(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6742907号
(P6742907)
(45)発行日　令和2年8月19日(2020.8.19)　(24)登録日　令和2年7月31日(2020.7.31)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 673B
G06F 21/33 (2013.01)　H04L 9/00 673A
G06F 21/33

請求項の数 17　(全 22 頁)

(21)出願番号　特願2016-547039(P2016-547039)
(86)(22)出願日　平成27年1月14日(2015.1.14)
(65)公表番号　特表2017-507562(P2017-507562A)
(43)公表日　平成29年3月16日(2017.3.16)
(86)国際出願番号　PCT/EP2015/050601
(87)国際公開番号　WO2015/107085
(87)国際公開日　平成27年7月23日(2015.7.23)
審査請求日　平成30年1月12日(2018.1.12)
(31)優先権主張番号　14/155,257
(32)優先日　平成26年1月14日(2014.1.14)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　516211547
ピアーウィッツ、ビョルン
ＰＩＲＲＷＩＴＺ，　Ｂｊｏｅｒｎ
ブルガリア国、１４６３　ソフィア、ビトシャ・ブールバード　１２８
Ｖｉｔｏｓｈａ　Ｂｏｕｌｅｖａｒｄ　１２８，　１４６３　Ｓｏｆｉａ，　Ｂｕｌｇａｒｉａ

最終頁に続く

(54)【発明の名称】識別および／または認証のシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
パーソナル電子デバイスを有するユーザが、受け手側システムにおける所望の業務または処理のために、ネットワークを介して、前記受け手側システムに登録および／またはログインすることを可能にするための認証システムであって、前記認証システムは、
前記パーソナル電子デバイスと前記受け手側システムの両方と前記ネットワークを介して通信する認証サーバと、ここにおいて、前記認証サーバは、前記ユーザのパーソナル電子デバイスを識別し、前記ユーザに固有に割り当てられるトークンＩＤを設定することによって前記ユーザのためのアカウントを設定するよう適応され、前記ユーザのパーソナル電子デバイスに、前記受け手側システムにおける認証を続けるか否かの前記ユーザの決定のための認証要求を送るよう適応される、
アクセス可能なメモリの上に前記ユーザの個人情報を記憶するように、引き続いて、前記個人情報を読み出すように、および、前記認証要求を受け取ることに応答して前記ユーザによって認可された場合、前記認証要求に応答して前記認証サーバに前記個人情報を送ることなく、前記受け手側システムに前記個人情報を送るように、前記パーソナル電子デバイスの上に保持されるソフトウェアアプリケーションによって構成される前記パーソナル電子デバイスと、ここにおいて、前記個人情報は、前記ユーザが、前記受け手側システムにおける前記所望の業務または処理を行うために、前記受け手側システムによって要求され、名前、住所、クレジットカード番号、電話番号、ｅｍａｉｌアドレスの少なくとも１つを含み、

前記ユーザに、前記所望の業務または処理のための前記トークンＩＤを求め、前記ユーザの前記トークンＩＤを参照して前記認証サーバと通信し、前記個人情報によって前記ユーザを識別または認証するために、前記パーソナル電子デバイスから前記個人情報を受け取るように、前記受け手側システム上に保持されたソフトウェアアプリケーションによって構成される前記受け手側システムと、
を備え、
前記ユーザによる前記業務または処理の要求に応答して、前記受け手側システムは、更に、ユーザに、彼の固有のトークンＩＤを求めるように、および、前記認証サーバに前記トークンＩＤを送るように構成され、
前記認証サーバは、前記ユーザの前記パーソナル電子デバイスが、前記受け手側システムにおける認証を続けるか否かの決定を前記ユーザに求めるように、前記受け手側システムからの前記トークンＩＤの受け取りに応答して、前記ユーザのパーソナル電子デバイスに認証要求を送るよう更に構成され、
前記ユーザによる認可の場合、前記パーソナル電子デバイスは、前記メモリから前記個人情報を読み出すように、および、前記受け手側システムに前記個人情報を送るように構成され、
前記受け手側システムは、前記個人情報によって前記ユーザを識別し、その後、識別された前記ユーザが、前記受け手側システムにおいて前記所望の業務または処理を行うために、識別された前記ユーザを前記受け手側システムに登録およびログインさせるよう更に構成される、認証システム。
【請求項２】
前記個人情報は、少なくとも３つのデータのサブセット、即ち、名のわからないサブセット、個人に関するサブセット、および、経済的なサブセットの間で区別されて前記パーソナル電子デバイスに記憶され、前記名の分からないサブセットは、前記ユーザを識別しない前記個人情報として定義され、前記個人に関するサブセットは、前記ユーザにコンタクトするために前記ユーザを識別する前記個人情報として定義され、前記経済的なサブセットは、経済的な処理をするために必要とされる前記ユーザの前記個人情報として定義され、
前記受け手側システムは、前記受け手側システムへの登録および／またはログインのために必要とされる前記個人情報のサブセットのタイプを前記ユーザに知らせるために、前記ユーザに、彼の固有なトークンＩＤを求めるよう適応される、
請求項１に記載の認証システム。
【請求項３】
前記パーソナル電子デバイスの前記メモリは、前記パーソナル電子デバイスによってアクセス可能な第１のコンピュータ読出し可能な記憶媒体である、請求項１または２のいずれか一項記載の認証システム。
【請求項４】
前記ユーザの前記個人情報は、暗号化され、前記第１のコンピュータ読出し可能な記憶媒体に記憶され、
前記暗号化は前記認証サーバによって生成され、第２のコンピュータ読出し可能な記憶媒体上に記憶された暗号化鍵に基づき、
前記パーソナル電子デバイスは、前記認証サーバから前記暗号化鍵を読出し、前記個人情報を復号化し、前記受け手側システムに、前記ユーザの前記復号化された個人情報を送るよう適応される、
請求項３に記載の認証システム。
【請求項５】
前記認証サーバによって割り当てられる前記トークンＩＤは、前記ユーザのパーソナル電子デバイスの固有の識別子に基づく、請求項１ないし４のいずれか一項記載の認証システム。
【請求項６】

前記認証サーバによって割り当てられる前記トークンＩＤは、前記認証サーバによって設定されるランダムなトークン鍵に基づく、請求項１ないし５のいずれか一項に記載の認証システム。

【請求項７】

前記受け手側システムは、前記ユーザからの処理要求の受け取りに応じて、ランダムコードを生成し、前記ランダムコードを認証サーバに送るように、および、前記ユーザのパーソナル電子デバイスから前記ランダムコードを受け取るように、および、前記生成され、受け取られたランダムコードに基づいて、前記受け手側システムに前記所望の業務または処理を要求するために固有の前記トークンＩＤを送った前記ユーザを認証するように適応され、

前記認証サーバは、前記認証要求と共に、前記受け手側システムから受け取られた前記ランダムコードを、前記ユーザのパーソナル電子デバイスに送るよう適応された、

請求項１ないし６のいずれか一項に記載の認証システム。

【請求項８】

前記メモリに記憶された前記ユーザの前記個人情報は、前記認証サーバに与えられたり、または、記憶されたりしない、請求項１ないし７のいずれか一項に記載の認証システム。

【請求項９】

前記認証サーバは、前記受け手側システムの識別情報を、前記認証要求と共に、前記ユーザの前記パーソナル電子デバイスに送るように、更に構成され、

前記ユーザの前記パーソナル電子デバイスは、前記受け手側システムの受け取られた前記識別情報にしたがって、前記ユーザの前記個人情報を、前記受け手側システムに送るように構成される、

請求項１ないし７のいずれか一項に記載の認証システム。

【請求項１０】

パーソナル電子デバイスを有するユーザが、受け手側システムにおける所望の業務または処理のために、前記受け手側システムに登録および／またはログインすることを可能にするための認証方法であって、

ａ）前記パーソナル電子デバイスと前記受け手側システムとネットワーク上で通信する認証サーバを提供することと、

ｂ）前記ユーザのパーソナル電子デバイスを識別し、前記ユーザに固有に割り当てられるトークンＩＤを設定することによって、前記認証サーバの上に前記ユーザのためのアカウントを設定することと、

ｃ）前記パーソナル電子デバイスのメモリの上に前記ユーザの個人情報を記憶することと、ここにおいて、前記個人情報は、前記ユーザが、前記受け手側システムにおける前記所望の業務または処理を行うために、前記受け手側システムによって要求され、名前、住所、クレジットカード番号、電話番号、ｅｍａｉｌアドレスの少なくとも１つを含み、

ｄ）前記受け手側システムが、前記ユーザに、前記所望の業務または処理のための固有の前記トークンＩＤを求めることと、

ｅ）前記受け手側システムが、前記ユーザのトークンＩＤを受け取ることに応じて、前記ユーザの入力されたトークンＩＤを参照して、前記認証サーバと通信することと、

ｆ）前記ユーザのパーソナル電子デバイスが、前記受け手側システムにおける認証を続けるか否かの決定を前記ユーザに求めるように、前記認証サーバが、前記受け手側システムからの前記トークンＩＤの受け取りに応答して、前記ユーザのパーソナル電子デバイスに認証要求を送ることと、

