

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5520813号  
(P5520813)

(45) 発行日 平成26年6月11日 (2014. 6. 11)

(24) 登録日 平成26年4月11日 (2014. 4. 11)

(51) Int.Cl.

F I

G 0 6 Q 20/40 (2012.01)

G 0 6 Q 20/40 1 1 0

請求項の数 19 (全 29 頁)

(21) 出願番号	特願2010-504222 (P2010-504222)	(73) 特許権者	508168790
(86) (22) 出願日	平成20年4月16日 (2008. 4. 16)		ビザ ユー. エス. エー. インコーポレイ
(65) 公表番号	特表2010-525461 (P2010-525461A)		テッド
(43) 公表日	平成22年7月22日 (2010. 7. 22)		アメリカ合衆国 9 4 1 2 8 - 8 9 9 9
(86) 国際出願番号	PCT/US2008/060508		カリフォルニア、 サンフランシスコ、 ビ
(87) 国際公開番号	W02008/131021		ー. オー. ボックス 8 9 9 9
(87) 国際公開日	平成20年10月30日 (2008. 10. 30)	(74) 代理人	110000855
審査請求日	平成23年4月15日 (2011. 4. 15)		特許業務法人浅村特許事務所
(31) 優先権主張番号	60/912, 406	(74) 代理人	100066692
(32) 優先日	平成19年4月17日 (2007. 4. 17)		弁理士 浅村 皓
(33) 優先権主張国	米国 (US)	(74) 代理人	100072040
			弁理士 浅村 肇
		(74) 代理人	100138346
			弁理士 畑中 孝之

最終頁に続く

(54) 【発明の名称】 取引のための個人認証方法、サーバ、およびその方法を実行するためのプログラム記憶媒体

(57) 【特許請求の範囲】

【請求項 1】

a) ディレクトリサーバで提示者の口座に対する口座識別子に関連するエリア識別子を受信するステップと、

b) 前記ディレクトリサーバによって、前記エリア識別子を使って、関連する信頼できる当事者を決定するステップと、

c) 検証リクエストメッセージを受け取りそして前記関連する信頼できる当事者を決定した後に、前記ディレクトリサーバによって前記信頼できる当事者に前記検証リクエストメッセージを送るステップであって、前記検証リクエストメッセージは、前記信頼できる当事者または前記提示者が、認証プログラムに参加しているかどうかに関する情報をリクエストする、ステップと

d) 前記信頼できる当事者または前記提示者が前記認証プログラムに参加して前記提示者に対して認証が利用可能かどうかを示す検証応答メッセージを受信するステップと、

e) 前記信頼できる当事者によって操作されるアクセス制御サーバから前記検証応答メッセージを受信した後に、前記ディレクトリサーバから前記アクセス制御サーバに第1の認証リクエストメッセージの送信するステップであって、前記アクセス制御サーバはその後に前記提示者に第2の認証リクエストメッセージを送信する、ステップと、からなる方法。

【請求項 2】

前記エリア識別子は、電話番号である、請求項 1 に記載の方法。

10

20

## 【請求項 3】

前記信頼できる当事者は、前記口座を維持する金融機関である、請求項 1 に記載の方法。

## 【請求項 4】

前記エリアス識別子を受信する前に、前記提示者は、通信デバイスを使って前記エリアス識別子を送る、請求項 1 に記載の方法。

## 【請求項 5】

前記信頼できる当事者は、前記口座識別子を発行した発行者である、請求項 1 に記載の方法。

## 【請求項 6】

前記提示者に選択するための口座番号のリストが提示される、請求項 1 に記載の方法。

## 【請求項 7】

a) 提示者の口座に対する口座識別子に関連するエリアス識別子を受信するための手順と、

b) 前記エリアス識別子を使って、関連する信頼できる当事者を決定するための手順と、

c) 検証リクエストメッセージを受け取りそして前記関連する信頼できる当事者を決定した後に、前記信頼できる当事者に前記検証リクエストメッセージを送るための手順であって、前記検証リクエストメッセージは、前記信頼できる当事者または前記提示者が、認証プログラムに参加しているかどうかに関する情報をリクエストする、手順と、

d) 前記信頼できる当事者または前記提示者が前記認証プログラムに参加し前記提示者に対して認証が利用可能かどうかを示す検証応答メッセージを受信するための手順と、

e) 前記信頼できる当事者によって操作されるアクセス制御サーバから前記検証応答メッセージを受信した後に、前記アクセス制御サーバに第 1 の認証リクエストメッセージを送信する手順であって、前記アクセス制御サーバはその後前記提示者に第 2 の認証リクエストメッセージを送信する、手順と、を実行させるためのプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

## 【請求項 8】

プロセッサと、

前記プロセッサに結合された請求項 7 に記載のコンピュータが読み取り可能な記憶媒体とを備えるディレクトリサーバ。

## 【請求項 9】

a) 通信デバイスを使用して提示者の口座に関連する口座識別子に関連するエリアス識別子をディレクトリサーバに提供するステップと、

b) 前記エリアス識別子を提供した後に、前記通信デバイスを使用して認証リクエストメッセージを受信するステップであって、前記ディレクトリサーバが検証リクエストメッセージを受け取りそして前記提示者に対して認証が利用可能であることを示す検証応答メッセージを受信することによって信頼できる当事者が認証プログラムに参加していることを決定した後に、前記認証リクエストメッセージが当該信頼できる当事者によって操作されるアクセス制御サーバから受信される、ステップと、

c) 前記認証リクエストメッセージを受信した後に、前記通信デバイスを使用して認証応答メッセージを送るステップと、からなる方法。

## 【請求項 10】

前記エリアス識別子は、電話番号である、請求項 9 に記載の方法。

## 【請求項 11】

前記提示者の音声を使って、前記エリアス識別子が提供される、請求項 9 に記載の方法。

## 【請求項 12】

前記提示者が操作する通信デバイスで、前記認証リクエストメッセージが受信される、請求項 11 に記載の方法。

**【請求項 13】**

前記認証応答メッセージは、パスワードまたはP I N番号を含む、請求項 12に記載の方法。

**【請求項 14】**

対面取引において前記エリアス識別子が業者に提供される、請求項 9に記載の方法。

**【請求項 15】**

業者に対して遠隔地に位置する通信デバイスを使って前記エリアス識別子が、前記業者に提供される、請求項 9に記載の方法。

**【請求項 16】**

前記認証応答メッセージは、少なくとも送り先アドレス、コンタクト情報または前記提示者の好みの少なくとも一つを含む、請求項 9に記載の方法。

**【請求項 17】**

a) 提示者の口座に関連する口座識別子に関連するエリアス識別子をディレクトリサーバに提供するための手順と、

b) 前記エリアス識別子を提供した後に、認証リクエストメッセージを受信するための手順であって、前記ディレクトリサーバが検証リクエストメッセージを受け取りそして前記提示者に対して認証が利用可能であることを示す検証応答メッセージを受信することによって信頼できる当事者が認証プログラムに参加していることを決定した後に、前記認証リクエストメッセージが当該信頼できる当事者によって操作されるアクセス制御サーバから受信される、手順と、

c) 前記認証リクエストメッセージを受信した後に、認証応答メッセージを送るための手順と、を実行させるためのプログラムを記憶したコンピュータが読み取り可能な記憶媒体。

**【請求項 18】**

対面取引において前記エリアス識別子が業者に提供される、請求項 17に記載のコンピュータが読み取り可能な記憶媒体。

**【請求項 19】**

業者に対して遠隔地に位置する通信デバイスを使って前記エリアス識別子が、前記業者に提供される、請求項 17に記載のコンピュータが読み取り可能な記憶媒体。

**【発明の詳細な説明】****【技術分野】****【0001】**

(関連出願とのクロスレファレンス)

本願はすべての目的のために、全体を参考例として本願で引用する、2007年4月17日に出願された米国特許出願第60/912,406号の非仮特許出願であり、この米国特許出願の権利を主張するものである。

**【背景技術】****【0002】**

(背景)

2人の当事者の間で取引(支払いを伴う取引または支払いを伴わない取引)を行う間、各当事者は不正を回避するために、他方の当事者のアイデンティティおよび/または他方の当事者に関係するデータを一般に認証を望む。

**【0003】**

遠隔通信デバイスによって開始され、このデバイスにより行われる取引は、対面取引よりも、より危険となり得る。その理由は、従来の対面認証手続きを実行できないからである。例えば遠隔取引を行う際に、消費者の運転免許証の写真をチェックすることができないからである。

**【発明の概要】****【発明が解決しようとする課題】****【0004】**

上記に鑑み、遠隔取引中に消費者のような個人のアイデンティティおよびプロフィールデータを認証するためのシステムが望まれている。認証システムは、実現および使用が容易であり、資源に最小限しか投資するだけでよく、システム参加者の間の高レベルの相互運用可能性を提供できることが望ましい。

【 0 0 0 5 】

取引に関係する別の問題は、一般に購入取引中に業者が支払いカード情報を受け取ることが多いことにある。業者が誠実でない場合、消費者の支払い情報は危うくなり得る。本発明の別の実施形態は、業者が消費者の支払い情報を保有することのないよう、支払い取引のような取引を開始するのにエリアス識別子を使用することに関する。

【 0 0 0 6 】

本発明の実施形態は、上記課題およびその他の課題を別々に、かつ総合的に解決するものである。

【課題を解決するための手段】

【 0 0 0 7 】

概要

本発明の実施形態は、個人の識別を認証し、所定のアイデンティティを有し、かつ対応する所定のプロフィールデータを有する者として自分を別の当事者に提示する個人（提示者）のプロフィールデータの有効性を判断するための方法およびシステムを含む。本発明の実施形態は、遠隔取引だけに限定されないが、本発明の実施形態は、対面で認証手続きを行うことが困難である遠隔取引で有利に使用できる。本発明の実施形態により、信頼できる当事者は、提示者のアイデンティティおよびプロフィールデータを認証することも可能となる。プロフィールデータの提供およびプロフィール更新のような別の能力も実行できる。

【 0 0 0 8 】

本発明の一実施形態は、a) 提示者の口座に対する口座識別子に関連するエリアス識別子を受信するステップと、b) 前記エリアス識別子を使って、信頼できる関連当事者を決定するステップと、c) 前記信頼できる関連当事者を決定した後に、前記信頼できる当事者に検証リクエストメッセージを送るステップとを備え、前記検証リクエストメッセージは、前記信頼できる当事者または前記提示者が、認証プログラムに参加しているかどうかに関する情報をリクエストし、d) 更に前記信頼できる当事者または前記提示者が前記認証プログラムに参加しているかどうかを示す検証応答メッセージを受信するステップを備える方法に関する。

【 0 0 0 9 】

本発明の別の実施形態は、a) 提示者の口座に対する口座識別子に関連するエリアス識別子を受信する符号と、b) 前記エリアス識別子を使って、信頼できる関連する当事者を決定する符号と、c) 前記信頼できる関連する当事者を決定した後に、前記信頼できる当事者に検証リクエストメッセージを送る符号とを備え、前記検証リクエストメッセージは、前記信頼できる当事者または前記提示者が、認証プログラムに参加しているかどうかに関する情報をリクエストし、d) 更に前記信頼できる当事者または前記提示者が前記認証プログラムに参加しているかどうかを示す検証応答メッセージを受信する符号を備えるコンピュータが読み取りできるメディアに関する。

【 0 0 1 0 】

本発明の別の実施形態は、a) 提示者の口座に関連する口座識別子に関連するエリアス識別子を提供するステップと、b) 前記エリアス識別子を提供した後に、認証リクエストメッセージを受信するステップと、c) 前記認証リクエストメッセージを受信した後に、認証応答メッセージを送るステップとを備える方法に関する。

【 0 0 1 1 】

本発明の別の実施形態は、a) 提示者の口座に関連する口座識別子に関連するエリアス識別子を提供する符号と、b) 前記エリアス識別子を提供した後に、認証リクエストメッセージを受信する符号と、c) 前記認証リクエストメッセージを受信した後に、認証応答

10

20

30

40

50

メッセージを送る符号とを備えるコンピュータが読み取りできるメディアに関する。

【0012】

図面および詳細な説明を参照し、以下、本発明の上記およびそれ以外の実施形態について更に詳細に説明する。

【図面の簡単な説明】

【0013】

【図1】本発明の一実施形態に係わるシステムのブロック図を示す。

【図2】本発明の別の実施形態に係わるシステムの別のブロック図を示す。

【図3】本発明の別の実施形態に係わるシステムの別のブロック図を示す。

【図4】支払い取引前に生じ得る登録プロセスの実施形態を示すフローチャートである。

【図5】支払い取引中に生じ得る登録プロセスの実施形態を示すフローチャートである。

【図6】支払い取引を開始するためのプロセスの実施形態を示すフローチャートである。

【図7】認証プロセスの実施形態を示すフローチャートである。

【図8】支払い認証プロセスの実施形態を示すフローチャートである。

【図9(a)】電話内の部品を示すブロック図である。

【図9(b)】代表的な支払いカードに存在し得る部品を示す。

【図10】コンピュータ装置内の部品のブロック図を示す。 図中、同様な番号は同様な要素を示し、一部のケースでは、同様な要素の説明を繰り返さないことがある。

【発明を実施するための形態】

【0014】

( 詳細な説明 )

