

(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
2022年12月22日(22.12.2022)



(10) 国際公開番号

WO 2022/264372 A1

(51) 国際特許分類:

G09C 1/00 (2006.01)

(21) 国際出願番号: PCT/JP2021/023077

(22) 国際出願日: 2021年6月17日(17.06.2021)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 日本電信電話株式会社 (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目5番1号 Tokyo (JP).

(72) 発明者: 高橋 慧 (TAKAHASHI, Satoshi); 〒1808585 東京都武蔵野市緑町三丁目9番1号 NTT 知的財産センタ内 Tokyo (JP).

長谷川 聡(HASEGAWA, Satoshi); 〒1808585 東京都武蔵野市緑町三丁目9番11号 NTT 知的財産センタ内 Tokyo (JP). 三浦 亮之(MIURA, Takayuki); 〒1808585 東京都武蔵野市緑町三丁目9番11号 NTT 知的財産センタ内 Tokyo (JP).

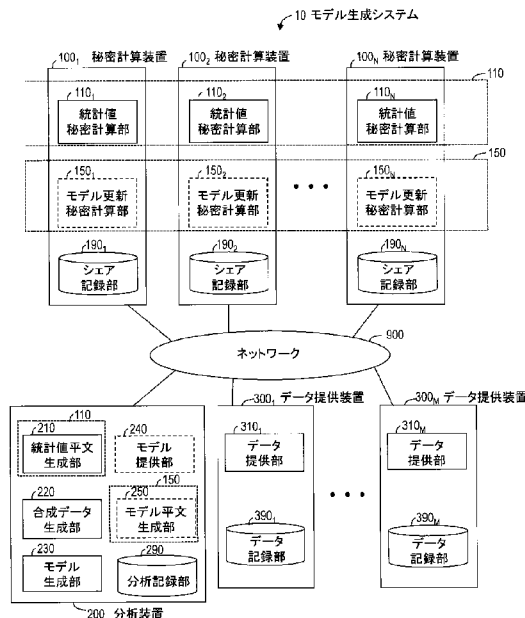
(74) 代理人: 中尾 直樹, 外 (NAKAO, Naoki et al.); 〒1600022 東京都新宿区新宿三丁目1番22号 新宿NSビル6階 Tokyo (JP).

(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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,

(54) Title: MODEL GENERATION SYSTEM, SECURE COMPUTATION DEVICE, ANALYSIS DEVICE, MODEL GENERATION METHOD, AND PROGRAM

(54) 発明の名称: モデル生成システム、秘密計算装置、分析装置、モデル生成方法、プログラム

[図1]



10 Model generation system

100-1, 100-2, 100-N Secure computation device

110-1, 110-2, 110-3 Statistic value secure computation unit

150-1, 150-2, 150-N Model update secure computation unit

190-1, 190-2, 190-N Share recording unit

200 Analysis device

210 Statistic value plain text generation unit

220 Synthetic data generation unit

230 Model generation unit

240 Model provision unit

250 Model plain text generation unit

290 Analysis recording unit

300, 300-M Data provision device

310-1, 310-M Data provision unit

390-1, 390-M Data recording unit

900 Network

(57) Abstract: A model generation system according to the present invention is provided with a statistic value secure computation means, a synthetic data generation unit, and a model generation unit. N is a predetermined integer of 3 or greater. The statistic value secure computation means receives input of predetermined N shares of data, obtains a prescribed statistic value by using secure computation, and outputs plain text of the statistic value. The synthetic data generation unit generates synthetic data that is pseudo-data exhibiting a statistic value identical to the statistic value. The model generation

[続葉有]

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, 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))

unit generates a prediction model by using the synthetic data.

(57) 要約：本発明のモデル生成システムは、統計値秘密計算手段、合成データ生成部、モデル生成部を備える。Nはあらかじめ定めた3以上の整数とする。統計値秘密計算手段は、あらかじめ定めたデータのN個のシェアを入力とし、所定の統計値を、秘密計算を用いて求め、統計値の平文を出力する。合成データ生成部は、前記統計値と同じ統計値となる疑似のデータである合成データを生成する。モデル生成部は、合成データを用いて予測モデルを生成する。

明 細 書

発明の名称：

モデル生成システム、秘密計算装置、分析装置、モデル生成方法、プログラム

技術分野

[0001] 本発明は、分析者に機密情報を開示することなく分析を行うためのモデル生成システム、秘密計算装置、分析装置、モデル生成方法、プログラムに関する。

背景技術

[0002] データの流通、活用が活発になった環境では、複数の組織が有するデータを連携させ、各組織の垣根をなくした上でAI（Artificial Intelligence）、回帰分析などを用いた予測モデルが構築されることなどが期待される。その際には、各組織間での情報漏洩を防ぐ手段として、非特許文献1，2に開示された秘密計算技術の活用が着目されている。また、データ活用の別のアプローチとして、非特許文献3に開示されたデータから生成される統計値を入力として擬似データを生成する匿名合成データ生成技術という手法も知られている。

先行技術文献

非特許文献

[0003] 非特許文献1：三品気吹，濱田浩気，五十嵐大，” 平文上の処理ロジックを再現した秘密計算ディープラーニング”，FIT2019(第18回情報科学技術フォーラム)，第2分冊，pp.81-88（2019）。

非特許文献2：五十嵐大，濱田浩気，菊池亮，千田浩司，” 超高速秘密計算ソートの設計と実装：秘密計算がスクリプト言語に並ぶ日”，CSS2017，pp.600-607（2017）。

非特許文献3：岡田莉奈，正木彰伍，長谷川聡，田中哲士，” 統計値を用いたプライバシー保護擬似データ生成手法”，CSS2017，pp.1366-1372(2017)。

