(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号

特表2009-537893

(P2009-537893A)

(43)公表日　平成21年10月29日(2009.10.29)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330B	5B276
G06F 15/00	(2006.01)	G06F	15/00	ZEC	5B285
G06F 21/22	(2006.01)	G06F	15/00	330C	5J104
H04L 9/32	(2006.01)	G06F	9/06	660E	
		H04L	9/00	673A	

審査請求 未請求　予備審査請求 有　（全 13 頁）

(21)出願番号　特願2009-510910 (P2009-510910)
(86)(22)出願日　平成19年5月17日 (2007.5.17)
(85)翻訳文提出日　平成20年11月18日 (2008.11.18)
(86)国際出願番号　PCT/NZ2007/000115
(87)国際公開番号　WO2007/136277
(87)国際公開日　平成19年11月29日 (2007.11.29)
(31)優先権主張番号　547322
(32)優先日　平成18年5月18日 (2006.5.18)
(33)優先権主張国　ニュージーランド(NZ)

(71)出願人　508342149
フロンデ　エニウェア　リミテッド
ニュージーランド国、ウェリントン、クィーンズ　ワーフ　３
(74)代理人　100065385
弁理士　山下　穣平
(72)発明者　パルフィーネ・ホライツ・ニコライ
ニュージーランド国、ウェリントン、チュートン　パーク、キャンブリアン　ストリート　５
(72)発明者　ウィリアムズ・アントニー・ジョン
ニュージーランド国、ウェリントン、ワデスタウン、ピット　ストリート　８０

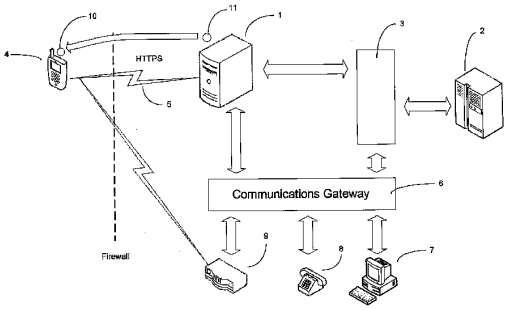
Fターム(参考)　5B276 FB05

最終頁に続く

(54)【発明の名称】無線トランザクションの認証方法

(57)【要約】

モバイル装置とリモートコンピュータのユーザとにトークンを関連付け、モバイル装置とリモートコンピュータとでトークンが一致することを確かめ、接続中にモバイル装置とリモートコンピュータとでトークンを更新する認証方法。好ましくはパスワード認証が第２の要素となる、２要素認証方法を使用される。



【特許請求の範囲】
【請求項１】
無線通信リンクを通じてモバイル装置とリモートコンピュータとの間でトランザクションの認証を提供する方法であって、
（ｉ） 以下の（ａ）、（ｂ）を含む第１の認証方法を行うこと、
（ａ） 前記モバイル装置に格納されたトークンが当該装置に関連付けられたトークンに一致することを前記リモートコンピュータで検証する
（ｂ） 前記既存トークンに置き換えるために、新規トークンをアクティブセッション中に前記リモートコンピュータから前記モバイル装置へ送信し、前記リモートコンピュータで前記新規トークンを前記モバイル装置に関連付ける
（ii） 前記トランザクションの処理に先立ち第２の認証方法を実行すること、を備える方法。
【請求項２】
前記第２の認証方法は前記トークンの認証とは別に実行される、請求項１に記載の方法。
【請求項３】
前記第２の認証方法は前記トークンが認証された後に実行される、請求項１に記載の方法。
【請求項４】
前記第２の認証方法は前記トークンが認証される前に実行される、請求項１に記載の方法。
【請求項５】
前記第２の認証方法の認証データは、前記モバイル装置から前記リモートコンピュータシステムへ独立したデータストリームで送信される、請求項１に記載の方法。
【請求項６】
前記第２の認証方法は安全な接続を介して行われる、請求項２～５のいずれか一項に記載の方法。
【請求項７】
前記安全な接続はｈｔｔｐｓプロトコルを使用する、請求項５に記載の方法。
【請求項８】
前記第２の認証方法は、前記モバイル装置から前記リモートコンピュータへパスワードを送信する、請求項１～７のいずれか一項に記載の方法。
【請求項９】
前記トークンは無線通信接続を確立する間に認証される、請求項１～８のいずれか一項に記載の方法。
【請求項１０】
前記パスワードは前記リモートコンピュータで認証される、請求項９に記載の方法。
【請求項１１】
前記パスワードは、前記リモートコンピュータシステムへリンクされた顧客コンピュータシステムによって認証される、請求項７に記載の方法。
【請求項１２】
前記顧客コンピュータシステムは銀行業務コンピュータシステムである、請求項９に記載の方法。
【請求項１３】
前記リモートコンピュータへ送信される前記トークンが別のセッションで使われていないことを確認するためチェックが行われる、請求項１～１２のいずれか一項に記載の方法。
【請求項１４】
前記チェックは認証中に行われる、請求項１３に記載の方法。
【請求項１５】

