(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7554197号
(P7554197)

(45)発行日　令和6年9月19日(2024.9.19)

(24)登録日　令和6年9月10日(2024.9.10)

(51)国際特許分類
Ｇ０６Ｆ　21/31　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/31

請求項の数　10　（全23頁）

(21)出願番号　特願2021-546845(P2021-546845)
(86)(22)出願日　令和2年2月11日(2020.2.11)
(65)公表番号　特表2022-520226(P2022-520226A)
(43)公表日　令和4年3月29日(2022.3.29)
(86)国際出願番号　PCT/EP2020/053478
(87)国際公開番号　WO2020/165174
(87)国際公開日　令和2年8月20日(2020.8.20)
審査請求日　令和5年2月6日(2023.2.6)
(31)優先権主張番号　115304
(32)優先日　平成31年2月11日(2019.2.11)
(33)優先権主張国・地域又は機関
ポルトガル(PT)

(73)特許権者　521353805
メディセウス ダドス デ サウーヂ ソシエテ アノニム
ポルトガル国，１６００ リスボン－カルニデ，エストラーダ ド パーソ ド ルミアル
(74)代理人　100099759
弁理士　青木 篤
(74)代理人　100123582
弁理士　三橋 真二
(74)代理人　100092624
弁理士　鶴田 準一
(74)代理人　100114018
弁理士　南山 知広
(74)代理人　100153729

最終頁に続く

(54)【発明の名称】　ワンクリックログイン手順

(57)【特許請求の範囲】

【請求項１】

アプリケーションサーバで安全なユーザログイン手順を実行する方法であって、

ａ．ユーザのパーソナルコンピュータデバイス１１０のプロセッサ２４０が、ログインソフトウェアアプリケーション１００を前記パーソナルコンピュータデバイス１１０にダウンロード及びインストールするとともに匿名識別子を生成することと、

ｂ．前記パーソナルコンピュータデバイス１１０の前記プロセッサ２４０が、前記パーソナルコンピュータデバイス１１０で前記ログインソフトウェアアプリケーション１００を実行し、関心のあるアプリケーションサーバ１４０に接続し、ユーザの匿名識別子を前記アプリケーションサーバ１４０に送信することと、

ｃ．前記アプリケーションサーバ１４０のプロセッサ４４０が、前記アプリケーションサーバ１４０のユーザ登録ソフトウェアアプリケーション４７０によって、前記ユーザの匿名識別子の受信を行うとともに前記アプリケーションサーバ１４０のユーザ登録データベース４８０に前記ユーザの匿名識別子の記録を行うことと、

ｄ．前記アプリケーションサーバ１４０の前記プロセッサ４４０が、前記パーソナルコンピュータデバイス１１０からログイン又はアクセス要求を受信し、前記ログイン又はアクセス要求は、ユーザの匿名識別子を含み、前記ユーザの匿名識別子が既知の匿名識別子であることを確認し、前記アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５によって、前記ユーザにアプリケーションサーバ１４０へのアクセスを許可することと、

を備え、
ログイン手順中に、前記パーソナルコンピュータデバイス１１０の前記プロセッサ２４０は、前記パーソナルコンピュータデバイス１１０のログインソフトウェアアプリケーション１００によって前記アプリケーションサーバ１４０にアクセスするために、ユーザ定義のユーザ名の形でユーザＩＤを開示せず、システムパスワードを使用せず、ログイン手順を実行し、ユーザは匿名ＩＤによって識別され、ユーザからの手動又は生体認証のログイン入力を必要としない、方法。
【請求項２】
前記ログインソフトウェアアプリケーション１００のインストールプロセスは、ユーザ識別検証ステップを備え、前記ユーザ識別検証ステップは、
ａ．前記パーソナルコンピュータデバイス１１０の前記プロセッサ２４０が、名前及び個人識別子を入力するユーザの動作を受け入れることと、
ｂ．前記パーソナルコンピュータデバイス１１０の前記プロセッサ２４０が、前記名前及び前記個人識別子を本人確認サーバ１３０に送信することと、
ｃ．前記本人確認サーバ１３０のプロセッサ３４０が、前記本人確認サーバ１３０の本人確認ソフトウェアアプリケーション３７０によって、受信したデータと、格納された名前及び個人識別子との照合を行うことと、
ｄ．前記本人確認サーバ１３０の前記プロセッサ３４０が、一致を取得すると、前記本人確認サーバ１３０の前記本人確認ソフトウェアアプリケーション３７０によって、一致したユーザのデータから、ユーザのパーソナルコンピュータデバイス１１０のユーザの既知の連絡先の番号又は電子アドレスを読み取ることと、
ｅ．前記本人確認サーバ１３０の前記プロセッサ３４０が、前記本人確認サーバ１３０の前記本人確認ソフトウェアアプリケーション３７０によって、ユーザの前記パーソナルコンピュータデバイス１１０の一致したユーザの既知の連絡先の番号又は電子アドレスにコマンドを送信し、ユーザに確認応答のプロンプトを出すことと、
ｆ．前記パーソナルコンピュータデバイス１１０の前記プロセッサ２４０が、前記本人確認サーバ１３０に応答を送信するユーザの前記パーソナルコンピュータデバイス１１０の確認プロンプトに応答することと、
ｇ．前記本人確認サーバ１３０の前記プロセッサ３４０が、ユーザ確認を受信すると、ユーザのＩＤが確認されるとともにインストールを完了してもよいというコマンドを前記パーソナルコンピュータデバイス１１０に送信することと、
を備え、
前記本人確認サーバ１３０は、ユーザの前記ログインソフトウェアアプリケーション１００によって一度だけコンタクトすればよく、前記本人確認ソフトウェアアプリケーション３７０は、ユーザＩＤを確認し、ユーザのログイン及びアクセス装置としてのパーソナルコンピュータデバイス１１０と共に前記ログインソフトウェアアプリケーション１００を認証する、請求項１に記載の方法。
【請求項３】
前記匿名識別子は、非対称システムにおいてランダムに生成された秘密暗号鍵から導出された少なくとも１０文字の公開暗号鍵である、請求項１に記載の方法。
【請求項４】
前記匿名識別子は、任意のランダムに生成された少なくとも１０文字の文字である、請求項１に記載の方法。
【請求項５】
前記ログイン又はアクセス要求は、単一のユーザ操作である、請求項１に記載の方法。
【請求項６】
前記ログインソフトウェアアプリケーション１００から生じたログイン要求のアプリケーションサーバ１４０による受信は、有効であるとともにユーザに前記アプリケーションサーバ１４０へのログインアクセスを許可するのに十分であると見なされる、請求項１に記載の方法。

【請求項７】
前記ログイン要求の前記アプリケーションサーバ１４０による受信は、有効な匿名識別子に関連付けられているものとして本人確認サーバ１３０によって認証される、請求項６に記載の方法。
【請求項８】
パーソナルコンピュータデバイス１１０、ログインソフトウェアアプリケーション１００及び匿名識別子を備えるログイン装置であって、前記ログイン装置は、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５に匿名識別子を送信し、前記ログイン及びアクセスソフトウェアアプリケーション４７５が受信した匿名識別子と前記アプリケーションサーバ１４０のユーザ登録データベース４８０に記録された複数の匿名識別子のうちの一つとの照合を行うことのみに基づいて、ログイン手順を開始するとともにアクセスを許可されるための許可された装置として、前記ログイン及びアクセスソフトウェアアプリケーション４７５によって認識される、ログイン装置。
【請求項９】
パーソナルコンピュータデバイス１１０のプロセッサ２４０及びアプリケーションサーバ１４０のプロセッサ４４０によって実行されるときに、各プロセッサによって、
ａ．ログインソフトウェアアプリケーション１００をユーザのパーソナルコンピュータデバイス１１０にダウンロード及びインストールするとともに匿名識別子を生成することと、
ｂ．前記パーソナルコンピュータデバイス１１０で前記ログインソフトウェアアプリケーション１００を実行し、関心のあるアプリケーションサーバ１４０に接続し、ユーザ登録ソフトウェアアプリケーション４７０にユーザの匿名識別子を送信することと、
ｃ．前記ユーザ登録ソフトウェアアプリケーション４７０によって、前記アプリケーションサーバ１４０のユーザ登録データベース４８０にユーザの匿名識別子の受信及び記録を行うことと、
ｄ．前記アプリケーションサーバ１４０において、前記パーソナルコンピュータデバイス１１０の前記ログインソフトウェアアプリケーション１００からログイン又はアクセス要求を受信し、前記ログイン又はアクセス要求は、ユーザの匿名識別子を含み、前記ユーザの匿名識別子が既知の匿名識別子であることを確認し、ログイン及びアクセスソフトウェアアプリケーション４７５によって、前記ユーザにアプリケーションサーバ１４０へのアクセスを許可することと、
を備える命令を有し、
ログイン手順中に、ユーザは、ログインソフトウェアアプリケーション１００によって前記アプリケーションサーバ１４０にアクセスするために、ユーザ定義のユーザ名の形でユーザＩＤを開示せず、システムパスワードを使用せず、ログイン手順を実行し、ユーザは匿名ＩＤによって識別され、ユーザからの手動又は生体認証のログイン入力を必要としない、少なくとも一つの非一時的な機械可読記憶媒体。
【請求項１０】
パーソナルコンピュータデバイス１１０のプロセッサ２４０及び本人確認サーバ１３０のプロセッサ３４０によって実行されるときに、各プロセッサによって、
ａ．ログインソフトウェアアプリケーション１００に名前及び個人識別子を入力するユーザの動作を受け入れることと、
ｂ．前記名前及び前記個人識別子を前記ログインソフトウェアアプリケーション１００から前記本人確認サーバ１３０に送信することと、
ｃ．前記本人確認サーバ１３０において、受信したデータと、格納された名前及び個人識別子との照合を、本人確認ソフトウェアアプリケーション３７０によって行うことと、
ｄ．一致を取得すると、前記本人確認ソフトウェアアプリケーション３７０によって、一致したユーザの情報から、ユーザのパーソナルコンピュータデバイス１１０のユーザの既知の連絡先の番号又は電子アドレスを読み取ることと、
ｅ．前記本人確認サーバ１３０の前記本人確認ソフトウェアアプリケーション３７０か

