケータ 3 1 1 の通知制御部 3 3 6 は、認証処理を含む一連の処理が完了したことを意図した通知制御を実行する。ここでの通知制御は、S 7 1 9 の通知処理と同じ処理でもよいし、処理完了を直接的に把握できるような通知であってもよい。

[0120] 実施例 1、2 においては、S 4 2 6 や S 7 2 1 以降の処理でクライアント端末 1 0 2 とサーバシステム 1 0 3 との間の通信ができない場合などにおいては、図 4、7 に示すシーケンスは異常終了する。このとき、シーケンス全体が正常終了しなかったにも関わらず、S 4 2 4、S 7 1 9 でウェアラブル端末 1 0 1 の通知制御部 3 3 6 はユーザ 4 0 1 に対して認証成功を通知してしまったことになり、購入処理に成功したとの誤解を与える懸念がある。

[0121] 一方で、本実施例によれば、通知のタイミングが Web サービス 3 4 1 での処理が完了の後になるため、そのような誤解を解消できるかもしれない。

[0122] なお、本発明は、実施例 1 と実施例 3 を組み合わせることで、実施例 1 の S 7 1 9 と実施例 3 の S 1 0 3 0 の両方のタイミングで異なる通知を行い、認証成功と処理完了を別々にユーザに通知することも可能である。

[0123] (他の実施例)

本発明は、上述した実施形態を適宜組み合わせることにより構成された装置あるいはシステムやその方法も含まれるものとする。

[0124] ここで、本発明は、上述した実施形態の機能を実現する 1 以上のソフトウェア（プログラム）を実行する主体となる装置あるいはシステムである。また、その装置あるいはシステムで実行される上述した実施形態を実現するための方法も本発明の一つである。また、そのプログラムは、ネットワーク又

は各種記憶媒体を介してシステム或いは装置に供給され、そのシステム或いは装置の1以上のコンピュータ（CPUやMPU等）によりそのプログラムが1以上のメモリーに読み出され、実行される。つまり、本発明の一つとして、さらにそのプログラム自体、あるいは該プログラムを格納したコンピュータにより読み取り可能な各種記憶媒体も含むものとする。また、上述した実施形態の機能を実現する回路（例えば、ASIC）によっても、本発明は実現可能である。

[0125] 本発明は上記実施の形態に制限されるものではなく、本発明の精神及び範囲から離脱することなく、様々な変更及び変形が可能である。従って、本発明の範囲を公にするために以下の請求項を添付する。

[0126] 本願は、2021年1月22日提出の日本国特許出願特願2021-009130を基礎として優先権を主張するものであり、その記載内容の全てをここに援用する。

請求の範囲

- [請求項1] 情報処理装置に接続される外部認証器を用いた認証処理を制御できるアプリケーションを実行する情報処理装置であって、
- ネットワークを介して通信するシステムに対してリクエストを送信する第1送信手段と、
- 検証用のデータを前記システムから受信する第1受信手段と、
- 前記検証用のデータを含む認証要求を外部認証器に送信する要求手段と、
- 前記外部認証器から、前記外部認証器が生成した署名データを受信する第2受信手段と、
- 前記署名データを前記システムに対して送信する第2送信手段と、
- 前記システムに登録済みの公開鍵を用いた前記署名データの検証処理の結果に基づくデータを受信する第3受信手段と、を有し、
- 前記外部認証器は、前記情報処理装置のユーザに装着され、
- 前記認証要求に応じた生体認証の結果、および、前記第3受信手段によるデータの受信に応じて前記情報処理装置から前記外部認証器に対して送信される要求、のすくなくとも何れかに応答して、前記外部認証器により前記ユーザに対して通知が行われることを特徴とする情報処理装置。
- [請求項2] さらに、前記認証要求に応じた生体認証の結果、および、前記第3受信手段によるデータの受信、のすくなくとも何れかに応答した、前記外部認証器を装着する前記ユーザのための表示を制御する制御手段を、有することを特徴とする請求項1に記載の情報処理装置。
- [請求項3] 前記制御手段は、前記外部認証器が前記通知のための機能をサポートしていない場合、前記表示の制御を行うことを特徴とする請求項2に記載の情報処理装置。
- [請求項4] 前記外部認証器による前記ユーザに対して通知は、前記認証要求に含まれる通知に関する制御情報に従い行われることを特徴とする請求

項 1 乃至 3 の何れか 1 項に記載の情報処理装置。

[請求項5] 前記外部認証器は、前記ユーザに装着されたままで生体認証が可能な、スマートウォッチ、イヤホン、およびスマートリングの何れかであることを特徴とする請求項 1 乃至 4 の何れか 1 項に記載の情報処理装置。

[請求項6] 情報処理装置に接続される外部認証器を用いた認証処理を制御するための該情報処理装置における方法であって、

ネットワークを介して通信するシステムに対してリクエストを送信する第 1 送信工程と、

検証用のデータを前記システムから受信する第 1 受信工程と、

前記検証用のデータを含む認証要求を外部認証器に送信する要求工程と、

前記外部認証器から、前記外部認証器が生成した署名データを受信する第 2 受信工程と、

前記署名データを前記システムに対して送信する第 2 送信工程と、

前記システムに登録済みの公開鍵を用いた前記署名データの検証処理の結果に基づくデータを受信する第 3 受信工程と、を有し、

前記外部認証器は、前記情報処理装置のユーザに装着され、

前記認証要求に応じた生体認証の結果、および、前記第 3 受信工程でデータの受信に応じて前記情報処理装置から前記外部認証器に対して送信される要求、のすくなくとも何れかに応答して、前記外部認証器により前記ユーザに対して通知が行われることを特徴とする方法。

[請求項7] 請求項 1 乃至 5 の何れか 1 項に記載の手段としてコンピュータを機能させるためのプログラム。

[請求項8] 外部認証器を用いた認証処理を制御できるアプリケーションを実行する情報処理装置に対して外部認証器として接続でき、前記情報処理装置のユーザに装着される認証器であって、

前記情報処理装置から認証要求を受け付けたことに応じて、前記ユ

ーザの生体情報を検出する検出手段と、

前記生体情報を用いた生体認証を実行する認証手段と、

前記生体認証が成功した場合に、前記認証要求に含まれる検証用のデータと前記生体情報に対応する秘密鍵を用いて、署名データを生成する生成手段と、

前記署名データを前記情報処理装置に送信する送信手段と、

通知手段と、を有し、

前記通知手段は、前記認証要求に応じた生体認証の結果、および、前記情報処理装置から前記外部認証器に対して送信される要求、の少なくとも何れかに応答して、前記ユーザに対して通知を行うことを特徴とする認証器。

[請求項9] 前記認証器による前記ユーザに対して通知は、前記認証要求に含まれる通知に関する制御情報に従い行われることを特徴とする請求項8に記載の認証器。

[請求項10] 前記認証器は、前記ユーザに装着されたままで生体認証が可能な、スマートウォッチ、イヤホン、およびスマートリングの何れかであることを特徴とする請求項8または9に記載の認証器。

[請求項11] 前記通知は、音、または振動による通知であることを特徴とする請求項8乃至10の何れか1項に記載の認証器。

[請求項12] 外部認証器を用いた認証処理を制御できるアプリケーションを実行する情報処理装置に対して外部認証器として接続でき、前記情報処理装置のユーザに装着され、通知手段を備える認証器における方法であって、