ｇ）認証を続けるとの決定の場合、前記受け手側システムが、前記個人情報によって前記ユーザを識別または認証するために、前記認証要求に応答して前記認証サーバに前記個人情報を送ることなく、前記個人情報を読み出し、前記受け手側システムに前記個人情報を送るように、前記ユーザが、前記パーソナル電子デバイスを認可することと、

ｈ）前記受け手側システムが、前記個人情報を受け取り、前記個人情報によって前記ユ

ーザを識別し、識別された前記ユーザは、その後、前記受け手側システムにおいて前記所望の業務または処理を行うために、前記受け手側システムに登録され、ログインされることと、
のステップを備える認証方法。
【請求項１１】
ステップｃ）における個人情報は、少なくとも、名のわからないサブセット、個人に関するサブセット、および、経済的なサブセットの間で、前記パーソナル電子デバイスの上で区別され、前記名の分からないサブセットは、前記ユーザを識別しない前記個人情報として定義され、前記個人に関するサブセットは、前記ユーザにコンタクトするために前記ユーザを識別する前記個人情報として定義され、前記経済的なサブセットは、経済的な処理をするために必要とされる前記ユーザの前記個人情報として定義され、
ステップｄ）における受け手側システムは、前記ユーザに、彼の固有なトークンＩＤを求め、登録および／またはログインのために必要とされる前記個人情報のサブセットのタイプを前記ユーザに知らせ、
ステップｆ）、ｇ）、および、ｈ）における前記個人情報は、前記ユーザの個人情報の前記名のわからないサブセット、前記個人に関するサブセット、または、前記経済的なサブセットのいずれかに対応する、
請求項１０に記載の認証方法。
【請求項１２】
ステップｃ）における前記パーソナル電子デバイスの前記メモリは、前記パーソナル電子デバイスによってアクセス可能な第１のコンピュータ読出し可能な記憶媒体である、請求項１０または１１のいずれか一項記載の認証方法。
【請求項１３】
ステップｃ）における前記ユーザの前記個人情報は、暗号化され、前記第１のコンピュータ読出し可能な記憶媒体上に記憶され、
前記暗号化は、前記認証サーバによって生成され、第２のコンピュータ読出し可能な記憶媒体上に記憶された暗号化鍵に基づき、
ステップｈ）において、前記パーソナル電子デバイスは、前記認証サーバから前記暗号化鍵を読出し、前記個人情報を復号化し、前記受け手側システムに前記ユーザの前記復号化された個人情報を送る、
請求項１２に記載の認証方法。
【請求項１４】
ステップｂ）において前記認証サーバによって割り当てられた前記トークンＩＤは、前記ユーザのパーソナル電子デバイスの固有な識別子に基づく、請求項１０ないし１３のいずれか一項記載の認証方法。
【請求項１５】
ステップｂ）において前記認証サーバによって割り当てられた前記トークンＩＤは、前記ユーザのパーソナル電子デバイスの固有な識別子と前記認証サーバによって設定されたランダムトークン鍵とに基づき、
更に、前記ユーザが、任意の時点において、前記ユーザのパーソナル電子デバイスの前記固有な識別子と前記認証サーバの前記ランダムトークン鍵とに基づいて新たなトークンＩＤを生成することができるステップｊ）を含む、
請求項１０ないし１４のいずれか一項に記載の認証方法。
【請求項１６】
前記受け手側システムによって、前記ユーザからの処理要求の受け取りに応じて、ランダムコードを生成し、前記ランダムコードを前記認証サーバに送るステップと、
前記認証サーバによって、前記認証要求と共に、前記受け手側システムから受け取られた前記ランダムコードを、前記ユーザのパーソナル電子デバイスに送るステップと、
前記受け手側システムによって、前記ユーザのパーソナル電子デバイスから前記ランダムコードを受け取り、前記生成され、受け取られたランダムコードに基づいて、前記受け

手側システムに前記所望の業務または処理を要求するために固有の前記トークンＩＤを送った前記ユーザを認証するステップと、
を更に備える、請求項１０ないし１５のいずれか一項に記載の認証方法。
【請求項１７】
少なくとも１つのプロセッサによって実行されたとき、前記少なくとも１つのプロセッサに、請求項１０ないし１６のいずれか一項に記載の方法の前記ステップを備える動作を実行させる命令のセットを記憶する、コンピュータ読出し可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、パーソナル電子デバイスを利用して認証を行うためのシステムと方法に関する。
【背景技術】
【０００２】
ほとんどのｗｅｂｓｉｔｅや購買キオスクは、処理（transaction）を行うためにｗｅｂｓｉｔｅを使用し、アカウント情報を変更する、等のために、ユーザに、登録することやログインすることを要求する。多くのｗｅｂｓｉｔｅは、ビジター、または、彼らの特性を表す統計のいずれかを識別し、従って、それによって、表示されたメッセージを適合させることができるように、ビジターの人物像を描き出すことを試みる。
【０００３】
ユーザを識別する幾つかの方法が知られており、そのような方法は、一般的に、直接的、または、間接的な方法のいずれかにはいる。間接的な方法は、例えば、クッキーを書いたり読んだりすること、インターネットプロトコル（Internet Protocol：ＩＰ）アドレスを探知すること、等を含む。そのような間接的な方法は、比較的に非侵入であるが、直接的な方法よりも正確性が非常に劣る。
【０００４】
ユーザを識別する直接的な方法は、識別と認証という２つのステップを含むユーザの特別な動的認識を必要とする。識別は、本質的に、「あなたは誰ですか？」という質問に答える認識ステップである。例えば、電子商取引サイト等のオンラインシステムをアクセスしたいユーザは、典型的にはｅｍａｉｌアドレス、ユーザＩＤ、メンバーシップ番号、等々のような固有の個人識別子を提示することによって、新たなユーザとして登録するか、または、既存のユーザとしてログインするかのいずれかができなければならない。
【０００５】
認証は、本質的に、「あなたが誰であるかをあなたが言っているのが本当にあなたであることを、あなたがどのように証明することができるか？」という質問に答える検証ステップである。典型的に、ｗｅｂｓｉｔｅは、ユーザとｗｅｂｓｉｔｅとによって表面上でのみ知られている、パスワード、ＰＩＮコード、等々を要求する。進歩した認証方法は、指紋、虹彩の特徴、等々のような生体認証データを利用する。
【０００６】
そのようなシステムは、伝統的に、秘密として保たれており、類推することが困難な認証情報に依存している。多くの権限は、ユーザについて知られている情報から導き出される可能性がより低いように、ユーザへの直接の参照を何ら持たないパスワードを要求する。更に、ユーザは、しばしば、複数のｗｅｂｓｉｔｅ上で同じパスワードを用いないように伝えられる。しかし、そのような要求は実施するのが難しく、従って、生来無頓着な多くの人は、複数のサイト上で類推が容易な同じパスワードを用い、全てのそのようなサイト上で彼らの情報をより安全が低い状態にする。
【０００７】
そのような典型的な識別と認証システムに対する問題点のいくつかは、以下を含む：
１）この中では「受け手側システム（recipient system）」と言われる、例えば電子商取引ｗｅｂｓｉｔｅ等のそのようなｗｅｂｓｉｔｅ（ユーザにとってのターゲットｗｅｂ

ｓｉｔｅ）は、適切な安全手段でもってユーザの個人情報を保護しなければならない。そのような情報の格納庫は、しばしば、名前、アドレス、クレジットカード番号、等々のような個人情報の大きなセットを不正に獲得する目的でのハッキング攻撃のターゲットである。

【０００８】

２）ユーザは、好ましくは、彼がアクセスを希望する各サイト毎に固有のパスワードを常に有して、任意のそのような受け手側システムのためのパスワードを生成し、慎重に保管し、定期的に更新しなければならない。

【０００９】

３）ユーザは、そのようなｗｅｂｓｉｔｅや受け手側システムにおいて初期登録するために、ｗｅｂｓｉｔｅにおいて彼の所望の業務を行うのに十分な彼の個人情報を送らなければならない。例えば、アイテムを購入し、彼の家の住所にそれを配達させることを望む電子商取引のユーザは、名前、住所、電話番号、ｅｍａｉｌアドレス、クレジットカード情報、等々のような彼の属性情報の全てを通信しなければならない。そのようなデータは、サイト毎に再入力されなければならず、時間を浪費し、タイプエラーをしがちである。

【００１０】

４）ユーザの住所またはｅｍａｉｌアドレス等の彼の情報が変更する場合、ユーザは、彼が将来の業務を行うことを望むｗｅｂｓｉｔｅ毎に、そのような情報を更新しなければならない。これは時間の浪費であり、しばしば、ユーザは、彼の送付先住所等、特定のｗｅｂｓｉｔｅ上で情報を更新してあるかどうかを覚えていない。これは、ユーザの配送が誤って旧住所に届けられる結果となり得る。

【００１１】

５）多くのユーザの個人情報を保管している受け手側システムは、しばしば、彼らのユーザの多くについての彼らの情報が現在用いられていないという課題を有し、大量のメーリングまたはｅｍａｉｌキャンペーンをより非効率で効果の少ないものにする。

