

SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

- 一 国際調査報告(条約第21条(3))

(57) 要約: 索引ビット列生成部(310)は、データセンタ装置(401)で保管される暗号化データの検索の際に索引として用いられるビット列を、暗号化データに関連付けて、索引ビット列として生成する。また、索引ビット列生成部(310)は、索引ビット列の複数のビット値を、共通鍵方式の索引鍵を用いて暗号化する。端末側データ送受信部(309)は、索引ビット列生成部(310)により複数のビット値が暗号化された後の索引ビット列である暗号化索引ビット列と、暗号化データとをデータセンタ装置(401)に送信する。

明 細 書

発明の名称：

データ処理装置、データ処理方法及びデータ処理プログラム

技術分野

[0001] 本発明は、秘匿検索技術に関する。

背景技術

[0002] 秘匿検索とは、暗号化データを暗号化したまま検索する技術である。

近年、秘匿検索は、クラウドサービスなどのインターネット上でデータを管理する際のサーバ管理者による盗聴からも機密情報を守るためのセキュリティ技術として注目されている。

[0003] 秘匿検索の基本的な流れは、下記の通りである。

まず、データを暗号化するユーザ（暗号化者）は、データを暗号化して暗号化データを生成する。また、ユーザ（暗号化者）は、生成した暗号化データを検索するためのキーワードを当該暗号化データに関連付ける。

関連付けたキーワードもデータに関する情報であるため、キーワードも暗号化される。暗号化されたキーワードは暗号化タグという。暗号化データと暗号化タグはデータセンタ装置に保管される。

暗号化タグは1個である必要はなく、複数の暗号化タグを暗号化データに関連付けることができる。

また、暗号化タグからキーワードが漏れることはない。

[0004] 検索を行うユーザ（検索者）は、検索したいキーワードを選び、そのキーワードと自身の持つ秘密鍵を用いて検索クエリを生成する。

検索クエリは、秘密鍵を用いてキーワードをランダム化したものであるため、検索クエリ自身から秘密鍵を類推するのは難しい。

そして、ユーザ（検索者）は、この検索クエリをデータセンタ装置に送信し、データセンタ装置に検索を要求する。

[0005] データセンタ装置は、ユーザ（暗号化者）から保管を依頼された暗号化デ

ータと暗号化タグを相互に対応付けて保管している。

データセンタ装置は、ユーザ（検索者）から検索クエリを受け取ったら、データセンタ装置が保管する暗号化タグの中から、検索クエリの生成に用いられたキーワードと同一のキーワードを含む暗号化タグを検索する。

この時、データセンタ装置は秘匿検索のための特殊な演算を行うことによって、暗号化タグを復号してキーワードを取り出すことなく、暗号化タグのキーワードと、検索クエリのキーワードが同一かどうかを判定できる。

そして、データセンタ装置はキーワードが検索クエリと同一と判定された暗号化タグと関連付けられた暗号化データをユーザ（検索者）に返却する。

[0006] なお、秘匿検索には、暗号化者と検索者が同一の秘密情報を保持しなくてはならない共通鍵方式と、暗号化者は誰でも良くて検索者のみが秘密情報を保持する特定ユーザに限定された公開鍵方式の2種類がある。

[0007] また、秘匿検索を実現する手法は、確定的暗号を利用する方法と、確率的暗号を利用する方法の2種類がある。

確定的暗号とは、同一のキーワードを暗号化した際に、何回繰り返して暗号化しても同一の暗号文が得られるという特徴を持つ暗号化方式である。

そのため、確定的暗号には、従来のデータベースで実現されている転置索引などの高速化手法を利用して、検索を高速に実施することができるという特徴がある。

その一方で、暗号化データの出現頻度をカウントする事ができるため、確定的暗号には、例えばキーワードが名字であった場合、一般的に知られている名字の人口比率の情報等を元にして、暗号化データの中身が推測できてしまうという欠点もある（例えば非特許文献2）。

[0008] 一方、確率的暗号とは、同一のキーワードを暗号化する場合でも、暗号化のたびに異なる暗号文となるという特徴を持つ暗号化方式である。

したがって、単純に暗号化データ同士を比較してもキーワードが同一かどうか分からない。このため、確定的暗号で問題となっていた出現頻度のカウントによるキーワードの推測ができない様になっており、その安全性が高い

事が特徴である。

その一方で、キーワードの同一性すら分からないため、従来のデータベースで実現されていた高速化手法が使えず、検索が遅いという欠点がある（例えば非特許文献1、非特許文献3、非特許文献4、非特許文献5）。

[0009] 確率的暗号を用いた秘匿検索を高速化する手法として、検索結果をキャッシュすることによって平均応答時間を短縮するアイデアが提案されている。

これは、一般的な検索では同じキーワードで2回以上検索される事があるという特徴に着目したものである。この手法では、1回目の検索では時間がかかるものの、その結果をキャッシュして2回目以降はキャッシュした結果を返すだけにすることで、検索の高速化を図っている（例えば特許文献1）。

[0010] また、確率的暗号を用いた秘匿検索方式において、キーワードの部分情報であるビット列を暗号化し、暗号化されたビット列をデータセンタ装置に送信することによって、秘匿検索を高速化する技術がある（例えば、特許文献2）。

特許文献2の技術では、暗号化されたビット列のうちの一部のビット値が開示されることで、データセンタ装置は当該ビット列を索引として用いることができる。この結果、特許文献2の技術により、秘匿検索を高速化することができる。更に、特許文献2の技術では、データセンタ装置に登録されている暗号化データの数が増加して検索速度が遅くなった場合に、ビット列内の秘匿されているビット値を追加でデータセンタ装置に開示することで、秘匿検索の検索速度を改善することができる。

先行技術文献

特許文献

[0011] 特許文献1：特開2005-134990号公報

特許文献2：国際公開2012/095973号

非特許文献

[0012] 非特許文献1：D. Boneh、G. D. Crescenzo、R. Ostrovsky、G. Persiano G、"Public Key Encr

yption with Keyword Search”、EUROCRYPT’ 2004、Lecture Notes in Computer Science、Vol. 3027、2004.

非特許文献2：M. Bellare、A. Boldyreva、A. O’Neill、“Deterministic and Efficiently Searchable Encryption”、CRYPTO’ 2007、Lecture Notes in Computer Science、Vol. 4622、2007.

非特許文献3：J. Katz、A. Sahai、B. Waters、“Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products”、EUROCRYPT 2008、Lecture Notes in Computer Science、Vol. 4965、2008.

非特許文献4：服部 充洋、森 拓海、伊藤 隆、松田 規、米田 健、太田 和夫、“Anonymous HIBE with Wildcards and Its Application to Secure Keyword Search for Group-Oriented Multi-User System”、SCIS’ 2010、3A4-2、電子情報通信学会、2010.

非特許文献5：Tatsuaki Okamoto、Katsuyuki Takashima、“Hierarchical Predicate Encryption for Inner-Products”、ASIA CRYPT’ 2009、Lecture Notes in Computer Science、Vol. 5912、2009.

発明の概要

発明が解決しようとする課題

[0013] 特許文献2では、データセンタ装置において索引として用いられるビット

列は公開鍵方式を用いて暗号化されている。このため、データセンタ装置でビット列の一部のビット値の復号する際に、復号処理に時間を要するという課題がある。

[0014] 本発明は、このような課題を解決することを主な目的とする。より具体的には、本発明は、索引として用いられるビット列の復号処理を高速化することにより、検索処理を高速化することを主な目的とする。

課題を解決するための手段

[0015] 本発明に係るデータ処理装置は、

データ保管装置で保管される暗号化データの検索の際に索引として用いられるビット列を、前記暗号化データに関連付けて、索引ビット列として生成する索引ビット列生成部と、

前記索引ビット列の複数のビット値を、共通鍵方式の索引鍵を用いて暗号化する索引ビット列暗号化部と、

前記索引ビット列暗号化部により前記複数のビット値が暗号化された後の前記索引ビット列である暗号化索引ビット列と、前記暗号化データとを前記データ保管装置に送信する送信部とを有する。

発明の効果

[0016] 本発明では、索引ビット列は、共通鍵方式の索引鍵を用いて暗号化される。このため、本発明によれば、索引ビット列の復号処理を高速化することができ、この結果、検索処理を高速化することができる。

図面の簡単な説明

[0017] [図1]実施の形態1に係る秘匿検索システムの構成例を示す図。

[図2]実施の形態1に係る秘匿検索システムを示す図。

[図3]実施の形態1に係る秘匿検索システムを示す図。

[図4]実施の形態1に係る秘匿検索システムを示す図。

[図5]実施の形態1に係る秘匿検索システムを示す図。

[図6]実施の形態1に係るアクセス端末装置の機能構成例を示す図。

[図7]実施の形態1に係るデータセンタ装置の機能構成例を示す図。

[図8]実施の形態1に係るアクセス端末装置の動作例を示すフローチャート図

。

[図9]実施の形態1に係るアクセス端末装置の動作例を示すフローチャート図

。

[図10]実施の形態1に係るアクセス端末装置の動作例を示すフローチャート図。

[図11]実施の形態1に係るデータセンタ装置の動作例を示すフローチャート図。

[図12]実施の形態1に係るデータセンタ装置の動作例を示すフローチャート図。

[図13]実施の形態1に係るデータセンタ装置の動作例を示すフローチャート図。

[図14]実施の形態1に係るアクセス端末装置のハードウェア構成例を示す図

。

[図15]実施の形態1に係るデータセンタ装置のハードウェア構成例を示す図

。

発明を実施するための形態

[0018] 実施の形態1.

本実施の形態では、暗号化データの検索の際に索引として用いられるビット列（以下、索引ビット列）を暗号化し、暗号化により得られた索引ビット列（以下、暗号化索引ビット列という）を暗号化タグに付加して秘匿検索を高速化する方式を説明する。

更に、本実施の形態1では、データセンタ装置に登録された暗号化データの数が増加して検索処理が遅くなった場合に、暗号化索引ビット列の暗号化されているビット値を段階的に開示することで、秘匿検索を安全に高速化する方式を説明する。

[0019] 図1は、秘匿検索システム100の構成例を示す図である。

[0020] 秘匿検索システム100は、鍵管理サーバ装置201、アクセス端末装置

301、データセンタ装置401を備える。

鍵管理サーバ装置201とアクセス端末装置301とは、LAN (Local Area Network) 102に接続されている。

LAN 102は、ネットワーク101を介してデータセンタ装置401と接続されている。

なお、アクセス端末装置301はデータ処理装置の例であり、データセンタ装置401はデータ保管装置の例である。

図1では、1つのアクセス端末装置301のみが示されているが、秘匿検索システム100に複数のアクセス端末装置301が含まれていてもよい。

[0021] 鍵管理サーバ装置201は、データセンタ装置401での保管対象となる保管対象データの暗号化に用いる暗号鍵及びタグの暗号化に用いる暗号鍵を生成する。

また、鍵管理サーバ装置201は、索引ビット列の暗号化に用いる複数の索引鍵を生成してもよい。

[0022] アクセス端末装置301は、ユーザが利用するPC (Personal Computer) である。

アクセス端末装置301は、保管対象データを生成し、生成した保管対象データを暗号化する。また、アクセス端末装置301は、暗号化により得られた暗号化データをデータセンタ装置401に保管する。また、アクセス端末装置301は、データセンタ装置401に、暗号化データの検索を要求する。そして、アクセス端末装置301は、データセンタ装置401から、取得された暗号化データを受信し、受信した暗号化データの復号を行う。

[0023] データセンタ装置401は、暗号化データを保管する大容量の記憶装置を持つサーバ装置である。

保管対象データは暗号化された状態で保管されるため、データセンタ装置401では保管対象データの中身を閲覧することができない。

[0024] ネットワーク101は、LAN 102とデータセンタ装置401を接続する通信路である。

例えば、インターネットなどが代表的なネットワーク 101 の例である。

[0025] ここで、図 2 ～図 5 を参照して、本実施の形態における秘匿検索システム 100 の概要を説明する。

[0026] 図 2 に示すように、アクセス端末装置 301 は、保管対象データを暗号化して、暗号化データを生成する。

また、アクセス端末装置 301 は、保管対象データからキーワードを抽出し、抽出したキーワードを乱数と暗号鍵を用いて暗号化して暗号化タグを生成する。

暗号化タグは、暗号化データの検索の際に照合されるデータである。

また、アクセス端末装置 301 は、保管対象データのキーワードに対して規定の演算を行って索引ビット列を生成する。アクセス端末装置 301 は、例えば、キーワードに対してハッシュ演算を行って索引ビット列を生成する。また、アクセス端末装置 301 は、ハッシュ演算に加え暗号鍵を用いて確定的暗号方式による暗号化を行って索引ビット列を生成してもよい。

そして、アクセス端末装置 301 は、索引ビット列を暗号化する。より具体的には、アクセス端末装置 301 は、共通鍵方式の索引鍵を用いて索引ビット列を暗号化する。

そして、アクセス端末装置 301 は、暗号化データと、暗号化タグと、索引ビット列を暗号化して得られた暗号化索引ビット列をデータセンタ装置 401 に送信する。

[0027] データセンタ装置 401 は、暗号化データと暗号化タグと暗号化索引ビット列を受信する。そして、データセンタ装置 401 は、暗号化データと暗号化タグと暗号化索引ビット列を相互に対応付けて記憶する。

[0028] 図 3 に示すように、データセンタ装置 401 に保管されている暗号化データを検索する際には、アクセス端末装置 301 は、検索対象のキーワードを暗号化してトラップドアを生成する。

そして、アクセス端末装置 301 は、トラップドアが含まれる検索クエリをデータセンタ装置 401 に送信する。

なお、データセンタ装置４０１に暗号化データを登録するアクセス端末装置３０１と、データセンタ装置４０１に暗号化データの検索を要求するアクセス端末装置３０１は一致していなくてもよい。

