(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6653268号
(P6653268)

(45)発行日　令和2年2月26日(2020.2.26)　(24)登録日　令和2年1月29日(2020.1.29)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675D
G06F 21/33	(2013.01)	H04L	9/00	673D
G06F 21/41	(2013.01)	G06F	21/33	
		G06F	21/41	

請求項の数 20　(全 22 頁)

(21)出願番号　特願2016-566912(P2016-566912)
(86)(22)出願日　平成27年5月1日(2015.5.1)
(65)公表番号　特表2017-519411(P2017-519411A)
(43)公表日　平成29年7月13日(2017.7.13)
(86)国際出願番号　PCT/US2015/028924
(87)国際公開番号　WO2015/168641
(87)国際公開日　平成27年11月5日(2015.11.5)
審査請求日　平成30年4月27日(2018.4.27)
(31)優先権主張番号　14/268,563
(32)優先日　平成26年5月2日(2014.5.2)
(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　100086771
弁理士　西島　孝喜
(74)代理人　100088694
弁理士　弟子丸　健
(74)代理人　100094569
弁理士　田中　伸一郎
(74)代理人　100067013
弁理士　大塚　文昭

最終頁に続く

(54)【発明の名称】異なるチャネル上で強力な認証イベントを伝えるシステム及び方法

(57)【特許請求の範囲】
【請求項１】
方法であって、
クライアント装置を認証するためにネットワーク上で認証装置の認証サービスにより認証を実行するステップであって、該認証は、
前記クライアント装置上の認証装置を用いて、該クライアント装置により認証結果を生成することと、
前記クライアント装置により、前記認証結果に基づいて、合法的なユーザが該クライアント装置を所有している可能性を示す保証レベルを算出することと、
前記クライアント装置により、前記保証レベルが閾値を上回るときに前記クライアント装置が認証されることを判定することと、
前記ネットワーク上で、成功した認証結果を前記認証サービスに提供することと、を含む、
ステップと、
前記クライアント装置が認証に成功したことに応答して、前記認証サービスにより、該クライアント装置、該クライアント装置がアクセスしようとするネットワークサービス、及び前記認証に使用された前記認証装置のタイプについての識別情報を含むトークンを生成するステップであって、該トークンは、前記クライアント装置及び前記ネットワークサービスの前記識別情報に関する署名を含む検証データを更に含む、ステップと、
前記認証サービスにより、前記クライアント装置に前記トークンを送信するステップと

、
前記ネットワークサービスにおいて前記クライアント装置から前記トークンを受信することに応答して、前記ネットワークサービスが、前記検証データを使用して前記トークンを検証し、かつ前記クライアント装置との１又は複数のトランザクションを、前記認証に使用された前記認証装置の前記タイプが該１又は複数のトランザクションに関する容認可能なクラス内であることに少なくとも一部基づいて許可又は拒絶する、ステップと、
を含む方法。
【請求項２】
前記署名は、第１のキーで生成され、前記方法は、前記ネットワークサービスにより、前記第１のキー、又は、前記第１のキーに対応する第２のキーを使用して前記署名を検証するステップを更に含む、請求項１に記載の方法。
【請求項３】
前記認証サービス及び前記ネットワークサービスの両方は、信頼できる当事者のネットワーク周辺内で実行される、請求項１に記載の方法。
【請求項４】
前記認証サービスは、前記ネットワークサービスを実行する信頼できる当事者の外部アイデンティティプロバイダにより実行される、請求項１に記載の方法。
【請求項５】
前記認証装置は、生体認証装置を含む、請求項１に記載の方法。
【請求項６】
前記ネットワークサービスは、前記認証装置について前記識別情報を使用してポリシーデータベースに問い合わせて、前記認証装置の１又は複数の特性を判定し、かつ、前記認証装置の前記１又は複数の特性に少なくとも一部基づいて前記１又は複数のトランザクションを許可又は拒絶する、請求項１に記載の方法。
【請求項７】
前記認証装置の前記１又は複数の特性の少なくとも１つは、前記認証装置の信頼性及び精度の尺度を含む、請求項６に記載の方法。
【請求項８】
前記認証装置の前記１又は複数の特性の少なくとも１つは、前記認証装置が実行されるセキュリティのレベルを含み、該セキュリティのレベルは他人受入率を含む、請求項７に記載の方法。
【請求項９】
前記認証装置の前記１又は複数の特性に加えて、前記ネットワークサービスは、前記１又は複数のトランザクションの１又は複数の特性に基づいて、前記１又は複数のトランザクションを許可又は拒絶する、請求項６に記載の方法。
【請求項１０】
前記１又は複数のトランザクションのうちの１つの前記１又は複数の特性は、前記トランザクションの金銭的価値を含む、請求項９に記載の方法。
【請求項１１】
方法であって、
クライアント装置を認証するために認証機能を有する認証装置を含むネットワーク装置でネットワーク上で認証を実行するステップであって、前記クライアント装置の前記ネットワーク認証は、セキュアな通信チャネル上で実行される、ステップと、
前記認証に使用された認証装置のタイプを識別する第１の識別情報を前記ネットワーク装置にて生成するステップと、
前記ネットワーク装置により、前記クライアント装置からネットワークサービスに送信されたネットワークパケットを受信するステップと、
前記ネットワーク装置により、前記第１の識別情報を含むために前記ネットワークパケットを修正して、前記ネットワークパケットを前記ネットワークサービスにルーティングするステップと、

前記ネットワークサービスにより、前記認証に使用された前記認証装置の前記タイプを判定するために前記第１の識別情報を使用して、前記認証に使用された前記認証装置の前記タイプに少なくとも一部基づいて前記クライアント装置との１又は複数のトランザクションを許可又は拒絶するステップと、
を含む方法。
【請求項１２】
前記ネットワーク装置により、認証装置ＩＤコードと仮想識別子（ＶＩＤ）コードとの間のマッピングを含むデータ構造に問い合わせることにより、前記第１の識別情報を識別するステップを更に含み、該第１の識別情報は、前記認証に使用された前記認証装置について認証装置ＩＤコードに関連した前記ＶＩＤコードの１つを含む、請求項１１に記載の方法。
【請求項１３】
前記ネットワーク装置は、ファイアウォール、仮想プライベートネットワーク（ＶＰＮ）装置、又は、トランスポートレイヤセキュリティ（ＴＬＳ）終点を含む、請求項１２に記載の方法。
【請求項１４】
前記ネットワーク装置及び前記ネットワークサービスの両方は、該ネットワークサービスを提供する信頼できる当事者のネットワーク周辺内で実行される、請求項１１に記載の方法。
【請求項１５】
前記認証装置は、生体認証装置を含む、請求項１１に記載の方法。
【請求項１６】
前記ネットワークサービスは、前記認証装置について前記第１の識別情報を使用してポリシーデータベースに問い合わせて、前記認証装置の１又は複数の特性を判定し、かつ、前記認証装置の前記１又は複数の特性に少なくとも一部基づいて前記１又は複数のトランザクションを許可又は拒絶する、請求項１１に記載の方法。
【請求項１７】
前記認証装置の前記特性の少なくとも１つは、前記認証装置の信頼性及び精度の尺度を含む、請求項１６に記載の方法。
【請求項１８】
前記認証装置の前記特性の少なくとも１つは、前記認証装置が実行されるセキュリティのレベルを含み、該セキュリティのレベルは他人受入率を含む、請求項１７に記載の方法。
【請求項１９】
前記認証装置の前記特性に加えて、前記ネットワークサービスは、前記トランザクションの１又は複数の特性に基づいて、前記トランザクションを許可又は拒絶する、請求項１６に記載の方法。
【請求項２０】
前記トランザクションの前記１又は複数の特性は、前記トランザクションの金銭的価値を含む、請求項１９に記載の方法。
【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。更に詳しくは、本発明は、異なるチャネル上で強力な認証イベントを伝え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、生体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、特許出願公開第２０１１／００８２８０１号（「‘８０１出願」）は、強力な認証（例えば、個人情報の盗難やフィッシングに対する保護）、セキュアなトランザクション（例えば、「ブラウザにおけるマルウェア」及びトランザクションについての「中間者」攻撃に対する保護）、並びに、クライアント認証トークンの登録／管理（例えば、指紋リーダ、顔認識装置、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（trusted platform modules）、その他）を提供するネットワーク上のユーザ登録及び認証のためのフレームワーク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。これらの改善の一部が、本特許出願の譲受人に譲渡される以下の１組の米国特許出願（「同時係属中の出願」）、即ち、第１３／７３０，７６１号、認証能力を判定するクエリシステム及び方法（Query System and Method to Determine Authentication Capabilities）、第１３／７３０，７７６号、複数の認証装置で効率的に名簿登録、登録、認証するためのシステム及び方法（System and Method for Efficiently Enrolling, Registering, and Authenticating With Multiple Authentication Devices）、１３／７３０，７８０、認証フレームワーク内でランダムチャレンジを処理するためのシステム及び方法（System and Method for Processing Random Challenges Within an Authentication Framework）、第１３／７３０，７９１号、認証フレームワーク内でプライバシークラスを実行するためのシステム及び方法（System and Method for Implementing Privacy Classes Within an Authentication Framework）、第１３／７３０，７９５号、認証フレームワーク内でトランザクションシグナリングを実行するためのシステム及び方法（System and Method for Implementing Transaction Signaling Within an Authentication Framework）、及び、第１４／２１８，５０４号、高度認証技術及びアプリケーション（Advanced Authentication Techniques and Applications）（以下「’５０４出願」）に記載されている。

