(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7064576号
(P7064576)

(45)発行日　令和4年5月10日(2022.5.10)

(24)登録日　令和4年4月26日(2022.4.26)

(51)国際特許分類			FI		
H04L	*9/32*	*(2006.01)*	H04L	9/32	200Z
G06F	*21/31*	*(2013.01)*	G06F	21/31	
G06F	*21/62*	*(2013.01)*	G06F	21/62	354
G06F	*21/64*	*(2013.01)*	G06F	21/64	

請求項の数　11　（全152頁）

(21)出願番号　特願2020-508980(P2020-508980)
(86)(22)出願日　平成30年4月27日(2018.4.27)
(65)公表番号　特表2020-519210(P2020-519210A)
(43)公表日　令和2年6月25日(2020.6.25)
(86)国際出願番号　PCT/US2018/029890
(87)国際公開番号　WO2018/201009
(87)国際公開日　平成30年11月1日(2018.11.1)
審査請求日　令和2年1月24日(2020.1.24)
(31)優先権主張番号　62/491,294
(32)優先日　平成29年4月28日(2017.4.28)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/535,601
(32)優先日　平成29年7月21日(2017.7.21)
最終頁に続く

(73)特許権者　519385320
アノノス インコーポレイテッド
アメリカ合衆国 ニューヨーク州 １０００３－１５０２ ニューヨーク パーク アベニュー サウス ２２８ スイート ９６０４９
(74)代理人　100094569
弁理士　田中 伸一郎
(74)代理人　100103610
弁理士　▲吉▼田 和彦
(74)代理人　100109070
弁理士　須田 洋之
(74)代理人　100067013
弁理士　大塚 文昭
(74)代理人　100086771
最終頁に続く

(54)【発明の名称】　非集中型システムで集中型プライバシー制御を実施するためのシステムや方法

(57)【特許請求の範囲】
【請求項１】
以下を含むシステム
ネットワーク上でデータを送信する通信インターフェース、コンピュータプログラムコードとデータ記録が可能な分散型台帳を持つ内臓メモリ、そしてメモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上のプロセスユニット
コンピュータプログラムコードとデータ記録が可能な分散型台帳を持つ内臓メモリ
メモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上の、プロセスユニットで、そのコードによって、一つ以上のプロセスユニットは、
最初のデータ主体に関連した最初のユーザーからデータを取得し、
最初のデータ主体のための、最初の動的に変化する一時的なユニーク識別子(DDID)を生成するが、ここでは、DDIDは、最初のデータ主体に関連する最初の値を置き換えるために集約され、
最初のDDIDを一つ以上の分散型台帳の最初の台帳の最初の要素に保存し、
最初の要求者からの、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、
最初の要求者が最初の値を受け取ることをオーソライズさていない場合、最初のDDIDを最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信し、そして、
最初の要求者が最初の値を受け取ることをオーソライズさている場合、最初のデータ主体に関連した最初の値を、最初のリクエストに応じて、ネットワーク上で最初の要求者へ送

信し、
前記システムでは、一つ以上のプロセスユニットがコンピュータプログラムコード内の指示を実行するために集約され、そのコードによって、一つ以上のプロセスユニットは、
プライバシーポリシーへの対策として最初のユーザーからリクエストを取得し、
少なくとも部分的にはリクエストを基にした最初のプライバシーポリシーを決定し、
ここにおいて、最初のDDIDは決定された最初のプライバシーポリシーを満たすために集約され、そして、
最初のDDIDを一つ以上のデータ記憶装置に保存し、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされていない場合、最初のDDIDを、最初のリクエストに応じて、ネットワーク上で送信し、そして最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされる場合、最初の値を、最初のリクエストに応じて、ネットワーク上で送信し、
コンピュータプログラムコードの指示を実行するために一つ以上のプロセスユニットが集約され、そのコードによって、一つ以上のプロセスユニットは、
最初のデータ主体に関連した最初の値を、最初の修正値に変更するために、最初のユーザーからリクエストを取得し、
データ主体に関連した最初の値を含む保管場所に、最初の修正値を保存する。
【請求項２】
請求項１のシステムにおいて、ネットワークが分散されており、ネットワークがノードの複数性を含み、ネットワークがそれぞれのノードに一つ以上の分散型台帳の最初のコピーを保存する。
【請求項３】
請求項２のシステムにおいて、一つ以上の分散型台帳の最初のものがblockchainを含み、最初の要素が最初のブロックを含む。
【請求項４】
請求項１のシステムにおいて、最初のDDID が最初のデータ主体に関連する最初の値を含む保管場所を示す。
【請求項５】
コンピュータにより実施される手法で以下を含む
最初のデータ主体に関連した最初のユーザーからデータを取得し、
最初のデータ主体のための、最初の動的に変化する一時的なユニーク識別子(DDID)を生成し、ここでは、DDIDは最初のデータ主体に関連する最初の値を置き換えるために集約され
最初のDDIDを一つ以上の分散型台帳の最初の台帳の最初の要素に保存し
最初の要求者からの、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し
最初の要求者が最初の値を受け取ることをオーソライズさていない場合、最初のDDIDを最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信し
最初の要求者が最初の値を受け取ることをオーソライズさている場合、最初のデータ主体に関連した最初の値を、最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信し、
前記コンピュータにより実施される手法において、さらに以下を含む
プライバシーポリシーへの対策として最初のユーザーからリクエストを取得し、
少なくとも部分的にはリクエストを基にした最初のプライバシーポリシーを決定し
ここにおいて、最初のDDIDは決定された最初のプライバシーポリシーを満たすために集約され、そして、
最初のDDIDを一つ以上のデータ記憶装置に保存し、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされていない場合、最初のDDIDを、最初のリクエストに応じて、ネットワーク上で送信し、そして最初のプライバシー

ポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされる場合、最初の値を、最初のリクエストに応じて、ネットワーク上で送信し、
最初のデータ主体に関連した最初の値を、最初の修正値に変更するために、最初のユーザーからリクエストを取得し、
データ主体に関連した最初の値を含む保管場所に、最初の修正値を保存する。
【請求項６】
請求項５のコンピュータにより実施される手法において、
ネットワークが分散されており、ネットワークがノードの複数性を含み、ネットワークがそれぞれのノードに一つ以上の分散型台帳の最初のコピーを保存する。一つ以上の分散型台帳の最初のものがblockchainを含み、最初の要素が最初のブロックを含む。
【請求項７】
請求項５のコンピュータにより実施される手法において、最初のDDID が最初のデータ主体に関連する最初の値を含む保管場所を示す。
【請求項８】
恒久的なプログラムストレージデバイスで、プログラマブルコントロールデバイスによって判読可能であり、格納された指示で構成され、その指示が実行されることでプログラマブルデバイスは、
最初のデータ主体に関連した最初のユーザーからデータを取得し、
最初のデータ主体のための、最初の動的に変化する一時的なユニーク識別子(DDID)を生成し、ここでは、DDIDは、最初のデータ主体に関連する最初の値を置き換えるために集約され、
最初のDDIDを一つ以上の分散型台帳の最初の台帳の最初の要素に保存し
最初の要求者からの、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し
最初の要求者が最初の値を受け取ることをオーソライズさていない場合、最初のDDID を最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信し
最初の要求者が最初の値を受け取ることをオーソライズさている場合、最初のデータ主体に関連した最初の値を、最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信し、
前記恒久的なプログラムストレージデバイスにおいて、指示によってプログラマブルコントロールデバイスは、さらに、
プライバシーポリシーへの対策として最初のユーザーからリクエストを取得し、
少なくとも部分的にはリクエストを基にした最初のプライバシーポリシーを決定し、
ここにおいて、最初のDDIDは決定された最初のプライバシーポリシーを満たすために集約され、そして、
最初のDDIDを一つ以上のデータ記憶装置に保存し、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされていない場合、最初のDDIDを、最初のリクエストに応じて、ネットワーク上で送信し、そして最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされる場合、最初の値を、最初のリクエストに応じて、ネットワーク上で送信し、
指示によってプログラマブルコントロールデバイスは
最初のデータ主体に関連した最初の値を、最初の修正値に変更するために、最初のユーザーからリクエストを取得し
データ主体に関連した最初の値を含む保管場所に、最初の修正値を保存する。
【請求項９】
請求項８の恒久的なプログラムストレージデバイスにおいて、
ネットワークが分散されており、ネットワークがノードの複数性を含み、ネットワークがそれぞれのノードに一つ以上の分散型台帳の最初のコピーを保存する。
【請求項１０】

請求項９の恒久的なプログラムストレージデバイスにおいて、一つ以上の分散型台帳の最初のものがblockchainを含み、最初の要素が最初のブロックを含む。
【請求項１１】
請求項８の恒久的なプログラムストレージデバイスにおいて、最初のDDID が最初のデータ主体に関連する最初の値を含む保管場所を示す。
【発明の詳細な説明】
【技術分野】
【０００１】
〔関連アプリケーションへの相互参照〕
［1］この出願は、2018年4月26日に出願された「非中央集権システムにおける中央集中プライバシー制御を実施するためのシステムおよび方法」の米国特許出願第15 / 963,609号に対する優先権を主張する。
2017年4月28日出願「ヘルスケアデータの収集と共有のAnonosizing」という表題の米国仮特許出願第62 / 491,294号。
2017年7月21日出願「仮名化を保持する動的な仮名化」という表題の米国仮特許出願第62 / 535,601号。
2017年9月4日出願「Anonos Global Data Protection Regulation Compliant Analytics」と題された米国仮特許出願第62 / 554,000号
2017年11月2日に出願された「Anonos BigPrivacy Compressible Dynamic De-Identifiers」と題された米国仮特許出願第62 / 580,628号
2018年3月17日に出願された「Anonos BigPrivacy GDPR Compliant Block Chain Systems and Methods」というタイトルの米国仮特許出願第62 / 644,463号
2018年3月28日に出願された「BigPrivacy Data Compliance in the Cloud」と題された米国仮特許出願第62 / 649,103号 これらが本書に組み込まれます。
【０００２】
〔発明分野〕
［2］本開示は、一般に、データセキュリティ、プライバシー、および精度の改善に関し、たとえばblockchain などのDistributed Ledger Technology (DLT)に格納されるなど、動的に変化する識別子を使用してデータの要素をレンダリングすることに関する。（注：本書では、「プライバシー」と「匿名」という用語は、データ保護、プライバシー、匿名、仮名、不明瞭さ、その他の行動を指すために交換可能に使用されます。事業体、企業体、または法人のグループのような個人は、無許可の当事者から自分自身に関する情報を隔離、隔離、または編集し、それによって自分自身に関する情報を選択的に提供します。本明細書では、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を含むデータストレージ要素を指すために使用され、たとえば複数のサイト、国、または機関に地理的に分散する場合があります。“ Distributed Ledger Technology ” DLTの使用例には、ブロックチェーン、暗号通貨（cryptocurrencies）、スマートコントラクト、さらには分散ファイルストレージも含まれます。
【背景技術】
【０００３】
[03]このセクションは、特許請求の範囲に記載されている本発明の背景または文脈を提供することを意図している。
本書の説明は、追求することができる概念を含むが、必ずしも以前に着想、実装、または説明された概念ではない。
したがって、本セクションで特に断りのない限り、このセクションで説明されていることは、本出願の説明および特許請求の範囲の先行技術ではなく、このセクションに含まれることにより先行技術であると認められない。
【０００４】
[04]これら3つの間には矛盾があります。
（i）データの価値を最大化するという当事者の目標と、個人のプライバシー権を尊重する

。
（ii）個人のプライバシー権を保護するという個人の目標と、高度にパーソナライズされたサービスの恩恵を受けるという目標。 そして
（iii）研究および商業を促進するための米国および国際政府機関の目標と、市民の権利を保護するという目標。
【０００５】
[05]ヘルスケア関連以外の関係者の1つの目標は、「高資格のある」見込み顧客に到達することです。必要な財源、動機、購入の権限を持っている見込みのあるバイヤーです。
商業関係者は、利子、素因、および取引を閉じる手段を考えると、適格な見込み客と取引を完了する可能性が非常に高いため、未分化の見込み客に到達するよりも利益があると考え、適格な見込み客に到達するために多くを支払います。
取引を完了する可能性に直接関係する見込み顧客向けの製品のパーソナライズ/カスタマイズのレベルは、個々の見込み客について利用可能な情報の深さと範囲によって強化されます。医療関係者の目標の1つは、人間の健康を改善する可能性のあるアプリケーションで発見を進めることを目標に、健康および/または病気に関する研究を行うことです。
【０００６】
[06]コンピュータネットワーク、インターネット、イントラネット、およびサポート技術の開発の出現と普及により、情報を電子形式で収集、送信、保存、分析、および使用するための費用対効果の高い技術が広く利用可能になりました。
その結果、エンティティは膨大な量の情報を容易に収集および分析できるようになりました。
しかし、これにより、（a）と（b）の間に緊張が生じました。
（a）見込み客を認定し、潜在的な顧客向けにパーソナライズ/カスタマイズされた製品を開発し、および/または健康関連またはその他の研究を実施するために利用できる情報量が増加している。
（b）多くのデータ要素の存在に気付かないことが多く、それらのデータ要素の効果的な制御がほとんどまたはまったくない場合が多い個人のセキュリティ、匿名性、プライバシーの低下。
【０００７】
[07]データ要素はさまざまなソースを通じてオンラインとオフラインの両方で収集できます。（ソーシャルネットワーキングサイトでの活動、電子またはデジタル記録、電子メール、報酬への参加、購入や場所を追跡するボーナスカードプログラムなど、インターネットでのブラウジングやその他のアクティビティ、実店舗やeコマースWebサイトでのアクティビティと購入など）
商人、医療関連およびその他のサービスプロバイダー、政府、およびその他の組織は、収集、保存、分析されるこの膨大な量のデータを使用して、パターンと相関関係を提案または見つけ、有用な結論を導き出します。
現在、膨大な量の情報が収集される可能性があるため、このデータは「ビッグデータ」と呼ばれることもあります。
このビッグデータ分析によりエンティティはデータの価値を解き放ち、最大化できるようになりました。
健康関連のエンティティがビッグデータにアクセスして医学研究を実施することがあります。ただし、行動マーケティングとビッグデータ分析により、関係者のプライバシーと匿名性ははるかに低くなりました。
【０００８】
[08]プライバシー/匿名性と価値/個人化/研究の間の矛盾を和解する試みは、実際の名前や識別情報ではなく代替識別子を使用することをしばしば伴いました。
ただし、これらの代替識別子は一般に静的に割り当てられ、長期にわたって持続します。
静的識別子は、真のアイデンティティを確認するために、より簡単に追跡、識別、相互参照され、関係者の同意なしにデータ要素に関連付けられたサブジェクトに関する追加デー

タを確認するために使用できます。
プライバシーおよび情報の専門家は、再識別手法が静的識別子に関連付けられたデータで使用される可能性があることを懸念し、特定のコンピューター、デバイス、またはアクティビティ（つまり、関連付けられた静的識別子を通じて）を識別できるデータが実際に匿名または保護された匿名の状態で維持されます。
識別子が時間とともに変化しない場合、敵対的エンティティは、追加のデータまたは外生データを永続的な識別子に追加、分析、関連付けるために無制限の時間を持ちます。さらにその時間は、暗号化されたデータに対して使用されるブルートフォース攻撃を実行する機会を敵対エンティティに提供します。
【０００９】
[09] 2011年のMcKinsey Global Instituteの報告によると：
・ビッグデータを最大限に活用する小売業者は、営業利益率を60%以上引き上げる可能性がある。;
・公共部門でビッグデータを活用することには大きな可能性がある。もし米国の医療機関がビッグデータを創造的かつ効果的に利用して効率性と品質を向上させれば、この部門は毎年3000億ドル以上の価値を生み出し、その2/3は米国の医療費を約8%削減することになる。;
ヨーロッパの先進国では、政府管理者はビッグデータ活用による業務効率化で1000億ユーロ(1490億ドル)以上の節約が可能だった。;
個人の位置情報を利用できるビッグデータを利用することで、6000億ドルの消費者余剰を獲得できる可能性がある。
【発明の概要】
【発明が解決しようとする課題】
【００１０】
[10] ビッグデータから得られる多くの潜在的な利益は、基になるデータの所有権/使用権に関する曖昧さ、基になるデータのプライバシーに関する緊張、二次的(プライマリとの比較)情報源から収集された誤ったデータ、および/または当事者の積極的な参加や検証なしに当事者の活動から推論された不正確な分析の結果のために、完全には実現されていない。
【００１１】
[11]ピアツーピアベースまたは他の非集中ベースでリンクされたネットワークまたはプラットフォームを含む、分散ネットワークまたはプラットフォーム(これには、許可を必要としないシステムや、blockchainなどの分散型元帳技術が含まれる。)の人気の爆発は、ユーザの所望のレベルのプライバシー/匿名性を維持することの困難性をさらに増大させ、一方で、認可された第三者による情報価値の適切な抽出、個人化されたサービスの提供を可能にしている。特に不変性,監査可能性および検証に関する分散元帳技術の要求により、少なくともそのような分散元帳に記録される情報の必然的に静的な性質のため、高レベルのプライバシー/匿名性を提供することはこれまで不可能であった。
【００１２】
[12] 必要とされているのは、静的及び/又は永続的なプライバシー/匿名性及びセキュリティシステムの限界を克服し、交換、収集、トランザクション、分析及び他の使用のためのデータの正確性を改善するシステム、方法、装置であり、例えば、blockchainのような分散元帳技術を使用して分散された様式でデータを格納するアプリケーションの場合である。別の言い方をすれば、本明細書に記載されているようなプライバシー/匿名性を強化する技術は、特定の時間および文脈が与えられた場合に、許可されたユーザがそのような情報の「真」意味をアンロックすることを可能にするツールを提供することによって、監査可能な情報ストアと不変の情報ストアとの間の緊張を調和させるのを助けることができる。
【課題を解決するための手段】
【００１３】
[13] 本発明の実施形態は、データが関係するサブジェクトが、「動的に匿名」すなわち、望まれる程度まで、匿名であることを可能にすることによって、データのプライバシーお

よびセキュリティを改善できる。本発明の実施形態は、プライバシー、匿名性、およびセキュリティを向上させてデータを作成、アクセス、使用(例えば、収集、処理、複製、分析、結合、修正、配布等。)、格納、消去し、それによって、より適格で正確な情報の可用性を容易にするシステム、方法、および装置を含む。また、データを第三者と共有することが許可されている場合、本発明の実施形態は、受信者への時間的、地理的、および/または目的が限定された情報の配信を可能にする動的に制御された方法で情報を共有することを容易にすることができる。本発明の実施形態は、時間の経過に伴う記録の不変性及び監査可能性を必要とするblockchain又は他の分散元帳技術上に構築された分散型ネットワークにおいても使用することができる。

【００１４】

[14] 既存のシステムと比較し電子データを使用するために簡単にアクセスできる場合（たとえば収集、処理、コピー、分析、結合、修正、配布など）、保存および消去は、データに関して、本発明の実施形態は、dynamically changing de-identifiers (“DDIDs”)を使用することができ人、場所、または物（例えば、イベント、文書、契約、またはスマート契約）、データが直接または間接的に関係または関連するもの（“Data Subject”）、および/またはData Subjectに関連するアクション、アクティビティ、プロセスおよび/または特性、時間的に一意の期間、データ主体が「dynamically anonymous」で動作できるようにします。

本明細書で使用されるDynamically anonymous” と“Dynamic Anonymity”は、匿名のままにしないという決定が下されるまで匿名のままでいるユーザーの能力を指し、目的の情報のみが1つ以上の目的の当事者と共有されます1つ以上のアクション、アクティビティ、プロセス、または特性との接続、それにより、本発明の実施形態は、信頼できる当事者またはプロキシであり得るデータ主体または制御エンティティの制御下で、データ主体がプライバシーの柔軟なレベルを維持する能力を可能にします。

【００１５】

[15]本発明の実施形態は、データの保持を防止するためにDDIDsを使用してもよい。

Data Subjectの1つ以上の側面に関する情報と、Data Subjectに関連するアクション、アクティビティ、プロセス、および特性を反映するデータ属性を第三者に提供することがあるメタデータと呼ばれることもあります。

（たとえば、限定ではなく例として、作成手段、目的、作成日時、Data Subjectの識別とデータ属性の作成者、データ属性が作成された場所、作成に使用される基準、またはデータ属性などの使用など）

これは、1つ以上の特定のデータ属性に関連付けられた情報の継続的な記録を確立するために、メタデータにアタッチする（または関連付ける）ものが必要であるという事実によるものです。

このアプリケーションで使用される「データ」、「属性」、「要素」、または同様の用語は以下が含まれます。

I 構造化データ（所定の構造化スキーマのデータ）、

（ii）非構造化データ

（iii）メタデータ

（iv）その他のデータ

（v）前述のタイプのいずれか 最初にアナログ形式で記録されたデータのうち、後でデジタル形式に変換されたデータ

【００１６】

[16]本発明の実施形態は、第１のデータ主体、アクション、アクティビティ、プロセス、および特性に関する特定の目的のために一度に第１のDDIDを使用し、その後、第１のData Subjectに関連して第２のDDIDを使用し、異なる目的のための行動、活動、プロセス、および特性、

別の目的などのために、最初のDDIDを2番目のData Subject、アクション、アクティビティ、プロセス、および特性に関連付けて使用します。

その結果、DDIDに関連付けられた基礎情報に関連付けられたデータを保持および集約しようとすると、異なるDDIDが同じデータサブジェクト、アクション、アクティビティ、プロセスおよび/または特性に関連付けられ、および/または同じDDIDがData Subject、アクション、アクティビティ、プロセス、特性、目的で使用されます。

【００１７】

[17]本発明の実施形態は、様々なアクション、アクティビティ、プロセスまたは特性に関して異なる時点でData Subjectsによって使用され、関連付けられた異なるDDIDを追跡および記録することができる。

これにより、特定のアクション、アクティビティ、プロセスまたは特性、および特定のデータサブジェクトに適用可能な情報の保存、選択、取得が可能になります。

逆に、システムはDDIDsを使用し、DDIDsとData Subject、アクション、アクティビティ、プロセス間の関係を決定するためにシステムの外部で利用可能な情報が不足しているため、システムの外部の第三者がデータを効果的に保持および集約できない場合があります。

【００１８】

[18]それぞれのDDIDは、特定のアクション、アクティビティ、プロセス、または特性に関して以下のように1つ以上のデータ属性に関連付けることができます。

a）現在のDDIDに関連付けられている間、データ主体に関連付けられているアクション、アクティビティ、プロセス、または特性を反映する情報（たとえば、現在のDDIDに関連付けられている間、データ主体の現在のWebベースのアクティビティを反映する閲覧情報）DDIDは別のDDIDに置き換えられます。

b）複数の前のDDIDに関連付けられているデータ主体に以前関連付けられていた過去のアクション、アクティビティ、プロセス、または特性に関する情報。

（例：データ主体が以前のブラウジングセッションで以前のDDIDに関連付けられている間にウェブサイトから収集したeコマースウェブサイトと価格情報を共有する。）

（c）現在のDDIDに関連付けられている間、データ主体に代わって望ましいアクション、アクティビティ、プロセス、または特性に関して促進するのに役立つ新しい情報（たとえば、現在望ましい衣服の購入のための新しい望ましいサイズと色を示すeコマースウェブサイト）。

本書の目的上、DDIDと時間的に一意な期間のDDIDに関連付けられたデータ要素の組み合わせは、temporal data representation「TDR」と呼ばれます。

【００１９】

[19]クローズドのシステムであるDynamic Anonymityの実施形態の実装の観点から、Data SubjectのIDを表すことを目的としたDDID、つまり「プライマリ識別子」は、データサブジェクトへのDDIDの割り当て期間中に一時的に一意である必要があります。－つまり、2つの既存のData Subjectが同時に同じプライマリ識別子DDIDを持つことはできません。

DDIDの一時的な一意性の要件は、Data SubjectのIDの分離がDDIDによって表されることが望ましい場合に適用されます。データ主体のIDの分離性以外の要素をDDIDで表現したい場合、それに応じてDDIDの割り当てを行い、目的の関連付け、関係などを表すことができます。

DDIDは、2つの方法でインスタンス化できます。

（i） 本発明の実装内（ii）外部で作成された識別子によるが、「一時的に一意」の要件（「Cookie」または他の一意の識別子）Data SubjectのIDの分離がDDIDで表されることが望ましい場合、Webサイトによって初めて訪問者に割り当てられると、DDIDとして効果的に機能します。

【００２０】

[20] Cookieは、一般にウェブサイトから送信され、データ主体がウェブサイトを閲覧している間にデータ主体のウェブブラウザに保存される小さなデータです。Data SubjectがWebサイトに戻るたびに、ブラウザはWebサイトに関連付けられたサーバーにCookieを

送り返し、Data SubjectがWebサイトに戻ったことを通知します。ただし、CookieがDDIDとして機能するために、ブラウザはWebサイトから送信されたCookieが閲覧セッション間で保持されないようにします。（ユーザーのCookie、キャッシュ、閲覧履歴ファイルを匿名システムのサーバーにコピーし、ユーザーのコンピューターから削除するようにするなど。）
ブラウジングセッションごとに新しいCookieが割り当てられるようにします。
このように、Webサイトによって発行されたさまざまなCookie（この実施形態は、データ主体のIDの分離を表すDDIDとして機能します。）は、システムに対して「外部」に作成され、閲覧セッションのそれぞれがウェブサイトによって無関係であると認識されるため、ステートフル情報を記憶するか、Data Subjectの閲覧アクティビティを集約します。これにより、Data Subjectは、必要な限り、動的に匿名のままになります。

【００２１】

[21]前記の実施形態の例で述べたように、Dynamic Anonymityシステムは、異なるブラウジングセッション、Cookieに関連するさまざまなアクション、アクティビティ、プロセスまたは特性に関する情報を収集および保持することができる。（この例では、データ主体のIDの分離を表すDDIDとして機能します。）
そして、Data Subjectが匿名を維持するという意思決定が行われるまで、またはその代わりにData Subjectの集約データプロファイルに結合された情報を保存し、その時点でData Subjectの集約データから必要な情報のみを取得するプロファイルは、1つまたは複数のアクション、アクティビティ、プロセスまたは特性に関連して、1つまたは複数の希望する関係者と共有する必要があります。
本発明のこの例示的な実施形態では、Data Subjectが全体のデータプロファイルからTDRとしてWebサイト（制御エンティティ）に情報を提供することを決定することが含まれる事があります。本発明の上記の例示的な実施形態では、
データサブジェクトがアクセスしたWebサイトによって割り当てられたCookieをDDIDとして使用する代わりに、（動的に変化するプロキシの削除、
DDIDとして、本発明の実装によって内部で作成されたか外部で作成されたかにかかわらず、システムはグローバル一意識別子（GUID）（つまり、コンピューターソフトウェアで識別子として使用される一意の参照番号）を使用する事があります。
上記では、Data Subjectによる閲覧活動のデータの収集に対する制御は、Data Subjectが訪問したウェブサイトではなく、Data Subjectまたは他の制御エンティティにあります。
さらに他の例ではData Subjectが集約するデータプロファイルからウェブサイトに情報を「プッシュ」するタイミングを決定するのではなく、
ウェブサイトは、適切な許可と認証を使用して情報を必要とするときに、Data Subjectの集計データプロファイルから関連情報および関連するDDIDとData Subjectの関連付け情報を「プル」することができます。

【００２２】

[22]他の例として、データ主体の集約データプロファイルの関連部分の送信を動的に匿名化し、制御する作業は、データ主体のクライアントデバイス自体によって処理される場合があります。
たとえば、特定のData Subjectの情報、関連するDDIDからData Subjectへの関連情報の完全な見解は、定められた、または柔軟な期間Data Subjectのクライアントデバイスに保存でき、その後、中央のDynamic Anonymityシステムに同期されます（また、データ主体が中央匿名システムに登録した他のクライアントデバイスと同期されます）。

【００２３】

[23] TDRおよびDDIDは、追跡および識別の目的で複数レベルの抽象化を含む場合があります。
本発明のいくつかの実施形態によるシステムは、ＴＤＲ（ＤＤＩＤ値と、もしあれば、ＤＤＩＤに関連付けられたデータ要素）を格納することができる。サブジェクト、データ属

性、アクション、アクティビティ、プロセス、または特性-これらによってTDRを特定のData Subject、データ属性、アクション、アクティビティ、プロセス、特性に後で再関連付けることが可能です。このようなシステムは、さまざまなDDID、Data Subject、データ属性、アクション、アクティビティ、プロセス、および特性の間の関係を明らかにするキーを参照して使用することにより、集約データプロファイルの開発を促進するために利用できます。
言い換えれば、本書に記載されているTDRおよびDDIDの使用によって提供される「Dynamic Anonymity」により、データ主体は進行中の技術的進歩（例えば、モノのインターネット（IoT）、個別化医療など）から利益を得ることができます。
プライバシー、匿名性、セキュリティ、または制御を放棄する必要はありません。
これは、以下の事柄によって達成されます。
（i）動的に変化するDDIDをData Subject、アクション、アクティビティ、プロセス、および特性に割り当てる。
（ii）DDIDとData Subject、アクション、アクティビティ、プロセス、および特性との関連付けに関する情報を保持する。
（iii）関連付け情報へのアクセス/使用を決定論的に制御する、データ主体および制御エンティティ（信頼できる関係者/プロキシ）を提供します。動的に変更可能なものを使用すると、一時的なDDID、現在のシステム、およびプロセス（Webブラウザーやデータ分析エンジンなど）は、関連付けられていない、または置き換えられたデータ要素間の関係を認識できない場合があります。
既存の機能を使用して情報を処理できますが、データ主体および信頼できる関係者/プロキシによって明示的に許可されている場合を除き、推論、相関、プロファイル、または結論を作成せずに処理します。
さらに、本発明の実施形態によって使用されるＤＤＩＤは、Data Subjectレベルまたはデータ記録レベルだけでなく、Dynamic Anonymityを可能にするデータ要素レベルで動的に置き換えることができる。 これは、個人が共有またはアクセスするデータを制御できることを意味し情報の「評価低下」なしに動的な識別解除を可能にします。

【００２４】

[24]データ要素レベルまでの情報の制御は、データレコードレベルまたはデータサブジェクトレベルのみを対象とした制御の範囲を超えて、ビッグデータの時に制御された情報共有を可能にします。
さらに、データサブジェクトと、データサブジェクトに関する情報を受信するWebサイトまたは他のエンティティとの間の「連結の関係」を可能にします。ほとんどの既存のシステムは、時間の経過とともに一意の識別子に関する情報を収集します。
DDIDにData Subjectに関する一定量の履歴またはその他の情報が含まれている場合でも、次にData Subjectがサイト、店舗、医師などにアクセスしたとき、DDIDに一意の識別子、名前、または電子メールアドレスが含まれている場合のみData Subjectは完全に異なります。たとえば、受信者は、データ主体を表す当時のDDIDを、データ主体を表すために以前に使用されたDDIDと関連付けることができます。その時点で、受信者は、データ主体に関するデータの収集に基づいてデータ主体と対話できますただし、受信者が次にデータサブジェクトに遭遇したとき、データサブジェクトは、データサブジェクトの希望がない限り再識別できません。

【００２５】

[25] Dynamic Anonymityは、制御された「データ融合」も可能にします。
（ここで、「データ融合」とは、異なるソースからのデータが互いに接触し、新しい事実が明らかになったときに発生するものとして定義されます。）
上記の間の接続を難読化することにより、データ、ID（Data Subjectおよび/または制御エンティティの）およびコンテキスト（たとえば、時間、目的、場所）の制御された匿名性を提供する。したがって、動的匿名により、付与された権利またはデータへのアクセスの取り消しまたは取り消しも可能になります。 （たとえば、特定の関係者にDDIDの基礎

となるデータへのアクセスを提供し、置換キーの変更によりアクセスを取り消すことができます。）
Data Subjectへのルールに違反することなく、追加の承認された二次利用をサポートするため（たとえば、1つまたは複数のDDIDが最初に1つまたは複数の交換キーを介してX線の結果にアクセスし、交換キーを変更することにより、後でX線の結果とフォローアップの結果を反映することがあります。）
【００２６】
[26]動的な匿名性が商業市場で依然として魅力的である理由は、多くの場合、企業が実際にやり取りするData Subjectが誰であるか（実際の「現実世界」のアイデンティティ）を気にしないからです。ターゲット設定が正確で無駄が少ないほど、匿名の消費者はパーソナライズされたサービスに好意的に反応する可能性が高くなります。
したがって、Dynamic Anonymityは、企業がデジタル世界のデータ主体をフォローして、本当に必要としない製品やサービスを購入するように説得しようとする必要性を取り除きます。これを使用すると、売り手と顧客のマッチングが期待でき高い収益が得られる事でしょう。
現在、多くの企業ができる最善の方法は、人口統計と統計を使用して潜在的な顧客を「セグメント化」することですが、個々の実際の関心についてはわからない場合があります。企業は代わりに、Data Subjectが何であるか、Data Subjectの行い、どのように動作するのを気にします。Dynamic Anonymityは、適格な見込み客であるセグメントのメンバーから個別の関心のある事を提供することにより、人口統計を改善します。
Dynamic Anonymityにより、Data Subjectが個人のプライバシー/匿名性の好みに応じてデータの使用を直接または間接的に制御できるようにする能力は、そのような管轄区域での異なるデータ使用/プライバシー/匿名性要件にもかかわらず、異なる管轄区域でのデータの異なる取り扱いをサポートできます。
（例：欧州連合の「基本的権利」と、プライバシーの権利/自由な表現の権利/データのプライバシー/匿名性に関する商取引の観点からの米国のバランスの違い）。
【００２７】
[27]医学および関連分野ではDynamic Anonymityは、防御的アプローチを使用してデータのプライバシー/匿名性を保護する従来のアプローチよりも良いと言えます。-たとえばマスキング手順が直接識別子に適用（名前、住所）。
不正な第三者による再識別の可能性を減らすために、マスキングまたは統計ベースの操作が準識別子（例：年齢、性別、職業）に適用されます。
データのプライバシー/匿名性を保護するためのこの防御的なアプローチは、再識別に対する保護とユーザー情報へのアクセスの保持とのトレードオフをもたらします。Data Subject間のアクション、アクティビティ、プロセス、特性を表します。
その意味は時間とともに変化する可能性があり、その結果、その時点で適切なキーが基になる値を識別する必要があります。
したがって、Dynamic Anonymityは、匿名性損失のリスクを最小限に抑えるために、情報コンテンツを永久に回復不能にして犠牲にしなければならないとい事が無くなります。代わりに、Dynamic Anonymityは匿名性の損失のリスクと失われた情報の量の両方を最小限に抑え、ほとんどのデータを承認のみで回復可能にします。
【００２８】
[28]本発明の実施形態によって使用されるキーは、対応するDDIDの使用に応じて異なり得る。たとえば、タイムキー（「TK」）を使用して、DDIDとデータ主体、アクション、アクティビティ、プロセス、および/または特性との関連付けの期間を関連付けることができます。すなわちアソシエーションキー（「AK」）を使用して、異なるDDIDを使用しているために、相互に識別できない2つ以上のデータ要素やTDR間のアソシエーションを明らかにすることができます。置換キー（「RK」）は、TDR内の1つ以上のデータ属性の置換にDDIDが使用される場合に使用できます。この場合、TDRに含まれる1つ以上のDDIDによって、ルックアップテーブルを参照し置換される1つ以上のデータ属性の値を決定で

きます。
【００２９】
[29]該当するTK、AK、RKにアクセスできない場合、第三者が1つ以上のData Subject、アクション、アクティビティ、プロセス、特性に関する情報を傍受した場合第三者は次のことができません。
（ｉ）本発明の関連付け機能の場合ＤＤＩＤと対応するデータ属性（ＴＤＲを含む）とを関連付けることにより、データ主体を再特定する。
（ｉｉ）本発明の置換機能の場合に情報を正しく理解するために、ＤＤＩＤによって表されるデータ要素の値を知ること。
逆に、本発明の実施形態は、データ主体または他の制御エンティティが、特定のアクション、アクティビティ、プロセスまたは特性に特に関係するデータ属性のみを1つまたは複数の所望の第三者に送信できるようにし得る。（システムの追跡/ロギング/記録機能により、Data Subjectに関連している事がシステムで認識されている。）
【００３０】
[30]以下の用語は、本書で説明される様々な実施形態に従って、データを匿名化することに関連して使用されてもよい。
【００３１】
[31]「A-DDID」、「Association DDID」：
識別データ要素およびデータ要素の値への逆参照（ポイント）を置き換えるため、非特定的な方法で、オプションで指定されたグループ化ルールに従って情報価値を伝えるために使用されるDDID（データ要素と値）を指す。参照解除を解決するために使用されるインデックスには、キー、スキーマ変換テーブル、匿名識別子、仮名識別子、トークンまたはその他の表現が含まれますが、これらに限定されません。A-DDIDの逆参照グループ化ルールは、少なくとも2種類のグループ化である可能性があります：数値とカテゴリ。数値は、A-DDIDで表される数値の範囲を指します。カテゴリのグループ化は、「相関関係」（つまり、2つ以上の関連または補完アイテム）を、各グループ化カテゴリ内の値間の相関関係を表すために選択されたA-DDIDに置き換えます。
A-DDID参照解除規則は、複数のフィールドをカバーする場合もあります。
たとえば、血液検査では、心臓発作のリスクを推測できるさまざまな変数をカバーできます。
そのため、ルールは、心臓発作のリスクを特定のカテゴリに割り当てるために必要なさまざまな組み合わせ（高、中、低など）を指定できます。
【００３２】
[32]「R-DDID」、「Replacement DDID」：識別データ要素を置き換え、データ要素の値への逆参照（たとえば、ポイント）に使用できるDDIDを指します。
【００３３】
[33]「Mosaic Effect」とは、一見匿名のデータセット間でデータを相互に関連付けることにより、Data Subjectを再識別する機能を指します。
【００３４】
[34]本書では、個人、場所、物などの1つ以上のData Subjectに関する情報、および関連するアクション、アクティビティ、プロセス、および/または特性に関するプライベートで安全な管理および使用のためのさまざまなシステム、方法、およびデバイスを開示します。本書で説明するシステム、方法、およびデバイスは、データに関連する要素を独立属性または依存属性にリンクし、データに関連する要素を独立属性または依存属性に分離することにより、Data Subject、アクション、アクティビティ、プロセス、および特性に関連するデータを抽象化できます。本開示の目的上、属性とは、個人、場所、物、および関連するアクション、アクティビティなどのデータ主体を直接または間接的に識別するために、独立してまたは他のデータ要素と組み合わせて使用できるデータ要素を指します。
Data Subjectには、固有の属性または属性の組み合わせがある場合があることに注意してください。（たとえば個々のデータ主体の社会保障番号、およびData Subjectが他のデー

タ主体と共有する属性または属性の組み合わせ。）
場合によっては、属性は、Data Subjectまたは関連するアクション、アクティビティ、プロセス、特性の電子またはデジタル表現である場合があります。
同様に、属性はData Subjectまたは関連するアクション、アクティビティ、プロセス、および/または特性に関連する情報またはデータの電子またはデジタル表現である場合があります。
属性の分離やリンク、再配置、定義、初期化、結合や拡張により、特定のデータ主体やグループ、関連するアクション、アクティビティ、プロセス、特性に関する属性の組み合わせを形成できます。
Data Subject、アクション、アクティビティ、プロセスは特性に関して、属性の組み合わせには、属性の任意の組み合わせ、および属性に追加または結合される他のデータが含まれる場合があります。
さらに、属性またはデータ属性の組み合わせはData Subjectを識別できますが、それはData Subjectではありません。-属性またはデータ属性の組み合わせによって識別される個人、法人は、その属性の組み合わせの対象であり、彼/彼女が興味を持っているため、それに関して関連当事者と見なされる場合があります。または、上記の属性またはデータ属性の組み合わせとの関連付けをされる場合があります。
【００３５】
[35] いくつかの実施形態では、クライアントサーバ構造またはアーキテクチャを利用して企業全体、オンプレミスまたはパブリッククラウド、プライベートまたはパブリックハイブリッドクラウド、または上記の任意の組み合わせ流事ができて、それ自体が仮想、論理、または物理であり得る1つ以上のプライベートクライアントに機能および/またはサービスを提供することができる。
データ主体デバイスに常駐する可能性のあるこれらのプライバシークライアント、サービスプロバイダーデバイス上で、クラウドネットワークを介してアクセス可能であり、クラウドネットワーク内に存在するか、同じコンピューティングデバイス上に存在します。
プライバシーサーバーは、ハードドライブ上のデータベースまたは、プライバシーサーバーに関連付けられた他のメモリ要素に保存されているデータ属性、Data Subjectの関連付け情報と対話することにより、そのような機能およびサービスの要求を開始する場合があります。例えば、データ属性は、1つまたは複数のプライベートクライアントからの機能およびサービスの要求に応じてデータベースに結合されたプライバシーサーバーによって、独立属性または依存属性にリンクされるか、独立属性または依存属性に分離されます。
注意すべきことは、本発明の実装は、単一のコンピュータまたはコンピューティングデバイスをプライベートサーバおよびクライアントの両方として使用し、他の実装は、1つまたは複数の場所にある1つまたは複数のコンピュータまたはコンピューティングデバイスをプライベートサーバとして使用します。
以下に限定されないが、本明細書で説明される特徴、機能、およびプロセスのうちの1つまたは複数を実行するために、複数のシステムモジュールを使用することができる。属性の組み合わせに必要な属性を決定および変更します。
DDID使用の追跡。既存のDDIDの期限切れまたは再割り当て。特定のアクション、アクティビティ、プロセス、または特性に関連する、または必要なデータの関連付けを有効化または提供します。
【００３６】
[36]実施形態ではこれらのモジュールは以下のように構成されたプライバシーサーバの抽象化モジュールを含みます。：
1つの属性を少なくとも1つのデータサブジェクト、アクション、アクティビティ、プロセス、および特性に動的に関連付けます。
特定のアクション、アクティビティ、プロセスまたは特性に関連する、または必要な必須属性を決定および変更します。 DDIDを生成、保存、および少なくとも1つのデータ属性に割り当てて、TDRを形成します。

TDRのDDIDコンポーネントを使用して、TDRに所定の有効期限を割り当てます。
【００３７】
[37] これらのシステムモジュール、および必要に応じて本書に開示される他のモジュールはプライバシーサーバコンピュータのプロセッサによって実行されるプログラムコード、またはプライバシーサーバコンピュータと通信する別のコンピュータで実装できる。
プログラムコードは、プロセッサによりアクセス可能なコンピュータ可読媒体に保存することができる。コンピュータ可読媒体は、揮発性でも不揮発性でもよく、取り外し可能または取り外し不能でもよい。
コンピュータ可読媒体は、RAM、ROM、ソリッドステートメモリ技術、消去可能プログラマブルROM（「EPROM」）、電気的消去可能プログラマブルROM（「EEPROM」）、CD-ROM、DVD、磁気であり得るが、これらに限定されない。カセット、磁気テープ、磁気ディスクストレージ、またはその他の磁気または光学ストレージデバイスとする。
特定の実施形態では、プライバシークライアントは、「スマート」デバイス、スマートフォン、タブレット、ノートブック、デスクトップコンピューターに常駐または実装され、プライベートクライアントは、プライベートクライアントからの情報の要求を処理して応答する1つ以上のプライベートサーバーと通信します。
（データ属性、属性の組み合わせ、やデータ属性とデータ主体の関連付けに関するリクエスト、例えば、Bluetooth、NFC、WiFi、3Gなどのさまざまなプロトコルを介して他のデバイスまたはネットワークに一般的に接続され、ある程度対話的かつ自律的に動作できるウェアラブル、可動、または不動の電子デバイスなど。）
【００３８】
[38]本発明の一実施形態では、属性および属性の組み合わせに関連付けられたDDIDは、範囲と期間が制限される場合があります。
さらに、DDIDは再割り当て可能であり、DDIDは異なる時点で複数のデータ主体または複数のアクション、アクティビティ、プロセス、または特性を参照できます。
DDIDは、TDRとその中に含まれるデータの適時性と顕著性を維持しながら、データトレイルをさらに抽象化し、希釈または減衰するために、構成可能なベースで再割り当て可能です。
【００３９】
[39]例えば、Data Subjectに関連して特定のアクション、アクティビティ、プロセス、または特性に関連する、または必要なすべてのデータ属性を保存、送信、または処理するのではなく、本発明の実施形態は、関連付け機能によって抽象化の初期層を導入してもよい。
例えば、各TDRに関連データ属性の一部のみを含めることにより。
このようにして、Data Subjectに関連するデータ属性は、一見無関係なTDR内で関連付けが解除される場合がありますが、
どの2つ以上のTDRを相互に関連付ける必要があるかを知るには、1つ以上のAKsへのアクセスと使用が必要です。TDRに含まれるまたは参照されるデータ属性のプライバシー、匿名性、およびセキュリティは、置換機能によってさらに改善または強化される場合があります。
（たとえば1つ以上のTDRに含まれるデータ属性をDDIDで置き換えることにより、1つ以上のRKにアクセスして使用し、ルックアップテーブルを使用して1つ以上の値を決定できるようにする置き換えられたデータ要素など）
TDR内に含まれる、または参照されるデータ属性のプライバシー、匿名性、およびセキュリティは、暗号化、トークン化、仮名化、削除などの他の既知の保護技術を使用することにより、さらに改善または強化できます。または、キーを第2レベルまたはnレベルのDDIDに置き換えて、抽象化の追加レイヤーを導入します。
【００４０】
[40]両方の時：
AKを要求するための、Data Subject、アクション、アクティビティ、プロセス、および

特性に関連するデータ属性の関連付け解除。
データ主体、アクション、アクティビティ、プロセス、および特性に関連するデータ属性の置換。
RKを必要とするため、有効なプライバシーレベル、匿名性、およびセキュリティは、DDIDに関連付けられた方法および頻度に基づいて強化されます。問題のデータ属性が変更され、変更可能です。
本発明の例示的な一実施形態では、分離および置換の目的でDDIDを割り当て、それらの最初に割り当てられた値を保持することができる。-永続的な割り当て。 本発明の別の例示的な実施形態では、DDIDは、関連付け解除、置換の目的で割り当てられ、値がアドホックベースで変更されるまで「アドホック変更可能性」まで最初に割り当てられた値を保持することができる。
本発明のさらに別の例示的な実施形態では、DDIDは、関連付け解除および置換の目的で割り当てられ、ランダム、固定、可変、または他の動的ベースに基づいて値が変更されるまで最初に割り当てられた値を保持することができる-「動的可変性」
【００４１】
[41] 本発明の実施形態は、システム内の識別参照を、本発明の1つまたは複数の実施形態と統合または通信することができる外部ネットワーク、インターネット、イントラネット、およびコンピューティングデバイスに置き換えることにより、抽象化の追加層を作成することができる。
そのため、ルックアップテーブルへのアクセスと使用を可能にし、1つ以上の外部ネットワーク、インターネット、イントラネット、および1つ以上のDDIDで置き換えられたコンピューティングデバイスのIDを特定するには、1つ以上のRKとAKが必要です。
【００４２】
[42]組み合わせてTDRを作成するDDIDの変更可能で再割り当て可能な特性により、TDRの受信者は、意図された時間に意図された目的のためにTDRに含まれる情報を利用できます。
これは、アソシエーションキー（一見無関係なTDRに含まれる情報の意味を理解するために、TDRをつなぐために必要な場合がある。）および置換キー（送信される一時的のDDIDによって表される情報の値を知るために必要な場合がある） TDRの一部としての第三者は、一時的に限られた有用性しか持たない場合がある。
AKとRKが関連の情報を公開しないよう意図され、目的と意図された時間が適用されなくなると、TDRのDDIDコンポーネントがData Subjectまたは他の管理者によって変更される可能性があるため、有用性は一時的に制限されます。
逆に、AKとRKによって明らかにされた関連情報は、データの追加の二次利用をサポートするために時間とともに変化する可能性があります。
【００４３】
[43]一例ではメンテナンスモジュールを使用して、特定のDDIDの特定の時点での関連付けに関する情報を、システムによってプライバシーサーバーに関連付けられる。
ただし、支配組織以外の当事者または支配組織によって承認された当事者はアクセスできません（この期間はタイムキー（TK）、その他で表される場合があります）。 一例では、プライバシーサーバーのメンテナンスモジュールと関連するデータベースは、DDIDと属性の組み合わせとのすべての関連付けを保存および保持します。
したがって、システムは、安全なデータ交換とデータ属性、属性の組み合わせ、およびTDRの否認防止を提供し、厳格なプライバシー、匿名性、およびセキュリティ基準を満たしながら、より安全なデータ関連の収集、使用、調査、および分析を促進します。
【００４４】
[44]たとえば、プライバシーサーバーと関連データベースの検証モジュールは、集約されたデータプロファイルに組み込まれた情報とDDIDの整合性の検証と検証を可能にする認証済みデータ構造を提供します。
【００４５】

[45]別の例では、本発明の実施形態の認証モジュールを使用して、特定の時間にData Subject、アクション、アクティビティ、プロセスまたは特性に関して続行する権限を匿名で検証することができる。 TDR割り当てを介して配置します。

【００４６】

[46] TDRに含まれるTDRとDDIDは、暗号化、トークン化、仮名化、削除などの既知の保護技術の高度なキーとしても使用できます。

認証モジュールは、TDR、DDID、非公開の関連データサブジェクト、属性、属性の組み合わせ、または関係者が確認されない限り、暗号化、トークン化、仮名化、削除など、TDRのコンテンツの保護技術を解除するために必要なキーを保留するために使用できます。

指定された時間、場所で、DDIDとTDRの確認、およびパスワード確認、多要素認証または類似の手段などの既知の確認技術により、希望するアクション、アクティビティ、プロセスまたは特性に関して参加する権限を与えられている。

【００４７】

[47]他の例ではアクセスログモジュールが提供され、アクセスログモジュールは、システムまたはプライバシーサーバーのエラーの場合に事後の裁判分析を可能にする情報を収集および保存できる。

【００４８】

[48]本発明の一実施形態の一態様によれば、本明細書では、電子情報の制御された配信を提供するコンピュータ実装方法が開示される。

一例では、方法は、コンピューティングデバイスでデータを受信するステップまたは動作を含み得る。

データの1つ以上の属性を識別します。

コンピューティングデバイスを介してDDIDを選択する。

選択したDDIDを1つ以上のデータ属性に関連付けます。

少なくとも選択されたDDIDと1つ以上のデータ属性から時間的に一意のデータ表現（TDR）を作成する。

【００４９】

[49]たとえば、DDIDを選択するステップには、時間的に一意の動的に変化するDDIDの生成、DDIDとして機能するシステム外部で作成された時間的に一意の動的に変化する値の受け入れまたは変更が含まれます。

【００５０】

[50]本書の目的上、「動的に変化する」という言葉は、Data Subject、アクション、アクティビティ、プロセス、または特性に関して割り当てられたDDIDを意味します。

（a）（i）所定の時間の経過による経時変化

（ii）柔軟な時間の経過

（iii）DDIDが作成された目的の期限切れ

（iv）Data Subject、行動、活動、プロセスまたは特性に関連する仮想または現実世界の場所の変更。

（b）同じまたは類似のデータ主体、アクション、アクティビティ、プロセス、特性に関して異なる時期、時間。

【００５１】

[51] 本書の目的のために、「時間的意思を持った物」は、DDIDをData Subject、行動、活動、プロセスまたは特性に割り当てる期間が無限ではないことを意味する。

Data Subject、アクション、アクティビティ、プロセス、または特性へのDDIDの割り当て期間が個別の時点で終了する場合、割り当ての終了時間に関する情報は既知であり、本発明の特定の実装では、 DDIDと前述のData Subject、アクション、アクティビティ、プロセス、または特性の間の関係または接続を識別するために使用されます。

【００５２】

[52]本書の目的上「ポリシー」という用語は、データセット（たとえば、任意の数の次元のデータセット）に対して、数学、論理、サンプリング、またはその他の機能をプログラ

ムで実施する方法を意味します。
これは、公開鍵暗号化、k匿名性、l多様性、「ノイズ」、差別的プライバシーの導入を含むがこれらに限定されないプライバシー強化技術（「PET」）を有効にするための施行メカニズムと同等以上です。
【００５３】
[53] 本書の目的上、「Non-Attributing Data Element Value」（NADEV）という用語は、A-DDIDが再識別されたときに明らかになる値、または特定のA- DDIDが再識別されました。
NADEVは、データセットの要素の派生または関連バージョンまたはサブセットを作成して、1つ以上のPETまたは他のプライバシーおよびセキュリティ強化の方法論のデータセットへの適用を反映してデータセットの選択された部分の事を言う。
たとえば、データセットにデータ被験者の心拍数の値が毎分65ビート含まれていると仮定すると、データの値は2つのNADEVに一般化できます。
たとえば、「1分あたり61～70拍の範囲」を指定するものと、単に「通常」を指定するもの。-各NADEVは、毎分65ビートの真のデータ値を開示せず、データ主体のアイデンティティを開示せずに、独立して個別に抑制または公開できます。
【００５４】
[54]別の例でこの方法は、選択されたDDIDと1つまたは複数のデータ属性との間の関連付けを失効させることもある。
また他の例では、選択されたDDIDが異なるデータ属性または時間キー（TK）またはその他の属性の組み合わせに関連付けられていた期間の情報を、コンピューティングデバイスがアクセス可能なデータベースに保存することができます。
【００５５】
[55]別の実施形態には、DDIDと初期データ属性との関連付けの有効期限後に、選択されたDDIDを他のデータ属性または属性の組み合わせに再関連付けすることも含まれる。
【００５６】
[56]一例では、DDIDの有効期限は所定の時間に発生します。または、有効期限は所定のイベント、目的、またはアクティビティの完了後に発生する場合があります。
他にもDDIDは、所定の期間、場所でのみ使用が許可されます。
【００５７】
[57]別の例では、
この方法には、1つ以上のデータ属性、属性の組み合わせ、およびTDRに関連付けられたDDIDを変更することが含まれます。
DDIDの変更は、ランダムまたはスケジュールに基づいて発生するか、または所定のアクティビティの目的とイベントの完了後に発生する可能性があります。
【００５８】
[58]本発明の別の実施形態の別の態様によれば、本明細書に開示されるのは、ネットワークを介したトランザクションを容易にする方法でありプライバシーサーバにてクライアントデバイスから要求を受信して実行する動作です。これはネットワークを介したアクティビティで要求されたアクティビティを完了するために、データベース内の複数のデータ属性または属性の組み合わせのどれが必要かを判断します。
DDIDの作成と受け入れ; DDIDを決定されたデータ属性に関連付けて、結合された時間的に一意のデータ表現（TDR）を作成します。
要求アクティビティを実行または開始するために、少なくとも1つのネットワークデバイスが結合した時間的に一意のデータ表現（TDR）にアクセスできるようにします。実行されたアクティビティに関連する追加情報を含む変更された時間的に一意のデータ表現（TDR）を受信します
変更された時間的に一意のデータ表現（TDR）、DDIDとデータサブジェクトの関連付け情報をメモリデータベースに保存する。
【００５９】

[59]例においてネットワークデバイスは、インターネットサービスプロバイダー、商人またはサービスプロバイダーにより運営されるサーバー、モバイルプラットフォームプロバイダーにより運営されるサーバー、またはクラウドコンピューティング環境内のサーバーを含む。

【００６０】

[60]本発明の別の実施形態の別の態様によれば、本書で開示されるのは、電子情報の制御された配信を提供する方法である。

一例では、この方法は、ネットワークを介してアクティビティを実施するためにプライベートサーバーでリクエストを受信することを含み得る。要求を満たすために必要であると判断されたプライバシーサーバーにアクセス可能なデータベースにあるデータの属性を選択しここで、必要と判断されないデータの他の属性は選択されません。選択した属性へのDDIDの割り当ての割り当てまたは受け入れ、プライバシーサーバーの抽象化モジュールで適用される属性の組み合わせにおいてDDIDは未選択の属性を明らかにしません。 DDIDが割り当てられた時間を記録します。

要求されたアクティビティが完了したという指示を受信します。 DDIDと、プライバシーサーバーで適用される決定された属性と属性の組み合わせを受信します。属性は、実行されたアクティビティに関する情報を含むように変更されます。

【００６１】

[61]一例でこの方法は、ＴＤＲ内に含まれる選択された属性の組み合わせのうちの１つまたは複数に追加のＤＤＩＤを割り当てることも含み得る。

別の例では、方法は、記録された時間を反映する時間キー（TK）を使用して、DDID、データ属性の組み合わせ、またはデータサブジェクトのアイデンティティと再関連付けすることを含みます。

このメソッドには、DDIDを他のデータ属性に再割り当てし、DDIDが再割り当てされた時刻を記録することも含まれます

実施されたアクティビティが完了した時間を記録し、DDIDと、それらが適用される決定された属性と組み合わせをプライバシーサーバーで受信します。

【００６２】

[62]別の例によれば、本書ではデータが少なくとも１つの属性を含む、データセキュリティを改善するコンピュータ実装方法が開示される。

一例では、この方法は、少なくとも１つの属性をＤＤＩＤに関連付けて、時間的に一意のデータ表現（ＴＤＲ）を作成することを含む。

ここで、一時的に一意のデータ表現（TDR）は、データ属性へのアクセスを、（たとえばオンラインWebサイトからの商品の購入を完了するなど）特定のアクションを実行するために必要な属性のみに制限します。

【００６３】

[63]方法は、関連付けキー（ＡＫ）を時間的に一意のデータ表現（ＴＤＲ）に割り当てることを含み得る。

ここでのアソシエーションキー（AK）へのアクセスは、（TDR）への許可されたアクセスに必要です。

【００６４】

[64]別の例では、この方法は、DDIDと少なくとも1つの属性との間の関連付けを失効させることも含み得る。

満了は所定の時間に発生し、所定のイベントおよびアクティビティの完了後に発生する場合がある。別の実施形態では、方法は、ＤＤＩＤと属性との間の関連付けの満了後に、ＤＤＩＤを再関連付けすることを含む。

【００６５】

[65]本発明の別の態様によれば、本書に開示されるのは、電子データセキュリティを改善するためのシステムである。

一例では、システムは属性をデータ主体、アクション、アクティビティ、プロセス、およ

び特性に動的に関連付けるように構成されたモジュールを含むことができます。
DDIDを生成または受け入れるように構成され、さらにDDIDを少なくとも1つのデータ属性に関連付けるように構成されたモジュールです。 DDIDに関連するアクティビティを追跡するように構成されたモジュール、アクティビティによって生成された追加の電子データをDDIDに関連付けるように構成されています。
この方法はまた、DDIDが適用可能なタイムキー（TK）またはその他によって反映される異なるデータ属性または属性の組み合わせに関連付けられた1つまたは複数の期間に関する情報をデータベースに保存することを含みます。

【００６６】

[66]本発明の別の実施形態の別の態様によれば、本書で開示されるのは、ネットワークを介して安全なプライベート活動を実施するためのデバイスである。
一例では、デバイスは、プログラムモジュールを実行するように構成されたプロセッサを含むことができます。（プログラムモジュールは少なくともプライバシークライアントを含む。）;プロセッサに接続されたメモリ
;ネットワークを介してデータを受信するための通信インターフェース
プライバシークライアントは、プライベートサーバーからネットワーク上でアクティビティを実行するために必要なDDIDおよび関連データ属性を含む、時間的に一意のデータ表現（TDR）を受信するように構成されています。

【００６７】

[67]デバイスを使用して行われたアクティビティをキャプチャし、行われたアクティビティを時間的に一意のデータ表現（ＴＤＲ）に関連付けるようにさらに構成され得る。
別の例では、プライバシークライアントは、キャプチャされたアクティビティと時間的に一意のデータ表現（TDR）をプライバシーサーバーに送信するように構成されてもよい。
一例では、プライバシークライアントは、モバイルアプリケーションとしてモバイルデバイス上に常駐してもよい。
別の例では、プライバシークライアントは、クラウドベースのアプリケーションとしてネットワークに常駐し、ネットワークを介してアクセス可能です。
またプライバシークライアントは、同じコンピューティングデバイスに常駐する場合があります。

【００６８】

[68]別の例では、デバイスは、モバイルデバイス上のジオロケーションモジュールも含むことができ、時間的に一意のデータ表現（TDR）はジオロケーションモジュールからの情報で修正される。
そして、時間的に一意のデータ表現（ＴＤＲ）は、デバイスのアイデンティティに関する情報へのアクセスを制限する。
デバイスには、ユーザーが特定の時間的にTDRに関連付けられたDDIDまたはデータ属性を変更するオプションを含むTDRを変更できるように構成されたユーザーインターフェイスも含まれる場合があります。これは、モバイルデバイスへの所定の物理的、仮想的または近接内の他のネットワークデバイスとのみ時間的にTDRを共有するための選択可能なオプションを含む。

【００６９】

[69]例では、デバイスは、共有された時間的に一意の表現（TDR）に応答して、モバイルデバイスの物理的、仮想的、または論理的な位置に基づいて、ターゲットを絞った広告またはマーケティング情報を受信します。ここで、共有されるTDRには、人口統計情報、時間情報、地理位置情報、サイコグラフィック情報とその他の形式が含まれます。
例では、共有の時間的にTDRは、モバイルデバイスを使用して行われた、または行われた購入トランザクションに関連する情報を含み、前回のまたは所望の購入トランザクションに基づいてターゲット広告またはマーケティング情報を受信します。
このようにして、ベンダーは、近くのユーザーと潜在的な顧客の関連する特性をほぼ即座に知ることができます。そのようなユーザーの身元を知ることも学習することもありませ

ん。ユーザー/潜在的な顧客のプライバシー/匿名性を損なうことなく、リアルタイムで行います。

【００７０】

[70] 本発明の別の実施形態の別の態様によれば、本明細書に開示されるのは、電子データのプライバシーおよび匿名性を提供するためのシステムである。

一例では、システムは、ユーザーデバイス上で動作する第1のプライバシークライアントを有する少なくとも1つのユーザーデバイスを含む。プロバイダーのデバイス上で動作する第2のプライバシークライアントを有する少なくとも1つのサービスプロバイダーデバイス。

ネットワークに接続された少なくとも1つのプライバシーサーバー。プライバシーサーバーは、第1および第2プライバシークライアントと通信します。

プライバシーサーバーは、データ属性の組み合わせを電子的にリンクし、分離する抽象化モジュールを含み、抽象化モジュールはDDIDをデータ属性と属性の組み合わせに関連付けます。

【００７１】

[71] 例では、プライバシーサーバは、前ＤＤＩＤの１つまたは複数を生成を受け入れる認証モジュールを含むことができる。

別の例では、プライバシーサーバーは、DDIDとそれらの属性の組み合わせのを保存するメンテナンスモジュールを含んでもよい。

また別の例では、プライバシーサーバーは、データ属性、属性の組み合わせ、およびDDIDの整合性を検証する検証モジュールを含む場合があります。

【００７２】

[72] 別の例では、プライバシーサーバーは、1つ以上のエラーが発生した場合に1つ以上の事件後の法医学分析で使用するためのDDIDおよびデータ属性に関する情報を収集および保存するアクセスログモジュールを含み得る。

【００７３】

[73]一例では、DDIDは所定の時間後に失効し、DDIDの失効後、抽象化モジュールはDDIDを別のデータ属性を別のデータ主体に割り当てる。

【００７４】

[74]本発明の別の実施形態の別の態様によれば、本明細書に開示されるのは、以下のための方法、コンピュータ可読媒体、およびシステムである。

（i）所定のデータセットの少なくとも1つの次元またはサブセットに対して1つ以上のポリシーを技術的に実施することにより、多次元データセットを変換する。

（ii）たとえば、1つまたは複数のA-DDIDを作成することにより、元の変換前、変換中、変換後にサブセクション（i）のデータセットを変換します。

（iii）Just-In-Time-Identity（JITI）またはその他のタイプのアクセス制御ベースのキーを使用して、データセットのすべてまたは一部へのアクセスを制限するポリシーを技術的に実施します。

（iv）パラメトリックまたはノンパラメトリック手法、数学的手法を適用して、変換されたデータセット内の情報をさまざまな業界に適したまたは業界に関連する価値指標に従ってランク付けまたは評価できるようにする。

データセットに匿名化を提供する際の有効性の定量的および/または定性的尺度の観点からランク付けまたは評価することができます。

【００７５】

[75]本発明の別の実施形態の別の態様によれば、コンピュータ可読媒体、および人工知能アルゴリズムを使用して、データセットのスキーマ、メタデータ、構造などを分析してアルゴリズムアクションを決定するシステム 事前に決定されたプライバシーポリシーに準拠するようにデータセットを不明瞭化、一般化、またはその他の方法で変換するために使用されます。

【００７６】

[76]本発明の別の実施形態の別の態様によれば、本書に開示されるのは、例えばネットワークまたはアプリケーションプログラムを介して「サービスとして」プライバシーポリシーを提供するための方法、コンピュータ可読媒体、およびシステムである。データの価値を最大限に引き出す方法、つまりデータの使用を可能にすると同時にデータのセキュリティとプライバシーを強化する方法で、規制、契約上の制限へのコンプライアンスを促進するためにユーザーに提供します。

【００７７】

[77]本発明の別の実施形態の別の態様によれば、本書に開示されるのは
コンピュータで読み取り可能なメディア、および分散型で保存されたユーザー情報に電子データのプライバシーと匿名性を提供するシステム（たとえば、許可のないシステム間、またはブロックチェーンなどの不変で検証可能な分散台帳技術の使用）の方法である。

【発明の効果】

【００７８】

[78]本開示の他の実施形態が本書に記載されている。様々な実施形態の特徴、ユーティリティ、利点は以下のより詳細な説明から明らかになる。

【図面の簡単な説明】

【００７９】

【図１】図１は、プライベートサーバーを含むシステムのブロック図の例を示している。

【図１Ａ】図１Ａは、本発明が外部データベースと相互作用するサービスとして提供される、プライベートサーバを含むシステムのブロック図の例を示している。

【図１Ｂ】図１Ｂは、データ属性、属性の組み合わせに関して、DDIDの割り当て、適用、期限切れ、リサイクルが発生するさまざまな方法を示しています。

【図１Ｃ－１】図１Ｃ－１は、信頼される側の観点から、プライバシーサーバーを含むシステムの潜在的な入力および出力フローを示しています。

【図１Ｃ－２】図１Ｃ－２は、データ主体の観点から、プライバシーサーバーを含むシステムの潜在的な入力および出力フローを示しています。

【図１Ｄ】図１Ｄは、ネットワーク血圧モニターに関連したDDIDの使用例を示しています。

【図１Ｅ】図１Ｅは、性感染症（ＳＴＤ）の患者にサービスを提供することに関連したＤＤＩＤの使用例を示している。

【図１Ｆ】図１Ｆは、クーポンの提供に関連したＤＤＩＤの使用の例を示している。

【図１Ｇ】図１Ｇは、血圧レベルを見ている医師に関連したＤＤＩＤの使用例を示している。

【図１Ｈ】図１Ｈは、教育関連情報において動的データ難読化をもたらすためにＤＤＩＤを使用する例を示している。

【図１Ｉ】図１Ｉは、Disassociation Level Determination (DLD)を実行し、匿名性測定スコア（ＡＭＳ）を作成するプロセスの例を示す。

