(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
2019年6月27日(27.06.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/124260 A1

(51) 国際特許分類:
*G09C 1/00* (2006.01)

(21) 国際出願番号： PCT/JP2018/046130

(22) 国際出願日： 2018年12月14日(14.12.2018)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
特願 2017-241895 2017年12月18日(18.12.2017) JP

(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: 田中 哲士 (**TANAKA, 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). 菊池 亮(**KIKUCHI, Ryo**); 〒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). 千田 浩司(**CHIDA, Koji**); 〒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).

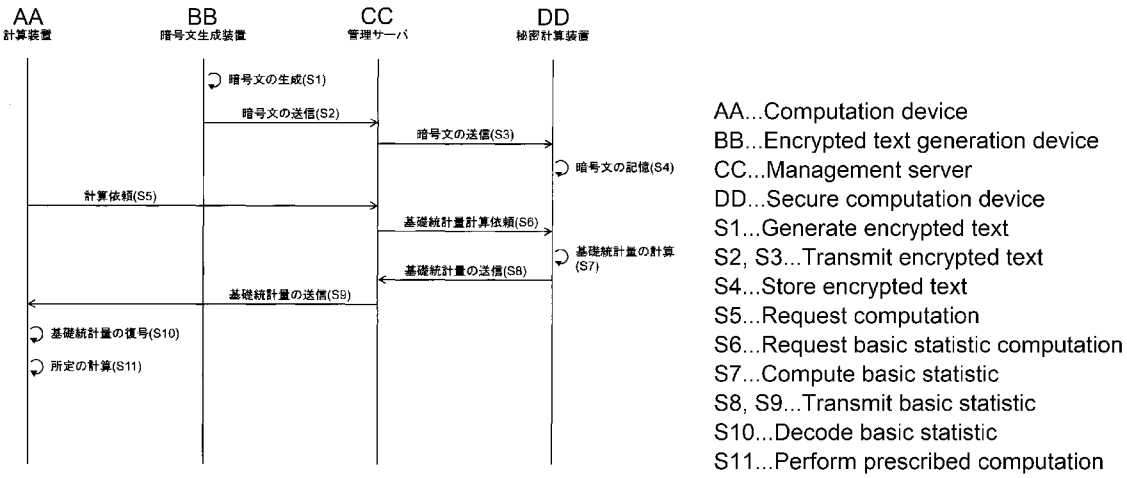
(74) 代理人: 中尾 直樹, 外 (**NAKAO, Naoki** et al.); 〒1600022 東京都新宿区新宿三丁目１番２２号 新宿ＮＳＯビル６階 Tokyo (JP).

(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 SYSTEM AND METHOD

(54) 発明の名称： 秘密計算システム及び方法

[図2]




(57) **Abstract:** A secure computation system that performs a computation on concealed data. The secure computation system comprises: an encrypted text generation device that generates encrypted text by encrypting data; a secure computation device that generates an encrypted basic statistic by using the encrypted text as the encrypted text has been concealed to securely compute a prescribed basic statistic; and a computation device that generates a decoded basic statistic by decoding the encrypted basic statistic and performs a prescribed computation using the decoded basic statistic.

(57) 要約：秘密計算システムは、データを秘匿化したまま計算を行う秘密計算システムであって、データを暗号化することにより暗号文を生成する暗号文生成装置と、暗号文を秘匿化したまま暗号文を用いて所定の基礎統計量を秘密計算することにより暗号化された基礎統計量を生成する秘密計算装置と、暗号化された基礎統計量を復号することにより復号された基礎統計量を生成し、復号された基礎統計量を用いて所定の計算を行う計算装置と、を備えている。

WO 2019/124260 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, 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))

# 明　細　書

## 発明の名称 ： 秘密計算システム及び方法

## 技術分野

[0001]　本発明は、データを秘匿しつつデータ処理を行う秘密計算の技術分野に関する。例えば、秘密多変量解析の技術に関する。

## 背景技術

[0002]　データを秘匿しつつデータ処理を行う秘密計算の従来技術として、特許文献１に記載された技術が知られている。秘密計算の従来技術では、以下の３個のフェーズが行われる。

[0003]　１．　暗号化フェーズ：データを暗号化し秘匿する。

２．　秘密計算フェーズ：暗号化したデータ、すなわち暗号文のまま、元のデータに対して目的の計算ができるアルゴリズム又はプロトコルを利用し、暗号文を処理する。

３．　復号フェーズ：秘密計算フェーズの処理の結果として得られる暗号文を復号し、目的の計算結果を取得する。

## 先行技術文献

## 特許文献

[0004] 特許文献1：特開２０１７－０２８６１７号公報

## 発明の概要

## 発明が解決しようとする課題

[0005]　上記の従来技術は、目的の計算処理を全て２．の秘密計算フェーズで行っている。

[0006]　一般に、秘密計算のアルゴリズムは、データを暗号化せずに計算するアルゴリズムよりも処理が複雑である。このため、秘密計算のアルゴリズムの計算の処理に要する時間は、平文の計算のアルゴリズムの計算の処理に要する時間よりも長い。このため、線型方程式の解決を必要とする線形回帰、行列の固有値及び固有ベクトルの計算を必要とする主成分分析といった複雑な計

