

(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
2023年12月14日(14.12.2023)

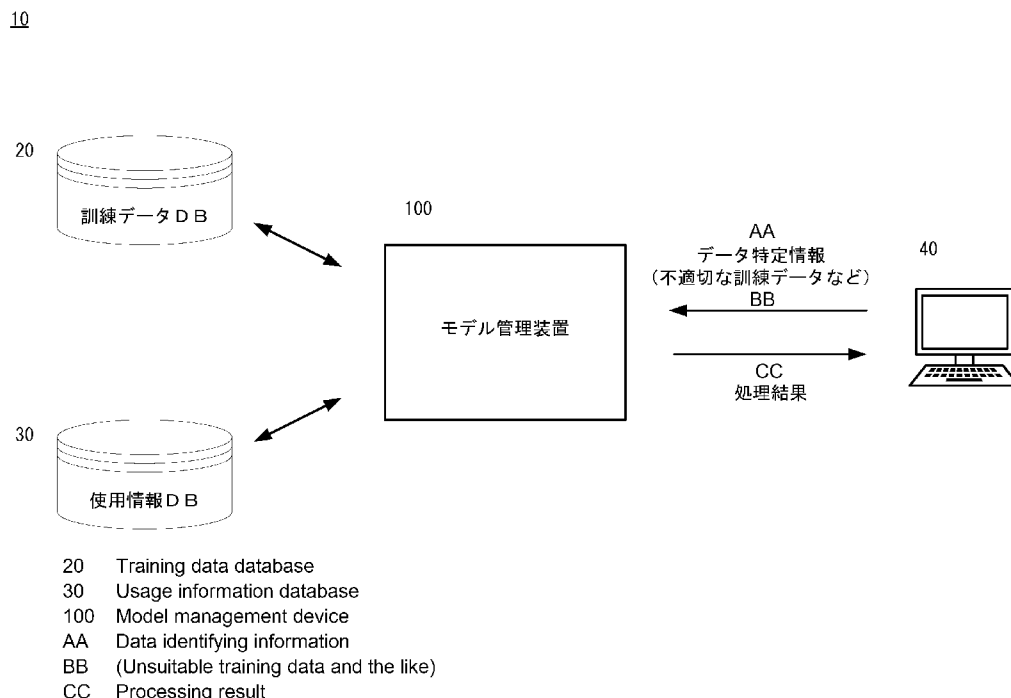


(10) 国際公開番号
WO 2023/238544 A1

- (51) 国際特許分類:
G06N 20/00 (2019.01) *G06F 21/62* (2013.01)
- (21) 国際出願番号: PCT/JP2023/016453
- (22) 国際出願日: 2023年4月26日(26.04.2023)
- (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 2022-093639 2022年6月9日(09.06.2022) JP
- (71) 出願人: コニカミノルタ株式会社 (**KONICA MINOLTA, INC.**) [JP/JP]; 〒1007015 東京都千代田区丸の内二丁目7番2号 Tokyo (JP).
- (72) 発明者: 三村 勇介 (**MIMURA, Yusuke**).
- (74) 代理人: 弁理士法人鷺田国際特許事務所 (**WASHIDA & ASSOCIATES**); 〒1600023 東京都新宿区西新宿1-23-7 新宿ファーストウエスト8階 Tokyo (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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,

(54) **Title:** MODEL MANAGEMENT DEVICE, MODEL MANAGEMENT SYSTEM, AND MODEL MANAGEMENT METHOD

(54) 発明の名称: モデル管理装置、モデル管理システム及びモデル管理方法



(57) **Abstract:** Disclosed is technology for managing training data used to train a machine-learning model. One aspect of the present disclosure relates to a model management device comprising: a data identifying unit that acquires data identifying information; a model identifying unit that, with reference to usage information of training data, identified a first machine-learning model which has been trained by using first training data identified by the data identifying information; and a processing unit that deletes the first training data from a first training data set used to train the first machine-learning

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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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:

- 国際調査報告 (条約第21条(3))

model, and thereby creates a second training data set and executes processing the first machine-learning model.

(57) 要約: 機械学習モデルを訓練するのに使用された訓練データを管理するための技術が開示される。本開示の一態様は、データ特定情報を取得するデータ特定部と、訓練データの使用情報を参照して、前記データ特定情報によって特定された第1の訓練データを使用して訓練された第1の機械学習モデルを特定するモデル特定部と、前記第1の機械学習モデルを訓練するのに使用された第1の訓練データセットから前記第1の訓練データを削除することによって第2の訓練データセットを作成し、前記第1の機械学習モデルに対する処理を実行する処理部と、を有する、モデル管理装置に関する。

明 細 書

発明の名称：

モデル管理装置、モデル管理システム及びモデル管理方法

技術分野

[0001] 本開示は、モデル管理装置、モデル管理システム及びモデル管理方法に関する。

背景技術

[0002] ディープラーニングなどの機械学習技術の進展によって、様々な技術分野に機械学習技術が広範に利用されている。機械学習技術では、一般に訓練データに依存して機械学習モデルの性能が変化しうることが知られている。また、その変化を予測することは困難であることも知られている。

先行技術文献

特許文献

[0003] 特許文献1：特開2020-102001号公報
特許文献2：特開2021-157313号公報

発明の概要

発明が解決しようとする課題

[0004] このように何れの訓練データを利用して機械学習モデルを訓練したか管理することは重要であると考えられる一方、機械学習モデルと、当該機械学習モデルを訓練するのに利用された訓練データとの関連付けを管理するデータ管理技術は、従来あまり注目されてこなかった。

[0005] 上記問題点に鑑み、本開示の1つの課題は、機械学習モデルを訓練するのに使用された訓練データを管理するための技術を提供することである。

課題を解決するための手段

[0006] 本開示の一態様は、データ特定情報を取得するデータ特定部と、訓練データの使用情報を参照して、前記データ特定情報によって特定された第1の訓

練データを使用して訓練された第1の機械学習モデルを特定するモデル特定部と、前記第1の機械学習モデルを訓練するのに使用された第1の訓練データセットから前記第1の訓練データを削除することによって第2の訓練データセットを作成し、前記第1の機械学習モデルに対する処理を実行する処理部と、を有する、モデル管理装置に関する。

