(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7599387号
(P7599387)

(45)発行日　令和6年12月13日(2024.12.13)

(24)登録日　令和6年12月5日(2024.12.5)

(51)国際特許分類
Ｇ０６Ｑ　50/10　(2012.01)

ＦＩ
Ｇ０６Ｑ　50/10

請求項の数　9　（全20頁）

(21)出願番号　特願2021-124775(P2021-124775)
(22)出願日　令和3年7月29日(2021.7.29)
(65)公開番号　特開2023-19795(P2023-19795A)
(43)公開日　令和5年2月9日(2023.2.9)
審査請求日　令和6年2月8日(2024.2.8)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110001689
青稜弁理士法人
(72)発明者　木谷 光博
東京都千代田区丸の内一丁目６番６号
株式会社日立製作所内
(72)発明者　シャフリル バンダラ
東京都千代田区丸の内一丁目６番６号
株式会社日立製作所内
審査官　田川 泰宏

最終頁に続く

(54)【発明の名称】　データ流通仲介装置およびデータ流通仲介方法

(57)【特許請求の範囲】

【請求項１】

データ所有者の提供するパーソナルデータを収集して提供するデータ提供者のデータ提供装置と、前記パーソナルデータに関連するサービス利用データを提供するサービス事業者のデータ利用装置との間に介在してデータのやりとりを仲介するデータ流通仲介装置であって、

前記データ提供装置の保持する前記パーソナルデータのメタデータであるパーソナルデータメタデータを取得するパーソナルデータメタデータ管理部と、

前記パーソナルデータの流通利用に関する利用規約に基づいて、前記サービス利用データに関するメタデータであるサービス利用データメタデータを生成するサービス利用データ属性管理部と、

前記パーソナルデータメタデータと、前記サービス利用データメタデータの差異を検出するメタデータ属性差異検出部と、

前記メタデータ属性差異検出部で検出されたメタデータの差異から前記パーソナルデータの内容の変換処理要否を判定するパーソナルデータ変換判定部と、

前記パーソナルデータの内容を対応するサービス利用データの内容に変換するパーソナルデータ変換処理部とを備え、

前記パーソナルデータ変換判定部により、前記パーソナルデータの内容の変換要否を判定し、前記パーソナルデータの内容が変換要と判定されたときに、前記パーソナルデータ変換処理部は、前記サービス利用データメタデータに基づいて、前記パーソナルデータの

内容を前記サービス利用データの内容に変換することを特徴とするデータ流通仲介装置。
【請求項２】
前記パーソナルデータの流通利用に関する利用規約は、前記データ提供装置と前記データ利用装置との間での相互通信によって取得され、
前記相互通信は、
サービスＩＤを含み、データ所有者端末により前記データ流通仲介装置に送信されるサービス利用要求メッセージと、
サービスＩＤを含み、前記データ流通仲介装置により前記データ利用装置に送信されるサービス利用規約要求メッセージと、
前記サービスＩＤに対応するサービス利用規約を含み、前記データ利用装置により前記データ流通仲介装置に送信されるサービス利用規約レスポンスとを含み、
前記利用規約は、前記サービスＩＤに対応するサービスを提供するサービス事業者によって定められることを特徴とする請求項１記載のデータ流通仲介装置。
【請求項３】
前記パーソナルデータ変換処理部は、前記サービス利用データメタデータに定義されたデータ項目ごとに定義された属性に合うように、前記パーソナルデータの内容を前記サービス利用データの内容に値を変換することを特徴とする請求項１記載のデータ流通仲介装置。
【請求項４】
前記パーソナルデータ変換判定部は、前記データ利用装置の提供するサービスのシナリオに基づいて、前記パーソナルデータの内容の変換要否を判定することを特徴とする請求項１記載のデータ流通仲介装置。
【請求項５】
前記パーソナルデータ変換判定部は、前記データ利用装置の提供するサービスのシナリオに基づいて、変換する内容を異ならしめることを特徴とする請求項４記載のデータ流通仲介装置。
【請求項６】
プライバシーランクデータを保持し、前記プライバシーランクデータに規定されたプライバシーランクに基づいた前記パーソナルデータの流通利用に関する利用規約に関する情報を保持することを特徴とする請求項１記載のデータ流通仲介装置。
【請求項７】
前記パーソナルデータの流通利用に関する利用規約を同意したか否かの情報を外部から受信し、
前記データ利用装置からサービス利用データ要求メッセージの受信後に、
前記パーソナルデータ変換判定部により、前記パーソナルデータの内容の変換要否を判定し、前記パーソナルデータの内容が変換要と判定されたときに、前記パーソナルデータ変換処理部は、前記サービス利用データメタデータに基づいて、前記パーソナルデータの内容を前記サービス利用データの内容に変換し、
前記データ利用装置に、前記サービス利用データを送信することを特徴とする請求項１記載のデータ流通仲介装置。
【請求項８】
データ提供装置が保持するデータカタログに基づく前記パーソナルデータメタデータを取得することを特徴とする請求項１記載のデータ流通仲介装置。
【請求項９】
データ所有者の提供するパーソナルデータを収集して提供するデータ提供者のデータ提供装置と、前記パーソナルデータに関連するサービス利用データを提供するサービス事業者のデータ利用装置との間に介在してデータのやりとりを仲介するデータ流通仲介装置が行うデータ流通仲介方法であって、
前記データ流通仲介装置が、前記データ提供装置の保持する前記パーソナルデータのメタデータであるパーソナルデータメタデータを取得するステップと、

前記データ流通仲介装置が、前記データ所有者と、前記データ提供者または前記サービス事業者との間により締結された契約に基づく前記パーソナルデータの流通利用に関する利用規約に基づいて、前記サービス利用データに関するメタデータであるサービス利用データメタデータを生成するステップと、
前記データ流通仲介装置が、前記パーソナルデータメタデータと、前記サービス利用データメタデータの差異を検出するステップと、
前記データ流通仲介装置が、前記パーソナルデータメタデータと、前記サービス利用データメタデータの差異を検出するステップにより検出されたメタデータの差異から前記パーソナルデータの内容の変換処理要否を判定するステップと、
前記パーソナルデータの内容の変換処理要否を判定するステップにより、変化要と判定されたときに、前記データ流通仲介装置が、前記サービス利用データメタデータに基づいて、前記パーソナルデータの内容を前記サービス利用データの内容に変換するステップとを有し、
前記パーソナルデータの流通利用に関する利用規約は、前記データ提供装置と前記データ利用装置との間での相互通信によって取得され、
前記相互通信は、
サービスＩＤを含み、データ所有者端末により前記データ流通仲介装置に送信されるサービス利用要求メッセージと、
サービスＩＤを含み、前記データ流通仲介装置により前記データ利用装置に送信されるサービス利用規約要求メッセージと、
前記サービスＩＤに対応するサービス利用規約を含み、前記データ利用装置により前記データ流通仲介装置に送信されるサービス利用規約レスポンスとを含み、
前記利用規約は、前記サービスＩＤに対応するサービスを提供するサービス事業者によって定められ、
前記パーソナルデータの内容を前記サービス利用データの内容に変換するステップにおいて、前記サービス利用データメタデータに定義されたデータ項目ごとに定義された属性に合うように、前記パーソナルデータの内容を前記サービス利用データの内容に変換することを特徴とするデータ流通仲介方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、データ流通仲介装置およびデータ流通仲介方法に係り、特に、パーソナルデータに基づいたサービスを行うサービス事業者とユーザとの規約に基づいてデータの利用を可能にし、パーソナルデータの利用促進とパーソナルデータに関するプライバシー保護を両立する用途に用いて好適なデータ流通仲介装置およびデータ流通仲介方法に関する。

