(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-50029
(P2019-50029A)
(43)公開日　平成31年3月28日(2019.3.28)

(51)Int.Cl.		F I		テーマコード（参考）
G06Q 20/40	(2012.01)	G06Q	20/40	5L055

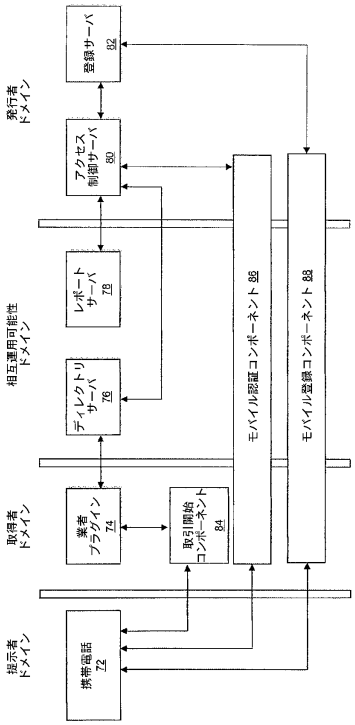
審査請求 有　請求項の数 16　ＯＬ　（全 28 頁）

(21)出願番号　特願2018-217863 (P2018-217863)
(22)出願日　平成30年11月21日 (2018.11.21)
(62)分割の表示　特願2016-159356 (P2016-159356)の分割
原出願日　平成20年4月16日 (2008.4.16)
(31)優先権主張番号　60/912,406
(32)優先日　平成19年4月17日 (2007.4.17)
(33)優先権主張国　米国 (US)

(71)出願人　508168790
ビザ　ユー．エス．エー．インコーポレイテッド
アメリカ合衆国　９４１２８－８９９９
カリフォルニア、　サンフランシスコ、ピー．オー．ボックス　８９９９
(74)代理人　110000855
特許業務法人浅村特許事務所
(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
最終頁に続く

(54)【発明の名称】取引の当事者を認証するための方法およびシステム

(57)【要約】
【課題】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ァイ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。
【解決手段】本発明の一実施形態は、提示者に関連する口座に関連するエリアス識別子を受信するステップと、この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ステップと、信頼できる関連した当事者を決定した後に、この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、検証応答メッセーを受信するステップとを含む方法に関する。
【選択図】図３



【特許請求の範囲】
【請求項１】
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、そして
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。
【請求項２】
前記エリアス識別子は、電話番号である、請求項１に記載の方法。
【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】
前記提示者に、認証リクエストメッセージの送信を開始するステップを更に含む、請求項１に記載の方法。
【請求項５】
前記提示者に、認証リクエストメッセージの送信を開始するステップを更に含み、その後、アクセス制御サーバが前記認証リクエストメッセージを提示者に送る、請求項１に記載の方法。
【請求項６】
前記エリアス識別子を受信する前に、前記提示者は、携帯電話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７】
ディレクトリサーバにより、前記ステップａ）～ｄ）を実行する、請求項１に記載の方法。
【請求項８】
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７に記載の方法。
【請求項９】
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ための符号と、
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ための符号とを備え、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ための符号を備えるコンピュータが読み取りできるメディア。
【請求項１０】
プロセッサと、
前記プロセッサに結合された請求項９に記載のコンピュータが読み取りできるメディアシステムとを備えるディレクトリサーバ。
【請求項１１】
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。
【請求項１２】
前記エリアス識別子は、電話番号である、請求項１１に記載の方法。
【請求項１３】
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１１に記載の方法。
【請求項１４】
前記提示者が操作する電話で、前記認証リクエストメッセージが受信される、請求項１３に記載の方法。
【請求項１５】
前記認証応答メッセージは、パスワードまたはＰＩＮ番号を含む、請求項１４に記載の方法。
【請求項１６】
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１１に記載の方法。
【請求項１７】
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１１に記載の方法。
【請求項１８】
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ための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。
【請求項１９】
プロセッサと、
前記プロセッサに結合されたアンテナと、
前記プロセッサに結合されたマイクと、
前記プロセッサに結合された請求項１８に記載のコンピュータが読み取りできるメディアとを備える電話。
【請求項２０】
前記プロセッサに結合された無接点要素を更に備える、請求項１９に記載の電話。
【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ァイ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、資源を最小限に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。

【０００５】

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。

【０００６】

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】

【０００７】

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ァイ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ァイルデータを認証することも可能となる。プロファイルデータの提供およびプロファイル更新のような別の能力も実行できる。

【０００８】

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。

【０００９】

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。

【００１０】

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。

【００１１】

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。

ＡＣＳ：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。

ＤＳ：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（ＭＰＩ）と発行者のＡＣＳ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。

ＩＶＲ：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。

ＳＭＳ：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ＳＭＳ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。

ＭＰＩ：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。

ＭＳＩＳＤＮ：モバイル加入者用ＩＳＤＮ番号－モバイル加入者用ＩＳＤＮ（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。

ＵＳＳＤ：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、ＧＳＭネットワークのチャンネルを通した情報の伝送をサポートするためのＧＳＭ（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。ＵＳＳＤ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。

ＷＡＰ：無線アプリケーションプロトコル－ＷＡＰブラウザは、ＰＣ（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ＷＡＰ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（ＳＭＳ）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ＴＣＰ／ＩＰ）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（ＰＤＡ）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。