【０００４】

手短に言うと、同時係属中の出願は、ユーザがクライアント装置上で生体認証装置（例えば、指紋センサ）などの認証装置（又は認証部）に登録される認証技術を記載している。ユーザが生体認証装置に登録されるとき、生体認証参考データが、（例えば、指をスワイプする、写真をスナップする、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、ネットワーク上で１つ以上のサーバ（例えば、同時係属中の出願で説明されているようにセキュアなトランザクションサービスが装備されたウェブサイト又は他の信頼できる当事者）に認証装置を登録して、その後、登録プロセス中に交換されるデータ（例えば、認証装置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信頼できる当事者と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において、ユーザを固有に識別するために使用可能な指紋データ及び他のデータなどの機密情報は、ユーザのプライバシーを保護するためにユーザの認証装置上でローカルに保持されてもよい。’５０４出願は、ほんの少数を挙げると、複合認証部を設計し、非侵入式ユーザ検証を用いて認証保証レベルをインテリジェントに生成し、新しい認証装置に認証データを転送し、クライアントリスクデータで認証データを増強し、及び、認証ポリシーを適応的に適用し、及び、トラストサークルを作成する技術を含む様々な更なる技術を記載している。

【図面の簡単な説明】

【０００５】

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１Ａ】セキュアな認証システムアーキテクチャの２つの異なる実施形態を図示している。

【図１Ｂ】セキュアな認証システムアーキテクチャの２つの異なる実施形態を図示してい

る。
【図２】鍵を認証装置に登録することができる方法を示すトランザクション図である。
【図３】遠隔認証を示すトランザクション図を図示している。
【図４】信頼できる当事者で認証する本発明の１つの実施形態を図示している。
【図５】登録又は認証動作がクエリポリシーで実行することができる方法を図示している。
【図６】異なるチャネル上で強力な認証イベントを伝えるシステムの１つの実施形態を図示している。
【図７】異なるチャネル上で強力な認証イベントを伝えるシステムの別の実施形態を図示している。
【図８】異なるチャネル上で強力な認証イベントを伝えるシステムの別の実施形態を図示している。
【図９】高度な認証でネットワーク装置上で強力な認証イベントを伝えるシステムの実施形態を図示している。
【図１０】異なるチャネル上で強力な認証イベントを伝える方法の実施形態を図示している。
【図１１】クライアント及び／又はサーバ計算装置アーキテクチャの実施形態を図示している。かつ
【図１２】クライアント及び／又はサーバ計算装置アーキテクチャの別の実施形態を図示している。
【発明を実施するための形態】
【０００６】
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、方法及び機械読み取り可能な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、多数の特定の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、これらの特定の詳細の一部がなくても実施でき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、周知の構造及び装置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。
【０００７】
以下に説明する本発明の実施形態には、生体モダリティ又はＰＩＮ入力などのユーザ検証機能を備えた認証装置が含まれる。これらの装置は、「トークン」、「認証装置」又は「認証部」と称される場合がある。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）を含む追加の生体認証装置を利用することができる。ユーザ検証機能としては、また、ＰＩＮ入力のような非生体モダリティを挙げることができる。認証部は、暗号動作及び鍵保管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エレメントのようなデバイスを使用することがあり得る。
【０００８】
モバイル生体認証の実装において、生体認証装置は、信頼できる当事者から遠隔にあってもよい。本明細書では、「遠隔」という用語は、生体認証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区域の一部ではない（例えば、依拠当事者の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、生体認証装置は、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、その他）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、その装置が依拠当事者（例えば、認証及び完全性保護の許容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／又はハッカーが生体認証装

置を侵入又は入れ替えさえ行っ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。生体認証装置における信頼性は、デバイスの特定の実装に依存する。

【０００９】

「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装置とのネットワークを介した通信などの非位置要素を含むことができる。更に、特定の実施形態が（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。

【００１０】

「信頼できる当事者」という用語は、時々、単にユーザのトランザクションを実行しようとしているエンティティ（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）のみならず、本明細書に記載された基礎となる認証技術を実行することができるそのエンティティの代わりに実装されるセキュアトランザクションサーバを指すために本明細書において使用される。セキュアトランザクションサーバは、所有される及び／又は信頼できる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信頼できる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。

【００１１】

「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、１つ以上の操作を応答性よく実行し、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装置）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おけ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。

【００１２】

例示的なシステムアーキテクチャ

図１Ａ～Ｂは、ユーザ認証に関して、クライアント側及びサーバ側の構成要素を含むシステムアーキテクチャの２つの実施形態を例示する。図１Ａに示される実施形態は、ウェブサイトと通信するためのブラウザプラグインベースのアーキテクチャを用いる一方で、図１Ｂで示される実施形態は、ブラウザを必要としない。認証装置にユーザを登録する、セキュアなサーバに認証装置を登録する、及び、ユーザを検証するなどの本明細書で記載される様々な技術は、これらのシステムアーキテクチャのいずれか上で実行されてよい。したがって、図１Ａに示すアーキテクチャは、以下で記載される実施形態のいくつかの動作を明示するために使用されるが、同じ基本原理は、（例えば、サーバ１３０とクライアント上のセキュアな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を除去することにより）図１Ｂに示すシステム上で容易に実行され得る。

【００１３】

図１Ａを参照すると、図示された実施形態は、エンドユーザを登録及び認証するための１つ以上の認証装置１１０～１１２を備えたクライアント１００を含む。上述したように、認証装置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、ユーザの音声を認識するためのマイクロフォン及び関連するソフトウェア）、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関連するソフトウェア）、及び、光学認識機能（例えば、ユーザの網膜をスキャンするための光ス

キャナ及び関連するソフトウェア）などの生体認証装置、並びに、ＰＩＮ検証など、非生体モダリティのサポートを含むことができる。認証装置は、暗号の動作及び鍵保管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、又は、セキュアエレメントを使用することがあり得る。

【００１４】

認証装置１１０～１１２は、セキュアトランザクションサービス１０１によって公開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、即ちＡＰＩ）を介してクライアントに通信可能に接続されている。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と通信を行い且つウェブブラウザ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とアプリケーションである。図示されたように、インターフェース１０２はまた、装置識別コードなどの認証装置１１０～１１２のそれぞれに関連する情報、ユーザ識別コード、認証装置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生体データ）、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装置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１２０に対するセキュア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、認証装置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。

【００１５】

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つの実施形態において、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内のウェブサーバ１３１（以下では単に「サーバ１３０」として時々称される）によってウェブページのＨＴＭＬコード内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、オンプレミス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）又はオフプレミス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。

【００１６】

セキュアトランザクションサーバ１３２～１３３は、ユーザデータ、認証装置データ、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。しかしながら、本発明の基本原理は、図１Ａに示される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内の論理的な構成要素の分離を必要としないことに留意すべきである。例えば、ウェブサイト１３１及びセキュアトランザクションサーバ１３２－１３３は、単一の物理サーバ又は他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。

【００１７】

上述したように、本発明の基本原理は、図１Ａに示されるブラウザベースアーキテクチャに限定されるものではない。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ために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施形態を示している。１つの実施形態において、アプリケーション１５４は、以下に詳細に説明したユーザ／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。

【００１８】

図１Ａ～Ｂに示された実施形態のいずれかにおいて、セキュアトランザクションサーバ１３２～１３３は、その後に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送信され且つセキュア記憶装置１２０内の認証装置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。

