

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6128565号

(P6128565)

(45) 発行日 平成29年5月17日(2017.5.17)

(24) 登録日 平成29年4月21日(2017.4.21)

(51) Int.Cl. F I  
**G06Q 20/40 (2012.01)** G06Q 20/40  
**G06Q 20/32 (2012.01)** G06Q 20/32 330

請求項の数 26 (全 25 頁)

|               |                               |           |                    |
|---------------|-------------------------------|-----------|--------------------|
| (21) 出願番号     | 特願2014-557079 (P2014-557079)  | (73) 特許権者 | 514208998          |
| (86) (22) 出願日 | 平成25年2月20日 (2013.2.20)        |           | グローバル ブルー エス. エー.  |
| (65) 公表番号     | 特表2015-510640 (P2015-510640A) |           | スイス, 1262 エザン, ルート |
| (43) 公表日      | 平成27年4月9日 (2015.4.9)          |           | ド クラシェ 7           |
| (86) 国際出願番号   | PCT/EP2013/053328             | (74) 代理人  | 100107456          |
| (87) 国際公開番号   | W02013/124290                 |           | 弁理士 池田 成人          |
| (87) 国際公開日    | 平成25年8月29日 (2013.8.29)        | (74) 代理人  | 100162352          |
| 審査請求日         | 平成27年9月24日 (2015.9.24)        |           | 弁理士 酒巻 順一郎         |
| (31) 優先権主張番号  | 201201227-4                   | (74) 代理人  | 100123995          |
| (32) 優先日      | 平成24年2月21日 (2012.2.21)        |           | 弁理士 野田 雅一          |
| (33) 優先権主張国   | シンガポール (SG)                   | (74) 代理人  | 100148596          |
|               |                               |           | 弁理士 山口 和弘          |

最終頁に続く

(54) 【発明の名称】 取引処理システム及び方法

(57) 【特許請求の範囲】

【請求項1】

ユーザ情報を安全に記憶する記憶部であって、前記ユーザ情報は、一人のユーザについて、移動通信装置の移動通信装置アプリケーションのインスタンスを識別する移動通信装置識別情報を含む移動通信装置情報と、前記移動通信装置識別情報に関連付けられた支払い口座情報及びユーザ検証情報とを含む、当該記憶部と、

記憶システム処理手段であって、

取引システムから、取引額情報、移動通信装置識別情報、及びユーザ検証情報を含む第1の取引許可要求メッセージを受信し、

前記受信したユーザ検証情報が、前記取引許可要求メッセージで識別される移動通信装置について記憶されているユーザ検証情報と一致するかどうかを判定する処理を行い、前記受信したユーザ検証情報が前記記憶されたユーザ検証情報と一致する場合には、

前記記憶部から、前記移動通信装置識別情報に関連付けられた支払い口座情報を検索し、

前記取引額情報及び前記支払い口座情報を含む第2の許可要求メッセージを許可システムに送信し、

前記許可システムから、前記第2の許可要求メッセージに応答する第1の許可応答メッセージを受信すると、前記支払い口座情報を特定することなく第2の許可応答メッセージを前記取引システムに送信させる、

ように構成された、当該記憶システム処理手段と、

10

20

を備える記憶システム。

【請求項 2】

前記記憶部に保持される前記移動通信装置情報が、前記移動通信装置識別情報に関連付けられた移動通信装置アクセス情報を含み、

前記記憶システム処理手段が、前記移動通信装置識別情報を含む移動通信装置アクセス情報要求を前記取引システムから受信するのに応答して、

前記移動通信装置識別情報に関連付けられた前記移動通信装置アクセス情報を前記記憶部から検索し、

前記取引システムに、前記移動通信装置識別情報に関連付けられた前記移動通信装置アクセス情報を含む移動通信装置アクセス情報応答を送信する、

ように構成される、請求項 1 に記載の記憶システム。

10

【請求項 3】

前記記憶システム処理手段が、前記取引システムから前記移動通信装置識別情報を含む移動通信装置アクセス情報要求を受信するのに応答して、

前記記憶部から前記移動通信装置識別情報に関連付けられたユーザ検証情報を検索し、

前記ユーザ検証情報のサブセットを決定し、

前記決定されたユーザ検証情報のサブセットの要求をさらに含む移動通信装置アクセス情報応答を前記取引システムに送信する、

ようにさらに構成される、請求項 2 に記載の記憶システム。

20

【請求項 4】

前記受信されたユーザ検証情報が、前記取引許可要求メッセージで識別される前記移動通信装置について記憶されたユーザ検証情報と一致するかどうかを判定する処理が、

前記受信されたユーザ検証情報が前記決定されたユーザ検証情報のサブセットと一致することを確認する処理、

を含む、請求項 3 に記載の記憶システム。

【請求項 5】

前記記憶部が、

暗号化された支払い口座情報、通貨選択の設定情報、および、非課税購入の設定情報、のうち少なくとも 1 つを安全に記憶する、

請求項 1 に記載の記憶システム。

30

【請求項 6】

取引システム及び請求項 1 に記載の記憶システムを備えるシステムであって、

前記取引システムが取引システム処理手段を備え、

前記取引システム処理手段は、商店システムから取引額情報及び移動通信装置識別情報を含む最初の取引許可要求メッセージを受信すると、

前記移動通信装置識別情報に関連付けられた移動通信装置アクセス情報を取得し、

取引額情報及びユーザ検証情報の要求を含む取引検証要求メッセージを前記移動通信装置に送信し、

前記移動通信装置からユーザ検証情報を含む取引検証応答メッセージを受信したのに応答して、前記取引額情報、前記移動通信装置識別情報及び前記ユーザ検証情報を含む第 1 の取引許可要求メッセージを前記記憶システムに送信する、

ように構成される、

システム。

40

【請求項 7】

取引システムを備えたシステムであって、

前記取引システムは取引システム処理手段を備え、

前記取引システム処理手段は、商店システムから取引額情報及び移動通信装置の移動通信装置アプリケーションのインスタンスを識別する移動通信装置識別情報を含む最初の取引許可要求メッセージを受信すると、

50

前記移動通信装置識別情報に関連付けられた移動通信装置アクセス情報を取得し、  
取引額情報及びユーザ検証情報の要求を含む取引検証要求メッセージを前記移動通信装置に送信し、

前記移動通信装置からユーザ検証情報を含む取引検証応答メッセージを受信したのに  
応答して、前記取引額情報、前記移動通信装置識別情報及び前記ユーザ検証情報を含む第  
1の取引許可要求メッセージを記憶システムに送信する、

ように構成される、

システム。

【請求項 8】

前記取引システム処理手段が、

前記商店システムから前記取引額情報及び前記移動通信装置識別情報を含む前記最初  
の取引許可要求メッセージを受信するのに応答して、前記移動通信装置識別情報を含む移  
動通信装置アクセス情報要求を前記記憶システムに送信し、

前記移動通信装置識別情報に関連付けられた前記移動通信装置アクセス情報を含む前  
記記憶システムからの移動通信装置アクセス情報応答に応答して、取引額情報及びユーザ  
検証情報の要求を含む前記取引検証要求メッセージを前記移動通信装置に送信する、

ように構成される、請求項 7 に記載のシステム。

【請求項 9】

前記システムは、商店システムをさらに備え、

前記商店システムは、

購入取引のために商品識別情報を入力する手段と、

前記購入取引のためにユーザの移動通信装置を識別する移動通信装置識別情報を入力す  
る手段と、

商店システム処理手段であって、当該商店システム処理手段は、

前記取引システムに前記取引額情報及び移動通信装置識別情報を含む最初の取引許可  
要求メッセージを送信し、

前記取引システムから第 2 の許可応答メッセージを受信すると、前記ユーザに前記購  
入取引を完了するための受領証を発行する、

ように動作する、当該商店システム処理手段と、

を含む、請求項 7 に記載のシステム。

【請求項 10】

前記移動通信装置識別情報を入力する手段が、

前記移動通信装置に関連付けられ前記移動通信装置識別情報を表す R F I D 識別子を読  
み取る R F I D 読み取り機、

を含む、請求項 9 に記載のシステム。

【請求項 11】

前記 R F I D 読み取り機が N F C 読み取り機である、請求項 10 に記載のシステム。

【請求項 12】

前記移動通信装置識別情報を入力する手段が、

前記移動通信装置によって表示され前記移動通信装置識別情報を表す視覚コードを撮像  
する撮像装置、

を含む、請求項 9 に記載のシステム。

【請求項 13】

前記移動通信装置識別情報が、前記移動通信装置のハードウェアの識別子と、前記移動  
通信装置の移動通信装置アプリケーションのインスタンスの識別子と、の代数的又はアル  
ゴリズムの組み合わせから生成される、請求項 7 に記載のシステム。

【請求項 14】

一意の前記移動通信装置識別情報が、前記移動通信装置及び前記移動通信装置アプリケ  
ーションのインスタンスを登録する登録処理の一部として登録サーバで生成される、請求  
項 13 に記載のシステム。

10

20

30

40

50

## 【請求項 15】

一人のユーザについて、移动通信装置の移动通信装置アプリケーションのインスタンスを識別する移动通信装置識別情報を含む移动通信装置情報と、前記移动通信装置識別情報に関連付けられた支払い口座情報及びユーザ検証情報とを含むユーザ情報、を記憶システムの記憶部に安全に記憶するステップと、

取引システムから、取引額情報、移动通信装置識別情報及びユーザ検証情報を含む第1の取引許可要求メッセージを、前記記憶システムで受信するステップと、

受信したユーザ検証情報が、前記取引許可要求メッセージで識別される移动通信装置について記憶されているユーザ検証情報と一致するかどうかを前記記憶システムで判定する処理を行うステップであって、受信したユーザ検証情報が、記憶されたユーザ検証情報と一致する場合には、

10

前記記憶システムが、前記記憶部から前記移动通信装置識別情報に関連付けられた支払い口座情報を検索するサブステップと、

前記記憶システムが、前記取引額情報及び前記支払い口座情報を含む第2の許可要求メッセージを許可システムに送信するサブステップと、

前記記憶システムが、前記許可システムから前記第2の許可要求メッセージに応答する第1の許可応答メッセージを受信すると、前記支払い口座情報を特定することなく第2の許可応答メッセージを前記取引システムに送信させるサブステップと、