前記情報処理装置から認証要求を受け付けたことに応じて、前記ユーザの生体情報を検出する検出工程と、

前記生体情報を用いた生体認証を実行する認証工程と、

前記生体認証が成功した場合に、前記認証要求に含まれる検証用のデータと前記生体情報に対応する秘密鍵を用いて、署名データを生成

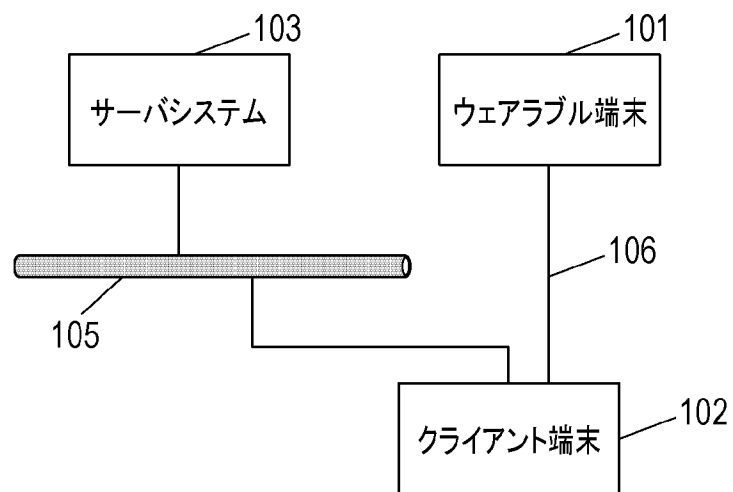
する生成工程と、

前記署名データを前記情報処理装置に送信する送信工程と、を有し、

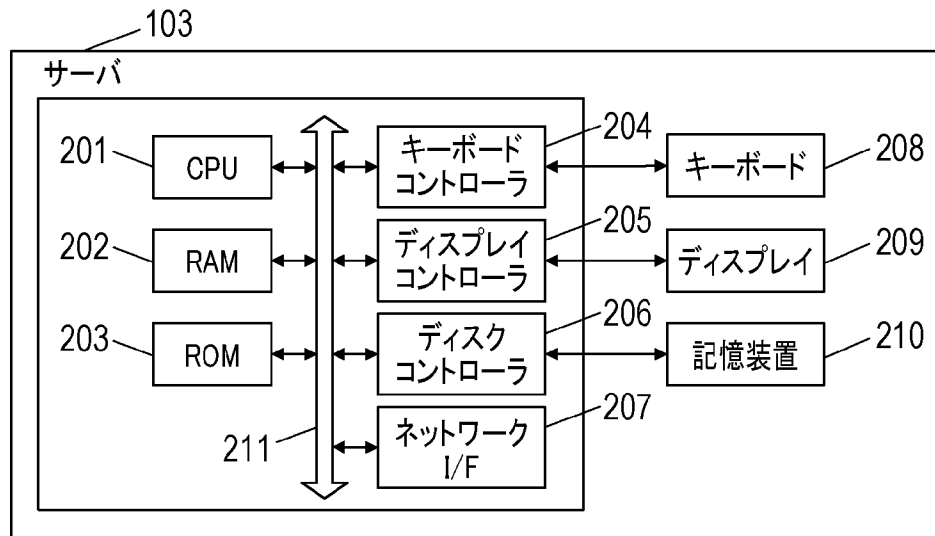
前記通知手段は、前記認証要求に応じた生体認証の結果、および、前記情報処理装置から前記外部認証器に対して送信される要求、の少なくとも何れかに応答して、前記ユーザに対して通知を行うことを特徴とする方法。

[請求項13] 請求項8乃至11の何れか1項に記載の手段としてコンピュータを機能させるためのプログラム。

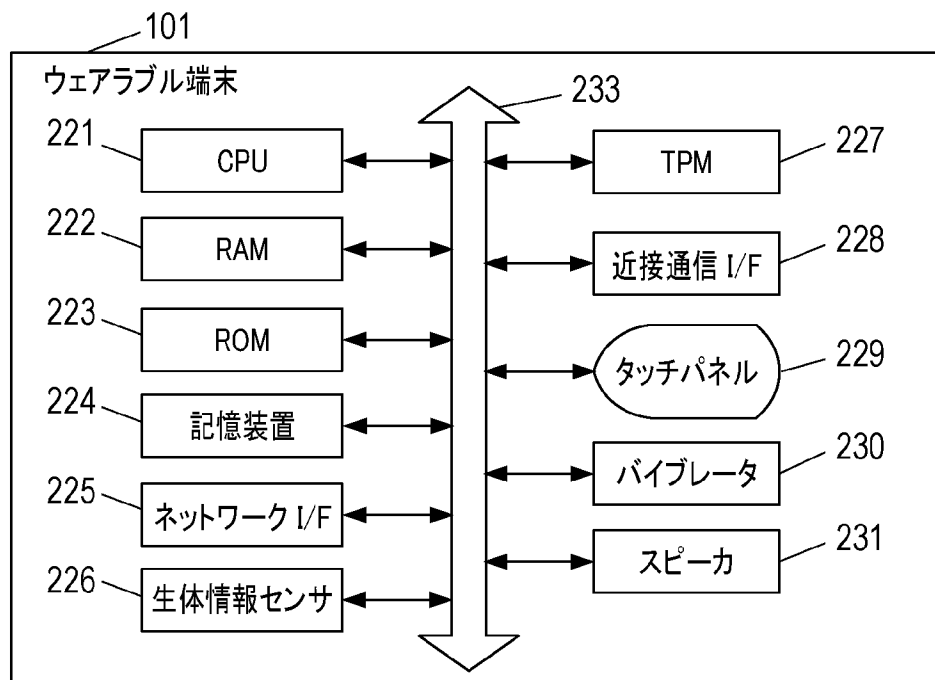
[図1]



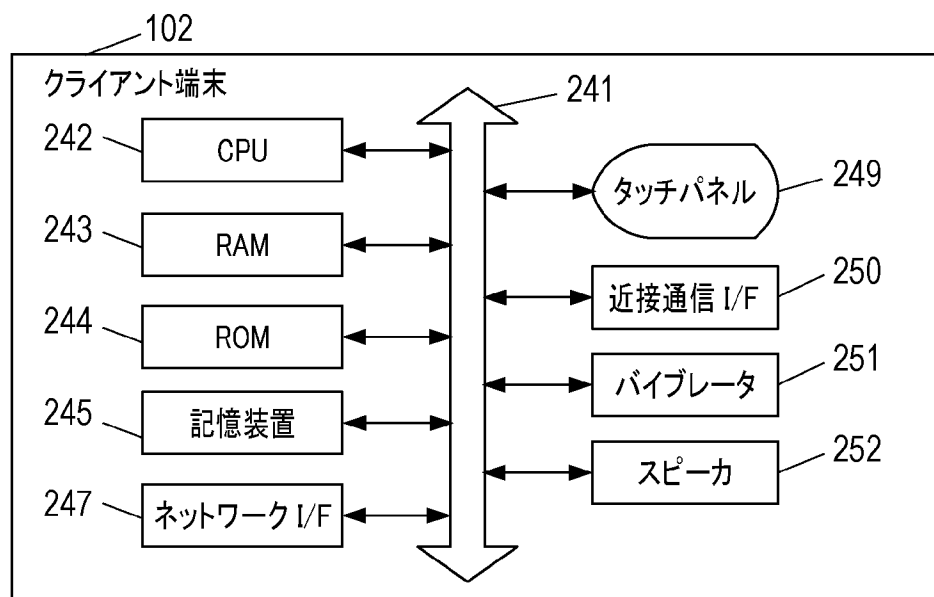
[図2A]