算を用いるアルゴリズムを秘密計算で全て処理してしまうと、処理に要する時間が膨大になってしまう可能性がある。

[0007] この発明の目的は、データを秘匿化したまま従来よりも速い速度で秘密計算を行うことができる秘密計算システム及び方法を提供することである。

## 課題を解決するための手段

[0008] この発明の一態様による秘密計算システムは、データを秘匿化したまま計算を行う秘密計算システムであって、データを暗号化することにより暗号文を生成する暗号文生成装置と、暗号文を秘匿化したまま暗号文を用いて所定の基礎統計量を秘密計算することにより暗号化された基礎統計量を生成する秘密計算装置と、暗号化された基礎統計量を復号することにより復号された基礎統計量を生成し、復号された基礎統計量を用いて所定の計算を行う計算装置と、を備えている。

## 発明の効果

[0009] データを秘匿化したまま従来よりも速い速度で秘密計算を行うことができる。

## 図面の簡単な説明

[0010] [図1]秘密計算システムの例を示すブロック図。

[図2]秘密計算方法の例を説明するための流れ図。

[図3]第一実施形態を説明するための図。

## 発明を実施するための形態

[0011] 以下、図面を参照して、この発明の一実施形態について説明する。

[0012] ［記法］

$m, L$をそれぞれ１以上の自然数とする。単一のデータを$a$のように記述する。また、$m$次のベクトルを$a=(a_1, \cdots, a_m)$のように記述する。また、$m$行$L$列の行列を$A=(a_{j,k})_{1 \leqq j \leqq m, 1 \leqq k \leqq L}$、または、$A=(a_1^T, \cdots, a_L^T)$のように記述する。$a_i (i=1, \cdots, L)$は$m$次元ベクトルである。$T$は、ベクトル又は行列の転置を意味する。

[0013] $n$を１以上の自然数とする。$a$の暗号文を$[a]=([a]_1, \cdots, [a]_n)$のように記述す

る。$[a]_i$を[a]のi番目のシェアと呼ぶ。ただし、n=1のとき、$[a]=[a]_1$である。また、$[a]=([a]_1,\cdots,[a]_m)$をm次のベクトルaの暗号文とする。同様に、$[A]=([a_{j,k}])_{1\leqq j\leqq m,1\leqq k\leqq L}$をm行L列の行列Aの暗号文とする。

[0014] ベクトルa内の要素の総和$s_a$を次式のように記述する。

[0015] $s_a=\Sigma_{j=1}^{m}a_j$

また、ベクトルaとベクトルbの要素同士の積abを次式の様に記述する。

[0016] $ab=(a_1b_1,\cdots,a_mb_m)$

更に、$a^2=aa$とする。

[0017] ［統計量］

a又はAの性質を示す量を統計量と呼ぶ。図３に、本発明で用いる統計量の例を示す。図３では、各統計量の記号・記法、定義及び定義と等価な式が示されている。

[0018] なお、図３の統計量の中の、レコード数、属性数、総和、二乗和及び積和の５つの統計量の少なくとも１つを基礎統計量と呼ぶことにする。

なお、図３では、レコード数、属性数、総和、二乗和及び積和は以下のように定義されている。

レコード数m:aの要素数、または、Aの行数

属性数L:Aの列数

総和$s_a$:$\Sigma_{j=1}^{m}a_j$

二乗和$s_{(a\hat{}2)}$:$\Sigma_{j=1}^{m}a_j^2$

積和$s_{ab}$:$\Sigma_{j=1}^{m}a_jb_j$

[0019] ［技術の概要］

後述する実施形態は、基礎統計量（すなわち、例えば、レコード数、属性数、総和、二乗和及び積和の少なくとも１つ）を秘密計算によって安全に計算し、基礎統計量を平文に復号して高速に分析等の計算を行う。後述する実施形態は、以下の３つのフェーズに分かれた処理を行う。

[0020] １． 暗号化フェーズ：データを暗号化し、秘匿する。

２． 秘密計算フェーズ：暗号文のままで、個々のデータから基礎統計量の

計算を処理する。

３． 計算フェーズ：計算された基礎統計量の暗号文を復号し、復号された基礎統計量を用いて目的とする計算を平文で処理する。

[0021] 後述する実施形態は、基礎統計量の計算処理にのみ秘密計算を適用している点で、従来手法と異なる。この手法を適用することで、線形回帰、主成分分析等の処理に比較的時間がかかる計算を従来よりも高速に処理可能である。

[0022] なお、線形回帰で用いる線型方程式は、例えば以下の式（１）に示す通り、基礎統計量によって構成される。

[0023] [数1]

$$\begin{pmatrix} m & s_{a_1} & \cdots & s_{a_L} \\ s_{a_1} & s_{a_1^2} & \cdots & s_{a_1 a_L} \\ \vdots & \vdots & \ddots & \vdots \\ s_{a_L} & s_{a_L a_1} & \cdots & s_{a_L a_L} \end{pmatrix} \begin{pmatrix} w_0 \\ w_1 \\ \vdots \\ w_L \end{pmatrix} = \begin{pmatrix} s_b \\ s_{a_1 b} \\ \vdots \\ s_{a_L b} \end{pmatrix} \quad \cdots (1)$$

