(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29日(29.12.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/269743 A1

(51) 国際特許分類:
G06Q 30/02 (2012.01)

(21) 国際出願番号： PCT/JP2021/023551

(22) 国際出願日： 2021年6月22日(22.06.2021)

(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: 森山 敏行 (**MORIYAMA, Toshiyuki**); 〒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). 瀧野 修(**TAKINO, Osamu**); 〒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). 太田 賢治(**OTA, Kenji**); 〒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). 高橋 慧(**TAKAHASHI, 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).

(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ＮＳＯ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,

(54) **Title:** SECURE COMPUTATION DEVICE, PURCHASE PREDICTION SYSTEM, SECURE COMPUTATION METHOD, AND PROGRAM

(54) 発明の名称： 秘密計算装置、購買予測システム、秘密計算方法、プログラム

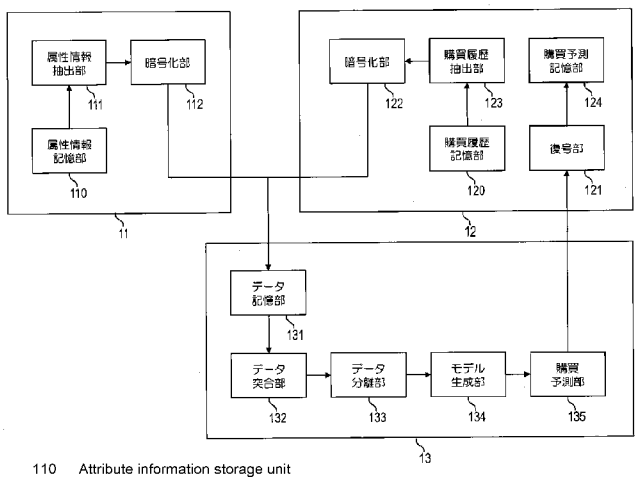


図2

110 Attribute information storage unit
111 Attribute information extraction unit
112, 122 Encryption unit
120 Purchase history storage unit
121 Decryption unit
123 Purchase history extraction unit
124 Purchase prediction storage unit
131 Data storage unit
132 Data reconciliation unit
133 Data separation unit
134 Model generation unit
135 Purchase prediction unit

(57) **Abstract:** This secure computation device comprises: a data reconciliation unit for reconciling ciphertexts of attribute information and ciphertexts of purchase history on the basis of a ciphertexts of user IDs by using secure computation processing; a data separation unit for extracting ciphertexts of user IDs corresponding to ciphertexts of attribute information that was not reconciled by using secure computation processing; a model generation unit for generating a predictive model on the basis of a supervised learning training dataset composed of ciphertexts of purchase history and ciphertexts

WO 2022/269743 A1

［続葉有］

CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, 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)）

of attribute information that was reconciled with the ciphertexts of the purchase history by using secure computation processing; and a purchase prediction unit for using secure computation processing to generate ciphertexts of purchase predictions on the basis of the ciphertexts of attribute information that was not reconciled and the predictive model, and transmits the ciphertexts of purchase predictions to a sales operator device.

(57) 要約：秘密計算装置は、秘密計算処理により、ユーザＩＤの暗号文に基づいて属性情報の暗号文と購買履歴の暗号文を突合するデータ突合部と、秘密計算処理により、突合されなかった属性情報の暗号文に対応するユーザＩＤの暗号文を抽出するデータ分離部と、秘密計算処理により、購買履歴の暗号文と、当該購買履歴の暗号文に突合された属性情報の暗号文からなる教師あり学習用データセットに基づいて予測モデルを生成するモデル生成部と、秘密計算処理により、突合されなかった属性情報の暗号文と予測モデルに基づいて、購買予測の暗号文を生成し、購買予測の暗号文を販売事業者装置に送信する購買予測部を含む。

明　細　書

発明の名称 ：

秘密計算装置、購買予測システム、秘密計算方法、プログラム

技術分野

[0001] 本発明は、データを秘匿したまま予測モデルを生成する秘密計算装置、購買予測システム、秘密計算方法、プログラムに関する。

背景技術

[0002] 従来、商品を販売する事業者（以降、販売事業者）が新商品を開発し市場に投入する場合、過去に自社商品を購入した購買履歴データをもとに分析などを行い、購買予測を立てている。

[0003] 特許文献１には、購買情報・商品属性情報・商品数情報から顧客別の商品属性に対する興味の値を計算し、購買が成功する確率を予測する手法が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特開２０１６－９１０８５号公報

発明の概要

発明が解決しようとする課題

[0005] 販売事業者は購買予測の精度を高めるために、保有している購買履歴データに不足している属性情報（購入者の性別・年代・年収等）を収集し、予測モデルを生成する必要があるが、プライバシーを守るために匿名加工されたり統計化されたデータしか取得できず、有用な購買予測を行えないことが予想される。

[0006] プライバシー保護の問題を解決できる秘密計算技術を販売事業者が導入し、属性情報を自ら入手し購買履歴を暗号化したまま計算することで安全に分析を行うことも可能ではあるが、属性情報の収集に膨大な稼働がかかると共に、平文に比べて秘密計算の処理に時間がかかるため、利用が進まないこと

が予想される。

[0007] そこで本発明では、個人の属性情報を秘匿したまま、精緻な予測モデルを生成することができる秘密計算装置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

[0008] 本発明の秘密計算装置は、データ記憶部と、データ突合部と、データ分離部と、モデル生成部と、購買予測部を含む。

[0009] データ記憶部は、データ保有者装置からユーザの属性情報とこれに対応するユーザＩＤを暗号化した暗号文を受信し、販売事業者装置からユーザの購買履歴とこれに対応するユーザＩＤを暗号化した暗号文を受信し、これらの暗号文を記憶する。データ突合部は、秘密計算処理により、ユーザＩＤの暗号文に基づいて属性情報の暗号文と購買履歴の暗号文を突合する。データ分離部は、秘密計算処理により、突合されなかった属性情報の暗号文に対応するユーザＩＤの暗号文を抽出する。モデル生成部は、秘密計算処理により、購買履歴の暗号文と、当該購買履歴の暗号文に突合された属性情報の暗号文からなる教師あり学習用データセットに基づいて予測モデルを生成する。購買予測部は、秘密計算処理により、突合されなかった属性情報の暗号文と予測モデルに基づいて、購買予測の暗号文を生成し、購買予測の暗号文を販売事業者装置に送信する。

発明の効果

[0010] 本発明の秘密計算装置によれば、個人の属性情報を秘匿したまま、精緻な予測モデルを生成することができる。

図面の簡単な説明

[0011] [図1]実施例１の購買予測システムの構成を示すシステム構成図。

[図2]実施例１の購買予測システムの各装置の機能構成を示すブロック図。

[図3]実施例１の購買予測システムの動作を示すシーケンス図。

[図4]秘密計算装置に送信される属性情報とユーザＩＤの暗号文を例示する図。

[図5]突合された属性情報と購買情報の暗号文の例を示す図。

[図6]生成される購買予測の暗号文の例を示す図。

[図7]実施例２の購買予測システムの構成を示すシステム構成図。

[図8]実施例２の購買予測システムの各装置の機能構成を示すブロック図。

[図9]実施例２の購買予測システムの動作を示すシーケンス図。

[図10]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

[0012] 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

[0013] 以下、データ保有者が持つユーザの属性情報と、販売事業者が持つユーザの購買履歴に基づいて生成される予測モデルにより、新たな購買候補ユーザを抽出する場面で用いられる実施例１の購買予測システムについて説明する。

