

(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
2016年10月6日(06.10.2016)



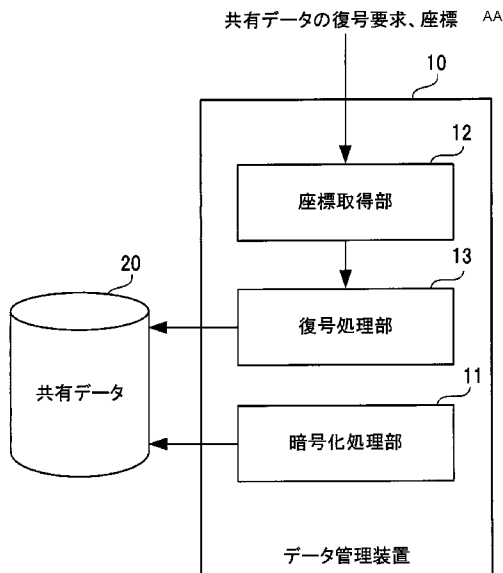
(10) 国際公開番号
WO 2016/158721 A1

- (51) 国際特許分類:
H04L 9/08 (2006.01) G06F 21/62 (2013.01)
G06F 21/60 (2013.01)
- (21) 国際出願番号: PCT/JP2016/059555
- (22) 国際出願日: 2016年3月25日(25.03.2016)
- (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 2015-066878 2015年3月27日(27.03.2015) JP
- (71) 出願人: NECソリューションイノベータ株式会社(NEC SOLUTION INNOVATORS, LTD.) [JP/JP];
〒1368627 東京都江東区新木場一丁目18番7号 Tokyo (JP).
- (72) 発明者: 野田 潤(NODA, Jun); 〒1368627 東京都江東区新木場一丁目18番7号NECソリューションイノベータ株式会社内 Tokyo (JP).
- (74) 代理人: 特許業務法人ブライタス(BRIGHTAS IP ATTORNEYS); 〒5300057 大阪府大阪市北区曽根崎2丁目5番10号 Osaka (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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),

[続葉有]

(54) Title: DATA MANAGEMENT DEVICE, DATA MANAGEMENT METHOD AND COMPUTER READABLE STORAGE MEDIUM

(54) 発明の名称: データ管理装置、データ管理方法、及びコンピュータ読み取り可能な記録媒体



- 10 Data management device
11 Encryption processing unit
12 Coordinates acquisition unit
13 Decryption processing unit
20 Shared data
AA Shared data decryption request and coordinates

(57) Abstract: A data management device 10 is for managing data shared by a plurality of users. The data management device 10 is provided with: an encryption processing unit 11 which encrypts shared data; a coordinates acquisition unit 12 which, when one of the plurality of users seeks decryption of shared data and coordinates that were pre-assigned to the one user are sent, asks each of the remaining users to send the coordinates respectively pre-assigned thereto; and a decryption processing unit 13 which, when each of the remaining users sends the respective pre-assigned coordinates, calculates a function from the coordinates sent from the one user and the coordinates sent from the remaining users, and uses a value obtained from the calculated function as a decryption key to decrypt the encrypted shared data.

(57) 要約: データ管理装置10は、複数のユーザで共有されるデータを管理するための装置である。データ管理装置10は、共有データを暗号化する、暗号化処理部11と、複数のユーザのうちの一つのユーザが共有データの復号を求めると共に、一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、座標取得部12と、残りのユーザそれぞれが、予め付与された座標を送信してきた場合に、一のユーザが送信してきた座標と、残りのユーザが送信してきた座標とから、関数を算出し、算出した関数から求められる値を復号キーとして用いて、暗号化された共有データを復号する、復号処理部13と、を備えている。

WO 2016/158721 A1



OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

データ管理装置、データ管理方法、及びコンピュータ読み取り可能な記録媒体

技術分野

[0001] 本発明は、データベースを管理するための、データ管理装置、データ管理方法、及びこれらを実現するためのプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

背景技術

[0002] 一般に、食品は、複雑な流通経路を辿って消費者の元へと供給されている。特に、加工食品においては、材料製造業者、加工業者等での処理が必要となるため、流通経路は更に複雑となる。

[0003] また、食品の安全性は、消費者の健康に関わることから、何らかの問題が生じた場合は、流通経路のどこに問題の原因が存在しているのかを特定する必要があるが、そのためには、川下から川上へと一社毎に、記録を辿っていく必要がある。従って、現状では、問題の原因の特定には、多くの人手と時間とが必要となる。

[0004] このような問題の解決策としては、川上側と川下側とで隣接する２社の間に、両者が共有するデータベースを設け、両者でデータ内容を共有することが挙げられる。具体的には、例えば、加工食品を製造する会社Ａと、そこに材料を供給する会社Ｂとの間に、両者が共有するデータベースを設け、両者のデータを共有しておくことが挙げられる。

[0005] この場合において、会社Ａが販売する加工食品に問題が発生したとする。その時、会社Ａは、共有データベースに格納されている会社Ｂのデータを調べることで、問題が、自社で生じたのか、会社Ｂで生じたのかを、迅速に分析することができる。

[0006] また、このような共有データベースは、例えば、特許文献１に開示された

システムによって実現できる。特許文献 1 に開示されたシステムによれば、2つの組織の間で、特定のデータを安全に共有化することができる。

先行技術文献

特許文献

[0007] 特許文献1：特開平 1 0 - 1 1 1 8 9 7 号公報

発明の概要

発明が解決しようとする課題

[0008] しかしながら、特許文献 1 に開示されたシステムでは、第三者によるデータの改竄を防ぐことはできるが、共有者の一方によるデータの改竄を防ぐことは困難である。このため、食品の流通過程に問題が生じたときに、共有者の一方がデータを改竄してしまい、問題の究明が困難になってしまう可能性がある。