【背景技術】

【０００２】

近年、各企業において法人・個人向けサービス提供のため、収集されたパーソナルデータを含む様々なデータを、各企業や産業間を跨いで流通、利活用するための論議や検討が活発化している。特に、パーソナルデータについては、プライバシー保護に関する法律であるＥＵのＧＤＰＲ（General Data Protection Regulation：一般データ保護規則）に代表されるように、データの主権者であるユーザ個人が自らのデータをコントロールすることの重要性とそのための仕組みが検討されている。その際、ユーザ個人で全てのデータをコントロールするのは難しいため、データ利用者である企業と、データの主権者である個人とは異なる独立した機関として、情報銀行やＰＤ（Personal Data Store）といったデータ流通の仲介役となるシステム（データ流通仲介システム）を設置し、データ流通とそのためのデータや手続きの管理をサポートするモデルが注目されている。その際、データ提供者にて収集され保有しているデータと、新たなサービスをユーザへ提供するサービス事業者が取り扱うデータの間で、それらの内容に差異がある場合があり、データ流通を実現する上で解くべき課題の一つとなっている。

【０００３】
データ流通仲介システムを用いたデータ流通に関する先行技術として、例えば、特許文献１がある。特許文献１では、データ主権者である個人、データ仲介者、データ提供者に対してインセンティブを付与する仕組みを導入し、データ流通を活性化するデータ流通制御に関するシステムが開示されている。また、この特許文献１では、データ流通の際、データ提供者において、予め定めたデータ形式へデータを変換して、データ流通仲介システムへ送信することが記載されている（段落[００６６]、[０１２８]）。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２０２０－１２９３１１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
上記特許文献１に記載されたデータ流通制御に関するシステムでは、データ提供企業のサーバが、提供依頼に提供条件のフォーマットに指定があるときには、指定されたフォーマットに変換することが述べられている。この特許文献１では、データ提供者におけるデータ形式変換についてのみ述べられており、データの内容そのものの変換方法については、具体的に言及されていない。ここでデータ形式とはＣＳＶ（Comma Separated Value）やＸＭＬ（eXtensible Markup Language）などのデータフォーマットのことを指し、データフォーマットを変換してもデータの内容そのものは変わらない。また、上記特許文献１では、サービス事業者から提供されるサービス内容と、データ提供者で保有するデータ仕様に合わせて動的に変わるデータ内容の変換処理や、変換処理のための変換要否の判定方法については明記されていない。
【０００６】
したがって、データ提供者がユーザ（パーソナルデータの所有者）との同意規約に基づいたデータの提供や、状況の変化に応じて、データを加工して提供することについては考慮されていない。例えば、通常時は、ユーザプライバシーの保護を厳密にし、緊急時には、プライバシー保護をゆるくして、データ利用することにより安全性を高めたり、公的なデータ利用が求められるときがある。
【０００７】
本発明の目的は、パーソナルデータに基づいたサービスを行うサービス事業者とユーザとの規約に基づいてデータの利用を可能にし、パーソナルデータの利用促進とパーソナルデータに関するプライバシー保護を両立することのできるデータ流通仲介システムを提供することにある。
【課題を解決するための手段】
【０００８】
本発明のデータ流通仲介装置の構成は、好ましくは、データ所有者の提供するパーソナルデータを収集して提供するデータ提供者のデータ提供装置と、パーソナルデータに関連するサービス利用データを提供するサービス事業者のデータ利用装置との間に介在してデータのやりとりを仲介するデータ流通仲介装置であって、データ提供装置の保持するパーソナルデータのメタデータであるパーソナルデータメタデータを取得するパーソナルデータメタデータ管理部と、パーソナルデータの流通利用に関する利用規約に基づいて、サービス利用データに関するメタデータであるサービス利用データメタデータを生成するサービス利用データ属性管理部と、パーソナルデータメタデータと、サービス利用データメタデータの差異を検出するメタデータ属性差異検出部と、メタデータ属性差異検出部で検出されたメタデータの差異からパーソナルデータの変換処理要否を判定するパーソナルデータ変換判定部と、パーソナルデータを対応するサービス利用データの変換するパーソナルデータ変換処理部とを備え、パーソナルデータ変換判定部により、パーソナルデータの変換要否を判定し、パーソナルデータが変換要と判定されたときに、パーソナルデータ変換

処理部は、サービス利用データメタデータに基づいて、パーソナルデータをサービス利用データに変換するようにしたものである。

【発明の効果】

【０００９】

本発明によれば、パーソナルデータに基づいたサービスを行うサービス事業者とユーザとの規約に基づいてデータの利用を可能にし、パーソナルデータの利用促進とパーソナルデータに関するプライバシー保護を両立することのできるデータ流通仲介システムを提供することができる。

【図面の簡単な説明】

【００１０】

【図１】データ流通仲介システムの概要構成図である。

【図２】実施形態１に係るデータ流通仲介装置の機能構成図である。

【図３】データ流通仲介装置のハードウェア・ソフトウェア構成図である。

【図４】データ提供装置がデータ流通仲介装置に提供するパーソナルデータの一例を示す図である。

【図５】データ流通仲介装置がデータ利用装置に提供するサービス利用データの一例を示す図である。

【図６】実施形態１に係る利用規約テーブルの一例を示す図である。

【図７】パーソナルデータメタデータの一例を示す図である。

【図８】サービス利用データメタデータの一例を示す図である。

【図９】データ流通制御データの一例を示す図である。

【図１０】実施形態１に係るスクリプト管理テーブルの一例を示す図である。

【図１１Ａ】データ流通仲介システムの処理を説明するシーケンスチャートである（その一）。

【図１１Ｂ】データ流通仲介システムの処理を説明するシーケンスチャートである（その二）。

【図１２】実施形態２に係るデータ流通仲介装置の機能構成図である。

【図１３】プライバシーランクデータの一例を示す図である。

【図１４】実施形態２に係る利用規約テーブルの一例を示す図である。

【図１５】実施形態２に係るスクリプト管理テーブルの一例を示す図である。

【発明を実施するための形態】

【００１１】

以下、本発明に係る各実施形態を、図１ないし図１５を用いて説明する。

【００１２】

〔実施形態１〕

以下、本発明に係る実施形態１を、図１ないし図１１Ｂを用いて説明する。

先ず、図１ないし図３を用いて本発明の実施形態１に係るデータ流通仲介システムの構成について説明する。

【００１３】

先ず、図１を用いてデータ流通仲介システムの概要構成について説明する。

データ流通仲介システムは、図１に示されるように、データ流通仲介装置１００、データ提供装置２００（図１では、データ提供装置２００ａ，２００ｂ，…，２００ｍと表記）、データ利用装置３００（図１では、データ利用装置３００ａ，３００ｂ，…，３００ｎと表記）、データ所有者端末１０（図１では、所有者端末１ａ，１０ｂ，…，１０ｌと表記）がネットワーク５により接続された形態である。ネットワーク５は、有線でも無線でもよく、インターネットのようなグローバルなネットワークでもよいし、ＬＡＮ（Local Area Network）でもよい。また、データ流通仲介装置１００、データ提供装置２００、データ利用装置３００、データ所有者端末１０のそれぞれが個別に接続されたネットワーク形態であってもよい。

【００１４】

データ流通仲介装置１００は、データ提供装置２００とデータ利用装置３００間におけるデータ流通を仲介して、必要なデータの変換や取捨選択を行う装置である。データ提供装置２００は、データ所有者のデータ（パーソナルデータ、詳細は後述）をデータ利用装置３００に提供する装置である。データ利用装置３００は、データ提供装置２００からサービス利用データ（詳細は後述）を受取ってサービスに利用する装置である。データ所有者端末１０は、データ所有者がデータに関する設定、データ提供者やデータ利用者とのデータ利用に関する規約の同意、パーソナルデータをデータ提供装置２００にアップロードする装置である。パーソナルデータは、データ所有者端末１０からアップロードするだけではなく、別の経路によってデータ提供装置２００に提供されることにしてもよい。

【００１５】

本実施形態の説明では、主に、自動車道路における緊急通報サービスシステムを例にして説明することにする。緊急通報サービスとは、自動車道路における自動車事故が発生した場合、緊急通報事業者が車両データから状況を把握し、状況に応じて救急車等を要請するサービスである。この場合には、データ所有者は、自動車のドライバーであり、パーソナルデータとしては、事故被害状況データ、自動車のドライバーの個人医療データ(血液型、アレルギー、既往歴)である。パーソナルデータが事故被害状況である場合には、データ提供者は、自動車メーカーとなり、データ利用者は、警察、保険会社、病院、ＪＡＦなどのロードサービス事業者となり、パーソナルデータが個人医療データである場合には、データ提供者は、ドライバーの係り付け病院となり、データ利用者は、保険会社、事故時の搬送病院である。

