(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 11 月 17 日(17.11.2016)

WIPO | PCT

(10) 国際公開番号
WO 2016/181904 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)　*G06F 21/60* (2013.01)
G06F 17/30 (2006.01)　*G06F 21/62* (2013.01)

(21) 国際出願番号: PCT/JP2016/063662

(22) 国際出願日: 2016 年 5 月 6 日(06.05.2016)

(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 2015-099204 2015 年 5 月 14 日(14.05.2015) 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: 桐淵　直人(KIRIBUCHI, Naoto); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ　知的財産センタ内 Tokyo (JP). 瀧口　浩義(TAKIGUCHI, Hiroyoshi); 〒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, 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), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[続葉有]

(54) **Title**: DATABASE SYSTEM AND DATABASE PROCESSING METHOD

(54) 発明の名称 : データベースシステム、データベース処理方法

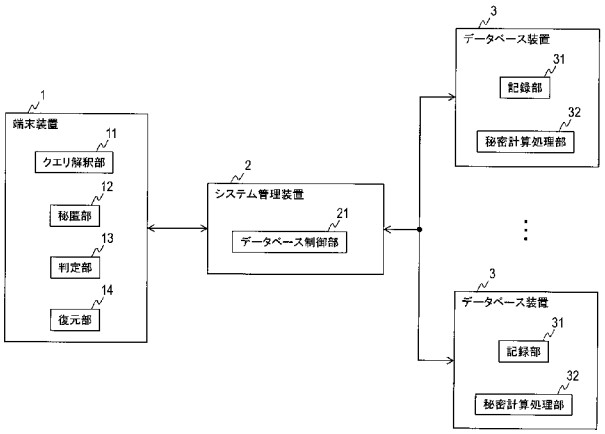

図1

1 Terminal device
2 System managing device
3 Database device
11 Query interpreting unit
12 Secrecy unit
13 Determining unit
14 Restoring unit
21 Database controlling unit
31 Recording unit
32 Secrecy calculation processing unit

(57) **Abstract**: This database system is provided with: a determining unit 13 that determines whether or not information to be registered in a database should be kept secret; a terminal device 1 that, when the determining unit 13 determines that the information should be kept secret, creates N-pieces (N is a predetermined positive integer) of fragmented information by secretly dividing the information and transmits the fragmented information to a system managing device 2; the system managing device 2 that transmits the N-pieces of the fragmented information received from the terminal device 1 to N number of database devices 3, respectively; and N number of database devices 3 that store the N-pieces of the fragmented information received from the system managing device 2, respectively.

(57) 要約:　データベースシステムは、データベースに登録しようとする情報を秘匿にするかどうかを判定する判定部１３と、判定部１３において秘匿にすると判定された場合には、Ｎを所定の正の整数として、情報を秘密分散することによりＮ個の断片情報を生成しシステム管理装置２に送信する端末装置１と、端末装置１から受信したＮ個の断片情報をそれぞれＮ個のデータベース装置３に送信するシステム管理装置２と、システム管理装置２から受信したＮ個の断片情報をそれぞれ格納するＮ個のデータベース装置３と、を備えている。

WO 2016/181904 A1

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 ： データベースシステム、データベース処理方法

技術分野

[0001] この発明は、暗号応用技術に関し、特にデータベースに格納するデータを明かすことなく情報処理を行う秘密計算の技術に関する。

背景技術

[0002] データベースに格納されるデータを秘匿する手法として、主に（１）透過的暗号化による暗号化、（２）検索可能暗号などによる暗号化、（３）完全準同型暗号による暗号化の３種類の手法が知られている。

（１）透過的暗号化は、データを暗号化してからデータベースに格納することでデータベースに格納されたデータを秘匿するものである（例えば、非特許文献１参照。）。

（２）検索可能暗号などによる暗号化は、暗号文の状態で特定の処理を行うことで、データを秘匿した状態での検索や、暗号方式に応じた操作を可能にするものである（例えば、非特許文献１参照。）。

（３）完全準同型暗号化による暗号化は、暗号文の状態で任意の処理を行うことにより、データを秘匿した状態での操作が可能にするものである（例えば、非特許文献１参照。）。

先行技術文献

非特許文献

[0003] 非特許文献1：Oracle Advanced Security, ［online］, ［平成 27 年 5 月 1 日検索］, インターネット〈URL：http://www.oracle.com/jp/products/database/options/advanced-security/overview/index.html〉

非特許文献2：D.X. Song, D. Wagner, and A. Perring, “Practical Techniques for Searches on Encrypted Data,” in IEEE Symposium on Security and Privacy, pages 44-55, 2000.

非特許文献3：C. Gentry, “Fully Homomorphic Encryption Using Ideal La

ttices," in STOC '09, pages 169-178, 2009.