[0009] 本発明の目的の一例は、上記問題を解消し、共有されているデータにおける共有者の一方による改竄を抑制し得る、データ管理装置、データ管理方法、及びコンピュータ読み取り可能な記録媒体を提供することにある。

課題を解決するための手段

[0010] 上記目的を達成するため、本発明の一側面におけるデータ管理装置は、複数のユーザで共有されるデータを管理するための装置であって、

前記共有データを暗号化する、暗号化処理部と、

前記複数のユーザのうちの一のユーザが前記共有データの復号を求めると共に、前記一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、座標取得部と、

前記残りのユーザそれぞれが、予め付与された前記座標を送信してきた場合に、前記一のユーザが送信してきた前記座標と、前記残りのユーザが送信してきた前記座標とから、関数を算出し、算出した関数から求められる値を復号キーとして用いて、暗号化された前記共有データを復号する、復号処理

部と、
を備えている、
ことを特徴とする。

[0011] また、上記目的を達成するため、本発明の一側面におけるデータ管理方法は、複数のユーザで共有されるデータを管理するための方法であって、

(a) 前記共有データを暗号化する、ステップと、
(b) 前記複数のユーザのうちの一のユーザが前記共有データの復号を求めると共に、前記一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、ステップと、
(c) 前記残りのユーザそれぞれが、予め付与された前記座標を送信してきた場合に、前記一のユーザが送信してきた前記座標と、前記残りのユーザが送信してきた前記座標とから、関数を算出し、算出した関数から求められる値を復号キーとして用いて、暗号化された前記共有データを復号する、ステップと、
を有する、
ことを特徴とする。

[0012] 更に、上記目的を達成するため、本発明の一側面におけるコンピュータ読み取り可能な記録媒体は、複数のユーザで共有されるデータをコンピュータによって管理するためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

前記コンピュータに、

(a) 前記共有データを暗号化する、ステップと、
(b) 前記複数のユーザのうちの一のユーザが前記共有データの復号を求めると共に、前記一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、ステップと、
(c) 前記残りのユーザそれぞれが、予め付与された前記座標を送信してき

た場合に、前記一のユーザが送信してきた前記座標と、前記残りのユーザが送信してきた前記座標とから、関数を算出し、算出した関数から求められる値を復号キーとして用いて、暗号化された前記共有データを復号する、ステップと、

を実行させる命令を含む、プログラムを記録していることを特徴とする。

発明の効果

[0013] 以上のように、本発明によれば、共有されているデータにおける共有者の一方による改竄を抑制することができる。

図面の簡単な説明

[0014] [図1]図1は、本発明の実施の形態におけるデータ管理装置の構成を概略的に示すブロック図である。

[図2]図2は、本発明の実施の形態におけるデータ管理装置の構成を具体的に示すブロック図である。

[図3]図3は、本発明の実施の形態において算出される関数及び復号キーの一例を示す図である。

[図4]図4は、本発明の実施の形態におけるデータ管理装置の動作を示すフロー図である。

[図5]図5は、本発明の実施の形態におけるデータ管理装置を実現するコンピュータの一例を示すブロック図である。

発明を実施するための形態

[0015] (実施の形態)

以下、本発明の実施の形態におけるデータ管理装置、データ管理方法、及びプログラムについて、図1～図5を参照しながら説明する。

[0016] [装置構成]

最初に、本実施の形態におけるデータ管理装置の構成について図1を用いて説明する。図1は、本発明の実施の形態におけるデータ管理装置の構成を概略的に示すブロック図である。

[0017] 図1に示す、本実施の形態におけるデータ管理装置10は、複数のユーザ

で共有されるデータ（以下「共有データ」と表記する。）20を管理するための装置である。図1に示すように、データ管理装置10は、暗号化処理部11と、座標取得部12と、復号処理部13とを備えている。このうち、暗号化処理部11は、共有データ20を暗号化する。

[0018] 座標取得部12は、複数のユーザのうちの一のユーザが共有データ20の復号を求めると共に、一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める。

[0019] 復号処理部13は、残りのユーザそれぞれが、予め付与された座標を送信してきた場合に、一のユーザが送信してきた座標と、残りのユーザが送信してきた座標とから、関数を算出する。そして、復号処理部13は、算出した関数から求められる値を復号キーとして用いて、暗号化された共有データを復号する。

[0020] このように、本実施の形態では、ユーザ全員から座標を取得して初めて共有データ20の復号が可能となる。また、各ユーザが、自身が保有する座標だけで、復号キーの元になる関数を算出することは不可能である。このため、本実施の形態によれば、共有データ20の共有者の一方による改竄が抑制されることになる。

[0021] ここで、図2及び図3を用いて、本実施の形態におけるデータ管理装置10の構成について更に具体的に説明する。図2は、本発明の実施の形態におけるデータ管理装置の構成を具体的に示すブロック図である。図3は、本発明の実施の形態において算出される関数及び復号キーの一例を示す図である。

[0022] 図2に示すように、本実施の形態では、データ管理装置10は、ネットワーク30を介して、A社のサーバ40と、B社のサーバ50とに接続されている。A社及びB社それぞれがユーザである。また、共有データ20は、データベース21に格納されている。

[0023] また、本実施の形態では、ユーザはA社とB社との2つであるので、デー

タ管理装置 10 が取得する座標の数は 2 つである。このため、復号処理部 13 は、 $y = ax + b$ で表される 1 次関数を算出する。なお、 a 及び b は任意の定数である。

