

令和5年1月18日判決言渡

令和4年（行ケ）第10013号 審決取消請求事件

口頭弁論終結日 令和4年11月8日

判 決

5

原 告 X

被 告 特 許 庁 長 官
同 指 定 代 理 人 松 田 直 也
高 瀬 勤
宮 下 誠
梶 尾 誠 哉
富 澤 美 加

10

主 文

15

- 1 原告の請求を棄却する。
- 2 訴訟費用は原告の負担とする。

事実及び理由

第1 請求

20

特許庁が不服2021-5195号事件について令和3年12月23日にした審決を取り消す。

第2 事案の概要

1 特許庁における手続の経緯等

25

- (1) 原告は、平成17年6月22日にした特許出願（特願2005-181485号）の一部を分割した特許出願（特願2010-29938号）を順次分割した特許出願（特願2014-2号、特願2014-217879号、特願2015-184536号、特願2016-203181号、特願20

18-38129号、特願2018-238015号及び特願2019-209204号)の一部を更に分割して、令和2年1月23日、発明の名称を「着信者主導による通信方法及び通信システム及び電子決済システム」とする発明について、新たに特許出願(特願2020-8794号。以下「本願」という。甲3)をした。

(2) 原告は、令和3年3月8日付けで拒絶査定(甲7)を受けたため、同年4月22日、拒絶査定不服審判(不服2021-5195号事件)を請求した。

原告は、同年5月27日付けの拒絶理由通知(甲8)を受けたため、同年8月17日付けで特許請求の範囲について手続補正(以下「本件補正」という。甲10)をした。

特許庁は、同年12月23日、「本件審判の請求は、成り立たない。」との審決(以下「本件審決」という。)をし、その謄本は、令和4年2月2日、原告に送達された。

(3) 原告は、令和4年2月24日、本件審決の取消しを求める本件訴訟を提起した。

2 特許請求の範囲の記載

本件補正後の特許請求の範囲は、請求項1ないし33からなり、その請求項1の記載は、次のとおりである(以下、請求項1に係る発明を「本願発明」という。甲10)。

【請求項1】

コンピュータによって実行される方法であって、
サービスの要求を受けるステップと、
前記要求を処理するために指示情報を使用するステップと、を含み、
前記指示情報が認証情報に基づいて設定された情報であり、
前記認証情報が物品から取得される情報であり、
前記物品が前記認証情報を利用者に提供する物品である、

方法。

3 本件審決の理由の要旨

- (1) 本件審決の理由は、別紙審決書（写し）記載のとおりである。

5 その要旨は、本願発明は、本願の出願前に頒布された刊行物である国際公開第2002/008981号（以下「引用文献1」という。甲1）に記載された発明、又は、引用文献1に記載された発明及び特開2004-303057公報（以下「引用文献2」という。甲2）に記載された事項に基づいて、当業者が容易に発明をすることができたものであり、特許法29条2項の規定により特許を受けることができないから、本願は拒絶すべきものであるというものである。

10

- (2) 本件審決が認定した引用文献1に記載された発明（以下「引用発明」という。）、本願発明と引用発明の一致点及び相違点は、次のとおりである。

ア 引用発明

15 携帯電話機1、商品提供元の店舗2、決済承認機関4が通信網5で接続され、

携帯電話機1の正面あるいは側面に機器製造番号及び携帯電話番号のバーコードが印刷された標識19、20を貼り付け、

20

利用者（商品購入者）は、自分が所持する携帯電話機1をモバイルショッピングモードに設定した後、入力手段14を使用し、商品を購入しようとしている店舗の識別情報としての店舗ID、自分の暗証番号（図7の706に登録した番号）、決済方法、商品の購入金額を入力し、決済方法には、クレジットカード決済、Webマネー決済、デビットカード決済があり、入力した情報をQR決済証明鍵発行要求として決済承認機関4の認証サーバ41に送信し、

25

認証OKとなり、与信OKである場合、認証サーバ41は、2次元コードで構成されたQR決済証明鍵を生成し、携帯電話機1に送信し、QR決

済証明鍵は、少なくとも決済番号、個人認証、氏名、決済方法の情報を含み、

5 利用者は予め選択してあった購入希望商品を店舗端末 2 2 の店員に提示し、購入希望商品の発注を行うと、利用者は Q R 決済証明鍵 1 2 0 1 が表示された状態の携帯電話機 1 を店舗端末 2 2 に付属した Q R コード読取装置 2 1 の読取部分に挿入装着し、Q R コード読取装置 2 1 が、携帯電話機 1 の表示部 1 1 に表示された Q R 決済証明鍵 1 2 0 1 を読み取ると共に、標識 1 9、2 0 から携帯電話製造番号と携帯電話番号を読み取り、その読取結果を店舗端末 2 2 に転送し、店舗端末 2 2 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び Q R 決済証明鍵 1 2 0 1 を決済承認要求として認証サーバ 4 1 に送信し、

15 認証サーバ 4 1 は、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末 2 2 から受信した Q R 決済証明鍵 1 2 0 1 の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、詳細決済承認を店舗端末 2 2 に返信し、

店舗端末 2 2 において、店員による決済ボタン操作が行われた場合は、店舗端末 2 2 は決済終了メッセージを認証サーバ 4 1 に送信し、決済終了情報を金融機関 4 2 に送信し、決済終了情報を受信した金融機関 4 2 では利用者の指定口座から代金を引き落とす手順を行う、

20 方法。

イ 本願発明と引用発明の一致点及び相違点
（一致点）

「コンピュータによって実行される方法であって、
サービスの要求を受けるステップと、
25 認証情報が物品から取得される情報であり、
前記物品が前記認証情報を利用者に提供する物品である、

方法。」である点。

(相違点 1)

本願発明は、「前記要求を処理するために指示情報を使用するステップ」を含むものであるのに対し、引用発明は、「指示情報」を含んでいるか定かではなく、このため、「前記要求を処理するために指示情報を使用するス

(相違点 2)

本願発明は、「前記指示情報が認証情報に基づいて設定された情報」であるのに対し、引用発明は、「指示情報」を含んでいるか定かではないため、「指示情報」が「携帯電話製造番号、携帯電話番号」に基づいて設定されているか不明である点。

4 取消事由

引用文献 1 を主引用例とする本願発明の進歩性の判断の誤り

第 3 当事者の主張

1 原告の主張

(1) 相違点 1 及び 2 の容易想到性の判断の誤り

本件審決は、①引用発明においては、携帯電話製造番号及び携帯電話番号は、本願発明の「認証情報」に相当するとした上で、「認証サーバ 4 1 は、利用者が選択した決済方法を認めたときに、QR 決済証明鍵を発行し、決済承認要求を受け付けると、QR 決済証明鍵の正規性を判断する点で、QR 決済証明鍵を発行したことを管理するための情報を有していることは自明の事項であり、この管理するための情報は、利用者が選択した決済方法を認証サーバ 4 1 が認めたことを示す情報であって、決済承認要求を認めることで、利用者が選択した決済方法に基づき決済が行われる点で、この情報を使った決済が行われるものといえることからすると、引用発明において、本願発明と同様の「指示情報」を有するものとすることは、当業者が適宜なし得た事項

であり、又は、引用発明において、本願発明の「指示情報」（本願明細書の発明の詳細な説明記載の「指示ファイル」の概念）が含まれないとしても、引用発明に、引用文献２記載の技術的事項（「利用者が、予め引出口座及び引き出しを希望する金額を設定するものであって、管理コンピュータ２１は、選択された現金自動預払機３０の端末識別子、取引依頼に含まれる預金口座識別子、引出希望金額、算出した取引予定時間、生成したパスワードに関するデータを含む取引条件管理データ２３０を取引条件管理データ記憶部２３に記録し、現金の引出処理段階において、利用者は、この入力欄６１１に携帯電話端末１０で受信したワンタイムパスワードを入力して、管理コンピュータ２１が取引条件管理データ２３０を抽出し、取引条件管理データ２３０に含まれるパスワードとの照合ができ、サービス要求に含まれる受付時刻が、取引条件管理データ２３０の取引予定時間内に含まれる場合、管理コンピュータ２１は取引条件に基づいて取引処理を実行すること。」）を適用することで、本願発明の「指示情報を使用する」構成とすることは、当業者が容易になし得た事項であるから、引用発明に基づき、相違点１に係る本願発明の構成とすることは、当業者が容易になし得た事項である、②ＱＲ決済証明鍵を発行したことを管理するための情報は、携帯電話製造番号及び携帯電話番号を含むＱＲ決済証明鍵発行要求に基づいて設定されているといえることから、この技術的思想に基づき、引用発明において、相違点２に係る本願発明の構成とすることは、当業者が容易になし得た事項である旨判断したが、以下のとおり、本件審決の判断は誤りである。

ア ①について

引用発明においては、「利用者（商品購入者）は、自分が所持する携帯電話機１をモバイルショッピングモードに設定した後、入力手段１４を使用し、商品を購入しようとしている店舗の識別情報としての店舗ＩＤ、自分の暗証番号（図７の７０６に登録した番号）、決済方法、商品の購入金額を

5 入力し、決済方法には、クレジットカード決済、Webマネー決済、デビットカード決済があり、入力した情報をQR決済証明鍵発行要求として決済承認機関4の認証サーバ41に送信し、認証OKとなり、与信OKである場合、認証サーバ41は、2次元コードで構成されたQR決済証明鍵を生成し、携帯電話機1に送信するものであるから、本件審決のいう引用発明の「QR決済証明鍵を発行したことを管理するための情報」は、認証情報（携帯電話製造番号及び携帯電話番号）が店舗端末22から認証サーバ41に送信される前に、認証情報に基づく認証とは無関係に生成される情報であり、本願発明の「指示情報」（「認証情報に基づいて設定された情報」）
10 といえない。

そして、引用発明において、認証情報（携帯電話製造番号及び携帯電話番号）に基づかずに生成された「QR決済証明鍵を発行したことを管理するための情報」を、本願発明の「指示情報」（「認証情報に基づいて設定された情報」）に置き換えるには、利用者端末に認証情報の読取装置が必要になり、装置の構造上の追加、変更が必要となるから、当業者が適宜なし得た事項であるとはいえない。
15

また、引用文献2には、設定された情報をファイルに保存し、利用者のサービス要求を受けた時に、そのファイルからその情報を取出して使用する技術的事項が開示されてはいるものの、引用発明において、本願発明の「指示情報」の開示がない以上、当該技術的事項から本願発明の構成とすることは、当業者が容易になし得た事項であるとはいえない。
20

したがって、相違点1に係る本願発明の構成は、引用発明又は引用発明及び引用文献2記載の技術事項に基づいて当業者が必要に応じて適宜なし得る事項であるとはいえないから、①の判断は誤りである。

25 イ ②について

②の判断は、①の判断を前提とするものであるところ、上記のとおり、

①の判断に誤りがあるから、②の判断も誤りである。

(2) 小括

5 以上のとおり、本件審決における相違点 1 及び 2 の容易想到性の判断に誤りがあるから、本願発明は、引用発明又は引用発明及び引用文献 2 記載の技術事項に基づいて、当業者が容易に発明をすることができたものであるとした本件審決の判断も、誤りである。

2 被告の主張

(1) 相違点 1 及び 2 の容易想到性の判断の誤りの主張に対し

10 ア 本願発明の「指示情報」は、本願明細書記載の「指示ファイル」の情報に対応するものであり、具体的な実施例としては、買い手の口座に対応する「指示ファイル」に設置（設定）した電子決済の「有効／無効フラグ」である（【0066】）。

15 次に、本願明細書の【0060】、【0061】、【0063】及び【0064】の記載から、本願発明の「物品」は、本願明細書記載の「識別 ID」を記録した「媒体」に対応するものであり、「電話番号」を含む「識別 ID」が、本願発明の「認証情報」に該当するものと解釈されるものであり、また、【0060】及び表 1 の記載から、「識別 ID」（認証情報）は、「用語」として列挙されている項目の一つであって、他の「通信 ID」、「銀行口座番号」、「仮想口座」等と紐づけられて設定されている情報であることを理解できる。

20 そして、本願明細書の全体をみても、「識別 ID」（認証情報）を用いて何らかの処理を行ってから、「指示情報」を設定したり、「識別 ID」自体を変更して「指示情報」を設定したりすることについての記載がないことからすると、本願発明の「指示情報が認証情報に基づいて設定された情報」とは、「指示情報」が「認証情報に紐付けられて設定された情報」とであると解釈できる。

しかるところ、引用発明では、利用者が携帯電話機 1 でクレジットカード決済、Web マネー決済、デビットカード決済の複数の決済方法の中からいずれの決済方法を有効とするか選択し、選択した決済方法を入力して認証サーバ 4 1 に送信し、認証サーバでは、選択された決済方法を含む QR 決済証明鍵を生成・発行し、その後の決済承認要求に対する処理を行っており、この処理では、「利用者が当該決済方法を有効であるとの意思表示」をしている。この「利用者が当該決済方法を有効であるとの意思表示」をしたことは、複数の決済方法のうち、いずれの決済方法が有効であるのかを判断するための情報として、決済承認要求に対する処理を行う認証サーバ 4 1 に記憶されていることは明らかであり、その情報は、利用者が選択した決済方法を認証サーバ 4 1 が認めたことを示す情報、すなわち、QR 決済証明鍵を発行したことを管理するための情報であって、QR 決済証明鍵発行要求に含まれる「携帯電話製造番号及び携帯電話番号」（本願発明の「認証情報」に相当する。）に紐付けられて設定された情報であるといえるから、本願発明の「指示情報」に対応する。