【００１２】

これらの問題点のいくつかに対する１つの部分的な解決策は、所謂「シングルサインオン（single sign-on）」方法であり、例えば、Ｆａｃｅｂｏｏｋ（登録商標）、Ｌｉｎｋｅｄ－Ｉｎ、Ｔｗｉｔｔｅｒ、等々のようなソシアルネットワークプラットホームである第１のシステムにおける固有のユーザアカウントに基づく。そのようなシングルサインオンシステムにおいて、例えば、ある種の業務を処理するための受け手側システムにログインするために、ユーザは、まず、受け手側システムを介してその第１のシステム（principal system）にログインしなければならない。ユーザが第１のシステムによって識別され、認証されると、第１のシステムは、あるデータを、受け手側システムと共有し、受け手側システムは、ユーザとのユーザセッションを設定する。

【００１３】

しかし、そのようなシングルサインオンシステムは、また、以下のような、ある不利な点を有する。

【００１４】

１）第１のシステムは、ユーザの個人情報を知らされなければならず、ユーザは、そのような第１のシステムが当該個人情報を持つことを望まないかもしれない。

【００１５】

２）第１のシステムは、ユーザが訪問し、業務を処理する受け手側システムの全てについて学習する。

【００１６】

３）受け手側システムは、第１のシステムとの信用関係を持たなければならない。

【００１７】

４）ユーザは、ユーザの個人データの正しい共有が起こっていると、第１のシステムと受け手側システムとの両方を信用しなければならない。

【００１８】

５）典型的にはソシアルネットワークプラットホームである第１のシステムは、ユーザの友人や知人も同様にしばしば訪れる受け手側システムについて学習し、第１のシステムのユーザの全ての間での追加のプライバシーと信用の問題を提起する。

【００１９】

６）どの受け手側システムもユーザが第１のシステムを介してアクセスするので、受け手側システム上のユーザのログインＩＤやパスワードはより大きな価値があるようになり、従って、より魅力的なハッキングターゲットになり、高められたセキュリティを必要とし、そのようなログイン資格が危うくされた場合に大きなリスクを生む。

【００２０】

従って、受け手側サイトにおいてユーザ情報を安全に保つ負担を軽減し、それによって、そのような受け手側システムに対するそれらのオーバヘッドコストを低減するシステムへの要求がある。

【発明の概要】

【００２１】

従って、上記不利な点に基づき、本発明の目的は、個別の認証情報を要求することのない信頼のおける認証が、それぞれの受け手側システムのためにユーザによって与えられることを可能にするシステムを提供することである。

【００２２】

これは、独立の請求項の特徴によって達成される。

【００２３】

本発明の更なる特別に利益のある実施形態が、従属の請求項の特徴によって提供される。

【００２４】

本発明は、ユーザが使用することを望む各受け手側システムについて１つずつ、複数の固有で複雑なパスワードを覚えておかなければならないユーザの負担を軽減し得る。それは、更に、サイト毎においてユーザの個人情報を入力するというユーザにとっての必要性を取り除き、また、彼が使用するサイトの全てを通して彼の情報を更新することが合理化される。更に、そのようなことは、任意の所与の受け手側システムについてより最新である各ユーザの個人情報の結果をもたらし得る。

【００２５】

認証システムが、パーソナル電子デバイスを有するユーザが、ネットワークを介して、受け手側システムに登録および／またはログインすることを可能にするために提供され、

この認証システムは、　パーソナル電子デバイスと受け手側システムの両方と、ネットワークを介して通信する認証サーバであって、ユーザのパーソナル電子デバイスを一意に識別し、ユーザにトークンＩＤを割り当てることによって、ユーザのためのアカウントを設定するよう適応され、ユーザのパーソナル電子デバイスに、受け手側システムにおける認証を続けるか否かのユーザの決定のための認証要求を送るよう適応される認証サーバと；　それにアクセス可能なメモリの上にユーザの個人情報を記憶するように、および、引き続いて、認証要求を受け取ることに応答してユーザによって認可された場合、個人情報を読出し、受け手側システムに個人情報を送るように、パーソナル電子デバイスの上に保持されるソフトウェアアプリケーションによって構成されるパーソナル電子デバイスと；

ユーザにトークンＩＤを求め、トークンＩＤを認証サーバに通信し、それによってユーザを識別するためにパーソナル電子デバイスから直接に個人情報を受け取るように、受け手側システム上に保持されたソフトウェアアプリケーションによって構成される受け手側システムと；　を備え、　ユーザによる処理要求に応答して、受け手側システムは、更に、ユーザに、彼の固有のトークンＩＤを求めるように、および、認証サーバにトークンＩＤを送るように構成され、　認証サーバは、受け手側システムにおける認証を続けるか否かの決定をユーザに求めるように更に構成されたユーザのパーソナル電子デバイスへの認証要求を送るよう更に構成され、その後、ユーザによる認可の場合、パーソナル電子デバイスは、メモリから個人情報を読み出すよう、および、それによってユーザを識別するた

めに受け手側システムに個人情報を送るよう構成され、　受け手側システムは、その後、ユーザを受け手側システムに登録およびログインさせるようさらに構成される。

【００２６】

更に、認証方法が、パーソナル電子デバイスを有したユーザが、受け手側システムに登録および／またはログインすることを可能にするために提供され、　この認証方法は、ａ）パーソナル電子デバイスと受け手側システムとネットワーク上で通信する認証サーバを提供することと；　ｂ）認証サーバにおいて、ユーザのパーソナル電子デバイスを一意に識別し、ユーザにトークンＩＤを割り当てることによって、認証サーバの上にユーザのためのアカウントを設定することと；　ｃ）パーソナル電子デバイスのメモリの上にユーザの個人情報を記憶することと；　ｄ）受け手側システムは、ユーザに、彼の固有のトークンＩＤを求め；　ｅ）受け手側システムが、ユーザのトークンＩＤを受け取ることに応じて、認証サーバと、ユーザの入力されたトークンＩＤを通信することと；　ｆ）認証サーバが、受け手側システムにおける認証を続けるか否かの決定をユーザに求める、ユーザのパーソナル電子デバイスへの認証要求を送ることと；　ｇ）ユーザが、認証を続けるとの決定の場合、パーソナル電子デバイスを、受け手側システムに個人情報を送るよう認可することと；　ｈ）パーソナル電子デバイスが、個人情報を読出し、受け手側システムに個人情報を送ることと；　ｉ）受け手側システムが、個人情報を受け取り、それによってユーザを識別し、ユーザが、その後、受け手側システムに登録され、ログインされることと、　のステップを備える。

【００２７】

コンピュータ読出し可能な記憶媒体は、少なくとも１つのプロセッサによって実行されたとき、少なくとも１つのプロセッサに、上述のステップを備える動作を実行させる命令のセットを記憶する。コンピュータ読出し可能な記憶媒体は、また、分散され得、即ち、受け手側システム、ユーザのＰＥＤ、並びに、認証サーバにおけるストレージを含むことが注記される。

【００２８】

本発明の上記および他の目的は、添付の図面に関連して与えられる以下の記載と好適な実施形態からより明瞭になる。

【図面の簡単な説明】

【００２９】

【図１】図１は、インターネットを介して等で全てが相互にネットワーク化される、ユーザと彼のパーソナル電子デバイス（personal electronic device：ＰＥＤ）、受け手側システム、認証サーバを示すネットワーク図である。

【図２】図２は、ユーザのＰＥＤ上で実行している携帯アプリケーションの例示のインターフェース画面である。

【図３】図３は、ユーザの固有のトークンＩＤをユーザに求める受け手側システムの例示のインターフェース画面である。

【図４】図３のインターフェース画面においてトークンＩＤを提示することに応答して認証サーバからＰＥＤによって受け取られた任意の認証要求を示す携帯アプリケーションの例示のインターフェース画面である。