発明の概要

発明が解決しようとする課題

[0004] 上記の（１）から（３）の手法は、いずれも暗号鍵を用いた方式であるため、暗号鍵が漏洩するリスクが存在する。

[0005] この発明の目的は、暗号鍵が漏洩するリスクがないデータベースシステム、データベース処理方法を提供することである。

課題を解決するための手段

[0006] この発明の一態様によるデータベースシステムは、データベースに登録しようとする情報を秘匿にするかどうかを判定する判定部と、判定部において秘匿にすると判定された場合には、Ｎを所定の正の整数として、情報を秘密分散することによりＮ個の断片情報を生成しシステム管理装置に送信する端末装置と、端末装置から受信したＮ個の断片情報をそれぞれＮ個のデータベース装置に送信するシステム管理装置と、システム管理装置から受信したＮ個の断片情報をそれぞれ格納するＮ個のデータベース装置と、を備えている。

発明の効果

[0007] 暗号鍵を用いないため、暗号鍵が漏洩するリスクがなくなる。

図面の簡単な説明

[0008] [図1]データベースシステムの例を説明するためのブロック図。

[図2]データ登録の処理の例を説明するための流れ図。

[図3]データ検索の処理の例を説明するための流れ図。

発明を実施するための形態

[0009] データベースシステムは、図１に示すように、端末装置１と、システム管理装置２と、Ｎ個のデータベース装置３を例えば備えている。

[0010] 端末装置１は、携帯電話、スマートフォン、ＰＣ等の情報端末である。端末装置１は、クエリ解釈部１１、秘匿部１２、判定部１３及び復元部１４を

例えば備えている。図１の例では、端末装置１は１個だけ描かれているが、異なる複数の端末装置１がシステム管理装置２に互いに通信可能な状態で接続されていてもよい。

[0011] システム管理装置２は、後述するようにデータベースシステムを管理するためのサーバである。システム管理装置２は、データベース制御部２１を例えば備えている。

[0012] データベース装置３は、後述するように秘密分散された断片が格納され、必要に応じて秘密計算により情報を復元する装置である。データベース装置３は、記録部３１及び秘密計算処理部３２を例えば備えている。

[0013] 秘密分散とは、入力されたデータを複数（N個）の断片に変換し、隔離することによって秘匿する技術である。Nは、所定の正の整数である。K個（KはN以下の正の整数。）の断片を集めることによってのみ元のデータを知ることができ、暗号鍵を用いないため危殆化による情報漏洩リスクがなくなる（例えば、参考文献１参照。）。

〔参考文献１〕A. Shamir, “How to Share a Secret,” Communications of the ACM 22, pages 612-613, 1979.

[0014] 秘密計算とは、秘密分散によって秘匿化されたC個（CはK以上N以下の正の整数。）の断片を用いて、元のデータを明かさずに処理を行う技術である。理論上は任意の関数の計算が実行できることが知られている。下記の参考文献２では基本演算となる乗算の方法が示されている。

〔参考文献２〕R. Gennaro, M.O. Rabin, and T. Rabin, “Simplified VSS and Fast-track Multiparty Computations with Applications to Threshold Cryptography,” 17th annual ACM symposium on Principles of distributed computing, ACM, 1998.

[0015] データベースの操作は、端末装置１から入力され、システム管理装置２を介して各データベース装置３で実行される。データベースのデータ処理は、一般のデータベースと同様に主に６個の処理で構成される。６個の処理は、１．テーブル定義、２．データ登録、３．データ検索、４．データ更新、５．

データ削除、６．テーブル削除である。以降、各処理について説明する。

[0016] ［テーブル定義］

テーブル定義は、データを格納する表を定義する操作である。

[0017] 端末装置１に入力されたクエリ（例えばSQL文）が、クエリ解釈部１１によって「テーブル定義」処理と判定された場合には、テーブル名、テーブルの各列の属性などの作成するテーブルに関する情報をシステム管理装置２に送信する。

[0018] システム管理装置２は、データベース制御部２１によりＮ個のデータベース装置に作成するテーブルに関する情報を送信する。

[0019] データベース装置３は、作成するテーブルに関する情報を記録部３１に記録し、完了通知をシステム管理装置２に返却する。

[0020] システム管理装置２は、Ｎ個のデータベース装置から正常に完了通知を受信したことを確認し、端末装置１に「テーブル定義」処理が正常に完了したことを知らせる。

[0021] 端末装置１は、クエリ解釈部１１により、入力されたクエリに対応した応答をユーザに通知する。

[0022] ［データ登録］

データ登録は、データを格納する操作である。

[0023] 端末装置１に入力されたクエリ（例えばSQL文）が、クエリ解釈部１１によって「データ登録」処理と判定された場合には、データを登録するテーブル名をシステム管理装置２に送信する。

[0024] システム管理装置１は、少なくとも1個のデータベース装置３から対象のテーブルに関する情報であるテーブル情報を取得し、その情報を端末装置１に返却する。

[0025] 端末装置１の判定部１３は、返却された情報から秘匿する列を判定する。すなわち、判定部１３は、データベースに登録しようとする情報を秘匿にするかどうかを判定する（ステップＡ１，図２）。