を実行する、当該判定する処理を行うステップと、

を備える、方法。

20

## 【請求項 16】

前記記憶部に保持される前記移动通信装置情報が、前記移动通信装置識別情報に関連付けられた移动通信装置アクセス情報、を含み、

前記方法が、

前記移动通信装置識別情報を含む移动通信装置アクセス情報要求を前記取引システムから受信したときのステップとして、

前記記憶システムが、前記移动通信装置識別情報に関連付けられた前記移动通信装置アクセス情報を前記記憶部から検索するステップと、

前記記憶システムが、前記移动通信装置識別情報に関連付けられた前記移动通信装置アクセス情報を含む移动通信装置アクセス情報応答を前記取引システムに送信するステップと、

30

をさらに備える、請求項 15 に記載の方法。

## 【請求項 17】

前記方法が、

前記取引システムから、前記移动通信装置識別情報を含む移动通信装置アクセス情報要求を受信したときのステップとして、

前記記憶システムが、前記移动通信装置識別情報に関連付けられたユーザ検証情報を検索するステップと、

前記記憶システムが前記ユーザ検証情報のサブセットを決定するステップと、

前記記憶システムが、前記決定されたユーザ検証情報のサブセットの要求をさらに含む移动通信装置アクセス情報応答を前記取引システムに送信するステップと、

40

をさらに備える、請求項 16 に記載の方法。

## 【請求項 18】

前記判定する処理が、

前記受信されたユーザ検証情報が前記決定されたユーザ検証情報のサブセットと一致することを確認する処理、

を含む、請求項 17 に記載の方法。

## 【請求項 19】

前記方法が、

暗号化された支払い口座情報、通貨選択の設定情報、および、非課税購入の設定情報、

50

のうち少なくとも1つを、前記記憶部に安全に記憶するステップ、  
をさらに備える、請求項15に記載の方法。

【請求項20】

前記方法が、

前記取引システムが商店システムから取引額情報及び移動通信装置識別情報を含む最初の取引許可要求メッセージを受信したときのステップとして、

前記取引システムが、前記移動通信装置識別情報に関連付けられた移動通信装置アクセス情報を取得するステップと、

前記取引システムが、前記移動通信装置に、取引額情報及びユーザ検証情報の要求を含む取引検証要求メッセージを送信するステップと、

10

前記移動通信装置からユーザ検証情報を含む取引検証応答メッセージを受信したのに応答して、前記取引システムが、前記記憶システムに、前記取引額情報、前記移動通信装置識別情報及び前記ユーザ検証情報を含む第1の取引許可要求メッセージを送信するステップと、

をさらに備える、請求項15に記載の方法。

【請求項21】

前記方法が、

前記取引システムが前記商店システムから前記取引額情報及び移動通信装置識別情報を含む最初の取引許可要求メッセージを受信したときのステップとして、

前記取引システムが、前記記憶システムに、前記移動通信装置識別情報を含む移動通信装置アクセス情報要求を送信するステップと、

20

前記移動通信装置識別情報に関連付けられた前記移動通信装置アクセス情報を含む前記記憶システムからの移動通信装置アクセス情報応答に応答して、前記取引システムが、取引額情報及びユーザ検証情報の要求を含む前記取引検証要求メッセージを前記移動通信装置に送信するステップと、

をさらに備える、請求項20に記載の方法。

【請求項22】

商店システムが、購入取引のために商品識別情報を受信するステップと、

前記商店システムが、前記購入取引のためにユーザの移動通信装置を識別する移動通信装置識別情報を受信するステップと、

30

前記商店システムが、前記取引システムに、前記取引額情報及び移動通信装置識別情報を含む最初の取引許可要求メッセージを送信するステップと、

前記商店システムが前記取引システムから第2の許可応答メッセージを受信すると、前記ユーザに前記購入取引を完了するための受領証を発行するステップと、

をさらに備える、請求項15に記載の方法。

【請求項23】

前記移動通信装置に関連付けられ前記移動通信装置識別情報を表すRFID識別子を読み取ることにより、前記移動通信装置識別情報の入力を受信するステップ、

をさらに備える、請求項22に記載の方法。

【請求項24】

40

前記移動通信装置によって表示された視覚コードであって、前記移動通信装置識別情報を表す当該視覚コード、を撮像することにより、前記移動通信装置識別情報の入力を受信するステップ、

をさらに備える、請求項22に記載の方法。

【請求項25】

前記移動通信装置識別情報が、前記移動通信装置のハードウェアの識別子と、前記移動通信装置の移動通信装置アプリケーションのインスタンスの識別子との、代数的又はアルゴリズム的組み合わせから生成される、請求項15に記載の方法。

【請求項26】

前記移動通信装置及び前記アプリケーションのインスタンスを登録する登録処理の一部

50

として、登録サーバが一意の移動通信装置識別情報を生成するステップ、  
をさらに備える、請求項 25 に記載の方法。

【発明の詳細な説明】

【技術分野】

【0001】

[0001] 本発明は、取引処理システム及び方法に関する。特に、本発明は、ユーザが支払いカード、小切手、又は現金を商店に提示する必要なしに、安全且つ信頼できる方法で顧客（ユーザ）と商店の間の取引を可能にするシステム及び方法に関する。

【背景技術】

【0002】

[0002] 顧客と商店間で現金を用いず取引を行うための安全な方法を提供する必要がある。現在、顧客と商店の間で現金を用いず取引を行う典型的な方法は、クレジットカード、デビットカード、前払いカード等の支払いカードを使用するものである。そのようなカードは、そのような取引を行う一般的な方法として小切手に取って代わっている。しかし、例えばチップや P I N カードの使用により支払いカードの使用の安全性が進歩したにも関わらず、そのようなカードの不正な使用は、今なお大きな問題である。

【0003】

[0003] 米国特許出願公開第 2011 / 0276478 号は、支払いを電話番号に関連付けるシステムを記載する。データ記憶設備とそのデータ記憶設備に結合されたインターチェンジが、電話番号と関連付けて購入の受領証を記憶する。インターチェンジは、共通形式プロセッサ、及び移動通信の複数の異なるコントローラとインターフェースをとる複数の変換器を含む。変換器は、種々の異なる形式のコントローラ及び共通形式の共通形式プロセッサと通信して、電話番号、商店、及び商店からの購入内容を特定する支払い要求の確認を取得するように構成される。確認が受け取られると、インターチェンジは、電話番号に関連付けられた資金を使用して、購入の代金を商店に支払い、購入の受領証を商店から受け取って記憶する。

【0004】

[0004] 米国特許出願公開第 2009 / 0307139 号は、ユーザの身元が確認されると金融取引を実施する命令コードを生成するように構成された、携帯電話の第 1 の安全な要素内のアプリケーションプログラムを使用して、販売時点で金融取引を認証する方法を記載する。ユーザの資格証明が電話機の第 2 の安全な要素に記憶され、第 2 の要素は、電話機へのユーザ入力の生体特徴からユーザの識別を検証し、ユーザの識別が検証されるのに応じて金融取引を認証するデータを生成するように動作する。店頭で、ユーザがアプリケーションを起動し、生体特徴を電話機に入力する。第 2 の安全な要素がユーザの身元を検証し、身元が確認されると、取引を認証するデータを生成する。命令コード及び認証データを含む金融取引データは、その後、電話機から販売地点に送信される。

【0005】

[0005] W O 2011 / 112752 号公報は、1 つ又は複数の移動装置を介して行われる電子商取引及び金融取引を容易にし、ユーザの移動装置との通信を介して行われる身元の確認と認証のためのトランザクションを容易にする技術を記載する。

【先行技術文献】

【特許文献】

【0006】

【特許文献 1】 米国特許出願公開第 2011 / 0276478 号

【特許文献 2】 米国特許出願公開第 2009 / 0307139 号

【特許文献 3】 W O 2011 / 112752 号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

[0006] 各種方式が提案されているが、顧客と商店間の取引を可能にするより安全な方法

10

20

30

40

50

がなお必要とされる。

【0008】

[0007]本発明は、そのような問題の技術的解決を提供しようとするものである。

【課題を解決するための手段】

【0009】

[0008]本発明の態様は特許請求の範囲で定義される。

【0010】

[0009]一実施形態では、記憶システムが、ユーザ（顧客）情報を安全に記憶する記憶部を備えることができ、ユーザ情報は、一人のユーザについて、移动通信装置の移动通信装置アプリケーションのインスタンスを識別する移动通信装置識別情報を含む移动通信装置情報と、移动通信装置識別情報に関連付けられた支払い口座情報及びユーザ検証情報とを含む。記憶システム処理手段は、取引システムから、取引額情報、移动通信装置識別情報、及びユーザ検証情報を含む第1の取引許可要求メッセージを受信し、受信したユーザ検証情報が、取引許可要求で識別される移动通信装置について記憶されているユーザ検証情報と一致するかどうかを判定する処理を行い、受信したユーザ検証情報が記憶されたユーザ検証情報と一致する場合には、記憶部から、移动通信装置識別情報に関連付けられた支払い口座情報を検索し、取引額情報及び支払い口座情報を含む第2の許可要求メッセージを許可システムに送信し、許可システムから第2の許可メッセージに応答する第1の許可応答メッセージを受信すると、支払い口座情報を特定することなく第2の許可応答メッセージを取引システムに送信させるように構成することができる。

10

20

【0011】

[0010]一実施形態では、取引システムが取引システム処理手段を備えることができ、取引システム処理手段は、商店システムから取引額情報及び移动通信装置識別情報を含む最初の取引許可要求メッセージを受信すると、移动通信装置識別情報に関連付けられた移动通信装置アクセス情報を取得し、移动通信装置に、取引額情報及びユーザ検証情報の要求を含む取引検証要求メッセージを送信し、移动通信装置から取引検証応答メッセージユーザ検証情報を受信するのに応答して、記憶システムに、取引額情報、移动通信装置識別情報、及びユーザ検証情報を含む第1の取引許可要求メッセージを送信するように構成される。

【0012】

[0011]一実施形態では、商店システムが、購入取引のために商品識別情報を入力する手段と、購入取引のためにユーザの移动通信装置を識別する移动通信装置識別情報を入力する手段と、商店システム処理手段であって、取引システムに、取引額情報及び移动通信装置識別情報を含む最初の取引許可要求メッセージを送信し、取引システムから第2の許可応答メッセージを受信すると、ユーザに購入取引を完了するための受領証を発行するように動作する当該商店システム処理手段と、を備えることができる。