発明の効果

[0007] 本開示によると、機械学習モデルを訓練するのに使用された訓練データを管理するための技術を提供することである。

図面の簡単な説明

[0008] [図1]図1は、本開示の一実施例によるモデル管理システムを示す概略図である。

[図2]図2は、本開示の一実施例によるモデル管理装置のハードウェア構成を示すブロック図である。

[図3]図3は、本開示の一実施例によるモデル管理装置の機能構成を示すブロック図である。

[図4]図4は、本開示の一実施例による訓練データの詳細情報を示す図である。

[図5]図5は、本開示の一実施例による使用情報を示す図である。

[図6]図6は、本開示の一実施例によるモデル管理処理を示すフローチャートである。

[図7]図7は、本開示の他の実施例によるモデル管理システムを示す概略図である。

発明を実施するための形態

[0009] 以下、図面を参照して本開示の実施の形態を説明する。

[0010] 以下の実施例では、機械学習モデルを訓練するのに使用された訓練データを管理するためのモデル管理装置が開示される。

[0011] 後述される実施例では、例えば、訓練データセットを使用して訓練された機械学習モデルの運用中、当該訓練データセットの一部又は全ての訓練デー

タの品質に関して問題があることが判明した場合に対処可能なモデル管理装置が開示される。

[0012] 例えば、訓練データについて機械学習モデルの性能の観点からの問題点が考えられうる。一例として、例えば、機械学習モデルを訓練するのに使用された訓練データセットのうち、ある施設における訓練データの取得手法が不適切であったり、あるいは、捏造されたものであることが、当該機械学習モデルの訓練後に判明するケースなどが考えられる。この場合、当該施設において取得された訓練データは不適切であり、機械学習モデルの性能を低下させる可能性がある。このため、当該施設において取得された訓練データの使用は回避される必要があり、不適切な訓練データを含む訓練データセットにより訓練された機械学習モデルは再訓練されることが望ましい。

[0013] 他の例として、データ取得した際の環境と運用時の環境とが異なってしまいうため性能が落ちるケースがある。例えば、コロナ禍前後で人々の生活様式、行動様式などが変化したため、コロナ禍前に取得された訓練データは、コロナ禍後に運用するシステムでは適切でない可能性がある。この場合、コロナ禍前に取得された訓練データは不適切であり、機械学習モデルの性能を低下させる可能性がある。このため、このようなコロナ禍前に取得された訓練データの使用は回避される必要があり、不適切な訓練データを含む訓練データセットにより訓練された機械学習モデルは再訓練されることが望ましい。

[0014] 更なる他の例として、例えば、ある業者によって作成されたアノテーション（注釈、ラベルなど）は品質が良くないことが、当該機械学習モデルの訓練後に判明するケースなどが考えられる。この場合、当該業者により注釈付けされた訓練データは不適切であり、機械学習モデルの性能を低下させる可能性がある。このため、当該業者により注釈付けされた訓練データの使用は回避される必要があり、不適切な訓練データを含む訓練データセットにより訓練された機械学習モデルは再訓練されることが望ましい。

[0015] すなわち、機械学習モデルを訓練するのに使用された訓練データの品質が判断され、基準を充足しない、疑わしい、又は現在の環境とは異なるデータ

は、機械学習モデルの性能の観点から訓練に使用しないようにされる必要がある。

[0016] あるいは、訓練データについて法規上及び／又は倫理上の観点からの問題点が考えられうる。一例として、例えば、商用利用が許可又はライセンスされていない、あるいは、以前は許可又はライセンスされていたが、以降において許可又はライセンスが無効になった訓練データが商用の機械学習モデルを訓練するのに使用されたことが、機械学習モデルの訓練後に判明するケースなどが考えられる。この場合、契約上の観点から、許可又はライセンスされていない訓練データの使用は回避される必要があり、当該訓練データを含む訓練データセットにより訓練された機械学習モデルは再訓練されることが望ましい。

[0017] 他の例として、例えば、データ使用を許諾していない、あるいは、データ使用を以前は許諾していたが、以降において許諾を取り消したいという申し出をした個人の訓練データが機械学習モデルを訓練するのに使用されたケースなどが考えられる。この場合、個人情報保護及び／又は個人情報保護に関する法規の観点から、データ使用を許諾されていない個人情報を含む訓練データの使用は回避される必要があり、当該訓練データを含む訓練データセットにより訓練された機械学習モデルは再訓練されることが望ましい。

[0018] 他の例として、例えば、採用のためのAI (Artificial Intelligence) を開発する際、年齢及び／又は性別を含む訓練データが機械学習モデルを訓練するのに使用されるケースなどが考えられる。この場合、倫理上の観点から、年齢及び／又は性別を含む訓練データの使用は回避される必要があり、当該訓練データを含む訓練データセットにより訓練された機械学習モデルは、不適切なデータを除いたデータセットで再訓練されることが望ましい。

[0019] [概略]

本開示を概略すると、このような不適切な訓練データが機械学習モデルを訓練するのに利用されたことが判明すると、本開示の一実施例によるモデル

管理装置は、不適切な訓練データを利用して訓練された機械学習モデルを特定し、不適切な訓練データを訓練データセットから削除し、不適切な訓練データを含まない訓練データセットを利用して、特定した機械学習モデルを再訓練してもよい。

[0020] 以下の実施例によるモデル管理システム10は、図1に示されるように、訓練データデータベース(DB)20、使用情報データベース(DB)30、端末40、及びモデル管理装置100を有する。

[0021] 訓練データDB20は、訓練データを格納する。具体的には、訓練データDB20は、モデル管理装置100によって管理される1つ以上の機械学習モデルを訓練するのに使用される訓練データを格納する。例えば、訓練データDB20は、訓練データと関連付けて、各訓練データの取得場所、取得時期、アノテーション情報、ライセンス情報、個人情報保護、倫理情報などの詳細情報を格納してもよい。

[0022] 使用情報DB30は、訓練データの使用情報を格納する。ここで、使用情報は、機械学習モデルと、当該機械学習モデルを訓練するのに使用された訓練データとの間の関連付けを示すものであってもよい。具体的には、使用情報DB30は、モデル管理装置100によって管理される1つ以上の機械学習モデルに対する訓練データの使用状況を示す使用情報を格納する。例えば、使用情報DB30は、モデル管理装置100によって管理される各機械学習モデルと関連付けて、当該機械学習モデルを訓練するのに使用された訓練データの識別情報を格納してもよい。

[0023] 端末40は、パーソナルコンピュータ(PC)、タブレット、スマートフォンなど、機械学習モデルの管理者などのユーザによって操作されてもよい。端末40は、モデル管理装置100に有線又は無線接続され、ユーザは、端末40を操作することによって、モデル管理装置100について後述される各種処理を実行させることができる。また、端末40は、不適切なデータを識別する識別情報などのデータ特定情報をユーザから受け付け、モデル管理装置100に提供してもよい。

