(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
2020年1月2日(02.01.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/003821 A1

(51) 国際特許分類:
G09C 1/00 (2006.01) *H04L 9/08* (2006.01)
G06F 16/28 (2019.01)

(21) 国際出願番号： PCT/JP2019/020337

(22) 国際出願日： 2019年5月22日(22.05.2019)

(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 2018-124568 2018年6月29日(29.06.2018) JP

(71) 出願人: ソニー株式会社 (**SONY CORPORATION**) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 Tokyo (JP).

(72) 発明者: 丸山 信也 (**MARUYAMA, Shinya**); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP). 内田 篤史(**UCHIDA, Atsushi**); 〒1080075 東京都港区港南１丁目７番１号 ソニー株式会社内 Tokyo (JP).

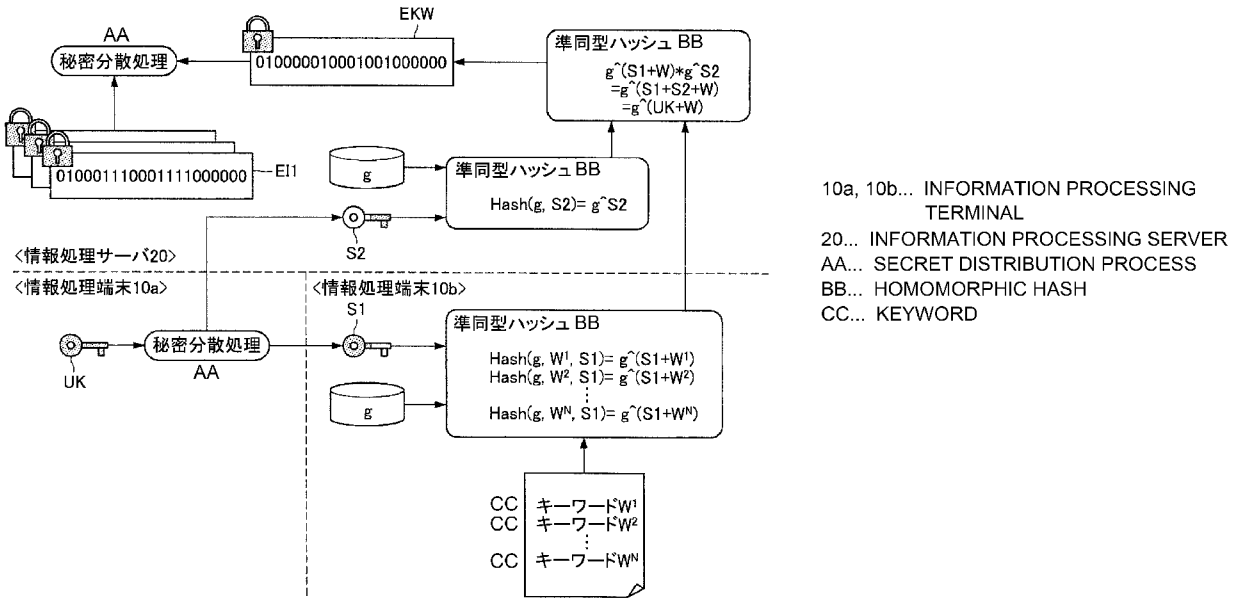
(74) 代理人: 特許業務法人酒井国際特許事務所 (**SAKAI INTERNATIONAL PATENT OFFICE**); 〒1000013 東京都千代田区霞が関３丁目８番１号 虎の門三井ビルディング Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

(54) **Title:** INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING METHOD, AND INFORMATION PROCESSING DEVICE

(54) 発明の名称： 情報処理システム、情報処理方法、および情報処理装置

[図8]



(57) **Abstract:** Provided is an information processing system including: a first device (10a) which divides a user key (UK) of a sharing source user by means of a secret distribution process, and generates a plurality of distribution keys (S1, S2); a second device (10b) which transmits a processing request pertaining to the execution of a prescribed process by using one of the plurality of distribution keys generated by the first device; and a third device (20) which makes a decision based on the processing request received from the second device and the one of the plurality of distribution keys generated by the first device.

WO 2020/003821 A1

[続葉有]

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

添付公開書類:

一 国際調査報告(条約第21条(3))

(57) 要約:共有元ユーザのユーザ鍵(ＵＫ)を秘密分散処理により分割し、複数の分散鍵(Ｓ１，Ｓ２)を生成する第１の装置(１０ａ)と、前記第１の装置が生成した複数の前記分散鍵のうちの１つを用いて所定の処理の実行に係る処理リクエストを送信する第２の装置(１０ｂ)と、前記第１の装置が生成した複数の前記分散鍵のうちの１つと、前記第２の装置から受信した前記処理リクエストに基づく判定を行う第３の装置(２０)と、を備える、情報処理システムが提供される。

明　細　書

発明の名称 ：

情報処理システム、情報処理方法、および情報処理装置

技術分野

[0001] 本開示は、情報処理システム、情報処理方法、および情報処理装置に関する。

背景技術

[0002] 近年、クラウドサービス等の普及に伴い、個人や企業などのデータをサービス提供者が管理するサーバに保管する場面が増加している。上記のようなサーバでは、セキュリティ性を確保するために、データの暗号化などを行うのが一般的である。また、近年では、データを暗号化したまま情報検索を実現する検索可能暗号技術も開発されている。例えば、特許文献１には、検索可能暗号を用いた情報検索において、大規模データに対する検索処理を高速化する技術が開示されている。

先行技術文献

特許文献

[0003] 特許文献1：特開２０１５－１３５５４１号公報

発明の概要

発明が解決しようとする課題

[0004] ここで、暗号化されたデータの検索は、当該データの所有者のみではなく、例えば、所有者に検索を許諾された他のユーザにより行われる場合も想定される。しかし、特許文献１に記載される技術では、マルチユーザによる情報検索に対する考慮が十分ではない。

[0005] そこで、本開示では、マルチユーザに対応した、よりセキュリティ性の高い情報検索を実現することが可能な、新規かつ改良された情報処理システム、情報処理方法、および情報処理装置を提案する。

課題を解決するための手段

[0006] 本開示によれば、共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成する第１の装置と、前記第１の装置が生成した複数の前記分散鍵のうちの１つを用いて所定の処理の実行に係る処理リクエストを送信する第２の装置と、前記第１の装置が生成した複数の前記分散鍵のうちの１つと、前記第２の装置から受信した前記処理リクエストに基づく判定を行う第３の装置と、を備え、前記第１の装置は、生成した複数の前記分散鍵のうち互いに異なる前記分散鍵を、共有先ユーザが利用する前記第２の装置、および前記第３の装置にそれぞれ配布し、前記第２の装置は、受信した前記分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を前記第３の装置に送信し、前記第３の装置は、前記第２の装置から受信したハッシュ値および前記第１の装置から受信した前記分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とを比較し、前記所定の処理を実行するか否かを判定する、情報処理システムが提供される。

[0007] また、本開示によれば、第１の装置が、共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成することと、第２の装置が、前記第１の装置が生成した複数の前記分散鍵のうちの１つを用いて所定の処理の実行に係る処理リクエストを送信することと、第３の装置が、前記第１の装置が生成した複数の前記分散鍵のうちの１つと、前記第２の装置から受信した前記処理リクエストに基づく判定を行うことと、を含み、前記第１の装置が、生成した複数の前記分散鍵のうち互いに異なる前記分散鍵を、共有先ユーザが利用する前記第２の装置、および前記第３の装置にそれぞれ配布することと、前記第２の装置が、受信した前記分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を前記第３の装置に送信することと、前記第３の装置が、前記第２の装置から受信したハッシュ値および前記第１の装置から受信した前記分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により

算出されたハッシュ値とを比較し、前記所定の処理を実行するか否かを判定することと、をさらに含む、情報処理方法が提供される。

[0008] また、本開示によれば、共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成する秘密分散処理部と、複数の前記分散鍵のうち互いに異なる前記分散鍵を、共有先ユーザが利用する端末、および暗号化データが保存されるサーバにそれぞれ送信する通信部と、を備える、情報処理装置が提供される。

発明の効果

[0009] 以上説明したように本開示によれば、マルチユーザに対応した、よりセキュリティ性の高い情報検索を実現することが可能となる。

[0010] なお、上記の効果は必ずしも限定的なものではなく、上記の効果とともに、または上記の効果に代えて、本明細書に示されたいずれかの効果、または本明細書から把握され得る他の効果が奏されてもよい。

図面の簡単な説明

[0011] [図1]検索可能暗号について説明するための図である。

[図2]本開示の一実施形態に係る情報処理方法と比較手法との差異について説明するための図である。

[図3]同実施形態に係る情報処理システムの構成例を示すブロック図である。

[図4]同実施形態に係る情報処理端末の機能構成例を示すブロック図である。

[図5]同実施形態に係る情報処理サーバの機能構成例を示すブロック図である。

[図6]同実施形態に係る暗号化インデックスの生成について説明するための図である。

[図7]同実施形態に係る暗号化データおよび暗号化インデックスの登録を行ったユーザ本人による暗号化データの検索について説明するための図である。

[図8]同実施形態に係る共有先ユーザによる暗号化データの検索について説明するための図である。

[図9]同実施形態に係る分散鍵の管理テーブルの一例を示す図である。

[図10]同実施形態に係る共有先ユーザが利用する情報処理端末による暗号化データの復号について説明するための図である。

[図11]同実施形態に係る情報処理サーバが制御するユーザインタフェースの一例を示す図である。

[図12]同実施形態に係る複数の共有先ユーザが存在する場合の処理について説明するための図である。

[図13]同実施形態に係る情報処理方法を適用した承認フローの一例について説明するための図である。

[図14]同実施形態に係る情報処理方法を適用した共有先ユーザの全員一致による処理実行の一例を示す図である。

[図15]同実施形態に係る暗号化データおよび暗号化インデックスの登録の流れを示すシーケンス図である。

[図16]同実施形態に係る分散鍵配布の流れを示すシーケンス図である。

[図17]同実施形態に係る検索処理の流れを示すシーケンス図である。

[図18]本開示の一実施形態に係るハードウェア構成例を示す図である。

発明を実施するための形態

[0012] 以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

[0013] なお、説明は以下の順序で行うものとする。

１．実施形態

１．１．背景

１．２．情報処理システム１の構成例

１．３．情報処理端末１０の機能構成例

１．４．情報処理サーバ２０の機能構成例

１．５．機能の詳細

１．６．動作の流れ

２．ハードウェア構成例

３．まとめ

[0014] ＜１．実施形態＞

＜＜１．１．背景＞＞

まず、本開示の一実施形態に係る背景について述べる。上述したように、近年では、クラウドサービス等の普及に伴い、個人や企業などのデータを、サービス提供者が管理するサーバに保管する場面が増加している。また、一般的なサーバでは、データベースを暗号化するなどの手法によりユーザのデータを保護している。

[0015] しかし、一般的なクラウドサービスでは、データを復号するための復号鍵もサーバで管理あれている場合もあり、権限を有するサービス管理者やサービスベンダーであれば、当該復号鍵を用いてユーザデータを復号することも可能である。このような事態を防ぐためには、サーバ上に保管されるユーザデータを、ユーザが利用するユーザ端末のみで復号できるように制御することが重要となる。

[0016] ここで、上記のような制御を実現する手法としては、例えば、クライアント側によるユーザデータの暗号化が挙げられる。ユーザは、クライアント端末が管理するユーザ固有鍵（以下、ユーザ鍵、とも称する）を用いて暗号化した暗号化データをサーバに送信、また保管し、復号の際には、サーバからダウンロードした上記暗号化データをユーザ鍵を用いて復号することができる。上記のようなクライアント側による暗号化技術によれば、復号鍵がサーバ上で管理されないため、上述したようなサービス管理者などによる不正なデータ取得を防止することが可能となる。

[0017] また、近年では、検索対象となるデータと検索ワードとを暗号化したまま検索処理を行うことが可能な検索可能暗号も普及している。

[0018] 図１は、検索可能暗号について説明するための図である。図１の左側には、ユーザＵが、クラウド側に設置されるサーバに暗号化データＥＤを登録する場合の処理の一例が示されている。

[0019] ユーザＵは、まず、ローカル側に設置されるクライアント端末を用いて、任意のデータＤをユーザ鍵ＵＫを用いて暗号化し、暗号化データＥＤを生成する。また、この際、クライアント端末は、データＤから抽出したキーワードリストをユーザ鍵ＵＫを用いて同様に暗号化し、暗号化インデックスＥＩを生成する。クライアント端末が生成した暗号化データＥＤおよび暗号化インデックスＥＩは、クラウド側に設置されるサーバに送信され、保管される。