[0024] 具体的には、図 3 に示すように、ユーザである A 社及び B 社は、それぞれ、データとして、2 次元平面における座標データを所有している。図 3 の例では、A 社は、点 P の座標 (x_1, y_1) を所有し、B 社は、点 Q の座標 (x_2, y_2) を所有している。

[0025] そして、例えば A 社が共有データ 20 を復号して更新することを求める場合は、A 社のサーバ 40 は、データ管理装置 10 に対して、共有データ 20 の復号を要求すると共に、点 P の座標 (x_1, y_1) を送信する。これにより、データ管理装置 10 において、座標取得部 12 は、A 社からの要求と点 P の座標とを受信すると、B 社のサーバ 50 に対して点 Q の座標 (x_2, y_2) を送信するように依頼する。

[0026] 続いて、B 社サーバ 50 から点 Q の座標 (x_2, y_2) が送信されてくると、データ管理装置 10 において、復号処理部 13 は、送信されてきた点 Q の座標と先に送信されてきた点 P の座標とを用いて、1 次関数 ($y = ax + b$) を算出する。

[0027] また、復号処理部 13 は、は、算出した 1 次関数に、予め設定された x (又は y) の値 X を代入して、 y (又は x) の値 Y を算出し、算出した値 Y を復号キーとして用いて、共有データ 20 を復号する。その後、A 社のサーバ 40 は、復号された共有データ 20 を更新する。

[0028] また、図 3 に示した例では、2 人のユーザがデータを共有する場合について説明しているが、本実施の形態はこれに限定されない。ユーザの数は、3 人以上であっても良い。つまり、復号処理部 13 は、ユーザが N 人である場合に、関数として ($N - 1$) 次関数を算出し、算出した ($N - 1$) 次関数の ($N - 1$) 個の変数に設定値を代入し、得られた残りの変数の値を、復号キーとして用いる、 N は 2 以上の自然数である。また、本実施の形態において、ユーザは、「個人」だけでなく、図 2 及び図 3 の例に示すように「組織」

であっても良い。

[0029] [装置動作]

次に、本発明の実施の形態におけるデータ管理装置 10 の動作について図 4 を用いて説明する。図 4 は、本発明の実施の形態におけるデータ管理装置の動作を示すフロー図である。以下の説明においては、適宜図 1 ～図 3 を参照する。また、本実施の形態では、データ管理装置 10 を動作させることによって、データ管理方法が実施される。よって、本実施の形態におけるデータ管理方法の説明は、以下のデータ管理装置 10 の動作説明に代える。

[0030] まず、前提として、共有データ 20 は、予め、データ管理装置 10 の暗号化処理部 11 によって暗号化された状態で、データベース 21 に格納されているとする。また、ユーザは、A 社及び B 社の 2 つであるとする。

[0031] 図 4 に示すように、まず、A 社のサーバ 40 及び B 社のサーバ 50 のいずれかから、共有データ 20 の復号要求と座標とが送信されてくると、データ管理装置 10 において、座標取得部 12 が、これらの復号要求と座標とを受信する（ステップ A1）。

[0032] 次に、座標取得部 12 は、他方のユーザに対して、座標の送信を要求する（ステップ A2）。そして、座標取得部 12 は、他方のユーザが、それが保有する座標を送信してきたかどうかを判定する（ステップ A3）。具体的には、座標取得部 12 は、他方のユーザのサーバから、座標データが送信されてくると、座標が送信されてきたと判定する。一方、座標取得部 12 は、他方のユーザのサーバから、設定時間が経過するまでにデータの送信が無かった場合、又は他方のユーザのサーバから、座標送信の拒否を示すデータの送信があった場合は、座標が送信されてこなかったと判定する。

[0033] ステップ A3 の判定の結果、他方のユーザが座標を送信してこなかった場合は、他方のユーザが共有データ 20 の更新に同意しなかった場合であるので、データ管理装置 10 における処理は終了する。

[0034] 一方、ステップ A3 の判定の結果、他方のユーザが座標を送信してきた場合は、座標取得部 12 は、送信してきた座標を受信し、受信した他方のユー

ザの座標と先に受信した座標とを復号処理部 13 に受け渡す。これにより、復号処理部 13 は、受け取った 2 つの座標を用いて、1 次関数 ($y = ax + b$) を算出する (ステップ A4)。

[0035] 次に、復号処理部 13 は、は、ステップ A4 で算出した 1 次関数に、予め設定された x (又は y) の値を代入して、 y (又は x) の値を算出し、算出した値を復号キーとして用いて、共有データ 20 を復号する (ステップ A5)。その後、復号を要求したサーバは、復号された共有データ 20 を更新する。

[0036] 以上のように、図 1 及び図 2 に示すデータ管理装置 10 によれば、データベース 21 を共有するユーザは、他方のユーザの許可を得ない限り、共有データを更新することができなくなる。このため、一方のユーザが勝手に共有データ 20 を改竄する事態の発生が抑制される。

[0037] [プログラム]

本実施の形態におけるプログラムは、コンピュータに、図 4 に示すステップ A1 ~ A5 を実行させるプログラムであれば良い。このプログラムをコンピュータにインストールし、実行することによって、本実施の形態におけるデータ管理装置 10 とデータ管理方法とを実現することができる。この場合、コンピュータの CPU (Central Processing Unit) は、暗号化処理部 11、座標取得部 12、及び復号処理部 13 として機能し、処理を行なう。

[0038] また、本実施の形態では、データベース 21 は、コンピュータに備えられたハードディスク等の記憶装置に、これらを構成するデータファイルを格納することによって実現できる。なお、データベース 21 を実現する記憶装置は、このデータファイルが格納された記録媒体を、コンピュータと接続された読取装置に搭載することによって実現されていても良い。