[0026] 秘匿にすると判定された情報、言い換えれば秘匿する列に格納する情報は

、端末装置１の秘匿部１２において秘密分散される。端末装置１は、秘密分散により断片に変換された情報と、秘匿にすると判定されなかった情報である、秘匿しない列に格納する平文の情報とを併せてシステム管理装置２に送信する。

[0027] このようにして、判定部１３において秘匿にすると判定された場合には、端末装置１の秘匿部１２は、その秘匿にする情報を秘密分散することによりＮ個の断片情報を生成しシステム管理装置に送信する（ステップＡ２，図２）。Ｎ個の断片情報は、それぞれＮ個のデータベース装置３に対応付けされている。

[0028] システム管理装置２は、端末装置１から受信したＮ個の断片情報をそれぞれＮ個のデータベース装置３に送信する（ステップＡ３，図２）。具体的には、システム管理装置２は、データベース制御部２１によりＮ個のデータベース装置３に「データ登録」処理に必要なテーブル名、登録する平文/断片データなどの情報を送信する。

[0029] データベース装置３は、システム管理装置２から受信したＮ個の断片情報をそれぞれ格納する（ステップＡ４，図２）。すなわち、各データベース装置３は、登録する断片情報を記録部３１に記録し、完了通知をシステム管理装置に返却する。

[0030] システム管理装置２は、Ｎ個のデータベース装置３から正常に完了通知を受信したことを確認し、端末装置１に「データ登録」処理が正常に完了したことを知らせる。

[0031] 端末装置１は、クエリ解釈部１１により、入力されたクエリに対応した応答をユーザに通知する。

[0032] ［データ検索］

データ検索は、格納されたデータから対象のデータを参照する操作である。

[0033] 端末装置１に入力されたクエリ（例えばSQL文）が、クエリ解釈部１１によって「データ検索」処理と判定された場合には、データを検索するテーブル

名をシステム管理装置２に送信する。

[0034] システム管理装置２は、少なくとも１個のデータベース装置３からデータ検索の対象となるテーブルに関する情報を取得し、その情報を端末装置１に返却する。

[0035] 端末装置１の判定部１３は、データベースを参照するための検索条件の全部又は一部を秘匿にするかどうかを判定する（ステップＢ１）。すなわち、判定部１３は、返却された情報から実行する「データ検索」処理に秘密計算処理が含まれるかどうかを判定する。例えばある年齢以上の人のidを検索する場合には、その年齢が秘匿にされる。

[0036] また、判定部１３は、データベースから参照しようとする情報が秘匿にされているかどうかを判定する（ステップＢ２）。例えば、判定部１３は、検索対象の列に断片が含まれている場合には、データベースから参照しようとする情報が秘匿にされていると判定する。

[0037] 判定部１３において検索条件の全部又は一部を秘匿にすると判定された場合には、端末装置１の秘匿部１２は、検索条件の全部又は一部を秘密分散することにより断片検索情報を生成しシステム管理装置２に送信する（ステップＢ３）。その際、判定部１３は、データベースを参照するための検索条件の全部又は一部を秘匿にするかどうかの判定結果と、データベースから参照しようとする情報が秘匿にされているかどうかの判定結果とについての情報をシステム管理装置２に送信してもよい。断片検索情報は、ＣをＫ以上Ｎ以下の正の整数として、Ｃ個生成される。各断片検索情報は、データベース装置３の何れかに対応付けされている。

[0038] （１）データベースを参照するための検索条件の全部又は一部を秘匿にすると判定されている場合、すなわち検索条件の全部又は一部を秘密分散することにより断片検索情報が生成されている場合には、システム管理装置２は、Ｃ個の断片検索情報のそれぞれを、対応するデータベース装置３に送信する（ステップＢ４）。

[0039] この場合、Ｃ個の断片検索情報をそれぞれ受信したＣ個のデータベース装

置３は、上記Ｃ個の断片検索情報に対応するＣ個の断片情報を秘密計算により見つける（ステップＢ５）。

[0040] システム管理装置２は、見つかったＣ個の断片情報の中のＫ個の断片情報を端末装置１に送信する（ステップＢ６）。例えば、システム管理装置２は、Ｃ個の断片情報をそれぞれＣ個のデータベース装置３から受信して、受信したＣ個の断片情報の中のＫ個の断片情報を端末装置１に送信する。また、システム管理装置２は、見つかったＣ個の断片情報がそれぞれ格納されているＣ個のデータベース装置３の中のＫ個のデータベース装置を選択し、選択されたＫ個のデータベース装置３からそれぞれＫ個の断片情報を受信し、受信したＫ個の断片情報を端末装置１に送信してもよい。

[0041] 端末装置１の復元部１４は、受信したＫ個の断片情報に基づいて元の情報を復元する（ステップＢ７）。その後、端末装置１のクエリ解釈部１１により、入力されたクエリに対応した応答がユーザに通知される。

