

明 細 書

発明の名称：匿名化データの粒度管理装置および粒度管理方法 技術分野

[0001] 本発明は、データ提供事業者、例えば複数のサービス提供事業者、複数のサービス享受事業者などから提供される匿名化データの粒度を評価し、管理する機能を有する匿名化データの粒度管理装置および粒度管理方法に関する。

[0002] 更に詳述すれば、本発明は、例えば、複数のサービス提供事業者や複数のサービス享受事業者側から提供される k -匿名性を満たす匿名化データ（以下、 k -匿名化データと言う）を受け、当該 k -匿名化データの粒度および k の値を元に当該データの受け入れ可否を評価し、当該 k -匿名化データから個人識別が識別されるような情報漏洩リスクの高いデータを拒否し、その他を受け入れ、管理する機能を有する匿名化データの粒度管理装置および粒度管理方法に関する。

本発明は、匿名化データの粒度管理装置および粒度管理方法にあって、匿名化に関係しない項目のデータ（非匿名化データ）についても、データ粒度を揃えて、受け入れを管理する機能を有するものであってもよい。

背景技術

[0003] インターネットの発展に伴い、企業の業種や業務内容を切り口にして、それぞれに有効なサービスを提供する各種サービス事業者、例えば飲食業界に対して人気メニューなどの商品情報を提供するサービス事業者や当該サービス事業者食材などを提供したりする卸サービス事業者や小売サービス事業者、食材などの生産事業者などが増加している。

[0004] 例えば、近年、インターネットやWebなどを利用して、飲食店などのサービス享受事業者側に特定の業務サービスを提供するサービス提供事業者側に対して、その特定の業務サービスの基盤となるサービス基盤を提供し、該サービス基盤に基づく業務サービスをもってサービス享受事業者側のビジネ

スを支援するサービス提供システムが存在する。

[0005] このようなサービス提供システムは、サービス基盤事業者装置、サービス提供事業者装置、サービス享受事業者装置、及びユーザ端末装置を有する。

[0006] サービス基盤事業者装置は、提供するサービス基盤に基づく機能（サービス）、例えばSaaS（Software as a Service）型による業務システムをサービス提供事業者装置に提供するシステム又は装置である。

[0007] サービス提供事業者装置は、サービス基盤事業者装置から提供されるサービス基盤に基づく業務システム（業務SaaS）を受けるシステム又は装置である。また、例えば、当該業務システムをサービス享受事業者（或いは直接ユーザから）の要求に応じてカスタマイズしてサービス享受事業者に提供するシステム又は装置である。

[0008] サービス享受事業者装置は、例えばユーザから提供されるユーザ情報をサービス提供事業者装置側に提供する装置である。

[0009] ユーザ端末装置は、例えば、自らユーザ情報を入力し、サービス享受事業者装置側に提供する端末である。また、このユーザ端末装置は、ユーザ自身の携帯端末をかざすことにより、当該携帯端末の情報を自動的に収集することができるようなものであってもよい。

そして、サービス享受事業者やサービス提供事業者が所有するオリジナルユーザ情報は、有益な情報を含んでいる。サービス基盤事業者は、この有益なオリジナルユーザ情報の提供を受け、当該情報の分析を可能とすれば、よりよいビジネス支援を行うことが期待できる。

[0010] 本技術分野の背景技術として、特開2009-93569号公報（特許文献1）、特開平9-153094号公報（特許文献2）、「個人情報匿名化技術」（非特許文献1）がある。

[0011] 特許文献1には、SaaS環境からSI環境へ変更する場合、SaaS形態で利用を始めた業務サービスにおいて、埋没コストや機会損失の発生を軽減するものであり、業務サービスをSaaS事業者環境（A社）からSI形態の環境（B市）に移行する場合、B市に業務サービスのアドレスを記録す

るサービスアドレスリストを設け、業務サービスの移行に合わせてサービスアドレスリストのアドレスを更新する。また、A社に蓄積された業務データも移行する場合、A社及びB市に業務データのアドレスを記録するデータアドレスリストを設け、業務データの移行に合わせて双方のデータアドレスリストのアドレスを更新する。それらの更新においては、アドレスが論理的に同一になるようにアクセス方法を変更する技術が開示されている。

[0012] 特許文献2には、顧客に関する情報と、顧客が商品の購入を検討したときに参照した商品の情報と、顧客が購入した商品の情報とから商品の販売促進効果を分析する販売促進効果分析方法及びその実施システムが開示されている。

[0013] 非特許文献1には、収集した個人情報を企業の資産として利用するためのk-匿名化技術が開示されている。

先行技術文献

特許文献

[0014] 特許文献1：特開2009-93569号公報

特許文献2：特開平9-153094号公報

非特許文献

[0015] 非特許文献1：http://www.meti.go.jp/policy/it_policy/daikoukai/igvp/contents/pdf/C-1.pdf

発明の開示

発明が解決しようとする課題

[0016] 特許文献1に記載されたようなサービス提供システムによれば、サービス基盤事業者は、サービス提供事業者の業務支援ができる。また、サービス提供事業者は、サービス享受事業者の業務支援ができる。そして、これらの業務支援により、システム全体の業務を効率化でき、業務効率を向上することができる。

[0017] また、係るサービスを提供する各サービス提供事業者及びサービス基盤事

業者側では、それぞれ各ユーザに関するデータ、例えば嗜好や行動履歴などのデータを保持（蓄積）、管理しているのが通常である。

[0018] 従って、このユーザに関するデータを分析し、当該分析結果に基づく有益な情報をサービス提供事業者からサービスの提供を受ける側のサービス享受事業者（店舗、一般企業など）に対して、提供できるシステムがあれば、より業務効率を向上することが期待できる。