[0024] したがって、基礎統計量を秘密計算で安全に計算した後に、例えば線型方程式を平文で解決することによって効率的にパラメータを推定することが可能である。

[0025] また、主成分分析は、例えば、Aの分散共分散行列$V=(\sigma_{as}, a_t)1 \leqq s, t \leqq L$又は相関係数行列$C=(\rho_{as}, a_t)1 \leqq s, t \leqq L$に対して、固有値及び固有ベクトル計算を行うことにより実施することができる。

[0026] 図３から、分散共分散行列は、基礎統計量から計算できることがわかる。さらに、相関係数行列も分散及び共分散から計算可能である。したがって、何れかの行列を用いる場合においても、基礎統計量さえ安全に計算することができれば、以降はその計算された基礎統計量を用いる事で主成分分析を実現できる。

[0027] ［暗号方式］

本発明では、暗号文を復号することなく、例えば以下の演算を実現できる

暗号方式を用いる。このような暗号方式を実現する手段として、参考文献１，２が知られている。

[0028] １．加算: [a],[b]を入力として、加算a+bの暗号文[a+b]を生成する。

２．乗算: [a],[b] を入力として、乗算abの暗号文[ab]を生成する。

３．総和: [a]を入力として、総和$s_a$の暗号文[$s_a$]を生成する。

４．積和:[a],[b]を入力として、積和$s_{ab}$の暗号文[$s_{ab}$]を生成する。

[0029] 〔参考文献１〕SHAMIR, Adi. "How to share a secret", Communications of the ACM, 1979, 22.11: p.612-613.

〔参考文献２〕GENTRY, Craig, et al. "Fully homomorphic encryption using ideal lattices", In: STOC. 2009. p.169-178.

[0030] ［実施形態］

秘密計算システムの実施形態は、図１に示すように、暗号文生成装置１、管理サーバ２、秘密計算装置３及び計算装置４を例えば備えている。この例では、暗号文生成装置１は、複数の登録端末$T_H$である。また、秘密計算装置３は、n台の秘密計算サーバ$M_1,\cdots,M_n$である。nは２以上の所定の整数である。さらに、計算装置４は、分析端末$T_A$である。

[0031] 暗号文生成装置１、管理サーバ２、秘密計算装置３及び計算装置４は、互いにネットワークを通じて通信可能であり、互いにデータの送受信が可能である。

[0032] 秘密計算システムは、［暗号方式］で述べた演算を処理できる秘密計算サーバ$M_1,\cdots,M_n$を用いる。各秘密計算サーバ$M_i$(i=1,…,n)はネットワークを通じて、別の秘密計算サーバ$M_j$にアクセス可能であり、互いにデータの送受信が可能である。

[0033] 秘密計算方法は、秘密計算システムを構成する装置が、図２及び以下に説明するステップＳ１からＳ１１の処理を行うことにより例えば実現される。

[0034] 暗号文生成装置１は、データを暗号化することにより暗号文を生成する（ステップＳ１）。生成された暗号文は、管理サーバ２に送信される（ステップＳ２）。

[0035] 暗号文生成装置１は、例えば複数の登録端末$T_H$である。この場合、複数の登録端末$T_H$のそれぞれは、自身が持つデータを例えば参考文献１，２に記載された手法で秘密分散することにより、データのシェアを生成する。この生成されたシェアが暗号文の一例である。

[0036] 管理サーバ２は、受信した暗号文を、秘密計算装置３に送信する（ステップＳ３）。

[0037] 秘密計算装置３は、受信した暗号文を記憶部に記憶させる（ステップＳ４）。例えば、受信した暗号文は、秘密計算装置３の秘密計算サーバ$M_i$($i=1,\cdots,n$)の図示していない記憶部に記憶される。

[0038] 計算装置４は、管理サーバ２に計算依頼を送信する（ステップＳ５）。計算装置４は、例えば分析端末$T_A$である。この場合、分析端末$T_A$は、計算依頼としての分析依頼を管理サーバ２に送信する。

[0039] 管理サーバ２は、受信した計算依頼に対応する計算を行うために必要な基礎統計量の計算依頼である基礎統計量計算依頼を秘密計算装置３に送信する（ステップＳ６）。

[0040] 秘密計算装置３は、記憶部から読み込んだ暗号文を用いて、この暗号文を秘匿化したまま、所定の基礎統計量を秘密計算することにより暗号化された基礎統計量を生成する（ステップＳ７）。

[0041] 秘密計算装置３は、例えば秘密計算サーバ$M_1,\cdots,M_n$である。この場合、秘密計算サーバ$M_1,\cdots,M_n$が、共同して、例えば参考文献１，２に記載された手法を用いて、記憶部から読み込んだ暗号文を用いて、この暗号文を秘匿化したまま、所定の基礎統計量を秘密計算する。

[0042] 生成された暗号化された基礎統計量は、管理サーバ２に送信される（ステップＳ８）。

所定の基礎統計量は、受信した基礎統計量計算依頼に対応する基礎統計量である。

[0043] 管理サーバ２は、受信した暗号化された基礎統計量を計算装置４に送信する（ステップＳ９）。

[0044] 計算装置４は、受信した暗号化された基礎統計量を復号することにより復号された基礎統計量を生成する（ステップＳ１０）。

[0045] 計算装置４は、復号された基礎統計量を用いて所定の計算を行う（ステップＳ１１）。所定の計算の例は、上記の実施形態のポイントの１つは、統計量のみで計算できる分析の特徴と秘密計算の性質を組み合わせた部分にある。