【００１６】

また、データ所有者端末１０は、専用のハードウェアにより実現されるものであってもよく、または、ＣＰＵ（Central Processing Unit：中央演算処理処置）およびメモリ等により構成され、各部の機能を実現するためのコンピュータプログラムをＣＰＵが実行することによりその機能を実現させるものであってもよい。例えば、データ所有者端末１０は、スマートフォンや自動車のカーナビゲーションシステム、車両に組み込まれてドライブ情報を収集するスマートデバイス等の移動通信端末装置であってもよく、または、据置き型の通信端末(例えば、パーソナルコンピュータ)であってもよい。

【００１７】

次に、図２を用いてデータ流通仲介装置の機能構成について説明する。

データ流通仲介装置１００は、図２に示されるように、データ提供者管理部１０１、サービス事業者管理部１０２、パーソナルデータ変換部１１０、利用規約管理部１２１、同意手続管理部１２２、データ流通制御部１３０、通信部１４０、記憶部１５０から構成される。

【００１８】

データ提供者管理部１０１は、データ提供装置２００によりデータを提供するデータ提供者の情報、データ提供装置２００により提供されたパーソナルデータの情報を管理する機能部である。

【００１９】

サービス事業者管理部１０２は、データ所有者端末１０を通じてユーザが利用しているサービスに関する様々な情報、すなわち、サービスの内容、サービスを提供する事業者の情報、サービスの利用状況などを管理する機能部である。

【００２０】

パーソナルデータ変換部１１０は、データ提供装置２００で収集、蓄積されるユーザのパーソナルデータをデータ利用装置３００へ流通制御する際に、ユーザのパーソナルデータの内容を変換する必要があるか否かを判定して、必要な場合に変換処理する機能部である。

【００２１】

パーソナルデータ変換部１１０は、パーソナルデータメタデータ管理部１１１、サービス利用データメタデータ管理部１１２、メタデータ属性差異検出部１１３、シナリオ毎サ

ービス利用データメタデータ特定部１１４、パーソナルデータ変換判定部１１５、パーソナルデータ変換処理部１１６のサブ機能部から構成される。

【００２２】

パーソナルデータメタデータ管理部１１１は、データ提供装置２００で収集、蓄積されるユーザのパーソナルデータのメタデータ（以下、単に「パーソナルデータメタデータ」という、詳細は後述）を、データ提供装置２００から取得し管理する機能部である。

【００２３】

サービス利用データメタデータ管理部１１２は、サービスで利用されるユーザのパーソナルデータに関するメタデータ（以下、単に「サービス利用データメタデータ」という、詳細は後述）を管理する機能である。

【００２４】

サービス利用データメタデータは、利用規約管理部１２１で管理されるユーザのパーソナルデータの収集、蓄積、利用用途を含むサービス規約情報と、同意手続管理部１２２で管理されるユーザの同意結果に基づき生成されるメタデータである。サービス利用データメタデータ管理部１１２により、ユーザ毎にカスタマイズされたサービス（サービスで利用するデータがユーザ毎に異なる）に対応したユーザのパーソナルデータのメタデータを管理することができる。また、サービス利用データメタデータをデータ流通仲介装置１００で生成せずとも、サービス事業者やデータ利用装置３００で生成されたサービスで利用されるユーザのパーソナルデータに関するメタデータを取得し管理するようにしてもよい。また、サービス利用データメタデータは、データ流通仲介装置１００の運用・管理者によって生成されたものでもよい。

【００２５】

メタデータ属性差異検出部１１３は、パーソナルデータメタデータ管理部１１１で管理されるパーソナルデータメタデータと、サービス利用データメタデータ管理部１１２で管理されるサービス利用データメタデータの差異を検出する機能部である。メタデータ属性差異検出部１１３における差異の検出は、パーソナルデータメタデータとサービス利用データメタデータにおけるメタデータの特定の属性（メタデータ属性）について行い、そのメタデータ属性の設定値の差分から検出することにより行われる。

【００２６】

シナリオ毎サービス利用データメタデータ特定部１１４は、サービス事業者で提供されるサービスのシナリオ（詳細は、後述）毎に利用されるサービス利用データメタデータを特定する機能部である。

【００２７】

パーソナルデータ変換判定部１１５は、メタデータ属性差異検出部１１３で検出されたメタデータ属性の設定値の差分に基づき、データ提供装置２００で取集、蓄積されるユーザのパーソナルデータを変換する必要があるか否かを判定する機能部である。

【００２８】

パーソナルデータ変換処理部１１６は、パーソナルデータ変換判定部１１５によりユーザのパーソナルデータを変換する必要があると判定された場合に、パーソナルデータメタデータ属性の設定と、サービス利用データメタデータ属性の設定に基づき、適切な変換処理を行う機能部である。

【００２９】

利用規約管理部１２１は、ユーザが利用したいデータ利用装置３００が提供するサービスに関して、ユーザとサービス事業者の間に合意するサービスの利用規約を、データ利用装置３００から取得し、不備がないか否かを確認して、ユーザに開示する規約を管理する機能部である。

【００３０】

同意手続管理部１２２は、サービス事業者のサービス利用規約に基づいて、データ所有者端末１０に送信する同意要求通知を生成し、その通知を受け取ったユーザがデータ所有者端末１０で同意するか否かを確定し、ユーザの同意結果を取得して管理する機能部であ

る。
【００３１】
データ流通制御部１３０は、同意手続管理部１２２で管理する、ユーザが同意したサービス利用規約に基づいて、データ提供装置２００で収集、蓄積されるユーザのパーソナルデータを、データ流通制御データ（詳細は後述）に基づいてデータ利用装置３００へ流通するためのデータフローを制御する。
【００３２】
通信部１４０は、ネットワーク５を介して、データ提供装置２００、データ利用装置３００、データ所有者端末１０との通信を行う機能部である。通信部１４０では、例えば、データ利用装置３００からユーザが利用したいサービスのサービス利用規約を受信し、利用規約管理部１２１に転送する。また、利用規約管理部１２１で受信したサービス利用規約をデータ所有者端末１０へ送信し、サービス利用規約の同意を求めるための通信を行い、また、データ所有者端末１０から同意の結果を受信する。
【００３３】
記憶部１５０は、データ提供者管理部１０１、サービス事業者管理部１０２、パーソナルデータ変換部１１０、利用規約管理部１２１、同意手続管理部１２２、データ流通制御部１３０が各部の機能を実現する際に生成したあるいは使用されるデータを記憶する機能部である。
【００３４】
記憶部１５０には、パーソナルデータ４０１、サービス利用データ４０２、パーソナルデータメタデータ４１１、サービス利用データメタデータ４１２、データ提供・データ利用情報データ４２０、利用規約テーブル４２１、同意手続情報データ４２２、データ流通制御データ４３１、スクリプトデータ４４１、スクリプト管理テーブル４４２が保持される。なお、各データの詳細は後に説明する。
【００３５】
次に、図３を用いてデータ流通仲介装置のハードウェア・ソフトウェア構成について説明する。
データ流通仲介装置１００のハードウェア構成としては、例えば、図３に示されるパーソナルコンピュータのような一般的な情報処理装置で実現される。
【００３６】
データ流通仲介装置１００は、ＣＰＵ（Central Processing Unit）５０２、主記憶装置５０４、ネットワークＩ／Ｆ（InterFace）５０６、表示Ｉ／Ｆ５０８、入出力Ｉ／Ｆ５１０、補助記憶Ｉ／Ｆ５１２が、バスにより結合された形態になっている。
【００３７】
ＣＰＵ５０２は、データ流通仲介装置１００の各部を制御し、主記憶装置５０４に必要なプログラムをロードして実行する。
【００３８】
主記憶装置５０４は、通常、ＲＡＭなどの揮発メモリで構成され、ＣＰＵ５０２が実行するプログラム、参照するデータが記憶される。
【００３９】
ネットワークＩ／Ｆ５０６は、ネットワーク５と接続するためのインタフェースである。
【００４０】
表示Ｉ／Ｆ５０８は、ＬＣＤ（Liquid Crystal Display）などの表示装置５２０を接続するためのインタフェースである。
【００４１】
入出力Ｉ／Ｆ５１０は、入出力装置を接続するためのインタフェースである。図５の例では、キーボード５３０とポインティングデバイスのマウス５３２が接続されている。
【００４２】
補助記憶Ｉ／Ｆ５１２は、ＨＤＤ（Hard Disk Drive）５５０やＳＳＤ（Solid State Drive）などの補助記憶装置を接続するためのインタフェースである。

