

(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
2021年1月14日(14.01.2021)



(10) 国際公開番号

WO 2021/005841 A1

(51) 国際特許分類:

G06Q 20/18 (2012.01) *H04L 9/08* (2006.01)

G06F 21/44 (2013.01) *H04L 9/32* (2006.01)

(21) 国際出願番号: PCT/JP2020/012426

(22) 国際出願日: 2020年3月19日(19.03.2020)

(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 2019-128812 2019年7月10日(10.07.2019) JP

(72) 発明者; および

(71) 出願人: 市橋 敬男 (ICHIHASHI Norio) [JP/JP];
〒2510004 神奈川県藤沢市藤が岡一丁目7番
15号 Kanagawa (JP). 海沼 健一 (KAINUMA

Kenichi) [JP/JP]; 〒1350061 東京都江東区豊洲
3-6-5 豊洲タワー906号 Tokyo (JP).
長内 弘喜 (OSANAI Hiroki) [JP/JP]; 〒2260016
神奈川県横浜市緑区霧が丘6-1-1-
15-305 Kanagawa (JP).

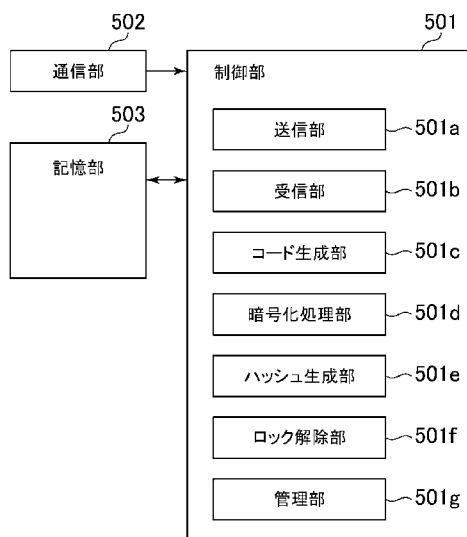
(74) 代理人: 特許業務法人 J A Z Y 国際特許事務
所 (JAZY INTERNATIONAL PATENT FIRM);
〒1000011 東京都千代田区内幸町2-2-1 日
本プレスセンタービル6F Tokyo (JP).

(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,

(54) Title: COMMUNICATION SYSTEM, COMMUNICATION METHOD, AND SENSOR UNIT

(54) 発明の名称: 通信システム、通信方法、およびセンサユニット

500



501 Control unit
501a Transmission unit
501b Reception unit
501c Code generation unit
501d Encryption processing unit
501e Hash generation unit
501f Unlocking unit
501g Management unit
502 Communication unit
503 Storage unit

(57) Abstract: The present invention provides a technology for enabling remote management of selling of commodities by a vending machine. The present invention pertains to a sensor unit 500 that is mounted to a vending machine and that unlocks the vending machine on the basis of encrypted data transmitted from a terminal device. This sensor unit is provided with: an encryption processing unit 501d that generates a public key and a secret key and that encrypts an unlocking code using the public key; a hash generation unit 501e that performs hashing, with a hash function, of sensor

HN, HR, HU, ID, IL, IN, IR, IS, 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,
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)）

information including at least a sensor ID and positional information of a sensor and outputs a hash value; a management unit 501g that stores and manages, in a storage unit 503, at least the public key and the hash value in association with each other; and an unlocking unit 501f that determines the success or failure of the encrypted data transmitted from the terminal device and that unlocks the vending machine when the encrypted data matches with the encrypted data generated by the encryption processing unit.

(57) 要約：自動販売機による商品の販売を遠隔管理できるようにする技術を提供する。本発明は、自動販売機に実装され、端末装置から送られてきた暗号化データに基づいて前記自動販売機のロックを解除するセンサユニット500であって、公開鍵と秘密鍵を生成し、開錠コードを公開鍵により暗号化する暗号化処理部501dと、少なくともセンサIDとセンサの位置情報を含むセンサ情報を、ハッシュ関数によりハッシュ化し、ハッシュ値を出力するハッシュ生成部501eと、少なくとも公開鍵とハッシュ値を対応付けて記憶部503に記憶し管理する管理部501gと、端末装置から送られてきた暗号化データの成否を判定し、暗号化データが、暗号化処理部が生成する暗号化データと合致する場合には、自動販売機のロックを解除するロック解除部501fとを備える。

明 細 書

発明の名称：通信システム、通信方法、およびセンサユニット
技術分野

[0001] 本発明は、通信システム、通信方法、およびセンサユニットに関する。

背景技術

[0002] インターネットなどの電気通信回線を利用したゲームの中には、特別なゲーム内アイテムやゲームキャラクタなどを得るための仕組みとして「ガチャ」と呼ばれる仕組みが採用されているものがある。「ガチャ」とは、硬貨を入れてハンドルひねると、玩具の入ったカプセルが出てくる自動販売機（所謂「ガチャガチャ」或いは「ガチャポン」：特許文献1参照）を模した仮想自動販売機である。

先行技術文献

特許文献

[0003] 特許文献1：特開平07-148358号公報

発明の概要

発明が解決しようとする課題

[0004] ガチャを利用したゲームでは、有料または無料で配布される仮想コインをガチャに投入することでアイテム等が得られる。この種のゲームにおいて有料のコインを購入することは課金と呼ばれる。有料のコインを必要とするガチャでは、一回数百円の課金で通常では得られない(或いは得難い)強力なアイテムや希少なキャラクタを入手することができる場合がある。このため、所望のアイテム等が得られるまで多額の課金を行い、その支払いに難儀するユーザもいる。これは、仮想自動販売機による商品販売に限らず、「ガチャガチャ」等を含む自動販売機による商品販売に共通の問題である。商品の売り手が買い手に直接対応する対面販売とは異なり、自動販売機による商品販売では売り手側が買い手に注意を促すことはできないからである。以下、本明細書では、「ガチャガチャ」などの実体のある自動販売機と仮想自動販売

機の両方を含めて「自動販売機」と呼ぶ。

[0005] 本発明は上述した事情に鑑みてなされたものであり、自動販売機による商品の販売を遠隔管理できるようにする技術を提供することを目的とする。

課題を解決するための手段

[0006] 上記課題を解決するために、本発明の第1態様に係る通信方法は、端末装置が、自動販売機に付された二次元コードを撮像して販売機IDを取得し、位置情報を取得し、前記販売機IDと前記位置情報を第1サーバ装置に送信することで、前記自動販売機のロック解除に関わる暗号化データの取得を要求する第1のステップと、第1サーバ装置が、前記販売機IDと位置情報とが、記憶している情報に合致するかを判定し、合致する場合には、商品情報を前記端末装置に送信する第2のステップと、第2のサーバ装置が、前記端末装置からの決済要求を受け、決済処理を実行し、決済トークンを前記第1サーバ装置に送信する第3のステップと、第1サーバ装置が、前記決済トークンを受信し、センサ情報をハッシュ関数によりハッシュ化したハッシュ値を生成し、前記端末装置に送信する第4のステップと、前記端末装置が、前記ハッシュ値により、ハッシュプールを実現する仮想サーバ装置群に対して検索要求を行う第5のステップと、前記仮想サーバ装置群が、前記検索要求を受け、ハッシュ値の存在を確認し、存在する場合には、公開鍵を第3サーバ装置に送信する第6のステップと、前記第3サーバ装置が、開錠コードを生成し、前記開錠コードを前記公開鍵により暗号化し、暗号化データを前記端末装置に送信する第7のステップと、前記端末装置が、前記暗号化データを前記自動販売機のセンサユニットに送信することで、前記自動販売機のロック解除を要求する第8のステップと、前記センサユニットが、前記暗号化データの成否を判断し、正しいと判断された場合には、前記自動販売機のロックを解除する第9のステップと、を有する。

[0007] そして、本発明の第2態様に係る通信システムは、自動販売機に付された二次元コードを撮像して販売機IDを取得し、撮像時の位置情報を取得し、前記販売機IDと前記位置情報を第1サーバ装置に送信すると共に、第1サ

サーバ装置より送られてきたハッシュ値によりハッシュプールを実現する仮想サーバ装置群に対して検索要求を行い、更には、第3サーバ装置から送られてきた暗号化データを前記自動販売機のセンサユニットに送信することで、前記自動販売機のロック解除を要求する端末装置と、前記販売機IDと位置情報とが、記憶している情報に合致するかを判定し、合致する場合には、商品情報を前記端末装置に送信すると共に、決済トークンを受信すると、記憶しているセンサ情報をハッシュ関数によりハッシュ化した前記ハッシュ値を生成し、前記端末装置に送信する第1サーバ装置と、前記端末装置から前記ハッシュ値による検索要求を受けると、前記ハッシュ値の存在を確認し、存在する場合には公開鍵を第3サーバ装置に送信する仮想サーバ装置群と、開錠コードを生成し、前記開錠コードを前記公開鍵により暗号化し、暗号化データを前記端末装置に送信する第3サーバ装置と、前記公開鍵を生成して前記仮想サーバ装置群に送信すると共に、前記端末装置から前記暗号化データを受信すると前記暗号化データの成否を判断し、正しいと判断された場合には、前記自動販売機のロックを解除するセンサユニットとを有する。

[0008] さらに、本発明の第3態様に係るセンサユニットは、自動販売機に実装され、端末装置から送られてきた暗号化データに基づいて前記自動販売機のロックを解除するセンサユニットであって、公開鍵と秘密鍵を生成し、開錠コードを公開鍵により暗号化する暗号化処理部と、少なくともセンサIDとセンサの位置情報を含むセンサ情報を、ハッシュ関数によりハッシュ化し、ハッシュ値を出力するハッシュ生成部と、少なくとも前記暗号化処理部が生成した前記公開鍵と前記ハッシュ生成部が生成した前記ハッシュ値を対応付けて記憶部に記憶し管理する管理部と、前記端末装置から送られてきた暗号化データの成否を判定し、前記暗号化データが、前記暗号化処理部が生成する暗号化データと合致する場合には、前記自動販売機のロックを解除するロック解除部とを備える。

発明の効果

[0009] 本発明によれば、自動販売機による商品の販売を遠隔管理できるようにす

る技術を提供することができる。特に、センサユニットは、ガチャ等の既存の自動販売機等に後付けで実装することが可能であり、その場合、既存の自動販売機等の販売を遠隔管理することが可能となる。

図面の簡単な説明

[0010] [図1]本発明の第1実施形態による無線通信システム1の構成例を示すブロック図である。

[図2]無線通信端末10と近距離無線通信する自動販売機30の正面図である。

[図3]無線通信端末10の構成例を示すブロック図である。

[図4]無線通信端末10の表示部110aに表示される画面G01の一例を示す図である。

[図5]無線通信端末10の表示部110aに表示される検索結果画面G02の一例を示す図である。

[図6]無線通信端末10の表示部110aに表示される決済手段選択画面G03の一例を示す図である。

[図7]無線通信端末10の制御部100が購入支援プログラム144aにしたがって実行するロック解除処理の流れを示すフローチャートである。

[図8]本発明の第2実施形態に係る通信システムの構成図である。

[図9]同システムによる処理手順を示す概念図である。

[図10]第1サーバ装置の構成図である。

[図11]第2サーバ装置の構成図である。

[図12]第3サーバ装置の構成図である。

[図13]端末装置の構成図である。

[図14]センサユニットの構成図である。

[図15]同システムによる処理手順を示すフローチャートである。

発明を実施するための形態

[0011] 以下、図面を参照しつつ本発明の実施形態を説明する。

[0012] <第1実施形態>

[0013] 図1は、本発明の第1実施形態による無線通信システム1の構成例を示すブロック図である。図1に示すように、無線通信システム1は、無線通信端末10と、無線通信網20に接続されたサーバ装置40とを含む。図1では詳細な図示を省略したが、無線通信網20には有線通信網が含まれ、サーバ装置40は当該有線通信網に接続されている。

[0014] 無線通信端末10は例えばスマートフォンである。無線通信端末10は無線通信網20に收容され、所定の無線通信規格（本実施形態ではW I - F I、但し、これには限定されない）にしたがって無線通信を行う。また、無線通信端末10は、上記無線通信規格とは異なる無線通信規格にしたがって他の装置と近距離無線通信を行う機能を備えている。以下では、後者の無線通信規格を「第1の無線通信規格」と呼び、前者の無線通信規格を「第2の無線通信規格」と呼ぶ。前述したように第2の無線通信規格の具体例はW I - F Iである。一方、第1の無線通信規格の具体例としては、B l u e t o o t h（登録商標）またはI r D Aが挙げられる。本実施形態では、第1の無線通信規格としてB l u e t o o t h（登録商標）が採用されている。

