

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7603121号
(P7603121)

(45)発行日 令和6年12月19日(2024.12.19)

(24)登録日 令和6年12月11日(2024.12.11)

(51)国際特許分類

F I

G O 6 F 21/64 (2013.01)

G O 6 F 21/32 (2013.01)

H O 4 L 9/32 (2006.01)

G O 6 F 21/64

G O 6 F 21/32

H O 4 L 9/32 2 0 0 Z

請求項の数 11 外国語出願 (全119頁)

(21)出願番号	特願2023-164916(P2023-164916)	(73)特許権者	516329587
(22)出願日	令和5年9月27日(2023.9.27)		ノック ノック ラブズ, インコーポレ
(62)分割の表示	特願2020-546306(P2020-546306)		イテッド
	)の分割		アメリカ合衆国 カリフォルニア州 9 4
原出願日	平成30年11月27日(2018.11.27)		3 0 3 パロ アルト ジェン ロード 2
(65)公開番号	特開2023-171851(P2023-171851		1 0 0 スイート 1 0 5
	A)	(74)代理人	100094569
(43)公開日	令和5年12月5日(2023.12.5)		弁理士 田中 伸一郎
審査請求日	令和5年10月4日(2023.10.4)	(74)代理人	100103610
(31)優先権主張番号	15/822,531		弁理士 ▲吉▼田 和彦
(32)優先日	平成29年11月27日(2017.11.27)	(74)代理人	100109070
(33)優先権主張国・地域又は機関	米国(US)		弁理士 須田 洋之
		(74)代理人	100067013
			弁理士 大塚 文昭
		(74)代理人	

最終頁に続く

(54)【発明の名称】 トランザクション確認及び暗号通貨のためのセキュアな鍵記憶装置の拡張

(57)【特許請求の範囲】

【請求項 1】

システムであって、
生体認証入力、手動ユーザ入力を介して、及び／又はクライアント装置に関連する現在の状態を検出することによって、ユーザをセキュアに認証する前記クライアント装置上の認証部と、
秘密鍵のセキュア記憶を維持するための鍵ストア回路及びロジックであって、前記鍵ストア回路及びロジックは、前記ユーザが前記認証部によって認証された状態で第1の秘密鍵を使用して、前記認証部の1つ以上の属性及び入力データを含むデジタルオブジェクト上に署名するためのデジタル署名を計算し、署名されるデジタルオブジェクトは前記第1の秘密鍵に対応する公開鍵を用いて信頼できる当事者によって検証可能である、鍵ストア回路及びロジックと、を備える、システム。

【請求項 2】

前記鍵ストア回路及びロジックに統合され、前記デジタル署名を計算するために実行される差し込み可能なダイジェスト／ハッシュ回路／ロジックを更に備える、請求項 1 に記載のシステム。

【請求項 3】

前記差し込み可能なダイジェスト／ハッシュ回路／ロジックが、前記入力データを指定の方法で前処理して、前記デジタルオブジェクトを生成するための前処理回路／ロジックを含む、請求項 2 に記載のシステム。

【請求項 4】

前記ユーザからの認証を受信して前記デジタル署名を続行する前に、前記入力データに関連する有効情報をセキュアに表示するためのセキュアトランザクション回路／ロジックを更に備える、請求項 3 に記載のシステム。

【請求項 5】

前記デジタルオブジェクトは前記認証部によって制御されない 1 つ以上のデータフィールドを含む、請求項 1 に記載のシステム。

【請求項 6】

前記認証部によって制御されない 1 つ以上のデータフィールドは数でマークされ、データ構造が後に続く、請求項 5 に記載のシステム。

【請求項 7】

前記信頼できる当事者は、いずれのエンティティが前記公開鍵と前記第 1 の秘密鍵のペアを生成するかを特定するためのものである、請求項 1 に記載のシステム。

【請求項 8】

前記デジタル署名は前記ユーザを検証するためのユーザ検証方法の 1 つ以上の特性を示す、請求項 1 に記載のシステム。

【請求項 9】

前記認証部の 1 つ以上の属性及び入力データはユーザによって確認された 1 つ以上のトランザクションテキスト、実際の個人識別番号（PIN）長及び前記認証部のファームウェアバージョンを含む、請求項 1 に記載のシステム。

【請求項 10】

前記デジタルオブジェクトは前記信頼できる当事者によって検証されるべきビットコインのフォーマットされたメッセージを含む、請求項 1 に記載のシステム。

【請求項 11】

前記署名されたデジタルオブジェクトは前記第 1 の秘密鍵とともに生成されたデジタル署名とともにブロックチェーンに追加されたブロックを含む、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、高度なユーザ認証技術及び関連する応用に関する。

【背景技術】

【0002】

図 1 は、生体認証装置 100 を有する例示的なクライアント 120 を示している。正常動作時において、生体認証センサ 102 は、ユーザからの生の生体認証データを読み取り（例えば、ユーザの指紋を獲得する、ユーザの音声を録音する、ユーザのスナップ写真を撮るなど）、特徴抽出モジュール 103 は、生の生体認証データの指定された特性を抽出する（例えば、指紋の特定領域、特定の顔特徴などに焦点を当てるなど）。照合部モジュール 104 は、抽出した特徴 133 を、クライアント 120 のセキュアストレージに格納された生体認証基準データ 110 と比較し、抽出した特徴と生体認証基準データ 110 との間の類似度に基づいてスコア 153 を生成する。生体認証基準データ 110 は、一般的に、ユーザが、指紋、音声サンプル、画像、又は他の生体認証データをデバイス 100 に登録する登録プロセスの結果である。次に、アプリケーション 105 は、スコア 135 を使用して、認証が成功したか否か（例えば、スコアが特定の指定閾値を上回っているか）を判定してもよい。

【0003】

システムはまた、生体認証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。かかるシステムでは、アプリケーション 105 によって生成されたスコア 135 及び／又は他の認証データは、リモートサーバによってユーザを認証するため、ネットワークを通じて送信されてもよい。例えば、米国特許出願公開第 2

10

20

30

40

50

011/0082801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。

【0004】

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いくつかは、2012年12月29日に本件の譲受人に譲渡された以下の一群の米国特許出願（「同時係属出願」）に記載されている：第13/730,761号、Query System and Method to Determine Authentication Capabilities；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 Challenges 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。

【0005】

簡単に言えば、同時係属出願は、ユーザがクライアントの生体認証デバイスを用いて登録を行って、（例えば、指スワイプ、画像スナップ、音声記録などによって）生体認証テンプレートデータを生成し；生体認証装置をネットワーク（例えば、同時係属出願に記載されているようなセキュア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）上で1つ以上のサーバに登録し；その後、登録プロセス中に交換されるデータ（例えば、生体認証装置内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、認証技術について記載している。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ているフレームワークでは、ユーザを固有に識別するのに使用することができる、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、ユーザのクライアントデバイス（例えば、スマートフォン、ノートブックコンピュータなど）上でローカルに保持されてもよい。

【0006】

上述したような認証コードは、指をスワイプするか又は暗証番号を入力するなどのユーザとの相互作用のいくつかの形態を必要とする。これらの「正常な」認証コードは、所定の時点でユーザを認証することが意図される。更に、「サイレントな」認証コードはまた、所定の時点で（ユーザよりもむしろ）ユーザのデバイスを認証するように設計されて使用可能である。これらのサイレントな認証コードは、ユーザとの相互作用（例えば、機器ID送信）なしで、ユーザのデバイスから抽出された情報に依拠することができる。

【0007】

しかしながら、必要とする明示的なユーザとの相互作用があまりにも多くの摩擦を提示する所定の使用ケースがある（例えば、近距離無線通信（NFC）の支払い、高価なトランザクションに縛られることなく認証を必要とする頻繁に使用されるアプリケーション）のに対して、機器ID送信などの「サイレントな」認証技術は、正当なユーザがデバイスを保有したままであることに十分な確実性を提供しない。

【0008】

Anthony J. Nicholson、「一時的な認証を使用したモバイル装置のセキュリティ (Mobile Device Security Using Transient Authentication)」、IEEE TRANSACTIONS ON MOBILE COMPUTING VOL. 5, NO. 11, pp. 1489-1502 (2006年11月); Mohammad O. Derawi、「生体認証歩行認識を使用した携帯電話における控えめなユーザ認証 (Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition)」、(2010年); 及び Koichiro Niinuma、Anil K. Jain、「時間情報を使用した連続的なユーザ認証 (Continuous User Authentication Using Temporal Information)」(現在、http://www.cse.msu.edu/biometrics/Publications/Face/NiinumaJain_ContinuousAuth_SPIE10.pdf) など、研究コミュニティによっていくつかの「連続的な」認証方法が提案されている。これらの方法のいくつかは、BehavioSec、「連続的認証における FAR/FRR/EER 測定 (Measuring FAR/FRR/EER in Continuous Authentication)」、ストックホルム、スウェーデン (2009年) など、業界によって採用されている。これらの方法は、一般に、正当なユーザが認証処理に対する摩擦を追加せずになおも装置を所有する保証レベルを提供するが、それらは、単一のモダリティにフォーカスしている (すなわち、ウェアラブルトークン、歩行認識、顔及び服色認識、並びにユーザのキーボード入力を使用する)。

10

【0009】

しかしながら、存在する1つの問題は、世界のいくつかの地域ではユーザのプライバシーを侵害するリスク推定を補うために、信頼できる当事者に対して位置データ又は他の個人 (例えば、顔画像、服の色、歩行又は入力特性、...) 又は環境データ (例えば、温度、湿度、無線 LAN の SSID、...) を直接提供することである。したがって、非侵襲型であり且つエンドユーザのプライバシーを適切に保護する、より高度なリモート認証技術が必要である。

20

【0010】

更に、現在の認証方法 (例えば、パスワード、指紋認証など) の強度は、経時的にほぼ一定であるが、結果として生じるリスクは、認証が行われる現在の環境 (例えば、使用される機器、機器が接続されるネットワークなど) に基づいて変化する。現在の検出されたリスクに基づいて認証モダリティを選択及び/又は組み合わせることが有益であろう。

30

【0011】

認証の保証レベルの向上を考えると、明確な認証方法のレベルを向上させるための典型的な方法は、より複雑なパスワードを要求するか又は気になる指紋や顔認識などのより正確な生体認証方法を使用するなどである。実際には、認証保証レベル (又はそれから導出されるトランザクションリスク) はまた、認証が以前と同じ装置から行われたかどうか及び認証の位置が最後に成功した認証の位置に現実的に近いかどうか (例えば、サンフランシスコでの午後1時における認証と東京での同日午後2時における認証は、1人のためには現実的ではないと思われる) などの他のデータに依存する。

【0012】

パスワードは、なおも支配的で明確な認証方法である。残念ながら、それらは、容易に攻撃され、それらの攻撃はうまく増減する。更に、パスワードを入力することは、特にスマートフォンなどの小型機器においては面倒である。結果として、多くのユーザは、自己の携帯電話をロックするためにパスワードベースの保護方法を全く使用していないか、又は、些細な PIN コードを使用している。

40

【0013】

いくつかのスマートフォンは、認証するためのより便利な方法を提供するために、指紋センサを使用している。認証のために生体認証モダリティを使用することは、攻撃耐性の十分ななりすましをしていないために且つ潜在的に生体認証基準データを適切に保護しないことによってプライバシーの問題を導入するために批判されている。

50

【0014】

生体認証モダリティを組み合わせるための様々な「融合」方法が提案されている。それらの一部は、本人拒否率（FRR）を低減することによって有用性の問題に対処する。その他は、他人受入率（FAR）を低減することによってセキュリティの問題に対処する。これらの方法は、これまでの静的な融合アルゴリズムを提案している。残念ながら、このアプローチは、（上述したように）「他の入力」に応じて変化する保証レベルをなおもたらす。

【0015】

特定のクラスのトランザクションについて、トランザクションに関連する危険性は、トランザクションが行われている位置に密接に関連することができる。例えば、外国資産制御リスト（例えば、キューバ、リビア、北朝鮮など）の米国事務所に記載されているものなど、制限された国に由来するように見えるトランザクションを許可するように勧められてもよい。他の場合には、より強固な認証機構が使用される場合にトランザクションが進行するのを可能とすることが望ましいことがある；例えば、企業の物理的な施設内で行われるトランザクションは、企業が業務を有していない遠隔地に位置するスターバックスから行われるものよりも少ない認証を必要とする場合がある。

【0016】

しかしながら、信頼性の高い位置データは、様々な理由のために容易に利用できない場合がある。例えば、エンドユーザの装置は、GPS機能を有していないことがあり、ユーザは、WiFi三角測量データが利用できない又は信頼できない位置にすることがあり、ネットワークプロバイダは、GPS、又はWiFi三角測量機能を強化するために、提供セルタワーの三角測量機能をサポートしていないことがある。装置の位置を推測するための他のアプローチは、組織のニーズを満たすために十分なレベルの保証を有していない可能性がある；例えば、地理的位置を決定するための逆IP検索は、十分に粒状であってもよく、又は、ユーザの装置の真のネットワーク起源をマスクするために設計されたプロキシによってマスクすることができる。

【0017】

これらの場合、トランザクションの危険性を評価しようとする組織は、個人が認証の決定を駆動するために特定の地理的領域に位置している追加の保証とともにそれらを提供するために追加のデータを必要とすることがある。

【0018】

組織が認証を展開するための他の課題は、特定のユーザの環境（位置、装置、ソフトウェア、オペレーティングシステム）によって提示される固有のリスクに認証機構の「強さ」を一致させることであり、ユーザ又は装置及び組織の管理ポリシーによって要求（制限された情報へのアクセスのための又は特定の操作を行うための要求）が行われる。

【0019】

現在までに、組織は、そのユーザの認証ニーズに対してかなり静的応答に頼らなければならなかった。すなわち、組織は、通常実行する操作中にユーザが直面するリスク及び任意の適用可能な規制委任の要件を評価し、その後、そのリスクから身を守り且つコンプライアンスを実現するために認証解決策を展開する。これは、通常、特にコストがかかり刈る管理するのに煩雑であり得るそれらの異なるユーザが直面する可能性のある多数の様々なリスクに対処するための複数の認証解決策を展開するために組織を必要とする。

【0020】

同時係属出願に記載された技術は、認証のために使用することができる組織がユーザの装置上の既存の機能を特定するのを可能とする抽象化を提供する。この抽象化は、異なる認証の様々な解決策を展開する必要性から組織を保護する。しかしながら、組織は、必要に応じて「正しい」認証機構を起動する方法をなおも必要とする。既存の実装は、認証機構が状況下で適切であるものを説明するために組織に機能を何ら提供しない。その結果、組織は、おそらくコードにおいてそれらの認証ポリシーを成文化する必要がある、解決策を脆くして新たな認証装置／トークンの使用を可能とするために将来的にコードの変更を

10

20

30

40

50

必要とするであろう。

【0021】

電子金融トランザクションは、今日、主にブラウザアプリケーションを使用したワールドワイドウェブを介して行われている。Amazon.com、デル、及びウォルマートのようなサイトは、それらのオンラインポータルを介して数十億ドルの商品を販売しており、銀行や証券会社は、それらの顧客がオンライン口座から数十億ドルの資金を移動するのを可能とする。これらのようなウェブサイトの1つの課題は、不正行為を検出する方法である。不正取引は、これらの企業に数十億ドルを要することができる。

【0022】

不正取引に対する防御に最初に使われるものは、ユーザのパスワードである。しかしながら、犯罪者は、様々な技術を介してパスワードを取得することができる。時々、パスワードは、複雑さに弱く、総当たり攻撃によって容易に推測又は判定されることができる。他のときには、マルウェア、ワーム又はウィルスは、ユーザのコンピュータに感染することができる。そして、パスワードは、キーストロークを記録するか又はメモリやハードディスク記憶装置をスキャンすることによって得られる。実装置が盗まれた場合、パスワードは、メモリ又は記憶装置に残っているデータから回復することができる。パスワードが危険にさらされると、犯罪者は、アカウントにアクセスして資金を引き出すか又は移動する能力を有する。

【0023】

ユーザのパスワードの違反によって引き起こされる損傷を防止しようとするために、金融トランザクションを扱うサイトは、トランザクションを開始した人が実際にアカウントを所有しているユーザであるかどうかを判定するために様々なメトリックが使用されているリスク評価を採用している。トランザクション時間、トランザクション位置及びトランザクション状況などの要因は、トランザクションがリスクを有しているかどうかを評価するための全てのよい方法である。例えば、ユーザが通常夜間に自己のアカウントにおいて任意のアクティビティを有していない場合、トランザクションが午前3:00から午後3:00に開始される可能性は低いであろう。同様に、ユーザが米国に住んでいるが、トランザクションが韓国で開始された場合、その位置の違いは、警告サインとなるであろう。最後に、処理されている金額が通常よりも大きさが大幅に異なる場合には、これは潜在的な不正行為の他の信号である。

【0024】

残念ながら、ウェブブラウザは、ウェブサイトがクライアントシステムについて得ることができる情報に非常に厳しい制限を設けている。ブラウザは、外部（及びおそらく悪意のある）世界にユーザの機器を公開していることから、必要よりも多いデータの漏洩は、独自のセキュリティリスクである。確かに、トランザクションの時間、（例えば、ユーザのIPアドレスを介して）トランザクションの位置及びトランザクションの大きさを記録することができる。ウェブサイトは、トランザクションが不正であるかどうかを判定するためにこのデータの全てを現在使用している。しかしながら、ブラウザによって提供される情報のこれらの基本的な部分を越えて、ウェブサイトは、リスク評価のために利用する他の情報を有していない。ブラウザが得ることができる情報の制限のため、ユーザのトランザクションについてのリスク評価は、非常に正確ではない。

【0025】

本発明のより良好な理解は、以下の図面と併せた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】

【0026】

本発明のより良好な理解は、以下の図面と併せた以下の詳細な説明から得ることができる。

【図1】 生体認証装置を有する例示的なクライアントを図示している。

【図2】 非侵襲型プライバシー保持認証装置（NIPPA）の1つの実施形態を図示して

10

20

30

40

50

いる。

【図 3】「正当なユーザ状態」及び次の正当なユーザ状態中における本発明の 1 つの実施形態の動作をグラフィカルに図示している。

【図 4】非侵襲型プライバシー保存認証のための方法の 1 つの実施形態を図示している。

【図 5】1 つの実施形態における位置ベースの認証のために用いられる距離関数を図示している。

【図 6】拡張された正当なユーザの状態ウィンドウを使用した本発明の 1 つの実施形態の動作をグラフィカルに図示している。

【図 7】本発明の 1 つの実施形態にかかる適応的認証モジュールを図示している。

【図 8】適応的な認証方法の 1 つの実施形態を図示している。

【図 9】1 つの実施形態にかかる適応的な認証をグラフィカルに図示している。

【図 10】複数の構成要素を有する複合認証装置の 1 つの実施形態を図示している。

【図 11】2 つの認証装置が構成要素を共有している 1 つの実施形態を図示している。

【図 12】構成要素を認証するための構成要素認証鍵 (CAK) の対を管理するための認証ロジックの構成要素を含む認証装置の 1 つの実施形態を図示している。

【図 13】2 つの構成要素間の認証の 1 つの実施形態を示すトランザクション図である。

【図 14】本発明の 1 つの実施形態にかかる静的認証装置を図示している。

【図 15】本発明の 1 つの実施形態にかかる動的認証装置を図示している。

【図 16】本発明の実施形態を実施することができる例示的なシステムアーキテクチャを図示している。

【図 17】認証ポリシーの位置認識アプリケーションを実行するためのシステムの 1 つの実施形態を図示している。

【図 18】認証ポリシーの例示的なセットを図示している。

【図 19】本発明の 1 つの実施形態にかかる方法を図示している。

【図 20】他のピア又はネットワーク機器の接近によって位置が決定又は確認される本発明の 1 つの実施形態を図示している。

【図 21】環境センサを使用した認証システムの 1 つの実施形態を図示している。

【図 22】環境センサを使用した認証方法の 1 つの実施形態を図示している。

【図 23】認証ポリシーを適応的に適用するためのシステムの 1 つの実施形態を図示している。

【図 24】認証ポリシーを適応的に適用するための方法の 1 つの実施形態を図示している。

【図 25】生体認証装置を有する例示的なクライアントを図示している。

【図 26 A】眼追跡モジュール及び顔認識モジュールを含む認証エンジンの 1 つの実施形態を図示している。

【図 26 B】眼追跡モジュール及び顔認識モジュールと組み合わせた発話認識モジュール及び唇運動分析モジュールを含む認証エンジンの 1 つの実施形態を図示している。

【図 27】本発明の 1 つの実施形態において使用されるウェブページについての例示的なヒートマップを図示している。

【図 28 A】エンドユーザに表示することができる例示的なテキスト、グラフィックス、写真、ビデオ、ブランク領域及び他のコンテンツを図示している。

【図 28 B】エンドユーザに表示することができる例示的なテキスト、グラフィックス、写真、ビデオ、ブランク領域及び他のコンテンツを図示している。

【図 29 A】眼追跡及び顔認識ベースの認証並びに音声認識及び唇運動分析認証を行う方法の実施形態を図示している。

【図 29 B】眼追跡及び顔認識ベースの認証並びに音声認識及び唇運動分析認証を行う方法の実施形態を図示している。

【図 30】本発明の実施形態を実施することができる異なるアーキテクチャの構成を図示している。

【図 31】クライアントリスク評価エージェントを含むクライアントアーキテクチャの 1 つの実施形態を図示している。

【図 3 2】クライアントリスク評価エージェントによって使用される例示的な種類のクライアント設定データを図示している。

【図 3 3】認証中にクライアントリスク評価を行うための方法の 1 つの実施形態を図示している。

【図 3 4】ローカルデバイスとのセキュアトランザクションを実行するクライアントの 1 つの実施形態を図示している。

【図 3 5】ローカルデバイスとのセキュアトランザクションを実行するためのクライアントアーキテクチャの 1 つの実施形態を図示している。

【図 3 6】ローカルデバイスとのセキュアトランザクションを実行するための方法の 1 つの実施形態を図示している。

10

【図 3 7】オンライントランザクションのユーザ確認のためのシステムの 1 つの実施形態を図示している。

【図 3 8】オンライントランザクションのユーザ確認のためのシステムに使用されるクライアントの 1 つの実施例の詳細を図示している。

【図 3 9】オンライントランザクションのユーザ確認のための方法の 1 つの実施形態を図示している。

【図 4 0】信頼できるクライアント装置から新たなクライアント装置に信頼を委任するためのシステムの 1 つの実施形態を図示している。

【図 4 1】信頼できるクライアント装置から新たなクライアント装置に信頼を委任するためのシステムの 1 つの実施形態の追加の詳細を図示している。

20

【図 4 2】信頼できるクライアント装置から新たなクライアント装置に信頼を委任するための方法の 1 つの実施形態を図示している。

【図 4 3】装置間でプライベートデータを同期するためのシステムの 1 つの実施形態を図示している。

【図 4 4】信頼サークルに装置を追加するための方法の 1 つの実施形態を図示している。

【図 4 5】装置間でデータを同期させるための方法の 1 つの実施形態を図示している。

【図 4 6 A】本発明の実施形態を実施することができる異なる例示的なアーキテクチャの構成を図示している。

【図 4 6 B】本発明の実施形態を実施することができる異なる例示的なアーキテクチャの構成を図示している。

30

【図 4 7】クライアント装置の認証装置が発見され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 4 8】ユーザが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 4 9】鍵が認証装置に登録される様態を示すトランザクション線図である。

【図 5 0】ユーザ認証が認証フレームワーク内で実装され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 5 1】トランザクションの詳細を検証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 5 2】本発明の 1 つの実施形態にかかる実施されたクエリポリシーフィルタを図示している。

40

【図 5 3】本発明の 1 つの実施形態におけるクエリポリシーの登録操作が実装される方法を示すトランザクション図である。

【図 5 4】複数の認証装置の処理を実現するためのアーキテクチャの 1 つの実施形態を図示している。

【図 5 5 A】複数の認証装置を処理するための本発明の 3 つの実施形態を図示している。

【図 5 5 B】複数の認証装置を処理するための本発明の 3 つの実施形態を図示している。

【図 5 5 C】複数の認証装置を処理するための本発明の 3 つの実施形態を図示している。

【図 5 6 A】ランダムチャレンジタイムアウトを検出して応答するためのトランザクション図を図示している。

50

【図 5 6 B】ランダムチャレンジタイムアウトを検出して応答するためのトランザクション図を図示している。

【図 5 7】本発明の 1 つの実施形態にかかるプライバシークラスを実装するためのアーキテクチャを図示している。

【図 5 8】本発明の 1 つの実施形態にかかるプライバシークラスを実装するためのトランザクション図である。

【図 5 9】認証及びトランザクションのために署名を使用するためのアーキテクチャの 1 つの実施形態を図示している。

【図 6 0】本発明の実施形態を実行するためのコンピュータシステムの例示的な実施形態を図示している。

【図 6 1】本発明の実施形態を実行するためのコンピュータシステムの例示的な実施形態を図示している。

【図 6 2】クライアントを認証するために信頼できる当事者によってメタデータが使用される 1 つの実施形態を図示している。

【図 6 3】鍵マスタ及び認証部を含む例示的なアーキテクチャを図示している。

【図 6 4】ビットコインフォーマットメッセージを処理するアーキテクチャの別の実施形態を図示している。

【図 6 5】仮想アプリケーション ID 及び／又は信頼できる当事者 ID を記憶及び処理する 1 つの実施形態を図示している。

【図 6 6】ブロックチェーンのブロックについての証明データを暗号化及び生成するためのアーキテクチャの 1 つの実施形態を図示している。

【図 6 7】本発明の 1 つの実施形態にかかるシステムを図示している。

【図 6 8】1 つの実施形態にかかるチップ (S o C) 上のシステムを図示している。

【発明を実施するための形態】

【0027】

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。

【0028】

以下に考察する本発明の実施形態は、生体認証デバイス又は P I N 入力などの認証能力を備えたクライアントデバイスをともなう。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目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。認証能力はまた、トラステッドプラットフォームモジュール (T P M) 及びスマートカードなどの非生体認証装置を含むことができる。

【0029】

モバイルバイオメトリックの実装において、生体認証装置は、信頼できる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、生体認証装置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、信頼できる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、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など）を介して又は U S B ポートなどの周辺入力を介して信頼できる当事

10

20

30

40

50

者に結合することができる。これらの条件下では、そのデバイスが信頼できる当事者（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、及び／又はハッカーが生体認証デバイスを侵害したかを、信頼できる当事者が知る方法がないことがある。生体認証装置における信頼度は、デバイスの特定の実装形態に依存する。

【0030】

「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。

【0031】

「信頼できる当事者」という用語は、本明細書では、ユーザ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）だけでなく、本明細書に記載する基本認証技術を実行してもよいそのエンティティの代理として実装されるセキュアトランザクションサーバも指すのに使用される場合がある。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。

【0032】

「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。

A. 非侵襲型のプライバシー保護認証

【0033】

本発明の1つの実施形態は、非侵襲型認証の状況を認識するための認証システムをトレーニングするために、「通常の」認証技術（例えば、指スワイプ、コード入力など）を使用する。更に、1つの実施形態は、認証が必要な場合に機器IDなどの機密情報よりもむしろ信頼できる当事者に対して装置の認証状態を返す。

【0034】

以下に記載される本発明のいくつかの実施形態は、（すなわち、明示的なユーザ認証を必要とせずに）完全に摩擦なしで動作することができる。行動又は他の技術は、認証されたユーザが装置の所有であるという現在の保証を示す保証レベルを継続的に測定するために使用することができる。保証レベルは、例えば、最後の明示的なユーザ認証（例えば、PIN又は指スワイプによるSIMカード又は電話のロック解除）から経過した時間に基づいて計算することができる。経過した時間量が特定の閾値（例えば、5秒、5分、1時間など）の範囲内であると仮定すると、装置は、「正当ユーザ状態」であり、保証レベルが最大値に設定される（例えば、-100から100の正規化されたスケールにおいて100）と考えることができる。

【0035】

正当ユーザ状態に続いて、保証レベルは、（例えば、装置センサから検出された非侵襲型の入力に基づいて）認証されたユーザが装置を所有していることを示す明示的なユーザ認証及び他の変数からの経過時間の組み合わせに基づいて測定することができる。例えば、ユーザの生体認証歩行は、ユーザの通常の歩行パターンから歩行「指紋」を生成するように設計されたソフトウェア及び／又はハードウェアと組み合わせて加速度計又は他の種類のセンサを使用して測定することができる。更に、正当ユーザの頻繁に訪問する目的地までの距離は、保証レベルを決定するために、追跡されて記憶され、その後に使用されることができる。例えば、ユーザがユーザの自宅や職場であるような既知の位置から信頼できる当事者に接続している場合、保証レベルは、比較的高い値に設定されることができるのに対して、装置が不明又は離れた位置から接続している場合、保証レベルは、低レベルに調整されることができる。

10

【0036】

様々な他のタイプの非侵襲型測定は、認証されたユーザが、例えば、例を挙げると、ネットワークの識別を含む装置又はクライアント装置がブルートゥース装置、近距離無線通信（NFC）装置、ルータやアクセスポイントなどのWi-Fi装置、スマートウォッチ、他のコンピューティング装置、Nymiブレスレットなどに接続されている装置を所有しているかどうかを決定するために実行することができる。Wi-Fi装置は、自宅におけるWi-Fiルータ及び同僚や家族が使用するWi-Fi対応のコンピュータなどの範囲においてWi-Fiネットワークの可視性を含むことができる。更に、加速度センサの特性及びデジタルカメラのセンサパターンノイズなどのクライアント装置の特定の具体的な特性は、非侵襲型測定のために使用することができる。通常ユーザ相互作用のタッチスクリーンジェスチャはまた、基準データ及び通常ユーザ相互作用からのユーザのタイピング行動として分析されて記憶されることができる。もちろん、上記は単なる例示である。本発明の基本原理は、非侵襲変数のいかなるセットにも限定されない。

20

【0037】

最終結果は、正当ユーザがなおも装置を所有しているという保証レベルが認証応答において信頼できる当事者に送信されることができるということである。1つの実施形態において、保証レベルは、「署名される」か又は鍵（例えば、以下に説明するように登録段階において確立されて証明された信頼できる当事者固有の鍵）によって認証される。1つの実施形態において、保証レベルは、-100と100の間の値に正規化され、-100は、「ほぼ確実に正当ユーザではない」ことを意味し、0は、「知らない」ことを意味し、100は、「ほぼ確実に正当ユーザである」ことを意味する。

30

【0038】

1つの実施形態において、信頼できる当事者は、保証レベルが想定されるトランザクションのために許容されない場合には、追加の「通常の」認証部応答を使用するためにクライアント装置に求めることができる。必要とされる認証のレベルにかかわらず、1つの実施形態は、信頼できる当事者に個人データを開示しない。その代わりに、信頼できる当事者に対して認証部を認証するために1つの特定の信頼できる当事者専用の暗号化鍵を使用する。

【0039】

非侵襲型プライバシー保護の認証を提供するためのアーキテクチャの1つの実施形態は、非侵襲型認証機構230からの入力（例えば、位置、歩行測定など）に基づいて現在の保証レベルを決定するための保証計算部212及び1つ以上の明示的なユーザ認証装置220-221（例えば、指紋センサ、IDコードを入力するための入力装置など）を含む非侵襲型プライバシー保護認証部（NIPPA）210を含む図2に示されている。1つの実施形態において、明示的なユーザ認証装置220-221は、図1に示されるように同一又は類似のアーキテクチャを含む。

40

【0040】

図2に示される実施形態において、非侵襲型認証部230は、位置センサ241及び（例えば、ファイルシステムやデータベースとして実装することができる）ユーザ／位置デ

50

ータ記憶装置 245 に記憶された履歴又はユーザ固有の位置データを使用して位置ベースの認証を行うための位置認証モジュール 231 を含む。例示としてであって限定されるものではないが、位置センサ 241 は、GPS 装置及び／又は（装置の現在位置を推定するために使用することができる）クライアント 200 が接続されている現在のアクセスポイント又はセルタワーを検出するためのモジュールを含むことができる。ユーザの位置に関連するデータを提供することができる任意のセンサを使用することができる。位置認証モジュール 231 は、クライアント装置の現在位置が保証レベルに及ぼす影響を決定する。例えば、（履歴又はユーザ固有の位置データ 245 に応じて）装置が現在「自宅」や「職場」の位置にある場合、保証レベルは、上方に調整されることができる。装置が現在離れた未知の位置にある場合、保証レベルは、下方に調整されることができる。1つの実施形態において（本明細書に記載される）「正当ユーザ状態」中にシステムを自動的にトレーニングすることに加えて、ユーザは、「信頼できる」として手動で特定の位置を指定する機能を備え、したがって、高い保証レベルを有する（例えば、ユーザが自宅又は職場にいるとき）。位置認証モジュール 231 の結果は、現在の保証レベルの計算に分解されることができる保証計算モジュール 212 に提供される。

【0041】

ユーザ行動認証モジュール 232 は、現在のユーザの行動が（ユーザ及び位置データ記憶装置 245 に記憶された）履歴ユーザ行動と一致している程度を判定するために、1つ以上のユーザ行動センサ 242 をあてにする。例えば、ユーザ行動センサ 242 は、ユーザ行動認証モジュールが装置 200 を現在所有しているユーザの歩行を判定するために使用することができる加速度計の測定値を提供することができる。そして、それは、正当なユーザが装置を所有しているという信頼のレベルに到達するために、（明示的なユーザ認証前であって記憶装置 245 に記憶されるのに続いて収集された）ユーザの既知の歩行とこれらの測定値を比較することができる。その結果は、それが現在の保証レベルの計算に分解されることができるように保証計算モジュール 212 に提供される。

【0042】

様々な他の／追加の認証装置 233 は、認証演算を実行するために他の／追加センサ 243 からデータを収集することができ、その結果は、現在の保証レベルの計算に分解されるように保証計算モジュール 212 に提供されることができる。

【0043】

図 2 において別個のモジュールとして示されているが、位置認証モジュール 231、ユーザ行動モジュール 232 及び任意の他の認証モジュール 233 は、保証計算モジュール 212 の一部を形成することができる。本発明の基本原理は、様々な異なる論理構成を使用して実装することができる。

【0044】

図示されたように、1つの実施形態において、保証計算モジュール 212 は、最後の明示的なユーザ認証から経過した時間量を測定する場合、タイマ 211 をあてにする。以下に詳細に述べられるように、最後の明示的なユーザ認証から経過した時間量は、装置が現在「正当ユーザ状態」にあるかどうかを判定し、それに応じて保証の測定値を調整するために使用することができる。

【0045】

保証計算モジュール 212 が現在の保証測定値に到達すると、それは、セキュア通信モジュール 213 を介して確立された信頼できる当事者（1つの実施形態においてはクラウドサービス）に測定値を通信することができる。例えば、非侵襲型認証部 230 を含む各認証部 220-221 は、信頼できる当事者固有の且つ登録動作（前認証）において証明された鍵を交換することができる。認証動作に返された保証レベルは、信頼できる当事者固有の認証鍵によって署名された／暗号化されたメッセージの一部とすることができる。更に、以下に説明するように、メッセージはまた、信頼できる当事者によって生成されたナンス（例えば、ランダムチャレンジ）を含むことができる。

【0046】

1つの実施形態において、セキュア記憶装置225は、認証部のそれぞれに関連し且つ信頼できる当事者とセキュア通信を確立するためにセキュア通信モジュール213によって使用される認証鍵を記憶するために設けられたセキュア記憶装置である。

【0047】

上述したように、1つの実施形態において、NIPPA210は、そのような認証成功のそれぞれの後に定義された時間ウィンドウ（T1秒まで）内で「正当ユーザ」状態を維持するために、既存の（明示的な）ユーザ認証技術（例えば、パスワードベースのシステムログイン、SIMカードロック解除など）を活用する。NIPPA210は、各種センサ241-243からユーザの行動を定期的に測定することができるとともに、「正当ユーザ」状態において測定値に応じて内部基準データベクトルを更新することができる。「正当ユーザ」状態におけるわけではないが、NIPPA210は、現在の測定値に基づいて基準データベクトルまでの正規化された「距離」を計算することができる。この「距離」は、正当ユーザがなおも認証部を所有したままであると確実に考えられる。

【0048】

ユーザを認証するように求められた場合、NIPPA210は、「正当ユーザ」状態にあるかどうかを判定するために検査することができる。そうである場合、認証は成功したとみなされ、最大保証レベル（例えば、100）が返される。「正当ユーザ」状態でない場合、NIPPA210は、最新の測定値に基づいて保証計算モジュール212によって計算された保証レベルを返すことができる。そして、NIPPA210は、現在時間tcに対するその測定値tmの時間差td（ $td = tc - tm$ ）に保証レベルを組み合わせることができる。1つの実施形態において、これは、以下のロジックを使用して行われる。

【0049】

（1）（保証レベル ≥ 0 ）の場合、得られた保証レベル＝保証レベル*（最大（ $T0 - td$ 、0）/ $T0$ ）、 $T0$ は最大許容時間差である；

【0050】

（2）（保証レベル < 0 ）の場合、得られた保証レベル＝保証レベル。

【0051】

上記式にかかる本発明の1つの実施形態の動作が図3に示されている。時間t1において、ユーザは、明示的な認証を実行する（例えば、SIMカードのロックを解除するために、指スワイプ、PIN入力など）。t1+T1までの時間ウィンドウは、「正当ユーザ」状態と考えられる。上述したように、非侵襲型認証部は、正当ユーザ状態内でトレーニングすることができる。例えば、ユーザの歩行が測定されることができ及び／又はユーザが訪れた位置が記録されることができ、その後非侵襲型認証を実行するために使用することができる。

【0052】

時間t2（正当ユーザ状態外）において、保証計算モジュール212は、非侵襲型認証部に基づいて保証レベルを計算する。その結果は、装置がほとんど正当なユーザの完全な制御下にあることを示す正である。この計算後、保証レベルは経時的に減少する（例えば、正当ユーザが非正当人に装置を公開することがある）。例えば、時間t3において、保証レベルは、時間t2から大きく低下している。1つの実施形態において、非侵襲型保証レベルは、過剰な電力及びCPU性能の消費を回避するために、定期的に計算されるのみである。

【0053】

t5において、他の非侵襲型保証レベルの計算が発生する。今回の結果は、装置が正当ユーザの完全な制御下でない可能性を示す負である。他の計算が非侵襲型認証部に基づいて実行されるまで（例えば、時間t6において）、この負の保証レベルは変更されない。

【0054】

1つの実施形態にかかる方法が図4-5に示されている。本方法は、図2に示されているようなものなどのシステムアーキテクチャ内に実装されることができるが、任意の特定のシステムアーキテクチャに限定されるものではない。

【0055】

401において、明示的な認証イベントは、装置のロックを解除するために指紋センサ上でのスワイプ又はPINの入力などが発生する。タイマはまた、明示的な認証イベントからの経過時間を測定するために開始されることができる。402において、正当ユーザ状態が入力され、403において、ユーザの行動の様々な態様は、後の参照（例えば、位置、ユーザ歩行など）のために測定されて記憶されることができる。（例えば、信頼できる当事者とのトランザクションから生じる）認証要求が404において判定された正当ユーザ状態中に発生した場合、405において最大保証レベルが選択され、420において信頼できる当事者に送信される。

【0056】

406において、（例えば、指定した時間量が経過したことをタイマが示すために）システムは、正当ユーザ状態を出す。407において、システムは、操作403に記憶された内部基準データに対するセンサからのデータを比較することによってユーザの行動を定期的に測定する。一例として、（正当ユーザ状態のときに収集された）ユーザの歩行に関連した測定値は、（407において収集された）現在の歩行測定値と比較されることができる。2つの間の相関（基準データまでの「距離」と称される）が計算されることができる。408において判定された正当ユーザ状態外の場合に認証要求を受信した場合、409において、現在の保証レベルが内部基準データまでの距離及び明示的な認証イベントからの潜在的な時間に基づいて計算される。そして、保証レベルは、420において信頼できる当事者に送信される。

【0057】

図5を参照すると、信頼できる当事者に送信される保証レベルが501において判定されたユーザとの現在のトランザクションのために許容可能である場合、信頼できる当事者は、クライアント装置に対して認証の成功を示す応答を送信することができる。そうでない場合、503において、信頼できる当事者は、追加認証（例えば、非侵襲型認証が不十分である場合の潜在的に明示的なユーザ認証）が必要であることを示す応答をクライアントに送信することができる。

【0058】

代替実施形態において、信頼できる当事者は、特定のトランザクションに必要な保証レベルを最初に指定することができ、非侵襲型認証技術が不十分である場合、システムは、潜在的に明示的なユーザ認証を使用して必要な保証レベルが満たされることを保証する。そして、システムは、信頼できる当事者に（保証レベルよりもむしろ）認証が成功した旨の指示を送信することができる。

【0059】

上述したように、本発明の1つの実施形態は、保証レベルを決定するために既知のユーザ位置のセットから距離を計算する。図6を参照すると、位置ベースの測定（例えば、GPSなど）は、以下のように「距離」関数を計算するために使用することができる。

【0060】

前処理動作において、全ての測定位置（ L_n ）は、それらの最も近い「領域」に割り当てられる。領域は、 r （例えば、10メートル）の半径を有する円として定義される。領域は、領域の最小数が全ての L_n をカバーするように配置される。 M 個の位置未満をカバーする全ての領域が領域のセットから削除される（すなわち、それらはユーザの「頻繁」位置と考えられない）。

【0061】

そして、「距離」（ d ）は、 $\text{距離} = (\text{領域} (R_n) \text{の最寄りの中央までの現在位置} (L_c) \text{の距離}) / r$ を用いて判定され、 r は、領域の半径である。 L_c が既存の領域内にある場合、この値は小さいか又は1に等しく、 L_c が外である場合には非常に大きくなる可能性がある。そして、保証レベルは、以下を使用して計算される： $\text{保証レベル} = \text{Max} (100 - 50 * \text{floor}(d), -100)$ 。これは-100から100の範囲である。

【0062】

上記実施形態のいくつかにおいて、明示的に認証に続く特定の時間ウィンドウ内で又は現在の行動が測定された行動に非常に類似している場合には正当ユーザがなおクライアント装置を所有したままであると仮定する。しかしながら、上記実施形態は、明示的な認証後に特定の時間ウィンドウ内の行動基準データを更新するのみである。

【0063】

図7に示されるように、本発明の1つの実施形態は、正当ユーザの状態についての標準的な時間ウィンドウに加えて行動基準データを更新するために拡張された時間ウィンドウを使用する（すなわち、システムをトレーニングする）。結果として、（標準時間ウィンドウ及び拡張時間ウィンドウを含む）完了時間ウィンドウは、以下のように定義されることができる：（1）正当ユーザ状態の時間ウィンドウが成功した明示的なユーザ認証に続く場合（すなわち、 $t_1 \dots t_1 + T_1$ ）、又は、（2）返された保証レベルがある閾値T（例えば、 t_2 、 t_4 において $T = 90$ など）以上である場合。彼の好意に対する行動基準を「シフト」するために攻撃者にとって非常に容易であることから、0に閾値を設定することは望ましくない。

B. 適応的認証技術

【0064】

図8は、適応的認証技術を実施するための本発明の1つの実施形態を図示している。上述した実施形態のように、本実施形態は、（例えば、位置、検知されたユーザの行動などに基づく）非侵襲型認証を行うための1つ以上の非侵襲型認証モジュール230と、（例えば、PIN、指紋スキャンなどを必要とする）明示的なユーザ認証を実行するための1つ以上の明示的な認証モジュール222とを含む。更に、前の実施形態と同様に、保証計算モジュール212は、例えば、（タイマ211によって提供される）最後の明示的な認証からの時間及び／又は様々な認証モジュール230、222によって提供される認証データに基づいて保証計算を行う。セキュア通信モジュール213は、（例えば、上述したようにセキュアな暗号化鍵を使用して）信頼できる当事者250とのセキュア通信を確立する。

【0065】

1つの実施形態において、適応的認証モジュール800は、信頼できる当事者250との現在のトランザクションのための十分な保証レベルに到達するために利用可能な非侵襲型認証技術及び明示的な／侵襲型認証技術の中から動的に選択する。代替的に又は追加的に、信頼できる当事者250における適応的認証モジュール810は、十分な保証レベルに到達するために認証選択技術を実行することができる。本発明の基本原理は、認証選択技術が（適応的認証モジュール800によって）クライアント装置200に又は（適応的認証モジュール810によって）信頼できる当事者250に実装されるかどうかにかかわらず同じままである。

【0066】

更に、図8に示されている「信頼できる当事者」250は、信頼できる当事者に代わって本明細書に記載された認証技術を実装することができ且つ信頼できる当事者に結果を提供することができる信頼できる第三者サーバを提示することができる。それゆえに、本発明の実施形態は、「信頼できる当事者」の観点で説明されるが、本発明の基本原理は、信頼できる当事者によって動作するネットワークの境界の外側にあるサーバを用いて実装することができる。

【0067】

以下により詳細に述べられるように、1つの実施形態において、適応的認証モジュール810は、クライアント装置に関連付けられた変数（例えば、現在のIPアドレスに基づいて、IPパケットの往復遅延時間など）に基づいてリスクレベルを判定するためにリスクエンジン812を含む。更に、保証レベルゲイン分析要素811は、現在の保証レベルが許容可能な保証レベルに到達するように増加されなければならない量を判定することができる。これらの要素は、信頼できる当事者の適応的認証モジュール810の構成要素として図8に示されているが、それらはまた、更に本発明の基本原理を順守しながらクライ

アントの適応的認証モジュール 800 に実装されてもよい。

【0068】

1つの実施形態において、（例えば、トランザクションを開始するために）クライアント装置 200 が信頼できる当事者 250 に接続されると、リスクエンジン 812 は、現在利用可能な全てのデータに基づいてリスク（又は保証レベル）を判定する。これは、例を挙げると、例えば、（例えば、IP アドレスに由来する又はモバイルネットワークオペレータによって提供される）クライアント装置 200 の地理的位置、クライアント装置 200 と信頼できる当事者 250 との間で送信されるパケットの往復遅延時間、クライアント装置 200 と信頼できる当事者 250 との間で送信されるネットワークパケットについてのホップ数、クライアント装置 200 において実行されるユーザエージェントによって送信される特定の「ユーザエージェント」文字列を含むことができる。1つの実施形態において、リスクエンジン 812 は、次に、指定されたトランザクションのためにユーザを認証するのに必要な追加の保証量を判定するために使用されることができる暗黙の「リスクスコア」（又はリスクスコアに逆に関連する予備保証レベル）に到達するためにこのデータを評価する。