【図５】図５は、受け手側システムの認証要求に応答してアクションをすることをユーザに求める携帯アプリケーションの例示のインターフェース画面である。

【図６】図６は、受け手側システムがユーザの認証を待っていることを示す受け手側システムの例示のインターフェース画面である。

【図７】図７は、ユーザが認可され、受け手側システムにログインされていることを示す受け手側システムの例示のインターフェース画面である。

【図８】図８は、認証要求の履歴を示す携帯アプリケーションの例示のインターフェース画面である。

【図９】図９は、ユーザの個人情報の名のわからないサブセットを示す携帯アプリケーションの例示のインターフェース画面である。

【図１０】図１０は、ユーザの個人情報の個人に関するサブセットを示す携帯アプリケーションの例示のインターフェース画面である。
【図１１】図１１は、ユーザの個人情報の経済的なサブセットを示す携帯アプリケーションの例示のインターフェース画面である。
【図１２】図１２は、ユーザのＰＥＤの固有のＰＥＤ　ＩＤを示す携帯アプリケーションの例示のインターフェース画面である。
【詳細な説明】
【００３０】
本発明の例示の実施形態が以下に説明される。以下の説明は、これらの実施形態の十分な理解と、これらの実施形態について実施可能にする説明とのための特定の具体例を与える。この技術分野に技量を有する者は、本発明がそのような具体例無しでも実施され得ることを理解する。他の場合には、周知の構成や機能は、実施形態の説明を不必要に分かりにくくすることを避けるために、詳細には示されず、説明されていない。
【００３１】
文脈が明確にその他のことを要求しない限り、本説明や特許請求の範囲を通して、「備える（comprise）」、「備えている（comprising）」、等々の用語は、排他的（exclusive）または網羅的（exhaustive）とは反対に、多くを含む意味（inclusive sense）で、即ち、「含むが、限定ではない（including, but not limited to）」の意味で解釈されるべきである。また、単数または複数の数を用いる語は、それぞれ、複数または単数を含む。追加的に、「この中（herein）」、「上（above）」、「以下（below）」、および、類似の意味の用語は、この出願の中で用いられるとき、この出願の特定の部分ではなく、この出願を全体として参照しなければならない。特許請求の範囲が、２つまたはそれより多くのアイテムのリストを参照して「または（or）」の用語を用いる場合、その用語は、用語の以下の解釈の全てを包含する：当該リストにおけるアイテムのいずれか、当該リストにおけるアイテムの全て、当該リストにおけるアイテムの任意の組み合わせ。「各々（each）」の用語が、数において少なくとも１つであるとして以前に持ち出された要素（element）を参照して用いられた場合、「各々（each）」の用語は、必ずしも複数の当該要素という意味を含まず、単数の要素を意味し得る。
【００３２】
図１は、携帯電話、ラップトップ、タブレットコンピュータ、等々のようなパーソナル電子デバイス３０を有するユーザ２０が、キオスク、ＡＴＭ、遠隔ワークステーション、コンピュータ、等のいずれかの他のデバイスを利用する、または、同じパーソナル電子デバイス３０上さえの、電子商取引ｗｅｂｓｉｔｅ等の受け手側システム４０に登録および／またはログインすることを可能にするためのコンピュータで実行される認証方法１０によって用いられるネットワーク構成を示す。この方法は、以下に詳細に説明される次のステップを備える。
【００３３】
第１に、パーソナル電子デバイス３０（personal electronic device：ＰＥＤ３０）と受け手側システム４０とネットワーク１５を介して通信できる、認証サーバ５０が提供される。
そのような認証サーバ５０は、例えば、ユーザ２０のＰＥＤ３０と受け手側システム４０と共に、インターネットに接続され得る（図１）。例えば、ユーザ２０は、電子商取引キオスク４０からギフトカードを購入しようと試みていてよい。
【００３４】
認証方法１０を用いることができる前に、ユーザ２０は、認証サーバ５０上にアカウントを設定し、ＰＥＤ３０の第１の非一時的なコンピュータ読出し可能な記憶媒体１６０上またはその他の場所等のＰＥＤ３０上のみであるが、認証サーバ５０上ではないところに記憶されるユーザ２０の個人情報６０を与えなければならない。認証サーバ５０は、例えば、固有のＰＥＤ　ＩＤ８０（図１２）を介して、または、ＰＥＤのある機能を介して等で、ユーザのパーソナル電子デバイス５０を一意に識別する。認証サーバ５０は、例えば

、ＰＥＤ３０上で実行する携帯アプリケーション３５を介してＰＥＤ３０と通信し、そのような携帯アプリケーション３５は、認証サーバ５０またはその他の場所からユーザ２０によってＰＥＤ３０にダウンロードされている。携帯アプリケーション３５は、好ましくは暗号化された接続を介して、固有なＰＥＤ　ＩＤ８０を認証サーバ５０に通信する。代替的に、ＰＥＤ３０は、ＳＭＳテキストメッセージ、チャットアプリケーション、ｅｍａｉｌ、等々を介して認証サーバ５０と通信し得る。ユーザ２０の個人情報６０は、好ましくは第１の非一時的なコンピュータ読出し可能な記憶媒体上で、ＰＥＤ３０上またはＰＥＤ３０によって記憶され、ＰＥＤ３０によってのみアクセス可能である。携帯アプリケーション３５は、好ましくは、ユーザアカウントを設定するために、認証サーバ５０と協働し、それによって、ユーザ２０が認証サーバ５０と直接協働する必要はない。

【００３５】

一実施形態において、個人データ６０は、個人データが暗号化された個人情報１４０になるように、暗号化鍵１３０で暗号化される。そして、暗号化鍵が、認証サーバ５０によって、好ましくは第２の非一時的なコンピュータ読出し可能な記憶媒体１７０上に記憶された状態で、暗号化された個人情報１４０は、ＰＥＤ３０または非一時的なコンピュータ読出し可能な記憶媒体１６０のいずれか上に記憶される。

【００３６】

認証方法１０は、好ましくは、覚えるのが楽で、タイプするのが簡単な、ユーザ２０のための固有のトークンＩＤを設定する。トークンＩＤ７０は、好ましくは、認証サーバ５０によって設定され、携帯アプリケーション３５によってＰＥＤ３０上に記憶される。トークンＩＤ７０は、固有なＰＥＤ　ＩＤ８０に基づいてもよく、または、代替的に、固有のＰＥＤ　ＩＤ８０と認証サーバ５０によって生成されるランダムトークン鍵１５０との組み合わせでもよく、例えば、彼のトークンＩＤ７０が不正で用いられていると彼が信じている場合、ユーザ２０は、好きなように、トークンＩＤ７０をリセットし得る。

【００３７】

受け手側システム４０との協働で、ユーザ２０は、彼のトークンＩＤ７０を求められる（図３）。ユーザ２０が彼のトークンＩＤ７０を思い出せない場合、例示として「スマートークン（Smartoken）」と呼ばれるトークンＩＤ７０（図２）を表示する、彼のＰＥＤ３０上の携帯アプリケーションを起動し得る。また、例えば、ユーザのＰＥＤ３０を無くしたり、盗まれたりした場合の不正の機会を減らすために、本技術において知られているように、携帯アプリケーション３５は、パスワード保護されるか、または、生体認証技術で保護され得る。

【００３８】

受け手側システム４０は、ユーザのトークンＩＤ７０を受け取ることに応じて、ユーザのトークンＩＤ７０を参照して、ＰＥＤ３０からのログインまたは登録情報を要求するために、認証サーバ５０と通信する（図６）。ソフトウェアアプリケーションまたはモジュールは、方法１０を実行するための受け手側システムのプロセッサに命令を与えるために、受け手側システム４０に保持されている。

【００３９】

認証サーバ５０は、受け手側システム４０から情報要求を受け取ることに応じて、ユーザのＰＥＤ３０に認証要求８５を送り、認証要求８５は、ユーザ２０に、受け手側システム４０における認証を続けるか否かの決定を求め、続ける場合であれば、好ましくは、ＰＥＤ３０が受け手側システム４０に提示することを認可されるユーザの個人情報６０のサブセット９０を選択するようにする。認証サーバ５０は、ＰＥＤ３０に、受け手側システム４０のＩＰアドレスやポート等のような受け手側システム４０の位置または識別情報を送り、結果、ＰＥＤ３０は、受け手側システム４０へのユーザの個人情報６０のサブセット９０をどのように、どこに送るかを知る。

【００４０】

処理を先に進めることにつて気が変わった場合、または、例えば、悪意のある第三者が受け手側システム４０上でユーザのＩＤ７０を不正に使っている場合、等、ユーザ２０が

認証を進めないと決定する場合、ユーザは、受け手側システム４０に個人情報６０を送ることを拒否する。受け手側システム４０は、結果、個人情報６０を待つことを止め、セッションをキャンセルし、デフォルトの待機ホーム画面等に戻る。

【００４１】

ユーザ２０は、認証を進めることを決定する場合、受け手側システム４０に送るべきユーザの個人情報のサブセット９０を選択し、ＰＥＤ３０に先に進むよう命令する（図５）。ＰＥＤ３０は、第１の非一時的なコンピュータ読出し可能な記憶媒体１６０から個人情報６０のサブセット９０を読出し、個人情報６０のサブセット９０を、好適には暗号化接続を介して、受け手側システム４０に送る。一実施形態において、ユーザの個人情報６０は、名のわからないサブセット（anonymous subset）１００（図９）、個人に関するサブセット（personal subset）１１０（図１０）、および、経済的なサブセット（economic subset）１２０（図１１）等のいくつかの異なるデータセットに分離される。従って、ユーザ２０は、認証サーバ５０によって求められた場合、受け手側システム４０にどの個人情報を送るべきかを決定し得る（図５、図９ないし１１）。名のわからないサブセット１００は、例えば、ユーザ２０の特定をしない情報を含み得る。個人情報１１０は、彼の名前、住所、電話番号、ｅｍａｉｌアドレス、ソシアルメディアＩＤ、等々のような、ユーザ２０の設定となる識別する個人情報６０を含み得る。経済的なサブセット１２０は、財務上の処理をするために有用な、名前、請求先アドレス、クレジットカード番号、有効期限日、ＣＳＶコード、等のクレジットカード情報、等々のようなユーザ２０の経済的な個人情報６０を含み得る。

【００４２】

受け手側システム４０は、個人情報６０のサブセット９０を受け取り。それによってユーザ２０を識別および／または認証し、ユーザのセッションを設定する。ユーザ２０は、続いて、受け手側システム４０に登録され、ログインされる（図７）。ユーザ２０が処理を行った後、非動作の所定の時間の後、または、ユーザ２０の受け手側システム４０からの明白なログオフの後、セッションは終了し、ユーザ２０は、受け手側システム４０に再ログインするために、上述の処理を繰り返す必要がある。