【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をブラウジングする。 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、エリアス識別子を受け取る。このエリアス識別子は、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。エリアス識別子は、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。エリアス識別子が受信された後に、この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。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。

【００２１】

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、送金などとすることができる。

【００２２】

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。

【００２３】

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。

【００２４】

図１は、業者２２と通信している提示者２１を示す。業者２２は、ウェブページインターフェース２３を提供でき、このウェブページインターフェース２３は、発行者のルックアップシステム２４に結合できる。発行者のルックアップシステム２４は、業者プラグイン（ＭＰＩ）２８、ディレクトリサーバ２７、アクセス制御サーバ２５、提示者のファイルデータベース２６だけでなく、チャレンジインターフェース２９にも作動的に結合できる。

【００２５】

図１では、提示者ドメインは、提示者２１と業者２２とを含む。提示者２１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２２は受領者の一例であり、提示者２１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２１は、インターネット２２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。

【００２６】

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２１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２１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２１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２１を認証するのに使用できる提示者のプロファイルデータを有することができる。この提示者のプロ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。

【００２７】

信頼できる当事者は、アクセス制御サーバ２５（ＡＣＳ）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ＡＣＳを共用してもよいし、またはＡＣＳ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。

【００２８】

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。

【００２９】

提示者のファイルデータベース２６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。

【００３０】

相互運用可能性ドメインは、ディレクトリサーバ２７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２７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、Ｖｉｓａのようなサービス機構によってディレクトリサーバ２７を作動させることができる。

【００３１】

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。

【００３２】

提示者２１と業者２２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。

【００３３】

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２１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２１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２１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（例えば電話）に関連させることができる。例えばエリアス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ス識別子は、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。

【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）サービスのような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。

【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。

【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ァイ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ァイルデータを使ってプロファイ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。

【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（または他のエリアス識別子）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２１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２１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２２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２１は、業者２２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２１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２２と相互対話できる。

【００４２】

発注後、提示者２１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２２に提供する。提示者２１の口座番号の代わりにこの情報を業者２２に提供することもできる。提示者２１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２１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２２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２２は、ウェブページインターフェース２３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２２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２３に入力してもよい。別の実施形態では、提示者２１はウェブページインターフェース２３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２３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２４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２４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２６を維持する。次に、発行者のルックアップシステム２４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）２８へ転送される。

【００４５】

次に、業者プラグイン（ＭＰＩ）２８は、提示者２１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２１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）２７およびアクセス制御サーバ（ＡＣＳ）２５に問い合わせが行われる。ディレクトリサーバ２７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２１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２１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）２５は、認証プログラムにより提示者２１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２１がデータ認証プログラムに入会していない場合、業者２２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２１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２１に与えてもよい。

【００４７】

発行者および提示者２１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使用できる場合、アクセス制御サーバ（ＡＣＳ）２５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（ＭＰＩ）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）このメッセージは、業者プラグイン（ＭＰＩ）２８へ送られる。

【００４８】

業者プラグイン（ＭＰＩ）２８は、次にチャレンジインターフェース２９を通して認証チャレンジを提示者２１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ジュール２９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（ＵＳＳＤ）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ＳＭＳ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。

【００４９】

提示者２１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ＳＭＳメッセージを介して発せられた場合、提示者２１はパスワードを含む応答ＳＭＳ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せられた場合、提示者２１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。

【００５０】

業者プラグイン（ＭＰＩ）２８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（ＡＣＳ）２５へ送られる。発行者のアクセス制御サーバ（ＡＣＳ）２５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（ＭＰＩ）２８へレポートする。次に、業者プラグイン（ＭＰＩ）２８は、ウェブページインターフェース２３を介して、検証の結果を業者２２へ通知する。検証に成功した場合、業者２２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。

【００５１】

取引が完了した後に、ウェブページインターフェース２３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２２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２１が正式に認証されたこと、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。

【００５２】

提示者２１と業者２２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２１ではなく、業者２２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２２はシステムと相互対話できる。業者２２が提示者２１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２１は自分のデバイスで認証チャンネルを受信し、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「ｃａｒｄ１」、「ｃａｒｄ２」、「ｃａｒｄ３」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、Ｔｅｌｃｏ５８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（ＰＡ　Ｒｅｑ（ｍ））を送る。次にアクセス制御サーバ（ＡＣＳ）２５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５６を介して電話会社（Ｔｅｌｃｏ）のインターフェース５８へ送られる。このようにするために、ディレクトリサーバ（ＤＳ）４８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、Ｔｅｌｃｏのインターフェース５８を介して提示者２１にアクセスできるインターフェース要素６０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６０は、携帯電話６０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４０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。

【００５９】

次に認証リクエストメッセージは提示者２１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２１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、Ｔｅｌｃｏのインターフェース５８を介し、発行者のアクセス制御サーバ（ＡＣＳ）２５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２１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１２はパスワードの有効性を判断する。発行者１２がパスワードを有効であると判断した後に、発行者１２は業者プラグイン（ＭＰＩ）２８へ支払い認証応答（ＰＡ　Ｒｅｓ（ｍ））メッセージを送る（ステップ９）。