[0014] 図１に示すように本実施例の購買予測システム１は、データ保有者装置１１と、販売事業者装置１２と、秘密計算装置１３を含み、各装置は通信可能にネットワークに接続されている。

[0015] 図２に示すように、データ保有者装置１１は、属性情報記憶部１１０と、属性情報抽出部１１１と、暗号化部１１２を含む。販売事業者端末１２は、購買履歴記憶部１２０と、復号部１２１と、暗号化部１２２と、購買履歴抽出部１２３と、購買予測記憶部１２４を含む。秘密計算装置１３は、データ記憶部１３１と、データ突合部１３２と、データ分離部１３３と、モデル生成部１３４と、購買予測部１３５を含む。

[0016] 以下、図３を参照して各構成要件の動作について説明する。

[0017] ＜データ保有者装置１１：属性情報記憶部１１０＞

属性情報記憶部１１０は、予めユーザの属性情報をユーザＩＤと対応付けて記憶している。

[0018] ＜属性情報抽出部１１１＞

属性情報抽出部１１１は、属性情報記憶部１１０から属性情報とユーザＩ

Ｄを抽出する（Ｓ１１１）。

[0019] ＜暗号化部１１２＞

暗号化部１１２は、抽出した属性情報とユーザＩＤを暗号化して秘密計算装置１３に送信する（Ｓ１１２）。図４に、秘密計算装置１３に送信される属性情報とユーザＩＤの暗号文の例を示す。なお、［＊］は、＊の暗号文を意味する。

[0020] ＜販売事業者装置１２：購買履歴記憶部１２０＞

購買履歴記憶部１２０は、予めユーザの購買履歴をユーザＩＤと対応付けて記憶している。

[0021] ＜購買履歴抽出部１２３＞

購買履歴抽出部１２３は、購買履歴記憶部１２０から購買履歴とユーザＩＤを抽出する（Ｓ１２３）。

[0022] ＜暗号化部１２２＞

暗号化部１２２は、抽出した購買履歴とユーザＩＤを暗号化して秘密計算装置１３に送信する（Ｓ１２２）。

[0023] ＜秘密計算装置１３：データ記憶部１３１＞

秘密計算装置１３のデータ記憶部１３１は、データ保有者装置１１からユーザの属性情報とこれに対応するユーザＩＤを暗号化した暗号文を受信し、販売事業者装置１２からユーザの購買履歴とこれに対応するユーザＩＤを暗号化した暗号文を受信し、これらの暗号文を記憶する（Ｓ１３１）。

[0024] ＜データ突合部１３２＞

データ突合部１３２は、秘密計算処理により、ユーザＩＤの暗号文に基づいて属性情報の暗号文と購買履歴の暗号文を突合する（Ｓ１３２）。図５に、突合された属性情報と購買情報の暗号文の例を示す。なお、［＊］は、＊の暗号文を意味する。

[0025] ＜データ分離部１３３＞

データ分離部１３３は、秘密計算処理により、突合されなかった属性情報の暗号文に対応するユーザＩＤの暗号文を抽出する（Ｓ１３３）。図５の例

では、ユーザＩＤの暗号文＝［Ｂ］、［Ｚ］が突合されなかった属性情報の暗号文に対応するユーザＩＤの暗号文に該当する。

[0026] ＜モデル生成部１３４＞

モデル生成部１３４は、秘密計算処理により、購買履歴の暗号文と、当該購買履歴の暗号文に突合された属性情報の暗号文からなる教師あり学習用データセットに基づいて予測モデルを生成する（Ｓ１３４）。

[0027] ＜購買予測部１３５＞

購買予測部１３５は、秘密計算処理により、突合されなかった属性情報の暗号文と予測モデルに基づいて、購買予測の暗号文を生成し、購買予測の暗号文を販売事業者装置１２に送信する（Ｓ１３５）。図６に、生成される購買予測の暗号文の例を示す。

[0028] ＜販売事業者装置１２：復号部１２１＞

販売事業者装置１２の復号部１２１は、購買予測の暗号文を受信し、受信した購買予測の暗号文を復号する（Ｓ１２１）。

[0029] ＜購買予測記憶部１２４＞

購買予測記憶部１２４は、復号された購買予測を記憶する（Ｓ１２４）。

実施例 2

[0030] 以下、生成した予測モデルに属性情報を入力して購買予測を生成する際に、平文データを用いることで処理時間の短縮を実現した、実施例２の購買予測システムについて説明する。

[0031] 図７に示すように本実施例の購買予測システム２は、データ保有者装置２１と、販売事業者装置２２と、秘密計算装置２３を含み、各装置は通信可能にネットワークに接続されている。

[0032] 図８に示すように、データ保有者装置２１は、属性情報記憶部１１０と、属性情報抽出部１１１と、暗号化部１１２と、復号部１１３と、購買予測部１１４を含む。販売事業者端末２２は、購買履歴記憶部１２０と、暗号化部１２２と、購買履歴抽出部１２３と、購買予測記憶部１２４を含む。秘密計算装置２３は、データ記憶部１３１と、データ突合部１３２と、データ分離

部１３３と、モデル生成部１３４を含む。

[0033] 実施例１との構成上の違いは、実施例１のデータ保有者装置１１には存在しなかった復号部１１３、購買予測部１１４が、本実施例のデータ保有装置２１に追加されている点、実施例１の販売事業者装置１２に存在した復号部１２１が、本実施例の販売事業者装置２２において省略されている点、実施例１の秘密計算装置１３に存在した購買予測部１３５が、本実施例の秘密計算装置２３において省略されている点である。

[0034] 実施例１と同様に、属性情報記憶部１１０は、予めユーザの属性情報をユーザＩＤと対応付けて記憶し、購買履歴記憶部１２０は、予めユーザの購買履歴をユーザＩＤと対応付けて記憶している。

[0035] また図９に示すように、ステップＳ１１１、Ｓ１１２、Ｓ１２３、Ｓ１２２、Ｓ１３１、Ｓ１３２は、実施例１と同じように実行される。以下、実施例１と異なる動作について詳細に説明する。

[0036] ＜秘密計算装置２３：データ分離部１３３＞

データ分離部１３３は、秘密計算処理により、突合されなかった属性情報の暗号文に対応するユーザＩＤの暗号文を抽出して、データ保有者装置２１に送信する（Ｓ１３３－２）。

[0037] ＜モデル生成部１３４＞

モデル生成部１３４は、秘密計算処理により、購買履歴の暗号文と、当該購買履歴の暗号文に突合された属性情報の暗号文からなる教師あり学習用データセットに基づいて予測モデルを生成して、データ保有者装置２１に送信する（Ｓ１３４）。

