

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2021年5月6日(06.05.2021)



(10) 国際公開番号

WO 2021/085519 A1

(51) 国際特許分類:
G06Q 50/10 (2012.01)

(21) 国際出願番号 : PCT/JP2020/040568

(22) 国際出願日 : 2020年10月29日(29.10.2020)

(25) 国際出願の言語 : 日本語

(26) 国際公開の言語 : 日本語

(30) 優先権データ :
特願 2019-198139 2019年10月31日(31.10.2019) JP

(71) 出願人: 国立大学法人大阪大学 (OSAKA UNIVERSITY) [JP/JP]; 〒5650871 大阪府吹田市山田丘1番1号 Osaka (JP).

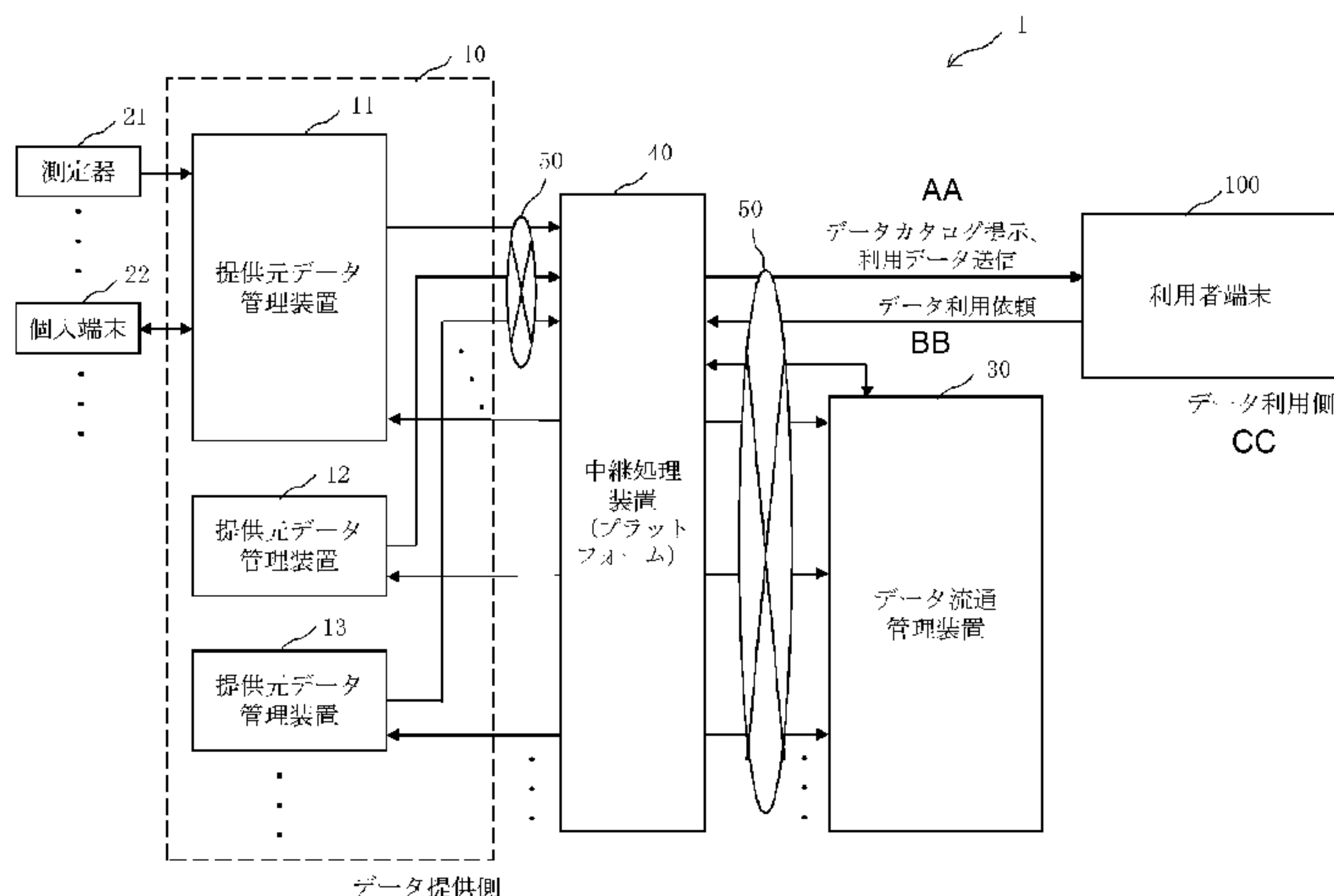
(72) 発明者: 八木 康史 (YAGI Yasushi); 〒5650871 大阪府吹田市山田丘1番1号 国立大学法人大阪大学内 Osaka (JP).

(74) 代理人: 特許業務法人 楓国際特許事務所 (KAEDE PATENT ATTORNEYS' OFFICE); 〒5400011 大阪府大阪市中央区農人橋1丁目4番34号 Osaka (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) Title: PERSONAL DATA DISTRIBUTION MANAGEMENT SYSTEM AND METHOD FOR SAME

(54) 発明の名称 : パーソナルデータ流通管理システム及びその方法



- 10 Data provision side
- 11, 12, 13 Provision source data management device
- 21 Measurement apparatus
- 22 Personal terminal
- 30 Data distribution management device
- 40 Relay processing device (platform)
- 100 User terminal
- AA Data catalog presentation, use data transmission
- BB Data use request
- CC Data use side

(57) Abstract: This personal data distribution management system (1) is independently provided with: provision source data management devices (11), (12), ..., a data distribution management device (30), and a relay processing device (40), which are connected on a network (50). The provision source data management device (11) is provided with a database (1103) which stores, as original data associated with personal real name information, personal data measured by a measurement apparatus (21) and attribute information related to the person and the measurement. The data distribution

MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告 (条約第21条(3))

management device takes in the original data except for the personal data and generates a data catalog. The relay processing device outputs, to a data user terminal (100), data except for the personal real name information from the database in each provision source data management device or the like on the basis of a data use request received from the outside. Accordingly, data distribution can be managed with reduced risk of leakage of the personal data or the personal real name information.

(57) 要約: パーソナルデータ流通管理システム(1)は、ネットワーク(50)上に接続された、提供元データ管理装置(11)、(12)、…と、データ流通管理装置(30)と、中継処理装置(40)とを個別に備える。提供元データ管理装置(11)は、測定器(21)で測定された個人のパーソナルデータ、個人及び測定に係る属性情報を個人の实名情報と対応付けた元データとして記憶するデータベース(1103)を備える。データ流通管理装置は、パーソナルデータを除く元データを取り込んでデータカタログが生成される。中継処理装置は、外部から受け付けたデータ利用依頼に基づいて、各提供元データ管理装置等のデータベースから個人の实名情報を除いたデータをデータ利用者端末(100)に出力する。これにより、パーソナルデータや個人の实名情報の情報漏洩に対するリスクを低減したデータ流通管理が可能となる。

明 細 書

発明の名称： パーソナルデータ流通管理システム及びその方法

技術分野

[0001] 本発明は、複数の個人から収集したパーソナルデータの流通を管理するパーソナルデータ流通管理の技術に関する。

背景技術

[0002] データが主導する経済成長と社会変革の実現においては、ビッグデータの利活用が鍵を握る。ビッグデータとして、特にパーソナルデータに対して注目が集まっている。パーソナルデータを使うことで、例えば、医療の進展や健康の増進などの様々な人々の利益に供することができること、また、各個人に向けたサービスもその対象となる個人のパーソナルデータを使って、より個人にマッチした質の高いサービスが構築できること、パーソナルデータを用いることで有効性の高いマーケティングができることなどが期待されている。

[0003] 2017年6月9日、「未来投資戦略2017」の中で、日本国内で業種・業界を超えてデータ流通・活用を促すための3つの具体的施策を推進することを閣議決定した。その施策とは、（1）産業データの連携・活用、（2）パーソナルデータの利活用、（3）民間企業分野のデジタルトランスフォーメーションの促進である。日本では、パーソナルデータの適正な利活用と適切な保護、また両者の間のバランスをとった取扱いを行うために、パーソナルデータストア（PDS）、情報銀行、データ取引市場といった仕組みが提案されている。2019年、情報銀行及びデータ取引市場の事例が徐々に始めてきた。PDSと情報銀行は、個人データの本人同意・ビッグデータ化を促す仕組みであり、データ取引市場は、流通・活用を促すためのマッチングに関する重要な仕組みに位置付けられる。

[0004] パーソナルデータは、個人が企業のサービスを利用するたびに、企業が取得することになるため、企業が管理する情報システムで管理・蓄積されてい

ることが多い。しかし、本来は個人のものであり、個人自らの判断でデータを蓄積・管理し、情報の存在事実も把握しているべきという考え方が社会通念としてあるため、個人データの流通は個人起点で実現する方向（データのポータビリティ）で検討が進められている。個人が企業に提供したパーソナルデータを自ら手元に集約して管理し、データ別に利活用条件を容易に設定するためのシステムとしてPDSが考えられた。個人情報保護法やガイドラインの規定により、企業がパーソナルデータを利活用する場合、事前の本人同意が必須となるが、PDSは本人同意をシステムの的に実現する仕組みである。PDS自体は、本人同意のシステムの実現であり、データ流通のための仕組みは含まない。企業側にとって、個人1人1人からパーソナルデータの利活用に関する同意を取り付けて収集するのはコストが大きい。情報銀行は、あらかじめ個人が自らのパーソナルデータの利活用条件を設定した上で、データの一部または全てを、情報銀行を運営する事業者に一括して信託する仕組みである。PDSとの連携により、個人がPDS等を用いて行う権利処理を代行することも可能としている。情報銀行は、第三者提供について、提供価格の折衝から、異なるデータ同士の接合など一手に行うことができる。

[0005] 欧州連合ではEU一般データ保護規則GDPR（General Data Protection Regulation）というパーソナルデータの処理と移転に関するルールが、新たに2016年4月に定められた。世界の潮流を生みつつあるGDPRの考えでは、第三者提供時に再同意を行う必要があるが、データの利用目的、利用者全て、情報銀行に信託していることになり、包括同意でしかないといえる。世界を見据えるなら、第三者提供時の再同意は外せない。なお、改正個人情報保護法において要配慮情報の1つに位置付けられる「健康・医療データ」及び「金融データ」（クレジット番号、銀行口座番号）の情報銀行による管理については、「情報信託機能の認定に係る指針ver.1.0」では対象外であり、2019年6月にパブコメ募集があったように検討途上である。「データ取引市場」は、パーソナルデータを手元のPDSで直接管理している個人、または個人からデータを預かり代行管理している情報銀行、自社の産業デ

一夕の効果的な利活用を目的として、パーソナルデータの収集ニーズを持つ企業（及び複数企業の集合体であるプラットフォーム）、それぞれの需給をマッチングさせるデータ売買の仕組みである。この市場の機能としては、データ売買に伴う価格形成・提示、取引条件の詳細化、取引対象の標準化、取引の信用保証等が想定されている。パーソナルデータの流通においては、世界を見据え、改正個人情報保護法ならびにGDPRに準拠した形式で、再同意プロセスを含むデータ取引市場の仕組み作りが有用である。

[0006] ところで、近年、個人のパーソナルデータの流通を実現するシステムが種々提案されている。例えば特許文献1には、個人のパーソナルデータを取得する事業者と、購入業者と、事業者と購入業者との間に介入し、購入業者からの申請及び申請対象のパーソナルデータの提供を仲介する仲介業者とを備えたパーソナルデータ提供システムが記載されており、個人に仮IDを付与することで、仲介業者及び購入業者に対して匿名性を確保可能にするようにしている。また、特許文献2には、パーソナルデータを記憶する複数の情報銀行装置と、データ利用装置との間に介設して、データ利用装置からの利用データ要求を支援する仲介装置が記載されている。特許文献3には、ユーザ情報記憶部を備えた管理用サーバと、ユーザ情報の要求を行う要求側サーバとを備えたパーソナルデータ管理システムが記載されている。

[0007] ユーザ情報記憶部を備えた管理用サーバと、ユーザ情報の要求を行う要求側サーバとを備えたパーソナルデータ管理システムが記載されている。

先行技術文献

特許文献

[0008] 特許文献1：特開2018-128884号

特許文献2：特許第6592213号

特許文献3：特許第6566278号

発明の概要

発明が解決しようとする課題

[0009] 特許文献 1 ～ 3 に記載されたデータ管理システム、データ提供システム及び仲介装置は、パーソナルデータを格納する提供元データ記憶部を備える一方、パーソナルデータの流通促進のためのカタログの作成、及びその保管を行う流通管理装置を備えたものではない。しかもデータ流通管理装置及び複数の提供元データ記憶部を個々に配設するシステム構成を採用する場合、システム全体としてパーソナルデータの情報セキュリティー、さらに G D P R に準拠し、かつ個人情報の保護を満たすように設計することは容易ではない。

