

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7448220号
(P7448220)

(45)発行日 令和6年3月12日(2024.3.12)

(24)登録日 令和6年3月4日(2024.3.4)

(51)国際特許分類		F I	
H 0 4 L	9/08 (2006.01)	H 0 4 L	9/08 C
H 0 4 L	9/32 (2006.01)	H 0 4 L	9/08 E
G 0 9 C	1/00 (2006.01)	H 0 4 L	9/32 2 0 0 A
		G 0 9 C	1/00 6 4 0 E
請求項の数 12 (全55頁)			
(21)出願番号	特願2020-542698(P2020-542698)	(73)特許権者	520136021
(86)(22)出願日	平成30年10月19日(2018.10.19)		オートンハイブ コーポレーション
(65)公表番号	特表2021-500831(P2021-500831 A)		AUTNHIVE CORPORATI ON
(43)公表日	令和3年1月7日(2021.1.7)		カナダ国 エル6エイチ 0シー3 オン
(86)国際出願番号	PCT/IB2018/058165		タリオ, オークビル, アッパー ミドル
(87)国際公開番号	WO2019/077581		ロード イースト 2 2 7 5 # 1 0 1
(87)国際公開日	平成31年4月25日(2019.4.25)	(74)代理人	110001438
審査請求日	令和3年10月18日(2021.10.18)		弁理士法人 丸山国際特許事務所
(31)優先権主張番号	62/574,285	(72)発明者	ビジャヤナラヤナン, デヴィ セルバ ク
(32)優先日	平成29年10月19日(2017.10.19)		マール
(33)優先権主張国・地域又は機関	米国(US)		カナダ国 エル6エイチ 0シー3 オン
前置審査			タリオ, オークビル, アッパー ミドル
		審査官	金沢 史明
			最終頁に続く

(54)【発明の名称】 マルチポイント認証のためのキー生成・預託システム及び方法

(57)【特許請求の範囲】

【請求項1】

アイデンティティを認証するためのキーを生成、配布、及び格納する方法において、サーバで第1のコンピューティングデバイスから登録要求を受け取るステップと、前記登録要求の受取りに応答して、少なくともクライアント登録コードを含む登録データを前記サーバから前記第1のコンピューティングデバイスに送るステップと、前記サーバで登録キー及びサーバキーを受け取るステップであって、前記登録キー及び前記サーバキーは前記第1のコンピューティングデバイスによって生成され、前記登録キーは、前記クライアント登録コード及び前記サーバキーのうちの少なくとも1つを含む、ステップと、前記サーバでピアリストを生成するステップであって、前記ピアリストは受信者コードを含んでいる、ステップと、前記サーバで配布キーを生成するステップであって、前記配布キーは、前記受信者コード及び前記サーバキーに基づいている、ステップと、前記サーバで、前記サーバに関連する1又は複数のデータベースに、前記登録キー、前記配布キー、及び前記ピアリストを格納するステップと、前記サーバから第2のコンピューティングデバイスに、前記配布キーを送るステップと、前記サーバで、前記第2のコンピューティングデバイスから預託キーを受け取るステップであって、前記預託キーは前記配布キーに基づいて生成される、ステップと、前記サーバに関連する前記1又は複数のデータベースにて、前記ピアリストに、前記第

2のコンピューティングデバイスから受け取った前記預託キーを格納するステップと、を含む、方法。

【請求項2】

前記第1のコンピューティングデバイスは、
前記サーバから前記登録データを受け取るステップと、
2つ以上の選択コードを含むユーザ入力を受け取るステップと、
前記2つ以上の選択コードを、少なくとも選択コードの第1のグループと選択コードの第2のグループとに分割するステップと、
前記選択コードの第1のグループからクライアントキーを生成するステップと、
前記選択コードの第2のグループから前記サーバキーを生成するステップと、
前記クライアントキーから、少なくともクライアントキーの第1の部分とクライアントキーの第2の部分の生成するステップと、
前記サーバキーから、少なくともサーバキーの第1の部分とサーバキーの第2の部分とを生成するステップと、
前記登録キーを生成するステップであって、前記登録キーは、前記クライアントキー、前記サーバキー、及び前記クライアント登録コードに基づいている、ステップと、
前記第1のコンピューティングデバイスのメモリに、前記クライアントキー及び前記クライアント登録コードを格納するステップと、
少なくとも前記登録キー及び前記サーバキーを前記サーバに送るステップと、
を行うように構成されている、請求項1に記載の方法。

10

20

【請求項3】

前記登録データが選択オブジェクトのグループを含む、請求項1に記載の方法。

【請求項4】

前記ユーザ入力が、生体認証データ、空間データ、及び時間データのうちの1又は複数を含む、請求項2に記載の方法。

【請求項5】

前記選択コードの第1のグループから前記クライアントキーを生成するステップは、
前記選択コードの第1のグループを構成する個々の選択コードを、変換された選択コードのグループに変換するステップと、
前記変換された選択コードのグループを構成する個々の変換された選択コードの各々を、クライアントプレキーを構成する1又は複数のキャラクタ列へと連結するステップと、
前記クライアントプレキーを前記クライアントキーに変換するステップと、
を含む、請求項2に記載の方法。

30

【請求項6】

前記選択コードの第2のグループから前記サーバキーを生成するステップは、
前記選択コードの第2のグループを構成する個々の選択コードを、変換された選択コードのグループに変換するステップと、
前記変換された選択コードのグループを構成する個々の変換された選択コードの各々を、サーバプレキーを構成する1又は複数のキャラクタ列へと連結するステップと、
前記サーバプレキーを前記サーバキーに変換するステップと、
を含む、請求項2に記載の方法。

40

【請求項7】

前記登録キーを生成するステップは、
前記クライアントキーの第1の部分と前記クライアントキーの第2の部分の少なくとも1つと、前記サーバキーの第1の部分と前記サーバキーの第2の部分の少なくとも1つとを連結して、第1のプレキーを構成する1又は複数のキャラクタ列を生成するステップと、
前記第1のプレキーを第2のプレキーに変換するステップと、
前記第2のプレキーと前記クライアント登録コードとを連結して、登録プレキーを構成する1又は複数のキャラクタ列を生成するステップと、
前記登録プレキーを前記登録キーに変換するステップと、

50

を含む、請求項 2 に記載の方法。

【請求項 8】

前記第 2 のコンピューティングデバイスから前記預託キーを受け取るステップでは、前記第 2 のコンピューティングデバイスは、

前記サーバから前記配布キーを受信し、

預託コードと前記預託キーとを生成し、前記預託キーは、前記預託コード及び前記配布キーに基づいており、

前記第 2 のコンピューティングデバイスのメモリに、前記配布キー及び前記預託キーを格納し、

前記サーバに前記預託キーを送るように構成されている、請求項 1 に記載の方法。

10

【請求項 9】

前記預託キーを生成することは、

前記配布キーと前記預託コードとを、預託プレキーを構成する 1 又は複数のキャラクタ列へと連結することと、

前記預託プレキーを前記預託キーに変換することと、

を含む、請求項 8 に記載の方法。

【請求項 10】

前記配布キーを生成するステップは、

前記サーバキー、前記登録キー、及び前記受信者コードのうちの 1 又は複数を、配布プレキーを構成する 1 又は複数のキャラクタ列へと連結するステップと、

20

前記配布プレキーを前記配布キーに変換するステップと、

を含む、請求項 1 に記載の方法。

【請求項 11】

サーバを備えるシステムにおいて、

前記サーバは、

サーバ命令を含むメモリと、

前記サーバ命令を実行するように構成された処理デバイスと、

を備えており、

前記サーバ命令は、前記処理デバイスに、

前記サーバで第 1 のコンピューティングデバイスからの登録要求を受け取る動作と、

30

前記登録要求の受取りに応答して、前記サーバから前記第 1 のコンピューティングデバイスに、少なくともクライアント登録コードを含む登録データを送る動作と、

前記サーバで登録キー及びサーバキーを受け取る動作であって、前記登録キー及び前記サーバキーは前記第 1 のコンピューティングデバイスで生成され、前記登録キーは、前記クライアント登録コード及び前記サーバキーのうちの少なくとも 1 つを含む、動作と、

前記サーバでピアリストを生成する動作であって、前記ピアリストは受信者コードを含んでいる、動作と、

前記サーバで配布キーを生成する動作であって、前記配布キーは、前記受信者コードと、前記サーバキーとに基づいている、動作と、

40

前記サーバで、前記サーバに関連する 1 又は複数のデータベースにて、前記登録キーと、前記配布キーと、前記ピアリストとを格納する動作と、

前記サーバから前記配布キーを第 2 のコンピューティングデバイスに送る動作と、

前記サーバで、前記第 2 のコンピューティングデバイスから預託キーを受け取る動作であって、前記預託キーは前記配布キーに基づいて生成される、動作と、

前記サーバに関連する前記 1 又は複数のデータベースにて前記ピアリストに、前記第 2 のコンピューティングデバイスから受け取った前記預託キーを格納する動作と、
を実行させる、システム。

【請求項 12】

前記サーバ命令は更に、前記処理デバイスに、

前記サーバで、前記第 1 のコンピューティングデバイスからログイン要求を受け取る動

50

作と、

前記サーバでログインソルトを生成する動作と、

前記サーバに関連する前記 1 又は複数のデータベースに前記ログインソルトを格納する動作と、

前記サーバから前記第 1 のコンピューティングデバイスに、少なくとも前記ログインソルトを含むログインデータを送る動作と、

前記サーバで、前記第 1 のコンピューティングデバイスからログインキー及び前記サーバキーを受け取る動作と、

前記サーバに関連する前記 1 又は複数のデータベースから、格納されている登録キー、前記ログインソルト、及び前記受信者コードを取得する動作と、

前記サーバで、比較ログインキーを生成する動作であって、前記比較ログインキーは前記格納されている登録キー及び前記ログインソルトに基づいている、動作と、

前記サーバで、前記比較ログインキーと前記第 1 のコンピューティングデバイスから受け取った前記ログインキーとを比較する動作と、

前記サーバで検証ソルトを生成する動作と、

前記サーバで配布キーを生成する動作であって、前記配布キーは、少なくとも前記第 1 のコンピューティングデバイスから受け取った前記サーバキーと、前記受信者コードとに基づいている、動作と、

前記サーバで検証キーを生成する動作であって、前記検証キーは、前記サーバキー、前記受信者コード、及び前記検証ソルトに基づいている、動作と、

前記サーバのピアリストに、前記検証キー及び前記検証ソルトを格納する動作と、

前記サーバから前記第 2 のコンピューティングデバイスに、前記検証キー及び前記検証ソルトを送る動作と、

前記サーバで、前記第 2 のコンピューティングデバイスから確認キーを受け取る動作と、

前記サーバに関連する前記 1 又は複数のデータベースから、格納されている配布キーと前記検証ソルトとを取得する動作と、

前記格納されている配布キーと前記検証ソルトに基づいて、第 2 の検証キーを生成する動作と、

前記第 2 のコンピューティングデバイスから受け取った前記確認キーを前記第 2 の検証キーと比較する動作と、

認証結果を生成する動作と、

を実行させる、請求項 1 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、ネットワーク又はシステムの認証（authentication）の分野に関し、より具体的には、ネットワークのユーザとネットワーク又はシステムを介してユーザとの間でやり取りされるデータの認証に関する。

【背景技術】

【0002】

全ての組織では、起こり得るセキュリティ侵害からデータを保護することが課題となっている。データセキュリティがあつてこそ、組織は、許可された者のみが複数のテクノロジーにわたっている組織のシステムにアクセス許可されることを確保できる。故に、データセキュリティと許可されたシステムへのアクセスとは、今日、組織が取り組まなければならない 2 つの大きな課題となっている。

【0003】

現在、システムとネットワークのユーザに関する様々な種類の認証をもたらす多数のシステム及び方法が存在している。これらの様々な種類の認証は、セキュリティと信頼性のレベルで異なっている。以下に、システム及びネットワークのための先行技術の認証方法の種類を例示する。

10

20

30

40

50

【0004】

2005年11月8日にIGTに付与された米国特許第6,962,530号は、ゲーム専用プラットフォームのためのアーキテクチャ及び方法を開示しており、当該アーキテクチャ及び方法は、ゲームコードやその他のデータを安全に格納及び検証することを特徴とする。この方法は更に、コンピュータ化された賭博ゲームシステムとの間でデータを安全に交換する能力をユーザにもたらす。この発明は、複数のデバイスの間においてログイン情報を広めることを含んでいない。

【0005】

2015年6月9日にNECソリューションイノベータ株式会社に付与された米国特許第9,053,306号は、ユーザが入力したログイン情報から第1のハッシュ値及び第2のハッシュ値を計算するように動作する認証システムを開示している。第1のハッシュ値と第2のハッシュ値とが一致する場合に、サーバと端末との間でセッションが確立される。この発明は、暗号化された詳細の一部を隠しておくことを含んでいない。

10

【0006】

2015年3月24日にマイクロソフト社に付与された米国特許第8,989,706号は、デバイスのための自動化された安全なペアリングに関するシステム、方法及び／又は技術を開示しており、デバイスを使用したコンテンツの並列ダウンロードに関連している。デバイスをペアリングするためのツールは、アドレスに基づく認証プロトコルと、キーに基づく認証プロトコルとを実行し得る。この発明は、暗号化された詳細の一部を隠しておくことを含んでいない。

20

【0007】

2013年1月15日にKoninklijke Philips Electronics N.V.に付与された米国特許第8,356,180号は、深い共通セキュリティドメインでのセキュア通信に関した多次元識別、認証、承認、及びキー配布のための方法を開示している。本発明は、ユーザがシステムにユーザのキーを明かすことなくして、トランザクションを認証することはできない。

【0008】

2000年8月25日にUnited Devices, Inc.に発行された米国特許第6,847,995号は、分散処理システム内で安全な転送をもたらすためのセキュリティアーキテクチャ及び方法を開示している。この発明は、多層暗号化を含んでおらず、又は、暗号化された詳細の一部を隠しておくことを含んでいない。

30

【0009】

Yaron Gviliが2016年11月23日出願した米国特許出願公開第2017/0149796号は、第三者の検証器が安全なデータの特徴を検証できるようにするためのシステム及び技術、又はその成功した通信を開示している。この発明は、多層暗号化を含んでおらず、又は、暗号化された詳細の一部を隠しておくことを含んでいない。

【0010】

2011年6月6日に寺西勇によって出願された米国特許出願公開第2011/0246779号は、離散対数ゼロ知識証明を可能にするゼロ知識証明システムを開示している。この発明は、多層暗号化を含んでおらず、又は、暗号化された詳細の一部を隠しておくことを含んでいない。

40

【0011】

先行技術の暗号化方法及びシステムは、ユーザとシステム又はネットワークとの間のデータ及び情報の転送における第三者の介入に対して特に脆弱である。第三者は、転送中のデータにアクセスできる場合にはその情報からログイン詳細を推定できる。ユーザとシステムの間で転送されたデータからログイン詳細の全てが利用可能であるならば、第三者はユーザのログイン詳細を使用してシステムにログインすることができる。これは、既知の認証方法やシステムが利用されている場合には、現在のシステムのセキュリティ上の危険を生じる。

【0012】

50

必要とされているものは、送られたデータに第三者が干渉することで、ユーザのログイン情報が取得されないようにする認証方法及びシステムである。

【発明の概要】

【0013】

ある態様では、本開示は、ユーザ、データ、ドキュメント、デバイス、及びトランザクションを認証することができる認証方法及びシステムに関する。本発明の実施形態は、任意のシステム又はネットワークで動作可能であって、プラットフォームに依存しない。本発明の認証方法及びシステムは、複数のデバイス間でログイン関連情報の固有部分を安全に生成して、分散させることが可能である。このようにして生成されたログイン関連情報は、システムに公開されることなく、ユーザ、データ、ドキュメント、デバイス、トランザクションなどを認証するために利用される。このシステムは、作成時、送信時、保存時、及び認証時にログイン関連情報を保護する。別の態様では、本開示は、システムにキーを明らかにすることなく認証することに関連している。

【0014】

別の態様では、本開示は、ユーザ認証のためのシステム及び方法に関しており、セキュア部分を含むクライアントシステムと、ユーザがクライアントシステムにアクセスして、ログイン情報の一部を保存できるように動作するユーザシステムと、クライアントシステム及びユーザシステムに対して情報を送受信するために動作する検証システムと、複数の同期要素を含む同期システムと、を備えており、ユーザのログイン関連情報の固有部分は、検証システムで双方向に送られ、そして、格納され、アクセスされ、使用される。

【0015】

更に別の態様では、本開示は、クライアントシステムとのユーザ対話 (user interaction) を認証するためのシステム及び方法に関連しており、当該システム及び方法は、ユーザデバイス、クライアントシステム、クライアント表示ユニット、及びクライアント検証システムを備えており、ユーザデバイス、クライアントシステム、クライアント表示ユニット、及びクライアント検証システムは、ユーザがシステムにユーザキーを明らかにすることなく、クライアントシステムとのユーザ対話を認証するように動作する。

【0016】

この点に関して、本発明の少なくとも1つの実施形態を詳細に説明する前に、本発明は、以下の説明に記載された、又は図面に示された構造の詳細と構成要素の配置とに限定されるものではないことは理解されるべきである。本発明は、他の実施形態が可能であって、様々な方法で実施できる。また、本明細書で採用されている表現及び用語は、説明の目的のためのものであって、限定的なものとはみなされるべきではないことも理解されるべきである。

【図面の簡単な説明】

【0017】

以下の詳細な説明を検討すると、本発明がより良く理解され、本発明の目的が明らかになるであろう。その詳細な説明は、添付の図面を参照している。

【0018】

【図1】図1は、本発明の認証システムの一実施形態を示すシステム図である。

【図2】図2は、本発明の実施形態のクライアントシステムと検証システムとの間でデータの転送を行うように動作する要素の構成を示すシステム図である。

【図3】図3は、本発明の実施形態の登録処理を行うために動作する要素の構成を示すシステム図である。

【図4】図4は、本発明の実施形態のアクセスプロセスを実行するように動作する要素の構成を示すシステム図である。

【図5】図5は、本発明の実施形態に従って、ハッシュ化されたOYパケット部分を処理するために動作する同期要素を示すシステム図である。

【図6】図6は、本発明の一実施形態による復号プロセスを実行するために動作する要素の構成を示すシステム図である。

【図 7】図 7 は、本発明の一実施形態のユーザデバイスの要素を示すシステム図である。

【図 8】図 8 は、本発明の一実施形態のクライアントシステムの要素を示すシステム図である。

【図 9】図 9 は、本発明の一実施形態のクライアント表示ユニットの要素を示すシステム図である。

【図 10】図 10 は、本発明の一実施形態の検証システムの要素を示すシステム図である。

【図 11】図 11 は、本発明の一実施形態に従って、クライアントシステムのセキュア部分にアクセスするためのユーザ認証要求の処理を行うために動作する要素の構成を示すシステム図である。

【図 12】図 12 は、本発明の一実施形態に従ってユーザの認証のためのノイズ及びキーの生成及び処理を行うために動作する要素の構成を示すシステム図である。

10

【図 13】図 13 は、本発明の実施形態に従ってユーザ認証のためのキーの検証を行うために動作する要素の構成を示すシステム図である。

【図 14】図 14 は、本発明の一実施形態に従ってユーザの認証のためのトークンの検証を行うために動作する要素の構成を示すシステム図である。

【図 15】図 15 は、本発明の一実施形態に従って、ユーザの認証のためのクライアント表示システムを介したチャレンジの検証を行うために動作する要素の構成を示すシステム図である。

【図 16】図 16 は、本発明の一実施形態に従って、ユーザ認証のためのユーザデバイスを介したチャレンジの検証を行うために動作する要素の構成を示すシステム図である。

20

【図 17】図 17 は、本発明の一実施形態に従った登録方法を示す。

【図 18】図 18 は、本発明の一実施形態に従った 1 又は複数のキーを作成する方法を示す。

【図 19】図 19 は、本発明の一実施形態に従った 1 又は複数のキーを配布する方法を示す。

【図 20】図 20 は、本発明の一実施形態に従ったログイン方法を示す。

【図 21】図 21 は、本発明の一実施形態に従った 1 又は複数のキーを作成する方法を示す。

【図 22】図 22 は、本発明の一実施形態に従った 1 又は複数の検証キーを配布する方法を示す。

30

【図 23】図 23 は、本発明の一実施形態に従ったローカルデータベースで検証キーを検証する方法を示す。

【図 24】図 24 は、本発明の一実施形態に従った検証プロセスを有効にする方法を示す。

【図 25】図 25 は、本発明の一実施形態に従った 1 又は複数のバーコードを生成する方法を示す。

【図 26】図 26 は、本発明の一実施形態に従った 1 又は複数のキーを生成する方法を示す。

【図 27】図 27 は、本発明の一実施形態に従った 1 又は複数のキーを生成する方法を示す。

【図 28】図 28 は、本発明の一実施形態に従った 1 又は複数のキーを生成する方法を示す。

40

【図 29】図 29 は、本発明の一実施形態に従ったウェブセッションを確立する方法を示す。

【0019】

図面では、本発明の実施形態が例示的に図示されている。本明細書及び図面は、例示の目的のみのための、そして、理解の助けとしてのものであり、本発明の範囲の定義として意図されたものではないことは明らかに理解される。

【発明を実施するための形態】

【0020】

本発明は、ユーザ、データ、ドキュメント、デバイス、及びトランザクションを認証す

50

るために動作する認証方法及びシステムである。本発明の実施形態は、任意の組織又は個人における任意のシステム又はネットワークで動作可能である。認証方法及びシステムは、複数のデバイスの間でログイン関連情報の固有部分を配布するために動作可能である。ログイン関連情報の配布された部分は、ログイン関連情報をシステムに明らかにすることなく、ユーザ、データ、ドキュメント、デバイス、及びトランザクションを認証するためにシステムによって利用される。ログイン関連情報は、多層暗号化及び／又はハッシュ化され、暗号化及び／又はハッシュ化された詳細情報の一部は隠される。ログイン関連情報が格納されている装置は全て、認証方法及びシステムにおいて利用される。ユーザに提供されたログイン関連情報は、システム又はどのユーザデバイスにも明らかにされず、及び／又はそれらに格納されない。データ、ドキュメント、デバイス、トランザクションの認証は、システムに公開されるキーを必要としない。

10

【0021】

本明細書では、「クライアントシステム」とは、組織又は個人のネットワーク又はシステムの何れかを意味する。本明細書では、「ユーザデバイス」とは、ユーザがクライアントシステムにログインするために使用するデバイスを意味し、例えば、ラップトップ、タブレット、携帯電話、スマートフォン、デスクトップコンピュータ、スマートウォッチ、コンピューティングデバイスであって、それによって、ユーザは、クライアントシステム又は安全なログインを必要とする他のデバイスにログインすることができる。ユーザとクライアントシステムの間での「情報の転送」に関する言及は、システムに関連して起こる情報の作成、転送、又は保存を含み得る。

20

【0022】

明確にするために、認証システムの他のユニット又は要素に「アクセス」する認証システムのユニット又は要素に言及する場合、これは以下の何れかを含み得る。(i) ユニット又は要素が他のユニット又は要素にアクセスして、そこから情報を取得すること、又は、(ii) ユニット又は要素が他のユニット又は要素に、取得又は生成される情報の要求を送り、その情報が要求に回答して取得又は生成されると、その情報が、要求を送ったユニット又は要素に送られること。

【0023】

ユーザがユーザデバイスを使用してクライアントシステムにログインする場合、ユーザデバイスとクライアントシステムの間でのログイン関連情報の生成、転送、格納、又は認証は、第三者による攻撃に対して脆弱であり得る。ユーザデバイス又はクライアントシステムに対する第三者の攻撃の結果、ユーザデバイスとクライアントシステムの間でのログイン関連情報の生成、転送、格納、及び／又は認証の間に、第三者がそのような情報を取得し、及び／又は不正な目的のために使用する可能性がある。例えば、第三者は、取得したログイン情報を使用してクライアントシステムにログインし、それによってクライアントシステムへの不正アクセスを達成したり、クライアントシステムからより多くのログイン関連情報を取得することやその他の方法によって、クライアントシステムに接続されているシステムへと横に移動する可能性がある。別の例としては、第三者は、攻撃によって得られたデータ、ドキュメント、又は取引情報を様々な不正な目的（例えば、他の当事者への情報の流布、市場での優位性を得るための情報の使用、身代金のための情報人質の保持、スパイ行為、破壊など）に利用し得る。本発明は、クライアントシステムの、並びに、クライアントシステムとユーザデバイスの間で生成、転送、及び／又は格納されるデータ、ドキュメント、又は取引情報の不正使用に対するクライアントシステムの脆弱性を減少させる。

30

40

【0024】

本発明の方法は、ユーザが、ユーザデバイスを利用して組織又は個人のクライアントシステムにログインすることを含む。ログイン関連情報は、単一若しくは多層のハッシュ化及び／又は暗号化プロセスを介してハッシュ化及び／又は暗号化される。特に、暗号化及び／又はハッシュ化されたキーの少なくとも一部が生成されて、ユーザのデバイスに格納されてよい。ログイン関連情報の他の固有部分は、環境内の他のデバイスに格納される。

50

複数のデバイス間でログイン関連情報の固有部分が配布されることは、クライアントシステムとユーザデバイス間で転送される情報にアクセスする第三者が、クライアントシステムへのログインを成功させるために必要な情報の一部又は全部を取得することができないことを意味する。

