(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-185253
(P2004-185253A)
(43)公開日　平成16年7月2日(2004.7.2)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 17/60	G06F 17/60	410E	3E044
G07F 7/02	G06F 17/60	310C	5K025
G07F 7/10	G06F 17/60	332	5K067
H04M 15/00	G06F 17/60	414	
H04Q 7/38	G06F 17/60	432Z	

審査請求 未請求　請求項の数 14　ＯＬ　（全 29 頁）　最終頁に続く

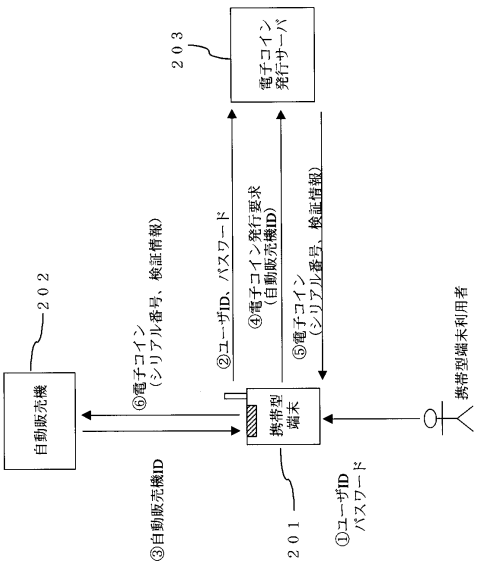
(21)出願番号　特願2002-350611(P2002-350611)
(22)出願日　平成14年12月3日(2002.12.3)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100111497
弁理士　波田　啓子
(74)代理人　100111800
弁理士　竹内　三明
(74)代理人　100114878
弁理士　山地　博人
(72)発明者　松田　規
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】電子コインシステム

(57)【要約】
【課題】ネットワークに接続されない自動販売機に対しても携帯機器からサービス要求を受け入れる安全なコインシステムを得る。
【解決手段】通常の通信路に接続可能な電子コイン発行サーバ２０３を設けて、無線路を介して携帯機器からの発行要求を受け、この要求の正当性を認証するユーザ認証部と、認証後に検証情報付で要求額の電子コインの発行を行う発行部と、発行に伴う課金を管理する課金部と備えた電子コイン発行サーバとし、無線路を介した携帯機器からのサービス要求に対し、電子コインサーバが保証する電子コインの投入を受けて、検証を行なう電子コイン検証部を備えて、検証後にサービスを行なう自動販売機２０２、とでシステムを構成する。
【選択図】　図４



【特許請求の範囲】
【請求項１】
無線路を介して携帯機器からの発行要求を受け、該要求の正当性を認証するユーザ認証部と、認証後に検証情報付で要求額の電子コインの発行を行う発行部と、上記発行に伴う課金を行う課金部、とを備えた電子コイン発行サーバと、
無線路を介した携帯機器からのサービス要求に対し、上記電子コインサーバが保証する電子コインの投入を受けて、検証を行なう電子コイン検証部を備えて、検証後にサービスを行なう自動販売機、とで構成されることを特徴とする電子コインシステム。
【請求項２】
電子コイン発行サーバは、携帯機器からの発行要求に対し、該要求額に相当するワンタイム電子コインまたはシリアル番号を付した電子コインを発行し、
自動販売機は、履歴管理部を備えて、上記ワンタイム電子コインの情報または電子コインの情報とシリアル番号によって使用を管理するようにしたことを特徴とする請求項１記載の電子コインシステム。
【請求項３】
自動販売機は、自身の識別記号を送信し、電子コイン発行サーバは、上記自動販売機の識別記号を電子コインの発行に加えて送信し、
自動販売機の検証部は、上記入力された自身の識別記号に基づく情報に基づいて検証するようにしたことを特徴とする請求項１記載の電子コインシステム。
【請求項４】
電子コイン発行サーバは、自動販売機の識別記号を基に改竄検出情報を含めた電子コインを作成し、
自動販売機は、そのコイン検証部を、上記改竄検出情報を解読する検証部としたことを特徴とする請求項３記載の電子コインシステム。
【請求項５】
自動販売機は、電子コインの使用履歴を管理する履歴管理部を備えて、また商品の価格を送信し、
上記履歴管理部は、携帯機器からの上記商品に対するサービス要求に対し、電子コインの積算管理をするようにしたことを特徴とする請求項２記載の電子コインシステム。
【請求項６】
電子コイン発行サーバは、期限情報を含めた電子コインを発行し、
自動販売機は、時計または期限管理機能と、電子コインの使用履歴を管理する履歴管理部を備えて、電子コインを用いたサービス要求に対して該電子コインが持つ上記期限情報に基づいて検証し管理するようにしたことを特徴とする請求項１記載の電子コインシステム。
【請求項７】
携帯機器に電子コイン保存部を備えて、電子コインサーバが保証する電子コインの金額またはシリアル番号を管理し、自動販売機での使用毎に使用額を積算管理するようにしたことを特徴とする請求項１記載の電子コインシステム。
【請求項８】
通信路を介して自動販売機と接続する電子コイン検証装置を備えて、
自動販売機は、電子コインによるサービス要求を受けると上記電子コイン検証装置に自身の自動販売機の識別記号と電子コインの情報を送信し、返送された検証結果に基づいてサービスを行なうようにしたことを特徴とする請求項１記載の電子コインシステム。
【請求項９】
電子コインに期限情報と金額情報を載せて、電子コイン検証装置は、上記電子コインの期限情報、使用管理情報に基づいて検証するようにしたことを特徴とする請求項８記載の電子コインシステム。
【請求項１０】
携帯機器に電子コイン保存部を備えて、電子コイン使用時には必要金額を投入するように

し、
自動販売機は、上記投入された電子コインの情報に基づいて電子コイン検証装置に送信するようにしたことを特徴とする請求項８記載の電子コインシステム。
【請求項１１】
電子コイン発行サーバは、期限情報を含めて発行し、また自動販売機の識別記号を基に改竄検出情報を含めた電子コインを作成し、
自動販売機は、時計または期限管理機能を備えて電子コインの使用履歴を検証し、上記改竄検出情報を解読する検証部としたことを特徴とする請求項５記載の電子コインシステム。
【請求項１２】
内部に携帯機器からの電子コインによるサービス要求を受けるデータ受信部と、
上記電子コインが保証されているかを自身の識別情報を含めて検証する電子コイン検証部と、
上記電子コインの履歴を管理する履歴管理部とを備えて、上記電子コインの検証後にサービスを行なうことを特徴とする電子コインシステム用自動販売機。
【請求項１３】
内部にユーザからの第１の識別情報に基づいてユーザを認証するユーザ認証部と、
上記認証結果と管理情報と電子コイン発行要求に基づいて第２の識別情報付で網と無線路を通じて要求先の携帯機器に電子コインを発行する電子コイン発行部とを備えて、上記電子コインの発行に基づいて課金することを特徴とする電子コイン発行サーバ。
【請求項１４】
内部に無線路と網を通じて電子コイン発行サーバに対して第１の識別情報付で必要な電子コインの発行を要求する電子コイン発行要求部と、
上記電子コイン発行サーバから無線路と網を通じて第２の識別情報付の電子コインを受け取り、自動販売機にサービス要求するデータ受信部と電子コイン送信部と、を備えたことを特徴とする電子コイン使用携帯機器。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、自動販売機やＰＯＳ端末を利用した商品販売に関して、金銭のやりとりを行うことなく、携帯電話等の携帯型端末を利用する事によって支払いを実現する電子コインシステムに関するものである。
【０００２】
【従来の技術】
図３９は、第１の従来例である特許文献１に示された従来の電子コインシステムを示す図である。本システムは、商品販売を行う自動販売機１１３０、自動販売機での購入動作を管理し、携帯型端末利用者（購入者）への課金を行う自動販売機管理装置１１４０、携帯型端末利用者が保有する携帯型端末１１５０から構成される。ここで、複数の自動販売機１１３０と、自動販売機管理装置１１４０は、自動販売機ネットワーク１１１０を介して接続されており、互いに通信が可能である。また、携帯型端末１１５０と自動販売機管理装置１１４０は、携帯電話網１１１１を介して、互いに通信が可能である。さらに、携帯型端末と自動販売機は、赤外線などによって互いに通信が可能１１２０である。
【０００３】
次に購入時の動作について説明する。携帯型端末利用者が、自動販売機１１３０で購入ボタンを選択すると、自動販売機１１３０から携帯型端末１１５０に購入確認情報が送信される。購入確認情報を受け取った携帯型端末１１５０は、購入確認メッセージを画面に表示して、ユーザに購入の確認を行う。携帯型端末利用者が、購入の確認を行うと、携帯型端末１１５０は自動販売機１１３０から自動販売機ＩＤを取得した後、自動販売機管理装置１１４０に、携帯電話網１１１１経由で自動販売機ＩＤと携帯端末ＩＤを送信する。
自動販売機管理装置１１４０は、図示されていない携帯電話会社が管理する利用者データ

ベースにアクセスし、課金が可能かどうかを判断する。課金可能である場合、自動販売機管理装置１１４０は、自動販売機ネットワーク１１１０経由で、自動販売機１１３０に対して販売許可信号を送付する。

【０００４】

販売許可信号を受信した自動販売機１１３０は、携帯型端末利用者に対して商品購入が可能となった事を提示し、購入商品の選択を求める。携帯型端末利用者が購入商品を選択したら、自動販売機１１３０は、商品を排出して携帯型端末利用者に渡すと同時に、販売した事を示す販売通知信号を、自動販売機ネットワーク経由で、自動販売機管理装置１１４０に送信する。

販売通知信号を受信した自動販売機管理装置１１４０は、販売金額を図示されていない携帯電話会社を通じて、別途料金請求を行う事により、料金の徴収を行う。

【０００５】

第１の従来の電子コインシステムは、自動販売機管理装置から自動販売機に送付される購入許可信号を、自動販売機ネットワークを介してではなく、携帯型端末経由で送信する方式が示されている。しかし、購入許可信号が保護されないまま携帯型端末に渡されるため、携帯型端末にて購入許可信号を２重使用することが可能となってしまう。

【０００６】

更に第２の従来例としてＩＣカード内蔵のプリペイドカードもあるが、サービス毎に認証鍵をもたせた別カードを作成するものである。

【０００７】

【特許文献１】

特開２００１－２９７３５５号公報

【０００８】

【発明が解決しようとする課題】

第１の従来の電子コインシステムは、上記のように自動販売機管理装置から、購入許可信号を自動販売機に送信する必要がある。従って、自動販売機管理装置と自動販売機が独自に設置された自動販売機ネットワークで接続されている必要がある。また、この通信路に対して、不正に購入許可信号が流されないように、ネットワークの保護を行う必要がある。そのため、自動販売機専用の、しかも不正を防ぐ複雑な機能を持ったネットワーク構築が必要であるという課題があった。

また、この自動販売機ネットワークが故障した場合、自動販売機管理装置と自動販売機間の通信が遮断されるため、携帯型端末を用いたコインレスでの商品購入が、行えなくなるという課題もある。

また購入許可信号を、携帯型端末経由で、自動販売機に送る方法も示されているが、購入許可信号が保護されないまま携帯型端末に渡るので、１回の支払いで複数回の商品購入が発生し得るという課題がある。

また、自動販売機で商品を購入するたびに、携帯型端末利用者は自動販売機管理装置と通信を行う必要があるため、従来の現金を用いた商品購入に比べ、商品購入に要する時間が長くなるという課題もある。

第２の従来例ではＩＣカード毎に認証鍵が必要であることの他に、複数のサービスを同一ＩＣカードで行うようにすると、多くの認証鍵を設定する必要があり、システムでの発行コストが高くなる。またＩＣカードの認証鍵漏洩の危険性が高い。更にＩＣカード自体を発行する必要がある等の課題がある。

【０００９】

この発明は上記のような課題を解決するためになされたもので、ネットワークに接続されていない自動販売機においても、携帯型端末を用いてコインレスで確実に対価対応の商品購入が行えることを目的とする。

