(19)日本国特許庁(JP)　(12)登録実用新案公報(U)　(11)実用新案登録番号
実用新案登録第3198589号
(U3198589)
(45)発行日　平成27年7月9日(2015.7.9)　(24)登録日　平成27年6月17日(2015.6.17)

(51)Int.Cl.　F I
G06F 21/34 (2013.01)　G06F 21/34
G06K 19/06 (2006.01)　G06K 19/06　１１２
G06K 7/10 (2006.01)　G06K 7/10　４６４

評価書の請求 未請求　請求項の数 13　ＯＬ　（全 10 頁）

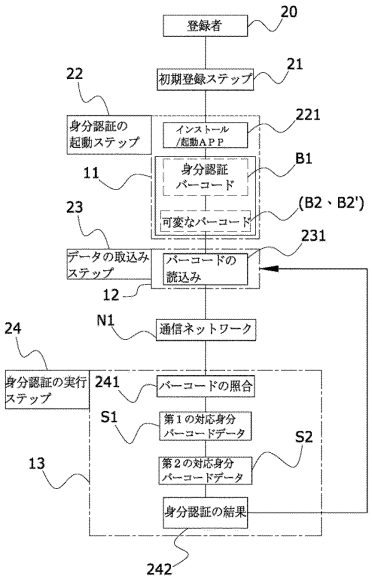
(21)出願番号　実願2015-2144(U2015-2144)
(22)出願日　平成27年4月28日(2015.4.28)

(73)実用新案権者　515116180
チュン　フワ　インターナショナル　コミュニケーション　ネットワーク　カンパニー　リミテッド
台湾　ニュー　タイペイ　シティ　２２１０２，　シーズー　ディストリクト，　シンタイ　５番　ロード，　セクター　１，　１００番，　２１階
(74)代理人　100137095
弁理士　江部　武史
(74)代理人　100173532
弁理士　井上　彰文
(74)代理人　100091627
弁理士　朝比　一夫

最終頁に続く

(54)【考案の名称】可変なバーコードを身分認証に用いるシステム

(57)【要約】　（修正有）
【課題】既存のバーコード読み取り装置を利用して、安全性の高い身分認証を行う可変なバーコードを身分認証に用いるシステムを提供する。
【解決手段】スマートフオンと、売り手側バーコードを読み取る装置と、認証機器側サーバーを含んである。そのシステムの実施方法について、登録者２０は先に一つのＡＰＰ２２１をスマートフオン１１にダウンロードして、そのＡＰＰ（アプリケーションプログラム）で自分の身分データを認証機器側のサーバー装置１３へアップロードして登録する。ユーザは取引処理におけるユーザの身分認証を行った時、ＡＰＰを展開して実行するにより、スマートフオンに二つのバーコードを表示する。その一つは身分データとしての身分認証バーコードＢ１であり、もう一つは身分データに応じて且つ一定の時間後に変化する可変なバーコードＢ２、Ｂ２‘である。この二つのバーコードをバーコード読取装置１２で読み取ってから、ユーザが元の登録者であるか否かを認証することができる。
【選択図】図２