[0039] ここで、本実施の形態におけるプログラムを実行することによって、データ管理装置 10 を実現するコンピュータについて図 5 を用いて説明する。図 5 は、本発明の実施の形態におけるデータ管理装置を実現するコンピュータの一例を示すブロック図である。

[0040] 図5に示すように、コンピュータ110は、CPU111と、メインメモリ112と、記憶装置113と、入力インターフェイス114と、表示コントローラ115と、データリーダ／ライタ116と、通信インターフェイス117とを備える。これらの各部は、バス121を介して、互いにデータ通信可能に接続される。

[0041] CPU111は、記憶装置113に格納された、本実施の形態におけるプログラム（コード）をメインメモリ112に展開し、これらを所定順序で実行することにより、各種の演算を実施する。メインメモリ112は、典型的には、DRAM（Dynamic Random Access Memory）等の揮発性の記憶装置である。また、本実施の形態におけるプログラムは、コンピュータ読み取り可能な記録媒体120に格納された状態で提供される。なお、本実施の形態におけるプログラムは、通信インターフェイス117を介して接続されたインターネット上で流通するものであっても良い。

[0042] また、記憶装置113の具体例としては、ハードディスクドライブの他、フラッシュメモリ等の半導体記憶装置が挙げられる。入力インターフェイス114は、CPU111と、キーボード及びマウスといった入力機器118との間のデータ伝送を仲介する。表示コントローラ115は、ディスプレイ装置119と接続され、ディスプレイ装置119での表示を制御する。

[0043] データリーダ／ライタ116は、CPU111と記録媒体120との間のデータ伝送を仲介し、記録媒体120からのプログラムの読み出し、及びコンピュータ110における処理結果の記録媒体120への書き込みを実行する。通信インターフェイス117は、CPU111と、他のコンピュータとの間のデータ伝送を仲介する。

[0044] また、記録媒体120の具体例としては、CF（Compact Flash（登録商標））及びSD（Secure Digital）等の汎用的な半導体記憶デバイス、フレキシブルディスク（Flexible Disk）等の磁気記憶媒体、又はCD-ROM（Compact Disk Read Only Memory）などの光学記憶媒体が挙げられる。

産業上の利用可能性

[0045] 以上のように、本発明によれば、共有されているデータにおける共有者の一方による改竄を抑制することができる。本発明は、複数のユーザでデータが共有されるシステムに有用である。

[0046] 上述した実施の形態の一部又は全部は、以下に記載する（付記１）～（付記６）によって表現することができるが、以下の記載に限定されるものではない。

[0047] （付記１）

複数のユーザで共有されるデータを管理するための装置であって、

前記共有データを暗号化する、暗号化処理部と、

前記複数のユーザのうちの一のユーザが前記共有データの復号を求めると共に、前記一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、座標取得部と、

前記残りのユーザそれぞれが、予め付与された前記座標を送信してきた場合に、前記一のユーザが送信してきた前記座標と、前記残りのユーザが送信してきた前記座標とから、関数を算出し、算出した関数から求められる値を復号キーとして用いて、暗号化された前記共有データを復号する、復号処理部と、

を備えている、

ことを特徴とするデータ管理装置。

[0048] （付記２）

前記復号処理部は、前記複数のユーザが N 人である場合に、前記関数として $(N-1)$ 次関数を算出し、算出した $(N-1)$ 次関数の $(N-1)$ 個の変数に設定値を代入し、得られた残りの変数の値を、前記復号キーとして用いる、

付記１に記載のデータ管理装置。

[0049] （付記３）

複数のユーザで共有されるデータを管理するための方法であって、

(a) 前記共有データを暗号化する、ステップと、

(b) 前記複数のユーザのうちの一のユーザが前記共有データの復号を求めると共に、前記一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、ステップと、

(c) 前記残りのユーザそれぞれが、予め付与された前記座標を送信してきた場合に、前記一のユーザが送信してきた前記座標と、前記残りのユーザが送信してきた前記座標とから、関数を算出し、算出した関数から求められる値を復号キーとして用いて、暗号化された前記共有データを復号する、ステップと、

を有する、

ことを特徴とするデータ管理方法。

[0050] (付記4)

前記(c)のステップにおいて、前記複数のユーザがN人である場合に、前記関数として $(N-1)$ 次関数を算出し、算出した $(N-1)$ 次関数の $(N-1)$ 個の変数に設定値を代入し、得られた残りの変数の値を、前記復号キーとして用いる、

付記3に記載のデータ管理方法。

[0051] (付記5)

複数のユーザで共有されるデータをコンピュータによって管理するためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、前記コンピュータに、

(a) 前記共有データを暗号化する、ステップと、

(b) 前記複数のユーザのうちの一のユーザが前記共有データの復号を求めると共に、前記一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、ステップと、

(c) 前記残りのユーザそれぞれが、予め付与された前記座標を送信して

きた場合に、前記一のユーザが送信してきた前記座標と、前記残りのユーザが送信してきた前記座標とから、関数を算出し、算出した関数から求められる値を復号キーとして用いて、暗号化された前記共有データを復号する、ステップと、

を実行させる命令を含む、プログラムを記録しているコンピュータ読み取り可能な記録媒体。

[0052] (付記6)

前記(c)のステップにおいて、前記複数のユーザがN人である場合に、前記関数として $(N-1)$ 次関数を算出し、算出した $(N-1)$ 次関数の $(N-1)$ 個の変数に設定値を代入し、得られた残りの変数の値を、前記復号キーとして用いる、