また、電子コイン発行サーバと１回通信を行うだけで、複数の商品を購入でき、購入までの時間を短縮することを目的とする。

また電子コイン発行サーバと自動販売機にのみ認証鍵を設けるだけで、携帯機器は認証鍵

が不要で小規模なものとして、システムを構築することを目的とする。
【００１０】
【課題を解決するための手段】
この発明に係る電子コインシステムは、通常の通信路に接続可能な電子コイン発行サーバを設けて、無線路を介して携帯機器からの発行要求を受け、この要求の正当性を認証するユーザ認証部と、認証後に検証情報付で要求額の電子コインの発行を行う発行部と、発行に伴う課金を行う課金部とを備えた電子コイン発行サーバとし、
無線路を介した携帯機器からのサービス要求に対し、電子コインサーバが保証する電子コインの投入を受けて、検証を行なう電子コイン検証部を備えて、検証後にサービスを行なう自動販売機、とでシステムを構成する。
【００１１】
【発明の実施の形態】
実施の形態１．
図１（ａ）は、この発明の実施の形態１における電子コインシステムの概略を示す図である。
図においてシステムは、携帯型端末利用者（商品購入者）が保有する携帯型端末２０１、商品を販売する自動販売機２０２、携帯型端末利用者からの要求により、自動販売機で利用が可能な電子コインを発行し、携帯型端末利用者の口座から料金引き落としを行う電子コイン発行サーバ２０３、携帯型端末と電子コイン発行サーバ間で通信を行う際に利用される携帯電話網２０４で構成されている。なお、携帯型端末２０１と自動販売機２０２は、赤外線を用いた通信を行う事ができる。
【００１２】
図１（ｂ）は、実施の形態１における自動販売機の機能を示す構成図である。図において、自動販売機２０２は、携帯型端末２０１からデータ受信を行う自動販売機側データ受信部３０３と、携帯型端末にデータ送信する自動販売機側データ送信部３０６と、携帯型端末に自動販売機ＩＤを送信する自動販売機ＩＤ送信部３０７と、利用者から送付された電子コインが正しいかどうかを検証する電子コイン検証情報を生成するための電子コイン検証情報生成部３０１と、電子コインが正しい事を検証する電子コイン検証部３０２と、利用された電子コインの履歴を管理する電子コイン履歴管理部３０５と、携帯型端末利用者に対して商品、もしくはサービスを提供する商品提供部３０４とで構成される。
【００１３】
図２は、実施の形態１における携帯型端末の機能を示す構成図である。
図において、携帯型端末２０１は、自動販売機に対してデータ送信を行う携帯型端末側データ送信部４０１と、自動販売機からのデータを受信する携帯型端末側データ受信部４０６と、携帯電話網を通して携帯電話会社のサーバや、インターネット上に設置されたサーバとデータ送受信を行う携帯電話網通信処理部４０２と、携帯電話網２０４を経由して接続した電子コイン発行サーバ２０３に対して電子コインの発行を依頼する電子コイン発行要求部４０３と、電子コイン発行サーバによって発行された電子コインを受信する電子コイン受信部４０５と、電子コインを自動販売機に送信する電子コイン送信部４０４とで構成される。なお、ここでいう携帯型端末は、単にパーソナルコンピュータに接続されるＰＤＡ等の携帯端末に限定されず、携帯電話も含めた広義の携帯機器を指している。
【００１４】
図３は、実施の形態１における電子コイン発行サーバの機能を示す構成図である。
図において、電子コイン発行サーバ２０３は、電子コインを発行した際に課金を行うため、また接続してきた携帯型端末利用者の認証を行うための携帯型端末利用者情報が格納されたユーザ情報管理部５０９と、接続してきた携帯型端末の利用者を認証するユーザ認証部５０８と、携帯型端末からのデータを受信する発行サーバ側データ受信部５０４と、携帯型端末から受信した電子コイン発行要求を解析する発行要求受信部５０２と、電子コインに付加したシリアル番号を管理し、発行する電子コインにシリアル番号を割り当てるシリアル番号管理部５０６と、シリアル番号と自動販売機ＩＤから電子コインを作成する電

子コイン発行部５０３と、電子コインの金額に応じて携帯型端末利用者に対して課金を行う発行金額課金部５０７と、発行した電子コインを携帯型端末に送付する電子コイン送信部５０５と、携帯型端末へのデータ送信を行う発行サーバ側データ送信部５０１とで構成される。

【００１５】

図４は実施の形態１における各機器間でのデータの流れを示した図であり、また図５は各機器で行われる処理のフローを示した図である。以下、図４および図５に基づいてシステムの動作を説明する。

まず図５のステップ（以後、Ｓと略記する）７０１において、携帯型端末利用者は、携帯型端末２０１を起動し、電子コインの発行を要求する機能を起動する。Ｓ７０２において、携帯型端末２０１は、携帯電話網および携帯電話網と接続された公衆回線などを介して、電子コイン発行サーバ２０３に接続する。Ｓ７０３において、携帯型端末利用者は、携帯型端末２０１に対してユーザＩＤとパスワードを入力する（図４の丸１）。Ｓ７０４において、携帯型端末は、入力されたユーザＩＤとパスワードを、電子コイン発行サーバに送付する（図４の丸２）。

Ｓ７０５において、電子コイン発行サーバ２０３は、携帯型端末２０１から送付されたユーザＩＤとパスワードを受信し、ユーザ情報管理部５０９に格納された情報と比較・検証する事により、登録された携帯型端末利用者である事を認証する。

【００１６】

Ｓ７０６において、携帯型端末は、例えば赤外線やＢｌｕｅｔｏｏｔｈ等の無線通信方式や、ケーブル接続による有線通信により、自動販売機２０２から自動販売機ＩＤを受け取る（図４の丸３）。Ｓ７０７において、携帯型端末２０１は、入力された自動販売機ＩＤから電子コイン発行要求を作成し、電子コイン発行サーバに送付する（図４の丸４）。

Ｓ７０８において、電子コイン発行サーバ２０３は、受信した電子コイン発行要求から自動販売機ＩＤを取得した後、電子コインにユニークに割り当てるシリアル番号を生成する。Ｓ７０９において、Ｓ７０８にて生成／取得した自動販売機ＩＤおよびシリアル番号から、電子コインを作成する。電子コイン８０１の構造は、例えば図６に示したように、シリアル番号８０２、電子コイン改竄検出情報８０３から構成される。電子コイン改竄検出情報８０３は、例えば図７（ａ）に示したように、電子コイン発行サーバおよび自動販売機のみが知っている秘密のアルゴリズムである電子コイン改竄検出情報生成アルゴリズム（秘密の方式）８１３を用いて、自動販売機ＩＤ８１１とシリアル番号８７２から生成される。また、電子コイン改竄検証情報８２３は、例えば図７（ｂ）に示したように、電子コイン発行サーバおよび自動販売機のみが知っている秘密の鍵情報から、一般に知られている例えばＭＡＣ（Ｍｅｓｓａｇｅ　ＡｕｔｈｅｎｔｉｃａｔｉｏｎＣｏｄｅ）等の技術を用いて、自動販売機ＩＤとシリアル番号から生成される。Ｓ７１０において、電子コイン発行サーバは、Ｓ７０９にて生成した電子コイン８０２を、携帯型端末２０１に送信する（図４の丸５）。

【００１７】

Ｓ７１１において、電子コイン発行サーバ２０３は、発行した電子コインの金額に応じて、携帯型端末利用者に課金を行う。この課金の方式としては、ユーザ情報管理部に保管されている情報を元にして、プリペイドによる引き落とし、銀行引き落とし、クレジットカード決済、携帯電話会社による利用料金の代行徴収、等によって行われる。

【００１８】

Ｓ７１２において、携帯型端末は、例えば赤外線やＢｌｕｅｔｏｏｔｈ等の無線通信方式や、ケーブル接続による有線通信により、電子コイン発行サーバから受信した電子コインを、自動販売機に送信する（図４の丸６）。

Ｓ７１３において、自動販売機２０２は、受信した電子コイン８０１から、シリアル番号８０２と、電子コイン改竄検出情報８０３を取り出す。そして、自己が保有する自動販売機ＩＤと、上記で取り出したシリアル番号から、電子コイン検証情報８２３を生成する。

Ｓ７１４において、電子コインから取り出した電子コイン改竄検出情報と、同じくＳ７１

３で生成した電子コイン検証情報から、電子コインが偽造されていない事や、改竄されていない事などを検証する。

【００１９】

Ｓ７１５において、自動販売機は、電子コイン８０１に含まれるシリアル番号８０２が、電子コイン履歴管理部３０５に格納されているかどうかを確認する。もし、シリアル番号が電子コイン履歴管理部に格納されていない場合、この電子コインは過去に使用された事がない（２重使用は行われていない）と判断する。その場合はＳ７１６において、自動販売機２０２は、ユーザに対して商品やサービスの提供を行う。選択できる商品やサービスが複数ある場合は、ユーザに対して商品の選択を求めた後、商品やサービスの提供を行う。Ｓ７１７において、自動販売機は、電子コインのシリアル番号８０２を、一度利用された電子コイン８０１の情報として、電子コイン履歴管理部３０５に保存する。

【００２０】

なお、Ｓ７０２において、携帯型端末から電子コイン発行サーバへの接続方法は、パケット通信や回線交換などによって行われるが、ＳＳＬ／ＴＬＳやＩＰＳｅｃなどの暗号通信技術を適用する事もできる。この場合、携帯型端末－電子コイン発行サーバ間の通信は暗号化されるため、通信路上をやりとりされる電子コインなどの情報が、第三者によって盗まれることを防止できる。

また、Ｓ７０４およびＳ７０５において、携帯型端末利用者の認証を、ユーザＩＤとパスワードによる方式で認証しているが、ＳＳＬクライアント認証機能などのＰＫＩ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒａｃｔｕｒｅ）技術を用いた認証方式を用いて実現してもよい。

また、Ｓ７０６において自動販売機ＩＤを取得するステップは、Ｓ７０６以前に実施されればよい。言い換えれば、Ｓ７０１とＳ７０２の間に実行してもよい。

【００２１】

また、Ｓ７０６において、携帯型端末は、自動販売機から自動販売機ＩＤを受け取る様にしたが、自動販売機に表示されている自動販売機ＩＤを、携帯型端末に備えられた入力装置を用いて携帯型端末利用者に入力させる事により、携帯型端末利用者から自動販売機ＩＤを受け取るようにすることもできる。この場合、自動販売機の構成は、自動販売機ＩＤを送信する自動販売機側データ送信部と自動販売機ＩＤ送信部が不要となるため、図８に示す構成となる。携帯型端末の構成は、自動販売機ＩＤを受信するための携帯端末側データ受信部が不要となるため、図９に示す構成となる。データの流れは、図１０に示したように、自動販売機２０２から送信していた自動販売機ＩＤを、携帯型端末利用者から与えられるようにする（図１０の丸３）。

【００２２】

また、Ｓ７０９において、図７（ａ）、（ｂ）に示した方法にて電子コイン改竄検出情報や検証情報を生成する事を示したが、公開鍵暗号技術の一つである電子署名を用いても、同様に電子コイン改竄検証情報を生成する事ができる。この場合、Ｓ７０９において、図７（ｂ）で示した秘密の鍵情報８２１として、電子コイン発行サーバ２０３のみが知っている秘密鍵情報が利用され、Ｓ７１４において、電子コイン発行サーバの公開鍵が、検証用のパラメータとして追加で利用される。

また、Ｓ７０９において、電子コインの構成を図６に示したが、この電子コインを利用できる自動販売機を識別するための情報として、利用可能の自動販売機ＩＤを含める事もできる。

また、Ｓ７０５とＳ７１１では、電子コイン発行サーバが保有するユーザ情報をベースとして認証や課金を行う事にしたが、このユーザ情報や課金情報等を電子コイン発行サーバで保有せず、携帯電話会社が保有するデータベースを用いて実現してもよい。

【００２３】

また、Ｓ７１２において、携帯型端末と自動販売機間の通信方式として、有線通信や無線通信による方式をあげたが、本発明では、携帯型端末と自動販売機間の通信方式は特に問わない。例えば、携帯型端末から自動販売機への通信を、２次元バーコードや文字表記等

の画像情報によるデータ送信にて実現する事も可能である。この場合、携帯型端末側データ送信部はバーコード等の画像表示機能を持つ液晶画面などを用いて実現され、自動販売機側データ受信部はバーコードリーダー等の画像読みとり装置を用いて実現される。
同じく、自動販売機から携帯型端末への通信を、２次元バーコードや文字表記等の画像情報によるデータ送信にて実現する事も可能である。この場合、自動販売機側データ送信部はバーコード表示機能を持つ液晶画面や、自動販売機本体への印字などを用いて実現され、携帯型端末側データ受信部はバーコードリーダーやデジタルカメラなどの画像読みとり装置を用いて実現される。
また、本実施の形態では、自動販売機を用いた例を示したが、ＰＯＳ端末での支払いや、コンサート会場での入場券などに適用する事もできる。

【００２４】
以上のように、１）電子コイン発行サーバと自動販売機のみが知っている電子コイン改竄検出情報生成アルゴリズム、もしくは２）ＭＡＣ等の公知な電子コイン改竄検出情報生成アルゴリズムと、電子コイン発行サーバと自動販売機のみが知っている秘密の鍵情報、もしくは３）公開鍵暗号技術によって実現される電子署名アルゴリズムと、電子コイン発行サーバのみが知っている秘密鍵、のいずれかを元にして電子コインの生成を行っているため、携帯型端末利用者などの第三者によって偽造する事ができない電子コインを実現することができる。
また、電子コインを作成する際に、電子コインにユニークにシリアル番号を割り当て、それを元に電子コインを生成する。そのため、自動販売機は、使用された電子コインのシリアル番号を管理する事により、２重使用を検出する事ができる。或は電子コインの発行に際してワンタイムコインとして発行し、自動販売機は、使用されたワンタイムコインを、電子コイン履歴管理部３０５で使用済ワンタイムコインの履歴として管理することにより、２重使用を禁止する。

【００２５】
また、自動販売機では、電子コインの正当性検証や２重使用の検証時に、電子コイン発行サーバと通信を行う必要が無いため、ネットワークに接続する必要がない。そのため、ネットワークに接続する事が困難な場所に設置される場合においても利用する事ができる。また、機器の開発コスト、設置費用、保守費用を大幅に削減する事ができる。
また、上記の幾つかの項目以外にも、以下の機能を実現する事ができる。
始めに、携帯型端末と電子コイン発行サーバ間では、ＳＳＬやＩＰＳｅｃ等の汎用暗号通信プロトコルを利用する事ができるので、携帯電話網を介して交換されている電子コインなどの情報を、第三者によって盗まれることがない。