【００６０】

一部の実施形態では、支払い認証応答（ＰＡ　Ｒｅｓ（ｍ））メッセージは、提示者２１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２１の送り先アドレスを発行者のＡＣＳ２５から業者プラグイン（ＭＰＩ）２８へ送ってもよい。かかる実施形態では、業者２２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２１により取引を開始した後に、発行者１２が以前収集した任意の適当な情報を、業者２２へ送ってもよい。

【００６１】

ステップ１０では、ウェブページインターフェース２３を使って、認証プロセスの結果が業者２２の被雇用者に伝えられる。ステップ１１において、業者プラグイン（ＭＰＩ）２８から業者の取得者１４へ応答メッセージ１１が送られる。取得者３０は、Ｔｅｌｃｏのインターフェース５８を介して提示者２１へ、およびウェブページインターフェース２３を介して業者２２へ、メッセージを送ることにより、取引を完了する。

【００６２】

別の実施形態では、提示者２１は業者のコールセンター４２を経由することなくウェブページインターフェース２３を介して業者のウェブサイトと相互対話できる。提示者２１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６０上で認証チャレンジを受信する。

【００６３】

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２２が、提示者２１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２１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２１に対して更に高いセキュリティを提供できる。

【００６４】

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７２を含む。業者プラグインインターフェース７４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８４と通信する。ディレクトリサーバ７６とレポートサーバ７８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８０と登録サーバ８２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８６とモバイル登録コンポーネント８８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。

【００６５】

上記とは異なり、携帯電話７２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ＰＣ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。

【００６６】

提示者のリクエスト時に、取引開始コンポーネント８４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８４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ＰＯＳターミナル内にあるか、またはこのＰＯＳ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８４は、ウェブページがインターネット環境内の標準的ＭＰＩと通信するのと同じように、業者プラグイン（ＭＰＩ）７４と通信できる。

【００６７】

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。

【００６８】

取引開始コンポーネント８４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（ＭＰＩ）７４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、ＩＶＲ、ＵＳＳＤ、ＳＭＳまたはＷＡＰを使って、携帯電話の番号を業者プラグイン（ＭＰＩ）７４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、ＰＣ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８４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（ｂａｃｋｗａｒｄｓ）の通信チャンネルも提供できる。

【００６９】

業者プラグイン（ＭＰＩ）７４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。

【００７０】

ディレクトリサーバ（ＤＳ）７６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ＤＩＮ（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（ＡＣＳ）８０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ＢＩＮ番号を更新できる。また、ディレクトリサーバ（ＤＳ）７６は、取引開始コンポーネント８４および業者プラグイン（ＭＰＩ）７４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。
【００７１】
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／またはエリアス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ＰＡＮ（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、ＩＶＲ、ＷＡＰ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ためのエリアスフィールドを含む。
【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、ＩＶＲ、ＷＡＰ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ＭＳＩＳＤＮ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ＭＳＩＳＤＮ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ＭＳＩＳＤＮ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ＭＳＩＳＤＮ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ＭＳＩＳＤＮをモバイル登録コンポーネント８８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８８は、口座データおよびＭＳＩＳＤＮ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Ａ－４）。発行者の登録サーバ８２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８８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８８は、メッセージングモバイルチャンネル（例えばＳＭＳ、ＵＳＳＤ）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－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８８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８８が確認応答を変換し、それを発行者の登録サーバ８２へ転送する（ステップＡ－８）。次に発行者の登録サーバ８２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）。

【００８０】

ある点において、登録サーバ８２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１０８）。

【００８１】

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８２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８８へ送ることができる（ステップ１０９）。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１１０）。提示者は携帯電話７２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８８へ伝送し戻す（ステップ１１１）。モバイル登録コンポーネント８８は、パスワードを変換し、それを発行者の登録サーバ８２へ転送する（ステップ１１２）。次に、発行者の登録サーバ８２は、登録通知をモバイル登録コンポーネント８８へ送る（ステップ１１３）。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、その通知を適合させ、それを提示者の携帯電話７２へ送る（ステップ１１４）。次に発行者の登録サーバ８２は、提示者の口座番号の一部により、アクセス制御サーバ８０を更新する（ステップ１１５）。

【００８２】

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８２は、モバイル登録コンポーネント８８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、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７２へ送る（ステップＢ－２）。

【００８３】

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８２は、（例えば提示者による入力がなくても）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８２は、発生したパスワードをモバイル登録コンポーネント８８へ送る（ステップＣ－２）。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、メッセージを適合させ、メッセージを提示者の携帯電話７２へ送る（ステップＣ－３）。

【００８４】

図５は、モバイルチャンネルを通し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８４を介して、支払い取引を開始する（ステップ２０１）。取引開始コンポーネント８４は、取引の詳細を変換し、それを業者プラグイン（ＭＰＩ）７４へ転送する（ステップ２０２）。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（ＭＰＩ）７４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２１８でフローが続く。

【００８５】

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、ディレクトリサーバ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）。ディレクトリサーバ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）。次にディレクトリサーバ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クトリサーバ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。次にディレクトリサーバ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（ＶＥ　ｒｅｑ）メッセージをディレクトリサーバ７６へ送る（ステップ３０４）。ディレクトリサーバ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クトリ

サーバ（ＤＳ）７６へ戻す（ステップ３０６）。ディレクトリサーバ７６は、検証加入応答（ＶＥ　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。

