(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
2020年4月30日(30.04.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/084751 A1

(51) 国際特許分類:
G09C 1/00 (2006.01) *H04L 9/36* (2006.01)

(21) 国際出願番号： PCT/JP2018/039818

(22) 国際出願日： 2018年10月26日(26.10.2018)

(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 気 株 式 会 社 (**NEC CORPORATION**) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者: 荒 木 俊 則 (**ARAKI, Toshinori**); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

(74) 代理人: 加藤 朝道(**KATO, Asamichi**); 〒2220033 神奈川県横浜市港北区新横浜２丁目１７番１９号加藤内外特許事務所内 Kanagawa (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, HR, HU, ID, IL, IN, IR, IS, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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).

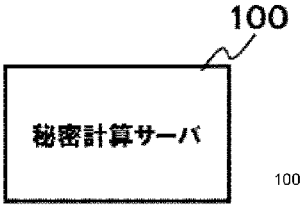
添付公開書類：

一 国際調査報告（条約第21条(3)）

WO 2020/084751 A1

(54) **Title:** SECRET CALCULATION SERVER, SYSTEM, SECRET CALCULATION METHOD, AND PROGRAM

(54) 発明の名称： 秘密計算サーバ、システム、秘密計算方法及びプログラム



100 Secret calculation server

(57) **Abstract:** The present invention provides a secret calculation server capable of performing high-speed secret calculation. The secret calculation server performs a shift operation with respect to shares that are secretly distributed. The secret calculation server may perform a shift operation when reducing effective digits in the secret information corresponding to the shares that are secretly distributed.

(57) 要約：秘密計算を高速に実行する秘密計算サーバを提供する。秘密計算サーバは、秘密分散されたシェアに対してシフト演算を行う。秘密計算サーバは、秘密分散されたシェアに対応する秘密情報の有効桁数を削減する場合に、シフト演算を行ってもよい。

明　細　書

発明の名称 ：

秘密計算サーバ、システム、秘密計算方法及びプログラム

技術分野

[0001] 本発明は、秘密計算サーバ、システム、秘密計算方法及びプログラムに関する。

背景技術

[0002] 秘密計算（マルチパーティ計算；ＭＰＣ（Multi Party Computation））と称される技術が存在する（例えば、特許文献１参照）。秘密計算（秘密分散型計算）では、複数のパーティ（秘密計算サーバ）がそれぞれの持つ秘密情報を隠しながら当該秘密情報を用いた種々の計算を行う。

[0003] 秘密計算では、秘密にする情報Ｓから秘密計算に参加するパーティに配付するシェア（秘密分散情報）が作成される。例えば、３台の秘密計算サーバにより秘密計算が行われる場合、秘密情報Ｓから３つのシェア｛s_1、s_2、s_3｝がランダムに作成され、各パーティに１つ又は２つのシェアが配分される。より具体的には、Ｎ（Ｎは自然数、以下同じ）を法とし、$s_1+s_2+s_3 \bmod N=S$となるようなシェアがランダムに生成される。なお、上記法Ｎには、素数や２の冪数（2^n；ｎは自然数、以下同じ）が選択されることが多い。また、「ａ ｍｏｄ ｂ」は整数ａを整数ｂで除算した際の余りを示す。

[0004] 非特許文献１には、秘密分散された数値をビット表現（２進数表記）に変換するビット分解と称される技術が開示されている。

先行技術文献

特許文献

[0005] 特許文献1：特開２０１８－０４５０１９号公報

非特許文献

[0006] 非特許文献1：Kazuma Ohara, Toshinori Araki, Hikaru Tsuchida and Furuk

awa Jun、”異なるサイズの環が混在する不正検知可能なマルチパーティ計算”、2018 Symposium on Cryptography and Information Security, Niigata, Japan, 2018, 2A1-4.

発明の概要

発明が解決しようとする課題

[0007] なお、上記先行技術文献の各開示を、本書に引用をもって繰り込むものとする。以下の分析は、本発明者らによってなされたものである。

[0008] 近年では、欧州にて施行が始まった一般データ保護規則等に代表されるように、個人情報の保護が強く求められている。そのため、特許文献１に開示されたようなデータ（情報）を秘密にしつつ当該データを用いた任意の演算が可能な秘密計算を種々のシステムやサービス等に適用することが検討されている。

[0009] 例えば、駅やイベント会場等の各所にカメラを設置し、当該カメラから取得される顔画像を利用した人流分析に秘密計算を適用することが検討されている。カメラを用いた人流分析では、例えば、駅及びイベント会場に設置されたカメラそれぞれから得られる画像を用いて各カメラに写る人物を特定する。その上で、各人物が撮影されたカメラの位置及び時刻を分析、集計することで、駅やイベント会場等を中心とした人流分析がなされる。ここで、上記のような人流分析を実現するためには、駅とイベント会場に設置されたカメラに写る人物を特定するための特徴量が必要となる。しかし、プライバシ保護が強く求められる現状では、各施設（駅、イベント会場）の管理主体が顔画像から抽出した特徴量といった個人情報を外部機関（人流分析をする機関）に提供することは困難である。しかし、このような問題は、秘密計算を用いることで解決できる。具体的には、駅等のカメラによる画像から算出された特徴量を秘密にする対象に設定し、複数の秘密計算サーバにて上記特徴量を用いた人物特定、人流分析を実現すればよい。

[0010] 上記人流分析以外にも、秘密計算の適用が有効なシステムは数多く存在する。例えば、電車等の利用者に関する認証システム（顔認証システム）が秘

密計算の適用が有効なシステムとして挙げられる。例えば、顔認証による認証システムの実現には、予め利用者の顔画像から取得された特徴量をデータベースに登録し、駅の改札（ゲート）に設定されたカメラから得られる特徴量と上記事前に登録した特徴量の比較（照合）が必要となる。その際、個人情報保護、プライバシ保護の観点からデータベースに登録する特徴量は秘密であることが望ましい。そこで、事前に登録する特徴量を秘密分散して顔認証に利用することが検討されている。

[0011] 人流分析システムや認証システムを例にとり説明したように、秘密計算では入力データを秘匿しつつ、当該入力データに対する任意の情報処理が可能である。そのため、個人情報を取り扱うシステムを対象として秘密計算の適用が進むものと予測される。一方で、秘密計算には、例えば、乗算処理を実行する際には秘密計算サーバ間で通信が必要となるなど演算結果を得るまでに比較的長い時間を要するという性質がある。結果を得るまでの時間に対して寛容なシステム、アプリケーションであれば上記秘密計算の性質は問題とはならない。しかし、人流分析や認証システムのようにリアルタイムに処理することが求められるシステムでは上記性質は許容されないことも多い。

[0012] 本発明は、秘密計算を高速に実行することに寄与する、秘密計算サーバ、システム、秘密計算方法及びプログラムを提供することを主たる目的とする。

課題を解決するための手段

[0013] 本発明乃至開示の第１の視点によれば、秘密分散されたシェアに対してシフト演算を行う、秘密計算サーバが提供される。

[0014] 本発明乃至開示の第２の視点によれば、上記秘密計算サーバと、第１の地点で取得された第１の移動体の識別情報を保持する第１の装置と、第２の地点で取得された第２の移動体の識別情報を保持する第２の装置と、のそれぞれに対して、前記秘密計算サーバへの前記第１、第２の移動体の識別情報の提供を要求する要求部と、前記第１、第２の移動体の識別情報の有効桁数を決定する、決定部と、前記秘密計算サーバに対し、前記決定された第１、第

２の移動体の識別情報の有効桁数に関する情報を通知すると共に、前記第１の移動体の識別情報と前記第２の移動体の識別情報とに基づいた移動体の移動に関する計算処理を指示する指示部と、を備える制御装置と、を含み、前記秘密計算サーバは、前記通知された有効桁数に関する情報に基づいて、前記第１、第２の移動体の識別情報に対して前記シフト演算を行う、システムが提供される。

[0015] 本発明乃至開示の第３の視点によれば、上記秘密計算サーバと、第１の地点から第２の地点へ移動する被認証体について、前記第１の地点において取得された生体情報を入力する生体情報入力部と、前記第１の地点において取得された生体情報を第１のシェア情報に秘密分散し、前記第１シェア情報を前記秘密計算サーバに送信する、秘密分散制御部と、を備える認証候補抽出装置と、を含み、前記秘密計算サーバは、前記被認証体の認証処理用の特徴情報であって、秘密分散された特徴情報を第２シェア情報として記憶する特徴情報記憶部と、前記第１及び第２のシェア情報を用いて、前記認証処理用の候補を抽出する、秘密計算実行部と、を備え、前記認証候補抽出装置は、前記被認証体が前記第１の地点から第２の地点へ到達する予測時間に基づいて、前記第２の地点において取得された被認証体の生体情報を用いて認証処理を行う記認証装置における認証処理に間に合う範囲で所定の要求精度を満たす候補を抽出できるよう、前記第１及び第２のシェア情報の有効桁数に関する情報を前記秘密計算サーバに通知する、処理性能調整部と、前記認証装置に対して、前記秘密計算サーバにより抽出された候補の特徴情報を送信する特徴情報送信部と、をさらに備え、前記秘密計算実行部は、前記通知された第１及び第２のシェア情報の有効桁数に関する情報に基づいて、前記第１及び第２のシェア情報に対して前記シフト演算を行う、システムが提供される。

[0016] 本発明乃至開示の第４の視点によれば、コンピュータにおいて、秘密分散されたシェアを入力するステップと、前記秘密分散されたシェアに対してシフト演算するステップと、を含む、秘密計算方法が提供される。

[0017] 本発明乃至開示の第５の視点によれば、秘密分散されたシェアを入力する処理と、前記秘密分散されたシェアに対してシフト演算する処理と、をコンピュータに実行させるプログラムが提供される。

なお、このプログラムは、コンピュータが読み取り可能な記憶媒体に記録することができる。記憶媒体は、半導体メモリ、ハードディスク、磁気記録媒体、光記録媒体等の非トランジェント（non-transient）なものとすることができる。本発明は、コンピュータプログラム製品として具現することも可能である。

発明の効果

[0018] 本発明乃至開示の各視点によれば、秘密計算を高速に実行することに寄与する、秘密計算サーバ、システム、秘密計算方法及びプログラムが提供される。

図面の簡単な説明

[0019] [図1]一実施形態の概要を説明するための図である。

[図2]本発明の第１の実施形態の人流分析システムの構成を示す図である。

[図3]本発明の第１の実施形態の人流分析システムの第１の装置の構成を示す図である。

[図4]本発明の第１の実施形態の人流分析システムの第１の装置が保持するデータの一例を示す図である。

[図5]本発明の第１の実施形態の人流分析システムの制御装置の構成を示す図である。

[図6]本発明の第１の実施形態の人流分析システムの秘密計算サーバの構成を示す図である。

[図7]本発明の第１の実施形態の人流分析システムの動作を表したシーケンス図である。

[図8]本発明の第１の実施形態の人流分析システムの動作を説明するための図である。

[図9]本発明の第１の実施形態の人流分析システムの動作を説明するための図

である。

[図10]本発明の第１の実施形態の人流分析システムの動作を説明するための図である。

[図11]本発明の第１の実施形態の人流分析システムの動作を説明するための図である。

[図12]本発明の第２の実施形態の認証システムの構成を示す図である。

[図13]本発明の第２の実施形態におけるカメラの設置例を示す図である。

[図14]本発明の第２の実施形態で用いる特徴情報（秘匿処理前）の一例を示す図である。

[図15]本発明の第２の実施形態の認証システムの動作を表したシーケンス図である。

[図16]本発明の第２の実施形態の認証システムの動作を説明するための図である。

[図17]本発明の第２の実施形態に係る変形例１の認証システムの構成を示す図である。

[図18]本発明の第２の実施形態に係る変形例１の動作を説明するための図である。

[図19]本発明の第２の実施形態に係る変形例１の認証システムの動作を表したシーケンス図である。

[図20]本発明の第２の実施形態に係る変形例２の認証システムの構成を示す図である。

[図21]本発明の第２の実施形態に係る変形例２の認証システムの動作を表したシーケンス図である。

[図22]本発明の第２の実施形態に係る変形例２の認証候補抽出装置による処理性能調整処理を表したフローチャートである。

[図23]秘密計算サーバのハードウェア構成の一例を示す図である。

発明を実施するための形態

[0020] 初めに、一実施形態の概要について説明する。なお、この概要に付記した

図面参照符号は、理解を助けるための一例として各要素に便宜上付記したものであり、この概要の記載はなんらの限定を意図するものではない。また、各図におけるブロック間の接続線は、双方向及び単方向の双方を含む。一方向矢印については、主たる信号（データ）の流れを模式的に示すものであり、双方向性を排除するものではない。さらに、本願開示に示す回路図、ブロック図、内部構成図、接続図などにおいて、明示は省略するが、入力ポート及び出力ポートが各接続線の入力端及び出力端のそれぞれに存在する。入出力インターフェイスも同様である。

[0021] 本願開示において、秘密にする数値が取り得る範囲を２進数表記した場合の桁数を有効桁数と表記する。例えば、有効桁数が「４」であれば秘密にする数値は０～１５（０ｂ０００００～０ｂ１１１１）のいずれかである。また、有効桁数が「３」でれば秘密にする数値は０～７（０ｂ０００～０ｂ１１１）のいずれかである。さらに、有効桁数の削減とは、有効桁数削減前の秘密にする数値を削減後の有効桁数により表記可能な範囲の数値に変換することを示す。例えば、４桁にて表現可能な数値「７」の有効桁数を１桁削減する場合を考える。この場合、数値７（０ｂ０１１１）を３桁の２進数にて表記可能な数値３（０ｂ０１１）に変換することが有効桁数の削減である。

[0022] 上述のように、秘密計算の適用が有効なシステムが種々存在する。しかしながら、そのようなシステムの中には、ある程度の処理速度が要求されるものが少なくない。例えば、上記説明した人流分析システムや認証システムがその代表である。一方で、発明者らが鋭意検討した結果、上記人流分析システム等では秘密情報の情報量（有効桁数）を抑制できる状況や抑制すべき状況が存在することが明らかとなった。

[0023] 例えば、人流分析システムでは大まかな人の流れを把握するのが目的であり、商品購入時の代金決済に使用されるような認証システムが要求する人物特定の精度は必要がない。つまり、人流分析システムでは、あるカメラに写る人物と他のカメラに写る人物が同一人物であるか否かの判定は多少精度が低くても許容できる。そのため、人物の特定に利用する特徴量の情報量、即

ち、各カメラから得られる特徴量（特徴ベクトルの各要素）の有効桁数を削減した後に人物を判定してもその影響は軽微である。また、画像から得られる特徴量の精度が高すぎると個人の特定が容易となるため、プライバシ保護の観点から考えても特徴量の有効桁数は少ない方が良いとも言える。

[0024] また、駅等における改札口にて用いられる認証システムでは、時間帯により利用者の数が大きく異なる。ここで、利用者の数が大きく異なるからと言って、認証の精度を低くしたり認証に長時間費やしたりすることは許容されない。そこで、異なる位置に設置されたカメラそれぞれから取得できる特徴量を用いた２段階の認証（仮認証、本認証）の実現が検討されている。具体的には、駅のプラットホーム等にカメラを設け、当該カメラから取得された画像の特徴量を用いて事前登録された特徴量の中から認証候補となる複数の特徴量を抽出する。また、改札の近傍に設置されたカメラから取得された特徴量と上記複数の特徴量のそれぞれを比較し、改札に立つ人物の認証（本認証）を行う。このような２段階の認証を行うことで、利用者の多寡に応じた認証精度及び認証時間の両立を図ることができる。例えば、朝夕の通勤ラッシュ時等の利用者が多いときには、プラットホームから改札までに利用者が移動する時間は長くなる。そのため、最初の認証（仮認証；複数候補の抽出）に比較的長い時間を要したとしても問題はない。一方で、利用者が少ないときはホームから改札までに利用者が移動する時間は短い。そのため、最初の認証は短時間で終了することが望ましい。特徴量（特徴ベクトル）の比較による認証では、各特徴量の有効桁数が大きければ処理時間は長く、有効桁数が小さければ処理時間は短い。即ち、特徴量が秘密分散され、且つ、２段階の認証を行うような認証システムでは、最初の認証を短時間で終了させることを目的として特徴量の有効桁数を削減することが有効となる。

[0025] 上記説明したように、秘密計算の適用が好適なシステムには秘密にする数値の有効桁数を削減した後に本来の処理（例えば、人物特定処理）を行うことが許容されるシステムが存在する。ここで、秘密計算を用いない通常の処理では、数値の有効桁数を削減することは比較的容易である。例えば、４桁

で表現される数値である「７」の桁数を１つ削減する場合を考える。この場合、数値「７」を２進数表記すると「０ｂ０１１１」であり、上位３ビットを抽出すれば当該数値「７」の桁数削減が実現できる（数値７は数値３に変換される）。

[0026] しかし、秘密計算では当該秘密情報である数値７は、シェアとして各秘密計算サーバに分散されて配置されている。そのため、当該秘密にされた数値７を２進数表記する際には、非特許文献１に開示された「ビット分解」と称される処理が必要となる。さらに、ビット分解された数値７の上位３ビットの抽出及び再配置には、非特許文献１に開示された「ビット結合（環合成プロトコル）」と称される処理が必要である。非特許文献１に開示されるように、上記ビット分解やビット結合を実行するためには各秘密計算サーバ間の連携（通信）が必要であり、当該処理には相応の実行時間が必要となる。

[0027] 秘密情報の有効桁数を削減する際、上記通常の計算で使用されるアルゴリズムを秘密計算に持ち込むとビット分解やビット結合が必要となり、秘密情報の有効桁数を削減してもシステム全体として期待した程の効果（実行速度の向上）が得られない可能性がある。さらに、場合によっては、有効桁数の削減に要する実行時間の増加が情報の有効桁数を削減したことによる実行時間の減少を上回る事態もあり得る。即ち、秘密計算では、秘密にされた数値に対する任意の演算が可能であるが、秘密情報が各秘密計算サーバに分散配置されているという特殊性から通常の計算で使用されるアルゴリズムを使用すると却ってシステムの性能を落とす可能性がある。

[0028] 図１に示す一実施形態に係る秘密計算サーバ１００は、上記秘密計算の特殊性を鑑み、秘密情報の有効桁数を実質的にシステムの実行時間に影響を与えることなく削減する。具体的には、秘密計算サーバ１００は、秘密情報の有効桁数を削減する必要がある場合に、当該秘密情報の有効桁数が減る方向に当該秘密情報から生成されたシェア（秘密情報に対応するシェア）に対してシフト演算を実行する。例えば、秘密計算サーバ１００は、削減する桁数に相当する数の右シフト演算を桁数削減の対象となるシェアに対して実行す

る。

[0029] 上記説明したように、乗算等の処理には秘密計算サーバ間の通信が必要であるが、シェアに対するシフト演算には当該サーバ間の通信は不要である。そのため、桁数削減（上位ビットの切り出し）に要する実行時間は短く、秘密情報の桁数を削減したことによる効果を最大限享受できる。即ち、秘密計算サーバ１００は、短時間で秘密情報の有効桁数を削減でき、当該有効桁数の削減によりシステム全体の実行時間を短縮することができる。

[0030] なお、上記シフト演算の実行により一部情報が破棄されるため有効桁数削減に伴う誤差の増大が懸念される。しかし、シフト演算により生じる誤差は、シフト量（右シフトする桁数）に依らず秘密計算サーバ１００の台数に応じた値に制限される。例えば、３台の秘密計算サーバ１００にて秘密計算を実行する場合には、シフト演算により有効桁数を削減することにより生じ得る誤差は、高々「－２」に制限される。即ち、シフト演算により有効桁数の削減を行うと、絶対値として最大「２」の誤差が生じ得るが、当該誤差の大きさは秘密情報の値が十分大きければその影響は軽微であると言える。つまり、秘密情報からシェアを生成する際の自然数Ｎが十分大きく、右シフトする桁数が相対的に小さければ有効桁数削減に伴う誤差は小さく、その影響も小さい。

[0031] シフト演算により有効桁数を削減した際に生じる誤差が上記のように制限される理由は以下のとおりである。

[0032] 秘密計算サーバ１００の台数をＫ（Ｋは自然数、以下同じ）とする。この場合、秘密情報Ｓから、Ｋ個のシェア｛s_1、s_2、・・・、s_K｝が生成される。シェアを生成する際の法Ｎは２の冪数（2^n）とする。なお、法Ｎは２の冪数に代えて素数であってもよい。上記条件の下、各シェアは下記の式（１）のように２進数表記できる。