- [0024] モデル管理装置100は、端末40から不適切な訓練データなどを示すデータ特定情報を取得すると、使用情報DB30に格納されている訓練データの使用情報を参照して、データ特定情報によって特定された訓練データによって訓練された機械学習モデルを特定する。そして、モデル管理装置100は、特定した機械学習モデルを訓練するのに使用された訓練データDB20に格納されている訓練データセットから、特定された訓練データを削除することによって訓練データセットを更新し、特定された機械学習モデルに対する処理（例えば、更新された訓練データセットによる機械学習モデルの再訓練など）を実行し、処理結果を端末40に報告する。
- [0025] ここで、モデル管理装置100は、サーバ、パーソナルコンピュータ（PC）、スマートフォン、タブレット等の計算装置によって実現されてもよく、例えば、図2に示されるようなハードウェア構成を有してもよい。すなわち、モデル管理装置100は、バスBを介し相互接続されるドライブ装置101、ストレージ装置102、メモリ装置103、プロセッサ104、ユーザインタフェース（UI）装置105及び通信装置106を有する。
- [0026] モデル管理装置100における後述される各種機能及び処理を実現するプログラム又は指示は、CD-ROM（Compact Disk-Read Only Memory）、フラッシュメモリ等の着脱可能な記憶媒体に格納されてもよい。当該記憶媒体がドライブ装置101にセットされると、プログラム又は指示が記憶媒体からドライブ装置101を介しストレージ装置102又はメモリ装置103にインストールされる。ただし、プログラム又は指示は、必ずしも記憶媒体からインストールされる必要はなく、ネットワークなどを介し何れかの外部装置からダウンロードされてもよい。
- [0027] ストレージ装置102は、ハードディスクドライブなどによって実現され、インストールされたプログラム又は指示と共に、プログラム又は指示の実行に用いられるファイル、データ等を格納する。
- [0028] メモリ装置103は、ランダムアクセスメモリ、スタティックメモリ等によって実現され、プログラム又は指示が起動されると、ストレージ装置10

2からプログラム又は指示、データ等を読み出して格納する。ストレージ装置102、メモリ装置103及び着脱可能な記憶媒体は、非一時的な有形の記憶媒体(non-transitory tangible storage medium)として総称されてもよい。

[0029] プロセッサ104は、1つ以上のプロセッサコアから構成されうる1つ以上のCPU(Central Processing Unit)、GPU(Graphics Processing Unit)、処理回路(processing circuitry)等によって実現されてもよく、メモリ装置103に格納されたプログラム、指示、当該プログラム若しくは指示を実行するのに必要なパラメータなどのデータ等に従って、後述されるモデル管理装置100の各種機能及び処理を実行する。

[0030] ユーザインタフェース(UI)装置105は、キーボード、マウス、カメラ、マイクロフォン等の入力装置、ディスプレイ、スピーカ、ヘッドセット、プリンタ等の出力装置、タッチパネル等の入出力装置から構成されてもよく、ユーザとモデル管理装置100との間のインタフェースを実現する。例えば、ユーザは、ディスプレイ又はタッチパネルに表示されたGUI(Graphical User Interface)をキーボード、マウス等を操作し、モデル管理装置100を操作する。

[0031] 通信装置106は、外部装置、インターネット、LAN(Local Area Network)、セルラーネットワーク等の通信ネットワークとの有線及び／又は無線通信処理を実行する各種通信回路により実現される。

[0032] しかしながら、上述したハードウェア構成は単なる一例であり、本開示によるモデル管理装置100は、他の何れか適切なハードウェア構成により実現されてもよい。

[0033] [モデル管理装置]

次に、図3～5を参照して、本開示の一実施例によるモデル管理装置100を説明する。本実施例によるモデル管理装置100は、訓練データの使用情報を参照して、データ特定情報によって特定された訓練データによって訓

練された機械学習モデルを特定し、特定した機械学習モデルを訓練するのに使用された訓練データセットから、特定された訓練データを削除し、更新された訓練データセットによって当該機械学習モデルに対する処理（例えば、再訓練など）を実行してもよい。

[0034] 図3は、本開示の一実施例によるモデル管理装置100の機能構成を示すブロック図である。図3に示されるように、モデル管理装置100は、データ特定部110、モデル特定部120及び処理部130を有する。例えば、データ特定部110、モデル特定部120及び処理部130の1つ以上の機能部は、1つ以上のプロセッサ104がストレージ装置102及び／又はメモリ装置103などの非一時的な有形の記憶媒体に格納されている1つ以上のプログラム又は指示を実行することによって実現されてもよい。

[0035] データ特定部110は、データ特定情報を取得する。具体的には、端末400などから訓練データを特定する識別情報を取得すると、データ特定部110は、取得した識別情報に基づいて、訓練データDB20に格納されている訓練データセットから識別情報に対応する訓練データを特定する。

[0036] 例えば、データ特定情報は、モデル管理装置100によって管理される機械学習モデルを訓練するのに使用されたが、訓練後に不適切なデータであることが判明した訓練データを示すものであってもよい。具体的には、データ特定情報は、当該訓練データを使用することによって機械学習モデルの性能を低下させる可能性がある訓練データを示すものであってもよい。例えば、そのような訓練データとして、不適切な取得手法によって取得された訓練データ、捏造された訓練データ、コロナ禍前に取得された訓練データ、不良業者によって注釈付けされた訓練データなどであってもよい。また、データ特定情報は、当該訓練データを使用することによって法規上及び／又は倫理上の観点から問題となり得る訓練データを示すものであってもよい。例えば、そのような訓練データとして、商用利用が許可又はライセンスされていない訓練データ、以前は許可又はライセンスされていたが、以降において許可又はライセンスが無効になった訓練データ、データ使用を許諾していない個人

に関する訓練データ、データ使用を以前は許諾していたが、以降において許諾を取り消したいという申し出をした個人に関する訓練データ、年齢及び／又は性別を含む訓練データなどがあげられる。

[0037] なお、データ特定情報は、個別の訓練データを特定する識別情報であってもよいが、これに限定されるものでない。例えば、データ特定情報は、訓練データDB20に格納されている複数の訓練データを特定又は抽出するためのデータ特定条件（例えば、特定の取得場所、取得時期、アノテーション業者などを示す）の形式で提供されてもよい。このようなデータ特定条件を端末40から取得すると、データ特定部110は、取得したデータ特定条件に該当する訓練データセットを訓練データDB20において特定してもよい。

[0038] 例えば、訓練データDB20が、図4に示されるような各訓練データに対する詳細情報を保持する場合、データ特定部110は、データ特定条件に該当する訓練データを検索し、検出した訓練データセットを当該データ特定条件に該当する訓練データとして抽出してもよい。例えば、データ特定条件が取得場所“施設A”である場合、データ特定部110は、取得場所“施設A”に該当する訓練データ#001、#005、#008を抽出してもよい。また、データ特定条件が個人情報保護“許諾”である場合、データ特定部110は、個人情報保護“許諾”に該当する訓練データ#001、#004、#006、#008を抽出してもよい。

[0039] モデル特定部120は、訓練データの使用情報を参照して、データ特定情報によって特定された訓練データを使用して訓練された機械学習モデルを特定する。具体的には、端末40などから取得したデータ特定情報に対応する訓練データが特定されると、モデル特定部120は、使用情報DB30に格納されている使用情報にアクセスし、特定された訓練データを使用して訓練された機械学習モデルを特定する。

[0040] 例えば、使用情報は、図4に示されるようなテーブル形式のデータ構造を有してもよく、例えば、“モデルインデックス”及び“データインデックス”の2つのカラムを有してもよい。“モデルインデックス”は、モデル管理

装置 100 によって管理される機械学習モデル # X 1, # X 2, . . . を識別する。また、“データインデックス”は、訓練データ DB 20 に格納されている訓練データ # 001, # 002, . . . を識別し、各機械学習モデルを訓練するのに使用された訓練データを示す。