そうすると、引用発明において、相違点 2 に係る本願発明の構成（「前記指示情報が認証情報に基づいて設定された情報」である構成）とすることは、当業者が容易になし得た事項である。また、引用発明において、相違点 1 に係る本願発明の構成（「前記要求を処理するために指示情報を使用するステップ」を含む構成）とすることは、当業者が容易になし得た事項である。

したがって、本件審決における相違点 1 及び 2 の容易想到性の判断に誤りはない。

イ これに対し、原告は、本件審決のいう引用発明の「QR 決済証明鍵を発行したことを管理するための情報」は、認証情報（携帯電話製造番号及び携帯電話番号）が店舗端末 2 2 から認証サーバ 4 1 に送信される前に、認

証情報に基づく認証とは無関係に生成される情報であり、本願発明の「指示情報」（「認証情報に基づいて設定された情報」といえない旨主張する。

5 しかしながら、前記アのとおり、引用発明の「QR決済証明鍵を発行したことを管理するための情報」は、決済承認を要求する前に、QR決済証明鍵発行要求に含まれる認証情報に基づいて設定された情報であって、決済等サービスを要求する前に事前に予約して設定された情報であるから、原告の上記主張は失当である。

(2) 小括

よって、原告主張の取消事由は理由がない。

10 第4 当裁判所の判断

1 本願明細書の記載事項

本願明細書（甲3）には、次のような記載がある（下記記載中に引用する図1、69、表1については別紙1を参照）。

(1) 【技術分野】

15 【0001】

本発明は、通信網上電子装置を用いた通信に関し、特に、通信接続の確立する段階に関し、通信のセキュリティの確保に関する。着信者又は着信側通信設備を支配する当事者の意思に従って、すべての作動を決定する通信とリモート制御機能との一体化に関する。

20 【背景技術】

【0002】

電気通信は広範囲に普及した。インターネットを活用したさまざまな情報技術サービスが一般社会に急速に浸透し、高速大容量常時接続通信が一般家庭に普及し、また発信者番号通知も一般化している。現在では発信者が通信
25 の主導権を握っている。

しかしながら、着信者の意思に反する迷惑通信、発信者の身元を偽る詐欺、

青少年に悪影響を及ぼすメール、頻繁にメールの大量送信による「攻撃」、受信メールの画面を見ただけで感染してしまうウイルス、「ワン切り」不完了呼によって電気通信事業者のネットワークに障害が発生し、長時間にわたり電話回線が広範囲に麻痺するという状況が生じるなど深刻な被害が発生している。また通信インフラの麻痺及び機能の低下、正常通信の溺没、等マイナスの問題も浮上した。既存の公衆通信仕組みの弱みによる以上の不法的または合法的な行為を誘発している。

従来の迷惑通信防止技術は、各警戒レベルに分けるものが有る。しかし、多様な状況に同時に対応できるものがない。例えば、「指定拒否」は指定された相手に対して受信拒否をするが、不特定多数の相手を全部指定しきれないという問題がある。「指定受信」では指定された相手からしか受信しないが、「鎖国主義」になってしまう（例えば、特許文献 1、非特許文献 1、2 参照。）。特許文献 6 の方法では、拒否番号を登録・解除するときの利便性を高めることができる。受信者が指定する受信条件により受信拒否し、電子メール送信者側で電子メールの転送可否を判定するが、しかし、条件の決め方自体が難しい、指定しきれないという問題もある（例えば、特許文献 2、3 参照）。受信した迷惑メールに未開封を記録し送信主へ逆課金するという方法もある（例えば、特許文献 4 参照）。到着した電子メールから発信者の識別情報を抽出するものもある（例えば、特許文献 5 参照）。

【 0 0 0 3 】

しかし、これらの技術は、（a）少なくとも迷惑通信が 1 回発生した後、いかに対応する（例えば、特許文献 6 参照）、及び、オプト・アウト方式の様な法規制は、当事者個人がすべての発信者を対応することを強制され、特にメールの場合ほとんど効果がない。その理由は： 1．発信者の数が膨大である。

1 回のみの発信でも迷惑であり、一つずつに拒否返信することは現実的ではない。例え拒否登録しても登録できる件数の記憶領域が限られ、無限に増や

することはできない。前記法規制も解決できない、例えば外国語の発信内容に対していかに規制するか、発信規制の法制度がない国の存在や、違反者を起訴することは発信者が組織ではなく個人の場合、現実的ではない。2. ワン切り迷惑通信に対処できない。3. 「オレオレ詐欺」のような発信者身元を偽ることによる犯罪行為、在宅確認電話が空巣犯罪者に利用されてしまう問題に対応できない。

(b) 完璧な受信条件の設定ができない。「指定受信」技術は、重要な通信が受信されない可能性が十分に存在する。厳しい法規制、登録者に対してのみ発信を許すオプト・イン方式は、表現の自由や営業の自由を妨げる。迷惑メールの概念として、どの内容のメールが迷惑メールに当たるかは、個別の着信者側の主観的要素を抜きに決定することができない、共通の基準が存在しない。公知の迷惑メール発信者データベース等の方法によるフィルタリング等の技術は着信者側の主観をまったく反映できないうえ、発信者アドレスが絶えず変化している現状では明らかに対応できる限界がある。

【0004】

(c) 一般に、従来の通信システムは、通信当事者が互いのアイデンティティを知っているという概念に前提としている。例えば個人の電話番号が個人のアイデンティティの役割を果たしている。このため安易に電話番号を未知の相手に公表すると、何かの危険が潜むことになる。一方、ネットワーク上一般向けの個人対個人、個人対会社などの取引、交際、求職など活動において、最初又は最後まで匿名通信必要な場合、一旦相手を招待したら、自分のメールアドレスまたは電話番号が相手に開示されるため、身をひきたい時簡単に相手と関係を断ち切れない。特許文献10では、匿名通信について、2つのステップを要し、専用の匿名通信センターを通して通信内容から双方の身元情報を取り除く通信チャンネルを設立するという方法が示されている。

(d) 技術の進歩に伴い、小形携帯通信装置が多機能化している。通信設備

の付属カメラ、付属位置情報装置、などの付属機能の活用、子供、ボケ老人、無人でも安全に通信手段としても監護のためにも使える、潜在的なニーズが満足されていない。例えば位置情報の活用について、走行経路を設定する制御手段を備えるものがあるが、計算量が大きく、携帯電話など小形装置に向かない（例えば、特許文献 7、8 参照）。GPS 衛星からの電波の受信手段を備えた携帯電話に関するものもあるが、迷惑通信を防止手段がない（例えば、特許文献 9 参照）。

特許文献 19～20、27～29 では、移動装置を決済に利用する技術が示されている。しかし、決済暗証番号を安全に使えない。特許文献 30～31 では、商取引時のキャッシュレス化に関する技術が示されている。しかし、資金の流動性が損なわれる。

(2) 【発明が解決しようとする課題】

【0005】

これらはすべて通信機能および通信に関係した機能を備えた電子装置（以下通信装置という）の管理者の意思、即ち迷惑通信をはじめとする他人意思による装置の動作を防止したい、及び自分意思から装置を制御したいという意思に関するものである。従来技術の問題点はこの意思を満足できないことである。この問題点を解決し、前記当事者の意思を満足させることが本発明の目的である。具体的に、前記当事者の意思通りに安心して通信資源を効率的な活用することは本発明の目的である。通信、通信装置を制御する機能、正常的に開放的に従来の通信機能を損なうことなく迷惑通信を排除し、無駄な通信量を削減し、監護、緊急通信、匿名通信、効率的な移動機位置情報サービス、等通信装置の付属装置を活用することが本発明の目的である。経路誘導サービスを提供するとともに、専用設備を設けることなく、交通状態を把握することと、安全で便利な電子決済および移動体料金収受システムを実現することも本発明の目的である。

【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、図1に示すように、本発明は通信装置の管理者が予め通信装置とネットワークの間に介在する電子秘書に指示を出し、前記電子秘書が前記管理者の指示内容に従って、内側又は外側（通信装置又はネットワーク）から到着する通信要求に対して、複数の処置する方法を備え、前記通信要求を受けた時、前記複数の処置する方法から一つを選び出して、前記通信要求を処置する；本明細書中に前記処置する方法を「待遇」といい、管理者により決める特定の通信要求に対する特定の処置をする方法を意味する。

従来概念の通信は発信者主導が普通であり、例えば相手に電話をかけると相手が受けることが当然と考えられてきた。応答方法も単純であるため、特別な用語で記述する必要がない。本発明は応答方法が多様に成っていて、簡潔に表現する適当な技術用語が存在しない。そのため「待遇」という言葉を使い、当事者双方の関係を表現する。

受信拒否待遇は発信者を完全拒否するという意思表示であり、通信許可待遇は従来の通信ニーズであり、制御許可待遇は潜在的なニーズ、発信者に通信装置の制御をあげたいという意思表示である。

本明細書中に使用する用語「制御許可」は、通信設備は被制御状態になり、発信者の命令を実行し、又は、指定される機能やプログラムを起動できるようにするという管理者の意思を表す。例えば、発信者が遠隔から通信装置付属のカメラを起動し着信側を監視でき、電子決済の確認を求める通信要求を受けた場合、本人認証プログラムが起動される。

本発明の思想は全ての発信者の通信が事前許可を得てから始まる。未知の発信者が許可なしに発信してきた場合、まず発信者の名前を尋ね、発信者身分を判断し、通信するか否かを決定する。これを申請受理という。この流れ

は受付や秘書の例にたとえることができる。所定のルールを事前に秘書に指示し、秘書は指示された訪問者が来た場合、指示された扱い方で応接し、知られない訪問者が来た場合、氏名や、用件を尋ね、上司に教えられたルールに基づき、訪問者を通させるか否かを決定する。例えば上司が来訪者の用件に興味があつたら通させる。上司の古い知り合いと判明したら通させる。賢い秘書なら訪問者を覚え、二回目の訪問者を親切に扱うか、門前払いするかをすぐに決められるだろう。

【発明の効果】

【0008】

(a) 迷惑メール、迷惑電話の防止。本発明最大の特徴は、迷惑通信が発生する前にその発生が論理上1回でも許されることなく阻止される。1. 発信者IDと着信者IDの対が合わないとは通信が許さない。たとえ発信者IDを偽造できても、受信者IDの対と合うようにすることはできない。発信者番号通知など、発信者IDが偽造できない場合、未知の発信者に限られる回数の申し込みの機会を与え、以後は無条件に拒否することで、プログラムによる自動的な迷惑通信の試みを阻止できる。2. ワン切り電話を行おうとする者に対し、自動的に申し込みの手順が始まり、送信者側に通信料金の課金が始まるため、制裁を与えることができる。3. 登録されなかった相手に対し決められた手順で自動確認されるので、老人などが不注意に騙される「オレオレ詐欺」にも対処できる。

(b) 同時に、着信者の質問を正確に答える相手の場合、例えば着信者の名前を回答できる場合、ほぼ従来と同様の正常的に開放的に通信機能をほぼ損なうことはない。発信者側の自由が制限されることはない。物を売りたい、宣伝する場合、相手が興味ある場合だけ、双方の利益になる。本発明は着信側に予め興味を声明する手段を備え、双方の利益になる通信を拒否しない。

(c) 本発明を受信サーバで運用する場合、迷惑通信の通信要求を発信す

る時点でそれを阻止できる。公衆網に大量の無駄なメールによる通信量の削減、設備の有効利用、通信会社の迷惑通信補償金の節約ができる。受信サーバで運用しなくても、通信契約の変更、法の整備実行のための社会的負担を減らし、迷惑メールの手動判断、削除処理時間の節約ができる。迷惑通信を排除することで、結果的に通信手段の活用が拡大する。

(d) 簡単な匿名通信、片側だけが発信を許す片道通信ができる。交際、求人求職活動などをより安心に、気楽に公衆通信網を介して行えるようになる。

(e) 当事者の一人一人の主観意識に合わせて自動的に相手を識別し、万一自動処理の問題で相手が不正な通信許可を入手しても、その許可を取消せる。

(f) 着信側通信機械の支配者の意思通りに安心して通信装置、通信付属装置を効率的に活用できる。監護、防犯、緊急通信、及び車両用走行誘導機能の一体化が実現できる。このため、新しい使い道、新しいニーズが生まれる。その他、各実施例別に課題、手段、効果を記述する。

(3) 【0010】

メール関係用語概念説明。メールの送信の流れは、一般に発信者端末（送信クライアント）から送信メールサーバ（受信サーバ）、送信メールサーバ（送信クライアント）から受信サーバ、受信サーバから着信者端末（受信クライアント）までである。送信メールサーバは、受信サーバと、送信クライアントの二つ役割を持つ。以下、本発明の実施の形態について図面を用いて説明する。

図1は本発明の一実施形態の概略構成例を示す図である。当事者端末101が電子秘書102を介在して網104における通信を行い、電子秘書は、当事者端末側又は通信サービスを提供するサーバ側に、電話通信の場合は、電話機側又は交換機側に組み込んでも良い。サーバ側に組み込む場合、通信