30

【0013】

[0012]一実施形態では、登録サーバを、移动通信装置のアプリケーションと通信して、移动通信装置のハードウェアの識別子と、アプリケーションのインスタンスとを識別し、アプリケーションのインスタンスの識別子及び移动通信装置のハードウェアの識別子から、その移动通信装置のアプリケーションのインスタンスの一意の移动通信装置識別情報を生成し、移动通信装置のアプリケーションで記憶するために一意の移动通信装置識別情報を送信するように構成することができる。

40

【0014】

[0013]一実施形態の方法は、一人のユーザについて、移动通信装置の移动通信装置アプリケーションのインスタンスを識別する移动通信装置識別情報を含む移动通信装置情報と、移动通信装置識別情報に関連付けられた支払い口座情報及びユーザ検証情報と、を含むユーザ情報を、記憶システムの記憶部に安全に記憶するステップと、取引システムから、取引額情報、移动通信装置識別情報、及びユーザ検証情報を含む第1の取引許可要求メッセージを記憶システムで受信するステップと、受信したユーザ検証情報が、取引許可要求

50

で識別される移動通信装置について記憶されているユーザ検証情報と一致するかどうかを記憶システムで判定し、受信したユーザ検証情報が記憶されたユーザ検証情報と一致する場合には、記憶システムが、記憶部から、移動通信装置識別情報に関連付けられた支払い口座情報を検索するステップと、記憶システムが、取引額情報及び支払い口座情報を含む第2の許可要求メッセージを許可システムに送信するステップと、記憶システムが、許可システムから第2の許可メッセージに応答する第1の許可応答メッセージを受信すると、支払い口座情報を特定することなく第2の許可応答メッセージを取引システムに送信させるステップと、を含むことができる。

#### 【0015】

[0014]一実施形態の方法は、登録サーバによって行われる、移動通信装置のアプリケーションと通信して、移動通信装置のハードウェアの識別子と、移動通信装置のアプリケーションのインスタンスの識別子とを識別するステップと、アプリケーションのインスタンスの識別子及び移動通信装置のハードウェアの識別子から、その移動通信装置のアプリケーションのインスタンスの一意の移動通信装置識別情報を生成するステップと、移動通信装置のアプリケーションで記憶するために一意の移動通信装置識別情報を送信するステップと、を含むことができる。

10

#### 【0016】

[0015]一実施形態は、ユーザの支払い口座の詳細が商店システムに提供されることなく取引を商店システムで行うことを可能にし、支払いは、安全な記憶システム、商店端末装置、及び移動通信装置のアプリケーションの対話を通じて実行される。

20

#### 【0017】

[0016]添付図面を参照して単なる例として実施形態を説明する。

#### 【図面の簡単な説明】

#### 【0018】

【図1】取引システムの一実施形態の概要を示す概略図である。

【図2A】例示的な商店端末装置(MTD)の概略図である。

【図2B】例示的なMTDの機能構成要素の概略ブロック図である。

【図3A】例示的な移動通信装置(MCD)の概略図である。

【図3B】例示的なMCDの機能構成要素の概略ブロック図である。

【図4】商店システムの概略図である。

30

【図5】例示的なホストシステムの概略図である。

【図6】例示的な記憶システムの概略図である。

【図7】取引の流れの一部を説明する流れ図である。

【図8】初期化処理を説明する図である。

【図9】処理の流れの代替図である。

#### 【発明を実施するための形態】

#### 【0019】

[0026]図1は、本発明を実施するシステムの例示的構成の概要を示す。例示的な実施形態は、顧客(ユーザ)と商店の双方に体感される使用の平易性と柔軟性を提供し、同時に動作の安全性と保全性を提供することができる。例示的な実施形態は、顧客の移動通信装置と商店システムの間の通信を可能にして、顧客が支払いカードを商店に提示する必要なしに、顧客と商店間の取引を支援する。

40

#### 【0020】

[0027]図1は、本発明の一実施形態を実施するシステムの例示的構成の概要を示す概略図である。本例の支払いサービスシステム24は、ここではホスト22-1~22-Nと表す複数のホストシステム(「取引システム」とも称する)22と、ここでは1つの保管システム10として表される1つ又は複数の保管システム(「記憶システム」とも称する)10とを備える。

#### 【0021】

[0028]図の例では、保管システム10は、保管処理ロジック(VPL)を実行する1つ

50

又は複数の保管部プロセッサ16と、暗号化された情報を保持する安全な保管記憶部12とを備える。さらに、記憶部14は、VPLを定義し、(1つ又は複数の)保管部プロセッサ16の動作を制御するために使用されるソフトウェア及びデータを備える。(1つ又は複数の)保管部プロセッサ16は、保管部—ホストインターフェース(VHI)18を介して安全なチャンネル21を通じてホストシステム22—1~22—Nと通信するように動作する。安全なチャンネル21は、直接の2地点間通信リンクを介するか、又は従来の2地点間通信技術を使用してネットワークを通じて確立される2地点間リンクを介して、2地点間チャンネルとして実装することができる。

#### 【0022】

[0029]図の例では、保管システムインターフェース(VSI)20は、保管システム10の(1つ又は複数の)保管部プロセッサ16と、加盟店銀行システム30などの外部システムとの間に安全な通信チャンネルを提供し、加盟店銀行システム30はさらに他のリンクでカード体系システム32—1~32—Nに、又は直接カード体系システム32—1~32—Nに接続される。カード体系システム32—1~32—Nは、さらに他の安全なリンクを介して、カード体系下で個々のカードを発行する役割を担う発行銀行34—1~34—Nのシステムに接続される。別の例では、VSI20は、例えばカード支払い方式を使用しない支払いの場合には、銀行間の転送のために銀行システム34—1~34—Nに直接接続することもできる。

#### 【0023】

[0030]例示的な実施形態では、ホストシステム22は、1つ又は複数の商店システム400の商店端末装置26に接続するように動作する。図1は、安全なリンク25を介して個々の商店端末装置(MTD)26—1~26—Nに直接接続されたホストシステム22—1を示す。図1に示す例示的な実施形態では、ホストシステム22—1は実質的に仮想販売時点情報管理(VPOS)システムとして動作し、商店端末装置26—1~26—Nは、情報の取得と提示のために個々の商店の従業員が保持する入力装置として機能する。商店端末装置26—1~26—Nは、例えば、タブレット型のコンピューティング装置から構成することができる。商店端末装置への接続は、例えば、ネットワーク(例えばインターネット又は商店にとってローカルなネットワーク)を通じて安全なチャンネルを介して直接の2地点間接続として確立することができる。或いは、後に図4を参照して説明するように商店端末システムを介して接続を確立してもよく、商店端末システムは、安全なチャンネルを介してホストシステム22—1に接続される。代替実施形態では、ホストシステム22—1は、そのような安全なチャンネルを介して商店システムと通信することもでき、商店システムは、商店サーバシステムと、例えば商店サーバシステムによってホスト22—1に接続された1つ又は複数の従来の販売時点情報管理装置(キャッシュレジスタ)を含むことに留意されたい。

#### 【0024】

[0031]図1には登録サーバ24も示し、これは、(1つ又は複数の)安全なチャンネル29を介して(例えば、携帯電話網、又は例えばインターネット、又は両者の組み合わせを介して)移動通信装置28と通信するように動作することができる。

#### 【0025】

[0032]本発明の例示的な実施形態では、スマートフォンなどの移動通信装置(MCD)28の使用を通じて顧客と商店の間で取引を行うことができる。以下の記述で説明するように、任意でホスト22—1と移動通信装置28間の帯域外通信チャンネル27を使用して、顧客の移動通信装置28と商店の商店端末装置26の間で情報交換を行うことができる。

#### 【0026】

[0033]図2Aは、タブレット形態の商店端末装置(MTD)26の概略図である。タブレット26は、タッチパッド207を備えたディスプレイ206、1つ又は複数のカメラ208(例えば、カメラをタブレットの前部及び／又は後部及び／又は側面に設けることができる)、及び1つ又は複数のスイッチ210(例えば、1つ又は複数のスイッチをタブレット26の前部及び／又は後部及び／又は側面に設けることができる)を含む。

## 【0027】

[0034]図2Bは、そのようなタブレット26に備えられる機能要素の概略図である。タブレット26は、1つ又は複数のプロセッサ202、並びに、揮発性メモリ（例えばRAM）及び不揮発性メモリ（例えばフラッシュメモリ、ROM等）を含むことが可能な1つ又は複数のメモリ装置204を含む。

## 【0028】

[0035]メモリ204は、タブレット26の（1つ又は複数の）プロセッサ202を制御するためのプログラム及びデータを保持する。タブレット26は、ディスプレイ206と、商店が当業者によく理解される方式で情報を入力し、ディスプレイ206に表示された情報を選択するためのタッチパッド207と、を含む。

10

## 【0029】

[0036]1つ又は複数のカメラ208は、視覚的に提示される情報（例えばバーコード、QRコード（登録商標）等）を取り込むために使用することができる。1つ又は複数のスイッチ210は、タブレットのオン／オフを切り替える、使用モードを選択する、アプリケーションを起動及び／又は終了する等のハード機能の制御に使用することができる。

## 【0030】

[0037]1つ又は複数のアンテナ214に接続されたWi-Fi（登録商標）及び／又はBluetooth（登録商標）トランシーバ212を使用して、タブレットと基地局間、及びタブレットと他の装置（例えば顧客の移動通信装置28）間のワイヤレス通信を可能にすることができる。任意で、タブレットは、RFIDアンテナ222に接続された内蔵無線周波識別（RFID）インターフェース220も備えることができる。RFIDインターフェース220を使用してRFIDコードを別の装置に提示したり、他の装置及び／又は読み取り対象の商品に設けられたRFIDコードを読み取るように構成したりすることができる。