[0041] 例えば、データ特定情報によって訓練データ # 001 が特定されると、モデル特定部 120 は、使用情報を参照して、データインデックス # 001 に対応するモデルインデックス # X 1 を特定してもよい。また、データ特定情報によって訓練データ # 002 が特定されると、モデル特定部 120 は、使用情報を参照して、データインデックス # 002 に対応するモデルインデックス # X 2 を特定してもよい。

[0042] 処理部 130 は、機械学習モデルを訓練するのに使用された訓練データセットから、データ特定情報によって特定された訓練データを削除することによって新たな訓練データセットを作成し、機械学習モデルに対する処理を実行する。具体的には、取得したデータ特定情報によって特定された訓練データを使用して訓練された機械学習モデルが特定されると、処理部 130 は、特定された機械学習モデルを訓練するのに使用された訓練データセットから特定された訓練データを削除し、残りの訓練データによって訓練データセットを更新してもよい。そして、処理部 130 は、更新した訓練データセットに基づいて当該機械学習モデルに対して処理を実行してもよく、例えば、更新した訓練データセットを使用して当該機械学習モデルを再訓練してもよい。

[0043] 例えば、上述したように、訓練データ # 001 が不適切なデータとして特定された場合、処理部 130 は、機械学習モデル # X 1 を訓練するのに使用された訓練データセット # 001, # 004, # 006, # 008, . . . から訓練データ # 001 を削除し、更新された訓練データセット # 004, # 006, # 008, . . . によって機械学習モデル # 1 を再訓練してもよい。同様に、訓練データ # 002 が不適切なデータとして特定された場合、処理部 130 は、機械学習モデル # X 2 を訓練するのに使用された訓練デー

タセット#002, #003, #005, #007, #009, . . . から訓練データ#002を削除し、更新された訓練データセット#003, #005, #007, #009, . . . によって機械学習モデル#2を再訓練してもよい。

[0044] また、処理部130は、データ特定情報によって特定された訓練データを訓練データDB20から削除してもよいし、あるいは、使用不可にしてもよい。これにより、使用不可となった訓練データの使用を回避することができ、また、使用不可となった訓練データに対して確保された記憶領域を解放することができる。

[0045] また、処理部130は、所与の時点において機械学習モデルが使用可能であるか判定してもよい。具体的には、ライセンスMの満了時など、訓練データの使用期限を示すデータ特定情報を取得すると、データ特定部110は、訓練データDB20の詳細情報を参照して、ライセンス情報として“ライセンスM”を有する訓練データ#001, #004, #006, #008を特定する。特定された訓練データ#001, #004, #006, #008は満了日後に使用不可となるため、処理部130は、ライセンスMの満了日後に訓練データ#001, #004, #006, #008を使用して訓練された機械学習モデルが運用不可になると判定してもよい。この場合、処理部130は、訓練データ#001, #004, #006, #008を削除した訓練データセットによって機械学習モデルを再訓練し、ライセンスMの満了日後には、再訓練された機械学習モデルを運用するようにしてもよい。これにより、ライセンスの期限に対応して機械学習モデルの運用を適切に管理することができる。

[0046] 本実施例によると、不適切なデータとして特定された訓練データを使用して訓練された機械学習モデルを、不適切なデータが削除された訓練データセットによって再訓練することが可能であり、機械学習モデルの性能の観点だけでなく、法規上及び／又は倫理上の観点からも適した機械学習モデルを再取得することができる。

[0047] [モデル管理処理]

次に、図6を参照して、本開示の一実施例によるモデル管理処理を説明する。当該モデル管理処理は、上述したモデル管理装置100によって実行され、より詳細には、モデル管理装置100の1つ以上のプロセッサ104が1つ以上のメモリ装置103に格納された1つ以上のプログラム又は指示を実行することによって実現されてもよい。図6は、本開示の一実施例によるモデル管理処理を示すフローチャートである。

[0048] 図6に示されるように、ステップS101において、モデル管理装置100は、データ特定情報を取得する。具体的には、モデル管理装置100は、端末40などを介しユーザから1つ以上の不適切な訓練データを特定するデータ特定情報を取得してもよい。例えば、データ特定情報は、訓練データを識別する識別情報であってもよいし、あるいは、1つ以上の訓練データを特定するデータ特定条件であってもよい。例えば、“取得場所が施設Aである”というデータ特定条件が提供されると、モデル管理装置100は、訓練データDB20の詳細情報を参照して、“取得場所”が“施設A”に該当する訓練データ#001、#005、#008を特定してもよい。

[0049] ステップS102において、モデル管理装置100は、使用情報を参照して、特定された訓練データを使用して訓練された機械学習モデルを特定する。具体的には、モデル管理装置100は、使用情報DB30に格納されている使用情報を参照して、ステップS101において特定された各訓練データを使用して訓練された機械学習モデルを特定してもよい。例えば、モデル管理装置100は、訓練データ#001、#005、#008を使用して訓練された機械学習モデルとして2つの機械学習モデル#X1、#X2を特定してもよい。

[0050] ステップS103において、モデル管理装置100は、特定された機械学習モデルを訓練するのに使用された訓練データセットから、特定された訓練データを削除する。例えば、ステップS102において機械学習モデル#X1、#X2が特定されると、モデル管理装置100は、機械学習モデル#X

1, #X2を訓練するのにそれぞれ使用された訓練データセット#TD1={#001, #004, #006, #008, ...}及び#TD2={#002, #003, #005, #007, #009, ...}を特定する。そして、モデル管理装置100は、訓練データセット#TD1, #TD#2から訓練データ#001, #005, #008を削除し、#TD1_deleted={#004, #006, ...}及び#TD2_deleted={#002, #003, #007, #009, ...}を作成する。

[0051] ステップS104において、モデル管理装置100は、機械学習モデルに対する処理を実行する。例えば、モデル管理装置100は、#TD1_deleted={#004, #006, ...}及び#TD2_deleted={#002, #003, #007, #009, ...}を使用して、機械学習モデル#X1, #X2をそれぞれ再訓練してもよい。

[0052] 本実施例によると、不適切なデータとして特定された訓練データを使用して訓練された機械学習モデルを、不適切なデータが削除された訓練データセットによって再訓練することが可能であり、機械学習モデルの性能の観点だけでなく、法規上及び／又は倫理上の観点からも適した機械学習モデルを再取得することができる。

[0053] [変形例]

次に、図7を参照して、本開示の他の実施例によるモデル管理システム10を説明する。本実施例によるモデル管理システム10は更に、データ変換装置50及び変換データベース(DB)60を有する。

[0054] データ変換装置50は、訓練データDB20に格納されている個人情報を含む訓練データから個人情報を削除又は秘匿化するためのデータ変換を実行し、変換された訓練データを変換DB60に格納する。

[0055] 変換DB60は、データから個人情報を秘匿化又は削除するようデータ変換装置50によって変換された訓練データを格納する。モデル管理装置100は、訓練データDB20に格納されている訓練データの代わりに、変換DB60に格納されている変換された訓練データを使用して、機械学習モデル