[0010] 本発明は、上記に鑑みてなされたもので、パーソナルデータの情報漏洩に対するリスクを低減可能にするデータ流通管理を行うパーソナルデータ流通管理システム及びその方法を提供するものである。

[0011] また、本発明は、実名等の個人情報の保護を図り、また G D P R に準拠しながらデータ流通管理を可能にするパーソナルデータ流通管理システム及びその方法を提供するものである。

課題を解決するための手段

[0012] 本発明に係るパーソナルデータ流通管理システムは、ネットワーク上に接続された、少なくとも 1 つの提供元データ管理装置と、データ流通管理装置と、中継処理装置とを個別に備える。前記提供元データ管理装置は、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に係る属性情報を前記個人の实名情報と対応付けた元データとして記憶するデータベースを備える。前記データ流通管理装置は、データ利用者端末からのデータ利用依頼を受け付ける利用依頼受付手段を備える。前記中継処理装置は、前記利用依頼受付手段で受け付けた前記データ利用依頼に基づいて、前記各提供元データ管理装置の前記データベースから前記データ利用依頼に該当する個人のパーソナルデータを選別すると共に対応する個人の实名情報を除いて前記データ利用者端末に出力するものである。

[0013] また、本発明に係るパーソナルデータ流通管理システムは、ネットワーク上に接続された、少なくとも 1 つの提供元データ管理装置と、データ流通管

理装置とを個別に備える。前記提供元データ管理装置は、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に関する属性情報を前記個人の実名情報と対応付けた元データとして記憶するデータベースを備える。前記データ流通管理装置は、前記各提供元データ管理装置の前記データベースに記憶されている、前記パーソナルデータを除く前記元データを取り込み、一元化し、かつ編集を行ってデータカタログを生成するカタログ管理手段を備える。

[0014] また、本発明に係るパーソナルデータ流通管理方法は、ネットワーク上に接続された、少なくとも1つの提供元データ管理装置と、データ流通管理装置と、中継処理装置とを個別に備える。前記データ流通管理装置の利用依頼受付手段が、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に関する属性情報を前記個人の実名情報と対応付けた元データとして生成して記憶する。前記データ流通管理装置が、データ利用者端末からのデータ利用依頼を受け付ける。前記中継処理装置が、前記データ流通管理装置で受け付けた前記データ利用依頼に基づいて、前記各提供元データ管理装置の前記データベースから前記データ利用依頼に該当する個人のパーソナルデータを選別すると共に対応する個人の実名情報を除いて前記データ利用者端末に出力するものである。

[0015] また、本発明に係るパーソナルデータ流通管理方法は、ネットワーク上に接続された、少なくとも1つの提供元データ管理装置と、データ流通管理装置とを個別に備える。前記提供元データ管理装置が、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に関する属性情報を前記個人の実名情報と対応付けた元データとして作成してデータベースに記憶する。前記データ流通管理装置のカタログ管理手段が、前記各提供元データ管理装置の前記データベースに記憶されている、前記パーソナルデータを除く前記元データを取り込み、一元化し、かつ編集を行ってデータカタログを生成するものである。

[0016] これらの発明によれば、データ流通管理装置は、パーソナルデータを除く

元データを取り込んでデータカタログを生成する。また、中継処理装置は、外部から受け付けたデータ利用依頼に基づいて、各提供元データ管理装置のデータベースから個人の実名情報を除いたデータをデータ利用者端末に出力する。これらにより、パーソナルデータや個人の実名情報の、各提供元データ管理装置のデータベースからの外部への情報漏洩に対するリスクを低減したデータ流通管理が可能となる。

発明の効果

[0017] 本発明によれば、パーソナルデータや個人の実名情報の情報漏洩に対するリスクを低減したデータ流通管理が可能となる。

図面の簡単な説明

[0018] [図1]本発明に係るパーソナルデータ流通管理システムの一実施形態を示す構成図である。

[図2]提供元データ管理装置の一実施形態を示す構成図である。

[図3]データ流通管理装置の一実施形態を示す構成図である。

[図4]利用者端末の一実施形態を示す構成図である。

[図5]元データの項目の一例を示すメモリマップ図で、（A）はデータ提供元の項目とメールアドレスの項目であり、（B）は個人の実名の項目、個人の属性情報などの項目を含む。

[図6]名寄せ処理の一例を示す説明図で、（A）は名寄せテーブル、（B）は二次仮名テーブルである。

[図7]カタログ管理処理の一例を示す説明図で、（A）は総合データカタログ、（B）は編集されたカタログである。

[図8]データ利用依頼の選択項目の一例を示す図表である。

[図9]最終仮名化処理を説明する図で、（A）はデータカタログ、（B）は振り直しの一例を示す図、（C）は提供用データを示す。

[図10]データ流通管理装置が行う名寄せ処理の一例を示すフローチャートである。

[図11]データ流通管理装置が行う再同意処理の一例を示すフローチャートで

ある。

[図12]データ提供元装置が行う再同意手続処理Ⅰの例を示すフローチャートである。

[図13]データ提供元装置が行う再同意手続処理ⅠⅠの例を示すフローチャートである。

発明を実施するための形態

[0019] 図1は、本発明に係るパーソナルデータ流通管理システムの一実施形態を示す構成図である。図1において、パーソナルデータ流通管理システム1は、データ提供側10と、データ流通管理装置30と、プラットフォームとして機能する中継処理装置40とを備え、それぞれインターネット等のネットワーク50を介してデータ通信可能にされている。パーソナルデータ流通管理システム1は、ネットワーク50を介して利用者端末100と接続可能にされている。

[0020] データ提供側10は、1群のデータセットを収集し、保管する単位である提供元データ管理装置として、少なくとも1つ以上の提供元データ管理装置11, 12, 13, …を備える。提供元データ管理装置11, 12, 13, …としては、法人、企業、大学法人、団体、個人が想定され、本実施形態では、それぞれ病院単位であり、また医局単位を含めてもよい。なお、本実施形態における個人の、又は診断でのパーソナルデータとしては、例えば心拍数、血圧その他の各種のバイタルデータ、さらに病院内での購買履歴情報等のデータ種類を含めてもよい。また、本実施形態では、データ提供側10及び利用者端末100の各主体は、本システムの団体に入会した会員であることを想定しているが、必ずしも必須ではない。会員は、ID、パスワードが付与され、これに基づいてデータの閲覧、利用依頼のサービスを受けることができる。

[0021] ここで、パーソナルデータ流通管理システム1が実行するデータ流通管理処理の概要を説明する。データ提供側10を構成する提供元データ管理装置11, 12, 13, …は、それぞれ複数の個人（例えば患者、被検診者）か

らパーソナルデータを収集する。パーソナルデータとしては種々の種類が想定される。収集された各種類のパーソナルデータは、データ提供側 10 の各提供元データ管理装置 11, 12, 13, …単位で、実名情報と対応付けられて格納される。

[0022] 一方、データ流通管理装置 30 は、データ取引市場として機能するもので、データ流通（個人のパーソナルデータの売買）促進のための宣伝用のデータカタログを作成して、ネットワーク 50 上で閲覧可能に提供する。この状態で、データ流通管理装置 30 は、ネットワーク 50 を経て第三者からのデータ利用依頼を受信すると、利用依頼の内容に該当するパーソナルデータを検索し、関係者及び個人に対する再同意手続処理を経て、所定の条件（ベネフィット）の下で利用者にデータ提供する。ベネフィットとしては、金銭、ポイント、また各種のサービス、その他の対価を含めてよい。

[0023] この場合において、個人が特定されることを防止するべく第 1、第 2 の仮名化を行うと共に、パーソナルデータの提供時には、復元できないように更なる振り直し化（提供用仮名化）を行って匿名にして、実データと共に第三者に提供する。また、第三者によるデータ利用に当たって、所定の条件としてパーソナルデータを提供した個人から再同意を得る場合に、データ収集の関係者を含めて再同意を得る必要がある場合、所定の優先順位で効率的な再同意手続処理を実行する。以下、詳述する。

[0024] 図 2 は、提供元データ管理装置 11 の一実施形態を示す構成図である。提供元データ管理装置 11, 12, 13, …は、同一構成であるので、以下、提供元データ管理装置 11 を代表にして説明する。提供元データ管理装置 11 は、プロセッサ（CPU）から構成される制御部 110 を備える。制御部 110 には、画像を表示する表示部 1101、外部から情報の入力、指示等を行う操作部 1102、及び所定のデータを格納する提供元データ DB 1103 が接続されている。

[0025] 測定器 21 は、本実施形態では、個人から各種のバイタルデータをパーソナルデータとして計測するものである。測定器 21 は、例えば心拍計とか血

圧計、あるいは生体内を測定（撮像）するMRI等の各種のセンサ、機器及び装置を含む。個人端末22は、パーソナルコンピュータ、スマートフォン、その他、各種のモバイル型情報通信端末を含み、SNS（Social Network System）、SMS（Short Message Service）あるいは電子メールを利用して情報の授受を行う。

[0026] 提供元データDB1103は、制御部110が行う提供元データ管理処理を制御する制御プログラムを記憶する他、測定器21で測定された複数の個人の実データであるパーソナルデータを含む元データを保管する。図5は、元データの項目例を示すメモリマップである。図5（A）はデータ提供元の項目、すなわち本実施形態ではデータセット単位の1つである、例えば病院「A」を示す。次いで病院Aの、本実施形態ではメールアドレスの項目がある。さらに図5（B）に示すように、個人の実名の項目に続いて、当該個人の性別、年齢、同じくメールアドレス、住所、一次仮名、情報口座、及び実データ（パーソナルデータ）の項目が個人の属性情報としてある。なお、一次仮名とは、病院「A」での元データ作成時に、個人の実名に対応して、典型的には適宜なルールに従って自動的に付与される識別情報をいう。情報口座は、システム上での個人を管理するためのアカウントであり、所在情報を含む。この情報口座は、個人のパーソナルデータの提供の都度、更新されるベネフィットの蓄積箇所をいう。

[0027] また、元データには、必要に応じて、その他の情報の項目が設けられている。本実施形態では、利権者、収集者、それらのメールアドレスなどの測定関与者の属性情報の項目がある。なお、利権者、収集者にも情報口座の項目を準備してもよい。利権者には例えば測定器や測定場所の提供者が該当し、収集者には測定作業に従事した者が該当する。さらに、他の属性情報として、データ種類、測定器（型名等）、他の種々の測定条件（例えば、測定日時、測定場所）が想定される。また、ベネフィットは、原則、データ利用者が負担するものとするが、データ流通管理装置30が一部負担したり、前払いしたりする態様もあり得る。ベネフィットの内容は、予め設定されていても

よいし、データ利用の申し込みの都度、交渉などを経て決める態様でもよい。

[0028] 制御部 110 は、プロセッサにより制御プログラムが実行されることにより、データ受付部 111、データ管理部 112 及び再同意処理部 113 として機能する。

[0029] データ受付部 111 は、図 5 に示す、個人単位の元データ表に各種のデータを操作部 1102 を介して、又は項目によっては自動的に登録する処理を行う。例えば、パーソナルデータは、個人の一次仮名で紐付けして測定器 21 の測定結果を自動的に入力する態様としてもよい。この場合、パーソナルデータをデータ提供側 10 で、あるいは病院「A」で利活用（一次利用）することについての各個人の、また必要に応じて利権者、収集者の同意を取得するものとする。

[0030] データ管理部 112 は、図 5 に例示する元データに基づいて、以下のデータ管理を行う。データ管理部 112 は、中継処理装置 40 にアップロード（あるいはリンク）するデータとして、実名情報を除いて、一次仮名と、実データであるパーソナルデータとの組からなる提供元データ（一次仮名、パーソナルデータ）を作成する。なお、この提供元データ（一次仮名、パーソナルデータ）は、中継処理装置 40 に持たせる態様その他、提供元データ管理装置 11 で持つ態様でもよい。

[0031] また、データ管理部 112 は、データ流通管理装置 30 に提出するデータとして、パーソナルデータを除いて、一次仮名と実名との組からなる名寄せ用テーブル（一次仮名、実名）を作成する。また、データ管理部 112 は、データ流通管理装置 30 に提出するデータとして、パーソナルデータを除いて、提供元、データ種類、属性情報及びデータ数の組からなるデータカタログ（提供元と、データ種類、測定器及び他の測定条件を含む属性情報と、データ数と）を一次仮名と紐付けて作成する。データ管理部 112 は、提供元データ管理装置 11 の立ち上げ時、あるいはその他の適宜のタイミングでデータの作成を行い、作成された各データをデータ流通管理装置 30 に送出す

る。名寄せ用テーブルは、データ流通管理装置 30 の名寄せ用データ DB 341 に格納される。データカタログは、データ流通管理装置 30 のデータカタログ DB 342 に格納される。

[0032] 再同意処理部 113 は、提供元データ管理装置 11 が担当する再同意のための処理を実行する。再同意処理は、第三者である利用者端末 100 からデータ利用依頼があった場合に、依頼内容に該当するパーソナルデータの個人から、更には必要に応じて提供元、属性情報の内の利権者及び収集者からデータ利用（二次利用）の同意書を取得する手続処理である。再同意処理は、後述するようにデータ流通管理装置 30 からの指示によって行われるもので、典型的には電子的かつネットワーク 50 を介して行うが、場合によっては、一部、他の通信手段を適用するケースもあり得る。