[0019] ここで、本発明における「ユーザ」とは、本システムを利用する個人、団体、企業であり、特定ユーザ（一の個人、一の団体、一の企業が特定可能なユーザ）と不特定ユーザ（個人、団体、企業が特定不可能又は特定困難なユーザ）を含む。ユーザが本システムで使用する端末等を「ユーザ側端末」と言う。以下、本発明において、ユーザに関して「個人」とした用語はユーザとしての団体及び企業を含むものである。

[0020] また、「サービス享受事業者」とは、本システムによる本来事業支援サービス（第1のサービス）の提供を受ける事業体であり、当該サービス享受事業者側に設けられたシステム構成装置を「サービス享受事業者装置」と言う。ここでの「側に設ける」との用語の意義は、サービス享受事業者内に設けることのみを意味するものではない。この「側に設ける」との用語は、以下同様に用いる。

[0021] また、「サービス提供事業者」とは、本システムによる本来事業支援サービス（第1のサービス）を提供する事業体であり、当該サービス提供事業者側に設けられたシステム構成装置を「サービス提供事業者装置」と言う。

[0022] また、「サービス基盤事業者」とは、複数のサービス提供事業者を束ねる企業であって、サービスの基盤、例えば業務や予約機能（業務サービスや予約サービス）などをサービス提供事業者及び／又はサービス享受事業者に提供する事業体である。そして、契約に基づきサービス享受事業者装置及び／又はサービス提供事業者装置から、情報を随時収集し、当該情報を例えば分析して、サービス享受事業者側及び／又はサービス提供事業者側に分析情報（第2のサービス）として提供する。当該サービス基盤事業者側に設けられ

たシステム構成装置を「サービス基盤事業者装置」と言う。

[0023] また、「データ提供事業者」とは、サービス提供事業者やサービス享受事業者を指している。そして、オリジナルユーザ情報 I a、I b、を k-匿名性を満たす匿名化データ X I a、X I b をサービス基盤事業者側に提供するデータとして送信する。当該データ提供事業者側に設けられたシステム構成装置を「データ提供事業者装置」と言う。

[0024] また、サービス基盤事業者は、複数のサービス提供事業者を束ねる企業であることから、当該サービス基盤事業者側において、複数のサービス提供事業者側に蓄積している各種データを融合し、分析することができれば、より高付加価値な分析が可能となり、その結果として、サービスをサービス提供事業者、又は／及びサービス享受事業者を含むユーザに対して、より高付加価値な分析結果を提供することが可能となる。

[0025] 大容量データの分析が可能な IT 環境が整いつつある現状にあっては、技術的には、大容量データから、上述した高付加価値な分析を行うことは可能である。

[0026] 「高付加価値な分析」とは、パーソナライゼーション (Personalization : 得意客、および見込みユーザごとの好みや属性に応じた情報を電子メールなどで発信すること) や併売リコメンド (recommendation : ユーザの好み进行分析し、各ユーザごとに興味のある情報を選択して表示するサービスのこと) などを実現可能にする基礎データを提供するための分析を言う。

[0027] 「粒度」とは、分析するデータの粗さ、あるいは細かさを示し、分析データの何処までを分析単位としてみるか、ということと言う。本例では、説明を簡略する意味で、主として k-匿名化データの粒度を挙げて説明する。

[0028] しかし、サービス提供事業者やサービス基盤事業者側において、この高付加価値な分析を行うとき、課題となるのが、各サービス享受事業者側の以下のような要望に対してどのように対処するか、大きな課題があった。

[0029] 例えば、特に同じ業種に属しているサービス享受事業者 (例えば、飲食店など) である場合、各サービス享受事業者間では、「同じ地区の同じジャン

ルのお店（サービス享受事業者）には、情報は提供したくない」と言う要望である。

[0030] また、業務サービス事業者を利用しているサービス享受事業者は、「同業他社のサービス享受事業者には、情報を提供したくない」と言う要望である。

[0031] 従来、このような要望に対処できるシステム、つまりサービス提供事業者、及びサービス基盤事業者において、複数のサービス享受事業者から収集した各種データを融合し、より高付加価値な分析を行い、当該分析情報をサービス享受事業者が相互にビジネス上有益と思われるサービスとして提供するものとして、例えば、「単純匿名化」を用いたサービス（以下、単純匿名化サービスと言う）が考えられる。すなわち、利用者（ユーザ）の情報から個人情報情報を分離し、「個人を特定できる識別情報（単独でも個人を一意に特定できる情報、例えば氏名、完全な住所、メールアドレス等）」は、「仮名化」などの「単純匿名化」を施した上で、サービス事業者が管理する方法である。つまり、これらの情報を分離して管理し、かつこれらの情報を統一のIDで紐付けし、関連性を維持しながら、機微な情報を管理する構成である。

[0032] この単純匿名化サービスによれば、「個人ごとの情報」は匿名化情報であるので、情報リスク低減の効果は期待できる。しかし、このような単純匿名化サービスは、個人情報情報を保護する、と言う観点から見ると、個人情報漏洩リスクを完全に取り去ることは難しい、と言う課題がある。

[0033] 係る課題（個人情報漏洩リスクのみ）を是正する方法として、非特許文献1に記載されたk-匿名化手法を用いることが考えられる。

[0034] しかし、k-匿名化技術を用いてデータを収集する場合、複数のデータ提供事業者間において、k-匿名化処理におけるデータ粒度をコントロールできない。

つまり、単純匿名化サービスは、サービス事業者側から、例えば「一部情報を匿名化して預けたい」、「個人ごとの情報を個人を特定できないように管理したい」、「匿名情報のみでサービスしたい」など、サービス事業者側