本発明の実施形態は、所定のアイデンティティを有する者であって、かつ所定の対応するプロファイルデータを有するものとして、自らを別の当事者（受領者）に提示する個人（提示者）のアイデンティティを認証し、かつその個人のプロファイルデータの有効性を判断するための方法およびシステムを提供するものである。消費者は提示者の一例となることがあり、受領者は、サービス提供者、政府機関、業者または取引を進める前に提示者のアイデンティティを認証する必要がある他の任意のエンティティとなり得る。アイデンティティの認証は、所定の個人であると主張する提示側当事者のアイデンティティを検証することに依存することができ、プロファイルデータの有効性の判断は、提示者によって提供されるプロファイルデータが実際にその提示者に関連していることの有効性の判断に依存することができる。他の機能、例えばプロファイルデータの供給およびプロファイルの更新も、本発明の実施形態で実行できる。これら機能は別々に実行してもよいし、または互いに組み合わせて実行してもよい。本発明の実施形態は、従来の対面認証手続きの実行が困難である遠隔取引を実行するのに使用することが好ましい。

【0015】

図示するように、本発明の一実施形態では、クレジットカードを使って購入することを業者に求めている消費者を、取引が進行する前に認証できる。クレジットカードの発行者は、取引が終了するまでに、消費者および消費者のプロファイルデータを認証することができる。（カード発行者は、銀行、クレジットユニオンまたは口座を使って消費者が取引を行うことができるように、消費者のために口座を開設できる他の機関となり得る。）消費者および消費者のデータが認証された後に、この情報は業者に送られる。次に業者は、発行者が消費者および消費者のデータを認証したことを知って、取引を進めることができる。クレジットカードの発行者が消費者および消費者のデータを認証すると、後でその取引が詐欺であると判断された場合、発行者がリスクを負う場合がある。したがって、本発明の実施形態を使用すれば、業者およびカード発行者は、行われている取引が正当であるとの、より高い確信を有し得る。

【0016】

以下、本発明の特定の実施形態の多くを詳細に説明する。一部の場合、次のような頭辞略語を使用する。

A C S : アクセス制御サーバ - アクセス制御サーバは、取引、例えば遠隔または対面購

10

20

30

40

50

入取引中に、提示者（例えば消費者、カード所有者）を認証できる能力をカード発行者に提供できる。

D S：ディレクトリーサーバ - ディレクトリーサーバを使って、業者プラグイン（M P I）と発行者のA C Sとの間で入会および認証情報を含むメッセージをルーティングできる。

I V R：相互対話音声応答ユニット - 相互対話音声応答ユニットは、通常の電話の通話を通してコンピュータ装置が音声およびタッチトーンを検出できるようにする電話技術を含むことができる。

S M S：ショートメッセージサービス - ショートメッセージサービスは、携帯電話との間で送られるメッセージを含むことができる。典型的なS M Sメッセージによって、ユーザーはメッセージ当たり160個までの文字を送ることができる。

10

M P I：業者プラグイン - 業者プラグインは、一部の実施形態では取得者のドメイン内で作動するコンポーネントとなり得る。オンライン環境では、この業者プラグインは、業者のために種々の認証機能を実行する。かかる機能として、カード番号に関して認証を利用できるかどうかを判断すること、および認証メッセージ内のデジタル署名の有効性の判断をすることが挙げられる。この業者プラグインでは、業者にアクセスできる適当なハードウェアおよび/またはソフトウェアによって具現化できる。

M S I S D N：モバイル加入者用I S D N番号 - モバイル加入者用I S D N（統合サービスデジタルネットワーク）番号は、消費者の電話番号とすることができる。

U S S D：非構造化補助サービスデータ - 非構造化補助サービスデータは、G S Mネットワークのチャンネルを通じた情報の伝送をサポートするためのG S M（モバイル通信のためのグローバル通信）に組み込まれた機能を有する。U S S Dは、セッションに基づく通信機能を提供し、よって種々のアプリケーションを可能にする。

20

W A P：無線アプリケーションプロトコル - W A Pブラウザは、P C（パソコン）に基づくウェブブラウザの基本サービスのすべてを提供でき、このW A Pブラウザは、携帯電話の制限内で運用できるように簡略化できる。

#### 【0017】

上記のように、本発明の実施形態は特に遠隔取引を行うのに有効である。形態または地上回線音声通話、ショートメッセージサービス（S M S）メッセージなどを含むが、これらだけに限定されない通信を通して、遠隔取引を行うことができる。種々のデータ転送プロトコル（例えばT C P / I P）も使用できる。携帯電話、スマートフォン、インターネット接続されたコンピュータまたはターミナル、パーソナルデジタルアシスタント（P D A）などを含むが、これらに限定されないデバイスからも、遠隔取引を開始できる。

30

#### 【0018】

本発明の実施形態は、携帯電話の使用および遠隔取引だけに限定されるものではなく、本発明の実施形態は、種々の通信デバイス、支払いチャンネルおよび認証チャンネルの使用も含むことができる。次に、通信デバイス、支払いチャンネルおよび認証チャンネルの数例について記載する。

【表 1】

ブラウジングチャンネル／環境／デバイス	支払いチャンネルまたはメカニズム	消費者認証チャンネル
消費者は、パソコン、例えばデスクトップコンピュータまたはラップトップコンピュータを使って業者のウェブサイトブラウジングする。 例えば消費者は、インターネットでポータブル音楽デバイスを購入する。	消費者は、自分のパソコンを使って業者のウェブサイト上のウェブページで自分の電話番号を入力する。	消費者によって作動されている形態または固定デバイス上で作動するクライアントアプリケーションを介し、または消費者のカード発行者または他のエンティティによって実現されている他の任意の適当なチャンネル／プロセスを介し、インバウンド(inbound)IVR通話を使って消費者を認証できる。
メールオーダー／電話オーダー(MOTO)。 例えば消費者は、レストランを呼び出すことにより、ピザを購入する。	業者のコールセンターのエージェントは、消費者の電話番号を入手し、その電話番号を業者のウェブサイト上のウェブページに入力する。	上記と同じ
IVRまたは他の自動化されたチャンネル、例えばUSSDまたはSMS。 例えば消費者は、電話を使って有料放送を購入する。	消費者は、(例えばIVRを介し)自動化サービスを呼び出し、支払い金額を選択し、自分の携帯電話番号を入力する。	上記と同じ
対面取引(業者はポイントオブセールス(POS)ターミナル、例えば電話に支払いの詳細を入力する)。 例えば消費者は、対面取引で行われたサービスに対して配管工に支払いをする。	業者は、自分の携帯電話から取引を開始する。 例えば業者はカード提示ステータスに関し、消費者の支払いカードの裏面に消費者のCVV-2番号を別個に入力できる。	上記と同じ
対面取引(消費者は携帯電話などに支払いの詳細を入力する)。 例えば消費者は、対面取引で行われたサービスに対し、配管工に支払いをする。	消費者は、自分の携帯電話から取引を開始する。 消費者は業者の電話番号および支払い金額を消費者の携帯電話に入力することによって取引を終了する。	上記と同じ

## 【0019】

次に、図を参照し、本発明の特定の実施形態について説明できる。一実施形態では、エリア識別子を受け取る。このエリア識別子は、提示者(例えば消費者)の口座に対する(口座番号のような)口座識別子に関連したものである。エリア識別子は、電話番号でよく、口座識別子はクレジットカードの口座番号のような口座番号でもよい。エリア識別子が受信された後に、このエリア識別子を使って信頼できる関連当事者を決定する。この信頼できる当事者を、クレジットカードの口座番号を提示者に発行した発行者とすることができる。

## 【0020】

次に、信頼できる関連当事者を決定した後に、この信頼できる当事者へ検証リクエストメッセージを送ることができる。検証リクエストメッセージは、信頼できる当事者または

10

20

30

40

50

提示者が認証プログラムに参加している旨の検証をリクエストする。例えばこのメッセージは、提示者および信頼できる当事者の一方または双方が認証プログラムに参加している旨の検証をリクエストできる。検証リクエストメッセージが送られた後に、検証応答メッセージが受信される。この検証応答メッセージは、信頼できる当事者または提示者は認証プログラムに参加しているかどうかを示す。

【 0 0 2 1 】

検証応答メッセージを受信した後に、消費者によって操作されている通信デバイス（例えば電話）に認証リクエストメッセージを送ることができる。次に消費者は、この消費者を認証する認証応答メッセージの送信を開始できる。消費者が認証された後に、消費者は行おうとしている取引を続けることができる。取引は購入取引、送金などとするこ

10

【 0 0 2 2 】

図 1 は、本発明の一実施形態に係わるシステムを示す。図 1 のシステムは、インターネットを通すか、または電話（例えば携帯電話）を使って行われるような遠隔取引を行うのに使用できる。

【 0 0 2 3 】

このシステムのコンポーネントは、提示者ドメイン、相互運用可能性ドメインおよび信頼できる当事者ドメイン内に設けられていることを特徴とし得る。本発明の別の実施形態では、このシステムにおけるコンポーネントは他のタイプのドメイン、すなわち異なるドメイン内にも存在し得る。本発明の一実施形態に係わるシステムは、単一ドメインまたはドメインの適当な任意の組み合わせ内にある任意の数のコンポーネントまたはこれらコンポーネントの組み合わせを含むことができる。図 1 における実施形態では、認証システムは、相互運用可能性ドメイン（*interoperability domain*）および発行者 / 信頼できる当事者ドメイン内に示されたコンポーネントを含むことができる。

20

【 0 0 2 4 】

図 1 は、業者 2 2 と通信している提示者 2 1 を示す。業者 2 2 は、ウェブページインターフェース 2 3 を提供でき、このウェブページインターフェース 2 3 は、発行者のルックアップシステム 2 4 に結合できる。発行者のルックアップシステム 2 4 は、業者プラグイン（*MP I*）2 8、ディレクトリサーバ 2 7、アクセス制御サーバ 2 5、提示者のファイルデータベース 2 6 だけでなく、チャレンジインターフェース 2 9 にも作動的に結合できる。

30

【 0 0 2 5 】

図 1 では、提示者ドメインは、提示者 2 1 と業者 2 2 とを含む。提示者 2 1 は、ユーザー、個人または消費者とすることができ、これらユーザー、個人または消費者のアイデンティティは認証中であり、および / またはこれらユーザー、個人、消費者のデータは有効性の判断中または提供中である。業者 2 2 は受領者の一例であり、提示者 2 1 は取引しようと試みている相手の当事者となり得る。提示者 2 1 は、インターネット 2 2 を通して、または通信デバイス、例えば携帯電話またはコンピュータ装置を直接使用することによって、認証システムにアクセスできる。

【 0 0 2 6 】

40

データ認証システムは、認証プログラムを作動させることができ、信頼できる当事者または信頼できる当事者によって作動されるコンポーネントを含むことができる。信頼できる当事者は、提示者のアイデンティティを認証し、提示者 2 1 に関連するデータの有効性の判断、データの提供または更新するエンティティとすることができる。一部の実施形態では、信頼できる当事者は、銀行、クレジットまたはデビットカード発行銀行、またはクレジットまたはデビットカードサービス機構（例えば *Visa*）とすることができる。図示して説明するように、銀行はこの提示者が使用するクレジットカードの発行銀行とすることができる。提示者 2 1 は、この銀行の顧客とすることができる。信頼できる当事者は、提示者 2 1 との間で確立された関係を有することができるので、提示者 2 1 を認証するのに使用できる提示者のプロフィールデータを有することができる。この提示者のプロフ

50

ファイルデータとして、提示者のソーシャルセキュリティ番号、誕生日、口座番号、配達先住所、好みなどを挙げることができる。

【 0 0 2 7 】

信頼できる当事者は、アクセス制御サーバ 2 5 ( A C S ) を所有または作動させることができ、このサーバは、特に認証プログラムへのアクセスを制御し、リクエストされたデータサービスを実行し、認証サービスに関係するデジタル署名された通知を受領者に提供するコンピュータ装置とすることができる。信頼できる多数の当事者が 1 つの A C S を共用してもよいし、または A C S に一人の信頼できる当事者を関連させてもよい。これとは異なり、各々が提示者のサブセットに関連するような多数のアクセス制御サーバを信頼できる一人の当事者が有してもよい。

10

【 0 0 2 8 】

本明細書で使用するような「サーバ」なる用語は、一般に強力なコンピュータまたはコンピュータのクラスター（群）のことである。例えばサーバは巨大なメインフレームでもよいし、ミニコンピュータクラスターでもよいし、またはユニットとして機能するサーバのグループでもよい。一例では、サーバはウェブサーバに結合されたデータベースとすることができる。更にサーバは、1 つ以上のクライアントコンピュータまたはポータブル電子デバイスのリクエストにサービスする単一のコンピュータとして作動できる。