チャンネルを通して当事者端末とつなげる。指示ファイル103は電子秘書に組み込み又は電子秘書と独立しても良い。管理者が直接に指示ファイルにデータを入力しても良い(図に示さず)。指示ファイルはデータ記憶装置の中に保存される。本発明の目的を達成して得る記憶装置であれば、例えば磁気記憶装置、RAM、ROMなどの電子メモリ回路の他に、光学記憶媒体などを採用することができる。指示ファイルの望ましい実装は、マルチメディア情報を含め、相互に関連するデータを整理・統合し、検索しやすいデータベースである。

(4) 【実施例6】

【0059】

実施形態、電子決済システム。

図69は電子決済に関する方法及びシステムを示すブロック図である。

〔分野〕 商取引時のキャッシュレス化を可能とするシステムに関する。特に、携帯電話などの通信端末を利用して即時に決済を行うことができる電子決済サーバ、電子決済システム、電子決済方法及びプログラムに関する。

〔背景〕 クレジットカード、デビットカード(キャッシュカードで買物)決済システムがある。インターネットビジネス(eビジネス)、携帯やPHSなどの携帯型通信機器を対象としたサービスも多く存在する。しかしながら、カードデータが簡単に盗まれる。デビットカードで買物時暗証番号の入力が不安全であり、暗証番号が指の動きから容易に盗まれる。端末に細工がなされていた場合や、回線が傍受されていた場合には、口座からお金を引き出すための情報が容易に盗まれる。このため偽造キャッシュカードと盗まれる暗証番号による被害が発生している。特許文献30、31は高額被害が発生しない専用口座を開設する技術を開示している。しかしながら普通口座と専用口座の間入出金作業が必要であり、普通口座資金の流動性が損なわれる。

〔課題〕 利便性と高額被害が発生しない安全性、資金の流動性を備えた決

済方法・システムである。

【0060】

〔手段〕電子決済を促進するために、任意のタイプの金融機関又は決済センター（以下「銀行」ともいう）口座（例えばデビットカード、クレジットカード）所有者（以下「買い手」ともいう）と売り手（図 69, 6902）の間の商決済を処理する電子決済システムおよび方法において、買い手（図 69, 6901）は

5 予定する買物を電子決済で支払するために、電子決済を予約する予約情報（図 69, A）を、銀行（図 69, 6903）に送信し、識別 I D（図 69, B）を使用して、商品（図 69, G）を購入する。

10 表 1 は、予約情報及びデータ、操作情報の簡単な実例を示している。

【0061】

この明細書で用いられる用語については、次のように定義する。

「通信 I D」とは、決済要求を買い手に確認する時の通信先を意味する。例えば、携帯電話番号、コンピュータ通信アドレス、等がこれに該当する。

15 「識別 I D」とは、買い手銀行口座と関連付けられた利用者識別子を意味する。例えば、電話番号、車両識別番号、等がこれに該当する。

「仮想口座」とは、予定する支払先に支払をするため想定 of 口座を意味する。例えば、鉄道、高速道路、現金自動預入支払機（A T M）出金、買物、インターネット商店、等特定売り手、機関、或は売り手グループに支払をするため想定 of 口座がこれに該当する。

20

「残高上限額」とは、仮想口座の残高を指定する値を意味する。予約する事により仮想口座の残高を残高上限額にセットする。

「確認不要限度額」とは、確認を省略しても良い支払上限額を意味する。

「確認不要累積限度額」とは、必ず確認を行う基準額を意味する。確認の省略は累積方式であり、確認を省略した支払額の累積額が前記基準額を超える場合（以下「累積超過」という）に、確認を行い、前記累積額をゼロにセッ

25

トして再び累積をする。

「残高通知額」とは、残高が少なくなり、予約する方が良いと思う額を意味する。

5 「自動回復日数」とは、自動的に残高を残高上限額まで回復する最短経過日数を意味する。

「決済予約確認要否」とは、識別 I D 媒体所持者が有料区域の入場口を通過する時に、退場口で発生する決済請求を利用者に予約するか否かを指定するフラグを意味する。

【 0 0 6 2 】

10 「確認情報」とは、決済要求の確認ために使用する情報を意味する。仮想口座の暗証番号に相当する。

表 1 に以上用語で示す情報と残高通知先と暗証番号は予約情報である。

「残高」とは、仮想口座の残高を意味する。

15 「通信確認」とは、備えられる制御許可待遇の 1 種類の待遇を意味する。待遇 I D は図 7 0 参照。

「操作情報」とは、通信確認待遇により起動される認証プログラムに入力する情報を意味する。

表 1 に仮想口座に使わない決済予約確認要否フラグを「-」で示す。

20 売り手は、利用金額の決済を要求する決済要求(図 69, C)を生成し、前記決済要求を承認するために、銀行に送信する。銀行は、前記決済要求に含まれる売り手識別子等から仮想口座を特定し、残高及び銀行口座残高(以下「総残高」という)は足りる場合、銀行は、買い手に前記決済要求を確認するために、確認要求(図 69, D)を買い手に提示する。買い手は、確認情報(図 69, E)を銀行に提示して前記決済要求を確認する。銀行は、買い手によって確認された後

25 のみ、承認(図 69, F)を売り手に送信し、決済を行う。

仮想口座は業種コード、売り手名、商品種類等買い手による指定の方法で

特定する。銀行は売り手識別子等入手可能な情報を買手に提供し、仮想口座との関連付けを選択させる。

本発明の決済処理に関するデータ構造等は、公知技術、例えば、特許文献27～29を参照する。

5 仮想口座は、従来技術の専用口座、保留預金（口座残高全体から自由に引出できない枠）、及びプリペイドカードと異なり、銀行口座から総残高を自由に引出できる。図73は、口座所有者が開設している銀行口座と予約している仮想口座の残高を模式的に示している。仮想口座の残高は総残高を越える場合も有りえる。決済可能金額が残高と総残高の両方以下である。仮想口座
10 は決済の安全性を保ちながら、資金の流動性を維持する効果が有る。複数の専用口座に入金し過ぎる場合、他の用途で資金を簡単に使えない不便がない。

【0063】

前記確認要求は請求原因と金額を含め、決済要求の確認を買手に求める。

銀行は速やかに処理することが要求される。銀行の役を果たす売り手自前の決済センターを運営しても良い。
15

任意の情報通信手段を利用できる。電話、メール、インターネット、など本実施形態目的を達成できる手段であれば良い。ネットワークに常時接続する通信手段を利用しても良い。例えば、モバイルインターネットWeb、又は、チャットライクな双方向通信(chat-like interaction)を通してても良い。

20 買手は発信して銀行から確認要求を取得しても良い。電子秘書は内側から到着する通信要求を解析して、決済要求を確認するための通信要求に対して、通信確認待遇を実施する。例えば、銀行の電子決済用電話番号への発信、又はURLで識別された電子決済のサービスを提供するWebページへのアクセスが検出される場合は認証プログラムが起動される。

25 予約情報に、確認基準を含めても良い。銀行は、予約情報に含まれる確認基準が前記決済要求に含まれるデータによって満たされる場合、確認要求と

確認情報の送受信を省略して決済要求を承認しても良い。前記確認基準の例は、制限はされないが、売り手識別子、支払限度額、決済日、決済時刻、又はそれらの組み合わせ、又は買い手が便利に感じるかもしれない他の基準を含んでいる。

5 銀行は、売り手通信モジュール、例えば、レジ端末を通じて決済要求を買い手に確認しても良い。確認要求を売買双方の装置に送信することを選択しても良い。又は、メールで確認を要求し、W e b で確認をしても良い。

 識別 I D 記録媒体は、売り手装置に合わせる任意の手段を使用しても良い。例えばバーコードを携帯のディスプレイに表示する。磁気カード、I D タグ、
10 I C カード、赤外線等近距離通信手段を使っても良い。識別 I D を売り手装置に手入力しても良い。更に、使用履歴、残高、総残高等を店の装置に表示やレシートに印刷する事を選択しても良い。

【 0 0 6 4 】

 識別 I D を記録した媒体を複製して家族等に使用させることができる。例えば、
15 子供がコンビニエンでジュースを買い、支払いのために識別 I D を記録したバーコードを貼っているカードを店員に提示し、親が自宅で携帯により決済要求を確認する事ができる。前記媒体が意思外に複製されたり落したり場合は、不正使用が容易に発見できるので、それを廃止すれば良い。

 利用者の取引銀行口座からすべての出金を確認に利用できる。例えば、A T M から現金を引出す場合、A T M を売り手 (図 69, 6902) とみなせばよい。利用者は口座番号又は一意な I D を磁気カード等媒体を通じて A T M に入力し、金額を入力し、銀行は利用者 (買い手) 通信モジュールを通じて引出したことを確認された後にのみ出金する。A T M で従来キャッシュカードの認証を加えて通信確認を行っても良い。

25 更に、銀行は取引毎に取引コードを生成して携帯に転送し、近距離通信手段を用いて、前記取引コードを A T M に入力して照合し、指紋で認証プログラ

ムを操作することにより、本人しか取引できないようにすることができる。
残高は仮想口座から電子決済による支払限度額であり、決済は決済金額を残
高から引き落とす。残高不足の場合、決済要求を否認する。残高の範囲内金
額は暗証番号と異なる確認情報で使える。残高は識別 I D と確認情報と買い
手通信装置が同時に盗まれる場合の最大損失額である。

確認不要限度額を超える支払いの試みを即座に所有者に通知し確認する。確
認不要限度額は、識別 I D だけで使える現金感覚の額である。決済要求を拒
否する場合は、確認情報を無効にして仮想口座を凍結しても良い。

確認を省略にした支払い金額を累積額に累積し、確認不要累積限度額を超
えようとする決済要求が発生する時、必ず確認を行い、その後、累積額をゼ
ロにリセットしてから累積する。まとまった額の支払を確認できる。確認不
要累積限度額は、識別 I D と確認情報が同時に盗まれる場合の最大損失額で
ある。

【 0 0 6 5 】

残高が残高通知額以下に減少した時、その旨を指定の残高通知先に送信する。
更に、一定の条件を満たす時、自動的に残高を残高上限額まで回復する（自
動回復）。例えば、前回予約又は自動回復してから、自動回復日数を経過して
いた条件を満たす場合、自動回復が行われる。

確認情報は、暗証番号等認証情報と性質が異なる。決済の重要度と使用環境
に合わせて使用することが可能である。前記仮想口座を公衆環境で支払いに
使う場合、暗証番号と異なる確認情報を使う方が良い。A T M コーナー等安
全に入力できる環境用仮想口座の確認情報は暗証番号と同じコードを使っ
ても良い。

用語「通信確認」とは、到着する通信要求に対して、着信音や振動等で所持
者の注意を喚起し、情報を受信して視覚又は聴覚的に提示し、認証プログラ
ムを自動的に起動することを含む。前記認証プログラムは入力される操作情

報を基に、登録した操作情報と照合し、一致する場合にのみ、予め登録された登録情報を外側（銀行）に送信する処理を含む。前記操作情報は、簡単なボタン操作、承認コード、音声、パスワード、指紋等人間の身体的特徴（生体情報）からなる群から選択されるものを含む。

5 前記登録情報として確認情報を使用する。

必要に応じ、図70に示す様な複数の通信確認待遇を備えることができる。

予約は識別ID又は口座番号と暗証番号に基づいて、インターネット又は電話又は銀行窓口等で行う。窓口しか予約できないようにしても良い。

【0066】

10 好ましくは、前記暗証番号（認証情報）は使い捨てパスワード（OTP）を使用する。毎回の通信が異なるパスワードを使うので、通信傍受被害が防げる。例えば、認証プログラムにOTPを実現する機能を備える。一時的に公衆電話でも予約が可能であり、回線盗聴被害を予防するために一日あたりの利用限度額を設定しても良い。更に確認情報はOTPを使用しても良い。

15 好ましくは、本人認証を経て電子決済を有効（決済を承認できる状態）にする。例えば、指示ファイルにアクセスし銀行に通信確認待遇を与える。又は、指示ファイルに電子決済の有効／無効フラグを設置し、フラグが無効にセットされる場合は、通信確認待遇が通信を拒否する。

20 前記本人認証は、通信装置付属の本人認証手段を利用するものであり、買い手は予め装置に本人識別情報を登録して置き、本人認証手段が起動されると、装置が操作者に前記本人識別情報を入力するように促し、入力した情報と登録した本人識別情報と照合し、照合結果が一致した（認証成功）場合、次の操作を許す。前記本人識別情報は、指紋等生体情報、或いはパスワード等を含む。

25 好ましくは、電子決済を有効にしてから、所定の時間、例えば、4時間を経過すると電子決済を無効（決済を承認できない状態）にする。

[効果]

最大限の安全度を望む場合、買物に出かける前に、残高を予定使用額に、確認不要限度額をゼロに、通信先を携帯電話番号に予約し、指紋で確認操作する。

5 通信先を店側に、識別 I D、確認情報を覚えるものに予約し、店で識別 I D、確認情報を手入力することにより記憶だけで支払できる。

【0067】

日常の支払時には、入力操作及び通信中に暗証番号を使わない。予約する時は暗証番号を安全に使えば良い。日常は暗証番号を全く使わない事もできる。
10 口座から用途別のお金の流出速度を自在に制御でき、流出速度以上のカード偽造の高額被害の可能性がなく、計画した流出速度範囲内の場合、自動回復により予約する手間もなく、家計の計画性が高まる。