【0025】

更に、現行システムの一態様では、データ、ドキュメント、デバイス、トランザクション、及び／又はユーザを認証するために、ユーザデバイスは、有効なキーを持っていること、及び／又はデバイスが既に認証されていることをクライアントシステムに対して証明する必要がある。これは、本発明では、ユーザデバイスがクライアントシステムにキーを明らかにすることなく達成される。故に、データ、ドキュメント、デバイス、トランザク

10

【0026】

ログイン関連情報は固有に作成され、且つ、格納及び／又は送られない。これは、ユーザデバイス支援マルチポイント認証と共に、第三者によるクライアントシステムへの不正アクセスを防ぐ。

【0027】

先行技術の認証システムの大半は、ユーザデバイスとクライアントシステムの間でのログイン関連情報の作成、格納、転送、及びシングルポイント認証を伴うため、先行技術のシステムは、ログイン関連情報が第三者によって危殆化されることに対して脆弱である。ログイン関連情報が第三者によって入手されてしまうと、その情報は、システムネットワークへのシングル認証ポイントにて認証なしでログインすることに使用され、或いは、データ、ドキュメント、又はトランザクション情報の不正使用に使用される可能性がある。本発明は、クライアントシステムへの、又は、データ、ドキュメント又は取引情報への不正アクセスを可能にするであろう第三者の情報へのアクセスに対して脆弱でないという点で、先行技術のシステムに勝る利点をもたらす。本発明の認証システムは、作成、格納、転送、及び認証ポイントで危殆化される可能性がある先行技術の認証の問題を解決する。

20

【0028】

先行技術のシステムに対する本発明の更なる利点の例としては、先行技術のシステムは一般に、任意のタイプのクライアントシステム、又は任意のタイプのユーザデバイスを用いて操作できないということがある。本発明は、任意のプラットフォーム、ソリューション、又は環境にわたって組織のデータにアクセスするために必要とされる安全なアクセスをユーザに提供するセキュア認証システムを組織にもたらす。本発明は、任意のタイプのクライアントシステムで、そして任意のプラットフォーム上の任意のタイプのユーザデバイスで使用するために、任意の組織によって実施可能である。

30

【0029】

先行技術に対する本発明の利点の更なる例は、本発明が、環境内のデバイスのハイブ（hive）認証を行うために動作することである。例えば、ジオ-テンポラル（geo-temporal）ゾーンにわたる複数のモバイルデバイス及び／又はストレージデバイスを、ハイブ認証の過程で承認することができる。先行技術のシステムは、ジオ-テンポラルゾーンにわたってハイブ承認を行う動作をすることができない。

40

【0030】

本発明の一実施形態は、セキュア部分を有するクライアントシステムへのユーザログインを目的として、又は、ユーザがそのようなシステムのセキュア部分にアクセスすることを目的として、ユーザを認証するために動作する複数の構成要素を含んでよい。例えば、本発明の一実施形態は、以下の3つの主要構成要素を含んでよい：（1）同期多面認証（Synchronized Multi-Faceted Authentication）（SMFA）；（2）対話型半自動認証（Interactive Semi-Manual Authentication）（ISMA）；及び（3）トランザクション認証。本発明のそのような実施形態の例をもたらすために、本発明の実施形態のこれらの3つの構成要素は全て、以下に説明される。当業者が読めば、以下に説明する3

50

つの構成要素のうちの1つ又は2つのみを含む構成、或いは、他の構成要素を組み込む構成のような本発明の他の構成が可能であることを認識するであろう。

【0031】

<同期多面認証 (Synchronized Multi-Faceted Authentication) (SMFA)>

本発明の認証方法及びシステムにおけるユーザのための認証プロセスが動作して、ランダムなマルチユニットのログイン関連情報の暗号化又はハッシュ化された部分が、デバイス (例えば、ユーザデバイス及び／又はシステムデバイス並びに記憶ユニット) の間で配布されて、それらデバイスの全て或いは1又は複数がユーザを認証するために利用される。

【0032】

従って、第三者による不正アクセスのように、ログインデータが作成、転送、格納、又は認証の際に危殆化される場合、未知のユーザの時間依存 (time-sensitive) ランダムログイン関連情報の暗号化又はハッシュ化された一部のみが取得され、このデータはユーザを認証するためには使用できない。

【0033】

より具体的には、本発明は、クライアントシステムにログインするためにチャレンジを行うことをユーザに要求するために動作可能であって、チャレンジは、例えば、ピン及び／又はパターンの静的チャレンジ、アニメーション及び／又は非アニメーションのチャレンジ、グラフィカル及び／又は非グラフィカルなチャレンジ、二次元及び／又は三次元のチャレンジ、動的及び／又は静的なゲーム化チャレンジ、及び／又は非ゲーム化インターフェースのチャレンジなどのチャレンジを行うことをユーザに要求するために動作可能である。システムは、一連のユニットを選択して、それらを用いてチャレンジを生成してよい。各ユニットにはランダムに複数の数字が割り当てられており、それらはログインイベントごとに変更されてよい。ユーザは、同一の認証イベント及び以降の任意の認証イベントにおいて、複数のチャレンジを選択してよい。

【0034】

チャレンジ中に選択された一連のユニットは、認証システムによって複数の固有システム部分に分割される。各ユニット部分におけるユニットは、個別にハッシュ化又は暗号化されてユニット結果を生成してよく、その後、各システム部分のユニットは、集合的にハッシュ化及び／又は暗号化されて、システム部分の結果が生成される。システム部分内の各ユニットに適用されるハッシュ化及び／又は暗号化の数と、各システム部分に適用されるハッシュ化及び／又は暗号化の数は、変化してよい。

【0035】

ハッシュ化及び／又は暗号化された結果の一部は、クライアント又は他のシステムの分散アーキテクチャの様々なデバイスに格納され、一部はユーザのデバイスに格納される。例えば、ハッシュ化及び／又は暗号化された結果の一部は、複数のユーザデバイス及びシステムデバイスに格納されてよい。

【0036】

ハッシュ化及び／又は暗号化された部分データを含むクライアントシステムデバイスの全てとユーザデバイスとは、それら自身を認可しなければならない。デバイスが一旦認証されると、その後、それらのデバイスはユーザを共同認証してもよい。

【0037】

本発明の認証システムは、プラットフォームに依存しないため、どのようなクライアントシステムでも使用できる。

【0038】

<対話型半自動認証 (Interactive Semi-Manual Authentication) (ISMA)>

本発明のユーザのための認証プロセスは、多層暗号化及び／又はハッシュ関数を使用して、ログイン情報が暗号化及び／又はハッシュ化されるように動作する。ランダム暗号化及び／又はハッシュ化の詳細の部分は、隠されて手動送信され、クライアントシステム又はユーザデバイス内に格納されず、これによって、送信、格納、又は認証の間に危殆化する可能性が減少する。

【0039】

本発明のシステムは、キー（即ち、キー#1）をモバイルデバイスに提供する。本発明の全てのキーは、多層暗号化及び／又はハッシュ関数を使用して暗号化及び／又はハッシュ化される。

【0040】

暗号化されたキーは、本発明の認証プロセスで使用するために必要とされ、従って、ユーザは最初に、本明細書に記載のSMFAプロセスを用いて認証を行い、そして、それによってキーを検証して、ユーザのデバイスを認証しなければならない。

【0041】

システムは、ランダム暗号化キーに基づいてチャレンジを生成し、当該キーは、ログインイベントごとに変更される。認証されたユーザは、認証されたデバイスを使用してチャレンジをスキャンする。このプロセスの最後に、ランダム暗号化されたキーの一部又は全部がユーザデバイスに送られる。

10

【0042】

本発明の幾つかの実施形態では、暗号化されたランダムキーの別のセットが存在してよく、当該セットは、ユーザデバイスによって生成されて、ログインイベントごとに変化してもよい。複数のキーが結合されて、暗号化された共有秘密キーが形成され得る。暗号化された共有秘密キーの一部又は全体は、ユーザの認証を要求している組織のクライアントシステムに送られる。

【0043】

暗号化の複数の層は、ユーザデバイスによって生成されてよい。そのような暗号化は、要素に個別に又は纏めて適用されてよい。例えば、ソルト及びivと共にランダムな3桁以上の数字（各ログインイベントの間に变化してよい）がユーザデバイスによって生成されてよく、又は他のタイプの暗号化及び／又はハッシュ化が適用されてよい。暗号化の別の層は、先行する暗号化にまとめて追加されてもよい。

20

【0044】

複数のランダムキャラクタは、複数の層の暗号化の結果として生じるパッケージから削除される。例えば、6つのランダムキャラクタがパッケージから削除されてよい。複数のランダムな数字及びキャラクタがユーザに提供され、暗号化された詳細は、ユーザデバイスの認証を要求しているクライアントシステムに送られる。

30

【0045】

ユーザデバイスの認証を要求するクライアントシステムは、ユーザデバイスに与えられた情報の提供をユーザに要求する。ユーザがそのような情報を提供した場合にのみ、クライアントシステムはユーザを認証できるようになる。このプロセスにより、第三者がユーザのログイン情報を傍受したり、推測したり、知ったりする可能性を減らすことができる。

【0046】

ユーザが認証されると、セッションが、時間ジオベースアクセスコードによって認証される。例えば、ジオベースアクセスコードは、トークン又は他の任意のタイプのジオベースアクセスコードであってよい。時間が経過した場合、又はジオアスペクト（geo aspect）が無効化された場合、ジオベースアクセスコードは無効化されてよい。例えば、ジオアスペクトは、ユーザがジオベースアクセスコードに関連するジオロケーション内に位置していない場合に無効化されてよい。

40

【0047】

<トランザクション認証>

本発明の認証システムのユーザ認証処理は、ユーザがクライアントシステムに自分のキーを明かすことなくトランザクションが認証されるように動作する。クライアントシステムは、ユーザのキーを、又はユーザのキーの有無を知らない。ユーザデバイスは、システムにキーを公開することなく、有効なキーを有していること、及び、ユーザとデバイスが認証されたことをシステムに証明する必要がある。これを達成するために、ユーザデバイスは、本明細書に記載されたSMFAプロセス及び／又は本明細書に記載されたISM

50

Aプロセスを用いて認証する必要がある。ユーザデバイスが認証されると、ユーザデバイスは、それが有している又はそれが受け取ったランダム一時キーを使用してよい。

【0048】

システムはチャレンジを生成する。このチャレンジは、多層暗号化、デジタル署名、及び／又はハッシュ化などの機能を使用して保護されてよい。保護されたパッケージは、認証を要求するユーザデバイスに送られる。ユーザデバイスはパッケージを検証し、ディスプレイに提供された復号キーを使用するか、チャレンジを解決する。

【0049】

ある実施例では、本発明の一実施形態は、システムが、1又は複数の桁が空白である複数のランダム桁数英数字コードを生成するように動作してよく、空白に記入されるべき対応アルファベット又は数字はまた、ISMAプロセスにおけるチャレンジと共にユーザに送られる。例えば、システムは、6桁以上の複数のランダム桁数英数字コードを生成してよく、他の任意の数のランダム桁数英数字コードを生成してよい。

【0050】

システムは、6桁以上のランダム桁数英数字コードに加えて他の要素を生成し、暗号化する。例えば、システムは、6以上のランダム桁数英数字コードを暗号化してよい。更なる暗号化及びセキュリティ機能（ソルト、iv、セキュアキーなどを含むがこれらに限定されない）、クライアントシステムによって適用されてもよい。システムは、その後、暗号化の結果にデジタル署名を追加する。この暗号化されて署名されたパッケージは、認証を要求するユーザデバイスに送られる。

【0051】

ユーザデバイスは、デジタル署名を確認し、そして、提供された復号キーを使用して、対応するアルファベット又は数字と共に6桁以上の英数字コードを再作成する。

【0052】

ユーザデバイスは、その後、セキュリティ機能と共に、再現された情報を暗号化する。次に、ユーザデバイスは、暗号化の結果にデジタル署名を追加する。この暗号化されて署名されたパッケージは、認証プロセスを行うクライアントシステムに送られる。

【0053】

クライアントシステムは、ユーザデバイスからのメッセージを受け取り、メッセージを受け取ると、デジタル署名を検証し、メッセージを復号し、送られたメッセージと比較する。比較により、受け取ったメッセージが送ったメッセージと同じであれば、クライアントシステムは、ユーザが必要なキーを持っていることを知っていることになる。ユーザデバイスが認証されると、セッションは、時間ジオベースアクセスコードによって認証されるが、これらのアクセスコードは、本明細書で既に説明したように、時間が経過すると、又は、ジオが無効になると無効になる。

【0054】

当業者が読めば、本発明の認証のための方法及びシステムは、様々な態様で実施できることを認識するであろう。図1乃至図17は、本発明の幾つかの実施形態の例を示しており、これらは本明細書で説明される。

【0055】

図1に示すように、認証システムは、クライアントシステム、ユーザシステム、検証システム、及び複数の記憶ユニットを含む多くの要素を含んでいる。認証システムは、ユーザのログインを証明する、検証するなどの多くの機能を実現するために動作可能である。

【0056】

ユーザシステム102は、クライアントシステム902にログインするためにユーザによって使用される。ユーザシステムは、本明細書に記載されているように、ユーザのアイデンティティの検証及び他の行為に関与するために動作可能である。ユーザがクライアントシステムの保護された領域へのアクセスを得るためには、ユーザのアイデンティティがクライアントシステムによって検証されなければならない。検証システム202は、クライアントシステムに対するユーザのアイデンティティの検証に従事するように動作可能で

ある。

【0057】

ユーザが、ユーザデバイス90を介して、クライアントシステムのセキュア領域にアクセスすることを希望する場合、ユーザは最初に、クライアントシステムに対してユーザのアイデンティティを証明する必要がある。クライアントシステムがユーザのアイデンティティの証明を受け取ると、システムは、その後、ユーザがクライアントシステムの保護コンテンツにアクセスすることを許可することができる。

【0058】

ユーザは、自分のアイデンティティを証明し、クライアントシステムのセキュア領域へのアクセスを得るためにユーザシステムを使用する。検証システム202は、ユーザのアイデンティティの信憑性を検証するために動作可能である。同期システム300は、1又は複数の同期要素302A・・・302Nの集合であり、ユーザのアイデンティティの信憑性を承認するために同期的に機能するように動作する。

【0059】

ユーザシステムは、複数の要素を含んでよい。本発明の一実施形態では、ユーザシステムは、証明ユニット104、表示ユニット106、処理ユニット108、承認ユニット112、記憶ユニット110、及び通信ユニット114を含んでよい。証明ユニットは、ユーザシステム102の初期アイデンティティを検証システムに証明するために動作可能である。表示ユニットは、例えば、クライアントシステム、検証システム、又は本発明の他のシステム若しくは要素からユーザシステムに転送されたチャレンジ又は他の情報などの情報をユーザに表示するために動作可能である。表示ユニットは更に、クライアントシステムによって生成された情報をユーザに表示するために動作可能である。表示ユニットはまた、入力デバイスに接続されてよく、或いは、タッチスクリーン又は他の入力操作性を有してよく、それによって、ユーザが情報を入力できる。ユーザが入力した情報は、表示ユニットに表示されてよく、さもなければ、ユーザシステムによって収集されて格納されてよく、クライアントシステム又は認証システムの別のシステム若しくは要素に転送されてよく、或いは、ユーザシステムで処理されてよい。処理ユニット108は、システム内の処理能力の全てを担う。承認ユニット112は、チャレンジと応答にアクセスして結果を提供することを担い、記憶ユニットは、一時的データと恒常的データの両方を記憶することを担う。通信ユニット114は、全ての外部通信を担う。

【0060】

検証システム202は、複数の要素を含んでよい。本発明の一実施形態では、検証システムは、マスク（masker）ユニット204、N - パケット生成器206、レポート生成器208、処理ユニット210、承認ユニット212、1又は複数の記憶ユニット214A・・・214N、及び通信ユニット216を含んでよい。マスクユニットは、クライアントシステム及びユーザシステムのために1又は複数の固有の非特定（non-identifying）識別子を生成するために動作する。処理ユニット210は、認証システムが要求するような情報やデータを処理するために動作する。承認ユニット212は、システム内部で受け取った応答にアクセスして、処理ユニットに送られる、又は通信ユニットを介してシステムの外部にある受信機に送られる結果を提供するために動作する。1又は複数の記憶ユニットは、一時的データと恒常的データの両方を記憶するために動作する。N - パケット生成器206は、認証情報のパケットを生成するために動作する。通信ユニット216は、検証システムの外部にある認証システムの全ての要素（即ち、クライアントシステム、ユーザシステムなど）との全ての通信を受信して転送するために動作する。

【0061】

当業者が読むと、本発明の実施形態では、図1の検証システムの要素として記載されているユニットの一部又は全てが、クライアントシステムのような認証システムのその他のシステム又は要素内に含まれてよいことを認識するであろう。本発明の幾つかの実施形態では、図1の検証システムの要素として記載されているユニットの一部又は全ては、スタンドアロンの要素であってよく、認証システムの如何なるシステムにも含まれていないが

、概ね認証システムに含まれていてよい。

【0062】

同期システム300は、1又は複数の同期要素302A・・・302Nを含んでよく、各同期要素は、複数のユニットを含んでよい。本発明の一実施形態では、少なくとも2つの同期要素は、証明ユニット304A・・・304N、記憶ユニット308A・・・308N、処理ユニット306A・・・306N、承認ユニット312A・・・312N、及び通信ユニット310A・・・310Nを含んでよい。証明ユニット304Aは、同期システム300の初期アイデンティティを検証システム202に証明するために動作する。

【0063】

ユーザシステム、検証システム、及び同期要素の間の通信は、そのようなシステム及び／又は要素の通信ユニットによって受信され、且つ、そのようなシステム及び／又は要素から転送される。システム及び／又は要素間のそのような通信の全ては、1又は複数のマスキング機能の使用によって保護されてよく、1又は複数のマスキング機能は、ハッシュ化及び／又は暗号化を含んでよい。

【0064】

図2に示すように、データは、クライアントシステム902と検証システムのマスカユニット204との間で、検証システムの通信ユニット216を介して転送されてよい。クライアントシステムと検証システムの間における、クライアントシステムを使用したい新規ユーザのセットアップに関連する最初の通信中に、クライアントシステムは、検証システムのマスカユニットと通信して、クライアントシステムとの保護された接続を確立するために新規ユーザに求められる資格情報を要求してよい。マスカユニットは、固有の保護された資格情報を生成し、クライアントシステムは当該資格情報を使用して、クライアントシステムと検証システムとの間のリンクを確立する。これらの固有の資格情報は、例えば、クライアントID、又は他の形態の資格情報を含んでよい。

【0065】

クライアントシステムと検証システムの間で信頼された接続が確立されると、マスカユニットは、演算、アルゴリズム、又は別のタイプのプロセスを実行して、ユーザには秘密である固有の非特定識別子を生成する。固有の非特定識別子は、検証システムに含まれる記憶ユニット214A（又は記憶ユニット214A・・・214Nの何れか）の1つに格納されてよい。

【0066】

マスカユニットは、ハッシュ化、暗号化、又は何らかの他のマスキング機能を使用して、非特定識別子をセキュアにしてよい。また、クライアントシステムは、利用可能な全ての同期要素のリストを検証システムに提供してよい。本発明の実施形態では、同期要素の1又複数は、検証システムの記憶ユニット214A・・・214Nの1又複数に格納されてよい。

【0067】

図3に示すように、本発明の登録プロセスは、ユーザがクライアントシステムに登録するために、ユーザと認証システムの初期対話中に必要とされる認証システムの要素の動作を含んでよい。クライアントシステム、ユーザシステムの要素、検証システムの要素、及び同期システムの要素間の全ての通信は、図3に示すように、ユーザシステム、検証システム、及び同期システムの通信ユニットを介して行われる。ユーザは、クライアントシステムのセキュア部分へのアクセスを許可されるためには、クライアントシステムに登録しなければならない。初期登録中、証明ユニット104は、証明情報を取得するためにクライアントシステムの1又は複数の記憶ユニット110にアクセスする。証明情報は、マスカユニットによって生成された非特定識別子、マスカユニットによって生成された秘密、及びユーザデバイスを識別し得る情報、並びに／或いは、固有のアプリケーション番号、又は、例えば生体情報（例えば、ユーザの指紋、ユーザの網膜スキャン、又はユーザの他の生体情報）や使用情報のようなユーザに関連する他の情報を含んでよい。証明ユニットが証明情報の全てを取得すると、証明情報は、ユーザシステムの1又は複数の記憶ユニッ

10

20

30

40

50

トに記憶されてよい。

【0068】

証明ユニット104が取得した証明情報は、ユーザシステムの通信ユニット114を介して、検証システムの処理ユニット210に安全に送られる。処理ユニット210は、検証システムの通信ユニット216を介して、検証システムの1又は複数の記憶ユニット214A・・・214Nから、ユーザの情報を取得する。処理ユニット210は、クライアントシステムから受け取った情報と、検証システムの1又は複数の記憶ユニットから取得した情報とを組み合わせ、情報のパッケージを作成する。処理ユニットは、そのような情報パッケージを承認ユニット212に送る。

【0069】

承認ユニット212は、先にクライアントシステムから受け取っており、検証システムの1又は複数の記憶ユニット214A・・・214Nに格納されている情報と、処理ユニットから受け取った情報パッケージの値を比較する。比較が成功する場合、承認ユニットは、ユーザシステムとの接続を受け入れる。比較が成功しない場合、承認ユニット212は、ユーザシステムとの接続を拒否する。承認システムの結果は、N-パケット生成器206に送られる。

【0070】

ユーザシステムとの接続が承認されない場合、ユーザを登録することを試みる認証システムの動作は終了する。本発明の一実施形態では、ユーザシステムとの接続が承認されると、N-パケット生成器は、ランダムチャレンジを生成する。ランダムチャレンジは、複数のパケット(N-パケット)を含んでよい。各Nパケットは、複数のランダム数字又は英数字/他のキャラクタ(N-RANC)を含む。

【0071】

N-パケットは、ユーザシステムの表示ユニット106に安全に送られる。本発明の実施形態では、これらに限定されないが、N-暗号化、ハッシュ化及び/又はデジタル署名を含む多層の保護を適用して、パケット生成器と表示ユニットの間で転送される中のN-パケットに保護が、例えば、転送前にN-RNAC及びN-パケットの両方の多層保護が適用されてよい。本発明の他の実施形態では、N-パケットは、N-RNACの有無に拘わらず、ユーザシステム又は別のシステムの要素によって生成できるであろう。ユーザは、この要素と対話して、OYパケットを生成する。

【0072】

表示ユニット106は、N-パケットを受け取り、N-パケットに含まれる情報をユーザに表示する。表示されたN-パケットから、ユーザは、1又は複数のN-パケットを入力し、それにより、選択されたN-パケットに関連するN-RANCを選択する。参照を容易にするために、ユーザによって選択されたN-パケットは、本明細書ではY-パケットとする。ユーザによって選択されたY-パケットの順序は、順序付け(Ordered)Y-パケット(OY-パケット)となるように保持される。OY-パケットは、表示ユニット106によってユーザシステムの処理ユニット108に送られる。ユーザシステムの処理ユニットは、OY-パケットを2つ以上の部分に分割する。各部分は、2つ以上のN-パケットを含んでいてよい。

【0073】

ユーザシステムの処理ユニットは、OY-パケットの各部分にマスキング機能を適用することにより、OY-パケットの情報をマスキングしてよい。例えば、ユーザシステムの処理ユニットは、OY-パケットに含まれるN-RNACの各々、及び/又はOY-パケットに含まれるY-パケットの各々、及び/又はOY-パケットの各々のうちの1又は複数のマスキングを適用してよい。1又は複数のマスキングの結果は、ユーザシステムの1又は複数の記憶ユニット110に格納されてよい。格納されない結果は、検証システムの処理デバイスに送られる。

【0074】

N-パケット生成器によって生成されたチャレンジは、ユーザシステムの表示ユニット

10

20

30

40

50

に送られ、複数のN - パケットを含んでおり、各Nパケットは、3つ以上のN - R A N Cを含んでよい。ユーザは、O Y - パケットを形成する複数のY - パケットを選択してよい。O Y パケットは、2つの部分（即ち、O Y A - 部とO Y B - 部）に分割されてよい。

【0075】

検証システムの処理ユニットは、ハッシュ化及び／又は暗号化を適用し、そして、検証システムの1又は複数の記憶ユニットに格納されたリストから、同期システムの2つ以上のランダム同期要素を選択してもよい。選択されたランダム同期要素は、同期レジストリを形成する。検証システムの処理ユニットは、個別に又は纏めてO Y - パケット部分に秘密を追加してよく、個別に及び／又は纏めてO Y - パケット部分に多層ハッシュ化及び／又は暗号化機能を実行してよい。次に、ハッシュ化及び／又は暗号化された固有のO Y - パケット部分は、1又は複数の同期要素の間で配布され、O Y - パケット部分が配布される1又は複数の同期要素の1又は複数の記憶ユニットに格納されてよい。その結果、固有のO Y - パケット部分が様々な同期要素に格納される。配布された情報部分は、同期要素の同期レジストリに格納されてよい。

