(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5980950号
(P5980950)
(45)発行日　平成28年8月31日(2016.8.31)　(24)登録日　平成28年8月5日(2016.8.5)

(51)Int.Cl.　　F I
G06Q 20/40 (2012.01)　　G06Q 20/40
G06F 21/33 (2013.01)　　G06F 21/33　350

請求項の数 17　(全 15 頁)

(21)出願番号　特願2014-550434(P2014-550434)
(86)(22)出願日　平成24年12月26日(2012.12.26)
(65)公表番号　特表2015-512068(P2015-512068A)
(43)公表日　平成27年4月23日(2015.4.23)
(86)国際出願番号　PCT/US2012/071673
(87)国際公開番号　WO2013/101843
(87)国際公開日　平成25年7月4日(2013.7.4)
審査請求日　平成26年10月10日(2014.10.10)
(31)優先権主張番号　13/340,521
(32)優先日　平成23年12月29日(2011.12.29)
(33)優先権主張国　米国(US)

(73)特許権者　506291542
ペイパル　インコーポレイテッド
アメリカ合衆国　カリフォルニア州　９５１３１　サンノゼ　ノース　ファースト　ストリート　２２１１
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　110000132
大菅内外国特許事務所特許業務法人
(72)発明者　タボー，セバスチアン　ルードヴィク，ジャン
アメリカ合衆国，カリフォルニア州　９５１２５，サンノゼ，ハミルトン　アヴェニュー　２１４５

最終頁に続く

(54)【発明の名称】マスタートークンの品質にサブトークンに関するメカニズムを利用するアプリケーションログイン

(57)【特許請求の範囲】
【請求項１】
方法を実施するようにコンピュータに命令するためのコンピュータ可読コードを格納するコンピュータ可読記憶媒体であって、
前記方法は、
サービスプロバイダとネットワーク上で通信するユーザデバイスを介してユーザを認証することと、
前記ユーザデバイス上にマスタートークンを生成することと、
前記マスタートークンにスコアを関係付けることと、
前記ユーザデバイス上に前記マスタートークンが存在するか否かをチェックすることと、
前記ユーザデバイス上で前記ユーザによって起動された複数のアプリに対して、前記マスタートークンの複数のサブトークンを生成することであって、前記複数のアプリのうちの１つのアプリを起動することは、前記１つのアプリが取引の検証へ直接進行するように、前記複数のサブトークンのうちの１つのサブトークンに応じて、前記１つのアプリによるログインプロセスをスキップすることを含む、ことと、
前記取引を検証することと、
を含む、ことを特徴とするコンピュータ可読記憶媒体。
【請求項２】
前記スコアは、前記ユーザの前記認証に基づいて、前記ユーザデバイスに割り当てられ

る、ことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項３】
前記ユーザデバイスを介して前記ユーザを認証することは、ユーザ名およびパスワード入力以上に前記ユーザを認証することをさらに含む、ことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項４】
前記ユーザを認証することをさらに含み、必要とされる認証の強度は、前記スコアに従って決定される、ことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項５】
前記スコアは、複数の登録パラメータに基づいて、前記ユーザデバイスに割り当てられ、
起動されたとき、前記１つのアプリによる前記ログインプロセスをスキップすることは、前記ユーザが前記ユーザの任意の証明の入力を求められないように、前記マスタートークンからの前記スコアの値が前記サービスプロバイダのポリシーに則していることに応じて、前記ユーザが認証されたと判定することを含む、
ことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項６】
ユーザ名およびパスワード入力以上に前記ユーザを認証することをさらに含み、前記認証は、前記ユーザのバイオメトリック識別を含む、ことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項７】
前記マスタートークンは、それを超えると有効でなくなる有効期限を有し、
前記アプリに対する前記マスタートークンの前記サブトークンは、前記マスタートークンとは異なる有効期限を有し、
前記アプリに対する前記サブトークンの前記有効期限は、前記スコアに基づいて決定される、
ことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項８】
前記マスタートークンは、特定の条件に応じて無効化され、
前記マスタートークンが無効化されたのに応じて、前記サブトークンがキャンセルされる、
ことを特徴とする請求項１に記載のコンピュータ可読記憶媒体。
【請求項９】
サービスプロバイダとネットワーク上で通信するユーザデバイスを介してユーザを認証することと、
前記ユーザデバイス上にマスタートークンを生成することと、
前記マスタートークンにスコアを関係付けることと、
前記マスタートークンが前記ユーザデバイス上に存在するか否かをチェックすることと、
前記ユーザデバイス上で前記ユーザによって起動された複数のアプリに対して、前記マスタートークンの複数のサブトークンを生成することであって、前記複数のアプリのうちの１つのアプリを起動することは、前記１つのアプリが取引の検証へ直接進行するように、前記複数のサブトークンのうちの１つのサブトークンに応じて、前記１つのアプリによるログインプロセスをスキップすることを含む、ことと、
前記取引を検証することと、
を含む、ことを特徴とする方法。
【請求項１０】
前記スコアは、前記ユーザの前記認証に基づいて、前記ユーザデバイスに割り当てられる、ことを特徴とする請求項９に記載の方法。
【請求項１１】

前記ユーザデバイスを介して前記ユーザを認証することは、ユーザ名およびパスワード入力以上に前記ユーザを認証することをさらに含む、ことを特徴とする請求項９に記載の方法。

【請求項１２】

前記ユーザを認証することをさらに含み、必要とされる認証の強度は前記スコアに従って決定される、ことを特徴とする請求項９に記載の方法。

【請求項１３】

ユーザ名およびパスワード入力以上に前記ユーザを認証することをさらに含み、前記認証は前記ユーザのバイオメトリック識別を含む、ことを特徴とする請求項９に記載の方法。

【請求項１４】

ユーザ名およびパスワード入力以上に前記ユーザを認証することをさらに含み、前記認証はデバイス識別を含む、ことを特徴とする請求項９に記載の方法。

【請求項１５】

前記スコアは、複数の登録パラメータに基づいて前記ユーザデバイスに割り当てられ、

起動されたとき、前記１つのアプリによる前記ログインプロセスをスキップすることは、前記ユーザの任意の証明の入力を前記ユーザが求められないように、前記マスタートークンからの前記スコアの値が前記サービスプロバイダのポリシーに則していることに応じて、前記ユーザが認証されたと判定することを含む、

