(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7599475号
(P7599475)

(45)発行日　令和6年12月13日(2024.12.13)

(24)登録日　令和6年12月5日(2024.12.5)

(51)国際特許分類

H04L 9/32 (2006.01)	H04L	9/32	200Z
G06F 21/62 (2013.01)	G06F	21/62	354
G06F 21/60 (2013.01)	G06F	21/60	320

請求項の数　20　（全71頁）

(21)出願番号　特願2022-506148(P2022-506148)
(86)(22)出願日　令和2年7月29日(2020.7.29)
(65)公表番号　特表2022-544067(P2022-544067A)
(43)公表日　令和4年10月17日(2022.10.17)
(86)国際出願番号　PCT/US2020/044086
(87)国際公開番号　WO2021/021942
(87)国際公開日　令和3年2月4日(2021.2.4)
審査請求日　令和5年7月28日(2023.7.28)
(31)優先権主張番号　62/881,025
(32)優先日　令和1年7月31日(2019.7.31)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　514108838
マジック リープ，インコーポレイテッド
Ｍａｇｉｃ Ｌｅａｐ，Ｉｎｃ．
アメリカ合衆国 フロリダ ３３３２２，プランテーション，ウエスト サンライズ ブールバード ７５００
７５００ Ｗ ＳＵＮＲＩＳＥ ＢＬＶＤ，ＰＬＡＮＴＡＴＩＯＮ，ＦＬ ３３３２２ ＵＳＡ
(74)代理人　100078282
弁理士　山本 秀策
(74)代理人　100113413
弁理士　森下 夏樹
(74)代理人　100181674
弁理士　飯田 貴敏

最終頁に続く

(54)【発明の名称】　分散型台帳を使用した拡張現実のためのユーザデータ管理

(57)【特許請求の範囲】

【請求項１】

ユーザデバイスであって、

コンピュータ実行可能命令を記憶するように構成される１つ以上のコンピュータ可読記憶デバイスと、

頭部搭載型ディスプレイと、

前記ユーザデバイスの周囲を検出するように構成されるセンサと、

ネットワークインターフェースと、

１つ以上のハードウェアコンピュータプロセッサであって、前記１つ以上のハードウェアコンピュータプロセッサは、前記１つ以上のコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記ユーザデバイスに、

第１のユーザと関連付けられるプライバシ設定を受信することと、

前記ネットワークインターフェースを介して分散型台帳マネージャに、分散型台帳上への記憶のために、前記プライバシ設定を伝送することであって、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、前記分散型台帳に書き込むように構成されるソフトウェアとを備える、ことと、

前記ネットワークインターフェースを介して前記分散型台帳マネージャから、前記第１のユーザと関連付けられる第１のパブリック暗号化キーを受信することと、

前記センサを介して、前記ユーザデバイスと関連付けられる環境データを収集することであって、前記センサは、前記ユーザデバイスの周囲を検出するように構成される、こ

と、
前記第１のパブリック暗号化キーに基づいて、前記環境データを暗号化することと、
前記暗号化された環境データにメタデータを意味論的にタグ付けすることであって、前記メタデータは、少なくとも、前記ユーザデバイスについての識別情報を示す、ことと、
前記ネットワークインターフェースを介してデータプラットフォームに、前記意味論的にタグ付けされ暗号化された環境データを伝送することであって、前記データプラットフォームは、１つ以上のデータベースを備える、ことと
を行わせる、１つ以上のハードウェアコンピュータプロセッサと
を備える、ユーザデバイス。
【請求項２】
前記データプラットフォームのオペレータは、前記オペレータが、前記環境データを解読するための適切なキーを有していないため、前記環境データへの直接アクセスを有さない、請求項１に記載のユーザデバイス。
【請求項３】
前記第１のパブリック暗号化キーは、前記プライバシ設定に少なくとも部分的に基づいて、前記分散型台帳マネージャによって生成される、請求項１に記載のユーザデバイス。
【請求項４】
前記センサは、加速度計、カメラ、およびＧＰＳセンサのうちの１つ以上のものを含む、請求項１に記載のユーザデバイス。
【請求項５】
前記メタデータは、暗号化されない、請求項１に記載のユーザデバイス。
【請求項６】
ユーザデバイスであって、
コンピュータ実行可能命令を記憶するように構成される１つ以上のコンピュータ可読記憶デバイスと、
頭部搭載型ディスプレイと、
１つ以上のハードウェアコンピュータプロセッサであって、前記１つ以上のハードウェアコンピュータプロセッサは、前記１つ以上のコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記ユーザデバイスに、
第１のユーザと関連付けられるプライバシ設定を受信することと、
分散型台帳マネージャに、前記プライバシ設定を伝送することと、
前記分散型台帳マネージャから、前記第１のユーザと関連付けられる第１のパブリック暗号化キーを受信することと、
１つ以上のセンサを介して、前記ユーザデバイスと関連付けられる環境データを収集することと、
前記第１のパブリック暗号化キーに基づいて、前記環境データを暗号化することと、
前記暗号化された環境データにメタデータを意味論的にタグ付けすることであって、前記メタデータは、少なくとも、前記ユーザデバイスについての識別情報を示す、ことと、
データプラットフォームに、前記意味論的にタグ付けされ暗号化された環境データを伝送することと
を行わせる、１つ以上のハードウェアコンピュータプロセッサと
を備える、ユーザデバイス。
【請求項７】
前記第１のパブリック暗号化キーは、前記プライバシ設定に少なくとも部分的に基づいて、前記分散型台帳マネージャによって生成される、請求項６に記載のユーザデバイス。
【請求項８】
前記１つ以上のセンサは、前記ユーザデバイスの周囲を検出するように構成される、請求項６に記載のユーザデバイス。
【請求項９】
前記１つ以上のセンサは、加速度計、カメラ、およびＧＰＳセンサのうちの１つ以上の

ものを含む、請求項６に記載のユーザデバイス。
【請求項１０】
前記メタデータは、暗号化されない、請求項６に記載のユーザデバイス。
【請求項１１】
前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、前記分散型台帳に書き込むように構成されるソフトウェアとを備える、請求項６に記載のユーザデバイス。
【請求項１２】
前記データプラットフォームは、１つ以上のデータベースを備える、請求項６に記載のユーザデバイス。
【請求項１３】
前記データプラットフォームのオペレータは、前記環境データを解読するための適切なキーを有していない、請求項６に記載のユーザデバイス。
【請求項１４】
ユーザデバイスによって実施される方法であって、
前記ユーザデバイスが、第１のユーザと関連付けられるプライバシ設定を受信することと、
前記ユーザデバイスが、分散型台帳マネージャに、前記プライバシ設定を伝送することと、
前記ユーザデバイスが、前記分散型台帳マネージャから、前記第１のユーザと関連付けられる第１のパブリック暗号化キーを受信することと、
前記ユーザデバイスが、１つ以上のセンサを介して、ユーザデバイスと関連付けられる環境データを収集することと、
前記ユーザデバイスが、前記第１のパブリック暗号化キーに基づいて、前記環境データを暗号化することと、
前記ユーザデバイスが、前記暗号化された環境データにメタデータを意味論的にタグ付けすることであって、前記メタデータは、少なくとも、前記ユーザデバイスについての識別情報を示す、ことと、
前記ユーザデバイスが、データプラットフォームに、前記意味論的にタグ付けされ暗号化された環境データを伝送することであって、前記データプラットフォームは、１つ以上のデータベースを備える、ことと
を含む、方法。
【請求項１５】
前記第１のパブリック暗号化キーは、前記プライバシ設定に少なくとも部分的に基づいて、前記分散型台帳マネージャによって生成される、請求項１４に記載の方法。
【請求項１６】
前記１つ以上のセンサは、前記ユーザデバイスの周囲を検出するように構成される、請求項１４に記載の方法。
【請求項１７】
前記１つ以上のセンサは、加速度計、カメラ、およびＧＰＳセンサのうちの１つ以上のものを含む、請求項１４に記載の方法。
【請求項１８】
前記メタデータは、暗号化されない、請求項１４に記載の方法。
【請求項１９】
前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、前記分散型台帳に書き込むように構成されるソフトウェアとを備える、請求項１４に記載の方法。
【請求項２０】
前記データプラットフォームのオペレータは、前記環境データを解読するための適切なキーを有していない、請求項１４に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】

（関連出願の相互参照）
本願は、参照することによってその全体として本明細書に組み込まれる、２０１９年７月３１日に出願され、「ＵＳＥＲ　ＤＡＴＡ　ＭＡＮＡＧＥＭＥＮＴ　ＦＯＲ　ＡＵＧＭＥＮＴＥＤ　ＲＥＡＬＩＴＹ　ＵＳＩＮＧ　Ａ　ＤＩＳＴＲＩＢＵＴＥＤ　ＬＥＤＧＥＲ」と題された、米国特許出願第６２／８８１，０２５号の優先権の利益を主張する。
（限定著作権表示）
【０００２】
本特許文書の開示の一部は、著作権保護の対象となる資料を含む。著作権者は、米国特許商標庁の特許ファイルまたは記録に見られるような、特許文書または特許開示の任意の者によるファクシミリ複製に異議を唱えないが、それ以外の場合は全ての著作権を留保する。
【０００３】
本開示は、セキュアデータ記憶、転送、およびアクセスのためのシステムおよび方法に関し、特に、データのルールベースの記憶、転送、およびアクセスのためのシステムおよび方法に関する。本システムおよび方法は、拡張、複合、または仮想現実環境内で使用されることができる。
【背景技術】
【０００４】
企業は、そのユーザまたは顧客に関する膨大な量のユーザデータを収集する。本ユーザデータは、例えば、標的化広告または統計的分析のために、コンピュータモデルを構築するために使用されることができる。企業は、本ユーザデータを利益のために収集および販売し、これは、ユーザのプライバシを犠牲にすることになり得、かつユーザの知識の及ばないところで行われ得る。最近、ユーザデータを収集および販売する、多くの企業が、誤った方法でデータを販売しているか、またはデータを盗難し、ブラックマーケットで後に販売している、サードパーティによって、セキュリティ侵害もしくはハッキングされているかのいずれかの状態にある。
【発明の概要】
【課題を解決するための手段】
【０００５】
本明細書に開示されるものは、分散型台帳を使用して、ユーザプライバシ設定を設定し、それにアクセスし、かつそれを修正するためのシステムおよび方法である。ある側面では、本システムは、ユーザと関連付けられる、プライバシ設定を受信し、少なくとも部分的に、プライバシ設定に基づいて、ソフトウエアコントラクトを作成することができる。本システムは、次いで、プライベートキーおよびパブリックキーを作成することができる。本システムは、ソフトウエアコントラクトおよびプライベートキーを分散型台帳内に記憶し、パブリックキーを、ユーザデータを収集し、ユーザデータにメタデータを意味論的にタグ付けするように構成される、デバイスに伝送することができる。
【０００６】
別の側面では、本システムは、データ仮想化プラットフォームから、特定のユーザに関するユーザデータへのアクセスのための要求を受信することができる。次いで、本システムは、以前に記憶されたソフトウエアコントラクトを検索し、ユーザと関連付けられる、ソフトウエアコントラクトの最新バージョンを特定し、検索に基づいて、ユーザデータが共有されることが許可されることを決定することができる。本システムは、次いで、データ仮想化プラットフォームに、ユーザデータをデータプラットフォームから抽出する方法に関する命令を伝送することができる。次いで、本システムは、データプラットフォームから、ユーザデータがデータ仮想化プラットフォームに伝送されたことの確認を受信することができ、次いで、本システムは、ユーザと関連付けられる、プライベート暗号化キーおよびソフトウエアコントラクトにアクセスすることができる。本システムは、次いで、データ照合システムに、プライベート暗号化キーおよびソフトウエアコントラクトと関連付けられる詳細を伝送し、次いで、データ照合システムから、プライベート暗号化キーお

よびユーザデータがマッチングすることのインジケーションを受信することができる。次いで、プライベート暗号化キーおよびユーザデータがマッチングすることの受信されたインジケーションに基づいて、データ仮想化プラットフォームに、データ仮想化プラットフォームがデータプラットフォームから受信された暗号化されたユーザデータを解読し得るように、プライベート暗号化キーを伝送する。

【０００７】

さらに別の側面では、本システムは、データ仮想化プラットフォームから、特定のユーザと関連付けられる、ユーザデータへのアクセスのための要求を受信することができる。次いで、本システムは、以前に記憶されたソフトウエアコントラクトを検索し、ユーザと関連付けられる、ソフトウエアコントラクトを特定し、検索に基づいて、ユーザデータが共有されることが許可されることを決定することができる。いくつかの側面では、ユーザデータは、１つまたはそれを上回るサードパーティサービスからのサードパーティデータを含むことができる。本システムは、次いで、サードパーティデータを１つまたはそれを上回るサードパーティサービスから抽出する方法に関する命令を準備し、データ仮想化プラットフォームに伝送し、データ仮想化プラットフォームから、サードパーティデータがデータ仮想化プラットフォームによって正常に読み出されたことの通知を受信することができる。通知の受信に応じて、本システムは、パブリック暗号化キーをソフトウエアコントラクトから読み出し、データ仮想化プラットフォームに、データ仮想化プラットフォームが、サードパーティデータを暗号化し、データプラットフォームに、記憶のために、サードパーティデータを伝送し得るように、パブリック暗号化キーを伝送することができる。

【０００８】

本明細書に説明される拡張現実、仮想現実、および複合現実システムは、単に、実施例であって、実施形態または側面を説明される特定の技術に限定するものとして解釈されるべきではない。したがって、拡張現実、仮想現実、および複合現実システムが、本明細書に説明されるが、実施形態および開示は、データを収集または生成する任意の消費者電子デバイスに適用されることができることを理解されたい。

【０００９】

本明細書に説明される主題の１つまたはそれを上回る実装の詳細は、付随の図面および下記の説明に記載される。他の特徴、側面、および利点は、説明、図面、ならびに請求項から明白となるであろう。本概要または以下の詳細な説明のいずれも、本開示の主題の範囲を定義または限定することを主張するものではない。本開示の付加的実施形態は、本開示の付加的説明としての役割を果たし得る、添付の請求項を参照して下記に説明される。

本発明は、例えば、以下を提供する。

（項目１）

ユーザデバイスであって、

コンピュータ実行可能命令を記憶するように構成される１つまたはそれを上回るコンピュータ可読記憶デバイスと、

頭部搭載型ディスプレイと、

前記ユーザデバイスの周囲を検出するように構成されるセンサと、

分散型台帳マネージャであって、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える、分散型台帳マネージャと、

１つまたはそれを上回るデータベースを備えるデータプラットフォームと、

ネットワークインターフェースと、

１つまたはそれを上回るハードウェアコンピュータプロセッサであって、前記１つまたはそれを上回るハードウェアコンピュータプロセッサは、前記１つまたはそれを上回るコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記ユーザデバイスに、

前記第１のユーザと関連付けられるプライバシ設定を受信することと、

分散型台帳マネージャに、前記プライバシ設定を伝送することと、

前記分散型台帳マネージャから、前記第１のユーザと関連付けられる第１のパブリック暗号化キーを受信することと、
前記センサを介して、前記ユーザデバイスと関連付けられる環境データを収集することと、
前記第１のパブリック暗号化キーに基づいて、前記環境データを暗号化することと、
前記暗号化された環境データにメタデータを意味論的にタグ付けすることであって、前記メタデータは、少なくとも、前記ユーザデバイスについての識別情報を示す、ことと、
データプラットフォームに、前記意味論的にタグ付けされ暗号化された環境データを伝送することであって、前記データプラットフォームは、１つまたはそれを上回るデータベースを備える、ことと
を行わせる、１つまたはそれを上回るハードウェアコンピュータプロセッサと
を備える、ユーザデバイス。
（項目２）
前記パブリック暗号化キーは、少なくとも部分的に、前記プライバシ設定に基づいて、前記分散型台帳マネージャによって生成される、項目１に記載のユーザデバイス。
（項目３）
前記センサは、加速度計、カメラ、およびＧＰＳセンサのうちの１つまたはそれを上回るものを含む、項目１－２のいずれか１項に記載のユーザデバイス。
（項目４）
前記メタデータは、暗号化されない、項目１－３のいずれか１項に記載のユーザデバイス。
（項目５）
ユーザデバイスであって、
コンピュータ実行可能命令を記憶するように構成される１つまたはそれを上回るコンピュータ可読記憶デバイスと、
頭部搭載型ディスプレイと、
ネットワークインターフェースと、
１つまたはそれを上回るハードウェアコンピュータプロセッサであって、前記１つまたはそれを上回るハードウェアコンピュータプロセッサは、前記１つまたはそれを上回るコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記ユーザデバイスに、
前記第１のユーザと関連付けられるプライバシ設定を受信することと、
前記分散型台帳マネージャに、前記ネットワークインターフェースを介して、分散型台帳上への記憶のために、前記プライバシ設定を伝送することと、
前記分散型台帳マネージャから、前記ネットワークインターフェースを介して、前記第１のユーザと関連付けられる第１のパブリック暗号化キーを受信することと、
前記センサを介して、前記ユーザデバイスと関連付けられる環境データを収集することであって、前記センサは、前記ユーザデバイスの周囲を検出するように構成される、ことと、
前記第１のパブリック暗号化キーに基づいて、前記環境データを暗号化することと、
前記暗号化された環境データにメタデータを意味論的にタグ付けすることであって、前記メタデータは、少なくとも、前記ユーザデバイスについての識別情報を示す、ことと、
データプラットフォームに、前記ネットワークインターフェースを介して、前記意味論的にタグ付けされ暗号化された環境データを伝送することであって、前記データプラットフォームは、１つまたはそれを上回るデータベースを備える、ことと
を行わせる、１つまたはそれを上回るハードウェアコンピュータプロセッサと
を備える、ユーザデバイス。
（項目６）
前記パブリック暗号化キーは、少なくとも部分的に、前記プライバシ設定に基づいて、前記分散型台帳マネージャによって生成される、項目５に記載のユーザデバイス。

（項目７）
前記センサは、加速度計、カメラ、およびＧＰＳセンサのうちの１つまたはそれを上回るものを含む、項目５－６のいずれか１項に記載のユーザデバイス。
（項目８）
前記メタデータは、暗号化されない、項目５－７のいずれか１項に記載のユーザデバイス。
（項目９）
方法であって、
第１のユーザと関連付けられるプライバシ設定を受信するステップと、
分散型台帳マネージャに、前記プライバシ設定を伝送するステップであって、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える、ステップと、
前記分散型台帳マネージャから、前記第１のユーザと関連付けられる第１のパブリック暗号化キーを受信するステップと、
センサを介して、前記ユーザデバイスと関連付けられる環境データを収集するステップであって、前記センサは、前記ユーザデバイスの周囲を検出するように構成される、ステップと、
前記第１のパブリック暗号化キーに基づいて、前記環境データを暗号化するステップと、
前記暗号化された環境データにメタデータを意味論的にタグ付けするステップであって、前記メタデータは、少なくとも、前記ユーザデバイスについての識別情報を示す、ステップと、
データプラットフォームに、前記意味論的にタグ付けされ暗号化された環境データを伝送するステップであって、前記データプラットフォームは、１つまたはそれを上回るデータベースを備える、ステップと
を含む、方法。
（項目１０）
前記パブリック暗号化キーは、少なくとも部分的に、前記プライバシ設定に基づいて、前記分散型台帳マネージャによって生成される、項目９に記載の方法。
（項目１１）
前記センサは、加速度計、カメラ、およびＧＰＳセンサのうちの１つまたはそれを上回るものを含む、項目９－１０のいずれか１項に記載の方法。
（項目１２）
前記メタデータは、暗号化されない、項目９－１１のいずれか１項に記載の方法。
（項目１３）
システムであって、
１つまたはそれを上回るコンピュータ可読記憶デバイスであって、前記１つまたはそれを上回るコンピュータ可読記憶デバイスは、
コンピュータ実行可能命令と、
ユーザと関連付けられるプライバシ設定と、
ソフトウエアコントラクトであって、前記ソフトウエアコントラクトは、少なくとも部分的に、前記プライバシ設定に基づく、ソフトウエアコントラクトと、
前記ユーザと関連付けられるプライベート暗号化キーであって、各ユーザは、１つのプライベート暗号化キーを割り当てられる、プライベート暗号化キーと、
前記ユーザと関連付けられるパブリック暗号化キーであって、各ユーザは、１つのパブリック暗号化キーを割り当てられる、パブリック暗号化キーと、
前記ユーザと関連付けられるユーザデータと、
を記憶するように構成される、１つまたはそれを上回るコンピュータ可読記憶デバイスと、
ネットワークインターフェースと、
１つまたはそれを上回るハードウェアコンピュータプロセッサであって、前記１つまた

はそれを上回るハードウェアコンピュータプロセッサは、前記１つまたはそれを上回るコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記システムに、
　第１のデバイスから、前記ネットワークインターフェースを介して、前記ユーザのうちの第１のユーザと関連付けられる第１のプライバシ設定を受信することと、
　少なくとも部分的に、前記第１のプライバシ設定に基づいて、第１のソフトウエアコントラクトを作成することであって、前記第１のソフトウエアコントラクトは、前記第１のプライバシ設定を実装するように構成される、ことと、
　前記第１のユーザと関連付けられる第１のプライベートキーを作成および暗号化することと、
　第１のソフトウエアコントラクトおよび暗号化された第１のプライベートキーを記憶することと、
　前記第１のユーザと関連付けられる第１のパブリックキーを作成することと、
　前記第１のデバイスに、前記ネットワークインターフェースを介して、前記第１のパブリックキーを伝送することであって、前記第１のデバイスは、第１のユーザデータを収集し、前記第１のユーザデータに第１のメタデータを意味論的にタグ付けするように構成される、ことと
　を行わせる、１つまたはそれを上回るハードウェアコンピュータプロセッサと
　を備える、システム。
（項目１４）
　前記第１のソフトウエアコントラクトは、スマートコントラクトである、項目１３に記載のシステム。
（項目１５）
　前記第１のソフトウエアコントラクトおよび暗号化された第１のプライベートキーは、分散型台帳内に記憶される、項目１４に記載のシステム。
（項目１６）
　１つまたはそれを上回るデータベースを備えるデータプラットフォームをさらに備え、
　前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、前記システムに、
　前記第１のデバイスから、第１のユーザデータを受信することであって、前記第１のユーザデータは、１つまたはそれを上回る意味論タグで意味論的にタグ付けされる、ことと、
　第１のユーザデータを前記データプラットフォーム内に記憶することであって、前記データプラットフォームは、前記分散型台帳と別個である、ことと、
　ハッシュ識別値を計算し、前記第１のユーザデータに割り当てることと、
　前記１つまたはそれを上回る意味論タグおよびハッシュ識別値を分散型台帳内にエンコーディングすることと
　を行わせるように構成される、項目１３－１５のいずれか１項に記載のシステム。
（項目１７）
　前記第１のプライバシ設定は、暗号化される、項目１３－１６のいずれか１項に記載のシステム。
（項目１８）
　前記第１のユーザデータは、少なくとも部分的に、前記第１のデバイスによって収集された環境データに基づく、項目１３－１７のいずれか１項に記載のシステム。
（項目１９）
　前記第１のユーザデータは、暗号化される、項目１３－１８のいずれか１項に記載のシステム。
（項目２０）
　前記第１のメタデータは、前記第１のユーザデータが収集された日付および時間を示すデータと、前記第１のユーザデータを収集したデバイスと、前記データが第１のユーザデータであることのインジケーションとを含む、項目１３－１９のいずれか１項に記載のシ

ステム。
（項目２１）
方法であって、
第１のデバイスから、複数のユーザのうちの第１のユーザと関連付けられる第１のプライバシ設定を受信するステップであって、前記複数のユーザの各ユーザは、プライバシ設定、パブリック暗号化キー、およびプライベート暗号化キーと関連付けられる、ステップと、
少なくとも部分的に、前記第１のプライバシ設定に基づいて、第１のソフトウエアコントラクトを作成するステップであって、前記第１のソフトウエアコントラクトは、前記第１のプライバシ設定を実装するように構成される、ステップと、
前記第１のユーザと関連付けられる第１のプライベートキーを作成および暗号化するステップと、
第１のソフトウエアコントラクトおよび暗号化された第１のプライベートキーを記憶するステップと、
前記第１のユーザと関連付けられる第１のパブリックキーを作成するステップと、
前記第１のデバイスに、前記第１のパブリックキーを伝送するステップであって、前記第１のデバイスは、第１のユーザデータを収集し、前記第１のユーザデータに第１のメタデータを意味論的にタグ付けするように構成される、ステップと
を含む、方法。
（項目２２）
前記第１のソフトウエアコントラクトは、スマートコントラクトである、項目２１に記載の方法。
（項目２３）
前記第１のソフトウエアコントラクトおよび暗号化された第１のプライベートキーは、分散型台帳内に記憶される、項目２２に記載の方法。
（項目２４）
第１のユーザデータを受信するステップであって、前記第１のユーザデータは、１つまたはそれを上回る意味論タグで意味論的にタグ付けされる、ステップと、
第１のユーザデータをデータプラットフォーム内に記憶するステップであって、前記データプラットフォームは、前記分散型台帳と別個であり、１つまたはそれを上回るデータベースを備える、ステップと、
ハッシュ識別値を計算し、前記第１のユーザデータに割り当てるステップと、
前記１つまたはそれを上回る意味論タグおよびハッシュ識別値を分散型台帳内にエンコーディングするステップと
をさらに含む、項目２１－２３のいずれか１項に記載の方法。
（項目２５）
前記第１のプライバシ設定は、暗号化される、項目２１－２４のいずれか１項に記載の方法。
（項目２６）
前記第１のユーザデータは、少なくとも部分的に、前記第１のデバイスによって収集された環境データに基づく、項目２１－２５のいずれか１項に記載の方法。
（項目２７）
前記第１のユーザデータは、暗号化される、項目２１－２６のいずれか１項に記載の方法。
（項目２８）
前記第１のメタデータは、前記第１のユーザデータが収集された日付および時間を示すデータと、前記第１のユーザデータを収集したデバイスと、前記データが第１のユーザデータであることのインジケーションとを含む、項目２１－２７のいずれか１項に記載の方法。
（項目２９）

システムであって、
１つまたはそれを上回るコンピュータ可読記憶デバイスであって、前記１つまたはそれを上回るコンピュータ可読記憶デバイスは、
コンピュータ実行可能命令と、
ユーザと関連付けられるプライバシ設定と、
ソフトウエアコントラクトであって、前記ソフトウエアコントラクトは、少なくとも部分的に、前記プライバシ設定に基づく、ソフトウエアコントラクトと、
前記ユーザと関連付けられるプライベート暗号化キーであって、各ユーザは、１つのプライベート暗号化キーを割り当てられる、プライベート暗号化キーと
を記憶するように構成される、１つまたはそれを上回るコンピュータ可読記憶デバイスと、
ユーザデータを表示するように構成されるユーザインターフェースを備えるデータ仮想化プラットフォームと、
前記ユーザと関連付けられるユーザデータを記憶するように構成されるデータプラットフォームと、
データ照合システムであって、前記データ照合システムは、前記ユーザデータが前記プライベート暗号化キーで解読され得るように、プライベート暗号化キーが暗号化されたユーザデータにマッチングするかどうかを決定するように構成される、データ照合システムと、
ネットワークインターフェースと、
１つまたはそれを上回るハードウェアコンピュータプロセッサであって、前記１つまたはそれを上回るハードウェアコンピュータプロセッサは、前記１つまたはそれを上回るコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記システムに、
前記データ仮想化プラットフォームから、前記ネットワークインターフェースを介して、第１のユーザデータへのアクセスのための要求を受信することであって、前記第１のユーザデータは、第１のユーザと関連付けられる、ことと、
前記ソフトウエアコントラクトを検索し、前記第１のユーザと関連付けられる前記ソフトウエアコントラクトの第１のソフトウエアコントラクトの最新バージョンを特定することと、
前記検索に基づいて、少なくとも部分的に、前記第１のソフトウエアコントラクトに基づいて、前記第１のユーザデータが共有されることが許可されることを決定することと、
前記第１のユーザデータを前記データプラットフォームから抽出するための命令を準備し、前記データ仮想化プラットフォームに、前記ネットワークインターフェースを介して伝送することと、
前記データプラットフォームから、前記ネットワークインターフェースを介して、前記第１のユーザデータが、暗号化されており、前記データ仮想化プラットフォームに伝送されたことの確認を受信することであって、前記確認は、伝送された前記第１のユーザデータの説明を含む、ことと、
前記確認の受信に応じて、前記第１のユーザと関連付けられる第１のプライベート暗号化キーおよび前記第１のソフトウエアコントラクトにアクセスすることと、
前記データ照合システムに、前記ネットワークインターフェースを介して、前記第１のソフトウエアコントラクトと関連付けられる前記第１のプライベート暗号化キーおよび詳細を伝送することと、
前記データ照合システムから、前記ネットワークインターフェースを介して、前記第１のプライベート暗号化キーおよび前記第１のユーザデータがマッチングすることのインジケーションを受信することと、
前記第１のプライベート暗号化キーおよび前記第１のユーザデータがマッチングすることの前記受信されたインジケーションに基づいて、前記データ仮想化プラットフォームに、前記ネットワークインターフェースを介して、前記データ仮想化プラットフォームが前