[0046] レコード数、総和、平均及び分散といった統計量は、個々のデータではなくデータ集合の特徴を示す数値である。そのため、これらの統計量のみを用いて計算する分析においては、データ集合について解ればよく、個々のデータそのものは必要としない。しかし、分析のアルゴリズム上、統計量を計算することは不可避であり、その統計量を計算するために個々のデータに触れなければならない。

[0047] 一方で、秘密計算は、暗号文によりデータを秘匿したまま安全に計算可能だが、一般に平文による計算よりも遅い。特に、除算等の複雑な計算処理に対しては速度差が顕著に現れるため、複雑な計算を要する分析を秘密計算で全て実装することはコストが高い。反対に、［暗号方式］の欄で示した加算や乗算は秘密計算でも十分高速であり、これらの演算に基づく基礎統計量は秘密計算で高速に処理できる。

[0048] したがって、基礎統計量に基づく統計量から計算できる分析では、基礎統計量を計算する部分のみを秘密計算で処理することで個々のデータの中身は秘匿し、計算した基礎統計量を平文に復号することで、分析の計算を高速に処理することができる。これにより、安全性と高速性を両立させた分析が実現される。

[0049] なお、上記の実施形態では、管理サーバ２と計算装置４とが別装置として記述されているが、管理サーバ２と計算装置４は同一の装置に実現されていてもよい。

[0050] ［実施例］

［[実施例１]］

実施例１は、線形単回帰分析を行う実施例である。より具体的には、実施例１は、計算装置４である分析端末$T_A$が、秘密計算装置３であるn台の秘密計算サーバ$M_1,\cdots,M_n$を用いて、暗号文生成装置１である登録端末$T_H$が持つm世帯の収入データaと支出データb間の以下の線形モデル

$b=w_0+w_1a$

について、パラメータ$w_0,w_1$の推定を行う実施例である。

[0051] 〈暗号化フェーズ〉

暗号化フェーズとして、ステップＳ１からＳ３において、以下の処理が行われる。

[0052] 登録端末$T_H$は、例えば参考文献１，２の暗号方式を用いて、a,b,mを暗号化する。

[0053] 登録端末$T_H$は、暗号文であるシェア$[a]_i$，$[b]_i$，$[m]_i$と平文mを秘密計算サーバ$M_1,\cdots,M_n$に対して送信する。

[0054] 〈秘密計算フェーズ〉

秘密計算フェーズとして、ステップＳ７からＳ９において、以下の処理が行われる。

[0055] 各秘密計算サーバ$M_i$は、［暗号方式］の欄で示した総和の秘密計算により、$[a]_i$，$[b]_i$を用いて、$[s_a]_i$，$[s_b]_i$を求める。ここで、$a=(a_1,\cdots,a_m)$として$s_a=\Sigma_{j=1}^{m}a_j$であり、$b=(b_1,\cdots,b_m)$として$s_b=\Sigma_{j=1}^{m}b_j$である。

[0056] 各秘密計算サーバ$M_i$は、［暗号方式］の欄で示した積和の秘密計算により、$[a]_i$，$[b]_i$を用いて、$[s_{a\hat{}2}]_i$と$[s_{ab}]_i$を求める。ここで、$a=(a_1,\cdots,a_m)$,$b=(b_1,\cdots,b_m)$として$s_{a\hat{}2}=\Sigma_{j=1}^{m}a_j^2$,$s_{ab}=\Sigma_{j=1}^{m}a_jb_j$である。

[0057] 各秘密計算サーバ$M_i$は、求めた$[s_a]_i$,$[s_b]_i$,$[s_{a\hat{}2}]_i$,$[s_{ab}]_i$と$[m]_i$を分析端末$T_A$に送信する。

[0058] 〈計算フェーズ〉

計算フェーズとして、ステップＳ１０及びＳ１１において、以下の処理が行われる。

[0059] 分析端末$T_A$は、受け取ったシェアを用いて、$s_a$，$s_b$，$s_{a\hat{}2}$，$s_{ab}$，mを復号する

。

[0060] 分析端末$T_A$は、$s_a$，$s_b$，mを用いて、$\mu_a=(1/m)s_a$，$\mu_b=(1/m)s_b$を計算する。

[0061] 分析端末$T_A$は、$s_a$，$s_b$，$s_{a\hat{}2}$，$s_{ab}$，mを用いて、$\sigma_a^2=(1/m)s_{a\hat{}2}-(1/m^2)s_a^2$，$\sigma_{a,b}=(1/m)s_{ab}-(1/m^2)s_as_b$を計算する。

[0062] 分析端末$T_A$は、$w_1=(\sigma_{a,b})/(\sigma_a^2)$を計算する。

[0063] 分析端末$T_A$は、$w_0=\mu_b-w_1\mu_a$を計算する。

[0064] [[実施例２]]

実施例２は、線形回帰分析を行う実施例である。より具体的には、実施例２は、計算装置４である分析端末$T_A$が、秘密計算装置３であるn台の秘密計算サーバ$M_1,\cdots,M_n$を用いて、暗号文生成装置１である登録端末$T_H$が持つレコード数m、属性数Lの行列Aとレコード数mのベクトルb間の以下の線形モデル