[0033] ［式１］

$$s_1 = a_{(1,n)}、\cdots、a_{(1,i+1)}、a_{(1,i)}、\cdots、a_{(1,1)}$$

$$s_2 = a_{(2,n)}、\cdots、a_{(2,i+1)}、a_{(2,i)}、\cdots、a_{(2,1)}$$

⋮

$s_K = a_{(K、n)}、\cdots、a_{(K、i+1)}、a_{(K、i)}、\cdots、a_{(K、1)}$

[0034] なお、上記式（１）において、ｉは２進数表記（ビット分解）されたシェアのビット位置を特定するためのサフィックス（インデックス）である。

[0035] 上記式（１）において、ｎ桁の秘密情報Ｓの有効桁数をｉ桁削減する場合について考える。式（１）において、各シェアのｉ桁より上位のビットが示す数値S_Uを下記の式（２）のとおり表記する。

[0036] ［式２］

$S_{(1、U)}$＝上位ビット｛$a_{(1、n)}、\cdots、a_{(1、i+1)}$｝の数値

$S_{(2、U)}$＝上位ビット｛$a_{(2、n)}、\cdots、a_{(2、i+1)}$｝の数値

⋮

$S_{(K、U)}$＝上位ビット｛$a_{(K、n)}、\cdots、a_{(K、i+1)}$｝の数値

[0037] 同様に、各シェアのｉ桁以下の下位ビットが示す数値S_Lを下記の式（３）のとおり表記する。

[0038] ［式３］

$S_{(1、L)}$＝下位ビット｛$a_{(1、i)}、\cdots、a_{(1、1)}$｝の数値

$S_{(2、L)}$＝下位ビット｛$a_{(2、i)}、\cdots、a_{(2、1)}$｝の数値

⋮

$S_{(K、L)}$＝下位ビット｛$a_{(K、i)}、\cdots、a_{(K、1)}$｝の数値

[0039] 桁数が削減された後の秘密情報Ｓ’は下記の式（４）として算出できる。

[0040] ［式４］

$S_{(1、U)} + S_{(2、U)} + \cdots + S_{(K、U)} \mod (n-i)$

[0041] 式（４）は、ｉ桁よりも上位のビットから定まる数値の総和を桁数削減後の桁数（ｎ－ｉ）で除算した結果の余りが秘密情報Ｓ’となることを示す。

[0042] 式（２）及び式（３）の表記を利用すると、秘密情報Ｓは下記の式（５）として表現できる。

[0043] ［式５］

$S_{(1、U)} + S_{(1、L)} + \cdots + S_{(K、U)} + S_{(K、L)} \mod N$

[0044] 式（４）及び（５）を参照すると、本来、各シェアのｉ桁以下の数値の加算によりｉ桁より上位に桁上がりする値が有効桁数の削減により失われるので、当該桁上がりする数値が有効桁数の削減に伴う誤差となることが分かる。また、ｉ桁より上位に桁上がりする数値の最大値は式（３）に示す各数値が最大の場合であり、桁上がりする数値の最小値は式（３）に示す各数値が最小の場合であることが分かる。式（３）に示す各数値が最大とは、２進数表記した各数値の全ビットが「１」の場合である。Ｋ台の秘密計算サーバ１００により秘密計算が行われる場合には、桁上がりする数値の最大値は「Ｋ－１」であり、当該値が最大誤差の絶対値となる。例えば、Ｋ＝３とすれば、誤差の絶対値は「２」となる。

[0045] なお、上記説明から明らかなとおり、有効桁数の削減により生じる誤差は、有効桁数の削減により上位の数値に加算される予定であった値である。従って、変換値（桁上がりする値が切り捨てられた値）から真値（正しく桁上がりが反映された値）の差分値（誤差）は、負の値となる。

[0046] 以下、具体的な数値例を参照しつつ、秘密計算サーバ１００による秘密情報Ｓの有効桁数削減について説明する。その際、秘密情報Ｓは４ビットの値（Ｎ＝１６、ｎ＝４）とし、当該４ビットの情報Ｓを３ビットの値（Ｎ＝８、ｎ＝３）に変換する場合について説明する。また、秘密計算サーバ１００の台数は「３」とし、秘密情報Ｓは「７」とする。この場合、数値「３」が誤差なく有効桁数が削減された値となる。

[0047] ［数値例１］

秘密情報Ｓが「７」の場合、例えば、下記に示すように３つのシェアが生成される。なお、各数値の２進数を括弧により併記する。

[0048] s_1＝５（０ｂ０１０１）

s_2＝７（０ｂ０１１１）

s_3＝１１（０ｂ１０１１）

[0049] 各秘密計算サーバ１００は、４ビットの秘密情報Ｓを３ビットの秘密情報Ｓ’に変換するため、自身が保有するシェアを１ビット右シフトする。当該

シフト演算の結果得られるシェアは以下のとおりとなる。

s_1'＝２（０ｂ０１０）

s_2'＝３（０ｂ０１１）

s_3'＝５（０ｂ１０１）

[0050] この場合、有効桁数が削減された後の秘密情報Ｓ’は、$s_1'+s_2'+s_3'$ ｍｏｄ ８＝２（０ｂ０１０）として計算される。従って、当該数値例１のようにシェアが作成された場合には、誤差として「－１」が発生する。

[0051] ［数値例２］

数値例１と同様に秘密情報Ｓが「７」の場合、各シェアが以下のように生成されることもあり得る。

[0052] s_1＝６（０ｂ０１１０）

s_2＝７（０ｂ０１１１）

s_3＝１０（０ｂ１０１０）

[0053] 各秘密計算サーバ１００は、自身が保有するシェアを１ビット右シフトする。当該シフト演算の結果得られるシェアは以下のとおりとなる。

s_1'＝３（０ｂ０１１）

s_2'＝３（０ｂ０１１）

s_3'＝５（０ｂ１０１）

[0054] この場合、有効桁数が削減された後の秘密情報Ｓ’は、$s_1'+s_2'+s_3'$ ｍｏｄ ８＝３（０ｂ０１１）として計算される。従って、当該数値例２のようにシェアが作成された場合には、誤差は生じない。

[0055] 以下に具体的な実施の形態について、図面を参照してさらに詳しく説明する。

[0056] ［第１の実施形態］

第１の実施形態について、図面を用いてより詳細に説明する。第１の実施形態では、人流分析システムに有効桁数の削減を適用する場合について説明する。

[0057] 図２は、本発明の第１の実施形態の人流分析システムの構成を示す図であ

る。図２を参照すると、第１の装置２１と、第２の装置２２と、３台の秘密計算サーバ３０に、制御装置１０を接続した構成が示されている。

[0058] 第１の装置２１は、第１の地点で取得された第１の移動体の識別情報として、駅や各種の施設に設置されたカメラにて取得された画像から得られた通行人の顔特徴データを保持する装置である。

[0059] 第２の装置２２は、第２の地点で取得された第２の移動体の識別情報として、第１の地点とは異なる駅や各種の施設に設置されたカメラにて取得された画像から得られた通行人の顔特徴データを保持する装置である。

[0060] ここで、第１の装置２１と第２の装置２２とは、互いに異なる管理主体（同一組織内でデータ管理責任者が異なる場合を含む。）によって管理されているものとする。また、第１の移動体の識別情報と第２の移動体の識別情報は、それぞれデータを外部に出さないように管理・運用されているものとする。即ち、前記第１、第２の移動体の識別情報は、それぞれの別の管理主体の下で取得されたデータであり、外部に出さない、一定期間経過後に破棄する等の条件の下に管理されている。

[0061] ３台の秘密計算サーバ３０は、第１の装置２１、第２の装置２２からそれぞれ、顔特徴データを秘密分散したシェア情報を受け取って、秘密分散方式の計算を行うサーバである。

[0062] 制御装置１０は、第１の装置２１、第２の装置２２に対し、秘密計算サーバ３０へのシェア情報の送信、及び、秘密計算サーバ３０に対し、シェア情報を用いた計算等を指示する装置である。さらに、制御装置１０は、各秘密計算サーバ３０に対する顔特徴データの有効桁数調整機能を備える。例えば、当該有効桁数調整機能による調整は、顔特徴データである特徴ベクトルの各要素値における所定桁数以下の切り捨てである。

[0063] 図３は、本発明の第１の実施形態の人流分析システムの第１の装置の構成を示す図である。図３を参照すると、タイマ２１２と、特徴量抽出部２１３と、特徴量保存部２１４と、秘密分散部２１５とを備え、カメラ２１１と接続された構成が示されている。

[0064] カメラ２１１は、駅や各種の施設に設置された防犯カメラ等である。タイマ２１２は、撮影日時を記録するために用いられる。なお、図３の例では、カメラの台数は１台であるが、カメラの台数に制限はない。例えば、日中撮影用のカメラと、夜間撮影用のカメラを切り替えて動画データを取得可能な構成であってもよい。また例えば、画角や撮影方向の異なるカメラが複数配置された構成であってもよい。

[0065] 特徴量抽出部２１３は、カメラ２１１にて撮影された動画データから画像を切り出して、その中に写りこんでいる人物の顔特徴データを抽出する。なお、１つの画像に複数の人物の顔が写りこんでいる場合、特徴量抽出部２１３は、１つの画像からそれぞれの人物の顔の領域を特定し、複数の顔特徴データを抽出する。

[0066] 特徴量保存部２１４は、特徴量抽出部２１３にて抽出された顔特徴データにタイマ２１２から取得した日時情報を対応付けて保存する。

[0067] 図４は、特徴量保存部２１４にて保存されている顔特徴データの一例を示す図である。図４の例では、タイマ２１２から供給された日時と、顔の特徴量情報（顔特徴データ）とを対応付けたエントリを保存している例が示されている。顔の特徴量情報の１１，２３，４５・・・は、予め定めた顔特徴（顔ノード）間の特徴ベクトルを表している。

[0068] 秘密分散部２１５は、制御装置１０からの要求に応じて、特徴量保存部２１４から顔特徴データを取り出して、秘密計算サーバ３０への送付用のシェア情報を生成し、秘密計算サーバ３０に送信する。

[0069] 上記のような第１の装置２１は、同一組織（施設）における顔認証データを用いた人流分析を行う装置に、秘密分散部２１５を追加したことでも実現できる。また、第２の装置２２は、少なくともカメラ２１１と撮影領域が異なるカメラを備えるほかは、第１の装置２１と同一の構成であるため、説明を省略する。

[0070] 続いて、制御装置１０の構成について図面を参照して詳細に説明する。図５は、本発明の第１の実施形態の人流分析システムの制御装置の構成を示す

図である。図５を参照すると、要求部１１と、決定部１２、指示部１３とを備えた構成が示されている。

[0071] 要求部１１は、予め設定された人流分析開始条件に基づいて、第１、第２の装置２１、２２に対し、秘密計算サーバ３０への送付用のシェア情報の生成と送信を要求する。人流分析開始条件としては、一定の時間毎に、過去一定期間に第１、第２の地点で撮影された動画に基づく、特定の精度の人流分析を行うといった条件が考えられる。また、人流分析開始条件としては、上記のような定期的なものだけでなく、例えば、ユーザから臨時的な人流分析を求める明示的な指示の受信を条件としてもよい。

[0072] 決定部１２は、システムの状況やユーザからの指示に応じて、各秘密計算サーバ３０が人流分析に使用するシェア情報（移動体の識別情報）の有効桁数を決定する。決定部１２は、当該決定した有効桁数を指示部１３に通知する。例えば、桁数の削減を行わない場合（第１、第２の装置２１、２２から供給されたシェア情報をそのまま使う場合）の人流分析の所要時間が３０分である一方、ユーザから要求された人流分析の処理速度（所要時間）が１５分である場合が想定される。この場合、決定部１２は、各秘密計算サーバ３０が秘密計算に使用するシェア情報（顔特徴データをなす特徴ベクトルの各要素）の有効桁をＸ桁からＹ桁に決定する。なお、決定部１２による有効桁数の決定は、システムに求められる処理時間と有効桁数削減により得られる効果（短縮時間）との関係を予め観測し、当該関係を制御装置１０に格納しておくことで実現できる。あるいは、システムに求められる処理時間を入力、有効桁数削減により得られる短縮時間を出力するような関数を定義し、当該関数を用いて有効桁数が決定されてもよい。

[0073] このように、決定部１２は、秘密計算サーバ３０によるシェア情報（移動体の識別情報）を用いた処理が所定の時間以内（上記の例では１５分以内）に終了するようにシェア情報の有効桁数を決定する。

[0074] 指示部１３は、上記要求部１１によるシェア情報を生成と送信が完了したタイミングで、秘密計算サーバ３０に秘密計算処理の実行を指示する。その

際、指示部１３は、上記決定部１２が決定した有効桁数に関する情報を人流分析実行指示に含め、当該情報を秘密計算サーバ３０に通知する。例えば、指示部１３は、有効桁数そのものを通知してもよいし、秘密計算サーバ３０にて削減する桁数を通知してもよい。後者の場合、指示部１３は、各秘密計算サーバ３０にて削減する有効桁数を算出し、当該算出した削減する有効桁数を人流分析実行指示に含める。上述のように、Ｘ桁からＹ桁に有効桁数が変更になった場合には、指示部１３は、（Ｘ－Ｙ）桁の桁数削減を各秘密計算サーバ３０に指示する。

[0075] なお、第１の装置２１、第２の装置２２はそれぞれ異なる管理主体により管理されているため、各装置が送信するシェア情報の桁数が同じとは限らず異なる場合もありうる。このような場合、制御装置１０は、各装置から供給されるシェアの有効桁数が同じとなるように、各装置から得られるシェアのそれぞれについて削減する有効桁数を指示してもよい。例えば、制御装置１０は、第１の装置２１から取得したシェアに対してはX_1-Y_1桁の削減、第２の装置２２から取得したシェアに対してはX_2-Y_2桁の削減を各秘密計算サーバ３０に対して指示してもよい。

[0076] 続いて、秘密計算サーバ３０の構成について図面を参照して詳細に説明する。図６は、本発明の第１の実施形態の人流分析システムの秘密計算サーバの構成を示す図である。図６を参照すると、秘密計算実行部３１を備える構成が示されている。

[0077] 秘密計算実行部３１は、第１、第２の装置２１、２２からシェア情報（顔特徴データ、特徴ベクトル）を取得する。また、秘密計算実行部３１は、制御装置１０から「人流分析実行指示」を取得する。秘密計算実行部３１は、人流分析実行指示に含まれる有効桁数に関する情報を確認する。当該情報に削減する有効桁数が記載されていれば、秘密計算実行部３１は、当該有効桁数の削減数に相当する数の右シフト演算をシェア情報に対して実行する。あるいは、人流分析指示に有効桁数そのものが含まれる場合には、秘密計算実行部３１は、現状の有効桁数と指示に含まれる有効桁数の差分を計算し、当

該差分値に相当する桁数の右シフトをシェア情報に対して実行する。

[0078] 有効桁数の調整の後、秘密計算実行部３１は、シェア情報を用いた人流分析に係る処理を実行する。

[0079] なお、秘密計算実行部３１は、制御装置１０等から予め取得した秘密計算回路（秘密計算プログラム）を実行することで上記有効桁数の削減処理を含む人流分析を行う。

[0080] 続いて、本実施形態の動作について図面を参照して詳細に説明する。図７は、本発明の第１の実施形態の人流分析システムの動作を表したシーケンス図である。

[0081] 図７を参照すると、まず、第１、第２の装置２１、２２において、それぞれ特徴量データ（顔特徴データ）の蓄積が行われる（ステップＳ００１ａ、Ｓ００１ｂ）。

[0082] その後、前記所定の人流分析開始条件が成立すると（ステップＳ００２）、制御装置１０は、第１、第２の装置２１、２２に対して、それぞれ秘密計算サーバ３０へのシェア情報の送信を指示する（ステップＳ００３）。

[0083] 第１、第２の装置２１、２２は、制御装置１０からの指示に基づいて、特徴量保存部２１４から顔特徴データを取り出して、秘密計算サーバ３０への送付用のシェア情報を生成し、秘密計算サーバ３０にそれぞれ送信する（ステップＳ００４ａ、Ｓ００４ｂ）。

[0084] 次に、制御装置１０は、秘密計算サーバ３０に対して、シェア情報による人流分析の実行を指示する（人流分析実行指示；ステップＳ００５）。その際、制御装置１０は、当該実行指示に有効桁数に関する情報（有効桁数情報）を含める。

[0085] 次に、秘密計算の実行指示を受けた秘密計算サーバ３０が互いに連携してシェア情報による人流分析処理を実行する（ステップＳ００６）。その際、各秘密計算サーバ３０は、制御装置１０から指示された有効桁数の調整を行う。例えば、各秘密計算サーバ３０は、指示された桁数の右シフト演算をシェア情報に対して行う。なお、人流分析処理の具体例については後に図８～

図１１を用いて詳細に説明する。

[0086] 最後に、秘密計算サーバ３０は、人流分析の結果（計算結果）を制御装置１０に送信する（ステップＳ００７）。なお、図７の例では、秘密計算サーバ３０が人流分析の結果（計算結果）を制御装置１０に送信することとしているが、人流分析の結果（計算結果）の送信先は、制御装置１０以外でもよい。例えば、顔特徴データの提供元である第１、第２の装置２１、２２に、人流分析の結果（計算結果）を送信してもよい。これにより、第１、第２の装置２１、２２の管理主体は、人流分析の結果（計算結果）に基づいて、施設の運用や、来訪者に対する案内表示の改善に役立てることができる。また、第１、第２の装置２１、２２の管理主体は、顔特徴データを互いに渡すことなく、前記人流分析の結果（計算結果）を得ることができる。

[0087] 続いて、上記ステップＳ００６における人流分析処理の具体例について説明する。

［移動人数の集計］

図８は、地点１のカメラに現れた人物と、地点２のカメラに現れた人物とのマッチングを行う例を示している。例えば、図８に示すように、２０１８／１／１１　１１：００－１１：３０の間の顔特徴データを照合することで、地点１と地点２間を移動した人数を計算することができる。秘密分散方式を用いることで、個々の秘密計算サーバ３０において、元の顔特徴データを復元できないようにしたまま、所望の計算処理を行わせることができる。例えば、地点１がＡ駅であり、地点２が、Ｂ球場（Ｂスタジアム）である場合、それぞれの管理主体が、Ａ駅で取得された顔特徴データと、Ｂ球場（Ｂスタジアム）で取得された顔特徴データを秘密にしたまま、Ａ駅からＢ球場（Ｂスタジアム）にＸＸ人移動したといった結果を得ることができる。また、この移動人数の集計結果は、個人情報を含まないため、第三者に有償で販売することなども可能となっている。なお、この顔特徴データの照合は、２つの特徴ベクトル間の距離を求め、その値を所定の閾値と比較することで実施することができる。

[0088] ［所要時間の集計］

図９は、地点１のカメラに現れた人物と、地点２のカメラに現れた人物とのマッチングを行って、データを結合し、所要時間の集計を行う例を示している。例えば、図９に示すように、特定の時間帯の顔特徴データを照合することで、地点１と地点２の双方に出現した人物を特定することができる。そして、その人物が撮影された時間の差により、当該人物が地点１と地点２間の移動に要した時間を求めることができる。同様に、例えば、地点１がＡ駅であり、地点２が、Ｂ球場（Ｂスタジアム）である場合、それぞれの管理主体がそれぞれ管理する顔特徴データを秘密にしたまま、Ａ駅からＢ球場（Ｂスタジアム）に移動した人の平均所要時間がＸＸ分であるといった結果を得ることができる。また、この所要時間の集計結果は、個人情報を含まないため、第三者に有償で販売することなども可能となっている。また、このとき、図９に示すように、結合データには、顔特徴データが削除され、個体を特定できないようになっていることが好ましい。

[0089] ［人流分析］

図１０は、地点１のカメラに現れた人物と、地点２のカメラに現れた人物とのマッチングを行って、データを結合し、人物毎の所要時間のリストを作成する例を示している。さらに、図１０の例では、作成した人物毎の所要時間のリストから人流分析を行った結果を作成している。図１１の人流分析を行った結果の例では、人物毎の所要時間のリストを用いて、地点１から地点２に移動した人数やその平均移動時間といった情報を得ることが可能となっている。このとき、図１０、図１１に示すように、分析結果からは、顔特徴データが削除され、かつ、Ｎｏ．１、Ｎｏ．２といった匿名化処理により個体を特定できない処理がなされていることが好ましい。同様に、例えば、地点１がＡ駅であり、地点２が、Ｂ球場（Ｂスタジアム）である場合、それぞれの管理主体がそれぞれ管理する顔特徴データを秘密にしたまま、Ａ駅からＢ球場（Ｂスタジアム）に移動した人がＸＸ人いて、その平均所要時間がＸＸ分であるといった結果を得ることができる。そしてこのような情報は、警