らユーザの前記パーソナルコンピュータデバイス１１０の一致したユーザの既知の連絡先の番号又は電子アドレスにコマンドを送信し、ユーザに確認応答のプロンプトを出すことと、

ｆ．ユーザが、前記パーソナルコンピュータデバイス１１０の確認プロンプトに応答したときに、前記パーソナルコンピュータデバイス１１０から前記本人確認サーバ１３０の前記本人確認ソフトウェアアプリケーション３７０に応答を送信することと、

ｇ．ユーザ確認を受信すると、ユーザのＩＤが確認されるとともに前記ログインソフトウェアアプリケーション１００のインストールを前記パーソナルコンピュータデバイス１１０で完了してもよいというコマンドを、前記本人確認ソフトウェアアプリケーション３７０からユーザの前記ログインソフトウェアアプリケーション１００に送信することと、

を備える命令を有し、

前記本人確認サーバ１３０は、ユーザの前記ログインソフトウェアアプリケーション１００によって一度だけコンタクトすればよく、本人確認プロセスは、ユーザのログイン装置としてのパーソナルコンピュータデバイス１１０と共に前記ログインソフトウェアアプリケーション１００を認証する、少なくとも他の一つの非一時的な機械可読記憶媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本願は、匿名識別子によってコンピュータシステムにログインするコンピュータユーザのコンピュータシステムへのログインプロセスにおける安全な識別の分野にある。

【背景技術】

【０００２】

コンピュータネットワークへのログイン－クライアントコンピュータのユーザがサーバコンピュータによって認識されるとともにアクセスが許可されるプロセス－は、ソフトウェアアプリケーション又はオペレーティングシステムにユーザ名及びパスワードを入力することによってほぼ普遍的に実現される。これは、ユーザが名前、個人識別データ及び設定と、多くの場合は公開されているとともに通常はユーザの名前に関連付けられて選択したユーザ名と、ユーザ及びホストコンピュータだけが知るユーザ定義のユーザ記憶パスワードと、を入力する登録プロセスを必要とする。登録プロセスは、コンピュータ又はコンピュータ端末で行われ、ユーザ名及びパスワードは、ホストコンピュータによって記録される。使用中、アクセスは、適切なユーザ名及びパスワードのフィールドにユーザが入力したデータの文字列と一致するホストコンピュータによってユーザに許可され、対応するユーザ名及びパスワードは、ユーザ登録時にプレーンテキストで又は暗号化若しくはハッシュ化された形式で記録される。

【０００３】

しかしながら、コンピュータユーザカウントの急増は、インターネットの特徴である問題を引き起こした。以前は、ユーザは、通常一つの学校又は職場のコンピュータカウントを有していたが、今日では、ユーザは、数十のアカウントを管理する必要があり、多くのホストコンピュータでユーザがパスワードを頻繁に変更する必要があるため、プロセスが更に困難になっている。これにより、パスワードの書き留めのような安全でない動作が発生する。使用中の全てのパスワードを覚えておくのは困難なプロセスであり、この困難は、セキュリティを低下させる動作につながる可能性がある。

【０００４】

さらに、ユーザ名及びパスワードに基づくユーザログインシステムを使用するほとんどのコンピュータシステムでは、システム管理者は、必要に応じて、リセットのためにユーザのパスワードにアクセスする権利を有する。これは、システム管理者がユーザ名のパスワードを新しい値にリセットするとともにユーザとしてログインする機会を有し、疑いを持たないユーザのＩＤの下で不正又は違法な操作を実行する可能性があることを意味する。パスワードリセットリンクをユーザの電子メールアドレスに送信することによってシステム管理者をバイパスするパスワードリセットプロセスは、より安全であるが、ホストコ

ンピュータがユーザのＩＤを知っている必要がある。現在の時刻に関連付けられたコードを生成する電子デバイスをユーザに提供すること並びにユーザ名及びパスワードの後にこのセッションコードを入力することをユーザに要求することのようなセキュリティを強化する他の方法がある。そのようなシステムは、煩雑でコストがかかり、ホストコンピュータごとに一つの新しい電子デバイスにアクセスする必要がある。最近、スマートフォンがセッションコードジェネレーターとして使用されるようになり、それは、専用デバイスよりも大きな利点があるが、各アプリケーションサーバによって各コンピュータユーザが特定のログインソフトウェアアプリケーションを利用できるようにする必要があり、スマートフォンのアプリケーションが乱雑になる。

【０００５】

さらに、個人データの不正使用又は同意のない使用に対する懸念が高まっている。通常、ユーザが公に知られているユーザ名を使用してＩＤを明らかにし、その後、ユーザの即時の知らないうちに変更される可能性のある本質的に安全でないパスワードを使用してユーザを確認する必要があるコンピュータシステムは、個人データの保護にはひどく不適切である。

【０００６】

明らかに、上記の全ての問題に対処できる新しい安全なログインシステムが必要であり、これは、ユーザ名／パスワードの方法を完全に排除することによって行う必要がある。これは、例えば、健康、生物測定、遺伝、民族、金融、財産、資産、税金、投票、購入及び取引履歴データ等の非常に機密性の高いデータを処理するコンピュータシステムで特に望ましい。人の名前又は人の名前にまでさかのぼることができる個人ＩＤを使用しない場合にこれらのデータの全てを明確かつ安全に人に関連付ける方法で管理することは、特に有用である。

【０００７】

従来技術では、パスワードを削除することを試みたがユーザ名を削除することを試みなかったケースがある。

【０００８】

米国特許第８９５４７５８号明細書は、パスワードを、ユーザが生成したジェスチャーに置き換え、このジェスチャーは、完全なログイン式を完成させるためにログインキーに追加される文字列に数学的に変換されて解釈される。換言すれば、米国特許第８９５４７５８号明細書は、英数字のパスワードを、人間のジェスチャーによってトレースされた空間内のポイントから派生したパスワードに置き換え、したがって、ホストコンピュータがユーザ名及び完全なログイン式を保存することをホストコンピュータに要求する。

【０００９】

米国特許第９２６４４２３号明細書は、ユーザの携帯電話のようなユーザの事前登録された通信デバイスに別のコンピュータ又は端末で開始されたユーザのログイン要求を受け入れるか拒否するかを示すプロンプトを送信することにより、パスワードレスログインを許可する。プロンプトへの応答はログイン権限サーバに送信され、ログイン権限サーバは、アクセスを許可又は拒否するためにユーザの応答をアプリケーションサーバに送信する。これは、複雑なシステムであり、四つの異なるコンピュータ：ユーザセッションが開始されるユーザのクライアントデバイス、ユーザのログイン手順の一部としてユーザが編集可能なフィールドを介してクライアントのユーザ識別子を受信するアプリケーションサーバ、アプリケーションサーバのユーザ認証要求を受信するログインオーソリティサーバ及びログイン要求を受け入れるとともに肯定的又は否定的に応答するために同一のユーザがログイン権限サーバから確認要求を受信する携帯電話のようなユーザデバイスを必要とする。さらに、ユーザは、乱数とすることができる又はユーザが選択することができるユーザ識別子によって識別される。上述した方法は、ユーザ名を知るためにアプリケーションサーバを必要とし、ログインが試行されるたびに四つのコンピュータの全てが参加する必要がある。