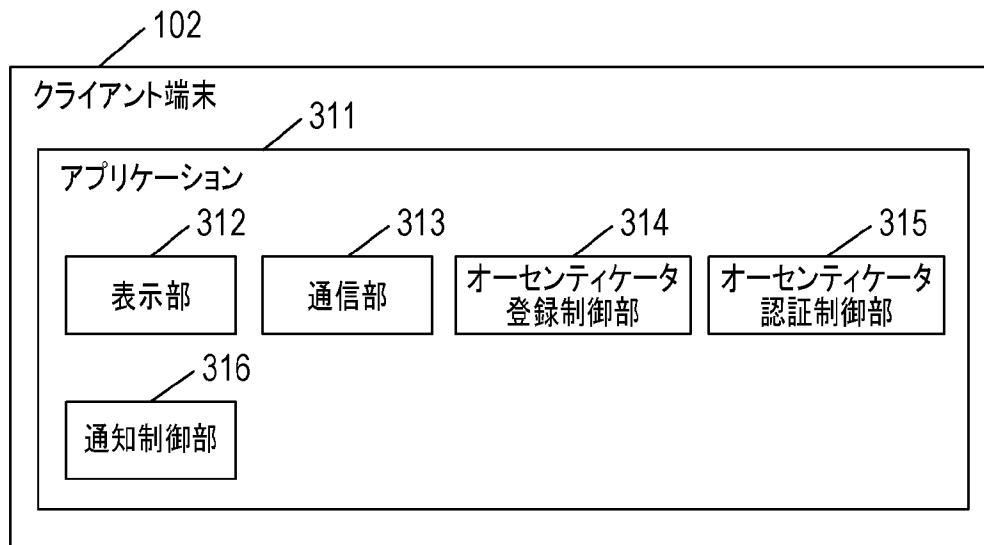
[図2B]



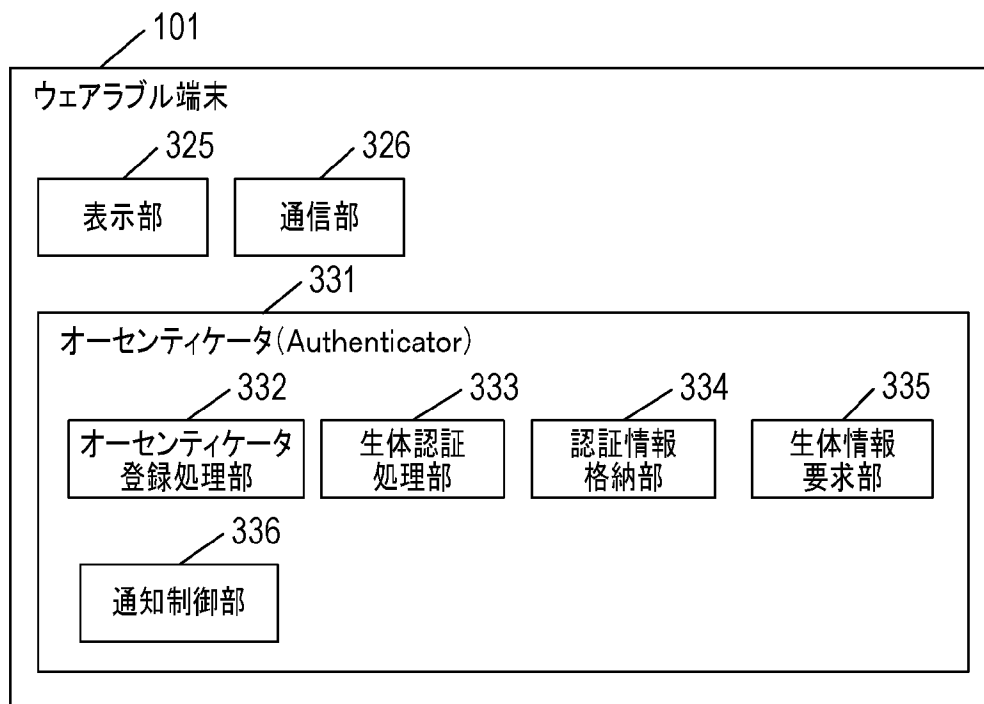
[図2C]



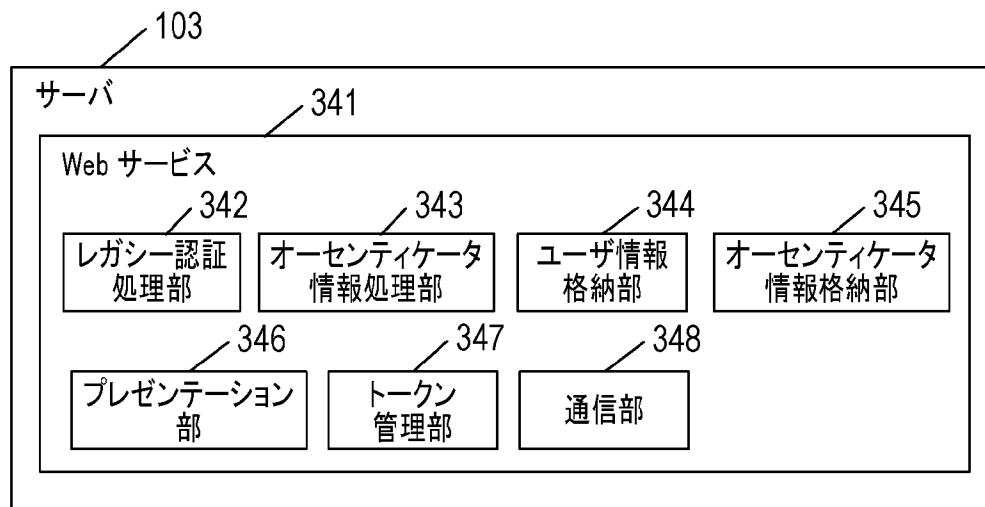
[図3A]