【００４３】

本発明の実施形態に従って、認証サーバ５０は、認証鍵情報を記憶するが、ユーザに関連したデータを記憶しない。例えば、認証サーバは、個人情報を復号化するためのユーザのトークンＩＤ、および／または、鍵を記憶するが、ユーザの個人情報６０を記憶しない。ユーザの個人情報６０は、ＰＥＤ３０の中、例えば、ＰＥＤ３０の中に含まれたコンピュータ読出し可能な媒体の中に、または、メモリカード、Ｂｌｕｅｔｏｏｔｈ（登録商標）またはニアフィールド通信、または、任意の他の手段を介してＰＥＤ３０に接続可能な、メモリカードまたはデバイス等のＰＥＤ３０によって読み出され得る外部のコンピュータ読出し可能な媒体の中に記憶されるのみである。鍵とデータ情報の区別は、ユーザの制御下で個人情報をＰＥＤ３０上にのみ保持することによって個人情報をより良く保護するという利点を与える。

【００４４】

利点のあることには、ユーザによって用いられるデバイスは、ランダムコード（例えば、各使用の後に変更されるワンタイムランダムコード）でもって追加的に識別される。従って、受け手側システム４０は、ランダムコードを生成するように構成される。この構成は、例えばプラグインによって実装され得る。

【００４５】

ユーザが、受け手側システム４０にログインし、彼自身のユーザトークンＩＤ７０を入力したい場合、プラグインは、固有のランダムコード（random code：ＲＣ）を生成し、ユーザのトークンＩＤ７０の代わりに、または、追加して、このコードを認証サーバ５０に送る。次に、認証サーバ５０は、生成されたランダムコードＲＣをＰＥＤ３０に転送する。

【００４６】

ＲＣの正しいＰＥＤへの転送は、例えば、受け手側システム４０から認証サーバ５０に、ユーザのトークンＩＤ７０とＲＣとの両方を送ることによって安全にされ得、結果、認証サーバは、対応するトークンＩＤに関連付けられて、ＲＣをＰＥＤに転送する。

【００４７】

そして、ＰＥＤは、データを送るようにユーザによって命令された場合、ＰＥＤは、ＲＣと共に受け手側システム４０にデータを送る。そして、受け手側システム４０によって生成されたランダムコードを、他の誰も他のどんな状況でも知ることができなかったであろうから、受け手側システムは、ＲＣを送ったデバイスが、ユーザのトークンＩＤ７０でログインしたのと同じ人物によって所有されていることを確認し得る。

【００４８】

特に、本発明の実施形態に従って、本デバイスは、携帯電話、ラップトップ、タブレットコンピュータ、等々のようなパーソナル電子デバイスを有するユーザが、キオスク、ＡＴＭ、遠隔ワークステーション、コンピュータ、または、同じパーソナル電子デバイス上でさえ、等のいずれかの他の電子デバイスを利用する電子商取引ｗｅｂｓｉｔｅ等の受け手側システムへの登録および／またはログインを可能にするためのコンピュータ実装される認証方法によって用いられるネットワーク構成である。

【００４９】

第１に、認証サーバが、パーソナル電子デバイス（personal electronic device：ＰＥＤ）と受け手側システムと、ネットワークを介して通信することができるように提供される。

そのような認証サーバは、例えば、ユーザのＰＥＤと受け手側システムと共に、インターネットに接続され得る。

【００５０】

認証方法を用いることができる前に、ユーザは、ＰＥＤのメモリの中にユーザの個人情報を記憶し、例えば、固有のＰＥＤ ＩＤまたはそれのある機能を介す等して、ユーザのパーソナル電子デバイスを一意に識別して、認証サーバ上にアカウントを設定しなければならない。認証サーバは、好ましくは、ユーザによって認証サーバまたは他の場所からユーザによってＰＥＤにダウンロードされている携帯アプリケーション等、ＰＥＤ上で実行する携帯アプリケーションを介してＰＥＤと通信する。携帯アプリケーションは、ユーザの個人情報と固有のＰＥＤ ＩＤとを、認証サーバの指示において、好ましくは全てが暗号化接続を介して、受け手側システムに通信する。好ましくは、ユーザは、認証サーバと直接に協働する必要なく、ＰＥＤ上で実行する携帯アプリケーションを介して、認証サーバ上に、彼のアカウントを設定する。

【００５１】

認証方法は、好ましくは、覚えるのが楽で、タイプすることが簡単である、ユーザのための固有のトークンＩＤを設定する。受け手側システムと協働して、ユーザは、彼のトークンＩＤを求められる。受け手側システムは、ユーザのトークンＩＤを受け取ることに応じて、ユーザのトークンＩＤを参照して、ＰＥＤからのログインまたは登録情報を直接に要求するために、認証サーバと通信する。認証サーバは、受け手側システムから情報要求を受け取ることに応じて、ユーザに受け手側システムにおける認証を進めるか否かの決定を求める認証要求をユーザのＰＥＤに送り、認証を進める場合、ＰＥＤがネットワークを介して受け手側システムに提示することを認可されたユーザの個人情報のサブセットを選択するような決定をユーザに求める。ユーザは、認証を進めることを決定する場合、受け手側システムに送るべきユーザの個人情報のサブセットを選択し、ＰＥＤに進めることを命令する。ＰＥＤは、そのメモリから個人情報のサブセットを読出し、好ましくは暗号化された接続を介して、その同じものを受け手側システムに送る。

【００５２】

受け手側システムは、個人情報のサブセットを受け取り、ユーザセッションを設定して、個人情報のサブセットによってユーザを識別または認証のいずれかをする。ユーザは、続いて、受け手側システムに登録され、ログインされる。ユーザが処理を行った後、非動

作の所定期間の後、または、ユーザが明白に受け手側システムのログオフをした後、セッションは終了し、ユーザは、受け手側システムに再ログインするために、上述のプロセスを繰り返さなければならない。

【００５３】

本発明は、受け手側サイトにおけるユーザ情報を安全にする負担を軽減し、それによって、そのような受け手側システムのためのオーバヘッドコストを低減するシステムである。

本発明は、ユーザが使用を望む受け手側システム各々について１つ、複数の、固有な、複雑なパスワードを覚えておかなければならないというユーザの負担を軽減し、更に、ユーザにとってのサイト毎に彼の個人情報を入力する必要性を取り除く。本システムは、ユーザが使用するサイトの全てを通して彼の情報が変更する場合、彼の情報を忘れずに更新しなければならないという必要性を取り除く。更に、本発明は、任意の所与の受け手側システムにとって、各ユーザの個人情報より最新であるとの結果となり、例えば、ネットワーク上の遠隔のデータ記憶位置上の代わりに、ユーザでもって個人情報を保持する。本発明の他の特徴や利点は、発明の本質を例示として示す添付の図面に関連して行われる以下のより詳細な説明から明瞭になる。

【００５４】

更に、本発明の他の態様に従って、プロセッサによって実行されたとき、上述の方法のいずれかを実行する命令を記憶するコンピュータ読出し可能な媒体がある。この媒体は、ネットワーク構成に分散されてもよく、そのパーツが、ＰＥＤにおいて、認証サーバにおいて、および、受け手側デバイスにおいて記憶される。パーソナル電子デバイスをもったユーザがネットワークを介して受け手側システムに登録および／またはログインすることを可能にするための認証サーバは：　ユーザのパーソナル電子デバイスを一意に識別し、ユーザにトークンＩＤを割り当てることによってユーザのためのアカウントを設定するためのアカウント管理手段と、　トークンＩＤを自動的に生成するためのトークン生成手段と、　パーソナル電子デバイスと受け手側システムとの両方とネットワークを介して通信するためであって、受け手側システムから、ランダムコードとともにユーザのトークンＩＤを受け取り、受け手側システムからトークンＩＤとランダムコードを受け取ることに応じて、ランダムコードを含んでユーザのＰＥＤに認証要求を送るよう構成された通信手段と、　を含む。

【００５５】

対応して、受け手側システムは、　ランダムコードを生成するランダムコード生成手段と、　トークンＩＤを与え、トークンＩＤでもってユーザの認証のために認証サーバに要求するようユーザに求めるための通信手段と、　ユーザから受け取られたランダムコードが、同じユーザのために認証サーバに与えられたランダムコードと一致するかどうかをチェックするための認証確認手段と、を含む。

【００５６】

パーソナル電子デバイスは、　暗号化された形態でユーザデータを記憶するストレージと、　上述のように受け手側システムと認証サーバと通信するための通信手段と、　ユーザデータの暗号化と復号化を行う暗号化／復号化手段と　を含み得る。

【００５７】

本発明の実施形態によって提供されるコンピュータ実装された認証方法は、パーソナル電子デバイスを有したユーザが受け手側システムに登録および／またはログインすることを可能にするためであって、　方法は、　ａ）パーソナル電子デバイスと受け手側システムとネットワーク上で通信する認証サーバを提供することと、　ｂ）認証システムにおいてユーザのパーソナル電子デバイスを一意に識別することによって、認証サーバ上にユーザのためのアカウントを設定し、ユーザにトークンＩＤを割り当てることと、　ｃ）パーソナル電子デバイスのメモリ上にユーザの個人情報を記憶することと、　ｄ）受け手側システムが、ユーザに対し、彼のトークンＩＤを求めることと、　ｅ）受け手側システムが、ユーザのトークンＩＤを受け取ったことに応じて、認証サーバと、ユーザの入力された