備員や案内員の最適配置によるセーフティ、おもてなし、観光客の行動傾向分析に基づく観光・街づくり等に役立てることができる。従って、本発明の人流分析システムは、移動体の移動に関する各種の分析をなしうるシステムとして機能するといえる。

[0090] なお、上記図８から図１０において同一人物として判定する閾値（一致率）は、求められる精度やカメラの解像度等に応じて適宜設定することができる。例えば、図１０では８５％以上の一致率が得られた場合に、同一人物として判定しているが、より厳密な判定が求められる場合には、一致率が９０％以上である場合に同一人物と判定するようにしてもよい。また、カメラの解像度が低かったり、撮影場所が暗く画質が低下している場合には、一致率が７０％以上である場合に同一人物と判定するようにしてもよい。このように、閾値（一致率）は、顔特徴データの精度（品質）や求められる分析結果の精度等に応じて調整することができる。

[0091] なお、上記した例では、顔特徴データは、日時情報を対応付けて保存されているものとして説明したが、顔特徴データの個々に日時情報を対応付けなくてもよい。例えば、一定の時間帯に認識された顔特徴データを、特徴量保存部２１４に保持させる構成であってもよい。

[0092] また、本実施形態によれば秘密計算サーバ３０が使用するシェア情報の桁数を調整することで、要求される処理速度、処理精度を満足する人流分析の結果を提供することが可能となる。例えば、地点２の警備の強化の必要人員を見積もるため、地点１（第１の地点）から地点２（第２の地点）の直近３０分の人流を１５分以内に把握したいといった用途に、本実施形態は好適に適用することができる。同様に、例えば、地点１のイベント会場で販売する商品の量を見積もるため、地点２（第２の地点）から地点１（第１の地点）の直近１時間の人流を１０分以内に把握したいといった用途にも、本実施形態は好適に適用することができる。

[0093] また、処理時間を短縮するという観点のほか、プライバシ保護の観点からあえて人物の同一性判定に関する精度を落としたいというニーズも想定され

る。この場合も同様に、顔特徴データの有効桁数を削減するといった処理を行うことで、人物の同一性判定の精度を落とすことができる。

[0094] ［第２の実施形態］

第２の実施形態について、図面を用いてより詳細に説明する。第２の実施形態では、認証システムに有効桁数の削減を適用する場合について説明する。

[0095] 図１２は、本発明の第２の実施形態の認証システムの構成を示す図である。図１２を参照すると、カメラ２が接続された認証装置４０と、カメラ１が接続された認証候補抽出装置５０と、３台の秘密計算サーバ６０とが接続された構成が示されている。認証候補抽出装置５０に接続されたカメラ１は第１の地点に設置され、認証装置４０に接続されたカメラ２は第２の地点に設置される（図１３参照）。

[0096] 認証候補抽出装置５０は、第１の地点から第２の地点へ移動する被認証体について、第１の地点において取得された生体情報を入力する。認証候補抽出装置５０は、被認証体の認証処理用の特徴情報を記憶する。例えば、被認証体が旅客である場合、第２の地点は、駅の改札前のカメラなどの旅客の生体情報の取得位置である。

[0097] 認証装置４０は、上記第２の地点において取得された被認証体の生体情報を用いて認証処理を行って、当該旅客に改札等を通過させてよいか否かを決定し、駅の改札のゲートを制御する。即ち、認証装置４０が認証処理を行う対象は、認証候補抽出装置５０にて抽出された候補となる。このように、第２の実施形態に係る認証システムでは、認証候補抽出装置５０で候補を絞り込み、認証装置４０が、この絞り込まれた候補を用いて認証を行う構成となっている。なお、第１の地点としては、駅の改札より手前の旅客が通過する可能性が高い場所（通路や階段）が選択される（図１３のカメラ１参照）。なお、上記の例はあくまで一例であり、被認証体と認証装置は、上記旅客と改札に限定されない。

[0098] 図１２を参照すると、認証装置４０は、第２の地点において取得された生

体情報を入力する特徴量抽出部４０１と、認証候補抽出装置５０から受信した特徴情報の候補と、前記第２の地点に設定されたカメラ２で撮影された画像から抽出した特徴情報を用いて、認証処理を行う認証処理部４０２と、を備える。そして、認証装置４０は、認証候補抽出装置５０から送信された特徴情報を用いて、カメラ２にて撮影された画像に写っている人物を特定する生体認証を行う。なお、このような特徴量抽出部４０１はカメラ２側に配置されていてもよい。この場合、特徴量抽出部４０１は、生体情報入力部として機能する。

[0099] なお、認証装置４０は、認証候補抽出装置５０から送信された特徴情報を所定のタイミングで破棄するものとする。このタイミングとしては、認証候補抽出装置５０から送信された特徴情報に適合する人物の認証に成功した場合と、認証候補抽出装置５０から送信された特徴情報に適合する人物が所定期間検出されなかった場合が考えられる。このようにすることで、認証装置４０に個人情報（特徴情報）が必要以上に長い時間保持される事態を防ぐことが可能となる。

[0100] また、以下の説明では、認証候補抽出装置５０から送信された特徴情報は顔認証用の特徴情報であり、認証装置４０は、いわゆる顔認証を行うものとして説明する。もちろん、本発明の適用範囲は顔認証に限られず、その他の生体情報による認証にも適用可能である。

[0101] 認証候補抽出装置５０は、特徴量抽出部５０１と、秘密分散制御部５０３と、特徴情報送信部５０４と、処理性能調整部５０５とを備える。

[0102] 特徴量抽出部５０１は、カメラ１にて撮影された画像から人の顔の部分を切り出し、その特徴量を抽出し、抽出した特徴量を並べて構成した特徴情報を構成して、秘密分散制御部５０３に送る。なお、１つの画像に複数の人物の顔が写りこんでいる場合、特徴量抽出部５０１は、１つの画像からそれぞれの人物の顔の領域を特定し、複数の特徴情報を計算する。また、このような特徴量抽出部５０１はカメラ１側に配置されていてもよい。この場合、特徴量抽出部５０１は、生体情報入力部として機能する。

[0103] 秘密分散制御部５０３は、特徴量抽出部５０１から受け取った特徴情報から秘密分散によるシェア情報を生成し、秘密計算サーバ６０に向けて当該シェア情報を送信する。さらに、秘密分散制御部５０３は、秘密計算サーバ６０に対して当該シェア情報を用いた計算を指示する。より具体的には、秘密分散制御部５０３は、秘密計算サーバ６０に対し、秘密計算サーバ６０がそれぞれ保持している人物データの中から、シェア情報として送信した人物の特徴と類似する特徴を持つ人物、即ち、認証処理用の特徴情報の候補の選択を指示する。

[0104] 秘密分散制御部５０３は、秘密計算サーバ６０から選択結果（認証処理用の特徴情報の候補）を受け取ると、特徴情報送信部５０４に認証装置４０への送信を指示する。なお、認証処理用の候補の数は、認証装置４０の応答性能に影響の無い範囲で最大値を採る方法や、所定の計算方法で計算した類似度が一定値以上である候補のみを選択する方法など種々の方法を採ることができる。また、秘密分散制御部５０３側で、認証処理用の候補の数を指定し、秘密計算サーバ６０側で指定された数の認証処理用の候補を抽出する方法も採用できる。

[0105] また、秘密分散制御部５０３が、認証装置４０に送信する認証処理用の候補となる特徴情報として、特徴量抽出部５０１にて抽出された特徴情報を送信してもよい。このようにすることで、認証装置４０において、人物の服装や髪形を用いた認証の精度を高めることが可能となる。

[0106] また、秘密分散制御部５０３は、秘密計算サーバ６０に実行させるための秘密計算回路（秘密計算プログラム）を配布する機能を備えていても良い。

[0107] 特徴情報送信部５０４は、認証装置４０に対し、秘密分散制御部５０３から受け取った認証処理用の特徴情報の候補を送信する。

[0108] 処理性能調整部５０５は、被認証体が第１の地点から第２の地点へ到達する予測時間に基づいて、認証装置４０における認証処理に間に合う範囲で所定の要求精度を満たす候補を抽出できるよう、秘密計算サーバ６０における秘密計算処理の性能を調整する。具体的には、処理性能調整部５０５は、カ

メラ１にて撮影された人物が、カメラ２にて撮影されるまでの時間を予測し、その時間に間に合うように、認証候補の算出処理に用いるシェア情報の有効桁数に関する情報を秘密計算サーバ６０に通知する。なお、カメラ１にて撮影された人物が、カメラ２にて撮影されるまでの時間は、カメラ１とカメラ２間の距離と、人の平均移動速度により計算することができる。人の平均移動速度として、各時間帯における平均的な移動速度を用いても良い。また、前記時間の予測にあたって、カメラ１とカメラ２間に複数の経路がある場合は、これらの経路が利用される確率を考慮してもよい。また、カメラ１とカメラ２間にエスカレーターや動く歩道等の移動手段がある場合には、これらが利用される確率を考慮して、時間を計算してもよい。

[0109] 図１３は、本発明の第２の実施形態におけるカメラの配置例を示す図である。この場合、処理性能調整部５０５は、カメラ１とカメラ２間の距離Ｄ１と、人の平均移動速度により、人物が、カメラ１にて撮影された後、カメラ２にて撮影されるまでの時間を計算することができる。

[0110] 上述のように、秘密計算処理の速度を調整する方法としては、秘密計算サーバ６０側で、認証処理用の特徴情報の候補を抽出する際の特徴情報を構成する情報要素（特徴量）の桁数を増減する方法を採用することができる。

[0111] 処理性能調整部５０５は、カメラ間の距離と人の移動速度から秘密計算サーバ６０にて認証処理用の候補抽出のために許容される処理時間を計算する。その後、処理性能調整部５０５は、秘密計算サーバ６０が照合処理に用いている特徴情報（シェア情報）の有効桁数が現状値（例えば、初期値；桁数削減なし）の場合に、実際の秘密計算サーバ６０の処理時間が上記許容される処理時間を超えるか否かを判定する。当該判定を実現するにあたり、秘密計算サーバ６０が扱うシェア情報の有効桁数と秘密計算サーバ６０の処理時間の関係を予め観測し、認証候補抽出装置５０に予め格納しておく。その上で、処理性能調整部５０５は、当該予め格納された関係（有効桁数と処理時間の関係）を参照することで上記判定を行う。

[0112] 処理性能調整部５０５は、現状の有効桁数では上記計算した処理時間を超

えてしまうと判断した場合に、秘密計算サーバ６０が処理するシェア情報の有効桁数削減を決定する。具体的には、処理性能調整部５０５は、上記予め格納された有効桁数と処理時間の関係から秘密計算サーバ６０にて処理するシェア情報の有効桁数を決定する。処理性能調整部５０５は、決定した有効桁数に関する情報を秘密計算サーバ６０に通知する。例えば、処理性能調整部５０５は、有効桁数そのものを秘密計算サーバ６０に通知してもよいし、有効桁数の増減値を秘密計算サーバ６０に通知してもよい。例えば、後者の場合であって、Ｘ桁からＹ桁に有効桁数を削減する場合には、Ｘ－Ｙ桁の有効桁数削減が秘密計算サーバ６０に通知される。

[0113] 秘密計算サーバ６０は、それぞれ特徴情報記憶部６０１と、秘密計算実行部６０２とを備えている。

[0114] 特徴情報記憶部６０１は、認証装置４０における照合対象となりうる人物の特徴情報を秘密分散により秘匿化した状態で保持している（人物の特徴情報を第２のシェア情報として保持している）。図１４は、本実施形態で用いる特徴情報（秘匿処理前）の一例を示す図である。以下の説明では、特徴情報は、＜１１，２３，４５，・・・＞といった人の顔の特徴量（例えば、特徴点間の距離）を所定の順序で並べたものであるものとして説明する。また、以下の説明では、顔認証技術により、図１４のユーザＩＤｘｘｘｘ０００１～ｘｘｘｘ０００５の５名のいずれかを特定する例を挙げて説明する。

[0115] 秘密計算実行部６０２は、秘密分散制御部５０３及び処理性能調整部５０５からの指示に従い、カメラ１の地点において取得された生体情報が秘密分散されたシェア情報（第１のシェア情報）として送信された人物の特徴と類似する特徴を持つ人物、即ち、認証処理用の特徴情報の候補を選択し、秘密分散制御部５０３に送る。このように、秘密計算実行部６０２は、２つのシェア情報（カメラ１の情報から生成された特徴情報と特徴情報記憶部６０１に格納された特徴情報）を用いて、認証処理用の候補を選択する。

[0116] さらに、秘密計算実行部６０２は、認証候補抽出装置５０から通知されたシェア情報の有効桁数に関する情報に基づいて、認証候補抽出処理に用いる

２つのシェア情報に対してシフト演算を行う。

[0117] 本実施形態では、秘密分散制御部５０３と秘密計算サーバ６０が、認証装置４０における認証処理が所定の時間内に完了するように、前記認証処理用の特徴情報の候補の数を設定する候補選択部として機能することになる。

[0118] なお、図１２の例では、３台の秘密計算サーバ６０が示されているが、秘密計算サーバ６０の数は、必要な処理速度や耐障害性によって決定されるべき事項であり、その数に制限はない。

[0119] 続いて、本実施形態の動作について図面を参照して詳細に説明する。図１５は、本発明の第２の実施形態の認証システムの動作を表したシーケンス図である。図１５を参照すると、まず、カメラ１が認証候補抽出装置５０に撮影データを送信する（ステップＳ１０１）。なお、カメラ１は、人物を認識できた都度、認証候補抽出装置５０へ撮影データを送信することとしてもよいし、人物の認識有無に拘わらず、所定の時間間隔で撮影データを繰り返し送信するものしてもよい。

[0120] 前記撮影データを受信した認証候補抽出装置５０は、撮影データに写っている人物の顔画像の特徴量を抽出し、特徴情報を作成する（ステップＳ１０２）。

[0121] 次に、認証候補抽出装置５０は、抽出した特徴情報から、秘密計算サーバ６０に送信するシェア情報を作成し、各秘密計算サーバ６０に送信する。さらに、認証候補抽出装置５０は、秘密計算サーバ６０に対し、送信した人物の特徴と類似する特徴を持つ候補の抽出を指示する（ステップＳ１０３）。認証候補抽出装置５０は、秘密計算サーバ６０にて有効桁数の調整が必要と判断した場合には、有効桁数に関する情報も併せて秘密計算サーバ６０に通知する。

[0122] 前記指示を受け取った秘密計算サーバ６０は、認証候補抽出装置５０から受信したシェア情報を用いて、カメラ１に撮影された人物と類似する特徴を持つ人物の候補を選択する（ステップＳ１０４）。そして、秘密計算サーバ６０は、認証候補抽出装置５０に対して、計算結果（選択結果）を送信する

（ステップＳ１０５）。なお、秘密計算サーバ６０は、有効桁数に関する情報が通知されている場合には、例えば、特徴量に対して指定された桁数の削減（指定された桁数の右シフト演算）を実行した後にカメラ１に撮影された人物と類似する特徴を持つ人物の候補を選択する。

[0123] 前記選択結果を受信した認証候補抽出装置５０は、秘密計算サーバ６０から受信した情報を用いて認証処理用の候補となる特徴情報を復元し、認証装置４０に送信する（ステップＳ１０６）。

[0124] なお、上記ステップＳ１０６において、秘密計算サーバ６０から受信した情報を用いて復元した認証処理用の候補となる特徴情報に代えて、認証候補抽出装置５０が、カメラ１の画像から作成した特徴情報を送信するようにしてもよい。この場合は、秘密計算サーバ６０から受信した情報を用いて復元した認証処理用の特徴情報の候補に基づいて、カメラ１の画像から作成した特徴情報が特定される。また、この時、ステップＳ１０５において、類似する特徴を持つ人物の候補を選択する処理を行うのではなく、カメラ１に撮影された人物と同一人物と判断される人物がいるかどうかを判断する処理にしても良い。このようにすることにより、認証装置４０における顔認証処理が１対１認証となり、計算コストを削減することができる。

[0125] 一方、カメラ２は、認証装置４０に撮影データを送信する（ステップＳ１０７）。そして、認証装置４０は、所定の時間内に、認証候補抽出装置５０から受信した認証処理用の特徴情報の候補を用いて、カメラ２にて撮影された人物の顔認証を実施する（ステップＳ１０８）。

[0126] 上記認証システムの効果について図面を参照して詳細に説明する。図１６は、本発明の第２の実施形態の認証システムの動作を説明するための図である。例えば、図１６に示すように、特徴情報＜１０，２３，３３，・・・＞を持つ人物がカメラ１、２で撮影された例を挙げて説明する。

[0127] この人物が第１の地点に設置されたカメラ１にて撮影されると、認証候補抽出装置５０は、特徴情報＜１０，２３，３３，・・・＞を抽出し、秘密計算サーバ６０に認証処理用の候補の選択を指示する。

[0128] 前記指示を受けた秘密計算サーバ６０は、例えば、図１６に示すように、特徴情報＜１１，２３，４５，・・・＞を持つユーザＩＤ：ｘｘｘｘ０００１の人物と、特徴情報＜１０，２３，３３，・・・＞を持つユーザＩＤ：ｘｘｘｘ０００４の人物とを選択する。そして、認証候補抽出装置５０は、認証装置４０に対して、ユーザＩＤ：ｘｘｘｘ０００１と、ユーザＩＤ：ｘｘｘｘ０００４の特徴情報を送信する。これにより、認証装置４０が照合を行う人物の数は５人から２人に減ることになる。

[0129] 認証装置４０は、カメラ２にて撮影された画像から抽出された特徴情報＜１０，２３，３３，・・・＞と、前記ユーザＩＤ：ｘｘｘｘ０００１と、ユーザＩＤ：ｘｘｘｘ０００４の特徴情報とをそれぞれ照合し、類似度の高い方を選択する。図１６の例では、認証装置４０は、カメラ２にて撮影された人物は、ユーザＩＤ：ｘｘｘｘ０００４の人物であると判定している。上述したように、認証装置４０が照合を行う人物の数は高々２人であるので、認証装置４０は、カメラ２にて撮影された人物をその要求される応答時間内に認証することが可能となる。

[0130] ［第２の実施形態の変形例１］

続いて、カメラ１とカメラ２間の混雑度に応じて秘密計算サーバ６０の処理速度を調節するようにした第２の実施形態に係る変形例１について図面を参照して詳細に説明する。図１７は、本発明の第２の実施形態に係る変形例１の認証システムの構成を示す図である。図１２に示した構成との相違点は、認証候補抽出装置５０ａに混雑度判定部５０６が追加されている点である。その他の構成は図１２に示す構成と同様であるので、以下、その相違点を中心に説明する。

[0131] 混雑度判定部５０６は、特徴量抽出部５０１にて、カメラ１にて撮影された画像から切り出された人の顔の部分の数に応じて、混雑度を判定し、その結果を処理性能調整部５０５に送信する。例えば、混雑度判定部５０６は、１つの画像に、所定の閾値より少ない顔が写っている場合に、混雑度＝小と判定し、処理性能調整部５０５に、混雑度情報（混雑度＝小）を送信する（

図１８参照）。なお、図１７の例では、混雑度判定部５０６が、特徴量抽出部５０１から取得した情報に基づいて混雑度を判定する構成を採用しているが、混雑度判定部５０６が別のカメラと接続され、特徴量抽出部５０１と独立して混雑度を測定する構成も採用可能である。

[0132] 処理性能調整部５０５は、混雑度情報（混雑度＝小）を受信すると、カメラ１にて撮影された人物が、カメラ２にて撮影されるまでの時間が通常より短くなるものと予測する。そして、処理性能調整部５０５は、その時間に間に合うように、秘密計算サーバ６０における秘密計算処理の速度を調整する。

[0133] 例えば、図１８に示すように、カメラ１には小数の人が写っていたとする。この場合、少ない乗客が電車を下車して改札に向かうため、カメラ１に写っている人がカメラ２の位置に移動する時間は、混雑時よりも短くなる。この場合、秘密計算サーバ６０における時間的余裕は縮小するので、処理性能調整部５０５は、秘密計算サーバ６０に対し、通常より精度が落ちるが処理速度の速い計算方法による候補の選択を指示する。具体的には、処理性能調整部５０５は、秘密計算サーバ６０に対し、通常時よりも少ない有効桁数を用いた認証用の候補選択を指示する。

