(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
2012 年 6 月 14 日(14.06.2012)

WIPO | PCT

(10) 国際公開番号
WO 2012/077541 A1

(51) 国際特許分類:
G06F 17/30 (2006.01)

(21) 国際出願番号: PCT/JP2011/077588

(22) 国際出願日: 2011 年 11 月 29 日(29.11.2011)

(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 2010-273556 2010 年 12 月 8 日(08.12.2010) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社日立製作所 **(HITACHI, LTD.)** [JP/JP]; 〒1008280 東京都千代田区丸の内一丁目６番６号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 吉野 雅之 **(YOSHINO Masayuki)** [JP/JP]; 〒2440817 神奈川県横浜市戸塚区吉田町２９２番地 株式会社日立製作所 横浜研究所内 Kanagawa (JP). 佐藤 尚宜 **(SATO Hisayoshi)** [JP/JP]; 〒2440817 神奈川県横浜市戸塚区吉田町２９２番地 株式会社日立製作所 横浜研究所内 Kanagawa (JP). 長沼 健 **(NAGANUMA Ken)** [JP/JP]; 〒2440817 神奈川県横浜市戸塚区吉田町２９２番地 株式会社日立製作所 横浜研究所内 Kanagawa (JP).

(74) 代理人: ポレール特許業務法人 **(POLAIRE I.P.C.)**; 〒1040032 東京都中央区八丁堀二丁目７番１号 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, 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, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

添付公開書類:

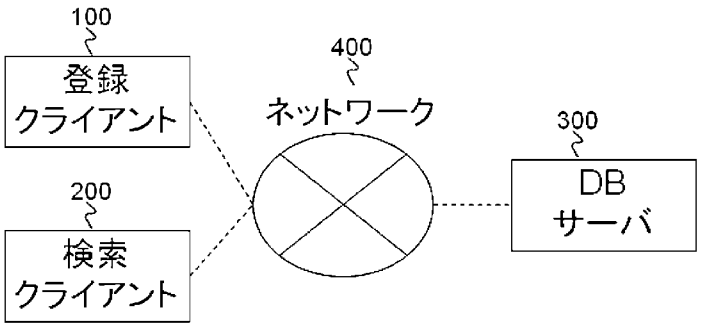
— 国際調査報告（条約第 21 条(3)）

(54) Title: SEARCHABLE ENCRYPTION PROCESSING SYSTEM

(54) 発明の名称 : 検索可能暗号処理システム

[図1]

図１



100 Registration client
200 Search client
300 Data base server
400 Network

(57) Abstract: In searchable encryption methods having practical performance, each time that data which has been deposited to a server is searched, leakage of the frequency of occurrences of search results or loss of safety of deposited data corresponding to the search results has occurred, resulting in a dangerous situation. In the searchable encryption processing system of the present invention, a data base server retaining data, a registration client which deposits the data into the data base server, and a search client which causes the data base server to search the data collaborate across a network, wherein the registration client, using a probabilistic encryption method which uses a mask using a homomorphic function and a hash value, deposits the encrypted data into the server, whereupon the search client, using probabilistic encryption which uses the mask which uses the homomorphic function for encryption of the search query, outputs the search query and non-corresponding data as search results without causing the data base server to unmask the mask and without allowing the frequency of occurrences of the data corresponding to the search to leak to the data base server.

(57) 要約:

[続葉有]

WO 2012/077541 A1

現実的な性能を有する、検索可能暗号方式ではサーバに預託したデータを検索するたびに、検索結果の出現頻度の漏洩や、検索結果に該当する預託データの安全性の低下を起しており、危険な状況にある。検索可能暗号処理ステムは、データを預かるＤＢサーバと、ＤＢサーバにデータを預託する登録クライアントと、ＤＢサーバにデータを検索させる検索クライアントがネットワーク経由で連携し、登録クライアントは、ハッシュ値と準同型関数を用いたマスクによる確率的暗号化方式を用いて、暗号化したデータをサーバに預託し、検索クライアントは、検索クエリの暗号化に準同型関数を用いたマスクによる確率的暗号化を用い、ＤＢサーバにマスクを解除させずに、かつ、ＤＢサーバに検索に該当するデータの出現頻度が漏洩しないよう、検索クエリと該当しないデータを検索結果として出力させる。

明　細　書

発明の名称 ： 検索可能暗号処理システム

技術分野

[0001] 本発明は、サーバ／クライアントモデルにおいて、サーバが、クライアントの要求に従って、暗号化データを復号せずに、預託された暗号化データを検索する、検索処理システムに関する。

背景技術

[0002] 情報システムの開発・運用管理費の効率化を目的に、近年、情報システムを自組織が維持するのではなく、他組織が提供する情報システムを利用する、クラウドと呼ばれる運用管理形態が脚光を浴びている。一方、クラウドにおいては、情報システムを管理する組織が、情報システムを利用する組織とは異なるため、情報漏えい等を防止する策や、事故発生後の原因究明、再発防止策等が自組織だけでは立てにくい。そのため、事前に、データの不正流出の予防策として、暗号技術を活用し、データの機密性を確保する必要がある。

[0003] サーバ／クライアントモデルにおいて、クライアントが、サーバにデータを預託しながら、サーバに対し、預託したデータの情報漏洩を防ぐ技術として、暗号技術を利用した方式が知られている。例えば、非特許文献１や非特許文献２には、クライアントの要求に従って、暗号化データを復号せずに、預託された暗号化データを検索する、検索処理方式が記載されている。この検索処理方式は、平文と暗号文が一対一の単純な対応関係を有する決定的暗号化方式よりも安全な、平文と暗号文が一対ｍの複雑な対応関係を有する確率的暗号化方式を採用しており、サーバ管理者への情報漏洩を防ぎながら、かつサーバに預託したデータを安全に検索するための技術が開示されている。

先行技術文献

非特許文献

[0004] 非特許文献1：Dawn Xiaodong Song, David Wagner, Arian Perrig. ”Practical Techniques for Searches on Encrypted Data”. In Proceedings of the 2000 IEEE Symposium on Security and Privacy, pages 44－55 (2000).

非特許文献2：Zhiqiang Yang, Sheng Zhong, Rebecca N. Wright. “Privacy-Preserving Queries on Encrypted Data”. In Proceedings of the 11th European Symposium on Research in Computer Security (Esorics), Volume 4189 of Lecture Notes in Computer Science, pages 476-495(2006).

発明の概要

発明が解決しようとする課題

[0005] しかしながら、非特許文献１、非特許文献２に記載された技術では、サーバに預託する確率的暗号化で暗号化したデータを復号化するために必要な、運用管理が複雑、クライアント・サーバ共に複雑である。更に、擬似乱数による確率的暗号化は、クライアントが検索をするまでは有効であるが、検索後は、検索に該当した暗号文の擬似乱数のマスクが解除されてしまい、暗号文の安全性が、確率的暗号化から、決定的暗号化に低下してしまう。しかも、クライアントは、検索時の要求(検索クエリ)の暗号化には、安全性の低い決定的暗号化方式を用いているため、頻度分析等の不正攻撃に対しても、脆弱である。

課題を解決するための手段

[0006] 前記課題を解決するために、検索可能暗号処理システムは、データを預かるＤＢサーバと、ＤＢサーバにデータを預託する登録クライアントと、ＤＢサーバにデータを検索させる検索クライアントがネットワーク経由で連携し、登録クライアントは、ハッシュ値と準同型関数の出力値によるマスクを用いた確率的暗号化方式により、暗号化したデータを、安全にサーバに預託し、検索クライアントは、検索クエリの暗号化に、複数の異なる入力値から同一の値を出力する準同型関数を用いたマスクによる確率的暗号化を用い、ＤＢサーバにマスクを解除させずに、かつ、ＤＢサーバに検索に該当するデー

タの出現頻度が漏洩しないよう、検索クエリと該当しないデータを検索結果として出力させ、検索クライアントは、検索結果を入手後、再暗号化を行い、ＤＢサーバにデータを再預託する。

発明の効果

[0007] クライアントがＤＢサーバを利用した検索後も、検索に該当したデータが確率的暗号で暗号化されており、安全性が高い。また、複雑な運用管理をクライアントに強いることなく、暗号化されたデータを効率的に復号化できる。

図面の簡単な説明

[0008] [図1]検索可能暗号処理システムの概略を例示する図である。

[図2]登録クライアントの機能の概略を例示する図である。

[図3]検索クライアントの機能の概略を例示する図である。

[図4]ＤＢサーバの機能の概略を例示する図である。

[図5]コンピュータの概略構成を例示する図である。

[図6]登録クライアントの出力部の表示内容を例示する図である。

[図7A]登録クライアントが作成する連結データのデータ構成を例示するブロック図である。

[図7B]登録クライアントが作成する連結データのデータ構成を例示するブロック図である。

[図7C]登録クライアントが作成する秘匿登録データのデータ構成を例示するブロック図である。

[図8]登録クライアントが秘匿登録データをＤＢサーバへ登録する処理を例示するシーケンス図である。

[図9A]ＤＢサーバのデータベース記憶部に記憶される、データベースの管理状態を例示する図である。

[図9B]ＤＢサーバのデータベース記憶部に記憶される、データベースの検索手順を例示する図である。

[図10]検索クライアントの出力部の表示内容を例示する図である。

[図11A]検索クライアントが作成する連結データのデータ構成を例示するブロック図である。

[図11B]検索クライアントが作成する連結データのデータ構成を例示するブロック図である。

[図11C]検索クライアントが作成する連結データのデータ構成を例示するブロック図である。

[図12]検索クライアントが、秘匿検索クエリを用い、ＤＢサーバ内のデータベースを検索する処理を例示するシーケンス図である。

[図13A]ＤＢサーバが通信部から受信した秘匿検索クエリを復号化した、連結データのデータ構成を例示するブロック図である。

[図13B]ＤＢサーバが、データベース記憶部に記憶した、秘匿登録データのデータ構成を例示するブロック図である。

[図13C]ＤＢサーバが作成する連結データのデータ構成を例示するブロック図である。

[図13D]ＤＢサーバが作成する連結データのデータ構成を例示するブロック図である。

[図14A]検索クライアントが通信部から受信した秘匿登録データのデータ構成を例示するブロック図である。

[図14B]検索クライアントが作成するデータC_Rのデータ構成を例示するブロック図である。

[図14C]ＤＢサーバが作成する連結データのデータ構成を例示するブロック図である。

発明を実施するための形態

[0009] 以下、本発明の実施の形態を図面に基づいて詳細に説明する。

[0010] 図１は、本実施形態の検索処理システムの概略図である。図示するように、検索処理システムは、登録クライアント100（Registration Client）と、検索クライアント200（Search Client）と、ＤＢサーバ300（Data Base Server）とを備え、登録クライアント100とＤＢサーバ300、検索クライアント200

とＤＢサーバ300は、ネットワーク400を介して相互に情報を送受信できるように構成されている。

[0011] ここで、本実施形態における登録クライアント100は、秘匿化したデータをＤＢサーバ300に送信するデータ登録用の送受信装置として機能し、検索クライアント200は、秘匿化した検索クエリをＤＢサーバ300に送信し、検索結果を受信する、検索用の送受信装置として機能し、ＤＢサーバ300は、秘匿化したデータをデータベースに保管し、またデータベース内のデータを検索するＤＢ管理用の送受信装置として機能する。

[0012] 図２は、登録クライアント100の機能概略図である。図示するように、登録クライアント100は、制御部110と、記憶部120と、入力部101と、出力部102と、通信部103とを備える。

[0013] 記憶部120は、登録データ記憶部130と、秘密鍵記憶部150と、パラメータ記憶部160と、一時情報記憶部180とを備える。

[0014] 登録データ記憶部130には、ＤＢサーバ300に送信するデータである、送信文を特定する情報が記憶される。ここで、本実施形態においては、入力部101を介して、受け付けた平文登録データ131を特定する情報と、ＤＢサーバ300に登録する、秘匿登録データ132を定する情報と、平文登録データ131と秘匿登録データ132の属性133を特定する情報とが記憶される。

[0015] 秘密鍵記憶部150には、安全性の観点から登録クライアント100が秘密に管理すべき、秘密鍵151を特定する情報が記憶される。ここで、本実施形態においては、暗号化部112に入力する秘密鍵151と、擬似乱数生成部114に入力する秘密鍵151と、圧縮関数部115に入力する秘密鍵151とを特定する情報が記憶される。

[0016] パラメータ記憶部160には、データの秘匿化に用いる、パラメータを特定する情報が記憶される。ここで、本実施形態においては、準同型関数部116に入力する関数パラメータ161と、基本演算部117に入力する検査パラメータ162とを特定する情報が記憶される。また、安全性の観点から、関数パラメータ161は、登録クライアント100が秘密に管理すべき情報である。

[0017] 一時情報記憶部180には、制御部110での処理で必要となる情報が記憶される。

[0018] 制御部110は、全体処理部111と、暗号化部112と、擬似乱数生成部114と、圧縮関数部115と、準同型関数部116と、基本演算部117とを備える。

[0019] 全体処理部111は、登録クライアント100における全ての処理を制御する。

[0020] 例えば、本実施形態において、全体処理部111は、入力部101を介して入力を受け付けた情報を、登録データ記憶部130に平文登録データ131として記憶する処理を行う。

[0021] また、本実施形態において、全体処理部111は、平文登録データ131を出力部102に表示する処理を行う。

[0022] また、本実施形態において、全体処理部111は、登録データ記憶部130に記憶した平文登録データ131を読み込み、それぞれ、暗号化部112と、擬似乱数生成部114と、圧縮関数部115と、準同型関数部116と、基本演算部117とに入力し、出力されたデータを、登録データ記憶部130に秘匿登録データ132として記憶する処理を行う。

[0023] また、本実施形態において、全体処理部111は、属性133と秘匿登録データ132を、通信部103を介してＤＢサーバ300に送信する処理を行う。

[0024] さらに、本実施形態において、全体処理部111は、ＤＢサーバ300より通信部103を介して受信した属性133と秘匿登録データ132を、一時情報記憶部180に記憶する処理と出力部102に表示する処理を行う。

[0025] 暗号化部112は、入力されたデータを暗号化したデータを出力する処理を行う。

[0026] 例えば、本実施形態においては、全体処理部111からデータと秘密鍵151が入力され、秘密鍵151を用い、暗号化したデータを出力する処理を行う。

[0027] 例えば、標準的な暗号化アルゴリズムの実装により、暗号化部112は実現される。

[0028] 擬似乱数生成部114は、擬似乱数を出力する処理を行う。

[0029] 例えば、擬似乱数生成部114は、温度、時間、電力量、等の物理現象から、

乱数を出力する。

[0030] 本実施形態においては、擬似乱数生成部114は、全体処理部111から入力された秘密鍵151を用い、擬似乱数を出力する。また、秘密鍵151のデータ値は新しいデータ値に更新され、再び、全体処理部111により秘密鍵記憶部150に記憶される。

[0031] 例えば、標準的な擬似乱数生成アルゴリズムの実装により、擬似乱数生成部114は実現される。

[0032] 圧縮関数部115は、入力されたデータを圧縮したデータを出力する処理を行う。

[0033] 例えば、本実施形態においては、全体処理部111から入力されたデータを固定長（ｈビット）の別のデータに変換し、出力する処理を行う。

[0034] 例えば、標準的な暗号ハッシュ関数アルゴリズムの実装により、任意長の入力データを固定長のデータへ変換する圧縮関数部115が実現できる。

[0035] 準同型関数部116は、入力されたデータに対し、関数計算の出力結果をデータとして出力する処理を行う。

[0036] 例えば、本実施形態においては、全体処理部111から入力されたデータを、準同型の性質を有する関数の入力値とみなし、全体処理部111から入力された関数パラメータ161を用いて、関数計算の出力値をバイナリ列で表現した固定長（ｆビット）のデータに変換する処理を行う。

[0037] ただし、準同型関数とは、関数Ｆと、入力変数ｘ、入力変数ｙに対し、

Ｆ（ｘ・ｙ）＝Ｆ（ｘ）？Ｆ（ｙ） (1)

が成り立つ関数を指す。ただし、・と？は、演算記号を表わし、加算用の演算記号+、乗算用の演算記号*、ビット毎の排他的論理和であるＸＯＲ(eXclusive OR)演算用の演算記号xor等が入る。

[0038] 本実施形態では、・と？にＸＯＲ演算記号xorが入る場合、即ち式（2）が成り立つ場合を示す。

Ｆ（ｘ xor ｙ）＝Ｆ（ｘ）xor Ｆ（ｙ） (2)

ただし、準同型関数が式（2）以外の演算記号で成り立つ時でも、本実施形

態は同様に実施できる。

[0039] なお、準同型関数を実現するアルゴリズムの実装により、準同型関数部116は実現される。

[0040] 基本演算部117は、加算、減算、比較算等の基本的な算術演算に関する処理を行う。

[0041] 例えば、本実施形態においては、基本演算部117は、全体処理部111から入力された２つのデータのビット毎の排他的論理和であるＸＯＲ演算や、比較演算の等号成立または不成立の検証結果を、データとして出力する処理を行う。

[0042] 以上に示した登録クライアント100は、例えば、図５（コンピュータの概略図）に示すような、ＣＰＵ(Central Processing Unit)501と、メモリ502と、ＨＤＤ(Hard Disk Drive)等の外部記憶装置503と、ＣＤ(Compact Disk)やＤＶＤ(Digital Versatile Disk)等の可搬性を有する記憶媒体508に対して情報を読み書きする読書装置507と、キーボードやマウス等の入力装置506と、ディスプレイ等の出力装置505と、通信ネットワークに接続するためのＮＩＣ(Network Interface Card)等の通信装置504と、これらを連結するシステムバス等の内部通信線(システムバスという)509と、を備えた一般的なコンピュータ500で実現できる。