【図１Ｊ】図１Ｊは、例示的な計算された匿名性測定スコアを示している。

【図１Ｋ】図１Ｋは、特定の計算された匿名性測定スコアについてData Subjectが必要とする同意／関与のレベルの例示的なカテゴリーを示している。

【図１Ｌ】図１Ｌは、緊急応答の領域でのＤＤＩＤの使用の例を示している。

【図１Ｍ】図１ＭはJust-In-Time-Identity (JITI)対応のセキュリティおよびプライバシーの使用例を示している。

【図１Ｎ】図１Ｎは、Just-In-Time-Identity (JITI)対応のセキュリティおよびプライバシーの使用例を示している。

【図１Ｐ－１】図１Ｐ－１は、静的匿名識別子の使用例を示している。

【図１Ｐ－２】図１Ｐ－２は、Just-In-Time-Identity (JITI)対応セキュリティおよびプライバシーの使用例を示している。

【図１Ｑ】図１Ｑは、医療サービスの文脈におけるJust-In-Time-Identity (JITI)対応のセキュリティおよびプライバシーの使用の例を示している。

【図１Ｒ】図１Ｒは、Just-In-Time-Identity (JITI)対応のセキュリティおよびプライバシーを実装するためのシステムの例を示している。
【図１Ｓ】図１Ｓは、Just-In-Time-Identity (JITI)対応のセキュリティおよびプライバシーを実装してＯｐｅｎＨｅａｌｔｈプラットフォーム（ＯＨ）をサポートするシステムの例を示している。
【図１Ｔ】図１Ｔはデータリスクを軽減するポリシー管理およびアクセス制御を実装するためのシステムの例を示している。
【図１Ｕ】図１Ｕは様々なデータリスク除去スキームの例を示している。
【図１Ｖ】図１Ｖは、購入のために利用可能にされた様々なデータリスク除去ポリシーの市場の一例を示している。
【図１Ｗ－１】図１Ｗ－１は、インテリジェントポリシーコンプライアンスエンジンの例を示しています。
【図１Ｗ－２】図１Ｗ－２は、インテリジェントポリシーコンプライアンスエンジンの使用に関する例示的なフロー図を示している。
【図１Ｘ－１】図１Ｘ－１は、シムを介してデータプライバシーサービスを提供するための例示的なシステムを示している。
【図１Ｘ－２】図１Ｘ－２は、ウェブブラウザ、デバイス、または他のセンサーからのインラインサービスを介してデータプライバシーサービスを提供するための例示的なシステムを示している。
【図１Ｙ－１】図１Ｙ－１は、データの匿名化システムを提供するクラウドベースのプラットフォームとアプリケーションを示しています。
【図１Ｙ－２】図１Ｙ－２は、匿名化されたデータを再識別するシステムを提供するクラウドベースのプラットフォームとアプリケーションを示しています。
【図１Ｙ－３】図１Ｙ－３は、抽出、変換、およびロード（ＥＴＬ）アプリケーションと統合するシステムを提供するためのクラウドベースのプラットフォームおよびアプリケーションを示している。
【図１Ｚ－１】図１Ｚ－１は、blockchainベースの技術に基づいて構築された分散型ネットワークを示しており、１つ以上の実施形態に従って、匿名化プライバシー制御を採用することができる。
【図１Ｚ－２】図１Ｚ－２は、１つ以上の実施形態による、blockchainベースの技術上に構築された分散ネットワークを示している。
【図１Ｚ－３】図１Ｚ－３は、１つ以上の実施形態による、blockchainベースの技術上に構築された分散ネットワークを示し、匿名化プライバシー制御が採用され得る。
【図２】図２は、ＴＤＲの生成および使用の例を示している。
【図３】図３は、ＴＤＲの生成および使用の例を示している。
【図４】図４は、ＴＤＲの生成および使用の例を示している。
【図５】図５は、システムの関連付け機能および置換機能による異なる抽象化レベルを有する２つの例示的な属性の組み合わせを示している。
【図６】図６は、属性の組み合わせを選択し、データを抽象化または匿名化するためのＴＤＲを生成し、データを再関連付けまたは匿名化するプロセスの例を示している（サンプル制御エンティティおよびシステムの観点から）
【図６Ａ】図６Ａは、１つ以上の外部データベースから属性を受信し、データを抽象化または匿名化するためにＴＤＲを生成し、その後、再関連付けまたは匿名化するプロセスの例を示す（サンプル制御エンティティおよびシステムの観点から）。
【図６Ｂ】図６Ｂは、組織の外部で識別可能な方法で明らかにするには機密性が高すぎると考えられるデータ要素に動的匿名性を提供するプロセスの例を示しています。
【図７】図７は、図６のプロセスの例を（受信者エンティティの観点から）示している。
【図８】図８は、権限を検証するプロセスの一例を示している。
【図９】図９は、検証されない限り、キー保護情報を保留するプロセスの例を示しています。

【図１０】図１０は、関係者の関心を匿名で分析するプロセスの例を示している。
【図１１】図１１は、DDIDと、生成、送信、追跡された属性の組み合わせを含む、関係者、サービスプロバイダー、プライバシーサーバー間の相互作用のさまざまな例を示しています。
【図１２】図１２は、DDIDと、生成、送信、追跡された属性の組み合わせを含む、関係者、サービスプロバイダー、プライバシーサーバー間の相互作用のさまざまな例を示しています。
【図１３】図１３は、DDIDと、生成、送信、追跡された属性の組み合わせを含む、関係者、サービスプロバイダー、プライバシーサーバー間の相互作用のさまざまな例を示しています。
【図１４】図１４は、DDIDと、生成、送信、追跡された属性の組み合わせを含む、関係者、サービスプロバイダー、プライバシーサーバー間の相互作用のさまざまな例を示しています。
【図１５】図１５は、DDIDと、生成、送信、追跡された属性の組み合わせを含む、関係者、サービスプロバイダー、プライバシーサーバー間の相互作用のさまざまな例を示しています。
【図１６】図１６は、DDIDと、生成、送信、追跡された属性の組み合わせを含む、関係者、サービスプロバイダー、プライバシーサーバー間の相互作用のさまざまな例を示しています。
【図１７】図１７は、DDIDと、生成、送信、追跡された属性の組み合わせを含む、関係者、サービスプロバイダー、プライバシーサーバー間の相互作用のさまざまな例を示しています。
【図１８】図１８は、DDIDと、生成、送信、追跡された属性の組み合わせを含む、関係者、サービスプロバイダー、プライバシーサーバー間の相互作用のさまざまな例を示しています。
【図１９】図１９は、複数のサービスプロバイダーがアクセスできる属性の組み合わせと、各サービスプロバイダーがプライバシーサーバーに再送信する属性の組み合わせの例を示しています。
【図２０】図２０は、サービスプロバイダーに送信され、サービスプロバイダーから再送信されたすべての属性の組み合わせを含む、関係者がアクセスできるデータを示しています。
【図２１】図２１は、制御エンティティとして機能し、さまざまなベンダーに情報を提供するサービスプロバイダーが、各ベンダーに、それに割り当てられたサービスを実行するのに必要な属性の組み合わせのみを提供する方法を示す。
【図２２】図２２は、制御エンティティとして機能し、さまざまなベンダーに情報を提供するサービスプロバイダーが、各ベンダーに、それに割り当てられたサービスを実行するのに必要な属性の組み合わせのみを提供する方法を示す。
【図２３】図２３は、インターネット広告の分野におけるＤＤＩＤの実装の一例を示している。
【図２４】図２４は、ヘルスケアの分野におけるＤＤＩＤの実装の例を示している。
【図２５】図２５は、ヘルスケアの分野におけるＤＤＩＤの実装の例を示している。
【図２６】図２６は、ヘルスケアの分野におけるＤＤＩＤの実装の例を示している。
【図２７】図２７は、動的に変更可能な一時的に一意の識別子（ＤＤＩＤ）を動的に作成、割り当て、変更、再割り当て、および使用するための技術を実装するためのプログラマブルデバイスの例のブロック図を示す。
【図２８】図２８は、ＤＤＩＤを動的に作成、割り当て、変更、再割り当て、および使用するための技術を実装するためのプライバシークライアントおよびプライバシーサーバーのネットワークを示すブロック図を示す。
【発明を実施するための形態】
【００８０】

[131]本書では、個人、場所、または物、ならびに関連する行動、活動、プロセス、および特性などの１つまたは複数のData Subjectに関する情報のプライベートかつ安全な管理および使用のための様々なシステム、方法、およびデバイスが開示される。本書に記載されているシステム、方法、およびデバイスは、データ主体および関連するアクション、アクティビティ、プロセス、特性に関連するデータを独立した属性および依存する属性と分離要素にリンクすることにより、データ主体および関連するアクション、アクティビティ、プロセス、特性に関連するデータ属性を抽象化します。その後、DDIDを選択データ属性または選択属性の組み合わせに関連付けて、TDRを作成できます。
このようにして、本発明の実施形態を利用して、人、場所、物、行動、プロセス、特性などのData Subjectにデータセキュリティ、プライバシー、匿名性、および正確さを提供することができる。blockchain技術によって提供されるような、不変、検証可能、分散型台帳の形で、分散ストレージシステム全体に保存されます。本書では、本発明の様々な実施形態が開示されている。

【００８１】

[132] Dynamic Anonymity /サークルオブトラスト（CoT）

【００８２】

[133] Dynamic Anonymityは、静的匿名性は幻想であり、静的識別子の使用には根本的に欠陥があるという原則に基づいています。
Dynamic Anonymityシステムは、さまざまな段階で再割り当て可能な動的識別子（DDID）を動的にセグメント化し、データストリーム要素に適用します。（注：動的セグメンテーションにはタイムラプスが含まれる場合がありますが、アクティビティ、場所、および主題によって決定される可能性が高くなります）
これにより、データストリーム要素を再ステッチする信頼できる当事者の能力や他のユーザーの能力を維持しながら、送信中、使用中、休憩中に意図せずに情報が共有されるリスクを最小限に抑えます。

【００８３】

[134]図1C-1に示すように、クリアテキストプライマリーキーを信頼の輪（「CoT」）内で内部的に使用して、Data Subject、アクション、アクティビティ、プロセス、特性を識別できます。ただし、これらのキーはCoTの外部では共有できません。むしろ、Dynamic Anonymityは、以下で構成されている可能性のある信頼の輪の外側で動的に変化し、再割り当て可能な複合キーを使用します。
（i）DDID;
（ii）Data Subject、アクション、アクティビティ、プロセス、および特性に関連付けられたDDID。
このアソシエーションに関する情報は、CoTの外部では利用できない場合があります（データサブジェクト、アクション、アクティビティ、プロセス、特性との接続を表すDDIDに、回復可能な情報が含まれていない場合、再構築できない場合があります。上記の1つまたは複数のData Subject、アクション、アクティビティ、プロセス、または特性に対して、それぞれの場合、接続は切断され、計算は不可能です）。

【００８４】

[135] Dynamic Anonymityは、分散プラットフォームや断片化されたエコシステムでプライバシー、匿名性、個人データ保護機能を強化し、
Data Subjectによって（Data Subjectに代わって）確立されたポリシーに従って、データへの優れたアクセスと使用を提供します。このようにして、クローズドシステムまたは分散システムの使用を選択した人を含むすべての人が、強化されたデータプライバシーと匿名性の恩恵を受けます。

【００８５】

[136] Dynamic Anonymityは、既存のビジネスおよびテクノロジーの慣行を変更することなく、特定の即時の利益をもたらします。 動的に変化する時間的に一意のDDIDを使用すると、現在のシステムとプロセス（Webブラウザーやデータ分析エンジンなど）は、デ

ータ要素間の関係を認識できません。 これらのシステムおよびプロセスは、Data Subjectおよび信頼できるプロキシがCircle of Trust（CoT）を介して明示的に許可している場合を除き、推論、相関、プロファイルまたは結論を作成せずに既存の機能を使用して情報を処理できます。 ただし、DDID、Dynamic Anonymity、Circle of Trust（CoT）の特定の属性と機能を活用する新しいビジネスとテクノロジーの実践から、さらに大きな利点が生まれます。

【００８６】

[137] Dynamic Anonymityは、データ処理の4つそれぞれのポイントで利点があります。

A.データキャプチャ

B.データ送信/保存

C.データ分析。

D.データのプライバシー/匿名管理

各ポイントで、データは、そのデータが関係するData Subjectによって、またはData Subjectに代わって指定されたPERMSに従って保護されます。

【００８７】

[138] A.データキャプチャ

【００８８】

[139]静的識別子がData Subjectに関連するデータのキャプチャに関連付けられるアプリケーションでは、動的匿名性は以下を提供できます。

1.経時的に変化する動的な識別子（DDIDを含む）（時間の経過、目的の変化、活動の一時停止、または仮想的または物理的な場所の変化によってトリガーされる）追跡、プロファイル、またはその他の方法での関連付けを制限するData Subject、アクション、アクティビティ、プロセス、特性を持つデータ。

2.各DDIDから、該当する1つ以上のData Subject、アクション、アクティビティ、プロセス、および/または特性への関連付け。該当するCoT内でのみ保存および認識されます。

3. Dynamic Anonymityは、CoT内のDDIDに関連付けられたデータを保存するオプションの機能も提供します。

【００８９】

[140] Dynamic Anonymityの重要な特徴は、データレコードレベルではなくデータ要素レベル、つまり、データサブジェクト、アクション、アクティビティに関連付けられた個々のデータ要素のレベルでデータ要素を匿名化および分離する機能です。サークルオブトラストは、データ要素とData Subject、アクション、アクティビティ、プロセス、および/または特性間の関係情報を保持し、データによって、データに代わって確立されたプライバシーポリシー、ルールに従って再関連付けを許可します。（本書では「PERMS」と呼ばれることもあります。）

【００９０】

[141]例：検索エンジン

【００９１】

[142]特定の検索エンジンを頻繁に使用する人を例に考察します。

今検索エンジンは、ユーザーに（ブラウザを介して）数か月または数年間持続する「Cookie」またはその他のデジタルフットプリントトラッカーを割り当てます。その後、蓄積され、多くの場合、分析され、さらに複数の関係者によって集約されます。-使用者はData Subjectによる同意を知らず個人を特定できる情報を公開することがよくあります。

【００９２】

[143] Dynamic Anonymityは、検索エンジンの自然な応答を活用して、初めて検索エンジンと対話していると認識された各Data Subjectの新しいCookie /デジタルフットプリントトラッカーを作成できます。

履歴、キャッシュ、Cookie /デジタルフットプリントトラッカー、および関連データを消去すると、検索エンジンはデータサブジェクトの新しいCookie /デジタルフットプリントトラッカーを生成します。

CoTは、Cookie /デジタルフットプリントトラッカーとData Subjectに関する情報を保存でき、オプションでクエリと選択したリンクのリストも保存できます。
【００９３】
[144]このアプローチでは、検索エンジンは、集計データ（トレンド検索用語、Webサイト、広告クリックなど）に引き続きアクセスできます。
ただし、観測データに基づいてData Subjectに関連する推論を引き出すことはできません。Data Subjectによって代わって確立されたプライバシー/匿名ポリシーおよびルールによって許可されている場合、CoTは検索エンジンがより詳細な分析を実行できるようにすることができます。
これは、HTTPプロキシまたはブラウザ拡張機能を使用して実装でき、既存の検索エンジンへの変更（または協力）は不要です
【００９４】
[145]昔、匿名のCookieは、プライバシーとアナリシスの両方をサポートの問題を解決していたはずです。
しかし全部のデータが一緒に格納され、Data Subject（「個人データ」または「PD」）にリンクまたはリンク可能な情報を簡単に生成できるランダムな静的識別子に関連付けられているため、匿名追跡Cookieはこの目標を達成できませんでした。これにより、静的な「匿名」識別子の値を無効化または減衰します。Dynamic Anonymityは、動的に変更および再割り当て可能なDDIDを採用し、結果のDDIDアソシエーションを保存し、Circles of Trust内でキーを覆い隠し、Data Subjectと信頼関係者/サードパーティの参加者間での参加を可能にする独自の相互作用モデルを提供することにより、これらの欠点を克服します。
【００９５】
[146] B.データ送信/保存
【００９６】
[147] CoTは、それぞれが1つ以上の独立したデータストレージ機能を提供する1つ以上のトラステッドパーティと、機密データをこれらのデータストアにセグメント化して送信する安全な手段で構成されます。
【００９７】
[148]またはDynamic Anonymity準拠のアプリケーション開発者は、CoT内にデータサブジェクトとDDIDの関連付けのみを保存し、代わりにDynamic Anonymity定義の手順を使用してデータを不明瞭化、暗号化、セグメント化することを選択できます。コンテキストまたはビジネス価値を失うことなく、アプリケーションが生成または収集した情報を独自の施設に安全に保存できるようにします。
【００９８】
[149]過去に本発明により使用されるものと類似の技術が以下のために使用されてきた。
-セグメントデータ;
-送信中のデータの暗号化と難読化
-保管中の配布、難読化、およびセキュリティの採用
Dynamic Anonymityはこれらの従来のアプローチを次のように改善します。
-動的に変更および再割り当て可能なDDIDを使用して、データ要素（データレコードに対して）レベルでデータを隠します。
-結果のDDIDアソシエーションの保存/信頼の輪内のキーの不明瞭化;
- Data Subjectと信頼関係者/サードパーティの参加者との間の参加を可能にするためのユニークな相互のモデルを提供します。
【００９９】
[150] C.データ分析
【０１００】
[151]データ「クレンジング」（データクリーニングおよびデータスクラブとも呼ばれる）の従来の手法は、主に2つの問題に悩まされています。

【０１０１】
[152] 1.所定のデータクレンジングテクニックは、無効の可能性があります。真剣な努力、または個人データを不明瞭にするための法的に認可された技術の使用にもかかわらず、「クレンジングされた」データからData Subjectと個人データを識別することは可能かもしれません。真剣な努力、または個人データを不明瞭にするために法的に認可された技術を使用しているにもかかわらず、「クレンジングされた」データからデータ主体と個人データを特定することは依然として可能です。
3つの有名な例：
a． 1990年代半ばマサチューセッツグループ保険委員会（GIC）は、重要な研究を支援するために、州の従業員による個々の病院訪問に関するデータを発表しました。ラタニャスウィーニーは当時MITの大学院生でしたが、ケンブリッジの有権者登録記録を購入し、2つのデータセットをリンクすることで、個別に完全に無害でしたが、名前、住所、社会保障番号などの明らかな識別子はすべて削除され「匿名化」されていました。
b. 2006年、UT-Austinの大学院生であったArvind Narayananは、アドバイザーと一緒に、「匿名化」されたNetflixデータセットをインターネットムービーデータベース（IMDb）にリンクすることにより、 多くのNetflixユーザーが再識別される可能性があるとした。
c． 2013年、ホワイトヘッド生物医学研究所のDr. Yaniv Erlich率いるチームは、2500のシーケンスされたゲノムをオープンなオンラインデータベースに配置するための国際的なコンソーシアムである1000 Genomes Projectに参加した男性を再特定しました。
【０１０２】
[153] 2.より効果的なデータクレンジング手法は、データ自体のビジネスでの価値を低下させる恐れがあります。多くの難読化手法は損失を伴います。
【０１０３】
[154]データのプライバシー/匿名性に対するDynamic Anonymityアプローチは、両方の落とし穴を同時に回避する方法を提供します。
【０１０４】
[155] D.データプライバシー/匿名管理
【０１０５】
[156]個人データを保護するために、Dynamic Anonymityは、データのプライバシー/匿名性を測定、指定、および強制する複数の手段を使用できます。
1. Data Subject、アクション、アクティビティ、プロセス、および/または特性に関連付けられたデータの潜在的な露出の種類ごとにプライバシー/匿名レベルを決定するシステム。
これらのプライバシー/匿名レベルは、一連の離散値（完全なプライバシー/匿名性と完全な公開の両極端の間）またはそのような数学的仕様（「匿名性スコア」または「AMS」）で構成されます。
2.データに関するポリシーによって許可または制限されるアクションを指定するPERMS。（例：共有、更新）。
3.アクセスレベル、権限、およびデータを相互に関連付けて、データタイプ、時間、アクセスを求める組織などを含む1つ以上の基準に基づいて、データへの特定レベルのアクセスを許可または拒否するPERMS。
【０１０６】
[157]Data Subject’s PERMSは、法定ポリシーと組み合わせたり、法規制によって制限されたりする場合があります。 （たとえば、米国の医療データは、米国の医療保険の携行性と責任に関する法律（HIPAA）に従って保護する必要があります。）
【０１０７】
[158]さらに、もし信頼できるパーティーによって許可され、データ所有者の同意がある場合、特定の制限された権限を変更または付与する申し出がData Subjectに提示され、受け入れられます。

【０１０８】
[159] Dynamic Anonymityは、プライバシー/匿名レベルの決定を使用して既存のフレームワークを改善し、各Data Subjectの指定されたプライバシーレベルと一致する方法でデータの不適切な使用を防止することもできます。
【０１０９】
[160]Dynamic De-Identifiers (DDIDs)
【０１１０】
[161]A dynamic de-identifier DDIDは一時的に制限された仮名で次の値を参照し不明瞭にします。
（i）データ主体、アクション、アクティビティ、プロセス、および特性を参照するプライマリーキー。
（ii）そのData Subjectの属性の値、アクション、アクティビティ、プロセス、および特性（例：郵便番号）
（iii）Data Subject、アクション、アクティビティ、プロセス、および特性に関連付けられているデータの種類またはタイプ。
【０１１１】
[162] DDIDは、そのコンテンツと参照する値（クリアテキスト）の間に認識可能な固有の計算可能な関係がない場合、データをさらに保護する場合があります。さらに、特定のDDIDとクリアテキスト値の間の関連付けは、Circle of Trust（CoT）の外部に公開されない場合があります。
静的識別子とは異なり、異なるコンテキスト、目的で、異なる時間に使用される場合、隠された値、キーは同じ関連付けられたDDIDを持つ必要はありません。
【０１１２】
[163] DDIDは、Circle of Trustで生成されるか、上記の基準が満たされる場合、外部IDをDDIDとして使用できます。
【０１１３】
[164] DDIDには時間制限があります。
【０１１４】
[165]前述のようにDDIDアソシエーションは時間的制限があります。
つまり、同じコンテキスト内であっても、単一のタイプのデータに関しては、特定のDDIDが一度に1つの値を参照する場合があります。（必要に応じて別の時間に別の値を参照することもできます。）
【０１１５】
[166]特定のDDIDの意味を解読、公開する為に、必然的にアプリケーションはDDIDが適用された時間に関する知識を持つ必要があります。
【０１１６】
[167]この知識は明白かもしれません。-つまり、割り当て時間は、DDIDが格納されたレコードまたはドキュメントの一部である場合もあれば、暗黙的である場合もあります。たとえば、データセット全体がバッチとして不明瞭になり、（処理に実際にかかる時間に関係なく）同じ瞬間を占有し、フィールドタイプごとにDDIDマッピングの一貫したセットが1つしかないと推定される場合があります。このようなデータを再構成するには、対応するDDID /値の関連付けのセット（CoT内に格納されている）への参照を提供する必要もあります。
【０１１７】
[168] DDIDは目的依存です。
【０１１８】
[169] DDIDもコンテキストや目的に依存することに注意してください。
-同じDDIDが複数のコンテキストで同時に発生する可能性があることを意味します。
たとえば、各レコードに社会保障番号（SSN）と郵便番号が含まれるストリームを考えます。すべてが単一の時間ブロックを占有します。

そのような場合、特定のDDIDを郵便番号の代替としても、SSNの代替としても使用できます。
【０１１９】
[170]上記のようにDDIDが参照するクリアテキストを取得するために、コンテキストの何らかの表示（郵便番号やSSN）が必要であることを意味します。
【０１２０】
[171]データをDDIDで置き換え
【０１２１】
[172]単一のデータストリームを同じ種類のデータ（郵便番号やSSNなど）に置き換え、DDIDで同じタイムブロックを占有するタスクを検討します。
本発明の潜在的な一実施形態においてそのような動作を実行するアプリケーションプログラミングインターフェース（ＡＰＩ）の（Ｊａｖａのようなもの）「擬似コード」記述は、このように見えます。：

```
interface DDIDMap {
DDID protect(Value cleartext);
Value expose(DDID ddid);
}
```

【０１２２】
[173]英語の「インターフェース」は同じ基礎データで動作する関数のコレクション（「DDIDMap」という）を定義しています。
ここでは、データ型は最初の大文字で示されます（例：「DDID」）。
変数または関数パラメーター名は、最初は小文字で示します（たとえば、「cleartext」関数パラメーターは、「Value」タイプのデータである必要があります。 ID、数量、名前、郵便番号）。
【０１２３】
[174] 1つの関数protect（）はクリアテキスト値を受け入れ、対応するDDIDを返します。
その値が以前に見られた場合、そのDDIDが返されます。
以前に検出されたことがない場合、新しいDDID（このデータセットに固有の）が生成され、その値に関連付けられて返されます。
【０１２４】
[175]関数expose（）はこのプロセスを逆にします。
DDIDが送られてきた時、以前のDDIDとしてエンコードされていたクリアテキスト値を検索して返します。
もし、指定されたDDIDが表示されたことがない時、エラーを示します。
【０１２５】
[176]こういった操作下で管理されるデータは、各クリアテキスト値からそれを置換したDDIDへの双方向マッピングであり元の値に戻ります。
【０１２６】
[177]特定のDDIDは単一の値のみを参照できると述べました。ただし、必要に応じて、このアルゴリズムのバリアントバージョンを実装して、値を複数のDDIDに関連付けることができます。
【０１２７】
[178]時間や目的によるDDIDの管理
【０１２８】
[179]上記の双方向DDID-to-valueマップは、
（i）単一の種類のデータ（つまり、同じタイプ、コンテキスト、目的を持つ）
で、（ii）同じ時間ブロック内。複数の時間とコンテキストにわたる操作をサポートするために、特定の時間と目的に適切なDDIDから値へのマップを提供する別の潜在的なAPIを配置できます。

```
interface DDIDMapManager {
DDIDMap getMap(Context context, Time time);
}
```

【０１２９】

[180]「context」や「emits」のキィは、特定の種類のデータが隠されていることを指します。（他ではassociation key や A_Kと呼ばれます。）

例えば、「context」は、隠されるデータが存在するテーブルと列の名前である場合があります（例：「employee.salary」）。また、目的や範囲のその他の非時系列表示を含めることもできます。

【０１３０】

[181]「time」は、DDIDがクリアテキスト値に関連付けられている（または関連付けられていた）事を示します。DDID-to-valueマップは時間のブロックにまたがっています。また、ブロック内には多くの時間インスタンスがあります。これは、それぞれの時間に関連付けられた時間ブロックを見つける関数が存在することを意味します。（これについては後ほど詳しく説明します。）

【０１３１】

[182]DDIDジェネレーションとタイムブロッキング戦略

【０１３２】

[183]注意： 異なる種類のデータは、異なるDDIDとの置換ができます。

次の2つのセクションで言及されているものに加え、DDIDのサイズは、普遍的に一意であるか、そのデータセット（またはタイムブロック）で一意であるかによって異なります。

使用するエンコードの種類（整数またはテキストなど）など

また、DDIDの生成は通常ランダムにする必要がありますが、デモンストレーション、テスト、またはデバッグの目的で確定的または疑似ランダムDDIDジェネレーターを使用することもできます。

【０１３３】

[184]<u>ユニークまたは再利用されたDDID</u>

【０１３４】

[185]潜在的な戦略により、特定のDDIDを同じコンテキスト内の2つの異なるData Subjectsに割り当てることができます。しかし、2つの異なる時間ブロックの間に限ります。たとえば、同じ時間固定レコードのコレクション内でのDDID "X3Q"は、ある時点で（1つのタイムブロックで）"80228"を参照する場合があります。

その後（別のタイムブロック）「12124」を参照します。（この戦略を「DDID再利用」と呼びます。）

【０１３５】

[186]別の方法は「再利用」を禁止し、同じコンテキストで特定のDDIDが単一のサブジェクトのみを参照できるように規定することです。

（サブジェクトは時間の経過とともに異なるDDIDを受信する場合があります。）

【０１３６】

[187]これらの2つの戦略の選択には、あいまいさの増加と、あいまいなデータに対して集計クエリを実行しやすくすることとのトレードオフが含まれます。

【０１３７】

[188]郵便番号ごとに患者をカウントしたいと考えてみましょう。

郵便番号のDDIDがユニークであれば、DDIDごとにカウントを集計できます。

そしてこれらのDDIDを対応する郵便番号に解決して再度集計することにより、CoTにクエリを終了するよう依頼します。

しかし、「再利用」DDIDがある場合、同じDDIDの2つのインスタンスが同じ値を参照していることを確認できないため、解決（および集約）のためにDDIDや対応するタイムリスト全体をCoTに送信する必要があります。

【０１３８】

[189] DDIDタイムブロック
【０１３９】
[190]実装には時間によってDDIDマップをセグメント化するための戦略を選択する自由もあります。
時間のブロックは、サイズと時間オフセットによって異なる場合があります。
サイズは、固定、ランダム、または時間ごとに割り当てられたレコードの数によって決定できます。（特定のコンテキストに無限サイズの時間ブロックを使用すると、「静的」識別子を使用するのと同等の動作が得られることに注意してください。）
【０１４０】
[191]実装
【０１４１】
[192]新しいDDIDの作成の戦略は多くあります。しかしそのようなDDIDを生成するためのAPIは、内部で実装されている戦略に関係なく、本質的に同一に見える場合があります。
例えば：

```
interface DDIDFactory {
DDID createDDID();
}
```

【０１４２】
[193]次に特定のDDIDの割当てにどのタイムブロックが関連付けられているかを判断するタスクを検討します。
タイムブロックには多くの時間のインスタンスを含めることができるため、各タイムブロックに何らかの「タイムキー」（このドキュメントの別の場所では「T_K」と略されます。）が必要になります。これは、関数が任意の時点で適切なキーを取得する必要があることを意味します。

```
TimeKey timeKey = getTimeKey(Time time);
```

そしてタイムブロッキングとDDID生成の両方の戦略は、隠されているデータの種類に依存します。
それはつまり、これらは両方とも特定の「context」に関連付けられています。つまり、「context」APIはそれぞれをサポートする機能に少なくとも1つ提供する必要があります。

```
interface Context {
TimeKey getTimeKey(Time time);
DDIDFactory createDDIDFactory();
}
```

【０１４３】
[194]これら2つの追加機能を考えると、
「DDIDManager」（前述）の「getMap（）」の実装は次のようになります。

```
DDIDMap getMap(Context context, Time time) {
TimeKey timeKey = context.getTimeKey(time);
DDIDMap map = getExistingMap(context, timeKey);
if (map was not found) then
DDIDFactory factory = context.createDDIDFactory();
map = createMap(factory);
storeNewMap(context, timeKey, map);
endif
return map;
}
```

【０１４４】
[195]「getExistingMap（）」は、特定のコンテキストとタイムキーに割り当てられたマップを探す関数です。

「createMap（）」は、指定されたDDIDファクトリを使用するマップを作成し「storeNewMap（）」は、新しく取得したマップを、後で取得するコンテキストとタイムキーに関連付けます。

【０１４５】

[196]コンテキストを使用したデータと属性タイプの不明瞭化

【０１４６】

[197] Dynamic Anonymityは、保護する次の種類のデータを定義できます。

（i）Data Subject、アクション、アクティビティ、プロセス、および特性（従業員IDなど）を参照する主キー

（ii）Data Subject、アクション、アクティビティ、プロセス、および特性に関連付けられているがユニークではない属性データ（従業員の郵便番号など）

（iii）関連付けが解除された（隠された）データ要素のタイプ自体の表示（「アソシエーションキー」または「A_K」）。

【０１４７】

[198]それぞれ、異なるコンテキストを定義することで実現できます。

まず（i）と（ii）を説明します。どちらもデータ値を不明瞭にすることでできます。（他の場所では「リプレイスメントキー（置換えキー）」DDID（「R_K」と略されます）に置き換えます。）

（iii）関連付けられていない（不明瞭な）データ要素のタイプの表示については、以下で説明します。

【０１４８】

[199]例を考えてみましょう。：

特定の日に顧客がどの製品を購入したかを記録した注文表。

各記録には、曜日番号、顧客ID、製品IDがあります。

CoTの外部にいる第三者が使用または分析するために、このデータを不明瞭にしたいと考えています。

特に、顧客IDと製品IDはわかりにくくしますが、曜日番号はそのままにしておきます。

【０１４９】

[200]そして2つの「コンテキスト」インスタンスを作成することができます。

1つは「顧客ID」用で、もう1つは「製品ID」用です。

DDIDは、理想的にはランダムである必要がありますが、ここでは、「DDIDFactory」が0から始まる整数のDDIDを順番に作成すると仮定します。

さらに、各DDIDマップの期限は3日間であると想定しているので、3日後、DDIDマッピングの新しいセットが使用されます。それはDDIDが「再利用」されることを意味します。異なるブロックを使用すると、同じDDIDが異なる値を参照できます。

（これは理想的な戦略ではないので説明のためにのみ使用しています。）

【０１５０】

[201]表1は、クリアテキストのサンプルデータを示しています。

【表１】

日	顧客 ID	製品 ID
1	500	ZZZ
2	600	XXX
3	600	YYY
4	700	TTT
5	500	YYY
6	600	TTT

【０１５１】

[202]上記のように指定した後、このデータは以下の表2のようになります。
【表２】

日	顧客ID	製品 ID
1	0	0
2	1	1
3	1	2
4	0	0
5	1	1
6	2	1

【０１５２】
[203]これを理解する為に、各カラムを読み、3日間ごとのグループで考えます。（DDIDの最初のタイムブロックは、それぞれ1～3日の不明瞭フィールド、2番目のカバーは4～6日目です。）。
【０１５３】
[204]最初の3日間の顧客IDは500、600、600です。結果のエンコードは0、1、1です（600が繰り返されるため、DDIDと1も繰り返されることに注意してください。）。
【０１５４】
[205] 2、3日目の顧客IDは700、600、500です。そして（0からやり直す）結果は0、1、2です（以前、500は0でしたが、現在は2です）。
【０１５５】
[206]製品IDは別のコンテキストを使用します。したがって、DDIDのストリームなので、ゼロからも開始します。初めてブロック（XXX、YYY、TTT）が（0、1、2）になります。2番目の時間ブロック（TTT、YYY、TTT）は（0、1、0）になります。
【０１５６】
[207]別の「コンテキスト」を使用して、列の名前が属性キー（A_K）である不明瞭なデータ要素のタイプ（上記iii）の表示を隠すことができます。
これは、セット全体に対してDDIDから値へのマッピングを使用して（列名を実質的にDDIDに置き換える）またはタイムブロックで（他のフィールドと同様に）行うことができます（適切にランダムなDDID生成戦略が雇用）影響を受けた記録は、CoTの支援なしでは分析できませんでした。
【０１５７】
[208]局所性と時間に関する注意
【０１５８】
[209]上記で定義されたAPIの例では、データがエンコードされると、各データムまたはレコードでエンコード時間が渡されることを前提としています。
これは、DDIDが同じコンテキスト内で「再利用」されている場合にのみ必要です（したがって、そのDDIDの2つの潜在的な意味を区別するのに時間が必要です）。
DDIDがコンテキストごとに1つの値にのみ割り当てられている場合、そのDDIDは（単一の）元の値を検出するのに十分です。
【０１５９】
[210]「再利用された」DDIDが異なるシステム間で採用されている場合、時間の問題も発生する可能性があります。
DDIDエンコーディングに関連付けられた時間を渡すことができない場合、（時系列の）「バッファ」を使用して、DDIDが元の割り当てに近すぎて再使用されないようにすることができます。そして、エンコードされるデータに関連付けられた時間を渡すことができる場合、その時間はローカルシステムクロックに対して健全性をチェックされます。
小さなウィンドウ（DDID再利用バッファより小さい）内のスキューは許容できますが、大

きな違いはエラーレポートを引き起こします。
【０１６０】
[211] 最後に、データがどこで符号化されるかに関しても柔軟性があることに注意してください。：データはCoT内に存在するマシンにストリームされ、符号化後にその宛先に送られます。しかし、代わりに、結果として生じるDDIDと値の関連付けが (a) ローカルホストに保存されず、 (b) 永続性のためにCoTホストに安全に(暗号化の使用、データ消失に対する適切な保護などを)ストリーミングし、重要なアプリケーションでの待ち時間が短くなるならば、上記アルゴリズムの符号化部分をCoTの外で実行することもできます。
【０１６１】
[212] Dynamic Anonymity： 評価減を伴わない識別の抹消
【０１６２】
[213]データのプライバシー/匿名性を保護するために、特定の状況(例：HIPAAまたは健康関連の状況)で従来から使用されている「識別解除」技法は、本質的に防御的であることが多い。例えば、許可されていない第三者による再識別の可能性を低減するために、一連のマスキングステップが直接識別子(名前、住所など)に適用され、マスキングや統計に基づく操作が準識別子(例えば、年齢、性別、職業)に適用される。このアプローチでは、再識別に対する保護と、使用可能な情報へのアクセスの維持との間にトレードオフが生じる可能性があります。
【０１６３】
[214] Dynamic Anonymityは、データが再識別されるリスクが統計的に有意ではないにもかかわらず情報の価値を保持し、承認された目的のために活用できるという点で大きな価値を持つ可能性がある。Dynamic Anonymityは、リスクを最小化するためには情報コンテンツの価値を犠牲にしなければならないという命題と伝統的な二分法を否定するかもしれないが、代わりにDynamic Anonymityは、リスクと失われる情報量の両方を最小限に抑え、すべてではないにしても、ほとんどの情報を復旧できるようにします。ただし、復旧できるのは、不正な敵/「ブラックハット」のようなハッカーによってではなく、Data Subject/Trusted Partyによって承認された場合のみです。
【０１６４】
[215] Dynamic Anonymityは、データのロック解除と価値の最大化を容易にする管理された環境において複数の関係者がさまざまな方法で情報を使用することを可能にします。Dynamic Anonymityは、潜在的なビジネスインテリジェンス、調査、分析、およびその他のプロセスの価値を最大化すると同時に、データプライバシー/匿名プロセスの品質とパフォーマンスを大幅に向上させる可能性があります。
【０１６５】
[216]機密データを収集または保存する際には、次の方法のいずれか、または複数を使用して、対象から機密データを「関連付け解除」することができます。いずれの方法を使用しても、価値が失われることはありません。
1.セグメント化：機密データは、データタイプごとに複数の部分に分割され、個別に(別の信頼の円で管理するか、同じ信頼される側で管理されている別のDDIDマッピングセットを使用します。)送信および/または格納されるため、各部分だけでは個人データが生成されません。
2.ID置換： 静的識別子は、動的に変化し再割り当て可能なDDIDで置き換えることができ、データとそのデータが参照する対象データとの関係を曖昧にする。
3.難読化：データ値とデータタイプインジケーターもDDIDで置き換えることができます。
【０１６６】
[217]これらの操作に関連付けられたDDIDは、図1C-1に示すように、トラスト・サークルCoTの関数内に格納されます。したがって、元のデータは、これらの変換を逆にすることによって再構成することができるが、それはCoT自身の協力によってのみであり、したがって、Data Subjectによってその代理でそのような許可が与えられた場合にのみ作動する。

【０１６７】
[218] 図1は、本発明の一実施形態の一例を示しており、これは、異なるアプリケーション56で使用するために、データ対象に関する様々なデータ属性およびデータ属性の組み合わせ(これには、行動データ、取引履歴、信用格付け、身元情報、ソーシャルネットワークデータ、個人履歴情報、医療および雇用情報、および教育履歴が含まれるが、これらに限定されない)を安全に管理するシステムプライバシーサーバー50、またはプライバシーサーバモジュールを含む。これらのアプリケーション56は、以下を含むが、限定はされない。
〇医療アプリケーション
・診療録
・モバイルアプリケーション
・リアルタイムクリティカルケアアプリケーション
・法規制の遵守(例：HIPAA)
・リサーチ
〇教育アプリケーション
・学生簿
・リサーチ
〇モバイルアプリケーション
・ジオロケーション(ビーコン、GPS、Wi-Fi指紋認証)
・モバイル決済とロイヤリティ
〇金融サービスアプリケーション
・銀行業・証券業等。
・決済処理
・クレジットカード業界(PCI)のセキュリティ
・認可
・カード会員資格の確認
・法令順守
・リサーチ
・クレジット査定
・不正行為の摘発
〇Webアプリケーション
・配役
・コンテンツレビュー
・eコマース
・ソーシャルネットワーク
〇「モノのインターネット」 アプリケーション
・テレマティクス
・スマートグリッド
・スマートシティ
・トラフィックの監視
・ユーティリティの監視
〇電源
〇燃料
〇上下水道
・廃棄物管理
・スマートオフィス
・スマートファクトリー
・スマートホーム
・コネクテッド・エンターテインメント
〇テレビ

〇ストリーミングデバイス
・自動化
〇HVAC
〇照明
・セキュリティ
〇窓/ドアロック
〇火災/煙/一酸化炭素検知器
・アプライアンス
・スマートカー
・農業フィールドセンサー
・ウェアラブル端末
・医療監視
・フィットネス機器
・アイウェア
・衣類
・ドローン
〇プライベートワイヤレス/有線ネットワーク
・クロップセンサ
・タグ付き動物追跡
・軍隊の動き
〇プライベートセキュリティアプリケーション
〇Eコマース・アプリケーション
〇オフラインの小売アプリケーション
〇人事/採用アプリケーション
〇政府機関向けアプリケーション
・国家安全保障アプリケーション
・コール詳細レコードの分析
・Web閲覧動作の分析
・オンラインおよびオフラインの購買行動の分析
・旅行行動分析
・ソーシャルメディア活動の分析
・友人・知人・その他の関係の輪の分析
〇弁護士/弁護士事務所への申請
・守秘義務・弁護士依頼権の保持について
・電子ディスカバリー
〇消費者コンテストへの応募
〇デートアプリケーション
〇ギャンブル、e-ワガリングアプリケーション（e-Wagering）

【０１６８】

[219]図1Aは一つ以上の外部データベース82から電子データを受信しData Subjectに関する一つ以上の外部データベース(これには、行動データ、取引履歴、信用格付け、身元情報、ソーシャル・ネットワーク・データ、個人履歴情報、雇用情報、医学および教育履歴が含まれる)からの種々のデータ属性及びデータ属性の組み合わせを、異なるアプリケーションで使用するためのTDRに安全に変換するプライバシー・サーバ50又はプライバシー・サーバ・モジュールを有するシステムを含む、本発明の実施形態の一例を示す。
あるいは、アプリケーションは、プライバシーサーバ50内にData SubjectからDDIDへの関連付け情報のみを格納し、動的匿名定義手順を使用して、外部データベース82内に格納されたデータを不明瞭にし、暗号化し、セグメント化する。このようにして、プライバシーサーバ50内に格納されたData SubjectからDDIDへの関連付け情報は、外部データベース82内で生成され、収集され、格納された情報により大きなコンテキストやビジネス上の

価値を提供することができる。

【０１６９】

[220]一例では本発明の実施形態は、一つ以上のアプリケーション56で使用するためのデータ対象の安全で包括的な集約データプロファイル58を形成することができる。

Data Subjectまたはそれに関連する関係者、例えばユーザ59は、Data Subjectの集約されたデータプロファイル58(データ属性の組合せまたはその一部で構成され、関連していないデータ・ソースの可能性があります。)に表現されるような特性の一つ以上に基づいて、ネットワーク72(例えば、サービスを受ける可能性や購買取引を行う可能性)を介してコミュニケート57することにデータサブジェクトに関連する関係者が関心を持っているベンダ、サービスプロバイダ、広告主または他のエンティティに、データサブジェクトの識別およびデータ属性をデータサブジェクトの集約されたデータプロファイル58から匿名で通信するか、または選択的に開示することができる。

このようにして、本発明の実施形態は、Data Subjectに関連するデータ属性及びデータ属性の組合せを管理する個人(「DRMI」)、関連当事者又は第三者、又は、一つ以上のデータ主題に関連するデータ属性及びデータ属性の組合せを管理する第三者からなる非識別のためのデジタル権利管理(「DRMD」)を提供する。

一例では、データ属性、データ属性の組合せ、データ主題及び/又は関連当事者に関する情報を他の当事者が利用できるようにする程度は、本発明の実施形態によって制御することができる。

【０１７０】

[221]図1および図1Aの例では複数のユーザ59、たとえばData Subjectまたはサービスプロバイダは、インターネットなどのネットワーク72にアクセスするために、スマートデバイス70、スマートフォン、タブレット、ノートブック、デスクトップコンピュータ、有線または無線デバイス、またはプライバシークライアントアプリケーション60を実行する他のコンピューティングデバイスなどのデバイスを利用する。

図1および図1Aに示すように、インターネットまたは他のパブリックまたはプライベート・ネットワークに接続されて通信するシステム80が示されており、このシステムは、一つ以上のデータベース82に安全に接続されたプライバシー・サーバ50を含むことができる。

一例では、5月50日のプライバシー・サーバは、サーバまたは他のコンピューティング装置上で実行されるコンピュータ・プログラム・モジュール、コード製品、またはモジュールを使用して実装される。

5月82日の一つ以上のデータベースは、RAID記憶装置、ネットワーク接続記憶装置、又は他の任意の従来のデータベースのような冗長位置にデータ(暗号化など)を安全に記憶する技術を含む、任意の従来のデータベース技術を用いて実施される。

【０１７１】

[222] 一例では、プライバシー・サーバ50は、本明細書に記載する操作、プロセス、機能またはプロセス・ステップのうちの一つ以上を実施し、プライバシー・サーバ50は、本発明の特定の実施に応じて、必要に応じて、他の操作、機能またはプロセス・ステップを含むか、または含むように構成することができ、これには、示されたモジュールによって実行される以下のプロセス、操作または機能が含まれる：

【０１７２】

[223]以下のプロセスを含む内部認証および外部認証の両方を提供することができる認証モジュール51：

a．TDRに対するプライバシークライアント60要求の内部認証、およびTDRのプライバシーサーバの50世代。

b．望まれる行動、活動、またはプロセスへの参加を可能にする前の外部認証、およびTDRの使用は、TDRの内容をアンロックするために必要とされる可能性がある、タイムキー(TK)、アソシエーションキー(AK)、置換キー(RK)を受信するために承認されたものとして受信者を認証するためのTDRの使用。

c．許可モジュールの一実施例はDDIDおよび関連するTDRの生成を、制御エンティティに

よって許可された他の主体に要求する能力の委任を可能にすることを含み得る。
【０１７３】
[224]以下のプロセスのうちの一つ以上を含み得る内部および外部抽象化を提供し得る抽象化モジュール52：
a． DDIDを生成するか、時間的に一意で動的に変化する値を受け入れまたは変更してDDIDとして機能させることにより、DDIDを選択します。
b．DDIDをデータ属性または属性組合せと関連付けて、与えられたデータ主題、動作、活動、プロセスまたは特性のTDRを形成する。
c．関連するデータ属性の一部のみをTDRに含めることによって、データ主題に関連する、および/または所与の行動、活動、プロセスまたは形質に関連するデータ属性を切り離す。
d． TDRに含まれるデータ属性をDDIDに置き換える。
e．本発明の1つ以上の実施形態と統合または通信することができる外部ネットワーク、インターネット、イントラネット、コンピューティングデバイスへの1つ以上の参照をDDIDで置き換えること。
【０１７４】
[225]以下を格納することができるメンテナンスモジュール53：
a．Data Subjects、行為、活動、プロセス又は特性、「関連データ」(最初にDDIDに関連付けられたデータ、および/または関連付け期間中および/またはその後にDDIDで集約されたデータとして定義されます。)
b．(a) 各DDIDが特定のデータ主題,属性,属性の組合せ,動作,活動,プロセス又は特性に関係していた期間に関する情報を反映するタイムキー(TK),(b) アソシエーションキー(AK)または (c) 置換キー(RK)に関するキー情報。
それによりTDRが後で、特定の属性、属性の組合せ、アクション、アクティビティ、プロセス、特性、関連するData Subjectsに再関連付けされることを可能にする。
さらに、保守モジュールは、安全な環境において、属性または属性の組み合わせの分析および処理を実行することができる。
【０１７５】
[226]システムエラー、誤用の場合に、事故後の法医学的分析を可能にするための情報を収集および記憶することを含み得るアクセスログモジュール54。
【０１７６】
[227]任意の時点におけるデータ属性、属性の組み合わせ、DDIDs、およびTDRsを含む集約データ・プロファイルの整合性を検証および検証することを含む検証モジュール55。
【０１７７】
[228]本書に記載されるように、本発明の実施形態は、電子データおよびネットワーク通信、分析および研究に関するプライバシー、匿名性、セキュリティ、および精度を促進することを目的とする。
一例では、Data Subject、動作、活動、プロセス又は特性に係るデータ要素を独立属性又は従属属性に分離することによって抽象化することができる。
本開示の目的のために、データ属性は、個人、場所又は物、及び関連する行動、活動、プロセス又は特性のようなData Subjectを識別するために、独立して又は他のデータ要素と組み合わせて使用することができる任意のデータ要素を指すことができる。
【０１７８】
[229]上述のように、人、場所又は物のようなData Subjectを識別するために使用することができるデータを抽象化することに加えて、図1又は図1Aの抽象化モジュール52は、以下を含むことができる。：
物理的または仮想的なものと実体;ハードウェアまたは仮想デバイス;ソフトウェアアプリケーション;法的エンティティ、オブジェクト;イメージ;オーディオまたはビデオ、情報;感覚情報;マルチメディア情報;地理位置情報;プライバシー、匿名情報;セキュリティ情報;送信者と受信者、メッセージ内容、メッセージ内のハイパーリンク、メッセージ内の埋め込み内容、およびメッセージの送受信に関連するデバイスとサーバーに関する情報を含む電

子メッセージング情報;ソーシャルメディアや電子フォーラム;オンラインのウェブサイトやブログ;RFID(無線周波数識別);トラッキング情報;税金情報、;教育情報;軍事、国防、その他の政府機関プログラムに関連する識別子;仮想現実情報;多人数参加型オンラインロールプレイングゲーム(ＭＭＯＲＰＧ);医療情報;バイオメトリックデータ;動作メトリック情報;遺伝情報;他のデータの物理的または仮想的な場所を参照するデータ;データや情報の実例や表現です。

【０１７９】

[230]本書に記載されるシステム、方法、および装置は、一例において、個人(DRMI)のためのデジタル権利管理および非識別(DRMD)のためのデジタル権利管理を提供するために使用される。

個人のデジタル権利管理は、関連当事者が1つ以上の関連当事者に関連するデータ属性を管理する個人指向プライバシー/匿名を含むことができる。

この場合、関連当事者が支配主体となります。あるいは、第三者は、1つまたは複数の関連当事者に関するデータ属性を管理することができ、それによって、エンティティ指向プライバシー/匿名性を備えることができる。この場合、第三者が支配主体となる。また、識別不能化のためのデジタル権利管理は、第三者が関連当事者に関連するデータ属性を管理し、データ属性および関連当事者に関する情報を他の当事者が利用できる程度を制御する、エンティティ指向プライバシー/匿名を含む。

【０１８０】

[231]本書に開示されるシステム、方法および装置は、1つまたは複数の関連当事者が、直接的または間接的に、データのオンラインデジタル指紋を管理できるように、DRMIを提供するために使用してもよい。また、関連当事者は、データ属性、Data Subjectまたは1つ以上の関連当事者に関連する情報を第三者が利用できるようにする範囲を制御して、情報およびデータを匿名で、再確認不可能な方法で利用できるようにすることができる。システム、方法及び装置は、関連当事者がある時点ではデータを共有したいが次の時点では共有したくないという動的に変化する環境を提供する。これは、時間間隔、特定の受信エンティティ、物理的または仮想的な所在、または共有されるデータの変化をトリガする他のメカニズムが、本質的に動的であり得ることを理解して行われる。DRMIを実施することは、匿名性の再確認を不可能にし、データ属性、Data Subjectおよび関係者に関する異なる情報を、動的に変化する、時間および/または場所に敏感な、ケースバイケースのベースで、異なる目的のために共有することを可能にする可能性がある。データ属性、Data Subject又は特定の時期及び場所における関係者に関連する情報に関する特定の必要性は、追加の不必要な情報を明らかにすることなく、調整することができる。ただし、そのような明らかにすることが、管理主体によって許可されている場合を除く。追加の不必要な情報は、例えば、Data Subject又は関連当事者の真の身元、メールアドレス、電子メールアドレス、以前のオンライン行動、又は関連当事者に関する特定の行動、活動、プロセス又は特性に関して非関連当事者にとって必要でない他の情報である。

【０１８１】

[232]本書に開示されたシステム、方法、および装置は、DRMDを提供するために使用し、結果、エンティティは、データ属性、Data Subject、およびそれらが責任を負う関係者に関連する情報のオンラインデジタル指紋を集中的に管理することができる。そのような機関は、他の関係者がどの程度の情報を利用できるようにするかを、再確認不能な方法と識別可能な方法でコントロールすることができる。

これにより、組織は、Data Subject、関連当事者、および規制上の保護と禁止の要望に従うための識別除去目的または義務を満たすことができる。

【０１８２】

[233]本発明のいくつかの実施形態の例示的な実施形態は、識別顔特性を示す画像またはビデオファイルから構成されるデータ属性に関して、DRMIまたはDRMD能力を提供するように構成することができる。

Data Subject又は関連当事者は,電子画像の中の特徴に基づいて同一性について推論する

ことができる他の者から利益を受ける。
しかしながら急速に拡大する商業的利用可能性および電子画像の利用可能性の増加と組み合わせた顔認識技術の利用は、データ対象および関係者のプライバシー/匿名性、セキュリティに関して問題がある。
一例では、プライバシー/匿名性、セキュリティは、顔画像およびData Subjectの特徴を含む写真であるデータ属性のコンテキストにおいて、Data Subjectおよび関連当事者に関して、本開示の1つ以上の態様を使用して保護することができる。
【０１８３】
[234]いくつかの実施の形態では、本書に開示されるシステム、方法、および装置は、データ属性を含むウェブサイトまたは他の電子画像共有アプリケーションへの登録、許可された訪問者対未登録/許可されていない訪問者としての当事者の状態を区別するように構成することができる。
また、ウェブサイトやその他の写真共有アプリケーションに登録、許可された訪問者が、データ対象者または関連当事者の連絡先、友人に関するデータ属性を含む場合と、データ対象者または関連当事者の連絡先/友人でない場合とを状況に応じて区別することができる。
例では本発明のシステムは、顔の特徴を含む画像データ属性が提示されるかどうかを制御することができる。
顔の特徴を含む画像データ属性が提示される場合、システムは、追加の保護技術を介して、意図しない二次的使用につながる可能性のある写真の無許可の使用およびコピーをさらに制御し、制限することができる。
さらに、本発明のいくつかの実施形態は、Data Subject、関連当事者、および制御エンティティに、どの追加当事者およびどの特定目的のために画像データ属性を提示することができるかを指定する能力を提供することができる。
データ属性が提示される場合、Data Subject、関係者又は制御主体は、画像が写真の不正使用及び複製を制限し、それによって画像の意図しない二次的使用のリスクを防止又は低減することを目的とする既知の保護技術を利用するか否かを指定することができる。
【０１８４】
[235]DRMIは、Data Subjectsおよび関連当事者が、直接的または間接的に、顔画像を含む写真を管理し、関連当事者に関連する写真を第三者が識別可能、識別不可能、再生可能、不可能な方法で利用できる範囲を制御できる。
【０１８５】
[236]本発明の潜在的な実施例は、ウェアラブル、埋め込み可能、埋め込み可能、または他の方法で接続可能なコンピューティング技術/デバイスの提供者によるDRMIの使用を含み、技術/デバイスを使用して取得され処理される情報に対する潜在的な公衆の関心を軽減する。
例えば、グーグル（登録商標）はDRMIを採用することでグーグルGLASS（登録商標）の広範な採用を促進することが可能となります。DRMIは、Data Subjectまたは関連当事者が登録を許可し、使用して撮影または表示された許可されていない写真のデジタル表示を禁止するデジタル表示禁止リスト(FTCが個人への望ましくない勧誘電話を制限するために管理している電話勧誘禁止リストに似ている)を確立することによって実現されます。(グーグルおよびグーグルGLASSは,Inc.の商標です。)
【０１８６】
[237]本発明の一例によって提供されるDRMIはさらに、プロのネットワーキングサイトLinkedIn.comのメンバーであるData Subjectまたは関係者に、第三者が写真を識別可能、識別不可能、再生可能、または再生不可能な方法で利用できるようにする範囲を管理する機能を提供することができる。Data Subjectまたは関連当事者の顔画像を含む写真へのアクセス、使用、およびコピーは、一例では、3層分類スキーマを使用して制御することができる。
【０１８７】

[238]カテゴリーA
LinkedInの登録/承認されたメンバーではないLinkedIn.comのサイトのビジターには、ステータスが適用される場合があります。これらは、登録/認定されたLinkedIn（登録商標）(LinkedIn（登録商標）、LinkedIn Corporationの商標です。)メンバーの顔画像を含む写真を閲覧またはコピーする手段を提供されない場合があります。代わりに、ウェブブラウザ、モバイルアプリケーションまたは他のアプリケーションを介して、写真がLinkedIn.comウェブサイトの登録/許可されたユーザのみに利用可能であることを示すグラフィック、画像、インジケータまたはアバターを提供することができます。
【０１８８】
[239]カテゴリーB LinkedInの登録/承認されたメンバーの連絡先が認証されていないメンバーにはステータスが適用される場合があります。
意図しない二次的使用につながる可能性のある写真の無許可の使用、コピーを制限することを目的とした追加の保護技術を使用することによって、彼らの写真を閲覧またはコピーするための限定された手段を得る。これらの追加の保護技術には、以下のものが含まれる。
1.イメージを小さなイメージタイルに分割するタイル処理。イメージタイルは連続したイメージとして表示されますが、イメージをコピーしようとしているエンティティでは、一度に1つのタイルピースに限定されます。
2.画像電子透かし技術の採用
3.レイヤーを非表示にして、顔の特徴を含む画像を透明な前景画像の後ろに配置する
4.カラープロファイルやパレットを使用せずに画像を提供する
5.イメージのコピーまたは使用を無効「右クリック 」にするテーブル・インストラクションによるダウンロードの防止
6.画像の 「右クリック」 コピーまたは使用を無効にするJavaScriptテクノロジによるダウンロードの防止
7.イメージの 「右クリック」 コピーまたは使用を無効にするFlashテクノロジーによるダウンロードの防止
8.URLエンコード方式による画像の非表示
9.METAタグを使用して、顔の特徴を含む画像が検索エンジンのスパイダー、ロボット、ロボット画像によってインデックスされるのを防止する
10.Robotを使用する。顔の特徴を含む画像が、検索エンジンのスパイダーやロボット、ロボットの画像にインデックスされるのを防ぐためだ。
【０１８９】
[240]カテゴリーC LinkedIn.comの登録/承認されたメンバーで他の登録/承認されたメンバーの認証された連絡先にも適用されます。これらの登録/認定されたメンバーには、他のLinkedIn（登録商標）メンバーの顔画像を含む写真を閲覧またはコピーするための完全な手段を提供することができます。
【０１９０】
[241]DRMDは、本発明のいくつかの例によって提供することができ、結果、エンティティは、責任を有する顔画像を含む写真データ属性を集中的に管理することができ、写真データ属性を他の関係者が識別可能、識別不可能、再生可能または再生不可能な方法で利用できるようにする程度を制御することができる。
【０１９１】
[242]本発明の可能な実施例の一つとして、顔の要素を閲覧できる前記登録・承認されたData Subjectまたは関係者の認識可能な顔の要素を含む、写真データ属性のData Subjectまたは関係者により承認されていない者による、要素の公開を制限するために、既知の顔画像認識能力を活用する、管理者によるDRMDを提供するシステムの使用を含むこともできる。言い換えると、顔の特徴がDRMDシステムに登録されている、登録・承認されたData Subjectまたは関係者の顔の要素を含む写真をアップロード、使用、または閲覧しようとするが、登録・承認されたData Subjectまたは関係者により承認されていない者は、登録・承認されたData Subjectまたは関係者の認識可能な顔の要素をブロックアウトまたは

「タグ外し」するために、DRMDシステムによって変更された写真の改訂版だけを見て使用することができる。例えば、DRMDを提供するシステムに登録された、Data Subjectまたは関係者の顔を含む公共のバーで撮影された写真は、Data Subjectまたは関係者により明確に承認されているバージョンを除き、写真の全てのバージョンに対し関係者の顔をブロックアウトまたは「タグ外し」するために修正され得る。

【０１９２】

[243]本発明の一例では、だれがどの情報を見るかという決定は、設定可能な状態で管理者によりなされるよう、承認モジュールを構成することができる。もう一つの例では、その設定可能なコントロールは、管理者それぞれに、データ属性から成る情報の構成を、いつでも動的に変更できる権限を与えることで、タイムリーにケースバイケースでなされる自動または手動の決定や更新を含むことができる。データ属性の構成を動的に変更することにより得られる、強化されたカスタマイズは、データ属性や関係者について提供される情報のより高い関連性と正確さへとつながる。ここに開示されているように、プライバシーと匿名性、セキュリティの構成要素としてのDDIDsの使用により、情報の受領者それぞれが、特定の目的それぞれに対して適切な異なる情報を受け取ることができ、それによって、従来の不変的で静的な識別子または他の機構を経由して提供される、古くて時間がかかり、正確ではなく徐々に増えていくデータとは異なり、新しい、タイムリーで関連性が高く正確な情報の配布を促す。

【０１９３】

[244]図1と図1Aには、コンピュータ、スマートフォーン、その他有線・無線機器を含むユーザー機器70で作動しているプライバシー・クライアント60の様々な例が示されており、そのユーザー機器は、インターネットや他の公共または私有のネットワークであるネットワーク72上で、プライバシーサーバー50と通信することもできる。

【０１９４】

[245]一例では、本開示の要素であるプライバシー・クライアントは、携帯機器上の常駐者となることもできる。プライバシー・クライアントは、携帯機器上の携帯アプリまたはオペレーティングシステムの一部として提供してもよく、または携帯機器の回路や素子に内蔵されるハード機器として構成してもよい。本開示の一つ以上の要素が組み込まれている携帯機器は、Data Subjectまたはその機器と繋がりがある関係者についての場所、活動、挙動についてのリアルタイム情報を保持してもよい。その携帯機器は、他の機器や情報源に対し、情報を送信したり、受信したり、処理したりすることもできる。プライバシー・クライアントと関わる携帯アプリは、管理者に、場所と時間に依存するアプリにおける、参加のタイミングとレベルと、個人的に識別できるのではなく、匿名で第三者と情報を共有する度合の両方についての管理権を提供することもできる。本開示の一つ以上の要素が組み込まれている携帯機器は、関連性のない、全く異なる情報源(携帯機器、従来のコンピュータ、またはその両方の組み合わせ)から集められた、ユーザー個人の好みについての情報を集約する携帯機器独自の能力を促進し、ユーザーの承認がある場合のみ、ユーザーの情報(匿名または個別の状態で)を、時間や場所に依存する、個別のビジネスチャンスを取り計らうために、業者と共有することもできる。ここで、より明確に理解されているように、ユーザーは、そのような時間や場所に依存する、個別のビジネスチャンスの利益により、取引と関連してユーザーが特定されることを良しとするかどうか、の判断をすることもできる。

【０１９５】

[246]例えば、本発明の実施形態無しに、従来のように携帯機器と関連している静的な識別子により、携帯アプリ提供者と他の第三者に、携帯機器の使用についての情報を集約させるようにすることもできる。そして、携帯機器の使用についてのデータを集約することにより、アプリ提供者と他の第三者は、その機器のユーザーとの一回限りの関わりからのデータを通しては得られない、その機器のユーザーの頻発する物理的な場所、通話の習慣、コンテンツの好み、オンライン取引についての情報を含むがそれに限定されない情報を得ることも可能である。本発明のいくつかの実施形態を用いることにより、アプリ提供者

と他の第三者は、Data Subjectと関係者による携帯機器の使用に関する情報の集約を妨げられるかもしれない。そして、本発明のいくつかの実施形態によれば、従来の静的な識別子とは異なる、動的に作成され、変更可能、再度割り当て可能なDDIDsを用いて、携帯機器、Data Subjectまたは関係者の識別情報を明らかにすることなく、地理的位置情報(例えば、道順や地図のアプリ)へのアクセスを要求する携帯アプリの使用を、携帯機器に提供するように構成されてもよい。

【０１９６】

[247]一例では、本発明の実施形態において、静的な識別子の集約よりもDDIDsを活性化させることにより、不変的で静的な識別子に対し、より強化されたプライバシー、匿名性、セキュリティー、そして正確さを提供するように構成されてもよい。それによって、本発明の実施形態は、ネットワークやインターネット中に残されている、オンライン電子指紋に対し、解決策を投じることができる。その結果、本発明の実施形態により、管理者に、誰がどのデータを見られるかを決定する権限を与え、データ集約者が、管理者の許可なしにData Subjectまたは関係者についてのデータの繋がりを理解するのを妨げ、管理者に、上流へまたは下流への情報の伝播についてのコントロール権を与えることもできる。

【０１９７】

[248]本発明の一例では、抽象化への複数の保護レベルを提供するために、DDIDsを用いたビッグデータ解析性の利点のために、継続したアクセスを提供することもできる。また、本発明のいくつかの要素が具体化されているシステムや方法、機器は、有効なビッグデータ解析性のために必要なデータへのアクセスを除外し、情報のお返しに無料または割引された製品やサービスを提供する経済モデルにはそぐわない、トラッキング拒否や他のイニシアティブの基本的な不具合を被らない。トラッキング拒否とは、Data Subjectや関係者が解析サービスや宣伝ネットワーク、ソーシャルネットワークを含む、ウェブサイトや第三者によるデータ収集者によるオンラインでの特定のトラッキングをオプトアウトできるような技術と方針提案である。トラッキング拒否は、Data Subjectや関係者に強化されたプライバシーや匿名性、セキュリティを提供するものの、オンラインからビッグデータ解析性まで、Data Subjectや関係者が、カスタマイズされた、個別に関連性のあるオファーを受け取る利得を拒否する。このことは、業者やサービス提供者、そしてData Subjectや関係者自身に対しても、ビッグデータ解析性がもたらす経済的な利得に影響を与える。

【０１９８】

[249]一方で、本発明のいくつかの実施形態には、(トラッキング拒否による、収益に対する、正味負の影響に対し)収益に対する、正味ゼロから正の影響がある。その理由は、本発明のいくつかの実施形態により、管理者が、受領者に従来のトラッキング技術を用い、存在している間TDRsをトラックすることができるデータ属性をTDRsに含めることもできるからである。管理者は、個別化とカスタマイズを促すために、トラッキングのみを経由して得られる情報よりも、より正確な情報を含めることもできる。例えば、管理者はウェブサイトとData Subjectや関係者の両者にとって有益な、その他特定の、より最新の情報で増補され、プライバシー・クライアント経由でそのウェブサイトへ送信された、Data Subjectや関係者についての属性の組み合わせに、ウェブサイト上での過去の閲覧についての特定のデータを含めるようにすることもできる。