発明の概要

発明が解決しようとする課題

[0004] しかしながら、非特許文献 1, 2 に示された秘密計算技術をすべての処理に適用すると処理コストが大きくなるという問題がある。また、匿名合成データ生成技術において、複数組織のデータを連携して合成データを生成するためには、平文でデータを取得し、各組織が有するデータを結合したテーブルを生成したうえで、必要な統計値を求める必要がある。本発明は、このような問題に鑑みてなされたものであり、データの機密性を維持しながら処理コストを抑えた予測モデルの生成技術を提供することを目的とする。

課題を解決するための手段

[0005] 本発明のモデル生成システムは、統計値秘密計算手段、合成データ生成部、モデル生成部を備える。N はあらかじめ定めた 3 以上の整数とする。統計値秘密計算手段は、あらかじめ定めたデータの N 個のシェアを入力とし、所定の統計値を、秘密計算を用いて求め、統計値の平文を出力する。合成データ生成部は、前記統計値と同じ統計値となる疑似のデータである合成データを生成する。モデル生成部は、合成データを用いて予測モデルを生成する。

発明の効果

[0006] 本発明のモデル生成システムによれば、統計値秘密計算手段への入力、データのシェアなので、データ自体を秘匿化できる。また、統計値秘密計算手段は統計値を平文で出力し、合成データの生成、予測モデルの生成は平文で行うので、処理コストを抑制できる。

図面の簡単な説明

[0007] [図1] 本発明のモデル生成システムの機能構成例を示す図。

[図2] データ提供装置が記録しているデータのシェアを秘密分散する処理フローを示す図。

[図3] 予測モデルを生成する処理フローを示す図。

[図4] 分析装置が記録している予測モデルのシェアと、データ提供装置が記録

しているデータのシェアを秘密分散する処理フローを示す図。

[図5]予測モデルを更新する処理フローを示す図。

[図6]コンピュータの機能構成例を示す図。

発明を実施するための形態

[0008] 以下、本発明の実施の形態について、詳細に説明する。なお、同じ機能を有する構成部には同じ番号を付し、重複説明を省略する。

実施例 1

[0009] <予測モデル生成>

図1に本発明のモデル生成システムの機能構成例を示す。図2は、データ提供装置が記録しているデータのシェアを秘密分散する処理フローを示す図である。図3は、予測モデルを生成する処理フローを示す図である。以下の説明では、 N はあらかじめ定めた3以上の整数、 n は1以上 N 以下の整数、 K はあらかじめ定めた2以上 N 以下の整数、 M は1以上の整数、 m は1以上 M 以下の整数とする。

[0010] モデル生成システム10は、ネットワーク900を介して内部または外部に存在するデータ提供装置300₁, ..., 300_Mと接続されている。データ提供装置300_mは、データを記録したデータ記録部390_mとデータ提供部310_mを備える。データ提供装置300_mは、データを提供する組織（企業、行政など）が保有するデータベースなどであり、データはデータ記録部390_mに記録されている。データ提供部310_mは、 N 個のシェアを生成し、モデル生成システム10にシェアを提供する（S311_m）。「シェア」とはデータの断片であり、 K 個以上のシェアを取得するとデータを復元できるが、 K 個未満のシェアからではデータは復元できない（秘密は漏れない）という特徴を有する。シェアに関する詳細は、非特許文献1, 2などに示されている。

[0011] モデル生成システム10は、ネットワーク900を介して接続された秘密計算装置100₁, ..., 100_Nと分析装置200を備える。秘密計算装置100_nは、統計値秘密計算部110_n, シェア記録部190_nを備える。統計値

秘密計算部 110_nは、あらかじめ定めたデータのN個のシェアの1つを入力とし、他の秘密計算装置 100₁, ..., 100_Nと協調した秘密計算によって、所定の統計値のシェアの1つを求める。秘密計算技術に関する詳細は、非特許文献 1, 2 などに示されている。シェア記録部 190_nは、データ提供装置 300₁, ..., 300_Mから取得したシェア、統計値秘密計算部 110_nが求めた統計値のシェアなどを記録する。図 2 に示すように、モデル生成システム 10 が予測モデルを生成する際は、予測モデル生成に必要なデータを保有するデータ提供装置 300_mがN個のシェアを生成し、モデル生成システム 10 にシェアを提供する (S 311_m)。秘密計算装置 100_nは、データのN個のシェアの中の1つを取得し、シェア記録部 190_nに記録する (S 101_n)。より具体的には、データ提供装置 300₁, ..., 300_Mが、1つ1つのシェアを秘密計算装置 100₁, ..., 100_Nに個別に送信すれば、データを秘匿化できる。ただし、秘匿化できるのであれば、データ提供部 310_mは、データ提供装置 300_mの外部に存在してもよい。

[0012] 分析装置 200 は、統計値平文生成部 210, 合成データ生成部 220, モデル生成部 230, 分析記録部 290 を備える。統計値平文生成部 210 は、秘密計算を用いて求めた所定の統計値のシェアをK個以上取得し、所定の統計値の平文を生成する (S 210)。合成データ生成部 220 は、前記統計値と同じ統計値となる疑似のデータである合成データを生成する (S 220)。モデル生成部 230 は、合成データを用いて予測モデルを生成する (S 230)。なお、分析装置 200 は、図 1 では秘密計算装置 100₁, ..., 100_Nとは別の装置として示しているが、いずれかの秘密計算装置 100_nが分析装置 200 を兼ねてもよい。

[0013] 図 1 と図 3 を参照しながら、予測モデルを生成する処理フローを説明する。モデル生成システム 10 は、統計値秘密計算手段 110、合成データ生成部 220、モデル生成部 230 を備える。合成データ生成部 220 とモデル生成部 230 は、分析装置 200 が備えている。統計値秘密計算手段 110 は、各秘密計算装置 100₁, ..., 100_Nが備える統計値秘密計算部 110₁