[0043] 例えば、記憶部120は、ＣＰＵ501がメモリ502または外部記憶装置503を利用することにより実現可能であり、制御部110と制御部110に含まれる各処理部は、外部記憶装置503に記憶されている所定のプログラムをメモリ502にロードしてＣＰＵ501で実行することで実現可能であり、入力部101は、ＣＰＵ501が入力装置506を利用することで実現可能であり、出力部102は、ＣＰＵ501が出力装置505を利用することで実現可能であり、通信部103は、ＣＰＵ501が通信装置504を利用することで実現可能である。

[0044] この所定のプログラムは、読書装置507を介して記憶媒体508から、あるいは、通信装置504を介してネットワークから、外部記憶装置503に記憶(ダウンロード)され、それから、メモリ502上にロードされて、ＣＰＵ501により実行

されるようにしてもよい。また、読書装置507を介して、記憶媒体508から、あるいは通信装置504を介してネットワークから、メモリ502上に直接ロードされ、ＣＰＵ501により実行されるようにしてもよい。

[0045] 図３は、検索クライアント200の機能概略図である。図示するように、検索クライアント200は、制御部210と、記憶部220と、入力部201と、出力部202と、通信部203とを備える。

[0046] 記憶部220は、検索クエリ記憶部230と、秘密鍵記憶部250と、パラメータ記憶部260と、受信データ記憶部270と、一時情報記憶部280とを備える。

[0047] 検索クエリ記憶部230には、ＤＢサーバ300に送信するデータである、送信文を特定する情報が記憶される。ここで、本実施形態においては、検索クライアント200が、入力部201を介して受け付けた平文検索クエリ231を特定する情報と、ＤＢサーバ300に送信する秘匿検索クエリ232と、平文検索クエリ231と秘匿検索クエリ232の属性233を特定する情報とが記憶される。

[0048] 秘密鍵記憶部250には、安全性の観点から検索クライアント200が秘密に管理すべき、秘密鍵251を特定する情報が記憶される。ここで、本実施形態においては、暗号化部212に入力する秘密鍵251と、復号化部213に入力する秘密鍵251と、擬似乱数生成部214に入力する秘密鍵251と、圧縮関数部215に入力する秘密鍵251とを特定する情報が記憶される。

[0049] パラメータ記憶部260には、データの秘匿化と秘匿化解除とに用いるパラメータを特定する情報が記憶される。ここで、本実施形態においては、準同型関数部216に入力する関数パラメータ261を特定する情報と、基本演算部217に入力する検査パラメータ262を特定する情報とが記憶される。また、安全性の観点から、関数パラメータ261は、検索クライアント200が秘密に管理すべき情報である。

[0050] 受信データ記憶部270には、通信部203を介して受信したデータを特定する情報が記憶される。ここで、本実施形態においては、受信データ記憶部270には、通信部203を介してＤＢサーバ300から受信したデータを特定する情報が、秘匿登録データ271として記憶される。また、秘匿登録データ271から、秘

匿化を解除したデータを、平文登録データ272として受信データ記憶部270に記憶する処理を行う。

[0051] 一時情報記憶部280には、制御部210での処理で必要となる情報が記憶される。

[0052] 制御部210は、全体処理部211と、暗号化部212と、復号化部213と、擬似乱数生成部214と、圧縮関数部215と、準同型関数部216と、基本演算部217とを備える。

[0053] 全体処理部211は、検索クライアント200における全ての処理を制御する。

[0054] 例えば、本実施形態において、全体処理部211は、入力部201を介して入力を受け付けた情報を、検索クエリ記憶部230に平文検索クエリ231として記憶する処理を行う。

[0055] また、本実施形態において、全体処理部211は、平文検索クエリ231を出力部202に表示する処理を行う。

[0056] また、本実施形態において、全体処理部211は、検索クエリ記憶部230に記憶した平文検索クエリ231を読み込み、それぞれ、暗号化部212と、擬似乱数生成部214と、圧縮関数部215と、準同型関数部216と、基本演算部217とに入力し、出力されたデータを秘匿検索クエリ232として検索クエリ記憶部230に記憶する処理を行う。

[0057] また、本実施形態において、全体処理部211は、通信部203を介して、属性233と秘匿検索クエリ232をＤＢサーバ300に送信する処理を行う。

[0058] また、本実施形態において、全体処理部211は、通信部203を介して、秘匿登録データ271をＤＢサーバ300から受信する処理を行う。

[0059] また、本実施形態において、全体処理部211は、通信部203を介して、受信した秘匿登録データ271を受信データ記憶部270に秘匿登録データ271として記憶する処理を行う。

[0060] また、本実施形態において、全体処理部211は、受信データ記憶部270に記憶した秘匿登録データ271を読み込み、それぞれ、復号化部213と、圧縮関数部215と、準同型関数部216と、基本演算部217とに入力し、出力されたデータ

を平文登録データ272として受信データ記憶部270に記憶する処理を行う。

[0061] また、本実施形態において、全体処理部211は、平文登録データ272を出力部202に表示する処理を行う。

[0062] さらに、全体処理部211は、ＤＢサーバ300より、通信部203を介して受信したデータを、一時情報記憶部280に記憶する処理と、出力部202に表示する処理を行う。

[0063] 暗号化部212は、入力されたデータを暗号化したデータを出力する処理を行う。

[0064] 例えば、本実施形態においては、全体処理部211からデータと秘密鍵251が入力され、秘密鍵251を用い、暗号化したデータを出力する処理を行う。

[0065] 復号化部213は、入力されたデータを復号化したデータを出力する処理を行う。

[0066] 例えば、本実施形態においては、全体処理部211からデータと秘密鍵251が入力され、秘密鍵251を用い、復号化したデータを出力する処理を行う。

[0067] 擬似乱数生成部114は、擬似乱数を出力する処理を行う。

[0068] 例えば、擬似乱数生成部214は、温度、時間、電力量、等の物理現象から、乱数を出力する。

[0069] 本実施形態においては、擬似乱数生成部214は、全体処理部211から入力された秘密鍵251を用い、擬似乱数を出力する。また、秘密鍵251のデータ値は新しいデータ値に更新され、再び、全体処理部211により秘密鍵記憶部250に記憶される。

[0070] 例えば、本実施形態においては、全体処理部211から入力された秘密鍵251を用い、擬似乱数を出力する処理を行う。

[0071] 圧縮関数部215は、入力されたデータを圧縮したデータを出力する処理を行う。

[0072] 例えば、本実施形態においては、全体処理部211から入力されたデータを固定長（ｈビット）の別のデータに変換し、出力する処理を行う。

[0073] 準同型関数部216は、入力されたデータに対し、関数計算の出力結果をデー

タとして出力する処理を行う。

[0074] 例えば、本実施形態においては、全体処理部211から入力されたデータを準同型の性質を有する関数の入力値とみなし、全体処理部211から入力された関数パラメータ261を用いて、関数計算の出力値をバイナリ列で表現した固定長（ｆビット）のデータに変換する処理を行う。

[0075] ただし、準同型関数は、関数Ｆと、入力変数ｘ、入力変数ｙに対し、式（2）が成り立つ場合を示すが、ビット毎の排他的論理和であるＸＯＲ演算以外の演算記号で準同型性が成り立つ時も、本実施形態は同様に実施できる。

[0076] 基本演算部217は、加算、減算、比較算等の基本的な算術演算に関する処理を行う。

[0077] 例えば、本実施形態においては、基本演算部217は、全体処理部211から入力された２つのデータのバイナリ値（２進数）の減算結果を、データとして出力する処理を行う。

[0078] 以上に示した検索クライアント200は、例えば、図５（コンピュータの概略図）に示すような、ＣＰＵ501と、メモリ502と、ＨＤＤ等の外部記憶装置503と、ＣＤやＤＶＤ等の可搬性を有する記憶媒体508に対して情報を読み書きする読書装置507と、キーボードやマウス等の入力装置506と、ディスプレイ等の出力装置505と、通信ネットワークに接続するためのＮＩＣ等の通信装置504と、これらを連結するシステムバス等の内部通信線(システムバスという)と、を備えた一般的なコンピュータで実現できる。

[0079] 例えば、記憶部220は、ＣＰＵ501がメモリ502または外部記憶装置503を利用することにより実現可能であり、制御部210と制御部210に含まれる各処理部は、外部記憶装置503に記憶されている所定のプログラムをメモリ502にロードしてＣＰＵ501で実行することで実現可能であり、入力部201は、ＣＰＵ501が入力装置506を利用することで実現可能であり、出力部202は、ＣＰＵ501が出力装置505を利用することで実現可能であり、通信部203は、ＣＰＵ501が通信装置504を利用することで実現可能である。

[0080] この所定のプログラムは、読書装置507を介して記憶媒体508から、あるい

は、通信装置504を介してネットワークから、外部記憶装置503に記憶(ダウンロード)され、それから、メモリ502上にロードされて、ＣＰＵ501により実行されるようにしてもよい。また、読書装置507を介して、記憶媒体508から、あるいは通信装置504を介してネットワークから、メモリ502上に直接ロードされ、ＣＰＵ501により実行されるようにしてもよい。

[0081] 図４は、ＤＢサーバ300の機能概略図である。図示するように、ＤＢサーバ300は、制御部310と、記憶部320と、入力部301と、出力部302と、通信部303と、を備える。

[0082] 記憶部320は、パラメータ記憶部360と、秘密鍵記憶部350と、データベース記憶部340と、検索クエリ記憶部330と、一時情報記憶部380とを備える。

[0083] パラメータ記憶部360には、秘匿検索クエリ332とデータベース341の関係の検査に用いる、パラメータを特定する情報が記憶される。ここで、本実施形態においては、準同型関数部316に入力する関数パラメータ361を特定する情報が記憶される。また、安全性の観点から、関数パラメータ361はＤＢサーバ300が秘密に管理すべき情報である。

[0084] 秘密鍵記憶部350には、安全性の観点からＤＢサーバ300が秘密に管理すべき、秘密鍵351を特定する情報が記憶される。ここで、本実施形態においては、復号化部313に入力する秘密鍵351とを特定する情報が記憶される。

[0085] データベース記憶部340には、通信部303を介して受信した登録データを特定する情報が記憶される。ここで、本実施形態においては、通信部303を介して登録クライアント100から受信した情報を、データベース記憶部340にデータベース341の構成情報として記憶する処理を行う。

[0086] 検索クエリ記憶部330には、通信部303を介して受信した検索クエリを特定する情報が記憶される。ここで、本実施形態においては、通信部303を介して検索クライアント200から受信した情報を、検索クエリ記憶部330に秘匿検索クエリ332として記憶する処理を行う。

[0087] 一時情報記憶部380には、制御部310での処理で必要となる情報が記憶される。

[0088] 制御部310は、全体処理部311と、復号化部313と、圧縮関数部315と、準同型関数部316と、基本演算部317と、を備える。

[0089] 全体処理部311は、ＤＢサーバ300における全ての処理を制御する。

[0090] 例えば、本実施形態において、全体処理部311は、通信部303を介して秘匿登録データ131を、登録クライアント100から受信する処理を行う。

[0091] また、本実施形態において、全体処理部311は、通信部303を介して受信した秘匿登録データ131を、データベース記憶部340にデータベース341の構成情報として記憶する処理を行う。

[0092] また、本実施形態において、全体処理部311は、通信部303を介して秘匿検索クエリ332を、検索クライアント200から受信する処理を行う。

[0093] また、本実施形態において、全体処理部311は、通信部303を介して受信した秘匿検索クエリ332を、検索クエリ記憶部330に記憶する処理を行う。

[0094] また、本実施形態において、全体処理部311は、検索クエリ記憶部330に記憶した秘匿検索クエリ332を読み込み、それぞれ、復号化部313と、圧縮関数部315と、準同型関数部316と、基本演算部317とに入力し、出力されたデータを、通信部303を介して、検索クライアント200に送信する処理を行う。

[0095] さらに、全体処理部311は、検索クライアント200または登録クライアント100より、通信部303を介して受信したデータに関する情報を、一時情報記憶部380に記憶する処理と、出力部302に表示する処理を行う。

[0096] 復号化部313は、入力されたデータを復号化したデータを出力する処理を行う。

[0097] 例えば、本実施形態においては、全体処理部311からデータと秘密鍵351が入力され、秘密鍵351を用い、復号化したデータを出力する処理を行う。

[0098] 圧縮関数部315は、入力されたデータを圧縮したデータを出力する処理を行う。

[0099] 例えば、本実施形態においては、全体処理部311から入力されたデータを固定長（ｈビット）の別のデータに変換し、出力する処理を行う。

[0100] 準同型関数部316は、入力されたデータに対し、関数計算の出力結果をデー

タとして出力する処理を行う。

[0101] 例えば、本実施形態においては、全体処理部311から入力されたデータを、準同型の性質を有する関数の入力値とみなし、全体処理部311から入力された関数パラメータ361を用いて、関数計算の出力値をバイナリ列で表現したデータを固定長（ｆビット）のデータに変換する処理を行う。

[0102] ただし、準同型関数は、関数Ｆと、入力変数ｘ、入力変数ｙに対し、式（2）が成り立つ場合を示すが、ビット毎の排他的論理和であるＸＯＲ演算以外の演算記号で準同型性が成り立つ時も、本実施形態は同様に実施できる。

[0103] 基本演算部317は、加算、減算、比較算等の基本的な算術演算に関する処理を行う。

[0104] 例えば、本実施形態においては、基本演算部317は、全体処理部311から入力された２つのデータのバイナリ値（２進数）の減算結果をデータとして出力する処理を行う。

[0105] また、本実施形態においては、基本演算部317は、全体処理部311から入力された２つのデータのバイナリ値（２進数）の比較結果をデータとして出力する処理を行う。

[0106] 以上に示したＤＢサーバ300は、例えば、図５（コンピュータの概略図）に示すような、ＣＰＵ501と、メモリ502と、ＨＤＤ等の外部記憶装置503と、ＣＤやＤＶＤ等の可搬性を有する記憶媒体508に対して情報を読み書きする読書装置507と、キーボードやマウス等の入力装置506と、ディスプレイ等の出力装置505と、通信ネットワークに接続するためのＮＩＣ等の通信装置504と、これらを連結するシステムバス等の内部通信線(システムバスという)とを備えた一般的なコンピュータで実現できる。

[0107] 例えば、記憶部120、220、320は、ＣＰＵ501がメモリ502または外部記憶装置503を利用することにより実現可能であり、制御部110、210、310と制御部110、210、310に含まれる各処理部は、外部記憶装置503に記憶されている所定のプログラムをメモリ502にロードしてＣＰＵ501で実行することで実現可能であり、入力部101、201、301は、ＣＰＵ501が入力装置506を利用することで

実現可能であり、出力部102、202、302は、ＣＰＵ501が出力装置505を利用することで実現可能であり、通信部103、203、303は、ＣＰＵ501が通信装置504を利用することで実現可能である。

[0108] この所定のプログラムは、読書装置507を介して記憶媒体508から、あるいは、通信装置504を介してネットワークから、外部記憶装置503に記憶(ダウンロード)され、それから、メモリ502上にロードされて、ＣＰＵ501により実行されるようにしてもよい。また、読書装置507を介して記憶媒体508から、あるいは通信装置504を介してネットワークから、メモリ502上に直接ロードされ、ＣＰＵ501により実行されるようにしてもよい。

[0109] 図６は、登録クライアント100の出力部102の表示内容600を例示した図である。図示するように、登録クライアント100は、管理方法の選択部610と、管理フォーム部620と、実行と表示されたボタンを指す実行ボタン650と、クリアと表示されたボタンを指すクリアボタン660とを備える。

[0110] 管理方法の選択部610は、データの登録と、データの更新と、データの削除となどの、データの管理に関する項目から構成される。例えば、本実施形態では、データ追加と、データ更新と、データ削除とを特定するラジオボタンを備える。また、入力部101を介し、各項目が選択可能である。

[0111] 管理フォーム部620は、管理方法の選択部610で特定された項目である、データの登録と、データの更新と、またはデータの削除とに応じて扱う、データの種類を示す属性621と、データの詳細内容を入力する入力フォーム622から構成される。例えば、本実施形態では、番号と、氏名と、Ｅメールと、所属部署とを指す属性621と、番号の入力用と、氏名の入力用と、Ｅメールの入力用と、所属部署の入力用とに設計された入力フォーム622を備える。各入力フォーム622に入力された情報は、記憶部120の一時情報記憶部180に記憶される。

[0112] クリアボタン660は、入力部101を介し、選択可能である。例えば、本実施形態では、クリアボタン660が選択されると、各入力フォーム622に入力された情報を消去する。

[0113] 実行ボタン650は、入力部101を介し、選択可能である。例えば、本実施形態では、実行ボタン650が選択されると、管理方法の選択部610で特定された項目と各フォームに入力された情報を基に、秘匿登録データ131を作成し、ＤＢサーバ300へ送信する処理を行う。以下では、管理方法の選択部610で、特定された項目がデータ登録である場合を説明するが、データ更新と、データ削除とが特定された場合も、同様の処理を行う。

[0114] 管理方法の選択部610で、特定された項目がデータ登録である場合に、実行ボタン650が選択された場合に、実施する秘匿登録データ131の処理手順をＳ701からＳ715に示す。