前記チェックは認証済みのセッション中に行われる、請求項１４に記載の方法。
【請求項１６】
前記リモートコンピュータによる前記トークンの認証を管理する前記モバイル装置へアプリケーションがダウンロードされる、請求項１～１５のいずれか一項に記載の方法。
【請求項１７】
前記トークンは前記アプリケーション内に格納される、請求項１６に記載の方法。
【請求項１８】
前記アプリケーションは難読化されたコードをに含まれ、前記トークンは前記難読化されたコード内に格納される、請求項１７に記載の方法。
【請求項１９】
前記アプリケーションは仮想マシンとして実行する、請求項１６～１８のいずれか一項に記載の方法。
【請求項２０】
前記アプリケーションはＪ２ＭＥで記述される、請求項１６～１９のいずれか一項に記載の方法。
【請求項２１】
前記アプリケーションは無線リンクを通じてダウンロードされる、請求項１６～２０のいずれか一項に記載の方法。
【請求項２２】
前記リモート装置へＵＲＬリンクがＷＡＰメッセージ内で送信され、前記アプリケーションは前記ＵＲＬリンクの起動時にダウンロードされる、請求項２１に記載の方法。
【請求項２３】
前記ＷＡＰメッセージは、インターネットバンキングセッションの間にユーザからのリクエストに応じて送信される、請求項２２に記載の方法。
【請求項２４】
前記ＷＡＰメッセージは、ユーザからのＳＭＳメッセージに応じて送信される、請求項２２に記載の方法。
【請求項２５】
前記ＵＲＬリンクは、前記モバイル装置に関連する固有のＵＲＬアドレスである、請求項２２～２４のいずれか一項に記載の方法。
【請求項２６】
前記モバイル装置へダウンロードされる前記アプリケーションにはユーザ固有シグネチャが挿入される、請求項１６～２４のいずれか一項に記載の方法。
【請求項２７】
前記ユーザ固有シグネチャはＪＡＲファイルに格納される、請求項２６に記載の方法。
【請求項２８】
前記ダウンロードされるアプリケーションは、前記アプリケーションをダウンロードするために使用する前記ＵＲＬを前記モバイル装置のメモリに格納する、請求項１６～２７のいずれか一項に記載の方法。
【請求項２９】
前記アプリケーションは、前記アプリケーションをダウンロードするために使用する前記ＵＲＬをチェックするため前記モバイル装置の前記メモリをチェックし、存在しないか前記アプリケーションに関連するＵＲＬと異なる場合には、前記アプリケーションは実行すべき起動コードの入力を要求する、請求項２８に記載の方法。
【請求項３０】
前記起動コードは、前記モバイル装置のユーザへ提供されるコードである、請求項２９に記載の方法。
【請求項３１】
前記起動コードと前記アプリケーションに格納された前記ユーザ固有シグネチャは、ユーザによる起動コードの入力があり次第、検証のため前記リモートコンピュータへ送信さ