【００２６】
また、携帯型端末と自動販売機間の通信回数は１往復だけですむ。そのため、有線や無線などによる双方向通信だけでなく、携帯型端末の液晶モニタを利用したバーコードや、携帯型端末に搭載されたデジカメによるバーコードリーダーなど、片方向でのみの情報伝達方式を用いても、携帯型端末利用者の負担は軽微である。これらの方式を採用する事により、電子コインシステム専用の通信設備を携帯型端末に設ける必要が無く、コストを削減できる。
また、自動販売機内では、商品を販売した対価として受け取った現金を管理する必要がないため、現金の盗難などの被害への対策が不要となる。そのため、自動販売機を管理する会社は、自動販売機に対してかける保険料のコストを削減できる。また、携帯型端末利用者も、商品購入の度に現金を利用する必要がないため、利便性が向上する。また、電話会社は、電子コインの購入によりパケット通信料が発生し、増収が見込める。さらに、電話会社は、料金徴収代行サービスなどにより、新たな収入源が得られる。

【００２７】
実施の形態２．
以上の実施形態１では、電子コインを作成する際に、電子コインにユニークにシリアル番号を割り当て、それを元に電子コインを生成するため、自動販売機側で使用されたシリア

ル番号を管理する事により、２重使用を検出する事ができる電子コインを実現したものであるが、電子コインと価値とのリンク情報がないため、電子コインの価値はシステムで固定にする必要がある。この実施の形態では、電子コインに任意の価値を持たせたシステムを説明する。

【００２８】

図１１は、本実施の形態における携帯型端末２０１ｃの機能を示す構成図である。

携帯型端末側データ送信部４０６、携帯型端末側データ受信部４０５、携帯電話網通信処理部４０２、電子コイン受信部４０５、電子コイン送信部４０４の各要素は、実施の形態１の図４で示した要素と同一のため、その説明は省略する。本実施の形態では、新たに、携帯型端末利用者もしくは自動販売機から必要な電子コインの金額を取得するための商品価格入力部４０７が付加されている。また、電子コイン発行要求部４０３は、自動販売機ＩＤに加え、商品価格から電子コイン発行要求を作成する。

図１２は、自動販売機２０２ｃの機能を示す構成図である。

自動販売機側データ送信部３０６、自動販売機側データ受信部３０３、自動販売機ＩＤ送信部３０７、電子コイン検証情報生成部３０１、電子コイン検証部３０２、商品提供部３０４、電子コイン履歴管理部３０５は、実施の形態１の図１（ｂ）で示した要素と同一のため、その説明は省略する。本実施の形態では、新たに、商品購入のために必要な商品価格を送信する商品価格送信部３０８が付加されている。

【００２９】

電子コイン発行サーバ２０３の機能構成は、実施の形態１で示した図３の構成と同一である。ただ、発行要求受信部にて、受信した電子コイン発行要求から、商品価格を取得する処理が加わる。また、電子コイン発行部５０２は、自動販売機ＩＤとシリアル番号に加え、商品価格も含めた情報から電子コインを作成する。また、発行金額課金部５０７では、固定料金ではなく、商品価格に応じた課金処理が行なわれる。

【００３０】

図１３は本実施の形態における各機器間でのデータの流れを示した図であり、また図１４は各機器で行われる処理のフローを示した図である。以下、図１３および図１４に基づいて動作を説明する。

Ｓ１７０１からＳ１７０５の処理は、図５に示したＳ７０１からＳ７０５の処理と同一であるため、ここでは説明は省略する。

Ｓ１７０６において、携帯型端末２０１ｃは、例えば赤外線やＢｌｕｅｔｏｏｔｈ等の無線通信方式や、ケーブル接続による有線通信により、自動販売機２０２ｃから自動販売機ＩＤと商品価格情報を受け取る（図１３の丸３）。この時送付される商品価格は、自動販売機に設定された標準価格や、携帯型端末利用者が自動販売機に対して購入したい商品を通知する事により、自動販売機側で決定される。Ｓ１７０７において、携帯型端末は、入力された自動販売機ＩＤと商品価格から電子コイン発行要求を作成し、電子コイン発行サーバに送付する（図１３の丸４）。この時作成される電子コイン発行要求８３１は、例えば図１５に示したような構造である。

【００３１】

Ｓ１７０８において、電子コイン発行サーバ２０３は、受信した電子コイン発行要求８３１から自動販売機ＩＤと商品価格情報を取得した後、電子コインにユニークに割り当てるシリアル番号を生成する。Ｓ１７０９において、Ｓ１７０８にて生成／取得した自動販売機ＩＤ、商品価格およびシリアル番号から、電子コイン８４１を作成する。電子コインの構造は、例えば図１６に示したように、シリアル番号８０２、商品価格８４２、電子コイン改竄検出情報８４３から構成される。電子コイン改竄検出情報は、例えば図１７に示したように、電子コイン発行サーバおよび自動販売機のみが知っている秘密のアルゴリズムである電子コイン改竄検出情報生成アルゴリズム８５２を用いて、自動販売機ＩＤとシリアル番号と商品価格から生成される。また、電子コイン改竄検証情報は、例えば図７（ｂ）に示したように、電子コイン発行サーバおよび自動販売機のみが知っている秘密の鍵情報８５４から、一般に知られている例えばＭＡＣ（Ｍｅｓｓａｇｅ　Ａｕｔｈｅｎｔｉｃ

ａｔｉｏｎ　Ｃｏｄｅ）等の技術を用いて、自動販売機ＩＤとシリアル番号と商品価格から生成される。Ｓ１７１０において、電子コイン発行サーバは、Ｓ１７０９にて生成した電子コイン８４１を、携帯型端末２０１ｃに送信する（図１３の丸５）。Ｓ１７１１において、電子コイン発行サーバは、発行した電子コインの商品価格に応じて、携帯型端末利用者に課金を行う。この課金の方式としては、ユーザ情報管理部に保管されている情報を元にして、プリペイドによる引き落とし、銀行引き落とし、クレジットカード決済、携帯電話会社による利用料金の代行徴収、等によって行われる。

【００３２】

Ｓ１７１２において、携帯型端末は、例えば赤外線やＢｌｕｅｔｏｏｔｈ等の無線通信方式や、ケーブル接続による有線通信により、電子コイン発行サーバから受信した電子コインを、自動販売機に送信する（図１３の丸６）。

Ｓ１７１３において、自動販売機２０２ｃは、受信した電子コイン８４１からシリアル番号８０２と、商品価格８４２と、電子コイン改竄検出情報８４３を取り出す。そして、自己が保有する自動販売機ＩＤと、上記で取り出したシリアル番号と商品価格から、電子コイン検証情報を生成する。Ｓ１７１４において、電子コインから取り出した電子コイン改竄検出情報と、同じくＳ１７１３で生成した電子コイン検証情報から、電子コインが偽造されていない事や、改竄されていない事などを検証する。Ｓ１７１５において、自動販売機は、電子コインに含まれるシリアル番号が、電子コイン履歴管理部３０５に格納されているかどうかを確認する。もし、シリアル番号が電子コイン履歴管理部に格納されていない場合、この電子コインは過去に使用された事がない（２重使用は行われていない）と判断し、Ｓ１７１６において、電子コインに格納された商品価格に応じて、ユーザに対して商品やサービスの提供を行う。選択できる商品やサービスが複数ある場合は、ユーザに対して商品の選択を求めた後、商品やサービスの提供を行う。Ｓ１７１７において、自動販売機は、電子コインのシリアル番号を、一度利用された電子コインの情報として、それらの数を積算し、電子コイン履歴管理部に保存する。または提供した商品価格の金額を積算し、後の課金のための情報として電子コイン履歴管理部に保存する。

【００３３】

なお、本実施の形態２においても、実施の形態１と同様に、携帯型端末から電子コイン発行サーバへの接続方法として、ＳＳＬ／ＴＬＳやＩＰＳｅｃなどの暗号通信技術を適用する事ができる。また、ＰＫＩによる携帯型端末利用者認証を行ってもよい。また、自動販売機ＩＤや商品価格の入力は、Ｓ１７０６以前であればいつでもよく、また、自動販売機ＩＤや商品価格の入力を、携帯型端末利用者に求める事もできる。また、電子署名技術を用いて電子コイン改竄検出情報を生成することも、また、電子コインに、自動販売機ＩＤを含める事もできる。また、電子コイン発行サーバがユーザ情報を持たず、携帯電話会社のデータベースを用いてユーザ認証／課金管理を行っても良い。その他通信方式として、２次元バーコードなどの画像を用いた通信を適用する事もでき、また、自動販売機以外の用途にも適用できる。

【００３４】

以上のように、電子コインの中に商品価格を含める事により、電子コインの価値を一定額に固定することなく、任意の価値に設定する事ができる。そのため、商品価格が同一でない複数の商品を扱うような自動販売機に対しても、本電子コインを適用する事によってキャッシュレスの買い物ができるようになる。

【００３５】

実施の形態３．

上記各実施の形態では、電子コインの２重使用を検出するために、自動販売機内で使用された電子コインのシリアル番号を管理している。しかし、２重使用を検出するためには、電子コイン履歴管理部に格納されたシリアル番号の消去を行う事ができず、自動販売機内に大きな記憶領域が必要になる。そこで、本実施の形態では、電子コインに有効期限を設ける事により、自動販売機内でのシリアル番号の保存期間を一定期間に押さえ、記憶領域の増大を防止したシステムを説明する。

【００３６】
図１８は、本実施の形態における自動販売機２０２ｄの機能を示す構成図である。
実施の形態３では、実施の形態２、図１２に示す構成に加えて、新たに電子コインの有効期限を検証するための現在時刻を管理する現在時刻管理部３０９が付加されている。その他の各要素は、図１２中の同番号の要素と同じものである。
【００３７】
図１９は、電子コイン発行サーバ２０３ｄの機能を示す構成図である。
実施の形態３では、実施の形態１、図３に示す構成に加えて、電子コインの有効期間を決定する有効期間管理部５１０が、新たに付加されている。その他の各要素は、図３の同番号のそれと同一である。また、電子コイン発行部５０３にて、自動販売機ＩＤとシリアル番号と商品価格に加え、有効期間を含めた情報を電子コインに含める。
携帯型端末の機能構成は、実施の形態２で示した構成と同一である。
【００３８】
図２０は各機器で行われる処理のフローを示した図である。以下、この図に基づいて動作を説明する。
Ｓ２４０１からＳ２４０７の処理は、図１４に示したＳ１７０１からＳ１７０７の処理と同一である。
Ｓ２４０８において、電子コイン発行サーバ２０３ｄは、受信した電子コイン発行要求から自動販売機ＩＤと商品価格を取得した後、電子コインにユニークに割り当てるシリアル番号を生成し、電子コインの有効期間を決定する。有効期間は、開始時刻と終了時刻から構成され、自動販売機の種別や、運用ルールによって任意に定める。
【００３９】
Ｓ２４０９において、Ｓ２４０８にて生成／取得した自動販売機ＩＤ、商品価格、シリアル番号、および有効期間から、電子コインを作成する。この電子コイン８６１の構造は、例えば図２１に示したように、シリアル番号８０２、商品価格８４２、有効期間８６２、電子コイン改竄検出情報８６３から構成される。電子コイン改竄検出情報８６３は、例えば図２２（ａ）に示したように、電子コイン発行サーバおよび自動販売機のみが知っている秘密のアルゴリズムである電子コイン改竄検出情報生成アルゴリズム８６５を用いて、自動販売機ＩＤ８１１とシリアル番号８１２と商品価格８４２と有効期間８６２から生成される。また、電子コイン改竄検証情報８６９は、例えば図２２（ｂ）に示したように、電子コイン発行サーバおよび自動販売機のみが知っている秘密の鍵情報８６７から、一般に知られているＭＡＣ等の技術を用いて、自動販売機ＩＤ８１１とシリアル番号８１２と商品価格８４２と有効期間８６２から生成される。
【００４０】
Ｓ２４１０からＳ２４１２の処理は、図１４に示したＳ１７１０からＳ１７１２の処理と同一である。
Ｓ２４１３において、自動販売機は、受信した電子コインからシリアル番号８０２と、商品価格８４２と、有効期間８６２と、電子コイン改竄検出情報８６３を取り出す。そして、自己が保有する自動販売機ＩＤと、上記で取り出したシリアル番号と商品価格と有効期間から、電子コイン検証情報８６９を生成する。
Ｓ２４１４およびＳ２４１５の処理は、図１４に示したＳ１７１５およびＳ１７１５の処理と同一である。
【００４１】
Ｓ２４１６において、自動販売機２０２ｄは、自己が管理している現在時刻が、Ｓ２４１３で取得した有効期間内であるかどうかを判定する。もし現在時刻が有効期間内であるなら、電子コイン８６１は有効とみなす。なお、電子コイン発行サーバ２０３ｄと自動販売機２０２ｄの時刻のズレを考慮し、現在時刻がわずかに有効期間から外れているだけであれば、その電子コインを有効とみなす事も可能である。Ｓ２４１７において、自動販売機は、要求商品が複数ある場合を含めて、電子コイン８６１に格納された商品価格に応じて、ユーザに対して商品やサービスの提供を行う。Ｓ２４１８において、自動販売機は、電

子コインのシリアル番号と有効期間を、一度利用された電子コインの情報として、電子コイン履歴管理部３０５に保存する。

【００４２】

なお、電子コイン履歴管理部３０５に格納されたシリアル番号は、Ｓ２４１６の検証において、有効期間が過ぎているため無効と判断されるものに関しては、削除してよい。この削除は任意のタイミングで実施可能であり、上記ステップとは別に実施してよい。

また、Ｓ２４０８において、開始時刻と終了時刻から構成される有効期間を生成したが、代わりに有効期間を発行時刻のみから構成される情報としてもよい。この場合、Ｓ２４１６において有効期間の確認を行う際、発行時刻と現在時刻とのズレが、自動販売機で事前に定められた範囲内におさまっている場合のみ有効と判断する。