[0038] ＜データ保有者装置２１：復号部１１３＞

データ保有者装置２１の復号部１１３は、受信したユーザＩＤの暗号文を復号する（Ｓ１１３）。

[0039] ＜属性抽出部１１１＞

属性情報抽出部１１１は、属性情報記憶部１１０から復号したユーザＩＤに対応する属性情報を抽出する（Ｓ１１１－２）

＜購買予測部１１４＞

購買予測部１１４は、復号したユーザＩＤに対応する属性情報と予測モデルに基づいて、購買予測を生成し、購買予測を販売事業者装置２２に送信する（Ｓ１１４）。

[0040] ＜販売事業者装置２２：購買予測記憶部１２４＞

販売事業者装置２２の購買予測記憶部１２４は、購買予測（平文）を受信し、受信した購買予測を記憶する（Ｓ１２４－２）。

[0041] ＜効果＞

上述の購買予測システムによれば、データ保有者の属性情報と販売事業者の購買履歴を暗号化して秘密計算装置に登録し、秘密計算装置内で暗号化したまま購買履歴と属性情報を結合するため、個人が特定されない状態でデータを利用することができる。

[0042] また、秘密計算技術を用い、秘密計算装置において暗号化したまま予測モデルを生成するため、予測モデルそのものも秘匿することができる。

[0043] 生成した予測モデルに、データ保有者が保有する属性情報のうちモデル生成に使用されなかった属性情報をテストデータとして利用することで、購買予測を生成することができ、これまで販売事業者が知り得なかった新たな顧客を抽出することができる。

[0044] 実施例２に開示したように、テストデータを平文で入力する構成とした場合、秘密計算技術を用いた予測よりも、数百倍の速度で処理することが可能となる。

[0045] また、販売事業者は、企業秘密である購買履歴をデータ保有者に開示する必要がない。

[0046] また、販売事業者は、データ保有者の属性情報を用いた幅広い購買予測データを受け取ることが可能になり、販売事業者が自ら属性情報を集めるよりも、効率的に販売予測を行うことができる。

[0047] また、データ保有者から販売事業者へ開示する属性情報は必要最小限に留めることが出来る。秘密計算装置に登録されたデータは秘密計算技術で処理

されるため、他者にデータを流出させるおそれがない。

[0048] ＜補記＞

本発明の装置は、例えば単一のハードウェアエンティティとして、キーボードなどが接続可能な入力部、液晶ディスプレイなどが接続可能な出力部、ハードウェアエンティティの外部に通信可能な通信装置（例えば通信ケーブル）が接続可能な通信部、ＣＰＵ（Central Processing Unit、キャッシュメモリやレジスタなどを備えていてもよい）、メモリであるＲＡＭやＲＯＭ、ハードディスクである外部記憶装置並びにこれらの入力部、出力部、通信部、ＣＰＵ、ＲＡＭ、ＲＯＭ、外部記憶装置の間のデータのやり取りが可能なように接続するバスを有している。また必要に応じて、ハードウェアエンティティに、ＣＤ－ＲＯＭなどの記録媒体を読み書きできる装置（ドライブ）などを設けることとしてもよい。このようなハードウェア資源を備えた物理的実体としては、汎用コンピュータなどがある。

[0049] ハードウェアエンティティの外部記憶装置には、上述の機能を実現するために必要となるプログラムおよびこのプログラムの処理において必要となるデータなどが記憶されている（外部記憶装置に限らず、例えばプログラムを読み出し専用記憶装置であるＲＯＭに記憶させておくこととしてもよい）。また、これらのプログラムの処理によって得られるデータなどは、ＲＡＭや外部記憶装置などに適宜に記憶される。

[0050] ハードウェアエンティティでは、外部記憶装置（あるいはＲＯＭなど）に記憶された各プログラムとこの各プログラムの処理に必要なデータが必要に応じてメモリに読み込まれて、適宜にＣＰＵで解釈実行・処理される。その結果、ＣＰＵが所定の機能（上記、…部、…手段などと表した各構成要件）を実現する。

[0051] 本発明は上述の実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で適宜変更が可能である。また、上記実施形態において説明した処理は、記載の順に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されると

してもよい。

[0052] 既述のように、上記実施形態において説明したハードウェアエンティティ（本発明の装置）における処理機能をコンピュータによって実現する場合、ハードウェアエンティティが有すべき機能の処理内容はプログラムによって記述される。そして、このプログラムをコンピュータで実行することにより、上記ハードウェアエンティティにおける処理機能がコンピュータ上で実現される。

[0053] 上述の各種の処理は、図１０に示すコンピュータ１００００の記録部１００２０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１００１０、入力部１００３０、出力部１００４０などに動作させることで実施できる。

[0054] 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、半導体メモリ等どのようなものでもよい。具体的には、例えば、磁気記録装置として、ハードディスク装置、フレキシブルディスク、磁気テープ等を、光ディスクとして、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ（Random Access Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）等を、光磁気記録媒体として、ＭＯ（Magneto-Optical disc）等を、半導体メモリとしてＥＥＰ－ＲＯＭ（Electrically Erasable and Programmable-Read Only Memory）等を用いることができる。

[0055] 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。

[0056] 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。

[0057] 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、ハードウェアエンティティ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。

請求の範囲

[請求項1] データ保有者装置からユーザの属性情報とこれに対応するユーザＩＤを暗号化した暗号文を受信し、販売事業者装置から前記ユーザの購買履歴とこれに対応する前記ユーザＩＤを暗号化した暗号文を受信し、これらの暗号文を記憶するデータ記憶部と、

秘密計算処理により、前記ユーザＩＤの暗号文に基づいて前記属性情報の暗号文と前記購買履歴の暗号文を突合するデータ突合部と、

秘密計算処理により、突合されなかった前記属性情報の暗号文に対応する前記ユーザＩＤの暗号文を抽出するデータ分離部と、

秘密計算処理により、前記購買履歴の暗号文と、当該購買履歴の暗号文に突合された前記属性情報の暗号文からなる教師あり学習用データセットに基づいて予測モデルを生成するモデル生成部と、

秘密計算処理により、突合されなかった前記属性情報の暗号文と前記予測モデルに基づいて、購買予測の暗号文を生成し、前記購買予測の暗号文を前記販売事業者装置に送信する購買予測部を含む

秘密計算装置。

[請求項2] データ保有者装置からユーザの属性情報とこれに対応するユーザＩＤを暗号化した暗号文を受信し、販売事業者装置から前記ユーザの購買履歴とこれに対応する前記ユーザＩＤを暗号化した暗号文を受信し、これらの暗号文を記憶するデータ記憶部と、

秘密計算処理により、前記ユーザＩＤの暗号文に基づいて前記属性情報の暗号文と前記購買履歴の暗号文を突合するデータ突合部と、

秘密計算処理により、突合されなかった前記属性情報の暗号文に対応する前記ユーザＩＤの暗号文を抽出して、前記データ保有者装置に送信するデータ分離部と、

秘密計算処理により、前記購買履歴の暗号文と、当該購買履歴の暗号文に突合された前記属性情報の暗号文からなる教師あり学習用データセットに基づいて予測モデルを生成して、前記データ保有者装置に