, ..., 110_N と分析装置200が備える統計値平文生成部210で構成される。統計値秘密計算手段110は、あらかじめ定めたデータのN個のシェアを入力とし、所定の統計値を、秘密計算を用いて求め、統計値の平文を出力する(S110)。より具体的には、統計値秘密計算部 110_n は、あらかじめ定めたデータのN個のシェアの1つを入力とし、他の秘密計算装置 100_1 , ..., 100_N の統計値秘密計算部 110_1 , ..., 110_N と協調した秘密計算によって、所定の統計値のシェアの1つを求める($S110_1$, ..., 110_N)。「統計値」とは、属性ごとの平均、分散共分散などとすればよいが、これらに限定されない。予測モデル生成に必要な統計値を適宜選べばよい。統計値平文生成部210は、秘密計算を用いて求めた所定の統計値のシェアをK個以上取得し、所定の統計値の平文を生成する(S210)。ステップ 110_1 , ..., 110_N とS210で、統計値秘密計算ステップ(S110)は構成される。

[0014] 合成データ生成部220が、統計値平文生成部210が出力した統計値と同じ統計値となる疑似のデータである合成データを生成する(S220)。モデル生成部230は、合成データを用いて予測モデルを生成する(S230)。合成データの生成(S220)は、非特許文献3に示された技術を利用すればよい。予測モデルの生成(S230)は、既存の技術を利用すればよい。例えば、予測モデルは、合成データを教師データとして学習した学習済みモデルでもよいし、回帰分析によって得られたモデルでもよい。予測したい事象に応じて予測モデルは適宜選択すればよい。

[0015] モデル生成システム10によれば、統計値秘密計算手段110への入力、データのシェアなので、データ自体を秘匿化できる。また、統計値秘密計算手段110は統計値を平文で出力し、合成データの生成、予測モデルの生成は平文で行うので、処理コストを抑制できる。さらに、秘密計算技術を利用する演算を少なくしているので、秘密計算技術で実施可能な演算の制限を受けにくくできる。

[0016] 例えば、データ提供装置 300_1 が、個人を特定する識別子(例えば、個人

を特定する番号など)と購買額のデータを保有し、データ提供装置300₂が、個人を特定する識別子と性別のデータを保有しているとする。秘密計算装置100₁, ..., 100_Nが、データ提供装置300₁から識別子と購買額のシェアを取得し、データ提供装置300₂から識別子と性別のシェアを取得する(S311₁, S311₂, S101₁, ..., S101_N)。そして、統計値秘密計算部110₁, ..., 110_Nが、秘密計算をもちいて、男性に限定した購買額の統計値のシェアと女性に限定した購買額の統計値のシェアを計算する(S110₁, ..., S110_N)。統計値平文生成部210は、秘密計算を用いて求めた性別ごとの統計値のシェアをK個以上取得し、性別ごとの統計値の平文を生成する(S210)。合成データ生成部220は、生成した統計値と同じ統計値となる疑似のデータである合成データを生成する(S220)。モデル生成部230は、合成データを用いて予測モデルを生成する(S230)。データ提供装置300₁のデータとデータ提供装置300₂のデータとを連携させることで性別ごとの予測モデルを生成できるので、データ提供装置300₁のデータだけの予測モデルよりも予測の精度を向上できる。

[0017] <予測モデル更新>

図4は、分析装置が記録している予測モデルのシェアと、データ提供装置が記録しているデータのシェアを秘密分散する処理フローを示す図である。図5は、予測モデルを更新する処理フローを示す図である。予測モデルの更新を行う場合は、秘密計算装置100_nは、モデル更新秘密計算部150_nも備える、また、分析装置200は、モデル提供部240とモデル平文生成部250も備える。

[0018] モデル提供部240は、既存の予測モデル(分析記録部290が記録している予測モデル)に関する情報を秘密計算装置100₁, ..., 100_Nに送信する(S240)。「予測モデルに関する情報」とは、予測モデル自体でもよいし、予測モデルのN個のシェアの中の1つでもよい。また、予測モデル生成に必要な追加データを保有するデータ提供装置300_mが追加データのN個のシェアを生成し、モデル生成システム10にシェアを提供する(S31

2_m)。秘密計算装置100_nは、予測モデルに関する情報と、追加データのN個のシェアの中の1つを取得し、シェア記録部190_nに記録する(S102_n)。データ提供装置300₁, ..., 300_Mが、1つ1つの追加データのシェアを秘密計算装置100₁, ..., 100_Nに個別に送信すれば、追加データを秘匿化できる。

[0019] モデル更新秘密計算部150_nは、予測モデルに関する情報と、あらかじめ定めた追加データのN個のシェアの1つを入力とし、他の秘密計算装置100₁, ..., 100_Nのモデル更新秘密計算部150₁, ..., 150_Nと協調した秘密計算によって、更新した予測モデルのシェアを求める(S150_n)。モデル平文生成部250は、秘密計算を用いて更新した予測モデルのシェアをK個以上取得し、更新された予測モデルの平文を生成する(S250)。モデル更新秘密計算手段150は、各秘密計算装置100₁, ..., 100_Nが備えるモデル更新秘密計算部150₁, ..., 150_Nと分析装置200が備えるモデル平文生成部250で構成される。モデル更新秘密計算手段150は、既存の予測モデルと、あらかじめ定めた追加データのN個のシェアを入力とし、秘密計算を用いて、予測モデルを更新する(S150)。ステップ150₁, ..., 150_NとS250で、モデル更新秘密計算ステップ(S150)は構成される。より具体的には、非特許文献1に示されたアルゴリズムなどにより更新すればよい。もしくは、データを追加した回帰分析などにより予測モデルを更新すればよい。

[0020] モデル生成システム10によれば、モデル更新秘密計算手段150への入力、追加データのシェアなので、追加データ自体を秘匿化しながら、予測モデルを更新できる。また、予測モデル生成の処理では、データ自体の秘匿化と、処理コストの抑制を得られる。ただし、予測モデルの更新に必要な計算は、秘密計算技術で実行可能な計算に制限される。

[0021] 例えば、データ提供装置300₁が、個人を特定する識別子(例えば、個人を特定する番号など)と購買額のデータを保有し、データ提供装置300₂が、個人を特定する識別子と性別のデータを保有している。そして、予測モデ