[0015] 図1における自動販売機30は、前述した「ガチャガチャ」である。自動販売機30は、第1の無線通信規格にしたがって無線通信端末10と近距離無線通信を行う機能を備えている。図1では、自動販売機30が1つだけ図示されているが、自動販売機30の数は2以上であってもよい。図2は、自動販売機30の正面図である。自動販売機30では、商品代金の投入（本実施形態では、仮想コインの入力）が行われた後にハンドル32が矢印方向に捻られると、玩具の入ったカプセルCが取出し口34から1つ出てくる。取出し口34の近傍には、自動販売機30を一意に示す識別子（例えば所定の文字数の英数文字よりなる文字列）に対応するマトリクス型二次元コードが印刷された印刷物36が貼り付けられている。

[0016] 自動販売機30では、商品の販売禁止を解除するセキュリティコードを近距離無線通信により受信するまで商品の販売が禁止されたロック状態となっており、セキュリティコードを未受信の状態でハンドル32が捻られてもカ

プセルCは出てこない。セキュリティコードはサーバ装置40によってランダムに生成される256バイトの1タイムデータである。サーバ装置40は、自動販売機30を一意に示す識別子を受信する毎に、その識別子に対応するセキュリティコードを発行し、当該識別子の送信元へ返信する。

[0017] サーバ装置40は、図1に示すように、ユーザDBと自動販売機管理DBとを有するコンピュータ装置であり、セキュリティコード発行および仮想通貨の発行の他に、仮想通貨の発行代金の決済（換言すれば、商品代金の決済）を行う。自動販売機管理DBには、自動販売機30の識別子に対応付けて、当該自動販売機30の設置場所を示す位置情報（例えば、設置場所の緯度および経度を示す情報）、セキュリティコードを発行するための情報が格納されている。セキュリティコードを所定の疑似乱数発生アルゴリズムにしたがって生成する場合、セキュリティコードを発行するための情報の具体例としては当該アルゴリズムにおける初期値（所謂疑似乱数のシード）や直前に発行したセキュリティコードが挙げられる。

[0018] ユーザDBは、無線通信システム1を利用して自動販売機30による商品の販売を解禁し、商品を購入しようとするユーザを管理するためのデータベースである。ユーザDBにはユーザを一意に示す識別子に対応付けて当該ユーザによる商品の購入履歴や商品代金の決済履歴を示す情報が格納されている。ユーザを一意に識別する識別子の具体例としては、無線通信システム1によるサービスの利用契約締結時にユーザに割り振られたユーザIDが挙げられる。

[0019] 本実施形態における商品代金の決済には、ブロックチェーンと呼ばれる分散型台帳技術が利用されている。ブロックチェーンとは、ブロックと呼ばれる順序付けられたレコードの連続的に増加するリストを持つデータベースである。本実施形態では、ブロックチェーンにおける各ブロックが1つの決済に対応し、各ブロックには決済に関する情報と決済の実行された時刻を示すタイムスタンプと、一つ前のブロックへのリンクとが含まれている。

[0020] 前述したように自動販売機30の取出し口34の近傍には、自動販売機3

0の一意に示す識別子に対応するマトリクス型二次元コードの印刷された印刷物36が貼り付けられている。無線通信端末10のユーザは、無線通信端末10を用いて上記マトリクス型二次元コードを読み取り、当該コードから得られた識別子をサーバ装置40へ送信することで、自動販売機30のロック状態を解除すること（すなわち、商品の販売を解禁すること）ができる。以下、自動販売機30による商品の販売を解禁する際に中心的な役割を果たす無線通信端末10について説明する。

[0021] 図3は、無線通信端末10の構成例を示すブロック図である。図3に示すように、無線通信端末10は、制御部100、ユーザインタフェース部110、第1無線通信部120、第2無線通信部130、記憶部140、およびこれら構成要素間のデータ授受を仲介するバス150を有する。なお、図3では、ユーザインタフェース部は「UI部」と略記されている。以下、本明細書においても同様に略記する。

[0022] 制御部100は、例えばCPU（Central Processing Unit）などのコンピュータである。制御部100は、記憶部140（より正確には不揮発性記憶部144）に格納されているプログラムを実行し、無線通信端末10の制御中枢として機能する。

[0023] UI部110は、無線通信端末10をユーザに利用させるためのユーザインタフェースを提供する装置の集合体である。図1に示すように、UI部110は、表示部110a、操作部110b、および撮像部110cを含む。UI部110は、これら各部の他にユーザの音声の收音および音声データの表す音声の出力を行う音声入出力部を含んでいるが、本発明との関連が薄いため音声入出力部の図示および詳細な説明は省略する。

[0024] 表示部110aは、例えば液晶ディスプレイとその駆動回路である。表示部110aは、制御部100による制御の下、無線通信端末10の利用をユーザに促す各種画面の画像を表示する。撮像部110cは例えばイメージセンサである。撮像部110cは、撮像視野内の画像を撮像し、その撮像結果を表す画像データを制御部100へ出力する。操作部110bは、表示部1

10aの表示領域を覆うように設けられた透明なシート状のタッチセンサである。操作部110bは、表示部110aとともに所謂タッチパネルを形成する。無線通信端末10のユーザは、操作部110bに対するタッチ操作或いはフリック操作により各種入力を行うことができる。操作部110bに対してユーザがタッチ操作或いはフリック操作等を行うと、操作部110bは、ユーザの操作内容を表すデータを制御部100へ出力する。これにより、ユーザの行った操作が制御部100に伝達される。

[0025] 第1無線通信部120は、第1の無線通信規格に準拠した無線通信を行う通信回路である。第1無線通信部120は、第1の無線通信規格に準拠した無線通信の相手装置から送信されてくるデータを受信して制御部100へ引き渡す一方、制御部100から引き渡されたデータを相手装置へ送信する。第2無線通信部130は、無線通信網20の基地局と第2の無線通信規格に準拠した無線通信を行う。第2無線通信部130は、制御部100から与えられたデータを無線通信網20へ送出するとともに、無線通信網20から送られてくるデータを受信し、受信したデータを制御部100へ引き渡す。

[0026] 記憶部140は、揮発性記憶部142と不揮発性記憶部144とを含む。揮発性記憶部142は、例えばRAM(Random Access Memory)である。揮発性記憶部142は、プログラムを実行する際のワークエリアとして制御部100によって利用される。不揮発性記憶部144は、例えばフラッシュROM(Read Only Memory)である。不揮発性記憶部144には、各種プログラムと各種データとが記憶されている。不揮発性記憶部144に記憶されているプログラムの具体例としては、制御部100にOS(Operating System)を実現させるカーネルプログラム、webブラウザや電子メールクライアントの各種アプリケーションプログラム、本発明の特徴を顕著に示すロック解除処理を制御部100に実行させる購入支援プログラム144aが挙げられる。

[0027] 不揮発性記憶部144に記憶されているプログラムのうち、購入支援プログラム144a以外のプログラムについては一般的なスマートフォンにイン

ストールされているものと特段に変わるところは無い。例えば、制御部 100 は、無線通信端末 10 の電源（図 3 では図示略）の投入を契機としてカーネルプログラムを不揮発性記憶部 144 から揮発性記憶部 142 へ読み出し、その実行を開始する。カーネルプログラムに従って作動し、OS を実現している状態の制御部 100 は、操作部 110b に対する操作により入力された指示に応じて、購入支援プログラム 144a や他のアプリケーションプログラムを実行することや UI 部 110 等の制御部 100 以外の構成要素の作動制御を行うことができる。このように、購入支援プログラム 144a 以外のプログラムについては一般的なスマートフォンにインストールされているものと特段に変わるところは無いため詳細な説明は省略し、以下では購入支援プログラム 144a を中心に説明する。

[0028] 操作部 110b に対する操作により購入支援プログラム 144a の実行を指示された制御部 100 は、購入支援プログラム 144a を不揮発性記憶部 144 から揮発性記憶部 142 へ読み出し、その実行を開始する。購入支援プログラム 144a にしたがって作動している制御部 100 は、図 4 に示す画面 G01 を表示部 110a に表示させる。

[0029] 画面 G01 における仮想操作子 B01 は、自動販売機 30 の設置場所を検索するための仮想操作子である。仮想操作子 B01 に対するタッチ操作が為されると、制御部 100 は、無線通信端末 10 の現在位置を示す位置情報をサーバ装置 40 へ送信する。なお、無線通信端末 10 の現在位置については GPS 等の既存技術を用いて特定すればよい。

[0030] サーバ装置 40 は、無線通信端末 10 から受信した位置情報の示す位置を中心とする所定範囲（例えば、半径 100 メートルの範囲）に設置されている自動販売機 30 を、自動販売機管理 DB を参照して特定する。そして、サーバ装置 40 は、特定した自動販売機 30 の設置場所を示す位置情報を無線通信端末 10 へ返信する。

[0031] サーバ装置 40 から返信されてくる位置情報を受信すると、制御部 100 は、図 5 に示す検索結果画面 G02 を表示部 110a に表示する。検索結果

画面G02の画像は、上記所定範囲の地図の画像に、現在位置を示すアイコン（図5では、星印のアイコン）と自動販売機30に対応するアイコン（図5では黒丸印のアイコン）をプロットして得られる画像である。検索結果画面G02を視認したユーザは、検索結果画面G02に表示された情報を参考に最寄りの自動販売機30の設置場所まで赴くことができる。

[0032] 画面G01における仮想操作子B02に対するタッチ操作が行われると、制御部100は表示部110aの表示画像を、図6に示す決済手段選択画面G03に遷移させる。決済手段選択画面G03は、商品を購入するための仮想コインの決済に用いる決済手段（クレジットカード等）をユーザに選択させるための画面である。操作部110bに対する操作により決済手段の選択が為されると、制御部100は、選択された決済手段を示す情報を揮発性記憶部142に書き込み、表示部110aの表示画像を画面G01に遷移させる。

[0033] 画面G01における領域A01には、撮像部110cによる撮像画像が表示される。無線通信端末10のユーザは、自動販売機30の識別子に対応するマトリクス型二次元コードの全体が領域A01に表示されるように、無線通信端末10を自動販売機30の取出し口34の近傍にかざしつつその姿勢を調整し、当該マトリクス型二次元コードの画像を撮像する。制御部100は、撮像された画像を解析することで自動販売機30の識別子を取得する。

[0034] 自動販売機30の識別子を取得すると、制御部100は、ロック解除処理を開始する。図7は、ロック解除処理の流れを示すフローチャートである。図7に示すように、制御部100は、まず、上記の要領で取得した識別子と、決済手段選択画面G03にて選択された決済手段を示す情報とを第2無線通信部130によりサーバ装置40へ送信する（ステップSA100）。

[0035] サーバ装置40は、無線通信端末10から送信された識別子および決済手段を示す情報を受信すると、自動販売機管理DBの格納内容を参照して当該識別子に対応するセキュリティコードを発行するとともに、商品購入のための仮想コインを発行して上記受信した情報の示す決済手段により商品代金の

決済を行う。そして、サーバ装置40は、発行したセキュリティコードおよび仮想コインを、上記識別子の送信元へ返信する。

[0036] 制御部100は、サーバ装置40から返信されてくるセキュリティコードおよび仮想コインを受信すると、受信したセキュリティコードおよび仮想コインを第1無線通信部120により自動販売機30へ送信する（ステップS A110）。

[0037] 自動販売機30は、無線通信端末10から送信されてくるセキュリティコードおよび仮想コインを受信すると、商品の販売を解禁する。これにより、自動販売機30により販売される商品の購入（本実施形態では、ガチャガチャの実行）が可能となる。自動販売機30は、無線通信端末10のユーザによる商品の購入が完了すると、再びロック状態に戻る。

[0038] 以上説明したように第1実施形態によれば、セキュリティコードの発行により、自動販売機による商品の販売を遠隔管理することが可能になる。例えば、所定の期間（例えば一か月）における商品購入代金の総額が予め定められた上限値に達した以降は当該期間が経過するまで新たなセキュリティコードの発行を差し止めることで、ガチャガチャに課金しすぎることを防ぐことができる。