$b=w_0+w_1a_1+\cdots+w_La_L$

について、パラメータ$w=(w_0,w_1,\cdots,w_L)$の推定を行う実施例である。

[0065] <暗号化フェーズ>

暗号化フェーズとして、ステップＳ１からＳ３において、以下の処理が行われる。

[0066] 登録端末$T_H$は、例えば参考文献１，２の暗号方式を用いて、A,b,m,Lを暗号化する。

[0067] 登録端末$T_H$は、暗号文であるシェア$[A]_i$，$[b]_i$，$[m]_i$，$[L]_i$と平文m,Lを秘密計算サーバ$M_1,\cdots,M_n$に対して送信する。

[0068] <秘密計算フェーズ>

秘密計算フェーズとして、ステップＳ７からＳ９において、以下の処理が行われる。

[0069] 各秘密計算サーバ$M_i$は、［暗号方式］の欄で示した総和の秘密計算により、$[A]_i$，$[b]_i$を用いて、$[s_A]_i=([s_{a1}]_i,\cdots,[s_{aL}]_i)$，$[s_b]_i$を求める。ここで、$q=1,\cdots,L$として$s_{aq}=\Sigma_{j=1}^m a_{j,q}$であり、$b=(b_1,\cdots,b_m)$として$s_b=\Sigma_{j=1}^m b_j$である。

[0070] 各秘密計算サーバ$M_i$は、［暗号方式］の欄で示した積和により、$[A]_i$，$[b]_i$を用いて、$[S_A]_i=([s_{ajak}]_i)_{1\leqq j,k\leqq L}$=と$[s_{Ab}]_i=([s_{a1b}]_i,\cdots,[s_{aLb}]_i)$を計算する。こ

こで、$s_{ajak}=\Sigma_{r=1}^{m}a_{r,j}a_{r,k}$であり、q=1,…,Lとして$s_{aqb}=\Sigma_{r=1}^{m}a_{r,q}b_r$である。

[0071] 各秘密計算サーバ$M_i$は、求めた$[s_A]_i$，$[s_b]_i$，$[S_A]_i$，$[s_{Ab}]_i$と$[m]_i$，$[L]_i$を分析端末$T_A$に送信する。

[0072] 〈計算フェーズ〉

計算フェーズとして、ステップＳ１０及びＳ１１において、以下の処理が行われる。

[0073] 分析端末$T_A$は、受け取ったシェアを用いて、$s_A$，$s_b$，$S_A$，$s_{Ab}$，m，Lを復号する。

[0074] 分析端末$T_A$は、$s_A$，$s_b$，$S_A$，$s_{Ab}$，m，Lを用いて、式（１）の線形方程式を構成する。

[0075] 分析端末$T_A$は、例えばGauss の消去法を用いて式（１）を解き、$w=(w_0,\cdots,w_L)$を求める。

[0076] [[実施例３]]

実施例３は、主成分分析を行う実施例である。より具体的には、実施例２は、計算装置４である分析端末$T_A$が、秘密計算装置３であるn台の秘密計算サーバ$M_1,\cdots,M_n$を用いて、暗号文生成装置１である登録端末$T_H$が持つレコード数m、属性数Lの行列であるデータAに対して主成分分析を行い、各主成分$p=(p_1,\cdots,p_L)$を求める実施例である。

[0077] 〈暗号化フェーズ〉

暗号化フェーズとして、ステップＳ１からＳ３において、以下の処理が行われる。

[0078] 登録端末$T_H$は、例えば参考文献１，２の暗号方式を用いて、A,m,Lを暗号化する。

[0079] 登録端末$T_H$は、暗号文であるシェア$[A]_i$，$[m]_i$，$[L]_i$と平文m,Lを秘密計算サーバ$M_1,\cdots,M_n$に対して送信する。

[0080] 〈秘密計算フェーズ〉

秘密計算フェーズとして、ステップＳ７からＳ９において、以下の処理が行われる。

[0081] 各秘密計算サーバ$M_i$は、［暗号方式］の欄で示した総和により、$[A]_i$を用いて、$[s]_i=([s_{a1}]_i,\cdots,[s_{aL}]_i)$を求める。ここで、$q=1,\cdots,L$として$s_{ai}=\Sigma_{j=1}^{m}a_{q,j}$である。

[0082] 各秘密計算サーバ$M_i$は、［暗号方式］の欄で示した積和により、$[A]_i$を用いて、$[S]_i=([s_{ajak}]_i)_{1\leqq j,k\leqq L}$を計算する。ここで、$s_{ajak}=\Sigma_{r=1}^{m}a_{r,j}a_{r,k}$である。

[0083] 各秘密計算サーバ$M_i$は、求めた$[s]_i$, $[S]_i$と$[m]_i$, $[L]_i$を分析端末$T_A$に送信する。

[0084] 〈計算フェーズ〉

計算フェーズとして、ステップＳ１０及びＳ１１において、以下の処理が行われる。

[0085] 分析端末$T_A$は、受け取ったシェアを用いて、s, S, m, Lを復号する。

[0086] 分析端末$T_A$は、s, S, m, Lを用いて、$V=(\sigma_{aj,ak})_{1\leqq j,k\leqq L}=((1/m)s_{ajak}-(1/m^2)s_{aj}s_{ak})_{1\leqq j,k\leqq L}$を求める。