【００１９】

デバイス登録及びトランザクション確認

本発明の１つの実施形態において、クライアントと認証サービスとの間の強力な認証は、異なるチャネル上で（例えば、異なる信頼できる当事者に）伝えられる。この点を踏まえて、認証サービスに対する登録及び認証に関連した特定の基本原理を図２～５に関して記載し、次に、異なるチャネル上で強力な認証を伝える本発明の実施形態の詳細な説明を行う。

【００２０】

図２は、認証装置の登録のための一連のトランザクションを図示している。登録時に、鍵は認証装置とセキュアトランザクションサーバ１３２～１３３のうちの１つとの間で共有される。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内に記憶される。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。しかしながら、以下に説明する他の実施形態において、非対称鍵を使用することができる。本実施形態において、公開鍵は、セキュアトランザクションサーバ１３２～１３３によって記憶されることができ、第２の関連する秘密鍵は、クライアントのセキュア記憶装置１２０に記憶されることができる。更に、別の実施形態において、鍵は、（例えば、セキュアトランザクションサーバ１３２～１３３よりもむしろ認証装置又は認証装置インターフェースによって）クライアント１００上に生成されることができる。本発明の基本原理は、任意の特定のタイプの鍵又は鍵を生成する方法に限定されるものではない。

【００２１】

動的対称鍵プロビジョニングプロトコル（ＤＳＫＰＰ）などのセキュア鍵プロビジョニングプロトコルはセキュア通信チャンネルを介してクライアントと鍵を共有するために使用することができる（例えば、コメントについての要求（ＲＦＣ）６０６３を参照）。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限定されるものではない。

【００２２】

図２に示される具体的な詳細を参照すると、ユーザ登録やユーザ検証が完了すると、サーバ１３０は、装置登録時にクライアントによって提示されなければならないランダム生成チャレンジ（例えば、暗号化ナンス）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る。セキュアトランザクションプラグインは、ランダムチャレンジを検出し、それをセキュアトランザクションサービス１０１に転送する。それに応答して、セキュアトランザクションサービスは、サーバ１３０（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のセッションを開始し、鍵プロビジョニングプロトコルを使用してサーバ１３０と通信する。サーバ１３０は、ユーザ名によってユーザを配置し、ランダムチャレンジを検証し、１つが送信された場合には装置の認証コードを検証し、ユーザのためにセキュアトランザクションデータベース１２０に新たなエントリを作成する。それはまた、鍵を生成し、データベース１２０に鍵を書き込み、鍵プロビジョニングプロトコルを使用してセキュアトランザクションサービス１０１に鍵を返送することができる。完了すると、認証装置及びサーバ１３０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。

【００２３】
図３は、登録された認証装置によるユーザ認証のための一連のトランザクションを図示している。装置登録が完了すると、サーバ１３０は、有効な認証トークンとしてローカル認証装置によって生成されたトークンを受け入れる。
【００２４】
ブラウザベースの実装を示す図３に示される特定の詳細を参照すると、ユーザは、ブラウザ１０４においてサーバ１３０のユニフォームリソースロケータ（ＵＲＬ）を入力する。（ブラウザよりもむしろ）スタンドアロンアプリケーション又はモバイル装置アプリケーションを使用する実装において、ユーザは、ネットワークサービス又はアプリケーションについてのネットワークアドレスを入力することができ、アプリケーションは、ネットワークアドレスにおけるネットワークサービスに自動的に接続しようとすることができる。
【００２５】
ブラウザベースの実装について、ウェブサイトは、ＨＴＭＬページにおいて登録された装置のためのクエリを埋め込む。これは、Ｊａｖａｓｃｒｉｐｔ（登録商標）を介して又はＨＴＴＰヘッダを使用してなど、ＨＴＭＬページにクエリを埋め込む以外の多くの方法で行うことができる。セキュアトランザクションプラグイン１０５は、ＵＲＬを受信し、（上述したように、認証装置及びユーザ情報データベースを含む）セキュア記憶装置１２０内を検索し且つこのＵＲＬ内に登録されたユーザが存在するかどうかを判定するセキュアトランザクションサービス１０１にそれを送信する。そうである場合、セキュアトランザクションサービス１０１は、セキュアトランザクションプラグイン１０５に対してこのＵＲＬに関連付けられている提供された装置のリストを送信する。そして、セキュアトランザクションプラグインは、登録されたＪａｖａＳｃｒｉｐｔ（登録商標）　ＡＰＩを呼び出し、サーバ１３０（例えば、ウェブサイト）にこの情報を渡す。サーバ１３０は、送信された装置リストから適切な装置を選択し、ランダムチャレンジを生成し、装置情報を送信し、クライアントに対して主張し返す。ウェブサイトは、対応するユーザインターフェースを表示し、ユーザからの認証を要求する。そして、ユーザは、（例えば、指紋リーダ上での指スワイプ、音声認識のための発話など）要求された認証手段を提供する。セキュアトランザクションサービス１０１は、ユーザを識別し（このステップは、ユーザ記憶をサポートしていない装置のために省略することができる）、データベースからユーザ名を取得し、鍵を使用して認証トークンを生成し、セキュアトランザクションプラグインを介してウェブサイトにこの情報を送信する。サーバ１３０は、セキュアトランザクションデータベース１２０からユーザを識別し、（例えば、その鍵のコピーを使用して）サーバ１３０において同じトークンを生成することによってトークンを検証する。検証されると、認証処理は完了する。
【００２６】
図４は、クライアントがチャレンジが満了したことを自動的に検出して、新しいチャレンジをサーバに透過的に（即ち、ユーザの介入なしに）要求する認証プロセスの別の実施形態を図示している。そして、サーバは、新たなランダムチャレンジを生成し、その後にサーバとのセキュア通信を確立するためにそれを使用することができるクライアントにそれを送信する。ユーザは認証要求のエラー又は拒否を受信しないため、エンドユーザ体験が改善される。
【００２７】
４５１において、ユーザは、ブラウザ１０４に特定のウェブサイトのＵＲＬを入力し、セキュアトランザクションサーバ１３２～１３３を含む企業／ウェブデスティネーションサーバ１３０内のウェブサーバ１３１に向けられる。４５２において、クエリは、ウェブサイトのＵＲＬに登録される装置を判定するために（ブラウザ及びプラグインを介して）セキュアトランザクションサービスに返送される。セキュアトランザクションサービス１０１は、４５３において、サーバ１３０に返送される装置のリストを識別するためにクライアント１００におけるセキュア記憶装置７２０をクエリする。４５４において、サーバ

４５４は、認証に使用する装置を選択し、ランダムチャレンジ及びタイムアウト指示を生成し、４５５において、セキュアトランザクションサービス１０１にこの情報を返送する。

【００２８】

４５６において、セキュアトランザクションサービス４５６は、タイムアウト期間の終わりに到達してランダムチャレンジがもはや有効でないことを自動的に検出する。タイムアウト期間の終了を表示及び検出する様々な異なる技術を採用することができる。１つの実施形態において、タイムアウト期間は、ランダムなチャレンジが有効とみなされる期間を含む。タイムアウト期間が経過した後、ランダムチャレンジは、もはやサーバ１３０によって有効とみなされない。１つの実施形態において、タイムアウト期間は、ランダムチャレンジがもはや有効でなくなる時点として単純に指定される。この時点に到達すると、ランダムチャレンジは無効である。他の実施形態において、タイムアウト期間は、現在のタイムスタンプ（すなわち、ランダムチャレンジがサーバ１３０によって生成された時間）及び持続時間を使用して指定される。そして、セキュアトランザクションサービス１０１は、ランダムチャレンジが無効になる時点を計算するためにタイムスタンプに持続時間値を追加することによってタイムアウト時間を計算することができる。しかしながら、本発明の基本原理は、タイムアウト期間を計算するための任意の特定の技術に限定されるものではないことに留意すべきである。

【００２９】

４５７において、ランダムチャレンジの終了を検出すると、セキュアトランザクションサービス１０１は、透過的に（すなわち、ユーザの介入なしで）サーバ１３０に通知し、新たなランダムチャレンジを要求する。応答として、４５８において、サーバ１３０は、新たなランダムチャレンジ及び新たなタイムアウト期間の指示を生成する。上述したように、新たなタイムアウト期間は、以前にクライアントに送信されたものと同じとすることができるか又は変更されることができる。いずれの場合においても、４５９において、新たなランダムチャレンジ及びタイムアウト指示がセキュアトランザクションサービス１０１に送信される。