【発明の概要】

【発明が解決しようとする課題】
【００１０】
ログイン制御がスマートフォンのようなユーザのパーソナルコンピュータデバイスに存在し、ログイン方法が従来のユーザ名又はいかなる種類のパスワード、ユーザのスマートフォン番号若しくは電子メールアドレスを使用せずにユーザのコンピュータ及び一つのアプリケーションサーバしか必要としない方法及び装置を発明した。アプリケーションサーバは、ユーザが興味のあるデータ処理を実行するために接続することを試みるサーバである。ログイン時には、ユーザは、アプリケーションサーバ又はホストコンピュータに対して匿名のままであり、匿名識別子によってのみ識別される。
【課題を解決するための手段】
【００１１】
本開示は、スマートフォン、タブレット、ラップトップコンピュータ又はパーソナルコンピュータのようなパーソナルコンピュータデバイスとして指定された、アプリケーションサーバにログインするためにユーザによって使用されるデバイスを記載する。パーソナルコンピュータデバイスは、プロセッサ、メモリ、データ記憶媒体、表示装置、キーボード、ポインティングデバイス、カメラ、マイクロフォン、モーションディテクタ等のような一つ又は複数の入力デバイス、通信サブシステム、オペレーティングシステム、電源及びソフトウェアプログラム命令を実行する手段が設けられている。パーソナルコンピュータデバイスは、プライベートネットワーク、パブリックネットワーク又はインターネットなどの通信ネットワークを介して、ホストコンピューティングシステム、企業サーバ、Ｗｅｂサーバ、クラウドコンピューティングシステム等の一つ以上のアプリケーションサーバに接続される。
【００１２】
アプリケーションサーバは、実質的には、パーソナルコンピュータデバイスと同一のコンポーネントを備えるが、その処理能力、メモリ及び記憶媒体は、容量が著しく大きく、アプリケーションサーバは、複数のユーザの同時処理に対応するために、著しく広い帯域幅を介して通信ネットワークにアクセスする。
【００１３】
ユーザの身元を検証し、ユーザのパーソナルコンピュータデバイスをユーザの制御下にあるデバイスとして認証するために、本開示の一実施形態では、アイデンティティ検証サーバが使用され、その構成要素及び容量は、上述したアプリケーションサーバのものと同様である。
【００１４】
本開示に記載された方法でデータを処理するために、参加するコンピュータは、記載されたタスクのために特別に書かれたコンピュータプログラムによってプログラムされる。パーソナルコンピュータデバイスは、少なくともログインソフトウェアアプリケーションを備え、アプリケーションサーバは、少なくともユーザ登録ソフトウェアアプリケーション並びにログイン及びアクセスソフトウェアアプリケーション（総称して、アプリケーションサーバソフトウェアアプリケーション）を備え、本人確認サーバは、少なくともユーザ本人確認ソフトウェアアプリケーションを備える。各タイプのコンピューター－パーソナルコンピュータデバイス、本人確認サーバ及びアプリケーションサーバ－の全てのソフトウェアアプリケーションは、三つのコンピュータシステムの全ての間の安全な通信を確保するために、少なくとも非対称鍵及びデジタル署名を生成する暗号化ソフトウェアも有する。
【００１５】
本発明の一態様では、ユーザ定義のユーザ名又はユーザ定義のパスワードなしで安全なユーザログイン手順を実行する方法を記載し、ユーザのパーソナルコンピュータデバイスは、ソフトウェア配布サービスに接続し、ログインソフトウェアアプリケーションをパーソナルコンピュータデバイスにダウンロード及びインストールし、ログインソフトウェアアプリケーションは、秘密鍵と、ユーザの匿名識別子としても機能する関連する公開鍵と

、を生成する。本開示では、公開鍵は、パーソナルコンピュータデバイスのログインソフトウェアアプリケーション並びにアプリケーションサーバのログイン及びアクセスソフトウェアアプリケーションによってのみ知られている。実行の際に、このログインソフトウェアアプリケーションは、アプリケーションサーバのログイン及びアクセスソフトウェアアプリケーションに接続するとともに匿名ＩＤを送信し、アプリケーションサーバは、ユーザ登録ソフトウェアアプリケーションによって匿名ＩＤをユーザ登録データベースに記録する。ユーザ登録プロセスが完了すると、ユーザは、ログインソフトウェアアプリケーションを実行し、アプリケーションサーバへのログインを要求し、匿名識別子によって自分自身を識別することができ、ログインプロセス及びユーザ匿名識別子は、アプリケーションサーバで実行されるログイン及びアクセスソフトウェアアプリケーションによって確認される。これは、ユーザによるユーザ名の入力及び作成されたことがないために存在しないシステムパスワードの入力を必要としなくなる。同様に、パーソナルコンピュータデバイスとアプリケーションサーバの間のこのようなログイン方法は、アプリケーションサーバに保存されている生体認証、指紋及び顔の画像ファイルをログイン確認用のパスワードとして使用せず、これらの要素は、実際のユーザを識別するのに非常に正確であるので、アプリケーションサーバは、匿名ユーザを簡単に再識別できる。

【００１６】

セキュリティを強化するために、パーソナルコンピュータデバイスで実行されるログインソフトウェアアプリケーションは、パーソナルコンピュータデバイスにローカルに格納されるとともにアプリケーションの操作を続行できるようにするためにユーザがロック解除することを要求するスクリーンロック装置を備えてもよい。ログインソフトウェアアプリケーションがインストールされて実行されると、ログインソフトウェアアプリケーションは、パーソナルコンピュータデバイスの許可されたユーザによって使用されていることを確認するためにユーザはスクリーンロック装置のロックを解除することを要求する。スクリーンロック装置のロック解除は、スマートフォン又はタブレットに存在するセキュリティ機能に応じて、従来のＰＩＮ番号によって行うことができる又は顔若しくは指紋の認証を介して実現できる。このようなＰＩＮ又はユーザの顔若しくは指紋のデジタル表現は、システムパスワードとしてアプリケーションサーバに送信されず、パーソナルコンピュータデバイス及びログインソフトウェアアプリケーションへのアクセスは、このローカルスクリーンロック装置を開くことによって行われる。スクリーンロック装置を開かないと、ログインソフトウェアアプリケーションを更に使用できなくなり、ログイン手順が許可されなくなる。スクリーンロック装置が正常に開かれると、ログインソフトウェアアプリケーションは、ユーザからログイン手順を引き継ぐ。

【００１７】

別の実施形態では、アプリケーションサーバが、名前のＩＤが未知であるユーザからのユーザ登録要求を信頼できるようにするために、ユーザＩＤを絶対的に確認することが重要である。これは、人口ユーザデータを既に含む別個の独立したユーザＩＤ検証サーバの機能を必要とする。このサーバは、少なくともユーザの名前及び連絡先の詳細を含む人口データによってユーザのＩＤを認証してもよい。これは、ユーザ登録時に１回だけ実行され、アプリケーションサーバがユーザの個人データ及び他の法的手続きを使用することの同意を含むユーザ設定をユーザによって入力できるようにしてもよい。この場合、ユーザは、名前と、全ての個人ＩＤを入力し、個人ＩＤは、名前、生年月日、性別、住所、郵便番号、及び、市民のＩＤ番号、パスポート番号等の正式な識別コードのような身元確認を容易にするために要求される。有利には、これらのデータは、パーソナルコンピュータデバイスを使用してユーザのＩＤカード又は運転免許証を写真撮影するとともに関心のあるデータを自動的かつ確実に取得するためにパーソナルコンピュータデバイスの文字認識ソフトウェアを使用することによって取得することができる。次に、名前及び個人ＩＤは、パーソナルコンピュータデバイスのログインソフトウェアアプリケーションによってユーザＩＤ検証サーバに送信され、ユーザＩＤ検証ソフトウェアアプリケーションは、データベースに保存されている特定の個人の個人記録を検索するためにこれらの個人ＩＤを使用

し、個人記録を見つけると、その人の既知の携帯電話番号又は電子メールアドレスを読み取る。有用な身元確認サーバは、国民身分証明書又は運転免許部門の公式政府データベース及び携帯電話事業者又は銀行のユーザデータベースを有する。受信した個人ＩＤとデータベースの個人記録との一致を見つけると、ユーザＩＤ検証サーバは、メッセージを作成することによってコマンドをユーザの既知の携帯電話番号に送信する又は既知の電子メールアカウントに電子メール若しくは進行中の新規ユーザ登録手順を認識するとともにその責を担うユーザによる確認応答を促す他の種類の電子メールを送信する。肯定応答を受信すると、ユーザのＩＤが確認され、ユーザのパーソナルコンピュータデバイスは、当該ユーザのログイン及びアクセスデバイスとして認証され、本人確認サーバのＩＤ検証ソフトウェアアプリケーションは、パーソナルコンピュータデバイスへのインストールを完了するとともに操作可能になることを許可されているログインソフトウェアアプリケーションにコマンドを送信する。この認証プロセスでは、ユーザのログインソフトウェアアプリケーションは、ユーザＩＤ検証ソフトウェアアプリケーションから本人確認サーバに一度だけ接続すればよく、ユーザＩＤ検証ソフトウェアアプリケーションは、ユーザのＩＤを検証し、ユーザのログイン及びアクセスデバイスとしてのパーソナルコンピュータデバイスと共にログインソフトウェアアプリケーションを認証する。

【００１８】

認証プロセスは、ユーザのパーソナルコンピュータデバイスが有効なログイン及びアクセスデバイスであることを確認し、アプリケーションサーバへのログインは、他のユーザの介入なしにパーソナルコンピュータデバイスのログインソフトウェアアプリケーションによってのみ実行される。ユーザは、インストールを完了するためにログインソフトウェアアプリケーションにキー入力する必要があるユーザの既知のアドレスへの確認コードの郵送のようにユーザのＩＤを完全に確認するために又は直接確認のための検証センターに物理的に直接出現するために他の手順を使用してもよい。州が提供する安全なＩＤ認証方法も有用である。

【００１９】

一実施形態では、匿名識別子は、暗号化された形式で本人確認サーバに送信され、ユーザの名前及び個人識別子とともに記録される。 この場合、後日正当な必要が生じた場合に、ユーザを再識別するために本人確認サーバを使用することができる。

【００２０】

その後にアプリケーションサーバへのログインを試行すると、ほとんどの実施形態では、ログインソフトウェアアプリケーションは、ユーザ名、個人識別子、パスワード、又は、ユーザの既知のＩＤを回復するために使用できるエレメントを送信しないことに留意すべきである。これは、データを取得する必要があるが名前でユーザを識別できるようにすることなく又はユーザの再識別を可能にする個人ＩＤを受信することなくデータを取得する場合に、貴重で機密性の高い個人データの処理に有用である。