【０１９９】

[250]図1及び図1Aを参照すると、本発明の実施形態の一つには、一つ以上の演算機器70に常駐する、またはネットワーク機器に常駐し、そのネットワーク機器を介してアクセスできる、コンピュータのハード、ファームウェア及びソフトから成る一つ以上のリモート・プライバシー・クライアント60が、プライバシー・サーバー50として機能する一つ以上の演算機器へ、リクエストや問い合わせを送受信する、コンピュータネットワーク72を含めることもできる。プライバシー・クライアントの演算機器70は、（i）プライバシー・サーバーからのサービスのリクエスト、またはライバシー・サーバーへの問い合わせの送信を可能にし、(ii)ユーザーインターフェース機能を提供し、(iii)アプリ処理機能を提供し、(iv)ローカライズされた記憶域とメモリを提供する、プログラムがインストールされ

た、スマート機器（装着可能で可動または不動なスマート機器）、スマートフォン、タブレット、ノートパソコン、デスクトップコンピュータ、またはその他の演算機器から構成されることも可能である。プライバシー・サーバー50である演算機器は、(i)プライバシー・クライアントからのサービスや問い合わせのリクエストに応え、(ii)システムを集中的または非集中的に管理し、(iii)アプリの大量処理能力があり、(iv)大容量の記憶域とメモリを提供する、プログラムがインストールされた、大容量パソコン、ミニコンピューター、メインフレームコンピュータ、またはその他の演算機器から構成されることも可能である。また、プライバシー・サーバー50は、ここで述べられた動作や機能の一つ以上を実施するように構成することもできる。プライバシー・サーバーとプライバシー・クライアントの間の通信機能は、コンピュータネットワーク、インターネット、イントラネット、公共または私有のネットワーク、または通信チャンネルのいずれかとその支援技術により構成され得る。

【０２００】

[251]図1及び図1Aを参照すると、本発明の別の実施形態の一つには、一つ以上の演算機器70に常駐する、またはネットワーク機器に常駐し、そのネットワーク機器を介してアクセスできる、コンピュータのハード、ファームウェア及びソフトから成る一つ以上のリモート・プライバシー・クライアント60が、プライバシー・サーバー50として機能する一つ以上の演算機器へ、リクエストや問い合わせを送信したり、その演算機器からサービスやレスポンスを受信したりする、コンピュータネットワークを含めることもできる。ここで、前記プライバシー・サーバー50は、インターネット、複数のインターネット、イントラネット、その他のネットワークを経由して、電子情報を、電子的に情報を受信し保存する手段を含む、カード、携帯機器、装着可能な機器、その他ポータブル機器へ送信することもできる。ここで、前記カード、携帯機器、装着可能な機器、その他ポータブル機器は、データ属性やDDIDsについての情報は、前記プライバシー・サーバーにより修正されるため、当てはまるのであれば、その時まで、データ属性やDDIDsについての前記情報を含む。

【０２０１】

[252]プライバシー・サーバーとプライバシー・クライアントは、
ここに記述されたプロセスや機能の一つ以上のステップや動作を実行するプログラムコードを含むモジュールを実装することもできる。プログラムコードは、プライバシー・サーバーまたはプライバシー・クライアントのプロセッサによりアクセス可能な、コンピュータが読み取り可能な媒体上に、保存してもよい。コンピュータが読み取り可能な媒体は、揮発性または不揮発性であり、取り外し可能または固定型であってもよい。コンピュータが読み取り可能な媒体は、RAM、ROM、固体メモリ技術、書き込み・消去可能ROM(「EPROM」)、電子的書き込み・消去可能ROM(「EEPROM」)、CD-ROM、DVD、磁気カセット、磁気テープ、磁気ディスク記憶装置、その他磁気または光学記憶装置、その他従来の記憶技術または記憶装置であることができるが、これらに限定されない。

【０２０２】

[253]プライバシー・サーバーと関連するデータベースは、TDRs、期間・タイムスタンプ、DDIDs、属性、属性の組み合わせ、Data Subject、関係者、関連するプロフィールについての情報、及びその他関連する情報を記憶することができる。プライバシー・サーバーと関連するデータベースは、管理者により管理され、管理者によりアクセスされるが、一例において、管理者の承認がなければ、他者によっては管理されない。一例においては、一つ以上のプライバシー・サーバーの認証モジュールが、TDRsを経由したデータへのアクセスを管理する。プライバシー・クライアントは、望ましい対応、活動、プロセスまたは特性を実施し、また、TDRsが、リクエストされた対応、活動、プロセスまたは特性について、特定の時間や場所で参加する権限があるかどうか、プライバシー・サーバーへ問い合わせをするために必要な情報を、プライバシー・サーバーへリクエストすることもできる。また、プライバシー・クライアントは、データ外挿のためにデータベースへ戻る必要がないよう、トラッキングデータのような、プライバシー・クライアントに関連するTDRsが

係わる、対応、活動、プロセスまたは特性についてのデータを集約することもできる。一例においては、他者によって収集された洞察が、その期間、TDRの一部となることもできる。

【０２０３】

[254]本発明のある実施例において、抽象化モジュール52は、管理者(Data Subjectや関係者である)が、Data Subjectに関するデータを属性にリンクする、またはData Subjectに関する別のデータを、様々な属性の組み合わせに分けたり、組み合わせたり、再配置したり、加えたりできる属性にリンクすることができるように構成される。これらの組み合わせに、属性のいかなる組み合わせ、またはData Subjectに関連する、以前作成された属性の組み合わせを含むこともできる。

【０２０４】

[255]プライバシー・サーバーを含む、それぞれの意図された対応、活動、プロセスまたは特性についてのこの例では、抽象化モジュールにおいて、例えば、属性の中から、望ましい対応、活動、プロセスまたは特性について必要なものだけを選択し、それらのデータ属性を一つ以上の属性の組み合わせにリンクする、またはそれらのデータ属性を一つ以上の属性の組み合わせに分けることにより、送信され、または記憶された情報を特定する度合いを、管理者が制限することができる。そして、管理者が、それぞれの属性の組み合わせに対し、TDRが形成されるように、DDIDを動的に作成したり割り当てたりするために、抽象化モジュールを使用してもよい。DDIDは、所定の遅れやキューで失効するように構成することもでき、他の対応、活動、プロセスまたは特性に関連する、またはData Subjectや関係者に関連するデータに、再利用されてもよい。それによって、プライバシー・サーバーの外で関連性の詳細な跡を残さないようにすることができる。ある例では、TDRが形成されるようにDDIDを割り当てる、または受け付ける前に、抽象化モジュールが、DDIDが他のTDRにおいて使用中ではないこと検証することもできる。この検証を行うためには、停止の可能性やシステム・ダウンの時間に対処するために、追加の緩衝タイムアウト期間を含めることもできる。望ましい対応、活動、プロセスまたは特性について生成されるデータ属性の数と関連するTDRsの数が大きくなるほど、得られるプライバシー、匿名性、セキュリティも高くなる。この状況では、TDRsの一つへのアクセスを得ようとする承認されていない者が、TDRに含まれているその情報へのアクセスだけを得ることになる。ある例では、一つのTDRに含まれている情報は、望ましい対応、活動、プロセスまたは特性について必要な属性の一部であってもよく、さらに、必要な属性を含む他のTDRsを決定するのに、またはTDRsに関連しうるData Subjectや関係者を特定するのに必要な情報を提供しない。

【０２０５】

[256]ある例では、抽象化モジュールによるTDRsは、ステップに関連する属性の特定のカテゴリーと共に、異なる対応、活動またはプロセスを記述または実施するのに必要な所定のステップと一致する一つ以上のプロセスと、特定の対応、活動、プロセスまたは特性について必要な、これらの属性を選択または組み合わせることにより、作成されてもよい。抽象化モジュールによるTDRs作成のプロセスは、管理者により直接行われてもよく、管理者により承認された一人以上の者により間接的に行われてもよい。

【０２０６】

[257]例えば、クレジットカードによる購入の情報が含まれている第一のデータベースには、クレジットカード発行者が、購入情報についてビッグデータ解析を行うために必要な情報が含まれていてもよい。ただし、そのデータベースには、クレジットカードの使用者を特定する情報が含まれている必要はない。クレジットカードの使用者を特定する情報は、DDIDsによるこの第一のデータベースに代表されており、DDIDsとユーザーを関連付ける際に必要な置き換えキー(RKs)は、プライバシー・サーバーやシステムモジュールがアクセス可能な別の安全なデータベースに保存されていてもよい。このように、DDIDsと関連する情報は、承認されていない者へは解読不能であるため、クレジットカードによる購入の情報が含まれている第一のデータベースへ、承認されていない侵入があった場合、シ

ステムは、クレジットカードの使用者のアイデンティティ保護を助け、金銭的損失を制限する。

【０２０７】

[258]さらに、本発明の一例では、携帯・装着可能・ポータブル機器からのデータのリアルタイムまたは一括解析は、携帯・装着可能・ポータブル機器のユーザーのプライバシーや匿名性を犠牲にすることなく、業者やサービスプロバイダなどの受信者に有利なように行うことができる。各ユーザーは、機器そのものまたは機器の使用と関連するData Subjectであるだけでなく、問題となっている携帯・装着可能・ポータブル機器の関係者と考えることもできる。受信者から出されたスペシャルオファーや他の利権と引き換えに、携帯・装着可能・ポータブル機器のユーザーは、例えば、特定の地理的位置から所定の距離内(例えば、1マイル、1000フィート、20フィート、または実装時の距離)にいる、または携帯・装着可能・ポータブル機器の場所に対し、所定のカテゴリー内(例えば、宝石、衣類、レストラン、本屋、またはその他の分野)にいる受信者と、ユーザーのリアルタイムの場所、リアルタイムの活動に応じて、または特定の時間の間、匿名で共有されている、特定されないTDRsを持つことを選択することもできる。このように、受信者は、年齢、性別、収入、その他の特徴の観点から、顧客の分布について、正確な集約された情報を得ることが可能となる。関係者について、どのサービス、望ましい在庫や他のセールス、サプライチェーン、または在庫関連の活動を提供したらよいか、を受信者がより有効に決定することができるこれらの分布は、異なる場所、一日の時間、曜日に、携帯・装着可能・ポータブル機器のユーザーにより共有される、TDRsによって明らかにされ得る。ある例では、携帯・装着可能・ポータブル機器のユーザーでもあり得る、Data Subjectと関係者は、(単に、Data Subjectまたは関係者が登録したと知っているだけで、どの特定の情報がどの特定のData Subjectまたは関係者に関連するかは知らない)受信者に対し、Data Subjectと関係者が望まない限り、個人情報を開示することなく、特別なアレンジやオファーから利益を受ける。

【０２０８】

[259]本発明の実装における一例では、承認モジュールが管理者に、他の誰に、TDR情報へのアクセス権または使用権が与えられるのか、についての管理権限を与えることができる。管理者は、さらに、他の者が持っている、システムに含まれている情報の特定の要素へのアクセス権の度合を管理する抽象化モジュールを用いることも可能である。例えば、管理者としての携帯・装着可能・ポータブル機器のプラットフォームプロバイダは、機器、Data Subjectまたは関係者である使用者のアイデンティティ、または、機器、Data Subjectまたは関係者である使用者の場所を明らかにする必要なく、携帯・装着可能・ポータブル機器のメーカーに、パフォーマンスデータを、提供することもできる。また、携帯・装着可能・ポータブル機器のプラットフォームプロバイダは、機器、Data Subjectまたは関係者である使用者のアイデンティティを明らかにする必要なく、携帯・装着可能・ポータブル機器のアプリプロバイダに、携帯・装着可能・ポータブル機器が地図やそのほかのアプリを使うのに必要な、地理的位置データを提供することもできる。逆に、携帯・装着可能・ポータブル機器のプラットフォームプロバイダは、システムを用いて、Data Subjectまたは関係者である機器の使用者だけではなく、その機器に関する場所とアイデンティティのデータを、緊急911システムへ提供することもできる。承認モジュール実装の一例には、管理者によって承認された他者に、DDIDsと関連するTDRsの生成をリクエストする、権限の委任を許可することを含めてもよい。

【０２０９】

[260]本発明の実装の一例によれば、受信者は個人が特定されるような情報の明示を要求することなく、関係者が収集する、ユーザーの体験や、場所による機会をカスタマイズするために、携帯・装着可能・ポータブル機器の関係者についての情報を、使用することが可能である。例えば、リアルタイム、またはほぼリアルタイムで、カントリー・ウェスタンとゴスペルを演奏するバンドが、コンサートに来ているData Subjectまたは関係者に関連するTDRsを受信することにより、コンサートに来ている関係者の大部分がゴスペルが好

きと判断し、コンサートの選曲を調整することができる。同様に、賞品やスペシャルオファーを表示するビデオ画面を使用する店舗では、携帯・装着可能・ポータブル機器のクライアントの顧客である、Data Subjectまたは関係者に関連するTDRsを受信し、分析することにより、店舗経営者は、リアルタイムで、いつ店舗に特定の分布の顧客が多いかを知ることができる。その店舗では、特定の分布を狙ったビデオを流し、携帯・装着可能・ポータブル機器のクライアント経由の店舗のシステムと通信しながら、Data Subjectまたは関係者の変化に対応し、一日を通してビデオを変えることができる。TDRsにおける情報より得られた分布には、Data Subjectまたは関係者の年齢、性別、収入のレベルが含まれていてもよいが、限定はされない。同様に、店舗内のある顧客の特定の場所を識別する、リアルタイムの地理的位置を使用している店舗では、Data Subjectまたは関係者の個人的な好みやブランドの好み、賞品購入の好みに関連するTDRsを受信して解析することにより、Data Subjectまたは関係者である顧客に対し、携帯・装着可能・ポータブル機器を経由して、スペシャルディスカウントやオファーを出すことができる。ここで、TDRsには、Data Subjectまたは関係者がいる店舗内の場所に置かれている商品に基づき、リアルタイムで付加される外来の情報が含まれる。

【０２１０】

[261]本発明の実装の一例として、プライバシー・サーバーは、DDIDと望ましい属性の組み合わせが結びつく間、TDRsを作成するため、プライバシー・サーバーの抽象化モジュールは、DDIDsを、Data Subjectの機器、サービスプロバイダの機器、アクセス可能なクラウドネットワーク、または同じ演算機器を含むがこれらに限定されない多数の場所に常駐している、プライバシー・クライアントからのリクエストや問い合わせに応じるのに必要な属性の組み合わせに割り当てる。プライバシー・クライアントのTDRは、設定された時間、対応、活動、プロセス、または特性の間、受信者と自由に交流することもできる。一例では、指定された受信者との交流の期間が終ると、プライバシー・クライアントは、プライバシー・クライアントの活動についての属性の組み合わせにより拡張されたTDRを、プライバシー・サーバーと関連するデータベースへ返却してもよい。そして、プライバシー・サーバーは、安全なデータベースにある、Data Subjectの集約されたデータプロフィールの属性の組み合わせを更新し保存するだけでなく、様々な属性の組み合わせを特定のData Subjectへ付け戻してもよい。一例では、この時に、属性の組み合わせに割り当てられたDDIDを、データの関係を不明のままにするために、他の対応、活動、プロセスや特性について、またはData Subjectに対して、再度割り当ててもよい。

【０２１１】

[262]本発明の他の実施例を、様々なシステムや機器を含め、詳細に述べる。ある実施形態では、電子データセキュリティを向上するシステムが開示されている。一例では、システムは、少なくとも一つの属性を少なくとも一つのData Subjectに動的に関連付けるように構成されている抽象化モジュール；DDIDsを生成、またはDDIDsとして機能する、時間的に固有で動的に変化する値を受信または変更するように構成され、さらに、DDIDを少なくとも一つのData Subjectに関連付けるように構成されている抽象化モジュール；およびDDIDsに関連する活動を記録するように構成され、また、いずれかの追加のDDIDs、記録された活動、そしてタイムキー(TKs)またはその他を用いて記録された活動を実施するのにDDIDsが使用される時間を関連付けるように構成されている維持管理モジュールを含んでもよい。一例においては、前記抽象化モジュールは、少なくとも一つのData Subjectに関連する属性を追加または削除するように構成され、また、抽象化モジュールは、少なくとも一つのData Subjectに既に関連する属性を変更するように構成されてもよい。

【０２１２】

[263]他の実施例では、ネットワーク上での安全でプライベート、匿名の活動を実施する機器が開示されている。一例では、前記機器は、プログラムモジュールを実行させるように構成されたプロセッサであって、前記プログラムモジュールは少なくとも一つのプライバシー・クライアントモジュールを含み；プロセッサに接続されたメモリ；および、ネットワーク上でデータを受信する通信インターフェース；を含んでもよく、Data Subjectの

機器、サービスプロバイダの機器、アクセス可能なクラウドネットワーク、または同じ演算機器に、プライバシー・サーバーとして常駐する前記プライバシー・クライアントは、プライバシー・サーバーから、ネットワーク上での活動を実施するために必要なDDIDsや関連するデータ属性を含むTDRsを受信するように構成されている。一例では、前記プライバシー・クライアントは、さらに前記機器を用いて実施された活動をキャプチャするように、また実施された活動を前記TDRsに関連付けるように構成されていてもよい。他の例では、前記プライバシー・クライアントは、キャプチャされた活動とTDRsを前記プライバシー・サーバーに送信するように構成されていてもよい。一例では、前記プライバシー・クライアントは、携帯アプリとして、携帯機器に常駐していてもよい。他の例では、前記プライバシー・クライアントは、クラウドベースのアプリとして、アクセス可能なネットワーク上に常駐していてもよい。他の例では、前記プライバシー・クライアントは、前記プライバシー・サーバーが、ローカルアプリとして常駐している、同じ演算機器に常駐していてもよい。

【０２１３】

[264]他の例では、前記機器は、地理的位置モジュールを含んでいてもよく、ここで、前記TDRsは地理的位置モジュールからの情報で変更され、前記TDRsは前記機器のアイデンティティについての情報へのアクセスを制限する。前記機器は、前記DDIDを変更するオプション、または特定のTDRに関連したデータ属性を含む、前記TDRsを変更することを、ユーザーに許可するように構成されたユーザーインターフェースを含んでもよい。前記ユーザーインターフェースは、前記携帯機器に、所定の物理的、仮想的、または理論的に近接する他のネットワーク機器とだけ、前記TDRsを共有する選択可能なオプションを含むこともできる。

【０２１４】

[265]他の例では、前記機器は、TDRsに応じて、物理的、仮想的、または理論的場所に応じた、狙った広告または販売情報を受け取ることもできる。ここで、前記TDRsは、前記機器のユーザーに関連する分布情報を含み、さらに分布情報に応じた狙った広告または販売情報の受信を含む。他の例では、前記TDRsは、前記機器を用いて、または用いることの望ましい、購入取引に関する情報を含んでもよく、さらに、以前のまたは望ましい購入取引に応じて、狙った広告または販売情報の受信を含む。

【０２１５】

[266]本発明の他の実施例では、電子データのプライバシーと匿名性を提供するシステムが開示されている。一例では、前記システムは、ユーザー機器上で動作する第一プライバシー・クライアントを持つ、少なくとも一つのユーザー機器；サービスプロバイダ機器上で動作する第ニプライバシー・クライアントを持つ、少なくとも一つのサービスプロバイダ機器；および、ネットワークと連動する少なくとも一つのプライバシー・サーバーであって、前記第一および第二のプライバシー・クライアントと通信する、前記プライバシー・サーバーを含んでいてもよく、前記プライバシー・サーバーは、電子的にData Subjectをデータ属性と属性の組み合わせにリンクし、データをデータ属性と属性の組み合わせに分割する抽象化モジュールを含み、前記抽象化モジュールはDDIDを前記データ属性と属性の組み合わせに関連付ける。一例において、前記プライバシー・サーバーは、一つ以上の前記DDIDsを生成する承認モジュールを含んでいてもよい。他の例では、前記プライバシー・サーバーは、前記DDIDsの組み合わせを、それらと関連するデータ属性と属性の組み合わせと共に保存する維持管理モジュールを含んでいてもよい。他の例では、前記プライバシー・サーバーは、データ属性、属性の組み合わせ、DDIDsの集約を検証する検証モジュールを含んでいてもよい。他の例では、前記プライバシー・サーバーは、エラーが起きた際に、一つ以上の事後捜査分析に使用するため、前記DDIDsとデータ属性に関連する情報を収集し保存するアクセスログを含んでいてもよい。一例では、前記DDIDは、所定の時間後に無効となり、前記抽象化モジュールが、前記DDIDを他のデータ属性またはData Subjectに割り当てる。

【０２１６】

[267]図1Bは、DDIDsの割り当て、適用、無効、再利用がどのように起こるか、いくつかの例を示している。ここで、本発明の実施形態の実装において、DDIDsは永久に存在するかもしれないが、複数のData Subjectやデータ属性、属性の組み合わせ、対応、活動、プロセス、特性に再利用されてもよい、ということに留意されたい。DDIDは再利用されるが、管理者により望まれ承認されていない限り、二つの同一のDDIDsを同時に使用することはできない。DDIDsの再割り当ては、同様の属性の組み合わせまたはData Subjectへ、または明確に異なる属性の組み合わせまたはData Subjectへ、DDIDsを再度割り当てる、既存のデータ収集と分析機能を用いて達成されてもよい。この再割り当てにより、動的に作成され、変更可能なデジタルDDIDsのプライバシー・匿名性とセキュリティの可能性が高まる。

【０２１７】

[268]図1Bに示されているように、システムは、いずれのDDIDの割り当てや失効、再利用が、以下のどの一つまたは一つ以上に対して起こるように構成されてもよい。(1)DDID(と関連するTDR)が作成された目的、例えば、特性の閲覧セッションやData Subject、取引等に関連する目的、における変化；(2)DDID(と関連するTDR)に関連する物理的場所における変化、例えば、物理的場所を出る、一般的な物理的場所への到着、特定の物理的場所への到着、物理的場所へ入る、その他物理的場所での動作；(3)DDID(と関連するTDR)に関連する仮想的場所における変化、例えば、仮想的場所へ入る、仮想的場所の変化、仮想的場所を出る、ウェブサイトの特定のページへの到着、特定のウェブサイトへの到着、またはその他仮想的場所での動作；および、または(4)時間の変化に対して、例えば、ランダムな時間で、所定の時間で、指定された間隔で、またはその他一時的な基準で理解されているように、システムに対して外部では、関連するデータと、Data Subjectまたは関係者のアイデンティティ、または異なるDDIDsやTDRsに関連する文脈データの間に、認識できる関係がないため、DDIDsは、データを文脈から切り離す。システムに対して内部では、Data Subjectや信頼できる者・代理人により承認されているため、関係情報は、使用できるように維持されている。

【０２１８】

[269]図1C-1に、信頼できる者または信頼できる代理人(図1C-1に「信頼できる代理人」と示されているが、以後「信頼できる代理人」や「信頼できる者」と称す)の視点による、信頼のサークル(CoT)の概念を示す。まず、図の左下にData Subjectが含まれている。Data Subjectによる参加は、一般的に、従来の「告知と同意」モデルを用いた、「交渉の余地なし」のオンライン利用規約に同意するかどうかの二分決定の形式をとるため、最新のデータを使用するシステムの図には、Data Subjectが含まれていない。初期点の後、「商品であって、顧客ではない」ため、Data Subjectは通常、それらのデータに起こることに影響を与える全ての権限を失う。これは、デジタルの時代において、壊れたモデルであり、現時点のまたは将来のデータ使用を有効に制限することは殆どないということが熟知されている。

【０２１９】

[270]一つの信頼のサークルと関連して、協力して働く二人以上の信頼できる者がいて、Data Subjectはいくつもの信頼のサークルに参加することもできる、ということに留意されたい。信頼のサークルは、より高いセキュリティのために、集中化された、または連合化されたモデルにより、実施することができる。図2の矢印は、データの動きを示している。データ入力と出力が異なる情報を含む。

【０２２０】

[271]図1C-1には、本発明の二つの実施形態のためのデータ処理の流れが示されている。本発明の第一の実施形態例では、ユーザー(1)が、ウェブ閲覧における望ましいアクションに参加するために、この実施形態例では、一つ以上のTDRs(各TDRは当初TDRと関わる活動に関連するデータ属性を収集し保持することを目的としたDDIDから構成される、またはData Subjectの集約されたデータプロフィールから取り出されたデータ属性または属性の組み合わせと共にDDIDから構成されてもよい)を形成することにより、特定のData Subje

ct(この例では、ユーザーがData Subject)についてのデータ入力を作成するシステムの使用に興味があるということを示すこともできる。一つ以上のTDRが係わるウェブ閲覧に関連するデータは、システムにより記録され収集され、信頼できる者や信頼できる代理人(3)として機能する管理者へ送信される。ウェブ閲覧に関連して収集され記録されたデータを反映するTDRsは、信頼できる代理人として機能する管理者が、ユーザーやData Subjectの集約されたデータプロフィールを増補するために選択する、ウェブ閲覧からの出力を示す。本発明の第ニの実施形態例では、ユーザー(2)はユーザーが所有し、Data Subject(1)についての個人情報を含むデータセットの、プライベートで匿名のバージョンを作成するために、システムの使用に興味があるということを示すこともできる。この例では、Data Subjectについての個人情報を含むユーザーのデータセットは、システムへの入力として機能してもよい。システムは、個人情報を反映しているデータセットに含まれるデータ値を特定し記録することもでき、信頼できる者または信頼できる代理人(3)として機能する管理者により行われる処理により、Data Subjectについての個人情報を再度特定するために、一つ以上の置き換えキー(RKs)が必要となるDDIDsと置き換わる、その個人情報を選択することもできる。この例では、その結果得られる変更されたデータセットは、Data Subjectの個人情報の代わりに、動的に変化するDDIDsを含むシステムからの出力を示す。この様に、どの一人または複数のData Subjectに関する個人情報へのアクセスが再度特定されることがなく、該当するData Subjectが「忘れ去られる権利」を持つ、すなわちインターネットからデジタルの記録を削除することができるように、RKsを将来変更することもできる。

【０２２１】

[272]図1C-1の、「プライバシーについての方針」と「承認リクエスト」とラベルされたボックスに示されているように、信頼できる者・代理人により管理される許可(「PERMs」)に合わせ、データの使用は「ユーザー」により管理され得る。「ユーザー」は、取り上げられているデータの対象者であるData Subject自身(例えば、自身のデータについての、ユーザー、消費者、患者等、ここでは「対象ユーザー」とする)であることもでき、取り上げられているデータの対象者ではない第三者(例えば、販売者、業者、医療提供者、合法的に許可された政府団体等、ここでは「非対象ユーザー」とする)であることもできる。

【０２２２】

[273]また、どのデータが誰によって使用されるか、何の目的で、どのくらいの期間等、許可された動作に関連するPERMsは、Data Subjectのアイデンティティや活動に対し、匿名性を提供する文脈で、いつ、どこで、どのようにDDIDsを使用するか、他のプライバシーを高める技術をDDIDsと関連してまたはDDIDsの代わりにいつ使用するか、取引を促す特定の情報をいつ提供するか、等の望ましい匿名性のレベルを指定することもできる。

【０２２３】

[274]本発明のData Subject実装(すなわち、DRMI)において、対象ユーザーは、微粒度の動的許可に解釈される、またはより詳細な動的パラメーターを指定する際に「カスタム」オプションとして選択される、所定の方針によりデータを使用する際のカスタマイズされたPERMS(例えば、ゴールド・シルバー・ブロンズ。これはあくまでも一例であり、数学的には、離散の選択肢のセット、または下限と上限の間の連続な値により表されてもよい、ということに留意されたい)を確立することもできる。

【０２２４】

[275]Dynamic Anonymity(DRMD)の「管理」実装において、非対象ユーザーが、適用される会社の、法律や規制によるデータ使用、プライバシー、匿名性の要件に準拠し、データの使用・アクセスを可能にするPERMsを確立することもできる。

【０２２５】

[276]PERMSに基づき図1C-1に反映されているCoT内では、ビジネスインテリジェンス、データ解析、その他の処理が以下の表3に示されているように、一つ以上のData Subjectについて、I、D、T、Xの組み合わせまたは補間により処理されてもよい。

【表３】

“I” Data Subject の識別子	“D” 値が指定された動的匿名子	“T” IとDが関連する間の時間	“X” T間の関連データ

【０２２６】

[277]図1C-2には、Data Subjectの視点からの信頼のサークル(CoT)が示されている。

【０２２７】

[278]図1Dには、地理的位置と血圧のレベルの両方を記録することができる、スマートフォンのアプリが図示されている。Dynamic Anonymityを用い、そのような機器はデータを二つの流れに分け、どちらの流れも、阻止されたり、侵害されたり(保存され検査されたり)した場合、CoT内に保護されている重要な情報を追加することなく、個人データ(PD)が明らかにならないよう、それぞれ隠された状態にすることができる。

【０２２８】

[279]とりわけ、図1Dには以下が示されている。

1.血圧モニターアプリ(A)は、信頼のサークル(B)内の信頼できる者に連絡し、Data Subjectである患者のDDIDをリクエストする。

2.信頼のサークルCoTは、Data SubjectのDDIDを提供する。

3.信頼できる者により運営されているアプリは、二つの周期的に変化する情報セット(一つはGPSデータ、もう一つは血圧のレベル)を返す。それぞれのセットは、DDIDs、オフセット(血圧レベルデータと地理的位置を隠すため)、時間周期ごとに更新される暗号化キーから成る。(これらは、後の使用のため、データベースに保存される。)

4.モニターアプリは、二つの暗号化され、隠されたデータの流れを、Dynamic Anonymityにより管理されている「代理人」アプリまたは社内ネットワークのネットワークアプライアンス(C)へ送信する。(ここで、場所とレベルは、それらに適用される、共に周期的に変化するオフセットを持つ。)

5.「代理人」(C)は、信頼できる者からのデータの流れ(DとE)(暗号解読キーだけが含まれている)を使用し、送信されたデータを「平文」へ変換する。また、代理人は、入って来るIPアドレスを隠し、DDIDsと隠された血圧レベルデータ(F)またはGPS位置(G)のデータの流れ(複数のData Subjectの情報を含む)を対応するデータベース(H)と(I)に提供する。

【０２２９】

[280]図1Dにおいて、信頼のサークルの外(とスマートフォンそのものの外)の各点では、患者のデータは保護されている。個人データ(PD)は利用可能になったり生成されたりしない。

- 信頼できる者(1と2)へ、また信頼できる者からの送信には、プライバシーや匿名性を侵害する個人データは含まれず、信頼できる者のデータベースに保存されることもない。
- 場所と血圧のレベル(4)は、データそのものが、患者の真の場所や血圧のレベルについて、直接的または間接的に、何かを公開したり、何かを含んでいたりすることのないよう、別々に送信され(どちらか一つの流れを阻止すると何も公開されない)、DDIDsにより施錠され、隠されている。
- Dynamic Anonymityの代理人(C)は、データを暗号解読するために、信頼できる者に接続されていなければならない(中間者攻撃を防ぐ)。それぞれは、元々のIPアドレスが暗号解読されたデータに関連付けられていることのないよう、暗号解読後、複数のデータの流れを統合させる。
- 停止したら、二つの別のデータベース(HとI)に常駐している場合、ホストの会社でも二つの関係を引き出したり、ましてデータを生成したData Subjectにそれぞれのセットのデータをリンクさせることができないように、血圧レベルと場所データはそれぞれ異なるセットのDDIDsを持つ。

【０２３０】
[281]図1Eには、新しいクリニックが、性感染症(STDs)のある20歳から30歳の患者を診察するのに、その場所を選ぶタスクをサポートする、本発明のある実施形態の使用が示されている。一つの「クレンジング」されたデータセットは、プライバシーと匿名性を保護するために、近隣から集約された、STDsの発生率を示してもよい。別のデータセットは、それぞれの近隣に患者が何人住んでいるかを示すこともできる。しかし、これらが集約されても、正確にいくつのSTDsと特定されたケースが、特定の年齢層に入るか、知ることはできない。
【０２３１】
[282]Dynamic Anonymityは、解析の二つの異なるモードをサポートすることにより、このジレンマを緩和する。
【０２３２】
[283]データが外部へさらされなければならない場合(すなわち、CoTの外)、個人データの要素は隠され、DDIDsとして符号化され、その結果の関連性と共に、CoTの内部に保存される。さらに、必要であれば、データ(またはフィールド)タイプ識別子は、同様にして隠される。
【０２３３】
[284]そして、解析された後、解析の結果を、(許可されれば)元のData Subject、フィールドタイプ、値に関連付け戻すことができる。
【０２３４】
[285]別の方法では、CoT内の異なる信頼できる者の間、同一の信頼できる者内の異なるデータストアの間、または信頼できる者とデータストアがCoT外にあるアプリ開発者の間で、連合化され、匿名化された問い合わせの使用を通して、Dynamic Anonymityにより無損失の解析ができる。
【０２３５】
[286]再び、STDsのある20歳から30歳の患者を診察するのに、クリニックを開設する場所を選ぶ問題を考える。Dynamic Anonymityシステムは、ターゲットとなる問い合わせが複数のデータストアに及び、それぞれの参加者が何の目的か分からないため、PDが漏洩するリスクもないように、問い合わせを分割することを許可することにより、既存の技術を向上させる。
【０２３６】
[287]このシナリオでは、複数の(かなり広い)地理的エリア内の、STDsのある20歳から30歳の患者の数の問い合わせが、信頼のサークル内にある多数の信頼できる者へ出される。この集約問い合わせは、以下のようないくつかのステップに分けられる。
1.広い地理的エリアで、20歳から30歳の患者を探す。
2.STDsのある患者だけを選ぶ。
3.彼らのプライバシーと匿名性の方針がこのレベルの解析を許可する患者だけ選ぶ。
4.これらの結果をこれらの患者の自宅の住所に「結び付ける」。
5.これらの結果を近隣エリアごとに集約し、患者の数だけ明らかにする。
【０２３７】
[288]この問い合わせを満たすのに必要なアクションは、全く異なるデータストア、異なる団体に及ぶが、もちろん信頼のサークルによって保護され、促進されている。
【０２３８】
[289]図1Eには、以下のプロセスが示されている。
1.将来のクリニックのオーナーが、信頼できる者に問い合わせを送り、STDsのある20歳から30歳の個人を探してくれるよう頼む。
2.信頼できる者は、医療に関連したデータストアに連絡し、STDsのある20歳から30歳の個人を探してくれるよう頼む。
3.医療に関連したデータストアが一致する記録を探す(識別可能なキーによってではなく、DDIDsで判断する)。

4.一致するDDIDsが信頼できる者へ送信される。
5.信頼できる者は、特定された個人を明らかにするため、これらのDDIDsを解く。
6.信頼できる者は、この特定の問い合わせを許可するプライバシーと匿名性の方針を持つ個人別に、そのリストにフィルタをかける。
7.CoTは、彼らの住所のデータベースを用い、近隣エリア別に、人数(または、問い合わせが不完全な場合、発生率)を集約し、望まれる結果を出す。

【０２３９】

[290]このシナリオでは、医療に関連するデータベースを運営している会社は、彼らが処理するデータの持ち主である患者のアイデンティティ、場所、他の特定可能な情報を知る(または漏洩する)必要はない。彼らが処理する記録はDDIDにより施錠され、いずれ隠される。そのため、特定の問い合わせを実施する際、またはその結果を送信する際、個人データは生成されない。

【０２４０】

[291]問い合わせをする者は、この情報にアクセスすることはできないということに留意されたい。CoTとの係わりは、問い合わせをし、高レベルで集約されたPDを含まない結果を受け取ることのみである。この情報にアクセスできないことで、結果の質や正確さ、精度に影響が出るということはない。従って、Dynamic Anonymityは、最終結果に寄与し、どの者にも何の利益もなくプライバシーと匿名性を脆弱にする個人データを排除する。関連性のないデータ、時間と手間のかかる解析をフィルタすることで、Dynamic Anonymityは受け取った情報の利用性と価値を確かに増している。

【０２４１】

[292]個人データは、信頼できる者により管理される信頼のサークル内(そのような情報にとって適切な場所)で、DDIDsが解かれる時のように、一時的に生成されるだけである。そのような動作は過渡的で、意図された問い合わせの結果以外に跡を残すことはなく、より高いセキュリティのために、特定の専用サーバーに制限されている。信頼のサークルの文脈内でのDDIDsの使用により、差別的または特定可能な結果を出し得る通常のデータ解析における欠陥を避けることができる。

【０２４２】

[293]図1Fには、本発明における一つの実施形態の使用が示されており、靴メーカーが、最近、ある市内でランニングに関するウェブ検索をした人々に、新しいラインの靴のクーポンを送ることができる。靴のディスカウントを提供する代わりに、そのメーカーは対象となる消費者のメールアドレスと住所を受け取り、クーポンを使用した人には、新しい靴の満足度を調べるアンケートを送りたい。

【０２４３】

[294]説明：
1.CoTの外にいるメーカーは、サーチエンジンから一致するDDIDsのリストを購入する。
2.Data Subjectのメールアドレスと住所へのアクセスを許可する(受け入れられた場合には)、オファーレターとポリシー変更と共に、DDIDsは一つ以上の信頼できる者へ提出される。
3.それぞれの信頼できる者は、オファーレターを、DDIDsと一致するData Subjectへ転送する(そのようなオファーを受け取ることをオプトインしている場合)。
4.Data Subjectである受取人がオファーを受け取ると、受取人のポリシーは、住所とメールアドレスを靴メーカーへ公開することを許可するように(一時的に)更新される。
5.この特定のオファーと限定された期間だけであるが、CoTの一部となった靴メーカーは、クーポンを受け取りたい人の住所とメールアドレスのリストを受け取る。このリストは、靴メーカーにとって、正確で的が絞られており、それゆえ最大の価値があるものでなければならない。これは、まさしく、より高いプライバシーと匿名性により、CoTが情報の価値を上げるということになる。靴メーカーは、メーカーのオファーに大いに興味のある人々へ、このようにしてメールや手紙が届くということで安心する。

【０２４４】

[295]図1Gは、GPSを用いた血圧モニターにより、Dynamic Anonymityを通して、患者の場所と血圧を確実に記憶する図1Dの例を基に立てられている。Dynamic Anonymityは以下のように活性化される。
1.保有しているデータに個人データが含まれていない場合、データ処理の流れに係わる経営者による、HIPAAデータの対処の負担を減らす。
2.医者によるデータへのアクセスと使用は、確実にHIPAAの義務を満たす。
【０２４５】
[296]以下のシナリオは、Data Subjectである患者とその医者が共に信頼のサークル内にアカウントを持つ場合を想定している。
【０２４６】
[297]説明：
1.モニタリングアプリは、患者の信頼できる者と協力し、医者が患者の血圧のレベル(GPS位置データではなく)にアクセスできるように、患者にそのプライバシーと匿名性のポリシーを更新することを許可する。この許可は、一時的(スナップチャットで共有される写真の一時限定性のように、一定時間後にこの許可は失効する)、または継続的でもよい。
2.医者は、(ウェブブラウザを経由して)モニター会社のサーバーではなく、医者のブラウザで動作する、ジャバスクリプトベースの血圧レベル閲覧アプリが立ち上がる、血圧モニターのウェブサイトを閲覧する。(すなわち、データを個人特定可能にする必要がある作業は、それ自身信頼されている、信頼できる者のサーバーを通して行われる。以下のステップ4と5を参照のこと。)
3.血圧レベル閲覧アプリは、医者に信頼できる者を介してログインするように促し(フェイスブック（登録商標）やグーグル（登録商標）のアカウントを用いて承認を取ること許可する、多くのアプリと同様)、信頼できる者に対し、自分を特定するためのセッションクッキーを受け取る。 (フェイスブック（登録商標）は、フェイスブック社の商標である。)
4.医者が閲覧できる時間の範囲を選択した後、閲覧アプリは、その患者の対応するDDIDsとオフセットを信頼できる者にリクエストする。
5.信頼できる者は、(患者のプライバシーと匿名性のポリシー規約を確認し)この情報への医者のアクセスを有効にし、DDIDsとオフセットを返す。
6.閲覧アプリは、自身の会社のウェブサイトへ連絡し、DDIDsに対応する血圧データをリクエストし、結果を受け取ってオフセットを適用し、血圧レベルをグラフにまとめる。
【０２４７】
[298]ここで、医者の画面上のイメージは、保護されたPHIデータである、HIPAAになる。医者がデータを印刷すると、その紙は、HIPAA対象となる。医者がグラフを閲覧し終わると、医者はログアウトまたはブラウザを閉じ、アプリは終了、データ消去となる。
【０２４８】
[299]再度特定された、HIPAAにより管理されているデータは、医者のブラウザにのみ常駐する。元々のアプリプロバイダのデータベースに保存されている血圧レベルデータは、手つかずで隠されたままとなる。信頼できる者のデータはも、同様に影響なしとなる。
【０２４９】
[300]血圧データを閲覧する許可は、信頼のサークル内のみで強制される。閲覧アプリだけでは、またはアプリの元のサーバーだけでは、(一般的なやり方同様に)強制はできない。このことは、データは、いかなる利用可能または特定可能な形態ではそこには存在しないため、侵入者は、血圧レベル閲覧アプリにハッキングするだけでは、非承認のアクセスを得ることはできない、ということを示す。「信頼のサークル」の動的データのプライバシーと匿名性の管理機能と共に、Dynamic Anonymity DDIDsの動的データ隠蔽機能により、データのプライバシーと匿名性、および個別化された医薬品・医学リサーチをサポートする価値が最大限に高まる。
【０２５０】
[301]図1Hでは、1H-Aに示される異なるノードは、Data Subjectのそれぞれに対し、関連付けられている、または再度特定可能であるため、第三者によるトラッキング、調査や

解析ができる二人の異なるData Subjectに関するデータ要素を示している。1H-Bは、文脈の損失なしに、Dynamic Anonymityと共に保持される同じデータの要素を簡略化し、図示している。家族教育における権利とプライバシー法(FERPA)は、個人特定可能な情報(PII)を公開する、生徒の教育記録へのアクセスと開示を規制する、連邦政府によるプライバシーについての法律である。ただし、FERPAによると、PIIは開示されない。PIIが記録から削除された場合、その生徒は匿名となり、プライバシーは保護され、その結果特定されないデータが開示される。法律で定義されたカテゴリー(名前、アドレス、ソーシャルセキュリティー番号、母親の旧姓、等)に加え、FERPAはPIIを以下のように定義する。「対象となる事情について個人的に知らない、学校のコミュニティにおいて妥当な者に、妥当な範囲で生徒を特定することを許可するような、単独または組み合わせて、特定の生徒に繋がる、または繋がりえる情報。」1H-Bに示されているように、Dynamic Anonymityの、Anonos可能な信頼のサークルを用い、管理された状態で、Data Subjectそれぞれとデータ要素の関係を曖昧にする機能により、PIIを開示することなく、教育に関連するデータを使用することができる。

【０２５１】

[302]図1Iには、本発明の一つの実施形態により、分離レベル決定(DLD)を行い、匿名性測定スコア(AMS)を作成するプロセスの例が示されている。DLDの決定には、適切な許可なしの侵入者による特定や再度関連付けの確率を低くするために必要な分離のレベルを評価するために、分離前のデータ要素の独特性の数学的、経験的解析が必然的に含まれる。DLDの値は、異なるタイプのデータ要素に適した分離・置き換えにふさわしいレベルを決定するための入力としても使用される。

【０２５２】

[303]AMSは、慎重な取扱いを要する、個人が特定され得る情報が、第三者により、匿名性の層レベルやカテゴリーにまで認識可能になることについて、数学的に求められた確定性のレベルを相関付けるためにも使用される。言い換えると、AMSの値は、データが使用される前に必要な同意のレベル・タイプを決定する、分離・置き換えアクティビティからの出力を評価する際に使用することもできる。

【０２５３】

[304]図1Iのステップ(1)では、データ属性は、DLDsを審査するために評価される。すなわち、データの要素は、匿名性保護が望ましく、個人的で、慎重を要し、特定するような情報等を、直接的・間接的に公開することが起こり得るかどうかを決定するために、分析される。ステップ(2)では、少なくとも部分的に、決定されたDLDsに基づき、分離の手段により、データ要素は動的に匿名化される。さらに、データ要素は、置き換えの過程も経る。ステップ(3)では、DDIDsの分離・置き換えの後、データ属性についてのData Subjectのアイデンティティが、第三者により認識され得ることと相関する、AMSを計算するために、例えば、数学関数・アルゴリズム(例えば図1Jに出力が反映されるような数学関数・アルゴリズム)を用た計算が行われる。最後に、ステップ(4)では、上記ステップ(3)で計算されたスコア・評価が、以下の図1Kに反映されている、AMSの使用の例のように、Data Subjectによる同意・関与を必要としない匿名化されたデータ属性について、第三者が、どのレベルの裁量・使用を行使するか、に対し、匿名化されたデータ属性についてのData Subjectにより必要とされる、同意・関与のレベルを特定するのに使用される。

【０２５４】

[305]異なる情報のカテゴリーには、再度識別され得ることの異なる統計的確率が含まれる。全てのデータ要素は、起こる配置、順番、頻度により決定される他の複数のデータと組み合わされた時の独自性のレベルだけではなく、固有の独自性のレベルに関連している。例えば、単一データ点を見た時に、女性か男性かの確率は各人に対しほぼ1：1であるため、性別のような単一データ点よりも、ソーシャルセキュリティー番号は、固有性が高く、より簡単に再特定されやすい。性別は、ソーシャルセキュリティー番号に比べ、識別子としては固有性が高くないため、ソーシャルセキュリティー番号に比べ、誰かを再特定するのに、独立して、性別が使われることはあまりない。

【０２５５】
[306]データ要素に適用された関連切り離しまたは置き換えのレベルや度合により、複数の評価を作成するために、匿名性測定スコア(AMS)の測定体系は、再特定の統計的確率に結び付く。単一データ点の例として、関連切り離しや置き換えが全くされていない、ソーシャルセキュリティー番号は、その固有性により再特定のリスクが非常に高いと分類されるという意味で、AMS評価100となり得る。一方で、関連切り離しや置き換えなしの単一データ点識別子としての性別は、非特定化対策なしでも再特定のリスクが低いと分類されるため、AMS評価10となり得る。
【０２５６】
[307]単一データ点としてのソーシャルセキュリティー番号を用いた例において、レベル1実装では、当初割り当てられた値、すなわち永久割り当て(例えば、データがハードコピーの状態で使用される場合)を保持しつつ、DDIDsを関連切り離しや置き換えの目的で割り当てることもできる。ソーシャルセキュリティー番号の場合、レベル1がDDIDsに適用されると、AMSスコアが10%減り、変更されたAMSスコアは90になる。これにより、再特定に関連するリスクのレベルは依然高いが、関連切り離しや置き換えがされていない要素よりも、より安全である。
【０２５７】
[308]レベル2実装の例では、ソーシャルセキュリティー番号は、当初割り当てられた値を、その値がある一方向、すなわちその場の変化性で変化するまで保持しつつ、関連切り離しや置き換えの目的で割り当てられたDDIDsを持つ。(例えば、新しい情報を、情報を電子的に受け取り保存する機能を含む、リモートカードや、携帯、装着可能、その他ポータブル機器に送信することにより、データの値が一方的に変えられる場合。)ソーシャルセキュリティー番号のAMSスコアは、それによりさらに10%減り、AMSのAMSスコアを達成することになる。
【０２５８】
[309]この例では、レベル3実装へと続くが、ソーシャルセキュリティー番号は、当初割り当てられた値を保持しつつ、関連切り離しや置き換えの目的で割り当てられたDDIDsを持つが、そのDDIDsは二方向に、すなわち動的変化性で変化する。(例えば、特定のデータを受け取り、それを動的に変化させることができる機能を持つ、クライアントやサーバーとクラウドや企業の機器の間で動的にデータを送受信することにより、データの値が双方に変化する場合。)ソーシャルセキュリティー番号のAMSスコアは、さらに50%減り、40.5となる。
【０２５９】
[310]DDIDsを使用し、関連切り離しや置き換えにより、非特定化対策をデータ点に適用することで、再特定のリスクは低くなる。AMSスコア決定は、一緒についてきた識別子の再特定の確率の関数から派生している。データ要素を曖昧にするために用いられる複数のプロセスと合わさり、このプロセスは、許可された使用、データ使用前に使用者が必要となる許可のレベルなど、様々な機能を決定するために、カテゴリーや他のタイプの分類体系へと分けられる。このプロセスは、単一または集約されたAMSスコアに適用できる。集約されたAMSスコアは、組み合わされたデータ点の固有性のレベルを表すために合成されたAMSスコアとして表される、複数のデータ点の再特定の起こりやすさを表している。
【０２６０】
[311]可能なカテゴリー分類体系の例として、AMSスコアは、カテゴリーA、B、Cに分けられる。ここで、カテゴリーAは、単一または集約されたスコアが75以上のデータであり、Data Subjectの現時点での、明確、明瞭な同意がある場合のみ使用可能である。カテゴリーBは、単一または集約されたスコアが40から74.9であり、Data Subjectの(i)現時点または(ii)事前の明確な同意がある場合に使用できるデータセットに適用される。カテゴリーCは、単一または集約されたスコアが39.9以下であり、Data Subjectの同意なしにデータセットを使用できる場合である。
【０２６１】

[312]図1Jに示された例においては、上記で議論されたソーシャルセキュリティー番号以外の識別子(すなわち、クレジットカード番号、ファーストネーム、ラストネーム、生年月日、年齢、性別)それぞれについて、関連切り離しや置き換えなしのAMSスコアが最初の欄に示されている。続く二つの欄(すなわち、レベル1とレベル2)では、AMSスコアはそれぞれ10%ずつ減らされ、最後の欄(すなわち、レベル3)では、AMSスコアはさらに50%減っており、永久割り当て(レベル1)、その場の変化性(レベル2)、動的変化性(レベル3)により、DDIDにより可能となる曖昧さが増加するにつれ、AMSスコアは減少している。

【０２６２】

[313]上記で述べたように、図1Jには、本発明の実施形態の一つに合わせ、例として計算された匿名性測定スコアが示されている。これらのAMSは図示の目的のみであり、あるタイプの個人的に特定され得る情報は、他のタイプの情報より、Data Subjectの真のアイデンティティをより公開しやすく、また、関連切り離しや置き換えの追加のレベル、例えば、その場の変化性(レベル2)や動的変化性(レベル3)により、匿名化のシステムや体系によりData Subjectが持つ匿名性を高めることができる、という事実を示す。

【０２６３】

[314]上記で述べられたように、図1Kには、本発明の一つの実施形態と合わせ、計算された匿名性測定スコアに対し、Data Subjectにより要求される同意や係わりのレベルについてのカテゴリーの例が図示されている。カテゴリー分類は、図示の目的のみであり、ある集約されたスコアは、異なるカテゴリーの処理に当てはまる、という事実を示す。例えば、カテゴリーAデータは、現時点での明確、明瞭なData Subjectの同意がある場合のみ使用可能であり、カテゴリーBデータは、現時点または以前の明確なData Subjectの同意がある場合に使用可能であり、カテゴリーCデータは、Data Subjectの同意なしに使用可能である。特定の実装の必要に見合うために、他の体系を用いてもよい。

【０２６４】

[315]図1Lには、DDIDsを緊急連絡の目的で使用する、本発明の実施形態の一例が示されている。図1Lのステップ(1)では、例えば、家が洪水域にあるか、人が動けない状態にあるか、または特定の救命装置や医療処置が必要か、など該当する緊急連絡の特徴を決めるために、データ属性が、評価される。ステップ(2)では、該当するデータ要素は、市民のプライバシーと匿名性を保護するために、DDIDsを用いた、関連切り離し・置き換えにより、信頼できる者によって動的に匿名化され、曖昧にされた情報は、DDIDが曖昧になった緊急連絡データベースに送られる。ステップ(3)では、データ要素が特定の緊急事態に対応すべきかどうか決定するために、信頼できる者によって、情報が評価される。最後に、ステップ(4)では、欲しい情報、または緊急事態とその対応の間だけDDIDsにより表される情報を明らかにするために、信頼できる者が、曖昧にされた緊急連絡データベースの関連キー(AKs)や置き換えキー(RKs)を提供する。

【０２６５】

[316]図1Lに反映されている実施形態の例では、必要となる関連キー(AKs)や置き換えキー(RKs)は、適切なトリガーとなる事態が発生すると付与されるため、そのときまで情報の特定が認識されない、または再特定されないようにするため、データは、動的DDIDが曖昧にされた状態で、緊急連絡データベースに常駐している。信頼できる者により行われるトリガーとなる動作により、事態のタイプにより、曖昧さまたは透明さの特定のレベルで適切なデータの一部に対し、時間限定のAKs・RKsが発行される。特定されうる情報は、緊急連絡データベースの中に維持管理されるが、動的DDIDは曖昧な状態である。信頼できるの者により管理されるデータマッピングエンジンは、該当する緊急事態の場合に提供される、データを識別または再特定するために必要な、動的に変化するDDIDsおよびAKsやRKsについての相関情報を維持管理する。

【０２６６】

[317]システムの外にあるポリシーは、全ての情報が一度に流出しないように、また、関係ないが慎重さを要する情報が原因もなく流出しないように、どの時間に、どのレベルの曖昧さまたは透明さが適切か、だけでなく、どの情報が、どの事態について適切か、事態

のどのステージで適切か、を判断する。これらの許可は、緊急時にトリガーとしてアクセスしやすいよう、コード化される。この方法により、静的なリストや一方向のみの通信に比べ、双方向の通信と、場所や影響を受けた個人の検証が可能になる。

【０２６７】

[318]AKsやRKsは、DDIDが曖昧にされた状態で、継続して電子的に情報が維持管理されるように、各緊急事態ごとに変更され、緊急連絡データベースに再導入される。すなわち、前の事態に対応して発行されたAKsやRKsの後に、新しいAKsやRKsでデータの一部分が読めるようにするには、新しいトリガーが必要となる。(すなわち、緊急事態の解決の後、以前発行されたAKsやRKsは、動的に変化するDDIDsに関連した、既にある特定の情報を明らかにすることはできない。)これにより、市民個人のプライバシーと匿名性が保護され、一方で、限定された時間だけ適切なデータへのアクセスを許可することにより、大規模な緊急事態における市民の安全も守ることができる。緊急事態管理側としては、これにより、大規模な緊急事態において、大量の情報の取り込みと、対処の手順採用の必要性を減らすことができる。

【０２６８】

[319]さらに、緊急事態の間に、避難中の「行方判明」や「行方不明」のステータス指定のように、個人についての新しいデータを加えることもできる。本発明の実施形態により、この新しい入力は、静止状態で保たれる個人のプロフィールの一部となり、同様の、または続いて起こる緊急事態に役立つのであれば、将来の承認された使用のために維持管理される。

【０２６９】

[320]地域のオプトインの例では、市民が、緊急時に必要となり得る情報をDDIDが曖昧にされた状態での緊急データベースに保存することもできる。緊急データベースは、地域のみまたはどこに保存されてもいいが、複数の管轄での事態に備え、相互に操作できる状態でなければならない。一度市民のデータがDDIDが曖昧にされた状態のシステムに入力されると、保存されているデータの適切な成分を識別・再特定する必要に応じて、信頼できる者により管理されるトリガーにより、動的で状況に応じた、AKsやRKsが発行されるまで、誰もそのデータを、認識できる、再特定できる状態で見たりアクセスしたりすることはできない。

【０２７０】

[321]緊急事態管理から見た、本発明の実施形態の二つの例は以下を含む。

1.インタラクティブスクリーンにより、オーバーレイが表示され、地理的情報システム(GIS)とほかのデータが、場所に限定されるデータに相関付けられる。すなわち、家をクリックすると、関連する災害のリスクと共に、管轄する期間がその所有地について保有する情報に加え、市民から提供された情報が表示される。例えば、洪水警報は、市民の特定の場所に応じ、異なる市民に異なる量の情報を与える通知のいい例である。一般的な洪水注意報は、その地域一帯に出されるが、特定の警報は、洪水のリスクがより高い洪水域に直接出されるべきである。

2.例えば、電子テーブルのようなより古い形態では、非地理的データを提供するよう増補されてもよい。

【０２７１】

[322]上記二つの形態では、相互に、またはリンクされてどちらにも表示されるデータ同様、相互動作可能である。

【０２７２】

[323]予報や注意報の場合、気象現象の局地性(気象レーダーやGISマッピングなどにより判断される)により、データベース内でさらに公開されてもよい、提供されるべき情報のサブセットが決められる。

【０２７３】

[324]他の例では、ターゲットとして特定の分布を調査している犯罪者がいるとする。この状況では、発信されたメッセージに対し一般的な外周をつくるために、特に曖昧にされ

た場所データに加え、連絡先と統計情報のようなDDIDsには、関連性がある。関連性のあるデータフィールドとそれらのDDIDsが有効になると、統計と一致する個人が特定され、犯罪活動の通知に載せられる。

【０２７４】

[325] 避難を要する緊急事態では、避難の補助や、緊急事態においてさらに援助が必要な市民を特定する事に加え、より効果的な人材配置において救急隊員をサポートするために、この情報がトリガーされる。ブリザードのような他の例では、救急隊員に、患者の携帯機器に関連するGPS情報により、除雪車による緊急搬送の必要のある腎臓透析患者が、正確に市内のどこにいるか知らせるために、このシステムがトリガーされる。そのGPS情報は、トリガーにより、適切な相関情報を反映するAKsやRKsが発行されるまで、認識されない、再特定されないDDIDsにより表示される。

【０２７５】

[326]Just-In-Time-Identity (JITI)により可能となる文脈化されたセキュリティとプライバシー

【０２７６】

[327]ここで、これから述べる動的匿名化の方法とシステムの参照のため、「実行時アイデンティティ」や「JITI」の用語が使用される。ここで、「JITIキー」や「キー」の用語は、「関連キー」、「置き換えキー」、「時間キー」、「AKs」、「RKs」、「TKs」、「キー」を指すために使われる。

【０２７７】

[328]このセクションで開示される、一般的な目的の粒度、文脈、プログラムされたデータの保護のための方法とシステムは、誰がデータにアクセスできるか(Anonos Just-In-Time-Identity (JITI)キーなしではデータは理解できないため)から的を外し、誰がJITIキーへアクセスできるか、そして、それぞれのJITIキーにより可能となる使用の範囲に注意を向ける。

【０２７８】

[329]文脈的に柔軟に、選択可能に、下位のデータ要素に至るまで、またはそれぞれのデータ要素のレベルに至るまで、技術的に、またプログラムにより、データのプライバシーとセキュリティのポリシーを強制することで、JITIは、承認されていないデータの使用を最小限に抑えつつ、承認されたデータの使用を最大化する。JITIにより、数学的、統計的、数理的測定とデータ使用のモニタリングを可能にすることで、確立されたプライバシーポリシーへの準拠と監査性が促される。JITIにより、同一のデータストアが、同時にプログラムにより、複数の会社、州、地域、国、産業、等に適用されるプライバシーポリシーをサポートすることが可能となり、理解不能な形態のデータをDDIDsから変換されたデータへと、動的に変化させることにより、リアルタイムで、そのポリシーの変化する要件に適応することができる。

【０２７９】

[330]ここで詳細に述べるように、JITIにより、最小のデータ要素のレベルまで下げられた(例えば、個々のデータレベルまで下げられた)データは、そのデータをDynamic De-Identifiers (DDIDs)と置き換えることにより、動的に曖昧化される。例えば、個人の実名を保存する代わりに、その人の名前がDDIDにより置き換えられる。重要なのは、JITIは、プレゼンテーション層でデータをマスキングするのではなく、データ要素をデータ層で置き換える。データ要素をDDIDsで置き換えることにより、要素レベルまで下げられたデータを、データ層で動的に隠すことにり、またデータ要素間の関係を切ることにより、DDIDsを理解でき形態に「変換」するのに必要なJITIキーへのアクセスがなければ、データは、トラッキング、プロファイリング、推測、推定、分析されにくくなり、また直接的、間接的に理解・相関されにくくなる。この適用の目的では、「変換」は、修正、短縮、圧縮、コード化、置き換え、解釈、演算、翻訳、暗号化、暗号解読、代入、交換、または、機械的、物理的、電子的、量子的、その他の手段によるDDIDsへの数学的関数・認識演算の実行を意味するが、これらに限定されない。

【０２８０】
[331]図1Hに戻ると、図1Hの左側の球は、メタデータ(すなわち他のデータについての情報を提供するデータ)が公開する、データ要素を表す上の三つの球の間の相互関係と、データ要素を表す下の四つの球の間の相互関係についてのデータ要素を表す。これによって、図1Hの左側の球の間の点線で表された、トラッキング、プロファイリング、推測、推定、分析、理解や相関が可能となる。図1Hの右側において、それぞれの球上の異なるデザインは、球で表されたデータ要素を置き換える際に使用される固有の動的匿名子(DDID)を表す。異なるDDIDsを使用する結果、データ要素を表す球間の相互関係を表す、図1Hの右側のいずれの球にも、メタデータは存在せず、関連もしていない。DDIDsを理解できる形態にするために必要なJITIキーへのアクセスがなければ、データ要素のDDIDsとの置き換えはできず、トラッキング、プロファイリング、推測、推定、分析、理解やデータ要素を表す球の間の相関の確立をしようとする試みに対し、顕著に困難さを増す。
【０２８１】
[332]前部での粒度、文脈、プログラムされた強制により、後部のデータ保護(例えば、セキュリティ、プライバシー、匿名性)への準拠を監査するのは容易であり、同一のデータを保護しつつ、広範囲の国内、海外からのデータ解析の受け入れやデータの価値を最大限にする使用に必要な責任や信頼が増す。データの源や使用により、同一のデータは、異なる管轄の要件にさらされることもある。例えば、心拍数の読み取り(例えば、一分間に55拍)を表すデータは、そのデータがどのようにキャプチャされたかにより、異なるプライバシーポリシーの対象となる。
【０２８２】
[333]例えば、データが、アメリカで個人用健康機器を使用してキャプチャされたのであれば、データの使用は、情報をキャプチャするのに使用された機器とアプリの利用規約の対象となる。データが、アメリカで医療サービスと関連してキャプチャされたのであれば、データの使用は、連邦の医療保険の携行性と責任に関する法律(HIPAA)と該当する州の法律の対象となる。データが、アメリカで連邦政府より資金を受けた研究と関連してキャプチャされたのであれば、データの使用は、以下に成文化されているように、「共通ルール」の対象となる。農務省による連邦規則集(CFR)第7巻パート1c; エネルギー省によるCFR第10巻パート745; 航空宇宙局によるCFR第14巻パート1230; 商務省国立標準技術研究所によるCFR第15巻パート27; 消費者製品安全委員会によるCFR第16巻パート1028; 国際開発庁(USAID)によるCFR第22巻パート225; 住宅・都市開発省によるCFR第24巻パート60; 司法省国立司法研究所によるCFR第28巻パート46; 国防省によるCFR第32巻パート219; 教育省によるCFR第34巻パート97; 退役軍人省、研究監督局、研究開発監督局によるCFR第38巻パート16;環境保護庁研究開発によるCFR第40巻パート26; 保健福祉省による(中央情報局、国土安全保障省、社会保障庁にも適用)CFR第45巻パート46; 全米科学財団によるCFR第45巻パート690; そして運輸省によるCFR第49巻パート11。その結果、JITIのような、完全に異なる、企業、産業、政府、規制者、その他利害関係者グループのプライバシーポリシーの管轄に合わせる等のため、拡張可能でプログラムによる、一般目的のデータ保護および法規制適合解決策が必要である。
【０２８３】
[334]ここに公開される好ましい実施形態の一つにおいて、プライバシーポリシーの粒度、文脈、プログラムされた強制のための方法やシステムの実装には、プライバシーポリシー侵害となるデータへの意図しないアクセスや使用を是正する、リアルタイムの匿名化と匿名化の手法やサービスが含まれ、データ保護への他の取り組みの限度を超えることができる。一方で、データ保護の他の取り組み(例えばデータのセキュリティ、プライバシー、匿名性の向上)は、一般的に二進法である。データ保護がデータ値を犠牲に促進されるか、またはデータ値がデータ保護犠牲に促進されるかのどちらかである。例えば、データのセキュリティ向上のために暗号化する取り組みは、データは保護されるものの、保護された形態では使用できず、逆に、いざ使用しようとして暗号解読されると、データは脆弱になる。

【０２８４】
[335]図1Mでは、データ保護(セキュリティとプライバシー)への他の取り組みのデータ値の保護への影響と、本発明、すなわち、JITIやここに含まれる他の発明が含まれた場合のデータ値の保護(拡張)への影響が比較されている。 図1Mの欄1には、二進法の代替法(例えば、暗号化)の効果が示されている。ここで、データが保護された形態の時、つまり使用不可の時、上の黒い球は、元のデータの値(保護されていない形態)を示し、点状の球は、データの損失を示す。図1Mの欄2には、本来の目的(「データ最小化」)以外の目的でデータを使用することへの懸念のために、データをエコシステムから削除することによる、また、匿名性を得るために、データを曖昧化する、従来の静的方法の使用のため、データの値の減少が示されている。図1Mの欄3には、JITIと共に、100%のデータ値がJITIと共に保持されていることが示されている。最後に、図1Mの欄4には、JITIを用いることによる、正のデータフュージョンの可能性が示されている。
【０２８５】
[336]また、JITIをベースにした技術は、データ保護のための他の既知の技術(例えば、セキュリティとプライバシー)の代わりに使用される必要はないということに留意されたい。実際には、JITIは、他の技術とつなげて使用することもできる。JITIを使用しデータをDDIDsへ変換することの第一の利点は、万が一、または他の手法が失敗した場合、DDIDsを理解できる形態に変換するのに必要なJITIキーへのアクセスがなければ、露出したデータは値も意味も持たなくなるということである。
【０２８６】
[337]図1Nには、JITIについての本発明の実施形態の一つにおける二つの重要なステップが示されている。ステップ1、つまり、図1Nを横切る線の上では、データ要素間の関係を推測・推察することができないよう、データ要素間の目に見えるリンクの削除を示している。データ要素をDDIDsに変換することにより、平文ソースデータは動的に隠蔽される。DDIDsで変換されたデータはまだ存在しているが、情報理論の観点から、データを理解するのに必要な知識や文脈は、JITIキーによりデータから切り離されている。それゆえ、DDIDsは根本的なデータ要素についての情報を含まない。ステップ2、すなわち図1Nを横切る線の下では、JITIキーにより可能であるポリシー管理(例えば、目的、場所、時間、他の指定されたトリガー要因)に基づき、データの選択的な開示を許可するJITIキーの割り当てが含まれる。選択的に公開されるデータにおいて、それぞれのキーホルダーに提供される詳細・明確さのレベル、例えば、元の平文、摂動値、要約情報など、もまた動的に管理される。とりわけ、連続的に、または平行してなされる、異なる選択的公開の数に制限はない。一つ以上の公開がなされる異なる承認されたユーザーの数に制限はない。そして、公開を管理する制約やポリシー(時間、目的、場所、その他(関連性、関係、量)、等)の数にも制限はない。
【０２８７】
[338]JITIを用いた、データ保護(例えば、データセキュリティ、プライバシー、匿名性)ポリシーの粒度、文脈、プログラムによる強制により、データ漏洩やデータ再特定が起こる確率、またはそのような事態のランク付け(つまり、非母数法)の統計的評価がサポートされる。データの値に依然アクセスすることができるが、特定される情報にはアクセスできないため、JITIは、情報理論の観点からすると、データ保護の他の手法よりもより効率的である。言い換えると、特定される情報には漏洩はなく、つまり漏洩した情報はゼロであり、一方、積極的なやり方で(それ自身、標準情報理論的最適化の対象となり得る)、データの値は安全に意図的に「漏洩される」。このことは、値が承認されたユーザーに利用可能になったということである。
【０２８８】
[339]粒度、文脈、プログラムされたJITIの構造は、データ漏洩や再特定の確率が顕著に低くなる、数学的な証明を支えている。JITIの有効性の数学的証明の例は、データ要素のレベルまでDDIDsと置き換えられた(ここで、このプロセスをデータの「Anonosizing」と呼ぶ)データは、高度に暗号化されたデータのアイデンティティを推測することより、再