[0115] 図７Ａは、本実施形態において、登録クライアント100が、出力部102に出力した入力フォーム622に入力された情報を基に作成する、連結データ703のデータ構成を示すブロック図の例である。

[0116] また、図７Ｂは、本実施形態において、登録クライアント100が、秘匿登録データ712を作成する過程において作成する、連結データ704のデータ構成を示すブロック図の例である。

[0117] また、図７Ｃは、本実施形態において、登録クライアント100が作成する、秘匿登録データ712のデータ構成を示すブロック図である。

[0118] 以下では、図７Ａと、図７Ｂと、図７Ｃとを用い、入力フォーム622に入力されたデータ値によらず、登録クライアント100が、毎回、データ値の異なる秘匿登録データ712を作成する処理手順を説明する。

[0119] 登録クライアント100の全体処理部111は、入力フォーム622に入力された情報を平文登録データ701として、記憶部120の登録データ記憶部130に記憶する処理を行う。このとき、平文登録データ701は、登録クライアント100の一時情報記憶部180にｍビットのバイナリ表現で構成されたデータとして記憶される。

[0120] 登録クライアント100の全体処理部111は、パラメータ記憶部160に記憶された検査パラメータ162を読み込み、誤り検査データ702として出力する処理を行う。このとき、出力された誤り検査データ702は、登録クライアント100の

一時情報記憶部180に、ｅビットのデータとして記憶される。

[0121] 登録クライアント100の全体処理部111は、平文登録データ701と誤り検査データ702を連結する処理を行う（S701）。

[0122] 連結処理では、平文登録データ701の各所に、分割した誤り検査データ702を挿入してもよい。例えば、平文登録データ701の初め（ヘッダ）と終わり（フッタ）に、誤り検査データ702を挿入してもよい。また、誤り検査データ702に平文登録データ701を乗算で掛け合わせるなど、混合させてもよい。

[0123] 以下では、図７Ａに示すように、登録クライアント100において、全体処理部111が入力した平文登録データ701の末尾に、誤り検査データ702を連結し、連結データ703を一つのデータとみなした場合を扱う。このとき、登録クライアント100の一時情報記憶部180には、連結データ703は（ｍ＋ｅ）ビットのデータとして記憶される。ただし、連結処理は、この場合に限定されるわけではなく、他の連結処理でも、同様に実施できる。

[0124] 次に、図７Ｂに示すように、登録クライアント100が作成する連結データ704のデータ構成を説明する。

[0125] 登録クライアント100の全体処理部111は、平文登録データ701と誤り検査データ702を連結したデータである連結データ703と、秘密鍵記憶部150に記憶された秘密鍵151とを暗号化部112へ入力する処理を行う(S702)。

[0126] 登録クライアント100の暗号化部112は、入力されたデータを暗号化し、データC_R705を出力する処理を行う(S703)。

[0127] 登録クライアント100において、全体処理部111が入力した連結データ703を暗号化部112が暗号化し、出力したデータをデータC_R705とみなす。このとき、データC_R705は、登録クライアント100の一時情報記憶部180には、ｃビットのデータとして記憶される(S704)。

[0128] なお、データC_R705は、連結データ703に依存、即ち、入力フォーム622の入力情報に依存して構わない。例えば、同一のデータ値を持つ連結データ703からは、同一のデータC_R705を出力してもよい。

[0129] 登録クライアント100の全体処理部111は、秘密鍵記憶部150から秘密鍵151

を読み出し、秘密鍵151を、擬似乱数生成部114に入力する処理を行う(S705)。

[0130] 登録クライアント100の擬似乱数生成部114は、入力された秘密鍵151を用い、擬似乱数を出力する処理を行う。このとき、擬似乱数は、登録クライアント100の一時情報記憶部180には、ｒビットのデータP_R706として記憶される(S706)。

[0131] 擬似乱数生成部114が出力する擬似乱数は、連結データ703、データC_R705に依存しない。従って、入力フォーム622の入力情報に依存せず、毎回、データ値の異なるデータP_R706を作成できる。

[0132] 登録クライアント100の全体処理部111は、秘密鍵記憶部150から秘密鍵151を読み出し、秘密鍵151と乱数生成部から出力されたデータP_R706を連結したデータを、圧縮関数部115に入力する処理を行う(S707)。

[0133] 登録クライアント100の圧縮関数部115は、入力されたデータを変換し、ハッシュ値を出力する処理を行う。このとき、ハッシュ値は、登録クライアント100の一時情報記憶部180には、ｈビットのデータH_R707として記憶される(S708)。

[0134] データH_R707は、圧縮関数の性質から、乱数とみなせる。データH_R707は、連結データ703、データC_R705に依存しない。従って、データP_R706同様、入力フォーム622の入力情報に依存せず、毎回、データ値の異なるデータH_R707を作成できる。

[0135] 登録クライアント100の全体処理部111は、データH_R707と、パラメータ記憶部160に記憶された関数パラメータ161とを準同型関数部116に入力する(S709)。

[0136] 登録クライアント100の準同型関数部116は、入力されたデータを準同型の性質を有する関数の入力値とみなし、関数パラメータ161を用いて、関数計算の出力値をバイナリ列で表現した準同型関数値を出力する処理を行う。このとき、準同型関数値は、登録クライアント100の一時情報記憶部180には、ｆビットのデータF_R708として記憶される(S710)。

[0137] なお、準同型関数をfuncとした場合、その入力値であるデータH_R707、出力値であるデータF_R708には、式（3）が成り立つ（ただし、関数パラメータ161の記述は省略）。

$$F_R = func(H_R) \quad (3)$$

データF_R708は、準同型関数部116が処理する準同型関数の性質から、入力されたデータ値が乱数の場合、出力も乱数とみなせる。また、データF_R708は、連結データ703と、データC_R705に依存しない。従って、データH_R707同様、入力フォーム622の入力情報に依存せず、毎回、データ値の異なるデータF_R707を作成できる。

[0138] 登録クライアント100の全体処理部111は、準同型関数部116から出力されたデータF_R708を、圧縮関数部115へ入力する処理を行う(S711)。

[0139] 登録クライアント100の圧縮関数部115は、入力されたデータを変換し、ハッシュ値を出力する処理を行う。このとき、ハッシュ値は、登録クライアント100の一時情報記憶部180には、ｇビットのデータG_R709として記憶される(S712)。

[0140] データG_R709は、圧縮関数の性質から、乱数である。従って、データF_R707と、データH_R707同様、入力フォーム622の入力情報に依存せず、毎回、データ値の異なるデータG_R709を作成できる。また、圧縮関数の性質から、逆像は計算困難であるため、データG_R709をＤＢサーバ300に登録しても、データの安全性に影響を与えない。

[0141] 図７Ｃは、本実施形態において、登録クライアント100が作成する秘匿登録データ712のデータ構成を示すブロック図である。

[0142] 登録クライアント100の全体処理部111は、データH_R707とデータC_R705とを基本演算部117へ入力する処理を行う(S713)。

[0143] 登録クライアント100の基本演算部117は、入力されたデータH_R707とデータC_R705とのビット毎の排他的論理和であるＸＯＲ算を計算し、その計算結果を、データD_R711として出力する処理を行う(S714)。

[0144] S714のxor算により、データH_R707とデータC_R705とデータD_R711とは式（

4）を満たす。

$$D_R = H_R \text{ xor } C_R \qquad (4)$$

S714の計算は、連結データ703やデータC_R705に依存しない、乱数であるデータH_R707を用いている。従って、連結データ703とデータC_R705の関係が一意に定まる場合でも、毎回、データ値が異なる、データH_R707を用いれば、異なるデータ値のデータD_R711が得られる。

[0145] 登録クライアント100の全体処理部111は、データP_R706とデータD_R711とデータG_R709とを連結し、作成したデータを、秘匿登録データ712として登録データ記憶部130へ記憶する処理を行う(S715)。

[0146] 秘匿登録データ712は、連結データ703やデータC_R705に依存しない乱数であるデータP_R706、データD_R711、データG_R709を用いており、毎回、異なるデータ値が得られる。その結果、データP_R706とデータD_R711とデータG_R709とを連結した秘匿登録データ712は、連結データ703とデータC_R705とは独立している。即ち、入力フォーム622の入力情報に依存せず、毎回、データ値の異なる秘匿登録データ712を作成できる。

[0147] なお、上記の処理手順は、固定されたものではなく、処理手順を変更してもよい。例えば、S713とS714の処理手順を変更し、S713でデータP_R706とデータH_R707とデータG_R709を連結してから、S714でデータH_R707とデータC_R705とのXOR算を計算してもよい。同様に、他の処理手順を変更してもよい。

[0148] また、上記の各処理を担当する制御部110は固定されたものではなく、担当する制御部110を変更してもよい。例えば、S711でデータF_R708を、圧縮関数部115ではなく、暗号化部112にデータF_R708を入力してもよく、S712では、暗号化部112から出力されたデータを、データG_R709として一時情報記憶部180に記憶してもよい。

[0149] また、秘匿登録データ712のデータ構成を変更し、それに併せて処理を変更してもよい。例えば、データP_R706に関する情報は、記憶部120に記憶し、秘匿登録データ712に含まないように構成しても構わない。この時、S706が出力するデータをデータH_R706とみなし、S707とS708に係る処理は削除可能であ

る。また、この時、S715で登録クライアント100の全体処理部111は、秘匿登録データ712として、データD_R711とデータG_R709とを連結すればよい。

[0150] 図８は、本実施形態において、ネットワーク400を経由し、登録クライアント100が、秘匿登録データ132をＤＢサーバ300へ登録する処理を示すシーケンス図である。

[0151] 登録クライアント100は、入力部101を経由し、ユーザからフォームへ入力された情報を一時情報記憶部180に記憶する処理を行う（Ｓ８０１）。

[0152] 登録クライアント100は、入力部101を経由し、ユーザにより実行ボタン650が選択されたことを検知し、フォームに入力された情報を、平文登録データ131として記憶部120へ記憶する処理を行う（Ｓ８０２）。

[0153] 登録クライアント100は、制御部110により秘匿登録データ132を作成し、記憶部120へ記憶する処理を行う（Ｓ８０３）。

[0154] 登録クライアント100は、通信部103からネットワーク400を経由し、属性133と秘匿登録データ132を、ＤＢサーバ300へ送信する処理を行う（Ｓ８０４）。

[0155] ＤＢサーバ300は、通信部303からネットワーク400を経由し、登録クライアント100が送信した属性133と秘匿登録データ132を受信する処理を行う（Ｓ８０５）。

[0156] ＤＢサーバ300は、制御部310により受信した属性133を用い、秘匿登録データ132を、データベース341の構成情報として記憶部320へ記憶する処理を行う（Ｓ８０６）。

[0157] ＤＢサーバ300は、秘匿登録データ132の登録処理の成否を、通信部303からネットワーク400を経由し、登録サーバへ送信する処理を行う（Ｓ８０７）。

[0158] 登録クライアント100は、通信部103からネットワーク400を経由し、ＤＢサーバ300が送信した秘匿登録データ132の登録処理の成否を受信する処理を行う（Ｓ８０８）。

[0159] 登録クライアント100は、出力部102を経由し、ユーザに、登録処理の成否を含む登録情報について表示する処理を行う（Ｓ８０９）。

[0160] 図９Ａは、ＤＢサーバ300における、記憶部320のデータベース記憶部340に記憶されるデータベース341の管理状態を例示した構成図である。

[0161] 例えば、本実施形態において、ＤＢサーバ300における、データベース341は、番号と、氏名と、Eメールとなどを示す属性901と、属性901に関連付けられた秘匿登録データ902(d_0、d_1、d_2、・・・)とから構成されている。

[0162] 図１０は、検索クライアント200の出力部202の表示内容1000を例示した図である。図示するように、検索クライアント200は、検索項目部1010と、検索フォーム部1020と、検索と表示されたボタンを指す検索ボタン1050と、クリアと表示されたボタンを指すクリアボタン1060とを備える。

[0163] 検索方法の選択部は、検索対象のデータの種類に関する項目から構成される。例えば、本実施形態では、番号と、氏名と、Ｅメールと、所属部署とを特定するラジオボタンを備える。また、入力部201を介し、各項目が複数選択可能である。

[0164] 検索フォーム部1020は、検索方法の選択部で特定された属性1011である、番号と、氏名と、Ｅメールと、所属部署との詳細内容を入力する入力フォーム1022から構成される。例えば、本実施形態では、番号の入力用と、氏名の入力用と、Ｅメールの入力用と、所属部署の入力用とに設計された入力フォーム1022を複数備える。各入力フォーム1022に入力された情報は、記憶部220の一時情報記憶部280に記憶される。

[0165] クリアボタン1060は、入力部201を介し、選択可能である。例えば、本実施形態では、クリアボタン1060が選択されると、各入力フォーム1022の入力情報を消去する。

[0166] 検索ボタン1050は、入力部201を介し、選択可能である。例えば、本実施形態では、検索ボタン1050が選択されると、検索方法の選択部で特定された属性1011と入力フォーム1022に入力された情報を基に、秘匿検索クエリ232を作成し、ＤＢサーバ300へ送信する処理を行う。以下では、検索方法の選択部で、ただ一つの属性1011（例えば氏名）が選択された場合を示すが、複数の入力フォーム1022に情報が入力された場合と、複数の属性1011が選択された場

合も、同様の処理で実施できる。

[0167] 検索方法の選択部で、特定された属性1011が、ただ一つである場合に、検索ボタン1050が選択された場合の処理手順は、Ｓ1101～Ｓ1112に従う。

[0168] 図１１Ａは、本実施形態において、検索クライアント200が、出力部202に出力した入力フォーム1022に入力された情報を基に作成する連結データ1103のデータ構成を示すブロック図の例である。

[0169] また、図１１Ｂは、本実施形態において、検索クライアント200が、秘匿検索クエリ1111を作成する過程において作成する連結データ1104のデータ構成を示すブロック図の例である。

[0170] また、図１１Ｃは、本実施形態において、検索クライアント200が作成する連結データ1108のデータ構成を示すブロック図である。

以下では、図１１Ａと、図１１Ｂと、図１１Ｃとを用い、入力フォーム1022に入力されたデータ値によらず、検索クライアント200が、毎回、データ値の異なる秘匿検索クエリ1111を作成する処理手順を説明する。

[0171] 検索クライアント200の全体処理部211は、入力フォーム1022に入力された情報を、平文検索クエリ1101として記憶部220の検索クエリ記憶部230に記憶する処理を行う。このとき、平文検索クエリ1101は、検索クライアント200の一時情報記憶部280にｍビットのバイナリ表現で構成されたデータとして記憶される。

[0172] 検索クライアント200の全体処理部211は、パラメータ記憶部260に記憶された検査パラメータ262を読み込み、誤り検査データ1102として出力する処理を行う。このとき、出力された誤り検査データ1102は、検索クライアント200の一時情報記憶部280に、ｅビットのデータとして記憶される。

[0173] 検索クライアント200の全体処理部211は、平文検索クエリ1101と誤り検査データ1102を連結する処理を行う(S1101)。

[0174] 連結処理では、平文検索クエリ1101の各所に、分割した誤り検査データ1102を挿入してもよい。例えば、平文検索クエリ1101の初め（ヘッダ）と終わり（フッタ）に、誤り検査データ1102を挿入してもよい。また、誤り検査デー

タ1102に平文検索クエリ1101を乗算で掛け合わせるなど、混合させてもよい。

[0175] 以下では、図１１Ａに示すように、検索クライアント200において、全体処理部211が入力した平文検索クエリの末尾に誤り検査データ1102を連結し、連結データ1103を一つのデータとみなした場合を扱う。このとき、検索クライアント200の一時情報記憶部280には、連結データ1103は（ｍ＋ｅ）ビットのデータとして記憶される。ただし、連結処理は、この場合に限定されるわけではなく、他の連結処理でも、同様に実施できる。

[0176] 次に、図11Ｂに示すように、検索クライアント200が作成する連結データ1104のデータ構成を説明する。

[0177] 検索クライアント200の全体処理部211は、平文検索クエリ1101と誤り検査データ1102を連結したデータである連結データ1103と、秘密鍵記憶部250に記憶された秘密鍵251とを暗号化部212へ入力する処理を行う（S1102）。

[0178] 検索クライアント200の暗号化部212は、入力されたデータを暗号化し、データC_s1105を出力する処理を行う(S1103)。

[0179] 検索クライアント200において、全体処理部211が入力した連結データ1103を暗号化部212が暗号化し、出力したデータをデータC_s1105とみなして扱えばよい。このとき、データC_s1105は、検索クライアント200の一時情報記憶部280に、ｃビットのデータとして記憶される(S1104)。

[0180] なお、データC_s1105は、連結データ1103に依存、即ち、入力フォーム1022の入力情報に依存してもよい。例えば、同一のデータ値を持つ連結データ1103からは、同一のデータC_s1105を出力してもよい。

[0181] 検索クライアント200の全体処理部211は、秘密鍵記憶部250から秘密鍵251を読み出し、秘密鍵251を擬似乱数生成部214に入力する処理を行う(S1105)。

[0182] 検索クライアント200の擬似乱数生成部214は、入力された秘密鍵251を用い、擬似乱数を出力する処理を行う。このとき、擬似乱数は、検索クライアント200の一時情報記憶部280に、ｒビットのデータP_s1106として記憶される(S1106)。

[0183] 擬似乱数生成部214が出力する擬似乱数は、連結データ1103、データC_S1105に依存しない。従って、入力フォーム1022の入力情報に依存せず、毎回、データ値の異なる、データP_S1106を作成できる。