【００３０】

図４に示されるトランザクション図の残りは、実質的に上述した方法と同様に動作する（例えば、図３を参照）。例えば、４６０において、認証ユーザインターフェースが表示され（例えば、指紋センサ上で指をスワイプするようにユーザを導く）、４６１において、ユーザは、認証を提供する（例えば、指紋スキャナ上で指をスワイプする）。４６２において、セキュアトランザクションサービスは、ユーザの身元を検証し（例えば、セキュア記憶装置７２０に記憶されたものとユーザから収集された認証データを比較する）、ランダムチャレンジを暗号化するために認証装置に関連付けられた鍵を使用する。４６３において、ユーザ名（又は他のＩＤコード）及び暗号化されたランダムチャレンジがサーバ１３０に送信される。最後に、４６４において、サーバ１３０は、ユーザ名（又は他のＩＤコード）を使用してセキュアトランザクションデータベース１２０内のユーザを識別し、認証処理を完了するために、セキュアトランザクションデータベース１２０に記憶された鍵を使用してランダムチャレンジを復号／検証する。

【００３１】

図５は、これらの技術を実装するためのクライアント－サーバアーキテクチャの１つの実施形態を図示している。図示されたように、クライアント１００に実装されたセキュアトランザクションサービス１０１は、サーバ１３０によって提供されたポリシーを分析し、登録及び／又は認証に使用される認証機能のサブセットを識別するためのポリシーフィルタ４０１を含む。１つの実施形態において、ポリシーフィルタ４０１は、セキュアトランザクションサービス１０１のコンテキスト内で実行されるソフトウェアモジュールとして実装される。しかしながら、更に本発明の基本原理を順守しながら、ポリシーフィルタ４０１は、任意の方法で実装されてもよく、ソフトウェア、ハードウェア、ファームウェア又はそれらの任意の組み合わせを含むことができることに留意すべきである。

【００３２】
図５に示される特定の実装は、上述した技術を使用してセキュア企業又はウェブデスティネーション１３０（単に「サーバ１３０」又は「信頼できる当事者」１３０と時々称する）との通信を確立するためのセキュアトランザクションプラグイン１０５を含む。例えば、セキュアトランザクションプラグインは、ウェブサーバ１３１によってＨＴＭＬコードに挿入された特定のＨＴＭＬタグを識別することができる。そえゆえに、本実施形態において、サーバポリシーは、ポリシーフィルタ５０１を実装するセキュアトランザクションサービス１０１にそれを転送するセキュアトランザクションプラグイン１０５に提供される。
【００３３】
ポリシーフィルタ５０１は、クライアントのセキュア記憶領域５２０から機能を読み出すことによってクライアント認証機能を決定することができる。上述したように、セキュア記憶装置５２０は、全てのクライアントの認証機能（例えば、認証装置の全ての識別コード）のリポジトリを含むことができる。ユーザが既にその認証装置にユーザを登録している場合、ユーザの登録データは、セキュア記憶装置５２０内に記憶される。クライアントが既にサーバ１３０に認証装置を登録している場合、セキュア記憶装置はまた、各認証装置に関連する暗号化された秘密鍵を記憶することができる。
【００３４】
セキュア記憶装置５２０から抽出される認証データ及びサーバによって提供されるポリシーを使用して、ポリシーフィルタ５０１は、その後、使用される認証機能のサブセットを識別することができる。構成に応じて、ポリシーフィルタ５０１は、クライアント及びサーバの双方によってサポートされている認証機能の完全なリストを識別することができるか又は完全なリストのサブセットを識別することができる。例えば、サーバが認証機能Ａ、Ｂ、Ｃ、Ｄ及びＥをサポートし、クライアントが認証機能Ａ、Ｂ、Ｃ、Ｆ及びＧを有する場合、ポリシーフィルタ５０１は、サーバに対する共通の認証機能のサブセット全体を識別することができる。あるいは、図５のユーザ設定５３０に示されるように、より高いレベルのプライバシーを望む場合、認証機能のより限定したサブセットをサーバに対して識別することができる。例えば、ユーザは、単一の共通の認証機能がサーバ（例えば、Ａ、Ｂ又はＣのいずれか）に対して識別されるべきであるにすぎないことを示すことができる。１つの実施形態において、ユーザは、クライアント１００の認証機能の全てについて優先順位付け方式を確立することができ、ポリシーフィルタは、サーバ及びクライアントの双方に共通の優先順位の最も高い認証機能（又はＮ個の認証機能の優先順位のセット）を選択することができる。
【００３５】
何の動作がサーバ１３０（登録又は認証）によって開始されかに応じて、図５に示されるように、セキュアトランザクションサービス１３０は、認証装置のフィルタリングされたサブセット（１１０～１１２）においてその動作を実行し、セキュアトランザクションプラグイン１０５を介してサーバ１３０に動作応答を返送する。あるいは、ウェブブラウザのプラグイン１０５構成要素に依存しない実施形態において、情報は、セキュアトランザクションサービス１０１からサーバ１３０に対して直接送られてもよい。
【００３６】
異なるチャネル上で強力な認証を伝えるためのシステム及び方法
１つの実施形態において、信頼できる当事者は、該信頼できる当事者が認証部モデルについセキュリティ特性を導出することができる認証に使用された認証部モデルの暗号証明を受信することができる。信頼できる当事者のウェブアプリケーションは、例えば、導出されたセキュリティ特性を使用することができる。例えば、銀行は、認証保証レベルが中である場合には口座状態を表示するにすぎないことがあり得、認証保証レベルが高である場合に限り、金融取引を可能にすることがあり得る。別の実施例として、法人は、認証保証レベルが中である場合に限り、電子メールへのアクセスを許可することができ、認証保証レベルが高である場合に限り、機密ファイルリポジトリへのアクセスを許可することが

できる。

【００３７】

何を「中間保証レベル」又は「高保証レベル」とみなすかは、領域及び垂直位置立てに左右される。米国の金融機関は、欧州連合（ＥＵ）、アフリカ、及び、アジアの金融機関と異なる規制に従わなければならない。電子商取引ウェブサイトは、やはり、認証保証レベルに関する異なる規制（又は皆無）に従わなければならない。しかし、それらの金融機関は、通常、特定のトランザクションについて何が容認可能な保証レベルとみなされるかについて、独自の考え方又は正式な方針さえ有する。正式な定義の例が、存在する（例えば、米国連邦機関について確立されたＳＰ－８００－６２３－２を参照されたい）。時には、そのようなポリシーとしては、識別強度（例えば、「顧客確認」（ＫＹＣ）ポリシーなど）の定義が挙げられる。そのような識別強度は、領域及び垂直位置固有のものでさえある。

【００３８】

実際の世界信頼できる当事者は、複雑なコンピューティングインフラ及びネットワークインフラを有することが多い。時には、信頼できる当事者は、（ａ）該当事者独自のデータセンタにおいてそのような認証サーバを操作したくないと考える場合があるか、又は、（ｂ）認証を１つの場所を集中させ、その後、認証されたデータを保護されたネットワークを介して最終的なＷｅｂサービスに送りたいと考える場合がある。

【００３９】

これらのニーズに対応するために、１つの実施形態において、信頼できる当事者により提供される１つ以上のＷｅｂサービスにアクセスしようとするクライアント装置は、初めに専用認証サーバ／サービスで認証される。認証成功に応答して、認証サーバは、認証成功の証明を含む認証トークンをクライアント装置に送信する。１つの実施形態において、トークンは、ユーザのアイデンティティ及びユーザがアクセスしようとしているＷｅｂサービスのアイデンティティ（例えば、ユーザ「ジョン・ドウ」及びＷｅｂサービス「ＸＹＺ」）の両方に関して生成された署名を含む。クライアント装置は、その後、ユーザが失敗せずに認証したという証明としてトークンをＷｅｂサービスに提示する。

【００４０】

１つの実施形態において、クライアント装置は、また、トークン内に含まれるか、又は、トークンとは別々に送られるかを問わず、ユーザを認証するために使用された認証装置に関係する詳細をＷｅｂサービスに提供する。例えば、クライアント装置は、認証部証明ＩＤ（ＡＡＩＤ）などの、ユーザを認証するために使用された認証部の形式を独自に識別する識別子を提供することができる。この実施形態において、クライアント装置内で使用されたそれぞれの異なった認証部の形式は、ＡＡＩＤにより識別することができる。信頼できる当事者は、その後、ＡＡＩＤを使用して、認証部の形式を識別して、使用された認証部の形式に基づいて認証ポリシーを実行することができる。