トークンＩＤを通信することと、　ｆ）認証サーバが、ユーザに受信側システムでの認証を続けるか否かの決定を求める認証要求をユーザのパーソナル電子デバイスに送ることと、　ｇ）認証を続けるとの決定をした場合、ユーザが、パーソナル電子デバイスを、受け手側システムに個人情報を送るよう認可することと、　ｈ）パーソナル電子デバイスが、個人情報を読み出して、受け手側システムに個人情報を送ることと、　ｉ）受け手側システムが、個人情報を受け取って、それによってユーザを識別することであって、ユーザが、引き続いて、受け手側システムに登録され、ログインされることと、　のステップを含む。

【００５８】

認証方法において、ステップｃ）における個人情報は、パーソナル電子デバイス上で、少なくとも名のわからないサブセット、個人に関するサブセット、および、経済的なサブセットの間で区別され、　ステップｄ）における受け手側システムは、ユーザに、彼の固有のトークンＩＤを求め、ユーザに、登録および／またはログインをするために必要とされる個人情報のサブセットのタイプを知らせ、　ステップｆ）、ｇ）、および、（ｉ）における個人情報は、ユーザの個人情報の名のわからないサブセット、個人に関するサブセット、および、経済的なサブセットのいずれかに対応する。ステップｃ）におけるパーソナル電子デバイスのメモリは、パーソナル電子デバイスによってアクセス可能な第１の非一時的なコンピュータ読出し可能な記憶媒体であってよい。ステップｃ）におけるユーザの個人情報は、暗号化され、第１の非一時的なコンピュータ読出し可能な記憶媒体に記憶されてよく、　暗号化は、認証サーバによって生成され、第２の非一時的なコンピュータ読出し可能な記憶媒体上に記憶される暗号化鍵に基づき、　ステップｈ）において、パーソナル電子デバイスは、認証サーバから、暗号化鍵を読出し、個人情報を復号化し、ユーザの復号化された個人情報を受け手側システムに送る。ステップｂ）において認証サーバによって割り当てられたトークンＩＤは、ユーザのパーソナル電子デバイスの固有な識別子、および／または、認証サーバによって設定されたランダムトークンに基づいてもよく、　更に、ユーザが、任意の時点で、ユーザのパーソナル電子デバイスと認証サーバのランダムトークン鍵とに基づいて新たなトークンＩＤを生成することができるステップｊ）を含む。

【００５９】

本発明の一態様に従って、非一時的なコンピュータ読出し可能な記憶媒体は、少なくとも１つのプロセッサによって実行されたとき、少なくとも１つのプロセッサに、　ｂ）認証システムにおいてユーザのパーソナル電子デバイスを一意に識別し、ユーザにトークンＩＤを割り当てることによって、パーソナル電子デバイスと受け手側システムとネットワーク上で通信をしている認証サーバ上に、ユーザのためのアカウントを設定することと、　ｃ）パーソナル電子デバイスにアクセス可能なメモリ上にユーザの個人情報を記憶することと、　ｄ）受け手側システムが、ユーザに、彼の固有のトークンＩＤを求めることと、　ｅ）受け手側システムは、ユーザのトークンＩＤを受け取ることに応じて、認証サーバと、ユーザの入力されたトークンＩＤを通信することと、　ｆ）認証サーバが、ユーザに受け手側システムにおける認証を続けるか否かの決定を求めるユーザのパーソナル電子デバイスへの認証要求を送ることと、　ｇ）パーソナル電子デバイスは、ユーザによってそうすることを認可された場合、受け手側システムに個人情報を送ることと、　ｈ）パーソナル電子デバイスが、個人情報を読出し、受け手側システムに個人情報を送ることと、　ｉ）受け手側システムが、個人情報を受け取り、それによってユーザを識別し、続いて、ユーザが受け手側システムに登録および／またはログインされること、　とをさせる命令のセットを記憶するために提供される。

【００６０】

更に、認証システムが、パーソナル電子デバイスを有したユーザが、認証システムは、受け手側システムに登録し、および／または、ログインすることを可能にするために提供され、システムは、　パーソナル電子デバイスと受け手側システムとの両方とネットワークを介して通信している認証サーバであって、ユーザのパーソナル電子デバイスを一意に

識別し、トークンＩＤをユーザに割り当てることによって、ユーザのためのアカウントを設定するように適応され、受け手側システムにおいて認証を続けるか否かのユーザの決定のためのユーザのパーソナル電子デバイスへの認証要求を送るように適応された認証サーバと、　アクセス可能なメモリ上にユーザの個人情報を記憶するよう適応され、その後、認証要求を受け取ることに応答してユーザによって認可されたとき、受け手側システムに個人情報を送るパーソナル電子デバイス上に保持されるソフトウェアアプリケーションと、　受け手側システム上に保持され、ユーザにトークンＩＤを求めるよう適応され、認証サーバにトークンＩＤを通信し、個人情報によってユーザを識別するためにパーソナル電子デバイスから直接に個人情報を受信するソフトウェアアプリケーションと、　を備え、

それによって、　受け手側システムは、ユーザによる処理要求に応答して、ユーザに、彼の固有なトークンＩＤを求め、トークンＩＤを認証サーバに送り、　認証サーバは、受け手側システムにおいて認証を進めてよいか否かの決定をユーザに求めるユーザのパーソナル電子デバイスへの認証要求を送り、　その後、ユーザにより認可された場合、パーソナル電子デバイスは、メモリから個人情報を読出し、個人情報によってユーザを識別するために受け手側システムに個人情報を送り、　ユーザは、その後、受け手側システムに登録され、ログインされる。

【００６１】

発明の特定の形態が示され、説明されたが、様々な変更が、発明の真意と範囲を逸脱することなくなされ得ることが明らかである。従って、本発明は、添付の特許請求の範囲による場合を除き、本発明が限定されることは意図されない。

【００６２】

本発明のある特徴または態様を説明する場合に用いられる特定の用語は、当該用語が関連付けられる本発明の任意の特定の特質、特徴、または、態様に制限されるように、当該用語がこの中で再定義されていることを暗示するとは考えられるべきでない。一般に、添付の特許請求の範囲の中で用いられる用語は、上記「詳細な説明」の項が明示的に当該用語を定義していない限り。明細書において開示された特定の実施形態に本発明を限定すると解釈されるべきではない。

【００６３】

従って、本発明の実際の範囲は、開示された実施形態だけでなく、本発明を実施または実装することの全ての均等な方法も包含する。

【００６４】

本発明の実施形態の上述の詳細な説明は、上述で開示されたきっちりの形態、または、この開示のなかで述べられた用法の特定の分野に余すところがない、または、限定するとは意図されない。本発明の特定の実施形態および例が例示の目的で上述されるが、様々な均等の変更が、関連する技術分野において技量を有する者が認識するように、本発明の範囲の中で可能である。また、この中で与えられる発明の教示は、必ずしも上述のシステムだけではなく、他のシステムにも適用され得る。上述の様々な実施形態の要件や動作は、更なる実施形態を提供するために組み合され得る。

【００６５】

付随する出願書類の中にリストされる全てのものを含め、併存する上記特許や特許出願、および、他の文献は、参照によってこの中に組み込まれる。発明の態様は、本発明の更なる実施形態を提供するために、上述の様々な文献のシステム、機能、および、コンセプトを利用するように、必要であれば、変更され得る。変更は、上記「詳細な説明」の観点で、本発明になされ得る。上記説明は、本発明のある実施形態を詳述し、意図された最良の形態を記載するが、上記体裁が文脈の中でどのように詳述されたかにかかわらず、本発明は、多くの方法で実施され得る。従って、実装の具体例は、依然としてこの中に開示された発明によって包含されるが、相当に変わり得る。上記したように、本発明のある特徴または態様を説明するときに用いられる特定の用語は、当該用語が関連付けられる本発明の任意の特質、特徴、または、態様に制限されるようにはこの中で再定義されていない。

【００６６】

本発明のある態様が、ある請求項の形で以下に提示されるが、発明者は、任意の数の請求項の形式で本発明の様々な態様を企図する。従って、発明者は、本発明の他と態様のためのそのような追加の請求項の形式をとるために、本出願の後で追加の請求項を加える権利を留保する。

以下に、本願出願当初の特許請求の範囲に記載の発明を付記する。

［Ｃ１］

パーソナル電子デバイスを有するユーザが、ネットワークを介して、受け手側システムに登録および／またはログインすることを可能にするための認証システムであって、前記認証システムは、

前記パーソナル電子デバイスと前記受け手側システムの両方と前記ネットワークを介して通信する認証サーバと、　前記認証サーバは、前記ユーザのパーソナル電子デバイスを一意に識別し、前記ユーザにトークンＩＤを割り当てることによって前記ユーザのためのアカウントを設定するよう適応され、前記ユーザのパーソナル電子デバイスに、前記受け手側システムにおける認証を続けるか否かの前記ユーザの決定のための認証要求を送るよう適応される、

