(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6689828号
(P6689828)
(45)発行日　令和2年4月28日(2020.4.28)　(24)登録日　令和2年4月10日(2020.4.10)

(51)Int.Cl.		F I		
G06F 21/33	(2013.01)	G06F	21/33	350
G09C 1/00	(2006.01)	G09C	1/00	640E
H04L 9/32	(2006.01)	H04L	9/00	675D
H04L 9/08	(2006.01)	H04L	9/00	601B
H04L 12/66	(2006.01)	H04L	12/66	B

請求項の数 3　(全 19 頁)

(21)出願番号　特願2017-514840(P2017-514840)
(86)(22)出願日　平成27年9月16日(2015.9.16)
(65)公表番号　特表2017-535837(P2017-535837A)
(43)公表日　平成29年11月30日(2017.11.30)
(86)国際出願番号　PCT/US2015/050348
(87)国際公開番号　WO2016/044373
(87)国際公開日　平成28年3月24日(2016.3.24)
審査請求日　平成30年9月14日(2018.9.14)
(31)優先権主張番号　14/487,992
(32)優先日　平成26年9月16日(2014.9.16)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　516329587
ノック　ノック　ラブズ,　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　９４３０３　パロ　アルト　ジェン　ロード　２１００　スイート　１０５
(74)代理人　100094569
弁理士　田中　伸一郎
(74)代理人　100088694
弁理士　弟子丸　健
(74)代理人　100103610
弁理士　▲吉▼田　和彦
(74)代理人　100067013
弁理士　大塚　文昭

最終頁に続く

(54)【発明の名称】認証サービスをネットワークアーキテクチャ内に統合するためのシステム及び方法

(57)【特許請求の範囲】
【請求項１】
システムであって、
内部ネットワークのためのネットワークセキュリティサービスを提供するためのネットワークセキュリティインフラストラクチャと、
前記既存のネットワークセキュリティインフラストラクチャに通信可能に結合される認証サーバと、
ユーザを認証するための、複数の認証デバイスが結合された認証クライアントを有するクライアントデバイスであって、前記認証クライアントが、前記認証サーバとの通信チャネルを確立し、前記認証デバイスのうちの１つ以上を前記認証サーバに登録するように構成され、前記認証デバイスが、登録に続いて、前記認証サーバによるオンライン認証を実行するために使用可能である、クライアントデバイスと、を備え、
前記認証クライアントが、前記内部ネットワークへのアクセスの獲得を試みることに応答して、前記登録された認証デバイスのうちの１つ以上を使用して、前記認証サーバによって前記ユーザを認証し、
前記認証サーバが、認証成功に応答して、暗号データ構造を前記クライアントデバイスに提供し、前記暗号データ構造が、前記認証サーバによって保持されるルート証明書の秘密鍵によって署名されたデジタル証明書及び前記デジタル証明書が有効である時間の長さを示すタイムスタンプを備え、前記デジタル証明書が、前記認証サーバによって生成された公開鍵／秘密鍵ペアを備え、

前記クライアントデバイスが、前記暗号データ構造を使用して、前記ネットワークセキュリティインフラストラクチャによって認証し、前記クライアントデバイスが、署名されたチャレンジを生成するために前記公開鍵／秘密鍵ペアの秘密鍵を用いて前記ネットワークセキュリティインフラストラクチャによって提供されるチャレンジに署名し、前記クライアントデバイスがさらに、ネットワークセキュリティインフラストラクチャへ前記暗号データ構造とともに前記署名されたチャレンジを送信し、

前記ネットワークセキュリティインフラストラクチャが、前記認証サーバによって確立された信用関係に基づいて、前記暗号データ構造を検証し、前記信用関係が、前記ルート証明書を使用して生成されたセキュリティインフラストラクチャ信用署名を含み、前記ネットワークセキュリティインフラストラクチャが、前記認証サーバによって提供される前記ルート証明書の公開鍵を使用して、前記デジタル証明書の前記署名を検証し、また、前記公開鍵／秘密鍵ペアの公開鍵を使用して前記署名されたチャレンジを検証し、前記暗号データ構造及び前記署名されたチャレンジを検証すると、前記ネットワークセキュリティインフラストラクチャが、前記クライアントデバイスによる前記内部ネットワークへのアクセスを提供する、システム。

【請求項２】

前記ネットワークセキュリティインフラストラクチャが、Ｍｉｃｒｏｓｏｆｔ　Ａｃｔｉｖｅ　Ｄｉｒｅｃｔｏｒｙ又はＫｅｒｂｅｒｏｓインフラストラクチャを備える、請求項１に記載のシステム。

【請求項３】

前記認証クライアントを前記認証サーバに結合するゲートウェイを更に備える、

請求項１に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、概して、データ処理システムの分野に関する。より具体的には、本発明は、認証サービスをネットワークアーキテクチャ内に統合するためのシステム及び方法に関する。

【背景技術】

【０００２】

システムはまた、バイオメトリックセンサを使用してネットワーク上でセキュアなユーザ認証を提供するために設計されている。そのようなシステムにおいて、認証部、及び／又は他の認証データにより生成されたスコアは、リモートサーバでユーザを認証するためにネットワークで送ることができる。例えば、米国特許出願公開第２０１１／００８２８０１号（「‘８０１出願」）は、強力な認証（例えば、個人情報の盗難及びフィッシングに対する保護）を提供する、ネットワーク上でのユーザ登録及び認証のためのフレームワーク、セキュアトランザクション（例えば、「マルウェア・イン・ザ・ブラウザ」及びトランザクションについての「マン・イン・ザ・ミドル」攻撃に対する保護）、及び、クライアント認証トークン（例えば、指紋リーダー、顔認識デバイス、スマートカード、トラステッドプラットフォームモジュールなど）の登録／管理について記載している。

【０００３】

本特許出願の譲受人は、‘８０１出願に記載された認証フレームワークに対する様々な改善を開発している。これらの改善のうちのいくつかは、本願と同じ譲受人に譲渡されている以下の組の米国特許出願に記載されており、その出願とは、第１３／７３０，７６１号、Ｑｕｅｒｙ　Ｓｙｓｔｅｍ　ａｎｄ　Ｍｅｔｈｏｄ　ｔｏ　Ｄｅｔｅｒｍｉｎｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ、第１３／７３０，７７６号、Ｓｙｓｔｅｍ　ａｎｄ　Ｍｅｔｈｏｄ　ｆｏｒ　Ｅｆｆｉｃｉｅｎｔｌｙ　Ｅｎｒｏｌｌｉｎｇ，Ｒｅｇｉｓｔｅｒｉｎｇ，ａｎｄ　Ａｕｔｈｅｎｔｉｃａｔｉｎｇ　Ｗｉｔｈ　Ｍｕｌｔｉｐｌｅ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｄｅｖｉｃｅｓ；第１３／７３０，７８０号、Ｓｙｓｔｅｍ　ａｎｄ　Ｍｅｔｈｏｄ　ｆｏｒ　Ｐｒｏｃｅｓｓｉｎｇ　Ｒａｎｄｏｍ　Ｃｈａｌｌｅｎｇ

ｅｓ Ｗｉｔｈｉｎ ａｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆｒａｍｅｗｏｒｋ；第１３／７３０，７９１号、Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｉｍｐｌｅｍｅｎｔｉｎｇ Ｐｒｉｖａｃｙ Ｃｌａｓｓｅｓ Ｗｉｔｈｉｎ ａｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆｒａｍｅｗｏｒｋ；第１３／７３０，７９５号、Ｓｙｓｔｅｍ ａｎｄ Ｍｅｔｈｏｄ ｆｏｒ Ｉｍｐｌｅｍｅｎｔｉｎｇ Ｔｒａｎｓａｃｔｉｏｎ Ｓｉｇｎａｌｉｎｇ Ｗｉｔｈｉｎ ａｎ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｆｒａｍｅｗｏｒｋ；及び第１４／２１８，５０４，Ａｄｖａｎｃｅｄ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｔｅｃｈｎｉｑｕｅｓ ａｎｄ Ａｐｐｌｉｃａｔｉｏｎｓ（以下において「‘５０４出願」）である。これらの出願は、本明細書において（「同時係属出願」）と呼ばれることがある。

【０００４】

手短に言えば、これらの同時係属出願は、ユーザが、クライアントデバイスにおいてバイオメトリックデバイス（例えば、指紋センサ）のような認証デバイス（又は認証部）によって登録する認証技術を記載している。ユーザがバイオメトリックデバイスによって登録されるとき、バイオメトリック参考データが（例えば、指をスワイプすること、写真をスナップすること、音声を録音することなどにより）捕捉される。ユーザは、その後、ネットワークを通じて１つ以上のサーバ（例えば、同時係属出願に記載されているようなセキュアなトランザクション／認証サービスを備えるウェブサイト又は他の依拠当事者）によって認証デバイスを登録／プロビジョニングし、その後、登録プロセス中に交換されるデータ（例えば、認証デバイスにプロビジョニングされる暗号鍵）を使用してそれらのサーバで認証することができる。認証されると、ユーザは、ウェブサイト又は他の依拠当事者と１つ以上のオンライントランザクションを実行することが許可される。同時係属出願に記載されたフレームワークでは、機密情報、例えば、ユーザを一意的に識別するために使用することができる指紋データ及び他のデータは、ユーザのプライバシーを保護するためにユーザの認証デバイスにローカルに保持されてもよい。