【００９０】

モバイルチャンネルによってＭＳＩＳＤＮが提供されない場合、業者プラグイン（ＭＰＩ）７４は、取引開始コンポーネント８４を通して提示者のＭＳＩＳＤＮをリクエストする（ステップ３Ａ－１）。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に送る（ステップ３Ａ－２）。次に提示者は、ＭＳＩＳＤＮを取引開始コンポーネント８４に送り戻す（ステップ３Ａ－３）。取引開始コンポーネント８４は、ＭＳＩＳＤＮを変換し、それを業者プラグイン（ＭＰＩ）７４に転送する（ステップ３Ａ－４）。

【００９１】

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。

【００９２】

図７を参照すると、業者プラグイン（ＭＰＩ）７４は、支払い者認証リクエスト（ＰＡ　ｒｅｑ）メッセージをアクセス制御サーバ８０へ送る（ステップ４０１）。次にアクセス制御サーバ８０は、認証リクエスト（ＭＳＩＳＤＮ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８６へ送る（ステップ４０２）。このメッセージを受信後、モバイル認証コンポーネント８６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４０３）。

【００９３】

提示者は携帯電話７２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８６へ送り戻す（ステップ４０４）。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（ＡＣＳ）８０へ送る（ステップ４０５）。次にアクセス制御サーバ（ＡＣＳ）８０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４０６）。次にアクセス制御サーバ（ＡＣＳ）８０は、支払い者認証応答（ＰＡ　Ｒｅｓ）メッセージを業者プラグイン（ＭＰＩ）７４へ送り戻す（ステップ４０７）。次に業者プラグイン（ＭＰＩ）７４は、認証応答メッセージをチェックする（ステップ４０８）。

【００９４】

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４Ｂ－１）。即時許可が適当でない場合、業者プラグイン（ＭＰＩ）７４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８６へ送る（ステップ４０９）。モバイル認証コンポーネント８６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４１０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４１１）。

【００９５】

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（ＡＣＳ）８０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８６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（ＭＰＩ）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８６へ送る（ステップ４Ｃ－１）。モバイル認証コンポーネント８６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７２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４０２へ戻ることができ、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。

【００９６】

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。

【００９７】

図８を参照すると、業者プラグイン（ＭＰＩ）は、支払い許可プロセスを許可システム７０へ送る（ステップ５０１）。許可システム７０は、支払い許可を処理する（ステップ５０２）。許可システム７０は、次に支払い許可応答をアクセス制御サーバ（ＡＣＳ）８０へ伝送する（ステップ５０３）。アクセス制御サーバ（ＡＣＳ）８０は、支払い許可応答を業者プラグイン（ＭＰＩ）７４へ伝送する（ステップ５０４）。次に、業者プラグイン（ＭＰＩ）７４は、支払い許可応答をチェックする（ステップ５０５）。

【００９８】

支払い取引が許可された場合、業者プラグイン（ＭＰＩ）７４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８６へ送る（ステップ５０６）。モバイル許可コンポーネント８６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７２へ送る（ステップ５０７）。

【００９９】

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（ＭＰＩ）７４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５Ａ－１および５Ａ－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７２へ送る。

【０１００】

ＩＩＩ．消費者用ポータブルデバイスおよびコンピュータ装置

【０１０１】

図９～１０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。

【０１０２】

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（例えばエクソンーモービル社から市販されているスピードパス（Ｓｐｅｅｄｐａｓｓ^{TM}）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（ＰＤＡ）、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。

【０１０３】

電話３２’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。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。

【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ＩＳＯ１４４４３／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^{TM}、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ー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も有することができる。かかるデバイスは、接触モードまたは無接点モードのいずれかで作動できる。

【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。

【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。

【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）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。