[0033] 本実施形態では、再同意の手続は予め設定された優先順位に従って行われる。すなわち、優先順位は、提供元、利権者及び収集者、最後に個人の順である。再同意処理部 113 は、電子的な再同意申請書が送付されてくると、再同意申請書中の、所要の単位毎に対応して設けられた、同意、不同意を表すチェックボックスに、操作部 1102 を操作してマークを記入して、返信指示を行う。

[0034] 再同意処理部 113 は、提供元データ管理装置 11 が不同意の場合には、再同意処理は終了し、一方、同意の場合には、同時に送信されてきた利権者及び収集者用の再同意申請書を、該当する利権者及び収集者に、本実施形態では電子メールで送信して、回答（返信）を待つ。再同意処理部 113 は、利権者及び収集者からの回答が不同意の分については作業を終了し、同意の分については、個人用の再同意申請書を該当する個人に電子メールで送信して、回答（返信）を待つ。かかる優先順位を設定することで、再同意手続を効率的に進めることができる。なお、利権者及び収集者、個人に対しては、再同意に対して種々の形態でのベネフィットが与えられ、例えば、前記したように図 5 に示す情報口座に振り込まれる。なお、再同意の他の形態及び再同意の処理方法については、後述する。

- [0035] 図3は、データ流通管理装置30の一実施形態を示す構成図である。データ流通管理装置30は、プロセッサ（CPU）から構成される制御部31を備える。制御部31には、画像を表示する表示部32、外部から情報の入力、指示等を行う操作部33、及び名寄せ用データを格納する名寄せ用データDB341、データカタログを格納するデータカタログDB342が接続されている。なお、データ流通管理のための制御プログラムは、これらのメモリ内のプログラム記憶領域に書き込まれていてもよい。
- [0036] 制御部31は、プロセッサにより制御プログラムが実行されることにより、名寄せ処理部311、カタログ管理部312、利用依頼受付部313及び提供用仮名化処理部314として機能する。
- [0037] 名寄せ処理部311は、図6に示すように、名寄せ用データDB341に格納された名寄せ用テーブル（一次仮名、実名）から二次仮名を作成し、名寄せ用データDB341に格納する。より詳細には、名寄せ処理部311は、提供元データ管理装置11, 12, 13, …からの名寄せ用テーブル（一次仮名、実名）を一元化（統合）し（図6（A）参照）、実名と一次仮名とを突き合わせる名寄せ処理を行って、一次仮名から統合された二次仮名を作成し、作成した二次仮名テーブル（図6（B）参照）を名寄せ用データDB341に格納する。なお、この名寄せ用テーブル（一次仮名、実名）をデータ流通管理装置30に送信する場合、提供元データ管理装置11, 12, 13, …からネットワーク50以外のネットワークを経由し、あるいは他の通信方式を利用するようにして、通信時における実名データの漏洩リスクを抑制している。図6の例では、病院「A」を診療した個人の一次仮名ID-a1と、病院Bを診療した個人の一次仮名ID-b5との実名が一致する同一人であり、図6（B）では、共通の二次仮名ID1に付け替えられている。なお、二次仮名は、例えば連続する個人番号でもよい。また、図6（B）の二次仮名テーブルとして、（二次仮名、実名）のテーブルとしてもよい。
- [0038] カタログ管理部312は、図7に示すように、データカタログDB342に格納された各提供元データ管理装置11, 12, 13, …からのデータカ

タログを一元化して統合し、総合データカタログを作成する。図7において、一次仮名と紐付けされたデータカタログ（提供元、データ種類などを含む属性情報、データ数）は、図6（B）を参照して二次仮名と対応付けられて、データ種類の項目に基づいて編集されている（図7（B）参照）。そして、総合データカタログの部分がネットワーク50上に提供されて閲覧対象とされる。なお、データカタログは、閲覧範囲の一部又は全部のデータ項目に基づいてソート処理が可能とされており、これにより利用者側の項目選定の利便性に供するようにしている。また、データカタログをネットワーク50上に提供する営業形態に代えて、人による営業で活用したり、また他の媒体に載せて利用したりする態様も採用可能である。

[0039] 利用依頼受付部313は、利用者端末100からの利用依頼を受け付けて、依頼内容に応じた処理を実行する。依頼内容は、例えば図8に示すように、データ項目に基づいて指定される。図8の例では、データ種類、データ提供元、測定器などを含む他の属性情報が想定される。なお、他の属性情報の依頼例として、個人の属性情報のうちの性別、年齢層を含める態様としてもよい。利用依頼受付部313は、依頼内容から、再同意を求める対象者を選出する。例えば、依頼内容にデータ提供元が含まれている場合には、当該提供元データ管理装置に対してのみ再同意処理を実行すればよい。指定がない場合には、全てが対象者となる。利用依頼受付部313は、依頼内容の情報を、対象となる提供元データ管理装置に、この例では中継処理装置40を経て送信し、再同意処理を指示する。なお、対象となる利権者及び収集者、さらに個人の選出については、前述した再同意処理部113が実行してもよいし、利用依頼受付部313が処理して、再同意処理の指示と対応付けて送信してもよい。

[0040] 提供用仮名化処理部314は、利用依頼のあった利用者へ提供する提供用データを、後述する中継処理装置40にアップされた、実名の項目を除いた、二次仮名に紐付けられた元データから編集して作成する。より具体的には、提供用仮名化処理部314は、再同意申請に対する不同意該当者を、図6

(B) の一次仮名、二次仮名テーブルから削除する処理と、削除後に残った二次仮名を報告用仮名に振り直す処理と、中継処理装置40にアップされた元データから報告用仮名が対応付けられた二次仮名を抽出して提供用データを作成する処理とを実行する。

[0041] 報告用仮名への振り直し処理は、例えば図9 (A) (B) (C) に示すように、データカタログに対応付けられている二次仮名の内、削除後に残った分に対して、例えば所定のソート処理を施すなどした後、例えば上から順に個別の識別情報に置換する(図9 (B) のテーブル参照)。個別の識別情報としては、所定のルールに従って付与する文字コード、例えば連続番号が想定される。図9 (B) では、二次仮名ID2 (「属性情報: a, c, …」を持つ。) が付与されている者が不同意該当者であり(図9 (A) 参照、回答結果: 不同意)、振り直し後は、図9 (C) の提供用テーブルに示すように削除されている。なお、図9 (C) に示す提供用データは、図9 (B) の振り直しテーブルを受けて、中継処理装置40で編集されたものである。編集後の提供用データは、中継処理装置40から利用者端末100に送出される。

[0042] 図4は、利用者端末100の一実施形態を示す構成図である。利用者端末100は、プロセッサ(CPU)から構成される制御部101を備える。制御部101には、画像を表示する表示部1001、外部から情報の入力、指示等を行う操作部1002、及び提供用データを一時的に格納する記憶部1003が接続されている。また、記憶部1003は、パーソナルデータ利用処理のための制御プログラム(インストールされたアプリケーションプログラム)を記憶している。利用者端末100は、本システム用の専用機である必要はなく、ネットワーク50を介して通信可能であれば、前記アプリケーションプログラムをインストールすることで、汎用のパーソナルコンピュータ装置でも適用可能である。また、モバイル端末でもよい。

[0043] 制御部101は、プロセッサにより制御プログラムが実行されることによって、閲覧処理部102、利用依頼処理部103として機能する。

[0044] 閲覧処理部102は、中継処理装置40あるいはデータ流通管理装置30

に対してデータカタログの閲覧要求を送信し、所定の条件下（例えば、会員であること）で、データカタログを閲覧可能に受信する。

[0045] 利用依頼処理部 103 は、利用を希望するパーソナルデータに関する項目を選択した内容を含む電子的な利用依頼書（利用申込書）を中継処理装置 40 を経由してデータ流通管理装置 30 に送信する。なお、利用依頼に応答して、本システム 1 から電子メールなどによって返信された提供用データに対する閲覧処理は、一般の電子メールの扱いと同様なので、説明は省略する。

[0046] 続いて、名寄せ処理、再同意処理、再同意手続処理の手順について説明する。

[0047] 図 10 は、データ流通管理装置 30 の制御部 31 が行う名寄せ処理の一例を示すフローチャートである。まず、制御部 31 は、内蔵タイマ等による計時によってカタログ作成のための所定のタイミングを確認すると、各データ提供元の提供元データ管理装置 11, 12, 13, …から、提供元データ（一次仮名、実名）、データカタログ（一次仮名、データ種類、属性情報、データ数）をそれぞれ受信する（ステップ S1）。次いで、制御部 31 は、全てのデータ提供元からの提供元データ（一次仮名、実名）を一元化し、同一の実名を持つ一次仮名毎に同一の二次仮名を所定のルールに従って付与する（ステップ S3）。そして、制御部 31 は、付与した二次仮名に基づいて、図 6（B）に示すような二次仮名テーブル（二次仮名、一次仮名）を作成し、保存する（ステップ S5）。

[0048] 図 11 は、データ流通管理装置 30 の制御部 31 が行う再同意処理の一例を示すフローチャートである。まず、制御部 31 は、利用依頼の有無を判断し（ステップ S11）、利用依頼がなければ本フローを抜け、利用依頼があれば、利用依頼書中から、該当するデータ提供元、データ種類、属性情報を抽出し、当該データ提供元に手続指示を行う（ステップ S13）。この時点で、対象外となったデータ提供元は除かれる。

[0049] 次いで、制御部 31 は、該当するデータ提供元からの、利用依頼に対する回答の有無を判断する（ステップ S15）。そして、制御部 31 は、利用不

同意分を二次仮名テーブルを参照して削除し、残った二次仮名に対して提供用仮名を振り直す（ステップS 17）。提供用仮名への振り直しによって、提供用データの個人が匿名化される。また、提供用仮名への振り直しを行うことで、利用依頼の毎に、同一の提供用仮名が付された個人が同一人である保証がなくなるため、複数回のデータ利用によっても個人の特定はできない。なお、データ提供元自体が不同意を回答してきた場合には、それ以降の利権者、収集者及び個人は全て不同意扱いとして処理する。

[0050] 図12は、提供元データ管理装置11の制御部110が行う再同意処理1の例を示すフローチャートである。制御部110は、中継処理装置40を介してデータ流通管理装置30から再同意処理の指示があると、操作部1102を介して自己のデータ提供元に対する再同意申請書への同意、不同意を入力する。不同意の場合には、そのまま返送して、本フローに入らない。

[0051] 一方、同意であれば、制御部110は、利用依頼に際して選択されたデータ種類に、測定関与者の属性情報中の利権者、収集者が含まれているか否かの判断を行う（ステップ#1）。制御部110は、該当する者がいなければ、本フローを抜け、一方、該当する者がいる場合、該当する利権者、収集者に再同意書面を電子メールで送信する（ステップ#3）。

[0052] 次いで、制御部110は、該当する全ての利権者、収集者から回答があったかどうかを判断する（ステップ#5）。制御部110は、該当する全ての利権者、収集者からの回答を待って、回答が不同意であった分を除いて、残りの該当する個人に再同意書面を電子メールで送信する（ステップ#7）。制御部110は、該当する全ての個人から回答があったかどうかを判断する（ステップ#9）。そして、制御部110は、回答結果をデータ流通管理装置30に返送する（ステップ#11）。

[0053] 続いて、本発明が適用可能な再同意の他の実施形態について説明する。前記した実施形態は、再同意を都度再同意として扱い、かつ利用者からの利用依頼に応答して同意するか否かを決定する方法であったが、本発明はこれに

限定されず、事前に許諾する形式の包括再同意の形式を採用してもよい。

[0054] なお、包括再同意には、部分包括再同意及び部分一括再同意を含めてもよい。包括再同意とは、図5に示す元データの全てのデータ項目（属性情報等の項目も含む）に対して再同意を事前に許諾（設定）することをいう。部分包括再同意とは、元データのうち特定の1又は複数のデータ項目について再同意を事前に許諾することをいう。部分一括再同意は、元データのうち特定の複数のデータ項目について一塊として再同意を事前に許諾することをいう。

[0055] 包括再同意が設定できる項目は、元データのうち、利用者による利用依頼の対象データ項目に対応する。図5（B）を参照すれば、「データ種類」、「実データ」の他、「性別」、「年齢」、「測定器」、さらに「他の測定条件」内の種々の項目などが含まれ得る。また、「データ提供側」を含めてもよい。具体的には、例えば、前記対象データ項目等のそれぞれに付随して「再同意」の項目が設定される。「再同意」の項目は、例えば「包括」と「都度」とが2者択一で交互に切り替わり設定されるようになっている。そして、提供元データ管理装置11の再同意処理部113は、再同意の要請時に、これらの各包括再同意項目の設定内容を参照するようにしている。詳細は、図13で説明する。また、他の設定態様としては、包括再同意、部分包括再同意及び部分一括再同意の項目が個別に準備され、包括再同意は2者択一形式で、部分包括再同意は、入力された所望する項目を論理和で、部分一括再同意は、入力された所望する項目を論理積で設定する態様でもよい。