[0020] また、図１の右側には、ユーザＵが、サーバに保管される暗号化データＥＤに対する検索を行う場合の処理の一例が示されている。

[0021] 検索処理においては、まず、クライアント端末が、ユーザＵにより入力された検索ワードをユーザ鍵ＵＫを用いて暗号化し、生成した暗号化キーワードＥＫＷをサーバに送信する。続いて、サーバは、受信した暗号化キーワードＥＫＷが、保存する暗号化インデックスＥＩに含まれるか否かを判定する。ここで、暗号化キーワードＥＫＷが暗号化インデックスＥＩに含まれる場合、サーバは、暗号化キーワードＥＫＷに対応する検索結果として、保存する暗号化データＥＤをクライアント端末に送信する。次に、クライアント端末は、受信した暗号化データＥＤをユーザ鍵ＵＫにより復号し、取得した平文などをユーザＵに提示する。

[0022] このように、検索可能暗号技術によれば、暗号化データを一度も復号することなく、当該暗号化データに対する情報検索を行うことができ、セキュリティ性をより向上させることが可能となる。

[0023] しかし、例えば、特許文献１に記載されるような検索可能暗号技術では、一般的に、マルチユーザによる情報検索が十分に考慮されていない。このため、暗号化データの登録を行ったユーザ以外が、当該暗号データに対する検索を行いたい場合、例えば、暗号化データの生成に用いた共有元ユーザのユーザ鍵を共有先ユーザにシェアすることなどが求められる。ここで、共有元ユーザとは、自身のユーザ鍵を用いて生成した暗号化データをサーバに登録したユーザであり、共有先ユーザとは、共有元ユーザにより当該暗号化デー

タの検索が許諾されたユーザを指す。しかし、共有元ユーザのユーザ鍵を共有先ユーザにシェアする場合、なりすましなどが可能となることから、セキュリティ性が低下することとなる。

[0024] また、マルチユーザによる検索を実現するために、共有元ユーザの端末で、共有先ユーザ毎に検索用の暗号化インデックスを生成することも可能であるが、この場合、共有先ユーザが増加した場合には、過去データを端末に取得して暗号化インデックスを再生成する必要があり、処理負担が大きい。

[0025] また上記の他にも、放送型暗号方式や、ペアリング方式、代理人再暗号化方式などが想定されるが、いずれも重い演算が必要となる。

[0026] 本開示の一実施形態に係る技術思想は上記の点に着目して発想されたものであり、マルチユーザに対応した、セキュリティ性および性能の高い情報検索を実現する。本開示の一実施形態に係る技術思想によれば、暗号化データを登録した共有元ユーザのユーザ鍵を共有先ユーザにシェアすることなく、共有先ユーザが当該暗号化データに対する情報検索を行うことが可能となる。

[0027] このために、情報処理方法を実現する情報処理システムは、共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成する第１の装置と、第１の装置が生成した複数の分散鍵のうちの１つを用いて所定の処理の実行に係る処理リクエストを送信する第２の装置と、第１の装置が生成した複数の分散鍵のうちの１つと、第２の装置から受信した処理リクエストに基づく判定を行う第３の装置と、を備える。ここで、第１の装置は、生成した複数の分散鍵のうち互いに異なる分散鍵を、共有先ユーザが利用する第２の装置、および第３の装置にそれぞれ配布してよい。また、第２の装置は、受信した分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を第３の装置に送信してよい。また、第３の装置は、第２の装置から受信したハッシュ値および第１の装置から受信した分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、上記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とを比較し、所定の処理を実

行するか否かを判定してよい。

[0028] また、第３の装置は、第２の装置から受信したハッシュ値および第１の装置から受信した分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、上記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とが一致する場合、所定の処理を実行してよい。

[0029] 図２は、本開示の一実施形態に係る情報処理方法と比較手法との差異について説明するための図である。なお、図２においては、自身のユーザ鍵ＵＫを用いて暗号化データＥＤおよび暗号化インデックスＥＩを生成しサーバに登録した共有元ユーザがユーザＵａとして示され、ユーザＵａの許諾に基づく暗号化データＥＤに対する検索を行う共有先ユーザがユーザＵｂとして示されている。

[0030] まず、比較手法について説明する。図２の左側には、一般的な検索可能暗号技術をマルチユーザ検索に適用した場合の比較手法の概要が示されている。

[0031] 比較手法の場合、共有先ユーザであるユーザＵｂは、共有元ユーザであるユーザＵａが暗号化データＥＤおよび暗号化インデックスＥＩの生成に用いたユーザＵａのユーザ鍵ＵＫをユーザＵａからシェアされることで、サーバに保管される暗号化データＥＤに対する検索を行うことができる。しかし、このようにユーザ鍵ＵＫを他のユーザにシェアする場合、なりすましなどが可能となることから、セキュリティ性が低下することとなる。

[0032] 一方、図２の右側には、本実施形態に係る情報処理方法（提案手法）の概要が示されている。本実施形態に係る情報処理方法では、まず、共有元ユーザであるユーザＵａが利用する第１の装置が、暗号化データＥＤおよび暗号化インデックスＥＩの生成に用いたユーザ鍵ＵＫを秘密分散処理により分散鍵Ｓ１および分散鍵Ｓ２に分割する。また、第１の装置は、生成した分散鍵Ｓ１および分散鍵Ｓ２を、共有先ユーザであるユーザＵｂが利用する第２の装置およびクラウド側に設置される第３の装置にそれぞれ配布する。

[0033] 次に、ユーザＵｂが利用する第２の装置は、ユーザＵｂにより入力された

検索ワードと分散鍵Ｓ１に基づく準同型ハッシュ演算を行い、算出したハッシュ値を第３の装置に送信する。

[0034] 次に、第３の装置は、第２の装置から受信したハッシュ値に対し、第１の装置から受信した分散鍵Ｓ２を用いてさらなる準同型ハッシュ演算を行う。続いて、第３の装置は、上記の準同型ハッシュ演算により算出したハッシュ値が暗号化インデックスＥＩに含まれるか否かを判定し、当該ハッシュ値が暗号化インデックスＥＩに含まれる場合には、ユーザＵｂが入力した検索ワードに対応する検索結果を第２の装置に送信してよい。ここで、上記の検索結果には、例えば、検索ワードを含む暗号化データＥＤや、検索ワードを含む暗号化データＥＤのリストなどが挙げられる。

[0035] このように、本実施形態に係る情報処理方法を実現する情報処理システムによれば、共有元ユーザのユーザ鍵を共有先ユーザにシェアすることなく、共有先ユーザが暗号化データの検索を行うことができ、セキュリティ性をより向上させることが可能となる。

[0036] 以下、本実施形態に係る情報処理方法を実現する情報処理システムが有する特徴と当該特徴により奏される効果について詳細に説明する。

[0037] ＜＜１．２．情報処理システム１の構成例＞＞

まず、本開示の一実施形態に係る情報処理システム１の構成例について説明する。図３は、本実施形態に係る情報処理システム１の構成例を示すブロック図である。図３を参照すると、本実施形態に係る情報処理システム１は、複数の情報処理端末１０と情報処理サーバ２０を備える。また、上記の各構成は、ネットワーク３０を介して、互いに通信が行えるように接続される。

[0038] （情報処理端末１０）

本実施形態に係る情報処理端末１０は、共有元ユーザまたは共有先ユーザが用いる情報処理装置である。すなわち、本実施形態に係る情報処理端末１０は、上述した第１の装置や第２の装置に相当する。なお、本実施形態に係る情報処理端末１０は、第１の装置であると同時に第２に装置であってもよ

い。情報処理端末１０を利用するユーザは、例えば、自身の登録した暗号化データに対する検索を他のユーザに許諾する共有元ユーザであると同時に、他のユーザが登録した暗号化データに対する検索を許諾された共有先ユーザで有り得る。

[0039] 本実施形態に係る情報処理端末１０は、例えば、ＰＣ（Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ）、スマートフォン、タブレットなどであってもよい。

[0040] なお、本開示では、情報処理端末１０を、クライアントと称する場合がある。また、本開示では、情報処理端末１０による処理を、ローカル側の処理、と称する場合がある。

[0041] （情報処理サーバ２０）

本実施形態に係る情報処理サーバ２０は、情報処理端末１０が生成した暗号化データや暗号化インデックスを保管し、また情報処理端末１０により処理リクエストに基づいて暗号化データに対する検索処理を実行する情報処理装置である。すなわち、本実施形態に係る情報処理サーバ２０は、上述した第３の装置に相当する。

[0042] なお、本開示では、情報処理サーバ２０を、単に、サーバと称する場合がある。また、本開示では、情報処理サーバ２０による処理を、クラウド側の処理、と称する場合がある。

[0043] （ネットワーク３０）

ネットワーク３０は、情報処理端末１０と情報処理サーバ２０、また情報処理端末１０同士を接続する機能を有する。ネットワーク３０は、インターネット、電話回線網、衛星通信網などの公衆回線網や、Ｅｔｈｅｒｎｅｔ（登録商標）を含む各種のＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）、ＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）などを含んでもよい。また、ネットワーク３０は、ＩＰ－ＶＰＮ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ－Ｖｉｒｔｕａｌ Ｐｒｉｖａｔｅ Ｎｅｔｗｏｒｋ）などの専用回線網を含んでもよい。また、ネットワーク３０は、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）など無線通信網を含んでもよい。

[0044] 以上、本開示の一実施形態に係る情報処理システム１の構成例について説明した。なお、図３を用いて説明した上記の構成はあくまで一例であり、本実施形態に係る情報処理システム１の構成は係る例に限定されない。本実施形態に係る情報処理システム１の構成は、仕様や運用に応じて柔軟に変形可能である。

[0045] ＜＜１．３．情報処理端末１０の機能構成例＞＞

次に、本開示の一実施形態に係る情報処理端末１０の機能構成例について説明する。図４は、本実施形態に係る情報処理端末１０の機能構成例を示すブロック図である。図４を参照すると、本実施形態に係る情報処理端末１０は、ユーザ鍵管理部１１０、入力部１２０、暗号化部１３０、秘密分散処理部１４０、復号部１５０、表示部１６０、通信部１７０を備える。

[0046] （ユーザ鍵管理部１１０）

本実施形態に係るユーザ鍵管理部１１０は、ユーザ鍵の生成や保存を行う。ユーザ鍵管理部１１０は、例えば、ユーザ鍵生成部とユーザ鍵保存部とを含んでもよい。

[0047] （入力部１２０）

本実施形態に係る入力部１２０は、ユーザによる暗号化対象データの入力や、検索ワードの入力を検出する。このために、本実施形態に係る入力部１２０は、例えば、キーボードやマウスなどの入力デバイスを備える。

[0048] （暗号化部１３０）

本実施形態に係る暗号化部１３０は、ユーザ鍵や分散鍵を用いた準同型ハッシュ演算を行う。本実施形態に係る暗号化部１３０は、ユーザ鍵を用いて暗号化データや暗号化インデックスを生成する登録処理部や、入力された検索ワードや分散鍵に基づく準同型ハッシュ演算を行う検索処理部として動作する。

[0049] （秘密分散処理部１４０）

本実施形態に係る秘密分散処理部１４０は、分散鍵の生成や、他の情報処理端末１０から受信した分散鍵の保管などを行う。本実施形態に係る秘密分

散処理部１４０は、例えば、ユーザ鍵を秘密分散処理により分割し複数の分散鍵を生成する。

[0050] （復号部１５０）

本実施形態に係る復号部１５０は、情報処理サーバ２０から受信した暗号化データをユーザ鍵を用いて復号する。

[0051] （表示部１６０）

本実施形態に係る表示部１６０は、画像やテキストなどの視覚情報を出力する。本実施形態に係る表示部１６０は、例えば、検索ワードなどの入力データの入力、および検索結果の提示などの処理リクエストの結果に係る表示を行うためのユーザインタフェースを具備する。

[0052] このために、本実施形態に係る表示部１６０は、視覚情報を提示する表示デバイスを備える。上記の表示デバイスには、例えば、液晶ディスプレイ（ＬＣＤ：Ｌｉｑｕｉｄ　Ｃｒｙｓｔａｌ　Ｄｉｓｐｌａｙ）装置、ＯＬＥＤ（Ｏｒｇａｎｉｃ　Ｌｉｇｈｔ　Ｅｍｉｔｔｉｎｇ　Ｄｉｏｄｅ）装置、タッチパネルなどが挙げられる。