[0029] データセンタ装置４０１は、アクセス端末装置３０１から検索クエリを受信した場合に、検索クエリに含まれているトラップドアを暗号化タグと照合する。

そして、データセンタ装置４０１は、照合の結果、トラップドアの生成に用いられたキーワードと同じキーワードで生成されている暗号化タグを特定し、特定したタグデータと対応付けられている暗号化データを抽出する。次に、データセンタ装置４０１は、抽出した暗号化データを検索クエリの送信元のアクセス端末装置３０１に送信する。

[0030] データセンタ装置４０１で保管されている暗号化データが増えてくると、検索効率が低下し、暗号化データの検索速度が遅くなる。

このような場合には、図４に示すように、暗号化データの保管を要求したアクセス端末装置３０１は、暗号化索引ビット列の一部のビット値をデータセンタ装置４０１に開示する。アクセス端末装置３０１は、１ビットずつ段階的にビット値を開示してもよいし、複数ビットずつ段階的にビット値を開示してもよい。また、アクセス端末装置３０１は、１度にすべてのビット値を開示してもよい。

ビット値の開示は、具体的には、アクセス端末装置３０１は、暗号化索引ビット列の生成に用いられた索引鍵をデータセンタ装置４０１に送信することで行われる。なお、この索引鍵の送信は暗号化通信により行われる。

[0031] データセンタ装置４０１は、アクセス端末装置３０１から送信された索引鍵を受信する。そして、データセンタ装置４０１は、受信した索引鍵を用いて暗号化索引ビット列の暗号化されているビット値の復号を行う。

例えば、図２に示すように、暗号化データと対応付けられている暗号化索引ビット列の暗号化前の値（つまり、索引ビット列の値）が「０１１」であるとする。

アクセス端末装置 301 が、最上位ビットのビット値を解除するための索引鍵をデータセンタ装置 401 に送信したと仮定する。

データセンタ装置 401 は、受信した索引鍵を用いて、上記「011」の索引ビット列のうち、最上位ビットのビット値である「0」を得る。

アクセス端末装置 301 は、図 5 に示すように、トラップドアと暗号化索引ビット列の最上位ビットのビット値である「0」を含む検索クエリをデータセンタ装置 401 に送信する。

データセンタ装置 401 は、最上位ビットのビット値が「0」である暗号化索引ビット列に対応付けられている暗号化タグを選択し、選択した暗号化タグのみをトラップドアと照合する。

更に検索効率が低下した場合には、アクセス端末装置 301 は、暗号化索引ビット列の下位のビット値をデータセンタ装置 401 に開示する。このようにすることで、検索効率が低下した場合にも、暗号化ビット列のビット値の開示により検索効率を改善することができる。

[0032] 本実施の形態では、索引ビット列は共通鍵方式で暗号化される。このため、データセンタ装置 401 は、高速に索引ビット列のビット値の復号を行うことができる。

また、本実施の形態では、アクセス端末装置 301 は、索引ビット列の生成過程で確定的暗号方式による暗号化を行う。このため、暗号化索引ビット列の全てのビット値がデータセンタ装置 401 に開示された場合でも、データセンタ装置 401 にキーワードが漏洩するおそれがない。例えば、暗号鍵を用いずにキーワードにハッシュ演算を行って索引ビット列を生成する場合は、ハッシュ演算は誰でも実行できるため、索引ビット列を誰でも生成することができる。このため、手当たり次第にキーワードのハッシュ値を計算することで、データセンタ装置 401 に保管されたハッシュ値と同じものが現れる可能性があり、その時索引ビット列の生成のもとになったキーワードを得ることができる。しかし、本実施の形態に係る索引ビット列は、確定的暗号方式の暗号が行われて生成された索引ビット列であるため、キーワードが漏

洩する心配はない。

[0033] 以上が、本実施の形態に係る秘匿検索システム１００における動作の概要であり、以下では、アクセス端末装置３０１及びデータセンタ装置４０１の内部構成を説明する。

[0034] 図６は、アクセス端末装置３０１の機能構成例を示す。

また、図１４は、アクセス端末装置３０１のハードウェア構成例を示す。

[0035] 図６に示すように、アクセス端末装置３０１は、データ暗号化部３０２、暗号化タグ生成部３０３、タグ付き暗号化データ生成部３０４、鍵管理部３０５、検索クエリ生成部３０６、データ復号部３０７、許可ビット位置指定部３０８、端末側データ送受信部３０９及び暗号化索引ビット列生成部３１０を備える。

[0036] 本実施の形態に係るアクセス端末装置３０１は、コンピュータである。

図１４に示すように、アクセス端末装置３０１は、ハードウェアとして、プロセッサ９３１、補助記憶装置９３２、メモリ９３３、通信インタフェース９３４及び入出力インタフェース９３５を備える。

補助記憶装置９３２には、データ暗号化部３０２、暗号化タグ生成部３０３、タグ付き暗号化データ生成部３０４、鍵管理部３０５、検索クエリ生成部３０６、データ復号部３０７、許可ビット位置指定部３０８、端末側データ送受信部３０９及び暗号化索引ビット列生成部３１０の機能を実現するプログラムが記憶されている。

これらプログラムは補助記憶装置９３２からメモリ９３３にロードされる。

そして、プロセッサ９３１がこれらプログラムを実行して、後述するデータ暗号化部３０２、暗号化タグ生成部３０３、タグ付き暗号化データ生成部３０４、鍵管理部３０５、検索クエリ生成部３０６、データ復号部３０７、許可ビット位置指定部３０８、端末側データ送受信部３０９及び暗号化索引ビット列生成部３１０の動作を行う。

図１４では、プロセッサ９３１がデータ暗号化部３０２、暗号化タグ生成

部 303、タグ付き暗号化データ生成部 304、鍵管理部 305、検索クエリ生成部 306、データ復号部 307、許可ビット位置指定部 308、端末側データ送受信部 309 及び暗号化索引ビット列生成部 310 の機能を実現するプログラムを実行している状態を模式的に表している。

アクセス端末装置 301 が行う動作は、データ処理方法に相当する。また、データ暗号化部 302、暗号化タグ生成部 303、タグ付き暗号化データ生成部 304、鍵管理部 305、検索クエリ生成部 306、データ復号部 307、許可ビット位置指定部 308、端末側データ送受信部 309 及び暗号化索引ビット列生成部 310 の機能を実現するプログラムは、データ処理プログラムに相当する。

通信インタフェース 934 は、外部装置と通信を行う。

入出力インタフェース 935 は、アクセス端末装置 301 のユーザからの指示を受け付け、また、アクセス端末装置 301 のユーザに情報を提示する。

[0037] 次に、図 6 に示すアクセス端末装置 301 の機能構成の詳細を説明する。

[0038] データ暗号化部 302 は、ユーザ又はアプリケーションからデータセンタ装置 401 で保管する保管対象データを受領する。また、データ暗号化部 302 は、共通鍵暗号を用いて保管対象データを暗号化し、保管対象データの暗号化データを得る。

データ暗号化部 302 が保管対象データの暗号化に用いる暗号鍵を以下では暗号鍵 $e_k a$ という。

また、データ暗号化部 302 は、保管対象データから後で検索に利用されるキーワードを抽出する。また、データ暗号化部 302 は、ユーザからデータに関連付けるキーワードを受領してもよい。

[0039] 暗号化タグ生成部 303 は、データ暗号化部 302 で保管対象データに関連付けられたキーワードを乱数と暗号鍵を用いて暗号化して暗号化タグを生成する。

暗号化タグ生成部 303 がキーワードの暗号化に用いる暗号鍵を以下では

暗号鍵 $e k b$ という。

[0040] 暗号化索引ビット列生成部 310 は、保管対象データのキーワードに対して規定の演算を行って索引ビット列を生成する。

また、暗号化索引ビット列生成部 310 は、索引鍵を用いて索引ビット列を暗号化する。

[0041] 本実施の形態では、暗号化索引ビット列生成部 310 は、索引ビット列の複数のビット値の各々を、異なる索引鍵を用いて暗号化する。例えば、索引ビット列が 3 ビットであれば、暗号化索引ビット列生成部 310 は、3 つの索引鍵を用いる。

暗号化索引ビット列生成部 310 が索引ビット列の暗号化に用いる索引鍵を以下では索引鍵 $i k$ という。以下では、「 $i k$ 」の後ろに索引鍵 $i k$ が対応しているビット位置を表す数字を付加する。例えば、索引ビット列が 3 ビットであれば、最上位ビットのビット値の暗号化に用いられる索引鍵は索引鍵 $i k 1$ と表記する。また、最下位ビットのビット値の暗号化に用いられる索引鍵は索引鍵 $i k 3$ と表記する。なお、「 $i k$ 」の後ろに数字が付加されない「索引鍵 $i k$ 」との表記は、複数の索引鍵の全て又は複数の索引鍵のうちの一部の索引鍵を意味する。

[0042] また、暗号化索引ビット列生成部 310 は、複数の暗号化データがデータセンタ装置 401 に保管される場合は、複数の暗号化データに対応させて複数の索引ビット列を生成する。そして、暗号化索引ビット列生成部 310 は、複数の暗号化データの複数の索引ビット列の暗号化に共通する索引鍵のセットを用いることができる。

つまり、暗号化索引ビット列生成部 310 は、複数の索引ビット列の同じビット位置にあるビット値を同じ索引鍵を用いて暗号化する。例えば、全ての索引ビット列が 3 ビットであれば、暗号化索引ビット列生成部 310 は、全ての索引ビット列の最上位ビットのビット値を索引鍵 $i k 1$ を用いて暗号化する。また、暗号化索引ビット列生成部 310 は、全ての索引ビット列の最下位ビットのビット値を索引鍵 $i k 3$ を用いて暗号化する。

このようにすることで、後述する許可ビット位置指定部 308 が索引鍵 i k 1 をデータセンタ装置 401 に送信するのみで、複数の暗号化データの複数の暗号化索引ビット列の最上位ビットのビット値を開示することができる。

なお、暗号化索引ビット列生成部 310 は、複数の索引ビット列の暗号化にそれぞれ異なる索引鍵のセットを用いてもよい。

[0043] また、本実施の形態では、暗号化索引ビット列生成部 310 は、索引ビット列の複数のビット値の各々を、異なる索引鍵を用いて暗号化するが、暗号化索引ビット列生成部 310 は、索引ビット列の複数のビット値を、索引ビット列のビット数よりも少ない個数の索引鍵を用いて暗号化してもよい。具体的には、索引ビット列が 3 ビットであれば、暗号化索引ビット列生成部 310 は、1 つ又は 2 つの索引鍵を用いるようにしてもよい。

[0044] また、暗号化索引ビット列生成部 310 は、後述する許可ビット位置以外のビット位置にある暗号化されたビット値は、許可ビット位置のビット値の暗号化に用いられた索引鍵では復号されない暗号化方式にて、索引ビット列の複数のビット値を暗号化する。

[0045] 暗号化索引ビット列生成部 310 は、索引ビット列生成部及び索引ビット列暗号化部に相当する。また、暗号化索引ビット列生成部 310 により行われる処理は、索引ビット列生成処理及び索引ビット列暗号化処理に相当する。

[0046] タグ付き暗号化データ生成部 304 は、データ暗号化部 302 で生成された暗号化データと、暗号化タグ生成部 303 で生成された暗号化タグと、暗号化索引ビット列生成部 310 で生成された暗号化索引ビット列を結合してタグ付き暗号化データを生成する。

そして、タグ付き暗号化データ生成部 304 は、タグ付き暗号化データを端末側データ送受信部 309 に出力する。

[0047] 鍵管理部 305 は、暗号鍵 $e k a$ 及び暗号鍵 $e k b$ を管理する。

より具体的には、鍵管理部 305 は、鍵管理サーバ装置 201 で生成され

た暗号鍵 $e_k a$ 及び暗号鍵 $e_k b$ を補助記憶装置 932 に格納する。

また、鍵管理部 305 は、暗号鍵 $e_k a$ 又は暗号鍵 $e_k b$ から複数の索引鍵 i_k ($i_k 1$, $i_k 2$, $i_k 3 \dots$) を生成し、生成した複数の索引鍵 i_k を補助記憶装置 932 に格納する。鍵管理部 305 は複数の索引鍵 i_k を補助記憶装置 932 に格納する代わりに、索引鍵 i_k が必要になる度に、暗号鍵 $e_k a$ 又は暗号鍵 $e_k b$ から生成してもよい。

また、鍵管理部 305 は、鍵管理サーバ装置 201 で暗号鍵 $e_k a$ と暗号鍵 $e_k b$ とは独立に生成された索引鍵 i_k を補助記憶装置 932 に格納するようにしてもよい。

また、鍵管理部 305 は、検索クエリ生成部 306 の検索クエリの生成のために暗号鍵 $e_k b$ を出力する。

また、鍵管理部 305 は、データ復号部 307 の暗号化データの復号のためにデータ復号部 307 に暗号鍵 $e_k a$ を出力する。

また、鍵管理部 305 は、暗号化索引ビット列内の特定のビット値の開示のために、開示対象のビット値に対応する索引鍵 i_k を許可ビット位置指定部 308 に出力する。

[0048] 検索クエリ生成部 306 は、ユーザから指定された検索キーワードを暗号鍵 $e_k b$ で暗号化してトラップドアを生成する。そして、検索クエリ生成部 306 は、トラップドアが含まれる検索クエリを生成し、検索クエリを端末側データ送受信部 309 に出力する。

また、開示済みビット値が存在する場合は、検索クエリ生成部 306 は、トラップドアと開示済みビット値とが含まれる検索クエリを生成し、検索クエリを端末側データ送受信部 309 に出力する。