特定するほうが確率は低くなる、と結論付けるデータ科学者による解析である。しかし、暗号化されたが「Anonosize」されていない他のデータと違い、Anonosizeされたデータは、データから値を生成するのに、その保護された形態で使用できる。さらに、(a) 異なる時間、異なる場所、異なる目的、他の基準に合わせて、異なるDDIDsを同じデータ要素に割り当てることができるため、JITIキーを持たないものが、保護されたデータを、トラック、プロファイル、推測、推察、解析、または理解するのが非常に難しくなる。(b) 何らかの理由で失効した場合、異なる時間、異なる場所、異なる目的、他の基準に合わせて、同一のDDIDを、異なるデータ要素に割り当てることができる(ただし、決してその必要があるわけではない)。これにより、これらの再度割り当てられたDDIDsは、何の意味もない関係や相関を持つデータ要素、または、DDIDsが以前割り当てられたいかなるデータ要素を参照するため、侵入者や他の「悪役」が、意味のある連続性や監査の跡を確立するのが非常に難しくなる。DDIDsやJITIキーの割り当て、適用、失効、再利用をトリガーする基準について、図1Bを参照する。

【０２８９】

[340]JITIによる、プライバシーポリシーの粒度、文脈、プログラムされた強制は、データが自身により特定可能ではなくても、データは他のデータと組み合わされた時に、プライバシーまたはセキュリティのリスクを呈す、という意味で定義された、「Mosaic Effect」を重度に低くする。例えば、ハーバード大学のレジデンスにおける政府とテクノロジーの教授である、ラタンヤ・スウィーニーは、たった3つの離散的識別子の知識の開示により、功績が称えられている。(1)郵便番号、(2)性別、(3)生年月日により、アメリカ人口の87%(つまり、2億4800万人のアメリカ市民のうち、2億1600万人)が個人的に再特定される。ただし、このことが正しくなるためには、郵便番号、性別、生年月日が同一の人に適用されるということを知っている必要がある。JITIを用いると、これらのデータ要素の持ち主は、これら三つ全てを同一の静的識別子に関連付けるのではなく、それぞれのデータ要素を異なる(または動的に変化する)DDIDに関連付けることで、隠蔽される。JITIを用いると、郵便番号、性別、生年月日が一人の人に適用されているのか、複数の人に適用されているのかを知るのが非常に難しくなる。よって、「Mosaic Effect」を重度に低くしている。

【０２９０】

[341]ここに開示されている、粒度、文脈、プログラムされたデータ保護の方法とシステムの実装には、保険のリスクを減らす、数学的、統計的、数理的モデルの開発を含む。ここに開示されている、粒度、文脈による、プログラムされたデータ保護により、値段をより良く評価し、リスクから守るアルゴリズムの開発の必要に応じ、適合性の数学的測定を可能にする。個々の消費者レベルでのデータのセキュリティ、プライバシー、匿名性の保護を確実にすることにより、リスク関連データの正確さと値が向上するような、広く人口代表型でより大量のデータを集約することがより可能となる。

【０２９１】

[342]ここに開示されている、粒度、文脈による、プログラムされたデータ保護の方法とシステムの他の実施形態では、複数の関連する者からの同意を得るために、DDIDsを変換する前に、複数のJITIキーの使用を要求することである。DDIDsからデータ値を取り出すのに、複数のJITIキーを要求すること(すなわち、全てのキーの断片または特定の割合のキーの断片が必要となる「mのn」モデル)で、それぞれの利害関係者により保持されているJITIキーが、理解できる形態へとDDIDsを同時変換させるトリガーに使用されることを要求することにより、複数の利害関係者による、または極秘データのアクセス・公開の状況における、様々な利害関係者の興味が尊重されるということが確実になる。

【０２９２】

[343]ここに開示されている、粒度、文脈による、プログラムされたデータ保護の方法とシステムの他の実施形態では、高粒度(JITIキートリガーとデータ要素の比が1：1までの低い割合で、ただし、多数対一、一対多数、多数対多数のJITIキートリガーとデータ要素のマッピングに限定すると解釈されるべきではないが、そのような実施形態も想定されて

いる)の、特に限定されないアクセスルールとDDIDsが承認され変換される、度合い、文脈、特定性、抽象、言語、正確さの複数のパラメータのうちのどれか、いくつか、または全てをカプセル化する。 この実施形態では、アクセスルールは、全ての明確なアクセスルールは守られ強制されている時のみ、DDIDsが解かれ、元の内容が明らかになるということをプログラムで強制的に確実にする一つ以上のJITIキーにコード化される。 JITIは、複数のポリシーが適用される場合、最も厳しいポリシーだけが強制されるように、「オーバーライド」を可能にすることにより割り当てられたJITIキーに実装された、複数またはカスケードのポリシーのサポートを提供する。または、代わりに、最も厳しいポリシーの集合体が、静的または動的に、または一括、ニアタイム、リアルタイムのシナリオで、組み合わされて新しい「最大限に」厳しいポリシーが作成される。

【０２９３】

[344]図1P-1には、金銭取引でキャプチャされ、仮想の消費者「スコット」(静的匿名識別子7abc1a23により、四つの異なる購入取引に示されている)により入り込んだメタデータが、どのように彼を再識別するのに使われるか、を示している。 JITIを用い、図1P-1で「スコット」と示されている、静的匿名識別子7abc1a23の発生それぞれが、最初に7abc1a23が割り当てられた後に、DDIDに置き換えられる。

【０２９４】

[345]一方、図1P-2では、DDID 7abc1a23はたった一回現れ、7abc1a23が以前現れた他の三回の取引記録では、DDIDsは代わりに、54&#3216、 DeTym321、HHyargLMと現れている。JITIを用いてスコットを指定するDDIDsを変えることで、それぞれの取引に対し、スコットを匿名化する。つまり、それぞれの取引に対し、JITIを付与している。その結果、これらの動的匿名の識別子を相関させても、スコットは再特定されない。

【０２９５】

[346]異なるJITIキーは、同じDDIDの異なる観点または潜在する値を「解く」ことができる。これにより、ユーザーの承認されたデータの使用(例えば、承認された目的、場所、時間、他の属性の使用)の文脈に応じて、各ユーザーから見える、詳細または曖昧のレベルに粒度管理が施される。この適用の目的に対し、「解く」とは、デコード、翻訳、公開、永久または過渡的に可視化する、または、より大きなセットのデータのサブセットから成る、独自の「スライス」を提供することを意味する。ここで、そのようなスライスは、データ要素を含まない、単一データ要素を含む、またはいかなる数のデータ要素の組み合わせを含んでもよい。JITIキーによりDDIDsを理解できる形態に変換することは、単独で、または他のトリガー要因との組み合わせで使用される、所定のJITIキートリガー要因(例えば、目的、場所、時間、または他の指定されたトリガーの要因)の存在により、曖昧化されたものも含め、DDIDsが、異なるユーザー、異なる時間、異なる場所、他の属性の使用、JITIキートリガー要因を満たす全て、に合わせ、異なる方法で変換されるように、トリガーされる。 上記で述べられたように、図1Bでは、データ要素(例えば、データ属性やデータ属性の組み合わせ)やJITIキーについてのDDIDsの割り当て、適用、失効、再生をトリガーする、様々な例のイベントを示している。

【０２９６】

[347]本発明の実施形態のもう一つの例は、医療サービスに関する。この実施形態の例では、平文値である、一分当たり55心拍数(BPM)が「ABCD」の値を持つDDIDに置き換えられる。説明を簡略化する目的のためだけに、この適用で与えられているDDIDsの例は、しばしば少ない文字数の列で表されているが、実際の実施形態では、DDIDsどの有限な長さであってもよい。この例で使用されているDDID、ABCDは、変更されていない元の値「55BPM」は、キーホルダーが、以下の適用(「適用」とは、JITIキーへのアクセスが以下に示される一つ、いくつか、またはすべての属性に基づくことを意味する)される要件を全て満たすJITIキーによってのみ変換されるようにプログラムされている。

1.)目的ベース： この例では、以下のいずれかについて

a. キーホルダーのアイデンティティの承認(例えば、パスワード、複数の要因の承認、または他の承認プロセスによる)： そして・または

b. JITIキーにより承認されるデータを閲覧する個人のキーホルダーの承認(例えば、キーホルダーの承認されたアイデンティティと患者を世話するよう指定された医療要員のアイデンティティを比べる)、またはJITIキーにより可能となる、ソースデータへのアクセスを可能にする属性の継承(例えば、個人が属する、セット、集合、グループ、クラス、その他の構成)による、前記キーホルダーの非間接の承認
2.)物理的場所ベース： この例では、以下のいずれかについて
a.) 医療の提供、または患者に関連した物理的場所(例えば、患者の部屋から、または患者の部屋と同じ階にある医療ステーションから一定の距離内)： そして・または
b.) 承認された、認証された人に関連した物理的場所(例えば、携帯電話、承認及び認証された看護師に着けるよう意図されたセンサーから一定の距離内)
3.)時間ベース： 許可される時間の検証(例えば、現在の時間と、キーホルダーが患者の世話をするように予定された時間との比較)

【０２９７】

[348]図1Qには、上記で述べられた医療サービス実施形態が示されている。例えば、プロバイダのシフト内に、患者の部屋からまたは関連する医療ステーションから一定の距離内で、承認された医療プロバイダにより使用される第一のJITIキーは、DDIDの元の値である「ABCD」を解くように構成され、プロバイダには、「55BPM」と表示される。プロバイダのシフト内に、ただし、患者の部屋からまたは関連する医療ステーションから一定の距離を超えて、承認された医療プロバイダにより使用される第二のJITIキーは、DDIDの元の値である「ABCD」の摂動(例えば、変更された)バージョンを解くように構成され、プロバイダには、「50から60BPM」と表示される。プロバイダのシフト外に、患者の部屋からまたは関連する医療ステーションから一定の距離を超えて、承認された医療プロバイダにより使用される第三のJITIキーは、DDIDの元の値である「ABCD」についての記述的ステートメントを解くように構成され、プロバイダには、「通常の心拍」の記述が表示されるが、患者の心拍について時間の情報はない。第四のシナリオでは、承認された医療プロバイダが(認証のアクションの成功に続き)、その患者の心拍データについての情報を公開するように承認はされていない、第四のJITIキーを保有し、プロバイダはDDID自身以外の情報を見ることができない。同様に、JITIキーが提示されない、または承認、認証されていない人がJITIキーを使おうとした場合、その人は、DDID自身以外の情報を見ることができない。

【０２９８】

[349]図1Rに、上記JITIの医療サービス実施形態例をサポートする、アーキテクチャの実施形態を示す。この実施形態には、以下で「Anonos JITIポリシーエンジン」と呼ばれているものを使い、DDIDsを取り出すのにユーザーの承認を検証するために、「承認モジュール」が使われている。ただし、様々なJITIキーのシナリオの順番と適用は、どの程度ソース値が公開され、医療プロバイダに返されるか、を指定することになる。「問い合わせインターフェース」を使用しているユーザーは、ポリシーエンジンと関わっており、「Anonosプラットフォーム」にあるデータ(例えば、DDIDs、JITIキー、いつDDIDsが変換されるかを決める役割とポリシー、及びDDIDsの別のレベルの抽象化を与えるDVALs)と「情報プラットフォーム」にあるデータ(例えば、DDIDsと共に、データ要素レベルで置き換えられた元のデータ)にアクセスしていることになる。この実施形態は、実際の利用者が信頼され、正しく承認されても、DDIDを自分自身で所有することは、元のデータ要素を解くのには不十分かもしれない、ということを示している。保存されたデータに対する全てのアクションは、DDIDsと一つ以上の有効なJITIキーの許容のセットの両方と協力して機能しなければならない。他全てのケースでは、「終了セッション」のステップは、「失敗終了」(つまり、アクセスを拒否し、停止、シャットダウン、アプリの終了等、特定のシナリオに適切なもの)となり、システムは値のあるデータを一切返さない。

【０２９９】

[350]以下の記述では、可能性のある全ての事項が含まれているわけでも、最小または最大の範囲の定義を意図したわけでもない。例えば、以下の記述では、従来の表形式データ

ベース構造を用いているが、あくまでも実装の一つの例、一つの実施形態にすぎない。JITIはNoSQLを用いて実装されても、他の手法で実装されてもよく、その手法には、特に制限なしに、発展しつつある技術、例えば、量子データベース、量子関係データベース、グラフデータベース、トリプルストア、S3DB(関係・XMLスキーマの剛性なしでセマンティックウェブでデータを表す方法)を含む。

【０３００】

[351]さらに、そのような手法やデータベースは、JITIの実施、またはここで述べられている本発明、同様の特許状または特許出願の他の側面のサポートするために使用されている、プライバシー・クライアントやプライバシー・サーバーのサポート、実施に使用され、またそれらプライバシー・クライアントやプライバシー・サーバーの作成、実装、展開に集約されてもよい。プライバシー・クライアントやプライバシー・サーバーのどちらかまたは両方が、クライアント側のアプリケーションに集約され、管理され、またそのデータに占領され、実施形態によっては、そのようなアプリケーションは、(i) インターネットに接続されていない、サイロ型コンピュータで動く; (ii) インターネット・オブ・シングス上の機器を含む、直接的、間接的にインターネットに接続された携帯機器; (iii) 自身でどの標準インターネットブラウザ(例えば、クロム、インターネットエクスプローラー、マイクロソフトエッジ、ファイアフォックス、オペラ、サファリ、ネイティブ・アンドロイドブラウザ、等)上でも動くアプリケーションとして、またはそれらのアプリケーションを通して直接動く; そして・または、(iv) 一般的にセマンティックウェブに関連するまたはその一部である、構成要素やサービスを使用する。同様に、以下に記述される、様々な問い合わせや記録作成・修正のイベントは、いかなる方法でも、関係データベース管理システム(RDBMS)タイプのデザインの実施形態を制限するものではない。そのような言語は、なされたアクションのタイプの特徴化を簡略化するためだけに使用される。

【０３０１】

[352]ここに記述される、DDIDsとJITIキーを用いた本発明の実施形態には、最小で、プライバシー・クライアント(及び、最大で、プライバシー・クライアントとプライバシー・サーバーの両方を等しい数で、それぞれ一つ以上、またそのようなクライアントとサーバーの多くの例を含む)がクライアント側(例えば、ブラウザで動いているアプリケーションの一部、ここに記述される、いかなるタイプの仮想的、物理的または論理的演算機器であり、そこでプライバシー・クライアントが動いている、及び、そこで動いている機器やアプリケーションが直接的・間接的にそのようなブラウザと関わる)に常駐することによる実装を含む。DDIDsとJITIキーを用いたそのような実装の一つは、統一的演算環境としてのセマンティックウェブ(リソース・ディスクリプション・フレームワークまたはRDFのような、ワールドワイド・ウェブ・コンソーシアム(W3C)により確立された基準によるウェブの拡張)のハーネス機能である。

【０３０２】

[353]図1Sには、NoSQL IndexedDBのような、ネイティブでW3C基準のデータ管理リソースを用いた、オープンハウスプラットフォーム(OH)をサポートする、JITIにより可能となるシステムのJITIにより可能となる実施形態を示す。ここで、プライバシー・クライアントとプライバシー・サーバーのどちらかまたは両方が、OHプラットフォームに常駐している、または論理的にOHプラットフォームの陰にいる。ここで、図1Sの例Aと対照すると、図1Sの例Bにおいて、全てのデータと、限定はされないが、プライバシー・クライアントとプライバシー・サーバーの機能を含む演算は、データプロバイダまたはドメイン消費者によりなされ、専用の演算インフラが、JITIにより可能となる、または他の動作をサポートするのに必要なくなる。セマンティックウェブを経由し、JITIにより可能となる配置としてOHを実装することにより、OHは、サーバー側のリソース上の制約から自由なデータ値とデータ保護(セキュリティとプライバシーの両方)を同時に最大化する、健康に関連するデジタルアセットを管理し、統合する。好ましくは、リソースの観点から、プライバシー・クライアントもプライバシー・サーバーもリソースを消費しないため、それにより、より良い拡張性を可能にし、実現する。

【０３０３】
[354]従来のDBと異なり、JITIにより可能となるシステムのメインDBに生データが記録されることはない(つまり、DDIDデータだけが記録される)。代わりに、二つのデータベースがある。「メインDB」(DDIDデータと共に)と、セルごとにメインDBを暗号解読するキーを含む、「JITI DB」である。「メインDB」におけるそれぞれの新しい値は、この例では、8文字の長さで、それぞれの文字は、aからz、AからZ、0から9のどれかである、固有のDDID値に割り当てられる。(そのようなシンタックスとストラクチャの制約は任意であり、推測するより再特定の可能性が低いようなランダムの値を挿入しつつ、ソースデータフィールドのタイプの元のシンタックス要件に準拠するよう、DDIDシンタックスの定義を含む、特定の使用や、ポリシー目標に合うように再構成できる。)トータルで、一文字に対し、62の可能な値がある(26のアルファベット小文字＋26のアルファベット大文字＋10の数字)。よって、62×8(約2.1834×10^{14})の可能な値がある(この範囲は、より高いエントロピーを得るために、さらに文字を足すことにより、著しく増加する)。これは、将来、BASE64(または他のコード)に簡単に変えることができる。この選択は、この実施形態例における、美的感覚のためだけである。

【０３０４】
[355]実施形態の一つでは、メインDBにおける、全てのDDIDに内在する値は、新しい、固有の8文字のDDIDに割り当てられる。便宜のため、DDIDそのものからDDIDに内在する値を区別するために、DDIDに内在する値を「DVAL」と呼ぶことにする。単純化のため、固有性を確認した場合、ランダムな8文字のDVALは充分固有である。将来の使用のため、非常に大きいデータセット(数兆の記録)に対しては、ランダム生成は充分ではないかもしれない。もとの生テーブルの順番が知られている場合(例えば、データベースインポートの間)、数列固有のIDは、推論攻撃を立ち上げるのに使用されるため、数列値(aaaaaaaaやaaaaaaab)は、使用されない。

【０３０５】
[356]ある実施形態では、それぞれの生値は、異なる初期化ベクトルのために、同じ平文に対しても、固有の暗号文を生成する、AESを用いて暗号化される。例えば、以下の表4では、例として「元の」値のセットが与えられている。

【表４】

名前	生年月日	場所
ジョン	1940年10月9日	パーガトリー
ポール	1942年6月18日	セント・ジョンズ・ウッド
ジョージ	1943年2月25日	ヘブン
リンゴ	1940年7月7日	ロサンゼルス

【０３０６】
[357]表4に示されている値のDVALは、(ランダム生成により)以下の表5に示されている値になるかもしれない。

【表５】

名前	生年月日	場所
93ziqklq	75goAaoa	ukyg8tbd
8sydz6q4	B5hnpkiE	7y6E21lg
Ct1tsBA0	Fp950mby	fbwui9ja
3mtxke9c	btoml49f	eFinqw1q

【０３０７】

[358]DVALのそれぞれを元の値に再度関連付けるために、DVALのそれぞれは、以下の表6(シークレットキー「デモ目的のみ」を用い、AES暗号化されている)に示されているように、暗号化された暗号文と初期化ベクトル(IV)と共に、DVALの表に書かれている。

【表６】

DDID	暗号文	初期化ベクトル
93ziqklq	acK1Z8Orw7BUwro9wrDCmMOGwqHDgsOawq/Cpw==	fCeCe66AA6EE4A44
8sydz6q4	ETLCmcO3UAgBYcK5wp0wwr5qKMO3w6E=	87DaDeF8eFaad2c1
Ct1tsBA0	wprCrcKbDSHDpCt2JCTCoMOEw4HCrUTDvw==	9bFbB6AcbCd3A5cF
3mtxke9c	wpbDuXR4w6ZKHSkiw6DCqGHDmyxHPA==	bdA0a691b2c6DBCC
75goAaoa	w4TDmMOgDcKYw6rCvhvCmcK7ZMOtXzBuw5k=	2fDDE99Da1A17f9f
B5hnpkiE	HUTCp31tw4Mrw55bS0/DsgTCssOCwq0=	20546c0DDBaf5dec
Fp950mby	wqYIAcOvw6jCmiYQLMOYwrJRPcKgLSk=	CBC0846fFFF78Bf0
btoml49f	VTE5lMO8PBUHw6vCp07DqXHCpFZZ	aDCCF6b94B175385
ukyg8tbd	w6zDu8KCRBfDt8OIwq1FwrltLWQ4PcOk	72e0BeCb691BC710
7y6E21lg	w6PDpMOIwo4AWMO8SU9rCcKFLsOfRMKY	3D2B4DDf512FF7FD
fbwui9ja	EXZeWT3Ctk3DnUHDl8KdRR/Cg8O9LQ==	E3Cf320aC66272Ab
eFinqw1q	wrDCucKZXcO2w5Q9woXCg8Kjw6nDpsKTBMO2wqY=	18673fc70ebEE00b

【０３０８】

[359]別の実施形態では、生値のそれぞれを隠すDDIDを生成するために、一方向のハッシュ関数が用いられる。さらに別の実施形態では、DDIDはDDID、その内在する値、他の関連するデータ(例えば、15分ごとに、世界郵便番号を8文字に分け、ランダムに記録したリスト)のいずれにも関連も相関もない、様々な確率統計プロセスを用いて生成される。

【０３０９】

[360]AESの例に戻ると、シークレットキーはデータを秘密にしておくもののため、初期化ベクトル(IV)は、暗号文と共に渡される。IVの利点の一つは、同じ平文の値が異なる暗号文を持つことができる、ということである。例えば、同じラストネームまたは郵便番号に対し、10の記録があるとすると、それら10の名前または10の郵便番号に対し、平文の値は同一であるが、DVALと暗号文、IVはすべて固有である。

【０３１０】
[361]Anonosizeされたデータベースの問い合わせには、ユーザーはJITIキーによる許可が必要である。これらは、広く、意図された目的、場所、使用時間、他の関連する属性に特定のポリシー管理に適用されるよう意図されたものである。さらに、JITIキーは失効ベースの制約を強制し、その結果、好ましい実施形態の一つにおいて、三つの手段となる。問い合わせ制約、表示制約、時間制約　JITIキーはJITIキーDBに記憶され、粒度アクセス管理を提供する。また、キーは、生データがどのように表示されるかを決める(例えば、DDIDの形態、変換ルールの一つに従い変換されて、または生)。
【０３１１】
[362]データの「Anonosizing」方法
【０３１２】
[363]上記で述べられたように、「匿名化する」または「匿名化」の用語は、データをデータ要素のレベルまで下げ、DDIDsで置き換えることである。より具体的には、ここで用いられる匿名化は、データの特定の使用をサポートする管理された条件下で、例えば、データの対象者または承認された第三者から承認されている指定された文脈内で、データのコード化とデコードを指す。
【０３１３】
[364]匿名化するデータの実装により、データ管理システムが元の値(例えば、経済的、機密情報的、その他)と、手つかずの、ただし例えば、データ対象者や承認された第三者により承認されるために明らかにされた特定される情報のレベルを可能にする、ユーティリティと共にデータを再生成する能力を維持することができる。いくつかの実施形態においては、データは、それぞれ指定されたデータの使用をサポートするのに必要な度合でのみ、公開される。データ管理を匿名化することにより、例えば、個人の集合や群の中でデータ要素を「特定する」そして「関連付ける」ことを通し、データ使用は、特定のデータ対象者や承認された第三者により許可された使用だけに制限される。新規の承認されたデータ使用があれば、全ての元のデータ値とユーティリティは、データ対象者または承認された第三者により承認されている程度に、新規のデータ使用をサポートするために保持される。たたし、不適切な、許可されていない情報を特定するような使用は防ぐことができる。
【０３１４】
[365][366]DDIDs動的に変化させることでデータをAnonosizingすることにより、Mosaic Effectにより、一見非特定のデータから個人が再特定される機能は最小化される。ハーバード大学教授のラタンヤ・スウィーニーの研究は、生年月日と性別と郵便番号が分かれば、アメリカ人の87%まで特定できるという証拠として上記で引用された。しかし、87%の再特定率を達成するために、生年月日と性別、郵便番号を組み合わせるためには、同一人物にたどりつくように、これら三つの情報を知る必要がある。DDIDsを用いて得られたダイナミズムの例として、異なるDDIDを生年月日、性別、郵便番号それぞれに関連付けることにより、ある生年月日、性別、郵便番号が同一人物に関連するのか、または異なる人々の組み合わせなのかは分からない。この知識の欠如により、いわゆる「Mosaic Effect」を通して再特定されることはない。
【０３１５】
[367]従って、匿名化の実施形態は、以下をふくむ。1.) 第一または第二の「準特定する」データ要素を含むデータフィールドを指定し、R-DDIDやA-DDIDで置き換える方法を提供する。ここで、これらのデータ要素はある人物についての情報を公開するが、その人物の真のアイデンティティが明確に公開されることはない。2.) 第一または第二の「準特定する」データ要素をR-DDIDやA-DDIDで置き換えるため、または、例えば、フィールドの長さや文字のタイプ(例えば、英字、数字、英数字、など)や、前記R-DDIDやA-DDIDを変えるダイナミズム要件(例えば、変化をもたらすトリガー、変化の頻度、等)のような、前記R-DDIDやA-DDIDに対するフォーマットの要件を特定するため、非参照ポリシーを確立する方法を提供する。
【０３１６】

[368]データAnonosizingポリシー管理とアクセスコントロール
【０３１７】
[369]いくつかのプライバシーポリシー(例えば、ファジー論理、非決定型、その他同様の手法を実施するもの)は、データの受取人にとって、真の内在するデータのどの閲覧が許可され許可されていないのかについて意図的に曖昧にされているが、ここに述べるのは、あるデータの閲覧が許可されているものと、許可されていないものの間の、はっきりとした「明確なライン」で区別することが強制できるような特定のポリシーである。(例えば、一分間に65という、もとの心拍数の値がA-DDIDsの使用を通して隠蔽されたNADEVsに変換される。) 具体的には、A-DDIDsにより隠蔽されているまたはされていないNADEVsは、以下を含むがこれらに限定されるものではない。(i) 合成データ、すなわち、ある状況に適用される、直接の測定により得られたのではなく、ビジネスのプロセスを実施するために持続的に記憶され使用されたデータ(さらに、以下で定義される); (ii) 派生したデータすなわち、元のデータの論理的拡張や修正に基づくデータ; (iii) 一般化されたデータ、すなわち、クラスや群のような、元のデータから推測や選択的抽出によって得られた、一般化されたバージョンのデータ; (iv) 集約、すなわち一つ以上のアルゴリズムを同一の記録内または複数の記録からの複数のデータ要素に適用して得られたもの。一つの例では、第一のNADEVは一分間に61から70の範囲を含み、第二のNADEVは単純に文字による記述「平常」を含む。(そのそれぞれは、抑制されるか個別に公開される。)さらに、そのような閲覧の作成や使用が承認される人々や団体(とその目的)も個別に指定される。また、そのようなポリシーにより、例えば、場所の名前、GPSの座標、または他の特定方法を介し、どこでそのようなデータの作成や使用が承認されるかを管理する、場所のパラメータに加え、いつ作成や使用が承認されるかを管理する時間のパラメータが設定される。
【０３１８】
[370]一般化されたデータの具体的な形態の一つは、非構造化データに対して起こる。ウィキペディアによると、「非構造化データ (または非構造化情報)とは、事前に定義されたデータモデルを持たない、または事前に定義されたように整理されていない情報を指す。非構造化情報は、典型的には、文が多いが、日付や数字、事実も含まれる。 このことは、不規則性と、データベースのフィールド形式で保存された、または文書内に注釈書きされた(セマンティックにタグ付けされたデータに比べ、従来のプログラムを用いて理解するのを困難にする曖昧さにつながる。」また、非構造化データには、写真、音声、ビデオなどのマルチメディアデータも含まれる。 重要なのは、データが構造化データであっても、非構造化データであっても、その組み合わせであっても、データは匿名化される。
【０３１９】
[371]2016年に、IBMは、「今日、データの80パーセントは画像、ソーシャルメディア、ニュース、メール、ジャーナル、ブログ、イメージ、音声やビデオのようなウェブ上の未開発で、非構造化データからきている。『ダークデータ』とも呼ばれ、非構造化データには、より早くより多くの情報を踏まえた判断に必要な、重要な洞察が含まれている。では、残りの20パーセントは？データ・ウェアハウスにある従来の構造化データであり、こちらも重要である。構造なしにはやっていけない。」と述べている。IBMの会長・社長・CEOのジニー・ロメッティは、「まず、データの現象である。データは目に見えなかったが、今は、特に、80パーセント以上の『非構造化データ』が目に見えるようになっている。本にあるような自然な言語、文学、ソーシャルメディア、ビデオ、音声、イメージ。インターネット・オブ・シングスから次から次へとやってくる。コンピュータは、非構造化データを処理し、記憶し、保存し、動かせるが、古いプログラム可能なコンピュータは、非構造化データが理解できない。ダークデータとは、様々なコンピュータネットワーク操作を通して得られるが、洞察を引き出したり、物事の決定にはどうやっても使えないデータのことである。データを収集する会社の能力は、データを解析できる能力を超えてしまっている。いくつかのケースでは、会社は、データが収集されていることにも気づいていない。IBMは、センサーにより生成されたデータやアナログからデジタルへの変換によるデータの約90パーセントは決して使われることがない。専門的にいうと、ダークデータは

、センサーやテレマティックスにより集められた情報を含む。この用語の最初の使用と定義は、コンサルティング会社のガートナーによりなされた。会社は、多くの理由でダークデータを保持するが、殆どの会社ではそのうちのたった1%しか解析していないと推定される。しばしば、法規制準拠と記録保持のために保存されている。いくつかの会社では、情報を処理するより良い解析手法やビジネス・インテリジェンス技術が得られれば、ダークデータは将来役に立つと信じられている。データ記憶装置は安価で、簡単にデータ保存ができるからだ。しかし、データの記憶と保存は、通常、返還される潜在利益よりも、大きな支出(とリスク)を必然的に伴う。」と言っている。Anonosizationは、そのような「ダークデータ」にも適用できる。

【０３２０】

[372]リサーチ会社IDCとデータ保存のリーダーEMC(現在DELLコンピュータにより所有されている)は、データは2010年当初から50倍に成長し、2020年までに40ゼタバイトにまで膨れ上がるだろうと予測している。コンピュータワールドは、非構造化情報は会社の全てのデータの70%から80%を占めるだろうと述べている。よって、どんな会社でも、確定ではないにしても、データの価値を高めつつデータプライバシーを保護する手段により、他の要件と合わせ、非構造化情報を実用的に役立たせるためには、非構造化情報を処理しなければならないだろう。

【０３２１】

[373]たとえば、限定する訳ではないが、電子医療記録(EMR)を考えてみる。EMRは、赤血球の数、血圧、ICDコードなどの特定のデータだけではなく、主にであってそれだけではないが、文から成る「ノート」のフィールドも含む。そのようなノートのフィールドのAnonosizationは、初期設定として(つまり、自動のオプトインで、オプトアウトにも変更できる)、そのフィールドをR-DDIDへと匿名化変換することになる。しかし、そのノートのフィールドに含まれているものも、データ対象者の重要な医療特徴かもしれない。それらの特徴のうち、ほんの少し、またはたった一つが公開されただけで、データ対象者は再特定されてしまうかもしれない。例えば、「連鎖球菌性咽頭炎」は、よくある状態であり、それにより再特定される可能性は低いが、「膵島細胞癌」や、全世界でも一年にごく数件しかない病気(または、希少疾病用医薬品の使用)の開示は、非常に稀であるため、それ自身、または他のデータと組み合わされると、データ対象者は簡単に再特定されてしまう。

【０３２２】

[374]これに対する解決策として、最初の試みでは、既に述べられたように、それ自身では、ノートのフィールドのいかなる情報も公開しないが、管理された条件下では、例えば、承認JITI keyが使用されると、ノートのフィールド全体を取り出す手段を提供する、R-DDIDと置き換えることにより、単純にノートフィールドが匿名化される。A-DDIDsの使用により、別の手段もある。A-DDIDsにより、群(例えば、膵島細胞癌の患者、連鎖球菌性咽頭炎の患者、分裂病の患者、過敏性腸症候群の患者、ここで、過敏性腸症候群は、恐らく、腸管内菌叢の研究をしている者にとっては、精神状態と相関していると信じられている)が特定され(とりわけ、手動で、機械学習のアプリケーションにより、人工知能のアプリケーションにより、量子コンピュータの使用により)、特定されたらそのようなA-DDIDsで表される。このように、A-DDIDは範囲(例えば、最高血圧〉140と〈160)に関連しているかもしれないが、A-DDIDは、EMRの中のノートフィールド内にある特定の状態に関連しているかもしれない。しかし、このA-DDIDの生成は、初期設定ではオプトアウトかもしれず、実際に生成されるためにはオーバーライドが必要であろう。さらに、ノートフィールドの、ベイジアン、マルコフ、発見的解析を含むがこれらに限定されない、どんな分析からも派生する値は、群の存在を定義するために使用することもできる。そして、その群のメンバーシップが、その群に属する全ての記録に割り当てられたA-DDIDにより有効になる。これらのアプリケーションを超えて、例えば、MRI、CT、放射断層撮影法の出力、超音波スキャンなど、スナップショット(X線の場合)として、またはビデオ(放射断層撮影法や超音波スキャンの場合)として表されているような、非構造化データのマルチメ

ディアの形態を考える。そのようなマルチメディアデータから抽出される情報は、実質的には制限はなく、非制限のまたはほぼ非制限の群の数に整理できる。それゆえ、群と、それに関連するデータ値は、Data Subjectのアイデンティティから独立して使用されるため、A-DDIDsは、Data Subjectに再特定されないやり方で、抽出されうる情報から、現在の情報に至るまで、そこから得られるどの群を匿名化するのにも使われる。全てのここまでのケースでは、A-DDIDs自身が他のA-DDIDsと関連しているかもしれず、しかしR-DDIDsとは関連しておらず、または関連している場合、どのA-DDIDsに対してR-DDIDのアクセスが必要なのか、つまり承認されていないのか、関連するA-DDIDsを再特定するために、抽出された情報を使用する必要がある者は、例えば、JITIキーを用いて承認される。R-DDIDsはData Subjectだけを参照するため、研究者は、A-DDIDsを再特定することによって得られる、医療情報だけが必要である。ここで、A-DDIDsは構造化データだけではなく、非構造化データ(または、非構造化データから推測・推察されたデータの構造化表現)も匿名化する。その結果、データ対象者のプライバシーは高まり、または最大化され、研究者へのデータ値も同様に増加または最大化される。

【０３２３】

[375]いくつかの実施例によると、NADEVまたはNADEVsのセットを生成するために、関連するデータセットに対し、一つ以上の変換が行われた後、プライバシー向上技術(PETs)、例えば、公共キー暗号化、k匿名性、ｌ多様化、「ノイズ」の導入、異なるプライバシー、準同型暗号化、デジタル権管理、アイデンティティ管理、抑制、一般化など、の要件に見合う、またはその要件を超えるために、変換の結果得られるデータのセットの各メンバー(または、そのメンバーの組み合わせ)は、A-DDIDsの使用により隠蔽される、またはポリシー作成者により望まれる度合まで隠蔽される。同時に、例えば、平均や合同平均、周辺的平均、分散、相関、正確さ、精度など、一つ以上の要因により測定されたデータの値は、(もとの変換されていないデータ、またはさらに変換される入力データ、の値に比べて)最大限にまたは最適なレベルで保たれる。これらの技術は、既存のデータ隠蔽方法に対し、利益をもたらす。なぜなら、少なくとも、既存の方法は一般的に; (i) ポリシーベースのみ(技術的強制がない);または(ii) 技術的に強制された場合、しばしば、顕著にデータの値を減らし、それによって望ましい解析、相関、発見または飛躍が起こることを防ぐ。

【０３２４】

[376]ここに開示される様々な実施形態に記述されているように、データ匿名化ポリシーのアプリケーションは、先に述べたように、単純または複雑なデータセットに対し、プログラムによりこれらのポリシーを強制する方法をもたらしている。そのような強制の本質は、限定はされないが、時間、目的、場所のJITIキーや値(または、他のタイプのアクセス管理ベースのキーや値)の組み合わせの使用により、データに対するさらなる制限や排除を生成することから成る。

【０３２５】

[377]そのようなデータ匿名化ポリシーの使用の部分的なユーティリティは、データを「原子的に」または「セル的に」、つまり、実装によりそれがどんなレベルであっても、データの単一ユニットのレベルまで下がって、データを変換する、ポリシーの能力から派生する。データの原子的ユニットは、解析や関連付け、演算、匿名化などの目的のために単一の存在として扱われる、一つのデータまたはデータのグループである。図1Uを参照し、以下で議論されるように、例えば、以前のデータ保護方法では、二次元のデータセットにおいて、「行ごとに」データを保護または暗号化、または「列ごとに」一般化することができたが、ここに述べられている技術では、行ごと、列ごと、3次、4次、またはn次ベクトルにより、またはこれらの組み合わせにより、データを保護または暗号化する。さらに、ここに述べられている技術は、逆の方向にも適用することができる。すなわち、多変数のデータセットの単一セルのレベルまで下がる、または連続的、非連続的、離散型セルの集合や順列まで下がる場合にも適用できる。これらの「セル操作」の機能、つまり、抑制、一般化、公共キー暗号化、k匿名性、ｌ多様化、「ノイズ」の導入、異なるプライバシー、準同型暗号化、デジタル権管理、アイデンティティ管理、その他のPETsは、データそれ

ぞれ、または新しいデータのグループをトークン化する、匿名化システムの能力により可能となる。

【０３２６】

[378]セルレベルでの、データのトークン化(つまり匿名化)は、NADEVsや他の値のヒエラルキーと他のデータやデータのグループへの参照のヒエラルキーに内蔵される。生成されたトークンは、アクセス管理や承認の情報と合わせ、関係及び検索データベースに保存され、A-DDIDsの使用により、トークンも隠蔽される。あるポリシーの実装は以下を含む(i) 初期またはセルレベルでのデータの保護;(ii) どの情報が公開されるべきか、いつまたはどのくらい公開されるべきか、誰に公開されるべきか、そして何の目的で公開されるべきかの管理;(iii) データが公開される時の「明確さ」の管理、例えば、ある承認された者は、ある承認された時間と場所でデータの平文値へのアクセスが与えられるが、一方で、データの真の値のNADEV表現だけが、データの特定性のレベルへのアクセスを持つ必要がない他の者に公開される。管理されたデータの公開は、あるランダム、確率、パラメータ、または非パラメータの側面の使用を含むが、いつ(すなわち、何時に)、どこで(つまり、どの物理的または仮想の場所で)、そしてなぜ(何の目的で)公開そのものが起こるのか、をコントロールする能力も含まれる。

【０３２７】

[379]図1Tは、本発明の実施形態の一つに合わせ、データリスク排除ポリシー管理とアクセス管理を実装するシステムの例を示す。まず、表101は、ソースデータ表の元の平文表現を表す。図示されているように、表101は、表のそれぞれのフィールドに、隠蔽されていない値、例えば、記録日、名前、心拍数、住所、市、州、国、生年月日を記憶する。表102はデータ表を表す。ここで、データは、データ要素レベルでトークン(つまり、ハンドルネーム)と置き換えられることにより変換される。例えば、表102の二行目の55の心拍数(bpm)の値がトークン値「RD-4a7e8d33」と置き換えられ、表102の二行目の1944年10月28日の生年月日は、トークン値「RD-4f0b03c0」と置き換えられる。 表103は、元のソースデータ表101の二行目のデータ公開を表している。ここで、表の選択値(例えば、心拍数フィールドと生年月日フィールド)が、データ要素レベルまでさげられており、一方で、残りのデータは匿名化・偽名化されたままである。表104は、一つ以上のポリシーにより、データ表に入れられた、内在するデータの、デジタルに隠蔽された、部分的に隠蔽された、粒化された、フィルタされた、または変換されたバージョンである、NADEVsの例を表す。例えば、表104に示されているように、二つのNADEVsは、元のソースデータ表101の二行目からの55の心拍数の値に対応するように入れられ、三つのNADEVsは、元のソースデータ表101からの生年月日の値1944年10月28日に対応して入れられている。最後に、表105が、隠蔽され、部分的に隠蔽され、粒化され、フィルタされ、そしてNADEVsに変換され、表104に挿入された、内在する値の例を示している。上記で説明したように、特定されるデータの必要なレベルだけが、一つ以上のポリシーに基づき、ある受取人に公開される。例えば、ある承認された受取人は、心拍数として、「55」のあたいを受け取り、他の人は、「51から60」NADEVを受け取り、また別の人は、「低い」NADEVを受け取る。 同様に、ある承認された受取人は、生年月日として、「1944年10月28日」の値を受け取り、他の人は、「1944年10月」NADEVを受け取り、また別の人は、「1901から1950」NADEVを受け取る。ここまででより理解されたかと思うが、NADEVは、関連するポリシーの実施とデザインにより、別々にまたは一緒に、粒度の大きいまた小さいデータの真の内在する値を明らかにするが、それぞれのNADEVは内在するデータに対し、正確である。

【０３２８】

[380]図1Uには、本発明の実施形態に合わせ、様々なデータリスク排除スキームの例が示されている。例えば、従来のデータ保護の手段(例えば、暗号化)は、スキーム106に示されている。スキーム106は、「二進」の保護スキームを表す。言い換えると、そのようなスキームは、単一のデータ要素全て(つまり、白い四角)を表す、またはどのデータ要素も示さない(つまり、黒い四角)。データ保護の新しい方法では、スキーム107に示されてい

るように、データは「二次元」で公開されたり隠蔽されたりする。言い換えると、データの公開は、行ベースまたは列ベースで行われる。最後に、スキーム108は、ここで述べられるように、多次元または「n次元」の保護スキームを示す。ここで、データは、二次元、三次元、またはn次元で、(セルの組み合わせを含む)個々のデータレベルで公開される(または隠蔽される)。

【０３２９】

[381]データAnonosizingポリシーの仮想マーケットプレイス

【０３３０】

[382]図1Vは、本発明の実施形態に合わせ、購入可能になった様々なデータリスク排除ポリシーに対し、スキーム110に示されるマーケットプレイスの例を示す。ここで述べられる、電子マーケットプレイスは、社内または第三者のポリシー業者から、異なるポリシーをいくつでも販売または消費可能にしている。ポリシーは、非パラメータ手段(すなわち、ランク順)、または、特定のポリシーの「ユーザー評価」に加え、量的・質的基準(例えば、表110に示されているように、「正確さ評価」、「プライバシー評価」)に対するあるポリシーのパラメータ手段、分析そして、そのポリシーの性能属性により、ランク付けされる。さらに、ランク付けと分析は、例えば、HIPAA、GLBAまたはFERPA(アメリカ)、またはヨーロッパ連合(EU)の一般データ保護規制(GDPR)など、特定のタイプのプライバシーまたはデータ値チャレンジ(つまり、表110の「対象エリア」)へのポリシーのアプリケーションに基づく。ポリシーが、内在するデータに技術的に強制される、文脈的使用と適用される法律や規制に基づき、ある特定のプライバシーポリシーの質や関連性の客観的測定を与えるマーケットプレイスはない。

【０３３１】

[383]データAnonosizationへの人口知能の適用

【０３３２】

[384]上記で議論されたように、本発明のある実施形態において、個人が作れる、音楽、映画、他のデジタルコンテンツの複製を制限する、会社により用いられるものと類似している、デジタル権管理(DRM)のような技術が用いられ、データ対象者の個人データの使用を承認するために、データを匿名化することにより、データの会社オーナーからデータ対象者またはデータ対象者が信頼する者へと権限を移している。このデータ保護のスキームは、ここで、「プライバシー権管理」(PRM)または「BigPrivacy」と呼ばれる。データ対象者が直接関わらない状況であっても、PRM技術は、データ対象者の権利を尊重する、データの責任ある使用を可能にするため、リスクを管理する。

【０３３３】

[385]PRMやBigPrivacyはDDIDsを伴う、静的で表面上は匿名の識別子を置き換えるために使用されます。前述のように、これらの動的識別子はデータをカプセル化し、データのライフサイクル全体からデータの要素レベルまでの再識別を制御します。したがって、同じデータでも技術的なポリシーによって人によってはその意味が異なります。BigPrivacyのテクノロジーは、機密データや識別データをセグメントに分割し、これらのセグメントを間接参照する場合があります。例： セグメント化されたデータ要素とIDとの間の関係を不明瞭可するDDIDポインター

【０３３４】

[386]PRMやBigPrivacyのテクノロジーは、さまざまなアプリケーションやプラットフォームから収集されたデータに共通のデータスキーマを課すこともできるため、異種のデータセット間の機能的な双方向の運用を可能にし、データ融合、ビッグデータ分析、機械学習、人工知能（AI）をサポートできます。Anonosizeされたデータは、データ主体または許可された第三者（“Trusted Party”）のコントロール下にある特定の条件下での使用のためにデコードされることもあります。

【０３３５】

[387]本書で説明する、いわゆるさまざまな“Intelligent Policy Compliance” システムとその方法には、データセットのデータスキーマ、メタデータ、構造を分析するAIのア

ルゴリズムが含まれます。さらにR－DDIDsやA－DDIDsを用いて、予め設定されたポリシーに基づいてデータセットを不明瞭化、一般化、変換するようなアルゴリズムを決定するためのデータセットのサンプルの記録も含まれるでしょう。

【０３３６】

[388]いくつかの実施形態では、Intelligent Policy Complianceシステムとその方法では、データのメタデータを分析することによってデータを分類することもあります。たとえば、「患者ID」や「処方ID」といったようなフィールド名を含む場合は、医療に関連しているデータセットであると言えます。遠隔データ検索、統計的手法などのアルゴリズムを含む高度な分類手法を使用して、分類の精度を高められます。データセットのサンプルの記録が使える場合、分類の精度がさらに向上する場合があります。いくつかの実施形態では、Intelligent Policy Complianceシステムとその方法は、それぞれの業界（医療分野など）や製品やサービス（携帯電話の通話記録など）に合わせることもあります。ニューラルネットワークのアルゴリズムを使うことで、異分野および業界のモデルを生成し、業界間および業界間のカテゴリ化ができるようになります。たとえば、航空機のジェットエンジンは水力発電タービンとは異なりますが、両方とも液体または気体の流れを誘導する機能を備えています。そのため、フロー測定のルールを提案するための概念モデルを生成することが可能です。

【０３３７】

[389]いくつかの実施形態では、Intelligent Policy Complianceシステムとその方法では、ある分類のデータのためのアクションを分析することがあります。上記の、R－DDIDsやA－DDIDsを用いているものが例です。この分析は、特定の方法でデータセットを変更するために適用されるアクションのセットを生成するために使用できます。上記の、R－DDIDやA－DDIDを用いているものが例です。たとえば、特定のプライバシーポリシーに準拠するために、ある人の電話番号をA－DDIDを用いて市外局番まで一般化することで、個人の名前とR－DDIDとの関連が完全に不明瞭になる場合があります。このような多くのプロセスは、Intelligent Policy Complianceシステムとその方法によって分析され、データセットに適したプロセスの組み合わせが生成されます。The combinations may embody a single “best” combination, multiple combinations selectable by a user, or any other set of combinations.

【０３３８】

[390]ユーザーは、ユーザーインターフェイスを介して、Intelligent Policy Complianceシステムとその方法によって生成されたプロセスを変更したり、そのままデータに適用したりできます。ユーザーがそのような決定をすると、以後のためにフィードバックループの一部として保存され、機械学習を効果的に使用して、Intelligent Policy Complianceシステムとその方法が成功と失敗から学習できるようになります。

【０３３９】

[391]図1W－1は、本発明の一実施形態による、Intelligent Policy Complianceエンジンの例を示しています。図に示すように、ユーザーはユーザーインターフェイスを使用して、Intelligent Policy Complianceエンジンと対話することができます。このエンジンは、分類サービスと分析サービスを実行するソフトウェアで構成されます。上記のように、分類サービスは、機械学習を含むAI関連の技術を使用して、対象のデータセットにどのカテゴリのデータが格納されているかを判断します。同様に、分析サービスは、決定されたカテゴリを分析し、データのタイプに適した複数のプライバシーポリシーを提案する場合があります。Intelligent Policy Complianceシステムは機械学習またはその他の方法を使用して、特定の種類のデータセットに対してどのデータプライバシーおよび匿名化ポリシーが最も効果的であるか（または、どれをユーザーが好むか）を「学習」し、潜在的なデータカテゴリとそれに関連するポリシーを保存し、更新することができます。

【０３４０】

[392]図1W－2は、この発明の実用例で、Intelligent Policy Complianceエンジンの使用に関する例示的なフロー図130を示しています。フロー図130の左側から始まり、ユ

ーザーは、データプライバシーシステムの分類サービスへのユーザーインターフェースを介してデータセット（関連するメタデータを含む）を提供することができる。分類サービスは、一般的に使用されるデータフィールド名とデータの種類、およびユーザーが保存する特定のカテゴリのデータとの関連付けに関する情報を取得します。この保存された履歴情報を活用して、ユーザーによって提供された着信データセットをAIにより分類サービスが分類します。次いで、決定されたデータ分類は、データプライバシーシステムの分析サービスに提供されることがあります。同様に、分析サービスは、以前の同様のデータセットに適用されたデータの匿名化プロセスに関する情報をストレージから取得する場合があります。返された情報の分析に基づいて、分析サービスはさまざまなポリシー決定を行い、さまざまなプロセスをデータセットに割り当てて、データの匿名化を行います。決定されたアクションとポリシーは、ユーザーインターフェースを介してユーザーが確認し、必要に応じて変更してから、匿名化ポリシーをデータセットに適用することができます。ユーザーの変更はデータストアに保存されるため、ポリシーが更新され、最終的なポリシーがユーザーに提示されて、承認を要求します。いつでもこのデータセットは使えるようになります。

【０３４１】

[393]合成データのAnonosizationへの応用とAnonosizationの合成データへの応用

【０３４２】

[394]Wikipediaによると、合成データとは「直接測定したものではない、特定の条件下で適用できるproduction data」のことであり、マグローヒル科学技術用語大辞典ではデータマネジメントの専門家であるCraig S. Mullinsがproduction dataとは「専門家がビジネスのために恒常的に蓄積し、活用する情報」としています。言い換えれば、合成データは様々なモデリングや、統計的解析、ベイズ法、マルコフ解析などを活用して作られたものであっても、実世界のデータを実際に測定したものの象徴ではないということです。むしろ、合成データは実世界のデータのモデルです。実世界のデータは最終的に実際のデータ主体に紐付けられており、そして、秘匿化された実世界のデータは、再特定された場合、それらのデータとデータ主体に関連付けられた準識別子が明らかになってしまうことには注意が必要です。対照的に、合成データは、平文であろうと再識別された形式であろうと、実世界のデータではなくむしろそのモデルを指します。したがって、合成データは実世界のデータの抽象的な統計特性を含む場合がありますが、合成データを生成するアプリケーションが接続されたままであるか、継続的なアクセスを持たない限り、合成データを間接参照して実世界のデータを生成することはできません。この場合、実世界のデータは、そのアプリケーションの許可された（あるいは潜在的には許可されていない）ユーザーがアクセスできる状態だといえます。

【０３４３】

[395]上で述べたような「プライバシーポリシー」 には、合成データの使用が含まれますが、これに限定されません。これは、合成データは実際のデータに存在するデータ主体（個人）に基づくものではなく、実際のデータ主体に直接の関わりがないデータは原則としてデータ主体のプライバシーを保護するためです。ただし、本書の他の場所で説明されているように、これは実際のところ必ずしも真実ではありません。

【０３４４】

[396]ゆえにプライバシーポリシーについては次のことが言えます： （i） プライバシーポリシーは合成データの使用を詳細に説明する。； （ii） プライバシーポリシーは合成データの匿名化を詳細に説明する。なぜなら原則として合成データからリバースエンジニアすることで実世界データのモデルを得ることができ、このモデルは実世界のデータとの高い関連性を示すために利用することができるからです。Mosaic Effectによって、匿名化された合成データは許可されたユーザーにのみ利用可能になります。これによって、この潜在的な欠陥を不正に悪用されることを防げます。； （iii） プライバシーポリシーは一定期間、合成データの生成者が実世界のデータにアクセスする権限をもっているが、その期間終了後に権限はJITIの期限、位置情報、目的によって制限されたキーで無効化

されることを明示する。； （iv） 匿名化された合成データだけでなく合成データを生成するアプリケーションも生成終了後に実世界のデータやそれに関連するデータ主体から切り離されるようにするため、上記の（ii）と（iii）の内容を組み合わせる。これはどのような目的で、どこで生成されたかによります。； （v） 実世界のデータと合成データについて書かれている以上の内容を支持する。

【０３４５】

[397]BigPrivacyは一部、大部分、または合成データのみの使用を指定するプライバシーポリシーを適用する場合があります。

【０３４６】

[398]他の場合では、合成データへのアクセスは、時間、場所、目的によって限定し、許可された当事者のみが利用できるように、一部、大部分、または合成データのみの匿名化を BigPrivacyが適用することがあります。

【０３４７】

[399]また他の場合では、最終的に総データの一部、大部分、またはすべてを含むかどうかにかかわらず、必要な時間、特定の場所、合成データの生成に必要な目的でのみ、実世界のデータおよび関連するデータ主体へのアクセスをBigPrivacyが制限できるようにします。

【０３４８】

[400]また他の場合では、合成データの上記の組み合わせを構成する一部、大部分またはすべてのデータセットをBigPrivacyはサポートすることもあります。

【０３４９】

[401]BigPrivacyの技術は、本書の説明の通り、データの最大限の活用を支援する方法で、規制や契約上の制限へのコンプライアンスを促進するために採用できます。例えば、データのセキュリティとプライバシーを担保しながらデータの使用の幅を広げることができます。

【０３５０】

[402]例えば、BigPrivacyは新たなデータ保護規制に企業が適応するために役立ちます。EU内のデータ主体に対する新しい規制であり、2018年春から非準拠のデータ管理者に対して多額の罰金および罰則が科せられる GDPRのようなケースにも対応できます。 GDPRは、EU市民の個人情報を含む場合は、データを扱う世界中の企業に適用され、現段階でその内容には、世界中での売上の最大4％の罰金、集団訴訟、データ管理者やデータ処理を担う業者の両方に対する責任、データ流出の通知義務が含まれます。

【０３５１】

[403]GDPRに関して、データ分析、人工知能、機械学習の以前の法的根拠は無効となります。GDPRにおいて同意は引き続き本的根拠に基づきますが、同意の定義は厳しくGDPRによって定義されます。「自由に基づき、明瞭で詳細な説明を受けた上で、データ主体が本人のデータが扱われることに同意すること」 が同意の現時点での定義です。データ分析、人工知能、機械学習の分野（例えばビッグデータ解析）ではよくあることですが、データ処理についてあいまいな説明や不明確さが含まれていた場合はGDPRのコンプライアンスを満たした同意ではないとみなされます。GDPRの下での厳密な要件を満たした同意によって、個々のデータ主体ではなくデータ管理者、処理者がリスクを負うようになっています。GDPRが制定される前は、広範な同意を完全に理解していないことに関連するリスクは、個々のデータ主体が負担しました。GDPRにおいては、広範な同意はもはやビッグデータの十分な法的根拠を提供しません。したがって、EUデータ主体の情報を管理するデータ管理者と処理者は、ビッグデータ処理の従来とは異なる法的根拠を満たす必要があります。GDPRの「正当な利益」に対する要求を満たすことで、企業はビッグデータ解析の法的根拠を新たに追加することができます。 これには以下の2つの技術的要件が満たされる必要があります・： 「Pseudonymisation」と「デフォルトでのデータ保護」 です。これらについては以下で詳細に説明します。

【０３５２】

[404]GDPR第4条（5）で「仮名化」 はデータを個人にリンクする手段から、データの情報価値を分離する必要、として定義されています。GDPRでは、データ自体と、データと個人を結びつける方法を、技術的、組織的に分離する必要があるとしています。データを個人と結びつける、個別に保護された手段へのアクセスを必要とせずにデータ要素間の相関が可能であるため、恒常的な識別子やデータマスキングなどの従来のアプローチはこの要件を満たしません。データから個人に結びつけることができることを、「相関効果」、「リンケージ攻撃による再識別」「Mosaic Effect」 といいます。これは、データを持っている人であれば特定の個人に結びつけることができるからです。

【０３５３】

[405]GDPR第25条は、新たに「デフォルトでのデータ保護」の義務を課しデータは基本的に保護されなければならないとし、データを使用するならば当然この段階を踏まなければならないとしています。（これはGDPRより前の、データは利用可能だが、利用するならデータ保護の段階を踏まないといけない、という考えとは対照的です。） また、時間、ユーザーに拘らず必要なデータのみを使用し、許可されていないユーザーの利用を禁止しています。

【０３５４】

[406]BigPrivacyはデータの個人への帰属可能性と、データの情報値を分離することにより仮名化をサポートすることができ、 GDPRのデフォルトでのデータ保護の要件を満たし、また、特定の時間、特定の目的、特定のユーザーに必要なデータのみを公開し、データを再保護します。BigPrivacy は「制限されたデータ要素」 （例 GDPRでの「個人情報」 、HIPAAでの「保護されたヘルスケア情報」 、契約上の保護情報など） を仮名化されたデータと置き換えることで要件を満たします。仮名化されたデータは一見すると元のデータと一致しています。 （この仮名化データでの置き換えは、本書でR－DDIDsと記載してきました。仮名化トークンは再特定に使われ、再特定識別子はデータ要素を置き換えるために使われるからです。）R－DDIDsを用いると、個人の特定や「リンケージ攻撃」に必要ではないトークンを用いてデータセットは細かく仮名化されます。さらに、 代替技術が一般にPETsに適用される傾向があるため、BigPrivacyによってより正確なデータを得られる場合があります。逆に、どのデータがどの目的に使用されるかわからなければ、データの価値が低下します。

【０３５５】

[407]上記のように、BigPrivacyは最初の段階でR－DDIDを用いて同じデータ要素の共通の出現を異なる仮名トークンで置き換えることが含まれる場合があります。2番目のステップには、特にデータを個人にリンクする手段を提供せずに、（つまり、識別要素を提供せずに）データ要素が属する「コホート」、「範囲」、「クラス」を含むようなNADEVsを挿入することを含みます。NADEVの例としては、個人の年齢を年齢範囲のデジタル表現に置き換えることがあります。そのような例では、特定の年齢範囲内の年齢を持つデータ主体には同じデジタル表現（つまりNADEV）が割り当てられ、年齢の「クラス」内にあることを反映します。A－DDIDsは、頻繁には出現しないNADEVsの代替データモデル（関連データ値または派生データ値）を保護データフィールドに挿入するためにも使用できます。NADE値を保護または隠蔽する一般的なA－DDIDsは、同じコホートまたはクラス内のすべての同一データ値（つまりNADEVs）に割り当てられます。これらのNADEVsは、処理を行うために変換する必要がないためです。このようにして、コホートトークン化が行われます。（i）コホートの値、つまりNADEV自体がデータの主要な識別子になります。つまり、NADEVは基本的にA－DDIDとして機能します。なぜなら NADEVの保護または難読化の段階は不要であり、関連性がなく、選択されていないからです。または（ii）追加のデータ保護が必要な場合、NADEVを隠すA－DDIDがデータの主要な識別子になります。現在のスキームでは、個人の身元がデータの主要な識別子として機能するため、このような匿名化は不可能です。

【０３５６】

[408]図1X－1は、BigPrivacy（140）を提供するアプリケーションの一般的なアプロー

チを示しています。特に、着信データは、「shim（シム）」アプリケーション（たとえば、API呼び出しを透過的にインターセプトし、渡された引数を変更する、操作自体を処理する、または操作を他の場所にリダイレクトする小さなライブラリ）を通じて、システムへのアクセスがある度にシステムに送信されます。シムは、元々開発されたものとは異なるソフトウェアプラットフォームでプログラムを実行するためにも使用できます。BigPrivacyの実装は、R－DDIDやA－DDIDと基になるデータ値との相関が数学的に導出されず、むしろランダムに相関するランダム化された探索テーブルを活用する可能性があるため、第三者は基になるデータを正式にキーへのアクセスがない限り再識別できません。

【０３５７】

[409]図1X－2に示されているように、データのシステムへの入出力時の非特定化や再特定化のポリシーを実行することによってブラウザ、デバイス、センサーにネットワークを介して影響を与え合うシステム（350）を使うことで、匿名化を行うこともできます。

【０３５８】

[410]図1Y－1は、BigPrivacyサービスを提供してデータの識別を解除するクラウドベースのプラットフォームとアプリケーションを示しています（160）。ユーザー、自動化プロセス、インターネット接続デバイス、またはその他の存在（ユーザー）は、データのプロパティを指定するメタデータとともに、「生の」データ（識別解除前に存在するデータ）をBigPrivacyクラウドプラットフォームプロセッサに送信できます。 （ステップ1）。データは、個々のデータ要素、レコード、データセット全体、またはそれらの任意の組み合わせとして指定できます。システムは、提供されたメタデータを分析し、別のインターフェイスを介して匿名化ポリシーを検索することにより、そのデータを処理する方法を決定できます（ステップ2）。匿名化ポリシーインターフェイスの下にあるポリシーは、リレーショナルデータベースにあるインテリジェントポリシーコンプライアンスエンジンに、サーバーのファイルシステム上のファイルとして、または他の手段で保存できます（ステップ3）。ユーザー提供のデータに適用するポリシーを決定すると、システムはポリシーごとにそのデータの識別を解除する場合があります。ユーザーがシステムを構成して、識別されていないデータをデータストア、メッセージバス、Map Reduceシステム、またはその他のエンドポイントに保存すると、システムは識別されていないデータをその宛先に送信できます（ステップ4）。識別されていないデータストレージに関する以前のオプションから非排他的に、ユーザーが「生の」データ要素と識別されていない値（R－DDIDs）とNADEVsの間のマッピングを保持するようにシステムを構成する場合A－DDIDs、または関連するA－DDIDsを非識別化することにより識別される場合、システムは将来の使用のためにデータスストレージに永続的なマッピングを確立できます（ステップ5）。ユーザーが識別解除されたデータセットまたはR－DDIDsとNADEVs、A－DDIDs、またはその両方のいずれかのマッピングを将来参照できるように、ユーザーは識別子を取得できます（ステップ6）。

【０３５９】

[411]上図1Y－1のステップ5で説明している恒常的なマッピングは、非特定化された、システムが生成したデータセットのR－DDIDs、NADEVs、A－DDIDsを復元する可能性のある再特定化キー（例 JITIキー）を生成するため手動で、あるいは自動キー生成サービスなどの方法により将来使用される可能性があります。

【０３６０】

[412]図1Y－2は、たとえば図1Y－1を参照して前述したBigPrivacyの識別解除フェーズによって識別解除されたデータを再識別できるようにBigPrivacyを提供するクラウドベースのプラットフォームとアプリケーションを示しています（170）。ユーザー、自動化プロセス、インターネット接続デバイス、またはその他の存在（ユーザー）は、データの要素の再識別を要求することができます。ユーザーは、識別解除フェーズ中にユーザーに返された一意の識別子を参照するか、明示的に再識別するデータを指定するか、または他の手段によって、再識別するデータの情報を提供することになります。また、ユーザーは、識別解除フェーズなどでユーザーに返された一意の識別子を指定するなどして、指定され

た識別解除されたデータとその再識別されたものとの間のマッピングを含むJITIキーのデータを提供します（ステップ1 ）。適切なユーザーのみが再識別されたデータにアクセスできるように、システムはJITIキー管理サービス（ステップ2）を使用してユーザーを認証し、そのリクエストを処理する前にユーザーのリクエストを承認します（ステップ3）。図1Y－1で前述したように、システムは、将来に備えてデータストレージに永続的なマッピングを確立することもできます（ステップ4）。次に、システムはユーザー指定の非識別データとJITIキーにアクセスし、JITIキーに含まれるデータごとに非識別マッピングを反転し、最終的に、要求された再識別データをユーザーまたは構成された許可済みの宛先に返す場合があります（ステップ5）。

【０３６１】

[413]複数のユーザーは、基になるデータ要素に対するアクセス権に基づいて、R－DDIDsおよびA－DDIDsの異なるセットを再識別できます。IDを介して（つまり、ユーザーがJITIキーを持っている場合、ユーザーはその中のすべてのデータを閲覧できます）、認証承認サービス（LDAPなど）へのアクセス要求、位置情報、一時的パラメータなどを介して、あるいはこれらと他の方法の任意の組み合わせを介してアクセス権の検証は行われます。このように、様々な人、サービス、や他のユーザーは、そのデータへのアクセス許可に基づいて、基礎となる生データの様々な「ビュー」を閲覧できます。

【０３６２】

[414]BigPrivacyは、非識別化の段階でNADEVsを生成する場合があります（A－DDIDsによっても不明瞭になっている可能性があります）。これにより、再特定されたデータが分析や他のアプリケーションで使用される前に合成データのデータセットの再識別（「コホートトークン化」）に必要になります。これは、再識別の段階でそのような操作を実行する必要があるシステムに対して、再識別にかかる速度、サーバーの電力使用量、マルチテナンシー能力、などの要因の改善を表します。

【０３６３】

[415]図1Y－3は、抽出（Extract）、変換（Transform）、および読み込み（Loading）（ETL）アプリケーションと統合するBigPrivacyのアプリケーションを示しています（180）。ユーザーはETLアプリケーションを使用して、データを調整、変換などを行ったり、BigPrivacyプラグイン（「アドオン」、つまりソフトウェアで追加または削除できるモジュール式の機能）で識別解除タスクを実行したりできます。（ステップ1）。ETLアプリケーションを使用して、ユーザーは、非識別データやマスター再識別データをローカルコンピューター、企業データセンター、BigPrivacyプラットフォームや他の許可された場所に保存できます（ステップ2 ）。ユーザーのETLアプリケーションとBigPrivacyプラットフォーム間の接続は、トランスポートレイヤーセキュリティ（TLS）、仮想プライベートネットワーク（VPN）、その他の方法などのプロトコルとサービスを使用することにより、業界標準のセキュリティで実現できます。システムは、ユーザーが指定した非識別データや再識別キーデータをインポートし、データを保存します（ステップ3）。将来的には、非識別データの再識別バージョンへのアクセス権を持つ別のユーザーがBigPrivacyとやり取りし、元々ETLアプリケーションで識別解除されたデータ要素の再識別を要求する可能性があります（ステップ4）。