【実用新案登録請求の範囲】
【請求項１】
サーバーで身分認証アプリケーションプログラム（ＡＰＰ）を実行することにより、通信ネットワークを介してユーザの身分認証に用いるシステムであって、当該システムは、
前記サーバーを含む認証機構と、
売り手側のリニアＣＣＤまたはＣＭＯＳバーコード読取装置と、
ユーザ側のスマートフォンと、を備え、
前記ユーザが先に前記スマートフオンで身分認証データを登録し、当該スマートフオンに前記身分認証ＡＰＰをインストールすることにより、当該身分認証ＡＰＰが同時に身分認証バーコードと、可変なバーコードとを生成し、
当該可変なバーコードは、当該身分認証バーコードデータに対応し、且つ所定の時間の経過で自動的に変化するバーコードであり、
前記リニアＣＣＤまたはＣＭＯＳバーコード読取装置は、前記ユーザの当該スマートフオンが表示する当該身分認証バーコード及び当該可変なバーコードの読取をし、且つ読取後、前記通信ネットワークを介して当該身分認証バーコード及び当該可変なバーコードを当該認証機構の当該サーバーへ送信し、
当該サーバーは、前記ユーザの当該身分認証バーコードを受信してから、当該身分認証バーコードを当該サーバーに格納してある身分データと照合し、照合が一致と認定された場合、前記所定の時間が異なる３つの対応可変なバーコードを生成し、そして、当該サーバー装置は、受信した当該可変なバーコードと当該３つの対応可変なバーコードとの照合を実行するにより、当該可変なバーコードは前記３つの対応可変なバーコードのいずれかと一致するか否かを確認することで、前記ユーザが元の登録者であるか否かを判断することを特徴とする可変なバーコードを身分認証に用いるシステム。
【請求項２】
当該認証機構の当該サーバーは、当該３つの対応可変なバーコードを、当該スマートフオンの当該身分認証ＡＰＰが当該可変なバーコードを生成することと同様に生成する、即ち、特別なアルゴリズムを利用して、当該可変なバーコードをランダムに変化させるものであり、一定なルールで推測することができないことを特徴とする請求項１に記載の可変なバーコードを身分認証に用いるシステム。
【請求項３】
当該認証機構の当該サーバーは、受信した当該身分認証バーコードを前記身分データと照合して、前記一致と認定しなかった場合、認証失敗と認定することを特徴とする請求項１に記載の可変なバーコードを身分認証に用いるシステム。
【請求項４】
当該認証機構の当該サーバーは、受信した当該身分認証バーコードを前記身分データと照合して、前記一致と認定した場合、前記所定の時間の前、中、後に変化する３つの対応可変なバーコードを生成することを実行することを特徴とする請求項１に記載の可変なバーコードを身分認証に用いるシステム。
【請求項５】
前記所定の時間が異なる当該３つの対応可変なバーコードは、当該スマートフオンの前記所定の時間と同じ時間で変化する同じ可変なバーコードと、前記所定の時間より前の時間内で変化する前の可変なバーコードと、前記所定の時間より後の時間内で変化する後の可変なバーコードと、を含むことを特徴とする請求項１の可変なバーコードを身分認証に用いるシステム。
【請求項６】
当該スマートフオンは、前記所定の時間の経過後に、新たな可変なバーコードを生成すると共に、前記可変なバーコードを消失させることを特徴とする請求項１の可変なバーコードを身分認証に用いるシステム。
【請求項７】
当該認証機構の当該サーバーは、当該可変なバーコードの前記照合を実行した後に、前

記一致するか否かにもかかわらず、生成した当該３つの可変なバーコードを消失させることを特徴とする請求項１の可変なバーコードを身分認証に用いるシステム。
【請求項８】
当該身分認証の結果が前記一致であった場合、当該サーバーは、認証成功という情報を当該売り手側へ送信することを特徴とする請求項１の可変なバーコードを身分認証に用いるシステム。
【請求項９】
当該身分認証の結果が前記一致でなかった場合、当該サーバーは、認証失敗という情報を当該売り手側へ送信することを特徴とする請求項１の可変なバーコードを身分認証に用いるシステム。
【請求項１０】
同じユーザに対し、同じ時間内に、認証結果が一致するか否かにもかかわらず、認証の実行は一回しか許されないことを特徴とする請求項１の可変なバーコードを身分認証に用いるシステム。
【請求項１１】
当該身分認証バーコード及び当該可変なバーコードの生成は、オフラインの状態で実行されることが可能であることを特徴とする請求項１の可変なバーコードを身分認証に用いるシステム。
【請求項１２】
当該可変なバーコードは、予め設定した前記所定の時間内に変化し、当該予め設定した前記所定の時間は、当該身分認証ＡＰＰが表示している時間であることを特徴とする請求項１の可変なバーコードを身分認証に用いるシステム。
【請求項１３】
当該身分認証及び当該可変なバーコードは、一つのアルゴリズムによって計算されてから、単一列のバーコードを生成することにより、前記単一列のバーコードを前記リニアＣＣＤまたはＣＭＯＳバーコード読取装置によって容易に読取られることを特徴とする請求項１の可変なバーコードを身分認証に用いるシステム。
【考案の詳細な説明】
【技術分野】
【０００１】
本考案は、可変なバーコードを身分認証に用いるシステムに係わり、特にスマートフオンのＡＰＰ（アプリケーションプログラム）でスマートフオンに、身分データとしての身分認証バーコードと、身分データに応じて且つ一定の時間後に変化する可変なバーコードとを生成し、この二つのバーコードをバーコードリーダで読み取ってから、認証機器側サーバーへ伝送して照合を行うことにより、認証することができる可変なバーコードを身分認証に用いるシステムに関する。
【背景技術】
【０００２】
現在のところ、様々な取引の振舞いに、現金支払いは面倒で時間もかかるので、クレジットカード、デビットカード、電子チケットなどが広く採用されている。しかしながら、偽カードや、詐欺的な使用などの問題も多発している。つまり、関連業界は、昔から便利で且つ安全な身分認証というニーズに完全に応じられていない。近年、スマートフオンは急速に普及しつつあるので、人々は自然に携帯電話で支払い、モバイル財布やモバイルで支払いを考える。しかし、コアの問題は、やはりユーザの身分を便利且つ安全で認証する方法を提供することにある。
【０００３】
その方法について、業界ではいつもＮＦＣ（近接無線通信）の情報伝送で認証の実行に焦点を絞るが、主要な携帯電話のオペレーティングシステムは、ＩＯＳ、Ａｎｄｒｏｉｄ、Ｗｉｎｄｏｗｓ（登録商標）の３つがあるため、一つのリーダーで読み取ることは困難を引き起こす。加えて、初期での顧客数が少ないので、売り手側は別にＮＦＣリーダーを