なお、開示済みビット値が存在する場合は、検索クエリ生成部 306 は、暗号化索引ビット列生成部 310 を用いて検索キーワードの暗号化索引ビット列を生成し、トラップドアと前記暗号化索引ビット列とが含まれる検索クエリを生成し、検索クエリを端末側データ送受信部 309 に出力するようにしてもよい。この場合、データセンタ装置 401 は、既の開示された索引鍵

i k を使って、前記暗号化索引ビット列から開示済みビット値を取得することができる。

[0049] データ復号部 307 は、データセンタ装置 401 から受信された暗号化データを、暗号鍵 e k a を用いて復号する。

[0050] 許可ビット位置指定部 308 は、許可ビット位置を指定する。

許可ビット位置は、暗号化索引ビット列の複数のビット位置のうち暗号化を解除してビット値を開示するビット位置である。

許可ビット位置指定部 308 は、ユーザからの指示に従って許可ビット位置を指定してもよいし、既定のアルゴリズムに従って許可ビット位置を指定してもよい。許可ビット位置指定部 308 は、1 ビットずつ段階的に許可ビット位置を指定してもよいし、1 度に 2 ビット以上を許可ビット位置に指定してもよい。また、許可ビット位置指定部 308 は、1 度に暗号化索引ビット列の全ビットを許可ビット位置に指定してもよい。許可ビット位置指定部 308 は段階的に許可ビット位置を指定する場合は最上位ビットから順に許可ビット位置を指定する。

許可ビット位置指定部 308 は、許可ビット位置に対応する索引鍵 i k を鍵管理部 305 から取得する。つまり、許可ビット位置指定部 308 は、許可ビット位置のビット値の暗号化に用いられた索引鍵 i k を鍵管理部 305 から取得する。そして、取得した索引鍵 i k を端末側データ送受信部 309 に出力する。

[0051] 端末側データ送受信部 309 は、鍵管理サーバ装置 201 から暗号鍵 e k a 及び暗号鍵 e k b を受信する。端末側データ送受信部 309 は、鍵管理サーバ装置 201 から複数の索引鍵 i k を受信する場合もある。

また、端末側データ送受信部 309 は、タグ付き暗号化データをデータセンタ装置 401 に送信する。

また、端末側データ送受信部 309 は、検索結果である暗号化データをデータセンタ装置 401 から受信する。

また、端末側データ送受信部 309 は、許可ビット位置のビット値の開示

のために、データセンタ装置４０１に索引鍵 i k を送信する。

端末側データ送受信部３０９は送信部に相当する。また、端末側データ送受信部３０９で行われる処理は送信処理に相当する。

[0052] 図７は、データセンタ装置４０１の機能構成例を示す。

図１５は、データセンタ装置４０１のハードウェア構成例を示す。

[0053] 図７に示すように、データセンタ装置４０１は、センタ側データ送受信部４０２、保管要求処理部４０３、データ記憶部４０４、開示ビット値復号部４０５、検索処理部４０６を備える。

[0054] 本実施の形態に係るデータセンタ装置４０１は、コンピュータである。

図１５に示すように、データセンタ装置４０１は、ハードウェアとして、プロセッサ９４１、補助記憶装置９４２、メモリ９４３、通信インタフェース９４４及び入出力インタフェース９４５を備える。

補助記憶装置９４２には、センタ側データ送受信部４０２、保管要求処理部４０３、開示ビット値復号部４０５及び検索処理部４０６の機能を実現するプログラムが記憶されている。

これらプログラムは記憶装置９４２からメモリ９４３にロードされる。

そして、プロセッサ９４１がこれらプログラムを実行して、後述するセンタ側データ送受信部４０２、保管要求処理部４０３、開示ビット値復号部４０５及び検索処理部４０６の動作を行う。

図１４では、プロセッサ９４１がセンタ側データ送受信部４０２、保管要求処理部４０３、開示ビット値復号部４０５及び検索処理部４０６の機能を実現するプログラムを実行している状態を模式的に表している。

データ記憶部４０４は補助記憶装置９４２により実現される。

通信インタフェース９４４は、外部装置と通信を行う。

入出力インタフェース９４５は、データセンタ装置４０１のユーザからの指示を受け付け、また、データセンタ装置４０１のユーザに情報を提示する。

[0055] 次に、図７に示すデータセンタ装置４０１の機能構成の詳細を説明する。

[0056] センタ側データ送受信部402は、アクセス端末装置301からタグ付き暗号化データを受信する。

また、センタ側データ送受信部402は、アクセス端末装置301から検索クエリを受信し、その応答として暗号化データを送信する。

また、センタ側データ送受信部402は、アクセス端末装置301から索引鍵ikを受信する。

[0057] 保管要求処理部403は、受信したタグ付き暗号化データを解析し、タグ付き暗号化データを暗号化データと暗号化タグと暗号化索引ビット列に分解する。そして、保管要求処理部403は、暗号化データと暗号化タグと暗号化索引ビット列を相互に対応付けてデータ記憶部404に格納する。

[0058] データ記憶部404は、暗号化データと暗号化タグと暗号化索引ビット列を相互に対応付けて記憶する。

[0059] 開示ビット値復号部405は、受信した索引鍵ikを用いて、暗号化索引ビット列の許可ビット位置のビット値の復号を行う。

[0060] 検索処理部406は、アクセス端末装置301から受信した検索クエリと、データ記憶部404内の暗号化タグとの照合処理を行う。

検索処理部406は、この照合処理によって、タグに含まれるキーワードと、検索クエリに含まれるキーワードが一致するかどうかを判定する。

その後、検索処理部406は、検索にヒットしたタグと関連付けられた暗号化データをデータ記憶部404から取得する。そして、検索処理部406は、取得した暗号化データをセンタ側データ送受信部402を介してアクセス端末装置301に返送する。

[0061] ***動作の説明***

次に、図8に基づき、アクセス端末装置301でのデータの暗号化処理を説明する。

[0062] 最初に、ステップS801において、データ暗号化部302は、ユーザから保管対象データを受け取り、保管対象データと関連付けるキーワードを決定する。

データ暗号化部 302 が保管対象データからキーワードを抽出してもよいし、ユーザがキーワードを指定してもよい。

また、1つのキーワードが保管対象データに関連付けられてもよいし、複数のキーワードが保管対象データに関連付けられてもよい。以下では、説明の簡明のために、1つのキーワードが保管対象データに関連付けられるものとする。

[0063] 次に、ステップ S802 において、データ暗号化部 302 は、保管対象データを暗号化して暗号化データを生成する。

より具体的には、データ暗号化部 302 は、鍵管理部 305 から暗号鍵 $e_k a$ を取得し、暗号鍵 $e_k a$ を用いて保管対象データを暗号化する。

データ暗号化部 302 は、キーワードを暗号化タグ生成部 303 に出力する。また、データ暗号化部 302 は、暗号化データをタグ付き暗号化データ生成部 304 に出力する。

[0064] 次に、ステップ S803 において、暗号化タグ生成部 303 は、暗号化タグを生成する。

より具体的には、暗号化タグ生成部 303 は、鍵管理部 305 から暗号鍵 $e_k b$ を取得し、キーワードを乱数と暗号鍵 $e_k b$ を用いて暗号化して暗号化タグを生成する。

暗号化タグ生成部 303 は、キーワードを暗号化索引ビット列生成部 310 に出力する。また、暗号化タグ生成部 303 は、暗号化タグをタグ付き暗号化データ生成部 304 に出力する。

[0065] 次に、ステップ S804 において、暗号化索引ビット列生成部 310 がキーワードに対して規定の演算を行って索引ビット列を生成する。

暗号化索引ビット列生成部 310 は、例えば、キーワードに対してハッシュ演算を行って索引ビット列を生成する。また、暗号化索引ビット列生成部 310 は、ハッシュ演算に加えて確定的暗号方式による暗号化を行って索引ビット列を生成してもよい。

[0066] 次に、ステップ S805 において、暗号化索引ビット列生成部 310 が索

引ビット列を暗号化して暗号化索引ビット列を生成する。

より具体的には、暗号化索引ビット列生成部 310 は、鍵管理部 305 から共通鍵方式の索引鍵 i_k を取得し、索引鍵 i_k を用いて索引ビット列を暗号化する。

暗号化索引ビット列生成部 310 は、暗号化索引ビット列をタグ付き暗号化データ生成部 304 に出力する。

[0067] 次に、ステップ S806 において、タグ付き暗号化データ生成部 304 が、暗号化データと暗号化タグと暗号化索引ビット列とを結合してタグ付き暗号化データを生成する。

タグ付き暗号化データ生成部 304 は、生成したタグ付き暗号化データを端末側データ送受信部 309 に出力する。

[0068] 次に、ステップ S807 において、端末側データ送受信部 309 が、タグ付き暗号化データをデータセンタ装置 401 に送信する。

[0069] 次に、図 11 に基づき、データセンタ装置 401 における暗号化データの保管処理を説明する。

[0070] まず、センタ側データ送受信部 402 がタグ付き暗号化データを受信すると（ステップ S1101 で YES）、ステップ S1102 において、保管要求処理部 403 が、タグ付き暗号化データを暗号化データと暗号化タグと暗号化索引ビット列に分解する。

[0071] そして、ステップ S1103 において、保管要求処理部 403 が、暗号化データと暗号化タグと暗号化索引ビット列とを相互に対応付けてデータ記憶部 404 に格納する。

[0072] 次に、図 9 に基づき、アクセス端末装置 301 での検索要求処理について説明する。

[0073] はじめにステップ S901 において、検索クエリ生成部 306 が、アクセス端末装置 301 を操作するユーザから、検索キーワードを取得する。

[0074] 次に、ステップ S902 において、検索クエリ生成部 306 は、検索キーワードを暗号化して、検索クエリ生成する。

より具体的には、検索クエリ生成部306は、鍵管理部305から暗号鍵e k bを取得し、暗号鍵e k bを用いて検索キーワードを暗号化する。そして、検索クエリ生成部306は、暗号化により得られたトラップドアが含まれる検索クエリを生成する。

[0075] 次に、ステップS903において、検索クエリ生成部306は、索引ビット列のいずれかのビット値が開示済みであるか否かを判定する。

[0076] 索引ビット列のいずれかのビット値が開示済みであれば（ステップS903でYES）は、ステップS904において、検索クエリ生成部306は、開示済みビット値を検索クエリに追加する。

[0077] 次に、ステップS905にて、端末側データ送受信部309が検索クエリをデータセンタ装置401に送信する。

[0078] 次に、ステップS906にて、端末側データ送受信部309が検索結果を受信した場合に（ステップS906でYES）、データ復号部307が、鍵管理部305から暗号鍵e k aを取得し、検索結果に含まれる暗号化データを暗号鍵e k aを用いて復号する（ステップS907）。

[0079] 次に、図12に基づき、データセンタ装置401での暗号化データ検索処理を説明する。

[0080] センタ側データ送受信部402が検索クエリを受信すると（ステップS1201でYES）、ステップS1202において、検索処理部406が、検索クエリに開示済みビット値が含まれているか否かを判定する。

[0081] 検索クエリに開示済みビット値が含まれていない場合（ステップS1202でNO）は、ステップS1204において、検索処理部406は、トラップドアを用いた検索を行う。つまり、検索処理部406は、トラップドアを暗号化タグと照合する。そして、検索処理部406は、トラップドアの生成に用いられたキーワードと同じキーワードで生成されている暗号化タグを特定し、特定したタグデータと対応付けられている暗号化データを抽出する。

[0082] 一方、検索クエリに開示済みビット値が含まれている場合（ステップS1202でYES）は、ステップS1203において、検索処理部406は、

検索クエリに含まれる開示済みビット値と同じビット値が含まれる暗号化索引ビット列に対応付けられた暗号化タグに限定してトラップドアを用いた検索を行う。

[0083] 最後に、センタ側データ送受信部402が、検索処理部406により抽出された暗号化データを検索クエリの送信元のアクセス端末装置301に送信する。

[0084] 次に、図10に基づき、アクセス端末装置301での索引ビット値開示処理を説明する。

[0085] まず、ステップS1001において、許可ビット位置指定部308が許可ビット位置を指定する。

例えば、データセンタ装置401における検索効率が閾値以下になった場合に、許可ビット位置指定部308は許可ビット位置を指定する。前述したように、許可ビット位置指定部308は、ユーザからの指示に従って許可ビット位置を指定してもよいし、既定のアルゴリズムに従って許可ビット位置を指定してもよい。許可ビット位置指定部308は、1ビットずつ段階的に許可ビット位置を指定してもよいし、1度に2ビット以上を許可ビット位置に指定してもよい。

[0086] 次に、ステップS1002において、許可ビット位置指定部308は、許可ビット位置のビット値の暗号化に用いられた索引鍵 i k を鍵管理部305から取得する。

許可ビット位置指定部308は鍵管理部305から取得した索引鍵 i k を許可ビット位置の情報とともに端末側データ送受信部309に出力する。

[0087] 次に、ステップS1003において、端末側データ送受信部309が索引鍵 i k を許可ビット位置の情報とともにデータセンタ装置401に送信する。

[0088] 次に、図13に基づき、データセンタ装置401における暗号化索引ビット列のビット値の復号処理を説明する。

[0089] センタ側データ送受信部402が索引鍵 i k を受信した場合（ステップS

1301でYES)に、ステップS1302にて、開示ビット値復号部405が索引鍵ikを用いて暗号化索引ビット列内の対応するビット値の復号を行う。

[0090] なお、暗号化開示ビット列内のいずれかのビット値の開示後に新たな暗号化データがデータセンタ装置401に登録された場合は、新たな暗号化データの登録時には、新たな暗号化データに対応する暗号化索引ビット列の全てのビット値は暗号化されている。アクセス端末装置301は、新たな暗号化データ対応する暗号化索引ビット列についても、対応するビット位置の索引鍵をデータセンタ装置401に送信し、データセンタ装置401は、暗号化索引ビット列内の対応するビット位置の復号を行う。