20

## 【0031】

[0038]タブレット26は、他のセンサ及びインターフェース、例えばGPSアンテナ226に接続された全地球測位衛星ロジック（GPSロジック）224も含むことができる。必要な場合は、外部スピーカに接続するオーディオジャック230に音声コーデック228を接続することができる。各種の他のセンサを使用してタブレットが場所及び／又は動きに反応するようにすることができ、そのようなセンサには例えば磁気センサ232、加速度計（加速度センサ）234、ジャイロ스코プ（ジャイロ）センサ236が含まれる。タブレット26には、内蔵バッテリー240、又はコネクタ242から供給される外部電力で電力を供給することができ、バッテリー240及びコネクタ242は、電力管理集積回路（PMIC）／ユニバーサルシリアルバス（USB）インターフェース238に接続される。

30

## 【0032】

[0039]図3Aは、移動通信装置（MCD）28の概略図である。移動通信装置28は、タッチパッド307を備えたディスプレイ306、1つ又は複数のカメラ308（例えば移動通信装置の前部及び／又は後部にカメラを設けることができる）、及び1つ又は複数のスイッチ310（例えば、1つ又は複数のスイッチを移動通信装置28の前部／後部及び／又は側面に設けることができる）を含む。

40

## 【0033】

[0040]図3Bは、そのような移動通信装置28に備えられる機能要素の概略図である。移動通信装置28は、1つ又は複数のプロセッサ302と、揮発性メモリ（例えばRAM）及び不揮発性メモリ（例えばフラッシュメモリ、ROM等）を含む1つ又は複数のメモリ装置304とを含む。

## 【0034】

[0041]メモリ304は、通信装置28の（1つ又は複数の）プロセッサ302を制御するためのプログラム及びデータを保持する。特に、移動通信装置は、移動通信装置を使用して取引を行うための取引アプリケーション（以下では、移動通信装置アプリケーション

50

(MCDAPP) 305と称する)を含むことができる。移動通信装置28は、ディスプレイ306と、当業者にはよく理解される方式で顧客が情報を入力し、ディスプレイ306に表示された情報を選択するためのタッチパッド307とを含む。ディスプレイを使用して、視覚的に読み取り可能なコード、例えば、下記で説明するように、移動通信装置を識別する一意の移動通信装置識別情報を商店端末装置又は商店端末システムに提供するために使用される移動通信装置上のアプリケーションのインスタンスの一意の識別子を表すバーコードやQRコードを表示することもできる。

#### 【0035】

[0042] 1つ又は複数のカメラ308を使用して、視覚的に提示される情報(例えばバーコード、QRコード等)を取り込むことができる。1つ又は複数のスイッチ310は、移動通信装置のオン/オフを切り替える、使用モードを選択する、アプリケーションを起動及び/又は終了する等のハード機能の制御に使用することができる。

10

#### 【0036】

[0043] 1つ又は複数のアンテナ314に接続されたWi-Fi及び/又はBluetoothトランシーバ312を使用して、移動通信装置と基地局間、及び移動通信装置と他の装置(例えば商店端末装置26)間のワイヤレス通信を可能にすることができる。任意で、移動通信装置は、適切なRFIDアンテナ322に接続された内蔵無線周波識別(RFID)インターフェース320も備えることができる。RFIDインターフェース320を使用してRFIDコードを別の装置に提示したり、他の装置及び/又は読み取り対象の商品に設けられたRFIDコードを読み取るように構成したりすることができる。

20

#### 【0037】

[0044] 1つ又は複数のアンテナ318に設けられるセルラトランシーバ316は、移動通信装置が移動遠隔通信ネットワーク(例えばセルラワイヤレスネットワーク)を介して通信できるようにするために提供される。

#### 【0038】

[0045] 移動通信装置28は、他のセンサ及びインターフェース、例えばGPSアンテナ326に接続された全地球測位衛星ロジック(GPSロジック)324も含むことができる。必要な場合は、外部スピーカに接続するオーディオジャック330に音声コーデック328を接続することができる。各種の他のセンサを使用して移動通信装置が場所及び/又は動きに反応するようにすることができ、そのようなセンサには、例えば、磁気センサ332、加速度計(加速度センサ)334、ジャイロスコープ(ジャイロ)センサ336が含まれる。移動通信装置28には、内蔵バッテリー340、又はコネクタ342から供給される外部電力で電力を供給することができ、バッテリー340及びコネクタ342は、電力管理集積回路(PMIC)/ユニバーサルシリアルバス(USB)インターフェース338に接続される。

30

#### 【0039】

[0046] 図4は、商店側の例示的構成の概略図である。この例では、1つ又は複数の商店端末装置26が、例えばWi-Fi基地局402とのWi-Fi接続を使用して無線通信することができる。Wi-Fi基地局402は商店サーバシステム404に接続され、商店サーバシステム404は安全な通信チャネルを介して図1に示すホストシステム22に接続される。この例では、例えば個々の商店端末装置26がRFIDインターフェースを備えない場合に使用するために、1つ又は複数のRFID読み取り機406を提供し、商店サーバシステム404に接続することができる。図4に示すように、顧客の移動通信装置28は商店システムのWi-Fi基地局にも接続することができ、それにより移動通信装置をホストシステム22に接続することを可能にすることが想定される(例えば、Wi-Fi基地局及び商店のサーバシステムを介してホストシステム22との間に安全なチャネル27を確立することにより)。

40

#### 【0040】

[0047] 顧客の移動通信装置28と商店端末システムの接続は各種方式で実現することができる。例えば、移動通信装置アプリケーション305が移動通信装置のジオロケーショ

50

ン機能を使用するように構成して（移動通信装置のW i F i、G P S、セルラ、及び加速度計／ジャイロ／磁気機能の1つ又は複数を使用する）移動通信装置の現在の位置を認識し、予め記憶された情報（例えばある地理的位置に紐付けされたS S I D及びパスフレーズ）を使用して、商店の構内にあるW i F i 基地局4 0 2に自動的に接続し、次いで商店システム4 0 4及び／又はホストシステム2 2への安全な接続を確立することができる。任意で、移動通信装置のディスプレイで指示を受信することにより基地局4 0 2への接続を承認するように顧客に促すことができ、顧客が接続に対して肯定の同意をした時にのみ接続が確立される。事前に記憶された情報に応答して自動的に接続するのに加えて、又はそれに代えて、一例では、商店の構内にあるW i F i 基地局4 0 2に接続するための情報は、顧客が商店の構内でR F I Dタグ又は表示された視覚コード（例えばバーコード、Q Rコード）を読み取ることによりS S I D及びパスフレーズを受け取るのに応答して実現することもでき、R F I Dタグ又は表示された視覚コードが、基地局4 0 2に接続するためのS S I D及びパスフレーズを提供する。

10

#### 【0041】

[0048]一例では、各商店端末装置がそのような視覚コード及び／又はR F I Dタグを備え、それを顧客の移動通信装置2 8のカメラ3 0 8又はR F I Dインターフェース3 2 0を使用して移動通信装置アプリケーションで読み取ることができる。商店端末装置2 6の視覚コード及び／又はR F I Dタグは、消費者の移動通信装置を商店のネットワークに無線接続するための情報を提供するだけでなく、顧客の移動通信装置2 8を商店端末装置2 6に接続できるようにして、顧客の移動通信装置2 8とその商店端末装置2 6間の取引を可能にするように構成することができる。

20

#### 【0042】

[0049]さらに他の例では、顧客の移動通信装置2 8とホストシステム2 2間の通信は、例えば携帯電話網を介して帯域外チャンネル2 7を使用して実施することができる。そのような例では、商店端末装置が商店端末装置2 6を識別する視覚コード及び／又はR F I Dタグを備えて、ホスト2 2を介して顧客の移動通信装置2 8を商店端末装置2 6に接続できるようにして、顧客の移動通信装置2 8とその商店端末装置2 6の間で取引を行えるようにすることができる。そのような例では、第1の安全なチャンネル2 5を介して商店端末装置2 6をホストシステム2 2に接続し、顧客の移動通信装置を、安全な帯域外チャンネル2 7を介してホスト2 2に接続することができ、商店端末装置と移動通信装置2 8間の接続は、移動通信装置アプリケーション3 0 5が商店端末装置2 6の視覚コード又はR F I Dタグから読み取られた情報（カメラ3 0 8及び／又はR F I Dインターフェース3 2 0を使用して）をホストシステム2 2に提供し、ホストシステム2 2が移動通信装置2 8と商店端末システム2 6の間の接続を確立することによって確立される。

30

#### 【0043】

[0050]安全な帯域外チャンネル2 7を介して顧客の移動通信装置2 8とホストシステム2 2の間に通信を提供するさらに他の例は、移動通信装置2 8に担持され、移動通信装置アプリケーションインスタンスの一意の移動通信装置識別情報を表す視覚コード及び／又はR F I Dタグを商店端末システム2 6で読み取ることによって実施することができる。移動通信装置2 8が担持する視覚コード及び／又はR F I Dタグは、商店端末装置2 6のカメラ2 0 8及び／又はR F I Dインターフェース2 2 0で読み取ることができる。そのような例では、商店端末装置2 6と移動通信装置2 8間の接続は、商店端末装置2 6が、移動通信装置2 8の視覚コード又はR F I Dタグから読み取った情報を安全なチャンネル2 5を介してホストシステムに提供することによって確立することができる。そして、ホストシステムは、例えば保管記憶部1 2又は商店端末装置のホスト2 2の記憶部に記憶された情報から、移動通信装置への帯域外チャンネルを特定する情報（例えば移動通信装置の携帯電話番号）を検索することができる。そして、ホストは検索した情報を使用して、商店端末システム2 6と移動通信装置2 8の間に接続を確立することができる。

40

#### 【0044】

[0051]図5は、ホストシステム2 2の概略図である。ホストシステム2 2は、図で識別

50

する安全なチャネル 25、27、及び 21 の確立を可能にする 1 つ又は複数のインターフェースを備えた 1 つ又は複数の従来のコンピュータサーバとして構成することができる。ホストシステム 22 は、1 つ又は複数のプロセッサ 510、ホストシステム機能を行うようにプロセッサ 520 を設定するためのデータ及びソフトウェアを保持するメモリ 520、並びにホストシステム 22 を制御するためのプログラム及びデータの恒久的な記憶を提供するデータストア 530 を含むことができる。メモリ 520 及び／又は記憶部 530 に保持されるソフトウェアは、例えば 1 つ又は複数のコンピュータプログラムによって実装される仮想販売時点情報処理（VPOS）モジュール 522 を含むことができ、これは、特に商店端末装置が情報を入出力するための単純な端末で、従来の販売時点処理機能をホストシステム 22 で行うべき場合に、商店端末装置の販売時点動作を行う。