を訓練してもよい。これにより、モデル管理装置100は、個人情報を含まない訓練データによって機械学習モデルを訓練することができる。なお、変換DB60は、訓練データDB20に格納されている各訓練データの詳細情報を変換された訓練データと関連付けて格納してもよい。

[0056] 本実施例によるモデル管理システム10において、不適切なデータを特定するデータ特定情報を取得すると、データ特定部110は、データ特定情報によって識別される不適切な訓練データを特定し、モデル特定部120は、使用情報を参照して、特定された不適切な訓練データを使用して訓練された機械学習モデルを特定する。そして、処理部130は、特定された機械学習モデルを訓練するのに使用された変換後の訓練データセットを変換DB60において特定し、特定した変換後の訓練データセットから不適切な訓練データを削除する。さらに、処理部130は、不適切な訓練データを削除した変換後の訓練データセットを使用して、当該機械学習モデルを再訓練してもよい。

[0057] 本実施例によると、個人情報を含む訓練データから個人情報を削除又は秘匿化するようデータ変換が実行され、変換された訓練データが機械学習モデルを訓練するのに使用される。機械学習モデルの運用中に不適切な訓練データが判明した場合であっても、不適切な訓練データを削除すると共に、更新された個人情報を含まない訓練データによって機械学習モデルを再訓練することができる。

[0058] なお、以上の説明に関して更に以下の付記を開示する。

(付記1)

データ特定情報を取得するデータ特定部と、

訓練データの使用情報を参照して、前記データ特定情報によって特定された第1の訓練データを使用して訓練された第1の機械学習モデルを特定するモデル特定部と、

前記第1の機械学習モデルを訓練するのに使用された第1の訓練データセットから前記第1の訓練データを削除することによって第2の訓練データセ

ットを作成し、前記第 1 の機械学習モデルに対する処理を実行する処理部と、

を有する、モデル管理装置。

(付記 2)

前記使用情報は、機械学習モデルと、前記機械学習モデルを訓練するのに使用された訓練データとの間の関連付けを示す、付記 1 に記載のモデル管理装置。

(付記 3)

前記訓練データは、取得場所、取得時期、アノテーション情報、ライセンス情報、個人情報保護及び倫理情報の 1 つ以上と関連付けされる、付記 1 又は 2 に記載のモデル管理装置。

(付記 4)

前記処理部は、前記第 2 の訓練データセットを使用して前記第 1 の機械学習モデルを再訓練する、付記 1 から 3 の何れか一項に記載のモデル管理装置。

(付記 5)

前記訓練データは、データから個人情報を秘匿化又は削除することによって生成される、付記 1 から 4 の何れか一項に記載のモデル管理装置。

(付記 6)

前記処理部は、所与の時点において前記第 1 の機械学習モデルが使用可能であるか判定する、付記 1 から 5 の何れか一項に記載のモデル管理装置。

(付記 7)

訓練データを格納する訓練データデータベース (DB) と、
前記訓練データの使用情報を格納する使用情報データベース (DB) と、
前記訓練データ DB と前記使用情報 DB と通信接続されるモデル管理装置と、

を有し、

前記モデル管理装置は、

データ特定情報を取得するデータ特定部と、

前記使用情報を参照して、前記データ特定情報によって特定された第1の訓練データを使用して訓練された第1の機械学習モデルを特定するモデル特定部と、

前記第1の機械学習モデルを訓練するのに使用された第1の訓練データセットから前記第1の訓練データを削除することによって第2の訓練データセットを作成し、前記第1の機械学習モデルに対する処理を実行する処理部と、

を有する、モデル管理システム。

(付記8)

データ特定情報を取得することと、

訓練データの使用情報を参照して、前記データ特定情報によって特定された第1の訓練データを使用して訓練された第1の機械学習モデルを特定することと、

前記第1の機械学習モデルを訓練するのに使用された第1の訓練データセットから前記第1の訓練データを削除することによって第2の訓練データセットを作成し、前記第1の機械学習モデルに対する処理を実行することと、
を有する、コンピュータが実行するモデル管理方法。

[0059] 以上、本開示の実施例について詳述したが、本開示は上述した特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本開示の要旨の範囲内において、種々の変形・変更が可能である。

[0060] 2022年6月9日出願の特願2022-093639号の日本出願に含まれる明細書、図面および要約書の開示内容は、すべて本願に援用される。

符号の説明

- [0061] 10 モデル管理システム
20 訓練データDB
30 使用情報DB
40 端末

- 50 データ変換装置
- 60 変換DB
- 100 モデル変換装置
- 110 データ特定部
- 120 モデル特定部
- 130 処理部

請求の範囲

- [請求項1] データ特定情報を取得するデータ特定部と、
訓練データの使用情報を参照して、前記データ特定情報によって特定された第1の訓練データを使用して訓練された第1の機械学習モデルを特定するモデル特定部と、
前記第1の機械学習モデルを訓練するのに使用された第1の訓練データセットから前記第1の訓練データを削除することによって第2の訓練データセットを作成し、前記第1の機械学習モデルに対する処理を実行する処理部と、
を有する、モデル管理装置。
- [請求項2] 前記使用情報は、機械学習モデルと、前記機械学習モデルを訓練するのに使用された訓練データとの間の関連付けを示す、請求項1に記載のモデル管理装置。
- [請求項3] 前記訓練データは、取得場所、取得時期、アノテーション情報、ライセンス情報、個人情報保護及び倫理情報の1つ以上と関連付けされる、請求項1に記載のモデル管理装置。
- [請求項4] 前記処理部は、前記第2の訓練データセットを使用して前記第1の機械学習モデルを再訓練する、請求項1に記載のモデル管理装置。
- [請求項5] 前記訓練データは、データから個人情報を秘匿化又は削除することによって生成される、請求項1に記載のモデル管理装置。
- [請求項6] 前記処理部は、所与の時点において前記第1の機械学習モデルが使用可能であるか判定する、請求項1に記載のモデル管理装置。
- [請求項7] 訓練データを格納する訓練データデータベース（DB）と、
前記訓練データの使用情報を格納する使用情報データベース（DB）と、
前記訓練データDBと前記使用情報DBと通信接続されるモデル管理装置と、
を有し、

前記モデル管理装置は、

データ特定情報を取得するデータ特定部と、

前記使用情報を参照して、前記データ特定情報によって特定された第1の訓練データを使用して訓練された第1の機械学習モデルを特定するモデル特定部と、

前記第1の機械学習モデルを訓練するのに使用された第1の訓練データセットから前記第1の訓練データを削除することによって第2の訓練データセットを作成し、前記第1の機械学習モデルに対する処理を実行する処理部と、

を有する、モデル管理システム。

[請求項8]

データ特定情報を取得することと、

訓練データの使用情報を参照して、前記データ特定情報によって特定された第1の訓練データを使用して訓練された第1の機械学習モデルを特定することと、

前記第1の機械学習モデルを訓練するのに使用された第1の訓練データセットから前記第1の訓練データを削除することによって第2の訓練データセットを作成し、前記第1の機械学習モデルに対する処理を実行することと、