【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。

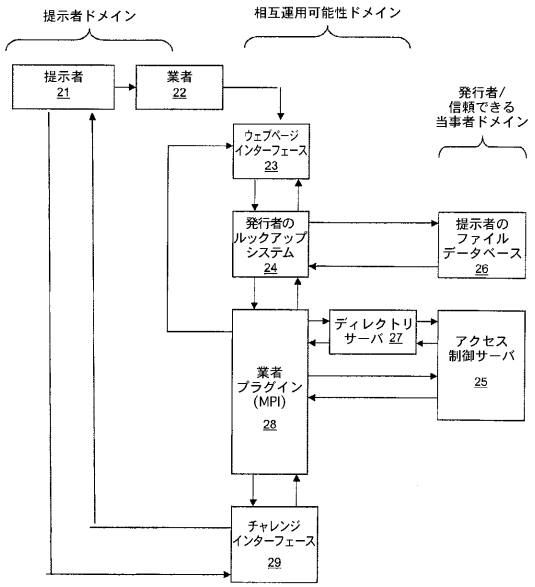
【０１１６】

「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。

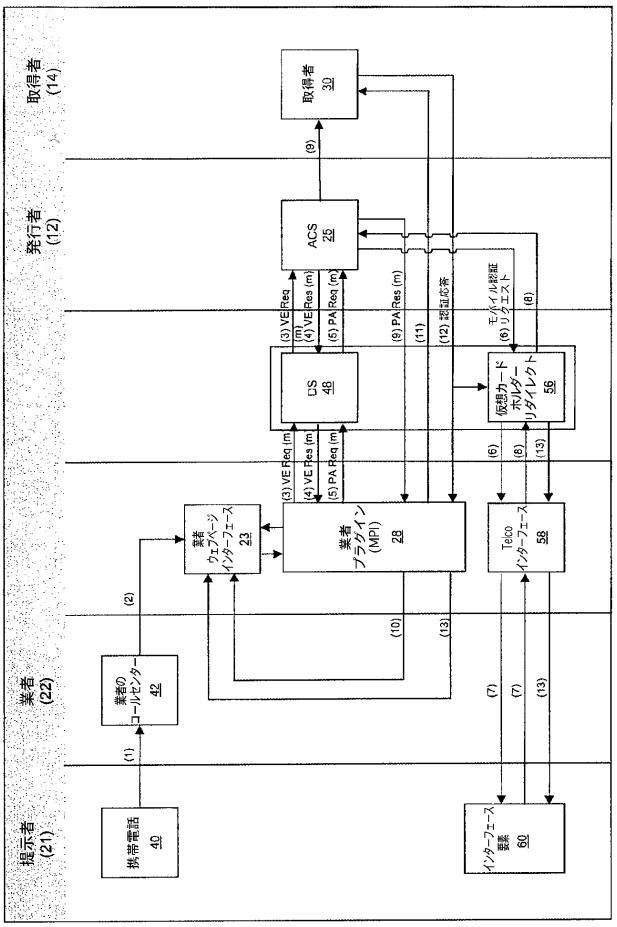
【０１１７】

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。

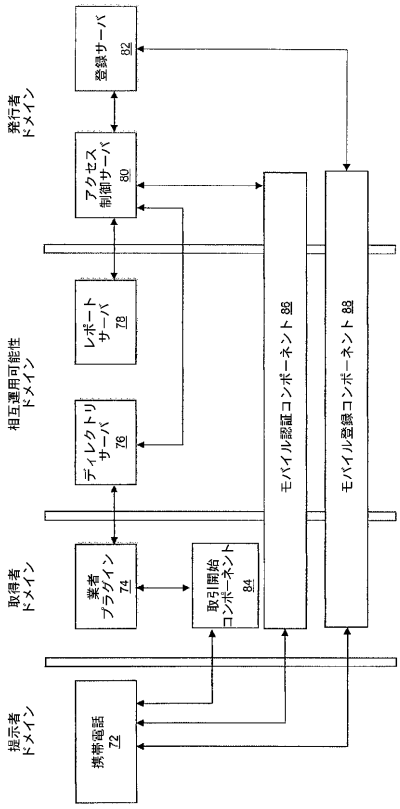
【図１】


提示者ドメイン
相互運用可能性ドメイン
提示者 21
業者 22
発行者/信頼できる当事者ドメイン
ウェブページインターフェース 23
発行者のルックアップシステム 24
提示者のファイルデータベース 26
ディレクトリサーバ 27
アクセス制御サーバ 25
業者プラグイン(MPI) 28
チャレンジインターフェース 29

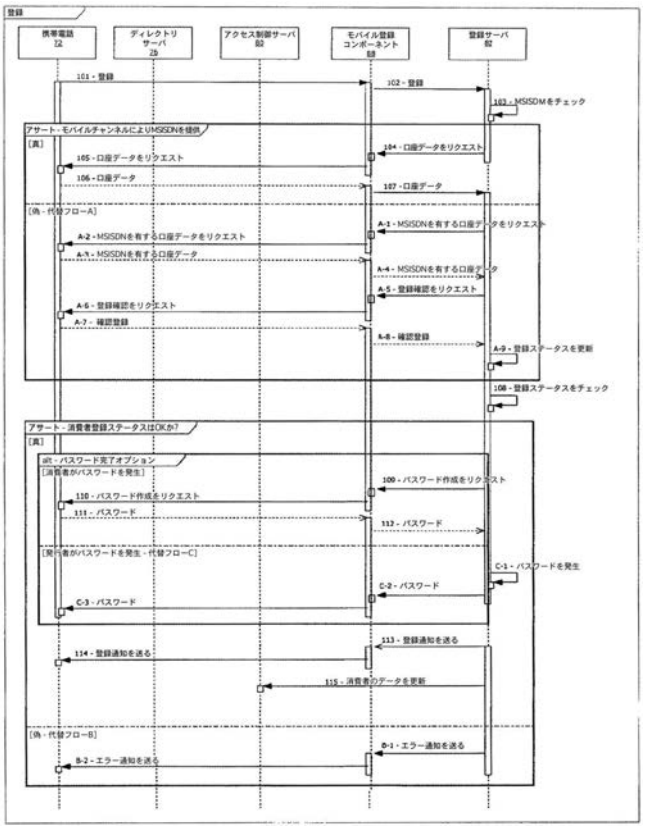
【図２】


取得者 (14)
発行者 (12)
業者 (22)
提示者 (21)
取得者 30
ACS 25
DS 48
仮想カードホルダーリダイレクト 56
業者ウェブページインターフェース 23
業者プラグイン(MPI) 28
Telcoインターフェース 58
業者のコールセンター 42
携帯電話 40
インターフェース群 60