[0087] 分析端末$T_A$は、Vを用いて、$C=((\sigma_{aj,ak})/(\sigma_{aj}^2\sigma_{ak}^2)^{1/2})_{1\leqq j,k\leqq L}$を求める。ここで、$\sigma_{aj}^2=(1/m)s_{aj\hat{}2}-(1/m^2)s_{aj}^2$であり、$\sigma_{ak}^2=(1/m)s_{ak\hat{}2}-(1/m^2)s_{ak}^2$である。

[0088] 分析端末$T_A$は、Cに対して固有値及び固有ベクトルの計算を行い、$p=(p_1,\cdots,p_L)$を求める。

[0089] ［プログラム及び記録媒体］

例えば、各装置における処理をコンピュータによって実現する場合、各装置の各部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、その各装置の処理がコンピュータ上で実現される。

[0090] 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。

[0091] また、各部の処理は、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構成することにしてもよいし、これらの処理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。

[0092] その他、この発明の趣旨を逸脱しない範囲で適宜変更が可能であることはいうまでもない。

# 請求の範囲

[請求項1] データを秘匿化したまま計算を行う秘密計算システムであって、

上記データを暗号化することにより暗号文を生成する暗号文生成装置と、

上記暗号文を秘匿化したまま上記暗号文を用いて所定の基礎統計量を秘密計算することにより暗号化された基礎統計量を生成する秘密計算装置と、

上記暗号化された基礎統計量を復号することにより復号された基礎統計量を生成し、上記復号された基礎統計量を用いて所定の計算を行う計算装置と、

を含む秘密計算システム。

[請求項2] 請求項１の秘密計算システムにおいて、

上記所定の基礎統計量は、上記データのレコード数、属性数、総和、二乗和、積和の少なくとも１つである、

秘密計算システム。

[請求項3] データを秘匿化したまま計算を行う秘密計算方法であって、

暗号文生成装置が、上記データを暗号化することにより暗号文を生成する暗号文生成装置と、

秘密計算装置が、上記暗号文を秘匿化したまま上記暗号文を用いて所定の基礎統計量を秘密計算することにより暗号化された基礎統計量を生成する秘密計算ステップと、

計算装置が、上記暗号化された基礎統計量を復号することにより復号された基礎統計量を生成し、上記復号された基礎統計量を用いて所定の計算を行う計算ステップと、

を含む秘密計算方法。

[図1]