アクセス可能なメモリの上に前記ユーザの個人情報を記憶するように、および、引き続いて、前記認証要求を受け取ることに応答して前記ユーザによって認可された場合、前記個人情報を読出し、前記受け手側システムに前記個人情報を送るように、前記パーソナル電子デバイスの上に保持されるソフトウェアアプリケーションによって構成される前記パーソナル電子デバイスと、

前記ユーザに前記トークンＩＤを求め、前記トークンＩＤを前記認証サーバに通信し、前記個人情報によって前記ユーザを識別するために前記パーソナル電子デバイスから直接に前記個人情報を受け取るように、前記受け手側システム上に保持されたソフトウェアアプリケーションによって構成される前記受け手側システムと、

を備え、

前記ユーザによる処理要求に応答して、前記受け手側システムは、更に、ユーザに、彼の固有のトークンＩＤを求めるように、および、前記認証サーバに前記トークンＩＤを送るように構成され、

前記認証サーバは、前記受け手側システムにおける認証を続けるか否かの決定を前記ユーザに求めるように更に構成された前記ユーザのパーソナル電子デバイスへの認証要求を送るよう更に構成され、

前記ユーザによる認可の場合、前記パーソナル電子デバイスは、前記メモリから前記個人情報を読み出すよう、および、前記個人情報によって前記ユーザを識別するために前記受け手側システムに前記個人情報を送るよう構成され、前記受け手側システムは、その後、前記ユーザを前記受け手側システムに登録およびログインさせるよう更に構成される、認証システム。

［Ｃ２］

前記個人情報は、少なくとも３つのデータのサブセット、即ち、名のわからないサブセット、個人に関するサブセット、および、経済的なサブセットの間で区別されて前記パーソナル電子デバイスに記憶され、

前記受け手側システムは、前記受け手側システムへの登録および／またはログインのために必要とされる前記個人情報のサブセットのタイプをユーザに知らせるために、前記ユーザに、彼の固有なトークンＩＤを求めるよう適応される、

［Ｃ１］に記載の認証システム。

［Ｃ３］

前記パーソナル電子デバイスの前記メモリは、前記パーソナル電子デバイスによってアクセス可能な第１のコンピュータ読出し可能な記憶媒体である、［Ｃ１］または［Ｃ２］のいずれか一項記載の認証システム。

［Ｃ４］

前記ユーザの前記個人情報は、暗号化され、前記第１のコンピュータ読出し可能な記憶

媒体に記憶され、
前記暗号化は前記認証サーバによって生成され、第２のコンピュータ読出し可能な記憶媒体上に記憶された暗号化鍵に基づき、
前記パーソナル電子デバイスは、前記認証サーバから前記暗号化鍵を読出し、前記個人情報を復号化し、前記受け手側システムに、前記ユーザの前記復号化された個人情報を送るよう適応される、
［Ｃ３］に記載の認証システム。
［Ｃ５］
前記認証サーバによって割り当てられる前記トークンＩＤは、前記ユーザのパーソナル電子デバイスの固有の識別子に基づく、［Ｃ１］ないし［Ｃ４］のいずれか一項記載の認証システム。
［Ｃ６］
前記認証サーバによって割り当てられる前記トークンＩＤは、前記認証サーバによって設定されるランダムなトークン鍵に基づく、［Ｃ１］ないし［Ｃ５］のいずれか一項に記載の認証システム。
［Ｃ７］
前記受け手側システムは、前記ユーザからの前記処理要求の受け取りに応じて、ランダムコードを生成し、前記ランダムコードを認証サーバに送るように、および、前記ユーザのパーソナル電子デバイスから前記ランダムコードを受け取るように、および、前記生成され、受け取られたランダムコードに基づいて、前記ユーザを認証するように適応され、
前記認証サーバは、前記認証要求と共に、前記受け手側システムから受け取られた前記ランダムコードを、前記ユーザのパーソナル電子デバイスに送るよう適応された、
［Ｃ１］ないし［Ｃ６］のいずれか一項に記載の認証システム。
［Ｃ８］
パーソナル電子デバイスを有するユーザが、受け手側システムに登録および／またはログインすることを可能にするための認証方法であって、
ａ）前記パーソナル電子デバイスと前記受け手側システムとネットワーク上で通信する認証サーバを提供することと、
ｂ）前記認証サーバにおいて、前記ユーザのパーソナル電子デバイスを一意に識別し、前記ユーザにトークンＩＤを割り当てることによって、前記認証サーバの上に前記ユーザのためのアカウントを設定することと、
ｃ）前記パーソナル電子デバイスのメモリの上に前記ユーザの個人情報を記憶することと、
ｄ）前記受け手側システムが、前記ユーザに、彼の固有のトークンＩＤを求めることと、
ｅ）前記受け手側システムが、前記ユーザのトークンＩＤを受け取ることに応じて、前記認証サーバと、前記ユーザの入力されたトークンＩＤを通信することと、
ｆ）前記認証サーバが、前記受け手側システムにおける認証を続けるか否かの決定を前記ユーザに求める前記ユーザのパーソナル電子デバイスへの認証要求を送ることと、
ｇ）前記ユーザが、認証を続けるとの決定の場合、前記パーソナル電子デバイスを、前記受け手側システムに前記個人情報を送るよう認可することと、
ｈ）前記パーソナル電子デバイスが、前記個人情報を読出し、前記受け手側システムに前記個人情報を送ることと、
ｉ）前記受け手側システムが、前記個人情報を受け取り、前記個人情報によって前記ユーザを識別し、前記ユーザは、その後、前記受け手側システムに登録され、ログインされることと、
のステップを備える認証方法。
［Ｃ９］
ステップｃ）における個人情報は、少なくとも、名のわからないサブセット、個人に関するサブセット、および、経済的なサブセットの間で、前記パーソナル電子デバイスの上

で区別され、
ステップｄ）における受け手側システムは、前記ユーザに、彼の固有なトークンＩＤを求め、登録および／またはログインのために必要とされる前記個人情報のサブセットのタイプを前記ユーザに知らせ、
ステップｆ）、ｇ）、および、ｉ）における前記個人情報は、前記ユーザの個人情報の前記名のわからないサブセット、前記個人に関するサブセット、または、前記経済的なサブセットのいずれかに対応する、
［Ｃ８］に記載の認証方法。
［Ｃ１０］
ステップｃ）における前記パーソナル電子デバイスの前記メモリは、前記パーソナル電子デバイスによってアクセス可能な第１のコンピュータ読出し可能な記憶媒体である、［Ｃ８］または［Ｃ９］のいずれか一項記載の認証方法。
［Ｃ１１］
ステップｃ）における前記ユーザの前記個人情報は、暗号化され、前記第１のコンピュータ読出し可能な記憶媒体上に記憶され、
前記暗号化は、前記認証サーバによって生成され、第２のコンピュータ読出し可能な記憶媒体上に記憶された暗号化鍵に基づき、
ステップｈ）において、前記パーソナル電子デバイスは、前記認証サーバから前記暗号化鍵を読出し、前記個人情報を復号化し、前記受け手側システムに前記ユーザの前記復号化された個人情報を送る、
［Ｃ１０］に記載の認証方法。
［Ｃ１２］
ステップｂ）において前記認証サーバによって割り当てられた前記トークンＩＤは、前記ユーザのパーソナル電子デバイスの固有な識別子に基づく、［Ｃ８］ないし［Ｃ１１］のいずれか一項記載の認証方法。
［Ｃ１３］
ステップｂ）において前記認証サーバによって割り当てられた前記トークンＩＤは、前記ユーザのパーソナル電子デバイスの固有な識別子と前記認証サーバによって設定されたランダムトークン鍵とに基づき、
更に、前記ユーザが、任意の時点において、前記ユーザのパーソナル電子デバイスの前記固有な識別子と前記認証サーバの前記ランダムトークン鍵とに基づいて新たなトークンＩＤを生成することができるステップｊ）を含む、
［Ｃ８］ないし［Ｃ１２］のいずれか一項に記載の認証方法。
［Ｃ１４］
前記受け手側システムによって、前記ユーザからの処理要求の受け取りに応じて、ランダムコードを生成し、前記ランダムコードを前記認証サーバに送るステップと、
前記認証サーバによって、前記認証要求と共に、前記受け手側システムから受け取られた前記ランダムコードを、前記ユーザのパーソナル電子デバイスに送るステップと、
前記受け手側システムによって、前記ユーザのパーソナル電子デバイスから前記ランダムコードを受け取り、前記生成され、受け取られたランダムコードに基づいて前記ユーザを認証するステップと、
を更に備える、［Ｃ８］ないし［Ｃ１３］のいずれか一項に記載の認証方法。
［Ｃ１５］
少なくとも１つのプロセッサによって実行されたとき、前記少なくとも１つのプロセッサに、［Ｃ８］ないし［Ｃ１４］のいずれか一項に記載の方法の前記ステップを備える動作を実行させる命令のセットを記憶する、コンピュータ読出し可能な記憶媒体。