10

#### 【0045】

[0052] VPOS モジュール 522 は、商店の構内でプリンタ（図示せず）を使用して受領書を印刷する、商店端末 26 又は顧客の移動通信装置 28 にダウンロード可能な受領証ファイルを生成する等の販売時点処理機能を提供するように構成することができる。VPOS モジュール 522 は、取引の許可や事前許可、取引の無効化、取引の返金処理、チップ（tip）管理、プロファイル管理、音声照会や報告の生成等の従来の販売時点機能を提供するように動作することができる。例示的实施形態では、VPOS モジュール 522 は、支払い処理モジュール 524 を使用して、許可、事前許可の無効化、及び返金処理等の取引処理を実施するように動作する。

#### 【0046】

20

[0053] 例えば 1 つ又は複数のコンピュータプログラムによって提供される支払い処理モジュール 524 は、移動通信装置 28 及び／又は商店端末装置 26 を使用して行われる動作に応答して取引処理を行う機能を提供する。支払い処理モジュール 524 は、有効な顧客の資格証明の検証、許可要求の処理、無効化要求の処理、返金要求の処理、音声照会要求の処理、事前許可要求の処理、一日の終わりの集計及び提出の処理、及び報告の処理、例えば記録及び日誌並びに／又は営業報告の生成の機能を提供するように構成することができる。支払い処理の態様のさらなる詳細は後述する。

#### 【0047】

[0054] 図 6 は、保管システム（安全な記憶システム）10 の概略ブロック図である。保管システム 10 は、1 つ又は複数のプロセッサ 16、暗号化された顧客レコード 612 を保持する安全な保管記憶部 12、及び（1 つ又は複数の）プロセッサ 16 を制御するためのソフトウェア及びプログラムを記憶するために使用される記憶部／メモリ 14 を備える。そのような顧客レコードの内容の例は下記で説明する。記憶部 14 に保持される処理モジュールは、例えば 1 つ又は複数のコンピュータプログラムにより実装される、保管記憶部 12 に保持されたデータを暗号化及び解読する暗号化モジュール 622 と、1 つ又は複数のコンピュータプログラムによって実装される、ホストシステム 22 との通信で要求及び応答を処理する要求処理モジュール 624 とを含むことができる。

30

#### 【0048】

[0055] 取引管理機能、報告生成機能、商店管理機能、端末フリート（fleet）管理機能、顧客管理機能等の機能を実装するさらに他の処理モジュール 626 も提供することができる。取引管理機能は、例えば、資格証明検証機能、一日の終わりの清算及び提出機能、顧客登録機能、顧客変更及び／又は登録削除機能を含むことができる。報告生成機能は、記録や日誌の生成及び営業報告の生成を含むことができる。商店管理機能は、商店のプロファイル管理や記録及び日誌及び／又は営業報告の生成を含むことができる。端末フリート管理機能は、同様に、端末プロファイル管理機能、端末の設置を制御する機能、端末のアップグレード及び端末の撤去、記録及び日誌及び／又は営業報告を生成する報告生成機能を含むことができる。顧客管理機能は、顧客のプロファイル管理、移動通信装置のアプリケーション ID の生成を含むことができる。これら処理の一部の態様のさらなる詳細については後述する。

40

#### 【0049】

50

[0056]図6に示すように、保管部－ホスト間インターフェース18は、1つ又は複数のホスト22への安全なチャンネルを支援し、保管システムインターフェース20は、加盟店銀行30及び／又はカード体系システム32への1つ又は複数のチャンネルを支援する。

【0050】

[0057]図7は、安全なチャンネル29を介して（携帯電話網又は例えばインターネット、又は両者の組み合わせを介して）移動通信装置28と通信するように動作する登録サーバ24を使用した例示的な登録処理を示す。

【0051】

[0058]図7に示すように、登録処理は、顧客が移動通信装置アプリケーションのダウンロードを要求することによって開始することができる。アプリケーションをダウンロードする要求は、移動通信装置の提供者のアプリケーションストアを介するか、又は直接登録サーバ24に行われる。したがって、ステップ42で、移動通信装置が、要求した移動通信装置アプリケーションを受信する。移動通信装置アプリケーションは、ユーザ登録のために登録サーバ24と対話するように構成されたユーザ登録サービス等の種々のサービスを提供する。移動通信装置アプリケーションは、登録用の公開鍵／秘密鍵の対に関連付けられた公開鍵を提供されるか、又はその記録を含み、その公開鍵に対応する秘密鍵は登録サーバ24で保持される。移動通信装置アプリケーションは、アプリケーションのインスタンスを表す一意の番号も提供されるか、又はその記録を含むことができ、一意の番号は、ダウンロードの通し番号を形成するアプリケーションの通し番号、又はダウンロードの通し番号から導出されるアプリケーションの通し番号の形態でダウンロード処理の一部として生成される。登録用の公開鍵及び／又はアプリケーションの通し番号は、アプリケーションのメタデータとして移動通信装置の記憶部に保持することができる。

【0052】

[0059]ステップ44で、移動通信装置アプリケーションが移動通信装置28で起動される。

【0053】

[0060]ステップ46で、移動通信装置アプリケーションが、図で29として模式的に表される安全な通信チャンネルを使用して登録サーバ24との間に安全なチャンネル又はリンクを確立する。上記のように、これは携帯電話網又はインターネットを通じた有線接続を介して提供される安全なチャンネルとすることができる。チャンネルは、例えばセキュアソケットレイヤ（SSL）接続として、及び／又は、下記のように公開鍵／秘密鍵の対の使用により、セキュリティを確保することができる。

【0054】

[0061]ステップ48で、移動通信装置アプリケーションはユーザにデータ入力画面を提供するように動作して、ユーザが電子メールアドレスと登録検証情報（すなわち登録処理に使用する検証情報）を、パスワード、パスフレーズ、又は他の形態の検証情報（例えば移動通信装置で入力されるジェスチャ）の1つ又は複数の形態で入力できるようにする。次いで、移動通信装置アプリケーションは、移動通信装置から、移動通信装置のハードウェアを識別するハードウェア情報を検索するように動作する。ハードウェア識別情報は、例えば、移動通信装置の国際モバイル機器識別（IMEI）、移動通信装置から取得される加入者識別モジュール（SIM）の集積回路カードID（ICCID）、又は移動通信装置のメディアアクセス制御（MAC）アドレスの1つ又は複数である。移動通信装置アプリケーションは次いで公開鍵を使用して、ユーザから入力された情報とハードウェア識別情報を暗号化するように動作し、それにより生成された安全なメッセージが登録サーバに送られる。セキュリティが保護されたメッセージの一部として、移動通信装置アプリケーションは、移動通信装置アプリケーションの特定のインスタンス（ダウンロード）を識別する情報を登録サーバに送信するように動作することもできる。これに代えて、又はこれに加えて、登録サーバは、移動通信装置アプリケーションによって開始されたセッションに一意の識別子を割り当てて移動通信アプリケーションを識別するように動作してもよい。

10

20

30

40

50

## 【0055】

[0062]安全なメッセージを受信すると、登録サーバは、登録サーバで保持されている秘密鍵を使用してメッセージを解読し、ユーザによって入力された電子メールアドレスと登録検証情報を抽出し、例えばユニフォームリソースロケータ（URL）の形態のリンクを、ユーザから提供された電子メールアドレスでユーザに送信される電子メールでユーザに送信するように動作することができる。上記リンクは、SSL又は他の安全な接続を使用してユーザアカウントの設定情報を提供することが可能な、登録サーバ24で提供される安全な登録用ウェブサイトを識別する。それに代えて、登録サーバは、2つのリンクを含む電子メールを送信してもよく、一方のリンクが移動装置から受信されるメッセージの有効性を確認し、第2のリンクは要求を拒否する。

10

## 【0056】

[0063]リンクを定義する情報をユーザが受信すると、ユーザは移動通信装置又は別の装置からそのリンクを使用して、登録サーバが提供する安全な登録ウェブサイトにアクセスし、登録情報を入力することができる。登録情報の入力が可能になる前に、ユーザは上記ステップ48で提供した電子メールアドレスと登録検証情報を移動通信装置アプリケーションを介して入力することができる。正しいユーザ名と登録検証情報が入力されると、安全なウェブサイトは従来の方式でページ及びフィールドを提供し、それらを使用して、電子メールアドレスで識別されるユーザアカウントとの関連で情報を入力することができる。登録情報は、電子メールアドレスで識別されるアカウントと関連付けてシステム10に記憶される1つ又は複数の支払い口座についての支払いの詳細を含む。例えば、クレジットカードについての支払い口座の詳細は、クレジットカード番号、クレジットカードに関連付けられたフルネーム、有効期限、カード検証値（CVV）を含むことができる。ユーザがアカウントを識別し、その後の入力を迅速に行うための簡略法として、各支払い口座にニックネームを関連付けることができる。種々の支払い口座の例には、クレジットカード、デビットカード、PayPalアカウント、銀行口座等がある。登録情報は、ユーザを識別する個人情報（例えばファーストネーム、ミドルネーム、及び名字、国籍、在住国等）や、ユーザの連絡先情報（自宅の住所（複数可）、職場の住所（複数可）、追加的な電子メールアドレス（複数可）、固定電話及び／又は携帯電話番号等）も含むことができる。登録情報は、顧客検証用のパスフレーズ等の顧客検証情報も含むことができる。顧客検証情報は登録検証情報と同じであってもよい。或いは、セキュリティを高めるために顧客検証情報が登録検証情報と異なることを要求してもよい。

20

30

## 【0057】

[0064]この情報が移動通信装置アプリケーションから提供される場合、この情報をさらに公開鍵で暗号化し、公開鍵を使用して登録サーバで解読することができる。移動通信装置の電子財布を、支払い口座用のニックネームで更新することもできる。