10

【0069】

1つの実施形態において、暗黙のリスクスコアに基づいて、信頼できる当事者 810 又はクライアント装置 800 における適応的認証モジュールは、意図したトランザクションについて必要なレベルまで全体の保証レベルを増加させる可能性を有する 1 つ以上の認証モジュール 222、230 のセットを決定する（すなわち、予備保証レベル／暗黙のリスクスコアと組み合わせた場合）。1つの実施形態において、保証レベルゲイン分析モジュール 811 は、必要なゲイン量を判定し、適応的認証モジュール 800、810 は、パラメータとして必要な保証レベルゲインの指示を備える。そして、適応的認証モジュール 800、810 は、（少なくとも）必要なゲインを達成するために、認証技術の最も便利なセット（非侵襲型 230 及び／又は明示的 222）を決定するようにこの「ゲイン」パラメータを使用する。適応的認証モジュール 800 は、信頼できる当事者 250 に応じて（例えば、認証された拡張として）、認証技術の選択されたセットの正式な記述を含むことができる。そして、信頼できる当事者 250 は、得られた全体的な保証レベルが必要なレベルを満たしているかどうかを検証することができる。

20

【0070】

例として、限定するものではないが、適応型認証モジュール 800 は、デバイスフィンガープリンティング（例えば、センサの欠陥又はカメラセンサパターンノイズを認識する）、環境情報（例えば、GPS ベースの位置、WiFi ネットワークから導出された位置、Nymi、スマートウォッチ（pebble）、又はヘッドセットのような周辺機器のような他のガジェットへの有線又は無線接続の存在、行動データ（例えば、ユーザがポケットから装置を取る方法、行動入力、歩行など）、装置が「信頼できる」状態にあった時間、及び潜在的に保証レベルにおいて必要な（残りの）ゲインを達成するために必要な 1 つ以上の認証モダリティ（生体認証又はその他）を使用した新たな明示的な認証の結果などの認証モダリティを組み合わせることができる。

30

【0071】

上記技術の結果は、ユーザが最も便利な認証方法を選択することができるということである。スマートフォンの場合、これは単に電話へのアクセスを有することができる（上記参照）。認証方法を選択するためにユーザに尋ね、その後、他の明示的な認証のためにユーザを必要とする代わりに、信頼できる当事者 250 は、少なくとも侵襲型の認証技術のセットを識別する適応的認証部 800、810 に対して必要な保証レベルゲインの指示を送信する。適応的認証モジュール 800、810 は、常には、（PIN 入力又は指スワイプなど）の明示的な（侵襲型）ユーザ認証も、単に非侵襲型モダリティに基づくものも必要としない。代わりに、認証部は、必要な保証レベルゲインが達成されるように（クライアント側の）利用可能な全てのモダリティの適切な組み合わせを選択する。

40

【0072】

50

上記詳細に述べたように、ハッキング／なりすましモダリティは時間がかかることがあるため、装置が信頼できる状態であったときからの時間が重要である。例えば、ユーザが電話を喪失し、誰かがそれをハッキングしようとする場合、指紋がディスプレイからキャプチャされ、適切なゴム指が作成された後にアクセスを得るために使用されることができ、それは一日かかることがある。その結果、最後の信頼できる状態から24時間以内に必要なPIN入力は、この種の攻撃に対して十分な保護になる。攻撃の次のレベルは、装置にアクセスする前に指紋がキャプチャされるものである。これらの攻撃は、実際にはそれほど頻繁に見られない。しかしながら、信頼できる当事者250がそのような攻撃に対する保護を必要とする場合には、適応的認証モジュール800、810は、生体認証モダリティを受け入れるために、位置データ又はその他のガジェットや周辺機器の存在を考慮する必要があるかもしれない。

10

【0073】

本発明の1つの実施形態にかかる方法が図9に図示されている。上述したように、本明細書において使用される「信頼できる当事者」は、ユーザの正確な認証に依存する実際の当事者であってもよく、又は、信頼できる当事者に代わってユーザを認証する第三者サービスであってもよい。

【0074】

901において、クライアント装置は、トランザクションを実行するために信頼できる当事者に接続する（例えば、オンラインアカウントにログインする取引、金融取引など）。902において、信頼できる当事者は、リスク値及びユーザを認証するのに必要な保証レベルゲインを決定するために、クライアント装置に関連する任意の利用可能なデータを分析する。例えば、データは、ユーザが未知のネットワーク位置（例えば、以前にユーザが訪れたことがない外国）から信頼できる当事者に接続していること及び／又はクライアントと信頼できる当事者との間のネットワークルーティングホップ数又はレイテンシが閾値以上であることを示すことができる。そのような場合、リスク値は、比較的高い値に設定することができる（又は、逆に、暗黙的な保証レベルを低くすることができる）。しかしながら、ユーザがちょうど最近装置に対して明示的に（例えば、PIN入力）認証された場合、これはリスクレベルを減少させる（又は暗黙的な保証レベルを上げる）傾向がある。

20

【0075】

トランザクションを完了するために必要な保証レベルに基づいて、保証レベルゲインを決定することができる。これは、例えば、暗黙的な保証レベル+保証レベルゲイン=必要な保証レベル、又は、保証レベルゲイン=必要な保証レベル-暗黙的な保証レベルなどの式を使用して達成されることができる。更に本発明の基本原則を順守しながら、様々な他の式が保証レベルゲインを決定するために使用することができる。

30

【0076】

903において、必要な保証レベルゲインの指示が受信される。非侵襲型認証技術が904において判定された保証レベルゲインを満たすのに十分である場合、それらは、ユーザを認証するために905において使用される。そうでない場合、907において、1つ以上の明示的な認証モダリティが潜在的に1つ以上の非侵襲型認証モダリティと組み合わせて実施される。上述したように、エンドユーザにとって最も負担が少ないようにモダリティが選択されてもよい（例えば、ユーザが指定した好みに基づいて）。

40

【0077】

図10は、上述した本発明の実施形態が認証モダリティを決定するために保証レベルを評価することができる方法をグラフィカルに図示している。時間t1において、ユーザは、明示的な認証（例えば、指スワイプ、PIN入力など）を実行する。時間t2において、信頼できる当事者は、a14の保証レベルゲインで認証を要求する。非侵襲型認証モダリティは、a14よりも高い保証レベルの全てを提供するので、明示的な認証をトリガする必要はない。

【0078】

50

これとは対照的に、時間 t_4 において、信頼できる当事者は、 a_{l4} の保証レベルゲインで認証を要求する。非侵襲型認証モダリティは、(グラフに示されるように)、その時点で a_{l5} を提供する。その結果、この場合には、適応型認証部モジュールは、 a_{l5} から a_{l4} まで保証レベルを上げるために少なくとも1つの明示的な認証モダリティを選択する。

【0079】

本発明の1つの実施形態は、エンドユーザのプライバシーを保護するように暗黙的な位置ベースの認証技術を使用する。上述したように、信頼できる当事者と(例えば、GPSによって提供されるような)ユーザの現在位置を共有することは、重要なプライバシーの問題を提起する。したがって、ユーザは、大抵の場合、そのようなデータを共有したがない。

10

【0080】

これらの問題に対処するために、本発明の1つの実施形態は、暗黙的なユーザ認証を行う際の因子としてジオロケーションを使用するが、信頼できる当事者に対してユーザの位置を開示していない。この実施形態は、(例えば、より大きな包括的な認証処理の一部として)単独で又は上述した他の非侵襲型230及び/又は明示的222な認証技術と組み合わせる実施することができる。クライアント装置から実際の位置を送信する代わりに、唯一の保証レベルが(少なくとも部分的に)ジオロケーションデータに基づいて送信されてもよく、それによってユーザのプライバシーを保護する。

【0081】

20

1つの実施形態は、ユーザ/装置の登録及び信頼できる当事者による登録のために以下の操作を使用する。

【0082】

1. ユーザは、彼/彼女が通常ウェブサイトによって認証を実行する1つ以上の位置を取得して指定する。これは、予め定義されたマイル又は(職場、自宅、輸送ルートなどのような)特定の位置内の領域とすることができる。これらの選択された位置は、クライアント装置上でローカルに記憶されることができ、信頼できる当事者に送信されない。これらの動作は、上述した位置認証モジュール231によって実行することができる。

【0083】

2. 1つの実施形態において、登録が完了した後、クライアント装置は、(例えば、本明細書に記載されたセキュア通信モジュール213及び他の登録技術を使用して)セキュア通信チャンネルを介して信頼できる当事者と鍵を共有する。

30

【0084】

1つの実施形態において、認証時に以下の動作が実行される。

【0085】

1. クライアント装置は、1つ以上のジオロケーション技術(例えば、埋め込まれたGPSなどの位置センサ241を使用して現在位置を取得するなど)を使用してその現在位置を判定する。

【0086】

2. クライアントにおける位置認証モジュール231は、既に登録された位置と現在位置を比較し、距離を示すスコア(例えば0から100)を生成する。そして、保証計算モジュール212は、(上述したように)その保証計算においてスコアを含むことができる。

40

【0087】

3. クライアント装置は、署名を生成し、スコア/保証レベルに署名し、最終的な認証のために信頼できる当事者250に送信する。

C. 複合認証部

【0088】

本明細書に記載された本発明の実施形態のいくつかは、以下のセキュリティ関連機能をカプセル化するクライアント側の「認証部」を使用する：

1. 暗号化認証鍵の記憶及び使用

50

2. 暗号化認証鍵の生成、記憶及び使用
3. ローカルユーザ検証又はユーザの存在の検証
4. エンドユーザについての情報のセキュア表示

【0089】

1つの実施形態において、上記機能（例えば、図3及び図4）の一部は任意である。更に、本発明の1つの実施形態は、以下のセキュリティ目的を実現する認証部を含む。

1. 証明鍵が以下を確実にする：（a）FIDO認証によって生成されて保護された認証鍵を証明するためにのみ使用される及び（b）FIDO認証境界を離れることはない。

2. ローカルユーザ検証（「ユーザ認証」とも呼ばれることもある）がサポートされるように請求されている場合、（a）認証がソフトウェアアプリケーション（例えば、認証部にPINを「入力する」マルウェア）によってバイパス／偽造されることができないことを確実にする。（b）認証データの機密性は保護されている（例えば、マルウェアは、ユーザ又は参照データのいずれによっても入力されたピンにアクセスすることができない）、及び（c）ユーザ認証は、新たな認証鍵を生成する前及びそのような認証鍵を使用する前の到達時間の前に必要とされる。

【0090】

認証部を実装する1つの方法は、単一の保護シェルによって保護された単一モジュールにおいて上記機能を担う構成要素の全てを実装することである。例えば、認証部全体は、（例えば、信頼できる実行をサポートするクライアントプラットフォーム上）信頼された実行環境（TEE）において実行されている信頼できるアプリケーション（TA）において実装されることができる。この実装において、TAは、実行時に認証部を変更することができず且つTEEがTAを保護することを保証するように署名されている。

【0091】

本発明の1つの実施形態において、各認証部は、独立したセキュリティ及び認証機能を含むそれぞれが独立した複数の構成要素に論理的に分割される。例えば、図11において、単一のシェルで保護されている単一モジュールにおいて上記機能を担う構成要素の全てを実装するよりもむしろ、認証部1100は、以下の2つの別個の独立した認証部の構成要素によって実装される：それぞれ独自の保護ロジック1110及び1112を有するユーザ検証構成要素（UVC）1101及び認証部カーネル（AK）1103。この例において、AK1103は、認証部1100についての証明鍵1104と認証鍵1105をセキュアに管理し、UVC1101は、ユーザ認証／存在機能1106及びセキュア表示機能1107を管理する（その具体的な例は、以下及び同時係属出願に記載されている）。

【0092】

以下に詳細に述べられるように、各構成要素の保護ロジック1110、1112は、クライアント装置上で実行される1つ以上の他の構成要素によって全ての構成要素を認証するための構成要素の認証エンジンを含むことができる（例えば、図13及び関連する文書を参照）。更に、保護ロジックは、クライアントプラットフォームに組み込まれた追加のハードウェア／ソフトウェア保護機構を利用することができる（例えば、セキュア要素（SE）、信頼技術のチェーン、信頼されたユーザインターフェース技術、OSベースの保護機構など）。これらの実施形態のそれぞれに関連する詳細が以下に記載される。

【0093】

図12は、複数の論理認証部1201-1202が保護された認証部構成要素のセットから構築された本発明の実施形態を図示している。具体的には、論理認証部1201の構成要素構成ブロックは、ユーザ検証及び存在を管理するためのユーザ検証構成要素（UVC）1210、エンドユーザに表示された情報が正確にトランザクションによって確認されていることを保証するための表示構成要素（DC）1212（すなわち、「あなたが見るものはあなたが署名するものである（What you See is what you Sign）又はWYSIWYS）、並びに（登録プロセスの一部として信頼できる当事者に対する認証部のモデル及び／又は完全性を証明するための）証明鍵1215及び（信頼できる当事者ごとに一意の認証鍵を使用して信頼できる当事者とのセキュアな通信を確立

するための) 認証鍵 1 2 1 6 をセキュアに管理するための認証部カーネル (A K) 構成要素 1 2 1 4 を含む。論理認証部 1 2 0 2 についての構成要素構築ブロックは、ユーザ検証及び存在を管理するための U V C 1 2 2 0 と、証明鍵 1 2 1 5 及び認証鍵 1 2 1 6 をセキュアに管理するための認証部カーネル (A K) 構成要素 1 2 1 4 とを含む。それゆえに、この例において、複数の論理認証部は、鍵を管理して保護するための同一の基本 A K 構成要素 1 2 1 4 を共有する。本発明の他の実施形態において、他の種類の構成要素は、複数の認証部間で共有することができる。上述したように、構成要素のそれぞれは、上記セキュリティ目標を満たしていることを保証するために独自の独立した保護ロジックを備えている。

【0094】

それぞれが独自の保護シェルを有する独立した別個の構成要素から構成されていることから、このようにして構成要素から構築された認証部は、「複合認証部」と称される。複合認証部のアプローチの1つの利点は、構成要素が1つの認証部のために構築されると、複数の認証部間で使用することができ、それによって新たなセキュア認証部がより効率的に構築されるのを可能とするということである。例えば、図 1 2 に示されるように、同じ認証部カーネル構成要素 1 2 1 4 は、2つの論理認証部 1 2 0 1 - 1 2 0 2 の間で共有される。更に、それぞれの認証部構成要素は、その特定のニーズのために最適化された方法で実装されることができる。例えば、限定はしないが、生体認証セグメンテーション及び照会アルゴリズムがセキュア要素 (S E) 又は信頼できる実行環境 (T E E) 内で実装するには大きすぎるかもしれない顔認識ベースの認証部のその認証及びユーザ認証鍵を保護するために S E / T E E を更に利用することができる。この例において、ユーザ検証構成要素 (例えば、セグメンテーション及び照合アルゴリズムを含む) は、S E / T E E の外部で実行されることができ一方で、認証カーネル構成要素は S E / T E E 内に実装されてもよい。同様に、T E E において実装される指紋ベースの認証部は、例えば、その証明及びユーザ認証鍵を保護し、したがって差分電力分析 (D P A) のようなハードウェアベースの攻撃に対して保護するために S E 認証カーネルを更に利用することができる。

【0095】

1つの実施形態において、以下のセキュリティ対策は、本明細書に記載された構成要素の認証部のためのセキュリティの許容レベルを提供するために実装される (例えば、上記指定されたセキュリティ目的を満たすために「許容される」)。これらのセキュリティ対策は、図 1 2 における認証部 1 2 0 1 を実装するために使用される構成要素 1 2 1 0、1 2 1 2、1 2 1 4 のそれぞれに関連する追加の詳細を示す図 1 3 を参照して説明される。

1. セキュリティ対策 (S M) 1: 1つの実施形態において、各構成要素 (例えば、図 1 2 ~ 1 3 に示されるユーザ検証構成要素 1 2 1 0、表示構成要素 1 2 1 2 又は認証カーネル 1 2 1 4) は、他の構成要素に登録して他の構成要素に送信されるメッセージを認証するために (潜在的に相互に) 使用されるそれ自身の「構成要素認証鍵」対 (C A K) (例えば、それぞれ C A K 対 1 3 0 4、1 3 0 5 及び 1 3 0 6) を有する。図 1 3 に示されるように、各構成要素 1 2 1 0、1 2 1 2、1 2 1 4 は、それぞれ C A K 対 1 3 0 4、1 3 0 5、1 3 0 6 を使用して、構成要素間の認証トランザクションに入るために、それぞれ、構成要素の認証ロジック 1 3 0 1、1 3 0 2、1 3 0 3 を含む。1つの実施形態において、本発明の基本原理は、そのような実装に限定されるものではないが、C A K 対 1 3 0 4、1 3 0 5、1 3 0 6 は、公開／秘密鍵対である。この実装において、構成要素のそれぞれは、それが認証する必要があるこれらの構成要素の公開鍵を備えている。例えば、U V C 1 2 1 0 は、D C 及び A K の公開鍵 (又は、少なくとも公開鍵を検証することができる) 1 3 2 1 を知っており、D C 1 2 1 2 は、U V C 及び A K の公開鍵 1 3 2 1 を知っており、A K 1 2 1 4 は、D C 及び U V C の公開鍵を知っている。1つの実施形態において、起動時に、構成要素は、これらの構成要素とその公開鍵を共有することによって通信する必要のある他の構成要素の登録トランザクションに最初に入る。そして、以下に記載される技術を使用してこれらの構成要素を使用して認証することができる。

2. セキュリティ対策 (S M) 2: 各構成要素は、これらの構成要素の公開 C A K を検

10

20

30

40

50

証することによってメッセージを受信する他の構成要素を認証することが可能である。例えば、図13において、AK1214は、全てのUV C1210及びDC1212の公開CAKを検証することができ、それは（すなわち、CAK対1304及び1305における公開鍵）をサポートしている。UV C及びDCはまた、相互認証が実装されている場合、AK1214の公開CAK（すなわち、CAK対1306）を検証することができる。
【0096】

図14は、2つの構成要素（AK1214及びDC1212）の間で認証を実施することができる方法を図示するトランザクション図である。トランザクション1400において、AKの構成要素認証ロジック1303は、チャレンジを生成し、トランザクション1401において、DCの構成要素認証ロジック1302に送信する。1つの実施形態において、チャレンジは、構成要素認証ロジック1303によって選択された乱数又はナンスである。操作1402において、DCの構成要素認証ロジック1302は、そのCAK対1305からの秘密鍵を使用してチャレンジにわたって署名及び潜在的に追加データ（例えば、ユーザがトランザクションの内容を承認したかどうか）を生成する。当業者によって理解されるように、署名を生成することは、秘密鍵を用いてチャレンジにわたってハッシュ関数を実装することを含むことができる。トランザクション1403において、DCの構成要素認証ロジック1302は、検証のためにAKの構成要素認証ロジック1303に署名を返送する。AKの構成要素認証ロジック1303は、現在のチャレンジ（例えば、それが以前に生成されたナンス）、DCのCAK対の秘密鍵を用いて生成された署名、及び、DCのCAK対の公開鍵を知っている。トランザクション1404では、乱数を使用して署名を検証するためにDCのCAKペアの公開鍵を使用し、それによってDCを認証する。DCはまた、相互認証が実装される場合、同様のトランザクションのセットを使用してAK1214の公開鍵を検証することができる。

3. セキュリティ対策（SM）3：特定の実装に応じて、追加のセキュリティ機構は、構成要素間の通信を保護するために利用することができる。補足ハードウェア／ソフトウェア保護機構1310としてこれらの追加のセキュリティ機構が図13に図示されている。例示として、限定されるものではないが、例を挙げると、これらのハードウェア／ソフトウェア保護機構1310は、セキュア要素（SE）、信頼技術のチェーン、信頼できるユーザインターフェース技術、OSレベルのアクセス制御機構、ホワイトボックス暗号化、コード難読化及び実行の完全性保護などのクライアントプラットフォームに組み込まれたそれらの機構を含むことができる。ARM（登録商標）TrustZone（商標）又は類似の技術を使用して、例えば、オペレーティングシステムは、（例えば、正当UV C及びDCなどの）信頼できるプログラムのみに対するAKのアプリケーションプログラミングインターフェース（API）へのアクセスを制限することができる。他の例として、オペレーティングシステムはまた、AKに対する任意のAPI呼び出しに対してUV C又はDCのパッケージ識別子を追加することができる。しかしながら、本発明の基本原理は、上述した特定のハードウェア／ソフトウェア保護機構に限定されないことに留意すべきである。

【0097】

例示として、1つの実施形態において、AK1214は、暗号化鍵のための良好な保護機構を提供するが、ユーザインターフェースを有していないセキュア要素内のアプレットとして実装される。UV C1210は、双方ともARM TrustZone又は類似の技術を利用するハードウェア（例えば、指紋センサ）及び信頼できる実行環境内の信頼できるアプリケーションの組み合わせとして実装されることができる。DC1212は、グローバルプラットフォームによって定義されたような「信頼できるユーザインターフェース」機能を使用して、信頼できるアプリケーションとして実装されることができる。それゆえに、本実施形態において、ユーザが指紋センサ上で指をスワイプすると、信頼できるアプリケーションが起動し、記憶された基準データに対して指紋データを検証する。そして、スコアは、（例えば、同時係属出願に記載されているように）ユーザを認証するために信頼できる当事者1320によって一連の認証トランザクションにその後に入るセキュ

ア要素として実装された A K 1 2 1 4 に送信される。

【0098】

更に、異なる U V C は、ホワイトボックス暗号化、コード難読化及びランタイム完全性保護の組み合わせを使用してリッチ O S（例えば、アンドロイド）において実行されているソフトウェア構成要素として実装されてもよい。例えば、顔認識ソフトウェアとの組み合わせで統合されたビデオカメラを使用することができる。他の U V C は、ホワイトボックス暗号化、コードの難読化及びランタイム完全性保護の組み合わせを使用してリッチ O S 上で実行され且つ P I N ベースのユーザ検証方法を提供する信頼できるアプリケーション又はソフトウェアとして実装されてもよい。

【0099】

それゆえに、本明細書に記載された構成要素ベースのアプローチは、異なる認証技術の要件に容易に適合可能である。例えば、音声認識や顔認識などのいくつかの種類の認証は、かなりの記憶要件及びこれらの認証種類のハードウェアインターフェース要件のために、通常の立地オペレーティングシステムを使用してソフトウェア構成要素として実装される必要がある。これらの異なる種類の認証の全ては、（説明したように、セキュア要素として実装することができる）同じ A K 構成要素を利用する異なる U V C 構成要素を使用して、セキュアな信頼できる方法で実装されることができる。

【0100】

上記アプローチにより、様々な構成要素は、暗号的に保護された（例えば、署名された）メッセージを使用して論理的に通信することに留意されたい。この論理的な通信は、（例えば、以下に説明されたセキュアトランザクションロジックなどの）いくつかの他のエンティティによって更に「促進」することができる。更に、1つの実施形態において、本明細書に記載された論理構成要素間メッセージングは、（例えば、それぞれ証明鍵 1 2 1 5 及び認証鍵 1 2 1 6 を使用して）認証部カーネル 1 2 1 4 と直接的に証明及び認証トランザクションに入る信頼できる当事者 1 3 2 0 に対して透過的である。1つの実施形態において、A K は、登録時に認証部のモデル及び／又は完全性を検証するために証明鍵 1 2 1 5 を使用する。例えば、信頼できる当事者は、A K が証明鍵 1 2 1 5 を使用して署名するチャレンジを送信することができる。そして、信頼できる当事者は、署名を検証するために対応する鍵（例えば、証明鍵が秘密鍵である場合には公開鍵）を使用する。認証部が信頼できる当事者に登録すると、認証鍵 1 2 1 6 は、その信頼できる当事者に割り当てられる。そして、A K は、登録後にその信頼できる当事者とのセキュア通信を確保するために信頼できる当事者に関連付けられた認証鍵 1 2 1 6 を使用する。

【0101】

追加のセキュリティ対策として、1つの実施形態において、各構成要素の構成要素の認証ロジック 1 3 0 1 - 1 3 0 3 は、構成要素妥協点が検出された場合には、その C A K 対を削除することができる。

【0102】

以下の2つの異なる種類の複合認証部が本発明の基本原理を利用して実装されることができる：「静的」複合認証部及び「動的」複合認証部。

静的複合認証部

【0103】

図 1 5 を参照すると、1つの実施形態において、以下の特性を有する複合認証部 1 5 0 1 は、本明細書において「静的」複合認証部と称される。

1. 各認証部 1 5 0 1 について、信頼できる当事者 1 3 2 0 は、（公開「構成要素認証鍵」（C A K）1 3 0 4、1 3 0 6 ではなく証明鍵対 2 1 5 に対応する）公開証明鍵に対するアクセスを有する／必要がある；及び鍵

2. 構成要素（例えば、U V C、D C 及び A K）の各サポートされた組み合わせについて、特定の認証部証明 I D（A A I D）1 5 0 5 が事前に指定されている。

【0104】

それゆえに、図 1 5 に示されるように、静的複合認証部について、各個別の認証部 1 5

10

20

30

40

50

01は、その特定のAAID1505によって特定される。AKは、1つ以上の認証鍵215を所有しており、また、信頼できる当事者1320とのトランザクションを行う際に使用されることになる予め定義されたAAID（及び関連する証明鍵）の1つを選択する。

【0105】

CAK対は、信頼できる当事者1320と共有されることはないことから、ユーザのプライバシーに影響を与えることなく認証部固有とすることができる。これはまた、個々の構成要素の成功したハッキングが検出された場合、そのような鍵は個別に取り消すことができることを意味する。CAKは、（公開的に視認可能な）「証明鍵」として使用されないことから、構成要素のハッキングは、認証部のハッキングと同等であると考えられない。更に、複合認証部1501の通信及びセキュリティ機構は、認証部外に視認可能でないことから、静的複合認証部の実装は、認証部1501と信頼できる当事者1320との間の相互作用を定義する仕様に影響しない。1つの実施形態において、各構成要素1510、1514には、AAIDと同様とすることができる固有の構成要素IDが割り当てられるが、それはAK1514にのみ関係する（RP又は他の外部エンティティには関係しない）。

10

【0106】

更なる最適化として、1つの実施形態において、オンライン証明書状態プロトコル（OCSP、RFC2560）は、各CAK証明書についての失効確認方法（例えば、「検証」）として使用することができる。具体的には、AK1514は、入力メッセージを受け入れるために公開CAKに関連するUVC又はDCの証明のために十分に最近のOCSP応答を必要とすることがある。AK1514はまた、全てのAAIDために使用される1つの証明鍵を有することができ、又は、それは、AAIDあたり1つの証明鍵又はそれらの組み合わせを必要に応じて有することができる。

20

【0107】

1つの実施形態において、AKはAAIDの静的リストを維持することができる。あるいは、それは、リストを更新するために使用される署名された「AAID更新」メッセージの一部である場合、外部エンティティ（例えばUVC／DC）から受信されたAAIDを許容することができる。1つの実施形態では、AAAID－更新メッセージは、以下の構造を有する：署名（`signing__key`、`AAID | AK－Component－ID | UVC／DC`の公開CAK）。プライベート`signing__key`は、AKベンダーによって所有されることができる。公開`signing__key`は、（信頼ストア実装における）AKの信頼ストアの直接的な部分であるか又は（すなわち、そのような証明書にチェーンされる）信頼ストアに記憶されたいくつかの証明書を使用して検証されることができる。

30

【0108】

図15に示されるユーザ装置1500のアーキテクチャはまた、信頼できる当事者1320との通信を確立するためのブラウザ／アプリケーション1510と、認証部との通信を可能とするためのセキュアトランザクションロジック1520とを含む。例えば、図示されたように、1つの実施形態において、セキュアトランザクションロジック1520は、様々な構成要素についてのアプリケーションプログラミングインターフェース（API）を露出することによって各認証部1501の構成要素1510、1514の間をメッセージが通過するのを可能とする。それゆえに、本実施形態において、登録データとメッセージの交換などの構成要素間の全ての通信は、セキュアトランザクションロジック1520を介して生じる。例示として、セキュアトランザクションロジック1520はまた、（その一部が以下に記載された）同時係属出願に記載された「セキュアトランザクションサービス」として実装することができる。ブラウザ／アプリケーション1510は、インターネットなどのネットワークを介して信頼できる当事者1320との通信を確立するために使用することができる。

40

動的複合認証部

【0109】

50

図16を参照すると、以下の特性を有する複合認証部1601は、「動的複合認証部」である：

1. 信頼できる当事者1320が（例えば、OSTP仕様において「鍵登録データ」と称される）証明メッセージを検証するために関連する公開鍵を有し且つ必要とするように、「構成要素認証鍵」（CAK）1604、1604が証明鍵として処理される場合；及び且つ

2. 信頼できる当事者1320が（認証部1601内の構成要素の数に応じた）複数のAAID1602、1603を受信する場合。1つの実施形態において、それは、セキュアトランザクションロジック1620及びブラウザ／アプリケーション1610を介してAK1614から送信された登録メッセージの一部として認証部1601の全ての構成要素1610、1614のAAID1602、1306を受信する。図16は、UVC1610及びAK1614のみを図示しているが、（図3に示されるような）代替実施形態は、AK、DC及びUVCについてのAAIDをRP1320に送信する。上述したように、しかしながら、本発明の基本原理は、認証を実現するための構成要素の任意の特定のセットに限定されるものではない。1つの実施形態において、RP1320に送信された登録メッセージはまた、複数の（連鎖した）署名、AKの証明鍵1605を有するもの及び他の構成要素（例えば、UVCの証明鍵1604及びDCの証明鍵（図示しない））のそれぞれについてのものを有する。上述したように、1つの実施形態において、AK1614は、他の構成要素との通信を信頼する場合にのみRP1320に対する独自の証明メッセージ内に他の構成要素の証明メッセージを含む。

【0110】

それゆえに、動的に構成された認証部1601は、動的に複数の構成要素を組み合わせることによって（又は、新たな認証部を取得するために2つの認証部を構成する当該他の方法で）実現される。CAKはこの実装においてRPに関連していることから、それらは、ユーザのプライバシーを保護するために1つの実施形態において特定の認証部である必要がない。代わりに、それらは、共有鍵として事前生成／投入されるか、又は、直接匿名認証（DAA）方式、ユーザのプライバシーを維持しながら信頼できるプラットフォームの認証を可能とする暗号化プロトコルを使用して認証される。複数のAAID及び連鎖した証明メッセージがRPに視認可能であるため、動的複合認証部の実装は、認証部1601と信頼できる当事者1320との間で使用される認証仕様に影響を与える。

UVC／DC証明検証

【0111】

動的又は静的認証部が使用されるかどうかにかかわらず、1つの実施形態において、UVC210及びDC212は、AK214と信頼できる当事者1320との間で使用される認証仕様に応じて処理されることができるよう、ユーザ検証結果（UVC）及びAK214に対する表示されたトランザクションテキスト（DC）のユーザの承諾などのそれらの出力データを送信する。

【0112】

登録のために、静的認証部による実施形態において、UVC210及びDC212は、構成要素ID（AAIDではない）を含むAK214に鍵登録メッセージを送信ことができ、構成要素IDは、AAIDに類似の識別子であるが、AKにのみ関連している。1つの実施形態において、鍵登録メッセージのユーザ認証鍵は空であり、鍵登録メッセージは、証明鍵の代わりにCAKによって署名される。

【0113】

認証のために、1つの実施形態において、UVC210及びDC212は、CAK（ユーザ認証鍵ではない）によって署名されたメッセージを作成する。

【0114】

以下の検証ステップは、本発明の1つの実施形態においてAKによって実現される。

1. 許容可能な公開CAKのリストを含む内部信頼ストアを検索する。公開CAKは、信頼ストアに直接記憶されてもよく又は信頼ストアにおいてルート証明書に連鎖するCA

Kのそれぞれについての公開鍵証明書であってもよい。

2. AKは、(例えば、SM1及びSM2に関して上述したように) 公開CAKを使用してUV C及び／又はDCからの入力データの署名を検証する。

3. 入力データのパッケージID又は類似のプラットフォームに提供された保護機構を使用するなどの追加のプラットフォーム固有の保護機構を検査する。

4. UV C又はDCの公開CAKを含む証明書の失効状態を検査する。AKは、証明書／鍵(すなわち、現在のUV C又はDCの)の非常に少数の失効情報にのみ関心があるため、(上述した) オンライン証明書状態プロトコル(OCSP)は、失効検査のために使用することができる。AKは、ネットワーク接続を有すると仮定されておらず、そのため、OCSP応答は、UV C及び／又はDCからの入力データの一部として予測される。

10

最適化された検証方法

【0115】

非対称鍵操作が対称鍵操作に比べて非常に高価であるのに対して、更なる最適化は、1つの実施形態で実現されることができる。そのような場合、AKに送信されるUV C及び／又はDCによって作成された鍵登録メッセージは、(例えば、上述したように空のユーザ認証鍵フィールドの代わりに) 対称鍵SKを含む。UV Cによって生成され且つAKに送信された変更された鍵登録データメッセージは、AKの公開CAK(又はターゲット構成要素に属するいくつかの他の信頼された公開鍵)を使用して暗号化されてもよい。UV C及び／又はDCによって生成され且つAKに送信された変更された署名メッセージは、CAKを使用して非対称的に署名されず、代わりに、SKによって計算されたハッシュベースのメッセージ認証コード(HMAC)を使用してセキュアにされる。AKは、鍵登録データメッセージの一部として受信した対称鍵を使用してHMACを検証する。

20

D. 位置認識認証技術

【0116】

本発明の1つの実施形態は、認証機構が認証のために使用されるクライアント装置の物理的位置に基づいて選択されるのを可能とする認証ポリシーを実装する。例えば、クライアント及び／又はサーバは、クライアント装置の物理的位置の判定を行うことができ、ポリシーールの順序付けられたセットを評価するポリシーエンジンにその位置を供給する。1つの実施形態において、これらのルールは、クライアントの位置がルール内の位置定義と一致した場合に適用されなければならない位置及び認証機構又は機構のクラスを指定する。

30

【0117】

図17に示されるように、本発明の1つの実施形態は、本明細書に記載された位置認識認証ポリシーを実現するための認証ポリシーエンジン1710を有するクライアント装置1700を含む。特に、本実施形態は、現在位置「クラス」を特定するために位置センサ1741(例えば、GPS装置)によって提供されるクライアント装置1700の現在位置を使用するための位置クラス判定モジュール1740を含む。以下に詳細に述べられるように、異なる位置「クラス」は、既知の地理的地点及び／又は領域を含んで定義されることができる。位置クラスデータは、継続的に更新され、持続的位置データ記憶装置1745(例えば、フラッシュ記憶装置又は他の持続的記憶装置)に記憶されることができる。そして、位置クラス判定モジュール1740は、クライアント装置1700についての現在位置クラスを判定するために、定義された「クラス」に対してセンサ1741によって提供される現在位置を比較することができる。

40

【0118】

1つの実施形態において、信頼できる当事者1750は、(信頼できる当事者から認証ポリシーエンジンへの点線で示すように) 各トランザクションについての認証ポリシーエンジン1710によって実装されるように認証ポリシーを指定する。それゆえに、認証ポリシーは、各信頼できる当事者の認証要件に固有に調整されることができる。更に、必要な認証のレベルは、(認証ポリシーによって定義されるように) 現在のトランザクションに基づいて決定することができる。例えば、かなりの量の金の転送を必要とするトランザ

50

クションは、比較的高い認証保証閾値を必要とすることがあるのに対して、非金融トランザクションは、相対的に低い認証保証閾値を必要とすることができる。それゆえに、本明細書に記載された位置認識認証技術は、特定のトランザクションについては十分であり得るが、他のトランザクションについてはより厳密な認証技術と組み合わせることができる。

【0119】

1つの実施形態において、位置クラス判定モジュール1740は、判定されたクラスに使用する認証技術1712を識別するためのルールセットを実装する認証ポリシーモジュール1711に対して判定されたクラスを提供する。例示として、限定されるものではないが、図18は、それぞれの定義された位置クラス1-5に使用することができる1つ以上の認証技術1-5を指定するルール1-5の例示的なセットを図示している。図18においてテーブルデータ構造として示されているが、本発明の基本原理は、ルールセットを実装するための特定の種類のデータ構造に限定されるものではない。

10

【0120】

認証ポリシーエンジン1710が認証技術1712のセットを選択すると、認証ポリシーエンジン1710は、信頼できる当事者1750によってユーザを認証するための1つ以上の明示的なユーザ認証装置1720-1721及び／又は非侵襲型認証技術1742-1743を使用して技術を実装することができる。例示として、限定されるものではないが、例を挙げると、明示的なユーザ認証1720-1721は、PIN、指紋認証、音声や顔認識及び網膜スキャンなどの秘密コードを入力するようにユーザに要求することを含むことができる。

20

【0121】

非侵襲型認証技術1742-1743は、ユーザを認証するためのユーザの行動に関するデータを収集するユーザ行動センサ1742を含むことができる。例えば、ユーザの生体歩行は、ユーザの通常の歩行パターンの歩行「指紋」を生成するように設計されたソフトウェア及び／又はハードウェアと組み合わせて、加速度計又は他の種類のセンサ1742を使用して測定することができる。以下に説明するように、他のセンサ1743は、認証に使用されるデータを収集するために使用することができる。例えば、ネットワークデータは、クライアント装置1700（例えば、既知のピアコンピュータ、アクセスポイント、セルタワーなど）の局所近傍内のネットワーク／コンピューティング装置を識別して収集することができる。

30

【0122】

1つの実施形態において、セキュア記憶装置1725は、認証装置1720-1721のそれぞれに関連付けられた認証鍵を記憶するために使用されるセキュア記憶装置である。以下に説明するように、認証鍵は、セキュア通信モジュール1713を介して信頼できる当事者1750とのセキュア通信チャンネルを確立するために使用することができる。

【0123】

位置の様々な異なる「クラス」は、本発明の基本原理と一致して定義されることができる。例示として、限定されるものではないが、以下の位置のクラスを定義することができる。

【0124】

クラス1：クライアントは、指定した位置の指定した半径内にある。このクラスにおいて、現在のクライアントの位置が指定された緯度及び経度を中心とする所定の半径の円で囲まれた領域内にある場合、関連付けられた認証ポリシーが適用される。

40

【0125】

クラス2：クライアントは、指定した境界領域内にある。このクラスにおいて、クライアントが緯度及び経度の対の順序付けられたセット（例えば、閉じた多角形）によって定義されたポリゴンによって囲まれた領域内に配置されている場合、関連付けられた認証ポリシーが適用される。

【0126】

クラス3：クライアントは、指定した境界の外側にある。このクラスにおいて、クライアントが緯度及び経度の対の順序付けられたセット（例えば、閉じた多角形）によって定

50

義されたポリゴンによって囲まれた領域の外側に配置されている場合、関連付けられた認証ポリシーが適用される。

【0127】

1つの実施形態において、追加のクラスは、上記定義されたクラス及びポリシールールのブール組み合わせを使用して定義される。例えば、ブール演算AND、OR、NOT及びブール演算のネストは、複雑な条件の発現を可能とする。そのようなポリシーは、例えば、クライアントが企業によって所有される様々な施設の1つに位置している場合に適用されるポリシーを実装するために使用することができる。

【0128】

限定されるものではないが以下を含む様々な異なる機構が（一般に位置センサ1741として図17に示される）クライアントの現在の物理的位置を判定するために使用することができる：

【0129】

GPS：組み込み型GPSセンサは、クライアントの位置の詳細を直接提供することができる。新たに発現する規格は、現在のGPS解決策においてこの欠点を解決する機能として提供される位置の認証を追加しようとする。

【0130】

ジオーIPルックアップ：クライアントのIPアドレスの逆引きは、クライアントの位置の粗近似を判定するために使用することができる。しかしながら、この方法によって得られた位置の信頼性は、IPアドレスがプロキシプロバイダを匿名化する既知の妥協ホストのブラックリストに対してクロスチェックするのを必要とするか又はホストの送信元IPアドレスを難読化するように設計された同様の解決策を必要とする。

【0131】

セルタワー三角測量：クライアント、サーバ及び無線キャリアインフラストラクチャ間の統合は、クライアント及びサーバが携帯信号強度三角測量を使用して物理的位置の高解像度判定を行うのを可能とする。

【0132】

Wi-Fiアクセスポイント三角測量：物理的位置を判定するための高解像度の方法は、既知の物理的位置を有する近隣のWi-Fiアクセスポイントの信号強度を三角測量することである。この方法は、施設内の装置の位置を判定する際に特に有効である。

【0133】

位置変位推定：装置の正確な位置は不明であってもよいが、位置の統計的確率は、ポリシーを評価する目的のために近似値として使用することができる。これは、既知の位置を有する開始点に対するデバイスの位置の変化に注目することによって計算されることができ、ユーザのデバイスは、過去に、既知の開始点を有していてもよく、その間におおよその位置を計算するのを可能とする既知又は推定距離及び方位を移動する。開始点からの変位を計算するための可能な方法は、加速度計（すなわち、歩行測定に基づいてユーザがどの程度歩行したかを測定するために加速度計を使用して）から収集された測定値、信号源の既知の固定セットからの信号強度の変化及び他の方法を使用して移動した推定距離を含むことができる。

【0134】

図19は、位置認識認証ポリシーを実装するための方法の1つの実施形態を図示している。本方法は、図17-18に示されたシステムアーキテクチャのコンテキスト内で実行されることができるが、任意の特定のシステムアーキテクチャに限定されるものではない。

【0135】

1901において、クライアントの位置は、1つ以上の利用可能な技術（例えば、GPS、三角測量、ピア／ネットワーク装置検出など）を使用して特定される。1902において、1つ以上の位置クラス（及びクラスの潜在的ブール組み合わせ）は、ポリシールールの既存のセットに基づいて現在位置について特定される。1903において、1つ以上の認証技術が位置クラスに応じて特定される。例えば、クライアント装置がユーザの自宅

10

20

30

40

50

又は職場又は他の信頼できる位置の定義された範囲内にあるように既知の位置に現在ある場合、最小の認証が必要とされることができ（又は全く必要とされない）。これに対して、クライアント装置が未知の位置及び／又は信頼できない既知の位置に現在ある場合、より厳密な認証（例えば、指紋スキャンなどの生体認証、PIN入力など）を必要とすることがある。1904において、認証技術が採用され、1905において認証が成功したと判定された場合、1906において認証を必要とするトランザクションが許可される。

【0136】

上述したように、必要な認証のレベルは、現在のトランザクションに基づいて決定することができる。例えば、かなりの量の金の転送を必要とするトランザクションは、比較的高い認証保証閾値を必要とすることがあるのに対して、非金融トランザクションは、相対的に低い認証保証閾値を必要とすることができ。それゆえに、本明細書に記載された位置認識認証技術は、特定のトランザクションについては十分であり得るが、他のトランザクションについてはより厳密な認証技術と組み合わせることができる。

【0137】

認証が成功しない場合、トランザクションは、1907においてブロックされる。この段階で、トランザクションは、完全にブロックされてもよく、又は、追加の認証ステップを要求することができる。例えば、ユーザが間違ったPINを入力した場合、ユーザは、PINを再入力する及び／又は生体認証を実行するように要求することができる。

【0138】

本明細書に記載された本発明の実施形態は、認証システムにとって多くの利点を提供する。例えば、記載された実施形態は、不正な位置からのアクセスを効率的にブロックし、（例えば、位置クラスによって定義されたように）認証を試行するようにユーザが許可された位置を制限することによって不正なアクセスを減らすために使用することができる。更に、本発明の実施形態は、位置固有のリスクに対応するために強力な認証を選択的に必要とすることがある。例えば、ユーザ／クライアントが不明又は予測されない位置から接続されたときに強力な認証を必要とする能力を保持しながら、信頼できる当事者は、ユーザが既知の場所からトランザクションに入っているときに認証の不便を最小化することができる。更に、本発明の実施形態は、情報に対する位置認識アクセスを可能とする。あるいは、位置中心のポリシーは、位置固有情報に対する追加のアクセスをユーザに提供するために信頼できる当事者によって使用されてもよい。例示として、限定されるものではないが、ウォルマートに位置するユーザは、自己の携帯電話においてAmazon.comのアカウントにログインするとき、Amazon.comからの特別オファーへのアクセスを許可されることができる。

【0139】

上述したように、クライアント装置1700の位置は、様々な異なる技術を用いて決定することができる。特定の一実施形態において、「位置」の定義は、（GPSのように）物理的座標のセットに結合されることはなく、代わりに、ピアデバイス又は他の種類のネットワークデバイスのセットの存在によって規定される。例えば、動作時に、クライアントの無線ネットワークアダプタ（例えば、Wi-Fiアダプタ、ブルートゥースアダプタ、LTEアダプタなど）は、一貫した基準でピアネットワークデバイス（例えば、他のコンピュータ、携帯電話、タブレットなど）及びネットワークインフラストラクチャデバイス（例えば、Wi-Fiアクセスポイント、セルタワーなど）のセットを「見る」ことができる。それゆえに、これらのデバイスの存在は、ユーザが動作時に認証のために使用することができる。他の位置は、ユーザが自宅にいるときと同様にしてデバイスの存在によって定義されることができる。

【0140】

例えば、本明細書に記載された技術を用いて、位置は、「仕事の同僚と」又は「職場で」として定義することができ、ユーザの仕事の同僚によって所有されることが知られているピア装置のセットの存在は、認証ポリシーによって軽減する必要があるリスクについてプロキシとして使用することができる。例えば、ユーザが既知のピア装置又は他の種類の

10

20

30

40

50

ネットワーク装置のセットに囲まれている場合、ユーザは、既知の装置が検出されない場合よりもリスクが少ないとみなされることができる。

【0141】

図20は、「位置」がピア装置及び他のネットワーク装置のセットによって定義されている1つの実施形態を図示している。図示の例では、クライアント装置1700は、2つの異なるピア装置2005-2006（例えば、クライアントコンピュータ、モバイル電話、タブレットなど）、2つの異なる無線アクセスポイント2010-2011；及び2つの異なるセルタワー2020-2021を「見る」。本明細書において使用される場合、クライアント装置1700は、他の装置のそれぞれとの接続を形式的に確立せずに「見る」ことができる。例えば、クライアントは、作動LANに接続された様々なピア装置を見ることができる及び／又はクライアントがそれらの装置に接続するかどうかにかかわらずそれらの装置によって生成された無線信号を見ることができる。同様に、クライアント装置1700は、様々な異なるWi-Fiアクセスポイント（例えば、近くのホテル、コーヒーショップ、作動Wi-FiアクセスポイントからのWi-Fi）についての基本サービスセット識別（BSSID）を見ることができる。クライアント装置1700はまた、潜在的に更に異なるセルキャリアによって運営される様々な異なるセルタワー2020-2021を見ることができる。これらの装置の存在は、ユーザの作動位置についての位置「指紋」を定義するために使用することができる。

【0142】

図示されたように、クライアント装置1700における装置近接検出口ジック2001は、視認可能な装置に関連するデータをキャプチャし、過去の装置近接データ2004に対して結果を比較することができる。過去の装置近接データ2004は、経時的及び／又はトレーニング処理によって生成することができる。例えば、1つの実施形態において、ユーザは、彼／彼女が工作中であるとき、自宅で又は他の位置で指定することができる（手動で又はクライアント1700によってそうするように要求したとき）。それに応じて、装置近接検出口ジック2001は、近傍の装置を検出し、持続的に過去の装置近接データ2004として結果を記憶することができる。ユーザがその後に位置に戻ると、装置近接検出口ジック2001は、両者の相関を生成するために過去の近接データ2004として記憶された装置に対して現在「見る」ように装置を比較することができる。一般に、相関が強いと、クライアントが指定した位置にある可能性が高い。時間の経過とともに、定期的に見られている装置は、（例えば、これらの装置は、ユーザの作動位置とより正確な相関を提供する傾向があるため）過去の装置近接データ2004において他の装置上に優先順位付けすることができる。