[0053] （通信部１７０）

本実施形態に係る通信部１７０は、ネットワーク３０を介して、情報処理サーバ２０や他の情報処理端末１０との情報通信を行う。本実施形態に係る通信部１７０は、例えば、登録処理において、暗号化部１３０が暗号化した暗号化データや暗号化インデックスを情報処理サーバ２０に送信する。また、通信部１７０は、例えば、検索処理において、暗号化部１３０が準同型ハッシュ演算により算出したハッシュ値を情報処理サーバ２０や他の情報処理端末１０に送信する。また、通信部１７０は、例えば、秘密分散処理部１４０が生成した分散鍵を情報処理サーバ２０や他の情報処理端末１０に送信する。また、通信部１７０は、他の情報処理端末１０が生成した分散鍵を受信する。

[0054] 以上、本実施形態に係る情報処理端末１０の機能構成例について説明した。なお、図４を用いて説明した上記の構成はあくまで一例であり、本実施形

態に係る情報処理端末１０の機能構成は係る例に限定されない。本実施形態に係る情報処理端末１０の機能構成は、仕様や運用に応じて柔軟に変形可能である。

[0055] ＜＜１．４．情報処理サーバ２０の機能構成例＞＞

次に、本開示の一実施形態に係る情報処理サーバ２０の機能構成例について説明する。図５は、本実施形態に係る情報処理サーバ２０の機能構成例を示すブロック図である。図５を参照すると、本実施形態に係る情報処理サーバ２０は、分散鍵管理部２１０、データ管理部２２０、処理部２３０、および端末通信部２４０を備える。

[0056] （分散鍵管理部２１０）

本実施形態に係る分散鍵管理部２１０は、情報処理端末１０から受信した分散鍵の保管や、共有元ユーザが共有先ユーザに配布した分散鍵のマッチングなどを管理する。

[0057] （データ管理部２２０）

本実施形態に係るデータ管理部２２０は、情報処理端末１０から受信した暗号化データや暗号化インデックスを保管する。

[0058] （処理部２３０）

本実施形態に係る処理部２３０は、情報処理端末１０から受信したハッシュ値に基づく判定を行い、情報処理端末１０に対する検索結果の提示などの処理を実行する。本実施形態に係る処理部２３０は、準同型ハッシュ処理部や、ハッシュ値に係るビット一致判定を行う判定部などを含んでもよい。なお、本実施形態に係る処理部２３０が実行する処理は、上記に限定されない。本実施形態に係る処理部２３０は、後述するように、受信したハッシュ値に基づく決済処理や文書公開などを行ってもよい。

[0059] （端末通信部２４０）

本実施形態に係る端末通信部２４０は、ネットワーク３０を介して、情報処理端末１０との情報通信を行う。本実施形態に係る端末通信部２４０は、例えば、情報処理端末１０から暗号化データや暗号化インデックスを受信す

る。また、本実施形態に係る端末通信部２４０は、例えば、情報処理端末１０からハッシュ値を受信し、当該ハッシュ値に基づく処理の結果などを情報処理端末１０に送信する。

[0060] 以上、本実施形態に係る情報処理サーバ２０の機能構成例について説明した。なお、図５を用いて説明した上記の機能構成はあくまで一例であり、本実施形態に係る情報処理サーバ２０の機能構成は係る例に限定されない。本実施形態に係る情報処理サーバ２０の機能構成は、仕様や運用に応じて柔軟に変形可能である。

[0061] ＜＜１．５．機能の詳細＞＞

次に、本実施形態に係る情報処理システム１が有する機能について詳細に説明する。上述したように、本実施形態に係る情報処理システム１は、検索可能暗号技術を用いたセキュリティ性の高いマルチユーザ検索を実現する。ここで、検索可能暗号技術の代表的な手法としては、公開鍵暗号方式、共通鍵暗号方式、ハッシュ方式などが挙げられる。

[0062] しかし、上記の公開鍵暗号方式は、ペアリングを用いた方式であるため性能に課題を有し、また共通鍵暗号方式は、シングルユーザであれば公開鍵暗号方式に比べ実用に耐え得る性能を得られるものの、マルチユーザへの適用が困難である。

[0063] このため、本実施形態に係る情報処理方法では、ハッシュ形式による検索可能暗号技術を採用する。ハッシュ形式とは、キーワードリストをハッシュ化したものを暗号化インデックスとして用いる方式であり、本実施形態に係る情報処理方法では、ユーザごとに固有のユーザ鍵を利用した鍵付きハッシュ（Ｋｅｙｅｄ　ｈａｓｈ）を用いることで秘匿性を確保することが可能である。

[0064] また、ハッシュ方式によれば、キーワード数に依らない固定長の暗号化インデックスを生成することができ、ハッシュ計算による処理が可能なため暗号化に比べ処理を高速化することが可能である。

[0065] なお、本実施形態に係る情報処理方法では、準同型ハッシュ演算により算

出したハッシュ値をそのものの他、当該ハッシュ値をＡＭＱ（Ａｐｐｒｏｘｉｍａｔｅ　Ｍｅｍｂｅｒｓｈｉｐ　Ｑｕｅｒｙ）形式にエンコードした暗号化インデックスが用いられてよい。上記のＡＭＱ形式には、例えば、ブルームフィルタやカウンティングフィルタが挙げられる。

[0066] ここで、情報処理端末１０による上記の暗号化インデックスの生成について詳細に述べる。図６は、本実施形態に係る暗号化インデックスの生成について説明するための図である。

[0067] まず、本実施形態に係る情報処理端末１０の暗号化部１３０は、ユーザ操作に基づいて、任意のデータＤに含まれるキーワードＷを抽出し、キーワードリストＫＬを生成する。この際、暗号化部１３０は、例えば、形態素解析によるキーワード抽出やｎ－ｇｒａｍによる単語抽出を行ってもよい。

[0068] 次に、本実施形態に係る暗号化部１３０は、生成したキーワードリストＫＬをユーザ鍵ＵＫを用いてハッシュ化し、暗号化インデックスＥＩを生成する。具体的には、本実施形態に係る暗号化部１３０は、各キーワードＷごとに、公開情報である準同型ハッシュパラメータｇ、ユーザ鍵ＵＫ、キーワードＷに基づく準同型ハッシュ演算を行い、算出したハッシュ値$g^{(UK+W)}$をブルームフィルタにマッピングすることで暗号化インデックスＥＩを生成することができる。このため、キーワードリストＫＬに複数のキーワードＷが含まれる場合には、ブルームフィルタには複数のビットが立つこととなる。暗号化部１３０は、１つのキーワードＷに対して異なるハッシュ関数を用いてハッシュ値を計算し複数のビットを立てることもできる。

[0069] 通信部１７０は、暗号化部１３０が上記のように生成した暗号化インデックスＥＩを、対応する暗号化データＥＤと共に情報処理サーバ２０に送信する。また、情報処理サーバ２０のデータ管理部２２０は、受信した暗号化インデックスＥＩおよび暗号化データＥＤを保管する。

[0070] 次に、暗号化データＥＤおよび暗号化インデックスＥＩの登録を行ったユーザ本人による暗号化データの検索について述べる。図７は、本実施形態に係る暗号化データＥＤおよび暗号化インデックスＥＩの登録を行ったユーザ

本人による暗号化データの検索について説明するための図である。

[0071] 登録を行ったユーザ本人による検索の場合、暗号化部１３０は、入力部１２０から出力される検索ワードリストＳＷＬに対し上述の準同型ハッシュ演算を行い、算出したハッシュ値をブルームフィルタにマッピングした暗号化キーワードＥＫＷを生成する。この際、検索ワードリストＳＷＬに複数の検索ワードが含まれ、かつ検索条件としてＡＮＤ検索が指定された場合には、暗号化部１３０は、各検索ワードに係るハッシュ値を単一のブルームフィルタにマッピングしてよい。一方、検索ワードリストＳＷＬに複数の検索ワードが含まれ、かつ検索条件としてＯＲ検索が指定された場合には、暗号化部１３０は、各検索ワードごとにブルームフィルタへのマッピングを行う。

[0072] また、通信部１７０は、暗号化部１３０が上記のように生成した暗号化キーワードＥＫＷを、情報処理サーバ２０に送信する。

[0073] 次に、情報処理サーバ２０の処理部２３０は、情報処理端末１０から受信した暗号化キーワードＥＫＷと、データ管理部２２０が保管する複数の暗号化インデックスＥＩの比較を行う。具体的には、処理部２３０は、暗号化キーワードＥＫＷと暗号化インデックスＥＩ１～ＥＩ３の間でビット単位の一致判定を行ってよい。

[0074] ここで、暗号化キーワードＥＫＷの１値ビットに対応するビットが、暗号化インデックスＥＩにおいても同様に１値ビットである場合、処理部２３０は、暗号化キーワードＥＫＷが暗号化インデックスＥＩに含まれていると判定し、検索結果ＳＲを端末通信部２４０を介して情報処理端末１０に送信する。検索結果ＳＲとしては、例えば、暗号化インデックスＥＩに対応する暗号化データＥＤや、暗号化データＥＤのリストなどが挙げられる。

[0075] 次に、本実施形態に係る共有先ユーザによる暗号化データの検索について説明する。図８は、本実施形態に係る共有先ユーザによる暗号化データの検索について説明するための図である。なお、図２においては、情報処理端末１０ａが共有元ユーザが利用する第１の装置に相当し、情報処理端末１０ｂが共有先ユーザが利用する第２の装置に相当する。また、情報処理サーバ２

０は、第３の装置に相当する。

[0076] まず、共有先ユーザが利用する情報処理端末１０ａの秘密分散処理部１４０は、共有元ユーザのユーザ鍵ＵＫを秘密分散処理により分割し、２つの分散鍵Ｓ１およびＳ２を生成する。この際、秘密分散処理部１４０は、加法準同型性を有する秘密分散処理を用いて分散鍵の生成を行う。なお、秘密分散処理部１４０は、共有元ユーザが共有先ユーザによる検索を許諾した際に１度だけ分散鍵の生成を行ってよい。ただし、共有先ユーザが利用する情報処理端末１０ｂの紛失時などにおいては、秘密分散処理部１４０は、再度、分散鍵の生成を行ってもよい。

[0077] また、通信部１７０は、分散鍵Ｓ１およびＳ２を情報処理端末１０ｂおよび情報処理サーバ２０にそれぞれ配布する。なお、情報処理端末１０ｂに対する分散鍵Ｓ１の配布については、例えば、近距離無線通信を利用した配布、ＱＲコード（登録商標）などの画像データを介した送付、情報処理サーバ２０を介したエンドツーエンド（ｅｎｄ　ｔｏ　ｅｎｄ）通信による配布などが想定される。

[0078] 次に、情報処理端末１０ｂの暗号化部１３０は、図中右側に示すように、検索ワードとして入力されたキーワードワードW^1～W^Nごとに、受信した分散鍵Ｓ１および準同型ハッシュパラメータｇを用いた、べき乗の準同型ハッシュ演算を行いハッシュ値$g^{(S1+WN)}$を算出する。ここで、準同型ハッシュパラメータｇは、予め情報処理端末１０ｂと情報処理サーバ２０とに共有された、同一の値を有する公開情報である。また、情報処理端末１０ｂの通信部１７０は、算出されたハッシュ値を情報処理サーバ２０に送信する。

[0079] 次に、情報処理サーバ２０の処理部２３０は、情報処理端末１０ｂから受信したハッシュ値$g^{(S1+WN)}$および情報処理端末１０ａから受信した分散鍵Ｓ２に基づく準同型ハッシュ演算を行う。

[0080] 具体的には、処理部２３０は、分散鍵Ｓ２と準同型ハッシュパラメータｇに基づいてべき乗の準同型ハッシュ演算を行いハッシュ値g^{S2}を算出する。続いて、処理部２３０は、算出したハッシュ値g^{S2}と情報処理端末１０ｂか

ら受信したハッシュ値ｇ(S1+WN)とに基づく乗算の準同型ハッシュ演算を行う。この際、算出されるハッシュ値は、ｇ(S1+W)＊ｇS2＝ｇ(S1+S2+W)＝ｇ(UK+W)、となり、図７を用いて説明した登録者本人による検索時のハッシュ値と同一となる。

[0081] このように、本実施形態に係る情報処理方法によれば、共有元ユーザのユーザ鍵を分割した２つの分散鍵Ｓ１およびＳ２を、共有先ユーザが利用する情報処理端末１０ｂおよび情報処理サーバ２０にそれぞれ配布することで、分散鍵Ｓ１およびＳ２のペアがマッチする場合にのみ、共有先ユーザが共有元ユーザと同様の情報検索を行うことが可能となる。

[0082] 本実施形態に係る情報処理方法によれば、分散鍵Ｓ１またはＳ２のみでは、暗号化データＥＤの取得が行えないため、サービス管理者などによる不正なデータ取得などを効果的に防止することが可能となる。