## 【0058】

[0065]ステップ50で、登録サーバは、数学的計算を行って、移動通信装置の移動通信装置アプリケーションのインスタンスを識別する情報を生成することができる。移動通信装置の移動通信装置アプリケーションのインスタンスを識別する情報は、一意の移動通信装置アプリケーションID（MCDA PID）の形態とすることができる。数学的計算では、例えば、移動通信装置ハードウェアの識別子及び移動通信装置アプリケーションインスタンスの識別を使用して（例えば2つの識別子の固定された組み合わせ、又は無作為の代数的若しくはアルゴリズム的組み合わせ）、一意の移動通信装置アプリケーションID（MCDA PID）を生成することができる。計算で使用する移動通信装置アプリケーションインスタンスの識別は、例えば、上記のように移動通信装置のダウンロード処理の一部として生成されるアプリケーションの通し番号（例えばダウンロード通し番号）、又はそのユーザの登録処理の時間及び／又は場所及び／又は順番（他のユーザについての他の登録処理に対して）に基づいてユーザに割り振られる一意の番号とすることができる。

40

## 【0059】

50

[0066]そして、ステップ52で、この一意のMCDA P P I Dが、その後MCDアプリケーションがバーコードやQRコード又は他の視覚コードの生成に使用できる番号として、又はコードそのものとして、移動通信装置に送信される。コードを使用して、RFIDタグ320を備える移動通信装置28（図3B参照）についてRFIDタグをそのコードでプログラムすることもできる。一意のMCDA P P I Dは、安全な電子メールとして、又は情報のパケットとして移動通信装置に送信することができ、MCDA P P I Dを開くために登録検証情報の入力进行を要求することができる。MCDA P P I Dは、移動通信装置アプリケーションのメタデータとして移動通信装置の記憶部に記憶される。

#### 【0060】

[0067]ステップ54で、登録サーバは、保管システム10との間に安全な接続を確立し、入力された情報を保管部プロセッサに供給して、レコード及び／又は顧客アカウント識別子の一部としてMCDA P P I Dを使用して、顧客の安全なレコードを設定する。安全な接続を提供するために、登録サーバに保管部の公開鍵／秘密鍵の対の公開鍵を提供することができ、秘密鍵は保管システムで保持される。したがって、登録サーバは保管部の公開鍵を使用して保管システムに送信される情報を暗号化することができ、保管システムはその秘密鍵を使用して情報を解読することができる。

#### 【0061】

[0068]ステップ56で、例えば移動通信装置28のユーザと登録サーバ24との間の登録セッションの一部として提供及び／又は生成された顧客及びMCDに関連するデータが、保管部12で安全なレコードに入れられる。情報は、上記のように初回の登録処理の一部として顧客から提供されるか、又は別個のセッション、例えば顧客のコンピュータ（図示せず）と登録サーバ24間の別個のセッションの一部として得ることができる。顧客について安全なレコードに保持される情報には、移動通信装置の移動通信装置アプリケーションのインスタンスを識別する移動通信装置の識別情報（例えばMCDA P P I D）等の移動通信装置情報が含まれる。移動通信装置情報は、移動通信装置のアクセス情報、例えば、携帯電話番号、電子メールアドレス、移動通信装置との通信に使用できるソーシャルメディアの識別情報、移動通信装置のアプリケーションのアプリケーション識別子（例えばMCDA P P）、又は移動通信装置との通信を可能にする他の情報も含むことができる。顧客についての安全なレコードに保持される情報は、移動通信装置の識別情報に関連付けられた支払い口座情報及び顧客検証情報も含むことができる。

#### 【0062】

[0069]登録処理の一部として顧客（ユーザ）から提供及び／又は登録処理の一部として生成することができ、保管記憶部12に保持される顧客の安全なレコード612の一部を形成することが可能な情報の例は、以下の1つ又は複数を含む。

- ・MCDA P P I D
- ・ユーザの見出し
- ・ユーザ名
- ・ユーザの電子メールアドレス
- ・ユーザの連絡先住所
- ・移動通信装置の連絡番号（例えば携帯電話番号）
- ・他の連絡先電話番号（複数可）
- ・1つ又は複数の支払い口座についての情報
- ・ユーザの検証用パスフレーズ及び／又はPIN
- ・他の検証情報
- ・ユーザ設定
- ・ユーザの国籍
- ・パスポート又は他の身元を特定する文書の情報

#### 【0063】

[0070]ここに記載する実施形態では、保管記憶部12の安全な顧客レコードに保持される移動通信装置情報が移動通信装置のアクセス情報を含むが、他の例では、それに代えて

、又はそれに加えて、移動通信装置のアクセス情報は、該当するセキュリティ要件に応じて、記憶部 14、ホストシステム 22、登録システム 24、又は他の場所の 1 つ又は複数で、移動通信装置の識別情報に関連付けられたレコードに保持することもできる。

#### 【0064】

[0071] 支払い口座についての情報は、例えば、クレジットカードの口座、デビットカードの口座、銀行口座等の支払いカードの口座を識別することができ、有効期限、カード検証値 (C V V) 又はカード検証コード (C V C) とともに称されるカードセキュリティコード (C S C) 等、支払い口座を使用した許可と支払いを可能にする情報を含む。

#### 【0065】

[0072] 顧客設定情報は、例えば、2 つ以上の支払い口座についての情報が提供される状況で優先される口座の自動的な識別を含むことができる。顧客設定情報は、例えば、商店の現地通貨、任意の支払い口座に対応するカード発行者の自国通貨、又は所与の状況における別の通貨で支払いを行えるように設定することもできる。顧客設定情報は、顧客が非課税の購入を行うことが可能な国にいる時に非課税の購入の選択肢を考慮するように設定することもできる。

10

#### 【0066】

[0073] 一例では、顧客検証用のパスフレーズは、所定の最小の長さとし、所定の最大の長さの間の長さの英数文字列 (単なる例として 4 ~ 16 文字の間、例えば 12 文字) を含むことができる。顧客が、取引を行うために移動通信装置の正当な使用を確認することが要求される検証プロセスで、パスフレーズの文字から無作為に選択された文字群 (例えば 12 文字のうち 4 文字) を顧客が入力する必要があるようにデフォルトを設定することができる。顧客が入力を要求されるパスフレーズの長さとし、文字数は、望ましい特定のセキュリティレベルに応じて選択することができ、顧客の検証を目的とする 12 文字のパスフレーズとそこからの 4 文字の無作為の選択の例に限定されないことが理解されよう。

20

#### 【0067】

[0074] 任意で、顧客は、移動通信装置の正当な使用を検証するために、顧客の検証用パスフレーズ全体及び／又は P I N 全体の 1 つ若しくは両者、又は 1 つ若しくは両者の一部分を要求することによって所望のセキュリティの度合いを選択することができる。他の可能な検証情報、例えば、移動通信装置で入力される一連のジェスチャや、チャレンジの質問と回答の対なども記憶することができる。

30

#### 【0068】

[0075] 登録処理の一部として入力される情報は、保管記憶部 12 で安全に保持され、記憶部 14 に保持される保管処理ロジックの制御下で (1 つ又は複数の) 保管部プロセッサ 16 からのみアクセスすることができる。

#### 【0069】

[0076] 保管記憶部 12 に保持されるデータは、適切な暗号化標準を使用してセキュリティ保護する。例示的实施形態では、記憶システムに記憶されるデータは A E S (Advanced Encryption Standard) 仕様を使用して暗号化され、外部の専用装置により公開鍵／秘密鍵の対が周期的に生成される。例示的实施形態では、安全なチャネル 21 及び 19 は専用の私設回線を使用するように設定され、インターネットプロトコルセキュリティ (I P S E C) に関連するプロトコルを使用して暗号化される。例示的实施形態では、安全なチャネル 25、27、及び 29 は公衆回線を使用し、セキュアソケットレイヤ (S S L) プロトコルを使用して暗号化される。他の実施形態では、異なるセキュリティ標準、例えば、今後開発及び／又は、例えば規制機関から要求されるセキュリティ標準を使用することが理解されよう。

40

#### 【0070】

[0077] 図 8 は、本明細書に記載されるシステムを使用して取引を行う方法の例を説明する流れ図である。

#### 【0071】

[0078] ステップ 62 で、顧客が購入しようとする商品の商品識別子を商店の商店端末装

50

置 26 で入力することができる。商品識別子は、商店端末装置で提示されるキーボードを使用して手動で情報を入力する、又は商品に設けられた R F I D タグをスキャンする、又は商品表面にバーコード、Q R コード、若しくは他の形態の視覚コードとして表された商品コードをスキャンすることにより入力することができる。

#### 【0072】

[0079] ステップ 64 で、顧客の移動通信装置 28 を商店端末装置に提示することができる。これは、商店端末装置 28 で移動通信装置 28 に表示されたコードを手動で入力する、又は移動通信装置 28 に表示されたバーコード、Q R コード、若しくは他の視覚コードをスキャンする、移動通信装置 28 の内部又は表面に設けられた R F I D タグを読み取る、又は例えばネットワークプロトコルを介して、又は S M S 及び／若しくは電子メールを使用してデータを交換することにより実現することができる。上記のように、移動通信装置から提供されるコードは、移動通信装置で保持される取引アプリケーションのインスタンスを識別する情報と移動通信装置のハードウェアを識別する情報とから生成できる一意のコードである。この一意のコードは、移動通信装置の当該インスタンスを含む移動通信装置の一意の識別子（一意の移動通信装置識別情報）を提供する。

10

#### 【0073】

[0080] ステップ 66 で、商店端末装置が、移動通信装置の検証情報を求める要求をホストシステム 22 に送信する。ホストに送信される要求は、移動通信装置から提供された一意の移動通信装置識別情報を含んでいる。商店端末装置は、例えばホスト公開鍵／秘密鍵の対の公開鍵を使用してこの通信を暗号化された通信として行うことができ、秘密鍵はホストシステム 22 でセキュアに保持される。そして、ホストシステム 22 は、ホストの公開鍵／秘密鍵の対の秘密鍵を使用して要求の内容を解読することができる。