記データプラットフォームから受信された前記暗号化された第１のユーザデータを解読し得るように、前記第１のプライベート暗号化キーを伝送することと
を行わせる、１つまたはそれを上回るハードウェアコンピュータプロセッサと
を備える、システム。
（項目３０）
前記第１のプライベート暗号化キーを含む前記プライベート暗号化キーは、分散型台帳内に記憶される、項目２９に記載のシステム。
（項目３１）
前記第１のソフトウエアコントラクトを含む前記ソフトウエアコントラクトは、スマートコントラクトである、項目２９－３０のいずれか１項に記載のシステム。
（項目３２）
前記第１のソフトウエアコントラクトを含む前記ソフトウエアコントラクトは、分散型台帳内に記憶される、項目２９－３１のいずれか１項に記載のシステム。
（項目３３）
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、前記システムに、
第２のプライベート暗号化キーを生成することと、
前記第２のプライベート暗号化キーを含む第２のソフトウエアコントラクトを生成および記憶することと、
前記データプラットフォームに、前記ネットワークインターフェースを介して、前記データプラットフォームが、前記第１のユーザデータを前記第１のプライベート暗号化キーで解読し、前記第１のユーザデータを前記第２のプライベート暗号化キーで再暗号化し得るように、前記第１のプライベート暗号化キーおよび前記第２のプライベート暗号化キーを伝送することと
を行わせるように構成される、項目２９－３２のいずれか１項に記載のシステム。
（項目３４）
前記第２のソフトウエアコントラクトはまた、前記データ仮想化プラットフォームに伝送された前記第１のユーザデータの説明を記憶する、項目３３に記載のシステム。
（項目３５）
少なくとも部分的に、前記第１のソフトウエアコントラクトに基づいて、共有されることが許可されることが決定される前記第１のユーザデータはまた、少なくとも部分的に、前記データ仮想化プラットフォームにアクセスする購入者デバイスと関連付けられるアカウントに基づき、前記購入者デバイスは、第１のユーザデータへのアクセスのための要求と関連付けられる、項目２９－３４のいずれか１項に記載のシステム。
（項目３６）
方法であって、
データ仮想化プラットフォームから、第１のユーザデータへのアクセスのための要求を受信するステップであって、前記第１のユーザデータは、第１のユーザと関連付けられ、前記データ仮想化プラットフォームは、前記ユーザデータを表示するように構成されるユーザインターフェースを備える、ステップと、
ソフトウエアコントラクトを検索し、前記第１のユーザと関連付けられる前記ソフトウエアコントラクトの第１のソフトウエアコントラクトの最新バージョンを特定するステップであって、前記ソフトウエアコントラクトは、少なくとも部分的に、前記プライバシ設定に基づく、ステップと、
前記検索に基づいて、少なくとも部分的に、前記第１のソフトウエアコントラクトに基づいて、前記第１のユーザデータが共有されることが許可されることを決定するステップと、
前記第１のユーザデータをデータプラットフォームから抽出するための命令を準備し、前記データ仮想化プラットフォームに伝送するステップであって、前記データプラットフォームは、前記ユーザと関連付けられるユーザデータを記憶するように構成される、ステ

ップと、
前記データプラットフォームから、前記第１のユーザデータが、暗号化されており、前記データ仮想化プラットフォームに伝送されたことの確認を受信するステップであって、前記確認は、伝送された前記第１のユーザデータの説明を含む、ステップと、
前記確認の受信に応じて、前記第１のユーザと関連付けられる第１のプライベート暗号化キーおよび前記第１のソフトウエアコントラクトにアクセスするステップと、
データ照合システムに、前記第１のソフトウエアコントラクトと関連付けられる前記第１のプライベート暗号化キーおよび詳細を伝送するステップであって、前記データ照合システムは、前記ユーザデータが前記プライベート暗号化キーで解読され得るように、プライベート暗号化キーが暗号化されたユーザデータにマッチングするかどうかを決定するように構成される、ステップと、
前記データ照合システムから、前記第１のプライベート暗号化キーおよび前記第１のユーザデータがマッチングすることのインジケーションを受信するステップと、
前記第１のプライベート暗号化キーおよび前記第１のユーザデータがマッチングすることの前記受信されたインジケーションに基づいて、前記データ仮想化プラットフォームに、前記データ仮想化プラットフォームが前記データプラットフォームから受信された前記暗号化された第１のユーザデータを解読し得るように、前記第１のプライベート暗号化キーを伝送するステップと
を含む、方法。
（項目３７）
前記第１のプライベート暗号化キーを含む前記プライベート暗号化キーは、分散型台帳内に記憶される、項目３６に記載の方法。
（項目３８）
前記第１のソフトウエアコントラクトを含む前記ソフトウエアコントラクトは、スマートコントラクトである、項目３６－３７のいずれか１項に記載の方法。
（項目３９）
前記第１のソフトウエアコントラクトを含む前記ソフトウエアコントラクトは、分散型台帳内に記憶される、項目３６－３８のいずれか１項に記載の方法。
（項目４０）
第２のプライベート暗号化キーを生成するステップと、
前記第２のプライベート暗号化キーを含む第２のソフトウエアコントラクトを生成および記憶するステップと、
前記データプラットフォームに、前記データプラットフォームが、前記第１のユーザデータを前記第１のプライベート暗号化キーで解読し、前記第１のユーザデータを前記第２のプライベート暗号化キーで再暗号化し得るように、前記第１のプライベート暗号化キーおよび前記第２のプライベート暗号化キーを伝送するステップと
をさらに含む、項目３６－３９のいずれか１項に記載の方法。
（項目４１）
前記第２のソフトウエアコントラクトはまた、前記データ仮想化プラットフォームに伝送された前記第１のユーザデータの説明を記憶する、項目４０に記載の方法。
（項目４２）
少なくとも部分的に、前記第１のソフトウエアコントラクトに基づいて、共有されることが許可されることが決定される前記第１のユーザデータはまた、少なくとも部分的に、前記データ仮想化プラットフォームにアクセスする購入者デバイスと関連付けられるアカウントに基づき、前記購入者デバイスは、第１のユーザデータへのアクセスのための要求と関連付けられる、項目３６－４１のいずれか１項に記載の方法。
（項目４３）
システムであって、
１つまたはそれを上回るコンピュータ可読記憶デバイスであって、前記１つまたはそれを上回るコンピュータ可読記憶デバイスは、

コンピュータ実行可能命令と、
ユーザと関連付けられるプライバシ設定と、
ソフトウエアコントラクトであって、前記ソフトウエアコントラクトは、少なくとも部分的に、前記プライバシ設定に基づく、ソフトウエアコントラクトと、
前記ユーザと関連付けられるパブリック暗号化キーであって、各ユーザは、１つのパブリック暗号化キーを割り当てられる、パブリック暗号化キーと
を記憶するように構成される、１つまたはそれを上回るコンピュータ可読記憶デバイスと、
ユーザデータを表示するように構成されるユーザインターフェースを備えるデータ仮想化プラットフォームと、
前記ユーザと関連付けられるユーザデータを記憶するように構成されるデータプラットフォームと、
ネットワークインターフェースと、
１つまたはそれを上回るハードウェアコンピュータプロセッサであって、前記１つまたはそれを上回るハードウェアコンピュータプロセッサは、前記１つまたはそれを上回るコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記システムに、
前記データ仮想化プラットフォームから、前記ネットワークインターフェースを介して、第１のユーザデータへのアクセスのための要求を受信することであって、前記第１のユーザデータは、第１のユーザと関連付けられる、ことと、
前記ソフトウエアコントラクトを検索し、前記第１のユーザと関連付けられる前記ソフトウエアコントラクトの第１のソフトウエアコントラクトを特定することであって、前記第１のソフトウエアコントラクトは、最新のバージョンである、ことと、
前記検索に基づいて、少なくとも部分的に、前記第１のソフトウエアコントラクトに基づいて、前記第１のユーザデータが共有されることが許可されることを決定することであって、前記第１のユーザデータは、１つまたはそれを上回るサードパーティサービスからの第１のサードパーティデータを含む、ことと、
前記第１のサードパーティデータを前記１つまたはそれを上回るサードパーティサービスから抽出するための命令を準備し、前記データ仮想化プラットフォームに、前記ネットワークインターフェースを介して、伝送することと、
前記データ仮想化プラットフォームから、前記ネットワークインターフェースを介して、前記第１のサードパーティデータが前記データ仮想化プラットフォームによって正常に読み出されたことの通知を受信することと、
前記通知の受信に応じて、第１のパブリック暗号化キーを前記第１のソフトウエアコントラクトから読み出すことと、
前記データ仮想化プラットフォームに、前記ネットワークインターフェースを介して、前記データ仮想化プラットフォームが、前記サードパーティデータを暗号化し、記憶のために、前記データプラットフォームに伝送し得るように、前記第１のパブリック暗号化キーを伝送することと
を行わせる、１つまたはそれを上回るハードウェアコンピュータプロセッサと
を備える、システム。
（項目４４）
前記第１のパブリック暗号化キーを含む前記パブリック暗号化キーは、分散型台帳内に記憶される、項目４３に記載のシステム。
（項目４５）
前記第１のソフトウエアコントラクトを含む前記ソフトウエアコントラクトは、スマートコントラクトである、項目４３－４４のいずれか１項に記載のシステム。
（項目４６）
前記第１のソフトウエアコントラクトを含む前記ソフトウエアコントラクトは、分散型台帳内に記憶される、項目４３－４５のいずれか１項に記載のシステム。

（項目４７）
前記サードパーティデータは、ソーシャルメディアデータを含む、項目４３－４６のいずれか１項に記載のシステム。
（項目４８）
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、前記システムに、
前記通知の受信に応じて、前記サードパーティデータの読出と関連付けられる詳細を説明するデータを記憶させるように構成される、項目４３－４７のいずれか１項に記載のシステム。
（項目４９）
前記サードパーティデータの読出と関連付けられる詳細を説明するデータは、前記サードパーティデータの抽出、処理、プロファイリングまたはタグ付け、および暗号化に関連する情報を含む、項目４８に記載のシステム。
（項目５０）
少なくとも部分的に、前記第１のソフトウエアコントラクトに基づいて、共有されることが許可されることが決定される前記第１のユーザデータはまた、少なくとも部分的に、前記データ仮想化プラットフォームにアクセスする購入者デバイスと関連付けられるアカウントに基づき、前記購入者デバイスは、第１のユーザデータへのアクセスのための要求と関連付けられる、項目４３－４９のいずれか１項に記載のシステム。
（項目５１）
方法であって、
データ仮想化プラットフォームから、第１のユーザデータへのアクセスのための要求を受信するステップであって、前記第１のユーザデータは、第１のユーザと関連付けられ、前記データ仮想化プラットフォームは、ユーザデータを表示するように構成されるユーザインターフェースを備える、ステップと、
ソフトウエアコントラクトを検索し、前記第１のユーザと関連付けられる前記ソフトウエアコントラクトの第１のソフトウエアコントラクトを特定するステップであって、前記第１のソフトウエアコントラクトは、最新のバージョンである、ステップと、
前記検索に基づいて、少なくとも部分的に、前記第１のソフトウエアコントラクトに基づいて、前記第１のユーザデータが共有されることが許可されることを決定するステップであって、前記第１のユーザデータは、１つまたはそれを上回るサードパーティサービスからの第１のサードパーティデータを含む、ステップと、
前記第１のサードパーティデータを前記１つまたはそれを上回るサードパーティサービスから抽出するための命令を準備し、前記データ仮想化プラットフォームに伝送するステップと、
前記データ仮想化プラットフォームから、前記第１のサードパーティデータが前記データ仮想化プラットフォームによって正常に読み出されたことの通知を受信するステップと、
前記通知の受信に応じて、第１のパブリック暗号化キーを前記第１のソフトウエアコントラクトから読み出すステップと、
前記データ仮想化プラットフォームに、前記データ仮想化プラットフォームが、前記サードパーティデータを暗号化し、記憶のために、データプラットフォームに伝送し得るように、前記第１のパブリック暗号化キーを伝送するステップと
を含む、方法。
（項目５２）
前記第１のパブリック暗号化キーを含む前記パブリック暗号化キーは、分散型台帳内に記憶される、項目５１に記載の方法。
（項目５３）
前記第１のソフトウエアコントラクトを含む前記ソフトウエアコントラクトは、スマートコントラクトである、項目５１－５２のいずれか１項に記載の方法。
（項目５４）

前記第１のソフトウエアコントラクトを含む前記ソフトウエアコントラクトは、分散型台帳内に記憶される、項目５１－５３のいずれか１項に記載の方法。
（項目５５）
前記サードパーティデータは、ソーシャルメディアデータを含む、項目５１－５４のいずれか１項に記載の方法。
（項目５６）
前記通知の受信に応じて、前記サードパーティデータの読出と関連付けられる詳細を説明するデータを記憶するステップをさらに含む、項目５１－５５のいずれか１項に記載の方法。
（項目５７）
前記サードパーティデータの読出と関連付けられる詳細を説明するデータは、前記サードパーティデータの抽出、処理、プロファイリングまたはタグ付け、および暗号化に関連する情報を含む、項目５６に記載の方法。
（項目５８）
少なくとも部分的に、前記第１のソフトウエアコントラクトに基づいて、共有されることが許可されることが決定される前記第１のユーザデータはまた、少なくとも部分的に、前記データ仮想化プラットフォームにアクセスする購入者デバイスと関連付けられるアカウントに基づき、前記購入者デバイスは、第１のユーザデータへのアクセスのための要求と関連付けられる、項目５１－５７のいずれか１項に記載の方法。
（項目５９）
データプラットフォームであって、
１つまたはそれを上回るコンピュータ可読記憶デバイスであって、前記１つまたはそれを上回るコンピュータ可読記憶デバイスは、
コンピュータ実行可能命令と、
ユーザと関連付けられるパブリック暗号化キーであって、各ユーザは、１つのパブリック暗号化キーを割り当てられる、パブリック暗号化キーと、
前記ユーザと関連付けられるユーザデータと、
前記ユーザデータと関連付けられる識別値と
を記憶するように構成される、１つまたはそれを上回るコンピュータ可読記憶デバイスと、
分散型台帳マネージャであって、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える、分散型台帳マネージャと、
ネットワークインターフェースと、
１つまたはそれを上回るハードウェアコンピュータプロセッサであって、前記１つまたはそれを上回るハードウェアコンピュータプロセッサは、前記１つまたはそれを上回るコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記データプラットフォームに、
第１のデバイスから、前記ネットワークインターフェースを介して、前記ユーザデータのうちの第１のユーザデータを受信することであって、前記第１のユーザデータは、暗号化され、第１のメタデータで意味論的にタグ付けされるデータを含む、ことと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内に、前記第１のユーザデータを記憶することと、
前記第１のユーザデータに関する識別値を計算することであって、前記識別値は、ハッシュアルゴリズムに基づく、ことと、
前記識別値を前記第１のユーザデータに割り当てることと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内に、前記計算された識別値を記憶することと、
前記分散型台帳マネージャに、前記ネットワークインターフェースを介して、トランザクションデータを伝送することであって、前記トランザクションデータは、前記計算され

た識別値、前記第１のメタデータ、および前記第１のユーザデバイスから前記データプラットフォームへの第１のユーザデータの転送に関連する情報を含む、ことと
を行わせる、１つまたはそれを上回るハードウェアコンピュータプロセッサと
を備える、データプラットフォーム。
（項目６０）
前記第１のメタデータは、前記第１のユーザデータが収集された日付および時間を示すデータと、前記第１のユーザデータを収集したデバイスと、前記データが第１のユーザデータであることのインジケーションとを含む、項目５９に記載のデータプラットフォーム。
（項目６１）
前記第１のユーザデータは、前記第１のユーザと関連付けられる第１のパブリック暗号化キーに基づいて暗号化される、項目５９－６のいずれか１項に記載のデータプラットフォーム。
（項目６２）
前記分散型台帳マネージャは、前記トランザクションデータを分散型台帳の中にエンコーディングするように構成される、項目５９－６１のいずれか１項に記載のデータプラットフォーム。
（項目６３）
前記第１のユーザデータは、少なくとも部分的に、前記第１のデバイスによって収集された環境データに基づく、項目５９－６２のいずれか１項に記載のデータプラットフォーム。
（項目６４）
方法であって、
第１のデバイスから、第１のユーザデータを受信するステップであって、前記第１のユーザデータは、暗号化され、第１のメタデータで意味論的にタグ付けされるデータを含む、ステップと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内に、前記第１のユーザデータを記憶するステップと、
前記第１のユーザデータに関する識別値を計算するステップであって、前記識別値は、ハッシュアルゴリズムに基づく、ステップと、
前記識別値を前記第１のユーザデータに割り当てるステップと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内に、前記計算された識別値を記憶するステップと、
分散型台帳マネージャに、前記ネットワークインターフェースを介して、トランザクションデータを伝送するステップであって、前記トランザクションデータは、前記計算された識別値、前記第１のメタデータ、および前記第１のユーザデバイスから前記データプラットフォームへの第１のユーザデータの転送に関連する情報を含み、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える、ステップと
を含む、方法。
（項目６５）
前記第１のメタデータは、前記第１のユーザデータが収集された日付および時間を示すデータと、前記第１のユーザデータを収集したデバイスと、前記データが第１のユーザデータであることのインジケーションとを含む、項目６４に記載の方法。
（項目６６）
前記第１のユーザデータは、前記第１のユーザと関連付けられる第１のパブリック暗号化キーに基づいて暗号化される、項目６４－６５のいずれか１項に記載の方法。
（項目６７）
前記分散型台帳マネージャは、前記トランザクションデータを分散型台帳の中にエンコーディングするように構成される、項目６４－６６のいずれか１項に記載の方法。
（項目６８）

前記第１のユーザデータは、少なくとも部分的に、前記第１のデバイスによって収集された環境データに基づく、項目６４－６７のいずれか１項に記載の方法。
（項目６９）
データプラットフォームであって、
１つまたはそれを上回るコンピュータ可読記憶デバイスであって、前記１つまたはそれを上回るコンピュータ可読記憶デバイスは、
実行可能命令と、
ユーザと関連付けられるユーザデータと、
を記憶するように構成される、１つまたはそれを上回るコンピュータ可読記憶デバイスと、
ユーザデータを表示するように構成されるユーザインターフェースを備えるデータ仮想化プラットフォームと、
データ照合システムであって、前記データ照合システムは、前記ユーザデータが前記プライベート暗号化キーで解読され得るように、プライベート暗号化キーが暗号化されたユーザデータにマッチングするかどうかを決定するように構成される、データ照合システムと、
ネットワークインターフェースと、
１つまたはそれを上回るハードウェアコンピュータプロセッサであって、前記１つまたはそれを上回るハードウェアコンピュータプロセッサは、前記１つまたはそれを上回るコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記データプラットフォームに、
前記データ仮想化プラットフォームから、前記ネットワークインターフェースを介して、第１のユーザデータの少なくとも一部へのアクセスのための第１の要求を受信することであって、前記第１のユーザデータは、第１のユーザと関連付けられる、ことと、
前記第１の要求の受信に応じて、前記１つまたはそれを上回るコンピュータ可読記憶デバイス内において、少なくとも部分的に、前記第１の要求に基づいて、前記第１のユーザデータを特定することであって、前記第１のユーザデータは、以前に、第１のデバイスから受信されており、受信に応じて、記憶されている、ことと、
前記データ仮想化プラットフォームに、前記ネットワークインターフェースを介して、前記第１のユーザデータの少なくとも一部を伝送することであって、前記第１のユーザデータは、暗号化され、第１のメタデータで意味論的にタグ付けされる、ことと、
データ照合システムに、前記ネットワークインターフェースを介して、前記データ仮想化プラットフォームへの前記第１のユーザデータの少なくとも一部の伝送の成功の確認と、伝送された前記第１のユーザデータの部分を説明する情報とを伝送することであって、前記データ照合システムは、前記第１のユーザと関連付けられる前記第１のユーザデータの少なくとも一部および第１のプライベート暗号化キーがマッチングすることを照合するように構成される、ことと
を行わせる、１つまたはそれを上回るハードウェアコンピュータプロセッサと
を備える、データプラットフォーム。
（項目７０）
前記第１のメタデータは、前記第１のユーザデータが収集された日付および時間を示すデータと、前記第１のユーザデータを収集したデバイスと、前記データが第１のユーザデータであることのインジケーションとを含む、項目６９に記載のデータプラットフォーム。
（項目７１）
前記第１のユーザデータは、前記第１のユーザと関連付けられる第１のパブリック暗号化キーに基づいて暗号化される、項目６９－７０のいずれか１項に記載のデータプラットフォーム。
（項目７２）
前記データ照合システムによって実施される照合されたマッチングは、前記第１のプライベート暗号化キーが前記第１のユーザデータの少なくとも一部を解読し得ることの決定

を含む、項目６９－７１のいずれか１項に記載のデータプラットフォーム。
（項目７３）
分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える分散型台帳マネージャをさらに備え、
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、前記データプラットフォームに、
前記分散型台帳マネージャから、前記ネットワークインターフェースを介して、前記第１のプライベート暗号化キーおよび第２のプライベート暗号化キーを受信することであって、前記第１および第２のプライベート暗号化キーは、前記第１のユーザと関連付けられる、ことと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内において、前記第１のユーザデータを特定することであって、前記第１のユーザデータは、以前に、第１のデバイスから受信されており、受信に応じて、記憶されている、ことと、
前記第１のユーザデータを前記第１のプライベート暗号化キーで解読することと、
前記解読された第１のユーザデータを前記第２のプライベート暗号化キーで暗号化することと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内に、前記第２のプライベート暗号化キーで暗号化された前記第１のユーザデータを記憶することと
を行わせるように構成される、項目６９－７２のいずれか１項に記載のデータプラットフォーム。
（項目７４）
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、前記データプラットフォームに、
前記データ仮想化プラットフォームから、前記ネットワークインターフェースを介して、一般的ユーザデータへのアクセスのための第２の要求を受信することであって、前記一般的ユーザデータは、前記ユーザデータと関連付けられる匿名化および仮名化されたデータを含み、前記ユーザのうちの任意のユーザを識別するために使用されることができない、ことと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内において、少なくとも部分的に、前記要求に基づいて、前記一般的ユーザデータを特定することと、
前記データ仮想化プラットフォームに、前記ネットワークインターフェースを介して、前記一般的ユーザデータの少なくとも一部を伝送することと
を行わせるように構成される、項目６９－７３のいずれか１項に記載のデータプラットフォーム。
（項目７５）
前記データプラットフォームはさらに、前記データ照合システムを備える、項目６９－７４のいずれか１項に記載のデータプラットフォーム。
（項目７６）
前記第１の要求は、少なくとも部分的に、前記第１のユーザと関連付けられる第１のソフトウエアコントラクトに基づく、項目６９－７５のいずれか１項に記載のデータプラットフォーム。
（項目７７）
伝送される前記第１のユーザデータの少なくとも一部は、少なくとも部分的に、前記第１のユーザと関連付けられる第１のソフトウエアコントラクトに基づく、項目６９－７６のいずれか１項に記載のデータプラットフォーム。
（項目７８）
伝送される前記第１のユーザデータの少なくとも一部は、少なくとも部分的に、前記データ仮想化プラットフォームにアクセスする購入者デバイスと関連付けられるアカウントに基づき、前記購入者デバイスは、第１のユーザデータへのアクセスのための要求と関連付けられる、項目６９－７７のいずれか１項に記載のデータプラットフォーム。

（項目７９）
方法であって、
データ仮想化プラットフォームから、第１のユーザデータの少なくとも一部へのアクセスのための第１の要求を受信するステップであって、前記第１のユーザデータは、第１のユーザと関連付けられ、前記データ仮想化プラットフォームは、ユーザデータを表示するように構成されるユーザインターフェースを備える、ステップと、
前記第１の要求の受信に応じて、１つまたはそれを上回るコンピュータ可読記憶デバイス内において、少なくとも部分的に、前記第１の要求に基づいて、前記第１のユーザデータを特定するステップであって、前記第１のユーザデータは、以前に、第１のデバイスから受信されており、受信に応じて、記憶されている、ステップと、
前記データ仮想化プラットフォームに、前記第１のユーザデータの少なくとも一部を伝送するステップであって、前記第１のユーザデータは、暗号化され、第１のメタデータで意味論的にタグ付けされる、ステップと、
データ照合システムに、前記データ仮想化プラットフォームへの前記第１のユーザデータの少なくとも一部の伝送の成功の確認と、伝送された前記第１のユーザデータの部分を説明する情報とを伝送するステップであって、前記データ照合システムは、前記第１のユーザと関連付けられる前記第１のユーザデータの少なくとも一部および第１のプライベート暗号化キーがマッチングすることを照合するように構成され、前記データ照合システムはさらに、前記ユーザデータが前記プライベート暗号化キーで解読され得るように、プライベート暗号化キーが暗号化されたユーザデータにマッチングするかどうかを決定するように構成される、ステップと
を含む、方法。
（項目８０）
前記第１のメタデータは、前記第１のユーザデータが収集された日付および時間を示すデータと、前記第１のユーザデータを収集したデバイスと、前記データが第１のユーザデータであることのインジケーションとを含む、項目７９に記載の方法。
（項目８１）
前記第１のユーザデータは、前記第１のユーザと関連付けられる第１のパブリック暗号化キーに基づいて暗号化される、項目７９－８０のいずれか１項に記載の方法。
（項目８２）
前記データ照合システムによって実施される照合されたマッチングは、前記第１のプライベート暗号化キーが前記第１のユーザデータの少なくとも一部を解読し得ることの決定を含む、項目７９－８１のいずれか１項に記載の方法。
（項目８３）
分散型台帳マネージャから、前記第１のプライベート暗号化キーおよび第２のプライベート暗号化キーを受信するステップであって、前記第１および第２のプライベート暗号化キーは、前記第１のユーザと関連付けられ、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える、ステップと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内において、前記第１のユーザデータを特定するステップであって、前記第１のユーザデータは、以前に、第１のデバイスから受信されており、受信に応じて、記憶されている、ステップと、
前記第１のユーザデータを前記第１のプライベート暗号化キーで解読するステップと、
前記解読された第１のユーザデータを前記第２のプライベート暗号化キーで暗号化するステップと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内に、前記第２のプライベート暗号化キーで暗号化された前記第１のユーザデータを記憶するステップと
をさらに含む、項目７９－８２のいずれか１項に記載の方法。
（項目８４）
前記データ仮想化プラットフォームから、一般的ユーザデータへのアクセスのための第

２の要求を受信するステップであって、前記一般的ユーザデータは、前記ユーザデータと関連付けられる匿名化および仮名化されたデータを含み、前記ユーザのうちの任意のユーザを識別するために使用されることができない、ステップと、
前記１つまたはそれを上回るコンピュータ可読記憶デバイス内において、少なくとも部分的に、前記要求に基づいて、前記一般的ユーザデータを特定するステップと、
前記データ仮想化プラットフォームに、前記一般的ユーザデータの少なくとも一部を伝送するステップと
をさらに含む、項目７９－８３のいずれか１項に記載の方法。
（項目８５）
前記データプラットフォームはさらに、前記データ照合システムを備える、項目７９－８４のいずれか１項に記載の方法。
（項目８６）
前記第１の要求は、少なくとも部分的に、前記第１のユーザと関連付けられる第１のソフトウエアコントラクトに基づく、項目７９－８５のいずれか１項に記載の方法。
（項目８７）
伝送される前記第１のユーザデータの少なくとも一部は、少なくとも部分的に、前記第１のユーザと関連付けられる第１のソフトウエアコントラクトに基づく、項目７９－８６のいずれか１項に記載の方法。
（項目８８）
伝送される前記第１のユーザデータの少なくとも一部は、少なくとも部分的に、前記データ仮想化プラットフォームにアクセスする購入者デバイスと関連付けられるアカウントに基づき、前記購入者デバイスは、第１のユーザデータへのアクセスのための要求と関連付けられる、項目７９－８７のいずれか１項に記載の方法。
（項目８９）
データ仮想化プラットフォームであって、
１つまたはそれを上回るコンピュータ可読記憶デバイスであって、前記１つまたはそれを上回るコンピュータ可読記憶デバイスは、
コンピュータ実行可能命令と、
ユーザと関連付けられるプライベート暗号化キーであって、各ユーザは、１つのプライベート暗号化キーを割り当てられる、プライベート暗号化キーと、
前記ユーザと関連付けられるユーザデータと
を記憶するように構成される、１つまたはそれを上回るコンピュータ可読記憶デバイスと、
分散型台帳マネージャであって、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える、分散型台帳マネージャと、
１つまたはそれを上回るデータベースを備えるデータプラットフォームと、
ネットワークインターフェースと、
１つまたはそれを上回るハードウェアコンピュータプロセッサであって、前記１つまたはそれを上回るハードウェアコンピュータプロセッサは、前記１つまたはそれを上回るコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記データ仮想化プラットフォームに、
前記分散型台帳マネージャから、前記ネットワークインターフェースを介して、前記プライベート暗号化キーのうちの第１のプライベート暗号化キーを受信することであって、前記第１のプライベート暗号化キーは、第１のユーザと関連付けられる、ことと、
前記分散型台帳マネージャから、前記ネットワークインターフェースを介して、前記ユーザデータのうちの第１のユーザデータを前記データプラットフォームから読み出すための命令を受信することであって、前記第１のユーザデータは、第１のユーザと関連付けられる、ことと、
前記受信された命令に基づいて、前記第１のユーザデータのための第１の要求を準備し

、前記データプラットフォームに、前記ネットワークインターフェースを介して、伝送することと、
　前記データプラットフォームから、前記ネットワークインターフェースを介して、前記第１の要求に基づいて、前記第１のユーザデータを受信することであって、前記第１のユーザデータは、暗号化される、ことと、
　前記第１のユーザデータを前記第１のプライベート暗号化キーで解読することであって、前記第１のユーザデータは、前記データプラットフォームから受信される、ことと、
　前記解読された第１のユーザデータを処理し、前記第１のユーザデータを匿名化および仮名化することと、
　前記匿名化および仮名化された第１のユーザデータに基づいて、前記第１のユーザを識別することが不可能であることを検証することによって、処理された第１のユーザデータを決定することと
　を行わせる、１つまたはそれを上回るハードウェアコンピュータプロセッサと
　を備える、データ仮想化プラットフォーム。
（項目９０）
　前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
　前記分散型台帳マネージャから、前記ネットワークインターフェースを介して、前記プライベート暗号化キーのうちの第２のプライベート暗号化キーを受信することであって、前記第２のプライベート暗号化キーは、第２のユーザと関連付けられる、ことと、
　前記分散型台帳マネージャから、前記ネットワークインターフェースを介して、前記ユーザデータのうちの第２のユーザデータを前記データプラットフォームから読み出すための第１の命令を受信することであって、前記第２のユーザデータは、第２のユーザと関連付けられる、ことと、
　前記第１の受信された命令に基づいて、前記第２のユーザデータのための第２の要求を準備し、前記データプラットフォームに、前記ネットワークインターフェースを介して、伝送することと、
　前記データプラットフォームから、前記ネットワークインターフェースを介して、前記第２の要求に基づいて、前記第２のユーザデータを受信することであって、前記第２のユーザデータは、暗号化される、ことと、
　前記第２のユーザデータを前記データプラットフォームから受信された前記第２のプライベート暗号化キーおよび前記第２のユーザデータで解読することと、
　前記解読された第２のユーザデータを処理し、前記第２のユーザデータを匿名化および仮名化することと、
　前記匿名化および仮名化された第２のユーザデータに基づいて、前記第２のユーザを識別することが不可能であることを検証することによって、処理された第２のユーザデータを決定することと
　を行うように構成される、項目８９に記載のデータ仮想化プラットフォーム。
（項目９１）
　前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
　前記匿名化および仮名化された第１のユーザデータに基づいて、前記第１のユーザを識別することが不可能であることを検証するように構成される、項目９０に記載のデータ仮想化プラットフォーム。
（項目９２）
　前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
　処理された第１のユーザデータを電子ユーザインターフェース上に表示するように構成される、項目８９－９１のいずれか１項に記載のデータ仮想化プラットフォーム。
（項目９３）
　前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
　前記電子ユーザインターフェースを介して、前記処理された第１のユーザデータの使用を終了するための第２の命令を受信することと、