に委ねられていることから、複数のデータ提供事業者間の匿名化データを融合して分析するに際して、データ粒度が異なることに起因して、分析の軸が合わずに、分析ができない、若しくは分析精度が下がる、という新たな課題があった。

[0035] また、分析方法として、特許文献2に記載の如く、サービス享受事業者側から収集した情報を、統計分析技術を利用して、分析する方法が考えられるが、当該統計分析では統計処理を行った分析であることから、個別のサービス享受事業者を推測することは不可能な分析結果となり、サービス享受事業者側にとって、上述したような高付加価値な分析情報を得ることは期待できない。

[0036] その一方、サービス享受事業者側は、各サービス享受事業者（自社）が持っている情報の中から特定の情報ならば、他のサービス提供事業者、或いは他のサービス享受授業者に対して有償で提供してもよいとの要望もある。つまり、自社にとって不都合がなければ、自社の情報を積極的に「売る」と言う発想である。

[0037] そこで、本発明は、例えば、サービス基盤事業者側において、当該サービス基盤事業者から提供される粒度定義書に基づき、複数のデータ提供事業者にて作成される様々なk-匿名化データテーブル（以下、k-匿名化データ、t bと言う）を収集し、当該k-匿名化データ、t bに含まれる情報を元に当該データを受入るか否かのデータ評価を可能とする匿名化データの粒度管理装置および粒度管理方法を提供することにある。

[0038] また、本発明は、受け入れデータに対して、タイムスタンプ、課金情報などを付与することが可能な匿名化データの粒度管理装置および粒度管理方法を提供することにある。

課題を解決するための手段

[0039] 上記課題を達成するために、本発明は、サービス基盤事業者装置側からデータ提供事業者装置側にデータ粒度を定義する粒度定義書類ファイル（以下、粒度定義書、CSVと言う）を送信し、当該粒度定義書、CSVに基づい

て、当該データ提供事業者装置側にて作成される k -匿名化データを含む k -匿名化データ。 t_b を受け、当該 k -匿名化。 t_b に含まれる、データの安全性の指標となる k の値および／またはデータの粒度の条件を満たしたデータのみを、受け入れるデータ評価を行う手段を設けたことにある。

[0040] k -匿名化データ j 。 t_b には、 k -匿名化データその他、非匿名化データが含まれていてもよい。 k -匿名化処理は、提供するデータの準識別子（氏名や住所など）に対して行う。

[0041] 具体的には、例えば以下のとおりである。

[0042] 本発明の匿名化データの粒度管理装置は、データ提供事業者装置と、サービス基盤事業者装置と、を有し、前記サービス基盤事業者装置は、前記データ提供事業者装置に対して、データの粒度を定義する粒度定義書、 CSV を配信する手段と、前記データ提供事業者装置側にて前記粒度定義書、 CSV に基づき作成される k -匿名化データを含む k -匿名化データ。 t_b を受ける手段と、前記 k -匿名化データ。 t_b の k -匿名化データの粒度および k の値をもって、前記 k -匿名化データを受け入れるか否かを評価する手段と、を有し、前記 k -匿名化データから、個人情報漏洩リスクを防止し、かつ複数の k -匿名化データの融合、分析精度を向上することを可能とすることを特徴とする。

[0043] 前記 k -匿名化データ。 t_b を受ける手段は、前記 k -匿名化データ。 t_b の前記粒度定義書、 CSV で定義されている k -匿名化処理された前記 k -匿名化データを受けるとき、前記データ提供事業者装置から当該データの提供者を特定する ID 、定義書 No を受ける、ことを特徴とする。

[0044] 前記匿名化データの粒度管理装置は、さらに、前記データ評価手段により、受入れ可能と判断した場合、当該データにタイムスタンプおよび報奨金情報を付与する手段と、前記データ受入れ否と判断した場合、その旨を前記データ提供事業者装置側に通知する手段、を有する、ことを特徴とする。

[0045] 前記匿名化データの粒度管理装置は、前記データ評価手段による評価結果、データ受入可とした場合、前記記憶手段に登録する手段、前記受入れたデ

ータを分析するデータ分析手段、を有し、前記サービス基盤事業者装置側にて、前記データ提供事業者装置から受入れ可能な複数のデータを分析対象データとして融合し、当該融合データを前記データ分析手段により、分析した分析データとし前記データ提供装置側に配信送付可能とすることを特徴とする。

[0046] 前記匿名化データの粒度管理装置であって、前記粒度定義書、CSVは、データ粒度定義が1種類、又は異なる複数の種類からなり、前記粒度定義書、CSVに基づき作成される前記k-匿名化データ、tbは1種類、又は2種類以上の複数のデータの集まりである、ことを特徴とする。

[0047] 本発明の匿名化データの粒度管理方法は、データ提供事業者装置と、サービス基盤事業者装置と、を有し、前記サービス基盤事業者装置側において、前記データ提供事業者装置側から送られてくる匿名化データの粒度を管理する方法であって、前記データ提供事業者装置に対して、データの粒度を定義する粒度定義書、CSVを配信するステップと、前記データ提供事業者装置側にて前記粒度定義書、CSVに基づき作成されるk-匿名化データを含むk-匿名化データ、tbを受け取るステップと、前記k-匿名化データ、tbのk-匿名化データの粒度およびkの値をもって、前記k-匿名化データを受け入れるか否かを評価するステップと、を有し、前記k-匿名化データから、個人情報漏洩リスクを防止し、かつ複数のk-匿名化データの融合、分析精度を向上することを特徴とする。

[0048] 前記匿名化データの粒度管理方法であって、さらに、前記データ評価手段により、受入れ可能と判断した場合、当該データにタイムスタンプおよび報奨金情報を付与するステップと、前記データ受入れ否と判断した場合、その旨を前記データ提供事業者装置側に通知するステップと、を有する、ことを特徴とする。