20

#### 【0074】

[0081] ステップ 68 で、ホストシステム 22 は、一意の移動通信装置識別情報を使用して移動通信装置 28 を識別し、取引処理サービスで使用するために登録された移動通信装置であることを確認する。例示的实施形態では、この検証は、ホスト 22 が一意の移動通信装置識別情報を含むメッセージを保管システム 10 に送信して、顧客の検証情報を求める要求を提供して移動通信装置が正当な方式で使用されていることを確認するように保管システム 10 に要求することを含む。この検証情報の要求は、例えば、顧客と通信するために移動通信装置 28 にアクセスする方法の詳細を求める移動通信装置アクセス情報要求の一部として提供することができる。例示的实施形態では、どのように移動通信装置へのアクセスを得られるかを定義した情報である移動通信装置アクセス情報は、保管システム 10 の保管記憶部 12 に保持することができる。これに代えて、又はこれに加えて、この情報は例えばホストシステム 22、又は登録サーバ 24 などの別のシステムに保持することもできる。これらの通信も公開鍵／秘密鍵の対による暗号化を使用して行うことができる。

30

#### 【0075】

[0082] 上記で説明したように、例示的实施形態では、顧客が入力を要求される検証情報は、英数文字からなるパスフレーズから選択された英数文字とすることができる。一例では、顧客レコードの一部である安全な保管記憶部は 12 文字のパスフレーズを含むことができ、顧客に 12 文字から無作為に選択した 4 文字を入力するように要求することができる。

40

#### 【0076】

[0083] この例では、保管システム 10 からの返信に応答して、ホストシステム 22 はステップ 70 で、帯域外チャネル 27 を介して直接移動通信装置と通信するか、又は商店端末装置 26 と通信して、パスフレーズから選択された文字の入力を顧客に要求するように動作する。

#### 【0077】

[0084] ステップ 72 で、顧客の移動通信装置 28 又は商店の商店端末装置 26 が、顧客が入力した応答を受信する。

50

## 【0078】

[0085]ステップ74で、顧客の応答が、移動通信装置又は商店端末装置からホストシステム22に送信される。

## 【0079】

[0086]ステップ76で、ホストが許可要求を保管システム10に送信する。

## 【0080】

[0087]ステップ78で、保管システム10の保管処理ロジック16が許可要求を受信し、要求は一意の移動通信装置識別情報、顧客検証情報、及び取引額情報を含んでいる。保管処理ロジックは、一意の移動通信装置識別情報に基づいて保管記憶部12から顧客アカウント情報を検索するように動作し、顧客によって入力された検証情報が正しいことを確認するように動作する。一意の移動通信装置識別情報及び検証情報が保管記憶部12にセキュアに記憶されている情報に対応する場合、保管処理ロジックは、安全な記憶部12から、事前に顧客が保管システム10に登録した顧客アカウントを識別する情報を検索するように動作する。上記のように、顧客アカウントは、支払い口座（一般にはクレジットカード口座やデビットカード口座等の支払いカード口座と呼ばれる）の形態をとることができる。

10

## 【0081】

[0088]ステップ78で、保管処理ロジックはさらに、保管システムインターフェース20を介して、加盟店銀行システム30及び／又はカード体系システム32に許可要求を送信して、要求される支払い口座を使用して要求される取引額についての許可を要求するように動作する。

20

## 【0082】

[0089]ステップ80で、保管処理ロジック16が加盟店銀行システム30及び／又はカード体系システム32から肯定の許可応答を受信するものとする。

## 【0083】

[0090]ステップ82で、保管部は、ホスト22に許可応答メッセージを送信して、支払いについての許可を確定する。ただし、ホスト22に送信される許可メッセージは、支払いが行われる支払い口座を識別する必要はなく、代わりに、保管システム10によって支払いが許可されたことを知らせる。

## 【0084】

30

[0091]ステップ84で、ホストは、商店端末装置26（及び／又は移動通信装置28）に許可要求を送信する。商店端末装置26に送信されるメッセージは、支払いが行われる支払い口座は知らせず、単に、システム24が取引の実行を許可しており、支払いが行われることを確認する。

## 【0085】

[0092]ステップ86で、取引を終えることにより、商店端末装置及び／又は移動通信装置により取引を完了することができる。

## 【0086】

[0093]上記のように、情報が保管システム10に登録され、登録処理の一部として移動通信装置28の取引アプリケーションのインスタンスについて一意の移動通信装置識別情報を生成することができる。

40

## 【0087】

[0094]図9は、図1に示す各種の論理エンティティによって行われるステップを示す取引過程の例を説明する概略図である。

## 【0088】

[0095]この例では、ステップ102で、MTD26で取引が開始され、これは、例えば取引の基盤となる1つ又は複数の商品IDの入力を含む。ステップ104で、MCDA P P I DがMCD28からMTD26に提供される。

## 【0089】

[0096]ステップ106で、MCDA P P I Dについての検証情報を求める要求が生成さ

50

れてホスト 2 2 に送信される。

【0090】

[0097]ステップ 1 0 8 で、ホスト 2 2 が検証情報の要求を保管部 1 0 に送信する。ステップ 1 1 0 で、保管部 1 0 が M C D A P P I D の検証情報を抽出する。上記のように、検証情報は、パスフレーズから選択された何文字かを含むことができ、文字はパスフレーズから無作為に選択される。ただし、図 8 を参照して説明した例に関する変形例では、この例では、保管部 1 0 は、顧客に要求される情報及び予想される応答を指定したメッセージでホスト 2 2 に検証情報を返すように動作する。

【0091】

[0098]ステップ 1 1 2 で、ホスト 2 2 は検証情報を、M C D 2 8 に、又は図示していないが代替として M T D 2 6 に、提供する。

10

【0092】

[0099]ステップ 1 1 4 で検証要求が M C D 2 8 に表示される。

【0093】

[00100]顧客は、ステップ 1 1 6 で必要な検証情報を入力するように促され、検証情報がホスト 2 2 に送信される。

【0094】

[00101]この例では、ホスト 2 2 が、ステップ 1 1 8 で、顧客から提供された応答が予想される応答であるかどうかを検証する（保管システム 1 0 が行うのではなく）。

【0095】

20

[00102]顧客から提供された検証情報が保管システム 1 0 からホスト 2 2 に提供された予想される検証情報と一致しない場合は、任意でステップ 1 2 0 で顧客にステップ 1 2 0 の検証情報の入力を再試行する動作を与えることができる。

【0096】

[00103]その場合は、次いでステップ 1 2 2 で検証情報がホスト 2 2 でもう一度検査される。

【0097】

[00104]ステップ 1 2 2 で検証情報が正しくない場合は、取引を終了し、ステップ 1 2 4 で M T D 2 6 に、及び／又はステップ 1 2 6 で M C D 2 8 に、その旨のメッセージを送信することができる。

30

【0098】

[00105]図 4 ではステップ 1 2 0 で再試行が 1 回のみ行われるように示すが、代替実施形態では、検証情報の入力を再試行する選択肢をこれよりも多く、又は少なく顧客に提供することができる。検証情報が M C D 2 8 で要求されるのに代えて、代替実施形態では、M C D 情報の入力は顧客によって M T D 2 6 で実施することもできる。

【0099】

[00106]ステップ 1 1 8 又は 1 2 2 で検証情報が正しいと判定される場合は、許可要求メッセージがホスト 2 2 から保管システム 1 0 に送信されて、顧客の取引の許可を要求する。許可要求メッセージは、M C D A P P I D、取引額、及び顧客の検証応答を含む。

【0100】

40

[00107]ステップ 1 2 8 で、保管システム 1 0 は、M C D A P P I D を使用して、保管記憶部 2 2 から M C D A P P I D に関連付けられた支払い口座情報を検索するように動作する。

【0101】

[00108]ステップ 1 3 0 で、保管システム 1 0 は、許可を要求するために必要な支払い口座情報と、顧客が指定した通貨で許可すべき取引額とを含む許可要求を生成する。そして、この許可要求が、直接、又は加盟店銀行システム 3 0 を介してカード体系システム 3 2 に送られる。カード体系システム 3 2 は、支払い口座に対応する発行銀行 3 4 と通信した後で、許可メッセージを保管システム 1 0 に返すことができる。

【0102】

50

[00109]ステップ134で、受信された許可応答が許可が却下されたことを示す場合は、保管部は却下メッセージをホスト22に送信する。

【0103】

[00110]この場合、ホスト22は次いでステップ136で、支払いが却下されたことを知らせる情報をMTD26及び／又はMCD28に送信して、ステップ138／140で取引を終了するように動作する。

【0104】

[00111]一方、保管システム10で受信された許可応答が許可が承認されたことを示す場合は、ステップ134で、保管部10が承認メッセージをホスト22に送信する。

【0105】

[00112]この場合、ホスト22は次いでステップ142でMTD26及び／又はMCD28にメッセージを送信して、ステップ144／146で取引を完了するように動作する。

【0106】

[00113]上記過程のステップで、図1に示すシステムの個々の構成要素間で各種メッセージがやり取りされる。所与の取引に関連するメッセージ同士を紐付けるために、各メッセージに取引識別子を付与することにより取引又はセッションについての要求メッセージ及び応答メッセージを紐付けることができる。

【0107】

[00114]図9の例では、通信は上記のように公開鍵／秘密鍵による暗号化を使用して実施することができることを理解されたい。

【0108】

[00115]例示的实施形態は、顧客と商店の双方に体感される使用の平易性と柔軟性を提供することができ、同時に動作の安全性と保全本性ももたらす。例示的实施形態では、顧客と商店間の取引は、顧客が商店に支払いカードを提示する必要なしに支援することができ、動作の安全性を高め、不正が行われる可能性を低減する。

【0109】

[00116]用語「顧客」と「ユーザ」は本明細書では同義で使用されることに留意されたい。上記の例示的实施形態では、取引は顧客（ユーザ）と商店の間で行われるものと説明した。しかし、他の例では顧客と商店の関係はより一般的に購入者と売り手の関係であってもよく、その場合取引はピアツーピアになることに留意されたい。例えば、取引は2人の私的な個人で行うこともでき、その場合「商店端末装置26」は売り手の移動通信装置であり、「商店システム400」は、売り手の移動通信装置を使用した販売を支援するためのホストシステムとなる。そのような例では、「顧客」は購入者であり、「顧客の（ユーザの）移動通信装置」は購入者の移動通信装置になる。他の例では、本明細書に記載されるシステムを企業間取引に使用することもできる。

【0110】

[00117]上記の実施形態を詳細に説明したが、上記の開示が完全に理解されれば、多数の変形例及び変更が当業者には明らかになろう。以下の特許請求の範囲はそのようなすべての変形例及び変更並びにそれらの均等物を包含するものと解釈すべきことが意図される。