【００２１】

インストールプロセス中に、パーソナルコンピュータデバイスのログインソフトウェアアプリケーションに含まれる暗号化キーソフトウェアプログラムは、Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ ａｎｄ Ａｄｌｅｍａｎ（ＲＳＡ）によって開発された既知の方法、又は、より好ましくは、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）の既知の方法を使用して暗号鍵の対を生成し、両方とも非対称暗号方法である。暗号鍵の各対は、秘密鍵及び公開鍵を備え、その使用は、暗号化コミュニティで広く知られており、以降、暗号鍵又は秘密鍵及び公開鍵と称する。都合よく、公開鍵は、ユーザの匿名識別子として使用され、関心のあるアプリケーションサーバでのログイン目的でのみ使用される。実際には、各公開鍵／匿名識別子が一つのアプリケーションサーバにのみログインするのに使用できるようにするために、互いに異なる関心のあるアプリケーションサーバにできるだけ多くログインする必要のために複数対の暗号鍵を生成してもよい。「公開」と記載しているが、実際には、ユーザの公開鍵は、アプリケーションサーバのログイン及びアクセスソフトウェアアプリケーションおよびパーソナルコンピュータデバイスのログインソフトウェアアプリケ

ーションにのみに知られており、ユーザを含む他の全ての関係者に秘密のままであることに留意すべきである。これは、追加のセキュリティ機能である。その理由は、ログインソフトウェアアプリケーションがインストールされているユーザのパーソナルコンピュータデバイスでのみログインプロセスを開始できるからである。このように、公開鍵／匿名識別子は、暗号化鍵を生成するとともに従来のユーザ定義のユーザ名及びパスワードなしで関心のあるアプリケーションサーバに安全にログインするために使用されるパーソナルコンピュータデバイスを操作するユーザの有効な機密識別子である。しかしながら、匿名識別を、暗号化公開鍵と同一にする必要はなく、実際には、他の十分に複雑な数値とすることができる。ユーザに加えて、本人確認サーバとアプリケーションサーバは、独自の暗号化キーの対を生成するとともにユーザのログインソフトウェアアプリケーションと安全に通信するためにソフトウェアを使用してもよい。

【００２２】

暗号化公開鍵でない場合、匿名識別子を、上述したように公開暗号化鍵として生成された匿名識別子と長さ及び複雑さが類似した任意のランダムに生成された番号とすることができる。

【００２３】

公開鍵／匿名識別子の重要な機能は、可能な限り一意に近い必要があることである。秘密暗号化鍵は、ログインソフトウェアアプリケーションに含まれる適切な暗号化ソフトウェアプログラムによって生成され、このプログラムは、関連する公開キーを計算する。秘密鍵（及び同一の又は同様の長さの関連する公開鍵）の少なくとも１０桁の数字は、地球上の全ての人間に一つの数字を割り当てることができるが、非常に短いので２人が乱数生成プロセスで同一の番号を受け取らないことを保証できない。少なくとも１００桁の数字によって、数字の間隔が著しく増大し、その結果、２人の異なる人物に同一の乱数が割り当てられる確率が低下し、一方、１０００桁以上の数字を使用すると、セキュリティが更に向上する。本明細書に開示される方法の現在の実装では、４０文字を表す２０バイトの１６進コードが使用され、ハッシュ番号は、２０４バイトにもなる可能性がある。更に高速なコンピュータが開発されるにつれて、それらの複雑さは将来増大する可能性がある。匿名識別子をユーザ名又はパスワードと見なすことができるが、ユーザ定義でもユーザ記憶可能でもユーザ入力でもないために、そのように見なすことができない。その長さ及び意味の欠如により、ユーザが簡単にアクセスできたとしてもユーザが簡単にコピーすること又は覚えることはほぼ不可能であるが、ユーザのパーソナルコンピュータデバイスのログインソフトウェアアプリケーションには隠されたままである。

【００２４】

匿名識別子として使用される公開鍵又はランダム番号を使用するそのようなログインプロセスは、ログインソフトウェアアプリケーションによってアプリケーションサーバのログイン及びアクセスソフトウェアアプリケーションに送信されるときに、アプリケーションサーバへのユーザログインアクセスを許可するためにアプリケーションサーバがそれらを有効かつ十分な手段であると見なすことを可能にする。

【００２５】

匿名識別子の実際の長さは、システム実装時のベストプラクティス及びＲＳＡ若しくはＥＣＤＳＡシステムの継続的な使用又は不正使用若しくは違反に対する更に安全な新しいシステムの採用によって決定される。

【００２６】

匿名識別子が一意であるとともにまだ帰属されていないことを保証する方法－可能性は低いが不可能ではない－は、匿名識別子を含むユーザ登録データベースを検索するとともに受信した新しいユーザの匿名識別子と完全に一致するものを探すための本人確認サーバによる手順を有する。一致するものが見つかると、本人確認サーバの本人確認ソフトウェアアプリケーションは、新しい秘密鍵又は新しい乱数を再生成するためにコマンドを発行してログインソフトウェアアプリケーションに送信し、その結果、新しい公開鍵／匿名識別子が生成される。本人確認サーバが、新しい匿名識別子が一意であることを確認したと

きにのみ、ログインソフトウェアアプリケーションのインストールを本人確認サーバにより終了するように指示される。

【００２７】

本願の方法を使用してコンピュータシステム及びアプリケーションサーバにログインすることにより、ユーザは、ログインソフトウェアアプリケーションでシングルクリック又はタッチすることによってログイン及びアクセス手順を開始することができ、これにより、ログイン及びアクセスソフトウェアアプリケーションへの匿名識別子の送信がトリガーされ、受信した匿名識別子のみに基づいてログインアクセスが許可される。

【００２８】

これらの操作及び設計機能により、ログインソフトウェアアプリケーションおよび匿名識別子を備えるパーソナルコンピュータデバイスは、ログイン装置となる。ログインするのは、もはやユーザではなくユーザの制御下にあるパーソナルコンピュータデバイスである。この特性は、本人確認サーバがユーザのＩＤを確認するために使用されたか否かとは無関係である。

【００２９】

更に高いセキュリティのために、デジタル署名を使用してもよい。デジタル署名は、デジタルメッセージ又はドキュメントの信頼性を検証するための数学的スキームである。有効なデジタル署名は、メッセージが既知の送信者によって作成された（ユーザが認証された）こと、送信者がメッセージの送信を否定できない（ユーザがメッセージを拒否できない）こと及びメッセージが転送中に変更されなかった（インテグリティが検証できる）こととを信じる理由を受信者に与える。既知のデジタル署名方法には、ＲＳＡベースの署名、ＤＳＡ（デジタル署名アルゴリズム）署名及びその他の方法を含み、ランダムに生成された秘密鍵と関連する公開鍵を使用する。ここで、この鍵の対を、匿名識別子の生成において上述したように生成されたものと同一にすることができる。本開示の一実施形態では、ログインソフトウェアアプリケーションは、デジタル署名ソフトウェアを備え、署名されるメッセージのコンテンツに適用されるユーザの秘密鍵の既知の数学的処理を使用して計算された、デジタル署名となるバイト配列を生成する。ここで、署名されるメッセージのコンテンツは、ユーザの公開鍵／匿名識別子である。デジタル署名及びメッセージそれ自体は、メッセージが実際にユーザのパーソナルコンピュータデバイスのログインソフトウェアアプリケーション又は他のユーザソフトウェアアプリケーションから発信されたことを確認する必要がある場合は常に、本人確認サーバ又はアプリケーションサーバに送信される。

【００３０】

受信側は、受信したデジタル署名をユーザの公開鍵を含むメッセージに変換し、それを読み取り、かつ、受信したメッセージそれ自体のコンテンツと比較することができる。一致する場合、ユーザは受信側によって認証される。同様に、本人確認サーバは、本人確認サーバの秘密鍵を使用してメッセージにデジタル署名することによってユーザのパーソナルコンピュータデバイスで秘密裏に終了するために、ログインソフトウェアアプリケーションのインストールのためのコマンドにデジタル署名し、この場合、署名メッセージはユーザの公開鍵／匿名識別子である。この実施形態では、このデジタル署名されたメッセージを受信した場合にのみ、ソフトウェアログインアプリケーションのインストールがパーソナルコンピュータデバイスで続行され、秘密裏に終了する。

【００３１】

ログインソフトウェアアプリケーションのインストールが秘密裏に完了すると、ユーザは、ログインソフトウェアアプリケーションに知られているアプリケーションサーバに接続するとともにユーザ登録手順を開始するためにログインソフトウェアアプリケーションを使用する。ここでは、デジタル署名、特に本人確認サーバによって生成されたデジタル署名が有用であり、この場合、アプリケーションサーバに送信されると、ユーザが存在すること、名前ＩＤが既に確認されていること、匿名識別子が未知であるが認証された人の有効なＩＤであること及び検証プロセスが既知の本人確認サーバによって実行されたこと

を保証する。これらの保証により、アプリケーションサーバのユーザ登録ソフトウェアアプリケーションは、ユーザの匿名識別子の下でユーザ登録データベースにユーザを記録できる。

【００３２】

ログイン手順は匿名であるが、匿名識別子は個人の一意のコードであり、かつ、個人の制御下にあるものとして本人確認サーバによって更に認証されている可能性があるパーソナルコンピュータデバイスに匿名識別子が存在することを理解すべきである。匿名識別子は、コピー、ハッキング又は侵入が困難であり、それによって、開示された方法は非常に安全なログイン手順となる。プロバイダが本開示に記載されているログイン装置及び方法の機能を使用することを望む他の任意のソフトウェアアプリケーションにログインソフトウェアアプリケーションを含めることができることに留意されたい。