[0039] 以上本発明の第1実施形態について説明したが、この実施形態に以下の変形を加えても勿論よい。

（1）上記実施形態における自動販売機30は「ガチャガチャ」であったが、清涼飲料水やアルコール飲料、食品、書籍、煙草などに自動販売機であっても勿論よく、また、コンピュータゲームにおける「ガチャ」等の仮想自動販売機であってもよい。つまり、自動販売機30により販売される商品は玩具等の実体のある物には限定されず、ゲーム内アイテムやゲームキャラクターのデータ等のデータであってもよい。また、上記実施形態では、商品の販売代金の決済に仮想コインを介在させたが、仮想コインを介在させず、従来のガチャガチャと同様に現実の貨幣のみで決済を行ってもよく、この場合、サーバ装置40にはセキュリティコードのみを返信させるようにすればよい。

[0040] (2) 上記実施形態における自動販売機 30 には、自動販売機 30 を一意に示す識別子に対応するマトリクス型二次元コードが印刷された印刷物 36 が貼り付けられていたが、当該識別子を表す文字列の印刷された印刷物が貼り付けられていてもよい。識別子を表す文字列の印刷された印刷物を撮像部 110c で撮像し、その撮像画像に文字認識を施すことで上記識別子を取得することができるからである。また、上記印刷物に印刷された文字列を視認したユーザが操作部 110b に対する操作（例えば、仮想キーボードに対する操作）により、当該文字列を構成する文字を 1 つずつ入力してもよく、この場合、撮像部 110c は省略可能である。

[0041] (3) 上記実施形態では、無線通信端末 10 を含む無線通信システム 1 について説明したが、無線通信端末 10 を単体で製造または販売してもよい。また、上記実施形態における無線通信端末 10 はスマートフォンであったが、タブレット端末やノート型パーソナルコンピュータ、或いはウェアラブルコンピュータなどのであってもよい。

[0042] 要は、制御部と、第 1 の無線通信規格にしたがって近距離無線通信を行う第 1 無線通信部と、前記第 1 の無線通信規格とは異なる第 2 の無線通信規格にしたがった通信を行う第 2 無線通信部と、を備え、前記制御部は、前記第 1 の無線通信規格にしたがって他の装置と近距離無線通信を行う自動販売機であって、商品の販売禁止を解除するセキュリティコードを受信するまで商品の販売が禁止されている自動販売機を一意に識別するために当該自動販売機に付与されている識別子の入力を契機として、前記第 2 の無線通信規格にしたがった通信により前記識別子を受信したことを契機として前記セキュリティコードを発行し前記識別子の送信元へ返信するサーバ装置へ宛てて、入力された識別子を前記第 2 無線通信部により送信し、前記サーバ装置から返信されてくるセキュリティコードを前記第 2 無線通信部により受信し、受信したセキュリティコードを前記第 1 無線通信部により前記自動販売機へ送信することを特徴とする無線通信端末、を提供すればよい。

[0043] (4) 上記実施形態では、無線通信端末 10 の不揮発性記憶部 144 に本発

明の特徴を顕著に示すロック解除処理を制御部 100 に実行させる購入支援プログラム 144 a が予めインストールされていたが、購入支援プログラム 144 a を単体で製造または販売してもよい。要は、コンピュータに、第 1 の無線通信規格にしたがって他の装置と近距離無線通信を行う自動販売機であって、商品の販売禁止を解除するセキュリティコードを受信するまで商品の販売が禁止されている自動販売機を一意に識別するために当該自動販売機に付与されている識別子の入力を契機として、前記第 1 の無線通信規格とは異なる第 2 の無線通信規格にしたがった通信により前記識別子を受信したことを契機として前記セキュリティコードを発行し前記識別子の送信元へ返信するサーバ装置へ宛てて、入力された識別子を前記第 2 の無線通信規格にしたがって送信する第 1 のステップと、前記サーバ装置から返信されてくるセキュリティコードを受信し、受信したセキュリティコードを第 1 の無線通信規格にしたがって前記自動販売機へ送信する第 2 のステップと、を実行させることを特徴とするプログラムを提供すればよい。

[0044] 従来の無線通信端末に上記プログラムをインストールし、当該無線通信端末の制御部（コンピュータ）を当該プログラムにしたがって作動させることで、当該無線通信端末を上記実施形態の無線通信端末 10 として機能させることが可能になるからである。なお、上記プログラムの具体的な提供態様としては、フラッシュ ROM などのコンピュータ読み取り可能な記録媒体に書き込んで配布する態様や、インターネットなどの電気通信回線経由のダウンロードにより配布する態様が考えられる。

[0045] <第 2 実施形態>

本発明の第 2 実施形態に係る通信システム、通信方法、及びセンサユニットによればガチャ等の自動販売機の販売に係るロックを、決済を完了したユーザの端末装置により解除し、商品を購入することができるようになる。特に、センサユニットは、既存の自動販売機に、後付けで実装することができ、その場合、当該自動販売機について、ユーザの端末装置によるロック解除、商品購入が可能となる。尚、デジタルの仮想自動販売機においては、セ

ンサユニットに相当する機能をプラグインにより後付けで実装することが可能である。以下、詳述する。

[0046] 図8には、本発明の第2実施形態に係る通信システムの構成を示し説明する。

[0047] 同図に示されるように、本実施形態に係る通信システムは、データベースサーバ装置等からなる第1サーバ装置200と、決済手段を実装した第2サーバ装置300と、第3サーバ装置400と、自動販売機800A乃至800C…（以下、総称するときは符号800を用いる）と、それら自動販売機800A乃至800C…に実装されたセンサユニット500A乃至500C…（以下、総称するときは符号500を用いる）と、ユーザの端末装置600と、ハッシュプールを実現する仮想サーバ装置群700とで構成されている。これら構成の一部の任意の組み合わせにより、通信システムを実現する場合もある。ユーザの端末装置600としては、スマートフォンやタブレット端末、ノート型パーソナルコンピュータ等、各種のものを採用することが可能である。

[0048] 以下、図9の概念図を参照して、無線通信システムによる処理手順を説明する。これは本実施形態に係る通信方法にも相当する。

[0049] ユーザの端末装置600は、自動販売機800に付された二次元コードを撮像し、自動販売機のIDを取得し、撮像時の位置情報を取得し、これら情報を第1サーバ装置200に送信することで、自動販売機800のロック解除に関わる暗号化データの取得を要求する。第1サーバ装置200は、取得した自動販売機のIDと位置情報とが、記録されている情報に合致するかを判定し、合致する場合には、当該自動販売機の取扱商品に関する商品情報を端末装置600に送信する。ユーザの端末装置600では、この商品情報が選択可能に表示され、所望とする商品が特定され、決済手続を進めることになる。

[0050] ユーザの端末装置600からの決済要求は、選択された決済手段を実現する第2サーバ装置300に送られ、当該第2サーバ装置300にて決済処理

が実行された後、決済トークンが第1サーバ装置200に送られる。第2サーバ装置200は、この決済トークンを受信すると、センサ情報をハッシュ関数によりハッシュ化したハッシュ値を生成し、ユーザの端末装置600に送信する。ユーザの端末装置600は、このハッシュ値を受信すると、ハッシュプールを実現する仮想サーバ装置群700に対して、受信したハッシュ値に基づく検索要求を行う。仮想サーバ装置群700は、この検索要求を受けると、ハッシュ値の存在を確認し、存在する場合には、公開鍵を第3サーバ装置400に送信する。第3サーバ装置400は、開錠コードを生成し、当該開錠コードを公開鍵により暗号化し、暗号化データを端末装置600に送信する。

[0051] こうして、端末装置600は、自動販売機800のセンサユニット500とBluetooth（登録商標）等の無線手段により、無線通信を行い、暗号化データをセンサユニット500に送信することで、自動販売機のロック解除をリクエストする。自動販売機側では、センサユニット500が、この暗号化データの成否を判断し、正しいと判断された場合には、自動販売機800のロックを解除する。こうして、ユーザは、自動販売機800より商品を取得する。

[0052] ここで、図10には、第1サーバ装置の構成を示し説明する。第1サーバ装置は、例えばデータベースサーバ装置等が、これにあたる。

[0053] 同図に示されるように、第1サーバ装置200は、制御部201と通信部202と記憶部203とを有する。制御部201と、通信部202と、記憶部203とは、バスを介して通信可能に接続されている。これら構成のほか、キーボードやマウス等の入力部や各種表示を行う液晶ディスプレイ等の表示部を有してもよい。

[0054] 通信部202は、例えば、ネットワークインタフェースカード（NIC ; Network Interface Card）等により実現されるもので、インターネット等の通信網900と有線又は無線で接続され、端末装置600等との間で通信を行う通信インタフェースである。

- [0055] そして、記憶部203は、例えば、RAM (Random Access Memory) やフラッシュメモリ (Flash Memory) 等の半導体メモリ素子、ハードディスクドライブ (HDD ; Hard Disc Drive) 、または光ディスク装置等で実現されるもので、制御部201で実行されるプログラムを予め記憶している。また、記憶部203は、販売機情報記憶部204、商品情報記憶部205、及びセンサ情報記憶部206を有する。
- [0056] より詳細には、販売機情報記憶部204は、販売機IDと、販売機の設置場所に係る位置情報と、取扱商品の商品ID等を紐づけて記憶している。商品情報記憶部205は、商品IDと、商品に関わる詳細情報 (型名、単価、数量等) を対応付けて記憶している。そして、センサ情報記憶部206は、センサユニット500のセンサIDと、位置情報 (ロケーション) 、実装されている自動販売機の販売機ID等を紐づけて記憶している。
- [0057] 制御部201は、CPU (Central Processing Unit) やMPU (Micro Processing Unit) 等で実現され、記憶部203に記憶されているプログラムを実行することで、送信部201a、受信部201b、商品情報特定部201c、及びハッシュ生成部201dとして機能する。尚、制御部201は、ASIC (Application Specific Integrated Circuit) やFPGA (Field Programmable Array) 等の集積回路で構成されてよい。
- [0058] 送信部201aは、例えば、商品情報記憶部205の商品情報や、ハッシュ生成部201dにより生成されたハッシュ値等を、通信部202を介してユーザの端末装置600に送信する。受信部201bは、ユーザの端末装置600から送られてきた販売機IDや位置情報、第2サーバ装置300から送られてきた決済トークン等を、通信部202を介して受信する。そして、商品情報特定部201cは、ユーザの端末装置600から送られてきた販売機IDに基づいて販売機情報記憶部204を参照して取扱商品の商品IDを特定し、当該商品IDに基づいて商品情報記憶部205を参照して商品情報を特定する。ハッシュ生成部201dは、センサ情報記憶部206に記憶されているセンサ情報をハッシュ関数によりハッシュ化し、ハッシュ値を生成

する。

[0059] 図11には、第2サーバ装置の構成を示し説明する。

[0060] 同図に示されるように、第2サーバ装置300は、制御部301と通信部302と記憶部303とを有する。制御部301と、通信部302と、記憶部303とは、バスを介して通信可能に接続されている。これら構成のほか、キーボードやマウス等の入力部や各種表示を行う液晶ディスプレイ等の表示部を有してもよい。

[0061] 通信部302は、例えば、NIC等により実現されるもので、インターネット等の通信網900と有線又は無線で接続され、端末装置600等との間で通信を行う通信インタフェースである。記憶部303は、例えば、RAMやフラッシュメモリ等の半導体メモリ素子、HDD、または光ディスク装置等で実現されるもので、制御部301で実行されるプログラムを予め記憶している。さらに、記憶部303は、決済情報を記憶している。制御部301は、CPUやMPU等で実現され、記憶部303に記憶されているプログラムを実行することで、送信部301a、受信部301b、及び決済処理部301cとして機能する。制御部301は、ASICやFPGA等の集積回路で構成されてよい。

[0062] 送信部301aは、例えば、決済トークンを、通信部302を介して第1サーバ装置200に送信する。受信部301bは、ユーザの端末装置600から送られてきた決済要求を、通信部302を介して受信する。決済処理部301cは、決済要求に基づいて決済処理を行う。決済処理の結果は、記憶部303に決済情報として記憶される。

[0063] 図12には、第3サーバ装置の構成を示し説明する。

[0064] 同図に示されるように、第3サーバ装置400は、制御部401と通信部402と記憶部403とを有する。制御部401と、通信部402と、記憶部403とは、バスを介して通信可能に接続されている。これら構成のほか、キーボードやマウス等の入力部や各種表示を行う液晶ディスプレイ等の表示部を有してもよい。