[0091] ***実施の形態の効果の説明***

本実施の形態では、アクセス端末装置301は、共通鍵方式の索引鍵を用いて索引ビット列を暗号化する。このため、本実施の形態によれば、アクセス端末装置301は、索引ビット列の復号処理を高速化することができ、この結果、検索処理を高速化することができる。

本実施の形態では、アクセス端末装置301は、共通鍵方式の索引鍵を用いて索引ビット列を暗号化する。このため、本実施の形態によれば、開示前の暗号化索引ビット列からは何も情報が漏れない。

本実施の形態では、アクセス端末装置301は、ハッシュ演算に加えて確定的暗号方式による暗号化を行って索引ビット列を生成する。このため、本実施の形態によれば、索引ビット列の全てのビット値が開示されてもキーワードが類推されるおそれが少ない。

[0092] ***ハードウェア構成の説明***

最後に、本実施の形態に係るアクセス端末装置301及びデータセンタ装置401のハードウェア構成例の補足説明を行う。

[0093] 図14及び図15に示すプロセッサ931及びプロセッサ941は、プロセッシングを行うIC(Integrated Circuit)である。

プロセッサ931及びプロセッサ941は、CPU(Central P

rocessing Unit)、DSP (Digital Signal Processor) 等である。

図14及び図15に示す補助記憶装置932及び補助記憶装置942は、ROM (Read Only Memory)、フラッシュメモリ、HDD (Hard Disk Drive) 等である。

図14及び図15に示すメモリ933及びメモリ943は、RAM (Random Access Memory) である。

図14及び図15に示す通信インタフェース934及び通信インタフェース944は、データの通信処理を実行する電子回路である。

通信インタフェース934及び通信インタフェース944は、例えば、通信チップ又はNIC (Network Interface Card) である。

図14及び図15に示す入出力インタフェース935及び入出力インタフェース945は、例えば、マウス、キーボード、ディスプレイ等である。

[0094] また、補助記憶装置932には、OS (Operating System) も記憶されている。

そして、OSの少なくとも一部がプロセッサ931により実行される。

プロセッサ931はOSの少なくとも一部を実行しながら、データ暗号化部302、暗号化タグ生成部303、タグ付き暗号化データ生成部304、鍵管理部305、検索クエリ生成部306、データ復号部307、許可ビット位置指定部308、端末側データ送受信部309及び暗号化索引ビット列生成部310の機能を実現するプログラムを実行する。

プロセッサ931がOSを実行することで、タスク管理、メモリ管理、ファイル管理、通信制御等が行われる。

また、データ暗号化部302、暗号化タグ生成部303、タグ付き暗号化データ生成部304、鍵管理部305、検索クエリ生成部306、データ復号部307、許可ビット位置指定部308、端末側データ送受信部309及び暗号化索引ビット列生成部310の処理の結果を示す情報、データ、信号

値及び変数値の少なくともいずれかが、補助記憶装置 932、メモリ 933、プロセッサ 931 内のレジスタ及びキャッシュメモリの少なくともいずれかに記憶される。

また、データ暗号化部 302、暗号化タグ生成部 303、タグ付き暗号化データ生成部 304、鍵管理部 305、検索クエリ生成部 306、データ復号部 307、許可ビット位置指定部 308、端末側データ送受信部 309 及び暗号化索引ビット列生成部 310 の機能を実現するプログラムは、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ（登録商標）ディスク、DVD 等の可搬記憶媒体に記憶されてもよい。

[0095] また、補助記憶装置 942 には、OS (Operating System) も記憶されている。

そして、OS の少なくとも一部がプロセッサ 941 により実行される。

プロセッサ 941 は OS の少なくとも一部を実行しながら、センタ側データ送受信部 402、保管要求処理部 403、開示ビット値復号部 405 及び検索処理部 406 の機能を実現するプログラムを実行する。

プロセッサ 941 が OS を実行することで、タスク管理、メモリ管理、ファイル管理、通信制御等が行われる。

また、センタ側データ送受信部 402、保管要求処理部 403、開示ビット値復号部 405 及び検索処理部 406 の処理の結果を示す情報、データ、信号値及び変数値の少なくともいずれかが、補助記憶装置 942、メモリ 943、プロセッサ 941 内のレジスタ及びキャッシュメモリの少なくともいずれかに記憶される。

また、センタ側データ送受信部 402、保管要求処理部 403、開示ビット値復号部 405 及び検索処理部 406 の機能を実現するプログラムは、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ブルーレイ（登録商標）ディスク、DVD 等の可搬記憶媒体に記憶されてもよい。

[0096] また、データ暗号化部 302、暗号化タグ生成部 303、タグ付き暗号化

データ生成部304、鍵管理部305、検索クエリ生成部306、データ復号部307、許可ビット位置指定部308、端末側データ送受信部309及び暗号化索引ビット列生成部310の「部」を、「回路」又は「工程」又は「手順」又は「処理」に読み替えてもよい。同様に、センタ側データ送受信部402、保管要求処理部403、開示ビット値復号部405及び検索処理部406の「部」を、「回路」又は「工程」又は「手順」又は「処理」に読み替えてもよい。

また、アクセス端末装置301及びデータセンタ装置401は、処理回路により実現されてもよい。処理回路は、例えば、ロジックIC(Integrated Circuit)、GA(Gate Array)、ASIC(Application Specific Integrated Circuit)、FPGA(Field-Programmable Gate Array)である。

この場合は、データ暗号化部302、暗号化タグ生成部303、タグ付き暗号化データ生成部304、鍵管理部305、検索クエリ生成部306、データ復号部307、許可ビット位置指定部308、端末側データ送受信部309及び暗号化索引ビット列生成部310は、それぞれ処理回路の一部として実現される。また、センタ側データ送受信部402、保管要求処理部403、開示ビット値復号部405及び検索処理部406も、それぞれ処理回路の一部として実現される。

なお、本明細書では、プロセッサと、メモリと、プロセッサとメモリの組合せと、処理回路との上位概念を、「プロセッシングサーキットリー」という。

つまり、プロセッサと、メモリと、プロセッサとメモリの組合せと、処理回路とは、それぞれ「プロセッシングサーキットリー」の具体例である。

符号の説明

[0097] 100 秘匿検索システム、101 ネットワーク、102 LAN、201 鍵管理サーバ装置、301 アクセス端末装置、302 データ暗号

化部、３０３ 暗号化タグ生成部、３０４ タグ付き暗号化データ生成部、
３０５ 鍵管理部、３０６ 検索クエリ生成部、３０７ データ復号部、３
０８ 許可ビット位置指定部、３０９ 端末側データ送受信部、３１０ 暗
号化索引ビット列生成部、４０１ データセンタ装置、４０２ センタ側デ
ータ送受信部、４０３ 保管要求処理部、４０４ データ記憶部、４０５
開示ビット値復号部、４０６ 検索処理部。

請求の範囲

- [請求項1] データ保管装置で保管される暗号化データの検索の際に索引として用いられるビット列を、前記暗号化データに関連付けて、索引ビット列として生成する索引ビット列生成部と、
- 前記索引ビット列の複数のビット値を、共通鍵方式の索引鍵を用いて暗号化する索引ビット列暗号化部と、
- 前記索引ビット列暗号化部により前記複数のビット値が暗号化された後の前記索引ビット列である暗号化索引ビット列と、前記暗号化データとを前記データ保管装置に送信する送信部とを有するデータ処理装置。
- [請求項2] 前記索引ビット列生成部は、
- 前記索引ビット列の生成過程において確定的暗号方式による暗号化を行って前記索引ビット列を生成する請求項1に記載のデータ処理装置。
- [請求項3] 前記索引ビット列暗号化部は、
- 前記索引ビット列の前記複数のビット値の各々を、異なる索引鍵を用いて暗号化する請求項1に記載のデータ処理装置。
- [請求項4] 前記索引ビット列暗号化部は、
- 前記索引ビット列の前記複数のビット値を、前記索引ビット列のビット数よりも少ない個数の索引鍵を用いて暗号化する請求項1に記載のデータ処理装置。
- [請求項5] 前記索引ビット列生成部は、
- 複数の暗号化データに関連付けて、複数の索引ビット列を生成し、
- 前記索引ビット列暗号化部は、
- 前記複数の索引ビット列の同じビット位置にあるビット値を同じ索引鍵を用いて暗号化する請求項1に記載のデータ処理装置。
- [請求項6] 前記送信部は、
- 前記暗号化索引ビット列と、前記暗号化データと、前記暗号化デー

タの検索の際に照合される暗号化されたタグである暗号化タグとを前記データ保管装置に送信する請求項 1 に記載のデータ処理装置。

[請求項7] 前記索引ビット列暗号化部は、

前記索引ビット列の複数のビット位置のうちビット値の開示が許可されるビット位置である許可ビット位置以外のビット位置にある暗号化されたビット値は、前記許可ビット位置のビット値の暗号化に用いられた索引鍵では復号されない暗号化方式にて、前記索引ビット列の前記複数のビット値を暗号化する請求項 1 に記載のデータ処理装置。

[請求項8] 前記データ処理装置は、更に、

前記送信部により前記データ保管装置に前記暗号化索引ビット列が送信され後に、前記許可ビット位置を指定する許可ビット位置指定部を有し、

前記送信部は、

前記許可ビット位置指定部により前記許可ビット位置が指定された後に、前記許可ビット位置のビット値の暗号化に用いられた索引鍵を前記データ保管装置に送信する請求項 7 に記載のデータ処理装置。

[請求項9] コンピュータが、データ保管装置で保管される暗号化データの検索の際に索引として用いられるビット列を、前記暗号化データに関連付けて、索引ビット列として生成し、

前記コンピュータが、前記索引ビット列の複数のビット値を、共通鍵方式の索引鍵を用いて暗号化し、

前記コンピュータが、前記複数のビット値が暗号化された後の前記索引ビット列である暗号化索引ビット列と、前記暗号化データとを前記データ保管装置に送信するデータ処理方法。

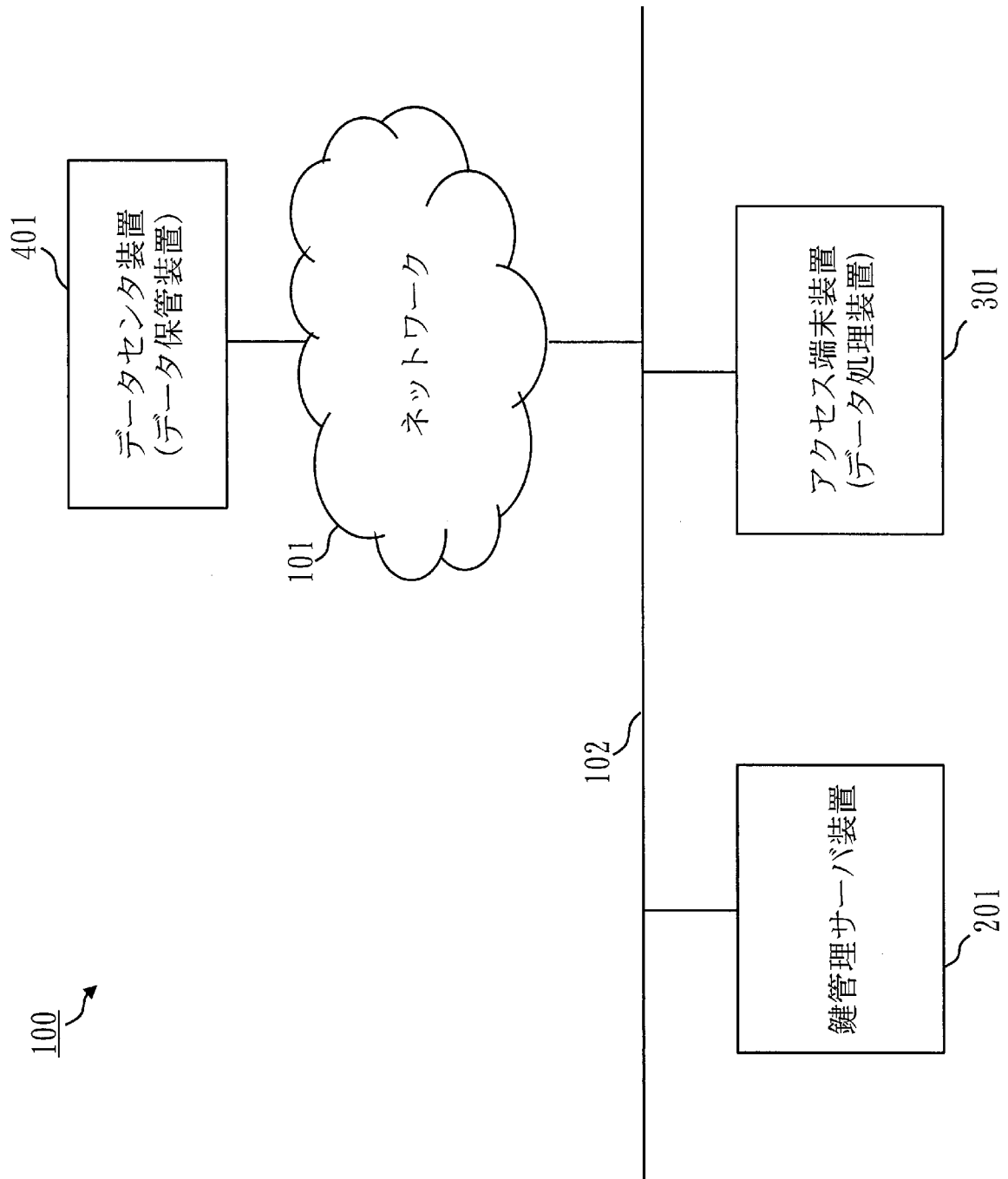
[請求項10] データ保管装置で保管される暗号化データの検索の際に索引として用いられるビット列を、前記暗号化データに関連付けて、索引ビット列として生成する索引ビット列生成処理と、