【００４３】
ＨＤＤ５５０は、大容量の記憶容量を有しており、本実施形態を実行するためのプログラムが格納されている。データ流通仲介装置１００には、データ提供者管理プログラム５６１、サービス事業者管理プログラム５６２、パーソナルデータ変換処理プログラム５７０、利用規約管理プログラム５８１、同意手続き管理プログラム５８２、データ流通制御プログラム５９０がインストールされている。
【００４４】
データ提供者管理プログラム５６１、サービス事業者管理プログラム５６２、パーソナルデータ変換処理プログラム５７０、利用規約管理プログラム５８１、同意手続き管理プログラム５８２、データ流通制御プログラム５９０は、それぞれデータ提供者管理部１０１、サービス事業者管理部１０２、パーソナルデータ変換部１１０、利用規約管理部１２１、同意手続管理部１２２、データ流通制御部１３０の機能を実現するプログラムである。
【００４５】
また、図示しなかったが、ＨＤＤ５５０には、パーソナルデータ４０１、サービス利用データ４０２、パーソナルデータメタデータ４１１、サービス利用データメタデータ４１２、利用規約テーブル４２１、同意手続情報データ４２２、データ流通制御データ４３１、スクリプトデータ４４１が格納される。
【００４６】
以上の例では、データ流通仲介装置１００は、情報処理装置が各部の機能を実現するためのコンピュータプログラムをＣＰＵが実行することによりその機能を実現させるとして記述したが、専用のハードウェアにより実現されるものであってもよい。
【００４７】
次に、図４ないし図１０を用いてデータ流通仲介システムで用いられるデータの詳細について説明する。
【００４８】
パーソナルデータ４０１は、データ提供装置２００がデータ所有者の個人的なデータを収集して、データ流通仲介装置１００に提供されるデータである。図４には、パーソナルデータ４０１の一例として、データ所有者の車両のドライブ情報として、ＪＳＯＮ（Java Script Object Notation）形式で記述した車両走行データが示されており、この図４の例では、車両データタイムスタンプ４０１ａ、車両位置データ（緯度）４０１ｂ、車両位置データ（経度）４０１ｃ、車両走行速度データ４０１ｄ、車両ブレーキ動作情報４０１ｅを含んでいる。
【００４９】
サービス利用データ４０２は、データ流通仲介装置１００が、パーソナルデータ４０１を必要に応じて変換して、データ利用装置３００に提供するデータである。
【００５０】
本実施形態の例では、サービスのシナリオによって異なった変換を施して、データ利用装置３００に提供することを前提としている。
【００５１】
例えば、図５の例では、図５（ａ）にデータ所有者の車両のドライブ時に、事故が発生していない定常時に提供されるデータが示されており、図５（ｂ）にデータ所有者の車両のドライブ時に、事故発生した時の緊急時に提供されるデータが示されている。
【００５２】
図５（ａ）の定常時に提供されるデータは、車両データタイムスタンプ４０２ａ、車両位置データ（エリアコード）４０２ｆのみを含んでいる。一方、図５（ｂ）の緊急時に提供されるデータは、より詳細なデータになっており、車両データタイムスタンプ４０２ａ、車両位置データ（緯度）４０２ｂ、車両位置データ（経度）４０２ｃ、車両走行速度データ４０２ｄ、車両ブレーキ動作情報４０２ｆを含んでいる。図５のサービス利用データは、後に説明する利用規約テーブル４２１（特に、規約ＩＤ＝Ａ３，Ａ４，Ａ６が関係）に従ったものである。

【００５３】
利用規約テーブル４２１は、データ所有者がデータ提供者またはデータ利用者との間で取り決めた利用規約の情報を格納するテーブルであり、図６に示されるように、規約ＩＤ４２２ａ、規約名４２２ｂ、規約内容４２２ｃの各フィールドから構成される。規約ＩＤ４２２ａには、利用規約の各レコードを一意に識別するＩＤが格納される。規約名４２２ｂには、利用規約の名称が格納される。規約内容４２２ｃには、利用規約の具体的な内容が格納される。
【００５４】
図６に示されるの利用規約の名称としては、サービス概要、事業者、利用データ、データ取得方法、利用目的、加工利用、第三者提供、保存期間、本人関与、問合せ先がある。
【００５５】
図６に示される利用規約テーブルの例は、事故緊急通報サービスを例にした場合であり、「利用データ」（規約ＩＤ４２２ａ「Ａ３」）の規約内容は、車両走行データ等である。そしてそれらの「データ取得方法」（規約ＩＤ４２２ａ「Ａ４」）は、定常時（事故発生無し）と緊急時（事故発生有り）で規約内容が異なる。緊急時の方が、定常時に比べて取得間隔が短く、データ提供装置２００からのデータ収集間隔が緊急時と同様の５０ミリ秒毎だとすると、定常時は、データ流通仲介装置１００がそこから間引かれたデータをデータ利用装置３００に提供することを示している。また、「加工利用」（規約ＩＤ４２２ａ「Ａ６」）として、定常時は位置情報データを、エリアコード情報に匿名加工し、位置情報とタイムスタンプデータの車両の安全確認に必要な最小限データのみを収集し、緊急時は、位置情報データを匿名加工せずに、緯度・経度や道路ＩＤといった詳細位置を特定できるデータを収集するようにし、事故検証に必要な位置情報、タイムスタンプデータ、車両走行速度、ブレーキ有無情報、加減速度情報の車両走行データを収集し、問い合わせ先情報は、定常・緊急に何れの状態にかかわらず秘匿化して収集するといったサービスに利用する具体的なデータとその秘匿化や匿名加工処理を規定している。
【００５６】
本実施形態のサービスのシナリオの例として、データ所有者の車両のドライブ時に、事故が発生していない定常時、事故発生した時の緊急時として示したように、複数のサービス提供のシナリオをサポートする場合には、その旨をデータ所有者がデータ提供者またはデータ利用者との間で取り決めた利用規約に記述する必要がある。
【００５７】
パーソナルデータメタデータ４１１は、パーソナルデータ４０１の項目やその記述形式を表すデータである。本実施形態のパーソナルデータメタデータ４１１は、パーソナルデータが車両走行データのときのメタデータであり、例えば、図７に示されるように、ＪＳＯＮ形式で、車両データタイムスタンプデータ項目４１１ａ、車両位置データ項目４１１ｂ、車両走行速度データ項目４１１ｃを含むデータである。
【００５８】
車両データタイムスタンプデータ項目４１１ａでは、車両データタイムスタンプの表現方法として、ＵＮＩＸ時刻を用いていることを示している。また、車両位置データ項目４１１ｂでは、車両位置データの表現方法として、緯度・経度で表され、Ｎ進法が１０（１０進法）であることを示している。さらに、車両走行速度データ項目４１１ｃとして、車両走行速度データの単位はｋｍ／ｈであることを示している。なお、システム上でのメタデータの具体的表現形式は、本例で示したＪＳＯＮ形式以外のものであってもよい。
【００５９】
サービス利用データメタデータ４１２は、サービス利用データ４０２の項目やその記述形式を表すデータである。本実施形態のサービス利用データメタデータ４１２は、パーソナルデータが車両走行データのときに、それを変換したサービス利用データ４０２のメタデータであり、図８に示されるように、サービスシナリオリスト４１２Ａとして、サービスのシナリオに応じた複数のメタデータが定義されている。図８の例では、サービスシナリオリスト４１２Ａの下位リストとして、事故緊急通報サービスの定常時リスト４１２Ａ