【００４１】

図６は、本発明の実施形態を実施することができる例示的なクライアント装置６００を図示している。特に、この実施形態は、認証サービス６５１と認証を調整し、トークンを受信し、かつ、認証成功に応答してＷｅｂサービス６５２にトークン（及び、他の情報）をその提示する多チャンネル認証モジュール６０４を含む。図示された実施形態は、また、合法的なユーザがクライアント装置６００を所有しているという保証レベルを生成する保証計算モジュール６０６を伴う認証エンジン６１０を含む。例えば、明示的及び非侵入式の認証結果６０５が、明示的なユーザ認証装置６２０～６２１、１つ以上のセンサ６４３（例えば、場所センサ、加速度計など）、及び、（例えば、最終の明示的認証以来の時間など）クライアント装置６００の現在の認証状態に関係する他のデータを使用して収集される。図６において別個のモジュールとして図示されていが、認証エンジン６１０及び多チャネル認証モジュール６０４は、本明細書に記載された動作の全てを実行する単一のモジュールとして実装することができる。

【００４２】

明示的認証は、例えば、生体技術を使用して（例えば、指紋認証装置上で指をスワイプする、画像をキャプチャするなどして）、及び／又は、ユーザが秘密のコードを入力することにより実行することができる。非侵入式の認証技術は、（例えば、ＧＰＳセンサを介した）クライアント装置６００の現在の検出された位置などのデータ、他の感知されたユーザ挙動（例えば、加速度計でのユーザの歩行運動の測定）、及び／又は、明示的な最終認証以来の時間などの変数に基づいて実行することができる。認証結果６０５が生成される方法に関係なく、保証計算モジュール６０６は、結果を使用して、合法的なユーザ６５０がクライアント装置６００を所有している可能性を示す保証レベルを判定することができる。１つの実施形態において、保証レベルを生成する代わりに、認証エンジン６１０は、認証結果がユーザを認証するのに十分である（例えば、明示的及び／又は黙示的認証結果に基づいて指定の閾値を上回る）かどうか単に判断することができる。そうであるならば、認証は成功であり、そうでなければ、認証は不成功であり、及び／又は、更なる認証は要求される。

【００４３】

セキュアな通信モジュール６１３が、認証サービスとのセキュアな通信を確立して認証の結果を提供する。例えば、認証レベルが指定の閾値を上回る場合、ユーザを、信頼できる当事者信頼できる当事者６１３に対して（例えば、本明細書で論じるようにセキュアな暗号化キーを使用して）失敗せずに認証することができる。公開鍵／秘密鍵対、又は、対称鍵を、暗号によりセキュアなハードウェア装置（例えば、セキュリティチップ）として実装することができるセキュアな記憶装置６２５に、又は、セキュアなハードウェア及びソフトウェアの任意の組み合わせを使用して記憶することができる。

【００４４】

１つの実施形態において、認証エンジン６１０を使用した認証の成功に応答して、認証サービス６５１は、多チャネル認証モジュール６０４にトークンを送信する。上述したように、トークンは、ユーザのアイデンティティ、及び、ユーザがアクセスしようとしているＷｅｂサービスのアイデンティティの両方に関して生成された署名を含むことができる。多チャネル認証モジュール６０４は、その後、ユーザが失敗せずに認証された証明としてＷｅｂサービス６５２にトークンを提示する。更に、多チャネル認証モジュール６０４は、ユーザを認証するために使用された認証装置に関係する詳細（例えば、デバイスのＡＡＩＤ）を提供することができる。

【００４５】

１つの実施形態において、Ｗｅｂサービス６５２は、ＡＡＩＤなどの詳細を使用して、認証ポリシーデータベース６９０に問い合わせて、詳細に基づいて認証ポリシーを実行する。１つの実施形態において、認証ポリシーデータベース９６０は、全ての既存の認証装置、種々のクラスの認証装置、種々のクラスの相互作用及び認証ルール（その実施例は、以下で論じる）のメタデータを含む。一般に、それぞれの信頼できる当事者は、履歴上重要なトランザクション及び／又は既知のデバイス機能に基づいて内部のリスク計算結果を使用して独自の認証ポリシーを実行することができる。

【００４６】

既存のデバイスのメタデータは、例えば、ファーストアイデンティティオンラインアライアンス仕様により（例えば、［ＦＩＤＯＵＡＦＭｅｔａｄａｔａ］として）定義されるように指定することができるが、本発明の基本原理は、特定の形式のメタデータに関係するものではない。メタデータとしては、それぞれの認証装置の信頼性及び精度に関係する特定のモデル情報及びデータを挙げることができる。例えば、「妥当性モデル１２３」指紋センサの記入事項は、センサが極秘データ（例えば、暗号によりセキュアなハードウェアにおいて、ＥＡＬ　３証明など）、及び、（ユーザ認証結果を生成するとき、センサがどれくらい信頼性があるかを示す）他人受入率を記憶する方法などのこのセンサに関係する技術的な詳細を含むことができる。

【００４７】

１つの実施形態において、データベース６９０に明記された認証装置クラスは、それら

のデバイスの機能に基づいて認証装置を論理的にグループ化することができる。例えば、ある特定の認証装置クラスは、（１）指紋センサ、（２）ＥＡＬ　３認定されている暗号的にセキュアなハードウェア内に機密データを記憶すること、及び、（３）１０００分の１以下の他人受入率による生体照合処理を使用することについて定義されることができる。別の例示的な装置クラスは、（１）顔認識装置、（２）暗号的にセキュアなハードウェア内に機密データを記憶せず、及び、（３）５００分の１以下の他人受入率による生体照合処理を使用することができる。それゆえに、上記基準を満たしている指紋センサ又は顔認識の実装は、データベース内の適切な認証装置クラス６９０に追加される。

【００４８】

様々な個人属性は、認証要素（例えば、指紋、ＰＩＮ、顔）の種類などの認証装置クラス、ハードウェアのセキュリティ保証のレベル、秘密の記憶位置、認証部によって暗号化操作が行われる位置（例えば、セキュアチップ又はセキュア筐体内）、及び様々な他の属性を定義するために使用することができる。使用することができる属性の他のセットは、「照合」操作が実行されているクライアント上の位置に関連する。例えば、指紋センサは、指紋センサ自体のセキュア記憶装置における指紋テンプレートのキャプチャ及び記憶を実装することができ、指紋センサハードウェア自体内でそれらのテンプレートに対して全ての検証を行い、高いセキュア環境をもたらす。あるいは、指紋センサは、単に指紋の画像をキャプチャするが、全てのキャプチャ、記憶及び比較操作を実行するためにメインＣＰＵ上でソフトウェアを使用する周辺機器とすることができ、あまりセキュアな環境をもたらさない。「照合」の実装に関連する様々な他の属性はまた、認証装置クラスを定義するために使用することができる（例えば、照合がセキュア要素、信頼された実行環境（ＴＥＥ）又は他のセキュアな実行環境の形態において行われる（又は行われない）かどうか）。

【００４９】

もちろん、これらは、単に認証装置クラスの概念を説明するための一例である。更に基本原理を順守しながら、様々な追加の認証装置クラスを指定することができる。更に、認証装置クラスが定義されている方法に応じて、単一の認証装置は、複数の装置クラスに分類されてもよいことに留意すべきである。

【００５０】

１つの実施形態において、ポリシーデータベース６９０は、新たな認証装置を分類することができる新たなクラスを潜在的に含む新たな認証装置クラスとともにそれらが市場に出るときに新たな認証装置についてのデータを含むように定期的に更新することができる。更新は、信頼できる当事者によって及び／又は信頼できる当事者のために更新を提供する責を負う第三者（例えば、信頼できる当事者によって使用されるセキュアトランザクションサーバプラットフォームを販売している第三者）によって行われることができる。

【００５１】

１つの実施形態において、相互作用クラスは、信頼できる当事者によって提供される特定のトランザクションに基づいて定義される。例えば、信頼できる当事者が金融機関である場合、相互作用は、トランザクションの金銭的価値に応じて分類することができる。「高値相互作用」は、５０００ドル以上の金額が関与する相互作用（例えば、振り込み、引き出しなど）と定義することができ、「中央値相互作用」は、５００ドル～４９９９ドルの金額が関与する相互作用と定義することができ、「低値トランザクション」は、４９９ドル以下の金額が関与するトランザクション（又は、金銭的なトランザクションを伴わないトランザクション）と定義することができる。

