(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-112773
(P2020-112773A)
(43)公開日　令和2年7月27日(2020.7.27)

(51)Int.Cl.		F I		テーマコード（参考）
G09C 1/00	(2006.01)	G09C 1/00	660D	
G06F 21/60	(2013.01)	G06F 21/60	320	
G06F 16/901	(2019.01)	G06F 16/901		

審査請求 未請求　請求項の数 6　OL　（全 16 頁）

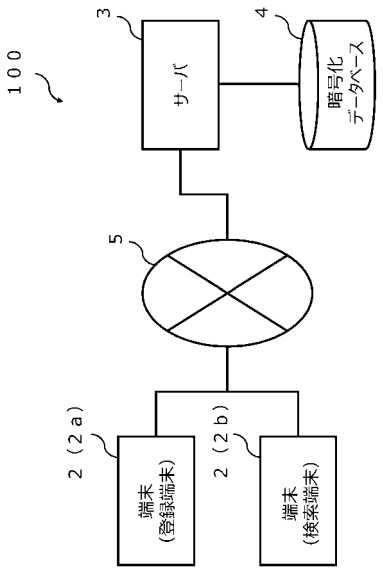
(21)出願番号　特願2019-111977 (P2019-111977)
(22)出願日　令和1年6月17日 (2019.6.17)
(31)優先権主張番号　特願2019-3908 (P2019-3908)
(32)優先日　平成31年1月11日 (2019.1.11)
(33)優先権主張国・地域又は機関
日本国 (JP)

(71)出願人　301022471
国立研究開発法人情報通信研究機構
東京都小金井市貫井北町４－２－１
(71)出願人　504133110
国立大学法人電気通信大学
東京都調布市調布ケ丘一丁目５番地１
(74)代理人　100120868
弁理士　安彦　元
(72)発明者　渡邊　洋平
東京都小金井市貫井北町４－２－１　国立研究開発法人情報通信研究機構内
(72)発明者　岩本　貢
東京都調布市調布ケ丘一丁目５番地１　国立大学法人電気通信大学内

最終頁に続く

(54)【発明の名称】動的検索可能暗号処理システム

(57)【要約】
【課題】効率性を向上させることができ、フォワード安全性を満たすようなことができる、動的検索可能暗号処理システムを提供する。
【解決手段】文書ファイルに対応する識別子とキーワードとの関係を示す参照テーブルから、前記文書ファイルに含まれる前記キーワードを抽出キーワードとして抽出し、前記文書ファイルに対応する識別子を抽出識別子として抽出し、前記抽出手段により抽出された前記抽出キーワードと前記抽出識別子とを連結させ、１組としたアドレスと、前記アドレスに含まれる前記抽出識別子を格納部とした関係を示す第１テーブルを生成し、前記第１テーブルにおける前記アドレスを擬似乱数生成関数により乱数化情報に変換して変換アドレスを生成し、前記変換アドレス手段により変換された前記変換アドレスと前記格納部との関係を示す第２テーブルを生成する。
【選択図】図１



【特許請求の範囲】
【請求項１】
端末とサーバがネットワークを介して接続され、暗号化されたデータテーブルを用いた動的検索可能暗号システムであって、
文書ファイルに対応する識別子とキーワードとの関係を示す参照テーブルから、前記文書ファイルに含まれる前記キーワードを抽出キーワードとして抽出するとともに、前記文書ファイルに対応する識別子を抽出識別子として抽出する抽出手段と、
前記抽出手段により抽出された前記抽出キーワードと前記抽出識別子とを連結させ、１組としたアドレス情報と、前記アドレス情報に含まれる前記抽出識別子との関係を示す第１テーブルを生成する第１テーブル生成手段と、
前記第１テーブルにおける前記アドレスを擬似乱数生成関数により乱数化情報に変換して変換アドレスを生成し、前記変換アドレスと前記抽出識別子との関係を示す第２テーブルを生成する第２テーブル生成手段と、
を備えること
を特徴とする動的検索可能暗号システム。
【請求項２】
前記第２テーブル生成手段は、
前記端末が保持する疑似乱数生成関数に関する鍵情報、前記端末が保持するステート情報に基づき、前記抽出識別子を初期化した第２テーブルを生成し、前記鍵情報と前記ステート情報の記憶後に、前記生成した前記第２テーブルを前記サーバに送信すること、
を特徴とする請求項１記載の動的検索可能暗号システム。
【請求項３】
前記端末は、
追加する文書ファイルに対応する識別子とキーワードとの関係を示す参照テーブルから、前記文書ファイルに含まれる前記キーワードを抽出キーワードとして抽出するとともに、前記文書ファイルに対応する識別子を抽出識別子として抽出し、前記抽出した前記抽出キーワードと前記抽出識別子とを連結させ、１組としたアドレス情報と、前記アドレス情報に含まれる前記抽出識別子との関係を示す第１テーブルを生成し、前記アドレスを擬似乱数生成関数により乱数化情報に変換して変換追加アドレスを生成し、前記抽出識別子をステート情報に記憶し、前記変換アドレスと前記抽出識別子を前記サーバに送信し、
前記サーバは、
前記端末により送信された前記変換アドレスを受信し、前記変換アドレスの乱数化情報のそれぞれが示すアドレスに、前記受信した前記抽出識別子を格納し、前記第２テーブルを更新すること、
を特徴とする請求項１又は２のいずれかに記載の動的検索可能暗号システム。
【請求項４】
前記端末は、
削除する文書ファイルに対応する前記抽出識別子を、前記ステート情報から削除し、前記削除した前記抽出識別子を前記サーバに送信し、
前記サーバは、
前記端末により送信された前記抽出識別子を受信し、前記サーバの第２テーブルで前記抽出識別子に対応する全ての格納領域をＮＵＬＬに変換し、前記第２テーブルを更新すること、
を特徴とする請求項１～３のいずれかに記載の動的検索可能暗号システム。
【請求項５】
前記第２テーブル生成手段は、
追加する文書ファイルと同じ大きさの文書ファイルのうち、最も多い抽出キーワードを含むことができる文書ファイルを特定し、前記追加文書ファイルに対応する変換アドレスの個数が、前記特定した文書ファイルに含まれる抽出キーワード数となるまで、ダミーフラグを示す識別情報と、カウンタ情報と、前期追加文書ファイルの抽出識別子とを連結さ