購入する意志が低い。したがって、悪循環の形態に陥ることが過言ではない。
【０００４】
一方、顧客は売り手側がＮＦＣリーダーを持っていないため、モバイル財布やモバイルでの支払いの申し込みは全然興味がない。また、ＡＰＰＬＥのような携帯電話メーカ、電信会社と銀行などは、モバイル財布のようなビジネスで儲けることができるが、売り手側が設備を買わないので、直ちに儲けることはできない。
【０００５】
この問題の解決提案として、一番簡単なことは、売り手側が既存のリニアＣＣＤまたはＣＭＯＳバーコードリーダ設備を採用することにある。これにより、設備を購入するためにお金を費やす必要がなく、直接に顧客の携帯電話に表示する身分認証バーコードを読み込むだけで、認証の目的を実現することができる。しかし、この方法だけでは、簡単に偽造に繋がるため、現在の市場では、暗号化された方法が採用されている。
【０００６】
しかし、バーコードを使用しても、暗号化にその形状を変更したものしか使用されていない。暗号化がある以上、復号化することを分かるシステム管理者が必ず存在し、加えて、暗号化されたデータは長期間識別システムに格納されるため、誰かが暗号解読する可能性がある。
【０００７】
米国特許Ｎｏ．8,931,703の「Payment Cards and Devices for displaying Barcodes」は、カードにバーコードが表示されるものを開示する。その支払いカードの性能については、スマートフオンに匹敵することができず、高価な電子カードを別に購入する必要がある。また、携帯も面倒であるから、消費者に受け入れることはない。
【０００８】
もう一つの米国特許Ｎｏ．8,600,883及び8,862,513の「mobile barcode generation and payment」は、予め携帯電話に電話番号と固定パスワードまたはＰＩＮ（個人暗証番号）を入力し、そして支払いプロバイダーを介して認証してから、バーコードを返送するにより、身分またはカード番号を識別することを開示する。しかし、この固定パスワードまたはＰＩＮは簡単に盗まれることがあるから、セキュリティのニーズを満たすことができない。
【先行技術文献】
【特許文献】
【０００９】
【特許文献１】米国特許第8,931,703号明細書
【特許文献２】米国特許第8,600,883号明細書
【特許文献３】米国特許第8,862,513号明細書
【考案の概要】
【考案が解決しようとする課題】
【００１０】
そこで、本考案は当該課題を解決するために開発したものであり、その目的は、主に売り手が既存のバーコード読み取り装置を利用して、更にスマートフオンと認証機構端サーバーとの協動で、安全性の高い身分認証を行う身分認証システムを提供することにある。
【課題を解決するための手段】
【００１１】
上記の目的を達成するために、本考案の可変なバーコードを身分認証に用いるシステムは、スマートフオンのＡＰＰによって、スマートフオンに、身分データとしての身分認証バーコードと、身分データに対応し且つ一定の時間後に変化する可変なバーコードとを生成し、この二つのバーコードをバーコードリーダで読み取ってから、認証機構側サーバーへ伝送し、認証機器側サーバーが認証リクエストを受信すると同時に生成した可変なバーコードデータとの照合で、ユーザが元の登録者であるか否かを認証することができる。前述の可変なバーコードは、適当な時間（約１分間）を経つと変化する。このような変化は