【0076】

図4に示すように、認証システムは、ユーザがクライアントシステムのセキュア部分へのアクセスを得るために、アクセスプロセスを実行するように動作してよく、それによって、登録されたユーザは、検証システムの動作を通じて自分自身を認証させることを試みる。ユーザシステムの要素と、検証システムの要素と、同期システムの要素との間での全ての通信は、図4に示すように、ユーザシステムの通信ユニットと、検証システムの通信ユニットと、同期システムの同期要素の通信ユニットとを介して行われる。ユーザシステムの証明ユニット104は、ユーザシステムの記憶ユニット110の1又は複数にアクセスして証明情報を取得する。証明情報は、非特定識別子及び秘密を含んでよい。

【0077】

証明ユニットが取得した証明情報の一部又は全部は、検証システムの通信ユニット216を介して、ユーザシステムの通信ユニット114から検証システムの処理ユニット210に安全に送られる。処理ユニット210は、検証システムの記憶ユニット214A・・・214Nにおける1又は複数からユーザのための情報を取得する。処理ユニット210は、クライアントシステムから受け取った情報と、検証システムの1又は複数の記憶ユニットから取得した情報とを組み合わせ、情報のパッケージを作成する。処理ユニットは、この情報のパッケージを検証システムの承認ユニット212に送る。

【0078】

承認ユニット212は、処理ユニット210から受け取った情報のパッケージの値を、クライアントシステムから先に受け取っており、検証システムに格納されている情報と比較する。比較が成功した場合（即ち、比較の結果、比較された情報の間での一致が得られた場合）、承認ユニットは、ユーザシステムとの接続を受け入れる。比較が成功しない場合、承認ユニットはユーザシステムとの接続を拒否する。承認システムの結果は、N - パケット生成器206に送られる。

【0079】

ユーザシステムとの接続が承認されなかった場合、ユーザを登録することを試みる認証システムの動作は終了する。ユーザシステムとの接続が承認された場合、N - パケット生成器は、ランダムチャレンジを生成する。ランダムチャレンジは、2つ以上のパケット（N - パケット）を含んでよい。各N - パケットは、更に2つ以上のランダムな数又は英数字（N - R A N C）を含む。多層ハッシュ化及び／又は暗号化が、表示ユニットに送られるチャレンジに適用されてよい。ハッシュ化及び／又は暗号化は、乱数発生器を用いて適用されてよい。

【0080】

N - パケットは、ユーザシステムの表示ユニット106に安全に送られる。本発明の実施形態は、多層ハッシュ化及び／又は暗号化を適用して、N - パケット生成器と表示ユニットの間でトランジット中のN - パケットを保護してよい。例えば、多層ハッシュ化及び

10

20

30

40

50

／又は暗号化は、転送に先立ってN - R N A C及び／又はN - パケットをハッシュ化及び／又は暗号化することを含んでよい。表示ユニット106は、N - パケットを受け取り、対応情報をユーザに表示する。表示された対応情報から、ユーザは、2つ以上の対応情報を選択し、N - パケットを選択すると、N - R A N Cが、選択されたN - ブラケットに関連付けられる。参照を容易にするために、ユーザによって選択されたN - パケットは、ここではY - パケットであって、これらのYパケットは順序付けられており、O Yパケットと称される。

【0081】

本発明の別の実施形態では、N - パケット生成器は、ユーザシステム又は他のシステムに存在してよく、当該システムは、ユーザシステム又は他のシステムからの任意の要素、例えばカメラ、スキャナなどを介してユーザとの対話によってYパケット及び／又はO Yパケットを生成してよい。

【0082】

O Yパケットは、表示ユニット106によってユーザシステムの処理ユニット108に送られる。ユーザシステムの処理ユニットは、O Y - パケットを複数の部分に分割する。各部分は、複数のN - パケットを含んでいる。

【0083】

ユーザシステムの処理ユニット108は、ユーザシステムの1又は複数の記憶ユニットから以前に格納されたO Y - パケット部分を取り出す。当該記憶ユニットには、そのような以前に格納されたO Y - パケット部分が格納されている。処理ユニットは、以前に格納されたO Y - パケット部分と、より最近に作成されたO Y - パケット部分とを、ユーザシステムの承認ユニット110に送る。ユーザシステムの承認ユニットは、ユーザシステムの処理ユニットから受け取った情報を、以前に格納されたO Y - パケット部分と比較して、承認結果又は否認結果の何れかを生成する。ユーザシステムの承認ユニットが生成した結果（承認結果又は否認結果の何れかである）は、ユーザシステムの処理ユニットに転送される。ユーザシステムの承認ユニットからの結果が否認結果の場合は、認証処理が停止される。

【0084】

ユーザシステムの承認ユニットの結果が承認結果である場合、ユーザシステムの処理ユニットは、新しく生成されたO Yパケット部分のうちの1又は複数のO Yパケット部分を、ユーザシステムの1又は複数の記憶ユニットに格納してよく、残りのO Yパケット部分を検証システムの処理ユニットに送る。検証システムの処理ユニットは、ユーザのために同期システム情報を同期レジストリから取得する。検証システムの処理ユニットは、受け取ったO Yパケット部分に秘密を追加して、これらのO Yパケット部分に多層ハッシュ化及び／又は暗号化機能を実行してよい。ハッシュ化及び／又は暗号化後、検証システムの処理ユニットは、ハッシュ化及び／又は暗号化された固有のO Yパケット部分を、同期システムの同期要素の処理ユニット302A・・・320Nの1又は複数に送ってよい。同期要素の各処理ユニットは、ハッシュ化された及び／又は暗号化された固有のO Yパケット部分を、検証システムの処理ユニット210から受け取る。ハッシュ化された及び／又は暗号化されたO Yパケット部分を受け取った同期化要素の各処理ユニットは、図5に示すように処理を行ってよい。同期要素の処理ユニット306A・・・306Nは、ハッシュ化及び／又は暗号化を復号して、1又は複数のN - パケット及びN - R A N Cを決定し、識別してよい。同期要素の処理ユニットは、同じ同期要素の承認ユニット312A・・・312NにN - パケット及びN - R A N Cを送ってよい。

【0085】

同期ユニットの証明ユニット304A・・・304Nは、同期要素の記憶ユニット308A・・・308Nから、以前に格納されたハッシュ化及び／又は暗号化O Y - パケット部分を取り出す。同期ユニットの証明ユニットは、ハッシュ化及び／又は暗号化を復号して、1又は複数のN - パケット及びN - R A N Cを決定及び識別してよく、当該N - パケット及びN - R A N Cは、同期要素の承認ユニットに送られる。同期要素の承認ユニット

10

20

30

40

50

は、受け取った最近生成されたN - パケット及びN - R A N Cを、以前に格納されたものと比較する。この比較に基づいて、パス値又はフェイル値が生成される。生成されたパス値又はフェイル値は、同期要素の証明ユニットに転送される。

【0086】

同期ユニットの証明ユニットは、同期ユニットの1又は複数の記憶ユニットから証明情報を取得し、前記証明情報と、証明ユニットが受け取ったパス値又はフェイル値との両方をハッシュ化及び／又は暗号化して、検証システムの処理ユニットに送ってよい。

【0087】

検証システムの処理ユニットは、ハッシュ化及び／又は暗号化された結果及び証明情報を、その情報を生成した同期要素の各々の証明ユニットから受け取る。明確にすると、複数の同期要素は、固有のO Y - パケット部分を受け取ってよく、それら同期要素の各々は、本明細書で説明されている方法に従ってO Y - パケット部分を処理するであろう。ユーザシステムの要素と、検証システムの要素と、クライアントシステムの要素との間の全ての通信は、図6に示すように、ユーザシステム、クライアントシステム、及び検証システムにおける通信ユニットを介して行われる。また、図6に示すように、検証システム202の処理ユニット210は、各同期要素302A・・・302Nから受け取った証明情報を復号し、復号された情報を検証システムの承認ユニット212に送る。検証システムの処理ユニット210は、検証システムの1又は複数の記憶ユニット214A・・・214Nから証明情報を取得する。検証システムの処理ユニットは、取得した証明情報を検証システムの承認ユニットに送る。検証システムの承認ユニットは、受け取った情報を用いて同期要素を承認する。

【0088】

検証システムの処理ユニットは、同期要素から受け取ったパス値及び／又はフェイル値の各々を復号する。復号された値は、検証システムの1又は複数の記憶ユニットに検証結果として保存される。検証結果レポートが、検証システムの処理ユニット又はレポート生成器208によって生成されてよく、このレポートは、様々な情報、例えば、要求された総同期要素、受け取ったパス値の数、受け取ったフェイル値の数、同期システムの信頼スコア、及び他の情報を含んでよい。

【0089】

検証システムの処理ユニットは、検証結果をハッシュ化又は暗号化し、ハッシュ化及び／又は暗号化された検証結果を、検証システムの通信ユニット216を介して、ユーザシステム102の処理ユニット108に送ってよい。ユーザシステムの処理ユニットは、ハッシュ化又は暗号化された検証結果をクライアントシステム902に送る。クライアントシステムは、クライアントシステムが受け取る検証結果に基づいて、検証システムの処理ユニット210に認証要求を検証システムの通信ユニット216を介して送る。検証システムの処理ユニットは、検証システムの1又は複数の記憶ユニットに保存されている検証結果を取得し、取得した検証結果を検証システムの承認ユニットに送る。検証システムの承認ユニットは、取得した検証結果を検討し、これらを承認してクライアントシステムに検証結果を送ってよい。クライアントシステムは、検証報告の結果に基づいてユーザを認証するか否かを決定する。

【0090】

ユーザが認証されて、クライアントシステムのセキュア部分へのアクセスが許可された後、ユーザは情報（即ち、データ、ドキュメント、取引情報など）にアクセスすること、及び／又はユーザ情報（即ち、テキスト、データなど）をクライアントシステムに提供することができる。ある例では、ユーザは、メッセージを送るために、クレジットカードによる支払いを伴う購入を行うために、電子署名を文書に添付するために、又は他の様々な目的のために、クライアントシステムにアクセスしてよい。ユーザシステムを用いたユーザとクライアントシステムとの対話の過程で、ユーザ情報がクライアントシステムとユーザシステムとの間で送られる。本発明は、このようなユーザ情報及び認証関連情報の作成、転送、格納及び認証の間のセキュリティを保護するために動作する。

【0091】

このようなセキュリティを達成するために、本発明の実施形態は、ユーザシステム、クライアントシステム、クライアント表示ユニット、及び検証システムを含んでよい。ユーザシステムは、クライアントデバイスに全体として又は部分的に含まれてよく、クライアントデバイスは、ユーザによって、クライアントシステムと通信し、クライアントシステムにアクセスするために利用される。当業者が読めば、本発明の実施形態は、ユーザデバイスとクライアントシステムとの間で転送されるユーザ認証関連情報のセキュリティを達成するものであって、また、他の要素を含んでよいことを認識するであろう。

【0092】

ユーザは、ユーザデバイスを使用して、クライアントシステムに対してユーザシステムとユーザ資格情報を検証する。ユーザがクライアントシステムのセキュア部分へのアクセスを許可されていることを確認するためには、ユーザ資格情報とユーザシステムは検証される必要がある。ユーザは、ユーザが認証されている場合、クライアントシステムのセキュア部分を介して特定の機能を実行し、又は、特定の情報にアクセスできるだけであろう。例えば、ユーザは、ユーザ及びユーザシステムが認証されている場合には、クライアントシステムを介して特定のトランザクションを承認できるだけであろう。クライアントシステムは、ユーザがアクセスを試みているシステムであり、従って、認証が実行されることを求める。本発明の検証システムは、ユーザ及びユーザシステムのアイデンティティを検証し、本明細書に記載されているように、ユーザ及びユーザシステムを認証されたものとしてクライアントシステムに認識させる。

【0093】

図7に示すように、ユーザシステム101は、クライアントシステムとの間でユーザ情報を転送するために利用されるものであって、複数の要素を含んでよい。例えば、本発明の一実施形態は、対話ユニット103、ベリファイア(verifier)生成器105、ノイズ生成器107、処理ユニット109、記憶ユニット111、及びリーダ(reader)ユニット113が組み込まれたユーザシステムを含んでよい。

【0094】

図8に示すように、本発明の一実施形態のクライアントシステム130は、複数の要素を含んでよい。例えば、本発明の一実施形態は、CSAP生成器131、記憶ユニット133、処理ユニット135、チャレンジ生成器137、及び承認ユニット139が組み込まれたクライアントシステムを含んでよい。

【0095】

図9に示すように、本発明の一実施形態のクライアント表示ユニット150は、複数の要素を含んでよい。例えば、本発明の実施形態は、対話ユニット151、処理ユニット153、一時記憶ユニット155、及びキー生成器157が組み込まれたクライアント表示ユニットを含んでよい。

【0096】

図10に示すように、本発明の一実施形態の検証システム140は、複数の要素を含んでよい。例えば、本発明の実施形態は、ランダムキー生成器141、ランダムテキスト生成器143、USID生成器145、及び処理ユニット147が組み込まれた検証システムを含んでよい。

【0097】

ユーザがクライアントシステムのセキュア部分へのログインを希望すると、ユーザは、クライアント表示ユニットとの対話によりその意志を宣言し、クライアント表示ユニットの対話ユニットを使用して要求を入力する。図11に示すように、対話ユニット151は、クライアント表示ユニットの処理ユニット153に要求を伝達し、クライアント表示ユニットの処理ユニットは、その後、検証システムの処理ユニット147に要求を伝達する。ユーザシステムの処理ユニット109は、アルファキー(αk)コンボを生成する要求を生成する。アルファキー(αk)コンボ(combo)は $\alpha k1$ 及び $\alpha k2$ からなり、検証システムの処理ユニット147を介してクライアント表示ユニットのキー生成器157に

送られる。クライアント表示ユニットのキー生成器 1 5 7 は、 $\alpha k 1$ 及び $\alpha k 2$ の両方を検証システムの処理ユニット 1 4 7 に送る。

【0098】

次に、検証システムの処理ユニット 1 4 7 は、検証システムのランダムテキスト生成器 1 4 3 にランダムテキストを要求し、検証システムの U S I D 生成器 1 4 5 に固有のシステム・イベント識別子 (U S I D) を要求する。ランダムテキスト生成器は、ランダムテキストを生成して検証システムの処理ユニット 1 4 7 に送る。U S I D 生成器は、U S I D を生成して検証システムの処理ユニットに送る。U S I D 生成器は、ユーザデバイスと、クライアントシステム内のセキュア領域に接続しようとしているイベントとを検証システムに特定するために動作する。U S I D は、1 又は複数のブラウザ内の各タブに固有のものであってよく、ユーザが使用するために開いているブラウザやタブの数を特定して制御する。

10

【0099】

検証システムの処理ユニット 1 4 7 は、 $\alpha k 2$ と共に受け取った U S I D とランダムテキストを結合してデータ列にして、そのデータ列を機械可読形式に変換し、その後、これをクライアント表示ユニットの処理ユニット 1 5 3 に送る。クライアント表示ユニットの対話ユニット 1 5 1 は、この情報をユーザシステムのリーダユニット 1 1 3 に利用可能にする。

【0100】

図 1 2 に示すように、図 1 1 のプロセスが完了した後、情報は、リーダユニット 1 1 3 を介してユーザシステムに利用可能になっている。リーダユニット 1 1 3 は、聴覚、視覚、触覚、プリント、動き、及び他の種類のセンサの何れかを含む 1 又は複数のセンサを含んでいてよい。それらセンサは、クライアントデバイスに組み込まれてよく、又は、クライアントデバイスの外部に組み込まれて、有線接続又は無線接続の何れかを介して接続されてよい。それらセンサは、ユーザに関連する情報を得るために利用されてもよい。

20

【0101】

リーダユニット 1 1 3 は、その後、取得した情報をユーザシステムの処理ユニット 1 0 9 に送る。ユーザシステムの処理ユニットは、リーダユニットから受け取った情報を分割してよく、その情報を保持してよい。ユーザシステムの処理ユニット 1 0 9 は、ユーザシステムのノイズ生成器 1 0 7 にノイズを要求する。ノイズ生成器は、ノイズを発生させて、そのノイズをユーザシステムの処理ユニットに送る。このノイズは、転送中の情報のアイデンティティをマスキングするために使用される。

30

【0102】

ユーザが以前にクライアントシステムで認証されたことがあるならば、ユーザシステムは、ランダムなデルタ 1 キー ($\delta k 1$) を有し得る。

【0103】

ユーザシステムの処理ユニットは、ユーザシステムのベリファイア生成器 1 0 5 に $\alpha k 2$ 及び $\delta k 1$ を送る。また、処理ユニットは、ユーザシステムのベリファイア生成器に、新しいベータキーを生成するように求める要求を送る。この要求に応答して、ベリファイア生成器は、 $\alpha k 2$ 及び $\delta k 1$ を用いてベータキー 1 ($\beta k 1$) 及びベータキー 2 ($\beta k 2$) を生成する。ベリファイア生成器 1 0 5 は、 $\beta k 1$ 及び $\beta k 2$ をユーザシステムの処理ユニット 1 0 9 に送る。

40

【0104】

ユーザシステムの処理ユニットは更に、ユーザシステムの記憶ユニット 1 1 1 にアクセスして、デルタ 1 キー及び／又はセッションコード及び／又はセッションコードの生成を要求する。記憶ユニット 1 1 1 は、ユーザシステムの処理ユニットにデルタ 1 キーを提供し、又は、セッションコードを生成して、これをユーザシステムの処理ユニットに提供する。例えば、ユーザシステムの処理ユニット 1 0 9 は、検証システムのランダムキー生成器 1 4 1 がランダムなデルタ 1 キー及び／又はセッションコードの生成を要求し、これを処理ユニット 1 0 9 に提供することを要求してよく、処理ユニット 1 0 9 は、提供される

50

$\delta k 1$ 又はSCのためのハッシュ値を生成してよい。

【0105】

ユーザシステムの処理ユニットは、ノイズ発生器、ユーザシステムの記憶ユニット、及びベリファイア生成器の各々から得られた情報を用いて、手動対話コード(MIC)を生成してもよい。ユーザシステムの処理ユニットは、ユーザシステムの対話ユニット103にMICを送ってよい。クライアント表示ユニットの対話ユニット103は、ユーザにMICを表示する。

【0106】

MICが生成される場合、残留データ(「ポスト-MICデータ」)が存在する。ユーザシステムの処理ユニットは、ポスト-MICデータに対して対称暗号化又は非対称暗号化を行ってよい。ユーザシステムの処理ユニットは、ポスト-MICデータとハッシュ値をクライアントシステムの処理ユニット135に送ってよい。

【0107】

図13に示すように、MIC、ポスト-MICデータ及びハッシュ値がユーザシステムによって生成されると、クライアントシステムの処理ユニット135は、ポスト-MICデータ及びハッシュ値を受け取る。クライアントシステムの処理ユニット135は、ハッシュ値を送り、そのハッシュ値はクライアントシステムの記憶ユニット133に一時的に格納される。ポスト-MICデータは、クライアント表示ユニットの処理ユニット153に送られる。

【0108】

クライアント表示ユニットの処理ユニット153は、 $\alpha k 1$ とポスト-MICデータをパッケージとして結合して、そのパッケージをクライアント表示ユニットのキー生成器157に送る。処理ユニット153は、クライアント表示ユニットのキー生成器157にガンマキー(γK)の生成を要求する。 γK は、クライアント表示ユニットのキー生成器157によってクライアント表示ユニットの処理ユニット153に送られる。

【0109】

そして、ユーザは、クライアント表示ユニットの対話ユニット151と対話することが要求される。ユーザは、MICを手動で入力する必要がある。入力されると、その後、MICは、クライアント表示ユニットの対話ユニットによって、クライアント表示ユニットの処理ユニット153に送られる。処理ユニット153は、 γK 、MIC、及びパッケージを使用して、SC又は $\delta k 1$ を使用可能にする。クライアント表示ユニットの処理ユニットは、SC又は $\delta k 1$ のハッシュ値を計算して、そのハッシュ値を検証のためにクライアントシステムの承認ユニット139に送る。

【0110】

クライアント表示ユニットの処理ユニットが受け取った又は生成した情報の何れも、クライアント表示ユニットの処理ユニット153の処理動作中の任意の時点にて、クライアント表示ユニットの一時記憶ユニット155に一時的に格納されてよい。

【0111】

クライアントシステムの処理ユニット135は、クライアントシステムの記憶ユニット133に一時的に格納されているハッシュ値を取得する。クライアントシステムの処理ユニット135は、SC又は $\delta k 1$ のハッシュ値の何れかと、記憶ユニットから取り出した値とを、クライアントシステムの承認ユニット139に送る。承認ユニット139は、ハッシュ値を比較して一致を判定する。

【0112】

ハッシュ値が一致する場合、承認ユニット139は、クライアントシステムの処理ユニット135に一致を伝える。

【0113】

図14に示すように、この一致確認を受け取ると、クライアントシステムの処理ユニット135は、クライアントセッションアクセスパス(Client Session Access Pass)(CSAP)をCSAP生成器131に要求する。CSAP生成器131は、CSAPを生

10

20

30

40

50

成し、CSAPは、クライアントシステムの記憶ユニット133に送られて、一時的に格納される。CSAP生成器131はまた、検証システムの処理ユニット147にCSAPを送る。検証システムの処理ユニット147は、クライアント表示ユニットの処理ユニット153にCSAPを送る。クライアント表示ユニットの処理ユニット153は、ユーザシステムの処理ユニット135にCSAPを送る。ユーザシステムの処理ユニット135は、クライアントシステムの承認ユニット139にCSAPを送る。クライアントシステムの承認ユニットは、CSAPを確認する。ユーザシステムの処理ユニットはその確認の通知を受け取って、ユーザがクライアントシステムのセキュア部分にアクセスすることを許可するように動作する。

【0114】

クライアントシステムの承認ユニット139が、値が一致しないと判定した場合、ユーザ、ユーザシステム及びクライアント表示ユニットは認証されない。

【0115】

クライアントシステムのCSAP生成器131は、ユーザ、ユーザシステム及びクライアント表示ユニットの認証に関連する条件を周期的にテストするために使用されてよい。これは、本明細書に記載された方法に従って、CSAPの生成と、クライアントシステムの処理ユニットによるその処理と、検証システム、ユーザシステム、クライアント表示ユニットの他の処理ユニットへのCSAPの転送と、クライアントシステム、ユーザシステム、及びクライアント表示ユニットの記憶ユニットへのCSAPの格納とを介してなされる。クライアントシステムの承認ユニットが、認証条件がCSAPに関して満たされていないと判断する場合、例えば、クライアントシステムの処理ユニットが受け取ったCSAPと格納されているCSAPとが一致しないとの判断の場合、ユーザ、ユーザデバイス及びクライアント表示ユニットの認証（即ち、CSAP認証）が取り消され、ユーザ、ユーザデバイス及びクライアント表示ユニットについてセキュア領域へのアクセスが終了する。

【0116】

本発明の実施形態で採用される認証用CSAP条件は、次元、ジオ - テンポラル、機械学習人工知能、行動、又はその他の条件の何れかに関連する条件を含んでよい。

【0117】

図15に示す本発明の別の実施形態では、ユーザは、クライアント表示ユニットを使用して、クライアントシステムのセキュア部分へのアクセスを介してトランザクションを有効にすることを試みる。クライアント表示ユニットの処理ユニット153は、クライアントシステムの処理ユニット135にトランザクションを有効にする要求を送る。その要求に応じて、クライアントシステムの処理ユニット135は、チャレンジを生成する要求をクライアントシステムのチャレンジ生成器137に送る。この要求に応じて、クライアントシステムのチャレンジ生成器137は、チャレンジを生成し、更には、チャレンジの結果にハッシュ値を適用して、解答及び／又はハッシュ値をクライアントシステムの記憶ユニット133に保存してよい。クライアントシステムのチャレンジ生成器137は、クライアントシステムの処理ユニット135にチャレンジを送る。

【0118】

クライアントシステムの処理ユニット135は、対称及び／又は非対称暗号化をチャレンジに適用してよい。処理ユニット135は、クライアント表示ユニットの処理ユニット153にチャレンジを送る。クライアント表示ユニットの処理ユニット153は、提供されたキーを用いてチャレンジを復号してよく、そして、クライアント表示ユニットの対話ユニット151にチャレンジを送る。本発明の一実施形態では、ユーザは、クライアント表示ユニットの対話ユニット151と対話して、チャレンジの解答を見つけることを要求されてよい。本発明の別の実施形態では、クライアント表示ユニットの処理ユニット153は、復号されたチャレンジを解決してよい。

【0119】

クライアント表示ユニットを使用するユーザがチャレンジの解答を見つけると、そのユーザの解答は、クライアント表示ユニットの処理ユニット153に送られる。クライアン

10

20

30

40

50

ト表示ユニットの処理ユニット153は、ユーザの解答に基づいてハッシュ値を生成してよく、クライアント表示ユニットの処理ユニットは更に、このハッシュ値及び／又は解答に対称暗号化又は非対称暗号化の何れかを加えてよい。クライアント表示ユニットの処理ユニットによる処理の結果（例えば、ハッシュ値又は暗号化されたハッシュ値、或いは、解答又は暗号化された解答）は、クライアントシステムの処理ユニット135に送られてよい。クライアントシステムの処理ユニット135は、格納されている解答及び／又はハッシュ値を取得するための要求をクライアントシステムの記憶ユニット133に送ってよい。この要求があると、クライアントシステムの記憶ユニット133は、格納されている解答及び／又は格納されているハッシュ値を取得し、格納されている解答及び／又は格納されているハッシュ値をクライアントシステムの処理ユニット135に送る。