前記索引ビット列の複数のビット値を、共通鍵方式の索引鍵を用い

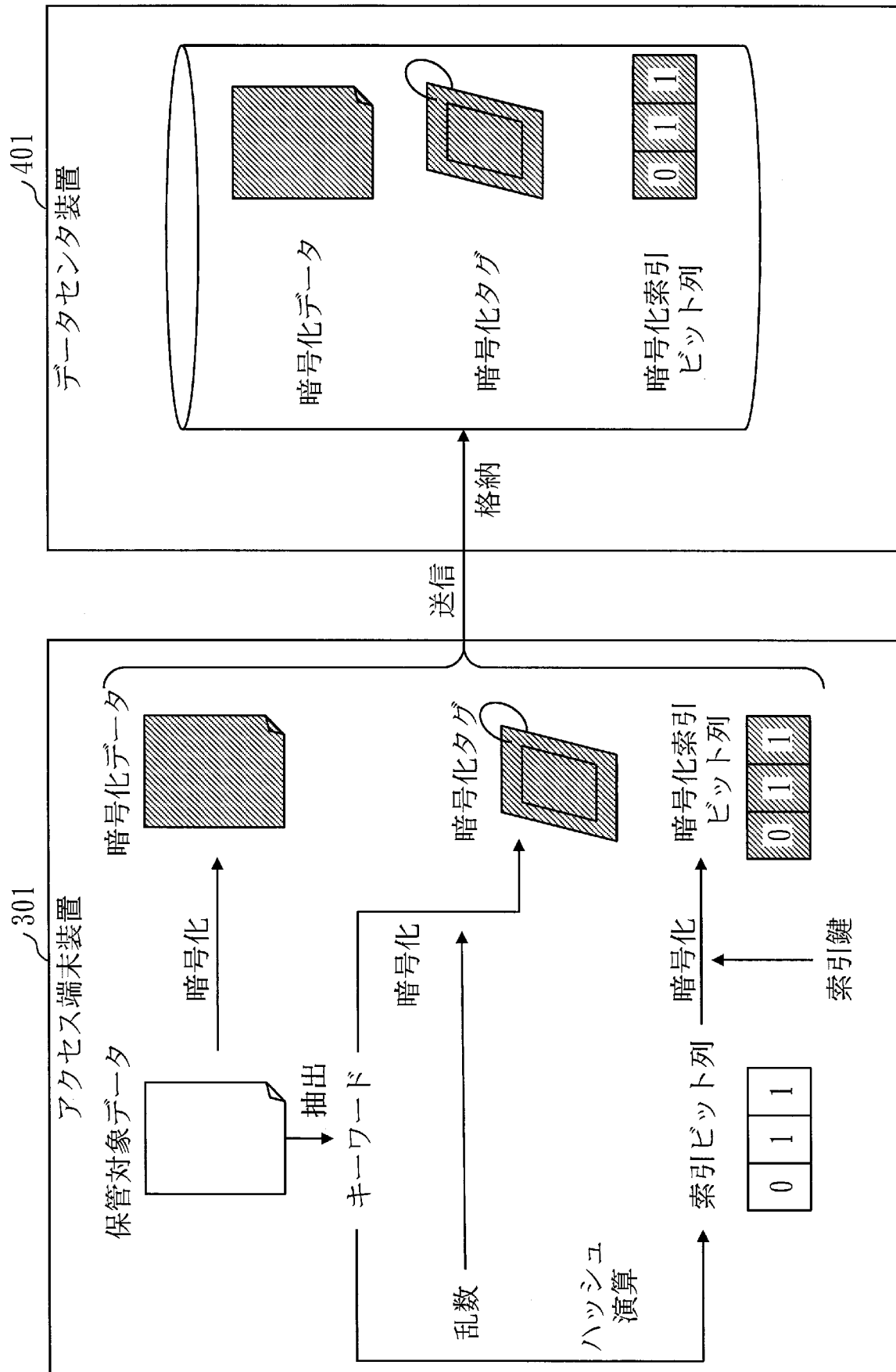
て暗号化する索引ビット列暗号化処理と、

前記索引ビット列暗号化処理により前記複数のビット値が暗号化された後の前記索引ビット列である暗号化索引ビット列と、前記暗号化データとを前記データ保管装置に送信する送信処理とをコンピュータに実行させるデータ処理プログラム。

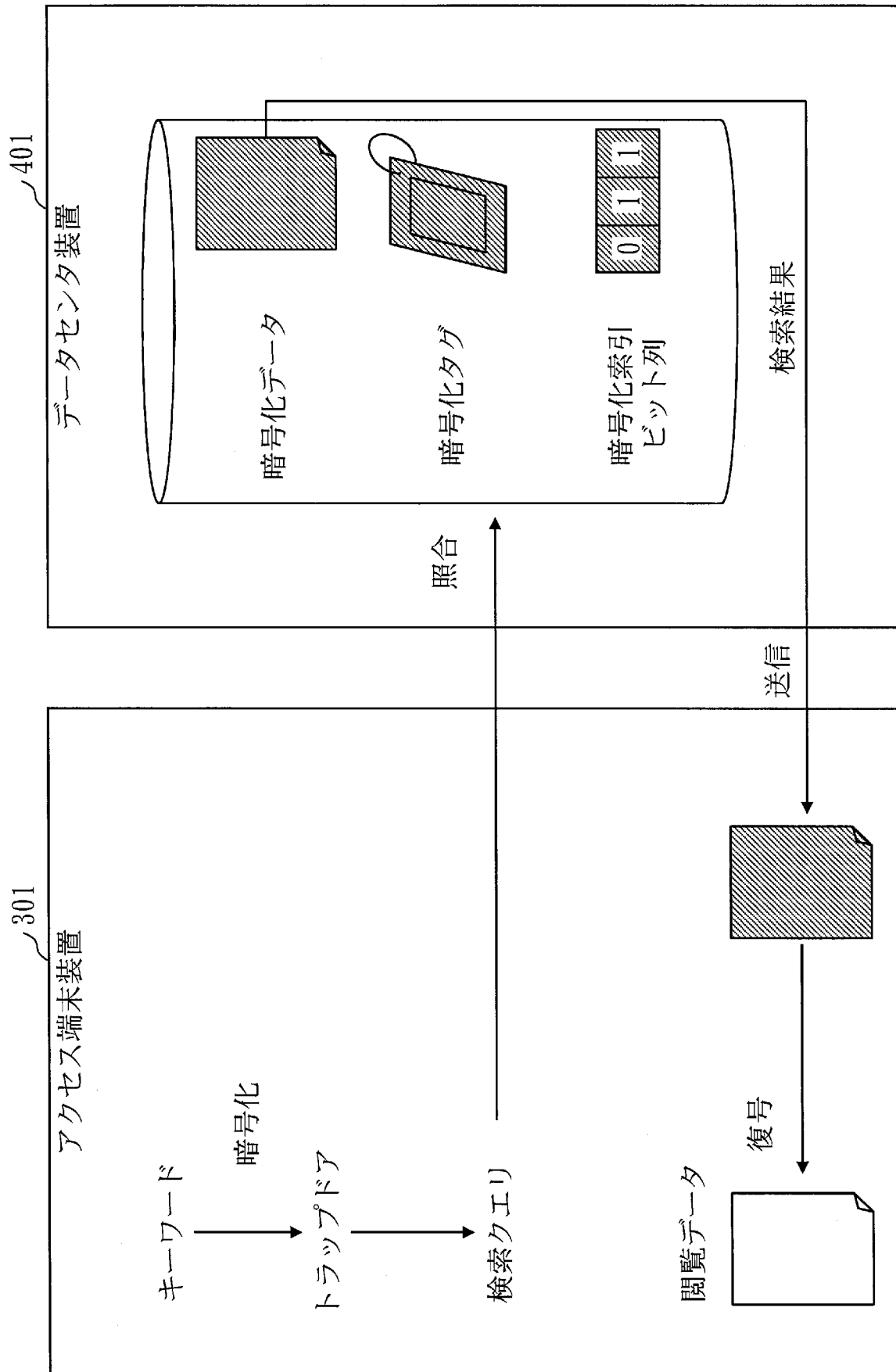
[図1]



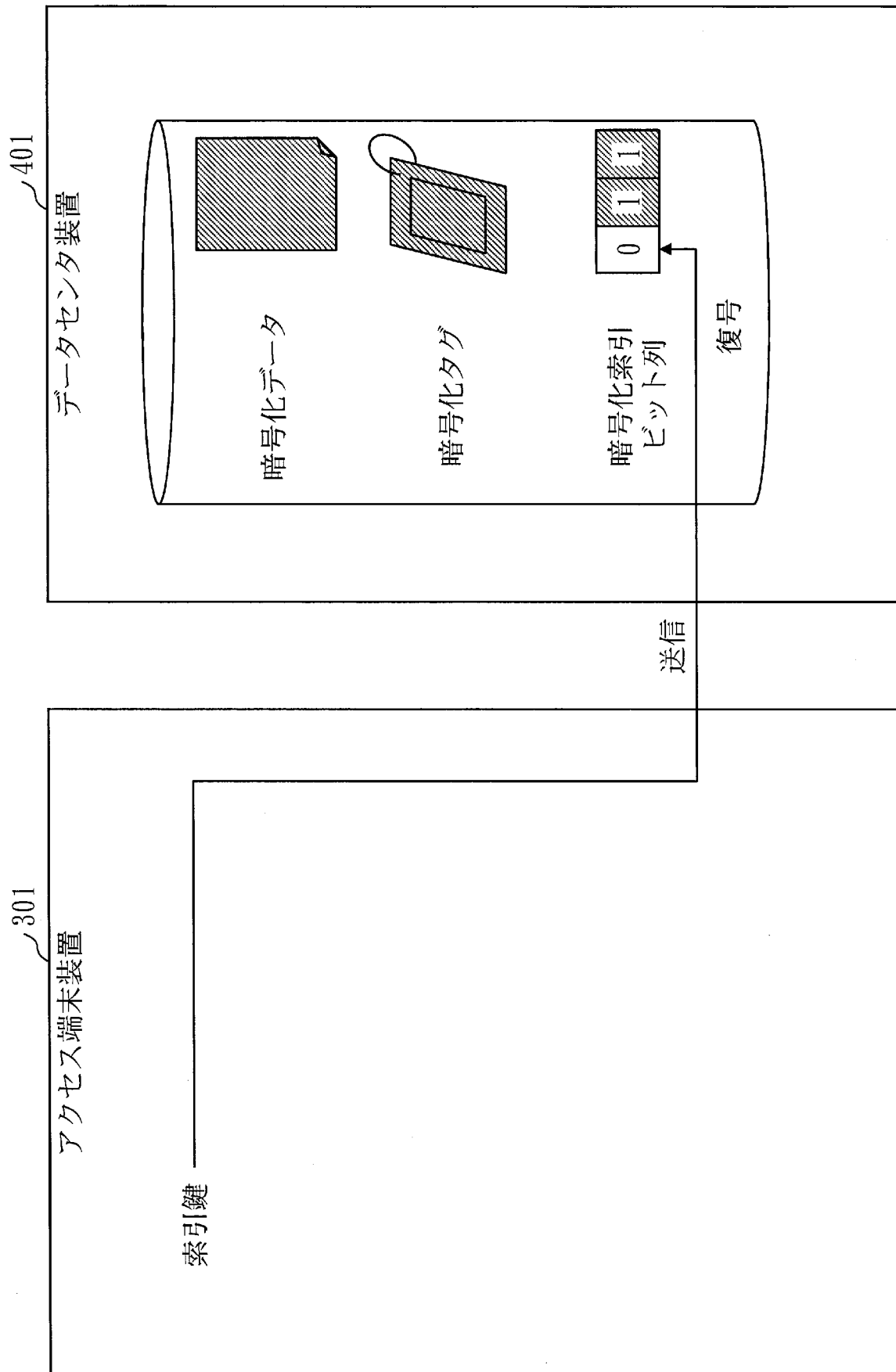
[図2]