ル生成の処理フローで生成された男性用の予測モデルと女性用の予測モデルが存在するとし、データ提供装置300₁は、予測モデル生成後に取得した個人を特定する識別子と購買額の追加データを保有し、データ提供装置300₂は、個人を特定する識別子と性別の追加データを保有しているとする。秘密計算装置100₁, ..., 100_Nが、データ提供装置300₁から識別子と購買額の追加データのシェアを取得し、データ提供装置300₂から識別子と性別の追加データのシェアを取得する(S312₁, S312₂, S102₁, ..., S102_N)。そして、モデル更新秘密計算部150₁, ..., 150_Nが、秘密計算をもちいて、男性に限定した購買額の予測モデルのシェアと女性に限定した購買額の予測モデルのシェアを計算する(S150₁, ..., S150_N)。モデル平文生成部250は、秘密計算を用いて更新した性別ごとの予測モデルのシェアをK個以上取得し、更新された性別ごとの予測モデルの平文を生成する(S250)。データ提供装置300₁の追加データとデータ提供装置300₂の追加データとを連携させることで、性別ごとの予測モデルを追加データで更新できるので、予測の精度を向上できる。

[0022] [プログラム、記録媒体]

上述の各種の処理は、図6に示すコンピュータ2000の記録部2020に、上記方法の各ステップを実行させるプログラムを読み込ませ、制御部2010、入力部2030、出力部2040、表示部2050などに動作させることで実施できる。

[0023] この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等のようなものでもよい。

[0024] また、このプログラムの流通は、例えば、そのプログラムを記録したDVD、CD-ROM等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータ

にそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

[0025] このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理の実行時、このコンピュータは、自己の記録媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、このコンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。また、サーバコンピュータから、このコンピュータへのプログラムの転送は行わず、その実行指示と結果取得のみによって処理機能を実現する、いわゆるASP (Application Service Provider) 型のサービスによって、上述の処理を実行する構成としてもよい。なお、本形態におけるプログラムには、電子計算機による処理の用に供する情報であってプログラムに準ずるもの（コンピュータに対する直接の指令ではないがコンピュータの処理を規定する性質を有するデータ等）を含むものとする。

[0026] また、この形態では、コンピュータ上で所定のプログラムを実行させることにより、本装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

符号の説明

[0027] 10	モデル生成システム	100 _n	秘密計算装置
110	統計値秘密計算手段	110 _n	統計値秘密計算部
150	モデル更新秘密計算手段	150 _n	モデル更新秘密計算部
190 _n	シェア記録部	200	分析装置
210	統計値平文生成部	220	合成データ生成部
230	モデル生成部	240	モデル提供部

250 モデル平文生成部

300_m データ提供装置

390_m データ記録部

290 分析記録部

310_m データ提供部

900 ネットワーク

請求の範囲

[請求項1]

Nはあらかじめ定めた3以上の整数とし、

あらかじめ定めたデータのN個のシェアを入力とし、所定の統計値を、秘密計算を用いて求め、前記統計値の平文を出力する統計値秘密計算手段と、

前記統計値と同じ統計値となる疑似のデータである合成データを生成する合成データ生成部と、

前記合成データを用いて予測モデルを生成するモデル生成部とを備えるモデル生成システム。

[請求項2]

請求項1記載のモデル生成システムであって、

既存の予測モデルに関する情報と、あらかじめ定めた追加データのN個のシェアとを入力とし、秘密計算を用いて、前記予測モデルを更新するモデル更新秘密計算手段

も備えるモデル生成システム。

[請求項3]

請求項2記載のモデル生成システムに含まれる複数の秘密計算装置の1つであって、

前記あらかじめ定めたデータのN個のシェアの1つを入力とし、他の秘密計算装置と協調した秘密計算によって、前記所定の統計値のシェアの1つを求める統計値秘密計算部と、

既存の予測モデルに関する情報と、前記あらかじめ定めた追加データのN個のシェアの1つとを入力とし、他の秘密計算装置と協調した秘密計算によって、前記予測モデルを更新した予測モデルのシェアを求めるモデル更新秘密計算部

を備える秘密計算装置。

[請求項4]

請求項1または2記載のモデル生成システムに含まれる分析装置であって、

Kはあらかじめ定めた2以上N以下の整数とし、

秘密計算を用いて求めた前記所定の統計値のシェアをK個以上取得

し、前記所定の統計値の平文を生成する統計値平文生成部と、
前記合成データ生成部と、前記モデル生成部と
を備える分析装置。

[請求項5] 請求項4記載の分析装置であって、
予測モデルのN個のシェアを生成するモデル提供部と、
秘密計算を用いて更新した前記予測モデルのシェアをK個以上取得
し、前記予測モデルの平文を生成するモデル平文生成部と、
を備える分析装置。

[請求項6] Nはあらかじめ定めた3以上の整数とし、
あらかじめ定めたデータのN個のシェアを入力とし、所定の統計値
を、秘密計算を用いて求め、前記統計値の平文を出力する統計値秘密
計算ステップと、
前記統計値と同じ統計値となる疑似のデータである合成データを生
成する合成データ生成ステップと、
前記合成データを用いて予測モデルを生成するモデル生成ステップ
と
を実行するモデル生成方法。

[請求項7] 請求項6記載のモデル生成方法であって、
既存の予測モデルに関する情報と、あらかじめ定めた追加データの
N個のシェアとを入力とし、秘密計算を用いて、前記予測モデルを更
新するモデル更新秘密計算ステップ
も実行するモデル生成方法。

[請求項8] 請求項3記載の秘密計算装置、もしくは請求項4または請求項5記
載の分析装置としてコンピュータを機能させるためのプログラム。

[図1]