【００４３】

なお、本実施の形態３においても、実施の形態２と同様に、接続方法として、各種暗号通信技術を適用できるし、ＰＫＩによる携帯型端末利用者認証を行える。また、自動販売機ＩＤや商品価格の入力を他のタイミングにしてもよく、また携帯型端末利用者に求めてもよい。また、電子署名技術を用いることや、電子コインに、自動販売機ＩＤを含めることを行ってもよい。また、携帯電話会社のデータベースを用いてユーザ認証／課金管理を行ってもよい。また、携帯型端末と自動販売機間の通信方式として、他の方式を用いてもよい。

【００４４】

また、本実施の形態は、他の実施の形態に対して、有効期間を管理する機能を付加した構成としてもよい。

以上のように、電子コインの中に有効期間を含め、自動販売機内の電子コイン履歴管理部でシリアル番号を管理するようにしたので、必要な記憶領域の増大が防止できる。

【００４５】

実施の形態４．

上記実施の形態では、電子コインの２重使用を検出するために、自動販売機内で管理されているシリアル番号の保存期間を一定期間として、記憶領域の増大を防止した。この実施の形態で利用される電子コインは、利用の度に電子コイン発行サーバにアクセスする必要があったが、電子コインを発行するために時間がかかるため、現金での購入に比べ、時間がかかる。本実施の形態は、事前に複数の電子コインを購入可能として、購入に必要な時間を短縮したシステムを説明する。

【００４６】

図２３は、本実施の形態における、携帯型端末２０１ｅの機能を示す構成図である。

実施の形態４では、実施の形態２、図１１に示す構成に加えて、新たに携帯型端末利用者から電子コインの発行枚数を受け取る発行枚数入力部４０８、購入した複数の電子コインを保存する電子コイン保存部４０９が加わる。また、電子コイン発行要求部は、自動販売機ＩＤ、商品価格に加え、発行枚数から電子コイン発行要求を作成する様に変更される。

【００４７】

図２４は、電子コイン発行サーバ２０３ｅの機能を示す構成図である。

実施の形態４では、実施の形態３、図１９の構成に加えて、携帯型端末から要求された発行枚数の数だけ電子コインの発行を行うように制御を行う発行枚数制御部５１１が、新たに付加される。また、電子コイン送信部５０５は、発行した発行枚数分の電子コインをまとめた電子コイン群を送付するように拡張される。また、発行金額課金部５０７は、商品価格と発行枚数から計算される合計金額分の課金が行われるように拡張される。

自動販売機の機能構成は、実施の形態３で示した構成と同一である。

【００４８】

図２５は実施の形態４における各機器間でのデータの流れを示した図であり、また図２６および図２７は各機器で行われる処理のフローを示した図である。以下、図２５ないし図２７に基づいて動作を説明する。

始めに、携帯型端末２０１ｅを用いて複数枚の電子コインを購入するフェーズの流れを説

明する。
Ｓ３１０１において、携帯型端末利用者は、携帯型端末を起動し、電子コインの発行要求機能を起動する。Ｓ３１０２において、携帯型端末２０１ｅは、各種の無線通信方式や、ケーブル接続による有線通信により、自動販売機２０２から自動販売機ＩＤと商品価格を受け取る（図２５の丸１）。Ｓ３１０３において、携帯型端末は、携帯電話網および携帯電話網と接続された公衆回線などを介して、電子コイン発行サーバ２０３ｅに接続する。Ｓ３１０４において、携帯型端末利用者は、携帯型端末に対してユーザＩＤとパスワードを入力する（図２５の丸２）。Ｓ３１０５において、携帯型端末は、入力されたユーザＩＤとパスワードを、電子コイン発行サーバ２０３ｅに送付する（図２５の丸３）。

【００４９】

Ｓ３１０６において、電子コイン発行サーバ２０３ｅは、携帯型端末から送付されたユーザＩＤとパスワードを受信し、ユーザ情報管理部５０９に格納された情報と比較・検証して、登録された携帯型端末利用者である事を認証する。
Ｓ３１０７において、携帯型端末２０１ｅは、携帯型端末利用者から、発行を要求する電子コインの発行枚数を受け取る。Ｓ３１０８において、携帯型端末は、Ｓ３１０２で受け取った自動販売機ＩＤと商品価格、Ｓ３１０７で入力された発行枚数から電子コイン発行要求を作成し、電子コイン発行サーバに送付する（図２５の丸５）。この電子コイン発行要求８７１は、例えば図２８に示すような構成となる。

【００５０】

Ｓ３１０９において、電子コイン発行サーバ２０３ｅは、受信した電子コイン発行要求から自動販売機ＩＤ８３２、商品価格８３３、発行枚数８７２を取得した後、電子コインにユニークに割り当てるシリアル番号を発行枚数の数だけ生成し、電子コインの有効期間を決定する。有効期間は、例えば開始時刻と終了時刻から構成される。
Ｓ３１１０において、Ｓ３１０９にて生成／取得した自動販売機ＩＤ、商品価格、シリアル番号、および有効期間から、発行枚数分の電子コインを作成する。電子コインの作成方法は、実施の形態３で示した方法と同一であるが、それぞれの電子コインに対して、Ｓ３１０９で生成したシリアル番号がそれぞれ割り当てられる。
Ｓ３１１１において、電子コイン発行サーバは、Ｓ３１１０にて生成した電子コインをまとめて電子コイン群を作成し、携帯型端末に送信する（図２５の丸６）。Ｓ３１１２において、電子コイン発行サーバは、発行した電子コインの商品価格と発行枚数に応じて積算して、携帯型端末利用者に課金を行う。この課金の方式としては、他の実施の形態で示される各種の方法がある。
Ｓ３１１３において、携帯型端末は、受け取った電子コインを携帯型端末内の記憶装置に保存する。なお、この時、自動販売機ＩＤと関連づけて保存してもよい。

【００５１】

次に、電子コインを使用するフェーズの処理の流れを示す。
Ｓ３２０１において、携帯型端末利用者は、携帯型端末２０１ｅを起動し、電子コインを使用する機能を起動する。Ｓ３２０２において、携帯型端末は、例えば記憶装置に保存された電子コインを読み出し、その電子コインを画面に表示し、携帯型端末利用者は使用する電子コインを選択する。Ｓ３２０３において、携帯型端末は、無線通信方式や有線通信により、電子コインを自動販売機に送信する（図２５の丸７）。
Ｓ３２０４からＳ３２０９までの処理は、実施の形態３で示したＳ２４１３からＳ２４１８の処理と同一である。

【００５２】

Ｓ３２１０において、携帯型端末は、使用した電子コインを記憶装置内から削除する。
なお、Ｓ３１０２で示した処理内容は、Ｓ３１０８より前であれば任意の場所で実行してもよい。
また、Ｓ３１０２で、自動販売機ＩＤと商品価格を取得した際、携帯型端末内に保管されている電子コインを検索して、該当する電子コインが存在する場合は、自動で電子コイン使用のための機能を起動してもよい。

また、Ｓ３１０７にて、携帯型端末利用者から希望する電子コインの発行枚数を受け取るが、この時、商品価格と発行枚数の組を複数受け取ってもよい。この場合、電子コイン発行サーバに送付される電子コイン発行要求は、例えば図２９の様になる。
また、Ｓ３２０２では、使用する電子コインを携帯型端末利用者に選択させているが、Ｓ３１０２の手順と同様にして自動販売機から自動販売機ＩＤと商品価格を取得し、その値を元に自動で使用する電子コインを選択してもよい。

【００５３】

なお、本実施の形態４においても、実施の形態３と同様に、接続方法として、各種の暗号通信技術を適用できるし、ＰＫＩによる携帯型端末利用者認証も行える。また、自動販売機ＩＤや商品価格の入力を、携帯型端末利用者に求める事もでき、電子署名技術を用いたり、電子コインに、自動販売機ＩＤを含めてもよい。その他の各種の変形ができることは、実施の形態３と同様である。また、自動販売機と電子コイン発行サーバ間での時刻のズレを考慮して有効期間の検証を行う事もでき、有効期限として発行時刻のみを格納してもよい。
更に、本実施の形態の構成を実施の形態１および実施の形態２の構成に対して付加して、同時に複数枚の電子コインの発行を行うようにしてもよい。

【００５４】

以上のように、電子コイン発行要求に希望する電子コインの発行枚数を格納し、電子コイン発行サーバにて複数枚の電子コインを一括して発行するので、２回目以降の商品購入時において改めて電子コイン発行が必要なくなり、商品購入の時間を短縮できる。
また、電子コイン発行要求に、商品価格と発行枚数の組を複数格納すれば、価格が異なる商品を買うための電子コインも、１回の電子コイン発行要求で生成できる。

【００５５】

実施の形態５．
上記の実施の形態では、電子コインの複数同時購入を可能とするシステムを示したが、更に自動販売機内プログラムのミス、または悪意ある第三者により、自動販売機内に格納されている電子コインの使用履歴が改竄される可能性を減らしたシステムを説明する。即ち本実施の形態は、電子コインの検証や使用履歴の管理を行う機能を、改竄などの不正から守る専用ハードウェアを用いて、安全性を高めている。

【００５６】

図３０は、本実施の形態における電子コインシステムの概略を示す全体構成図である。
図において、図２に示した構成に対し、新たに自動販売機に内蔵もしくは横に設置され、電子コインの検証や利用履歴の管理を行う専用の、電子コイン検証装置２０５が付加されている。この専用装置は、実施の形態４で自動販売機内に実装されていた機能のうち、改竄などの不正に対しての保護が必要な機能を、別ハードウェアとしたものである。
自動販売機との通信は、専用の接続線によって実現される。これらのハードウェアによる専用装置は、一般に、改竄や解析などに対しての耐性を持つ耐タンパ装置と呼ばれる。

【００５７】

図３１は、本実施の形態における自動販売機２０２ｆの機能を示す構成図である。
実施の形態３、図１８の構成に加えて、実施の形態５では、新たに、電子コインの有効性を検証するための電子コイン検証装置２０５と通信を行うための検証装置連携部３１０が付加されている。
携帯型端末の機能構成は、実施の形態４で示した構成と同一である。
電子コイン発行サーバの機能構成は、実施の形態４で示した構成と同一である。
図３２は、電子コイン検証装置の機能を示す構成図である。図において、自動販売機ＩＤ送信部３０７、電子コイン検証情報生成部３０１、電子コイン検証部３０２、電子コイン履歴管理部３０５、現在時刻管理部３０９は、実施の形態３で自動販売機２０２ｄに実装される機能と同一である。これらに自動販売機からのデータを受信するための検証装置側データ受信部３１２、自動販売機へのデータ送信を行うための検証装置側データ送信部３１１を加えたもので構成されている。

【００５８】
図３３は実施の形態５における各機器間でのデータの流れを示した図であり、また図３４と図３５は各機器で行われる処理のフローを示した図である。以下、図３３ないし図３５に基づいて動作を説明する。
始めに、携帯型端末を用いて複数枚の電子コインを購入するフェーズの流れを説明する。
Ｓ３９０１において、携帯型端末利用者は、携帯型端末を起動し、電子コイン発行要求機能を起動する。Ｓ３９０２において、自動販売機２０２ｆは、電子コイン検証装置２０５から、電子コイン検証装置内に格納されている自動販売機ＩＤを取得する。
Ｓ３９０３からＳ３９１４までの動作は、図２６のＳ３１０２からＳ３１１３までの動作と同一である。

【００５９】
次に、電子コインを使用するフェーズの処理の流れを示す。
Ｓ４００１からＳ４００３間での処理は、図２７のＳ３２０１からＳ３２０３までの処理と同一である。
Ｓ４００４において、自動販売機２０２ｆは、携帯型端末から受信した電子コインを、電子コイン検証装置２０５に送付し、電子コインの検証を要求する。
Ｓ４００５からＳ４００８までの処理は、図２７のＳ３２０４からＳ３２０７のステップの実行者が、自動販売機から電子コイン検証装置に変更された点が異なるが、処理の内容としては同一である。
Ｓ４００９において、電子コイン検証装置は、Ｓ４００５からＳ４００８までの処理結果を、自動販売機に送付する。

【００６０】
Ｓ４０１０において、自動販売機は、電子コイン検証装置から送付された検証結果が「検証ＯＫ」であった場合は、選択できる商品やサービスが複数ある場合を含めて電子コインに格納された商品価格に応じて、ユーザに対して商品やサービスの提供を行う。Ｓ４０１１において、自動販売機は、電子コインを使用した事を電子コイン管理装置に通知する。
Ｓ４０１２において、電子コイン検証装置は、電子コインのシリアル番号と有効期間を、一度利用された電子コインの情報として、電子コイン履歴管理部３０５に保存する。
Ｓ４０１３において、携帯型端末は、使用した電子コインを記憶装置内から削除する。
なお、Ｓ３９０２および３９０３で示した処理内容は、Ｓ３９０９より前であれば任意のステップで実行してもよい。

【００６１】
また、実施の形態５では、自動販売機ＩＤ送信部、電子コイン検証情報生成部、電子コイン検証部、電子コイン履歴管理部、現在時刻管理部を、電子コイン検証装置内で実装する方式を示したが、これら全ての処理ブロックを電子コイン検証装置で実装しなくてもよい。例えば、前記機能ブロックのうち、一部のみを電子コイン検証装置内で実現し、他機能を自動販売機内に実装してもよい。