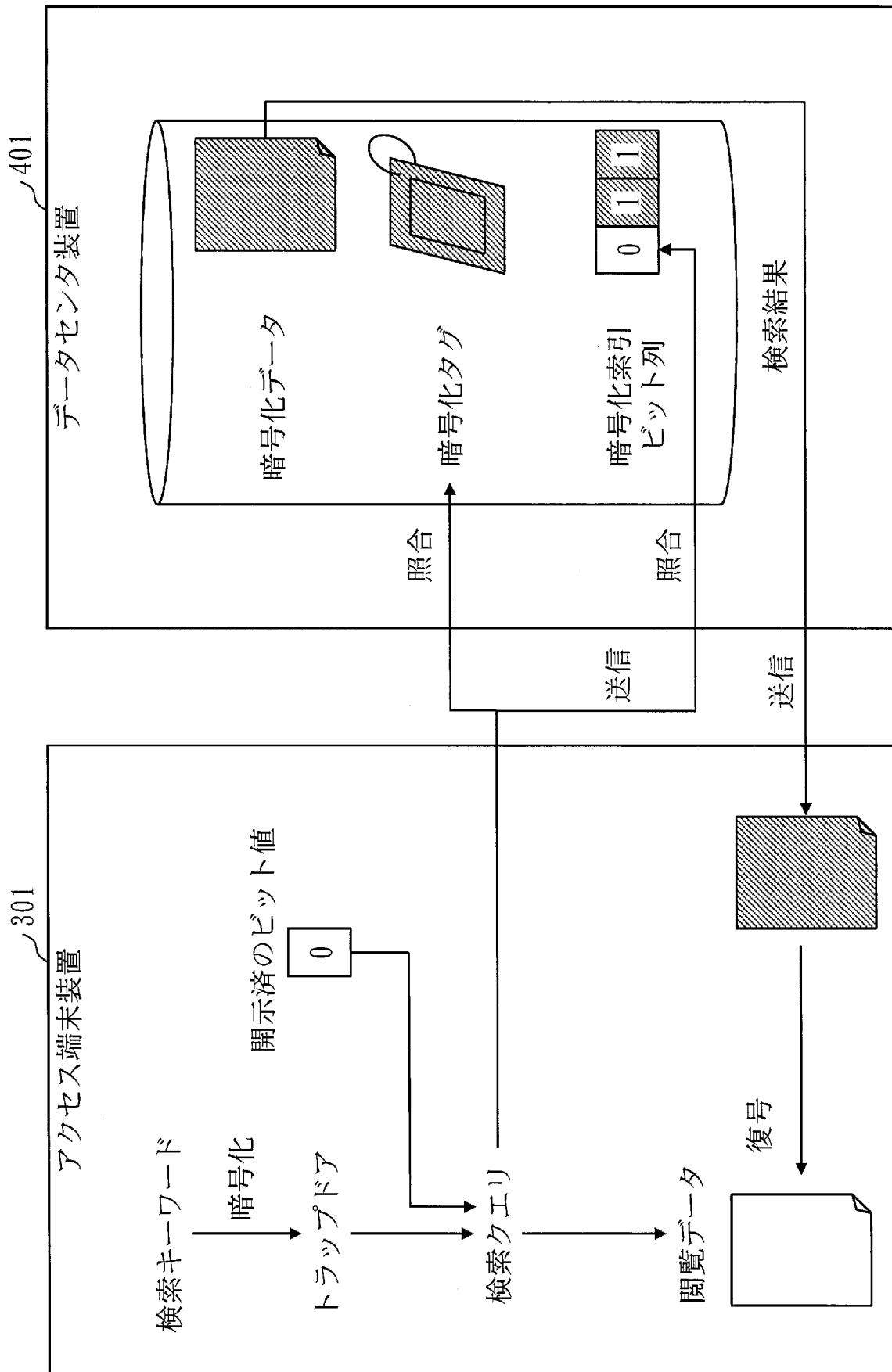
[図3]



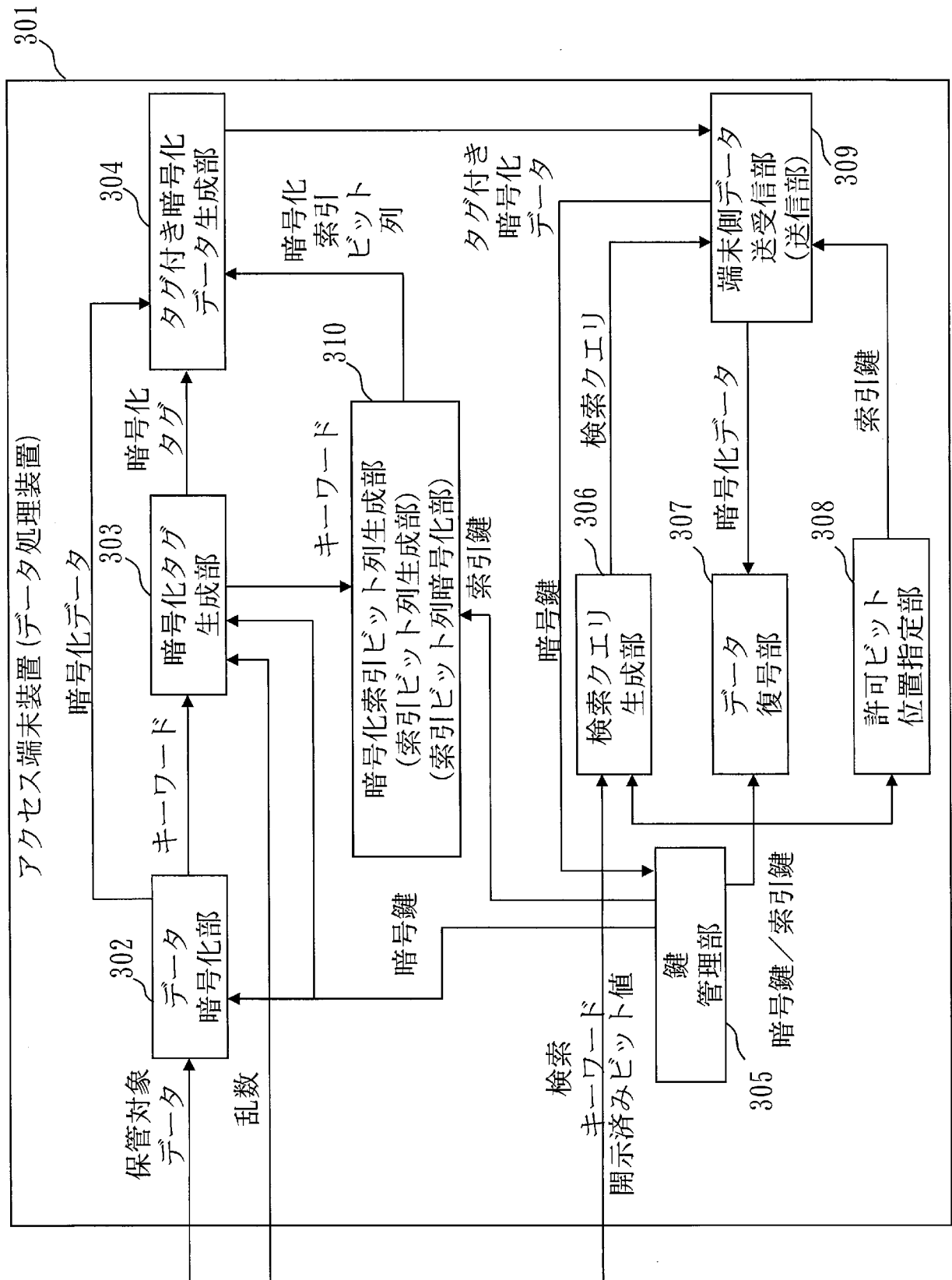
[図4]



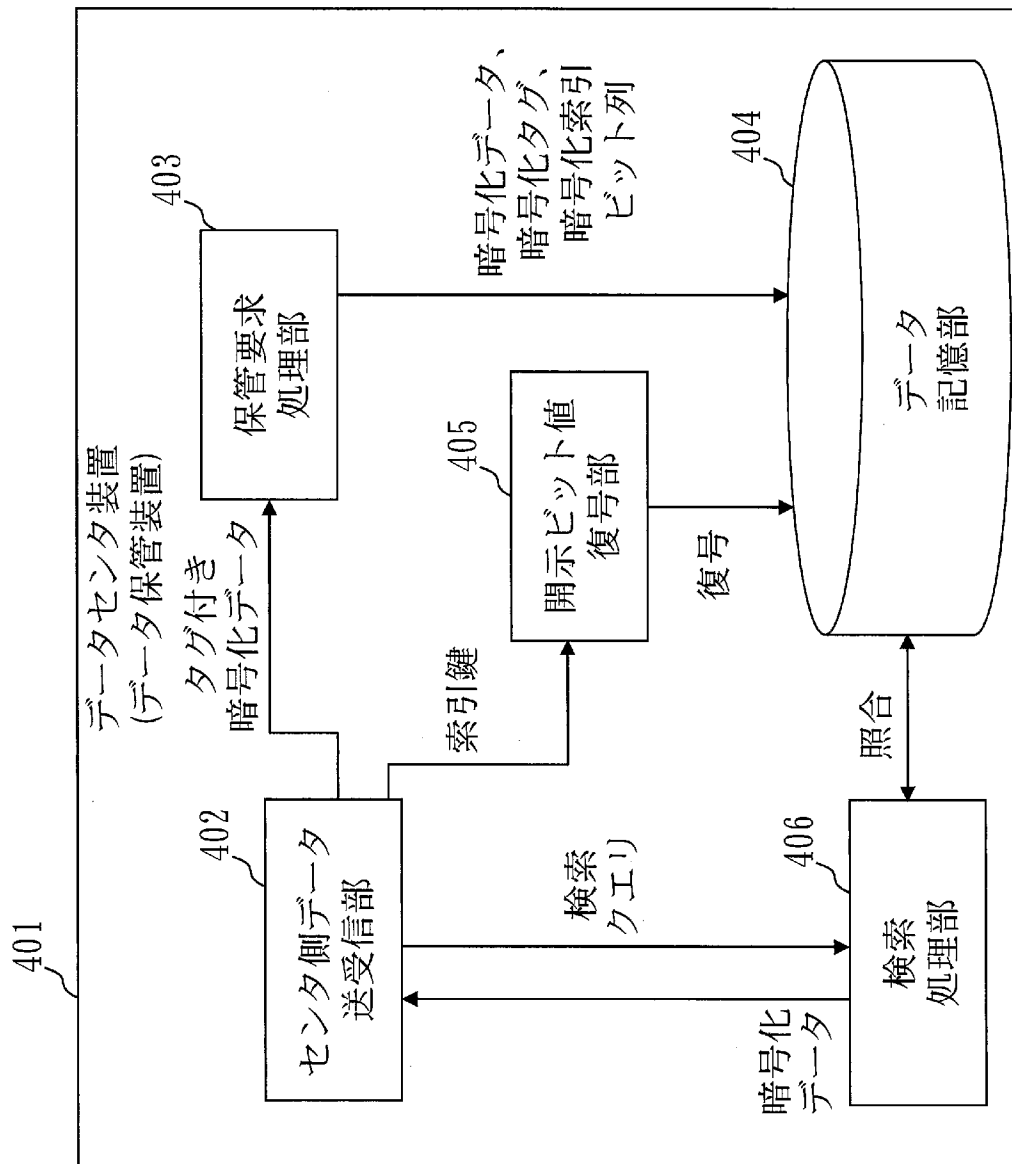
[図5]



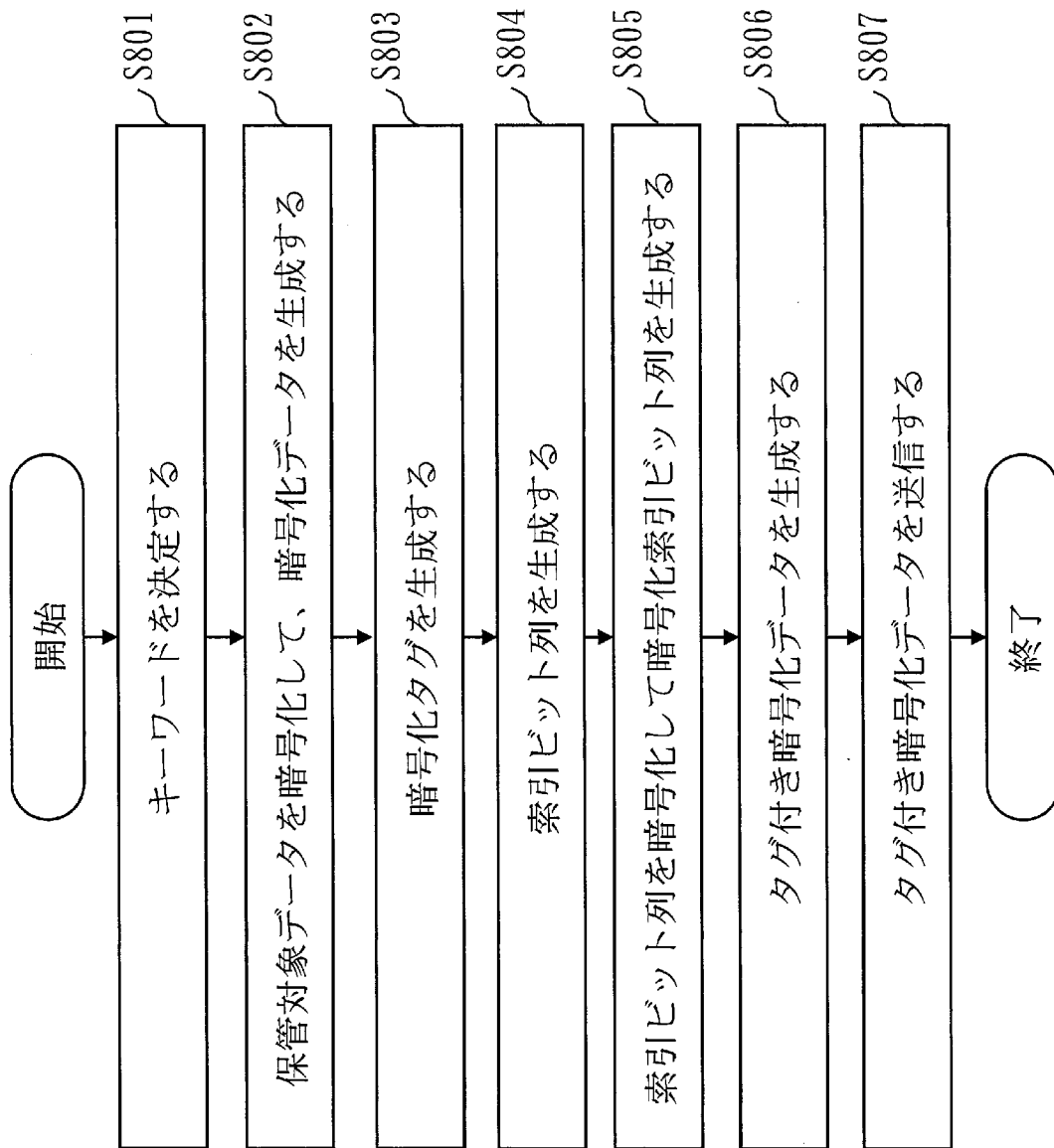
[図6]