[0049] 前記匿名化データの粒度管理方法であって、前記データ評価手段による評価結果、データ受入可とした場合、前記記憶手段に登録するステップと、前記受入れたデータを分析するステップと、を有し、前記サービス基盤事業者

装置側にて、前記データ提供事業者装置から受入れ可能な複数のデータを分析対象データとして融合し、当該融合データを前記データ分析手段により、分析した分析データとし、配信することを特徴とする。

発明の効果

[0050] 本発明によれば、サービス基盤事業者側において、データ粒度を定義しているので、データ提供事業者からの k -匿名化データの準識別子、例えば場所、時間の粒度が揃った k -匿名化処理データを収集することができ、データ提供事業者間のデータを統合／融合して分析する際、分析の軸が合った分析作業をスムーズに行うことができる。

[0051] また、サービス基盤事業者側で、 k -匿名化データの k の値を指定することによって、データ提供事業者側から見れば、データ提供事業者から収集したデータは、既に k 匿名化されている故に、サービス基盤事業者にて個人情報漏洩対策（ k -匿名化処理）を改めてする行う必要がない、と言う効果を奏する。

[0052] 例えば、単純匿名化では、個人情報漏洩リスクがあったが、 k -匿名化により、個人情報リスクを除去することができ、より安全、安心なサービスを提供することが可能である。また、 k -匿名化したデータであってもデータ提供事業者間のデータ共有や統合／融合が可能である。

[0053] 上述した以外の課題、構成及び効果は、以下の実施形態の説明により明らかにされる。

図面の簡単な説明

[0054] [図1]本発明の匿名化データの粒度管理装置が提供されるサービス提供システムの全体概要を示す図である。

[図2]図1のサービス基盤事業者装置とデータ提供事業者装置の各構成を示すブロック図である。

[図3]図2のサービス基盤事業者装置の演算装置（制御手段）の構成例を示すブロック図である。

[図4]図2の粒度定義書管理マスタDBのテーブル例を示す図である。

[図5]図2の粒度定義書管理マスタDBの粒度定義書。CSV例を示す図である。

[図6]図2のk-匿名化データ作成部により作成されるk-匿名化データ。tbのデータの構成例を示す図である。

[図7]k-匿名化データ。tb（テーブル名G0001。tb）の一例（k=1であって、データ受入れ不可）を示す図である。

[図8]k-匿名化データ。tb（テーブル名G0001。tb）の一例（k=2であって、データ受入れ可）を示す図である。

[図9]k-匿名化データ管理マスタDB3122のテーブル例である。

[図10]本発明の匿名化データの粒度管理装置の処理フローを説明するフローチャート図である。

発明を実施するための形態

[0055] 以下、その実施態様について図面を参照して説明する。まず、サービス享受事業者のビジネスを支援するサービス提供システムの概略について説明する。

[0056] サービス提供システムは、アプリケーションサービスやSI、つまり予約機能や業務SaaSなどのサービス（第1のサービスS1）をサービス提供事業者側に提供するサービス基盤事業者システム又は装置（以下、サービス基盤事業者装置と称する）と、サービス享受事業者（飲食店など）の要望に応じて第1のサービスをカスタマイズしてサービス享受事業者に提供するサービス提供事業者システム又は装置（以下、サービス提供事業者装置と称する）と、から構成される。

[0057] サービス享受事業者（飲食店など）は、ユーザ（消費者）に飲食や商材などを提供し、またユーザからユーザ情報（オリジナル情報）の提供を受ける。

[0058] サービス基盤事業者装置は、SaaS以外、例えばOSを含むプラットフォームを貸し出しするPaaS（Platform as a Service）、ASP（Application Service Provider）サービス等を提供する装置であってもよい。

[0059] 以下、飲食業界（飲食店）と、そのサービス提供事業者と、サービス基盤事業者とを主として説明する。

[0060] まず、サービス提供システムの概要について説明する。サービス提供システムのサービス基盤事業者装置は、サービス提供事業者装置に対して予約管理サービス（アプリケーションサービス）などを提供するアプリケーションサーバ（以下、サービス基盤事業者用サーバと称する）を有する。

[0061] サービス提供事業者装置は、この予約管理サービスをサービス享受事業者の要望に沿ってカスタマイズし、サービス享受事業者からユーザ（消費者）の予約情報を受付け管理するアプリケーションサーバ（以下、サービス提供事業者用サーバと称する）を有する。つまり、サービス基盤事業者装置とサービス提供事業者装置との協働をもって、サービス享受事業者のビジネスを支援する仕組みである。

[0062] このような仕組みのシステムは、一般的にサービス享受事業者毎の個別案件ベースで対応するものである。

従って、サービス基盤事業者装置は、サービス提供事業者装置に対して、第1のサービスS1を提供し、サービス提供事業者装置はサービス享受事業者に対して、カスタマイズした第1のサービス（サービス開始）を提供し、また該提供した第1のサービスに基づくユーザ情報（オリジナル情報）Ia、Ibなどを管理するのみであった。

[0063] このサービス提供方法としては、例えばSaaSが挙げられる。SaaSとは、情報システム（ソフトウェア）が提供する機能（第1のサービス）を、サービス提供事業者やサービス享受事業者が、特に新たなシステムを構築・導入することなく、ネットワーク経由で利用することを可能にするICT活用環境である。

[0064] 一般的には、SaaSでは、必要なときに必要なサービスを、特別なシステム構築の必要もなく素早く利用できるというメリットがある。また、SaaSでは、社内に特別な環境を用意する必要はないことから、その機能（サービス）の運用開始時間を早め、コストも低減できる。また、インターネッ