【０３６４】

[416]上記で説明したように、データを匿名化することでデータ流出や訴訟のリスクを回避できます。 例： （i） EUではGDPRの第33，34条； （ii）アメリカでは （a）HIPAA漏えい時の通知規則45 CFR §§ 164．400－414 などの連邦法 （b） 47州の法律の下、コロンビア特別区、グアム、プエルトリコおよびバージン諸島は、個人または政府機関が個人を特定できる情報を含む情報のセキュリティ侵害を個人に通知することを要求する法律； （iii）他にも法令で同様の通知義務が課されています。言い換えると、匿名化されたデータが侵害された場合、データ管理者はデータ主体に違反を通知する必要はありません。データは再識別の観点から保護されたままであるためです。また、キー管理システムの確立された機能を活用して、盗まれたキーを使用してマスターテーブル

にアクセスするのがさらに難しくなる場合があります。“Heartbeat”証明書や複数キーの要求、GPSの要求などは特定のシステムのキーを管理するために使用されることがあります。さらに、そのような制御の組み合わせによってアクセスが提供される情報価値のレベルは、個別に制限される場合があります。

【０３６５】

[417]BigPrivacyのすべてのタイプは、データの変換や非識別／再識別ポリシーエンジン、APIコールや「シム」への参照を必要とせずに、それらのNADEVsを使用した完全なパフォーマンス分析と処理を可能にする匿名化によってNADEVsを補助します。具体的には、A－DDIDsは直接処理することができ、その匿名化された抽象化レベルで目的の結果が達成された場合にのみ、NADEVを取得するために「call」が発行されます。そのような場合、NADEVは、A－DDIDがクエリに関連するコホートまたはクラスを表す少数のユーザー（たとえば、データテーブルから50人のユーザー）に対してのみ取得できます。一方、A－DDIDがクエリに関連するコホートまたはクラスと一致しない大多数のユーザー（データテーブルの残りの500，000ユーザー）は、自身のデータが取得される必要はありません。上記にもかかわらず、BigPrivacyはNADEVがA－DDIDによって秘匿化されることを必要としません。なぜなら、BigPrivacyはその方法と装置を提供するだけであり、NADEVがA－DDIDによって隠されていない場合、NADEVはA－DDIDとして効果的に機能するからです。

【０３６６】

[418]BigPrivacyは、様々なレベルの抽象化もサポートできます。プライマリおよびセカンダリレベルまたはテーブルをサポートするだけでなく、NADEVsを含む、更に高次のレベルまたはテーブルは、プライマリテーブルを参照することによって明らかにされた人物、会社や属性の「真の」値ではない架空の人物、会社や属性にデータを関連付けるR－DDIDsやA－DDIDsを表すことができます。これにより、NADEVs、R－DDIDsやA－DDIDsが関連する「真の」人、会社や属性の識別情報が明らかになることは防げますが、NADEVs、R－DDIDsやA－DDIDsが一般的な（ただし身元不明の）個人、会社や属性に関連する場合はわかってしまいます。さまざまなタイプのデータコントローラーがそれぞれのレベルの識別データを必要とすることがあるため、特定の許可要件を満たすために必要な場合にのみ、高次のレベルの個人情報を明らかにせずに、さまざまなテーブル、レベルやJITIキーへのアクセスを提供できます。

【０３６７】

[419]BigPrivacyを使用すると、データ処理において、データ主体の「忘れられる権利」を実装することができます（GDPR第17条で必要な場合）。たとえば、匿名化ポリシーエンジンと個人情報の関連付けに必要なキーを「削除」することで個人データを、データ自体の削除を必要とせずに消すことができます。むしろ、データとデータ主体のもつ真の個人情報との間のリンクのみを探索テーブルまたはデータベースから削除するだけでよいのです。

【０３６８】

[420]量子コンピューター、量子コンピューティング、量子暗号、量子プライバシーへの匿名化の応用

【０３６９】

[421]以下のように、昔のコンピューター（CC）と量子コンピューター（QC）を区別します。情報は2進数（またはビット、つまり0または1）です。ここで使用されるQCは、表現可能な情報の最小部分が量子ビット（または量子ビット）である量子マシンを指します。量子ビットは、0か1（あるいは両方）になります。量子ビットは通常、原子または光子ですが、原則として、十分に小さい粒子、つまり量子力学的原理が適用される粒子です。この量子力学的特性は重ね合わせと呼ばれます。さらに、QCの量子ビットはもつれがあります。つまり一つの量子ビットに変更があれば他の量子ビットも影響を受けます。（対照的に、CCではビットはそれぞれ独立しており、一つが変更されてもほかが変更されるとは限りません。）

【０３７０】
[422]これらの特徴　（重ね合わせともつれ合い）があるため、QCは大量の演算を並行して行えます（CCは直列での計算を行い、並列計算のためにはバイト数を増やすだけでなく更にプロセッサが必要です）。　例えば、CCでは天文学的数字ほどの時間がかかるような問題解決で、事実上解決不可能なものでも、QCなら数秒で処理できます
【０３７１】
[423]現在の暗号化方式には、とくに公開鍵暗号化と楕円曲線暗号化が含まれますが、その最初の暗号化は、非常に大きな合成数（つまり、p1　＊　p2）の素因数（p1およびp2）を特定することによってのみ解読できます。ビット数の大きい公開鍵暗号は、地球上の最速のコンピュータでも解除することができません　（例えば512，　1024，　2048ビットの暗号化）。一方、QCはほんの数秒で、ありうる計算すべて行い暗号を解除（breAK）します。
【０３７２】
[424]BigPrivacyの外部での識別解除には、いわゆるワンウェイハッシュ関数が含まれることがよくあります。これは、原則として、「逆方向」、つまりハッシュから再識別された元の文字列まで初期値を決定できないためです。繰り返しますが、QCは一方向ハッシュから元の文字列を迅速に決定できますが、CCはブルートフォース攻撃を実行して（基礎となるハッシュアルゴリズムの悪用が分からない場合）ハッシュをデコードする必要があります。　これには、長い年月が終了までにかかります。一般に、本書の他の場所で説明されている他のプライバシー強化技術（PETs）を含む、他の形式の匿名化に関して同じ欠陥が存在します。
【０３７３】
[425]何らかの方法で元の情報をエンコードすることがすべての暗号化方法の基本的な問題です。理論的には、少なくともQCでは、QCで簡単に解読できない方法でも、データ主体とそのすべての準識別子は、ある程度深いレベルで回復可能であり、つまりエンコードされた形式から再識別可能です。BigPrivacyは実装がエンコードを防止することを要求せず、BigPrivacyはエンコードに依存しませんが、R－DDIDsまたはA－DDIDsを生成するかどうかに関係なく、元のデータの関連のない文字列の動的置換に依存します。文字列が基本的にランダムであり、QCの理想に適していても、他の方法が存在するプロパティの場合、任意のタイプのDDIDを再識別する手段はありません。DDIDは任意の文字列であり、元データのエンコーディングではないからです。さらに、同じデータは異なるDDIDsで表されるため、DDIDs間の関係すらありません。別の言い方をすれば、DDIDsは最大限にエントロピーであり、情報理論的な観点から、データ主体または元のデータに関する有用な情報を含みません。このため、QCは、そのコンテンツに関する一切の情報を含まないDDIDsに基づいて元のコンテンツを判別できません。このため、とりわけDDIDsは、量子コンピューティングの世界であっても、個人のプライバシーを保護し、匿名化されたデータの再識別を防止する技術を提供します。
【０３７４】
[426]したがって、BigPrivacyは、プライバシーを最大限に高めるという目標だけでなく、同時にデータの価値を最大限に高めるという目標にも取り組んでいます。対照的に、他のPETsは、データの価値を減らすことを犠牲にしてプライバシーを向上させます。または、逆に、データの価値を増加または最大化した結果としてプライバシーを保護できなくなります。そのため、たとえQCがプライバシーを守れたとしても、引き換えにデータの価値が下がります。これは、並列計算が可能で計算が早くても、データの価値を高めたり、有効にしたりしないためです。代わりに、QCがすべてのコンピューティングの標準になったとしても、BigPrivacyだけが（QCと組み合わせて）データのプライバシーとデータの価値を最大化できます。
【０３７５】
[427]BigPrivacyは、QCで暗号化されたフォームを含めて、暗号化されたフォームにも適用できます。言い換えると、BigPrivacyはコンピューターの基本的な性質から計算的に

独立しています。元のデータ（暗号化の可否に関わらず）とBigPrivacyによる匿名化後のデータとの間のリンクを切断するためです。

【０３７６】

[428]BigPrivacyは、基本的な量子力学的特性を利用することもできます。たとえば、QCはそれ自体が真の乱数を生成するのに向いています。ただし、計算可能な関数への入力として真の乱数を使用すると、元のデータとそのデータのランダム化の間に相関関係が存在するため、匿名化の意味がなくなってしまいます。ただし、BigPrivacyでは、前述のように、真の乱数はDDIDとしてのみ使用されます。乱数は独立しており、基礎となるデータとの相関（または関係）はありません。このようにして、BigPrivacyはQCのプロパティを実際に活用して、ある例では、DDID（R－DDIDまたはA－DDIDのいずれか）と基礎となるデータとの間に相関が全くない（またはほとんどない）ことを確認できます。

【０３７７】

[429]分散システムでの集中BigPrivacyコントロールの実施

【０３７８】

[430]前述のBigPrivacyテクノロジーは、P2Pベースまたは他の非集中ベースでリンクされたネットワークまたはプラットフォーム（許可なしシステムまたは分散型台帳技術を含む）を含む分散ネットワークまたはプラットフォーム（許可を必要としないシステムまたは中央化されていない技術を含む）上や全体で、集中プライバシーおよびセキュリティ制御の制御者による確立、施行、検証、および変更をできるようになります。

【０３７９】

[431]本発明のある場合では、blockchainベースの技術に基づいて構築された分散ネットワークに適用されます。Blockchainは、今日の人気のある暗号通貨プラットフォームの多くの背後にある基盤技術です。Blockchainは、暗号通貨と暗号通貨取引を可能にする用途で最もよく知られていますが、医療データの保存、サプライチェーン管理、金融取引管理と検証、いわゆる「スマートコントラクト」やSNSの有効化と実装など、幅広いアプリケーションがあります。

【０３８０】

[432]「blockchain」という用語には単一の定義はありませんが、一般に次の2つのいずれを意味します。（i）特定の方法またはプロセスを記録するために、デジタル化された分散台帳で、分散型のコンピューターのP2Pネットワーク。 （ii）トランザクション自体を表すために使用される基礎となるデータ構造（つまりブロック）、つまり、データのブロックのチェーンを記述し、各ブロックが前のブロックにリンク（または「チェーン」）されている特定のアルゴリズム／プログラミング方法。本書で使用されるように、blockchainは文脈的にどちらかの意味または両方の意味を持ち得ます。「blockchain」という用語が使用されるときは、その意味を詳細に説明します。Blockchainネットワークに参加している、どのクライアントまたはノードがトランザクションを始めたかに関わらず、データの「ブロック」の形でネットワークに記録され、タイムスタンプが付けられ、blockchainの前のブロックにリンクされます。各ブロックを前のブロックにリンクすると、トランザクションのチェーンの整合性が確認されます。すなわち、blockchainの最初のブロックまでさかのぼります。各ブロックを前のブロックにリンクできないことは、改ざん（blockchain内のブロックに保存されているデータのあらゆる種類の変更）、詐欺などを示す可能性のあり、その整合性の確認が取れないことを意味します。ブロック内の情報は暗号化され、暗号化方法によって保護されます。

【０３８１】

[433]Blockchainは、分散ネットワーク全体に保存されます。つまり、ブロックに保存されたデータの中央化された、「公式のコピー」は存在しません。代わりに、blockchainの同一のコピーが複数存在する可能性があります。ネットワーク内の特定のノードでのblockchainのインスタンス化はすべて同一です（もしノードにblockchainの最新バージョンがない場合、このノードはが暗号通貨ネットワークに「追いついた」または合流するまでのトランザクションの検証に関してネットワークを離れたと見なされます）。このストレ

ージの分散化された性質は、blockchain自体に不可欠な重要な側面です。トランザクションをblockchainに追加するプロセスは、「ノード」をマイニングすることによって実行されます。マイニングは、本質的には、特定の仮想通貨を生成する（暗号通貨の場合）ために使用できるアルゴリズムプロセスです。blockchain内のトランザクションを検証することもできます。

【０３８２】

[434]上記のように、EUのGDPRは、データ「管理者」（つまり、単独または他者と共同で個人データの処理の目的と手段を決定する個人または法人、公的機関、機関またはその他の団体）およびデータの「処理者」（つまり、個人または法人、公的機関、機関、または管理者に代わって個人データを処理するその他の機関）に特定の義務を課しています。GDPRは、データ処理者に罰則を導入することに加えて、個人情報の管理者にさらに厳しい義務を課し、違反に対する潜在的な罰則を大幅に増やします。

【０３８３】

[435]GDPRの第17条は、「消去する権利／忘れられる権利」、つまり、継続的なデータ管理について、正当な理由がない場合に個人データの削除または削除を要求する権利を個々のデータ主体に提供する権利を成文化しています。

【０３８４】

[436]blockchainの重要な特徴は、その整合性（つまり、ネットワークのユーザーがチェーンのブロックに格納されたデータの正確性を信頼できること）であり、その不変性によって保証されます。ブロックが検証されてチェーンに追加されると、通常は削除、編集、または更新されません。実際、blockchainは、任意の1つのブロックに保存されたデータを変更すると、チェーン内のすべての下流にあるブロックが「破損」（無効化）するように設計されています。ほとんどの場合、blockchainデータは暗号化または静的トークン化によって保護されていますが、GDPR（またはそのような権利を提供する他の同様の規制）に従ってデータをblockchainから削除するよう要求して「消去する権利／忘れられる権利」を行使したい場合もあるかもしれません。パブリックblockchainプラットフォームでは、このようなリクエストはチェーン全体の整合性を破壊することなく実現することはできません。

【０３８５】

[437]英国の金融行為監督機構（FCA）は、blockchain技術を開発している企業に、不変性とGDPRの非互換性に注意するよう警告しています。管理者が必要に応じてblockchainを編集できるようにするなど、この問題に対するいくつかの解決策が提案されています。ただし、上記のように、blockchainを編集すると、blockchainの概念が破壊されます。blockchainが可変になり、blockchainの整合性に関する保証人が削除されるためです。

【０３８６】

[438]GDPRは、データの管理人が従来どおりの中央集権的なプレイヤーであると仮定して設計されました。GDPRは、blockchainなどの分散型システムを考慮しませんでした。ここで説明するBigPrivacy技術は、いくつかの理由により、基礎となるblockchainテクノロジーに大幅に機能を追加します。たとえば、BigPrivacyを使用すると、blockchainがデータに対して不変のままであると同時に、GDPRの「消去する権利／忘れられる権利」の基準にデータを準拠させることができます。ここで説明するBigPrivacy手法（たとえば、DDIDの使用）は、分散ストレージシステムの新しい形式にも適用できます（その新規性は、たとえば、GDPR自体が、ユーザーデータを格納する不変の分散型台帳の使用を考慮せず、その要件の実装に影響するということは証明しています）。BigPrivacyはさらに、blockchainを使用して、GDPRの下でのデータ管理者および処理者の他の義務を果たすことを可能にします。これについては、以下でさらに詳しく説明します。

【０３８７】

[439]消去する権利／忘れられる権利図

【０３８８】

[440]図1Z－1では、匿名化プライバシー制御が採用され得るblockchainベースの技術に

基づいて構築された例示的な分散ネットワークのケースが示されている。図1Z－1の上部（185）は、データ主体の名前がblockchainに保存される前に暗号化（たとえば、目的の暗号化アルゴリズムを使用）または静的トークンに置き換えられている状況を示しています。この例では、頭文字「ABCD」は、そのような暗号化またはトークン化プロセスの結果の例示的な表現として使用されます。適切なキーへのアクセスにより、「ABCD」の暗号化／トークン化された値は「John Smith」であったと判断できます。これは不変であり、上記の「消去する権利／忘れられる権利」をユーザーに与えなければならないというGDPRの要件と矛盾します。これは、暗号化された形式で格納されているにもかかわらず「John Smith」がblockchain185自体に含まれているためです。

【０３８９】

[441]図1Z－1（187）の下部は、この例では「DDID652」である動的非識別子（DDID）がblockchainで、つまり「ABCDの暗号化／トークン化された値の代わりに」使用できることを示しています。本書で説明しているように、DDID（「DDID652」）は、データ主体が「消去する権利／忘れられる権利」を行使し、DDIDが「null」エントリを指すようになる場合を除き、データ主体の根底にある名前「John Smith」への「ポインター」として機能します。この方法で、blockchainの不変の性質と参照整合性を維持しながら、データ主体が「消去する権利／忘れられる権利」を行使できるようにする柔軟性を提供できます。また、「John Smith」または「null」または値0だけでなく、必要な他の値を含む他の場所をDDIDが指すこともできるということは重要です。Big Privacy対応の例（187）では、従来のblockchainの例（185）と比較して、「John Smith」の値は実際にはblockchain自体に含まれていません。むしろ、値「John Smith」を含む場所を一時的に指すDDID（「DDID652」）はblockchain内に含まれています。DDID値はblockchain187において不変のままですが、DDIDが指す値はblockchain自体を変更せずに値を変更できます。

【０３９０】

[442]他の例では、BigPrivacyは、両方の当事者によって満たされた「スマートコントラクト」の場合に（つまり多くの独立した規定のうち少なくとも1つは両方の当事者によって合意された場合に）「消去する権利／忘れられる権利」に対応することができます。BigPrivacyがこのレベルのプライバシー／匿名性を提供できる理由は、双方が契約を履行すると、相手方の記録が不要になるためです（つまり、相手方に対する義務がすでに満たされているため）。一例では、スマートコントラクトに関係する人の個人情報を消去する／忘れられるというこの要求は、金融商品の取引または交換の際に生じる可能性がある。

【０３９１】

[443]RedHatのチーフセキュリティアーキテクトであるMike Bursellは、次のように、スマートコントラクトのパフォーマンスに関する機密性、整合性、および可用性が重要な問題であると述べています。『契約（スマートコントラクト）が終了し、blockchainまたは分散台帳に移行すれば、それはほとんど定義上変更不能です。しかし、契約が終了する前はどうでしょうか？この投稿の冒頭で説明したタイプの単純な契約は分割不能です。つまり「不可分で既約」なのです。ほとんどの場合、それらは瞬間的に発生します。

「スマートコントラクト」についても同様です。スマートコントラクトにはプロセッシングが必要なため、時間とともに存在することになります。これは、処理中に、脆弱性があらゆる攻撃を受ける可能性があることを意味します。［2つの関連する要素］標準リスト［は以下を含みます］：

機密性：「スマートコントラクト」の状態は、スヌーピングの対象となる場合があり、非対称の知識や非承認者への漏洩につながる可能性があります。

整合性：これは、多くの「スマートコントラクト」にとって悪夢のようなものです。あるユーザーが基礎となる契約の当事者であるかどうかに関係なく、スマートコントラクトを実行するコードの内部状態を（意図的かどうかに関わらず）変更できる場合、その「スマートコントラクト」の結果は変わります。この場合、契約の関係者は異議を唱えることになるでしょう。さらに、整合性の欠損ではなく、欠損の疑いがあるということが整合性の

根拠になります。ランタイムの統合、ましてや欠損の表示は実行に際して非常に困難である。』

【０３９２】

[444]BigPrivacyの技術によって、例えば、スマートコントラクトの関係者の情報や契約内容を保護する上での、上記のようなスヌーピングの問題はなくなります。言い換えれば、BigPrivacyは、あらゆる手段でスヌーピングが発生する可能性があることを前提としていますが、そのようなスヌーピングによって取得されるデータは、スヌーパーにとって価値がないことは確実です。その理由は、データがDDIDに過ぎず、スヌーパーが必要とする「実際の」価値のあるデータ。整合性に関して、BigPrivacyは、規約自体（スマートコントラクトの関係者のIDを含む）をスヌーパーが利用できないようにすることで、関係者が意図的にまたは意図せずにコードを変更しないことを保証します。コードを変更すると、完全にランダムな結果が生成されます。

【０３９３】

[445]データ保護を前提とした設計

【０３９４】

[446]GDPR第25条では、データ管理者が「処理手段の決定時および処理自体の両方で」適切なセーフガードを実装することを義務付けています。第25条では、これは、「個人データの仮名化」が一つの方法だとしています。

【０３９５】

[447]データ保護を前提とした設計は、できるだけ早く行われる必要があります。そのため、デフォルトでは、データの使用は、データ主体によって承認された特定の使用をサポートするために必要な最小限の範囲と時間に制限されます。今日のスタンダードでは、データは使用可能であり、それを保護するための手間と努力が必要です。GDPRは、この現状の標準を変更する必要があることを義務付けています。仮名化、GDPR第25条で特に言及されている項目、またはその他の手段のいずれであるかにかかわらず、GDPRは、最も早い時点で保護を示し、データ主体によって特に許可された用途に限定されることを必要とします。

【０３９６】

[448]GDPR詳説78項は、次の通りです。：「個人の権利と自由の保護に関して、個人情報の処理にはこの規則の要求が満たされるように適正な対策が技術的、組織的に講じられる必要がある。この規制へのコンプライアンスを実証できるようにするために、データ管理者は内部ポリシーを採用し、特に設計段階からデータ保護とデフォルトのデータ保護の原則を満たす手段を実装する必要がある。そのような対策には、できるだけ早期の仮名化が含まれる。」

【０３９７】

[449]GDPR　4条（5）では、「仮名化」とは、データの情報価値を再識別のリスクから分離することを要求していると定義しています。GDPRの法定／規制のインセンティブおよび仮名化に対する報酬の恩恵を受けるには、この分離が必要です。同じ個人データ要素（データ主体の名前など）の複数の出現を「静的」（または永続的な）トークンに置き換えると、相関関係とリンケージ攻撃を再特定するため、データの情報値を再特定のリスクから分離できません（別名「モザイク効果」）。これは、動的な識別子の代わりに「静的な」（または永続的な）識別子が使用されているために可能です。

【０３９８】

[450]前述のように、データを保護するための「静的な」トークン化アプローチでは、永続的な識別子を使用します。データベース内またはデータベース間で繰り返される特定のトークン化された文字列を検索することにより、悪意のある攻撃者または侵入者は、データ主体の身元を明らかにするのに十分な情報を得ることができます。これは、内部データソースと外部データソースを組み合わせてブレンドする分析およびその他のプロセスのスコープ問題の増加です。対照的に、データ要素が別の仮名化DDIDで保存されるたびに置き換えられた場合、各DDIDは他のDDIDとアルゴリズム関係を持たないため、同じ悪意のあ

る侵入者は、DDIDsが属している、または関連していると判断できなくなります。ましてデータ主体の名前やその他の識別情報を明らかにできないは言うまでもありません。

【０３９９】

[451]ここで図1Z－2を参照すると、ある例による、blockchainベースの技術に基づいて構築された別の例示的な分散ネットワークが示されています。図1Z－2は、データ主体の名前が暗号化される（たとえば、暗号化アルゴリズムを使用する）か、または静的トークンで置き換えられる状況を示しています。これらの目的のために、頭文字「ABCD」は、このような暗号化またはトークン化プロセスの結果の例示的な表現として再び使用されます。「ABCD」の同じ暗号化／トークン化された値は、複数のblockchainで「John Smith」を参照するために使用されます。これは、図1Z－2でブロック ＃1 （190） とブロック ＃2 （192）として示されており、それぞれデータ「ABCD 」のそれぞれのブロックです。前述のように、同じ暗号化／トークン化された値（この例では「ABCD」）の永続的な（または静的な）使用は、「ABCD」＝「John Smith」を示すキーまたはマッピングへのアクセスを必要とせずに、最終的にJohn Smithの再識別につながる可能性があります。John Smithの身元情報を保護できない場合は、上記のGDPRの第25条および詳説78項に基づくデータ管理者の義務違反の可能性が高いです。

【０４００】

[452]ここで図1Z－3を参照すると、ある例で、匿名化プライバシー制御が採用され得る、blockchainベースの技術上に構築されたさらに別の例示的な分散ネットワークが示されます。図1Z－3は、異なるblockchainで異なるDDIDを使用する方法を示しています（この例では、ブロック＃1（195）で「DDID652」が使用され、ブロック＃2（196）で「DDID971」が使用されています） DDIDは、「John Smith」の名前の値への「ポインター」として機能します。この方法で、GDPR 4条（5）における仮名化のための要件と、GDPR 25条の設計段階でのデフォルトのデータ保護を満たすために必要なダイナミズムを提供しながらblockchainの不変の性質と参照整合性を維持できます。

【０４０１】

[453]したがって、BigPrivacyは、検証のために基盤となるblockchainアルゴリズムを変更する必要はありません。むしろ、Anonos BigPrivacyは、現在実装されているblockchainには次のことができないという事実を前提としています。（i）GDPRの主要な要素に準拠すること（GDPRは個々のデータ主体のプライバシーを保護するための技術的要件を課す）また（ii）データが不変のままにすることGDPRによって課せられたこれらの技術的要件（前述の忘却権および設計およびデフォルトによるデータ保護など）および不変性に関するblockchainの要件は、この発明がblockchainの実装に適用されない限り満たすことができません。さらに、BigPrivacyを使用して、そのような「スマートコントラクト」の実行前、実行中、および実行後の「スマートコントラクト」に対する元の取引相手のIDを保護することができます。

【０４０２】

[454]blockchainなどのテクノロジーには、著作権登録の認証、ワイヤレスユーザー、ミュージシャン、アーティスト、写真家、作家など、著作権で保護されたコンテンツのコンテンツ作成者へのデジタル使用と支払いを追跡します。さらにサプライチェーン内を移動する高価値部品を追跡できます。他にもワイヤレスネットワークのスペクトル共有の保護、オンライン投票を可能にします。 「管理された資格」の有効化や医療記録の情報システムの実装、デジタルアートの所有権の特定と検証、ゲーム資産（デジタル資産）の所有権の取得も可能になります。ピアツーピア保険、パラメトリック保険、マイクロ保険など、保険業界向けの新しい販売方法を可能にします。また、シェアリングエコノミーやモノのインターネット（IoT）などの分野での共同作業を可能にします。

【０４０３】

[455]図2は、本発明の例で、プライバシーサーバの抽象化モジュール、例えば図1および図1Aに示す抽象化モジュール52によって行われ得るプロセス動作またはステップの例を示します。一例では、ステップ1で、関係者ZZ（「RP ZZ」として表示）がプライバシー

クライアントを介してリクエストを送信します。または、目的のアクション、アクティビティ、プロセス、または特性に関して、プライバシーサーバーと同じコンピューティングデバイス上で、プライバシーサーバーに常駐します。リクエストの開始は、予測可能、ランダム、自動または手動で開始できるように構成可能です。たとえば、関係者RP ZZは、Webブラウジングのリクエストを送信します。

【０４０４】

[456]ステップ2では、例えば、プライバシーサーバの抽象化モジュールは、所望のアクション、アクティビティ、プロセスまたは特性に関して実行するのに必要な属性の組み合わせを決定し、それらを属性の組み合わせA（「AC A」）としてデータベースから取得する。このシステムの実装例では、プライバシーサーバーの抽象化モジュールは、属性を追加または削除し、属性の組み合わせを取得し、任意の組み合わせ内の属性を変更するように構成されています。

【０４０５】

[457] スポーツ用品を販売するeコマースサイトに関する例では、プライバシーサーバーの抽象化モジュールは、個人の身長、体重、および予算に関連する属性が、望ましいアクション、アクティビティ、プロセス、または特性に関して実行するために必要であると判断する場合があります。指定されたデータ主体の身長、体重、および予算の属性をデータベースから取得して、それから構成される属性の組み合わせを形成する場合があります。血圧情報のリクエストを送信した医師の例では、プライバシーサーバーの抽象化モジュールは、最新の記録された収縮期および拡張期血圧値で構成される属性が、所望のアクション、アクティビティ、プロセスまたは特性に関して実行するために必要であると判断します。したがって、指定された個人の最新の収縮期および拡張期血圧値を取得して、それから構成される属性の組み合わせを形成できます。別の例としては、ランニングシューズのオンラインストアにアクセスするユーザーが関係すします。オンライン小売業者は、ユーザーが誰であるか、またはユーザーが過去にサイトにアクセスしたことがあるかどうかを知らない場合があります。ユーザーは、訪問したことのあるサイトでランニングシューズの買い物をしていることを知りたかったり、訪問したサイトで、過去数週間に他のサイトで見た靴を知りたかったりする場合があります。ユーザーは、最近の買い物や他のユーザーが設定した情報のみを訪問先サイトにリリースするようにプライバシーサーバーに通知できます。その結果、この例では、プライバシーサーバーは次の属性を選択できます。靴のサイズ＝ 9、最近他のWebサイトで閲覧した靴＝ Nike X、Asics Y、New Balance Z、閲覧した靴の平均価格＝ 109ドル、客の郵便番号＝ 80302、客の性別＝男性、買い物客の重量＝ 185ポンド。プライバシーサーバーは、これらの属性を収集し、一意のDDIDを生成するか、一時的に一意の動的に変化する値を受け入れ、または変更してDDIDとして機能し、DDIDを属性に割り当て、訪問したWebサイトにTDRとして送信します。ユーザーがSauconyモデル123を表示する場合、Webサイトは、表示された靴に関連する属性に関連する情報にこの属性を追加し、この情報を拡張TDRの一部としてプライバシーサーバーに送信します。

【０４０６】

[458]さらに別の例では、銀行員が、銀行と一緒に保持している口座に普通預金口座を追加したいクライアントと協力しています。銀行員は、クライアントに関するすべての情報を知る必要はなく、口座を開設するために必要な情報だけを知る必要があります。本発明を使用して、銀行家は、プライバシークライアントを介して銀行のプライバシーサーバに問い合わせて、顧客の新しい普通預金口座の開設を要求することができます。銀行のプライバシーサーバーは、リクエストの送信元と目的のアクションのデータ承認の制限を決定する場合があります。銀行のプライバシーサーバーは、顧客に関する次の属性を収集する場合があります。名前＝ Jane Doe、現在の口座番号＝ 12345678、現在の口座の種類＝確認、顧客の住所＝ 123 Main Street、Boulder、CO 80302、その他の署名者アカウント＝ Bill Doe、署名者と顧客＝夫の関係。銀行のプライバシーサーバーがこれらの属性を収集した後、これらの属性にDDIDを割り当て、プライバシークライアントを介

して情報を拡張TDRとして銀行員に送信します。

【０４０７】

[459]データ管理者は、一例では、属性の組み合わせAにデータ属性を含めることを選択できます。これにより、TDRの受信者は既存の追跡技術を使用して、結果のTDRが存在する間、関係者ZZを匿名で追跡できます。データ管理者は、既存の追跡技術を介して利用可能なデータよりも正確なデータを含めて、関連当事者ZZへの提案のパーソナライズとカスタマイズを容易にすることもできます。

【０４０８】

[460]ステップ3では、一例では、DDIDの要求がプライバシーサーバー（「PS」）に対して行われます。これには、特定の抽象化レベルのリクエスト、および特定のアクティビティ、要求されたアクション、プロセス、または特性に対応するシステムで使用されるDDIDとして機能する、一意のDDIDの生成または一時的に一意の動的に変化する値の受け入れまたは変更の要求が含まれる場合があります。DDIDを割り当てる前に、PSはDDID値が別のTDRによってアクティブに使用されていないことを確認します。潜在的な停止やシステムのダウンタイムに対処するためのバッファー期間を含む場合があります。

【０４０９】

[461]ステップ4で、一例では、PSの抽象化モジュールは、アクション、アクティビティ、プロセス、または特性に関する要求に応じてDDIDを割り当てて保存します。ステップ4は、さらに、関係者ZZによって要求されたウェブブラウジングにDDID　Xを割り当てる動作を含むことがあります。

【０４１０】

[462]ステップ5で、一例では、PSの抽象化モジュールは、取得した適用可能な属性の組み合わせで、DDID　XをTDRを作成します。TDR自体には、関係者ZZの実際の識別に関する情報が含まれていない場合がありますが、プライバシーサーバーのメンテナンスモジュールは、TDRを関連者ZZに再度関連付けるために必要な情報を含む場合があります。ステップ5は、属性の組み合わせ要求を、組み合わせに関連付けられたデータ主体に関連付けるセキュアデータベースを含むこともあります。これにより、関連する当事者ZZに特定の属性の目的のアクション、アクティビティ、プロセス、または特性に関して実行する必要があると見なされる組み合わせAを与えることができます。

【０４１１】

[463]図3は、本発明で、プライバシーサーバの抽象化モジュールによって取られ得る追加のステップの例を示す。ステップ6で、一例では、関係者ZZのWebブラウジングリクエスト用に作成されたTDRは、データ主体のデバイス、サービスプロバイダーデバイス、クラウドネットワーク経由でアクセス可能なクラウドクライアント、または該当するサービスプロバイダー、ベンダー、またはマーチャントへのプライバシーサーバーと同じコンピューティングデバイスの内部にあるプライバシークライアントを通じて伝送される。プライバシークライアントは、サービスプロバイダー、ベンダー、またはマーチャントとの望ましいブラウジングアクティビティに関連するデータを取得することもできます。

【０４１２】

[464]TDRの目的が達成されるか、所定の時間的制限に達すると、1つの例では、プライバシークライアントを介してプライバシーサーバーにTDRを送信できます。ステップ7で、戻ってくるTDRにTDRが作成された目的のアクション、アクティビティ、プロセス、または特性のそれぞれの新しい属性の組み合わせを追加します。図3に示す例では、関連当事者ZZは、サービスプロバイダー、マーチャント、またはベンダーに関連して目的のWebブラウジングを実行し、実行された所望のWebブラウジングに関連する属性の組み合わせを反映する属性の組み合わせQ（「AC　Q」）が生成されます。Webブラウジングが完了するか、TDRの一時的な制限が期限切れになると、Webブラウジングに関連するデータを反映する属性の組み合わせQで強化されたTDRを持つプライバシークライアントは、データをサービスプロバイダー、ベンダー、またはマーチャントからプライバシーサーバーに転送します。プライバシーサーバーでデータが受信されると、時間キー（TKs）または別の

方法、およびサービスプロバイダー、ベンダー、またはマーチャントから返された関連する属性の組み合わせによって、一例ではタイムスタンプがTDRに関連付けられますあるいは、その組み合わせは更新され、データ主体の集約データプロファイル内の安全なデータベースに保存される場合があります。

【０４１３】

[465]図4は、本発明のある例による、図3の動作に続いて行われ得る追加のステップの例を示しています。各拡張TDRがプライバシーサーバーによって受信されると、プライバシーサーバーのメンテナンスモジュールは、時間キー（TK）またはその他、DDID、および適切な属性のデータ主体との組み合わせによってタイムスタンプを関連付けることにより、ソースデータを更新します。図4の例に示すように、プライバシーサーバーは、タイムキー（TK）または別の方法で、タイムスタンプを記録し、DDID、属性の組み合わせA、および属性の組み合わせQを、セキュアなデータベース内の関連する関係者ZZと関連付けます。タイムスタンプ、DDID、属性の組み合わせ、データ主体、および関連するプロファイル間の関係情報は、プライバシーサーバーのメンテナンスモジュールで適宜保存、更新、または削除できます。これには、一例では、すべてのタイムスタンプ、DDID、属性の組み合わせ、データ主体、およびデータ主体の集約データプロファイル内の安全なデータベース内のプロファイル間のすべての関係情報の保存または更新が含まれます。属性の組み合わせからの望ましいアクション、アクティビティ、プロセス、または特性に関する新しいデータの関連付けが完了すると、一例では、DDIDは、上記と同じ方法で新しいTDRで使用するために再割り当てされます。

【０４１４】

[466]図5は、本発明のある例での、システムの例示的な多層抽象化実装と比較した場合の、システムの例示的な単一層抽象化実装間の違いを強調しています。図5に示す例1は、Webブラウジングアクティビティに関する図2～4の説明で前述したように、抽象化の単一層を持つシステムの例を示しています。図5の例1は、図2－4のWebブラウジングアクティビティに起因する最終処分の例を示しています。ここでは、セキュアデータベースが、タイムキー（TK）の属性の組み合わせA、Q、および要求する関連パーティZZに関連付けられたDDIDXなどによってタイムスタンプを関連付ける記録で更新されます。例1に関しては、システム外の関係者は、属性の組み合わせまたはデータ主体に関する識別情報にアクセスできないことに注意が必要です。ただし、システム内では、ここで説明する置換キー（RK）のユーザーは、関連当事者ZZ、属性の組み合わせA、属性の組み合わせQ、タイムスタンプとDDID　Xとの関係を示しています。

【０４１５】

[467]図5の例2は、一例で、システムの多層抽象化実装の1つの潜在的な実装を反映している。抽象化の機能は、ばらばらの異なるものではなく、システム内の複数のアプリケーションの機能です。TDRの動的な性質により、抽象化レベル間で同じベースライン原則を使用しながら、要求に応じてデータに関して対話を提供できます。この例では、プライバシーサーバーAおよび関連する安全なデータベースへのアクセスが許可されたユーザーは、DDID　X、DDID　P、DDID　TS、DDID　YYの関連付け、および関連する属性の組み合わせとDDIDsに紐付いたタイムスタンプのそれぞれにアクセスできます。ただし、ある例では、ユーザーは、開示された異なるDDID間の関連付けに関する情報にアクセスできません。プライバシーサーバーBおよび関連する安全なデータベースにアクセスした場合にのみ、DDID　XとDDIDの関係、およびDDID　TSとDDID　YYの関係に関する第2レベルの抽象化が明らかになります。図5に示すように、この2番目の抽象化レベルは、サブジェクトDDとDDID　XおよびP、およびサブジェクトCVとDDID　TSおよびYYの関係です。

【０４１６】

[468]サブジェクトCVおよびサブジェクトDDが問題のデータ主体のIDを反映する場合、例2はシステムの2層抽象化実装の1つの潜在的な実装を反映します。ただし、サブジェクトCVおよびサブジェクトDDの値にそれぞれ動的に変更可能なDDIDが割り当てられている場合、例2はシステムの3層抽象化実装の1つの潜在的な実装を反映します。望ましいレベ

ルのセキュリティとプライバシー／匿名性を実現するために、システムのすべての要素を複数のレベルで抽象化できます。

【０４１７】

[469]システムの利用例では、図5の例1と例2の両方が、プライバシーサーバーの検証モジュールがTDRやデータプロファイルで具体化された属性の組み合わせとDDIDを検証および検証することを許可する認証済みデータ構造を表すことがあります巡回冗長検査（CRC）、メッセージ認証コード、電子透かし、リンクベースのタイムスタンプ方法論などの方法論による任意の時点。これらの方法により、各データ主体、属性、属性の組み合わせ、集約データプロファイル、および異なる時点でプライバシーサーバーに含まれる他の要素の構成を確認することにより、さまざまな時点でのデータの状態と構成を検証できます。

【０４１８】

[470]さらに、他の使用例では、図5の使用例1および使用例2の両方に、システム関連のエラーまたは誤用が発生した場合の事後の法的分析を可能にするアクセスログモジュールで必要なデータを含むことがある。

【０４１９】

[471]図6は、ある使用例における、データセキュリティおよびデータプライバシーや匿名性を提供するプロセスの一例を示す。図6は、1つの例で、管理者またはシステムによって実装できるプロセスを示しています。図6－10に概説されている操作は、Simple Object Access Protocol（SOAP）、Representational State Transfer（REST）Application Programming Interfaces（API）、またはService Oriented Architecture（SOA）などの既知のプログラミング技術、さらにヘルスケア向けHL7、携帯電話事業者向けSID、小売向けARTS、保険向けACORD、マルチコモディティモデル向けM3、製造およびサプライチェーン向けOAGIS、石油＆ガス／ユーティリティなどのPPDMなどの標準的な業界標準データモデルによって円滑に行うことが可能になります。

【０４２０】

[472]図6のステップ1で、システムへの入力としてデータ属性が受信または作成されます。本開示の目的で前述したように、データ属性とは、個人、場所、物、または関連するアクション、行動、プロセスまたは特性などのデータ主体を識別するために、個別に、あるいは他のデータ要素と組み合わせて使用できるデータ要素を指します。1777 6th Street, Boulder, Colorado 80302で構成される住所はデータ属性の1つの例です。

【０４２１】

[473]図6のステップ2では、データ属性が該当するサブジェクトに関連付けられています。上記の例では、データ属性の住所は、コロラド市裁判所に関連付けられています。

【０４２２】

[474]図6のステップ3では、当てはまるカテゴリ、値、分類からなるデータ属性と決定因子にそれぞれのデータの要素が結び付けられ、ユーザーの実行したいアクション、行動、処理や記録に関して、属性の活用をしやすくしています。たとえば、上記のデータ属性の住所に関連付けられる要素は次の場合が想定されます。（a）住所として分類される （b）値：1； 7； 7； 7； 6th； S； t； r； e； e； t； B； o； u； l； d； e； r； C； o； l； o； r； a； d； o； 8； 0； 3； 0； 2； 、あるいはこれらの値の組み合わせとして分類される （c）建物は静止しており、自然の中の一部とみなされる対象の建物に関連するデータ属性の別の例は、建物の状態です（a）建物の状態として分類される （b）良好な状態を示す値を持つ （c）建物の状態が経時的に改善または劣化する可能性があるため、本質的に変数として分類される対象の建物に関連するデータ属性の別の例は、（a）建物内にオフィスを持つ組織として分類される（b）コロラド州ボールダーオルタナティブセンテンシングプログラム（CASP）の値として分類される （c）CASPは将来オフィスの場所を変更する可能性があるため、本質的に変数として分類される外的因子による情報は、データ主体に関連付けられた属性を含む場合があることに注意してください。たとえば、上記の建物の場合、ボールダーコロラドオルタナティブセンテンシングプログラム（CASP）がコロラド市裁判所ビルに事務所を構え、John S

mithがCASPで働いており、平日のJohn Smithがボルダーの6番街1777に現れることを知っている場合、その元の人はこの外的因子による情報を使用して、ボルダーのコロラド市裁判所ビルの住所を識別することができます。したがって、John SmithがCASPで働いているという事実は、データ主体の属性である可能性があり、データ主体、つまり住所の建物を明らかにしている可能性があります。

【０４２３】

[475]図6のステップ4では、システムに入力された各データ属性が、データ主体の集約データプロファイル（たとえば、図1および1Aを参照）に追加されます。上記の例では、前述のデータ属性がコロラド市裁判所の集計データプロファイルに追加されます。

【０４２４】

[476]ステップ5で、属性の組み合わせが識別および形成され、目的のアクティビティ、アクション、プロセス、または特性に関するサポートが提供されます。このステップでは、特定のアクション、アクティビティ、プロセス、または特性に関して必要な属性を指定するテンプレートの作成または読み込みを行うことがあります。たとえば、eコマースアクションの場合、テンプレートは、データ主体の年齢、性別、サイズ、および好みの色に関する情報を属性として要求できます。旅行予約機能を使用する別の例では、テンプレートは、属性としてエコノミークラス、ビジネスクラス、またはファーストクラスによるデータ主体の空の旅の手段に関する情報を要求する場合があります。プライバシーサーバーは、さまざまなアクション、アクティビティ、プロセスや特性をサポートするために、複数のそのようなテンプレートを読み込みするか、アクセスすることができます。さらに、プライバシーサーバーは、制御者の必要に応じて、必要な新しいアクション、アクティビティ、プロセスや特性に関する新しいテンプレートの作成や既存のテンプレートの手動オーバーライドを容易にするように構成できます。このような手動のオーバーライドは、たとえば、データ主体のモバイルデバイスで実行されているプライバシークライアントのGUIによって行うことができます。たとえば、データ主体は、GUIを使用して、Data Subjectがクルーズ船で旅行している可能性があるため、エコノミークラス、ビジネスクラス、またはファーストクラスによるData Subjectの好みの旅行手段に関する情報の要求をオーバーライドできます。したがって、同様にData Subjectは、属性としてスイート、バルコニー、ステートルーム、外側のステートルーム、または内側のステートルームのいずれを望んでいるかを指定することができます。この例では、GUIにより、データ主体は、データ主体の集約データプロファイルから送信するための最小限の属性を選択できます。

【０４２５】

[477]ステップ6で、プライバシーサーバーは、データ主体のデバイス、サービスプロバイダーデバイス、クラウドネットワークを介してアクセス可能であり、特定のアクション、アクティビティ、プロセス、または特性に関するプライバシーネットワークと同じコンピューティングデバイスに存在する可能性があるプライバシークライアントから要求を受信します。プライバシークライアントからプライバシーサーバーが受信する可能性のある要求の性質と内容は、システムがDRMI、DRMDなどとして実装されているかどうか、要求が医療、教育、モバイル金融、Web、IoT、その他のアプリケーションなどに関係するかどうかなど、さまざまな要因によって性質が異なる場合があります。

【０４２６】

[478]ステップ7では、特定のアクション、アクティビティ、プロセス、または特性に関して、セキュリティ、匿名性、プライバシー、および関連性に適したレベルの抽象化レベルに関する決定が行われます。たとえば、システムは、関連するデータ属性をリンクし、特定のアクション、アクティビティ、プロセス、または特性に関して望ましいと判断されたTDRに関連データ属性を分離することにより、抽象化の初期層を導入できます。個別の属性、属性の組み合わせ、またはその両方を、置換キー（RKs）にアクセスしないと理解できないDDIDで置き換えることにより、データ属性をTDRに分離するだけでなく、抽象化の追加レイヤーを導入できます。TDR内に含まれる、または参照される属性のプライバシー、匿名性、セキュリティは、暗号化、トークン化、仮名化、削除などの既知の保護技術

を使用することでさらに改善または強化でき、追加のDDIDsを使用してネットワーク、インターネット、イントラネット、および本発明の実装と統合または通信することができるサードパーティコンピュータを参照することでさらに抽象化層を導入できます。

【０４２７】

[479]ステップ8で、所望のアクション、アクティビティ、プロセスまたは特性に関して必要な場合がある適用可能なテンプレートに関連付けられた属性に基づいて、プライバシーサーバからの制御者によって所望の属性の組み合わせが選択されます。抽象化モジュールは、制御者によって制御されるか、承認されたパーティとして別のユーザーに委任される可能性のある適切な属性を決定できます。承認を受けたユーザーは、抽象化モジュールを使用して、既定のテンプレートに基づいて属性を選択し、その場で属性を選択できます、または、他の方法の中でも、適切な入力を上手く検出します。

【０４２８】

[480]スポーツ機器を販売するeコマースサイトのステップ8の例では、制御者として機能しているインターネットブラウザープロバイダーは、プライバシーサーバーの抽象化モジュールを使用して、データ主体の身長、体重、予算に関する情報を決定します。これらの情報は例えばカヤックやパドルなどの適切なスポーツ用品のオプションを提供するために、受信側のWebサイトにとって必要です。

【０４２９】

[481]ステップ9で、プライバシーサーバーの抽象化モジュールは一意のDDIDsを生成するか、時間的に一意の動的に変化する値を受信または変更してDDIDsとして機能し、DDIDをステップ8の各属性の組み合わせに割り当ててTDRsを形成します。これらのDDIDsは、置換または単純な関連付けなどのさまざまな機能を提供することができます。たとえば、制御者として機能するインターネットブラウザープロバイダーが抽象化モジュールに単一レイヤーの抽象化でTDRを作成するように指示した場合、関連付けキー（AKs）にアクセスせずに同じデータ主体の他のTDRに視覚的に関連付けられていないDDIDを割り当てることがあります。別の例として、制御者として機能するインターネットブラウザプロバイダーが抽象化モジュールに2層の抽象化でTDRを作成するように指示した場合、（i）TDRの期間のデータ属性に関連付けられるDDIDsを割り当て、（ii ）さらに、Ab5のDDIDをデータ主体の体重に、67hのDDIDをデータ主体の身長に、Gw2のDDIDをデータ主体の予算に割り当てることにより、データ属性をさらに抽象化します。ステップ9は、データベースから属性を取得することも含み、これらの属性はデータ主体に関連する。ステップ9で使用されるDDIDsは、現在使用されておらず期限切れの、以前に使用されていたDDIDsから選択できます。

【０４３０】

[482]ステップ10で、属性の組み合わせとDDIDsで構成されるTDRsが、プライバシーサーバーによって、受信者に関連する望ましいアクション、アクティビティ、プロセス、または特性に関連して受信者が使用するために、プライバシークライアントを介して受信者に送信されます。たとえば、上記の例では、制御者として機能するインターネットブラウザープロバイダーは、DDIDとAb5、67h、およびGw2で構成される第2レベルの抽象化データ属性で構成されるTDRを受信者としてeコマースサイトに配信できます。

【０４３１】

[483]ステップ11で、TDRs（属性の組み合わせと、実行したいアクション、アクティビティ、プロセス、または特性に関するDDIDsで構成される場合があります）が、プライバシークライアントを用いて受信者によって受信されます。システムの使用目的がビッグデータ分析の出力の作成であれば、TDRの受信が最後のステップになる場合があります。（たとえば、該当するData Subject（s）に「忘れられる権利」が保障されるようにビッグデータ分析用に秘匿化／匿名化されたデータを提供する図Zで説明した本発明のありうる使用例を参照してください。）ただし、TDRsのよりインタラクティブな活用には、オプションとしてステップ12から17が含まれます。

【０４３２】

[484]オプションのステップ12で、TDRs（目的のオンラインアクション、アクティビティ、プロセス、または特性の属性の組み合わせとDDIDsで構成されます）は、プライバシークライアントによって受信者によって解釈され、AKsやRKsの使用へのアクセスを提供します。これはTDRsの内容を理解するために必要です。たとえば、上記の例では、受信者としてのeコマースサイトがRK情報にアクセスして、Ab5に起因する値であるデータ主体の体重、67hに起因する値である身長、Gw2に起因する値である予算の情報を取得します。

【０４３３】

[485]オプションのステップ13で、プライバシークライアントは、元のTDRデータ属性をTDR形式の新しい情報として増強するオンラインアクション、アクティビティ、プロセス、または特性に関連付けられた新しいデータ属性を取得できます。

【０４３４】

[486]オプションのステップ14で、プライバシークライアントは、元のTDRデータ属性をTDR形式の新しい情報として拡張する、目的のオンラインアクション、アクティビティ、プロセス、または特性に関連付けられたオフラインアクティビティに関連付けられた新しいデータ属性を取得します。

【０４３５】

[487]オプションのステップ15で、プライバシークライアントは、オンライン／オフラインセッションに関連するDDIDと属性の組み合わせで構成されるTDRをプライバシーサーバーに送信します。

【０４３６】

[488]ステップ14および15のコンテキストでは、TDRsはプライバシークライアントを介してAKsまたはRKsなしでプライバシーサーバーに送信されるため、分解されて匿名化された形式で送信されます。ゆえに、TDRsを何者かが傍受しても、希望するアクション、アクティビティ、プロセス、または特性といったデータ主体に関する情報は一切開示されません。

【０４３７】

[489]オプションのステップ16で、一例では、属性の組み合わせの再集計は、プライバシーサーバーに存在するアソシエーションキー（AKs）および（DKs）によるDDIDと属性の組み合わせ間の関係情報のメンテナンスモジュールによるアプリケーションを介して実行されます。この例では、元のTDRsまたは変更されたTDRsがプライバシーサーバーに戻り、推奨されたkayAKsおよびパドルに関する新しい情報をデータ主体の集計データプロファイルに変更または追加する可能性があります。

【０４３８】

[490]属性の組み合わせからの望ましいアクション、アクティビティ、プロセス、または特性に関する前述の再データの再集計が完了すると、この例では、DDIDが期限切れであると見なされ、オプションのステップ17、他のユーザー属性、属性の組み合わせ、データ主体、アクション、アクティビティ、プロセス、特性、またはデータの再割当てと使用のためにシステムに再導入されます。同時に上記と同じ方法で新しいTDRsを形成します。

【０４３９】

[491]たとえば、上記のステップ9で属性に割り当てられたDDIDs Ab5、67h、およびGw2は、他のデータ主体に関連するデータ属性に、たとえば同様のケースホップまたは遠隔ケースリープ方式で割り当てられます。たとえば、ケースホップの場合、Ab5の初期データ主体と同様の重みの2番目のデータ主体への再関連付け、または重みに関するデータの一部または同じ番号を含むが同じデータ主体と関連付けられていないものの再関連付けが含まれる場合があります。一方、遠隔ケースリープでは、DDIDを待機している無関係のデータ属性にAb5を再割り当てする必要があります。

【０４４０】

[492]図6の2番目の例では、医師は、看護師によってオフラインで収集され、データ主体の集計データプロファイルにオンラインで入力された患者のデータ主体に関する血圧情報

を要求できます。この要求により、上記のステップ8の一部として、プライバシーサーバーの抽象化モジュールが、データ主体の最新の収縮期血圧と拡張期血圧の値で構成される属性の組み合わせを抽出する場合があります。ステップ9の一部として、データ主体のIDを指定する代わりに、プライバシーサーバーは、これらの属性の組み合わせをプライバシーサーバーによって割り当てられたDDIDと組み合わせて、TDRを形成する場合があります。ステップ10の一部として、サブジェクトデバイス、サービスプロバイダーデバイス、クラウドネットワークを介してアクセス可能であり、クラウドネットワークに存在する、あるいはプライバシーサーバーと同じコンピューティングデバイスに常駐するプライバシークライアントを介して、割り当てられたDDIDとともに血圧属性を医師に伝えることができます。この時点で、血圧に関するDDIDと属性の組み合わせの組み合わせがTDRを構成します。ステップ12の一部として、受信者としての医師は、RKsを介して血圧値を読み取り、ステップ13および14の一部として、血圧測定を新たな属性として、これに関するオンラインおよびオフラインの観察結果、推奨事項、またはコメントを記録します。ステップ15の一部として、オンライン／オフライン情報で補強されたTDRは、プライバシークライアントを介してプライバシーサーバーに返されます。ステップ16の一部として、プライバシーサーバーはこの情報を使用して、データ主体の集計データプロファイルを更新できます。この方法では、TDRの意図しない受信者は、データ主体のIDを相関させることができず、医師による使用後の同様のケースホップまたは遠隔ケースリープ方式で別のデータ主体に再割り当てできるDDIDのみが表示されます。

【０４４１】

[493]図6Aは、外部データベースとの相互作用を含む使用例での、データセキュリティ、データプライバシーおよび匿名性を提供するプロセスの例を示します。図6Aは、一例において、制御者またはシステムによって実装され得るプロセスステップを示しています。

【０４４２】

[494]図6Aのステップ1で、サードパーティのデータソースが、システムへの入力としてデータ主体に関係するデータ属性を含むデータを送信します。図6Aでは、システムへのデータ主体入力に関するデータ属性を含むデータを提出する前に、サードパーティのデータソースがデータベースで直接または間接的に保持する各データ主体の集約データプロファイル（例　図1A）をすでに作成していることに注意が必要です。

【０４４３】

[495]ステップ2で、プライバシーサーバーは、データ主体のデバイス、サービスプロバイダーデバイス、クラウドネットワークを介してアクセス可能であり、特定のアクション、アクティビティ、プロセス、または特性に関するプライバシーネットワークと同じコンピューティングデバイスに存在する可能性があるプライバシークライアントから要求を受信します。プライバシークライアントからプライバシーサーバーが受信するリクエストの性質と内容は、システムがDRMI、DRMDなどとして実装されているかどうか、リクエストが医療、教育、モバイル、金融、Web、モノのインターネット、その他のアプリケーションなどに関連するかどうかなど、さまざまな要因によって異なる場合があります。

【０４４４】

[496]TDR内に含まれる、または参照される属性のプライバシー、匿名性、セキュリティは、暗号化、トークン化、仮名化、削除などの既知の保護技術を使用することでさらに改善または強化でき、追加のDDIDsを使用してネットワーク、インターネット、イントラネット、および本発明の実装と統合または通信することができるサードパーティコンピュータを参照することでさらに抽象化層を導入できます、

【０４４５】

[497]ステップ3では、特定のアクション、アクティビティ、プロセス、または特性のセキュリティ、匿名性、プライバシー、および関連性に適したレベルの抽象化レベルに関する決定が行われます。たとえば、システムは、置換キー（RKs）にアクセスしないと理解できないDDIDsでそれらを表すことにより、個々の属性、属性の組み合わせ、またはその両方を抽象化することにより、抽象化を導入できます。TDR内に含まれる、または参照され

る属性のプライバシー、匿名性、セキュリティは、暗号化、トークン化、仮名化、削除などの既知の保護技術を使用することでさらに改善または強化でき、追加のDDIDsを使用してネットワーク、インターネット、イントラネット、および本発明の実装と統合または通信することができるサードパーティコンピュータを参照することでさらに抽象化層を導入できます。

【０４４６】

[498]ステップ4で、所望のアクション、アクティビティ、プロセスまたは特性に関して必要な場合がある適用可能なテンプレートに関連付けられた属性に基づいて、プライバシーサーバからの制御者によって所望の属性の組み合わせが選択されます。抽象化モジュールは、制御者によって制御されるか、承認されたパーティとして別のユーザーに委任される可能性のある適切な属性を決定できます。承認を受けたユーザーは、抽象化モジュールを使用して、既定のテンプレートに基づいて属性を選択し、その場で属性を選択できます、または、他の方法の中でも、適切な入力を上手く検出します。

【０４４７】

[499]ステップ4の1つの例では、ヘルスケア研究の研究で、制御者として機能している病院は、プライバシーサーバーの抽象化モジュールを使用して、研究施設に情報を送信する前にデータ主体の身長、体重、名前に関する情報を難読化します。

【０４４８】

[500]ステップ5で、プライバシーサーバーの抽象化モジュールは、DDIDをステップ4の各属性の組み合わせに割り当てて、TDRsを形成します。これらのDDIDsは、置換または単純な関連付けなどのさまざまな機能を提供することができます。ある例として、制御者として機能する病院が抽象化モジュールに2層の抽象化でTDRを作成するように指示した場合、Ab5のDDIDをデータ主体の体重、67hのDDIDをデータ主体の身長、データ主体の名前をGw2のDDIDに割り当てることでデータ属性を抽象化し、置換キー（RKs）へのアクセスなしでは理解できません。ステップ9はまた、データベースから属性を取得することを含み、これらの属性はデータ主体に関連する。ステップ5で使用されるDDIDsは、現在使用されておらず期限切れの、以前に使用されていたDDIDsから選択できます。

【０４４９】

[501]ステップ6で、属性の組み合わせとDDIDsで構成されるTDRsが、プライバシーサーバーによって、受信者に関連する望ましいアクション、アクティビティ、プロセス、または特性に関連して受信者が使用するために、プライバシークライアントを介して受信者に送信されます。たとえば、上記の例では、管理者として機能する病院は、Ab5、67h、およびGw2で構成される抽象データ属性で構成されるTDRを受信者である研究施設に配信できます。

【０４５０】

[502]ステップ7で、TDRs（属性の組み合わせと、実行したいアクション、アクティビティ、プロセス、または特性に関するDDIDsで構成される場合があります）が、プライバシークライアントを用いて受信者によって受信されます。たとえば、上記の例では、受信者しての研究施設は、分析のための情報を受け取りますが、体重、身長に関する個人識別情報が漏れることはありません。むしろ、研究施設は、関連するRK情報へのアクセスを許可されない限り解読できないAb5、67hおよびGw2を受け取ります。目的がビッグデータ分析である限り、TDRsの受信は最後のステップになる可能性がありますが、TDRsのよりインタラクティブな使用にはオプションのステップ8から13が含まれる場合があります。

【０４５１】

[503]オプションのステップ8で、TDRs（目的のアクション、アクティビティ、プロセス、または特性の属性の組み合わせとDDIDsで構成されます）は、プライバシークライアントによって受信者によって解釈され、AKsやRKsの使用へのアクセスを提供します。これはTDRsの内容を理解するために必要です。

【０４５２】

[504]オプションのステップ9で、プライバシークライアントは、元のTDRデータ属性をT

DR形式の新しい情報として増強するオンラインアクション、アクティビティ、プロセス、または特性に関連付けられた新しいデータ属性を取得できます。

【０４５３】

[505]オプションのステップ10で、プライバシークライアントは、元のTDRデータ属性をTDR形式の新しい情報として拡張する、目的のオンラインアクション、アクティビティ、プロセス、または特性に関連付けられたオフラインアクティビティに関連付けられた新しいデータ属性を取得します。

【０４５４】

[506]オプションのステップ11で、プライバシークライアントは、オンライン／オフラインセッションに関連するDDIDと属性の組み合わせで構成されるTDRをプライバシーサーバーに送信します。TDRsはプライバシークライアントを介してAKsまたはRKsなしでプライバシーサーバーに送信されるため、分解されて匿名化された形式で送信されます。ゆえに、TDRsを何者かが傍受しても、希望するアクション、アクティビティ、プロセス、または特性といったデータ主体に関する情報は一切開示されません。

【０４５５】

[507]オプションのステップ12で、一例では、属性の組み合わせの再集計は、プライバシーサーバーに存在するアソシエーションキー（AKs）および置換キー（RKs）によるDDIDと属性の組み合わせ間の関係情報のメンテナンスモジュールによるアプリケーションを介して実行されます。この例では、元のTDRsまたは変更されたTDRsがプライバシーサーバーに戻り、推奨されたkayAKsおよびパドルに関する新しい情報をデータ主体の集計データプロファイルに変更または追加する可能性があります。

【０４５６】

[508]属性の組み合わせからの望ましいアクション、アクティビティ、プロセス、または特性に関する前述の再データの再集計が完了すると、この例では、DDIDが期限切れであると見なされ、オプションのステップ13、他のユーザー属性、属性の組み合わせ、データ主体、アクション、アクティビティ、プロセス、特性、またはデータの再割当てと使用のためにシステムに再導入されます。同時に上記と同じ方法で新しいTDRsを形成します。

【０４５７】

[509]図6Bは、使用例でデータベースに含まれる、機密性が高く、組織の外部で識別可能な方法で公開できないと考えられるデータ要素に動的匿名性を提供する方法を示しています（データベースが図1Aに示すようにシステムの内部にあっても、図1Bに示すように外部にあっても）。データ主体または機密性の高いアクション、アクティビティ、プロセスや特性（直接識別子）を直接識別するデータ、またはデータを間接的に識別するデータ他のデータ（準識別子）と組み合わせた場合の対象または機密のアクション、アクティビティ、プロセスや特性などがそのようなデータ要素の例です。システムは、データをDDIDsで置き換えることにより、組織の外部に公開されると、機密データを動的に隠蔽する場合があります。DDIDsと不明瞭な機密データとの関連付けを理解するために必要なキーは、Circle of Trust（CoT）で安全に保持され、許可された関係者のみが利用できるようになります。DDIDsを「設計」する（つまり、データ隠蔽戦略をそのように計画する）ことにより、データ主体または信頼できる当事者が確立したPERMSと一貫性のあるDDIDのさまざまなレベルのデータ使用や分析を可能にします。DDIDsで表される機密データは、データ主体または信頼できる当事者によって、元になる機密データを受信や利用することを承認された当事者からキーが要求されるまで開示されないことがあります。

【０４５８】

[510]使用例では、上記の機密データの不明瞭化は、データベースから機密データの要求を上記のコンピューターアプリケーションの提示層で傍受し、上記のように機密データをDDIDに置き換えることにより、対象のデータベースにデータを要求する特定のコンピュータアプリケーションに関してのみ行われます。他にも次のような導入例が考えられます。データベース接続レベルで機密データの要求を傍受したり、機密データを上記のDDIDに置き換えたりすることにより、対象のデータベースからデータを要求するコンピュータアプ

リケーションに関して機密データの不明瞭化を行うことができます。

【０４５９】

[511]図6Bは、1つの例で、管理者またはシステムが機密情報を匿名化するために実装できるプロセスを示しています。

【０４６０】

[512]ステップ1の図6Bでは、プライバシーサーバーは、データ主体のデバイス、サービスプロバイダーデバイス、クラウドネットワークを介してアクセス可能であり、プライバシーサーバーと同じコンピューティングデバイスに存在するプライバシークライアントからリクエストを受信します。このリクエストはデータベースに含まれる、機密性が高く、組織の外部で識別可能な方法で公開できないと考えられるデータ要素（データベースが図1Aに示すようにシステムの内部にあっても図1Bに示すように外部にあっても）に対するものです。データ主体または機密性の高いアクション、アクティビティ、プロセスや特性（直接識別子）を直接識別するデータ、またはデータを間接的に識別するデータ他のデータ（準識別子）と組み合わせた場合の対象または機密のアクション、アクティビティ、プロセスや特性などがそのようなデータ要素の例です。プライバシークライアントからプライバシーサーバーが受信する可能性のある要求の性質と内容は、システムがDRMI、DRMDなどとして実装されているかどうか、要求が医療、教育、モバイル金融、Web、IoT、その他のアプリケーションなどに関係するかどうかなど、さまざまな要因によって性質が異なる場合があります。

【０４６１】

[513]ステップ2では、抽象化モジュールは、セキュリティ、プライバシー、匿名性、および機密情報要素の関連性に必要な抽象化レベルを決定します。データ主体または信頼関係者とDDIDの関連付け戦略は、PERMSによって許可されたデータの使用／分析の範囲と一致する機密データ要素のために開発されています。

【０４６２】

[514]ステップ3では、機密データ要素を動的に隠すために抽象化モジュールによって決定されたDDIDがプライバシークライアントに送信されます。

【０４６３】

[515]ステップ4では、抽象化モジュールによって決定されたDDIDsでデータ要素を置き換えることにより、機密データ要素が動的に隠され、結果のDDIDsを使用して、組織外部に通信されるデータの機密データ要素が置き換えられます。ステップ3の例を示します。プレゼンテーションでデータベースからの機密データの要求を傍受し、上記のコンピュータアプリケーションの層と、抽象化モジュールによって決定されるように、機密データをDDIDで置き換えることで、対象のデータベースからデータを要求する特定のコンピューターアプリケーションに関してのみ、機密データ要素の不明瞭化が発生します。ステップ3の例を示します。プレゼンテーションでデータベースからの機密データの要求を傍受し、上記のコンピュータアプリケーションの層と、抽象化モジュールによって決定されるように、機密データをDDIDで置き換えることで、対象のデータベースからデータを要求する特定のコンピューターアプリケーションに関して、機密データ要素の不明瞭化が発生します。

【０４６４】

[516]ステップ5で、DDIDと不明瞭な機密データ要素との関連付けを理解するために必要なキーが、Circle of Trust（CoT）に安全に保存されます。

【０４６５】

[517]ステップ6では、DDIDと、Circle of Trust（CoT）に安全に保存されている不明瞭な機密データ要素との関連付けを理解するために必要なキーを、許可された関係者のみが利用できるようにします。DDIDsで表される機密データは、データ主体または信頼できる当事者によって、元になる機密データを受信や利用することを承認された当事者からキーが要求されるまで開示されません。