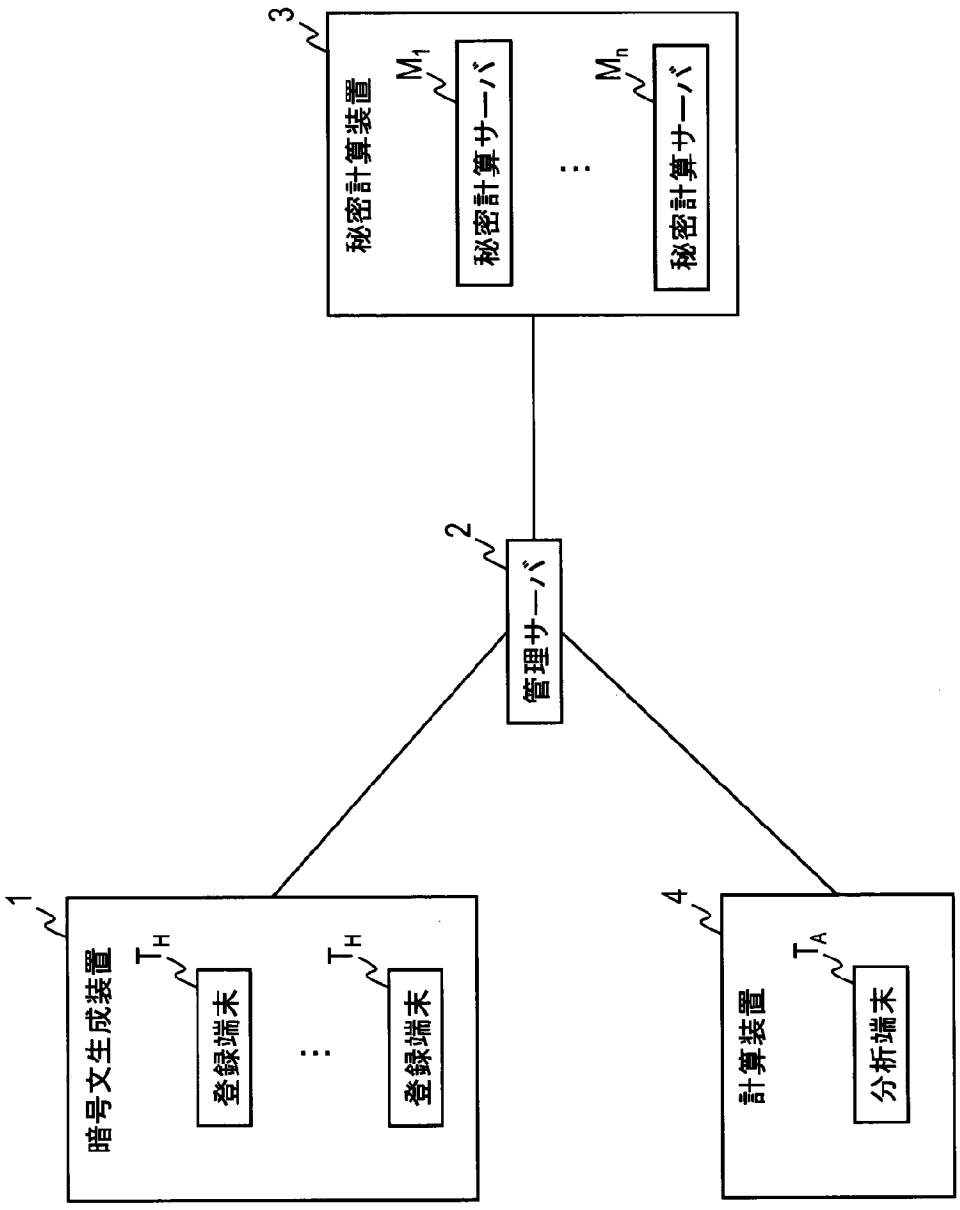

3
秘密計算装置
$M_1$
秘密計算サーバ
$M_n$
秘密計算サーバ
2
管理サーバ
1
暗号文生成装置
$T_H$
登録端末
$T_H$
登録端末
4
計算装置
$T_A$
分析端末

図1

[図2]

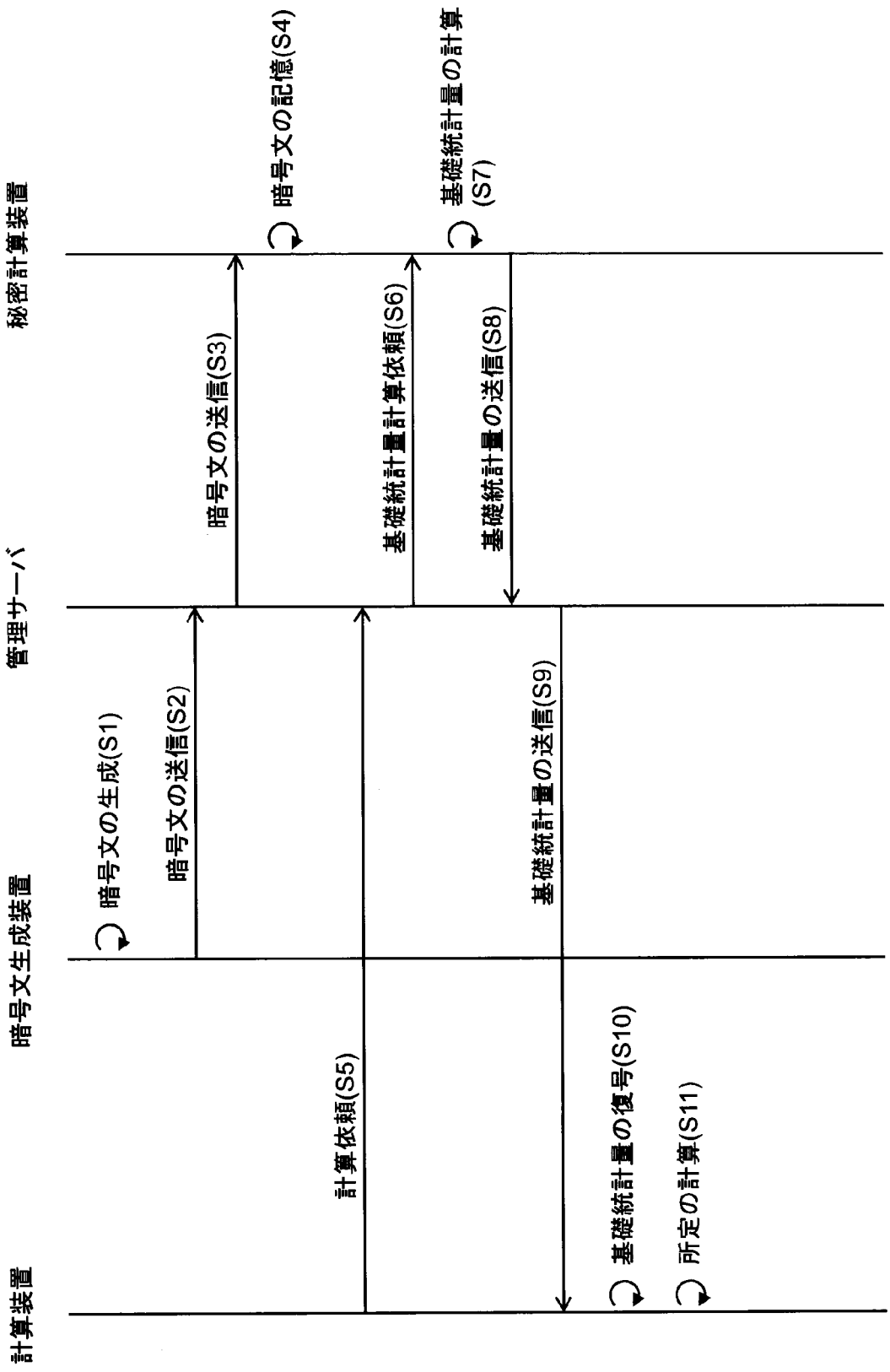

計算装置
暗号文生成装置
管理サーバ
秘密計算装置
暗号文の生成(S1)
暗号文の送信(S2)
暗号文の送信(S3)
暗号文の記憶(S4)
計算依頼(S5)
基礎統計量計算依頼(S6)
基礎統計量の計算(S7)
基礎統計量の送信(S8)
基礎統計量の送信(S9)
基礎統計量の復号(S10)
所定の計算(S11)