せ、１組のダミーアドレス情報とし、前期ダミーアドレス情報を疑似乱数生成関数により乱数化情報に変換して変換ダミーアドレスを生成し、前記変換ダミーアドレス情報が指し示すアドレスに前記抽出識別子を格納すること、を繰り返し、前記第２テーブルを生成すること、を特徴とする請求項１～４のいずれかに記載の動的検索可能暗号システム。
【請求項６】
前記端末は、
検索するキーワードと前記ステート情報に含まれる各識別子を検索識別子として連結させ、１組としたアドレス情報と、前記アドレス情報を擬似乱数生成関数により乱数化情報に変換して変換アドレスを生成し、前記変換アドレスを前記サーバに送信し、
前記サーバは、
前記端末により送信された前記変換アドレスを受信し、前記サーバの第２テーブルで前記変換アドレスに対応する全ての格納領域を参照し、前記格納領域がＮＵＬＬではなく、所定の識別子が格納される格納先の抽出識別子を取得し、前記端末に送信すること、
を特徴とする請求項１～５のいずれかに記載の動的検索可能暗号システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、端末とサーバがネットワークを介して接続され、暗号化されたデータテーブルを用いた動的検索可能暗号システムに関する。
【背景技術】
【０００２】
近年、クラウドサービスの普及により、企業等はオンラインストレージ等の外部ストレージサービスを利用し、社内における膨大な文書ファイルを管理サーバ（クラウドサーバ）上で保存・管理させる事例が増加しつつある。管理サーバ上に保存・管理される文書ファイルは、管理サーバ上に保存される前に暗号化される。そして、暗号化された文書ファイルは、外部ストレージサービスで提供される管理サーバの暗号化データベースに保存される。暗号化された文書ファイルは、暗号化されたままの状態でキーワード検索することが可能であり、このような暗号化処理技術は検索可能暗号（Searchable Symmetric Encryption：SSE）として知られている。
【０００３】
さらに、検索可能暗号の中でも、管理サーバ上の暗号化データベースに保存された暗号化文書ファイルに対して、任意のタイミングで暗号化文書ファイルを追加及び削除等の動的な更新を可能にする研究が進められており、動的検索可能暗号（Dynamic Searchable Symmetric Encryption：DSSE）として知られている。
【０００４】
動的検索暗号では、管理サーバ上に保存された暗号化データベース上のファイルに対してキーワード検索を行えることができることに加え、プロトコルの途中であっても、ファイル及びそれに付随するキーワードの暗号化データベースへの追加や削除が可能となる。以前より、最も強い安全性（例えば、検索を何度実行しても、検索データベース上のファイルについて全く情報が漏れない）を満たすためには、理論的に非効率な方法でしか実現できないことが知られていたため、最低限満たすべき安全性（例えば、検索回数に応じて、多少の本質的ではない情報の漏洩を許す）を満たした上で効率的な方式の研究が行われ、さらに、最低限満たすべき安全性に加え、フォワード安全性（新たに追加されたファイルに、過去に検索されたキーワードが含まれていることが漏れない）を満たす方式が知られている（例えば、非特許文献１参照）。
【０００５】
非特許文献１の開示技術では、端末側でキーワードに関する情報（各キーワードのこれまでの検索回数、各キーワードを含むファイルの数）をステート情報として保持し、ステート情報を利用して、暗号化インデックステーブルのアドレス部を作成することを特徴としており、アドレス部の生成はサーバ側で行う。なお、暗号化インデックステーブルへの

ダミーエントリの追加方法については開示されていない。
【先行技術文献】
【非特許文献】
【０００６】
【非特許文献１】M.Etemad、A.Kupcu、C.Papamanthou、D.Evans、「Efficient dynamic searchable encryption with forward privacy」、In Proceedings of Privacy Enhancing Technologies (PoPETs)、2018年、p.5-20
【発明の概要】
【発明が解決しようとする課題】
【０００７】
非特許文献１の開示技術では、端末側でキーワードに関する情報をステート情報として保持する必要があり、ステート情報は端末が保持するキーワード数に依存するため、対象データの大きさの効率性に問題があった。また、アドレス部の生成をサーバ側で行うため、フォワード安全性を達成するためには検索時にアドレス部の再登録が必要である。本来は検索の処理だけのところを、検索と再登録の２つの処理が必要となるため、再登録の操作や処理の分だけ操作が発生し、効率性を低下させることになる。さらに、暗号化インデックステーブルへのダミーエントリの追加方法は不明であり、より強い、現実的な状況に整合した安全性を達成できるか不明である。
【０００８】
そこで、本発明は、上述した問題点に鑑みて案出されたものであり、その目的とするところは、効率性を向上させることができ、フォワード安全性を満たすようなことができる、動的検索可能暗号処理システムを提供することにある。
【課題を解決するための手段】
【０００９】
第１発明に係る動的検索可能暗号処理システムは、端末とサーバがネットワークを介して接続され、暗号化されたデータテーブルを用いた動的検索可能暗号システムであって、文書ファイルに対応する識別子とキーワードとの関係を示す参照テーブルから、前記文書ファイルに含まれる前記キーワードを抽出キーワードとして抽出するとともに、前記文書ファイルに対応する識別子を抽出識別子として抽出する抽出手段と、前記抽出手段により抽出された前記抽出キーワードと前記抽出識別子とを連結させ、１組としたアドレス情報と、前記アドレス情報に含まれる前記抽出識別子との関係を示す第１テーブルを生成する第１テーブル生成手段と、前記第１テーブルにおける前記アドレスを擬似乱数生成関数により乱数化情報に変換して変換アドレスを生成し、前記変換アドレスと前記抽出識別子との関係を示す第２テーブルを生成する第２テーブル生成手段と、を備えることを特徴とする。
【００１０】
第２発明に係る動的検索可能暗号処理システムは、第１発明において、前記第２テーブル生成手段は、前記端末が保持する疑似乱数生成関数に関する鍵情報、前記端末が保持するステート情報に基づき、前記抽出識別子を初期化した第２テーブルを生成し、前記鍵情報と前記ステート情報の記憶後に、前記生成した前記第２テーブルを前記サーバに送信すること、を特徴とする。
【００１１】
第３発明に係る動的検索可能暗号処理システムは、第１発明又は第２発明において、前記端末は、追加する文書ファイルに対応する識別子とキーワードとの関係を示す参照テーブルから、前記文書ファイルに含まれる前記キーワードを抽出キーワードとして抽出するとともに、前記文書ファイルに対応する識別子を抽出識別子として抽出し、前記抽出した前記抽出キーワードと前記抽出識別子とを連結させ、１組としたアドレス情報と、前記アドレス情報に含まれる前記抽出識別子との関係を示す第１テーブルを生成し、前記アドレスを擬似乱数生成関数により乱数化情報に変換して変換追加アドレスを生成し、前記抽出識別子をステート情報に記憶し、前記変換アドレスと前記抽出識別子を前記サーバに送信

し、前記サーバは、前記端末により送信された前記変換アドレスを受信し、前記変換アドレスの乱数化情報のそれぞれが示すアドレスに、前記受信した前記抽出識別子を格納し、前記第２テーブルを更新すること、を特徴とする。