[0083] また、本実施形態に係る情報処理サーバ２０の分散鍵管理部２１０は、情報処理端末１０ａの秘密分散処理部１４０からの削除リクエストを受信した場合、該当する分散鍵を削除してよい。上記の機能によれば、例えば、許諾した期間が経過した場合や、情報処理端末１０ｂの紛失時などにおいても、情報処理サーバ２０が保管する暗号化データＥＤを安全に保護することが可能となる。

[0084] 次に、本実施形態に係る分散鍵管理部２１０による分散鍵の管理方法について説明する。上記では、処理部２３０が、情報処理端末１０ｂから受信したハッシュ値と、情報処理端末１０ａから受信した分散鍵を用いて算出したハッシュ値とに基づく乗算の準同型ハッシュ演算を行うことを述べた。この際、本実施形態に係る処理部２３０は、例えば、分散鍵管理部２１０が記憶する管理テーブルに基づいて、情報処理端末１０ｂに対応する分散鍵を特定し、当該分散鍵を分散鍵管理部２１０から取得することができる。

[0085] 図９は、本実施形態に係る分散鍵の管理テーブルの一例を示す図である。図９に示すように、本実施形態に係る分散鍵の管理テーブルには、例えば、分散鍵ＩＤ、共有先ユーザＩＤ、共有元ユーザＩＤ、および分散鍵が登録さ

れる。

[0086] 例えば、図８に示した一例の場合、情報処理端末１０ｂの利用者である共有先ユーザ（ユーザＢ）が、上述したユーザインタフェースを介してサービスにログインすることで、共有先ユーザ（ユーザＢ）に対応する共有先ユーザＩＤ（ユーザＩＤ^{B}）が特定される。

[0087] また、共有先ユーザ（ユーザＢ）が上記ユーザインタフェース上において、検索対象として共有元ユーザ（ユーザＡ）が所有する暗号化データを指定することで、共有元ユーザＩＤ（ユーザＩＤ^{A}）が特定される。

[0088] この場合、本実施形態に係る処理部２３０は、上記で特定された共有先ユーザＩＤ（ユーザＩＤ^{B}）と共有元ユーザＩＤ（ユーザＩＤ^{A}）とをキーに管理テーブルを検索することで、分散鍵ＩＤ（５）に対応する分散鍵（分散鍵^{BA}）を取得することが可能である。

[0089] なお、図９では、共有元ユーザ本人が検索を行う場合の鍵にも秘密分散処理が適用される一例を示している（分散鍵^{AA}、分散鍵^{BB}が該当）。この場合、共有元ユーザ本人が検索を行う場合にも図８に示したような分散鍵を用いた準同型ハッシュ演算による処理が行われてよい。

[0090] 一方、上述したように、共有元ユーザは、自身のユーザ鍵ＵＫを情報処理端末１０に保管することができるため、図９に示す自身の分散鍵（分散鍵^{AA}、分散鍵^{BB}が該当）は、必ずしも情報処理サーバ２０に保管されなくてもよい。

[0091] なお、共有先ユーザが、検索が許諾されている全ての共有元ユーザのデータを検索する場合、処理部２３０は、共有先ユーザＩＤに紐付く全ての共有元ＩＤと、対応する分散鍵とをスキャンして取得することも可能である。

[0092] 次に、共有先ユーザが利用する情報処理端末１０による暗号化データの復号について説明する。図８に示した検索により、共有先ユーザが利用する情報処理端末１０ｂは、検索結果として暗号化データＥＤを情報処理サーバ２０からダウンロードすることが可能である。

[0093] しかし、暗号化データＥＤは、共有元ユーザに固有のユーザ鍵ＵＫ（秘密

鍵）で暗号化されているため、ユーザ鍵ＵＫを保持しない情報処理端末１０ｂは、そのままでは暗号化データＥＤを復号することができない。

[0094] そこで、本実施形態に係る情報処理方法では、プロキシ暗号による再暗号化を適用することで、上記の点を解決する。

[0095] 図１０は、本実施形態に係る共有先ユーザが利用する情報処理端末１０による暗号化データの復号について説明するための図である。

[0096] 上述したように、共有元ユーザが利用する情報処理端末１０ａは、暗号化データＥＤおよび暗号化インデックスＥＩを情報処理サーバ２０に送信した後、生成した分散鍵Ｓ１およびＳ２を、情報処理サーバ２０および共有元ユーザにより暗号化データＥＤの検索が許諾された共有先ユーザが利用する情報処理端末１０ｂにそれぞれ配布する。

[0097] 次に、情報処理端末１０ａの秘密分散処理部１４０は、共有先ユーザが利用する情報処理端末１０ｂから、共有先ユーザの公開鍵ＰＫを受信し、公開鍵ＰＫと共有元ユーザの秘密鍵SK^{A}を用いて再暗号化鍵ＲＥＫを生成する。また、通信部１７０は、秘密分散処理部１４０が生成した再暗号化鍵ＲＥＫを情報処理サーバ２０に送信する。

[0098] この後、共有先ユーザが利用する情報処理端末１０ｂによる情報検索に係る処理リクエストの結果、対応する暗号化データＥＤが存在する場合、処理部２３０は、情報処理端末１０ａから受信した再暗号化鍵ＲＥＫを用いて暗号化データＥＤを再暗号化した再暗号化データＲＥＤを生成し、端末通信部２４０が検索結果として再暗号化データＲＥＤを情報処理端末１０ｂに送信する。

[0099] 次に、情報処理端末１０ｂの復号部１５０は、受信した再暗号化データＲＥＤを共有先ユーザの秘密鍵SK^{B}を用いて復号する。

[0100] このように、本実施形態に係る情報処理方法によれば、共有元ユーザの秘密鍵を共有先ユーザが利用する情報処理端末１０ｂにシェアしなくとも、情報処理端末１０ｂが共有先ユーザの秘密鍵を用いて、共有元ユーザのデータを閲覧することが可能となる。

[0101] 次に、本実施形態に係るユーザインタフェースについて説明する。上述したように、本実施形態に係る情報処理サーバ２０は、検索ワードなどの入力データの入力、および処理リクエストのけ結果に係る表示を行うためのユーザインタフェースを制御してよい。共有元ユーザや共有先ユーザは、上記のユーザインタフェースを介して、検索のリクエストや検索結果の閲覧を行うことができる。

[0102] 図１１は、本実施形態に係る情報処理サーバ２０が制御するユーザインタフェースＵＩの一例である。ユーザは、例えば、図１１の左側に示すように、ユーザインタフェースＵＩに表示される検索フィールドＦ１に認識の検索ワードを入力し、検索ボタンを押下することで、当該検索ワードが含まれる暗号化データのリストの一覧を取得できてもよい。

[0103] 図１１に示す一例の場合、ユーザインタフェースＵＩには、ユーザが検索フィールドＦ１に入力した検索ワード「土地」が含まれる暗号化データのリストが、データの所有者ごとに表示されている。ユーザが他のユーザにデータの検索を許諾されている共有先ユーザである場合、検索結果には、「日記１」や「日記２」のような自身のデータに係るリストのみではなく、「相続１」のような共有元ユーザのデータに係るリストも表示される。

[0104] また、この際、共有先ユーザは、例えば、表示されるリストから「相続１」などのデータを選択することで、図１１の右側に示すように、選択したデータの詳細情報を確認することができる。上記の詳細情報には、暗号化される前のデータそのものや、公開状況などが含まれてもよい。

[0105] このように、本実施形態に係る情報処理方法を実現する情報処理システム１によれば、日記や遺言などの秘匿性の高い文書データを、許諾したユーザにのみ安全かつ少ない処理負担で検索させることが可能となり、検索処理を伴う各種のサービスにおいて活用が見込まれる。

[0106] なお、上記では、本実施形態に係る第２の装置が１つである場合、すなわち共有先ユーザが１人である場合を主な例として説明した。一方、本実施形態に過かある第２の装置の数、すなわち共有先ユーザの数は係る例に限定さ

れない。本実施形態に係る第２の装置、共有先ユーザは複数であってもよい。

[0107] すなわち、共有元ユーザが利用する情報処理端末１０ａの秘密分散処理部１４０は、秘密分散処理により、共有先ユーザの数に１を加えた数の分散鍵を生成してよい。例えば、共有先ユーザが１人である場合、共有元ユーザが利用する情報処理端末１０ａの秘密分散処理部１４０は、共有先ユーザが利用する情報処理端末１０ｂと情報処理サーバ２０にそれぞれ配布するための合計２つの分散鍵を生成してよい。また、例えば、共有先ユーザが３人である場合、共有元ユーザが利用する情報処理端末１０ａの秘密分散処理部１４０は、３人の共有先ユーザが利用する３つの情報処理端末１０ｂと情報処理サーバ２０にそれぞれ配布するための合計４つの分散鍵を生成してよい。

[0108] 図１２は、本実施形態に係る複数の共有先ユーザが存在する場合の処理について説明するための図である。なお、図１２には、第１の装置に相当する情報処理端末１０ａを利用する共有元ユーザにより、第２の装置に相当する情報処理端末１０ｂ－１および１０ｂ－２を利用する２人の共有先ユーザが設定された場合の一例が示されている。

[0109] 図１２に示す一例の場合、共有元ユーザが利用する情報処理端末１０ａの秘密分散処理部１４０は、共有元ユーザのユーザ鍵ＵＫを秘密分散処理により分割し、３の分散鍵Ｓ１～Ｓ３を生成している。また、情報処理端末１０ａの通信部１７０は、秘密分散処理部１４０が生成した３つの分散鍵Ｓ１～Ｓ３を、情報処理端末１０ｂ－１、情報処理端末１０ｂ－２、情報処理サーバ２０にそれぞれ配布している。

[0110] この際、本実施形態に係る第３の装置に相当する情報処理サーバ２０は、第２の装置に相当する複数の情報処理端末１０ｂのすべてが、分散鍵を用いた準同型ハッシュ演算により、順に算出したハッシュ値と、ユーザ鍵ＵＫに基づく準同型ハッシュ演算により算出されたハッシュ値との比較を行うことで、所定の処理の実行可否を判定してよい。

[0111] より具体的には、本実施形態に係る第２の装置に相当する複数の情報処理

端末１０ｂは、処理理リクエストの起点となる起点端末と、処理リクエストが経由する経由端末に分けられる。例えば、処理リクエストが、検索結果の提示に係るリクエストである場合、上記の起点端末とは、検索を実行したい共有先ユーザの一人により任意の検索ワードが入力される端末を指す。

[0112] 図１２に示す一例の場合、情報処理端末１０ａから分散鍵Ｓ１を配布された情報処理端末１０ｂ－１が上記の起点端末に相当する。この際、情報処理端末１０ｂ－１は、分散鍵Ｓ１、およびユーザが入力した検索ワードから抽出した検索ワードリストＳＷＬに基づく準同型ハッシュ演算により算出したハッシュ値を、経由端末に相当する情報処理端末１０ｂ－２に送信する。

[0113] 次に、経由端末に相当する情報処理端末１０ｂ－２は、経由端末に相当する情報処理端末１０ｂ－１から受信したハッシュ値、および分散鍵Ｓ２に基づく準同型ハッシュ演算により算出したハッシュ値を算出する。

[0114] ここで、未だ他の準同型ハッシュ演算を行っていない他の経由端末が存在する場合、情報処理端末１０ｂ－２は、算出したハッシュ値を当該他の経由端末のうちの１つに送信してよい。一方、図１２に示すように、準同型ハッシュ演算を行っていない他の経由端末が存在しない場合、情報処理端末１０ｂ－２は、算出したハッシュ値を第３の装置に相当する情報処理サーバ２０に送信する。

[0115] 次に、情報処理サーバ２０は、すべての第２の装置、すなわち情報処理端末１０ａから分散鍵が配布された情報処理端末１０ｂにより順に算出されたハッシュ値に対し、情報処理端末１０ａから受信した分散鍵Ｓ３に基づく準同型ハッシュ演算により算出したハッシュ値を乗算することで、ユーザ鍵ＵＫと同様のハッシュ値を取得することができる。

[0116] このように、本実施形態に係る情報処理システム１によれば、情報処理端末１０ａから分散鍵を配布された他の情報処理端末１０ｂによる準同型ハッシュ演算が行われない限り、ある情報処理端末１０ｂが単独でデータにアクセスすることを防止することができる。また、それぞれの情報処理端末１０ｂは、準同型ハッシュ演算の結果としてのハッシュ値のみを受信するため、

他の情報処理端末１０ｂに配布された分散鍵を入手することができないことから、共有先ユーザの１人が他の共有先ユーザに配布された分散鍵を傍受し不当な情報取得を行うことを防止することができる。