前記受信された第２の命令に基づいて、前記処理された第１のユーザデータおよび第１のプライベート暗号化キーを含む前記第１のユーザと関連付けられる任意のデータを削除することと
を行うように構成される、項目８９－９２のいずれか１項に記載のデータ仮想化プラットフォーム。
（項目９４）
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
前記処理された第１のユーザデータをさらに処理し、分析された第１のユーザデータを作成することであって、前記分析された第１のユーザデータは、１つまたはそれを上回る分析ツールが前記データに適用された処理された第１のユーザデータを含み、前記１つまたはそれを上回る分析ツールは、集約、事前分析、およびコンテキスト化のうちの１つまたはそれを上回るものを含む、ことと、
前記分析された第１のユーザデータをメタデータでエンコーディングすることであって、前記メタデータは、少なくとも、前記分析された第１のユーザデータが第１のユーザと関連付けられることを示す、ことと、
前記分析された第１のユーザデータを監視し、前記データ仮想化プラットフォームからの前記分析された第１のユーザデータの一部または全ての非認可エクスポートを防止することと
を行うように構成される、項目８９－９３のいずれか１項に記載のデータ仮想化プラットフォーム。
（項目９５）
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
前記データ仮想化プラットフォームからの分析データを伝送するための第３の要求を受信することであって、前記分析データは、前記データ仮想化プラットフォームによって起動された分析と関連付けられる結果と、前記第１のユーザと関連付けられるデータとを含む、ことと、
前記第３の要求に基づいて、前記データ仮想化プラットフォームによって起動される分析と関連付けられるデータを伝送し、前記第１のユーザと関連付けられるデータは伝送しないことと
を行うように構成される、項目９４に記載のデータ仮想化プラットフォーム。
（項目９６）
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
前記電子ユーザインターフェースを介して、前記処理された第１のユーザデータの使用を終了するための第３の命令を受信することと、
前記受信された第３の命令に基づいて、前記処理された第１のユーザデータおよび第１のプライベート暗号化キーを含む前記第１のユーザと関連付けられる任意のデータを削除することと
を行うように構成される、項目９５に記載のデータ仮想化プラットフォーム。
（項目９７）
第１のユーザデータを読み出すための命令は、少なくとも部分的に、前記第１のユーザと関連付けられる第１のソフトウエアコントラクトに基づく、項目８９－９６のいずれか１項に記載のデータ仮想化プラットフォーム。
（項目９８）
第１のユーザデータを読み出すための命令は、少なくとも部分的に、前記データ仮想化プラットフォームにアクセスする購入者デバイスと関連付けられるアカウントに基づき、前記購入者デバイスは、第１のユーザデータへのアクセスのための要求と関連付けられる、項目８９－９７のいずれか１項に記載のデータ仮想化プラットフォーム。
（項目９９）
方法であって、
分散型台帳マネージャから、前記プライベート暗号化キーのうちの第１のプライベート

暗号化キーを受信するステップであって、前記第１のプライベート暗号化キーは、第１のユーザと関連付けられ、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える、ステップと、
前記分散型台帳マネージャから、前記ユーザデータのうちの第１のユーザデータをデータプラットフォームから読み出すための命令を受信するステップであって、前記第１のユーザデータは、第１のユーザと関連付けられ、前記データプラットフォームは、１つまたはそれを上回るデータベースを備える、ステップと、
前記受信された命令に基づいて、前記第１のユーザデータのための第１の要求を準備し、前記データプラットフォームに伝送するステップと、
前記データプラットフォームから、前記第１の要求に基づいて、前記第１のユーザデータを受信するステップであって、前記第１のユーザデータは、暗号化される、ステップと、
前記第１のユーザデータを前記第１のプライベート暗号化キーおよび前記データプラットフォームから受信された第１のユーザデータで解読するステップと、
前記解読された第１のユーザデータを処理し、前記第１のユーザデータを匿名化および仮名化するステップと、
前記匿名化および仮名化された第１のユーザデータに基づいて、前記第１のユーザを識別することが不可能であることを検証することによって、処理された第１のユーザデータを決定するステップと
を含む、方法。
（項目１００）
前記分散型台帳マネージャから、前記プライベート暗号化キーのうちの第２のプライベート暗号化キーを受信するステップであって、前記第２のプライベート暗号化キーは、第２のユーザと関連付けられる、ステップと、
前記分散型台帳マネージャから、前記ユーザデータのうちの第２のユーザデータを前記データプラットフォームから読み出すための第１の命令を受信するステップであって、前記第２のユーザデータは、第２のユーザと関連付けられる、ステップと、
前記第１の受信された命令に基づいて、前記第２のユーザデータのための第２の要求を準備し、前記データプラットフォームに伝送するステップと、
前記データプラットフォームから、前記第２の要求に基づいて、前記第２のユーザデータを受信するステップであって、前記第２のユーザデータは、暗号化される、ステップと、
前記第２のユーザデータを前記データプラットフォームから受信された前記第２のプライベート暗号化キーおよび前記第２のユーザデータで解読するステップと、
前記解読された第２のユーザデータを処理し、前記第２のユーザデータを匿名化および仮名化するステップと、
前記匿名化および仮名化された第２のユーザデータに基づいて、前記第２のユーザを識別することが不可能であることを検証することによって、処理された第２のユーザデータを決定するステップと
をさらに含む、項目９９に記載の方法。
（項目１０１）
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
前記匿名化および仮名化された第１のユーザデータに基づいて、前記第１のユーザを識別することが不可能であることを検証するように構成される、項目１００に記載の方法。
（項目１０２）
処理された第１のユーザデータを電子ユーザインターフェース上に表示するステップをさらに含む、項目９９－１０１のいずれか１項に記載の方法。
（項目１０３）
前記電子ユーザインターフェースを介して、前記処理された第１のユーザデータの使用を終了するための第２の命令を受信するステップと、
前記受信された第２の命令に基づいて、前記処理された第１のユーザデータおよび第１のプライベート暗号化キーを含む前記第１のユーザと関連付けられる任意のデータを削除

するステップと
をさらに含む、項目９９－１０２のいずれか１項に記載の方法。
（項目１０４）
前記処理された第１のユーザデータをさらに処理し、分析された第１のユーザデータを作成するステップであって、前記分析された第１のユーザデータは、１つまたはそれを上回る分析ツールが前記データに適用された処理された第１のユーザデータを含み、前記１つまたはそれを上回る分析ツールは、集約、事前分析、およびコンテキスト化のうちの１つまたはそれを上回るものを含む、ステップと、
前記分析された第１のユーザデータをメタデータでエンコーディングするステップであって、前記メタデータは、少なくとも、前記分析された第１のユーザデータが第１のユーザと関連付けられることを示す、ステップと、
前記分析された第１のユーザデータを監視し、前記データ仮想化プラットフォームからの前記分析された第１のユーザデータの一部または全ての非認可エクスポートを防止するステップと
をさらに含む、項目９９－１０３のいずれか１項に記載の方法。
（項目１０５）
前記データ仮想化プラットフォームからの分析データを伝送するための第３の要求を受信するステップであって、前記分析データは、前記データ仮想化プラットフォームによって起動された分析と関連付けられる結果と、前記第１のユーザと関連付けられるデータとを含む、ステップと、
前記第３の要求に基づいて、前記データ仮想化プラットフォームによって起動される分析と関連付けられるデータを伝送し、前記第１のユーザと関連付けられるデータは伝送しないステップと
をさらに含む、項目１０４に記載の方法。
（項目１０６）
前記電子ユーザインターフェースを介して、前記処理された第１のユーザデータの使用を終了するための第３の命令を受信するステップと、
前記受信された第３の命令に基づいて、前記処理された第１のユーザデータおよび第１のプライベート暗号化キーを含む前記第１のユーザと関連付けられる任意のデータを削除するステップと
をさらに含む、項目１０５に記載の方法。
（項目１０７）
第１のユーザデータを読み出すための命令は、少なくとも部分的に、前記第１のユーザと関連付けられる第１のソフトウエアコントラクトに基づく、項目９９－１０６のいずれか１項に記載の方法。
（項目１０８）
第１のユーザデータを読み出すための命令は、少なくとも部分的に、前記データ仮想化プラットフォームにアクセスする購入者デバイスと関連付けられるアカウントに基づき、前記購入者デバイスは、第１のユーザデータへのアクセスのための要求と関連付けられる、項目９９－１０７のいずれか１項に記載の方法。
（項目１０９）
データ仮想化プラットフォームであって、
１つまたはそれを上回るコンピュータ可読記憶デバイスであって、前記１つまたはそれを上回るコンピュータ可読記憶デバイスは、
コンピュータ実行可能命令と、
ユーザと関連付けられるユーザデータと
を記憶するように構成される、１つまたはそれを上回るコンピュータ可読記憶デバイスと、
分散型台帳マネージャであって、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える、分散型

台帳マネージャと、
ネットワークインターフェースと、
１つまたはそれを上回るハードウェアコンピュータプロセッサであって、前記１つまたはそれを上回るハードウェアコンピュータプロセッサは、前記１つまたはそれを上回るコンピュータ可読記憶デバイスと通信し、前記コンピュータ実行可能命令を実行し、前記データ仮想化プラットフォームに、
前記分散型台帳マネージャから、前記ネットワークインターフェースを介して、サードパーティデータを１つまたはそれを上回るサードパーティサービスのうちの第１のサードパーティサービスから読み出すための第１の命令を受信することであって、前記サードパーティデータは、第１のユーザと関連付けられる、ことと、
前記命令に基づいて、前記第１のユーザと関連付けられる前記第１のサードパーティサービスからサードパーティデータを読み出すことと、
前記サードパーティデータを処理し、前記サードパーティデータをメタデータでエンコーディングすることであって、前記メタデータは、前記サードパーティデータが読み出されたサードパーティサービスと、前記サードパーティデータが前記第１のユーザと関連付けられることとを示す、ことと、
サードパーティデータと、前記第１のユーザと関連付けられる以前に読み出されたデータを組み合わせることと、
前記分散型台帳マネージャに、前記ネットワークインターフェースを介して、読み出されたサードパーティデータの通知を伝送することであって、前記通知は、前記サードパーティデータが読み出された時間と、前記サードパーティデータが読み出されたサービスとを含む、ことと
を行わせる、１つまたはそれを上回るハードウェアコンピュータプロセッサと
を備える、データ仮想化プラットフォーム。
（項目１１０）
前記１つまたはそれを上回るサードパーティサービスは、ソーシャルメディアサービスを含む、項目１０９に記載のデータ仮想化プラットフォーム。
（項目１１１）
前記サードパーティデータを読み出すための命令は、前記第１のサードパーティサービスと関連付けられる第１のユーザアカウント情報を含む、項目１０９－１１０のいずれか１項に記載のデータ仮想化プラットフォーム。
（項目１１２）
前記サードパーティデータを読み出すための命令は、少なくとも１つのＡＰＩコールを前記第１のサードパーティサービスに実施する方法に関する命令を含む、項目１０９－１１１のいずれか１項に記載のデータ仮想化プラットフォーム。
（項目１１３）
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
前記サードパーティデータを処理し、前記データ仮想化プラットフォームによって必要とされない任意の余剰情報を除去するように構成される、項目１０９－１１２のいずれか１項に記載のデータ仮想化プラットフォーム。
（項目１１４）
前記１つまたはそれを上回るハードウェアコンピュータプロセッサはさらに、
前記サードパーティデータを処理し、前記データを前記データ仮想化プラットフォームによって好まれる構成にフォーマット化するように構成される、項目１０９－１１３のいずれか１項に記載のデータ仮想化プラットフォーム。
（項目１１５）
データ仮想化プラットフォームであって、
分散型台帳マネージャから、サードパーティデータを１つまたはそれを上回るサードパーティサービスのうちの第１のサードパーティサービスから読み出すための第１の命令を受信するステップであって、前記サードパーティデータは、第１のユーザと関連付けられ

、前記分散型台帳マネージャは、分散型台帳と、前記分散型台帳を読み取り、そこに書き込むように構成されるソフトウェアとを備える、ステップと、
前記命令に基づいて、前記第１のユーザと関連付けられる前記第１のサードパーティサービスからサードパーティデータを読み出すステップと、
前記サードパーティデータを処理し、前記サードパーティデータをメタデータでエンコーディングするステップであって、前記メタデータは、前記サードパーティデータが読み出されたサードパーティサービスと、前記サードパーティデータが前記第１のユーザと関連付けられることとを示す、ステップと、
サードパーティデータと、前記第１のユーザと関連付けられる以前に読み出されたデータを組み合わせるステップと、
前記分散型台帳マネージャに、読み出されたサードパーティデータの通知を伝送するステップであって、前記通知は、前記サードパーティデータが読み出された時間と、前記サードパーティデータが読み出されたサービスとを含む、ステップと
を含む、データ仮想化プラットフォーム。
（項目１１６）
前記１つまたはそれを上回るサードパーティサービスは、ソーシャルメディアサービスを含む、項目１１５に記載の方法。
（項目１１７）
前記サードパーティデータを読み出すための命令は、前記第１のサードパーティサービスと関連付けられる第１のユーザアカウント情報を含む、項目１１５－１１６のいずれか１項に記載の方法。
（項目１１８）
前記サードパーティデータを読み出すための命令は、少なくとも１つのＡＰＩコールを前記第１のサードパーティサービスに実施する方法に関する命令を含む、項目１１５－１１７のいずれか１項に記載の方法。
（項目１１９）
前記サードパーティデータを処理し、前記データ仮想化プラットフォームによって必要とされない任意の余剰情報を除去するステップをさらに含む、項目１１５－１１８のいずれか１項に記載の方法。
（項目１２０）
前記サードパーティデータを処理し、前記データを前記データ仮想化プラットフォームによって好まれる構成にフォーマット化するステップをさらに含む、項目１１５－１１９のいずれか１項に記載の方法。
【図面の簡単な説明】
【００１０】
【図１】図１は、ユーザデータトランザクションシステムの実施例を図示し、本システムのコンポーネント間の相互作用およびデータ転送の実施例を含む。
【００１１】
【図２Ａ】図２Ａは、ユーザのためのプライバシ設定を作成または更新するための例示的方法のフロー図を示す。
【００１２】
【図２Ｂ】図２Ｂ－２Ｃは、ユーザのためのプライバシ設定を作成または更新するための例示的方法のスイムレーンフロー図を示す。
【図２Ｃ】図２Ｂ－２Ｃは、ユーザのためのプライバシ設定を作成または更新するための例示的方法のスイムレーンフロー図を示す。
【００１３】
【図３】図３は、ユーザデータを特定、伝送、および解読するための例示的方法のフロー図を示す。ある付加的または代替ブロックが、図４、６Ａ、および６Ｂに描写される。
【００１４】
【図４】図４は、新しいプライベート暗号化キーを生成し、ユーザデータを新しいプライ

ベート暗号化キーで再暗号化するための方法のフロー図を示す。ある付加的または代替ステップが、図３に描写される。

【００１５】

【図５】図５は、ユーザデータに１つまたはそれを上回るサードパーティサービスから読み出されたソーシャルメディアデータを付加するための方法のフロー図を示す。ある付加的または代替ステップが、図６Ｂに描写される。

【００１６】

【図６Ａ】図６Ａは、ユーザデータを検証、処理、および監視するための方法のフロー図を示す。ある付加的または代替ステップが、図３に描写される。

【００１７】

【図６Ｂ】図６Ｂは、匿名化および仮名化されたユーザデータのための要求を処理するための方法の実施例のフロー図を示す。ある付加的または代替ステップが、図３および５に描写される。

【００１８】

【図７Ａ】図７Ａは、空間コンピューティングデバイスまたはウェアラブルディスプレイシステムの実施例を図示する。

【００１９】

【図７Ｂ】図７Ｂは、ユーザデータトランザクションシステムの一実施形態を図式的に図示する。

【００２０】

【図８】図８は、それを用いて本明細書で議論されるある方法が実装され得る、コンピュータシステムを図示する。

【００２１】

図面全体を通して、参照番号は、参照される要素間の対応を示すために再使用され得る。図面は、本明細書に説明される例示的実施形態を図示するために提供され、本開示の範囲を限定することを意図するものではない。

【発明を実施するための形態】

【００２２】

詳細な説明

概要

空間コンピューティングデバイス、およびそのようなデバイスを企業のユーザまたは顧客に提供する、企業は、そのようなユーザに関連するユーザデータを収集することができ、これは、環境データ、すなわち、空間コンピューティングデバイスの周囲に基づくデータを含むことができる。ユーザが、空間コンピューティングデバイス上で生成し、それと相互作用するであろう、ユーザデータのタイプは、今日多くの他のプラットフォームまたはサービス上で利用可能なものよりはるかに取扱に注意を要し、かつ貴重であり得る。例えば、ユーザデータは、ユーザの環境（例えば、ユーザの自宅、寝室、オフィス、近隣の人々の顔および身体、または同等物）およびユーザの個人的識別（例えば、製品、人々、場所についてのユーザの個人的選好、ユーザの個人的識別データ、または同等物）についての情報を提供し得るため、より取扱に注意を要する。ユーザデータはまた、ユーザの物理的能力（例えば、ユーザが眼鏡を要求するかどうか、またはユーザが要求し得る処方箋、ユーザの身長、ユーザの体重、ユーザの歩幅、ユーザの身体の外観、または同等物）についての情報を提供し得る。いくつかの実施例では、ユーザデータは、ユーザの健康（例えば、心拍数、ユーザの皮膚を通したユーザの血液の分析、または同等物）についての情報を提供し得る。ユーザデータが使用される方法の制御を提供するように、本情報を保護することが望ましくあり得る。空間コンピューティングデバイスまたは関連付けられるシステムが、ユーザが、ユーザの個人的プライバシ選好に基づいて、ユーザのデータのデータ収集および／または共有を制御するように、ユーザが本情報に関する保護レベルを制御することを許可することが有利であり得る。例えば、いくつかの実施形態では、ユーザは、プライバシ設定の付加的変化が、新しい記憶場所に追加され得、以前のプライバシ設定

もまた、精査され得る、不変の分散型台帳上に記憶され得る、更新可能プライバシ設定を提供することができる。

【００２３】

パブリック－キー暗号法およびパブリック分散型台帳技術（例えば、ブロックチェーン、ビットコイン、イーサリアム、タングル、または同等物）とソフトウエアコントラクト（例えば、スマートコントラクトまたは同等物）のためのサポートの併用を通して、ユーザは、その独自のデータの制御およびプライバシを維持することができる。例えば、ユーザは、そのデータ（例えば、彼らから収集されたユーザデータ）が、少しでも利用可能である、または共有されるかどうかを制御し、それへのアクセスを有する人物を管理し、アクセス可能または共有されるデータの部分を管理し、データのどの部分が誰にアクセス可能であるかを管理することができ、ユーザは、データの一部または全てへのアクセスを提供することから利点を享受することができる。加えて、本明細書に説明されるシステムおよび方法はまた、そのようなサービスのプロバイダ（例えば、ユーザデータを収集する、または収集した企業、ユーザデータを管理するために雇用されたサードパーティ企業、または同等物）と、ユーザデータを収集するデバイスを使用することを選定する人物との間の信頼を促すことができる。

【００２４】

ソフトウエアコントラクト（例えば、スマートコントラクト、イーサリアムスマートコントラクト、チューリング完全スマートコントラクト、または同等物）とキー暗号法の組み合わせは、最も豊富なデータセットを含むように調整され得る、ソリューションを提供することができる。本明細書に説明されるシステムおよび方法は、ユーザのユーザデータへのアクセス、すなわち、その制御を維持するためのユーザフレンドリーな方法を提供することができる。

【００２５】

いくつかの実施形態では、キー暗号法（例えば、パブリックキー暗号法または同等物）は、プラットフォームのユーザ毎に、一対の暗号化キー、すなわち、パブリックキーおよびプライベートキーを生成するように構成されることができる。パブリックキーは、公的に共有されることができるが、プライベートキーは、ユーザの制御下にのみ留まるように意図される。キー暗号法の１つの利点は、ユーザデータがプライベートに保たれるように、データ機密性を含むことができる。例えば、ユーザは、その以前に生成されたパブリックキーを使用して、そのユーザデータを暗号化することができ、ユーザのみが、後の時点において、そのプライベートキーを使用して、ユーザデータを解読することが可能であろう。キー暗号法の別の利点は、データ真正性を含むことができ、ユーザは、彼らがそれを生み出したことを証明するために、そのプライベートキーを使用して、データのいくつかの断片にデジタル的に署名することができる。

【００２６】

分散型台帳は、ソフトウエアコントラクトサポートと併せて、口座残高の状態を追跡し、１つの有効状態から別の状態へのスマートコントラクトの遷移を促進するように構成され得る、パーミッションレス、トラストレス、検閲耐性、かつ不変の台帳を提供することができる。時として、共有台帳または分散型台帳技術もしくはＤＬＴとも称され、また、タングルおよび他の形態の分散型記憶装置も含み得る、分散型台帳は、複数の施設、国、または機関を横断して地理的に拡散される、複製、共有、および同期されたデジタルデータのコンセンサスであり得る。１つの形態の分散型台帳設計は、ブロックチェーンシステムであって、これは、パブリックまたはプライベートのいずれかであることができる。台帳は、ピアツーピアネットワーク内に分散されてもよく、いくつかのノード（デバイス）、有向非巡回グラフ（ＤＡＧ）、または他のデータ構造を横断して拡散される、分散型データベースを備えてもよい。説明されるようなデータ機密性および真正性は、分散型台帳によって提供されることができ、また、キー暗号法を介して、分散型台帳のコンテキスト外でも使用されることができる。情報セキュリティのコンテキストにおいて、分散型台帳はまた、改良されたデータ完全性および否認防止を提供することができる。パブリック分

散型台帳技術の１つの利点は、例えば、データが許可を伴わずに操作されないことを確実にすることによって、データ完全性を含むことができる。パブリック分散型台帳技術の別の利点は、例えば、ユーザが、インターネットの使用を通して、分散型台帳に関するデータに接続およびアクセスし得る、データ可用性およびアクセス性を含むことができる。例えば、中央組織は、分散型台帳に関する任意の当事者への特殊権限をブロックまたは付与することができない。パブリック分散型台帳技術の別の利点は、例えば、検閲耐性を含むことができる。例えば、中央組織は、誰がブロックチェーンに関するデータを記憶することができ、誰が記憶することができないかを制御することができない。

【００２７】

現在、分散型台帳技術は、その限界を有する。例えば、本技術は、高価であって（例えば、トランザクション手数料が高くあり得る）、全体的にセキュアではなく（例えば、５１％攻撃、チェーン分岐の可能性、または同等物）、全体的にスケーラブルではなく、およびデータベースを伴う従来的一元型サービスより低速であり得る。分散型台帳技術の改良が、進められており、本明細書に説明されるシステムおよび方法に影響を及ぼし得る。分散型台帳技術に関する現在の限界は、本明細書に説明されるシステムおよび方法に関する限界として解釈されるべきではない。

【００２８】

分散型台帳技術の改良は、本明細書に説明されるシステムおよび方法の改良に変換されるであろう。例えば、いくつかの改良は、より低いトランザクション手数料、増加されたセキュリティ（例えば、ブロックチェーンの最終的状態を達成する、５１％攻撃に対する耐性、分岐の可能性を限定する、または同等物）、増加されたスケーラビリティ（例えば、シャーディング、異なるコンセンサス機構、または同等物の使用および実装を通して）、または本明細書に説明されるシステムおよび方法を直接または間接的に改良し得る、他の新しい特徴もしくは利点を含み得る。

【００２９】

現在、分散型台帳に関する大量のデータを記憶することは、高価または煩雑であり得るため、データベースを用いて、セキュアサーバに関するデータを記憶するが、ユーザのプライバシ設定を分散型台帳上に記憶し得る、ソリューションを実装することが所望される。しかしながら、分散型台帳技術が改良されるにつれて、ユーザのプライバシ設定およびユーザデータの両方が、分散型台帳を介して記憶およびアクセスされ得ることを理解されたい。

【００３０】

加えて、ヒトによって使用可能かつ容易に学習される、コンピュータユーザインターフェースの設計は、困難であり得る。本開示の双方向かつ動的ユーザインターフェースの種々の実施形態は、有意な研究、開発、改良、反復、および試験の結果である。本簡単でない開発は、以前のシステムに優る有意な認知および人間工学的効率ならびに利点を提供し得る、本明細書に説明されるユーザインターフェースをもたらした。双方向かつ動的ユーザインターフェースは、ユーザのために、低減された頭脳的作業量、改良された意思決定、低減された作業ストレス、または同等物を提供し得る、改良されたヒトとコンピュータの相互作用を含む。例えば、本明細書に説明される双方向ユーザインターフェースとのユーザ相互作用は、リソース依存性、または、データ変換、関係の最適化された表示を提供し得、ユーザが、前のシステムより迅速に、そのような情報にアクセスし、それをナビゲートし、それを査定し、それを会得することを可能にし得る。

【００３１】

本明細書に説明されるシステムおよび方法の１つの利点は、データプラットフォームのオペレータ、空間コンピューティングデバイスと関連付けられるサービス、およびユーザデータを収集する任意の関連サービスが、データが、暗号化され、オペレータが、ユーザデータを解読するための適切なキーを有しないであろうため、ユーザデータへの直接アクセスを有しないであろうことである。例えば、そのような実装の利点は、セキュリティ侵害の際、ユーザデータが、盗難される場合、暗号化に基づいて、ユーザデータが適切なキ

ーを伴わずに解読されることが困難乃至ほぼ不可能であろうことである。加えて、政府機関が、オペレータからのユーザデータの提出を命じる場合、オペレータは、ユーザデータを解読し、そのような提出命令に準拠することが不可能であろう。これは、オペレータが、そのような取扱に注意を要するユーザデータを漏洩する公的な関係を回避することを可能にするであろう。

【００３２】

いくつかの状況では、ユーザは、そのユーザデータをホストするどのような人物であっても、いかようにも、ユーザデータを修正または悪用することはないと信頼しなければならない。ユーザは、そのユーザデータをアップロードする前に、そのユーザデータのハッシュをブロックチェーンに記憶することができるため、そのユーザデータが不正開封されたかどうかを照合することが容易である。例えば、アップロードされたユーザデータの新しいハッシュが、決定され、記憶されたハッシュと比較されることができる。したがって、本明細書に説明されるシステムおよび方法の別の利点は、ユーザデータが修正されたかどうかを照合するための照合プロシージャが存在し得ることである。

【００３３】

いくつかの実施形態では、万が一ユーザが、そのプライベートキーを紛失した、または忘れた場合、プライベートキー復元オプションが、利用可能であり得る。例えば、一連の２要素認証機構（例えば、電子メール、Ｆａｃｅｂｏｏｋ、ＳＭＳ、電話、Ｐｈｏｎｅ－ａ－Ｆｒｉｅｎｄ、または同等物）を使用して、ユーザは、異なるデバイスを横断して、そのアカウントと関連付けられるそのプライベートキーへのアクセスを読み出すことが可能である。これは、同一ユーザが、異なるデバイスおよび異なるプラットフォーム上にログインされることを許可するであろう。

【００３４】

いくつかの実施形態では、ユーザデータを支援またはホストするエンティティが、ユーザデータへのアクセスを一方的に破壊またはブロックするという問題点が存在し得る。しかしながら、いくつかの実施形態では、非一元型クラウド記憶ソリューションが、実装されることができる（例えば、Ｓｉａ、Ｓｔｏｒｊ、Ｆｉｌｅｃｏｉｎ、および／またはＩＰＦＳ）。暗号化されたユーザデータは、非一元型クラウド上に記憶され得、支援またはホストエンティティは、記憶されたユーザデータの制御を殆どまたは全く有しないであろう。

【００３５】

加えて、いくつかの実施形態では、ユーザは、サードパーティによるユーザデータへのアクセスを許可し得、そのようなユーザデータは、一時的にのみアクセス可能であり得るが、サードパーティは、依然として、ユーザデータを不正使用し得る。いくつかの実施形態では、非一元型エスクロー状機構が、実装され、悪用されたユーザデータの紛争を解決することができる。ユーザが、サードパーティに、ユーザのユーザデータにアクセスするための許可を付与後、ユーザデータを受信する、またはそれにアクセスする、サードパーティは、ユーザデータを乱用（例えば、ユーザデータを他の非認可サードパーティと共有する、またはそれに販売する、ユーザデータのセキュリティ侵害または非認可アクセスからの不十分な保護または保護の怠慢、もしくは同等物）しないことの約束として、ある量のコイン、トークン、または資金を託すことを要求されるであろう。ユーザが、ユーザがアクセスを与えたサードパーティが、事前に構成されたプライバシ同意に違反したと訴える場合、例えば、自律分散型組織（ＤＡＯ）が、誰に責任があるかを決定することができる（例えば、ＯｐｅｎＺｅｐｐｅｌｉｎおよびＡｒａｇｏｎは、ＤＡＯがそのような決定を行うことを許可するためのプラットフォームを提供する）。プライバシのセキュリティ侵害があったことが決定される場合、例えば、サードパーティによって託されたトークンは、消滅または削除されるか、もしくはユーザに送信されるかのいずれかとなり得る。これは、サードパーティが、ユーザデータを悪用しないように動機付ける。代替として、任意のサードパーティは、彼らが所有する資金の非常に大きな割合を託すように義務付けられ得る。サードパーティが、サードパーティがトランザクションしているユーザのいずれ

かのプライバシを侵害する場合、ＤＡＯは、サードパーティに責任があるかどうかの決定を行うことができる。サードパーティに責任がある場合、全ての託された資金は、消滅または削除されるか、もしくは影響を受けたユーザ間で共有されるかのいずれかとなるであろう。これは、託された総額が、十分に高額である場合、サードパーティに害を及ぼし得るため、サードパーティが、ユーザのいずれかの信頼を侵害しないように動機付けるであろう。