詳細説明

使われる従来技術（通信ソフト、コマンド送信、プログラムの実行、I C
15 カード、O T P 等）の詳細は省略する。

図 7 0、図 7 1 は本発明電子決済機能を有する移動電話機一実施例の T D B、R 1 D B を示す。構成を示すブロック図基本的に図 2 6 と同じである。前記 R 1 D B は図 2 B に示すものの実施例である。説明しやすいため、発信番号を利用する。実施例 4 のように、インターネット常時接続、パケット通信など通信手段を利用することもでき、発信者をメールアドレスなど I D による識別することもできる。
20

図 7 4 は、図 7 3 に示す仮想口座模式図における取引処理の流れ図である。図 7 5 は、図 7 4 に示す承認処理の流れ図である。

次は仮想口座「買物」の予約を説明する。通信 I D「090-1234-5678、商店」、
25 識別 I D「045-1234-5678」、確認情報「456」、と他の表 1 に示す予約情報が送信される。表 1 に示す確認情報及び買い手指紋を指示ファイル記憶する。

通信 I D は、確認要求が携帯と商店の端末双方に送信されことを意味する。
前記携帯の裏側に、識別 I D として自宅電話番号を記録したバーコードを
貼っておく。

【 0 0 6 8 】

5 売り手は、レジ端末等のバーコードリーダーにより識別 I D を読み取って、
識別 I D と売り手口座番号と商店名と請求金額（A）等を銀行に送信して決
済を要求する（図 74, 7401）。買い手が携帯を忘れた場合は自宅番号をレジ端
末に手入力する。

10 銀行は識別 I D から口座番号を検索し、例えば最初の支払額 A は 500 円
であり、総残高（B）は 200,000 円である場合には、B は足りるため処理を
続き（7402, YES）、特定の仮想口座を特定できない場合、買物口座を選択する
（7403）。A は残高 100,000 円を超えない（7404, YES）、承認処理（7405）が
行われ、確認不要限度額 1,000 円を超えない（図 75, 7501）ため、銀行は確
認を省略し、直ぐに決済要求を承認し、確認を省略した支払の金額 500 円を
15 累積額（C）に累積し（図 75, 7502）、C は 500 円となり、A を口座から引
落し、売り手の口座に移転することとなり、同時に A を仮想口座から引落し、
新たな総残高は $200,000 - 500 = 199,500$ 円、残高は $100,000 - 500 = 99,500$ 円
となる（7407）。

20 2 回目の買物の支払額 A は 600 円である場合には、C に累積すると C は
1,100 円となり、確認不要累積限度額を超える（7503, YES）ため、銀行は識
別 I D から携帯番号を検索し、決済要求を確認するため携帯に発信し、同時
に、確認要求をレジ端末にも表示する（7504）。買い手はレジに確認情報「456」
を入力して、又は、携帯に起動された認証プログラムに指紋センサーを通し
て指紋を入力して、決済要求を確認する。確認情報が間違った等決済要求が
25 確認されない場合（7505, N0）、取引を拒否する（7406）。確認された場合、取
引を承認し、累積超過の場合、累積額 C を 0 円にセットされ（7506）、新た

な総残高は $200,000-1,100=198,900$ 円、残高は $100,000-1,100=98,900$ 円となる。

2 相違点 1 及び 2 の容易想到性の判断の誤り

(1) 引用文献 1 の記載事項

5 引用文献 1（甲 1）には、次のような記載がある（下記記載中に引用する図 1 ないし 4、7、9 ないし 13 については別紙 2 を参照）。

ア 「技術分野

本発明は、携帯電話機等のネットワークに接続可能な端末を用いてスーパーマーケット等の各種の店舗、インターネットのサーバ上に開設されている電子店舗、あるいは飲料水等の自動販売機で購入する商品の代金の決済
10 を行う商取引方法及び装置並びにシステムに関するものである。

背景技術

携帯電話機に WWW 閲覧機能（W o r l d W i d e W e b）を付加したことにより、携帯電話機を使用してインターネットにアクセスし、各種の情報、物品、役務サービスを閲覧し、必要に応じて、それらの情報、物品、役務サービスの提供を注文するという取引形態が急速に拡大している。こ
15 こで、本発明では、形状を有しない音楽ソフトなどの情報（コンテンツ）、形状を有する物品、宅配サービス、介護サービスなどの役務サービスを全て商取引の対象となる商品と定義する。この場合、公共機関が提供する無料の介護サービスもあるが、無料であっても取引の対象となる商品に含む
20 ものとする。

しかし、携帯電話機を使用して商品の発注を行ったとしても、その決済方法としては、銀行振込みや現金の送付、商品到着時の代金引換などの従来の商慣習に従った方法が踏襲されている。

25 最近では、このような旧来方法に代えて、商品の注文と同時に、クレジットカード番号を商品提供元（店舗）に通知し、クレジットカード会社を通

じて決済する方法が実施されている。

しかし、この決済方法は、クレジットカード会社と本人だけが知るべき番号あるいは情報が外部に漏れないことを前提にしており、外部に漏れた場合には悪用される危険性がある。

5 そこで、2001年5月から開始される次世代移動通信サービスでは、携帯電話機にUIM（User Identity Module）と呼ばれるICカードを搭載し、このICカード内の暗号プログラムによりクレジットカード番号等の秘密データを暗号化し、決済を行うという方法が考えられている。

10 しかし、暗号プログラムにより暗号化して保存したとしても、携帯電話機自体を紛失した場合には、不正な第三者に解読されてしまい、悪用される危険性がある。特に、ICカード内にはクレジットカード番号のみでなく、銀行口座番号や保険証番号、電子マネーなどの他の秘密データも同時に保存する形態が多くなると考えられるので、不正な第三者に解読された
15 場合の危険性は旧来の決済方法よりも高くなるという問題がある。

また、非接触型ICカード同様、無線を利用したネットワークは特に有線ネットワーク以上に不正アクセスを含むハッキング等、情報が外部に漏れる可能性が高くなるという問題がある。

20 また、不正な店舗の出現により、店舗での決済時に秘密データが盗聴され、悪用される危険性がある。

また、携帯電話機自体のコストも上昇し、さらに電力消費も増加し、電池寿命が短くなるという問題がある。

25 本発明はこのような問題を解決するためになされたものであり、その目的は、クレジットカード番号等の秘密データを本人認証機関やクレジットカード会社以外に開示することなく本人認証を行い、安全に購入商品の決済を行うことができる商取引方法及び装置、並びにシステムを提供することにあ

る。」（１頁５行～３頁１行）

イ 「図１は、本発明の商取引方法を実施するシステムの全体構成の実施形態を示すシステム構成図であり、商品購入者が使用するネットワーク端末としての携帯電話機１、商品提供元の店舗２、飲料水等の自動販売機３、
5 決済承認機関４で構成され、これらが通信網５で接続されている。通信網５は、無線回線と有線回線及びインターネット網を含むものである。ここで、ネットワーク端末とは、インターネット等のネットワークに接続可能な端末を示すものであり、以下の例に示す携帯電話機１の他、ＰＨＳ、ＰＤＡ、パーソナルコンピュータ、デジタルテレビ等、種々のものが含まれる。

10 携帯電話機１は、インターネット網に接続可能な機能を有する市販の携帯電話機であり、図２（ａ）の概略ブロック図に示すように、表示部１１、無線送受信部１２、制御部１３、入力部１４、送受話器１５、メモリ１６、外部入出力インタフェース１７を備えている。表示部１１にはインターネット接続モードにおいて、図２（ｂ）に示すように、ニュース、モバイルバン
15 キング、カード／証券／保険、モバイルショッピングなどのインターネット接続メニューが表示されるようになっている。」（１１頁２１行～１２頁１０行）

「本実施形態の携帯電話機１には、図３（ａ），（ｂ）の正面図及び側面図に示すように、機器製造番号を図３（ｃ）のようなバーコード３１で記録した第１の標識１９と、携帯電話番号をバーコード３１で記録した第２の
20 標識２０が貼り付けられている。

これらの標識１９，２０のバーコードは、図４（ａ）に示すように、所定波長 λ_a の照射光に対し記録情報を所定波長 λ_a または λ_b の反射光により出射する結晶粉末を混入した印刷材料で印刷されている。この結晶
25 粉末は、米国ＳＵＮＳＴＯＮＥ社が提供しているものであり、医薬品や紙幣の真贋識別用に採用されているものである。この場合、用途及び使用シ

システムに応じて、照射光の波長と出射光の波長が異なるように特性が調整されている。

本発明では、このような特殊な結晶粉末を混入した記録インクまたはトナーで機器製造番号及び携帯電話番号のバーコードを標識 19, 20 に印刷し、これを携帯電話機 1 の正面あるいは側面に貼り付け、その標識 19, 20 に記録されたバーコードを所定波長 λ_a の照射光で読み取るようにしている。

このような特殊な記録インクまたはトナーで記録した機器製造番号及び携帯電話番号の標識 19, 20 を携帯電話機 1 に貼り付けておくことにより、予め定めた波長の照射光以外では機器製造番号及び携帯電話番号を読み取ることができない。よって、機器製造番号及び携帯電話番号を決済承認機関 4 に事前登録しておくことにより、当該携帯電話機 1 が本システムでの商取引を利用できる正当な機器であるか否かを識別することができる。また、側面の標識 20 は、携帯電話機 1 の改造を防止できる役目を果たしている。」(13 頁 11 行～14 頁 8 行)

ウ 「標識 19, 20 のバーコードは、図 4 (b) に示すような断面構成の読取装置 40 内に挿入され、予め定めた波長の照射光を照射することによって読み取られる。この読取装置 40 は、店舗 2 や自動販売機 3 に設置される。

一方、表示部 11 には図 3 (d) に示すようなコードキャラクタ情報画像としての 2 次元コード 32 で構成された決済承認鍵情報が表示される。この 2 次元コード 32 は、日本自動車工業会及び日本文具協会の標準コードに設定されているものである。これについては、例えば特開平 10-214317 号公報等で開示されているので、ここでの詳細な説明は省略する。

この 2 次元コード (以下、QR コードと言う) を用いれば、携帯電話機

1 の表示部の面積内で約 7 0 0 0 文字（数字）をコード化して記録することができる。本発明では、この QR コードを決済承認鍵の情報を表現するために使用している。詳しくは、QR コードで構成された決済承認鍵の情報を携帯電話機 1 に転送して図 3（a）のように表示部 1 1 に表示させ、この表示状態の携帯電話機 1 を標識 1 9，2 0 の読取共用の読取装置 2 1 に挿入し、決済承認鍵の情報を読み取るようにしている。」（1 4 頁 1 2 行～1 5 頁 2 行）

「図 1 に戻り、店舗 2 には標識 1 9，2 0 と QR コードの読取共用の読取装置 2 1 が設置され、読み取った標識 1 9，2 0 と QR コードを POS 端末で構成される店舗端末 2 2 に入力し、店舗端末で代金の決済を行うようになっている。自動販売機 3 にも標識 1 9，2 0 と QR コードの読取共用の読取装置 3 3 が設置されている。」（1 5 頁 1 4 行～1 8 行）

エ 「一方、承認機関 4 は、認証サーバ 4 1 と金融機関（銀行またはクレジット会社） 4 2、店舗情報データベース（DB） 4 3，利用者情報データベース（DB） 4 4、購入履歴データベース（DB） 4 5 を備えている。

認証サーバ 4 1 は、携帯電話機 1 からの本人認証及び店舗認証要求に対して、本人認証及び店舗認証さらには金融機関 4 2 に対する与信照会を行い、予め登録してある本人および店舗であり、しかも金融機関 4 2 から与信 OK の回答があった場合には商品の代金決裁を携帯電話機 1 を使用して許可する処理を行うものであり、店舗登録処理プログラム 4 1 0、利用者登録処理プログラム 4 1 1、購入履歴管理プログラム 4 1 2、不正利用管理プログラム 4 1 3、認証処理プログラム 4 1 4、QR 決済鍵生成プログラム 4 1 5、送受信プログラム 4 1 6 を備えている。なお、各データベース 4 3、4 4、4 5 のデータを暗号化して保存するための暗号化／複合化プログラムが必要に応じて組み込まれる。また、QR コードを暗号化して送信するための暗号化プログラムおよび復号するための復号プログラム

が組み込まれる。QRコードを暗号化することにより、不正な取引をさらに困難にすることができる。」（15頁19行～16頁9行）

「認証処理プログラム414は、携帯電話機1からの本人認証及び店舗認証要求に対して、本人認証及び店舗認証さらには金融機関42に対する与信照会を行い、予め登録してある本人および店舗であり、しかも金融機関42から与信OKの回答があった場合には商品の代金決済を携帯電話機1を使用して許可する処理を行うものである。

QR決済鍵生成プログラム415は、商品の代金決済を許可するために、QRコードで構成された決済証明鍵の情報を生成して携帯電話機1に渡すプログラムである。QRコードで構成された決済証明鍵の情報（以下、QR決済証明鍵情報）は、店舗が購入者本人及び店舗の認証結果を含む詳細な決済承認の情報を認証サーバ41から受け取るための鍵となる情報であり、本システムでこのQR決済証明鍵情報を店舗の読取装置21で読み取り、その読み取ったQR決済証明鍵情報を店舗端末から認証サーバ41に送信することにより、店舗端末22では購入者本人及び店舗の認証結果を含む詳細な決済承認の情報を受け取ることができる。この場合、読取装置21で読み取ったQR決済証明鍵情報が認証サーバ41で生成したものと異なる場合には決済承認の情報を取得することができない。」（16頁24行～17頁14行）