付記5に記載のコンピュータ読み取り可能な記録媒体。

[0053] 以上、実施の形態を参照して本願発明を説明したが、本願発明は上記実施の形態に限定されるものではない。本願発明の構成や詳細には、本願発明の Scope 内で当業者が理解し得る様々な変更をすることができる。

[0054] この出願は、2015年3月27日に提出された日本出願特願2015-066878を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

[0055] 10 データ管理装置

11 暗号化処理部

12 座標取得部

13 復号処理部

20 共有データ

21 データベース

30 ネットワーク

40、50 サーバ

110 コンピュータ

- 1 1 1 C P U
- 1 1 2 メインメモリ
- 1 1 3 記憶装置
- 1 1 4 入力インターフェイス
- 1 1 5 表示コントローラ
- 1 1 6 データリーダ／ライタ
- 1 1 7 通信インターフェイス
- 1 1 8 入力機器
- 1 1 9 ディスプレイ装置
- 1 2 0 記録媒体
- 1 2 1 バス

請求の範囲

[請求項1]

複数のユーザで共有されるデータを管理するための装置であって、
前記共有データを暗号化する、暗号化処理部と、

前記複数のユーザのうちの一のユーザが前記共有データの復号を求めると共に、前記一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、座標取得部と、

前記残りのユーザそれぞれが、予め付与された前記座標を送信してきた場合に、前記一のユーザが送信してきた前記座標と、前記残りのユーザが送信してきた前記座標とから、関数を算出し、算出した関数から求められる値を復号キーとして用いて、暗号化された前記共有データを復号する、復号処理部と、

を備えている、

ことを特徴とするデータ管理装置。

[請求項2]

前記復号処理部は、前記複数のユーザが N 人である場合に、前記関数として $(N-1)$ 次関数を算出し、算出した $(N-1)$ 次関数の $(N-1)$ 個の変数に設定値を代入し、得られた残りの変数の値を、前記復号キーとして用いる、

請求項1に記載のデータ管理装置。

[請求項3]

複数のユーザで共有されるデータを管理するための方法であって、
(a) 前記共有データを暗号化する、ステップと、

(b) 前記複数のユーザのうちの一のユーザが前記共有データの復号を求めると共に、前記一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、ステップと、

(c) 前記残りのユーザそれぞれが、予め付与された前記座標を送信してきた場合に、前記一のユーザが送信してきた前記座標と、前記残りのユーザが送信してきた前記座標とから、関数を算出し、算出した

関数から求められる値を復号キーとして用いて、暗号化された前記共有データを復号する、ステップと、
を有する、
ことを特徴とするデータ管理方法。

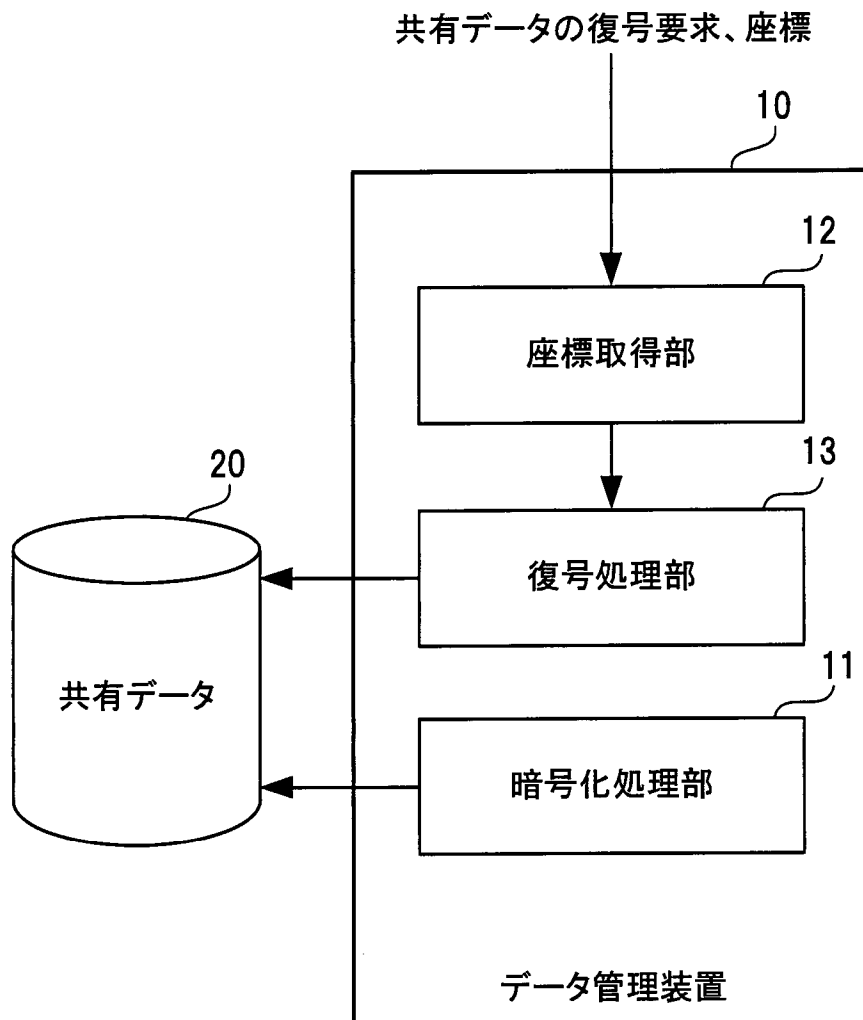
[請求項4] 前記(c)のステップにおいて、前記複数のユーザがN人である場合に、前記関数として $(N-1)$ 次関数を算出し、算出した $(N-1)$ 次関数の $(N-1)$ 個の変数に設定値を代入し、得られた残りの変数の値を、前記復号キーとして用いる、
請求項3に記載のデータ管理方法。