れる、請求項２９に記載の方法。
【請求項３２】
前記モバイル装置に対して前記起動コードとユーザ固有シグネチャの有効性が立証される場合は前記モバイル装置へトークンが送信される、請求項３１に記載の方法。
【請求項３３】
前記方法は、オンラインバンキングトランザクションの実行を可能にするため実行される、請求項１～３２のいずれか一項に記載の方法。
【請求項３４】
前記オンラインバンキングトランザクションは、請求書支払いと、資金振替と、トランザクション履歴の入手と、口座残高の閲覧とからなるグループから選ばれる、請求項３３に記載の方法。
【請求項３５】
請求項１～３４のいずれか一項に記載の方法に従いモバイル装置側の認証を実行するモバイル装置のためのソフトウェア。
【請求項３６】
請求項３５に記載のソフトウェアを含むモバイル装置。
【請求項３７】
請求項１～３６のいずれか一項に記載の方法に従いリモートコンピュータ側の認証を実行するリモートコンピュータのためのソフトウェア。
【請求項３８】
請求項３７に記載のソフトウェアを含むリモートコンピュータ。
【請求項３９】
請求項１～３４のいずれか一項に記載の方法を実行するように構成されたモバイル商取引システム。
【請求項４０】
ユーザ識別情報に関連付けられたセキュリティトークンを格納するメモリを含むコンピュータと、
モバイルネットワークから前記コンピュータへ認証情報を伝達する通信ゲートウェイとを備え、
前記コンピュータは、モバイル装置とのセッション中にユーザに関連付けられたトークンを検証し、新規トークンを生成し、これをメモリに格納し、前記通信ゲートウェイを通じてこれを前記モバイル装置へ転送し、且つ受信した前記トークンと前記モバイル装置から受信した第２の認証コードとに基づきトランザクションを認証するように適合されている、
モバイル商取引システム。
【請求項４１】
認証トークンを格納し、セッションを開始するときに無線リンクを介して前記トークンを送信し、且つ前記トークンを前記セッション中に受信される新規トークンに置き換えるよう構成されたモバイル無線通信装置。
【請求項４２】
請求項１～３４のいずれか一項に記載の方法を実行するよう構成されたモバイル無線通信装置。
【請求項４３】
無線通信サービスと通信するコンピュータプラットフォームであって、前記コンピュータプラットフォームは、複数のユーザと関連付けられた複数のトークンを格納し、セッションを開始する間に受信するトークンが当該ユーザに関連付けられたトークンに一致するか否かを検証し、セッション中に新規トークンを生成し、これを各ユーザに関連付け、且つ前記ユーザのモバイル装置へこれを転送するよう構成される、
コンピュータプラットフォーム。
【請求項４４】

請求項１～３４のいずれか一項に記載の方法を実行するよう構成されたコンピュータプラットフォーム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は無線トランザクションに用いる認証方法に関わり、特に、限定的にではないが、セルラー通信ネットワークにおける商業トランザクションに、関する。この方法は好ましくは、ユーザパスワードと認証トークンとを利用する２要素認証方法に用いられる。

【背景技術】

【０００２】

モバイルバンキング等の商業トランザクションや機密トランザクションとに関連してモバイルサービスの需要が拡大している。インターネットバンキング等のサービスでは一般的に１要素認証（すなわちパスワード）だけですまされるが、無線通信リスクに対する認識の高まりから、セルラー通信ネットワーク経由のモバイルバンキングには、より一層のセキュリティが望ましいと考えられている。

【０００３】

２通りの認証方法（例えばユーザパスワードとセキュリティトークンまたはセキュリティキーとの組み合わせ）を要求する２要素認証はより強固な保護を提供する。無線トランザクションに用いるセキュリティトークンを生成し配布する方法はいくつか公知であり、特許文献１、特許文献２、特許文献３で説明されている。

【０００４】

これらの方法では使用が１回きりのシングルユーストークン（トランザクションを行うたびに申請しなければならない）か永続トークンを使用する。トランザクションのたびにトークンを請求しなければならない点でシングルユーストークンは不便である。永続トークンは、いつでも有効に使用できる一方、トークンを第三者が入手した場合にセキュリティ上のリスクを生じさせる。

【特許文献１】国際公開第２００２／１９５９３号パンフレット（ＷＯ０２／１９５９３）

【特許文献２】国際公開第２００１／１７３１０号パンフレット（ＷＯ０１／１７３１０）

【特許文献３】国際公開第２００３／０６３４１１号パンフレット（ＷＯ０３／０６３４１１）

【発明の開示】

【発明が解決しようとする課題】

【０００５】

ユーザ入力を最小限に抑えながら強固なセキュリティを提供する認証方法の提供が望ましい。ユーザの関与を最小限に抑えながら一連の経路を通じて稼動できる認証プロセスが望ましい。また、このプロセスを様々なモバイル装置で使用できると望ましい。認証プロセスはまた、スプーフィング、フィッシング、傍受、ソフトウェアの逆コンパイル、ソフトウェアの取り替え、データまたはソフトウェアの不正操作、ならびにセキュリティトークンへのアクセスに対し良好な保護を提供するべきである。ユーザによるトランザクションの拒否も最小限に抑えるべきである。