10

【0120】

クライアントシステムの処理ユニット135は、クライアント表示ユニットの処理ユニット153から受け取った、暗号化されたハッシュ値若しくは解答及び／又は非暗号化されたハッシュ値を復号する。クライアントシステムの処理ユニット135は、クライアント表示ユニットの処理ユニット153から受け取ったハッシュ値及び／又は解答（暗号化されていない形式）と、格納されている解答及び／又はハッシュ値とを、承認のためにクライアントシステムの承認ユニット139に送る。クライアントシステムの承認ユニット139は、受け取った解答を格納されている解答と、及び／又は受け取ったハッシュ値を格納されているハッシュ値と比較する。

【0121】

受け取った解答及び／又はハッシュ値が、格納されている解答及び／又はハッシュ値と一致する場合、承認ユニット139は、クライアントシステムの処理ユニット135に一致の確認を送る。一致が確かである場合、クライアントシステムの処理ユニット135は、トランザクションの認証が正常に完了したことを確認するために、一致の確認をクライアントシステムに送り、クライアントシステムはそれによってトランザクションを承認する。

20

【0122】

受け取った解答及び／又はハッシュ値が、格納されている解答及び／又はハッシュ値と一致しない場合、承認ユニット139は、一致しない旨の通知をクライアントシステムの処理ユニット135に送る。クライアントシステムの処理ユニットは、その通知をクライアントシステムに送り、クライアントシステムにトランザクションの認証を行わないように通知する。

30

【0123】

本発明の別の実施形態では、検証システムの処理ユニットは、図14を参照してクライアントシステムの処理ユニットについて説明した機能を実行することができる。本発明のそのような実施形態では、チャレンジ生成器及び承認ユニットは、クライアントシステム又は検証システムの何れかに含まれてよく、それらチャレンジ生成器及び承認ユニットは、図14に従って説明されたものと同じチャレンジ生成器137及び承認ユニット139の機能を有する。

【0124】

ユーザがユーザシステムを使用してトランザクションを有効にすることを試みる本発明の別の実施形態を図16に示す。本発明のこのような実施形態では、ユーザシステムの処理ユニット109は、クライアントシステムの処理ユニット135にトランザクションを有効にする要求を送る。その要求に応じて、クライアントシステムの処理ユニット135は、チャレンジを生成する要求をチャレンジ生成器137に送る。この要求に応じて、チャレンジ生成器137はチャレンジを生成し、更には、チャレンジの結果（チャレンジの解答）にハッシュ値を適用し、その解答及び／又はハッシュ値をクライアントシステムの記憶ユニット133に保存する。

40

【0125】

クライアントシステムの処理ユニット135は、チャレンジに対称及び／又は非対称暗

50

号化を適用してよい。処理ユニット135は、暗号化されているかも知れないチャレンジを、ユーザシステムの処理ユニット109に送る。ユーザシステムの処理ユニット109は、チャレンジが暗号化されている場合には、チャレンジを復号して、チャレンジをユーザシステムの対話ユニット103に送る。本発明の一実施形態では、ユーザは、チャレンジの解答を見つけるために、ユーザシステムの対話ユニット103と対話することが要求されてよい。本発明の別の実施形態では、ユーザシステムの処理ユニット109は、復号されたチャレンジを解決してよい。

【0126】

ユーザがチャレンジに対する解答を見つけると、ユーザの解答はユーザシステムの処理ユニット109に送られる。ユーザシステムの処理ユニット109は、ユーザの解答に基づいてハッシュ値を生成してよく、ユーザシステムの処理ユニット109は更に、このハッシュ値及び／又は解答に対称又は非対称暗号化の何れかを加えてよい。ユーザシステムの処理ユニット109による処理の結果（例えば、ハッシュ値又は暗号化されたハッシュ値と、解答又は暗号化された解答）は、クライアントシステムの処理ユニット135に送られてよい。クライアントシステムの処理ユニット135は、格納されている解答及び／又は格納されているハッシュ値を取得するための要求をクライアントシステムの記憶ユニット133に送ってよい。この要求があると、クライアントシステムの記憶ユニット133は、格納されている解答及び／又は格納されているハッシュ値を取得し、格納されている解答及び／又は格納されているハッシュ値をクライアントシステムの処理ユニット135に送る。

【0127】

クライアントシステムの処理ユニット135は、ユーザシステムの処理ユニット109から受け取った、暗号化されているハッシュ値又は解答を復号する。クライアントシステムの処理ユニット135は、ユーザシステムの処理ユニット109から受け取ったハッシュ値及び解答（暗号化されていない形式）と、格納された解答及び／又はハッシュ値とを、承認のためにクライアントシステムの承認ユニット139に送る。クライアントシステムの承認ユニット139は、受け取った解答と格納されている解答とを、及び／又は受け取ったハッシュ値と格納されているハッシュ値とを比較する。

【0128】

受け取った解答が格納されている解答と一致し、及び／又は受け取ったハッシュ値が格納されているハッシュ値と一致する場合、承認ユニット139は、クライアントシステムの処理ユニット135に一致の確認を送る。クライアントシステムの処理ユニット135は、トランザクションの認証が完了して成功したことを確認するために、一致の確認をクライアントシステムに送る。

【0129】

受け取った解答が格納された解答と一致し、及び／又は受け取ったハッシュ値が格納されているハッシュ値と一致する場合、その後、承認ユニット139は、一致しない旨の通知をクライアントシステムの処理ユニットに送る。クライアントシステムの処理ユニットは、その通知をクライアントシステムに送り、クライアントシステムにトランザクションの認証を行わないように助言する。

【0130】

本発明の別の実施形態では、検証システムの処理ユニットは、図16を参照してクライアントシステムの処理ユニットについて説明した機能を実行することができる。本発明のそのような実施形態では、チャレンジ生成器及び承認ユニットが、クライアントシステム又は検証システムの何れかに含まれてよく、それらチャレンジ生成器及び承認ユニットは、図16に従って説明されたものと同じチャレンジ生成器137及び承認ユニット139の機能を有する。

【0131】

認証のためのシステム及びネットワークは、1又は複数の第1のピア、1又は複数のサーバ、及び、1又は複数の第2のピアで構成されており、各々は、少なくともプロセッサ

10

20

30

40

50

及び送受信機を備えてよい。加えて、1又は複数の第1のピア及び1又は複数の第2のピアは、個別にメモリを備えてよい。幾つかの実施形態では、1又は複数の第1のピア及び1又は複数の第2のピアの各々は、表示装置を備えてよい。1又は複数のサーバは、更にデータベースを備えてよい。

【0132】

第1のピア、第2のピア、及びサーバの各々の送受信機は、外部ソース (exogenous source) との間で情報を送受信するように構成されてよい。幾つかの実施形態では、第1のピアは、サーバとの間で情報を送受信するように構成されてよく、サーバは、第1のピアと第2のピアの両方との間で情報を送受信するように構成されてよく、第2のピアは、サーバとの間で情報を送受信するように構成されてよい。第1のピア及び第2のピアのメモリと、サーバのデータベースとは、情報を記憶し、情報の取得を可能にするように構成されてよい。表示装置は、ユーザがディスプレイと対話するための手段、例えば、データを入力し、キャラクタを選択し、オブジェクトを選択するための手段を更に備えてよい。

【0133】

第1のピア、第2のピア又はサーバのプロセッサは、処理マイグレータ (migrator)、データマニピュレータ、データ変換器、処理生成器、及び処理検証器で構成されてよい。処理マイグレータは、第1のピア、第2のピア、又はサーバ内のある構成要素から、第1のピア、第2のピア、又はサーバ内の別の構成要素にデータを移行するように構成されてよい。例として、限定ではないが、処理マイグレータは、第1のピアのメモリから第1のピアのプロセッサへ、或いは、第2のピアのプロセッサから第2のピアの送受信機へデータを移動するように構成されてよい。データマニピュレータは、データを操作するように、例えば、結合、分離、分離及び再結合、リオーダなどを行うように構成されていてよい。例として、限定されないが、第1のピアのデータマニピュレータは、又は複数のキャラクタ列を第1の部分と第2の部分に分割するように構成されてよく、サーバのデータマニピュレータは、データの第1の部分とデータの第2の部分とを結合して、単一のデータパケットを生成するように構成されてよい。

【0134】

データ変換器は、第1のキャラクタ列を第2のキャラクタ列に変換するように構成されてよく、第1のキャラクタ列及び第2のキャラクタ列の各々は、長さ、構成、又は配置のうちの任意の1又は複数の異なっておりよい。幾つかの実施形態では、データ変換器は、ハッシュアルゴリズムを第1のキャラクタ列に適用するように構成されてよい。他の実施形態では、データ変換器は、第1のキャラクタ列に暗号化プロトコルを適用するように構成されてよい。更に他の実施形態では、データ変換器は、第1のキャラクタ列に復号プロトコルを適用するように構成されてよい。他の実施形態ではまた、データ変換器は、ハッシュアルゴリズム、暗号化プロトコル、復号プロトコル、又はデータ変換の他の既知方法の任意の組合せを、第1のキャラクタ列に適用して、第2のキャラクタ列を生成するように構成されてよい。

【0135】

処理生成器は、データを生成するように構成されてよい。幾つかの実施形態では、データは、任意の長さの1又は複数のキャラクタ列で構成されてよく、また、バーコードなどで構成されてよい。幾つかの実施形態では、データは、ランダムな方法又は規則的な方法の何れかで生成されてよい。処理検証器は、2つ以上のデータを比較して、それらのデータが同一であるか異なるかを判定するように構成されてよい。幾つかの実施形態では、処理検証器と処理生成器は対になって、第1のキャラクタ列と第2のキャラクタ列が同一であるかどうかを判定して、第1のキャラクタ列と第2のキャラクタ列の同一性に基づいて応答を生成するように構成されてよい。

【0136】

認証方法は、登録方法1700とユーザログイン方法2000とを含んでよい。幾つかの実施形態では、登録方法1700は、1又は複数のキーを生成することと、1又は複数のキーを配布することと、1又は複数のキーをローカルデータベースに格納することと、

1又は複数のキーをサーバデータベースに格納することを含んでよい。図17に図示されているように、登録方法1700は更に、第1のピア1701、サーバ1750、及び少なくとも1つの第2のピア1775の間での通信を含んでよい。

【0137】

登録方法1700の幾つかの実施形態では、サーバ1750は、第1のピア1701から登録要求1702を受け取ってよい。サーバ1750は、登録データ1751を第1のピア1701に送ってよい。登録データ1751は、登録方法1700に必要な任意のデータを含んでよい。幾つかの実施形態では、登録データ1751は、クライアント登録コード1703を含んでよい。クライアント登録コード1703は、文字、数字、記号、又はそれらの任意の組合せで構成される1又は複数のキャラクタを含んでよく、サーバ1750によって生成されてよい。別の実施形態では、登録データは、ユーザ選択オブジェクトを含んでいる。更に別の実施形態では、登録データは、クライアント登録コード1703、ユーザ選択オブジェクト、及び登録に必要な他のデータのうちの1又は複数からなる組合せで構成されてよい。

【0138】

登録方法1700は、サーバキー1705及びクライアントキー1706をユーザ入力1704から生成することを更に含んでよい。幾つかの実施形態では、サーバキー1705とクライアントキー1706が使用されて、登録キー1707が生成される。他の実施形態では、サーバキー1705、クライアントキー1706、及び少なくとも1つのクライアント登録コード1703が、登録キー1707を生成するために使用される。他の実施形態は、クライアントキー1706、サーバキー1705、及びクライアント登録コード1703の様々な組合せを備えており、それらは、登録キー1707を生成するために使用される。例えばクライアントキー1706、クライアント登録コード1703のような一部の情報は、第1のピア1701のメモリ1708に格納されてよい。更に、登録方法1700は、第1のピア1701からサーバ1750に情報を転送することを含んでよい。幾つかの実施形態では、登録キー1707及びサーバキー1705がサーバ1750に転送される。

【0139】

登録方法1700は、サーバ1750にて第1のピア1701から情報を受け取ることを含んでよい。幾つかの実施形態では、サーバ1750で受け取った情報は、登録キー1707とサーバキー1705を含んでよい。サーバ1750は、受信者コード1752を生成してよい。更に、サーバ1750は、送信者コード1754を生成してよい。更に、サーバ1750は、配布コード1756を生成してよい。サーバキー1705、受信者コード1752、及び送信者コード1754は、配布キー1753を生成するために使用されてよい。幾つかの実施形態では、配布キー1753は、サーバキー1705、受信者コード1752、送信者コード1754、又はそれらの任意の組合せのうちの任意の1又は複数から生成されてよい。例えば受信者コード1752、配布キー1753のような一部の情報は、サーバ1750のデータベース1757に格納されてよい。登録方法1700は、サーバ1750から少なくとも1つの第2のピア1775に情報を転送することを更に含んでよい。幾つかの実施形態では、配布キー1753及び配布コード1756は、少なくとも1つの第2のピア1775に転送される。

【0140】

登録方法1700は、1又は複数のキーをローカルデータベースに格納することを更に含んでよい。図17に図示されているように、少なくとも1つの第2のピア1775は、サーバ1750から情報を受け取ってよい。幾つかの実施形態では、情報は、配布キー1753及び配布コード1756を含んでよい。第2のピアは、預託(deposit)コード1776を生成してよい。更に、配布キー1753及び預託コード1776は、預託キー1777を生成するために使用されてよい。幾つかの実施形態では、預託キー1777は、配布キー1753のみを、預託コード1776のみを、又は配布キー1753と預託コード1776の任意の組合せを使用して生成されてよい。例えば、配布キー1753、預託

10

20

30

40

50

キー１７７７、配布コード１７５６のような一部の情報は、第２のピアデバイス１７７５のメモリ１７５８に格納されてよい。登録方法１７００は、第２のピア１７７５からサーバ１７５０に情報を転送することを更に含んでよい。幾つかの実施形態では、預託キー１７７７及び配布コード１７５６は、サーバ１７５０に転送される。

【０１４１】

登録方法１７００は、第２のピア１７７５から情報を受け取り、その情報をローカルデータベースに格納するように構成されてよい。幾つかの実施形態では、サーバ１７５０は、第２のピア１７７５から情報を受け取る。受け取った情報は、預託キー１７７７と、配布コード１７５６と、サーバ１７５０による情報の保存に又は第２のピア１７７５における識別に必要な他の情報とから構成されてよい。

10

【０１４２】

次に図１８を参照すると、幾つかの実施形態では、１又は複数のキーを生成すること１８００は、第１のピア１８０１で行われてよい。第１のピア１８０１は、任意のＩｏＴデバイス、即ち、ネットワークに接続し、データを送る能力を有する任意のデバイスであってよく、携帯電話、パーソナルアシスタント、ボタン、ホームセキュリティシステム、電化製品などを含むがこれらに限定されない。第１のピア１８０１は、サーバ１８５０に登録を要求してよい。幾つかの実施形態では、サーバ１８５０は、登録データを第１のピア１８０１に送ってよい。登録データは、第１のピア１８０１の送受信機１８４１によって受け取られてよく、また、第１のピア１８０１において１又は複数のキー１８００を生成するために必要な任意のデータを含んでよい。幾つかの実施形態では、登録データは、クライアント登録コード１８０３を含んでよい。他の実施形態では、登録データは、クライアント登録コード１８０３と、ユーザ入力１８０４の前駆体（precursor）として機能する追加データとを含んでよい。クライアント登録コード１８０３は、任意の長さの１又は複数のキャラクタ列で構成されてよい。

20

【０１４３】

ユーザ入力１８０４は、情報の離散的ユニットを含むユーザ生成データを任意の形態で含んでよい。幾つかの実施形態では、ユーザ入力１８０４は、例えば、指紋、虹彩などの生体情報データを含んでいる。そのような実施形態では、生体情報データは、識別子を含む情報の離散的ユニットに分割されてよい。識別子は、固有の選択コード１８０９に変換されてよい。他の実施形態では、ユーザ入力１８０４は、任意の数の空間的及び／又は時間的データを含んでよい。空間データ及び／又は時間データは、識別子を含む情報の離散的ユニットに分割されてよい。識別子は、固有の選択コード１８０９に変換されてよい。更に別の実施形態では、ユーザ入力１８０４は、生体情報データと空間的及び／又は時間的データの組合せを含んでよく、それらデータの各々が固有の選択コード１８０９を生成するために使用されてよい。

30

【０１４４】

他の実施形態では、ユーザ入力１８０４は、１又は複数の選択オブジェクトを含んでよい。１又は複数の選択オブジェクトは、画像、アイコン、トークン、ボタン、或いは、選択オブジェクトのグループからユーザが１又は複数の選択オブジェクトを選択することを可能にする他のオブジェクトであってよい。幾つかの実施形態では、選択オブジェクトは、送受信機１８４１で受け取られ、処理マイグレータ１８４２は、選択オブジェクトを表示装置１８４３にマイグレートしてよい。表示装置１８４３上でユーザによって選択されると、選択オブジェクトは、任意の数のキャラクタ、例えば、文字、数字、記号からなる選択コード１８０９に変換されてよい。特定の実施形態では、選択オブジェクトは画像であって、サーバ１８５０から受け取られてよい。各画像には固有の選択コード１８０９が割り当てられる。選択オブジェクトの組合せのユーザによる選択は、ユーザによる選択オブジェクトの選択に固有である選択コード１８０９の組合せを含むユーザ入力１８０４を生成する。幾つかの実施形態では、生体情報データ、空間データ及び／又は時間データ、及び選択オブジェクトの任意の組合せが、ユーザ入力１８０４を構成してよい。

40

【０１４５】

50

幾つかの実施形態によれば、ユーザは、2つ以上の選択コード1809を含むユーザ入力1804を生成してよい。選択コードの数はnに等しい。データマニピュレータ1844は、選択コードを2つ以上のグループに分割するように構成されてよい。幾つかの実施形態では、データマニピュレータ1844は、選択コード1809を第1のグループ1810と第2のグループ1811とに分割するように構成されてよい。第1のグループ1810は、1乃至n-1個の選択コード1809からなり、第2のグループ1811は、1乃至n-1個の選択コード1809からなる。第1のグループ1810及び第2のグループ1811の各選択コード1809は、データ変換器1845によって、個別に1又は複数のキャラクタ列に変換1812されてよく、その結果、変換された選択コードの第1のグループ1813と、変換された選択コードの第2のグループ1815とが得られる。幾つかの実施形態では、変換1812は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換1812は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換1812は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。変換された選択コードの第1のグループ1813は、クライアントプレキー（pre-key）1814を生成するために使用されてよい。変換された選択コードの第1のグループ1813を構成する個々の変換された選択コードは、データマニピュレータ1844によって結合されて、クライアントプレキー1814を構成する1又は複数のキャラクタ列を形成してよい。幾つかの実施形態では、個々の変換済み選択コードは、ユニットの連結（concatenation）を通じて結合される。連結は、個々の変換された選択コードの各々を1ユニットとして使用することを含んでよく、又は、個々の変換された選択コードの一部を1ユニットとして使用することを含んでよい。クライアントプレキー1814は、データ変換器1845によってクライアントキー1806に変換1812されてよい。幾つかの実施形態では、変換1812は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換1812は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換1812は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。クライアントキー1806は、処理マイグレータ1842によって第1のピア1801のメモリ1808に格納されてよい。

【0146】

変換された選択コードの第2のグループ1815は、サーバプレキー1816を生成するために使用されてよい。変換された選択コードの第2のグループ1815を構成する個々の変換された選択コードは、データマニピュレータ1844によって結合されて、サーバプレキー1816を構成する1又は複数のキャラクタ列を形成してよい。幾つかの実施形態では、個々の変換済み選択コードは、ユニットの連結によって結合されてよい。連結は、個々の変換された選択コードの各々をユニットとして使用することであってよく、或いは、個々の変換された選択コードの一部をユニットとして使用することであってよい。サーバプレキー1816は、データ変換器1845によってサーバキー1805に変換1812されてよい。幾つかの実施形態では、変換1812は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換1812は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換1812は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。

【0147】

幾つかの実施形態では、登録キー1807が生成されてよい。クライアントキー1806及びサーバキー1805の各々は、データマニピュレータ1844によって、クライアントキーの第1の部分1817、クライアントキーの第2の部分1818、サーバキーの第1の部分1819、及びサーバキーの第2の部分1820に分割されてよい。幾つかの実施形態では、クライアントキー1806は、3つ以上の部分に分割されてよい。同様に、サーバキー1805は、3つ以上の部分に分離されてよい。クライアントキーの第1の部分1817とクライアントキーの第2の部分1818とは、クライアントキー1806を構成するキャラクタの異なる部分を含んでよい。特定の実施形態では、クライアントキーの第1の部分1817及びクライアントキーの第2の部分1818の各々は、クライア

ントキー 1806 を構成するキャラクタの半分であってよい。サーバキーの第 1 の部分 1819 及びサーバキーの第 2 の部分 1820 は、サーバキー 1805 を構成するキャラクタの異なる部分を含んでよい。特定の実施形態では、サーバキーの第 1 の部分 1819 及びサーバキーの第 2 の部分 1820 の各々は、サーバキー 1805 を構成するキャラクタの半分であってよい。クライアントキーの第 1 の部分 1817、クライアントキーの第 2 の部分 1818、サーバキーの第 1 の部分 1819、及びサーバキーの第 2 の部分 1820 は、ユニットの連結を介してデータマニピュレータ 1844 によって結合されて、第 1 のプレキー 1821 を構成する 1 又は複数のキャラクタ列を形成してよい。データマニピュレータ 1844 による連結は、クライアントキーの第 1 の部分 1817、クライアントキーの第 2 の部分 1818、サーバキーの第 1 の部分 1819、及びサーバキーの第 2 の部分 1820 の各々をユニットとして使用することを含んでよく、クライアントキーの第 1 の部分 1817、クライアントキーの第 2 の部分 1818、サーバキーの第 1 の部分 1819、及びサーバキーの第 2 の部分 1820 のピースをユニットとして使用することを含んでよい。更に、連結は、クライアントキー 1806 又はサーバキー 1805 の分割によって生成された部分の任意の組合せを使用することを含んでよい。第 1 のプレキー 1821 は、データ変換器 1845 によって、第 2 のプレキー 1822 を構成する 1 又は複数のキャラクタ列に変換 1812 されてよい。幾つかの実施形態では、変換 1812 は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換 1812 は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換 1812 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。第 2 のプレキー 1822 は、登録プレキー 1823 を生成するために使用されてよい。幾つかの実施形態では、第 2 のプレキー 1822 及びクライアント登録コード 1803 がデータマニピュレータ 1844 によって連結されて、登録プレキー 1823 を構成する 1 又は複数のキャラクタ列が形成されてよい。連結は、第 2 のプレキー 1822 とクライアント登録コード 1803 の各々をユニットとして使用することを含んでよく、第 2 のプレキー 1822 とクライアント登録コード 1803 のピースをユニットとして使用することを含んでよい。登録プレキー 1823 は、データ変換器 1845 によって、登録キー 1807 を構成する 1 又は複数のキャラクタ列に変換 1812 されてよい。幾つかの実施形態では、変換 1812 は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換 1812 は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換 1812 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。

【0148】

第 1 のピア 1801 は、サーバ 1850 に情報を送ってよい。幾つかの実施形態では、第 1 のピア 1801 の処理マイグレータ 1842 は、登録キー 1807 及びサーバキー 1805 を第 1 のピア 1801 の送受信機 1841 にマイグレートしてよく、送受信機 1841 が、登録キー 1807 及びサーバキー 1805 をサーバ 1850 に送ってよい。他の実施形態では、第 1 のピア 1801 の送受信機 1841 は、登録キー 1807、サーバキー 1805、及び登録方法に必要なその他の情報をサーバ 1850 に送ってよい。

【0149】

登録方法は、1 又は複数のキーを配布すること 1900 を更に含んでよい。図 19 に図示されているように、サーバ 1950 の送受信機 1941 は、第 1 のピア 1901 から情報を受け取ってよい。幾つかの実施形態では、サーバ 1950 の送受信機 1941 は、第 1 のピア 1901 から登録キー 1907 を受け取ってよい。サーバ 1950 の送受信機 1941 は、第 1 のピア 1901 からサーバキー 1905 を受け取ってよい。サーバ 1950 の送受信機 1941 は、第 1 のピア 1901 から登録キー 1907 及びサーバキー 1905 の両方を受け取ってよい。処理マイグレータ 1942 は、登録キー 1907 及びサーバキー 1905 をサーバ 1950 のプロセッサにマイグレートしてよい。登録キー 1907 は、処理マイグレータ 1942 によってサーバ 1950 のデータベース 1957 に格納されてよい。サーバ 1950 の処理生成器 1946 は、ピアリスト (peer list) 1958 を生成してよい。ピアリスト 1958 は、ネットワーク上のピアデバイス、例えば第 1 の

10

20

30

40

50

ピア1901、第2のピア1975などのリストを含んでよい。また、ピアリストは、受信者コード1952及び配布コード1956を含んでよく、これらは、任意の長さの1又は複数のキャラクタ列を含んでよい。更に、サーバ1950の処理生成器1946は、送信者コード1954を生成してよく、これもまた、任意の長さの1又は複数のキャラクタ列を含んでよい。