[0134] 続いて、本変形例１の動作について図面を参照して詳細に説明する。図１９は、本発明の第２の実施形態に係る変形例１の認証システムの動作を表したシーケンス図である。図１５に示したシーケンス図との相違点は、ステップＳ１０２の特徴量抽出の後、（混雑度による）処理性能調整処理（ステップＳ２０１）が追加されている点である。その他の処理は図１５のシーケンス図に示す処理と同様であるので、説明を省略する。

[0135] 以上説明したように、本変形例１によれば、カメラ１とカメラ２間の混雑度に応じて秘密計算サーバ６０の処理速度を調節し、認証装置４０における処理時間を最適化することが可能となる。即ち、本変形例は、特に、鉄道における改札システムに好適に適用できる。例えば、乗客数の少ない平日の昼間などは、混雑度が低くなるが、混雑度に応じ、旅客の移動速度は速くなる

ので、その時間を考慮して認証候補の迅速な算出が可能となる。

[0136] なお、上記変形例では、カメラ１にて撮影された画像から切り出された人の顔の数をカウントして、混雑度を判定するものとして説明したが、曜日や時間帯により混雑度が既知である場合には、これらの日時情報を用いて推定した混雑度を用いてもよい。また、カメラ１にて撮影された画像から切り出された人の顔の数と、日時情報との双方を用いて混雑度を計算してもよい。

[0137] また、混雑度による秘密計算処理の速度の調整は、あくまで一例であり、駅等の構造によっては、混雑度が低くても各人の移動所要時間は大きく変わらないという場合もある。逆に、ある程度、混雑してくると、各人の移動所要時間が大きく変わる場合もある。より望ましくは、直近の認証処理で得られた各人の実際の移動所要時間と混雑度に応じて適宜性能を調整する方法も採用可能である。

[0138] ［第２の実施形態の変形例２］

続いて、認証装置４０における認証処理の応答性能に応じて秘密計算サーバ６０の処理性能を調節するようにした第２の実施形態に係る変形例２について図面を参照して詳細に説明する。図２０は、本発明の第２の実施形態に係る変形例２の認証システムの構成を示す図である。図１２に示した構成との相違点は、認証候補抽出装置５０ｂに応答性能取得部５０７が追加されている点である。その他の構成は図１２に示す構成と同様であるので、以下、その相違点を中心に説明する。

[0139] 応答性能取得部５０７は、認証装置４０から、応答性能として、認証装置４０に特徴情報を送信してからその結果が得られるまでの平均応答時間を取得する。そして、応答性能取得部５０７は、取得した応答性能を処理性能調整部５０５に送信する。

[0140] 処理性能調整部５０５は、平均応答時間が所定の目標応答時間（閾値１）より長くなると、認証装置４０における応答時間が短くなるように、秘密計算サーバ６０における秘密計算処理の速度を調整する。また、処理性能調整部５０５は、平均応答時間が所定の目標応答時間（閾値２；但し閾値１≧閾

値２）より短くなると、認証装置４０における応答時間が長くなるように、秘密計算サーバ６０における処理性能を調整する。

[0141] 続いて、本変形例の動作について図面を参照して詳細に説明する。図２１は、本発明の第２の実施形態に係る変形例２の認証システムの動作を表したシーケンス図である。図１５に示すシーケンス図との相違点は、ステップＳ１０２の特徴量抽出の前に、（認証装置４０の応答性能による）処理性能調整処理（ステップＳ３０１）が追加されている点である。その他の処理は図１５のシーケンス図に示す処理と同様であるので、説明を省略する。

[0142] 図２２は、認証候補抽出装置５０ｂによる処理性能調整処理を表したフローチャートである。図２２を参照すると、認証候補抽出装置５０ｂは、例えば、平均応答時間が所定の目標応答時間（閾値１）より長くなっている場合（ステップＳ４０１のＹＥＳ）、認証装置４０における認証処理の計算コストが軽減されるように、秘密計算サーバ６０に候補選択処理の変更を指示する。例えば、処理性能調整部５０５は、秘密計算サーバ６０に対し、候補選択処理における特徴量の桁数を増大（例えば、初期値に復帰）を指示することで、より精度の高い候補の抽出を実現する。これにより、認証装置４０が照合を行う人物の数が減るため、認証装置４０における応答時間が短くなる。これにより、認証装置４０における処理遅れなどを未然に防止することが可能となる。

[0143] 一方、平均応答時間が所定の目標応答時間（閾値２）より短くなっている場合（ステップＳ４０２のＹＥＳ）、処理性能調整部５０５は、認証装置４０に処理能力に余裕があると判断する。この場合、処理性能調整部５０５は、秘密計算サーバ６０における候補選択処理に使用する特徴量の有効桁数を減少させることで、認証装置４０と、秘密計算サーバ６０の処理能力を平準化する。これにより、認証装置４０において特徴情報が保持される期間を最適化することが可能となる。一方で、上記処理により、認証装置４０が照合を行う人物の数が増え、認証装置４０の応答時間が増大することになるが、人物が第１の地点から第２の地点に移動する時間の範囲であれば問題はない

。

[0144] 以上説明したように、本変形例では、認証候補抽出装置５０ｂは、認証装置４０の認証処理の平均応答時間に応じて、秘密計算サーバ６０が認証処理用の候補の抽出に用いる特徴情報に含まれる特徴量の桁数を増減する。その結果、秘密計算サーバ６０における秘密計算処理の速度が最適化される。

[0145] なお、変形例２では、認証装置４０における認証処理の応答性能の指標として、平均応答時間を用いるものとして説明したが、平均応答時間に代えて、最大応答時間、応答時間の中央値や最頻値などを用いることも可能である。

[0146] 以上、第２の実施形態及び変形例について説明したが、他の変形も勿論可能である。

[0147] 例えば、上記した実施形態では、被認証体の識別情報として顔特徴データを用いるものとして説明したが、顔特徴データ以外の生体情報を用いた認証にも適用することも可能である。例えば、会社の入り口にて、上記したカメラ１を配置し、認証候補の絞込みを行ない、会社内のセキュリティエリアに配置したカメラ２による虹彩認証等を行う認証装置４０に認証処理の候補を送信する形態も採用可能である。

[0148] また、秘密計算サーバ６０における秘密計算処理の速度を調整することにより、認証処理用の候補の抽出処理の性能を調整するものとして説明したが、前記認証処理用の候補の抽出処理の性能の調整方法はこれに限られない。例えば、秘密計算の方式そのものを変更したり、秘密計算サーバ６０における秘密分散法による処理方式（アルゴリズムやパラメータ）を変更したりする方法も採用可能である。また、秘密計算サーバ６０を複数グループ用意し、それぞれに認証処理用の候補の抽出処理を分担させて、それぞれにより精度の高い候補の抽出処理を行わせる方法も採用可能である。

[0149] また、認証装置４０における認証処理として、秘密計算方式を用いることも可能である。

[0150] また、カメラ１における混雑度や認証装置４０の応答性能に基づいて、秘

密計算サーバ６０の処理性能を調節する例を挙げて説明したが、その他のパラメータを用いて、秘密計算サーバ６０の処理性能を調節してもよい。例えば、カメラ１で撮影された画像の品質としては、顔の向きや、表情、顔色、輝度（撮影時間による）等の違いがあり、これらは、撮影時間や顔の向きやカメラとの距離等によって変わりうる。このようなカメラ１で撮影された画像の品質に応じて、前記認証処理用の候補の選択に用いる特徴情報に含まれる特徴量の桁数を増減してもよい。例えば、カメラ１で撮影された画像中の被認証体の像が粗い場合、秘密計算サーバ６０の候補の選択精度も落ちることになる。この場合、処理性能調整部５０５は、秘密計算サーバ６０の候補の選択精度が変わらない範囲で、候補選択処理における特徴量の桁数を減少させればよい。これにより、秘密計算サーバ６０の計算リソースを他の被認証体の候補の抽出に当てることが可能となる。

[0151] また、認証候補抽出装置５０が、カメラ１にて撮影された顔画像を用いて認証処理用の候補を選択するものとして説明したが、カメラ１にて撮影された顔画像以外の情報を用いて、認証処理用の候補の絞り込みを行ってもよい。例えば、ある旅客の定期券や切符の情報などから、下車する駅が絞り込める場合は、これらの情報を用いて、認証処理用の候補の絞り込みを行ってもよい。

[0152] また、第２の地点が改札付近、第１の地点がその手前の通路や階段であるものとして説明したが、第１、第２の地点の組み合わせは、上記の例に限られない。例えば、ビルやイベント会場での入出場管理や港や空港等での入出場管理にも適用することができる。また、旅客が改札口から出ることを前提に、第２の地点が改札付近であるものとして説明したが、旅客が改札口から入るケースにも適用することができる。この場合、第２の地点が入場改札付近、第１の地点がその手前の通路や階段として選択される。

[0153] ［ハードウェア構成］

続いて、システムに含まれる各装置のハードウェア構成について説明する。

[0154] 図２３は、秘密計算サーバ１００のハードウェア構成の一例を示す図である。秘密計算サーバ１００は、所謂、情報処理装置（コンピュータ）により実現され、図２３に例示する構成を備える。例えば、秘密計算サーバ１００は、内部バスにより相互に接続される、ＣＰＵ（Central Processing Unit）１０１、メモリ１０２、入出力インターフェイス１０３、通信手段であるＮＩＣ（Network Interface Card）１０４等を備える。

[0155] 但し、図２３に示す構成は、秘密計算サーバ１００のハードウェア構成を限定する趣旨ではない。秘密計算サーバ１００は、図示しないハードウェアを含んでもよい。秘密計算サーバ１００に含まれるＣＰＵ等の数も図２３の例示に限定する趣旨ではなく、例えば、複数のＣＰＵ１０１が秘密計算サーバ１００に含まれていてもよい。

[0156] メモリ１０２は、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）、補助記憶装置（ハードディスク等）等である。

[0157] 入出力インターフェイス１０３は、図示しない入出力装置のインターフェイスである。入出力装置には、例えば、表示装置、操作デバイス等が含まれる。表示装置は、例えば、液晶ディスプレイ等である。操作デバイスは、例えば、キーボードやマウス等である。

[0158] 秘密計算サーバ１００の機能は、上述の処理モジュールにより実現される。当該処理モジュールは、例えば、メモリ１０２に格納されたプログラムをＣＰＵ１０１が実行することで実現される。また、そのプログラムは、ネットワークを介してダウンロードするか、あるいは、プログラムを記憶した記憶媒体を用いて、更新することができる。さらに、上記処理モジュールは、半導体チップにより実現されてもよい。即ち、上記処理モジュールが行う機能は、何らかのハードウェア、或いはハードウェアを利用して実行されるソフトウェアにより実現できればよい。

[0159] なお、各実施形態にて説明した秘密計算サーバ（３０、６０）や制御装置１０等も情報処理装置（コンピュータ）により実現可能であり、そのハードウェア構成は当業者にとって明らかであるため詳細な説明を省略する。

[0160] ［変形例］

なお、上記実施形態にて説明した秘密計算サーバやシステムの構成、動作は例示であって秘密計算サーバ等の構成、動作を限定する趣旨ではない。例えば、第１の実施形態では、制御装置１０から秘密計算サーバ３０に有効桁数に関する情報を通知しているが、当該情報を第１、第２の装置２１、２２を経由して当該情報を秘密計算サーバ３０に通知してもよい。この場合、第１、第２の装置２１、２２のそれぞれは、シェア情報を秘密計算サーバ３０に送信する際に有効桁数に関する情報を併せて通知すればよい。

[0161] あるいは、制御装置１０は、秘密計算サーバ３０に対して「人流分析」に費やすことができる時間や当該人流分析を終了させる時刻を通知し、秘密計算サーバ３０がこれらの情報に基づいて自立的に有効桁数の調整（削減）を行ってもよい。

[0162] なお、引用した上記の特許文献等の各開示は、本書に引用をもって繰り込むものとする。本発明の全開示（請求の範囲を含む）の枠内において、さらにその基本的技術思想に基づいて、実施形態ないし実施例の変更・調整が可能である。また、本発明の全開示の枠内において種々の開示要素（各請求項の各要素、各実施形態ないし実施例の各要素、各図面の各要素等を含む）の多様な組み合わせ、ないし、選択（部分的削除を含む）が可能である。すなわち、本発明は、請求の範囲を含む全開示、技術的思想にしたがって当業者であればなし得るであろう各種変形、修正を含むことは勿論である。特に、本書に記載した数値範囲については、当該範囲内に含まれる任意の数値ないし小範囲が、別段の記載のない場合でも具体的に記載されているものと解釈されるべきである。

符号の説明

[0163] １０ 制御装置

１１ 要求部

１２ 決定部

１３ 指示部

２１　第１の装置

２２　第２の装置

３０、６０、１００　秘密計算サーバ

３１　秘密計算実行部

４０　認証装置

５０、５０ａ、５０ｂ　認証候補抽出装置

１０１　ＣＰＵ（Central Processing Unit）

１０２　メモリ

１０３　入出力インターフェイス

１０４　ＮＩＣ（Network Interface Card）

２１１　カメラ

２１２　タイマ

２１３、４０１、５０１　特徴量抽出部

２１４　特徴量保存部

２１５　秘密分散部

４０２　認証処理部

５０３　秘密分散制御部

５０４　特徴情報送信部

５０５　処理性能調整部

５０６　混雑度判定部

５０７　応答性能取得部

６０１　特徴情報記憶部

６０２　秘密計算実行部

請求の範囲

[請求項1] 秘密分散されたシェアに対してシフト演算を行う、秘密計算サーバ。

[請求項2] 前記秘密分散されたシェアに対応する秘密情報の有効桁数を削減する場合に、前記シフト演算を行う、請求項１に記載の秘密計算サーバ。

[請求項3] 前記シフト演算は右シフトである、請求項１又は２に記載の秘密計算サーバ。

[請求項4] 前記秘密分散されたシェアは２の冪乗又は素数を法とする、請求項１乃至３のいずれか一項に記載の秘密計算サーバ。

[請求項5] 請求項１乃至４のいずれか一項に記載の秘密計算サーバと、

第１の地点で取得された第１の移動体の識別情報を保持する第１の装置と、第２の地点で取得された第２の移動体の識別情報を保持する第２の装置と、のそれぞれに対して、前記秘密計算サーバへの前記第１、第２の移動体の識別情報の提供を要求する要求部と、

前記第１、第２の移動体の識別情報の有効桁数を決定する、決定部と、

前記秘密計算サーバに対し、前記決定された第１、第２の移動体の識別情報の有効桁数に関する情報を通知すると共に、前記第１の移動体の識別情報と前記第２の移動体の識別情報とに基づいた移動体の移動に関する計算処理を指示する指示部と、

を備える制御装置と、

を含み、

前記秘密計算サーバは、前記通知された有効桁数に関する情報に基づいて、前記第１、第２の移動体の識別情報に対して前記シフト演算を行う、システム。

[請求項6] 前記決定部は、

前記秘密計算サーバによる前記第１、第２の移動体の識別情報を用

いた処理が所定の時間以内に終了するように前記第１、第２の移動体の識別情報の有効桁数を決定する、請求項５に記載のシステム。

[請求項7] 請求項１乃至４のいずれか一項に記載の秘密計算サーバと、

第１の地点から第２の地点へ移動する被認証体について、前記第１の地点において取得された生体情報を入力する生体情報入力部と、

前記第１の地点において取得された生体情報を第１のシェア情報に秘密分散し、前記第１シェア情報を前記秘密計算サーバに送信する、秘密分散制御部と、

を備える認証候補抽出装置と、

を含み、

前記秘密計算サーバは、

前記被認証体の認証処理用の特徴情報であって、秘密分散された特徴情報を第２シェア情報として記憶する特徴情報記憶部と、

前記第１及び第２のシェア情報を用いて、前記認証処理用の候補を選択する、秘密計算実行部と、

を備え、

前記認証候補抽出装置は、

前記被認証体が前記第１の地点から第２の地点へ到達する予測時間に基づいて、前記第２の地点において取得された被認証体の生体情報を用いて認証処理を行う認証装置における認証処理に間に合う範囲で所定の要求精度を満たす候補を選択できるよう、前記第１及び第２のシェア情報の有効桁数に関する情報を前記秘密計算サーバに通知する、処理性能調整部と、

前記認証装置に対して、前記秘密計算サーバにより選択された候補の特徴情報を送信する特徴情報送信部と、

をさらに備え、

前記秘密計算実行部は、

前記通知された第１及び第２のシェア情報の有効桁数に関する情報

に基づいて、前記第１及び第２のシェア情報に対して前記シフト演算を行う、システム。

[請求項8] 前記処理性能調整部は、前記第１の地点と前記第２の地点間の混雑度に基づいて、前記予測時間を計算する請求項７に記載のシステム。

[請求項9] 前記処理性能調整部は、前記認証装置の認証処理の応答時間に応じて、前記認証処理用の候補の選択に用いる特徴情報に含まれる特徴量の桁数を増減する請求項７又は８に記載のシステム。