【課題を解決するための手段】

【０００６】

本明細書ではいくつかの実施形態を説明するが、以下の実施形態は制限されない代表的実施形態として読むべきものである。

【０００７】

一代表的実施形態によると、無線通信リンクを通じてモバイル装置とリモートコンピュータとの間でトランザクションの認証を提供する方法が提供され、この方法は、

（ｉ）　以下の（ａ）、（ｂ）を含む第１の認証方法を行うこと、

（ａ） 前記モバイル装置に格納されたトークンが当該装置に関連付けられたトークンに一致することを前記リモートコンピュータで検証する
（ｂ） 前記既存トークンに置き換えるために、新規トークンをアクティブセッション中に前記リモートコンピュータから前記モバイル装置へ送信し、前記リモートコンピュータで前記新規トークンを前記モバイル装置に関連付ける
（ii） 前記トランザクションの処理に先立ち第２の認証方法を実行すること、を備える。

【０００８】
この方法を実装するソフトウェアと、このソフトウェアを実行するモバイル装置及びリモートコンピュータも提供される。

【０００９】
もうひとつの実施形態によるとモバイル商取引システムが提供され、このシステムは、
ユーザ識別情報に関連付けられたセキュリティトークンを格納するメモリを含むコンピュータと、
モバイルネットワークから前記コンピュータへ認証情報を伝達する通信ゲートウェイとを備え、
前記コンピュータは、モバイル装置とのセッション中にユーザに関連付けられたトークンを検証し、新規トークンを生成し、これをメモリに格納し、前記通信ゲートウェイを通じてこれを前記モバイル装置へ転送し、且つ受信した前記トークンと前記モバイル装置から受信した第２の認証コードとに基づきトランザクションを認証するように適合されている。

【００１０】
さらに、このシステムで使用するモバイル装置とコンピュータが提供される。

【００１１】
本明細書に組み込まれこれの一部をなす添付の図面は本発明の実施形態を図示するものであり、上に記された本発明の概説と下に記された実施形態の詳しい説明と併せて本発明の原理を説明するのに役立つ。

【発明を実施するための最良の形態】

【００１２】
図１は、本発明の認証方法を実行する１つの可能なシステムを概略的に示すものである。この認証方法は、リモートコンピュータでトークンをモバイル装置とユーザとに関連付けることと、モバイル装置とリモートコンピュータとでトークンが一致することを確立することと、接続中にモバイル装置とリモートコンピュータとでトークンを更新することとを含む。好ましくは２要素認証方法を使用する。好ましい実施形態においては従来のパスワード認証が第２の要素となる。

【００１３】
図１を参照しながら一例としてモバイルバンキングを説明する。リモートコンピュータ１はインターネットバンキングビジネス層３（これはクライアントコンピュータシステム２内にあるソフトウェア層であったり、中間コンピュータでホストされるソフトウェアであったりする）を通じてクライアントコンピュータシステム２（この場合は基幹バンキングシステム）へ接続する。リモートコンピュータ１は無線リンク５を通じてモバイル装置４と通信できる（このリンクは通常ならばモバイル通信提供業者を経由する）。

【００１４】
リモートコンピュータ１とビジネス層３は通信ゲートウェイ６へ接続し、この通信ゲートウェイ６は、インターネットバンキングと、テレフォンバンキングと、ＳＭＳ通信とを提供するためリモートコンピュータ７と、電話８と、ＳＭＳサーバ９との通信を助ける。

【００１５】
ユーザはモバイルバンキングを行うため以下に記すいくつかのチャネルのひとつを通じてサービスをリクエストできる。

【００１６】

１．　銀行にて－　ユーザは自身の銀行の支店を訪れ、自身の身元を認証し、着脱可能メディア、データ回線等によって自身のモバイル無線装置４へアプリケーションを無線でダウンロードする。