【００１２】

第４発明に係る動的検索可能暗号処理システムは、第１発明～第３発明において、前記端末は、削除する文書ファイルに対応する前記抽出識別子を、前記ステート情報から削除し、前記削除した前記抽出識別子を前記サーバに送信し、前記サーバは、前記端末により送信された前記抽出識別子を受信し、前記サーバの第２テーブルで前記抽出識別子に対応する全ての格納領域をＮＵＬＬに変換し、前記第２テーブルを更新すること、を特徴とする。

【００１３】

第５発明に係る動的検索可能暗号処理システムは、第１発明～第４発明において、前記第２テーブル生成手段は、追加する文書ファイルと同じ大きさの文書ファイルのうち、最も多い抽出キーワードを含むことができる文書ファイルを特定し、前記追加文書ファイルに対応する変換アドレスの個数が、前記特定した文書ファイルに含まれる抽出キーワード数となるまで、ダミーフラグを示す識別情報と、カウンタ情報と、前期追加文書ファイルの抽出識別子とを連結させ、１組のダミーアドレス情報とし、前期ダミーアドレス情報を疑似乱数生成関数により乱数化情報に変換して変換ダミーアドレスを生成し、前記変換ダミーアドレス情報が指し示すアドレスに前記抽出識別子を格納すること、を繰り返し、前記第２テーブルを生成すること、を特徴とする。

【００１４】

第６発明に係る動的検索可能暗号処理システムは、第１発明～第５発明において、前記端末は、検索するキーワードと前記ステート情報に含まれる各識別子を検索識別子として連結させ、１組としたアドレス情報と、前記アドレス情報を擬似乱数生成関数により乱数化情報に変換して変換アドレスを生成し、前記変換アドレスとを前記サーバに送信し、前記サーバは、前記端末により送信された前記変換アドレスを受信し、前記サーバの第２テーブルで前記変換アドレスに対応する全ての格納領域を参照し、前記格納領域がＮＵＬＬではなく、所定の識別子が格納される格納先の抽出識別子を取得し、前記端末に送信すること、を特徴とする。

【発明の効果】

【００１５】

第１発明～第６発明によれば、動的検索可能システムは、参照テーブルから文書ファイルと検索キーワードとの対応を示すアドレス情報を抽出し、第１テーブルと第２テーブルとを生成する。これにより、端末が保持する全ての文書ファイルとキーワードの対応を識別子により操作することができ、識別子のみを保存すれば良く、端末側が保持する情報を小さくできる。これにより、端末とサーバにおける効率性を向上させることができる。

【００１６】

特に、第１発明によれば、第１テーブル生成手段は、抽出された抽出キーワードと文書ファイルの識別子とを連結させ、１組としたアドレス情報と、アドレス情報に含まれる抽出識別子との関係を示す第１テーブルを生成する。このため、ステート情報はキーワード数に依存することがない。これにより、効率性を向上させることができる。

【００１７】

特に、第１発明によれば、第２テーブル生成手段は、アドレス情報を端末が保持する擬似乱数生成関数により端末側で乱数化情報に変換する。このため、疑似乱数生成用の鍵をキーワードごとに生成、サーバに渡し、サーバ側で疑似乱数を生成させる必要がなくなる。これにより、第三者へ必要以上の情報が漏洩することを防ぎ、フォワード安全性を達成することができる。

【００１８】

特に第２発明によれば、第２テーブル生成手段は、端末が保持する疑似乱数生成関数に関する鍵情報、端末が保持するステート情報により、初期化した第２テーブルを生成し、

サーバに送信する。このため、端末とサーバで共通の初期化テーブルを介したやり取りが可能となる。

【００１９】

特に、第３発明によれば、端末は、追加する文書ファイルに対応する抽出識別子と抽出キーワードとを連結させ、１組としたアドレス情報と、前記アドレス情報に含まれる前記抽出識別子との関係を示す第１テーブルを生成し、前記アドレスを擬似乱数生成関数により乱数化情報に変換して変換追加アドレスを生成し、前記抽出識別子をステート情報に記憶し、前記変換アドレスと前記抽出識別子を前記サーバに送信し、前記サーバは、前記端末により送信された前記変換アドレスを受信し、前記変換アドレスの乱数化情報のそれぞれが示すアドレスに、前記受信した前記抽出識別子を格納し、前記第２テーブルを更新する。このため、追加依頼された抽出識別子を適切な箇所に格納することができる。

【００２０】

特に、第４発明によれば、端末は削除する文書ファイルに対応する抽出識別子をステート情報から削除し、抽出識別子をサーバに送信し、サーバは、抽出識別子を受信し、第２テーブルで抽出識別子に対応する全ての格納領域をＮＵＬＬに変換し、前記第２テーブルを更新する。このため、削除依頼された抽出識別子が格納されている箇所を、全て空（ＮＵＬＬ）に設定することができる。

【００２１】

特に、第５発明によれば、第２テーブルに保存される変換アドレスの個数が、対象とする文書ファイルと同じ大きさの文書ファイルのうち、最も多い抽出キーワードを含む文書ファイルを特定する。このため、文書ファイルは、登録したい文書ファイルと同じ大きさの文書ファイルのうち、最も多くのキーワードを含むもののキーワード数と等しくなるようダミーエントリを容易に生成できる。これにより、サーバは、文書ファイルの候補を絞り込むことができなくなり、より強い安全性を実現させることができる。

【００２２】

特に、第６発明によれば、端末は端末上に保存されている各識別子を用い、検索キーワードと各識別子を連結したものを元に疑似乱数生成関数により乱数化情報を生成し、それら全てをサーバに送信し、サーバは各乱数化情報がアドレス情報として指し示す第２テーブルの格納値を調べ、ＮＵＬＬ以外の格納値を全て端末に送り返す。このため、端末とサーバ間においてやり取りされる情報に文書ファイルに関する情報は含まれない。これにより、フォワード安全性を満たすことができる。

【図面の簡単な説明】

【００２３】

【図１】図１は、第１実施形態における動的検索可能暗号処理システムの全体構成を示すブロック図である。

【図２】図２（ａ）は、第１実施形態における動的検索可能暗号処理システム１００の構成の一例を示す模式図であり、図２（ｂ）は、動的検索可能暗号処理システム１００の機能の一例を示す模式図である。

【図３】図３（ａ）は、第１実施形態におけるセットアップ処理における対応テーブルの一例を示す管理テーブルであり、図３（ｂ）は、第１実施形態におけるセットアップ処理における第１テーブルの一例を示す管理テーブルであり、図３（ｃ）は、第１実施形態におけるセットアップ処理における第２テーブルの一例を示す管理テーブルである。