トやWANを使用することになるが、ネットワークやブラウザの技術革新により、社内システムを利用するのとほぼ同等の操作が可能である。

[0065] また、サービス提供事業者やサービス享受事業者にとっては、サービス基盤事業者から提供されるSaaSやSI及び運用・保守を利用することにより、コスト削減、売上拡大を図ることが期待できる。

[0066] 本発明は、斯様なデータ提供事業者の装置（サービス提供事業者装置A、B、サービス享受事業者装置a1、a2、b1、b2など）からのデータを評価し、データ共有や融合、また個人情報漏洩リスクを取り去るものである。

[0067] 以下、本発明の実施例について図面に基づき、説明する。本実施例は、K-匿名化データであっても、間接個人識別が可能な提供データは、その受け入れを拒否し（個人情報漏洩防止）、第三者に公開しても個人識別の特定が困難なデータのみを受け入れ、当該受け入れた複数のデータを融合して効率的に分析することを可能とするものである。

実施例 1

[0068] 図1は、本発明の匿名化データの粒度管理装置をサービス基盤事業者装置に適用したサービス提供システムの全体構成を示す図である。

[0069] サービス提供システムは、データ提供事業者のデータ提供事業者装置12、サービス基盤事業者のサービス基盤事業者装置3、を有する。

[0070] データ提供事業者装置12は、複数のサービス提供事業者A、B・・・の複数のサービス提供事業者装置2、複数のサービス享受事業者a、b・・・のサービス享受事業者装置1、を有する。

[0071] データ提供事業者装置12は、データ提供事業者用サーバ121からなる。

各サービス享受事業者装置1は、例えば複数の店舗a1、a2や複数の企業b1、b2側の装置であって、サービス享受事業者用サーバ11からなる。そして、各サービス享受事業者用サーバ11は、オリジナルユーザ情報IaやIbをサービス提供事業者装置2に対して出力する。

- [0072] このオリジナルユーザ情報 I a や I b は、サービス基盤事業者装置 3 からネットワーク 4 を経由して提供する第 1 のサービス S 1（業務／予約機能など）に対応してユーザ側から送られてくるものである。
- [0073] 各サービス提供事業者装置 2 は、各オリジナルユーザ情報 I a、I b を受け、当該オリジナルユーザ情報の出所元、つまりユーザが特定できない程度に k-匿名化し、当該匿名化ユーザ情報 X I a、X I b を k-匿名化データとしてネットワーク 4 を介してサービス基盤事業者装置 3 側に送信する。
- [0074] k-匿名化は、例えば上述した非特許文献 1 の k 匿名化手法を利用する。その k-匿名化については後述する。
- [0075] サービス基盤事業者装置 3 は、サービス基盤事業者用サーバ 3 1 からなる。サービス基盤事業者用サーバ 3 1 は、データ提供事業者用サーバ 1 2 1 側に対して、データ粒度を定義する粒度定義書、C S V（Comma Separated Values：カンマで区切ったファイル形式）を配信し、また当該粒度定義書、C S V に基づき作成され、前記データ提供事業者用サーバ 1 2 1 から提供される k-匿名性を満たすデータを受け、当該データを評価する機能を有する。
- [0076] 図 2 は、サービス基盤事業者用サーバ 3 1 およびデータ提供事業者用サーバ 1 2 1 の構成を示すブロック図である。
- [0077] サービス基盤事業者用サーバ 3 1 は、入出力装置（入出力インターフェース）3 1 1、記憶装置（記憶手段）3 1 2、演算装置（演算手段）3 1 3、を有する。
- [0078] 入出力装置 3 1 1 は、k-匿名化データを含む k-匿名化データ、t b を受信し、また後述するデータ受け入れ否通知、分析データをデータ提供事業者装置 1 2 側に送信する機能を有する。
- [0079] 記憶装置 3 1 2 は、データ提供事業者管理マスタ D B 3 1 2 1、k-匿名化データ管理 D B 3 1 2 2、粒度定義書管理マスタ D B 3 1 2 3、分析データ登録 D B 3 1 2 4（図 3 参照）、を有する。
- [0080] データ提供事業者管理マスタ D B 3 1 2 1 は、データ提供事業者マスタテーブル（図示せず）を有する。データ提供事業者マスタテーブルは、サービ

ス提供事業者装置 2 に関連するプロフィールの各情報、例えばサービス提供事業者名（A、B・・・）、メールアドレス、住所などの情報を記憶管理するテーブルスキームを構成する。

[0081] k-匿名化データ管理 DB 3 1 2 2 は、k-匿名化データ管理テーブル T 2 を有する。k-匿名化データ管理テーブル T 2（図 9 参照）については後述する。

[0082] 粒度定義書管理マスタ DB 3 1 2 3 は、複数の粒度定義書 1. CSV、粒度定義書 2. CSV、粒度定義書 3. CSV を有する。粒度定義書. CSV（図 5 参照）については後述する。

[0083] 演算装置 3 1 3 は、CPU などの制御手段 3 1 3 1 を有する。制御手段 3 1 3 1 は、データ提供事業者認識部 3 1 3 1 1、k-匿名化データ評価部 3 1 3 1 2、データ登録部 3 1 3 1 3、データ分析部 3 1 3 1 4、を有する。

[0084] データ提供事業者認識部 3 1 3 1 1 は、データ提供事業者装置 1 2 1 からの k-匿名化データの提供者を、提供者 ID をもって認識する。

[0085] k-匿名化データ評価部 3 1 3 1 2 は、データ提供事業者装置 1 2 1 からの k-匿名化データを受け入れるか否かを評価する。その評価は、データの粒度および k の値をもって実施する。