[0065] 通信部402は、例えば、NIC等により実現されるもので、インターネット等の通信網900と有線又は無線で接続され、端末装置600等との間で通信を行う通信インタフェースである。記憶部403は、例えば、RAMやフラッシュメモリ等の半導体メモリ素子、HDD、または光ディスク装置等で実現されるもので、制御部401で実行されるプログラムを予め記憶している。制御部401は、CPUやMPU等で実現され、記憶部403のプログラムを実行することで、送信部401a、受信部401b、コード生成部401c、及び暗号化処理部401dとして機能する。制御部401は、ASICやFPGA等の集積回路で構成されてよい。

[0066] 送信部401aは、例えば、暗号化処理部401dで生成される暗号化データを、通信部402を介してユーザの端末装置600に送信する。受信部401bは、仮想サーバ装置群700から送られてきた公開鍵を、通信部402を介して受信する。コード生成部401cは、開錠コードを生成する。そして、暗号化処理部401dは、公開鍵により開錠コードを暗号化し、暗号化データを生成する。

[0067] 図13には、端末装置の構成を示し説明する。

[0068] 同図に示されるように、端末装置600は、制御部601と、通信部602と、操作部603と、表示部604と、撮像部605と、記憶部606とを有する。各部601～606は、制御バスを介して通信自在に接続されている。通信部602は、例えば、NIC等により実現されるもので、インターネット等の通信網4と有線又は無線で接続され、第1サーバ装置200等との間で通信を行う通信インタフェースである。

[0069] 操作部603は、マウスやキーボード等で実現され、ユーザによる各種操作入力を受け付ける。表示部604は、液晶ディスプレイ等により実現され、各種表示を行う。尚、操作部603と表示部604とをタッチパネルとして一体に構成してもよい。撮像部605は、販売機800に付された二次元コード等を撮像する。記憶部606は、例えば、RAMやフラッシュメモリ等の半導体メモリ素子、HDD、または光ディスク装置等で実現されるもの

で、制御部601で実行されるプログラムを記憶している。

[0070] 制御部601は、CPUやMPU等で実現され、記憶部606に記憶されているプログラムを実行することで、送信部601a、受信部601b、コード解析部601c、位置情報取得部601d、及び要求部601eとして機能する。なお、制御部11は、ASICやFPGA等の集積回路で構成されてよい。

[0071] より詳細には、送信部601aは、撮像部605による販売機800に付された二次元コードの撮像、更にはコード解析部601cによる解析で得られた販売機IDと、位置情報取得部601dにより得られた位置情報を、通信部602を介して、第1サーバ装置200に送信する。受信部601bは、第3サーバ装置400から送られてきた暗号化データ等を、通信部602を介して受信する。コード解析部601cは、撮像部605により撮像された二次元コードを解析し、販売機IDを取得する。位置情報取得部601dは、GPS (Global Positioning System) やBLE (Bluetooth (登録商標) Low Energy) などの手段により、撮像時点での端末装置600 (または、販売機800) の位置情報を取得する。そして、要求部601eは、センサユニット500に対して、ロック解除に係る要求等を、操作部603の操作に基づいて行う。

[0072] 図14には、センサユニットの構成を示し説明する。このセンサユニットは、自動販売機800に実装されるモジュールである。

[0073] 同図に示されるように、自動販売機800に実装されるセンサユニット500は、全体の制御を司る制御部501と、通信部502と、記憶部503とを有する。通信部502は、例えば、インターネット等の通信網4と有線又は無線で接続され、或いは、Bluetooth (登録商標) 等の近距離無線通信により、ユーザの端末装置600や、第1サーバ装置200等との間で通信を行う通信インタフェースである。記憶部503は、例えば、RAMやフラッシュメモリ等の半導体メモリ素子で実現されるもので、制御部501で実行されるプログラムを記憶している。更に、記憶部503は、生成

されたコードや暗号化された暗号化データ、生成されたハッシュ等を記憶している。

[0074] 制御部501は、CPU等で実現され、記憶部503に記憶されているプログラムを実行することで、送信部501a、受信部501b、コード生成部501c、暗号化処理部501d、ハッシュ生成部501e、ロック解除部501f、及び管理部501g等として機能することになる。

[0075] 送信部501aは、生成された公開鍵を、通信部502を介して、ハッシュプールを実現する仮想サーバ装置群700に送信する。受信部501bは、ユーザの端末装置600から送信された暗号化データを、通信部502を介して受信する。コード生成部501cは、変動数開錠コードを生成する。ここで、変動数とは、所定のアルゴリズムにより生成されるコードが都度変更されることを意味する。

[0076] 暗号化処理部501dは、例えば公開鍵暗号方式（Public-key cryptography）に基づいて、公開鍵と秘密鍵を生成し、必要に応じて、後述するハッシュ値を公開鍵とを対応付ける。更に、必要に応じて、変動数開錠コードを公開鍵により暗号化する。ここで、一般に公開鍵暗号方式では、公開鍵を公開し、受信者は、公開鍵と対になる秘密鍵を保持し、必要に応じて受信内容を秘密鍵で復号するが、本実施形態では、センサユニット500が送信者でもあり受信者でもあることになる。なお、公開鍵暗号方式には、鍵生成アルゴリズム、暗号化アルゴリズム、及び復号アルゴリズムの3つのアルゴリズムがあり、これらに基づいて、鍵生成、暗号化、及び復号を行う。

[0077] より詳細には、鍵生成アルゴリズムでは、公開鍵秘密鍵ペアを生成し、出力する。暗号化アルゴリズムでは、公開鍵と平文（この例では、変動数開錠コード）と呼ばれるビット列の入力を受け、暗号文（暗号化データ）を生成し、出力する。そして、復号アルゴリズムでは、秘密鍵と暗号文（暗号化データ）の入力を受け、平文（この例では、変動数開錠コード）を生成し、出力する。

[0078] ハッシュ生成部501eは、センサ情報（センサID、位置情報等）をハ

ッシュ関数によりハッシュ化し、ハッシュ値を出力する。ロック解除部501gは、ユーザの端末装置600から送られてきた暗号化データの成否を判定し、暗号化データが保有している暗号化データ（又は変動数開錠コード）と合致する場合には、ロックを解除（アンロック）する。ここで、ロックの解除とは、例えば、自動販売機がガチャである場合には、商品搬出に係る駆動系のロックを解除し、商品を搬出することをいう。管理部501hは、暗号化処理部501dが生成した公開鍵とハッシュ生成部501eが生成したハッシュ値を対応付けて記憶部503に記憶し、管理する。

[0079] 以下、図15のフローチャートを参照して、無線通信システムによる処理手順を詳細に説明する。これは、本実施形態に係る通信方法にも相当する。

[0080] ユーザの端末装置600は、自動販売機800に付されている二次元コードを撮像部605で撮像し、コード解析部601cが画像を解析することで自動販売機の販売機IDを取得し（S1）、位置情報取得部601dがGPSやGLEなどの手段により撮像時の位置情報を取得し（S2）、送信部601aが、通信部602を介して、販売機IDと位置情報を第1サーバ装置に送信することで、自動販売機800のロック解除に関わる暗号化されたデータの取得を要求する（S3）。

[0081] 第1サーバ装置200は、通信部202を介して、受信部201bが、これら販売機IDと位置情報を受信し（S4）、商品情報特定部201cが、取得した販売機IDと位置情報とが、販売機情報記憶部204に記録されている情報に合致するかを判定し、合致する場合には、当該自動販売機の取扱商品に関する商品情報を商品情報記憶部205から読み出し（S5）、送信部201aが、通信部202を介して、商品情報をHTML型式等でユーザの端末装置600に送信する（S6）。

[0082] ユーザの端末装置600では、通信部602を介して、受信部601bが商品情報を受信すると（S7）、表示部604に商品情報が決済手段と共に選択可能に表示され、操作部603の操作により所望とする商品が特定されると、要求部601eが、通信部602を介して、第2サーバ装置300に

対して決済要求を行う（S 8）。

[0083] 第2サーバ装置300は、通信部302を介して、受信部301bが決済要求を受信すると（S 9）、決済処理部301cが電子決済に係る決済処理を行い（S 10）、送信部301aが、通信部302を介して、電子決済が完了したことを証明する決済トークンを第1サーバ装置200に送信する（S 11）。

[0084] 第1サーバ装置200は、通信部202を介して、受信部201bが決済トークンを受信すると（S 12）、ハッシュ生成部201dが、センサ情報記憶部206に記憶されているセンサ情報（センサIDやセンサロケーション等）をハッシュ関数によりハッシュ化したハッシュ値を生成し、送信部201aが、通信部202を介して、ユーザの端末装置600に送信する（S 13）。なお、ハッシュ生成部201dが、ハッシュ化に用いるハッシュ関数は、センサユニット501のハッシュ生成部501eで用いるハッシュ関数と同じであり、ハッシュ化の対象となるセンサ情報も同じであるので、センサユニット501側と同じハッシュ値を生成することが可能となっている。

[0085] ユーザの端末装置600は、通信部602を介して、受信部601bが、ハッシュ値を受信すると（S 14）、要求部601eが、通信部602を介して、ハッシュプールを実現する仮想サーバ装置群700に対して、受信したハッシュ値に基づく検索要求を行う（S S 15）。仮想サーバ装置群700は、この検索要求を受けると、ハッシュ値の存在を確認し、存在する場合には、公開鍵を第3サーバ装置400に送信する（S 16）。

[0086] 第3サーバ装置400は、通信部402を介して、受信部401bが公開鍵を受信すると（S 17）、コード生成部401cが変動数開錠コードを生成し、暗号化処理部401dが暗号化ロジックに基づいて開錠コードを公開鍵により暗号化し、送信部401aが、通信部402を介して、暗号化データを端末装置600に送信する（S 18）。なお、第3サーバ装置400で暗号化処理に用いる暗号化ロジックは、センサユニット500で用いる暗号

化ロジックと同じである。また、コード生成部401cで用いられるコード生成ロジックも、センサユニット500で用いるものと同じである。

[0087] ユーザの端末装置600は、受信部601bが、通信部602を介して、暗号化データを受信すると(S19)、要求部601eが、通信部602を介して、自動販売機800に実装されるセンサユニット500と、Bluetooth(登録商標)等の近距離無線通信により、暗号化データを送信することで、センサアンロック要求を行う(S20)。

[0088] 自動販売機側800では、センサユニット500の送信部501aが、通信部502を介して、暗号化データを受信し(S21)、ロック解除部501fが、暗号化データの成否を判断し、暗号化データが正しいと判断された場合には、自動販売機800のロックを解除する(S22)。こうして、ユーザは、自動販売機800より商品を取得する。

[0089] なお、暗号化データの成否については、センサユニット500で、コード生成部501cにより変動数開錠コードを生成し、暗号化処理部501dで暗号化ロジックにより暗号化した暗号化データと、受信した暗号化データとを比較することで判断してもよい。あるいは、受信した暗号化データを、暗号化処理部501dの復号ロジックにより復号し、変動数開錠コードを得て、それをコード生成部501cにより生成した変動数開錠コードと比較することで判断するようにしてもよい。

[0090] 以上説明したように第2実施形態によれば、ユーザの端末装置には、センサ情報に基づき生成されたハッシュ値と暗号化データのみが与えられるにすぎないので、変動数開錠コードがWeb上に流出することを防止でき、よりセキュアな取引が実現される。

[0091] また、データベースサーバ等からなる第1サーバ装置、暗号化データを生成する第3サーバ装置では、ハッシュ生成、暗号化データ生成にあたり、センサユニットと同じロジックを用いているので、変動数開錠コードやハッシュの送受を行う必要がなく、その点でもよりセキュアな取引が実現される。

[0092] また、暗号化データは、ハッシュプールから公開鍵を受け取った第3サー

バ装置が、変動数開錠コードを当該公開鍵で暗号化することで生成されるので、暗号化データの漏えいを防止することができる。すなわち、暗号化データの漏えい事故の抑止に対する優位性を確保することが可能となる。

[0093] さらに、ハッシュ値は第1サーバ装置で生成されユーザの端末装置に送られ、暗号化データは第3サーバ装置で生成されユーザの端末装置に送られるなど、情報分散化により攻撃対象を拡大しているので、攻撃の抑止にもつながる。