【００６２】
なお、本実施の形態５においても、実施の形態４と同様に、接続方法として、各種の暗号通信技術を適用する事ができるし、ＰＫＩによる携帯型端末利用者認証も行える。また、自動販売機ＩＤや商品価格の入力を、携帯型端末利用者に求める事もでき、電子署名技術を用いたり、電子コインに、自動販売機ＩＤを含める事もできる。その他の各種の変形ができることは、上記各実施の形態で述べた通り、明らかである。
更に実施の形態を実施の形態１、実施の形態２、および実施の形態３と組合わせてもよい。

【００６３】
以上のように、電子コインの検証や使用履歴の管理を行う機能を、改竄などの不正から守るための専用ハードウェアを用いるので、自動販売機内プログラムのミス、または悪意ある第三者によって、自動販売機内に格納されている電子コインの使用履歴が改竄されることを防止できる。

【００６４】
実施の形態６．
上記実施の形態では、専用のハードウェアを用いて、電子コインの使用履歴を安全に管理するシステムを示した。本実施の形態では、電子コイン全体を自動販売機に送付することなく、携帯型端末が正しい電子コインを保有している事を認証するプロトコルを用いることで、通信途中での電子コインの盗難を防止するシステムを説明する。
【００６５】
図３６は、本実施の形態における電子コイン検証装置２０５ｇの機能を示す構成図である。
実施の形態５、図３２の構成に加えて、実施の形態６では、携帯型端末が正しい電子コインを保有しているかどうかを認証するための電子コイン認証要求部３１３が付加されている。
図３７は、本実施の形態における携帯型端末２０１ｇの機能を示す構成図である。
実施の形態４、図２３の構成に加えて、実施の形態６では、新たに、電子コインを解析して一部情報のみを自動販売機に送付する電子コイン断片送信部４０４、自動販売機（もしくは電子コイン検証装置）に対して正しい電子コインを保持している事を証明するための電子コイン認証応答部４１０が付加されている。
自動販売機、電子コイン発行サーバに関しては、実施の形態５で示した機能構成と同一である。
【００６６】
図３８は実施の形態６における各機器で行われる処理のフローを示した図であり、以下、図３８に基づいて電子コインの使用動作を説明する。
なお、携帯型端末を用いて電子コインを購入するフェーズの流れは、実施の形態５で示した図３４に示す処理の流れと同一である。
先ず、Ｓ４３０１とＳ４３０２の処理は、実施の形態５で示したＳ４００１とＳ４００２の処理と同一である。
Ｓ４３０３において、携帯型端末２０１ｇは、電子コインの中に含まれる「電子コイン改竄検出情報」以外の電子コイン部分情報を自動販売機に送付する。
【００６７】
Ｓ４３０４において、自動販売機は、携帯型端末から受信した電子コイン部分情報を、電子コイン検証装置に送付し、電子コインの検証を要求する。
Ｓ４３０５において、電子コイン検証装置２０５は、受信した電子コイン部分情報からシリアル番号と、商品価格と、有効期間を取り出す。そして、自己が保有する自動販売機ＩＤと、上記で取り出したシリアル番号と商品価格と有効期間から、電子コイン検証情報を生成する。Ｓ４３０６において、電子コイン検証装置は、自動販売機を経由して携帯型端末と通信を行い、例えばＣｈａｌｌｅｎｇｅ－ａｎｄ－Ｒｅｓｐｏｎｓｅプロトコルとして一般に知られている通信プロトコルを用いて、携帯型端末が保有する「電子コイン改竄検出情報」と、Ｓ４３０５にて電子コイン検証装置が生成した「電子コイン検証情報」が同一である事を認証する。認証の結果、携帯型端末が、正しい電子コイン改竄検出情報を保持していると認証できた場合は、次のステップに進む。
Ｓ４３０７からＳ４３１３までの処理は、実施の形態５で示したＳ４００７からＳ４０１３の処理内容と同一である。
【００６８】
なお、本実施の形態６においても、接続方法として、各種の暗号通信技術を適用する事ができるし、ＰＫＩによる携帯型端末利用者認証も行える。また、自動販売機ＩＤや商品価格の入力を、携帯型端末利用者に求める事もでき、電子署名技術を用いることや、電子コインに、自動販売機ＩＤを含める事もできる。また、その他の各種の変形ができることは、明らかである。更に自動販売機以外の用途にも適用する事ができ、ハードウェアの機能構成も各種の変形ができる。
更に、本実施の形態と、実施の形態１ないし実施の形態４の構成と組合わせることもでき

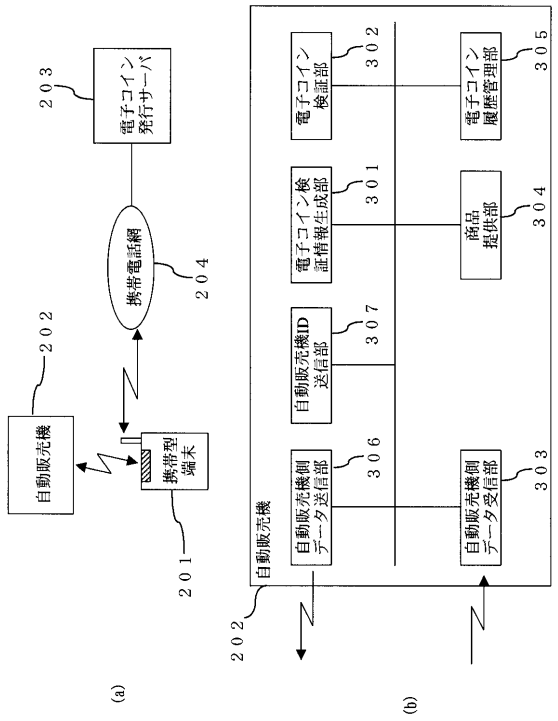
る。
【００６９】
【発明の効果】
以上のようにこの発明によれば、携帯機器からの要求により電子コインを発行する電子コイン発行サーバと、電子コインを検証する自動販売機を備えたので、通常の自動販売機であっても、検証機能を付加するだけでコインレスでサービス提供を安全確実に行なえる効果がある。
【図面の簡単な説明】
【図１】この発明の実施の形態１における電子コインシステムと実施の形態１における自動販売機の構成を示す図である。
【図２】実施の形態１における携帯型端末の構成を示す図である。
【図３】実施の形態１における電子コイン発行サーバの構成を示す図である。
【図４】実施の形態１における各機器間のデータの流れを示す図である。
【図５】実施の形態１における各機器が行なう処理フローを示す図である。
【図６】実施の形態１における電子コインの構成を示す図である。
【図７】実施の形態１における改竄検出／検証情報生成方法を説明する図である。
【図８】実施の形態１における他の自動販売機の構成を示す図である。
【図９】実施の形態１における他の携帯型端末の構成を示す図である。
【図１０】実施の形態１の各機器間における他のデータの流れを示す図である。
【図１１】この発明の実施の形態２における携帯型端末の構成を示す図である。
【図１２】実施の形態２における自動販売機の構成を示す図である。
【図１３】実施の形態２における各機器間のデータの流れを示す図である。
【図１４】実施の形態２における各機器が行なう処理フローを示す図である。
【図１５】実施の形態２における携帯型端末が送信する電子コイン発行要求の情報内容を示す図である。
【図１６】実施の形態２における電子コインの構成を示す図である。
【図１７】実施の形態２における改竄検出／検証情報生成方法を説明する図である。
【図１８】この発明の実施の形態３における自動販売機の構成を示す図である。
【図１９】実施の形態３における電子コイン発行サーバの構成を示す図である。
【図２０】実施の形態３における各機器が行なう処理フローを示す図である。
【図２１】実施の形態３における電子コインの構成を示す図である。
【図２２】実施の形態３における改竄検出／検証情報生成方法を説明する図である。
【図２３】この発明の実施の形態４における携帯型端末の構成を示す図である。
【図２４】実施の形態４における電子コイン発行サーバの構成を示す図である。
【図２５】実施の形態４における各機器間のデータの流れを示す図である。
【図２６】実施の形態４における各機器が行なう処理フローを示す図である。
【図２７】実施の形態４における各機器が行なう処理フローを示す図である。
【図２８】実施の形態４における携帯型端末が送信する電子コイン発行要求の情報内容を示す図である。
【図２９】実施の形態４における携帯型端末が送信する他の電子コイン発行要求の情報内容を示す図である。
【図３０】この発明の実施の形態５における電子コインシステムの構成を示す図である。
【図３１】実施の形態５における自動販売機の構成を示す図である。
【図３２】実施の形態５における電子コイン検証装置の構成を示す図である。
【図３３】実施の形態５における各機器間のデータの流れを示す図である。
【図３４】実施の形態５における各機器が行なう処理フローを示す図である。
【図３５】実施の形態５における各機器が行なう処理フローを示す図である。
【図３６】この発明の実施の形態６における電子コイン検証装置の構成を示す図である。
【図３７】実施の形態６における携帯型端末の構成を示す図である。
【図３８】実施の形態６における各機器が行なう処理フローを示す図である。

【図３９】従来の電子マネーシステムの構成を示す図である。

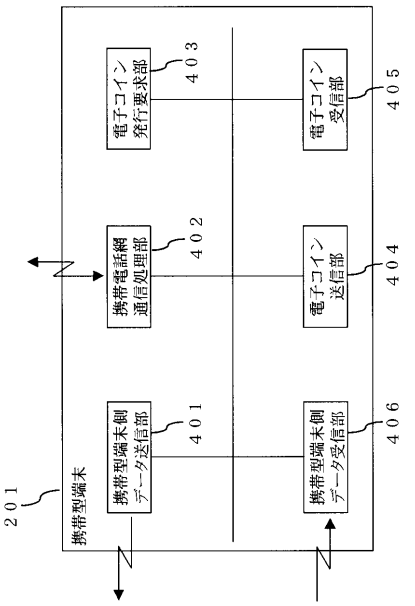
【符号の説明】

２０１、２０１ｂ、２０１ｃ、２０１ｅ、２０１ｇ　携帯型端末（携帯機器）、２０２、２０２ｂ、２０２ｃ、２０２ｄ、２０２ｆ　自動販売機、２０３、２０３ｄ、２０３ｅ　電子コイン発行サーバ、２０５、２０５ｇ　電子コイン検証装置、３０１　電子コイン検証情報生成部、３０２　電子コイン検証部、３０５電子コイン履歴管理部、３０７　自動販売機ＩＤ（識別記号）送信部、３０８商品価格送信部、３０９　現在時刻管理部、３１０　検証装置連携部、電子コイン認証要求部、４０３　電子コイン発行要求部、４０４　電子コイン送信部、４０５　電子コイン受信部、４０７　商品価格入力部、４０９　電子コイン保存部、４１０　電子コイン認証応答部、５０３　電子コイン発行部、５０６　シリアル番号管理部、５０７　発行金額課金部、５０８　ユーザ認証部、５１０　有効期間管理部。

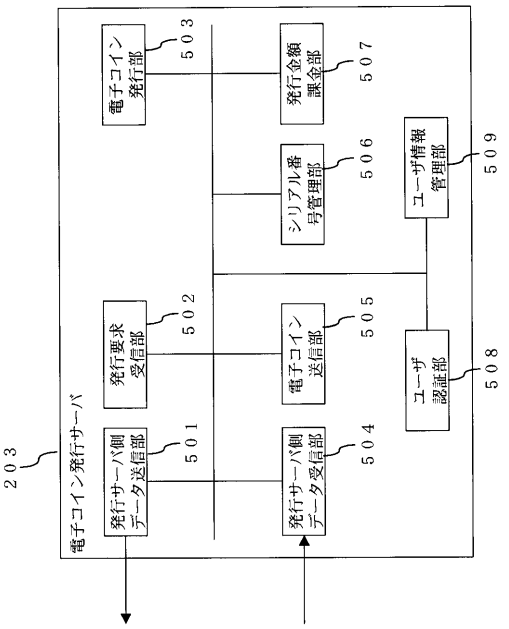
【図１】



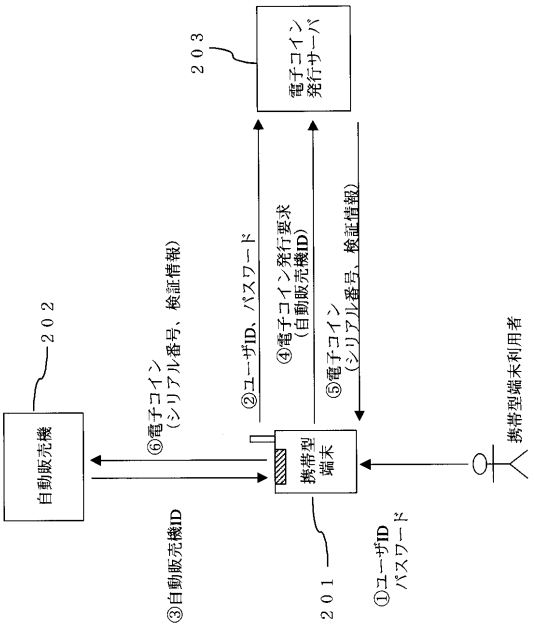
【図２】



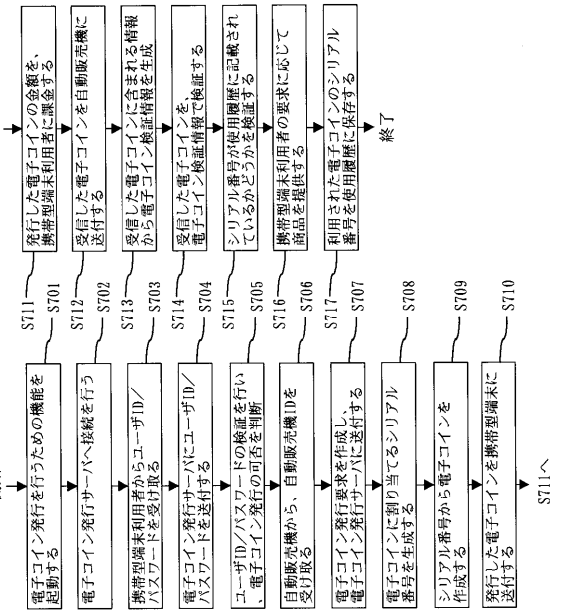
【図３】


電子コイン発行サーバ
２０３
発行サーバ側
データ送信部
５０１
発行要求
受信部
５０２
発行サーバ側
データ受信部
５０４
電子コイン
送信部
５０５
ユーザ
認証部
５０８
電子コイン
発行部
５０３
シリアル番
号管理部
５０６
ユーザ情報
管理部
５０９
発行金額
課金部
５０７