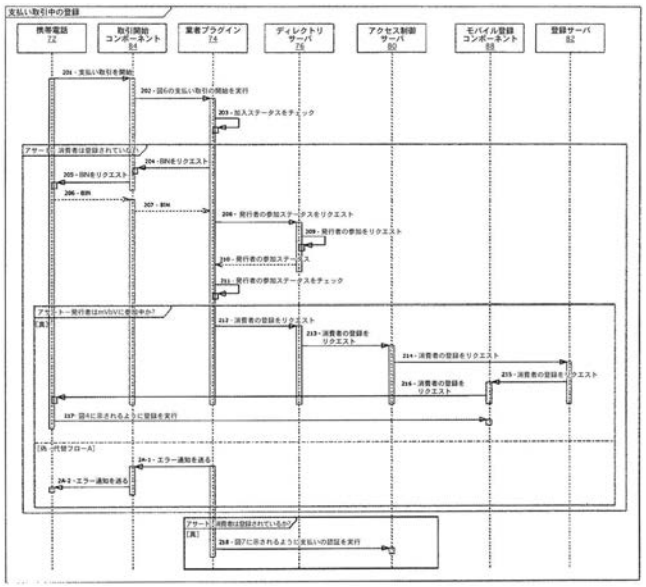
【図３】


発行者ドメイン
相互運用可能性ドメイン
取得者ドメイン
提示者ドメイン
登録サーバ 82
アクセス制御サーバ 80
レポートサーバ 78
ディレクトリサーバ 76
業者プラグイン 74
取引開始コンポーネント 84
携帯電話 72
モバイル認証コンポーネント 86
モバイル登録コンポーネント 88

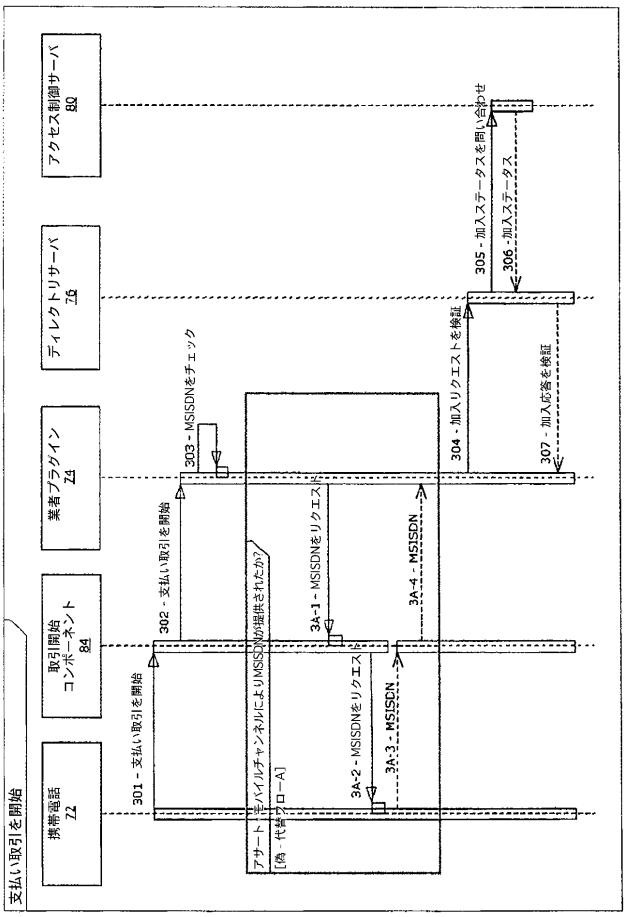
【図４】


登録
携帯電話 72
ディレクトリサーバ 76
アクセス制御サーバ 80
モバイル登録コンポーネント 88
登録サーバ 82
101 - 登録
102 - 登録
103 - MSISDNをチェック
アサート - モバイルチャンネルによりMSISDNを提供
[真]
104 - 口座データをリクエスト
105 - 口座データをリクエスト
106 - 口座データ
107 - 口座データ
[偽 - 代替フローA]
A-1 - MSISDNを有する口座データをリクエスト
A-2 - MSISDNを有する口座データをリクエスト
A-3 - MSISDNを有する口座データ
A-4 - MSISDNを有する口座データ
A-5 - 登録確認をリクエスト
A-6 - 登録確認をリクエスト
A-7 - 確認登録
A-8 - 確認登録
A-9 - 登録ステータスを更新
108 - 登録ステータスをチェック
アサート - 消費者登録ステータスはOKか?
[真]
alt - パスワード完了オプション
[消費者がパスワードを発生]
109 - パスワード作成をリクエスト
110 - パスワード作成をリクエスト
111 - パスワード
112 - パスワード
[発行者がパスワードを発生 - 代替フローC]
C-1 - パスワードを発生
C-2 - パスワード
C-3 - パスワード
113 - 登録通知を送る
114 - 登録通知を送る
115 - 消費者のデータを更新
[偽 - 代替フローB]
B-1 - エラー通知を送る
B-2 - エラー通知を送る