【００５２】

関与する金額に加えて、相互作用クラスは、関与するデータの感度に基づいて定義されてもよい。例えば、ユーザの機密又はプライベートデータを開示するトランザクションは、「機密開示相互作用」として分類することができるのに対して、そのようなデータを開示しないものは、「非機密開示相互作用」として定義することができる。様々な他の種類の相互作用は、異なる変数並びに様々な最小値、最大値及び中間レベルを使用して定義す

ることができる。

【００５３】

最後に、認証ルールのセットは、認証装置、認証装置クラス及び／又は相互作用クラスを含むように定義することができる。例示として、限定されるものではないが、特定の認証ルールは、（相互作用クラスによって指定されたような）「高価値トランザクション」について、ＥＡＬ　３認定された暗号的にセキュアなハードウェアに検知データを記憶する指紋センサのみであること、及び、（認証装置クラスとして指定されたような）１０００分の１以下の他人受入率を有する生体照合処理が使用可能であることを指定することができる。指紋装置が利用できない場合、認証ルールは、許容される他の認証パラメータを定義することができる。例えば、ユーザは、ＰＩＮやパスワードを入力し、また、（例えば、以前に信頼できる当事者に対してユーザによって提供された）個人的な一連の質問に回答する必要があることがある。認証装置及び／又は認証装置クラスに指定された上記個人属性のいずれかは、認証要素の種類（例えば、指紋、ＰＩＮ、顔）、ハードウェアのセキュリティ保証のレベル、秘密の記憶位置、認証部によって暗号化操作が行われる位置などのルールを定義するために使用することができる。

【００５４】

代替的に又は追加的に、ルールは、他の値が十分である限り、特定の属性が任意の値をとることができることを指定することができる。例えば、信頼できる当事者は、ハードウェアにそのシードを記憶してハードウェアで計算を実行する指紋認証装置が使用されなければならないことを指定することができるが、（これらのパラメータを満たす認証装置のリストを含む認証装置クラスによって定義されているような）ハードウェアの保証レベルを気にしない。

【００５５】

更に、１つの実施形態において、ルールは、特定の認証装置が特定の種類の相互作用の認証に使用することができることを単に指定することができる。例えば、組織は、「検証モデル１２３の指紋センサ」のみが高値トランザクションについて許容可能であることを指定することができる。

【００５６】

更に、ルール又はルールのセットは、順序付けられてランク付けされた相互作用のための認証ポリシーの組み合わせを作成するために使用することができる。例えば、ルールは、個別の認証ポリシーについてのポリシーの組み合わせを指定することができ、信頼できる当事者の認証の好みを正確に反映したリッチポリシーの作成を可能とする。これは、例えば、指紋センサが好ましい旨を信頼できる当事者が指定するのを可能とするが、どれも利用できない場合は、信頼できるプラットフォームモジュール（ＴＰＭ）ベースの認証又は顔認識のいずれかが次の最良の選択肢（例えば、優先順位順）として同様に好ましい。

【００５７】

１つの実施形態において、認証ポリシーエンジン６８０は、クライアント６００とのトランザクションを許可するかどうかを判定する際に、相互作用クラス、認証装置クラス及び／又は認証機器データをあてにする認証ルールを実装する。例えば、ウェブサイト６５２とのトランザクションに入ろうとしているクライアント装置６００のユーザに応じて、認証ポリシーエンジン６９０は、適用可能な１つ以上の相互作用クラス及び関連する認証ルールのセットを識別することができる。認識ポリシーエンジン６９０は、その後、これらのルールを適用して、多チャネル認証モジュール６０４により提供されたトークンが十分であるかどうか判断することができる。トークンが十分である場合（例えば、容認可能な認証装置が現在のトランザクションに使用された場合）、クライアント装置６００は、Ｗｅｂサービス６５２とトランザクションを実行することが許可される。そうでない場合、トランザクションは拒絶され、及び／又は、更なる認証が要求される。

【００５８】

本発明の３つの異なる実施形態のアーキテクチャ上の実行例が、図７～９に図示されている。図７に示す実施形態において、高度な認証機能７００を有するクライアント装置（

例えば、上述したクライアント装置など）が、信頼できる当事者７５５の専用認証サービス７５１（例えば、１つ以上の認証サーバ）に認証される。信頼できる当事者７５５は、複数のＷｅｂサービス７５２ａ～ｃを含む。認証が成功した場合、認証サービス７５１は、ユーザ／クライアント装置のアイデンティティ及びＷｅｂサービス７５２ｃに関する署名を含む認証トークンをクライアント装置７００に戻す。更に、言及したように、トークンは、認証中に使用された形式の認証部のアイデンティティを含むことができる。クライアント装置７００は、その後、Ｗｅｂサービス７５２ｃにトークンを提示して、トランザクションを開始する。使用された認証装置が（例えば、所望のトランザクションに関する容認可能な装置クラス内で）容認可能であると想定して、Ｗｅｂサービス７５２ｃは、トランザクションを許可する。

【００５９】

図８は、信頼できる当事者がユーザを認証する認証サービス８５１を有する外部識別するプロバイダ８０１を使用する実施形態を図示している。この実施形態において、信頼できる当事者８０２は、クライアント６００にＷｅｂサービス８５２ａ～ｂを提供する前に、アイデンティティプロバイダ８０１により実行された認証を信頼する。図７に示す実施形態の場合と同様に、高度な認証機能７００を有するクライアント装置が、アイデンティティプロバイダ８０１により管理された専用認証サービス８５１に認証される。認証が成功した場合、認証サービス８５１は、ユーザ／クライアント装置のアイデンティティ及びＷｅｂサービス８５２ｃに関する署名を含む認証トークンをクライアント装置７００に戻す。更に、言及したように、トークンは、認証中に使用された形式の認証部のアイデンティティを含むことができる。クライアント装置７００は、その後、Ｗｅｂサービス８５２ｂにトークンを提示して、トランザクションを開始する。使用された認証装置が（例えば、所望のトランザクションに関する容認可能な装置クラス内で）容認可能であると想定して、Ｗｅｂサービス８５２ｂは、トランザクションを許可する。

【００６０】

図９は、信頼できる当事者９５５が高度な認証サービスを含むファイアウォール、仮想プライベートネットワーク（ＶＰＮ）装置、又は、トランスポートレイヤセキュリティ（ＴＬＳ）コンセントレータなどのネットワークレイヤ装置９５１を認証する実施形態を図示している。従来の実施形態の場合と同様に、高度な認証機能７００を有するクライアント装置は、認証成功に応答してウェブサービス９５２ｃへのアクセスが提供される。従来の実施形態とは対照的に、認証装置９５１は、クライアントがその後Ｗｅｂサービス９５２ｃにアクセスするために使用するトークンをクライアント７００に背中で提供しない。むしろ、この実施形態において、全ての認証は、ネットワークレイヤ（例えば、ＴＣＰ／ＩＰネットワーク内のＩＰパケットレイヤ）にて実行され、ネットワークレイヤ装置９５１は、Ｗｅｂサービス９５２ｃに直接にクライアント７００を接続する（例えば、クライアント７００と信頼できる当事者９５５との間の全てのネットワークトラフィックがネットワークレイヤ装置９５１中を流れるからである）。

【００６１】

１つの実施形態において、クライアント結氷を防ぐ７００が認証に成功した場合、クライアントへの／からのネットワークレイヤパケットには、関連した認証セキュリティ特性識別子（例えば、先に論じたようなＡＡＩＤなどの認証部の識別子）でタグ付けすることができる。例えば、１つの実施形態において、それぞれのＡＡＩＤは、１２ビット仮想識別子（ＶＩＤ）にマッピングされ、クライアントへの／からのそれぞれのパケットは、ＶＩＤでタグ付けされる。例えば、イサーネットネットワーク上でバーチャルＬＡＮ（ＶＬＡＮ）をサポートして、そのようなタグ付けのサポートを提供するＩＥＥＥ　８０２．１Ｑなどのネットワーク規格を使用することができる。

【００６２】

あるいは、１つの実施形態において、タグ付けは、ＨＴＴＰなどのより高位プロトコル上で行われる。これは、認証サーバ９５１が、また、ＴＬＳ終点（例えばＴＬＳコンセントレータ）としての役割を果たす場合に特に興味深い。この場合、認証装置のＡＡＩＤ（