ことを特徴とする請求項９に記載の方法。

【請求項１６】

前記マスタートークンは、それを超えると有効でなくなる有効期限を有し、

前記アプリに対する前記マスタートークンの前記サブトークンは、前記マスタートークンとは異なる有効期限を有し、

前記アプリに対する前記サブトークンの前記有効期限は、前記スコアに基づいて決定される、

ことを特徴とする請求項９に記載の方法。

【請求項１７】

前記マスタートークンは、特定の条件に応じて無効化され、

前記マスタートークンが無効化されたのに応じて、前記サブトークンがキャンセルされる、

ことを特徴とする請求項９に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本開示は、概してハンドヘルドモバイルもしくは他の消費者電子デバイスを利用してネットワーク上で実施される通信用のセキュリティに関し、より詳細には、デバイス上の複数のアプリを利用するとき、迅速なログインもしくはログインの繰り返しの回避のいずれかを通してユーザに利便性を提供するデバイス上で実行するアプリへログインするためのセキュリティメカニズムに関する。

【背景技術】

【０００２】

モバイルウェブブラウザを有する携帯電話、スマートフォン、電子ノートパッドなどの多くの小型、ハンドヘルド消費者電子デバイスは、例えば、テキスティング（テキストメッセージの送受信）、ソーシャルネットワーキング、電子メール、電子商取引（電子デバイスを利用して、インターネットおよび他のコンピュータネットワークなどの電子ネットワーク上での製品もしくはサービスの売買のことを概して称する）を含む種々のタイプの通信用に種々のアプリケーションプログラムもしくは“アプリ”の利用を可能にする。これらの種々のタイプの通信用に利用されるアプリは、アプリの利用に対する無認可アクセスを認めない点において、幾つかの形式のセキュリティから利益を受け、かつそれに依存

し、したがって、ログインの幾つかの形式を必要とすることがある。例えば、銀行もしくは他の金融サービスプロバイダは、金融サービスプロバイダにおけるデバイスユーザアカウントに対するアクセスを可能とするモバイルデバイス上で使用するためのアプリを提供してもよい。同様に、例えば、電子メールおよびソーシャルネットワーキングの場合には、電子メールアカウントのオーナーもしくはオーナーのソーシャルネットワーキングページの偽装を防ぐことが望ましくかつ重要でありうる。したがって、ユーザデバイス上のアプリの多くは、アプリのユーザを認証するために、安全なログインの幾つかの形式を必要とすることがある。多くのアプリが単一のデバイス上で一度に使用されるとき、ユーザは、あるアプリから別のアプリへと切り替えるとき、または、ユーザが既にログアウトした以前使用したアプリに戻るとき、複数のログインもしくは繰り返しのログインに由来する幾つかの不便（例えば、所望のタスクを実現するうえでの遅延）に遭遇することがある。

【発明の概要】

【０００３】

本発明の一つ以上の実施形態に従い、ユーザが多数のアプリを起動するとき、ユーザが異なる各アプリに繰り返しログインする必要がなく、多数のアプリがデバイス上でアクセス可能になるように、ユーザがデバイスにログインすることを可能にするための方法およびシステムが、提供される。メカニズムは、品質スコアを有するマスタートークンを提供することと、最初のログインによって提供されるセキュリティレベルを評価するためのスコア品質とサブトークンを利用することができる各アプリ用のサブトークンを提供することと、アプリがそれ自身のログインプロセスを短縮するかスキップすることを可能にすることと、ユーザに向上したレベルの効率および利便性を提供することと、で開示される。

【０００４】

一つ以上の実施形態においては、システムは、プロセッサと、方法を実施するようにプロセッサに命令するためのコンピュータ可読コードを有するコンピュータ可読媒体とを含み、方法は、サービスプロバイダとネットワーク上で通信するユーザデバイスを介してユーザを認証することと、ユーザデバイス上でマスタートークンを生成することと、マスタートークンがデバイス上に存在するか否かをチェックすることと、ユーザによって起動されたデバイス上のアプリ用にマスタートークンのサブトークンを生成することと、アプリが取引の検証に直接進行するように、サブトークンに応じてアプリによるログインプロセスを飛び越えることを含むアプリの起動をすることと、サブトークンに含まれる情報に基づいて取引を検証することと、を含む。

【０００５】

本開示のこれらおよび他の態様は、添付の図面と併せて以下に説明される実施形態の詳細な記述から容易に明らかになるであろう。

【図面の簡単な説明】

【０００６】

【図１】一つ以上の実施形態に従って、複数のアプリにログインするためのサブトークンを利用してネットワーク上で通信する、スコアベースの迅速なログイン用のシステムを示すシステム図である。

【図２】一つ以上の実施形態に従って、複数のアプリにログインするためのサブトークンを利用してネットワーク上で通信する、スコアベースの迅速なログイン用のメカニズムを示すブロック図である。

【図３】一つ以上の実施形態に従って、複数のアプリにログインするためのサブトークンを利用してネットワーク上で通信する、スコアベースの迅速なログイン用の方法を示すプロセスフロー図である。

【０００７】

本発明の実施形態およびその利点は、以下に続く詳細な説明を参照することによって、最良に理解される。

【発明の詳細な説明】

【０００８】

本発明の一つ以上の実施形態に従い、ユーザの経験を顕著に改善することができる（例えば一つ以上のアプリに対する）連続的ログインを容易にするために使用することができる認証をデバイスに対するログインが提供するように、デバイスに対して安全にログインして、ネットワーク上で通信するための方法およびシステムが提供される。換言すると、安全なデバイス結合は、アプリ（アプリケーションプログラム）を変更するとき、ログインの繰り返しを回避することによってユーザに利便性を提供してもよい。一実施形態においては、ユーザおよびデバイスは、例えば、バイオメトリック技術を利用して、最初のログインにおいて、強力に認証されてもよい。強力な認証の結果として、一時的マスタートークンが生成され、アプリがユーザからの当該アプリへのログインを必要とすることなく、アプリに対して安全なログインを提供するためにサブトークンを利用して、他のアプリケーションが一時的マスタートークンを活用することができる。したがって、ユーザが多数のアプリを起動するときに、ユーザが異なる各アプリに繰り返しログインする必要なく、多数のアプリがデバイス上でアクセス可能になるように、ユーザは、デバイスにログインすることが可能となってもよい。幾つかの実施形態に従い、唯一つのアプリに対する複数のログインもしくは一度のログインさえも回避することによって、オンラインショッピング、ポイントオブセール（ＰＯＳ）におけるサービスプロバイダ支払から会計するときの待ち時間を減少させ、オフグリッド（ｏｆｆ－ｔｈｅ－ｇｒｉｄ）取引を解決するのに役立つことがある。一実施形態においては、バイオメトリクスはしたがって、ユーザを“安全にする”ためだけに使用されるのではなく、ユーザに時間節約という利便性を提供するためにも使用されることがある。