、システム管理者が次のバーコードへ如何に変化するかを推測することができない。変更されたバーコードは、認証機構の中にもはや存在しないことにより、解読することができない。

【考案の効果】

【００１２】

従って、スキミング、解読や偽造のような問題を解決することができる。更に、本考案のもう一つの特徴について、顧客が携帯電話を使用している場合、ネットワークの接続は必要ないことにある。バーコードは、携帯電話が携帯自体のＡＰＰでタイミングモードに基づいて生成するもので、認証機構への返送で生成することではないので、顧客の使用が非常に便利である。

【図面の簡単な説明】

【００１３】

本考案の目的、技術特徴、及び実施後の効果を一層理解するために、以下の図面を参照してより詳しく説明する。

【図１】図１は、本考案のシステムの概略ブロック図である。

【図２】図２は、本考案のシステムの概略フローチャートである。

【図３】図３は、本考案の実施概略図（一）である。

【図４】図４は、本考案の実施概略図（二）である。

【考案を実施するための形態】

【００１４】

図１を参照し、本考案の可変なバーコードを身分認証に用いるシステムは、主にユーザ側Ｕ１であるスマートフオン１１と、売り手側Ｃ１であるリニアＣＣＤまたはＣＭＯＳバーコード読取り装置１２と、認証機構側ＩＤ１であるサーバー装置１３とから構成してなる。売り手側Ｃ１と認証機構側ＩＤ１は、通信ネットワークＮ１（例えば、インターネットまたはモバイル通信３/４Ｇ）を介して相互に通信可能に接続される。即ち、売り手側Ｃ１は、リニアＣＣＤまたはＣＭＯＳバーコード読み取り装置１２によって読取ったバーコードデータを様々な通信ネットワークＮ１を介して、認証機構側ＩＤ１のサーバー装置１３へ伝送するにより、身分認証の作業を行う。また、売り手側Ｃ１は一般的に店舗を指し、認証機構側ＩＤ１は、認証システムの経営者、銀行、金融機関などである。

【００１５】

図２を参照し、また図１から続いて、本考案の可変なバーコードを身分認証に用いるシステムの実施方法のステップについて、下記の通り説明する。

【００１６】

（１）登録者２０による初期登録の実行ステップ２１

登録者２０は（ユーザ）、自分のスマートフオン１１で身分認証を行えるＡＰＰ２２１をインストールし、インストールの完了後に、初期登録を行う。登録が行われる時、認証機構側ＩＤ１のサーバー装置１３は、スマートフオン１１から伝送してきた電話番号と起動コードに基づいて、スマートフオン１１が認証機構側ＩＤ１での登録ステップを完了し、将来的に取引可能な時に、身分認証を実行できる。

前述から続いて、ユーザは身分認証ステップを実行したい時、次のステップへ進む。

【００１７】

（２）身分認証の起動ステップ２２

ユーザは、スマートフオン１１でＡＰＰ２２１をインストール/起動してから、スマートフオン１１のスクリーンに身分認証バーコードＢ１と、可変なバーコード（Ｂ２、Ｂ２‘）とを生成する。前述の身分認証バーコードＢ１と可変なバーコード（Ｂ２、Ｂ２‘）の生成には、ネットワークの接続は必要ない。バーコードは、携帯電話自体のＡＰＰでタイミングモードに基づいて生成されるもので、認証機構への返送で生成することではない。従って、オフラインでインターネット接続しない場合、バーコードの生成には全然影響を与えないので、ユーザにとって利便性がよい。

【００１８】

（３）データの取り込みステップ２３

ユーザは売り手側Ｃ１（例えば、店舗）に前述のスマートフオン１１のバーコードを提示し、そして売り手側Ｃ１は既存のリニアＣＣＤまたはＣＭＯＳバーコード読取り装置１２によってバーコード（身分認証バーコードＢ１と可変なバーコードＢ２）の読取りのステップ２３１を行う。また、読取り作業の完了後に、通信ネットワークＮ１を介して身分認証バーコードＢ１と可変なバーコードＢ２を認証機構側ＩＤ１へ送信する。