[0184] データP_S1106は、擬似乱数生成関数の性質から、乱数を出力する。また、データP_S1106は、連結データ703、データC_S705に依存しない。従って、データP_S1106は、入力フォーム1022の入力情報に依存せず、毎回、データ値の異なるデータF_S1107を作成できる。

[0185] 検索クライアント200の全体処理部211は、データP_S1106と、パラメータ記憶部260に記憶された関数パラメータ261とを準同型関数部216に入力する(S1107)。

[0186] 検索クライアント200の準同型関数部216は、入力されたデータを、準同型の性質を有する関数の入力値とみなし、関数パラメータ261を用いて、関数計算の出力値をバイナリ列で表現した準同型関数値を出力する処理を行う。このとき、準同型関数値は、検索クライアント200の一時情報記憶部280に、fビットのデータF_S1107として記憶される(S1108)。

[0187] なお、準同型関数をfuncとした場合、その入力値であるデータP_S、出力値であるデータF_Sには、式（5）が成り立つ（ただし、関数パラメータ261の記述は省略）。

$$F_S = \mathrm{func}(P_S) \qquad (5)$$

データF_S1107は、準同型関数部216が処理する準同型関数の性質から、入力されたデータ値が一様に分布する乱数の場合、出力も同様に一様分布する。また、データF_S1107は、連結データ1103とデータC_S1104に依存しない。従って、データP_S1106同様、入力フォーム1022の入力情報に依存せず、毎回、データ値の異なるデータF_S1107を作成できる。

[0188] 図11Cは、本実施形態において、検索クライアント200が作成する連結データ1108のデータ構成を示すブロック図である。

[0189] 検索クライアント200の全体処理部211は、データP_S1106とデータF_S1107とを連結し、作成した連結データ1104と、データC_S1105とを基本演算部217へ

入力する処理を行う(S1109)。

[0190] 検索クライアント200の基本演算部217は、入力された連結データ1104と、データC_S1105とのビット毎の排他的論理和であるＸＯＲ算を計算し、その計算結果をデータD_S1110として出力する処理を行う(S1110)。

[0191] Ｓ1110の計算は、連結データ1103やデータC_S1105に依存しない、乱数であるデータP_S1106を用いている。従って、連結データ1103とデータC_S1105の関係が一意に定まる場合でも、毎回、データ値が異なる、データP_S1106を用いれば、異なるデータ値のデータD_S1110が得られる。

[0192] 検索クライアント200の全体処理部211は、データD_S1110とデータF_S1107とを連結したデータである連結データ1108と、秘密鍵記憶部250に記憶された秘密鍵251とを暗号化部212へ入力する処理を行う(S1111)。

[0193] 検索クライアント200の暗号化部212は、入力されたデータを暗号化し、暗号化したデータを、全体処理部211は、秘匿検索クエリ1111として検索クエリ記憶部230へ記憶する処理を行う(S1112)。

[0194] 秘匿検索クエリ1111は、暗号化部に入力された連結データが乱数とみなせるため、出力された秘匿検索クエリ1111も、同様に乱数とみなせる。そのため、検索クライアント200が、例え不正傍受可能なネットワーク400経由で、ＤＢサーバ300に送信しても、秘匿検索クエリ1111は安全である。

[0195] 秘匿検索クエリ1111は、連結データ1103やデータC_S1105に依存しない、乱数であるデータP_S1106とデータF_S1107とを用いており、毎回、異なるデータ値が得られる。その結果、データD_S1106とデータF_S1107とを連結した秘匿検索クエリ1111は、連結データ1103とデータC_R1105とは独立している。即ち、入力フォーム1022の入力情報に依存せず、毎回、データ値の異なる秘匿検索クエリ1111を作成できる。

[0196] なお、上記の処理手順は、固定されたものではなく、処理手順を変更してもよい。例えば、S1109とS1110の処理手順を変更し、S1109でデータC_S1105と、データP_S1106と、のXOR算を計算してから、S1110でデータF_S1107とデータD_S1110とを連結してもよい。同様に、他の処理手順を変更してもよい。

[0197] また、上記の各処理を担当する制御部210は固定されたものではなく、担当する制御部210を変更してもよい。例えば、S1105で、擬似乱数生成部214ではなく、圧縮関数部215に秘密鍵251を入力してもよい。

[0198] また、秘密検索クエリ1111のデータ構成を変更し、それに併せて処理を変更してもよい。例えば、全体処理部211がデータF_S1107と、秘密鍵記憶部250に記憶された秘密鍵251とを暗号化部212へ入力する処理を行い(S1111)、暗号化部が出力したデータと、データD_S1106とを、連結したデータを、秘密検索クエリ1111とみなしてもよい (S1112)。

[0199] 図１２は、本実施形態において、ネットワーク400を経由し、検索クライアント200が送信した秘密検索クエリ232を用い、ＤＢサーバ300がデータベース341を検索する処理を示すシーケンス図である。

[0200] 検索クライアント200は、入力部201を経由し、ユーザから、フォームへ入力された情報を一時情報記憶部280に記憶する処理を行う（Ｓ１２０１）。

[0201] 検索クライアント200は、入力部201を経由し、ユーザにより、検索ボタン1050が選択されたことを検知し、フォームに入力された情報を平文検索クエリ231として記憶部220へ記憶する処理を行う（Ｓ１２０２）。

[0202] 検索クライアント200は、制御部210により、秘密検索クエリ232を作成し、記憶部220へ記憶する処理を行う（Ｓ１２０３）。

[0203] 検索クライアント200は、通信部203からネットワーク400を経由し、属性233と秘密検索クエリ232を、ＤＢサーバ300へ送信する処理を行う（Ｓ１２０４）。

[0204] ＤＢサーバ300は、通信部303からネットワーク400を経由し、検索クライアント200が送信した属性233と秘密検索クエリ232を受信する処理を行う（Ｓ１２０５）。

[0205] ＤＢサーバ300は、制御部310により、属性233を用い、データベース341から、秘密検索クエリ332に関係する秘密登録データ902を検索する処理を行う（Ｓ１２０６）。

[0206] ＤＢサーバ300は、秘密検索クエリ332に該当する検索結果（属性901と秘密

登録データ902の一部を抜粋）を、通信部303からネットワーク400を経由し、検索サーバへ送信する処理を行う（Ｓ１２０７）。

[0207] 検索クライアント200は、通信部203からネットワーク400を経由し、ＤＢサーバ300が送信した秘匿検索クエリ232に該当する検索結果を受信する処理を行う（Ｓ１２０８）。

[0208] 検索クライアント200は、制御部210により、秘匿検索クエリ232に該当する検索結果から、平文登録データ272を復元する（S1209）。

[0209] 検索クライアント200は、出力部202を経由し、抽出した平文登録データ272を記憶部220に記憶する。また、抽出した平文登録データ272を、出力部202に表示する処理を行ってもよい（Ｓ１２１０）。

[0210] 本実施形態において、Ｓ１２０６で示した、ＤＢサーバ300の制御部310が秘匿登録データ902を検索する処理手順は、以下、S1301からS1318に従う。

[0211] なお、ＤＢサーバ300の全体処理部311は、受信した属性233に関係する、データベース341の属性901に関連付けられた秘匿登録データ902を検索対象とする。

[0212] 図９Ｂは、図９Ａに示した、構成図を用い、ＤＢサーバ300の記憶部320のデータベース記憶部340に記憶された、データベース341における、検索対象を例示した構成図である。

[0213] 例えば、受信した属性233が、氏名に関する情報である場合、図９Ｂの太線の実線枠が囲んだ部分が示すように、ＤＢサーバ300の全体処理部311は、データベース341の氏名に関係する属性901を、検索対象の秘匿登録データ902として扱う。

[0214] なお、以下、秘匿登録データ902を検索するS1301からS1318の処理手順は、検索対象である秘匿登録データ902の全て、または検索対象である秘匿登録データ902から任意に抽出した秘匿登録データ902、または一定数の秘匿登録データ902に対して、実施する。

[0215] 図１３Ａは、本実施形態において、ＤＢサーバ300が、通信部303から受信した秘匿検索クエリを復号化した、連結データ1301のデータ構成を示すブロ

ック図の例である。

[0216] また、図１３Ｂは、本実施形態において、ＤＢサーバ300が、データベース記憶部340に記憶した、データベース341における、秘匿登録データ1304のデータ構成を示すブロック図の例である。

[0217] また、図１３Ｃは、本実施形態において、ＤＢサーバ300が、連結データ1301を用い、秘匿登録データ1304を検索する過程において作成する連結データ1308のデータ構成を示すブロック図の例である。

[0218] また、図１３Ｄは、本実施形態において、ＤＢサーバ300が、連結データ1301を用い、秘匿登録データ1304を検索する過程において作成する連結データ1311のデータ構成を示すブロック図の例である。

[0219] 以下では、図１３Ａと、図１３Ｂと、図１３Ｃと、図１３Ｄとを用い、ＤＢサーバ300が、毎回、データ値の異なる連結データ1301を用いても、正しく秘匿登録データ1304を検索する処理手順を説明する。

[0220] ＤＢサーバ300の全体処理部311は、通信部303を用い、秘匿検索クエリ1300を受信する処理を行う。このとき、ＤＢサーバ300の全体処理部311は、秘匿検索クエリ1300を、検索クエリ記憶部330に記憶する。

[0221] ＤＢサーバ300の全体処理部311は、秘匿検索クエリ1300と、秘密鍵記憶部350に記憶された秘密鍵351とを復号化部313へ入力する処理を行う(S1301)。

[0222] ＤＢサーバ300の復号化部は、入力された秘匿検索クエリ1300を復号化し、連結データ1301を出力する処理を行う(S1302)。このとき、図１３Ａに示すように、連結データ1301は、ＤＢサーバ300の一時情報記憶部280に、（ｈ＋ｆ）ビットのバイナリ表現で構成されたデータとして記憶される。

[0223] ＤＢサーバ300の全体処理部311は、連結データ1301からデータD_S1302を取り出す処理を行う（S1303）。

[0224] S1303は、例えば、図１３Ａに示すように、ＤＢサーバ300が、全体処理部311が、連結データ1301から、データD_S1302に該当する最初のhビットを、抽出すればよい。

[0225] ＤＢサーバ300の全体処理部311は、データベース記憶部340に記憶されてい

る、データベース341にある秘匿登録データ1304を読み出し、秘匿登録データ1304から、データD_R1306を取り出す処理を行う（S1304）。

[0226] S1304は、例えば、図１３Ｂに示すように、ＤＢサーバ300が、全体処理部311が、秘匿登録データ1304から、データP_R1305に該当する最初のｒビットと、データG_R1307に該当する最後のｇビットとを取り除いたデータを、データD_R1306とみなして扱えばよい。

[0227] 図１３Ｃは、本実施形態において、ＤＢサーバ300が作成する連結データ1308のデータ構成を示すブロック図である。

[0228] 登録クライアント100がデータC_R705の確率的暗号化に利用したデータH_R707と、検索クライアント200がデータC_S1105の確率的暗号化に利用したデータP_S1106と、の相関関係が取れるかを、準同型関数部316を利用して検査する。

[0229] ＤＢサーバ300の全体処理部311は、データD_R711とデータD_S1302とを基本演算部317へ入力する処理を行う(S1305)。

[0230] 登録クライアント100の基本演算部117は、入力されたデータD_R1309とデータD_S1310とのビット毎の排他的論理和であるＸＯＲ算を計算し、その計算結果を連結データ1308として出力する処理を行う(S1306)。

[0231] S1305とS1306では、登録クライアント100の入力フォーム622に入力された情報を隠すためのデータH_R707と、検索クライアント200が入力フォーム1022に入力された情報を隠すためのデータP_S1106との関係式を導く。

[0232] 実際、S1306のxor算により、登録クライアント100と検索クライアント200の入力情報が等しい、即ち、データC_s705とデータC_R1105のデータ値が等しい場合、以下の式（6）が導ける。

$$D_s \text{ xor } D_R = P_S \text{ xor } H_R \quad (\text{ただし、} C_s = C_R \text{のとき}) \qquad (6)$$

図１３Ｄは、本実施形態において、ＤＢサーバ300が作成する連結データ1311のデータ構成を示すブロック図の例である。

[0233] ＤＢサーバ300の全体処理部311は、連結データ1308と、パラメータ記憶部360に記憶された関数パラメータ361とを準同型関数部316に入力する(S1307)。

[0234] ＤＢサーバ300の準同型関数部316は、入力されたデータを準同型の性質を有する関数の入力値とみなし、関数パラメータ361を用いて、関数計算の出力値をバイナリ列で表現した準同型関数値を出力する処理を行う。このとき、準同型関数値は、ＤＢサーバ300の一時情報記憶部380には、hビットのデータF_D1312として記憶される(S1308)。

$$F_D = F(P_S \text{ xor } H_R) = F_S \text{ xor } F_R \qquad (7)$$

なお、式(7)は、式(3)と、式（5）と、式（6）とより導ける。

[0235] ＤＢサーバ300の全体処理部311は、連結データ1301からデータF_S1303を取り出す処理を行う（S1309）。

[0236] S1309は、例えば、図１３Ａに示すように、ＤＢサーバ300が、全体処理部311が入力した連結データ1301から、データF_S1303に該当する最後のfビットを抽出すればよい。

[0237] ＤＢサーバ300の全体処理部311は、データF_D1312とデータF_S1303を、基本演算部317に入力する処理を行う(S1310)。

[0238] ＤＢサーバ300の基本演算部317は、入力されたデータF_D1312とデータF_S1303とのビット毎の排他的論理和であるＸＯＲ算を計算し、その計算結果をデータD_D1313として出力する処理を行う(S1311)。

[0239] データC_s705とデータC_R1105のデータ値が同じ、即ち、式（7）が成り立つ場合、S1311の処理は、式(8)に基づく。

$$D_R = F_D \text{ xor } F_S = F_R \qquad (8)$$

従って、データC_s705とデータC_R1105のデータ値が等しい場合、データD_R1313のデータ値はデータF_R708と等しい。

[0240] ＤＢサーバ300の全体処理部311は、データD_R1313を、圧縮関数部315へ入力する処理を行う(S1312)。

[0241] ＤＢサーバ300の圧縮関数部315は、入力されたデータを変換し、ハッシュ値を出力する処理を行う。このとき、ハッシュ値は、登録クライアント100の一時情報記憶部180には、ｇビットのデータG_D1314として記憶される(S1313)。

[0242] ＤＢサーバ300の全体処理部311は、データG_D1314とデータG_R1307を基本演算部317に入力する処理を行う(S1314)。

[0243] ＤＢサーバ300の基本演算部317は、入力されたデータG_D1314と、データG_R1307とのビット毎の排他的論理和であるＸＯＲ算を計算し、その計算結果をデータE_D1315として出力する(S1315)。

[0244] 式(5)が成り立つ場合、データG_D1314のデータ値はデータG_R1307と等しく、式(9)より、データE_D1315のデータ値は0になる。

$$G_D \text{ xor } G_S = 0 \qquad (9)$$

ＤＢサーバ300の全体処理部311は、任意の数だけ、データE_D1315のビット値が0であるかを判定する(S1316)。

[0245] S1316で調査したデータE_D1315のデータ値が0でない場合、ＤＢサーバ300の全体処理部311は、秘匿検索クエリ1300と秘匿登録データ1304の関係がないと判断する。このとき、検索対象である秘匿登録データ1304の全て、または検索対象である秘匿登録データ1304から任意に抽出した秘匿登録データ1304の全て、または検索した秘匿登録データ1304が一定数に達するまで、ＤＢサーバ300の制御部310は、S1304に戻り、秘匿登録データ1304を検索する処理を続ける(S1317)。

[0246] S1316で調査したデータE_D1315のデータ値が0である場合、ＤＢサーバ300の全体処理部311は、秘匿検索クエリ1300と秘匿登録データ1304の関係があると判断する。このとき、判断された秘匿登録データ1304と、関連する属性901に対応する秘匿登録データ1304とを、秘匿検索クエリ1300に該当する検索結果とみなす(S1318)。

[0247] 例えば、図９Ｂに示すように、検索結果は、検索した属性901が氏名に関する情報であり、秘匿検索クエリ1300に関係がある秘匿登録データ1304がd_{k+1}であるとＤＢサーバ300の全体処理部311が判断した場合、判断された秘匿登録データ1304であるd_{k+1}と、属性901が対応する図９Ｂの太枠の点線で囲まれた秘匿登録データ1304（d_k、d_{k+2}、d_{k+3}、・・・）を、秘匿検索クエリ1300に該当する検索結果とみなす。

[0248] 以上に示したように、登録クライアント100が、毎回、異なるデータ値を有する秘匿登録データ712を作成し、検索クライアント200が、毎回、異なるデータ値を有する秘匿検索クエリ1111を作成した場合にも、受信した秘匿検索クエリ1300に該当する秘匿登録データ1304を正しく検索できる。

[0249] また、式（6）に示したように、検索過程において、データC_s705とデータC_R1105のデータ値を互いに相殺しており、ＤＢサーバ300には、データC_s705とデータC_R1105のデータ値が漏洩しない。

[0250] なお、上記の処理手順は固定されたものではなく、処理手順を変更してもよい。例えば、S1303とS1305、S1304とS1306の処理手順をそれぞれ変更し、S1304でデータD_R1306を取り出し、S1306でデータD_S1302を取り出してもよい。同様に、他の処理手順を変更してもよい。