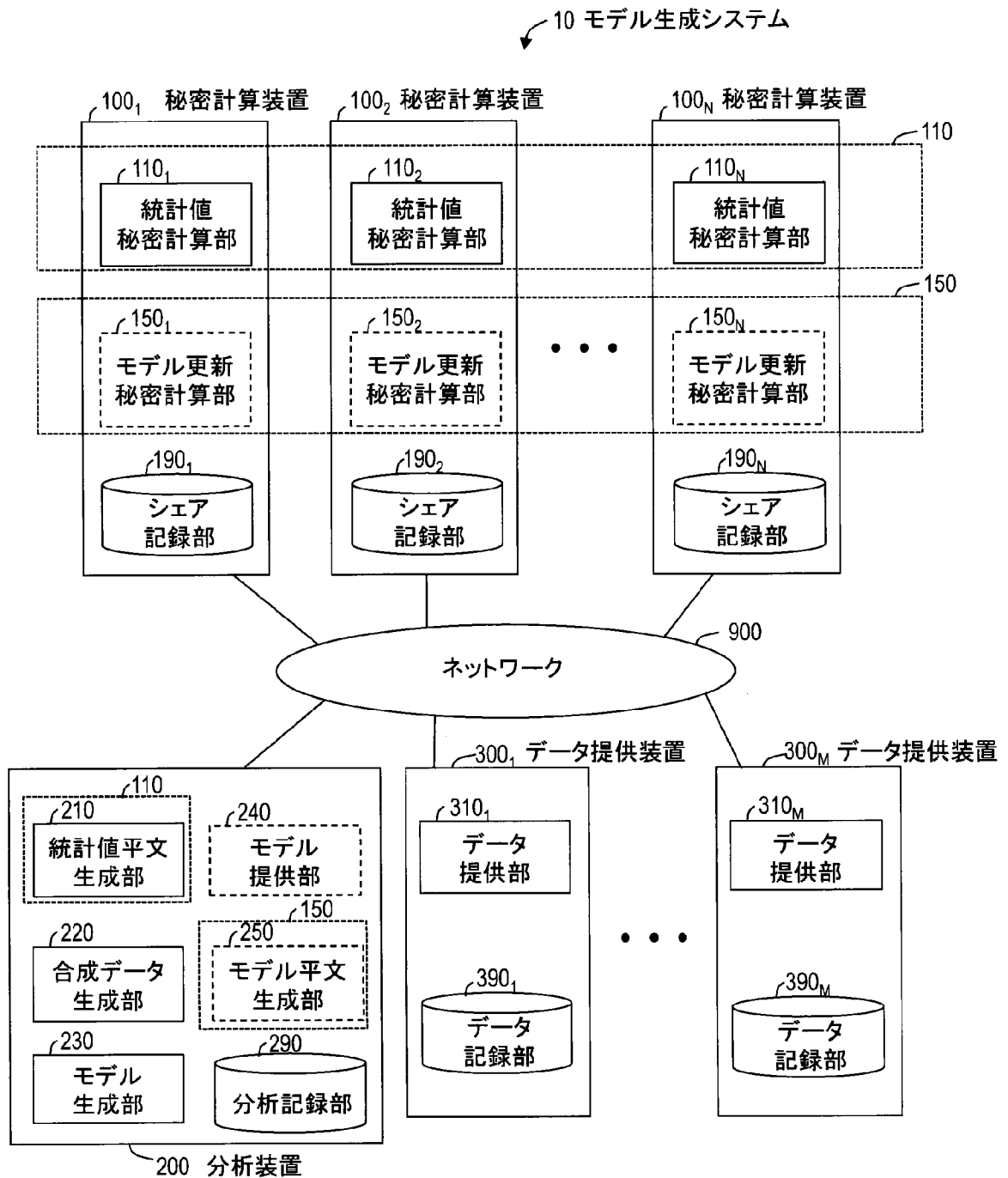


図1

[図2]

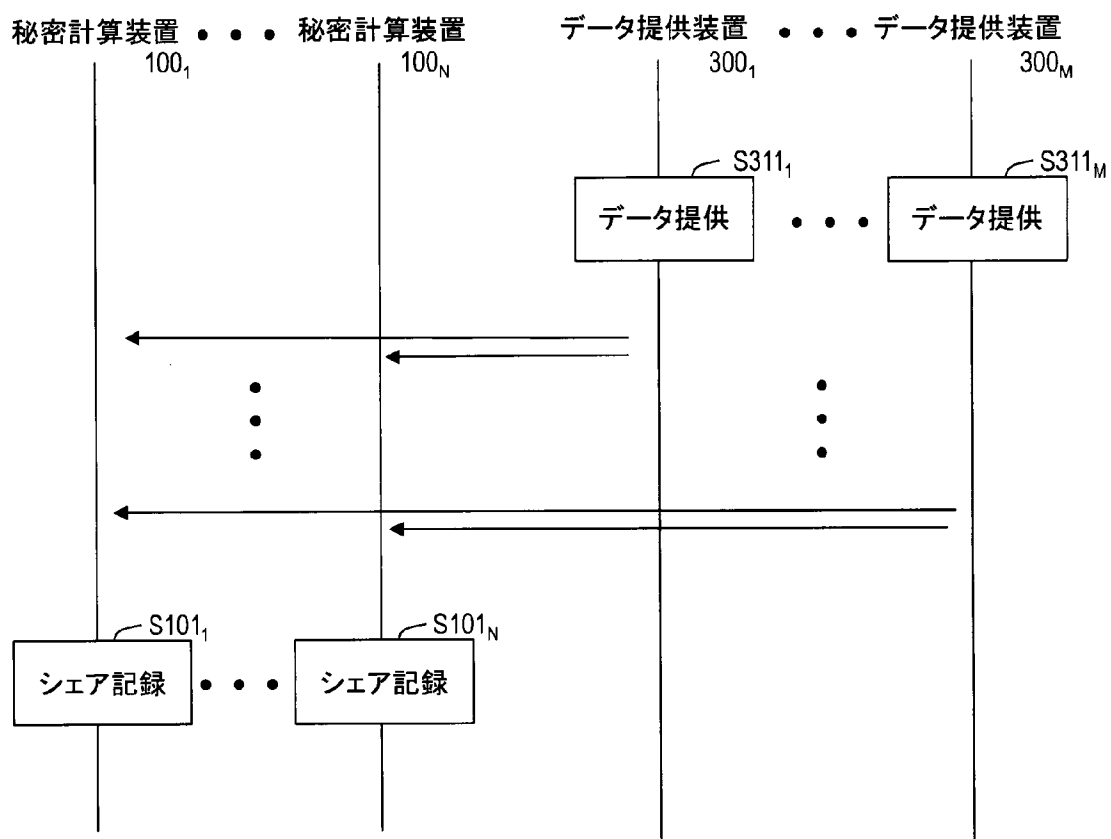


図2

[図3]