【0143】

1つの実施形態において、認証ポリシーエンジン1710は、各信頼できる当事者1750についてユーザによって必要とされる認証のレベルを判定するために、装置近接検出口ジック2001によって提供される相関結果を使用することができる。例えば、高い相関が存在する場合（すなわち、指定された閾値以上）、認証ポリシーエンジンは、エンドユーザによる明示的な認証を必要としない。これとは対照的に、ユーザの現在位置と過去の装置近接データ2004との間に低い相関がある場合（すなわち、指定された閾値未満）、認証ポリシーエンジン1710は、より厳密な認証（例えば、指紋スキャンなどの生体認証及び／又はPIN入力要求）を必要とすることができる。

【0144】

1つの実施形態において、装置近接検出口ジック2001は、認証されたクライアントの近傍にある他の装置のセットを識別する。例えば、ユーザの同僚のいくつかは既に正常に認証された場合、ユーザが彼／彼女のピアの存在下で動作しているという理由だけで、ユーザが信頼性の低い認証部によって所定のデータにアクセスするのを可能とするように関連付けられた低いリスクがあってもよい。本実施形態において、802.11nなどの規格上のピアツーピア通信は、これらのピアが既に認証されていることを証明するために使用することができるピアから認証トークンを収集するために使用することができる。

【0145】

他の実施形態において、装置近接検出口ジック2001はまた、（例えば、ユーザの携帯電話又はタブレットなどの）ユーザのクライアントと対にされる以前に認証された装置を検出することができる。認証しようとしている同一のユーザによって使用される他の認証装置の存在は、特に同じアプリケーションにアクセスするとき、認証決定に対する入力として使用することができる。

【0146】

1つの実施形態において、過去の装置近接データ2004は、収集されて複数の装置間で共有され、中間認証サービスに記憶されて維持されることができる。例えば、各位置におけるピア及びネットワーク装置のグループの履歴が追跡されて各装置の装置近接検出口ジック2001にアクセス可能な中央データベースに記憶されることができる。このデータベースは、特定の位置から試行される認証のリスクを判定するための入力として使用されることができる。

E. 補足センサ及び／又は位置データを使用した位置確認についての実施形態

【0147】

上述したように、本発明の1つの実施形態は、認証に使用されるリスク計算に対する補足入力を提供するためにモバイル装置からの追加センサ1743からのデータを利用する。これらの補足入力は、エンドユーザの装置の位置の主張を確認するか又は反論するかに役立つことができる保証の追加レベルを提供することができる。

【0148】

図21に示されるように、装置の位置の補足的な保証を提供する追加センサ1743は、温度センサ2101、湿度センサ2102及び圧力センサ2103（例えば、気圧又は高度計圧力センサ）を含むことができる。1つの実施形態において、センサは、位置センサ1741によって提供される位置（又は本明細書に記載された様々な他の技術を用いて導出される位置）について既知の補足データ2110に対して相関をとるために、認証ポリシーエンジン1710の補足データ相関モジュール2140によってそれぞれ使用される温度、湿度及び圧力測定値を提供する。そして、相関の結果は、特定のトランザクションのために1つ以上の認証技術1712を選択するために認証ポリシーモジュール1711によって使用される。図21に示されるように、補足位置データ2110は、外部ソース（例えば、インターネット又はその他のモバイル装置）及びローカルデータソース（例えば、装置が正当ユーザの所有であることが知られている期間中に収集された履歴データ）から収集されたデータを含んでいてもよい。

【0149】

補足データ相関モジュール2140は、補足位置データ2110に対して相関をとるために様々な異なる方法で追加センサ1743によって提供されるデータを使用することができる。例えば、1つの実施形態において、補足位置データ2110は、位置センサ1741によって提供される位置における現在のローカル気象条件を含む。リアルタイムローカル気象データ2110に対する追加センサ1743から収集された湿度、温度又は気圧を比較することにより、補足データ相関モジュール2140は、センサデータがローカル条件と矛盾している場合を特定する。例えば、クライアント装置のGPS測定値が装置外であり、更に、温度、湿度又は気圧は、ローカル気象条件と一致しないことを示した場合、補足データ相関モジュール2140は、低い相関スコアを生成することができ、位置は、あまり信頼できないとみなすことができる。その結果、認証ポリシーモジュール1711は、トランザクションを承認するために、より厳密な認証技術1712（例えば、指紋、PIN入力など）を必要とする場合がある。

【0150】

他の例として、（補足位置データ2110を備える）主張された位置の既知の地理的又はネットワークトポロジに対して高度計圧力センサ2103によって提供される高度を比較することにより、補足データ相関モジュール2140は、主張された位置が本物でないことを知らせる不一致を特定することができる。例えば、ユーザが主張する位置の逆IP

10

20

30

40

50

検索がアンデス山脈にあるものとしてそれらを特定するが、装置からの高度計データは、装置が海面であることを示す場合、補足データ相関モジュール2140は、低い相関スコアを生成することができ、位置は、あまり信頼できないとみなすことができる。低い相関スコアの結果として、認証ポリシーモジュール1711は、トランザクションのための強力な認証によって高いリスクを軽減しようとすることができる。

【0151】

1つの実施形態において、補足データ相関モジュール2140は、ユーザがそれらの既知のユーザと同じ物理的位置で動作していない旨を示唆する異常を識別するために即時領域内の複数の他のエンドユーザに対してユーザの装置におけるセンサ1743から収集されたデータを比較する。例えば、認証されたユーザのセットが同じ物理的領域を操作している人を特定した場合、それらのユーザの装置の全ては、領域内の局所的な温度が10℃であり、補足データ相関モジュール2140は、その温度センサ2101がローカル温度が20℃であることを示すエンドユーザについて低い相関を生成することができることに留意されたい。その結果、認証ポリシー1711は、より厳密な認証技術1712を必要とすることがある。

【0152】

更に他の例として、補足データ相関モジュール2140は、特定のユーザの過去のデータに対して現在の測定値を比較することができる。例えば、上述したように、センサデータは、ユーザが装置1700を所有していることが知られている期間（例えば、明示的な認証に続く期間）中に分析することができる。そして、補足データ相関モジュール2140は、疑わしい動作を識別するためにローカルデータの不連続を探すことができる。例えば、ユーザの周囲温度が通常は10℃と20℃の間を浮動し且つそれは現在30℃である場合、これは、ユーザが典型的な位置にない示すことができ、それによって低い相関を生成して認証ポリシーモジュール1711にトランザクションの精査の追加レベルを要求させる。

【0153】

補足データ相関モジュール2140は、更に本発明の基本原則を順守しながら、センサデータと補足位置データとの間の様々な異なる種類の相関を実行することができる。例えば、2つのデータセット間の統計的関係を決定するために様々な公知の相関機構が使用されることができる。1つの実施形態において、認証ポリシーエンジン1711に提供される相関スコアは、相関のレベルを示す正規化値（例えば、0-1の間）を含む。1つの実施形態において、様々な閾値レベルは、センサ1743と補足位置データ2110との間において検出された差異のために設定されることができる。例えば、温度センサ2101が（他の装置又はインターネットから収集された）現在の温度から3度以上外れた温度を測定する場合、第1の閾値がトリガされることができる（相関スコアの低下をもたらす）。そして、現在の温度から3度外れた各追加の温度は、満たされた新たな閾値をもたらすことができる（対応する相関スコアの低下をもたらす）。しかしながら、これらは、本発明の1つの実施形態の単なる例示であることに留意すべきである。本発明の基本原則は、相関を行ういかなる特定の方法にも限定されない。

【0154】

本発明の1つの実施形態にかかる方法が図22に図示されている。2201において、（例えば、装置におけるGPSモジュールを介して）クライアント装置によって報告された現在位置が読み取られる。2202において、補足位置データは、クライアント装置からのセンサデータとともに報告された位置について収集される。上述したように、補足位置データは、（例えば、インターネット上の他のクライアント及び／又はサーバから）ローカル又はリモートの収集されることができ、報告された位置についての現在の温度、圧力及び／又は湿度などのデータを含むことができる。センサデータは、温度センサ、気圧又は高度計圧力センサ及び／又は湿度センサによって提供されることができる。

【0155】

2203において、装置のセンサによって提供される補足位置データとセンサデータと

の間で相関が行われる。1つの実施形態において、比較的高い相関は、2204において比較的高い相関スコアをもたらす一方で、低い相関は比較的低い相関スコアをもたらす。上述したように、1つの実施形態において、相関スコアは、センサの読み取り値と補足データとの類似度を示す正規化値（例えば、0-1の間）である。

【0156】

2205において、1つ以上の認証技術が（少なくとも部分的に）相関スコアに基づいて選択される。例えば、比較的低い相関スコアが提供される場合、より厳密な認証技術が選択されることができ、一方で、比較的高い相関が存在する場合、より少ない厳密な認証技術が選択されることができ（潜在的にエンドユーザによる明示的な認証を必要としないもの）。

【0157】

ユーザが2206において判定された選択された技術を使用して正常に認証した場合、トランザクションは、2207において進められるのを可能とする。そうでない場合、トランザクションは、2208においてブロックされる。

【0158】

多くの利点が上記実施形態で実現される。例えば、これらの実施形態は、他のソースからの位置データ収集のための追加の保証レベルを提供する：その位置が認証される追加の保証を得るために、組織が他のソース（IP、GPSなど）から収集された位置データを補足することを可能にする。更に、本発明の実施形態は、不正な位置からのトランザクションをブロックすることができ、ユーザが更に認証を試みることができる位置を制限することによって不正なアクセスを減らす。更に、これらの実施形態は、位置に特有のリスクに応答するためにより強力な認証を強制することができる（例えば、ユーザ／クライアントが不明又は予測されない位置からアクセスしているか又はその真実性の位置が複数の入力を使用して十分に適格化することができないときにより強力な認証を必要とする能力を保持しながら、信頼できる当事者は、ユーザが既知の位置からの情報にアクセスしているときに認証の不便を最小化することができる）。

F. クライアント認証機能に基づく認証ポリシーの適応的応用

【0159】

図23に示されるように、本発明の1つの実施形態は、組織—例えばセキュアトランザクションサービス1750を有する信頼できる当事者（以下、単に「信頼できる当事者」という）—が相互作用の特定のクラスに適している認証の種類を指定するのを可能とする適応的認証ポリシーエンジン2345を含む。図示されたように、適応的認証ポリシーエンジン2345は、信頼できる当事者1750において実行される認証エンジン2311内のモジュールとして実装することができる。この実施形態において、適応的認証ポリシーエンジン2345は、既存の認証装置2329についてのデータ、認証装置クラス2328、相互作用クラス2327及び認証ルール2326を含むポリシーデータベース2325に応じて実行する。

【0160】

1つの実施形態において、認証装置データ2329は、クライアント1700によって使用することが知られている明示的なユーザ認証装置1720-1721のそれぞれに関連するデータを含む。例えば、ポリシーデータベース2325は、センサが機密データ（例えば、暗号的にセキュアなハードウェアにおいて、EAL3証明書など）及び他人受入率（信頼できるセンサがユーザ認証結果を生成したときの方法を示す）を記憶する方法などのこのセンサに関連する技術詳細とともに「検証モデル123」指紋センサについてのエントリを含むことができる。

【0161】

1つの実施形態において、認証装置クラス2328は、それらの装置の機能に基づいて認証装置2329の論理グループを指定する。例えば、ある特定の認証装置クラス2328は、（1）指紋センサ、（2）EAL3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未満の他人受入率による

10

20

30

40

50

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。他の装置クラス 2 3 2 8 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) 2 0 0 0 分の 1 未満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や顔認識の実装は、適切な認証装置クラス 2 3 2 8 に追加される。

【0 1 6 2】

様々な個人属性は、認証要素（例えば、指紋、P I N、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 C P U 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（T E E）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）。

【0 1 6 3】

もちろん、これらは、単に認証装置クラス概念の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。

【0 1 6 4】

1 つの実施形態において、ポリシーデータベース 2 3 2 5 は、新たな認証装置 2 3 2 9 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 2 3 2 8 とともにそれらが市場に出るときに新たな認証装置 2 3 2 9 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。

【0 1 6 5】

1 つの実施形態において、相互作用クラス 2 3 2 7 は、信頼できる当事者 2 3 2 5 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、5 0 0 0 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、「中間値相互作用」は、\$ 5 0 0 から \$ 4 9 9 9 の量が関与するものとして定義することができ；「低価値トランザクション」は、\$ 4 9 9 以下の量が関与するものとして定義することができる。

【0 1 6 6】

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。

【0 1 6 7】

最後に、認証ルール 2 3 2 6 のセットは、認証装置 2 3 2 9、認証装置クラス 2 3 2 7

及び／又は相互作用クラス 2327 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 2327 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、EAL3 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 2328 として指定されたような）1000 分の 1 未満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。

10

【0168】

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 2328 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。

20

【0169】

更に、1 つの実施形態において、ルールは、特定の認証装置 2329 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」のみが許容可能であることを指定することができる。

【0170】

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。

30

【0171】

1 つの実施形態において、適応的認証ポリシーエンジン 2345 は、クライアント 1700 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 2327、認証装置クラス 2328 及び／又は認証機器データ 2329 をあてにする認証ルール 2326 を実装する。例えば、信頼できる当事者のウェブサイト又は他のオンラインサービス 2346 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 1700 のユーザに応じて、適応的認証ポリシーエンジン 2345 は、適用可能な 1 つ以上の相互作用クラス 2327 及び関連する認証ルール 2326 のセットを識別することができる。そして、（クライアントの認証エンジン 2310 内の構成要素として図 23 に図示された）クライアント装置 1700 における適応的認証ポリシーモジュール 2350 との通信を介してこれらのルールを適用することができる。そして、適応的認証ポリシーモジュール 2350 は、指定された認証ポリシーを順守するために 1 つ以上の認証技術 2312 のセットを識別することができる。例えば、認証技術の優先順位セットが信頼できる当事者の適応的認証ポリシーエンジン 2345 によって指定された場合、適応的認証ポリシーモジュール 2350 は、クライアント 1700 において利用可能な最も優先度の高い認証技術を選択することができる。

40

【0172】

認証技術 2312 の結果は、現在のユーザが正当ユーザであるという保証レベルを生成

50

する保証計算モジュール2340に提供される。1つの実施形態において、保証レベルが十分に高い場合、クライアントは、トランザクションを可能とする信頼できる当事者の認証エンジン2311に対して成功した認証の結果を通信する。

【0173】

1つの実施形態において、クライアント装置センサ1741-1743からのデータはまた、保証レベルを生成するために保証計算モジュール2340によって使用されることができる。例えば、位置センサ（例えば、GPS装置）は、クライアント装置1700の現在の位置を示すことができる。クライアント装置が予想される位置（例えば、家庭又は職場）にある場合、保証計算モジュール2340は、保証レベルを増加させるためにこの情報を使用することができる。これとは対照的に、クライアント装置1700が予想されない位置にある場合（例えば、ユーザが以前に訪れていない外国）、保証計算モジュール2340は、保証レベルを下げるためにこの情報を使用することができる（それによって、許容できる保証レベルに到達するためにより厳密な明示的なユーザ認証を必要とする）。上述したように、温度、湿度、加速度計データなどの様々な追加のセンサデータは、保証レベルの計算に組み込むことができる。

【0174】

図23に示されるシステムは、クライアント認証機能及び他の情報が信頼できる当事者に通信される特異性に基づいて異なって動作することができる。例えば、1つの実施形態において、明示的なユーザ認証装置1720-1721のそれぞれの特定のモデル及びクライアント装置1700におけるセキュリティハードウェア／ソフトウェア及びセンサ1741-1743の具体的な詳細は、信頼できる当事者1750に通信することができる。そのため、本実施形態において、適応的認証ポリシーエンジン2345は、現在のトランザクションとクライアントに関連するリスクのために実装された認証ルールに基づいて、認証の所望のモードを具体的に識別することができる。例えば、適応的認証ポリシーモジュール2345は、指定されたトランザクションのためにクライアントにインストールされた「検証モデル123」指紋センサを介して認証を要求することができる。

【0175】

他の実施形態において、クライアント装置1700の認証機能の唯一の一般的な記述は、ユーザのプライバシーを保護するために設けられてもよい。例えば、クライアント装置は、EAL3に認定された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指紋センサを有し及び／又はN分の1未満の他人受入率を有する生体照合処理を使用するように通信することができる。これらの装置の特定のモデルを開示することなく、他の認証装置の機能及び仕様に関連する同様の一般的な情報を指定することができる。そして、適応的認証ポリシーエンジン2345は、データベース2325内の該当する認証装置クラス2338に認証装置を分類するために、この一般的な情報を使用することができる。トランザクションを実行するための要求に応じて、適応的認証ポリシーモジュール2345は、そのクラスがトランザクションを完了するのに十分である場合には特定の認証装置を使用するようにクライアント装置1700に指示することができる。

【0176】

更に他の実施形態において、クライアント装置1700は、信頼できる当事者に対して認証機能に関連するいかなるデータも通信しない。むしろ、本実施形態において、適応的認証ポリシーモジュール2345は、必要な認証のレベルを通信し、クライアントにおける適応的認証ポリシーモジュール2350は、認証のレベルを満たす1つ以上の認証技術を選択する。例えば、適応的認証ポリシーモジュール2345は、認証装置の唯一の特定のクラスを使用することができる（相互作用クラス2327によって指定された）「高価値トランザクション」として現在のトランザクションが分類されていることを通信してもよい。上述したように、それはまた、優先順位付けの方法で認証クラスを通信することができる。この情報に基づいて、クライアントにおける適応的認証ポリシーモジュール2350は、現在のトランザクションのために必要な1つ以上の認証技術2312を選択することができる。

【0177】

図23に示されるように、クライアント装置1700は、各信頼できる当事者についてのポリシーデータを記憶／キャッシュするために独自のポリシーデータベース2390を含むことができる。ポリシーデータベース2390は、信頼できる当事者のポリシーデータベース2325内に記憶されたデータのサブセットを含むことができる。1つの実施形態において、ポリシーデータの異なるセットは、（各信頼できる当事者の異なる認証ポリシーを反映する）各信頼できる当事者のためのデータベース2390に記憶される。これらの実施形態において、（すなわち、様々なトランザクション種類に関連付けられたルールがローカルポリシーデータベース2390内で利用可能であるため）トランザクションの特定のカテゴリの単なる指示（例えば、「高価値トランザクション」、「低価値トランザクション」など）は、必要な認証技術2312を選択するために、クライアント装置1700における適応的認証ポリシーモジュール2350にとって十分な情報であってもよい。そのため、適応的認証ポリシーモジュール2345は、適応的認証ポリシーモジュール2350がその相互作用クラスに関連付けられたルールに基づいて認証技術2312を識別するために使用する現在のトランザクションの相互作用クラスを単に示すことができる。

10

【0178】

クライアント装置機能に基づいて適応的認証を行うための方法が図24に図示されている。本方法は、図23に示されたシステム上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るものではない。

20

【0179】

2401において、クライアントは、信頼できる当事者とのトランザクションを実行しようとする。例示として、限定されるものではないが、クライアントは、オンライン購入のための支払い情報を入力することができるか又は銀行口座間で資金を転送することを試みることができる。2402において、トランザクションが分類される。例えば、上述したように、トランザクションは、関与する金額又は関与する情報の機密性などの変数に基づいて特定の相互作用クラスに関連付けられてもよい。

【0180】

2403において、トランザクションのカテゴリに関連付けられた1つ以上のルールが識別される。上記例を参照すると、トランザクションが「高価値トランザクション」として分類される場合、このトランザクション種類に関連付けられたルールが選択されてもよい。2404において、トランザクション種類に関連付けられたルールが実行され、上述したように、情報は、トランザクションを完了するために認証要求を示すクライアントに送信される。上述したように、これは、特定の認証装置を識別し、認証装置のクラスを識別し又は（例えば、クライアントがルールのローカルコピーを保持する場合）実施される必要がある特定のルールを単に示すことを含んでもよい。

30

【0181】

いずれの場合においても、2405において、1つ以上の認証技術のセットは、ルール及びクライアントの認証機能を介して指定された要件に基づいて選択される。2406において認証が成功したと判定された場合、トランザクションは、2407において許可される。そうでない場合、トランザクションは、2408においてブロックされる（又は追加の認証がユーザから要求される）。

40

【0182】

本明細書に記載された本発明の実施形態から実現される多くの利点がある。例えば、これらの実施形態は、信頼できる当事者に認証機能を統合するのに必要な作業量を減らすことができる。例えば、認証ポリシーを体系化するためのコードを書く代わりに、ルールは、簡単なグラフィカルユーザインターフェースを介して設定されることができる。統合する必要がある全ての信頼できる当事者は、クラスの相互作用のポリシー（例えば：「多額送金（Large Money Transfers）」）を定義し、正しい認証機構を判定して活用するためにポリシーエンジンと相互作用するときに、そのポリシー識別子を使用する統合コード

50

を有する。

【0183】

更に、これらの実施形態は、認証ポリシーの管理を簡素化する。コードから認証ポリシーを発現することにより、このアプローチは、コードの変更を必要とせずに自己の認証ポリシーを組織が容易に更新するのを可能とする。規制委任の新たな解釈を反映するため又は既存の認証機構への攻撃に対応するための変更は、ポリシーの単純な変更となり且つ迅速に行うことができる。

【0184】

最後に、これらの実施形態は、認証技術の将来の改良を可能とする。新たな認証装置が利用可能になると、組織は、新たな又は生じたリスクに対処するためにその妥当性を評価することができる。新しく利用できる認証装置を統合するには、認証装置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、新しいコードを書き込む必要はない。

G. 認証時における眼追跡のためのシステム及び方法

【0185】

一般に、認証技術は、(a) 秘密情報が認証に使用される場合又は (b) 偽の入力を生成することが困難である場合、なりすましに対してロバストである。ほとんどのシステムは、今日、パスワードベースの認証をあてにしている。パスワードは、再現するのが容易であるため、セキュアに保持される必要がある。したがって、パスワード攻撃は、通常、ユーザのパスワードへのアクセスを得ることにフォーカスする。最近の攻撃は、パスワードが検証のために記憶されたサーバの脆弱性を実証している。

【0186】

パスワードベースの認証とは対照的に、認証のために生体認証を使用した場合、生体認証情報は、通常公開される。例えば、指紋は、ユーザによってタッチされた（ほとんど）全ての物体から取得することができる。同様に、ユーザの顔は、通常は隠されていないため、誰かに見られてキャプチャされることがあり、大抵の場合にはソーシャルネットワーク上で公開される。

【0187】

同じ生体認証特性を有する別人を「生成」することが困難であるため、現実の世界では、我々は、人を見るときに我々自身の認識能力をあてにすることができる。例えば、同じ顔及び癖を有する別人を「生成」することは困難である。これは、政府がパスポート、IDカード、運転免許証及び他の文書における顔の写真を含むためである。しかしながら、仮想世界において、我々は、システムを偽装するために同じ顔をしている別人を「生成」する必要はないが、顔の画像などのコンピュータが認識する何かのみを生成する必要がある。換言すれば、「モラルは、検証者が以下の2つのことを確認することができる場合にのみ生体認証が良好に動作するということである：1つ目は生体認証が検証時に人から到来するものであること、2つ目は生体認証がファイル上のマスタ生体認証と一致すること」「（本明細書の特許請求の範囲前に提供された参考文献のリストからの参考文献1を参照）。

【0188】

過去には、自動顔認識の研究は、静止画や動画を使用して顔の信頼性の認識にフォーカスしている。例えば、以下の参考文献2を参照のこと。いくつかの比較的ロバストな顔認識技術が存在しており、システムは今日市販されている（参考文献3を参照）。しかしながら、「生存性」検出、すなわち、「生体認証がファイル上のマスタ生体認証と一致する... 検証」にはあまり注意が払われない。いくつかの使用ケースにおいて、なりすまし保護は、必要とされていないか又は（例えば、法執行アプリケーションのために）更に人間によって行われている。

【0189】

一方ではノートブックやスマートフォンなどのコンピューティング装置におけるカメラの普遍性と他方では最も一般的な認証方法としてのパスワードの弱点は、一般に、生体認

10

20

30

40

50

証方法、特に顔認識の採用を促進する。認証方法としての顔認識の第1の大規模な「トライアル」は、GoogleのAndroid 4（別名、「アイスクリームサンドイッチ」）において行われ、静止画像認識に基づいていた。これらの技術は、写真によって容易にだまされることができる（参考文献4を参照）。Android 4.1（別名、「ジェリービーン」）における生存性検出のいくつかの並べ替えを含む改善された方法でさえも、カメラに対してコンピュータディスプレイ上で1つは開いた眼を有し且つ閉じた眼を有する電子的に変更されたものというシーケンス内の2枚の写真を提示することによって容易にだまされることができる（参考文献5を参照）。

【0190】

この弱点は、モバイル装置のリソースの制約によるものであると主張することができるが、それはまた、PCやアンチスプーフィング検出の研究であっても利用可能な市販のソフトウェアがまだ非常に成熟していないことを示している。本特許出願の譲受人は、この知見を確認するPCベースの顔認識ソフトウェアを使用してテストを実行した。

【0191】

Windows 7（登録商標）ベースのサムスンシリーズ5（登録商標）ノートブック上で動作する説得力のあるBioTrust 3.00.4063は、「高」に設定されたセキュリティ設定であっても生存性検査を全く実行しない。通常のコンピュータのモニタ上に表示される単純な顔画像は、システムを成功裏に偽装するのに十分であった。

【0192】

Macbook Air（登録商標）上で動作するKeyLemon 2.6.5は、生存性チェックとして単純な点滅テストを実行する。3つの画像のシーケンスを表示することによって、成功裏に偽装することができる：（1）顔の実画像（例えば、ウェブカムによって作成される）、（2）眼が閉じているかどうかを調べるために眼が再着色されている、実画像の修正、（3）再度の実画像。

【0193】

アンチスプーフィング検出は、異なるアルゴリズムを比較するときのNIST生体認証ベンダーテストなどの標準的なテストの一部ではない。例えば、参考文献6-8を参照のこと。2011年にいくつかの研究者によって組織された最初に知られている公開競技の1つは（参考文献9を参照）、いくつかのアルゴリズムの初期の成功を示したが、それは320×240ピクセルの解像度を持つビデオに基づいていた。典型的なコンピューティング装置は、少なくとも640×480ピクセルの前方に面したカメラの解像度を提供する。

【0194】

図25は、顔認識を行うための生体認証装置2500を有する例示的なクライアント2520を図示している。正常に動作させた場合、生体認証センサ2502（例えば、カメラ）は、ユーザから生の生体データを読み取り（例えば、ユーザの写真をスナップする）、特徴抽出モジュール2503は、生の生体データの指定された特性を抽出する（例えば、特定の顔特徴をフォーカスするなど）。照会モジュール2504は、クライアント2520におけるセキュア記憶装置に記憶された生体認証テンプレートデータ2510で抽出された特徴を比較し、抽出された特徴と生体認証テンプレートデータ2510との間の類似性に基づいてスコア及び／又ははい／いいえ応答を生成する。生体認証テンプレートデータ2510は、典型的には、ユーザが装置2500によって顔画像又は他の生体情報を登録する登録処理の結果である。そして、アプリケーション2505は、認証が成功したかどうかを判定するためにスコア又ははい／いいえ結果を使用することができる。

【0195】

（1）-（8）として図25において特定された、顔認識システムを偽装するために攻撃の複数の潜在的なポイントがある（参考文献10、11を参照）。（例えば、電子署名を用いて）生体認証テンプレート（6）の完全性を保証し且つ（例えば、（a）ホワイトボックス暗号化方法、（b）コード難読化及び（c）装置結合の組み合わせを適用することによって）特徴抽出部（3）、特徴ベクトル（4）、照会部（5）及びその最終結果（

10

20

30

40

50

8) の完全性を保護するための周知の保護機構がある。

【0196】

特徴抽出部(2)に対して古いキャプチャデータを再生することに対する保護機構は、(少なくとも理論的に)信頼できるコンピューティンググループのアプローチによって且つARM TrustZoneに対する潜在的な拡張によってカバーされる。基本的に、本アプローチは、センサに暗号化保護機構(例えば、HMAC又は電子署名)を追加し、現在のスマートカードチップに使用される保護機構に類似する改竄防止の方法でセンサをカプセル化することである。特徴抽出エンジンは、入力データの完全性を確認することができる。

【0197】

以下に記載される本発明の実施形態は、ユーザの「生存性」を確認するために眼追跡技術を利用するが、1つの実施形態において、これらの技術は、偽の生体認証を検出するための1つ以上の既存の技術と組み合わされる(参考文献1を参照)。これは、現在進行中の研究の分野である。既存の研究は、偽の生体認証についての保護アプローチの4つの異なるクラスを識別している(参考文献12を参照)：

1. データドリブン特性評価

a. 静止画像

i. 2次元フーリエスペクトルを分析する再スキャン画像によって解像度の低下を検出する(参考文献13)

ii. 画像プリントに対する実際の顔の異なる反射特性を利用する。この理論は、ランバート反射特性に基づいている(参考文献14)

iii. 印刷欠陥に起因する実際の顔と画像プリントの異なるマイクロテクスチャを利用する(参考文献15)

iv. 他の方法と組み合わせて印刷された画像における品質劣化やノイズ付加を利用する(参考文献16)

b. 映像

v. 各カメラセンサは、独自の特性を有し、モニタに表示された映像の再キャプチャは、アーチファクトを引き起こす。これは、なりすましを検出するために使用することができる(参考文献12)。

vi. 画像によるなりすましの場合、顔背景依存性がある(参考文献17)。

vii. なりすまし攻撃の場合、顔は、通常、より多くの剛体運動を示す(参考文献18)。

c. 静止画像及び動画像の組み合わせ(参考文献12)

2. ユーザ行動モデリング(参考文献12)

3. ユーザ相互作用のニーズ(参考文献12)。

4. 追加装置(参考文献12)

【0198】

単に既存のセンサ技術に基づく最も効果的な非侵襲型機構は、動き、テクスチャ及び生存性検出の組み合わせに基づいているように見える。参考文献9を参照のこと。

テクスチャの違い

【0199】

画像を印刷して再スキャンする影響を検出することができる。印刷して再スキャンすることによって画像の品質が向上しないことは直感的に明らかである。参考文献15の研究は、差異がマイクロテクスチャを分析することによってアルゴリズム的に検出されることができることを示している：「実際の顔と顔プリントとの差異をよく見ると、写真は平面剛体とみなすことができるのに対して、人の顔は複雑な非剛体3次元物体であるため、人の顔やプリントが様々な方法で光を反射することが明らかになる」。

【0200】

このアルゴリズムは、NUSA写真偽者データベースに含まれる画像に対してテストされている。性能は、最適化されていないC++コードを使用して3GBのRAMを有する

10

20

30

40

50

2.4 GHzのIntel Core 2 Duo CPUにおいて画像を処理するために、平均で16.5msであることが報告されている。

可視光の代わりの赤外線

【0201】

赤外スペクトルで画像又は映像を表示することは困難である。その結果、参考文献19において提案されている顔の熱パターンのキャプチャに基づく生存性検出は、可視光のパターンをキャプチャするよりもロバストである。残念ながら、赤外線センサは、高価であり、典型的なノートブック、タブレット又はスマートフォンに含まれていない。

オプティカルフローベースの方法

【0202】

実際の顔は、3次元物体である。顔は、典型的には、通常の会話において移動している。中央の顔部品、すなわち、カメラに対して短距離を有する部品の2次元動きは、カメラからの長距離を有する顔領域の2次元動きに比べて高いことが予想される（参考文献20、21、22）。この種の検出について、少なくとも3つの連続した画像のシーケンスが必要である。

【0203】

参考文献21の研究は、SART-2プロジェクト、モバイルワークステーションについての生体認証セキュリティシステムの一部である。

静止画像の代わりの動画像

【0204】

参考文献23において、点滅ベースの生存性の検出方法が記載されている。この方法は、単純な写真ベースのなりすまし攻撃に対してかなりロバストであるように見える。顔を認識することに加えて、本方法は、眼を配置し、眼を閉じると観測された画像シーケンスにおいて視認可能であるかどうかを検査する。Android 4.1の大規模試験からわかるように、この方法は、「フォトショップ」攻撃に対して明らかに非常にロバストではない。参考文献5を参照のこと。

【0205】

一般に、そのような動画ベースのシステムを偽装するために、攻撃者は、小さな画像シーケンスを生成しなければならない、センサにシーケンスを提示しなければならない。強力な画像エディタ、無料のビデオエディタ及びタブレットPCを有する世界において、これは比較的容易に達成される。

【0206】

そのような方法は、「公知の相互作用」として特徴付けられる。すなわち、攻撃者は、事前に必要な相互作用を知っており、照会画像シーケンスを準備することができる。

【0207】

参考文献23において、シーンと眼の瞬きのコンテキストが分析に含まれる。Intel Core 2 Duo 2.8GHz、2GBのRAMにおいて測定された性能は、ビデオフレームあたり約50ms（20FPS）である。

チャレンジレスポンス方法

生体認証のコンテキストにおいて、チャレンジ応答は、以下のように定義される：

【0208】

この方法は、個体から直接応答を誘発することによって人の存在を確認するために使用される。応答は、自発的又は非自発的であることができる。自発的な応答において、エンドユーザは、システムが提示するものに意識的に反応する。非自発的応答において、エンドユーザの身体は、自動的に刺激に応答する。チャレンジ応答は、攻撃からシステムを保護するために使用することができる。

(National Science & Technology Council's Subcommittee on Biometrics) (国立科学技術会議の生体認証小委員会)

マルチモーダルシステム

【0209】

10

20

30

40

50

なりすまし攻撃、ノイズの多いデータなどに対する生体認証方法のロバスト性を向上させるためにマルチモーダルシステムが提案されている。参考文献 25 を参照のこと。

【0210】

そのようなマルチモーダルシステムに対するシミュレートされたなりすまし攻撃の効果は、参考文献 26 において分析されている。主な結果は、全ての融合方式がなりすまし攻撃に対するロバスト性を向上させないということであり、いくつかの融合方式において、マルチモーダルシステムの全体を偽装するために単一の生体認証方法のみを偽装するのに十分であることを意味する。実際のなりすまし攻撃による既存の方式の分析は、同様の結果をもたらす。参考文献 27 を参照のこと。

【0211】

一般に、マルチモーダルシステムの3つの異なるクラスがある。

1) 成功裏に単一の形質を偽装するシステムは、システム全体を偽装するのに十分である。小さな FRR のためのマルチモーダルシステムの最適化は、通常、そのような結果をもたらす。

2) 以下のシステム：

a) 複数の形質が成功裏にシステム全体を偽装するために偽装されなければならない；及び、

b) このマルチモーダルシステム内の任意の1つの形質を偽装することは、単一のモーダルシステムにおいて同じ形質を偽装するよりも複雑ではない。

3) 以下のシステム：

a) 複数の形質が成功裏にシステム全体を偽装するために偽装されなければならない；及び、

b) このマルチモーダルシステム内のいずれかの形質を偽装することは、単一のモーダルシステムにおいて同じ形質を偽装するよりも複雑である。以下に記載される本発明の実施形態は、このカテゴリに入る。

【0212】

本発明の1つの実施形態は、ランダムに配置されて画面上に表示される関心領域を変化させることに対する応答を測定するために、認証処理の一部として眼追跡を行う。例えば、ランダムな画面レイアウト混合テキスト、空き領域、画像や映像クリップのシーケンスは、非侵襲者の眼球運動を誘導するためにユーザに提示することができる。同時に、眼追跡技術は、眼が予想される方法で画面レイアウトに反応していることを確認するために使用される。そして、この情報は、予想される顔がなおも存在することを確認するために顔認識技術と組み合わせることができる。更に、上述したように、眼追跡及び顔認識技術は、正当ユーザが装置を所有することを保証するのに十分なレベルに到達するために他の技術（例えば、位置ベースの認証、非侵襲型ユーザ存在検出、指紋スキャンなど）と組み合わせることができる。

【0213】

ウェブページや他のコンテンツの種類を読むことは、コンテンツに沿った眼の円滑なスイープをとまなうが、「凝視」と称される）一連の短い停止及び迅速な「衝動」はない。一連の凝視及び衝動の結果は、「スキャンパス (scanpath)」と称される。スキャンパスは、認知意図、関心及び特徴性を分析するのに有用である（「眼追跡」についての現在のウィキペディアの記事 en.wikipedia.org/wiki/Eye_tracking を参照）。「ヒートマップ」は、ウェブページや電子メールを表示する際に凝視された人々のグループの分野を示す集計表示である（Hartzell、「クレイジーエッグヒートマップは人々があなたのウェブサイトをクリックした位置を示す (Crazy Egg Heatmap Shows Where People Click on Your Website)」(2012年11月30日)、現在 www.michaelhartzell.com/Blog/bid/92970/Crazy-Egg-Heatmap-shows-where-people-click-on-your-website を参照）。

【0214】

図 2 6 A に図示されるように、本発明の 1 つの実施形態は、本明細書に記載された顔認識を実行するための顔認識モジュール 2 6 0 4 及び眼追跡動作を実行するための眼追跡モジュール 2 6 0 5 を含むクライアント装置 2 6 0 0 における認証エンジン 2 6 1 0 を備える。1 つの実施形態において、顔認識モジュール 2 6 0 4 及び眼追跡モジュール 2 6 0 5 は、それぞれの操作を実行する装置上でカメラ 2 6 0 2 によってキャプチャされたビデオ画像 2 6 0 3 のシーケンスを分析する。

【0 2 1 5】

その顔認識動作を実行するために、顔認識モジュール 2 6 0 4 は、セキュアな顔認識データベース 2 6 4 6 に記憶された顔認識テンプレートをあてにする。特に、上述したように、顔認識モジュール 2 6 0 4 内の照会ロジックは、顔認識データベース 2 6 4 6 に記憶された顔テンプレートデータとビデオ画像 2 6 0 3 から抽出された顔特徴を比較し、抽出された特徴と顔テンプレートデータとの類似度に基づいて「スコア」を生成する。上述したように、データベース 2 6 4 6 に記憶された顔テンプレートデータは、ユーザが装置 2 6 0 0 に顔画像又は他の生体データを登録する登録処理によって生成することができる。そして、顔認識モジュール 2 6 0 4 によって生成されたスコアは、正当ユーザが現在のトランザクションを開始しているという保証を表現する保証レベル 2 6 0 6 を形成するために、（例えば、以下に説明する眼追跡モジュール 2 6 0 5 などの）他の認証モジュールからのスコアと組み合わせることができる。1 つの実施形態において、各スコアは、特定のトランザクションについての十分な保証レベル 2 6 0 6 を生成するために特定の閾値に到達しなければならない。（閾値に到達したと仮定した）1 つの実施形態において、スコアは、他の数式を使用してともに加算又は組み合わせることができる（例えば、スコアは、重み付け、平均化、ともに加算又は任意の他の方法で組み合わせることができる）。

【0 2 1 6】

眼追跡分析を行うために、眼追跡モジュール 2 6 0 5 は、セキュアな眼追跡データベース 2 6 4 5 内に記憶された眼追跡テンプレートをあてにする。別個のデータベースとして図示されているが、眼追跡データベース及び顔認識データベースは、実際には同じセキュアなデータベースとすることができる。1 つの実施形態において、眼追跡テンプレートは、クライアント装置のディスプレイ 2 6 0 1 上でユーザに対して表示されることになるテキスト、グラフィックス、写真、ビデオ及び／又は空白領域（そのいくつかの例は、以下の図 2 8 A - B に示されている）並びに潜在的にコンテンツが表示される順序を指定する。更に、眼追跡テンプレートは、ユーザに表示されるコンテンツに応じてユーザの眼の予想される動作特性を特定するデータを含む（例えば、ヒートマップの形態で、以下参照）。眼追跡モジュール 2 6 0 5 内の照会ロジックは、予想される動きと実際の動きとの類似度に基づいて「スコア」に到達するために（ビデオ画像からキャプチャされた）実際の動きとユーザの眼の予想される運動を比較する。上述したように、スコアは、その後、保証レベル 2 6 0 6 を形成するために（例えば、顔認識モジュール 2 6 0 4 などの）他の認証モジュールからのスコアと組み合わせることができる。データベース 2 6 4 6 に記憶された眼追跡テンプレートデータは、それぞれ表示されたウェブページ又は他の表示された画像に応答して、他のユーザ及び／又は装置の実際のユーザの記録された眼の動きを使用してコンパイルすることができる。例えば、顔認識テンプレートと同様に、眼追跡テンプレートは、ユーザが装置 2 6 0 0 に彼／彼女の眼の動きを登録する登録処理の一部として生成することができる。

【0 2 1 7】

1 つの実施形態において、眼追跡モジュール 2 6 0 5 は、表示される画像（テキスト、グラフィックス、ビデオ、画像、及び／又は空白領域を含むことができる）とユーザの眼球運動との相関を判定する。例えば、動画がディスプレイの右下に表示されている場合、ユーザの大部分は、この領域に注目を向けるであろう。それゆえに、眼追跡モジュール 2 6 0 5 がユーザの眼が指定された期間（例えば、2 秒）内にこの領域に移動したことを検出した場合、それは、ユーザの眼とテンプレートとの高い相関を検出し、相対的に高いスコアをもたらす。これとは対照的に、ユーザの眼がこの領域に移動しない（又は全く移動

しない) 場合、眼追跡モジュール 2605 は、低い相関と対応する低いスコアを検出する。
【0218】

図 26A に示されるように、様々な他の明示的なユーザ認証装置 2620-2621 及びセンサ 2643 がクライアント装置 2600 上に構成されることができる。これらの認証装置及びセンサは、保証レベル 2606 を生成するとき (すなわち、本明細書に記載された眼追跡及び顔認識に加えて)、(必要に応じて) 認証エンジン 2610 によって使用される追加の認証データを提供することができる。例えば、センサは、クライアント装置 2600 の位置を判定するために位置センサ (例えば、GPS) を含むことができる。クライアント装置が予想位置にある場合には、認証エンジンは、保証レベル 2606 を増加させるためにこのデータを使用することができる。これに対して、クライアント装置が異常位置 (例えば、他の国) にある場合、これは、保証レベル 2606 に負に影響を与えることができる。このように、認証データは、非侵襲的に (すなわち、エンドユーザから明示的な入力なしに収集されたセンサデータを使用して) 生成することができる。

10

【0219】

更に、他の非侵襲型技術は、最後の明示的なユーザ認証から経過した時間を監視する認証エンジン 2610 を含む。例えば、ユーザが指紋又は他の生体認証装置 2620-2621 を使用して認証されたか又は最近 (例えば、10 分以内) パスワードを入力した場合、それは、保証レベル 2606 を増加させるためにこの情報を使用する。これに対して、ユーザが数日間明示的に認証されていない場合、それは、顔認識モジュール 2605 及び眼追跡モジュール 2605 によってより厳密な認証を必要とすることができる (例えば、それは、保証レベルを現在のトランザクションについて許容可能な値まで増加させるために通常よりもテンプレートデータとの高い相関を必要とすることができる)。

20

【0220】

1つの実施形態において、セキュア記憶装置 2625 は、信頼できる当事者 (例えば、クラウドサービス 2650 又は他の種類のネットワークサービス) とセキュア通信を確立するために、認証部のそれぞれに関連付けられ且つセキュア通信モジュール 2613 によって使用されるために設けられた認証鍵を記憶するセキュア記憶装置である。

【0221】

図 26B は、認証エンジン 2610 が、顔認識モジュール 2604 及び眼追跡モジュール 2605 に加えて (又はその代わりに) 音声認識モジュール 2660 及び唇運動分析モジュール 2670 を含む別の実施形態を図示している。1つの実施形態では、ユーザの音声は、マイクロフォン 2680 を介して捕捉され、アナログ音声信号は、アナログ-デジタル (A/D) 変換器 2681 を介してデジタル信号に変換される。音声認識モジュール 2660 は、デジタル音声信号を音声データベース 2665 内に記憶されたユーザの声紋と比較する。1つの実施形態では、声紋は、ユーザが特定の単語又はフレーズを話すように促されるトレーニング/登録プロセス中に生成される。発話された言語/フレーズから得られるデジタル化された音声信号を受信すると、音声認識モジュール 2660 は、ユーザの音声の特定の特性 (例えば、スペクトル特性、音標ベースの分類など) を捕捉し、音声データベース 2665 内に結果を記憶することによって声紋を生成する。音声認識モジュール 2660 は、声紋を生成し、捕捉された音声信号と声紋を比較する際に、これらに限定されるものではないが、周波数推定、隠れマルコフモデル、ガウス混合モデル、パターンマッチングアルゴリズム、ニューラルネットワーク、行列表現、ベクトル量子化、及び決定木に基づく技術を含む様々な音声認識技術を利用することができる。

30

40

【0222】

1つの実施形態では、ユーザは、クライアント装置のディスプレイ 2601 上に表示された単語及び/又はフレーズの特定のシーケンスを発話するように促される。これらは、音声認識モジュール 2660 が、声紋内に捕捉されたものと類似の音声特性を比較できるように、登録プロセス中に使用されるものと同じ単語/フレーズ又は同様の単語/フレーズとすることができる。

【0223】

50

その分析に応答して、音声認識モジュール 2660 は、捕捉された音声及び声紋が類似しているか又は非類似である程度を示す「スコア」又は他の値を生成する。そして、これらの結果は、認証エンジン 2610 によって使用されて、保証レベル 2606 を増減させる。例えば、正当ユーザが指示された単語／フレーズを発話した 97% の機会がある場合、保証レベル 2606 は、増大されることができる。対照的に、正当ユーザが単語／フレーズを発声していなかった 97% の機会が存在する場合、保証レベル 2606 は、減少されることができる。

【0224】

更に、1つの実施形態はまた、ユーザが単語／フレーズを発声する際にユーザの唇の動きの分析を実行する唇運動分析モジュール 2670 も含む。例えば、唇運動分析モジュール 2670 は、ユーザが単語／フレーズを発声しているときにユーザのビデオ画像 2603 を比較し、マイクロフォン 2680 を介して捕捉された音声ストリームが映像ストリームに一致する程度を判定することができる。ユーザの唇が、捕捉された音声ストリームと同期していない場合、これは、現在のユーザがシステムをなりすましていることを示すことができる（例えば、正当ユーザの音声の録音を再生する）。同期が存在するかどうかを判定するために、唇運動分析モジュール 2670 は、特定の音標及び音量レベルを特定の唇／口位置及び／又は移動と関連付けるようにトレーニングされることができる。例えば、ユーザの口が開いている（すなわち、唇が分離されている）期間は、ユーザの口が閉じているとき（唇が一体になる）よりも大きな音量をもたらすことが予想されるであろう。同様に、母音の音は、ユーザの唇が分離されている期間に聞こえ、ユーザの唇が一体になっている期間に子音が聞こえることが予想されるであろう。