[0056] 提供元データ管理装置11のデータ管理部112は、個人、利権者、収集者からの包括再同意に対する「包括」と「都度」（「包括」からの解除含む）の要請を受け付けて対応する「再同意」の項目について「包括」、「都度」を選択する。各包括再同意項目は、実データ取得時点での設定の他、その後の任意の時点で変更することが可能であってもよい。なお、提供元データ管理装置11のデータ管理部112は、個人、利権者、収集者に予めIDなどを付与し、あるいは当人のメールアドレスからの設定内容の書き換えを受

け付ける権限を与えることで、当人についての包括再同意の項目を書き換え可能にするようにしてもよい。

[0057] 図13は、提供元データ管理装置11の制御部110が行う再同意処理11の例を示すフローチャートである。図13は、図12のフローチャートに対して、包括再同意の項目の設定内容に対応した処理を付加した再同意手続を示したもので、具体的には、ステップ#23～ステップ#37を付加乃至修正した点で相違し、その他の処理は同一である。

[0058] ステップ#23では、利用依頼のあったデータ種類に対し、包括再同意、部分包括再同意、部分一括再同意を承諾している利権者、収集者を検索する。そして、検索された1又は複数の該当者はステップ#25、ステップ#27をスルーして、ステップ#29に進み、検索された該当者が同意有りとして処理される。一方、ステップ#25で都度再同意の利権者、収集者には再同意の書面が送付され、回答を待つ（ステップ#27）。そして、包括再同意した者と都度再同意した者とがまとめられてステップ#31に進む。

[0059] 次に、ステップ#31では、不同意分を除き、該当する個人は、利用依頼のあったデータ種類に対し、包括再同意、部分包括再同意、部分一括再同意を承諾している者を検索する。そして、検索された1又は複数の個人はステップ#33、ステップ#35をスルーして、ステップ#37に進み、検索された該当者が同意有りとして処理される。一方、ステップ#33で都度再同意の個人には再同意の書面が送付され、回答を待つ（ステップ#35）。そして、包括再同意した個人と都度再同意した個人とがまとめられてステップ#39に進む。このように、予め包括再同意等をしていることで、当人に対する同意書の発送、返送作業を省略でき、手続がよりスムーズとなる。

[0060] なお、提供元データには、（提供用仮名、パーソナルデータ）に限らず、利用依頼に該当する項目、個人の一部の属性情報、例えば性別、年齢などを含めてもよい。

[0061] 本システム1では、実名情報と実データとをそれぞれの提供元データ管理装置11, 12, 13, …でのみ所持し、取引市場に対応するデータ流通管

理装置 30 では実データを所持せず、中継処理装置 40 では実名情報を所持しないようにした。このように元データを分散して所持したことで、一箇所で所持して状態で情報漏洩した場合に比してセキュリティリスクが大幅に低減される。また、データ流通管理装置 30、中継処理装置 40 のいずれも実名情報と実データとを同時に所持しないため、これらの装置から個々人のパーソナルデータが特定されることもない。また、各装置が別団体で管理されている場合、個々の法的ダメージは抑えられる。

[0062] 以上説明したように、本発明に係るパーソナルデータ流通管理システムは、ネットワーク上に接続された、少なくとも 1 つの提供元データ管理装置と、データ流通管理装置と、中継処理装置とを個別に備える。前記提供元データ管理装置は、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に係る属性情報を前記個人の実名情報と対応付けた元データとして記憶するデータベースを備える。前記データ流通管理装置は、データ利用者端末からのデータ利用依頼を受け付ける利用依頼受付手段を備える。前記中継処理装置は、前記利用依頼受付手段で受け付けた前記データ利用依頼に基づいて、前記各提供元データ管理装置の前記データベースから前記データ利用依頼に該当する個人のパーソナルデータを選別すると共に対応する個人の实名情報を除いて前記データ利用者端末に出力するものである。

[0063] また、本発明に係るパーソナルデータ流通管理システムは、ネットワーク上に接続された、少なくとも 1 つの提供元データ管理装置と、データ流通管理装置とを個別に備える。前記提供元データ管理装置は、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に係る属性情報を前記個人の实名情報と対応付けた元データとして記憶するデータベースを備える。前記データ流通管理装置は、前記各提供元データ管理装置の前記データベースに記憶されている、前記パーソナルデータを除く前記元データを取り込み、一元化し、かつ編集を行ってデータカタログを生成するカタログ管理手段を備える。

[0064] また、本発明に係るパーソナルデータ流通管理方法は、ネットワーク上に

接続された、少なくとも1つの提供元データ管理装置と、データ流通管理装置と、中継処理装置とを個別に備える。前記データ流通管理装置の利用依頼受付手段が、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に係る属性情報を前記個人の実名情報と対応付けた元データとして生成して記憶する。前記データ流通管理装置が、データ利用者端末からのデータ利用依頼を受け付ける。前記中継処理装置が、前記データ流通管理装置で受け付けた前記データ利用依頼に基づいて、前記各提供元データ管理装置の前記データベースから前記データ利用依頼に該当する個人のパーソナルデータを選別すると共に対応する個人の実名情報を除いて前記データ利用者端末に出力するものである。

[0065] また、本発明に係るパーソナルデータ流通管理方法は、ネットワーク上に接続された、少なくとも1つの提供元データ管理装置と、データ流通管理装置とを個別に備える。前記提供元データ管理装置が、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に係る属性情報を前記個人の実名情報と対応付けた元データとして作成してデータベースに記憶する。前記データ流通管理装置のカatalog管理手段が、前記各提供元データ管理装置の前記データベースに記憶されている、前記パーソナルデータを除く前記元データを取り込み、一元化し、かつ編集を行ってデータCatalogを生成するものである。

[0066] これらの発明によれば、データ流通管理装置は、パーソナルデータを除く元データを取り込んでデータCatalogを生成する。また、中継処理装置は、外部から受け付けたデータ利用依頼に基づいて、各提供元データ管理装置のデータベースから個人の実名情報を除いたデータをデータ利用者端末に出力する。これらにより、パーソナルデータや個人の実名情報の、各提供元データ管理装置のデータベースからの外部への情報漏洩に対するリスクを低減したデータ流通管理が可能となる。

[0067] また、本発明は、前記Catalog管理手段は、生成したデータCatalogを前記ネットワーク上で閲覧可能な状態にすることが好ましい。この構成によれ

ば、カタログが効率的に公表される。

[0068] また、本発明は、前記提供元データ管理装置は、前記データ利用依頼の受け付けに応じた前記データ流通管理装置からの指示に従って、依頼対象のパーソナルデータを有する個人を特定し、当該個人の情報通信端末にデータ提供許否の問い合わせ情報を送信し、提供許否の回答を受信する再同意処理手段を備え、前記データ流通管理装置は、データ提供不同意の回答のあった個人のパーソナルデータの出力を制御するデータ出力制御手段を備えることが好ましい。この構成によれば、データ提供に対する許否に基づいてパーソナルデータの提供が制御される。また、パーソナルデータが利用者側に提供される際には実名情報が除かれるので、利用者側で実名情報とパーソナルデータとが紐付けられることはない。

[0069] また、本発明は、前記再同意処理手段は、測定に関与した者の情報通信端末にデータ提供許否の問い合わせを指示する第1問い合わせ処理と、前記第1の問い合わせ処理でデータ提供同意の回答のあった関与者が関与した測定器で測定されたパーソナルデータの個人の情報通信端末にデータ提供許否の問い合わせを指示する第2問い合わせ処理とを行うことが好ましい。この構成によれば、第1問い合わせ処理で、測定に関与した者に対して問い合わせが実行され、この第1問い合わせ処理でデータ提供同意の回答のあった関与者によって測定されたパーソナルデータの個人へ第2の問い合わせ処理が行われる。個人の人数の方が、測定に関与した者に比して多数であることを考慮すると、先ず、第1の問い合わせ処理で関与者の結果を得るように優先順位を設定する方が、全員に対して一律に、乃至個人から関与者への順で問い合わせを行う場合に比して効率的な再同意処理が可能となる。

[0070] また、本発明は、前記提供元データ管理装置は、前記ネットワーク上に複数の提供元データ管理装置を有することが好ましい。この構成によれば、元データの分散配置がより効果的に行われる。

[0071] また、本発明は、前記提供元データ管理装置は、前記各個人の実名に対応付けて一次仮名を付与しており、前記データ流通管理装置は、前記提供元デ

一タ管理装置毎に記憶されている各個人の実名を一元化し、共通の実名に共通の二次仮名を付与する名寄せ処理を実行する名寄せ処理手段を備えることが好ましい。この構成によれば、各データ提供元管理装置の各元データを一元化する際に、併せて一元化された仮名、すなわち二次仮名が設定される。

[0072] また、本発明は、前記名寄せ処理手段は、前記各提供元データ管理装置から前記実名及び一次仮名を取得し、前記実名と前記一次仮名との突き合わせによる名寄せ処理を施して前記一次仮名から統一された前記二次仮名を生成することが好ましい。この構成によれば、実名と一次仮名との突き合わせによる名寄せ処理によって、一次仮名から統一された二次仮名が生成される。

[0073] また、本発明は、前記データ出力制御手段は、再同意申請に対する不同意該当者を、前記二次仮名テーブルから削除する処理と、削除後に残った二次仮名を報告用仮名に振り直す処理とを行うことが好ましい。この構成によれば、同一のデータ項目に対しても、利用依頼時の不同意の状況によって報告用仮名が変わり、同じ報告用仮名でも同一人とは限らなくなって、匿名性が維持される。

[0074] また、本発明は、前記データベースは、前記元データのうち所定のデータ項目に対して包括再同意か都度再同意かを選択設定可能な包括再同意項目を含み、前記提供元データ管理装置は、前記包括再同意項目に対する設定を受け付けて設定内容を変更するデータ管理部を備え、前記再同意処理部は、利用依頼のあったデータ項目に対応した前記包括再同意項目の設定内容が許諾である場合、データ提供を許可したとして前記データ提供許否の問い合わせ情報の送信を省くことが好ましい。この構成によれば、包括合意をしている者については合意書の取得作業が省略でき、効率的かつ迅速となる。

[0075] また、本発明は、前記データ流通管理装置が、生成した前記データカタログを前記ネットワーク上で閲覧可能な状態にすることが好ましい。これにより、カタログが効率的に公表される。

符号の説明

[0076] 1 パーソナルデータ流通管理システム

- 1 1, 1 2, 1 3 提供元データ管理装置
- 1 1 0 制御部
- 1 1 3 再同意処理部
- 1 1 0 3 提供用データ D B (データベース)
- 2 1 測定器
- 2 2 個人端末
- 3 0 データ流通管理装置
- 3 1 制御部
- 3 1 1 名寄せ処理部
- 3 1 2 カタログ管理部 (カタログ管理手段)
- 3 1 3 利用依頼受付部 (利用要求受付手段)
- 3 1 4 提供用仮名化処理部 (データ出力制御手段)
- 3 4 1 名寄せ用データ D B
- 3 4 2 データカタログ D B
- 4 0 中継処理装置
- 5 0 ネットワーク
- 1 0 0 利用者端末 (データ利用者端末)

請求の範囲

- [請求項1] ネットワーク上に接続された、少なくとも1つの提供元データ管理装置と、データ流通管理装置と、中継処理装置とを個別に備え、
- 前記提供元データ管理装置は、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に係る属性情報を前記個人の实名情報と対応付けた元データとして記憶するデータベースを備え、
- 前記データ流通管理装置は、データ利用者端末からのデータ利用依頼を受け付ける利用依頼受付手段を備え、
- 前記中継処理装置は、前記利用依頼受付手段で受け付けた前記データ利用依頼に基づいて、前記各提供元データ管理装置の前記データベースから前記データ利用依頼に該当する個人のパーソナルデータを選別すると共に対応する個人の实名情報を除いて前記データ利用者端末に出力するパーソナルデータ流通管理システム。
- [請求項2] ネットワーク上に接続された、少なくとも1つの提供元データ管理装置と、データ流通管理装置とを個別に備え、
- 前記提供元データ管理装置は、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に係る属性情報を前記個人の实名情報と対応付けた元データとして記憶するデータベースを備え、
- 前記データ流通管理装置は、前記各提供元データ管理装置の前記データベースに記憶されている、前記パーソナルデータを除く前記元データを取り込み、一元化し、かつ編集を行ってデータカタログを生成するカタログ管理手段を備えたパーソナルデータ流通管理システム。
- [請求項3] 前記カタログ管理手段は、生成したデータカタログを前記ネットワーク上で閲覧可能な状態にする請求項2に記載のパーソナルデータ流通管理システム。
- [請求項4] 前記提供元データ管理装置は、前記データ利用依頼の受け付けに応じた前記データ流通管理装置からの指示に従って、依頼対象のパーソナルデータを有する個人を特定し、当該個人の情報通信端末にデータ