【 0 0 2 9 】

提示者のファイルデータベース 2 6 は、信頼できる当事者が管理するか、または信頼できる当事者に関連するデータベースとすることができる。このデータベースは認証プログラム内への加入に成功した提示者に関する情報を記憶できる。かかる情報として、プログラムアイデンティティ番号および口座番号のような識別子、プロファイルデータおよびパスワードを挙げることができる。

20

【 0 0 3 0 】

相互運用可能性ドメインは、ディレクトリサーバ 2 7 も含む。この相互運用可能性ドメインは、一部の実施形態では信頼できる当事者および受領者の双方が使用するコンポーネントを含むことができる。ディレクトリサーバ 2 7 は、提示者がデータ認証サービスを利用できるかどうかを判断できる。一部のケースでは、V i s a のようなサービス機構によってディレクトリサーバ 2 7 を作動させることができる。

【 0 0 3 1 】

30

データ認証サービスシステム内の提示者と、信頼できる当事者と、受領者との間のそれぞれの関係によって広いレンジのサービスを提供することが可能となっている。かかるサービスの例として、アイデンティティ認証、プロファイルの有効化、プロファイルデータ提供およびプロファイルデータ更新を挙げることができる。プロファイルの有効性判断の一実現例は、提示者のアドレスの有効性を判断するように作動し、プロファイルデータ更新の一実現例は、提示者の口座情報を更新するように作動する。

【 0 0 3 2 】

提示者 2 1 と業者 2 2 との間の支払いを伴わない関連する取引および支払いを伴う関連する取引において、認証システムを使用できる。支払いに関連する取引において、別の作動、例えば金融口座からのデビットおよびクレジットの認証を行うこともできる。発行者の認証および決済システムのような別のシステムも使用できる。

40

【 0 0 3 3 】

次に、提示者の加入プロセスについて説明する。一実施形態では、提示者 2 1 は認証プログラムに参加するために、信頼できる当事者と共に登録される。登録に成功すると、信頼できる当事者は提示者にプログラムアイデンティティ番号（または他のエリアス識別子）および認証パスワード、トークンまたは他の認証要素を提供またはこれらを割り当てることができる。認証パスワード、トークンまたは他の認証要素によって、信頼できる当事者は、提示者 2 1 のアイデンティティを認証することが可能となる。その理由は、信頼できる当事者および提示者 2 1 しかパスワード、トークンまたは他の認証要素を知らないからである。ある方法でエリアス識別子および / または認証要素を通信デバイス（例えば電

50

話)に関連させることができる。例えばエリア識別子を電話番号とし、認証要素を電話用のSIMカード番号とすることができる。

【0034】

プログラムアイデンティティ番号とは、認証プログラムを使用するのに、適正に入会している提示者を識別する番号のことである。プログラムアイデンティティ番号またはエリア識別子は、一般に口座識別子、例えば提示者21に関連する口座番号にリンクできる。

【0035】

プログラムアイデンティティ番号は任意の適当なタイプの数を含むことができる。プログラムアイデンティティ番号の一例として、乱数または一連の数字から生じた数字を挙げることができる。一実施形態では、プログラムアイデンティティ番号を電話番号とすることができる。このことは、その電話番号を有する電話を使って音声またはショートメッセージサービス(SMS)メッセージにより、認証システムと提示者21が相互対話するケースで便利である。取引を行う際に、提示者の口座番号の代わりにプログラムアイデンティティ番号を使用してもよい。

10

【0036】

本発明の実施形態では、アイデンティティ番号を一般に通信デバイスまたは通信サービスアドレスまたは識別子(例えば電話番号、eメールアドレス)などに対応させることができる。電話番号をアイデンティティ番号として使用する場合、システムは提示者の電話番号を自動的に決定するために自動番号識別(ANI)サービスのようサービスを使用してもよい。これとは異なり、提示者21の音声を使用するか、または提示者の電話に電話番号をマニュアルで入力することにより、提示者21に対して提示者の電話番号を提供することを求めてもよい。

20

【0037】

本発明の実施形態では、アイデンティティ番号は追加情報、例えば口座識別子(例えば口座番号)または受領者識別番号の少なくとも一部を含んでもよい。例えば実施中の取引がクレジットカードを必要とする場合、追加情報を、カード口座番号の最初の6桁に対応するクレジットカード発行者の銀行識別番号(BIN)とすることができる。この追加識別情報は、多数の口座または受領者が所定の提示者アイデンティティ番号に関連し得るときに有効である。

30

【0038】

入会プロセス中、提示者21は入会データ、認証データおよびプロフィールデータを信頼できる当事者に提供できる。信頼できる当事者が提示者21を認証し、提示者が認証プログラムに参加しているかどうかを判断するように、これらタイプのデータを使って提示者のアイデンティティを検証できる。その後の取引中に提示者を認証するのに認証データを使用できる。認証データの例として、パスワード、チップカード内のユニークなデータ、生体測定データなどを挙げることができる。種々のタイプの認証データを使用できると理解すべきである。かかるデータが信頼できる当事者のもとのファイルに存在しない場合、その後の取引中にプロフィールデータを使ってプロフィールデータの有効性の判断および/またはそのデータの提供をできる。

40

【0039】

提示者の入会プロセスは種々の方法で行うことができる。例えばオンライン、人と人との相互対話、電話での会話またはメールを通して、この入会プロセスを行うことができる。オンライン入会プロセスの例では、提示者は入会ウェブサイトに進み、プログラムアイデンティティ番号(または他のエリア識別子)および認証要素を得るための適当な情報を提供できる。一部の実施形態では、入会していない提示者が取引を行おうとする最初のときに、入会を自動的に開始することもできる。

【0040】

次に、図1を参照し、データ認証プログラムに関連するデータ認証プロセスについて説明できる。このデータ認証プログラムは、受領者、例えば業者22が提示者21を認証し

50

たいような種々の状況に使用できる。例えば支払いを伴わない例では提示者 2 1 は、(受領者のウェブサイトの一例である) 政府のウェブサイトに進み、スモールビジネスライセンス (small business licence) のための申請書の書き込みを行うことができる。種々の政府機関は、自らのウェブサイトを通してオンラインサービスを提供している。一般に政府機関は、提示者 2 1 が入力した情報 (例えば氏名、住所など) を確認したい。本発明の実施形態は、支払いを伴う例でも同じように作動できる。例えば次の例は、顧客が業者 2 2 を呼び出し、発注し、自分のクレジットカードで注文に対する支払いを計画する場合のデータ認証プログラムの作動について述べたものである。

【0041】

提示者 2 1 は、業者 2 2 が物品またはサービスに対する発注に応じることを求めることにより、取引を開始する。別の実施形態では、提示者 2 1 はウェブブラウザまたは e メールなどを使用してインターネットを通して SMS メッセージを使って、業者 2 2 と相互対話できる。

【0042】

発注後、提示者 2 1 は、可能な場合に追加識別情報、例えば BIN (銀行識別番号) および / または追加識別子で補強されたアイデンティティ番号、例えば携帯電話の番号を業者 2 2 に提供する。提示者 2 1 の口座番号の代わりにこの情報を業者 2 2 に提供することもできる。提示者 2 1 が手動で提供するのではなく、ANI (自動番号識別) のようなシステムを使って、携帯電話の番号のようなアイデンティティ番号またはアイデンティティ番号の一部を自動的に決定することもできる。

【0043】

(提示者 2 1 は、このアイデンティティ番号を認証システムに直接には入力しないと仮定した場合) 業者 2 2 はアイデンティティ番号を受けた後に、この番号をデータ認証システムに入力する。業者 2 2 は、ウェブページインターフェース 2 3 を使用するか、または他の、ある手段を通して、認証システムとインターフェースできる。例えば業者 2 2 はアイデンティティ番号をウェブページインターフェース 2 3 に入力してもよい。別の実施形態では、提示者 2 1 はウェブページインターフェース 2 3 または他のあるインターフェースを通してシステムにアイデンティティ番号を直接入力できる。

【0044】

ウェブページインターフェース 2 3 によりアイデンティティ番号が受信された後に、発行者のルックアップシステム 2 4 は、アイデンティティ番号を受信し、このアイデンティティ番号に関連する発行者を判断する。一旦、対応する判断が決定されると、発行者のルックアップシステム 2 4 は、アイデンティティ番号を発行者に電子的に送る。発行者はアイデンティティ番号を口座番号に変換するのに使用される提示者のファイルデータベース 2 6 を維持する。次に、発行者のルックアップシステム 2 4 により、口座番号およびアイデンティティ番号が業者プラグイン (MPI) 2 8 へ転送される。

【0045】

次に、業者プラグイン (MPI) 2 8 は、提示者 2 1 がデータ認証プログラムに参加しているかどうかをチェックする。一実現例では、提示者 2 1 が認証プログラムに参加しているかどうかをチェックするのに、2 フェーズプロセスが使用される。この 2 フェーズプロセスでは、ディレクトリサーバ (DS) 2 7 およびアクセス制御サーバ (ACS) 2 5 に問い合わせが行われる。ディレクトリサーバ 2 7 はアイデンティティ番号を受信し、このアイデンティティ番号に関連する発行者がデータ認証プログラムに参加しているかどうかを判断する。発行者が提示者 2 1 のアイデンティティを認証し、提示者に関係するデータサービスを提供したい場合、提示者 2 1 はデータ認証プログラムを使用できる。アイデンティティ番号を受信した後に、アクセス制御サーバ (ACS) 2 5 は、認証プログラムにより提示者 2 1 が入会しているかどうか、およびアイデンティティ番号に関連するデバイスのタイプ (例えば携帯電話) が認証システムによりサポートされているかどうかを判断する。

【0046】

発行者がデータ認証プログラムに参加していないか、または提示者 2 1 がデータ認証プログラムに入会していない場合、業者 2 2 は取引を中断するか、または他のある態様で取引を進めるかどうかを判断できる。発行者が認証プログラムに参加しているが、提示者 2 1 が入会していない場合、データ認証プログラムに入会する機会を提示者 2 1 に与えてもよい。

#### 【 0 0 4 7 】

発行者および提示者 2 1 の双方がデータ認証プログラムに参加している場合、およびアイデンティティ番号に関係するデバイスをプログラムで利用できる場合、アクセス制御サーバ ( A C S ) 2 5 は、遠隔認証リクエストメッセージを発生し、(例えば業者プラグイン ( M P I ) が取得者または他の信頼できる当事者のホストとなっている場合に) このメ  
10  
ッセージは、業者プラグイン ( M P I ) 2 8 へ送られる。

#### 【 0 0 4 8 】

業者プラグイン ( M P I ) 2 8 は、次にチャレンジインターフェース 2 9 を通して認証チャレンジを提示者 2 1 へ発生する。このようにするために、業者プラグインは、提示者の支払いカード番号とアイデンティティ番号とを関連付ける。アイデンティティ番号が携帯電話の番号に対応している場合、この電話番号はアイデンティティ番号から抽出され、この番号を使って認証チャレンジを提示者の電話へ送る。チャレンジインターフェースモ  
20  
ジュール 2 9 を使って、認証チャレンジを顧客の携帯電話へ送るのに、非構造化補助サービスデータ ( U S S D ) プロトコルを使用してもよい。当業者であれば、他のプロトコルまたは通信方法も使用できることが認識できよう。例えば認証チャレンジを S M S メッセージ、自動化された予備記録電話発呼、または相互対話チャットメッセージとすることができる。

#### 【 0 0 4 9 】

提示者 2 1 は、認証チャレンジを受信すると、所定の認証データに応答する。例えば認証チャレンジが S M S メッセージを介して発せられた場合、提示者 2 1 はパスワードを含む応答 S M S メッセージを送ることができる。電話の呼び出しにより認証チャレンジが発  
30  
せられた場合、提示者 2 1 は電話のキーパッドを使うか、自分の音声を使ってパスワードを提供できる。この方法とは異なり、他のタイプの認証データ、例えば生体測定データ、チップカードデータなども使用できる。

#### 【 0 0 5 0 】

業者プラグイン ( M P I ) 2 8 が提示者の認証データを一旦受信すると、取引データ、例えばカードの口座番号および有効期限日を含むカードデータが添付され、発行者のアクセス制御サーバ ( A C S ) 2 5 へ送られる。発行者のアクセス制御サーバ ( A C S ) 2 5  
30  
は、認証データの有効性の判断をし、その有効性の判断の結果を業者プラグイン ( M P I ) 2 8 へレポートする。次に、業者プラグイン ( M P I ) 2 8 は、ウェブページインターフェース 2 3 を介して、検証の結果を業者 2 2 へ通知する。検証に成功した場合、業者 2 2 には提示者の口座識別子 (例えば口座番号) またはその一部を提供できる。次に発行者には取引の詳細が通知され、取引は完了するまで続行できる。