送信するモデル生成部を含む

秘密計算装置。

[請求項3] データ保有者装置と、販売事業者装置と、秘密計算装置を含む購買予測システムであって、

前記データ保有者装置は、

ユーザの属性情報をユーザＩＤと対応付けて記憶する属性情報記憶部から前記属性情報と前記ユーザＩＤを抽出する属性情報抽出部と、

抽出した前記属性情報と前記ユーザＩＤを暗号化して前記秘密計算装置に送信する暗号化部を含み、

前記販売事業者装置は、

前記ユーザの購買履歴を前記ユーザＩＤと対応付けて記憶する購買履歴記憶部から前記購買履歴と前記ユーザＩＤを抽出する購買履歴抽出部と、

抽出した前記購買履歴と前記ユーザＩＤを暗号化して前記秘密計算装置に送信する暗号化部を含み、

前記秘密計算装置は、

秘密計算処理により、前記ユーザＩＤの暗号文に基づいて前記属性情報の暗号文と前記購買履歴の暗号文を突合するデータ突合部と、

秘密計算処理により、突合されなかった前記属性情報の暗号文に対応する前記ユーザＩＤの暗号文を抽出するデータ分離部と、

秘密計算処理により、前記購買履歴の暗号文と、当該購買履歴の暗号文に突合された前記属性情報の暗号文からなる教師あり学習用データセットに基づいて予測モデルを生成するモデル生成部と、

秘密計算処理により、突合されなかった前記属性情報の暗号文と前記予測モデルに基づいて、購買予測の暗号文を生成し、前記購買予測の暗号文を前記販売事業者装置に送信する購買予測部を含む

購買予測システム。

[請求項4] データ保有者装置と、販売事業者装置と、秘密計算装置を含む購買

予測システムであって、

前記データ保有者装置は、

ユーザの属性情報をユーザＩＤと対応付けて記憶する属性情報記憶部から前記属性情報と前記ユーザＩＤを抽出する属性情報抽出部と、

抽出した前記属性情報と前記ユーザＩＤを暗号化して前記秘密計算装置に送信する暗号化部を含み、

前記販売事業者装置は、

前記ユーザの購買履歴を前記ユーザＩＤと対応付けて記憶する購買履歴記憶部から前記購買履歴と前記ユーザＩＤを抽出する購買履歴抽出部と、

抽出した前記購買履歴と前記ユーザＩＤを暗号化して前記秘密計算装置に送信する暗号化部を含み、

前記秘密計算装置は、

秘密計算処理により、前記ユーザＩＤの暗号文に基づいて前記属性情報の暗号文と前記購買履歴の暗号文を突合するデータ突合部と、

秘密計算処理により、突合されなかった前記属性情報の暗号文に対応する前記ユーザＩＤの暗号文を抽出して、前記データ保有者装置に送信するデータ分離部と、

秘密計算処理により、前記購買履歴の暗号文と、当該購買履歴の暗号文に突合された前記属性情報の暗号文からなる教師あり学習用データセットに基づいて予測モデルを生成して、前記データ保有者装置に送信するモデル生成部を含み、

前記データ保有者装置は、

受信した前記ユーザＩＤの暗号文を復号する復号部と、

復号した前記ユーザＩＤに対応する前記属性情報と前記予測モデルに基づいて、購買予測を生成し、前記購買予測を前記販売事業者装置に送信する購買予測部を含む

購買予測システム。

[請求項5] 秘密計算装置が実行する秘密計算方法であって、

データ保有者装置からユーザの属性情報とこれに対応するユーザＩＤを暗号化した暗号文を受信し、販売事業者装置から前記ユーザの購買履歴とこれに対応する前記ユーザＩＤを暗号化した暗号文を受信し、これらの暗号文を記憶するステップと、

秘密計算処理により、前記ユーザＩＤの暗号文に基づいて前記属性情報の暗号文と前記購買履歴の暗号文を突合するステップと、

秘密計算処理により、突合されなかった前記属性情報の暗号文に対応する前記ユーザＩＤの暗号文を抽出するステップと、

秘密計算処理により、前記購買履歴の暗号文と、当該購買履歴の暗号文に突合された前記属性情報の暗号文からなる教師あり学習用データセットに基づいて予測モデルを生成するステップと、

秘密計算処理により、突合されなかった前記属性情報の暗号文と前記予測モデルに基づいて、購買予測の暗号文を生成し、前記購買予測の暗号文を前記販売事業者装置に送信するステップを含む

秘密計算方法。

[請求項6] 秘密計算装置が実行する秘密計算方法であって、

データ保有者装置からユーザの属性情報とこれに対応するユーザＩＤを暗号化した暗号文を受信し、販売事業者装置から前記ユーザの購買履歴とこれに対応する前記ユーザＩＤを暗号化した暗号文を受信し、これらの暗号文を記憶するステップと、

秘密計算処理により、前記ユーザＩＤの暗号文に基づいて前記属性情報の暗号文と前記購買履歴の暗号文を突合するステップと、

秘密計算処理により、突合されなかった前記属性情報の暗号文に対応する前記ユーザＩＤの暗号文を抽出して、前記データ保有者装置に送信するステップと、

秘密計算処理により、前記購買履歴の暗号文と、当該購買履歴の暗号文に突合された前記属性情報の暗号文からなる教師あり学習用デー

タセットに基づいて予測モデルを生成して、前記データ保有者装置に送信するステップを含む

秘密計算方法。

[請求項7] コンピュータを請求項１または２に記載の秘密計算装置として機能させるプログラム。

[図1]

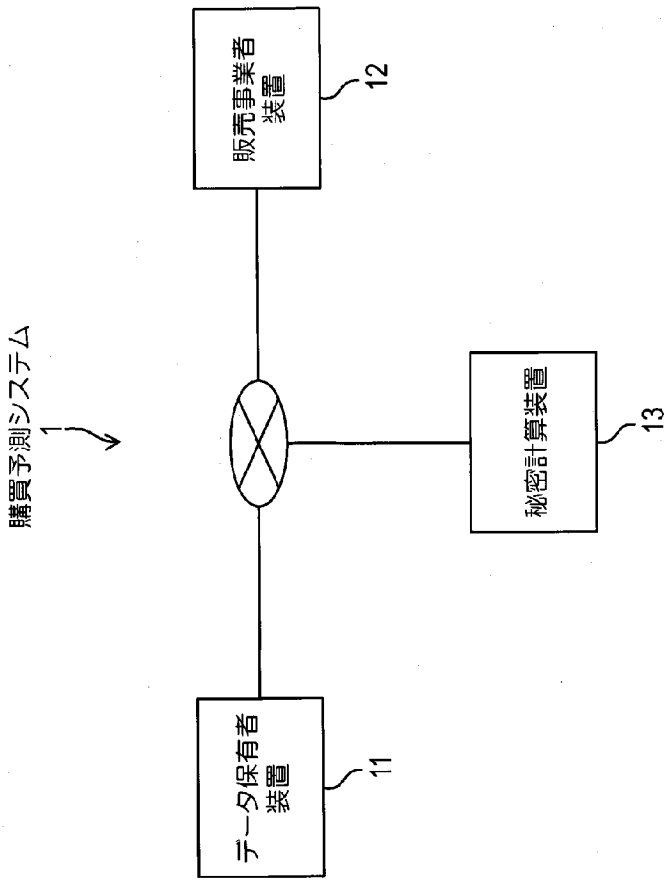


図1

[図2]