【0150】

幾つかの実施形態では、サーバ1950は、第1のピア1901から登録キー1907を受け取ってよい。登録キー1907は、任意の数の登録キーサブパート (subparts) を生成するために使用されてよい。データマニピュレータは、登録キー1907から登録キーサブパートを生成してよい。これらの実施形態では、登録キー1907は、 n に等しい任意の数のキャラクタを含んでよい。各登録キーサブパートは、 $n-1$ に等しい任意の数又は組合せのキャラクタを含んでよい。サーバ1950は、1又は複数のランダムなキャラクタ列を生成してよい。登録キーサブパートの各々は、データマニピュレータ1944によって、1又は複数のランダムなキャラクタ列と連結されてよい。幾つかの実施形態では、連結されたキャラクタ列は変換1912されてよい。生成された連結キャラクタ列又は変換された連結キャラクタ列の各々は、1又は複数の第2のピア1975に送られてよい。

【0151】

サーバ1950は、第1のピア1901からサーバキー1908を受け取ってよい。サーバキー1908は、任意の数のサーバキーサブパートを生成するために使用されてよい。データマニピュレータは、サーバキー1908からサーバキーサブパートを生成してよい。これらの実施形態では、サーバキー1908は、 n に等しい任意の数のキャラクタを含んでよく、各サーバキーサブパートは、 $n-1$ に等しい任意の数又はキャラクタの組合せを含んでよい。サーバ19050は、1又は複数のランダムなキャラクタ列を生成してもよい。サーバキーサブパートの各々は、データマニピュレータ1944によって、1又は複数のランダムなキャラクタ列と連結されてよい。幾つかの実施形態では、連結されたキャラクタ列は変換1912されてよい。各生成された連結キャラクタ列又は変換された連結キャラクタ列は、1又は複数の第2のピア1975に送られてよい。

【0152】

サーバ1950のデータマニピュレータ1944は、サーバキー1905、受信者コード1952、送信者コード1954、配布コード1956、又は登録キー1907の任意の組合せを組み合わせ、配布プレキー1959を生成してよい。幾つかの実施形態では、配布プレキーは、サーバキー1905、送信者コード1954、及び受信者コード1952を含んでおり、これらは、ユニットの連結によって結合されて1又は複数のキャラクタ列が形成されてよい。連結は、サーバキー1905、送信者コード1954、及び受信者コード1952の各々をユニットとして使用することを含んでよく、サーバキー1905、送信者コード1954、及び受信者コード1952のピースをユニットとして使用することを含んでよい。配布プレキー1959は、データ変換器によって、配布キー1953を構成する1又は複数のキャラクタ列に変換1912されてよい。幾つかの実施形態では、変換1912は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換1912は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換1912は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。配布キー1953は、処理マイグレータ1942によってサーバ1950のデータベース1957に格納されてよい。サーバ1950は、第2のピア1975に情報を送るように構成されてよい。幾つかの実施形態では、サーバ1950の処理マイグレータ1942は、配布キー1953及び配布コード1956をサーバ1950の送受信機1941にマイグレートしてよい。他の実施形態では、サーバ1950の送受信機1941は、配布キー1953、配布コード1956、及び登録方法に必要なその他の情報を第2のピア1975に送ってよい。幾つかの実施形態では、サーバ1950は、登録キー1907、サーバキー1905、及び配布キー1953の任意の組合せを、サーバ1950のデータ

10

20

30

40

50

ベース 1957 に格納してよい。

【0153】

サーバ 1950 は、2 以上の配布キー 1953 を生成し、2 以上の第 2 のピア 1975 にデータを送ってよい。幾つかの実施形態では、ピアリスト 1958 は、ネットワーク上の 2 以上の第 2 のピア 1975 のリストを含んでよい。第 2 のピアは、ネットワーク上にあり、サーバ 1950 とデータを送受信することができる任意の IoT デバイス、サーバ、又は任意のデバイスを含んでよい。サーバ 1950 は、各第 2 のピア 1975 に対して固有の配布コード 1956 を生成してよい。サーバ 1950 は、各第 2 のピア 1975 に対して固有の受信者コード 1952 を生成してよい。これらの実施形態では、各第 2 のピア 1975 のために生成された配布キー 1953 は、他の第 2 のピア 1975 のために生成された配布キー 1953 とは異なってよいが、第 1 のピア 1901 から受け取った基礎となるサーバキー 1905 は同じであってよい。

10

【0154】

幾つかの実施形態によれば、登録キー 1907 が使用されて、配布プレキー 1959 が生成されてよい。これらの実施形態では、登録キー 1907、送信者コード 1954、受信者コード 1952、及びサーバキー 1905 の任意の組合せが使用されて、配布プレキー 1959 が生成されてよい。

【0155】

図 17 を再度参照すると、登録方法 1700 は、1 又は複数のキーをローカルデータベースに格納することを含んでよい。幾つかの実施形態では、第 2 のピア 1775 は、第 2 のピア 1775 の送受信機を介してサーバ 1750 と情報を送受信するように構成されてよい。第 2 のピア 1775 は、第 2 のピア 1775 の送受信機を介してサーバ 1750 から配布キー 1753 を受け取ってよい。第 2 のピア 1775 は、サーバ 1750 から配布コード 1756 を受け取ってよい。幾つかの実施形態では、第 2 のピア 1775 は、サーバ 1750 から配布キー 1753 及び配布コード 1756 を受け取ってよい。配布キー 1753 及び配布コード 1756 は、第 2 のピア 1775 のメモリ 1778 に格納されてよい。第 2 のピア 1775 は、預託コード 1776 を生成してよい。預託コード 1776 は、任意の長さの 1 又は複数のキャラクタ列であってよく、ランダムに生成されてよい。或いは、預託コード 1776 は、サーバ 1750 によって生成され、第 2 のピア 1775 によって受け取られてよい。預託コード 1776 及び配布キー 1753 は、ユニットの連結によって結合されて、預託プレキー 1779 を構成する 1 又は複数のキャラクタ列が形成されてよい。連結は、預託コード 1776 と配布キー 1753 の各々をユニットとして使用することを含んでよく、預託コード 1776 と配布キー 1753 のピースをユニットとして使用することを含んでよい。預託プレキー 1779 は、預託キー 1777 を構成する 1 又は複数のキャラクタ列に変換 1712 されてよい。幾つかの実施形態では、変換 1712 は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換 1712 は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換 1712 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。預託キー 1777 は、第 2 のピア 1775 のメモリ 1778 に格納されてよい。幾つかの実施形態では、第 2 のピア 1775 は、預託キー 1777 及び配布コード 1756 をサーバ 1750 に送ってよい。他の実施形態では、第 2 のピア 1775 は、預託キー 1777、配布コード 1756、及び登録方法 1700 に必要な他の情報をサーバ 1750 に送ってよい。

20

30

40

【0156】

登録方法 1700 は、1 又は複数のキーをサーバデータベースに格納することを更に含んでもよい。図 19 に示すように、サーバ 1950 の送受信機 1941 は、第 2 のピア 1975 から情報を受け取ってよい。幾つかの実施形態では、サーバ 1950 の送受信機 1941 は、配布コード 1956 を受け取ってよい。幾つかの実施形態では、サーバ 1950 の送受信機 1941 は、預託キー 1977 を受け取ってよい。他の実施形態では、サーバ 1950 の送受信機 1941 は、配布コード 1956 及び預託キー 1977 を受け取ってよい。更に別の実施形態では、サーバ 1950 の送受信機 1941 は、配布コード 19

50

56、預託キー1977、及び登録方法に必要な他の情報を受け取ってよい。配布コード1956及び預託キー1977は、処理マイグレータ1942によってサーバ1950のデータベース1957に格納されてよい。

【0157】

特定の実施形態では、登録方法1700は、1又は複数のキーを作成することと、1又は複数のキーを配布することと、1又は複数のキーをローカルデータベースに格納することと、1又は複数のキーをサーバデータベースに格納することとを含んでよい。図17に図示されているように、登録方法1700は、第1のピア1701からの登録要求1702から始まってよい。登録要求1702は、1又は複数のサーバ1750との間で送受信されてよい。1又は複数のサーバは、登録データ1751を第1のピア1701に送ってよい。次に図18を参照すると、特定の実施形態では、第1のピア1801がサーバ1850から登録データを受け取ってよい。登録データは、クライアント登録コード1803と1又は複数の選択オブジェクトとを含んでよい。クライアント登録コード1803は、単一の8桁のキャラクタ列を含んでよい。選択オブジェクトは、幾つかの画像を含んでよい。特定の実施形態では、選択オブジェクトは、60に等しい数の選択オブジェクトを含んでよい。各選択オブジェクトは、固有の選択コード1809を含んでよい。選択コード1809は、1又は複数のキャラクタ列を含んでよく、特定の実施形態では、各選択コードは、5つのキャラクタからなる列を含んでよい。ユーザは、サーバ1850によって受け取られた選択オブジェクトから幾つかの選択オブジェクトを選択してよい。特定の実施形態では、ユーザは、6つの選択オブジェクトを選択してよい。ユーザによる選択オブジェクトの選択は、選択コード1809の集合からなるユーザ入力1804を生成してよく、それら選択コード1809は、各選択コード1809に関連付けられた特定の選択オブジェクトを選択することによって選択されてよい。特定の実施形態では、ユーザ入力1804は、6つの5キャラクタの選択コード1809を含んでいる。

【0158】

ユーザ入力1804は、第1のグループ1810と第2のグループ1811とに分割されてよい。特定の実施形態では、第1のグループ1810と第2のグループ1811の各々は、3つの異なる選択コード1809を含んでいる。第1のグループ1810及び第2のグループ1811を構成する各選択コード1809は、1又は複数のキャラクタ列に変換1812されてよい。特定の実施形態では、各選択コード1809は、ハッシュアルゴリズムを使用して変換されてよく、変換された選択コードの第1のグループ1813と変換された選択コードの第2のグループ1815とをまとめて含んでよい。変換された選択コードの第1のグループ1813及び変換された選択コードの第2のグループ1815の各々が結合されて、クライアントプレキー1814及びサーバプレキー1816の各々が生成されてよい。特定の実施形態では、変換された選択コードの第1のグループ1813を構成する3つの変換された選択コードが連結されて、クライアントプレキー1814を構成する1又は複数のキャラクタ列が生成されてよい。同様に、変換された選択コードの第2のグループ1815を構成する3つの変換された選択コードが連結されて、サーバのプレキー1816を構成する1又は複数のキャラクタ列が生成されてよい。クライアントプレキー1814はクライアントキー1806に、サーバプレキー1816はサーバキー1805に変換1812されてよい。特定の実施形態では、変換1812は、ハッシュアルゴリズムを使用することを含む。

【0159】

登録キー1807は、クライアントキー1806、サーバキー1805、及びクライアント登録コード1803の組合せを用いて生成されてよい。特定の実施形態では、クライアントキー1806は、第1の部分1817及び第2の部分1818に、サーバキー1805は、第1の部分1819及び第2の部分1820に分割される。第1のプレキー1821は、クライアントキー1806の任意の部分とサーバキー1805の任意の部分とを連結することで1又は複数のキャラクタ列を形成することによって生成されてよい。第1のプレキー1821は、第2のプレキー1822を構成する1又は複数のキャラクタ列に

変換 1 8 1 2 されてよい。特定の実施形態では、変換 1 8 1 2 は、ハッシュアルゴリズムを使用することを含む。登録プレキー 1 8 2 3 は、クライアント登録コード 1 8 0 3 と第 2 のプレキー 1 8 2 2 を連結して、1 又は複数のキャラクタ列を形成することによって生成されてよい。登録プレキー 1 8 2 3 は、登録キー 1 8 0 7 に変換されてよく、変換 1 8 1 2 は、ハッシュアルゴリズムを使用することを含んでよい。特定の実施形態では、クライアントキー 1 8 0 6 及びクライアント登録コード 1 8 0 3 は、第 1 のピア 1 8 0 1 のメモリ 1 8 0 8 に格納されてよい。更に、サーバキー 1 8 0 5 及び登録キー 1 8 0 7 は、1 又は複数のサーバ 1 8 5 0 に送られてよい。

【0160】

登録方法は、1 又は複数のキーを配布することで構成されてよい。図 1 9 に示す特定の実施形態では、サーバ 1 9 5 0 は、第 1 のピア 1 9 0 1 から登録キー 1 9 0 7 及びサーバキー 1 9 0 5 を受け取ってよい。登録キーは、サーバ 1 9 5 0 のデータベース 1 9 5 7 に格納されてよい。サーバ 1 9 5 0 は、ネットワーク上の第 2 のピア 1 9 7 5 のリストを含むピアリスト 1 9 5 8 を生成してよい。第 2 のピア 1 9 7 5 の各々について、サーバ 1 9 5 0 は、受信者コード 1 9 5 2 及び配布コード 1 9 5 6 を生成してよい。特定の実施形態では、受信者コード 1 9 5 2 及び配布コード 1 9 5 6 は、特定の第 2 のピア 1 9 7 5 及び特定のトランザクションの両方に固有であってよい。更に、サーバ 1 9 5 0 は、送信者コード 1 9 5 4 を生成してよく、送信者コード 1 9 5 4 は、特定のサーバ 1 9 5 0 に固有であってよい。特定の実施形態では、受信者コード 1 9 5 2、送信者コード 1 9 5 4、及びサーバキー 1 9 0 5 は、連結によって結合されて、配布プレキー 1 9 5 9 を構成する 1 又は複数のキャラクタ列が生成されてよい。配布プレキー 1 9 5 9 は、配布キー 1 9 5 3 に変換 1 9 1 2 されてもよい。特定の実施形態では、変換 1 9 1 2 は、ハッシュアルゴリズムを使用することを含んでよい。幾つかの実施形態では、複数の固有の配布キー 1 9 5 3 が生成されてよく、各々は、異なる受信者コード 1 9 5 2 を含んでおり、ピアリスト 1 9 5 8 からの関連する異なる配布コード 1 9 5 6 を有する。固有の配布キー 1 9 5 3 の各々は、最終的には、異なる第 2 のピア 1 9 7 5 に送られてよい。特定の実施形態では、複数の固有の配布キー 1 9 5 3 が同一のサーバキー 1 9 0 5 から生成されて、固有の配布キー 1 9 5 3 の各々は、ネットワーク上の別個の第 2 のピア 1 9 7 5 に転送される。

【0161】

登録方法は、図 1 7 に図示されているように、1 又は複数のキーをローカルデータベースに格納することを更に含んでよい。特定の実施形態では、第 2 のピア 1 7 7 5 は、サーバ 1 7 5 0 から配布キー 1 7 5 3 及び配布コード 1 7 5 6 を受け取ってよい。この実施形態では、第 2 のピア 1 7 7 5 は、ネットワーク内の複数の第 2 のピア 1 7 7 5 のうちの 1 つであってよく、上述したように、第 1 のピア 1 7 0 1 とサーバ 1 7 5 0 の間の同じトランザクションから生じる配布キー 1 7 5 3 及び配布コード 1 7 5 6 を受け取る。第 2 のピア 1 7 7 5 は、配布キー 1 7 5 3 及び配布コード 1 7 5 6 を第 2 のピア 1 7 7 5 のメモリ 1 7 7 8 に格納してよい。更に、第 2 のピア 1 7 7 5 は、預託コード 1 7 7 6 を生成してよい。特定の実施形態では、預託コード 1 7 7 6 は、8 つのキャラクタの単一の列を含んでいる。預託コード 1 7 7 6 と配布キー 1 7 5 3 は、連結により結合されて、預託プレキー 1 7 7 9 を構成する 1 又は複数のキャラクタ列が生成されてよい。預託プレキー 1 7 7 9 は、預託キー 1 7 7 7 に変換 1 7 1 2 されてよい。特定の実施形態では、変換 1 7 1 2 は、ハッシュアルゴリズムを使用することを含んでよい。第 2 のピア 1 7 7 5 は、1 又は複数のサーバ 1 7 5 0 に情報を送ってよい。特定の実施形態では、複数の第 2 のピア 1 7 7 5 は、サーバ 1 7 5 0 に情報を送ってよい。情報は、配布コード 1 7 5 6、預託キー 1 7 7 7、及び登録プロセス 1 7 0 0 を実行するために必要な他の任意の情報を含んでよい。

【0162】

登録方法 1 7 0 0 は、サーバデータベースに 1 又は複数のキーを格納することを含んでよい。幾つかの実施形態では、サーバ 1 7 5 0 は、1 又は複数の第 2 のピア 1 7 7 5 から情報を受け取るように構成されてよい。特定の実施形態では、サーバ 1 7 5 0 は、配布コード 1 7 5 6 及び預託キー 1 7 7 7 を含む情報を複数の第 2 のピア 1 7 7 5 から受け取

10

20

30

40

50

てよい。サーバ1750は、配布コード1756及び預託キー1777をデータベース1757に格納してよい。図19を参照すると、配布コード1956及び預託キー1977は、データベース1957内に格納されたピアリスト1958に格納されてよい。特定の実施形態では、配布コード1956及び預託キー1977は、格納された配布キー1953及び受信者コード1952と対にされており、それは、第1のピア1901と、サーバ1950と、特定の第2のピア1975との間で行われたトランザクションに固有のものであってよい。

【0163】

認証方法は、図20に示すように、ログイン方法を含んでよい。ログイン方法2000は、1又は複数のログインキーを作成すること、1又は複数の検証キーを配布し、ローカルデータベース内の検証キーを検証すること、検証プロセスを有効にすることから構成されてもよい。更に、ログイン方法2000は、1又は複数の第1のピア2001と、1又は複数のサーバ2050と、1又は複数の第2のピア2075との間の通信を含んでよい。

【0164】

ログイン方法2000は、第1のピア2001を含んでよく、第1のピアは、ユーザと対話するように構成されてよい。第1のピア2001は、ログイン要求2002してよく、ログイン要求2002は、1又は複数のサーバ2050に送られてよい。サーバ2050は、ログイン要求2002を受け取り、ログインデータ2051を生成してよい。幾つかの実施形態では、ログインデータ2051は、ログインソルト2024を構成してよい。ログインソルトは、文字、数字、記号、又はそれらの任意の組合せからなる1又は複数のキャラクタを含んでよい。幾つかの実施形態では、ログインデータ2051は、ユーザ選択オブジェクトを含んでよい。他の実施形態では、ログインデータ2051は、1又は複数のログインソルト2024と、ユーザ選択オブジェクトと、ログイン方法2000に必要な他の任意のデータとを含んでよい。

【0165】

1又は複数のログインキーを生成することは、ユーザ入力2004からサーバキー2005及びクライアントキー2006を生成することを更に含んでよい。幾つかの実施形態では、サーバキー2005及びクライアントキー2006が使用されて、ログインキー2099が生成されてよい。他の実施形態では、サーバキー2005、クライアントキー2006、及び少なくともログインソルト2024が、ログインキー2099を生成するために使用されてよい。他の実施形態では、クライアントキー2006、サーバキー2005、及びログインソルト2024の異なる組合せが、ログインキー2099を生成するために使用されてよい。例えばクライアントキー2006、ログインソルト2024のような幾らかの情報が、第1のピア2001のメモリ2008に格納されてよい。更に、1又は複数のログインキーを生成することは、第1のピア2001からサーバ2050に情報を転送することを含んでよい。幾つかの実施形態では、ログインキー2099及びサーバキー2005がサーバ2050に転送される。

【0166】

また、図20に示すように、1又は複数の検証キーを配布することは、サーバ2050にて第1のピア2001から情報を受け取ることを含んでよい。幾つかの実施形態では、サーバ2050で受け取った情報は、ログインキー2099及びサーバキー2005を含んでよい。サーバ2050は、受信者コード2052を生成してよい。更に、サーバ2050は、送信者コード2054を生成してよい。更に、サーバ2050は、配布コード2056を生成してよい。サーバキー2005、受信者コード2052、及び送信者コード2054が使用されて検証キー2062が生成されてよい。幾つかの実施形態では、検証キー2062は、1又は複数のサーバキー2005、受信者コード2052、検証ソルト2024、又は送信者コード2054、或いは、それらの任意の組合せから生成されてよい。幾つかの情報、例えば、受信者コード2052、検証キー2062は、サーバ2050のデータベース2057に格納されてよい。幾つかの実施形態では、検証キー2062は、サーバ2050のデータベース2057に格納されなくてもよい。複数の検証キーを

10

20

30

40

50

配布することは、サーバ 2050 から少なくとも 1 つの第 2 のピア 2075 に情報を転送することを更に含んでよい。幾つかの実施形態では、検証キー 2062 及び配布コード 2056 は、少なくとも 1 つの第 2 のピア 2075 に転送される。

【0167】

ログイン方法 2000 は、ローカルデータベース上で 1 又は複数の検証キーを検証することを更に含んでよい。図 20 に図示されているように、少なくとも 1 つの第 2 のピア 2075 は、サーバ 2050 から情報を受け取ってよい。幾つかの実施形態では、情報は、検証キー 2062 及び配布コード 2056 を含んでよい。他の実施形態では、情報は、検証キー 2062、配布コード 2056、及び検証ソルト 2063 を含んでよい。第 2 のピア 2075 は、配布コード 2056 と検証キー 2062 の任意の組合せを使用して、対応する配布キーが第 2 のピア 2075 のメモリ 2078 に格納されている可能性があることを突き止めて確認してよい。格納された配布キーが使用されて、確認キー 2081 が生成されてよい。幾つかの実施形態では、格納された配布キー 2053 と、サーバ 2050 から受け取った検証ソルト 2063 とが使用されて、確認キー 2081 が生成されてよい。第 2 のピア 2075 は、サーバ 2050 に情報を送ってよく、この情報は、確認キー 2081、配布コード 2056、及びログイン方法 2000 に必要な他の情報の任意の組合せを含んでよい。

【0168】

検証プロセスを有効にすることは、第 2 のピア 2075 から情報を受け取り、受け取った情報をサーバ 2050 のデータベース 2057 に格納されている情報と比較することを含んでよい。幾つかの実施形態では、サーバ 2050 は、第 2 のピア 2075 から情報を受け取る。受け取った情報は、確認キー 2081 と、結果と、配布コード 2056 と、サーバ 2050 による情報の保存又は比較に、又は第 2 のピア 2075 の特定に必要な他の情報とを含んでよい。

【0169】

図 21 に示されているように、1 又は複数のログインキー 2100 を生成することは、幾つかの実施形態では、第 1 のピア 2101 で行われてよい。第 1 のピア 2101 は、任意の IoT デバイス、即ち、ネットワークに接続し、データを送る能力を有する任意のデバイスであってよく、携帯電話、パーソナルアシスタント、ボタン、ホームセキュリティシステム、家電製品などを含むがこれらに限定されない。第 1 のピア 2101 は、サーバ 2150 からログインを要求してよい。幾つかの実施形態では、サーバ 2150 の送受信機は、ログインデータを第 1 のピア 2101 に送ってよい。ログインデータは、第 1 のピア 2101 の送受信機 2141 で受け取られてよく、第 1 のピア 2101 でログイン方法を開始するために必要なデータを含んでよい。幾つかの実施形態では、ログインデータは、ログインソルト 2124 を構成してよい。他の実施形態では、ログインデータは、ログインソルト 2124 と、ユーザ入力 2104 の前駆体として機能する付加的なデータとを含んでよい。ログインソルト 2124 は、任意の長さの 1 又は複数のキャラクタ列を含んでよい。

【0170】

また、図 21 に示すように、ユーザ入力 2104 は、情報の離散的なユニットを構成する任意の形態のユーザ生成データを含んでよい。幾つかの実施形態では、ユーザ入力 2104 は、例えば、指紋、虹彩などの生体情報データを含んでいる。それらの実施形態では、生体情報データは、識別子を含む情報の離散的なユニットに分割されてよい。識別子は、固有の選択コード 2109 に変換されてよい。

【0171】

他の実施形態では、ユーザ入力 2104 は、1 又は複数の選択オブジェクトを含んでよい。1 又は複数の選択オブジェクトは、画像、アイコン、トークン、ボタン、或いは、ユーザが選択オブジェクトのグループから 1 又は複数の選択オブジェクトを選択することを可能にする任意の他のオブジェクトであってよい。選択オブジェクトは、第 1 のピア 2101 の表示装置 2143 に表示されてよく、任意の数のキャラクタ、例えば、文字、数字

、記号を含む選択コード 2109 に変換されてよい。特定の実施形態では、選択オブジェクトは画像であって、サーバ 2150 から受け取られてよい。各画像には固有の選択コード 2109 が割り当てられており、選択オブジェクトの組合せのユーザによる選択は、選択コード 2109 の組合せを含むユーザ入力 2104 を生成し、当該組合せは、ユーザによる選択オブジェクトの選択に固有である。