例えば、ＡＡＩＤを含む文字列データ）を含むために新しいヘッダ部を追加することができる。このフィールドは、ユーザにより使用される認証部９５１に関係するＡＡＩＤを含む。この場合、ネットワーク装置は、そのようなヘッダ部が決して入トラフィックから直接に通過されないことを確保する。

【００６３】

上記の実施形態において、認証サーバ７５１、８５１、９５１は、Ｗｅｂサービス７５２、８５２、９５２がセキュリティ特性を要求することを可能にする更なるウェブサービスインターフェースを提供することができる。このアプローチの１つの潜在的な欠点は、認証サーバ及びネットワークに掛かる（更なるトラフィックによる）負荷の増大（即ち、サーバへの更なる要求）である。

【００６４】

したがって、（特定の領域及び垂直位置についてのみ最適化することができる）（相対的に小）数の離散的保証レベルを定義しようとし、かつ、セキュリティ特性の全ての関連の局面の説明を含もうとする代わりに、上記の実施形態は、関連のセキュリティ特性を識別する普遍的な方法を提供し、かつ、特に、個々の規制及びポリシーについて意味を判定するために一般マーケット及び信頼できる当事者７５５、８０２、９５５に任せる。

【００６５】

更に、それぞれのＷｅｂサービスが直接に認証サーバにアクセスすることを必要とする代わりに、上述の実施形態において、認証サーバは、関連のセキュリティ特性（例えば、トークン）を含む認証されたデータ構造を作成する。Ｗｅｂサービスは、その後、このデータ構造を検証して、そのコンテンツに基づいて判定を行うことができる。認証された方法で認証セキュリティ特性の識別子（例えば、ＡＡＩＤ）をトラフィック／メッセージに追加することができる。

【００６６】

図９に示すなどのインフラの場合、データ構造は、明示的に認証される必要がない場合があり、（即ち、ＤＭＺでは）そのようなファイアウォール／ＶＰＮサーバ９５１の背後のネットワークトラフィックは、典型的には「セキュアである」と考えられるからである。これは、ネットワークチャネル自体が認証されたトラフィックのみがサーバへ送信されることを保証することを意味する。

【００６７】

様々な異なる一体化オプションが、既存の認証プロトコル（例えば、同時係属中の出願及び現行のＦＩＤＯ規格に記載されたプロトコルなど）に本発明の実施形態を一体化するために企図されている。例えば、セキュリティアサーションマークアップ言語（ＳＡＭＬ）連邦プロトコルを使用するとき、認証セキュリティ特性識別子は、例えば、ＯＡＳＩＳセキュリティアサーションマークアップ言語（ＳＡＭＬ）Ｖ２．０（２００５年３月１５日）の認証コンテキストにおいて記載されるような認証コンテキストに追加することができる。オープンＩＤコネクトを使用するとき、認証セキュリティ特性識別子は、ＯｐｅｎＩＤコネクションコア１．０－ドラフト１７（２０１４年２月３日）のセクション３．２．２．１０及び３．２．２．１１で論じているように、ＩＤトークンの一部である認証方法参考文献（ＡＭＲ）に追加することができる。

【００６８】

図１０は、本発明の１つの実施形態による方法を図示している。１００１にて、ユーザは、認証サービスに対する遠隔認証を実行する。１つの実施形態において、信頼できる当事者とのトランザクションを開始しようとするときに認証サービスにユーザを再方向付けすることができる。１００２にて、（例えば、本明細書で記載される技術又は他の認証技術のいずれかを使用して）ユーザが認証に成功すると、認証サービスは、ユーザ及びサービスの識別子及び認証部ＩＤ（例えば、ＡＡＩＤ）に関する署名を含むトークンを生成してユーザに送る。１００３にて、ユーザは、成功した認証の証拠としてトークンをサービスに送る。サービスは、その後、トークン上の署名を検証し、検証が成功した場合、１００５にて判定し、その後、１００６にて、信頼できる当事者は、（例えば、ＡＡＩＤでポ

リシーデータベースに問い合わせることにより）認証に使用された認証部のアイデンティティに少なくともある程度基づくポリシーを実行する。例えば、先に論じたように、ポリシーは、特定の認証部又は種々のクラスの認証部のためにのみ特定のトランザクションを可能にするために実行することができる。１００５にて検証が失敗した場合、ランザクションは、１００７にて拒絶される。

【００６９】

例示的なデータ処理装置

図１１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１１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１１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１１００は、処理システム１１２０に結合されているバス１１５０と、電源１１２５と、メモリ１１３０と、不揮発性メモリ１１４０（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１１５０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ることができる。処理システム１１２０は、メモリ１１３０及び／又は不揮発性メモリ１１４０から命令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１１５０は、上記構成要素を一体に相互接続し、また、任意のドック１１６０、ディスプレイコントローラ及びディスプレイ装置１１７０、入力／出力装置１１８０（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１１９０（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１２は、本発明のいくつかの実施形態において使用されることができ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１２００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装置とすることができる。他の例として、データ処理システム１２００は、ネットワークコンピュータ又は他の装置内の埋め込み処理装置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１２００の例示的なアーキテクチャは、上述した携帯機器のために使用することができる。データ処理システム１２００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１２２０を含む。処理システム１２２０は、メモリ１２１０、（１つ以上のバッテリを含む）電源１２２５、オーディオ入力／出力１２４０、ディスプレイコントローラ及びディスプレイ装置１２６０、任意の入力／出力１２５０、入力装置１２７０及び無線送受信機１２３０に連結されている。図１２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１２００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１２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１２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１２１０は、データ処理システム１２００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１２４０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、及び／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装置１２６０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１２３０（例えば、ＷｉＦｉ送受信機、赤外線送受信機、ブルートゥース（登録商標）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つ以上の入力装置１２７０は、ユーザがシステムに入力を提供するのを可能とする。これらの入力装置は、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とすることができる。任意の他の入力／出力１２５０は、ドック用コネクタとすることができる。

【００７４】

上述したように、本発明の実施形態は、様々なステップを含んでもよい。ステップは、汎用又は特殊目的のプロセッサに特定のステップを実行させる機械実行可能な命令に具現化することができる。あるいは、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、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。

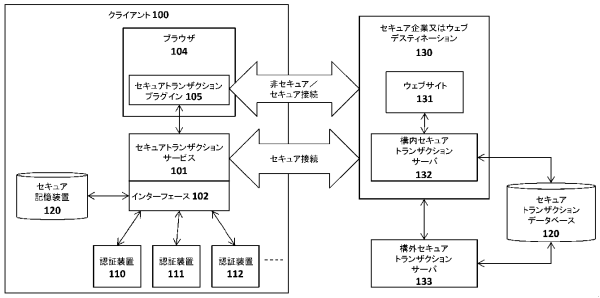
【００７６】

上記の説明全体を通じて、説明の目的のために、多数の特定の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、これらの特定の詳細の一部がなくても実施できることは、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装置は、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。

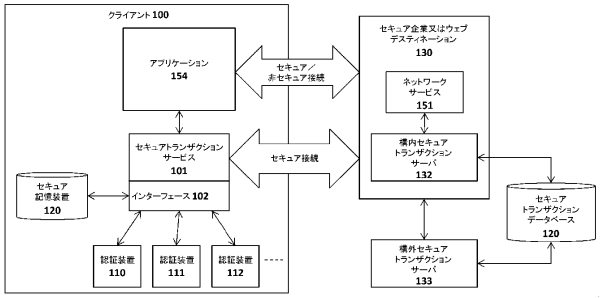
【００７７】

上述したように、本発明の実施形態は、様々なステップを含んでもよい。ステップは、汎用又は特殊目的のプロセッサに特定のステップを実行させる機械実行可能な命令に具現化することができる。あるいは、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。