[0086] データ登録部 3 1 3 1 3 は、k-匿名化データ評価部 3 1 3 1 2 により、受け入れ可と評価したデータを k-匿名化データ融合管理マスタ DB 3 1 2 2 に登録する。

[0087] データ分析部 3 1 3 1 4 は、受け入れた複数のデータを分析し、当該分析データをデータ提供事業者事業者用サーバ側からの要求に応じて提供する。

[0088] また、制御手段 3 1 3 1 は、図 3 に示す如く、タイムスタンプ部 3 1 3 1 5、報奨金情報付与部 3 1 3 1 6、データ分析部 3 1 3 1 4、分析データ配信部 3 1 3 1 7、データ受入否通知およびデータ廃棄機能を有するデータ受入可否結果通知部&データ廃棄部 3 1 3 1 8、を有する。

[0089] タイムスタンプ部 3 1 3 1 5 は、受け入れたデータにタイムタイムスタンプを付与する。報奨金情報付与部 3 1 3 1 6 は、受け入れたデータで報奨金

対象である旨を示す情報を付与する。

- [0090] 分析データ配信部 3 1 3 1 7 は、データ分析部 3 1 3 1 4 による分析結果をデータ提供事業者サーバ 1 2 1 側に配信する。
- [0091] データ受入可否結果通知部 & データ廃棄部 3 1 3 1 8 は、k-匿名化データ評価部 3 1 3 1 2 による評価結果のデータ受入可否をデータ提供者装置 1 2 1 側に通知する。ここで、k-匿名化データ受け入れ否と評価した場合には、その旨をデータ提供事業者事業者サーバ 1 2 1 側に通知すると共に当該評価対象データを廃棄する。
- [0092] データ提供事業者事業者用サーバ 1 2 1 は、粒度定義書、CSV 要求部 1 2 1 1、粒度定義書、CSV 受信部 1 2 1 2、提供元データ登録 DB 1 2 1 3、k-匿名化データ作成部 1 2 1 4、k-匿名化データ送信部 1 2 1 5、データ受入否通知および分析データ受信部 1 2 1 6、を有する。
- [0093] 粒度定義書、CSV 要求部 1 2 1 1 は、提供元のデータ、つまりオリジナルユーザ情報を第三者に対して、提供しようとする場合、サービス基盤事業者用サーバ 3 1 に対して、粒度定義書、CSV の要求を行う。
- [0094] 粒度定義書、CSV 受信部 1 2 1 2 は、サービス基盤事業者用サーバ 3 1 からの粒度定義書、CSV（粒度定義書 1、CSV、粒度定義書 2、CSV、粒度定義書 3、CSV）を受信する。この粒度定義書、CSV は、ネット上に公開しておき、データを提供する側に適した粒度定義書、CSV をダウンロードするようにしてもよい。
- [0095] k-匿名化データ作成部 1 2 1 4 は、粒度定義書、CSV に基づいて、提供元データ登録 DB 1 2 1 3 の元データ（オリジナルユーザ情報）を入力し、k-匿名化データを作成する。
- [0096] k-匿名化データ送信部 1 2 1 5 は、k-匿名化データ作成部 1 2 1 4 により作成された k-匿名化データ（年代、地域など）をサービス基盤事業者サーバ 3 1 側に送信する。このとき、データ提供事業者を示す提供者 ID（G、A、Y など）、定義書 No（1、2、3）を別ファイルで送信する。
- [0097] データ受入否通知および分析データ受信部 1 2 1 6 は、データ受入拒否さ

れたとき、サービス基盤事業者サーバ31からの通知を受け、また分析データを受信する

[0098] 図4は、粒度定義管理マスタDB3123のテーブルT1の内容を示す図である。同図において、テーブルT1は、定義書No(1、2、3)と定義書名(定義書1. CSV、定義書2. CSV、定義書3. CSV)の情報を含んでいる。

[0099] 図5は、定義書1. CSV、定義書2. CSV、定義書3. CSVの各一例を示す図である。同図において、定義書1. CSVは、「k, 年代(幅), 年代(始まり), 居住地域, 勤務地地域, 1日, 週(始まり), 1年(始まり)」等の定義項目を有する。

[0100] そして、定義書1. CSVは、「k, 年代(幅), 年代(始まり), 居住地域, 勤務地地域, 1日, 週(始まり), 1年(始まり)」が、「2, 3才, 0才, 市区町村, 都道府県, 5時-29時, 月曜日, 1月1日」の例をしている。

定義書2. CSVは、「k, 年代(幅), 年代(始まり), 居住地域, 勤務地地域, 1日, 週(始まり), 1年(始まり)」が、「2, 5才, 0才, 市区町村, 都道府県, 5時-24時, 月曜日, 1月1日」であり、定義書3. CSVは、「k, 年代(幅), 年代(始まり), 居住地域, 勤務地地域, 1日, 週(始まり), 1年(始まり)」が、「5, 3才, 0才, 市区町村, 都道府県, 5時-29時, 月曜日, 1月1日」の例を示している。

また、定義書n. CSVは、「k, 年代(幅), 年代(始まり), 居住地域, 勤務地地域, 1日, 週(始まり), 1年(始まり)」が、「5, 10才, 0才, 市区町村, 都道府県, 0時-24時, 日曜日, 第1週目の日曜日」の例を示している。

[0101] 図6は、k-匿名化データ. tbのデータ構成を示す図である。同図において、データとして、年代、居住地域、その他が含まれる。年代、居住地域は、準識別子であるので、これらはデータ提供事業者側にて、サービス基盤事業者側から送信される粒度定義書. CSVに従って、k-匿名化する。