【０００９】

一つ以上の実施形態に従い、品質スコアを有するマスタートークンを提供することと、最初のログインによって提供されるセキュリティレベルを評価するために、サブトークンとスコア品質を利用することができる、一つ以上のアプリ（例えば、各アプリがそれ自身のサブトークンを有する）に対するサブトークンを提供することと、アプリがそれ自身へのログインプロセスを安全に短縮するか、スキップすることを可能にすることと、ユーザに対して向上したレベルの効率と利便性を提供することのメカニズムが開示される。一実施形態においては、マスタートークンを生成する同一のアプリは、任意の他のアプリに対してサブトークンを生成し、アプリのアプリケーションプログラミングインターフェイス（ＡＰＩ）を介してアプリとのインターフェイスを提供する。別の実施形態においては、各アプリはそれ自身のサブトークンを生成し、ＡＰＩを介してマスタートークンにアクセスする。一実施形態においては、マスタートークンは、ルートトークンにリンクされるサブトークンを含むトークンのツリー（データ構造）のうちのルートトークンであってもよい。結果として、ユーザが、モバイルデバイス上の一つ以上のアプリにアクセスするとき、アプリにおけるログインプロセスを経験する必要がない。それでも、ログインは、サービスプロバイダによって予め決められたリスクパラメータに基づいて、高額購入などの特定の状況において必要とされることがある。

【００１０】

一実施形態においては、買い物の会計もしくは既知のモバイルデバイス上のアプリとの他の金融取引プロセスを経験するとき、消費者が必ずしも常に彼らのパスワードを入力する必要がないように、デバイス上のアプリのセキュリティ機能を可能にするために、モバイルデバイスは、例えば、サービスプロバイダ、販売者、銀行もしくは他の商業的エンティティとのアカウントに結合されるか、結合を経験する。このデバイス結合は、種々の支払フロー、リスク管理プロセスおよびモデル、ならびに他のデバイスベースの論理における余分なログインをスキップすることなどの機能用に基礎として役立つことができる。一実施形態においては、デバイスは、一つ以上のデバイス識別子を含みうるデバイス識別（ＩＤ）を得るために、例えば、デバイス照合を通して、最初のログイン中に結合されてもよい。

【００１１】

デバイス結合は、バイオメトリック技術（例えば、指紋スキャン、網膜スキャン、声紋

）および、代替もしくはそれに加えて、デバイス上に存在する一意的なデバイス識別子（例えば、国際移動体装置識別番号（ＩＭＥＩ）、デバイス名、種々の修正変更日チェック（例えば、以前インストールされたバージョン由来の異なるタイムスタンプを有するファームウェアの新バージョン）および他の変数もしくは識別子の組み合わせ）に基づいてもよい。デバイスの当該一意的な識別子の利用は、ユーザがデバイス上での連続的ログインのスキップを望む場合に、デバイス上のアプリにわたって、サービスプロバイダがユーザを記憶することを可能にしてもよい。複数のモバイルデバイスは単一のアカウントに結合されてもよい。

【００１２】

図１は、一つ以上の実施形態に従い、サービスプロバイダ（ＳＰ）１２０を利用して、商業的エンティティ（例えば、販売者１３０）へとネットワーク１０６（例えば、インターネット）上で通信するために、モバイルデバイス１０４（“ユーザデバイス”とも称される）を利用するユーザ１０２によって、複数のアプリにログインし、支払（もしくは他のセキュリティの必要な金融取引）をするためにサブトークンを利用するスコアベースの迅速なログイン用のシステム１００を示す。サービスプロバイダ１２０は、支払プロバイダであってもよいし、ＳａｎＪｏｓｅ，ＣＡのＰａｙＰａｌ，Ｉｎｃ．などの金融サービスの他のプロバイダであってもよい。ネットワーク１０６は、単一ネットワークもしくは複数のネットワークの組み合わせとして実装されてもよい。例えば、種々の実施形態においては、ネットワーク１０６は、一つ以上のイントラネット、ランドラインネットワーク、ワイヤレスネットワークもしくはインターネットを含む他の適切なタイプの通信ネットワークを含んでもよい。別の実施例においては、ネットワークは、インターネットなどの他の通信ネットワークで通信するように適応されたワイヤレス遠距離通信ネットワーク（例えば携帯電話ネットワーク）を含んでもよい。

【００１３】

モバイルデバイス１０４は、例えば、ラップトップ、スマートフォン、タブレット、または他のモバイルコンピューティングもしくは通信デバイス、インターネット接続を有するテレビ、セットトップボックス、他のネットワーク接続されたデバイスであってもよい。クライアントとして機能することがある（“クライアントデバイス”１０４とも称される）モバイルデバイス１０４は、ネットワーク１０６上での有線もしくはワイヤレス通信用に構成されたハードウェアとソフトウェアの任意の適切な組み合わせを利用して実現されてもよい。例えば、モバイルデバイス１０４は、ネットワーク１０６と連通するユーザ１０２（例えば、クライアントもしくは消費者）のパーソナルコンピュータとして実現されてもよい。また、例えば、モバイルデバイス１０４は、ワイヤレス電話（例えば、携帯電話）、パーソナルデジタルアシスタント（ＰＤＡ）、ノートブックコンピュータとして実現されてもよい。