#### 【 0 0 5 1 】

取引が完了した後に、ウェブページインターフェース 2 3 を使ってアイデンティティ番号に対応する提示者のデバイス (例えば電話) および業者 2 2 にメッセージを送ることができる。例えば提示者の電話番号を使用する提示者の電話に対し、提示者 2 1 が正式に認  
40  
証されたこと、および取引が成功裏に完了したことを示すメッセージを送ることができる。セキュリティのレベルを高めるために、図 1 に示されているすべてのメッセージを暗号化できると理解すべきである。

#### 【 0 0 5 2 】

提示者 2 1 と業者 2 2 とが自ら取引するように本発明の実施形態を実現することもできる。提示者 2 1 ではなく、業者 2 2 に関連するアイデンティティ番号を提供することにより、業者 2 2 はシステムと相互対話できる。業者 2 2 が提示者 2 1 のアイデンティティ番号をシステムに提供することもできる。提示者 2 1 は自分のデバイスで認証チャンネルを  
50

受信し、上記のように認証データに応答できる。別の実施形態では、提示者 21 は業者のアイデンティティ番号および取引に対する支払い金額を提供することにより、システムと相互対話できる。

【0053】

本発明の実施形態では、提示者 21 が多数の支払いカード（例えば 3 枚以上のクレジットカード）を有し得ることに留意されたい。一実施形態では、提示者 21 が無線電話のような通信デバイスを使用している場合、提示者 21 に選択のための主要口座番号のリストを提示できる。提示者 21 が電話番号による取引を行うときに、取引を行うために最終的に主要デフォルト口座番号を使用するよう、この提示者のそのときの電話番号を主要デフォルト口座番号に対応させることができる。別の実施形態では、主要口座番号のリストを提示者 21 に提示し、取引を行う前に取引で使用する口座番号を提示者 21 が選択する。この場合、電話番号に関連するデフォルト口座番号は存在しなくてもよい。更に別の実施形態では、リスト内の各主要口座番号に関連する異なるエリアス識別子が存在し得る。例えば異なる 3 つの主要口座番号に対して、これらエリアス識別子を単に「card 1」、「card 2」、「card 3」としてもよい。

【0054】

図 2 は、本発明の別の実施形態にかかわる別のシステムのブロック図を示す。ここには、メッセージのフローも示されている。図 2 に示されたコンポーネントの一部は、図 1 のコンポーネントの一部に類似する。図 2 は更に、業者のコールセンター 42 と通信する携帯電話 40 だけでなく、Telco（電話会社）58 のインターフェースに結合されたインターフェース要素 60 も示しており、Telco 58 のインターフェースは、次に仮想カードホルダーリダイレクトモジュール 56 に結合されている。図 2 には特に発行者 12 および取得者 14 も示されている。

【0055】

この実施形態では、提示者 21 はクレジットカード（または他のある支払いデバイス）を使って、業者 22 との購入取引を開始する。カード取引について詳細に説明するが、この取引は上記とは異なり、ストアードバリューカード（stored value card）、デビットカード、無接点電話、スマートカードなどで実施することもできる。

【0056】

提示者 21 は、業者のコールセンター 42 を呼び出すのに自分の携帯電話 40 を使用する（ステップ 1）。提示者 21 は次に（例えば音声によるか、または電話番号を電話 40 に入力するなどして）エリアス識別子、例えばアイデンティティ番号を提供する。このアイデンティティ番号は、携帯電話 40 に関連する電話番号の一部またはすべてを含むことができる。追加識別子情報は、提示者 21 が保有するクレジットカードのクレジットカード番号に関連する BIN（銀行識別番号）などを含むことができる。別のタイプのエリアス識別子は、ニックネームでもよいし、または使用中の特定のクレジットカードに対して提示者 21 が割り当てた他のエリアスでもよい。次に業者 22 は、エリアス識別子のうちの 1 つ以上を業者のウェブページインターフェース 23 に入力できる（ステップ 2）。

【0057】

業者プラグイン（MPI）28 は、エリアス識別子を受信し、この識別子は検証リクエストメッセージ（VE Req（m））内でディレクトリサーバ（DS）48 へ送られる（ステップ 3）。ディレクトリサーバ 48 は、検証リクエストメッセージを受信した後に、提示者 21 に対する認証を利用できるかどうかを判断するように、アクセス制御サーバ 25 に問い合わせを行う（ステップ 3）。この例では、検証リクエストメッセージ（VE Req（m））は、エリアス識別子、例えば携帯電話 40 の電話番号を含む。

【0058】

アクセス制御サーバ（ACS）25 は、ディレクトリサーバ 48 にメッセージを通過させることにより、検証応答（VE Res（m））メッセージを送ることにより応答する（ステップ 4）。検証応答メッセージを受信した後に、業者プラグイン（MPI）28 は、ディレクトリサーバ（DS）48 を通して、アクセス制御サーバ（ACS）25 に支払

い認証リクエストメッセージ ( P A R e q ( m ) ) を送る。次にアクセス制御サーバ ( A C S ) 2 5 は、モバイル認証リクエストメッセージを発生し ( ステップ 6 )、このメッセージは仮想カードホルダーリダイレクトモジュール 5 6 を介して電話会社 ( T e l c o ) のインターフェース 5 8 へ送られる。このようにするために、ディレトリサーバ ( D S ) 4 8 は、提示者のクレジットカード番号と、その提示者の電話番号とを再関連付けし、 T e l c o のインターフェース 5 8 を介して提示者 2 1 にアクセスできるインターフェース要素 6 0 にコンタクトする ( ステップ 6 および 7 )。インターフェース要素 6 0 は、携帯電話 6 0 上のユーザーインターフェースを含むことができるし、または携帯電話 4 0 を除くデバイス上のユーザーインターフェースを含むこともできる。

【 0 0 5 9 】

10

次に認証リクエストメッセージは提示者 2 1 へ送られ、所定のパスワードまたは他の認証データで応答するよう、提示者 2 1 を促す ( ステップ 7 )。ステップ 8 では、認証データに、使用中のクレジットカードに関連するカード番号が再添付され、 T e l c o のインターフェース 5 8 を介し、発行者のアクセス制御サーバ ( A C S ) 2 5 へ補助応答メッセージが送られる。ステップ 9 では、提示者 2 1 からのパスワードを含む認証応答メッセージを受信した後に、発行者 1 2 はパスワードの有効性を判断する。発行者 1 2 がパスワードを有効であると判断した後に、発行者 1 2 は業者プラグイン ( M P I ) 2 8 へ支払い認証応答 ( P A R e s ( m ) ) メッセージを送る ( ステップ 9 )。

【 0 0 6 0 】

一部の実施形態では、支払い認証応答 ( P A R e s ( m ) ) メッセージは、提示者 2 1 に関する追加情報 ( 例えば送り先住所、コンタクト情報、例えば e メールアドレス、好みなど ) を含むことができる。例えば提示者 2 1 の送り先アドレスを発行者の A C S 2 5 から業者プラグイン ( M P I ) 2 8 へ送ってもよい。かかる実施形態では、業者 2 2 がかかる追加情報を維持する必要がないことが好ましい。したがって、提示者 2 1 により取引を開始した後に、発行者 1 2 が以前収集した任意の適当な情報を、業者 2 2 へ送ってもよい。

20

【 0 0 6 1 】

ステップ 1 0 では、ウェブページインターフェース 2 3 を使って、認証プロセスの結果が業者 2 2 の被雇用者に伝えられる。ステップ 1 1 において、業者プラグイン ( M P I ) 2 8 から業者の取得者 1 4 へ応答メッセージ 1 1 が送られる。取得者 3 0 は、 T e l c o のインターフェース 5 8 を介して提示者 2 1 へ、およびウェブページインターフェース 2 3 を介して業者 2 2 へ、メッセージを送ることにより、取引を完了する。

30

【 0 0 6 2 】

別の実施形態では、提示者 2 1 は業者のコールセンター 4 2 を経由することなくウェブページインターフェース 2 3 を介して業者のウェブサイトと相互対話できる。提示者 2 1 は、自分のアイデンティティ番号を「支払いページ」に入力でき、その後、インターフェース要素 6 0 上で認証チャレンジを受信する。

【 0 0 6 3 】

図 2 に示されたフローは、多数の利点を有する。例えば図 2 において、業者 2 2 が、提示者 2 1 が使用しているクレジットカードの実際の口座番号を見なくても、または所有していなくても、提示者 2 1 を迅速かつ効率的に適正に認証できる。一部の業者または業者の被雇用者が、提示者の支払い口座番号を不正に使用する可能性があるので、このことは提示者 2 1 に対して更に高いセキュリティを提供できる。

40

【 0 0 6 4 】

図 3 には、本発明の別の実施形態にかかわるシステムの別のブロック図が示されている。このシステムは、提示者ドメイン内にある携帯電話 7 2 を含む。業者プラグインインターフェース 7 4 は、取得者ドメイン内にあり、この取得者ドメイン内の取引開始コンポーネント 8 4 と通信する。ディレトリサーバ 7 6 とレポートサーバ 7 8 とは、相互運用可能性ドメイン内にあり、アクセス制御サーバ 8 0 と登録サーバ 8 2 は発行者ドメイン内にある。この実施形態では、モバイル認証コンポーネント 8 6 とモバイル登録コンポーネン

50

ト 8 8 は、取得者ドメイン、相互運用可能性ドメインおよび発行者ドメイン内で働くことができる。

【 0 0 6 5 】

上記とは異なり、携帯電話 7 2 はデータを送信および/または受信できる任意の適当な通信デバイス（例えば固定電話、インターネット上の P C など）とすることができる。上記のように、消費者（または提示者）は、携帯電話の番号、携帯電話の番号 + チェック数字、または他の適当なエリアス識別子に基づき、取引を開始できる。エリアス識別子は、支払い口座番号に対する代替手段として使用できる。消費者は取引を開始し、および/または取引を認証するように自分の携帯電話または携帯電話番号/エリアスも使用できる。消費者は認証プログラム登録をするのに、自分の携帯電話も使用できる。

10

【 0 0 6 6 】

提示者のリクエスト時に、取引開始コンポーネント 8 4 により業者は支払いプロセスを開始することが可能となる。この取引開始コンポーネント 8 4 は、ハードウェア、ソフトウェアの適当な任意の組み合わせの形態にすることができる。一部のケースでは、このコンポーネントは（例えば P O S ターミナル内にあるか、またはこの P O S ターミナルに接続された）業者によって操作されるハードウェア内に存在してもよい。取引開始コンポーネント 8 4 は、ウェブページがインターネット環境内の標準的 M P I と通信するのと同じように、業者プラグイン（ M P I ） 7 4 と通信できる。

【 0 0 6 7 】

従来の実施形態と同じように、取引が開始されるときに、提示者の支払いカードの番号を業者に提供しないことが望ましい。その代わりにモバイル取引インジケータと共に提示者の電話番号/エリアスまたは他の識別子に基づいて取引を開始する。

20

【 0 0 6 8 】

取引開始コンポーネント 8 4 は、あるレンジの取引開始シナリオを促進できる。このシナリオは、消費者の携帯電話の番号を自動的に業者プラグイン（ M P I ） 7 4 に送ることを可能にするシナリオと、消費者の携帯電話の番号をマニュアルで入力できるようにするシナリオとに分割できる。上記のように、 I V R、 U S S D、 S M S または W A P を使って、携帯電話の番号を業者プラグイン（ M P I ） 7 4 に自動的に送ってもよい。この方法とは異なり、電話番号をシステム内にマニュアルで入力してもよい。例えばこの電話番号は、 P C に向かっているコールセンターのエージェント、受け取りデバイスとして自分の携帯電話を使用するモバイル業者などにより、認証システムへマニュアルで入力してもよい。取引開始コンポーネント 8 4 は、提示者に取引のステータスを通知するよう、業者に対し、後方向（ b a c k w a r d s ）の通信チャンネルも提供できる。

30

【 0 0 6 9 】

業者プラグイン（ M P I ） 7 4 は、多数の機能を実行できる。例えばこのプラグインは、カード番号を使用することなく、携帯電話の番号に基づき、取引の処理を促進できる。更にこのプラグインは、検証メッセージ内に携帯チャンネル/デバイス識別子を含ませ、よって携帯チャンネルを介して取引を認証することを発行者に促すこともできる。更にこのプラグインは、それぞれの発行者による新しい提示者のオンライン加入を可能にするように、業者側への後方向の通信も提供できる。

40

【 0 0 7 0 】

ディレクトリサーバ（ D S ） 7 6 も多数の機能を提供する。このサーバは、携帯電話の番号および/または他のエリアス識別子を D I N（銀行識別番号）にマッピングでき、認証リクエストを適当な発行者にルーティングすることを可能にする。消費者が自分のカード、電話番号またはエリアス識別子を変更したい場合、アクセス制御サーバ（ A C S ） 8 0 から（逆の場合も同様）携帯電話番号および/またはエリアス識別子および/または B I N 番号を更新できる。また、ディレクトリサーバ（ D S ） 7 6 は、取引開始コンポーネント 8 4 および業者プラグイン（ M P I ） 7 4 と共同して、適当な発行者による新しい提示者のオンライン加入も容易にできる。