図2

[図3]

| 統計量 | 記号・記法 | 定義 | 等価な式 |
|---|---|---|---|
| レコード数 | $m$ | a の要素数，または，$A$ の行数 | - |
| 属性数 | $L$ | $A$ の列数 | - |
| 総和 | $s_{\mathbf{a}}$ | $\sum_{j=1}^{m} a_j$ | - |
| 二乗和 | $s_{\mathbf{a}^2}$ | $\sum_{j=1}^{m} a_j^2$ | - |
| 積和 | $s_{\mathbf{ab}}$ | $\sum_{j=1}^{m} a_j b_j$ | - |
| 平均 | $\mu_{\mathbf{a}}$ | $\frac{1}{m}\sum_{j=1}^{m} a_j$ | $\frac{1}{M} s_{\mathbf{a}}$ |
| 二乗平均 | $\mu_{\mathbf{a}^2}$ | $\frac{1}{m}\sum_{j=1}^{m} a_j^2$ | $\frac{1}{m} s_{\mathbf{a}^2}$ |
| 積和平均 | $\mu_{\mathbf{ab}}$ | $\frac{1}{m}\sum_{j=1}^{m} a_j b_j$ | $\frac{1}{m} s_{\mathbf{ab}}$ |
| 分散 | $\sigma_{\mathbf{a}}^2$ | $\frac{1}{m}\sum_{j=1}^{m} (a_j - \mu_{\mathbf{a}})^2$ | $\frac{1}{m} s_{\mathbf{a}^2} - \frac{1}{m^2} s_{\mathbf{a}}^2$ |
| 共分散 | $\sigma_{\mathbf{a},\mathbf{b}}$ | $\frac{1}{m}\sum_{j=1}^{m} (a_j - \mu_{\mathbf{a}})(b_j - \mu_{\mathbf{b}})$ | $\frac{1}{m} s_{\mathbf{ab}} - \frac{1}{m^2} s_{\mathbf{a}} s_{\mathbf{b}}$ |
| 標準偏差 | $\sigma_{\mathbf{a}}$ | $\sqrt{\frac{1}{m}\sum_{j=1}^{m} (a_j - \mu_{\mathbf{a}})^2}$ | $\sqrt{\sigma_{\mathbf{a}}^2}$ |
| 相関係数 | $\rho_{\mathbf{a},\mathbf{b}}$ | $\frac{\sigma_{\mathbf{a},\mathbf{b}}}{\sigma_{\mathbf{a}}\sigma_{\mathbf{b}}}$ | $\frac{\sigma_{\mathbf{a},\mathbf{b}}}{\sqrt{\sigma_{\mathbf{a}}^2 \sigma_{\mathbf{b}}^2}}$ |

図3

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2018/046130

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G09C1/00(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

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 2016/178291 A1 (NEC CORP.) 10 November 2016, paragraphs [0033]-[0072], [0122]-[0139] & US 2018/0139045 A1, paragraphs [0073]-[0122], [0182]-[0207] | 1-3 |
| X | 田中哲士, 他, 公的統計への秘密計算適用に向けたミクロデータの統計分析, マルチメディア, 分散, 協調とモバイル(DICOMO2017)シンポジウム論文集, 21 June 2017, pp. 424-429 in particular, 2.3 Secure computation, 4.1 Secure computation of linear-regression, 5.1 Implementation environment, non-official translation (TANAKA Satoshi et al., "Statistical analysis of microdata for applying secure computation to official statistics", Proceedings of Multimedia, Distributed, Cooperative, and Mobile (DICOMO 2017) Symposium) | 1-3 |

☐ 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<br>05 March 2019 (05.03.2019) | Date of mailing of the international search report<br>12 March 2019 (12.03.2019) |
| Name and mailing address of the ISA/<br>Japan Patent Office<br>3-4-3, Kasumigaseki, Chiyoda-ku,<br>Tokyo 100-8915, Japan | Authorized officer<br><br>Telephone No. |

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１８／０４６１３０

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

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

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）

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 | WO 2016/178291 A1 (日本電気株式会社) 2016.11.10,<br>段落 0033-0072, 0122-0139<br>& US 2018/0139045 A1, 段落 0073-0122, 0182-0207 | 1-3 |
| X | 田中 哲士, 他,<br>公的統計への秘密計算適用に向けたミクロデータの統計分析,<br>マルチメディア, 分散, 協調とモバイル(DICOMO2017)シンポジウム論文集, 2017.06.21, pp. 424-429<br>特に, 2.3 秘密計算, 4.1 線形回帰の秘密計算及び5.1 実装環境 | 1-3 |

☐　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 |
|---|---|
| ０５．０３．２０１９ | １２．０３．２０１９ |

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　４５３８
金沢　史明
電話番号　０３－３５８１－１１０１　内線　３５４６