【００３６】

いくつかの実施形態では、分散されるシステムは、多くの場合、フォールトトレランスであるように設計される。したがって、クラスタ内のノードのうちの１つが、ダウンする場合でも、本システムは、エンドユーザの視点から、完全に機能したままである。しかしながら、ノードが、適切に機能し続け、正しく機能しているかのように作用するが、注意深く異なる機能を実施する場合、データの完全性に害を及ぼし、および／またはユーザの体験に影響を及ぼし得る。そのような不正挙動を考慮して、ノードは、例えば、ビザンチンフォールトトレランスと呼ばれる。多くの異なる形態のコンセンサスプロトコルが存在するが、プルーフ・オブ・ステーク（ＰｏＳ）およびルーフ・オブ・ワーク（ＰｏＷ）は、それらがビザンチンフォールトトレランスを考慮するため、最も一般的なもののうちの２つである。例えば、ＰｏＷは、不正挙動マイナが、それらがネットワークの残りより高速でブロックを算出することを所望する場合、非常に大量の算出リソースを費やすように強制することによって、ビザンチンフォールトトレランスを考慮する。ネットワークを攻撃しようとするのではなく、攻撃者（例えば、不正挙動マイナまたは同等物）は、正当なマイナとしてネットワークをサポートすることによって、より多くの金銭を儲け得る。別の実施例では、ＰｏＳは、マイナがブロックを生成することを所望する場合、マイナに多額の資金を託すように強制することによって、ビザンチンフォールトトレランスを考慮する。別のマイナまたは異なる完全ノードが、対応するブロックチェーンを照合しようとし、マイナのうちの１つが、不正挙動し、正しくないブロックを算出したことを確認する場合、それらは、ネットワークの残りに信号伝達するであろう。ネットワークを攻撃しようとするのではなく、攻撃者（例えば、不正挙動マイナまたは同等物）は、正当なマイナとしてネットワークをサポートすることによって、より多くの金銭を儲け得る。

【００３７】

いくつかの実施形態では、本明細書に説明されるアーキテクチャは、ユーザのセンサデータに依存する、オブジェクト認識装置（ＯＲ）をサポートすることができる。いくつかの実施例では、空間コンピューティングデバイスプロバイダが、サードパーティＯＲをプロバイダのサーバ上にホストする場合、プロバイダは、ユーザのデータをいくつかの時点で解読することが可能である必要がある。これは、プロバイダがユーザのデータへの直接アクセスを有することなく、外部ＯＲが起動し得ないことを意味する。別の実施例では、プロバイダが、サードパーティにＯＲをその独自のサーバ上で起動させ、ユーザのユーザデータへのアクセスを有するサードパーティに関するユーザ制御を与えるように選定する場合、ユーザは、プロバイダがそもそもユーザデータを解読することが可能ではなくても、ユーザのユーザデータへのサードパーティアクセスを許可するオプションを有する。

例示的ユーザデータトランザクションシステム

【００３８】

図１は、ユーザデータトランザクションシステム１００の実施例を図示し、本システムのコンポーネント間の相互作用およびデータ転送の実施例を含む。例えば、どのようにユーザデータトランザクションシステム１００の内部コンポーネントまたはシステムが、相互作用するかと、どのデータが、コンポーネントまたはシステム間で転送されるかとである。エージェント１０６、分散型台帳１０８、およびソフトウエアコントラクト１１０は、ユーザデータトランザクションシステム１００のコンポーネントまたはシステムである、（例えば、他の実施形態および実施例に関して）本明細書に説明されるエージェント、分散型台帳、およびソフトウエアコントラクトと同一であってもよい。また、説明されるシステムおよびコンポーネントは、１つのコンポーネントまたは多くのコンポーネントを

含むことができる。本明細書に説明されるコンポーネントは、包括的であることを意味するものではなく、どのコンポーネントが実装され得るかのサンプルにすぎない。いくつかのコンポーネントは、組み合わせられてもよく、その他は、除去される、または類似コンポーネントで代用されてもよい。また、いくつかのコンポーネントは、１つのシステムの一部、または同一もしくは類似機能を達成するためにともに接続され、稼動する、複数のシステムの一部であることができる。

例示的エージェント

【００３９】

いくつかの実施形態では、エージェント１０６は、分散型台帳１０８、データプラットフォーム１１２、データ仮想化システム１１１、およびユーザデバイス１０２（例えば、セルラー電話、タブレットコンピュータ、電子リーダ、スマートウォッチ、頭部搭載型拡張、仮想、または複合現実ディスプレイシステム、ウェアラブルディスプレイシステム、図７Ａのウェアラブルディスプレイシステム１０００、もしくは同等物）を含み得る、種々のシステムと電子通信することができる。いくつかの実施形態では、エージェント１０６は、ローカルエリアネットワークを介して、またはインターネットを介して接続される、複数のシステムを備えることができる。また、いくつかの実施形態では、例えば、エージェント１０６、またはその一部は、ユーザデバイス１０２、データプラットフォーム１１２、データ仮想化システム１１１、もしくは購入者デバイス１０４上に位置することができる。例えば、エージェント１０６と、データプラットフォーム１１２とを含む、ユーザデータプライバシシステム１０３は、プライバシ中央データ記憶ソリューションを備えることができる。プライバシ中央データ記憶ソリューションは、プライベート、パブリック、またはプライベートコンポーネントとパブリックコンポーネントの組み合わせであることができる。いくつかの実施形態では、データまたは情報（例えば、ユーザデータまたは同等物）は、プライバシ中央データ記憶ソリューション（またはそのコンポーネント）から、アプリケーションプログラミングインターフェース（ＡＰＩ）コールの使用を通して、アクセスされることができる。エージェント１０６は、種々のシステムから受信し、処理し、分散型台帳（例えば、ブロックチェーン、タングル、または同等物）内に記憶する、情報を決定することができる。

【００４０】

いくつかの実施形態では、エージェント１０６は、ソフトウエアコントラクト１１０（例えば、スマートコントラクトまたは同等物）を生成し、ソフトウエアコントラクト１１０を分散型台帳１０８内に記憶するために使用し得る、データまたは命令を種々のシステムから受信することができる。例えば、エージェント１０６は、プライバシ設定命令をユーザデバイス１０２から受信することができ、エージェント１０６は、次いで、命令を処理し、プライバシ設定命令を捕捉する、スマートコントラクトを生成することができ、次いで、エージェント１０６は、スマートコントラクトをブロックチェーンに書き込むことができる。エージェント１０６を含む、種々のシステムによって伝送および受信される、データのタイプは、図２－６におけるフローチャートに関してさらに詳細に説明される。

【００４１】

ソフトウエアコントラクト１１０を生成し、分散型台帳１０８上に記憶することに加え、エージェント１０６はまた、プライベートキーおよびパブリックキーを生成することができる。本明細書に議論されるように、キー暗号法（例えば、パブリックキー暗号法または同等物）は、プラットフォームのユーザ毎に、対の暗号化キー、すなわち、パブリックキーおよびプライベートキーを生成するように構成されることができる。パブリックキーは、公的に共有されることができるが、プライベートキーは、ユーザの制御下にのみ留まるように意図される。キー暗号法の１つの利点は、ユーザデータがプライベートに保たれるように、データ機密性を含むことができる。例えば、ユーザは、その以前に生成されたパブリックキーを使用して、そのユーザデータを暗号化することができ、ユーザのみが、後の時点に、そのプライベートキーを使用して、ユーザデータを解読することが可能であろう。キー暗号法の別の利点は、データ真正性を含むことができ、ユーザは、彼らがそれ

を生み出したことを証明するために、そのプライベートキーを使用して、データのいくつかの断片にデジタル的に署名することができる。プライベートおよびパブリックキーは、分散型台帳１０８またはソフトウエアコントラクト１１０内に記憶され、キーが生成されたユーザと関連付けられることができる。プライベートおよびパブリックキーは、本明細書にさらに詳細に説明されるように、分散型台帳１０８またはソフトウエアコントラクト１１０から読み出され、種々のシステムに伝送されることができる。プライベートキーは、例えば、データ仮想化システム１１１、データプラットフォーム１１２、および／またはユーザデバイス１０２に伝送される、もしくはそこから受信されることができる。

【００４２】

エージェント１０６は、分散型台帳１０８内に記憶されるソフトウエアコントラクト１１０を読み取り、そのユーザの関連付けられるソフトウエアコントラクト１１０内に反映された特定のユーザの共有設定に基づいて、データを抽出するための命令を生成することができる。そのような命令は、例えば、データ仮想化システム１１１が、関連データをデータプラットフォーム１１２から、または関連データが記憶される、１つまたはそれを上回るサードパーティサービスを介して読み出し得るように、データ仮想化システム１１１に伝送されることができる。

【００４３】

いくつかの実施形態では、種々のシステムによってアクセスまたは転送されるデータに関するデータ転送もしくはトランザクション情報は、データ仮想化システム１１１またはデータプラットフォーム１１２によって、エージェント１０６に伝送されることができる。例えば、データ仮想化システム１１１またはデータプラットフォーム１１２は、それが１つまたはそれを上回るサードパーティサービス（例えば、ソーシャルネットワーク、ファイル記憶サービス、または同等物）もしくはデータプラットフォームから受信する、ユーザデータを読み出し／アクセスし、または修正し、そのような情報の読出／アクセスおよび修正は、追跡ならびに監視されることができる。読出／アクセスおよび修正情報もまた、要約ならびに説明され、次いで、任意のさらなる処理および分散型台帳１０８上への記憶のために、エージェント１０６に送信されることができる。本情報は、例えば、誰が、どのタイプのデータに、いつアクセスしたかを追跡または監視するために使用されることができる。

【００４４】

ある実装では、エージェント１０６（またはエージェント１０６の１つまたはそれを上回る側面）は、「仮想コンピューティング環境」を含む、またはその中に実装されることができる。本明細書で使用されるように、用語「仮想コンピューティング環境」は、広義には、例えば、本明細書に説明されるモジュールまたは機能性の１つまたはそれを上回る側面を実装するために１つまたはそれを上回るプロセッサ（例えば、図８の実施例において下記に説明されるように）によって実行される、コンピュータ可読プログラム命令を含むものと解釈されるべきである。さらに、本実装では、エージェント１０６の１つまたはそれを上回るモジュールもしくはエンジンは、仮想コンピューティング環境によって受信された入力に応答して、ルールまたは他のプログラム命令を実行し、仮想コンピューティング環境の動作を修正する、仮想コンピューティング環境の１つまたはそれを上回るルールエンジンを備えるものと理解され得る。例えば、ユーザデバイス１０２から受信された要求は、仮想コンピューティング環境の動作を修正し、エージェント１０６に、ソフトウエアコントラクト１１０、パブリックまたはプライベートキーを生成させる、もしくは他の動作を実施させるものと理解され得る。そのような機能性は、入力に応答して、かつ種々のルールに従って、仮想コンピューティング環境の動作の修正を備えてもよい。（本開示全体を通して説明されるような）仮想コンピューティング環境によって実装される他の機能性はさらに、仮想コンピューティング環境の動作の修正を備えてもよく、例えば、仮想コンピューティング環境の動作は、例えば、エージェント１０６によってデータプラットフォーム１１２から集められた情報に応じて、変化してもよい。仮想コンピューティング環境の初期動作は、仮想コンピューティング環境の確立として理解され得る。いくつか

の実装では、仮想コンピューティング環境は、コンピューティングシステムの１つまたはそれを上回る仮想機械もしくは他のエミュレーションを備えてもよい。いくつかの実装では、仮想コンピューティング環境は、遠隔でアクセス可能であり得、必要に応じて、急速にプロビジョニングされ得る、物理的コンピューティングリソースの集合（一般に、「クラウド」コンピューティング環境と称される）を含む、ホストされたコンピューティング環境を備えてもよい。

分散型台帳

【００４５】

分散型台帳１０８は、エージェント１０６または別個のシステムの一部であることができる。分散型台帳１０８は、１つまたはそれを上回るソフトウエアコントラクト１１０、複数のプライベートおよびパブリックキー、種々のシステムによってアクセスまたは転送されるデータに関するデータ転送またはトランザクション情報、および／または任意の他の関連情報（例えば、データがアクセスされた時間、アクセスと関連付けられるアカウント、アクセスされたデータが属する人物、データにアクセスするための適切な許可が適切であったかどうか、データにアクセスするために使用されたパブリックまたはプライベートキー、もしくは同等物）を記憶するように構成されることができる。

【００４６】

分散型台帳は、ソフトウエアコントラクトサポートと併せて、口座残高の状態を追跡し、ソフトウエアコントラクト１１０の１つの有効状態から別の状態への遷移を促進するように構成され得る、パーミッションレス、トラストレス、検閲耐性、かつ不変の台帳を提供することができる。ソフトウエアコントラクト１１０（例えば、スマートコントラクト、イーサリアムスマートコントラクト、チューリング完全スマートコントラクト、または同等物）とキー暗号法の組み合わせは、最も豊富なデータセットを含むように調整され得る、ソリューションを提供することができる。本明細書に説明されるシステムおよび方法は、ユーザのユーザデータへのアクセスおよび／またはその制御を維持するためのユーザフレンドリーな方法を提供することができる。

【００４７】

いくつかの実施形態では、種々のシステムによってアクセスまたは転送されるデータに関するデータ転送またはトランザクション情報は、分散型台帳１０８内に記憶されることができる。例えば、データ仮想化システム１１１は、それが１つまたはそれを上回るサードパーティサービス（例えば、ソーシャルネットワーク、ファイル記憶サービス、または同等物）もしくはデータプラットフォーム１１２から受信する、ユーザデータを読み出し／アクセスし、または修正してもよく、そのような読出／アクセスおよび修正情報は、追跡および監視されることができる。読出／アクセスおよび修正情報はまた、要約および説明され、次いで、任意のさらなる処理および分散型台帳１０８上への記憶のために、エージェント１０６に送信されることができる。本データ転送またはトランザクション情報は、例えば、誰が、どのタイプのユーザデータに、いつアクセスしたかを追跡または監視するために使用されることができる。

【００４８】

最新技術における分散型台帳のある実装に関して、非効率性（例えば、ブロックチェーンの種々のブロックへのより低速の書込）が存在し得るが、本技術は、迅速に改良され、まもなく、非効率性は、従来的データベースまたは分散型データベースと比較して、最小限となる、または存在しなくなるであろう。したがって、本明細書における実施形態および実施例は、ユーザデータを処理および記憶するために使用される、データプラットフォーム１１２を開示するが、分散型台帳１０８は、データプラットフォーム１１２と併せて、またはデータプラットフォーム１１２の代わりに、そのようなユーザデータを記憶するために使用されることができることを理解されたい。

【００４９】

いくつかの実施形態では、プライベートブロックチェーンまたは分散型台帳が、実装されることができる。プライベート分散型台帳は、完全性を保証する、企業間のセキュアサ

ービスを構築するときに有用であり得る。例えば、３つの企業間の株式決済サービスが、プライベート分散型台帳を使用し、したがって、３つの企業は、同一情報へのアクセスを有し、相互に信頼する必要はない。代替として、銀行が、支払のよりセキュアかつより高速の転送のためにプライベート分散型台帳を有し得る。非一元型消費者対応製品を構築するとき、１つの目標は、ユーザがサービスプロバイダを信頼する必要がない、システムを構築することであり得る。エンドユーザは、そのデータにアクセスした人物および頻度を確認することが可能であるべきである。ユーザは、ライトまたはフルノードを同期させ、自らのトランザクションを照合する能力を有するべきである。別のアドレスとトランザクションを行うとき、ユーザは、そのトランザクション履歴を確認し、あるアドレスを信頼すべきかどうかに関して自ら決定を行うことが可能であるべきである。

ソフトウエアコントラクト

【００５０】

いくつかの実施形態では、ソフトウエアコントラクト１１０は、コードのラインの中に直接書き込まれている２人の当事者間の同意の条件を用いた自己実行コントラクトである。コードおよびその中に含有される同意は、分散され、非一元化された、分散型台帳ネットワークを横断して存在する。例えば、ソフトウエアコントラクト１１０は、信頼されたトランザクションおよび同意が、中央当局、法的システム、または外部施行機構の必要なく、異種の匿名の当事者間で行われることを許可することができる。それらは、トランザクションを追跡可能、トランスペアレント、かつ不可逆的にする。標準的コントラクトは、関係の条件（通常、法律によって施行可能なもの）を概略するが、ソフトウエアコントラクト１１０は、暗号化コードとの関係を施行する。例えば、ソフトウエアコントラクト１１０は、それらがプログラムされる通り正確に実行する、プログラムである。

【００５１】

いくつかの実施形態では、ユーザは、その個別のユーザデバイス１０２を通して、ユーザの個人的プライバシ設定を更新することができる。いったん更新が、受信／アクセスされると、エージェント１０６は、次いで、新しいソフトウエアコントラクト１１０を準備し、それを分散型台帳１０８に保存するであろう。分散型台帳（例えば、ブロックチェーン、または同等物）の技術に基づいて、ユーザのソフトウエアコントラクトの多くの古いバージョンが、存在し、種々の場所（例えば、ブロックチェーンのブロック）において視認可能／アクセス可能となり得ることを理解されたい。したがって、エージェント１０６は、最新バージョンである、ソフトウエアコントラクト１１０を区別することが可能であることが望ましい。例えば、エージェント１０６は、保存されているソフトウエアコントラクト１１０のバージョンを示す、英数字識別子を用いて、ソフトウエアコントラクト１１０を処理することができる。別の実施例では、日付が、各ソフトウエアコントラクト１１０とともに含まれることができる。別の実施例では、各ソフトウエアコントラクト１１０は、全てのソフトウエアコントラクトの精査に応じて、分散型台帳１０８上のある場所が精査または分析されないであろうように、以前のソフトウエアコントラクトへの参照を含むことができる（例えば、より古いブロックは、含まれる参照に基づいてか、またはソフトウエアコントラクトが、より新しいブロック内に見出され、本質的に、より最新であろうためかのいずれかにおいて、検索されることを必要としないであろう）。

【００５２】

いくつかの実施形態では、ソフトウエアコントラクト１１０が、使用されることができ、ソフトウエアコントラクト１１０は、同意のネゴシエーションまたは実施をデジタル的に促進、照合、もしくは施行するように意図される、コンピュータプロトコルを含むことができる。ソフトウエアコントラクト１１０は、サードパーティを伴わずに、追跡可能かつ不可逆的であり得る、信用できるトランザクションの実施を可能にすることができる。多くの種類の契約上の条項が、部分的または完全に、自己実行する、自己施行する、もしくは両方であるようにされ得る。ソフトウエアコントラクト１１０は、従来的コントラクト法より優れ、コントラクトと関連付けられる、他のトランザクションコストを低減させる、セキュリティを提供することができる。ソフトウエアコントラクト１１０の一実施例

は、スマートコントラクトである。スマートコントラクト１１０のためのＳｏｌｉｄｉｔｙプログラミング言語における擬似コードの実施例が、下記に提供される。

【００５３】

【化１－１】

```
pragma solidity ^0.4.18;
contract SmartContract {
 struct UserData {
```

【化１－２】

```
string URI;
string metadata;
string hash;
}
struct AcceptedBuyer {
address acceptedBuyer;
string key;
}
// list of addresses belonging to users who opted in to share their data
address[] userAddresses;
// list of structs containing the entities the user has agreed to share
// their data with, alongside a decryption key that only that entity can access
mapping(address => AcceptedBuyer[]) acceptedBuyers;
// list of entities who want to get access to the user's data but have
// not been granted permission by the user yet
mapping(address => address[]) pendingBuyers;
// list of structs pointing to a URI where the encrypted data is stored
// along with some metadata the user is willing to publicize; the
// metadata can be used by the entities to find out which user's data
// they'd like to access
mapping(address => UserData[]) userData;
}
```

【００５４】

以下の例示的フローは、ユーザによって設定されたプライバシ設定に基づいて、データベースが暗号化されたデータで機能し得る方法を図示する。例示的フローは、それらが使用および動作されるにつれたシステムのいくつかの利点を示すことに役立つ。明示的に述べられない他のフローも、本明細書に記載される開示に基づいて、生成される、または存在し得ることを理解されたい。

【００５５】

暗号化キーに関して、例示的フローは、以下を含むことができる。本実施例では、スマートコントラクトは、ユーザが、ユーザデータへのアクセスを有するであろう、認可された当事者のリストを追加または除去する度に継続的に更新される、スモールデータベースとして作用する。例えば、ユーザのプライベートキーは、認証プロセス後、対応するユーザデバイス（例えば、１０２）にセキュアに転送されることができる。次いで、サードパーティは、分散型台帳トランザクションを介して、ユーザの環境データへのアクセスを要求することができる。ユーザは、その環境データへのアクセスを拒否する、または無料もしくは有料で、アクセスを付与することができる。例えば、ユーザは、定額前払手数料、ユーザの環境データのサブスクリプションを要求し得る、またはユーザの環境データに関する入札プラットフォームが、導入されることができる。ここで、例えば、ユーザが、ユーザの環境データへのアクセスを許可し、サードパーティが、適切な支払または同意を行うと仮定する。ユーザが、空間コンピューティングデバイスの使用を通して、新しい環境

データを生成すると、空間コンピューティングデバイスは、（例えば、暗号化されたデータデータベース１１６内の）暗号化されたデータをデータプラットフォーム（例えば、１１２）に記憶し、ソフトウエアコントラクト１１０の状態を更新し、新しいデータが生成または記憶されたことを示す。次いで、サードパーティが、ソフトウエアコントラクト１１０にクエリすると、解読キーおよびユーザの環境データを読み出すべきファイル場所のリストが読み出される。ユーザは、後に、サードパーティをソフトウエアコントラクトから除去（例えば、新しいソフトウエアコントラクトを作成し、古いソフトウエアコントラクトを置換すること、または同等物によって）し、ユーザの環境データへのアクセスを除去することができる。

【００５６】

加えて、別の例示的フローでは、データプラットフォーム（例えば、１１２）上に記憶されるセンサデータが存在し得る場合でも、データプラットフォームのオペレータは、オペレータが必要なキーへのアクセスを有しないであろうため、データを解読することが可能であろう。例えば、非対称プライベートキーが、ユーザのために生成されることができ、ユーザの空間コンピューティングデバイスにセキュアに転送されることができる。一時的対称ファイル暗号化キーもまた、生成されることができる。空間コンピューティングデバイスによって生成されたユーザのセンサデータ（例えば、環境データまたは他のユーザデータ）は、一時的対称ファイルを使用して暗号化され、ユーザのセンサデータのハッシュも同様に、算出される。暗号化されたセンサデータは、データプラットフォーム（例えば、空間コンピューティングデバイスの販売者によって動作される）上に記憶され、統一資源識別子（ＵＲＩ）が、読み出される。空間コンピューティングデバイスは、分散型台帳上のソフトウエアコントラクトにクエリし、センサデータに関心がある全ての保留中のサードパーティのリストを読み出す。

【００５７】

いくつかの実施形態では、空間コンピューティングデバイスは、周期的に、分散型台帳のライトノードとユーザデバイス１０２を同期させることができる。ライトノード、すなわち、軽量ノードは、完全分散型台帳をダウンロードしなくてもよい。代わりに、ライトノードは、ブロックヘッダのみをダウンロードし、トランザクションの真正性を検証する。ライトノードは、システムを維持し、その上で起動することが容易である。ユーザは、ユーザがそのセンサデータへの許可を付与することを所望する、サードパーティを選択する。許可を付与することと引き換えに、資金、ポイント、クレジット、または同等物の即座転送、もしくはサードパーティとユーザとの間のサブスクリプションモデルが、分散型台帳上で生じ得る。サードパーティに関して、空間コンピューティングデバイスは、提供されるパブリックキーを使用して、対称ファイル暗号化キーを暗号化する。暗号化されたキーは全て、サードパーティアドレスとともに、承認されたサードパーティに関して記憶される。ユーザは、センサデータのＵＲＩ、ハッシュ、およびあるメタデータをソフトウエアコントラクトに追加する。本ステップのセットは、さらなるセンサデータが生成される度に繰り返されることができる。承認されたサードパーティは全て、ソフトウエアコントラクトにクエリし、そのプライベートキーを使用して、一時的対称ファイル暗号化キーを読み出し、次いで、センサデータをダウンロードし、それを解読することができる。随時、ユーザが、そのセンサデータへのアクセスを有する人物を変更することを所望すると、ユーザは、単に、ユーザのプライバシ設定を更新する。ユーザのプライバシ設定の更新は、ユーザデバイスが、ソフトウエアコントラクトを更新するとき、一時的対称ファイル暗号化キーを再算出し、他の当事者のパブリックキーを省略するようにトリガするであろう。選択された当事者は、以前に生成されたデータへのアクセスを有することができるが、任意の新しく生成されたセンサデータへのアクセスを有し得ない。加えて、一時的対称ファイル暗号化キーは、セキュリティ追加のために、周期的に、またはファイル毎ベースで、再算出されることができる。いくつかの実施形態では、ユーザのアドレスに対応する、ソフトウエアコントラクトの任意の修正は、非対称プライベートキーによって署名されなければならない。

【００５８】
いくつかの実施形態では、ブロックチェーンは、分散型台帳として使用される。ブロックチェーントランザクションのコストは、選択されたソフトウエアコントラクトプラットフォームに基づく。例えば、イーサリアムプラットフォームが、選択および実装される場合、トランザクション時間およびコストは、ネットワーク使用量および最終ソフトウェアまたはスマートコントラクトの状態に大きく依存する。コストは、例えば、ソフトウエアコントラクトを公開する、サードパーティがユーザのデータへのアクセスを得るための要求を行う、ユーザが承認されたサードパーティのリストを更新する、およびユーザが新しいユーザデータのためのメタデータを追加することと関連付けられ得る。いくつかの実施形態では、ユーザが承認されたサードパーティのリストを更新することおよびユーザが新しいユーザデータのためのメタデータを追加することは、ソフトウエアコントラクトが、あまり頻繁ではなく、はるかに低いコストでユーザに更新されるように、バッチ化されることができる。加えて、イーサリアムはまた、ユーザの代わりに、トランザクションに対して支払われ得るように、ソフトウエアコントラクトを介した方法を模索しており、これは、説明されるシステムおよび方法を実装するために望ましいであろう。これは、ユーザがそのデータへのアクセスを許可することである程度の金銭またはポイントを稼ぐまで、新しいユーザが参加することに役立つ方法を提供し得、彼らのためのさらなるトランザクションをサポートすることができる。また、ＥＯＳは、委任されたプルーフ・オブ・ステークと呼ばれる、異なるコンセンサス機構を使用する、別のタイプのソフトウエアコントラクトプラットフォームである。より低いセキュリティおよび完全性を犠牲にして、全てのトランザクションは、全ての人に無料であって、コストは、完全に回避されることができ、他のスマートコントラクトプラットフォームの有用な代替であることができる。

例示的データプラットフォーム

【００５９】
データプラットフォーム１１２は、例えば、匿名化および仮名化されたデータデータベース１１４と、暗号化されたデータデータベース１１６と、データ照合システム１１８とを備えることができる。データプラットフォーム１１２はまた、データを処理および記憶するために使用されることができる。例えば、データプラットフォーム１１２は、ユーザデータ、または、ユーザデバイス１０２がユーザデバイス１０２の環境について収集する、データ（例えば、人々の顔、部屋サイズ、芸術作品、またはプライベートもしくはパブリック空間内の人物の周囲にあるであろう任意のものを含む、部屋またはエリアについての周囲情報）を含む、環境データを記憶することができる。いくつかの実施形態では、データプラットフォーム１１２はまた、複数のプライベートおよびパブリックキー、種々のシステムによってアクセスまたは転送されるデータに関するデータ転送またはトランザクション情報、もしくは任意の他の関連情報（例えば、データがアクセスされた時間、アクセスと関連付けられるアカウント、属するデータにアクセスした人物、データにアクセスする適切な許可が適切であったかどうか、データにアクセスするために使用されたパブリックまたはプライベートキー、または同等物）を記憶することができる。いくつかの実施形態では、いくつかのデータは、分散型台帳１０８上への記憶のためにエージェント１０６に伝送されるまで、一時的に記憶される。いくつかの実施形態では、データの一部は、データプラットフォーム１１２内に記憶され、他の部分は、分散型台帳１０８内に記憶される。しかし、いくつかの実施形態では、データは、冗長性または効率性の形態として、両方のシステム内に記憶されることができる。

【００６０】
空間コンピューティングデバイス上に生成されるユーザデータのタイプは、非常に個人的であって、ある場合には、機密である、専有である、または取扱に注意を要し得る。そのようなユーザデータは、ユーザの環境のモデルを構築し、コンテンツ持続性および共有体験を可能にするために使用されることができる。これを行うことは、ユーザの周囲内の実オブジェクトを検出し、意味論的に標識するためのオブジェクト認識装置パイプラインと、オクルージョンおよび衝突検出のための稠密メッシュを構築する、世界再構築パイプ

ラインと、同一空間内のユーザが同一座標フレーム内で動作することを保証するためのマップマージパイプラインと、作成またはユーザと共有された仮想コンテンツをピン留めし、復元する能力とを伴う。例えば、単一ユーザのセッションは、上記の可能性として考えられるものの全てを行うために、数百メガバイトのユーザデータを生成し得る。本ユーザデータは、魅力的かつ没入型の体験を作成するために、セキュア化された様式で保存されるが、また、ユーザ、空間コンピューティングデバイスのプロバイダ、およびあるサードパーティに利用可能であることが所望される。分散型台帳の使用を伴わずに、そのようなデータを収集するための例示的フローは、以下の通りである。

【００６１】

１．ユーザが、空間コンピューティングデバイスを用いて、未加工センサデータを捕捉する。

【００６２】

２．ユーザが、空間コンピューティングデバイスに関するデータを暗号化する。

【００６３】

３．ユーザが、暗号化されたデータを、空間コンピューティングデバイスを提供する、空間コンピューティング企業によって所有される、クラウド記憶装置（例えば、データプラットフォーム）に保存する。

【００６４】

４．空間コンピューティング企業が、製造プロセスの間にデバイス上に記憶されたユーザのキーのコピーを維持する。

【００６５】

５．空間コンピューティング企業が、ユーザのデータを解読し、ユーザの環境のモデルを構築する。

【００６６】

６．空間コンピューティング企業が、ユーザのデータを解読し、サードパーティと共有する。

【００６７】

本明細書に説明されるシステムおよび方法は、ユーザに、ユーザのユーザデータへのアクセスを有する人物、アクセスするために利用可能なユーザのデータの部分、ユーザのデータのどの部分が誰に利用可能であるか、ユーザがそのユーザデータへのアクセスを提供することから利点を享受し得る、プラットフォーム、およびユーザのユーザデータの完全性を保証するための機構の個人化された制御を与えるであろう、ソリューションを提供する。例えば、ユーザは、そもそも空間コンピューティング企業をデータ自体を解読することが可能にさせずに、サードパーティにユーザのユーザデータへのアクセスを付与するためのオプションを有する。グローバル消費者データプライバシ法の絶えず変化する分野では、空間コンピューティング企業の取扱に注意を要するデータへのアクセスを限定する、実装は、セキュリティ侵害またはそのようなプライバシ法への非準拠の場合に有利である。