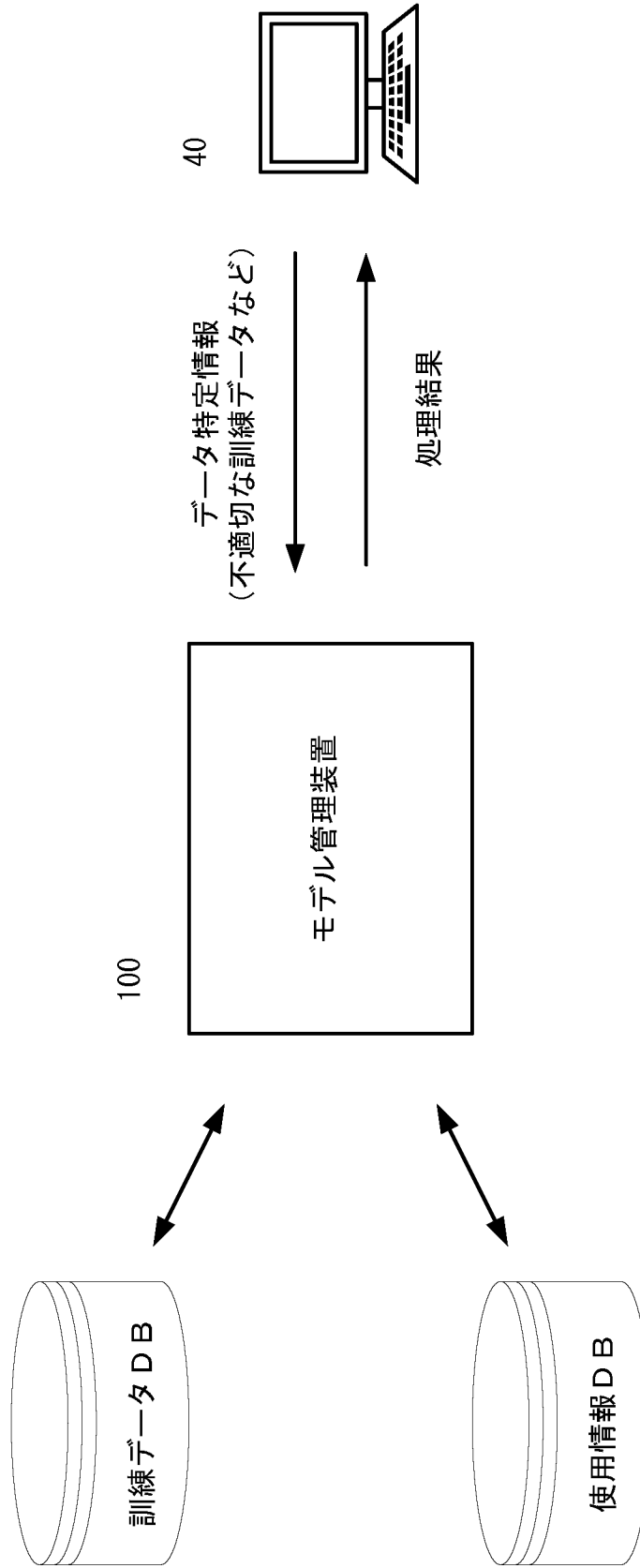
を有する、コンピュータが実行するモデル管理方法。

[図1]