【００１９】

（４）身分認証の実行ステップ２４

前のステップから続いて、認証機構側ＩＤ１のサーバー装置１３は、売り手側Ｃ１から伝送されてきた身分認証バーコードＢ１と可変なバーコードＢ２を受信して、バーコードの照合ステップ２４１を行う。先に、第１の対応バーコードデータＳ１を利用して身分認証バーコードＢ１との照合を実行する。両方が一致した場合、スマートフオン１１のＡＰＰと同じ方式に基づき、所定の時間より前（前の時間）、所定の時間と同じ（即ちスマートフオン１１と同じ時間）、所定の時間より後（即ち、以後の時間）の時間で変化する３つの対応可変なバーコードデータを生成することにより、第２の対応バーコードデータＳ２が形成される。

【００２０】

そして、サーバー装置１３は、受信した可変なバーコードＢ２を第２の対応バーコードデータＳ２との照合を実行するにより、可変なバーコードＢ２は第２の対応バーコードデータＳ２が含有する３つの対応可変なバーコードデータのいずれかと一致するか否かを確認する。可変なバーコードＢ２が３つのいずれかと一致した場合、「一致」と判断して、身分認証結果２４２を生成する。もし、両者の照合した結果が全て一致した場合、身分認証の結果は「成功」と認定され、両者の照合のいずれかが一致しなかった場合、身分認証の結果は「失敗」と認定される。

【００２１】

前述のように、身分認証結果２４２を生成してから、サーバー装置１３はその身分認証結果２４２を売り手側Ｃ１のリニアＣＣＤまたはＣＭＯＳバーコード読み取り装置１２へ返送するにより、売り手側Ｃ１はこのユーザが元の登録者であるか否かを確認する。

【００２２】

認証機構側ＩＤ１は、本来的に、スマートフオン１１の所定の時間と同じ時間で変化する同じ可変なバーコードＢ２を生成する。前の時間での対応可変なバーコードを生成する理由として、通信ネットワークＮ１の遅延を避けるためである。後の時間での対応可変なバーコードを生成する理由として、スマートフオン１１と認証機構側ＩＤ１との時間差を避けるためである。

【００２３】

図３を参照し、スマートフオン１１の表示画面１１２を示す。図２の身分認証の起動ステップ２２から続いて、ＡＰＰを実行すると、身分認証バーコードＢ１と可変なバーコードＢ２両方を同時に画面１１２に表示する。また、図３に示すように、可変なバーコードＢ２が一定の時間内に変化する。本図には、画面１１２に秒読み区１１３を設けてあり、その秒読み区１１３の時間は身分認証バーコードＢ１と可変なバーコードＢ２両方の表示後、秒読みを開始する。時間の範囲は、例えば６０秒を設定してもよいが、これに限定されない。

【００２４】

同時に図４を参照して、一定（所定）の時間（例えば６０秒）が経つと、可変なバーコードＢ２が変化するにより、新たな可変なバーコードＢ２‘を生成し、且つ秒読み区１１３での秒読みも再度開始する。このように、可変なバーコードＢ２は照合ステップを完了するとまたは秒読みを終わると自動的に消える。認証機構側ＩＤ１のサーバー装置１３で生成した可変なバーコードＢ２は、認証時に一致するか否かにも係わらず、自動的に消える。

【００２５】

同じ時間で同じユーザに対して、認証時に一致するか否かにも係わらず、認証の実行は一回しか許されない。従って、たとえスキミングされても横領させないようになっている。可変なバーコードＢ２の変化方式は、特別なアルゴリズムを利用して、ランダムな変化を生成するものであり、一定なルールで推測することができない。

【００２６】

前述から分かるように、本考案の可変なバーコードを身分認証に用いるシステムは、ユーザ側に二つのバーコードを生成且つ表示するＡＰＰをインストールしてあるスマートフオンと、売り手側に設けてあるリニアＣＣＤまたはＣＭＯＳバーコード読取装置と、認証機構側のサーバー装置とを構成してなる可変なバーコードを身分認証に用いるシステムである。このシステムにおいて、ＡＰＰが生成してある第１のバーコードデータは、唯一な身分データとしての身分認証バーコードであり、第２のバーコードデータは、身分データに対応し且つ一定の時間後に変化する可変なバーコードである。認証機構側のサーバー装置も同じ時間で同じ可変なバーコードを生成する。