提供許否の問い合わせ情報を送信し、提供許否の回答を受信する再同意処理手段を備え、

前記データ流通管理装置は、データ提供不同意の回答のあった個人のパーソナルデータの出力を制御するデータ出力制御手段を備えた請求項1～3のいずれかに記載のパーソナルデータ流通管理システム。

〔請求項5〕 前記再同意処理手段は、測定に参与した者の情報通信端末にデータ提供許否の問い合わせを指示する第1問い合わせ処理と、前記第1の問い合わせ処理でデータ提供同意の回答のあった関与者が関与した測定器で測定されたパーソナルデータの個人の情報通信端末にデータ提供許否の問い合わせを指示する第2問い合わせ処理とを行う請求項4に記載のパーソナルデータ流通管理システム。

〔請求項6〕 前記提供元データ管理装置は、前記ネットワーク上に複数の提供元データ管理装置を有する請求項4又は5に記載のパーソナルデータ流通管理システム。

〔請求項7〕 前記提供元データ管理装置は、前記各個人の実名に対応付けて一次仮名を付与しており、

前記データ流通管理装置は、前記提供元データ管理装置毎に記憶されている各個人の実名を一元化し、共通の実名に共通の二次仮名を付与する名寄せ処理を実行する名寄せ処理手段を備えた請求項6に記載のパーソナルデータ流通管理システム。

〔請求項8〕 前記名寄せ処理手段は、前記各提供元データ管理装置から前記実名及び一次仮名を取得し、前記実名と前記一次仮名との突き合わせによる名寄せ処理を施して前記一次仮名から統一された前記二次仮名を生成する請求項7に記載のパーソナルデータ流通管理システム。

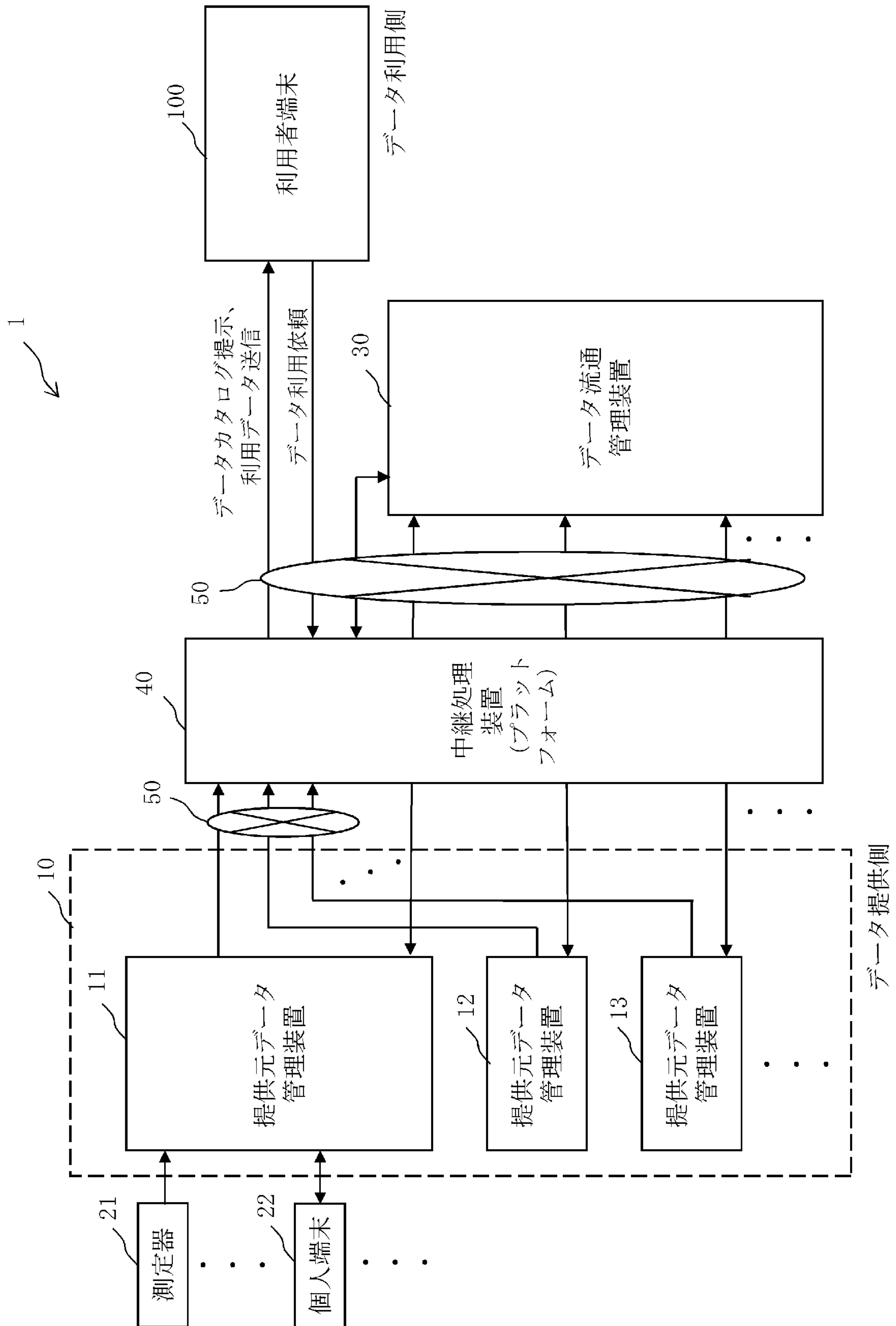
〔請求項9〕 前記データ出力制御手段は、再同意申請に対する不同意該当者を、前記二次仮名テーブルから削除する処理と、削除後に残った二次仮名を報告用仮名に振り直す処理とを行う請求項6に記載のパーソナルデータ流通管理システム。

- [請求項10] 前記データベースは、前記元データのうち所定のデータ項目に対して包括再同意か都度再同意かを選択設定可能な包括再同意項目を含み、
- 前記提供元データ管理装置は、前記包括再同意項目に対する設定を受け付けて設定内容を変更するデータ管理部を備え、
- 前記再同意処理部は、利用依頼のあったデータ項目に対応した前記包括再同意項目の設定内容が許諾である場合、データ提供を許可したとして前記データ提供許否の問い合わせ情報の送信を省くことを特徴とする請求項4～9のいずれかに記載のパーソナルデータ流通管理システム。
- [請求項11] ネットワーク上に接続された、少なくとも1つの提供元データ管理装置と、データ流通管理装置と、中継処理装置とを個別に備え、
- 前記データ流通管理装置の利用依頼受付手段が、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に係る属性情報を前記個人の実名情報と対応付けた元データとして生成して記憶し、
- 前記データ流通管理装置が、データ利用者端末からのデータ利用依頼を受け付け、
- 前記中継処理装置が、前記データ流通管理装置で受け付けた前記データ利用依頼に基づいて、前記各提供元データ管理装置の前記データベースから前記データ利用依頼に該当する個人のパーソナルデータを選別すると共に対応する個人の実名情報を除いて前記データ利用者端末に出力するパーソナルデータ流通管理方法。
- [請求項12] ネットワーク上に接続された、少なくとも1つの提供元データ管理装置と、データ流通管理装置とを個別に備え、
- 前記提供元データ管理装置が、測定器で測定された個人のパーソナルデータ、前記個人及び前記測定に係る属性情報を前記個人の実名情報と対応付けた元データとして作成してデータベースに記憶し、

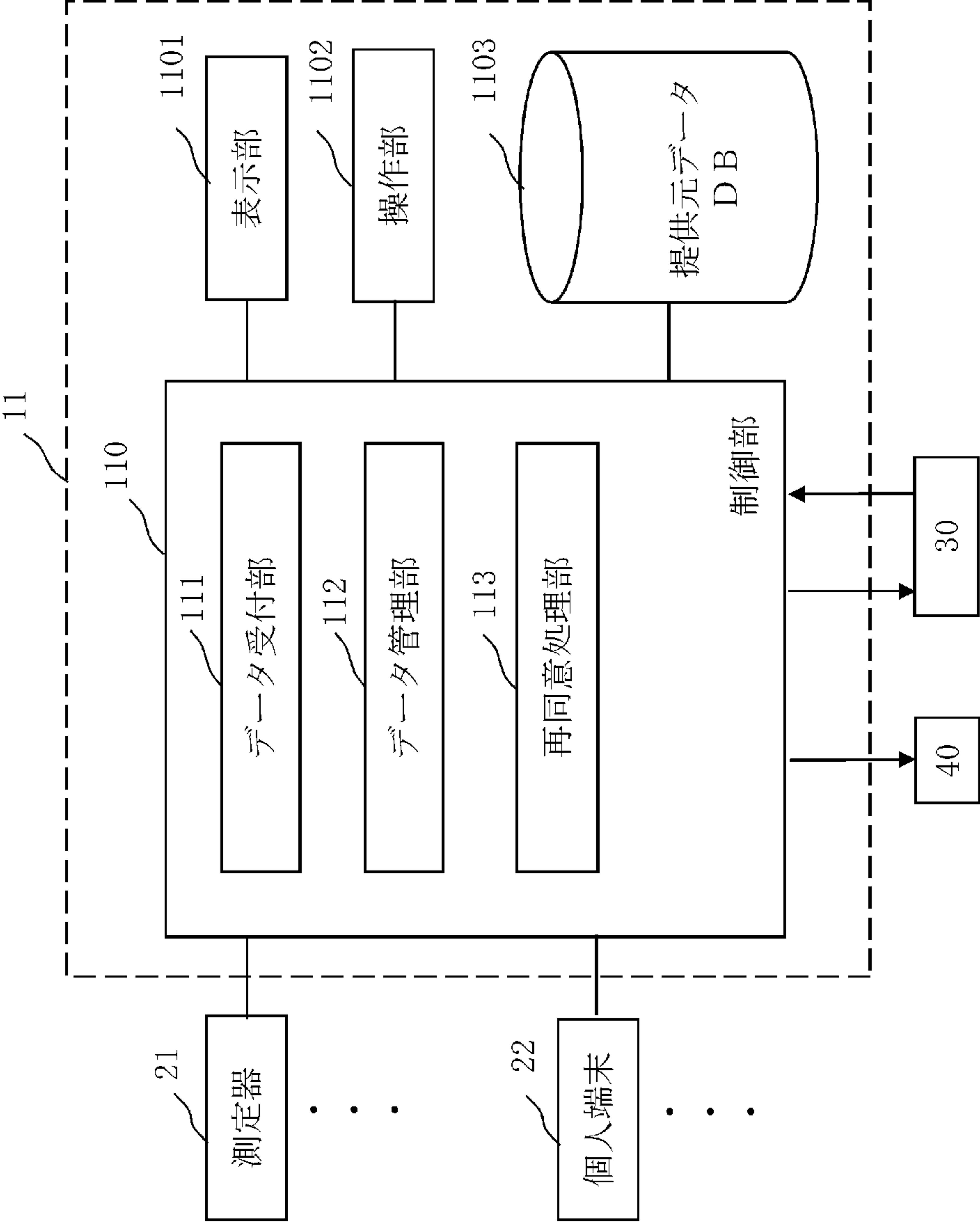
前記データ流通管理装置のカタログ管理手段が、前記各提供元データ管理装置の前記データベースに記憶されている、前記パーソナルデータを除く前記元データを取り込み、一元化し、かつ編集を行ってデータカタログを生成するパーソナルデータ流通管理方法。