[請求項10] コンピュータにおいて、

秘密分散されたシェアを入力するステップと、

前記秘密分散されたシェアに対してシフト演算するステップと、

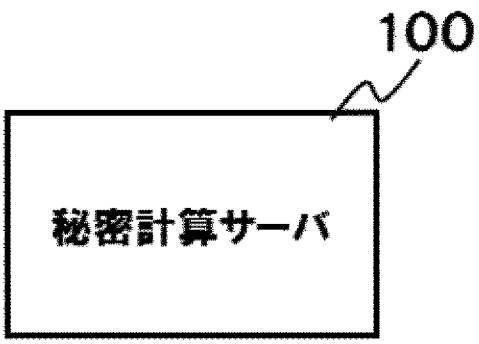
を含む、秘密計算方法。

[請求項11] 秘密分散されたシェアを入力する処理と、

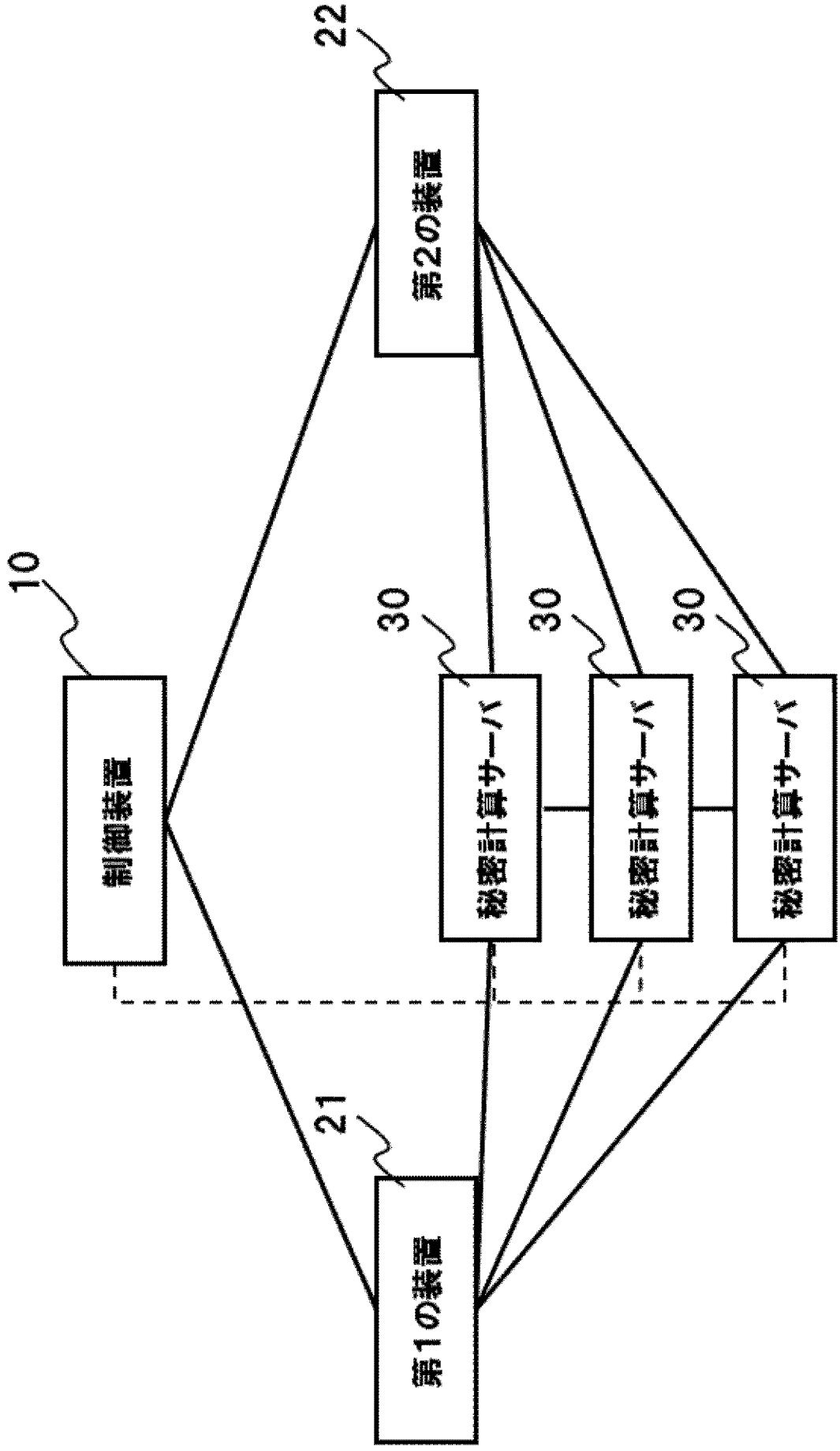
前記秘密分散されたシェアに対してシフト演算する処理と、

をコンピュータに実行させるプログラム。

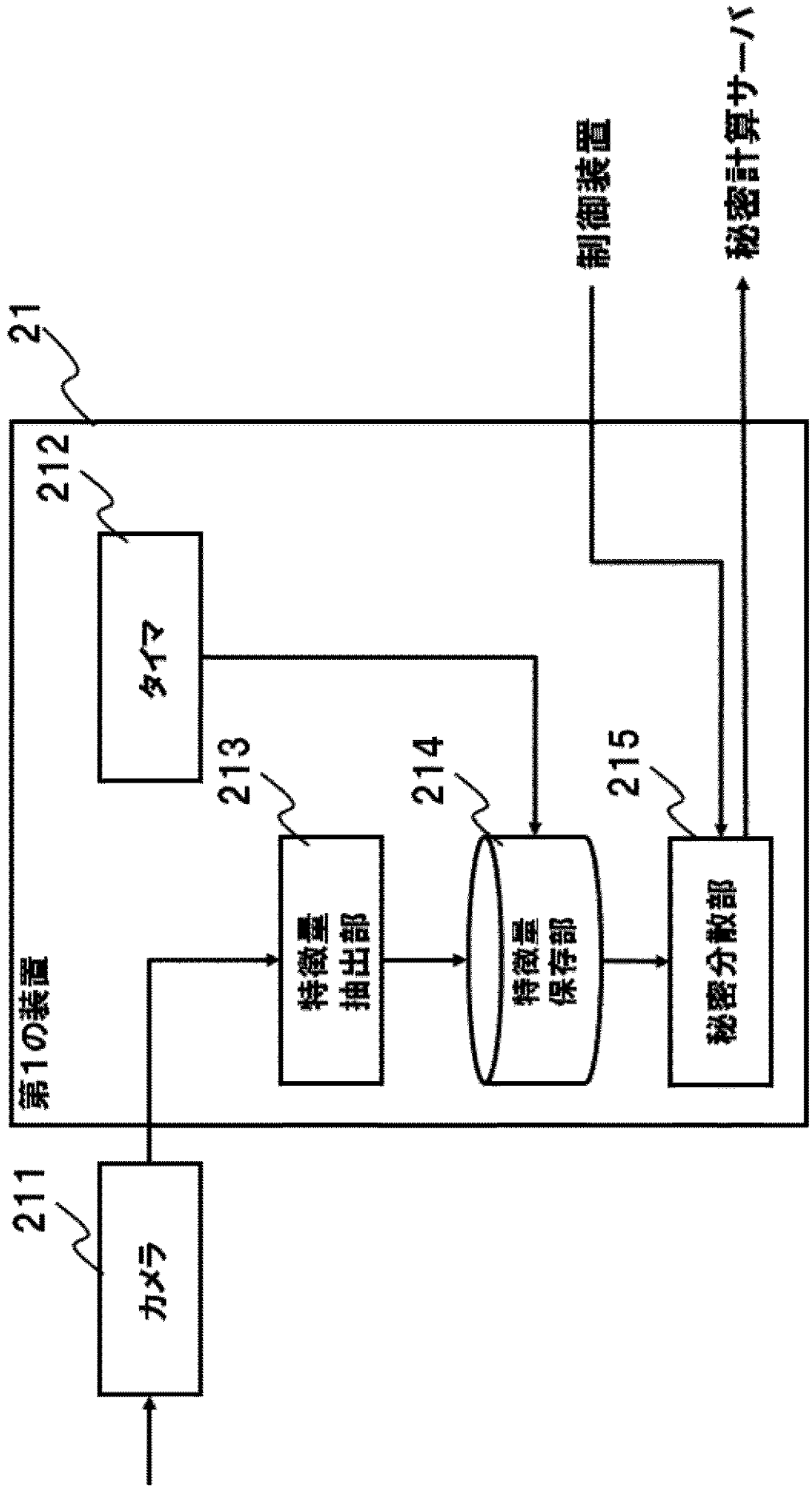
[図1]



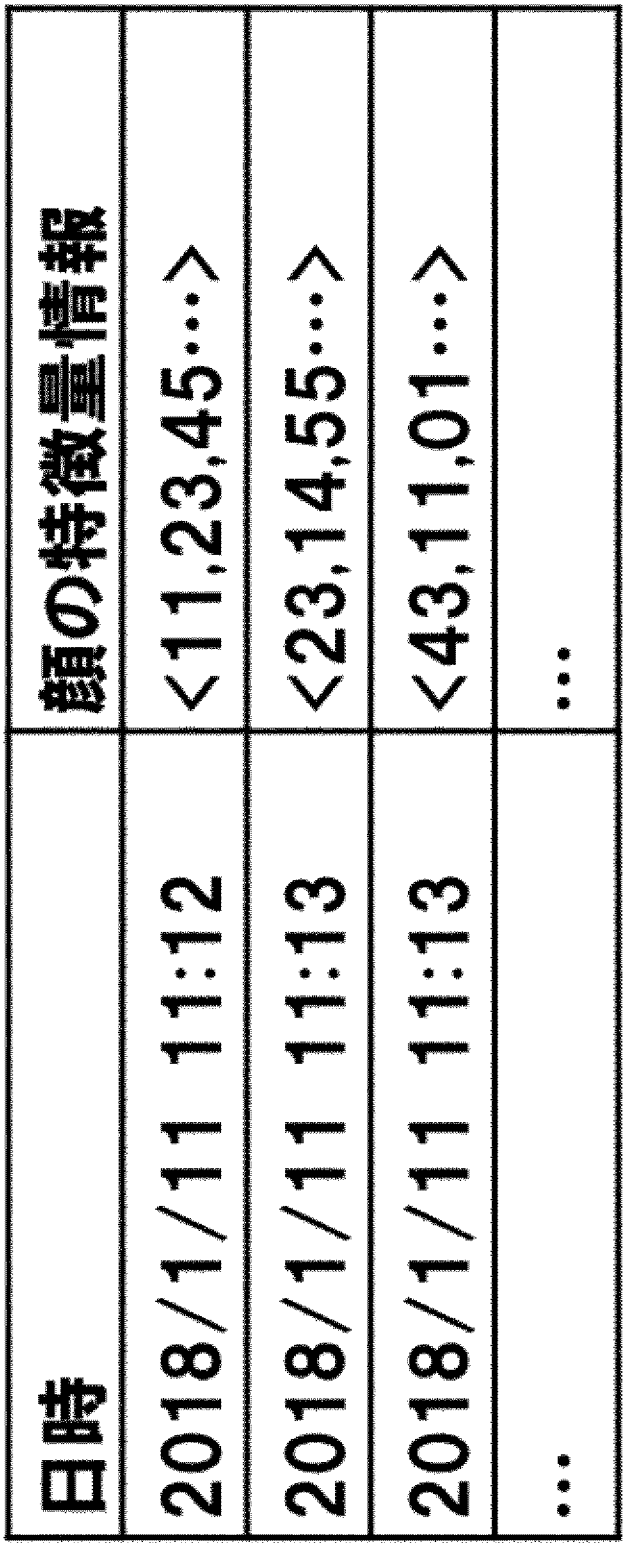
[図2]



[図3]

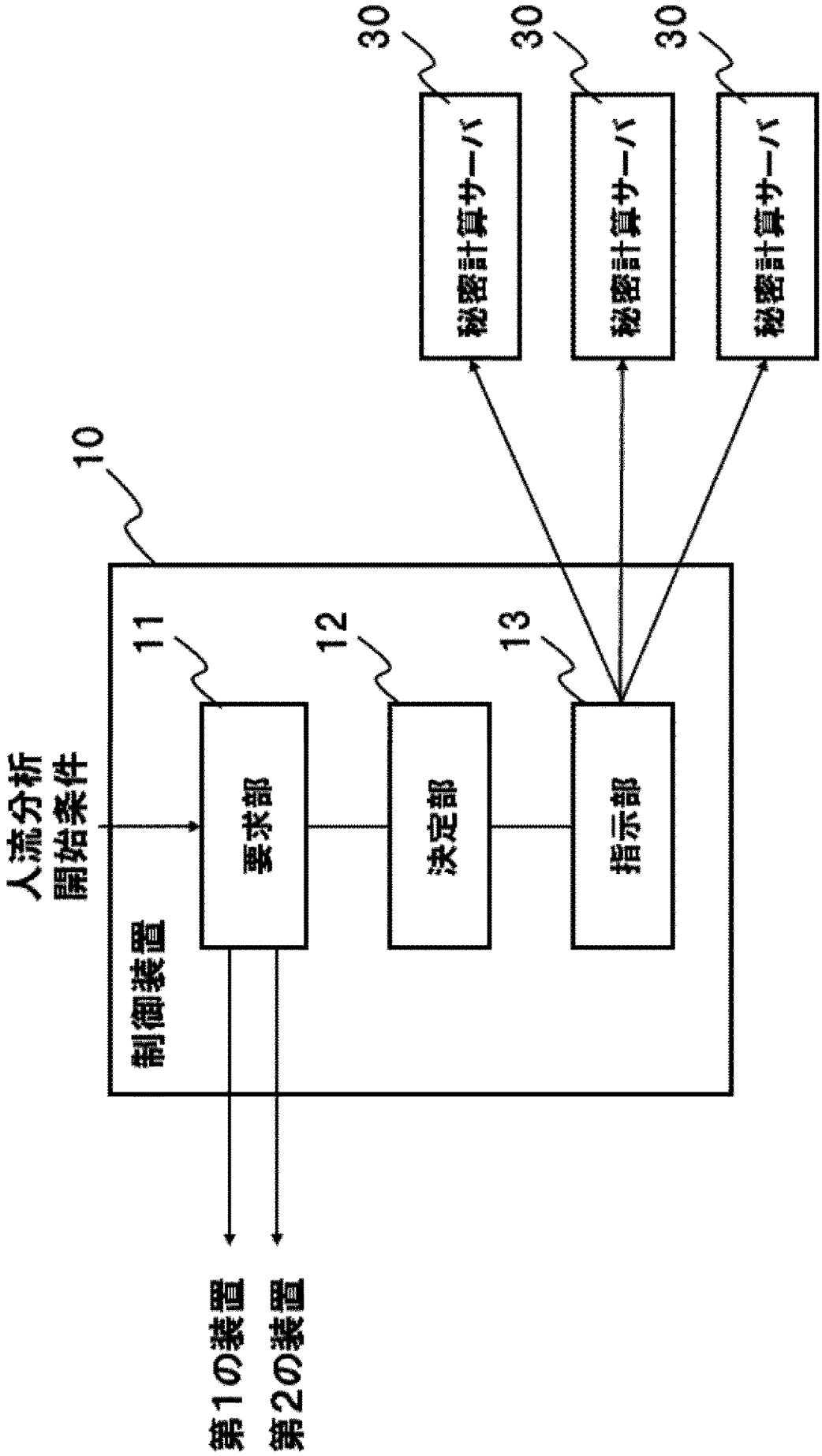

制御装置
秘密計算サーバ
21
212
タイマ
213
214
215
特徴量抽出部
特徴量保存部
秘密分散部
第1の装置
211
カメラ

[図4]

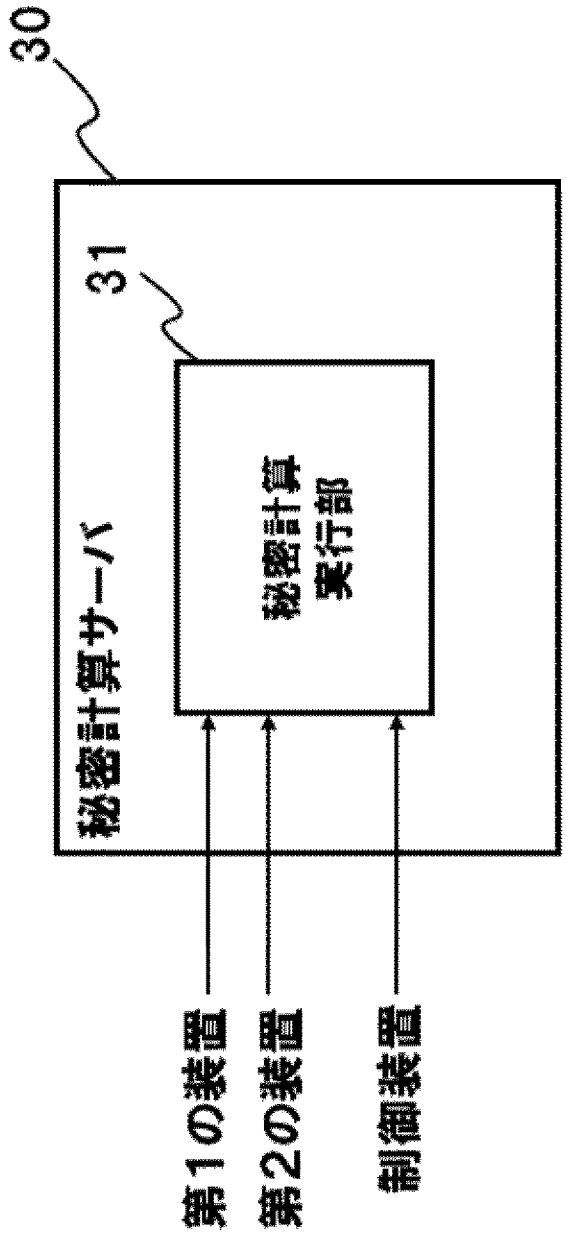


日時	顔の特徴量情報
2018/1/11 11:12	<11,23,45…>
2018/1/11 11:13	<23,14,55…>
2018/1/11 11:13	<43,11,01…>
…	…

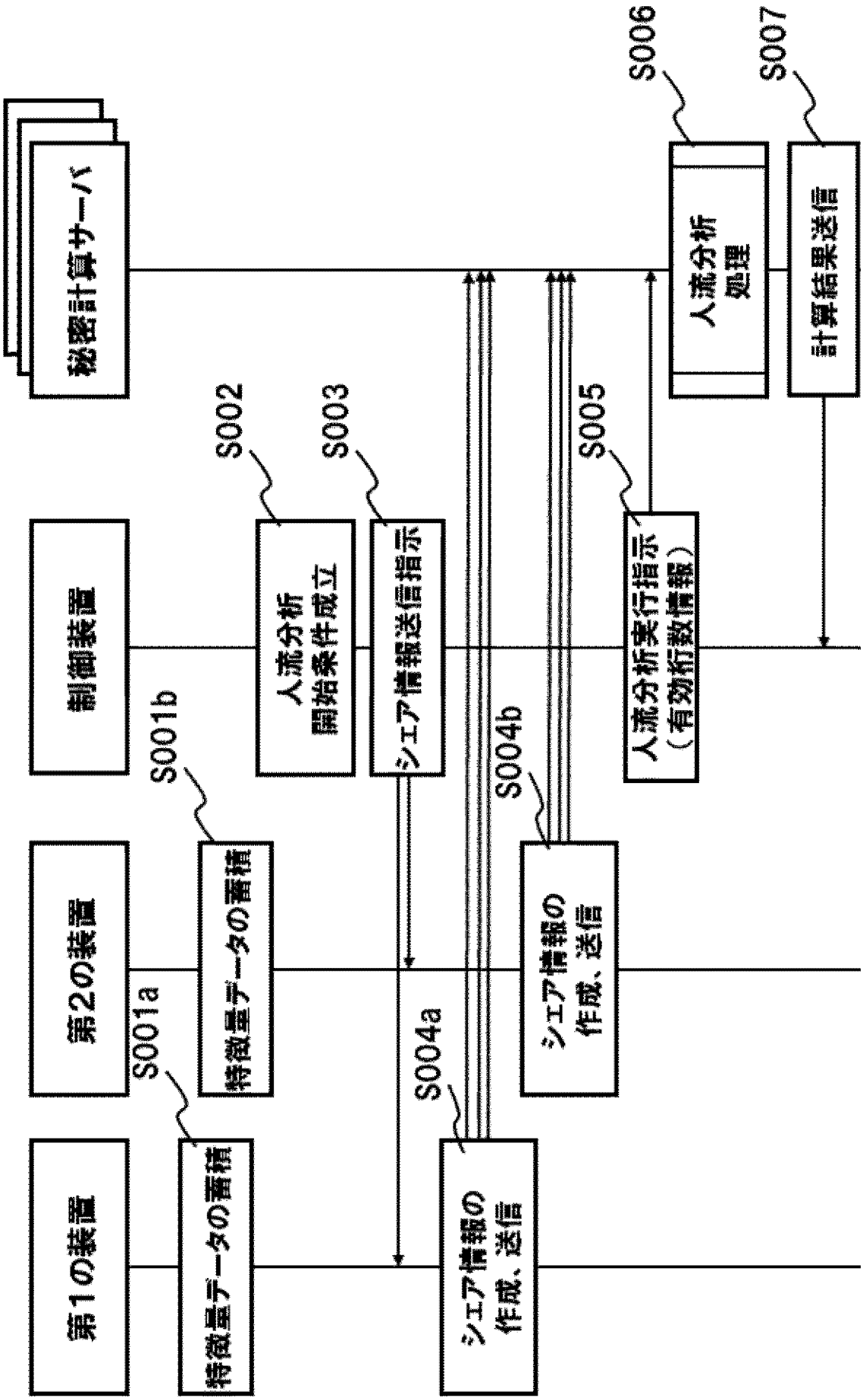
[図5]


30
30
30
秘密計算サーバ
秘密計算サーバ
秘密計算サーバ
10
11
12
13
人流分析
開始条件
要求部
決定部
指示部
制御装置
第1の装置
第2の装置