【０００５】

‘５０４出願は、複合認証部を設計するための技術と、認証保証レベルをインテリジェントに生成する技術と、非侵入型ユーザ検証を使用する技術と、認証データを新規の認証デバイスに移動する技術と、クライアントリスクデータによって認証データを増加させる技術と、認証方針を最適に適用する技術と、トラストサークルを作成してほんの少数を指名する技術と、を含む様々な付加的技術を記載している。

【０００６】

同時係属出願に記載されているリモート認証技術を活用するために依拠当事者のウェブベースの又は他のネットワーク対応のアプリケーションを増強するには、通常は、アプリケーションを認証サーバと直接統合することを必要とする。これは、依拠当事者が、同時係属出願に記載される技術によって提供される認証の柔軟性を得るために、アプリケーションを更新して認証サーバと統合するための労力を費やすことが必要になるので、このような認証の採用に対する障害をもたらす。

【０００７】

いくつかの事例において、依拠当事者は、フェデレーションソリューションと既に統合している場合があり、したがって、単純な統合の経路は、単に、オンライン認証サポートをフェデレーションソリューションに統合することである。残念なことに、この手法は、他のレガシーシステム（ＶＰＮ、Ｗｉｎｄｏｗｓ Ｋｅｒｂｅｒｏｓの展開など）に対処しておらず、該レガシーシステムは、フェデレーションプロトコルの認識が不足している（したがって、オンライン認証機能によって増大されたフェデレーションサーバによってフロントエンドになり得る）か、又は、オンライン認証機能の直接的な統合を可能にするための十分な拡張性が不足している。したがって、特定の依拠当事者アプリケーションについて解決しなければならない重要な問題は、アプリケーション自体のコードを修正することを必要とせずに、それらをオンライン認証システムに統合すること可能にする方法を見出すことである。

【０００８】
本発明のより良好な理解は、以下の図面とともに以下の詳細な説明から得ることができる。
【図面の簡単な説明】
【０００９】
【図１Ａ】セキュア認証システムアーキテクチャについての２つ異なる実施形態を示す。
【図１Ｂ】セキュア認証システムアーキテクチャについての２つ異なる実施形態を示す。
【図２】鍵が認証デバイスに登録される態様を示すトランザクション線図である。
【図３】リモート認証を示すトランザクション線図を示す。
【図４】セキュアソケットレイヤー（ＳＳＬ）仮想プライベートネットワーク（ＶＰＮ）ゲートウェイを通して、ユーザを内部ネットワークに接続するためのシステムを示す。
【図５】認証サーバをネットワークインフラストラクチャ内に統合するためのシステムの１つの実施形態を例示する。
【図６】ネットワークインフラストラクチャ内に統合された認証サーバを使用して認証を行うための方法の１つの実施形態を示す。
【図７】認証サーバをＫｅｒｂｅｒｏｓインフラストラクチャ内に統合するためのシステムの１つの実施形態を示す。
【図８】Ｋｅｒｂｅｒｏｓインフラストラクチャ内に統合された認証サーバを使用して認証を行うための方法の１つの実施形態を示す。
【図９】サーバ及び／又はクライアントのために使用されるコンピュータアーキテクチャについての１つの実施形態を示す。
【図１０】サーバ及び／又はクライアントのために使用されるコンピュータアーキテクチャについての１つの実施形態を図示する。
【発明を実施するための形態】
【００１０】
以下に説明するものは、高度な認証技術及び関連するアプリケーションを実行するための装置、方法及び機械可読媒体の実施形態である。説明を通して、説明の目的のために、多数の具体的な詳細が本発明の完全な理解を提供するために記載されている。しかしながら、本発明が、これらの具体的な詳細の一部がなくても実施され得ることは当業者にとって明らかであろう。他の例において、周知の構造及びデバイスは示されていないか、又は、本発明の基本原理を曖昧にすることを避けるためにブロック図の形態で示されている。
【００１１】
以下に説明する本発明の実施形態には、バイオメトリックモダリティ又はＰＩＮ入力などのユーザ検証機能を備えた認証デバイスが含まれる。これらのデバイスは、本明細書において、「トークン」、「認証デバイス」、又は「認証部」と呼ばれることがある。特定の実施形態は、顔認識ハードウェア／ソフトウェア（例えば、ユーザの顔を認識してユーザの眼の動きを追跡するためのカメラ及び関連するソフトウェア）にフォーカスしており、いくつかの実施形態は、例えば、指紋センサ、音声認識ハードウェア／ソフトウェア（例えば、マイクロフォン及びユーザの音声を認識するための関連するソフトウェア）、及び、光学的認識機能（例えば、ユーザの網膜をスキャンするための光学スキャナ及び関連するソフトウェア）を含む追加のバイオメトリックデバイスを利用することができる。ユーザ検証機能は、ＰＩＮ入力のような、非バイオメトリックモダリティを含んでもよい。認証部は、暗号操作及び鍵記憶のためにトラスデッドプラットフォームモジュール（ＴＰＭ）、スマートカード及びセキュア要素のようなデバイスを使用することがあり得る。
【００１２】
モバイルバイオメトリックの実装において、バイオメトリックデバイスは、依拠当事者からリモートにあってもよい。本明細書で用いるとき、「リモート」という用語は、バイオメトリックセンサが通信可能に結合されているコンピュータのセキュリティ境界の一部ではない（例えば、依拠当事者コンピュータと同じ物理的筐体内に埋め込まれていない）ことを意味する。一例として、バイオメトリックデバイスは、ネットワーク（例えば、イ

ンターネット、無線ネットワークリンクなど）を介して又はＵＳＢポートなどの周辺入力を介して依拠当事者に結合することができる。これらの条件下では、そのデバイスが依拠当事者（例えば、認証強度及び完全性保護の許容可能なレベルを提供するもの）によって認証されるものであるかどうか及び／又はハッカーがバイオメトリックデバイスを侵害したかどうか若しくは更には交換したかどうかを依拠当事者が知る方法はない可能性がある。バイオメトリックデバイスにおける信頼度は、デバイスの特定の実装形態に依存する。

【００１３】

「ローカル」という用語は、ユーザが現金自動預け払い機（ＡＴＭ）又は店舗販売時点情報管理（ＰＯＳ）小売チェックアウトの位置などの特定の位置において個人がトランザクションを完了していることを意味するために本明細書において使用される。しかしながら、以下に説明するように、ユーザを認証するために用いられる認証技術は、リモートサーバ及び／又は他のデータ処理デバイスとのネットワークを介した通信などの非位置的構成要素（non-location component）を含むことができる。更に、具体的な実施形態が（ＡＴＭや小売店など）本明細書において記載されるが、本発明の基礎原理は、トランザクションがエンドユーザによってローカルに開始される任意のシステムのコンテキスト内で実装されてもよいことに留意すべきである。

【００１４】

用語「依拠当事者」とは、本明細書において、ユーザトランザクションがそれによって試みられるエンティティ（例えば、ユーザトランザクションを実行するウェブサイト又はオンラインサービス）だけでなく、セキュアトランザクションサーバ（本明細書で説明される基礎となる認証技術を実行し得るそのエンティティの代わりに実装される」と呼ばれることがある）も指すために使用されることがある。セキュアトランザクションサーバは、所有される及び／又は依拠当事者の制御下にあってもよく、又は、事業構成の一部として依拠当事者に対してセキュアトランザクションサービスを提供する第三者の制御下にあってもよい。

【００１５】

「サーバ」という用語は、クライアントからネットワークを介してリクエストを受信し、応答として１つ以上の操作を実行し、クライアントに通常は操作の結果を含む応答を送信するハードウェアプラットフォーム上で（又は複数のハードウェアプラットフォームにわたって）実行されるソフトウェアを指すために本明細書において使用される。サーバは、クライアントに対してネットワーク「サービス」を提供する又は提供するのに役立つように、クライアントのリクエストに応答する。重要なことは、サーバが単一のコンピュータ（例えば、サーバソフトウェアを実行する単一のハードウェアデバイス）に限定されるものではなく、実際には、潜在的に複数の地理的位置にある複数のハードウェアプラットフォームにまたがってもよいということである。

例示的なオンライン認証アーキテクチャ及びトランザクション

【００１６】

図１Ａ～Ｂは、システムアーキテクチャについての２つの実施形態を示し、このシステムアーキテクチャは、認証デバイスを登録（「プロビジョニング」とも呼ばれることがある）してユーザを認証するために、クライアント側及びサーバ側の構成要素を備える。図１Ａに示す実施形態は、ウェブサイトと通信するためにウェブブラウザプラグインベースのアーキテクチャを使用し、一方、図１Ｂに示す実施形態は、ウェブブラウザを必要としない。ユーザを認証デバイスに登録すること、認証デバイスをセキュアなサーバに登録すること、及びユーザを検証することなどの、本明細書に記載の様々な技術は、これらのシステムアーキテクチャのうちの任意のものに実装されてもよい。このように、図１Ａに示すアーキテクチャは、以下で説明する実施形態のうちのいくつかの操作を説明するために使用され、一方、同じ基本原理が図１Ｂに示すシステムにおいて容易に（例えば、サーバ１３０とセキュアトランザクションサービス１０１との間の通信のための媒介としてのブラウザプラグイン１０５を取り除くことによって）実装され得る。