【図４】図４は、第１実施形態における検索処理の対応を示す説明図である。

【図５】図５は、第１実施形態における検索処理の対応を示す説明図である。

【図６】図６は、第１実施形態における文書ファイルが含み得る最大のキーワード個数を示す説明図である。

【図７】図７（ａ）、（ｂ）は、第１実施形態における動的検索可能暗号処理システムの動作の一例を示すフローチャートである。

【発明を実施するための形態】

【００２４】

以下、本発明の実施形態における動的検索可能暗号処理システム１００の一例について、図面を参照しながら説明する。

【００２５】

（第１実施形態）

図１は、本実施形態における動的検索可能暗号処理システム１００の全体構成を示すブロック図である。

【００２６】

本実施形態の動的検索可能暗号処理システム１００は、図１に示すように、例えば、社内の複数の端末２（登録端末２ａ、検索端末２ｂ）と公衆通信網５（ネットワーク）を介して接続されるサーバ３により構成される。サーバ３は、暗号化データベース４を備え、暗号化された文書ファイル及び暗号化インデックステーブル（または第２テーブル)を保存する。

【００２７】

登録端末２ａ及び検索端末２ｂは、例えば、パーソナルコンピュータ（ＰＣ）等の電子機器が用いられ、文書ファイルを暗号化し、サーバ３への登録操作や処理を行う。サーバ３は、例えば、オンラインストレージ等の外部ストレージサービスを運用するクラウドサーバ等の電子機器が用いられる。サーバ３は、暗号化データベース４に保管される暗号化文書ファイルの更新や検索（動的検索）を行う。

【００２８】

図２は、本発明が適用される動的検索可能暗号処理システムの構成の一例を示すブロック図である。

【００２９】

図２（ａ）は、第１実施形態における動的検索可能暗号処理システム１００の構成の一例を示す模式図である。

【００３０】

図２（ａ）に示すように、動的検索可能暗号処理システム１００を構成する端末２は、筐体１０と、ＣＰＵ（Central Processing Unit）１１と、ＲＯＭ（Read Only Memory）１２と、ＲＡＭ（Random Access Memory）１３と、記憶部分１４と、Ｉ／Ｆ１５～１７とを備える。各々の構成であるＩ／Ｆ１５～１８は、内部バス１８により接続される。

【００３１】

ＣＰＵ１１は、動的検索可能暗号処理システム１００全体を制御する。ＲＯＭ１２は、ＣＰＵ１１の動作コードを格納する。ＲＡＭ１３は、ＣＰＵ１１の動作時に使用される作業領域である。記憶部分１４は、例えば、端末の属性情報、関連情報、登録端末２ａに生成される各テーブル、擬似ランダム関数の他に、暗号共通鍵等の情報を記憶する。記憶部分１４は、例えば、端末の操作者に関する情報、操作者に関する認証情報等の各種情報、その他、登録、更新、検索ログ等の各種情報が各々対応付けられて記憶されてもよい。なお、例えば、動的検索可能暗号処理システム１００は、図示しないＧＰＵ（Graphics Processing Unit）を有してもよい。ＧＰＵを有することで、通常よりも高速演算処理が可能となる。

【００３２】

Ｉ／Ｆ１５は、公衆通信網５を介して端末２等との各種情報の送受信を行うためのインターフェースである。Ｉ／Ｆ１６は、入力部分２０との情報の送受信を行うためのインターフェースである。入力部分２０として、例えば、キーボードが用いられ、動的検索可能暗号処理システム１００の管理者等は、入力部分２０を介して、各種情報又はサーバ３の制御コマンド等を入力する。Ｉ／Ｆ１７は、出力部分１９との各種情報の送受信を行うためのインターフェースである。出力部分１９は、記憶部分１４に保存された各種情報、又はサーバ３の処理状況等を出力する。出力部分１９として、ディスプレイが用いられ、例えばタッチパネル式でもよい。

【００３３】

図２（ｂ）は、動的検索可能暗号処理システム１００の機能の一例を示す模式図である

。動的検索可能暗号処理システム１００を構成する端末２とサーバ３の機能を示す。

【００３４】

端末２は、例えば、端末２の全体を制御する制御部２１、文書ファイルに含まれるキーワードの抽出、文書ファイルに対応する識別子を抽出識別子として抽出する抽出部２２、第１テーブルの生成を行う第１テーブル生成部２３、第２テーブルの生成を行う第２テーブル生成部２４、公衆通信網５を介してサーバ３とデータのやり取りを行う送受信部２５、文書ファイル、キーワード、各テーブル、擬似乱数生成関数、鍵情報、ステータス情報、各種アプリケーション等のデータ及び情報を記憶する記憶部２６を少なくとも備える。

【００３５】

サーバ３は、例えば、サーバ３の全体及び暗号化データベース４を制御する制御部３１、端末２から受信した第２テーブルの初期化、追加、削除等を行う更新部３２、端末２からの検索を実行し、検索結果を出力する検索部３３、公衆通信網５を介して複数の端末２とデータのやり取りを行う送受信部３５、暗号化文書ファイル、第２テーブル、擬似乱数生成関数、鍵情報、各種アプリケーション等のデータ及び情報を記憶する記憶部３５を少なくとも備える。

【００３６】

図２（ｂ）に示した端末２及びサーバ３の機能は、ＣＰＵ１１が、ＲＡＭ１３を作業領域として、記憶部分１４等に記憶されたプログラムを実行することにより実現される。

【００３７】

記憶部２６及び記憶部３５として、例えばＨＤＤのほか、ＳＳＤ等のデータ保存装置が用いられ、例えば、暗号化データベース４と一体に具現化されてもよい。記憶部２６及び記憶部３５には、例えば、ＲＡＭ及びＲＯＭを含み、各々で実行されるプログラム等が記憶される。なお、端末２及びサーバ３により実行される各機能は、各制御部が、ＲＡＭを作業領域として、各々の記憶部に記憶されたプログラムを実行することにより実現することができる。

【００３８】

図３は、動的検索可能暗号処理システム１００のセットアップ処理における各テーブルの一例を示す管理テーブルである。

【００３９】

図３（ａ）は、例えば、端末２に保持される参照テーブル４０aであり、文書ファイル（f_n）と各々の文書ファイル対応する識別子（id_n）と各文書ファイル（f_n）に対応するキーワードとの関係を対応付けて格納される。図３（ｂ）は、端末２で生成される第１テーブル４０ｂであり、参照テーブル４０ａから抽出部２２により抽出され、抽出キーワード（w_d）と抽出識別子（id_n）とを連結させ、１組としたアドレス情報と、アドレス情報に含まれる抽出識別子（id_n）とが各々対応付けて格納される。図３（ｃ）は、第１テーブル４０ｂにおけるアドレスを擬似乱数生成関数により乱数化情報に変換して変換アドレスを生成し、変換アドレスと抽出識別子（id_n）とが各々対応付けられて格納される。

【００４０】

ここで、文書ファイルは、文書ファイルの集合をＦで表し、各文書ファイル$f_{id} \in F$には、それぞれ対応する識別子$id \in \{0, 1\}^l$（ｌはｋの多項式）が付され、文書ファイルf_{id}を単にｉｄと書く。$\Lambda := \{0, 1\}^\lambda$（λはｋの多項式）をあり得る全てのキーワードの集合とし、例えば、ビット列ではなく文字列として表現されてもよい。また、識別子id_iである文書ファイルに含まれるキーワードの集合をW_iとする。