【００１４】

図１に示されるように、ブラウザアプリ１０８は、モバイルデバイス１０４上で実行し、ネットワーク１０６上で使用可能な情報をユーザ１０２が閲覧することを許可するために、ユーザインターフェイスを提供するために使用されてもよい。例えば、ブラウザアプリ１０８は、ネットワーク１０６上で使用可能な情報を閲覧するためのウェブブラウザとして実現されてもよい。一実施形態においては、ブラウザアプリ１０８は、ネットワーク１０６を介して販売者１３０およびサービスプロバイダ１２０とインターフェイス接続して通信するように構成されたプロセッサによって実行可能なグラフィカルユーザインターフェイス（ＧＵＩ）などのソフトウェアプログラムを含んでもよい。例えば、ユーザ１０２は、品目を見つけて購入するために、販売者１３０を介して販売者ウェブサイトにアクセスしてもよい。ユーザ１０２は、クライアントモバイルデバイス１０４を通して、サービスプロバイダ１２０を介して販売者１３０に対するアカウントを生成して支払をするために、サービスプロバイダサーバ１２２と通信してもよい。モバイルデバイス１０４は、サービスプロバイダサーバ１２２との迅速な支払をすることを含む、ユーザ１０２に対して利用可能なさらなる特性を作成するために望まれるような他のアプリ１１０を含んでも

よい。例えば、アプリ１１０は、ネットワーク１０６を介してオンラインサイトを通してユーザ１０２が情報を送受信することを可能にするインターフェイスおよび通信プロトコルを含んでもよい。アプリ１１０は、クライアント側セキュリティ特性を実現するためのセキュリティアプリケーション、ネットワーク１０６上の適切なアプリケーションプログラミングインターフェイス（ＡＰＩ）とインターフェイス接続するためのプログラマチッククライアントアプリケーション、種々の他のタイプの一般的に既知のプログラムおよびアプリケーションを含んでもよい。

【００１５】

モバイルデバイス１０４は、ユーザの登録および認証用のアプリケーション１１２、１１４も含んでもよい。例えば、アプリケーション１１２は、サービスプロバイダ１２０とのアカウントおよびセキュリティアイデンティティを確立するために提供されてもよい。アプリケーション１１２は、ユーザが、デバイス上の（例えば）指紋リーダに彼の指をスキャンするとき、ユーザの指紋がデバイス１０４に対するＩＤとして、かつ、サービスプロバイダ１２０でのアカウント用のＩＤとして確立され、アプリケーション１１２がＳＰ１２０での登録を提供しうるように、例えば、デバイス１０４とユーザ１０２を接続するユーザ１０２用のバイオメトリックアイデンティティを確立してもよい。端末（ハンドセット）製造者（例えば、デバイス１０４の製造者）は、この機能を提供することがあるが、オペレーティングシステム（ＯＳ）プロバイダもしくはサービスプロバイダ（ＳＰ１２０もしくは信頼されたサービスマネージャ（ＴＳＭ）など）によって提供される可能性もある。登録プロセスは、ＳＰ１２０による将来のリスク管理を可能とする多数の種々の態様を含んでもよい。マスタートークンを生成するか可能とするために必要とされる多くのパラメータは、（例えば、登録時に）予め決定され、各ＳＰは、その後、それらのサブトークンの生成に含まれるこれらの“共有”パラメータの全てもしくはほとんどを使用することができる。登録時に予め決定されたパラメータは、マスタートークン内に事前設定されたパラメータに対して、“チェックリスト”もしくは“ショッピングリスト”の様に使用されてもよい。ユーザが連続的購入をするとき、例えば、特別のセキュリティが必要とされるか否かの決定は、マスタートークンもしくはサブトークンから利用可能なパラメータによって、ならびに、サービスプロバイダによって予め決定されたリスクパラメータに基づいて誘発される可能性がある。

【００１６】

アプリケーション１１４は、例えば、ユーザ１０２がデバイス１０４に連続的にログインするとき、（例えば）ユーザの指紋を照合することによって、ユーザ１０２およびデバイス１０４に対して認証を提供してもよい。

【００１７】

販売者１３０は、彼らのウェブサイトを通して製品もしくはサービスなどの種々の品目を提供するサービスプロバイダ（例えば、販売者サイト、オークションサイト、市場またはＰ２Ｐ振替、もしくは任意の他のＰ２Ｐ様情報伝達を含むソーシャルネットワーキングサイト）であってもよい。販売者１３０（販売者の任意の代理人もしくは従業員である可能性がある）は、モバイルデバイスから販売者サイトを通して購入をする消費者からのオンライン取引を処理してもよい。販売者１３０は、例えば、クライアントモバイルデバイス１０４およびサービスプロバイダサーバ１２２と、ネットワーク１０６上で通信することによって、種々のオンライン取引を自動的に処理することが可能な販売者サーバ１３２を操作してもよい。販売者サーバ１３２は、購入用に製品もしくはサービスを提供するために、購入アプリ１３４を実行してもよい。販売者サーバ１３２は、ブラウザアプリ１３６と他のアプリケーション１３８も実行してもよい。ブラウザアプリ１３６および他のアプリケーション１３８は、例えば、サービスプロバイダ１２０を通して迅速な支払を可能にするために、情報を送受信するために、販売者がサービスプロバイダ１２０ウェブサイトにアクセスして、サービスプロバイダサーバ１２２と通信することを可能にしてもよい。一つ以上の実施形態に従い、消費者（例えば、ユーザ１０２）は、ログインする必要なく、（サービスプロバイダ１２０を通して）販売者１３０との取引（例えば支払）をする

ためにアプリにアクセスし、これによって、サービスプロバイダサーバ１２２とのより迅速なサービス（例えば、支払処理の完了）を可能にする可能性がある。

【００１８】

サービスプロバイダ１２０は、例えば、ユーザ１０２の代わりに、販売者１３０とのオンライン金融情報取引用の処理を提供するオンライン支払プロバイダであってもよい。サービスプロバイダサーバ１２２は、一つ以上のアイデンティティアプリ１２４を含み、一つ以上のアイデンティティアプリ１２４は、ユーザ１０２による品目、製品、サービスの購入を容易にするために、ネットワーク１０６上での販売者サーバ１３２と同様に、クライアントモバイルデバイス１０４と相互作用するために適応されてもよい。サービスプロバイダサーバ１２２は、アカウントデータベース１２６内の複数のユーザおよび販売者アカウントを維持するように構成され、各販売者アカウントは、ユーザ１０２および一つ以上の販売者１３０を含む個々のユーザに関連付けられたアカウント情報１２８を含むか、アカウント情報１２８から分離されてもよい。例えば、アカウント情報１２８は、ユーザ１０２と販売者１３０の間のオンライン取引を容易にするために使用されることがある、フルネーム、商号、住所、電子メールアドレス、電話番号、ウェブサイトアドレス、もしくは他のタイプの金融情報のうちの一つ以上などのユーザ１０２および販売者１３０のアイデンティティ情報を含んでもよい。アカウント情報１２８もしくはアイデンティティアプリ１２４は、モバイルデバイス１０４などのユーザデバイス用のデバイス識別子（例えば、上述されたＩＭＥＩ番号などのデバイス上に存在する一意的なデバイス識別子）を含んでもよい。したがって、アイデンティティアプリ１２４は、迅速な支払を可能とするために、情報を処理し、獲得し、格納するために販売者サーバ１３２、ユーザ１０２、モバイルデバイス１０４、もしくは他の受取人と相互作用するように構成されてもよい。