[0042] （２）データベースを参照するための検索条件の全部又は一部を秘匿にすると判定されていない場合、かつ、データベースから参照しようとする情報が秘匿にされていると判定されている場合には、システム管理装置２は、Ｎ個のデータベース装置３の中のＫ個のデータベース装置３にそれぞれ格納されたＫ個の断片情報を読み込み端末装置１に送信する（ステップＢ６）。例えば、システム管理装置２は、Ｎ個の断片情報をそれぞれＮ個のデータベース装置３から受信して、受信したＮ個の断片情報の中のＫ個の断片情報を端末装置１に送信する。また、システム管理装置２は、Ｎ個のデータベース装置３の中のＫ個のデータベース装置３を選択し、選択されたＫ個のデータベース装置３からそれぞれＫ個の断片情報を受信し、受信したＫ個の断片情報を端末装置１に送信してもよい。

[0043] 端末装置１の復元部１４は、受信したＫ個の断片情報に基づいて元の情報を復元する（ステップＢ７）。その後、端末装置１のクエリ解釈部１１により、入力されたクエリに対応した応答がユーザに通知される。

[0044] この（２）の場合には、図３のステップＢ３からステップＢ５の処理は行

われない。

[0045] （３）データベースを参照するための検索条件の全部又は一部を秘匿にすると判定されていない場合、かつ、データベースから参照しようとする情報が秘匿にされていると判定されていない場合には、システム管理装置２は、少なくとも１個のデータベース装置３に検索命令を送信する。

[0046] 検索命令を受けたデータベース装置３は、記録部３１から検索対象情報を取得し、検索結果をシステム管理装置２に返却する。

[0047] システム管理装置２は、データベース装置３からの結果を端末装置１に返却する。

[0048] その後、端末装置１のクエリ解釈部１１により、入力されたクエリに対応した応答がユーザに通知される。

[0049] この（３）の場合には、図３のステップＢ３からステップＢ７の処理は行われない。

[0050] ［データ更新］

データ更新は、格納された対象のデータを更新する操作である。

[0051] 端末装置１に入力されたクエリ（例えばSQL文）が、クエリ解釈部１１によって「データ更新」処理と判定された場合には、データを更新するテーブル名をシステム管理装置２に送信する。

[0052] システム管理装置２は、少なくとも1個のデータベース装置３から対象のテーブルに関する情報を取得し、その情報を端末装置１に返却する。

[0053] 端末装置１は、返却された情報から秘匿する列および実行する「データ更新」処理に秘密計算処理が含まれるかを判定する。秘匿する列に格納する情報は、端末装置１の秘匿部１２により秘密分散される。秘密分散により断片に変換された情報と、秘匿しない列に格納する平文の情報および秘密計算処理の有無はシステム管理装置２に送信される。例えば住所、電話番号等の秘匿にすべきプライベートな情報を秘匿にしたまま更新する場合に、「データ更新」処理に秘密計算が行われる。

[0054] システム管理装置２は、データベース制御部２１によりＮ個のデータベー

ス装置３に「データ更新」処理に必要なテーブル名、更新する平文/秘匿データなどの情報を送信する。

[0055] データベース装置３は、秘密計算処理が含まれる場合のみ秘密計算処理部３２による秘密計算処理を実施し、更新する情報を記録部３１に記録し、完了通知をシステム管理装置２に返却する。

[0056] システム管理装置２は、Ｎ個のデータベース装置から正常に完了通知を受信したことを確認し、端末装置１に「テーブル更新」処理が正常に完了したことを知らせる。

[0057] 端末装置１は、クエリ解釈部１１により、入力されたクエリに対応した応答をユーザに通知する。

[0058] ［データ削除］

データ削除は、格納された対象のデータを削除する操作である。

[0059] 端末装置１に入力されたクエリ（例えばSQL文）が、クエリ解釈部１１によって「データ削除」処理と判定された場合には、データを削除するテーブル名をシステム管理装置２に送信する。

[0060] システム管理装置２は、少なくとも1個のデータベース装置３から対象のテーブルに関する情報を取得し、その情報を端末装置１に返却する。

[0061] 端末装置１の判定部１３は、返却された情報から「データ削除」処理に秘密計算処理が含まれるか判定し、システム管理装置２のデータベース制御部２１によりＮ個のデータベース装置３に「データ削除」処理に必要なテーブル名、削除条件などの情報を送信する。例えば秘匿にされたid等の情報を秘匿にされた状態のまま削除する場合に、「データ削除」処理に秘密計算処理が行われる。

[0062] データベース装置３は、秘密計算処理が含まれる場合のみ秘密計算処理部３２による秘密計算処理を実施し、削除する情報を記録部３１から削除し、完了通知をシステム管理装置２に返却する。

[0063] システム管理装置２は、Ｎ個のデータベース装置から正常に完了通知を受信したことを確認し端末装置１に「データ削除」処理が正常に完了したこと

を知らせる。

[0064] 端末装置１は、クエリ解釈部１１により、入力されたクエリに対応した応答をユーザに通知する。

[0065] ［テーブル削除］

テーブル削除は、定義された対象の表を削除する操作である。

[0066] 端末装置１に入力されたクエリ（例えばSQL文）は、クエリ解釈部１１によって「テーブル削除」処理と判定され、削除するテーブル名をシステム管理装置２に送信する。