- [0102] 図7は、図6の一具体例を示すものであって、 k -匿名化データ、 t_b のテーブル名：G0001、 t_b 、 $k=2$ の例を示す図である。同図において、テーブルT3は、準識別子として、年代、居住地域の2項目のデータを含んでいる。また、その他として、支払方法、金額のデータを含んでいる。
- [0103] ここで、「年代：30-34 居住地域：東京都品川区」、「年代：35-39 居住地域：東京都港区」、「年代：20-24 居住地域：東京都港区」、「年代：25-29 居住地域：東京都品川区」は、それぞれ $k=2$ を満たすので、これらのデータは受入れ可と評価する。しかし、「年代：30-34 居住地域：東京都港区」、「年代：60-64 居住地域：東京都品川区」は、 $k=1$ なので、これらのデータは受入れ否と評価する。
- [0104] 図8は、テーブル名：G0001、 t_b 、 $k=2$ に対して、 k -匿名化データ評価部31312により、評価した後、受入れデータのみを含むテーブルT3'の例を示す図である。
- [0105] 図9は、 k -匿名化データ管理マスタDB3122のテーブルT2の内容を示す図である。同図において、テーブルT2は、テーブル名（G0001、 t_b 、G0002、 t_b 、A0001、 t_b 、G0003、 t_b 、Y0001、 t_b 、G0004、 t_b ）、データ提供事業者ID（G、G、A、G、Y、G）、時刻（タイムスタンプ）、報奨金、レコード数、項目数（ k -匿名化処理した準識別子；年代、地域の項目数）、粒度定義書No（1、1、2、2、3、3）などの情報を含んでいる。
- [0106] 図10は、サービス基盤事業者用サーバとデータ提供事業者用サーバの各処理手順を示すフローチャートである。
- [0107] データ提供事業者用サーバ121は、ステップS121にて、サービス基盤事業者用サーバ31に粒度定義書要求する。
- [0108] サービス基盤事業者用サーバ31は、ステップS311にて、前記粒度定義書要求を受信する。次いで、ステップS312にて、当該粒度定義書要求に応じた粒度定義書、CSV（例えば、粒度定義書1、CSV）を粒度定義書管理マスタDB3123から抽出し、データ提供事業者用サーバ121に

送信する。

[0109] データ提供事業者用サーバ121は、ステップS122にて、粒度定義書1．CSVを受信する。

[0110] 次に、ステップS123にて、粒度定義書1．CSVに基づき作成されるk-匿名化データをサービス基盤事業者用サーバ31に送信する。

[0111] サービス基盤事業者用サーバ31は、ステップS313にて、k-匿名化データを受信する。このとき、k-匿名化データその他、当該データの提供者を特定するデータ提供者ID（図9参照）、定義書No（図4参照）も受信する。これらは、データ提供事業者用サーバ121から送信するものであるが、k-匿名化データと、データ提供者ID、定義書Noは、別ファイルで送信する。

[0112] 次に、ステップS314にて、k-匿名化データを評価する。このデータ評価は、k-匿名化データの粒度およびkの値を元に実行する。

[0113] 例えば、サービス基盤事業者用サーバ121側にてkの値が2と定義している場合、kの値が2以上の場合は、データ受入可と評価し、2以下の場合には、K-匿名化データであっても、間接的に個人情報が特定される可能性が高いと判断し、データ受入否と評価する。このkの値は、2以上の複数に設定する。また、このkの値は、データを提供する提供者側により、設定してもよい。

[0114] ステップS315にて、データ受入可否の結果は、ステップS322にて、データ提供事業者側サーバ121に通知する。

ステップS315にて、データ受入否とした場合には、その旨の通知と共に、このときの評価対象データをステップS321に廃棄処理する。

データ提供事業者用サーバ121では、ステップS126にて、その通知を受け、この通知により、受け入れ可否を把握することができる。

[0115] データ受入可とした場合には、ステップS316にて、当該データの受け入れ日を示すタイムスタンプを受け入れデータに付与する。また、ステップS317にて、当該受け入れデータの価値を示す報奨金情報を付与する。こ

これらのステップは、必要に応じて行う。

[0116] 次に、ステップS 3 1 8にて、受け入れたデータをK-匿名化データ登録DB 3 1 2 2に登録する。

[0117] ステップS 3 1 9にて、例えば、データ提供事業者側からの依頼に基づき、当該依頼に適したK-匿名化データ（1以上）をk-匿名化データDB 3 1 2 2から抽出し、当該抽出データのデータ分析を行う。

[0118] この分析データは、ステップS 3 2 0にて、データ提供事業者用サーバ1 2 1に送信する。そして、この送信は、例えば、データ提供者用サーバ1 2 1側でのステップS 1 2 4におけるk-匿名化データ要求に基づいて実行される。データ提供事業者用サーバ1 2 1は、ステップS 1 2 5にて、分析K-匿名化データを受信する。

[0119] 上述した実施例の如く、データ評価、分析のシステム化により、粒度定義書に合っており、かつデータ評価基準を充足していれば、その提供データに対して報奨金（値段）情報を付けて支払うような仕組みを容易に実現できる。

[0120] また、分析のシステム化により、粒度定義書に合っていれば、その提供データに対して報奨金（値段）を付けて支払うような仕組みを容易に実現できる。

[0121] 上述した実施例では、k-匿名化データを受信し、次いで当該データを評価し、受入れデータのみをk-匿名化データ管理マスタ3 1 2 2に登録するステップとしているが、k-匿名化データを一旦k-匿名化データ管理マスタ3 1 2 2に登録した後、分析データとして受入れ可能か否かを評価し、当該データの中から受入れ可のデータのみを分析対象のデータとするステップとしてもよい。

[0122] なお、本発明は上述した実施例に限定されるものではなく、様々な変形例が含まれる。例えば、上述した実施例は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施例の構成の一部を他の実施例の構