【００１９】

電子メールサービスプロバイダ１４０は、販売者１３０、サービスプロバイダ１２０などのネットワーク１０６に接続されたエンティティと、ユーザ１０２などの個人用の電子メールサービスを提供してもよい。電子メールサービスプロバイダ１４０は、例えば、クライアントモバイルデバイス１０４、サービスプロバイダサーバ１２２、販売者サーバ１３２、ソーシャルネットワーキングサーバ１５２と、ネットワーク１０６上で通信することによって、自動的に電子メールサービスを提供することが可能な電子メールサーバ１４２を操作してもよい。電子メールサーバ１４２は、電子メールサービスを提供するための電子メールアプリ１４４を実行してもよい。電子メールサーバ１４２は、他のアプリケーション１４８も実行してもよい。

【００２０】

ソーシャルネットワーキングサービス１５０は、ユーザ１０２などのネットワーク１０６に接続される個人（および可能性のある他のエンティティ）用のソーシャルネットワークを提供してもよい。ソーシャルネットワーキングサービス１５０は、ネットワーク１０６に接続されるユーザ１０２などの種々のサービス利用者に対するアクセス用のソーシャルネットワーキングウェブサイトを提供することができるネットワーキングアプリ１５４を実行しうるサーバ１５２を操作してもよい。サーバ１５２は、ソーシャルネットワーキングサービスおよびウェブサイトアクセスを提供するための他のアプリケーション１５８を実行してもよい。

【００２１】

図２は、一つ以上の実施形態に従い、複数のアプリに対するログイン用のサブトークンを利用して、ネットワーク上で通信するスコアベースの迅速なログイン用のメカニズム２００を示す。図２に示されるように、ユーザ（例えば、ユーザ１０２）は、バイオメトリクス用に可能とされることがある、ユーザデバイス１０４に対するバイオメトリック入力２０８を提供してもよい。例えば、ユーザは、指紋読み取り性能を有するモバイルデバイス上で彼の指紋をスキャンしてもよい。バイオメトリクスの利用は、（例えば、ＰＩＮの代わりに）電話のロック解除をするために実施することができるユーザの強力な認証を含む。

【００２２】
バイオメトリック入力２０８に応じて、マスタートークン２０１は、幾つかの制御パラメータ（例えば、時間、範囲、適用分野、設定用パラメータ）を有するように（応答２０９において）生成されてもよい。マスタートークン２０１がパラメータを利用して生成されると、マスタートークン２０１に関連付けられたスコアが得られてもよい。例えば、デバイスＩＤ、ユーザの指紋読み出し性能、指紋の認識された回数、（例えば、デバイス１０４のＧＰＳ（グローバル測位システム）からの）位置などを知ると、マスタートークンの品質は、より高いかより低くなり、０－１００％の範囲内の品質スコアを生成する。例えば、最初のスコアは９０％であるが、不良な読み出し、未知のデバイスもしくは異常な位置は、４０％に過ぎないスコアが帰するマスタートークン２０１を生成する可能性がある。スコアに基づいて、それらのアプリケーション（例えば、アプリ２２４、２３４、２４４、２５４）を介して種々のサービスプロバイダは、ログインが必要とされるか否か、もしくはログインをバイパスすることができるか否かを判定する可能性がある。スコアは、各アプリに対応するサブトークン（例えば、アプリ２２４、２３４、２４４、２５４に対して、其々サブトークン２０２、２０３、２０４、２０５）上で利用可能であってもよい。

【００２３】
マスタートークン２０１およびそれに関連付けられたスコアで、サービスプロバイダもしくは他のエンティティ（例えば、商業的エンティティ１３０、サービスプロバイダ１２０、電子メールサービスプロバイダ１４０、ソーシャルネットワーキングサービス１５０）は、そのアプリケーション（例えば、其々商業的エンティティアプリ２３４、サービスプロバイダアプリ２２４、電子メールサービスプロバイダアプリ２４４、ソーシャルネットワーキングアプリ２５４）が、認証された（例えば、今知られている）ユーザおよびマスタートークン２０１を活用するために検証されたデバイス（例えば、デバイス１０４）のＯＳ上で稼動するのを可能にし、また、マスタートークン２０１のスコアもしくは品質に基づいて、上記アプリのフローにおける機能の幾つかを自動的に起動するためのサブトークンを生成することを可能にする。マスタートークン２０１に関連づけられた品質スコアは、ＯＳレベルにおける処理負荷を軽減するような処理を可能とし、ログインおよびサブトークン生成を加速することがある。

【００２４】
マスタートークン２０１は、図２に示されるように、デバイス１０４上に格納され、デバイス１０４上のメモリに格納されうるツリーデータ構造２１０へとリンクするための規定を有してもよい。マスタートークン２０１は、例えば、耐タンパー性コンポーネント、暗号による保護、もしくは他の類似するセキュリティ技術を利用して、デバイス１０４上の信頼されるもしくは安全な領域に格納されてもよい。ツリーデータ構造２１０およびサブトークンは、同様に保護されてもよい。

【００２５】
図２に示されるように、マスタートークン２０１は、ツリー２１０のルート（根）トークンとして格納され、その後に生成されるサブトークン（例えば、サブトークン２０２、２０３、２０４、２０５）がマスタートークン２０１へとリンクされて、ツリー２１０を形成してもよい。図２に示されるように、サブトークン２０２－２０５は、“複数のリーフ（葉）”として表されているが、ツリー２１０は、幾つかの実施形態においては、中間の例えばリーフではない（ｎｏｎ－ｌｅａｆ）ノードを有してもよい。

【００２６】
図２に示されるように、各サブトークンは、デバイス１０４上の特定のアプリに対して生成され、サブトークンが生成されたアプリによってのみ使用されてもよい。例えば、サブトークン２０３は、商業的エンティティアプリ２３４に属し、商業的エンティティアプリ２３４はデバイス１０４上で稼動し、購入アプリ１３４と通信することによって商業的エンティティ１３０と相互作用するために使用されてもよい。同様に、サブトークン２０２は、図２に示されたような、金融サービスプロバイダアプリ２２４などに属する。各サ