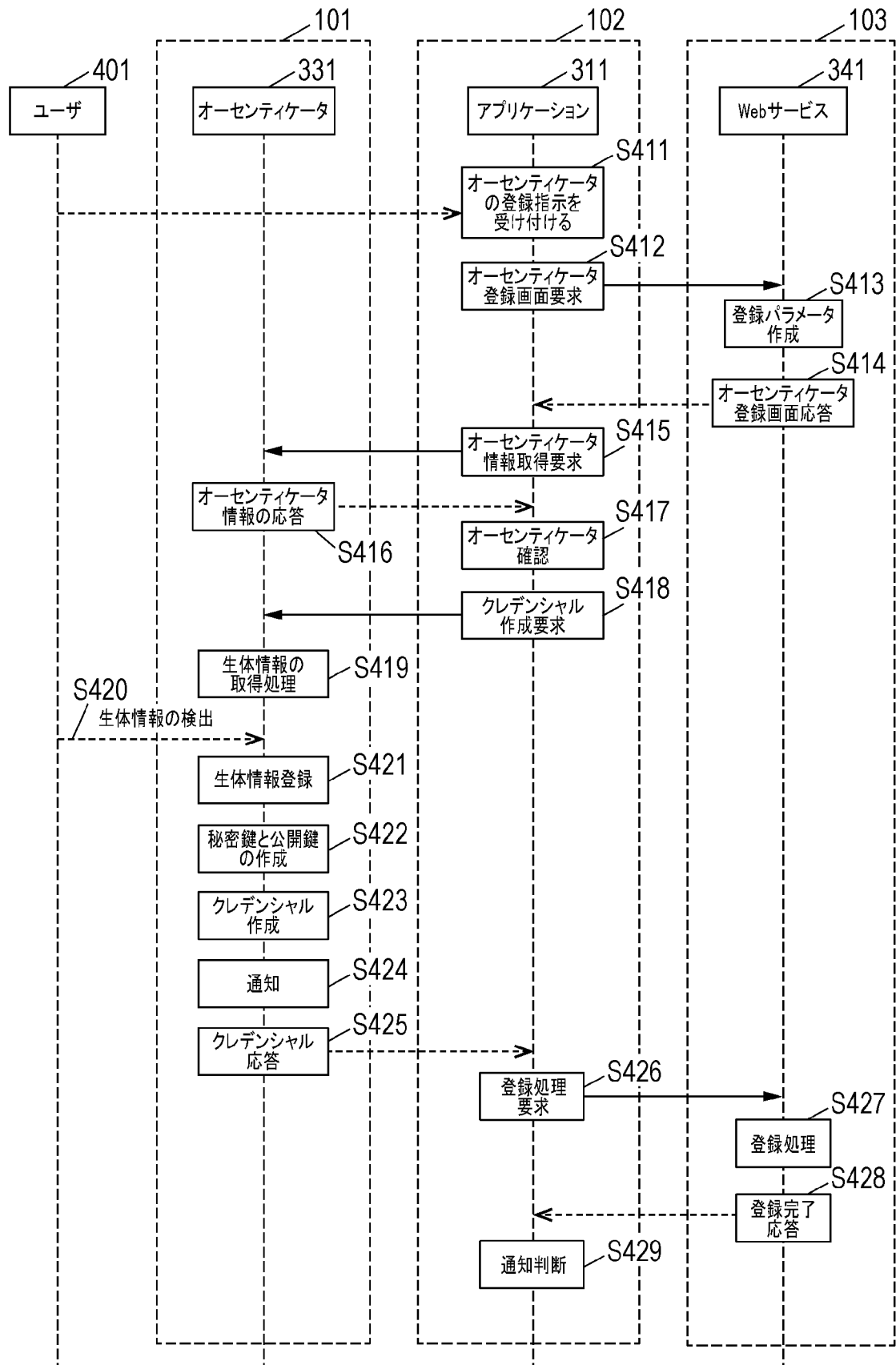
[図3B]



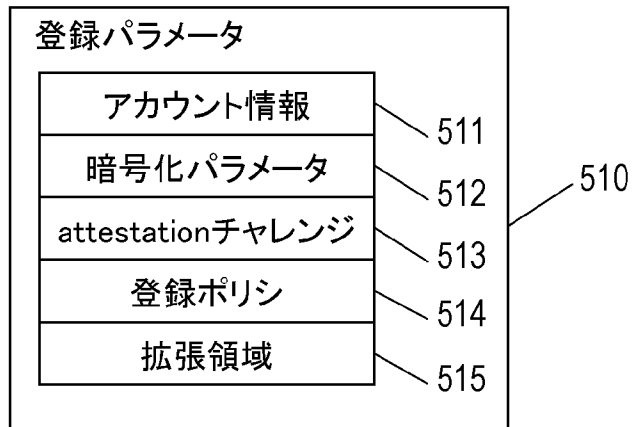
[図3C]



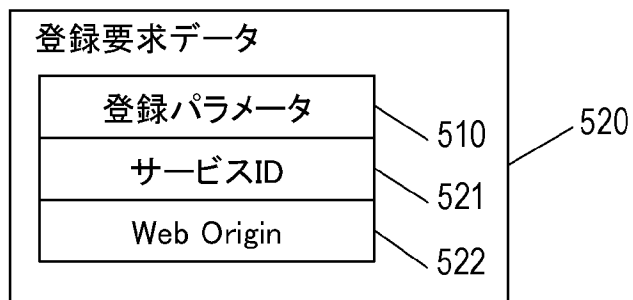
[図4]



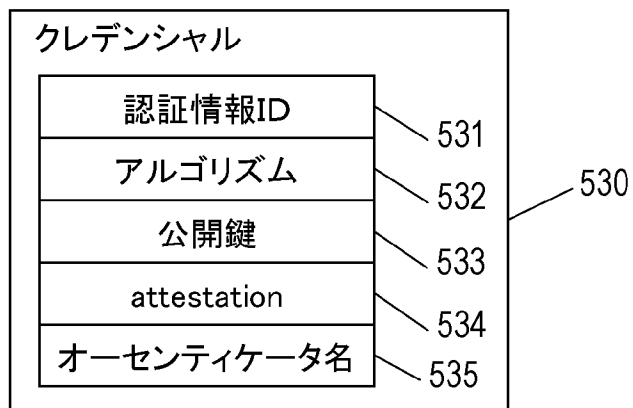
[図5A]



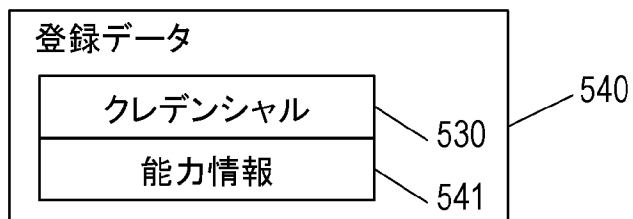
[図5B]



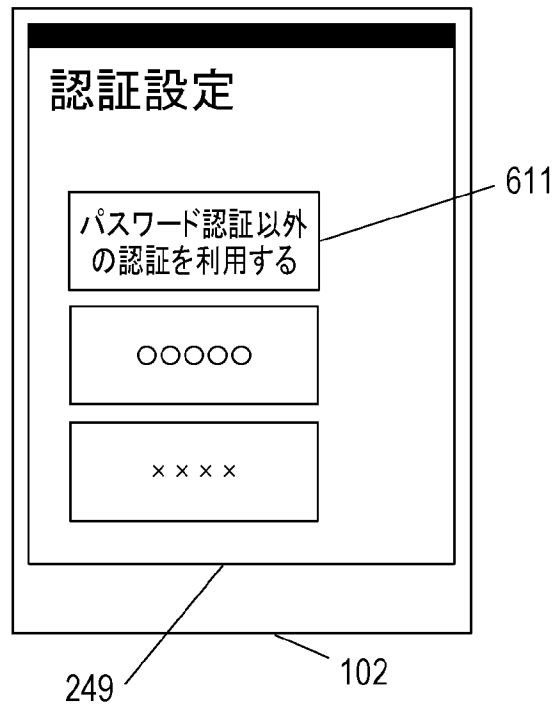
[図5C]