【００２７】

実施の時、ユーザは、先にスマートフオンにＡＰＰをダウンロードし且つインストールすると共に、会員となるように、認証機構側のサーバー装置に登録する。ユーザは、売り手側で取引を行うために使用者の身分を認証する時、ユーザがＡＰＰを起動して、ネットワークとの接続なしに、スマートフオンに２種類のバーコードを表示する。売り手側は、既存のリニアＣＣＤまたはＣＭＯＳバーコード読取装置によって、その２種類のバーコードを読取ると共に、その２種類のバーコードを認証機構側のサーバー装置へ伝送して身分認証を行う。

【００２８】

サーバー装置は、スマートフオンと同じ身分登録データ及び可変なバーコードの生成方法を格納してあるので、身分認証を行う時に、一致性を照合することで、身分認証を行える。身分認証を実行するには、サーバー装置は、身分認証バーコードとペアする第１の対応バーコードデータを格納してあり、サーバー装置は身分認証バーコードを受信してから、同時に所定の時間の前、中、後に変化した３つの第２の対応可変なバーコードデータを生成する。そして、サーバー装置は、受信した可変なバーコードを第２の対応可変なバーコードデータとの照合を実行するにより、可変なバーコードは第２の対応バーコードデータが含有する３つの対応可変なバーコードデータのいずれかと一致するか否かを確認する。それらが一致した場合、ユーザが元の登録者と認定され、さらに認証「成功」という情報をすぐに売り手側へ返送する。これにより、身分認証を完了する。

【００２９】

以上から分かるように、バーコードがハッカーによって盗まれた場合でも、横領することができない。これは、また一つのアルゴリズムを要するから、可変なバーコードを正しく取得できる。更に、本考案のもう一つの特徴として、顧客は使用の時、ネットワークの接続を必要としないことである。バーコードは、携帯電話自体のＡＰＰでタイミングモードに基づいて生成されるもので、認証機構への返送で生成することではない。

【００３０】

従って、ユーザにとって利便性は非常によい。このように、本考案は、前述の通りにより実行すれば、売り手側が既存のバーコードデータ読取装置を利用して、同時にスマートフオンと認証機器側サーバーにより、ハードウエアデバイスの追加購入が必要なしに、身分認証を実行できる。しかも、利便性がよく、安全性の高い、可変なバーコードを身分認証に用いるシステムを提供することが確実に実現できる。

【００３１】

但し、当該内容は本考案の好ましい実施態様であり、本考案の実施範囲を限定するではない。当考案の主旨と範囲を逸脱しない範囲内において、この技術分野に精通する者によって行われた変更及び修正は全て当考案の範囲内に覆うべきである。

【産業上の利用可能性】

【００３２】

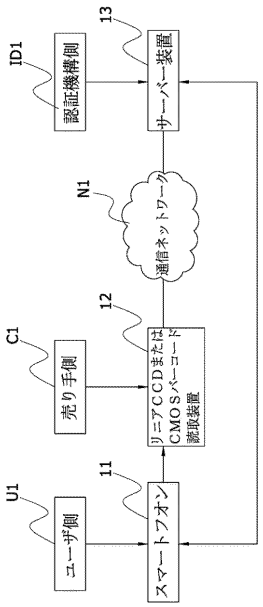
本考案によれば、変更されたバーコードは、認証機構の中にもはや存在しないことにより、解読することができない。そのため、スキミング、解読や偽造のような問題を解決することができる。更に、顧客が使用の場合、ネットワークとの接続の必要はない。バーコードは、携帯電話が携帯自体のＡＰＰでタイミングモードに基づいて生成されるもので、認証機構への返送で生成することではない。したがって、顧客の使用が非常に便利です。