[0251] また、上記の各処理を担当する制御部310は固定されたものではなく、担当する制御部310を変更してもよい。例えば、ＤＢサーバ300が暗号化部312を備える場合、S1312でデータD_R1313を、圧縮関数部315ではなく、暗号化部312に入力してもよく、S1314では、暗号化部312から出力されたデータを、データG_D1314として一時情報記憶部380に記憶してもよい。

[0252] また、検索処理に該当する判定基準を変更してもよい。例えば、S1316において、データE_D1315の任意のビットが0と等しいのを判定するのではなく、変更可能な特定の値と、データE_D1315のデータ値との大小関係等の判定式を用いて判定するようにしてもよい。

[0253] また、秘匿検索クエリ1301に該当する、秘匿登録データ1304のデータ構成を変更し、検索結果を構成してもよい。例えば、データG_R1307に関する情報は、検索結果に含まないように構成しても構わない。

[0254] また、ＤＢサーバ300が擬似乱数生成部314を備えるならば、全体処理部311が擬似乱数生成部314に秘密鍵351を入力し、擬似乱数生成部314が出力した擬似乱数を、データG_R1307の代わりに連結したデータを、秘匿検索クエリ1301に該当する秘匿登録データ1304として、検索結果に含めてもよい。また、データG_R1307と擬似乱数を、共に秘匿検索クエリ1301に該当する秘匿登録デー

タ1304として、検索結果に含めてもよく、擬似乱数の代わりに、一般的なインデックスを用いてもよい。

[0255] また、ＤＢサーバ300が暗号化部313を備えるならば、全体処理部311が、秘匿検索クエリ1301に該当する秘匿登録データ1304と、秘密鍵351を暗号化部313に入力し、出力したデータを、検索結果とみなしてもよい。秘匿検索クエリ1301に該当する秘匿登録データ1304が擬似乱数または一般的なインデックスと連結されている場合、暗号化部313への入力値が随時異なるため、暗号化部313が出力するデータは、乱数とみなせる。従って、ＤＢサーバ300が、例え不正傍受可能なネットワーク400経由で、検索クライアント200に送信しても、検索結果は安全である。

[0256] 本実施形態において、S1209で示した、検索クライアント200の制御部210が、受信した秘匿登録データ1304の全てまたは一部に対する秘匿登録データ1304を復号し、平文登録データ272を抽出する処理手順は、以下、Ｓ1401からＳ1411の処理手順に従う。

[0257] 図１４Ａは、本実施形態において、検索クライアント200が、通信部203から受信した秘匿登録データ1401のデータ構成を示すブロック図の例である。

[0258] また、図１４Ｂは、本実施形態において、ＤＢサーバ300が、秘匿登録データ1401を復号化する過程において作成するデータC_R1405のデータ構成を示すブロック図の例である。

[0259] また、図１４Ｃは、本実施形態において、ＤＢサーバ300が、秘匿登録データ1401を復号化する過程において作成する連結データ1409のデータ構成を示すブロック図の例である。

[0260] 以下では、図１４Ａと、図１４Ｂと、図１４Ｃと、図１４Dとを用い、検索クライアント200が、秘匿登録データ1401から平文登録データ1410を復号化する処理手順を説明する。

[0261] 検索クライアント200の全体処理部211は、通信部203を用い、秘匿登録データ1401を受信する処理を行う。このとき、検索クライアント200は、登録データ1401を、検索クエリ記憶部230に、(r+h+g)ビットのバイナリ表現で構成さ

れたデータとして記憶する。

[0262] 検索クライアント200の全体処理部211は、秘匿登録データ1401からデータP_R1402を取り出す処理を行う(S1401)。

[0263] S1401は、例えば、図１４に示すように、検索クライアント200が、全体処理部211が入力した秘匿登録データ1401から、データP_R1402に該当する最初のｒビットを抽出すればよい。

[0264] 検索クライアント200の全体処理部211は、秘密鍵記憶部250から秘密鍵251を読み出し、秘密鍵251とデータP_R1402を圧縮関数部215に入力する処理を行う(S1402)。

[0265] 検索クライアント200の圧縮関数部215は、入力されたデータを変換し、ハッシュ値を出力する処理を行う(S1403)。このとき、ハッシュ値は、検索クライアント200の一時情報記憶部280には、ｈビットのデータH_S1407として記憶される。

[0266] 図１４Ｂは、本実施形態において、ＤＢサーバ300が作成するデータC_R1405のデータ構成を示すブロック図である。

[0267] 検索クライアント200の全体処理部211は、データD_R1403とデータH_S1407とを基本演算部217へ入力する処理を行う(S1404)。

[0268] 検索クライアント200の基本演算部217は、入力されたデータD_R1403とデータH_S1407とのビット毎の排他的論理和であるＸＯＲ算を計算し、その計算結果をデータC_R1405として出力する処理を行う(S1405)。

[0269] S1407のxor算では、データH_R1407とデータD_R1403とデータC_R1405とは式(10)を満たす。

$$C_R = H_R \text{ xor } D_R \qquad (10)$$

なお、式(10)は、式(4)を変形した数式である。

[0270] 検索クライアント200の全体処理部211は、基本演算部217が出力したデータと、秘密鍵記憶部250に記憶された秘密鍵251とを復号化部213へ入力する処理を行う(S1406)。

[0271] 検索クライアント200の復号化部は、入力されたデータC_R1405を復号化し

、連結データ1409を出力する処理を行う(S1407)。このとき、図１４Ｃに示すように、連結データ1409は、検索クライアント200の一時情報記憶部280に、（ｍ＋ｅ）ビットのデータとして記憶される。

[0272] 検索クライアント200の全体処理部211は、連結データ1409から誤り検査データ1411を取り出す処理を行う(S1408)。

[0273] 例えば、図１４Ｃに示すように、検索クライアント200が、全体処理部211が入力した連結データ1403から、データ終わりのｅビットを誤り検査データ1411とみなし抽出すればよい。

[0274] 検索クライアント200の全体処理部211は、パラメータ記憶部260に記憶された検査パラメータ262を読み込み、検査用のデータに変換したデータと、誤り検査データ1411とを基本演算部217へ入力する処理を行う(S1409)。

[0275] 検索クライアント200の基本演算部217は、入力された、検査用に変換されたデータと、誤り検査データ1411を比較し、その比較結果を出力する処理を行う(S1410)。

[0276] 例えば、バイナリ列で表わされた検査用のデータと誤り検査データが等しければ、等号を表わすビット（１）を出力し、等しくない場合は、不等号を表わすビット（０）を出力する処理を行う。

[0277] 例えば、基本演算部217が、等号を表わすビット（１）を出力した場合は、検索クライアント200の全体処理部211は、正しい検索結果であると判断する処理を行う。また、基本演算部217が、不等号を表わすビット（０）を出力した場合は、ＤＢサーバ300の全体処理部311は、誤った検索結果であると判断する処理を行う。

[0278] 検索クライアント200の全体処理部211は、基本演算部217が出力した結果に応じ、連結データ1402から抽出した平文登録データ1410を検索結果とする処理を行い、平文登録データ1410を復元する処理（S1209）を終了する(S1411)。例えば、図１４Ｃに示すように、検索クライアント200が、全体処理部211が入力した連結データ1409から、データ初めのｍビットを平文登録データ1410とみなす。

[0279] なお、ＤＢサーバ300の不正対策に万全を期したい場合、検索に該当した検索結果はＤＢサーバ300から削除し、復号化した平文登録データ1410の順番をランダムにシャッフルした後、検索クライアント200または登録クライアント100から、ＤＢサーバ300に秘匿登録データを再登録するように処理してもよい。

符号の説明

[0280] １００：登録クライアント、２００：検索クライアント、３００：ＤＢサーバ、４００：ネットワーク、５００：コンピュータ、１０１、２０１、３０１：入力部、１０２、２０２、３０２：出力部、１０３、２０３、３０３：通信部、１１０、２１０、３１０：制御部、１１１、２１１、３１１：全体処理部、１１２、２１２：暗号化部、２１３、３１３：復号化部、１１４、２１４：擬似乱数生成部、１１５、２１５、３１５：圧縮関数部、１１６、２１６、３１６：準同型関数部、１１７、２１７、３１７：基本演算部、１２０、２２０、３２０：記憶部、１３０：登録データ記憶部、１３１、２７２、７０１、１４１０：平文登録データ、１３２、２７１、７１２、１３０４、１４０１：秘匿登録データ、１３３、２３３：属性、２３０、３３０：検索クエリ記憶部、２３１、１１０１：平文検索クエリ、２３２、３３２、１１１１、１３００：秘匿検索クエリ、３４０：データベース記憶部、３４１：データベース、１５０、２５０、３５０：秘密鍵記憶部、１５１、２５１、３５１：秘密鍵、１６０、２６０、３６０：パラメータ記憶部、１６１、２６１、３６１：関数パラメータ、１６２、２６２：検査パラメータ、２７０：受信データ記憶部、１８０、２８０、３８０：一時情報記憶部、５０１：ＣＰＵ(Central Processing Unit)、５０２：メモリ、５０３：外部記憶装置、５０８：記憶媒体、５０７：読書装置、５０６：入力装置、５０５：出力装置、５０４：通信装置、５０９：内部通信線、６００：出力部１０１の表示内容、６１０：管理方法の選択部、６２０：管理フォーム部、６２１、１０１１：属性、６２２、１０２２：入力フォーム、６５０：実行ボタン、６６０、１０６０：クリアボタン、１０００：出力部１０２の表示内容

、１０１０：検索項目部、１０２０：検索フォーム部、１０５０：検索ボタン、７０２、１４１１：誤り検査データ、７０３、７０４、１１０３、１１０４、１１０８、１３０１、１３０８、１３１１、１４０９：連結データ、７０５：データC_R、７０６：データP_R、７０７：データH_R、７０８：データF_R、７０９：データG_R、７１１：データD_R、１１０２：誤り検査データ、１１０５：データC_S、１１０６：データP_S、１１０７：データF_S、１１１０：データD_S、１３０２：データD_S、１３０３：データF_S、１３０５：データP_R、１３０６：データD_R、１３０７：データG_R、１３０９：データD_R、１３１０：データD_S、１３１２：データF_D、１３１３：データD_D、１３１４：データG_D、１３１５：データE_D、１４０２：データP_R、１４０３：データD_R、１４０４：データG_R、１４０５：データC_R、１４０７：データH_S。

請求の範囲

［請求項1］ 確率的暗号化方式により暗号化された登録データを記憶するＤＢサーバと、

検索クライアントとを含み、

前記検索クライアントから受信した、前記ＤＢサーバが記憶するデータの検索を要求する検索クエリに従い、前記ＤＢサーバが記憶する前記データの暗号化を解除せずに、検索する検索可能暗号処理システムであって、

前記確率的暗号化方式は、同一のデータ値の平文から異なるデータ値の暗号文を生成するデータの暗号化方式であり、

前記検索クライアントは、前記検索クエリを記憶する記憶部と、前記検索クエリを暗号化する制御部と、暗号化した前記検索クエリを送信する通信部とを備え、

前記検索クライアントにおける前記制御部は、第1の乱数を生成する乱数生成部と、前記第1の乱数により前記検索クエリを前記確率的暗号化方式で暗号化する基本演算部と、前記第1の乱数を入力値とする準同型関数の関数値を出力値とする準同型関数部とを備え、

前記検索クライアントにおける前記制御部は、前記準同型関数部が出力した前記関数値を変換し、ハッシュ値を出力する圧縮関数部を備え、

前記ＤＢサーバは、前記検索クエリを受信する通信部と、暗号化された前記検索クエリと暗号化された前記登録データを記憶する記憶部と、記憶する前記登録データが前記検索クエリに該当するかを決定する制御部とを備え、

前記ＤＢサーバにおける前記制御部は、暗号化された前記登録データと暗号化された前記検索クエリとの乱数の相関を導出する全体処理部と、前記相関を入力値とする準同型関数の関数値を出力値とする準同型関数部とを備え、

前記検索クライアントが送信する暗号化された前記検索クエリは、前記基本演算部により、前記確率的暗号化方式で暗号化された暗号文と、前記圧縮関数部が出力する前記ハッシュ値から構成されるデータが暗号化されていることを特徴とする検索可能暗号処理ステム。

［請求項2］ 確率的暗号化方式により、暗号化された登録データを記憶するＤＢサーバと、

検索クライアントとを含み、

前記検索クライアントから受信した、前記ＤＢサーバが記憶するデータの検索を要求する検索クエリに従い、前記ＤＢサーバが記憶する前記データの暗号化を解除せずに、検索する検索可能暗号処理システムであって、

前記確率的暗号化方式は、同一のデータ値の平文から異なるデータ値の暗号文を生成するデータの暗号化方式であり、

前記検索クライアントは、前記検索クエリを記憶する記憶部と、前記検索クエリを暗号化する制御部と、暗号化した前記検索クエリを送信する通信部とを備え、

前記検索クライアントにおける前記制御部は、乱数を生成する乱数生成部と、前記乱数により前記検索クエリを前記確率的暗号化方式で暗号化する基本演算部と、前記乱数を入力値とする準同型関数の関数値を出力値とする準同型関数部とを備え、

前記ＤＢサーバは、前記検索クエリを受信する通信部と、暗号化された前記検索クエリと暗号化された前記登録データを記憶する記憶部と、記憶する前記登録データが前記検索クエリに該当するかを決定する制御部とを備え、

前記ＤＢサーバにおける前記制御部は、暗号化された前記登録データと、暗号化された前記検索クエリとの乱数の相関を導出する全体処理部と、前記相関を入力値とする準同型関数の関数値を出力値とする準同型関数部とを備え、

前記検索クライアントが送信する暗号化された前記検索クエリは、前記基本演算部により、前記確率的暗号化方式で暗号化された前記データと、前記準同型関数部が出力した前記関数値から構成されるデータが暗号化されることを特徴とする検索可能暗号処理ステム。

[請求項3] 請求項１記載の検索可能暗号処理システムであって、

、前記確率的暗号化方式により、前記登録データを暗号化する登録クライアントを有し、

前記ＤＢサーバの前記通信部は、暗号化した前記登録データを受信し、前記ＤＢサーバの前記記憶部は前記登録データを記憶し、

前記登録クライアントは、前記登録データを記憶する記憶部と、前記登録データを暗号化する制御部と、暗号化した前記登録データを送信する通信部とを備え、

前記登録クライアントにおける前記制御部は、第２の乱数を生成する乱数生成部と、前記第２の乱数により前記登録データを前記確率的暗号化方式で暗号化する基本演算部と、前記第２の乱数を入力値とする準同型関数の関数値を出力値とする準同型関数部と、を備えることを特徴とする検索可能暗号処理ステム。

[請求項4] 請求項３記載の検索可能暗号処理システムであって、

前記登録クライアントが送信する暗号化された前記登録データは、前記乱数部が出力した前記第２の乱数と、前記基本演算部により前記確率的暗号化方式で暗号化された暗号文と、前記準同型関数部が出力する前記関数値から構成されることを特徴とする検索可能暗号処理システム。

[請求項5] 請求項４記載の検索可能暗号処理システムであって、

前記ＤＢサーバの前記通信部は、前記検索クエリに該当する、暗号化された前記登録データを送信し、

前記検索クライアントの前記通信部は、暗号化された前記登録データを受信し、前記検索クライアントの前記制御部は、前記登録データ

を復号化し、

前記検索クライアントの前記制御部は、暗号化された前記登録データを暗号化した第３の乱数を出力する圧縮関数部を備え、前記検索クライアントの前記基本演算部は、前記登録データの暗号化を解除することを特徴とする検索可能暗号処理ステム。

［請求項6］ 請求項５記載の検索可能暗号処理システムであって、

前記ＤＢサーバの前記基本演算部は、前記登録データから任意のデータを抽出し、前記圧縮関数部が出力した前記第３の乱数から、指定されたデータ長分を検査することを特徴とする検索可能暗号処理ステム。

［請求項7］ 請求項６記載の検索可能暗号処理システムであって、

前記登録クライアントの前記記憶部は、前記登録クライアントの前記準同型関数部に入力可能な関数パラメータを記憶し、

前記検索クライアントの前記記憶部は、前記検索クライアントの前記準同型関数部に入力可能な関数パラメータを記憶し、

前記ＤＢサーバの前記記憶部は、前記ＤＢサーバの前記準同型関数部に入力可能な関数パラメータを記憶することを特徴とする検索可能暗号処理システム。

［請求項8］ 請求項７記載の検索可能暗号処理システムであって、

前記検索クライアントの前記記憶部は、暗号化を解除した前記登録データの検査用のパラメータを記憶し、

前記検索クライアントは、暗号化を解除した前記登録データから検査用のデータを抽出し、前記検査用のパラメータとの関係を検査する全体処理部を備えることを特徴とする検索可能暗号処理ステム。