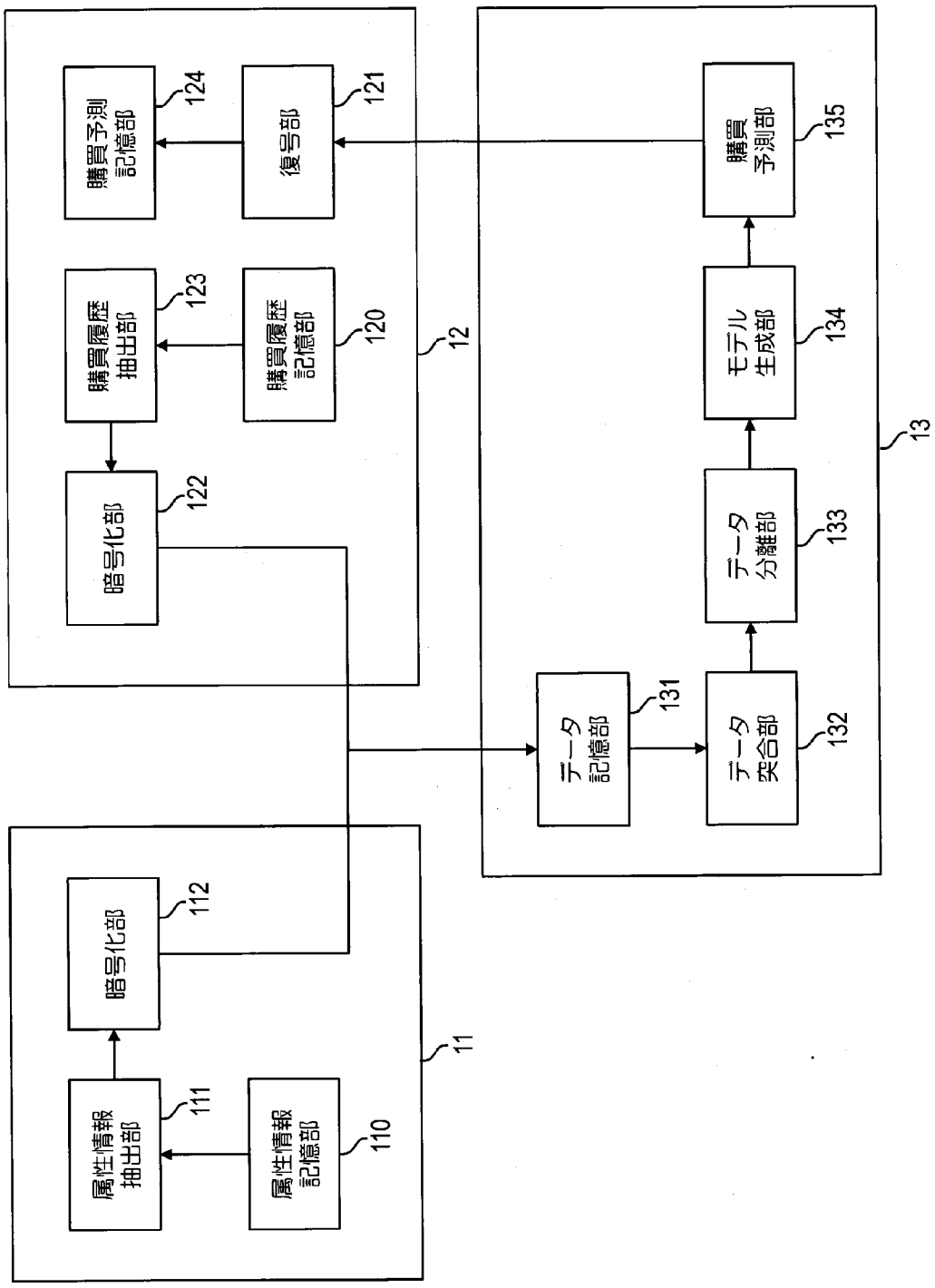

属性情報記憶部
110
属性情報抽出部
111
暗号化部
112
11
購買履歴記憶部
120
購買履歴抽出部
123
暗号化部
122
購買予測記憶部
124
復号部
121
12
データ記憶部
131
データ突合部
132
データ分離部
133
モデル生成部
134
購買予測部
135
13

図2

[図3]