[請求項5] 複数のユーザで共有されるデータをコンピュータによって管理するためのプログラムを記録したコンピュータ読み取り可能な記録媒体であって、
前記コンピュータに、
(a) 前記共有データを暗号化する、ステップと、
(b) 前記複数のユーザのうちの一のユーザが前記共有データの復号を求めると共に、前記一のユーザに予め付与されている座標を送信してきた場合に、残りのユーザに対して、それぞれに予め付与されている座標の送信を求める、ステップと、
(c) 前記残りのユーザそれぞれが、予め付与された前記座標を送信してきた場合に、前記一のユーザが送信してきた前記座標と、前記残りのユーザが送信してきた前記座標とから、関数を算出し、算出した関数から求められる値を復号キーとして用いて、暗号化された前記共有データを復号する、ステップと、
を実行させる命令を含む、プログラムを記録しているコンピュータ読み取り可能な記録媒体。

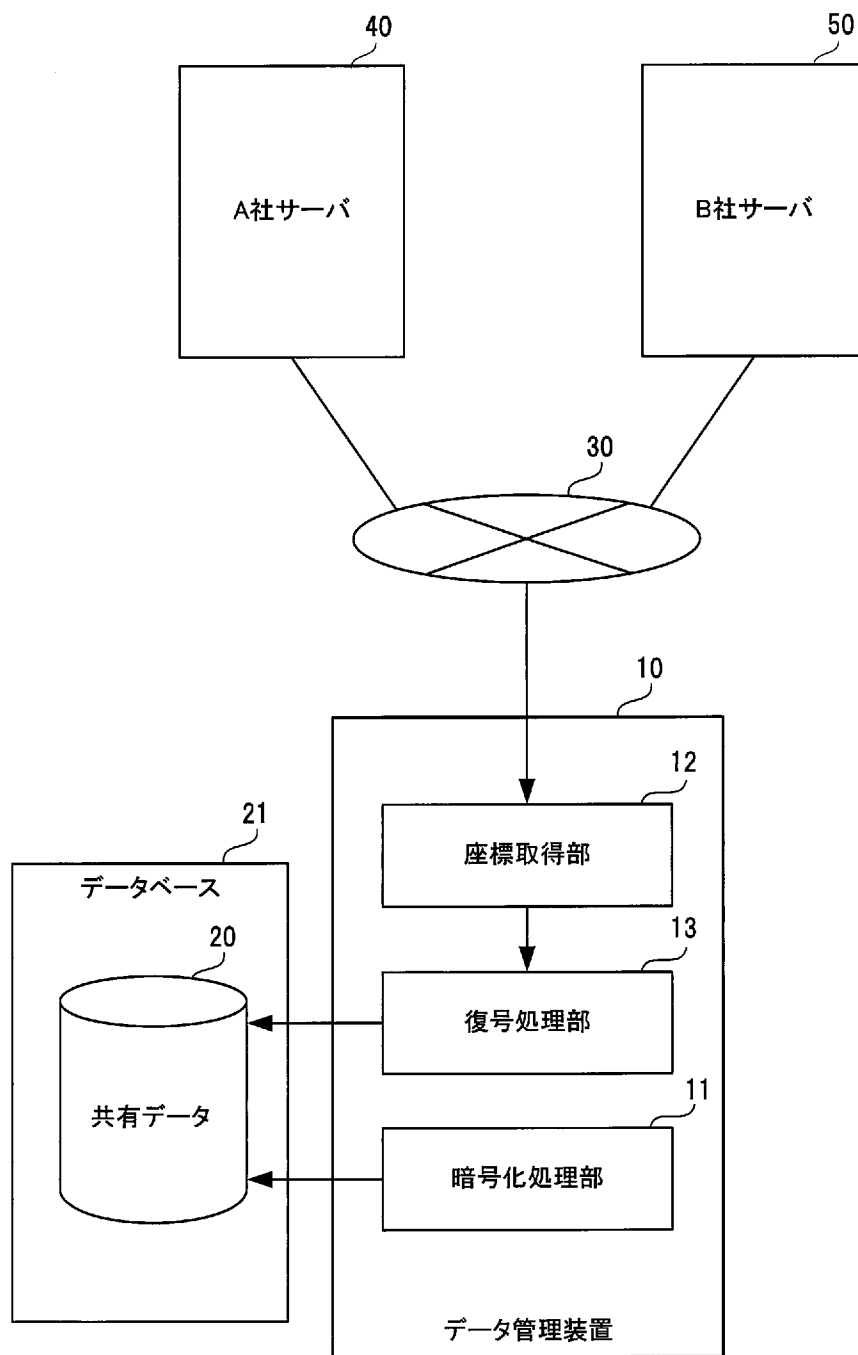
[請求項6] 前記(c)のステップにおいて、前記複数のユーザがN人である場合に、前記関数として $(N-1)$ 次関数を算出し、算出した $(N-1)$ 次関数の $(N-1)$ 個の変数に設定値を代入し、得られた残りの変