[0117] なお、本実施形態に係る情報処理サーバ２０の処理部２３０が実行する処理は、暗号化データの検索結果の提示に限定されない。本実施形態に係る情報処理方法は、上述した秘密分散処理および検索可能暗号技術をベースとした種々の処理に適用され得る。

[0118] 例えば、本実施形態に係る情報処理方法は、決算処理等に係る承認フローの一部として用いることが可能である。図１３は、本実施形態に係る情報処理方法を適用した承認フローの一例について説明するための図である。

[0119] 図１３には、担当社員により依頼された決済処理を、課長、部長を経て経理部が承認する場合の一例が示されている。

[0120] 図１２に示す一例の場合、まず、経理部が管理する第１の装置により、ユーザ鍵ＵＫが秘密分散処理により分割され、また生成された分散鍵Ｓ１～Ｓ３が、担当社員、課長、部長が利用する第２の装置にそれぞれ配布される。

[0121] 上記の配布処理の後、担当社員が利用する第２の装置は、配布された分散鍵Ｓ１、準同型ハッシュパラメータｇ、および担当社員により入力された決済文書であるデータＤに基づく準同型ハッシュ演算処理を行い、算出したハッシュ値を直属の上長である課長が利用する第２の装置に送信する。

[0122] 次に、課長が利用する第２の装置は、受信したハッシュ値と、分散鍵Ｓ２、準同型ハッシュパラメータｇに基づく準同型ハッシュ演算を行い、算出したハッシュ値を次の承認先である部長が利用する第２の装置に送信する。

[0123] 次に、部長が利用する第２の装置は、受信したハッシュ値と、分散鍵Ｓ３、準同型ハッシュパラメータｇに基づく準同型ハッシュ演算を行い、算出したハッシュ値を最終承認先である経理部が管理する第３の装置に送信する。

[0124] ここで、上記のように複数の第２の装置により順に算出されたハッシュ値は、電子署名としての役割を果たすものあってよい。第３の装置は、受信した上記の電子署名の検証を行うことで、決済処理を実行するか否かを判定す

ることができる。

[0125] 具体的には、経理部が管理する第３の装置は、部長が利用する第２の装置から受信したハッシュ値が、ユーザ鍵ＵＫと決済文書であるデータＤに基づく準同型ハッシュ演算により算出されたハッシュ値とが一致するか否かを判定する（$g^{(S1+S2+S3+D)}$？＝$g^{(UK+D)}$）。

[0126] ここで、両者が一致する場合（$g^{(S1+S2+S3+D)}$＝＝$g^{(UK+D)}$）、第３の装置は、決済文書であるデータＤに係る決済処理を実行してよい。

[0127] 以上、本実施形態に係る情報処理方法が、決済処理などに係る承認フローの一部として適用される場合について説明した。本実施形態に係る情報処理方法を適用した上記のような承認フローによれば、非常にセキュリティ性の高い承認フローを実現するとともに、正規の承認ルートを通っていない申請を確実に棄却することが可能となる。

[0128] また、本実施形態に係る情報処理方法は、分散鍵が配布された共有先ユーザの全員一致による所定の処理の実行に適用されてもよい。図１４は、本実施形態に係る情報処理方法を適用した共有先ユーザの全員一致による処理実行の一例を示す図である。

[0129] 図１４には、父が遺した遺言が家族全員の意思の一致により公開される場合の一例が示されている。

[0130] 図１３に示す一例の場合、まず、第１の装置により、ユーザ鍵ＵＫが秘密分散処理により分割され、また生成された分散鍵Ｓ１～Ｓ３が、母、長女、長男が利用する第２の装置にそれぞれ配布される。また、図１３に示す一例では、第１の装置により生成された遺言公開リクエストであるデータＤが、起点端末である母が利用する第２の装置に送信されている。

[0131] 上記の配布処理の後、母が利用する第２の装置は、配布された分散鍵Ｓ１、準同型ハッシュパラメータｇ、および遺言公開リクエストであるデータＤに基づく準同型ハッシュ演算処理を行い、算出したハッシュ値を長女が利用する第２の装置に送信する。

[0132] その後、長女および長男が利用する第２の装置は、図１３で示した処理と

同様の処理を行う。

[0133] また、父の残した遺言を保管する第３の装置は、長男が利用する第２の装置から受信したハッシュ値が、ユーザ鍵ＵＫとデータＤに基づく準同型ハッシュ演算により算出されたハッシュ値とが一致するか否かを判定する（$g^{(S1+S2+S3+D)}$？＝$g^{(UK+D)}$）。

[0134] ここで、両者が一致する場合（$g^{(S1+S2+S3+D)}$＝＝$g^{(UK+D)}$）、第３の装置は、父の遺言が暗号化された暗号化データＥＤを、母、長女、長男が利用する第２装置に送信してよい。

[0135] 以上、本実施形態に係る情報処理方法が、分散鍵が配布された共有先ユーザの全員一致による所定の処理の実行に適用される場合について説明した。本実施形態に係る情報処理方法を適用した上記のような処理実行によれば、秘匿性が高くかつ重要な文書の公開などを、関係者全員の意思の一致にのみ基づいて実行することが可能となる。

[0136] なお、図１３および図１４に示した一例の場合、第１の装置および第３の装置は、同一の装置として実現されてもよい。本実施形態に係る情報処理システム１の機能構成は、適用されるサービスに応じて柔軟に変形可能である。

[0137] ＜＜１．６．動作の流れ＞＞

次に、本開示の一実施形態に係る情報処理システム１の動作の流れについて詳細に説明する。

[0138] まず、本実施形態に係る情報処理システム１による暗号化データおよび暗号化インデックスの登録の流れについて述べる。図１５は、本実施形態に係る暗号化データおよび暗号化インデックスの登録の流れを示すシーケンス図である。

[0139] 図１５を参照すると、まず、共有元ユーザが利用する第１の装置に相当する情報処理端末１０ａのユーザ鍵管理部１１０ａが、ユーザ鍵の生成を行う（Ｓ１１０１）。また、ユーザ鍵管理部１１０ａは、ステップＳ１１０１において生成したユーザ鍵を内部ストレージなどに保存する。

[0140] 次に、入力部１２０ａがユーザの入力操作に基づいて、暗号化の対象となるデータを取得する（Ｓ１１０３）。また、入力部１２０ａは、ステップＳ１１０２において取得したデータを暗号化部１３０ａに送信する（Ｓ１１０４）。

[0141] また、ユーザ鍵管理部１１０ａは、暗号化部１３０ａからの要求などに基づいて、ステップＳ１１０２において保存したユーザ鍵を暗号化部１３０ａに送信する。

[0142] 次に、暗号化部１３０ａは、ステップＳ１１０４において受信したデータからキーワードの抽出を行う（Ｓ１１０６）。

[0143] また、暗号化部１３０ａは、ステップＳ１１０４において受信したデータを、ステップＳ１１０５において受信したユーザ鍵を用いて暗号化して暗号化データを生成し（Ｓ１１０７）、同様に、ステップＳ１１０６において抽出したキーワードを暗号化し暗号化インデックスを生成する（Ｓ１１０８）。

[0144] 続いて、暗号化部１３０ａは、ステップＳ１１０７およびＳ１１０８において生成した暗号化データおよび暗号化インデックスを、通信部１７０ａを介して、第３の装置に相当する情報処理サーバ２０に送信する（Ｓ１１０９）。

[0145] 次に、情報処理サーバ２０のデータ管理部２２０は、ステップＳ１１０９において受信した暗号化データおよび暗号化インデックスの保存を行う（Ｓ１１１０およびＳ１１１１）。

[0146] 以上、本実施形態に係る暗号化データおよび暗号化インデックスの登録の流れについて説明した。次に、本実施形態に係る分散鍵配布の流れについて説明する。図１６は、本実施形態に係る分散鍵配布の流れを示すシーケンス図である。

[0147] 図１６を参照すると、まず、共有元ユーザが利用する第１の装置に相当する情報処理端末１０ａのユーザ鍵管理部１１０ａが、図１５に示すステップＳ１１０２において保存したユーザ鍵を秘密分散処理部１４０ａに送信する

（Ｓ１２０１）。

[0148] 次に、秘密分散処理部１４０ａは、ステップＳ１２０１において受信したユーザ鍵を秘密分散処理により分割し２つの分散鍵を生成する（Ｓ１２０２）。

[0149] 次に、秘密分散処理部１４０ａは、ステップＳ１２０２において生成した分散鍵のうちの一方を、通信部１７０ａを介して、第２の装置に相当する情報処理端末１０ｂに配布する（Ｓ１２０３）。

[0150] 情報処理端末１０ｂの秘密分散処理部１４０ｂは、ステップＳ１２０３において受信した分散鍵を保存する（Ｓ１２０４）。

[0151] また、秘密分散処理部１４０ａは、ステップＳ１２０２において生成した分散鍵のうちのもう一方を、通信部１７０ａを介して、第３の装置に相当する情報処理サーバ２０に配布する（Ｓ１２０５）。

[0152] 情報処理サーバ２０の分散鍵管理部２１０は、ステップＳ１２０５において受信した分散鍵を保存する（Ｓ１２０６）。

[0153] 以上、本実施形態に係る分散鍵配布の流れについて説明した。次に、本実施形態に係る検索処理の流れについて説明する。図１７は、本実施形態に係る検索処理の流れを示すシーケンス図である。

[0154] 図１７を参照すると、まず、第２の装置に相当する情報処理端末１０ｂの入力部１２０ｂが、ユーザによる入力操作に基づいて、検索ワードを取得する（Ｓ１３０１）。また、入力部１２０ｂは、ステップＳ１３０１において取得した検索ワードを暗号化部１３０に送信する（Ｓ１３０２）。

[0155] 次に、秘密分散処理部１４０ｂが、暗号化部１３０ｂによる要求などに基づいて、図１６に示すステップＳ１２０４において保存した分散鍵を暗号化部１３０に送信する（Ｓ１３０３）。

[0156] 次に、暗号化部１３０ｂは、ステップＳ１３０２において受信した検索ワード、およびステップＳ１３０３において受信した分散鍵に基づく準同型ハッシュ演算を行う（Ｓ１３０４）。

[0157] 暗号化部１３０ｂは、ステップＳ１３０４において算出したハッシュ値を

、通信部１７０ｂを介して、第３の装置に相当する情報処理サーバ２０に送信する（Ｓ１３０５）。

[0158] 次に、情報処理サーバ２０の分散鍵管理部２１０は、ステップＳ１３０５においてハッシュ値を受信した処理部２３０による要求などに基づいて、図１６のステップＳ１２０６において保存した分散鍵を処理部２３０に送信する（Ｓ１３０６）。

[0159] 次に、処理部２３０は、ステップＳ１３０５において受信したハッシュ値、およびステップＳ１３０６において受信した分散鍵に基づくハッシュ演算を行う（Ｓ１３０７）。

[0160] 続いて、処理部２３０は、ステップＳ１３０７において算出したハッシュ値と、図１５に示すステップＳ１１１１において保存した暗号化インデックスと、の間におけるビット一致判定を行う（Ｓ１３０８）。

[0161] ここで、検索ワードが暗号化インデックスに含めていると判定した場合、処理部２３０は、当該検索ワードに対応する検索結果を情報処理端末１０ｂに送信する（１３０９）。

[0162] 次に、情報処理端末１０ｂの復号部１５０ｂは、ステップＳ１３０９において受信した検索結果の復号を行う（Ｓ１３１０）。

[0163] ＜２．ハードウェア構成例＞

次に、本開示の一実施形態に係る情報処理端末１０および情報処理サーバ２０に共有するハードウェア構成例について説明する。図１８は、本開示の一実施形態に係る情報処理端末１０および情報処理サーバ２０のハードウェア構成例を示すブロック図である。図１８を参照すると、情報処理サーバ２０は、例えば、プロセッサ８７１と、ＲＯＭ８７２と、ＲＡＭ８７３と、ホストバス８７４と、ブリッジ８７５と、外部バス８７６と、インターフェース８７７と、入力装置８７８と、出力装置８７９と、ストレージ８８０と、ドライブ８８１と、接続ポート８８２と、通信装置８８３と、を有する。なお、ここで示すハードウェア構成は一例であり、構成要素の一部が省略されてもよい。また、ここで示される構成要素以外の構成要素をさらに含んでも

よい。

[0164] （プロセッサ８７１）

プロセッサ８７１は、例えば、演算処理装置又は制御装置として機能し、ＲＯＭ８７２、ＲＡＭ８７３、ストレージ８８０、又はリムーバブル記録媒体９０１に記録された各種プログラムに基づいて各構成要素の動作全般又はその一部を制御する。