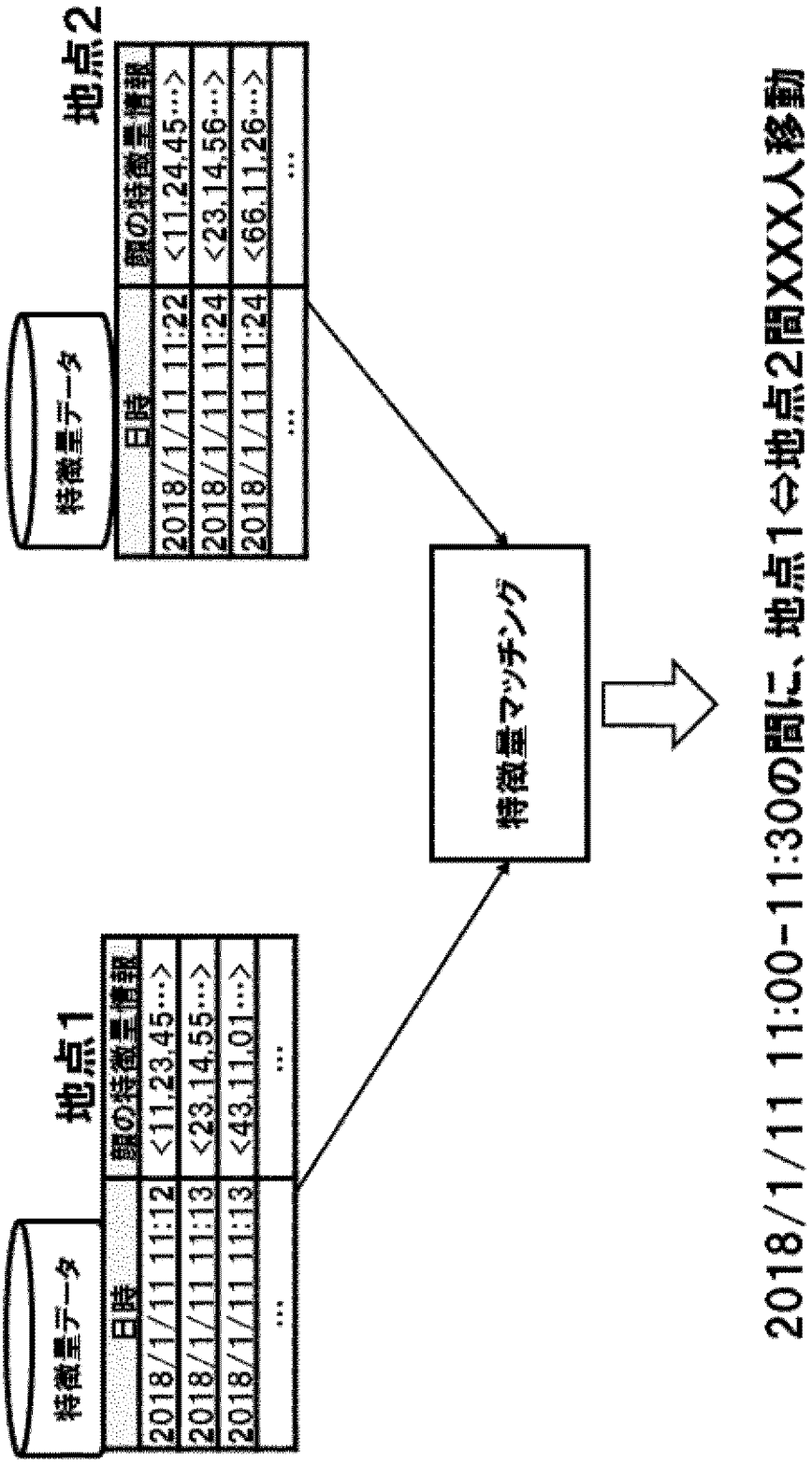
[図6]



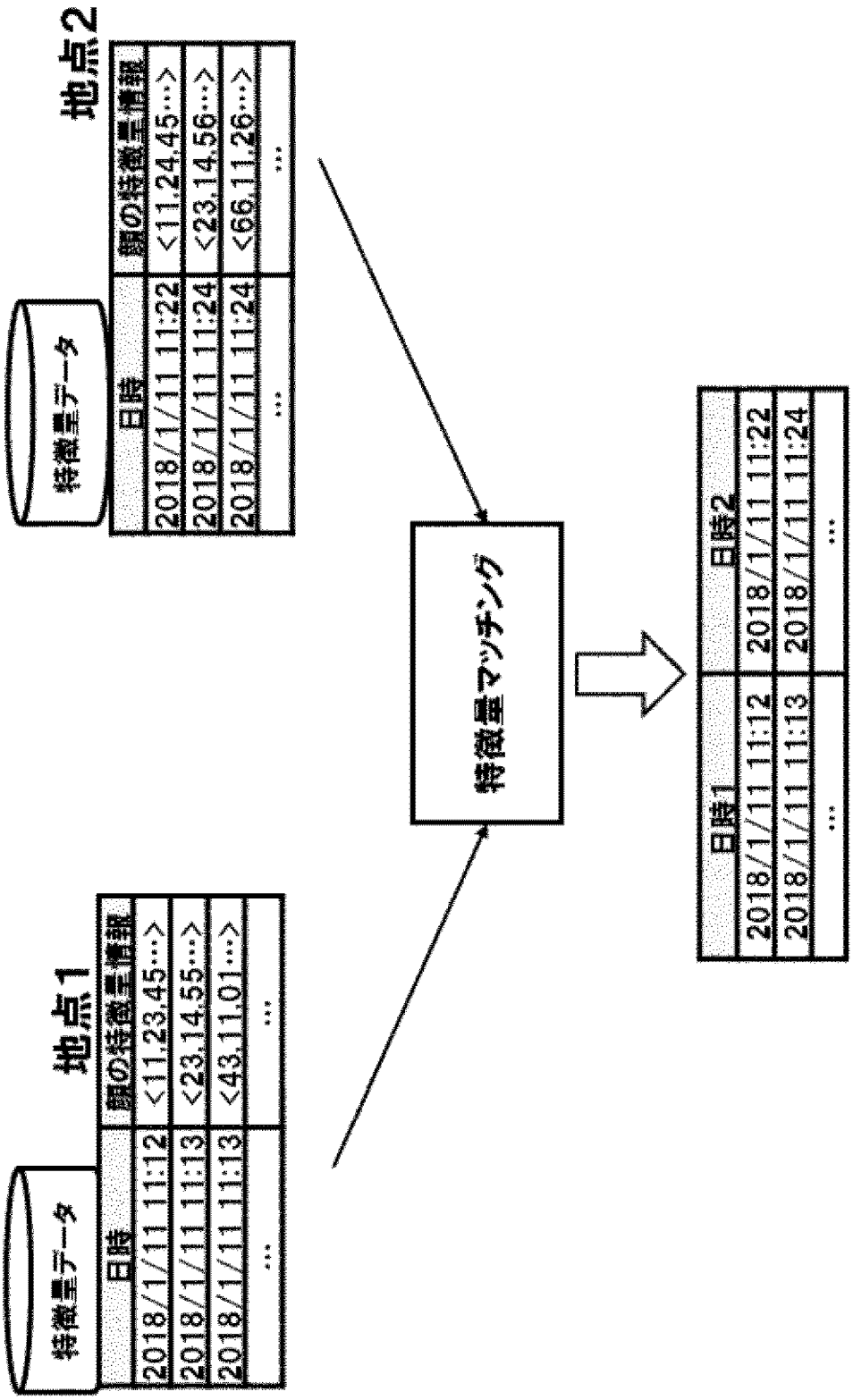
[図7]


秘密計算サーバ
制御装置
第2の装置
第1の装置
S001a
S001b
S002
S003
S004a
S004b
S005
S006
S007
特徴量データの蓄積
特徴量データの蓄積
人流分析
開始条件成立
シェア情報送信指示
シェア情報の
作成、送信
シェア情報の
作成、送信
人流分析実行指示
（有効桁数情報）
人流分析
処理
計算結果送信

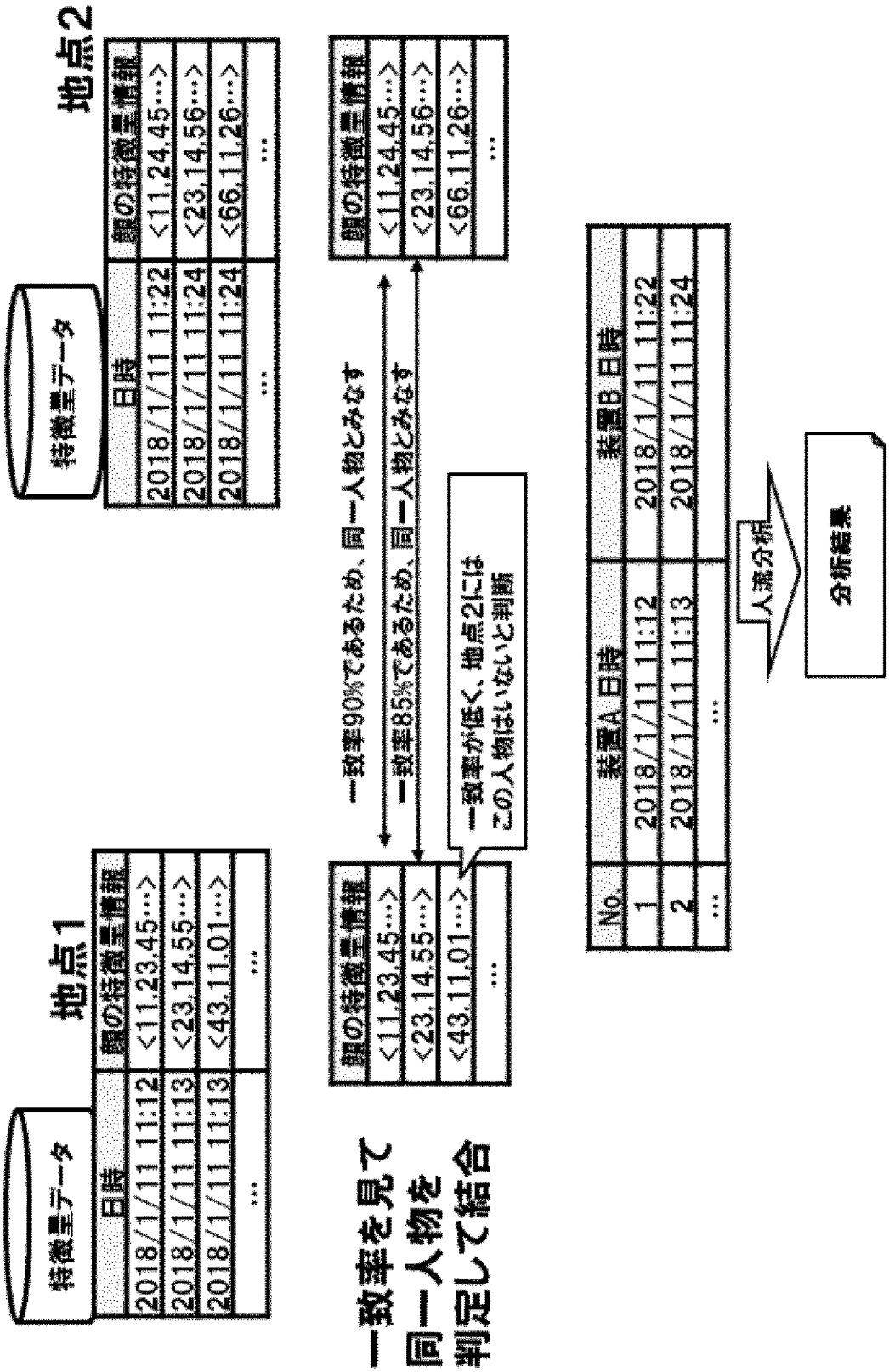
[図8]


地点1
特徴量データ
日時
顔の特徴量情報
2018/1/11 11:12
<11,23,45…>
2018/1/11 11:13
<23,14,55…>
2018/1/11 11:13
<43,11,01…>
…
地点2
特徴量データ
日時
顔の特徴量情報
2018/1/11 11:22
<11,24,45…>
2018/1/11 11:24
<23,14,56…>
2018/1/11 11:24
<66,11,26…>
…
特徴量マッチング
2018/1/11 11:00-11:30の間に、地点1⇔地点2間XXX人移動

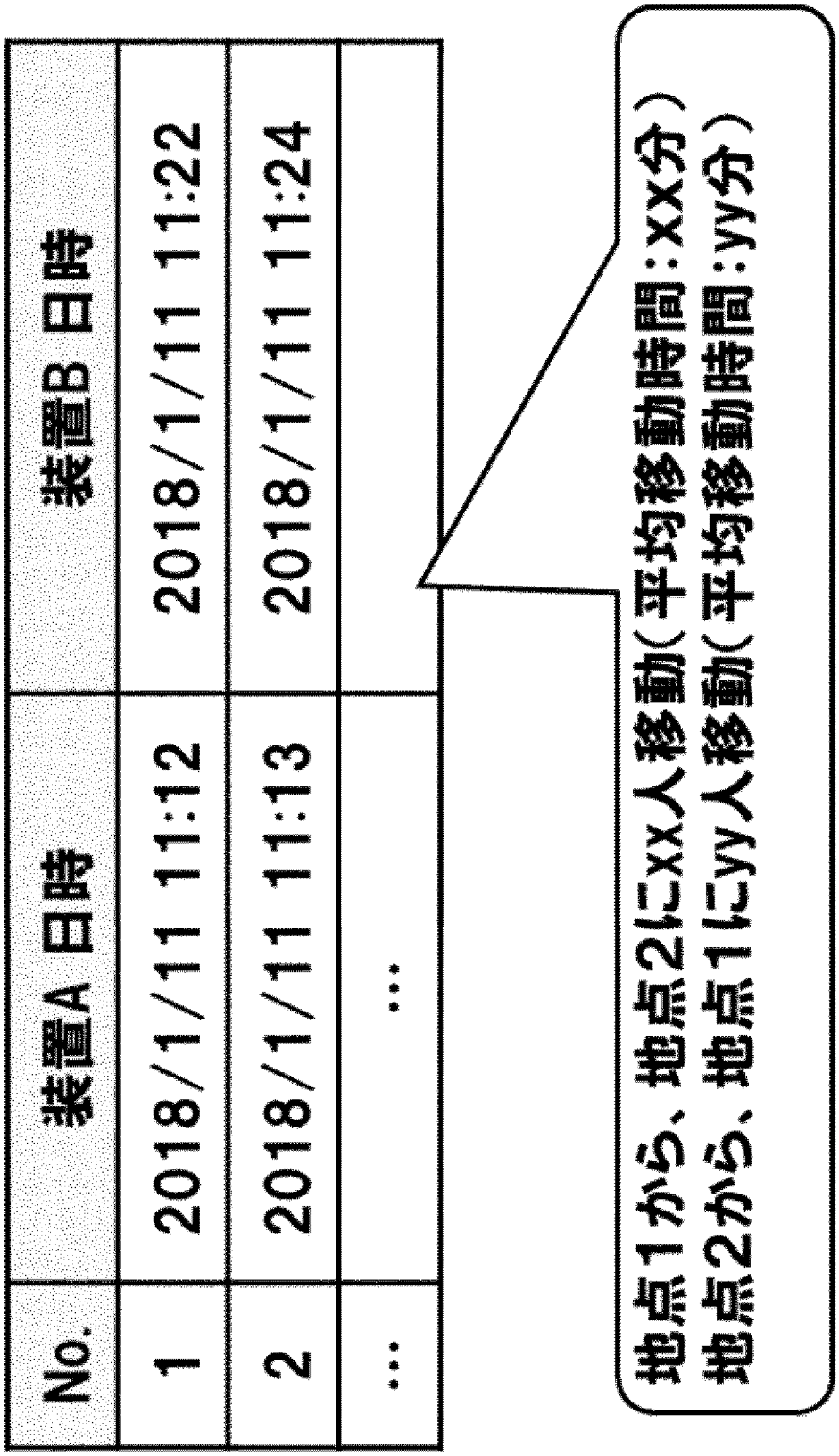
[図9]


地点2
特徴量データ
日時
顔の特徴量情報
2018/1/11 11:22
<11,24,45…>
2018/1/11 11:24
<23,14,56…>
2018/1/11 11:24
<66,11,26…>
…
…
地点1
特徴量データ
日時
顔の特徴量情報
2018/1/11 11:12
<11,23,45…>
2018/1/11 11:13
<23,14,55…>
2018/1/11 11:13
<43,11,01…>
…
…
特徴量マッチング
日時1
日時2
2018/1/11 11:12
2018/1/11 11:22
2018/1/11 11:13
2018/1/11 11:24
…
…

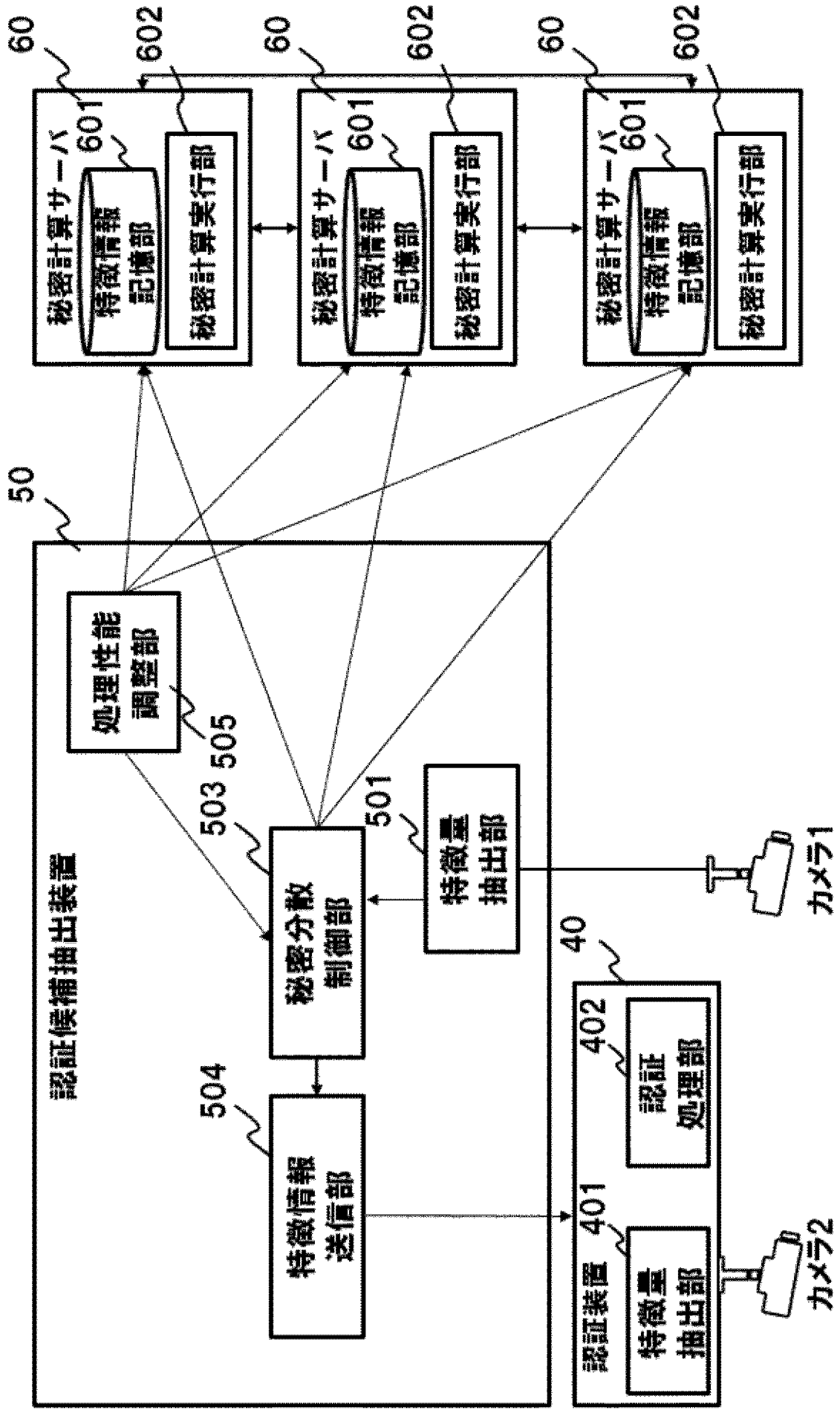
[図10]


地点1
特徴量データ
日時
顔の特徴量情報
2018/1/11 11:12
<11,23,45…>
2018/1/11 11:13
<23,14,55…>
2018/1/11 11:13
<43,11,01…>
…
地点2
特徴量データ
日時
顔の特徴量情報
2018/1/11 11:22
<11,24,45…>
2018/1/11 11:24
<23,14,56…>
2018/1/11 11:24
<66,11,26…>
…
一致率を見て
同一人物を
判定して結合
顔の特徴量情報
<11,23,45…>
<23,14,55…>
<43,11,01…>
…
顔の特徴量情報
<11,24,45…>
<23,14,56…>
<66,11,26…>
…
一致率90%であるため、同一人物とみなす
一致率85%であるため、同一人物とみなす
一致率が低く、地点2には
この人物はいないと判断
No.
装置A 日時
装置B 日時
1
2018/1/11 11:12
2018/1/11 11:22
2
2018/1/11 11:13
2018/1/11 11:24
…
…
人流分析
分析結果