例示的匿名化および仮名化されたデータデータベース

【００６８】

匿名化および仮名化されたデータデータベース１１４は、任意の参照またはデータの起源のインジケーションを除去するように処理されている、ユーザデータまたは環境データを含むことができる。例えば、匿名化および仮名化されたデータデータベース１１４上に記憶されるそのような情報にアクセスする、エンティティは、データと関連付けられる人物／ユーザまたは人々／複数のユーザを逆行分析することが不可能となるであろう。いくつかの状況（例えば、スモールデータセットまたは同等物）では、エンティティは、ある要因に基づいて、かつエンティティ独自の専有情報または他の公的にアクセス可能な情報に基づいて、可能性が高いユーザを統計的に絞り込むことが可能であり得ることを理解されたい。しかしながら、データ自体が、それ自体でデータが属する人物を示すべきではない。例えば、ある企業が、Ｍｏｎｔａｎａ州Ｂｕｔｔｅにおける、ユーザデバイス１０２を使用する、任意のユーザに関する、匿名化および仮名化されたデータデータベース１１

４からの匿名化および仮名化されたデータにアクセスし得るとすると、これは、１０人に関する結果を提供し得る。企業は、次いで、結果のみに基づいて、または付加的専有もしくは公的に利用可能なデータを用いてのいずれかにおいて、ある閾値内において、１０人のうちの何人かを決定し得る。しかしながら、データ匿名化および仮名化されたデータ自体は、そのようなインジケーションを提供せず、特に、結果のみに基づく、任意の逆行分析が、可能な限り限定されることが所望される。したがって、データを匿名化および仮名化するアルゴリズムが、適切に試験および実装されていることが証明され、匿名化および仮名化されたデータは、いくつかの実施形態では、サードパーティに提供される前に、照合されることが重要である。

【００６９】

いくつかの実施形態では、データ仮想化システム１１１が、データプラットフォーム１１２からのデータを要求すると、データプラットフォーム１１２は、匿名化および仮名化されたデータデータベース１１４にアクセスし、関連する暗号化されたユーザデータを特定し、匿名化および仮名化されたデータをデータ仮想化システム１１１に伝送することができる。トランザクションについてのデータは、記録されることができ、トランザクションについての情報は、処理および分散型台帳１０８上への記憶のために、エージェント１０６に伝送されることができる。処理は、トランザクションデータと特定のユーザまたはユーザデバイス１０２もしくは分散型台帳上の場所を関連付けることを含むことができる。処理はまた、任意のエラーを伴わずに、かつ最適化または効率的読出もしくは精査のために、分散型台帳１０８内に適切に保存するように、データをフォーマット化することを含むことができる。

例示的な暗号化されたデータデータベース

【００７０】

暗号化されたデータデータベース１１６は、ユーザデバイス１０２から受信された暗号化されたユーザデータまたは環境データを記憶することができる。いくつかの実施形態では、データプラットフォーム１１２は、記憶に先立って、データを暗号化することができる。いくつかの実施形態では、ユーザデバイス１０２は、記憶のために、データプラットフォーム１１２に伝送することに先立って、データを暗号化することができる（例えば、パブリックまたはプライベート暗号化キーを用いて）。いくつかの実装では、ユーザデバイス１０２が、例えば、セキュリティ侵害の場合、ユーザデバイス１０２独自のデータを暗号化し、全体的システムセキュリティを増加させることが所望され得る。セキュリティ侵害が、生じ、データプラットフォーム１１２が、危殆化される場合、暗号化されたデータは、暗号化されたデータが、暗号化解除されてデータプラットフォーム１１２に到着することが決してなく、かつ解読のために必要なキーが別個の場所（例えば、分散型台帳１０８またはユーザデバイス１０２）内に記憶され得るため、任意のセキュリティ侵害者にとって有用ではなくなるはずである。

【００７１】

いくつかの実施形態では、データ仮想化システム１１１が、データプラットフォーム１１２からのデータを要求すると、データプラットフォーム１１２は、暗号化されたデータデータベース１１６にアクセスし、関連する暗号化されたユーザデータを特定し、暗号化されたデータをデータ仮想化システム１１１に伝送することができる。トランザクションについてのデータは、記録されることができ、トランザクションについての情報は、処理および分散型台帳１０８上への記憶のために、エージェント１０６に伝送されることができる。処理は、トランザクションデータと特定のユーザまたはユーザデバイス１０２もしくは分散型台帳１０８上の場所を関連付けることを含むことができる。処理はまた、任意の誤差を伴わずに、かつ最適化または効率的読出もしくは精査のために、分散型台帳１０８内に適切に保存するように、データをフォーマット化することを含むことができる。

例示的データ照合システム

【００７２】

データ照合システム１１８は、種々のシステム間の伝送に先立って、種々の情報を照合

することができる。例えば、図３に関してさらに詳細に説明されるように、データ照合システム１１８は、プライベート暗号化キーおよびソフトウェアまたはスマートコントラクト基準もしくはルール、ならびに関連する暗号化されたユーザデータがデータ仮想化システム１１１に伝送されたことの確認を受信することができる（例えば、伝送の時間およびタイプを説明する情報ならびにユーザデータの説明、または関連し得る任意の他の情報を含む）。データ照合システム１１８は、次いで、暗号化されたユーザデータおよびプライベート暗号化キーがマッチングすることを照合し（例えば、データを解読することによって）、次いで、照合結果をエージェント１０６に伝送し、エージェントが、照合されたプライベート暗号化キーをデータ仮想化システム１１１に伝送し、すでに受信された暗号化されたユーザデータを解読することを可能にすることができる。

例示的データ仮想化システム

【００７３】

データ仮想化システム１１１は、購入者デバイス１０４と、データプラットフォーム１１２と、エージェント１０６と通信することができる。データ仮想化システム１１１は、ある情報またはユーザデータにアクセスする、それを要求する、もしくはそれを読み出すための要求を購入者デバイス１０４から受信することができる。例えば、データ仮想化システム１１１は、ユーザデータをデータプラットフォーム１１２から要求し、許可される場合、要求されたユーザデータ（例えば、暗号化されたユーザデータ）を受信することができる。いくつかの実施形態では、（例えば、ソフトウエアコントラクトの条件に基づいて）データを抽出する方法または抽出すべきデータに関する命令が、データ仮想化システム１１１が要求をデータプラットフォーム１１２に送信することに先立って、データ仮想化システム１１１に伝送されることができる。加えて、例えば、データ仮想化システム１１１は、１つまたはそれを上回るユーザデバイスのユーザデータもしくはユーザと関連付けられる、プライベート暗号化キーを受信することができる。プライベート暗号化キーは、データプラットフォーム１１２から受信された暗号化されたユーザデータを解読するために使用されることができる。加えて、いくつかの実施形態では、データトランザクション情報（例えば、１つまたはそれを上回るサードパーティサービスまたはデータプラットフォームからのユーザの関連データのダウンロード、読出、アクセス、または受信、もしくは同等物に関する情報）が、記憶のために、エージェント１０６に伝送されることができる。

【００７４】

データ仮想化システム１１１は、ユーザインターフェースを備え、購入者デバイス１０４による、データ仮想化システム１１１によって受信および解読された任意のユーザデータの相互作用ならびに操作を促進することができる。データ仮想化システム１１１はまた、購入者デバイス１０４が相互作用および操作するための統計的結果、チャート、グラフ、ならびにモデルを提供するように構成される、分析ツールを提供することができる。データ仮想化システム１１１はまた、分析の結果のダウンロードを可能にすることができる。しかしながら、いくつかの実施形態では、可能性として、例えば、ソフトウエアコントラクト１１０によって決定付けられるユーザプライバシ設定に基づいて、データ仮想化システム１１１は、解読されたユーザデータのダウンロードまたは伝送をブロックし、解読されたユーザデータの使用をアクティブ購入者デバイス１０４セッションのみに限定することができる。セッションの終了に応じて、データは、削除され、新しいプライベート暗号化キーが、ユーザデータを解読するために準備され、セキュリティを向上させるであろう（例えば、リリースされたプライベート暗号化キーが、もはや有用ではなくなるように）。本プロセスは、例えば、図３および４に関してさらに詳細に説明される。

例示的ユーザデバイス

【００７５】

ユーザデバイス１０２は、いくつかの実施形態では、エージェント１０６と、データプラットフォームと通信することができる。例えば、ユーザデバイス１０２は、パブリックまたはプライベート暗号化キーをエージェントから受信し、任意の収集または生成された

ユーザデータもしくは環境データを暗号化することができる。暗号化されたユーザデータは、記憶のために、ある時間インターバル（例えば、データが生成されるにつれてリアルタイムで、毎日、毎時、またはネットワークへの接続に応じて、もしくは任意の他の所望の時間またはインターバル）において、データプラットフォームに伝送されることができる。いくつかの実施形態では、キーは、ユーザデバイス１０２に送信されず、収集または生成されたユーザデータは、暗号化、次いで、記憶のために、データプラットフォーム１１２に伝送されることができる。上記および本明細書に議論されるように、いくつかの実装では、ユーザデバイス１０２が、例えば、セキュリティ侵害の場合、ユーザデバイス１０２独自のデータを暗号化し、全体的システムセキュリティを増加させることが所望され得る。セキュリティ侵害が、生じ、データプラットフォーム１１２が、危殆化される場合、暗号化されたデータは、暗号化されたデータが、暗号化解除されてデータプラットフォーム１１２に到着することが決してなく、かつ解読のために必要なキーが別個の場所（例えば、分散型台帳１０８またはユーザデバイス１０２）内に記憶され得るため、任意のセキュリティ侵害者にとって有用ではなくなるはずである。

【００７６】

ユーザデバイス１０２と関連付けられる、ユーザはまた、ユーザプライバシ設定またはプライバシ設定を提供することができる。ユーザは、ユーザ自身のユーザデータまたはそのデバイスによって生成された環境データの制御を有する。ユーザはまた、他のソース（例えば、（例えば、サードパーティ、他のデバイス、ユーザ自身、または利用可能な任意の他のデータ）からアクセス可能なユーザデータの制御を有する。例えば、ユーザは、ウェブブラウザまたは他の入力方法を介して、ユーザのユーザデータと関連付けられる、ユーザのプライバシ設定もしくはプライバシルールを示すことができる。プライバシ設定は、ユーザデータのアクセス性、共有、または販売に関する限定を示すことができる。例えば、プライバシ設定は、限定ではないが、以下、すなわち、ユーザデータにアクセスする、またはそれを購入することができる、もしくはそれらができない、購入者のタイプ、アクセス可能なデータのタイプに関する限定（例えば、環境データ、ユーザと関連付けられるサードパーティデータ、ユーザ提供データ、または同等物）、データがアクセス可能なときに関する限定（例えば、（例えば、時刻、週、または月）、データがアクセス可能な頻度に関する限定、アクセスの目的、アクセスのタイプ（例えば、接続またはアクセスする機械のタイプ）、アクセスの場所（例えば、（例えば、ＩＰを介して決定されるような購入者システムの生産国）、外部データソースに関する許可（例えば、ソーシャルメディアデータがユーザデータを付加するためにインポートされ得るかどうか）、もしくは任意の他の関連要因を示すことができる。プライバシ設定はまた、ブラックリストまたはホワイトリスト、ユーザに特定の人物、エンティティ、企業へのアクセスをブロックまたは許可する能力をオファーすること、もしくは名前またはタイプによる同等物を含むことができる。例えば、ユーザは、全ての銀行または関連付けられる企業をブラックリストに追加し、全てのユーザデータを銀行および関連付けられる企業によってアクセスされないようにブロックすることができる。いくつかの実施形態では、ユーザプライバシ設定またはプライバシルールは、ユーザによって随時更新されることができる。ユーザが、ユーザのプライバシ設定を更新後、ユーザのユーザデータに関する全ての将来的トランザクションイベントは、新しく更新されたプライバシ設定によって制御されるであろう。

例示的購入者デバイス

【００７７】

購入者デバイス１０４は、データ仮想化システム１１１と通信することができる。購入者デバイス１０４は、購入者によって動作される、またはそれと関連付けられることができる。購入者は、購入者デバイス１０４を使用して、データ仮想化システム１１１を通して、利用可能なユーザデータを購入する、それを閲覧する、それにアクセスする、それを精査する、それを分析する、またはそれと相互作用することができる。購入者が購入またはアクセスし得る、任意のユーザデータは、少なくとも部分的に、各ユーザの個別のソフトウエアコントラクトの中にプログラムされるような各ユーザのプライバシ設定に基づく

ことを理解されたい。いくつかの実施形態では、ソフトウエアコントラクトはまた、そのデータへのアクセスを有するべきである、または有するべきではない、購入者のタイプを定めることができる。例えば、特定のユーザは、その信用価値に影響を及ぼし得ることを恐れ得るため、全ての銀行または銀行販売員がそのデータにアクセスすることを禁止し得る。

【００７８】

いくつかの実施形態では、データ仮想化システム１１１は、ユーザインターフェースを備え、購入者デバイス１０４による、データ仮想化システム１１１によって受信および解読された任意のユーザデータの相互作用ならびに操作を促進することができる。データ仮想化システム１１１はまた、購入者デバイス１０４が相互作用および操作するための統計的結果、チャート、グラフ、ならびにモデルを提供するように構成される、分析ツールを提供することができる。データ仮想化システム１１１はまた、分析の結果のダウンロードを可能にすることができる。しかしながら、いくつかの実施形態では、可能性として、例えば、ソフトウエアコントラクト１１０によって決定付けられる、ユーザプライバシ設定に基づいて、データ仮想化システム１１１は、解読されたユーザデータのダウンロードまたは伝送をブロックし、解読されたユーザデータの使用を限定することができる（例えば、使用は、アクティブ購入者デバイス１０４セッションのみに限定される、またはある分析ツールは、ブロックまたは限定され得る、もしくは同等物である）。例えば、アクティブ購入者デバイス１０４セッションの終了に応じて、データは、削除され、新しいプライベート暗号化キーが、ユーザデータを解読するために準備され、セキュリティを向上させるであろう（例えば、リリースされたプライベート暗号化キーがもはや有用ではないように）。本プロセスは、例えば、図３および４に関してさらに詳細に説明される。

【００７９】

ユーザデバイス１０２または購入者デバイス１０４は、例えば、図７Ａを参照して説明されるウェアラブルディスプレイシステム１０００、または図７Ｂを参照して説明されるデバイス７０２ａ－７０２ｃ、もしくは図８を参照して説明されるユーザデバイス８２４等の拡張、複合、または仮想現実ディスプレイデバイスを含んでもよい。

種々のシステム間の例示的データフローの説明

【００８０】

図２－６は、種々のシステムおよびコンポーネントを横断して、ユーザデータまたは環境データと関連付けられる、ユーザプライバシ設定を受信および実装するための種々の方法のフロー図を示す。ある順序が、図２－６に描写されるが、データは、任意の順序において、かつ任意の方向または組み合わせにおいて、種々のシステム間で往復してフローし得ることを理解されたい。例えば、１つのシステムのある能力は、別のシステムまたはシステムのセット上に実装されることができる。加えて、例えば、１つのシステムは、いくつかのシステムから成ることができる。

ユーザプライバシ設定の例示的処理

【００８１】

図２Ａは、ユーザのためのプライバシ設定を作成または更新するための例示的方法２００のフロー図を示す。

【００８２】

ブロック２０２では、ユーザデバイス１０２が、ユーザと関連付けられる、プライバシ設定を受信する。ユーザデバイス１０２は、新しいまたは更新されたプライバシ設定を暗号化することができる。プライバシ設定は、新しい設定または以前に受信された設定の更新を含むことができる。

【００８３】

ブロック２０４では、エージェント１０６が、新しいまたは更新されたプライバシ設定を受信し、必要な場合、プライバシ設定を解読する。ブロック２０６では、エージェント１０６が、受信されたプライバシ設定に基づいて、ソフトウエアコントラクト（例えば、スマートコントラクトまたは同等物）を作成する。

【００８４】
ブロック２０８では、エージェント１０６が、プライベート暗号化キーを作成する。ブロック２１０では、エージェント１０６が、プライベート暗号化キーを暗号化する。例えば、プライベート暗号化キーは、パブリック暗号化キーで暗号化されることができる。
【００８５】
ブロック２１２では、エージェント１０６が、ソフトウエアコントラクトおよび暗号化されたプライベート暗号化キーを分散型台帳１０８内に記憶する。エージェント１０６は、分散型台帳１０８と通信し、種々のデバイス間の中間体として作用する。ある分散型台帳技術に関する限界に起因して、エージェントは、分散型台帳と相互作用し、それに保存するために使用される、要求されるコンポーネントであり得る。いくつかの実施形態では、エージェント１０６は、必要とされなくてもよく、分散型台帳１０８自体が、エージェント１０６の役割を充足させることが可能であり得る。
【００８６】
ブロック２１４では、エージェント１０６が、パブリック暗号化キーを作成する。図２－６に関して説明される全てのブロックと同様に、ブロック２１４は、ブロック２０６後に生じるが、ブロック２１４は、ブロック２０４直後に、ブロック２０４に先立って（例えば、ユーザが、最初に、アカウントを作成する、またはエージェント１０６に接続するとき）、ブロック２０８後、または本システムおよび方法の意図される目的を遂行するために十分な任意の順序において生じ得ることを理解されたい。
【００８７】
ブロック２１６では、エージェント１０６が、パブリック暗号化キーをユーザデバイスに１０２に伝送する。ブロック２１８では、ユーザデバイス１０２が、パブリック暗号化キーをエージェント１０６から受信する。
【００８８】
ブロック２２０では、ユーザデバイスが、環境データを収集し、これは、ユーザデータの少なくとも一部であって、例えば、ユーザデバイス１０２の周囲に基づく。
【００８９】
ブロック２２２では、ユーザデバイス１０２が、パブリック暗号化キーを使用して、収集された環境データおよび任意の他のユーザデータを暗号化する。ブロック２２４では、暗号化された環境データは、メタデータで意味論的にタグ付けされる。いくつかの実施形態では、メタデータは、暗号化解除され、個人的に識別可能な情報を含有しない。例えば、意味論注釈またはタグ付けは、暗号化されたデータを精査する、コンピュータおよび／または管理者が、暗号化されたデータについての情報（例えば、それは誰のデータか、データと関連付けられるユーザデバイス、または同等物）を確認することが可能であり得るように、付加的情報を暗号化された環境データに加えることを含むことができる。いくつかの実施形態では、意味論タグ付けは、ユーザプライバシをさらに保護するような範囲内に限定されることができる。
【００９０】
ブロック２２６では、意味論的にタグ付けおよび暗号化されたデータが、データプラットフォーム１１２への暗号化された接続によって、電子的に伝送される。いくつかの実施形態では、データプラットフォーム１１２は、データ記憶媒体（例えば、データレイク、ＮｏＳＱＬデータベース、または同等物）であることができる。いくつかの実施形態では、データプラットフォーム１１２は、一連またはセットのデータ記憶媒体であることができる。いくつかの実施形態では、データプラットフォーム１１２は、データ照合システム（例えば、１１８）を含み、データプラットフォーム１１２へおよびそこから伝送されるデータに関する処理および照合を実施することができる。ブロック２２８では、データプラットフォーム１１２が、意味論的にタグ付けおよび暗号化されたデータを受信する。
【００９１】
ブロック２３０では、データプラットフォーム１１２が、意味論的にタグ付けおよび暗号化されたデータを記憶する。いくつかの実施形態では、ブロック２３２では、記憶され

ることに応じて、意味論的にタグ付けおよび暗号化されたデータが、ハッシュ識別（例えば、最小３２バイト）を割り当てられる。いくつかの実施形態では、意味論的にタグ付けおよび暗号化されたデータは、別のタイプの識別値または参照番号を割り当てられることができる。

【００９２】

ブロック２３４では、データプラットフォーム１１２が、データトランザクション（例えば、意味論的にタグ付けおよび暗号化されたデータまたはデータトランザクションに関する任意の他の関連情報の受信および処理）の通知をエージェント１０６に伝送する。データプラットフォーム１１２はまた、ハッシュ識別値（またはハッシュが使用されない場合、任意の他の識別値）および意味論タグ付け情報を伝送する。ブロック２３６では、エージェント１０６が、情報および／またはデータを受信する。

【００９３】

ブロック２３８では、エージェント１０６が、ハッシュ識別値および／またはトランザクションデータを分散型台帳１０８の中にエンコーディングする。例えば、ハッシュ識別値およびトランザクションデータは、ブロック２１２内に記憶されたソフトウエアコントラクトおよび暗号化されたプライベート暗号化キーへの参照とともに、またはそのコピーとともに、記憶されることができる。ハッシュ識別値、トランザクションデータ、ソフトウエアコントラクト、およびプライベート暗号化キー間の関係を追跡する利点は、ユーザが、ユーザのプライバシ設定を精査し、トランザクションデータに基づいて、プライバシ設定が意図される通りに機能している、または該当する場合、変更が、例えば、プライバシ設定に行われるべきであることを照合し得ることである。

【００９４】

図２Ｂ－２Ｃは、ユーザのためのプライバシ設定を作成または更新するための例示的方法のスイムレーンフロー図を示す。図２Ａと同様に、図２Ｂ－２Ｃは、データ記憶媒体、ユーザのデバイス、Ｏｒａｃｌｅ、およびデータ仮想化アプリケーションによって実施される、種々のステップを示す。

プライバシ設定に基づく、ユーザデータの例示的特定、照合、および伝送の促進

【００９５】

図３は、ユーザデータを特定、伝送、および解読するための例示的方法のフロー図を示す。ある付加的または代替ブロックが、図に示されるように、図４、６Ａ、および６Ｂに描写される。

【００９６】

ブロック３０２では、エージェント１０６が、１人またはそれを上回るユーザと関連付けられ得る、ユーザデータのための要求を受信する。要求についてのさらなる詳細は、図６Ｂのブロック６２２に関連して説明される。

【００９７】

ブロック３０４では、エージェント１０６が、分散型台帳１０８、すなわち、１人またはそれを上回るユーザと関連付けられるソフトウエアコントラクトに関する分散型台帳を検索する。ユーザプライバシ設定に基づく、ソフトウエアコントラクトの作成の例示的説明は、図２Ａ－２Ｃに関して、かつ本明細書に提供される。

【００９８】

ブロック３０６では、エージェント１０６が、関連ソフトウエアコントラクトを含む、分散型台帳１０８の最新セクションを特定する。ある場合には、あるユーザに関して、ユーザのそれぞれと関連付けられる、１つのみのソフトウエアコントラクトが存在し得る。ある場合には、他のユーザに関して、ユーザのそれぞれと関連付けられる、２つまたはそれを上回るソフトウエアコントラクトが存在し得る。これは、例えば、いくつかの分散型台帳技術では、データが、ブロック内に記憶され得るためである。いったんブロックが、分散型台帳に書き込まれると、ブロックは、改変または除去されることができない。したがって、ソフトウエアコントラクトの任意の更新は、新しいソフトウエアコントラクトとして、新しいブロックに書き込まれなければならない。ユーザが、複数の更新をそのプラ

イバシ設定に提供する場合、分散型台帳の複数のブロックに保存される、複数のソフトウエアコントラクトが存在するであろう。分散型台帳内に記憶されるプライバシ設定の古いバージョンを有する利点は、ユーザ（または他のエンティティ）が、直接または間接的にのいずれかにおいて、対応するソフトウエアコントラクト内に表されるようなそのプライバシ設定の変更の履歴を閲覧することを可能にする。エージェント１０６にとって、特定のユーザに関して、新しいソフトウエアコントラクトを書き込むとき、ソフトウエアコントラクトが関連付けられる人物、ある場合には、ソフトウエアコントラクトのバージョンまたはそれが作成されたときの参照またはインジケーションを含むことは、有益である。いくつかの実施例では、エージェント１０６は、複数のソフトウエアコントラクトが特定のユーザに関して存在する場合、トランザクション情報（例えば、ブロックデータが特定のブロックに書き込まれた日付および時間またはブロックが分散型台帳に書き込まれた日付ならびに時間）に依拠して、最も最近のソフトウエアコントラクトを決定することができる。

【００９９】

ブロック３０８では、エージェント１０６が、その最新ソフトウエアコントラクトのそれぞれに基づいて、そのユーザデータの共有を許可する、１人またはそれを上回るユーザを決定する。例えば、あるユーザは、任意の情報を、ユーザデータのための受信された要求と関連付けられる特定の購入者と共有することを所望しない場合があり、それらのユーザと関連付けられるデータは、共有またはアクセス可能にされるべきではない。要求され、ユーザが共有を許可する、ユーザデータのみが、要求と関連付けられる購入者と共有される、またはそれにアクセス可能にされるべきである。

【０１００】

ブロック３１０では、エージェント１０６が、命令をデータ仮想化システム１１１に発行し、要求され、共有を許可したユーザと関連付けられる、ユーザデータを抽出する。ブロック３１２では、データ仮想化システム１１１が、命令をブロック３１０から受信する。

【０１０１】

ブロック３１４では、データ仮想化システム１１１が、エージェント１０６から受信された命令に基づいて、ユーザデータをデータプラットフォーム１１２から要求する。ブロック３１６では、データプラットフォーム１１２が、ユーザデータへのアクセスのための要求を受信する。

【０１０２】

ブロック３１８では、データプラットフォーム１１２が、１つまたはそれを上回るデータベース内の共有を許可した１人またはそれを上回るユーザに関する、関連する暗号化されたユーザデータを特定し、読み出す。データプラットフォーム１１２がユーザデータと相互作用する方法に関する付加的詳細は、図２および４－６に関連して説明される。ブロック３２０では、データプラットフォーム１１２が、関連する暗号化されたユーザデータをデータ仮想化システム１１１に伝送または利用可能にする。ブロック３２１では、データ仮想化システムが、関連する暗号化されたユーザデータをブロック３２０から受信する、またはそれにアクセスする。

【０１０３】

ブロック３２２では、データプラットフォーム１１２が、データ照合システム１１８およびエージェント１０６に、関連する暗号化されたユーザデータが、ブロック３２０、３２１において、正常に伝送された、またはデータ仮想化システム１１１によって受信されたことの確認を伝送する。ブロック３２３では、エージェントが、確認を受信し、ブロック３２４では、データ照合システム１１８が、確認を受信する。

【０１０４】

ブロック３２５では、エージェント１０６が、プライベート暗号化キーを、共有を許可した１人またはそれを上回るユーザと関連付けられるソフトウエアコントラクトから読み出す、もしくはそれにアクセスする。ブロック３２７では、プライベート暗号化キーが、データ照合システム１１８に伝送され、ブロック３３１では、エージェントが、ブロック

４０２において開始する、図４に説明される付加的ステップを実施する。ブロック３２９では、データ照合システム１１８が、プライベート暗号化キーを受信する。

【０１０５】

ブロック３２６では、データ照合システム１１８が、例えば、各キーと関連付けられるユーザデータを正常に解読することによって、ユーザデータおよびプライベート暗号化キーがマッチングすることを照合する。

【０１０６】

ブロック３２８では、ユーザデータが正常に解読されたかどうかに基づいて、データ照合システム１１８が、照合結果をエージェント１０６に伝送する。いくつかの実施形態では、複数のユーザのユーザデータが、照合されるべきであって、一部のみが、成功し、残りの部分が、不成功である（例えば、プライベート暗号化キーが、ユーザの一部に関するデータを適切に解読し得ない）場合、結果全体が、処理のために、エージェント１０６に伝送されることができる。

【０１０７】

ブロック３３０では、エージェント１０６が、照合結果を受信する。いくつかの実施形態では、プライベート暗号化キーのうちのいくつかが、正常に照合され、その他が、そうではなかった場合、成功した部分は、データ仮想化システム１１１に伝送されることができる。いくつかの実施形態では、プライベート暗号化キーのうちのいくつかが、正常に照合され、その他が、そうではなかった場合、何も、データ仮想化システム１１１に伝送されず、エージェント１０６は、照合が成功するまで、他の潜在的プライベート暗号化キーを用いて、ブロック３２５－３２８におけるプロセスを繰り返し、次いで、全ての関連および照合されたプライベート暗号化キーをともに伝送する。全てのプライベート暗号化キーをともに伝送すること、または購入者が要求を調節もしくはキャンセルすることを所望する場合、任意のものを提示することに先立って、購入者に、データ仮想化システム１１１を使用して、全てのデータが利用可能ではないことをプロンプトすることが所望され得る。いくつかの実施形態では、プライベート暗号化キーのうちのいくつかが、ブロック３２６において、データ照合システム１１８によって、正常に照合され、その他が、そうではなかった場合、成功部分は、データ仮想化システムに伝送されることができ、ブロック３２５、３２７、３２９、３２６、および３２８におけるプロセスは、正しいプライベート暗号化キーが特定されるまで、不成功部分に関して繰り返され、次いで、データ仮想化システム１１１に伝送することができる。

【０１０８】

データ仮想化システム１１１を使用する、購入者が、遅延されず、ブロック３３２において、付加的新しいプライベート暗号化キーがブロック３３０から受信またはアクセスされるにつれて、付加されるデータを用いて、データをより迅速に精査し得るように、任意のプライベート暗号化キーを、いったん照合されると、データ仮想化システム１１１に伝送し、任意の付加的照合されたプライベート暗号化キーを、いったん照合されると、後に伝送ことが所望され得る。いくつかの実施形態では、プライベート暗号化キーが、データ照合システム１１８によるある試行回数（例えば、１、２、３等）後、照合されることができない場合、最終エラーが、エージェント１０６に出力され、次いで、照合されることができないプライベート暗号化キーと関連付けられる、その特定のユーザデータに関連するデータ仮想化システム１１１に出力され得る。ブロック３３２では、データ仮想化システム１１１が、照合されたプライベート暗号化キーを受信する、またはそれにアクセスする。

【０１０９】

ブロック３３４では、ブロック３２１からの関連する暗号化されたユーザデータおよびブロック３３２から受信されたマッチングならびに照合されたプライベート暗号化キーに基づいて、データ仮想化システム１１１は、データプラットフォームから受信された暗号化されたユーザデータのセット毎に、関連付けられるプライベート暗号化キーを使用して、ブロック３３２においてエージェント１０６から受信またはアクセスされるプライベー