【００３３】

したがって、アプリケーションサーバが、ユーザの身元が本人確認サーバによって確認及び認証されたログインソフトウェアアプリケーションから発信されたログイン要求を受信すると、アプリケーションサーバは、ユーザの匿名識別子のみに基づいてログイン要求に対するアクセスを許可し、アプリケーション機能のレベルを提供し、かつ、認証されているが未知の人物であるユーザとの安全通信を行う。これは、アプリケーションサーバが機密性の高い個人データを処理する場合である。

【００３４】

ユーザの身元が本人確認サーバによって確認されていない場合、アプリケーションサーバは、ユーザの匿名識別子のみに基づいてログイン要求へのアクセスを許可することができ、これは、ユーザの名前ＩＤの絶対的な確実性を必要としない状況で適切である。これは、アプリケーションサーバがユーザの習慣、訪問、好み又は選択を追跡しようとするとともにユーザがこの情報を喜んで共有する場合である。

【００３５】

本開示に記載されたログイン手順が、サーバコンピュータでユーザセッションを開くためだけでなく、クライアントとサーバとの間で情報のやり取りが行われるたびに使用され、それによってユーザの匿名識別子を継続的に検証することができる限り、ログイン手順を、継続的なアクセス検証手順と見なすことができ、エクスプレッションログイン手順は、継続的なアクセス検証手順の意味も含む。

【００３６】

別の態様では、非一時的なコンピュータ可読記憶媒体を記載する。コンピュータ可読媒体は、実行されるときに、ソフトウェア配布サービスに接続し、ログインソフトウェアアプリケーションをダウンロードしてパーソナルコンピュータデバイスにインストールし、匿名識別子を生成し、匿名識別子をアプリケーションサーバに送信するログインソフトウェアアプリケーションを実行するようにパーソナルコンピュータデバイスのプロセッサを構成するコンピュータ実行可能命令を有する。別の命令は、匿名識別子を受信するとともにユーザ登録データベースに記録するためにアプリケーションサーバのプロセッサも構成する。匿名識別子を送信することによってアプリケーションサーバにログインするためにログインソフトウェアアプリケーションを使用すると、アプリケーションサーバのプロセッサは、受信した匿名識別子を処理し、ユーザ登録データベースのエントリの一つと照合を試行し、最後に、にアプリケーションサーバに対するログインソフトウェアアプリケーション及びユーザアクセスを許可するように構成される。

【００３７】

使用中、本開示のログイン及びアクセス方法は、コンピュータにログインするための更に便利で実用的な方法を提供するが、それは、セキュリティを低下させず、実際には、従来技術の方法と比べてセキュリティを強化する。プロセスを自動化するとともにユーザのパーソナルコンピュータデバイスに配置することにより、ユーザは、もはや複数のパスワードの記憶又は書き留めの必要がなくなり、ユーザ名で自分自身を識別する必要もなくなる。これにより、連続して入力された誤ったパスワードが多すぎるために発生するキーエ

ラー、誤ったパスワード及びロックされたアカウントが大幅に削減される。しかしながら、最も重要な利点は、ユーザがログインソフトウェアアプリケーションで接続するアプリケーションサーバを選択するだけで、マウスクリック、指タップ又はその他のポインターアクションの一つのアクションで成功裏にログインできることである。システムパスワードがない場合、匿名識別子によってログインするプロセスを引き継ぐのはパーソナルコンピュータデバイスである。ユーザのパーソナルコンピュータデバイスに存在するログインファイルが登録時にユーザによって各アプリケーションサーバに対して定義された一つ又は複数の特定のユーザ名及びパスワードを含む現在のパスワード管理システムと本開示の方法と異なることに留意されたい。従来技術のこの方法では、パーソナルコンピュータデバイスは、ユーザ定義及びユーザ入力のユーザ名及びシステムパスワードを送信することによって、関心のあるアプリケーションサーバにログインする。

【００３８】

本願の他の例示的な実施形態は、図面と併せて以下の詳細な説明をレビューした後に当業者には明らかになるであろう。

【図面の簡単な説明】

【００３９】

【図１ａ】本開示の例示的な実施形態によるログインソフトウェアアプリケーションをダウンロード及びインストールするとともに本人確認サーバでユーザのＩＤを検証するために使用されるシステムアーキテクチャのブロック図である。

【図１ｂ】本開示の例示的な実施形態によるアプリケーションサーバに安全にログインするために使用されるシステムアーキテクチャのブロック図である。

【図２】本開示の例示的な実施形態によるパーソナルコンピュータデバイスのブロック図である。

【図３】本開示の例示的な実施形態による本人確認サーバのブロック図である。

【図４】本開示の例示的な実施形態によるアプリケーションサーバのブロック図である。

【図５ａ】本開示の例示的な実施形態によるメッセージが有効であることを検証するためにメッセージにデジタル署名する方法のブロック図である。

【図５ｂ】本開示の例示的な実施形態によるメッセージが有効であることを検証するためにメッセージにデジタル署名する方法のブロック図である。

【図５ｃ】本開示の例示的な実施形態によるメッセージが有効であることを検証するためにメッセージにデジタル署名するための方法のブロック図である。

【図６】本開示の例示的な実施形態によるパーソナルコンピュータデバイスにログインソフトウェアアプリケーションをダウンロード及びインストールするための方法のフローチャートである。

【図７】本開示の例示的な実施形態によるパーソナルコンピュータデバイスがアプリケーションサーバに安全にログインするための方法のフローチャートである。

【発明を実施するための形態】

【００４０】

図面では、番号は、明細書の同様の要素及び機能を示す。

【００４１】

図１ａは、本開示のログインソフトウェアアプリケーションをダウンロード及びインストールするために必要なコンピュータキテクチャのブロック図である。これは、ユーザのパーソナルコンピュータデバイスにログインソフトウェアアプリケーションを成功裏にインストールするために必要な最初のステップである。ログインソフトウェアアプリケーション１００は、インターネット上のソフトウェア配布サービス１０５に存在する。スマートフォン、タブレット、ラップトップコンピュータ又はパーソナルコンピュータのようなパーソナルコンピュータデバイス１１０を操作するユーザは、ソフトウェア配布サービス１０５から所望のログインソフトウェアアプリケーション１００をダウンロードする。ユーザは、図６に記載された方法に従ってユーザのパーソナルコンピュータデバイス１１０にログインソフトウェアアプリケーション１００をインストールする。

【００４２】
パーソナルコンピュータデバイス１１０は、通信ネットワーク１２０を介して本人確認サーバ１３０に接続する。このサーバ１３０は、一致するユーザをユーザデータベース内で検索し、それを見つけると、ユーザのＩＤを確認し、図６のステップ６００～６３０に記載された方法に従ってログインソフトウェアアプリケーション１００の継続的なインストールを可能にする。
【００４３】
図１ｂは、本開示において新しいユーザを作成するために必要とされるコンピュータキテクチャの例のブロック図である。これは、ログインソフトウェアアプリケーション１００がインストールされた後にユーザのパーソナルコンピュータデバイスが関心のあるアプリケーションサーバにこのユーザを登録するための要求を送信する第２のステップである。 ユーザは、図７のステップ７００～７３０に記載された方法に従って通信ネットワーク１２０を介してアプリケーションサーバ１４０に接続するために、パーソナルコンピュータデバイス１１０内でログインソフトウェアアプリケーション１００を実行する。ログインソフトウェアアプリケーション１００は、オプションの認証プロセスが使用されたときに本人確認サーバによって発行された場合のユーザの匿名識別子及び本人確認データを送信する。 アプリケーションサーバ１４０は、ユーザの匿名識別子及び識別確認データを受信し、それが成功裏に検証されると、ユーザをそのユーザ登録データベースに有効な新規ユーザとして記録する。
【００４４】
図１ｂは、本開示においてアプリケーションサーバ１４０のユーザ登録データベース４８０に既に登録されているユーザのために新しいログイン手順を開始するために必要とされるコンピュータキテクチャの例のブロック図でもある。これは、新規ユーザが成功裏に登録された後にユーザのパーソナルコンピュータデバイス１１０のログインソフトウェアアプリケーション１００がログイン手順を開始するために関心のあるアプリケーションサーバ１４０に要求を送信する第３のステップである。ユーザは、図７に記載された方法に従って通信ネットワーク１２０を介してアプリケーションサーバ１４０に接続するためにユーザのパーソナルコンピュータデバイス１１０でログインソフトウェアアプリケーション１００を実行する。ログインソフトウェアアプリケーション１００は、ユーザの匿名識別子を送信する。アプリケーションサーバ１４０は、ユーザの匿名識別子を受信し、図７のステップ７６０～７９０に記載された方法に従ってユーザの匿名識別子を成功裏に検証すると、ユーザがログインするとともにアプリケーションサーバ１４０でユーザセッションを開始することを可能にする。
【００４５】
図１ａ及び１ｂは、本願の匿名ログイン手順に必要な最小限のコンピュータキテクチャの例を示す。本人確認サーバ１３０は、使用される場合、ユーザのＩＤを検証するとともにアプリケーションサーバ１４０に接続してログインするのに使用されるパーソナルコンピュータデバイス１１０を認証するために、一度だけ使用される。
【００４６】
図２において、例示的なパーソナルコンピュータデバイス１１０をブロック図の形で示す。この例では、パーソナルコンピュータデバイス１１０は、メインプロセッサ２４０を備え、メインプロセッサ２４０は、通信サブシステム２１０のような様々なデバイスサブシステム、キーボード、マウス又はタッチスクリーンのような入力装置２２０及びスクリーンのようなディスプレイ２３０に接続する。パーソナルコンピュータデバイス１１０が個別に識別されない他の多くのコンポーネントを有することを理解すべきである。
【００４７】
通信サブシステム２１０は、ログインソフトウェアアプリケーション１００のダウンロード及びインストール、ユーザＩＤ検証、ユーザ登録、匿名識別子の送信並びにログイン手順の開始及び終了に関与するような本開示に記載されているデータ交換を管理するようにパーソナルコンピュータデバイス１１０をソフトウェア配布サービス１０５、本人確認