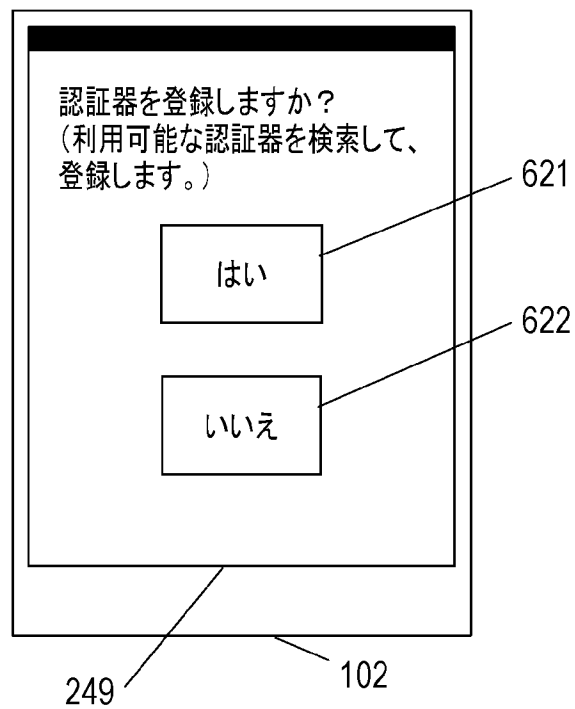
[図5D]



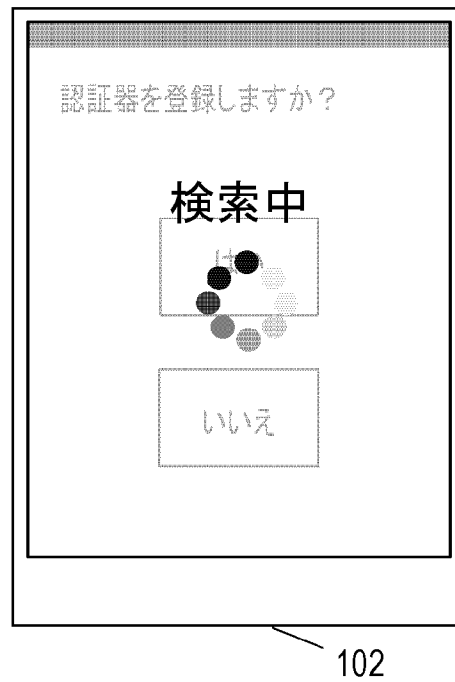
[図6A]



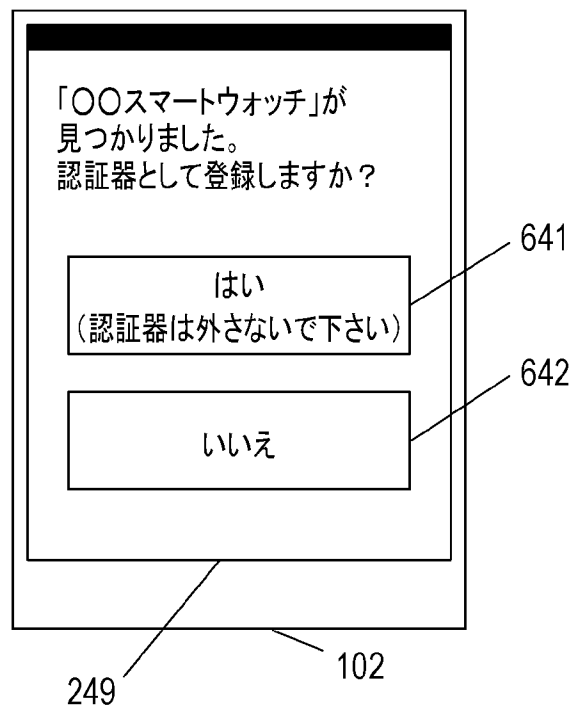
[図6B]



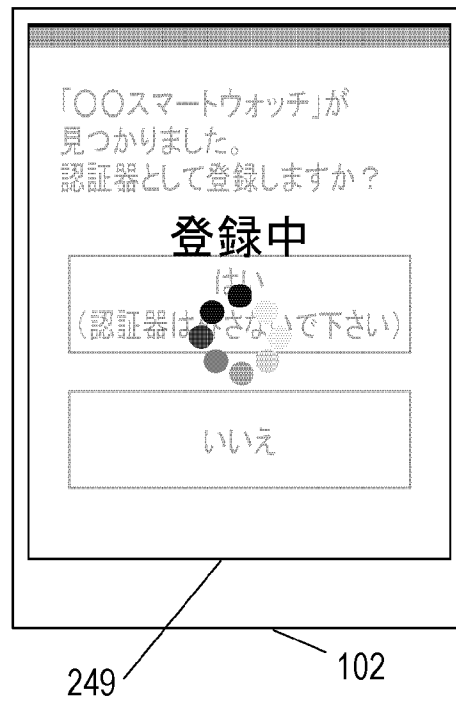
[図6C]



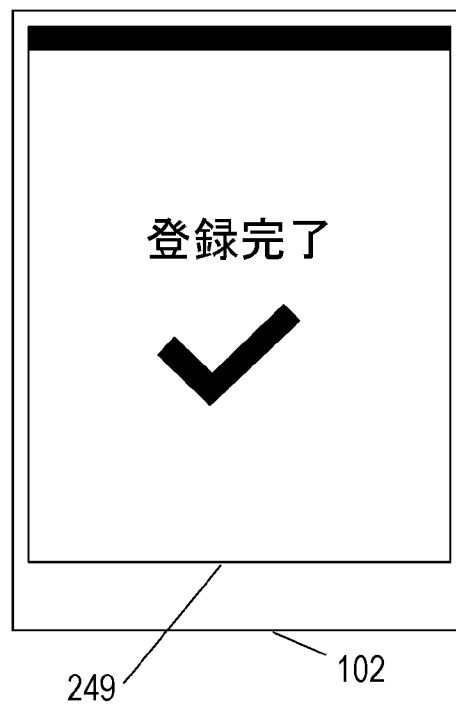
[図6D]