[0094] そして、公開鍵を管理しているのが、ハッシュプールであることから、攻撃を受けた場合には、即座にエリアを移して再建することが可能であるので、公開鍵をより安全に管理することが可能となる。

[0095] さらに、第3サーバ装置で生成される暗号化データは、短時間で更新されるので、攻撃を受けた場合でも、その解読の可能性は確率的にはゼロに等しい。

[0096] また、ハッシュ管理を基礎としているので、確率上、システムが増大すればするほど安全性はより高まっていくといえる。

[0097] 仮に、自動販売機に実装されたセンサユニットが物理的攻撃を受けた場合でも、その被害は当該自動販売機だけにおよび、他には影響を与えないので、即座に対処することが可能となる。

[0098] 以上、本発明の第2実施形態について説明したが、本実施形態は、これに限定されず種々の改良、変更が可能である。例えば、各自動販売機に実装されたセンサユニットが所定単位でセンサネットワークを形成し、ハッシュプールへの公開鍵のアップロード等を、電源残量に余裕のあるセンサユニットが統括して行うようにして、省電力化を実現するようにしてもよいことは勿論である。

符号の説明

[0099] 1…無線通信システム、10…無線通信端末、20…無線通信網、30…自動販売機、40…サーバ装置。100…制御部、110…UI部、110a…表示部、110b…操作部、110c…撮像部、120…第1無線通信

部、130…第2無線通信部、140…記憶部、142…揮発性記憶部、144…不揮発性記憶部、144a…購入支援プログラム、150…バス、200…第1サーバ装置、300…第2サーバ装置、400…第3サーバ装置、500…センサユニット、600…端末装置、700…仮想サーバ装置群、800…自動販売機。

請求の範囲

- [請求項1] 端末装置が、自動販売機に付された二次元コードを撮像して販売機IDを取得し、位置情報を取得し、前記販売機IDと前記位置情報を第1サーバ装置に送信することで、前記自動販売機のロック解除に関わる暗号化データの取得を要求する第1のステップと、
- 第1サーバ装置が、前記販売機IDと位置情報とが、記憶している情報に合致するかを判定し、合致する場合には、商品情報を前記端末装置に送信する第2のステップと、
- 第2のサーバ装置が、前記端末装置からの決済要求を受け、決済処理を実行し、決済トークンを前記第1サーバ装置に送信する第3のステップと、
- 第1サーバ装置が、前記決済トークンを受信し、センサ情報をハッシュ関数によりハッシュ化したハッシュ値を生成し、前記端末装置に送信する第4のステップと、
- 前記端末装置が、前記ハッシュ値により、ハッシュプールを実現する仮想サーバ装置群に対して検索要求を行う第5のステップと、
- 前記仮想サーバ装置群が、前記検索要求を受け、ハッシュ値の存在を確認し、存在する場合には、公開鍵を第3サーバ装置に送信する第6のステップと、
- 前記第3サーバ装置が、開錠コードを生成し、前記開錠コードを前記公開鍵により暗号化し、暗号化データを前記端末装置に送信する第7のステップと、
- 前記端末装置が、前記暗号化データを前記自動販売機のセンサユニットに送信することで、前記自動販売機のロック解除を要求する第8のステップと、
- 前記センサユニットが、前記暗号化データの成否を判断し、正しいと判断された場合には、前記自動販売機のロックを解除する第9のステップと、を有する

通信方法。

[請求項2] 前記第9のステップにおいて、前記センサユニットでは、開錠コードを生成し、前記開錠コードを暗号化し、暗号化データを、前記端末装置から送られてきた暗号化データと比較することで、暗号化データの成否を判断する

請求項1に記載の通信方法。

[請求項3] 前記開錠コードとは、変動数開錠コードである

請求項1又は請求項2に記載の通信方法。

[請求項4] 自動販売機に付された二次元コードを撮像して販売機IDを取得し、撮像時の位置情報を取得し、前記販売機IDと前記位置情報を第1サーバ装置に送信すると共に、第1サーバ装置より送られてきたハッシュ値によりハッシュプールを実現する仮想サーバ装置群に対して検索要求を行い、更には、第3サーバ装置から送られてきた暗号化データを前記自動販売機のセンサユニットに送信することで、前記自動販売機のロック解除を要求する端末装置と、

前記販売機IDと位置情報とが、記憶している情報に合致するかを判定し、合致する場合には、商品情報を前記端末装置に送信すると共に、決済トークンを受信すると、記憶しているセンサ情報をハッシュ関数によりハッシュ化した前記ハッシュ値を生成し、前記端末装置に送信する第1サーバ装置と、

前記端末装置から前記ハッシュ値による検索要求を受けると、前記ハッシュ値の存在を確認し、存在する場合には公開鍵を第3サーバ装置に送信する仮想サーバ装置群と、

開錠コードを生成し、前記開錠コードを前記公開鍵により暗号化し、暗号化データを前記端末装置に送信する第3サーバ装置と、

前記公開鍵を生成して前記仮想サーバ装置群に送信すると共に、前記端末装置から前記暗号化データを受信すると前記暗号化データの成否を判断し、正しいと判断された場合には、前記自動販売機のロック

を解除するセンサユニットと、を有する
通信システム。

[請求項5] 前記センサユニットでは、開錠コードを生成し、前記開錠コードを暗号化し、暗号化データを、前記端末装置から送られてきた暗号化データと比較することで、暗号化データの成否を判断する
請求項4に記載の通信システム。

[請求項6] 前記開錠コードとは、変動数開錠コードである
請求項4又は請求項5に記載の通信システム。

[請求項7] 自動販売機に実装され、端末装置から送られてきた暗号化データに基づいて前記自動販売機のロックを解除するセンサユニットであって、

公開鍵と秘密鍵を生成し、開錠コードを公開鍵により暗号化する暗号化処理部と、

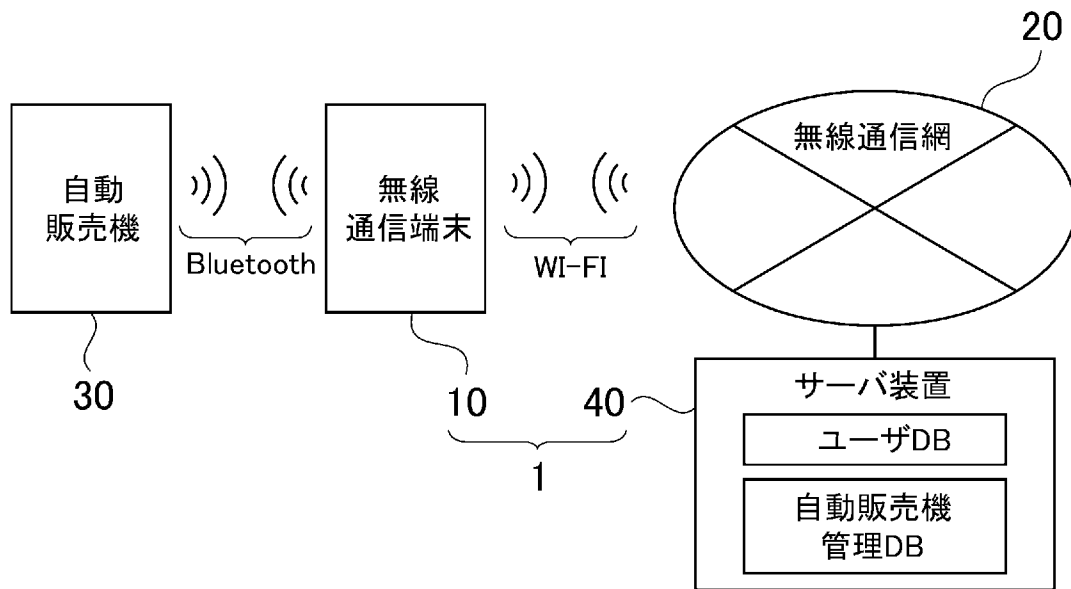
少なくともセンサIDとセンサの位置情報を含むセンサ情報を、ハッシュ関数によりハッシュ化し、ハッシュ値を出力するハッシュ生成部と、

少なくとも前記暗号化処理部が生成した前記公開鍵と前記ハッシュ生成部が生成した前記ハッシュ値を対応付けて記憶部に記憶し管理する管理部と、

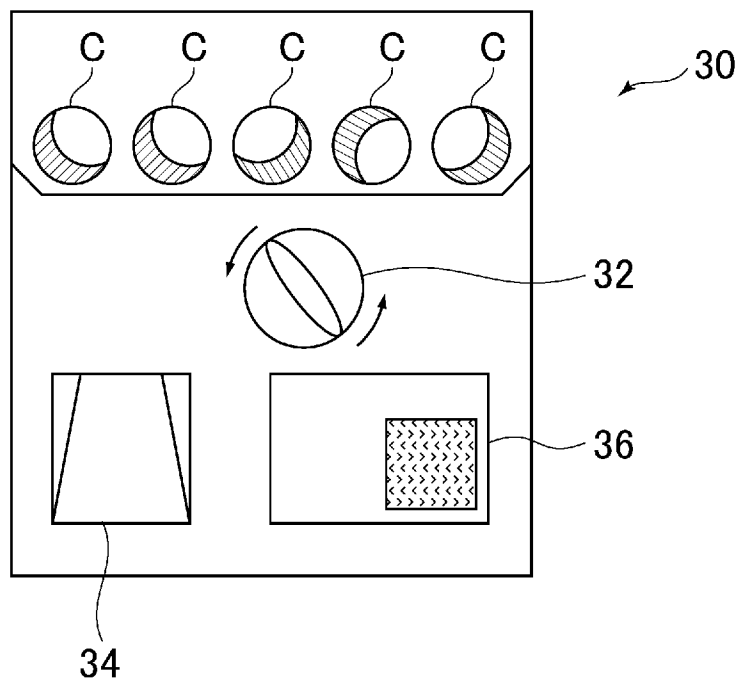
前記端末装置から送られてきた暗号化データの成否を判定し、前記暗号化データが、前記暗号化処理部が生成する暗号化データと合致する場合には、前記自動販売機のロックを解除するロック解除部と、を備えた

センサユニット。

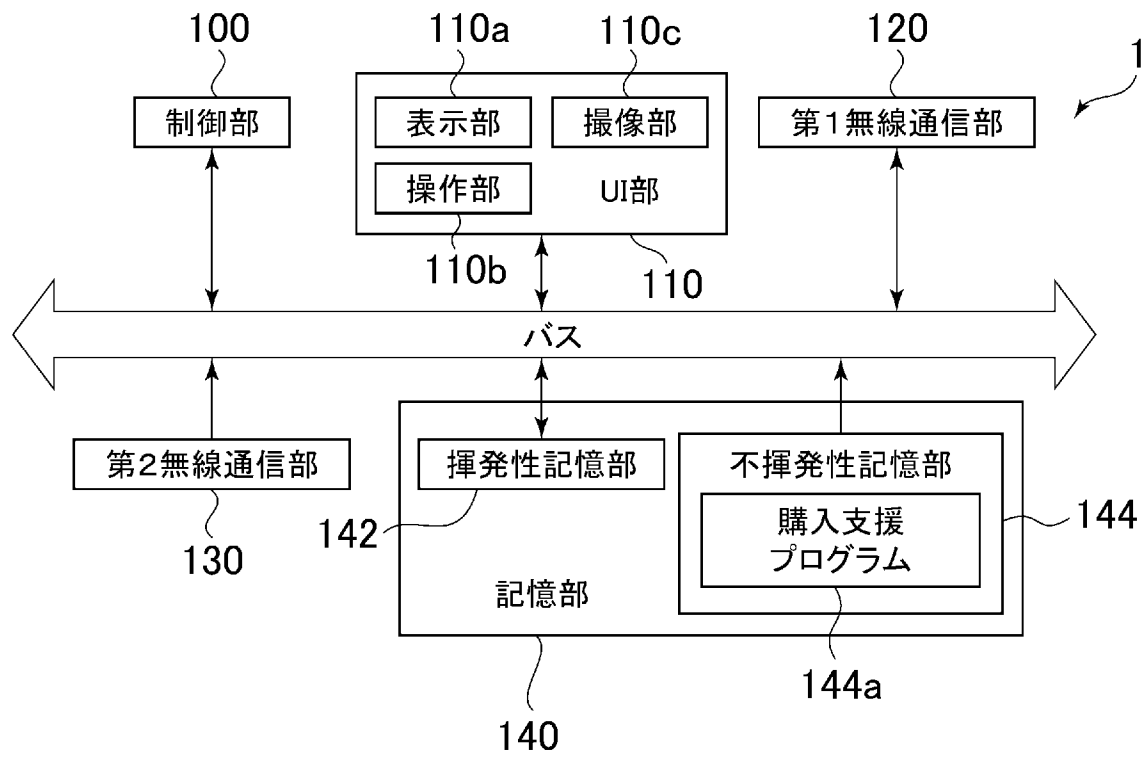
[図1]