成に置き換えることが可能であり、また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

[0123] また、上記の各構成、機能、処理部、処理手段等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリや、ハードディスク、SSD (Solid State Drive) 等の記録装置、又は、ICカード、SDカード、DVD等の記録媒体に置くことができる。

[0124] また、制御線や情報線は説明上必要と考えられるものを示しており、製品上必ずしも全ての制御線や情報線を示しているとは限らない。実際には殆ど全ての構成が相互に接続されていると考えてもよい。

符号の説明

- [0125] 1 サービス享受事業者装置
2 サービス提供事業者装置
2 1 サービス提供事業者用サーバ
3 サービス基盤事業者装置
3 1 サービス基盤事業者用サーバ
1 2 1 データ提供事業者用サーバ
1 2 1 1 粒度定義書要求部
1 2 1 2 粒度定義書受信部
1 2 1 3 提供元データ登録部
1 2 1 4 k-匿名化データ作成部
1 2 1 5 k-匿名化データ送信部
3 1 1 入出力装置
3 1 2 記憶装置

3 1 3 演算装置

3 1 3 1 制御手段

3 1 2 1 データ提供事業者管理マスタDB

3 1 2 2 k-匿名化融合管理マスタDB

3 1 2 3 粒度定義書管理マスタDB

3 1 2 4 分析データ登録DB

請求の範囲

[請求項1]

データ提供事業者装置と、サービス基盤事業者装置と、を有し、
前記サービス基盤事業者装置は、
前記データ提供事業者装置に対して、データの粒度を定義する粒度定義書、CSVを配信する手段と、
前記データ提供事業者装置側にて前記粒度定義書、CSVに基づき作成されるk-匿名化データを含むk-匿名化データ、tbを受ける手段と、
前記k-匿名化データ、tbのk-匿名化データの粒度およびkの値をもって、前記k-匿名化データを受け入れるか否かを評価する手段と、
を有し、
前記k-匿名化データから、個人情報漏洩リスクを防止し、かつ複数のk-匿名化データの融合、分析精度を向上することを可能とする匿名化データの粒度管理装置。

[請求項2]

請求項1に記載された匿名化データの粒度管理装置であって、
前記k-匿名化データ、tbを受ける手段は、前記k-匿名化データ、tbの前記粒度定義書、CSVで定義されているk-匿名化処理された前記k-匿名化データを受けるとき、前記データ提供事業者装置から当該データの提供者を特定するID、定義書Noを受けることを特徴とする匿名化データの粒度管理装置。

[請求項3]

請求項1に記載の匿名化データの粒度管理装置であって、
前記サービス基盤事業者装置は、
さらに、前記データ評価手段により、受入れ可能と判断した場合、当該データにタイムスタンプおよび報奨金情報を付与する手段と、
前記データ受入れ否と判断した場合、その旨を前記データ提供事業者装置側に通知する手段、
を有する、

ことを特徴とする匿名化データの粒度管理装置。

[請求項4]

請求項1に記載の匿名化データの粒度管理装置であって、

前記サービス基盤事業者装置は、

前記データ評価手段による評価結果、データ受入可とした場合、前記記憶手段に登録する手段、

前記受入れたデータを分析するデータ分析手段、

を有し、

前記サービス基盤事業者装置側にて、前記データ提供事業者装置から受入れ可能な複数のデータを分析対象データとして融合し、当該融合データを前記データ分析手段により、分析した分析データとし前記データ提供装置側に配信送付可能とする

ことを特徴とする匿名化データの粒度管理装置。

[請求項5]

請求項1～請求項4の何れか1項に記載の匿名化データの粒度管理装置であって、

前記粒度定義書．CSVは、データ粒度定義が1種類、又は異なる複数の種類からなり、前記粒度定義書．CSVに基づき作成される前記k-匿名化データ．tbは1種類、又は2種類以上の複数のデータの集まりである

ことを特徴とする匿名化データの粒度管理装置。

[請求項6]

データ提供事業者装置と、サービス基盤事業者装置と、を有し、

前記サービス基盤事業者装置側において、前記データ提供事業者装置側から送られてくる匿名化データの粒度を管理する方法であって、

前記データ提供事業者装置に対して、データの粒度を定義する粒度定義書．CSVを配信するステップと、

前記データ提供事業者装置側にて前記粒度定義書．CSVに基づき作成されるk-匿名化データを含むk-匿名化データ．tbを受けるステップと、

前記k-匿名化データ．tbのk-匿名化データの粒度およびkの

値をもって、前記 k - 匿名化データを受け入れるか否かを評価するステップと、

を有し、

前記 k - 匿名化データから、個人情報漏洩リスクを防止し、かつ複数の k - 匿名化データの融合、分析精度を向上することを可能とする匿名化データの粒度管理方法。

[請求項7]

請求項6に記載の匿名化データの粒度管理方法であって、

さらに、前記データ評価手段により、受入れ可能と判断した場合、当該データにタイムスタンプおよび報奨金情報を付与するステップと、

前記データ受入れ否と判断した場合、その旨を前記データ提供事業者装置側に通知するステップ、

を有する、

ことを特徴とする匿名化データの粒度管理方法。

[請求項8]

請求項6に記載の匿名化データの粒度管理方法であって、

前記データ評価手段による評価結果、データ受入可とした場合、前記記憶手段に登録するステップと、

前記受入れたデータを分析するステップと、

を有し、

前記サービス基盤事業者装置側にて、前記データ提供事業者装置から受入れ可能な複数のデータを分析対象データとして融合し、当該融合データを前記データ分析手段により、分析した分析データとし前記データ提供装置側に配信送付可能とする

ことを特徴とする匿名化データの粒度管理方法。