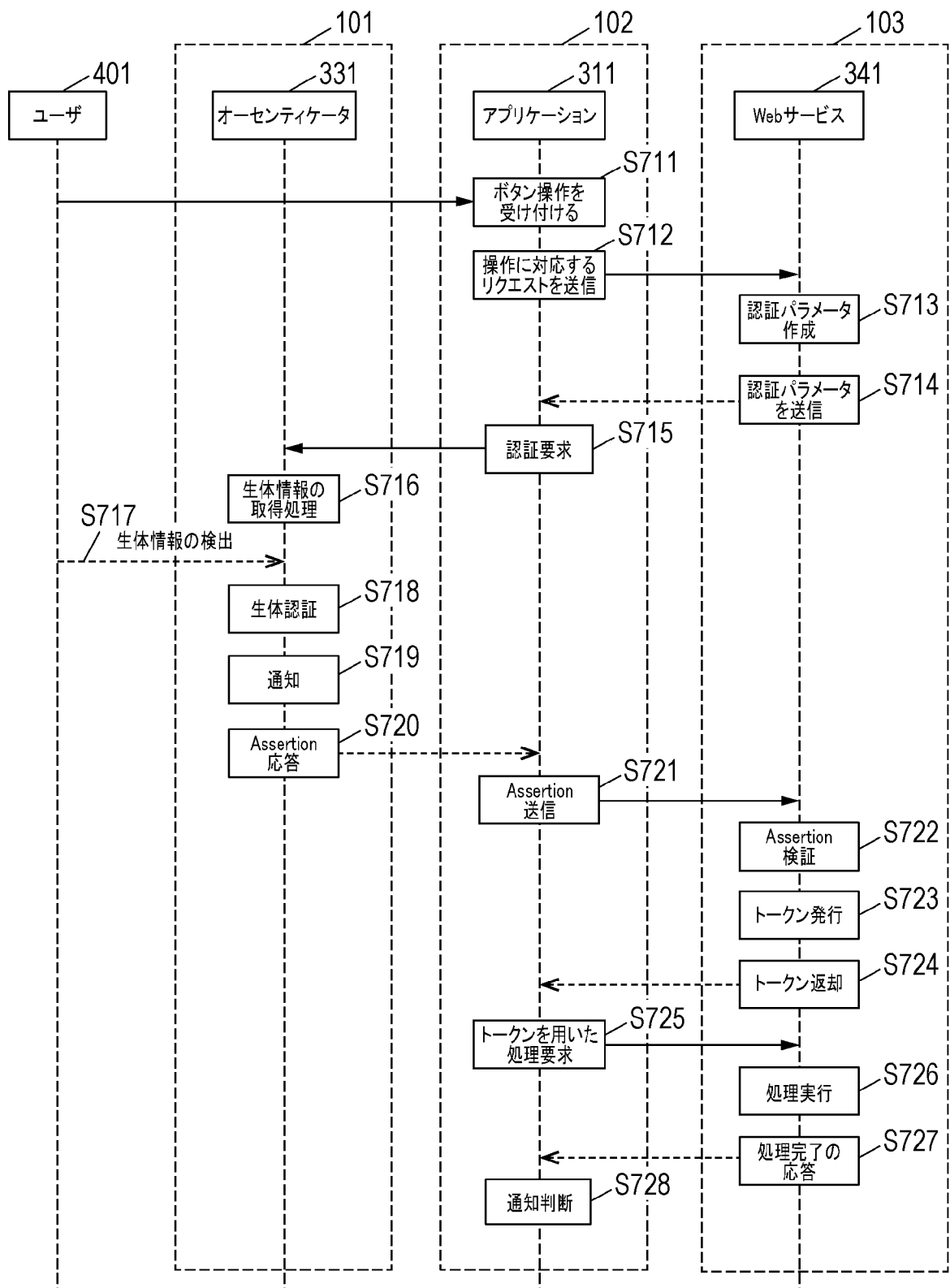
[図6E]



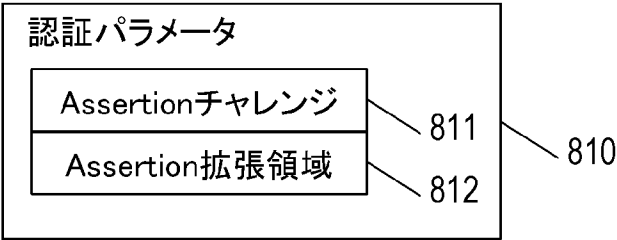
[図6F]



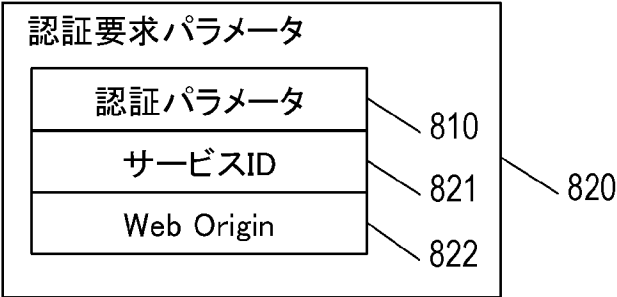
[図7]



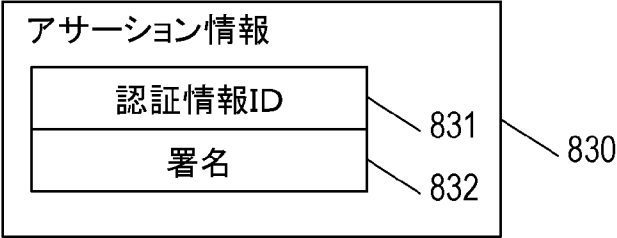
[図8A]



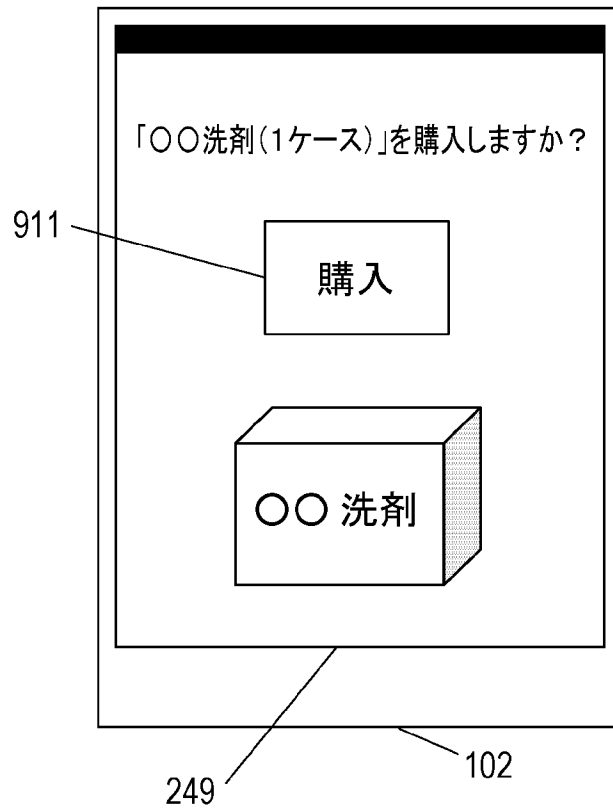
[図8B]



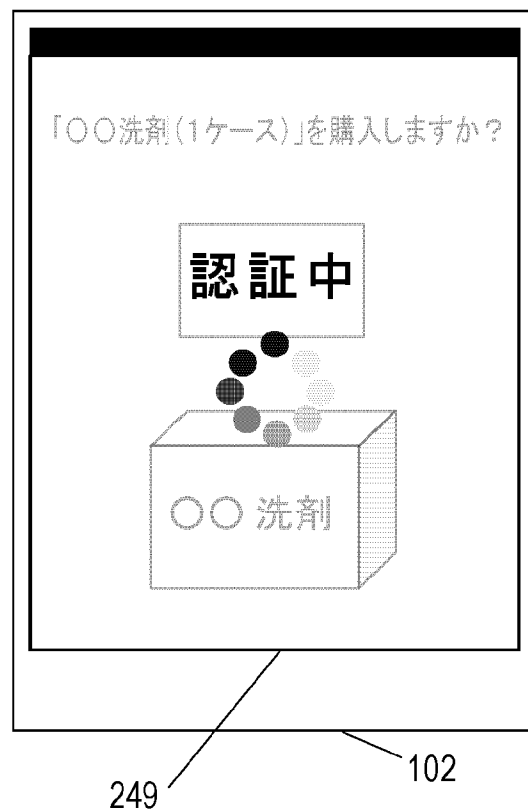
[図8C]