【０４６６】

[518]図7は、この開示の例で受信者によって実施され得るプロセスステップの例を示しま

す。

【０４６７】

[519]ステップ1で、TDRの期間中にデータ属性に関連付けられるDDIDと組み合わされた制御者によって選択された属性の組み合わせで構成されるTDRが、データ主体のデバイス上にあるプライバシークライアントによって受信者クライアントによって受信されます。サービスプロバイダーデバイス上、クラウドネットワーク経由でアクセス可能で、クラウドネットワーク内に常駐、またはプライバシーサーバーと同じコンピューティングデバイス上に常駐し、目的のアクション、アクティビティ、プロセス、または特性に関するリクエストを示しますたとえば、上記のカヤックの例では、eコマースサイト受信者は、目的のアクション、アクティビティ、プロセス、または特性に関するデータ主体のTDR要求を受信する場合があります。

【０４６８】

[520]ステップ2で、TDRs（目的のオンラインアクション、アクティビティ、プロセス、または特性の属性の組み合わせとDDIDsで構成される場合があります）は、AKsやRKsの使用へのアクセスを提供するプライバシークライアントによって受信者によって解釈されます。これはTDRsの内容を理解するために必要です。たとえば、上記の例では、eコマースサイトは、データ主体のデバイス、サービスプロバイダーデバイス、クラウドネットワーク経由でアクセスできる、クラウドネットワーク内にある、またはプライバシーサーバーと同じコンピューティングデバイス上にあるRKの情報にアクセスして、Ab5に起因する値であるデータ主体の体重、67hに起因する値である身長、Gw2に起因する値である予算の情報を取得します。

【０４６９】

[521]ステップ3では、一例では、受信者は、受信したTDR情報を使用して、データ主体の送信された属性に対する応答をカスタマイズすることができます。カヤックの例では、これにより、eコマースサイトは情報を使用して、購入するカヤックとパドルに関するデータ主体の提案を提供できます。

【０４７０】

[522]ステップ4で、一例では、プライバシークライアントは、データ主体のデバイス、サービスプロバイダーデバイスに存在するプライバシークライアントへのアクセスにより、属性の組み合わせに関連付けられた受信者で実行されるオンラインアクティビティのデータを取得します。プライバシークライアントは、クラウドネットワーク経由でアクセスでき、クラウドネットワークに常駐するか、プライバシーサーバーと同じコンピューティングデバイスに常駐します。

【０４７１】

[523]ステップ5で、一例では、受信者は、属性の組み合わせに関連付けられたオフラインアクティビティのデータを取得し、オンラインデータに変換します。カヤックの例などでは、データ主体もeコマースサイトによって運営されている物理的な店舗のロイヤルティリワードメンバーであり、顧客の情報をさらに収集できるようにすれば、受信者はオンラインコンポーネントで受信データをさらに増やすことができます。

【０４７２】

[524]ステップ5で、一例では、プライバシークライアントは、属性の組み合わせとDDIDsに関連付けられたオンラインセッションおよびオフラインアクティビティに関連するデータを、非集計および匿名化形式でプライバシーサーバーに送信します。

【０４７３】

[525]ステップ6では、TDRsのDDIDコンポーネントがシステムに再導入され、他の属性、属性の組み合わせ、データ主体、アクション、アクティビティ、プロセス、特性、またはデータとともに使用され、上記と同じ方法で新しいTDRsが形成されます。　後に同じDDIDが存在する場合がありますが、このDDIDでは、データ主体に関連付けられている他のTDRまたは以前に関連付けられていたTDRに接続できない場合があります。たとえば、その日または週の後半に、eコマースサイトで同じDDIDが再び表示される場合がありますが

、完全に異なるデータ主体に関する異なる情報が添付されます。
【０４７４】
[526]図7の2番目の例では、血圧情報を要求する医師は、ステップ1の一部として、プライバシークライアントを介して、最後に記録された収縮期および拡張期血圧値とプライバシーサーバーによってデータ主体に割り当てられたDDIDで構成されるTDRを受信します。ステップ2および3の一部として、医師は血圧情報を読み取ることができます。ステップ4および5の一部として、医師は血圧に関する観察、推奨事項、またはコメントを追加できます。これは、ステップ6の一部として、データ主体のデバイスに存在するプライバシークライアントを介してプライバシーサーバーに送信されます。サービスプロバイダーデバイス上、クラウドネットワークを介してアクセス可能であり、クラウドネットワーク内に存在するか、プライバシーサーバーと同じコンピューティングデバイス上に存在します。
【０４７５】
[527]図8は、導入例での、特定の時間や場所でのアクション、アクティビティ、プロセスまたは特性に関して進行する権限を検証するプロセスの一例を示しています。
【０４７６】
[528]ステップ1では、一例として、受信者は、プライバシーサーバーにリクエストを送っています。これはデータ主体のデバイス、サービスプロバイダーデバイス、クラウドネットワークに常駐するプライバシークライアントを介してアクセス可能です。このリクエストでは非公開のデータ主体やTDRに関連付けられた関連者が参加する権限があるかどうかを確認します。たとえば、eコマースサイトでおすすめされているkayAKsとパドルを検索した後、購入する準備ができた場合、eコマースサイトはプライバシーサーバーの認証モジュールに照会して、関連当事者が要求されたトランザクションを完了することが許可されます。
【０４７７】
[529]ステップ2で、一例では、プライバシーサーバーの認証モジュールは、TDRに含まれるDDIDをデータベースに含まれる許可されたDDIDのリストと比較して、データ主体または関連当事者の承認を指定された時間や場所での活動、プロセスまたは特性に関して決定します。カヤックの例では、プライバシーサーバーの認証モジュールは、使用されているDDIDがまだアクティブで承認されていることを確認し、それにより、データ主体または関連者が目的のトランザクションの完了を承認されていることを示します。
【０４７８】
[530]オプションで、ステップ3で、一例では、プライバシーサーバーは、データ主体のデバイス上、サービスプロバイダーデバイス上、クラウドネットワーク経由でアクセス可能でクラウドネットワーク上に存在する、またはプライバシーサーバー（この場合はeコマースサイト）と同じコンピューティングデバイスで、目的のトランザクションへの参加が許可されていることを確認します。
【０４７９】
[531]オプションのステップ3が呼び出された場合、1つの例では、ステップ4で、プライバシークライアントを制御している関係者が許可されていると確認されたかどうかを確認します。たとえば、信頼できるユーザーになりすましてユーザー名、パスワード、クレジットカードの詳細などの情報を取得しようとする試み（「フィッシング」とも呼ばれます）を避けるため、ステップ4では、既知の承認技術によるカヤック機器の認定再販業者である電子商取引サイトによる検証が必要になる場合があります。
【０４８０】
[532]ステップ5において、一例では、検証が得られた場合、プライバシーサーバの認証モジュールは、認可ステータス情報をプライバシークライアントの制御下の当事者に送信する。
【０４８１】
[533]ステップ6では、一例では、許可ステータス情報を使用して、目的としているアクション、アクティビティ、プロセス、または特性に関する処理を許可または拒否します。

【０４８２】
[534]ステップ7で、認証機能が実行され、オプションの追加検証ステップが完了すると、プライバシーサーバーは、プライバシークライアントを介して、TDRコンテンツを解釈するために必要なAKやRKの情報を送信します。製品とトランザクションは、受信者によって処理されます。受信者は、上記の例ではeコマースサイトです。
【０４８３】
[535]図8の2番目の例では、医師はプライバシークライアントを介してプライバシーサーバーにTDRを送信し、患者であるデータ主体が探索的研究への参加を許可されているかどうかを確認します。これにより、ステップ2の一部として、プライバシーサーバーの認証モジュールは、TDRのデータ主体のDDIDをデータベースに含まれる許可DDIDのリストと比較して、データ主体が調査への参加を許可されているかどうかを判断します。オプションで、ステップ3で、プライバシーサーバーの認証モジュールは、データ主体が探索的研究の参加者であることを要求する権限があることを確認するために、医師に要求することができます。オプションのステップ3が呼び出されると、ステップ4で、パスワードの確認や多要素認証などの既知の承認方法によって医師が承認されているかどうかを確認します。ステップ5で検証が得られた場合、プライバシーサーバーの認証モジュールは、プライバシークライアントを介して承認ステータス情報を送信し、ステップ6で承認ステータスを使用して、データ主体の参加要求を許可または拒否します。探索的研究とステップ7は、TDRコンテンツの解釈と続行に必要なAKやRKキー情報へのアクセスを提供します。
【０４８４】
[536]図9は、導入例での、置換キー（RK）またはアソシエーションキー（AK）の情報または他の保護情報が検証されない限り開示を差し控えるプロセスの例を示します。ステップ1に示すように、一例では、TDRを含むプライバシークライアントを制御する当事者は、データ主体のデバイス、サービスプロバイダーデバイス、アクセス可能なプライバシークライアントを介してプライバシーサーバーの認証モジュールに、AKやRKや暗号化、トークン化、仮名化などの手法を使用して保護されたTDRデータ属性のロック解除に必要なキーのリクエストを送信します。これはクラウドネットワーク経由、またはプライバシーサーバーと同じコンピューティングデバイス上にあるデータ主体のデバイスを通じて送信されます。
【０４８５】
[537]カヤックの例では、転送中のデータを保護するためにさまざまな追加手順を使用してデータを送信できますが、受信者のeコマースサイトでは、プライバシークライアントから最初に送信された身長、体重、予算という3つの情報をロック解除や関連付けのためにキーが必要になる場合があります。ステップ2で、一例では、プライバシーサーバーの認証モジュールはTDR受信者属性の組み合わせを、正しい受信者属性の組み合わせと比較して、TDR受信者が正しい受信者かどうかを判断します。プライバシーサーバーの認証モジュールが、TDR受信者属性の組み合わせが許可された受信者属性の組み合わせと一致することを確認した場合、ステップ3の一部としてプライバシークライアントを介して、1つの例ではTDRのロックを解除するために必要なキーをTDR受信者に送信します。
【０４８６】
[538]図8の2番目の例では、ステップ1で、要求された血圧情報を含む暗号化、トークン化、または削除されたTDRを受信した医師は、プライバシークライアントを介してプライバシーサーバーの認証モジュールにTDRを送信して、医師が要求された情報を表示する権限があります。ステップ2で、プライバシーサーバーの認証モジュールは、医師のTDR情報を、正しい受信者属性の組み合わせと比較して、医師が許可された受信者であるかどうかを判断します。プライバシーサーバーの認証モジュールが、医師のTDR情報が承認された受信者属性の組み合わせと一致することを確認した場合、プライバシーサーバーの認証モジュールは、暗号化、トークン化、あるいは一部省略された、血圧情報を含むTDRのセキュリティを解除するために必要なキーが医師に送信されます。
【０４８７】

[539]図10は、導入例で、匿名方式で関係者の関心を分析する例を示しています。ステップ1で、一例では、関係者（RP）は、モバイルやウェアラブルデバイス上のプライバシークライアントを介して販売者／サービスプロバイダーと共有する属性の組み合わせ（AC）を選択します。たとえば、eコマースサイトを利用するのではなく、関連当事者は物理的なスポーツ店な場所に行き、身長、体重、および予算に関する同じ情報をモバイルまたはウェアラブルデバイスを介して共有できます。

【０４８８】

[540]ステップ2で、一例では、プライバシーサーバーは、モバイル／ウェアラブル／ポータブルデバイスに常駐するプライバシークライアント上でTDRを形成するためにDDIDを属性の組み合わせに割り当てることができます。

【０４８９】

[541]ステップ3では、一例では、TDRは、モバイル／ウェアラブル／ポータブルデバイスに常駐するプライバシークライアントを介してマーチャント／サービスプロバイダの受信者に送信されます。kayAKsの例を上げると、ストアは、店舗内のデバイス、ビーコンなどを介して、データ主体のモバイル／ウェアラブル／ポータブルデバイスから3つの個別のTDR対応データ属性を受信できます。

【０４９０】

[542]ステップ4では、一例では、マーチャント／サービスプロバイダの受信者は、関係者により許可され、モバイル／ウェアラブル／ポータブルデバイスに常駐するプライバシークライアントにより商人／サービスプロバイダの受信者に送信される属性の組み合わせを見ることができる。たとえば、店舗では、顧客の身長、体重、予算を表示できます。

【０４９１】

[543]ステップ5では、一例では、マーチャント／サービスプロバイダの受信者は、データ主体や関係者が誰なのかをまだ知らなくても匿名でデータ主体や顧客に提案を行うことができる。

【０４９２】

[544]ステップ6では、一例では、データ主体や顧客は、客にピッタリの商品を見つけたというマーチャント／サービス提供者の受信者の申し出に応答することもできる。

【０４９３】

[545]本書で説明するシステムおよび方法は、通信ネットワークを利用しながら、データのより大きな匿名性とプライバシー／匿名性およびセキュリティの向上を達成する方法を関連当事者に提供することができます。これらのシステムや方法がなければ、ネットワークサービスやデータ主体のアクティビティに識別情報を関連付けたテクノロジープロバイダーを介した、ネットワーク上やネットワーク間の関連者のアクティビティに基づいて、第三者がデータ主体または関連当事者の真のアイデンティティを取得できる場合があります

【０４９４】

[546]ここでは、データセキュリティとデータプライバシー／匿名性を提供する他のさまざまな方法を開示します。一例には以下のような段階があります。コンピューティングデバイスで電子データ要素を受信し、電子データ要素のデータ属性を識別し、コンピューティングデバイスを介してDDIDを選択し、選択したDDIDをデータ属性に関連付け、選択された一意のDDIDとデータ属性からTDRを作成します。

【０４９５】

[547]一例では、データ要素を選択するステップは、一意のDDIDを生成するか、別の例では、DDIDとして機能する、動的に変化する値を受け入れたり変更したりします。一例では、この方法は、選択されたDDIDとデータ属性との間の関連付けを期限切れにすることも可能です。別の例では、選択された一意のDDIDが異なるデータ属性または属性の組み合わせに関連付けられていた期間に関する情報を、コンピューティングデバイスにアクセス可能なデータベースに格納するという方法もあります。別の実施形態では、この方法は、DDIDとデータ属性との間の関連付けの満了に続いて、選択された一意のDDIDをデータ属性と再度関連付けることもあります。一例では、DDIDの期限切れは所定の時間や、所定のイベン

トまたはアクティビティの完了後に設定されます。別の例では、TDRは、指定の期間中または所定の場所でのみ使用が許可されます。別の例では、データ属性に割り当てられた一意のDDIDを変更することを含むことができ、一意のDDIDは、ランダムまたはスケジュールベースに変更したり、または所定のアクティビティまたはイベントの完了後に変更したりするという方法があります。

【０４９６】

[548]ここでは、ネットワークを介したトランザクションを容易にする別の方法をお伝えします。ある例の流れを説明します。ネットワークを介してアクティビティを実施するために、クライアントデバイスからプライバシーサーバで要求を受信するステップがあります。データベース内の複数のデータ属性のうち、要求されたアクティビティを完了するために必要なものを決定し、 DDIDを作成します。 DDIDを決定されたデータ属性に関連付けて、結合されたTDRを作成します。要求されたアクティビティを実行または開始するために、結合されたTDRを少なくとも1つのネットワークデバイスからアクセス可能にします。実行されたアクティビティに関連する追加情報を含む変更されたTDRを受信します。変更されたTDRをメモリデータベースに保存します。別の方法の導入例として、電子情報の制御された配信を行う方法を説明します。この方法は、プライバシー制御モジュールでネットワークを介してアクティビティを実施する要求を受信します。要求を満たすために必要であると判断されたプライバシー制御モジュールにアクセス可能なデータベース内にあるデータ主体の属性を選択します。ここで必要でないと判断されたデータ主体の他の属性は選択されません。 DDIDを、プライバシー制御モジュールの抽象化モジュールを使用して、選択された属性とデータ主体に適用します。DDIDは、選択されていない属性を表示しません。一意のDDIDが割り当てられた時間を記録します。要求されたアクティビティが完了したら、一意のDDIDと決定された属性、およびプライバシー制御モジュールで適用されるデータ主体を受信します。属性は、実施されたアクティビティに関する情報を含むように変更されます。実施されたアクティビティが完了した時間を記録し、一意のDDIDと決定された属性、およびそれらが適用されるデータ主体がプライバシー制御モジュールで受信されます。

【０４９７】

[549]他には、選択された属性またはデータ主体の1つまたは複数に追加のDDIDを割り当てるという方法もあります。別の例で、記録された時間を使用して、一意のDDIDおよびデータ属性をデータ主体の真のアイデンティティに再関連付けする方法もあります。この方法では、一意のDDIDを他のデータ属性に再割り当てし、一意のDDIDが再割り当てされた時刻を記録します。

【０４９８】

[550]ここでは、データセキュリティを改善するための別の方法を説明します。この方法では、データ主体を何かしらの属性に関連付けます。 DDIDを少なくとも1つの属性に関連付けてTDRを作成します。 TDRは、データ主体の属性へのアクセスを、特定のアクションを実行するために必要な属性のみに制限します。また他の方法は、関連付けキー（AK）や置換キー（RK）をTDRに割り当てて、TDRへの許可されたアクセスにはAKやRKへのアクセスが必要になります。さらに別の方法では、DDIDと属性との間の関連付けを特定の時間や所定のイベントやアクティビティの完了後に期限切れにします。別の実施形態では、DDIDと属性との間の関連付けの満了後に、DDIDを異なる属性と再関連付けすることもできます。この方法では、DDIDが異なるデータ属性または属性の組み合わせに関連付けられていた期間に関する情報をデータベースに保存します。

【０４９９】

[551]TDRsを形成するためにDDIDs を異なるアトリビュートの組み合わせに連携させるには多様な方法が考えられる。DDIDs は特定の変化し得る長さを持ち、数、性質、真相または特性といった多様な構成コードから成され得る。一つの例として、メンテナンスモジュールによって管理され、異なった方法で解離したアトリビュートの組み合わせを再統合するために必要な、連携キー（AKs）または置き換えキー（RKs）に接続可能な、オーソ

ライズされた当事者のみが、どのアトリビュートの組み合わせがほかのアトリビュートの組み合わせ、Data Subjects、関連当事者、統合データプロファイルと正しく連携されるか決定する機能を持つ。しかしながら、サイトはリアルタイムでTDRs内に含まれるアトリビュートの組み合わせを追跡し、利用する可能性があり、そしてサイトは一時的に存在しており、関連したDDIDs は他の行動、活動、処理、特性、アトリビュートの組み合わせ、Data Subjectsや関連当事者に後で再利用され得ると理解される。

【０５００】

[552]送信されるアトリビュートの組み合わせには、単数もしくは複数の明示的なデータ、個人を特定する情報（PII）、行動に関連するデータ派生データ、リッチデータ、その他のデータの組み合わせが含まれている可能性がある。

【０５０１】

[553]例A

【０５０２】

[554]最初の例では、関連当事者がコントロールしている実態であり、相手方のアトリビュートの組み合わせがリリースされる指定先とオーソライズされるように構成されている。例Aは、3つの異なる業界における通信ネットワーク(“ CN ”s)の2つのサービスプロバイダー（“ SP ”s）が提供する4種類のオンラインセッションで動作する、関連当事者（当事者Xまたは“ RP X ”）によって生成される情報を、システムがどのように処理するのかを示している。図11から20はこの例を説明しており、本発明の具体化の一つの例として様々な段階と状況下で情報がどのように処理されるのかを示している。図11から20は一例としてのみの提示であり、本発明が図11から20の例示以外でも多様な方法で実行が可能であることが理解できる。

【０５０３】

[555]図11は関連する当事者Xがアトリビュートの組みあわせA（明示的データ）をパンドラ・ラジオ（“ SP1 ”）のようなウェブのサービスプロバイダーにオンラインのインターネット（“ コミュニケーション・ネットワーク1 ” または “ CN1 ”）を通じて送信する例示である。アトリビュートの組み合わせAは、プライバシーサーバー（“ PS ”）の抽象的モジュールによって、DDID 1の識別コードを割り当てられている（一時限定的）。識別コードはアトリビュートの組み合わせAと一体となって、CN1そしてセキュリティクライアントを介してSPIへ伝達される。図11では、DDID 1とアトリビュートの組み合わせAが、一時限定的に関連当事者Xの代わりにTDRを表象している。

【０５０４】

[556]図12はSP1と情報交換する際、関連当事者Xが、プライバシークライアントにアトリビュートの組み合わせA1として送信されSP1に探知される活動情報（行動に関連する情報）を生成したことを示しており、プライバシークライアントは、Data Subjectデバイス、サービスプロバイダーデバイスに内在するか、クラウドネットワークを介してアクセス可能または内在する、もしくはプライバシーサーバーへ遡りプライバシーサーバーと同じコンピューターデバイスに存在しうる。プライバシーサーバーのメンテンナンスモジュールは、アトリビュートの組み合わせと様々なDDIDコードについての情報を保持しており、各アトリビュートに関連づけられたCNとSP同様、コードは各アトリビュートの組み合わせに対し、時の経過と共に異なる時点で割り振られている。 図12では、DDID1の組み合わせ、アトリビュートの組み合わせA、アトリビュートの組み合わせA1が、一時限定的にDDID 1、アトリビュートの組み合わせA、アトリビュートの組み合わせA1の連携期間のみ当事者Xの代わりとしてTDR を表している。求められている行動、活動またはアトリビュートの組み合わせからの処理に関した新しいデータの連携を完了するにあたり、DDID 1は新しいTDR における使用のため再割り当てされうる。図13から20に示されたDDIDsとアトリビュートの組み合わせも、DDIDsとアトリビュートの組み合わせのが一時的に連携する期間のTDRs を表している。

【０５０５】

[557]図13は関連当事者Xが別のアトリビュートの組み合わせE（明示的データ）をパンド

ラ・ラジオ（“SP1”）へオンラインインターネット接続（“CN1”）を介して送信する例を示している。アトリビュートの組み合わせEは、プライバシーサーバー（“PS”）によって一時的に DDID 4の識別コードを割り振られており、識別コードはアトリビュートの組み合わせEと一体となって、CN1そしてセキュリティクライアントを介してSPIへ伝達される。

【０５０６】

[558]図14は、この例においてSP1と情報交換する際、関連当事者Xが、アトリビュートの組み合わせE1としてプライバシークライアントを介してプライバシーサーバーの抽象的モジュールへ遡って送信されSP1に探知される活動情報（行動に関連する情報）を生成したことを示しており、プライバシークライアントは、Data Subjectデバイス、サービスプロバイダーデバイスに内在するか、クラウドネットワークを介してアクセス可能または内在する、もしくはプライバシーサーバーと同じコンピューターデバイスに存在しうる。

【０５０７】

[559]図15は関連当事者Xがアトリビュートの組み合わせQ（明示的データ）を別のバージョンのSP1パンドラ・ラジオへモバイルアプリケーション形式で、モバイルデバイス通信（“コミュニケーション・ネットワーク2”または“CN2”）を介して送信する例を示している。アトリビュートの組み合わせQは、プライバシーサーバーによって一時的に DDID 9の識別コードを割り振られており、識別コードはアトリビュートの組み合わせQと一体となって、TDR としてCN2そしてセキュリティクライアントを介してSP1へ伝達される。

【０５０８】

[560]図16は、SP1と情報交換する際、関連当事者Xが、アトリビュートの組み合わせQ1としてプライバシークライアントを介してプライバシーサーバーの抽象的モジュールへ遡って送信されSP1に探知される活動情報（行動に関連する情報）を生成したことを示しており、プライバシークライアントは、Data Subjectデバイス、サービスプロバイダーデバイスに内在するか、クラウドネットワークを介してアクセス可能または内在する、もしくはプライバシーサーバーと同じコンピューターデバイスに存在しうる。

【０５０９】

[561]図17は関連当事者Xがアトリビュートの組み合わせP（明示的データ）をプライバシークライアントを介して送信する例を示しており、プライバシークライアントは、Data Subjectデバイス、サービスプロバイダーデバイスに内在するか、クラウドネットワークを介してアクセス可能または内在する、もしくはFitBitなどのウェアラブルデバイス通信（“コミュニケーション・ネットワーク3”または“CN3”）を介したエクササイズ活動に関連したモニタリングサービスを提供するサービスプロバイダー（“SP2”）に対してのプライバシープロバイダーとして、プライバシーサーバーと同じコンピューターデバイスに存在しうる。アトリビュートの組み合わせPはPSよって一時的に DDID 7の識別コードを割り振られており、識別コードはアトリビュートの組み合わせPと一体となって、TDR としてCN3そしてセキュリティクライアントを介してSP2へ伝達される。

【０５１０】

[562]図18はこの環境下でSP2と情報交換する際、SP2が関連当事者Xによって達成された、望ましい一日の消費カロリー（派生データ）のうちの割合を計算し、その情報がプライバシークライアントを介して信する例を示しており、プライバシークライアントは、Data Subjectデバイス、サービスプロバイダーデバイスに内在するか、クラウドネットワークを介してアクセス可能または内在する、もしくはアトリビュートの組み合わせP1 としてプライベートサーバーへ遡ってプライバシーサーバーと同じコンピューターデバイスに存在しうる。

【０５１１】

[563]図19はアトリビュートの組み合わせが各SPに接続可能でありプライバシークライアントを介して再送信される例を示しており、プライバシークライアントは、Data Subjectデバイス、サービスプロバイダーデバイスに内在するか、クラウドネットワークを介してアクセス可能または内在する、もしくはプライベートサーバーへ遡ってプライバシーサー

バーと同じコンピューターデバイスに存在しうる。図19はSP内またはSP間の利用セッションがセッションの間またはセッション中の小集団となりうることで、一例として、メンテナンスモジュールによって保持されるセキュリティ連携キーへのアクセスなしにSPがアトリビュートの組み合わせ間の連携を決定づけるために必要な情報を持たないことを強調している。しかし、一例として、SPは各一時的な期間中に作成された、変化するDDIDsによって決定されるアトリビュートの組み合わせへのアクセスを持っている。例えば、SP1はDDID 1 とDDID 9が双方とも、SP1に保持されているウェブサイトの2つの異なるバージョン、つまりオンラインインターネット接続とモバイルデバイス接続の2つによるアクセスを行った関連当事者Xに付随しているとは認識しない。

【０５１２】

[564]図20はSPへ送信、そしてSPから再伝達された全ての情報を含む、関連当事者Xにアクセス可能なデータの例を示している。図19は、メンテナンスモジュールによって保持されるセキュリティ連携キーへアクセスすることで、関連当事者Xがコントロールする実体として、一例を挙げると、集合体SPが集約と標準化の目的でアトリビュートの組み合わせ間の連携を決定づけるために必要な情報を持ちうることを強調している。加えて、関連当事者Xは使用するための情報を保持したり、またはデータファシリテータのための利用、分析と保護環境下でのデータ処理を実行するためのメンテナンスモジュールを保持する可能性がある。新しいアトリビュートの組み合わせZは、関連当事者Xが他のどんな音楽の選択を好むかが一日の望ましいカロリー消費量を達成することを補助するかを予測するためにDDID 1、 DDID 9、 DDID 4、DDID 7に関連する全てのデータを比較することで、メンテナンスモジュールによって関連当事者Xのリクエストに対して生成される新しいデータ（“リッチデータ”）を表している。アトリビュートの組み合わせZは、その他の多種のDDIDsと関連したデータ同様、この予想によって成された他の音楽の選択肢のリストを含む可能性がある。アトリビュートの組み合わせZは、コントロール実体として機能している関連当事者Xが要求するまで他の当事者（SP1、SP2 、その他）と通信を行うことはない。関連当事者Xがアトリビュートの組み合わせZと共有を要求すると、一例としては、関連当事者Xによって指定された受容者へ伝達されるに先立ってDDID コードを割り当てられる。この新しいアトリビュートの組み合わせは、関連当事者Xにより決定された受容実体へ割り当てられると、より全体的で流動的になる。

【０５１３】

[565]例B

【０５１４】

[566]図21-22に示された二つ目の例では、サービスプロバイダー（“SP3”）が、SP3 に関連したアトリビュートの組み合わせがリリースされる先の当事者を決定するようオーソライズされたコントロール実体システムとなるようシステムが構成された例を示している。SP3はクライアントの特定性とプライバシー、匿名性の保護を向上するためシステムを使用する可能性がある。これは潜在的にプライバシーや匿名性が失われること、また市場への浸透、SP3 の提供と利用が増大することの結果として、消費者や自治体の反発の可能性を削減することも含まれている。図21から22は一例としてのみの提示であり、本発明が図21から22の例示以外でも多様な方法で実行が可能であることが理解できる。

【０５１５】

[567]図21と22は、ウェブサイト会社などその他の情報をキャプチャすることを手助けするインプット技術提供者（“ITV”）、オンライン電子決済処理などのプロセス技術提供者（”PTV”）、そして電子的に選択された製品を消費者へ届けるアウトプット技術提供者(“OTV”)のそれぞれへ、各々が割り当てられたサービス提供に必要なアトリビュートの組み合わせのみをSP3 が提供することの例示である。どの提供者もSP3 クライアントの特定性を開示する個人特定情報（“PII”）へのアクセスはできない。

【０５１６】

[568]図23はインターネットの行動に関係した広告配信における、ダイナミックに形成された、変更可能、再割り当て可能なDDIDs の履行例を示している。現在の発明のいくつか

の実施による利点なしでは、元々インターネットの行動に関係した広告配信は広告ネットワークに基づいており、クッキーをユーザーのウェブブラウザに配置し、同じ広告ネットワークの広告を載せているウェブサイトの訪問者を追跡することでプロファイルを構築している。

【０５１７】

[569]典型的に、ユーザーが図23のウェブサイト（“Website1”）を始めて訪問すると、前述のウェブサイトは（i）コンテンツをウェブサイトからユーザーのブラウザに届ける（ii）クッキーをユーザーのブラウザへ送信する（iii）広告コンテンツを広告ネットワーク（“広告ネットワーク1”）からウェブサイト上で作動させるため、ユーザーのブラウザからウェブアドレスへダイレクトする。上述（ii）で送信されたクッキーは、ユーザーに選択されたウェブサイトに連携していることから“ファーストパーティー・クッキー”と言われる。ファーストパーティー・クッキーは、ログイン状況、買い物かごの商品やその他ユーザーの体験を向上させる関連情報といった“ステータス”の情報を保つ手助けをするためユーザーにとっても利点になり得る。上記の（iii）の一部分にて、ユーザーのブラウザが広告ネットワーク1から広告情報を要求すると、広告ネットワーク1は広告をユーザーのブラウザへ送付し、ウェブサイト1の一部として表示される。過去にユーザーのブラウザが広告コンテンツを広告ネットワーク1へ要求したことがない場合、広告ネットワーク1はクッキーも送付する。このクッキーは、ユーザーが意図して訪問したウェブページから送付されたものではないためサードパーティー・クッキーと呼ばれる。広告ネットワーク1が過去にユーザーを追跡したことがない場合、広告ネットワーク1は従来型の広告配信技術に基づいた広告として機能する。（例：ウェブサイト1のコンテンツの性質が送信される）ユーザーが繰り返し広告ネットワーク1の広告を載せたウェブサイトを訪れると、広告ネットワーク1（広告ネットワーク1からユーザーのブラウザへ送信されたサードパーティー・クッキーを経由して）は訪問したページ、各ページでの滞在時間、ユーザーのSNSやオンライン・オフライン購買行動などその他の不定要素に基づいてそのユーザーの行動関連データのプロファイルを構築する。広告ネットワーク1の動作またはサードパーティーのデータプロバイダから取得し統合された情報から収集されたユーザー情報と心理学と人口統計学をあわせている。広告ネットワーク1によって生成され管理されるユーザーのプロファイルに基づいて、広告ネットワーク1は、そのユーザーが最も関心を示すと決定づけた内容に応じてそのユーザーをターゲットとした広告を表示することができる。

【０５１８】

[570]この慣例的なサードパーティー広告ネットワークによるサイト間、ページ間のユーザー追跡は、プライバシー・匿名性の問題を提起している。これに応じて、組員の団体、常勤職員、公共活動が一体となってウェブの標準化を図る国際的団体であるワールド・ワイド・ウェブ・コンソーシアム（W3C）を中心に、分野を超えた規制者、市民組織、営利団体による採択に向けて、トラッキング拒否機能（DNT）の取り組みが開始された。主要なブラウザ（例：インターネットエクスプローラー、クローム、ファイアフォックス、サファリ）は現在DNTを選択できる設定を設けているが、どのように受容側のウェブサイトがDNTに対応するかという協定はなされていない。

【０５１９】

[571]それにも拘らず、プロバイダはDNTが、ファーストパーティー・ウェブサイトではなく、サードパーティー・ウェブサイトの追跡に適用されるということを認識している。W3C標準の草案では、ファーストパーティーがDNT：1のシグナルを受け取った場合、ファーストパーティーは通常の情報収集とデータ利用を行う。これはファーストパーティーエクスピリエンスの文脈で、コンテンツ、サービス、広告のカスタマイズが可能ということである。推奨下では、ファーストパーティーはネットワークの相互関係データを自身でデータ収集ができなかったサードパーティーと共有するべきでないとされている。しかしながら、処理データはファーストパーティーの下に動作しているプロバイダに共有されている可能性がある。

【０５２０】

[572]トラッキング拒否環境では、ユーザーがウェブサイト（“ウェブサイト1”）を方も運すると、ユーザーのブラウザはウェブサイト1へユーザーが追跡を望まないという通知を送信する。そしてウェブサイト1はユーザーのブラウザへファーストパーティー・クッキーとコンテンツ、ブラウザがウェブサイト1上の広告を広告ネットワーク1（“広告ネットワーク1”）から表示するようリクエストするアドレスを送信する。広告ネットワーク1はそのリクエストを追跡しないものとして受け取り、広告コンテンツをユーザーのブラウザへ送信するが、サードパーティー・クッキーはユーザーのブラウザへ配置されない。広告は従来型のターゲティング方法でユーザーへ提供され、ページのコンテンツに対しての広告などを含むがそれだけに限定されない。（例：コンテンツターゲティング）トラッキング拒否機能がどのように実行されるかによって、上述のように、ファーストパーティーに関しては、コンセンサスによる制限はほとんどなされていない。（ファーストパーティーがDNTユーザーのネットワーク相互関係をデータを自身で収集することが出来なかったサードパーティーと共有すべきでないという点を除く）

【０５２１】

[573]対照的に、本発明を実施した場合、インターネットの元来の収益モデルを維持するためにコンテンツとターゲティングした広告を届ける一方で、関連当事者のユーザーのプライバシー、匿名性を保護するためにトラッキング拒否機能を実行することが可能である。図23は広告配信における本発明の潜在的な活用の数を示している。

【０５２２】

[574]図23のステップ1では、例として、Data Subject または関連当事者がウェブサイト1を始めて訪問し、ブラウザがトラッキング拒否ヘッダーをウェブサイト1へ送信している。Data Subject または関連当事者が望めば、ブラウザはTDR をウェブサイト1へ送信することが可能で、このようにして“ステータス”情報を隠すことができ、Data Subject または関連当事者の体験を向上させることが出来る。ウェブサイト1はData Subject または関連当事者のブラウザへコンテンツを送信する。

【０５２３】

[575]ステップ2では、例として、Data Subject または関連当事者のブラウザが広告ネットワーク1（TDRの有無を問わず）からの広告をウェブサイト1へ要求している。TDR が送信されないときは、Data Subject または関連当事者のブラウザは広告ネットワーク1からページのコンテンツに基づいた従来型のターゲット広告を受信する。TDR が送信されるときは、広告ネットワーク1はData Subject または関連当事者に関連性のある内容に基づいた高次元のターゲティング広告をData Subject または関連当事者のブラウザに送信することができる。この点において、広告ネットワーク1によるTDRに基づいた広告は、従来型の広告やData Subject または関連当事者から広告ネットワーク1が収集した行動に関係するプロファイル情報を集約したもの（そのため一般的にはより推論的である）よりも、よりData Subject または関連当事者に関連性の高いものとなる。

【０５２４】

[576]ステップ3で、例として、Data Subject または関連当事者が新たなウェブサイト（“ウェブサイトN”）を訪問するときにステップ1、2と類似の処理が発生する。TDR が含まれてる場合はウェブサイトのコンテンツと広告コンテンツは高次元でターゲティングされている。しかし、少なくとも広告ネットワーク1はData Subject または関連当事者から情報を収集したり、追跡することはできない。さらに、ブラウザ内のプライバシークライアントまたはその他のメカニズムを通して、TDR はウェブサイトあるいは広告ネットワーク1に送信された情報を保持している可能性がある。

【０５２５】

[577]まとめると、既存のターゲティング広告技術では、ユーザーはオンライン上のどこからでも追跡されうるし、特定のユーザーの嗜好に対しての推測を立て集約したデータを基に広告表示が成される。つまりユーザーのプライバシー、匿名性はなく、低・中程度の広告関連性しかないということである。本発明とトラッキング拒否機能の要素を合わせることで、どのウェブサイト、広告ネットワークにどのような情報を送信するかユーザーが

選択することを可能にする。これによりプライバシー、匿名性だけではなく広告の関連性（ユーザーにとっての）を増強すると同時に、売り手にとっての実販売量と投資還元を向上させる。

【０５２６】

[578]図24と25は、ヘルスケア領域における本発明の実施例の潜在的な利点を示している。図24はヘルスケアの情報システムにおいて個人特定情報（PII）、個人保険情報（PHI）といった、ユーザー、患者の機密性やプライバシー、匿名性を保護する本発明のひとつの実行例として、一時的なユニークで目的限定的なデータ表現（TDRs）が利用されるかを強調している。本発明を活用することで、ヘルスケアシステムは機密性のあるPII、PHIを明らかにしないリアルタイムのTDRs を、それらの情報のコンテクストやアクセスを失わずに生成することができる。ステップ1.0では、情報は登録のプロセスに関係したPII、PHIを含むインプットとしてシステムに受け取られる。PII、PHI情報のプライバシー、匿名性を 保護するため、登録のプロセスのアウトプットは、PII、PHIの情報を明らかにすることなくPII、PHIのユーザー情報[A]はTDRs （動的に変化し再割り当て可能なDDIDsとPII、PHI情報から構成される）に置き換えられ、そのため機密性のあるPII、PHIデータが開示されることはない。このユーザーデータ（PII、PHI情報の代わりのTDRsを含む）は、PII、PHI情報[B]を開示することなく、D1でユーザーデータファイルを生成、増大または代替するためのインプットとして使用される。同様に、ステップ2.0の予約プロセスからアウトプットされたPII、PHI情報は、PII、PHIの情報を明らかにすることなく TDRs（動的に変化し再割り当て可能なDDIDsとPII、PHI情報から構成される）に置き換えられ、そのため機密性のあるPII、PHIデータが開示されることはない。この医療データ（PII、PHI情報の代わりのTDRsを含む）は PII、PHI情報[C]を開示することなく、D2で医療データファイルを生成、増大または代替するためのインプットとして使用される。D2 からの医療データ（ステップ3.0の医療情報検索プロセスを経た後）は、ユーザープロファイル検索のステップ4.0で、インプットとしてD1からのユーザーデータファイルと結合される。このとき一時的なユニークで目的限定的なデータ表現（TDRs）のみを接続し使用することによって、PII、PHI情報は開示されることがない。ステップ4.0のユーザープロファイル検索で生じるアウトプットの要素を構成するPII、PHIユーザー情報は、PII、PHI情報を開示することなく、TDRs （動的に変化し再割り当て可能なDDIDsとPII、PHI情報から構成される）に置き換えられ、そのため機密性のあるPII、PHIデータが開示されることはない。最後に、D1おいて、ユーザーデータ（PII、PHI情報の代わりのTDRsを含む）予約記録ブラウズ処理のステップ5.0で、インプットとして使用される。このとき一時的なユニークで目的限定的なデータ表現（TDRs）のみを接続し使用することによって、PII、PHI情報は開示されることがない。オーソライズされたヘルスケアまたは不随サービスでの目的で、ユーザーデータファイル、医療データファイルからの詳細情報へのアクセスが要求されるときは、適用可能なTDRs and DDIDsに関連した機密性のあるPII、PHIデータを識別するために、関連キー(AKs) と置き換えキー(RKs) が使用される。

【０５２７】

[579]図25は動的変化があり再割り当て可能なTDRs （動的に変化し再割り当て可能なDDIDsとPII、PHI情報から構成される）が、患者の医療記録に含まれるPII、PHIのプライバシー、匿名性を保護するために使用される例を示している。図25は本発明を複数レベルの抽象性を伴い実施する様子を示しており、望まれるサービスや許可された機能を提供するために必要な個人特定情報のレベルでのみ“プライバシーの輪”が供給されることが示されている。この例では、地方自治体、国家レベルでの各プロバイダは各々の許容された目的に適した関連する組み合わせを受け取る。一時的なユニークで目的限定的なデータ表現（TDRs）はユーザー、患者の個人特定情報（PII）、個人保険情報（PHI）の気密性、プライバシー、匿名性を保護するために使用されうる。本発明を活用することで、ヘルスケア関連情報は機密性のあるPII、PHIを明らかにしないTDRs を使用することができ、かつそれらの情報のコンテクストやアクセスを失うこともない。それぞれの連続したレベル（下層のプロバイダレベルから始まり上層の国家レベルまで）にてPII、PHI情報から TDRs

（動的に変化し再割り当て可能なDDIDsとPII、PHI情報から構成される）に置き換えられた情報を受け取るが、一時的なユニークで目的限定的なデータ表現（TDRs）に代理されるためPII、PHI情報は開示されることがない。特定の段階で、オーソライズされた使用目的でPII、PHI情報へのアクセスが要求されるときは、適用可能なTDRs and DDIDsに関連した機密性のあるPII、PHIデータを識別するために、関連キー(AKs) と置き換えキー(RKs) が使用される。加えて、DDIDs は時間の経過とともに変化し、また新しいDDIDsに紐づいた情報は、Data Subjectまたは患者の特定性を開示することなく追加情報を反映させることが可能なため、DDIDsは水平の学習を向上するために自己規制を補助することができる。これは、分析を実施するために必要なデータから“コンテクスト”や“メタ”を切り離すためにDDIDs を使用することで可能となる。ヘルスケア領域には複数のプレーヤーが存在し、多くは異なるデータ構成を使用している。Dynamic Anonymity は、DDIDsを動的に割り当て、再割り当て、追跡することで、特定情報を開示することなく、効果的な調査と分析を可能にし、異なるソースからの異なるフォーマットの異種データを収集し、情報を共通の構成に標準化し、“コンテクスト”や“メタ”を切り離す補助をする。この方法論を用いると、このプロセスから個人を特定することは不可能であるため、合意を得ることを思慮することなく、異なるソースからのData Subjectまたは患者についての単体のデータを繋げることが可能になる。図1C-1に示された信用の円（“CoT”）の内部に限って、個人特定情報は、情報を個人と関連づけるマッピングエンジンへのアクセスによってアクセス可能である。適切に管理、規制することで、信用のおける当事者、プロキシは、個人特定情報と機能性情報の間の差分を一致させるため、信用の円（“CoT”）を介してコントロールをオファーできる。例えば、現在のヘルスケア、ライフサイエンスリサーチ領域では、個人が再特定されてしまうリスクをから、最小限の個人特定情報のみ調査に使用されると保証するために“データの最小化”の試みがなされている。 Dynamic Anonymity は、法強化のための規制による負担、プライバシー、匿名性に付随するレビューや開発のための企業負担を相当に軽減できる。同時に、ヘルスケア関連の調査、開発においてより完結したデータセットの入手を可能にする。HIPAA は個人保険情報（PHI）を匿名化するために4番目の方法論を用いている。PHIは匿名化されると、HIPAA の制約下に置かれずあらゆる目的において使用可能になる。しかし、既存のHIPAA匿名化の方法論には、懸念点があり、オーソライズさていない匿名データの再特定化が法的信用性に欠けること、匿名データの使用における公的な透明性が十分でないことが挙げられる。さらに、2014年9月22日付けで有効化された米国HIPAA 、HITECH法の最終規則によって、適用主体に加えて事業提携者も直接的にHIPAA のコンプライアンスの責任を負うこととなった。本発明は、情報の価値を損なうことなく、HIPAAの対象となる情報の匿名性を確保する手段を提供する。本発明を活用することで、ほとんどのデータをHIPAA コンプライアンスを遵守したものとすることができる。

【０５２８】

[580]図26は本発明のモバイル、ウェアラブル、ポータブルデバイス通信における本発明の実施例の潜在的な利点を示している。ここに示される、モバイル、ウェアラブル、ポータブルのシステム実行アプリケーションは、位置と時間によって左右されるアプリケーションのタイミングと参画レベルを管理しているコントロール実体を提供しうる。コントロール実体は、アトリビュートの組み合わせがサードパーティーに共有される度合いをコントロールするため、プライバシーサーバーの抽象的なモジュールの性能を用いることがあり、そうすることで匿名または個人特定的である度合いが図られる。例えば、既存システムのモバイル、ウェアラブル、ポータブルデバイスに関連した静的な識別子は、モバイル、ウェアラブル、ポータブルデバイスの使用に付属するアトリビュートの組み合わせデータを、モバイル、ウェアラブル、ポータブルプリケーションプロバイダとその他のサードパーティーが集約することを可能にする。本発明の活用することで、アプリケーションプロバイダとその他のサードパーティーが、モバイル、ウェアラブル、ポータブルデバイスの使用に付属するアトリビュートの組み合わせを集約することを防ぎうる。さらに、静的な識別子ではなくTDRs や DDIDsを利用することで、モバイル、ウェアラブル、ポータブ

ルデバイスやユーザーを特定することなく、モバイル、ウェアラブル、ポータブルデバイスが、地理的情報（例：道案内や地図のアプリケーション）を必要とするモバイルアプリケーションを使うことも可能にしうる。

【０５２９】

[581]図27は、ここで述べられる一つ以上のプロセス、方法、ステップ、特徴または要素の実行に従ってプログラマブルデバイス2700を描写している簡素化されたファンクション・ブロック・ダイアグラムの例である。プログラマブルデバイス2700は一つ以上の電気回路通信2710、メモリ2720、ストレージデバイス2730、プロセッサー2740、コントロール主体インターフェース2750、ディスプレイ2760そして通信バス2770を含み得る。プロセッサー2740は、適切な、プログラマブル・コントロール・デバイスまたはその他のプロセシングユニットであり、プログラマブルデバイス2700によって実行される多くの機能のオペレーションを管理すると考えられる。プロセッサー2740はディスプレイ2760を表示し、コントロール主体のインプットをコントロール主体インターフェース2750から受信すると考えられる。埋め込まれたプロセッサーは、本発明による技術を実行するために活用されうる、多目的で安定したプログラマブル・コントロール・デバイスを提供する。

【０５３０】

[582]ストレージデバイス2730はアトリビュートの組み合わせ、ソフトウェア（例：デバイス2700上の様々な機能の実行のため）、選択情報、デバイスのプロファイル情報、その他の適当なデータを格納し得る。ストレージデバイス2730は、ハードドライブやソリッドステートメモリ、ROMなどの永久メモリ、RAMなどの半永久メモリまたはキャッシュなど、有形に記録されるデータとプログラム指示用の、一つ以上の記録媒体を保持していると考えらえる。プログラム指示は、好ましいコンピュータ・プログラミング言語でコード化されたソフトウェアの実行で構成され得る。

【０５３１】

[583]メモリ2720は、デバイスの機能を実行するために使用される一つ以上の異なる種類の記録モジュールを含む。例えば、メモリ2720は、キャッシュ、ROM、そしてRAMを包括する。通信バス2770は、少なくともメモリ2720、ストレージデバイス2730、プロセッサー2740の相互間でのデータの転送のためのデータ転送経路を提供する。

【０５３２】

[584]バスとして言及しているが、通信バス2770は特定のデータ転送技術に限定されない。コントロール主体インターフェース2750はコントロール主体とプログラマブルデバイス2700との通信を可能にする。例えば、コントロール主体インターフェース2750は、ボタン、キーパッド、ダイアル、クリックホイール、マウス、タッチスクリーンやボイスコマンドスクリーン、その他の出力形式やユーザーインターフェースなど、様々な形態をとることが出来る。

【０５３３】

[585]ひとつの実施例として、プログラマブルデバイス2700は、データ処理可能なプログラマブルデバイスにもなり得る。例えば、プログラマブルデバイス2600は、センサーと通信かつ埋め込み可能な、識別可能なデバイス（スマートフォン、タブレット、ノートブック、デスクトップコンピュータを除く）や、識別デバイスや機械読み取り可能なデバイス（“スマートデバイス”）、スマートフォン、タブレット、ノートブック、デスクトップコンピュータ、その他個人に所属するデバイスとなり得る。

【０５３４】

[586]図28は、図27は、ここで述べられる一つ以上のプロセス、方法、ステップ、特徴または要素の実行に従ってネットワークデバイスシステム2800を描写したブロック・ダイアグラムの例である。前述のプライバシークライアントは、例えば、スマートデバイス（例：ウェアラブル、可動式、固定式のスマートデバイス）2810、スマートフォン2820、タブレット2830、ノートブック2840、デスクトップコンピュータ2850上で履行され得る。これらの各デバイスは一つ以上のネットワーク2860によってプライバシーサーバー2

870と接続しており、タイムキー（TKs）あるいは連携キー（AKs）、置き換えキー（RKs）そしてそれらに関連する情報によってアトリビュートの組み合わせについての情報、TDRs, Data Subjects, 集約された Data Subject プロファイル、タイムスタンプを格納するためにデータベース2880と連結される。データベース2880は系統立てられたデータベース、系統立てられていないフラットファイルを含む何らかの好ましい形式の記録データである。プライバシーサーバー2870も、アトリビュートの組み合わせについての情報、TDRs, Data Subjects, 集約された Data Subject プロファイル、タイムスタンプのためのリモートストレージを提供しており、それは、タイムキー（TKs）あるいは連携キー（AKs）、置き換えキー（RKs）そして、それらに関連しており、デバイス2810、2820、2830、2840、2850、またデータベース2880上か他のデータベース（図に示されていない）内の適当なデバイス上にあるプライバシークライアントに送信されている情報によって為されている。

【０５３５】

[587]図28には単体ネットワーク2860が示されているが、ネットワーク2860は複数の相互接続ネットワークにもなり得、プライバシーサーバー2870はデバイス2810、2820、2830、2840、2850上のプライバシークライアントに、または他のネットワーク2860を介してその他の適当なデバイス上にあるプライバシークライアントに接続される。ネットワーク2860は、ローカルエリアのものから広域あるいはグローバルインターネットまで、どんなタイプのネットワークにもなり得る。

【０５３６】

[588]本発明を実施することで、プライバシーとセキュリティのアプリケーションを様々な産業、環境、技術に限らず、オンライン処理やヘルスケア、教育、カード支払やその処理、情報セキュリティ、輸送、サプライチェーンマネジメント、製造供給源のプランニング、位置情報、モバイルまたはセルラーシステム、エネルギーやスマートグリッド技術、インターネット、防衛や知能技術またはプログラムにおいても提供することが可能である。

【０５３７】

[589]オンライン処理環境での使用された場合、本発明の実施は消費者に自身のデータの収集をコントロールすることを可能にし、データの管理者に、データ通信と拡散に関与するサードパーティーが特定の機能を提供するために必要な情報のみを受け取るようにさせることが可能である。結果として増加する消費者の確信は“モノのインターネット”の有益性に対する満足度を継続させ、また前述の通り、対象や関連する当事者の権利を破棄することなく、かつ事業者を規制下に留めておくことができる。

【０５３８】

[590]ヘルスケア領域では、本発明の実施例は、匿名性を向上させることで既存のヘルスケアの法規の有効性を保つことが可能である。さらに、本発明の実施例は、データの機密性保護の増加に由来する、調査に対して患者が懸念を持つ可能性を改善することで、消費者個人と社会が一体となってヘルスケアのビッグデータ分析の有益性を享受できる。

【０５３９】

[591]別の例示として、教育の場で使用された場合、本発明の実施例は、教育者と管理者に生徒に関連した分類データにアクセスできるツールを提供し、生徒のプライバシーや匿名性の権利を侵害することなく、個人としての生徒と、集合体としての学校のシステムがより高度なデータ分析の恩恵を受けることが可能になる。

【０５４０】

[592]国家セキュリティの設定においての本発明の実施例としては、政府の国家セキュリティ組織が、各電気通信ユーザーによって集約された限定的な通話の記録を、個人を特定可能な情報を得ることなく分析することができる。例えば、発信時間、‘発信’’受信’番号、通話時間、‘発信’’受信’の郵便番号は、発信または受信した電話番号、それに紐づく個人情報を開示することなく入手することが可能である。この例では、セキュリティ組織は限定的な通話記録を分析することで、不審な行動が見られた場合に、追加の詳細な通話記録を

得るためにどの時点で証明書やそのほかの司法承認を発行するか判断することができる。このようにして、本発明の実施例は国家セキュリティの権益にも有効であり、同時に司法判断が追加の詳細開示を求めるまで通話者のプライバシー、匿名性は確保することができる。

【０５４１】

[593]例

【０５４２】

[594]以下の例はさらなる実施例に関連した記述である。 例1はシステムで、次の構成を含む。ネットワーク経由でデータを送信する通信インターフェース、コンピュータプログラムコードを持つ内臓メモリー、そしてメモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上のプロセスユニットである。そのプログラムコードによって、一つ以上のプロセスユニットは動的に変化する一時的なユニーク識別子を生成し、ファーストクライアントから生成された、最初のデータ対象に関連する特定情報のための最初のリクエストをネットワーク上で受信し、最初に生成された識別子が最初のデータ対象を特定するために使用される間の、最初の時間単位を定義する情報で構成される最初の時間単位のデータを生成し、メモリに最初に生成された識別子と最初の時間単位のデータを保存し、そして最初に生成された識別子をネットワークを通してファーストクライアントへ送信する。

【０５４３】

[595]例2は例1の主題を包括しており、コンピュータプログラムコード指示により、一つ以上のプロセスユニットに、一つ以上のデータアトリビュートを最初に生成された識別子と関連させる。

【０５４４】

[596]例3は例2の主題を包括しており、ここでは、最初に生成された識別子と紐づいた一つ以上のデータアトリビュートのうち、少なくとも一つが、動作、処理、目的、最初のデータ対象の特性に関係している。

【０５４５】

[597]例4は例3の主題を包括しており、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが以下の動作を行う。最初の時間単位の間に、最初に生成された識別子と紐づいた一つ以上のデータアトリビュートのうち、少なくとも一つのための二番目のリクエストをネットワーク上でセカンドクライアントから受信し、二番目のリクエストをオーソライズし、最初の時間帯の間に最初に生成された識別子に関連している、要求された一つ以上のデータアトリビュートをセカンドクライアントが決定づける権利をネットワーク上で付与する。

【０５４６】

[598]例5は例1の主題を包括しており、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初または第二の時間帯の間に、一つ以上のデータアトリビュートを第二のデータ主題と関連させる。

【０５４７】

[599]例6は、例の主題を包括しており、ここではコンピュータプログラムコードの指示により、一つ以上のプロセスユニットが以下の動作を行う。最初のリクエストに応じて、最初のデータ主題を伴う二番目に生成された識別子と連携し、二番目に生成される識別子が最初のデータ主題を定義するために使用されている間に、第二の時間帯を定義する情報を含む第二の時間単位データで構成される第二の時間単位データを作成し、メモリに二番目に生成された識別子と第二の時間単位のデータを保存し、そして第二に生成された識別子をネットワークを通してファーストクライアントへ送信する。

【０５４８】

[600]例7は例6の主題を包括しており、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが一つ以上のデータアトリビュートと第二に生成された識別子を連携し、そこでは二番目に生成された識別子と紐づいた一つ以上のデータアトリビュー

トのうち、少なくとも一つが、動作、処理、目的、最初のデータ対象の特性に関係している。

【０５４９】

[601]例8は例7の主題を包括しており、最初に生成された識別子に関連した一つ以上のデータアトリビュートのうち少なくとも一つは、第二に生成された識別子に関連した一つ以上のデータアトリビュートのうちの少なくとも一つと異なっている。

【０５５０】

[602]例9は例3の主題を包括しており、コンピュータプログラムコードの指示により、第二の時間帯の間に、一つ以上のプロセスユニットが、最初に生成された識別子を二番目のデータ主題と関連させ、ここでは最初の時間帯に最初に生成された識別子に関連した一つ以上のデータアトリビュートのうち、少なくとも一つが、第二の時間帯で最初に生成された識別子に関連づけられた一つ以上のデータアトリビュートのうちの少なくとも一つと同様である。

【０５５１】

[603]例10は例1の主題を包括しており、コンピュータプログラムコードの指示によって一つ以上のプロセスユニットが以下の動作を行う。二番目のデータ主題と関連した二番目の識別子をネットワーク上でセカンドクライアントから受信し、二番目の識別子を二番目のデータ主題と連携させ、二番目の識別子が二番目のデータ主題を定義するために使用されている間に、第二の時間帯を定義する情報を含む第二の時間単位データで構成される第二の時間単位データを作成し、メモリに第二の識別子と第二の時間単位のデータを保存する。

【０５５２】

[604]例11は例4の主題を包括しており、コンピュータプログラムコードにより、一つ以上のプロセスユニットが、要求された第二の時間帯に最初に生成された識別子と連携した一つ以上のデータアトリビュートをセカンドクラアントが決定づける権利を、ネットワーク上で取り消す。

【０５５３】

[605]例12は、コンピューターで実行可能な格納された指示で構成される、恒久的なコンピューター判読可能な媒体で、ここでは一つ以上のプロセスユニットが以下の動作を行う。動的に変化する一時的なユニーク識別子を生成し、ファーストクライアントから、最初のデータ対象に関連する生成された識別子のための最初のリクエストをネットワーク上で受信し、最初のリクエストに応じて、最初のデータ主題を伴う最初に生成された識別子と連携し、最初に生成される特定識別子が最初のデータ主題を定義するために使用されている間に、最初の時間帯を定義する情報を含む最初の時間単位データで構成される最初の時間単位データを作成し、メモリに最初に生成された識別子と最初の時間単位のデータを保存し、そして最初に生成された識別子をネットワークを通してファーストクライアントへ送信する。

【０５５４】

[606]例13は例12の主題を包括しており、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、一つ以上のデータアトリビュートを最初の識別子と関連させる。

【０５５５】

[607]例14は例13の主題を包括しており、最初の識別子と紐づいた一つ以上のデータアトリビュートのうち、少なくとも一つが、動作、処理、目的、最初のデータ対象の特性に関係している。

【０５５６】

[608]例15は例14の主題を包括しており、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが以下の動作を行う。最初の時間単位の間に、最初に生成された識別子と紐づいた一つ以上のデータアトリビュートのうち、少なくとも一つのための二番目のリクエストをネットワーク上でセカンドクライアントから受信し、二番目のリク

エストをオーソライズし、最初の時間帯の間に最初に生成された識別子に関連している、要求された一つ以上のデータアトリビュートをセカンドクライアントが決定づける権利をネットワーク上で付与する。

【０５５７】

[609]例16は例12の主題を包括しており、コンピュータプログラムコードの指示により、第二の時間帯に、一つ以上のプロセスユニットが最初に生成された識別子を第二のデータ主題と関連付ける。

【０５５８】

[610]例17は例12の主題を包括しており、コンピュータプログラムコードの指示により、最初の時間帯に、一つ以上のプロセスユニットが最初に生成された識別子を第二のデータ主題と関連付ける。

【０５５９】

[611]例18は例12の主題を包括しており、ここではコンピュータプログラムコードの指示により、一つ以上のプロセスユニットが以下の動作を行う。最初のリクエストに応じて、最初のデータ主題を伴う二番目に生成された識別子と連携し、二番目に生成される識別子が最初のデータ主題を定義するために使用されている間に、第二の時間帯を定義する情報を含む第二の時間単位データで構成される第二の時間単位データを作成し、メモリに二番目に生成された識別子と第二の時間単位のデータを保存し、そして第二に生成された識別子をネットワークを通してファーストクライアントへ送信する。

【０５６０】

[612]例19は例18の主題を包括しており、ここでは最初の時間帯と第二の時間帯は重複しない。

【０５６１】

[613]例20は例18の主題を包括しており、ここでは最初の時間帯と第二の時間帯は一部重複する。

【０５６２】

[614]例21は例18の主題を包括しており、こではコンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、一つ以上のデータアトリビュートを第二の識別子と関連させ、そこでは第二の識別子と関連した一つ以上のデータアトリビュートのうち少なくとも一つが、動作、処理、目的、最初のデータ対象の特性に関係している。

【０５６３】

[615]例22は例21の主題を包括しており、　最初に生成された識別子に関連した一つ以上のデータアトリビュートのうち少なくとも一つは、第二に生成された識別子に関連した一つ以上のデータアトリビュートのうちの少なくとも一つと異なっている。

【０５６４】

[616]例23は例14の主題を包括しており、こではコンピュータプログラムコードの指示により、第二の時間帯に、一つ以上のプロセスユニットが、最初に生成された識別子を第二のデータ主題と関連させ、そこでは、最初の時間帯に最初に生成された識別子に関連した一つ以上のデータアトリビュートのうち少なくとも一つは、第二の時間帯に最初に生成された識別子に関連した一つ以上のデータアトリビュートのうちの少なくとも一つと同様である。

【０５６５】

[617]例24は例12の主題を包括しており、コンピュータプログラムコードの指示によって一つ以上のプロセスユニットが以下の動作を行う。二番目のデータ主題と関連した二番目の識別子をネットワーク上でセカンドクライアントから受信し、二番目の識別子を二番目のデータ主題と連携させ、二番目の識別子が二番目のデータ主題を定義するために使用されている間に、第二の時間帯を定義する情報を含む第二の時間単位データで構成される第二の時間単位データを作成し、メモリに第二の識別子と第二の時間単位のデータを保存する。

【０５６６】

[618]例25は例24の主題を包括しており、二番目の識別子がHTTクッキーを包括している。

【０５６７】

[619]例26は例12の主題を包括しており、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが以下の動作を行う。最初の時間帯に最初に生成された識別子と関連した最初のデータ主題の識別のため、二番目のリクエストをネットワーク上でセカンドクライアントから受信し、二番目のリクエストがオーソライズされることを決定し、セカンドクライアントが、最初の時間帯の間に最初のデータ主題の識別を決定づける権利をネットワーク上で付与する。

【０５６８】

[620]例27は例26の主題を包括しており、コンピュータプログラムコードにより、一つ以上のプロセスユニットが、最初の時間帯にセカンドクラアントが最初のデータ主題の識別を決定づける権利を、ネットワーク上で取り消す。

【０５６９】

[621]例28は例15の主題を包括しており、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、第二の時間帯に最初に生成された識別子と関連した、要求された一つ以上のデータアトリビュートをセカンドクラアントが決定づける権利を、ネットワーク上で取り消す。

【０５７０】

[622]例29は例13の主題を包括しており、ここでは最初に生成された識別子は、最初に生成された識別子と関連する一つ以上のデータアトリビュートから数学的に導かれたものではない。

【０５７１】

[623]例30は例12の主題を包括しており、ここでは第二のデータ主体のために、最初に生成された識別子は主要な識別子を含んでいる。

【０５７２】

[624]例31はシステムで、次の構成を含む。ネットワーク経由でデータを送信する通信インターフェース、コンピュータプログラムコードを持つ内臓メモリー、そしてメモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上のプロセスユニットである。そのプログラムコードによって、一つ以上のプロセスユニットは動的に変化する一時的なユニーク識別子を生成し、最初の一時的なユニーク識別子をを最初のデータ主体と連携し、一つ以上のデータアトリビュートを最初の一時的なユニーク識別子と連携し、最初の一時的なユニーク識別子が最初のデータ対象を特定するために使用され、関連する一つ以上のデータアトリビュートを検索している間に、最初の時間単位を定義する情報で構成される最初の時間単位のデータを生成し、メモリに最初の一時的なユニーク識別子、一つ以上のデータアトリビュート、最初の時間単位のデータを保存し、そして最初の一時的なユニーク識別子をネットワークを通してファーストクライアントへ送信する。

【０５７３】

[625]例32は例31の主題を包括しており、最初の一時的なユニーク識別子を生成する指示が、時間、目的そして位置のいずれかのうち少なくとも一つの要因に基づいて実行される。

【０５７４】

[626]例33は例31の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初の一時的なユニーク識別子が最初のデータ主題を識別し関連する一つ以上のデータアトリビュートを検索することを終了する。

【０５７５】

[627]例34は例33の主題を包括しており、ここでは、最初の一時的なユニーク識別子が最初のデータ主題を識別し関連する一つ以上のデータアトリビュートを検索することを終了する指示は、時間、目的そして位置のいずれかのうち少なくとも一つの要因に基づいて実行される。

【０５７６】
[628]例35は例31の主題を包括しており、ここで、最初の一時的ユニーク識別子に関連する一つ以上のデータアトリビュートのうち、少なくとも一つが動作、処理、目的、最初のデータ対象の特性に関係している。
【０５７７】
[629]例36は例31の主題を包括しており、ここではコンピュータプログラムコードの指示によって、二番目の時間帯で、一つ以上のプロセスユニットが最初の一時的ユニーク識別子を二番目のデータ主題と連携させる。
【０５７８】
[630]例37は例31の主題を包括しており、ここではコンピュータプログラムコードの指示によって、最初の時間帯で、一つ以上のプロセスユニットが最初の一時的ユニーク識別子を二番目のデータ主題と連携させる。
【０５７９】
[631]例38は例31の主題を包括しており、ここではコンピュータプログラムコードの指示によって、最初の時間帯に、最初の一時的なユニーク識別子と関連した最初のデータ主題の識別のため、最初のリクエストをネットワーク上でセカンドクライアントから受信し、最初のリクエストがオーソライズされることを決定し、セカンドクライアントが、最初の時間帯の間に最初のデータ主題の識別を決定づける権利をネットワーク上で付与する。
【０５８０】
[632]例39は例38の主題を包括しており、ここでは、コンピュータプログラムコードにより、一つ以上のプロセスユニットが、最初の時間帯にセカンドクラアントが最初のデータ主題の識別を決定づける権利を、ネットワーク上で取り消す。
【０５８１】
[633]例40は例31の主題を包括しており、ここではコンピュータプログラムコードの指示によって、最初の時間帯に、最初の一時的なユニーク識別子と関連した一つ以上のデータアトリビュートのため、最初のリクエストをネットワーク上でセカンドクライアントから受信し、最初のリクエストがオーソライズされることを決定し、セカンドクライアントが、最初の時間帯の間に要求された、最初の一時的なユニーク識別子と関連した一つ以上のデータアトリビュートの識別を決定づける権利をネットワーク上で付与する。
【０５８２】
[634]例41は例40の主題を包括しており、ここでは、コンピュータプログラムコードにより、一つ以上のプロセスユニットが、最初の時間帯の間に、要求された最初の一時的なユニーク識別子と関連した一つ以上のデータアトリビュートの識別をセカンドクライアントが決定づける権利を、ネットワーク上で取り消す。
【０５８３】
[635]例42は例31の主題を包括しており、ここで、最初の一時的なユニーク識別子は、最初の一時的なユニーク識別子と関連する一つ以上のデータアトリビュートから数学的に導かれたものではない。
【０５８４】
[636]例43は例31の主題を包括しており、ここで、最初の一時的なユニーク識別子は最初のデータ主体の識別のために主要な識別子を包括している。
【０５８５】
[637]例44はコンピューターで実行可能な格納された指示で構成される、恒久的なコンピューター判読可能な媒体で、ここでは一つ以上のプロセスユニットが以下の動作を行う。一時的なユニーク識別子を生成し、最初の一時的なユニーク識別子を最初のデータ主体と連携し、一つ以上のデータアトリビュートを最初の一時的なユニーク識別子と連携し、最初の時間単位データを生成する。そこでは、最初の一時的なユニーク識別子が最初のデータ主題を識別するために使用され、関連する一つ以上のデータアトリビュートを検索している間に、最初の時間単位データが最初の時間帯を定義する情報を含む最初の時間単位データを構成し、メモリに最初の一時的なユニーク識別子と一つ以上のデータアトリビュー

ト、そして最初の時間単位データを保存し、そして最初の一時的なユニーク識別子と一つ以上のデータアトリビュートをネットワークを通してファーストクライアントへ送信する。

【０５８６】

[638]例45は例44の主題を包括しており、ここでは、最初の一時的ユニーク識別子を生成する指示が、時間、目的そして位置のいずれかのうち少なくとも一つの要因に基づいて実行される。

【０５８７】

[639]例46は例44の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初の一時的なユニーク識別子が最初のデータ主題を識別し関連する一つ以上のデータアトリビュートを検索することを終了する。

【０５８８】

[640]例47は例46の主題を包括しており、ここでは、最初の一時的なユニーク識別子が最初のデータ主題を識別し関連する一つ以上のデータアトリビュートを検索することを終了する指示が、時間、目的そして位置のいずれかのうち少なくとも一つの要因に基づいて実行される。

【０５８９】

[641]例48は例44の主題を包括しており、ここで、最初の一時的ユニーク識別子に関連する一つ以上のデータアトリビュートのうち、少なくとも一つが動作、処理、目的、最初のデータ対象の特性に関係している。

【０５９０】

[642]例49は例44の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、二番目の時間帯に、最初の一時的なユニーク識別子を二番目のデータ主題と連携させる。

【０５９１】

[643]例50は例44の主題を包括しており、ここでは、指示により、一つ以上のプロセスユニットが、二番目の時間帯に、最初の一時的なユニーク識別子を二番目のデータ主題と連携させる。

【０５９２】

[644]例51は例44の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが以下の動作を行う。最初の時間帯に、最初の一時的なユニーク識別子と関連した最初のデータ主題の識別のため、最初のリクエストをネットワーク上でセカンドクライアントから受信し、最初のリクエストがオーソライズされることを決定し、セカンドクライアントが最初の時間帯の間に最初のデータ主題の識別を決定づける権利をネットワーク上で付与する。

【０５９３】

[645]例52は例51の主題を包括しており、ここでは、コンピュータプログラムコードにより、一つ以上のプロセスユニットが、最初の時間帯の間に、セカンドクライアントが最初の時間帯の間に最初のデータ主題の識別を決定づける権利を、ネットワーク上で取り消す。

【０５９４】

[646]例53は例44の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが以下の動作を行う。最初の時間帯に、最初の一時的なユニーク識別子に関連した一つ以上のデータアトリビュートの識別のため、最初のリクエストをネットワーク上でセカンドクライアントから受信し、最初のリクエストがオーソライズされることを決定し、セカンドクライアントが最初の時間帯の間に、要求された最初の一時的なユニーク識別子に関連した一つ以上のデータアトリビュートの識別を決定づける権利をネットワーク上で付与する。

【０５９５】

[647]例54は例53の主題を包括しており、ここでは、コンピュータプログラムコードにより、一つ以上のプロセスユニットが、最初の時間帯の間に、セカンドクライアントが最初の時間帯の間に、要求された最初の一時的なユニーク識別子に関連した一つ以上のデータ

アトリビュートの識別を決定づける権利を、ネットワーク上で取り消す。
【０５９６】
[648]例55は例44の主題を包括しており、ここで、最初の一時的なユニーク識別子は、最初の一時的なユニーク識別子と関連する一つ以上のデータアトリビュートから数学的に導かれたものではない。
【０５９７】
[649]例56は例44の主題を包括しており、ここで、最初の一時的なユニーク識別子は最初のデータ主題のために主要な識別子を包括する。
【０５９８】
[650]例57はデバイスで、次の構成を含む。ネットワーク経由でデータを送信する通信インターフェース、コンピュータプログラムコードを持つ内臓メモリー、そしてメモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上のプロセスユニットである。そのプログラムコードによって、一つ以上のプロセスユニットは、ネットワーク上で一時的なユニーク識別子をプライバシーサーバーからリクエストし、最初の一時的なユニーク識別子をデバイスのユーザーである最初のデータ主体と連携し、一つ以上のデータアトリビュートを最初の一時的なユニーク識別子と連携し、最初の時間単位のデータを生成する。そこでは、最初の一時的なユニーク識別子が最初のデータ対象を特定するために使用され、関連する一つ以上のデータアトリビュートを検索している間に、最初の時間単位データが最初の時間単位を定義する情報を構成し、メモリに最初の一時的なユニーク識別子、一つ以上のデータアトリビュート、最初の時間単位のデータを保存し、そして、最初の条件が満たされたと判別されたことに対応して、最初の一時的なユニーク識別子、最初の時間単位データ、一つ以上のデータアトリビュートをネットワークを通してファーストクライアントへ送信する。
【０５９９】
[651]例58は例57の主題を包括しており、ここでは、最初の条件が満たされたという判別が以下のうち少なくとも一つを含む。事前に決定された時間量が経過した、柔軟性のある時間量が経過した、最初の一時的なユニーク識別子の目的が無効になった、または最初のデータ主体の位置が変更された。
【０６００】
[652]例59は例57の主題を包括しており、ここではコンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初の一時的なユニーク識別子と関連した一つ以上のデータアトリビュートを修正する。
【０６０１】
[653]例60は例57の主題を包括しており、ここで、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、一時的なユニーク識別子の使用を追跡する。
【０６０２】
[654]例61は例57の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、一時的なユニーク識別子が最初のデータ主体の識別を決定づけ一つ以上の関連する一つ以上のデータアトリビュートを検索する権利を、ネットワーク上で取り消す。
【０６０３】
[655]例62は例57の主題を包括しており、ここでは、デバイスはプライバシーサーバーと同じコンピューターデバイスに存在する。
【０６０４】
[656]例63は例57の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、一時的なユニーク識別子の変更に応じて、最初の時間単位データまたは一つ以上のデータアトリビュート、または最初の一時的なユニーク識別子、最初の時間単位データ、一つ以上のデータアトリビュートのうち少なくともひとつを、ネットワーク上で、ファーストプライバシーサーバーにデバイスと同期するよう登録された一つ以上のクライアントデバイスへ送信する。

【０６０５】
[657]例64は例57の主題を包括しており、ここで、最初の一時的なユニーク識別子、最初の時間単位データ、一つ以上のデータアトリビュートがネットワーク上でファーストプライバシーサーバーへHTTPクッキーの形式で送信される。
【０６０６】
[658]例65は例57の主題を包括しており、ここで、最初の一時的なユニーク識別子は、最初の一時的なユニーク識別子と関連する一つ以上のデータアトリビュートから数学的に導かれたものではない。
【０６０７】
[659]例66は例57の主題を包括しており、ここで、一時的なユニーク識別子が最初のデータ主体のために主要な識別子を含む。
【０６０８】
[660]例67はコンピューターで実行可能な格納された指示で構成される、恒久的なコンピューター判読可能な媒体で、ここでは一つ以上のプロセスユニットが以下の動作を行う。ネットワーク上で一時的なユニーク識別子をプライバシーサーバーからリクエストし、最初の一時的なユニーク識別子をファーストクライアントデバイスのユーザーである最初のデータ主体と連携し、一つ以上のデータアトリビュートを最初の一時的なユニーク識別子と連携し、最初の時間単位のデータを生成する。そこでは、最初の一時的なユニーク識別子が最初のデータ対象を特定するために使用され、関連する一つ以上のデータアトリビュートを検索している間に、最初の時間単位データが最初の時間単位を定義する情報を構成し、ファーストクライアントデバイスのメモリに最初の一時的なユニーク識別子、一つ以上のデータアトリビュート、最初の時間単位のデータを保存し、そして、最初の条件が満たされたと判別されたことに対応して、最初の一時的なユニーク識別子、最初の時間単位データ、一つ以上のデータアトリビュートをネットワークを通してファースプライバシーサーバーへ送信する。
【０６０９】
[661]例68は例67の主題を包括しており、ここでは、最初の条件が満たされたという判別が以下のうち少なくとも一つを含む。事前に決定された時間量が経過した、柔軟性のある時間量が経過した、最初の一時的なユニーク識別子の目的が無効になった、または最初のデータ主体の位置が変更された。
【０６１０】
[662]例69は例67の主題を包括しており、ここではコンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初の一時的なユニーク識別子と関連した一つ以上のデータアトリビュートを修正する。
【０６１１】
[663]例70は例67の主題を包括しており、ここではコンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初の一時的なユニーク識別子の使用を追跡する。
【０６１２】
[664]例71は例67の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、一時的なユニーク識別子が最初のデータ主体の識別を決定づけ一つ以上の関連する一つ以上のデータアトリビュートを検索する権利を取り消す。
【０６１３】
[665]例72は例67の主題を包括しており、ここでは、ファーストクライアントデバイスはプライバシーサーバーと同じコンピューターデバイスに存在する。
【０６１４】
[666]例73は例67の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、一時的なユニーク識別子の変更に応じて、最初の時間単位データまたは一つ以上のデータアトリビュート、または最初の一時的なユニ

ーク識別子、最初の時間単位データ、一つ以上のデータアトリビュートのうち少なくともひとつを、ネットワーク上で、ファーストプライバシーサーバーにデバイスと同期するよう登録された一つ以上のクライアントデバイスへ送信する。.