オ 「図7は、利用者情報DBの登録情報の一例を示す図であり、利用者ID701、利用者名702、住所703、携帯電話製造番号（機器製造番号）704、携帯電話番号705、本システムを利用する際の暗証番号706、性別707、生年月日708、デビットカード番号709、クレジットカード番号710、Webマネー口座番号711、個人特徴情報712が登録されるようになっている。」（17頁20行～25行）

カ 「図10及び図11は、スーパーマーケット等の一般の店舗で携帯電話

機 1 を利用した商品購入時の決裁方法を示すフローチャートである。

まず、利用者（商品購入者）は、自分が所持する携帯電話機 1 をモバイルショッピングモードに設定した後、入力手段 1 4 を使用し、商品を購入しようとしている店舗の識別情報としての店舗 I D，自分の暗証番号（図 7 の 7 0 6 に登録した番号）、決裁方法、商品の購入金額を入力する（ステップ 1 0 0 1）。ここで、店舗又は商品の識別情報を、店舗内に設置されている発信機等から外部入出力インタフェース 1 7 を介して取り込むようにしてもよい。

また、決裁方法については、クレジットカード決裁、Web マネー決裁、デビットカード決裁があるが、クレジットカード決裁を選択した場合については支払い回数とクレジットカード番号を入力する。また、Web マネー決裁を選択した場合には Web マネー口座番号（図 7 の 7 1 1 に登録した番号）を入力する。同様に、デビットカード決裁を選択した場合にはデビットカード番号（図 7 の 7 0 9 に登録した番号）を入力する。なお、以下のフローチャートでは人間が行う操作はステップ 1 0 0 1 のように 2 重枠線で囲む形式で表記している。

入力が終了したならば、送信操作を行う。すると、ステップ 1 0 0 1 で入力した情報が QR 決裁証明鍵発行要求として認証サーバ 4 1 に送信される。

この QR 決裁証明鍵発行要求を受信した認証サーバ 4 1 は、店舗及び利用者の認証処理を行う（ステップ 1 0 0 2）。すなわち、QR 決裁証明鍵発行要求の中に含まれる店舗 I D によって店舗情報 DB 4 3 を検索し、当該店舗 I D の店舗が登録されているか否かを調べる。同様に、暗証番号、クレジットカード番号（または Web マネー口座番号、デビットカード番号）によって利用者情報 DB 4 4 を検索し、当該暗証番号及びクレジットカード番号（または Web マネー口座番号、デビットカード番号）の利用者が

利用者情報DB 4 4に登録されているか否かを調べる。その結果、店舗IDが登録されていなかった場合は、不正店舗であるか、未登録の店舗であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ1 0 0 3）。また、暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）が登録されていなかった場合も、不正利用者であるか、未登録の利用者であるので、取引不可のメッセージを携帯電話機1に返信する（ステップ1 0 0 3）。携帯電話機1では、取引不可のメッセージが表示部1 1に表示されると共に、ステップ1 0 0 1で入力した店舗ID等の情報が自動消去される。

しかし、店舗ID及び暗証番号及びクレジットカード番号（またはWebマネー口座番号、デビットカード番号）が正しく登録されていた場合には、正規登録の店舗であり、かつ正規登録の利用者であるものと認証し、認証OKとする。

認証OKとなった場合には、認証サーバ4 1は金融機関4 2に対して利用限度額あるいは残高の与信照会を送信する。そして、金融機関4 2における与信処理（ステップ1 0 0 4）によって与信OKまたは与信NGの与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたはQR決裁証明鍵を生成する（ステップ1 0 0 5）。すなわち、与信NGの与信結果が返送されてきた場合には、認証サーバ4 1は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機1に送信する。しかし、与信OKであった場合には、図3（d）で示したような2次元コードで構成されたQR決裁証明鍵を生成し（ステップ1 0 0 6）、これを携帯電話機1に送信する。このQR決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。」（19頁5行～21頁3行）

キ 「携帯電話機1では、受信したQR決裁証明鍵を図12（a）に符号1

201で示すように表示部11に表示する。同時に、例えば「この携帯電話機で決裁できます。代金決裁時に読取装置に挿入して下さい。」といったメッセージが表示される。

5 そこで、利用者は予め選択してあった購入希望商品を店舗端末22の店員に提示し、購入希望商品の発注を行う（ステップ1007）。店員は店舗端末によって購入希望商品の代金を入力する（ステップ1008）。

10 これと並行して、利用者はQR決裁証明鍵1201が表示された状態の携帯電話機1を店舗端末22に付属したQRコード読取装置21の読取部分に挿入装着する（ステップ1009）。すると、QRコード読取装置21は、携帯電話機1の表示部11に表示されたQR決裁証明鍵1201を読み取ると共に（ステップ1011）、標識19, 20から携帯電話製造番号と携帯電話番号を読み取り（ステップ1010）、その読取結果を店舗端末22に転送する。

15 店舗端末22は、携帯電話機1から読み取った携帯電話製造番号、携帯電話番号及びQR決裁証明鍵1201を決裁承認要求として認証サーバ41に送信する。この場合、QR決裁証明鍵1201については、認証サーバ自身が発行したものであることが分かればよいので、決裁番号及び個人認証といった一部の情報のみを送信してもよい。図11では、決裁番号及び個人認証の情報のみを決裁承認要求の中に含ませて送信していることを示している。」（21頁4行～24行）

20 ク 「認証サーバ41は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報DB44の登録内容と照合して調べる（ステップ1012）。この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図9）に登録した後（ステップ1013）、不正利用メッセージを店舗端末22および携帯電話機

1 に送信する。

不正利用メッセージを受信した携帯電話機 1 では、不正利用メッセージ自体が QR 決裁証明鍵 1 2 0 1 の消去コマンドとして機能し、表示部 1 1 に表示されていた QR 決裁証明鍵 1 2 0 1 が消去される。

5 店舗端末 2 2 では、不正利用メッセージを受けたことにより、表示部に不正利用者であることが表示され、処理が終了される（ステップ 1 0 1 4）。そして、店員により代金決裁ができない旨が利用者に口頭で通知される。

しかし、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末 2 2 から受信した QR 決裁証明鍵 1 2 0 1 の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、
10 認証サーバ 4 1 は詳細決裁承認を店舗端末 2 2 に返信する。この詳細決裁承認の情報には、QR 決裁証明鍵 1 2 0 1 と同様の情報の他に、当該利用者の購入履歴の情報や利用者本人の写真などの個人特徴情報が含まれている。」（2 1 頁 2 5 行～2 2 頁 1 9 行）

15 ケ 「詳細決裁承認の情報の全部または一部を利用者情報として表示部に表示する（ステップ 1 0 1 5）。図 1 2（b）にその例を示している。店員は、その表示内容と購入希望商品の内容及び代金を見て、利用者本人に購入意思を確認する（ステップ 1 0 1 6）。

本人の購入意思の確定応答があったならば、決裁ボタン操作によって決裁を完了する（ステップ 1 0 1 7）。決裁ボタン操作が行われた場合は、店舗端末 2 2 は決裁終了メッセージを認証サーバ 4 1 に送信する。この決裁終了メッセージを受信した認証サーバ 4 1 は利用者の購入履歴情報を更新する（ステップ 1 0 1 8）。この後、確認用の決裁内容を携帯電話機 1 に送信する。また、決裁終了情報を金融機関 4 2 に送信する。これにより、
20 携帯電話機 1 の表示部 1 1 には、図 1 3 に示すような確認用の決裁内容 1 3 0 1 が表示される。この決裁内容 1 3 0 1 は、利用者自身が消去するま

で保存することができる。ただし、QR決裁証明鍵1301は1回限り有効であるので、所定時間後に自動的に消去される。

また、決裁終了情報を受信した金融機関42では利用者の指定口座から代金を引き落とす手続を行う。

5 以上により、携帯電話機1を使用して一般店舗での商品購入時の決裁を行うことができる。なお、利用者が購入意思を撤回した場合に、店舗端末でのキャンセル操作によって店舗端末の処理は終了する。また、利用者自身が携帯電話機1でキャンセル操作を行った場合にも、決裁処理は途中で終了し、QR決裁証明鍵1301等の情報は全て消去される。

10 以上の説明から明らかなように、本取引方法によれば、店舗側に利用者のクレジット番号等の秘密情報を伝えることなく、認証サーバ41が発行したQR決裁証明鍵のみで代金決裁を行うことができる。また、携帯電話機1内にクレジットカード番号等の秘密情報を全く保持しない構成であるので、万一、携帯電話機1を紛失したとしても、代金決裁に悪用される危険性は全く生じない。さらに、特殊な結晶粉末を混入して記録した標識によって携帯電話製造番号と電話番号の正当性を判定しているため、携帯電話機自身の改造による悪用を防止することができ、決済に使用される機器のセキュリティ性を高めることにより、利用者および店舗の双方に有益な効果を発揮する。」（22頁20行～23頁25行）

20 コ 「なお、QR決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成されるものとしたが、決裁番号、個人認証、氏名の一部または全部を元に生成した1回限りのパスワードであってもよい。

25 この場合には、例えば、認証サーバ41と携帯電話機1とに、同一ロジックによるパスワード生成プログラムを備え、2回目にアクセスするときは、1回目に送信された暗証番号等に基づき自動生成されたパスワードを携

携帯電話機 1 から自動送信し、認証サーバ 4 1 側では、当該携帯電話機 1 の携帯電話番号等及び自動送信されたパスワードと、前記認証サーバ 4 1 で自動生成されたパスワードとを比較することにより、認証を行う。

5 3 回目以降は、前回自動生成されたパスワードに基づき新たなパスワードを自動生成、自動送信することとしてもよい。

このような、いわゆるワンタイムパスワードと呼ばれるものを用いることにより、セキュリティ性を高めることができるとともに、2 回目以降のアクセス時に、暗証番号の入力を省略することができる。」(2 4 頁 1 7 行～2 5 頁 6 行)

10 (2) 相違点 1 及び 2 の容易想到性について

ア 本件審決認定の引用発明、一致点、相違点 1 及び 2 については、当事者間に争いが無い。

15 なお、本件審決は、一致点の認定に際し、引用発明は、「利用者は予め選択してあった購入希望商品を店舗端末 2 2 の店員に提示し、購入希望商品の発注を行うと」、「店舗端末 2 2 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び QR 決済証明鍵 1 2 0 1 を決済承認要求として認証サーバ 4 1 に送信」することから、この「決済承認要求」は、本願発明の「サービスの要求」に相当し、このとき、引用発明の「購入希望商品の発注」は、本願発明の「サービス」に相当すると認定したところ、
20 引用発明の「決済承認要求」が「サービスの要求」に相当するというのであれば、要求の対象となる「サービス」に相当するのは、「決済承認」と理解するのが自然であるから、引用発明において本願発明の「サービス」に相当するのは、「購入希望商品の発注に係る決済承認」と解すべきであり、
25 この点において、本件審決の上記認定は適切ではない。また、本件審決は、引用発明の「携帯電話製造番号、携帯電話番号」は、本願発明の「認証情報」に相当するとした上で、引用発明は、「携帯電話機 1 の正面あるいは側

面に機器製造番号及び携帯電話番号のバーコードが印刷された標識 19, 20 を貼り付け」るものであって、機器製造番号及び携帯電話番号をバーコードとして印刷した「標識 19, 20」は、本願発明の「物品」に相当し、引用発明において、「標識 19, 20」にバーコードとして印刷された機器製造番号及び携帯電話番号は、店舗端末 22 が読み取る点で、本願発明の「前記認証情報が物品から取得される情報」に相当する旨認定したところ、「物品」とは、一般に、「しなもの。もの。不動産以外の有体物。」（広辞苑第七版）を意味するが、バーコードとして印刷した「標識 19, 20」は、目印又は図形であって、「しなもの」や「有体物」とはいえず、「標識 19, 20」が印刷された「携帯電話機 1」を「物品」と解すべきであるから、この点において、本件審決の上記認定は適切ではない。もっとも、このように本件審決の認定には適切でない部分を含むが、一致点の認定自体には誤りがない。

イ 本願発明の特許請求の範囲の請求項 1 の記載は、
「コンピュータによって実行される方法であって、
サービスの要求を受けるステップと、
前記要求を処理するために指示情報を使用するステップと、を含み、
前記指示情報が認証情報に基づいて設定された情報であり、
前記認証情報が物品から取得される情報であり、
前記物品が前記認証情報を利用者に提供する物品である、
方法。」というものである。

上記記載によれば、本願発明は、サービスの要求を受けるステップと、前記要求を処理するために「指示情報」を使用するステップと、を含むコンピュータによって実行される方法であり、本願発明の「指示情報」は、コンピュータがサービスの要求を処理するために使用する情報であって、利用者に提供する、物品から取得される認証情報に基づいて設定された情