【００４１】

動的検索可能暗号処理システム１００は、セットアップ（Setup）の実行時に、タイムスタンプｔ：＝０として初期化し、登録端末２ａまたは検索端末２ｂは、検索（Search）及び更新（Update）の各操作を行うごとに、タイムスタンプをインクリメントされるようにしてもよい。

【００４２】

図３（ａ）は、第１実施形態における参照テーブル４０ａの一例を示す参照テーブルである。参照テーブル４０ａは、暗号化対象の文書ファイルとその文書ファイルが含むキーワードの集合（ｉｄ，W_{id}） として対応付けられる。参照テーブル４０ａは、例えば、ｔ時点での文書ファイルf_1（識別子id_1）～文書ファイルf_n（識別子id_n）に含まれる全てのキーワードw_1～w_dが各々対応付ける。文書ファイルf_1にキーワードw_1が含まれている場合は、例えば、参照テーブル４０ａの対応する箇所にフラグ（例えば、×）が付されて記憶される。

【００４３】

図３（ｂ）は、第１実施形態における第１テーブル４０ｂの一例を示す管理テーブルである。インデックステーブル４０ｂは、対応テーブル４０ａから各文書ファイルにキーワードが含まれている対応箇所のみ（フラグ×の箇所）が抽出される。

【００４４】

次に、第１テーブル４０ｂは、アドレス情報（部）と抽出識別子（例えば、文書管理番号）の組み（対）の関係により構成される。アドレス情報は、例えば、キーワードw_iと文書ファイルの文書番号ｉｄの連結（$w_i||id$）であり、抽出識別子は、例えば、文書ファイルf_{id}の抽出識別子ｉｄとなる。

【００４５】

図３（ｃ）は、第１実施形態における第２テーブルの一例を示す管理テーブルである。第２テーブル４０ｃは、第１テーブル４０ｂのアドレス情報（部）と抽出識別子（例えば、文書管理番号）の対の関係性を隠すため、例えば、ユーザのみが知る擬似乱数生成関数πを用いて、変換された関係性の対として生成される。

【００４６】

第２テーブル４０ｃは、第１テーブル４０ｂのキーワードw_iと文書ファイルの文書番号ｉｄの連結（$w_i||id$）を、擬似乱数生成関数πを用いて乱数化される。アドレスは、例えば、π（k，$w_i||id$）として変換され、識別子は、例えば、文書ファイルf_{id}の識別子ｉｄがアドレスπ（k，$w_i||id$）と関連付けられて記憶される。

【００４７】

図４は、第１実施形態における検索処理の対応を示す説明図である。検索端末２ｂから入力される検索キーワードｑを用いて、サーバ３の暗号化データベース４に記憶されている暗号化文書ファイルの検索を行う。

【００４８】

第２テーブル４０ｃは、第２テーブル生成部２４により、 第１テーブル４０ｂの検索キーワードｑと文書ファイルの文書番号ｉｄの 連結（$q||id$）を、擬似乱数生成関数πを用いて乱数化し、 検索端末２ｂは、変換アドレスをサーバ３に送信し、 サーバ３は、検索端末２ｂにより送信された変換アドレスを受信する。サーバ３の第２テーブル４０ｃで変換アドレスに 対応する全ての格納領域を参照し、格納領域がＮＵＬＬではなく、所定の識別子が格納される格納先の抽出識別子を取得する。

【００４９】

図５は、第１実施形態における検索処理の対応を示す説明図である。暗号化サーバ３は、例えば、検索端末２ｂから送信された変換アドレスを受信し、第２テーブル４０ｃを参照し、検索依頼のあったアドレス情報のうち、π（k，$q||id_1$）及びアドレス情報π（k，$q||id_3$）と対になる検索識別子で関連付けられる文書ファイルが登録されているため、該当する検索識別子id_1及びid_3を、検索端末２ｂに送信する。

【００５０】

図６は、文書ファイルf_{id}が含み得る最大のキーワード数を示す説明図である。文書ファイルf_{id}はw_{id}に含まれるキーワードの組み合わせからなるファイルとみなすが、max_{id}をf_{id}が含むことのできるキーワードの最大個数（例えば、１０個）とする。文書ファイルの最大キーワードの個数は、最も小さいキーワード$w \in \Lambda$から順にそのサイズを加算し、$|f_{id}|$を超える手前までに加算したキーワードw_jの合計個数となる。

【００５１】

文書ファイルの最大キーワードの個数、例えば、μ_{id}個のエントリを登録すると同時に、（$max_{id} - \mu_{id}$）個のダミーエントリを追加してもよく、これにより、ｉｄを格納しているアドレスの個数を｜f_{id}｜個に常に統一することが可能となる。そのため、サーバは文書ファイルf_{id}の候補を絞り込むことができない。

【００５２】

次に、図７（ａ）、（ｂ）は、第１実施形態における動的検索可能暗号処理システムの動作の一例を示すフローチャートである。

【００５３】

先ず、動的検索可能暗号処理システム１００の登録端末２ａは、抽出ステップＳ１１０～第２テーブル生成ステップＳ１３０を実行する。

【００５４】

＜抽出ステップＳ１１０＞

登録端末２ａの抽出部２２は、文書ファイルと抽出キーワードの抽出を行う（抽出ステップＳ１１０）。抽出ステップＳ１１０では、文書ファイルに対応する識別子とキーワードとの関係を示す参照テーブルから、文書ファイルに含まれるキーワードを抽出キーワードとして抽出する。そして、文書ファイルに対応する識別子を抽出識別子として抽出する。

【００５５】

＜第１テーブル生成ステップＳ１２０＞

次に、第１テーブル生成部２３は、抽出ステップＳ１１０により抽出されたアドレス情報と識別子に対して、アドレス情報と識別子との対応を第１テーブル４０ｂとして生成する（第１テーブル生成ステップＳ１２０）。第１テーブル生成部は、抽出ステップＳ１１０により抽出された抽出キーワードと抽出識別子とを連結させ、１組としたアドレス情報と、アドレス情報に含まれる前記抽出識別子との関係を示す第１テーブルを生成する。

【００５６】

また、第１テーブル生成部２３は、抽出ステップＳ１１０により抽出された全てのアドレス情報及び識別子に、更新があるかを判別する。そして、追加または削除の変更がある場合は、アドレス情報に含まれる文書ファイルを特定する抽出識別子を変更に応じて、暗号化文書ファイルの追加または削除する変更を行う。