１、緊急時リスト４１２Ａ２の２種類のシナリオで用いられるメタデータの例を記載している。

【００６０】

サービスシナリオリスト４１２Ａの先頭の定常時リスト４１２Ａ１には、車両データタイムスタンプデータ項目４１２Ａ１ａ、車両位置データ項目４１２Ａ１ｂを含んでいる。そして、車両データタイムスタンプの表現方法は、ＵＴＣ時刻を用いていることを示している。また、車両位置データの表現方法は、エリアコードで表され、Ｎ進法はＮＵＬＬ、すなわち、Ｎ進法表現は使用しないことを示している。

【００６１】

続く緊急時リスト４１２Ａ２には、車両データタイムスタンプデータ項目４１２Ａ２ａ、車両位置データ項目４１２Ａ２ｂ、車両走行速度データ項目４１２Ａ２ｂを含んでいる。そして、車両データタイムスタンプの表現方法は、ＵＴＣ時刻を用いていることを示している。また、車両位置データの表現方法は、緯度・経度で表され、Ｎ進法が１０（１０進法）であることを示している。さらに、車両走行速度データの単位はｍ／ｓｅｃであることを示している。このようなリストによって複数のメタデータを定義し、サービスのシナリオ毎に使用するメタデータを切り替えることができる。なお、システム上でのメタデータの具体的表現形式は、本例で示したＪＳＯＮ形式以外のものであってもよい。

【００６２】

データ流通制御データ４３１は、データ流通制御部１３０が他のコンポーネントとデータのやり取りに関する手順やデータ形式を記述するデータであり、例えば、図９に示されるように、ＸＡＣＭＬ（eXtensible Access Control Markup Language）のようなＸＭＬベースのマークアップ言語を使用して、データアクセス制御のルールを記述し、そのルールに則ってデータフローを制御する情報を記述するデータである。なお、データ流通制御データ４３１の記述は、ＸＡＣＭＬ以外の記述形式でもよい。

【００６３】

スクリプト管理テーブル４４２は、データ項目ごとに、変換前と変換後のデータの属性のペアと、変換を実現するためのスクリプトの情報を記述するテーブルであり、図１０に示されるように、データＩＤ４４２ａ、変換前属性４４２ｂ、変換後属性４４２ｃ、変換用スクリプト４４２ｄの各フィールドからなる。データＩＤ４４２ａには、データの種別を一意に識別するＩＤが格納される。変換前属性４４２ｂには、データＩＤ４４２ａのデータの変換前の属性が格納される。変換後属性４４２ｃには、データＩＤ４４２ａのデータの変換前の属性が格納される。変換用スクリプト４４２ｄには、変換を実現するためのスクリプトの名称やＩＤが格納される。

【００６４】

データ提供・データ利用情報データ４２０は、図示しなかったが、データ流通仲介装置１００が、データ提供装置２００、データ利用装置３００を利用するためのネットワークアドレスやその他の論理的情報である。

【００６５】

同意手続情報データ４２２は、図示しなかったが、データの所有者が利用規約に同意したか否か、同意日時などのデータの所有者の同意に関する情報に関するデータである。

【００６６】

スクリプトデータ４４１は、図示しなかったが、パーソナルデータ４０１から、サービス利用データ４０２に変換を行うためのスクリプトを記述するデータである。

【００６７】

次に、図１１Ａ、図１１Ｂを用いてデータ流通仲介システムの処理について説明する。

【００６８】

先ず、データ所有者端末１０は、ユーザ（データ所有者）の操作に応じて、データ流通仲介装置１００にデータ利用装置３００が提供するサービス利用要求メッセージＭ０１を送信する（図１１Ａ）。サービス利用要求メッセージＭ０１は、図示しなかったが、サービスＩＤとユーザＩＤ等を含むメッセージである。ここで、サービスＩＤは、データ利用

装置３００が提供するサービスを識別する識別子であり、ユーザＩＤは、ユーザを識別する識別子である。

【００６９】

データ流通仲介装置１００は、通信部１４０よりサービス利用要求メッセージＭ０１を受信し、受信したサービス利用要求メッセージＭ０１に関する情報を保持する。

【００７０】

次に、データ提供・データ利用情報データ４２０には、サービスＩＤとデータ利用装置３００とを関連付ける情報が予め定義されており、データ流通仲介装置１００は、受信したサービス利用要求メッセージＭ０１に含まれるサービスＩＤに該当するデータ利用装置３００に、該サービスＩＤにおけるサービス利用規約要求メッセージＭ０２を通信部１４０により送信する。

【００７１】

データ利用装置３００は、送信されたサービス利用規約要求メッセージＭ０２を受信し、データ利用装置３００は、受信したサービス利用規約要求メッセージＭ０２に含まれるサービスＩＤに対応するサービス利用規約データの情報を含むサービス利用規約レスポンスＲ０１をデータ流通仲介装置１００に返信する。

【００７２】

ここで、サービスＩＤに対応するサービス利用規約データは、該サービスＩＤに対応するサービスを提供するサービス事業者が定めた利用規約を表現する情報を含むデータである。

【００７３】

次に、利用規約管理部１２１は、サービス利用規約データに該サービスの利用規約に不備がないか否かを確認し、不備がある場合には、該サービスの利用規約を修正し、ユーザに開示する規約を確定して（Ｓ０１）、サービス利用規約データの情報を、図６に示した利用規約テーブル４２１として保管する（Ｓ０２）。

【００７４】

そして、データ流通仲介装置１００は、通信部１４０を介して、データ利用装置３００に、サービス利用規約確定通知Ｎ０１を送信し、データ所有者端末１０に、サービス利用規約の内容を含むサービス利用規約通知Ｎ０２を行う。

【００７５】

次に、同意手続管理部１２２は、データ所有者が送信したサービス利用規約に同意することを要求する同意要求メッセージＭ０３を、データ所有者端末１０に送信する。

【００７６】

データ所有者端末１０は、サービス利用規約の内容と、同意要求メッセージＭ０３を受け取ったことをデータ所有者に知らせ、表示画面を通じて受け取ったサービス利用規約の内容と、同意要求メッセージＭ０３の内容を表示する。データ所有者は、表示されている画面に表示されているサービス利用規約の内容と、同意要求メッセージＭ０３の内容に基づき、新たに利用したいサービスの利用規約を同意するか否かの意思表示し（Ｓ０３）、データ所有者端末１０は、同意した場合に、同意通知Ｎ０３をデータ流通仲介装置１００に送信する。

【００７７】

次に、同意手続管理部１２２は、通信部１４０を介して同意通知Ｎ０３から同意したサービスに関する情報を取得し、例えば、どのデータ所有者が、どのサービスに、どのような利用規約を同意するかを、同意手続情報データ４２２として保管する（Ｓ０４）。

【００７８】

次に、パーソナルデータメタデータ管理部１１１は、パーソナルデータメタデータ提供要求メッセージＭ１１をデータ提供装置２００に送信し、する。パーソナルデータメタデータ４１１の提供を要求する（図１１Ｂ）。パーソナルデータメタデータ４１１は、データ提供装置２００で保有するパーソナルデータのデータカタログとして公開されたものである。一方、データカタログとして公開されていない場合でも、データ所有者の権利とし

て、データ所有者がデータ所有者端末１０からデータ流通仲介装置１００を介して、データ提供装置２００にパーソナルデータメタデータ４１１の提供を依頼することができる。

【００７９】

次に、パーソナルデータメタデータ管理部１１１は、データ提供装置２００から提供されるパーソナルデータメタデータ４１１を含むパーソナルデータメタデータレスポンスＲ１１を受信し、受信した図７に示すパーソナルデータメタデータ４１１を保管する（Ｓ１１）。

【００８０】

次に、サービス利用データメタデータ管理部１１２は、パーソナルデータの収集、蓄積、利用用途を含む利用規約テーブルの情報と、同意手続情報データ４２２に基づき、図８に示すサービス利用データメタデータ４１２を生成し（Ｓ１２）、そのサービス利用データメタデータ４１２を保管する（Ｓ１３）。