ト暗号化キーを用いて、暗号化されたユーザデータを解読することができる。
【０１１０】
ブロック３３６では、データ仮想化システム１１１が、データ仮想化システム１１１を使用する、購入者が、データが関連付けられる、ユーザを識別することができないように、解読されたユーザデータを匿名化および仮名化する。例えば、仮名化は、データ管理および匿名化プロシージャであって、それによってデータ記録内の個人的に識別可能な情報フィールドは、１つまたはそれを上回る人工識別子、すなわち、仮名によって置換される。置換されたフィールドまたは置換されたフィールドの集合毎の単一仮名が、残りがデータ分析およびデータ処理のために好適であるまま、データ記録を殆ど識別可能ではないものにする。いくつかの実施形態では、仮名化されたデータは、情報の追加を用いて、データのオリジナル状態に復元されることができ、これは、次いで、個人が再識別されることを可能にする一方、匿名化されたデータは、データのオリジナル状態に決して復元されることができない。いくつかの実施形態では、仮名化が、所望されるほど効果的ではない場合（例えば、ブロック３３８および事前構成または自動閾値参照）、断片化またはユーザデータを改変する他の方法も同様に、使用されることができる。
【０１１１】
ブロック３３８では、データ仮想化システム１１１が、ユーザデータのいずれかの再識別が、不可能である、すなわち、事前構成または自動閾値（例えば、データと特定の人物を関連付けることができないことの４０％、５０％、５１％、８０％、９０％、９５％、９９％の可能性）内において統計的に不可能であることを検証および再検証するための試験を実行する。
【０１１２】
ブロック３４０では、いったんデータ仮想化システム１１１が、閉じられると（例えば、購入者からの終了するための命令の受信に応じて）、データ仮想化システム１１１は、セッションを閉じ、受信した任意のユーザデータおよびプライベート暗号化キーを消去する。また、ブロック３４２では、図６Ａが、購入者がデータ仮想化システム１１１と相互作用し得る方法、およびユーザデータがさらにブロック６０２においてデータ仮想化システム１１１からエクスポートされる、または取り出されないように保護される方法に関する付加的詳細を説明する。
新しいプライベート暗号化キーの例示的生成およびユーザデータへの適用
【０１１３】
図４は、新しいプライベート暗号化キーを生成し、ユーザデータを新しいプライベート暗号化キーで再暗号化するための方法４００のフロー図を示す。ある付加的または代替ステップが、図３に描写される。プライベート暗号化キーが、図３におけるブロック３３０において、データ仮想化システム１１１に伝送された後、図３におけるブロック３３１は、ブロック４０４において開始するプロセスを含むことができる。
【０１１４】
ブロック４０４では、エージェント１０６が、図３におけるブロック３３０においてデータ仮想化システム１１１に伝送または利用可能にされるプライベート暗号化キーと関連付けられる、任意のユーザデータのための新しいプライベート暗号化キーを生成することができる。新しいプライベート暗号化キーを生成して、任意の分散型プライベート暗号化キーと関連付けられるユーザデータを再暗号化することが望ましい。例えば、購入者が、それがデータ仮想化システムを通して受信する、プライベート暗号化キーのいずれかを公開することになる場合、ユーザデータのセキュリティおよびプライバシは、危殆化され得る。いくつかの実施形態では、購入者は、データ仮想化システム１１１が受信またはアクセスする、任意のプライベートキーへの直接アクセスを有しないであろうが、新しいプライベート暗号化キーを生成することは、購入者が、例えば、認可を伴わずに、データ仮想化システムをハッキングし、キーを読み出す場合、依然として、よりセキュアである。
【０１１５】
ブロック４０６では、エージェント１０６が、新しいプライベート暗号化キーを、その

データが、図３において共有またはアクセスされた、ユーザと関連付けられる、更新されたソフトウエアコントラクト内に記憶する。データ仮想化システムへおよびそこからのデータトランザクションに関する任意の情報も同様に、いくつかの実施形態では、更新されたソフトウエアコントラクトとともに記憶されるであろう。例えば、図３におけるブロック３３０でのプライベート暗号化キーの伝送に関連する伝送詳細は、更新されたソフトウエアコントラクト内に記憶されるであろう。

【０１１６】

ブロック４０８では、エージェント１０６が、新しいプライベート暗号化キーおよび古いプライベート暗号化キー（例えば、図３におけるブロック３３０で伝送されたキー）をデータプラットフォーム１１２に伝送または利用可能にする。ブロック４１０では、データプラットフォームが、新しいプライベート暗号化キーをエージェント１０６から受信する。

【０１１７】

ブロック４１２では、データプラットフォーム１１２が、それがブロック４１０において受信したプライベート暗号化キーと関連付けられる、ユーザデータを特定する。ブロック４１４では、データプラットフォーム１１２が、ユーザデータを古いプライベート暗号化キーで解読し、次いで、ユーザデータを新しいプライベート暗号化キーで再暗号化する。次いで、ブロック４１６では、再暗号化されたユーザデータが、１つまたはそれを上回るデータベース内に記憶される。

ユーザデータにサードパーティデータを付加する実施例

【０１１８】

図５は、ユーザデータに１つまたはそれを上回るサードパーティサービスから読み出された、またはアクセスされたサードパーティデータを付加するための方法５００のフロー図を示す。ある付加的または代替ステップが、図６Ｂに描写される。任意のサードパーティデータが、読み出され、またはアクセスされ、ユーザデータに付加することができることを理解されたい。例えば、サードパーティデータは、（例えば、信用調査機関または信用格付サービスからの）財務上のデータ、ソーシャルメディアデータ（例えば、Ｆａｃｅｂｏｏｋ、ＭｙＳｐａｃｅ、ＬｉｎｋｅｄＩｎ、Ｉｎｓｔａｇｒａｍ、Ｓｎａｐｃｈａｔ等）、個人的データ（例えば、Ｄｒｏｐｂｏｘ、Ｂｏｘ、ＧｏｏｇｌｅＤｒｉｖｅ、ＡｐｐｌｅのｉＣｌｏｕｄ等のファイル共有サイトにアップロードされた）、ビデオストリーミングサービス（例えば、Ｎｅｔｆｌｉｘ、Ａｍａｚｏｎ Ｐｒｉｍｅ Ｖｉｄｅｏ、Ｈｕｌｕ等）からの任意の閲覧習慣、電子メールまたはチャットサービス（例えば、Ｇｍａｉｌ、Ｙａｈｏｏ Ｍａｉｌ、Ｇｏｏｇｌｅ Ｈａｎｇｏｕｔｓ、Ｚｏｏｍ Ｖｉｄｅｏ、ＷｈａｔｓＡｐｐ、Ｆａｃｅｂｏｏｋ Ｍｅｓｓｅｎｇｅｒ、Ｏｕｔｌｏｏｋ等）からのコンテンツ、またはユーザがアクセスを提供することを所望する、任意の他のサードパーティサービスを含むことができる。

【０１１９】

本明細書に説明される図６Ｂにおけるブロック６２２からのプロセス後に開始し得る、ブロック５０４では、エージェント１０６が、データ仮想化システム１１１から受信されたユーザデータのための要求に基づいて、特定のユーザまたはユーザのセットと関連付けられる、分散型台帳１０８内の１つまたはそれを上回るソフトウエアコントラクトを検索することができる（要求に関するさらなる情報および詳細に関しては、図６Ｂ参照）。

【０１２０】

ブロック５０６では、エージェント１０６が、１人またはそれを上回るユーザに関する関連ソフトウエアコントラクトを含む、分散型台帳の最新セクションを特定することができる。上記に説明されるように、ある場合には、あるユーザに関して、ユーザのそれぞれと関連付けられる、１つのみのソフトウエアコントラクトが存在し得る。ある場合には、他のユーザに関して、ユーザのそれぞれと関連付けられる、２つまたはそれを上回るソフトウエアコントラクトが存在し得る。これは、例えば、いくつかの分散型台帳技術では、データが、ブロック内に記憶され得るためである。いったんブロックが、分散型台帳に書

き込まれると、ブロックは、改変または除去されることができない。したがって、ソフトウエアコントラクトの任意の更新は、新しいソフトウエアコントラクトとして、新しいブロックに書き込まれなければならない。ユーザが、複数の更新をそのプライバシ設定に提供する場合、分散型台帳の複数のブロックに保存される、複数のソフトウエアコントラクトが存在するであろう。分散型台帳内に記憶されるプライバシ設定の古いバージョンを有する利点は、ユーザ（または他のエンティティ）が、直接または間接的にのいずれかにおいて、対応するソフトウエアコントラクト内に表されるようなそのプライバシ設定の変更の履歴を閲覧することを可能にする。エージェント１０６にとって、特定のユーザに関して、新しいソフトウエアコントラクトを書き込むとき、ソフトウエアコントラクトが関連付けられる人物、ある場合には、ソフトウエアコントラクトのバージョンまたはそれが作成されたときの参照またはインジケーションを含むことは、有益である。いくつかの実施例では、エージェント１０６は、複数のソフトウエアコントラクトが特定のユーザに関して存在する場合、トランザクション情報（例えば、ブロックデータが特定のブロックに書き込まれた日付および時間またはブロックが分散型台帳に書き込まれた日付および時間）に依拠して、最も最近のソフトウエアコントラクトを決定することができる。

【０１２１】

ブロック５０８では、エージェント１０６が、分散型台帳内に記憶され、ソフトウエアコントラクトによって表される、ユーザプライバシ設定に基づいて、収集されたデータおよび１つまたはそれを上回るサードパーティサービスからのデータの共有を許可する、１人またはそれを上回るユーザを決定する。

【０１２２】

ブロック５１０では、エージェント１０６が、命令をデータ仮想化システム１１１に発行し、要求され、1つまたはそれを上回るサードパーティサービスからの共有を許可したユーザと関連付けられる、ユーザデータを抽出する。命令はまた、ソフトウエアコントラクトに関する詳細と、データ仮想化システム１１１にアクセスする購入者と共有されるべき、および共有されるべきではない、データのタイプと、データのための要求を開始した人物とを含むことができる。ブロック５１２では、データ仮想化システム１１１が、命令をブロック５１０から受信する、またはそれにアクセスする。

【０１２３】

ブロック５１４では、データ仮想化システム１１１が、１つまたはそれを上回るサードパーティサービスのうちの１つから許可される、サードパーティデータを読み出す、またはそれにアクセスする。例えば、読出は、ＡＰＩコールの使用を通して、または任意の他の利用可能な手段によって、実施されることができる。

【０１２４】

ブロック５１６では、データ仮想化システム１１１が、サードパーティデータをプロファイリングし、それにメタデータをタグ付けする。いくつかの実施形態では、メタデータは、サードパーティデータが生じた場所、サードパーティデータが関連付けられるユーザ、データが読み出された時間、または任意の他の関連情報を説明することができる。

【０１２５】

ブロック５１８では、サードパーティデータが、クレンジングおよびフォーマット化されることができる。例えば、いくつかの実施形態では、データは、編集され、ユーザプライバシ設定またはソフトウエアコントラクトに基づいて共有されることが許可されない、任意の情報を除去することができる。いくつかの実施形態では、余剰または非関連情報が、読み出されてもよく（例えば、ＡＰＩを通して）、データは、データ仮想化システム１１１要件または購入者もしくはシステムの表示選好に準拠するようにフォーマット化されなければならない。

【０１２６】

ブロック５２０では、データ仮想化システム１１１が、任意の以前に記憶されたユーザデータにサードパーティデータを付加し、コンテキスト化することができる。例えば、データ付加は、外部当局ソースからのサードパーティデータとファーストパーティ顧客デー

タの既存のデータベースをマージすることを意味し得る。また、例えば、コンテキスト化は、エンティティのコンテキスト情報に基づいて、エンティティに関連するデータ（例えば、人物または都市）を識別するプロセスであり得る。例えば、コンテキストまたはコンテキスト情報は、（フィルタリング、集約、および推定を介して）具体的用途の範囲内において決定を行うために要求される推測の量を効果的に低減させるために使用され得る、任意のエンティティについての任意の情報であり得る。コンテキスト化は、次いで、エンティティのコンテキスト情報に基づいて、エンティティに関連するデータを識別するプロセスである。コンテキスト化は、非関連データを検討から除外することができ、大規模なデータ集約的用途において、量、速度、および多様性を含む、いくつかの側面から、データを低減させる潜在性を有する。コンテキスト化の利点は、用途／サービス／ユーザからの関心に基づいて、データの量を低減させる潜在性を含むことができる。加えて、コンテキスト化の別の利点は、非関連データを除外することによって、データプロセス、クエリ、および／または送達のスケーラビリティならびに効率性を改良することができることである。

【０１２７】

ブロック５２２では、データ仮想化システム１１１が、ブロック５１４において読み出された新しいサードパーティデータの通知およびトランザクション詳細をエージェント１０６に伝送することができる。ブロック５２４では、エージェント１０６が、新しいサードパーティデータの通知およびトランザクション詳細を受信することができる。

【０１２８】

ブロック５２６では、エージェント１０６が、データトランザクション情報（例えば、データ抽出、プロファイリングおよび処理、暗号化等）を分散型台帳１０８の中にエンコーディングすることができる。加えて、ブロック５２６では、エージェント１０６が、サードパーティデータが読み出された、ユーザ（または複数のユーザ）と関連付けられる、パブリック暗号化キーを読み出し、ブロック５２８では、パブリック暗号化キーをデータ仮想化システム１１１に伝送することができる。ブロック５３０では、データ仮想化システムが、パブリック暗号化キーを受信する。

【０１２９】

ブロック５３２では、データ仮想化システム１１１が、ブロック５１４においてサードパーティサービスから読み出される、またはアクセスされる、サードパーティデータを暗号化し、いくつかの実施形態では、サードパーティデータを任意の以前に記憶されたユーザデータで暗号化する。ブロック５３２における暗号化が、処理が、ブロック５１６、５１８、および５２０において、データ仮想化システム１１１によって、サードパーティデータに対して実施された後、生じるであろう。

【０１３０】

ブロック５３４では、データ仮想化システム１１１が、暗号化されたユーザデータをデータプラットフォーム１１２に伝送または利用可能にする。ブロック５３８では、データプラットフォーム１１２が、暗号化されたユーザデータを受信し、またはそれにアクセスし、ブロック５４０では、暗号化されたユーザデータを１つまたはそれを上回るデータベース内に記憶する。

【０１３１】

ブロック５３６では、いったんデータ仮想化システム１１１が、閉じられると（例えば、購入者からの終了するための命令の受信に応じて）、データ仮想化システム１１１は、セッションを閉じ、データ仮想化システム１１１が受信した任意のユーザデータ（任意のサードパーティデータを含む）および任意のプライベート暗号化キーを消去する。また、図６Ａおよび６Ｂは、購入者がデータ仮想化システム１１１と相互作用し得る方法、およびユーザデータがさらにブロック６０２においてデータ仮想化システム１１１からエクスポートされる、または取り出されないように保護される方法に関する付加的詳細を説明する。

ユーザデータのさらなる検証、処理、および監視

【０１３２】
図６Ａは、ユーザデータを検証、処理、および監視するための方法６００のフロー図を示す。ある付加的または代替ステップが、図３に描写される。
【０１３３】
図３からのブロック３４２におけるプロセス後に開始し得る、ブロック６０４では、例えば、データ仮想化システム１１１が、ユーザデータに対して、集約、事前分析、および／またはコンテキスト化を実施する。例えば、集約は、集計関数または集約関数を含むことができ、これは、データの複数の行の値が、ともにグループ化され、単一記述値を形成し得る、関数である。いくつかの一般的集計関数は、ａｖｅｒａｇｅ（すなわち、算術平均）、ｃｏｕｎｔ、ｍａｘｉｍｕｍ、ｍｅｄｉａｎ、ｍｉｎｉｍｕｍ、ｍｏｄｅ、ｒａｎｇｅ、ｓｕｍ、ｎａｎｍｅａｎ（「ｎｉｌ」または「ｎｕｌｌ」としても知られる、ＮａＮ値を無視する平均）、またはｓｔｄｄｅｖを含むことができる。事前分析は、例えば、任意のデータにアクセスすることに先立って構成されるであろう、購入者がユーザデータを分析する方法を説明するように構成されることができる。次いで、ブロック６０６では、データ仮想化システム１１１が、ユーザデータを、上記および本明細書に説明される、メタデータでエンコーディングする。
【０１３４】
ブロック６０８では、データ仮想化システム１１１が、機械学習または人工知能（ＡＩ）を用いて、ユーザデータを監視し、ユーザデータの非認可エクスポートを防止する。いくつかの実施形態では、データ仮想化システム１１１からのあるユーザデータの非認可エクスポートを防止し、ユーザデータのセキュリティおよびプライバシを潜在的に増加させることが望ましい。例えば、購入者が、ユーザデータをシステムから取り出すことになる場合、購入者は、次いで、データを販売する、またはそれを公開し得る。
【０１３５】
いくつかの実施形態では、機械学習が、ユーザデータおよびデータ仮想化システム１１１との購入者相互作用を監視し、ユーザデータの非認可エクスポートを防止するために使用されることができる。例えば、データ仮想化システム１１１（または、他の実施形態では、１つまたはそれを上回る他のシステム）は、機械学習アルゴリズムまたはＡＩを実装し、ユーザデータおよびユーザデータの操作を監視し、ユーザデータまたはユーザデータの一部がデータ仮想化システム１１１からエクスポートまたはコピーされないことを確実にすることができる。
【０１３６】
いくつかの異なるタイプのアルゴリズムも同様に、データ仮想化システム１１１によって使用されてもよい。例えば、本明細書におけるある実施形態は、ロジスティック回帰モデルを使用してもよい。しかしながら、線形回帰モデル、離散選択モデル、または一般化線形モデル等の他のモデルも、可能性として考えられる。機械学習アルゴリズムは、データ仮想化システム１１１によって受信された新しい入力に基づいて、経時的に、モデルを適応的に開発および更新するように構成されることができる。例えば、モデルは、新しいユーザ情報が、データ仮想化システム１１１によって受信される、または読み出されるにつれて、周期的ベースで再生成され、ユーザデータが更新されるにつれて、モデル内の予測をより正確に保つことに役立つことができる。データ仮想化システム１１１は、さらに本明細書に詳細に説明される。
【０１３７】
パラメータ関数または予測モデルを生成および更新するために使用され得る、機械学習アルゴリズムのいくつかの非限定的実施例は、回帰アルゴリズム（例えば、通常の最小二乗法回帰等）、インスタンスベースのアルゴリズム（例えば、学習ベクトル数値化等）、決定木アルゴリズム（例えば、分類および回帰ツリー等）、ベイズアルゴリズム（例えば、単純ベイズ等）、クラスタ化アルゴリズム（例えば、ｋ－平均クラスタリング等）、関連付けルール学習アルゴリズム（例えば、アプリオリアルゴリズム等）、人工ニューラルネットワークアルゴリズム（例えば、パーセプトロン等）、深層学習アルゴリズム（例え

ば、深層ボルツマン機械等）、次元性低減アルゴリズム（例えば、主成分分析等）、アンサンブルアルゴリズム（例えば、スタックによる一般化等）、または他の機械学習アルゴリズムを含む、教師ありおよび教師なし機械学習アルゴリズムを含むことができる。

【０１３８】

これらの機械学習アルゴリズムは、ｋ－平均アルゴリズム等の階層クラスタ化アルゴリズムおよびクラスタ分析アルゴリズムを含む、任意のタイプの機械学習アルゴリズムを含んでもよい。ある場合には、機械学習アルゴリズムの実施は、人工ニューラルネットワークの使用を含んでもよい。機械学習技法を使用することによって、膨大な量（テラバイトまたはペタバイト等）の関与者相互作用データが、ユーザ選好を識別するために分析されてもよい。これらのユーザ選好は、履歴データを使用して、オフラインで決定されてもよい。さらに、決定された選好は、次いで、本明細書に開示される技法を使用しない、他のマッチングを行うシステムと比較して、増加されたユーザ享受、その結果、関与を提供し得る、マッチングするプラン（下記にさらに詳細に説明されるように）を選択するためにリアルタイムで使用されてもよい。

【０１３９】

ブロック６１０では、購入者が、データ仮想化システム１１１の仮想環境内のユーザデータおよび任意の他の統計的データを分析し得る。購入者は、結果として生じる分析および認可されるデータのみを抽出することができる。例えば、あるユーザは、その個別のユーザデータのエクスポートを認可し得る一方、他のユーザは、任意のエクスポートまたはいくつかのエクスポート能力を認可しない場合がある（例えば、ユーザのユーザデータの一部のみが、エクスポート可能であり得、別の部分は、エクスポート不能であり得る）。

【０１４０】

ブロック６１２では、いったんデータ仮想化システム１１１が、閉じられると（例えば、購入者からの終了するための命令の受信に応じて）、データ仮想化システム１１１は、セッションを閉じ、データ仮想化システム１１１が受信した任意のユーザデータおよび任意のプライベート暗号化キーを消去する。

匿名化および仮名化されたユーザデータのための要求

【０１４１】

図６Ｂは、匿名化および仮名化されたユーザデータのための要求を処理するための方法６５０の実施例のフロー図を示す。ある付加的または代替ステップが、図３および５に描写される。

【０１４２】

ブロック６１４では、データ仮想化システム１１１が、ユーザデータのアクセスまたは購入のための要求を購入者から受信する。要求は、関連付けられるソフトウエアコントラクトならびに任意のすでに処理および記憶された匿名化および仮名化されたユーザデータを用いたチェックを要求する、ユーザデータのための要求を含むことができる。例えば、いくつかの実施形態では、本システム（例えば、データプラットフォーム１１２、エージェント１０６等）は、ユーザデータを匿名化または匿名化し、処理されたデータをデータプラットフォーム１１２内に記憶することができる。いくつかの実施形態では、匿名化および仮名化されたユーザデータは、ユーザデータが十分に匿名化および仮名化されていることを確実にするためにチェックならびに照合されることができる。いくつかの実施形態では、ユーザは、そのプライバシ設定内に、彼らが、そのデータが匿名化および仮名化され、および／または購入者に提供されることを可能にするであろうかどうかを示さなければならない。いくつかの実施形態では、ユーザは、インジケーションを行う必要がない場合があり、代わりに、いくつかまたは全てのそのデータは、匿名化および仮名化され、購入者に提供されてもよい。いくつかの実施形態では、匿名化および仮名化されたユーザデータは、全体として、ユーザについての汎用の統計的情報のみを含む。あるフィルタリングオプションが、データ仮想化システム１１１を介して、匿名化および仮名化されたユーザデータの閲覧を精緻化するために利用可能であり得る。

【０１４３】

ブロック６１６では、データ仮想化システム１１１が、ソフトウエアコントラクトによって表され、施行されるようなプライバシ設定を介して、購入者と共有されるために利用可能かつ認可される、要求されるユーザデータの部分（例えば、匿名化および仮名化されたユーザデータ）と、ユーザから付加的承認を要求する、要求されるユーザデータの部分とを決定するための要求を処理する。

【０１４４】

ブロック６１８では、付加的承認をユーザから要求する、要求されるユーザデータの部分に関して、データ仮想化システム１１１が、エージェント１０６に、ユーザデータに関する要求を伝送する、または要求のバッチを利用可能にする。ブロック６２０では、エージェント１０６が、ユーザデータに関する要求を受信する。

【０１４５】

ブロック６２２では、エージェント１０６が、ブロック６１４において受信された要求に基づいて、分散型台帳１０８、すなわち、１人またはそれを上回るユーザと関連付けられる1つまたはそれを上回るソフトウエアコントラクトに関する分散型台帳を検索する。ユーザプライバシ設定に基づく、ソフトウエアコントラクトの作成の例示的説明は、図２Ａ－２Ｃに関して、かつ本明細書に提供される。付加的ステップが、図３および５に関連して議論される。例えば、図３におけるブロック３０２および図５におけるブロック５０２において開始する、ブロック６２２から継続する、ステップが存在する。

【０１４６】

ブロック６２４では、付加的承認をユーザから要求せず、購入者と共有されるために利用可能かつ認可される、要求されるユーザデータの部分に関して、データ仮想化システム１１１が、匿名化および仮名化されたユーザデータのための要求をデータプラットフォーム１１２に伝送する。ブロック６２６では、データプラットフォーム１１２が、匿名化および仮名化されたユーザデータのための要求を受信する。

【０１４７】

ブロック６２８では、データプラットフォーム１１２が、任意の匿名化および仮名化されたユーザデータを特定し、データ仮想化システム１１１に伝送する。ブロック６３０では、データプラットフォーム１１２が、任意の匿名化および仮名化されたユーザデータを受信する。

【０１４８】

ブロック６３２では、いったんデータ仮想化システム１１１が、閉じられると（例えば、購入者からの終了するための命令の受信に応じて）、データ仮想化システム１１１は、セッションを閉じ、データ仮想化システム１１１が受信した任意の匿名化および仮名化されたユーザデータならびに任意のプライベート暗号化キーを含む、任意のユーザデータを消去する。

例示的空間コンピューティングデバイス

【０１４９】

空間コンピューティングデバイスまたは頭部搭載型ディスプレイ（ＨＭＤ）等のウェアラブルディスプレイシステムは、ハンドヘルドユーザ入力デバイス等のコンパニオンデバイスと協働するように構成されてもよい。空間コンピューティングデバイスは、空間コンピューティングデバイスのユーザの環境を結像し得る、カメラ等の外向きに面した画像捕捉デバイスを含むことができる。画像捕捉デバイスは、共有情報またはデータ（例えば、共有キー、共有秘密、または署名キー）を空間コンピューティングデバイスとコンパニオンデバイスとの間に確立するために、コンパニオンデバイス上に表示される情報またはデータ（例えば、キーまたは秘密）を捕捉および取得するために使用されることができる。共有データは、ひいては、空間コンピューティングデバイスまたはコンパニオンデバイスによって使用され、セキュアデータ転送またはデータプラットフォームのため／からのデータを暗号化／解読することができる。

【０１５０】

図７Ａは、仮想現実（ＶＲ）、拡張現実（ＡＲ）、または複合現実（ＭＲ）体験をディ

スプレイシステム装着者または視認者１００４に提示するために使用され得る、空間コンピューティングデバイスまたはウェアラブルディスプレイシステム１０００の実施例を図示する。ウェアラブルディスプレイシステム１０００は、本明細書に説明される用途または実施形態のいずれかを実施するようにプログラムされてもよい。ディスプレイシステム１０００は、ディスプレイ１００８と、ディスプレイ１００８の機能をサポートするための種々の機械的および電子的モジュールならびにシステムとを含む。ディスプレイ１００８は、フレーム１０１２に結合されてもよく、これは、ディスプレイシステムユーザ、装着者、または視認者１００４によって装着可能であって、ディスプレイ１００８を装着者１００４の眼の正面に位置させるように構成される。ディスプレイ１００８は、ライトフィールドディスプレイであってもよい。いくつかの実施形態では、スピーカ１０１６が、フレーム１０１２に結合され、ユーザの外耳道に隣接して位置付けられる。いくつかの実施形態では、示されない、別のスピーカが、ユーザの他の外耳道に隣接して位置付けられ、ステレオ／調節可能音制御を提供する。ディスプレイ１００８は、有線導線または無線コネクティビティ等によって、ローカルデータ処理モジュール１０２４に動作可能に結合１０２０され、これは、フレーム１０１２に固定して取り付けられる、ユーザによって装着されるヘルメットまたは帽子に固定して取り付けられる、ヘッドホンに内蔵される、または別様に、ユーザ１００４に除去可能に取り付けられる（例えば、リュック式構成において、ベルト結合式構成において）等、種々の構成において搭載されてもよい。

【０１５１】

フレーム１０１２は、フレーム１０１２に取り付けられ、または搭載され、装着者の眼の画像を取得する、１つまたはそれを上回るカメラを有することができる。一実施形態では、カメラは、眼が直接結像され得るように、装着者の眼の正面のフレーム１０１２に搭載されてもよい。他の実施形態では、カメラは、フレーム１０１２のステムに沿って（例えば、装着者の耳の近くに）搭載されることができる。そのような実施形態では、ディスプレイ１００８は、装着者の眼からの光をカメラに向かって反射させる、材料でコーティングされてもよい。光は、虹彩特徴が赤外線画像内で顕著であるため、赤外線光であってもよい。

【０１５２】

ローカル処理およびデータモジュール１０２４は、ハードウェアプロセッサと、不揮発性メモリ（例えば、フラッシュメモリ）等の非一過性デジタルメモリとを備えてもよく、その両方とも、データの処理、キャッシュ、および記憶を補助するために利用されてもよい。データは、（ａ）（例えば、フレーム１０１２に動作可能に結合される、または別様にユーザ１００４に取り付けられてもよい）、画像捕捉デバイス（カメラ等）、マイクロホン、慣性測定ユニット、加速度計、コンパス、ＧＰＳユニット、無線デバイス、またはジャイロスコープ等のセンサから捕捉されるデータ、または（ｂ）可能性として、処理もしくは読出後にディスプレイ１００８への通過のために、遠隔処理モジュール１０２８または遠隔データリポジトリ１０３２を使用して入手ならびには処理されるデータを含んでもよい。ローカル処理およびデータモジュール１０２４は、これらの遠隔モジュール１０２８、１０３２が、ローカル処理およびデータモジュール１０２４へのリソースとして利用可能であるように、有線または無線通信リンク等を介して、通信リンク１０３６または１０４０によって、遠隔処理モジュール１０２８および遠隔データリポジトリ１０３２に動作可能に結合されてもよい。画像捕捉デバイスは、眼画像処理プロシージャにおいて使用される眼画像を捕捉するために使用されることができる。加えて、遠隔処理モジュール１０２８および遠隔データリポジトリ１０３２は、相互に動作可能に結合されてもよい。

【０１５３】

いくつかの実施形態では、遠隔処理モジュール１０２８は、画像捕捉デバイスによって捕捉されたビデオ情報等のデータまたは画像情報を分析および処理するように構成される、１つまたはそれを上回るプロセッサを備えてもよい。ビデオデータは、ローカル処理およびデータモジュール１０２４内にローカルで、または遠隔データリポジトリ１０３２内に記憶されてもよい。いくつかの実施形態では、遠隔データリポジトリ１０３２は、デジ

タルデータ記憶設備を備えてもよく、これは、インターネットまたは「クラウド」リソース構成における他のネットワーキング構成を通して利用可能であってもよい。いくつかの実施形態では、全てのデータが、記憶され、全ての算出が、ローカル処理およびデータモジュール１０２４において実施され、遠隔モジュールからの完全に自律的な使用を可能にする。

【０１５４】

いくつかの実装では、ローカル処理およびデータモジュール１０２４または遠隔処理モジュール１０２８は、本明細書に説明されるようなシステムおよび方法の実施形態を実施するようにプログラムされる。画像捕捉デバイスは、特定の用途のためのビデオ（例えば、眼追跡用途のための装着者の眼のビデオまたはジェスチャ識別用途のための装着者の手もしくは指のビデオ）を捕捉することができる。ビデオは、処理モジュール１０２４、１０２８の一方または両方によって分析されることができる。ある場合には、虹彩コード生成のうちの少なくとも一部を（例えば、「クラウド」内の）遠隔処理モジュールにオフロードすることは、算出の効率または速度を改良し得る。本明細書に開示されるシステムおよび方法のパラメータは、データモジュール１０２４または１０２８内に記憶されることができる。