【0172】

幾つかの実施形態では、ユーザは、選択コードの数が n に等しい 2 つ以上の選択コード 2109 を含むユーザ入力 2104 を生成してよい。選択コード 2109 は、データマニピュレータ 2144 によって第 1 のグループ 2110 と第 2 のグループ 2111 とに分割されてよい。ここで、第 1 のグループ 2110 は、1 乃至 $n-1$ 個の選択コード 2109 を含んでおり、第 2 のグループ 2111 は、1 乃至 $n-1$ 個の選択コード 2109 を含んでいる。第 1 のグループ 2110 及び第 2 のグループ 2111 の各選択コード 2109 は、データ変換器 2145 によって 1 又は複数のキャラクタ列に個別に変換 2112 されてよく、その結果、変換された選択コードの第 1 のグループ 2113 と変換された選択コードの第 2 のグループ 2115 とが得られる。幾つかの実施形態では、変換 2112 は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換 2112 は、暗号化手段を使用することを含んでよい。更に他の実施形態では、変換 2112 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。変換された選択コードの第 1 のグループ 2113 が使用されて、クライアントプレキー 2114 が生成されてよい。変換された選択コードの第 1 のグループ 2113 を構成する個々の変換された選択コードは、データマニピュレータ 2144 によって結合されて、クライアントプレキー 2114 を構成する 1 又は複数のキャラクタ列が形成されてよい。幾つかの実施形態では、個々の変換された選択コードは、ユニットの連結によって結合されてもよい。連結は、変換された個々の選択コードをユニットとして使用することを含んでよく、変換された個々の選択コードのピースをユニットとして使用することを含んでよい。クライアントプレキー 2114 は、データ変換器 2145 によってクライアントキー 2106 に変換されてよい。幾つかの実施形態では、変換 2112 は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換 2112 は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換 2112 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。クライアントキー 2106 は、処理マイグレータ 2147 によって、第 1 のピア 2101 のメモリユニット 2108 に格納されてよい。ログイン方法によって生成されたクライアントキー 2106 は、処理検証器 2147 によって、アイデンティティの登録処理の間に第 1 のピア 2101 のメモリ 2108 に格納されたクライアントキー 2106 と比較されてよい。

【0173】

変換された選択コードの第 2 のグループ 2115 が使用されて、サーバプレキー 2116 が生成されてよい。変換された選択コードの第 2 のグループ 2115 を構成する個々の変換された選択コードは、データマニピュレータ 2144 によって結合されて、サーバプレキー 2116 を構成する 1 又は複数のキャラクタ列が形成されてよい。幾つかの実施形態では、個々の変換された選択コードは、ユニットの連結によって結合されてよい。連結は、変換された個々の選択コードをユニットとして使用することを含んでよく、変換された個々の選択コードのピースをユニットとして使用することを含んでよい。サーバプレキー 2116 は、データ変換器 2145 によってサーバキー 2105 に変換 2112 されてよい。幾つかの実施形態では、変換 2112 は、ハッシュアルゴリズムを使用して構成されてもよい。他の実施形態では、変換 2112 は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換 2112 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。

【0174】

幾つかの実施形態では、ログインキー 2199 が生成されてよい。クライアントキー 2106 及びサーバキー 2105 の各々は、データマニピュレータ 2144 によって、クラ

10

20

30

40

50

クライアントキーの第1の部分2117、クライアントキーの第2の部分2118、サーバキーの第1の部分2119、及びサーバキーの第2の部分2120に分割されてよい。クライアントキーの第1の部分2117及びクライアントキーの第2の部分2118は、クライアントキー2106を構成するキャラクタの異なる部分を含んでよい。特定の実施形態では、クライアントキーの第1の部分2117及びクライアントキーの第2の部分2118の各々は、クライアントキー2106の半分であってもよい。サーバキーの第1の部分2119及びサーバキーの第2の部分2120は、サーバキー2105を構成するキャラクタの異なる部分を含んでよい。特定の実施形態では、サーバキーの第1の部分2119及びサーバキーの第2の部分2120の各々は、サーバキー2105を構成するキャラクタの半分であってもよい。クライアントキーの第1の部分2117、クライアントキーの第2の部分2118、サーバキーの第1の部分2119、及びサーバキーの第2の部分2120は、ユニットの連結を介してデータマニピュレータ2144によって結合されて、第1のプレキー2121を構成する1又は複数のキャラクタが形成されてよい。連結は、クライアントキーの第1の部分2117、クライアントキーの第2の部分2118、サーバキーの第1の部分2119、及びサーバキーの第2の部分2120の各々をユニットとして用いることを含んでよく、或いは、クライアントキーの第1の部分2117、クライアントキーの第2の部分2118、サーバキーの第1の部分2119、及びサーバキーの第2の部分2120のピースをユニットとして用いることを含んでよい。

【0175】

第1のプレキー2121は、データ変換器2145によって、第2のプレキー2122を構成する1又は複数のキャラクタ列に変換2112されてよい。幾つかの実施形態では、変換2112は、ハッシュアルゴリズムを使用して構成されてもよい。他の実施形態では、変換2112は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換2112は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。第2のプレキー2122が使用されて、登録プレキー2123が生成されてよい。幾つかの実施形態では、第2のプレキー2122とクライアント登録コード2103は、データマニピュレータ2144によって連結されて、登録プレキー2123を構成する1又は複数のキャラクタ列が形成されてよい。連結は、第2のプレキー2122とクライアント登録コード2103の各々をユニットとして用いることを含んでよく、第2のプレキー2122とクライアント登録コード2103のピースをユニットとして用いることを含んでよい。クライアント登録コード2103は、処理マイグレータ2142によって登録処理中に第1のピア2101のメモリ2108に格納されてよい。登録プレキー2123は、データ変換器2144によって、登録キー2107を構成する1又は複数のキャラクタ列に変換されてよい。幾つかの実施形態では、変換2112は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換2112は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換2112は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。幾つかの実施形態では、登録キー2107は、図17に示す登録方法1700の間に第1のピア1701によって生成された登録キー1707と同一であってもよい。図21を参照すると、登録キー2107が使用されてログインキー2199が生成されてよい。幾つかの実施形態では、登録キー2107とログインソルト2124が使用されて、ログインキー2199が生成されてよい。登録キー2107及びログインソルト2124は、データマニピュレータ2144によって連結されて、ログインプレキー2198を構成する1又は複数のキャラクタ列が形成されてよい。連結は、登録キー2107とログインソルト2124の各々をユニットとして用いることを含んでよく、登録キー2107とログインソルト2124のピースをユニットとして用いることを含んでよい。ログインプレキー2198が使用されて、ログインキー2199が生成されてよい。幾つかの実施形態では、ログインプレキー2198は、データ変換器2145によってログインキー2199に変換されてよい2112。幾つかの実施形態では、変換2112は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換2112は、暗号化方法を使用することを含んでよい。更に他の実施形態で

10

20

30

40

50

は、変換 2 1 1 2 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。

【0 1 7 6】

第 1 のピア 2 1 0 1 は、サーバ 2 1 5 0 に情報を送ってよい。幾つかの実施形態では、第 1 のピア 2 1 0 1 の送受信機 2 1 4 1 は、ログインキー 2 1 9 9 及びサーバキー 2 1 0 5 をサーバ 2 1 5 0 に送ってよい。他の実施形態によれば、第 1 のピア 2 1 0 1 の送受信機 2 1 4 1 は、ログインキー 2 1 9 9 と、サーバキー 2 1 0 5 と、ログイン方法に必要な他の情報とをサーバ 2 1 5 0 に送ってよい。

【0 1 7 7】

ログイン方法は、1 又は複数の検証キーを配布することを更に含んでよい。図 2 2 に図示されているように、サーバ 2 2 5 0 は、第 1 のピア 2 2 0 1 から情報を受け取ってよい。幾つかの実施形態では、サーバ 2 2 5 0 の送受信機 2 2 4 1 は、第 1 のピア 2 2 0 1 からログインキー 2 2 9 9 を受け取ってよい。サーバ 2 2 5 0 の送受信機 2 2 4 1 は、第 1 のピア 2 2 0 1 からサーバキー 2 2 0 5 を受け取ってよい。サーバ 2 2 5 0 の送受信機 2 2 4 1 は、ログインキー 2 2 9 9 及びサーバキー 2 2 0 5 の両方を第 1 のピア 2 2 0 1 から受け取ってよい。幾つかの実施形態では、サーバ 2 2 5 0 は、比較ログインキー 2 2 6 0 を生成してよい。比較ログインキー 2 2 6 0 は、サーバ 2 2 5 0 のデータベース 2 2 5 7 に格納されている登録キー 2 2 0 7 を登録方法中に使用することで生成されてよい。サーバ 2 2 5 0 の処理マイグレータ 2 2 4 2 は、登録キー 2 2 0 7 及びログインソルト 2 2 2 4 をデータベース 2 2 5 7 からマイグレートしてよい。サーバ 2 2 5 0 のデータマニピュレータ 2 2 4 4 は、連結により登録キー 2 2 0 7 とログインソルト 2 2 2 4 を結合して、比較ログインプレキーを生成してよい。比較ログインプレキーは、データ変換器 2 2 4 5 によって比較ログインキー 2 2 6 0 に変換 2 2 1 2 されてよい。幾つかの実施形態では、変換 2 2 1 2 は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換 2 2 1 2 は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換 2 2 1 2 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。サーバ 2 2 5 0 の処理検証器 2 2 4 7 は、第 1 のピア 2 2 0 1 が送ったログインキー 2 2 9 9 と比較ログインキー 2 2 6 0 とを比較して、第 1 のピア 2 2 0 1 と通信してもよい。否かを判定してよい。

【0 1 7 8】

ログインキー 2 2 9 9 は、処理マイグレータ 2 2 4 2 によってサーバ 2 2 5 0 のデータベース 2 2 5 7 に格納されてよい。サーバは、データマイグレータ 2 2 4 2 を使用して、以前に格納されたピアリスト 2 2 5 8 にアクセスしてよい。格納されたピアリスト 2 2 5 8 は、例えば第 1 のピア 2 2 0 1、第 2 のピア 2 2 7 5 のようなネットワーク上のピアデバイスのリストを含んでよい。ピアリストはまた、受信者コード 2 2 5 2 及び配布コード 2 2 5 6 を含んでよく、これらは、任意の長さの 1 又は複数のキャラクタ列を含んでよい。更に、サーバ 2 2 5 0 の処理生成器 2 2 4 6 は、送信者コード 2 2 5 4 を生成してよく、これもまた、任意の長さの 1 又は複数のキャラクタ列を含んでよい。

【0 1 7 9】

サーバ 2 2 5 0 のデータマニピュレータ 2 2 4 4 は、サーバキー 2 2 0 5、受信者コード 2 2 5 2、送信者コード 2 2 5 4、配布コード 2 2 5 6、又はログインキー 2 2 9 9 の任意の組合せを組み合わせ、配布プレキー 2 2 5 9 を生成してもよい。幾つかの実施形態では、配布プレキー 2 2 5 9 は、サーバキー 2 2 0 5、送信者コード 2 2 5 4、及び受信者コード 2 2 5 2 を含んでおり、これらは、ユニットの連結によって結合されて、1 又は複数のキャラクタ列が形成されてよい。連結は、サーバキー 2 2 0 5、送信者コード 2 2 5 4、受信者コード 2 2 5 2 の各々をユニットとして用いることを含んでよく、サーバキー 2 2 0 5、送信者コード 2 2 5 4、受信者コード 2 2 5 2 のパーツをユニットとして用いることを含んでよい。配布プレキー 2 2 5 9 は、データ変換器 2 2 4 5 によって、配布キー 2 2 5 3 を構成する 1 又は複数のキャラクタ列に変換 2 2 1 2 されてよい。幾つかの実施形態では、変換 2 2 1 2 は、ハッシュアルゴリズムを使用することを含んでよい。

他の実施形態では、変換 2 2 1 2 は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換 2 2 1 2 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。配布キー 2 2 5 3 は、サーバ 2 2 5 0 のデータベース 2 2 5 7 に格納されてよい。検証プレキー 2 2 6 1 は、サーバ 2 2 5 0 のデータマニピュレータ 2 2 4 4 によって生成されてよい。幾つかの実施形態では、配布キー 2 2 5 3 と、サーバ 2 2 5 0 の処理生成器 2 2 4 6 によって生成され、任意の数のキャラクタを含んでいる検証ソルト 2 2 6 3 とが連結されて、検証プレキー 2 2 6 1 が生成されてよい。検証プレキー 2 2 6 1 は、データ変換器 2 2 4 5 によって検証キー 2 2 6 2 に変換 2 2 1 2 されてよい。幾つかの実施形態では、変換 2 2 1 2 は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換 2 2 1 2 は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換 2 2 1 2 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。

10

【0180】

サーバ 2 2 5 0 は、第 2 のピア 2 2 7 5 に情報を送るように構成されてよい。幾つかの実施形態では、サーバ 2 2 5 0 の送受信機 2 2 4 1 は、検証キー 2 2 6 2 及び配布コード 2 2 5 6 を第 2 のピア 2 2 7 5 に送ってよい。他の実施形態では、サーバ 2 2 5 0 の送受信機 2 2 4 1 は、検証キー 2 2 6 2、配布コード 2 2 5 6、検証ソルト 2 2 6 3、及びログイン方法 2 0 0 0 に必要な他の情報を第 2 のピア 2 2 7 5 に送ってよい。幾つかの実施形態では、サーバ 2 2 5 0 は、配布キー 2 2 5 3、検証ソルト 2 2 6 3、及び配布コード 2 2 5 6 の任意の組合せを第 2 のピア 2 2 7 5 に送ってよい。

20

【0181】

サーバ 2 2 5 0 は、1 又は複数の検証キー 2 2 6 2 を生成し、1 又は複数の第 2 のピア 2 2 7 5 にデータを送ってよい。幾つかの実施形態では、ピアリスト 2 2 5 8 は、ネットワーク上の 1 又は複数の第 2 のピア 2 2 7 5 のリストを含んでよい。第 2 のピアは、ネットワーク上にあって、サーバ 2 2 5 0 からデータを送受信することができる任意の IoT デバイス、サーバ、又は任意のデバイスを含んでよい。サーバ 2 2 5 0 は、各第 2 のピア 2 2 7 5 に対して固有の配布コード 2 2 5 6 を生成してよい。サーバ 2 2 5 0 は、各第 2 のピア 2 2 7 5 に対して固有の受信者コード 2 2 5 2 を生成してよい。これらの実施形態では、各第 2 のピア 2 2 7 5 のために生成される検証キー 2 2 6 2 は、他の第 2 のピア 2 2 7 5 のために生成される検証キー 2 2 6 2 とは異なってよいが、第 1 のピア 2 2 0 1 から受け取った基礎となるサーバキー 2 2 0 5 は同一であってよい。検証キー 2 2 6 2 は、サーバ 2 2 5 0 のデータベース 2 2 5 7 に格納されても、格納されていなくてもよい。

30

【0182】

ここで図 2 3 を参照すると、ログイン方法は、ローカルデータベース上の 1 又は複数のログインキーを検証することを含んでよい。幾つかの実施形態では、第 2 のピア 2 3 7 5 は、情報を受け取ってサーバ 2 3 5 0 に送るように構成されてよい。第 2 のピア 2 3 7 5 の送受信機 2 3 4 1 は、サーバ 2 3 5 0 から検証キー 2 3 6 2 を受け取ってよい。第 2 のピア 2 3 7 5 の送受信機 2 3 4 1 は、サーバ 2 3 5 0 から配布コード 2 3 5 6 を受け取ってよい。幾つかの実施形態では、第 2 のピア 2 3 7 5 の送受信機 2 3 4 1 は、検証キー 2 3 6 2、配布コード 2 3 5 6、及び検証ソルト 2 3 6 3 をサーバ 2 3 5 0 から受け取ってよい。配布コード 2 3 5 6 は、第 2 のピア 2 3 7 5 のメモリ 2 3 7 8 に格納されている全ての配布コード 2 3 5 6 にわたって、処理検証器 2 3 4 7 によって比較されてよい。サーバ 2 3 5 0 から受け取った配布コード 2 3 5 6 が、第 2 のピア 2 3 7 5 のメモリ 2 3 7 8 に格納されている配布コード 2 3 5 6 と同一である場合、第 2 のピア 2 3 7 5 の処理生成器 2 3 4 6 は、肯定的である結果 2 3 8 2 を生成してよい。第 2 のピア 2 3 7 5 が受け取った配布コード 2 3 5 6 が、第 2 のピア 2 3 7 5 のメモリ 2 3 7 8 に格納されている配布コード 2 3 5 6 と同一でない場合、第 2 のピア 2 3 7 5 の処理生成器 2 3 4 6 は、否定的である結果 2 3 8 2 を生成してよい。幾つかの実施形態では、検証キー 2 3 6 2 はまた、同一の配布コード 2 3 5 6 の場所を確認するために使用される。第 2 のピア 2 3 7 5 が、第 2 のピア 2 3 7 5 のメモリ 2 3 7 8 に格納された 1 又は複数の配布コード 2 3 5 6 が、

40

50

サーバ2350から受け取った配布コード2356と同一であると判定した場合、第2のピア2375の処理マイグレータ2342は、一致する配布コード2356に関連する配布キー2353をメモリ2378から削除してもよい。第2のピア2375のメモリ2378から削除された配布キー2353と検証ソルト2363とがデータマニピュレータ2344で使用されて、連結によって確認プレキー2380が生成されてよい。確認プレキー2380は、データ変換器2345によって確認キー2381に変換されてよい。幾つかの実施形態では、変換2312は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換2312は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換2312は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。

10

【0183】

幾つかの実施形態では、第2のピア2375は、サーバ2350から配布キーと検証ソルト2363を受け取ってよい。第2のピア2375は、配布キー及び検証ソルト2363を連結して検証プレキーを生成することで、第2のピア2375にて検証キー2362を生成してよい。検証プレキーは、検証キー2362に変換2312されてよい。

【0184】

幾つかの実施形態では、第2のピア2375は、比較検証キー2383を生成してよい。第2のピア2375は、サーバ2350から受け取った検証ソルト2363と格納されている配布キー2353とを連結することにより比較検証プレキーを生成することで、比較検証キー2383を生成してよい。比較検証プレキーは、比較検証キーに変換2312されてよい。幾つかの実施形態では、比較検証キー2383は、受け取った検証キー2362と処理検証器2347によって比較されて、結果2382が生成されてよい。幾つかの実施形態では、結果2382は、検証キー2362と比較検証キー2383とを比較して生成された結果と、受け取られた配布コード2356と格納されている配布コード2356とを比較して生成された結果とを含んでよい。確認キー2381は、検証ソルト2363と、第2のピア2375のメモリ2378から取得された預託キー2377から生成されてよい。預託キー2377と検証ソルト2363は、データマニピュレータ2344によって連結されて確認プレキー2380が生成されてよい。確認プレキー2380は、確認キー2381に変換2312されてよい。確認キー2381、配布コード2356、及び結果2382の任意の組合せは、第2のピア2375からサーバ2350に送られてよい。

20

30

【0185】

第2のピア2375は、サーバ2350にデータを送るように構成されてよい。幾つかの実施形態では、第2のピア2375の送受信機2341は、結果2382、配布コード2356、及び確認キー2381の任意の組合せをサーバ2350に送ってよい。幾つかの実施形態では、第2のピア2375は、トランザクションに関連付けられている全てのデータを削除するように構成されてよい。特定の実施形態では、第2のピア2375は、第2のピア2375のメモリ2378又は第2のピア2375のプロセッサから、配布コード2356、預託キー2377、配布キー2353、検証キー2362、検証ソルト2326、確認プレキー2380、及び確認キー2381の任意の組合せを削除してよい。幾つかの実施形態では、データの削除は、サーバ2350へのデータの送信と同時に起こってよい。他の実施形態では、データの削除は、サーバ2350にデータを送った後に起こってよい。

40

【0186】

ここで図24を参照すると、ログイン方法は、検証プロセス2400を有効にすることを更に含んでよい。サーバ2450は、1又は複数の第2のピア2475からデータを受け取るように構成されてよい。幾つかの実施形態では、サーバ2450の送受信機2441は、確認キー2481、結果2482、及び配布コード2456の任意の組合せを受け取ってよい。サーバ2450は、第2のピア2475から受け取った結果2482を承認してよい。結果が肯定的である場合、サーバ2450の処理検証器2447は、第2のピア

50

ア 2 4 7 5 から受け取った配布コード 2 4 5 6 を、サーバ 2 4 5 0 のデータベース 2 4 5 7 に格納されている全て又は一部の配布コード 2 4 5 6 と比較してよい。サーバ 2 4 5 0 のデータベース 2 4 5 7 に格納されている配布コード 2 4 5 6 が第 2 のピア 2 4 7 5 から受け取った配布コード 2 4 5 6 と同一である場合、その後、サーバ 2 4 5 0 の処理マイグレータ 2 4 4 2 は、検証ソルト 2 4 6 3 と、配布コード 2 4 5 6 に関連付けられてサーバ 2 4 5 0 のデータベース 2 4 5 7 に格納されている可能性のある配布キー 2 4 5 3 との任意の組合せを取得してよい。幾つかの実施形態では、取得された配布キー 2 4 5 3 は、登録プロセス中に格納された配布キー 2 4 5 3 であってもよい。取得された検証ソルト 2 4 6 3 と取得された配布キー 2 4 5 3 とは、データマニピュレータ 2 4 4 4 によって使用されて、検証ソルト 2 4 6 3 と配布キー 2 4 5 3 とを連結して検証プレキー 2 4 6 1 が生成されてよい。検証プレキー 2 4 6 1 は、データ変換器 2 4 4 5 によって検証キー 2 4 6 2 に変換 2 4 1 2 されてよい。幾つかの実施形態では、変換 2 4 1 2 は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換 2 4 1 2 は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換 2 4 1 2 は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。

10

【0187】

サーバ 2 4 5 0 の処理検証器 2 4 4 7 は、生成された検証キー 2 4 6 2 を第 2 のピア 2 4 7 5 から受け取った確認キー 2 4 8 1 と比較し、処理生成器 2 2 4 6 が認証結果 2 4 6 4 を生成してよい。検証キー 2 4 6 2 が第 2 のピア 2 4 7 5 から受け取った確認キー 2 4 8 1 と同一である場合、結果は肯定的、例えば認証成功であってよい。検証キー 2 4 6 2 が、第 2 のピア 2 4 7 5 から受け取った確認キー 2 4 8 1 と同一でない場合、認証結果 2 4 6 4 は、否定的、例えば、認証失敗又は脅威であってよい。サーバ 2 4 5 0 の処理マイグレータ 2 4 4 2 は、認証結果 2 4 6 4 をデータベース 2 4 5 7 に格納してよい。幾つかの実施形態では、認証結果 2 4 6 4 は、登録方法の間に生成された関連する配布キー 2 4 5 3 と共に格納される。

20

【0188】

サーバ 2 4 5 0 は、新しい配布キー 2 4 5 3 を 1 又は複数の第 2 のピア 2 4 7 5 に送ってよい。図 1 9 を参照すると、サーバ 1 9 5 0 は、サーバ 1 9 5 0 のデータベース 1 9 5 7 に新しいピアリスト 1 9 5 8 を生成してよい。幾つかの実施形態では、サーバ 1 9 5 0 は、新しい受信者コード 1 9 5 2 と新しい配布コード 1 9 5 6 の任意の組合せを割り当ててよく、新しい受信者コード 1 9 5 2 と新しい配布コード 1 9 5 6 の任意の組合せを使用して、1 又は複数の配布キー 1 9 0 0 を配布することと同一であってもよい方法で新しい配布キー 1 9 5 3 を生成してよい。サーバ 1 9 5 0 は、新たに生成された配布キー 1 9 5 3 を、第 2 のピア 1 9 7 5 に送ってよく、第 2 のピア 1 9 7 5 は、以前に配布キー 1 9 5 3 を格納していた第 2 のピア 1 9 7 5 とは異なってよい。

30

【0189】

ウェブ認証方法は、バーコードを生成することと、1 又は複数のキーを生成することと、ウェブセッションを確立することとを含んでよい。更に、ウェブ認証システムは、1 又は複数の第 1 のデバイス、第 2 のデバイス、第 1 のサーバ、第 2 のサーバ、及びインターネットアプリケーションの間での通信を含んでよい。1 又は複数の第 1 のデバイス、第 2 のデバイス、第 1 のサーバ、及び第 2 のサーバは、少なくともプロセッサと送受信機とを含んでよい。1 又は複数の第 1 のデバイス及び 1 又は複数の第 2 のデバイスは更に、それぞれのメモリを含んでよい。幾つかの実施形態では、1 又は複数の第 1 のデバイス及び 1 又は複数の第 2 のデバイスの各々は、表示装置を含んでよい。1 又は複数の第 1 のデバイス及び 1 又は複数の第 2 のデバイスの各々は、バーコードをスキャンするための手段を含んでよい。1 又は複数の第 1 のサーバ及び第 2 のサーバは、更にデータベースを含んでよい。

40

【0190】

第 1 のデバイス、第 2 のデバイス、第 1 のサーバ、及び第 2 のサーバの送信機は、外部ソースと情報を送受信するように構成されてよい。幾つかの実施形態では、第 1 のデバイ

50

スは、第2のデバイス、第1のサーバ、及び第2のサーバの任意の組合せとの間で情報を送受信するように構成されてよい。第1のサーバ及び第2のサーバは、第1のデバイスと第2のデバイスの両方との間で情報を送受信するように構成されてよく、第2のデバイスは、第1のサーバ、第1のデバイス、及び第2のサーバの任意の組合せとの間で情報を送受信するように構成されてよい。第1のデバイス及び第2のデバイスのメモリと、サーバのデータベースとは、情報を格納し、情報の取得を可能にするように構成されてよい。表示装置は、更に、ユーザがディスプレイと対話する、例えば、データの入力、キャラクタの選択、オブジェクトの選択などを行うための手段を含んでよい。インターネットアプリケーションは、第1のサーバ、第2のサーバ、第1のデバイス、及び第2のデバイスの任意の組合せから情報を送信又は受信するように構成されてよい。