【図１】

図 1

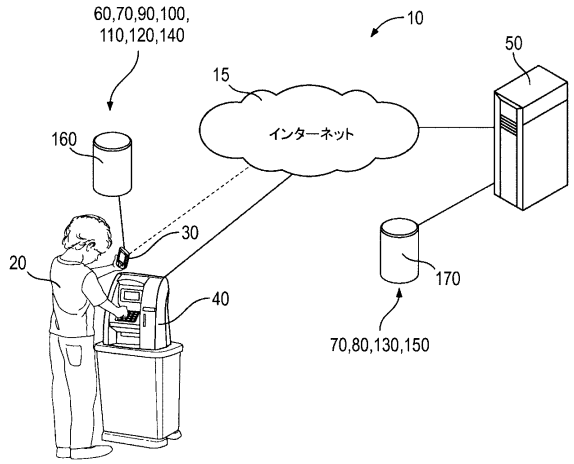

FIG. 1

【図２】

図 2

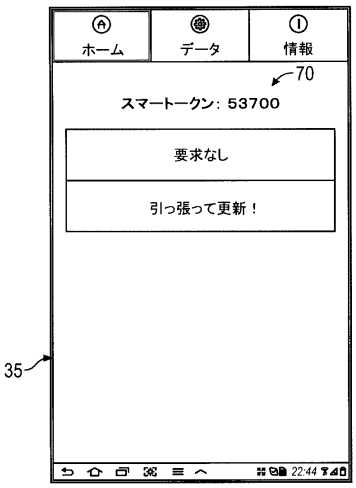

FIG. 2

【図３】

図 3

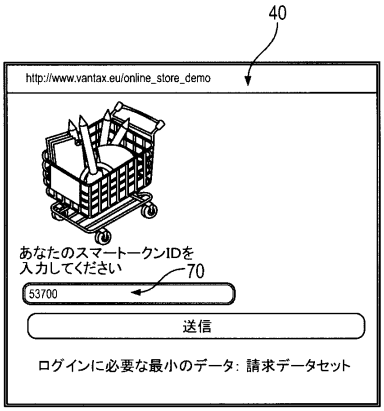

FIG. 3

【図４】

図 4

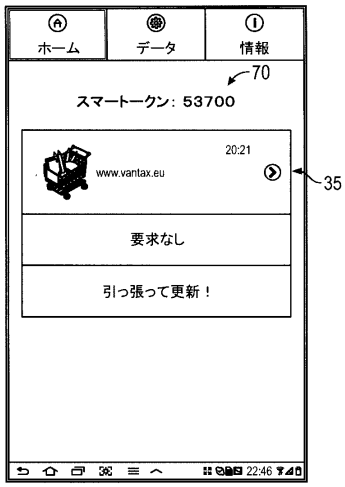

FIG. 4

【図５】

図５

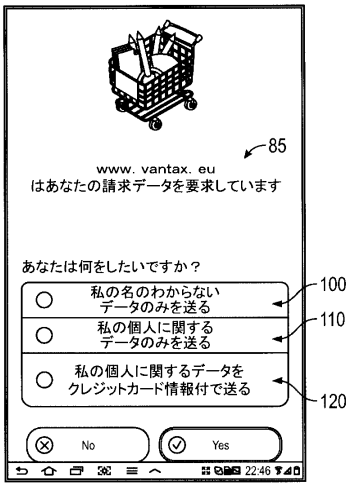

FIG. 5

【図６】

図６

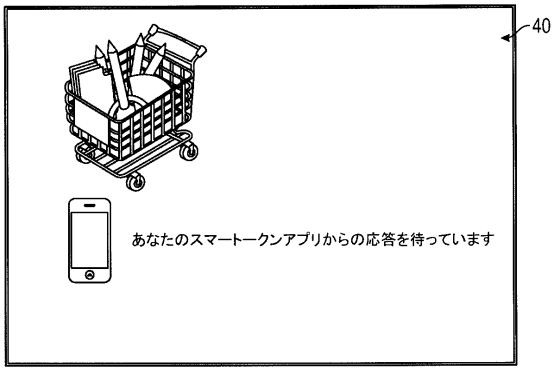

FIG. 6

【図７】

図７

FIG. 7

【図８】

図８

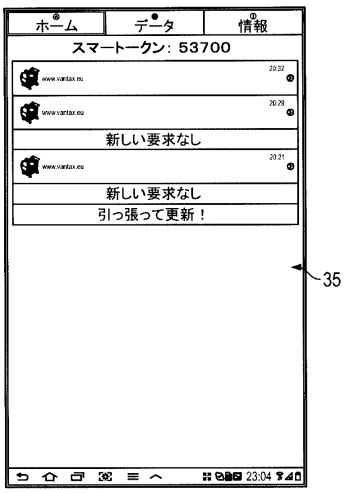

FIG. 8

【図９】

図 9

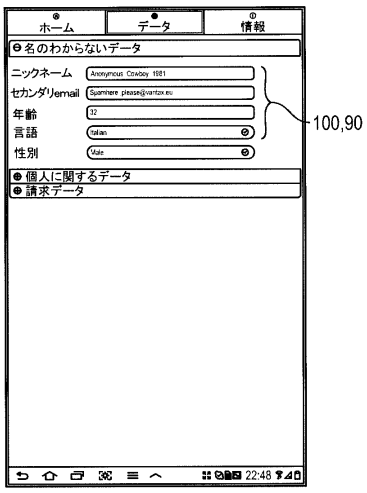

FIG. 9

【図１０】

図 10

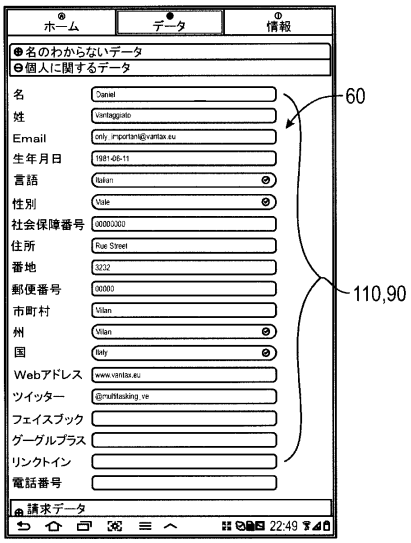

FIG. 10

【図１１】

図 11

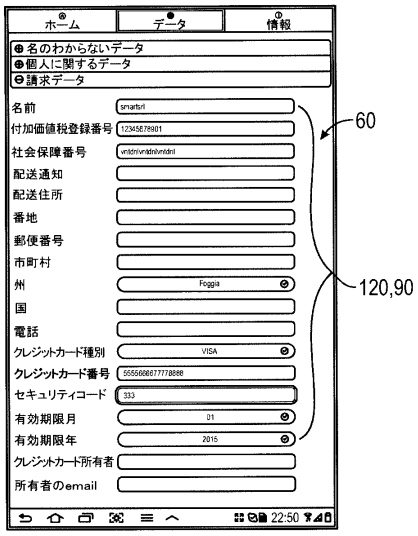

FIG. 11

【図１２】

図 12

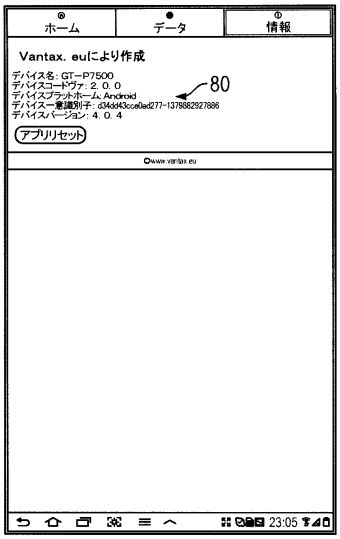

FIG. 12

フロントページの続き

(73)特許権者 516211558
バンタジアト、ダニエル
ＶＡＮＴＡＧＧＩＡＴＯ, Ｄａｎｉｅｌｅ
イタリア国、アイ－３０１７４ メストレ、ビア・ブレンドーレ ２／デー
Ｖｉａ Ｂｒｅｎｄｏｌｅ ２／ｄ, Ｉ－３０１７４ Ｍｅｓｔｒｅ, Ｉｔａｌｙ
(74)代理人 100108855
弁理士 蔵田 昌俊
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100179062
弁理士 井上 正
(74)代理人 100189913
弁理士 鵜飼 健
(74)代理人 100199565
弁理士 飯野 茂
(72)発明者 ピアーウィッツ、ビョルン
ブルガリア国、１４６３ ソフィア、ビトシャ・ブールバード １２８
(72)発明者 バンタジアト、ダニエル
イタリア国、アイ－３０１７４ メストレ、ビア・ブレンドーレ ２／デー

審査官 金沢 史明

(56)参考文献 特開２００８－２８７６８７（ＪＰ, Ａ）
特開２０１３－１４５５３３（ＪＰ, Ａ）
特開２００６－２６８６４１（ＪＰ, Ａ）
特開２００２－２９８０５４（ＪＰ, Ａ）
米国特許出願公開第２０１１／０２３７２２２（ＵＳ, Ａ１）
特開２００４－１８５４５４（ＪＰ, Ａ）
特開２００６－１７４３２０（ＪＰ, Ａ）
米国特許出願公開第２０１３／０１２４８５５（ＵＳ, Ａ１）
米国特許出願公開第２０１３／０３０５３２５（ＵＳ, Ａ１）
米国特許出願公開第２０１２／０１４４４６１（ＵＳ, Ａ１）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／３０－２１／４６
Ｇ０６Ｆ ２１／６０－２１／６２