【００１７】

図１Ａを最初に参照すると、示している実施形態は、エンドユーザを登録して検証するために、１つ以上の認証デバイス１１０～１１２（時として、認証「トークン」又は「認証部」と当該技術分野において呼ばれることがある）を備えるクライアント１００を含む。上記のように、認証デバイス１１０～１１２は、指紋センサ、音声認識ハードウェア／ソフトウェア（例えば、ユーザの声を認識するためのマイクロフォン及び付随するソフトウェア）、顔認識ハードウェア／ソフトウェア（例えば、ユーザの顔を認識するためのカメラ及び付随するソフトウェア）、及び、光学的認識機能（例えば、ユーザの網膜をスキャンするための光学式スキャナ及び付随するソフトウェア）のようなバイオメトリックデバイス、並びに、ＰＩＮ検証のような非バイオメトリックモダリティのための支持を含んでもよい。認証デバイスは、トラステッドプラットフォームモジュール（ＴＰＭ）、スマートカード、又はセキュア要素を暗号操作及び鍵記憶のために使用してもよい。

【００１８】

認証デバイス１１０～１１２は、セキュアトランザクションサービス１０１によって露出されたインターフェース１０２（例えば、アプリケーションプログラミングインターフェース又はＡＰＩ）を介してクライアントに通信可能に結合されている。セキュアトランザクションサービス１０１は、ネットワークを介して１つ以上のセキュアトランザクションサーバ１３２～１３３と通信を行い、かつウェブブラウザ１０４のコンテキスト内で実行されるセキュアトランザクションプラグイン１０５とインターフェースするためのセキュアアプリケーションである。例示されたように、インターフェース１０２はまた、デバイス識別コードなどの認証デバイス１１０～１１２のそれぞれに関連する情報、ユーザ識別コード、認証デバイスにより保護されたユーザ登録データ（例えば、スキャンされた指紋又は他のバイオメトリックデータ）、及び本明細書に記載されたセキュア認証技術を実行するために使用される認証デバイスによりラップされた鍵を記憶するクライアント１００のセキュア記憶装置デバイス１２０に対するセキュアなアクセス権を提供することができる。例えば、以下に詳細に説明するように、固有の鍵は、認証デバイスのそれぞれに記憶され、インターネットなどのネットワークを介してサーバ１３０と通信するときに使用することができる。

【００１９】

後述するように、特定の種類のネットワークトランザクションは、ウェブサイト１３１又は他のサーバとのＨＴＴＰ又はＨＴＴＰＳトランザクションなどのセキュアトランザクションプラグイン１０５によって、サポートされる。１つの実施形態では、セキュアトランザクションプラグインは、セキュアエンタープライズ又はウェブデスティネーション１３０の内部のウェブサーバ１３１（時として、単に「サーバ１３０」と呼ばれることがある）によってウェブページのＨＴＭＬコードの中に挿入された特定のＨＴＭＬタグに応答して開始される。そのようなタグを検出することに応答して、セキュアトランザクションプラグイン１０５は、処理のために、セキュアトランザクションサービス１０１に、トランザクションを転送することができる。更に、特定の種類のトランザクション（例えば、セキュア鍵交換などの）について、セキュアトランザクションサービス１０１は、内部設置トランザクションサーバ１３２（すなわち、ウェブサイトと同じ位置に配置された）又は外部設置トランザクションサーバ１３３との直接の通信チャンネルを開くことができる。

【００２０】

セキュアトランザクションサーバ１３２～１３３は、ユーザデータ、認証デバイスデータ、鍵、及び、後述するセキュア認証トランザクションをサポートするために必要な他のセキュア情報を記憶するためにセキュアトランザクションデータベース１２０に結合される。しかし、本発明の基礎となる原理は、図１Ａに示すセキュアエンタープライズ又はウェブデスティネーション１３０内の論理的構成要素の分離を必要としないことに留意するべきである。例えば、ウェブサイト１３１とセキュアトランザクションサーバ１３２～１３３とは、単一の物理サーバ又は別個の物理サーバ内に実装されてもよい。更に、ウェブサイト１３１及びトランザクションサーバ１３２～１３３は、以下に説明する機能を実行

するための１つ以上のサーバ上で実行される統合されたソフトウェアモジュール内に実装されてもよい。

【００２１】

上記のように、発明の基礎となる原理は、図１Ａに示すブラウザベースのアーキテクチャに限定されない。図１Ｂは、スタンドアロンアプリケーション１５４が、ネットワークを介してユーザを認証するセキュアトランザクションサービス１０１によって提供される機能を利用する代替の実装を示す。１つの実施形態において、アプリケーション１５４は、以下で詳細に説明するユーザ／クライアント認証技術を実行するためのセキュアトランザクションサーバ１３２～１３３に依存する１つ以上のネットワークサービス１５１との通信セッションを確立するように設計されている。

【００２２】

図１Ａ及び図１Ｂに示された実施形態のどちらにおいても、セキュアトランザクションサーバ１３２～１３３は、次いでセキュアトランザクションサービス１０１に対してセキュアに伝送され、かつセキュア記憶装置１２０内の認証デバイスに記憶される鍵を生成することができる。更に、セキュアトランザクションサーバ１３２～１３３は、サーバ側のセキュアトランザクションデータベース１２０を管理する。

【００２３】

認証デバイスをリモートで登録すること、及び依拠当事者によって認証することと関連する特定の基本原理を図２～３について説明し、それに続いて、セキュア通信プロトコルを使用して信用を確立するための本発明の実施形態について詳細に説明する。

【００２４】

図２は、クライアントにおける認証デバイス（例えば、図１Ａ～Ｂのクライアント１００におけるデバイス１１０～１１２）を登録する（時として、認証デバイスを「プロビジョニングする」と呼ぶことがある）ための一連のトランザクションを示す。簡潔性のために、セキュアトランザクションサービス１０１とインターフェース１０２とは、認証クライアント２０１として一緒に組み合わされ、セキュアトランザクションサーバ１３２～１３３を含むセキュアエンタープライズ又はウェブデスティネーション１３０は、依拠当事者２０２として表されている。

【００２５】

認証部（例えば、指紋認証部、音声認証部など）の登録の間、認証部と関連する鍵は、認証クライアント２０１と依拠当事者２０２との間で共有される。図１Ａ～Ｂに戻って参照すると、鍵は、クライアント１００のセキュア記憶装置１２０、及びセキュアトランザクションサーバ１３２～１３３によって使用されるセキュアトランザクションデータベース１２０内に記憶されてもよい。１つの実施形態において、鍵は、セキュアトランザクションサーバ１３２～１３３のいずれかによって生成された対称鍵である。しかし、下記の別の実施形態では、非対称鍵が使用される。本実施形態では、公開鍵／秘密鍵のペアが、セキュアトランザクションサーバ１３２～１３３によって生成されてもよい。公開鍵は、次いで、セキュアトランザクションサーバ１３２～１３３によって記憶されてもよく、そして、関連する秘密鍵は、クライアントにおけるセキュア記憶装置１２０に記憶されてもよい。代替の実施形態では、鍵（複数可）が、クライアント１００において（例えば、セキュアトランザクションサーバ１３２～１３３ではなく、認証デバイス又は認証デバイスインターフェースによって）生成されてもよい。本発明の基本原理は、任意の特定の種類の鍵又は鍵の生成方法に限定されるものではない。

【００２６】

セキュア鍵プロビジョニングプロトコルが、１つの実施形態において使用されて、セキュア通信チャネルを介してクライアントと鍵を共有する。鍵プロビジョニングプロトコルの１つの例は、Ｄｙｎａｍｉｃ Ｓｙｍｍｅｔｒｉｃ Ｋｅｙ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ（ＤＳＫＰＰ）（例えば、Ｒｅｑｕｅｓｔ ｆｏｒ Ｃｏｍｍｅｎｔｓ（ＲＦＣ）６０６３を参照）である。しかしながら、本発明の基本原理は、いかなる特定の鍵プロビジョニングプロトコルにも限定されるものではない。１つの特定の実施形

態では、クライアントは、公開／秘密鍵ペアを生成して、証明鍵によって証明されてもよい公開鍵をサーバに送る。

【００２７】

図２に示す特定詳細を参照すると、登録プロセスを開始するために、依拠当事者２０２は、デバイス登録の間に認証クライアント２０１によって提示されなければならない、ランダムに生成されたチャレンジ（例えば、暗号ノンス）を生成する。ランダムチャレンジは、限られた期間について有効であり得る。それに応答して、認証クライアント２０１は、依拠当事者２０２（例えば、アウトオブバンドトランザクション）とのアウトオブバンドセキュア接続を開始し、そして、鍵プロビジョニングプロトコル（例えば、上記のＤＳＫＰＰプロトコル）を使用して依拠当事者２０２と通信する。セキュア接続を開始するために、認証クライアント２０１が、ランダムチャレンジを（場合によっては、ランダムチャレンジを介して生成された署名とともに）依拠当事者２０２に提供し戻してもよい。加えて、認証クライアント２０１は、ユーザの識別（例えば、ユーザＩＤ又は他のコード）、及び（例えば、プロビジョニングされている認証デバイス（複数可）の種類を一意的に識別する認証証明ＩＤ（ＡＡＩＤ）を使用して）登録されるプロビジョニングされるべき認証デバイス（複数可）の識別を伝送してもよい。