数の値を、前記復号キーとして用いる、
請求項 5 に記載のコンピュータ読み取り可能な記録媒体。

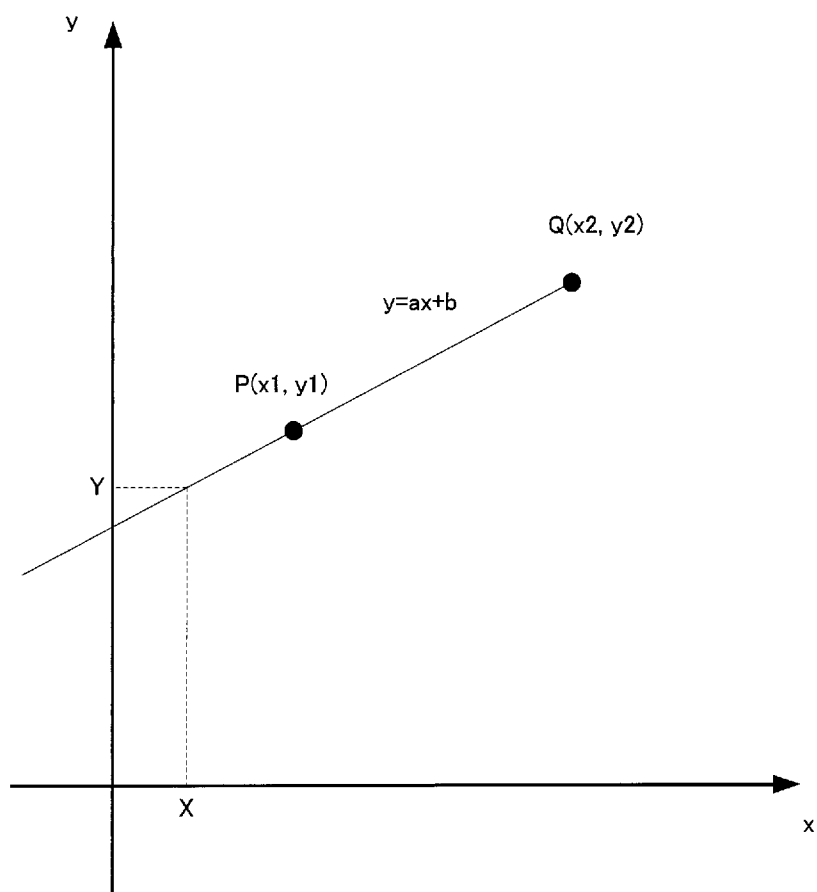
[図1]



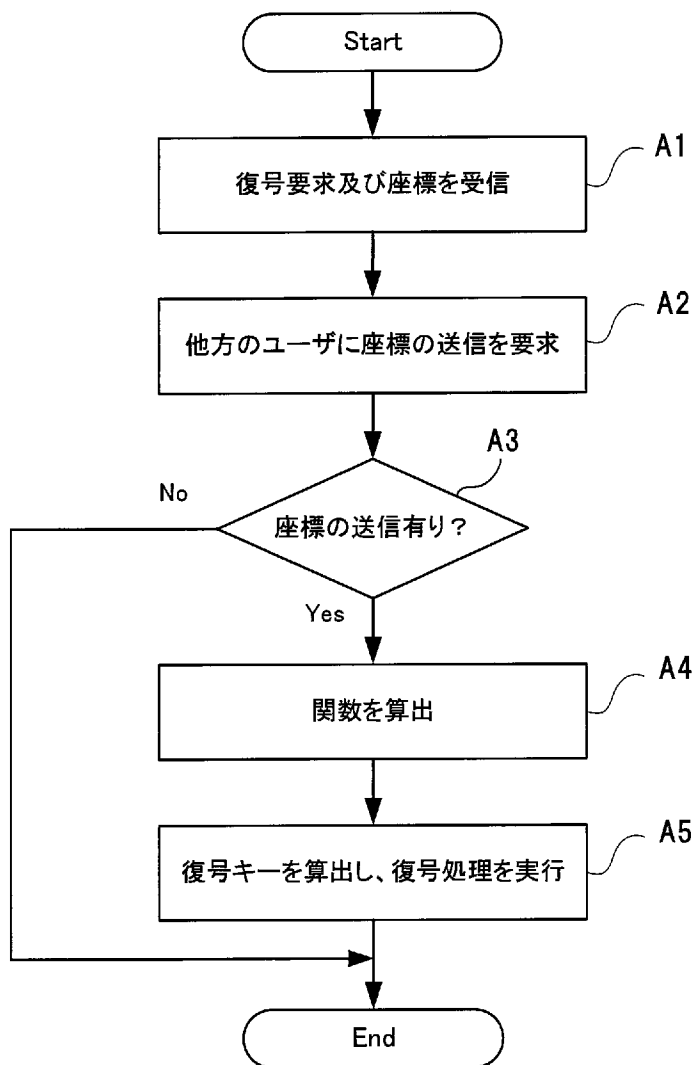
[図2]