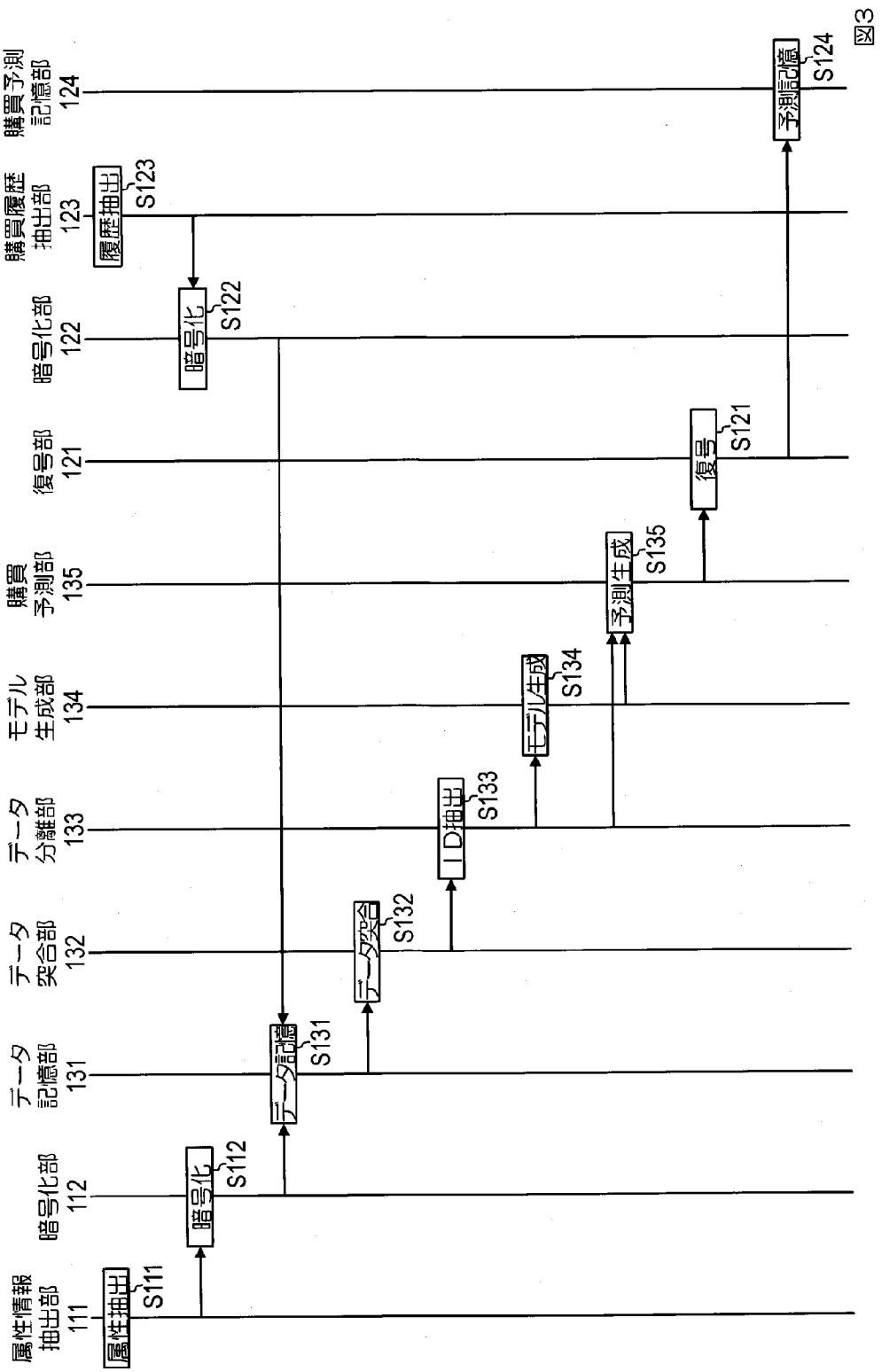

属性情報抽出部 111
暗号化部 112
データ記憶部 131
データ突合部 132
データ分離部 133
モデル生成部 134
購買予測部 135
復号部 121
暗号化部 122
購買履歴抽出部 123
購買予測記憶部 124
属性抽出
S111
暗号化
S112
データ記憶
S131
データ突合
S132
ID抽出
S133
モデル生成
S134
予測生成
S135
復号
S121
暗号化
S122
履歴抽出
S123
予測記憶
S124

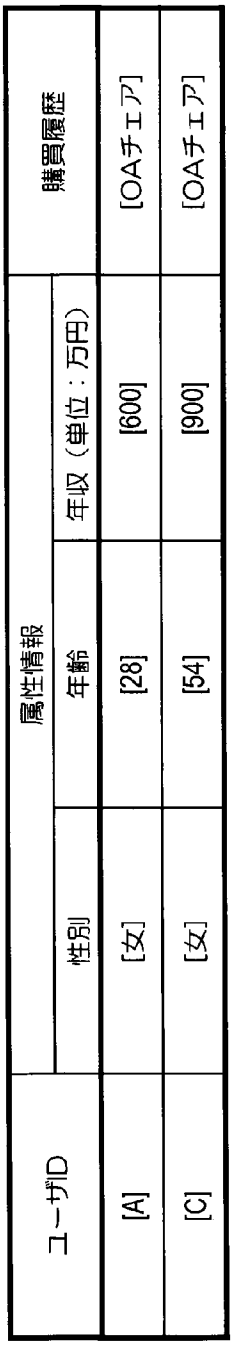
図3

[図4]

図4

ユーザID	属性情報		
	性別	年齢	年収（単位：万円）
[A]	[女]	[28]	[600]
[B]	[男]	[43]	[700]
[C]	[女]	[54]	[900]
[Z]	[男]	[35]	[600]

[図5]



ユーザID	属性情報			購買履歴
	性別	年齢	年収（単位：万円）	
[A]	[女]	[28]	[600]	[OAチェア]
[C]	[女]	[54]	[900]	[OAチェア]

図5

[図6]

図6

ユーザID	購買予測
[B]	[高級チェア]
[Z]	[座椅子]

[図7]

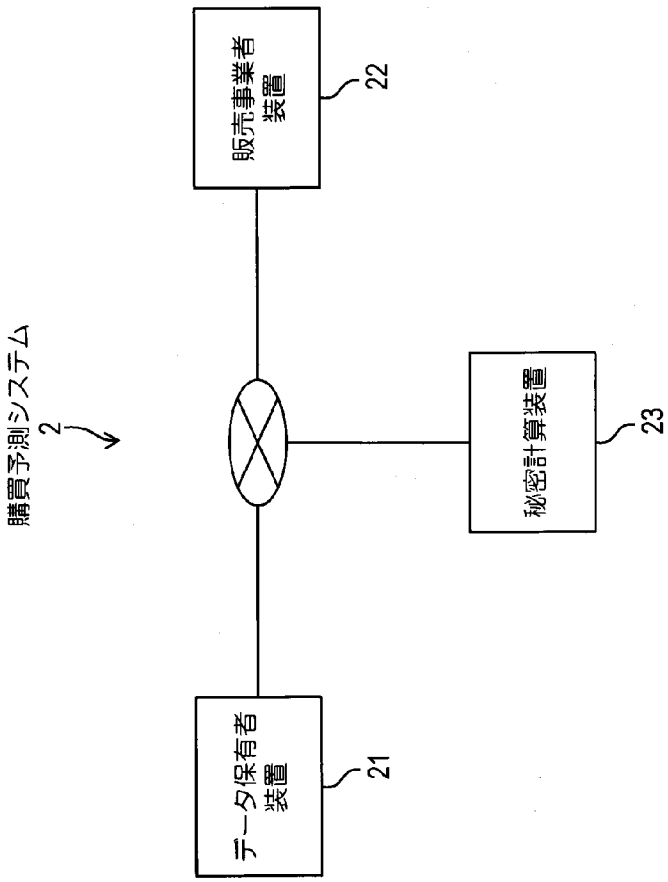
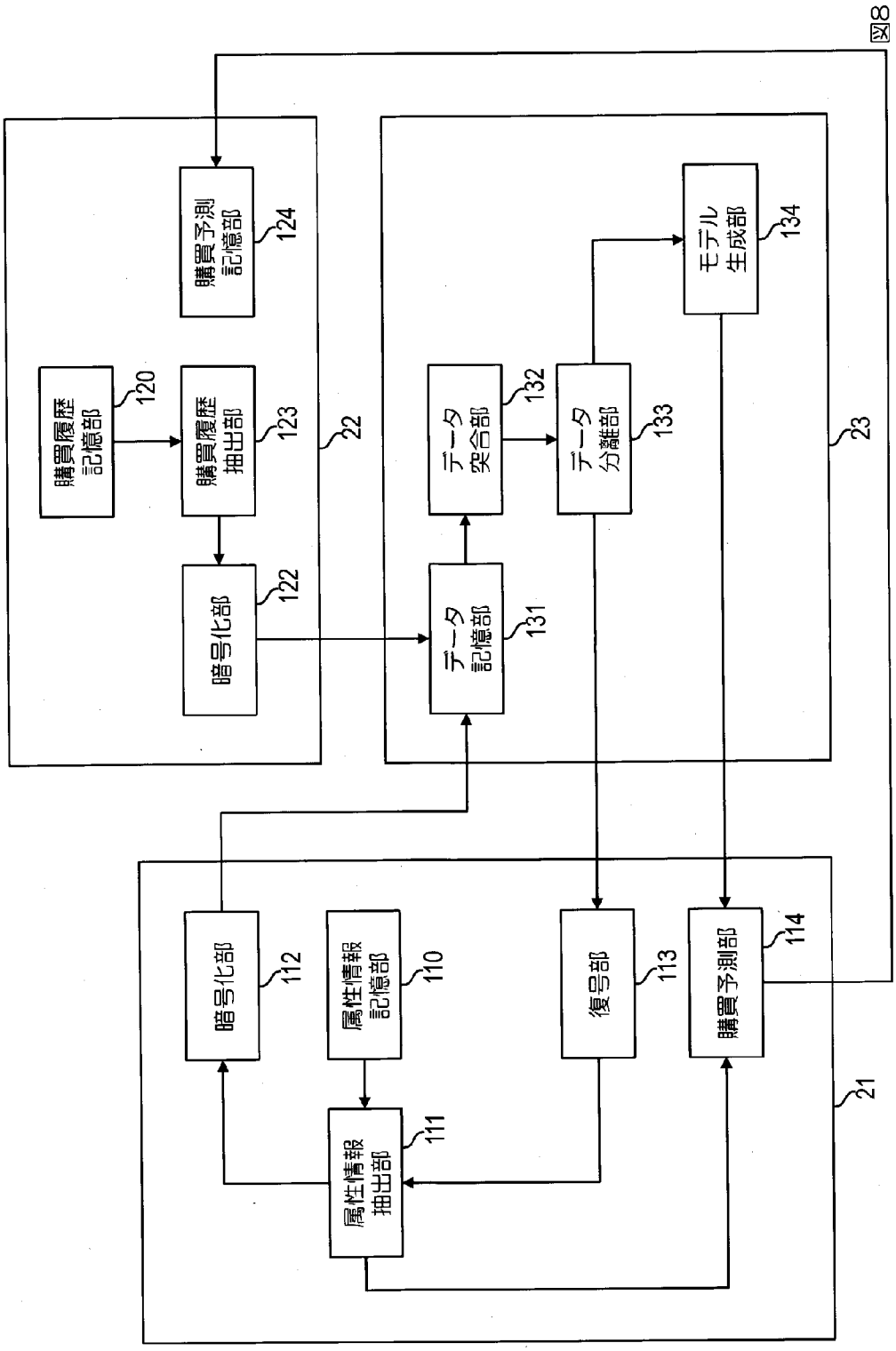