【００２８】

依拠当事者は、ユーザ名又はＩＤコード（例えば、ユーザアカウントデータベースの中の）によってユーザを探索し、ランダムチャレンジを検証し（例えば、署名を使用して、又は、単にランダムチャレンジを送られたものと比較して）、送られたものならば（例えば、ＡＡＩＤ）認証デバイスの認証コードを検証し、そして、ユーザ及び認証デバイス（複数可）について新規エントリをセキュアトランザクションデータベース（例えば、図１Ａ～Ｂにおけるデータベース１２０）に作成する。１つの実施形態では、依拠当事者は、それが認証のために受け取る認証デバイスのデータベースを維持する。それは、ＡＡＩＤ（又は、他の認証デバイス（複数可）のコード）によってこのデータベースに問合せることにより、プロビジョニングされている認証デバイス（複数可）が認証に対して許容可能か否かを判定してもよい。肯定の場合、次いで、それは、登録プロセスを続行することになる。

【００２９】

１つの実施形態では、依拠当事者２０２は、プロビジョニングされているそれぞれの認証デバイスに対して認証鍵を生成する。それは、セキュアデータベースに鍵を書込み、鍵プロビジョニングプロトコルを使用して鍵を認証クライアント２０１に送り返す。一旦完了すると、認証デバイスと依拠当事者２０２とは、対称鍵が使用された場合には同じ鍵を共有し、非対称鍵が使用された場合には異なる鍵を共有する。例えば、非対称鍵が使用された場合、依拠当事者２０２は、公開鍵を記憶して、認証クライアント２０１に秘密鍵を提供してもよい。依拠当事者２０２から秘密鍵を受け取ると、認証クライアント２０１は、鍵を認証デバイスにプロビジョニングする（それを認証デバイスと関連するセキュア記憶装置内に記憶する）。それは、次いで、（下記のように）ユーザの認証の間、鍵を使用してもよい。代替の実施形態では、鍵（複数可）が、認証クライアント２０１によって生成され、そして、鍵プロビジョニングプロトコルが、依拠当事者２０２に鍵（複数可）を提供するために使用される。いずれにせよ、一旦プロビジョニングが完了すると、認証クライアント２０１及び依拠当事者２０２はそれぞれ鍵を有し、そして、認証クライアント２０１は、依拠当事者に完了を通知する。

【００３０】

図３は、プロビジョニングされた認証デバイスによるユーザ認証のための一連のトランザクションを示す。一旦デバイス登録が（図２に記載されているように）完了すると、依拠当事者２０２は、有効な認証応答としてクライアントにおけるローカル認証デバイスによって生成された認証応答（時として「トークン」と呼ばれることがある）を受け取ることになる。

【００３１】

図３に示す特定詳細を参照すると、ユーザが認証を必要とする依拠当事者２０２によってトランザクションを開始すること（例えば、依拠当事者のウェブサイトからの支払い、秘密ユーザアカウントデータにアクセスすることなどを開始すること）に応答して、依拠当事者２０２は、ランダムチャレンジ（例えば、暗号ノンス）を含む認証リクエストを生成する。１つの実施形態では、ランダムチャレンジは、それと関連する時間制限（例えば、それが指定期間の間、有効である）を有する。依拠当事者は、また、認証のために、認証クライアント２０１によって使用されるべき認証部を識別してもよい。上記のように、依拠当事者は、クライアントにおいて利用可能なそれぞれの認証デバイスをプロビジョニングして、それぞれのプロビジョニングされた認証部のための公開鍵を記憶してもよい。このように、それは、認証部の公開鍵を使用するか、又は、認証部ＩＤ（例えば、ＡＡＩＤ）を使用することにより、使用されるべき認証部を識別してもよい。代替として、それは、ユーザが選択してもよい認証選択肢のリストをクライアントに提供してもよい。

【００３２】

認証リクエストの受取りに応答して、ユーザは、認証をリクエストするグラフィカルユーザインターフェース（ＧＵＩ）を（例えば、ウェブページ又は認証アプリケーション／アプリのＧＵＩの形式で）提示されてもよい。ユーザは、次いで、認証（例えば、指紋リーダー上で指をスワイプすることなど）を実行する。それに応答して、認証クライアント２０１は、認証部と関連する秘密鍵を有するランダムチャレンジを介して署名を含む認証応答を生成する。それは、また、ユーザＩＤコードのような他の関連するデータを認証応答の中に含んでもよい。

【００３３】

認証応答を受け取ると、依拠当事者は、ランダムチャレンジを介して（例えば、認証部と関連する公開鍵を使用して）署名を検証して、ユーザの識別を確認してもよい。一旦認証が完了すると、示すように、ユーザは、依拠当事者によってセキュアトランザクションに入ることが許可される。

【００３４】

Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ（ＴＬＳ）又はＳｅｃｕｒｅ Ｓｏｃｋｅｔｓ Ｌａｙｅｒ（ＳＳＬ）のようなセキュア通信プロトコルが、図２～３に示すトランザクションのうちの一部又は全てについて、依拠当事者２０１と認証クライアント２０２との間のセキュア接続を確立するために使用されてもよい。

認証サービスをネットワークアーキテクチャと統合するためのシステム及び方法

【００３５】

多くのレガシーシステムは、ユーザ名及びパスワード以外の認証方法に対するサポートを特徴とし得る。例えば、セキュアソケットレイヤー（ＳＳＬ）仮想プライベートネットワーク（ＶＰＮ）システムは、ワンタイムパスワード（ＯＴＰ）の使用をサポートする。Ｋｅｒｂｅｒｏｓなどのシステムは、ユーザが、デジタル証明書を使用してネットワーク又はサービスに対して認証することを可能にする。

【００３６】

本明細書に記載される本発明の実施形態は、これらの特徴を活用して、（構成変更以外の）レガシーシステム自体に対するいかなる変更も必要とすることなく、オンライン認証サービスをこのようなレガシーシステムと統合する。

【００３７】

セキュアソケットレイヤー（ＳＳＬ）仮想プライベートネットワーク（ＶＰＮ）のセキュリティを増大させるために、企業は、ＯＴＰ手法に基づく二要素認証ソリューションを展開する。ＲＳＡ ＳｅｃｕｒＩＤ又はＯＡＴＨなどのソリューションは、ユーザが、ＯＴＰ生成器を運搬し、ＶＰＮに対する認証のために、ユーザ名及びパスワードと組み合わせて、この生成器によって生成されるＯＴＰを入力することを必要とする。

【００３８】

図４は、ＳＳＬ ＶＰＮゲートウェイ４１５と組み合わせて動作するように構成されるＯＴＰ検証サーバ４２５を示す。動作に際し、ユーザは、ウェブブラウザ４１０を開き、

ＳＳＬ　ＶＰＮゲートウェイ４１５に移動し、ユーザＩＤフィールド４１２及びパスワードフィールド４１３を含むＨＴＭＬベースのログインフォーム４１１をレンダリングする。ユーザは、ユーザＩＤをＵＩＤフィールド４１２に、また、ＯＴＰを（それ自体を、又はユーザの静的パスワードに添付して）パスワードフィールド４１３に入力することができる。ＨＴＭＬフォーム４１１を介してユーザ名及びパスワードに入力した後に、ユーザは、結果をＳＳＬ　ＶＰＮゲートウェイ４１５に提出する。

【００３９】

ＳＳＬ　ＶＰＮゲートウェイ４１５は、ユーザストア４２０に対してユーザ名及びパスワードを検証し（例えば、ユーザ名が存在すること、及び正しいパスワードが入力されたことを検証し）、ユーザによって入力されたＯＴＰをＯＴＰ検証サーバ４２５に提供することによってＯＴＰを検証する。ＯＴＰ検証サーバ４２５がＯＴＰを検証して肯定応答を提供した場合、ＳＳＬ　ＶＰＮゲートウェイ４１５は、保護された内部ネットワーク４３０へのユーザアクセスを付与する。

【００４０】

上記のように、上の実施例において、ＳＳＬ　ＶＰＮゲートウェイ４１５は、別個のフォーム要素をレンダリングして、ＯＴＰの入力を可能にし、一方で他の事例において、ＳＳＬ　ＶＰＮゲートウェイ４１５は、単に、ユーザが、それらのＯＴＰをフォームのパスワードフィールドの中のパスワードに添付することに依存することができる。更に、ＳＳＬ　ＶＰＮゲートウェイ４１５は、一次ユーザ名及びパスワードがユーザストア４２０の検証によって受け取られなかった場合に、アクセスを直ちに拒絶することができる。ＳＳＬ　ＶＰＮゲートウェイ４１５とＯＴＰ検証サーバ４２５との間の通信は、ＳＳＬ　ＶＰＮゲートウェイベンダ又はＯＴＰ検証サーバベンダのいずれかによって提供されるプラグインによって容易にすることができる。しかし、大部分のＳＳＬ　ＶＰＮゲートウェイは、リモート認証ダイヤルインユーザサービスを（ＲＡＤＩＵＳ；ＲＦＣ　２８６５を参照されたい）の統合をサポートする。したがって、ＯＴＰソリューションによるＲＡＤＩＵＳのサポートは、ＯＴＰサーバプロバイダがＳＳＬ　ＶＰＮゲートウェイ固有のコネクタを開発することに対する必要性を取り除く。