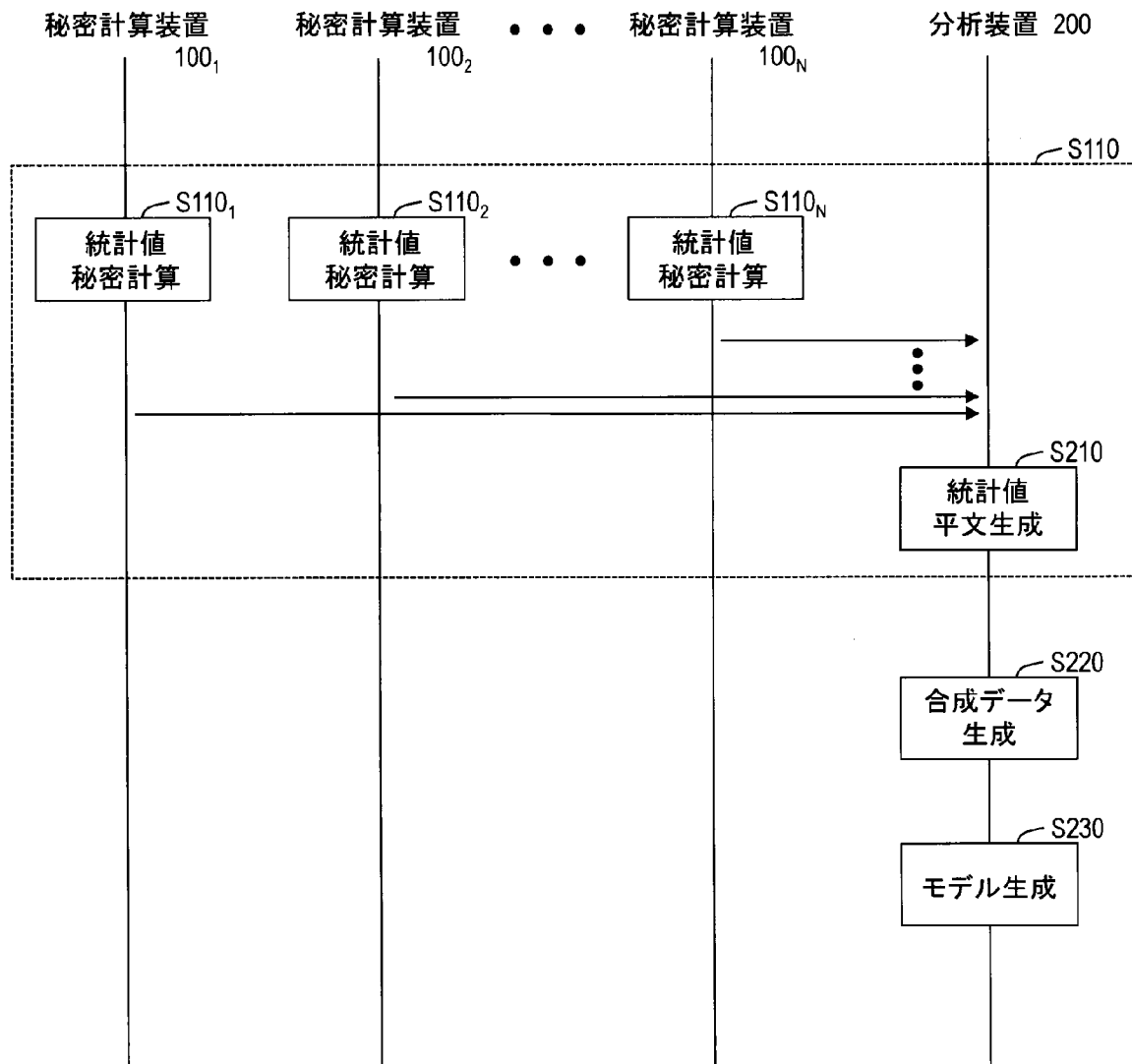


図3

[図4]