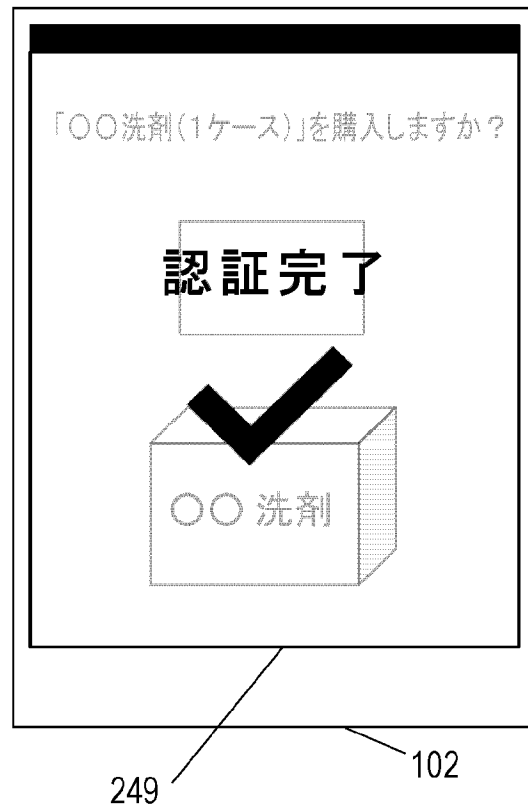
[図9A]



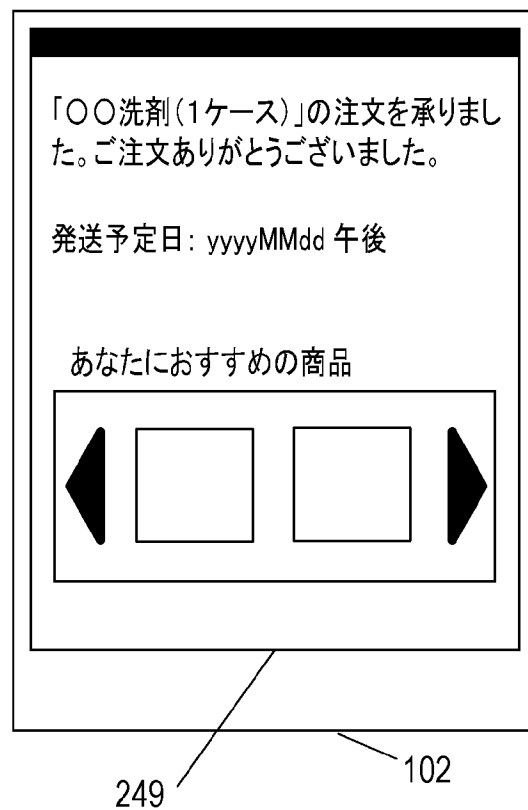
[図9B]



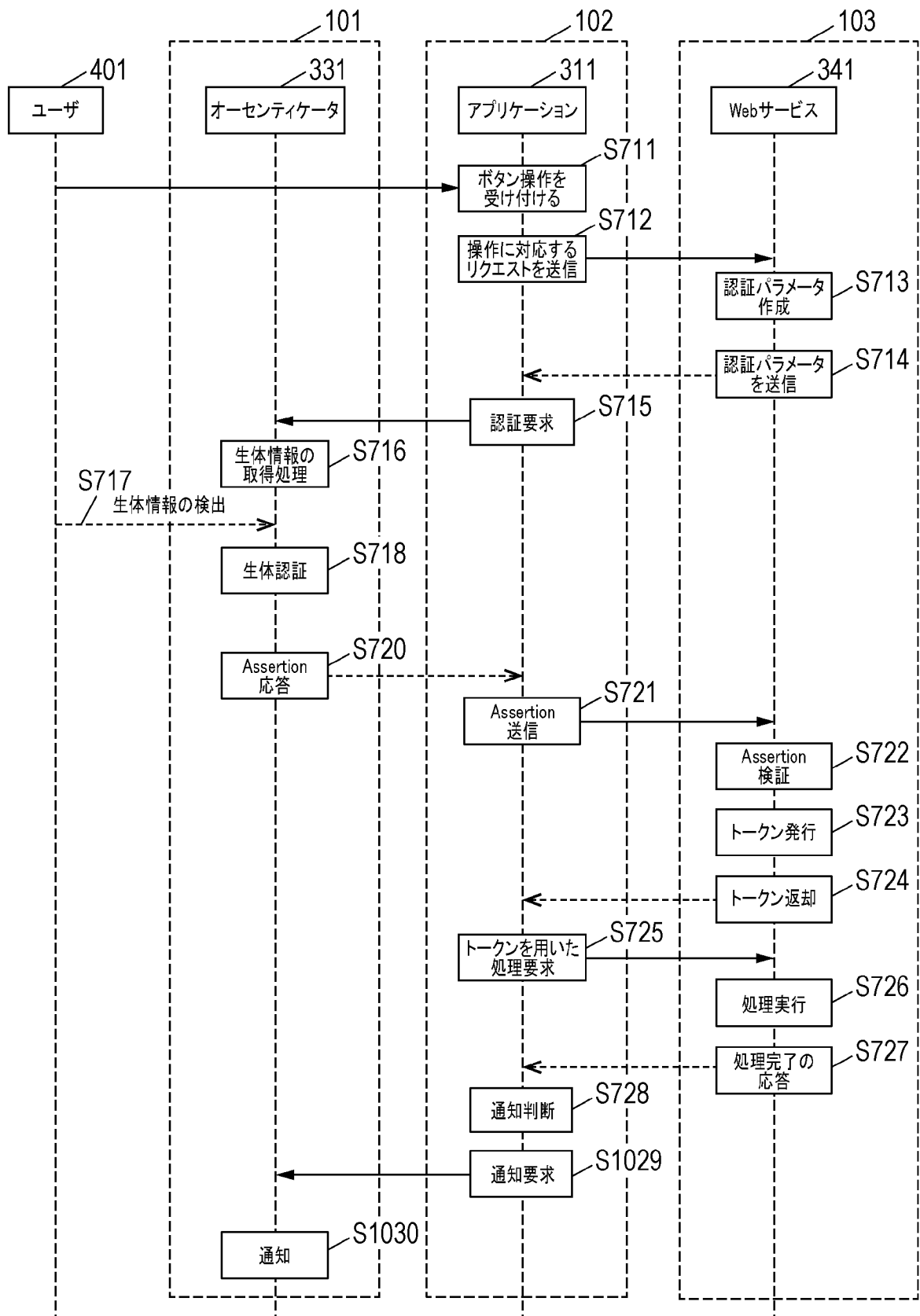
[図9C]