【００５７】

＜第２テーブル生成ステップＳ１３０＞

第２テーブル生成部２４は、第１テーブルの各アドレス情報を乱数化情報に変換して第２テーブルを生成する（第２テーブル生成ステップＳ１３０）。第２テーブル生成部２４は、第１テーブル４０ｂに含まれる各アドレス情報を、登録端末２ａの記憶部２６に記憶される擬似乱数生成関数及びその鍵により乱数化情報に変換し、第２テーブル４０ｃとして生成する。

【００５８】

（第２実施形態）

図７（ｂ）は、動的検索可能暗号処理システム１００のサーバ３における検索処理について、受信ステップＳ２１０～結果送信ステップＳ２３０を実行する。

【００５９】

まず、検索端末２ｂは、検索するキーワードとステート情報に含まれる各識別子を検索識別子として連結させ、１組としたアドレス情報を生成する。

【００６０】

次に、アドレスを擬似乱数生成関数により乱数化情報に変換して変換アドレスを生成し、変換アドレスをサーバ３に送信する。

【００６１】

＜受信ステップＳ２１０＞

サーバ３の送受信部３４は、検索端末２ｂから送信された変換アドレスを受信する（受信ステップＳ２１０）。

【００６２】
＜更新ステップＳ２２０＞
検索部３３は、暗号化データベース４に格納される第２テーブルを参照し、第２テーブル４０ｃで変換アドレスに対応する全ての格納領域を参照し、格納領域がＮＵＬＬではなく、所定の識別子が格納される格納先の抽出識別子を取得する。（検索ステップＳ２２０）。判別の結果に応じて、$X_q^{(t)}$に加え、送られてきた値の全ての変換アドレスをチェックする。ここで、tは現時点での時刻を表す。
【００６３】
＜結果送信ステップＳ２３０＞
送受信部３４は、検索依頼のあった検索端末２ｂに、検索結果である検索識別子を送信する。（送信ステップＳ２３０）。検索結果である各文書ファイル$f_{id} \in F$は、共通鍵暗号で暗号化され（図示せず）、サーバ３の暗号化データベース４に保存される。なお、全ての暗号化文書ファイルは、文書ファイルの識別子ｉｄと併せて、サーバ３の暗号化データベース４に保存される。
【００６４】
これにより、本実施形態における動的検索可能暗号処理システム１００の動作が終了する。
【００６５】
（第３実施形態）
次に、端末２（登録端末２ａ）における第２テーブルの初期化処理について説明する。端末２は、第２テーブル生成ステップＳ１３０において、端末２ａが保持する 疑似乱数生成関数に関する鍵情報、端末２ａが保持するステート情報に基づき、抽出識別子を初期化した第２テーブル４０ｃを生成し、鍵情報とステート情報の端末２ｂの記憶部２６に記憶させる。その後に、生成した第２テーブル４０ｃをサーバ３に送信する。
【００６６】
本実施例によれば、検索端末２ｂは検索依頼の対象となる検索キーワードと端末に保存されたステート情報に含まれる全ての検索識別子ｉｄに応じて生成された変換アドレスを生成し、送信する。サーバ３は、受信した変換アドレスから、第２テーブルの変換アドレスが指し示すアドレスに格納された値を確認する。そのため、サーバ３はステート情報に含まれる識別子に関する変換アドレスに対応する格納領域のみを参照する。これにより、検索端末２ｂとサーバ３との間で、その時点の検索に必要なだけの情報がやり取りされ、検索後のアドレスの再登録が不要となり、フォワード安全性を達成することができるとともに、効率性を向上させることができる。
【００６７】
（第４実施形態）
次に、動的検索可能暗号処理システム１００における、端末２とサーバ３における文書ファイルの追加の処理について説明する。
【００６８】
まず、登録端末２ａは、追加する文書ファイルに対応する識別子とキーワードとの関係を示す参照テーブル４０ａから、文書ファイルに含まれる前記キーワードを抽出キーワードとして抽出する。そして、文書ファイルに対応する識別子を抽出識別子として抽出し、抽出した抽出キーワードと抽出識別子とを連結させ、１組としたアドレス情報と、アドレス情報に含まれる抽出識別子との関係を示す第１テーブルを生成する。
【００６９】
次に、登録端末２ａの記憶部２６に記憶される擬似乱数生成関数により、アドレス情報を乱数化情報に変換して、変換追加アドレスを生成する。登録端末２ａは、抽出識別子をステート情報に記憶し、その後に、変換アドレスと抽出識別子をサーバ３に送信する。
【００７０】
登録端末２ａにおける文書ファイルの更新（追加）は、例えば、以下の処理で実行される。

【００７１】
＜＜時刻tにおける文書ファイル（ｉｄ,W_{id}） の追加＞＞
端末２（登録端末２ａ）は記憶部２６に登録されるアプリケーション（Updateアルゴリズム:図示せず）により、全ての$w \in W_{id}$ に対してπ（ｋ，ｗ||ｉｄ） を計算する。ダミーアドレスではないことを示すため、π（ｋ，0||ｗ||ｉｄ）としてもよい。ここで計算された値が、第２テーブル４０ｃのアドレスとなる。登録端末２ａは、計算した値全て及びｉｄをサーバ３に送信し、登録端末２ａに記憶されるステート情報$\sigma^{(t)}$にｉｄを追加し、ステート情報$\sigma^{(t+1)}$とする。
【００７２】
サーバ３は、登録端末２ａにより送信された変換アドレス及び抽出識別子を受信し、第２テーブル４０ｃの変換アドレスの乱数化情報のそれぞれが示すアドレスに、受信した抽出識別子を格納し、第２テーブル４０ｃを更新し、ＥＤＢ$^{(t+1)}$とする。
【００７３】
（第５実施形態）
次に、動的検索可能暗号処理システム１００における、端末２とサーバ３における文書ファイルの削除の処理について説明する。
【００７４】
本実施形態によれば、ｉｄが格納値として第２テーブルに含まれる数μ_{id}を、対応する文書ファイルf_{id}が含み得るキーワードの最大数max_{id}に合わせるため、（max_{id}-μ_{id}）個のダミーアドレスとして、π（ｋ，1||1||ｉｄ）～π（ｋ，1|| max_{id}-μ_{id} ||ｉｄ）を生成し、それぞれが指し示す第２テーブル中のアドレスにｉｄを格納してもよい。このため、文書ファイルf_{id}が含むことのできる最大数のキーワード（max_{id}個）になるまでｉｄのダミーエントリを追加することができる。これにより、より強い安全性を備えることが可能となる。
【００７５】
登録端末２ａは、削除する文書ファイルに対応する抽出識別子を、記憶部２６に記憶されるステート情報から削除し、削除した抽出識別子をサーバ３に送信する。
【００７６】
＜＜時刻tにおけるｉｄに対応する文書ファイルの削除＞＞
登録端末２ａは、サーバ３に操作の対象となる抽出識別子（ｉｄ）を送信する。そして記憶部２６に記憶されるステート情報$\sigma^{(t)}$から対象の抽出識別子（ｉｄ）を削除し、ステート情報$\sigma^{(t+1)}$とする。
【００７７】
サーバ３は、削除対象となる抽出識別子を受信し、第２テーブル４０ｃの格納されている値が抽出識別子（ｉｄ）の部分を、全てＮＵＬＬに置き換える処理を繰り返し、全て置き換えた第２テーブル４０ｃを更新し、ＥＤＢ$^{(t+1)}$とする。
【００７８】
さらに、本実施形態によれば、動的検索可能暗号処理システム１００は、例えば、複数の医療機関をまたがったデータベースにおける検索サービスに適用することが可能である。これにより、病院のデータベースに記憶される個人情報が、患者カルテ（ファイル）の更新、または検索される際に、必要以上に漏洩することを防ぐことが可能となる。
【００７９】
さらに、本実施形態によれば、動的検索可能暗号処理システム１００は、例えば、クラウドサーバを介してやり取りされるメールサービス等において、ユーザは過去にやり取りしたメールやアーカイブしたメール等を暗号化したまま検索が可能となる。そのため、クラウド側にメールの内容が漏洩することを防ぐことが可能となる。
【００８０】
動的検索可能暗号処理システム１００において、ステート情報は必ずしも端末に保存される必要はなく、また、端末が保持するステート情報を公開しても良い。そのため、前記ステート情報を端末ではなくサーバに保存したとしても、それによって安全性が損なわれ