【０６１５】

[667]例74は例67の主題を包括しており、ここで、最初の一時的なユニーク識別子、最初の時間単位データ、一つ以上のデータアトリビュートがネットワーク上でファーストプライバシーサーバーへHTTPクッキーの形式で送信される。

【０６１６】

[668]例75は例67の主題を包括しており、ここで、最初の一時的なユニーク識別子は、最初の一時的なユニーク識別子と関連する一つ以上のデータアトリビュートから数学的に導かれたものではない。

【０６１７】

[669]例76は例67の主題を包括しており、ここで、一時的なユニーク識別子は最初のデータ主体のために主要な識別子を含む。

【０６１８】

[670]例77はデバイスで、次の構成を含む。ネットワーク経由でデータを送信する通信インターフェース、コンピュータプログラムコードを持つ内臓メモリー、そしてメモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上のプロセスユニットである。そのプログラムコードのによって、一つ以上のプロセスユニットは、以下の行動を起こす。ネットワーク上でファーストプライバシーサーバーから最初の一時的なユニーク識別子を獲得し、ここでは、最初の時間帯に、最初の一時的なユニーク識別子はファーストプライバシーサーバーにてデバイスのユーザーである最初のデータ主体と連携されている。次に一つ以上のデータアトリビュートを最初の一時的なユニーク識別子と連携し、最初の時間単位のデータを生成する。そこでは、最初の一時的なユニーク識別子が最初のデータ対象を特定するために使用され、関連する一つ以上のデータアトリビュートを検索している間に、最初の時間単位データが最初の時間単位を定義する情報を構成する。そしてメモリに最初の一時的なユニーク識別子、一つ以上のデータアトリビュート、最初の時間単位のデータを保存し、最初の一時的なユニーク識別子、最初の時間単位データ、一つ以上のデータアトリビュートをネットワーク上でファーストプライバシーサーバーへ送信する。そして、二番目の一時的なユニーク識別子をファーストプライバシーサーバーからネットワーク上で受信し、ここで、二番目の一時的なユニーク識別子は、二番目の時間帯で、ファーストプライバシーサーバーで最初のデータ主体、一つ以上のデータアトリビュートと連携される。

【０６１９】

[671]例78は例77の主題を包括しており、ここでは、一つ以上のプロセスユニットに、二番目の一時的なユニーク識別子をネットワーク上でファーストプライバシーサーバーから受信させるコンピュータプログラムコードの指示は最初の条件が満たされたという判別に応じて実行される。

【０６２０】

[672]例79は例78の主題を包括しており、最初の条件が満たされたという判別が以下のうち少なくとも一つを含む。事前に決定された時間量が経過した、柔軟性のある時間量が経過した、最初の一時的なユニーク識別子の目的が無効になった、または最初のデータ主体の位置がへんこうされた。

【０６２１】

[673]例80は例77の主題を包括しており、ここではコンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初の一時的なユニーク識別子と関連した一つ以上のデータアトリビュートを修正する。

【０６２２】

[674]例81は例77の主題を包括しており、ここではコンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初の一時的なユニーク識別子の使用を追跡す

る。
【０６２３】
[675]例82は例77の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、一時的なユニーク識別子が最初のデータ主体の識別を決定づけ一つ以上の関連する一つ以上のデータアトリビュートを検索する権利を取り消す。
【０６２４】
[676]例83は例77の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、ファーストプライバシーサーバーから最初のデータ主体または一つ以上のデータアトリビュートの識別が最初の要求者に明らかにされるかの承認を要求し、ファーストプライバシーサーバーから最初のデータ主体または一つ以上のデータアトリビュートの識別を最初の要求者へ開示して良いという承認の受信に応じて、最初のデータ主体または一つ以上のデータアトリビュートの識別を最初の要求者へ送信する。
【０６２５】
[677]例84は例83の主題を包括しており、ここでは、承認要求が、さらに、特定の動作、活動、処理または特性に対しては、最初のデータ主体または一つ以上のデータアトリビュートの識別を最初の要求者へ開示して良いという要求された承認を含んでいる。
【０６２６】
[678]例85は例83の主題を包括しており、承認要求がさらに、特定の時間、または位置においては、最初のデータ主体または一つ以上のデータアトリビュートの識別を最初の要求者へ開示して良いという要求された承認を含んでいる。
【０６２７】
[679]例86は例84の主題を包括しており、承認要求がさらに、特定の動作、活動、処理または特製に対しては、最初のデータ主体または一つ以上のデータアトリビュートの識別を最初の要求者へ開示して良いという要求された承認を含んでいる。
【０６２８】
[680]例87はシステムで、次の構成を含む。ネットワーク経由でデータを送信する通信インターフェース、コンピュータプログラムコードを持つ内臓メモリー、そしてメモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上のプロセスユニットである。そのプログラムコードによって、一つ以上のプロセスユニットは動的に変化する一時的なユニーク識別子を生成し、生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと関連するように、最初のデータ主体からの最初の要求をネットワーク上で受信し、最初の要求に応じて、最初に生成された動的に変化する一時的なユニーク識別子を最初のデータ主体のアトリビュートと連携し、動的に変化する一時的なユニーク識別子の価値を最初の判読できない形式へ変換する。この点において、第一キーは、最初の判読不可形式を、最初に生成された動的に変化する一時的なユニーク識別子のファーストビューに戻すために使用され、第二キーは、最初の判読不可形式を最初に生成された動的に変化する一時的なユニーク識別子のセカンドビューに変換するために使用され、さらに第一キーは第二キーと異なるものであり、ファーストビューはセカンドビューと異なるものである。そして、メモリに最初に生成された動的に変化する一時的なユニーク識別子、第一キー、第二キー、最初の判読不可形式を保存し、そして最初の判読不可形式ネットワークを通して最初のデータ主体へ送信する。
【０６２９】
[681]例88は例87の主題を包括しており、ここで、ファーストビューはセカンドビューよりもより詳細を提供する。
【０６３０】
[682]例89は例87の主題を包括しており、ここで判読不可形式は暗号化されたテキストを含む。
【０６３１】

[683]例90は例87の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初に生成された動的に変化する一時的なユニーク識別子を第二のデータ主体と連携もさせる。

【０６３２】

[684]例91は例90の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、最初に生成された動的に変化する一時的なユニーク識別子を第二のデータ主体のアトリビュートと連携させる、コンピュータプログラムコードの指示が少なくとも以下のいずれかの状況で実施される。動的に変化する一時的なユニーク識別子が最初のデータ主体と連携された時間と異なる時点である、最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと連携された時と異なる現実あるいは仮想地点である、または最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体と連携されたものとは異なる目的である。

【０６３３】

[685]例92は例87の主題を包括しており、ここでは、コンピュータプログラムコードの指示により、一つ以上のプロセスユニットが、二番目に生成された動的に変化する一時的なユニーク識別子を最初のデータ主体のアトリビュートと連携させる。

【０６３４】

[686]例93は例92の主題を包括しており、ここでは、一つ以上のプロセスユニットが、二番目に生成された動的に変化する一時的なユニーク識別子を最初のデータ主体のアトリビュートと連携させるコンピュータプログラムコードの指示が、少なくとも以下のいずれかの状況で実施される。動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと連携された時間と異なる時点である、最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと連携された時と異なる現実あるいは仮想地点である、または最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと連携されたものとは異なる目的である

【０６３５】

[687]例94はコンピューターで実行可能な格納された指示で構成される、恒久的なコンピューター判読可能な媒体で、ここでは一つ以上のプロセスユニットが以下の動作を行う。一つ以上のプロセスユニットは動的に変化する一時的なユニーク識別子を生成し、生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと関連するように、最初のデータ主体からの最初の要求をネットワーク上で受信し、最初の要求に応じて、最初に生成された動的に変化する一時的なユニーク識別子を最初のデータ主体のアトリビュートと連携し、動的に変化する一時的なユニーク識別子の価値を最初の判読できない形式へ変換する。この点において、第一キーは、最初の判読不可形式を、最初に生成された動的に変化する一時的なユニーク識別子のファーストビューに戻すために使用され、第二キーは、最初の判読不可形式を最初に生成された動的に変化する一時的なユニーク識別子のセカンドビューに変換するために使用され、さらに第一キーは第二キーと異なるものであり、ファーストビューはセカンドビューと異なるものである。そして、メモリに最初に生成された動的に変化する一時的なユニーク識別子、第一キー、第二キー、最初の判読不可形式を保存し、そして最初の判読不可形式ネットワークを通して最初のデータ主体へ送信する。

【０６３６】

[688]例95は例94の主題を包括しており、ここではファーストビューはセカンドビューよりもより詳細を提供する。

【０６３７】

[689]例96は例94の主題を包括しており、判読不可形式のフォームは非暗号化テキストを含んでいる。

【０６３８】

[690]例97は例94の主題を包括しており、ここでは指示が、さらに、一つ以上のプロセスユニットに最初に生成された動的に変化する一時的なユニーク識別子を二番目のデータ主

体のアトリビュートと連携させる指示を含んでいる。
【０６３９】
[691]例98は例97の主題を包括しており、ここでは、一つ以上のプロセスユニットが、最初に生成された動的に変化する一時的なユニーク識別子を二番目のデータ主体のアトリビュートと連携させるコンピュータプログラムコードの指示が、少なくとも以下のいずれかの状況で実施される。動的に変化する一時的なユニーク識別子が最初のデータ主体と連携された時間と異なる時点である、最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと連携された時と異なる現実あるいは仮想地点である、または最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体と連携されたものとは異なる目的である。
【０６４０】
[692]例99は例94の主題を包括しており、ここでは指示が、さらに、一つ以上のプロセスユニットに二番目に生成された動的に変化する一時的なユニーク識別子を最初のデータ主体のアトリビュートと連携させる指示を含んでいる。
【０６４１】
[693]例100は例99の主題を包括しており、ここでは、一つ以上のプロセスユニットが、二番目に生成された動的に変化する一時的なユニーク識別子を最初のデータ主体のアトリビュートと連携させるコンピュータプログラムコードの指示が、少なくとも以下のいずれかの状況で実施される。最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体と連携された時間と異なる時点である、最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと連携された時と異なる現実あるいは仮想地点である、または最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体と連携されたものとは異なる目的である。
【０６４２】
[694]例101はコンピュータにより実施される手法の構成で、一つ以上の動的に変化する一時的なユニーク識別子を生成し、生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと関連するように、最初のデータ主体からの最初の要求をネットワーク上で受信し、最初の要求に応じて、最初に生成された動的に変化する一時的なユニーク識別子を最初のデータ主体のアトリビュートと連携し、動的に変化する一時的なユニーク識別子の価値を最初の判読できない形式へ変換する。この点において、第一キーは、最初の判読不可形式を、最初に生成された動的に変化する一時的なユニーク識別子のファーストビューに戻すために使用され、第二キーは、最初の判読不可形式を最初に生成された動的に変化する一時的なユニーク識別子のセカンドビューに変換するために使用され、さらに第一キーは第二キーと異なるものであり、ファーストビューはセカンドビューと異なるものである。そして、メモリに最初に生成された動的に変化する一時的なユニーク識別子、第一キー、第二キー、最初の判読不可形式を保存し、そして最初の判読不可形式ネットワークを通して最初のデータ主体へ送信する。
【０６４３】
[695]例102は例101の主題を包括しており、ここで、ファーストビューはセカンドビューよりも詳細を提供する。
【０６４４】
[696]例103は例101の主題を包括しており、ここでは指示が、さらに、最初に生成された動的に変化する一時的なユニーク識別子を、二番目のデータ主体のアトリビュートと連携させる指示を含んでいる。
【０６４５】
[697]例104はれい103の主題を包括しており、ここでは、最初に生成された動的に変化する一時的なユニーク識別子を二番目のデータ主体のアトリビュートと連携させる行為が、少なくとも以下のいずれかの状況で実施される。最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体と連携された時間と異なる時点である、最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと

連携された時と異なる現実あるいは仮想地点である、または最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体と連携されたものとは異なる目的である。

【０６４６】

[698]例105は例101の主題を包括しており、二番目に生成された動的に変化する一時的なユニーク識別子を最初のデータ主体に連携させることをさらに含んでいる。

【０６４７】

[699]例106は例105の主題を包括しており、ここでは、二番目に生成された動的に変化する一時的なユニーク識別子を最初のデータ主体のアトリビュートと連携させる行為が、少なくとも以下のいずれかの状況で実施される。最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体と連携された時間と異なる時点である、最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体のアトリビュートと連携された時と異なる現実あるいは仮想地点である、または最初に生成された動的に変化する一時的なユニーク識別子が最初のデータ主体と連携されたものとは異なる目的である。

【０６４８】

[700]例107はシステムで、次の構成を含む。ネットワーク経由でデータを送信する通信インターフェース、コンピュータプログラムコードを持つ内臓メモリー、一つ以上のデータソース、そしてメモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上のプロセスユニットである。そのプログラムコードによって、一つ以上のプロセスユニットは、データ主体の多数性に付属する一つ以上のデータソースからデータを取得し、多数のデータ主体のうち最初のデータ主体のため、動的に変化する一時的なユニーク識別子を生成する。その点では、一つ以上のデータソースの中の、最初のデータ主体が最初のデータソースと二番目のデータソースのそれぞれに最初のデータ主体がある。そして、一つ以上の類似識別子に対応して、一つ以上の動的に変化する一時的なユニーク識別子を生成し、その点においては、各類似識別子は値を持っている。　そして、最初のデータソース内の一つ以上の類似の識別子の値に対する最初の要求をネットワーク上で受信し、二番目のデータソース内の一つ以上の類似の識別子の値に対する二番目の要求をネットワーク上で受信して、最初の要求で得た値を、一つ以上の第四の動的に変化する一時的なユニーク識別子へ変換し、二番目の要求で得られた値を、一つ以上の第四の動的に変化する一時的なユニーク識別子に変換する。そして、最初の動的に変化する一時的なユニーク識別子、二番目の動的に変化する一時的なユニーク識別子、一つ以上の第三の動的に変化する一時的なユニーク識別子、一つ以上の第四の動的に変化する一時的なユニーク識別子を、メモリに保存し、最初の動的に変化する一時的なユニーク識別子、二番目の動的に変化する一時的なユニーク識別子、一つ以上の第三の動的に変化する一時的なユニーク識別子、一つ以上の第四の動的に変化する一時的なユニーク識別子を、ネットワーク上で送信する。

【０６４９】

[701]例108は例107の主題を包括しており、ここでは最初の動的に変化する一時的なユニーク識別子がReplacement DDID （R-DDID）を含んでいる。

【０６５０】

[702]例109は例108の主題を包括しており、一つ以上の第三の動的に変化する一時的なユニーク識別子がAssociation DDIDs （A-DDIDs）を含んでいる。

【０６５１】

[703]例110は例107の主題を包括しており、ここでは、R-DDID が特定の値を含んでいる。

【０６５２】

[704]例111は例107の主題を包括しており、ここではA-DDID が特定の値を含んでいる。

【０６５３】

[705]例112は例109の主題を包括しており、指令によって、一つ以上のプロセスユニットがR-DDIDを R-DDIDのファーストビューへ変換するために第一キーを使用し、R-DDIDを R-DDIDのセカンドビューへ変換するために第二キーを使用し、この点では、第一キー

は第二キーと異なるものである。

【０６５４】

[706]例113は例109の主題を包括しており、指令によって、一つ以上のプロセスユニットが最初のA-DDIDを 最初のA-DDIDのサードビューへ変換するために第三キーを使用し、最初のA-DDIDを 最初のA-DDIDのフォースビューへ変換するために第四キーを使用し、この点では、第三キーは第四キーと異なり、サードビューはフォースビューと異なるものである。

【０６５５】

[707]例114は例107の主題を包括しており、ここでは、最初の第二の動的に変化する一時的なユニーク識別子は最初のデータソースと二番目のデータソースにおいて同じ値を持つ。

【０６５６】

[708]例115は例107の主題を包括しており、ここでは、一つ以上の第三の動的に変化する一時的なユニーク識別子のうち少なくとも一つは、最初の判読不可形式を含んでいる。

【０６５７】

[709]例116は例107の主題を包括しており、ここでは、一つ以上の第四の動的に変化する一時的なユニーク識別子のうち少なくとも一つは、第二の判読不可形式を含んでいる。

【０６５８】

[710]例117は例115の主題を包括しており、ここでは判読不可形式は暗号化データを含んでいる。

【０６５９】

[711]例118は例116の主題を包括しており、ここでは最初の判読不可形式は暗号化データを含んでいる。

【０６６０】

[712]例119は例107の主題を包括しており、ここでは一つ以上のデータソースのうち少なくとも一つのデータソースが特定のサブセット、人口、データ主体の集団を含んでいる。

【０６６１】

[713]例120は例107の主題を包括しており、ここでは、一定時間の間、一つ以上のデータソースがデータ主体の特定の多様性に付属する。

【０６６２】

[714]例121は例109の主題を包括しており、ここでは、一つ以上のA-DDIDのうち少なくとも一つが、離散した値、または離散した値の組あわせを含んでいる。

【０６６３】

[715]例122は例109の主題を包括しており、ここでは、一つ以上のA-DDIDsのうち少なくとも一つが散した値、または離散した値の組あわせを含んでいる。

【０６６４】

[716]例123は例94はコンピューターで実行可能な格納された指示で構成される、恒久的なコンピューター判読可能な媒体で、ここでは一つ以上のプロセスユニットが以下の動作を行う。データ主体の多数性に付属する一つ以上のデータソースのそれぞれからデータを取得し、多数のデータ主体のうち最初のデータ主体のため、最初の動的に変化する一時的なユニーク識別子を生成する。ここでは、一つ以上のデータソースの中の、最初のデータ主体が最初のデータソースと二番目のデータソースのそれぞれに最初のデータ主体がある。そして、最初のデータソースと二番目のデータソースそれぞれの、一つ以上の類似識別子に対応し、一つ以上の第二の動的に変化する一時的なユニーク識別子を生成し、ここでは、各類似識別子は値を持っている。そして、最初のデータソース内の一つ以上の類似の識別子の値に対する最初の要求をネットワーク上で受信し、二番目のデータソース内の一つ以上の類似の識別子の値に対する二番目の要求をネットワーク上で受信して、最初の要求で得た値を、一つ以上の第三の動的に変化する一時的なユニーク識別子へ変換し、二番目の要求で得られた値を、一つ以上の第四の動的に変化する一時的なユニーク識別子に変換する。そして、最初の動的に変化する一時的なユニーク識別子、二番目の動的に変化す

る一時的なユニーク識別子、一つ以上の第三の動的に変化する一時的なユニーク識別子、一つ以上の第四の動的に変化する一時的なユニーク識別子を、メモリに保存し、最初の動的に変化する一時的なユニーク識別子、二番目の動的に変化する一時的なユニーク識別子、一つ以上の第三の動的に変化する一時的なユニーク識別子、一つ以上の第四の動的に変化する一時的なユニーク識別子を、ネットワーク上で送信する。

【０６６５】

[717]例124は例123の主題を包括しており、ここでは最初の動的に変化する一時的なユニーク識別子はReplacement DDID （R-DDID）を含む。

【０６６６】

[718]例125は例124の主題を包括しており、ここでは一つ以上の第三の動的に変化する一時的なユニーク識別子はAssociation DDID （A-DDID）を含む。

【０６６７】

[719]例126は例125の主題を包括しており、ここではR-DDIDは特定の値を持つ。

【０６６８】

[720]例127は例123の主題を包括しており、ここではA-DDIDは特定の値を持つ。

【０６６９】

[721]例128は例125の主題を包括しており、指令によって、一つ以上のプロセスユニットがR-DDIDを R-DDIDのファーストビューへ変換するために第一キーを使用し、R-DDIDを R-DDIDのセカンドビューへ変換するために第二キーを使用し、この点では、第一キーは第二キーと異なるものである。

【０６７０】

[722]例129は例125の主題を包括しており、指令によって、一つ以上のプロセスユニットが最初のA-DDIDを 最初のA-DDIDのサードビューへ変換するために第三キーを使用し、最初のA-DDIDを 最初のA-DDIDのフォースビューへ変換するために第四キーを使用し、この点では、第三キーは第四キーと異なり、サードビューはフォースビューと異なるものである。

【０６７１】

[723]例130は例123の主題を包括しており、ここではここでは、最初の第二の動的に変化する一時的なユニーク識別子は最初のデータソースと二番目のデータソースにおいて同じ値を持つ。

【０６７２】

[724]例131は例123の主題を包括しており、ここでは、一つ以上の第三の動的に変化する一時的なユニーク識別子のうち少なくとも一つは、最初の判読不可形式を含んでいる。

【０６７３】

[725]例132は例123の主題を包括しており、ここでは、一つ以上の第四の動的に変化する一時的なユニーク識別子のうち少なくとも一つは、第二の判読不可形式を含んでいる。

【０６７４】

[726]例133は例131の主題を包括しており、ここでは最初の判読不可形式は暗号化データを含む。

【０６７５】

[727]例134は例132の主題を包括しており、ここでは最初の判読不可形式は暗号化データを含む。

【０６７６】

[728]例135は例123の主題を包括しており、ここでは一つ以上のデータソースのうち少なくとも一つのデータソースが特定のサブセット、人口、データ主体の集団を含んでいる。

【０６７７】

[729]例136は例123の主題を包括しており、ここでは、一定時間の間、一つ以上のデータソースのそれぞれがデータ主体の特定の多様性に付属する。

【０６７８】

[730]例137は例125の主題を包括しており、ここでは、一つ以上のA-DDIDのうち少なく

とも一つが、数値グルーピングかカテゴリー断定的なグルーピングのどちらかを含む。
【０６７９】
[731]例138は例125の主題を包括しており、一つ以上のA-DDIDのうち少なくとも一つが離散した値、または離散した値の組あわせを含んでいる。
【０６８０】
[732]例139はコンピュータにより実施される手法の構成で、最初のデータ主体の多数性に付属する、一つ以上のデータソースのそれぞれからデータを取得し、最初のデータ主体の多数性の、最初のデータ主体のため、最初の動的に変化する一時的なユニーク識別子を生成する。ここでは、一つ以上のデータソースの中の、最初のデータ主体が最初のデータソースと二番目のデータソースのそれぞれに最初のデータ主体がある。そして、最初のデータソースと二番目のデータソースそれぞれの、一つ以上の類似識別子に対応し、一つ以上の第二の動的に変化する一時的なユニーク識別子を生成し、ここでは、各類似識別子は値を持っている。そして、最初のデータソース内の一つ以上の類似の識別子の値に対する最初の要求をネットワーク上で受信し、二番目のデータソース内の一つ以上の類似の識別子の値に対する二番目の要求をネットワーク上で受信して、最初の要求で得た値を、一つ以上の第三の動的に変化する一時的なユニーク識別子へ変換し、二番目の要求で得られた値を、一つ以上の第四の動的に変化する一時的なユニーク識別子に変換する。そして、最初の動的に変化する一時的なユニーク識別子、二番目の動的に変化する一時的なユニーク識別子、一つ以上の第三の動的に変化する一時的なユニーク識別子、一つ以上の第四の動的に変化する一時的なユニーク識別子を、メモリに保存し、最初の動的に変化する一時的なユニーク識別子、二番目の動的に変化する一時的なユニーク識別子、一つ以上の第三の動的に変化する一時的なユニーク識別子、一つ以上の第四の動的に変化する一時的なユニーク識別子を、ネットワーク上で送信する。
【０６８１】
[733]例140は例139の主題を包括しており、ここでは最初の動的に変化する一時的なユニーク識別子はReplacement DDID （R-DDID）を含む。
【０６８２】
[734]例141は例140の主題を包括しており、ここでは一つ以上の第三の動的に変化する一時的なユニーク識別子はAssociation DDID （A-DDID）を含む。
【０６８３】
[735]例142は例139の主題を包括しており、ここではR-DDIDは特定の値を持つ。
【０６８４】
[736]例143は例139の主題を包括しており、ここではA-DDIDは特定の値を持つ。
【０６８５】
[737]例144は例141の主題を包括しており、R-DDIDを R-DDIDのファーストビューへ変換するために第一キーを使用し、R-DDIDを R-DDIDのセカンドビューへ変換するために第二キーを使用する行為を含む。ここでは、第一キーは第二キーと異なるものである。
【０６８６】
[738]例145は例141の主題を包括しており、最初のA-DDIDを 最初のA-DDIDのサードビューへ変換するために第三キーを使用し、最初のA-DDIDを 最初のA-DDIDのフォースビューへ変換するために第四キーを使用する行為を含む。ここでは、第三キーは第四キーと異なり、サードビューはフォースビューと異なるものである
【０６８７】
[739]例146は例139の主題を包括しており、ここでは、最初の第二の動的に変化する一時的なユニーク識別子は、最初のデータソースと二番目のデータソースにおいて同じ値を持つ。
【０６８８】
[740]例147は例139の主題を包括しており、ここでは、一つ以上の第三の動的に変化する一時的なユニーク識別子のうち少なくとも一つは、最初の判読不可形式を含んでいる。
【０６８９】

[741]例148は例139の主題を包括しており、ここでは、一つ以上の第四の動的に変化する一時的なユニーク識別子のうち少なくとも一つは、二番目の判読不可形式を含んでいる。

【０６９０】

[742]例149は例147の主題を包括しており、ここでは最初の判読不可形式は暗号化データを含む。

【０６９１】

[743]例150は例148の主題を包括しており、ここでは最初の判読不可形式は暗号化データは暗号化データを含む。

【０６９２】

[744]例151は例139の主題を包括しており、ここでは一つ以上のデータソースのうち少なくとも一つのデータソースが特定のサブセット、人口、データ主体の集団を含んでいる。

【０６９３】

[745]例152は例139の主題を包括しており、ここでは、一定時間の間、一つ以上のデータソースのそれぞれがデータ主体の特定の多様性に付属する。

【０６９４】

[746]例153は例141の主題を包括しており、ここでは、一つ以上のA-DDIDのうち少なくとも一つが、数値グルーピングかカテゴリー断定的なグルーピングのどちらかを含む。

【０６９５】

[747]例154は例141の主題を包括しており、一つ以上のA-DDIDのうち少なくとも一つが離散した値、または離散した値の組あわせを含んでいる。

【０６９６】

[748]例155はシステムで、次の構成を含む。ネットワーク経由でデータを送信する通信インターフェース、コンピュータプログラムコードを持つ内臓メモリー、一つ以上のデータソース、そしてメモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上のプロセスユニットである。そのプログラムコードによって、一つ以上のプロセスユニットは、プライバシーポリシーへの対策として最初のユーザーからリクエストを取得し、少なくとも部分的にはリクエストを基にした最初のプライバシーポリシーを決定し、データ主体の最初の複数性に関連した最初のユーザーからデータを取得し、最初のデータ主体の最初の複数性のため、最初の動的に変化する一時的なユニーク識別子(DDID)を生成する。ここでは、動的に変化する一時的なユニーク識別子は、最初のデータ主体に関連する最初の値を置き換えるためと、決定された最初のプライバシーポリシーを満たすため集約される。そして、最初の動的に変化する一時的なユニーク識別子を一つ以上のデータ記憶装置に保存し、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされていない場合、最初の動的に変化する一時的なユニーク識別子を、最初のリクエストに応じて、ネットワーク上で送信し、そして最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされる場合、最初の値を、最初のリクエストに応じて、ネットワーク上で送信する。

【０６９７】

[749]例156は例155の主題を包括しており、ここでは最初の動的に変化する一時的なユニーク識別子はReplacement DDID （R-DDID）を含む。

【０６９８】

[750]例157は例155の主題を包括しており、ここでは一つ以上の第三の動的に変化する一時的なユニーク識別子はAssociation DDID （A-DDID）を含む。

【０６９９】

[751]例158は例156の主題を包括しており、ここではR-DDIDは特定の値を持つ。

【０７００】

[752]例159は例157の主題を包括しており、ここではA-DDIDは特定の値を持つ。

【０７０１】

[753]例160は例159の主題を包括しており、ここでは特定の値が、階級、サブセット、

最初の値を置き換える値の幅を含んでいる。
【０７０２】
[754]例161は例155の主題を包括しており、ここでは、最初のユーザーからのプライバシーポリシーへの対策の要求、データ主体の最初の複数性に関連するデータ、最初の値に対する最初の要求がのうち少なくとも一つがシムを介して受け取られる。
【０７０３】
[755]例162は例155の主題を包括しており、ここでは最初の値が類似識別子を含む。
【０７０４】
[756]例163は例162の主題を包括しており、ここでは類似識別子が構造化されていないデータを含む。
【０７０５】
[757]例164は例162の主題を包括しており、ここでは類似識別子が階級、集団、値の幅を含む。
【０７０６】
[758]例165は例155の主題を包括しており、ここではプライバシーポリシーが統合データの生成を規定する。
【０７０７】
[759]例166は例165の主題を包括しており、ここではプライバシーポリシーが統合データのためのDDIDsの生成をさらに指定する。
【０７０８】
[760]例167は例155の主題を包括しており、ここでは最初のユーザーから得られたデータのうち少なくともいくつかが統合データを規定する。
【０７０９】
[761]例168は例155の主題を包括しており、ここでは最初のユーザーから得られたデータが単独で統合データを規定する。
【０７１０】
[762]例169はコンピュータにより実施される手法の構成で、プライバシーポリシーへの対策として最初のユーザーからリクエストを取得し、少なくとも部分的にはリクエストを基にした最初のプライバシーポリシーを決定し、データ主体の最初の複数性に関連した最初のユーザーからデータを取得し、最初のデータ主体の最初の複数性のため、最初の動的に変化する一時的なユニーク識別子(DDID)を生成する。ここでは、動的に変化する一時的なユニーク識別子は、最初のデータ主体に関連する最初の値を置き換えるためと、決定された最初のプライバシーポリシーを満たすため集約される。そして、最初の動的に変化する一時的なユニーク識別子を一つ以上のデータ記憶装置に保存し、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされていない場合、最初の動的に変化する一時的なユニーク識別子を、最初のリクエストに応じて、ネットワーク上で送信し、そして最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされる場合、最初の値を、最初のリクエストに応じて、ネットワーク上で送信する。
【０７１１】
[763]例170は例169の主題を包括しており、ここでは最初の動的に変化する一時的なユニーク識別子はReplacement DDID （R-DDID）を含む。
【０７１２】
[764]例171は例169の主題を包括しており、ここでは一つ以上の第三の動的に変化する一時的なユニーク識別子はAssociation DDID （A-DDID）を含む。
【０７１３】
[765]例172は例169の主題を包括しており、ここではR-DDIDは最初の値を置き換える特定の値を持つ。.
【０７１４】

[766]例173は例171の主題を包括しており、ここではA-DDIDは特定の値を持つ。
【０７１５】
[767]例174は例173の主題を包括しており、ここでは特定の値が、階級、サブセット、最初の値を置き換える値の幅を含んでいる。
【０７１６】
[768]例175は例169の主題を包括しており、ここでは、最初のユーザーからのプライバシーポリシーへの対策の要求、データ主体の最初の複数性に関連するデータ、最初の値に対する最初の要求のうち少なくとも一つがシムを介して受け取られる。
【０７１７】
[769]例176は例169の主題を包括しており、ここでは最初の値は類似識別子を含む。
【０７１８】
[770]例177は例176の主題を包括しており、ここでは類似識別子が構造化されていないデータを含む。
【０７１９】
[771]例178は例176の主題を包括しており、ここでは類似識別子が階級、集団、値の幅を含む。
【０７２０】
[772]例179は例169の主題を包括しており、ここではプライバシーポリシーが統合データの生成を規定する。
【０７２１】
[773]例180は例179の主題を包括しており、ここではプライバシーポリシーが統合データのためのDDIDsの生成をさらに指定する。
【０７２２】
[774]例181は例169の主題を包括しており、ここでは最初のユーザーから得られたデータのうち少なくともいくつかが統合データを規定する。
【０７２３】
[775]例182は例169の主題を包括しており、ここでは最初のユーザーから得られたデータが単体で統合データを規定する。
【０７２４】
[776]例183は恒久的なプログラムストレージデバイスで、プログラマブルコントロールデバイスによって判読可能であり、格納された指示で構成される。その指示が実行されることでプログラマブルデバイスは以下の動作を行う。プライバシーポリシーへの対策として最初のユーザーからリクエストを取得し、少なくとも部分的にはリクエストを基にした最初のプライバシーポリシーを決定し、データ主体の最初の複数性に関連した最初のユーザーからデータを取得し、最初のデータ主体の最初の複数性のため、最初の動的に変化する一時的なユニーク識別子(DDID)を生成する。ここでは、動的に変化する一時的なユニーク識別子は、最初のデータ主体に関連する最初の値を置き換えるためと、決定された最初のプライバシーポリシーを満たすため集約される。そして、最初の動的に変化する一時的なユニーク識別子を一つ以上のデータ記憶装置に保存し、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされていない場合、最初の動的に変化する一時的なユニーク識別子を、最初のリクエストに応じて、ネットワーク上で送信し、そして最初のプライバシーポリシーに従って最初のリクエストが最初の値を受け取ることをオーソライズされる場合、最初の値を、最初のリクエストに応じて、ネットワーク上で送信する。
【０７２５】
[777]例184は例183の主題を包括しており、ここでは最初の動的に変化する一時的なユニーク識別子はReplacement DDID （R-DDID）を含む。
【０７２６】
[778]例185は例183の主題を包括しており、ここでは一つ以上の第三の動的に変化する

一時的なユニーク識別子はAssociation DDID （A-DDID）を含む。
【０７２７】
[779]例186は例185の主題を包括しており、ここではR-DDIDは最初の値を置き換える特定の値を持つ。
【０７２８】
[780]例187は例185の主題を包括しており、ここではA-DDIDは特定の値を持つ。
【０７２９】
[781]例188は例187の主題を包括しており、ここでは特定の値が、階級、サブセット、最初の値を置き換える値の幅を含んでいる。
【０７３０】
[782]例189は例183の主題を包括しており、ここでは、最初のユーザーからのプライバシーポリシーへの対策の要求、データ主体の最初の複数性に関連するデータ、最初の値に対する最初の要求のうち少なくとも一つがシムを介して受け取られる。
【０７３１】
[783]例190は例183の主題を包括しており、ここでは最初の値は類似識別子を含む。
【０７３２】
[784]例191は例190の主題を包括しており、ここでは類似識別子が構造化されていないデータを含む。
【０７３３】
[785]例192は例190の主題を包括しており、ここでは類似識別子が階級、集団、値の幅を含む。
【０７３４】
[786]例193は例183の主題を包括しており、ここではプライバシーポリシーが統合データの生成を規定する。
【０７３５】
[787]例194は例193の主題を包括しており、ここではプライバシーポリシーが統合データのためのDDIDsの生成をさらに指定する。
【０７３６】
[788]例195は例183の主題を包括しており、ここでは最初のユーザーから得られたデータのうち少なくともいくつかが統合データを規定する。
【０７３７】
[789]例196は例183の主題を包括しており、ここでは最初のユーザーから得られたデータが単体で統合データを規定する。
【０７３８】
[790]例197はシステムで、次の構成を含む。ネットワーク経由でデータを送信する通信インターフェース、コンピュータプログラムコードとデータ記録が可能な分散型台帳を持つ内臓メモリー、そしてメモリと接続され、コンピュータプログラムコードの指示を実行するよう設定された一つ以上のプロセスユニットである。そのプログラムコードによって、一つ以上のプロセスユニットは、以下の動作を行う。最初のデータ主体に関連した最初のユーザーからデータを取得し、最初のデータ主体のための、最初の動的に変化する一時的なユニーク識別子(DDID)を生成する。ここでは、DDIDは、最初のデータ主体に関連する最初の値を置き換えるために集約される。そして、最初のDDIDを一つ以上の分散型台帳の最初の台帳の最初の要素に保存し、最初の要求者からの、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、最初の要求者が最初の値を受け取ることをオーソライズさていない場合、最初のDDIDを最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信し、そして、最初の要求者が最初の値を受け取ることをオーソライズさている場合、最初のデータ主体に関連した最初の値を、最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信する。
【０７３９】
[791]例198は例197の主題を包括しており、ここでは、ネットワークが分散されており

、ネットワークがノードの複数性を含み、ネットワークがそれぞれのノードに一つ以上の分散型台帳の最初のコピーを保存する。

【０７４０】

[792]例199は例198の主題を包括しており、ここでは、一つ以上の分散型台帳の最初のものがblockchainを含み、最初の要素が最初のブロックを含む。

【０７４１】

[793]例200は例197の主題を包括しており、ここでは、一つ以上のプロセスユニットがコンピュータプログラムコード内の指示を実行するために集約され、そのコードによって、一つ以上のプロセスユニットは、プライバシーポリシーへの対策として最初のユーザーからリクエストを取得し、少なくとも部分的にはリクエストを基にした最初のプライバシーポリシーを決定する。ここにおいて、最初のDDID は決定された最初のプライバシーポリシーを満たすために集約される。

【０７４２】

[794]例201は例197の主題を包括しており、ここでは最初のDDID が最初のデータ主体に関連する最初の値を含む保管場所を示す。

【０７４３】

[795]例202は例201の主題を包括しており、ここでは一つ以上のプロセスユニットがコンピュータプログラムコード内の指示を実行するために集約され、そのコードによって、一つ以上のプロセスユニットは、データ主体に関連した最初の値を最初の修正値に変更するために、最初のユーザーからリクエストを取得し、データ主体に関連した最初の値を含む保管場所に、最初の修正値を保存する。

【０７４４】

[796]例203は例197の主題を包括しており、ここでは最初のデータ主体がスマートコントラクトの最初の実行可能な期間を含む。

【０７４５】

[797]例204はコンピュータにより実施される手法の構成で、最初のデータ主体に関連した最初のユーザーからデータを取得し、最初のデータ主体のための、最初の動的に変化する一時的なユニーク識別子(DDID)を生成する。ここでは、DDIDは、最初のデータ主体に関連する最初の値を置き換えるために集約される。そして、最初のDDIDを一つ以上の分散型台帳の最初の台帳の最初の要素に保存し、最初の要求者からの、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、最初の要求者が最初の値を受け取ることをオーソライズさていない場合、最初のDDIDを最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信し、そして、最初の要求者が最初の値を受け取ることをオーソライズさている場合、最初のデータ主体に関連した最初の値を、最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信する。

【０７４６】

[798]例205は例204の主題を包括しており、ここでは、ネットワークが分散されており、ネットワークがノードの複数性を含み、ネットワークがそれぞれのノードに一つ以上の分散型台帳の最初のコピーを保存すし、一つ以上の分散型台帳の最初のものがblockchainを含み、最初の要素が最初のブロックを含む。

【０７４７】

[799]例206は例204の主題を包括しており、ここでは、プライバシーポリシーへの対策として最初のユーザーからリクエストを取得し、少なくとも部分的にはリクエストを基にした最初のプライバシーポリシーを決定する。ここにおいて、最初のDDID は決定された最初のプライバシーポリシーを満たすために集約される。

【０７４８】

[800]例207は例204の主題を包括しており、ここでは最初のDDID が最初のデータ主体に関連する最初の値を含む保管場所を示す。

【０７４９】

[801]例208は例207の主題を包括しており、ここでは、データ主体に関連した最初の値

を最初の修正値に変更するために、最初のユーザーからリクエストを取得し、データ主体に関連した最初の値を含む保管場所に、最初の修正値を保存する。

【０７５０】

[802]例209は例204の主題を包括しており、ここでは最初のデータ主体がスマートコントラクトの最初の実行可能な期間を含む。

【０７５１】

[803]例210は恒久的なプログラムストレージデバイスで、プログラマブルコントロールデバイスによって判読可能であり、格納された指示で構成される。その指示が実行されることでプログラマブルデバイスは以下の動作を行う。最初のデータ主体に関連した最初のユーザーからデータを取得し、最初のデータ主体のための、最初の動的に変化する一時的なユニーク識別子(DDID)を生成する。ここでは、DDIDは、最初のデータ主体に関連する最初の値を置き換えるために集約される。そして、最初のDDIDを一つ以上の分散型台帳の最初の台帳の最初の要素に保存し、最初の要求者からの、最初のデータ主体に関連する最初の値に対する、最初の要求をネットワーク上で受信し、最初の要求者が最初の値を受け取ることをオーソライズさていない場合、最初のDDIDを最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信し、そして、最初の要求者が最初の値を受け取ることをオーソライズさている場合、最初のデータ主体に関連した最初の値を、最初のリクエストに応じて、ネットワーク上で最初の要求者へ送信する。

【０７５２】

[804]例211は例210の主題を包括しており、ここでは、ネットワークが分散されており、ネットワークがノードの複数性を含み、ネットワークがそれぞれのノードに一つ以上の分散型台帳の最初のコピーを保存する。

【０７５３】

[805]例212は例210の主題を包括しており、ここでは、一つ以上の分散型台帳の最初のものがblockchainを含み、最初の要素が最初のブロックを含む。

【０７５４】

[806]例213は例210の主題を包括しており、ここでは、コンピュータプログラムコード内の指示により、プログラマブルコントロールデバイスは、プライバシーポリシーへの対策として最初のユーザーからリクエストを取得し、少なくとも部分的にはリクエストを基にした最初のプライバシーポリシーを決定する。ここにおいて、最初のDDID は決定された最初のプライバシーポリシーを満たすために集約される。

【０７５５】

[807]例214は例210の主題を包括しており、ここでは最初のDDID が最初のデータ主体に関連する最初の値を含む保管場所を示す。

【０７５６】

[808]例215Exampleは例214の主題を包括しており、ここでは、コンピュータプログラムコード内の指示により、プログラマブルコントロールデバイスは、データ主体に関連した最初の値を最初の修正値に変更するために、最初のユーザーからリクエストを取得し、データ主体に関連した最初の値を含む保管場所に、最初の修正値を保存する。

【０７５７】

[809]例216は例210の主題を包括しており、ここでは最初のデータ主体がスマートコントラクトの最初の実行可能な期間を含む。

【０７５８】

[810]本発明の方法論はこれまでに述べられ、特定の手順で特定の操作について触れ示されたが、これらの操作は組み合わせられ、小分類され、また本発明のsub-divided,手引きから乖離することなく、同様の手法に対して順序づけを変更したりされる。従って、特筆されることがない限り、操作の手順と組み合わせは本発明に限定したものではない。例えば、非限定的な他の実施例として、ここに述べられる操作量は、述べられたものと異なる手順で再配置され機能し得る。

【０７５９】

[811]この明細書において、必要に応じて本発明の少なくとも一つの実施例において、“一つの実施例”や“一例”という言及には、実施例に関して記述される特定の特質、構造、特徴が含まれると理解されたい。

【０７６０】

[812]ここで使用される“ブラウザ”という用語はウェブブラウザだけでなく、例えばX-Windowsで使用されるプログラマブルディスプレイエンジン、デスクトップのヴァーチャル化に使用される遠隔表示機器、テキスト、マルチメディアメッセージを他の当事者（例えは、フェイスブックメッセンジャー、ワッツアップ、スナップチャット、ウィッカー、サイバーダスト、その他のこういった機能を提供するユーザー・企業アプリケーション）で有効にする、アプリケーションやデバイスのユーザーインターフェースなどにも言及している。ここで使用される“ウェブ”という用語はワールドワイドウェブ（ＷＷＷ）だけでなく、例えば純粋に逐語的に連携したドキュメントや、複数の主体間または、単数の主体のみ（イントラネットなど）で拡散する、内部連携したデバイスなどにも言及している。 ここで使用される“デバイス”という用語は、例えばヴァーチャルマシン（VM）やnodeJSがホストするマイクロデバイスなどの実存または“仮想”のデバイスに言及している。サーバーは異なるコンピュータやデバイス上、または同じコンピューターデバイス内の複数の要素で構成される。同様に、クライアントは異なるコンピュータやデバイス上、または同じコンピューターデバイス内の複数の要素で構成される。サーバーとクライアントはインターネットのような媒体を介して通信するが、例えばリモートプロシージャコール（RPC）やオペレーションシステム・アプリケーションプログラミングインタフェース（APIs）も活用し通信する。

【０７６１】

[813]典型的な本発明の実施例、発明の様々な特徴についての上述の記載は、時に一つの実施例、図式または記述にまとめられており、それは、発明を効率化し、一つ以上の様々な発明点の理解を補助する目的である。しかしながら、本発明の手法は、主張されている発明が各々の主張において明確に列挙されているよりも多くの性能を必要とするという意図を反映させていると解釈されるものではない。むしろ、発前述の本発明の各実施例の全ての性能にみられる発明点は少なく、述べられている各実施例は一つ以上の発明的特徴を含み得る。

【０７６２】

[814]本発明は実施例に言及し詳細に示されており、本発明の真の趣旨および範囲から逸脱することなく、当業者は、形式と詳細にその他の様々な変化を与えることが可能であると考えられる。

【図面】

【図１】

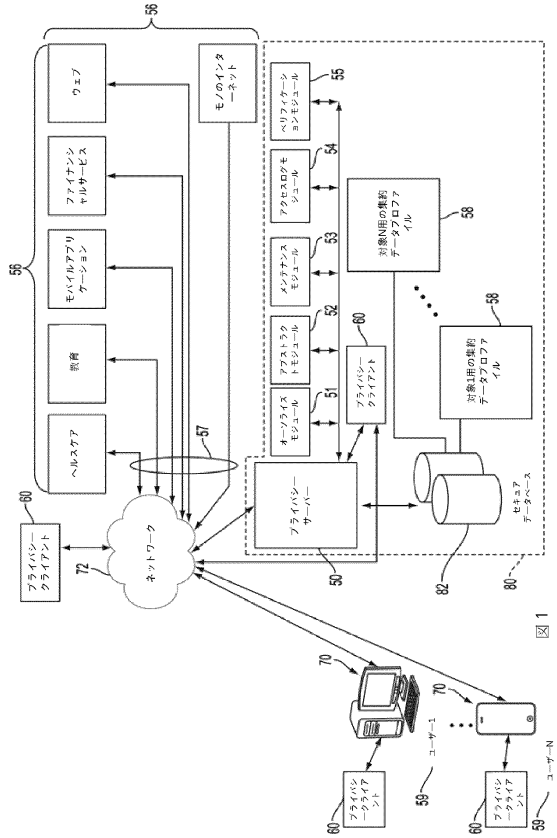


図１

【図１Ａ】

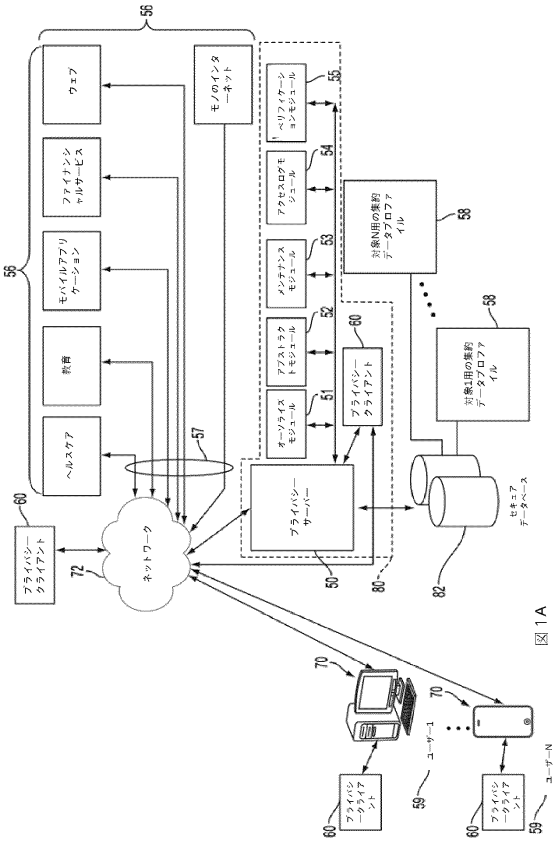


図１A

【図１Ｂ】

図１B

データトリビュートとアトリビュートの組み合わせについては、以下のいずれか、あるいはいくつかにおいて、DDIDの割り当て、適用、失効、再利用が起こる可能性がある。

1. 目的に基づく
   A. ブラウジング
   B. データ主題
   C. 処理
   D. その他
2. 物理的位置に基づく
   A. 入力
   B. 終了
   C. 変更
   D. 一般
   E. 具体
   F. その他
3. 仮想的位置に基づく
   A. 入力
   B. 終了
   C. 変更
   D. ページ
   E. サイト
   F. その他
4. 一時的な要因に基づく
   A. ランダム
   B. セット
   C. インターバル
   D. その他

【図１Ｃ－１】

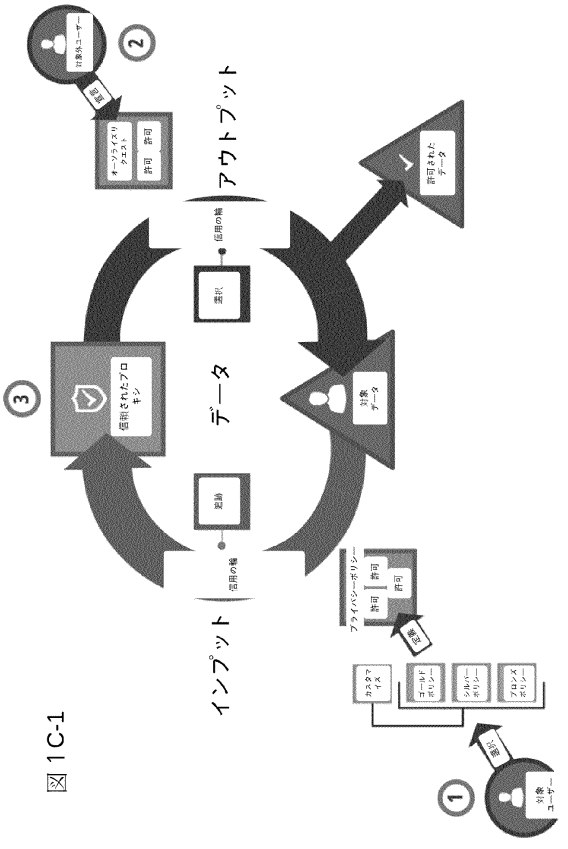


図1C-1

【図１Ｃ－２】

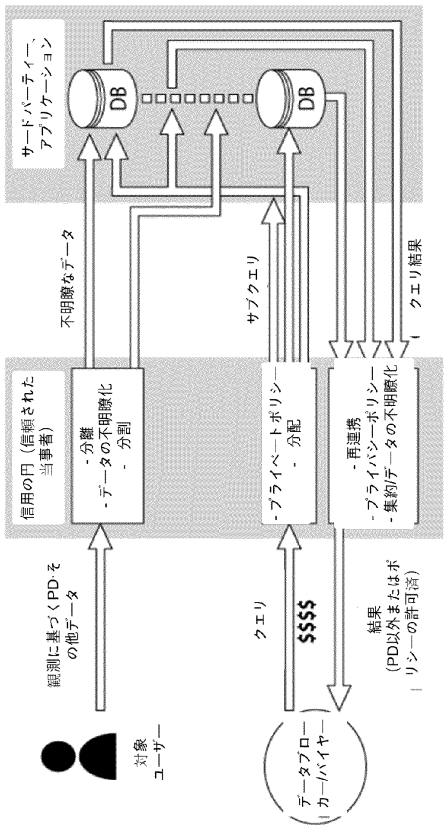


図 1C-2

【図１Ｄ】

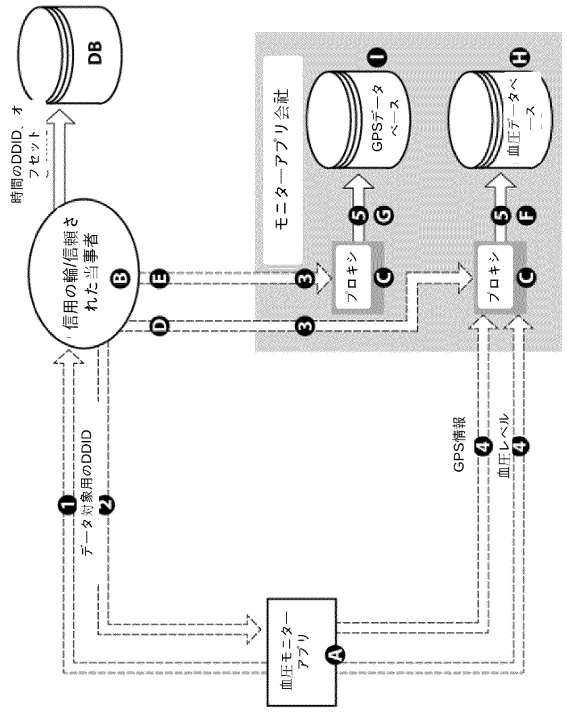


図 1D

【図１Ｅ】

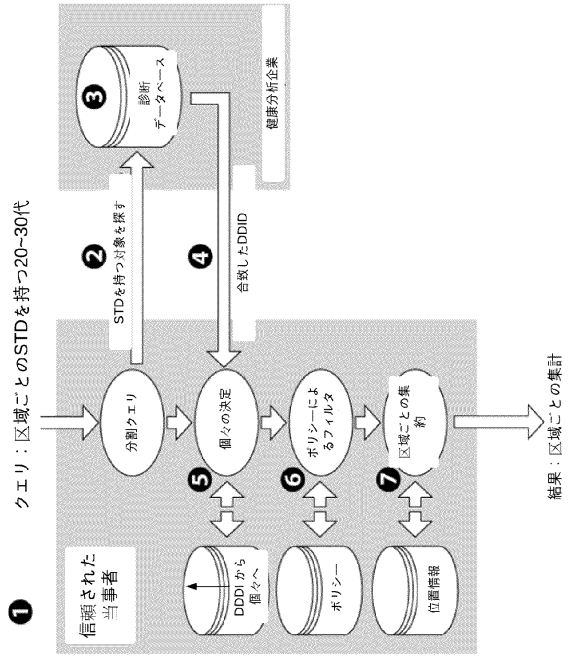


図 1E

【図１Ｆ】

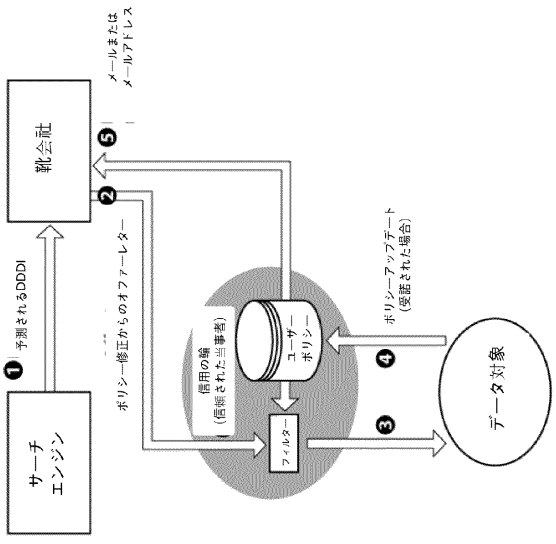


FIG. 1F

【図１Ｇ】

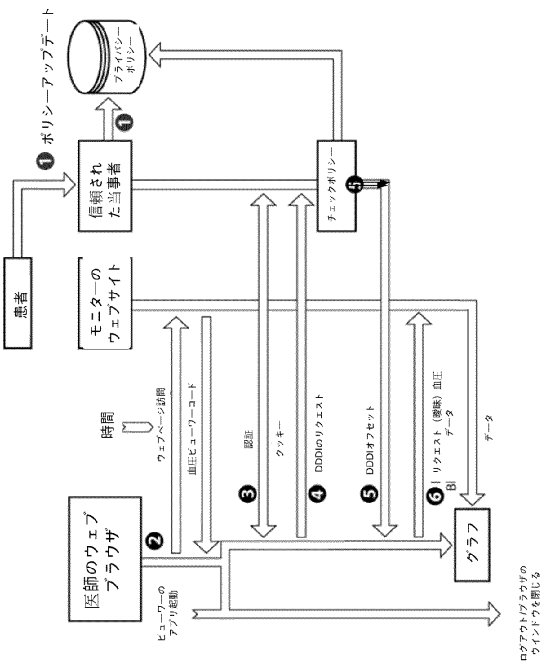


図1G

【図１Ｈ】

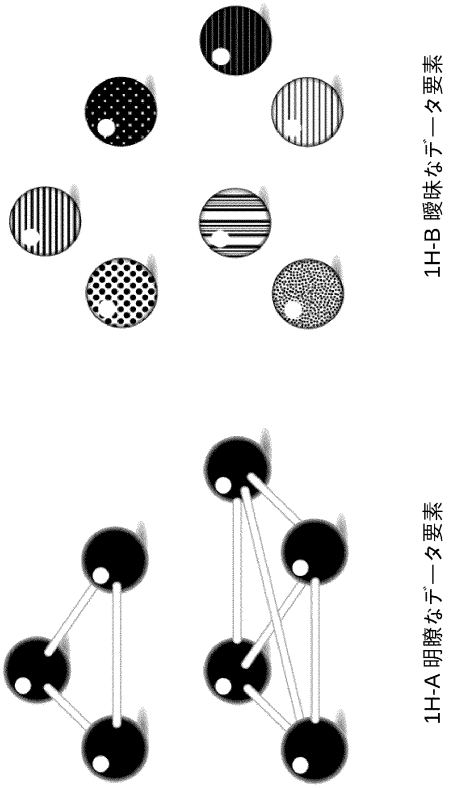


図1H

【図１Ｉ】

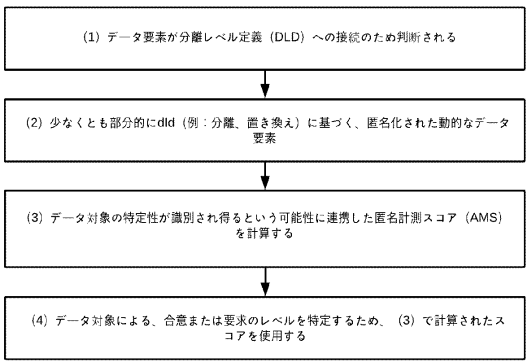


図1I

【図１Ｊ】

	非分離/置き換え	分離/置き換えレベル1	分離/置き換えレベル2	分離/置き換えレベル3
社会保障番号	100	90	81	40.5
クレジットカード番号	75	67.5	60.75	30.375
名	25	22.5	20.25	10.125
姓	25	22.5	20.25	10.125
生年月日	25	22.5	20.25	10.125
年齢	20	18	16.2	8.1
性別	10	9	8.1	4.05