図7

[図8]


図8
購買予測記憶部
124
購買履歴記憶部
120
購買履歴抽出部
123
22
暗号化部
122
データ突合部
132
データ分離部
133
モデル生成部
134
データ記憶部
131
23
暗号化部
112
属性情報記憶部
110
復号部
113
購買予測部
114
属性情報抽出部
111
21

[図9]

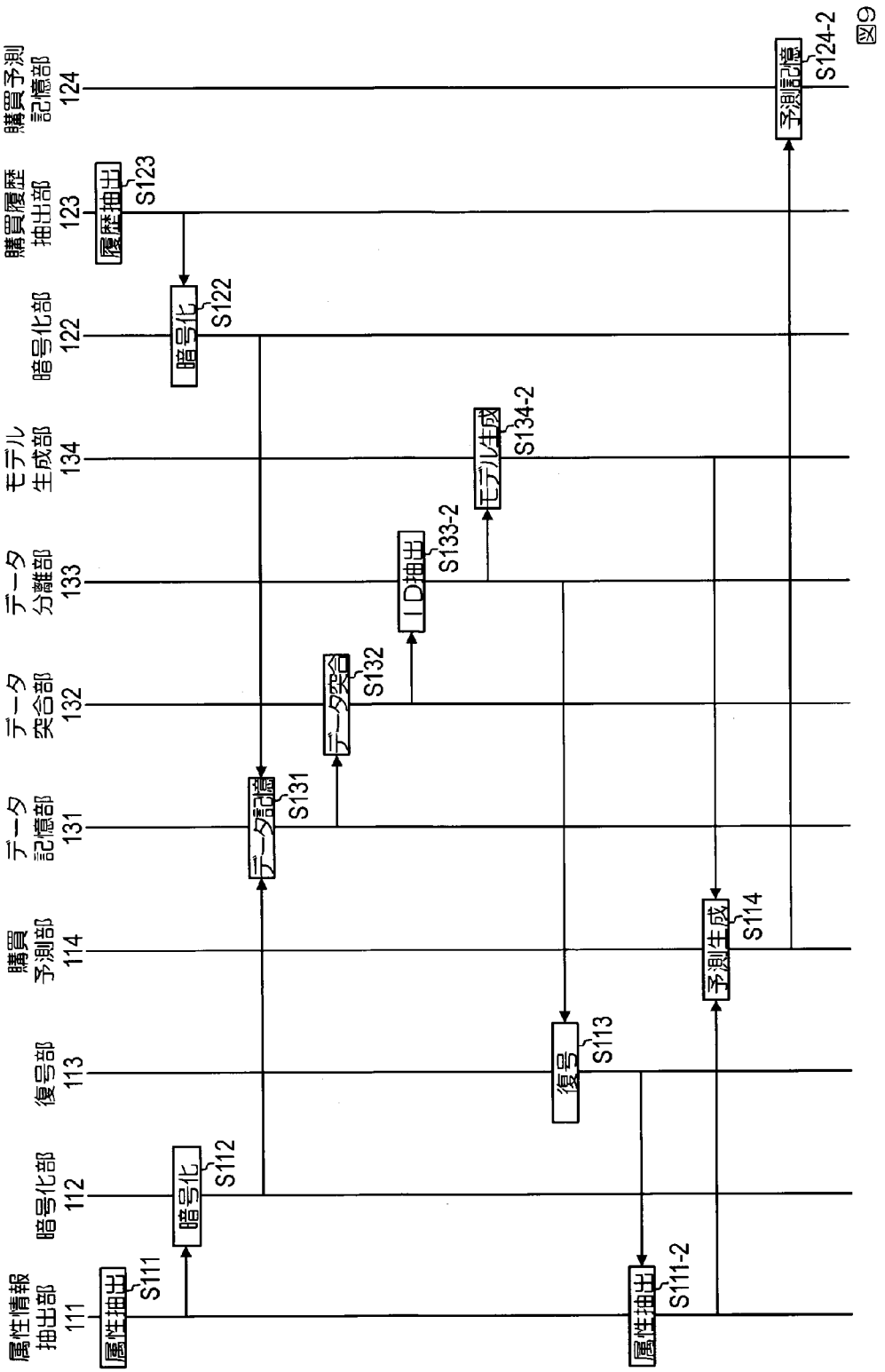

属性情報抽出部 111
暗号化部 112
復号部 113
購買予測部 114
データ記憶部 131
データ突合部 132
データ分離部 133
モデル生成部 134
暗号化部 122
購買履歴抽出部 123
購買予測記憶部 124
属性抽出
S111
暗号化
S112
復号
S113
予測生成
S114
データ記憶
S131
データ突合
S132
ID抽出
S133-2
モデル生成
S134-2
暗号化
S122
履歴抽出
S123
予測記憶
S124-2
属性抽出
S111-2