【0225】

更に、1つの実施形態では、唇運動分析モジュール 2670 は、ビデオ画像 2603 内に捕捉された唇運動と、唇移動データベース 2675 内に記憶されたユーザの基準運動とを比較することができる。声紋と同様に、基準唇運動は、特定の単語／フレーズを話すユーザの画像が記録される登録プロセス中に捕捉されることができ、関連データは、データベース 2675 内で抽出及び記憶される。

【0226】

1つの実施形態では、スコア又は他の値は、ビデオ 2603 上で捕捉されたユーザの唇の動きと予想されるものとの間の相関を示すために、唇運動分析モジュール 2670 によって生成される。例えば、音声及び映像が同期しているように見える場合、唇運動分析モジュール 2670 は、音声及び映像が同期から外れて現れる場合よりも比較的高いスコアを生成することができる。同様に、唇運動分析モジュール 2670 は、ビデオ画像 2603 内で検出された唇運動が、唇運動データベース 2675 内に記憶された基準唇運動と高い相関を有する場合に、比較的高いスコアを生成することができる。

【0227】

1つの実施形態では、音声認識モジュール 2660、唇運動分析モジュール 2670、顔認識モジュール 2604 及び／又は眼追跡モジュール 2605 の分析は、正当ユーザがクライアント装置 2600 を所有している可能性を提供する保証レベル 2606 を生成するように組み合わせることができる。本発明の実施形態は、これらのモジュールのうちのいずれか 1つ、又はこれらのモジュールの任意の組み合わせで実装されて、保証レベル 2606 を生成することができる。そして、この保証レベル 2606 は、本明細書に記載される様々な他の認証技術と組み合わせで使用されることができる。

【0228】

図 26A からのいくつかの構成要素は、この実施形態の追加の特徴（例えば、センサ 2643、眼追跡データベース 2645、顔認識データベース 2646、明確なユーザ認証装置 2620-2621、セキュア記憶装置 2625 など）を不明瞭にすることを回避するために図 26B には示されていないが、これらの構成要素は、図 26B の実施形態に含まれるとみなされることができる。

【0229】

ウェブページ用に生成された例示的な「ヒートマップ」が図 27 に示されている。色コードは、ユーザがみながら自己の眼を固定したウェブページの領域を表す。赤色は（ユーザがより頻繁にこれらの領域を見る傾向があったことを意味する）最大の固定量を示し、（より少ない固定を示す）黄色、（更に少ない固定を示す）青色、そして（固定なし又は閾値未満の固定を示す）無色が続く。

【0230】

ウェブページを設計する際に、眼追跡及びヒートマップ分析がユーザビリティの分析の一部として実行される。研究（例えば、参考文献 29、30 を参照）は、ウェブユーザがページの折り目上の情報を見て時間の 80 % を費やすことが示されている。ユーザはスクロールしないが、彼らは折り目以下に注意の 20 % のみを割り当てる。ウェブユーザは、ページの左半分を見て時間の 69 % を費やすとともに右半分を見て 30 % を費やす。それゆえに、従来のレイアウトは、サイトが役立つ可能性が高くなる。

【0231】

モニタ上に表示される静止画像又は映像を提示するようななりすまし攻撃は、おそらく画面レイアウトに相関しないであろうスキャンパスとして眼追跡モジュール 205 によって検出することができる。様々な種類の眼追跡方法が利用可能である：高精度の特殊な装置及び標準のウェブカムを用いた方法に基づくソフトウェア（参考文献 33 を参照）。

【0232】

図 28 A は、クライアント装置のディスプレイ 2601 に表示されるテキスト 2805 及び画像及び／又は映像 2801 の例示的なグループ化を図示している。1つの実施形態において、グループ化は、ウェブページに統合される。しかしながら、本発明の基本原理は、ウェブベースの組織に限定されるものではない。グループ化はまた、スクリーンセーバーや他のアプリケーションの一部とすることができる。1つの実施形態において、テキスト 2805 及び画像／映像 2801 は同時に表示される。他の実施形態において、テキストは最初に表示され、画像／映像 2801 が続く。いずれの場合にも、予想は、ユーザの眼が（画像／映像 2801 が表示される）ディスプレイ 2601 の右下に向けられるというものである。

【0233】

図 28 B は、テキスト領域 2805 及び 3つの画像／映像要素 2800－2802 を含む他の例を図示している。1つの実施形態において、画像／映像要素 2800 は最初に表示され、画像／映像要素 2801 が続き、画像／映像要素 2802 が続く。そのような場合、ユーザの眼は、ディスプレイの左上角から右下、その後左下へと移動する必要がある。

【0234】

1つの実施形態において、特定の画像／映像要素 2800－2802 及び他のコンテンツ種類は、眼追跡モジュール 2605 によってランダムに選択され、それによって認証及びなりすま시를困難とする。更に、特定の位置は、異なる画像／映像要素 2800－2802 はランダムに選択される。そのような場合、眼球運動テンプレートは、コンテンツを表示するための特定の動作モードを指定することができるが、実際の位置の実際のコンテンツを指定しない。ユーザの眼が表示されるコンテンツに向けて引き寄せなければならないことを仮定する眼追跡モジュール 2605 によって選択され、これが検出された程度に基づいて相関及びスコアを生成する。

【0235】

更に、独自のコンテンツを生成するよりもむしろ、眼追跡モジュール 2605 は、信頼できる当事者 2650 の既存のウェブページ又は装置上でローカルに記憶されている画像などの既存のコンテンツを使用することができる。例えば、信頼できる当事者が金融機関であり、ユーザが金融トランザクションに入ろうとしている場合、トランザクション中に通常表示されるウェブページが表示されることができる。そのような場合、眼追跡モジュール 2605 は、眼追跡データベース 2645 から（図 27 に示されるような）ウェブページのヒートマップを取り出し、相関がヒートマップ及びエンドユーザによってみられる

位置に対して存在するかどうかを判定することができる。

【0236】

要約すると、本明細書に記載された実施形態は、テキスト、空き領域、画像及び映像クリップを混合したランダム画面レイアウトのシーケンスを提示し、キャプチャされたスキャンパスを生成するユーザの眼を継続的に追跡することができる。そして、相関がキャプチャされたスキャンパスと予想されるスキャンパスとの間で行われる。更に、本発明の1つの実施形態は、その後、顔が更に認識されていることを再確認することができる。

【0237】

全ての人々が平等に同じ画像又は画像シーケンスに惹かれるわけではない。例えば、一部の人々は、動物、テキスト、既知又は未知の人間の顔や身体、神秘的なシンボル又は数式であるよりも多くの技術に惹かれる。これを念頭において、眼追跡モジュール2605の1つの実施形態は、異なる種類の画像によって誘発される眼球運動の固有の特徴を人に学習させる。そして、ビデオ画像2603及び（眼追跡データベース2645に記憶されている）基準データから測定された特性の類似度が保証レベル2606を生成するために使用される（すなわち、正当ユーザの眼が「チャレンジ」画像、映像及びディスプレイ2601上に表示される他のコンテンツに続いているという確実性）。

【0238】

本発明の1つの実施形態にかかる方法が図29A-Bに図示されている。本方法は、図26Aに示されるものなどのシステムアーキテクチャ内に実装されることができ、任意の特定のシステムアーキテクチャに限定されるものではない。

【0239】

最初に図29Aを参照すると、2901において、特定の眼追跡テンプレートが、所与のユーザ及び／又はトランザクションのために選択される。2902において、テンプレートにしたがってコンテンツを表示している間に、ユーザの顔の画像のシーケンスが捕捉される。例えば、テンプレートは、コンテンツの種類、コンテンツの位置及びコンテンツを表示するタイミングを指定することができる。あるいは、テンプレートは、一般に、眼追跡の種類を指定することができ、眼追跡モジュール2605は、コンテンツを表示する方法、場所及び時間を決定することができる。

【0240】

コンテンツが選択されて表示される方法にかかわらず、2903において、顔認識が行われ、2904において、キャプチャされた画像のシーケンスを使用して眼追跡分析が行われる。2905において、キャプチャされた画像と顔のテンプレートとの相関に基づいて顔の保証レベルが生成される。同様に、2906において、眼追跡保証レベルは、ユーザの眼の動きとユーザの眼の予想される動きとの相関に基づいて生成される。

【0241】

図29Bは、図29Aの動作と並行して実行されることができ、音声認識動作及び唇運動相関動作のシーケンスを図示している。あるいは、図29A-Bの動作は、許容可能な保証レベルに到達するまで、任意の順序で順次実行されてもよい。

【0242】

2911において、クライアント装置を所有している現在のユーザの音声及び映像が捕捉されてデジタル化される。2912において、特定の声紋が音声データベース（例えば、登録プロセス中にユーザに対して以前に記録されたもの）から選択され、音声認識動作が実行される。2917において、現在のユーザの声と声紋との間の相関を示すスコア／保証レベルが生成される。2913において、デジタル化された音声と、現在のユーザについて捕捉された映像の唇運動との間の相関が判定され、2915において、同期レベルに基づいてスコア／保証レベルが生成される。2914において、映像内の捕捉された唇運動と、正当ユーザの登録プロセス中に収集された基準唇運動データとの間で相関が実行される。2916において、捕捉された唇運動が基準唇運動と一致する程度を示すスコア／保証レベルが生成される。2917、2915、及び／又は2916に続いて、得られたスコアを2905及び2906の結果と組み合わせて、2907において最終保証レベ

10

20

30

40

50

ルを生成する。上述したように、2907において組み合わせた結果が十分であると判定された場合、2909において、トランザクションが許可される。そうでない場合、2908において、追加の認証技術が必要とされることができる。

【0243】

並列処理2903／2905及び2904／2906として図29A－Bに示されているが、顔認識動作2903／2905が最初に行われてもよく、その後、顔認識動作が高い相関／保証レベルをもたらした場合（又はその逆）、眼追跡動作2904／2906が行われてもよい。同様に、音声認識動作2912及び唇運動動作2912／1913、2915／2916は、並行して又は順次（例えば、許容可能な保証レベルに到達するまで）行われてもよい。

10

【0244】

2907において、顔認証及び眼追跡を組み合わせた結果が現在のトランザクションが進行するのを可能とするのに十分であるかどうかに関して判定が行われる。そうである場合、トランザクションは2909において許可される。そうでない場合、2908において、トランザクションは、許可されないか又は追加の認証技術が保証のレベルを上げるために要求される。例えば、この段階において、ユーザは、指紋センサ上で指をスワイプするか又はユーザのアカウントに関連付けられたPINを入力するよう求められることができる。追加の認証技術が十分であると2910において判定された場合、トランザクションは、2909において許可される。

H. 認証時にリスク評価のためのクライアントデータを収集して利用するためのシステム及び方法

20

【0245】

認証部のいくつかの種類は非常に信頼でき、他はそうでない。それゆえに、信頼できる当事者が（例えば、上下にその保証を調整するために）リスク評価のために使用することができる認証部の読み取り値及びクライアントデータの特定の種類の有することができるという保証の範囲がある。例えば、リモート認証部がセキュア要素又は信頼できる実行環境（TEE）を有する場合、認証は証明鍵によってセキュアに署名することができる。証明鍵は、セキュア要素の内側にあり、任意の外部エンティティによってアクセスできない。実際の認証操作は、セキュア要素内で実行される。証明鍵の署名を使用して、信頼できる当事者は、リモート認証部が認証の試みの責を負うことを確実に知ることができる。

30

【0246】

リモート認証部がセキュア要素を欠いている場合、証明署名は、攻撃のためにドアを開くソフトウェアで行う必要がある。これを緩和する1つの方法は、ソフトウェアで保護された「ホワイトボックス」の証明鍵を記憶することである。証明鍵は、ホワイトボックスから出ることができず、認証試行において署名を実行することができない。しかしながら、認証を行っているコードや証明署名を行っているホワイトボックスが切り離されている（及びホワイトボックスがソフトウェアベースである）ことから、これは、セキュア要素又は信頼できる実行環境（TEE）を使用するよりも信頼できる。

【0247】

最後に、上記の全てを欠いて、全体の認証動作は、ソフトウェアで完全に行うことができる。認証コード及び証明鍵自体が双方とも損なわれることがあるため、これは最もセキュアでない。

40

【0248】

上記の例のいずれにおいても、認証実行時（例えば、以下に説明するように保証レベルを生成する際）にクライアントリスクが評価されることができるよう認証が行われる特定の方法を決定するために信頼できる当事者がクライアントデータを収集することができた場合には有益であろう。

【0249】

追加のデータを介してリスク評価を改善することにより、本発明の1つの実施形態は、クライアントデータを収集して各クライアントに関連するリスクを評価することによって

50

不正なトランザクションを回避する。クライアントに関連付けられたリスクのレベルは、特定のトランザクションについてユーザを認証するために使用されなければならない認証技術を指定するために使用することができる。リスクを評価するために、本発明の1つの実施形態は、(1) リスク計算に有用なデータの種類の、(2) ウェブブラウザがセキュアに提供することができない追加データを取得する方法、及び(3) ユーザのプライバシーを侵害しない方法でそれを行う方法を判定する。

【0250】

ウィルス、ワーム及びマルウェアがコンピュータに感染する最大の理由の1つは、オペレーティングシステムが潜在的な脆弱性を閉じるように最近更新されていないためである。オペレーティングシステムにおけるこれらの脆弱性は、公衆に知られると、犯罪者によって悪用されることが非常に容易である。より長くシステムが更新せずに行ってしまうほど、潜在的な脆弱性が悪用するために存在することが多くなり、パスワードが悪意のあるコードによって損なわれる可能性があるリスクが大きくなる。ウェブブラウザは、ウェブサイトがユーザのコンピュータの更新履歴にアクセスするのを可能としない。それが行った場合、ウェブサイトは、システム上にあることが知られている脆弱性に基づいて潜在的な被害者を識別することができる。したがって、本発明の1つの実施形態は、(ブラウザプラグインよりもむしろ)現在のオペレーティングシステムのバージョンを判定するためにクライアントデータ及び／又は最近オペレーティングシステム更新された方法を収集するネイティブアプリケーションとして実行されるセキュアエージェントとして動作する。

【0251】

悪意のあるコードに対する1つの防衛は、ユーザのコンピュータに感染した後は、ウィルス対策ソフトウェア(例えば、Windows(登録商標)のDefender(登録商標))である。悪意のあるコードが既にシステムに侵襲しているにもかかわらず、ウィルス対策ソフトウェアは、少なくとも悪いことが発生したことをユーザに警告し、それによって与えられた最終的な損傷を制限する。ユーザは、アカウントのパスワードを変更し、最近のトランザクションを検証することができる。しかしながら、何のウィルス対策ソフトウェアもインストールされていないか又はウィルス対策ソフトウェアはインストールされているが最近実行されていない場合には、悪意のあるコードがコンピュータ上に存在することをユーザが認識していないことが高い可能性がある。そのコンピュータ上で発生したトランザクションは、詐欺のリスクが高いであろう。ウェブブラウザは、ウィルス対策ソフトウェアがコンピュータにインストールされているかどうかを明らかにしない。それゆえに、1つの実施形態において、ネイティブエージェントアプリケーションは、ウィルス対策ソフトウェアがインストールされているかどうか、そうである場合には最近はどのように更新及び／又は実行されているかを判定するためにクライアント設定データを配置して収集する。

【0252】

特にワームに対する他の防衛は、ファイアウォールである。ソフトウェアファイアウォールがインストールされてユーザの機器上で有効になっている場合、攻撃のエントリポイントの数は大幅に削減される。通常はランダムインターネットホストから有線を介して到来する任意の要求にサービスを提供するオープンポートは去勢される。それゆえに、ポートを聞いているサービスがパッチ適用されていないセキュリティホールを有していても、通信がそれにアクセスするのを許可されていないことからリスクが排除される。一方、ソフトウェアファイアウォールなしで実行しているコンピュータは、特にそれが最近更新されていない場合には、ワームに感染するはるかに大きな可能性を有する。ウェブブラウザは、ポートスキャンを介して、限られた成功によって間接的にファイアウォールを検出することができる。したがって、1つの実施形態において、ネイティブエージェントアプリケーションは、ファイアウォールがインストールされているかどうか、そうである場合には最近はどのように更新されたかを判定するために、ファイアウォール設定データを配置して収集する。

【0253】

ユーザのコンピュータが物理的に盗まれた場合、かなりの情報量が犯罪者によって収集され、不正行為を犯すために使用されることができる。ユーザの機器がパスワードで保護され、好ましくはハードドライブ全体がそのパスワードで暗号化されている場合には、盗難のためにリークされた情報のリスクが軽減される。そうでない場合、より高いレベルのリスクが評価されることができる。それゆえに、1つの実施形態において、ネイティブエージェントアプリケーションは、ハードドライブの内容が暗号化されたかどうかを判定し、クライアントのリスク評価の一部としてこの情報を使用する。

【0254】

更に、上述したように、クライアントが認証を実行するためにセキュア要素又は信頼できる実行環境（TEE）を使用している場合、信頼できる当事者は、クライアントによって提供された認証が正当なものであるという高い保証を有することができる。リモート認証部がセキュア要素を欠いている場合には、ソフトウェア保護「ホワイトボックス」は、認証データ（例えば、証明鍵）を保護するために使用することができる。しかしながら、上述したように、認証を行っているコード及び認証署名を行っているホワイトボックスが切り離されている（及びホワイトボックスがソフトウェアベースである）ことから、これは、セキュア要素又は信頼できる実行環境（TEE）を使用するよりも信頼できる。最後に、上記の全てを欠いて、全体の認証動作（上述したように最もセキュアな方法でない）は、ソフトウェアで完全に行うことができる。本発明の1つの実施形態は、認証を行う際にクライアントのリスクが評価されることができるように、認証が行われている特定の方法を判定するために信頼できる当事者が上記クライアントデータを収集するのを可能とする。

【0255】

図30に示されるように、本発明の1つの実施形態において、クライアント装置3000は、1つの実施形態において、様々な種類のクライアント設定データ3050を収集し、応答的にクライアント3000のリスクレベルを計算するクライアントリスク評価エージェント3004を含む。1つの実施形態において、クライアントリスク評価エージェント3004は、クライアント3000のネイティブオペレーティングシステム（OS）3010内で直接実行するように設計されたネイティブコードエージェントアプリケーションである。したがって、クライアントリスク評価エージェント3004は、セキュリティ上の理由からクライアントデータにアクセスする能力が制限されているブラウザプラグインや他の種類のプログラムコードに関連する制限を受けない。換言すれば、クライアントリスク評価エージェント3004は、ブラウザコンテキストにおいて実行されているHTML及びJavaScriptコードがアクセスを許可されないデータを収集するように許可される。それゆえに、認証エンジン3010がブラウザコンテキスト内で実装されることができるにもかかわらず、それは、クライアントリスク評価エージェント3004によって提供される追加リスク分析に対するアクセスを有する（認証エンジン3010は、更に本発明の基本原則を順守しながらブラウザコンテキスト内に実装される必要がないことに留意すべきである）。

【0256】

1つの実施形態において、認証エンジン3010は、正当ユーザがクライアント装置3000を所有している可能性に対応する保証レベルを計算するための保証レベル計算モジュール3006を含む。そして、ネットワークを介したリモートの信頼できる当事者3051との保留トランザクション（例えば、金融トランザクション、オンライン購入、ユーザのアカウントにおける機密情報へのアクセスなど）が完了したかどうかを判定するために、この保証レベルを使用することができる。1つの実施形態において、信頼できる当事者3051は、所定のトランザクションに必要な保証レベルを指定することができる。例えば、かなりの金額の転送をともなう金融トランザクションについて、信頼できる当事者3051は、例えば、ユーザの電子メールアカウントへのアクセスをともなうトランザクションより比較的高い保証レベルを必要とすることがある。単一のエンティティとして図

示されているが、「信頼できる当事者」は、本明細書に記載された基本認証技術を実行するための独立したセキュアトランザクションサーバを備えたウェブサイト又は他のオンラインサービスを含むことができる。

【0257】

1つの実施形態において、保証レベル計算モジュール3006は、クライアントリスク評価エージェント3004によって収集されたユーザの機密情報を開示することなく、信頼できる当事者3051に対して（例えば、値、比率、コードなどとして指定された）保証レベルを送信し、それによってユーザのプライバシーを保護する。他の実施形態において、保証レベル計算モジュール3006は、現在のトランザクションに必要な保証レベルを知っており、保証レベルが十分に高いかどうかを判定し、再度信頼できる当事者3051に対してユーザの個人情報を開示することなく、トランザクションが信頼できる当事者3051に対して許可又は拒否されるかどうかの指示を送信する。

10

【0258】

1つの実施形態において、クライアント装置3000と信頼できる当事者3051との間の通信は、第1の鍵を使用して外向きの通信を暗号化し且つ第2の鍵を使用して到来通信を復号することができるセキュア通信モジュール3013を介してセキュアにされる。対称鍵暗号化方式において、第1及び第2の鍵は同じである。非対称鍵暗号化方式において、鍵は異なる。しかしながら、本発明の基本原理は、暗号化の任意の特定の種類に限定されるものではない。

【0259】

1つの実施形態において、保証レベル計算モジュール3006は、クライアントリスク評価エージェント3004によって提供されるリスクデータに加えて現在のユーザ認証結果3005に基づいて保証レベルを決定する。特に、ユーザ認証結果3005は、1つ以上の明示的なユーザ認証装置3020-3021を介して現在又は最近の明示的なユーザ認証の結果を含むことができる。これは、例えば、指紋認証装置を介した指紋認証、カメラ及び顔認識ハードウェア／ソフトウェアを介した顔認識認証、マイク及び音声認識ハードウェア／ソフトウェアを介した音声認識、カメラ及び関連するハードウェア／ソフトウェアを使用した網膜スキャン、キーパッドを介したエンドユーザによるパスワード／PIN入力、及び／又は、様々な他の種類の明示的なユーザ認証装置及び／又は技術を含むことができる。

20

【0260】

1つの実施形態において、セキュア記憶装置3025は、各ユーザ認証装置3020-3021についての生体認証基準データレコードを暗号的に保護する（例えば、記憶装置3025をセキュアにするために対称鍵を使用してデータをラッピング）。セキュア記憶装置3025は、認証装置3020-3021のセキュアな周囲の外側に図示されているが、1つの実施形態において、各認証装置3020-3021は、生体認証基準データレコードを暗号的に保護するために、独自の統合されたセキュア記憶装置を有してもよい。

30

【0261】

明示的なユーザ認証に加えて、認証エンジン3010の1つの実施形態は、保証レベルを生成するために保証計算モジュール3006によって使用されるようにセンサ3043からデータを収集する。例示として、センサ3043は、ユーザの現在位置を示すためにGPSセンサなどの位置センサを含むことができる。クライアント装置3000がユーザの仕事又は自宅などの予想位置にある場合、これは、ユーザが正当ユーザである可能性を増加させる。これとは対照的に、ユーザが以前に訪問していない外国などの予想位置にある場合、これは、ユーザが正当ユーザでない可能性を増加させる。それゆえに、1つの実施形態において、保証計算モジュール3006は、ユーザが予想位置にある場合には保証レベルを増加させ、ユーザが予想されない位置にある場合には保証レベルを減少させる傾向がある。

40

【0262】

温度センサ、湿度センサ及び加速度計などの様々な追加センサ3043は、ユーザ認証

50

に関連するデータを収集するために使用することができる。例えば、温度／湿度センサは、位置センサによって指定された位置についての既知の温度／湿度と比較することができる現在の温度／湿度を提供することができる。値が大きく異なっている場合、これは、クライアント装置 3000 が偽装されていることを示すことができる。主張された位置及び温度／湿度の比較は、図 46A-B に関して以下に説明されるセキュアトランザクションサーバ 4632 などのリモートサーバにおいて行うことができる。他の実施形態において、装置における加速度計は、ユーザの歩行を測定し、ユーザの既知の歩行に対してこれらの測定値を比較するために使用することができる。歩行が一致する場合（指定された閾値内）、これは、正当ユーザがクライアント装置 3000 を所有している可能性を増加させる。

10

【0263】

図 31 に示されるように、リスクの判定に関連する各種のクライアント設定データは、例えば、ハードウェアデータ 3101、オペレーティングシステムデータ 3102 及びアプリケーションデータ 3103 を含んで収集されて使用されることができる。例示として、限定されるものではないが、ハードウェアデータ 3101 は、クライアント装置モデル、プロセッサ名／種類、ブート ROM バージョン及び管理コントローラバージョンを含むことができる。オペレーティングシステムデータ 3102 は、現在のオペレーティングシステムバージョン、OS が更新された日付及び現在のブートモード（例えば、ハードドライブからの起動）を含むことができる。アプリケーションデータ 3103 は、ファイアウォールがアクティブであるかどうかについての指示、ファイアウォールの種類及びバージョン、ウィルス対策ソフトウェアが現在のバージョン及びウィルス定義ファイルに対するアップデートとともにインストールされているかどうかについての指示、ウィルス対策ソフトウェアがアクティブである（例えば、実行時にクライアント装置をアクティブに監視する）かどうかについての指示、最後の完全な及び／又は部分的なウィルススキャンの指示、並びに、最近のウィルススキャンの結果を含むことができる。更に、アプリケーションデータ 3103 又は OS データ 3102 は、暗号化された又はセキュアな方法でデータがユーザの持続的な記憶装置（例えば、ハードドライブ、フラッシュメモリなど）に記憶されているかどうかについての指示を含むことができる。

20

【0264】

上述したように、1つの実施形態において、保証レベル計算モジュール 3006 は、正当ユーザが現在のトランザクションを試みているという保証レベルに到達するためにクライアントリスク評価エージェント 3004 によって提供されるリスク評価データ及びユーザ認証結果 3005 の双方を分解する。例示として、限定されるものではないが、現在のクライアントがアクティブファイアウォール又はウィルス検出ソフトウェアを有していないことをクライアント設定データ 3050 が示す場合、それは、クライアントが有効なこれらの特徴を有するクライアントよりも高いリスクを表すことを保証計算モジュール 3006 に報告することができる。同様に、ウィルス検出ソフトウェアが（例えば、閾値時間内に）最近更新又は実行されていない場合、クライアントリスク評価エージェント 3004 は、保証レベル計算モジュール 3006 に対して高くなったリスクを報告することができる。リスクレベルは、更に本発明の基本原則を順守しながら様々な方法で指定することができる。例えば、リスクレベルは、比率（例えば、0%＝最小リスク、100%＝最大リスク、及び、異なるレベルの中間リスクを表す中間の全ての数）又はスケール上の数値（例えば、1＝最小リスク、10＝最大リスク、及び、異なるレベルの中間リスクを表す中間の全ての数）に基づくことができる。

30

40

【0265】

リスクデータが設けられる方法にかかわらず、1つの実施形態において、保証レベル計算モジュール 3006 は、クライアントリスク評価エージェント 3004 によって提供されるリスクデータに基づいて必要な認証のレベルを判定する。例えば、クライアントリスク評価が相対的に高いリスク値（例えば、10のうちの9又は10）を示す場合、保証レベル計算モジュール 3006 は、現在のトランザクションについてユーザを認証するため

50

に P I N / パスワードの入力及び / 又は指紋スキャンなどのより信頼性がある及び / 又は明示的なユーザ認証を必要とすることができる。これとは対照的に、クライアントリスク評価が比較的低いリスク（例えば、10のうちの1又は2）を示す場合、保証レベル計算モジュール3006は、位置ベースの認証及び / 又は現在のトランザクションについての最近の明示的なユーザ認証への依存などの非侵襲型ユーザ認証を必要とすることができる。【0266】

図31におけるデータが簡略化のために表形式で配置されていることに留意すべきである。実際のクライアント設定データ150は、例を挙げると、バイナリファイル、階層型ファイルシステム構造、リンクリスト及びOSレジストリ形式を含む様々な異なる形式で記憶することができる。本発明の基本原理は、任意の特定の設定データの形式に限定されるものではない。

【0267】

図30に示されるように、1つの実施形態において、クライアントリスク評価エージェント3004は、（例えば、OSによって露出されるアプリケーションプログラミングインターフェース（API）に対して適切な呼び出しを行うことにより）OSを介してクライアント設定データ3050へのアクセスを備える。他の実施形態において、クライアントリスク評価エージェント3004は、データが記憶されている基本ファイルシステムから直接クライアント設定データ3050にアクセスする。1つの実施形態において、クライアントリスク評価エージェント3004は、基本設定データへのセキュアなアクセスを備える。信頼技術チェーン及びセキュアエンクレープなどの設定データ3050のセキュリティを保証するために様々なセキュリティ機能が実装されてもよい。

【0268】

追加的なリスク情報がウェブサイトを提供されるのを可能とする1つの考慮事項は、ブラウザが最初の位置でこの情報を提供していない理由のために合理性が無視されていないことである。確かに、悪意あるウェブサイトは、この情報を十分に使用することができ、ウェブブラウザの開発者は、届かないところにこの情報を残すための十分な理由を有する。それゆえに、上述したように、1つの実施形態において、基本クライアント設定データ3050は、信頼できる当事者3051に直接提供されない。むしろ、1つの実施形態において、クライアントリスクデータは、クライアントリスク評価エージェント3004によってクライアント装置上で直接評価され、リスク値は、保証レベルの計算に提供される。全ての信頼できる当事者3051は、（保証レベルが事前に指定されている場合）認証が成功したかどうか及び / 又は現在の保証レベルを知る必要がある。このようにして、クライアント設定データ3050は、本開示から保護される。

【0269】

認証時にクライアントのリスクを評価するための方法の1つの実施形態が図32に示されている。本方法は、図30-31に示されるアーキテクチャ上で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るものではない。

【0270】

3201において、クライアントのリスクに関連するクライアント設定データが取得される。これは、例えば、ファイアウォール又はウィルス検出ソフトウェアの存在及び現在の状態及び / 又はオペレーティングシステムの現在のバージョン（例えば、OSが最近更新された）を含むことができる。3202において、クライアント設定データは、クライアントのリスク値を判定するために評価される（例えば、リスクレベルを特定可能な比率、数値又はその他のデータ）。3203において、クライアントリスク評価を使用して、保証レベルが判定される。1つの実施形態において、高いリスク値は、より高い保証レベルを必要とする（例えば、10のリスク値は90%超の保証レベルを必要とすることができる）。他の実施形態において、評価されたリスクに基づいて保証レベル自体が計算される。例えば、上述したように、リスク値は、（前の又は現在のユーザ認証を含む）現在の保証レベルを判定するために多くの変数の1つとして含まれることができる。

【0271】

3204において、成功裏に完了した場合、現在のトランザクションについての許容レベルまで保証レベルを上げるように認証技術が選択される。例えば、リスクが高い場合、明示的なユーザ認証を必要とすることができる。リスクが低い場合、前の最近の認証又は非侵襲型認証で十分である。

【0272】

3205において、認証が成功したかどうかについての判定が行われる。そうである場合、トランザクションは、3208において許可される。そうでない場合、3206において、1つ以上の追加の認証技術が必要とされることができ、又はトランザクションが許可されることができ。例えば、現在の保証レベルが不十分である場合、ユーザは、信頼できる当事者3051に対して以前に提供された秘密情報を入力するように要求してもよく、又は、他の／追加の認証を提供してもよい。3207において追加の認証技術が十分であると判定された場合、トランザクションは、3208において許可される。そうでない場合、トランザクションは、3206において禁止される。

I. ローカルトランザクションの認証を行うためのシステム及び方法

【0273】

本明細書に記載された本発明の実施形態は、ローカルセキュアトランザクション装置を介してローカルトランザクションを開始するためにユーザを認証するための技術を含む。例示として、ローカルトランザクションは、引き出し、転送又は他のユーザの開始操作とすることができ、セキュアトランザクション装置は、金融トランザクションを実行することができるATM又は他のローカル装置とすることができる。同様に、ローカルトランザクションは、ローカルセキュアトランザクション装置を備えた小売店や他の小売位置において商品やサービスを購入するために支払いを完了したことを含むことができる。

【0274】

図33に示されるように、1つの実施形態において、生体認証装置及び関連するソフトウェアを有するクライアント装置3300は、ローカルセキュアトランザクション装置3350上でトランザクションを実行するためにセキュアトランザクションサービス3351によって信頼できる当事者に対してネットワークを介して認証する。特に、クライアント装置3300のユーザがセキュアトランザクション装置3350を使用してローカルにトランザクションを実行することを望む場合、それは、信頼できる当事者3351との一連の認証トランザクションを開始する（その例は、以下に説明される）。例えば、ユーザは、クライアント装置3300における指紋センサ上で指をスワイプするか及び／又はクライアントのキーパッドを介してPIN若しくは他の秘密コードを入力することを必要とされることができ。そして、認証の結果は、ユーザのプライベートデータ（例えば、指紋データ、PIN、又は、任意の他のプライベートユーザデータ）を送信することなく、クライアント装置3300から信頼できる当事者3351に対して送信されることができ、それによってユーザのプライバシーを保護する。

【0275】

認証の成功に応答して、信頼できる当事者3351は、操作を実行するためにローカルセキュアトランザクション装置3350に信号を送信することができる。例えば、ローカルセキュアトランザクション装置がATMである場合、信号は、指定された現金額を分配するようにATMを指示することができる。ローカルセキュアトランザクション装置3350が小売チェックアウト装置の場合、成功した支払いの指示が送信されることができ、ユーザのアカウントが引き落とされることができ。

【0276】

更に、図33に示されるように、ユーザ認証処理を補足するために、クライアント装置3300とローカルセキュアトランザクション装置3350との間にローカルセキュア通信チャンネルが確立されることができ。ローカルセキュアチャンネルは、例を挙げると、近距離無線通信(NFC)、ブルートゥース又はWi-Fi（例えば、802.11xチャンネル）などの様々な無線通信技術を利用してクライアント装置3300及びローカルセキュアトランザクション装置3350上の無線通信インターフェースを使用して確立さ

10

20

30

40

50

ることができる。例えば、位置セキュアトランザクション装置 3350 の近傍における場合、クライアント装置 3300 は、認証中にデータを交換するために、ローカルセキュアトランザクション装置 3350 の無線インターフェースとの無線インターフェースを介して近距離無線通信（NFC）ハンドシェイクを実行し、ローカルセキュアチャンネルを確立することができる。

【0277】

クライアント装置 3300 の現在位置を確立することから、ローカルセキュアチャンネルの単なる存在は認証データを含む。したがって、この情報は、認証処理中のクライアント装置 3300 の現在位置の証明として信頼できる当事者 3351 によって使用されることができる。1つの実施形態において、信頼できる当事者 3351 は、2つの位置の値が一致していることを確認するためにクライアント装置 3300 によって報告された現在の GPS 位置を使用してローカルセキュアトランザクション装置 3350 によって提供される位置を比較することができる。

【0278】

更に、信頼できる当事者 3351 は、クライアント装置 3300 に対して秘密コード又は他の認証データを送信することができ、そして、クライアント装置 3300 は、クライアント装置を認証するために、セキュアローカルチャンネルを介してローカルセキュアトランザクション装置 3350 に中継することができる。例えば、1つの実施形態において、信頼できる当事者 3351 は、クライアント装置 3300 に対してバーコードを、ローカルセキュアトランザクション装置 3350 に対して対応するコードを送信する。ローカルセキュアトランザクション装置 3350 は、その後、認証を実行するためにバーコードスキャナ又はカメラを使用して（例えば、クライアント装置 3300 のディスプレイから）バーコードを読み取ることができる（すなわち、バーコードから読み取ったコードと信頼できる当事者から受信したコードを比較する）。あるいは、ローカルセキュアトランザクション装置 3350 は、その後にコードが一致することを確認する信頼できる当事者に対してバーコードから読み取ったコードを送信することができる。逆に、信頼できる当事者 3351 は、認証のためにその後にクライアント装置 3300 にデータを中継するローカルセキュアトランザクション装置 3350 に対して秘密のコード又は他の認証データを送信することができる。それゆえに、ローカルセキュアチャンネルは、様々な認証技術のデータを交換するために使用することができる。

【0279】

上述したように、1つの特定の実施形態において、ローカルセキュアトランザクション装置 3350 は A T M 装置である。A T M 機器は、それらの入力／出力制御（例えば、カードリーダー、キーボード、スクリーン、カメラなど）が「外界」のために露出され、それらが改竄のために容易に利用可能であることから、脆弱な装置である。例えば、デビットカードの記録及びピンは、隠された磁気ストライプリーダー、鏡及びビデオカメラなどのローテク装置によって容易に盗まれることがある。1つの実施形態において、クライアント 3300 と信頼できる当事者 3351 との間の通信をともなうリモート認証技術は、A T M 機器について的大幅に改善した認証を提供するために使用される。このリモート認証と統合すると、A T M 自体は、カードリーダー、タッチスクリーン又はキーボードなどのレガシー入力／出力制御を有する必要はない。それが必要とする全ては、ネットワーク接続及び現金を分配するためのスロットである。それ自体の認証は、生体認証装置を備えた顧客のクライアント装置 3300 上で実行されることができる。

【0280】

1つの実施形態において、現金の引き出しのために、ユーザは、信頼できる当事者 3351 に対して認証するために A T M 機器の周辺を入力してリモート認証アプリケーションを開始する。そして、ユーザは、引き出しのための金額を入力し、モバイル装置における指紋センサを使用して指をスワイプ（又は以下に説明するような任意の他の種類のユーザ認証）する。ユーザの存在及び認証が信頼できる当事者 3351 によって確認された場合、指定された金額が A T M のスロットから分配される。

【0281】

この実施形態は、より強力な認証を提供するだけでなく、それはまた、複雑で高価なATMを、構築して維持するのに大幅に安価である単純で信頼性のある金ディスペンサに変換する。これらの新たなATMは、長時間使用可能である。生体認証関連の認証機能に対する全ての更新が信頼できる当事者のクライアント装置3300及び／又はセキュアトランザクションサーバ3351に直接導入されていることから、それらは頻繁に更新を必要としない。

【0282】

本発明の1つの実施形態の付加的なアーキテクチャの詳細が図34に示されている。図示されたように、本実施形態のクライアント装置3300は、本明細書に記載された様々なローカル認証技術を調整するためにローカルセキュアトランザクション装置3350及び信頼できる当事者3351の双方と通信するローカル認証アプリケーション3304を含む。1つの実施形態において、ローカル認証アプリケーション3304は、ローカルセキュアトランザクション装置3350とのローカルセキュアチャンネルを確立し、認証エンジン3310は、正当ユーザがクライアント装置3300を所有していることを検証するために信頼できる当事者によってリモート認証を実行する。

【0283】

1つの実施形態において、認証エンジン3310は、上述した同時係属特許出願に記載されているように信頼できる当事者のセキュアトランザクションサーバとの一連のトランザクションに入力することによって認証を行う。例えば、これらのトランザクションは、（例えば、指スワイプ、画像スナップ、音声記録などすることによって）生体認証テンプレートデータを生成するためにユーザがクライアントの生体認証装置に登録する登録処理を含むことができる。登録は、信頼できる当事者のセキュアトランザクションサーバの指示下とすることができ、又は、ユーザによって自律的に行うことができる。そして、ユーザは、ネットワークを介してセキュアトランザクションサーバに生体認証装置に登録し、その後、登録処理中に交換されたデータを使用してこれらのサーバによって認証することができる（例えば、生体認証装置にプロビジョニングされた暗号化鍵）。

【0284】

1つの実施形態において、認証エンジン3310は、正当ユーザがクライアント装置3300を所有している可能性に対応する保証レベルを計算するための保証レベル計算モジュール3306を含む。そして、信頼できる当事者3351がローカルセキュアトランザクション装置3350においてローカルトランザクション（例えば、金融トランザクション、小売購入、ユーザのアカウント内の機密情報へのアクセスなど）を許可する必要があるかどうかを判定するために、この保証レベルを使用することができる。1つの実施形態において、信頼できる当事者3351は、特定のトランザクションに必要な保証レベルを指定することができる。例えば、かなりの金額の転送をとまなう金融トランザクションについて、信頼できる当事者3351は、例えば、ユーザのアカウントへのアクセスをとまなうトランザクションよりも比較的高い保証レベルを必要とすることができる。

【0285】

1つの実施形態において、保証レベル計算モジュール3306は、ユーザの機密情報を開示することなく、信頼できる当事者3351に対して（例えば、値、比率、コードなどとして指定された）保証レベルを送信し、それによってユーザのプライバシーを保護する。他の実施形態において、保証レベル計算モジュール3306は、現在のトランザクションに必要な保証レベルを知っており、保証レベルが十分に高いかどうかを判定し、再度信頼できる当事者3351に対してユーザの個人情報を開示することなく、トランザクションが信頼できる当事者3351に対して許可又は拒否されるかどうかの指示を送信する。

【0286】

1つの実施形態において、クライアント装置3300と信頼できる当事者3351との間の通信は、第1の鍵を使用して外向きの通信を暗号化し且つ第2の鍵を使用して到来通信を復号することができるセキュア通信モジュール3313を介してセキュアにされる。

10

20

30

40

50

対称鍵暗号化方式において、第1及び第2の鍵は同じである。非対称鍵暗号化方式において、鍵は異なる。しかしながら、本発明の基本原理は、暗号化の任意の特定の種類に限定されるものではない。

【0287】

1つの実施形態において、保証レベル計算モジュール3306は、1つ以上の明示的なユーザ認証装置3320-3321を介して現在又は最近の明示的なユーザ認証結果を含むことができる現在のユーザ認証結果3305に少なくとも部分的に基づいて保証レベルを判定する。これは、例えば、指紋認証装置を介した指紋認証、カメラ及び顔認識ハードウェア／ソフトウェアを介した顔認識認証、マイク及び音声認識ハードウェア／ソフトウェアを介した音声認識、カメラ及び関連するハードウェア／ソフトウェアを使用した網膜スキャン、キーパッドを介したエンドユーザによるパスワード／PIN入力、及び／又は、様々な他の種類の明示的なユーザ認証装置及び／又は技術を含むことができる。

10

【0288】

1つの実施形態において、セキュア記憶装置3325は、各ユーザ認証装置3320-3321についての生体認証基準データレコードを暗号的に保護する（例えば、記憶装置3325をセキュアにするために対称鍵を使用してデータをラッピング）。セキュア記憶装置3325は、認証装置3320-3321のセキュアな周囲の外側に図示されているが、1つの実施形態において、各認証装置3320-3321は、生体認証基準データレコードを暗号的に保護するために、独自の統合されたセキュア記憶装置を有してもよい。

【0289】

明示的なユーザ認証に加えて、認証エンジン3310の1つの実施形態は、保証レベルを生成するために保証計算モジュール3306によって使用されるようにセンサ3343からデータを収集する。例示として、センサ3343は、ユーザの現在位置を示すためにGPSセンサなどの位置センサを含むことができる。クライアント装置3300がローカルセキュアトランザクション装置3350の既知の近傍などの予想位置にある場合、これは、ユーザが正当ユーザである可能性を増加させる。これに対して、ユーザがローカルセキュアトランザクション装置3350の近くでないことをGPSの読み取り値が示す場合、これは、トランザクションを開始するユーザが正当ユーザでないことを示す。それゆえに、1つの実施形態において、保証計算モジュール3306は、ユーザが予想位置にある場合には保証レベルを増加させ、ユーザが予想されない位置にある場合には保証レベルを減少させる傾向がある。

20

30

【0290】

温度センサ、湿度センサ及び加速度計などの様々な追加センサ3343は、ユーザ認証に関連するデータを収集するために使用することができる。例えば、温度／湿度センサは、位置センサによって指定された位置についての既知の温度／湿度と比較することができる現在の温度／湿度を提供することができる。値が大きく異なっている場合、これは、クライアント装置3300が偽装されていることを示すことができる。主張された位置及び温度／湿度の比較は、信頼できる当事者3351によって使用されるセキュアトランザクションサーバなどのリモートサーバにおいて行うことができる。他の実施形態において、装置における加速度計は、ユーザの歩行を測定し、ユーザの既知の歩行に対してこれらの測定値を比較するために使用することができる。歩行が一致する場合（指定された閾値内）、これは、正当ユーザがクライアント装置3300を所有している可能性を増加させる。

40

【0291】

ローカル認証アプリケーション3304は、更に本発明の基本原理を順守しながら様々な方法で実装することができる。例えば、1つの実施形態において、ローカル認証アプリケーション3304は、信頼できる当事者3351にとって具体的に設計される。例えば、信頼できる当事者が金融機関（例えば、Wells Fargo（登録商標））である場合、ローカル認証アプリケーション3304は、その銀行のために／によって具体的に設計されたアプリケーションとすることができる。他の実施形態において、同じローカル認証アプリケーション3304は、例えば、ユニバーサルローカル認証アプリケーション

50

として、様々な信頼できる当事者間で共有することができる。更に、別個の論理要素として図34に図示しているが、図34における認証エンジン3310は、ローカル認証アプリケーション3304内に統合することができる。他の実施形態において、ローカル認証アプリケーション3304は、ウェブブラウザコンテキスト内で実行されるウェブブラウザ又はアプリケーションとすることができる（例えば、トランザクションを開始するためにユーザがローカルセキュアトランザクション装置3350の近傍に入るか又は信頼できる当事者のウェブページに接続するとき）。

【0292】

ローカル認証アプリケーション3304は、信頼できる当事者によって必要とされる実装に応じて様々なローカル機能を実行することができる。例えば、1つの実施形態において、ローカル認証アプリケーション3304は、信頼できる当事者3351によって提供された秘密コード（又は他の認証データ）を受信し、（例えば、バーコードを介して又は上述したような他の通信技術を使用して）認証のためにローカルセキュアトランザクション装置3350に対して秘密コードをセキュアに送信する。あるいは、1つの実施形態において、ユーザは、ローカルセキュアトランザクション装置3350に秘密コードを手動で入力することができる。同様に、ローカルセキュアトランザクション装置3350によって受信された秘密コードなどの認証データは、ローカル認証アプリケーション3304に中継されることができ、その後、認証エンジン3310に認証データを中継する及び／又は（例えば、クライアント装置3300の位置の証明として）信頼できる当事者3351をあてにする。

【0293】

クライアント装置の認証を行うための方法の1つの実施形態が図35に示されている。本方法は、図33-34に示されるアーキテクチャ上で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るものではない。

【0294】

3501において、クライアントは、ローカルセキュアトランザクション装置（例えば、ATM）の近傍に入り、3502において、ローカルチャンネルを介してローカルセキュアトランザクション装置との間にセキュア接続が確立される。上述したように、ローカルチャンネルは、近距離無線通信、ブルートゥース、Wi-Fi、又はクライアント装置及びローカルセキュアトランザクション装置の双方によってサポートされる他の種類のプロトコルを使用して実装することができる。動作3502は、いくつかの実施形態においては必要とされないことがある。例えば、正当ユーザがクライアント装置を所有している旨の高レベルの保証を有する信頼できる当事者によってクライアント装置が認証することが可能である場合、及び、クライアント装置が信頼できる当事者に対してその現在位置を確認することが可能である場合、ローカルチャンネルは必要でないことがある。

【0295】

3503において、クライアント装置は、ネットワークを介して信頼できる当事者を認証する。正当ユーザが装置を所有しているという保証レベルを生成するために任意の利用可能な技術は、この動作のために使用することができる。例えば、ユーザは、生体認証指紋認証装置上で指をスワイプする、顔認識のための顔画像をキャプチャする及び／又は秘密コードを入力することによって明示的な認証を実行することができる。あるいは、非侵襲型認証技術は、ユーザが最近（例えば、指定された期間内に）クライアント装置に明示的に認証されているかどうかを判定して、及び／又は、位置データ、温度／圧力データ及び／又は加速度計データなどのセンサデータを使用して行うことができる。