ブトークンは、デバイス１０４上で稼動中であって且つマスタートークン２０１を生成するのと同一のアプリであってもよいサービスプロバイダアプリ（例えば、アプリ１１２もしくはアプリ１１４）によって、特定のアプリに対して生成されてもよい。あるいは、各アプリは、マスタートークン２０１に認可された許可およびアクセスを利用して、それ自身のサブトークンを生成してもよい。例えば、アプリ２３４はサブトークン２０３を生成し、アプリ２２４はサブトークン２０２を生成し、アプリ２４４はサブトークン２０４を生成し、アプリ２５４はサブトークン２０５を生成してもよい。サブトークンの生成は、“マスター”サービスプロバイダアプリ（例えば、アプリ１１２、１１４）を含む各アプリ（例えば、アプリ２３４、２２４、２４４、２５４）用のＡＰＩの利用によって容易にされることがある。

【００２７】

サブトークンは、金融サービスプロバイダアプリ２２４用のサブトークン２０２に関連付けられたカウントダウンタイマー２１２などの特定の機能を与えられてもよい。当該実施例においては、マスタートークンによって提供される境界を特別な機能が踏み越えることができないことを保証するために、サブトークン自身のアプリではなくて“マスター”サービスプロバイダアプリがサブトークンを生成することが望ましい可能性がある。例えば、サブトークン２０２用のカウントダウンタイマーは、マスタートークン２０１用の有効期限よりも長い合計時間を有することが許可されず、それは、“マスター”サービスプロバイダアプリ（例えば、アプリ１１２、１１４）のみがサブトークン２０２を生成することを可能として、かつアプリ２２４が、それ自身のサブトークンを生成することを不可能とすることによって、実現することができる。

【００２８】

図３は、一つ以上の実施形態に従い、複数のアプリに対するログイン用のサブトークンを利用して、ネットワーク上で通信するスコアベースの迅速ログイン用の方法３００を示す。方法３００のステップ３０１において、ユーザ（例えば、ユーザ１０２）は、バイオメトリック技術などの強力な認証の形式を利用して、デバイス（例えば、デバイス１０４）をロック解除してもよい。例えば、ユーザは、デバイスをロック解除するために、指紋リーダに指をスキャンしてもよいし、サービスプロバイダ（ＳＰ）へと許容可能な音声サンプルもしくは他の形式のセキュリティを与えて、結果としてデバイスとユーザの強力な結合をもたらす。

【００２９】

ステップ３０２において、アプリケーションマスタートークン（例えば、マスタートークン２０１）は、幾つかの制御パラメータ（例えば、有効期限、範囲、適用分野、種々のパラメータ用の設定）を有するデバイス上に生成されてもよい。

【００３０】

ステップ３０３において、マスタートークンの品質のスコアが、種々のパラメータ（例えば、デバイスＩＤ、ユーザ指紋読み出し品質、当該指紋が認識された回数、デバイス位置、ＳＰによって保持された履歴データ）の品質に基づいてマスタートークンに対して得られてもよい。

【００３１】

ステップ３０４において、ユーザがアプリを起動するとき、アプリは、（バックグラウンドにおいて）コールを行い、マスタートークンのデバイス上の存在、マスタートークンに関連付けられたスコアをチェックし、かつ、マスタートークンとその品質スコアを検索する。あるいは、これらのステップは、“マスター”サービスプロバイダアプリ（例えば、登録アプリ１１２もしくは認証アプリ１１４）によって上述されたように実施されてもよい。

【００３２】

ステップ３０５において、サブトークン（例えば、サブトークン２０２、２０３、２０４、２０５）は、ＳＰリスクポリシー（例えば、時間、有効期限、アクティブモード期間）に則してパラメータを有するアプリ用に（例えば、アプリが起動されるとき）生成され

てもよい。

【００３３】

ステップ３０６において、ユーザがアプリ（例えば、任意のアプリ２２４、２３４、２４４、２５４）を起動するとき、ユーザは、証明（例えば、電話番号とＰＩＮ、もしくは電子メールとパスワード）を入力することを求められない。なぜなら、ユーザは、マスタートークン２０１からの品質スコアが、ＳＰによって開発されて受諾されたポリシーにのっとっているか否かを既に検証されているからである。例えば、金融サービスプロバイダアプリ２２４は、９９％スコアを要求とし、ソーシャルネットワーキングアプリ２５４は８０％スコアのみを要求としてもよい。

【００３４】

ステップ３０７において、アプリは、ログインプロセスを飛び越えて（スキップして）、取引の検証へと直接進行してもよい。取引は、例えば、商業的エンティティアプリ２３４を利用する販売者エンティティにおける買い物の場合、購入であってもよい。さらには、サービスプロバイダ１２０を利用する買い物の会計プロセスが、サブトークンで検証された別のアプリケーション（例えば、ソーシャルネットワーキングアプリ２５４）に由来する場合、ユーザは、サービスプロバイダ１２０を利用して支払をするためにクリックし、金額を検証し、確認をクリックするだけでよい。

【００３５】

ステップ３０８において、異なるアプリケーション（例えば、アプリ２２４、２３４、２４４、２５４）は、異なる期間生きた状態にあり（有効なままであり）、マスタートークン２０１とは異なる期間生きた状態にあるサブトークン（例えば、其々、サブトークン２０２、２０３、２０４、２０５）を有してもよい。例えば、あるアプリから別のアプリに対して、より低いセキュリティ要求もしくはより低いプライバシー懸念のために、より長い時間が許可されることがあり、当該決定はマスタートークン由来のより低いスコアに基づく可能性がある。例えば、現在マスタートークン２０１が以前よりも低いスコアを有する場合、アプリは、より低いマスタートークン品質スコアのより大きい認知されたリスクをオフセットするために、より短期間の間、有効であるように、サブトークンを選択してもよい。

【００３６】

ステップ３０９において、例えば、ユーザのバイオメトリック登録に対して、ユーザのバイオメトリック入力に不一致が存在するか、デバイスが長期間オフグリッドであるか、アップデートがアプリケーションに対してなされた場合、マスタートークンは、無効化することができる。マスタートークンの無効化は、結果として、全ての既存のサブトークンをキャンセルするか消去することができる。ユーザおよびデバイスが再度強固に結合される（例えば、ユーザが、満足なバイオメトリック入力２０８でデバイスに対してログインする）と、マスタートークン２０１が生成されて、サブトークンが再発行されてもよい。