【 0 0 7 1 】

50

レポートサーバ 78 はレポートを提供する。このサーバは、携帯電話の番号および / またはエリア識別子も記録できる。

【0072】

アクセス制御サーバ (ACS) 80 は、多数の機能を実行できる。例えば識別された取引を受信すると、このサーバはモバイル認証コンポーネント 86 を介した、携帯電話 72 への認証リクエストメッセージの送信を開始できる。ポジティブな認証応答メッセージを受信すると、アクセス制御サーバ (ACS) 80 は、提示者の携帯電話の番号を提示者の登録された P A N (主要口座番号) に変換できる。

【0073】

モバイル認証コンポーネント 86 は、取引を認証するために提示者とアクセス制御サーバ (ACS) 80 との間で双方向のモバイルチャンネルを提供する。この双方向のチャンネルは、I V R、W A P または提示者の携帯電話 72 にローディングされたクライアントアプリケーションを含むことができる。

【0074】

登録サーバ 82 は、登録機能を提供すると共に、携帯電話番号および / またはかかるデータののためのエリアフィールドを含む。

【0075】

モバイル登録コンポーネント 88 は、提示者と登録サーバ 82 との間で双方向のモバイルチャンネルを提供する。このチャンネルは、提示者の認証プログラムに登録するのに使用され、提示者の登録された携帯電話 72 が正しいことを保証するように使用される。モバイルチャンネルの例として、I V R、W A P または提示者の携帯電話にロードされるクライアントアプリケーションを挙げることができる。このチャンネルは、モバイル認証コンポーネント 86 と同じでもよいし、またはこのコンポーネントに基づくものでもよい。

【0076】

図 4 は、支払い取引を開始する前に、提示者がデータ認証プログラムに登録する場合のプロセスフローを示す。この例では、提示者はモバイルチャンネルを通し、特定の口座を登録できる。

【0077】

図 4 を参照すると、提示者は自分の携帯電話 72 を使って、発行者に関連する口座を発行者の認証プログラムに登録する。これを行うために、携帯電話 72 は発行者のモバイル登録コンポーネント 88 と通信することができる。モバイル登録コンポーネント 88 は、着信登録リクエストを変換し、これを発行者の登録サーバ 82 (ステップ 102) へ転送する。発行者の登録サーバ 82 は、携帯電話 72 のための M S I S D N がモバイルチャンネルを通過したかどうかをチェックする (ステップ 103)。

【0078】

モバイルチャンネルを介し、携帯電話 72 のための M S I S D N が提供される場合、発行者の登録サーバ 82 は、提示者からの別の口座データをリクエストし、モバイル登録コンポーネント 88 に口座データリクエストを送る (ステップ 104)。モバイル登録コンポーネント 88 は、モバイルチャンネルおよび提示者のデバイス能力に基づき、リクエストを適合させ、これを提示者の携帯電話 72 へ送る (ステップ 105)。次に、提示者は携帯電話 72 を使用し、口座データをモバイル登録コンポーネント 88 へ伝送し戻す (ステップ 106)。次に、モバイル登録コンポーネント 88 は、口座データを変換し、それを発行者の登録サーバ 82 へ転送する (ステップ 107)。

【0079】

代替フロー A に示されるように、モバイルチャンネルにより M S I S D N が提供されない場合、発行者の登録サーバ 82 は、リクエストをモバイル登録コンポーネント 88 へ送ることにより、提示者からの M S I S D N を含む別の口座データをリクエストする (ステップ A - 1)。次に、モバイル登録コンポーネント 88 は、モバイルチャンネルおよび提示者のデバイス能力に基づきリクエストを適合させ、それを提示者の携帯電話 72 へ送る (ステップ A - 2)。次に、提示者は、携帯電話 72 を使って口座データおよび M S I S

10

20

30

40

50

D Nをモバイル登録コンポーネント 8 8へ送り戻す(ステップ A - 3)。次に、モバイル登録コンポーネント 8 8は、口座データおよび M S I S D Nを変換し、それを発行者の登録サーバ 8 2へ転送する(ステップ A - 4)。発行者の登録サーバ 8 2は、この情報を受信した後に、モバイル登録コンポーネント 8 8へ登録確認リクエストを送る(ステップ A - 5)。モバイル登録コンポーネント 8 8は、メッセージングモバイルチャンネル(例えば S M S、U S S D)に基づき、リクエストを適合させ、それを提示者の携帯電話 7 2へ送る(ステップ A - 6)。提示者は確認リクエストを受信し、そのリクエストを受け入れ、モバイル登録コンポーネント 8 8へ転送し戻す(ステップ A - 7)。モバイル登録コンポーネント 8 8が確認応答を変換し、それを発行者の登録サーバ 8 2へ転送する(ステップ A - 8)。次に発行者の登録サーバ 8 2は、ペンディング中の提示者の登録ステータスを更新する(ステップ A - 9)。

10

**【 0 0 8 0 】**

ある点において、登録サーバ 8 2は、提示者の登録ステータスの有効性をチェックする(ステップ 1 0 8)。

**【 0 0 8 1 】**

提示者の登録が受け入れ可能である場合、発行者の登録サーバ 8 2は、パスワード作成リクエストをモバイル登録コンポーネント 8 8へ送ることができる(ステップ 1 0 9)。モバイル登録コンポーネント 8 8は、モバイルチャンネルおよび提示者のデバイス能力に基づき、リクエストを適合させ、それを提示者の携帯電話 7 2へ送る(ステップ 1 1 0)。提示者は携帯電話 7 2を使って、パスワードを提供し、このパスワードをモバイル登録コンポーネント 8 8へ伝送し戻す(ステップ 1 1 1)。モバイル登録コンポーネント 8 8は、パスワードを変換し、それを発行者の登録サーバ 8 2へ転送する(ステップ 1 1 2)。次に、発行者の登録サーバ 8 2は、登録通知をモバイル登録コンポーネント 8 8へ送る(ステップ 1 1 3)。モバイル登録コンポーネント 8 8は、モバイルチャンネルおよび提示者のデバイス能力に基づき、その通知を適合させ、それを提示者の携帯電話 7 2へ送る(ステップ 1 1 4)。次に発行者の登録サーバ 8 2は、提示者の口座番号の一部により、アクセス制御サーバ 8 0を更新する(ステップ 1 1 5)。

20

**【 0 0 8 2 】**

代替フロー B では、提示者の登録に失敗している。発行者の登録サーバ 8 2は、モバイル登録コンポーネント 8 8に登録通知エラーを送る(ステップ B - 1)。モバイル登録コンポーネント 8 8は、モバイルチャンネルおよび提示者のデバイス能力に基づき、エラーメッセージを適合させ、そのエラーメッセージを提示者の携帯電話 7 2へ送る(ステップ B - 2)。

30

**【 0 0 8 3 】**

代替フロー C は、発行者が発生したパスワードに関するものである。このプロセスフローでは、発行者の登録サーバ 8 2は、(例えば提示者による入力がなくとも)ユニークなパスワードを発生する(ステップ C - 1)。発行者の登録サーバ 8 2は、発生したパスワードをモバイル登録コンポーネント 8 8へ送る(ステップ C - 2)。モバイル登録コンポーネント 8 8は、モバイルチャンネルおよび提示者のデバイス能力に基づき、メッセージを適合させ、メッセージを提示者の携帯電話 7 2へ送る(ステップ C - 3)。

40

**【 0 0 8 4 】**

図 5 は、モバイルチャンネルを通じた支払い取引中の登録のためのフローチャートを示す。図 5 を参照すると、提示者は取引開始コンポーネント 8 4を介して、支払い取引を開始する(ステップ 2 0 1)。取引開始コンポーネント 8 4は、取引の詳細を変換し、それを業者プラグイン(M P I) 7 4へ転送する(ステップ 2 0 2)。次に、図 6 に示されており、以下、更に詳細する開始する支払い取引プロセスを実行する。業者プラグイン(M P I) 7 4は、リターンされた提示者の加入ステータスをチェックする。提示者が登録されている場合、図 7 に示されており、以下更に説明する支払い認証プロセスを実行しながら、ステップ 2 1 8 でフローが続く。

**【 0 0 8 5 】**

50

提示者が登録されなかった場合、業者プラグイン（MPI）74は、取引開始コンポーネント84へBIN（銀行識別番号）情報のためのリクエストを送る（ステップ204）。取引開始コンポーネント84は、モバイルチャンネルおよび提示者のデバイス能力に基づき、リクエストを適合させ、このリクエストを提示者の携帯電話72へ送る（ステップ205）。提示者は携帯電話72を使って、リクエストされたBIN情報を提供し、この情報を取引開始コンポーネント82へ伝送し戻す（ステップ206）。取引開始コンポーネント84はリクエストされた口座データを変換し、このデータを業者プラグイン（MPI）74へ転送する（ステップ207）。次に業者プロセス（MPI）74は、ディレトリサーバ76へ収集した口座データを送ることにより、発行者の参加ステータスをリクエストする（ステップ208）。ディレトリサーバ76は、この情報を受信した後に、発行者の登録ステータスをチェックする（ステップ209）。次にディレトリサーバ76は、発行者の登録ステータスを業者プラグイン（MPI）74へ送り戻す（ステップ210）。業者プラグイン（MPI）74は発行者の登録ステータスをチェックする（ステップ211）。

#### 【0086】

発行者が認証プログラムに参加した場合、業者プラグイン（MPI）74は提示者の登録リクエストをディレトリサーバ76へルーティングする（ステップ212）。次に提示者を正式に登録するよう、発行者に対してBINおよび電話番号が送られる。次にディレトリサーバ76は、提示者の登録リクエストをアクセス制御サーバ（ACS）80へルーティングする（ステップ213）。アクセス制御サーバ（ACS）80は提示者の登録リクエストを発行者の登録サーバ82へルーティングする（ステップ214）。次に発行者の登録サーバ82は、提示者の登録リクエストをモバイル登録コンポーネント88へ送る（ステップ215）。モバイル登録コンポーネント88は、モバイルチャンネルおよび提示者のデバイス能力に基づき、リクエストを適合させ、このリクエストを提示者の携帯電話72へ送る（ステップ216）。次に図4に示された提示者登録プロセスを実行できる（ステップ217）。提示者の登録に成功すると、以下、より詳細に説明する図7のプロセスに従って、支払い取引が認証される。

#### 【0087】

発行者が認証プログラムに参加していないケースでは、業者プラグイン（MPI）74は、「発行者無登録」タイプのエラーメッセージを取引開始コンポーネント84へ送る。この取引開始コンポーネント84は、モバイルチャンネルおよび提示者のデバイス能力に基づき、リクエストを適合させ、このリクエストを提示者の携帯電話72へ送る（ステップ2A-1）。この場合、認証は行われず、支払い取引を放棄できる。

#### 【0088】

図6は、提示者が支払い取引を開始するプロセスのためのフローチャートを示す。このプロセスは、提示者がモバイルチャンネルを通して業者/取得者と支払い取引を開始すると決定したときにスタートする。このプロセスは、モバイルチャンネルを通し、支払い取引の開始に成功したときに（まだ認証されていない）、終了できる。

#### 【0089】

図6を参照すると、提示者は取引開始コンポーネント84を通して自分の携帯電話72を使って支払い取引を開始する（ステップ301）。取引開始コンポーネント84は、支払い開始リクエストを変換し、このリクエストを業者プラグイン（MPI）に転送する（ステップ302）。業者プラグイン（MPI）は、MSISDN（携帯電話番号）がモバイルチャンネルを通過したことを検証する（ステップ303）。次に、業者プラグイン（MPI）64は、検証加入リクエスト（Verify req）メッセージをディレトリサーバ76へ送る（ステップ304）。ディレトリサーバ76は、このメッセージを受信した後に、提示者の加入ステータスに関してアクセス制御サーバ（ACS）76に問い合わせをする。アクセス制御サーバ（ACS）76は、提示者の加入ステータスをディレトリサーバ（DS）76へ戻す（ステップ306）。ディレトリサーバ76は、検証加入応答（Verify res）メッセージを業者プラグイン（MPI）74へ戻す（ステップ307

）。加入応答ステータスを受信した後に、提示者は図 5 で説明されている登録プロセス（支払い取引中の登録）をスタートできる。

【 0 0 9 0 】

モバイルチャンネルによって M S I S D N が提供されない場合、業者プラグイン（ M P I ） 7 4 は、取引開始コンポーネント 8 4 を通して提示者の M S I S D N をリクエストする（ステップ 3 A - 1）。取引開始コンポーネント 8 4 は、モバイルチャンネルおよび提示者のデバイス能力に基づき、リクエストを適合させ、このリクエストを提示者の携帯電話 7 2 に送る（ステップ 3 A - 2）。次に提示者は、M S I S D N を取引開始コンポーネント 8 4 に送り戻す（ステップ 3 A - 3）。取引開始コンポーネント 8 4 は、M S I S D N を変換し、それを業者プラグイン（ M P I ） 7 4 に転送する（ステップ 3 A - 4）。 10