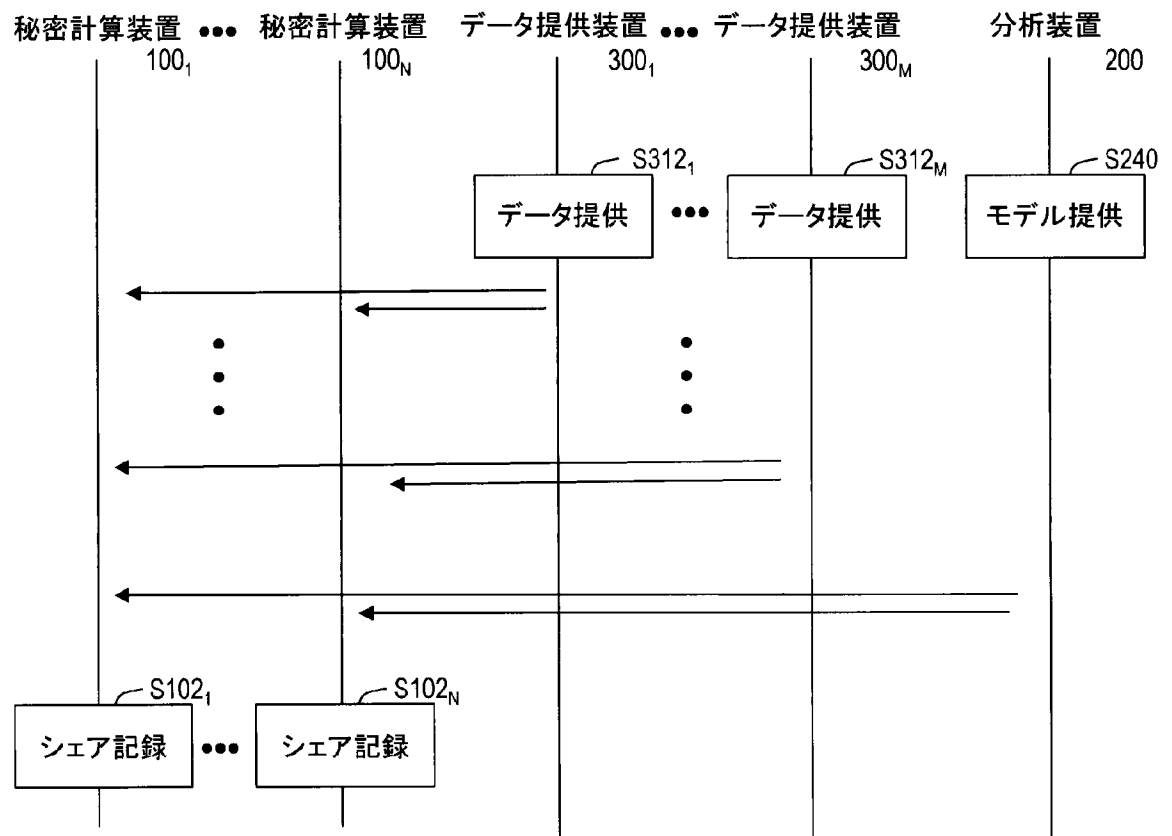


図4

[図5]

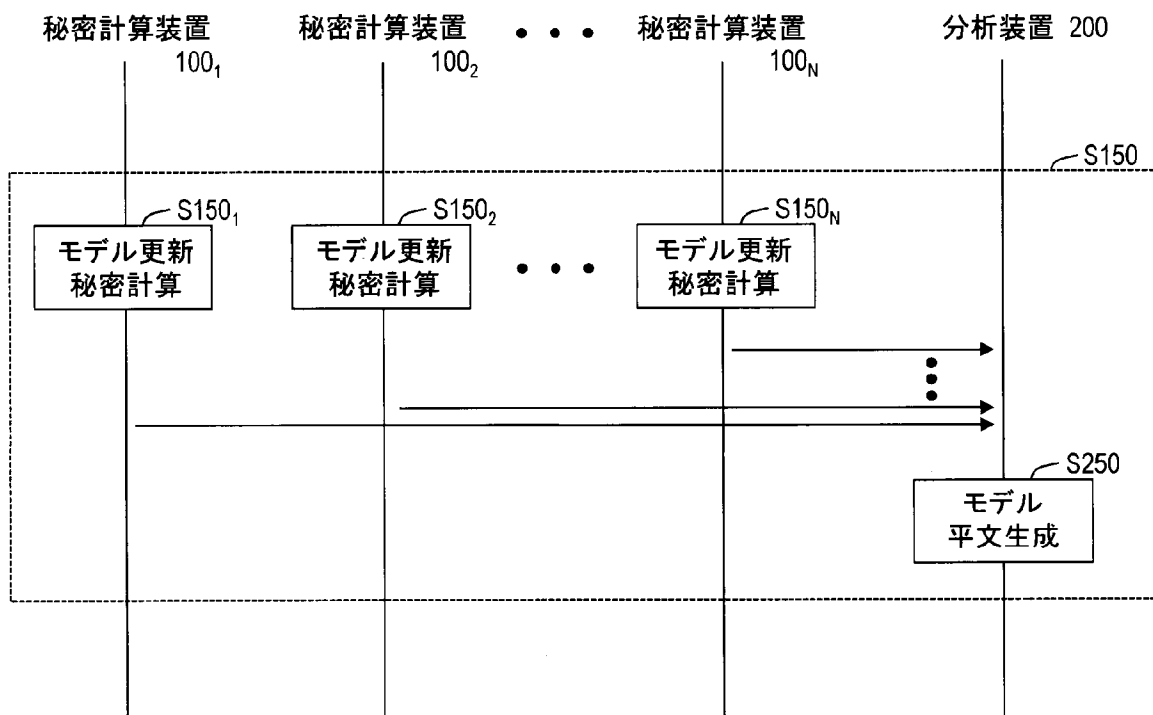


図5

[図6]