【０１５５】

分析の結果は、付加的動作または処理のために、処理モジュール１０２４、１０２８の一方または両方によって使用されることができる。例えば、種々の用途では、バイオメトリック識別、眼追跡、ジェスチャ、オブジェクト、姿勢の認識または分類等が、ウェアラブルディスプレイシステム１０００によって使用されてもよい。例えば、ウェアラブルディスプレイシステム１０００は、装着者１００４の手の捕捉されたビデオを分析し、装着者の手およびウェアラブルディスプレイシステムによるジェスチャを認識してもよい（例えば、実または仮想オブジェクトを取り上げる、合意または不合意（例えば、「サムズアップ」または「サムズダウン」）をシグナリングする等）。

【０１５６】

ヒト視覚系は、複雑であって、深度の現実的知覚を提供することは、困難である。理論によって限定されるわけではないが、オブジェクトの視認者は、輻輳・開散運動と遠近調節の組み合わせに起因して、オブジェクトを３次元として知覚し得ると考えられる。相互に対する２つの眼の輻輳・開散運動移動（例えば、眼の視線を収束させ、オブジェクトを固視するための相互に向かった、またはそこから離れる瞳孔の回転移動）は、眼の水晶体の合焦（または「遠近調節」）と緊密に関連付けられる。通常条件下、焦点を１つのオブジェクトから異なる距離における別のオブジェクトに変化させるための眼の水晶体の焦点の変化または眼の遠近調節は、「遠近調節－輻輳・開散運動反射」として知られる関係下、同一距離への輻輳・開散運動の合致する変化を自動的に生じさせるであろう。同様に、輻輳・開散運動の変化は、通常条件下、遠近調節の合致する変化を誘起するであろう。遠近調節と輻輳・開散運動との間のより良好な合致を提供するディスプレイシステムが、３次元画像のより現実的かつ快適なシミュレーションを形成し得る。

別の例示的ユーザデータトランザクションシステム

【０１５７】

図７Ｂは、ユーザデータトランザクションシステムの一実施形態を図式的に図示する。ユーザデータトランザクションシステムは、図１に説明されるユーザデータトランザクションシステム１００に類似することができる。エージェント（例えば、図１のエージェント１０６）および本開示の他のシステムおよびコンポーネントの使用を通して記憶ならびに実装される、プライバシ設定に基づいて、ユーザデータをセキュアに交換するためのシステムおよび方法は、１つまたはそれを上回るユーザデバイス７０２ａ－７０２ｃ（例えば、図１からのユーザデバイス１０２または購入者デバイス１０４もしくは図７Ａのウェアラブルディスプレイシステム１０００）、１つまたはそれを上回るエージェント７０６（例えば、図１からのエージェント１０６）、１つまたはそれを上回るデータプラットフォーム７１２（例えば、図１からのデータプラットフォーム１１２）、およびデータ仮想

化システム７１１（例えば、図１からのデータ仮想化システム１１１）によって実装されることができる。図７Ｂに示される非限定的例示的実施形態では、ユーザ７０１ａは、ユーザデバイス７０２ａおよび７０２ｂ（例えば、ユーザデバイス１０２は、そのようなデバイスを含むことができる）を動作させ、そのユーザプライバシ設定を作成および修正することができる。図７Ｂに示される非限定的例示的実施形態では、購入者７０１ｂは、ユーザデバイス７０２ｃを動作させ、ユーザ７０１ａまたは他のユーザと関連付けられる、ユーザデータを閲覧する、それと相互作用する、それに付加的データを付加する、およびそれを分析することができる。

【０１５８】

ユーザデバイス７０２ａ－７２０ｃは、例えば、セルラー電話、タブレットコンピュータ、電子リーダ、スマートウォッチ、頭部搭載型拡張、仮想、または複合現実ディスプレイシステム、ウェアラブルディスプレイシステム、図７Ａのウェアラブルディスプレイシステム１０００、または同等物を含むことができる。ユーザデバイス７０２ａ－ｃは、通信リンク１２０ａ、１２０ｂ、例えば、セルラー通信リンクまたはインターネット接続を使用して、ネットワーク７１８上で他のデバイスと通信することができる。ネットワーク７１８は、有線または無線通信リンクによってアクセス可能なローカルエリアネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、またはインターネットであって、例えば、米国電気電子学会（ＩＥＥＥ）８０２．１１規格を実装することができる。

【０１５９】

エージェント７０６は、通信リンク１２６を使用して、ネットワーク７１８上の他のデバイス、例えば、ユーザデバイス７０２ａおよび７０２ｂと通信することができる。データプラットフォーム７１２は、ネットワーク７１８上の他のデバイス、例えば、エージェント７０６と通信することができる。データ仮想化システム７１１は、ネットワーク７１８上の他のデバイス、例えば、エージェント７０６またはユーザデバイス７０２ｃと通信することができる。通信リンク１２０ａ、１２０ｂ、１２６、７２４、７２６、または７２８は、有線または無線通信、セルラー通信、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ローカルエリアネットワーク（ＬＡＮ）、広域ローカルエリアネットワーク（ＷＬＡＮ）、無線周波数（ＲＦ）、赤外線（ＩＲ）、もしくは任意の他の通信方法またはシステムであることができる。

【０１６０】

ユーザデバイス７０２ａおよび７０２ｂは、暗号化されたユーザデータをデータプラットフォーム７１２に伝送することができる。ユーザデバイス７０２ａおよび７０２ｂはまた、ユーザ７０１ａによって、分散型台帳（例えば、図１の分散型台帳１０８）を含み得る、エージェント７０６を介して、ユーザ７０１ａのプライバシ設定を構成または修正するために使用されることができる。購入者７０２ｂは、ユーザデバイス７０２ｃ（例えば、図１の購入者デバイス１０４）を使用して、データ仮想化システム７１１と通信し、データプラットフォーム上に記憶される暗号化されたユーザデータと相互作用することができる。

付加的実装詳細および実施形態

【０１６１】

本開示の種々の実施形態は、任意の可能性として考えられる技術的詳細レベルの統合における、システム、方法、またはコンピュータプログラム製品であってもよい。コンピュータプログラム製品は、プロセッサに本開示の側面を行わせるためのコンピュータ可読プログラム命令をその上に有する、コンピュータ可読記憶媒体（または複数の媒体）を含んでもよい。

【０１６２】

例えば、本明細書に説明される機能性は、ソフトウェア命令が、１つまたはそれを上回るハードウェアプロセッサもしくは任意の他の好適なコンピューティングデバイスによって実行される、ソフトウェア命令によって、またはそれに応答して実行されるにつれて、実施されてもよい。ソフトウェア命令または他の実行可能コードは、コンピュータ可読記

憶媒体（または複数の媒体）から読み取られてもよい。

【０１６３】

コンピュータ可読記憶媒体は、命令実行デバイスによる使用のためのデータまたは命令を留保および記憶し得る、有形デバイスであることができる。コンピュータ可読記憶媒体は、例えば、限定ではないが、電子記憶デバイス（任意の揮発性または不揮発性電子記憶デバイスを含む）、磁気記憶デバイス、光学記憶デバイス、電磁記憶デバイス、半導体記憶デバイス、または前述の任意の好適な組み合わせであってもよい。コンピュータ可読記憶媒体のより具体的実施例の非包括的リストは、以下、すなわち、ポータブルコンピュータディスケット、ハードディスク、ソリッドステートドライブ、ランダムアクセスメモリ（ＲＡＭ）、読取専用メモリ（ＲＯＭ）、消去可能プログラマブル読取専用メモリ（ＥＰＲＯＭまたはフラッシュメモリ）、静的ランダムアクセスメモリ（ＳＲＡＭ）、ポータブルコンパクトディスク読取専用メモリ（ＣＤ－ＲＯＭ）、デジタル多用途ディスク（ＤＶＤ）、メモリスティック、フロッピー（登録商標）ディスク、その上に記録される命令を有する、パンチカードまたは溝内の隆起構造等の機械的にエンコーディングされたデバイス、および前述の任意の好適な組み合わせを含む。本明細書で使用されるようなコンピュータ可読記憶媒体は、無線波または他の自由に伝搬する電磁波、導波管または他の伝送媒体を通して伝搬する電磁波、（例えば、光ファイバケーブルを通して通過する、光パルス）、もしくはワイヤを通して伝送される電気信号等、それ自体が、一過性信号であるものとして解釈されない。

【０１６４】

本明細書に説明されるコンピュータ可読プログラム命令は、個別のコンピューティング／処理デバイスに、コンピュータ可読記憶媒体または外部コンピュータもしくは外部記憶デバイスから、ネットワーク、例えば、インターネット、ローカルエリアネットワーク、広域ネットワーク、または無線ネットワークを介して、ダウンロードされることができる。ネットワークは、銅伝送ケーブル、光学伝送ファイバ、無線伝送、ルータ、ファイアウォール、スイッチ、ゲートウェイコンピュータ、またはエッジサーバを備えてもよい。各コンピューティング／処理デバイス内のネットワークアダプタカードまたはネットワークインターフェースは、コンピュータ可読プログラム命令をネットワークから受信し、個別のコンピューティング／処理デバイス内のコンピュータ可読記憶媒体の中への記憶のために、コンピュータ可読プログラム命令を転送する。

【０１６５】

本開示の動作を行うためのコンピュータ可読プログラム命令（本明細書では、例えば、「コード」、「命令」、「モジュール」、「アプリケーション」、「ソフトウェアアプリケーション」、または同等物とも称される）は、アセンブラ命令、命令セットアーキテクチャ（ＩＳＡ）命令、機械命令、機械依存命令、マイクロコード、ファームウェア命令、状態設定データ、集積回路網のための構成データ、またはＳｍａｌｌｔａｌｋ、Ｃ＋＋、もしくは同等物等のオブジェクト指向プログラミング言語、および「Ｃ」プログラミング言語または類似プログラミング言語等の手続型プログラミング言語を含む、１つまたはそれを上回るプログラミング言語の任意の組み合わせにおいて書き込まれる、ソースコードもしくはオブジェクトコードのいずれかであってもよい。コンピュータ可読プログラム命令は、他の命令から、またはそれ自体から呼出可能であってもよい、もしくは検出されたイベントまたはインタラプトに応答して呼び出されてもよい。コンピューティングデバイス上での実行のために構成される、コンピュータ可読プログラム命令は、コンピュータ可読記憶媒体上に、または、次いで、コンピュータ可読記憶媒体上に記憶され得る、デジタルダウンロードとして提供されてもよい（かつ、元々、実行に先立って、インストール、解凍、または解読を要求する、圧縮またはインストール可能フォーマットで記憶されてもよい）。そのようなコンピュータ可読プログラム命令は、部分的または完全に、コンピューティングデバイスによる実行のために、実行コンピューティングデバイスのメモリデバイス（例えば、コンピュータ可読記憶媒体）上に記憶されてもよい。コンピュータ可読プログラム命令は、完全に、ユーザのコンピュータ（例えば、実行コンピューティングデバ

イス）上で、部分的に、ユーザのコンピュータ上で、独立型ソフトウェアパッケージとして、部分的に、ユーザのコンピュータ上で、かつ部分的に、遠隔コンピュータ上で、または完全に、遠隔コンピュータもしくはサーバ上で実行されてもよい。後者のシナリオでは、遠隔コンピュータは、ローカルエリアネットワーク（ＬＡＮ）または広域ネットワーク（ＷＡＮ）を含む、任意のタイプのネットワークを通して、ユーザのコンピュータに接続されてもよい、または接続は、外部コンピュータに行われてもよい（例えば、インターネットサービスプロバイダを使用して、インターネットを通して）。いくつかの実施形態では、例えば、プログラマブル論理回路網、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）、またはプログラマブル論理アレイ（ＰＬＡ）を含む、電子回路網は、本開示の側面を実施するために、コンピュータ可読プログラム命令の状態情報を利用して、電子回路網を個人化することによって、コンピュータ可読プログラム命令を実行してもよい。

【０１６６】

本開示の側面は、本開示の実施形態による、方法、装置（システム）、およびコンピュータプログラム製品のフローチャート図またはブロック図を参照して本明細書に説明される。フローチャート図またはブロック図の各ブロックおよびフローチャート図またはブロック図内のブロックの組み合わせは、コンピュータ可読プログラム命令によって実装されることができることを理解されたい。

【０１６７】

これらのコンピュータ可読プログラム命令は、コンピュータまたは他のプログラマブルデータ処理装置のプロセッサを介して実行される命令が、フローチャートまたはブロック図ブロックもしくは複数のブロック内に規定された機能／行為を実装するための手段を作成するように、汎用コンピュータ、特殊目的コンピュータ、または他のプログラマブルデータ処理装置のプロセッサに提供され、機械を生産してもよい。これらのコンピュータ可読プログラム命令はまた、その中に記憶される命令を有するコンピュータ可読記憶媒体が、フローチャートまたはブロック図ブロックもしくは複数のブロック内に規定された機能／行為の側面を実装する、命令を含む、製造品を備えるように、コンピュータ、プログラマブルデータ処理装置、または他のデバイスに、特定の様式において機能するように指示し得る、コンピュータ可読記憶媒体内に記憶されてもよい。

【０１６８】

コンピュータ可読プログラム命令はまた、コンピュータ、他のプログラマブル装置、または他のデバイス上で実行される命令が、フローチャートまたはブロックもしくは複数のブロック内に規定された機能／行為を実装するように、コンピュータ、他のプログラマブルデータ処理装置、または他のデバイス上にロードされ、一連の動作ステップをコンピュータ、他のプログラマブル装置、または他のデバイス上で実施させ、コンピュータ実装プロセスを生産してもよい。例えば、命令は、最初に、遠隔コンピュータの磁気ディスクまたはソリッドステートドライブ上で搬送されてもよい。遠隔コンピュータは、命令またはモジュールを遠隔コンピュータの動的メモリの中にロードし、モデムを使用して、電話、ケーブル、または光学ラインを経由して、命令を送信してもよい。サーバコンピューティングシステムにローカルのモデムは、データを電話／ケーブル／光学ライン上で受信し、適切な回路網を含む、コンバータデバイスを使用して、データをバス上に設置してもよい。バスは、データをメモリに搬送してもよく、そこからプロセッサは、命令を読み出し、実行してもよい。メモリによって受信された命令は、随意に、コンピュータプロセッサによる実行の前または後のいずれかにおいて、記憶デバイス（例えば、ソリッドステートドライブ）上に記憶されてもよい。

【０１６９】

図中のフローチャートおよびブロック図は、本開示の種々の実施形態による、システム、方法、およびコンピュータプログラム製品の可能性として考えられる実装のアーキテクチャ、機能性、および動作を図示する。本点では、フローチャートまたはブロック図内の各ブロックは、規定された論理機能を実装するための１つまたはそれを上回る実行可能命令を備える、命令のモジュール、セグメント、または一部を表し得る。いくつかの代替実

装では、ブロック内に記載される機能は、図中に記載の順序外で生じてもよい。例えば、連続して示される２つのブロックは、実際は、実質的に並行して実行されてもよい、またはブロックは、時として、関わる機能性に応じて、逆順で実行されてもよい。加えて、あるブロックは、いくつかの実装では、省略されてもよい。本明細書に説明される方法およびプロセスは、また、いずれの特定のシーケンスにも限定されず、それに関連するブロックまたは状態は、適切な他のシーケンスで実施されることができる。

【０１７０】

したがって、動作は、特定の順序において図面に描写され得るが、そのような動作は、示される特定の順序または順次順序で実施される、または全ての図示される動作が、望ましい結果を達成するために実施される必要はないことを認識されたい。さらに、図面は、フローチャートの形態における１つまたはそれを上回る例示的プロセスを図式的に描写し得る。しかしながら、描写されない他の動作も、図式的に図示される、例示的方法およびプロセス内に組み込まれることができる。例えば、１つまたはそれを上回る付加的動作が、図示される動作のいずれかの前、後、それと同時に、またはその間に実施されることができる。加えて、動作は、他の実装では、再配列される、または並べ替えられてもよい。ある状況では、マルチタスクおよび並列処理が、有利であり得る。さらに、上記に説明される実装における種々のシステムコンポーネントの分離は、そのような分離を全ての実装において要求するものと理解されるべきではなく、説明されるプログラムコンポーネントおよびシステムは、概して、単一ソフトウェア製品内にともに統合される、または複数のソフトウェア製品の中にパッケージ化されることができることを理解されたい。加えて、他の実装も、以下の請求項の範囲内である。ある場合には、請求項に列挙されるアクションは、異なる順序で実施され、依然として、望ましい結果を達成することができる。

【０１７１】

また、ブロック図またはフローチャート図の各ブロックおよびブロック図またはフローチャート図内のブロックの組み合わせは、規定された機能または行為を実施する、もしくは特殊目的ハードウェアおよびコンピュータ命令の組み合わせを行う、特殊目的ハードウェアベースのシステムによって実装されることができることに留意されたい。例えば、前節に説明されるプロセス、方法、アルゴリズム、要素、ブロック、アプリケーション、または他の機能性（または機能性の一部）のいずれかは、特定用途向けプロセッサ（例えば、特定用途向け集積回路（ＡＳＩＣ））、プログラマブルプロセッサ（例えば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ））、特定用途向け回路網、または同等物（そのいずれかはまた、本技法を遂行するためのソフトウェア命令のカスタムプログラミング／実行を用いることで、カスタム有線論理、論理回路、ＡＳＩＣ、ＦＰＧＡ等を組み合わせ得る）等の電子ハードウェア内に具現化される、または完全もしくは部分的に、それを介して自動化されてもよい。

【０１７２】

上記に述べられたプロセッサまたはデバイスのいずれかは、本明細書では、例えば、「コンピュータ」、「コンピュータデバイス」、「コンピューティングデバイス」、「ハードウェアコンピューティングデバイス」、「ハードウェアプロセッサ」、「処理ユニット」、または同等物と称され得る、上記に述べられたプロセッサのいずれかを組み込む。上記に実施形態のコンピューティングデバイスは、概して（必ずしもではないが）、ＭａｃＯＳ、ｉＯＳ、Ａｎｄｒｏｉｄ、Ｃｈｒｏｍｅ ＯＳ、Ｗｉｎｄｏｗｓ（登録商標） ＯＳ（例えば、Ｗｉｎｄｏｗｓ（登録商標） ＸＰ、Ｗｉｎｄｏｗｓ（登録商標） Ｖｉｓｔａ、Ｗｉｎｄｏｗｓ（登録商標）７、Ｗｉｎｄｏｗｓ（登録商標）８、Ｗｉｎｄｏｗｓ（登録商標）１０、Ｗｉｎｄｏｗｓ（登録商標） Ｓｅｒｖｅｒ等）、Ｗｉｎｄｏｗｓ（登録商標） ＣＥ、Ｕｎｉｘ（登録商標）、Ｌｉｎｕｘ（登録商標）、ＳｕｎＯＳ、Ｓｏｌａｒｉｓ、Ｂｌａｃｋｂｅｒｒｙ ＯＳ、ＶｘＷｏｒｋｓ、または他の好適なオペレーティングシステム等のオペレーティングシステムソフトウェアによって制御または協調されてもよい。他の実施形態では、コンピューティングデバイスは、専有オペレーティングシステムによって制御されてもよい。従来のオペレーティングシステムは、とりわけ、実行の

ためのコンピュータプロセスを制御およびスケジュールし、メモリ管理を実施し、ファイルシステム、ネットワーキング、Ｉ／Ｏサービスを提供し、グラフィカルユーザインターフェース（「ＧＵＩ」）等のユーザインターフェース機能性を提供する。

【０１７３】

例えば、図８は、その上に種々の実施形態が実装され得る、コンピュータシステム８００を図示する、ブロック図である。そのようなコンピュータシステム８００は、本明細書に説明されるようなエージェント、分散型台帳、ユーザデバイス、データプラットフォーム、またはデータ仮想化システムの一部を含むことができる。コンピュータシステム８００は、図７Ｂを参照して説明されるシステムを実装するために使用されることができる。コンピュータシステム８００は、情報を通信するためのバス８０２または他の通信機構と、情報を処理するためにバス８０２と結合される、ハードウェアプロセッサまたは複数のプロセッサ８０４とを含む。ハードウェアプロセッサ８０４は、例えば、１つまたはそれを上回る汎用マイクロプロセッサであってもよい。

【０１７４】

コンピュータシステム８００はまた、プロセッサ８０４によって実行されるための情報および命令を記憶するためにバス８０２に結合される、ランダムアクセスメモリ（ＲＡＭ）、キャッシュ、または他の動的記憶デバイス等のメインメモリ８０６を含む。メインメモリ８０６はまた、プロセッサ８０４によって実行されるための命令の実行の間、一時的変数または他の中間情報を記憶するために使用されてもよい。そのような命令は、プロセッサ８０４にアクセス可能な記憶媒体内に記憶されると、コンピュータシステム８００を、命令内に規定された動作を実施するようにカスタマイズされる、特殊目的機械の中にレンダリングする。

【０１７５】

コンピュータシステム８００はさらに、プロセッサ８０４のための静的情報および命令を記憶するためにバス８０２に結合される、読取専用メモリ（ＲＯＭ）８０８または他の静的記憶デバイスを含む。磁気ディスク、光ディスク、またはＵＳＢサムドライブ（フラッシュドライブ）等の記憶デバイス８１０が、情報および命令を記憶するために提供され、バス８０２に結合される。

【０１７６】

コンピュータシステム８００は、情報をコンピュータユーザに表示するために、バス８０２を介して、陰極線管（ＣＲＴ）またはＬＣＤディスプレイ（またはタッチスクリーン）等のディスプレイ８１２に結合されてもよい。コンピュータシステム８００は、バス８０２またはネットワークリンク８２０を介して、例えば、ユーザデバイス１０２、１０４、７０２ａ－７０２ｃ、１０００等の拡張、複合、または仮想現実ディスプレイデバイスを含み得る、ユーザデバイス８２４に結合されてもよい。さらに、コンピュータシステム８００自体もまた、例えば、ユーザデバイス１０２、１０４、７０２ａ－７０２ｃ、１０００等の拡張、複合、または仮想現実ディスプレイデバイスを含んでもよい。英数字および他のキーを含む、入力デバイス８１４が、情報およびコマンド選択をプロセッサ８０４に通信するために、バス８０２に結合される。別のタイプのユーザ入力デバイスは、方向情報およびコマンド選択をプロセッサ８０４に通信するための、かつディスプレイ８１２上のカーソル移動を制御するための、マウス、トラックボール、またはカーソル方向キー等のカーソル制御８１６である。本入力デバイスは、典型的には、デバイスが平面内の位置を規定することを可能にする、２つの軸、すなわち、第１の軸（例えば、ｘ）および第２の軸（例えば、ｙ）における２自由度を有する。いくつかの実施形態では、カーソル制御と同一方向情報およびコマンド選択は、カーソルを伴わずに、タッチスクリーン上でタッチを受信することを介して、実装されてもよい。

【０１７７】

コンピューティングシステム８００は、ユーザインターフェースモジュールを含み、コンピューティングデバイスによって実行されるコンピュータ実行可能プログラム命令として、大容量記憶デバイス内に記憶され得る、ＧＵＩを実装してもよい。コンピュータシス

テム８００はさらに、下記に説明されるように、コンピュータシステムと組み合わせて、プログラムコンピュータシステム８００を特殊目的機械であるようにさせる、またはプログラムする、カスタマイズされた有線論理、１つまたはそれを上回るＡＳＩＣまたはＦＰＧＡ、ファームウェアまたはプログラム論理を使用して、本明細書に説明される技法を実装してもよい。一実施形態によると、本明細書の技法は、プロセッサ８０４が、メインメモリ８０６内に含有される１つまたはそれを上回るコンピュータ可読プログラム命令の１つまたはそれを上回るシーケンスを実行することに応答して、コンピュータシステム８００によって実施される。そのような命令は、メインメモリ８０６の中に、記憶デバイス８１０等の別の記憶媒体から読み込まれてもよい。メインメモリ８０６内に含有される命令のシーケンスの実行は、プロセッサ８０４に、本明細書に説明されるプロセスステップを実施させる。代替実施形態では、有線回路網が、ソフトウェア命令の代わりに、またはそれと組み合わせて、使用されてもよい。

【０１７８】

種々の形態のコンピュータ可読記憶媒体が、実行のために、１つまたはそれを上回るコンピュータ可読プログラム命令の１つまたはそれを上回るシーケンスをプロセッサ８０４に搬送する際に関わってもよい。例えば、命令は、最初に、遠隔コンピュータの磁気ディスクまたはソリッドステートドライブ上で搬送されてもよい。遠隔コンピュータは、命令を遠隔コンピュータの動的メモリの中にロードし、モデムを使用して、電話回線を経由して、命令を送信することができる。コンピュータシステム８００にローカルのモデムは、データを電話回線上で受信し、赤外線伝送機を使用して、データを赤外線信号に変換することができる。赤外線検出器は、赤外線信号内で搬送されるデータを受信することができ、適切な回路網は、データをバス８０２上に設置することができる。バス８０２は、データをメインメモリ８０６に搬送し、そこからプロセッサ８０４は、命令を読み出し、実行する。メインメモリ８０６によって受信された命令は、随意に、プロセッサ８０４による実行の前または後のいずれかにおいて、記憶デバイス８１０上に記憶されてもよい。

【０１７９】

コンピュータシステム８００はまた、バス８０２に結合される、通信インターフェース８１８を含む。通信インターフェース８１８は、ローカルネットワーク８２２に接続される、ネットワークリンク８２０に結合する、双方向データ通信を提供する。例えば、通信インターフェース８１８は、統合されたサービスデジタルネットワーク（ＩＳＤＮ）カード、ケーブルモデム、衛星モデム、またはモデムであって、データ通信接続を対応するタイプの電話回線に提供してもよい。別の実施例として、通信インターフェース８１８は、ローカルエリアネットワーク（ＬＡＮ）カードであって、データ通信接続を互換性があるＬＡＮ（またはＷＡＮと通信するためのＷＡＮコンポーネント）に提供してもよい。無線リンクもまた、実装されてもよい。任意のそのような実装では、通信インターフェース８１８は、種々のタイプの情報を表す、デジタルデータストリームを搬送する、電気、電磁、または光学信号を送信および受信する。

【０１８０】

ネットワークリンク８２０は、典型的には、データ通信を、１つまたはそれを上回るネットワークを通して、他のデータデバイスに提供する。例えば、ネットワークリンク８２０はローカルネットワーク８２２を通して、インターネットサービスプロバイダ（ＩＳＰ）８２６によって動作される、ユーザデバイス８２４またはデータ機器への接続を提供してもよい。ＩＳＰ８２６は、ひいては、本明細書では、一般に、「インターネット」８２８と称される、世界中のパケットデータ通信ネットワークを通して、データ通信サービスを提供する。ローカルネットワーク８２２およびインターネット８２８は両方とも、デジタルデータストリームを搬送する、電気、電磁、または光学信号を使用する。デジタルデータをコンピュータシステム８００におよびそこから搬送する、種々のネットワークを通した信号ならびにネットワークリンク８２０上および通信インターフェース８１８を通した信号は、伝送媒体の例示的形態である。

【０１８１】

コンピュータシステム８００は、ネットワーク、ネットワークリンク８２０、および通信インターフェース８１８を通して、メッセージを送信し、プログラムコードを含む、データを受信することができる。インターネット実施例では、サーバ８３０は、インターネット８２８、Ｐ８２６、ローカルネットワーク８２２、および通信インターフェース８１８を通して、アプリケーションプログラムのために要求されるコードを伝送し得る。例えば、サーバ８３０は、ユーザのデータトランザクションシステム１００、データ可視化システム１１１、エージェント１０６、データプラットフォーム１１２、またはユーザデータプライバシシステム１０３のうちのいくつかまたは全てを含んでもよい。

【０１８２】

受信されたコードは、受信されるにつれて、プロセッサ８０４によって実行される、または後の実行のために、記憶デバイス８１０または他の不揮発性記憶装置内に記憶されてもよい。

付加的考慮点

【０１８３】

上記に説明されるように、種々の実施形態では、ある機能性は、ウェブベースのビューア（ウェブブラウザ等）または他の好適なソフトウェアプログラムを通して、ユーザによってアクセス可能であってもよい。そのような実装では、ユーザインターフェースは、サーバコンピューティングシステムによって生成され、（例えば、ユーザのコンピューティングシステム上で起動する）ユーザのウェブブラウザに伝送されてもよい。代替として、ユーザインターフェースを生成するために必要なデータ（例えば、ユーザインターフェースデータ）は、サーバコンピューティングシステムによって、ユーザインターフェースが生成され得る、ブラウザに提供されてもよい（例えば、ユーザインターフェースデータは、ブラウザがウェブサービスにアクセスすることによって実行されてもよく、ユーザインターフェースデータに基づいて、ユーザインターフェースをレンダリングするように構成されてもよい）。ユーザは、次いで、ウェブ－ブラウザを通して、ユーザインターフェースと相互作用してもよい。ある実装のユーザインターフェースは、１つまたはそれを上回る専用ソフトウェアアプリケーションを通してアクセス可能であってもよい。ある実施形態では、本開示のコンピューティングデバイスまたはシステムのうちの１つまたはそれを上回るものは、モバイルコンピューティングデバイスを含んでもよく、ユーザインターフェースは、そのようなモバイルコンピューティングデバイス（例えば、スマートフォンまたはタブレット）を通してアクセス可能であってもよい。

【０１８４】

いくつかの実施形態では、データは、必要に応じて、チャートおよびグラフ等の視覚的表現等のグラフィカル表現内に提示され、ユーザが、大量のデータを快適に精査し、視覚的刺激に関連するヒトの特に高いパターン認識能力を利用することを可能にしてもよい。いくつかの実施形態では、本システムは、合計、計数、および平均等の集計量を提示してもよい。本システムはまた、情報を利用して、将来的展開を補間または外挿、例えば、予想してもよい。

【０１８５】

さらに、本明細書に説明される双方向かつ動的ユーザインターフェースは、ユーザインターフェースと下層システムおよびコンポーネントとの間の効率的相互作用における革新によって可能にされる。例えば、本明細書に開示されるものは、ユーザ入力の受信、種々のシステムコンポーネントへのそれらの入力の変換および送達、入力送達に応答した複雑なプロセスの自動および動的実行、本システムの種々のコンポーネントおよびプロセス間の自動相互作用、ならびにユーザインターフェースの自動および動的更新の改良された方法である。本明細書に説明される双方向ユーザインターフェースを介したデータの相互作用および提示は、故に、以前のシステムに優る認知および人間工学的効率ならびに利点を提供し得る。