【図 1】

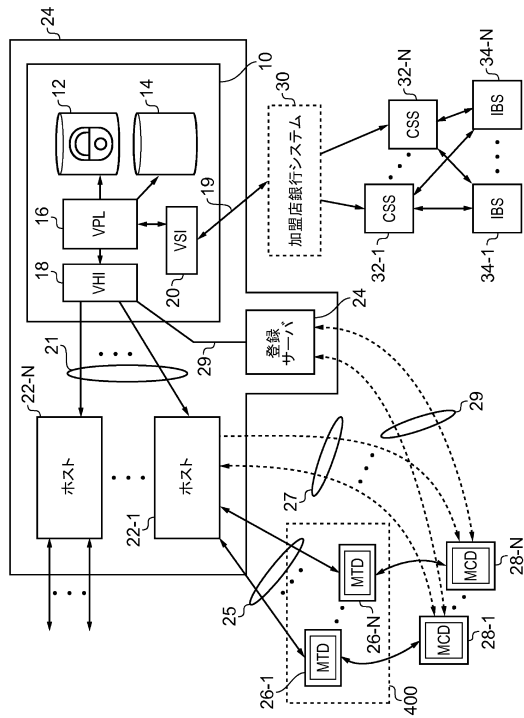


FIG. 1

【図 2 A】

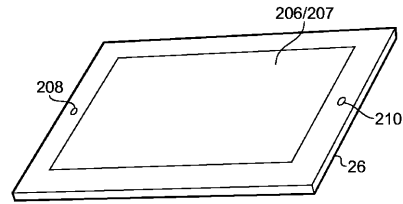


FIG. 2A

【図 2 B】

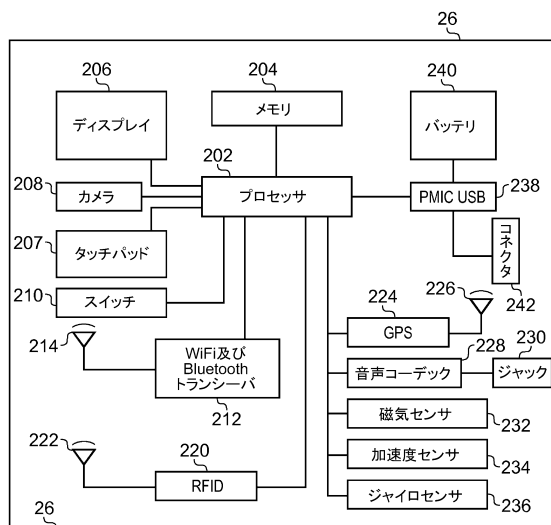


FIG. 2B

【図 3 A】

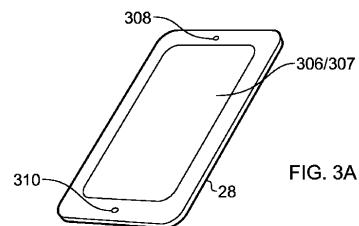


FIG. 3A

【図 3 B】

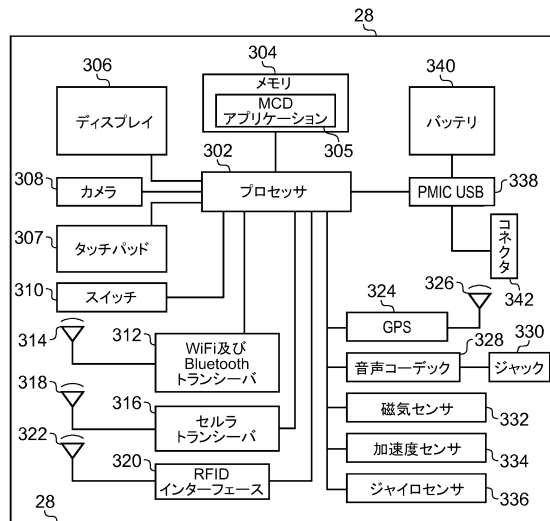


FIG. 3B

【図 4】

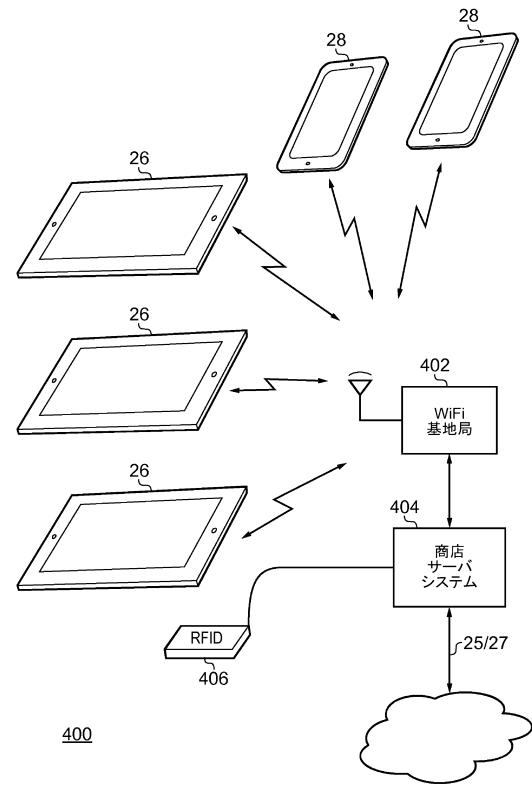


FIG. 4

【図 5】

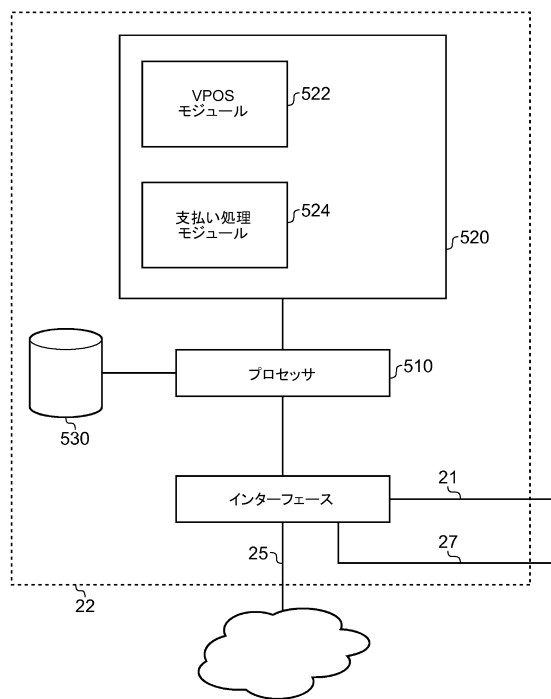


FIG. 5

【図 6】

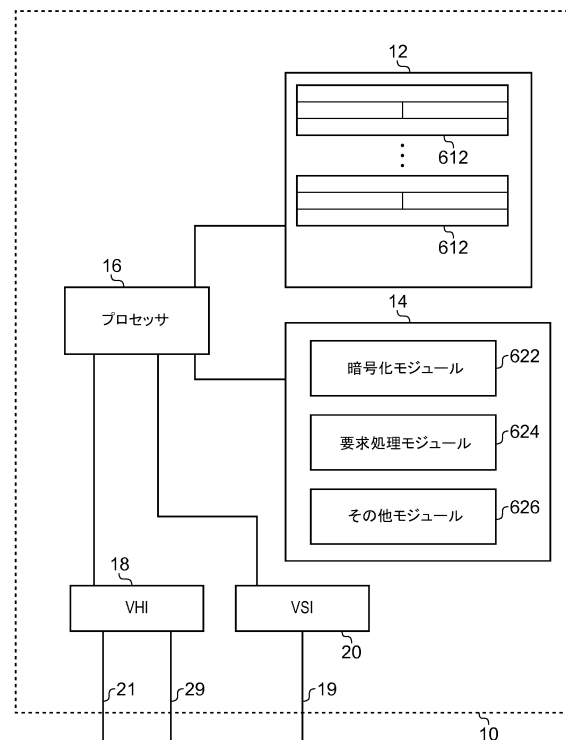


FIG. 6

【図 7】



FIG. 7

【図 8】



FIG. 8

【図 9】

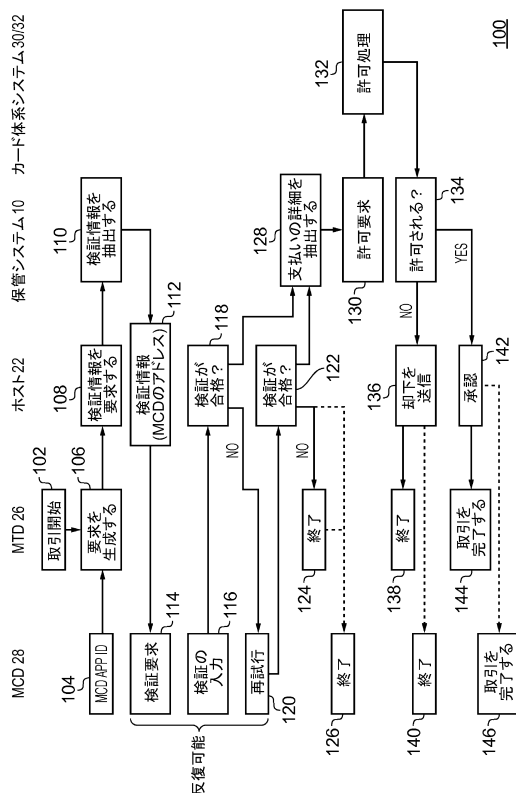


FIG. 9

---

フロントページの続き

- (72)発明者 ハナフィ, ワリード  
シンガポール, 229665, シンガポール, ケアンヒル プラザ ナンバー24-03,  
ケアンヒル ロード 53
- (72)発明者 バッシ, ステファノ  
イタリア, アイ-21013 ヴァレーゼ, ガララテ, ヴィア カルロ ノエ 33, ケ  
アオブ グローバル ブルー イタリア ソチエタ レスポンサビリタ リミタータ

審査官 梅岡 信幸

- (56)参考文献 特開2010-225108 (JP, A)  
国際公開第2010/021302 (WO, A1)  
特開2005-167412 (JP, A)  
特開2011-035622 (JP, A)

- (58)調査した分野(Int.Cl., DB名)  
G06Q 10/00-99/00