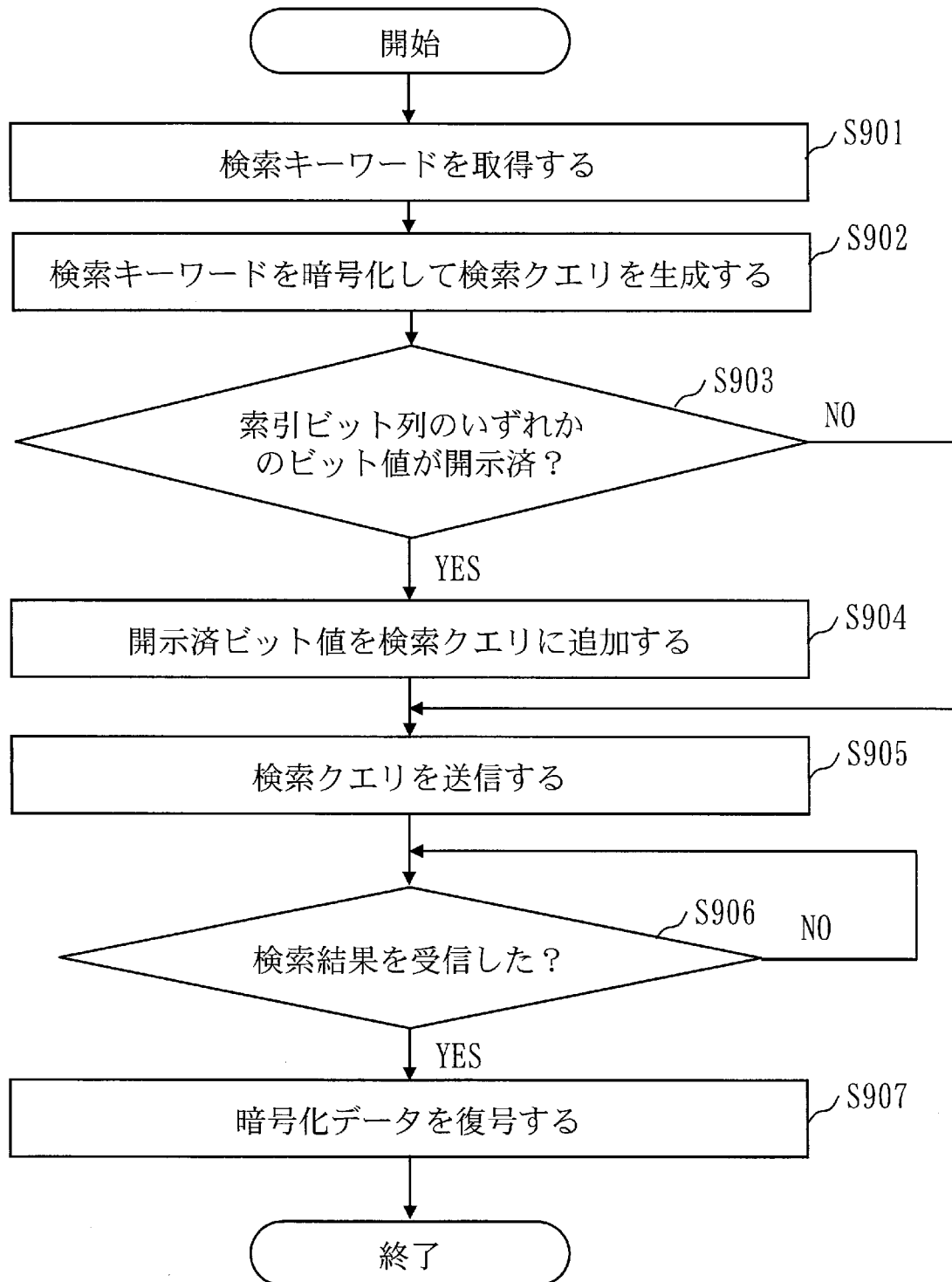
[図7]



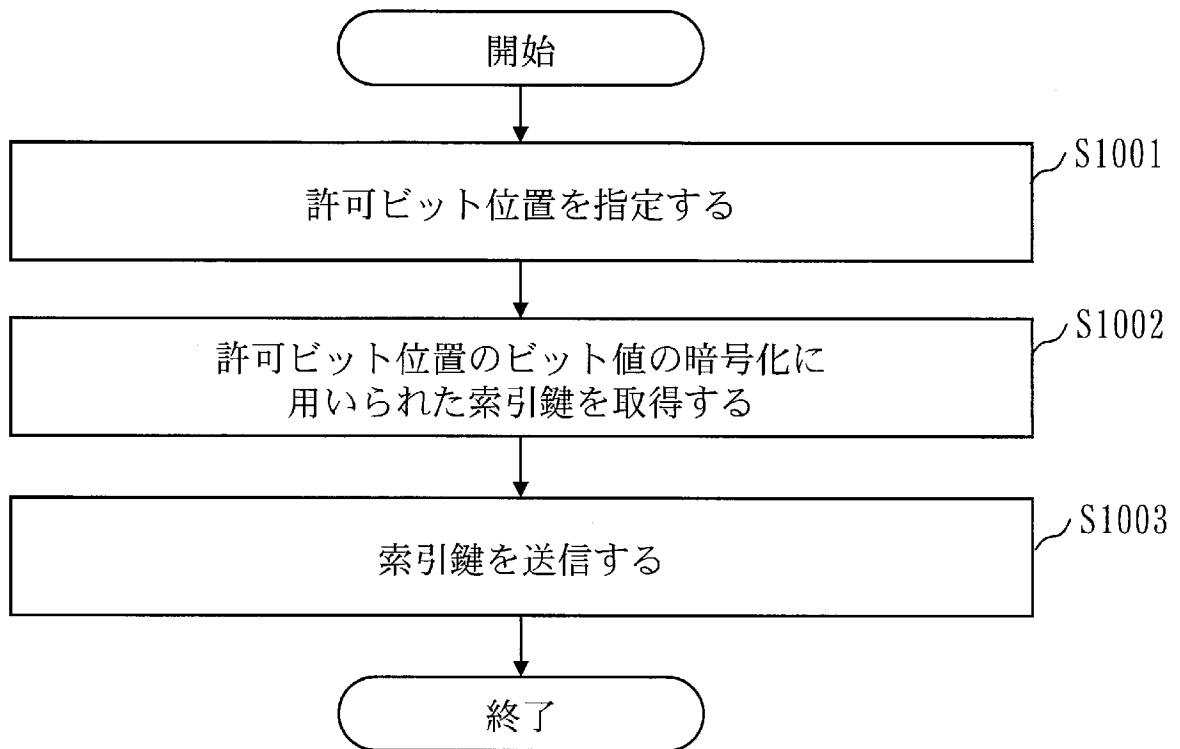
[図8]



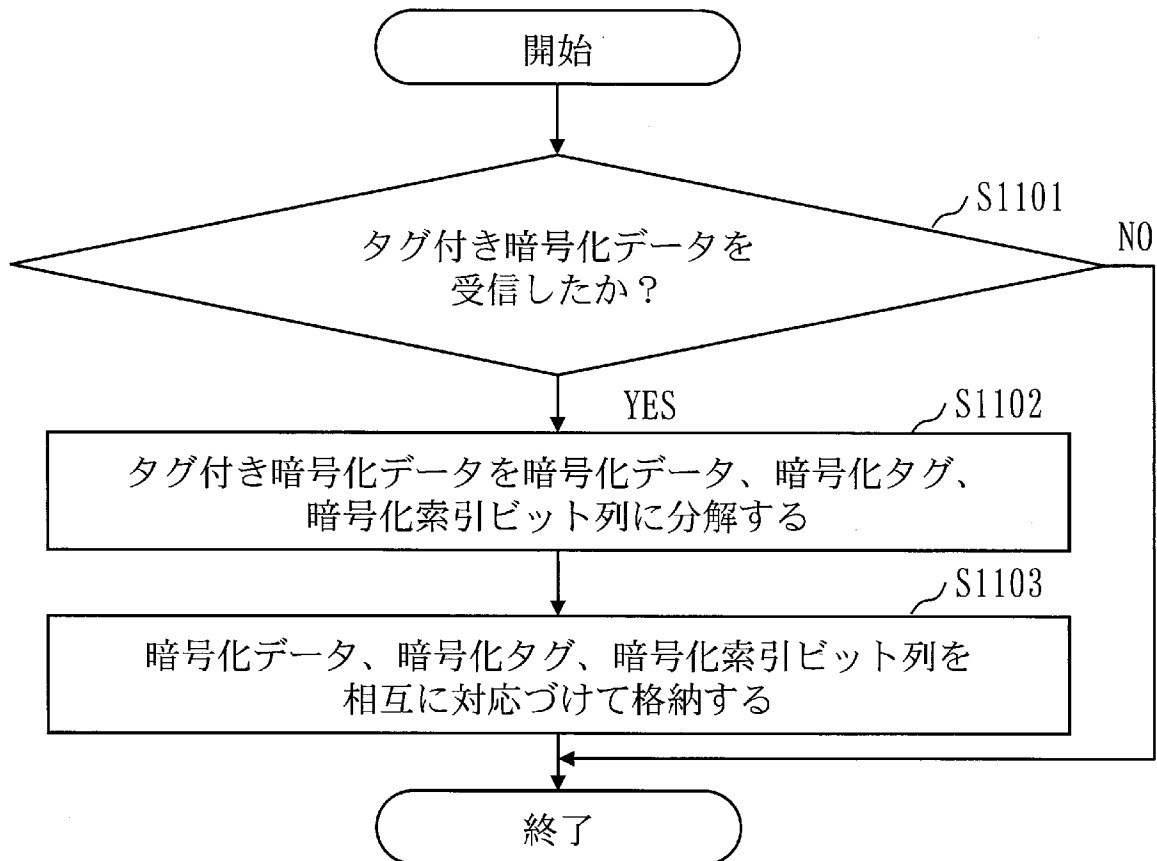
[図9]



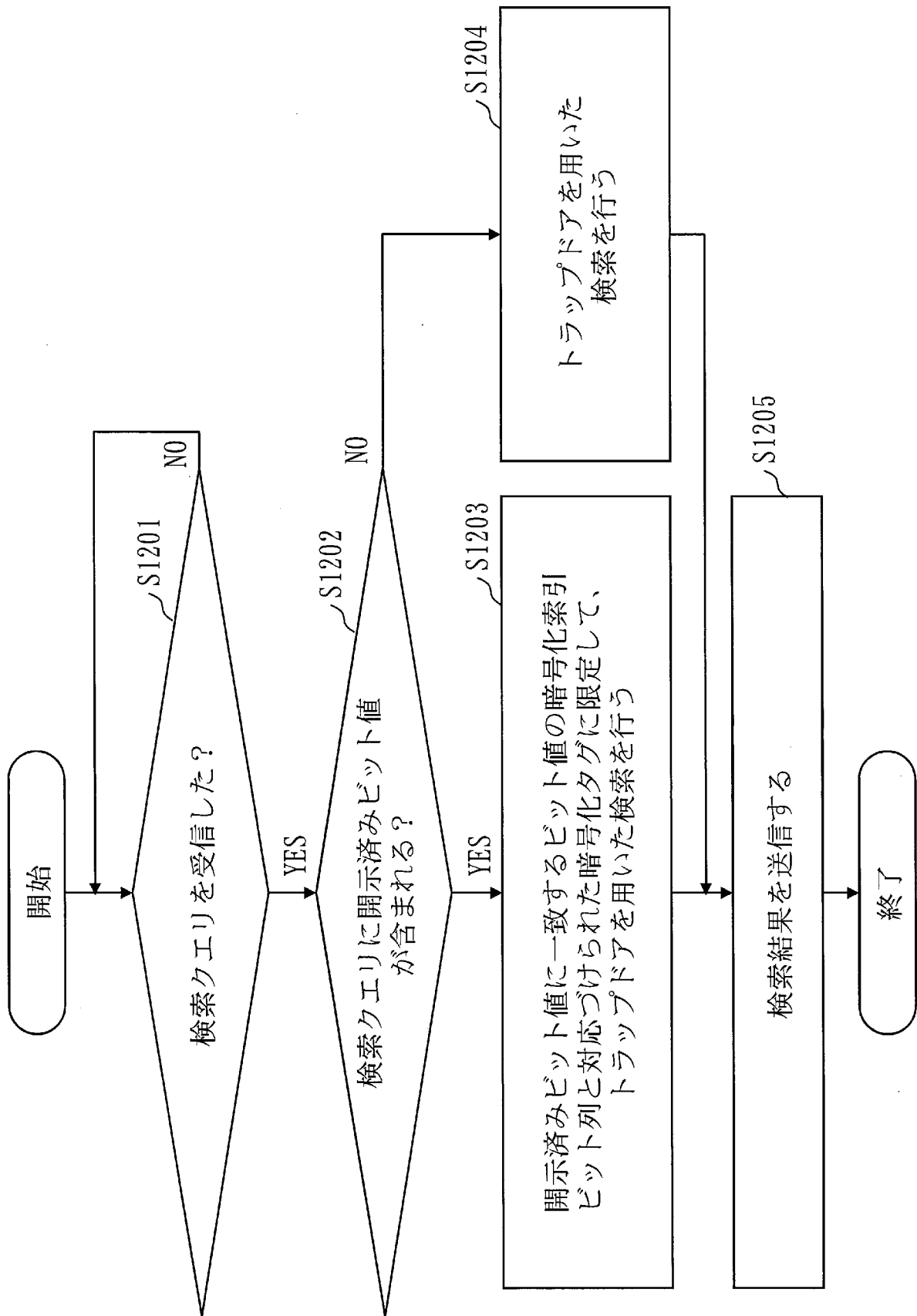
[図10]