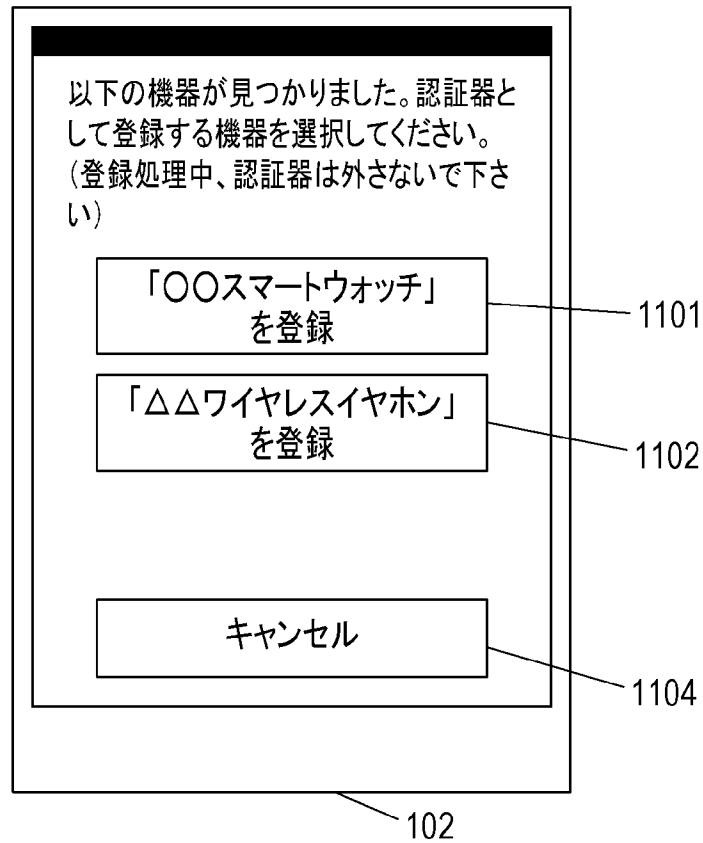
[図9D]



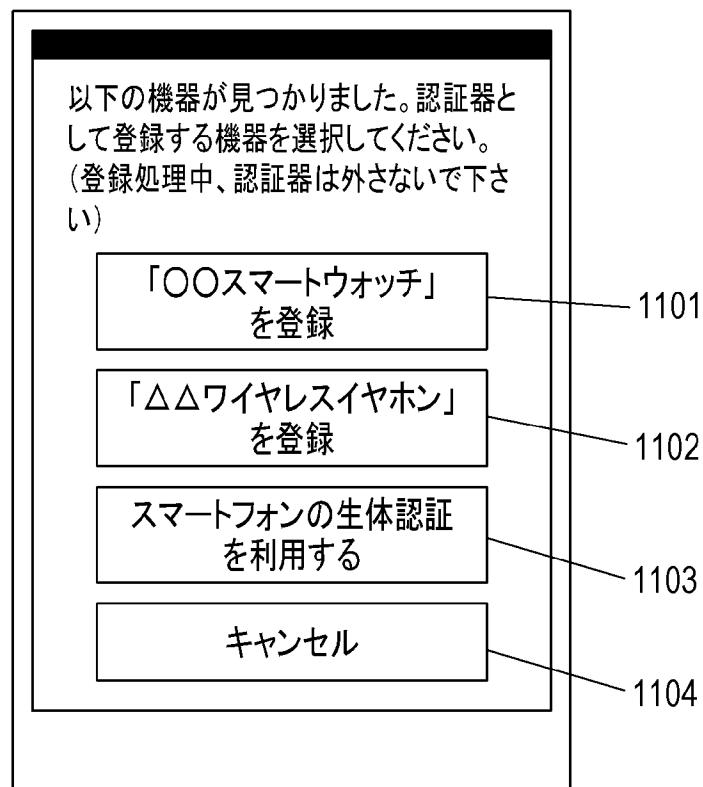
[図10]



[図11A]



[図11B]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/047909

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/32**(2013.01)i; **G06F 21/33**(2013.01)i; **G06F 3/01**(2006.01)i

FI: G06F21/32; G06F3/01 515; G06F21/33

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)

G06F21/32; G06F21/33; G06F3/01

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 1971-2022
 Registered utility model specifications of Japan 1996-2022
 Published registered utility model applications of Japan 1994-2022

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 2019-101504 A (CANON KK) 24 June 2019 (2019-06-24) paragraphs [0016]-[0167], fig. 1, 12, 13	1-5, 7
Y		1-13
Y	JP 2019-151997 A (DENSO CORP) 12 September 2019 (2019-09-12) paragraphs [0017], [0053]-[0102], fig. 1, 6, 11	1-13
Y	JP 2017-50810 A (PANASONIC INTELLECTUAL PROPERTY CORPORATION OF AMERICA) 09 March 2017 (2017-03-09) paragraphs [0039]-[0046], [0081]-[0087], fig. 2, 8, 9	1-13

☐ Further documents are listed in the continuation of Box C.☒ 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

08 March 2022

Date of mailing of the international search report

22 March 2022

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915
 Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2021/047909

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
JP	2019-101504	A	24 June 2019	US 2019/0165937 A1 paragraphs [0033]-[0178], fig. 1, 12, 13 EP 3489852 A1 CN 110059459 A	
JP	2019-151997	A	12 September 2019	US 2020/0391696 A1 paragraphs [0034], [0070]- [0119], fig. 1, 6, 11 WO 2019/167470 A1	
JP	2017-50810	A	09 March 2017	US 2017/0069179 A1 paragraphs [0051]-[0058], [0093]-[0099], fig. 2, 8, 9 CN 106502316 A	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/32(2013.01)i; G06F 21/33(2013.01)i; G06F 3/01(2006.01)i FI: G06F21/32; G06F3/01 515; G06F21/33		
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）） G06F21/32; G06F21/33; G06F3/01		
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 - 2022年 日本国実用新案登録公報 1996 - 2022年 日本国登録実用新案公報 1994 - 2022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 2019-101504 A (キヤノン株式会社) 24.06.2019 (2019 - 06 - 24) 段落[0016]-[0167], 図1, 12, 13	1-5, 7
Y		1-13
Y	JP 2019-151997 A (株式会社デンソー) 12.09.2019 (2019 - 09 - 12) 段落[0017], [0053]-[0102], 図1, 6, 11	1-13
Y	JP 2017-50810 A (パナソニック インテレクチュアル プロパティ コーポレー ション オブ アメリカ) 09.03.2017 (2017 - 03 - 09) 段落[0039]-[0046], [0081]-[0087], 図2, 8, 9	1-13
☐ 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、一般的な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抵触するものではなく、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 08.03.2022		国際調査報告の発送日 22.03.2022
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号		権限のある職員（特許庁審査官） 中里 裕正 5S 9364 電話番号 03-3581-1101 内線 3546

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2021/047909

引用文献			公表日	パテントファミリー文献			公表日
JP	2019-101504	A	24.06.2019	US	2019/0165937	A1	
				段落[0033]-[0178], 図1, 12, 13			
				EP	3489852	A1	
				CN	110059459	A	
JP	2019-151997	A	12.09.2019	US	2020/0391696	A1	
				段落[0034], [0070]-[0119], 図1, 6, 11			
				WO	2019/167470	A1	
JP	2017-50810	A	09.03.2017	US	2017/0069179	A1	
				段落[0051]-[0058], [0093]-[0099], 図2, 8, 9			
				CN	106502316	A	