10

【0191】

第1のデバイス、第2のデバイス、第1のサーバ、及び第2のサーバのプロセッサは、処理マイグレータ、データマニピュレータ、データ変換器、処理生成器、及び処理検証器を含んでよい。処理マイグレータは、第1のデバイス、第2のデバイス、第1のサーバ、又は第2のサーバ内の1つの構成要素から、第1のデバイス、第2のデバイス、第1のサーバ又は第2のサーバ内の別の構成要素にデータをマイグレートするように構成されてよい。例えば、限定ではないが、処理マイグレータは、第1のデバイスのメモリから第1のデバイスのプロセッサにデータを移動させるように、或いは、第2のデバイスのプロセッサから第2のデバイスの送受信機にデータを移動させるように構成されてよい。データマニピュレータは、データを操作するように構成されていてよく、例えば、結合、分離、分離及び再結合、リオーダなどの処理を行うように構成されていてよい。例えば、限定ではないが、第1のデバイスのデータマニピュレータは、1又は複数のキャラクタ列を第1の部分と第2の部分に分割するように構成されてよく、サーバのデータマニピュレータは、データの第1の部分とデータの第2の部分とを結合して、1又は複数のキャラクタ列を生成するように構成されてよい。

20

【0192】

データ変換器は、第1のキャラクタ列を第2のキャラクタ列に変換するように構成されてよく、ここで、第1のキャラクタ列及び第2のキャラクタ列の各々は、長さ、構成、又は配置のうちの任意の1又は複数が異なってよい。幾つかの実施形態では、データ変換器は、ハッシュアルゴリズムを第1のキャラクタ列に適用するように構成されてよい。他の実施形態では、データ変換器は、第1のキャラクタ列に暗号化プロトコルを適用するように構成されてよい。まだ他の実施形態では、データ変換器は、第1のキャラクタ列に復号プロトコルを適用するように構成されてもよい。更に他の実施形態では、データ変換器は、ハッシュアルゴリズム、暗号化プロトコル、復号プロトコル、又はデータ変換の他の既知の方法の任意の組合せを、第1のキャラクタ列に適用して、第2のキャラクタ列を生成するように構成されてよい。

30

【0193】

処理生成器は、データを生成するように構成されてよい。幾つかの実施形態では、データは、任意の長さの1又は複数のキャラクタ列を含んでよく、バーコードなどを含んでもよい。幾つかの実施形態では、データは、ランダムな方法又は規則的な方法で生成されてよい。処理検証器は、2つ以上のデータを比較して、それらのデータが同一であるか異なるかを判定するように構成されてよい。幾つかの実施形態では、処理検証器及び処理生成器は対になって、第1のキャラクタ列と第2のキャラクタ列が同一であるかどうかを判断し、第1のキャラクタ列と第2のキャラクタ列の同一性に基づいて応答を生成してよい。

40

【0194】

ウェブ認証方法は、図25に示すように、バーコードを生成することを含んでよい。バーコード2500の生成は、インターネットアプリケーション2590で開始されてよい。幾つかの実施形態では、ユーザは、ログイン要求によってインターネットアプリケーション2590でバーコード2500の生成を開始してよい。第1の合意プロトコルペア2646は、処理生成器2646によって生成されてよい。幾つかの実施形態では、第1の

50

合意プロトコルペア 2 6 4 6 は、インターネットアプリケーション 2 5 9 0 にて処理生成器 2 6 4 6 によって生成されてよい。第 1 のキー合意プロトコルペア 2 5 2 6 は、当技術分野の通常の技術を有する者に普通に知られている任意のキー合意プロトコルペアを含んでよい。幾つかの実施形態では、第 1 のキー合意プロトコルペア 2 5 2 6 は、楕円曲線ディフィーヘルマン (Elliptic-curve Diffie-Hellman) (E C D H) ペアを含んでよい。幾つかの実施形態によれば、インターネットアプリケーション 2 5 9 0 は、第 1 のサーバ 2 5 2 5 に情報を送るように構成されてよい。処理マイグレータ 2 6 4 2 は、インターネットアプリケーション 2 5 9 0 の送受信機 2 5 4 1 に情報を転送してよい。インターネットアプリケーション 2 5 9 0 は、第 1 の公開キー 2 5 0 3、第 1 の秘密キー 2 5 0 4、及びバーコード 2 5 0 5 を生成するために必要な他の情報の任意の組合せを送ってよい。

10

【0195】

幾つかの実施形態では、第 1 のサーバ 2 5 2 5 は、インターネットアプリケーション 2 5 9 0 から情報を受け取るように構成されてよい。第 1 のサーバ 2 5 2 5 の送受信機 2 5 4 1 は、第 1 の公開キー 2 5 0 3、第 1 の秘密キー 2 5 0 4、及びインターネットアプリケーション 2 5 9 0 からバーコード 2 5 0 0 を生成するための他の必要な情報の任意の組合せを受け取ってよい。第 1 のサーバ 2 5 2 5 は、ランダムキー 2 5 2 7 を生成してよく、ランダムキー 2 5 2 7 は、第 1 のサーバ 2 5 2 5 の処理生成器 2 6 4 6 によって生成されてよい。ランダムキー 2 5 2 7 は、任意の長さの 1 又は複数のキャラクタ列を含んでよく、キャラクタは、文字、数字、及び記号を含んでよい。幾つかの実施形態では、バーコード 2 5 0 5 が生成されてよい。処理生成器 2 5 4 6 は、バーコード前駆体を使用してバーコード 2 5 0 5 を生成してよい。バーコード 2 5 0 5 は、任意のタイプのバーコード 2 5 0 5 を含んでよく、限定ではなく、任意の線形バーコード、2 次元バーコード、又は当技術分野の通常の技術を有する者に普通に知られている任意のタイプの読取可能なインデシア (indicia) を含んでいる。幾つかの実施形態では、バーコード 2 5 0 5 は、Q R コード (登録商標) を含んでよい。バーコード 2 5 0 5 は、第 1 の公開キー 2 5 0 3、第 1 の秘密キー 2 5 0 4、ランダムキー 2 5 2 7、及びバーコード 2 5 0 0 を生成するために必要な他の情報の任意の組合せから生成されてよい。特定の実施形態では、バーコード 2 5 0 5 は、第 1 のサーバ 2 5 2 5 のデータマニピュレータ 2 5 4 4 によって生成されてよく、また、第 1 の公開キー 2 5 0 3 及びランダムキー 2 5 2 7 に基づいてよい。第 1 のサーバ 2 5 2 5 は、インターネットアプリケーション 2 5 9 0 に情報を転送するように構成されてよい。幾つかの実施形態では、第 1 のサーバ 2 5 2 5 の送受信機 2 5 4 1 は、インターネットアプリケーション 2 5 9 0 に情報を送るように構成されてよい。特定の実施形態では、第 1 のサーバ 2 5 2 5 は、バーコード 2 5 0 5 をインターネットアプリケーション 2 5 9 0 に送ってよい。インターネットアプリケーション 2 5 9 0 は、送受信機 2 5 4 1 でバーコード 2 5 0 5 を受け取ってよく、インターネットアプリケーション 2 5 9 0 の表示装置 2 5 9 0 にバーコード 2 5 0 5 を表示してよい。

20

30

【0196】

ウェブ認証方法は、図 2 6、図 2 7、及び図 2 8 に示すように、1 又は複数のキーを生成することを含んでよい。図 2 6 を参照すると、1 又は複数のキー 2 6 0 0 を生成することは、第 1 のデバイス 2 6 5 0 がバーコード 2 6 0 5 をスキャンすることを含んでよい。第 1 のデバイス 2 6 5 0 のデータマニピュレータ 2 6 4 4 は、バーコード 2 6 0 5 内に含まれる情報から、ランダムキー 2 6 2 7、第 1 の公開キー 2 6 0 3、又はランダムキー 2 6 2 7 及び第 1 の公開キー 2 6 0 3 を生成してもよい。データマニピュレータ 2 6 4 4 は、1 又は複数のキー 2 6 0 0 を生成するために、バーコード 2 6 0 5 内に含まれる任意の情報を外挿してよい。更に、第 1 のデバイス 2 6 5 0 の処理生成器 2 6 4 6 は、第 2 のキー合意プロトコルペア 2 6 5 1 を生成してよい。第 2 のキー合意プロトコルペア 2 6 5 1 は、当技術分野の通常の技術を有する者に普通に知られている任意のキー合意プロトコルペアを含んでよい。幾つかの実施形態では、第 2 のキー合意プロトコルペア 2 6 5 1 は、楕円曲線ディフィーヘルマン (E C D H) ペアを含んでよい。幾つかの実施形態では、第 2 のキー合意プロトコルペア 2 6 5 1 は、第 2 の秘密キー 2 6 5 2 と第 2 の公開キー 2 6

40

50

5 3とを含んでよい。バーコード2 6 0 5から外挿された (extrapolated) 第2の秘密キー2 6 5 2と第1の公開キー2 6 0 3は、データマニピュレータ2 6 4 4によって結合されて、秘密キー2 6 5 4が生成されてよい。第1のデバイス2 6 5 0の処理生成器2 6 4 6は、ソルト2 6 5 5、初期化ベクトル2 6 5 6、及び反復数2 6 5 7の任意の組合せを生成してもよい。特定の実施形態では、第1のデバイス2 6 5 0の処理生成器2 6 4 6は、ソルト2 6 5 5、初期化ベクトル2 6 5 6、及び反復数2 6 5 7の各々を生成してよい。ソルト2 6 5 5、初期化ベクトル2 6 5 6、及び反復数2 6 5 7の各々は、任意の長さの1又は複数のキャラクタ列を含んでよく、キャラクタは、文字、数字、又は記号の任意の組合せを含んでよい。初期化ベクトル2 6 5 6は、n個に等しいキャラクタ数であってよく、更にIVの第1の部分2 6 5 8及びIVの第2の部分2 6 5 9を含んでもよい。IVの第1の部分2 6 5 8及びIVの第2の部分2 6 5 9は、それぞれ、1乃至n-1のキャラクタ数であってよい。反復数2 6 5 7は、nに等しいキャラクタ数であってよく、更にINの第1の部分2 6 6 0とINの第2の部分2 6 6 1を含んでよい。INの第1の部分2 6 6 0及びINの第2の部分2 6 6 1は、それぞれ、1乃至n-1のキャラクタ数であってよい。データマニピュレータ2 6 4 4は、IVの第1の部分2 6 5 8及びIVの第2の部分2 6 5 9を初期化ベクトル2 6 5 6から生成してよい。データマニピュレータ2 6 4 4は、INの第1の部分2 6 6 0及びINの第2の部分2 6 6 1を反復数2 6 5 7から生成してよい。幾つかの実施形態によれば、秘密キー2 6 5 4、ソルト2 6 5 5、IVの第1の部分2 6 5 8、及びINの第1の部分2 6 6 0は、データ変換器2 6 4 5によって、マスクされた秘密キー2 6 6 2、マスクされたソルト2 6 6 3、マスクされたIVの第1の部分2 6 6 4、及びマスクされたINの第1の部分2 6 6 5にそれぞれ変換されてよい。幾つかの実施形態では、初期化ベクトル2 6 5 6は、データ変換器2 6 4 5によってマスクされたIVの第1の部分2 6 6 4に変換されてよい。同様に、反復数2 6 5 7は、データ変換器2 6 4 5によって、マスクされたINの第1の部分2 6 6 5に変換2 6 1 2されてよい。幾つかの実施形態では、変換2 6 1 2は、ハッシュアルゴリズムを使用することを含んでよい。他の実施形態では、変換2 6 1 2は、暗号化方法を使用することを含んでよい。更に他の実施形態では、変換2 6 1 2は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。幾つかの実施形態では、反復数2 6 5 7は、INの第1の部分2 6 6 0及びINの第2の部分2 6 6 1を生成せず、そのまま残っていてよく、その結果生じるINの第1の部分2 6 6 0は変換2 6 1 2されなくてよい。

【0 1 9 7】

第1のデバイス2 6 5 0の処理生成器2 6 4 6は、クライアントキー2 6 6 6を生成してよい。クライアントキー2 6 6 6は、任意の長さの1又は複数のキャラクタ列を含んでよく、キャラクタは、文字、数字、又は記号の任意の組合せを含んでよい。幾つかの実施形態では、クライアントキー2 6 6 6は、データ変換器2 6 4 5によって第1のマスクされたクライアントキー2 6 6 7に変換2 6 1 2されてよい。他の実施形態では、クライアントキー2 6 6 7は、データ変換器2 6 4 5によって、第2のマスクされたクライアントキー2 6 6 8に変換2 6 1 2されてよい。更に他の実施形態では、クライアントキー2 6 6 7は、データ変換器2 6 4 5によって、第1のマスクされたクライアントキー2 6 6 7及び第2のマスクされたクライアントキー2 6 6 8のそれぞれに変換2 6 1 2されてよい。変換2 6 1 2は、ハッシュアルゴリズムを使用することを含んでよい。更に、変換2 6 1 2は、暗号化手段を使用することを含んでよい。幾つかの実施形態では、変換2 6 1 2は、ハッシュアルゴリズムと暗号化方法の組合せを使用することを含んでよい。第1のデバイス2 6 5 0は、第1のサーバ2 6 2 5に情報を送るように構成されてよい。幾つかの実施形態では、第1のデバイス2 6 5 0の送受信機2 6 4 1は、第1のマスクされたクライアントキー2 6 6 7、第2のマスクされたクライアントキー2 6 6 8、マスクされた秘密キー2 6 6 2、マスクされたソルト2 6 6 3、マスクされたIVの第1の部分2 6 6 4、及びマスクされたINの第1の部分2 6 6 5の任意の組合せを第1のサーバ2 6 2 5に送るように構成されてよい。幾つかの実施形態では、第1のデバイス2 6 5 0は、IVの第2の部分2 6 5 9及びINの第2の部分2 6 6 1のそれぞれを第1のデバイス2 6 5 0

10

20

30

40

50

の表示装置 2669 に表示してよい。特定の実施形態では、反復数 2657 は、その全体として第 1 のデバイス 2650 の表示装置 2669 に表示されてよい。

【0198】

図 27 を参照すると、1 又は複数のキーを生成することは、第 1 のサーバ 2725 が第 1 のデバイス 2750 から情報を受け取ることを含んでよい。幾つかの実施形態では、第 1 のサーバ 2725 の送受信機 2741 は、マスクされた秘密キー 2762、第 2 のマスクされたクライアントキー 2768、マスクされたソルト 2763、マスクされた IV の第 1 の部分 2764、マスクされた IN の第 1 の部分 2765、及びマスクされた第 1 のマスクされたクライアントキー 2767 の任意の組合せを第 1 のデバイス 2750 から受け取ってよい。幾つかの実施形態では、第 1 のサーバ 2725 の処理マイグレータ 2742 は、第 1 のデバイス 2750 から受け取ったマスクされた秘密キー 2762、第 2 のマスクされたクライアントキー 2768、マスクされたソルト 2763、マスクされた IV の第 1 部分 2764、マスクされた IN の第 1 の部分 2765、及び第 1 のマスクされたクライアントキー 2767 のうちの 1 又は複数を、第 1 のサーバ 2725 のデータベース 2729 に格納してよい。特定の実施形態によれば、第 1 のサーバ 2725 の処理マイグレータ 2742 は、第 1 のサーバ 2725 のデータベース 2729 に第 1 のマスクされたクライアントキー 2767 を格納してもよい。

【0199】

第 1 のサーバ 2725 は、インターネットアプリケーション 2790 に情報を送るよう構成されてよい。特定の実施形態では、第 1 のサーバ 2725 の送受信機 2741 は、マスクされた秘密キー 2762、第 2 のマスクされたクライアントキー 2768、マスクされたソルト 2763、マスクされた IV の第 1 の部分 2764、マスクされた IN の第 1 の部分 2765、及び第 1 のマスクされたクライアントキー 2767 の任意の組合せを第 1 のサーバ 2725 に送ってよい。特定の実施形態では、第 1 のサーバ 2725 の送受信機 2741 は、マスクされた秘密キー 2762、第 2 のマスクされたクライアントキー 2768、マスクされたソルト 2763、マスクされた IV の第 1 の部分 2764、及びマスクされた IN の第 1 の部分 2765 を第 1 のサーバ 2725 に送ってよい。他の実施形態では、第 1 のサーバ 2725 の送受信機 2741 は、マスクされた秘密キー 2762、第 2 のマスクされたクライアントキー 2768、マスクされたソルト 2763、及びマスクされた IV の第 1 の部分 2764 の任意の組合せ（今後、纏めて「受信データ 2728」と称される）をインターネットアプリケーション 2790 に送ってよい。

【0200】

図 28 に図示されているように、1 又は複数のキーを生成すること 2800 は、インターネットアプリケーション 2890 の送受信機 2841 が第 1 のサーバ 2825 から、受け取ったデータ 2828 を受け取ることを含んでよい。第 1 のデバイス 2850 は、ユーザ入力 2869 を含んでよい。このユーザ入力 2869 は、IV の第 2 の部分 2659 及び IN の第 2 の部分 2661（図 26 参照）を含んでよく、それらはそれぞれキャラクタ列を含んでよい。ユーザ入力 2869 は、IV の第 1 の部分と反復数とを含んでよい。幾つかの実施形態では、ユーザ入力 2869 は、第 1 のデバイス 2850 の表示装置 2869 に表示されてよい。1 又は複数のキーを生成することは、ユーザ入力 2869 がインターネットアプリケーション 2890 に入力されることを含んでよい。インターネットアプリケーション 2890 のデータ変換器 2844 は、受け取ったデータ 2828 を、秘密キー 2854、IN の第 1 の部分 2860、ソルト 2855、IV の第 1 の部分 2858、及びクライアントキー 2866 のうちの 1 又は複수에交換 2812 してよい。交換 2812 は、ハッシュアルゴリズムを使用することを含んでよい。更に、交換 2812 は、暗号化手段を使用することを含んでよい。交換は、復号手段を使用することを含んでよい。幾つかの実施形態では、交換 2812 は、ハッシュアルゴリズム、暗号化方法、又は復号方法の任意の組合せを使用することを含んでよい。幾つかの実施形態では、インターネットアプリケーション 2890 のデータ変換器 2844 は、ユーザ入力 2869 と受信データ 2828 の両方を使用して、秘密キー 2854、IN の第 1 の部分 2860、ソルト 28

55、IVの第1の部分2858、及びクライアントキー2866のうちの1又は複数へと受信データを変換2812してよい。処理マイグレータ2842は、インターネットアプリケーション2890の記憶装置2891にクライアントキー2866を格納してよい。インターネットアプリケーション2890のデータ変換器2845は、クライアントキー2866を第3のマスクされたクライアントキー2892に変換2812してよい。幾つかの実施形態では、第3のマスクされたクライアントキー2892は、処理マイグレータ2842によって、インターネットアプリケーション2890の送受信機2841にマイグレートされてよい。インターネットアプリケーション2890の送受信機2841は、第3のマスクされたクライアントキー2892を第1のサーバ2825に送ってもよい。
【0201】

ウェブ認証方法は、ウェブセッションを確立することを含んでよい。図29に図示されているように、第1のサーバ2825の送受信機2941は、インターネットアプリケーション2990から、第3のマスクされたクライアントキー2992を受け取ってよい。幾つかの実施形態では、第1のサーバ2825の処理マイグレータ2942は、格納されている第1のマスクされたクライアントキー2967を第1のサーバ2825のデータベース2929から取得してよい。処理検証器2947は、取得した第1のマスクされたクライアントキー2967を、インターネットアプリケーション2990から受け取った第3のマスクされたクライアントキー2992と比較してよい。処理生成器2946は、第1のマスクされたクライアントキー2967と第3のマスクされたクライアントキー2992の同一性に基づいて結果2930を生成してよい。第1のサーバ2825の送受信機2941は、その結果2930を第2のサーバ2980に送ってよい。第2のサーバ2980の送受信機2941は、第1のサーバ2825から結果2930を受け取りウェブトークン2931を生成してよい。ウェブトークン2931は、処理生成器2946によって生成されてよい。幾つかの実施形態では、ウェブトークン2931は、ウェブセッションの確立を承認するための当該分野で知られている任意の手段であってよい。第2のサーバ2980は、生成されたウェブトークン2931を第1のサーバ2825に送ってよい。第1のサーバ2825の送受信機2941は、第2のサーバ2980からウェブトークン2931を受け取り、受け取ったウェブトークン2931をインターネットアプリケーション2990に送ってよい。インターネットアプリケーション2990の送受信機2941は、第1のサーバ2825からウェブトークン2931を受け取ってよい。

【0202】

幾つかの実施形態では、インターネットアプリケーションは、受け取ったウェブトークンを第2のサーバに送ってよい。第2のサーバは、ウェブブラウザからウェブトークンを受け取り、ウェブセッションを確立してよい。更に、第2のサーバは、第1のサーバに情報を送るように構成されてよい。幾つかの実施形態では、第2のサーバは、インターネットアプリケーションからのウェブトークンの受信に関する情報を送ってよい。インターネットアプリケーションからのウェブトークンの受信に関する情報は、インターネットアプリケーションに関する任意の情報、インターネットアプリケーションのユーザに関する情報、ウェブセッションへのアクセスに関する情報、本明細書に記載されたシステムの任意の構成要素に関する場所的及び／又は時間的な情報を含むが、これらに限定されない。第1のサーバは、ウェブトークンの受信に関する情報を第2のサーバから受け取ってよい。幾つかの実施形態では、第1のサーバは、第1のデバイスに情報を送るように構成されてよく、限定ではないが、ウェブトークンの受信に関する情報が含まれてよい。

【0203】

本明細書に記載された実施形態の他の変形例もまた、本発明の範囲から逸脱することなく実施され得ることは、当業者には理解されるであろう。その他の変更もそれ故に可能である。