[請求項13] 前記データ流通管理装置が、生成した前記データカタログを前記ネットワーク上で閲覧可能な状態にする請求項12に記載のパーソナルデータ流通管理方法。

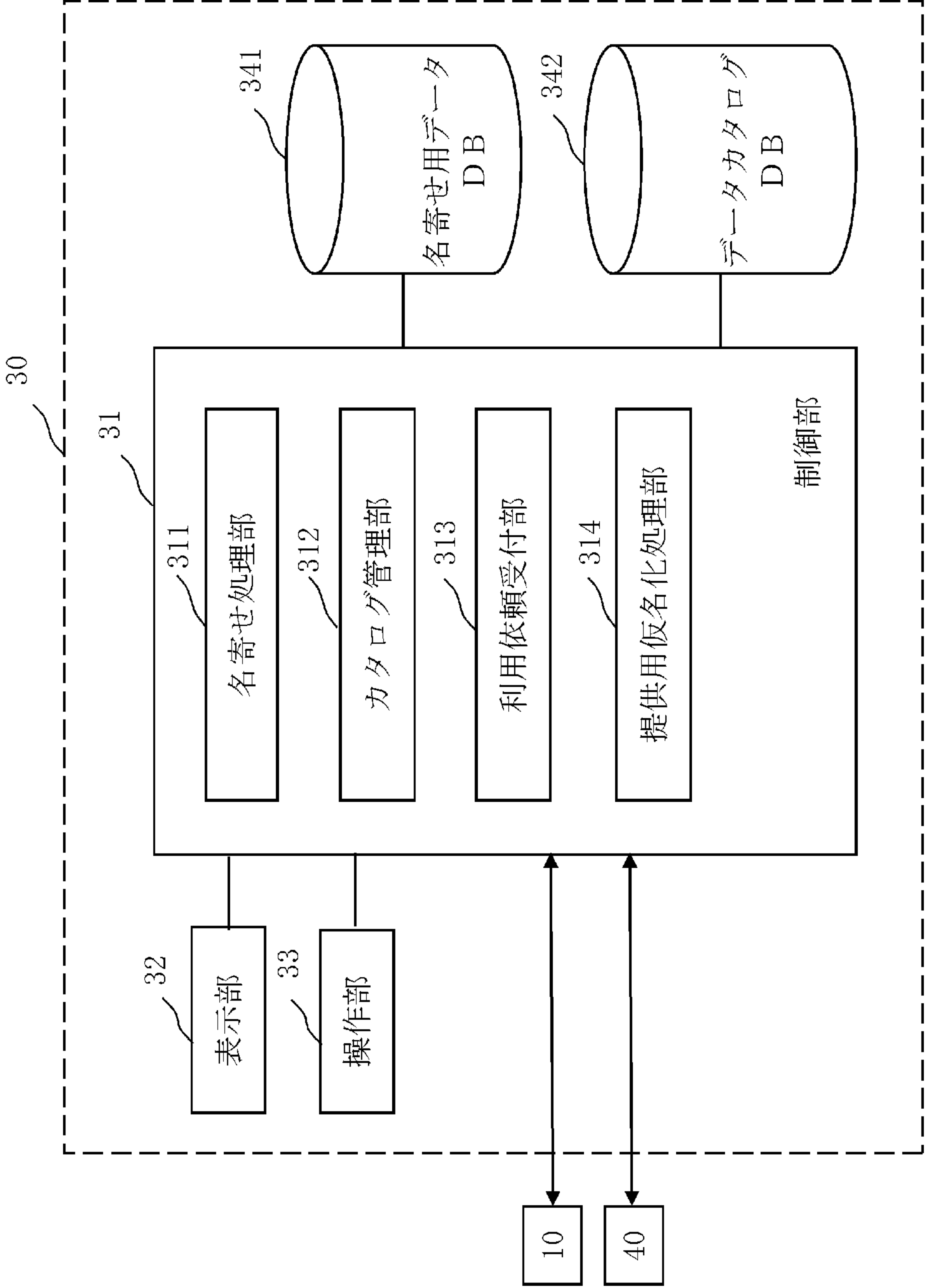
【図1】



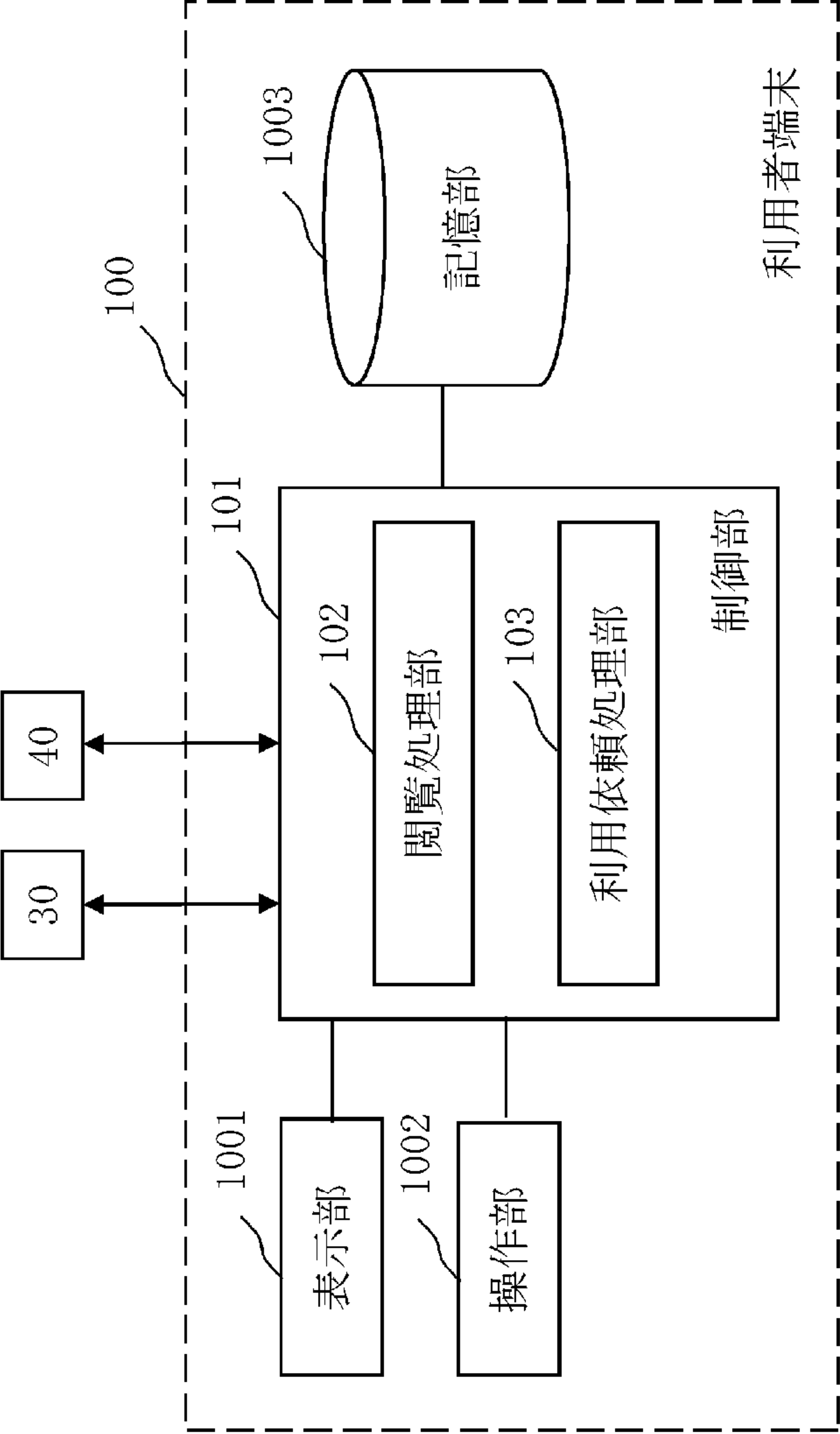
[図2]



[図3]



[図4]



[図5]

(A)

データ提供元	メールアドレス
A	

(B)

実名	性別	年齢	メールアドレス	住所	一次仮名	情報口座	実データ

・
・
・

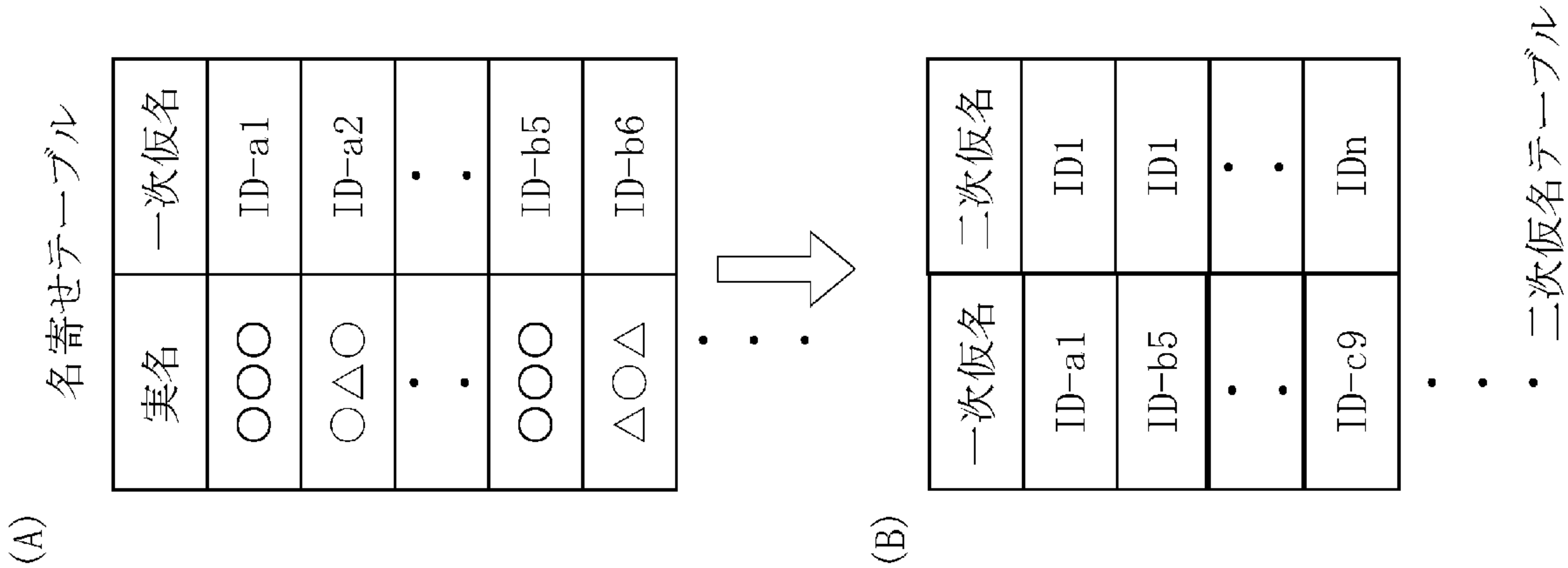
利権者	メールアドレス	収集者	メールアドレス	データ種類	測定器	他の測定条件（測定日時、場所他）

・
・
・

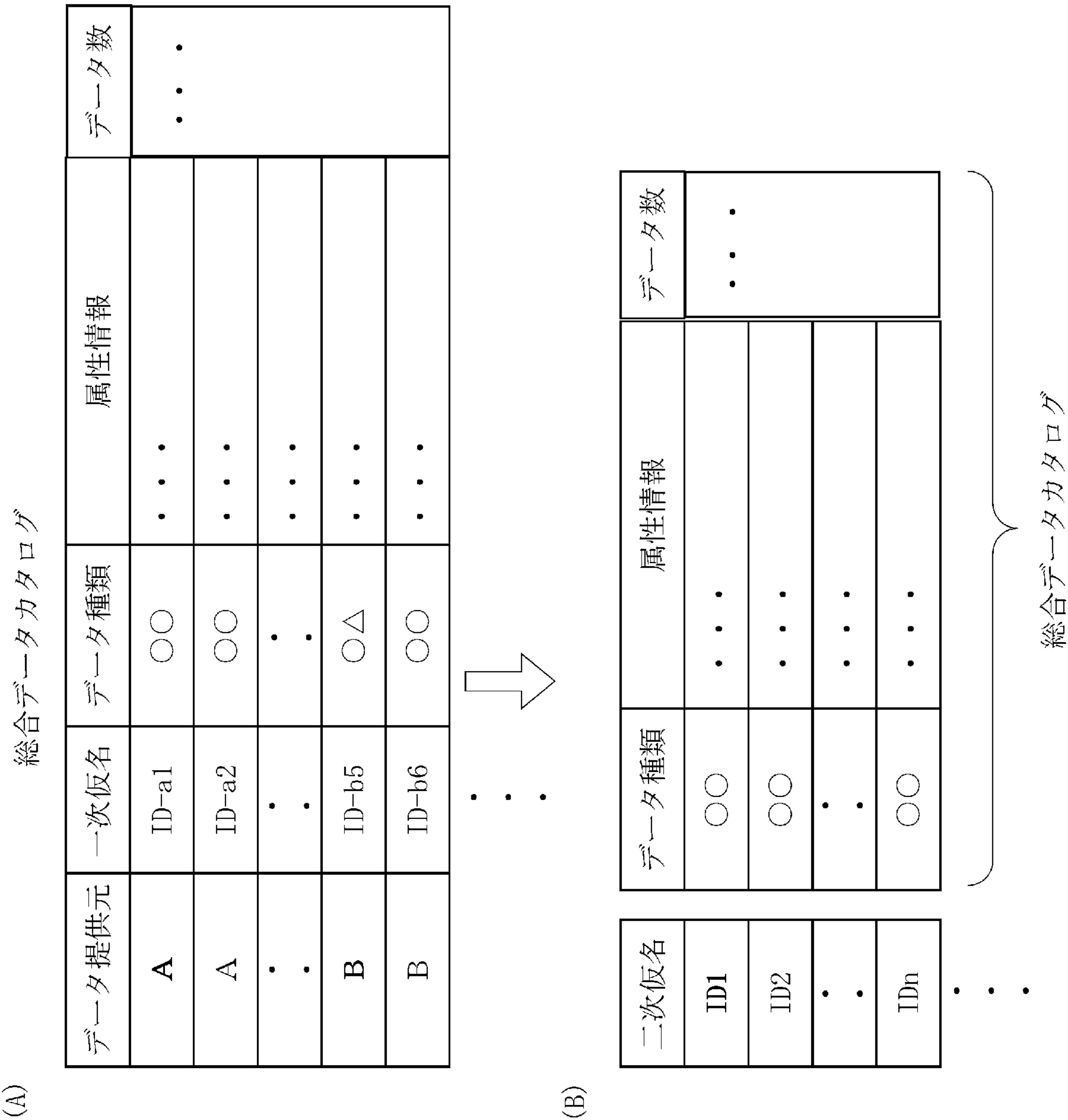
↓
データ数

属性情報

[図6]