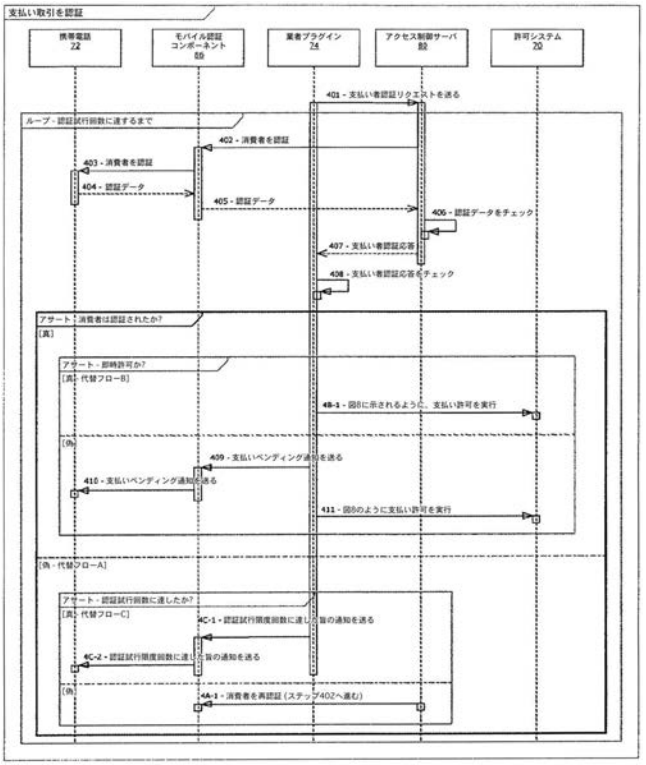
【図５】


支払い取引中の登録
携帯電話 72
取引開始コンポーネント 84
業者プラグイン 74
ディレクトリサーバ 76
アクセス制御サーバ 80
モバイル登録コンポーネント 88
登録サーバ 82

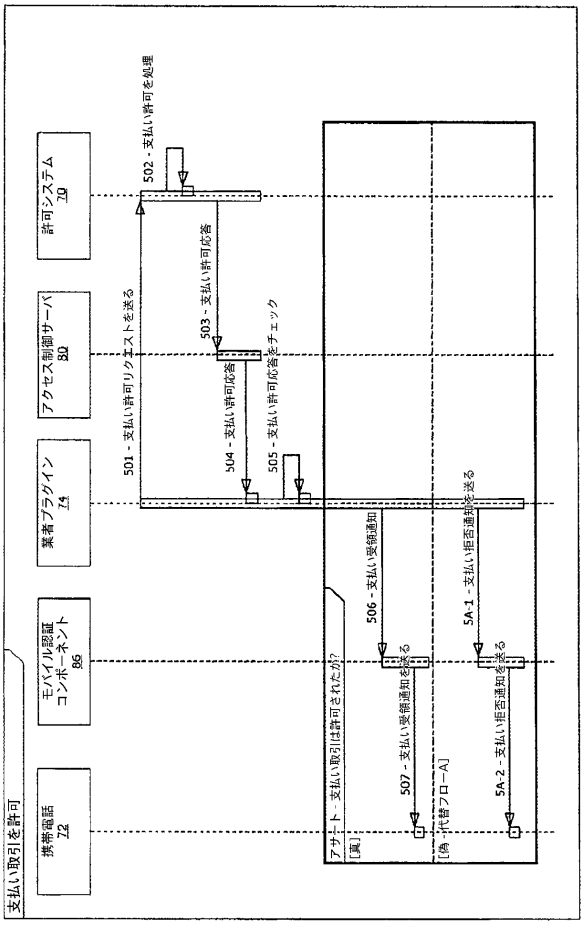
【図６】


支払い取引を開始
携帯電話 72
取引開始コンポーネント 84
業者プラグイン 74
ディレクトリサーバ 76
アクセス制御サーバ 80
301 - 支払い取引を開始
302 - 支払い取引を開始
303 - MSISDNをチェック
304 - 加入リクエストを検証
305 - 加入ステータスを問い合わせ
306 - 加入ステータス
307 - 加入応答を検証
3A-1 - MSISDNをリクエスト
3A-2 - MSISDNをリクエスト
3A-3 - MSISDN
3A-4 - MSISDN
アサート - モバイルチャンネルによりMSISDNが提供されたか?
[偽 - 代替フローA]

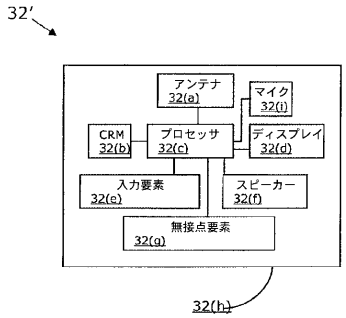
【図７】


支払い取引を認証
携帯電話 72
モバイル認証コンポーネント 86
業者プラグイン 74
アクセス制御サーバ 80
許可システム 70
401 - 支払い者認証リクエストを送る
ループ - 認証試行回数に達するまで
402 - 消費者を認証
403 - 消費者を認証
404 - 認証データ
405 - 認証データ
406 - 認証データをチェック
407 - 支払い者認証応答
408 - 支払い者認証応答をチェック
アサート - 消費者は認証されたか?
[真]
アサート - 即時許可か?
[真] - 代替フローB]
48-1 - 図8に示されるように、支払い許可を実行
[偽]
409 - 支払いペンディング通知を送る
410 - 支払いペンディング通知を送る
411 - 図9のように支払い許可を実行
[偽 - 代替フローA]
アサート - 認証試行回数に達したか?
[真] - 代替フローC]
4C-1 - 認証試行限度回数に達した旨の通知を送る
4C-2 - 認証試行限度回数に達した旨の通知を送る
[偽]
4A-1 - 消費者を再認証 (ステップ402へ進む)