【００４１】

図５に示されるように、本発明の１つの実施形態は、ネットワークインフラストラクチャを変化させることなく、オンライン認証技術（例えば、図１Ａ～Ｂ、及び図３に関して上で説明したものなど）を統合するために、ＳＳＬ　ＶＰＮゲートウェイ５１５の既存の特徴に依存する。示されるように、この実施形態は、上で説明したＯＴＰ検証サーバ４２５と潜在的に同じ（又は類似する）様式で、ＳＳＬ　ＶＰＮゲートウェイ５１５に通信可能に結合される認証サーバ２０２を含む。認証サーバ２０２はまた、１つ以上の認証デバイス１１０～１１２（例えば、指紋認証部、音声認証部、網膜スキャン認証部など）を使用するユーザを認証するための認証クライアント２０１を有するクライアントデバイス５１０にも通信可能に結合される。認証サーバ２０２は、図５のブラウザを介して（例えば、図１Ａに示される実施形態と類似する様式で）認証クライアント２０１に結合されるが、本発明の基本原理は、ブラウザベースの実装に限定されない。

【００４２】

１つの実施形態において、ＳＳＬ　ＶＰＮゲートウェイ５１５と、ブラウザ５１０と、認証サーバ２０２との間の相互作用は、以下の通りである。ユーザは、ウェブブラウザ５１０を開き、ＪａｖａＳｃｒｉｐｔ（登録商標）などのブラウザ実行可能コード５１２を含むウェブページ５１１をレンダリングするＳＳＬ　ＶＰＮゲートウェイ５１５に移動する。１つの実施形態において、ブラウザ実行可能コード５１２は、認証サーバ２０２との通信チャネルを確立し、認証クライアント２０１をトリガーしてユーザを認証することによって、認証をトリガーする。１つの実施形態において、認証サーバ２０２及びクライアント２０１は、図３に関して上で説明したものなどの、一連の認証トランザクションに入る。例えば、認証サーバ２０２は、ランダムチャレンジ（例えば、暗号ノンス）を含む認証リクエストを生成することができ、また、認証のために認証クライアント２０１によっ

て使用される認証部１１０～１１２を識別することができる（又はそうしない場合がある）。認証リクエストの受取りに応答して、ユーザは、認証をリクエストするグラフィカルユーザインターフェース（ＧＵＩ）を（例えば、ウェブページ又は認証アプリケーション／アプリのＧＵＩの形式で）提示されてもよい。ユーザは、次いで、認証（例えば、指紋リーダー上で指をスワイプすることなど）を実行する。それに応答して、認証クライアント２０１は、認証部と関連する秘密鍵を有するランダムチャレンジを介して署名を含む認証応答を生成する。それは、また、ユーザＩＤコードのような他の関連するデータを認証応答の中に含んでもよい。認証応答を受け取ると、認証サーバ２０２は、ランダムチャレンジを通じて（例えば、認証部と関連する公開鍵を使用して）署名を検証し、ユーザの識別を確認する。１つの実施形態において、ＪａｖａＳｃｒｉｐｔ又は他のブラウザ実行可能コード５１２は、認証サーバ２０２と認証クライアント２０１との間で上記の認証メッセージを渡す。

【００４３】

１つの実施形態において、認証成功に応答して、認証サーバ２０２は、本明細書で「チケット」と称される暗号データ構造を生成し、ブラウザ５１０に渡す。１つの実施形態において、チケットは、ＨＴＭＬフォーム５１１のフィールドを介してＳＳＬ　ＶＰＮゲートウェイ５１５に提出することができるランダムな数字列又は他の形式のワンタイムパスワード（ＯＴＰ）を備える。例えば、上記のように、別個のフィールドを、チケットについてＨＴＭＬフォーム５１１で定義することができ、又はチケットを、ユーザの静的パスワードの最後に添付することができる。どのようにチケットが入力されたかにかかわらず、１つの実施形態において、ＪａｖａＳｃｒｉｐｔ又は他のブラウザ実行可能コード５１２は、チケットをＳＳＬ　ＶＰＮゲートウェイ５１５に提出する。受信すると、ＳＳＬ　ＶＰＮゲートウェイ５１５は、認証サーバ２０２との通信を介してチケットを検証する（例えば、チケットを認証サーバに提供し、チケットが有効であることを示す通信を受信する）。例えば、ＳＳＬ　ＶＰＮゲートウェイ５１５からチケット及び他のユーザデータ（例えば、ユーザＩＤ又は他の形式の識別子）を受け取ると、認証サーバ２０２は、該チケットと、ブラウザ５１０に提供されるチケットとを比較することができる。チケットがマッチした場合、認証サーバ２０２は、「認証成功」メッセージをＳＳＬ　ＶＰＮゲートウェイ５１５に送信する。チケットがマッチをしなかった場合、認証サーバは「認証失敗」メッセージをＳＳＬ　ＶＰＮゲートウェイ５１５に送信する。１つの実施形態において、ＳＳＬ　ＶＰＮゲートウェイ５１５は、（本発明の基本原理は、いかなる特定のプロトコルにも限定されないが）ＲＡＤＩＵＳを使用して認証サーバ２０２に対してチケットを検証する。検証されると、ＳＳＬ　ＶＰＮゲートウェイ５１５は、保護された内部ネットワーク５３０へのユーザアクセスを付与する。

【００４４】

意味深いことに、ＳＳＬ　ＶＰＮゲートウェイ５１５と認証サーバ２０２との間のトランザクションは、ＯＴＰ検証サーバ４２５によって提供される成功／失敗メッセージと同じ様式で（同じプロトコル及びデータフィールドを使用して）実装することができることである。その結果、ＳＳＬ　ＶＰＮゲートウェイ５１５は、本明細書に記載される本発明の実施形態を実装するために再構成する必要はなく、それによって、実装を単純化し、それと関連する時間及び費用を低減させる。

【００４５】

上記の手法において、ＳＳＬ　ＶＰＮログインページ５１１は、認証をトリガーするために、カスタムＪａｖａＳｃｒｉｐｔ又は他のブラウザ実行可能コード５１２を含むようにカスタマイズすることができる。当然、ユーザがインストールされた認証クライアント２０１を有しない場合に、代替の実施形態を実装することができる。

【００４６】

更に、ＪａｖａＳｃｒｉｐｔ又は他のブラウザ実行可能コード５１２によるＳＳＬ　ＶＰＮゲートウェイ５１５との通信は、ユーザがＳＳＬ　ＶＰＮゲートウェイ５１５に対して認証するために通常使用する、同じＨＴＭＬフォーム５１１を通して容易にすることが

できる。この目的は、デフォルトのＳＳＬ　ＶＰＮのＨＴＭＬフォーム５１１において既存のパスワード又はＯＴＰフィールドを使用してＪａｖａＳｃｒｉｐｔ又は他の実行可能コードによって得られるチケットを渡すことである（ここでも、単純化し、上記の技術を実装することと関連する時間及び費用を低減させる）。

【００４７】

これらの技術は、ＶＰＮ固有の統合を開発することなく、多数のＶＰＮソリューションに関する良定義問題に対処するので、この統合を達成することは、比較的少ない労力しか必要とせず、また、認証サービスプロバイダ（すなわち、認証サーバ２０２及びクライアント２０１を管理するエンティティ）が、セキュアリモートアクセスを送達するためのパッケージ化されたソリューションを提供することを可能にする。

【００４８】

本発明の１つの実施形態による方法が図６に示されている。本方法は、図５に示されるアーキテクチャのコンテキスト内に実装することができるが、任意の特定のシステムアーキテクチャに限定されない。

【００４９】

６０１で、ユーザは、ブラウザを開き、ＳＳＬ　ＶＰＮゲートウェイに移動する。６０２で、ＳＳＬ　ＶＰＮゲートウェイは、ブラウザ実行可能コードを含むページをレンダリングして、クライアントに対する認証をトリガーする。６０３で、ブラウザ実行可能コードは、認証サーバとの接続を確立して、ユーザの認証をトリガーする。６０４で、ブラウザ実行可能コードは、認証クライアントと認証サーバとの間でメッセージを交換して、ユーザを認証する（図１Ａ～Ｂ、図３、及び図５に関する上の説明を参照されたい）。認証されると、認証サーバは、チケットを返す。

【００５０】

６０５で、ブラウザ実行可能コードは、チケットをＳＳＬ　ＶＰＮゲートウェイに提出し、６０６で、ＳＳＬ　ＶＰＮゲートウェイは、認証サーバに対してチケットを検証する。上記のように、これは、認証サーバが、（例えば、ＲＡＤＩＵＳを介して）チケットの有効性を確認するために、チケットを、動作６０４において返されるチケットと比較することを含むことができる。６０７で、チケットが検証されると、ＳＳＬ　ＶＰＮゲートウェイは、保護された内部ネットワークへのユーザアクセスを付与する。

【００５１】

レガシーシステムが認証のためにデジタル証明書の使用を受け入れる場合に、レガシーシステムと統合するための代替的な手法が可能である。Ｋｅｒｂｅｒｏｓを使用するＶＰＮ又はＷｉｎｄｏｗｓ　Ａｃｔｉｖｅ　Ｄｉｒｅｃｔｏｒｙなどのこれらのソリューションは、通常、証明書認証を行うために、クライアント側構成要素を含む。

【００５２】

クライアント側での統合が主にブラウザベースであった（例えば、ＪａｖａＳｃｒｉｐｔを使用する）、上で概説した統合手法とは異なり、この実施形態において、認証クライアント２０１の要素は、統合を達成するために、レガシーソリューションのクライアント側に統合されるが、上述のように、いかなるサーバ側の統合も必要でない。