【００８１】

次に、データ利用装置３００からのサービス利用データ要求メッセージＭ１２をデータ流通仲介装置１００が受信し、データ流通制御部１３０がそのデータ要求の内容の妥当性を判定することにより、データ流通仲介装置１００が、データ提供装置２００へのパーソナルデータ要求メッセージＭ１３を送信するか、データ要求に対する拒否のレスポンスを、データ利用装置３００へ送信するかを決定する。

【００８２】

データ流通制御部１３０がそのデータ要求の内容の妥当性と判定したときには、データ所有者が新たに利用したいサービスで必要なパーソナルデータ要求メッセージＭ１３をデータ提供装置２００に送信する。

【００８３】

なお、必ずしもデータ利用装置３００からのデータ要求メッセージＭ１２がなくとも、データ所有者端末１０からサービス要求メッセージＭ０１を受けたときに、データ提供装置２００へのパーソナルデータ要求メッセージＭ１３を送信するようにしてもよい。

【００８４】

次に、データ提供装置２００は、データ流通仲介装置１００からの要求に対し、同意手続情報データ４２２を参照し、ユーザが同意済みであることを確認し、ユーザＩＤとデータ項目を使って必要なパーソナルデータを検索し、それらのパーソナルデータ４０１を含むパーソナルデータ提供レスポンスＲ１２を、データ流通仲介装置１００に送信する。

【００８５】

次に、メタデータ属性差異検出部１１３は、図７のパーソナルデータメタデータ４１１と、図８に示されるサービス利用データメタデータ４１２の差異を検出する（Ｓ１４）。図８で示したように、シナリオ毎サービス利用データメタデータ特定部１１４は、現在どのシナリオのサービスが提供されているかを検出し、その検出した情報から、図８のメタデータのリストの内、どのメタデータを使用すべきかを特定する。現在どのシナリオのサービスが提供されているかを検出する方法として、例えば、データ利用装置３００からのサービス利用データ要求メッセージＭ１２の内容によって検出する（例えば、パラメータに、“定常時”、“緊急時”をつける）ことが考えられる。そして、パーソナルデータ変換判定部１１５は、Ｓ１４でのメタデータ属性差異検出部１１３でのメタデータの差異検出結果に基づき、パーソナルデータの変換要否を判定する（Ｓ１５）。パーソナルデータの変換が必要だと判定された場合には（Ｓ１５：Ｙｅｓ）、パーソナルデータ変換処理部１１６は、パーソナルデータの変換処理を行う（Ｓ１６）、一方、Ｓ１６でパーソナルデータの変換が不要だと判定された場合には（Ｓ１５：Ｎｏ）、パーソナルデータの変換処理Ｓ１６は、スキップされる。

【００８６】

例えば、Ｓ１６のパーソナルデータの変換処理は、例えば、図１０に示したスクリプト管理テーブル４４２を参照し、該当するデータ項目と変換の仕様に従って対応するスクリプトを実行することにより実現することができる。また、一つの変換プログラムにより全

てのデータ項目の変換を行うようにしてもよい。

【００８７】

次に、データ流通仲介装置１００は、受信した新たに利用したいサービスのために必要なパーソナルデータに関し、データ提供・データ利用情報データ４２０を参照し、データ利用装置３００に提供するための図９に示されるデータ流通制御データ４３１を生成する（Ｓ１７）。

【００８８】

次に、データ流通仲介装置１００は、パーソナルデータ４０１を変換せずに、あるいは、Ｓ１６で変換したデータを、サービス利用データ４０２として、サービス利用データ４０２を含むサービス利用データ転送レスポンスＲ１２をデータ利用装置３００に送信する。サービス利用データ転送レスポンスＲ１２には、データ所有者を識別するためのユーザＩＤと、サービスを識別するためのサービスＩＤ、該サービスで必要なサービス利用データ４０２のデータ項目が含まれる。

【００８９】

次に、データ流通仲介装置１００は、データ利用装置３００に提供したデータ提供履歴を更新する（Ｓ１８）。データ提供履歴には、タイムスタンプ、ユーザＩＤ、サービスＩＤ、データ項目が含まれる。

【００９０】

次に、データ利用装置３００は、サービス提供のためにデータを利用し（Ｓ１９）、データ所有者端末１０にサービス提供通知を送信する（Ｎ１１）。

【００９１】

本実施形態によれば、データ提供者にて収集され保有しているデータと、新たなサービスを提供するサービス事業者が取り扱うデータの間で、それらの内容に差異がある場合に、データ変換要否を判定し、適当なデータ変換処理を行った後、データを流通させることができる。また、データ提供者で保有されるデータ仕様が変更になった場合や、サービス事業者が新たなサービスの提供を開始する場合や、提供するサービスが複数のシナリオを持っている場合等、データ提供者で保有されるデータおよび、サービスで使用されるデータの動的な変化に対応して、データ変換要否判定と、適当なデータ変換処理を行って、データを流通させることができるため、サービス提供で用いることができないデータが流通してしまうことを抑止し、データ流通を活性化することができる。また、実施形態はパーソナルデータの流通に関する例を挙げて説明したが、パーソナルデータに限る必要はなく企業で保有する法人データに対しても本発明を適用することができ、上記と同様の効果を得ることができる。

【００９２】

〔実施形態２〕

以下、本発明に係る実施形態２を、図１２ないし図１５を用いて説明する。

【００９３】

実施形態１では、データ提供者にて収集され保有しているデータと、新たなサービスを提供するサービス事業者が取り扱うデータの間で、それらの内容に差異がある場合に、データ流通仲介装置でデータ変換要否を判定し、適当なデータ変換処理を行うデータ流通仲介システムの例を説明した。

【００９４】

本実施形態では、実施形態１のデータ流通仲介システムをベースとして、データ所有者のプライバシー保護のためのプライバシーランクという概念を導入したシステムに関するものである。

【００９５】

以下、実施形態１のデータ流通仲介システムと異なる所を中心に説明する。

【００９６】

先ず、図１２を用いて実施形態２に係るデータ流通仲介装置の機能構成図について説明する。

実施形態２に係るデータ流通仲介装置は、実施形態１と比べて、プライバシーランクデータ４２３を保持していることが異なっている。

【００９７】

プライバシーランクデータ４２３については、図１３を用いて以下に詳細に説明する。

プライバシーランクデータ４２３は、個人のプライバシーの保護するランクに従って、データ変換の仕方を記述するデータであり、例えば、図１３に示されように、プライバシーランク４２３ａ、車両位置データ４２３ｂの各フィールドを有する。

【００９８】

プライバシーランク４２３ａには、プライバシーランクを表すコードが格納される。車両位置データ４２３ｂには、サービス利用データ４０２でのデータ表現の形態が格納される。

【００９９】

図１３の例では、プライバシーランクの数が小さいほど、より強くプライバシーの保護するように設定されている。例えば、プライバシーランク４２３ａの値「１」では、サービス利用データとしては、国のコード「カントリーコード」のみが利用されるが、プライバシーランク４２３ａの値「５」では、サービス利用データとしては、国のコードのみが利用されるが、「道路ＩＤ＋道路区間ＩＤ＋緯度経度」のように、車両がどこを走行しているかの詳細な情報が開示される。

【０１００】

次に、図１４を用いて実施形態２に係る利用規約テーブルの一例について説明する。

実施形態２に係る利用規約テーブル４２１は、図６に示した実施形態１の利用規約テーブル４２１で規約ＩＤ４２２ａ「Ａ６」、規約ＩＤ４２２ｂ「加工利用」に該当する規約内容４２２ｃの値のみ異なっている。

【０１０１】

本実施形態の利用規約テーブル４２１の該当する規約内容では、定常時の位置情報データの加工と問合せ先情報がプライバシーランクを用いて記述されている。

【０１０２】

次に、図１５を用いて実施形態２に係るスクリプト管理テーブルの一例を説明する。

本実施形態スクリプト管理テーブルでは、図１４の利用規約テーブル４２１に規定されている加工内容に従って、データＩＤ４４２ａ「Ｄ２００」のパーソナルデータの変換の属性として、変換前属性４４２ｂのプライバシーランク４の表現「緯度経度」から、変換後属性４４２ｃのプライバシーランク３の表現「エリアコード」で表現されることを示している。