【 0 0 9 1 】

図 7 は、提示者が認証しなければならない、支払い取引を開始した場合のプロセスを示す。このプロセスは、提示者が支払い取引を開始し、取引を終了するための認証の用意ができたときにスタートする。認証が終わると許可を行うことができる。

【 0 0 9 2 】

図 7 を参照すると、業者プラグイン（ M P I ） 7 4 は、支払い者認証リクエスト（ P A r e q ）メッセージをアクセス制御サーバ 8 0 へ送る（ステップ 4 0 1）。次にアクセス制御サーバ 8 0 は、認証リクエスト（ M S I S D N に関連する 2 つ以上の口座識別子が存在し得る）をモバイル認証コンポーネント 8 6 へ送る（ステップ 4 0 2）。このメッセージを受信後、モバイル認証コンポーネント 8 6 は、モバイルチャンネルおよび提示者の 20 デバイス能力に基づき、リクエストを適合させ、それを提示者の携帯電話 7 2 へ送る（ステップ 4 0 3）。

【 0 0 9 3 】

提示者は携帯電話 7 2 を使ってリクエストされた認証データ（例えばパスワード）を提供し、この認証データを含む応答をモバイル認証コンポーネント 8 6 へ送り戻す（ステップ 4 0 4）。モバイル認証チャンネルは、応答を変換し、有効性の判断のためにその応答をアクセス制御サーバ（ A C S ） 8 0 へ送る（ステップ 4 0 5）。次にアクセス制御サーバ（ A C S ） 8 0 は認証応答を受信し、受信した認証データをチェックする（ステップ 4 0 6）。次にアクセス制御サーバ（ A C S ） 8 0 は、支払い者認証応答（ P A R e s ） 30 メッセージを業者プラグイン（ M P I ） 7 4 へ送り戻す（ステップ 4 0 7）。次に業者プラグイン（ M P I ） 7 4 は、認証応答メッセージをチェックする（ステップ 4 0 8）。

【 0 0 9 4 】

消費者が認証された場合、即時許可が適当であるかどうかの判断が行われる。この即時許可が適当である場合、プロセスは、図 8 に示され、以下により詳細に説明する許可プロセスに進むことができる（ステップ 4 B - 1）。即時許可が適当でない場合、業者プラグイン（ M P I ） 7 4 は、支払い未決通知メッセージをモバイル認証コンポーネント 8 6 へ送る（ステップ 4 0 9）。モバイル認証コンポーネント 8 6 は、モバイルチャンネルおよび提示者のデバイス能力に基づき、通知を適合させ、それを提示者の携帯電話 4 1 0 へ送る。次に図 8 に示されており（かつ、以下により詳細に説明するような）認証された支払い取引プロセスを実行する（ステップ 4 1 1）。 40

【 0 0 9 5 】

提示者が認証されないときには、図 7 の代替フロー A が生じ得る。アクセス制御サーバ（ A C S ） 8 0 は、発行者の認証規則に応じ、モバイル認証コンポーネント 8 6 を通して、提示者に認証リクエストを再発行してもよいし、または認証の試行回数に達した旨を提示者に通知してもよい。認証試行回数に達した場合、業者プラグイン（ M P I ）は、「認証試行回数限度到達」タイプの通知をモバイル認証コンポーネント 8 6 へ送る（ステップ 4 C - 1）。モバイル認証コンポーネント 8 6 は、モバイルチャンネルおよび提示者のデバイス能力に基づき、通知を適合させ、それを提示者の携帯電話 7 2 へ送る（ステップ 4 C - 2）。認証試行回数に達していない場合、プロセスはステップ 4 0 2 へ戻ることができる。認証試行回数に達するまでプロセスを続けることができる。 50

## 【 0 0 9 6 】

図 8 は、認証された支払い取引を許可しなければならないプロセスを説明できる。この許可は、即座に行ってもよいし延期してもよい。提示者が支払い取引を認証したときに、このプロセスはスタートし、支払い認証に成功したときに、このプロセスは終了する。

## 【 0 0 9 7 】

図 8 を参照すると、業者プラグイン ( M P I ) は、支払い許可プロセスを許可システム 7 0 へ送る ( ステップ 5 0 1 ) 。許可システム 7 0 は、支払い許可を処理する ( ステップ 5 0 2 ) 。許可システム 7 0 は、次に支払い許可応答をアクセス制御サーバ ( A C S ) 8 0 へ伝送する ( ステップ 5 0 3 ) 。アクセス制御サーバ ( A C S ) 8 0 は、支払い許可応答を業者プラグイン ( M P I ) 7 4 へ伝送する ( ステップ 5 0 4 ) 。次に、業者プラグイン ( M P I ) 7 4 は、支払い許可応答をチェックする ( ステップ 5 0 5 ) 。

10

## 【 0 0 9 8 】

支払い取引が許可された場合、業者プラグイン ( M P I ) 7 4 は、支払い受け入れ通知メッセージをモバイル許可コンポーネント 8 6 へ送る ( ステップ 5 0 6 ) 。モバイル許可コンポーネント 8 6 は、モバイルチャンネルおよび提示者のデバイス能力に基づき、その通知を適合させ、それを提示者の携帯電話 7 2 へ送る ( ステップ 5 0 7 ) 。

## 【 0 0 9 9 】

支払い取引が拒否され、許可されない場合、業者プラグイン ( M P I ) 7 4 は、支払い拒否通知メッセージをモバイル許可コンポーネントへ送る ( ステップ 5 A - 1 および 5 A - 2 ) 。モバイル許可コンポーネントがモバイルチャンネルおよび提示者のデバイス能力に基づき、通知を適合させ、それを提示者の携帯電話 7 2 へ送る。

20

## 【 0 1 0 0 】

I I I . 消費者用ポータブルデバイスおよびコンピュータ装置

## 【 0 1 0 1 】

図 9 ~ 1 0 は、本発明の実施形態に係わるシステム内で使用されるコンピュータ装置内に存在し得るポータブルコンピュータデバイスおよびサブシステムのブロック図を示す。上記一部の実施形態では、提示者は、支払いカード ( 例えばクレジットカード ) および認証チャレンジを受けるための電話またはその他の通信デバイスを有することができる。別の実施形態では、提示者は、支払い取引を行うために電話を使用することができ、支払いデータを提供し、かつ認証チャレンジのためのインターフェースとして作動するために、電話を使用することができる。カードおよび電話は消費者用ポータブルデバイスの例であり、本発明の実施形態は、これら特定の消費者用ポータブルデバイスだけに限定されるわけではない。

30

## 【 0 1 0 2 】

消費者用ポータブルデバイスの例は、任意の適当な形態となり得る。例えば適当な消費者用ポータブルデバイス消費者の財布および / またはポケットに入ることができるよう ( 例えばポケットサイズとなるよう ) 、ハンドヘルドかつコンパクトにし得る。これらデバイスとして、スマートカード、 ( 磁気ストライプを有するが、マイクロプロセッサを有しない ) 通常のクレジットカードまたはデビットカード、キーチェーンデバイス ( 例えばエクソン - モービル社から市販されているスピードパス ( S p e e d p a s s <sup>T M</sup> ) ) などを挙げる  
ことができる。消費者用ポータブルデバイスの他の例として、携帯電話、パーソナルデジタルアシスタント ( P D A ) 、ページャー、支払いカード、セキュリティカード、アクセスカード、スマートメディア、トランスポンダおよび同等物がある。消費者用ポータブルデバイスは、デビットデバイス ( 例えばデビットカード ) 、クレジットデバイス ( 例えばクレジットカード ) またはストアードバリューデバイス ( 例えばストアードバリューカード ) でもよい。

40

## 【 0 1 0 3 】

電話 3 2 ' の形態をした消費者用ポータブルデバイスの一例は、図 9 ( a ) に示されるような本体およびコンピュータが読み取りできるメディアを含むことができる ( 図 9 ( a ) は、多数のコンポーネントを示し、本発明の実施形態に係わる消費者用ポータブルデバ

50

イスは、かかるコンポーネントのサブセットの適当な任意の組み合わせを含むことができる）。コンピュータが読み取りできるメディア 32 (b) は、本体 32 (h) 内に存在していてもよいし、または本体から取り外し可能でもよい。本体 32 (h) は、プラスチック基板、ハウジングまたは他の構造体の形態とし得る。コンピュータが読み取りできるメディア 32 (b) は、データを記憶するメモリでよく、磁気ストライプ、メモリチップ、ユニークに派生されたキー、暗号化アルゴリズムなどを含む任意の適当な形態とし得る。このメモリは、情報、例えば金融情報、（例えば地下鉄または列車のパス内に記憶されるような）乗り換え情報、（アクセスバッジ内に記憶されるような）アクセス情報なども記憶することが好ましい。金融情報として、銀行口座情報、銀行識別番号（BIN）、クレジットまたはデビットカード番号情報、口座バランス情報、有効期限日、氏名、誕生日の  
10  
ような消費者の情報などを挙げることができる。この情報のいずれも、電話 32' によって送信できる。

#### 【0104】

メモリ内の情報は、従来通り、クレジットカードに関連するデータトラックのフォームでもよい。かかるトラックは、トラック 1 とトラック 2 とを含む。トラック 1（「国際航空運輸協会」）はトラック 2 よりも多くの情報を記憶しており、カード所有者の氏名だけでなく、口座番号およびその他の自由裁量のデータも含む。このトラックは、クレジットカードによる予約を安全にする際に、航空会社によってときどき使用されている。トラック 2（「米国銀行協会」）は、現在最も一般的に使用されているものである。このトラックは、ATM およびクレジットカードチェッカーによって読み取られるトラックである。  
20  
ABA（米国銀行協会）は、このトラックの仕様を設計し、すべての世界の銀行は、この仕様を守らなければならない。このトラックは、カード所有者の口座、暗号化された PIN、プラスその他の自己裁量データを含む。

#### 【0105】

コンピュータが読み取りできるメディア 32 (b) またはメモリは、任意の適当な順序で、上記ステップのうちのいずれかを実行するための符号を含むことができる。例えばコンピュータで読み取りできるメディア 32 (b) は、a) 提示者の口座に関連する口座識別子に関連するエリアス識別子を提供するための符号、b) エリアス識別子を提供した後に認証リクエストメッセージを受信するための符号、および c) 認証リクエストメッセージを受信した後に認証応答メッセージを送るための符号を含むことができる。  
30

#### 【0106】

電話 32' は更に無接点要素 32 (g) も含むことができ、この無接点要素はアンテナのような関連する無線転送（例えばデータ送信）要素を有する半導体チップ（または他のデータ記憶要素）を含むことができる。無接点要素 32 (g) は、電話 32' に関連しており（例えば電話内に埋め込まれており）、セルラーネットワークを介して送信されるデータまたは制御命令は、無接点要素インターフェース（図示されず）により、無接点要素 32 (g) へ印加できる。無接点要素インターフェースは、モバイルデバイス回路（および従ってセルラーネットワーク）と光学的無接点要素 32 (g) との間でのデータおよび/または制御命令の交換を可能にするように機能する。

#### 【0107】

無接点要素 32 (g) は、一般に規格化されたプロトコルまたはデータ転送機構（例えば ISO 14443 / NFC）に従って、近接電磁界通信（NFC）能力（または近接電磁界通信メディア）を使って、データを転送および受信できる。この近接電磁界通信能力は、短距離通信能力、例えば RFID、ブルートゥース<sup>TM</sup>、赤外線、または電話 32' と問い合わせデバイスとの間でデータを交換するのに使用できる他のデータ転送能力のことである。従って、電話 32' は、セルラーネットワークおよび近接電磁界通信能力の双方により、データおよび/または制御命令を伝送し、かつ転送できる。

#### 【0108】

電話 32' は、電話 32' の機能を処理するためのプロセッサ 32 (c)（例えばマイクロプロセッサ）と、消費者が電話番号およびその他の情報およびメッセージを見ること  
50

ができるようにするディスプレイ 32 (d) も含むことができる。この電話 32' は、更に消費者（または提示者）がデバイスに情報を入力できるようにするための入力要素 32 (e) と、消費者が音声通信、音楽などを聞くことができるようにするスピーカ 32 (f) と、消費者が電話 32' を通して自分の音声を送信できるようにするためのマイク 32 (i) とを含むことができる。電話 32' は、無線電話転送（例えばデータ送信）のためのアンテナ 32 (a) も含むことができる。

#### 【0109】

上記のように、一部の実施形態では提示者または消費者は、デビット、クレジットまたはスマートカードの形態をした消費者用ポータブルデバイスを使用できる。カードの形態をした消費者用ポータブルデバイスは、オプションとして磁気ストライプのような特徴部

10

#### 【0110】

図 9 (a) にはカード 32" の形態をした消費者用ポータブルデバイスの一例が示されている。図 9 (a) は、プラスチックの基板 32 (m) を示す。このプラスチック基板 32 (m) の上には、ポイントオブセールスターミナルのようなアクセスデバイスとのインターフェースをするための無接点要素 32 (o) が存在していてもよいし、またはこの要素はプラスチック基板内に埋め込まれていてもよい。このカードには、消費者情報 32 (p)、例えば口座番号、有効期限日および消費者の氏名をプリントしてもよいし、またはエンボス加工してもよい。プリント基板 32 (m) には、磁気ストライプ 32 (n) も存在してもよい。