【0296】

保証レベルが生成される方法にかかわらず、認証の結果は、ユーザのプライバシーを保護するようにして（例えば、クライアント装置を具体的に識別するデータを提供することなく）ネットワークを介して信頼できる当事者に提供することができる。例えば、上述したように、保証レベル自体及び／又は認証の成功又は失敗の指示は、機密ユーザ情報を開示することなく信頼できる当事者に提供されることができる。

【0297】

3504において認証が成功したと判定された場合、3507において、ローカルトランザクションが許可される。1つの実施形態において、これは、1つ以上の動作を実行するためのローカルセキュアトランザクション装置を指示する信号を送信する信頼できる当事者を含む。例えば、ローカルセキュアトランザクション装置がATMである場合、動作は、ユーザ指定の現金額の分配を含むことができる。ローカルセキュアトランザクション装置がデビット装置である場合（例えば、ユーザが購入を行っている小売店や他の位置）、信頼できる当事者が送信した信号は、トランザクションについての支払いを確認することができる（それに応じてユーザのアカウントを引き落とす）。これらは単に例示であることに留意すべきである。更に本発明の基本原理を順守しながら、様々な代替アプリケーションを使用することができる。

10

【0298】

（例えば、許容可能な保証レベルに到達していなかったために）3504における認証が失敗した場合、3505において、トランザクションが拒否され及び／又は1つ以上の追加の認証技術が必要とされることができる。例えば、ユーザは、1つ以上の追加技術（例えば、初期認証が指紋である場合には秘密コード入力など）を使用して、追加の認証を提供するために必要とされることができる。3506において追加の技術が十分であると判定された場合、トランザクションは、3507において許可される。そうでない場合、トランザクションは、再度拒否され及び／又は追加の認証技術が試みられる。

J. オンライントランザクションのためのユーザ確認

20

【0299】

信頼できる当事者とのトランザクションを完了することが1人以上の他のユーザからの承認を必要とする様々なシナリオがある。例示として、限定されるものではないが、親は、子供によって開始された金融トランザクションを承認したいことがあり、司令官は、兵士によって開始されたトランザクションを承認する必要があることがあり、管理者は、従業員によって開始されたビジネストランザクションを承認する必要があることがあり、暗号化鍵管理システムは、それが委任される前に、複数のユーザが特定のトランザクションを承認するのを必要とすることがある。

【0300】

本発明の1つの実施形態は、マルチユーザ確認アプリケーションを可能とするようにネットワークを介してユーザの強力な認証を提供するために、本明細書に記載された技術を使用する。セキュアトランザクションサービス3650を有する信頼できる当事者（以下、単に「信頼できる当事者」という）とのトランザクションを開始しようとするユーザによって制御されるリモート認証機能3600を有するクライアント装置を示す図36にそのような一例が示されている。1つの実施形態において、クライアント装置3600のユーザは、本明細書に記載された1つ以上のリモート認証技術（例えば、指紋センサ上で指をスワイプするなどの生体認証入力、PIN又はパスワード入力などを提供する）を使用して信頼できる当事者3650によって認証する。

30

【0301】

図示された実施形態において、他のクライアント装置3601-3602は、クライアント装置3600のユーザについての「承認者」として信頼できる当事者に登録されたユーザを有する。それゆえに、特定の種類のトランザクション（例えば、指定された閾値を超える量を含む金融トランザクション）について、信頼できる当事者は、クライアント装置3601-3602のユーザから承認を必要とすることがある。以下に説明するように、本明細書に記載されたリモート認証技術は、承認処理の一部として使用される。

40

【0302】

1つの実施形態において、クライアント装置3600のユーザによる認証の成功に回答して、信頼できる当事者3650における通知生成ロジックは、クライアント装置3600のユーザがトランザクションを完了しようとすることを示す「承認者」として登録されたユーザを他のクライアント装置3601-3602に対して通知を送信する。通知は、

50

本発明の基本原理に基づいて様々な方法で送信することができる。例えば、クライアント装置 3601-3602 がモバイル装置である場合、クライアント装置 3601-3602 にプッシュ通知が送信されることができる。代替的に又は追加的に、通知は、電子メール、テキストメッセージ（例えば、SMS）、インスタントメッセージ又はクライアント装置 3601-3602 にメッセージを配信することができる任意の他の技術を介して送信されてもよい。

【0303】

1つの実施形態において、通知は、クライアント装置 3600 のユーザによって試みられたトランザクションの詳細を含む。例えば、トランザクションが金融トランザクションである場合、通知は、処理された特定の金額と行われた金融トランザクションの種類（例えば、引き出し、口座間転送など）を含むことができる。あるいは、通知は、信頼できる当事者における承認サービスに対してクライアント装置 3601-3602 のユーザを誘導するハイパーリンク又は他の種類のポインタなどのリンクを含むことができる。リンクの選択に応じて、クライアント装置のユーザ 3601-3602 は、（例えば、ウェブページ又は情報を提供するための他の有用なフォーマットで）トランザクションの詳細を提供してもよい。

【0304】

1つの実施形態において、通知に応答してトランザクションの詳細を検討する際に、クライアント装置 3601-3602 のユーザは、（例えば、本明細書に記載された多要素認証技術を使用して）信頼できる当事者とのリモート認証を実行し且つトランザクションの承認を示すことによって要求を確認することができる。

【0305】

本発明の1つの実施形態に使用されるクライアント装置 3600-3602 の追加のアーキテクチャの詳細が図 37 に示されている。特に、本実施形態のクライアント装置 3600-3602 は、信頼できる当事者 3650 と通信して本明細書に記載されたトランザクション承認技術を調整するためのセキュアトランザクションアプリケーション 3704 を含む。セキュアトランザクションアプリケーション 3704 は、セキュアなアプリケーションプログラミングインターフェース（API）を介して認証エンジン 3710 とインターフェースするスタンドアロン型アプリケーションとすることができる。あるいは、セキュアトランザクションアプリケーション 3704 は、モバイル装置アプリケーション又はウェブブラウザのプラグインとして実装することができる。

【0306】

本明細書に記載されたユーザ確認処理を調整することに加えて、1つの実施形態において、セキュアトランザクションアプリケーション 3704 は、各ユーザに表示されるテキストがトランザクションに関連する実際のテキストであることを保証する。例えば、アプリケーション 3704 は、セキュアウィンドウ内にテキストを表示し、トランザクションを確認するために認証を提供するようにユーザに求めることができる。アプリケーションは、タイマを開始し、（例えば、コンテンツの署名を生成することによって）定期的にユーザに表示される現在のウィンドウの内容を確認することができる。検証期間はランダムに選ばれてもよい。それゆえに、アプリケーションは、各ユーザがウィンドウにおいて有効なトランザクションの詳細を見ることを継続的に保証する（それによってトランザクションのテキストが「中間者」攻撃によって変更されていないことを保証する）。コンテンツが改竄されたことをアプリケーションが検出した場合、それは、トランザクションの承認が生成されるのを防止する。

【0307】

1つの実施形態において、ユーザが有効な認証（例えば、指紋センサ上で指をスワイプ）を提供した後、クライアント装置は、ユーザを識別し、トランザクションの詳細（例えば、表示されたテキスト）及び信頼できる当事者から提供されたランダムチャレンジ（例えば、トークンは、トランザクションの詳細とナンスにわたって署名することができる）を有するトークン（暗号化署名）を生成する。これは、トランザクションの詳細がサーバ

10

20

30

40

50

とクライアントの間で変更されていないことを信頼できる当事者 3650 が確認するのを可能とする。1つの実施形態において、アプリケーション 3704 は、その後にユーザ名によってユーザを識別してトークンを検証する信頼できる当事者に対して生成されたトークン及びユーザ名を送信する。検証が成功すると、確認メッセージがクライアントに送られ、トランザクションが処理される。

【0308】

上記技術は、クライアント装置 3600 に由来するトランザクション及びクライアント装置 3601－3602 のユーザに由来する承認トランザクションの双方の要求／確認について実施されてもよい。

図 37 を参照すると、1つの実施形態において、認証は、各ユーザをリモート認証するために信頼できる当事者 3650 によって一連のトランザクションを実行するように設計されたクライアント装置 3600－3602 における認証エンジン 3710 を介して行うことができる。例えば、同時係属出願に記載されるように、認証フレームワーク及び関連する認証技術が使用されることができ、ユーザは、（例えば、指スワイプ、画像スナップ、音声記録などによって）クライアントの生体認証装置 3720－3721 に登録して生体認証テンプレートデータを生成し、生体認証装置をネットワーク（例えば、セキュア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）にわたって1つ以上の信頼できる当事者 3650 に登録し、その後、登録プロセス中に交換されるデータ（例えば、生体認証装置内にプロビジョニングされる暗号化鍵）を使用して、それらの信頼できる当事者 3650 によって認証する。1つの実施形態において、信頼できる当事者による「登録」は、各ユーザ認証装置 3720－3721 について信頼できる当事者と対称又は非対称鍵を交換し、各認証装置 3720－3721 に関連したセキュア記憶装置 3725 内に鍵を記憶することを含む。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も限定されるものではない。

【0309】

認証段階中において、例えば、署名を生成し、署名を検証し、及び／又は、クライアント 3600－3602 と信頼できる当事者 3650 との間の通信を暗号化するために鍵が使用される。認証されると、ユーザは、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。更に、1つの実施形態において、ユーザを固有に識別することができる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クライアント装置（例えば、スマートフォン、ノートブックコンピュータなど）上でローカルに保持することができる。

【0310】

1つの実施形態において、認証エンジン 110 は、正当ユーザがクライアント装置 100 を所有している可能性に対応する保証レベルを計算するための保証レベル計算モジュール 3706 を含む。そして、それは、信頼できる当事者 3650 が現在のトランザクションを承認する必要があるかどうかを判定するために、この保証レベルを使用することができる。1つの実施形態において、信頼できる当事者 3650 は、所与のトランザクションに必要な保証レベルを指定することができる。例えば、かなりの金額の転送をとまなう金融トランザクションについて、信頼できる当事者 3650 は、例えば、金の交換やユーザ情報への単なるアクセスをとまなわないトランザクションよりも比較的高い保証レベルを必要とすることができる。

【0311】

1つの実施形態において、保証レベル計算モジュール 106 は、ユーザの機密情報を開示することなく、信頼できる当事者 3650 に対して（例えば、値、比率、コードなどとして指定された）保証レベルを送信し、それによってユーザのプライバシーを保護する。他の実施形態において、保証レベル計算モジュール 3706 は、現在のトランザクション

に必要な保証レベルを知っており、保証レベルが十分に高いかどうかを判定し、信頼できる当事者 3650 に対してユーザの個人情報を開示することなく、トランザクションが信頼できる当事者 3650 に対して許可又は拒否されるかどうかの指示を送信する。

【0312】

1つの実施形態において、クライアント装置 3600-3602 と信頼できる当事者 3650 との間の通信は、第1の鍵を使用して外向きの通信を暗号化し且つ第2の鍵を使用して到来通信を復号することができるセキュア通信モジュール 3713 を介してセキュアにされる。対称鍵暗号化方式において、第1及び第2の鍵は同じである。非対称鍵暗号化方式において、鍵は異なる。しかしながら、本発明の基本原理は、暗号化の任意の特定の種類に限定されるものではない。

10

【0313】

1つの実施形態において、保証レベル計算モジュール 3706 は、1つ以上の明示的なユーザ認証装置 3720-3721 を介して現在又は最近の明示的なユーザ認証結果を含むことができる現在のユーザ認証結果 3705 に少なくとも部分的に基づいて保証レベルを判定する。これは、例えば、指紋認証装置を介した指紋認証、カメラ及び顔認識ハードウェア／ソフトウェアを介した顔認識認証、マイク及び音声認識ハードウェア／ソフトウェアを介した音声認識、カメラ及び関連するハードウェア／ソフトウェアを使用した網膜スキャン、キーパッドを介したエンドユーザによるパスワード／PIN 入力、及び／又は、様々な他の種類の明示的なユーザ認証装置及び／又は技術を含むことができる。

20

【0314】

1つの実施形態において、セキュア記憶装置 3725 は、各ユーザ認証装置 3720-3721 についての生体認証基準データレコードを暗号的に保護する（例えば、記憶装置 3725 をセキュアにするために対称鍵を使用してデータをラッピングする）。セキュア記憶装置 3725 は、認証装置 3720-3721 のセキュアな周囲の外側に図示されているが、1つの実施形態において、各認証装置 3720-3721 は、生体認証基準データレコードを暗号的に保護するために、独自の統合されたセキュア記憶装置を有することができる。

【0315】

明示的なユーザ認証に加えて、認証エンジン 3710 の1つの実施形態は、保証レベルを生成するために保証計算モジュール 3706 によって使用されるセンサ 3743 からデータを収集することによって非侵襲型認証を行う。例示として、センサ 3743 は、ユーザの現在位置を示すために GPS センサなどの位置センサを含むことができる。クライアント装置 3600-3602 が既知の近傍などの予想位置（例えば、「自宅」や「オフィス」の位置）にある場合、これは、ユーザが正当ユーザである可能性を増加させる。これに対して、ユーザが予想位置にないことを GPS の読み取り値が示す場合、これは、トランザクションを開始するユーザが正当ユーザでないことを示す。それゆえに、1つの実施形態において、保証計算モジュール 3706 は、ユーザが予想位置にある場合には保証レベルを増加させ、ユーザが予想されない位置にある場合には保証レベルを減少させる。

30

【0316】

温度センサ、湿度センサ及び加速度計などの様々な追加センサ 3743 は、ユーザ認証に関連するデータを収集するために使用されることができる。例えば、温度／湿度センサは、位置センサによって指定された位置についての既知の温度／湿度と比較することができる現在の温度／湿度を提供することができる。値が大きく異なっている場合、これは、クライアント装置 3600-3602 が偽装されていることを示すことができる。主張された位置及び温度／湿度の比較は、信頼できる当事者 3650 によって使用されるセキュアトランザクションサーバなどのリモートサーバにおいて行うことができる。他の実施形態において、装置における加速度計は、ユーザの歩行を測定し、ユーザの既知の歩行に対してこれらの測定値を比較するために使用することができる。歩行が一致する場合（指定された閾値内）、これは、正当ユーザがクライアント装置 3600-3602 を所有している可能性を増加させる。

40

50

【0317】

他の非侵襲型認証技術は、最後に成功したユーザ認証から経過した時間量を測定することを含む。例えば、ユーザが明示的なユーザ認証をごく最近行った場合（例えば、わずか数分前に指紋センサ上で指をスワイプするなど）、これは、正当ユーザがクライアント装置を所有したままであることを示す傾向がある（それによって高い基準保証レベルをもたらす）。これとは対照的に、最後の明示的な認証が数時間又は数日前であった場合、新たな明示的なユーザ認証は、許容可能な保証レベルに到達するのを必要とされることができる。

【0318】

本発明の1つの実施形態にかかる方法が図38に示されている。3801において、クライアントのユーザは、N人の他のユーザによる確認を必要とするトランザクションをトリガする。例えば、信頼できる当事者のユーザのアカウントは、ユーザによって開始された特定の種類のトランザクション（又は全てのトランザクション）が1人以上の他のユーザによる確認を必要とすることを示すことができる。例えば、ユーザのアカウントは、1人以上の親又は保護者による認証を必要とする未成年としてユーザを識別することができる。ユーザはまた、本明細書に記載された認証技術の1つ以上を実装することによって3801において認証される。

【0319】

3802において、サーバは、ユーザによってトリガされたトランザクションを確認する必要があるN人の他のユーザを選択する。例えば、ユーザによるトランザクションの開始を検出すると、信頼できる当事者は、トランザクションがトランザクションを確認することができるユーザの確認及び識別を必要とすることを判定するために、そのユーザデータベースにクエリすることができる。1つの実施形態において、トランザクションを確認することができるユーザの全てのサブセットは、実際にトランザクションを確認することができる。例えば、ユーザが2人の親を有する未成年である場合、1つの実施形態において、通知は、双方の親に送信されてもよいが、いずれかの親による確認は、トランザクションが進行するのを可能とする。同様に、ビジネストランザクションを確認するために認証された10人のユーザがいてもよいが、2つの確認のみがトランザクションを進行できるようにするために必要とされる。

【0320】

1つの実施形態において、（例えば、ユーザがプッシュ通知を受信することができるクライアント装置を有する場合）トランザクションを確認することができるそれらのユーザのクライアント装置に対してプッシュ通知が送信されることができる。代替的に又は追加的に、通知は、電子メール、テキストメッセージ（例えば、SMS）、インスタントメッセージ又はクライアント装置にメッセージを配信することができる任意の他の技術を介して送信されてもよい。1つの実施形態において、ユーザは、2つ以上の通信チャンネルを介して確認メッセージを受信するためにサーバに登録されることができる。例えば、ユーザは、プッシュ通知及び確認要求を含む電子メールの双方を受信することができる。

【0321】

確認要求が送信される方法にかかわらず、3803において、N人のユーザの全て又はサブセットは、確認処理の一部としてサーバと認証を行う。任意のリモート認証技術は、ユーザを認証してトランザクションを確認するために使用することができる。例えば、ユーザは、信頼できる当事者に以前に登録されたクライアントにおける生体認証装置に対して生体データを提供することによってトランザクションを確認することができる（例えば、指紋スキャナ上で指をスワイプ）。上述したように、トランザクションに関連する詳細は、テキスト及び他の情報をセキュアに表示することができるセキュアトランザクションアプリケーションを介してユーザに提供することができる（すなわち、ユーザがトランザクションを確認する場合、彼／彼女がトランザクションを説明する実際の不変のテキストを見たことを保証する）。

【0322】

3804において最小指定数のユーザが要求を確認したことが判定されると、トランザクションは、3807において許可される。本方法の1つの実施形態は、確認要求が送信されてからの経過時間を測定するために確認のタイマを開始する。3805において確認タイマが閾値（例えば、数時間、日など）に到達したと判定されると、トランザクションは、3806において禁止される。タイマ閾値に到達するまで、本方法は、3804において最小指定数のユーザが要求を確認するのを待機する。

K. 信頼を委任するためのシステム及び方法

【0323】

既存の認証システムは、新たな認証部が信頼できるクライアントに登録された認証部を使用して有効にするのを可能としない。例えば、ユーザが多くウェブサイトに登録された後に電話の音声認証システムをインストールする携帯電話における指紋センサを有する場合、彼女は、彼女が指紋センサによって使用していた全てのウェブサイトで彼女の音声認証部を自動的に登録する方法を有しない。むしろ、この場合、ユーザは、信頼できる当事者によって音声認証部を登録するために、同じ登録及び登録処理を介してステップしなければならない。同様に、ユーザが認証部の新たなセットを使用して新たな装置を購入した場合、ユーザは、サーバによって新たな認証部の全てを再登録及び再登録する必要がある。

【0324】

以下に記載される本発明の実施形態は、既に有効とされて1つ以上の信頼できる当事者に登録されている信頼されたクライアント装置を使用してユーザが新たなクライアント装置の認証部を容易に有効として登録するのを可能とする。特に、これらの実施形態は、新たな認証部を有効にし、新たなクライアント装置を有効にし、複数のクライアント装置間で同期して登録を維持するために使用することができる。

【0325】

図39は、本発明の1つの実施形態にかかる高レベルの信頼委任の概要を提供する。信頼できる装置3902、すなわち、1つ以上の信頼できる当事者3950に登録されている認証部を有する装置は、ユーザの新たなクライアント装置3900とセキュア接続を確立する。セキュア接続が確立される特定の方法は、本発明の基本原理に関係がない。クイックレスポンス（QR）コードを使用してHTTPS接続を確立する近距離無線通信（NFC）、ブルートゥース、直接WiFiなどの様々な技術が使用されることができる。1つの実施形態において、装置は、セキュア接続のために必要な大規模ランダムトークン（LRT）を交換することができ、オンラインサービスに捕捉されたLRTを提供することによって接続を確立することができ、サービスを介してセキュア通信をブートストラップすることができる。

【0326】

1つの実施形態において、セキュア接続が信頼できるクライアント装置3902と新たなクライアント装置3900との間で確立されると、信頼できる装置から新たな装置に登録データを転送して統合するためにセキュアプロトコルが実装される（詳細は後述する）。登録が転送されると、登録を検証するために新たなクライアント装置3900と信頼できる当事者3950との間に他のセキュアプロトコルが実装される（例えば、1つの実施形態におけるHTTPS）。

【0327】

本明細書に記載された実施形態は、信頼できる当事者3950との認証トランザクションに使用される認証データの転送をフォーカスしているが、信頼できる当事者は、本発明の基本原理を順守するために必要とされない場合がある。例えば、信頼できる装置3902は、（例えば、新たなクライアント装置3900を使用してローカルに認証するための認証データを提供するために）任意の信頼できる当事者がシステムにかかわることなく新たなクライアント装置3900に認証データを提供するためにセキュア接続を確立することができる。

【0328】

図40に示されるように、信頼委任モジュール4000-4001は、セキュア接続を確立し、登録を交換し、各信頼できる当事者3950におけるセキュアトランザクションサービス4004で登録を検証するために、それぞれ、新たな装置3900及び信頼できる装置3902上で実行することができる。本明細書で使用されるように、「信頼できる認証部」は、ユーザが1つ以上の信頼できる当事者に既に登録されている認証部である。新たな「新たな認証部」は、ユーザが現在信頼できる認証部とともに使用されている全ての信頼できる当事者の登録を可能にしたいものである。それゆえに、認証エンジン3711は、信頼できる当事者に1つ以上のユーザ認証装置3720-3721を以前に登録した場合、信頼できる認証部と考えられる。1つの実施形態の目的は、信頼できる認証部に新たな認証部から新たな装置3900の認証エンジン3710を有効にすることである。10
「信頼できる装置」は、信頼できる認証部を有するものであり、「新たな装置」は、新たな認証部を有するものである。

【0329】

信頼委任は、信頼できる認証部を使用して新たな認証部を有効にする処理を指す。したがって、信頼委任の前提条件は、ユーザが信頼できる装置を有し、ユーザが新たな装置を有し、ユーザが信頼できる装置から新たな装置に信頼を委任することを望むことである。

【0330】

図40を参照すると、1つの実施形態において、ユーザは、初期のセキュア接続を確立するために、新たなクライアント装置3900における信頼委任アプリケーション4000及び信頼できるクライアント装置の信頼委任アプリケーション4001を開始する。20
1つの実施形態において、信頼委任アプリケーションは、本明細書に記載された信頼委任動作を実行するように具体的に設計されたモバイル装置のアプリケーションとすることができる。他の実施形態において、信頼委任アプリケーションは、彼／彼女が（例えば、埋め込まれたJavaScriptや他のアプレット又は実行可能なプログラムコードを含むウェブページを経由して）信頼の委任を実行するように望んでいることを示すユーザに回答して実行されるブラウザプラグインとすることができる。更に、信頼委任アプリケーション4000-4001は、信頼できる当事者との認証を管理するように設計された認証アプリケーションなどのより大きなアプリケーション内のソフトウェアモジュールとすることができる。しかしながら、本発明の基本原理は、信頼委任アプリケーション4000-4001の任意の特定の実装に限定されるものではないことに留意すべきである。30

【0331】

1つの実施形態において、信頼できる装置3902における信頼委任動作を承認するために、ユーザは、信頼できる装置の認証エンジン3711でローカルに認証する（例えば、ユーザ認証装置3722-3723に対して生体認証入力を提供する）。同様に、1つの実施形態において、ユーザは、新たなクライアント装置3900における認証エンジン3710を使用してローカル認証することができる。これら2つの認証ステップは、委任処理を実行するために信頼委任アプリケーション4000-4001の認証を提供することができる。

【0332】

上述したように、信頼委任アプリケーション4000-4001は、セキュア接続を確立するために、それぞれのクライアント装置3900、3902において利用可能な通信インターフェースのいずれか（例えば、ブルートゥース接続用のブルートゥースインターフェース、NFC接続用のNFCインターフェースなど）を利用することができる。40

【0333】

セキュア接続が確立されると、1つの実施形態において、信頼できるクライアント3902の信頼委任アプリケーション4001は、信頼できる当事者に登録されている信頼できるクライアントにおける鍵の数(N)を示すデータを提供する。これに回答して、1つの実施形態において、信頼委任アプリケーション4000は、1つの秘密鍵(ND__Uauth.priv)と1つの公開鍵(ND__Uauth.pub)とを含むN個の新たな装置鍵対(ND__Uauth)を生成し、信頼できる装置3902の信頼委任アプリケー50

ション４００１にＮ個の新たな装置公開鍵を送信する。

【０３３４】

１つの実施形態において、信頼委任アプリケーション４００１は、その後、Ｎ個の新たな装置の各公開鍵のそれぞれに関連する署名（ＴＤ＿Ｕａｕｔｈ．ｓｉｇ）を生成するために、その対応する信頼できる装置秘密鍵（ＴＤ＿Ｕａｕｔｈ．ｐｒｉｖ）によってＮ個の新たな装置の公開鍵のそれぞれに署名する。１つの実施形態において、「対応する」秘密鍵は、信頼できる当事者に対応する特定の登録に関連付けられた秘密鍵である。信頼委任アプリケーション４００１はまた、信頼委任が発生したときに正確に検証するために、信頼できる当事者によってその後に使用されることができる生成された署名にタイムスタンプを挿入することができる。１つの実施形態において、信頼できるクライアント３９０２の信頼委任アプリケーション４００１は、新たなクライアント３９００の信頼委任アプリケーション４０００に対して、各信頼できる当事者に関連するその他の登録データとともに生成された署名のそれぞれを送信する。各信頼できる当事者についてのデータは、１つ以上の信頼できる当事者ＩＤコード（例えば、信頼できる当事者におけるサービスを特定するアプリケーションＩＤコード）、信頼できる当事者のユーザのために登録されたユーザ名、認証時に適切な鍵を見つけるために信頼できる当事者が使用する鍵ＩＤコード、及び、認証処理に関連する他のデータを含むことができる。

【０３３５】

１つの実施形態において、信頼委任アプリケーション４０００が署名や他の登録データを受信すると、新たなクライアント装置３９００が信頼できる当事者３９５０に接続したときに、それがその後に使用されることができるように、それはローカルセキュア記憶装置３７２５にこのデータを統合する。

【０３３６】

１つの実施形態において、登録データベースがローカルセキュア記憶装置３７２５に記憶された後、一連のブートストラップ動作は、信頼できるクライアント装置３９０２に以前に登録された信頼できる当事者（例えば、ウェブサイト、サービスなど）によって新たなクライアント装置３９００において委任された登録を利用するために信頼委任アプリケーション４０００によって実行されることができる。あるいは、記載されたブートストラップ動作は、（図４０に示されるようにセキュアトランザクションサービス４００４との直接通信を介して）認証エンジン３７１０自体によって行うことができる。本発明の基本原理は、新たなクライアント装置３９００における特定のソフトウェア構成要素が動作を実行するのにかわらず同じままである。

【０３３７】

特に、１つの実施形態において、信頼できる当事者３９５０のセキュアトランザクションサービス４００４は、セキュアトランザクションサービス４００２及び信頼委任アプリケーション４０００によってサポートされるリモート認証プロトコルを使用して新たなクライアント装置３９００上の登録があることを検出する。１つの実施形態において、ユーザは、新たなクライアント装置３９００から生体認証や他の形態の認証（例えば、セキュアコードを入力する）を実行するためにセキュアトランザクションサービス４００４によって最初に求められることがある。更に、この段階において、セキュアトランザクションサービス４００４は、署名に挿入されたタイムスタンプを検証し、タイムスタンプが時間の閾値量よりも古くないことを確認することができる。

【０３３８】

ユーザが許容可能な保証レベルで生体又は他の認証データを成功裏に提供すると仮定すると、信頼委任アプリケーション４０００及び／又は新たな認証部３７１０は、以下の３つの証明を含む応答を準備する：

１．信頼できる当事者に関連した新たな装置公開鍵にわたる証明（ＮＤ＿Ｕａｕｔｈ．ｐｕｂ）。１つの実施形態において、証明は、（例えば、信頼できる当事者の公開鍵を使用して）公開鍵にわたって生成された署名を含む。

２．信頼できる当事者に関連した新たな装置秘密鍵を使用した証明（ＮＤ＿Ｕａｕｔｈ

10

20

30

40

50

・ `priv`)。1つの実施形態において、証明を生成するために、秘密鍵は、(例えば、信頼できる当事者から送信されたランダムチャレンジなどの)信頼できる当事者によって公知のコンテンツにわたって署名を生成するために使用される。信頼できる当事者は、(ステップ1において)公開鍵を備えているので、コンテンツを復号することができ、それによって秘密鍵がコンテンツを暗号化するために使用されたことを確認する。

3. (例えば、公開鍵を取得するためにそのセキュアトランザクションデータベース4025をクエリするために鍵IDを使用することができるよう)公開鍵を配置するために信頼できるクライアント装置によって以前に生成され且つ信頼できる当事者で使用する鍵ID (`TD__Uauth.keyid`) とともにこの特定の信頼できる当事者のための新たな装置公開鍵に関連付けられた署名 (`TD__Uauth.sig`) 。

10

【0339】

1つの実施形態において、上記データの全ては、リモート認証応答において信頼できる当事者のセキュアトランザクションサービス4004に送信される。

【0340】

1つの実施形態において、上記証明を受信した後、セキュアトランザクションサービス4004は、以下の検証を行ってもよい：

1. 鍵IDを使用して信頼できる装置の公開鍵 (`TD__Uauth.pub`) を配置する。

2. 信頼できる装置の公開鍵 (`TD__Uauth.pub`) を使用して信頼できる装置によって生成された署名 (`TD__Uauth.sig`) を検証する。

20

3. 新たな装置の公開鍵 (`ND__Uauth.pub`) を使用して新たな装置の秘密鍵によって生成された署名 (`ND__Uauth.sig`) を検証する。且つ

4. 信頼できる当事者に関連した新たな装置公開鍵 (`ND__Uauth.pub`) にわたって証明を検証する。1つの実施形態において、この検証は、信頼できる当事者の秘密鍵を使用して実行される。

【0341】

信頼できる装置から新たな装置に登録データをセキュアに転送するための方法の1つの実施形態が図41に示されており、信頼できる当事者の登録データを検証するための方法の1つの実施形態が図42に示されている。これらの方法は、図39-40に示されたシステムアーキテクチャのコンテキスト内で実装されることができ、本発明の基本原理は、任意の特定のシステムアーキテクチャに限定されるものではない。

30

【0342】

最初に図41を参照すると、4101において、新たな装置は、信頼できる装置とセキュア通信チャネルを確立し、生成する鍵対の数(N)を判定する。上述したように、これは、信頼できる当事者と信頼できる手段によって登録された鍵対の数とすることができる。

【0343】

4102において、新たな装置は、N個の新たな公開鍵／秘密鍵の対を生成する。対称鍵を利用する代替実装において、新たな装置は、信頼できる当事者と共有される単一の(対称)鍵を生成することができる。4103において、N個の公開鍵は、信頼できる装置に送信され、4104において、信頼できる装置は、署名を生成するに対応する秘密鍵で各公開鍵を署名する。4105において、署名は、信頼できる当事者についての他の登録データとともに新たな装置に送信される(例えば、鍵ID、アプリケーションIDなど)。最後に、4106において、登録データ及び署名の全ては、認証エンジンによって使用されるローカルセキュアデータベース内に統合される。

40

【0344】

ここで図42を参照すると、4201において、(図41から委任操作を既に実行した)新たなクライアントは、信頼できる当事者とセキュア接続を確立する。4202において、信頼できる当事者は、新たな装置に委任されている既存の登録があることを検出する。応答において、4203において、信頼できる当事者は、新たな装置に認証要求を行う

50

。そして、ユーザは、1つ以上の生体又は他の認証技術を使用して認証することができる。上述したように、4204において、新たな装置は、新たな装置公開鍵にわたる証明、（例えば、チャレンジにわたって）新たな装置秘密鍵を用いて生成された署名、及び、信頼できる装置の秘密鍵及び関連する鍵IDを用いて生成された署名を含む応答を準備する。4205において、応答における全てのデータは、信頼できる当事者に送信され、4206において、信頼できる当事者は、応答に含まれるデータを検証する（1つの実施形態の詳細については上記参照）。検証が成功した場合、4207において、ユーザによって試行されるトランザクションが許可される。

【0345】

本明細書に記載された技術は、（上述したように）異なる装置における2つの認証部間で信頼を委任するために使用することができる。更に、1つの実施形態において、これらの技術は、同じ装置における2つの認証部間で信頼を委任するために使用することができる。この場合、2つの装置間のセキュア接続を確立する必要はないが、他の全ての操作は、装置内の2つの認証部間で行われてもよい。

【0346】

更に、関連するオペレーションのいくつかは、様々な方法で実施することができることに留意すべきである。例えば、信頼を委任するためのセキュアプロトコルは、新たな装置よりもむしろ信頼できる装置によって開始することができる。いずれの場合においても、新たな装置（又はより具体的には新たな装置における認証部）は、新たな鍵対の数（ N_{D_Uauth} ）を生成することができ、信頼できる装置における認証部は、これらの鍵対の公開鍵に署名することができる。

L. プライバシー強化データ同期のためのシステム及び方法

【0347】

現在のシステムは、クラウドサービスを利用して複数のクライアント装置間でデータを同期させるために存在する。ユーザが装置上で新たな文書を作成する場合（例えば、絵をスナップ、ワープロ文書作成など）又は既存の文書を修正する場合、ユーザが参加しているクラウドサービスは、通常、「クラウドに」新たな／修正された文書のコピーを記憶する。ユーザが第2の装置（例えば、職場のコンピュータ又は他の家族メンバーによって使用される他の装置）からクラウドサービスにアクセスする場合、クラウドサービスは、装置を同期するように構成されることができる。

【0348】

存在する1つの問題は、データが暗号化されていない形式でクラウドサービスに頻繁に記憶され、連邦政府機関による様々な種類のサイバー攻撃やクエリに対してデータを弱くすることである。

【0349】

以下に記載される本発明の実施形態は、プライバシー強化方法において装置間でデータを同期するのを可能とするプロトコル及び技術のセットを提供する。これらのプロトコル及び技術を使用して、クラウドサービスは、平文（例えば、暗号化されていない形式）でデータにアクセスする必要はなく、それによってユーザのプライバシーを保護する。

【0350】

最初の問題として、以下に説明される技術は、装置間でデータを同期するために、本明細書に記載された高度な認証技術に依存しないことに留意すべきである。例えば、これらの同期技術は、本発明の他の実施の形態について説明したように、リモートユーザ認証のためのシステムのコンテキスト外で使用することができる。しかしながら、これらの同期技術は、これらのリモートユーザ認証の実施形態の同期を実行するために使用することができる。例えば、1つの実施形態において、ユーザが訪れた各ウェブサイト又は他のオンラインサービスの登録データは、これらの同期技術を使用して複数の装置間で同期することができる。

【0351】

本明細書において使用されるように、「サークル」は、ユーザによって信頼できる装置

10

20

30

40

50

のネットワークを意味し、「サークルid」は、サークルを識別する識別子（例えば、容易に推測することができないもの）を意味する。「サークルクラウド」は、サークル及び信頼チェーン（以下に定義）についての情報を記憶するために使用されるオンラインサービスを意味し、クライアント装置のための通信ハブとして機能する。1つの実施形態において、サークルクラウドは、（少なくとも暗号化されていない形式で）いかなる機密データも記憶しない。用語「d. pub」は、装置の公開鍵を指し、「d. priv」は、装置の秘密鍵を指し、d. pub / d. priv は、装置 d の非対称公開鍵 / 秘密鍵の対を指す。1つの実施形態において、d. priv は、装置 d を出ることではない。「信頼チェーン」は、ユーザ及びそれらの関係によって信頼できる装置に関する情報を含むサークルクラウドに記憶されている永続データを意味する。「サークルチャンネル」は、それらの間でデータを交換して同期させるために2つ（又はそれ以上）の装置によって使用されるサークルクラウドによって提供されるセキュア通信チャンネルを意味する。

10

【0352】

本発明の1つの実施形態は、新たなユーザ装置が（a）サークルに参加し、（b）その後、サークルと同期するのを可能とするためのプロトコル及び関連する技術を含む。これらの実施形態は、本明細書に記載されたプロトコル及び技術をそれぞれ実装するためのプライバシー同期アプリケーション4311-4313及び参加及び同期に使用されるデータをそれぞれ記憶するためのセキュアデータ記憶装置4321-4332を有する3つのクライアント装置4301-4303をそれぞれ示す図43に関して説明される。本明細書において、装置4301は、時々、装置d1と称され、装置4302は、時々、装置d2と称され、装置4303は、時々、装置d3と称される。

20

【0353】

1つの実施形態において、参加及び同期は、複数の記憶装置サーバを含む複数のサークルクラウド4350を介して行われる。サークルクラウド4350内の信頼チェーン4360は、以下に説明するように、装置4301-4303の間のデータ定義の信頼関係を維持する。サークルチャンネル4370は、データを交換して同期させるために2つ以上の装置によって使用されるサークルクラウドによって提供されるセキュア通信チャンネルを備える。

a. サークルに参加

【0354】

装置4302（d2）は、ユーザ（すなわち、信頼できる装置の「サークル」）に属する装置4301（d1）及び4303（d3）の既存のネットワークに参加する。装置4302は、既にそのサークルの一部である他の装置4301がそれを許可した場合にのみ既存のサークルに参加することができる。

30

【0355】

信頼できる装置4301を使用して新たな装置4302を認証するための方法の1つの実施形態が図44に示されている。4401において、ユーザは、既存の信頼できる機器4301において新たな装置4302を認証する。例えば、1つの実施形態において、ユーザは、信頼できる装置4301におけるそのプライバシー同期アプリケーション4311及び新たなクライアント装置4302におけるプライバシー同期アプリケーション4312を開始することができる。

40

【0356】

4402において、1つの実施形態において、プライバシー同期アプリケーション4311-4312は、装置4301-4302にセキュア接続を確立させる。セキュア接続を確立するために、クイックレスポンス（QR）コードを使用してHTTPS接続を確立する近距離通信（NFC）、ブルートゥース、直接Wifiなどの様々な技術が使用されることができる。

【0357】

4403において、装置4301は、新たな装置4302に対して本明細書において「join1_data」と称されるセキュアデータを送信する。1つの実施形態において

50

、`join1_data`は、以下のフィールドを含む：{`d1.pub`，`sk.sym`，`circle-id`}。ここで、`d1.pub`は、装置4301の公開鍵であり、`sk.sym`は、装置4301によって生成されるランダム生成セッション鍵であり、`circle-id`は、装置4302が参加しているサークルを識別する固有の識別コードである。
【0358】

4404において、装置4302は、`join1_data`を読み込み、以下を含むことができる応答を準備する：

- ・ $\text{HMAC}(\text{sk.sym}, \text{d2.pub} \parallel T) \parallel \text{d2.pub} \parallel T$ 。ここで、 T はタイムスタンプである。

- ・ $\text{trust-block1} = S(\text{d2.priv}, \text{d1.pub}) \parallel \text{d1.pub} \parallel \text{d2.pub}$ 。

10

HMAC は、ハッシュベースのメッセージ認証コードの略であることに留意されたい。上記実施形態において、 HMAC は、タイムスタンプと装置4302の公開鍵を連結し、 HMAC 又は類似のアルゴリズムを使用して`sk.sym`によって結果の完全性を保護することによって生成される。更に、`trust-block1`は、装置4301の公開鍵にわたる装置4302の秘密鍵で生成された署名を含む。1つの実施形態において、`trust-block1`エントリはまた、タイムスタンプ(T)を含む。

【0359】

図44を参照すると、4405において、装置4302は、サークルクラウド4350にセキュアに接続し、 HMAC 及び`trust-block1`を含む応答を送信する。サークルクラウド4350は、装置4301によって受信したデータを記憶し、装置4301が接続するのを待機する。

20

【0360】

4406において、装置4301は、`circle-id`を使用してサークルクラウドに接続し、動作4405から装置4302の応答に含まれるデータの完全性を検証し、`trust-block2`を生成する。特に、1つの実施形態において、装置4301は、`sk.sym`を使用して`d2.pub`及び T を読み取って完全性を検証する（例えば、`d2.pub`及び T を復号するために`sk.sym`を使用する）。そして、装置4301は、自己の秘密鍵`d1.priv`を使用して`d2.pub`に署名し、`d1.priv`によって`d2.pub`にわたって生成された署名を含む $\text{trust-block2} = S(\text{d1.priv}, \text{d2.pub}) \parallel \text{d2.pub} \parallel \text{d1.pub}$ を生成する。1つの実施形態において、`trust-block2`はまた、タイムスタンプ(T)を含む。そして、装置4301は、サークルクラウド4350に対して`trust-block2`を含む上記データを送信する。

30

【0361】

4407において、サークルクラウド4350は、信頼チェーン4360に双方の信頼ブロックを追加する。1つの実施形態において、上記動作の後、装置4302は、`circle-id`に関連付けられているサークルに参加する。このサークル内の全ての装置4301、4303は、装置4302を信頼し、装置4302は、これらの装置の全てを信頼する。いかなる信頼された装置も、本明細書に記載された技術を使用して新たな装置を認証できることに留意されたい。

40

b. サークルとの同期

【0362】

この処理の間、同じサークルに属する装置4301-4303は、それらの間でデータを同期させる。この処理の上に実装された異なるアプリケーション固有のサブプロトコルが存在することができる。例えば、オンラインクラウド記憶装置アプリケーションは、全ての装置において同期されたユーザのデータを保持することを望むことができ、サークルクラウド上で暗号化されたコピーを保持することを望むことができる。他のアプリケーションは、サークル内の装置にメッセージを伝播することができる。例えば、1つの実施形態において、リモートの信頼できる当事者を認証するために1つの装置によって使用され

50

る登録データは、サークル内の全ての装置間で同期させることができる。更に本発明の基本原理を順守しながら、他の様々なアプリケーション及びサブプロトコルが実装されることができる。そのような全てのサブプロトコルは、以下に説明する基本処理ブロックを使用することができる。

【0363】

信頼チェーン

【0364】

「サークル参加」処理（図44）において明らかにされたように、信頼チェーン4360に入るものは、装置2が装置1によって信頼されていることを主張する証拠になる。それゆえに、信頼チェーン4360は、2つの装置間の信頼関係を主張するそれぞれの認証ブロックのチェーンである。1つの実施形態において、信頼チェーンは交換可能であり、装置4301が装置4302を信頼する場合、装置4302は装置4301を信頼することを意味する。信頼チェーン4360は、装置4301が装置4302を信頼すると主張するブロックがあり且つ装置4302が装置4301を信頼すると主張するブロックがない場合には壊れていると考えられる。1つの実施形態において、信頼チェーン4360はまた、過渡的であり、装置4301が装置4302を信頼し且つ装置4302が装置4303を信頼する場合、装置4301は装置4303を信頼することを意味する。1つの実施形態において、信頼チェーンは、circle-id固有であり、装置に関するいかなる機密情報も含まない。

【0365】

1つの実施形態では、信頼チェーン4360は、複数の信頼ブロックを含み、各ブロックは、以下のデータを含む： $\{di.pub, dj.pub, S(di.priv, dj.pub), S(dj.priv, di.pub)\}$ —すなわち、各装置の公開鍵と、他の各装置の公開鍵に対して各装置の秘密鍵を使用して生成された署名と、を含む。

【0366】

上記主張は、装置diが装置djを信頼し且つその逆もしかりであることを意味する。1つの実施形態において、信頼チェーン4360は、サークル内にある装置を判定して検証するために装置4301-4302によって使用される。それらが同じサークル内にあることを装置が確認した後、それらは、それらの間で暗号化されたデータを同期させるためにサークルチャンネル4370を使用することができる。

【0367】

1つの実施形態では、装置diが装置djと同じサークルにあるかどうかを判定するために、以下の動作が実行される：（a）各ノードが信頼チェーン内の装置であり且つ各矢印が信頼チェーン内のブロックに対応する方向グラフを構築し、（b）di及びdjを接続する直接経路が存在するかどうかを判定する。

【0368】

サークルチャンネル

【0369】

1つの実施形態において、図45に示される処理は、同一サークル内の他の装置との間でデータを同期させるために実施される。図示された例において、装置4301（d1）は、新たなデータを有し且つ他の装置に送信したい装置である。4501において、装置4301は、circle-idに関連付けられている信頼チェーン4360をダウンロードし、信頼チェーン（例えば、装置4302-4303）から同じサークル内の他の装置を識別し、信頼チェーンを使用して同じサークル内の他の装置の公開鍵を取得する。

【0370】

4502において、装置4301は、（例えば、乱数発生のための既知の技術を使用して）ランダムな暗号化鍵（REK）を生成する。4503において、装置4301は、サークル内の他の装置のそれぞれについて相互セッション鍵（SK）を導出する。1つの実施形態において、装置4301は、他の装置のそれぞれに対してDiffie-Hellman鍵交換アルゴリズムを使用してSKを導出する。Diffie-Hellmanは

10

20

30

40

50

、互いの事前の知識を有しない2つの当事者が共有秘密鍵を共同で確立するのを可能とする周知のアルゴリズムである。この場合、例えば、第1の装置が鍵対を有し、第2の装置にその公開鍵を提供する場合、第2の装置は、その秘密鍵及び第1の装置の公開鍵を使用して独立して新たな鍵（本特許出願においてはSK）を自動的に導出することができる（及びその逆もしかり）。1つの実施形態において、装置4301は、各他の装置4302、4303について異なるSKを生成するためにこれらの技術を使用する。

【0371】

4504において、装置4301は、各装置について導出されたSKによってREKを暗号化し、それらと適切な公開鍵を結合する。例えば、装置di及びdjについてのSKi及びSKjをそれぞれ生成する装置d1について、それは以下のようにREKを暗号化するためにセッション鍵を使用する：

{d1. pub, di. pub, E(SKi, REK)} (装置diについて)

{d1. pub, dj. pub, E(SKj, REK)} (装置djについて)

処理の終了時に、装置di及びdjのそれぞれは、（上述したようにDiffie-Hellmanを使用して各装置によって独立して導出された）それぞれのセッション鍵を使用してREKを復号することができる。

【0372】

4505において、装置4301は、REKによって同期するようにデータを暗号化する—すなわちE(REK, 同期されるデータ)。上述したように、任意のデータは、例を挙げると、マルチメディアファイル、生産性文書及び／又はクライアント設定データ（例えば、上述したように信頼できる当事者登録データ）などのようにして同期させることができる。

【0373】

4507において、装置4301は、各SKを用いて暗号化されたREK及びREKによって暗号化された同期されるデータをサークルチャンネルに提供する：

[{d1. pub, di. pub, E(SKi, REK)}, {d1. pub, dj. pub, E(SKj, REK)}, ...]