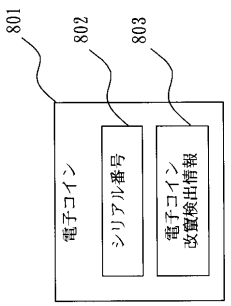
【図４】


２０３
電子コイン
発行サーバ
２０２
自動販売機
⑥電子コイン
（シリアル番号、検証情報）
③自動販売機ID
②ユーザID、パスワード
④電子コイン発行要求
（自動販売機ID）
⑤電子コイン
（シリアル番号、検証情報）
携帯型
端末
２０１
①ユーザID
パスワード
携帯型端末利用者

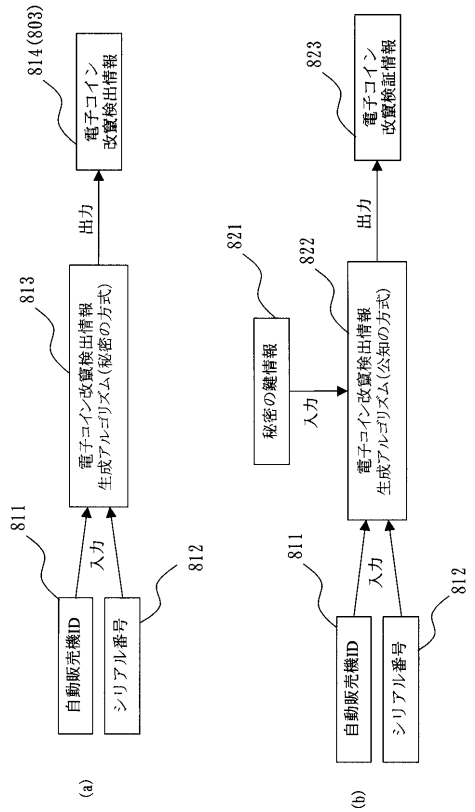
【図５】


開始
S710より
電子コイン発行を行うための機能を
起動する
S701
電子コイン発行サーバへ接続を行う
S702
携帯型端末利用者からユーザID／
パスワードを受け取る
S703
電子コイン発行サーバにユーザID／
パスワードを送付する
S704
ユーザID／パスワードの検証を行い
、電子コイン発行の可否を判断
S705
自動販売機から、自動販売機IDを
受け取る
S706
電子コイン発行要求を作成し、
電子コイン発行サーバに送付する
S707
電子コインに割り当てるシリアル
番号を生成する
S708
シリアル番号から電子コインを
作成する
S709
発行した電子コインを携帯型端末に
送付する
S710
S711へ
S711
発行した電子コインの金額を、
携帯型端末利用者に課金する
S712
受信した電子コインを自動販売機に
送付する
S713
受信した電子コインに含まれる情報
から電子コイン検証情報を生成
S714
受信した電子コインを、
電子コイン検証情報で検証する
S715
シリアル番号が使用履歴に記載され
ているかどうかを検証する
S716
携帯型端末利用者の要求に応じて
商品を提供する
S717
利用された電子コインのシリアル
番号を使用履歴に保存する
S718
終了

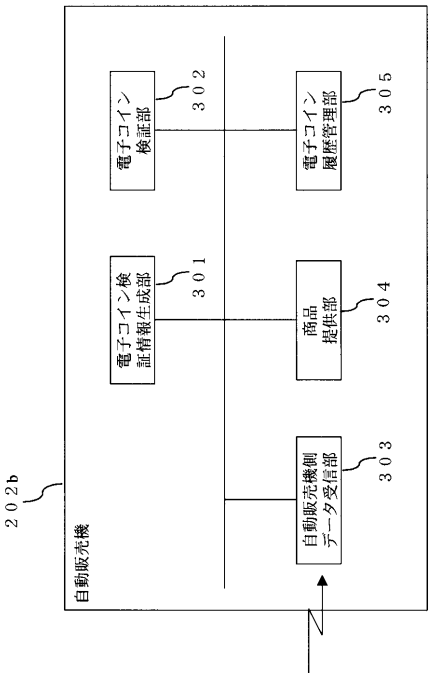
【図６】


801
802
803
電子コイン
シリアル番号
電子コイン
改竄検出情報

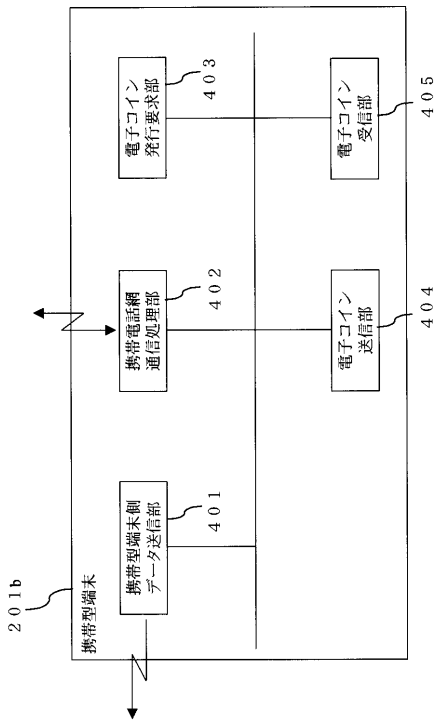
【図７】


814(803)
電子コイン
改竄検出情報
出力
813
電子コイン改竄検出情報
生成アルゴリズム(秘密の方式)
入力
811
自動販売機ID
入力
シリアル番号
812
(a)
821
秘密の鍵情報
入力
822
電子コイン改竄検出情報
生成アルゴリズム(公知の方式)
出力
823
電子コイン
改竄検証情報
811
自動販売機ID
入力
シリアル番号
812
(b)

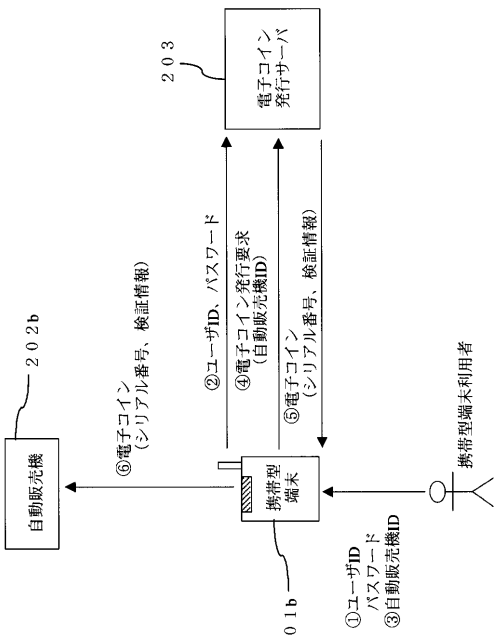
【図８】


202b
自動販売機
電子コイン検
証情報生成部
301
電子コイン
検証部
302
商品
提供部
304
電子コイン
履歴管理部
305
自動販売機側
データ受信部
303

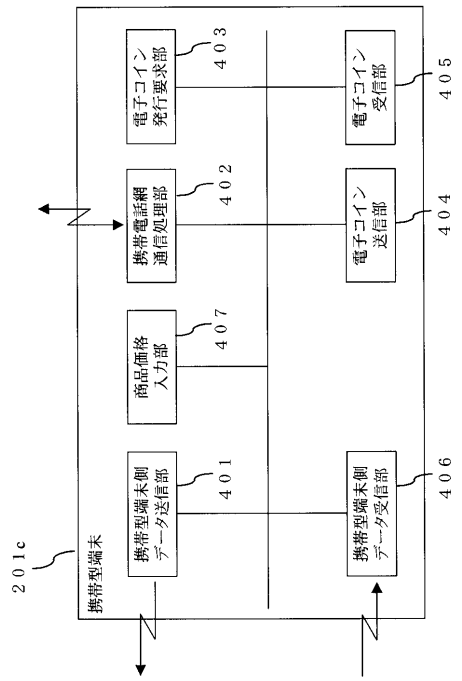
【図９】


201b
携帯型端末
携帯型端末側
データ送信部
401
携帯電話網
通信処理部
402
電子コイン
送信部
404
電子コイン
発行要求部
403
電子コイン
受信部
405

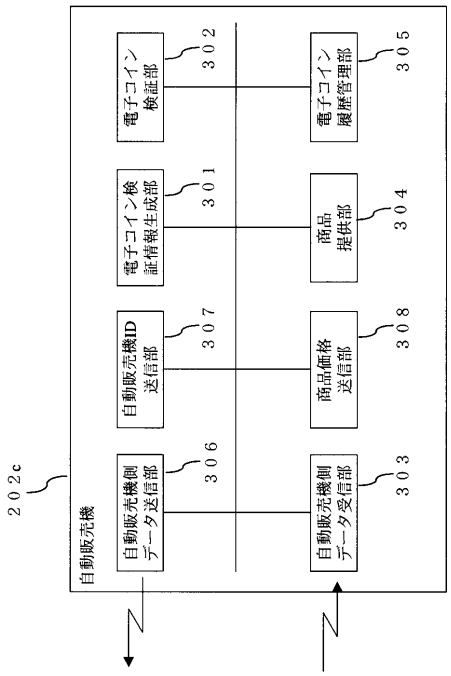
【図１０】


202b
自動販売機
⑥電子コイン
(シリアル番号、検証情報)
203
電子コイン
発行サーバ
②ユーザID、パスワード
④電子コイン発行要求
(自動販売機ID)
⑤電子コイン
(シリアル番号、検証情報)
携帯型
端末
201b
①ユーザID
パスワード
③自動販売機ID
携帯型端末利用者