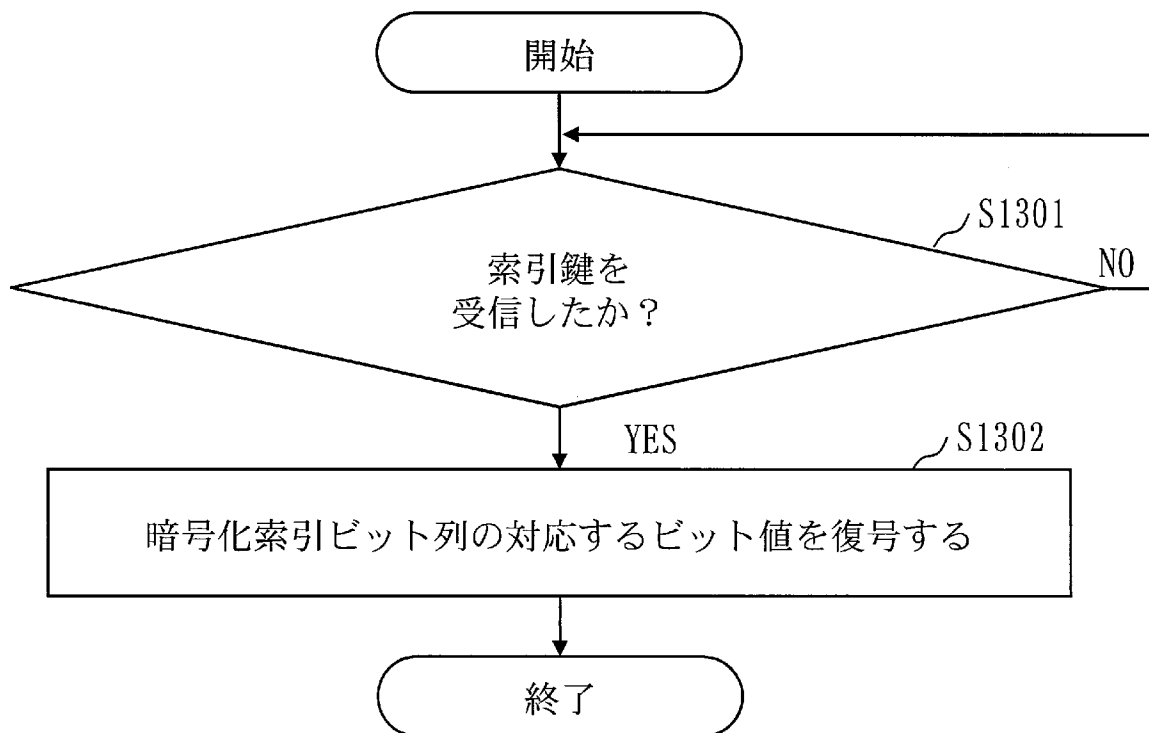
[図11]



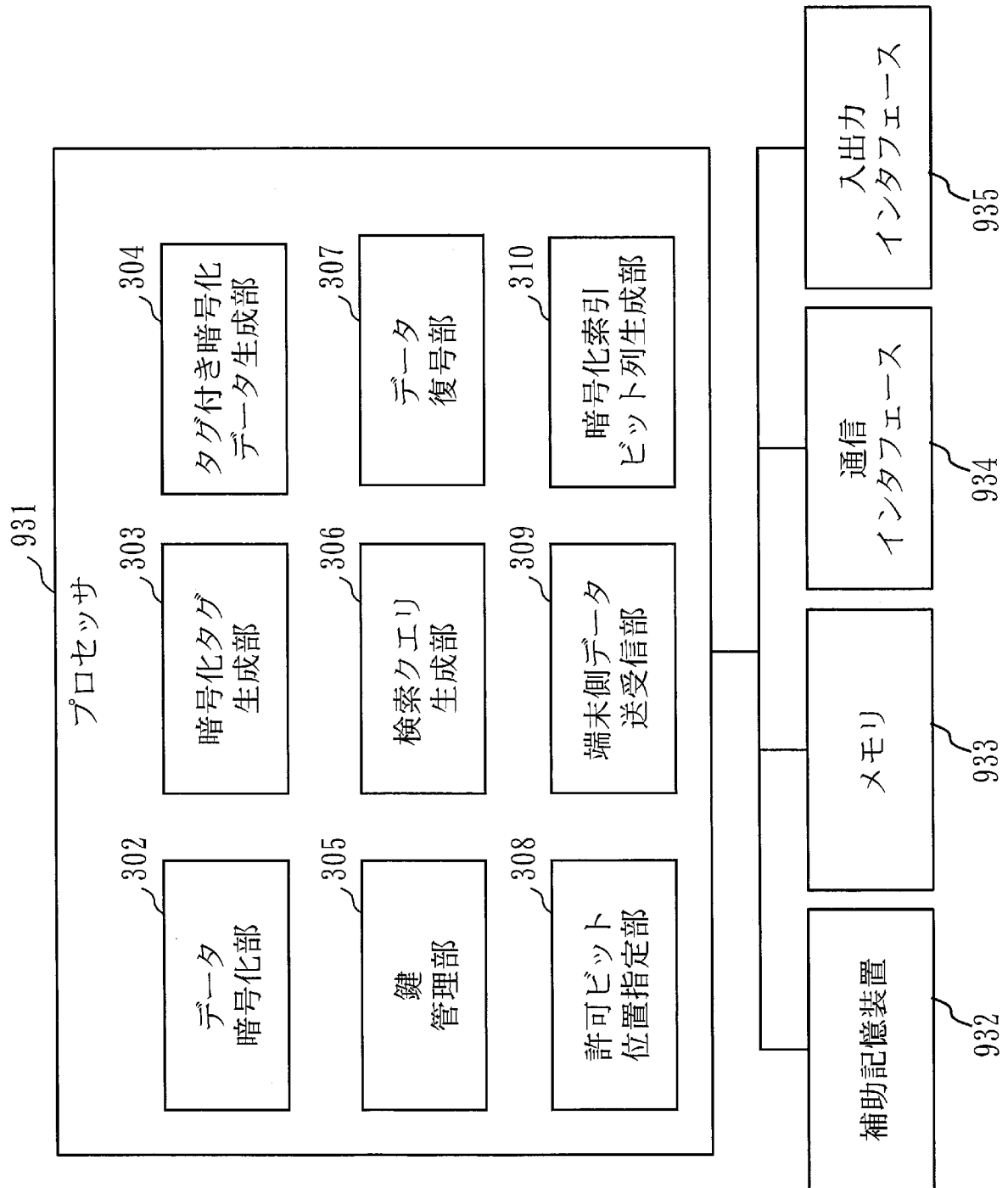
[図12]



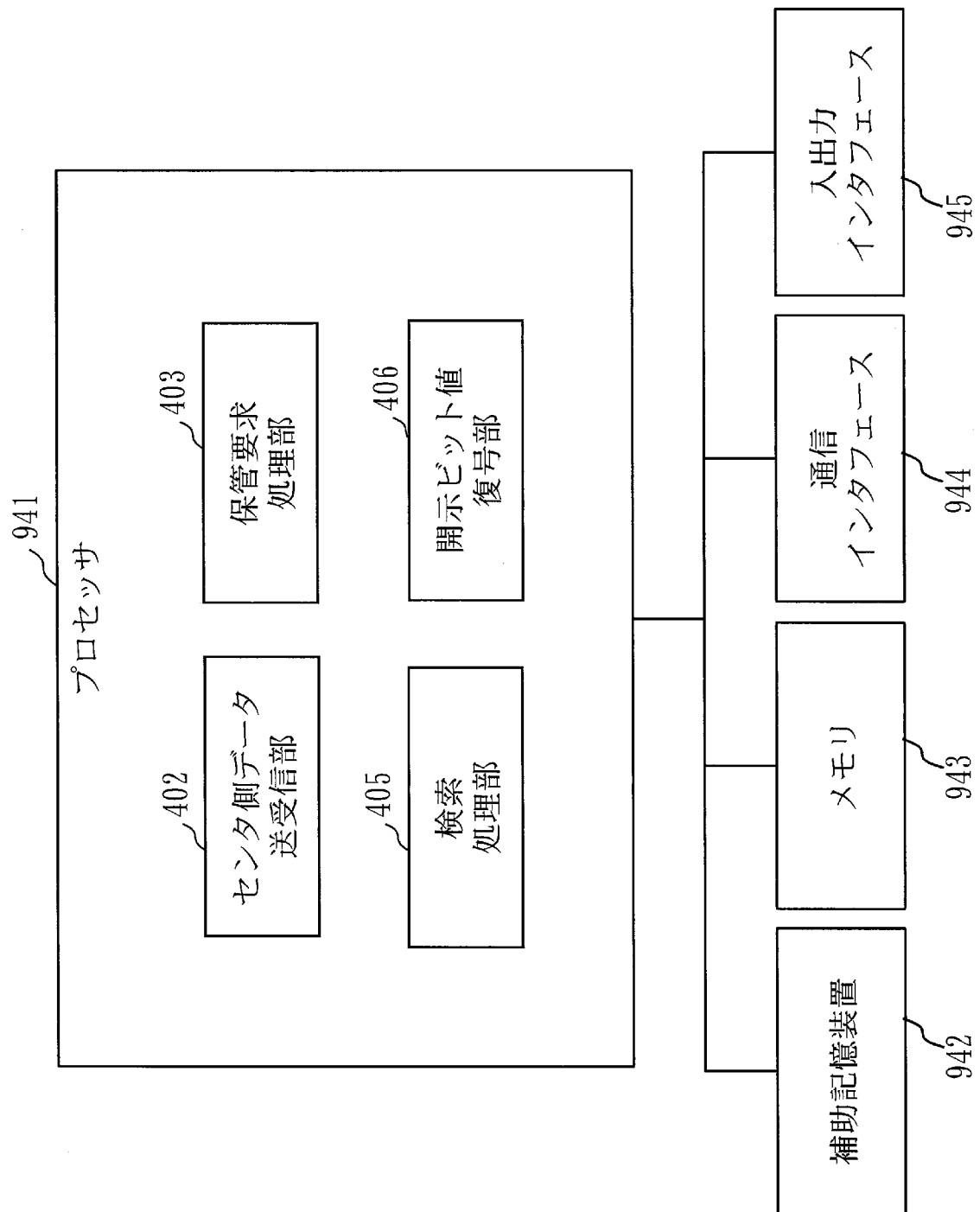
[図13]



[図14]



[図15]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2017/032919

A. CLASSIFICATION OF SUBJECT MATTER

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

Int. Cl. G09C1/00, G06F17/30

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

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2017

Registered utility model specifications of Japan 1996-2017

Published registered utility model applications of Japan 1994-2017

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	WO 2012/095973 A1 (MITSUBISHI ELECTRIC CORP.) 19 July 2012, paragraphs [0027]-[0161] & US 2013/0287210 A1, paragraphs [0105]-[0528] & EP 2665052 A1 & CN 103329184 A	1-10
A	松田規ほか, 安全性と高速性の両立を目指した検索可能暗号 (1), 2012 年暗号と情報セキュリティシンポジウム予稿集, 30 January 2012, pp. 1-6, non-official translation (MATSUDA, Nori et al. Retrievable Encryption Aimed at Balancing Safety and Speed (1). Proceedings of the 2012 Symposium on Cryptography and Information Security.)	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
30.11.2017

Date of mailing of the international search report
12.12.2017

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/JP2017/032919

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	松田規ほか, 検索可能暗号の高速化と Web アプリケーションへの適用方式に関する提案, マルチメディア, 分散, 協調とモバイル (DICOMO2013) シンポジウム論文集, 情報処理学会シンポジウムシリーズ, vol. 2013, no. 2, 03 July 2013, pp. 2067-2073 (MATSUDA, Nori et al. Efficient Searchable Encryption and Its Application to Web Services. Multimedia, Distributed, Cooperative, and Mobile Symposium (DICOMO2013). IPSJ Symposium Series.)	1-10
A	JP 2007-52698 A (KDDI CORP.) 01 March 2007, paragraphs [0013]-[0031] (Family: none)	1-10
A	JP 2010-503118 A (MICROSOFT CORP.) 28 January 2010, paragraphs [0021]-[0023] & US 2008/0059414 A1, paragraphs [0026]-[0028] & WO 2008/030717 A1 & EP 2064638 A1	1-10

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G09C1/00(2006.01)i, 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（I P C））

Int.Cl. G09C1/00, 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	1971-2017年
日本国実用新案登録公報	1996-2017年
日本国登録実用新案公報	1994-2017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	WO 2012/095973 A1（三菱電機株式会社） 2012.07.19, 段落 [0027] - [0161] & US 2013/0287210 A1, 段落 [0105] - [0528] & EP 2665052 A1 & CN 103329184 A	1-10
A	松田規ほか, 安全性と高速性の両立を目指した検索可能暗号（1）, 2012年 暗号と情報セキュリティシンポジウム予稿集, 2012.01.30, p.1-6	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

30.11.2017

国際調査報告の発送日

12.12.2017

国際調査機関の名称及びあて先

日本国特許庁（I S A / 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）

行田 悦資

5 S

6304

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	松田規ほか, 検索可能暗号の高速化とWebアプリケーションへの適用方式に関する提案, マルチメディア, 分散, 協調とモバイル (DI COMO 2013) シンポジウム論文集, 情報処理学会シンポジウムシリーズ, Vol.2013, No. 2, 2013.07.03, p.2067-2073	1-10
A	JP 2007-52698 A (KDD I 株式会社) 2007.03.01, 段落 [0013] - [0031] (ファミリーなし)	1-10
A	JP 2010-503118 A (マイクロソフト コーポレーション) 2010.01.28, 段落 [0021] - [0023] & US 2008/0059414 A1, 段落 [0026] - [0028] & WO 2008/030717 A1 & EP 2064638 A1	1-10