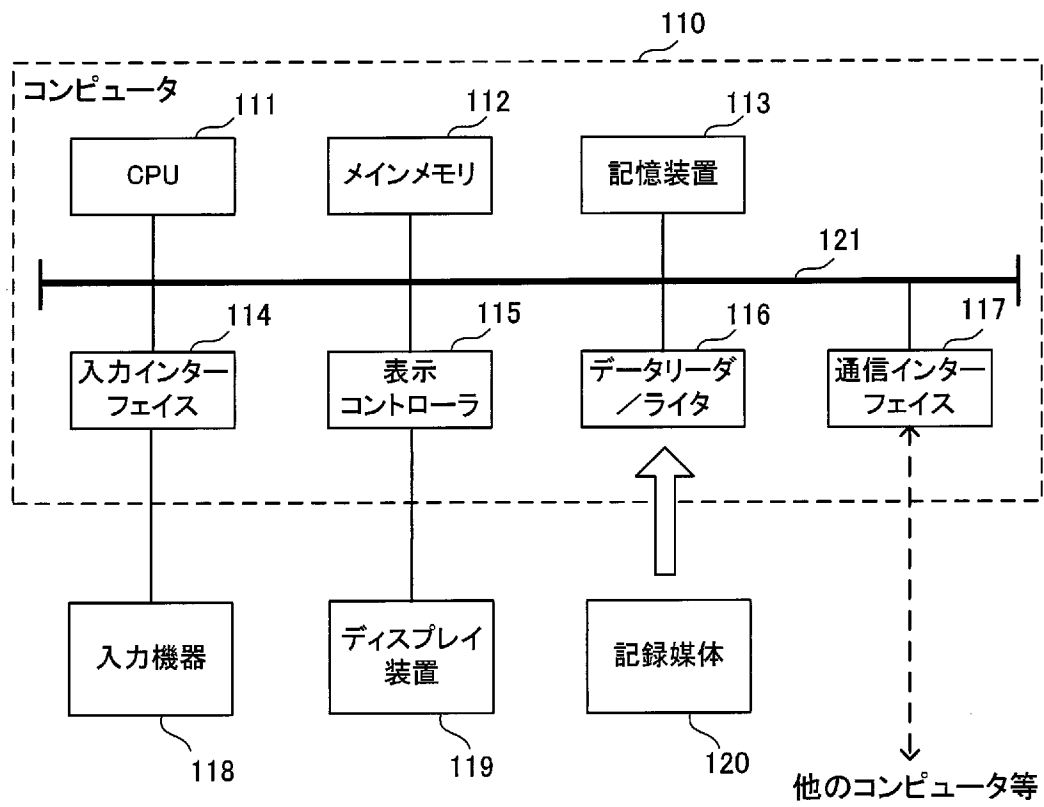
[図3]



[図4]



[図5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/059555

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)i, G06F21/60(2013.01)i, G06F21/62(2013.01)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)

H04L9/08, G06F21/60, G06F21/62

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JSTPlus/JMEDPlus/JST7580(JDreamIII), IEEE Xplore, file encryption, secret sharing

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/0175000 A1 (Germano Caronni), 09 September 2004 (09.09.2004), paragraphs [0001] to [0008]	1-6
Y	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, HANDBOOK of APPLIED CRYPTOGRAPHY, CRC Press, 1997, p.524-526 especially 12.7 Secret sharing, Shamir's threshold scheme	1-6
Y	JP 2002-111659 A (NEC Software Hokuriku, Ltd.), 12 April 2002 (12.04.2002), paragraphs [0001], [0031] to [0057]	1-6

☒ 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
16 June 2016 (16.06.16)

Date of mailing of the international search report
28 June 2016 (28.06.16)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/059555

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2008-103936 A (Toshiba Corp., Toshiba Solutions Corp.), 01 May 2008 (01.05.2008), paragraphs [0017] to [0068]	1-6
A	JP 2003-348065 A (Japan Datacom Co., Ltd.), 05 December 2003 (05.12.2003), paragraphs [0007] to [0011], [0022] to [0049]	1-6
A	JP 11-317734 A (Hitachi, Ltd.), 16 November 1999 (16.11.1999), paragraphs [0015] to [0042]	1-6

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2016/059555

US 2004/0175000 A1	2004.09.09	(Family: none)	
JP 2002-111659 A	2002.04.12	(Family: none)	
JP 2008-103936 A	2008.01.31	US 2008/0095375 A1	2008.04.24
		paragraphs [0045]	
		to [0102]	
		CN 101166089 A	2008.04.23
JP 2003-348065 A	2003.12.05	(Family: none)	
JP 11-317734 A	1999.11.16	US 6477254 B1	2002.11.05
		column 2, line 45	
		to column 7, line 41	
		EP 936776 A2	1999.08.18

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. H04L9/08(2006.01)i, G06F21/60(2013.01)i, G06F21/62(2013.01)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. H04L9/08, G06F21/60, G06F21/62

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	1971-2016年
日本国実用新案登録公報	1996-2016年
日本国登録実用新案公報	1994-2016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
file encryption, secret sharing

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	US 2004/0175000 A1 (Germano Caronni) 2004.09.09, 段落[0001]-[0008]	1-6
Y	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, HANDBOOK of APPLIED CRYPTOGRAPHY, CRC Press, 1997, p.524-526 especially 12.7 Secret sharing, Shamir's threshold scheme	1-6
Y	JP 2002-111659 A (北陸日本電気ソフトウェア株式会社) 2002.04.12, 段落[0001], [0031]-[0057]	1-6

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	「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
「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	「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
「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)	「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
「O」 口頭による開示、使用、展示等に言及する文献	「&」 同一パテントファミリー文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願	

国際調査を完了した日

16.06.2016

国際調査報告の発送日

28.06.2016

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

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)

中里 裕正

5 S

9364

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	JP 2008-103936 A (株式会社東芝, 東芝ソリューション株式会社) 2008. 05. 01, 段落[0017]-[0068]	1-6
A	JP 2003-348065 A (ジャパンデータコム株式会社) 2003. 12. 05, 段落[0007]-[0011], [0022]-[0049]	1-6
A	JP 11-317734 A (株式会社日立製作所) 1999. 11. 16, 段落[0015]-[0042]	1-6

US 2004/0175000 A1	2004. 09. 09	ファミリーなし	
JP 2002-111659 A	2002. 04. 12	ファミリーなし	
JP 2008-103936 A	2008. 01. 31	US 2008/0095375 A1 段落[0045]-[0102] CN 101166089 A	2008. 04. 24 2008. 04. 23
JP 2003-348065 A	2003. 12. 05	ファミリーなし	
JP 11-317734 A	1999. 11. 16	US 6477254 B1 2 欄 45 行-7 欄 41 行 EP 936776 A2	2002. 11. 05 1999. 08. 18