【００５３】

図７に示される具体的な実施形態において、認証クライアント２０１は、書名付き証明書を管理するための資格情報プロバイダ構成要素７１１を備え、それを使用して、Ｋｅｒｂｅｒｏｓインフラストラクチャ７３０を介してネットワークリソースへのアクセスを獲得する。例えば、１つの実施形態において、認証クライアント２０１は、資格情報プロバイダ構成要素７３０を使用して、資格情報プロバイダフレームワークを介してＷｉｎｄｏｗｓ（登録商標）オペレーティングシステムに統合することができる。しかしながら、本発明の基本原理は、Ｋｅｒｂｅｒｏｓの実装又は任意の特定のタイプのオペレーティングシステムに限定されないことに留意するべきである。

【００５４】

この実施形態はまた、（例えば、図１Ｂ及び図３に関して上述したように）エンドユー

ザを認証するために一連の認証トランザクションに入る、認証サーバ７２５と認証クライアント２０１との間の通信にも依存する。１つの実施形態において、アクティブディレクトリ７３５及びＫｅｒｂｅｒｏｓインフラストラクチャ７３０は、認証サーバ７２５によって保持されるルート証明書を信用するように構成される。ユーザが認証されると、認証サーバ７２５は、認証サーバ７２５によって保持されるルート証明書を使用して署名する暗号公開鍵／秘密鍵ペアを備える短期証明書を発行する（例えば、ルート証明書の秘密鍵によって短期証明書に署名する）。具体的には、１つの実施形態において、短期証明書の公開鍵は、ルート証明書の秘密鍵によって署名される。鍵ペアに加えて、短期証明書はまた、短期証明書が有効である時間の長さ（例えば、５分、１時間など）を示すタイムスタンプ／タイムアウトデータも含むことができる。

【００５５】

１つの実施形態では、資格情報プロバイダ７１１が認証サーバから署名付き短期証明書を受信すると、短期証明書を含むＫｅｒｂｅｒｏｓインフラストラクチャ７３０によってチャレンジ応答トランザクションに入る。具体的には、Ｋｅｒｂｅｒｏｓインフラストラクチャは、チャレンジ（例えば、ノンスなどのランダムデータ）を資格情報プロバイダ７１１に送信し、次いで、短期証明書の秘密鍵を使用してチャレンジに署名する。次いで、短期証明書をＫｅｒｂｅｒｏｓインフラストラクチャに送信し、（１）（信用するように構成された）認証サーバ７２５によって提供されるルート証明書の公開鍵を使用して、短期証明書の署名を検証し、（２）短期証明書からの公開鍵を使用して、チャレンジを通じて署名を検証する。どちらの署名も有効であった場合、Ｋｅｒｂｅｒｏｓインフラストラクチャは、Ｋｅｒｂｅｒｏｓチケットを資格情報プロバイダ７１１に発行し、次いで、それを使用して、Ｋｅｒｂｅｒｏｓインフラストラクチャによって管理されるファイルサーバ、電子メールアカウント、その他などのネットワークリソースへのアクセスを獲得することができる。

【００５６】

これらの技術を使用して、認証サーバ７２５及びクライアント２０１は、既存のアクティブディレクトリ７３５及びＫｅｒｂｅｒｏｓインフラストラクチャ７３０に対する大幅な修正を伴わずに統合することができる。むしろ、必要とされるのは、アクティブディレクトリ７３５／Ｋｅｒｂｅｒｏｓインフラストラクチャが、認証サーバ７２５によって保持されるルート証明書を信用するように構成することだけである。

【００５７】

図８は、オンライン認証インフラストラクチャをレガシーシステムと統合するための方法の１つの実施形態を示す。本方法は、図７に示されるアーキテクチャのコンテキスト内に実装することができるが、任意の特定のシステムアーキテクチャに限定されない。

【００５８】

８０１で、ユーザは、Ｗｉｎｄｏｗｓデバイスなどのデバイスを開き、ログインを試みる。８０２で、認証クライアントがトリガーされて、ユーザを認証する。それに応答して、認証クライアントは、認証サーバによってオンライン認証を行う。例えば、上で論じたように、認証クライアントは、１つ以上の認証デバイス（例えば、指紋認証デバイス、音声認証デバイス、その他）をサーバに事前に登録しておくことができる。次いで、図１Ａ～Ｂ及び図３に関して上述したような一連のトランザクションを使用して、サーバによって認証することができる。例えば、認証サーバは、ランダムチャレンジによって認証リクエストを認証クライアントに送信することができ、認証クライアントは、使用される認証デバイスと関連する秘密鍵を使用して署名する。認証サーバは、次いで、公開鍵を使用して署名を検証することができる。

【００５９】

認証に使用される特定のプロトコルにかかわらず、認証が成功した場合、８０３で、認証サーバは、認証サーバによって維持されるルート証明書の秘密鍵を使用して署名される短期デジタル証明書を認証クライアントに返す。上記のように、ルート証明書は、アクティブディレクトリ／Ｋｅｒｂｅｒｏｓインフラストラクチャによって信用される。

【００６０】
８０４で、認証クライアントは、次いで、短期デジタル証明書を使用して、Ｋｅｒｂｅｒｏｓインフラストラクチャに対して認証する。例えば、Ｋｅｒｂｅｒｏｓインフラストラクチャは、チャレンジ（例えば、ノンスなどのランダムデータ）を認証クライアントに送信することができ、次いで、短期証明書の秘密鍵を使用してチャレンジに署名する。次いで、短期証明書をＫｅｒｂｅｒｏｓインフラストラクチャに送信し、８０５で、（信用するように構成された）認証サーバによって提供されるルート証明書の公開鍵を使用して、短期証明書の署名を検証し、短期証明書からの公開鍵を使用して、チャレンジを通じて署名を検証する。どちらの署名も有効であった場合、８０６で、Ｋｅｒｂｅｒｏｓインフラストラクチャは、Ｋｅｒｂｅｒｏｓチケットを認証クライアントに発行し、次いで、それを使用して、Ｋｅｒｂｅｒｏｓインフラストラクチャによって管理されるファイルサーバ、電子メールアカウント、その他などのネットワークリソースへのアクセスを獲得することができる。
【００６１】
最終的には、認証サーバ及び認証クライアントを使用したオンライン認証を使用して、レガシーシステムのためのフロントエンドの認証を行うことができ、バックエンドのレガシーアプリケーションインフラストラクチャに対する変更を必要とすることなく、効率的なオンライン認証のあらゆる柔軟性を獲得することになる。
【００６２】
本明細書に記載される実施形態を通して実現される数多くの利点としては、以下が挙げられるが、それらに限定されない。
【００６３】
初期の統合労力の低減：依拠当事者が、オンライン認証機能を組み込むためにアプリケーションを書き換えることなくオンライン認証を展開すること、又はサードパーティのフェデレーションサーバとの統合を有効にすることを可能にする。
【００６４】
ポリシー管理の簡略化：コードの他に認証ポリシーを表すことによって、この手法は、組織が、コードの変更を必要とすることなく、容易にそれらの認証ポリシーを更新することを可能にする。規制委任の新しい解釈を反映するための、又は既存の認証機構に対する攻撃に応答するための変更が、ポリシーの単純な変更になり、かつ素早く遂行することができる。
【００６５】
将来の詳細化の有効化：新しい認証デバイス及び機構が利用可能になるので、組織は、新しい又は新生のリスクに対処するときに、デバイス／機構の適切さを評価することができる。新しく利用できる認証デバイスを統合するには、デバイスをポリシーに加えることだけしか必要としない。直ちに新しい能力を展開するために、更にはレガシーアプリケーションにさえ、新しいコードを書き込む必要はない。
【００６６】
直接的なトークンコストの低減：レガシーＯＴＰ手法は、（安くなりつつあるが）ユーザ単位ではどちらも比較的高価である物理的なハードウェアトークンに依存し、喪失／破損、取り替えコストといった問題をもたらす。本明細書に記載されているオンライン認証手法は、エンドユーザのデバイス上で既に利用可能である能力を活用し、エンドユーザ毎に専用の認証ハードウェアを入手するコストを排除することによって、展開コストを激減させることができる。
【００６７】
間接的な展開コスト：ＯＴＰ手法は、通常、ＩＴ管理者が、エンドユーザのトークンをＯＴＰ検証サーバにプロビジョニングすることを必要とし、ソフトウェアベースのデスクトップＯＴＰ発生器は、依然として、初期の展開中にヘルプデスクの介入を必要とする。本オンライン認証手法は、エンドユーザのデバイス上で既に利用可能である能力を活用し、展開のためのセルフサービスの登録モデルを送達することによって、展開コストを激減

させることができる。

【００６８】

改善されたエンドユーザエクスペリエンス：ＯＴＰ手法は、ユーザが、それらのＯＴＰ発生器を持ち歩くこと（多くの人が忘れるので、一時的なアクセスを可能にするための追加的なヘルプデスクコストが生じる）だけでなく、ＯＴＰをアプリケーションに手動で入力することを必要とする。ＦＩＤＯ手法は、ユーザ名／パスワード及びＯＴＰ入力を、指紋センサの上で指をスワイプすることのような、より簡単な何かと置き換えることによって、エンドユーザに対する認証の影響を激減させることができる。