【０１８６】

本開示の種々の実施形態は、改良を種々の技術および技術分野に提供する。例えば、上

記に説明されるように、既存のデータ記憶装置および処理技術（例えば、メモリデータベース内を含む）は、種々の点において限定され（例えば、手動データ精査は、低速であって、コストがかかり、かつあまり詳細ではない、データは、非常に膨大である等）、本開示の種々の実施形態は、そのような技術に優る有意な改良を提供する。加えて、本開示の種々の実施形態は、コンピュータ技術に分離不可能に結び付けられる。特に、種々の実施形態は、グラフィカルユーザインターフェースを介したユーザ入力の検出、それらのユーザ入力に基づく表示される電子データの更新の計算、関連電子データの自動処理、および双方向グラフィカルユーザインターフェースを介した表示される画像の更新の提示に依拠する。そのような特徴およびその他（例えば、大量の電子データの処理および分析）は、コンピュータ技術に密接に結び付けられ、それによって可能にされ、コンピュータ技術がなければ、存在しないであろう。例えば、種々の実施形態を参照して下記に説明される表示されるデータとの相互作用は、その上にそれらが実装される、コンピュータ技術を伴わずに、ヒト単独によっては、合理的に実施されることができない。さらに、コンピュータ技術を介した本開示の種々の実施形態の実装は、種々のタイプの電子データとのより効率的相互作用およびその提示を含む、本明細書に説明される利点の多くを可能にする。

【０１８７】

種々の実施形態では、それを用いて具現化されるプログラム命令を有する、コンピュータ可読記憶媒体と、プログラム命令を実行し、１つまたはそれを上回るプロセッサに、上記または下記に説明される実施形態の１つまたはそれを上回る側面（添付の請求項の１つまたはそれを上回る側面を含む）を備える、動作を実施させるように構成される、１つまたはそれを上回るプロセッサとを備える、システムまたはコンピュータシステムが、開示される。

【０１８８】

種々の実施形態では、コンピュータ可読記憶媒体を備える、コンピュータプログラム製品が、開示され、コンピュータ可読記憶媒体は、それを用いて具現化される、プログラム命令を備え、プログラム命令は、１つまたはそれを上回るプロセッサに、上記および／または下記に説明される実施形態の１つまたはそれを上回る側面（添付の請求項の１つまたはそれを上回る側面を含む）を備える、動作を実施させるために１つまたはそれを上回るプロセッサによって実行可能である。

【０１８９】

多くの変形例および修正が、上記に説明される実施形態に行われてもよく、その要素は、他の容認可能実施例に該当すると理解される。全てのそのような修正および変形例は、本開示の範囲内の本明細書に含まれるように意図される。前述の説明は、ある実施形態を詳述する。しかしながら、文書中に現れる前述の詳細度にかかわらず、本システムおよび方法は、多くの方法において実践されることができることを理解されたい。また、上記に述べられるように、本システムおよび方法のある特徴または側面を説明するときの特定の専門用語の使用は、専門用語が、それとその専門用語が関連付けられる、本システムおよび方法の特徴または側面の任意の具体的特性を含むように制限されるように本明細書に再定義されることを含意すると捉えられるべきではないことに留意されたい。

【０１９０】

とりわけ、「～できる（ｃａｎ）」、「～し得る（ｃｏｕｌｄ）」、「～し得る（ｍｉｇｈｔ）」、または「～し得る（ｍａｙ）」等の条件文は、別様に具体的に記載されない限り、または使用されるような文脈内で別様に理解されない限り、概して、ある実施形態がある特徴、要素、および／またはステップを含む一方、他の実施形態がそれらを含まないことを伝えることが意図される。したがって、そのような条件文は、概して、特徴、要素、および／またはステップが、１つまたはそれを上回る実施形態に対していかようにも要求されること、もしくは１つまたはそれを上回る実施形態実施形態が、著者の入力もしくは促しの有無を問わず、これらの特徴、要素、および／またはステップが任意の特定の実施形態において含まれる、もしくは実施されるべきかどうかを決定するための論理を必然的に含むことを含意することを意図されない。

【０１９１】
本明細書で使用されるような用語「コンポーネント」、「エージェント」、「モジュール」、「デバイス」、「機構」、「ユニット」、「要素」、「部材」、「装置」、「機械」、「プロセッサ」、または「システム」は、手段プラス機能請求項用語を想定するものと解釈されるべきではない。例えば、そのような用語を用いて説明される要素は、特殊または特定のプログラミングの使用または適用を伴わずに、用語と関連付けられる任意の請求される動作を実施することが可能であるものとして解釈されるべきである。
【０１９２】
用語「実質的に」は、用語「リアルタイム」と併用されるとき、当業者によって容易に理解されるであろう、語句を形成する。例えば、そのような言語は、遅延または待機を全くもしくは殆ど判別可能ではない、またはそのような遅延が、混乱、苛立ち、もしくは別様に当惑をユーザにもたらないほど十分に短い、速度を含むであろうことが、容易に理解される。
【０１９３】
語句「Ｘ、Ｙ、およびＺのうちの少なくとも１つ」または「Ｘ、Ｙ、またはＺのうちの少なくとも１つ」等の接続的用語は、別様に具体的に述べられない限り、一般に、アイテム、用語等が、Ｘ、Ｙ、またはＺのいずれか、もしくはそれらの組み合わせであり得ることを伝達するために使用されるものとして、コンテキストとともに理解されるべきである。例えば、用語「または」は、例えば、要素のリストを接続するために使用されるとき、用語「または」が、リスト内の要素のうちの１つ、いくつか、または全てを意味するように、その包含的意味（かつその排他的意味ではなく）で使用される。したがって、そのような接続的用語は、概して、ある実施形態が、Ｘのうちの少なくとも１つ、Ｙのうちの少なくとも１つ、およびＺのうちの少なくとも１つがそれぞれ存在することを要求することを含意するように意図するものではない。
【０１９４】
本明細書および添付の請求項で使用されるような用語「ａ」は、排他的解釈ではなく、包含的解釈を与えられるべきである。例えば、具体的に記載されない限り、用語「ａ」は、「正確に１つ」または「１つかつ１つのみ」を意味するものと理解されるべきではなく、代わりに、用語「ａ」は、請求項または本明細書のいずれかの場所内で使用されるかどうかにかかわらず、かつ請求項または本明細書内のいずれの場所の「少なくとも１つ」、「１つまたはそれを上回る」、または「複数の」等の数量詞請の使用にかかわらず、「１つまたはそれを上回る」もしくは「少なくとも１つ」を意味する。
【０１９５】
とりわけ、「～できる（ｃａｎ）」、「～し得る（ｃｏｕｌｄ）」、「～し得る（ｍｉｇｈｔ）」、「～し得る（ｍａｙ）」、「例えば（ｅ．ｇ．）」、および同等物等、本明細書で使用される条件文は、別様に具体的に記載されない限り、または使用されるような文脈内で別様に理解されない限り、概して、ある実施形態がある特徴、要素、および／またはステップを含む一方、他の実施形態がそれらを含まないことを伝えることが意図される。したがって、そのような条件文は、概して、特徴、要素、および／またはステップが、１つまたはそれを上回る実施形態に対していかようにも要求されること、もしくは１つまたはそれを上回る実施形態が、著者の入力または促しの有無を問わず、これらの特徴、要素、および／またはステップが任意の特定の実施形態において含まれる、もしくは実施されるべきかどうかを決定するための論理を必然的に含むことを含意することを意図されない。用語「～を備える（ｃｏｍｐｒｉｓｉｎｇ）」、「～を含む（ｉｎｃｌｕｄｉｎｇ）」、「～を有する（ｈａｖｉｎｇ）」、および同等物は、同義語であり、非限定的方式で包括的に使用され、付加的要素、特徴、行為、動作等を除外しない。例えば、１つまたはそれを上回るプロセッサを備える、汎用コンピュータは、他のコンピュータコンポーネントを除外するものとして解釈されるべきではなく、可能性として、とりわけ、メモリ、入／出力デバイス、および／またはネットワークインターフェース等のコンポーネントを含んでもよい。

【０１９６】
上記の詳細な説明は、種々の実施形態に適用されるような新規特徴を図示、説明、および指摘しているが、図示されるデバイスまたはプロセスの形態および詳細の種々の省略、代用、ならびに変更が、本開示の精神から逸脱することなく行われてもよいことを理解されたい。認識され得るように、本明細書に説明される本発明のある実施形態は、本明細書に記載される特徴および利点の全てを提供しない、形態内に具現化されてもよく、いくつかの特徴は、その他と別個に使用または実践されてもよい。本明細書に開示されるある発明の範囲は、前述の説明によってではなく、添付の請求項によって示される。請求項の等価性の意味および範囲内に該当する、全ての変更は、その範囲内に包含されるべきである。
【０１９７】
本明細書に説明される、ならびに／または添付される図に描写されるプロセス、方法、およびアルゴリズムはそれぞれ、具体的かつ特定のコンピュータ命令を実行するように構成される、１つまたはそれを上回る物理的コンピューティングシステム、ハードウェアコンピュータプロセッサ、特定用途向け回路、および／または電子ハードウェアによって実行される、コードモジュールにおいて具現化され、それによって完全もしくは部分的に自動化され得る。例えば、コンピューティングシステムは、具体的コンピュータ命令とともにプログラムされた汎用コンピュータ（例えば、サーバ）または専用コンピュータ、専用回路等を含むことができる。コードモジュールは、実行可能プログラムにコンパイルおよびリンクされる、動的リンクライブラリ内にインストールされ得る、またはインタープリタ型プログラミング言語において書き込まれ得る。いくつかの実装では、特定の動作および方法が、所与の機能に特有の回路によって実施され得る。
【０１９８】
さらに、本開示の機能性のある実装は、十分に数学的、コンピュータ的、または技術的に複雑であるため、（適切な特殊化された実行可能命令を利用する）特定用途向けハードウェアもしくは１つまたはそれを上回る物理的コンピューティングデバイスは、例えば、関与する計算の量もしくは複雑性に起因して、または結果を実質的にリアルタイムで提供するために、機能性を実施する必要があり得る。例えば、ビデオは、多くのフレームを含み、各フレームは、数百万のピクセルを有し得、具体的にプログラムされたコンピュータハードウェアは、商業的に妥当な時間量において所望の画像処理タスクまたは用途を提供するようにビデオデータを処理する必要がある。
【０１９９】
コードモジュールまたは任意のタイプのデータは、ハードドライブ、ソリッドステートメモリ、ランダムアクセスメモリ（ＲＡＭ）、読取専用メモリ（ＲＯＭ）、光学ディスク、揮発性もしくは不揮発性記憶装置、同一物の組み合わせ、および／または同等物を含む、物理的コンピュータ記憶装置等の任意のタイプの非一過性コンピュータ可読媒体上に記憶され得る。本方法およびモジュール（またはデータ）はまた、無線ベースおよび有線／ケーブルベースの媒体を含む、種々のコンピュータ可読伝送媒体上で生成されたデータ信号として（例えば、搬送波または他のアナログもしくはデジタル伝搬信号の一部として）伝送され得、種々の形態（例えば、単一もしくは多重化アナログ信号の一部として、または複数の離散デジタルパケットもしくはフレームとして）をとり得る。開示されるプロセスまたはプロセスステップの結果は、任意のタイプの非一過性有形コンピュータ記憶装置内に持続的もしくは別様に記憶され得る、またはコンピュータ可読伝送媒体を介して通信され得る。
【０２００】
本明細書に説明される、および／または添付される図に描写されるフロー図における任意のプロセス、ブロック、状態、ステップ、もしくは機能性は、プロセスにおいて具体的機能（例えば、論理もしくは算術）またはステップを実装するための１つまたはそれを上回る実行可能命令を含む、コードモジュール、セグメント、またはコードの一部を潜在的に表すものとして理解されたい。種々のプロセス、ブロック、状態、ステップ、または機能性は、組み合わせられる、再配列される、本明細書に提供される例証的実施例に追加さ

れる、そこから削除される、修正される、または別様にそこから変更されることができる。いくつかの実施形態では、付加的または異なるコンピューティングシステムもしくはコードモジュールが、本明細書に説明される機能性のいくつかまたは全てを実施し得る。本明細書に説明される方法およびプロセスはまた、いずれの特定のシーケンスにも限定されず、それに関連するブロック、ステップ、または状態は、適切な他のシーケンスで、例えば、連続して、並行して、またはある他の様式で実施されることができる。タスクまたはイベントが、開示される例示的実施形態に追加される、またはそこから除去され得る。さらに、本明細書に説明される実装における種々のシステムコンポーネントの分離は、例証目的のためであり、全ての実装においてそのような分離を要求するものとして理解されるべきではない。説明されるプログラムコンポーネント、方法、およびシステムは、概して、単一のコンピュータ製品においてともに統合される、または複数のコンピュータ製品にパッケージ化され得ることを理解されたい。多くの実装変形例が、可能である。

【０２０１】

本プロセス、方法、およびシステムは、ネットワーク（または分散）コンピューティング環境において実装され得る。ネットワーク環境は、企業全体コンピュータネットワーク、イントラネット、ローカルエリアネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、パーソナルエリアネットワーク（ＰＡＮ）、クラウドコンピューティングネットワーク、クラウドソースコンピューティングネットワーク、インターネット、およびワールドワイドウェブを含む。ネットワークは、有線もしくは無線ネットワークまたは任意の他のタイプの通信ネットワークであり得る。

【０２０２】

本開示のシステムおよび方法は、それぞれ、いくつかの革新的側面を有し、そのうちのいかなるものも、本明細書に開示される望ましい属性に単独で関与しない、またはそのために要求されない。本明細書に説明される種々の特徴およびプロセスは、相互に独立して使用され得る、または種々の方法で組み合わせられ得る。全ての可能性として考えられる組み合わせおよび副次的組み合わせが、本開示の範囲内に該当することが意図される。本開示に説明される実装の種々の修正が、当業者に容易に明白であり得、本明細書に定義される一般原理は、本開示の精神または範囲から逸脱することなく、他の実装に適用され得る。したがって、請求項は、本明細書に示される実装に限定されることを意図されず、本明細書に開示される本開示、原理、および新規の特徴と一貫する最も広い範囲を与えられるべきである。

【０２０３】

別個の実装の文脈において本明細書に説明されるある特徴はまた、単一の実装における組み合わせにおいて実装されることができる。逆に、単一の実装の文脈において説明される種々の特徴もまた、複数の実装において別個に、または任意の好適な副次的組み合わせにおいて実装されることができる。さらに、特徴がある組み合わせにおいて作用するものとして上記に説明され、さらに、そのようなものとして最初に請求され得るが、請求される組み合わせからの１つまたはそれを上回る特徴は、いくつかの場合では、組み合わせから削除されることができ、請求される組み合わせは、副次的組み合わせまたは副次的組み合わせの変形例を対象とし得る。いかなる単一の特徴または特徴の群も、あらゆる実施形態に必要もしくは必須ではない。

【図面】

【図１】

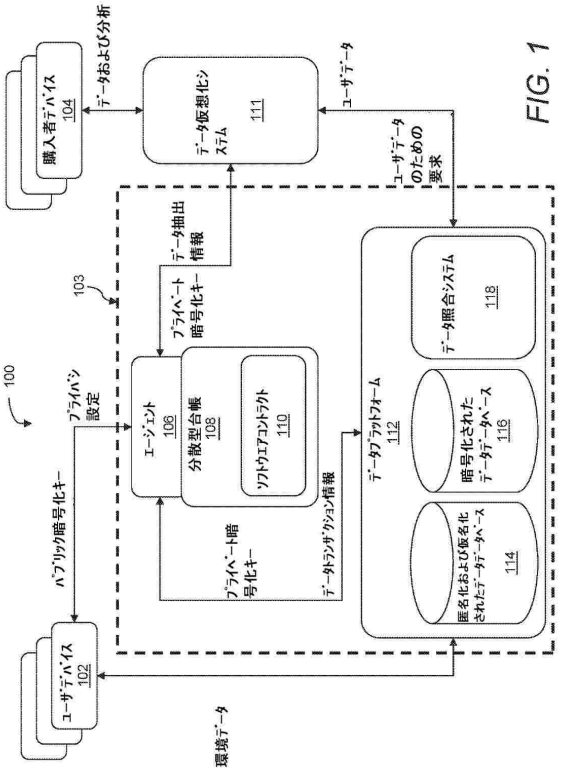

FIG. 1

【図２Ａ】

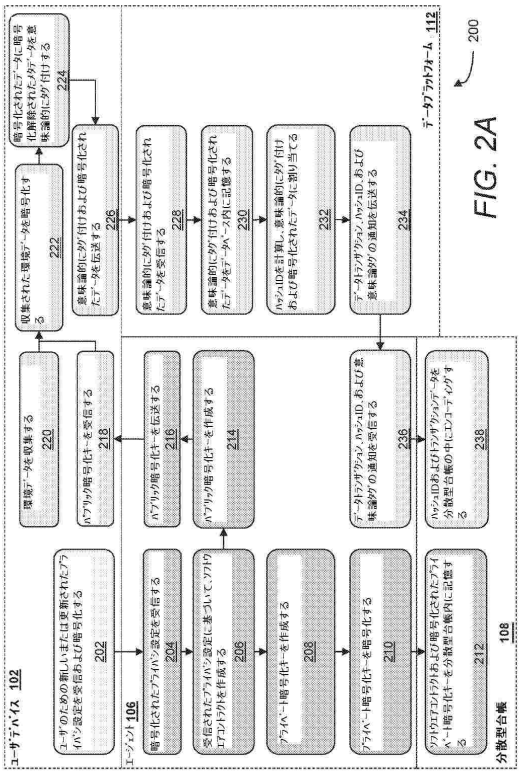

FIG. 2A

【図２Ｂ】

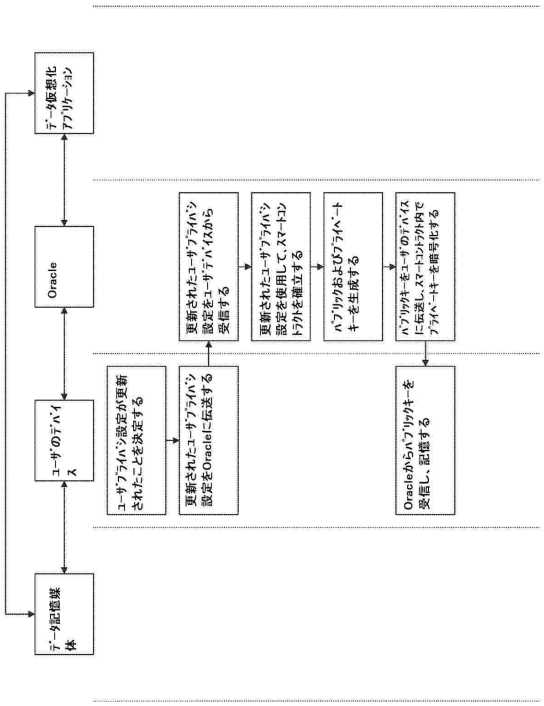

FIG. 2B

【図２Ｃ】

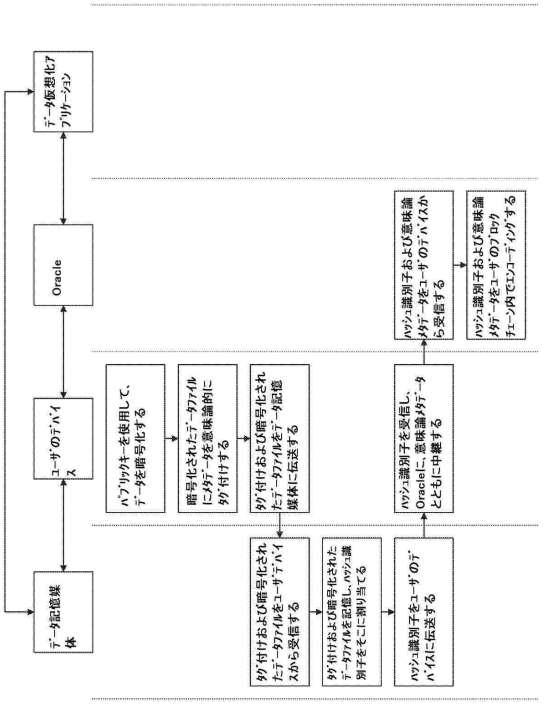

FIG. 2C

【図３】

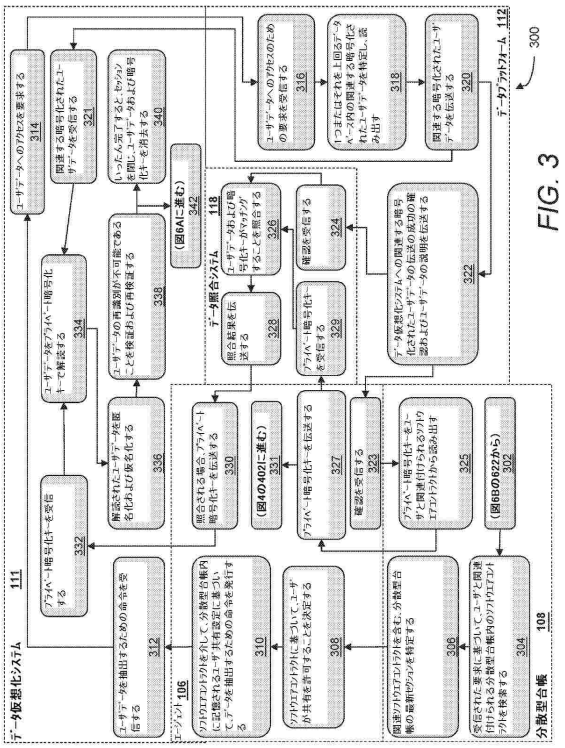

FIG. 3

【図４】

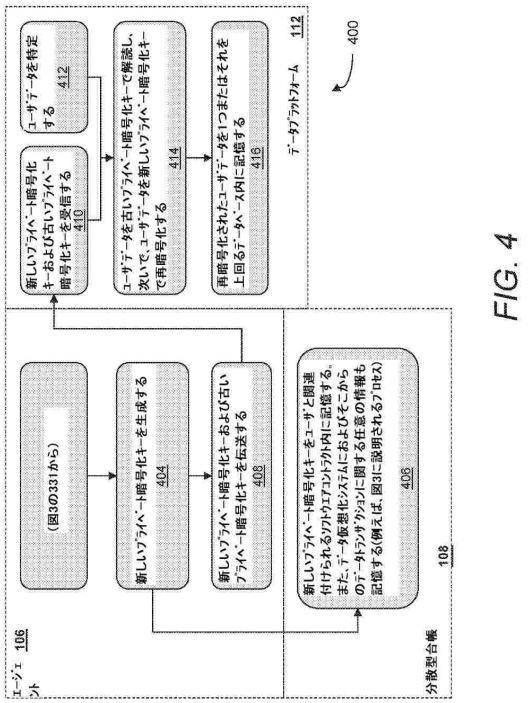

FIG. 4

【図５】

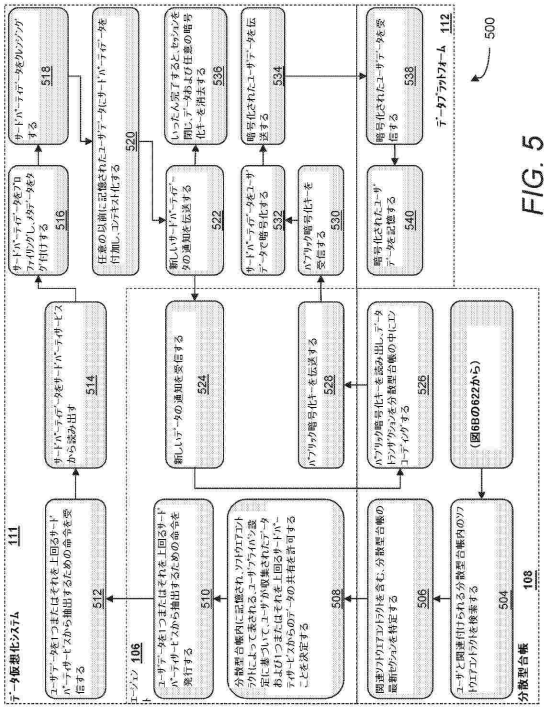

FIG. 5

【図６Ａ】

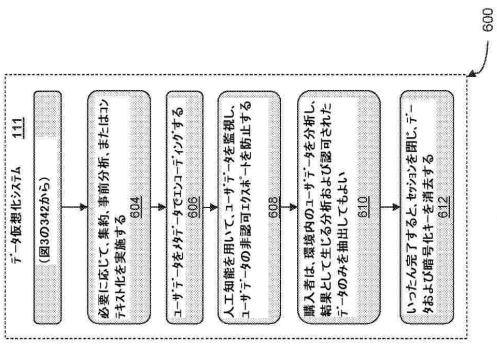

FIG. 6A

【図６Ｂ】

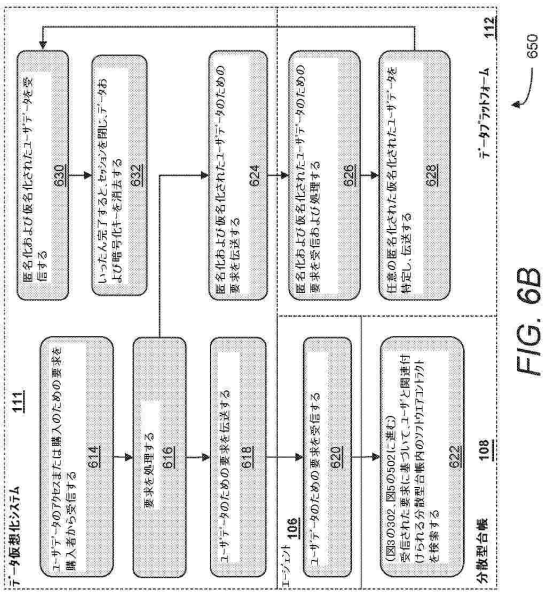

FIG. 6B

【図７Ａ】

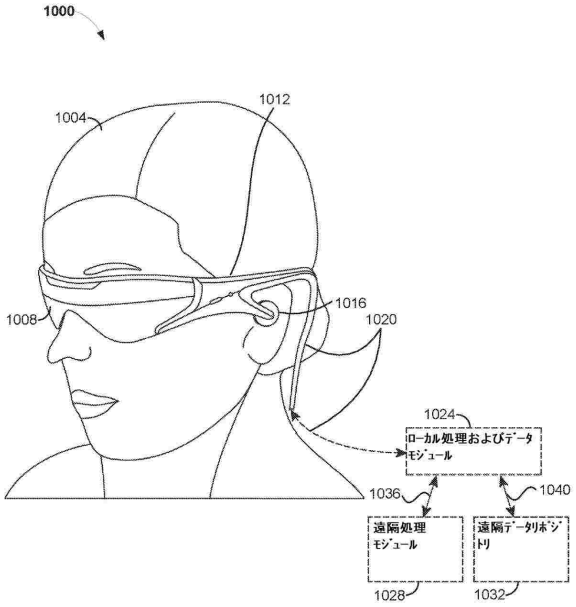

FIG. 7A

【図７Ｂ】

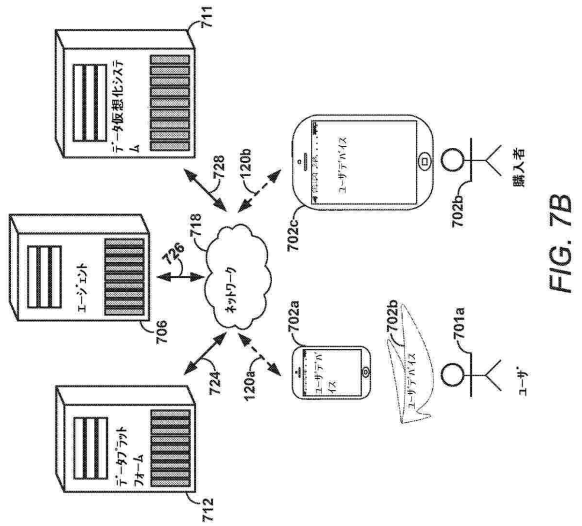

FIG. 7B

【図８】

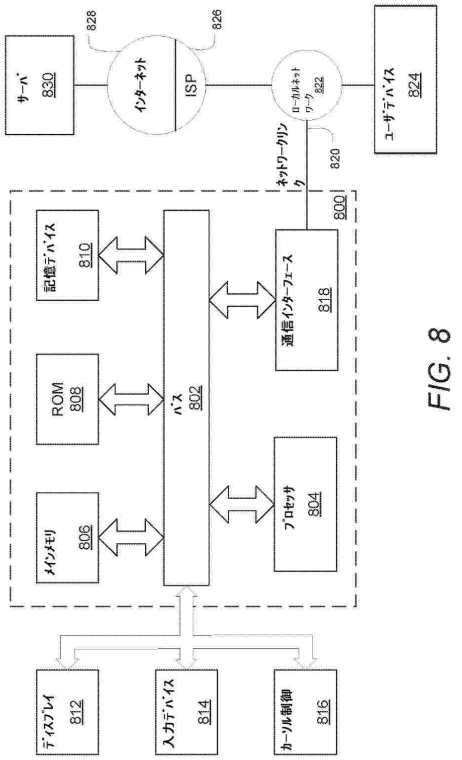

FIG. 8

フロントページの続き

(74)代理人　100181641
弁理士　石川 大輔
(74)代理人　230113332
弁護士　山本 健策
(72)発明者　キャンベル， ジョン
アメリカ合衆国 フロリダ ３３４２８， ボカ ラトン， グランド ヴェルデ ウェイ ９８００，アパートメント ４１３
(72)発明者　オルシャンスキー， ダニエル
アメリカ合衆国 カリフォルニア ９４０４０， マウンテン ビュー， エスキュエラ アベニュー ３３３， アパートメント ２３０
(72)発明者　カー， マイケル ロイヤル
アメリカ合衆国 テキサス ７８７３７， オースティン， レキシントン ドライブ ２５１

審査官　行田 悦資

(56)参考文献
特開２００４－１９２３５３（ＪＰ，Ａ）
特開２０００－１５６８８３（ＪＰ，Ａ）
特表２０１８－５２２３２４（ＪＰ，Ａ）
米国特許出願公開第２０１６／０３３５８０２（ＵＳ，Ａ１）
国際公開第２０１９／１０１２２５（WO，Ａ２）
米国特許出願公開第２０１９／００２８２７７（ＵＳ，Ａ１）
米国特許出願公開第２０１９／０１６６１０１（ＵＳ，Ａ１）
特開２００７－１３４８６６（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０６Ｆ　２１／６２
Ｇ０６Ｆ　２１／６０