20

#### 【0111】

図 9 (b) に示されるように、カード 32" は磁気ストライプ 32 (n) および無接点要素 32 (o) の双方を含むことができる。別の実施形態では、カード 32" 内に磁気ストライプ 32 (n) と無接点要素 32 (o) の双方が存在してもよい。別の実施形態では、カード 32" 内に磁気ストライプ 32 (n) または無接点要素 32 (o) のいずれかが存在してもよい。

#### 【0112】

これまで説明した図（例えば図 1 ~ 3）における種々の参加者および要素は、本明細書に説明した機能を容易にするよう、1 つ以上のコンピュータ装置を使って作動できる。これら図内の要素のいずれも、本明細書に記載した機能を容易にするよう、適当な任意の数のサブシステムも使用できる。図 10 に示されたサブシステムは、システムバス 775 を介して相互に接続されており、追加サブシステム、例えばプリンタ 774、キーボード 778、固定ディスク 779（またはコンピュータが読み取りできるメディアを含む他のメモリ）、ディスプレイアダプタ 782 に結合されたモニタ 776、およびその他の装置が示されている。I/O コントローラ 771 に結合している周辺機器および入力/出力 (I/O) デバイスは、任意の数の公知の手段、例えばシリアルポート 777 により、コンピュータシステムに接続できる。コンピュータ装置をワイドエリアネットワーク、例えばインターネット、マウス入力デバイスまたはスキャナーに接続するのに、例えばシリアルポート 777 または外部インターフェース 781 を使用できる。システムバスを介した相互接続により、中央プロセッサ 773 は、各サブシステムと通信し、システムメモリ 772 または固定ディスク 779 からの命令の実行だけでなく、サブシステムの間の情報交換の制御も可能にしている。システムメモリ 772 および/または固定ディスク 779 は、コンピュータが読み取りできるメディアを具現化できる。これら要素のいずれも、前に説明した特徴部品内に存在していてもよい。例えば前に説明したディレクトリサーバおよびアクセス制御サーバは、図 10 に示されたこれらコンポーネントのうちの 1 つ以上を有することができる。

30

40

#### 【0113】

本発明の一実施形態に係わるコンピュータで読み取りできるメディアは、上記機能のいずれかを実行するための符号を含むことができる。例えば上記ディレクトリサーバは、a

50

）提示者の口座に関連する口座識別子に関連するエリアス識別子を提供する符号と、b）前記エリアス識別子を提供した後に、認証リクエストメッセージを受信する符号と、c）前記認証リクエストメッセージを受信した後に、認証応答メッセージを送る符号とを備えることができる。このディレクトリサーバは、コンピュータが読み取りできるメディアに結合されたプロセッサも有することができ、このプロセッサは、コンピュータが読み取りできるメディア上のコンピュータフローによって具現化される命令を実行する。

【0114】

本明細書で使用した用語および表現は、本発明を説明する用語として用いたものであり、本発明を限定するために用いたものではない。特許請求の範囲内において種々の変形が可能であることが認識できるので、かかる用語および表現の使用にあたり、図面に示し、説明した特徴部、およびその一部の均等物を排除する意図はない。更に本発明の範囲から逸脱することなく、本発明の任意の実施形態の1つ以上の特徴部を、本発明の他の実施形態の他の1つ以上の特徴部と組み合わせることができる。

10

【0115】

また、上記本発明は、コンピュータソフトウェアをモジュラー態様または統合態様で使用する制御ロジックの形態で実現できるとも理解すべきである。当業者であれば、本明細書に記載した開示および教示内容に基づき、ハードウェアを使用し、更にハードウェアとソフトウェアの組み合わせを使って本発明を実施するための他の手段および/または方法も想到できよう。

【0116】

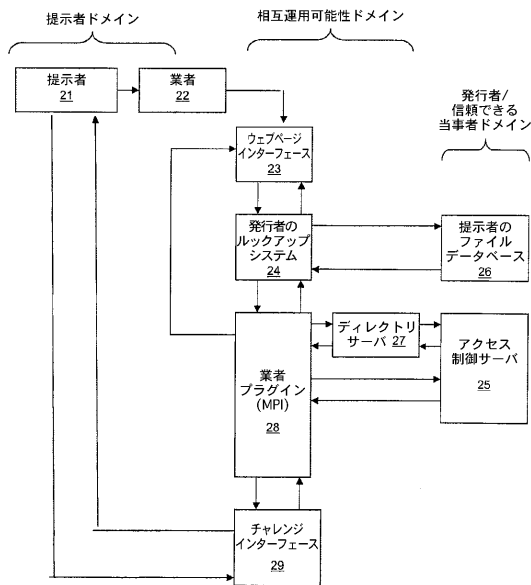
「1つの」、「ある」または「この」なる記載は、特に反対のことを示さない限り、「1つ以上」のものも意味する。

20

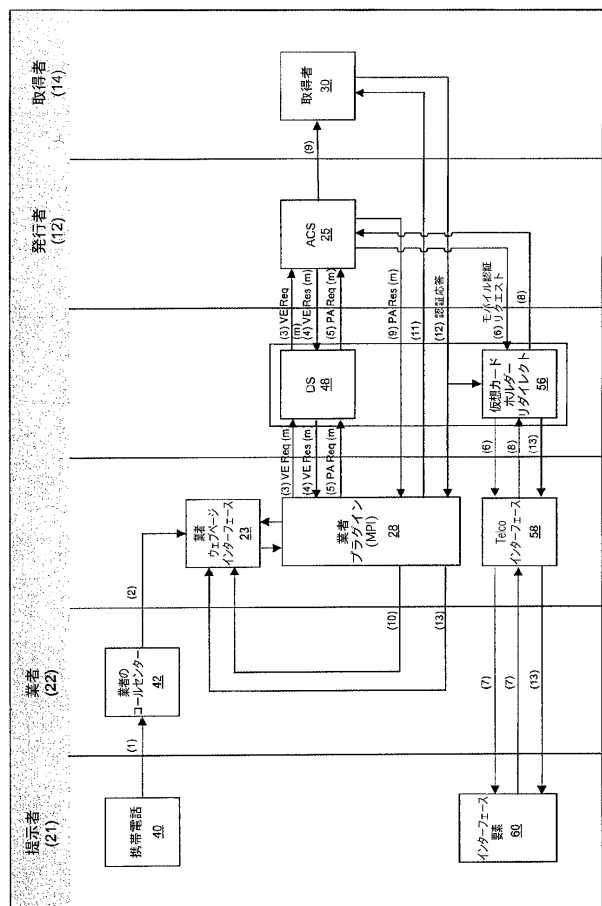
【0117】

上記すべての特許、特許出願、刊行物および説明は、すべての目的のためにこれらの全内容を本明細書で参考例として援用する。これらのいずれも、従来技術として認めるものではない。