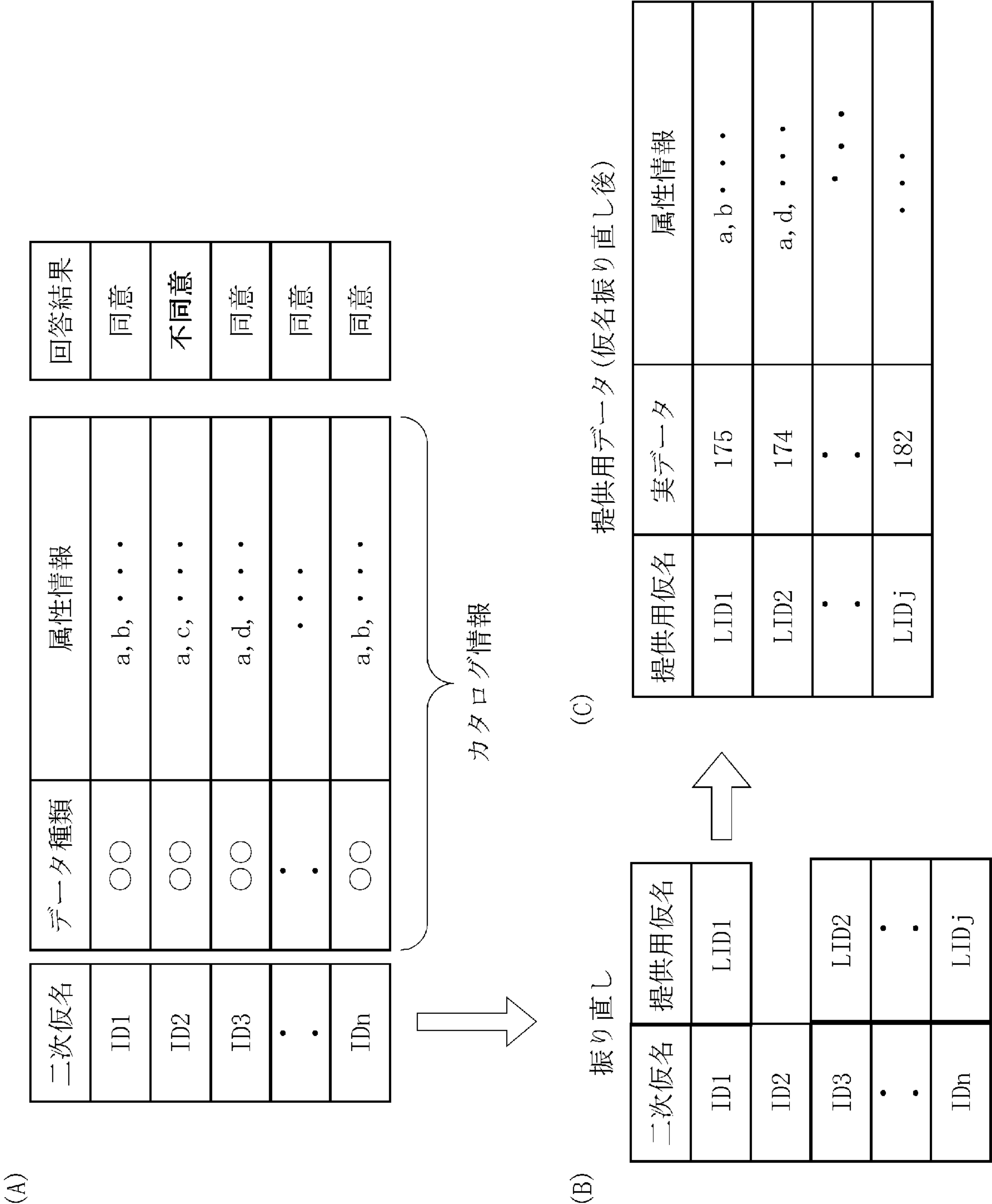
[図7]



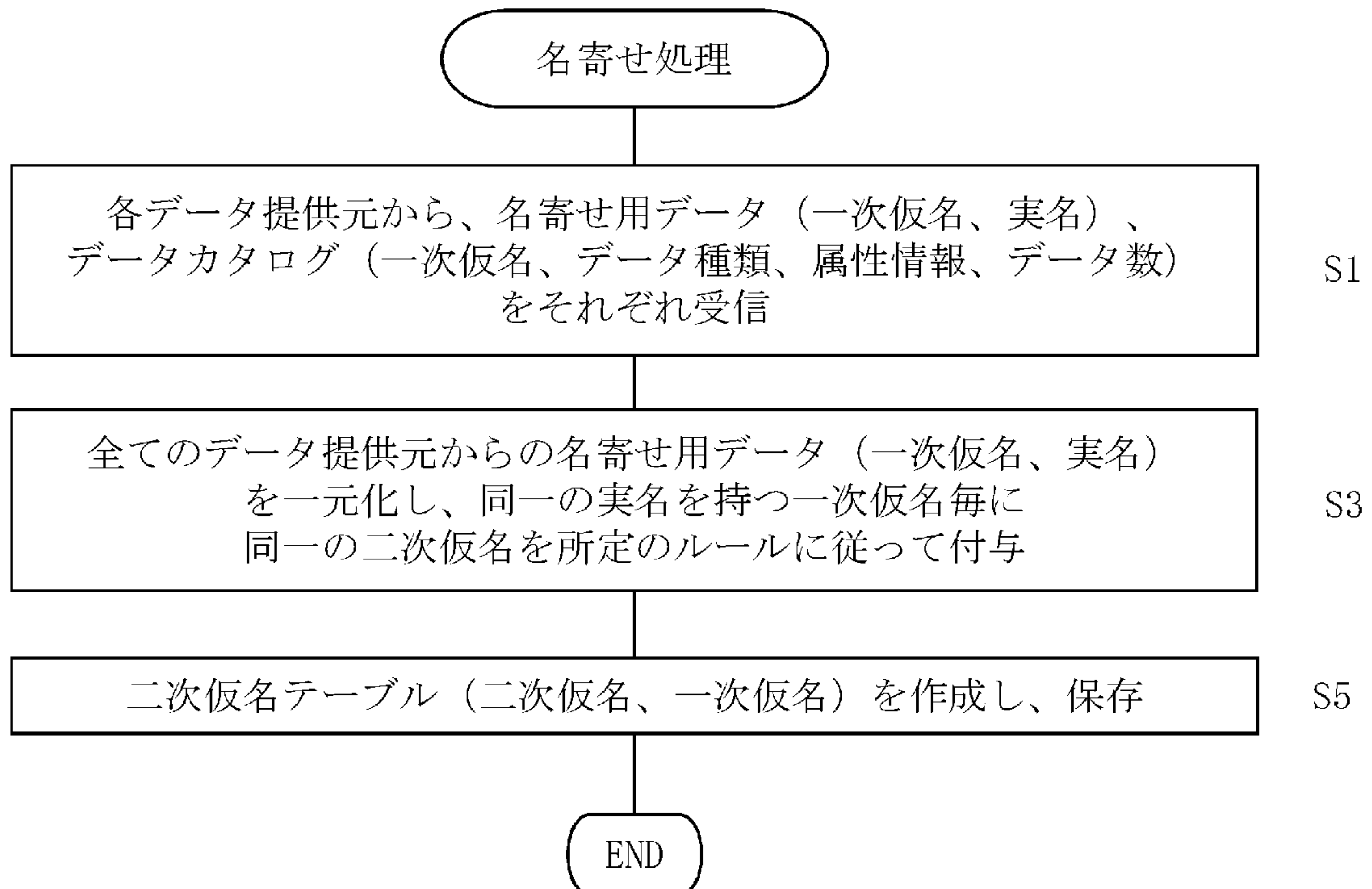
[図8]

利用依頼選択項目	
データ種類	〇〇
データ提供元	A
測定器	
他の属性情報	

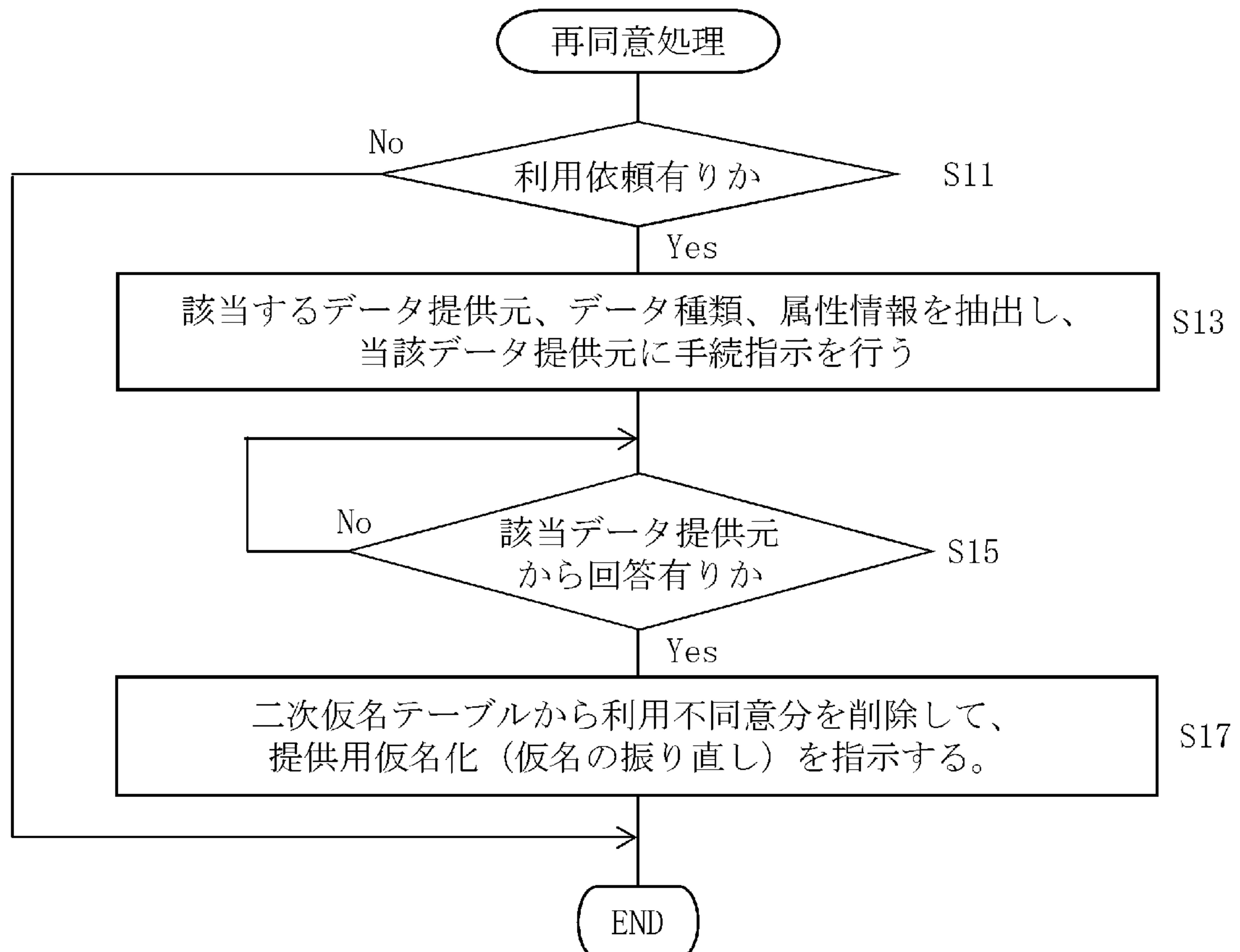
[図9]