サーバ１３０及びアプリケーションサーバ１４０のような他のコンピュータに接続するために使用される。

【００４８】

メインプロセッサ２４０は、データ及びプロセッサ実行可能命令２６０を格納することができる少なくとも一つのメモリ２５０に関連付けられ、実行されるときに、ログインソフトウェアアプリケーション１００をダウンロードし、ＲＳＡ又はＥＣＤＳＡ方法又は同等のものの一つに従うログインソフトウェアアプリケーション１００に含まれる暗号化ソフトウェアプログラム２８０を使用して秘密鍵及び関連する公開鍵／匿名識別子を生成するプロセッサ２４０を構成する。

【００４９】

図３において、例示的な本人確認サーバ１３０をブロック図の形で示す。この例では、本人確認サーバ１３０は、通信サブシステム３１０に接続するメインプロセッサ３４０を備える。本人確認サーバ１３０が個別に識別されない他の多くのコンポーネントを有することを理解すべきである。

【００５０】

通信サブシステム３１０は、ユーザＩＤ検証及びパーソナルコンピュータデバイス１１０認証に関与するような本開示に記載のデータ交換を管理するように本人確認サーバ１３０をパーソナルコンピュータデバイス１１０のような他のコンピュータに接続するために使用される。

【００５１】

メインプロセッサ３４０は、データ及びプロセッサ実行可能命令３６０を格納することができる少なくとも一つのメモリ３５０に関連付けられ、実行されるときに、先ず、ユーザのパーソナルコンピュータデバイスのログインソフトウェアアプリケーション１００から本人確認の要求を受信し、次に、ユーザＩＤ検証ソフトウェアアプリケーション３７０のステップを実行し、最後に、検証が成功した場合にインストールを続行するとともに成功裏に終了するためにコマンド３８０をログインソフトウェアアプリケーション１００に発行するプロセッサ３４０を構成する。

【００５２】

図４において、例示的なアプリケーションサーバ１４０をブロック図の形で示す。この例では、アプリケーションサーバ１４０は、通信サブシステム４１０に接続するメインプロセッサ４４０が設けられている。アプリケーションサーバ１４０が別に識別されない他の多くのコンポーネントを有することを理解すべきである。

【００５３】

通信サブシステム４１０は、パーソナルコンピュータデバイス１１０への接続及び匿名識別子で識別されるログインソフトウェアアプリケーション１００から送信された情報の受信に関与するような本開示に記載のデータ交換を管理するようにパーソナルコンピュータデバイス１００のような他のコンピュータに接続するために使用される。

【００５４】

メインプロセッサ４４０は、データ及びプロセッサ実行可能命令４６０を格納することができる少なくとも一つのメモリ４５０に関連付けられ、実行されるときに、パーソナルコンピュータデバイス１１０のログインソフトウェアアプリケーション１００からの要求を、最初の接続ではユーザ登録ソフトウェアアプリケーション４７０によって処理されるとともに全ての接続ではログイン及びアクセスソフトウェアアプリケーション４７５によって処理される匿名識別子の形式で受信するプロセッサ４４０を構成する。最初の接続により、ユーザ登録ソフトウェアアプリケーション４７０は、匿名識別子が既に存在するか否かをチェックし、存在しない場合、ユーザ登録データベース４８０に新しいエントリを作成する。全ての接続により、ログイン及びアクセスソフトウェアアプリケーション４７５は、受信した匿名識別子と匿名識別子を含むユーザ登録データベース４８０とを照合することによって、匿名識別子の有効性を検証する。匿名識別子が成功裏に一致した場合、プロセッサ４４０は、ログインソフトウェアアプリケーション１００へのログインアクセ

スを許可するとともにユーザセッション４９０を開くようにアプリケーションサーバ１４０で構成される。

【００５５】

図５ａ、図５ｂ及び図５Ｃに、メッセージにデジタル署名して検証するための本開示の方法のブロック形式の例を示す。この場合、署名されるメッセージは、匿名の識別子である。

【００５６】

図５ａにおいて、パーソナルコンピュータデバイス１１０のログインソフトウェアアプリケーション１００は、デジタル署名された匿名識別子メッセージ５２０を生成するようにデジタル署名アルゴリズムのような既知の方法を使用して匿名識別子を含むメッセージ５１０にデジタル署名するために秘密暗号鍵５００を使用する。

【００５７】

図５ｂにおいて、パーソナルコンピュータデバイス１１０のログインソフトウェアアプリケーション１００は、通信ネットワーク１２０を使用して、デジタル署名された匿名識別子メッセージ５２０及び匿名識別子メッセージ５１０をアプリケーションサーバ１４０に送信する。

【００５８】

図５ｃにおいて、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５に含まれるデジタル署名ソフトウェアは、デジタル署名された匿名識別子メッセージ５２０及び匿名識別子メッセージ５１０を受信し、デジタル署名アルゴリズムのような既知の方法を使用して、デジタル署名された匿名識別子メッセージ５２０を処理し、処理の結果と、匿名識別子５１０を含むメッセージとを比較する。二つの表現が等しい場合、アプリケーションサーバ１４０は、ログイン又はアクセス要求が匿名識別子によって識別されるユーザから発信されたという保証を有する。

【００５９】

図６において、ログインソフトウェアアプリケーション１００をダウンロードし、ユーザの身元を確認し、それをパーソナルコンピュータデバイス１１０に成功裏にインストールするための本開示の方法のフローチャート形式の例を示す。

【００６０】

ステップ６００において、ユーザは、スマートフォン又はタブレットのようなパーソナルコンピュータデバイス１１０を操作し、それをＡｐｐ　Ｓｔｏｒｅ、Ｇｏｏｇｌｅ（登録商標）Ｐｌａｙ又はソフトウェア配布ウェブサーバのようなソフトウェア配布サービス１０５に向け、所望のログインソフトウェアアプリケーション１００をダウンロードする。パーソナルコンピュータを使用する場合、ユーザは、ソフトウェア配布ウェブサーバ１０５にアクセスし、所望のログインソフトウェアアプリケーション１００をダウンロードする。ユーザは、パーソナルコンピュータデバイス１１０へのログインソフトウェアアプリケーション１００のインストールを開始する。

【００６１】

インストールプロセスにおいて、ログインソフトウェアアプリケーション１００は、４桁、６桁又はそれを超える数字又は英数字のＰＩＮ、顔又は指紋の写真、パーソナルコンピュータデバイス１１０に存在するバイオメトリック認識機能の他の手段の使用のようなスクリーンロック装置のコードを入力するようにユーザに要求する。このスクリーンロックコード及びデバイスは、パーソナルコンピュータデバイス１１０に残り、そのデジタル表現は、本人確認サーバ１３０又はアプリケーションサーバ１４０のような外部パーティに送信されない。これは、ローカルに保存されたコードである。この実施形態は、機密性の高い個人データの処理を含むアプリケーションにおいて特に有用であり、この場合、パーソナルコンピュータデバイス１１０を不正アクセス及びログイン装置としての不正使用から保護することが重要である。

【００６２】

他の実施形態では、特に企業システムでは、ユーザを知る必要があり、この場合、アプ

リケーションサーバ１４０は、ユーザを組織の有効なメンバーとして認識することができるようにするために、ログインソフトウェアアプリケーション１００のインストールは、ユーザ登録時に送信することができる名前、ユーザ名、個人ＩＤ、好み及び他の関心のある情報を入力するユーザを含む。現在のログインシステムとの違いは、パスワードがユーザによって生成されないこと又はパスワードが企業アプリケーションサーバ１４０に格納されないことである。全ての実施形態において、ログインは、ユーザがログインソフトウェアアプリケーション１００上で少なくともスクリーンロックデバイスを開くとともに関心のあるアプリケーションサーバ１４０のログインボタンの選択及びクリック又はタッチすることによって実現される。