例示的なデータ処理デバイス

【００６９】

図９は、本発明のいくつかの実施形態において使用することができる例示的なクライアント及びサーバを図示するブロック図である。図９は、コンピュータシステムの様々な構成要素を図示しているが、そのような詳細は本発明に適切でないため、構成要素を相互接続する任意の特定のアーキテクチャ又は方法を表すことを意図するものではないことを理解すべきである。より少ない構成要素又は複数の構成要素を有する他のコンピュータシステムもまた、本発明によって使用可能であることが理解されるであろう。

【００７０】

図９に示されるように、データ処理システムの形態であるコンピュータシステム９００は、処理システム９２０に結合されているバス（複数可）９５０と、電源９２５と、メモリ９３０と、不揮発性メモリ９４０（例えば、ハードドライブ、フラッシュメモリ、相変化メモリ（ＰＣＭ）など）とを含む。バス（複数可）９５０は、当該技術分野において周知であるように、様々なブリッジ、コントローラ及び／又はアダプタを介して互いに接続され得る。処理システム９２０は、メモリ９３０及び／又は不揮発性メモリ９４０から命令（複数可）を取得することができ、上述したように動作を実行するための命令を実行することができる。バス９５０は、上記構成要素を一体に相互接続し、また、任意のドック９６０、ディスプレイコントローラ及びディスプレイデバイス９９０、入力／出力デバイス９８０（例えば、ＮＩＣ（ネットワークインターフェースカード）、カーソル制御（例えば、マウス、タッチスクリーン、タッチパッドなど）、キーボードなど）及び任意の無線送受信機（複数可）９９０（例えば、ブルートゥース（登録商標）、ＷｉＦｉ、赤外線など）にそれらの構成要素を相互接続する。

【００７１】

図１０は、本発明のいくつかの実施形態において使用され得る例示的なデータ処理システムを図示するブロック図である。例えば、データ処理システム１０００は、ハンドヘルドコンピュータ、パーソナルディジタルアシスタント（ＰＤＡ）、携帯電話、ポータブルゲームシステム、ポータブルメディアプレーヤ、タブレット、又は、携帯電話、メディアプレーヤ及び／又はゲームシステムを含むことができるハンドヘルドコンピューティングデバイスとすることができる。別の例として、データ処理システム１０００は、ネットワークコンピュータ又は別のデバイス内の埋め込み処理デバイスとすることができる。

【００７２】

本発明の１つの実施形態によれば、データ処理システム１０００の例示的なアーキテクチャは、上述した携帯デバイスのために使用することができる。データ処理システム１０００は、集積回路上の１つ以上のマイクロプロセッサ及び／又はシステムを含むことができる処理システム１０２０を含む。処理システム１０２０は、メモリ１０１０、（１つ以上のバッテリを含む）電源１０２５、オーディオ入力／出力１０４０、ディスプレイコントローラ及びディスプレイデバイス１０６０、任意の入力／出力１０５０、入力デバイス（複数可）１０７０及び無線送受信機（複数可）１０３０に結合されている。図１０には示されていない追加の構成要素はまた、本発明の特定の実施形態においてデータ処理システム１０００の一部であってもよく、本発明の特定の実施形態において図１０に示されるよりも少ない構成要素が使用可能であることが理解されるであろう。更に、図１０には示されていない１つ以上のバスは、当該技術分野において周知であるように様々な構成要素

を相互接続するために使用することができることが理解されるであろう。

【００７３】

メモリ１０１０は、データ処理システム１０００による実行のためのデータ及び／又はプログラムを記憶する。オーディオ入力／出力１０４０は、例えば、音楽を再生するためにマイクロフォン及び／又はスピーカを含むことができ、並びに／又はスピーカ及びマイクロフォンを介して電話機能を提供することができる。ディスプレイコントローラ及びディスプレイデバイス１０６０は、グラフィカルユーザインターフェース（ＧＵＩ）を含むことができる。無線（例えば、ＲＦ）送受信機１０３０（例えば、ＷｉＦｉ送受信機、赤外線送受信機、ブルートゥース送受信機、無線携帯電話送受信機など）は、他のデータ処理システムと通信するために使用することができる。１つ以上の入力デバイス１０７０は、ユーザがシステムに入力を提供するのを可能にする。これらの入力デバイスは、キーパッド、キーボード、タッチパネル、マルチタッチパネルなどであってもよい。任意の他の入力／出力１０５０は、ドック用コネクタであってもよい。

【００７４】

上述したように、本発明の実施形態は、様々な工程を含んでもよい。工程は、汎用又は特殊目的のプロセッサに特定の工程を実行させる機械実行可能な命令で具現化され得る。代替的に、これらの工程は、工程を実行するためのハードワイヤードロジックを含む特定のハードウェア構成要素によって又はプログラミングされたコンピュータ構成要素及びカスタムハードウェア構成要素の任意の組み合わせによって実行することができる。

【００７５】

本発明の要素はまた、機械実行可能なプログラムコードを記憶する機械可読媒体として提供することができる。機械可読媒体としては、フロッピーディスク、光ディスク、ＣＤ－ＲＯＭ及び光磁気ディスク、ＲＯＭ、ＲＡＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、磁気若しくは光カード、又は、電子プログラムコードを記憶するのに適した他の種類の媒体／機械可読媒体を挙げることができるが、これらに限定されるものではない。

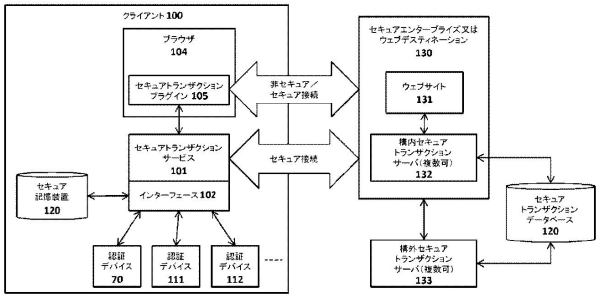
【００７６】

上記の説明全体を通じて、説明の目的のために、多数の具体的な詳細が本発明の完全な理解を提供するために記載された。しかしながら、本発明は、これらの具体的な詳細の一部がなくても実施され得ることは、当業者にとって明らかであろう。例えば、本明細書に記載された機能モジュール及び方法は、ソフトウェア、ハードウェア又はそれらの任意の組み合わせとして実装されてもよいことは、当業者にとって容易に明らかであろう。更に、本発明のいくつかの実施形態は、モバイルコンピューティング環境のコンテキストで本明細書において記載されているが、本発明の基本原理は、モバイルコンピューティングの実装に限定されるものではない。実質的に任意の種類のクライアント又はピアデータ処理デバイスは、例えば、デスクトップ又はワークステーションコンピュータを含むいくつかの実施形態で使用することができる。したがって、本発明の範囲及び趣旨は、以下の特許請求の範囲の観点から判断されるべきである。

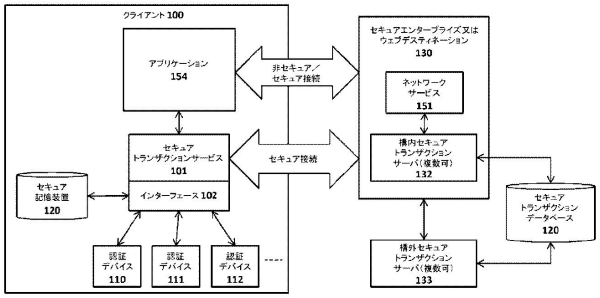
【００７７】

上述したように、本発明の実施形態は、様々な工程を含んでもよい。工程は、汎用又は特殊目的のプロセッサに特定の工程を実行させる機械実行可能な命令で具現化され得る。代替的に、これらの工程は、工程を実行するためのハードワイヤードロジックを含む特定のハードウェア構成要素によって又はプログラミングされたコンピュータ構成要素及びカスタムハードウェア構成要素の任意の組み合わせによって実行することができる。