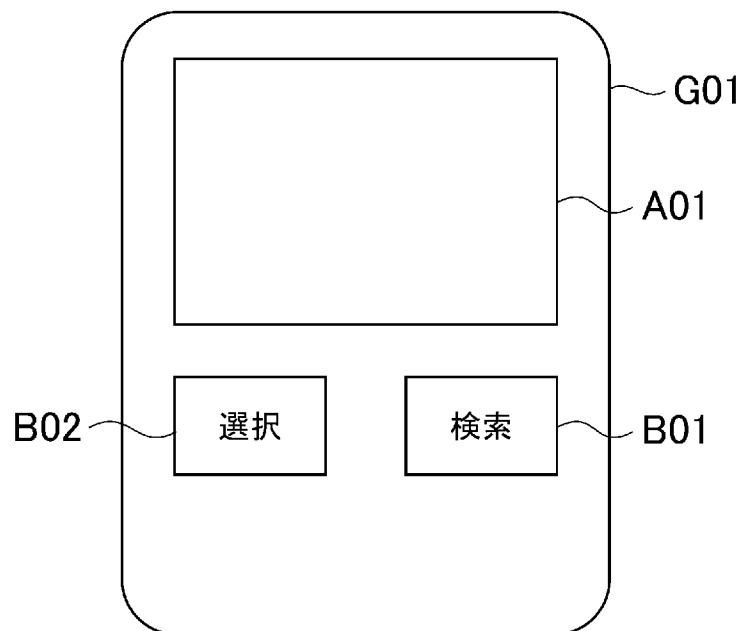
[図2]



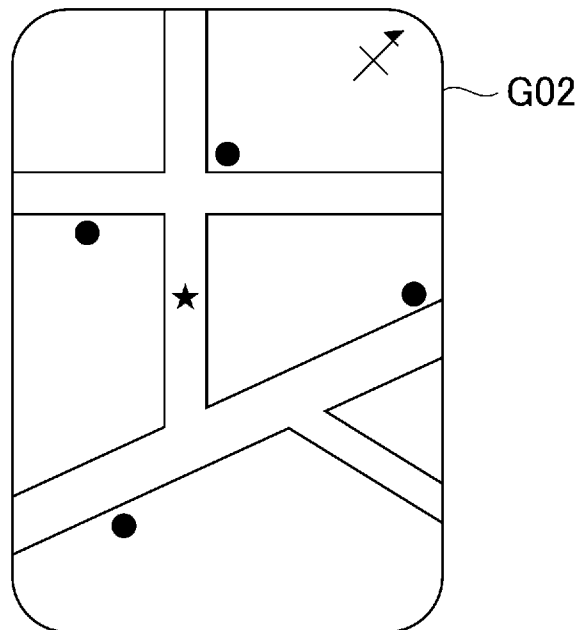
[図3]



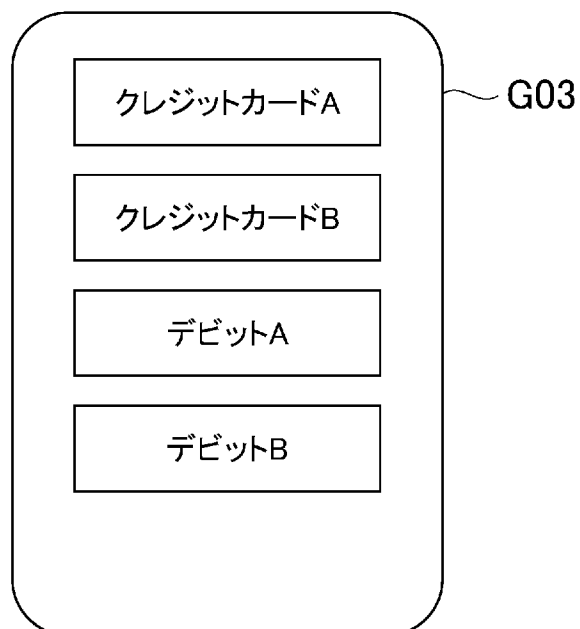
[図4]



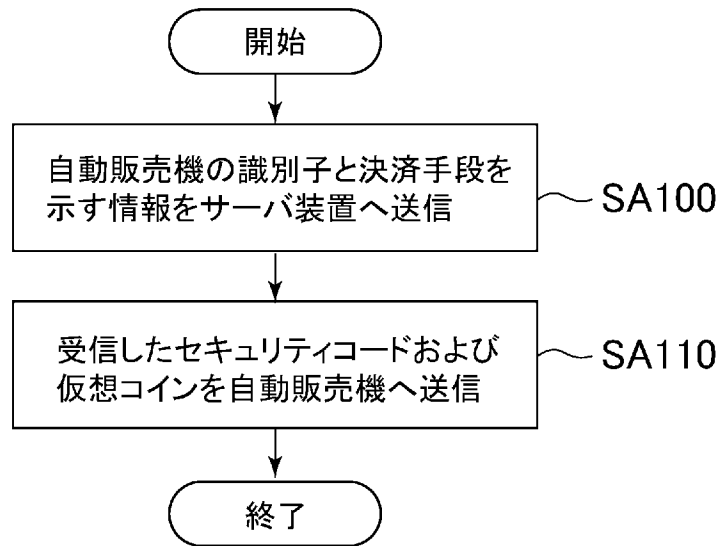
[図5]



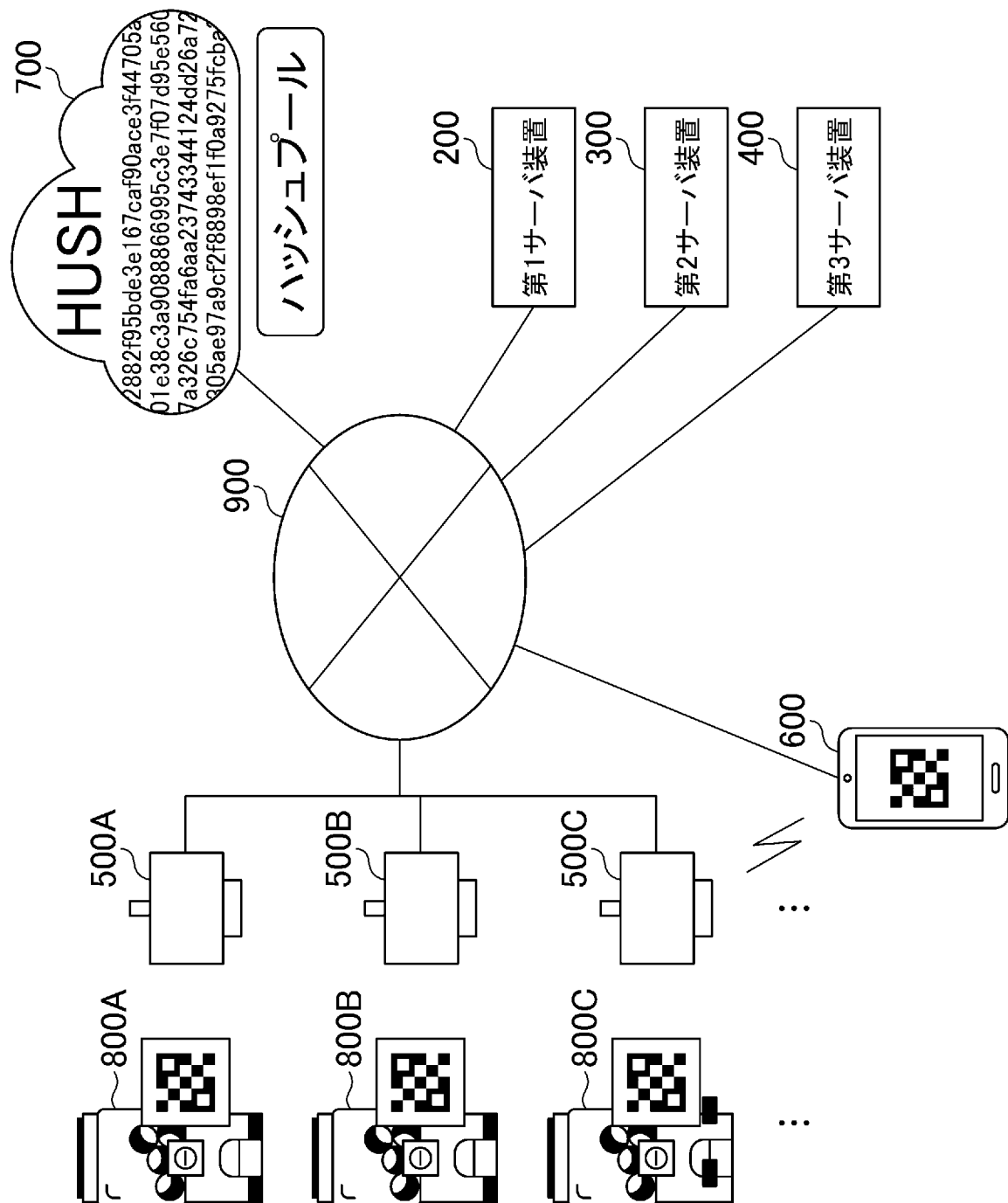
[図6]



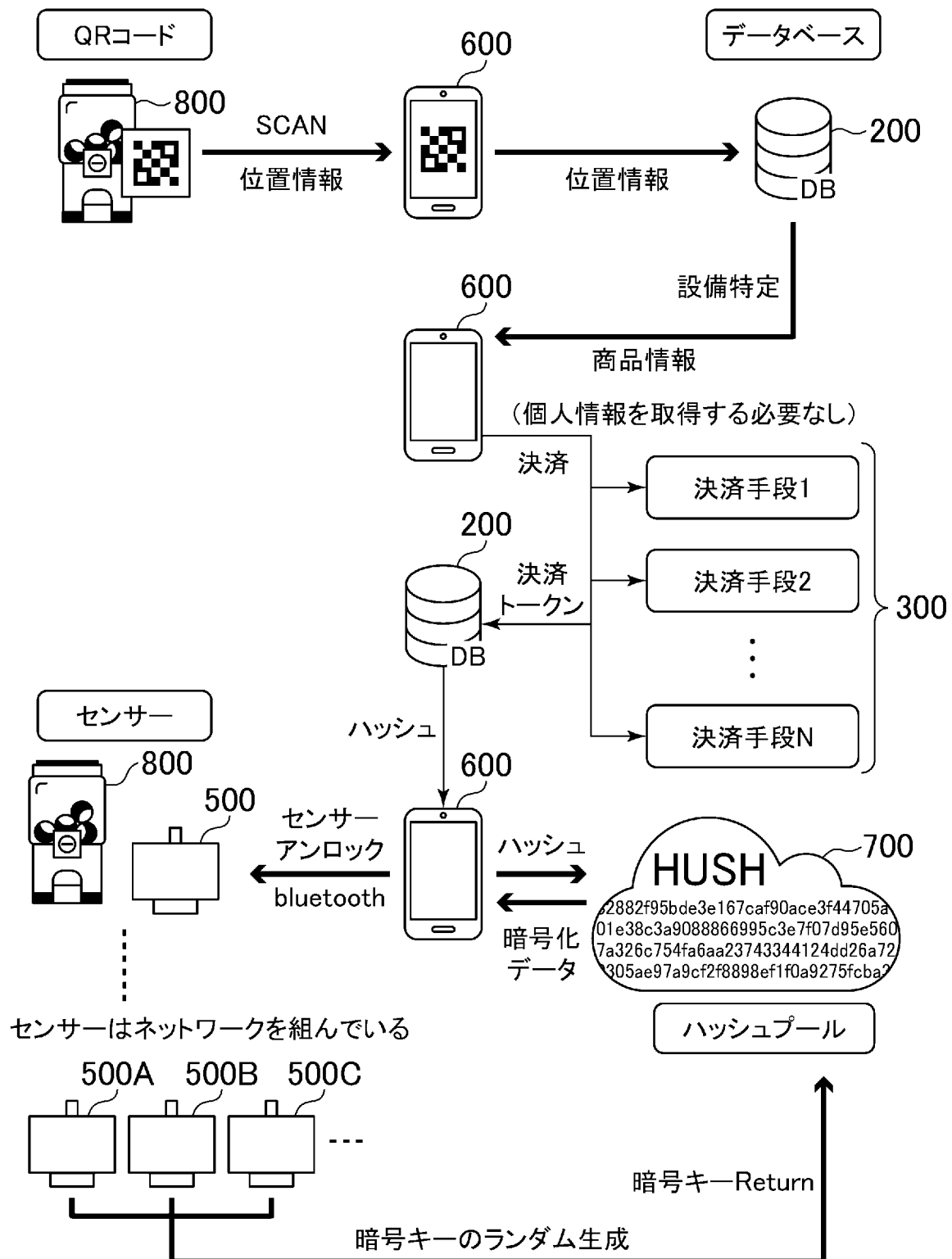
[図7]