【０１０３】

以上、本実施形態によれば、プライバシーランクを導入することにより、利用規約改定時にも、プライバシーランクデータ４２３のみを修正すればよいので、システムの改変を最低限に抑えて、メンテナンス性を向上させることができる。

【符号の説明】

【０１０４】

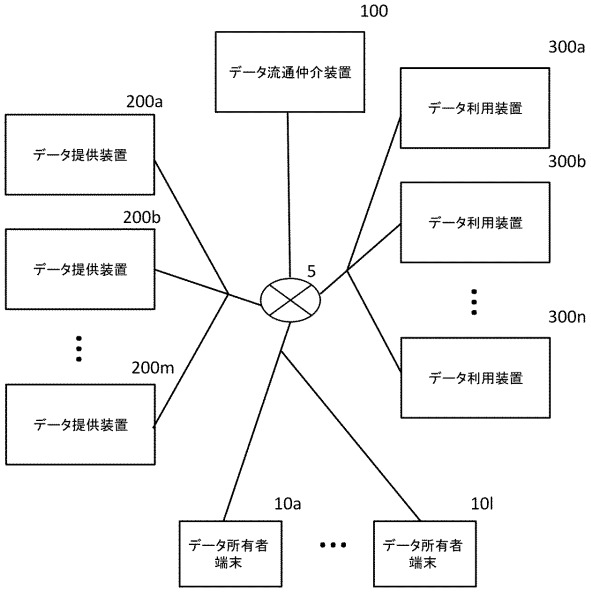
５…ネットワーク、１０…データ所有者端末、１００…データ流通仲介装置、２００…データ提供装置、３００…データ利用装置、１０１…データ提供者管理部、１０２…サービス事業者管理部、１１０…パーソナルデータ変換部、１１１…パーソナルデータメタデータ管理部、１１２…サービス利用データメタデータ管理部、１１３…メタデータ属性差異検出部、１１４…シナリオ毎サービス利用データメタデータ特定部、１１５…パーソナルデータ変換判定部、１１６…パーソナルデータ変換処理部、１２１…利用規約管理部、１２２…同意手続管理部、１３０…データ流通制御部、１４０…通信部、１５０…記憶部、４０１…パーソナルデータ、４０２…サービス利用データ、４１１…パーソナルデータメタデータ、４１２…サービス利用データメタデータ、４２０…データ提供・データ利用情報データ、４２１…利用規約テーブル、４２２…同意手続情報データ、４２３…プライバシーランクデータ、４３１…データ流通制御データ、４４１…スクリプトデータ、４４２

…スクリプト管理テーブル

【図面】

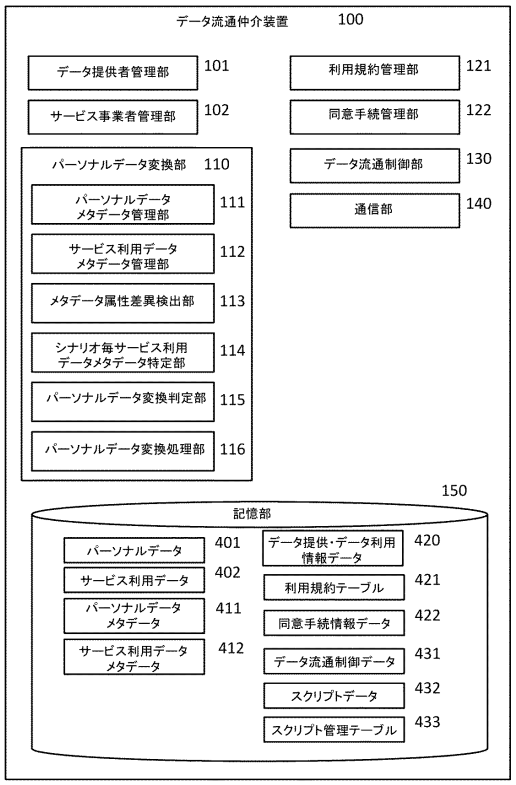
【図１】

図1



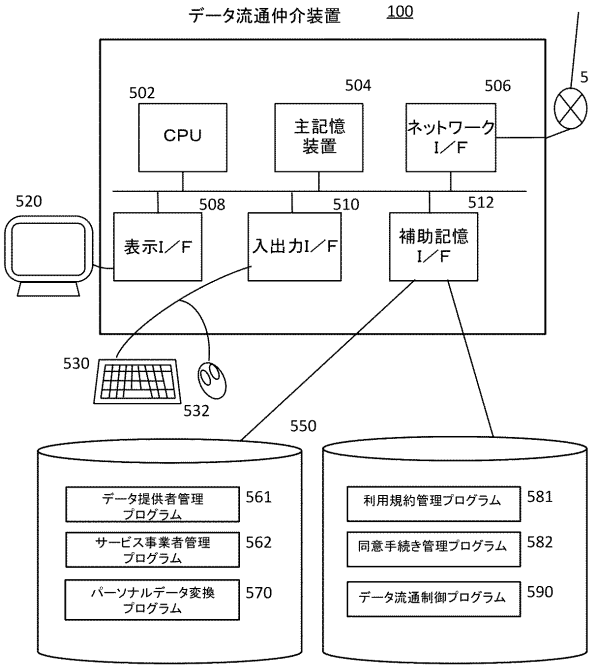
【図２】

図2



【図３】

図3



【図４】

図4

パーソナルデータ（車両走行データ） 401

```
{
  “timestamp” :  1560000000,
  “latitude” :  3538.98,
  “longitude” :  13939.6,
  “speed” :  57.96,
  “brake” :  0
},
```

401a 401b 401c 401d 401e

【図５】

図5

（a）

定常時

サービス利用データ（車両走行データ） 402

```
{
402a  "timestamp" :  "2020-08-05 10:05:39 UTC",
402f  "area" :  "Yokohama"
},
```

（b）

緊急時

サービス利用データ（車両走行データ） 402

```
{
402a  "timestamp" :  2020-08-05 11:01:05 UTC,
402b  "latitude" :  3638.98,
402c  "longitude" :  24939.6,
402d  "speed" :  47.96,
402e  "brake" :  1
},
```

【図６】

図6

利用規約テーブル 421

421a 421b 421c

規約ID	規約名	規約内容
A1	サービス概要	事故緊急通報サービス
A2	事業者	A社
A3	利用データ	氏名 車両固有ID 車両走行データ 問い合わせ先データ ・・・
A4	データ取得方法	・定常時は200ミリ秒毎に定期的 ・緊急時は50ミリ秒毎に定期的
A5	利用目的	事故対応サービス
A6	加工利用	・定常時は、位置情報データをエリアコード情報に匿名加工し、位置情報とタイムスタンプデータの車両の安全確認に必要な最小限データのみを収集。 ・緊急時は、位置情報データを匿名加工せずに緯度・経度や道路IDといった詳細位置を特定できるデータを収集するようにし、事故検証に必要な位置情報、タイムスタンプデータ、車両走行速度、ブレーキ有無情報、加減速度情報の車両走行データを収集。 ・問い合わせ先情報は、定常・緊急に何れの状態にかかわらず秘匿化して収集。住所について定常時は区や市町村情報を収集し、緊急時は番地や建物を含む情報を収集
A7	第三者提供	なし
A8	保存期間	サービス解約まで
A9	本人関与	開示、利用停止、訂正、削除、同意撤回
A10	問合せ先	電話番号：XX-XX-XX メール：XX@A社.com 住所：東京都XX区XXX1丁目1番地

【図７】

図7

パーソナルデータ（車両走行データ）メタデータ 411

```
{
411a  "車両データタイムスタンプデータ":{
        "表現方法" : "UNIX時刻"
      },
411b  "車両位置データ":{
        "表現方法" : "緯度経度",
        "N進法" : 10,
      },
411c  "車両走行速度データ":{
        "単位" : "km/h"
      },
      ・・・
}
```