【００１７】

２．　ＳＭＳ－　ユーザはモバイルバンキングをリクエストするＳＭＳメッセージを送信し、銀行は信用証明を確認し、確認がとれる場合はモバイルバンキングアプリケーションをクライアントへ送信するようリモートコンピュータ１に指示する。

【００１８】

３．　電話－　ユーザは銀行に電話をかけてモバイルバンキングをリクエストする。ユーザ信用証明の確認がとれると、リモートコンピュータ１はモバイルバンキングアプリケーションをクライアントへ送信するよう指示される。

【００１９】

４．　インターネットバンキング－　ユーザはインターネットバンキングセッション中にモバイルバンキングサービスをリクエストする。インターネットバンキングへのログオンのときにユーザ信用証明の確認がとれると、モバイルバンキングアプリケーションは自動的にユーザへ送信される。

【００２０】

モバイルバンキングサービスを申請する方法は様々で、上記が例にすぎないことは理解されよう。

【００２１】

モバイルバンキングアプリケーションは様々な方法で引き渡すことができる。これはリモートコンピュータ１からモバイル無線装置４へ直接的に引き渡すことができる。ただし好ましい一方法ではＵＲＬを組み込んでＷＡＰメッセージをモバイル装置４へ送信することによってアプリケーションのダウンロードを可能にする。このＵＲＬをユーザに固有のものにすればセキュリティは増す。ユーザは安全なｈｔｔｐｓ接続を確立し、ＵＲＬからアプリケーションをダウンロードできる。モバイルバンキングアプリケーションを安全に引き渡すにあたって様々な方法を使用できることは理解されよう。

【００２２】

モバイルバンキングアプリケーションを引き渡し、起動し、使用する方法にはいくつかある。以下２つの実施形態を説明する。

【００２３】

第１の実施形態によると、モバイルバンキングアプリケーションの引き渡しにあたってはモバイルバンキングアプリケーションにセキュリティトークン１０を組み込む。同じセキュリティトークン１１がリモートコンピュータ１に格納され、ユーザＩＤ（ユーザ名、電話番号、その他）と関連付けられる。ユーザが無線モバイル装置４を使ってモバイルバンキングサービスへのアクセスを試みるときには、モバイルバンキングアプリケーションがリモートコンピュータ１との接続を確立する。リモートコンピュータ１は、この接続を確立する間に、リモートコンピュータ１でユーザＩＤに関連付けられたトークン１１にトークン１０が一致するか否かを確かめる。このプロセスは水面下で行われ、ユーザ入力は要求されない。リモートコンピュータ１は好ましくは、同じトークンを使って別の接続が確立されていないことをもチェックする。このチェックは接続を確立する間に、及び／またはセッション中に、行うことができる。トークンはユーザの電話番号に関連付けるのが好ましく、こうすればトークンは特定の装置に関連付けられる。トークンは接続を確立する間に確認されることのが好ましいが、接続が確立した後にトークンが確認されてもよいことは理解されよう。

【００２４】

トークン１０の有効性が立証されると、リモートコンピュータ１はユーザＩＤに関連付けられた新しいトークンを生成し、新しいトークンはリモートコンピュータ１にて、モバイル装置４へ送信され、前のトークンに置き換わる。このようにトークンは１回のセッションだけで使われ、トークンが傍受されてもその後に接続を確立することはできない。