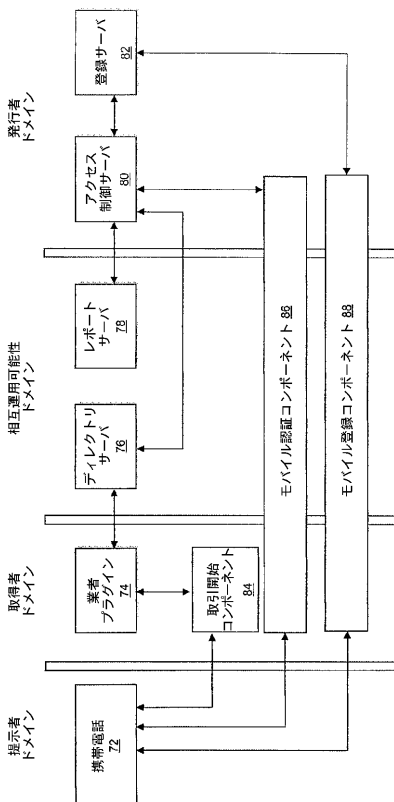
【図 1】



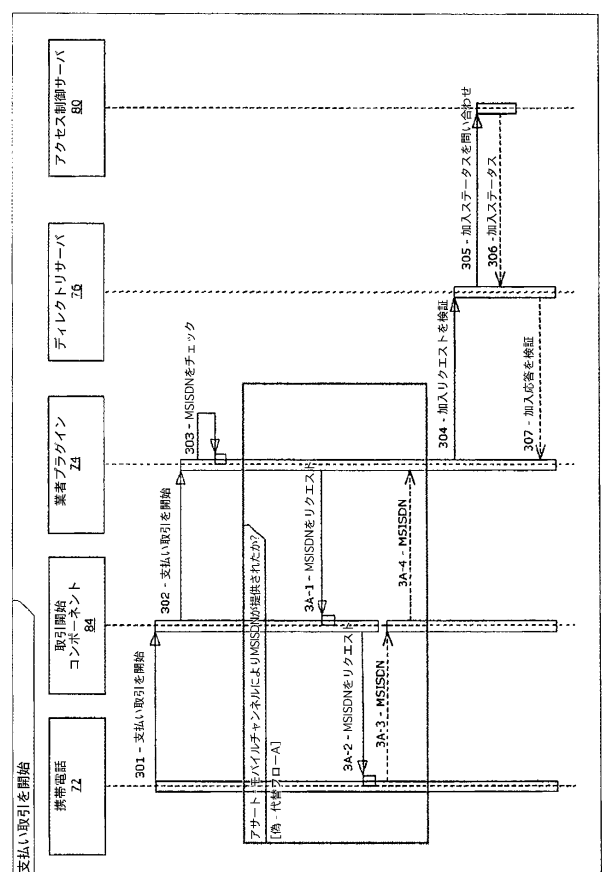
【図 2】



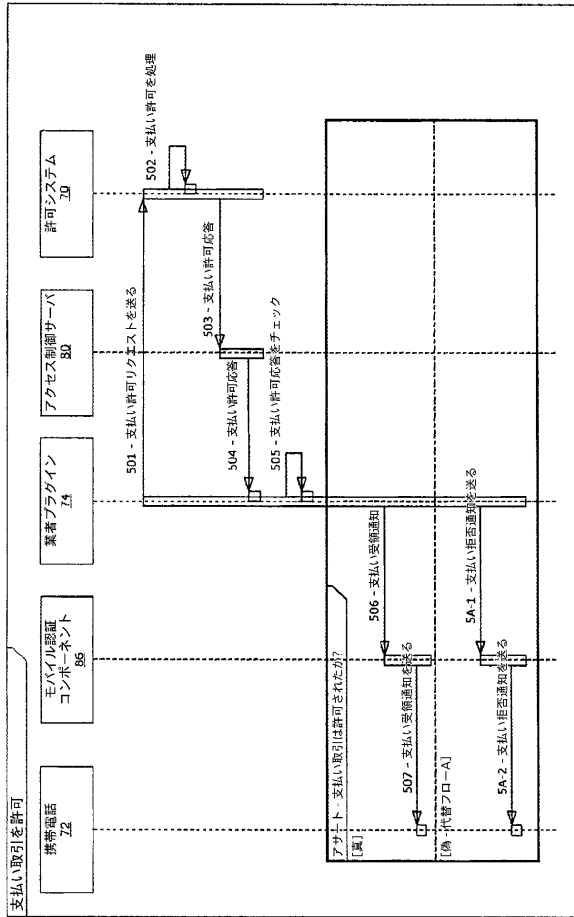
【図 3】



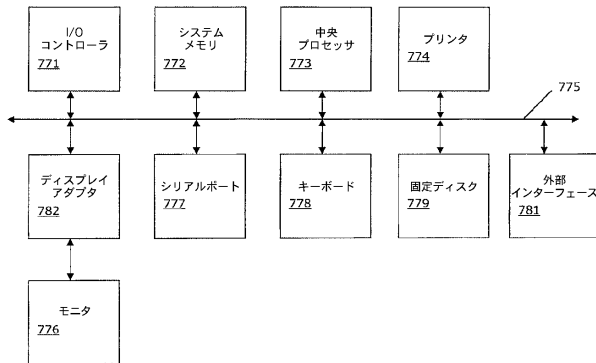
【図 6】



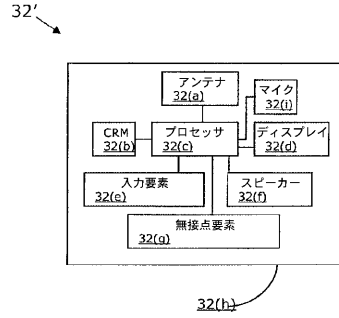
【圖 8】



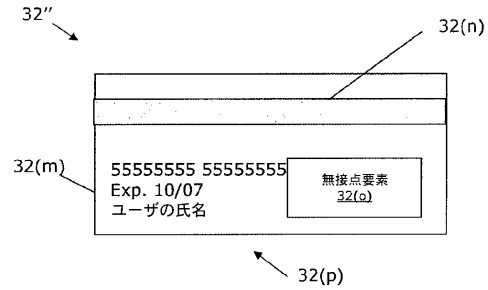
【 図 1 0 】



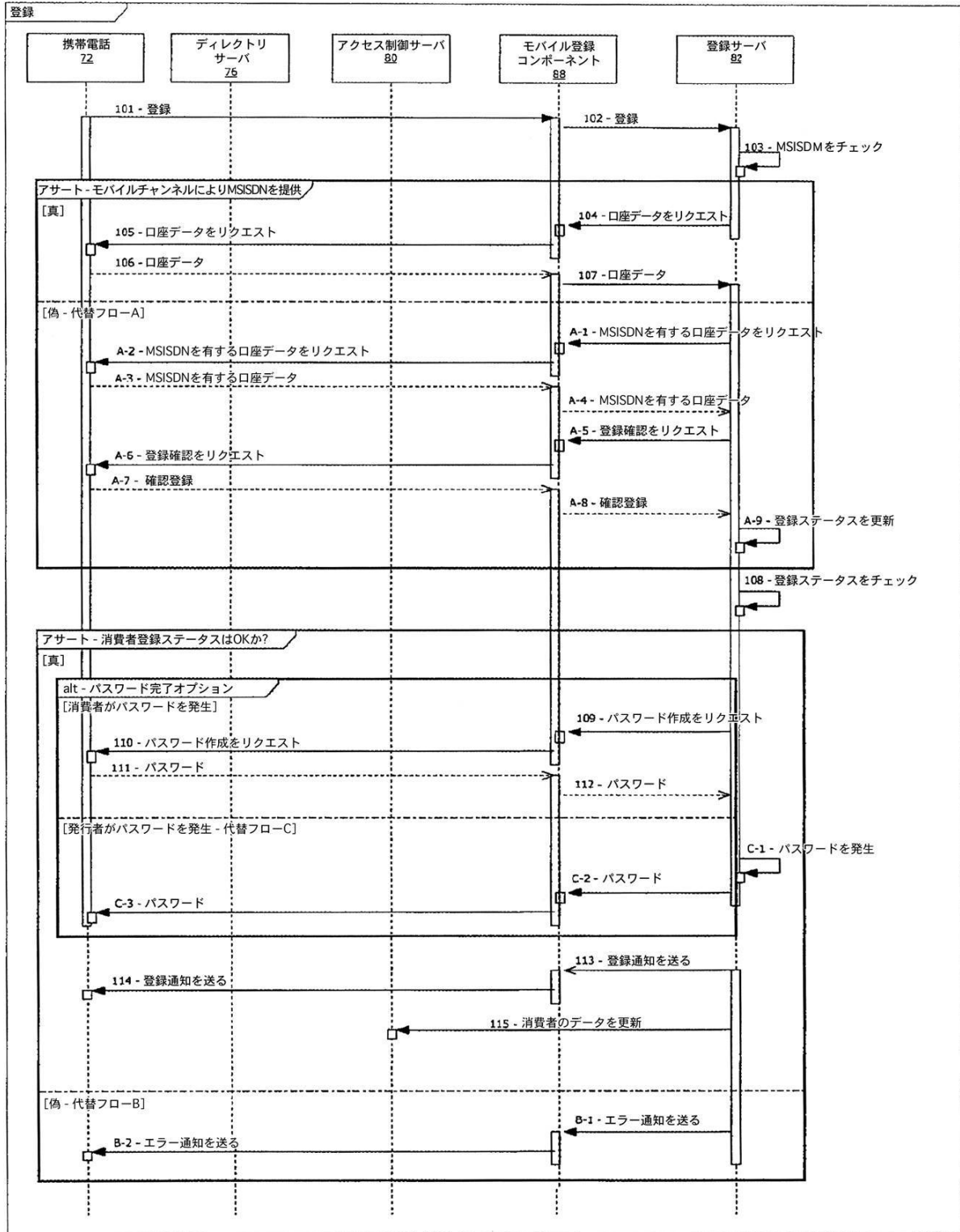
【 図 9 ( a ) 】



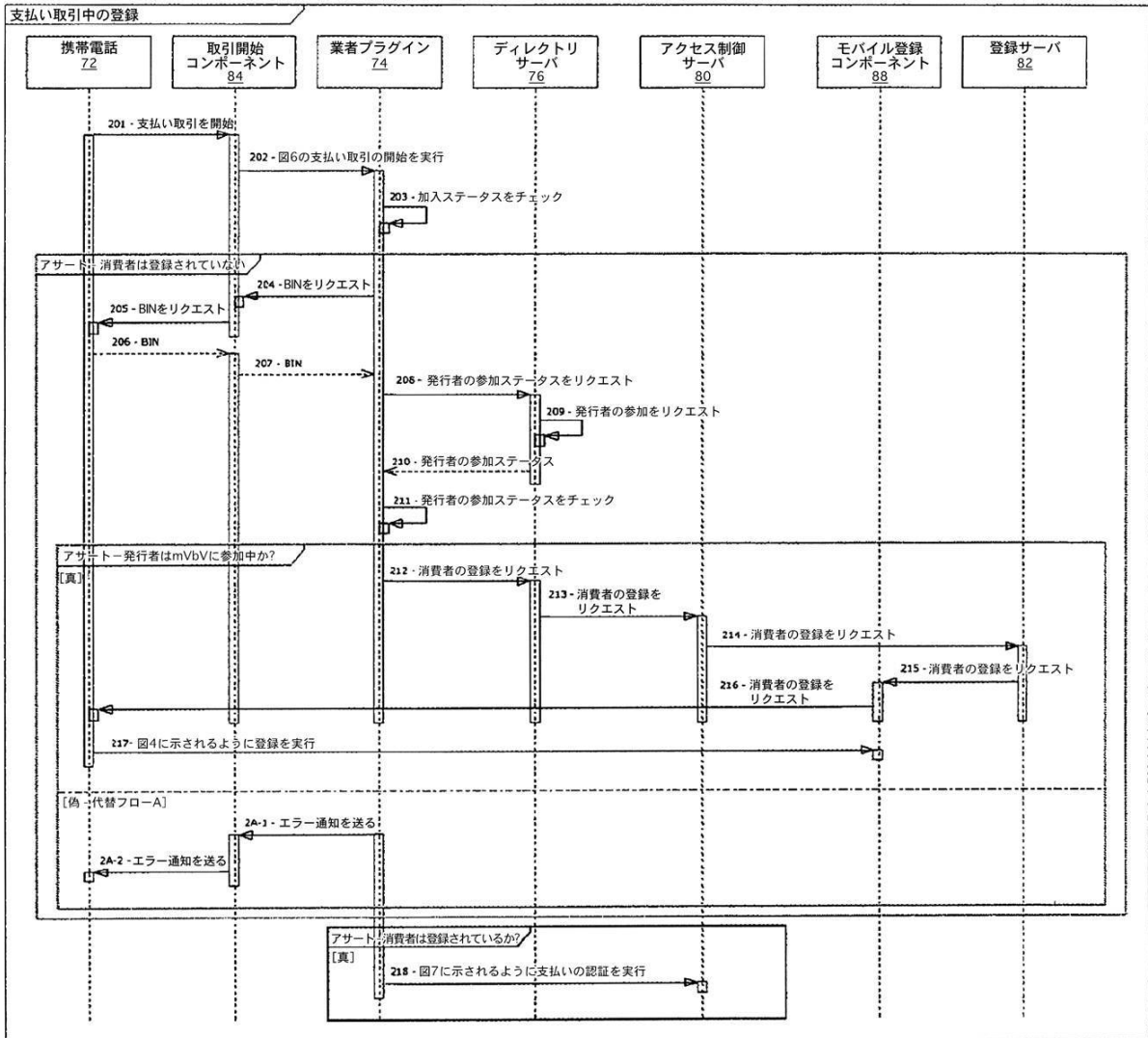
【 図 9 ( b ) 】



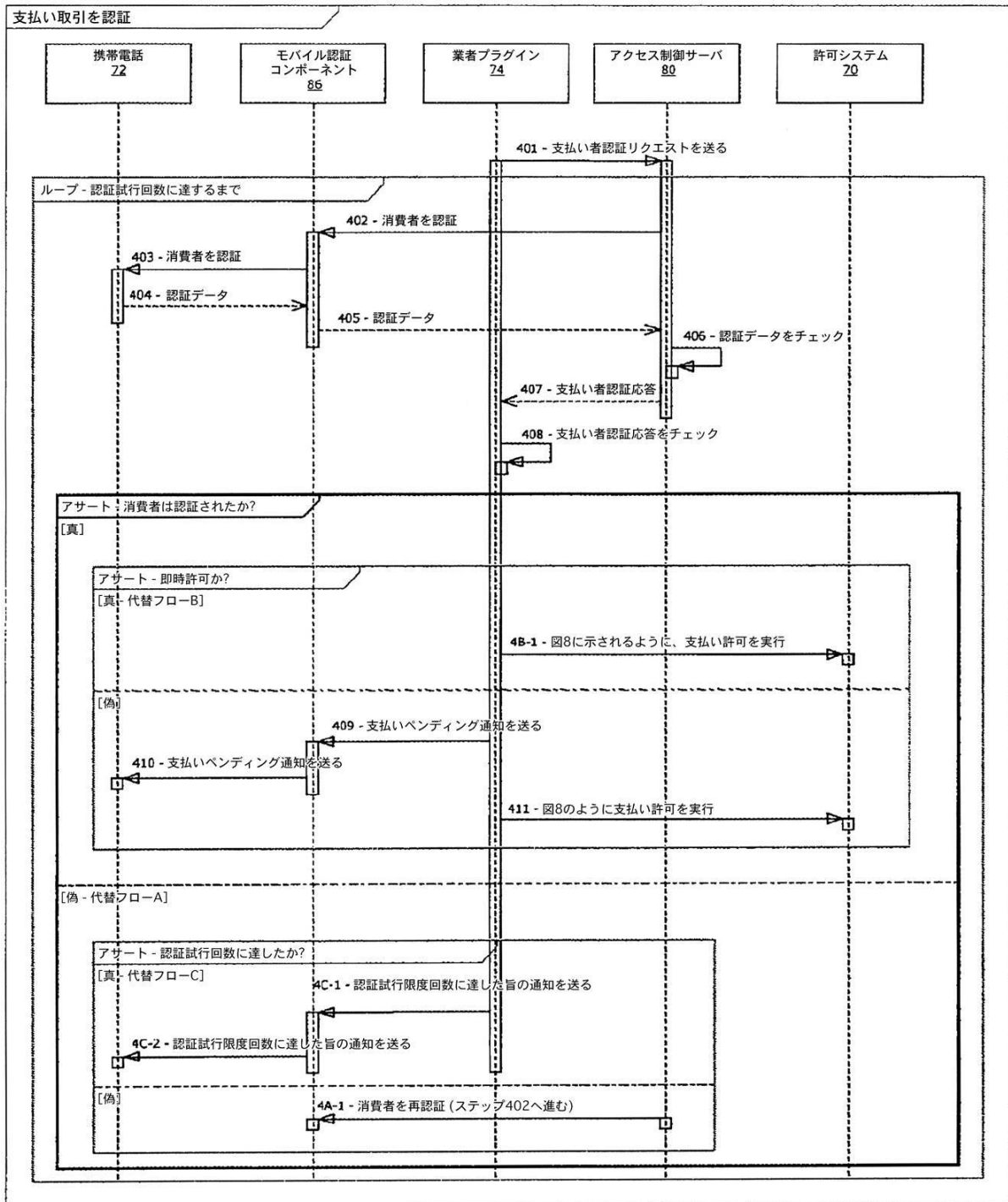
【図 4】



【図5】



【図 7】



## フロントページの続き

- (74)代理人 100094673  
弁理士 林 鈺三
- (74)代理人 100091339  
弁理士 清水 邦明
- (74)代理人 100159525  
弁理士 大日方 和幸
- (74)代理人 100147658  
弁理士 岩見 晶啓
- (72)発明者 ウェントカー、デイヴィッド  
アメリカ合衆国、カリフォルニア、サンフランシスコ、サンタ アナ アベニュー 307
- (72)発明者 リンデルシー、マイケル  
アメリカ合衆国、カリフォルニア、メンロ パーク、ダラム ストリート 416
- (72)発明者 ブランド、オリヴィエ  
アメリカ合衆国、カリフォルニア、ウォールナット クリーク、オリンピック ブールバード 2017
- (72)発明者 ディミック、ジェームズ  
イギリス国、パークシャー、マイデンヘッド、フィッシュリー ロード、サンドパイパーズ
- (72)発明者 グレウォール、トリブワン エイ・シング  
イギリス国、ハートフォードシャー、リックマンズワース、ザ パイウェイ 9

審査官 田付 徳雄

- (56)参考文献 国際公開第01/097118(WO, A1)  
特開2002-334291(JP, A)  
特開2003-099687(JP, A)  
特開2002-183612(JP, A)

- (58)調査した分野(Int.Cl., DB名)  
G06Q 10/00 - 50/34