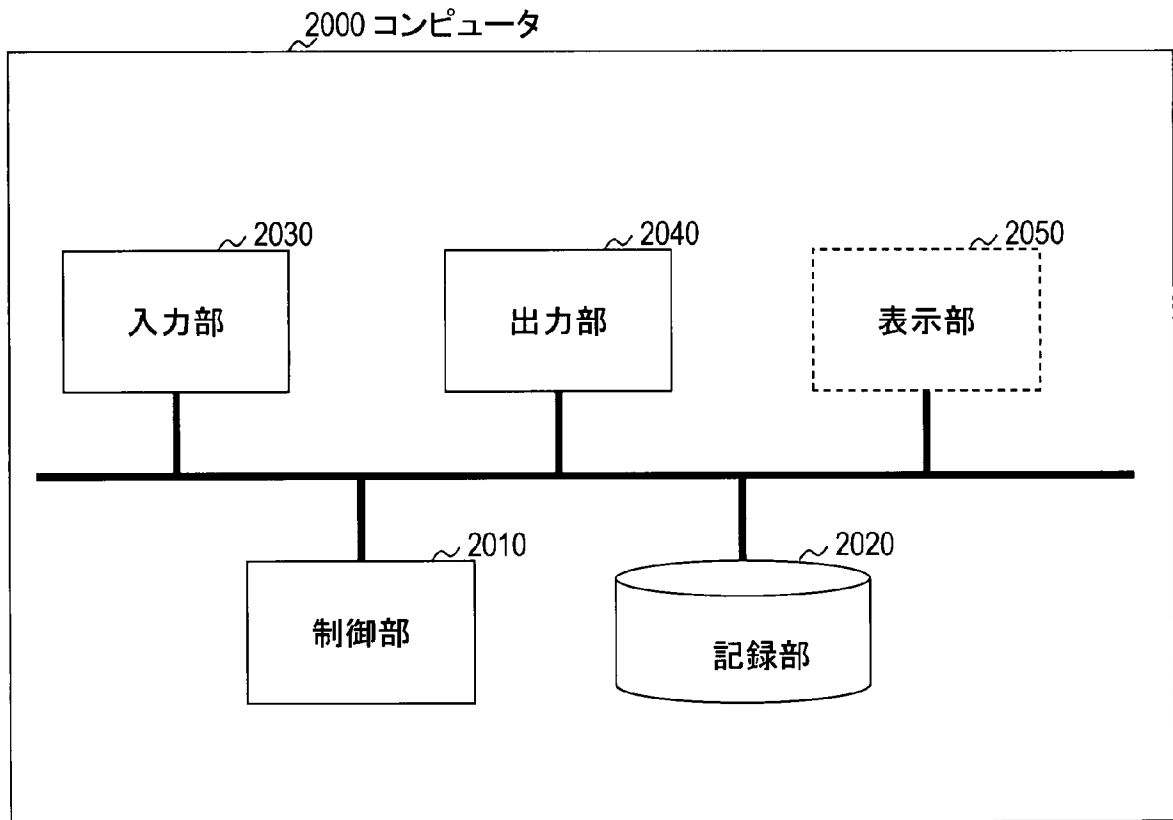


図6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/023077

A. CLASSIFICATION OF SUBJECT MATTER

G09C 1/00(2006.01)i

FI: G09C1/00 650Z

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)

G09C1/00

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.
Y	岡田 莉奈 ほか, 統計値を用いたプライバシー保護疑似データ生成手法, コンピュータセキュリティシンポジウム2017 論文集, 一般社団法人情報処理学会, 16 October 2017, pp. 1366-1372, in particular, page 1367, left column, line 9 to right column, line 2, page 1371, left column, lines 6-14, etc., (OKADA, Rina et al. Privacy Preserved Synthetic Datasets Generation by Using Statistics.), non-official translation (Proceedings of Computer Security Symposium 2017. Information Processing Society of Japan.)	1-8



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
03 September 2021 (03.09.2021)Date of mailing of the international search report
14 September 2021 (14.09.2021)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/JP2021/023077

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	五十嵐 大 ほか , 軽量検証可能 3 パーティ秘関関数計算の効率化及びこれを用いたセキュアなデータベース処理 , 2011 年 暗号と情報セキュリティシンポジウム概要集 , 25 January 2011, pp. 1-8, in particular, page 1, left column, lines 1-19, page 1, right column, line 12 to page 2, left column, line 10, page 7, left column, line 18 to page 8, right column, line 4, etc. non-official translation (IGARASHI, Dai et al. Efficient three-party secure function evaluation that enables lightweight detection and secure database processing using this. Summaries of the Symposium on Cryptography and Information Security 2011.)	1-8
Y	宮島 洋文 ほか , セキュアマルチパーティ計算によるエッジシステム上の BP 学習法の提案 , 情報処理学会 研究報告 マルチメディア通信と分散処理(DPS), 14 December 2020, vol. 2020-DPS-185, no. 13, pp. 1-7, in particular, page 1, right column, lines 20-26, page 2, left column, lines 24-38, page 2, left column, line 41 to page 2, right column, line 13, page 3, right column, line 27 to page 5, right column, line 11, table 2, fig. 1, etc., (MIYAJIMA, Hirofumi et al. Proposal of BP learning with IoT using Secure Multiparty Computation. IPSJ Technical Report: Distributed Processing System (DPS).)	2-3, 5, 7

A. 発明の属する分野の分類（国際特許分類（IPC）） G09C 1/00(2006.01)i FI: G09C1/00 650Z														
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）） G09C1/00 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2021年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2021年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2021年</td> </tr> </table> 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）			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				
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													
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												
Y	岡田 莉奈 ほか、統計値を用いたプライバシー保護擬似データ生成手法、コンピュータセキュリティシンポジウム2017 論文集、一般社団法人情報処理学会、2017.10.16, pp.1366-1372 特に第1367頁左側欄第9行目-右側欄第2行目、第1371頁左側欄6-14行目等	1-8												
Y	五十嵐 大 ほか、軽量検証可能3パーティ秘匿関数計算の効率化及びこれを用いたセキュアなデータベース処理、2011年 暗号と情報セキュリティシンポジウム概要集、2011.01.25, pp.1-8 特に第1頁左側欄第1-19行目、第1頁右側欄12行目-第2頁左側欄第10行目、第7頁左側欄第18行目-第8頁右側欄第4行目等	1-8												
Y	宮島 洋文 ほか、セキュアマルチパーティ計算によるエッジシステム上のBP学習法の提案、情報処理学会 研究報告 マルチメディア通信と分散処理（DPS）, 2020.12.14, Vol. 2020-DPS-185 No. 13, pp.1-7 特に第1頁右側欄第20-26行目、第2頁左側欄第24-38行目、第2頁左側欄41行目-第2頁右側欄第13行目、第3頁右側欄第27行目-第5頁右側欄第11行目、表2、図1等	2-3, 5, 7												
☐ 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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“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	“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	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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													
“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	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日 03.09.2021	国際調査報告の発送日 14.09.2021													
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） 児玉 崇晶 5S 3651 電話番号 03-3581-1101 内線 3546													