[0165] （ＲＯＭ８７２、ＲＡＭ８７３）

ＲＯＭ８７２は、プロセッサ８７１に読み込まれるプログラムや演算に用いるデータ等を格納する手段である。ＲＡＭ８７３には、例えば、プロセッサ８７１に読み込まれるプログラムや、そのプログラムを実行する際に適宜変化する各種パラメータ等が一時的又は永続的に格納される。

[0166] （ホストバス８７４、ブリッジ８７５、外部バス８７６、インターフェース８７７）

プロセッサ８７１、ＲＯＭ８７２、ＲＡＭ８７３は、例えば、高速なデータ伝送が可能なホストバス８７４を介して相互に接続される。一方、ホストバス８７４は、例えば、ブリッジ８７５を介して比較的データ伝送速度が低速な外部バス８７６に接続される。また、外部バス８７６は、インターフェース８７７を介して種々の構成要素と接続される。

[0167] （入力装置８７８）

入力装置８７８には、例えば、マウス、キーボード、タッチパネル、ボタン、スイッチ、及びレバー等が用いられる。さらに、入力装置８７８としては、赤外線やその他の電波を利用して制御信号を送信することが可能なリモートコントローラ（以下、リモコン）が用いられることもある。また、入力装置８７８には、マイクロフォンなどの音声入力装置が含まれる。

[0168] （出力装置８７９）

出力装置８７９は、例えば、ＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）、ＬＣＤ、又は有機ＥＬ等のディスプレイ装置、スピーカ、ヘッドホン等のオーディオ出力装置、プリンタ、携帯電話、又はファクシミリ等、取得し

た情報を利用者に対して視覚的又は聴覚的に通知することが可能な装置である。また、本開示に係る出力装置８７９は、触覚刺激を出力することが可能な種々の振動デバイスを含む。

[0169] （ストレージ８８０）

ストレージ８８０は、各種のデータを格納するための装置である。ストレージ８８０としては、例えば、ハードディスクドライブ（ＨＤＤ）等の磁気記憶デバイス、半導体記憶デバイス、光記憶デバイス、又は光磁気記憶デバイス等が用いられる。

[0170] （ドライブ８８１）

ドライブ８８１は、例えば、磁気ディスク、光ディスク、光磁気ディスク、又は半導体メモリ等のリムーバブル記録媒体９０１に記録された情報を読み出し、又はリムーバブル記録媒体９０１に情報を書き込む装置である。

[0171] （リムーバブル記録媒体９０１）

リムーバブル記録媒体９０１は、例えば、ＤＶＤメディア、Ｂｌｕ－ｒａｙ（登録商標）メディア、ＨＤ　ＤＶＤメディア、各種の半導体記憶メディア等である。もちろん、リムーバブル記録媒体９０１は、例えば、非接触型ＩＣチップを搭載したＩＣカード、又は電子機器等であってもよい。

[0172] （接続ポート８８２）

接続ポート８８２は、例えば、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）ポート、ＩＥＥＥ１３９４ポート、ＳＣＳＩ（Ｓｍａｌｌ　Ｃｏｍｐｕｔｅｒ　Ｓｙｓｔｅｍ　Ｉｎｔｅｒｆａｃｅ）、ＲＳ－２３２Ｃポート、又は光オーディオ端子等のような外部接続機器９０２を接続するためのポートである。

[0173] （外部接続機器９０２）

外部接続機器９０２は、例えば、プリンタ、携帯音楽プレーヤ、デジタルカメラ、デジタルビデオカメラ、又はＩＣレコーダ等である。

[0174] （通信装置８８３）

通信装置８８３は、ネットワークに接続するための通信デバイスであり、

例えば、有線又は無線ＬＡＮ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、又はＷＵＳＢ（Ｗｉｒｅｌｅｓｓ　ＵＳＢ）用の通信カード、光通信用のルータ、ＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ　Ｄｉｇｉｔａｌ　Ｓｕｂｓｃｒｉｂｅｒ　Ｌｉｎｅ）用のルータ、又は各種通信用のモデム等である。

[0175] ＜３．まとめ＞

以上説明したように、本開示の一実施形態に係る情報処理方法を実現する情報処理システムは、共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成する第１の装置と、第１の装置が生成した複数の分散鍵のうちの１つを用いて所定の処理の実行に係る処理リクエストを送信する第２の装置と、第１の装置が生成した複数の分散鍵のうちの１つと、第２の装置から受信した処理リクエストに基づく判定を行う第３の装置と、を備える。ここで、第１の装置は、生成した複数の分散鍵のうち互いに異なる分散鍵を、共有先ユーザが利用する第２の装置、および第３の装置にそれぞれ配布してよい。また、第２の装置は、受信した分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を第３の装置に送信してよい。また、第３の装置は、第２の装置から受信したハッシュ値および第１の装置から受信した分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、上記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とを比較し、所定の処理を実行するか否かを判定してよい。

[0176] 上記の構成によれば、マルチユーザに対応した、よりセキュリティ性の高い情報検索を実現することが可能となる。

[0177] 以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本開示の技術的範囲に属するものと了解される。

[0178] また、本明細書に記載された効果は、あくまで説明的または例示的なもの

であって限定的ではない。つまり、本開示に係る技術は、上記の効果とともに、または上記の効果に代えて、本明細書の記載から当業者には明らかな他の効果を奏しうる。

[0179] また、コンピュータに内蔵されるＣＰＵ、ＲＯＭおよびＲＡＭなどのハードウェアに、情報処理端末１０や情報処理サーバ２０が有する構成と同等の機能を発揮させるためのプログラムも作成可能であり、当該プログラムを記録した、コンピュータに読み取り可能な記録媒体も提供され得る。

[0180] また、本明細書の情報処理システム１の処理に係る各ステップは、必ずしもシーケンス図に記載された順序に沿って時系列に処理される必要はない。例えば、情報処理システム１の処理に係る各ステップは、シーケンス図に記載された順序と異なる順序で処理されても、並列的に処理されてもよい。

[0181] なお、以下のような構成も本開示の技術的範囲に属する。

（１） 共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成する第１の装置と、 前記第１の装置が生成した複数の前記分散鍵のうちの１つを用いて所定の処理の実行に係る処理リクエストを送信する第２の装置と、

前記第１の装置が生成した複数の前記分散鍵のうちの１つと、前記第２の装置から受信した前記処理リクエストに基づく判定を行う第３の装置と、

を備え、

前記第１の装置は、生成した複数の前記分散鍵のうち互いに異なる前記分散鍵を、共有先ユーザが利用する前記第２の装置、および前記第３の装置にそれぞれ配布し、 前記第２の装置は、受信した前記分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を前記第３の装置に送信し、

前記第３の装置は、前記第２の装置から受信したハッシュ値および前記第１の装置から受信した前記分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とを比較し、前記所定の処理を実行するか否かを判定する、

情報処理システム。

（２）　前記第３の装置は、前記第２の装置から受信したハッシュ値および前記第１の装置から受信した前記分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とが一致する場合、前記所定の処理を実行する、

前記（１）に記載の情報処理システム。

（３）　前記所定の処理は、前記第３の装置が保存する暗号化データに対する検索結果の提示を含み、　前記第２の装置は、受信した前記分散鍵、および検索ワードに基づく準同型ハッシュ演算により算出したハッシュ値を前記第３の装置に送信し、

前記第３の装置は、前記第２の装置から受信したハッシュ値が、前記暗号化データに対応する暗号化インデックスに含まれる場合、前記検索ワードに対応する検索結果を前記第２の装置に送信し、

前記暗号化インデックスは、前記暗号化データから抽出されたキーワードリスト、および前記共有元ユーザの前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値である、

前記（１）に記載の情報処理システム。

（４）　前記検索結果は、前記検索ワードを含む前記暗号化データ、または前記検索ワードを含む前記暗号化データのリストのうち少なくともいずれか含む、

前記（３）に記載の情報処理システム。

（５）　前記第３の装置は、前記検索結果として、プロキシ暗号を用いて前記暗号化データを再暗号化した再暗号化データを前記第２の装置に送信する、

前記（３）に記載の情報処理システム。

（６）　前記第１の装置は、前記分散鍵を配布した前記第２の装置から前記共有先ユーザの公開鍵を受信し、前記公開鍵と前記共有元ユーザの秘密鍵を用いて生成した再暗号化鍵を前記第３の装置に送信し、

前記第３の装置は、受信した前記再暗号化鍵を用いて前記暗号化データを再暗号化した前記再暗号化データを前記第２の装置に送信し、

前記第２の装置は、受信した前記再暗号化データを前記共有先ユーザの秘密鍵を用いて復号する、

前記（５）に記載の情報処理システム。

（７） 前記第１の装置は、前記暗号化データと、前記暗号化データから抽出した前記キーワードリストおよび前記共有元ユーザの前記ユーザ鍵に基づく準同型ハッシュ演算により生成した前記暗号化インデックスとを、前記第３の装置に送信する、

前記（３）～（６）のいずれかに記載の情報処理システム。

（８） 前記第１の装置は、前記キーワードリストおよび前記共有元ユーザの前記ユーザ鍵に基づく準同型ハッシュ演算により算出したハッシュ値をＡＭＱ（Ａｐｐｒｏｘｉｍａｔｅ Ｍｅｍｂｅｒｓｈｉｐ Ｑｕｅｒｙ）形式にエンコードした前記暗号化インデックスを生成する、前記（７）に記載の情報処理システム。

（９） 前記ＡＭＱ形式は、少なくともブルームフィルタを含む、

前記（８）に記載の情報処理システム。

（１０）前記第３の装置は、前記第１の装置からの削除リクエストに基づいて、前記第１の装置から受信した前記分散鍵を削除する、

前記（１）～（９）のいずれかに記載の情報処理システム。

（１１） 前記第１の装置は、前記秘密分散処理により、前記共有先ユーザの数に１を加えた数の前記分散鍵を生成する、

前記（１）～（１０）のいずれかに記載の情報処理システム。

（１２） 前記第１の装置は、互いに異なる前記分散鍵を、複数の前記第２の装置および前記第３の装置にそれぞれ配布し、

前記第３の装置は、複数の前記第２の装置のすべてが、前記分散鍵を用いた準同型ハッシュ演算により、順に算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とを比較する、

前記（１１）に記載の情報処理システム。

（１３）　複数の前記第２の装置は、前記処理リクエストの起点となる起点端末と、前記処理リクエストが経由する経由端末とを含み、

前記起点端末は、受信した前記分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を前記経由端末に送信し、

前記経由端末は、受信した前記分散鍵、および前記起点端末または他の前記経由端末から受信したハッシュ値に基づく準同型ハッシュ演算により算出したハッシュ値を、当該準同型ハッシュ演算を行っていない他の前記経由端末または前記第３の装置に送信する、前記（１２）に記載の情報処理システム。

（１４）　前記経由端末は、準同型ハッシュ演算を行っていない他の前記経由端末が存在する場合、前記ハッシュ値を当該他の前記経由端末のうちの１つに送信し、準同型ハッシュ演算を行っていない他の前記経由端末が存在しない場合、算出したハッシュ値を前記第３の装置に送信する、

前記（１３）に記載の情報処理システム。

（１５）　前記所定の処理は、決済処理を含み、

前記第３の装置は、前記第２の装置から受信したハッシュ値と、前記ユーザ鍵と前記入力データに基づく準同型ハッシュ演算により算出されたハッシュ値とが一致する場合、前記決済処理を実行する、

前記（１）～（１４）のいずれかに記載の情報処理システム。

（１６）　前記所定の処理は、文書の公開処理を含み、

前記第３の装置は、前記第２の装置から受信したハッシュ値と、前記ユーザ鍵と前記入力データに基づく準同型ハッシュ演算により算出されたハッシュ値とが一致する場合、前記文書の公開処理を実行する、

前記（１）～（１５）のいずれかに記載の情報処理システム。

（１７）　前記第３の装置は、前記入力データの入力、および前記処理リクエストの結果に係る表示を行うためのインタフェースを制御する、

前記（１）～（１６）のいずれかに記載の情報処理システム。

（１８）　第１の装置が、共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成することと、

第２の装置が、前記第１の装置が生成した複数の前記分散鍵のうちの１つを用いて所定の処理の実行に係る処理リクエストを送信することと、

第３の装置が、前記第１の装置が生成した複数の前記分散鍵のうちの１つと、前記第２の装置から受信した前記処理リクエストに基づく判定を行うことと、

を含み、

前記第１の装置が、生成した複数の前記分散鍵のうち互いに異なる前記分散鍵を、共有先ユーザが利用する前記第２の装置、および前記第３の装置にそれぞれ配布することと、　前記第２の装置が、受信した前記分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を前記第３の装置に送信することと、