[0067] システム管理装置２は、データベース制御部２１によりＮ個のデータベース装置３に「テーブル削除」処理に必要なテーブル名などの情報を送信する。

[0068] データベース装置３は、削除する情報を記録部から削除し、完了通知をシステム管理装置２に返却する。

[0069] システム管理装置２は、Ｎ個のデータベース装置３から正常に完了通知を受信したことを確認し、端末装置１に「テーブル削除」処理が正常に完了したことを知らせる。

[0070] 端末装置１は、クエリ解釈部１１により、入力されたクエリに対応した応答をユーザに通知する。

[0071] ［変形例等］

端末装置１のクエリ解釈部１１は、一般的なデータベース操作命令（例えば、SQL文）に対応していてもよい。これにより、データベースを利用する外部プログラムを改造せずにセキュアなデータベースを利用することができる。

[0072] 例えば、外部プログラムが一般的なWeb三層モデルのシステム上に存在する場合、データベースに対する操作命令はアプリケーション・サーバからデータベース・サーバに送信されるため、アプリケーション・サーバからのデータベース操作命令を端末装置１に送信することで、アプリケーション・サーバ上の外部プログラムを改造することなくセキュアなデータベースを利用で

きる。

[0073] また、データベース装置３として、既存のデータベース装置を用いてもよい。これにより、コストの削減を行うことができる。

[0074] データベースの機能は、秘密計算を含む操作と秘密計算を含まない操作に分けられる。例えば、秘匿した年齢に対する検索には秘密計算が含まれるが、条件の指定されていない検索には秘密計算が含まれない。秘密計算が含まれない操作は、一般のデータベースの操作と同等であるため、既存のデータベースの該当機能をそのまま利用することで処理可能である。秘密計算が含まれる場合にのみ、秘密計算処理部３２が処理を行えばよい。例えば、既存のデータベースに備えられた外部機能呼出部により呼び出されれることにより、秘密計算処理部３２が処理を行う。

[0075] これにより、秘密計算が含まれない操作についてのプログラムが、既存データベースで代用されるため、不要となり、発明全体のプログラムの量を削減することができる。

[0076] 上記の例では、判定部１３は、端末装置１に備えられているが、判定部１３は端末装置１の外部に備えられていてもよい。例えば、判定部１３は、システム管理装置２に備えられていてもよい。

[0077] [プログラム及び記録媒体]

データベースシステム、データベース処理方法において説明した処理は、記載の順にしたがって時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

[0078] また、データベースシステムを構成する各装置又は各部における各処理をコンピュータによって実現する場合、その各装置又は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、その各処理がコンピュータ上で実現される。

[0079] 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。

[0080] また、各装置又は各部は、上記の通り、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、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

[0081] 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] データベースに登録しようとする情報を秘匿にするかどうかを判定する判定部と、

上記判定部において秘匿にすると判定された場合には、Ｎを所定の正の整数として、上記情報を秘密分散することによりＮ個の断片情報を生成しシステム管理装置に送信する端末装置と、

上記端末装置から受信したＮ個の断片情報をそれぞれＮ個のデータベース装置に送信する上記システム管理装置と、

上記システム管理装置から受信したＮ個の断片情報をそれぞれ格納するＮ個のデータベース装置と、

を含むデータベースシステム。

[請求項2] 請求項１のデータベースシステムにおいて、

上記判定部は、データベースから参照しようとする情報が秘匿にされているかどうかを判定し、

ＫをＮ以下の所定の正の整数として、上記判定部において秘匿にされていると判定された場合には、上記システム管理装置は、上記Ｎ個のデータベース装置の中のＫ個のデータベース装置にそれぞれ格納されたＫ個の断片情報を読み込み上記端末装置に送信し、

上記端末装置は、上記システム管理装置から受信したＫ個の断片情報に基づいて元の情報を復元する、

データベースシステム。

[請求項3] 請求項１又は２のデータベースシステムにおいて、

上記判定部は、データベースを参照するための検索条件の全部又は一部を秘匿にするかどうかを判定し、

ＣをＫ以上Ｎ以下の正の整数として、上記判定部において上記検索条件の全部又は一部を秘匿にすると判定された場合には、上記端末装置は、上記検索条件の全部又は一部を秘密分散することによりＣ個の断片検索情報を生成し上記システム管理装置に送信し、