【００３７】

種々の実施形態の実現においては、本発明の実施形態は、パーソナルコンピュータ、ラップトップ、ＰＤＡ、携帯電話または他のパーソナルコンピューティングもしくは通信デバイスなどのパーソナルコンピューティングデバイスを含んでもよい。支払プロバイダシステムは、支払プロバイダシステムによって提供される支払サービスを提供するために、コンピュータシステムもしくはネットワークを定義するために組み合わせられるサーバ、もしくは複数のサーバ、コンピュータ、プロセッサなどのネットワークコンピューティングデバイスを含んでもよい。

【００３８】

この点においては、コンピュータシステムは、情報を通信するためにバスもしくは他の通信メカニズムを含み、処理コンポーネント（例えば、プロセッサ、マイクロコントローラ、デジタル信号プロセッサ（ＤＳＰ）など）、システムメモリコンポーネント（例えば、ＲＡＭ）、スタティック格納コンポーネント（例えば、ＲＯＭ）、ディスクドライブコンポーネント（例えば、磁気もしくは光学）、ネットワークインターフェイスコンポーネ

ント（例えば、モデムもしくはイーサネットカード）、ディスプレイコンポーネント（例えば、ＣＲＴもしくはＬＣＤ）、入力コンポーネント（例えば、キーボードもしくはキーパッド）および／もしくはカーソル制御コンポーネント（例えば、マウスもしくはトラックボール）などのコンポーネントとサブシステムを相互接続する。一実施形態においては、ディスクドライブコンポーネントは、一つ以上のディスクドライブコンポーネントを有するデータベースを含んでもよい。

【００３９】

コンピュータシステムは、プロセッサによる特定の動作を実施して、システムメモリコンポーネントに含まれる一つ以上の命令の一つ以上のシーケンスを実行する。当該命令は、スタティック格納コンポーネントもしくはディスクドライブコンポーネントなどの別のコンピュータ可読媒体からシステムメモリコンポーネントへと読み出されてもよい。他の実施形態においては、ハードワイヤード回路は、本発明を実現するために、ソフトウェア命令も代わりに、もしくはソフトウェア命令と組み合わせて使用されてもよい。

【００４０】

論理は、コンピュータ可読および実行可能媒体にエンコードされ、実行用のプロセッサに対する命令の提供に関与する任意の媒体のことを称する。当該媒体は、不揮発性媒体、揮発性媒体、伝送媒体を含むがそのいずれにも限定はされない多くの形式をとることがある。一実施形態においては、コンピュータ可読媒体は非一時的である。種々の実施においては、不揮発性媒体は、ディスクドライブコンポーネントなどの光学もしくは磁気ディスクを含み、揮発性媒体は、システムメモリコンポーネントなどのダイナミックメモリを含み、伝送媒体は、バスを含む配線を含む、同軸ケーブル、銅線、光ファイバを含む。一実施例においては、伝送媒体は、ラジオ波および赤外データ通信中に生成されるような、音波もしくは光波の形式をとってもよい。

【００４１】

コンピュータ可読および実行可能な媒体の幾つかの共通形式は、例えば、フロッピーディスク、フレキシブルディスク、ハードディスク、磁気テープ、任意の他の磁気媒体、ＣＤ－ＲＯＭ、任意の他の光媒体、パンチカード、紙テープ、穴のパターンを有する任意の他の物理媒体、ＲＡＭ、ＲＯＭ、Ｅ２ＰＲＯＭ、ＦＬＡＳＨ－ＥＰＲＯＭ、任意の他のメモリチップもしくはカートリッジ、キャリア波、コンピュータが読み出すために適応される任意の他の媒体を含む。

【００４２】

種々の実施形態においては、本発明を実現するための命令シーケンスの実行は、コンピュータシステムによって実施されてもよい。種々の他の実施形態においては、通信リンク（例えば、ＬＡＮ、ＷＬＡＮ、ＰＴＳＮまたは種々の他の有線もしくはワイヤレスネットワーク）によって結合された複数のコンピュータシステムは、お互いに協働して本発明を実現するための命令シーケンスを実施してもよい。

【００４３】

本明細書で記述されるモジュールは、本明細書に記述されたステップを実行するか処理するために、一つ以上のコンピュータ可読媒体に具現化されるか、一つ以上のプロセッサと組み合わせられる可能性がある。

【００４４】

コンピュータシステムは、通信リンクおよび通信インターフェイスを通して、一つ以上のプログラム（即ち、アプリケーションコード）を含むメッセージ、データ、情報および命令を送受信してもよい。受信されたプログラムコードは、実行用のディスクドライブコンポーネントもしくは他の幾つかの不揮発性格納コンポーネントに受信され、および／もしくは格納されると、プロセッサによって実行されてもよい。

【００４５】

適用可能な場合、本開示によって提供された種々の実施形態は、ハードウェア、ソフトウェアもしくはハードウェアとソフトウェアの組み合わせを利用して実現されてもよい。また、適用可能な場合、本明細書で説明された種々のハードウェアコンポーネントおよび

／もしくはソフトウェアコンポーネントは、本開示の趣旨から逸脱することなく、ソフトウェア、ハードウェアおよび／もしくはその双方を含む合成コンポーネントに組み合わせられてもよい。適用可能な場合、本明細書で説明された種々のハードウェアコンポーネントおよび／もしくはソフトウェアコンポーネントは、本開示の趣旨から逸脱することなく、ソフトウェア、ハードウェアもしくはその双方を含むサブコンポーネントに分離されてもよい。さらには、適用可能な場合、ソフトウェアコンポーネントはハードウェアコンポーネントとして実装（例えば、バーチャルセキュアエレメント（ｖＳＥ）実装もしくは論理ハードウェア実装）されてもよいし、その逆であってもよいことを予期される。