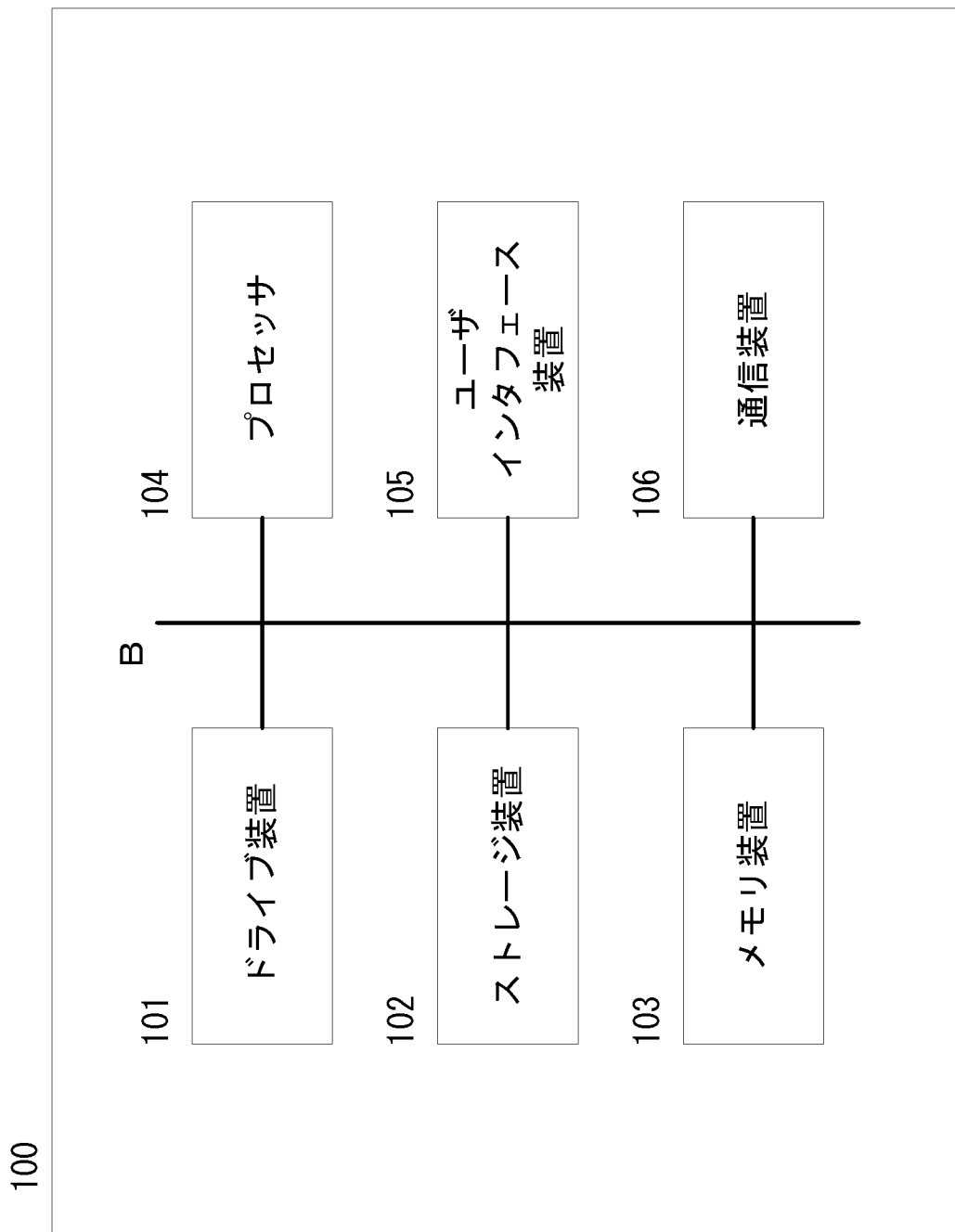
10

20

30

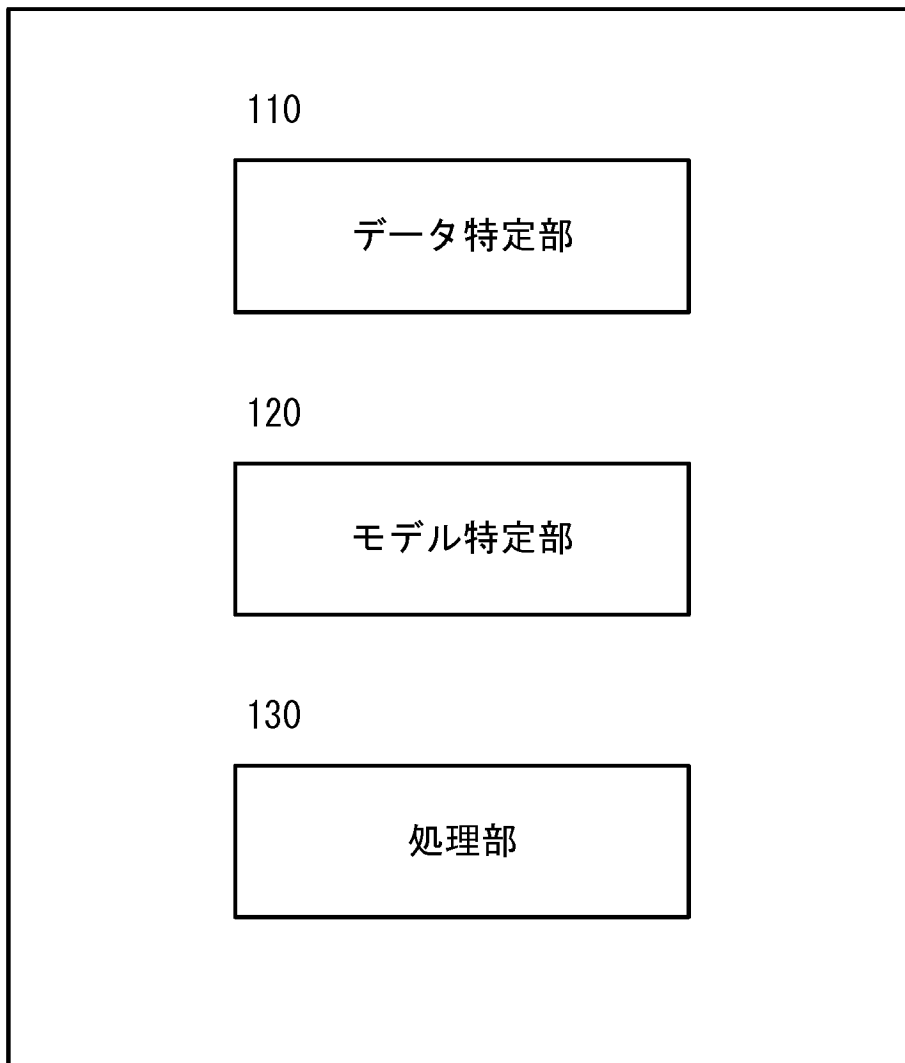


[図2]



[図3]