E(REK, 同期されるデータ)

【0374】

データがサークルチャンネルに提供された後、4506において、同じサークル内の個々の装置は、それらの公開鍵（例えば、装置diについて{d1. pub, di. pub, E(SKi, REK)}に対応するレコードをダウンロードし、同じSK（例えば、SKi）を導出し、REKを復号し、同期するデータを復号するためにREKを使用する。

【0375】

1つの実施形態において、上述したような「サークル参加」動作は、装置1及び装置2の双方においてユーザ認証を必要とすることがある。このプロトコルが本明細書に記載されたリモート認証技術を使用して実装される場合、ユーザは、例えば、「サークル参加」処理を開始して完了するために双方の装置を認証するために指を「スワイプする」のを必要とすることがある。これに対して、1つの実施形態において、記載されたような装置間の同期データは、ユーザ認証を必要としない。

【0376】

本明細書に記載されたプロトコル及び関連する技術は、互いを信頼する装置のネットワークが構築されるのを可能とする。重要なことは、クラウドに送信され且つクラウドから送信されてクラウド内に記憶された全てのデータは暗号化される。したがって、データは、クラウド上にいかなる機密データも記憶することなく複数の装置間で同期させることができ、改善されたユーザのプライバシー保護をもたらす。

【0377】

上述した本発明の実施形態は、参加クラウド記憶装置が平文でユーザのデータのいずれかを表示することができない（すなわち、データはクラウドにおいて暗号化されている）装置同期のためのプライベート同期プロトコルを実装する。これらの実施形態は、以下を

10

20

30

40

50

含む様々な新規で有益な機能を含むが、これらに限定されるものではない。

- ・装置が他の装置を認証するための公開鍵及び秘密鍵を有する装置同期プロトコルを実装するためのシステム及び方法。

- ・同じサークル内の装置間の信頼関係を示すために信頼チェーンを実装するためのシステム及び方法。

- ・相互セッション鍵及びこれらの鍵によって暗号化データを生成するために装置が *D i f f i e - H e l l m a n* 又は類似の鍵交換アルゴリズムを使用するためのシステム及び方法。

- ・ *c i r c l e - i d* のハッシュが装置自体の代わりにサークルクラウドに記憶されているシステム及び方法。

- ・サークルクラウドがサークルのサークルチャンネル内にデータを置くのを許容する前に装置を認証するためにチャレンジレスポンスプロトコルを使用するシステム及び方法。

- ・持続的なサークルグループ鍵が同期データを暗号化するために使用されるシステム及び方法。

- ・複数の装置間でユーザのデータ（文書、ファイル、写真など）を共有するために記載されたプライベート同期プロトコルを使用し、クラウド上のデータの暗号化されたバックアップを記憶するアプリケーション。

- ・装置の秘密鍵（*d . p r i v*）及びこの鍵を使用する全ての動作がネットワークを介してユーザをリモート認証するために認証部内に実装されたシステム及び方法。

- ・ユーザの装置間で認証部の登録を共有するために新たな装置に対してユーザ制御の信頼委任を実行するために本発明の実施形態と組み合わせて記載されたプライベート同期プロトコルを使用するアプリケーション。

- ・新規登録が他の装置に委任されるたびにユーザが認証部によって認証する必要はない、ユーザの装置間の新規登録を共有するために新たな装置に対してユーザ制御の信頼委任を行うために本発明の実施形態と組み合わせて記載されたプライベート同期プロトコルを使用するアプリケーション。

- ・これらの認証部が同じサークルに属する他の認証部による単一の認証部の登録を共有するように認証鍵対を同期させるために、上述したプライベート同期プロトコルを使用している、同じユーザに属し且つサークルを形成する認証部のセット。

M. 例示的なシステムアーキテクチャ

【0378】

「信頼できる当事者」という用語は、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ことに留意すべきである。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。これらの区別は、「信頼できる当事者」が、ウェブサイト4631及び他のネットワークサービス4651のみならず、ウェブサイトやネットワークに代わって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4632-4633を含むことができることを示す、以下に述べられる図46A-Bにおいて指定される。

【0379】

特に、図46A-Bは、ユーザを認証するためのクライアント側と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つの実施形態を図示している。図46A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使用する一方で、図46Bに示される実施形態は、ブラウザを必要としない。本明細書に記載された様々な高度な認証技術及び関連するアプリケーションは、これらのシステムアーキテクチャのいずれかにおいて実装されることができる。例えば、上述したクライアン

10

20

30

40

50

ト装置における認証エンジン（例えば、230）は、インターフェース4602を含むセキュアトランザクションサービス4601の一部として実装されることができる。しかしながら、上述した実施形態は、図46A-Bに示されたもの以外のハードウェア及びソフトウェアのロジック構成を用いて実現されてもよいことに留意すべきである。

【0380】

図46A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4610-4612を備えたクライアント4600を含む。上述したように、認証装置4610-4612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ソフトウェア）、及び光学認識能力（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ソフトウェア）などの生体認証装置、並びにトラステッドプラットフォームモジュール（TPM）及びスマートカードなどの非生体認証装置を含むことができる。ユーザは、セキュアトランザクションサービス4601が（インターフェース4602を介して）セキュア記憶装置4620に生体認証テンプレートデータとして格納することができる生体認証データを提供する（例えば、指紋認証装置上で指をスワイプする）ことによって、生体認証装置に登録することができる。

【0381】

セキュア記憶装置4620は、認証装置4610-4612のセキュア周辺装置の外側に示されているが、1つの実施形態では、各認証装置4610-4612は、独自の統合セキュア記憶装置を有してもよい。更に、各認証装置4610-4612は、生体認証基準データレコードを暗号的に保護（例えば、記憶装置4620をセキュアにするため、データレコードをラッピング）してもよい。

【0382】

認証装置4610-4612は、セキュアトランザクションサービス4601によって露出されたインターフェース4602（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4601は、ネットワーク上で1つ以上のセキュアトランザクションサーバ4632-4633と通信し、ウェブブラウザ4604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4605とインターフェース接続するためのセキュア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4602はまた、装置識別コード、ユーザ識別コード、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）などの認証装置4610-4612のそれぞれに関連する情報と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鍵とを記憶するクライアント4600におけるセキュア記憶装置4620に対するセキュアアクセス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4630と通信するときに使用されることができる。

【0383】

装置の登録に加えて、セキュアトランザクションサービス4601は、その後、ネットワークを介してセキュアトランザクションサーバ4632-4633に生体認証装置を登録し、その後、登録処理中に交換されたデータを使用してこれらのサーバによって認証することができる（例えば、生体認証装置にプロビジョニングされた暗号化鍵）。認証処理は、本明細書に記載された認証技術のいずれかを含むことができる（例えば、明示的又は非侵襲型認証技術に基づいて、クライアント4600において保証レベルを生成し、セキュアトランザクションサーバ4632-4633に結果を送信する）。

【0384】

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4631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4605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 4630 の内部のウェブサーバ 4631（時として、単に「サーバ 4630」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 タグに回答して開始される。そのようなタグを検出することによって、セキュアランザクションプラグイン 4605 は、処理のために、セキュアランザクションサーバ 4601 に、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、セキュアランザクションサーバ 4601 は、内部設置ランザクションサーバ 4632（すなわち、ウェブサイトと同じ位置に配置された）又は外部設置ランザクションサーバ 4633 との直接の通信チャンネルを開くことができる。

10

【0385】

セキュアランザクションサーバ 4632－4633 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ランザクションデータベース 4640 に結合される。しかしながら、本発明の基本原理は、図 46A に示されるセキュア企業又はウェブデスティネーション 4630 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 4631 とセキュアランザクションサーバ 4632－4633 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 4631 及びランザクションサーバ 4632－4633 は、後述する機能を行うために 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。

20

【0386】

上述したように、本発明の基本原理は、図 46A 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 46B は、スタンドアロンアプリケーション 4654 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ランザクションサーバ 4601 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 4654 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ランザクションサーバ 4632－4633 に依存する 1 つ以上のネットワークサービス 4651 との通信セッションを確立するように設計されている。

30

【0387】

図 46A－B に示された実施形態のいずれかにおいて、セキュアランザクションサーバ 4632－4633 は、その後にセキュアランザクションサーバ 4601 に対してセキュアに送信され且つセキュア記憶装置 4620 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、セキュアランザクションサーバ 4632－4633 は、サーバ側のセキュアランザクションデータベース 4640 を管理する。

【0388】

認証装置が検出、登録、登録、認証を行うための例示的な一連のランザクションが図 47－51 に示されている。これらのランザクションのいくつかの態様は、上述した O S T P プロトコルにおいて使用されている（本明細書に組み込まれる追加の詳細については、O S T P フレームワーク（2011 年 3 月 23 日）を参照）。これらのランザクションの基本的な動作の理解は、本発明の実施形態を実施することができるコンテキストを提供する。

40

【0389】

以下に記載される動作は、認証装置の検出（図 47）、ユーザの認証装置による登録（図 48）、認証装置の登録（図 49）、登録された認証装置によるユーザ認証（図 50）、認証後のセキュアランザクションの実装（図 51）を含む。

【0390】

図 47 は、クライアント機器上で認証装置を検出するための一連のランザクションを図示している。装置の検出が成功裏に完了すると、サーバ 4730 は、クライアントに接

50

続されている認証装置に関する網羅的な情報を保有し、強化されたセキュリティインフラストラクチャを使用するのに最も適切である装置を評価することができるようになる。サーバ4730のみが認証装置のリストをフィルタリングする。ユーザは、このリストを備え、更なる認証及びセキュアトランザクションの実施のために使用するために認証装置のうちの1つ（又は組み合わせ）を選択することができる。

【0391】

動作において、ユーザは、ブラウザにおいてユーザ名とパスワードで認証し、ウェブサイトにログインする。これは、ユーザがユーザ名とパスワードを提供するために必要とされる唯一の時間である。サーバ4730は、（例えば、セキュアトランザクションデータベース4720をクエリすることによって）ユーザが強化されたセキュリティを現在使用していないと判定し、強化されたセキュリティに変更するようにユーザに提案を提供する。

10

【0392】

1つの実施形態において、サーバ4730は、セキュアトランザクションプラグイン4705が検出するHTMLページにおいて「装置のクエリ」タグを含む。タグの検出に回答して、セキュアトランザクションプラグイン4705は、その後に装置のセキュリティ特性を含むシステムに取り付けられた全ての認証装置に関する網羅的な情報を作成するセキュアトランザクションサービス4701に対してリクエストを再ルーティングする。1つの実施形態において、情報は、予め指定されたデータスキーマを使用して送信前にXML形式でパッケージ化される。

【0393】

セキュアトランザクションプラグイン4705は、セキュアトランザクションサービス4701からこの情報を受信し、1つの実施形態において、登録されたコールバックを介してウェブページのJavaScriptに情報を渡す。そして、それは、ブラウザ4704に情報を表示する方法を選択する。ウェブサイトによってフィルタリングされたリストは、ユーザに示されることができ、ユーザは、認証装置のうちの1つ又は組み合わせを選択することができる。

20

【0394】

図48は、認証装置によってユーザを登録する一連のトランザクションを図示している。1つの実施形態において、登録は、本明細書に記載された本発明の実施形態によって提供される強化されたセキュリティを使用するための前提条件である。登録は、同じ認証装置が後続のトランザクション中にユーザを認証するために使用することができるように、ユーザの生体情報読み取り値（例えば、指紋、音声サンプルなど）を取ることを含む。登録動作は、サーバ4730との相互作用なしに、クライアント上で単独に行うことができる。登録のために提供されるユーザインターフェースは、ブラウザの拡張機能において表示されることができ、又は、別個のアプリケーション若しくはモバイル装置アプリケーションにおいて表示されることができ。

30

【0395】

登録動作は、装置が検出されるとすぐに開始されてもよい。ユーザは、セキュリティを強化するために検出された装置のうちの1つ又はグループを使用することができる。動作において、ユーザは、ブラウザ、アプリケーション又はモバイル装置アプリケーションにおいて表示された装置リストから装置を選択することができる。図48に示されるブラウザベースの実装について、セキュアトランザクションプラグイン4705は、装置固有の登録グラフィカルユーザインターフェース（GUI）を表示する。セキュアトランザクションプラグイン4705は、セキュアトランザクションサービス4701に対して装置識別子及び登録要求を送信し、完了を待機する。ユーザが既にクライアントの認証装置に登録されている場合、ユーザは、自己の身元を確認する必要があるのみとすることができる（すなわち、それらは再度登録する必要はない）。ユーザが現在登録されていない場合、セキュアトランザクションサービス101は、（例えば、装置インターフェース4702を介して）物理的認証装置を活性化することによって登録処理を開始する。そして、ユーザは、セキュアトランザクションプラグイン4705のGUIと相互作用し、指定された

40

50

登録ステップに続く（例えば、指をスワイプする、マイクに向かって話す、画像をスナップするなど）。完了すると、ユーザは、認証装置に登録される。重要なことは、ユーザが装置に登録されると、それらは、本明細書に記載された任意のウェブサイト又はネットワークサービスに登録又は認証するためにこの登録を使用することができるということである。

【0396】

図49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4732-4733のうちの1つとの間で共有される。鍵は、クライアント4700のセキュア記憶装置4720、及びセキュアトランザクションサーバ4732-4733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4720内に格納される。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4732-4733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、後述する別の実施形態では、非対称鍵が使用されてもよい。この実施形態では、公開鍵は、セキュアトランザクションサーバ4732-4733によって格納されてもよく、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4720に格納されてもよい。更に、1つの実施形態（以下に同様に説明する）において、鍵は、（例えば、セキュアトランザクションサーバ4732-4733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4700上に生成されることができる。

【0397】

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通じてクライアントと鍵を共有するのに使用されてもよい（例えば、コメント要請(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も限定されるものではない。

【0398】

図49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認証が完了すると、サーバ4730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り得る。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4701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4730とのアウトオブバンドセッション（例えば、アウトオブバンドトランザクション）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4730と通信する。サーバ4730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4720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4720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4701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4730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。

【0399】

図50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4730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。

【0400】

ブラウザベースの実装を示す図50に示される特定の詳細を参照すると、ユーザは、ブラウザ4704においてサーバ4730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

できる。

【0401】

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4705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4720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4701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4701は、セキュアトランザクションプラグイン4705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 APIを呼び出し、サーバ4730(例えば、ウェブサイト)にこの情報を渡す。サーバ4730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、指紋リーダー上での指スワイプ、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4701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はこの情報を送信する。サーバ4730は、セキュアトランザクションデータベース4720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4730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。

10

20

【0402】

図51は、ブラウザベースの実装のためのセキュアトランザクションを図示している。セキュアトランザクションは、特定の種類のトランザクション(例えば、金融トランザクション)についての強力なセキュリティを提供するように設計されている。図示される実施形態では、ユーザは、トランザクションを委任する前に各トランザクションを確認する。図示された技術を使用して、ユーザは、彼／彼女が委任したいものを正確に確認し、彼／彼女がGUIに表示された見るものを正確に委任する。換言すれば、本実施形態は、ユーザが確認しなかったトランザクションを委任するためにトランザクションテキストが「中間者」によって変更されないことを保証する。

30

【0403】

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4705は、ブラウザコンテキスト内にウィンドウ5101を表示して、トランザクションの詳細を示す。セキュアトランザクションサーバ4701は、ウィンドウに表示されるテキストが誰かによって改竄されていないことを定期的に(例えば、ランダムな間隔で)検証する。

【0404】

以下の例は、この実施形態の動作を強調する助けとなる。ユーザは、マーチャントサイトから購入する品目を選び、「チェックアウト」を選択する。マーチャントサイトは、本明細書に記載する発明の実施形態のうち1つ以上を実装するセキュアトランザクションサーバ4732-4733を有する、サービスプロバイダ(例えば、PayPal)にトランザクションを送る。マーチャントサイトは、ユーザを認証し、トランザクションを完了する。

40

【0405】

セキュアトランザクションサーバ4732-4733は、トランザクション詳細(TD)を受信し、「セキュアトランザクション」要求をHTMLページに入れ、クライアント4700に送る。セキュアトランザクション要求は、トランザクション詳細及びランダムチャレンジ(例えば、ランダムナンス)を含む。セキュアトランザクションプラグイン4

50

705は、トランザクション確認メッセージの要求を検出し、全てのデータをセキュアトランザクションサービス4701に転送する。ブラウザ又はプラグインを使用しない1つの実施形態では、情報は、セキュアトランザクションサーバからクライアント4700上のセキュアトランザクションサービスに直接送られてもよい。

【0406】

ブラウザベースの実装について、セキュアトランザクションプラグイン4705は、（ブラウザコンテキスト内で）ユーザにトランザクション詳細を有するウィンドウ5101を表示し、トランザクションを確認するために認証を提供するようにユーザに要求する。ブラウザやプラグインを使用していない実施形態において、セキュアトランザクションサービス4701又はアプリケーション4754は、ウィンドウ5101を表示することができる。セキュアトランザクションサービス4701は、タイマを起動し、ユーザに対して表示されているウィンドウ5101の内容を検証する。検証期間はランダムに選ばれてもよい。セキュアトランザクションサービス4701は、ユーザがウィンドウ5101において有効なトランザクション詳細を見るのを保証する。コンテンツが改竄されていることを検出した場合、確認トークンが生成されるのを防止する。

【0407】

ユーザが有効な認証（例えば、指紋センサ上での指スワイプ）を提供した後、装置は、ユーザを識別し、トランザクション詳細やランダムチャレンジによってトークン（暗号化署名）を生成する（すなわち、トークンは、トランザクション詳細及びナンスにわたって計算される）。これにより、トランザクション詳細がサーバとクライアントとの間で変更されていないことを、セキュアトランザクションサーバ4732－4733が保証することを可能にする。セキュアトランザクションサービス4701は、セキュアトランザクションサーバ4732－4733にトークンを転送するセキュアトランザクションプラグイン4705に対して生成されたトークン及びユーザ名を送信する。セキュアトランザクションサーバ4732－4733は、ユーザ名によってユーザを識別し、トークンを検証する。検証が成功すると、確認メッセージがクライアントに送られ、トランザクションが処理される。

セキュアクエリのためのシステム及び方法

クライアント認証機能を判定するためのポリシー

【0408】

上述したように、本発明の1つの実施形態は、セキュアトランザクションサーバがサーバによって受け入れられた認証機能を示すクライアントに対してサーバポリシーを送信するクエリポリシーを実装する。そして、クライアントは、それがサポートする及び／又はユーザが使用する願望を示した認証機能のサブセットを識別するためにサーバポリシーを分析する。次に、クライアントは、提供されたポリシーに一致する認証トークンのサブセットを使用してユーザを登録及び／又は認証する。したがって、クライアントは、認証能力に関する網羅的な情報（例えば、その認証デバイスの全て）、又はクライアントを固有に識別するのに使用されるかもしれない他の情報を送信することを求められないので、クライアントのプライバシーに対する影響は少ない。

【0409】

例示として、限定されるものではないが、クライアントは、例を挙げると、指紋センサ、音声認識機能、顔認識機能、眼／光学的認識機能、信頼できるプラットフォームモジュール（TPM）及びスマートカードなどの多くの認証機能を含むことができる。しかしながら、プライバシー上の理由から、ユーザは、その能力の全てに関する詳細を要求サーバに対して明かすのを望まないことがある。このため、本明細書に記載する技術を使用して、セキュアトランザクションサーバは、例えば、指紋、光学的、又はスマートカード認証をサポートすることを示すサーバポリシーを、クライアントに送信してもよい。次に、クライアントは、サーバポリシーを独自の認証能力に対して比較し、利用可能な認証オプションのうち1つ以上を選んでよい。

【0410】

図52は、これらの技術を実装するためのクライアントー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4700に実装されたセキュアトランザクションサービス4701は、サーバ4730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5201を含む。1つの実施形態において、ポリシーフィルタ5201は、セキュアトランザクションサービス4701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則を順守しながら、ポリシーフィルタ5201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。

10

【0411】

図52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4730（単に「サーバ4730」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4705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4731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。このため、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5201を実装するセキュアトランザクションサービス4701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4705に提供される。

【0412】

ポリシーフィルタ5201は、クライアントのセキュア記憶領域5220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5220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）のレジス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5220内に記憶される。クライアントが既にサーバ4730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。

20

【0413】

セキュア記憶装置5220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5201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5201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をサポートし且つ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5201は、以下のサーバに対する一般的な認証機能の全体のサブセットを識別することができる：A、B及びC。あるいは、図52におけるユーザ嗜好5230によって示されるように、より高いレベルのプライバシーが所望される場合、認証機能のより限定されたサブセットがサーバに対して識別されることができる。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4700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。

30

40

【0414】

何の動作がサーバ4730（登録又は認証）によって開始されかに応じて、図52に示されるように、セキュアトランザクションサービス4730は、認証装置のフィルタリングされたサブセット（4710-4712）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4705を介してサーバ4730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4705の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4701からサーバ4730に対して直接送られ

50

てもよい。

【0415】

図53は、クエリポリシートランザクションを有する例示的な一連の登録についての追加の詳細を示すランザクション図を示している。図示された実施形態において、ユーザは、サーバ4730に装置を以前に登録していない。したがって、5301において、ユーザは、5302においてクライアントブラウザ4704を介してサーバ4730に転送される最初のワンタイム認証工程としてユーザ名とパスワードを入力することができる。しかしながら、ユーザ名及びパスワードは、本発明の基本原則を順守するために必要とされないことに留意すべきである。

【0416】

ユーザは、5303において判定されたように強化されたセキュリティに以前に登録していないことから、サーバ4730は、5304においてクライアントに対してそのサーバポリシーを伝送する。上述したように、サーバポリシーは、サーバ4730によってサポートされている認証機能の指示を含むことができる。図示された例において、サーバポリシーは、ランザクション5306を介してセキュアランザクションサービス4701に渡される。

【0417】

ランザクション5307において、セキュアランザクションサービス4701は、認証機能のフィルタリングされたリストに到達するために、クライアントの機能（及び上述したような装置の優先順位方式及び／又はユーザ選好などの潜在的に他の情報）とサーバポリシーを比較する。そして、装置（4702）のフィルタリングされたリストは、鍵（5308及び5309）を生成し、その後、登録応答としてその順番でこれらをサーバ4730に対して返送するセキュアランザクションサービス4701に対してこれらの鍵の公開部分を提供する。サーバは、認証装置を証明し、セキュアランザクションデータベース内に公開鍵を記憶する。ここで用いられるトークン証明は、登録中に、認証装置アイデンティティを有効化する処理である。それは、クライアントによって報告された装置が実際に主張されたものであることをサーバが暗号的に確認するのを可能とする。

【0418】

代替的に又は追加的に、5307において、ユーザは、リストを確認し及び／又はこの特定のサーバ4730で使用する特定の認証機能を選択する機会を提供することができる。例えば、フィルタリングされたリストは、指紋スキャン、顔認識及び／又は音声認識による認証を使用するための選択肢を示すことができる。次いで、ユーザは、サーバ4730による認証時にこれらの選択肢の1つ以上を使用するために選択することができる。

【0419】

クライアントにおいてサーバポリシーをフィルタリングするための上述した技術は、上述した一連のランザクションの様々な異なる段階（例えば、装置検出、装置登録、装置プロビジョニング、ユーザ認証などの際）で実施することができる。すなわち、本発明の基本原則は、図53に記載された特定のセットのランザクション及び特定のランザクションの順序に限定されるものではない。

【0420】

更に、上述したように、ブラウザプラグインアーキテクチャは、本発明の基本原則を順守するために必要とされない。ブラウザ又はブラウザプラグイン（例えば、スタンドアロンアプリケーション又はモバイル装置のアプリケーションなど）をとまなうアーキテクチャについて、図53に示されるランザクション図（及び本明細書に開示されたランザクション図の残りは、ブラウザ4704が削除され、セキュアランザクションサービス4701がサーバ4730と直接通信するように簡略化することができる。

複数の認証装置によって効率的に登録、登録、

及び認証するためのシステム及び方法

【0421】

本発明の1つの実施形態は、複数の装置を同時に登録、登録及び認証することができ、

10

20

30

40

50

それによって効率及びユーザ体験を向上させることができる。例えば、一度に単一の装置についての登録及び認証を要求する代わりに、装置のリストがクライアントに送信されることができる。そして、対称又は非対称鍵は、1つの動作又はクライアント上でローカルに実行される一連のシーケンシャル動作において複数の装置に登録されることができる。認証のために、いくつかのトークン／装置は、特定のトランザクションのために同時に選択されることができる。

【0422】

図54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。図示されるように、クライアント4700に実装されたセキュアトランザクションサービス4701は、各装置が登録／登録されるときにサーバ4730との継続的な往復通信を必要とすることなく、一度に複数の装置の登録及び登録などの指定された動作を実行するための複数装置処理ロジック5401を含む。同様に、サーバ4730は、複数の認証装置に向けてコマンドを発行するための複数装置処理ロジックを含む。1つの実施形態において、複数装置処理ロジック5401は、セキュアトランザクションサービス4701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、複数装置処理ロジック5401は、更に本発明の基本原則を順守し且つソフトウェア、ハードウェア若しくはファームウェア構成要素又はそれらの任意の組み合わせを含むことができながら、任意の方法で実装されることができることに留意すべきである。

【0423】

上述した実施形態のように、図54に示される特定の実装は、（上述したように、ウェブサーバ4731及びセキュアトランザクションサーバ4732－4733を含むことができる）サーバ4730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4705を含む。それゆえに、サーバ4730は、セキュアトランザクションプラグイン4705を介してセキュアトランザクションサービス4701と通信する。上述したように、しかしながら、ブラウザベースのプラグインアーキテクチャは、本発明の基本原則を順守する必要はない。

【0424】

サーバ4730における複数装置処理ロジック5402は、複数の認証装置4710－4712において動作を実行するクライアント4700における複数装置処理ロジック5401によって実行されるコマンドを通信することができる。例示として、複数装置処理ロジック5402は、N個の認証装置のそれぞれに登録されるためにN個の鍵を生成することができる。その後、N個の装置に登録するためのコマンドとともに複数装置処理ロジック5401にセキュアに送信することができる。そして、複数装置処理ロジック5401は、サーバとの更なる相互作用なしで、N個全ての装置について（例えば、認証装置4710－4712について）同時に又は一連のシーケンシャルな動作において登録を行うことができる。そして、単一の応答は、N個全ての装置の登録完了を示すためにサーバ4730に送信されることができる。

【0425】

例示的な複数の装置の一連のトランザクションが図55A－Cに示されている。図55Aは、サーバ4730とのいかなる相互作用もなしで行うことができる複数装置の登録処理を図示している（例えば、認証装置にユーザを登録することは、クライアントにおけるセキュアトランザクションサービス4701の制御下で行うことができる）。代替の実施形態において、サーバ4730は、N個の装置にユーザを登録するためにクライアント（図示しない）に要求を送信することができる。図55B－Cは、サーバ4730に複数の装置に登録するための2つの異なる実施形態を図示している。

【0426】

図55Aにおける登録処理を参照すると、5501において、ユーザは、（利用可能な認証装置の全て又はサブセットを表す）クライアントにおけるN個の認証装置に登録する意欲を示す。これに応答して、セキュアトランザクションプラグインは、5502におい

10

20

30

40

50

て呼び出され、5503において、認証装置#1に処理又は登録することによってユーザが歩行するように装置固有のグラフィカルユーザインターフェース（GUI）が生成される登録処理の間、ユーザは、示されるように（例えば、指紋センサ上で指を配置すること、マイクに向かって発話すること、カメラで写真をスナップすることなどによって）セキュアトランザクションプラグインと相互作用する。1つの実施形態において、5504において、登録がN番目の装置について完了するまで、N個の装置のそれぞれについて登録が行われる。異なる装置固有のスクリプト及び／又はユーザインターフェースは、個々の認証装置にユーザを登録するためにユーザに提示されることができる。上述したように、ユーザが各装置に登録するのにともない、ユーザ登録データは、クライアント4700におけるセキュア記憶装置720内に記憶されることができ、セキュアトランザクションサービス4701を介してのみアクセス可能とされることができる。N個全ての装置の登録が完了すると、通知がトランザクション5504－5505を介してサーバ4730に送信されることができる。

【0427】

登録が行われる方法にかかわらず、完了すると、サーバ4730にN個の装置を登録するために図55Bに示されるトランザクション図が使用されることができる。5510において、サーバ4730は、上述したように、時間の制限されたウィンドウについてのみ有効であるとしてでき且つ暗号化ナンスなどのランダム生成コードを含むことができるユーザ固有のランダムチャレンジを生成する。5511において、サーバ4730にN個の認証装置を登録するためにコマンドとともにランダムチャレンジが送信される。5512において、セキュアトランザクションサービス4701は、サーバ4730とのセキュア接続を形成し、ランダムチャレンジとともにN個の装置についての識別データを送信する。1つの実施形態において、セキュア接続は、HTTPS接続である。しかしながら、本発明の基本原理は、いかなる特定のセキュア接続種類に限定されるものではない。

【0428】

5513において、サーバ4730は、N個の装置を証明し、N個の装置のそれぞれについての鍵を生成し、セキュア接続を介してセキュアトランザクションサービスにN個の鍵を返送する。1つの実施形態において、セキュア接続を介してクライアントと鍵を交換するために動的対称鍵プロビジョニングプロトコル（DSKPP）が使用される。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技術に限定されるものではない。あるいは、DSKPPプロトコルに依存しない実施形態において、鍵は、各認証装置において生成されてもよく、そしてサーバ4730に送信されてもよい。

【0429】

5514－5515において、セキュアトランザクションサービスの複数装置処理ロジックは、N個の装置のそれぞれにN個の鍵のそれぞれを登録する。上述したように、各鍵は、クライアントのセキュア記憶装置720内に記憶され、その各装置に関連付けられることができる。登録が各認証装置について完了すると、5516において、通知がセキュア接続を介してサーバに送信される。

【0430】

1つの実施形態において、各認証装置に登録された鍵は対称鍵である。それゆえに、各鍵の同一のコピーは、クライアントにおけるセキュア記憶装置720及びサーバ4730におけるセキュアトランザクションデータベース4720に記憶される。代替の実装において、非対称鍵対が生成されてもよく、鍵の1つがサーバにおけるセキュアトランザクションデータベース4720内の公開鍵及びクライアントのセキュア記憶装置720に記憶された秘密鍵として維持される。しかしながら、本発明の基本原理は、暗号化鍵の任意の特定の種類に限定されるものではないことに留意すべきである。

【0431】

サーバ4730よりもむしろクライアントにおいて鍵が生成される代替の実装が図55Cに示されている。この実装において、5511においてランダムチャレンジを有する装置を登録するための要求を受信した後、セキュアトランザクションサービス4701の複

数装置処理ロジックは、1120において、N個の装置のそれぞれについてN個の鍵を生成する。生成されると、鍵は、5513-5514においてN個の装置のそれぞれに登録され、登録は上述したようにセキュア記憶装置720内に記憶される。全ての鍵が登録されると、セキュアトランザクションサービス4701は、(クライアントの身元を検証するために)ランダムチャレンジとともに5515においてサーバに通知を提供する。そして、サーバ4730は、上述したように、セキュアトランザクションデータベース4720に登録を記憶することができる。

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

【0432】

本発明の1つの実施形態は、ランダムチャレンジがサーバによって生成されて処理される方法を改善する。1つの実施形態において、ランダムチャレンジは、暗号化ナンスとしてのランダム生成コードを含む。現在のシステムにおいて、サーバがクライアントにランダムチャレンジを送信した後、クライアントが指定されたタイムアウト期間内に応答しない場合には、ランダムチャレンジはもはや有効でなく、クライアントは、その後の認証試行に応答してエラーを受信する(例えば、ユーザは、指紋リーダー上で指をスワイプして拒否される)。

【0433】

本発明の1つの実施形態において、クライアントは、チャレンジが満了したことを自動的に検出し、サーバから新たなチャレンジを透過的に要求する(すなわち、ユーザの介入なしに)。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。

【0434】

図56Aは、登録処理のコンテキスト内で使用される1つのそのような実施形態を図示し、図56Bは、認証処理のコンテキスト内で使用される実施形態を図示している。しかしながら、本発明の基本原理は、図56A-Bに示されるもの以外のコンテキスト内で使用されてもよいことに留意すべきである。例えば、本明細書に記載された技術は、時間に敏感なコードがサーバからクライアントに通信される任意の処理で使用することができる。

【0435】

最初に図56Aを参照すると、5601において、サーバ4730は、ランダムチャレンジ及びタイムアウト期間の指示を生成する。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4730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4730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4701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。

【0436】

タイムアウト期間が指定される又は計算される方法にかかわらず、5602において、ランダムチャレンジ及びタイムアウト指示が(図示された例においてはブラウザ4704及びセキュアトランザクションプラグイン4705を介して)セキュアトランザクションサービス4701に送信される。5603において、セキュアトランザクションサービス4701は、ランダムチャレンジがタイムアウトしたことを検出し、サーバ4730から送信されたタイムアウト指示に基づいてもはや有効ではない。例示として、ユーザは、一

連のトランザクションを完了する前に、彼／彼女のクライアント機器をオフにすることができ、又は、彼／彼女のノートブックコンピュータの蓋を閉じることができる。トランザクションがユーザの相互作用を必要とするものである場合、ユーザは、単に離れて歩くか又はG U I内に表示されたメッセージを無視することができる。

【0437】

5604において、ランダムチャレンジがもはや有効でないことを検出すると、セキュアトランザクションサービス4701は、(図示された例においてはセキュアトランザクションプラグイン4705及びブラウザ4704を介して)サーバ4730に対して新たなランダムチャレンジの要求を送信する。5605において、サーバ4730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指示を生成する。1つの実施形態において、タイムアウト期間は、動作5601と同じであるか又は変更されることができる。例えば、サーバ4730は、クライアントによってデータトラフィックを低減するために又はランダムチャレンジによって提供されるセキュリティのレベルを増加させるために時間を低減させるためにタイムアウト期間の持続時間を増加させることができる。5606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4701に送信される。

【0438】

トランザクションの残りの部分は、上述したように発生する。例えば、セキュアトランザクションサービスは、図49、図55B又は図55Cに関して上述したように、装置登録及び鍵交換を行うために、5607においてサーバに対して直接セキュア接続を開く。5608において、サーバ4730は、(例えば、ユーザ名又は他のIDによって)ユーザを識別し、認証装置を証明し、装置についての鍵を生成する。上述したように、鍵は、対称鍵又は非対称鍵とすることができる。5609において、鍵はセキュア接続を介してセキュアトランザクションサービス4701に送信され、5610において、セキュアトランザクションサービス4701は、認証装置に鍵を登録する。5611において、登録が完了した通知がサーバ4730に送信される。

【0439】

それゆえに、図56Aに示される実施形態において、装置登録に使用される鍵は、図55Bに示される実施形態のようにサーバ4730において生成される。しかしながら、本発明の基本原理はまた、図55Cに関して上述したように、クライアント4700におけるセキュアトランザクションサービス4701によって鍵が生成される実施形態において使用することができる。

【0440】

図56Bは、認証処理のコンテキスト内で実装される本発明の1つの実施形態を図示している。5651において、ユーザは、ブラウザ4704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4732-4733を含む企業／ウェブデスティネーションサーバ4730内のウェブサーバ4731に向けられる。5652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4701は、5653において、サーバ4730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4700におけるセキュア記憶装置720をクエリする。5654において、サーバ5654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、5655において、セキュアトランザクションサービス4701にこの情報を返送する。

【0441】

5656において、セキュアトランザクションサービス5656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。上述したように、タイムアウト期間の終了を指示して検出するために、様々な異なる技術が使用されることができる(図56A及び関連するテキストを参照)。5657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4701は

、透過的に（すなわち、ユーザの介入なしで）サーバ４７３０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、５６５８において、サーバ４７３０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、５６５９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４７０１に送信される。

【０４４２】

図５６Ｂ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５０を参照）。例えば、５６６０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）、５６６１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）。５６６２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。５６６３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４７３０に送信される。最後に、５６６４において、サーバ４７３０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４７２０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４７２０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。

認証フレームワーク内でプライバシークラスを処理するためのシステム及び方法

【０４４３】

１つの実施形態において、プライバシー保護の複数のクラスは、エンドユーザによって事前に定義、選択及び／又は変更されることができる。プライバシークラスは、漏洩情報を用いてクライアントが識別されることができる確率に基づいて定義されることができる。比較的高いプライバシーレベルを有するプライバシークラスにおいて、クライアント装置に関する比較的小さい情報は、本明細書に記載された認証技術を実行するために公表される。１つの実施形態において、ユーザは、異なるサーバと通信するときに可能な最小量の情報を開示するために選択することができる（すなわち、各ウェブサイト又はネットワークサービスに影響を与える最低許容プライバシーを有するトランザクションを選択することができる）。

【０４４４】

図５７は、プライバシークラスを実装するための高レベルのアーキテクチャを図示している。図示されたように、本実施形態のセキュアトランザクションサービス４７０１は、認証装置に関連する情報などのクライアント情報についてサーバ４７３０から受信したクエリを分析し、そのようなクエリに回答してプライバシーポリシーを実行し、使用中の特定のプライバシークラスに基づいて収集されたクライアント情報を含む応答を生成するためのプライバシー管理ロジック５７０１を含む。１つの実施形態において、プライバシー管理モジュール５７０１は、セキュアトランザクションサービス４７０１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則を順守しながら、プライバシー管理モジュール５７０１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。

【０４４５】

プライバシー管理ロジック５７０１によって利用されるプライバシークラスは、クライアント４７００において事前に指定されて記憶されることができる（例えば、セキュア記憶装置５７２０内に記憶される）。１つの実施形態において、３つのプライバシークラスが定義される：高いプライバシーへの影響、中間のプライバシーへの影響及び低いプライバシーへの影響。各プライバシークラスは、漏洩情報がユーザ／クライアントを固有に識別するために使用することができた確率に基づいて定義することができる。例えば、低い

プライバシー影響トランザクションについての脆弱な情報は、インターネットを介して一意に識別されるユーザ又はマシンの10%の確率をもたらすことができる。中程度のプライバシー影響トランザクションは、一意に識別されるユーザ又はマシンの50%の確率をもたらすことができ、高いプライバシー影響トランザクションは、ユーザ又はマシンが一意に識別される100%の確率をもたらすことができる。更に本発明の基本原則を順守しながら、様々な他のクラスのプライバシーレベルが定義されることができる。

【0446】

1つの実施形態において、各信頼できる当事者（例えば、各ウェブサイト4731又はサービス4751）は、必要なプライバシークラス又は他のプライバシーの閾値を指定することができる。例えば、セキュリティのレベルの高まりを必要とするウェブサイト及びサービスは、高いプライバシー影響クラスに応じて通信するのを可能とすることができるのみであるのに対して、他のウェブサイト／サービスは、中間プライバシー影響又は低いプライバシー影響クラスを使用して相互作用を許可することができる。1つの実施形態において、サーバ4730から送信されたクライアント情報のクエリは、取得されるべきである情報のプライバシークラスを指定する（すなわち、低、中、高）属性を含む。それゆえに、プライバシー管理ロジック5701は、各信頼できる当事者についての最高の承認プライバシークラスの情報を記憶する。1つの実施形態において、信頼できる当事者が既に承認されたものよりも高いプライバシークラスに属する情報を要求するたびに、ユーザは、この信頼できる当事者についてのこの新たなプライバシークラスを恒久的に承認（又は拒否）するように求められる。ユーザの承認に回答して、プライバシー管理ロジックは、（例えば、URLを介して識別される）信頼できる当事者と新たなプライバシークラス間の新たな関連付けを記憶することができる。

【0447】

ユーザ嗜好5730は、単純化のために図57におけるプライバシー管理ロジックに直接適用されているが、ユーザは、ブラウザベースのグラフィカルユーザインターフェース（図示しない）を介して嗜好を指定することができることに留意すべきである。そのような場合、ユーザは、ブラウザウィンドウを介してプライバシー設定を入力する。そして、セキュアトランザクションプラグイン4705は、プライバシー管理ロジック5701に対して又はプライバシー管理ロジック5701によってアクセス可能な設定データファイルに対して新たな設定を記憶する。要するに、本発明の基本原則は、プライバシー管理ロジックを構成するための特定の機構に限定されるものではない。

【0448】

様々な種類のクライアントデータは、例えば、機器モデル識別子、クライアントソフトウェア情報、クライアント機能及びクライアント装置上に構成された各認証装置に関連する様々なレベルの情報（例えば、装置IDコード、ベンダーIDコード、装置クラスIDなど）を含む様々なプライバシークラスレベルで指定することができる。この情報の異なる組み合わせは、異なるプライバシークラスを定義する上で特定のパーセンテージを決定するために収集されてもよい。

【0449】

図58は、定義されたプライバシークラスを使用して要求者に対して情報を提供するための一連のトランザクションを図示している。5801において、サーバ4730は、クライアント装置情報についてのクエリを含む通知を生成する。5802において、クエリがクライアントに送信され、最終的にセキュアトランザクションサービス4701によって受信される。5803において、セキュアトランザクションサービスのプライバシー管理ロジックは、応答についてのプライバシークラスを判定し、必要な情報を収集する。上述したように、N個の異なるプライバシークラスレベルが定義されることができ、セキュアトランザクションサービス4701は、クライアントに関するできるだけ少ない情報を同時に漏洩しながら要求者の要件に適合するものを選択することができる。5804において、収集された情報は、サーバ4730に送信され、5805において、サーバは、クライアントによる1つ以上の後続のトランザクションのために情報を使用する。

トランザクション署名を使用して認証フレームワークをインプラントするためのシステム及び方法

【0450】

本発明の一実施形態は、クライアントとのセッションを維持するのに、いかなるトランザクション状態もサーバ上で維持する必要がないように、セキュアトランザクションサーバにおいてトランザクション署名を用いる。特に、トランザクションテキストなどのトランザクション詳細は、サーバによって署名されたクライアントに送信されることができる。次に、サーバは、クライアントが受信した署名付きトランザクション応答が有効であることを、署名を検証することによって検証してもよい。サーバは、トランザクションの内容を持続的に格納する必要はなく、それにより、多数のクライアントのために相当量の格納スペースが消費され、サーバに対するサービス種類攻撃の拒否の可能性が開かれる。

10

【0451】

クライアント4700とのトランザクションを開始するウェブサイト又は他のネットワークサービス(5901)を示す本発明の1つの実施形態が図59に示されている。例えば、ユーザは、ウェブサイト上で購入する品目を選択していてもよく、チェックアウトし支払う準備ができていてもよい。図示される例では、ウェブサイト又はサービス5901は、(本明細書に記載するように)署名を生成して検証するための署名処理論理5903と、(例えば、上述した認証技術を使用して)クライアント認証5904を実行するための認証論理とを含むセキュアトランザクションサーバ5902に、トランザクションをハンドオフする。

20

【0452】

1つの実施形態では、セキュアトランザクションサーバ5902からクライアント4700に送られる認証要求は、(上述したような)暗号化ナンスなどのランダムチャレンジと、トランザクション詳細(例えば、トランザクションを完了するために提示される特定のテキスト)と、(セキュアトランザクションサーバによってのみ知られている)秘密鍵を使用して、ランダムチャレンジ及びトランザクション詳細を通じて署名処理論理5903によって生成される署名とを含む。

【0453】

上記情報がクライアントによって受信されると、ユーザは、認証がトランザクションを完了するために必要とされるという指示を受信することができる。これに回答して、ユーザは、例えば、指紋スキャナにわたって指をスワイプするか、画像をスナップするか、マイクロフォンに向かって発話するか、又は所与のトランザクションに対して許可された他の任意の種類の認証を行ってもよい。1つの実施形態では、ユーザが認証装置4700によって成功裏に検証されると、クライアントは：(1)ランダムチャレンジ及びトランザクションテキスト(両方とも、サーバによってクライアントに以前提供されたもの)、(2)ユーザが成功裏に認証を完了したことを証明する認証データ、並びに(3)署名を、サーバに返送する。

30

【0454】

次に、セキュアトランザクションサーバ5902上の認証モジュール5904は、ユーザが適正に認証されていることを確認してもよく、署名処理論理5903は、秘密鍵を使用して、ランダムチャレンジ及びトランザクションテキストを通じて署名を再生成する。署名がクライアントによって送られたものと一致した場合、サーバは、トランザクションのテキストがウェブサイト又はサービス5901から最初に受信したときのものと同じであると検証することができる。セキュアトランザクションサーバ5902は、セキュアトランザクションデータベース4720内にトランザクションのテキスト(又は他のトランザクションデータ)を持続的に記憶するのに必要でないため、記憶及び処理リソースは保存される。

40

カノニカル認証システム

【0455】

IT革新の数年後であっても、パスワードは、依然として最も広く使用されている認証

50

方法である。しかしながら、ユーザ又はサービスプロバイダのいずれも、適切にパスワードを処理しておらず、この形態の認証を本質的に安全ではなくしている。一方、1億超の信頼済みプラットフォーム（TPM）及び15000万個を超えるセキュアエレメントが出荷されており、マイクロフォン及びカメラは、最もスマートフォン及び指紋センサに統合され、信頼できる実行環境（TEE）が上昇している。パスワード又はワンタイムパスワード（OTP）よりも良好な認証方法が存在する。

【0456】

2007年では、平均ユーザは、25個のアカウントを有し、6.5個のパスワードを使用し、ログインを1日に8回行った。今日では、事柄は非常に悪い。600万個のアカウントの分析は、10,000個の共通のパスワードがアカウントの30%へのアクセスを有することを示した（Burnett、2011年）。銀行アカウントのパスワードを見る場合であっても、ユーザの73%が、そのオンラインバンクパスワードを少なくとも1つの非金融サイトと共有していることを見出し（Trusteer, Inc.、2010年）、これは、非バンクサイトがハッキングされたときにバンクアカウントが脅かされていることを意味する。

10

【0457】

認証、異種認証、及び信頼できるクライアント環境を含む、パスワードを置き換えるためのいくつかの提案がなされてきた。

【0458】

認証のサイロ：現在の代替技術は、それぞれの独自のサーバ技術を必要とする。したがって、現在の認証アーキテクチャは、認証方法、関連するクライアント実装、及び関連するサーバ技術を含む、サイロからなる。

20

【0459】

研究コミュニティによって提案される革新的な認証方法は、クライアント実装に加えて、完全なサーバソフトウェアが実装及び展開される必要があるため、広く展開されていない。より良好なユーザ検証方法のための競争を有する代わりに、認証企業は、最良のサーバ技術のための闘いに直面している。

【0460】

異種認証：ユーザは、スタンドアロンPC、タブレット又はスマートフォンを使用して認証することができる。従業員は、いくつかの装置を制御することができる一方で、他は、ユーザによって制御されることができる（David A. Willis, Garner、2013年）。モバイルデバイス及びBYOD傾向の増大した採用は、ますます不均質な認証ランドスケープにつながる。全ての必要性を満たす1つの認証方法には、到達していないと思われる。

30

【0461】

信頼できるクライアント環境：クライアント側マルウェアは、パスワード又はOTPを捕捉して開示することができる。それは、表示された後に確認されるトランザクションを変更することができ、又は認証された通信チャンネルを悪用して意図しないアクションを実行することができる。認証—ユーザ名及びパスワードによるものであっても、クライアント側で少なくとも1つの信頼できる構成要素を必要とする。