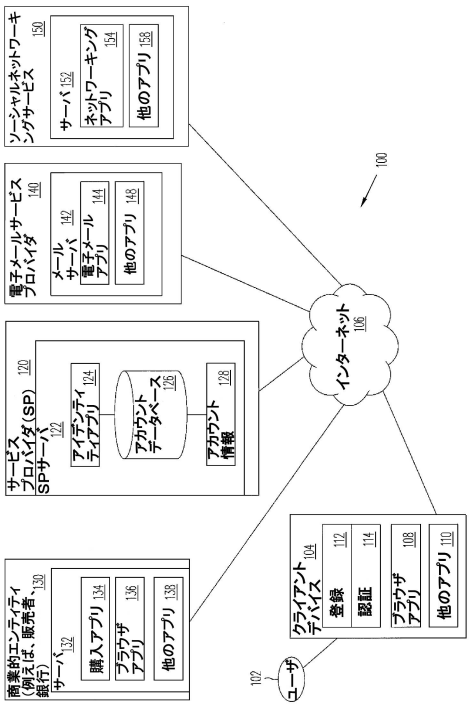
【００４６】

本開示に従う、プログラムコードおよび／もしくはデータなどのソフトウェアは、一つ以上のコンピュータ可読および実行可能媒体に格納されてもよい。本明細書で同定されるソフトウェアは、ネットワークされたおよび／もしくはその他の一つ以上の汎用もしくは専用コンピュータおよび／もしくはコンピュータシステムを利用して実現されてもよいことも、予期される。適用可能な場合、本明細書で記述された種々のステップの順序は、本明細書で記述された特徴を提供するために、変更されてもよいし、合成ステップへと組み合わせられてもよいし、および／もしくは、サブステップに分離されてもよい。

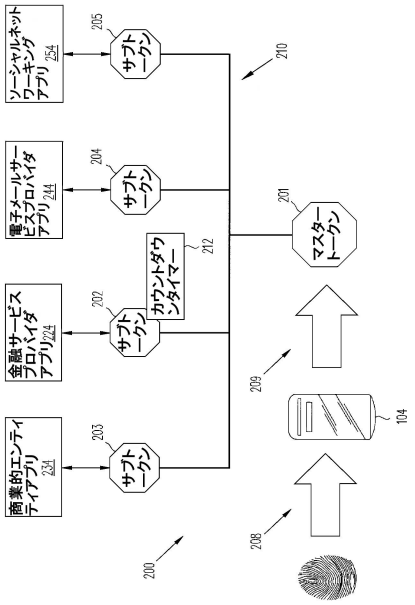
【００４７】

前述の開示は、開示された詳細な形式もしくは特定の利用分野へと本発明を限定することを意図するものではない。本明細書で明白に記述されるか暗示されるか関わらず、本発明に対して、種々の代替実施形態および／もしくは改変が本開示に照らして可能であることが予期される。本開示の種々の実施形態が記述されてきたが、当業者は、本発明の範囲から逸脱することなく、変更が形式および詳細においてなされてもよいことを認識するであろう。したがって、本発明は請求項によってのみ限定される。

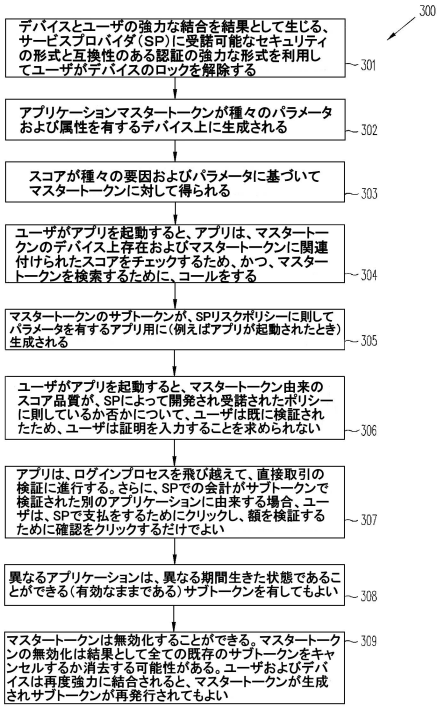
【図１】



【図２】



【図３】


300
デバイスとユーザの強力な結合を結果として生じる、サービスプロバイダ（SP）に受諾可能なセキュリティの形式と互換性のある認証の強力な形式を利用してユーザがデバイスのロックを解除する
301
アプリケーションマスタートークンが種々のパラメータおよび属性を有するデバイス上に生成される
302
スコアが種々の要因およびパラメータに基づいてマスタートークンに対して得られる
303
ユーザがアプリを起動すると、アプリは、マスタートークンのデバイス上存在およびマスタートークンに関連付けられたスコアをチェックするため、かつ、マスタートークンを検索するために、コールをする
304
マスタートークンのサブトークンが、SPリスクポリシーに則してパラメータを有するアプリ用に（例えばアプリが起動されたとき）生成される
305
ユーザがアプリを起動すると、マスタートークン由来のスコア品質が、SPによって開発され受諾されたポリシーに則しているか否かについて、ユーザは既に検証されたため、ユーザは証明を入力することを求められない
306
アプリは、ログインプロセスを飛び越えて、直接取引の検証に進行する。さらに、SPでの会計がサブトークンで検証された別のアプリケーションに由来する場合、ユーザは、SPで支払をするためにクリックし、額を検証するために確認をクリックするだけでよい
307
異なるアプリケーションは、異なる期間生きた状態であることができる（有効なままである）サブトークンを有してもよい
308
マスタートークンは無効化することができる。マスタートークンの無効化は結果として全ての既存のサブトークンをキャンセルするか消去する可能性がある。ユーザおよびデバイスは再度強力に結合されると、マスタートークンが生成されサブトークンが再発行されてもよい
309

フロントページの続き

(72)発明者　マーディカー，ウペンドラ　エス.
アメリカ合衆国，カリフォルニア州　９５１２５，サンノゼ，ハミルトン　アヴェニュー　２１４５

審査官　青柳　光代

(56)参考文献　国際公開第２０１１／００６７９０（WO，Ａ１）
米国特許出願公開第２００７／０１９２６１９（ＵＳ，Ａ１）
特表２００６－５１４５０２（ＪＰ，Ａ）
特表２０１２－５３３２４９（ＪＰ，Ａ）
特開２００３－２５６３７６（ＪＰ，Ａ）
特開２００８－０８３７５９（ＪＰ，Ａ）
米国特許出願公開第２０１０／０２１２００４（ＵＳ，Ａ１）
特開２０１１－１３３９５１（ＪＰ，Ａ）
特開２００７－０９４５４８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００　－　９９／００
Ｇ０６Ｆ　２１／３３