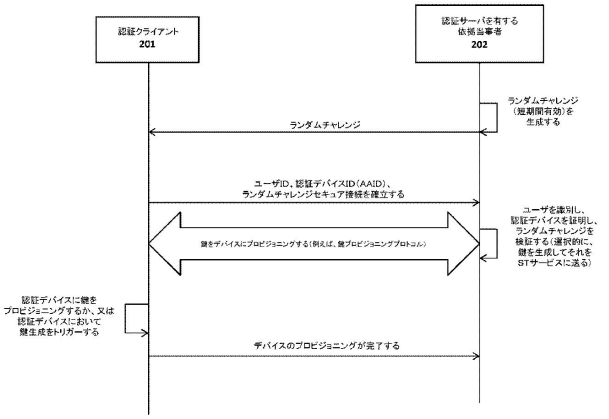
【図１Ａ】



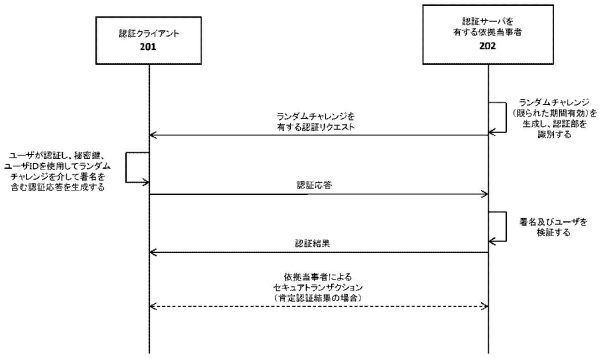
【図１Ｂ】



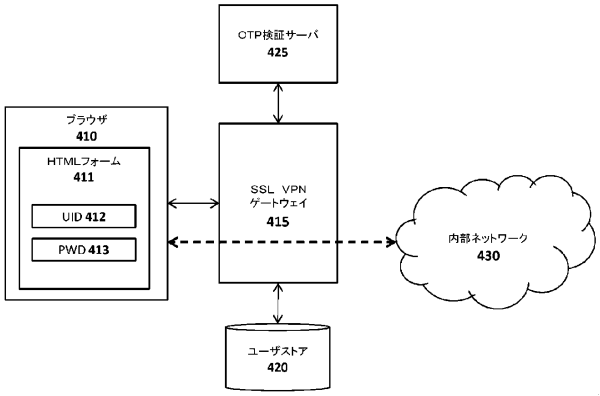
【図２】



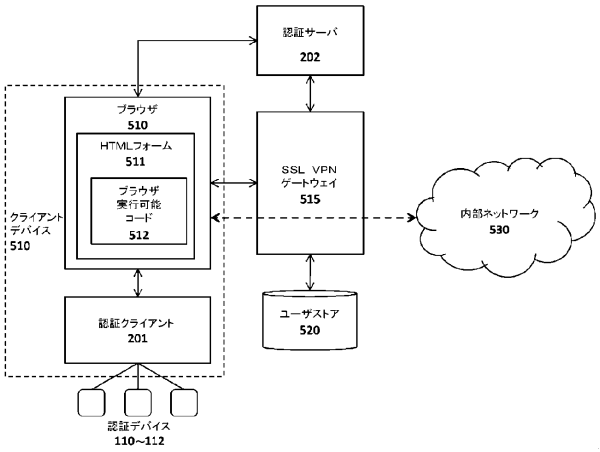
【図３】



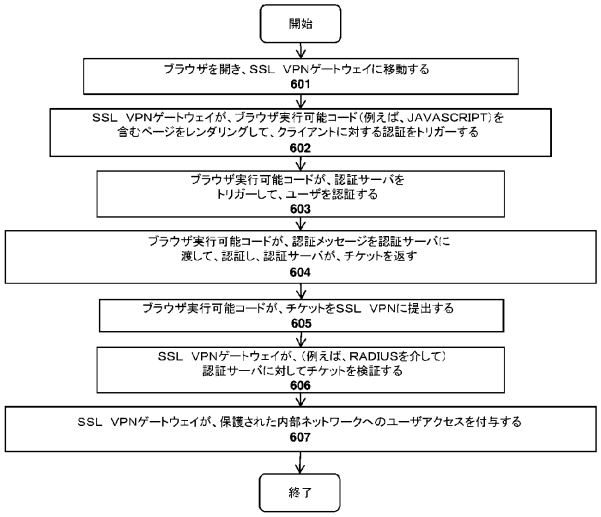
【図４】



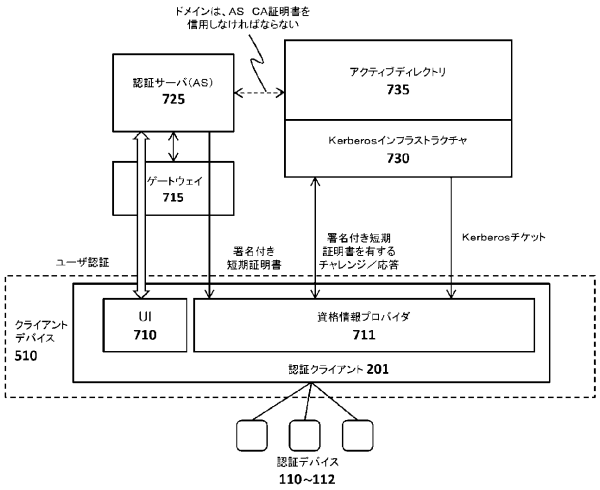
【図５】



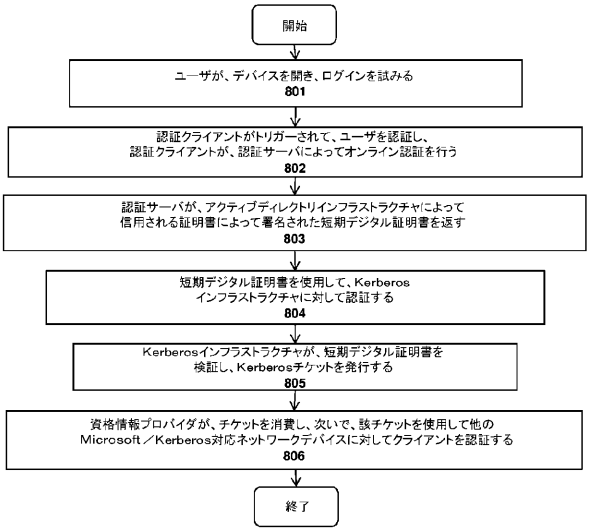
【図６】



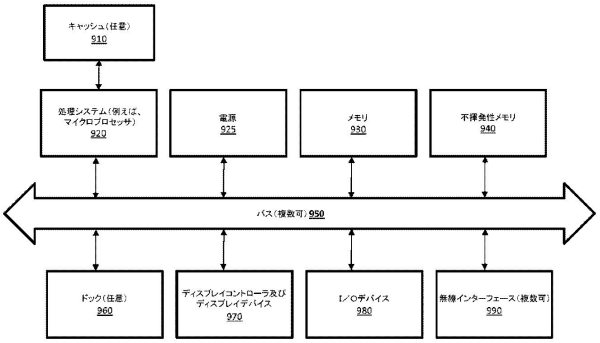
【図７】


ドメインは、AS CA証明書を
信用しなければならない
認証サーバ(AS)
725
アクティブディレクトリ
735
Kerberosインフラストラクチャ
730
ゲートウェイ
715
ユーザ認証
署名付き
短期証明書
署名付き短期
証明書を有する
チャレンジ/応答
Kerberosチケット
クライアント
デバイス
510
UI
710
資格情報プロバイダ
711
認証クライアント 201
認証デバイス
110~112

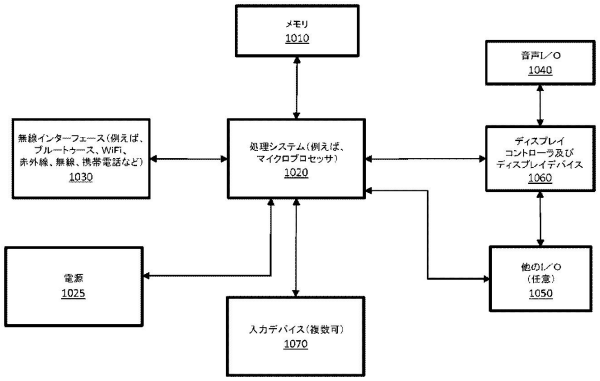
【図８】


開始
ユーザが、デバイスを開き、ログインを試みる
801
認証クライアントがトリガーされて、ユーザを認証し、
認証クライアントが、認証サーバによってオンライン認証を行う
802
認証サーバが、アクティブディレクトリインフラストラクチャによって
信用される証明書によって署名された短期デジタル証明書を返す
803
短期デジタル証明書を使用して、Kerberos
インフラストラクチャに対して認証する
804
Kerberosインフラストラクチャが、短期デジタル証明書を
検証し、Kerberosチケットを発行する
805
資格情報プロバイダが、チケットを消費し、次いで、該チケットを使用して他の
Microsoft／Kerberos対応ネットワークデバイスに対してクライアントを認証する
806
終了

【図９】


キャッシュ(任意)
910
処理システム(例えば、
マイクロプロセッサ)
920
電源
925
メモリ
930
不揮発性メモリ
940
バス(複数可) 950
ドック(任意)
960
ディスプレイコントローラ及び
ディスプレイデバイス
970
I/Oデバイス
980
無線インターフェース(複数可)
990

【図１０】


メモリ
1010
音声I/O
1040
無線インターフェース(例えば、
ブルートゥース、WiFi、
赤外線、無線、携帯電話など)
1030
処理システム(例えば、
マイクロプロセッサ)
1020
ディスプレイ
コントローラ及び
ディスプレイデバイス
1060
電源
1025
他のI/O
(任意)
1050
入力デバイス(複数可)
1070

フロントページの続き

(74)代理人 100086771
弁理士 西島 孝喜
(74)代理人 100109070
弁理士 須田 洋之
(74)代理人 100109335
弁理士 上杉 浩
(74)代理人 100120525
弁理士 近藤 直樹
(74)代理人 100139712
弁理士 那須 威夫
(72)発明者 ウイルソン ブレンドン ジェイ
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ジェン ロード ２１００ スイート １０５
(72)発明者 バグダサリアン ダヴィット
アメリカ合衆国 カリフォルニア州 ９４３０３ パロ アルト ジェン ロード ２１００ スイート １０５

審査官 上島 拓也

(56)参考文献 米国特許第０８５８４２２４（ＵＳ，Ｂ１）
米国特許出願公開第２０１４／０１８９８２８（ＵＳ，Ａ１）
特表２０１０－５０５２８６（ＪＰ，Ａ）
特開２００５－０９２６１４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／３３
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／０８
Ｈ０４Ｌ ９／３２
Ｈ０４Ｌ １２／６６