報であると解される。

そして、本願明細書には、本願発明の「指示情報」について定義した記載はもとより、「指示情報」の用語を明示的に用いた記載はなく、「指示情報」を特定の情報に限定する記載や特定の場所に保存された情報に限定する記載もないことに鑑みると、本願発明の「指示情報」は、上記のとおり、
5 解釈するのが相当である。

なお、本件審決は、本願明細書の【0006】、【0010】、【0062】及び【0066】の記載から、本願発明の「指示情報」は、発明の詳細な説明の「指示ファイル」の情報に対応するものと解釈できる、実施例6では、(a)「買い手」が予め「銀行」に対して、買い手の口座に対応する指示ファイルに電子決済の有効／無効フラグを設置し、(b)売り手は、利用金額の決済を要求する決済要求を銀行に送信し、銀行は指示ファイルの有効／無効フラグが有効の場合(買い手によって確認された後)、承認を売り手に送信し、決済を行うものである、このとき、(b)の処理が「指示情報」
10 を「使用する」ことを意味すると解釈できると判断したが、本件審決の上記説示においては、「指示ファイル」の「電子決済の有効／無効フラグ」に係る情報が、「利用者」に提供する、いかなる「物品」から取得された「認証情報」に基づいて設定されたのか、その論証・あてはめが不十分であり
15 (【0063】には、「前記暗証番号(認証情報)は使い捨てパスワード(OTP)を使用する。」との記載があるが、本願明細書には、OTPがどのように生成され、どのように提供されたのかについての記載はない。)、また、本願発明の特許請求の範囲の記載及び本願明細書の記載に照らすと、本願発明の「指示情報」を実施例6の「指示ファイル」の情報の態様のものに限定すべき理由はないから、本件審決の上記説示は、この点において、相
20 当とはいえない。
25

ウ 引用例1には、一般の店舗で携帯電話1を利用した商品購入時の決済方

法（図１０及び１１）に関し、①「図１は、本発明の商取引方法を実施するシステムの全体構成の実施形態を示すシステム構成図であり、商品購入者が使用するネットワーク端末としての携帯電話機１、商品提供元の店舗２、…決済承認機関４で構成され、これらが通信網５で接続されている。」

（前記（１）イ）、「承認機関４は、認証サーバ４１と金融機関（銀行またはクレジット会社）４２、店舗情報データベース（ＤＢ）４３、利用者情報データベース（ＤＢ）４４、購入履歴データベース（ＤＢ）４５を備えている。」

（同エ）、②「利用者（商品購入者）は、自分が所持する携帯電話機１をモバイルショッピングモードに設定した後、入力手段１４を使用し、商品を購入しようとしている店舗の識別情報としての店舗ＩＤ、自分の暗証番号

（図７の７０６に登録した番号）、決済方法、商品の購入金額を入力する（ステップ１００１）。」、「決済方法については、クレジットカード決済、

Ｗｅｂマネー決済、デビットカード決済がある」、「入力が終了したならば、送信操作を行う。すると、ステップ１００１で入力した情報がＱＲ決済証明鍵発行要求として認証サーバ４１に送信される。」、「このＱＲ決済証明

鍵発行要求を受信した認証サーバ４１は…ＱＲ決済証明鍵発行要求の中に含まれる店舗ＩＤによって店舗情報ＤＢ４３を検索し、当該店舗ＩＤの店舗が登録されているか否かを調べる。同様に、暗証番号、クレジットカード番号（またはＷｅｂマネー口座番号、デビットカード番号）によって利

用者情報ＤＢ４４を検索し、当該暗証番号及びクレジットカード番号（またはＷｅｂマネー口座番号、デビットカード番号）の利用者が利用者情報

ＤＢ４４に登録されているか否かを調べる。その結果、…店舗ＩＤ及び暗証番号及びクレジットカード番号（またはＷｅｂマネー口座番号、デビットカード番号）が正しく登録されていた場合には、正規登録の店舗であり、

かつ正規登録の利用者であるものと認証し、認証ＯＫとする。」、「認証ＯＫとなった場合には、認証サーバ４１は金融機関４２に対して利用限度額あ

るいは残高の与信照会を送信する。そして、金融機関 4 2 における与信処理（ステップ 1 0 0 4）によって与信 OK または与信 NG の与信結果が返信されたならば、その与信結果に応じて、取引不可メッセージまたは QR 決裁証明鍵を生成する（ステップ 1 0 0 5）。すなわち、与信 NG の与信結果が返送されてきた場合には、認証サーバ 4 1 は、残高不足等のメッセージを含む取引不可メッセージを携帯電話機 1 に送信する。しかし、与信 OK であった場合には、図 3（d）で示したような 2 次元コードで構成された QR 決裁証明鍵を生成し（ステップ 1 0 0 6）、これを携帯電話機 1 に送信する。この QR 決裁証明鍵は、少なくとも決裁番号、個人認証、氏名、決裁方法の情報を含むもので構成される。」（以上、同カ）、③「携帯電話機 1 では、受信した QR 決裁証明鍵を図 1 2（a）に符号 1 2 0 1 で示すように表示部 1 1 に表示する。…そこで、利用者は予め選択してあった購入希望商品を店舗端末 2 2 の店員に提示し、購入希望商品の発注を行う（ステップ 1 0 0 7）。店員は店舗端末によって購入希望商品の代金を入力する（ステップ 1 0 0 8）。」、「これと並行して、利用者は QR 決裁証明鍵 1 2 0 1 が表示された状態の携帯電話機 1 を店舗端末 2 2 に付属した QR コード読取装置 2 1 の読取部分に挿入装着する（ステップ 1 0 0 9）。すると、QR コード読取装置 2 1 は、携帯電話機 1 の表示部 1 1 に表示された QR 決裁証明鍵 1 2 0 1 を読み取ると共に（ステップ 1 0 1 1）、標識 1 9、2 0 から携帯電話製造番号と携帯電話番号を読み取り（ステップ 1 0 1 0）、その読取結果を店舗端末 2 2 に転送する。」、「店舗端末 2 2 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び QR 決裁証明鍵 1 2 0 1 を決裁承認要求として認証サーバ 4 1 に送信する。」（以上、同キ）、④「認証サーバ 4 1 は、決裁承認要求を受信したならば、まず、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 DB 4 4 の登録内容と照合して調べる（ステップ 1 0 1 2）。この結果、いずれか一方

の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベース（図 9）に登録した後（ステップ 1013）、不正利用メッセージを店舗端末 22 および携帯電話機 1 に送信する。…携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末 22 から受信した QR 決裁証明鍵 1201 の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ 41 は詳細決裁承認を店舗端末 22 に返信する。」（以上、同ク）、⑤「本人の購入意思の確定応答があったならば、決裁ボタン操作によって決裁を完了する（ステップ 1017）。決裁ボタン操作が行われた場合は、店舗端末 22 は決裁終了メッセージを認証サーバ 41 に送信する。」「決裁終了情報を受信した金融機関 42 では利用者の指定口座から代金を引き落とす手続を行う。」（以上、同ケ）との記載がある。

上記記載によれば、引用発明においては、利用者が、自分が所持する携帯電話機 1 に店舗 ID、暗証番号、決裁（決済）方法、商品の購入金額を入力し、QR 決裁証明鍵発行要求として認証サーバ 41 に送信し、QR 決裁証明鍵発行要求を受信した認証サーバ 41 は、店舗及び利用者の認証処理を行い、認証が認められる場合、決済方法の情報を含む QR 決裁証明鍵を生成し、これを携帯電話機 1 に送信し、その後、利用者が店舗において購入希望商品の発注を行う際、店舗端末 22 に付属した QR コード読取装置 21 は、携帯電話機 1 の表示部 11 に表示された QR 決裁証明鍵 1201 を読み取るとともに、携帯電話機 1 の正面あるいは側面に印刷された標識 19、20 から携帯電話製造番号と携帯電話番号を読み取り、その読取結果を店舗端末 22 に転送し、店舗端末 22 は、携帯電話機 1 から読み取った携帯電話製造番号、携帯電話番号及び QR 決裁証明鍵 1201 を決裁承認要求として認証サーバ 41 に送信し、認証サーバ 41 が、携帯電話製造番号及び携帯電話番号が正当か否かを利用者情報 DB 44 の登録内

容と照合して調べ、この結果、いずれか一方の番号が未登録のものであるか、登録された番号と異なる場合には、不正利用であるものと判断し不正利用情報データベースに登録した後、不正利用メッセージを店舗端末２２及び携帯電話機１に送信し、一方、携帯電話製造番号及び携帯電話番号の両方が正当なものであり、しかも店舗端末２２から受信したＱＲ決裁証明鍵１２０１の情報（全部または一部）が自分自身で発行した正規のものであると認められた場合には、認証サーバ４１は詳細決裁承認を店舗端末２２に返信し、店員が、利用者本人に購入意思を確認した上で、決済処理が行われていることを理解できる。

しかるところ、前記アのとおり、引用発明において、認証サーバ４１が「決済承認要求」（引用例１記載の「決裁承認要求」。以下同じ。）を受け付けることは、本願発明の「サービスの要求を受けるステップ」に相当するものである。そして、認証サーバ４１は、決裁承認要求を受け付けると、決裁承認要求に含まれる携帯電話製造番号及び携帯電話番号の両方が正当であることを利用者情報ＤＢ４４の登録内容と照合して確認し、かつ、ＱＲ決裁証明鍵が自ら発行した正規のものであると認めた場合、決裁承認要求に係る決裁承認を店舗端末２２に返信していることからすれば、認証サーバ４１が、利用者情報登録ＤＢ４４に登録された携帯電話機１の携帯電話製造番号及び携帯電話番号と紐づけて自らが発行したＱＲ決裁証明鍵の情報を管理し、店舗端末２２から送信された決裁承認要求に含まれる携帯電話製造番号、携帯電話番号及びＱＲ決裁証明鍵の情報が上記情報と一致する場合には、決裁承認の処理を行い、そうでない場合には、決裁承認の処理を行わない制御を行うための情報を有していることは自明であり、また、利用者情報登録ＤＢ４４に登録された携帯電話製造番号及び携帯電話番号が携帯電話機１から取得されたことも自明である。

そうすると、かかる制御を行うための情報は、「コンピュータ」である認

証サーバ４１が、「サービスの要求」としてのＱＲ決裁承認要求を認めるか否かを処理するために使用する情報であって、「物品」である携帯電話機１から取得される「認証情報」である携帯電話製造番号及び携帯電話番号に基づいて設定された情報であるといえるから、本願発明の「指示情報」に相当するものと認められる。

以上によれば、引用例１に接した当業者は、引用発明において、かかる制御を行うための情報を有しているものと理解するから、相違点１に係る本願発明の構成（「（ＱＲ決裁承認要求に係る）前記要求を処理するために指示情報を使用するステップ」の構成）及び相違点２に係る本願発明の構成（「前記指示情報が認証情報に基づいて設定された指示情報」であるとの構成）とすることを容易に想到することができたものと認められる。

これと同旨の本件審決の判断は、結論において相当である。

(3) 原告の主張について

原告は、本件審決のいう引用発明の「ＱＲ決済証明鍵を発行したことを管理するための情報」は、認証情報（携帯電話製造番号及び携帯電話番号）が店舗端末２２から認証サーバ４１に送信される前に、認証情報に基づく認証とは無関係に生成される情報であり、本願発明の「指示情報」（「認証情報に基づいて設定された情報」）といえない旨主張する。

しかしながら、本件審決のいう引用発明の「ＱＲ決済証明鍵を発行したことを管理するための情報」とは、前記(2)で説示した、認証サーバ４１が、利用者情報登録ＤＢ４４に登録された携帯電話機１の携帯電話製造番号及び携帯電話番号と紐づけて自らが発行したＱＲ決裁証明鍵の情報を管理し、店舗端末２２から送信された決裁承認要求に含まれる携帯電話製造番号、携帯電話番号及びＱＲ決裁証明鍵の情報が上記情報と一致する場合には、決裁承認の処理を行い、そうでない場合には、決裁承認の処理を行わない制御を行うための情報と同旨の情報をいうものと解されるところ、引用例１の記載（前

記(1)ク) から、携帯電話 1 の携帯電話製造番号及び携帯電話番号は、Q R 決
裁承認要求がされる前から、承認機関 4 の利用者情報登録 D B 4 4 に登録さ
れた情報であることは明らかであるから、上記制御を行うための情報も、Q
R 決裁承認要求がされる前に、当該携帯電話製造番号及び携帯電話番号に基
づいて設定されたものとみるのが自然である。