前記第３の装置が、前記第２の装置から受信したハッシュ値および前記第１の装置から受信した前記分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とを比較し、前記所定の処理を実行するか否かを判定することと、

をさらに含む、

情報処理方法。

（１９）　共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成する秘密分散処理部と、

複数の前記分散鍵のうち互いに異なる前記分散鍵を、共有先ユーザが利用する端末、および暗号化データが保存されるサーバにそれぞれ送信する通信部と、

を備える、

情報処理装置。

（２０）　前記ユーザ鍵を用いて前記暗号化データを生成する暗号化部、

をさらに備え、

前記通信部は、前記暗号化データを前記サーバに送信し、

前記共有先ユーザは、前記共有元ユーザにより前記暗号化データの検索が許諾されたユーザである、

前記（１９）に記載の情報処理装置。

符号の説明

[0182]

１０	情報処理端末
１１０	ユーザ鍵管理部
１２０	入力部
１３０	暗号化部
１４０	秘密分散処理部
１５０	復号部
１６０	表示部
１７０	通信部
２０	情報処理サーバ
２１０	分散鍵管理部
２２０	データ管理部
２３０	処理部
２４０	端末通信部

請求の範囲

[請求項1] 共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成する第１の装置と、　前記第１の装置が生成した複数の前記分散鍵のうちの１つを用いて所定の処理の実行に係る処理リクエストを送信する第２の装置と、

前記第１の装置が生成した複数の前記分散鍵のうちの１つと、前記第２の装置から受信した前記処理リクエストに基づく判定を行う第３の装置と、

を備え、

前記第１の装置は、生成した複数の前記分散鍵のうち互いに異なる前記分散鍵を、共有先ユーザが利用する前記第２の装置、および前記第３の装置にそれぞれ配布し、　前記第２の装置は、受信した前記分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を前記第３の装置に送信し、

前記第３の装置は、前記第２の装置から受信したハッシュ値および前記第１の装置から受信した前記分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とを比較し、前記所定の処理を実行するか否かを判定する、

情報処理システム。

[請求項2] 前記第３の装置は、前記第２の装置から受信したハッシュ値および前記第１の装置から受信した前記分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とが一致する場合、前記所定の処理を実行する、

請求項１に記載の情報処理システム。

[請求項3] 前記所定の処理は、前記第３の装置が保存する暗号化データに対する検索結果の提示を含み、　前記第２の装置は、受信した前記分散鍵

、および検索ワードに基づく準同型ハッシュ演算により算出したハッシュ値を前記第３の装置に送信し、

前記第３の装置は、前記第２の装置から受信したハッシュ値が、前記暗号化データに対応する暗号化インデックスに含まれる場合、前記検索ワードに対応する検索結果を前記第２の装置に送信し、

前記暗号化インデックスは、前記暗号化データから抽出されたキーワードリスト、および前記共有元ユーザの前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値である、

請求項１に記載の情報処理システム。

[請求項4] 前記検索結果は、前記検索ワードを含む前記暗号化データ、または前記検索ワードを含む前記暗号化データのリストのうち少なくともいずれか含む、

請求項３に記載の情報処理システム。

[請求項5] 前記第３の装置は、前記検索結果として、プロキシ暗号を用いて前記暗号化データを再暗号化した再暗号化データを前記第２の装置に送信する、

請求項３に記載の情報処理システム。

[請求項6] 前記第１の装置は、前記分散鍵を配布した前記第２の装置から前記共有先ユーザの公開鍵を受信し、前記公開鍵と前記共有元ユーザの秘密鍵を用いて生成した再暗号化鍵を前記第３の装置に送信し、

前記第３の装置は、受信した前記再暗号化鍵を用いて前記暗号化データを再暗号化した前記再暗号化データを前記第２の装置に送信し、

前記第２の装置は、受信した前記再暗号化データを前記共有先ユーザの秘密鍵を用いて復号する、

請求項５に記載の情報処理システム。

[請求項7] 前記第１の装置は、前記暗号化データと、前記暗号化データから抽出した前記キーワードリストおよび前記共有元ユーザの前記ユーザ鍵に基づく準同型ハッシュ演算により生成した前記暗号化インデックス

とを、前記第３の装置に送信する、

請求項３に記載の情報処理システム。

[請求項8] 前記第１の装置は、前記キーワードリストおよび前記共有元ユーザの前記ユーザ鍵に基づく準同型ハッシュ演算により算出したハッシュ値をＡＭＱ（Ａｐｐｒｏｘｉｍａｔｅ Ｍｅｍｂｅｒｓｈｉｐ Ｑｕｅｒｙ）形式にエンコードした前記暗号化インデックスを生成する、

請求項７に記載の情報処理システム。

[請求項9] 前記ＡＭＱ形式は、少なくともブルームフィルタを含む、

請求項８に記載の情報処理システム。

[請求項10] 前記第３の装置は、前記第１の装置からの削除リクエストに基づいて、前記第１の装置から受信した前記分散鍵を削除する、

請求項１に記載の情報処理システム。

[請求項11] 前記第１の装置は、前記秘密分散処理により、前記共有先ユーザの数に１を加えた数の前記分散鍵を生成する、

請求項１に記載の情報処理システム。

[請求項12] 前記第１の装置は、互いに異なる前記分散鍵を、複数の前記第２の装置および前記第３の装置にそれぞれ配布し、

前記第３の装置は、複数の前記第２の装置のすべてが、前記分散鍵を用いた準同型ハッシュ演算により、順に算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とを比較する、

請求項１１に記載の情報処理システム。

[請求項13] 複数の前記第２の装置は、前記処理リクエストの起点となる起点端末と、前記処理リクエストが経由する経由端末とを含み、

前記起点端末は、受信した前記分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を前記経由端末に送信し、

前記経由端末は、受信した前記分散鍵、および前記起点端末または

他の前記経由端末から受信したハッシュ値に基づく準同型ハッシュ演算により算出したハッシュ値を、当該準同型ハッシュ演算を行っていない他の前記経由端末または前記第３の装置に送信する、請求項１２に記載の情報処理システム。

[請求項14] 前記経由端末は、準同型ハッシュ演算を行っていない他の前記経由端末が存在する場合、前記ハッシュ値を当該他の前記経由端末のうちの１つに送信し、準同型ハッシュ演算を行っていない他の前記経由端末が存在しない場合、算出したハッシュ値を前記第３の装置に送信する、

請求項１３に記載の情報処理システム。

[請求項15] 前記所定の処理は、決済処理を含み、

前記第３の装置は、前記第２の装置から受信したハッシュ値と、前記ユーザ鍵と前記入力データに基づく準同型ハッシュ演算により算出されたハッシュ値とが一致する場合、前記決済処理を実行する、

請求項１に記載の情報処理システム。

[請求項16] 前記所定の処理は、文書の公開処理を含み、

前記第３の装置は、前記第２の装置から受信したハッシュ値と、前記ユーザ鍵と前記入力データに基づく準同型ハッシュ演算により算出されたハッシュ値とが一致する場合、前記文書の公開処理を実行する、

請求項１に記載の情報処理システム。

[請求項17] 前記第３の装置は、前記入力データの入力、および前記処理リクエストの結果に係る表示を行うためのインタフェースを制御する、

請求項１に記載の情報処理システム。

[請求項18] 第１の装置が、共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成することと、

第２の装置が、前記第１の装置が生成した複数の前記分散鍵のうちの１つを用いて所定の処理の実行に係る処理リクエストを送信するこ

とと、

第３の装置が、前記第１の装置が生成した複数の前記分散鍵のうちの１つと、前記第２の装置から受信した前記処理リクエストに基づく判定を行うことと、

を含み、

前記第１の装置が、生成した複数の前記分散鍵のうち互いに異なる前記分散鍵を、共有先ユーザが利用する前記第２の装置、および前記第３の装置にそれぞれ配布することと、　前記第２の装置が、受信した前記分散鍵、および入力データに基づく準同型ハッシュ演算により算出したハッシュ値を前記第３の装置に送信することと、

前記第３の装置が、前記第２の装置から受信したハッシュ値および前記第１の装置から受信した前記分散鍵に基づく準同型ハッシュ演算により算出したハッシュ値と、前記ユーザ鍵に基づく準同型ハッシュ演算により算出されたハッシュ値とを比較し、前記所定の処理を実行するか否かを判定することと、