【００６３】

ステップ６１０は、ユーザＩＤを絶対的に確認するとともにログインソフトウェアアプリケーション１００及びパーソナルコンピュータデバイス１１０を認証する必要がある一実施形態の一態様を記載する。必要でない場合、動作はステップ６３５に進む。必要な場合、ログインソフトウェアアプリケーション１００は、現在の新規ユーザが既に知られているために本人確認のデータベースに記録されている可能性が高い大量の個人データを含む本人確認サーバ１３０に接続する。ユーザの名前及び個人ＩＤを受信すると、本人確認サーバ１３０の本人確認ソフトウェアアプリケーション３７０は、それ自体のデータベース内で同一のユーザを見つけるためにユーザの身元詳細を使用する。それを見つけると、本人確認ソフトウェアアプリケーション３７０は、ユーザの携帯電話番号、電子メールアドレス又は他の電子アドレスのような見つかったユーザレコードの連絡先の詳細を読み取り、携帯電話にテキストメッセージを送信する又はユーザの電子メールに電子メールメッセージを送信し、名前及び新しいユーザ登録手順の開始者であるか否かを確認するように所有者に要求する。この確認は、パーソナルコンピュータデバイス１１０のスクリーンに表示されるリンクの単なるクリック又はタッチのように簡単にすることができる。このリンクをクリックすると、既知のスマートフォン、タブレット又はコンピュータのパーソナルコンピュータデバイス１１０上で、受信した情報をユーザが実際に確認した情報が本人確認サーバ１３０に返送される。確認は、テキストメッセージ又は電子メールに数値コードを含めることによって更に安全にすることができ、その後、ユーザは、ログインソフトウェアアプリケーション１００に手動で入力するように要求され、これは、銀行及び州機関によって使用される非常に安全な手順である。ユーザがその応答を入力し、ログインソフトウェアアプリケーション１００がそれを送信した後、ログインソフトウェアアプリケーション１００は、本人確認サーバ１３０による応答を待機する。

【００６４】

ステップ６２０において、本人確認ソフトウェアアプリケーション３７０は、ユーザから受信された又は受信されなかった応答を処理する。ユーザ入力－肯定的又は否定的－に基づく本人確認ソフトウェアアプリケーション３７０による決定を行うことができる又は本人確認サーバ１３０で実行される本人確認ソフトウェアアプリケーション３７０に含まれるタイマーによってカウントされる一定時間後、例えば、６０秒後に応答がない場合に否定的であると判断する。

【００６５】

ユーザの応答が否定的である場合又は応答がなかった場合、ステップ６２５において、本人確認ソフトウェアアプリケーション３７０は、ユーザのパーソナルコンピュータデバイス１１０のログインソフトウェアアプリケーション１００が待機していたコマンドを送信し、この場合、コマンドは、ユーザのパーソナルコンピュータデバイス１１０へのログインソフトウェアアプリケーション１００のインストールを停止するためのものである。

【００６６】

ユーザ応答が肯定的であるとともに事前設定された時間内に受信された場合、ステップ６３０において、本人確認ソフトウェアアプリケーション３７０は、ユーザ本人確認データ（タイムスタンプ、確認番号、本人確認サーバ１３０の名前及びアドレス）及びコマンドを、インストールを続行することを可能にするログインソフトウェアアプリケーション

１００に送信する。両方とも、ログインソフトウェアアプリケーション１００によって記録される。

【００６７】

ステップ６３５において、ログインソフトウェアアプリケーション１００は、暗号化ソフトウェアプログラム２８０を使用して、ユーザの暗号化秘密鍵及び公開鍵／匿名識別子を生成する。

【００６８】

ステップ６４０において、ログインソフトウェアアプリケーション１００は、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５に接続し、匿名識別子によって識別されるユーザのために、新しいユーザ登録手順を要求する。コマンドが送信された後、ログインソフトウェアアプリケーション１００は、アプリケーションサーバ１４０による応答を待機する。

【００６９】

ステップ６５０において、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５は、要求がログインソフトウェアアプリケーション１００の本物のコピー及び有効なインストールからのものであるかどうかをテストし、これは既知の暗号化方法によって実現される。

【００７０】

テストが成功しなかった場合、ステップ６５５において、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５は、新しいユーザ登録手順の要求を拒否し、動作を終了するコマンドをログインソフトウェアアプリケーション１００に送信する。テストが成功した場合、ステップ６６０において、ログイン及びアクセスソフトウェアアプリケーション４７５は、動作を継続するとともに必要な場合のユーザの暗号化公開鍵／匿名識別子及びユーザＩＤ検証データをアプリケーションサーバ１４０に送信するコマンドをログインソフトウェアアプリケーション１００に送信する。

【００７１】

ステップ６７０において、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５は、必要な場合の送信された暗号化公開鍵／匿名識別子及びユーザ識別確認データをログインソフトウェアアプリケーション１００から受信し、ユーザ登録ソフトウェアアプリケーション４７０によって、ユーザ登録データベース４８０の新しいユーザを作成する。

【００７２】

ステップ６８０において、アプリケーションサーバ１４０による新しいユーザの記録が成功すると、ログイン及びアクセスソフトウェアアプリケーション４７５によって送信されたコマンドがログインソフトウェアアプリケーション１００に送信され、ログインソフトウェアアプリケーションのインストールが成功裏に終了したと記録できることを通知する。ログインソフトウェアアプリケーション１００は、ログイン操作についてユーザを確認するとともにログイン装置としてのパーソナルコンピュータデバイス１１０と共にソフトウェアログインアプリケーション１００を認証したコンピュータシステムとして、アプリケーションサーバ１４０の名前を記録する。この時点までに成功裏にインストールされたログインソフトウェアアプリケーション１００のみが、着信ログイン要求を受信する関心のあるアプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５によって認識される。これに失敗すると、もはやアプリケーションサーバ１４０によるログイン試行が許可されない。

【００７３】

図７において、ログインソフトウェアアプリケーション１００がユーザのパーソナルコンピュータデバイス１１０に成功裏にインストールされた後にユーザ名又はパスワードなしで匿名識別子によりアプリケーションサーバ１４０にログインするための本開示の方法のフローチャート形式の例を示す。

【００７４】

ステップ７００において、ユーザは、パーソナルコンピュータデバイス１１０のログインソフトウェアアプリケーション１００を実行し、ステップ６００で以前に定義されたスクリーンロック装置のロックを解除するように促される。

【００７５】

ステップ７１０において、パーソナルコンピュータデバイス１１０のログインソフトウェアアプリケーション１００は、スクリーンロック装置へのロック解除入力をテストし、それが有効であるか無効であるかを判定する。有効なエントリは、ログインソフトウェアアプリケーション１００のインストール時に定義されたＰＩＮと一致する入力されたＰＩＮ又はパーソナルコンピュータデバイス１１０の生体認証機能によって認識されるユーザの顔又は指紋である。

【００７６】

ステップ７１５でスクリーンロック装置へのロック解除入力が無効であると見なされた場合、ログインソフトウェアアプリケーション１００は、ユーザに対する継続的な動作を拒否する。ステップ７２０において有効であるとみなされる場合、継続的な動作が許可され、ユーザがログインを許可される場所が複数ある場合、ユーザは、ログインソフトウェアアプリケーション１００でログイン用のアプリケーションサーバ１４０を選択することができる。

【００７７】

ステップ７３０において、選択されたアプリケーションサーバ１４０への接続が行われ、ログイン手順が要求される。

【００７８】

ステップ７４０において、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５は、要求がログインソフトウェアアプリケーション１００の本物のコピー及び有効なインストールからのものであるか否かをテストし、これは、既知の暗号化方法によって実現される。ログインソフトウェアアプリケーション１００のコピーが正当であることを確認するために、ログイン及びアクセスソフトウェアアプリケーション４７５は、ステップ６６０及び６７０でログインソフトウェアアプリケーション１００に送信されたコマンドを照会し、それが存在するか否か及び最初に発行されたものと同一であるか否かを確認してもよい。

【００７９】

テストが成功しなかった場合、ステップ７４５において、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５は、ログインアクセスを拒否し、動作を終了するコマンドをログインソフトウェアアプリケーション１００に送信する。ログインソフトウェアアプリケーション１００及びパーソナルコンピュータデバイス１１０の識別詳細及び他の識別詳細を、アプリケーションサーバ１４０によってセキュリティログファイルに記録してもよい。

【００８０】

テストが成功した場合、ステップ７５０において、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５は、ユーザログイン手順を続行することを許可し、ユーザの公開鍵／匿名識別子を送信するためにログインソフトウェアアプリケーション１００にその旨のコマンドを送信する。

【００８１】

ステップ７６０において、アプリケーションサーバ１４０のログイン及びアクセスソフトウェアアプリケーション４７５は、公開鍵／匿名識別子を受信し、一致する匿名識別子を探すためにユーザ登録データベース４８０を検索する。ステップ７７０において、アプリケーションサーバ１４０内のログイン及びアクセスソフトウェアアプリケーション４７５は、一致が見つかったか否かをテストする。

【００８２】

ステップ７７５で一致が見つからない場合、ログイン及びアクセスソフトウェアアプリケーション４７５は、ユーザのログインソフトウェアアプリケーション１００へのログイ

ンアクセスを拒否する。ステップ７８０で一致が見つかった場合、ログイン及びアクセスソフトウェアアプリケーション４７５は、ユーザのログインソフトウェアアプリケーション１００へのログインアクセスを許可する。ステップ７９０において、ユーザセッションを、パーソナルコンピュータデバイス１１０又はアプリケーションサーバ１４０に存在するこれら又は他のソフトウェアアプリケーションを使用してアプリケーションサーバ１４０で開始する。ユーザセッションは、ユーザがログインソフトウェアアプリケーション１００若しくはアプリケーションサーバ１４０でログアウトコマンドを発行するとき又はログインソフトウェアアプリケーション１００若しくはログイン及びアクセスソフトウェアアプリケーション４７５の事前設定されたタイムアウトデバイスが所定の非活動期間の後にトリガーされた場合、ステップ７９５で終了する。