［請求項9］ 請求項８記載の検索可能暗号処理システムであって、

前記登録クライアントは、前記登録データを決定的暗号化方式で暗号化する暗号化部を備え、

前記決定的暗号化方式は、同一のデータ値の平文からデータ値が等

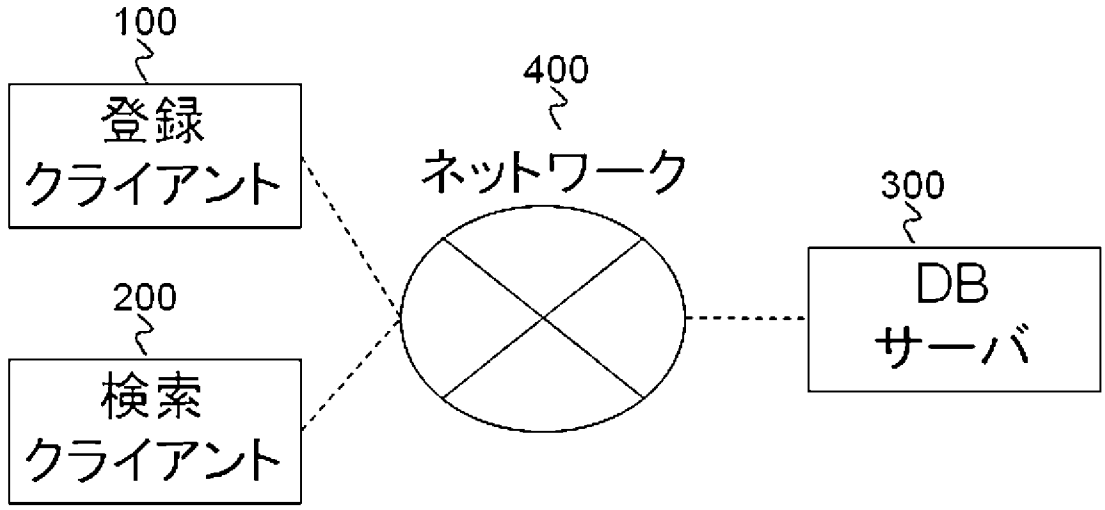
しい暗号文を生成するデータの暗号化方式であることを特徴とする検索可能暗号処理ステム。

［請求項10］ 請求項９記載の検索可能暗号処理システムであって、

前記登録クライアントの前記記憶部は、暗号化されていない、登録用のデータを記憶し、前記登録クライアントの前記記憶部に記憶した検査用のパラメータから、誤り検査用のデータを抽出し、前記登録用のデータと結合させる全体制御部を備えることを特徴とする検索可能暗号処理ステム。

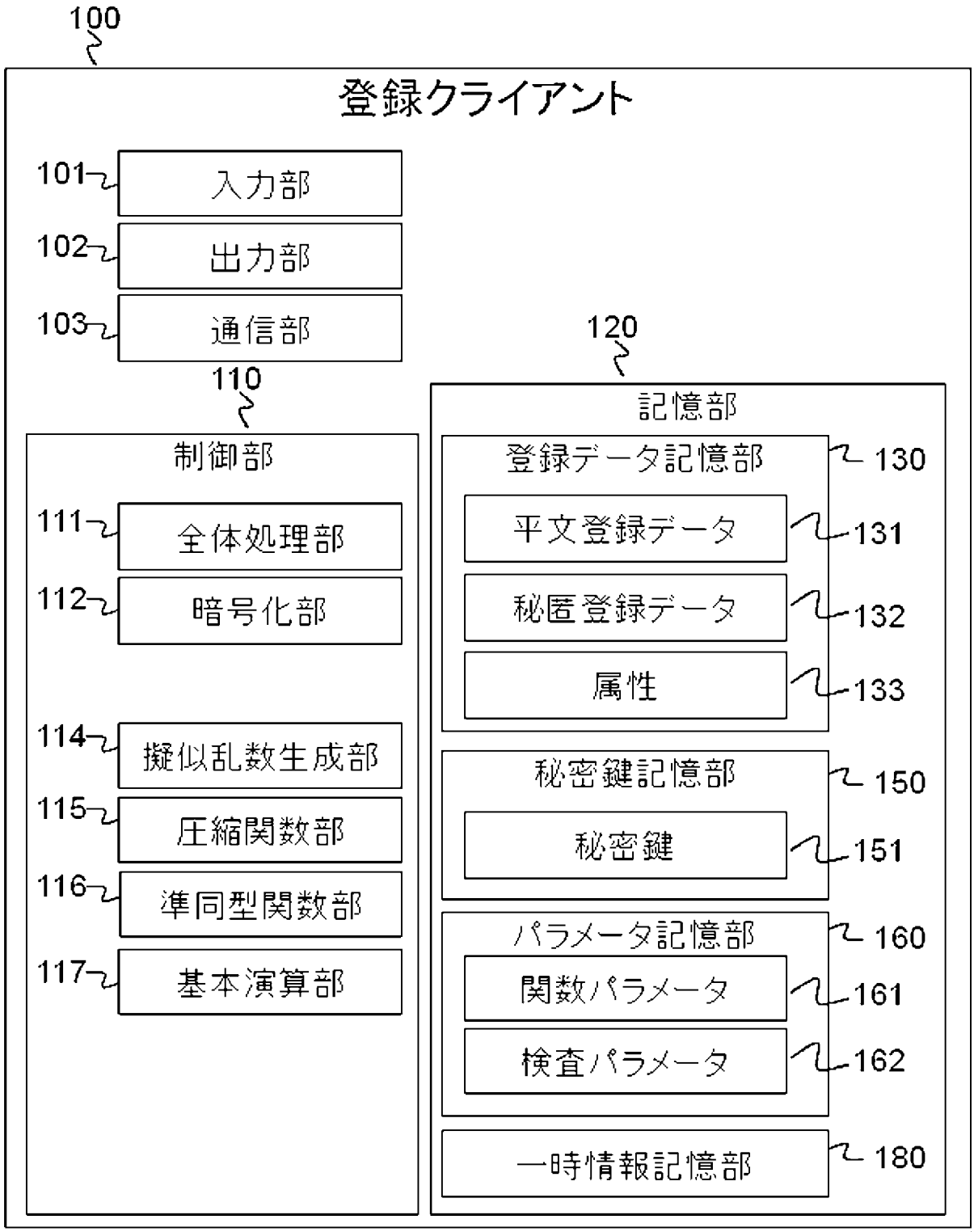
[図1]

図1



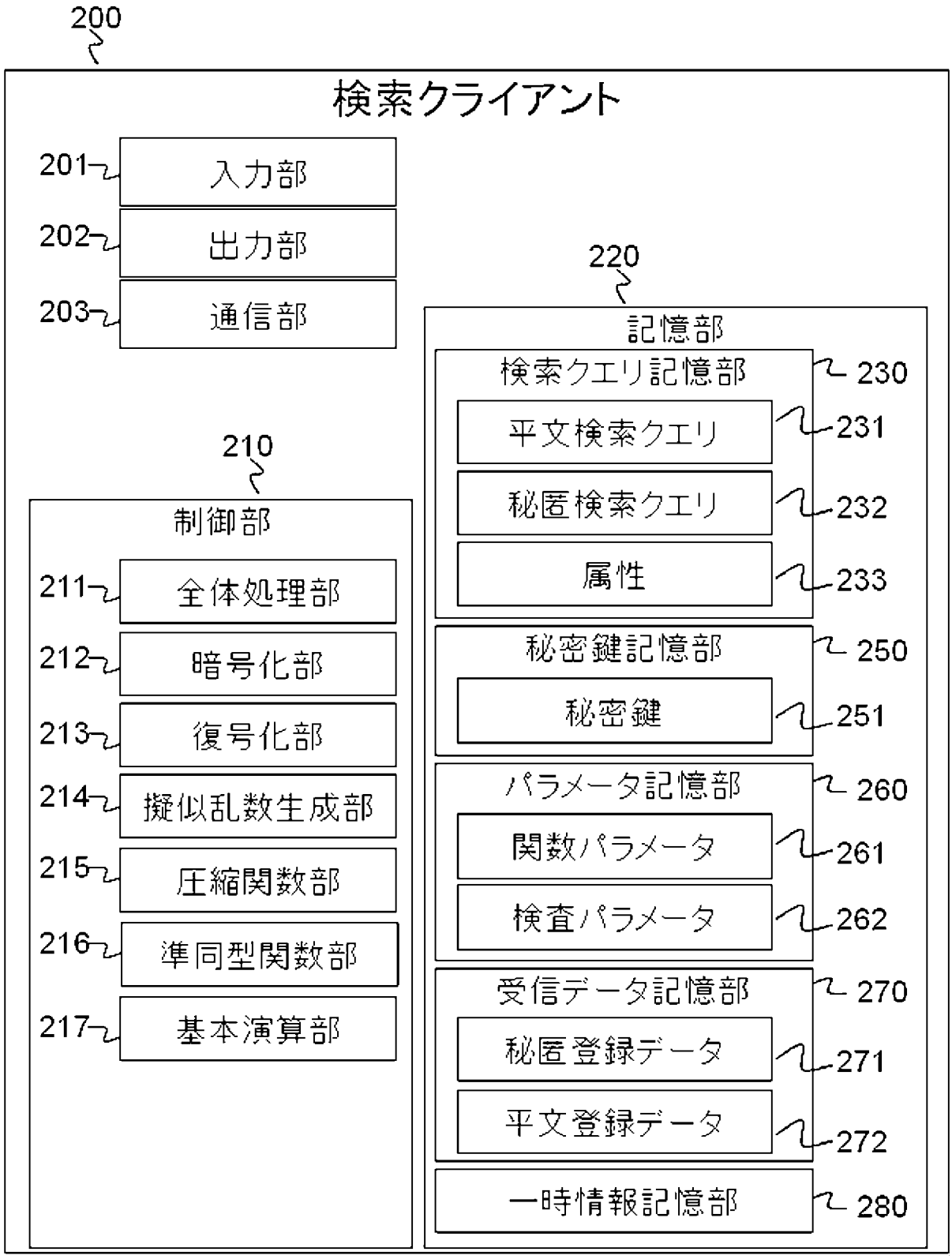
[図2]

図2


100
登録クライアント
101
入力部
102
出力部
103
通信部
110
制御部
111
全体処理部
112
暗号化部
114
擬似乱数生成部
115
圧縮関数部
116
準同型関数部
117
基本演算部
120
記憶部
登録データ記憶部
130
平文登録データ
131
秘匿登録データ
132
属性
133
秘密鍵記憶部
150
秘密鍵
151
パラメータ記憶部
160
関数パラメータ
161
検査パラメータ
162
一時情報記憶部
180

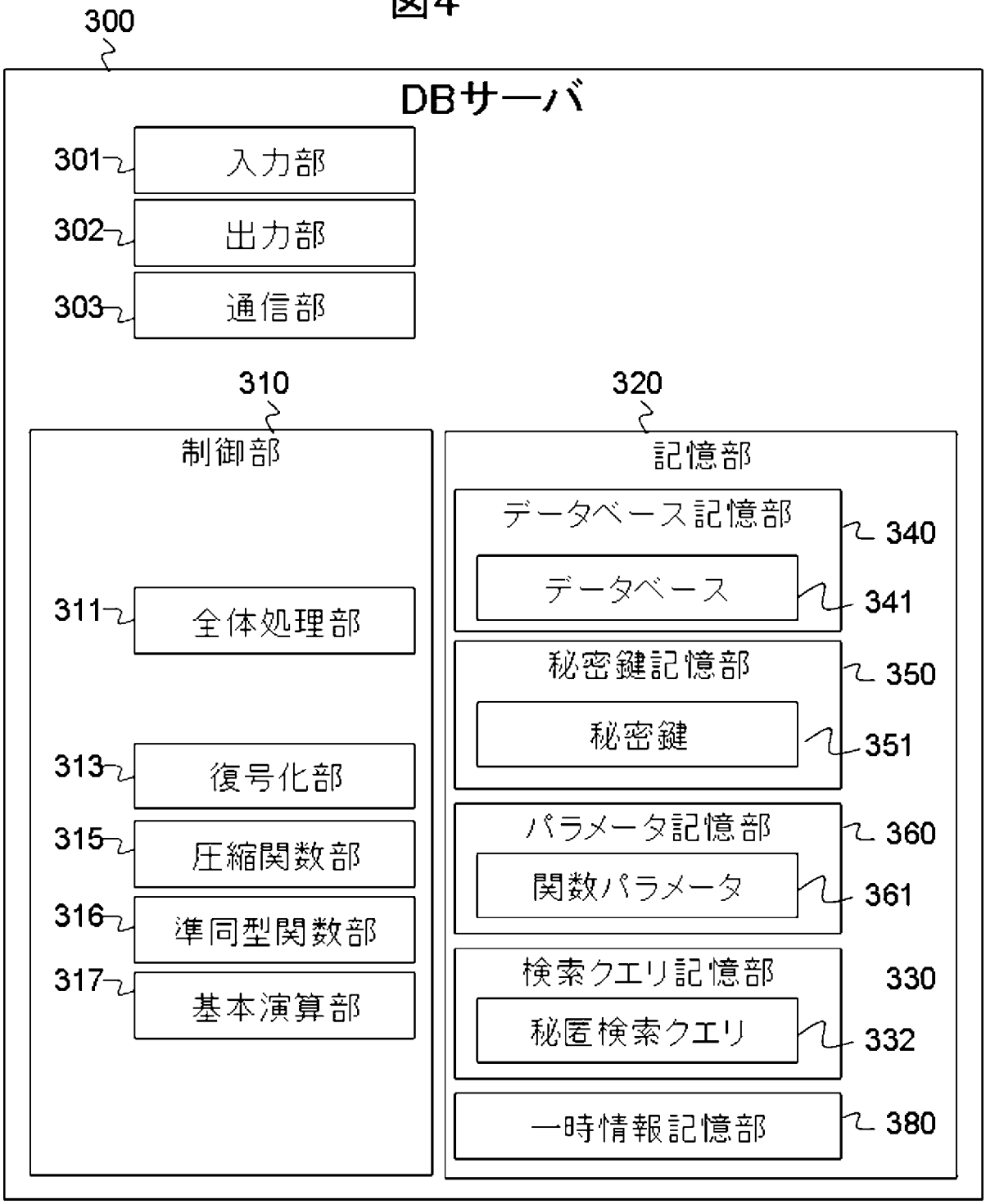
[図3]

図3


200
検索クライアント
201
入力部
202
出力部
203
通信部
210
制御部
211
全体処理部
212
暗号化部
213
復号化部
214
擬似乱数生成部
215
圧縮関数部
216
準同型関数部
217
基本演算部
220
記憶部
検索クエリ記憶部
230
平文検索クエリ
231
秘匿検索クエリ
232
属性
233
秘密鍵記憶部
250
秘密鍵
251
パラメータ記憶部
260
関数パラメータ
261
検査パラメータ
262
受信データ記憶部
270
秘匿登録データ
271
平文登録データ
272
一時情報記憶部
280

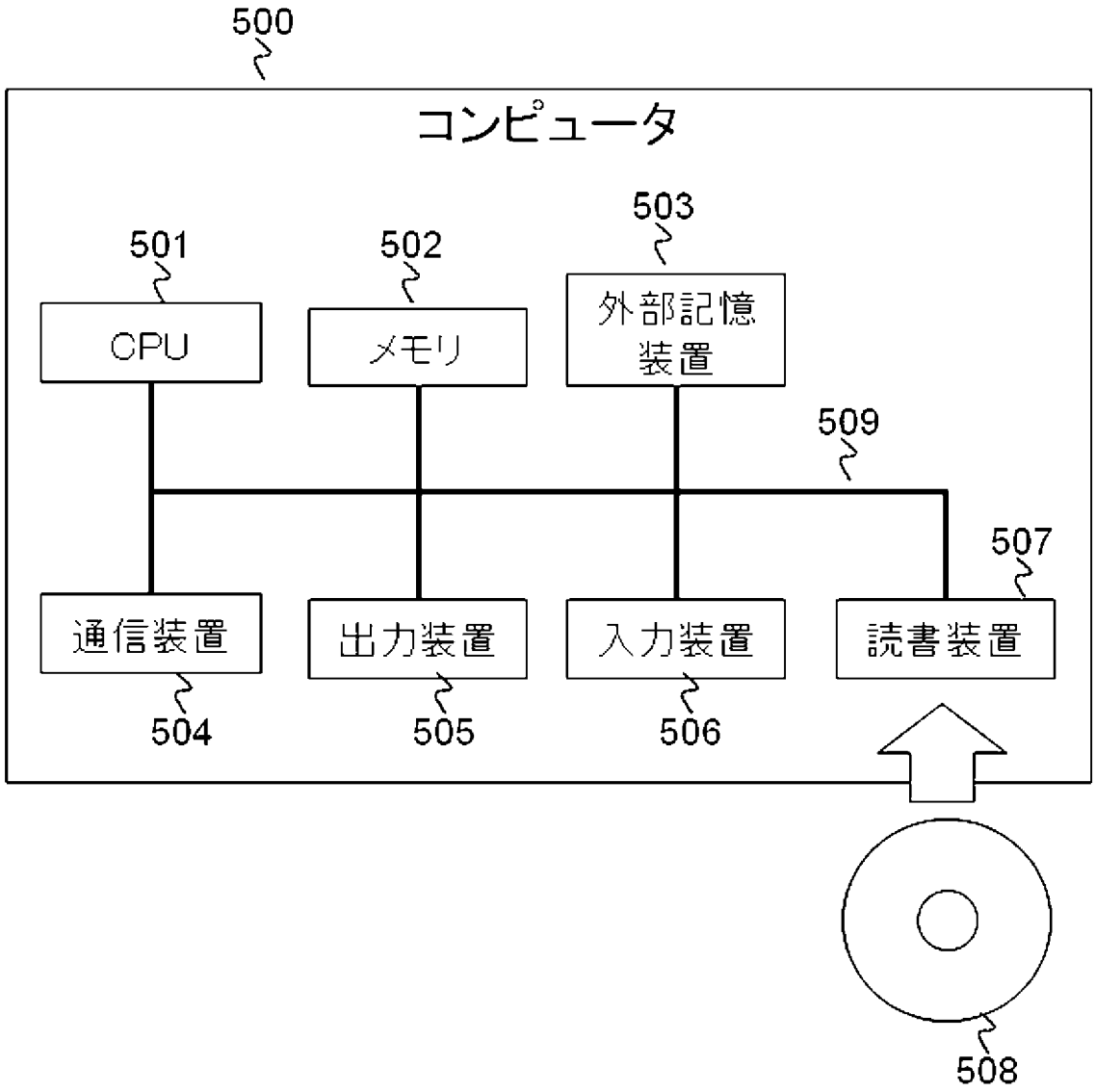
[図4]