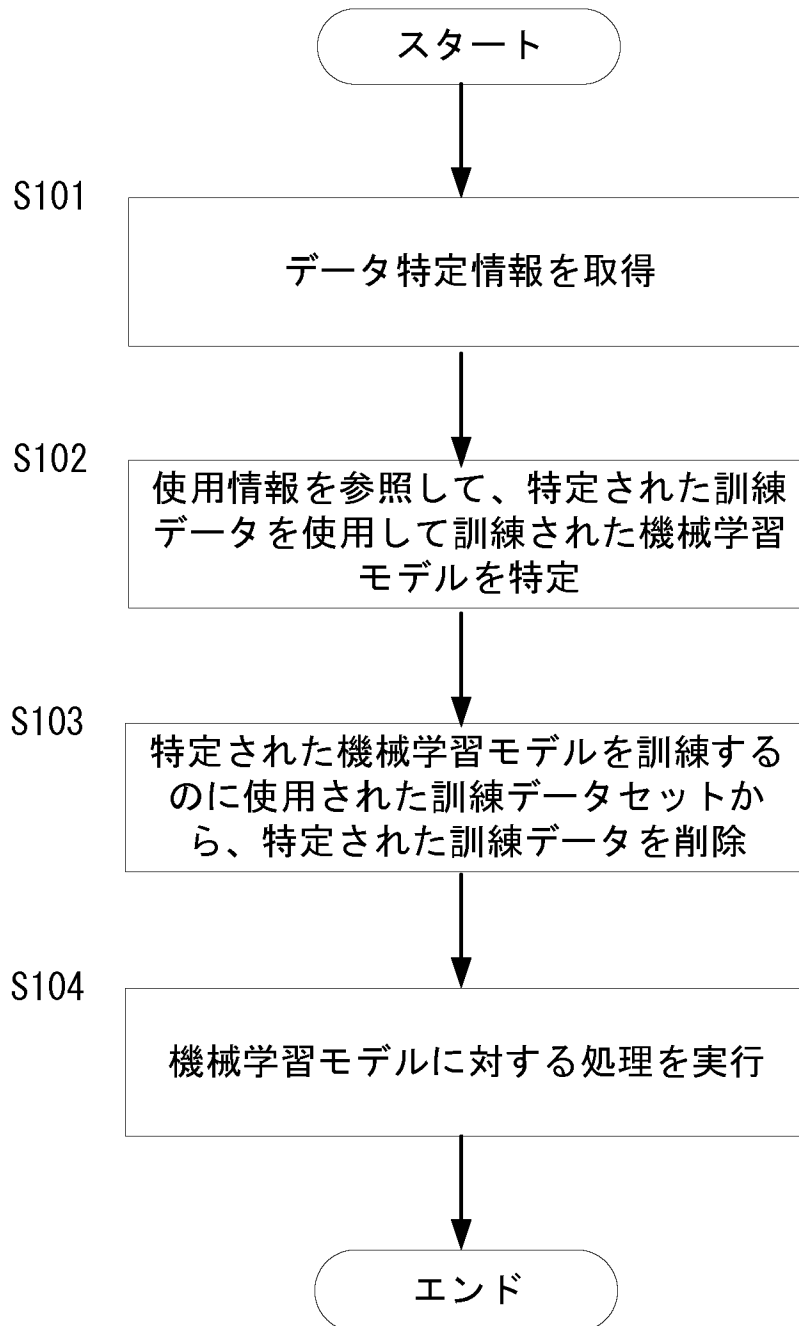
100



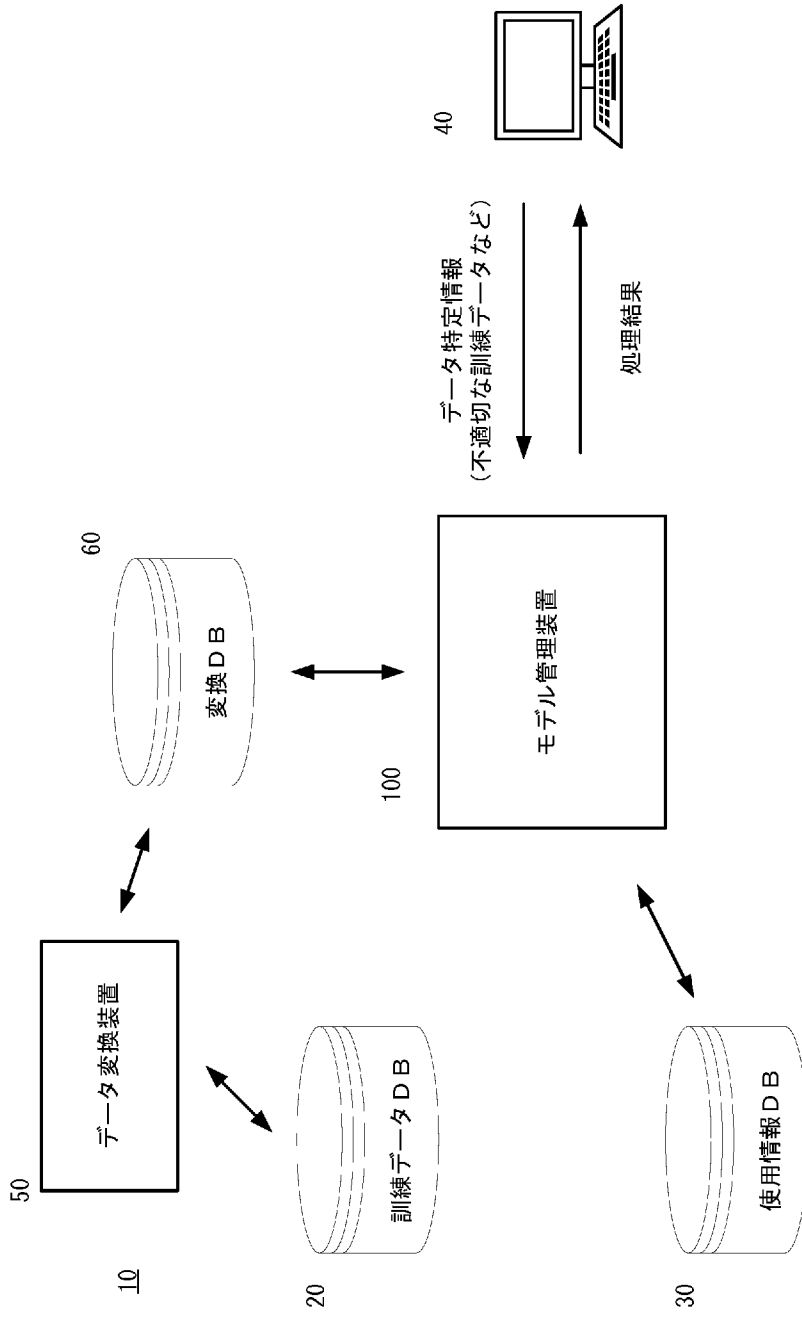
[図5]

モデルインデックス	データインデックス
#X1	#001
#X1	#004
#X1	#006
#X1	#008
...	...
#X2	#002
#X2	#003
#X2	#005
#X2	#007
#X2	#009
...	...

[図6]



[図7]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/016453

A. CLASSIFICATION OF SUBJECT MATTER		
<i>G06N 20/00</i> (2019.01)i; <i>G06F 21/62</i> (2013.01)i FI: G06N20/00; G06F21/62 345		
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) G06N3/00-99/00; G06F16/00-16/958; G06F21/60-21/64; G06T7/00; G06V10/70-10/86		
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 1971-2023 Registered utility model specifications of Japan 1996-2023 Published registered utility model applications of Japan 1994-2023		
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.
A	WO 2020/202731 A1 (SONY CORP) 08 October 2020 (2020-10-08) abstract, paragraphs [0097]-[0102], [0125]-[0134], [0200]-[0206], [0225]-[0237], fig. 13	1-8
A	JP 2022-64214 A (BLUEBOOKS CO LTD) 25 April 2022 (2022-04-25) abstract, paragraphs [0005]-[0012], [0091]-[0110], [0137]-[0139], [0144]-[0156], fig. 1, 12-13, 24-25	1-8
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
<p>* Special categories of cited documents:</p> <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“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)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p> <p>“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</p> <p>“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</p> <p>“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</p> <p>“&” document member of the same patent family</p>		
Date of the actual completion of the international search 07 July 2023		Date of mailing of the international search report 18 July 2023
Name and mailing address of the ISA/JP Japan Patent Office (ISA/JP) 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915 Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No. PCT/JP2023/016453

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2020/202731 A1	08 October 2020	EP 3951665 A1 abstract, paragraphs [0097]- [0102], [0125]-[0134], [0200]- [0206], [0226]-[0238], fig. 13	
		US 2022/0172047 A1	
		CN 113632113 A	
<hr/>			
JP 2022-64214 A	25 April 2022	(Family: none)	
<hr/>			

A. 発明の属する分野の分類（国際特許分類（IPC）） G06N 20/00(2019.01)i; G06F 21/62(2013.01)i FI: G06N20/00; G06F21/62 345		
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）） G06N3/00-99/00; G06F16/00-16/958; G06F21/60-21/64; G06T7/00; G06V10/70-10/86 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 1971-2023年 日本国実用新案登録公報 1996-2023年 日本国登録実用新案公報 1994-2023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
A	WO 2020/202731 A1 (ソニー株式会社) 08.10.2020 (2020-10-08) 要約, 段落[0097]-[0102], [0125]-[0134], [0200]-[0206], [0225]-[0237], 図13	1-8
A	JP 2022-64214 A (株式会社ブルーブックス) 25.04.2022 (2022-04-25) [要約], 段落[0005]-[0012], [0091]-[0110], [0137]-[0139], [0144]-[0156], 図1, 12-13, 24-25	1-8
<input type="checkbox"/> C欄の続きにも文献が列挙されている。 <input checked="" type="checkbox"/> 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	07.07.2023	国際調査報告の発送日 18.07.2023
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） 多賀 実 5B 9367 電話番号 03-3581-1101 内線 3545	

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2023/016453

引用文献			公表日	パテントファミリー文献			公表日
WO	2020/202731	A1	08.10.2020	EP	3951665	A1	
				要約, 段落[0097]-[0102], [0125]-[0134], [0200]- [0206], [0226]-[0238], 図 13			
				US	2022/0172047	A1	
				CN	113632113	A	

JP	2022-64214	A	25.04.2022	(ファミリーなし)			