【００２５】
モバイル無線装置４へ提供されるモバイルバンキングアプリケーションは、高度なセキュリティを提供することが好ましい。これを達成する機能には次のものがある。
【００２６】
１．　難読化されたコード（つまり、圧縮され理解できないコード）
２．　仮想マシン（つまり、各アプリケーションは他のコンポーネントとやり取りせずに独自のスペースで実行する）
３．　検査済みコード（つまり、マシンクラスを無効にできないことを確認するためにチェック）
これらの機能を達成するため、アプリケーションはＪａｖａ（登録商標）　Ｊ２ＭＥコードで記述するのが好ましい。
【００２７】
トークンは、アクセスや操作が困難なものであるべきである。トークンは、アクセスや操作が困難となる形でモバイルバンキングアプリケーションに埋め込むのが好ましい。好ましくは、無線モバイル装置４に格納されるモバイルバンキングアプリケーション内でバイトコードとしてトークンを格納する。
【００２８】
好ましくは、第２の認証方法を上述した認証トークン方法と組み合わせて使用する。好ましい第２の認証方法はユーザパスワードの提出である。これは既存のインターネットバンキングセキュリティに整合するため、最小限の調整ですむ。上記の方法に従い安全なｈｔｔｐｓ接続が確立すると、無線モバイル装置４で実行するモバイルアプリケーションがユーザパスワードの入力を要求する。ユーザがパスワードを入力すると、無線リンク５を通じてリモートコンピュータ１に伝達される。パスワードはリモートコンピュータ１で検証してもよく、認証のためクライアントコンピュータシステム４に伝達してもよい。
【００２９】
インターネットバンキングアプリケーションの場合、銀行は一般的にクライアントコンピュータシステム４によるパスワード認証の実行を好む。これ以外のアプリケーションでは当分野で公知の一連の認証方法から第２の認証方法を選ぶことができる。この２要素認証方法には、トークンとパスワードが別々の時間に送信され（つまりトークンは接続を確立する間に送信され、パスワードは安全なセッション中に送信される）、且つ別々のデータストリームで送信されるという利点がある。これはトークンとパスワードの両方の傍受を困難なものにする。
【００３０】
第２の実施形態によると、サービスのリクエストに応じてアプリケーションをダウンロードさせるためユーザ固有ＵＲＬをユーザに送信する。そのユーザのアプリケーションにはユーザ固有シグネチャを挿入する。好ましい一実施形態において、このユーザ固有シグネチャはＪＡＲファイルに含まれる。
【００３１】
そしてユーザはユーザ固有シグネチャを含むアプリケーションをユーザ固有ＵＲＬからダウンロードし、自身のモバイル装置でアプリケーションを実行する。アプリケーションはまず、ユーザ固有ＵＲＬに一致するＵＲＬがモバイル装置のメモリに格納されているか否かをチェックする。アプリケーションは、ＵＲＬが存在しないかＵＲＬが異なる場合に、起動の実行を要求する。このようにアプリケーションは、インストールされたアプリケーションのインスタンスが正しいか否かを実行のたびにチェックする。
【００３２】
これは悪質なアプリケーションへの取り替えを防ぎ、アプリケーションの新バージョンがダウンロードされる場合に起動を要求する。
【００３３】
ＵＲＬが一致する場合は、予め安全な経路を通じて支給された起動コードの提供をユーザに求める。入力された起動コードとユーザ固有シグネチャはリモートコンピュータへ送

信され、リモートコンピュータに格納されたユーザの値にそれらが一致する場合はリモートコンピュータがリクエストを検証し、リモートモバイル装置へトークンを送信する。トークンは好ましくは、難読化されたバイトコードとしてモバイル装置に格納されたアプリケーション内に格納されるが、どこかよそに格納することもできる。

【００３４】

使用にあたってはユーザがパスワードを入力し、そのパスワードと、ユーザ固有シグネチャと、トークンは認証のためリモートコンピュータへ送信される。認証されると、新しいトークンがモバイル装置へ送信されて古いトークンに取って代わり、１回のトランザクションセッションを行うことができる（構成に依存する）。

【００３５】

認証検査に合格するとユーザは請求書の支払い、資金振替、トランザクション履歴の入手、口座残高の閲覧といったインターネットバンキングトランザクションを行うことができる。ただし別なアプリケーションにおいては様々な商業トランザクションやその他のトランザクションを行えることは理解されよう。

【００３６】

したがって、電話機に暗号機能を用意する必要のない様々な既存無線モバイル装置に供給できる方法及びシステムが提供される。この方法は大々的な修正やシステムコンポーネントの追加をともなわずに既存のシステムに容易に適用でき、方法の実施にあたって費用効果を上げることができる。方法は容易に実施でき、顧客はこれを容易に利用できる。トークンから提供される追加的セキュリティはユーザに気づかれない。ユーザ固有シグネチャをアプリケーションに含めることによって第３の認証要素が提供され、ユーザ固有ダウンロードＵＲＬの使用と格納によってアプリケーションは装置に結び付けられる。２つの要素が別々に処理されることによってデータの傍受やセキュリティの妨害は困難となるため、この方法は高度なセキュリティを提供する。さらにソフトウェアは、ソフトウェアやデータのアクセスまたは変更を極めて困難なものにする。特定のモバイル装置とトークンとの結合関係によって別の装置を使った第三者によるアクセスの試みは規制され、ユーザによるトランザクションのできるだけの拒否は制限される。これまで本発明の方法及びシステムをモバイルバンキングアプリケーションとの関係で説明してきたが、これ以外の幅広いアプリケーションに本発明の方法を適用できることは理解されよう。