図9

[図10]

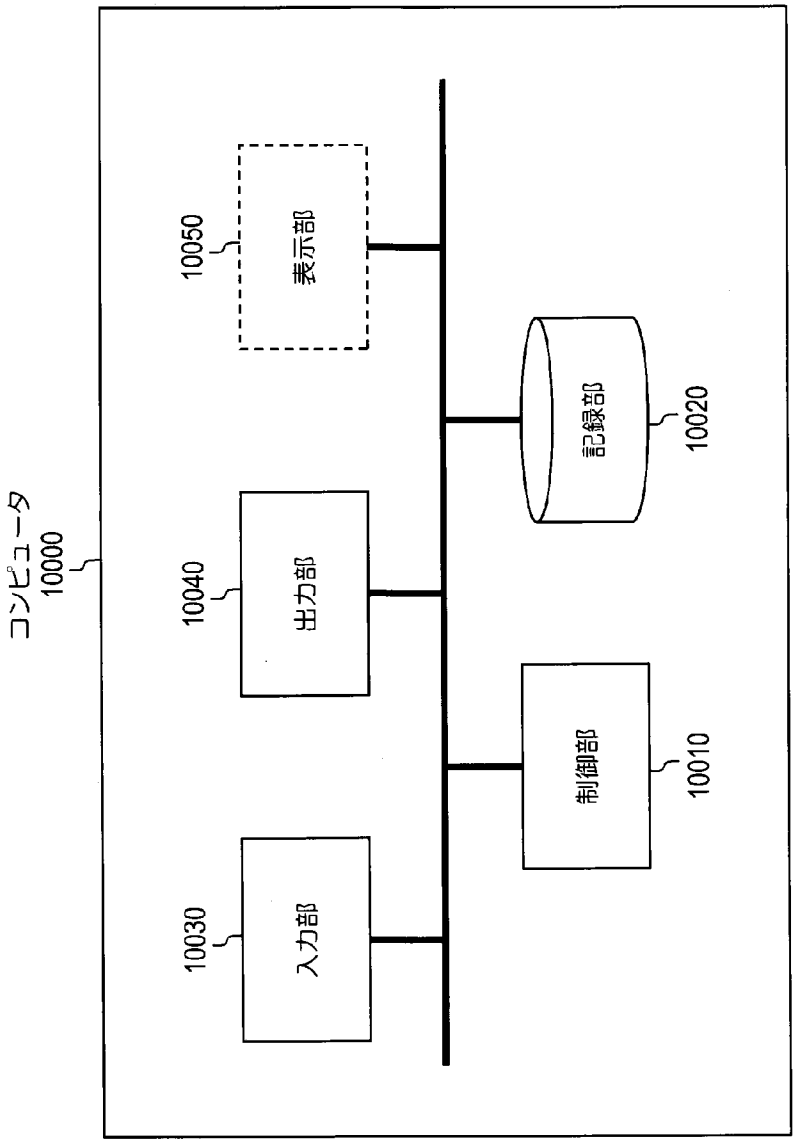

コンピュータ
10000
表示部
10050
記録部
10020
出力部
10040
制御部
10010
入力部
10030

図10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/023551

A. CLASSIFICATION OF SUBJECT MATTER
G06Q 30/02(2012.01)i
FI: G06Q30/02

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06Q10/00-99/00

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	JP 2020-149693 A (ACTAPIO INC) 17 September 2020 (2020-09-17) paragraphs [0014]-[0033], [0040], [0047]-[0048], [0132]-[0136], [0151]-[0153], [0165]-[0170], [0196]	1-7
Y	JP 2018-54765 A (NEC CORP) 05 April 2018 (2018-04-05) paragraphs [0002]-[0014], [0022]-[0045]	1-7
Y	JP 2017-225116 A (PALO ALTO RESEARCH CENTER INCORPORATED) 21 December 2017 (2017-12-21) paragraphs [0012]-[0014], [0017]	1, 3-5, 7
Y	JP 6351813 B1 (YAHOO JAPAN CORP) 04 July 2018 (2018-07-04) paragraphs [0019]-[0026], [0035]-[0036]	2, 6-7

☐ 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	Date of mailing of the international search report
08 September 2021 (08.09.2021)	21 September 2021 (21.09.2021)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/023551

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2020-149693 A	17 Sep. 2020	US 2020/0293898 A1 paragraphs [0007]-[0014], [0042]-[0053], [0060], [0067]-[0068], [0152]-[0163]	
JP 2018-54765 A	05 Apr. 2018	US 2018/0089574 A1 paragraphs [0003]-[0018], [0050]-[0074]	
JP 2017-225116 A	21 Dec. 2017	US 2017/0366519 A1 paragraphs [0019]-[0021], [0024] EP 3258669 A1 KR 10-2017-0142872 A	
JP 6351813 B1	04 Jul. 2018	(Family: none)	

国際調査報告

国際出願番号
PCT/JP2021/023551

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06Q 30/02(2012.01)i
FI: G06Q30/02

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

G06Q10/00-99/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２１年
日本国実用新案登録公報	１９９６－２０２１年
日本国登録実用新案公報	１９９４－２０２１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2020-149693 A (アクタピオ，インコーポレイテッド) 17.09.2020 (2020-09-17) 段落0014-0033，0040，0047-0048，0132-0136，0151-0153，0165-0170，0196	1-7
Y	JP 2018-54765 A (日本電気株式会社) 05.04.2018 (2018-04-05) 段落0002-0014,0022-0045	1-7
Y	JP 2017-225116 A (パロ・アルト・リサーチ・センター・インコーポレーテッド) 21.12.2017 (2017-12-21) 段落0012-0014，0017	1,3-5,7
Y	JP 6351813 B1 (ヤフー株式会社) 04.07.2018 (2018-07-04) 段落0019-0026，0035-0036	2,6-7

☐ 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。

＊ 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	国際調査報告の発送日
08.09.2021	21.09.2021

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）
谷川　智秀 5L 5876
電話番号 03-3581-1101 内線 3560

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/JP2021/023551

引用文献	公表日	パテントファミリー文献	公表日
JP 2020-149693 A	17.09.2020	US 2020/0293898 A1 段落0007-0014, 0042-0053, 0060, 0067-0068, 0152-0163	
JP 2018-54765 A	05.04.2018	US 2018/0089574 A1 段落0003-0018, 0050-0074	
JP 2017-225116 A	21.12.2017	US 2017/0366519 A1 段落0019-0021, 0024 EP 3258669 A1 KR 10-2017-0142872 A	
JP 6351813 B1	04.07.2018	（ファミリーなし）	