ることはない。

【００８１】

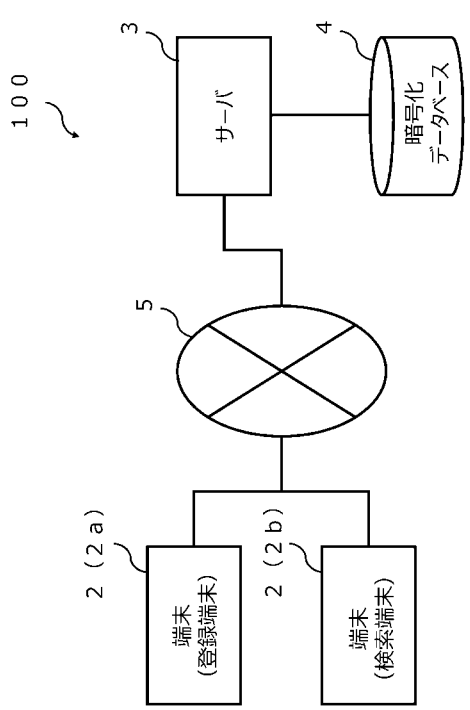
本発明の実施形態を説明したが、各実施形態は例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれるとともに、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

【符号の説明】

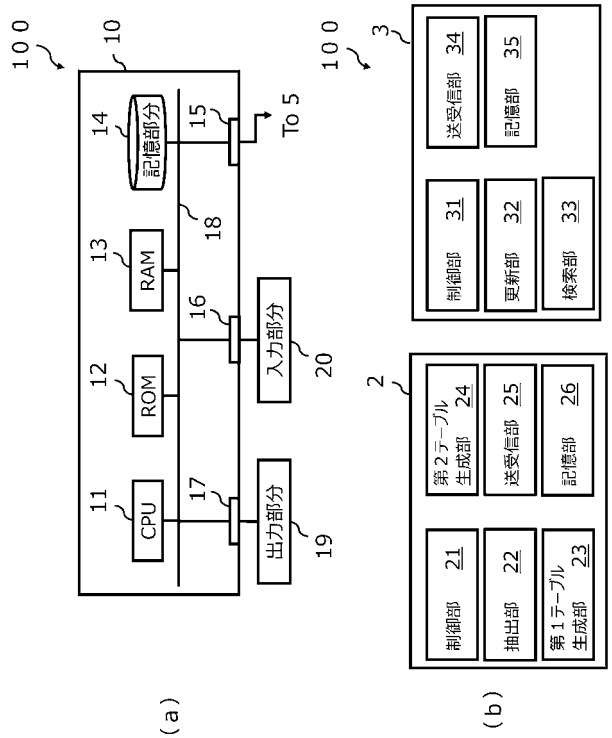
【００８２】

１０　：筐体
１１　：ＣＰＵ
１２　：ＲＯＭ
１３　：ＲＡＭ
１４　：記憶部分
１５　：Ｉ／Ｆ
１６　：Ｉ／Ｆ
１７　：Ｉ／Ｆ
１８　：内部バス
１９　：出力部分
１００　：動的検索可能暗号処理システム
２　：端末
２ａ　：登録端末
２ｂ　：検索端末
２０　：入力部分
２１　：制御部
２２　：抽出部
２３　：第１テーブル生成部
２４　：第２テーブル生成部
２５　：送受信部
２６　：記憶部
３　：サーバ
３１　：制御部
３２　：更新部
３３　：検索部
３４　：送受信部
３５　：記憶部
４　：暗号化データベース
４０ａ　：参照テーブル
４０ｂ　：第１テーブル
４０ｃ　：第２テーブル
５　：公衆通信網
Ｓ１１０　：抽出ステップ
Ｓ１２０　：第１テーブル生成ステップ
Ｓ１３０　：第２テーブル生成ステップ
Ｓ２１０　：受信ステップ
Ｓ２２０　：更新ステップ
Ｓ２３０　：結果送信ステップ