【符号の説明】

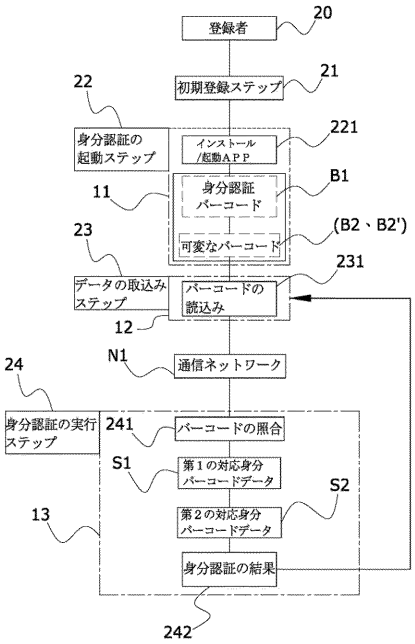
【００３３】

１　：身分認証システム
Ｕ１　：ユーザ側
Ｃ１　：売り手側
１１　：スマートフオン
１２　：リニアＣＣＤまたはＣＭＯＳバーコード読取装置
１１２　：画面
１１３　：秒読み区
１１３‘：秒読み区
ＩＤ１　：認証機構側
１３　：サーバー装置
Ｎ１　：通信ネットワーク
２０　：登録者
２１　：初期登録ステップ
２２　：身分認証の起動ステップ
２２１　：インストール/起動ＡＰＰ
２３　：データの取込みステップ
２３１　：バーコードの読込み
２４　：身分認証の実行ステップ
２４１　：バーコードの照合
２４２　：身分認証の結果
Ｂ１　：身分認証バーコード
Ｂ１‘　：身分認証バーコード
Ｂ２　：可変なバーコード
Ｂ２‘　：可変なバーコード
Ｓ１　：第１の対応身分バーコードデータ
Ｓ２　：第２の対応身分バーコードデータ

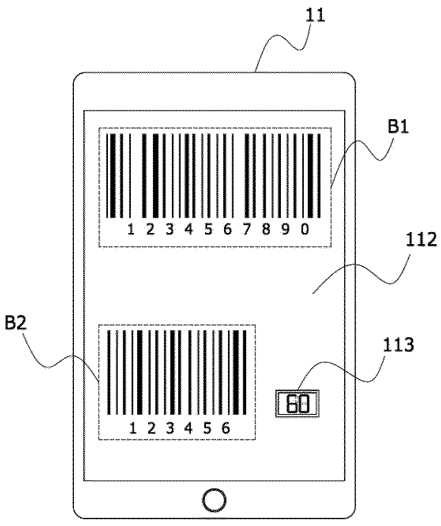
【図１】


ID1
認証機構側
13
サーバー装置
N1
通信ネットワーク
12
C1
売り手側
リニアCCDまたは
CMOSバーコード
読取装置
11
U1
ユーザ側
スマートフォン

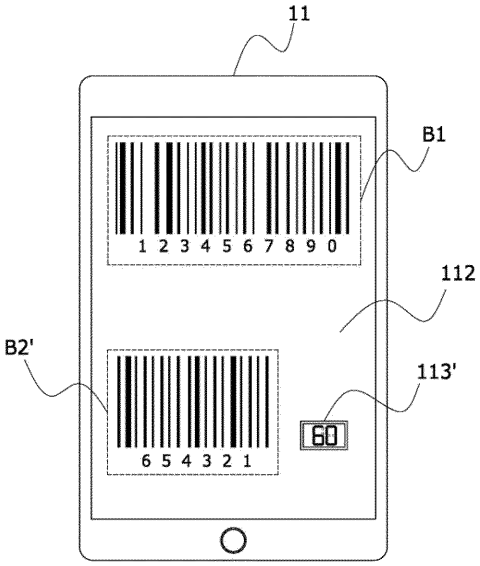
【図２】


登録者
20
初期登録ステップ
21
22
身分認証の
起動ステップ
インストール
/起動ＡＰＰ
221
身分認証
バーコード
B1
11
可変なバーコード
(B2、B2')
23
データの取込み
ステップ
バーコードの
読込み
231
12
N1
通信ネットワーク
24
身分認証の実行
ステップ
241
バーコードの照合
S1
第１の対応身分
バーコードデータ
S2
第２の対応身分
バーコードデータ
13
身分認証の結果
242

【図３】


11
B1
1 2 3 4 5 6 7 8 9 0
112
B2
113
1 2 3 4 5 6
60

【図４】


11
B1
1 2 3 4 5 6 7 8 9 0
112
B2'
113'
6 5 4 3 2 1
60

フロントページの続き

(72)考案者　リュウ，　ケニス
台湾　ニュー　タイペイ　シティ，　シイン　ティエン　ディストリクト，　ミン　チュアン　ロード，　１０８－３番，　９階