図4


300
DBサーバ
301
入力部
302
出力部
303
通信部
310
制御部
311
全体処理部
313
復号化部
315
圧縮関数部
316
準同型関数部
317
基本演算部
320
記憶部
データベース記憶部
340
データベース
341
秘密鍵記憶部
350
秘密鍵
351
パラメータ記憶部
360
関数パラメータ
361
検索クエリ記憶部
330
秘匿検索クエリ
332
一時情報記憶部
380

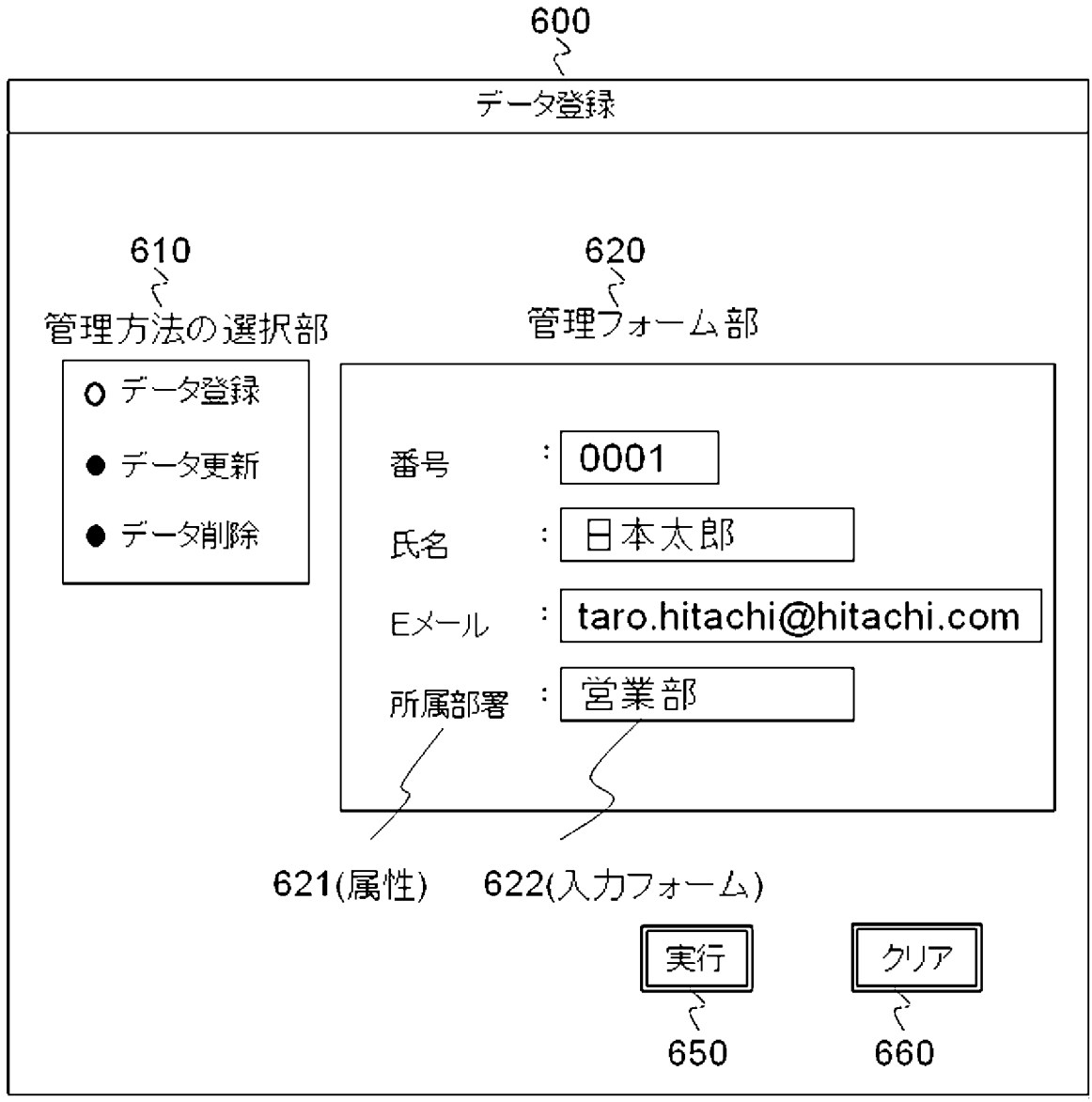
[図5]

図5


500
コンピュータ
501
CPU
502
メモリ
503
外部記憶装置
509
507
通信装置
出力装置
入力装置
読書装置
504
505
506
508

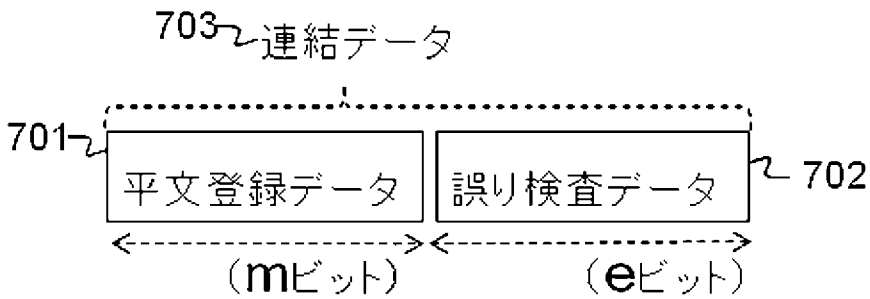
[図6]

図6


600
データ登録
610
管理方法の選択部
620
管理フォーム部
データ登録
データ更新
データ削除
番号 : 0001
氏名 : 日本太郎
Eメール : taro.hitachi@hitachi.com
所属部署 : 営業部
621(属性)
622(入力フォーム)
実行
クリア
650
660

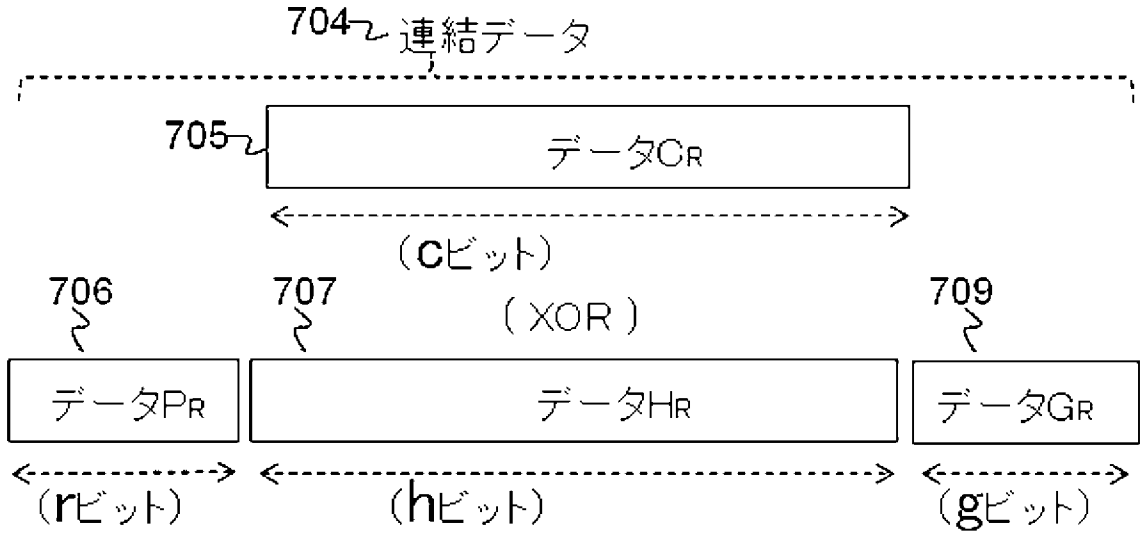
[図7A]

図7A


703
連結データ
701
平文登録データ
誤り検査データ
702
(mビット)
(eビット)

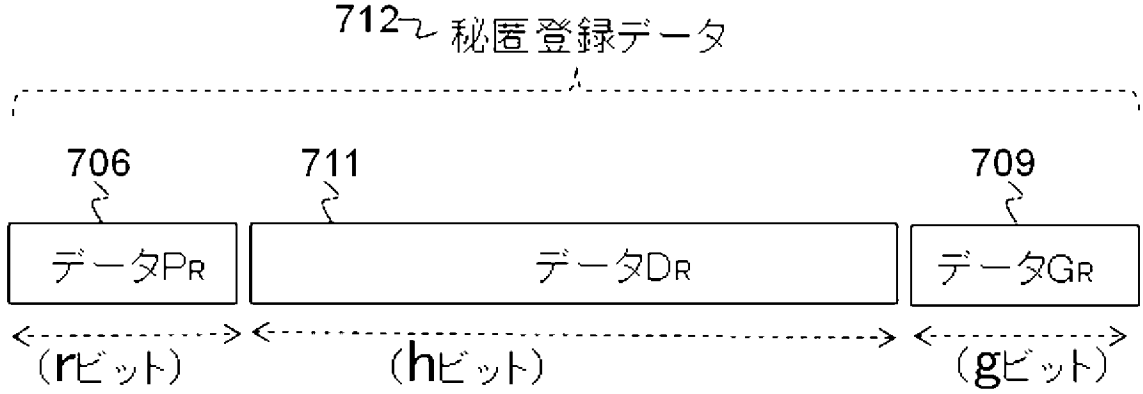
[図7B]

図７Ｂ



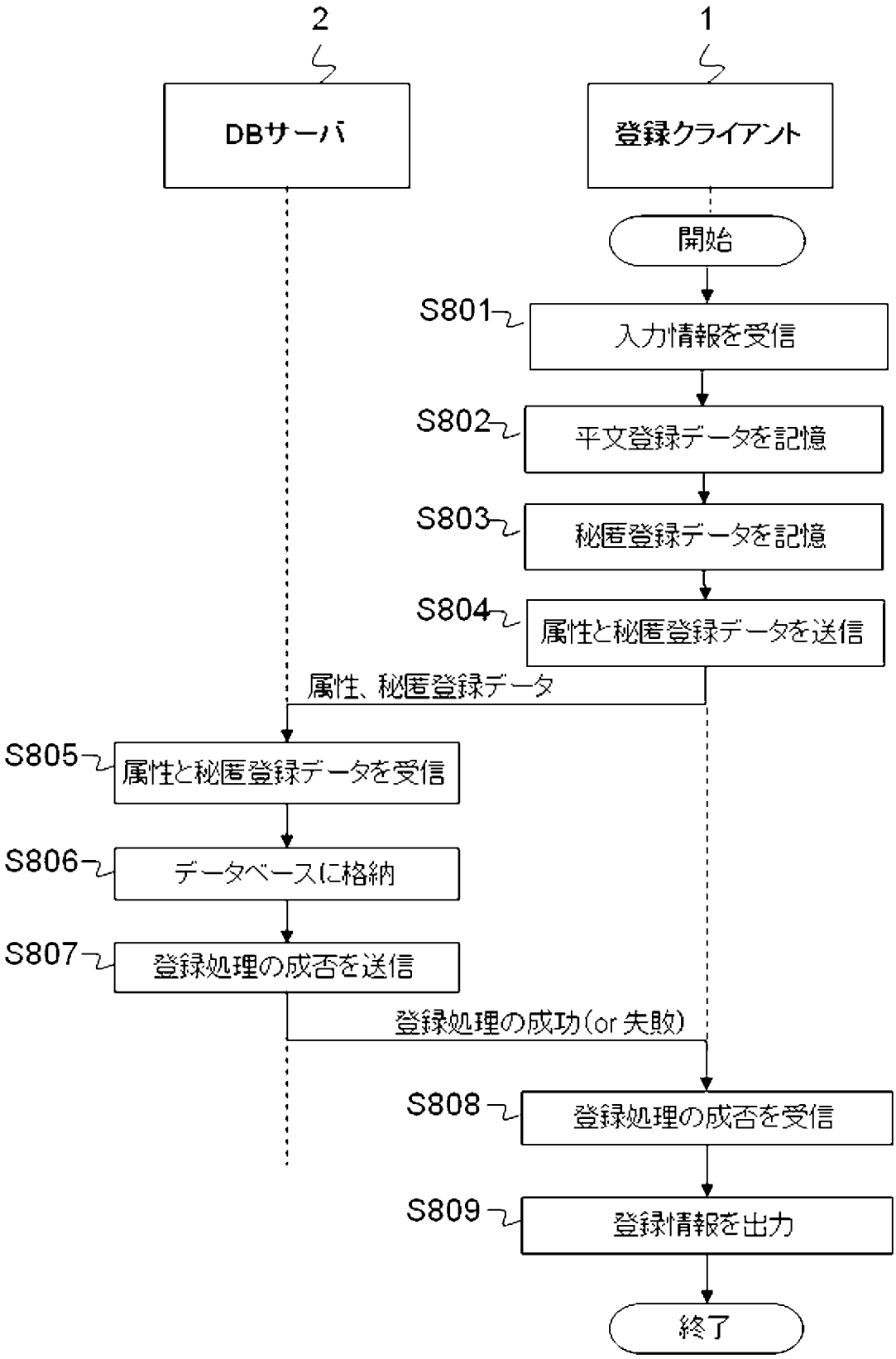
[図7C]

図７Ｃ



[図8]

図8


2
1
DBサーバ
登録クライアント
開始
S801
入力情報を受信
S802
平文登録データを記憶
S803
秘匿登録データを記憶
S804
属性と秘匿登録データを送信
属性、秘匿登録データ
S805
属性と秘匿登録データを受信
S806
データベースに格納
S807
登録処理の成否を送信
登録処理の成功(or 失敗)
S808
登録処理の成否を受信
S809
登録情報を出力
終了

[図9A]

図９Ａ

901(属性)

902
(秘匿登録
データ)

番号	氏名	Eメール	部署	・・・	・・・
d_0	d_1	d_2	d_3	・・・	d_{k-1}
d_k	d_{k+1}	d_{k+2}	d_{k+3}	・・・	d_{2k-1}
d_{2k}	d_{2k+1}	d_{2k+2}	d_{2k+3}	・・・	d_{3k-1}
d_{3k}	d_{3k+1}	d_{3k+2}	d_{3k+3}	・・・	d_{4k-1}
・・・	・・・	・・・	・・・	・・・	・・・

[図9B]

図９Ｂ

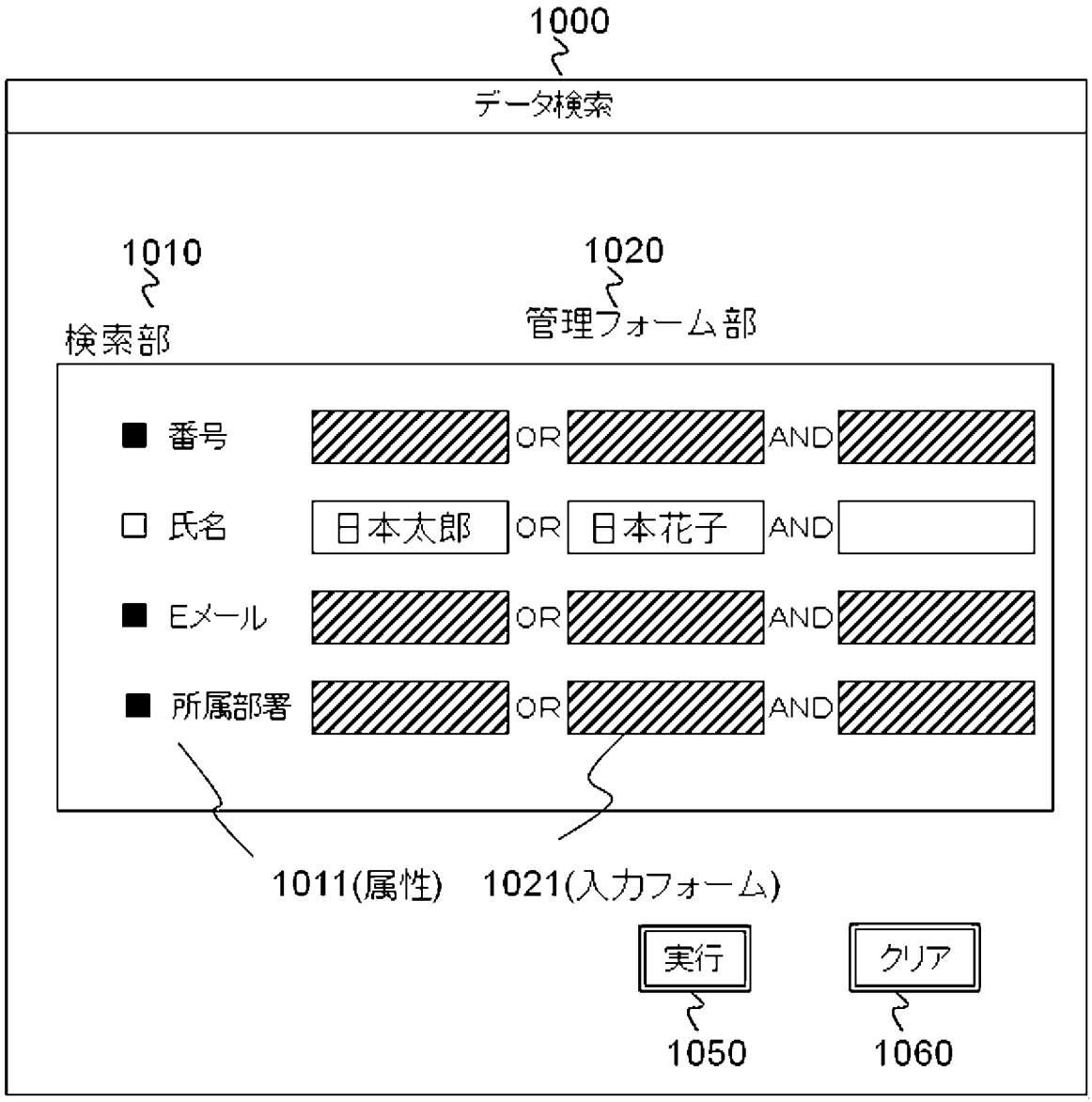
901(属性)