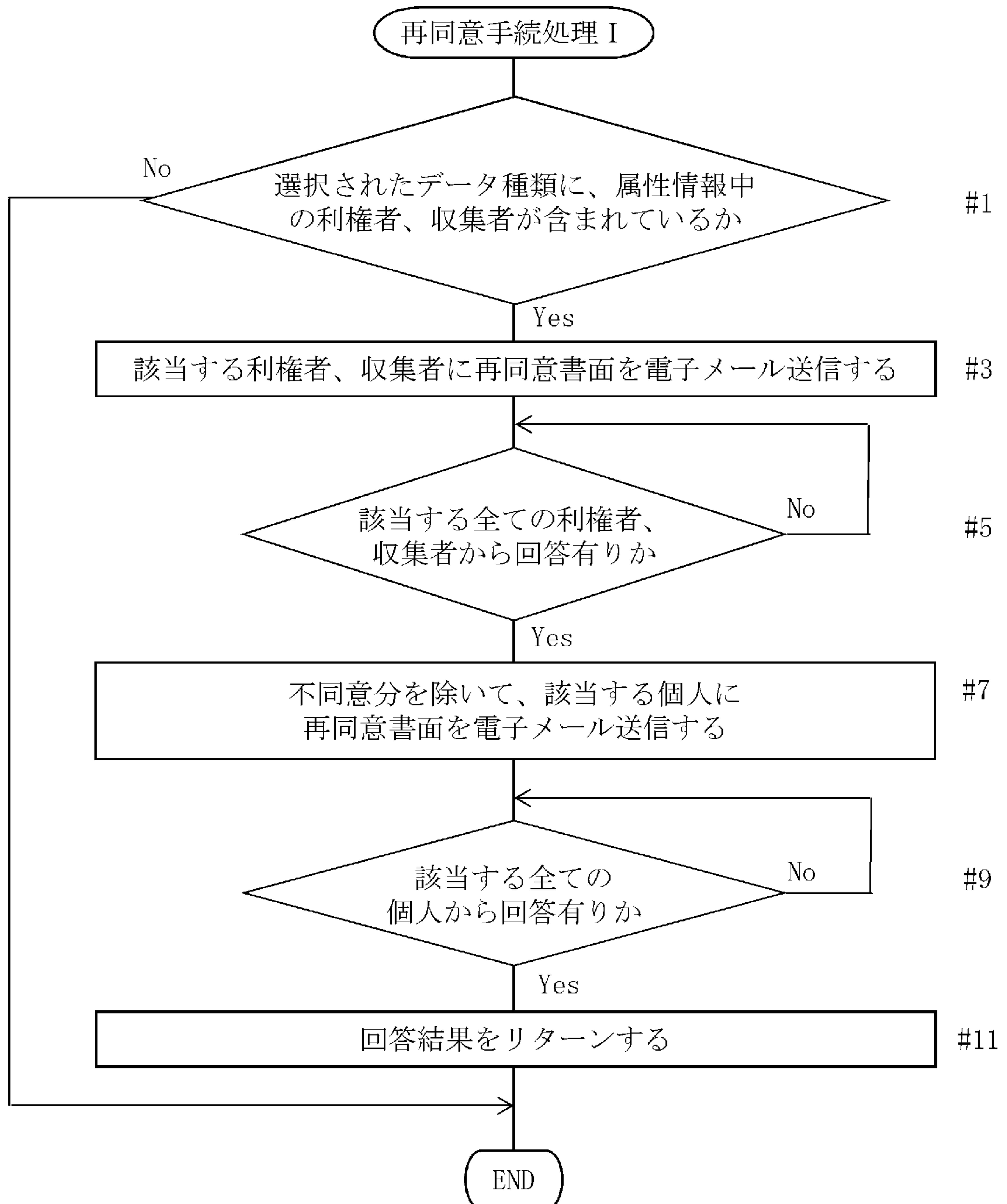
[図10]



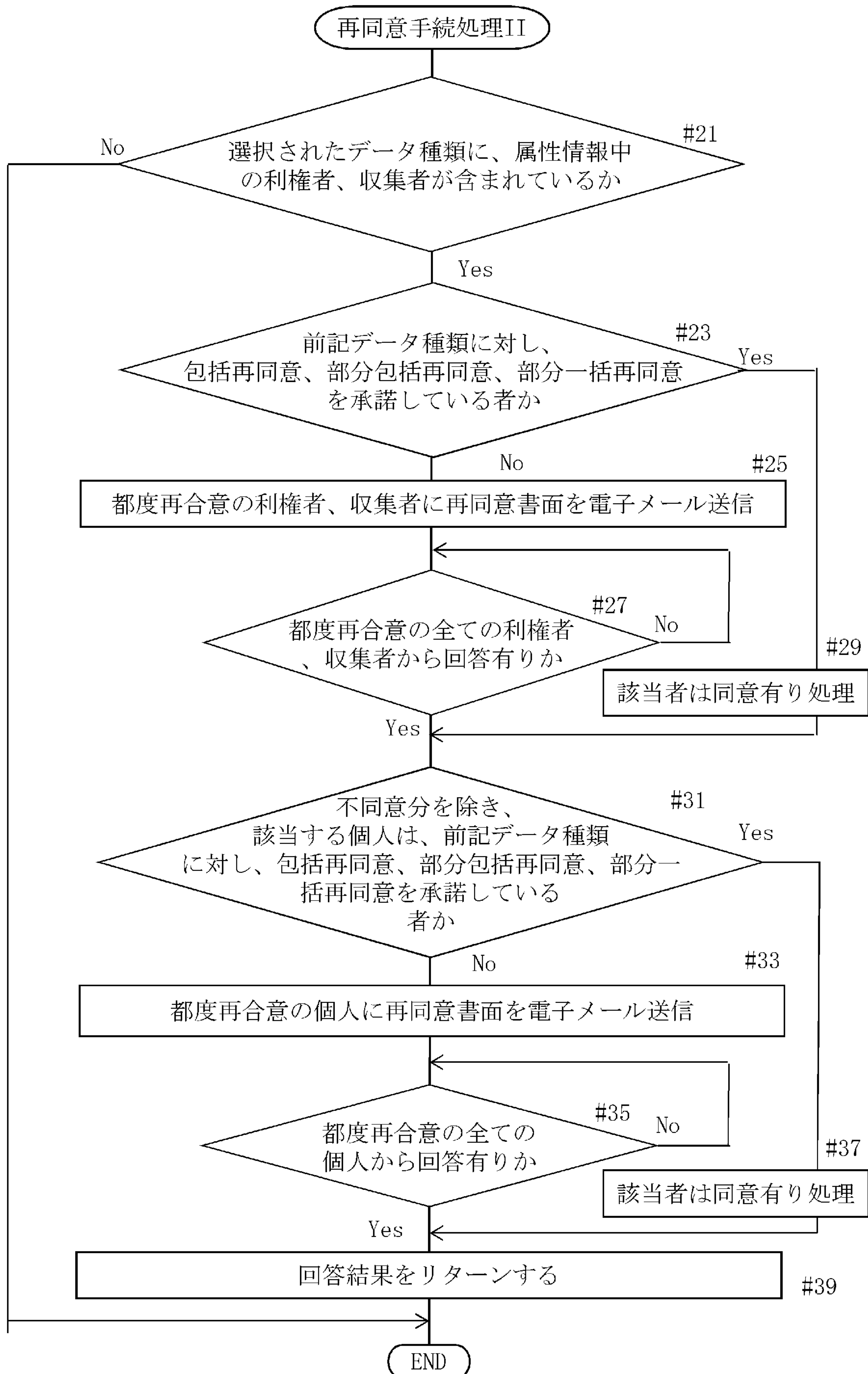
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/040568

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 50/10(2012.01) i

FI: G06Q50/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q10/00-99/00; G16H10/00-80/00; G06F21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2021

Registered utility model specifications of Japan 1996-2021

Published registered utility model applications of Japan 1994-2021

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2019-128681 A (FUJITSU LTD.) 01 August 2019 (2019-08-01) paragraphs [0010], [0012]-[0013], [0021]-[0023], [0028], [0031]-[0039]	2-3, 12-13 1, 4, 6, 11 5, 7-10
Y A	JP 2005-346248 A (MPO CO., LTD.) 15 December 2005 (2005-12-15) paragraphs [0029], [0038]	1, 4, 6, 11 5, 7-10
Y A	JP 2014-199589 A (NIFTY CORPORATION) 23 October 2014 (2014-10-23) paragraphs [0026]-[0032], [0078]	1, 4, 6, 11 5, 7-10
Y A	渡邊 涼介, 企業における個人情報・プライバシー情報の利活用と管理, 第 1 版, 株式会社青林書院, 02 May 2018, page 106, ISBN:978-4-417-01735-6, p. 106, non-official translation (WATANABE, Ryosuke, "Personal information in the company, Utilization and management of privacy information", 1st edition, SEIRIN SHOIN)	4, 6 5, 7-10



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

18 January 2021 (18.01.2021)

Date of mailing of the international search report

26 January 2021 (26.01.2021)

Name and mailing address of the ISA/

Japan Patent Office

3-4-3, Kasumigaseki, Chiyoda-ku,

Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2020/040568

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2007-141192 A (JAPAN MEDICAL INFORMATION RESEARCH INSTITUTE, INC.) 07 June 2007 (2007-06-07) paragraphs [0011], [0016], [0019], [0025]	1-13
A	JP 2011-34223 A (NTT DOCOMO INC.) 17 February 2011 (2011-02-17) paragraphs [0013]-[0019], [0033]-[0035]	1-13
A	JP 2013-54732 A (NHN CORPORATION) 21 March 2013 (2013-03-21) paragraphs [0030], [0042], [0047]	1-13
A	JP 2007-264827 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 11 October 2007 (2007-10-11) paragraphs [0040]-[0041], [0045], [0058]-[0060], [0070], [0096]	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2020/040568

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2019-128681 A	01 Aug. 2019	US 2019/0228180 A1 paragraphs [0039], [0041]-[0042], [0050]-[0052], [0057], [0060]-[0068]	
JP 2005-346248 A	15 Dec. 2005	(Family: none)	
JP 2014-199589 A	23 Oct. 2014	(Family: none)	
JP 2007-141192 A	07 Jun. 2007	(Family: none)	
JP 2011-34223 A	17 Feb. 2011	(Family: none)	
JP 2013-54732 A	21 Mar. 2013	US 2013/0232183 A1 paragraphs [0044], [0059], [0064]	
		KR 10-2013-0024345 A	
		JP 2014-142973 A	
JP 2007-264827 A	11 Oct. 2007	(Family: none)	

国際調査報告		国際出願番号 PCT/JP2020/040568
A. 発明の属する分野の分類（国際特許分類（IPC）） G06Q 50/10(2012.01)i FI: G06Q50/10		
B. 調査を行った分野		
調査を行った最小限資料（国際特許分類（IPC）） G06Q10/00-99/00; G16H10/00-80/00; G06F21/00		
最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922 - 1996年 日本国公開実用新案公報 1971 - 2021年 日本国実用新案登録公報 1996 - 2021年 日本国登録実用新案公報 1994 - 2021年		
国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
X	JP 2019-128681 A（富士通株式会社）01.08.2019（2019 - 08 - 01） 段落[0010], [0012]-[0013], [0021]-[0023], [0028], [0031]-[0039]	2-3, 12-13
Y		1, 4, 6, 11
A		5, 7-10
Y	JP 2005-346248 A（株式会社エム・ピー・オー）15.12.2005（2005 - 12 - 15） 段落[0029], [0038]	1, 4, 6, 11
A		5, 7-10
Y	JP 2014-199589 A（ニフティ株式会社）23.10.2014（2014 - 10 - 23） 段落[0026]--[0032], [0078]	1, 4, 6, 11
A		5, 7-10
Y	渡邊 涼介，企業における個人情報・プライバシー情報の利活用と管理，第1版，株式会社青林書院，2018.05.02，第106頁，ISBN:978-4-417-01735-6 p.106	4, 6
A		5, 7-10
☒ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技術水準を示すもの “E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの “L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す） “O” 口頭による開示、使用、展示等に言及する文献 “P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献 “T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの “X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの “Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの “&” 同一パテントファミリー文献		
国際調査を完了した日 18.01.2021	国際調査報告の発送日 26.01.2021	
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 渡邊 加寿磨 5L 5875 電話番号 03-3581-1101 内線 3563	

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2007-141192 A (株式会社医療情報総合研究所) 07.06.2007 (2007 - 06 - 07) 段落[0011], [0016], [0019], [0025]	1-13
A	JP 2011-34223 A (株式会社エヌ・ティ・ティ・ドコモ) 17.02.2011 (2011 - 02 - 17) 段落[0013]-[0019], [0033]-[0035]	1-13
A	JP 2013-54732 A (エヌエイチエヌ コーポレーション) 21.03.2013 (2013 - 03 - 21) 段落[0030], [0042], [0047]	1-13
A	JP 2007-264827 A (松下電器産業株式会社) 11.10.2007 (2007 - 10 - 11) 段落[0040]-[0041], [0045], [0058]-[0060], [0070], [0096]	1-13

引用文献			公表日	パテントファミリー文献	公表日
JP	2019-128681	A	01.08.2019	US 2019/0228180 A1 段落[0039],[0041]-[0042], [0050]-[0052],[0057],[0060]-[0068]	
JP	2005-346248	A	15.12.2005	(ファミリーなし)	
JP	2014-199589	A	23.10.2014	(ファミリーなし)	
JP	2007-141192	A	07.06.2007	(ファミリーなし)	
JP	2011-34223	A	17.02.2011	(ファミリーなし)	
JP	2013-54732	A	21.03.2013	US 2013/0232183 A1 段落[0044],[0059],[0064] KR 10-2013-0024345 A JP 2014-142973 A	
JP	2007-264827	A	11.10.2007	(ファミリーなし)	