【００８３】

本発明は、ユーザがワンクリック又はワンタッチでアプリケーションサーバに安全にログインすることを可能にし、本明細書の好ましい実施形態では、ユーザ名又はユーザ記憶可能なユーザ名がなく、識別情報が開示されず、パスワードが存在しないが、ユーザはユーザの匿名識別子によって確実に識別及び認証される。

【００８４】

本発明の例示的な実施形態の前述の説明において、開示を合理化するとともに様々な発明の態様の一つ以上の理解を助けるために本発明の様々な特徴を時々単一の実施形態、図又はその説明にグループ分けしていることを理解すべきである。しかしながら、この開示方法は、特許請求の範囲の発明が各請求項に明示的に記載されているよりも多くの特徴を必要とするという意図を反映していると解釈されるべきではない。 むしろ、本発明の態様は、上述した単一の開示された実施形態の全ての特徴よりも少ないものにあり、本明細書に記載の各実施形態は、複数の本発明の特徴を有してもよい。

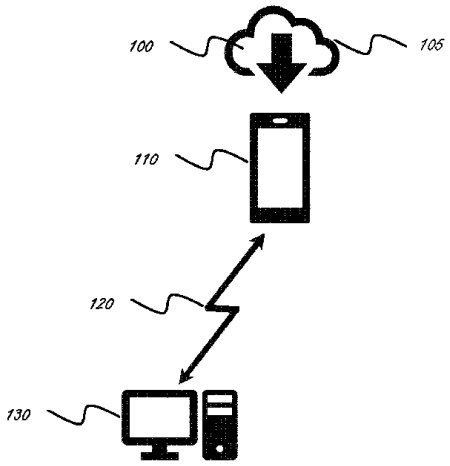
【００８５】

本発明は、その実施形態を参照して特に示されるとともに説明されてきたが、本発明の精神及び範囲から逸脱することなく形態及び詳細における他の様々な変更を行うことができることが当業者によって理解されるであろう。

【図面】

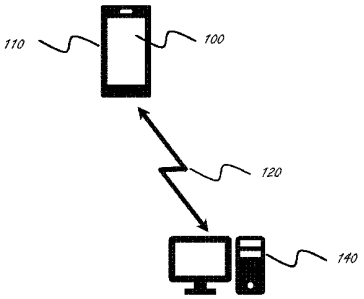
【図１ａ】

Fig. 1a



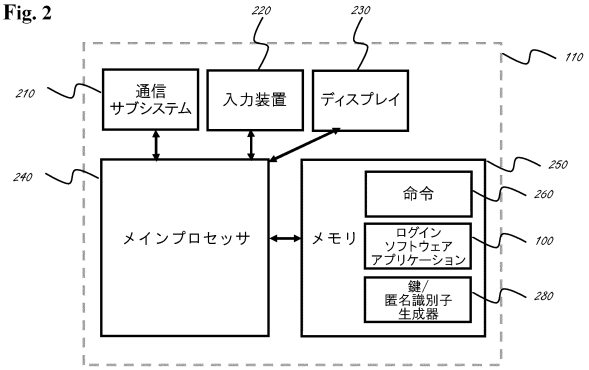
【図１ｂ】

Fig. 1b



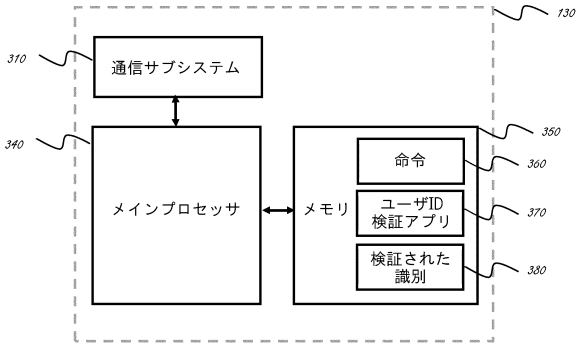
【図２】

Fig. 2



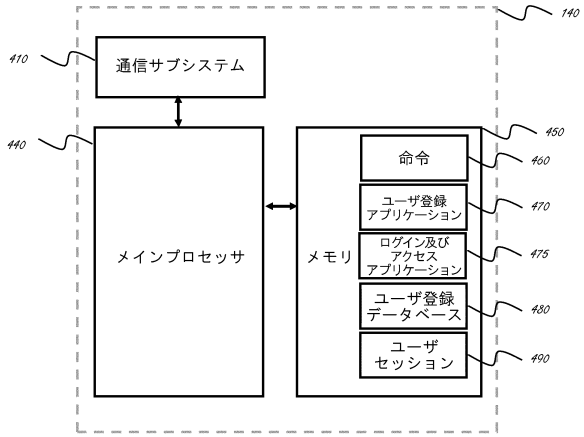
【図３】

Fig. 3



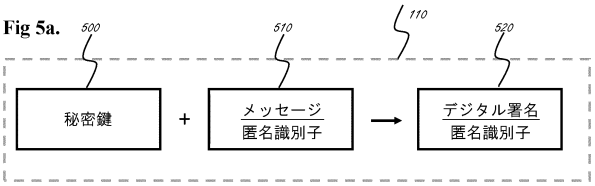
【図４】

Fig. 4



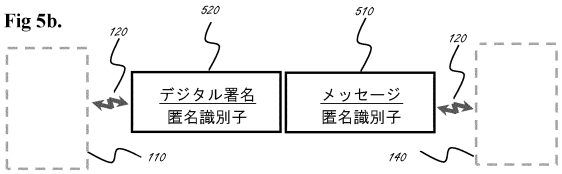
【図５ａ】

Fig 5a.



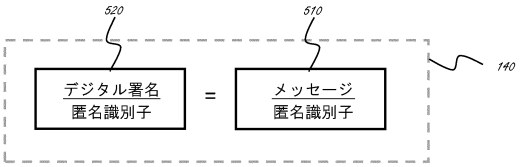
【図５ｂ】

Fig 5b.



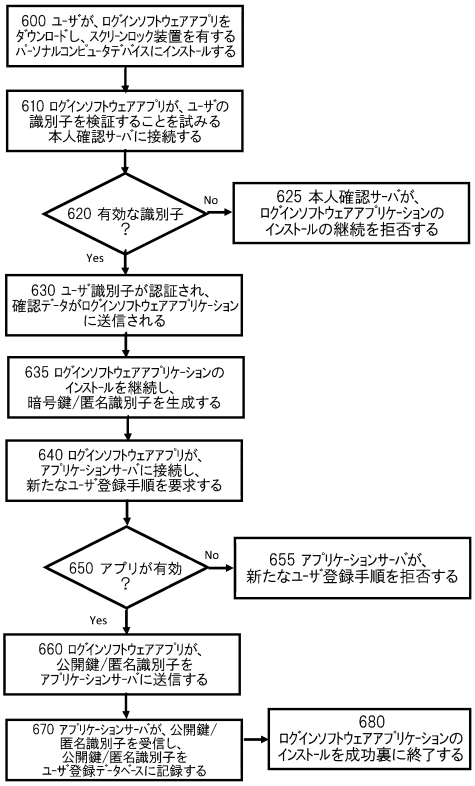
【図５ｃ】

Fig. 5c



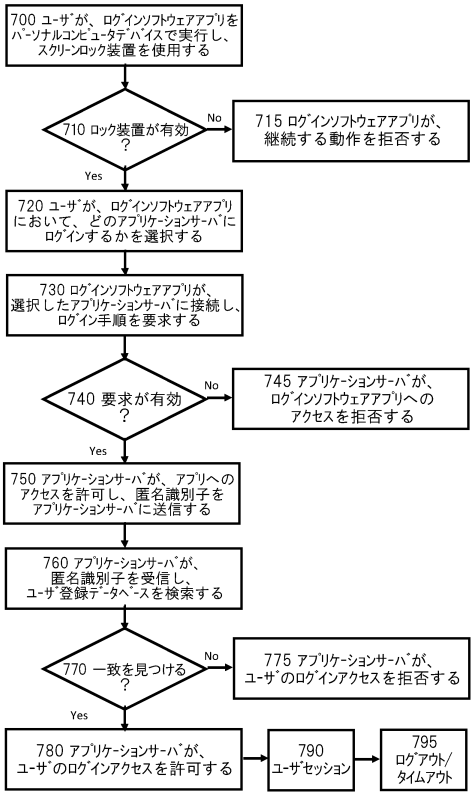
【図６】

Fig. 6



【図７】

Fig.7



フロントページの続き

弁理士　森本 有一
(72)発明者　ペテル ビラックス
ポルトガル国，１６４９－０３８ リスボン，エストラーダ ド パーソ ド ルミアル，カンプス ド ルミアル，エディフィシオ エレ
(72)発明者　ヒカルド ロウラ
ポルトガル国，１６００ リスボン－カルニデ，エストラーダ ド パーソ ド ルミアル，セー／オー メディセウス ダドス デ サウーデ ソシエテ アノニム

審査官　岸野 徹
(56)参考文献　特開２０１２－１２３５５２（ＪＰ，Ａ）
米国特許出願公開第２０１６／０１０５２９０（ＵＳ，Ａ１）
特開２０１３－１６１１２３（ＪＰ，Ａ）
特開２０１８－０３２２３５（ＪＰ，Ａ）
国際公開第２０１７／２０７３１６（WO，Ａ１）
特表２０１９－５２４０１６（ＪＰ，Ａ）
特開２０１２－００３６４８（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１