40

【0462】

今日では、パスワード又はOTPベースの認証の代替は、スケーリングしていない。これは、主に、認証構築ブロックの最適な組み合わせに起因する。この制限に対処するために、本発明の1つの実施形態は、様々な異なる方法で実装されることができるカノニカル構築ブロックを特定し、既存のプラットフォーム機能内での統合に好適な一周知の機能的認証システムを更にもたらす。

【0463】

パスワードに対する最近の大規模攻撃は、全てサーバ側に集中していた。そのような攻撃は、努力及びユーザが取るセキュリティ対策から独立している。図60に示される攻撃分類では、これらの攻撃は、（1）によってラベル付けされる。この単一の脅威クラスに

50

対する保護手段の導入は、ユーザ（２－３）をなりすまし、認証セッション（４）を模倣することを含む、ユーザデバイス（２－４）から認証資格情報を盗んで悪用する攻撃に対して攻撃者の焦点を移す可能性が非常に高い。項目（５）及び（６）は、ユーザのデバイスの物理的盗難と、データの盗用（５）及び／又はユーザのなりすましのためのデバイスの悪用を含む。しかしながら、攻撃は、いくつかの種類のスケール変更可能な攻撃、すなわち、いくつかの固定コストを有する攻撃であるが、多数の販売可能な物品の潜在性に焦点を合わせる可能性が非常に高い。個々のデバイスを物理的に攻撃することは可能であるが、スケーラブルではない。

【０４６４】

本発明の１つの実施形態では、比較的低いエントロピーを有するハッシュされたパスワードを記憶する代わりに、非対称の公開鍵がサーバ上に記憶されることができ、関連する秘密鍵は、機器内に記憶されることができる。所与の公開鍵から秘密鍵を計算することは、ファクタリング（RSA）を必要とするか、又は離散的な対数問題（DSA／ECDSA）を解くことを必要とするため、非常にリソースを消費する。秘密鍵は、マルウェア攻撃に対して少なくとも保護されるべきである。１つの実施形態では、これは、クライアント装置上の信頼できる実行環境（TEE）又はセキュアエレメント（SE）を使用して達成される。

【０４６５】

ほとんどのクライアント装置が常にオンラインであることを前提として、秘密鍵を抽出する代わりに、マルウェアは、単にそれを悪用するように試みることができる。このような攻撃から保護するために、（a）鍵を使用するアクセスは、適格なアプリに限定されるべきであり、（b）マルウェアによってエミュレートすることができないいくつかの種類のユーザ対話が必要とされる。TrustedUI（Global Platform、2013年）を使用して、このような種類のユーザ対話を実施することができる。セキュアエレメントは、典型的には、ユーザインターフェースを有さず、したがってこの種類の保護を提供しないことに留意されたい。

【０４６６】

上述の保護手段を実施するとき、認証はセキュアである。しかしながら、攻撃者は、認証セッションを制御するアプリの攻撃に焦点を当ててもよい。既存のPC感染率（APWG、2014年）は、これらの種類の攻撃の実現可能性を実証する。現在のモバイルアプリよりも高い保護を有する認証部を有する場合、この認証部は、特定のトランザクションのユーザの確認を表示及び取得するために使用することができる。そのような場合、感染したアプリは、（a）ユーザによって拒絶されるであろう悪意のあるトランザクション、又は（b）署名後に修正される署名されたトランザクションをもたらすことができる。これは、TrustedUI実装のための第2の使用事例である。

【０４６７】

１つの実施形態では、物理的鍵抽出を保護するために、セキュアエレメントが使用される。SEの基礎となるチップハードウェアは、典型的には、物理的攻撃に対する最新の保護対策を実施する。（Dr. Sergei Skorobogatov, University of Cambridge、2011年）。更に、１つの実施形態では、物理的ユーザ対話の必要性を満たすために、指紋センサなどのTrustedUI又は他の専用のユーザ検証ハードウェアが使用されてもよい。

【０４６８】

攻撃者がデバイスへの物理的アクセスを獲得する場合、攻撃者は、それを抽出する代わりに鍵を悪用することを試みることができる。このような攻撃から保護するために、低い他人受入率、良好ななりすまし方法、及び抗ハンマー機構を有する有効なユーザ検証方法が使用される（すなわち、潜在的な総当たりの試みの数を効果的に制限するために）。

【０４６９】

スケーラブルな攻撃が優勢であることを考慮すると、１つの実施形態は、スケーラブルな攻撃の対策を実施した後に、物理的攻撃の対策に焦点を当てている。

【0470】

クライアント側の証明のための良好な保護は有益であるが、実際には、遠隔パーティ（すなわち、サーバ側）も、使用されるセキュリティを理解することに関心がある。その結果、本発明の1つの実施形態は、遠隔サーバに対するクライアント側セキュリティ特性を「証明する」。有効であるために、これらの証明技術は、クライアント側保護と少なくとも同じ強度である必要がある。

【0471】

実際の解決策では、証明のプライバシーも重要である。直接匿名証明（DAA）などの方法は、良好な選択である。残念ながら、元のDAA法は、標準的なハードウェアに実装された場合には遅すぎた。改善されたペアリングベースのDAAスキームは、はるかに速い。TPMv2のTCG（Liqun Chen, HP Laboratories及びJiangtao Li, Intel Corporation、2013年）が採用されている。

10

【0472】

典型的な署名は、アプリによって制御される、署名されたオブジェクトと、秘密鍵を使用して計算された署名とからなる。そのため、検証部にとって、署名対象オブジェクトのデータは、アプリが署名対象オブジェクトのコンテンツを制御している場合と同じくらい信頼できるものである。

【0473】

図61に示されるように、1つの実施形態では、秘密鍵6105は、アプリ6101よりも信頼できる、証明された認証部6102によって保護される。認証部は、（例えば、ユーザが本明細書に記載されるような確認のテキストを確認することを可能にするために）トランザクション確認構成要素6109と、（例えば、生体認証又は他の種類のユーザ認証を可能にするために）ユーザ検証構成要素6106を含むことができる。1つの実施形態では、証明モジュール6103は、秘密鍵6105を使用して、認証部属性及びアプリケーションデータを含むオブジェクト上に署名6108を生成して署名されたオブジェクト6107を生成する。図示されるように、1つの実施形態では、署名されるオブジェクトは、認証部及びアプリケーションデータの証明された属性の連結を含む。署名されたオブジェクトで使用される属性は、例えば、（a）ユーザによって確認されるトランザクションテキスト、（b）最小PIN長とは対照的な実際の個人識別番号（PIN）長、又は（c）認証部実装のファームウェアバージョンを含むことができる。

20

30

【0474】

図示された実装は、（アプリ6101に付与される代わりに）鍵6105の排他的制御が認証部6102に付与されるため、既存のシステムよりもセキュアである。1つの実施形態では、認証部6102によって排他的に制御される、署名されたオブジェクトは、アプリ6101によって制御されるデータのために予約された「スロット」を有する（図61において「アプリデータ」として識別される）。その結果、この実施形態では、アプリ6101は、任意の形態の、署名されたオブジェクトを任意に作成することを許可されない。各署名されたオブジェクトは類似しているため、信頼できる当事者6110のオブジェクト検証モジュール6111は、信頼された属性が信頼された認証部6102によって寄与されたことを信頼することができる。1つの実施形態では、オブジェクト検証モジュール6111は、認証部6102に関連付けられた公開鍵及びメタデータ6112（例えば、認証部タイプ、モデル及び／又はバージョン）を使用して、署名6108を検証する。

40

【0475】

1つの実施形態では、図61に示されるような認証システムを組み立てるために使用され得る1組のカノニカル構築ブロックが定義される。特定の組の構築ブロックは、以下を含む。

1. 暗号化鍵を生成し、そのような鍵をリモートパーティに証明するためのハードウェア及び／又はソフトウェア。

2. 試験された署名を生成するためのハードウェア及び／又はソフトウェア。

50

3. ユーザを検証するためのハードウェア及び／又はソフトウェア。

4. エンティティに鍵をバインドする（例えば、定義されたソフトウェアアプリケーションのセットへのそのような鍵の「使用」アクセスを制限する）ハードウェア及び／又はソフトウェア。

【0476】

全ての構築ブロックが存在する必要はない。構築ブロック#1のみを使用して、認証システムを構築することができる。必要に応じて、他の構築ブロックを追加することができる。全体的なセキュリティ特性及び有用性特性は、使用される構築ブロックの特定の実装に依存する。

【0477】

図62は、クライアント側認証部6201、クライアント側プラットフォーム6202（例えば、Android OS又はWindows OSを使用するモバイルデバイス）、リモート当事者6203及びメタデータ6304を含む、1つの特定の実施形態を図示している。認証部6201の1つの実施形態は、認証鍵を生成し、リモート当事者6203に対する認証鍵の証明をサポートする。上述のものを含む様々な証明方法がサポートされる。FIDO基本証明（Rolf Lindemann、Davit Baghdaryan 及びEric Tiffany、2014年）、DAA（Ernie Brickell, Intel Corporation; Jan Camenisch, IBM Research; Liqun Chen, HP Laboratories、2004年）、ECDAA（Ernie Brickell, Intel Corporation; Jiangtao Li, Intel Labs）。

【0478】

リモート当事者は、証明オブジェクトを検証するために使用するメタデータ6204へのアクセスを有する。認証部は、物理的に別個のエンティティ（例えば、暗号化SDカード、USB暗号トークンなど）として実装されてもよいが、クライアント側プラットフォーム（例えば、埋め込まれたセキュアエレメント、TPM、TEE）に物理的に埋め込まれてもよい。

【0479】

認証部6201は、必要に応じて、ユーザを検証する能力を有してもよい。しかしながら、本発明の基本原理は、いかなる特定のユーザ検証方法にも限定されない。しかしながら、リモート当事者は、証明オブジェクト及びメタデータ6204を見ることによって、ユーザ検証方法を学習することができる。

【0480】

本発明の実施形態は、任意の特定のワイヤプロトコル又はプロトコルメッセージを符号化に依存しない。唯一の要件は、証明オブジェクト及び証明された署名オブジェクトなどの認証部6201によって生成されるアサーションは、リモート当事者6203によって「理解される」必要があるということである。具体的なワイヤの形態は、特定のプラットフォームに依存することができる。

【0481】

このセクションは、これらのカノニカル構築ブロックをどのように使用することができるかについての第1の印象を与えることを意図している。

【0482】

現在の認証フレームワークでは、FIDO UAF仕様では、クライアントは非常に「重い」。本明細書に記載される手法により、クライアントは、（1）プロトコル関連タスク（プラットフォームに実装するにはあまりにも具体的すぎる）の全てを実行するアプリケーションソフトウェア開発キット（App SDK）と、（2）鍵をソフトウェアアプリケーションのセットにバインドするなどのセキュリティ関連タスクを実装するプラットフォーム機能と、の2つの部分に容易に分割することができる。このアプローチでは、別個のエンティティであるFIDOクライアントなどのクライアントは消える。

【0483】

10

20

30

40

50

以下は、これらのカノニカル構築ブロックを支持するように拡張されたAndroidプラットフォーム上に実装されるFIDO UAFの例である。

【0484】

AttestationType：それを明示的に設定する必要はない。Android Appsは全て、Android-Attestation法（例えば、FIDO App SDKを介して）のみを使用することができることを知っている。

【0485】

AAID：認証部のそれぞれのクラスの一意の識別子（例えば、上述の「認証部証明ID」）。1つの実施形態では、AAIDは、鍵を作成するときに指定されたユーザ検証方法を使用して、Android KeyStore実装に低減される。KeyStoreは、ユーザ検証方法（及びそれ自体のKeyStore暗号実装に関する静的知識）に基づいて、AAIDを調べる。

【0486】

ユーザ名：1つの実施形態は、（App SDKを介して）モバイルアプリがKey Aliasをkey IDの連結及び存在する場合はユーザ名に設定することを可能にする。

【0487】

App ID：app ID結合（支持される場合）を用いて対処される。

【0488】

要約すると、本発明の1つの実施形態は、クライアント側認証部をリモート当事者に対して認証するためのシステムを含み、システムは、以下を含む：

（1）（i）暗号化鍵ペア（「認証鍵」）を生成する回路及び／又はプログラムコードと、（ii）鍵生成エンティティの識別情報をリモート当事者に証明する回路及び／又はプログラムコードと、を含む、クライアント側認証部。

（2）リモート当事者に利用可能に作成された証明を検証するために十分な情報を少なくとも含む、認証部に関するデータ。このデータは、上記「メタデータ」と称される。

（3）生成された認証秘密鍵を使用して暗号化動作を実行して、秘密認証鍵を所有することをリモート当事者に証明するための暗号化動作を実行する回路及び／又はプログラムコード。

【0489】

更に、認証部は、認証秘密鍵の使用を制限して、署名されたオブジェクトのみに明確に定義された暗号署名動作を実行することが知られている場合がある。この署名されたオブジェクトは、認証部によって制御されるデータフィールドと、任意のデータ（認証部によって制御されない）を含むように明確にマークされた1つ以上のデータフィールドとを含む。認証部は、それらをマジック数MNで開始し、その後、明確に定義されたデータ構造で開始することによって、そのようなオブジェクトを示すことができる。この署名動作は、本明細書では「証明された署名」と呼ばれる。このマジック数MNは、自由に選択されることができ、固定され、周知である必要がある。このマジック数を設定する方法の一例は、「ATTESTED_SIGNATURE」である。

【0490】

更に、1つの実施形態では、クライアント側認証部は、任意のユーザ検証方法を使用してユーザを検証する能力を有し、このユーザ検証方法の特性は静的であり（すなわち、任意の認証部について経時的に変化しない）、メタデータに記載されている。ユーザ検証方法は、任意に複雑であってもよく、複数の生体認証及び非生体認証（例えば、PIN又は指紋、PIN／指紋と組み合わせた発話者認識、顔認識など）から構成されてもよい。

【0491】

更に、1つの実施形態では、（a）鍵は、証明された署名のためにのみ使用されてもよく、（b）認証部は、ユーザ検証方法の特性が認証部によって制御されるデータフィールド（例えば、証明された署名）に記載されているユーザ検証方法を使用してユーザを検証する能力を有する。ユーザ検証方法は、任意に複雑であってもよく、複数の生体認証及び非生体認証（例えば、PIN又は指紋、PIN／指紋と組み合わせた発話者認識、顔認識

10

20

30

40

50

など) から更に構成されてもよいことに留意されたい。

【0492】

1つの実施形態では、プライベート認証鍵6105へのアクセスは、指定されたアプリケーションのセットに限定される。更に、セットは、プラットフォーム（例えば、オペレーティングシステム）によって同等とみなされる用途に制限されてもよい。一例として、認証鍵へのアクセスは、鍵生成をトリガしたアプリケーションと同じパッケージ署名鍵を使用して署名されたアプリケーションに、オペレーティングシステムによって制限されてもよい。更に、アプリケーションのセットは、同等であるとみなされるアプリケーションファセットのリストを介して、アプリケーション開発者によって同等であると考えられるアプリケーションを含んでもよい。

10

【0493】

更に別の実施形態では、認証部6102は、トランザクションテキストをセキュアに表示し、この特定のトランザクションを確認する（又は拒否する）ためにユーザに尋ねることをサポートする。トランザクションテキストは、証明された署名に暗号的に結合されてもよい（すなわち、トランザクションテキストの暗号ハッシュは、認証部によって制御されるフィールドのうちの1つに含まれる）。

【0494】

本発明の1つの実施形態は、プラットフォーム（例えば、OS又はウェブブラウザ）上のFIDO UAF/U2Fスタック（認証部に属していない）のセキュリティ関連タスクを実装し、他のプロトコル処理タスクの実装をアプリに残すことによって、プラットフォーム内に特定のプロトコルを実装する必要性を除去する（すなわち、FIDOクライアントを有する必要性を除去する）。

20

トランザクション確認及び暗号通貨実装のためのセキュアな鍵ストアを使用するシステム及び方法

【0495】

上述のセキュア記憶装置3725などのセキュアな鍵ストアのための既存のインターフェースは、暗号署名を計算する際に、任意のデータを更新方法に渡すことを可能にし、署名対象のオブジェクトの制御を完全にコーリングアプリケーションに残す。このような更新された方法の一例は、以下のURLで説明され、AndroidプラットフォームのJava実装を説明する）：[https://developer.android.com/reference/java/security/Signature.html#update\(byte\[\]\)](https://developer.android.com/reference/java/security/Signature.html#update(byte[]))

30

【0496】

データは、（例えば、信頼できる実行環境において）「KeyMaster」と呼ばれる場合があるモジュール内に実装される署名アルゴリズムによって解釈される。このデータは、典型的には、署名鍵に関連付けられた特定のハッシュアルゴリズム（例えば、SHA256を楕円曲線デジタル署名アルゴリズムを用いて使用するときのSHA256）を使用してハッシュされる任意のデータであると予想される。

【0497】

この手法は、「あなたが見るものはあなたが署名するものである（what you see is what you sign）」（WYSIWYS）の実装では、署名されているオブジェクトの信頼が、オペレーティングシステムのアプリケーションレベル（例えば、Android実装のAndroid OS アプリレベルなど）に制限されるため、困難である。WYSIWYSは、望ましくないトランザクションを署名する際に、攻撃者がユーザをだますことを防止するため、重要なセキュリティ機能である。この問題に関連する更なる詳細は、以下の参考文献に見出すことができる：

40

<https://pdfs.semanticscholar.org/15ce/5b7ae2118cb1ab47b66392e0a565ae969f43.pdf>
<http://www.sciencedirect.com/science/article/pii/S0167404898800058>

50

`https://pdfs.semanticscholar.org/b52c/726fab56bb7f929e8c6b11112afd78db359.pdf`
【0498】

参照により本明細書に組み込まれる以下の文献は、本明細書に記載される本発明の実施形態に有用な背景を提供する。

`https://fidoalliance.org/specs/fido-v2.0-rd-20170927/fido-client-to-authenticator-protocol-v2.0-rd-20170927.html` (Client-to-Authプロトコル、V2.0)

`https://www.w3.org/TR/webauthn` (ウェブ認証仕様)

`https://tools.ietf.org/html/rfc7049` (RFC 7049、「CBOR」)

【0499】

図63は、上記の制限に対処する装置6300の1つの実施形態を図示している。例示的な装置は、(例えば、本明細書に記載される技術を使用して)ユーザ認証を実行するための、鍵マスタ6310及び鍵マスタ拡張部6311を介してアクセス可能なセキュア鍵ストア6320を含む。鍵マスタ及び鍵マスタ拡張部は、認証部6100を形成する。本発明の1つの実施形態は、以下のように構築される新たな(導出された)ハッシュ関数を実装する：

`KM_DIGEST_WEBAUTHN_SHA256`

【0500】

a. 1つの実施形態では、入力データ6301は、機能`authenticatorGetAssertion`についてRFC7049に記載されているように、簡潔バイナリオブジェクト表現(CBOR)を使用してフォーマットされる。フィールド「拡張部」は、上述のウェブ認証仕様に記載されているような`txGeneric`拡張部を含むことができる。

【0501】

b. その拡張部が含まれる場合、鍵マスタ実装6310は、信頼できる実行環境(TEE)の`TrustedUI`機能を使用して6302でコンテンツを表示し、鍵マスタ拡張部6311を使用してトランザクションを認可するようにユーザに尋ねる。ユーザがトランザクションに同意し、ユーザが6303で肯定的に検証された場合にのみ、認証部6100は、鍵マスタ6310機能を使用して関連する応答に署名する。

【0502】

c. 次に、鍵マスタ実装6310は、6312でウェブ認証仕様にしたがって、最終的な署名されたオブジェクトを生成し、そのSHA256ハッシュを計算する。

【0503】

d. 6313において、最終的な楕円曲線デジタル署名アルゴリズム(ECDSA)署名がこのハッシュ上で計算される。

【0504】

1つの実施形態では、鍵は、このハッシュアルゴリズムと併せてのみ使用することができる。そのため、不要なトランザクションを表すことができる任意のハッシュ値を盲検的に符号化することはない。

【0505】

この実施形態は、特定の入力及び出力機能の文脈内で説明されているが、本発明の基本原理は、この特定の実施に限定されない。1つの実施形態では、同様の動作を行うが、ビットコイン入力/出力機能を使用する。図64は、例えば、ビットコイン形式入力メッセージ6401を図示している。次に、鍵マスタ実装6410は、信頼できる実行環境(TEE)の`TrustedUI`機能を使用して6402でコンテンツを表示し、ユーザに、ビットコイントランザクションを認可することを確認する。ユーザが同意し、ユーザが正に検証された場合にのみ、認証部6100は、関連する応答に署名する。次に、鍵マ

10

20

30

40

50

スタ実装 6 4 1 0 は、6 4 1 2 で最終署名されたオブジェクトを生成し、その S H A 2 5 6 ハッシュを計算する。次いで、6 4 1 3 において最終的な E C D S A 署名をハッシュ上で計算する。

【0 5 0 6】

上記の実施態様には多くの利点がある。例えば、基本 O S の主要な変化は必要ではなく、方法ごとに 1 つの追加の K M _ D I G E S T _ * 及びハッシュアルゴリズムを追加する必要がある。T E E のセキュリティ及び T r u s t e d U I 機能の進歩は、アプリベンダーにとって活用されて容易に利用可能となり得る。

【0 5 0 7】

更に、鍵ストアに実装された既存のハードウェア鍵証明技術は、活用することができる。これにより、信頼できる当事者は、下にあるセキュリティの強い指示を提供する。最後に、ユーザは、トランザクションを実際に認可／署名する前に、正しいトランザクション及びユーザ承認を表示するためにシステムを信頼することができる。

F I D O 及びウェブ認証の仮想 R P I D

【0 5 0 8】

F I D O 認証は、信頼できる当事者 (R P) を用いて認証するために使用され得る。したがって、R P によって登録された認証部を使用することができる。認証プロトコルは標準化されているが、追加の認証部を登録するプロセスは独自である。更なる認証部を登録するための標準化された A P I を提供するために、R P の臨界質量を期待することは、現実的ではない。本発明の実施形態は、追加の認証部を登録するための標準化された方法としてブロックチェーンの使用を提供する。

【0 5 0 9】

F I D O 及びウェブ認証は、アプリケーション I D (F I D O の A p p I D) 又は信頼できる当事者 I D (ウェブ認証における R P I D) によって信頼できる当事者に認証鍵 (公開鍵資格ソース) を接続する。ブロックチェーンの世界では、台帳自体は、ユーザ (公開鍵によって表される) と、台帳コンテンツを評価し得る任意の信頼できる当事者との間の仲介として機能する。結果として、公開鍵作成時に、鍵が使用される信頼できる当事者／複数の当事者の名前はまだ知られていない。グローバル相関ハンドルの問題を回避するために、ユーザは、複数の鍵ペアを生成し、単一の鍵ペア (又は更には複数の鍵ペア) を、1 つの特定の信頼できる当事者又は独自の裁量における信頼できる当事者の特定のセットとともに使用することができる。

【0 5 1 0】

本発明の実施形態は、F I D O 世界に構成された「仮想 R P I D」の技術を提供し、それによって、F I D O 認証部をブロックチェーンの文脈で使用することを可能にする。特に、F I D O クライアントは、A p p I D を検証するエンティティである。同様に、ウェブ認証において、「プラットフォーム」(すなわち、ウェブブラウザ又はオペレーティングシステム)は、R P I D を検証するエンティティである。

【0 5 1 1】

本発明の 1 つの実施形態は、特定の構文の「仮想」A p p I D / R P I D を作成するための、F I D O クライアント／プラットフォームのためのプロセス及びアーキテクチャを含む (例えば、d i d : / / 3 4 5 6 9 8 7 6 a f 7 6 8 c 7 e 7 9 7 3 2 4) 。そのような「仮想」A p p I D / R P I D は、任意のドメイン名サービス (D N S) 内の既存のエントリに依存しない。更に、任意の仮想 A p p I D / R P I D は、h t t p 及び h t t p s とは異なる関連プロトコル名を有する。そのような「仮想」A p p I D / R P I D は、「仮想」A p p I D / R P I D を非一元的識別子 (D I D) として使用するブロックチェーン内の特定のエントリを指す。

【0 5 1 2】

図 6 5 は、認証エンジン 3 7 1 0 によって作成されて管理された「仮想」A p p I D / R P I D (例えば、F I D O クライアントと一体化された)を含む記録 6 5 0 1 を有する例示的なデバイス 6 5 0 0 を図示している。D I D レコード 6 5 0 1 に含まれる仮想 I

10

20

30

40

50

Dは、本明細書に記載されるように、信頼できる当事者6503と関連付けられてそれとの認証に使用される。

【0513】

1つの実施形態では、複数の「仮想」AppID/RPID6502は、相関ハンドルを有さないエンティティとの共有を回避するために作成される。DIDレコード6501は、複数の公開鍵記録を含んでもよく、それらのそれぞれは、公開鍵及び／又は「失効日」に対する証明ステートメントを含むことができる。新しい公開鍵レコードがそのようなDIDレコード6501に追加された場合、ブロックDIDレコードチェーンは、新しい公開鍵レコードが、記録されたに含まれるいくつかの既存の公開鍵記録に関連する秘密鍵によって署名されることを検証する。失効日でエントリを追加する場合、関連する公開鍵は、この日付の後に信頼されない。

10

【0514】

更に、本発明の1つの実施形態は、認証のために、信頼できる当事者6503にDIDレコード6501を導入する。この「登録」プロセスでは、信頼できる当事者(RP)6503は、署名されたナンス(例えば、FIDO及びウェブ認証署名アサーション形式のいずれかで)DID6501を識別子として返す、装置6500にナンスを送信する。登録応答を検証するとき、信頼できる当事者6503は、公開鍵が関連するDID6501に正しく属することを確認し、証明ステートメントは、信頼できる当事者6503の要件(例えば、十分なセキュリティ)を実際に満たすことを確認する。

【0515】

記録に属する各公開鍵記録は、DID6501によって表される特定の「仮想」AppID/RPIDに登録された認証部を表す。これにより、ユーザは、ユーザが認証部を追加、組み合わせ、又は除去することを可能にするために、それぞれのRPが同じプロトコルを実装することを必要とせずに、異なるRPの認証部を管理する標準化された方法を提供する。

20

【0516】

「ブロックチェーン」は、近年、顕著な注意を受けた比較的新しい概念である。最もよく知られているブロックチェーンは、ビットコインで使用されるものであるが、例えば、イーサリアムを含む他のものがある。一般に、ブロックチェーンは、一体にリンクされ、暗号的に固定されるレコード(「ブロック」)のセットを連続的に増加させる。各ブロックは、それを以前のブロック、関連するトランザクションデータ、及びタイムスタンプにリンクするポインタを含んでもよい。

30

【0517】

ほとんど全てのブロックチェーン技術は、追加されるデータの公開鍵署名を必要とする。これは、本質的に、公開鍵に関連付けられたアイデンティティをもたらす。関連する秘密鍵の正当な所有者のみが、この秘密鍵で署名を作成することが可能であると想定される。例えば、ビットコインでは、公開鍵は、関連するビットコイン「貨幣」の「所有者」であり、関連する秘密鍵へのアクセスを有する人が所有者であることを成功裏に請求することができることを意味する。秘密鍵が失われると、関連する「貨幣」が失われ、盗まれた場合、「貨幣」は、他の誰かによって請求されることができる。

40

【0518】

イーサリアムのような現代のブロックチェーン(<https://www.ethereum.org/>)は、スマート契約などのより一般的な概念をサポートする。このような構成では、収縮利益は公開鍵に結び付けられ、影響は、ビットコインに類似しており、すなわち、鍵が収縮利益を盗まれた場合には、他の誰かによって請求されることができる。

【0519】

その結果、秘密鍵をセキュアに記憶するために、有意な強調が置かれる。この必要性を満たすために、いくつかの企業は、その顧客の代わりにそのような秘密鍵を維持する(例えば、ビットコイン鍵の「ビットコインアカウントサービス」)。他には、Mt. Gox BitX、サークル、及びコインベースが挙げられる。そのような中央サービスは、盗難

50

者にとって理想的な標的であり、実際にMt. Goxがハッキングされた。代替的な実施例は、ローカル「ウォレット」を含む。それらのうちのいくつかは、リッチオペレーティングシステム上で実行される「ソフトウェア」で実装され、他はハードウェアトークン内に実装される。

【0520】

残念ながら、この段階では、公開鍵に関連する秘密鍵が、ハードウェアトークン内で強く保護されるか、又はある程度の「ソフトウェア」ウォレットで弱く保護されているかどうかを破棄する方法は存在しない。これはまた、ビットコインアカウントサービスのユーザが、それらの鍵をどのくらい良好に保護しているか、及び署名を作成する前に、どのような種類のユーザが鍵のニーズとどのように相互作用するかを証明しないことも意味する。すなわち、ユーザが、「あなたが見たものがあなたが署名するもの(What-you-see-is-what-you-sign)」特徴、及びどのように実装されているかに依存し得る。より一般的には、ビットコイン、イーサリアム、及び他のブロックチェーンにおけるそのような鍵の証明の概念は存在しない。

10

【0521】

本発明の1つの実施形態は、秘密鍵のセキュリティを文書化するために、本明細書に記載される認証部証明ステーションを使用する。具体的には、1つの実施形態では、記載された認証部アーキテクチャを使用して、以下の使用事例を実施することができる。

【0522】

1. 電子金銭の分配は、特定のセキュリティ特性を有する「ウォレット」に限定される。これは、例えば、秘密鍵を保護するための信頼された実行環境を使用するウォレット又は他のセキュアな記憶装置のみを含むことができる。

20

【0523】

2. トランザクションは、ユーザが、例えば、あなたが見たものがあなたが署名するもの(What-you-see-is-what-you-sign)などの技術を用いて認証部上のトランザクションを明確に確認した場合にのみ承認される。

【0524】

3. ユーザは、サービスを使用するとき(例えば、ビットコインアカウントサービスを使用した場合)、自分の秘密鍵がどのくらい強く保護されているかを検証することができる。

30

【0525】

このような使用事例は、弱いウォレットに起因する驚くべきことを回避し、また、非評判のような概念を支援するのに役立つ。

これらのシナリオにおけるユーザの秘密鍵の改善された保護を提供するために、本発明の1つの実施形態は、そのようなブロックチェーン概念に対する認証のために、認証部、認証部証明書及びメタデータステートメントを導入する。具体的には、1つの実施形態では、「ブロックチェーン認証部」は、上述の認証部(FIDO認証部を含む)と同様の方法で使用されるが、(FIDOアサーションなどのアサーションに加えて)特定のブロックチェーンメッセージを署名するための追加のサポートとともに使用される。

【0526】

40

証明書は、公開鍵が最初に導入されたときにブロックチェーンに追加されているデータブロックのために、証明ステートメントを追加することができる。そのような証明ステートメントの例としては、FIDO UAF認証装置コマンド、2017年2月のFIDOアライアンス実装ドラフト02、セクション5.2(TAG__UAFV1__REG__ASSERTION)及びセクション4.2(登録応答メッセージ)、並びに2017年8月のウェブ認証：公開鍵資格レベル1にアクセスするためのAPI、W3Cワーキングドラフト11、セクション5.3.4(証明オブジェクトの生成)に定義されるものが挙げられる。

【0527】

1つの実施形態では、証明ステートメントは、(1)任意の個人データを含まず、(2)

50

）署名によって一体に保護されるので、証明ステートメントは、ブロックの一部（例えば、特別なメッセージタイプとして）であってもよく、（１）が任意の個人データを含まず、（２）が署名によって一体に保護される。１つの実施形態では、ブロックチェーンサポート（例えば、ビットコイン、イーサリアム、．．．）を指定するために、認証部に関連するメタデータステートメントに指示が追加される。更に、ブロックチェーンブロックタイプは、認証機能（例えば、ビットコイン署名スクリプト）を参照するために使用され得る。

【０５２８】

図６６は、図６１に関して前述したいくつかの特徴を再現している。しかしながら、この特定の実装では、証明モジュール６１０３は、ブロックチェーンに追加された新しいブ
ロック６６０８を含む署名されたオブジェクト６６０７を、秘密鍵で生成された署名６６
０９とともに生成する。１つの特定の実装では、署名対象のオブジェクトはまた、１つ以
上の証明された属性６６１１を含むことができる。前述したように、署名されるオブジェ
クトは、認証部６１０２及びブロック６６０８の証明された属性６６１１の連結を含むこ
とができる。署名されたオブジェクト内で使用される証明された属性６６１１は、例えば
、（ａ）ユーザによって確認されるトランザクションテキスト、（ｂ）最小ＰＩＮ長とは
対照的な実際の個人識別番号（ＰＩＮ）長、又は（ｃ）認証部６１０２のファームウェア
バージョンを含むことができる。特に明記しない限り、図６６の他の構成要素は、図６１
に関して上述したように実質的に動作する。

例示的なデータ処理デバイス

【０５２９】

図６７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６７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。

【０５３０】

図６７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６７
００は、処理システム６７２０に結合されているバス（複数可）６７５０と、電源６７２
５と、メモリ６７３０と、不揮発性メモリ６７４０（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）を含む。バス（複数可）６７５０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６７２０は、メモリ６７３０及び／又は不揮発
性メモリ６７４０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６７５０は、上記構成要素を一体に相互接
続し、また、任意のドック６７６０、ディスプレイコントローラ及びディスプレイ装置６
７７０、入力／出力装置６７８０（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）６７９０（例えば、ブルートゥース、Ｗｉ
Ｆｉ、赤外線など）にそれらの構成要素を相互接続する。

【０５３１】

図６４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６４００は、ハンドヘル
ドコンピュータ、パーソナルデ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６４００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。

【０５３２】

10

20

30

40

50

本発明の1つの実施形態によれば、データ処理システム6400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6400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6420を含む。処理システム6420は、メモリ6410、（1つ以上のバッテリーを含む）電源6425、オーディオ入力／出力6440、ディスプレイコントローラ及びディスプレイ装置6460、任意の入力／出力6450、入力装置（複数可）6470及び無線送受信機（複数可）6430に結合されている。図64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6400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64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64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。

10

【0533】

メモリ6410は、データ処理システム6400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ことができる。音声入力／出力6440は、例えば、音楽を再生するための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装置6460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6430（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つ以上の入力装置6470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してすることができる。任意の他の入力／出力6450は、ドック用コネクタとすることができる。

20

【0534】

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。

30

【0535】

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。

【0536】

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。

40

【0537】

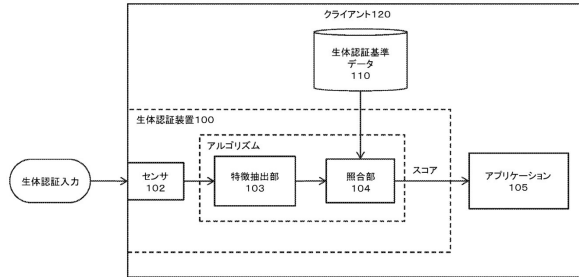
上述したように、本発明の実施形態は、様々な工程を含んでもよい。工程は、汎用又は

50

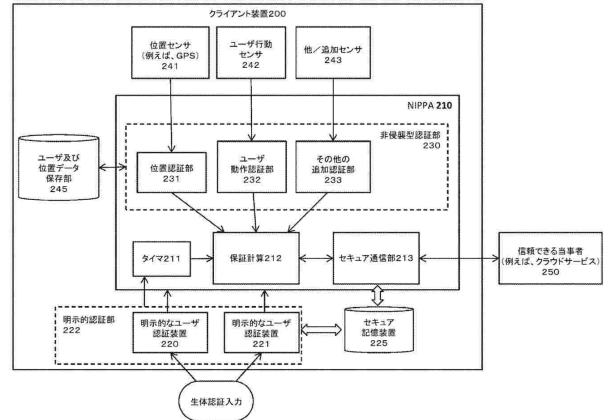
特殊目的のプロセッサに特定の工程を実行させる機械実行可能な命令で具現化され得る。代替的に、これらの工程は、工程を実行するためのハードワイヤードロジックを含む特定のハードウェア構成要素によって、又はプログラミングされたコンピュータ構成要素及びカスタムハードウェア構成要素の任意の組み合わせによって、実行することができる。