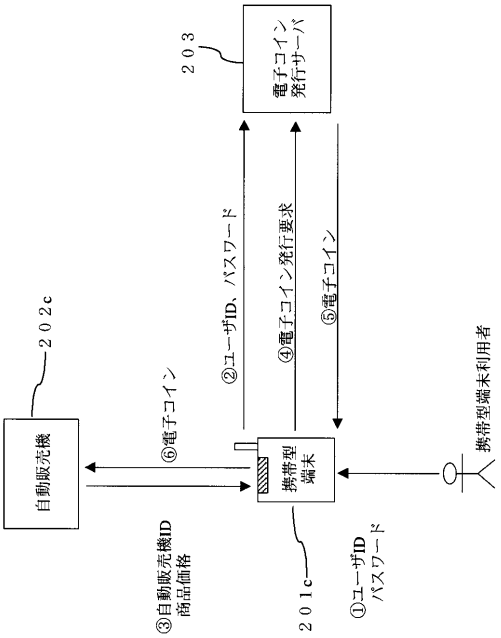
【図１１】



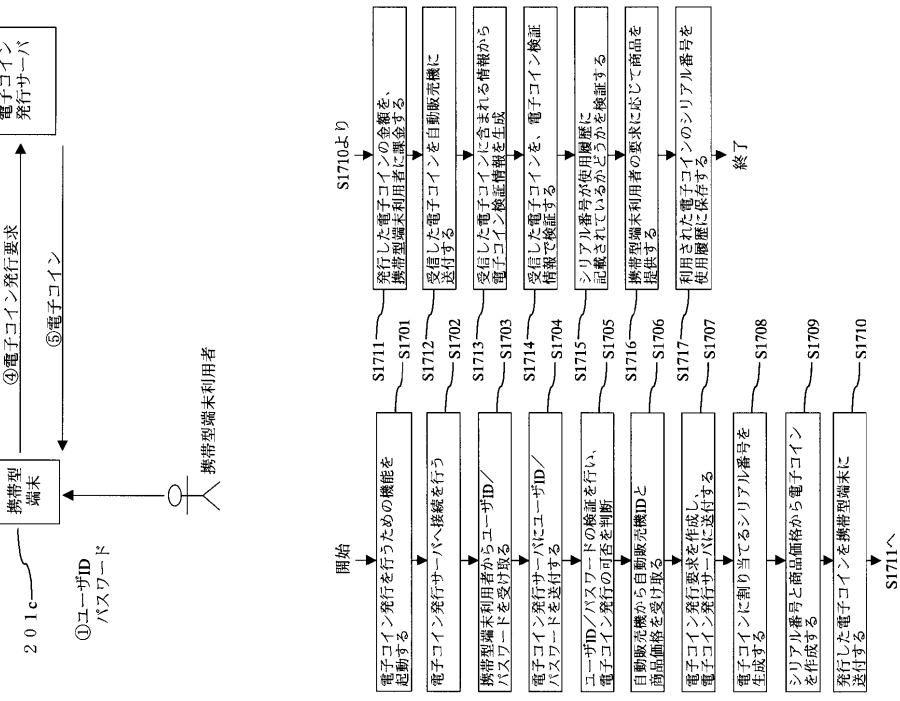
【図１２】



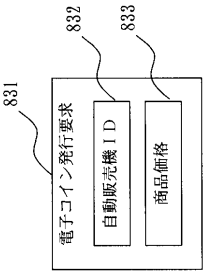
【図１３】



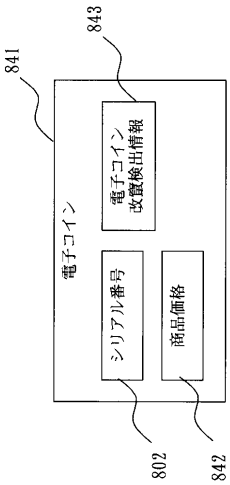
【図１４】



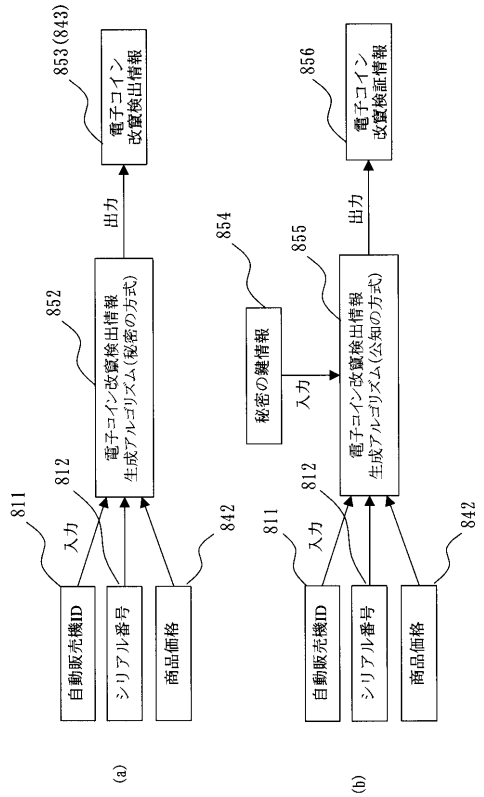
【図１５】



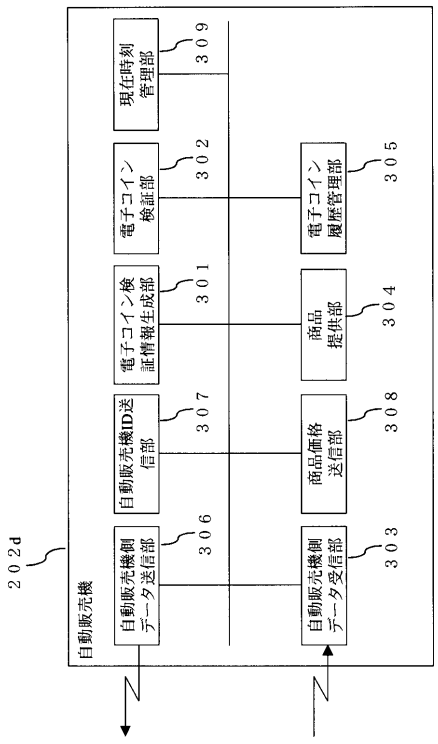
【図１６】



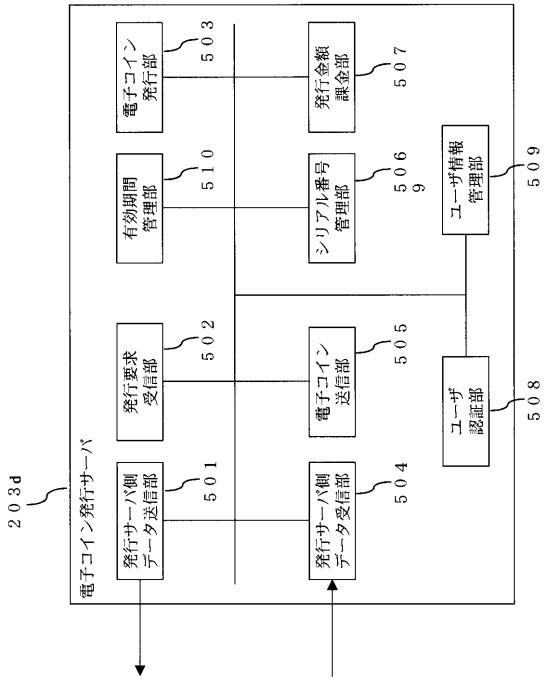
【図１７】



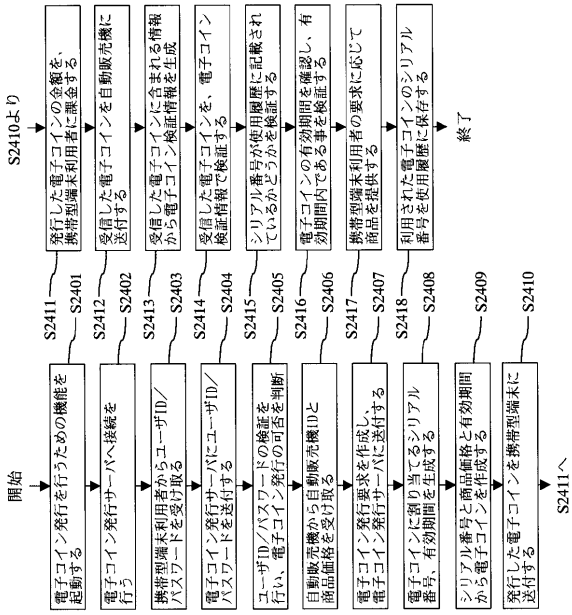
【図１８】



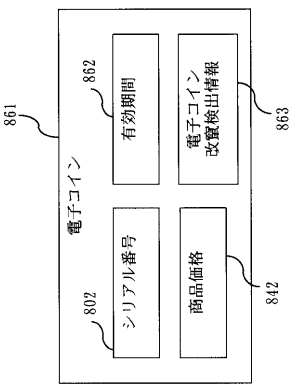
【図１９】



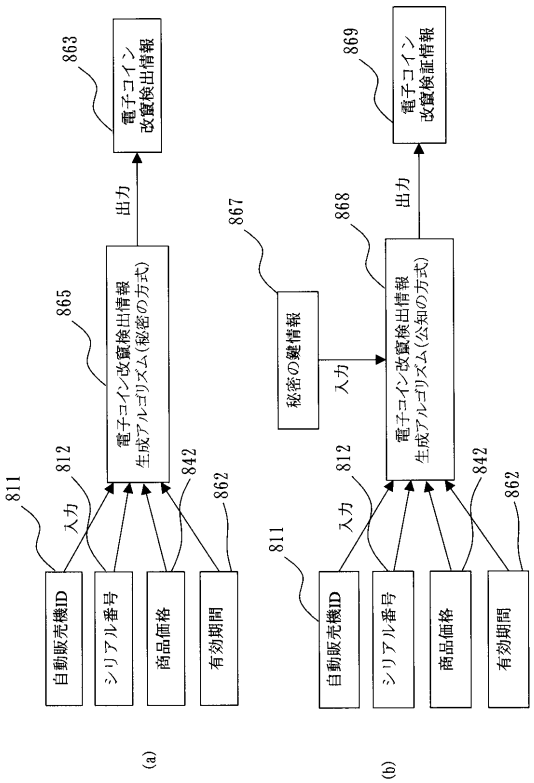
【図２０】



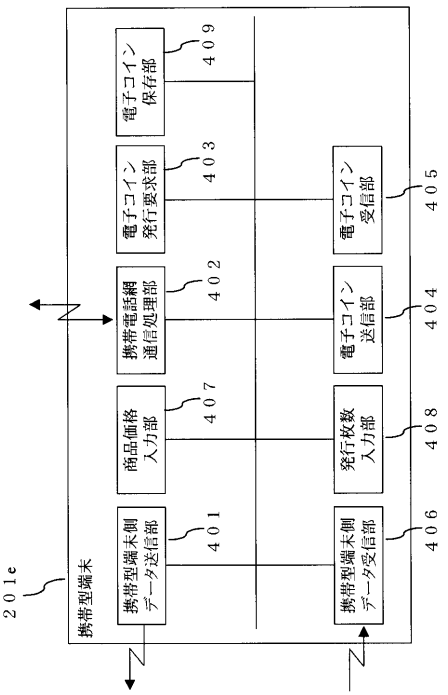
【図２１】



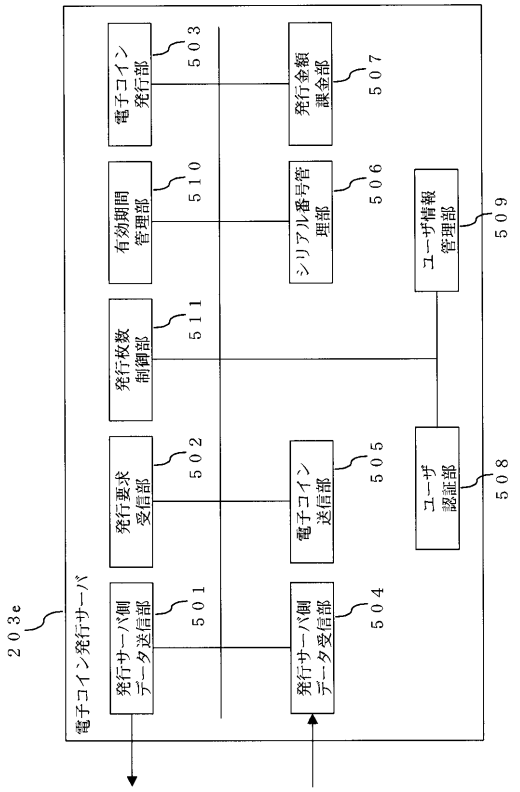
【図２２】



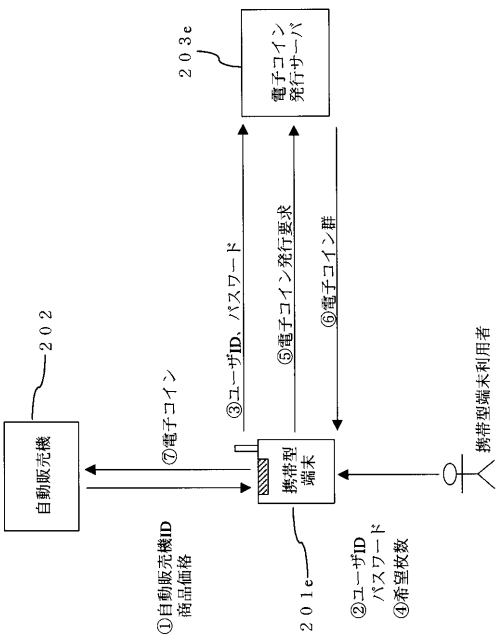
【図２３】



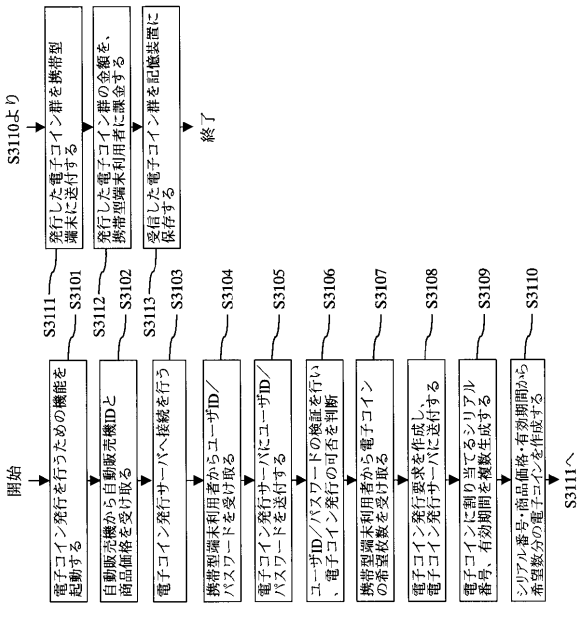
【図２４】



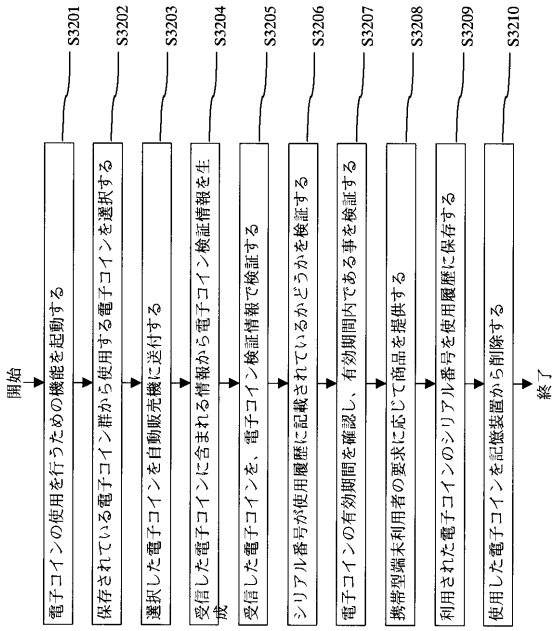
【図２５】



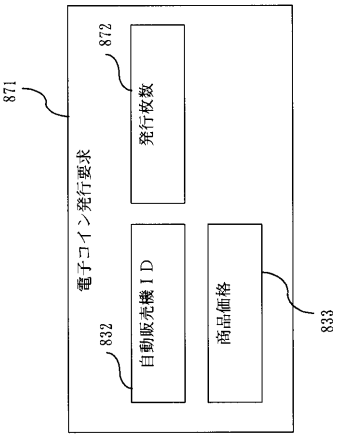
【図２６】



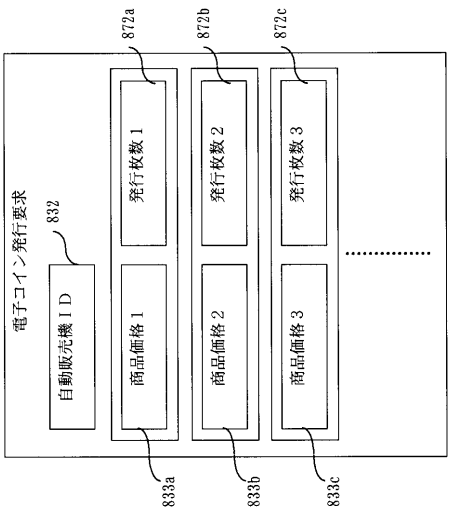
【図２７】



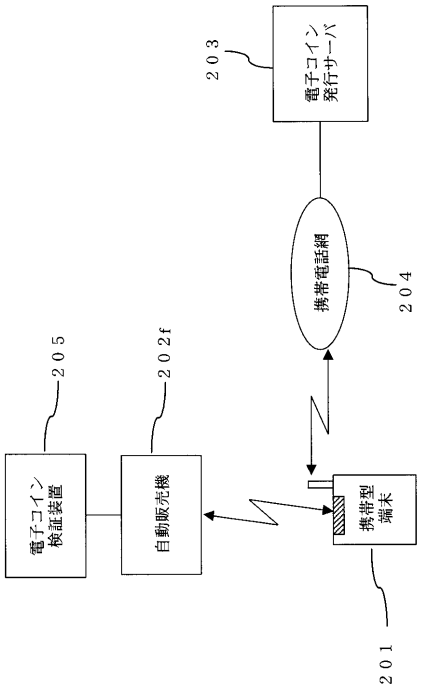