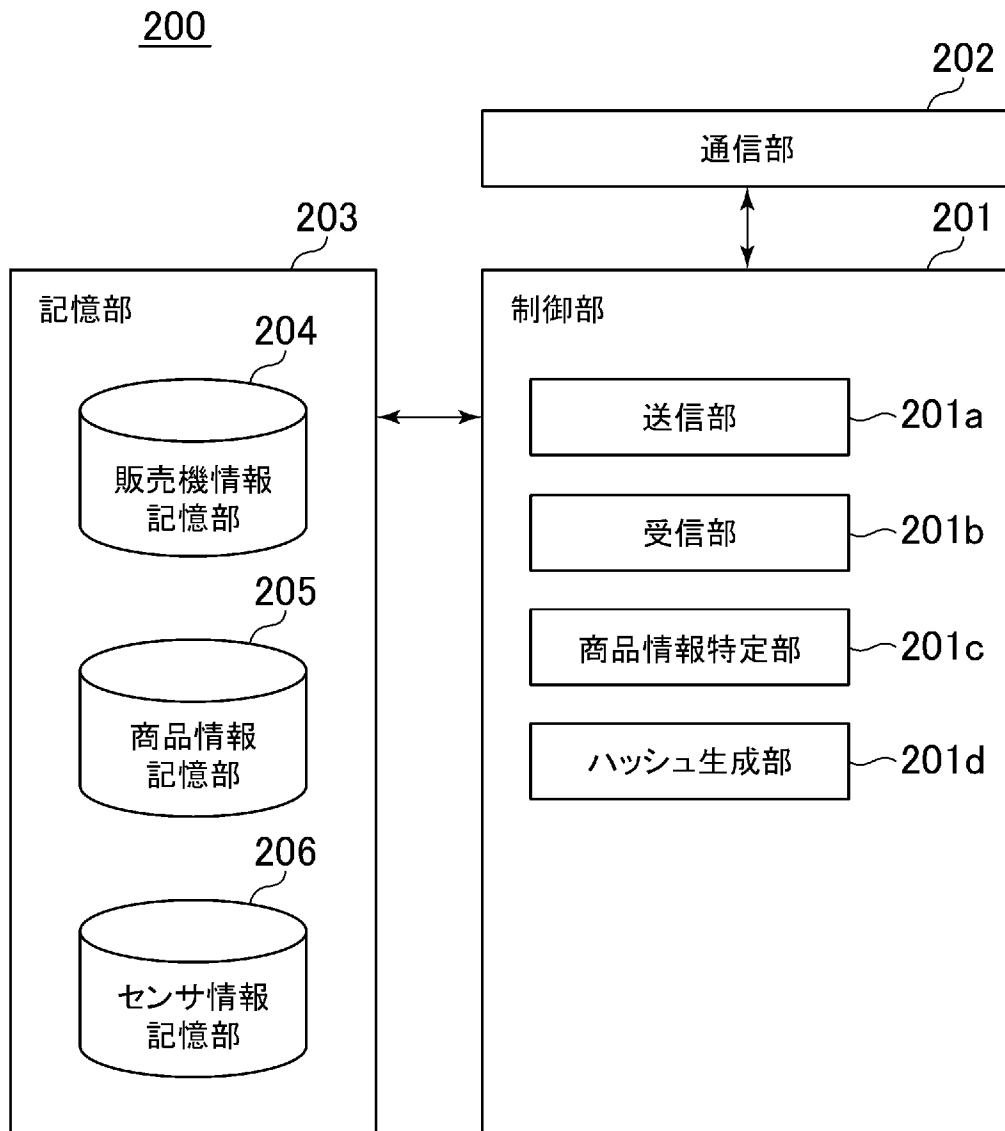
[図8]



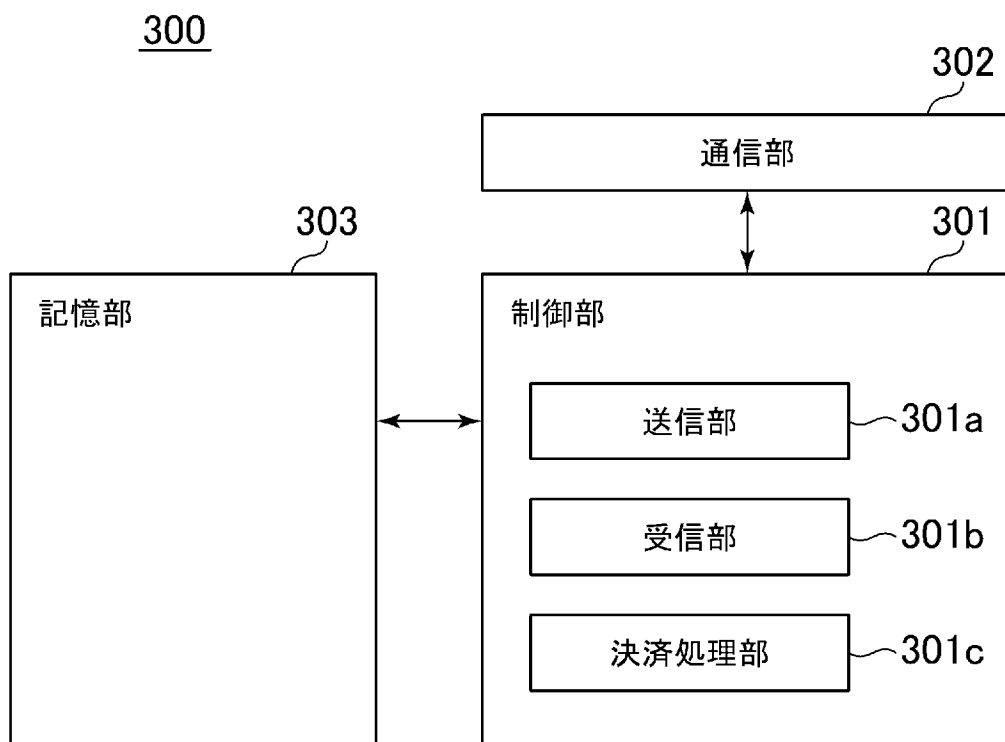
[図9]



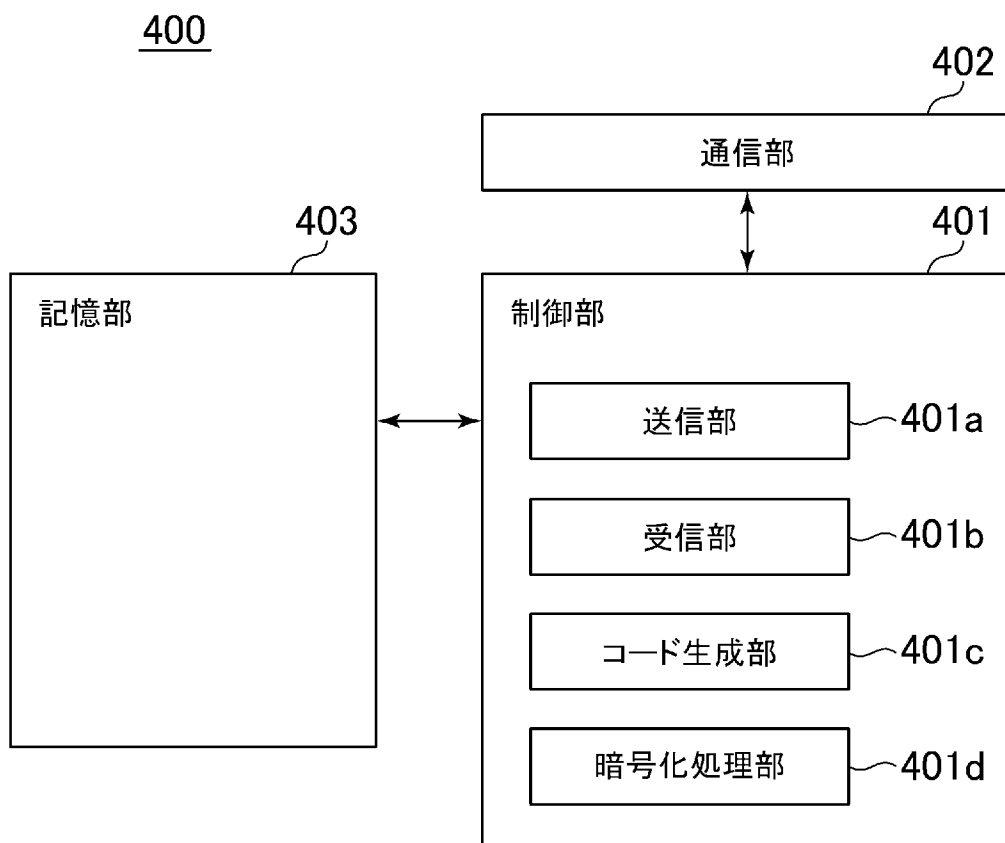
[図10]



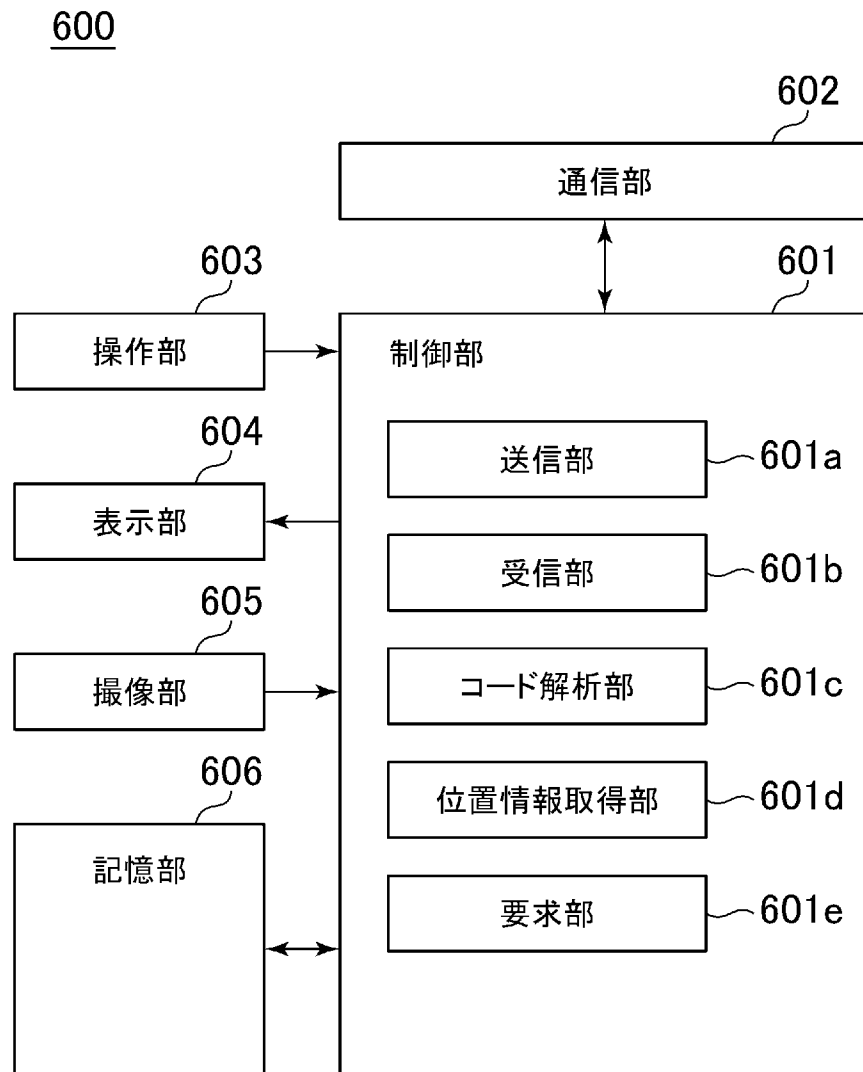
[図11]