したがって、原告の主張は、その前提において採用することができない。
その他原告は縷々主張するが、いずれも理由はない。

(4) 小括

以上によれば、本願発明は、当業者が引用例 1 に基づいて容易に発明をす
ることができたものと認められるから、原告主張の取消事由は理由がない。

3 結論

以上のとおり、原告主張の取消事由は理由がなく、本件審決にこれを取り消
すべき違法は認められない。

したがって、原告の請求は棄却されるべきものであるから、主文のとおり判
決する。

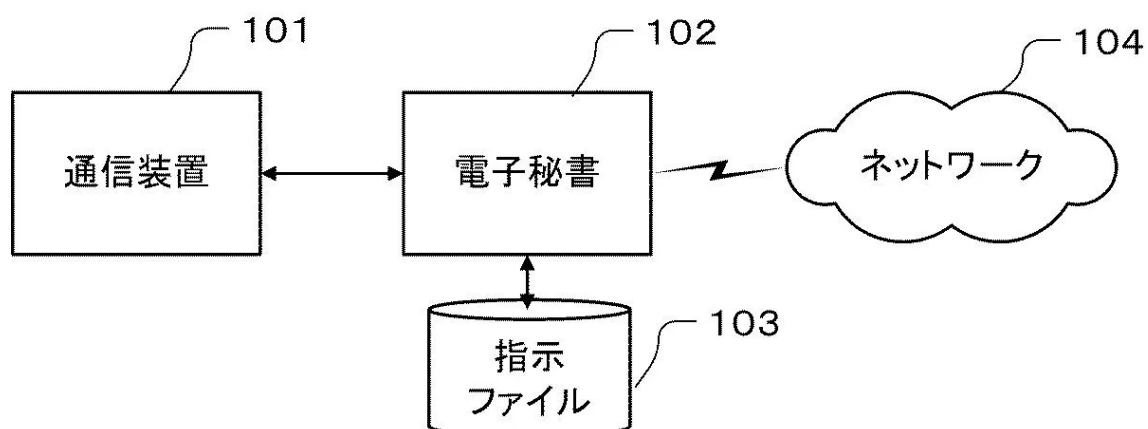
知的財産高等裁判所第 1 部

裁判長裁判官 大 鷹 一 郎

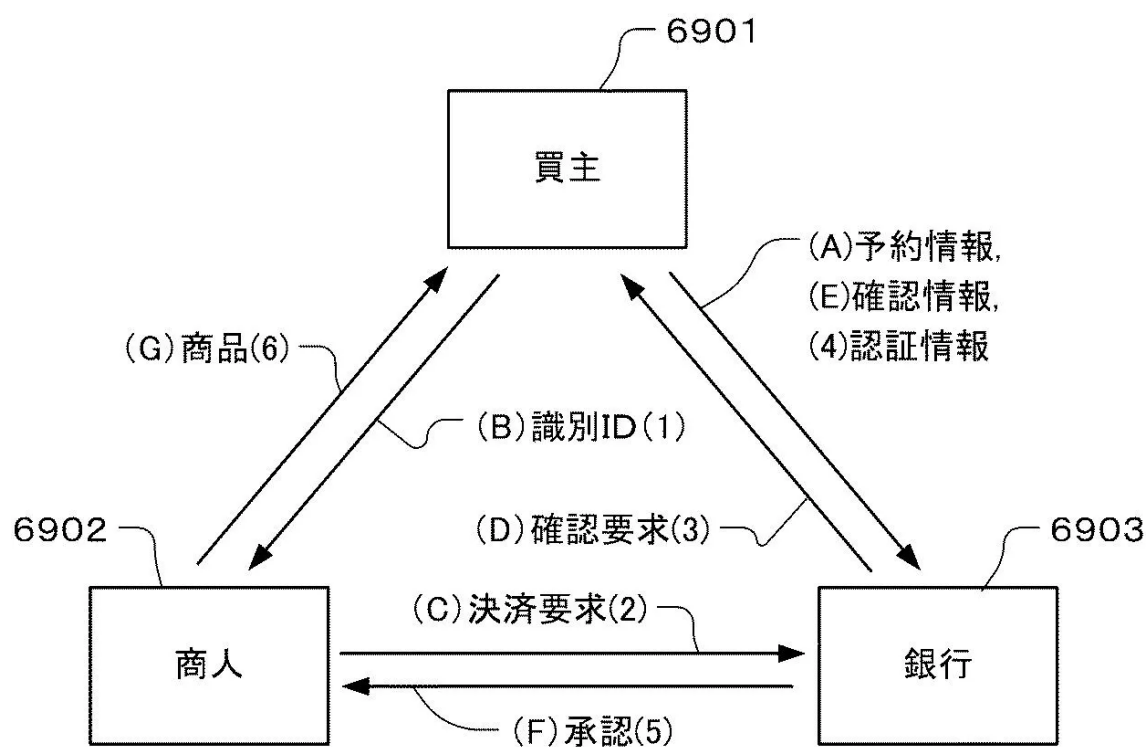
裁判官 小 川 卓 逸

裁判官 遠 山 敦 士

【図 1】



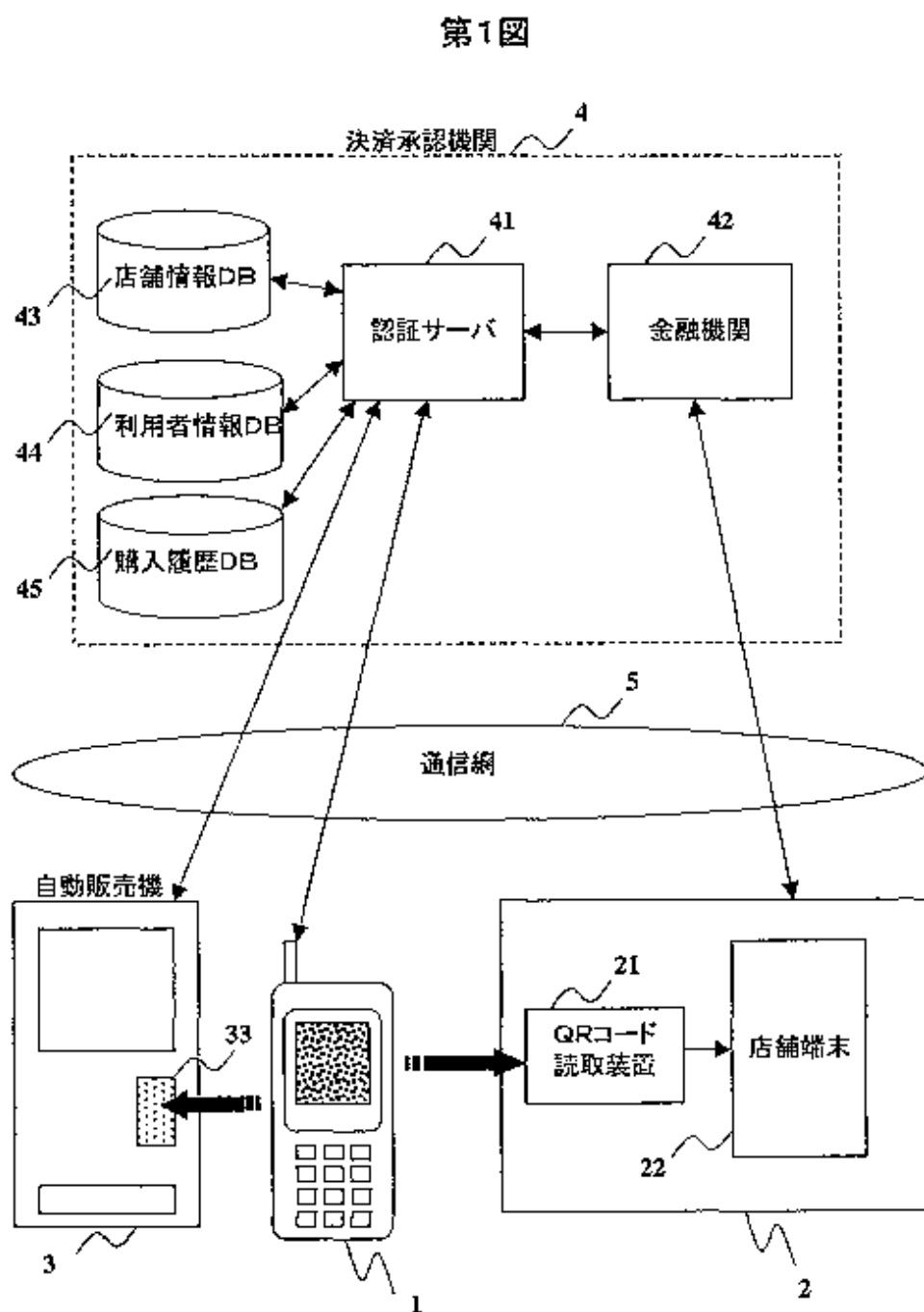
5 【図 6 9】



【表 1】

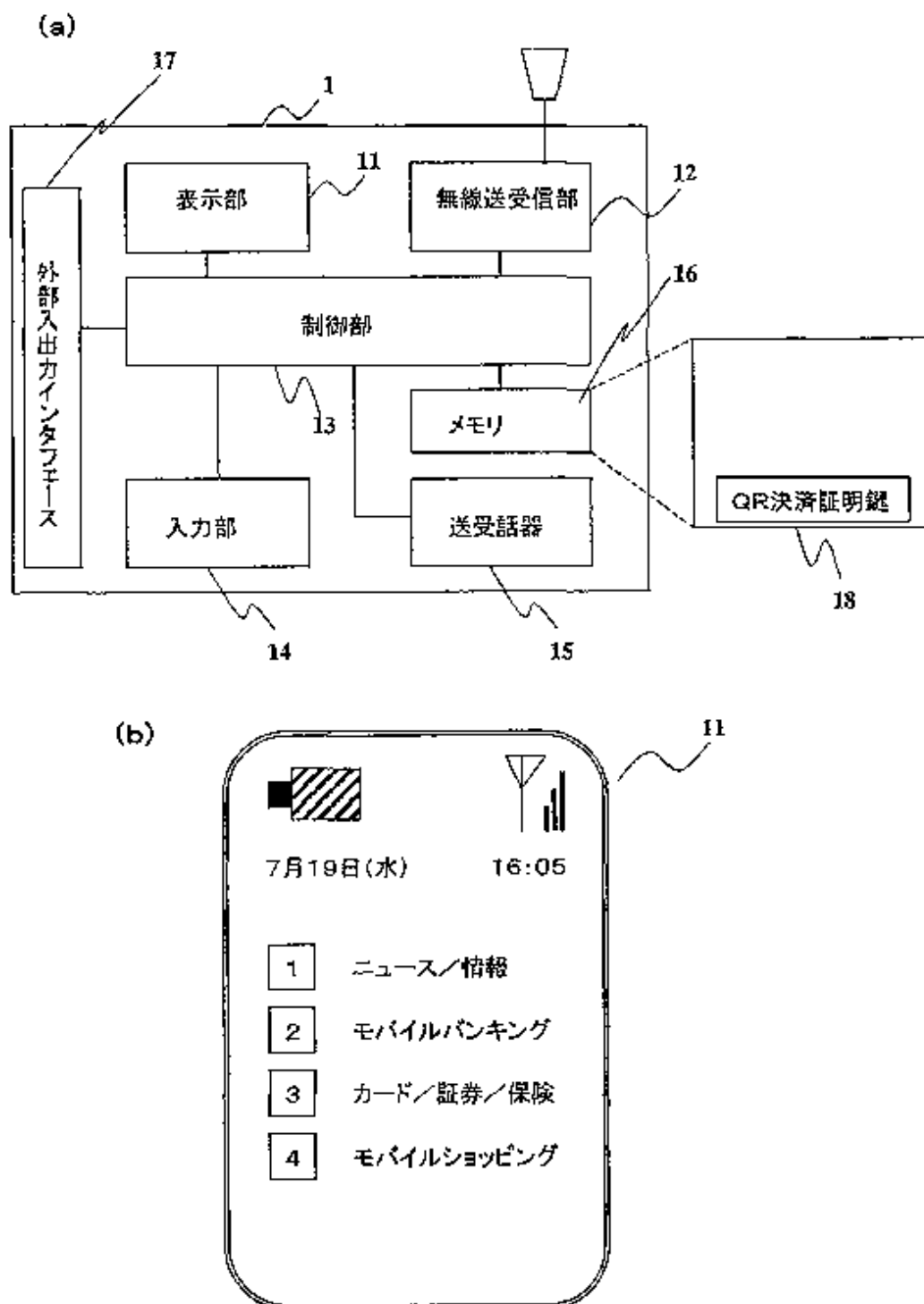
用語	実施例				
通信ID	090-1234-5678	090-1234-5678	090-1234-5678, 商店	abc@docomo.ne.jp	090-1234-5678
識別ID	非接触ICカード番号	ナンバープレート番号	045-1234-5678	abc@y.ne.jp	キャッシュカード番号
銀行口座番号	123-12345	123-12345	123-12345	123-12345	123-12345
仮想口座	鉄道会社	高速道路	買物	ネット商店	ATM出金
残高上限額	20,000円	30,000円	100,000円	30,000円	500,000円
確認不要限度額	560円	1,000円	1,000円	0円	0円
確認不要 累積限度額	5,000円	5,000円	5,000円	0円	0円
残高通知額	2,000円	3,000円	10,000円	10,000円	300,000円
残高通知先	abc@y.ne.jp	abc@y.ne.jp	abc@y.ne.jp	abc@y.ne.jp	abc@y.ne.jp
自動回復日数	30日	10日	30日	60日	30日
決済予約確認 要否	不要	要	-	-	-
確認情報	456	456	456	456	****
暗証番号	*****	*****	*****	*****	*****
通信確認待遇ID	3	4	5	6	5
操作情報	YESボタン	はい	指紋	456	指紋