【図２８】



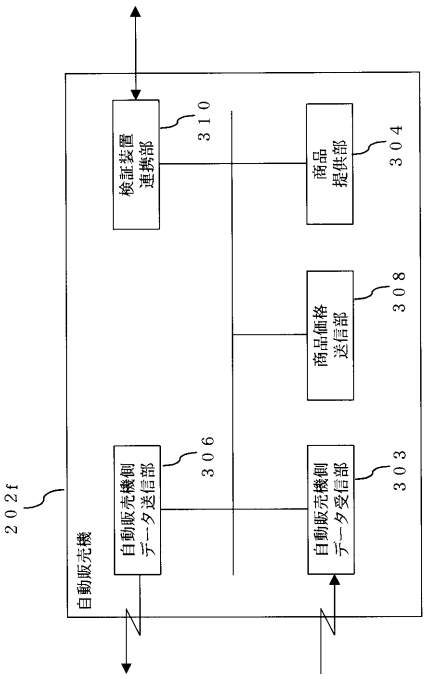
【図２９】



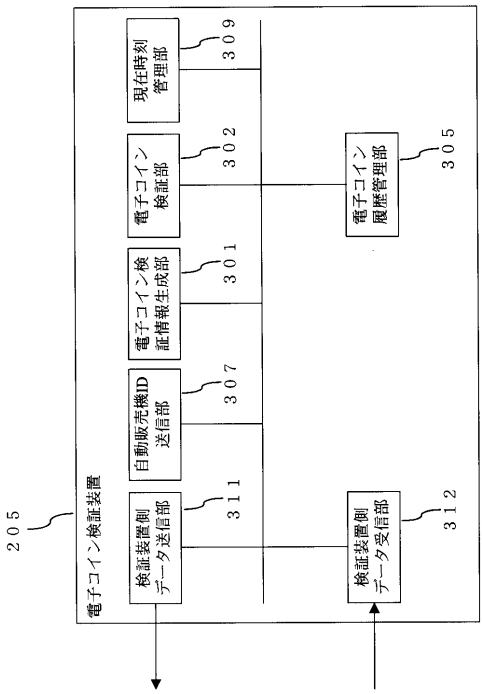
【図３０】



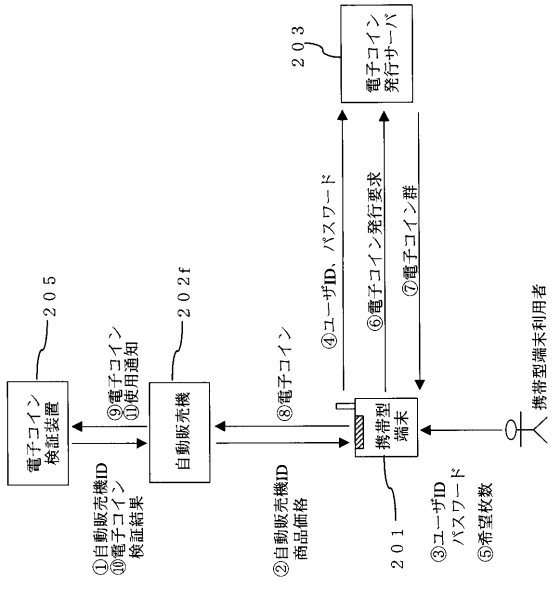
【図３１】



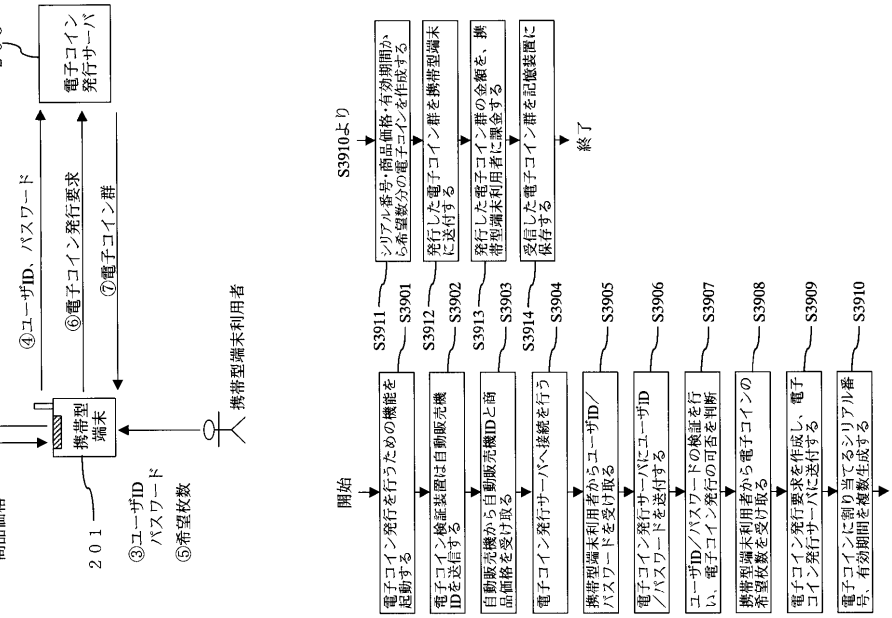
【図３２】



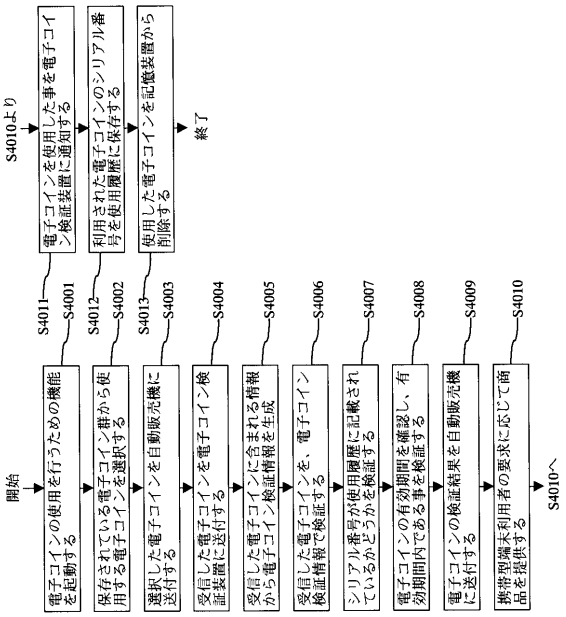
【図３３】



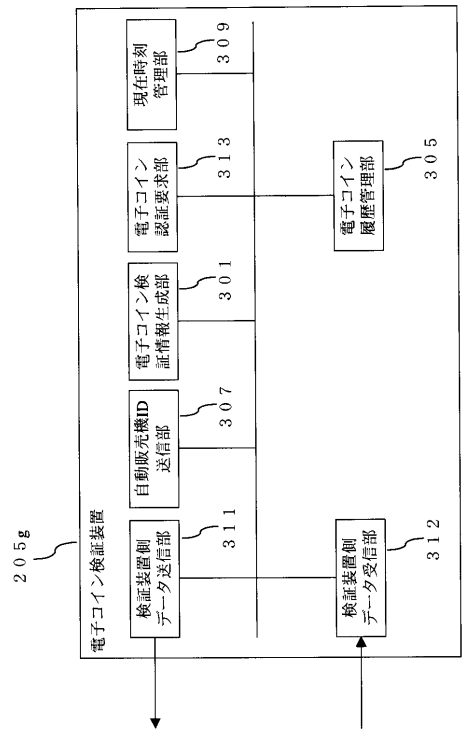
【図３４】



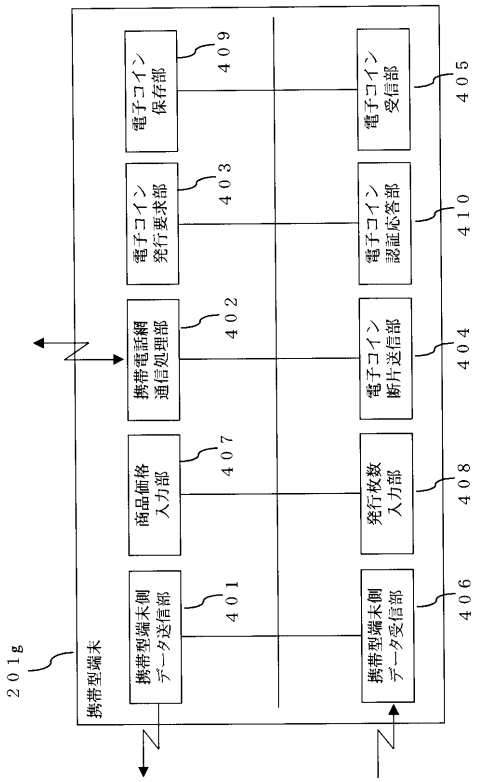
【図３５】



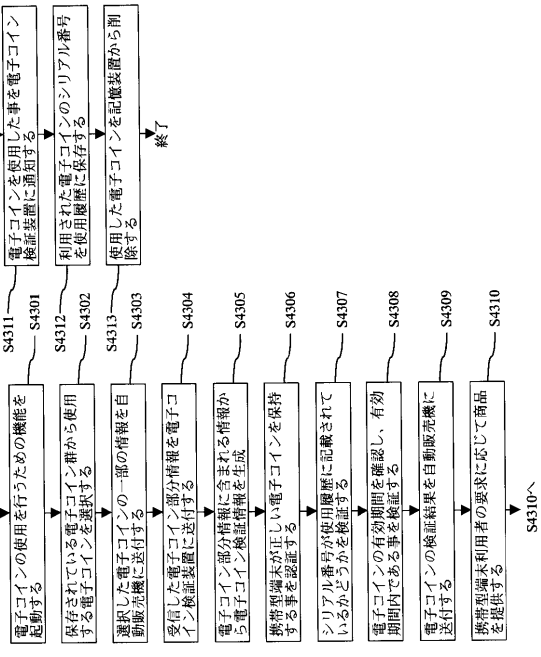
【図３６】



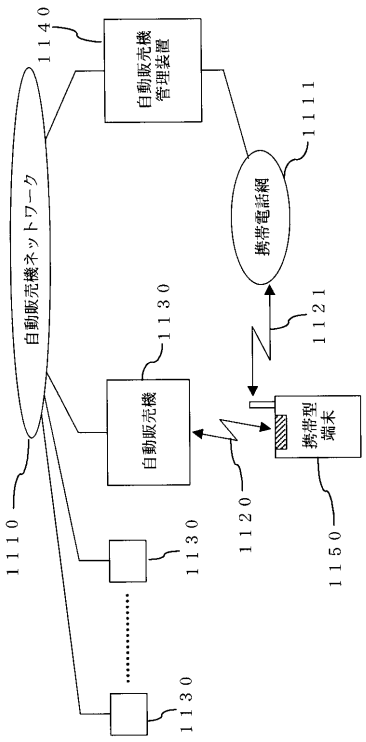
【図３７】



【図３８】



【図３９】


自動販売機ネットワーク
1110
自動販売機管理装置
1140
携帯電話網
1111
1121
自動販売機
1130
1120
携帯型端末
1150
1130
1130

フロントページの続き

(51)Int.Cl.[7]	FI		テーマコード（参考）
	Ｇ０６Ｆ 17/60	５０６	
	Ｇ０７Ｆ 7/02	Ｚ	
	Ｇ０７Ｆ 7/10		
	Ｈ０４Ｍ 15/00	Ｂ	
	Ｈ０４Ｂ 7/26	１０９Ｍ	

(72)発明者 米田 健
東京都千代田区丸の内二丁目２番３号 三菱電機株式会社内

Ｆターム(参考) 3E044 AA01 BA10 DC06 DE01
5K025 AA09 BB10 EE18 EE24 EE30 FF17 FF25 GG12 GG24
5K067 AA30 AA34 BB04 BB21 DD04 DD17 EE02 EE13 EE16 HH22
KK13 KK15