【図面】

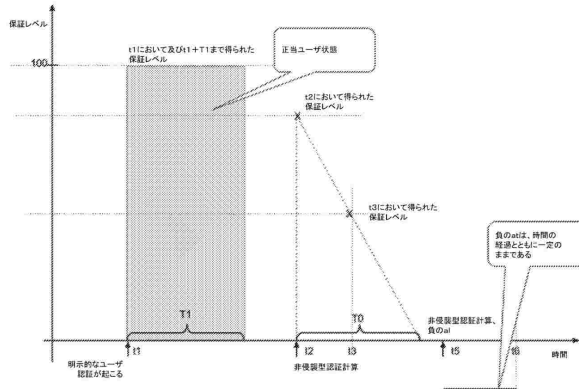
【図 1】



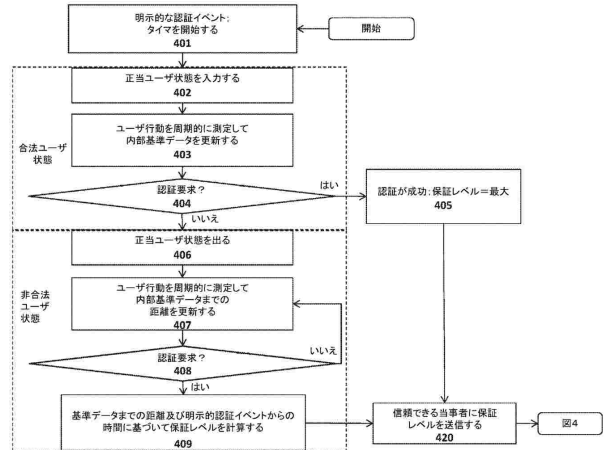
【図 2】



【図 3】



【図 4】



10

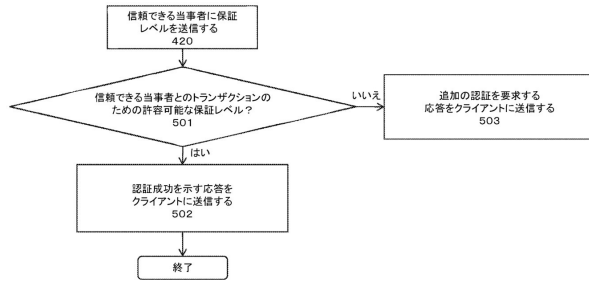
20

30

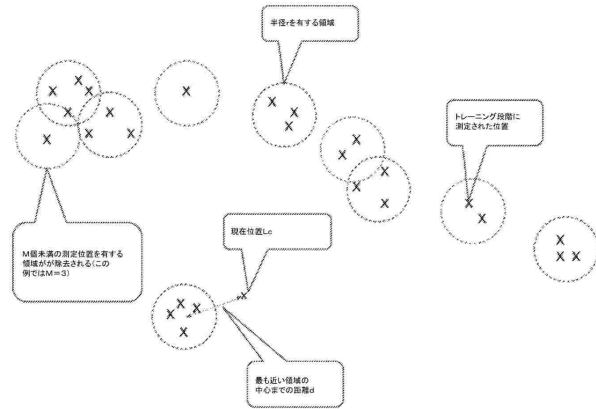
40

50

【図 5】

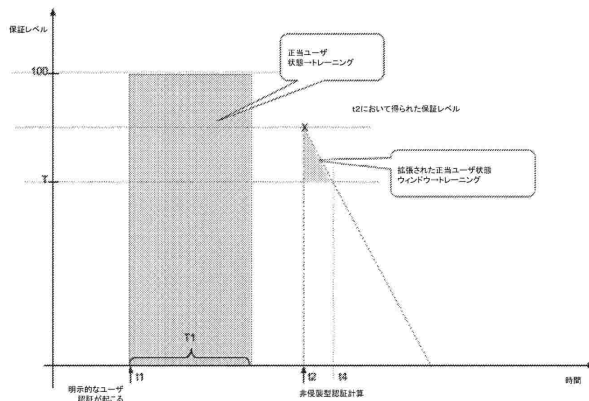


【図 6】

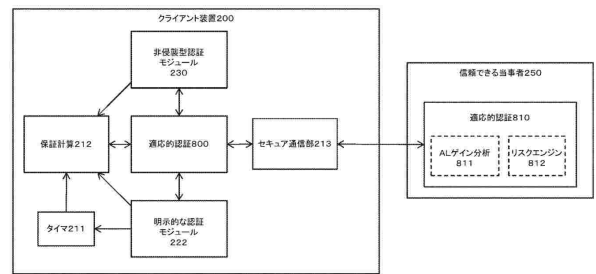


10

【図 7】



【図 8】



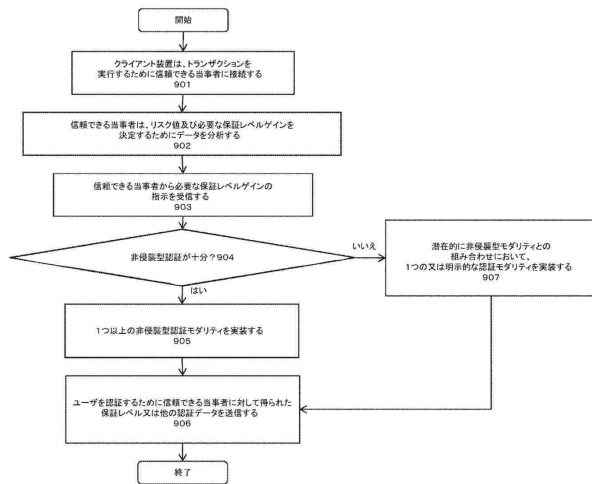
20

30

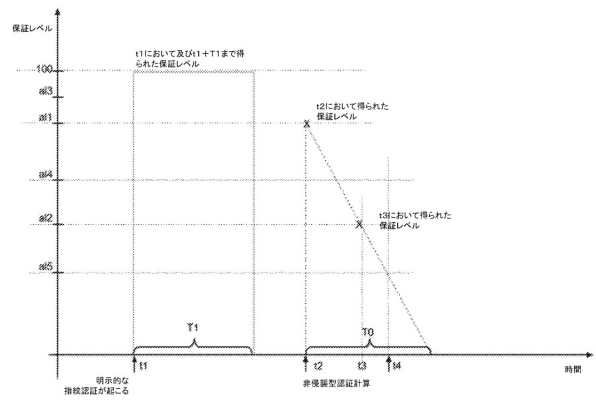
40

50

【図 9】

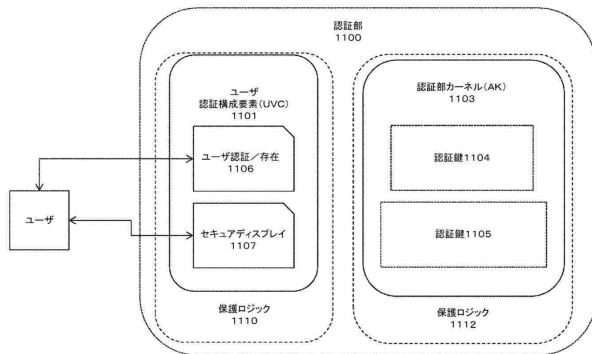


【図 10】

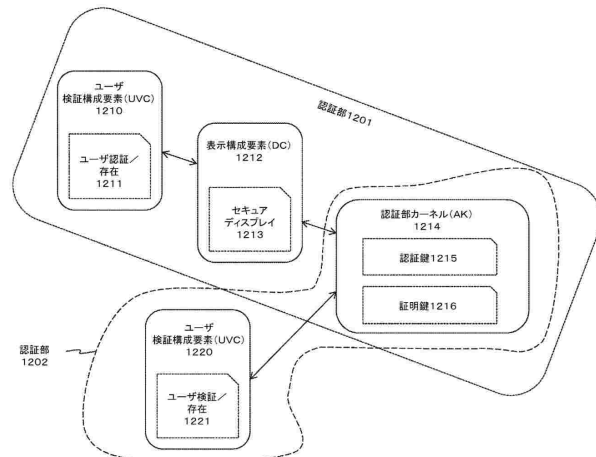


10

【図 11】



【図 12】



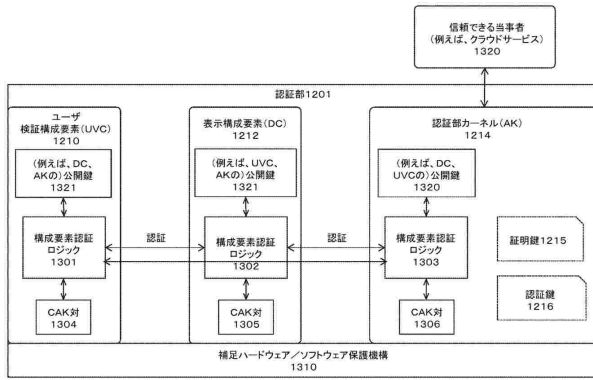
20

30

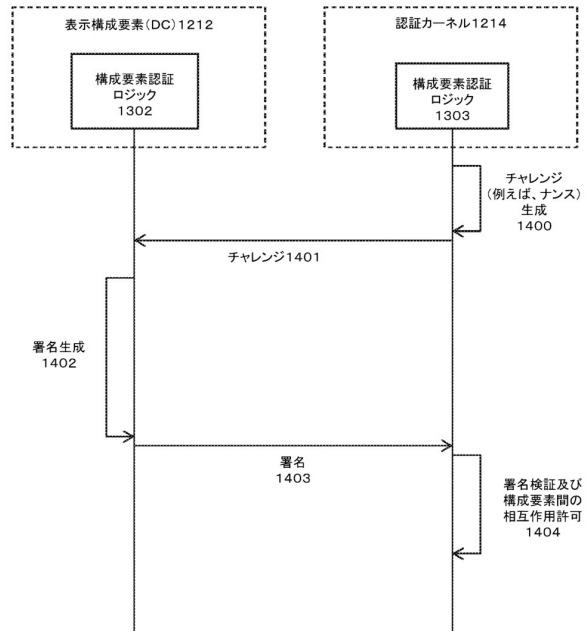
40

50

【図 13】

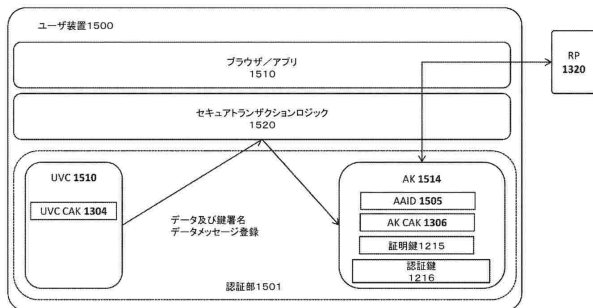


【図 14】

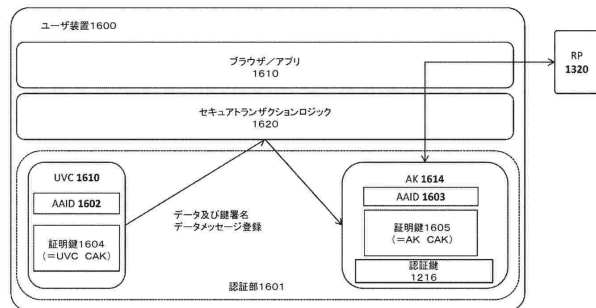


10

【図 15】



【図 16】



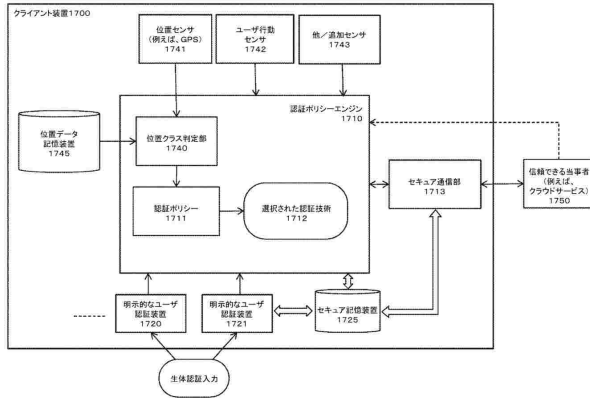
20

30

40

50

【図 17】

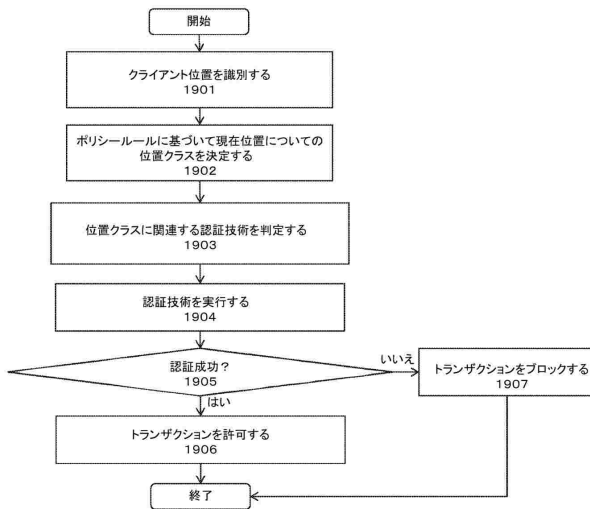


【図 18】

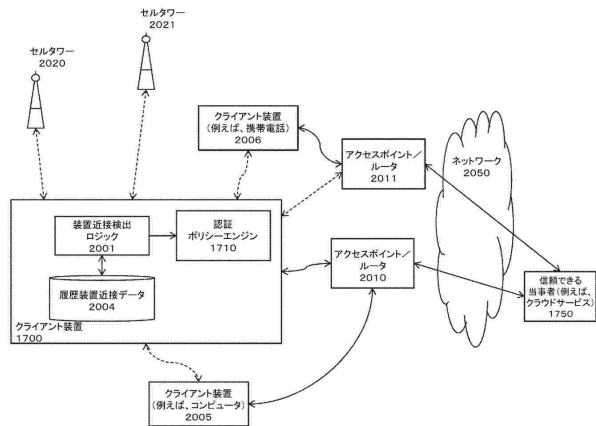


10

【図 19】



【図 20】



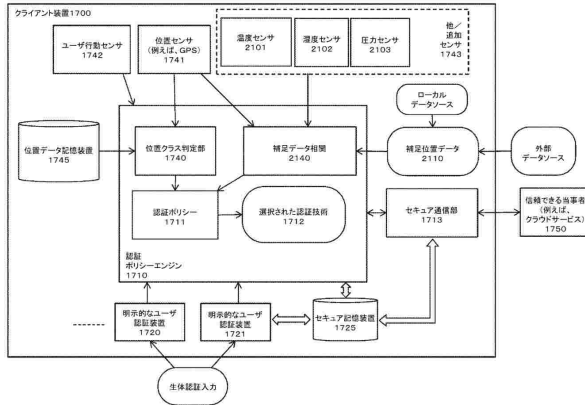
20

30

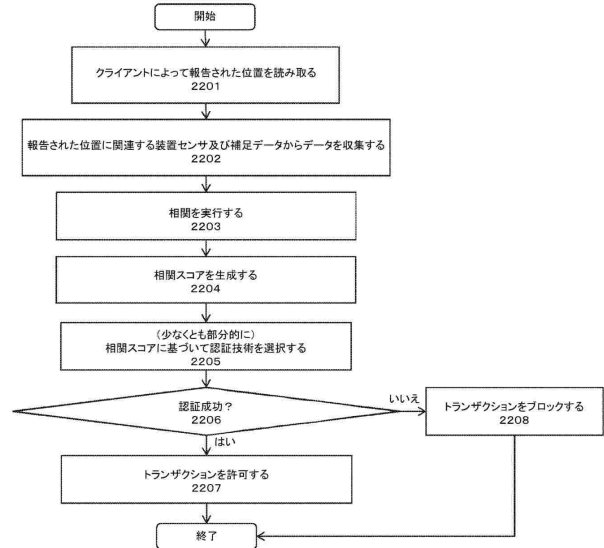
40

50

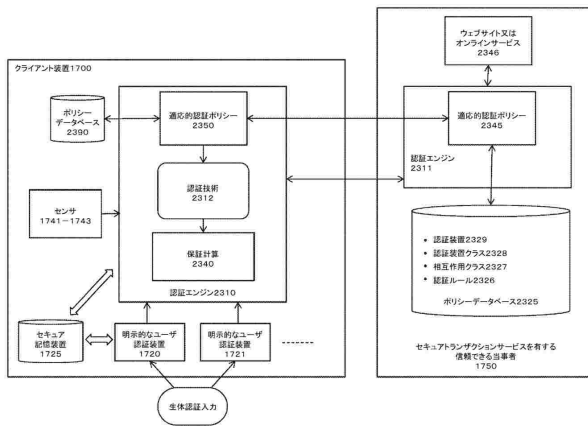
【図 2 1】



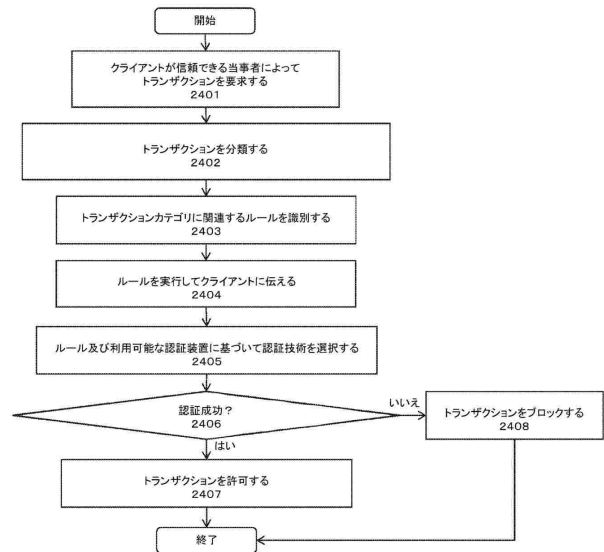
【図 2 2】



【図 2 3】



【図 2 4】



10

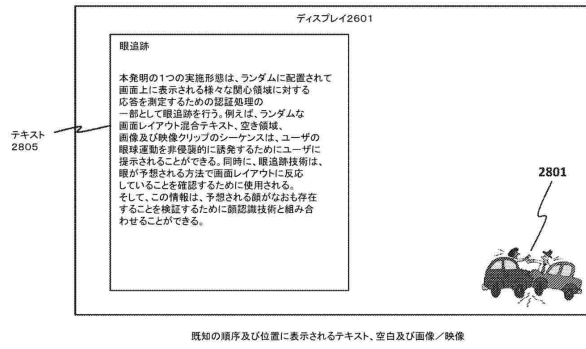
20

30

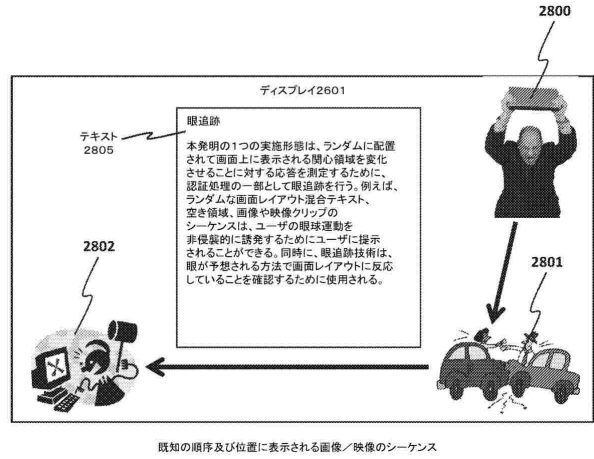
40

50

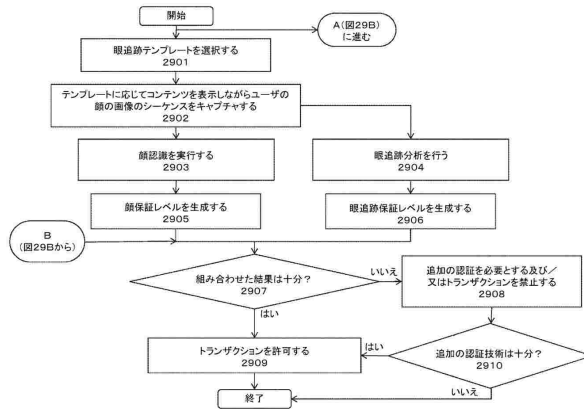
【図 28 A】



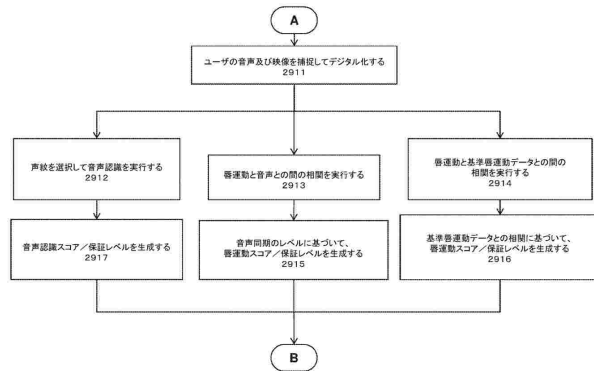
【図 28 B】



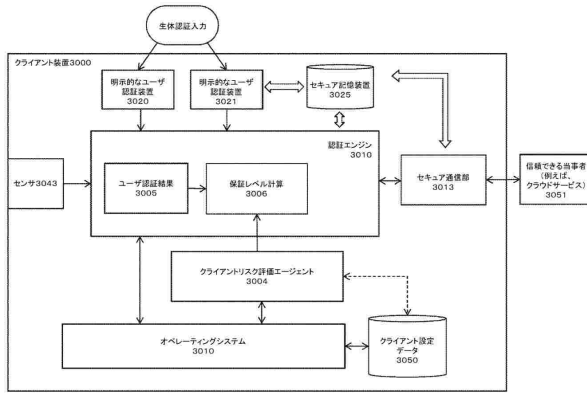
【図 29 A】



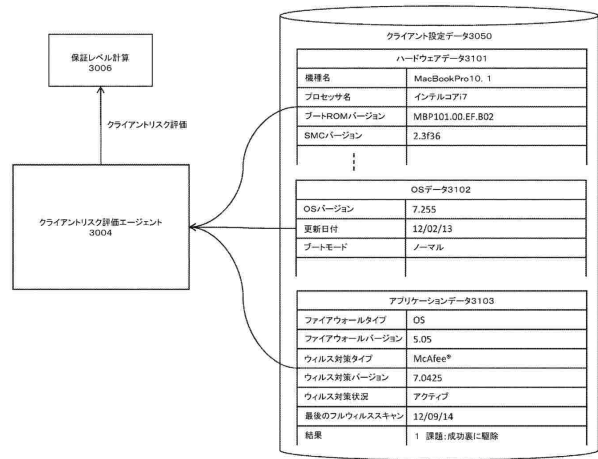
【図 29 B】



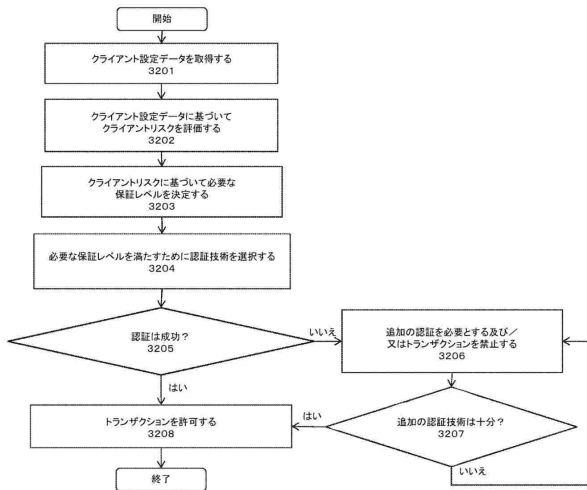
【図 30】



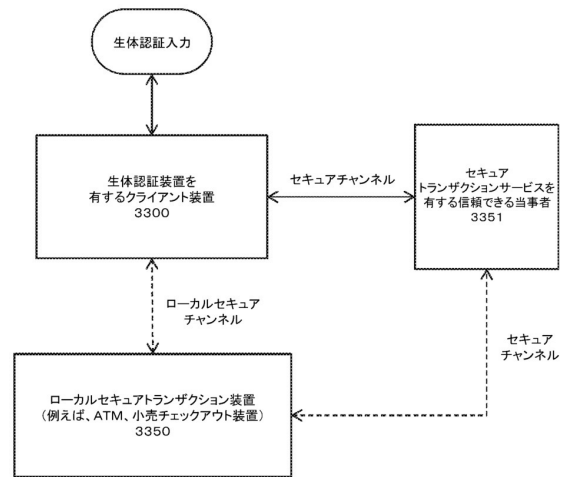
【図 31】



【図 32】



【図 33】



10

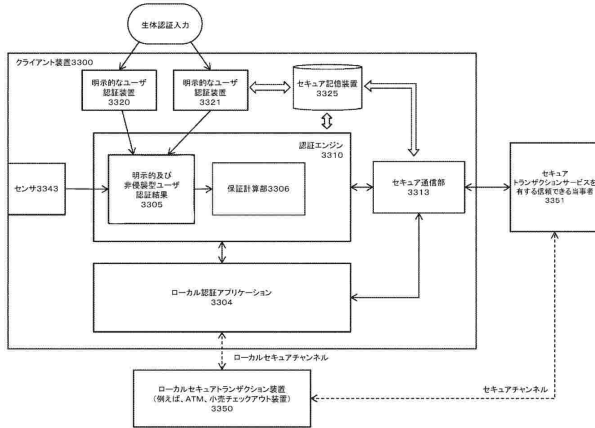
20

30

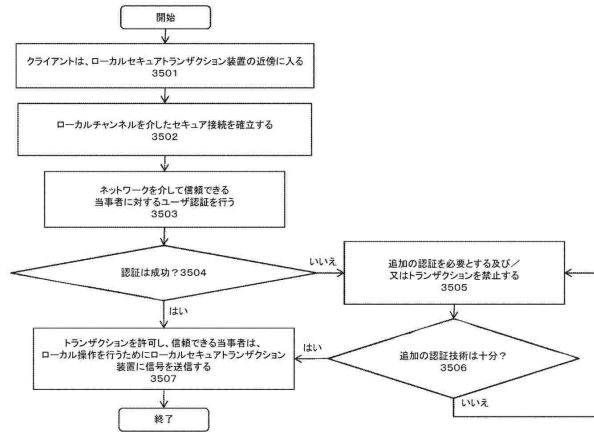
40

50

【図 34】

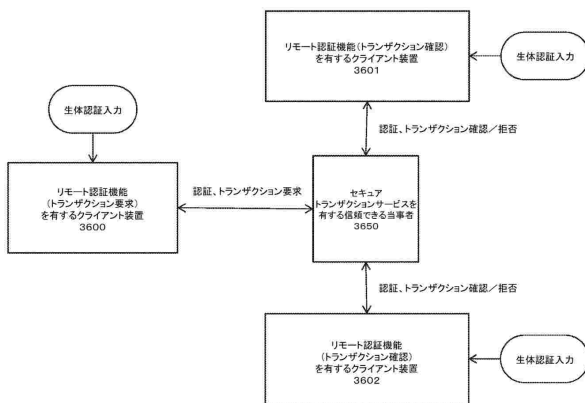


【図 35】

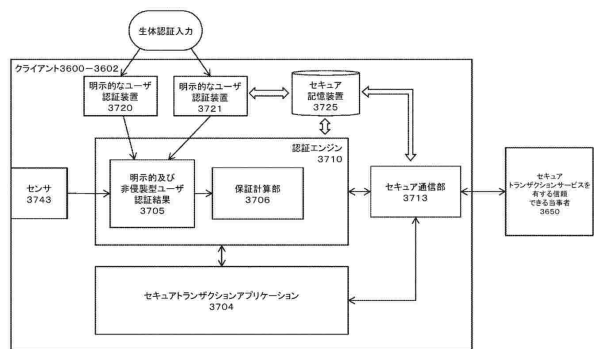


10

【図 36】

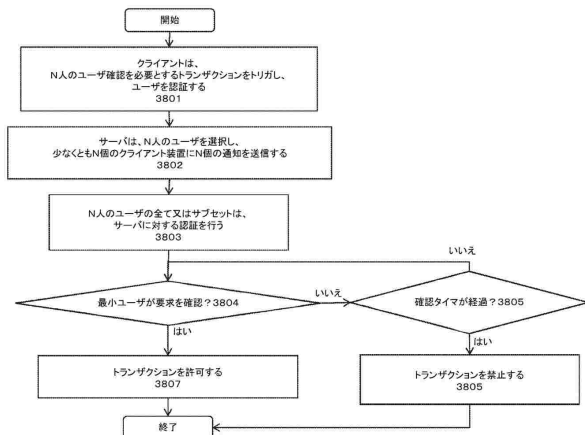


【図 37】

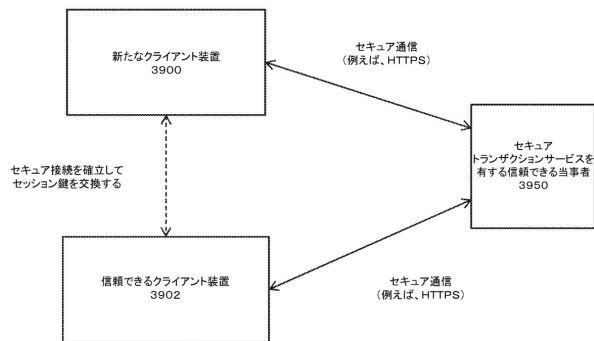


20

【図 38】



【図 39】

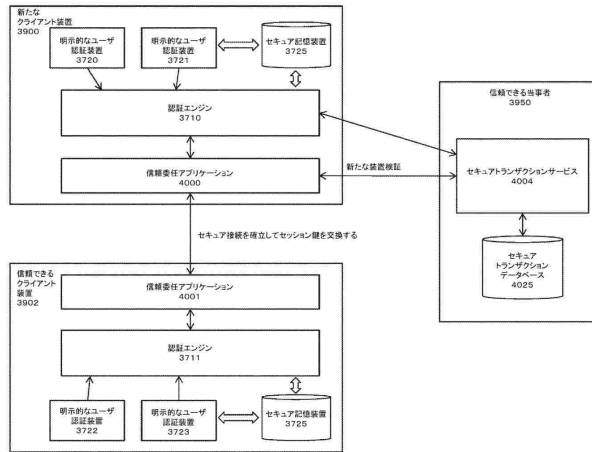


30

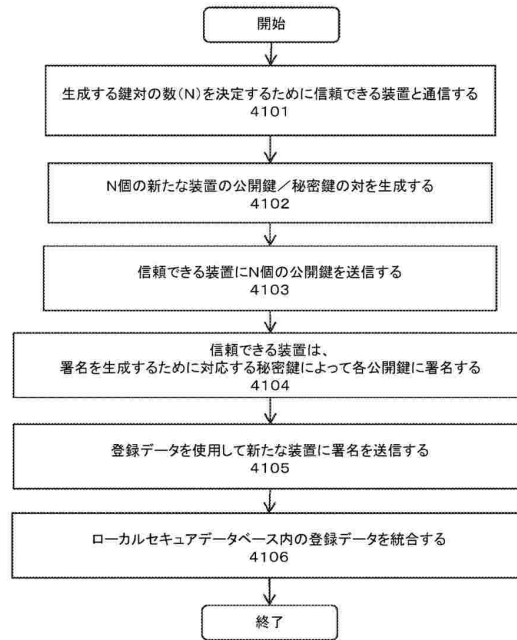
40

50

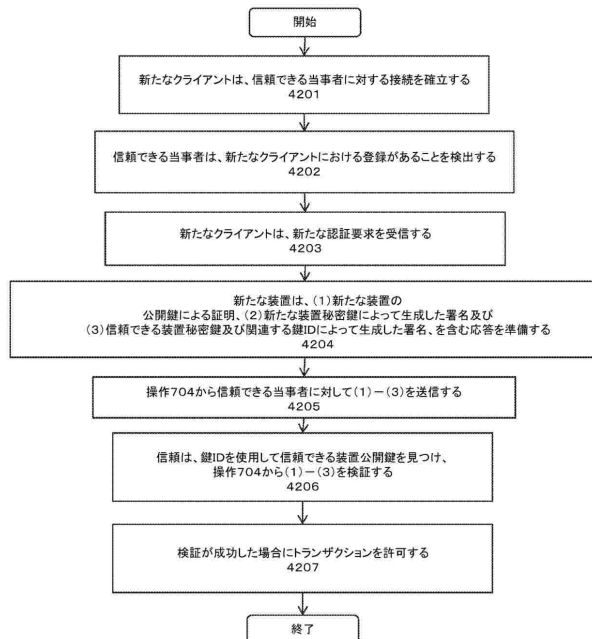
【図 40】



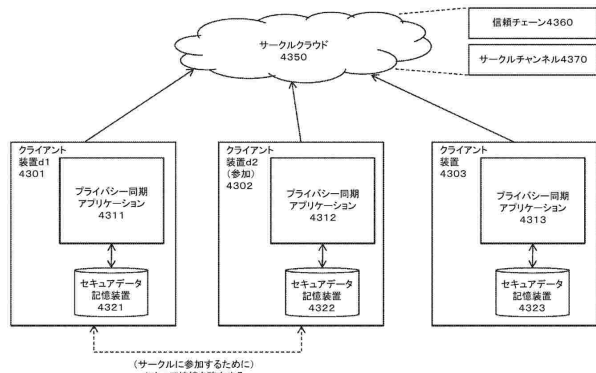
【図 41】



【図 42】



【図 43】



10

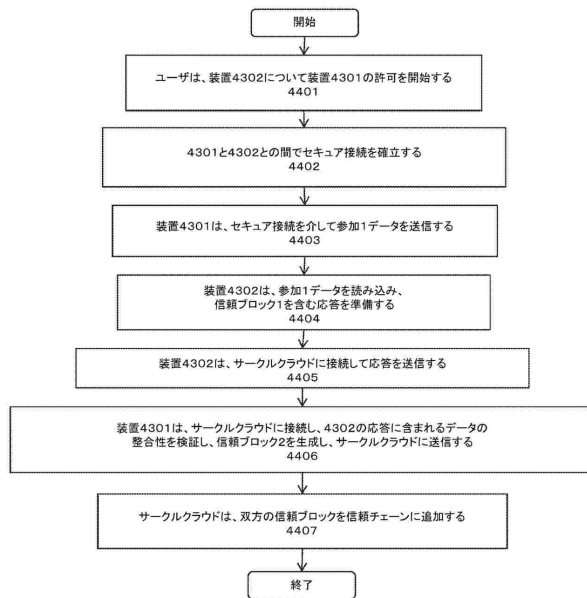
20

30

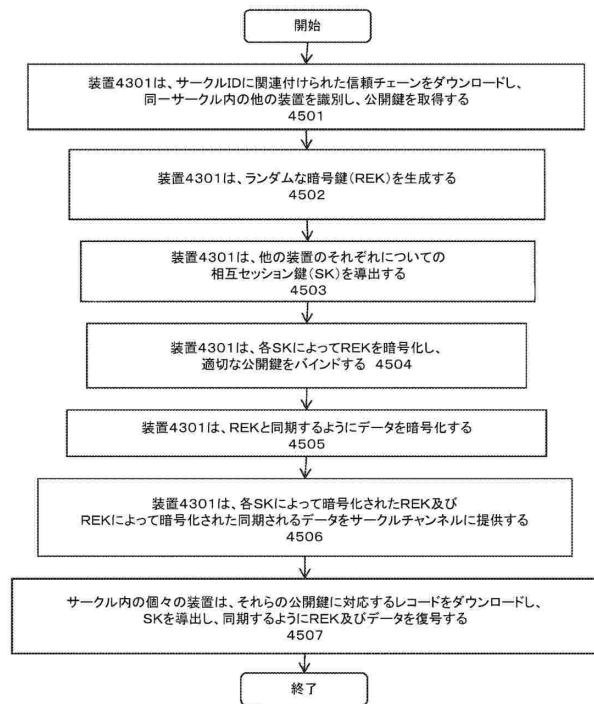
40

50

【図 4 4】



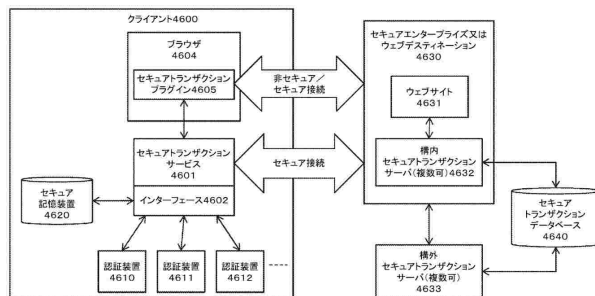
【図 4 5】



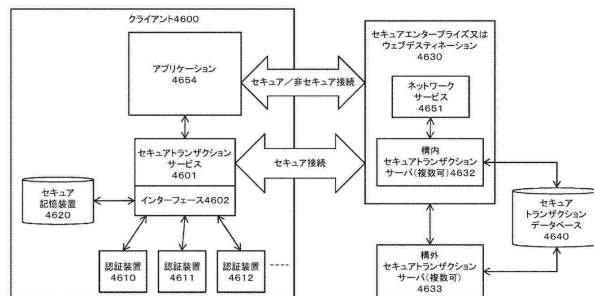
10

20

【図 4 6 A】



【図 4 6 B】

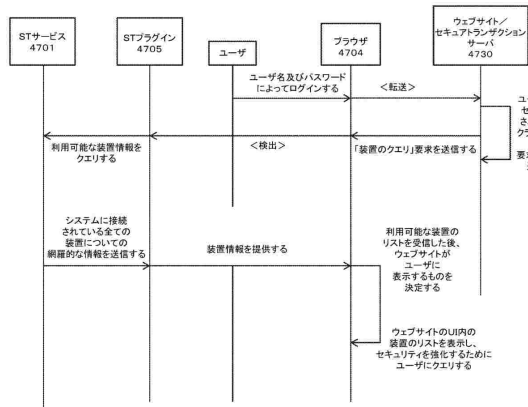


30

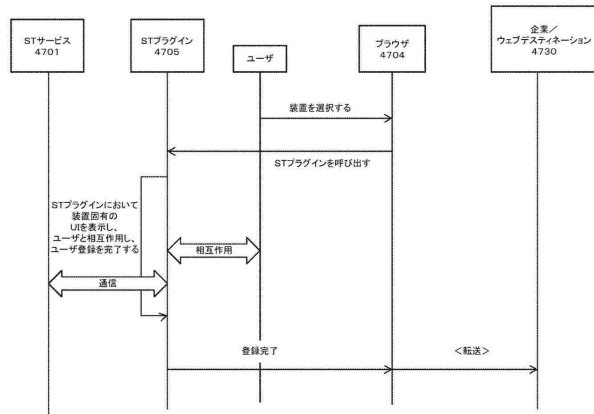
40

50

【図 47】

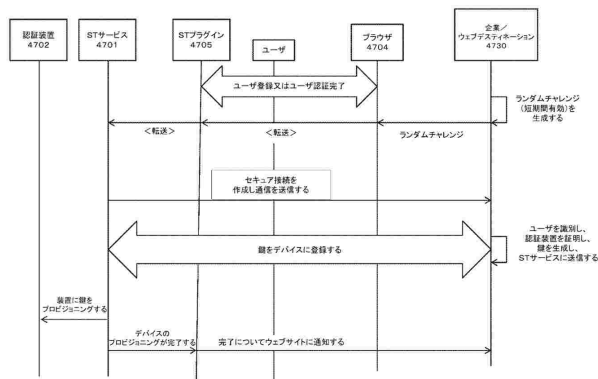


【図 48】

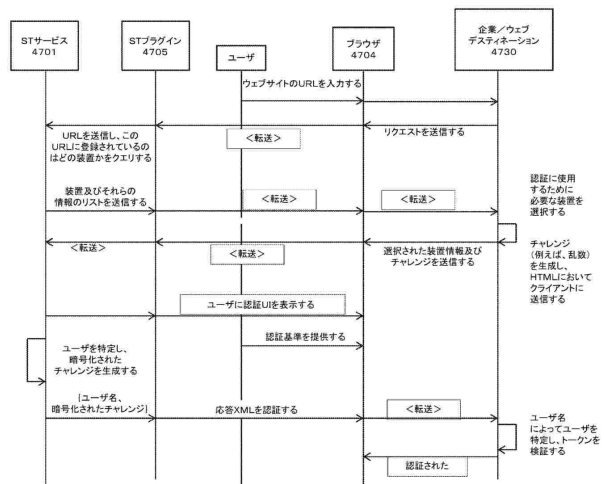


10

【図 49】



【図 50】



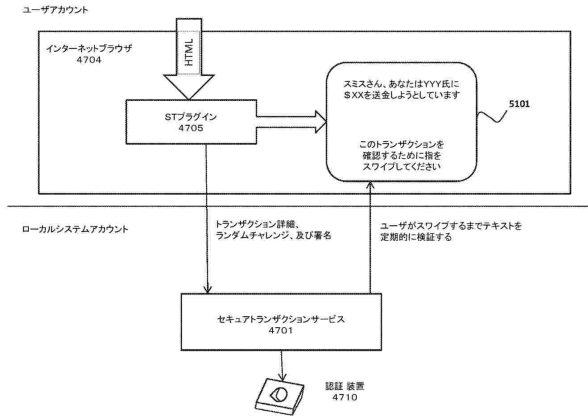
20

30

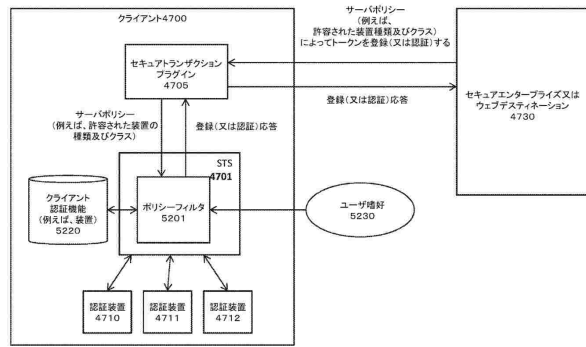
40

50

【図 5 1】

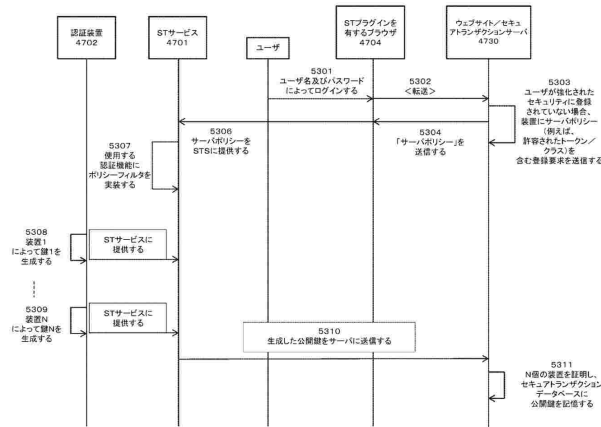


【図 5 2】

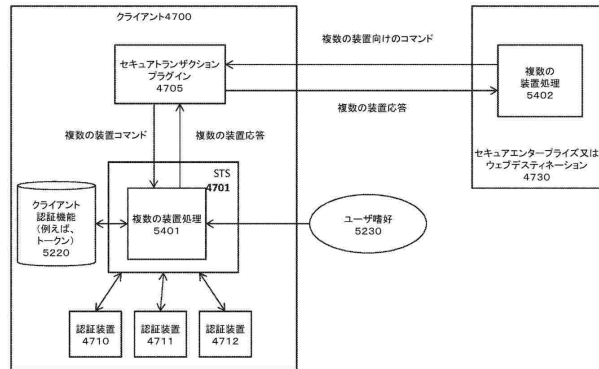


10

【図 5 3】



【図 5 4】



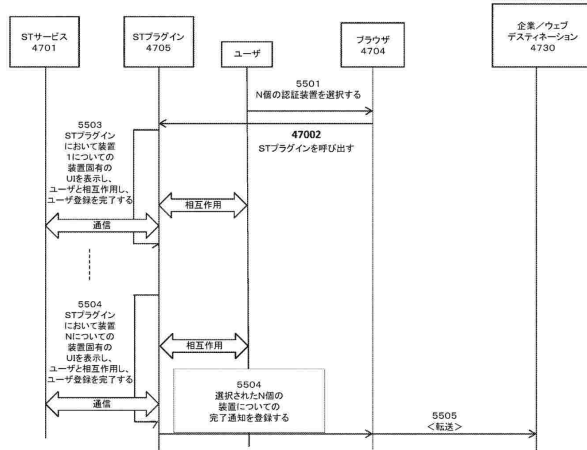
20

30

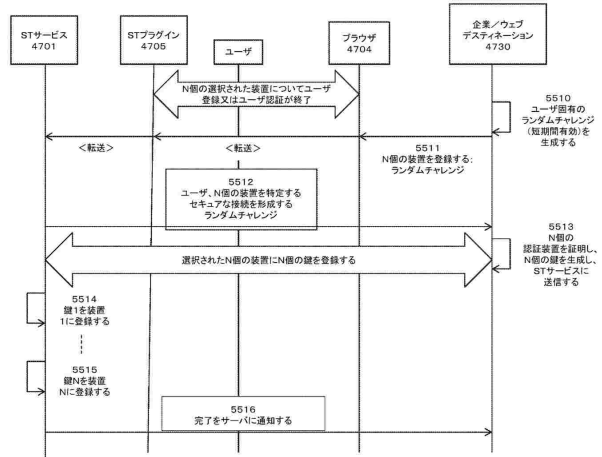
40

50

【図 5 5 A】

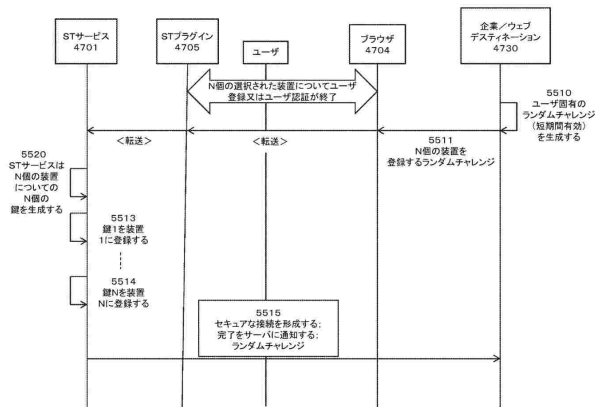


【図 5 5 B】

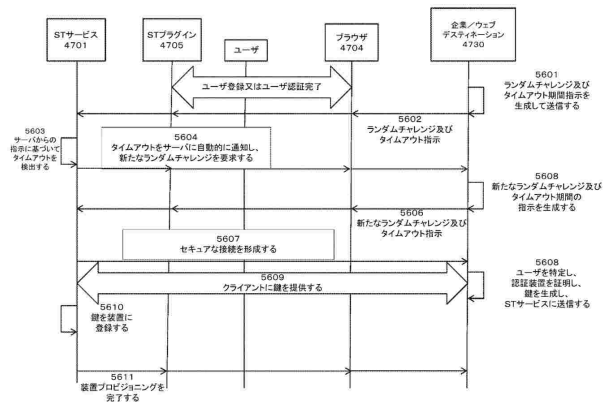


10

【図 5 5 C】



【図 5 6 A】



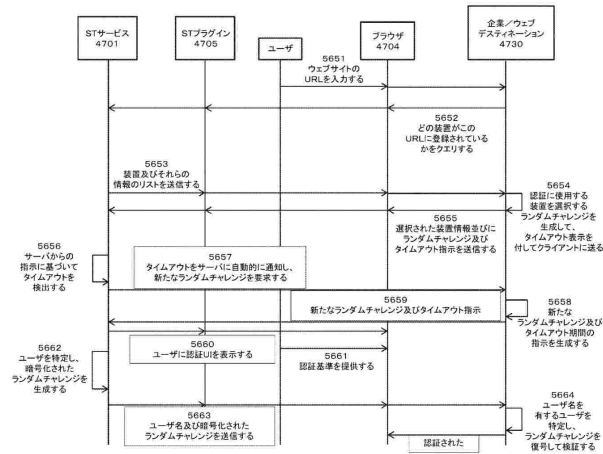
20

30

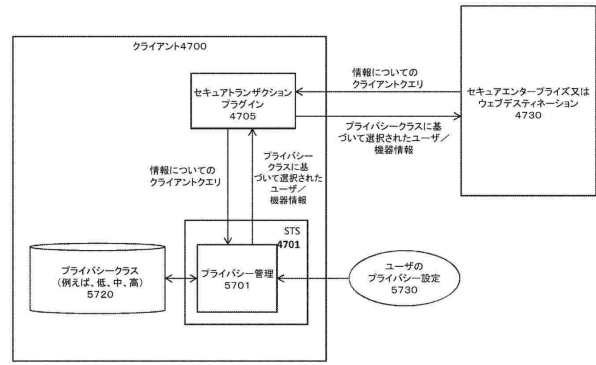
40

50

【図 5 6 B】

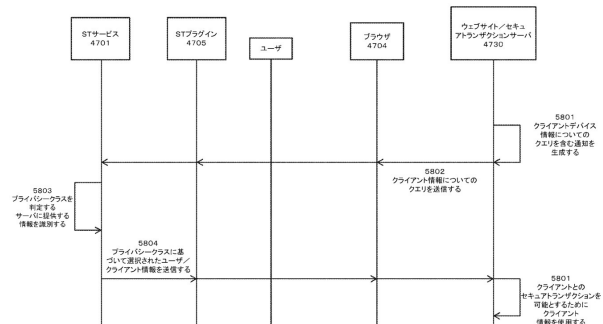


【図 5 7】

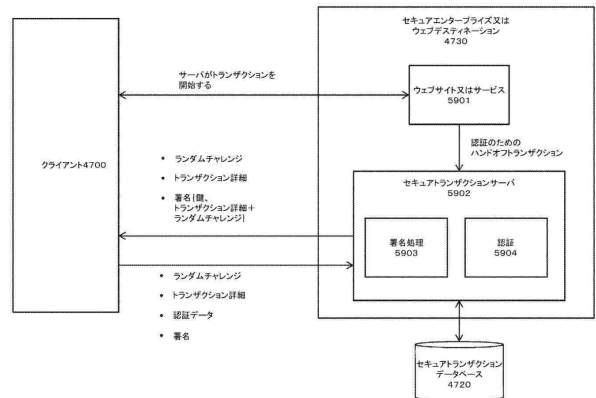


10

【図 5 8】



【図 5 9】



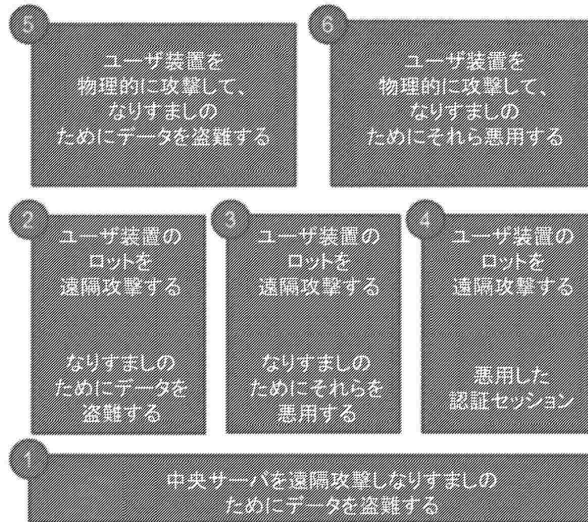
20

30

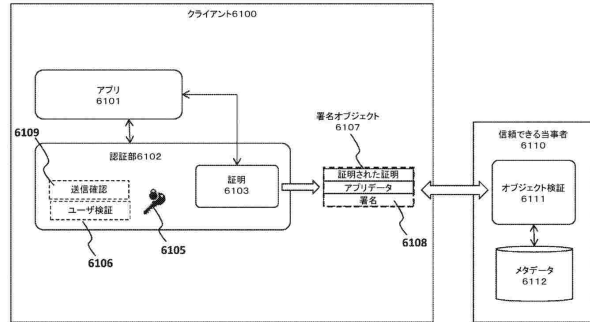
40

50

【図 60】

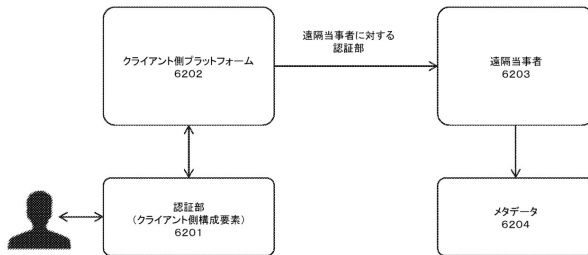


【図 61】

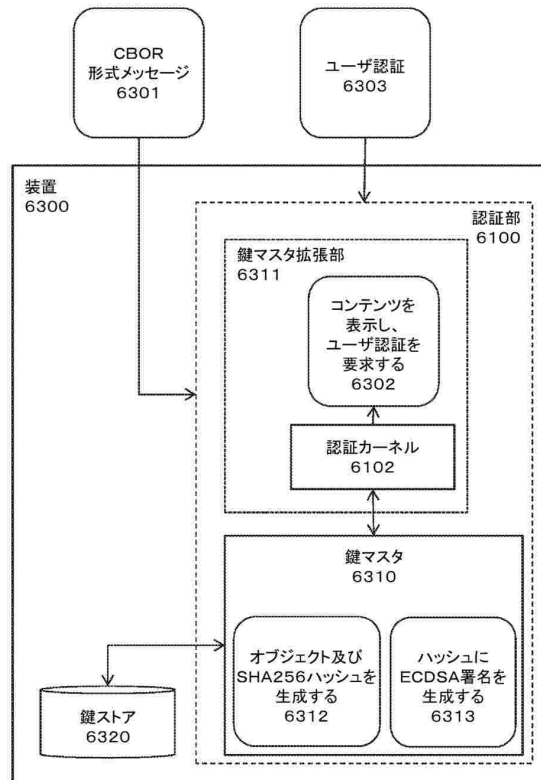


10

【図 62】



【図 63】



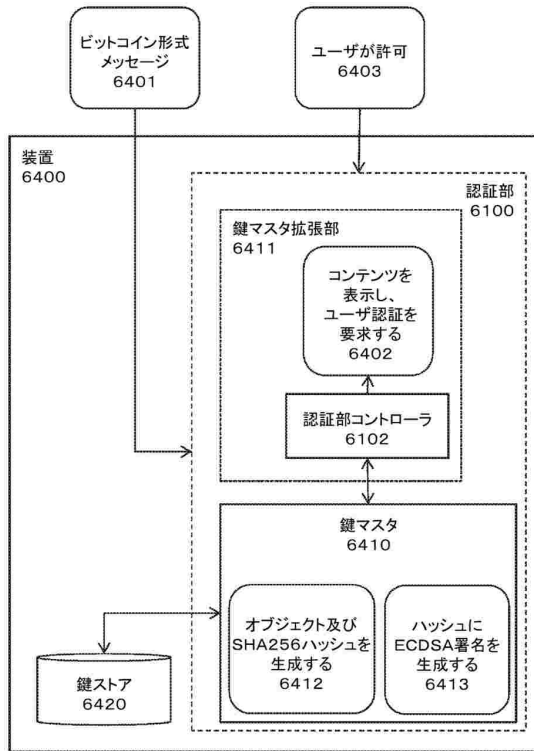
20

30

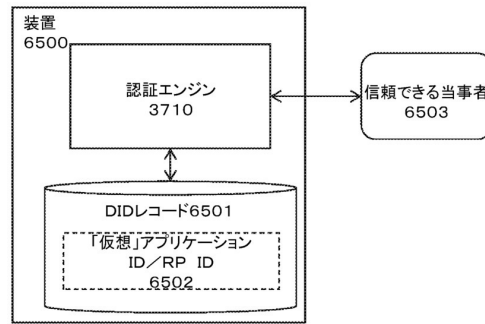
40

50

【図 6 4】



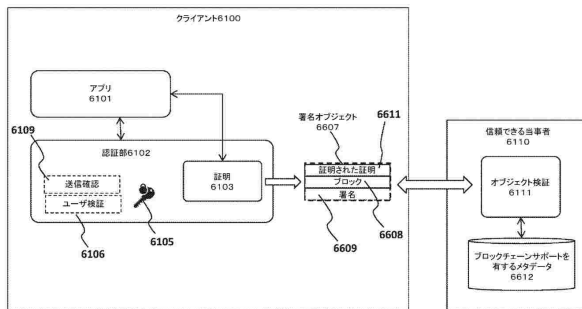
【図 6 5】



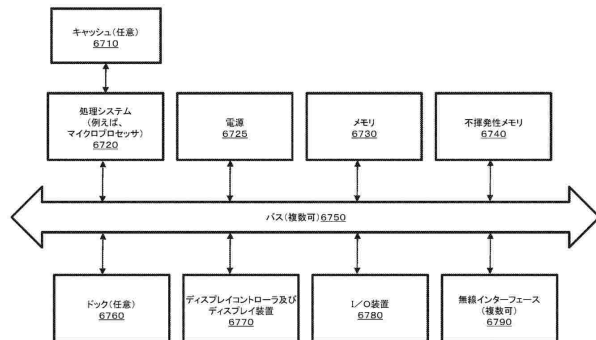
10

20

【図 6 6】



【図 6 7】

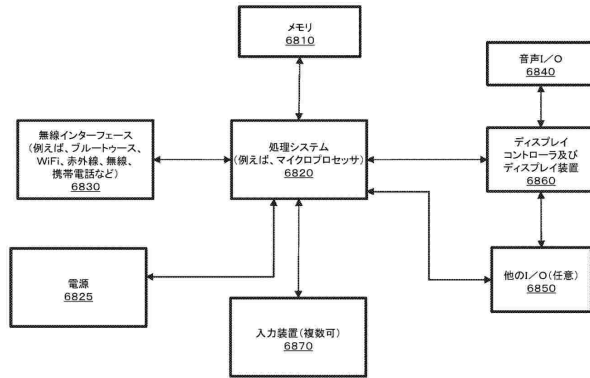


30

40

50

【図 68】



10

20

30

40

50

フロントページの続き

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 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 岸野 徹
(56)参考文献 特開2017-152880 (JP, A)
特表2016-521403 (JP, A)
特開2017-157926 (JP, A)
米国特許出願公開第2017/0317833 (US, A1)
(58)調査した分野 (Int.Cl., DB名)
G06F 21/64
G06F 21/32
H04L 9/32