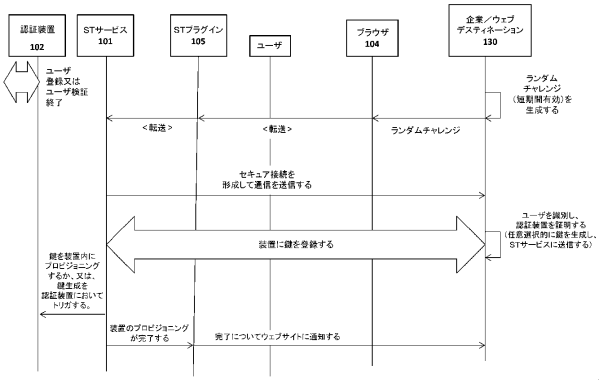
【図１Ａ】



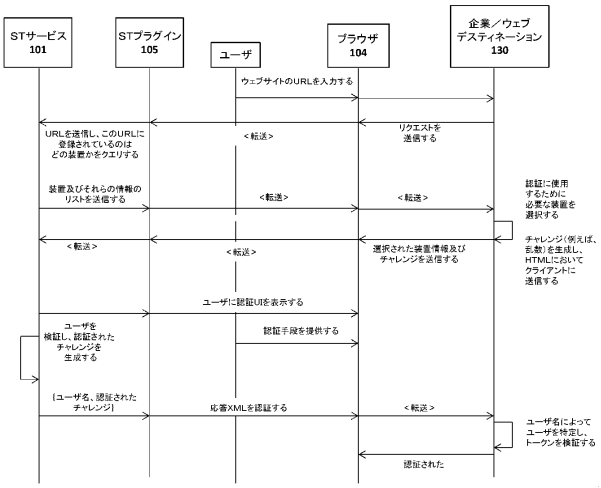
【図１Ｂ】



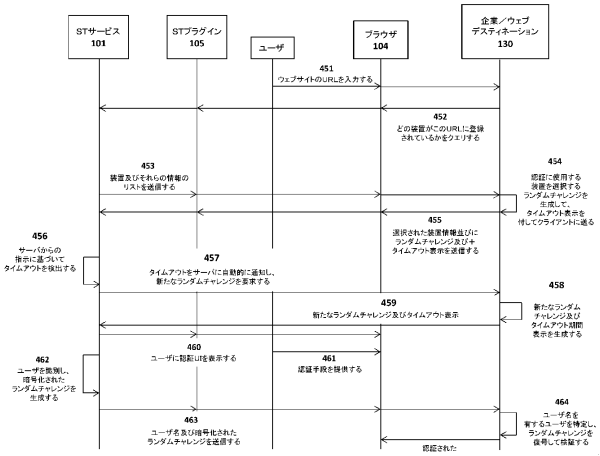
【図２】



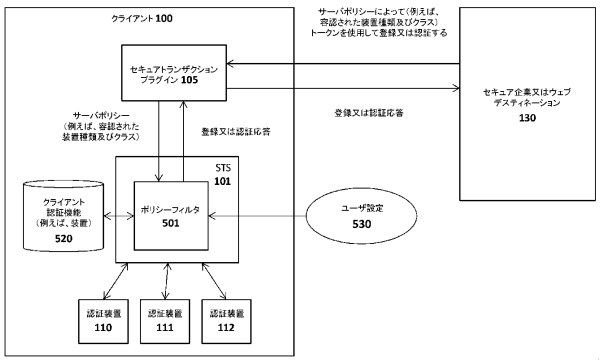
【図３】



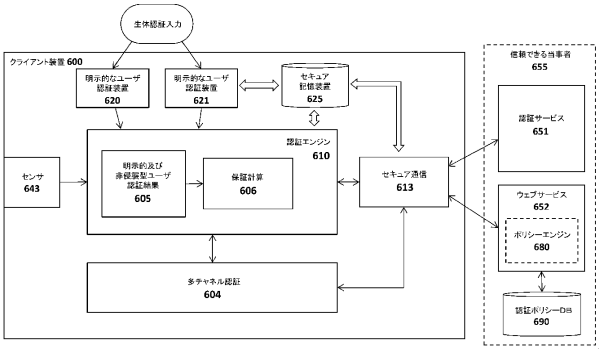
【図４】



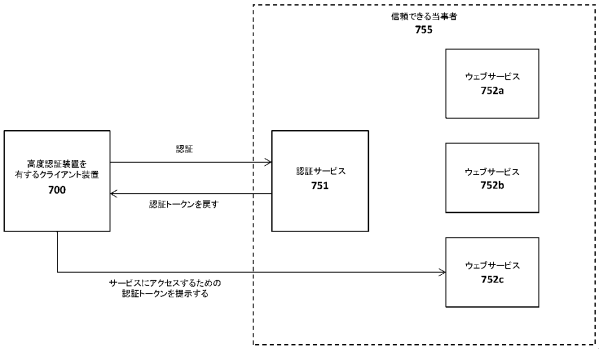
【図５】



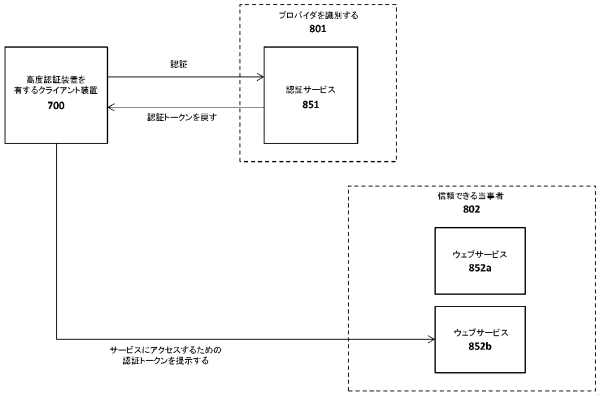
【図６】



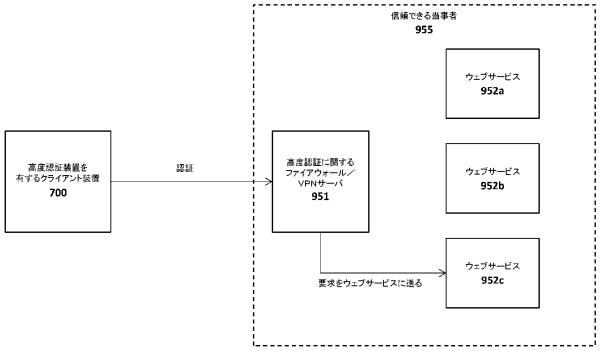
【図７】



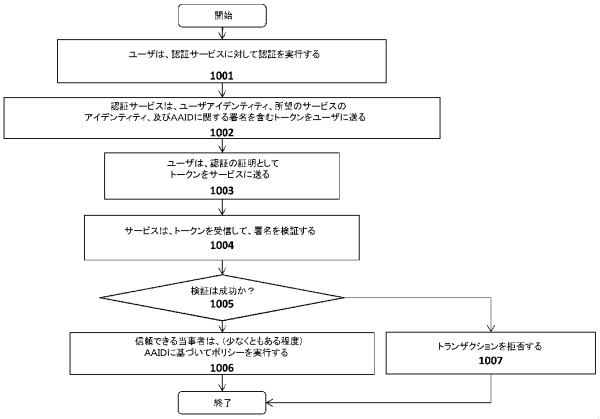
【図８】



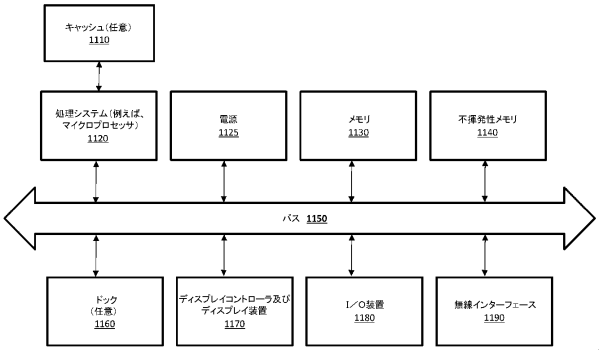
【図９】



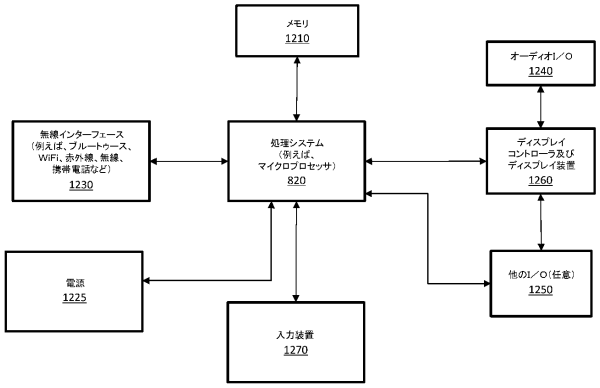
【図１０】



【図１１】



【図１２】



フロントページの続き

(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
(72)発明者 ドゥンケルバーガー フィリップ
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 リンデマン ロルフ
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 金沢 史明

(56)参考文献 特表２０１３－５２２７２２（ＪＰ，Ａ）
特開２００４－３４８３０８（ＪＰ，Ａ）
米国特許出願公開第２０１２／０１０２５５３（ＵＳ，Ａ１）

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