上記システム管理装置は、上記端末装置から受信したＣ個の断片検索情報をそれぞれＣ個のデータベース装置に送信し、

上記Ｃ個のデータベース装置が、上記Ｃ個の断片検索情報に対応するＣ個の断片情報を秘密計算により見つけ、

上記システム管理装置は、上記Ｃ個の断片情報の中のＫ個の断片情報を上記端末装置に送信し、

上記端末装置は、受信したＫ個の断片情報に基づいて元の情報を復元する、

データベースシステム。

[請求項4] 判定部が、データベースに登録しようとする情報を秘匿にするかどうかを判定する判定ステップと、

端末装置が、上記判定ステップにおいて秘匿にすると判定された場合には、Ｎを所定の正の整数として、上記情報を秘密分散することによりＮ個の断片情報を生成しシステム管理装置に送信するステップと、

システム管理装置が、上記端末装置から受信したＮ個の断片情報をそれぞれＮ個のデータベース装置に送信するステップと、

Ｎ個のデータベース装置が、上記システム管理装置から受信したＮ個の断片情報をそれぞれ格納するステップと、

を含むデータベース処理方法。

[図1]

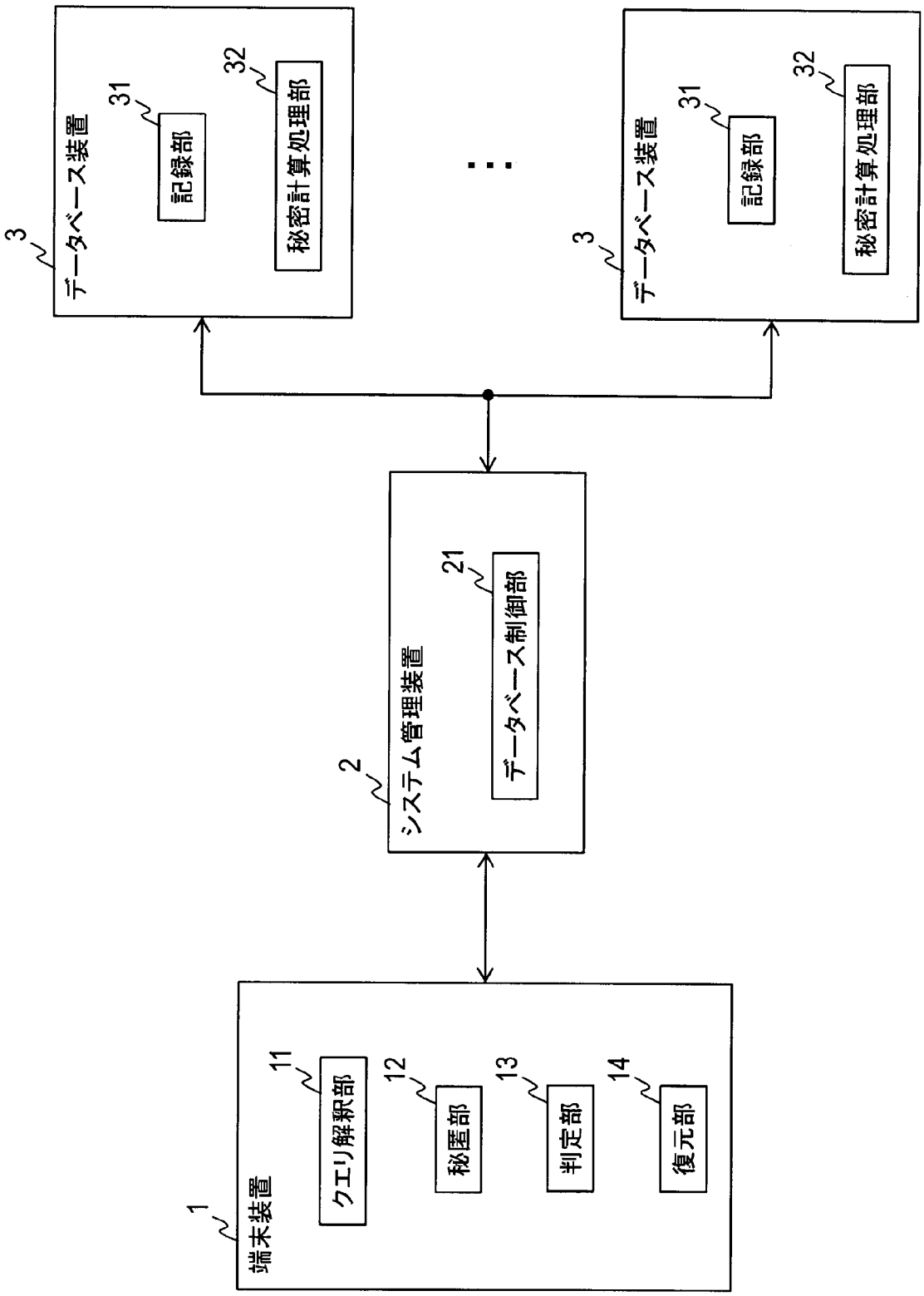
3
データベース装置
31
記録部
32
秘密計算処理部
3
データベース装置
31
記録部
32
秘密計算処理部
2
システム管理装置
21
データベース制御部
1
端末装置
11
クエリ解釈部
12
秘匿部
13
判定部
14
復元部

図1

[図2]