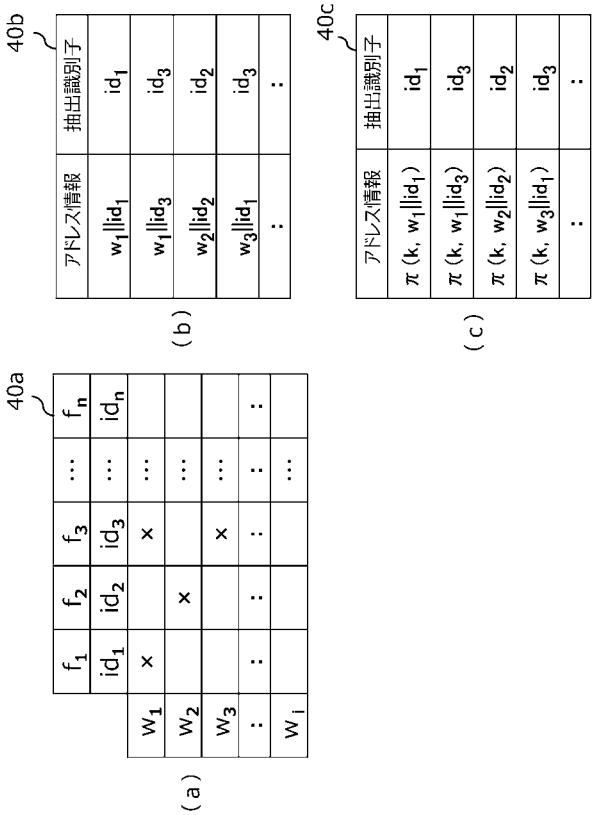
【図１】


１００
３
サーバ
４
暗号化
データベース
５
２（２ａ）
端末
（登録端末）
２（２ｂ）
端末
（検索端末）

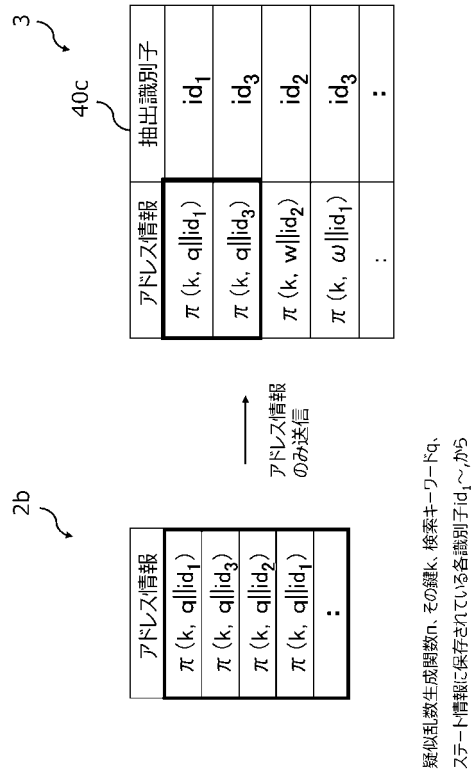
【図２】


１００
１０
１１
CPU
１２
ROM
１３
RAM
１４
記憶部分
１５
To 5
１６
１７
１８
１９
出力部分
２０
入力部分
２
第２テーブル
生成部
２４
送受信部
２５
記憶部
２６
制御部
２１
抽出部
２２
第１テーブル
生成部
２３
１００
３
制御部
３１
更新部
３２
検索部
３３
送受信部
３４
記憶部
３５
（ａ）
（ｂ）

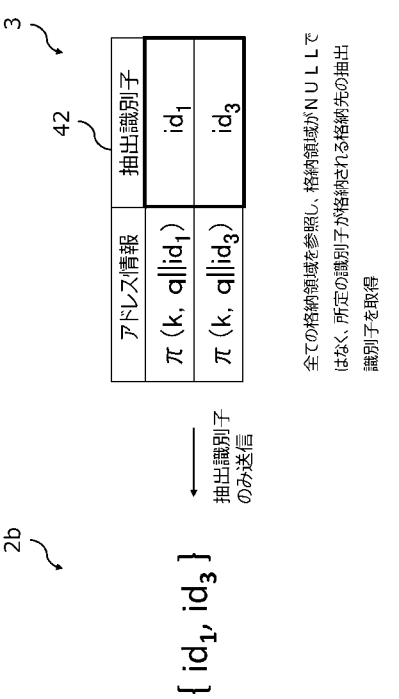
【図３】


40a
f1 f2 f3 … fn
id1 id2 id3 … idn
w1 x x … …
w2 x … …
w3 x … …
: : : : :
wi … …
（ａ）
40b
アドレス情報 抽出識別子
w1‖id1 id1
w1‖id3 id3
w2‖id2 id2
w3‖id1 id3
: :
（ｂ）
40c
アドレス情報 抽出識別子
π（k, w1‖id1） id1
π（k, w1‖id3） id3
π（k, w2‖id2） id2
π（k, w3‖id1） id3
: :
（ｃ）

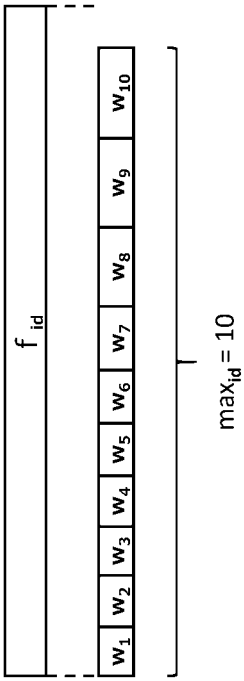
【図４】


3
40c
アドレス情報 抽出識別子
π（k, q‖id1） id1
π（k, q‖id3） id3
π（k, w‖id2） id2
π（k, ω‖id1） id3
: :
2b
アドレス情報
π（k, q‖id1）
π（k, q‖id3）
π（k, q‖id2）
π（k, q‖id1）
:
アドレス情報
のみ送信
疑似乱数生成関数n、その鍵k、検索キーワードq、
ステート情報に保存されている各識別子id1～から
送信するアドレス情報を計算

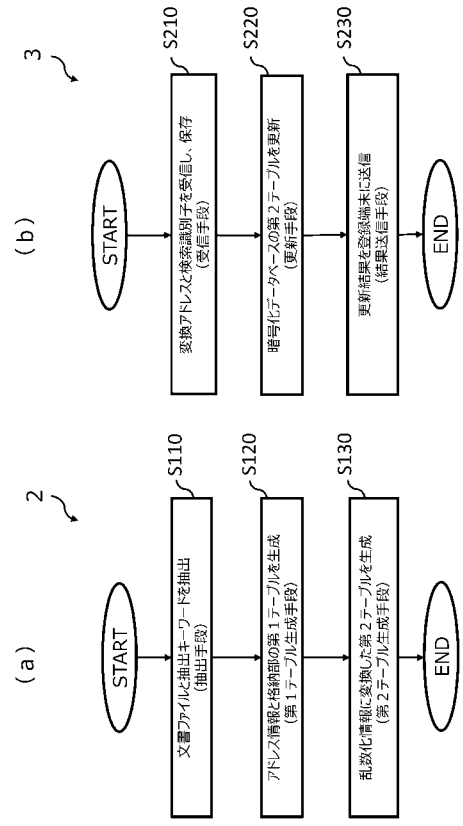
【図５】


3
42
アドレス情報
抽出識別子
π (k, q||id1)
id1
π (k, q||id3)
id3
全ての格納領域を参照し、格納領域がＮＵＬＬでは なく、所定の識別子が格納される格納先の抽出識別子を取得
抽出識別子のみ送信
2b
{ id1, id3 }

【図６】


f id
w1
w2
w3
w4
w5
w6
w7
w8
w9
w10
max id = 10

【図７】


(a)
2
START
文書ファイルと抽出キーワードを抽出（抽出手段）
S110
アドレス情報と格納部の第１テーブルを生成（第１テーブル生成手段）
S120
乱数化情報に変換した第２テーブルを生成（第２テーブル生成手段）
S130
END
(b)
3
START
変換アドレスと検索識別子を受信し、保存（受信手段）
S210
暗号化データベースの第２テーブルを更新（更新手段）
S220
更新結果を登録端末に送信（結果送信手段）
S230
END

フロントページの続き

(72)発明者　太田　和夫
東京都調布市調布ケ丘一丁目５番地１　国立大学法人電気通信大学内