【図 1】



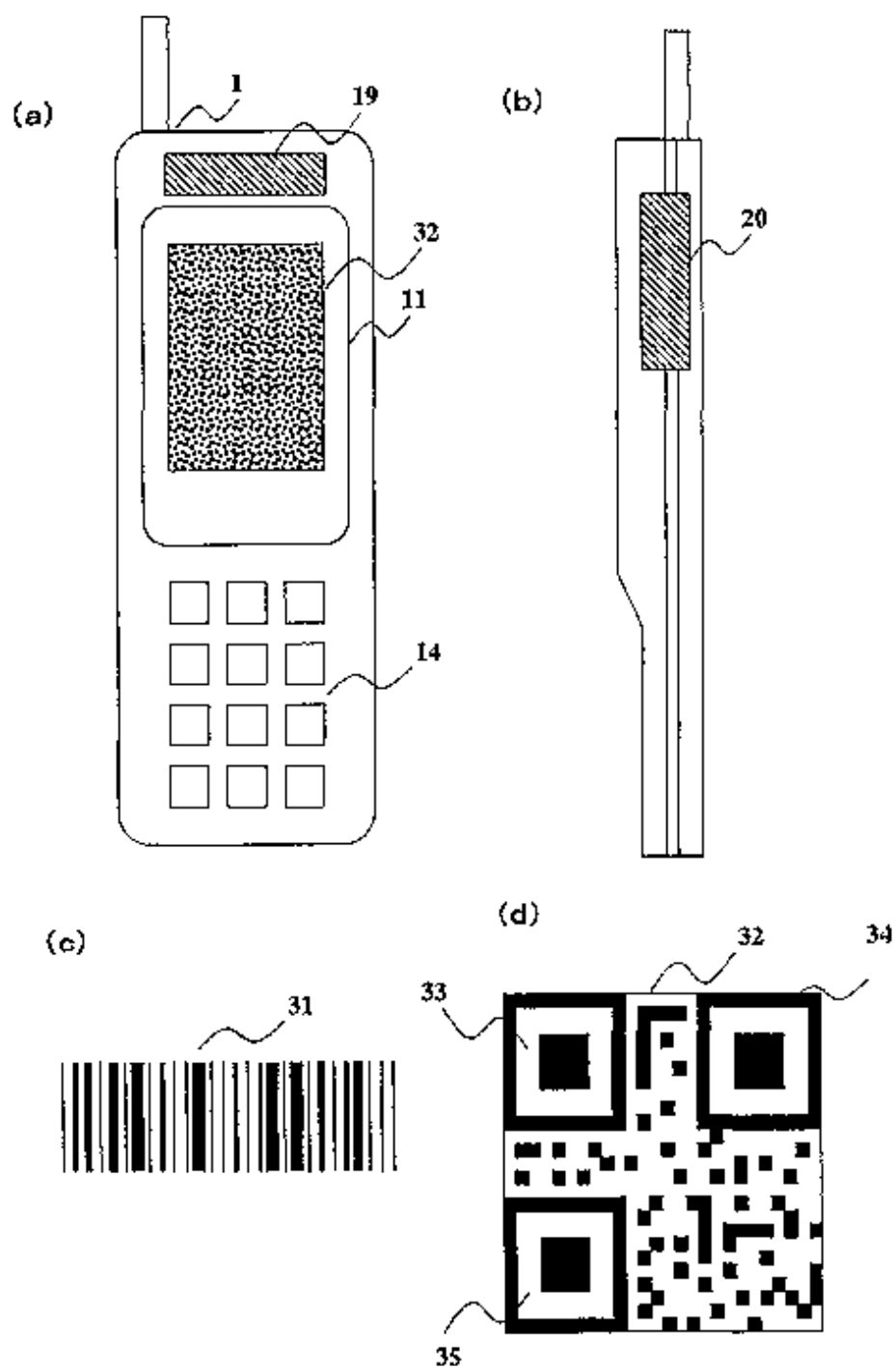
【図2】

第2図



【図3】

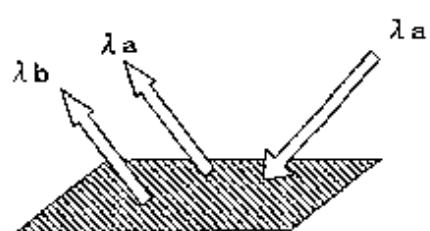
第3図



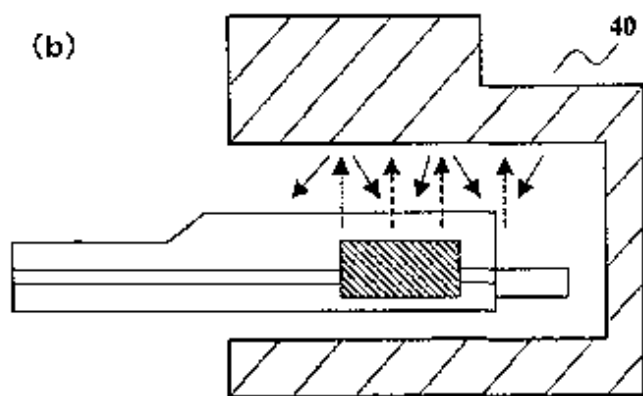
【図 4】

第4図

(a)



(b)



【図 7】

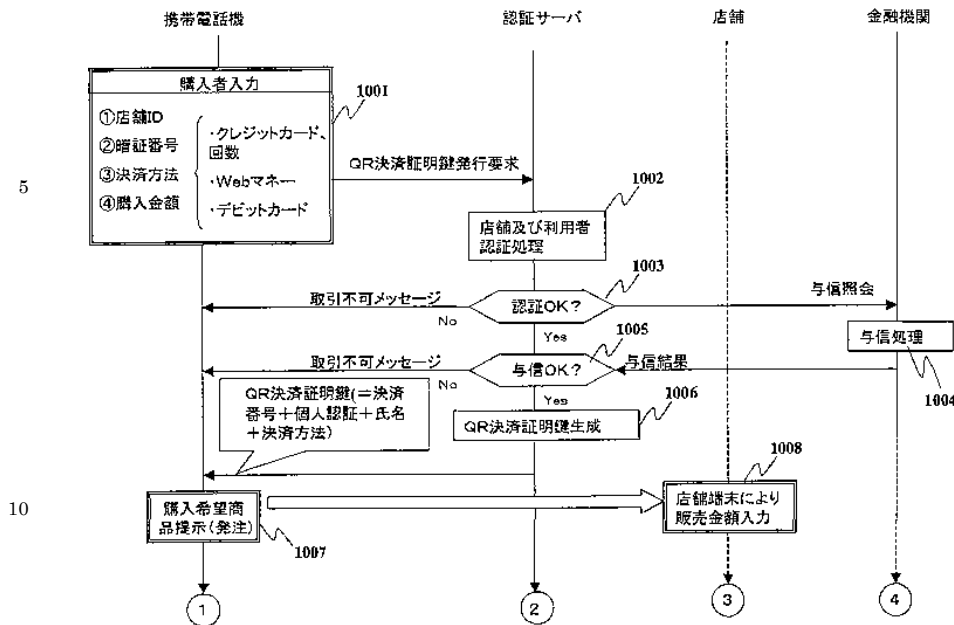
利用者情報データベース					
利用者ID	利用者名	住所	携帯電話製造番号	携帯電話番号	暗証番号
UR001	木村XX	東京都中央区XX町5-2	MMAB1234	090-3221-XXXX	4123
UR002	田中XX	東京都目黒区XX町3-1	MMAB1235	090-3332-XXXX	9198
UR199	佐藤XX	東京都品川区YR町1-1	MMAB9933	090-4521-XXXX	0678

性別	生年月日	デビットカード番号	クレジットカード番号	Webマネー口座番号	個人特徴情報
男	1960/03/05	ABC銀行123899	NNM23567	WMN5678	写真ID4567

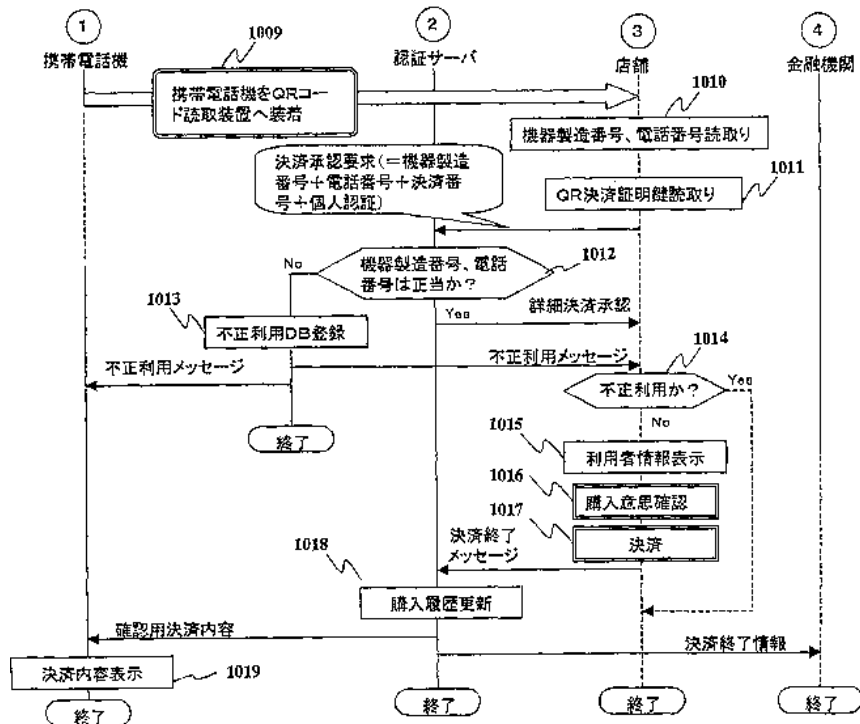
【図 9】

不正利用情報データベース		
携帯電話製造番号	携帯電話番号	店舗ID
—	090-123999XX	—
NNM4567	090-113599XX	—
—	—	BB098

【図 10】

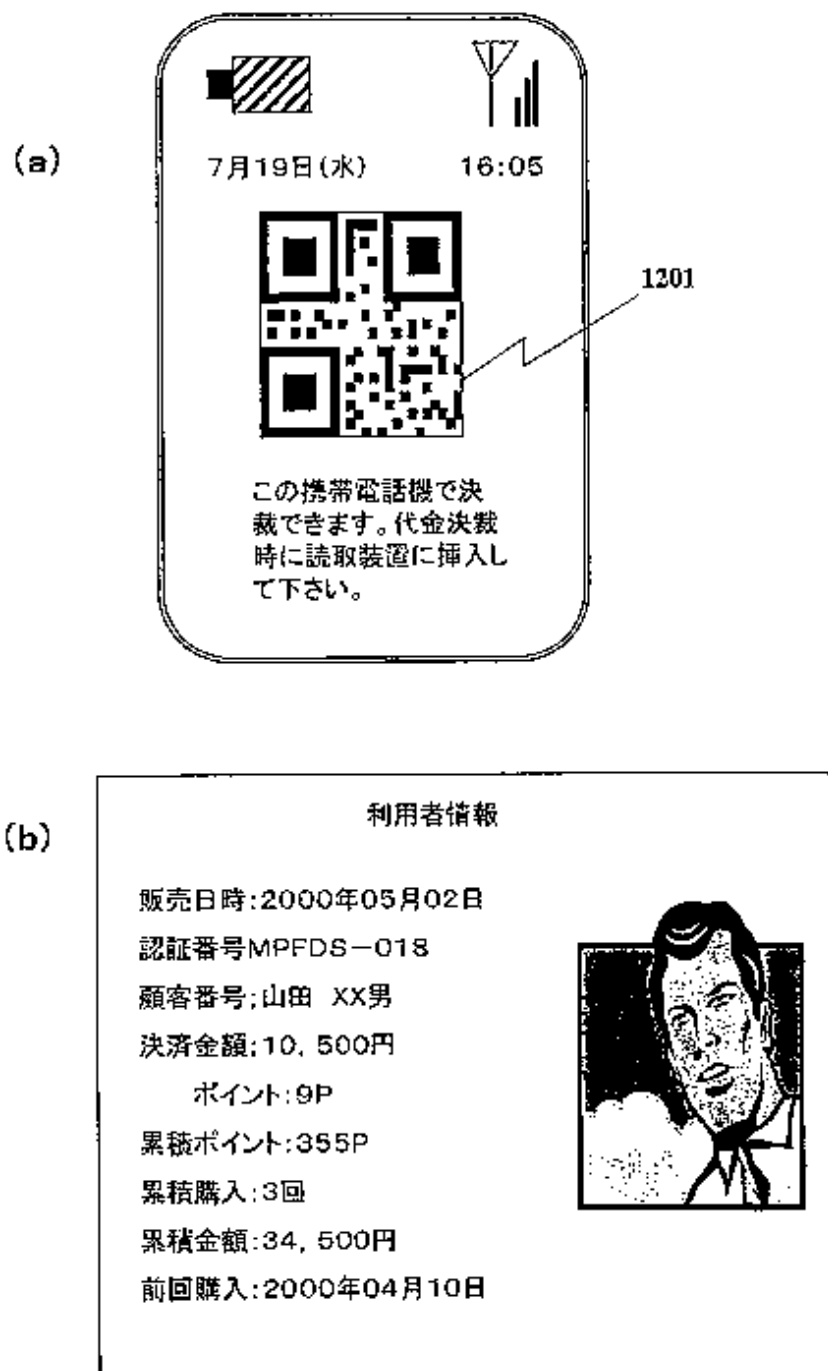


【図 11】



【図 1 2】

第12図



【図13】

第13図