レベル1=

DDIdは、当初割り当てられた数値を分離、置き換えそして保持する目的で割り当てられる。例：恒久的割り当て

レベル2=

DDIdは、当初割り当てられた数値を、数値が臨機応変に変更されるまで、分離、置き換えそして保持する目的で割り当てられる。例：臨機応変な変更可能性

レベル3=

DDIdは、当初割り当てられた数値を、数値がランダム、固定的、変更され得るあるいはその他の動的な要因で変更されるまで、分離、置き換えそして保持する目的で割り当てられる。例：動的な変更可能性

図1J

【図１Ｋ】

カテゴリA＝集計スコア75以上
カテゴリB＝集計スコア40から74.9
カテゴリC＝集計スコア39.9以下

カテゴリA＝データセットはデータ対象の現在の明確な合意表明をもって使用され得る

カテゴリB＝データセットはデータ対象の(i)現在または(ii)事前の合意表明をもって使用され得る

カテゴリC＝データセットはデータ対象の合意を求めずに使用され得る

図1K

【図１Ｌ】

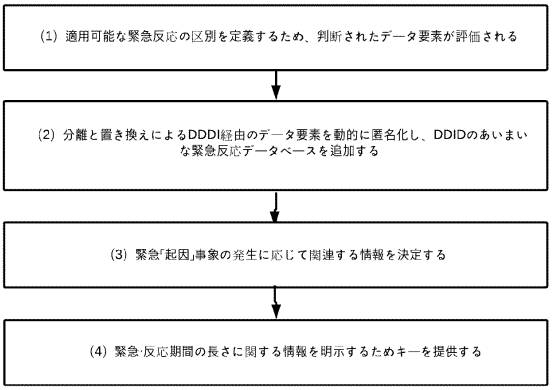


図1L

【図１Ｍ】

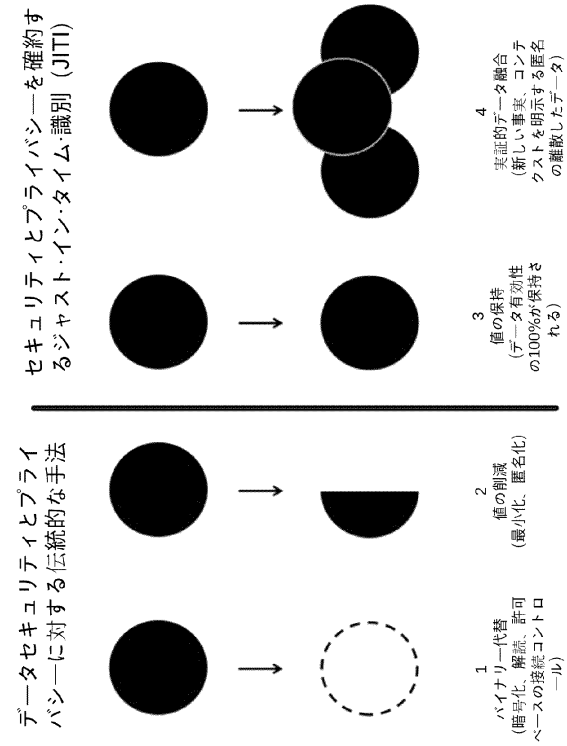


図1M

【図１Ｎ】

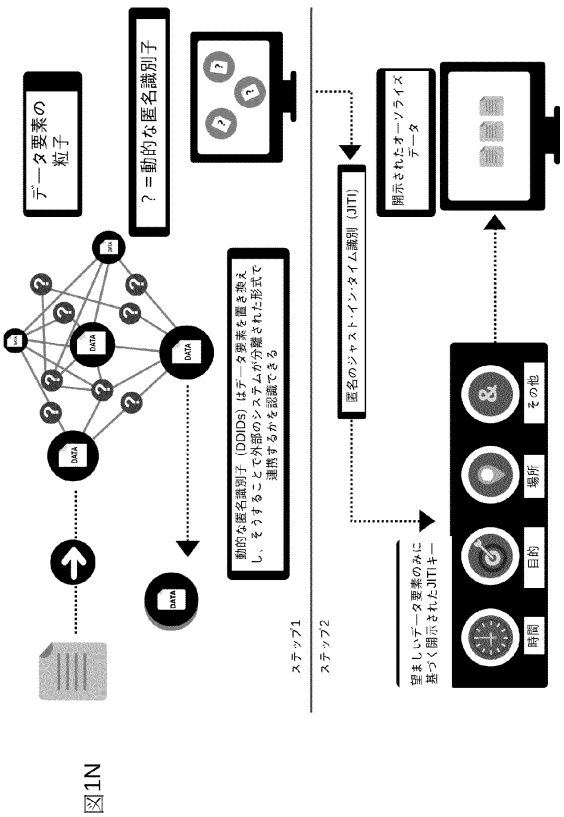


図1N

【図１Ｐ－１】

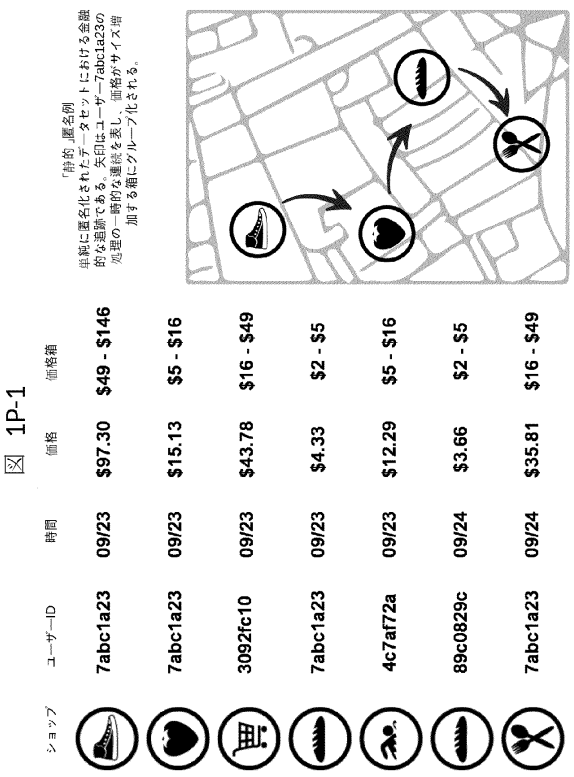


図 1P-1

【図１Ｐ－２】

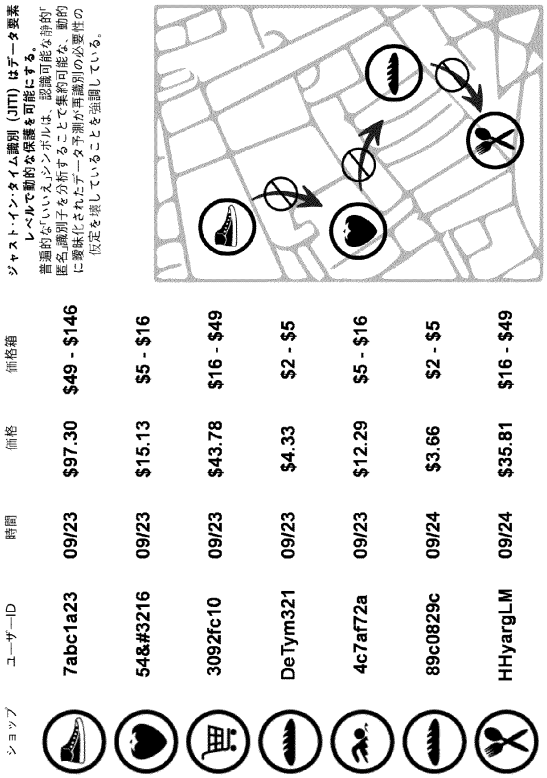


図 1P-2

【図１Ｑ】

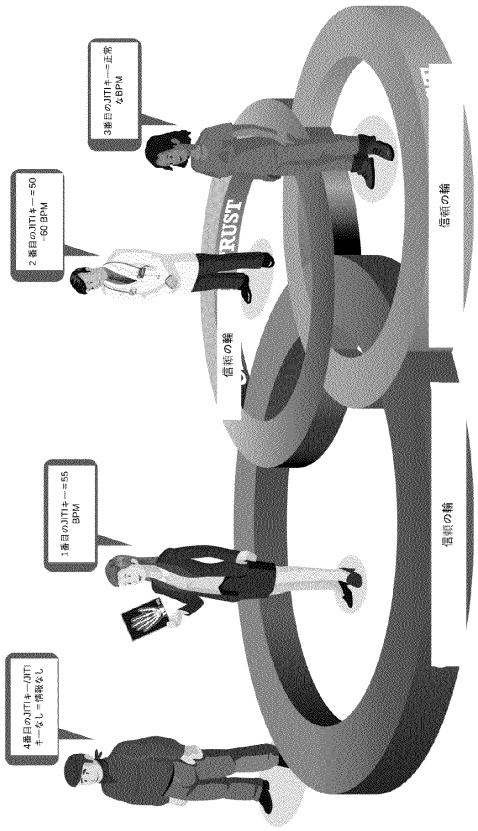


図 1Q

【図１Ｒ】

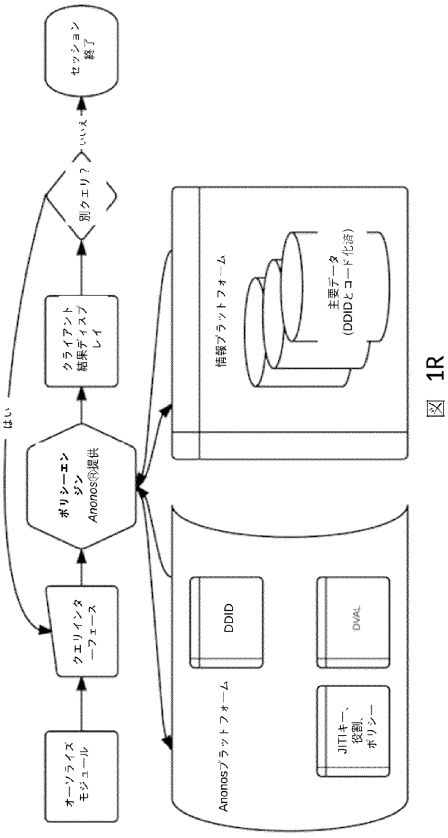


図 1R

【図１Ｓ】

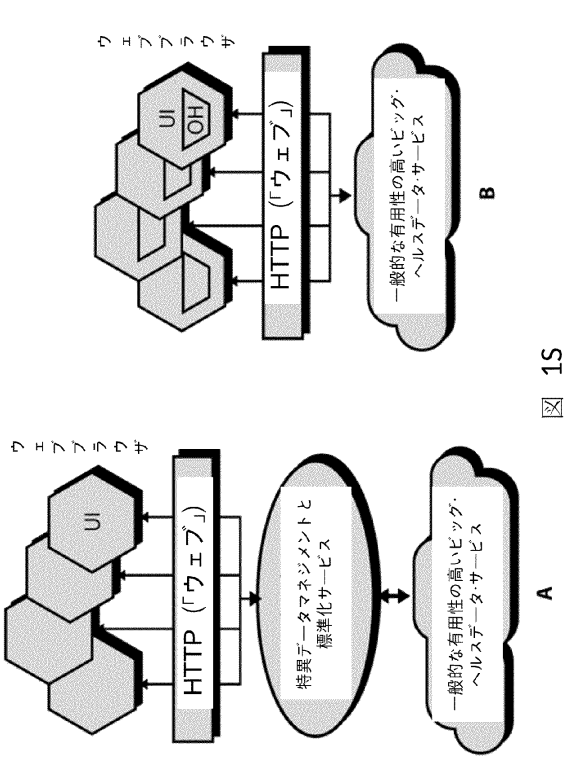


図 1S

【図１Ｔ】

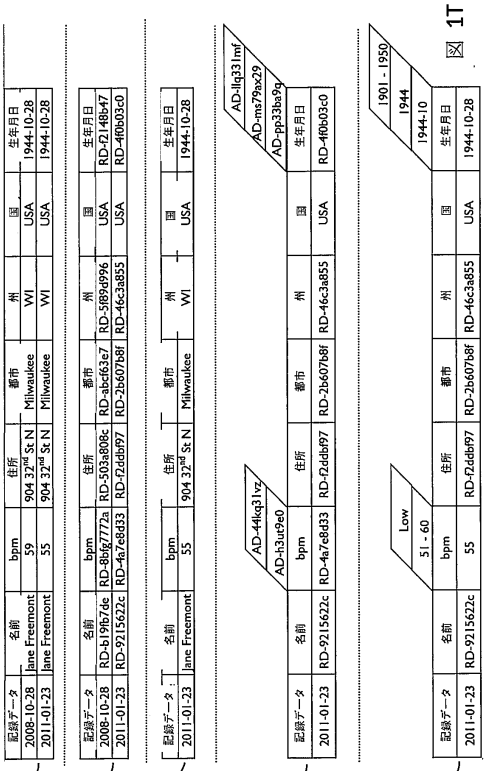


図 1T

【図１Ｕ】

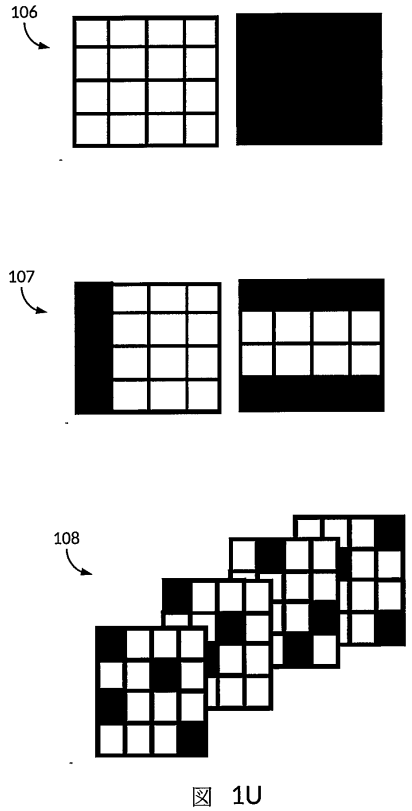


図 1U

【図１Ｖ】

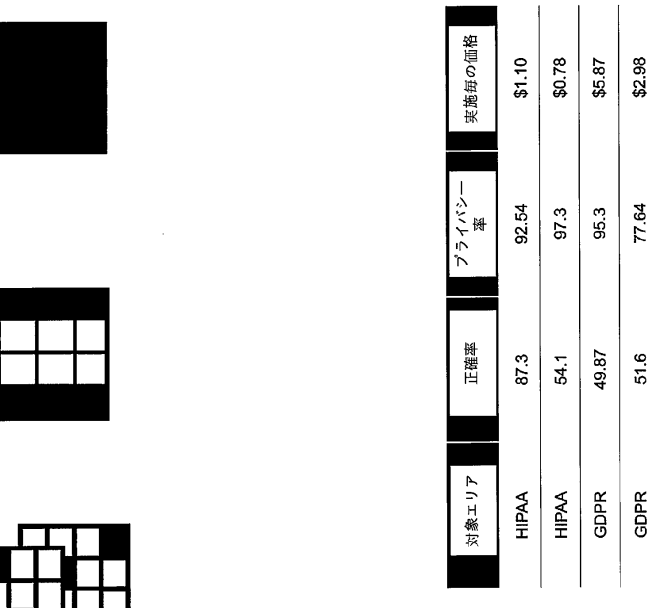


図 1V

【図１Ｗ－１】

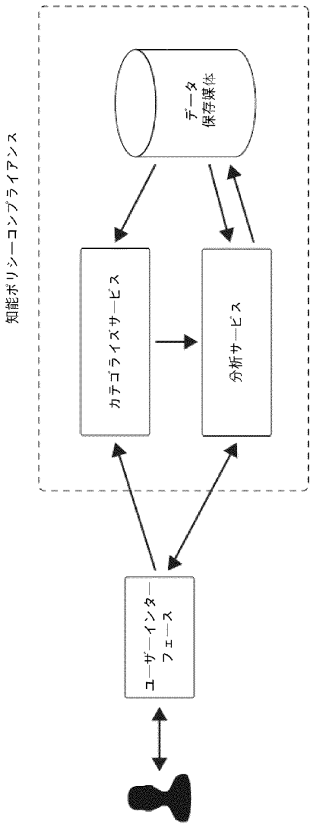


図 1W-1

【図１Ｗ－２】

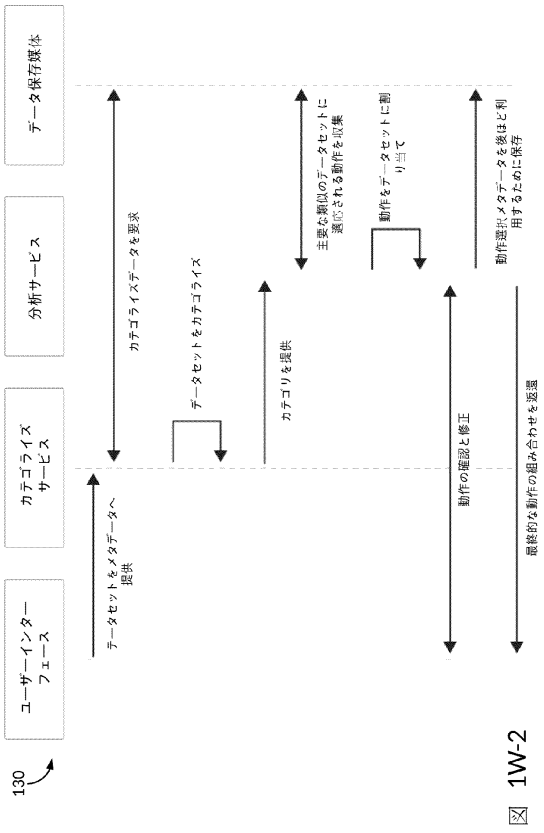


図 1W-2

【図１Ｘ－１】

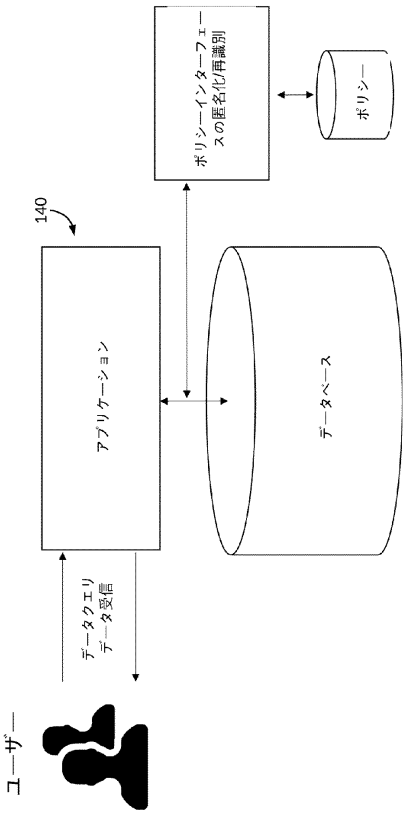


図 1X-1

【図１Ｘ－２】

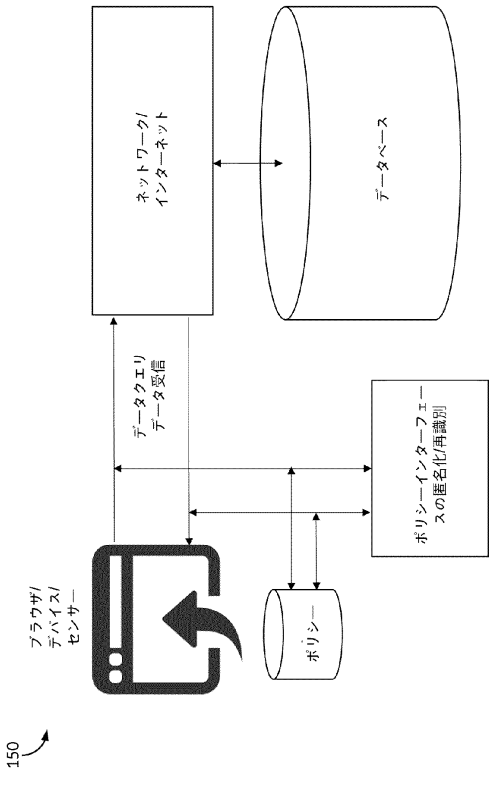


図 1X-2

【図１Ｙ－１】

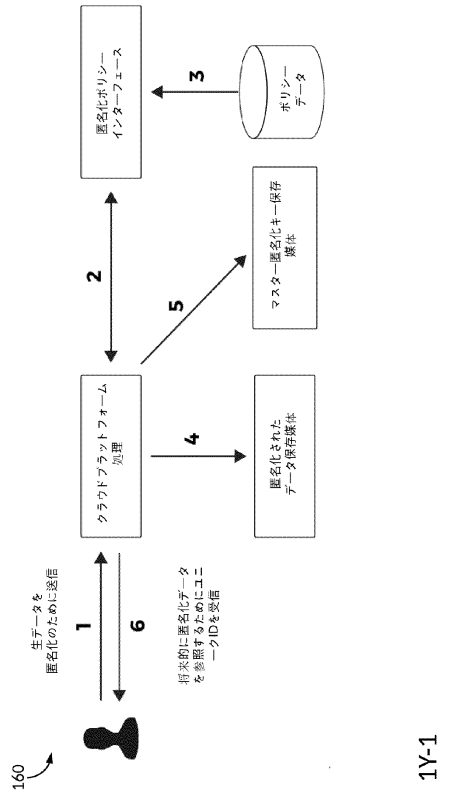


図 1Y-1

【図１Ｙ－２】

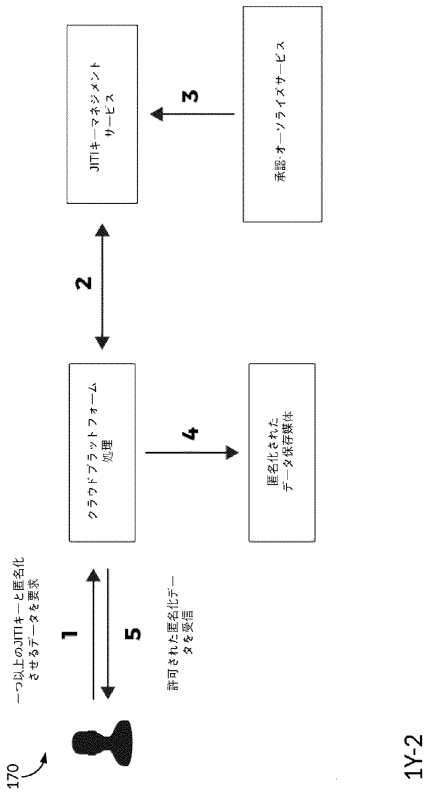


図 1Y-2

【図１Ｙ－３】

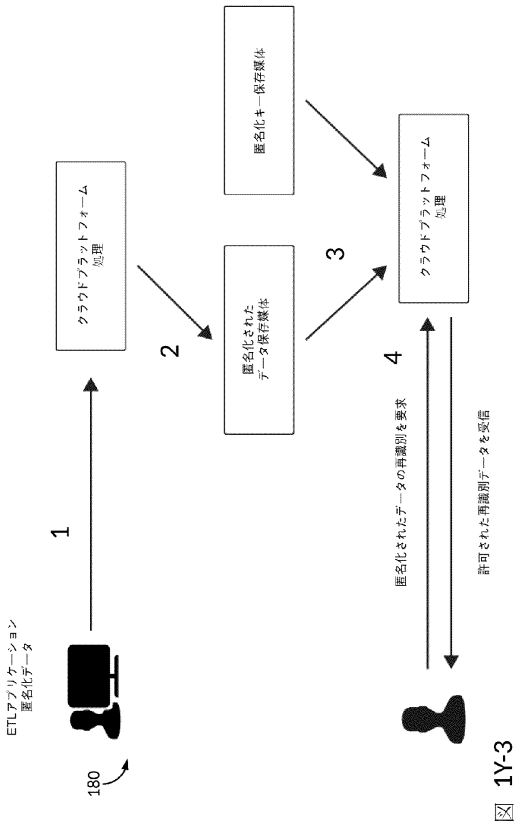


図 1Y-3

【図１Ｚ－１】

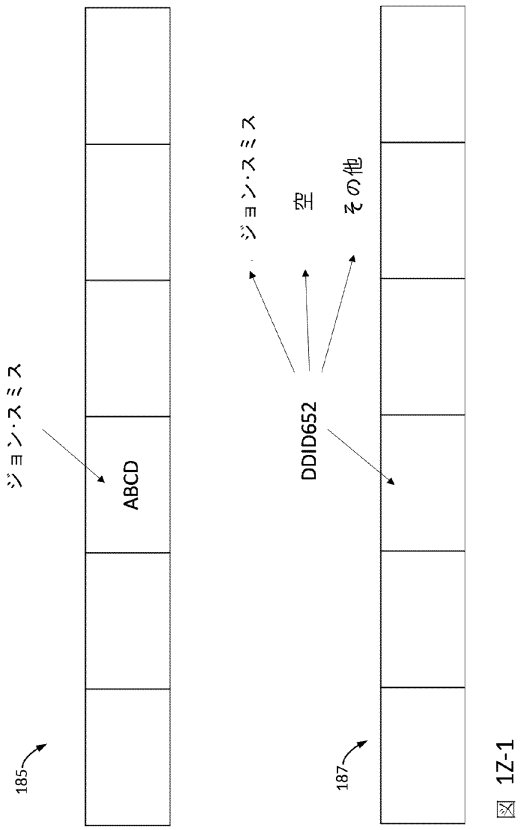


図 1Z-1

【図１Ｚ－２】

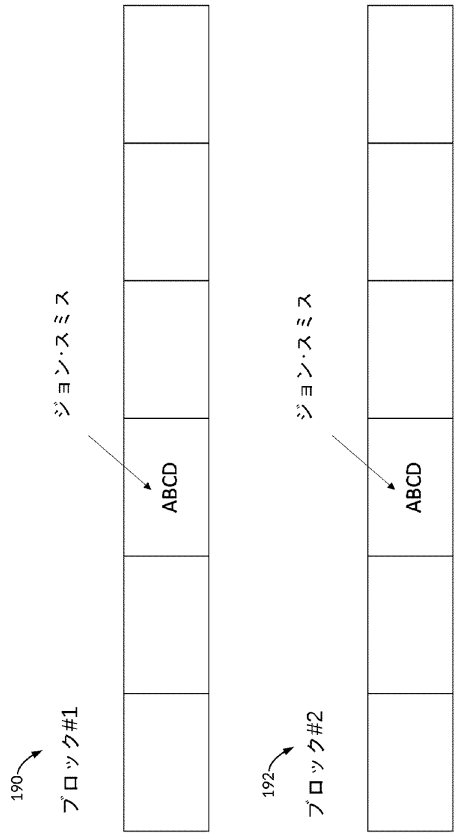


図 1Z-2

【図１Ｚ－３】

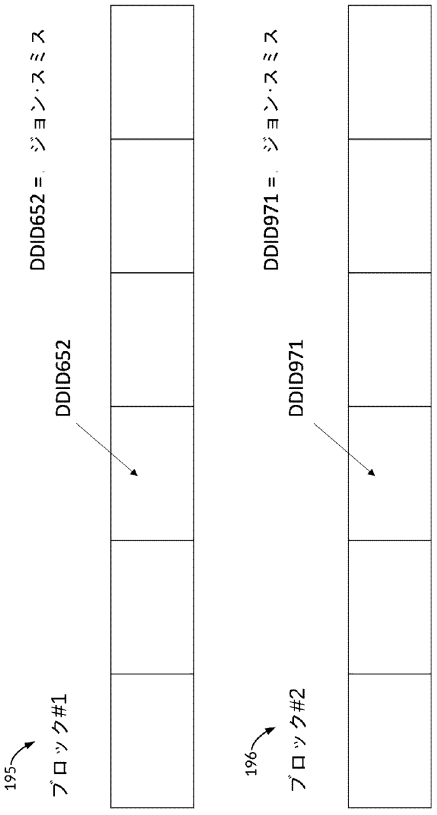


図 1Z-3

【図２】

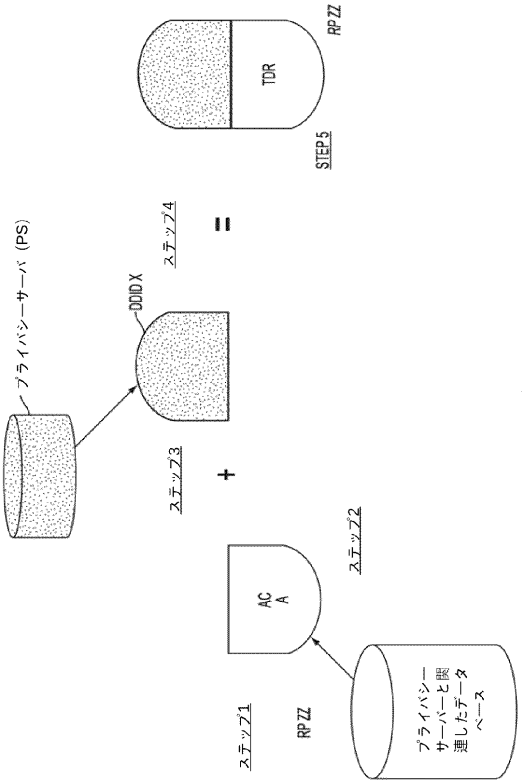


図 2

【図３】

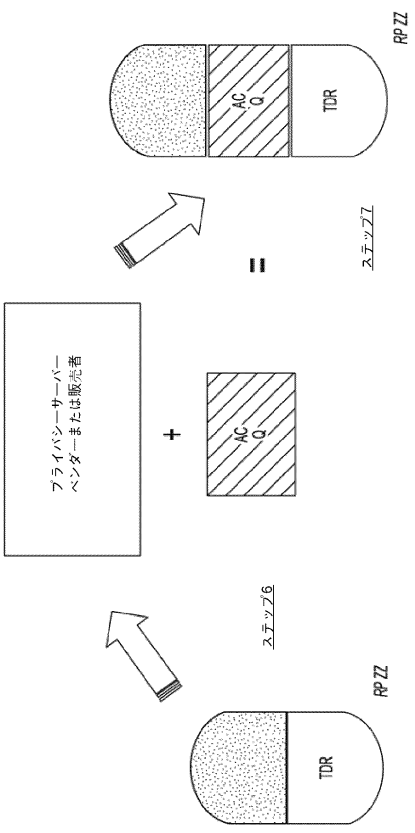


図 3

【図４】

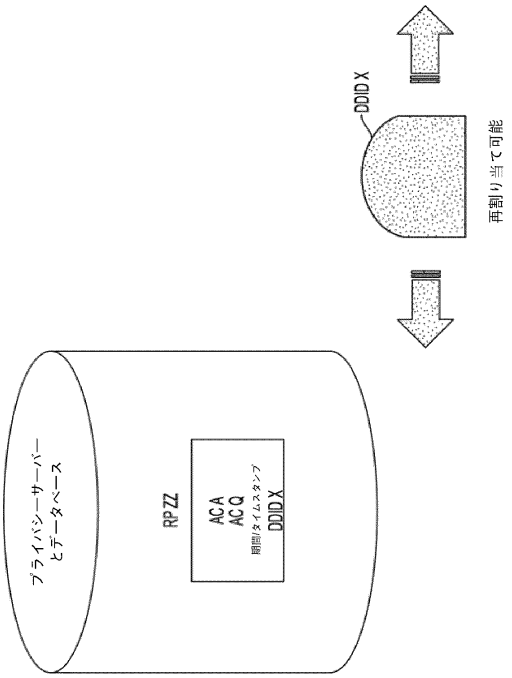


図 4

【図５】

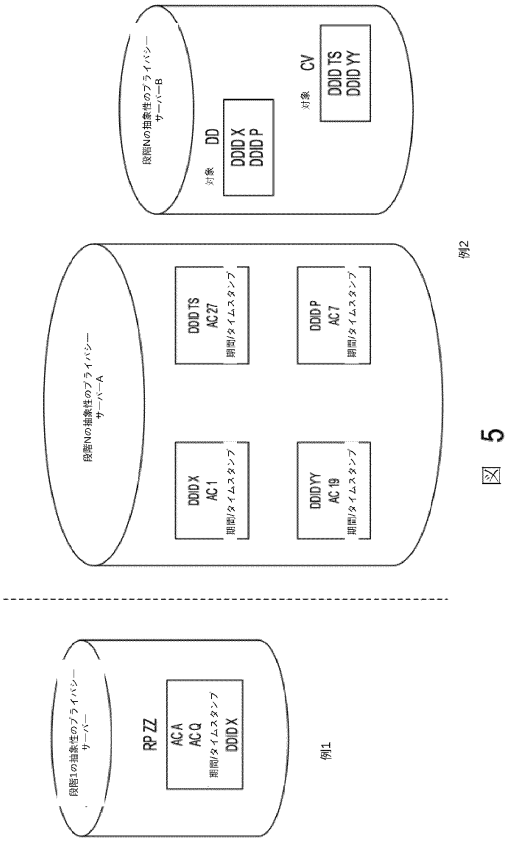


図 5

【図６】

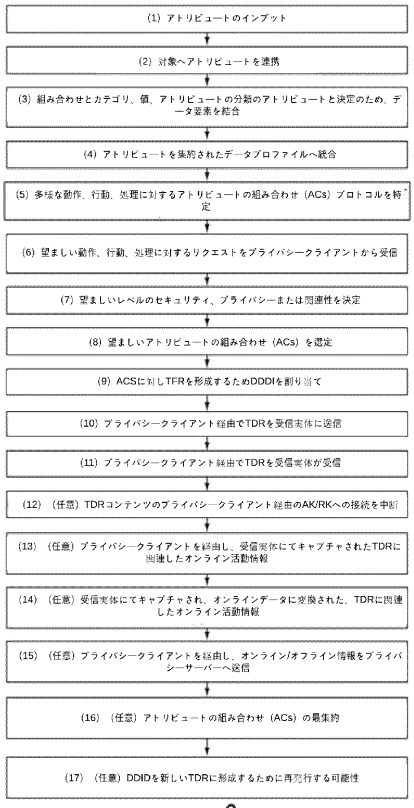


図 6

【図６Ａ】

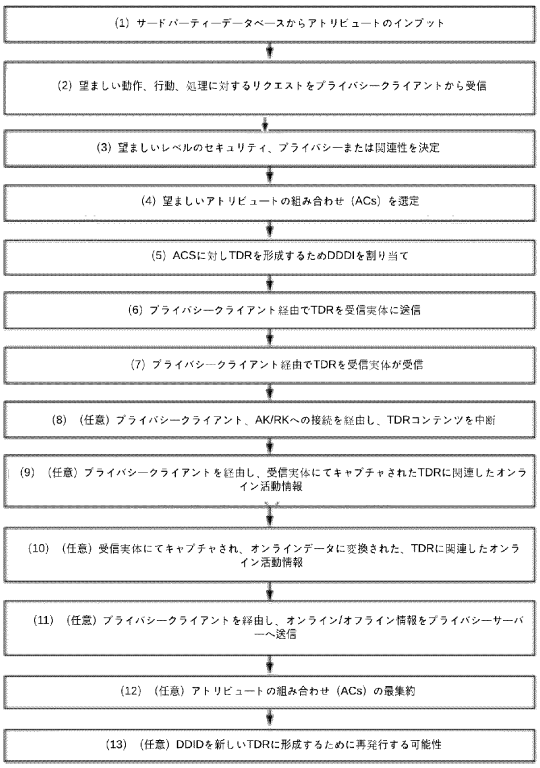


図 6A

【図６Ｂ】

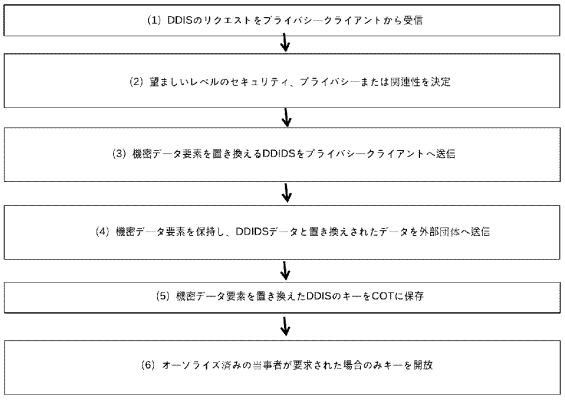


図 6B

【図７】

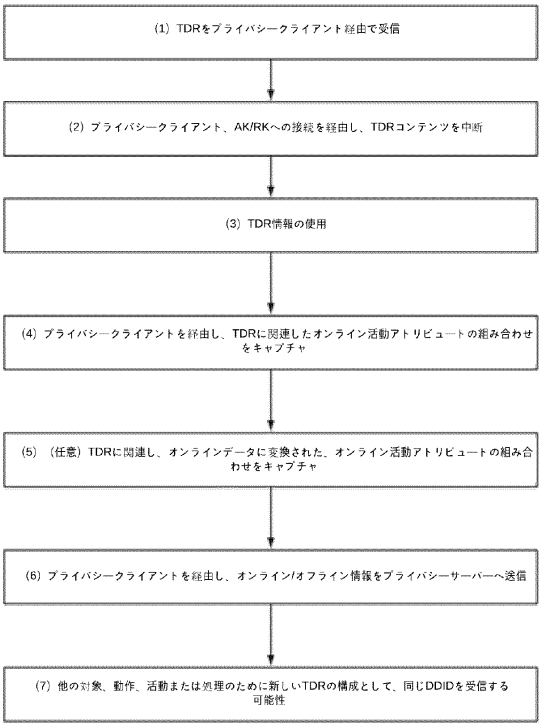


図 7

【図８】

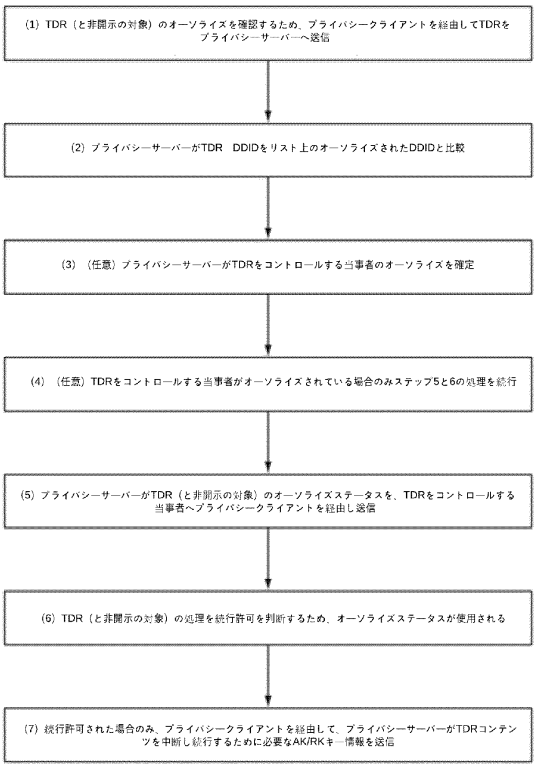


図 8

【図９】

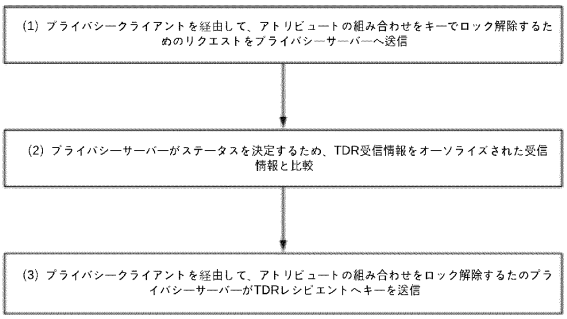


図 9

【図１０】

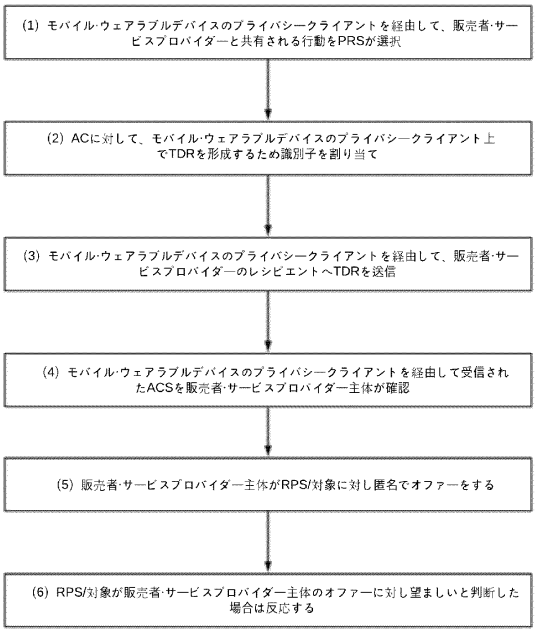


図 10

【図１１】

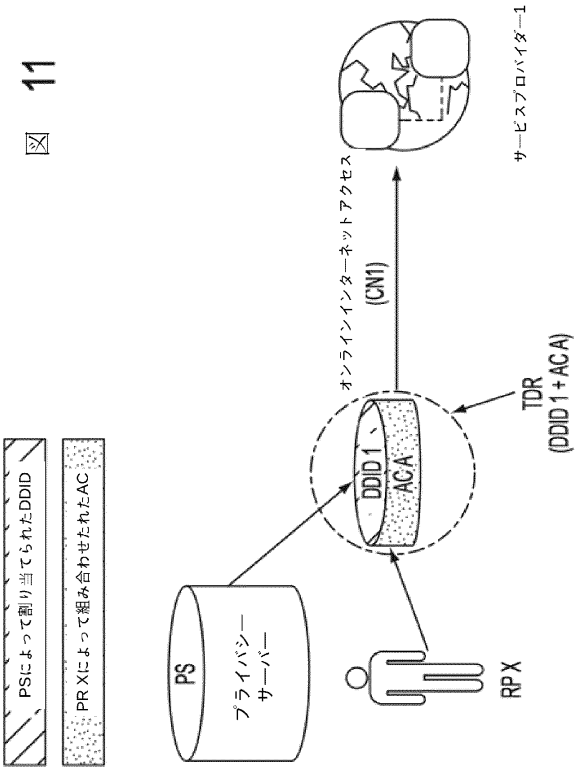


図 11

【図１２】

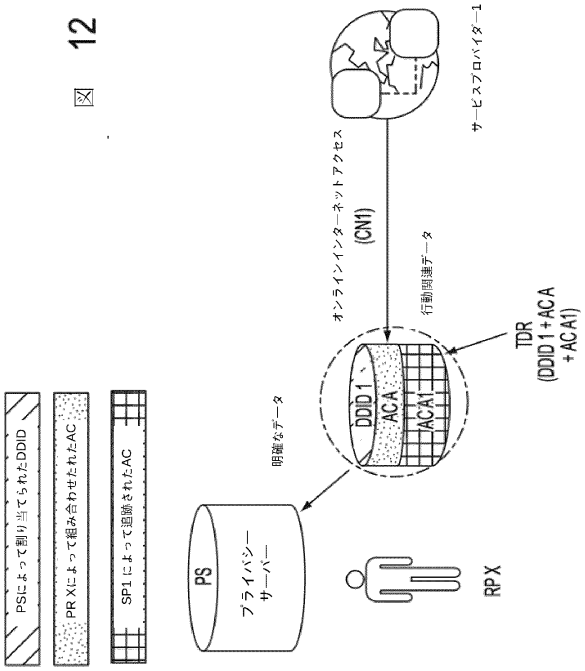


図 12

【図１３】

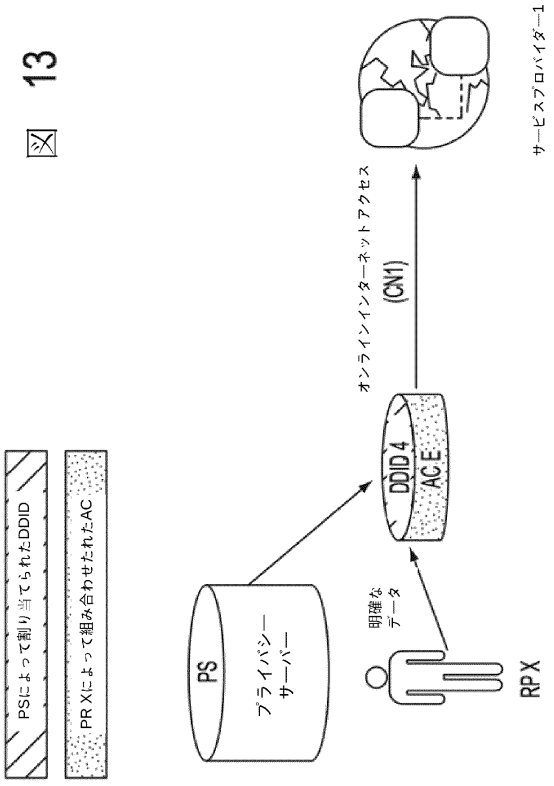
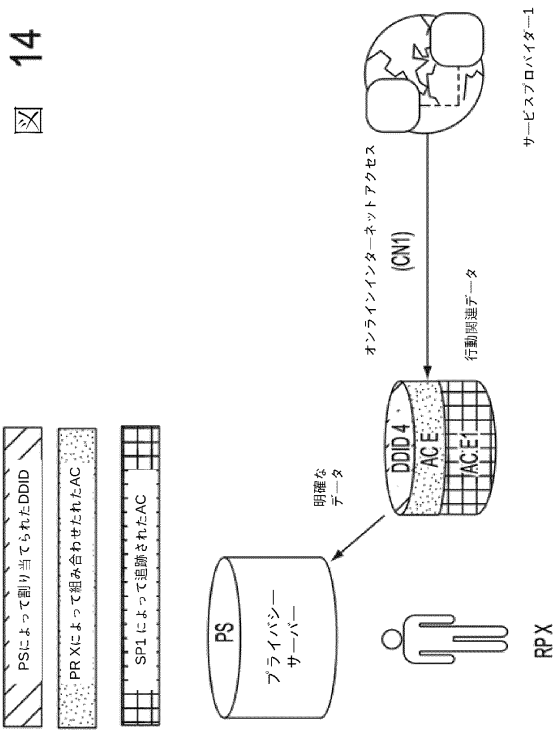
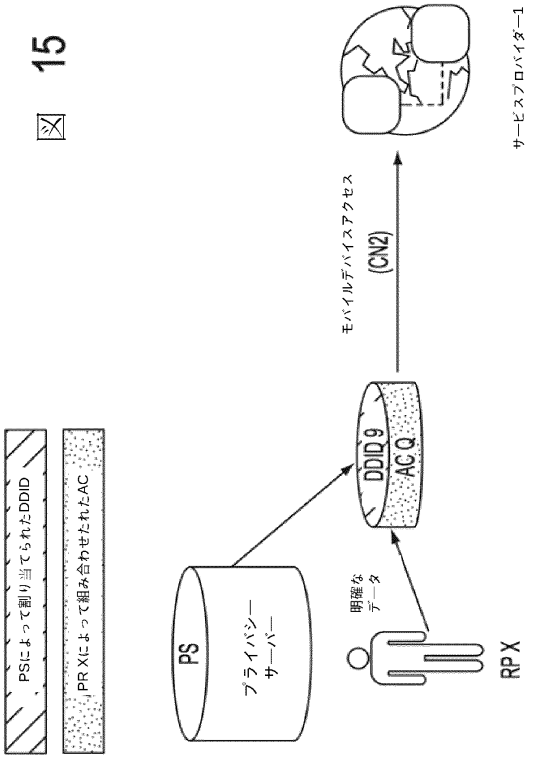


図 13

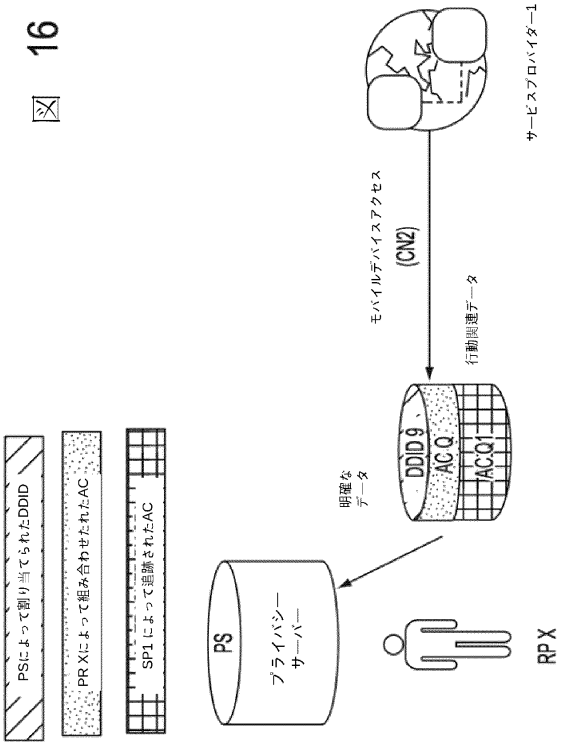
【図１４】



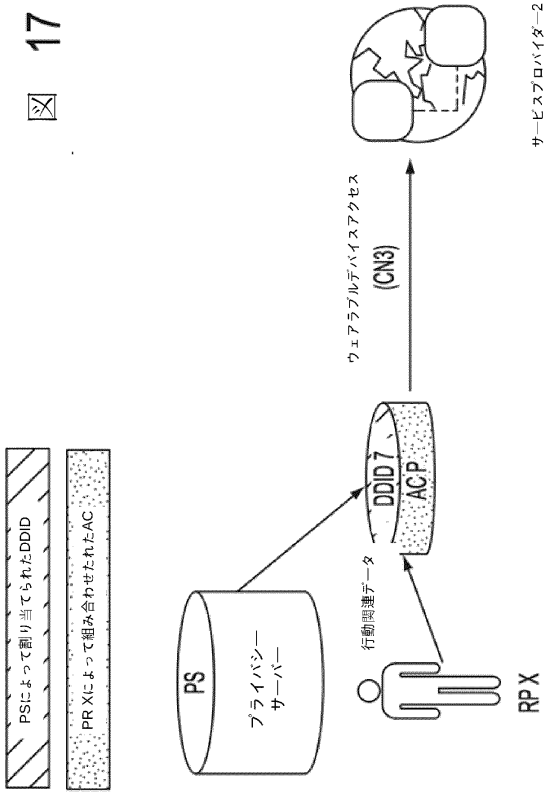
【図１５】



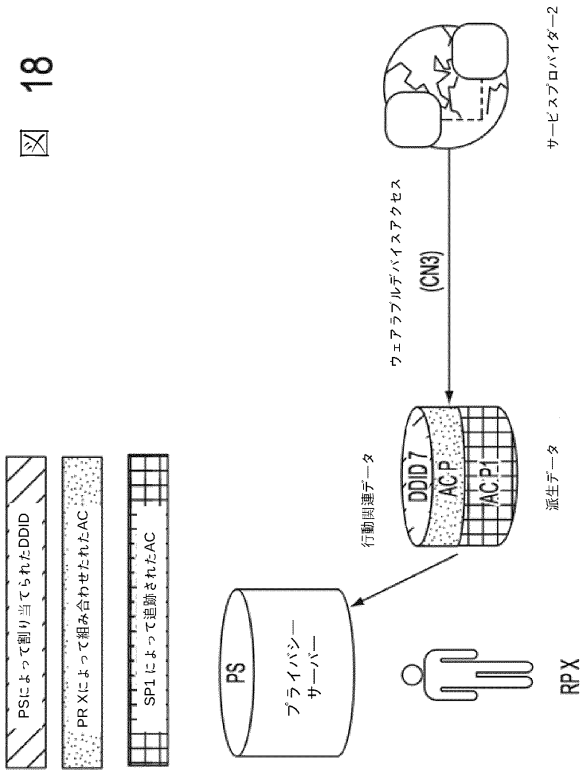
【図１６】



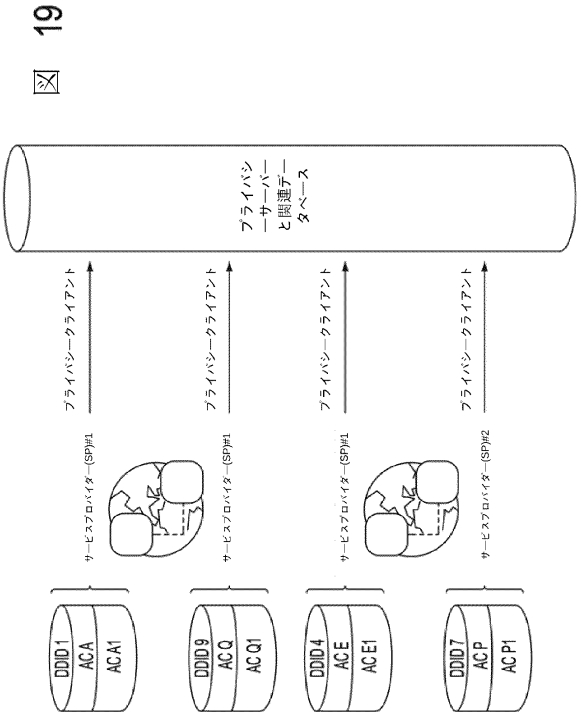
【図１７】



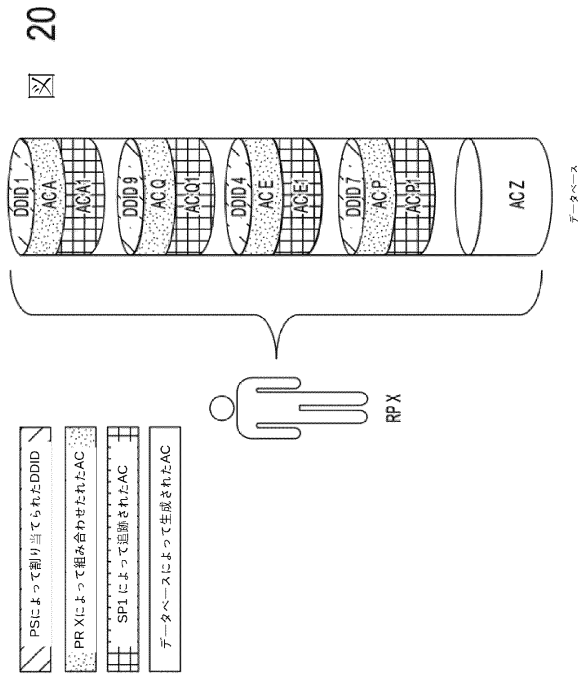
【図１８】



【図１９】



【図２０】



【図２１】

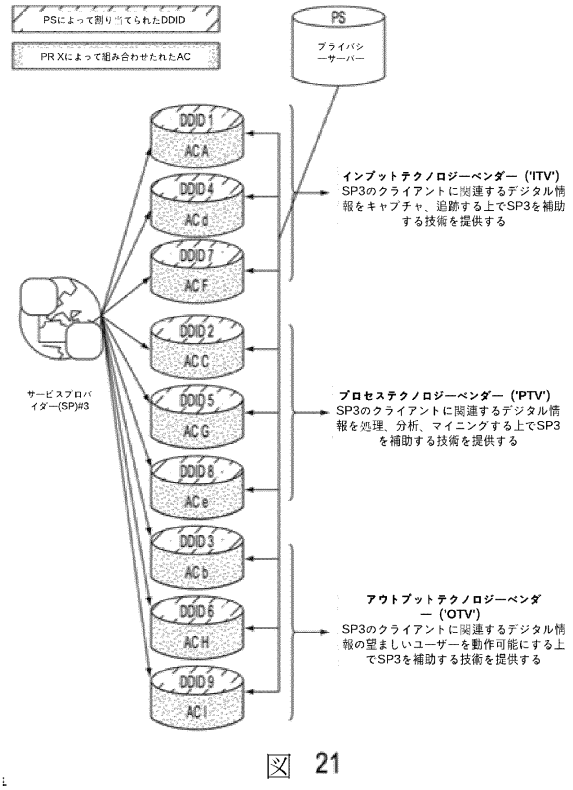


図 21

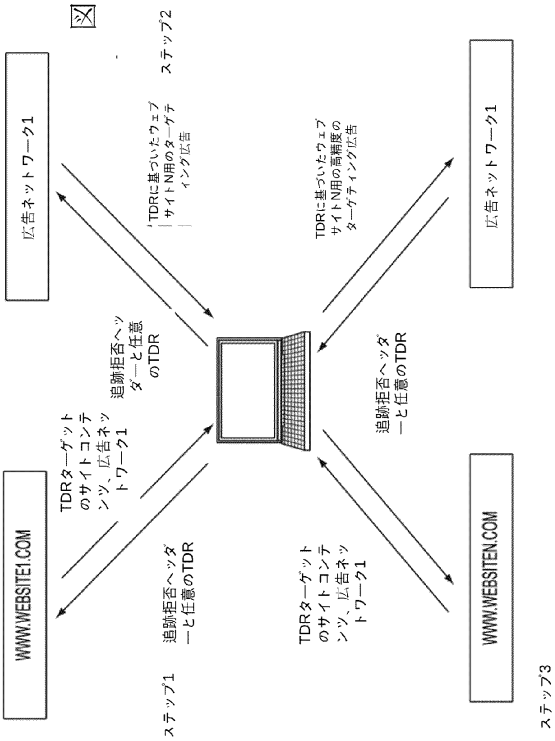
【図２２】

図 22

プライバシーサーバーと関連したデータベース	
アトリビュートの組み合わせ	DDIDS
インプットテクノロジープロバイダー	
A	1
d	4
F	7
プロセステクノロジープロバイダー	
C	2
G	5
e	8
アウトプットテクノロジープロバイダー	
b	3
H	6
I	9

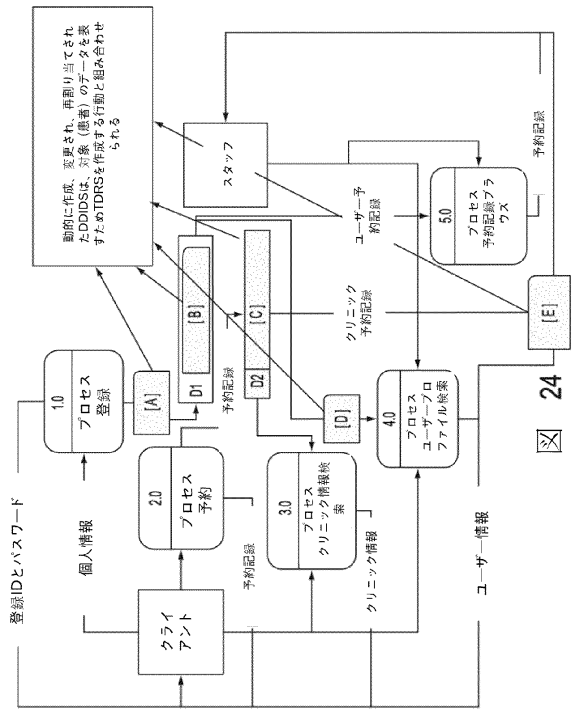
【図２３】

図 23



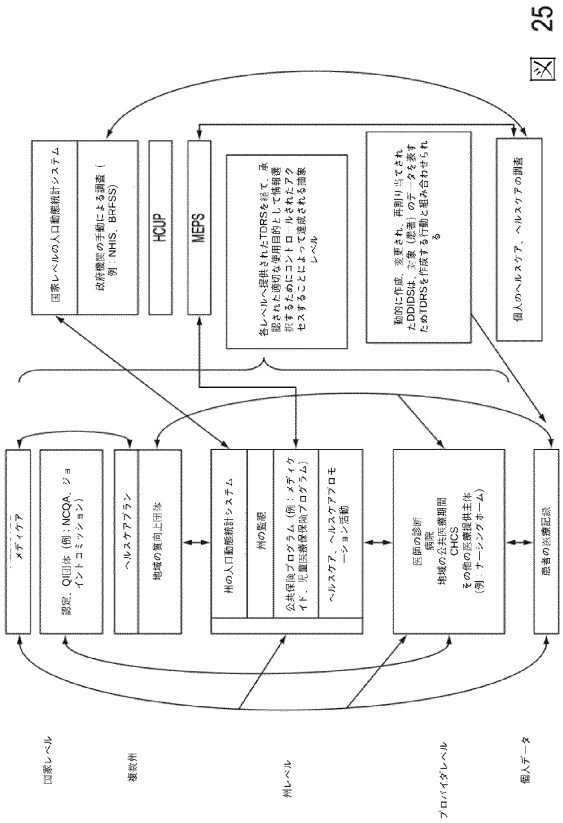
【図２４】

図 24



【図２５】

図 25



【図２６】

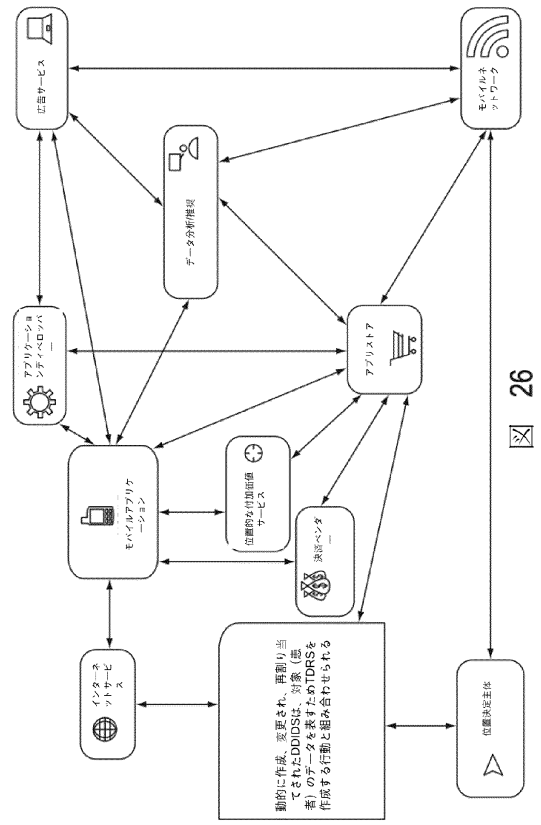


図 26

【図２７】

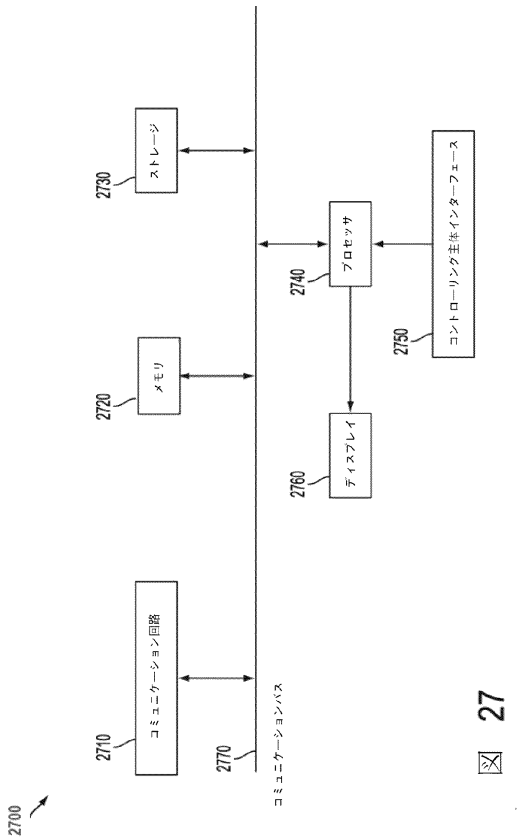


図 27

【図２８】

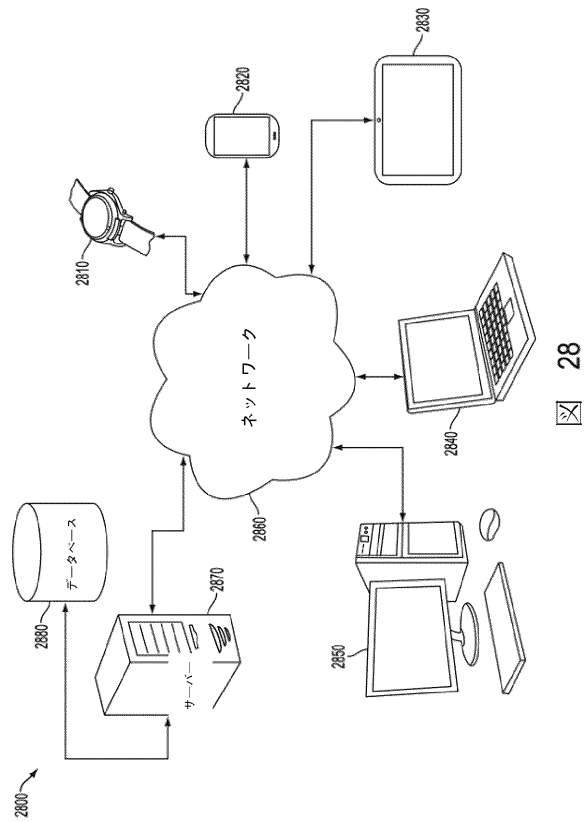


図 28

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 15/963,609
(32)優先日 平成30年4月26日(2018.4.26)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 62/580,628
(32)優先日 平成29年11月2日(2017.11.2)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 62/554,000
(32)優先日 平成29年9月4日(2017.9.4)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 62/644,463
(32)優先日 平成30年3月17日(2018.3.17)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 62/649,103
(32)優先日 平成30年3月28日(2018.3.28)
(33)優先権主張国・地域又は機関
米国(US)
前置審査
弁理士 西島 孝喜
(74)代理人 100109335
弁理士 上杉 浩
(74)代理人 100120525
弁理士 近藤 直樹
(74)代理人 100139712
弁理士 那須 威夫
(74)代理人 100176418
弁理士 工藤 嘉晃
(72)発明者 ラフィーバー マルコム ゲイリー
アメリカ合衆国 ニューヨーク州 １０００３－１５０２ ニューヨーク パーク アベニュー サウス ２２８ スイート ９６０４９
(72)発明者 マイヤーソン テッド エヌ
アメリカ合衆国 ニューヨーク州 １０００３－１５０２ ニューヨーク パーク アベニュー サウス ２２８ スイート ９６０４９
(72)発明者 メイソン スティーヴン
アメリカ合衆国 ニューヨーク州 １０００３－１５０２ ニューヨーク パーク アベニュー サウス ２２８ スイート ９６０４９
審査官 青木 重徳
(56)参考文献 米国特許出願公開第２０１５／０３７９３０３（ＵＳ，Ａ１）
米国特許出願公開第２０１６／０２９２６７２（ＵＳ，Ａ１）
特開２０１７－２０７９７９（ＪＰ，Ａ）
(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／６４
Ｇ０６Ｆ ２１／６２

G06F 21/31