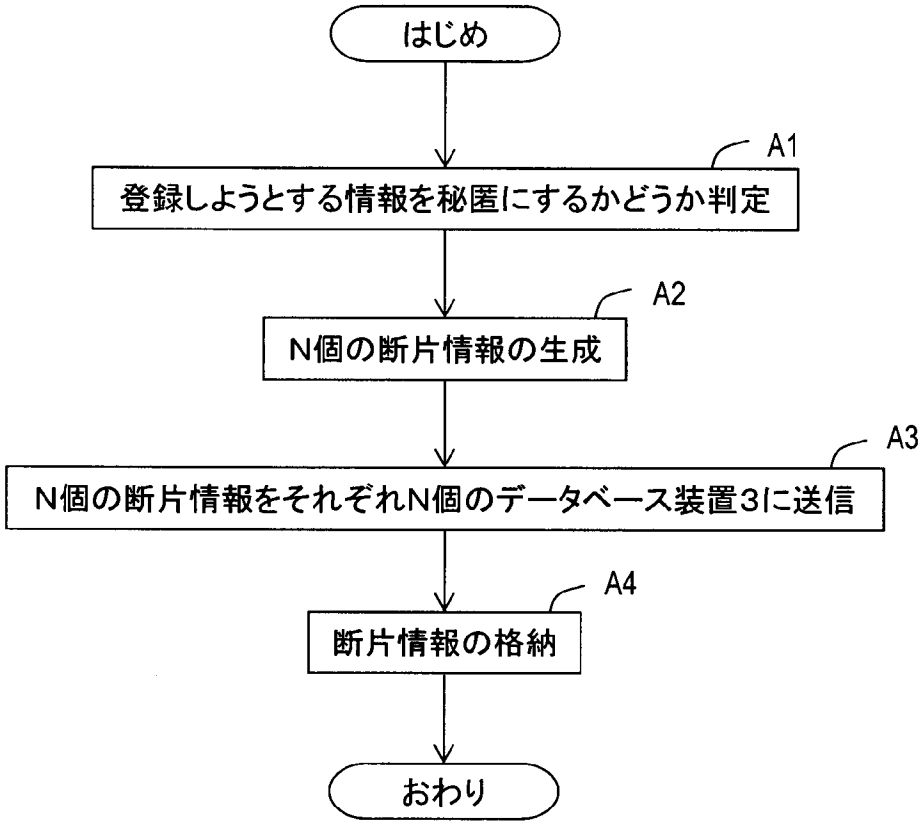
はじめ
A1
登録しようとする情報を秘匿にするかどうか判定
A2
N個の断片情報の生成
A3
N個の断片情報をそれぞれN個のデータベース装置3に送信
A4
断片情報の格納
おわり

図2

[図3]

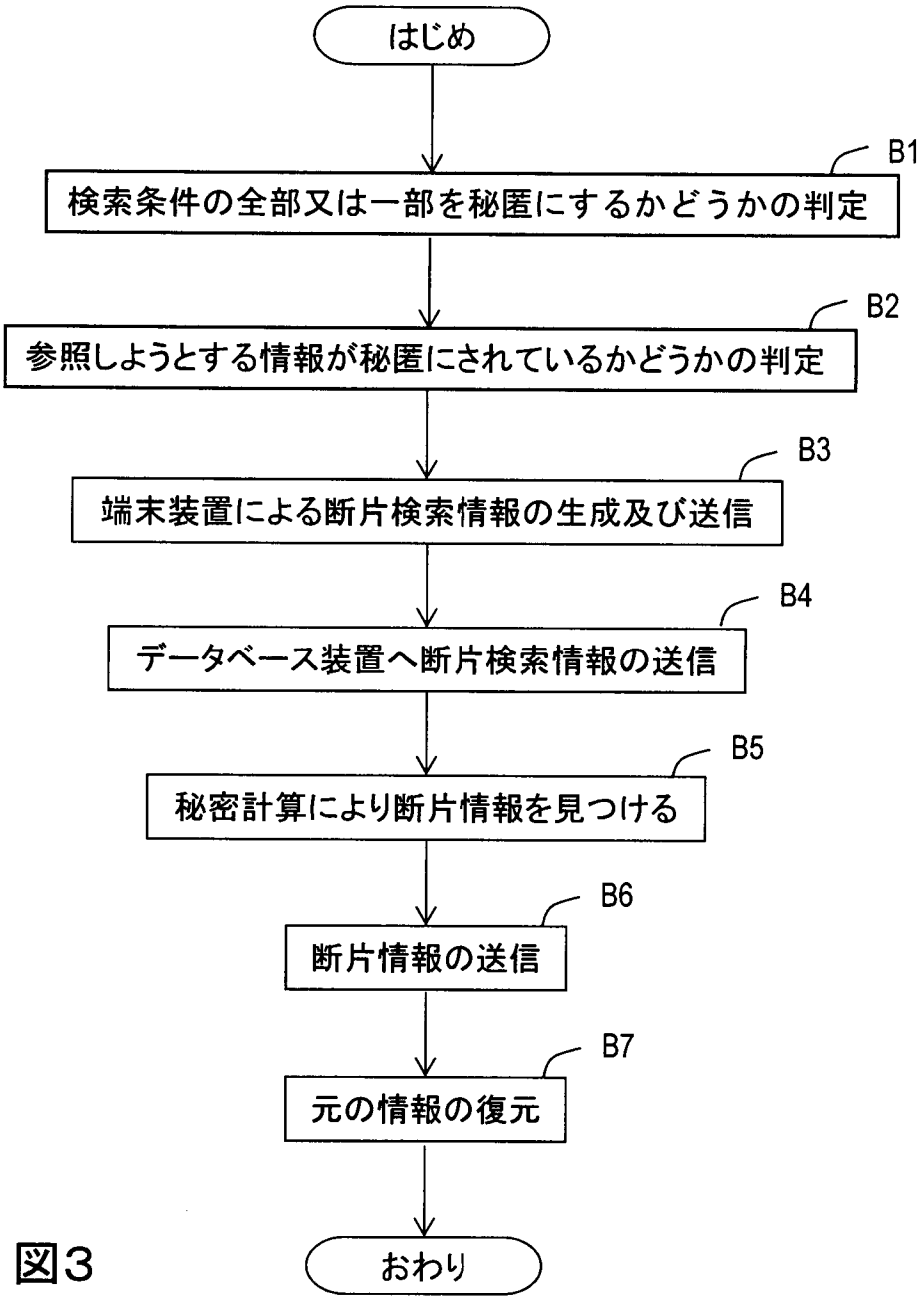
はじめ
B1
検索条件の全部又は一部を秘匿にするかどうかの判定
B2
参照しようとする情報が秘匿にされているかどうかの判定
B3
端末装置による断片検索情報の生成及び送信
B4
データベース装置へ断片検索情報の送信
B5
秘密計算により断片情報を見つける
B6
断片情報の送信
B7
元の情報の復元
おわり