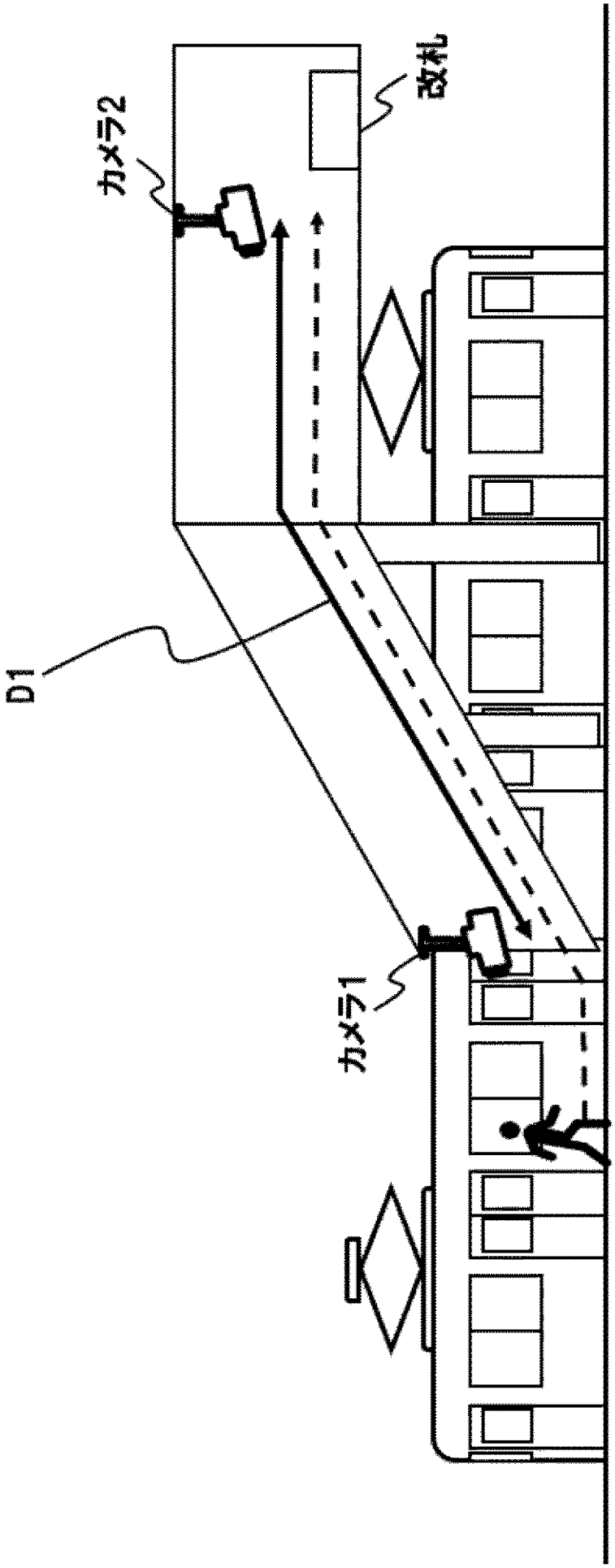
[図11]


No.
装置A 日時
装置B 日時
1
2018/1/11 11:12
2018/1/11 11:22
2
2018/1/11 11:13
2018/1/11 11:24
…
…
地点1から、地点2にxx人移動(平均移動時間:xx分)
地点2から、地点1にyy人移動(平均移動時間:yy分)

[図12]


60
602
秘密計算サーバ
601
特徴情報記憶部
秘密計算実行部
50
認証候補抽出装置
処理性能調整部
505
503
秘密分散制御部
501
特徴抽出部
504
特徴情報送信部
カメラ1
40
402
認証処理部
認証装置
401
特徴抽出部
カメラ2

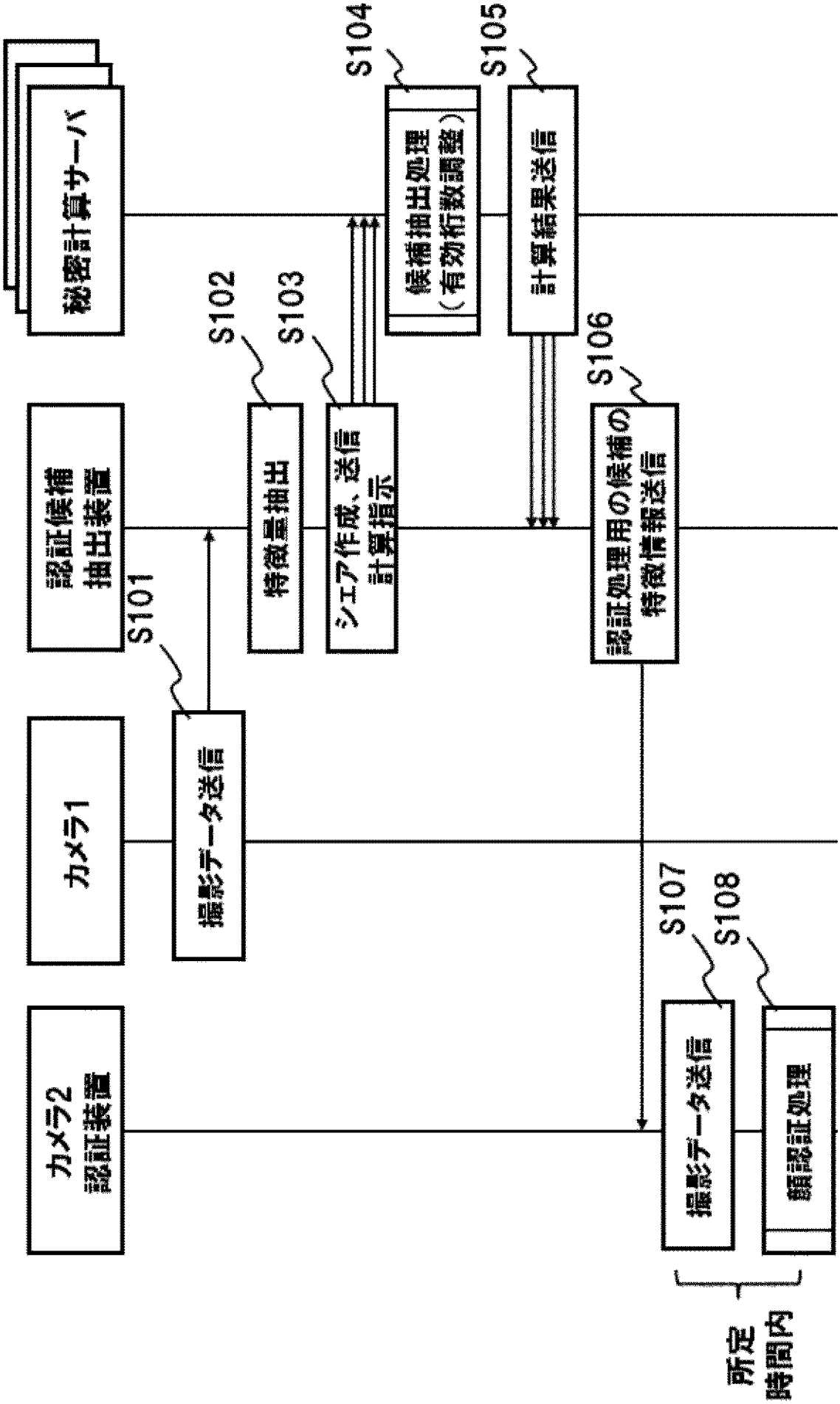
[図13]



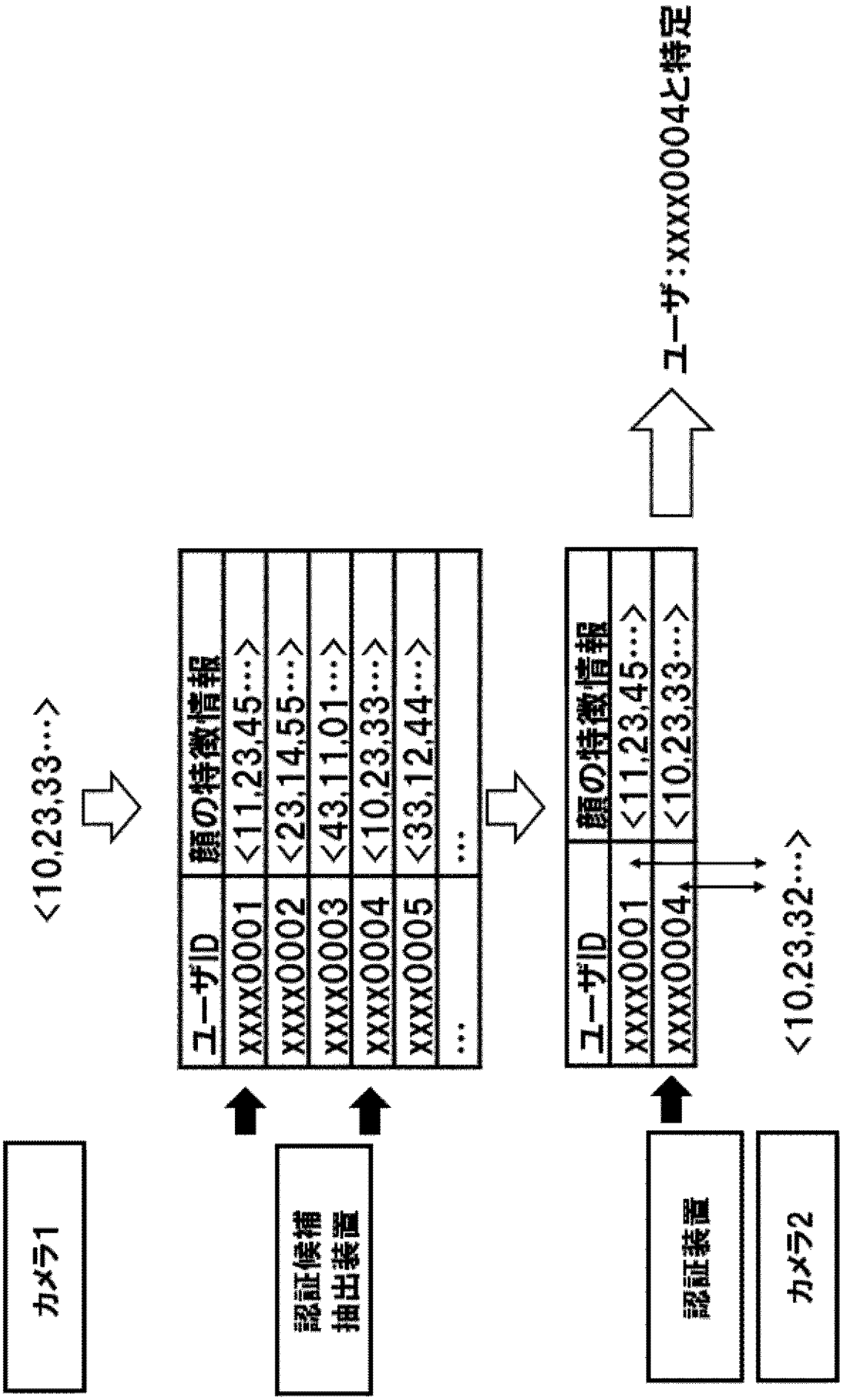
[図14]

ユーザID	顔の特徴情報
XXXX0001	<11,23,45…>
XXXX0002	<23,14,55…>
XXXX0003	<43,11,01…>
XXXX0004	<10,23,33…>
XXXX0005	<33,12,44…>
…	…

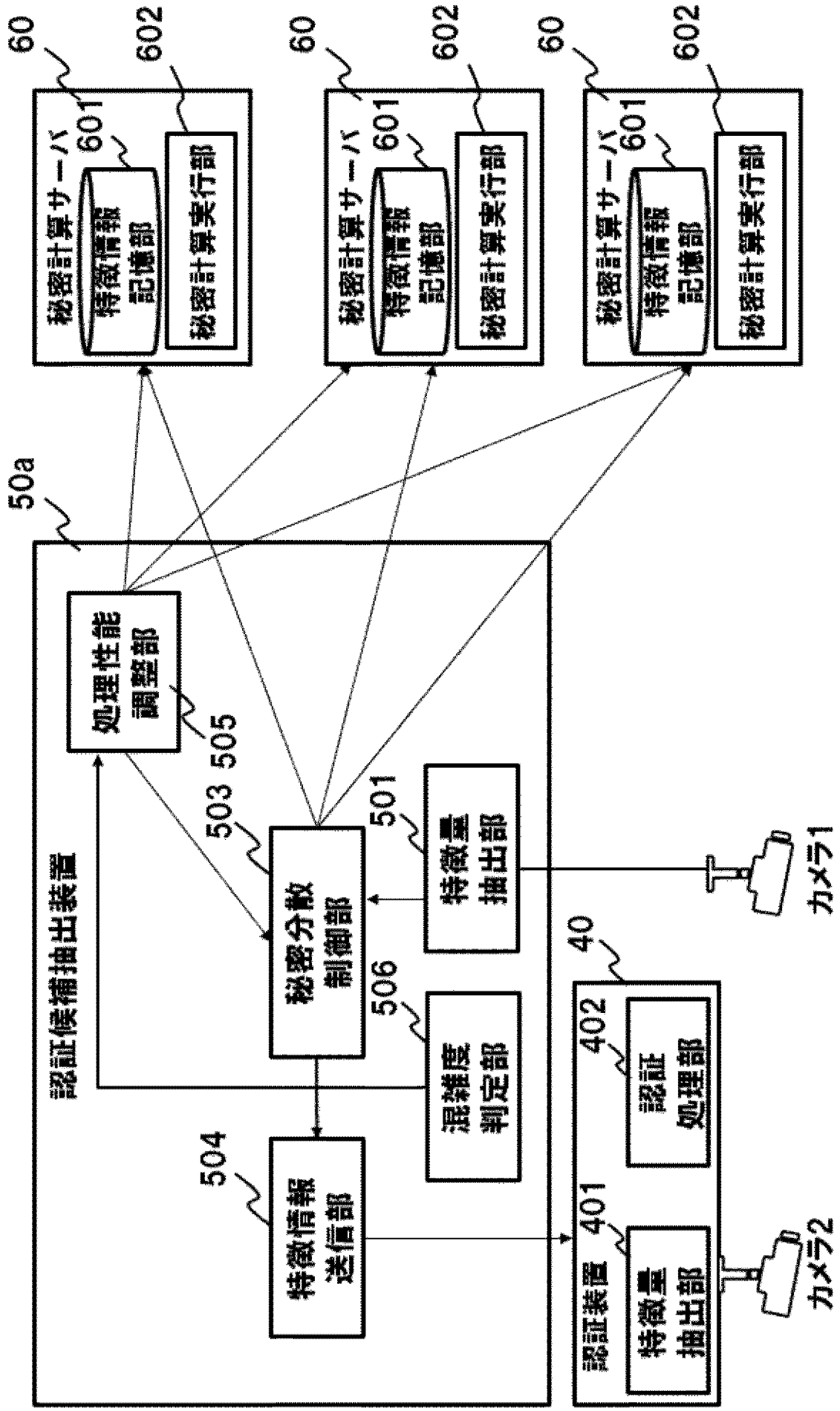
[図15]


秘密計算サーバ
認証候補抽出装置
カメラ1
カメラ2認証装置
S101
撮影データ送信
S102
特徴量抽出
S103
シェア作成、送信計算指示
S104
候補抽出処理（有効桁数論理）
S105
計算結果送信
S106
認証処理用の候補の特徴情報送信
S107
撮影データ送信
S108
顔認証処理
所定時間内

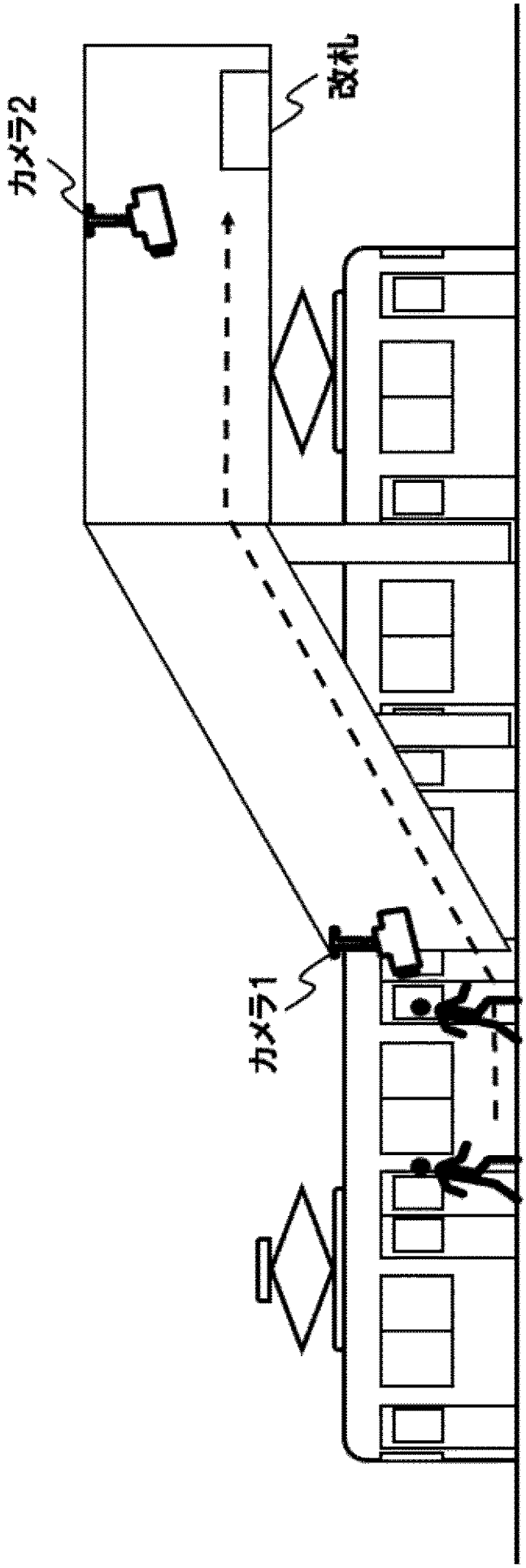
[図16]


カメラ1
認証候補抽出装置
ユーザID
顔の特徴情報
XXXX0001
<11,23,45・・・>
XXXX0002
<23,14,55・・・>
XXXX0003
<43,11,01・・・>
XXXX0004
<10,23,33・・・>
XXXX0005
<33,12,44・・・>
<10,23,33・・・>
認証装置
カメラ2
<10,23,32・・・>
ユーザ：XXXX0004と特定

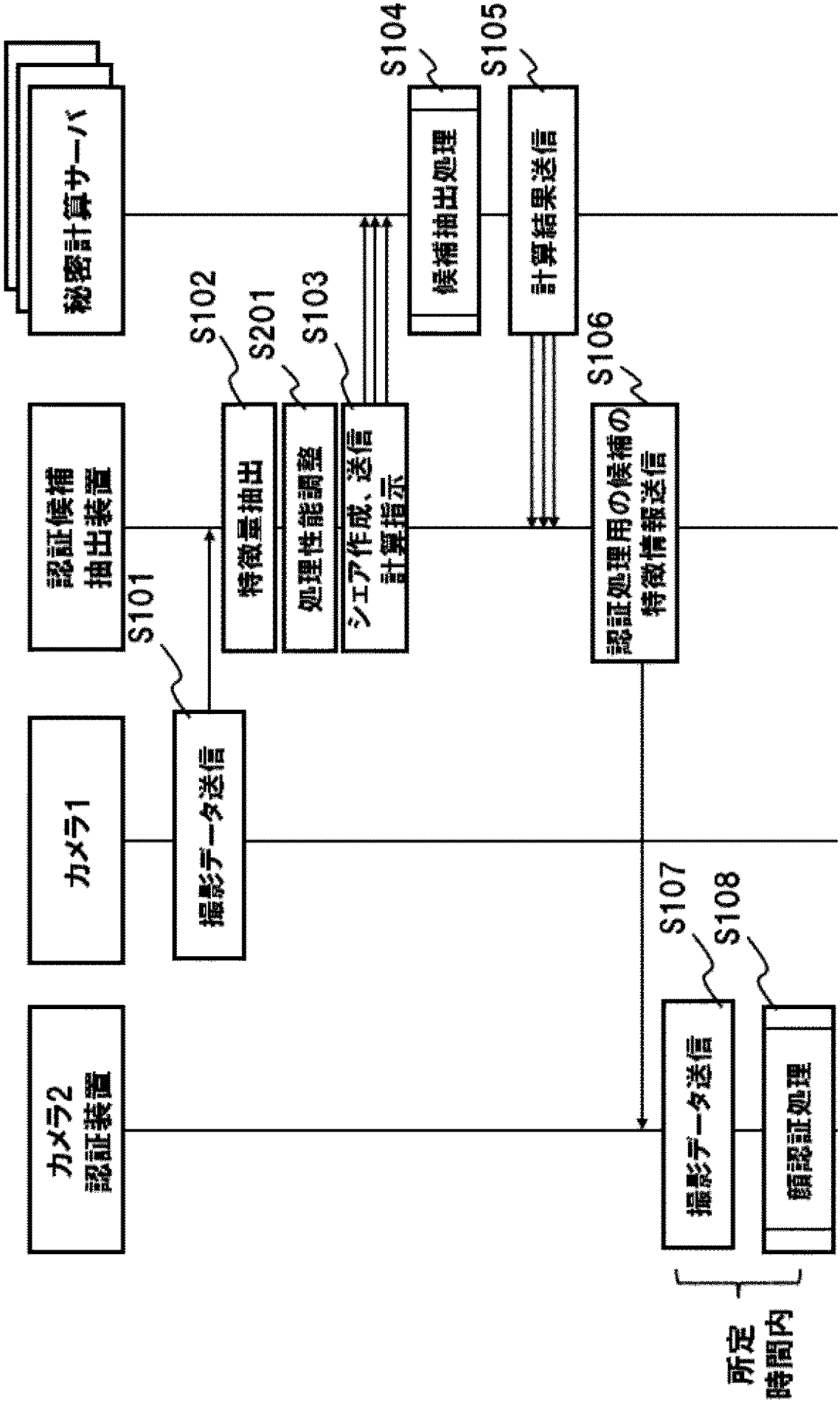
[図17]