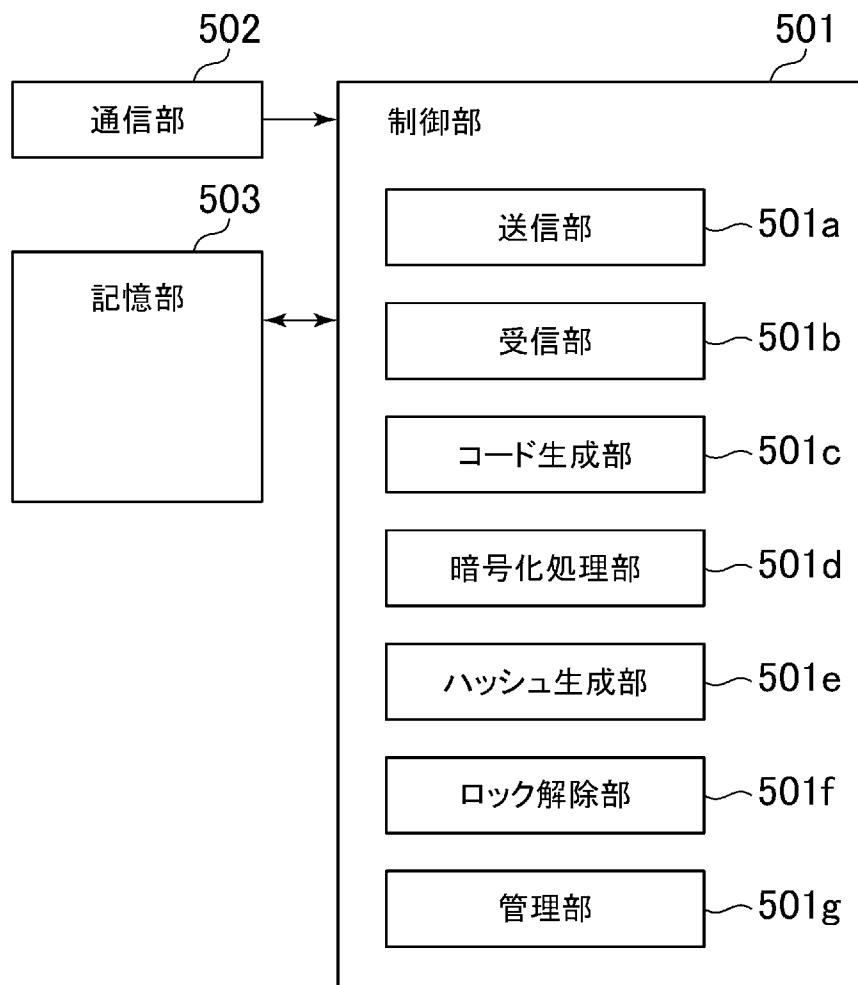
[図12]



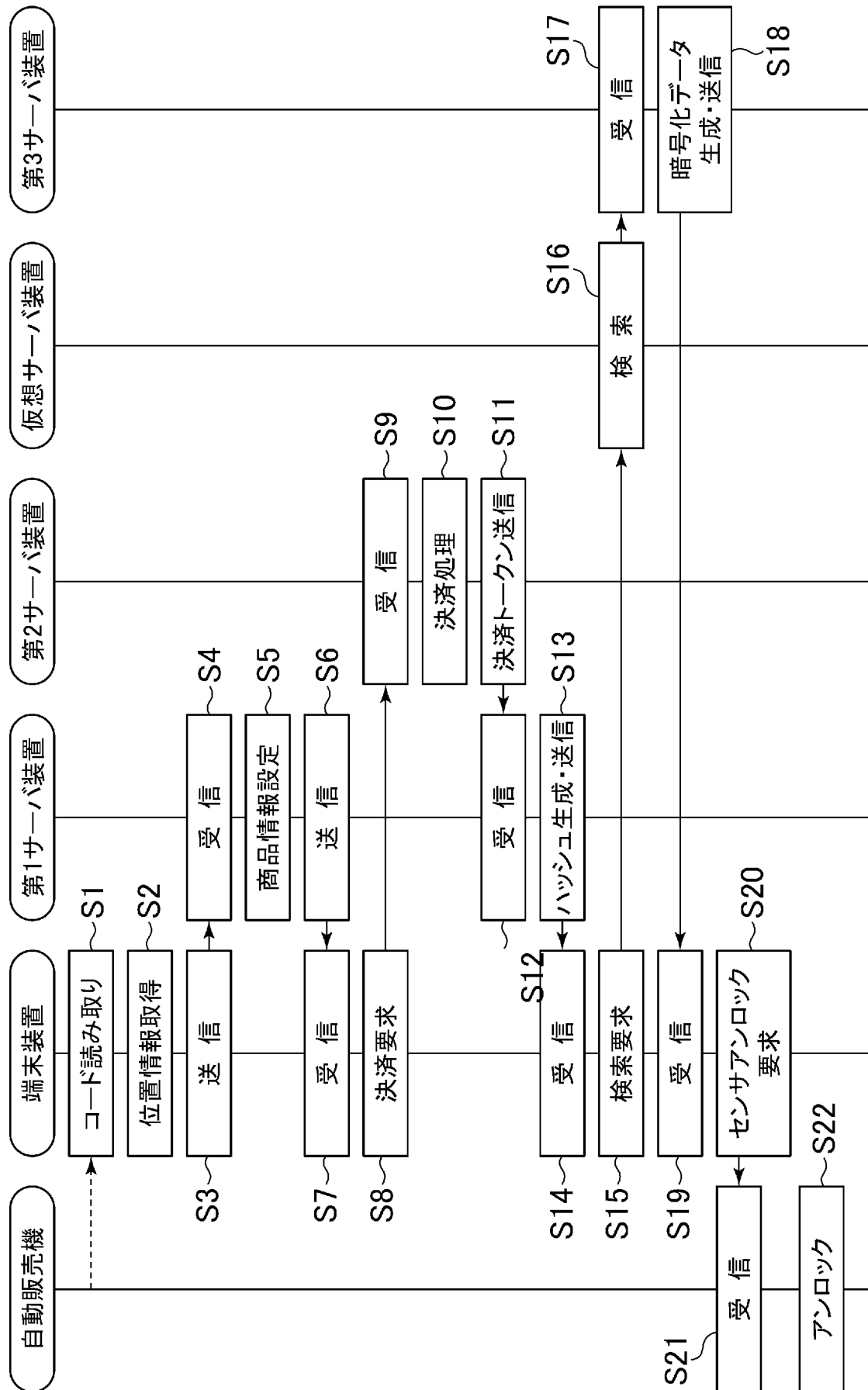
[図13]



[図14]

500

[図15]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/012426

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl. G06Q20/18 (2012.01) i, G06F21/44 (2013.01) i, H04L9/08 (2006.01) i, H04L9/32 (2006.01) i

FI: G06Q20/18, H04L9/00601F, H04L9/00601B, H04L9/00673B, G06F21/44

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. G06Q20/18, G06F21/44, H04L9/08, H04L9/32

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 1971-2020

Registered utility model specifications of Japan 1996-2020

Published registered utility model applications of Japan 1994-2020

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.
A	JP 2002-117442 A (TIETECH CO., LTD.) 19.04.2002 (2002-04-19), entire text, all drawings	1-7
A	JP 2004-348238 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 09.12.2004 (2004-12-09), entire text, all drawings	1-7
A	JP 2002-140756 A (IDS KK) 17.05.2002 (2002-05-17), entire text, all drawings	1-7
A	JP 2002-150370 A (SANYO ELECTRIC CO., LTD.) 24.05.2002 (2002-05-24), entire text, all drawings	1-7
A	JP 2002-298203 A (MITSUBISHI ELECTRIC CORPORATION) 11.10.2002 (2002-10-11), entire text, all drawings	1-7



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
12.06.2020

Date of mailing of the international search report
23.06.2020

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/012426

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2013-235442 A (JAPAN MACHINE SERVICE CO., LTD.) 21.11.2013 (2013-11-21), entire text, all drawings	1-7
A	WO18/042669 A1 (RAKUTEN, INC.) 08.03.2018 (2018-03-08) entire text, all drawings	1-7
A	US 2017/0266544 A1 (HUANG, M. J.) 21.09.2017 (2017-09-21), entire text, all drawings	1-7
A	US 2012/0187187 A1 (DUFF, Z. W.) 26.07.2012 (2012-07-26), entire text, all drawings	1-7

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2020/012426

JP 2002-117442 A	19.04.2002	(Family: none)
JP 2004-348238 A	09.12.2004	(Family: none)
JP 2002-140756 A	17.05.2002	(Family: none)
JP 2002-150370 A	24.05.2002	(Family: none)
JP 2002-298203 A	11.10.2002	(Family: none)
JP 2013-235442 A	21.11.2013	JP 5035715 B1
WO 18/042669 A1	08.03.2018	US 2019/0325411 A1 CN 109906464 A
US 2017/0266544 A1	21.09.2017	US 10252149 B2
US 2012/0187187 A1	26.07.2012	WO 2012/097398 A1 EP 2666119 A1 CN 103534710 A

A. 発明の属する分野の分類（国際特許分類（IPC）） G06Q 20/18(2012.01)i; G06F 21/44(2013.01)i; H04L 9/08(2006.01)i; H04L 9/32(2006.01)i FI: G06Q20/18; H04L9/00 601F; H04L9/00 601B; H04L9/00 673B; G06F21/44		
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）） G06Q20/18; G06F21/44; H04L9/08; H04L9/32		
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 1971-2020年 日本国実用新案登録公報 1996-2020年 日本国登録実用新案公報 1994-2020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
A	JP 2002-117442 A（株式会社タイテック）19.04.2002（2002-04-19） 全文, 全図	1-7
A	JP 2004-348238 A（日本電信電話株式会社）09.12.2004（2004-12-09） 全文, 全図	1-7
A	JP 2002-140756 A（株式会社アイディーエス）17.05.2002（2002-05-17） 全文, 全図	1-7
A	JP 2002-150370 A（三洋電機株式会社）24.05.2002（2002-05-24） 全文, 全図	1-7
A	JP 2002-298203 A（三菱電機株式会社）11.10.2002（2002-10-11） 全文, 全図	1-7
A	JP 2013-235442 A（株式会社日本マシンサービス）21.11.2013（2013-11-21） 全文, 全図	1-7
A	WO 18/042669 A1（楽天株式会社）08.03.2018（2018-03-08） 全文, 全図	1-7
☒ 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 12.06.2020		国際調査報告の発送日 23.06.2020
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） 松野 広一 5R 3658 電話番号 03-3581-1101 内線 3502

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
A	US 2017/0266544 A1 (HUANG, Ming-Jian) 21.09.2017 (2017 - 09 - 21) 全文, 全図	1-7
A	US 2012/0187187 A1 (DUFF, Zachary W.) 26.07.2012 (2012 - 07 - 26) 全文, 全図	1-7

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/JP2020/012426

引用文献			公表日	パテントファミリー文献			公表日
JP	2002-117442	A	19.04.2002	(ファミリーなし)			
JP	2004-348238	A	09.12.2004	(ファミリーなし)			
JP	2002-140756	A	17.05.2002	(ファミリーなし)			
JP	2002-150370	A	24.05.2002	(ファミリーなし)			
JP	2002-298203	A	11.10.2002	(ファミリーなし)			
JP	2013-235442	A	21.11.2013	JP	5035715	B1	
WO	18/042669	A1	08.03.2018	US	2019/0325411	A1	
				CN	109906464	A	
US	2017/0266544	A1	21.09.2017	US	10252149	B2	
US	2012/0187187	A1	26.07.2012	WO	2012/097398	A1	
				EP	2666119	A1	
				CN	103534710	A	