【図８】

図8

サービス利用データ（車両走行データ）メタデータ 412

```
412A  "サービスシナリオリスト"[
412A1  "定常時":{
412A1a  "車両データタイムスタンプデータ":{
          "表現方法" : " UTC時刻"
        },
412A1b  "車両位置データ":{
          "表現方法" : "エリアコード",
          "N進法" : null,
        },
        ・・・
      }
412A2  "緊急時":{
412A2a  "車両データタイムスタンプデータ":{
          "表現方法" : " UTC時刻"
        },
412A2b  "車両位置データ":{
          "表現方法" : "緯度経度",
          "N進法" : 10,
        },
412A2c  "車両走行速度データ":{
          "単位" : "m/sec"
        },
        ・・・
      }
]
```

【図９】

図9

データ流通制御データ　431

```
<?xml version="1.0" encoding="UTF-8"?>
<Request xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-
17" CombinedDecision="false" ReturnPolicyIdList="true">
  <Attributes Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject">
    <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role" IncludeInResult=
"false">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">serv
iceProvider</AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-
id" IncludeInResult="false">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">vehi
cle</AttributeValue>
    </Attribute>
  </Attributes>
  <Attributes Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
    <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-
id" IncludeInResult="false">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">GET
</AttributeValue>
    </Attribute>
  </Attributes>
</Request>
```

【図１０】

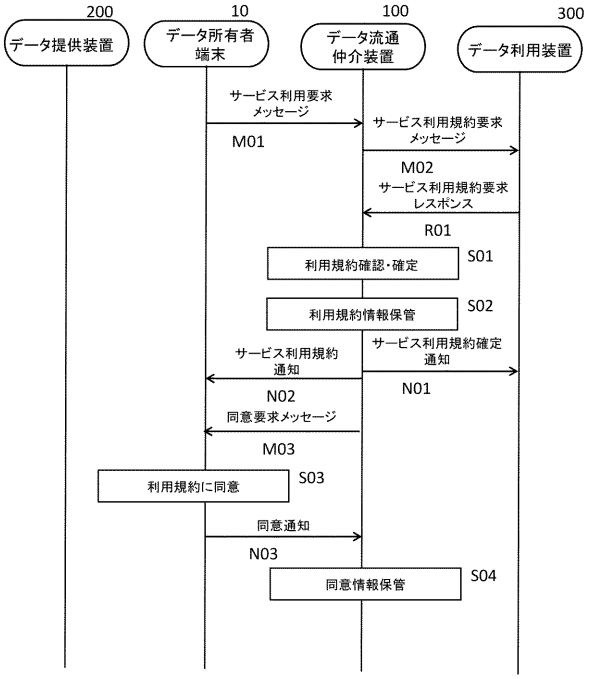
図10

スクリプト管理テーブル　442

	442a	442b	442c	442d
	データID	変換前属性	変換後属性	変換用スクリプト
	D100 (車両データタイムスタンプ)	Unix時刻	UTC時刻	ScriptA
	D200 (車両位置データ)	緯度経度	エリアコード	ScriptB
	D300 (車両走行位置データ)	単位km/h	単位m/sec	ScriptC
	・・・	・・・	・・・	・・・

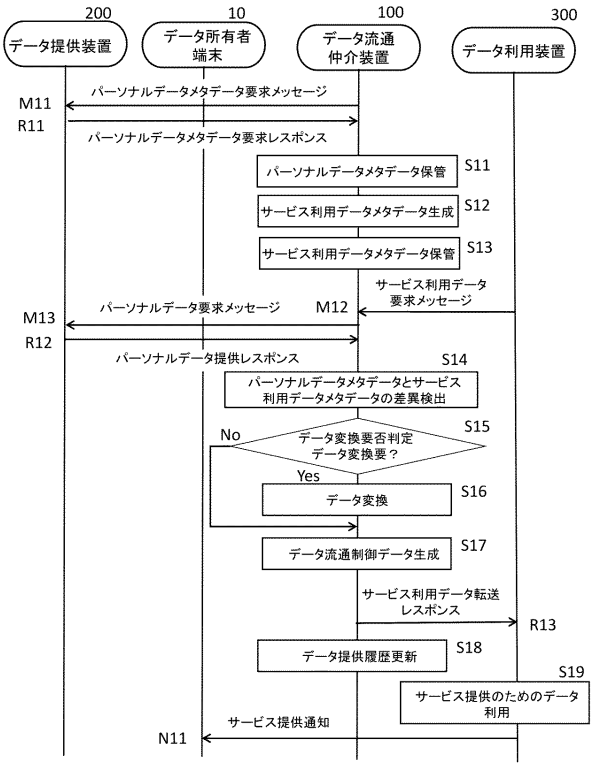
【図１１Ａ】

図11A



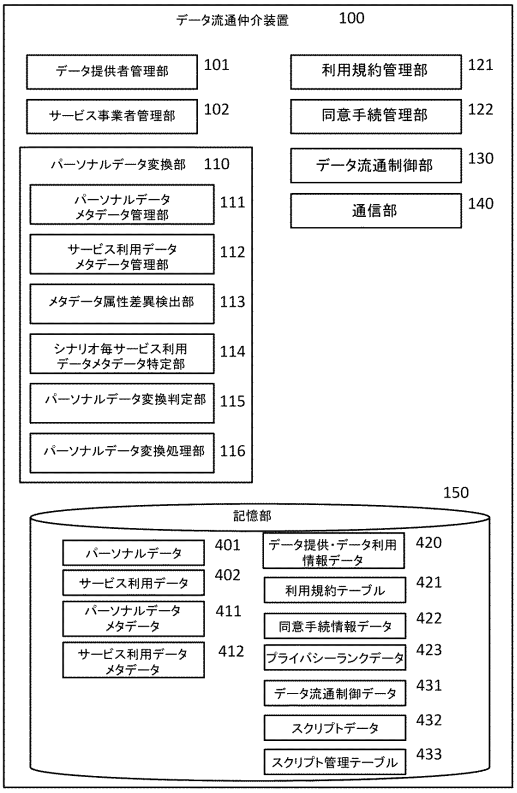
【図１１Ｂ】

図11B



【図１２】

図12



【図１３】

図13

プライバシーランクデータ 423

423a プライバシーランク	423b 車両位置データ
1	カントリーコード
2	都道府県コード
3	エリアコード
4	緯度経度
5	道路ID＋道路区間ID＋緯度経度

【図１４】

図14

利用規約テーブル 421

421a 規約ID	421b 規約名	421c 規約内容
A1	サービス概要	事故緊急通報サービス
A2	事業者	A社
A3	利用データ	氏名 車両固有ID 車両走行データ 問い合わせ先データ ・・・
A4	データ取得方法	・定常時は200ミリ秒毎に定期的 ・緊急時は50ミリ秒毎に定期的
A5	利用目的	事故対応サービス
A6	加工利用	・定常時は、位置情報データをプライバシーランク4からプライバシーランク3となるように匿名加工し、位置情報とタイムスタンプデータの車両の安全確認に必要な最小限データのみを収集。 ・緊急時は、位置情報データを匿名加工せずに、事故検証に必要な位置情報、タイムスタンプデータ、車両走行速度、ブレーキ有無情報、加減速度情報の車両走行データを収集。 ・問い合わせ先情報は、定常・緊急に何れの状態にかかわらず秘匿化して収集。住所について定常時はプライバシーランク3の情報を収集し、緊急時はプライバシーランク2の情報を収集
A7	第三者提供	なし
A8	保存期間	サービス解約まで
A9	本人関与	開示、利用停止、訂正、削除、同意撤回
A10	問合せ先	電話番号：XX-XX-XX メール：XX@A社.com 住所：東京都XX区XXX1丁目1番地

【図１５】

図15

スクリプト管理テーブル 442

442a データID	442b 変換前属性	442c 変換後属性	442d 変換用スクリプト
D100 (車両データタイムスタンプ)	Unix時刻	UTC時刻	ScriptA
D200 (車両位置データ)	プライバシーランク 4	プライバシーランク 3	ScriptB
D300 (車両走行位置データ)	単位km/h	単位m/sec	ScriptC
・・・	・・・	・・・	・・・

フロントページの続き

(56)参考文献　特開２０１６－１９２２１８（ＪＰ，Ａ）
国際公開第２０２１／０８５５１９（WO，Ａ１）
特開２００４－１８５５２１（ＪＰ，Ａ）
国際公開第２００８／１０８１５８（WO，Ａ１）
特開２０１５－１３８５３４（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００