60
602
秘密計算サーバ
601
特徴情報記憶部
秘密計算実行部
50a
認証候補抽出装置
処理性能調整部
505
503
秘密分散制御部
501
特徴量抽出部
506
照合判定部
504
特徴情報送信部
カメラ1
40
402
認証処理部
認証装置
401
特徴量抽出部
カメラ2

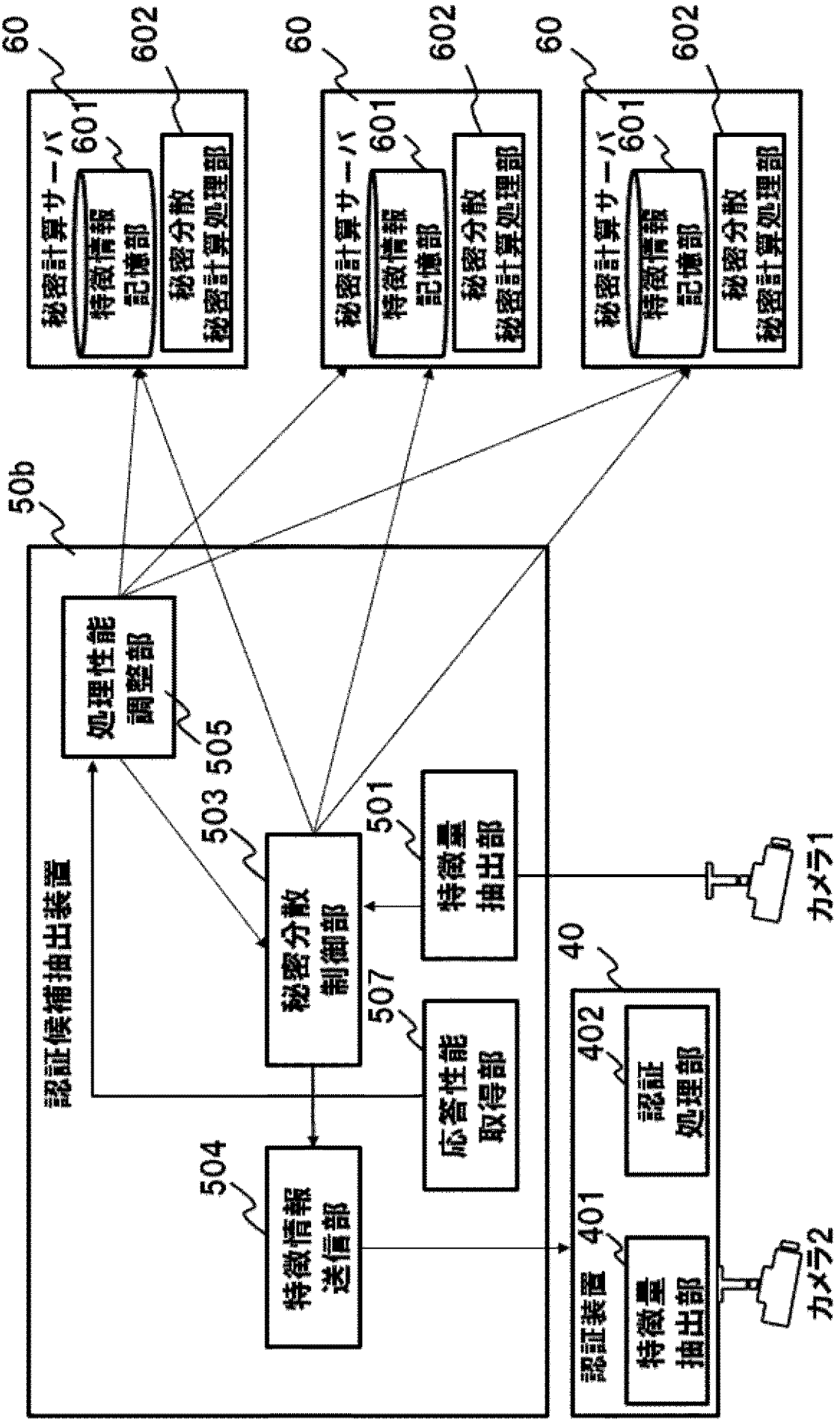
[図18]



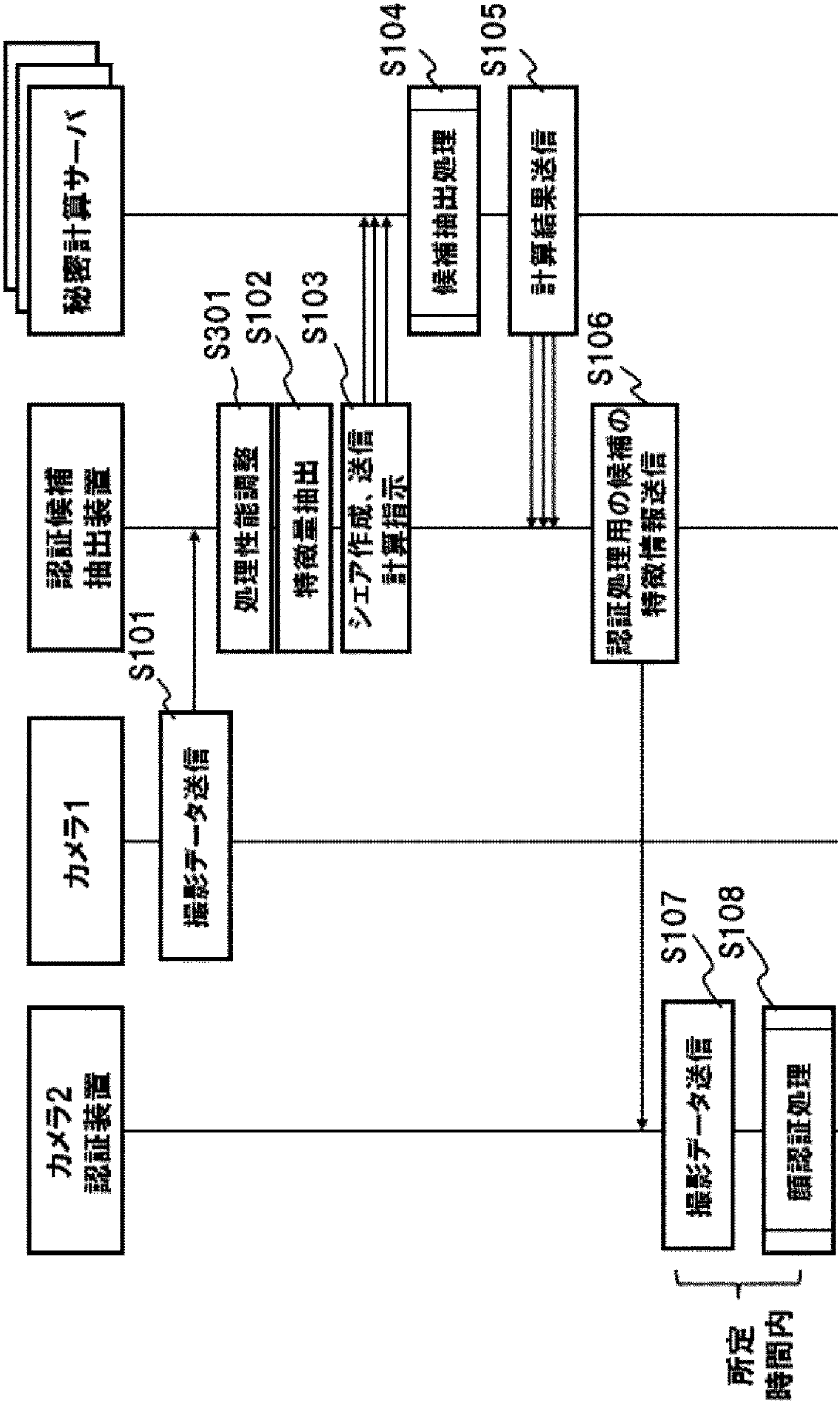
[図19]


秘密計算サーバ
認証候補抽出装置
カメラ1
カメラ2認証装置
S101
撮影データ送信
S102
特徴量抽出
S201
処理性能調整
S103
シェア作成、送信計算指示
S104
候補抽出処理
S105
計算結果送信
S106
認証処理用の候補の特徴情報送信
S107
撮影データ送信
S108
顔認証処理
所定時間内

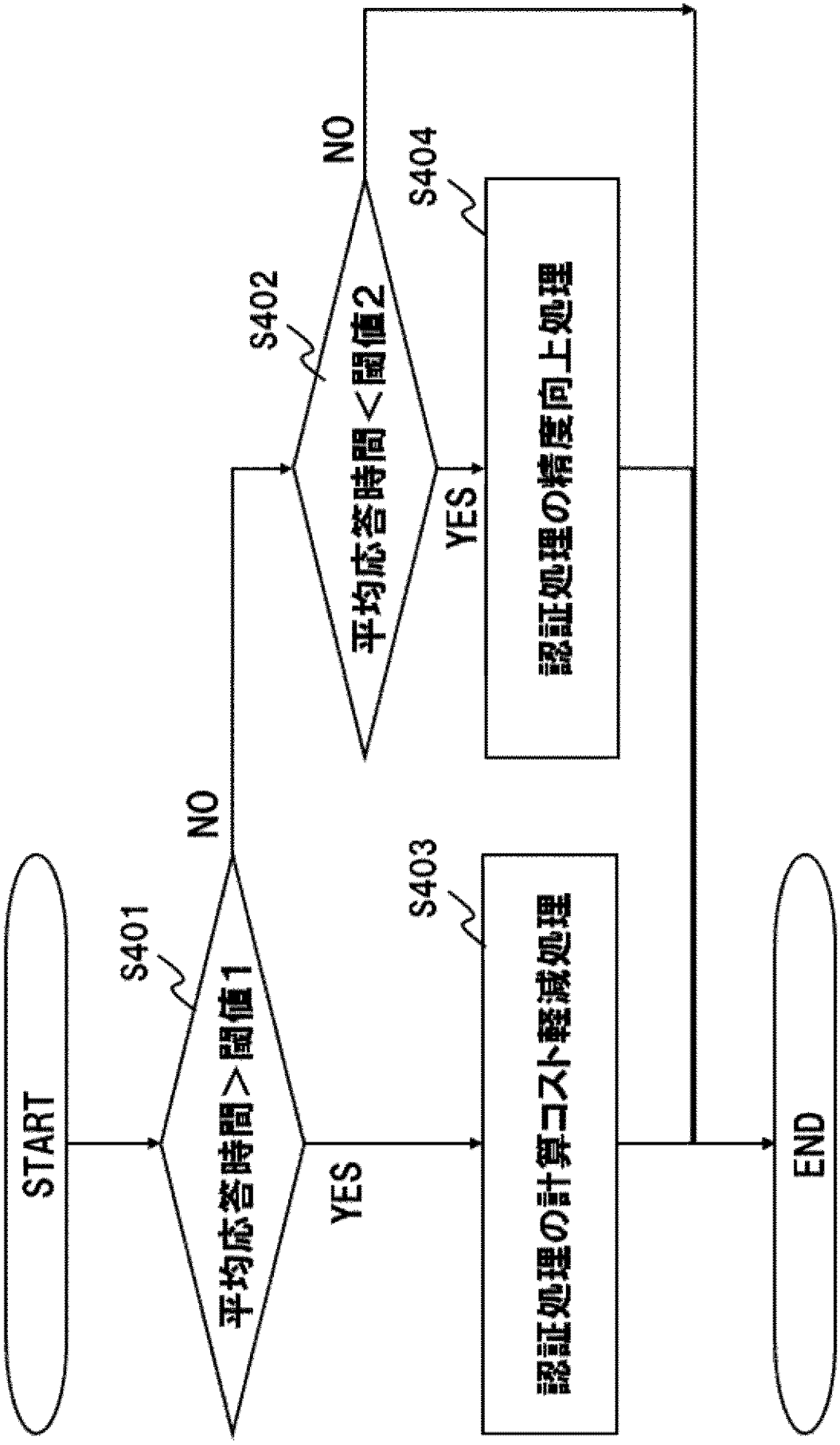
[図20]


60
602
秘密計算サーバ
601
特徴情報記憶部
秘密分散秘密計算処理部
50b
認証候補抽出装置
処理性能調整部
505
503
秘密分散制御部
501
特徴量抽出部
507
応答性能取得部
504
特徴情報送信部
カメラ1
40
402
認証処理部
認証装置
401
特徴量抽出部
カメラ2

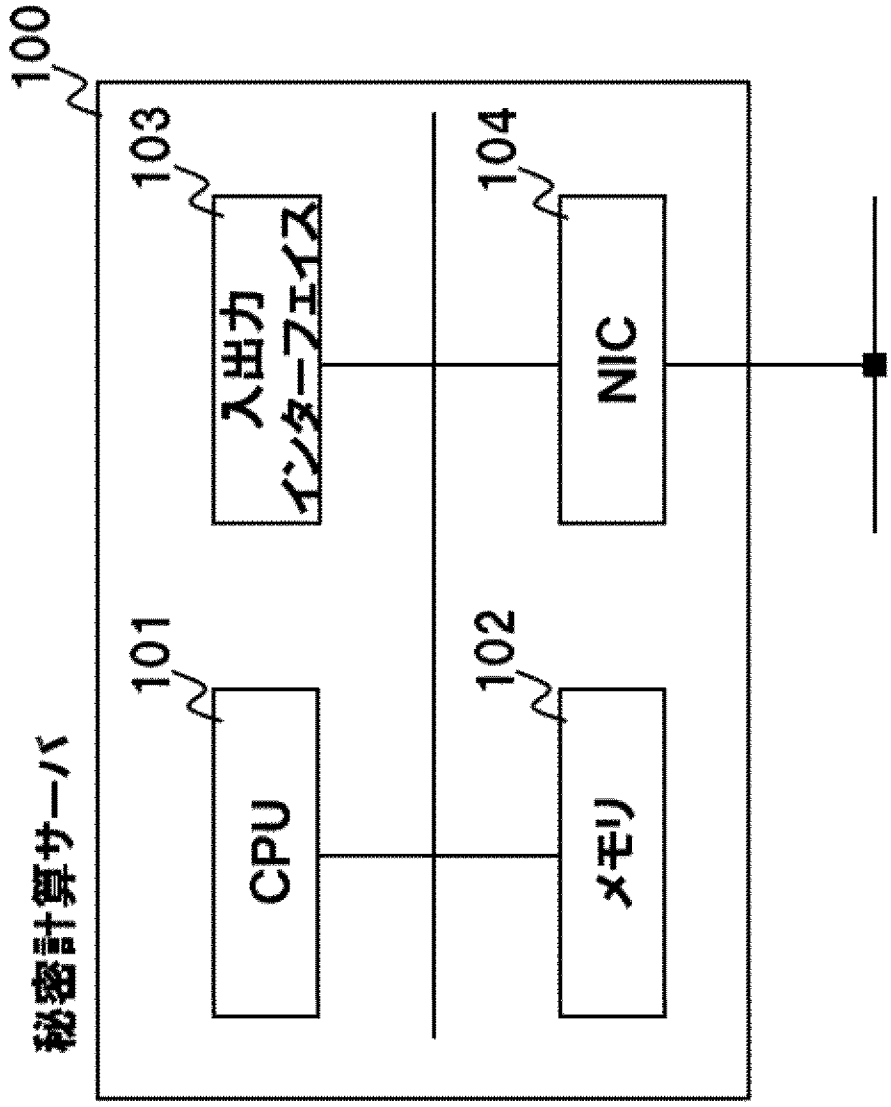
[図21]


秘密計算サーバ
認証候補抽出装置
カメラ1
カメラ2認証装置
S101
撮影データ送信
S301
処理性能調整
S102
特徴量抽出
S103
シェア作成、送信計算指示
S104
候補抽出処理
S105
計算結果送信
S106
認証処理用の候補の特徴情報送信
S107
撮影データ送信
S108
顔認証処理
所定時間内

[図22]


START
S401
平均応答時間＞閾値1
YES
NO
S402
平均応答時間＜閾値2
YES
NO
S403
認証処理の計算コスト軽減処理
S404
認証処理の精度向上処理
END

[図23]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/039818

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G09C1/00(2006.01)i, H04L9/36(2006.01)i

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)
Int.Cl. G09C1/00, H04L9/36

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 1971-2019
Registered utility model specifications of Japan 1996-2019
Published registered utility model applications of Japan 1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JSTPlus/JMEDPlus/JST7580(JDreamIII), IEEE Xplore, THE ACM DIGITAL LIBRARY

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	CATRINA, O. et al., Secure computation with fixed-point numbers, LNCS, Financial Cryptography and Data Security, January 2010, vol. 6052, pp. 35-50	1, 3-4, 10-11 2 5-9
Y	JP 7-146777 A (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) 06 June 1995, paragraphs [0027], [0032]-[0035], fig. 2, 6, 10 (Family: none)	2

☒ 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
10.01.2019	22.01.2019

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

International application No.
PCT/JP2018/039818

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	濱田 浩気 ほか, 秘密計算による分散医療統計システムの実装評価, 情報処理学会研究報告コンピュータセキュリティ (CSEC), 19 May 2016, vol. 2016-CSEC-73, no. 20, pp. 1-7, (HAMADA, Koki et al.), non-official translation (Implementation evaluation of distributed medical statistics system by secret calculation, SIG Technical Report Computer Security (CSEC))	1-11
A	原 佑輔 ほか, 車載カメラを用いた深層学習による人流推定法の提案, 情報処理学会研究報告高度交通システムとスマートコミュニティ (ITS), 01 March 2018, vol. 2018-ITS-72, no. 3, pp. 1-8, (HARA, Yusuke et al., SIG Technical Reports, Intelligent Transport Systems and Smart Community (ITS)), non-official translation (A proposal of human flow estimation method by deep learning using in-vehicle camera)	1-11
E, X	WO 2018/212015 A1 (NEC CORPORATION) 22 November 2018, paragraphs [0069]-[0126], fig. 1-4 (Family: none)	1, 3-4

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０３９８１８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(2006.01)i, H04L9/36(2006.01)i

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））

Int.Cl.　G09C1/00, H04L9/36

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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）

JSTPlus/JMEDPlus/JST7580 (JDreamIII), IEEE Xplore, THE ACM DIGITAL LIBRARY

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
X Y A	CATRINA, Octavian et al., Secure Computation with Fixed-Point Numbers, LNCS, Financial Cryptography and Data Security, 2010.01, Vol.6052, pp.35-50	1, 3-4, 10-11 2 5-9
Y	JP 7-146777 A（松下電器産業株式会社）1995.06.06, 段落［００２７］、［００３２］－［００３５］、図２、６、１０（ファミリーなし）	2

☑　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矛盾するものではなく、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
１０．０１．２０１９	２２．０１．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　４２２９
青木　重徳
電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　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	濱田　浩気　ほか，秘密計算による分散医療統計システムの実装評価，情報処理学会　研究報告　コンピュータセキュリティ（ＣＳＥＣ），2016.05.19，Vol.2016-CSEC-73 No.20，pp.1-7	1-11
Ａ	原　佑輔　ほか，車載カメラを用いた深層学習による人流推定法の提案，情報処理学会　研究報告　高度交通システムとスマートコミュニティ（ＩＴＳ），2018.03.01，Vol.2018-ITS-72 No.3，pp.1-8	1-11
Ｅ，Ｘ	WO 2018/212015 A1（日本電気株式会社）2018.11.22， 段落［００６９］－［０１２６］、図１－４（ファミリーなし）	1,3-4