【００３７】

これまで本発明をその実施形態の説明によって例証し、実施形態を詳しく説明してきたが、添付の請求項の範囲をかかる記述に制限したり何らかの形で限定する意図はない。追加の利点と修正は当業者にとって明白であろう。したがって本発明はその幅広い態様において、図示し説明した具体的詳細と、代表的装置及び方法と、説明のための例とに限定されない。よって、出願者の発明概念の精神または範囲から逸脱することなく、かかる記述から逸脱することはありえる。

【図面の簡単な説明】

【００３８】

【図１】本発明の認証方法を実装するのに適したモバイル商取引システムの概略図を示す。

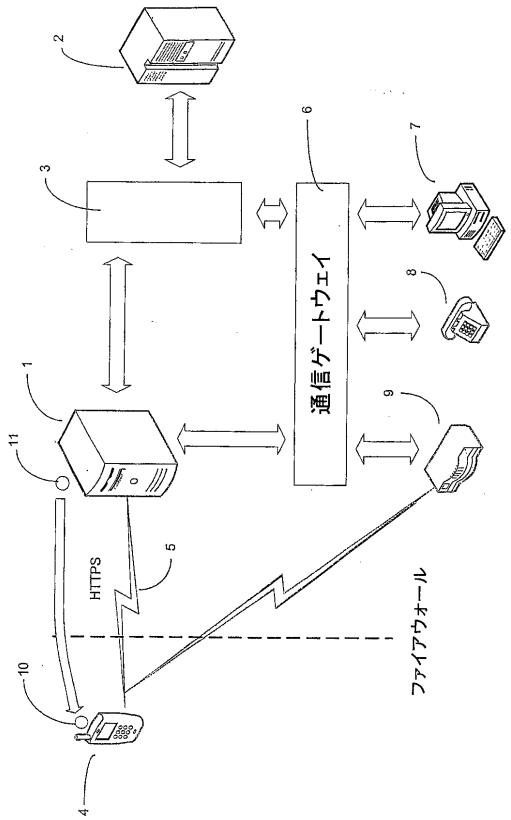
【符号の説明】

【００３９】

１　リモートコンピュータ
２　クライアントコンピュータシステム
３　インターネットバンキングビジネス層
４　モバイル装置
５　無線リンク
６　通信ゲートウェイ
７　リモートコンピュータ
８　電話

９　ＳＭＳサーバ

【図１】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NZ2007/000115

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/32 (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT: authenticate, token, verify, update, two-factor and similar terms.
USPTO: two-factor, authenticate, token, replace and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2002/019593 A2 (TELEFONAKTIEBOLAGET LM ERICSSON (publ)) 7 March 2002 Page 5 line 22-Page 9 line 28	1-44
A	US 2005/0150945 A1 (CHOI) 14 July 2005 Page 1 Para 0006-Page 4 Para 0041	1-44
A	WO 2001/017310 A1 (TELEFONAKTIEBOLAGET LM ERICSSON (publ)) 8 March 2001 Page 4 line 15-Page 5 line 8	1-44

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 August 2007	20 AUG 2007
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **JUZER KHANBHAI** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 2176

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/NZ2007/000115

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	2002/019593	AU	82795/01	EP	1314278		
US	2005/0150945	CA	2489951	EP	1544819	KR	2005006203
WO	2001/017310	AU	70471/00	CN	1385051	EP	1208715
		MX	PA02002018	ZA	200201005		

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

Ｆターム(参考) 5B285 AA01 BA03 CB45 CB52 CB55 CB56 CB62 CB72 CB95 DA03
DA05 DA10
5J104 AA07 AA16 EA03 EA08 EA16 KA01 KA11 KA21 NA05 NA36
NA38 PA01