902
(秘匿登録
データ)

番号	氏名	Eメール	部署	・・・	・・・
d_0	d_1	d_2	d_3	・・・	d_{k-1}
d_k	d_{k+1}	d_{k+2}	d_{k+3}	・・・	d_{2k-1}
d_{2k}	d_{2k+1}	d_{2k+2}	d_{2k+3}	・・・	d_{3k-1}
d_{3k}	d_{3k+1}	d_{3k+2}	d_{3k+3}	・・・	d_{4k-1}
・・・	・・・	・・・	・・・	・・・	・・・

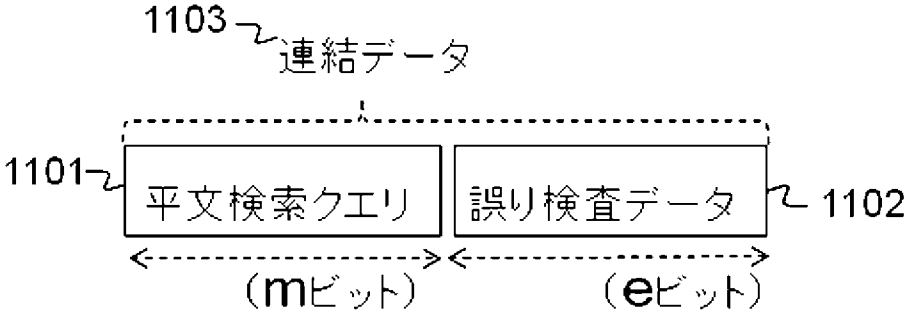
[図10]

図10



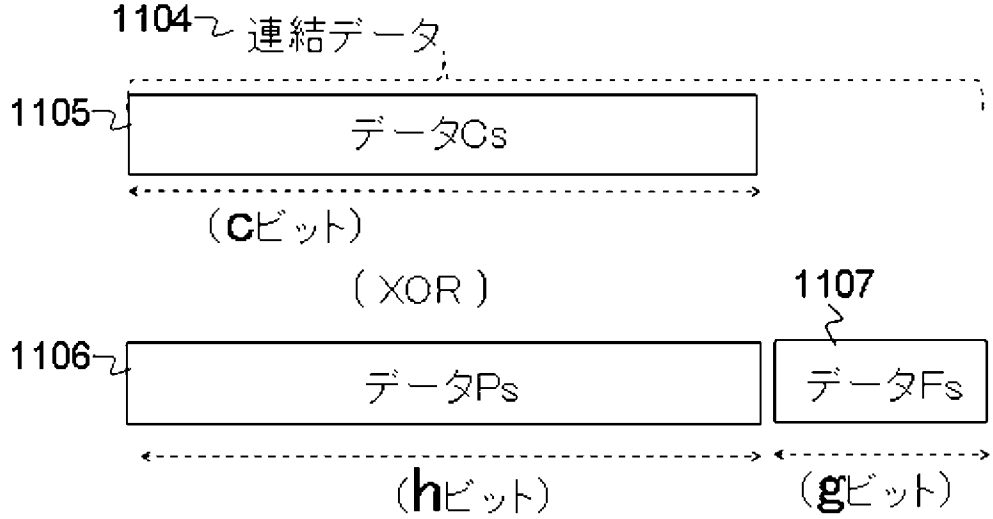
[図11A]

図11A



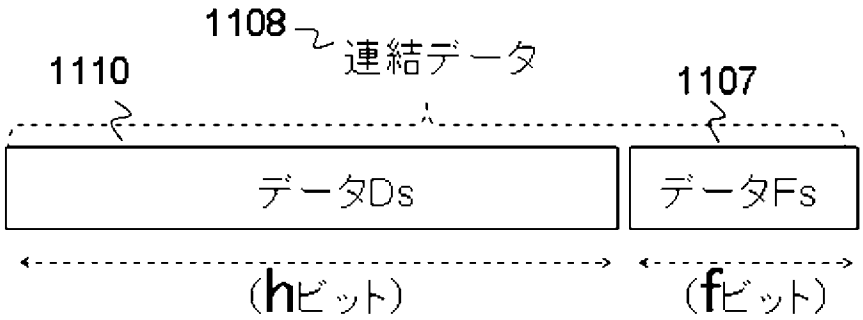
[図11B]

図11B



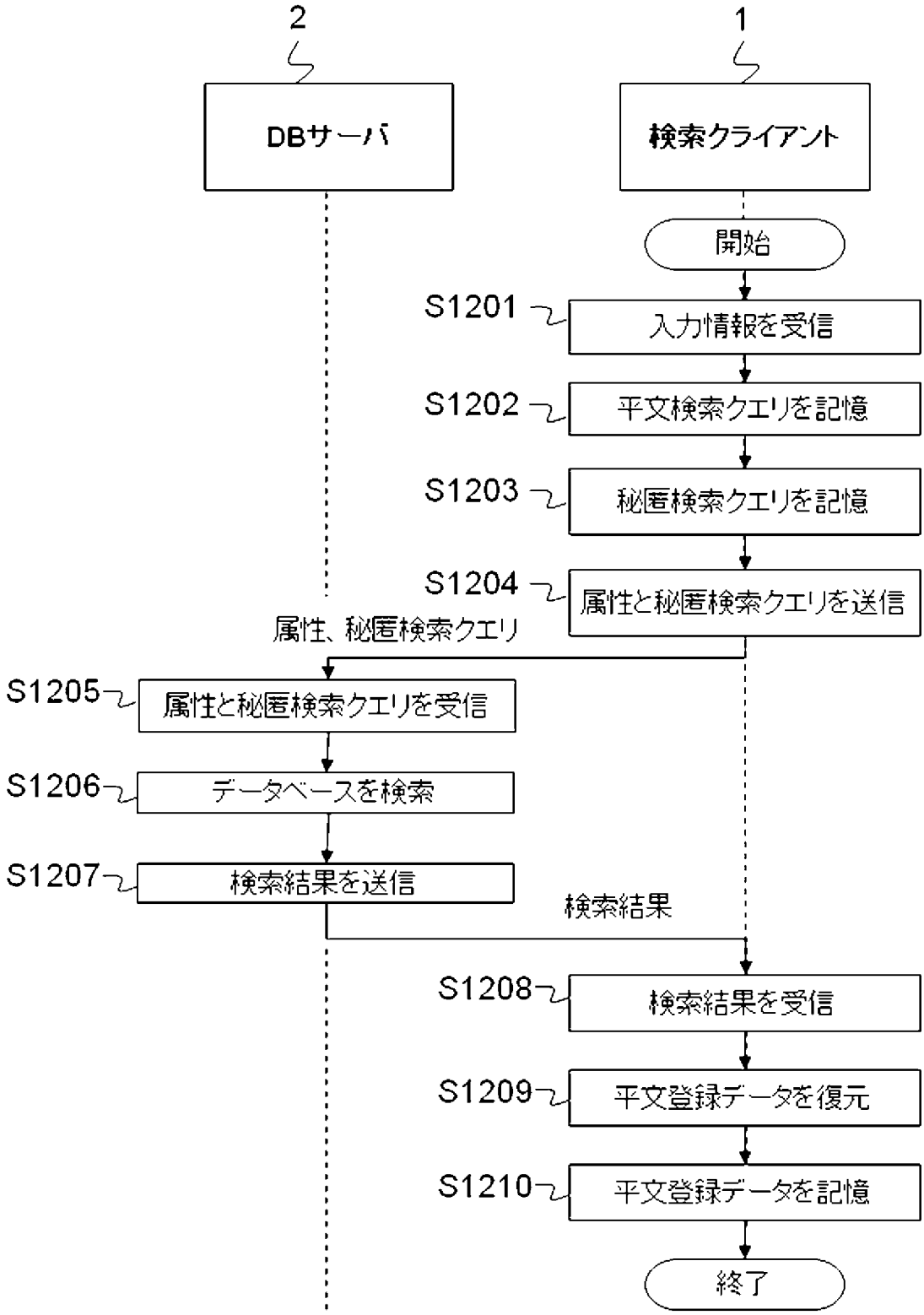
[図11C]

図11C



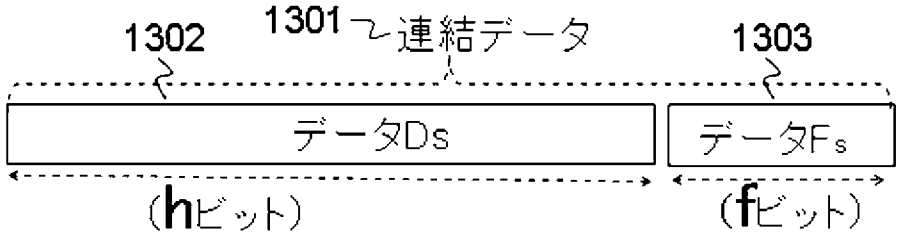
[図12]

図12


2
1
DBサーバ
検索クライアント
開始
S1201
入力情報を受信
S1202
平文検索クエリを記憶
S1203
秘匿検索クエリを記憶
S1204
属性と秘匿検索クエリを送信
属性、秘匿検索クエリ
S1205
属性と秘匿検索クエリを受信
S1206
データベースを検索
S1207
検索結果を送信
検索結果
S1208
検索結果を受信
S1209
平文登録データを復元
S1210
平文登録データを記憶
終了

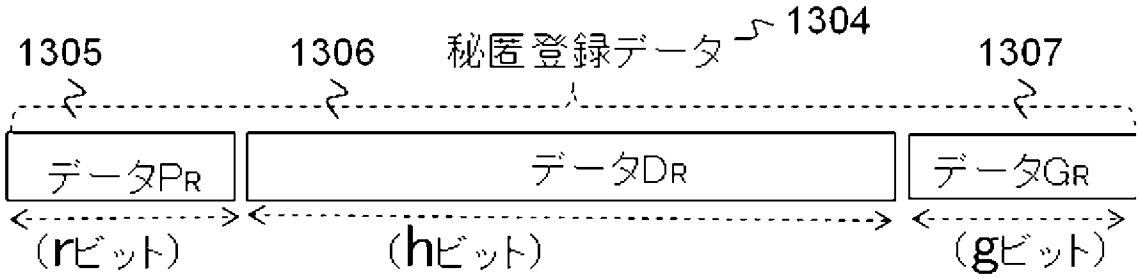
[図13A]

図13A



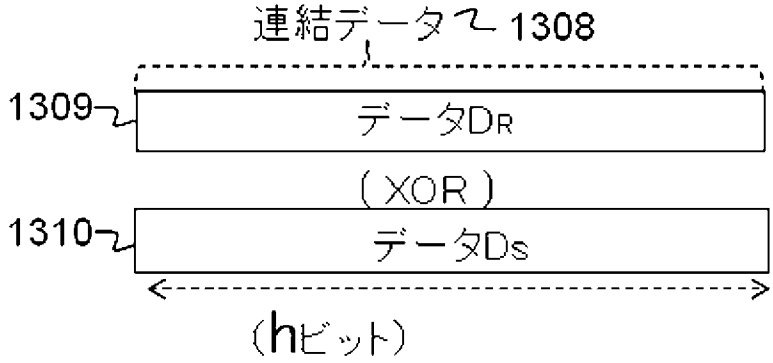
[図13B]

図13B



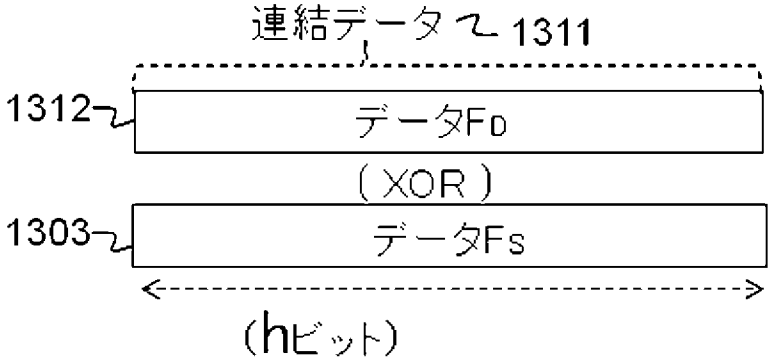
[図13C]

図13C



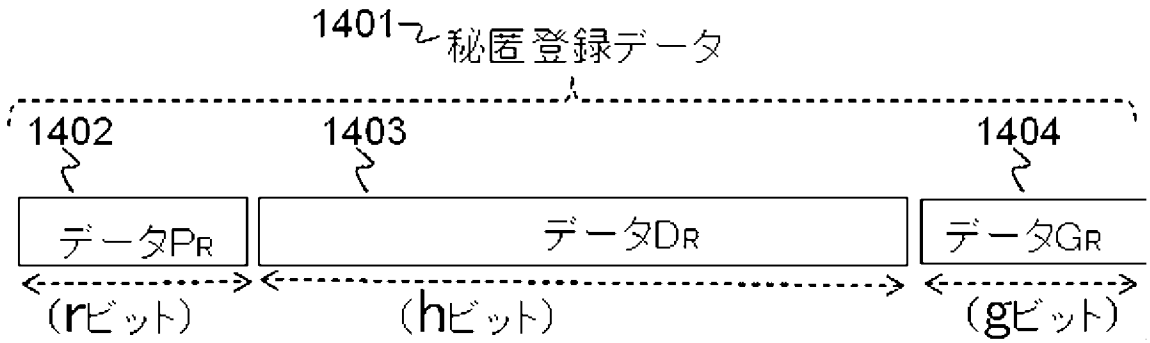
[図13D]

図13D



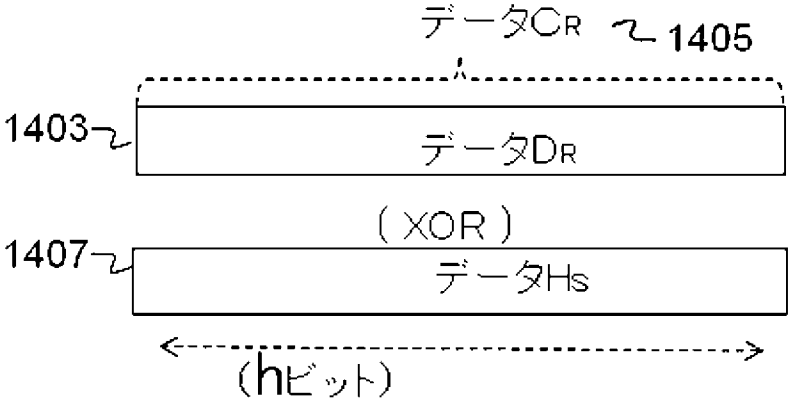
[図14A]

図１４Ａ



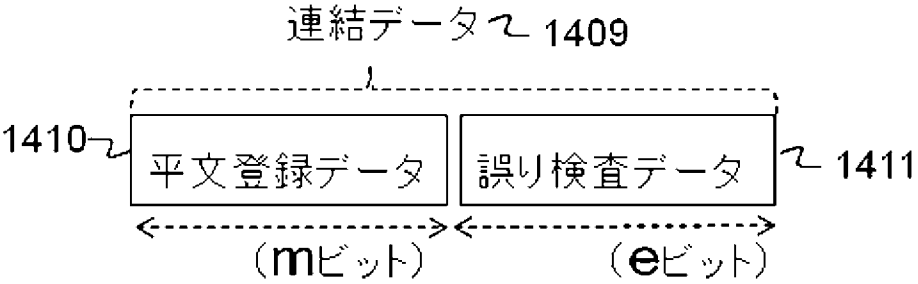
[図14B]

図１４Ｂ



[図14C]

図１４Ｃ



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/077588

A. CLASSIFICATION OF SUBJECT MATTER
G06F17/30(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)
G06F17/30

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	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

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.
A	JP 2007-114494 A (Nippon Telegraph and Telephone Corp.), 10 May 2007 (10.05.2007), entire text; all drawings (Family: none)	1-10

☐ 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
27 December, 2011 (27.12.11)	17 January, 2012 (17.01.12)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／０７７５８８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F17/30(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.　G06F17/30

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	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１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
A	JP 2007-114494 A（日本電信電話株式会社）2007.05.10, 全文全図（ファミリーなし）	1-10

☐　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 ２７．１２．２０１１	国際調査報告の発送日 １７．０１．２０１２
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）　５Ｍ　４０５２ 岩田　淳 電話番号　０３－３５８１－１１０１　内線　３５９９