10

20

30

40

50

【図面】

【図 1】

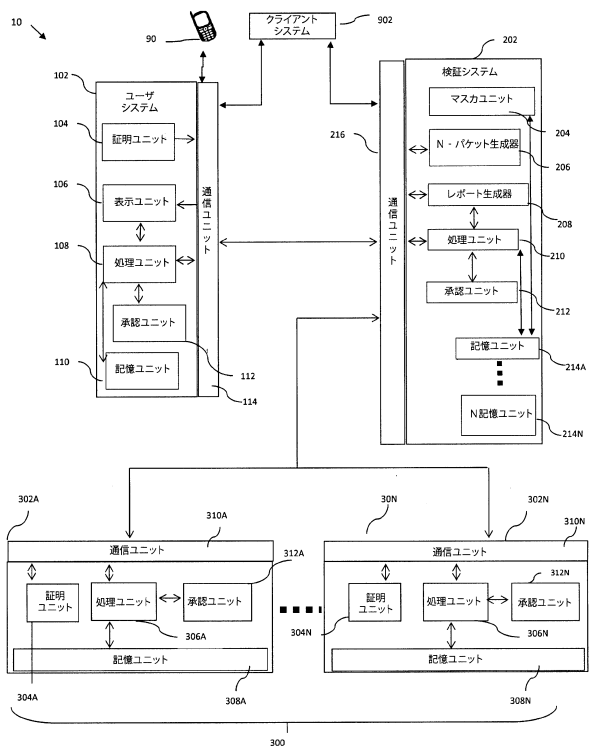


FIG. 1

【図 2】

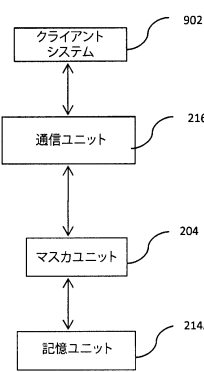


FIG. 2

【図 3】

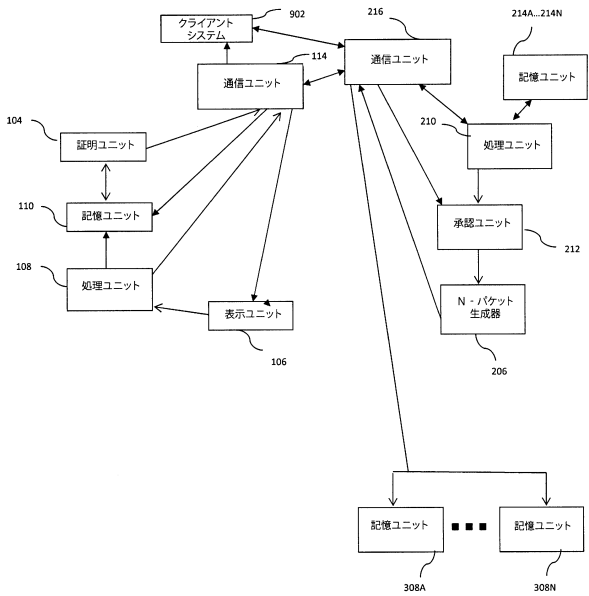


FIG. 3

【図 4】

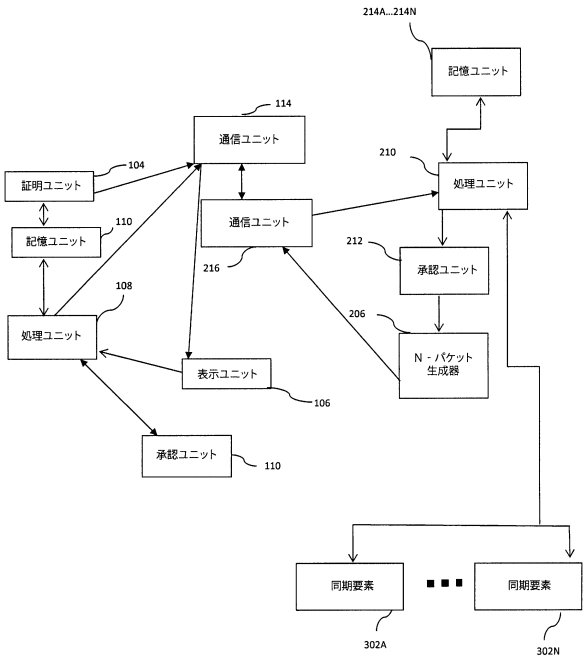


FIG. 4

【図 5】

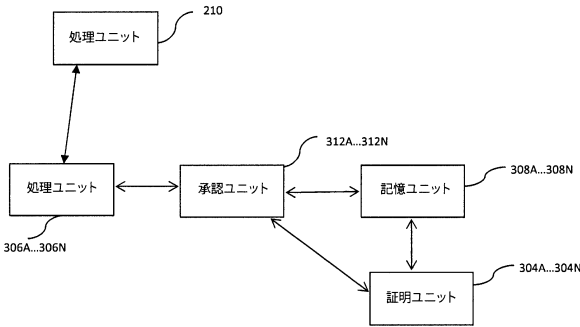


FIG. 5

【図 6】

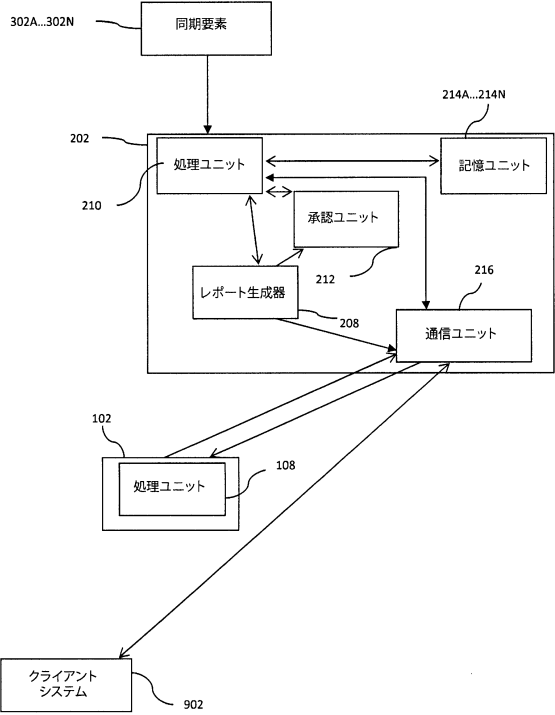


FIG. 6

【図 7】

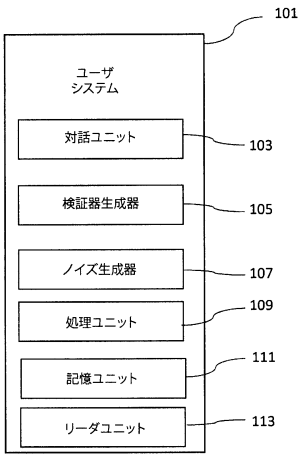


FIG. 7

【図 8】

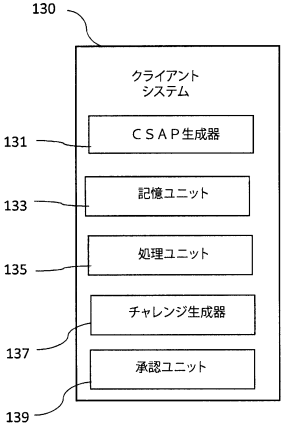


FIG. 8

10

20

30

40

50

【図 9】

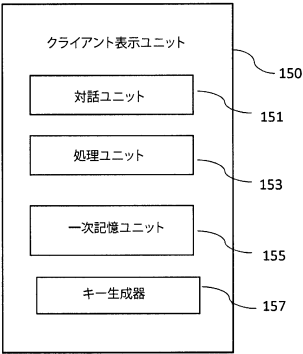


FIG. 9

【図 10】

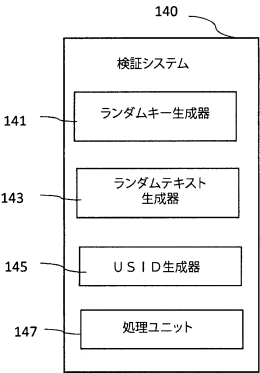


FIG. 10

【図 11】

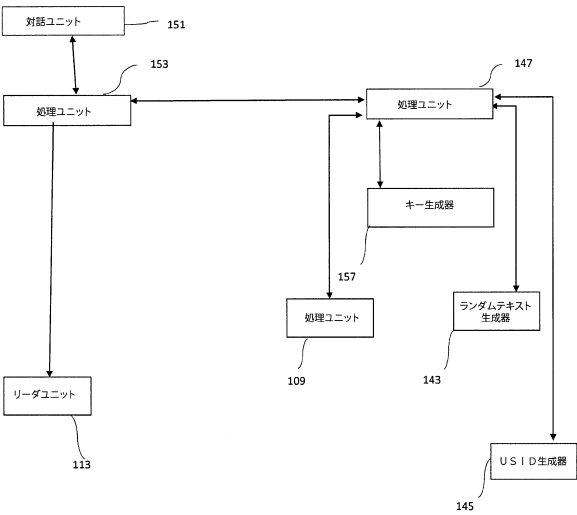


FIG. 11

【図 12】

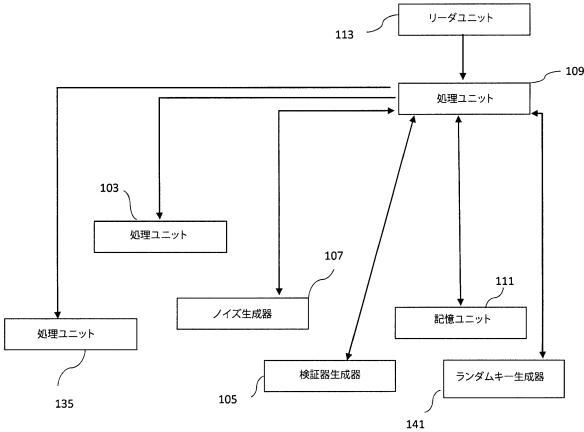


FIG. 12

【図 1 3】

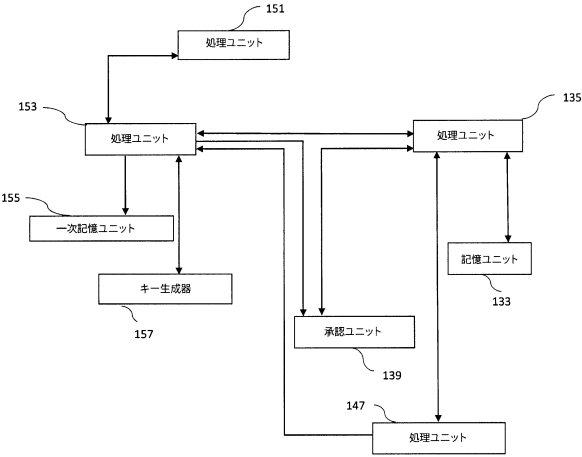


FIG. 13

【図 1 4】

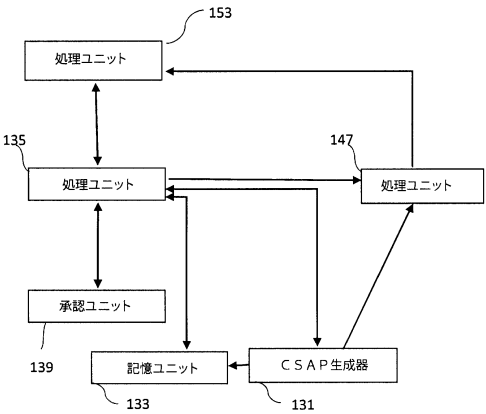


FIG. 14

【図 1 5】

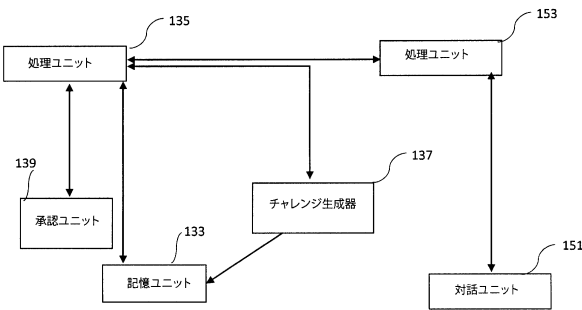


FIG. 15

【図 1 6】

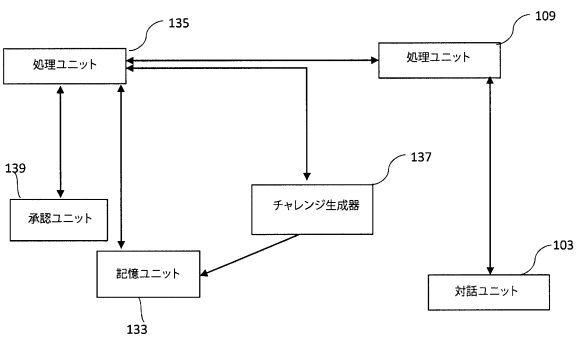


FIG. 16

10

20

30

40

50

【図 17】

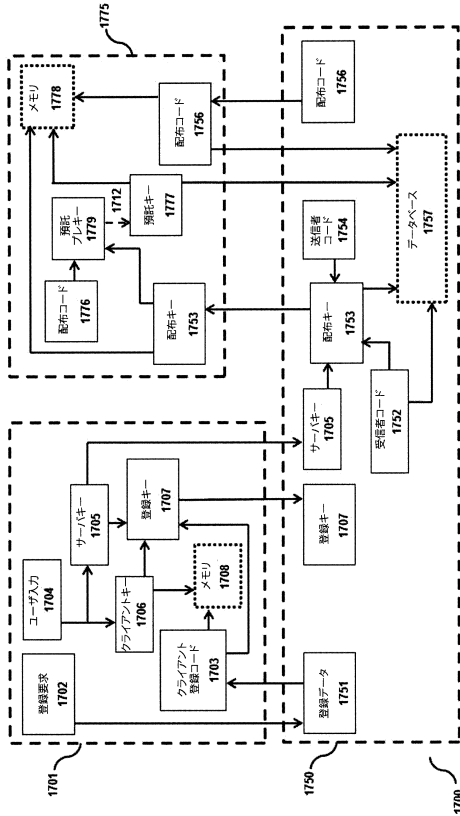


FIGURE 17

【図 18】

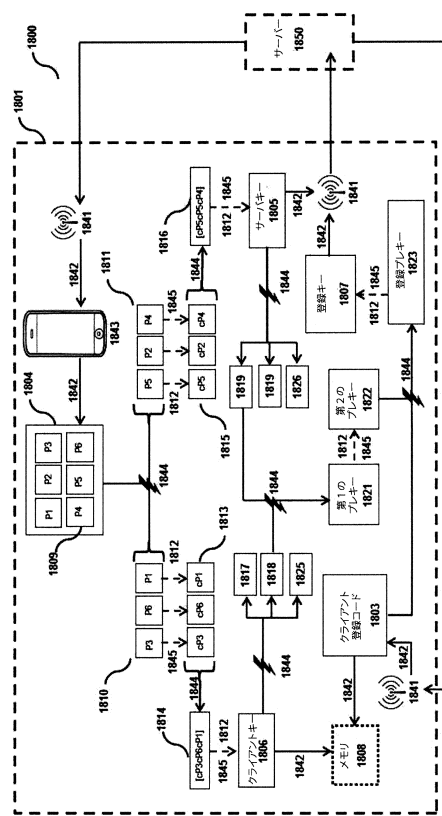


FIGURE 18

【図 19】

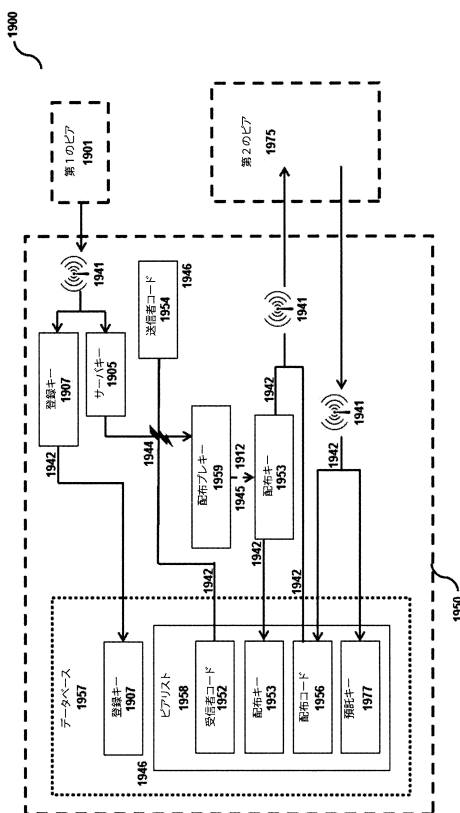


FIGURE 19

【図 20】

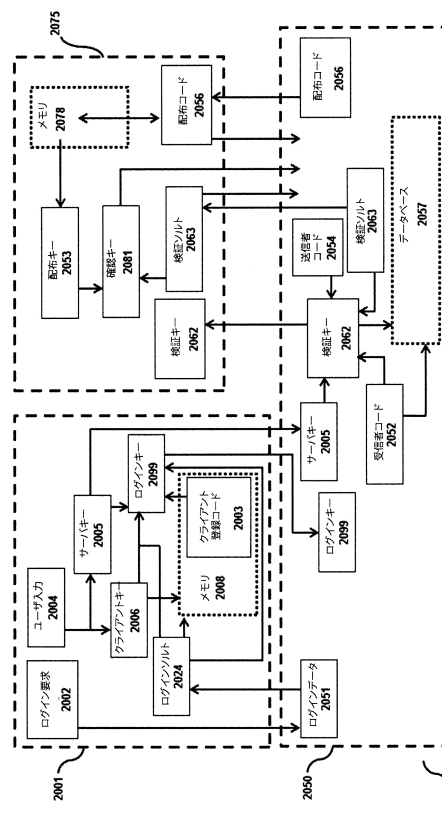


FIGURE 20

【図 2 1】

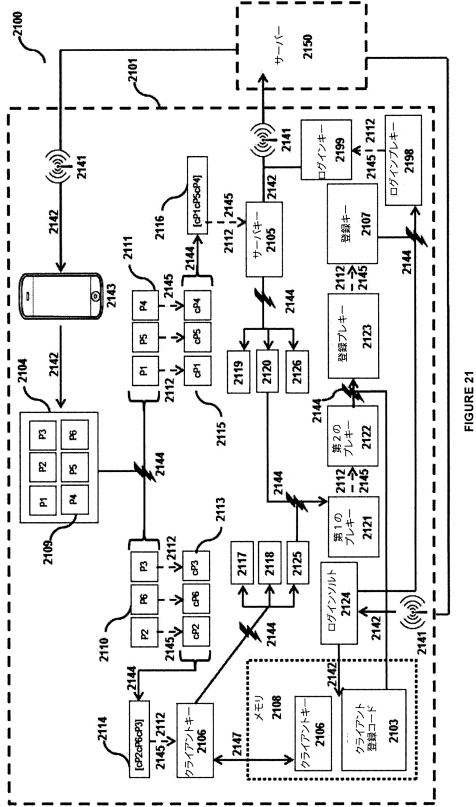


FIGURE 21

【図 2 2】

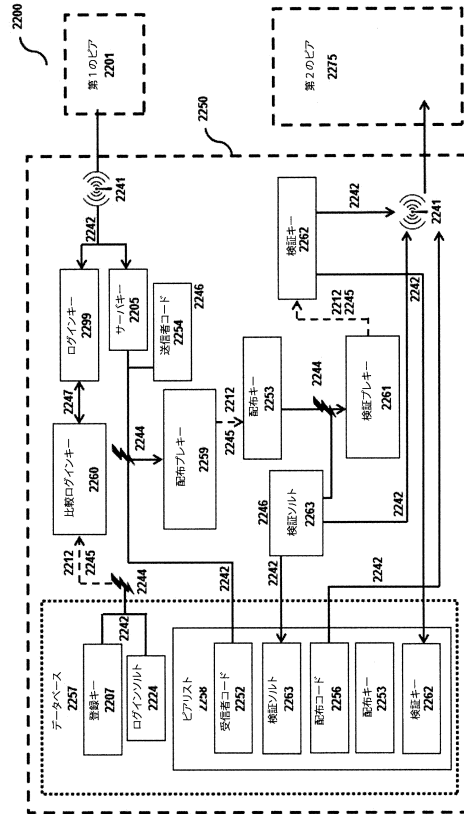


FIGURE 22

【図 2 3】

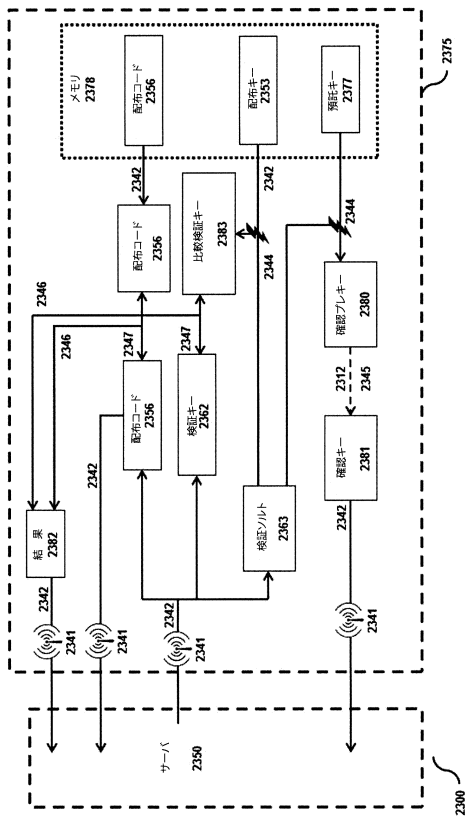


FIGURE 23

【図 2 4】

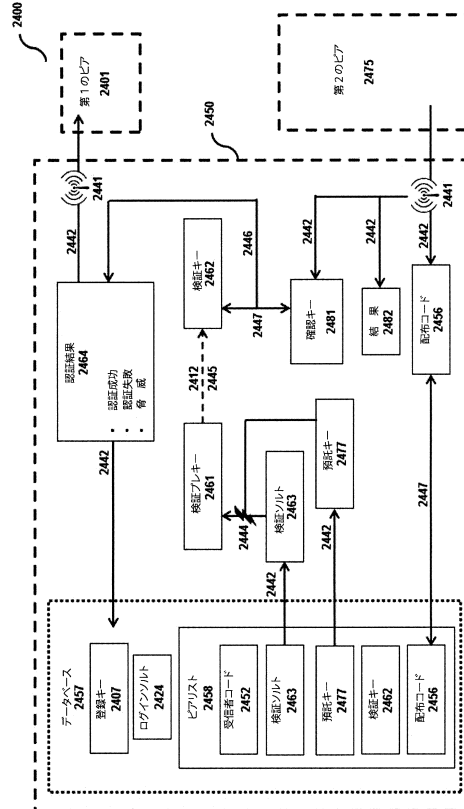


FIGURE 24

10

20

30

40

50

【図 25】

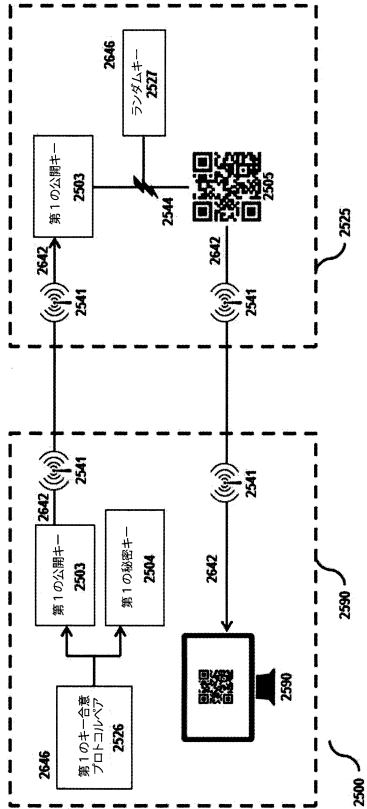


FIGURE 25

【図 26】

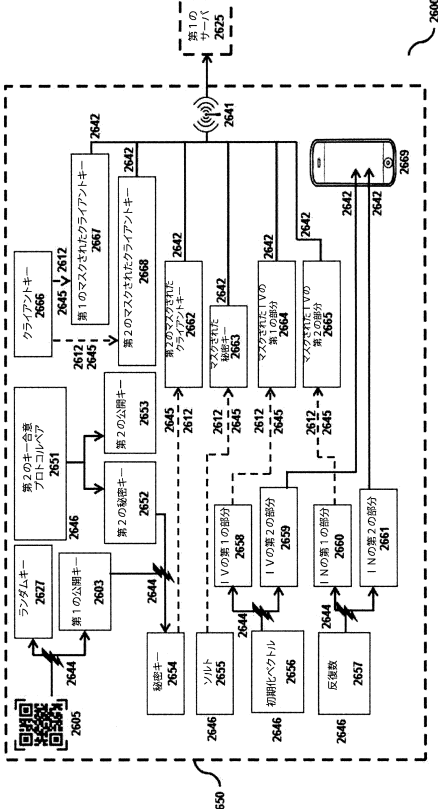


FIGURE 26

【図 27】

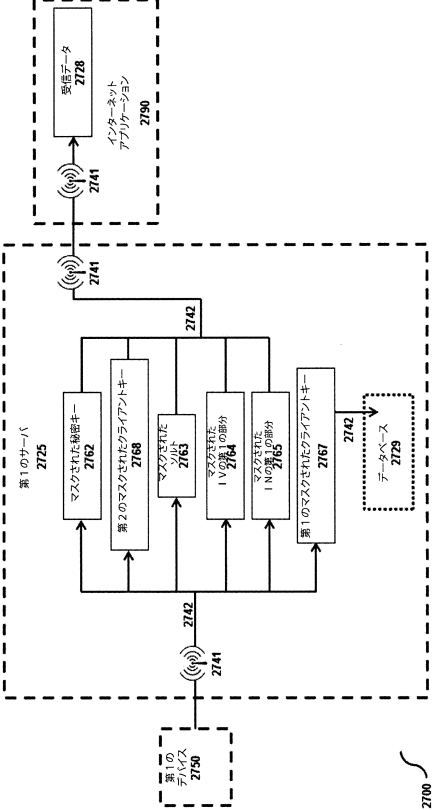


FIGURE 27

【図 28】

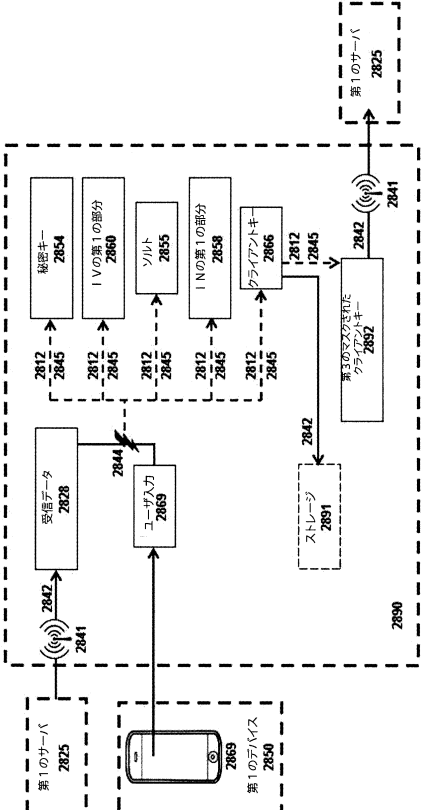


FIGURE 28

10

20

30

40

50

【図 29】

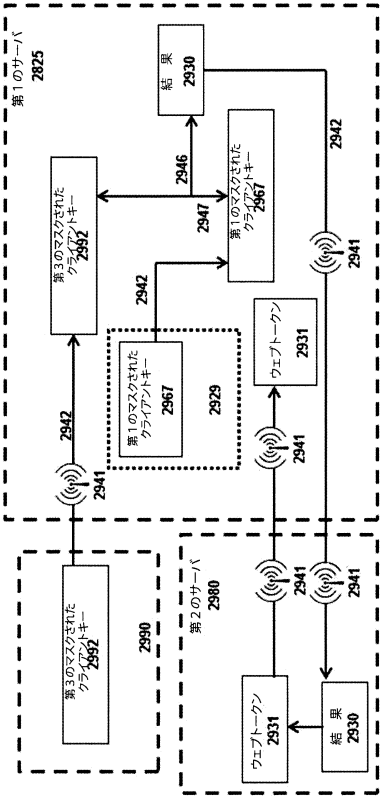


FIGURE 29

フロントページの続き

- (56)参考文献 特開 2009-169614 (JP, A)
特開 2004-213247 (JP, A)
特表 2006-511104 (JP, A)
国際公開第 2017/134759 (WO, A1)
- (58)調査した分野 (Int.Cl., DB名)
H04L 9/08
H04L 9/32
G09C 1/00