図3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2016/063662

A. CLASSIFICATION OF SUBJECT MATTER
G09C1/00(2006.01)i, *G06F17/30*(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)
G09C1/00, G06F17/30, 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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2009-180912 A (Toshiba Solutions Corp.), 13 August 2009 (13.08.2009), paragraphs [0011] to [0050], [0053] to [0054]; fig. 1 to 11 (Family: none)	1-4
Y	JP 2009-187339 A (NEC Corp.), 20 August 2009 (20.08.2009), paragraphs [0032] to [0040], [0053] to [0060], [0090] to [0095], [0101]; fig. 3, 6, 14 to 15 (Family: none)	1-4
Y	Shota MINAKAMI et al., "Design and Implementation of Secret Sharing Distributed Database System", IEICE Technical Report, 22 January 2009 (22.01.2009), vol.108, no.415, pages 51 to 56	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	Date of mailing of the international search report
04 July 2016 (04.07.16)	12 July 2016 (12.07.16)

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/JP2016/063662

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Koji CHIDA et al., "Kokimitsu Data mo Anzen ni Niji Riyo Kano na 'Himitsu Keisan Gijutsu'", NTT Gijutsu Journal, 01 March 2014 (01.03. 2014), vol.26, no.3, pages 67 to 70	1-4
T	Naoto KIRIBUCHI et al., "Design of a Database System Processable under Keeping Data Confidentiality", Computer Security Symposium 2015 (CSS 2015), 14 October 2015 (14.10.2015), 2C2-4, pages 419 to 426	1-4

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１６／０６３６６２

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, G06F17/30(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.　G09C1/00, G06F17/30, 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）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2009-180912 A（東芝ソリューション株式会社）2009.08.13, 段落［００１１］－［００５０］、［００５３］－［００５４］、［図１］－［図１１］（ファミリーなし）	１－４
Y	JP 2009-187339 A（日本電気株式会社）2009.08.20, 段落［００３２］－［００４０］、［００５３］－［００６０］、［００９０］－［００９５］、［０１０１］、［図３］、［図６］、［図１４］－［図１５］（ファミリーなし）	１－４

☑　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
０４．０７．２０１６	１２．０７．２０１６

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
Ｙ	水上　翔太、他，秘密分散共有法を用いた分散データベースシステムの設計及び実装，電子情報通信学会技術研究報告，2009.01.22，Ｖｏｌ．１０８、Ｎｏ．４１５，ｐ．５１－５６	３
Ａ	千田　浩司、他，高機密データも安全に二次利用可能な「秘密計算技術」，ＮＴＴ技術ジャーナル，2014.03.01，Vol. 26，No. 3，pp. 67-70	１－４
Ｔ	桐淵　直人、他，秘匿した状態で処理可能なデータベースの設計，コンピュータセキュリティシンポジウム　２０１５　（ＣＳＳ　２０１５），2015.10.14，２Ｃ２－４，ｐ．４１９－４２６	１－４