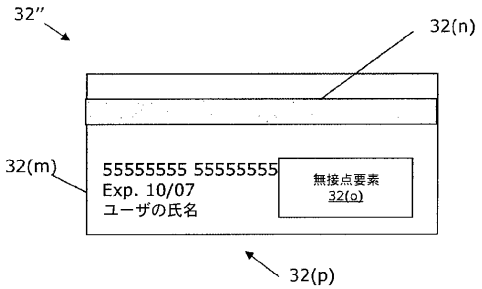
【図８】


支払い取引を許可
携帯電話 72
モバイル認証コンポーネント 86
業者プラグイン 74
アクセス制御サーバ 80
許可システム 70
501 - 支払い許可リクエストを送る
502 - 支払い許可を処理
503 - 支払い許可応答
504 - 支払い許可応答
505 - 支払い許可応答をチェック
506 - 支払い受領通知
507 - 支払い受領通知を送る
5A-1 - 支払い拒否通知を送る
5A-2 - 支払い拒否通知を送る
アサート - 支払い取引は許可されたか?
[真]
[偽 - 代替フローA]

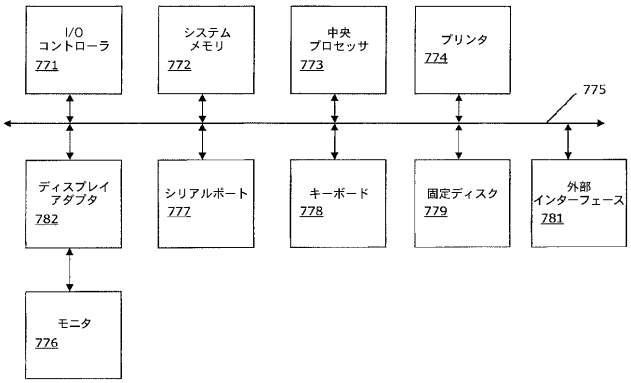
【図９（ａ）】



【図９（ｂ）】



【図１０】



【手続補正書】
【提出日】平成30年12月19日(2018.12.19)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンピュータからの認証リクエストをモバイルデバイスによって受信するステップであって、前記認証リクエストは、
エリアス識別子の受信と、
当該エリアス識別子に関連する口座番号と前記口座番号を発行した発行者の決定と、に応じて提供される、ステップと、
提示者のＰＩＮまたはパスワードを含む認証応答を前記モバイルデバイスによって前記コンピュータに提供するステップであって、前記コンピュータは、前記口座番号とＰＩＮまたはパスワードを含む取引データを含む要求を発行者のコンピュータに送信し、当該発行者のコンピュータは、前記ＰＩＮまたはパスワードを検証する、ステップと、
を含む方法。
【請求項２】
前記モバイルデバイスによって前記エリアス識別子を前記コンピュータに提供するステップを更に含む、請求項１に記載の方法。
【請求項３】
前記モバイルデバイスが携帯電話である、請求項１に記載の方法。
【請求項４】

前記エリアス識別子は、複数のエリアス識別子の中から選択されたエリアス識別子である、請求項１に記載の方法。
【請求項５】
前記エリアス識別子は、前記モバイルデバイスに関連付けられた電話番号である、請求項１に記載の方法。
【請求項６】
前記認証応答は前記ＰＩＮを含む、請求項１に記載の方法。
【請求項７】
前記認証応答は暗号化される、請求項１に記載の方法。
【請求項８】
前記取引データは暗号化される、請求項１に記載の方法。
【請求項９】
プロセッサと、
プロセッサによって実行可能なコードを含むコンピュータ読み取り可能な媒体と、からなるモバイルデバイスであって、
前記コードは
前記コンピュータからの認証リクエストをモバイルデバイスによって受信するステップであって、前記認証リクエストは、
エリアス識別子の受信と、
当該エリアス識別子に関連する口座番号と前記口座番号を発行した発行者の決定と、に応じて提供される、ステップと、
提示者のＰＩＮまたはパスワードを含む認証応答を前記モバイルデバイスによって前記コンピュータに提供するステップであって、前記コンピュータは、前記口座番号とＰＩＮまたはパスワードを含む取引データを含む要求を発行者のコンピュータに送信し、当該発行者のコンピュータは、前記ＰＩＮまたはパスワードを検証する、ステップと、
からなる方法をプロセッサによって実行可能としたコードである、モバイルデバイス。
【請求項１０】
前記方法は、
前記モバイルデバイスによって前記エリアス識別子を前記コンピュータに提供するステップを更に含む、請求項９に記載のモバイルデバイス。
【請求項１１】
前記モバイルデバイスは携帯電話である、請求項９に記載のモバイルデバイス。
【請求項１２】
前記エリアス識別子は、複数のエリアス識別子の中から選択されたエリアス識別子である、請求項９に記載のモバイルデバイス。
【請求項１３】
前記エリアス識別子は、前記モバイルデバイスに関連付けられた電話番号である、請求項９に記載のモバイルデバイス。
【請求項１４】
前記認証応答は前記ＰＩＮを含む、請求項９に記載のモバイルデバイス。
【請求項１５】
前記認証応答は暗号化される、請求項９に記載のモバイルデバイス。
【請求項１６】
前記取引データは暗号化される、請求項９に記載のモバイルデバイス。

フロントページの続き

(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、バークシャー、マイデンヘッド、フィッシェリー　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、リックマンスワース、ザ　バイウェイ　９

Ｆターム(参考) 5L055 AA75