をさらに含む、

情報処理方法。

[請求項19] 共有元ユーザのユーザ鍵を秘密分散処理により分割し、複数の分散鍵を生成する秘密分散処理部と、

複数の前記分散鍵のうち互いに異なる前記分散鍵を、共有先ユーザが利用する端末、および暗号化データが保存されるサーバにそれぞれ送信する通信部と、

を備える、

情報処理装置。

[請求項20] 前記ユーザ鍵を用いて前記暗号化データを生成する暗号化部、

をさらに備え、

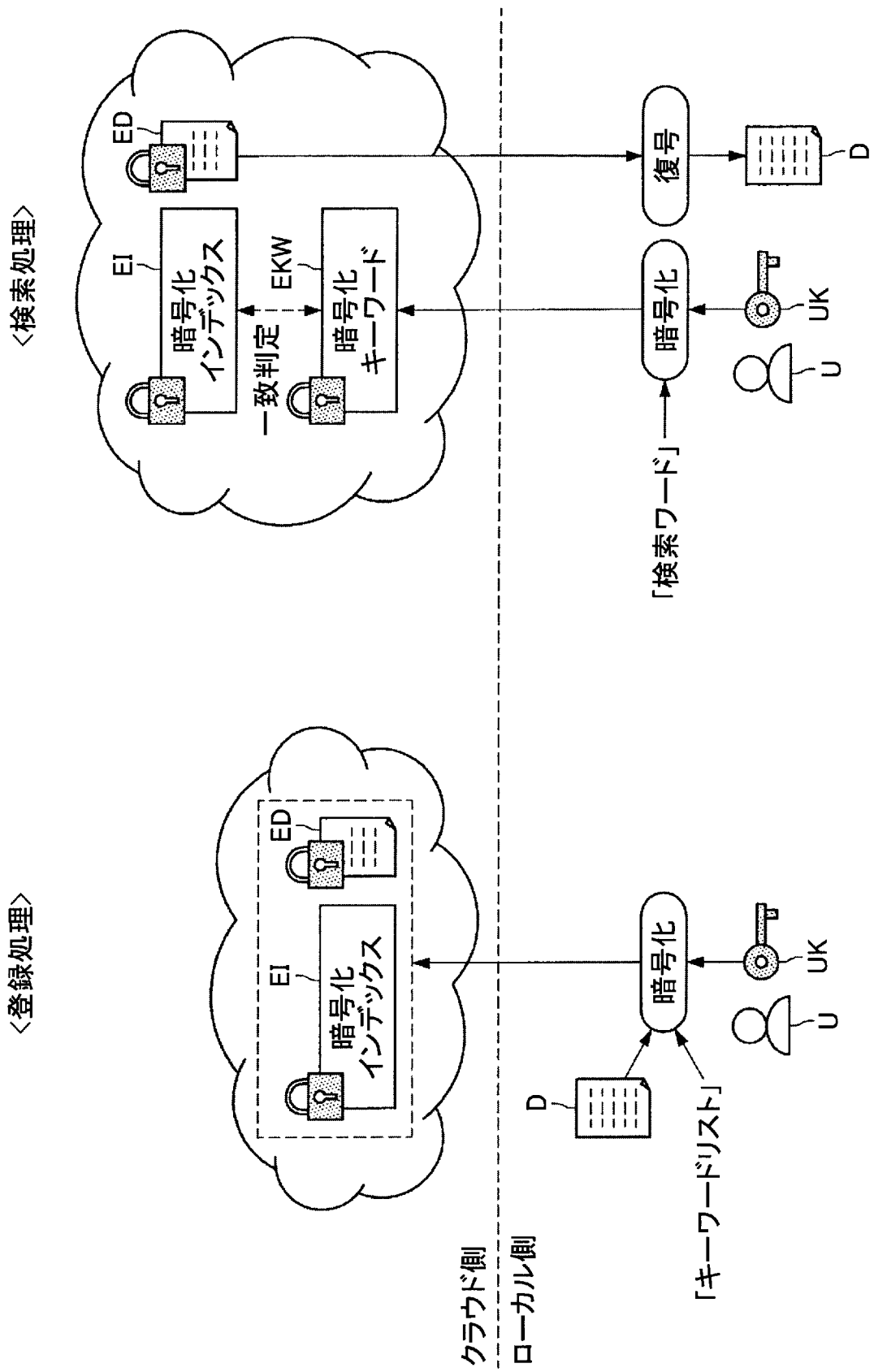
前記通信部は、前記暗号化データを前記サーバに送信し、

前記共有先ユーザは、前記共有元ユーザにより前記暗号化データの

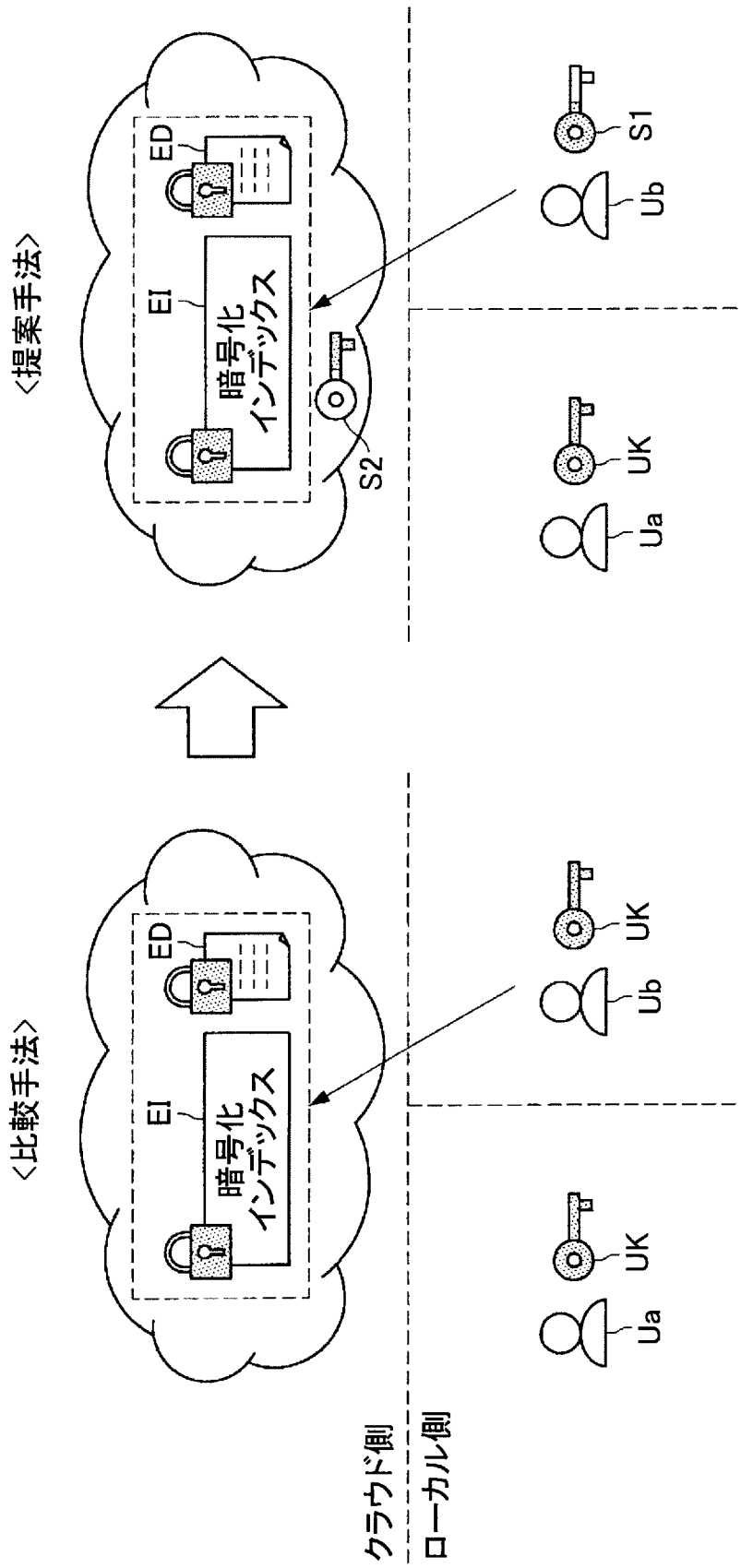
検索が許諾されたユーザである、

請求項１９に記載の情報処理装置。

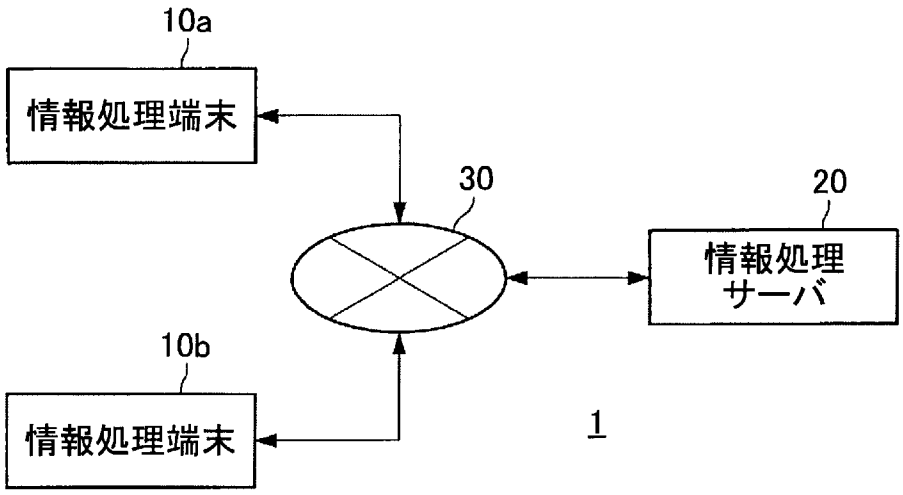
[図1]


〈検索処理〉
〈登録処理〉
ED
EI
暗号化
インデックス
EKW
暗号化
キーワード
一致判定
復号
D
暗号化
UK
U
「検索ワード」
「キーワードリスト」
クラウド側
ローカル側

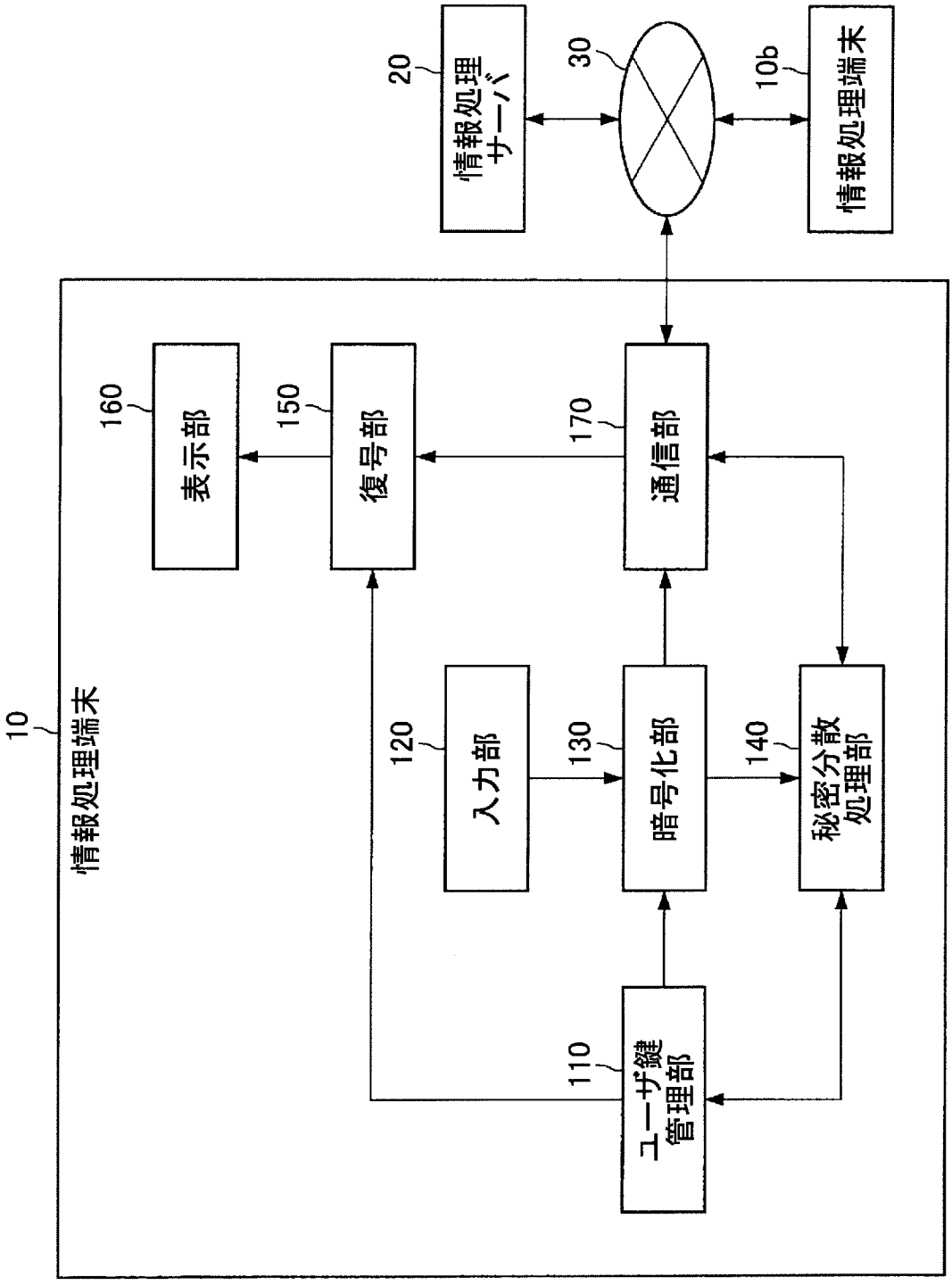
[図2]


〈提案手法〉
ED
EI
暗号化
インデックス
S2
S1
Ub
UK
Ua
〈比較手法〉
ED
EI
暗号化
インデックス
UK
Ub
UK
Ua
クラウド側
ローカル側

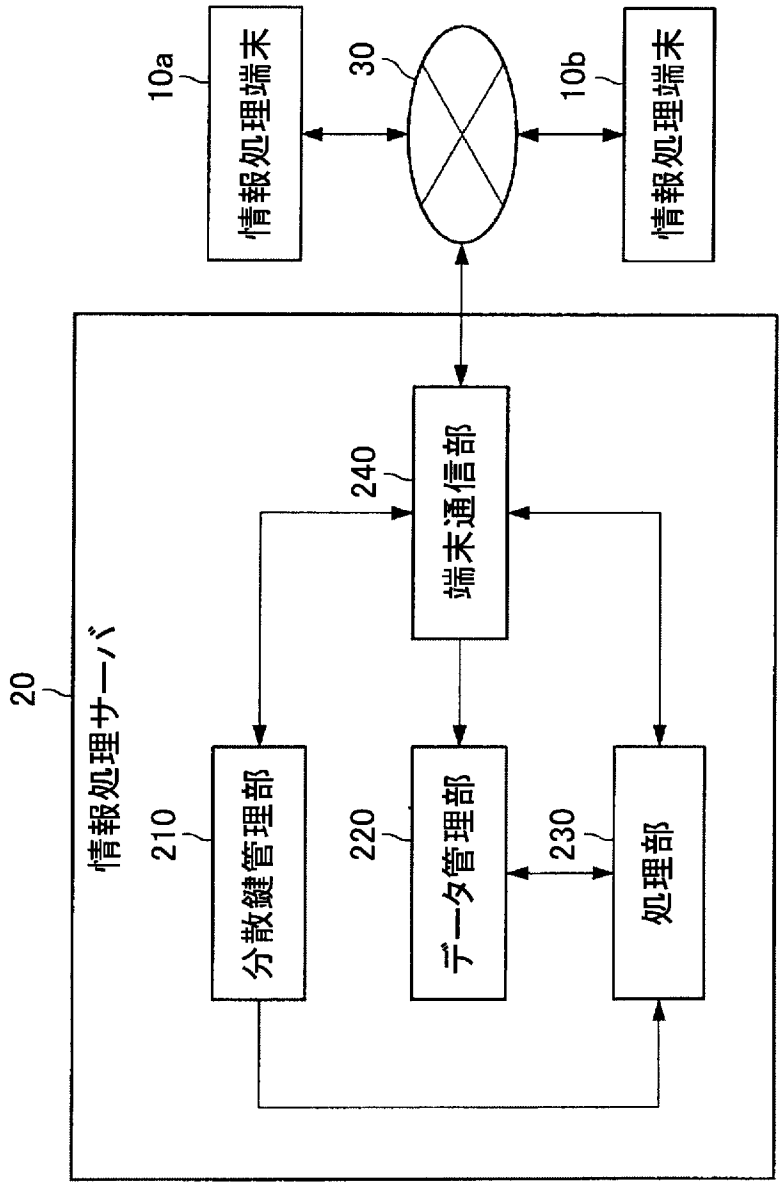
[図3]



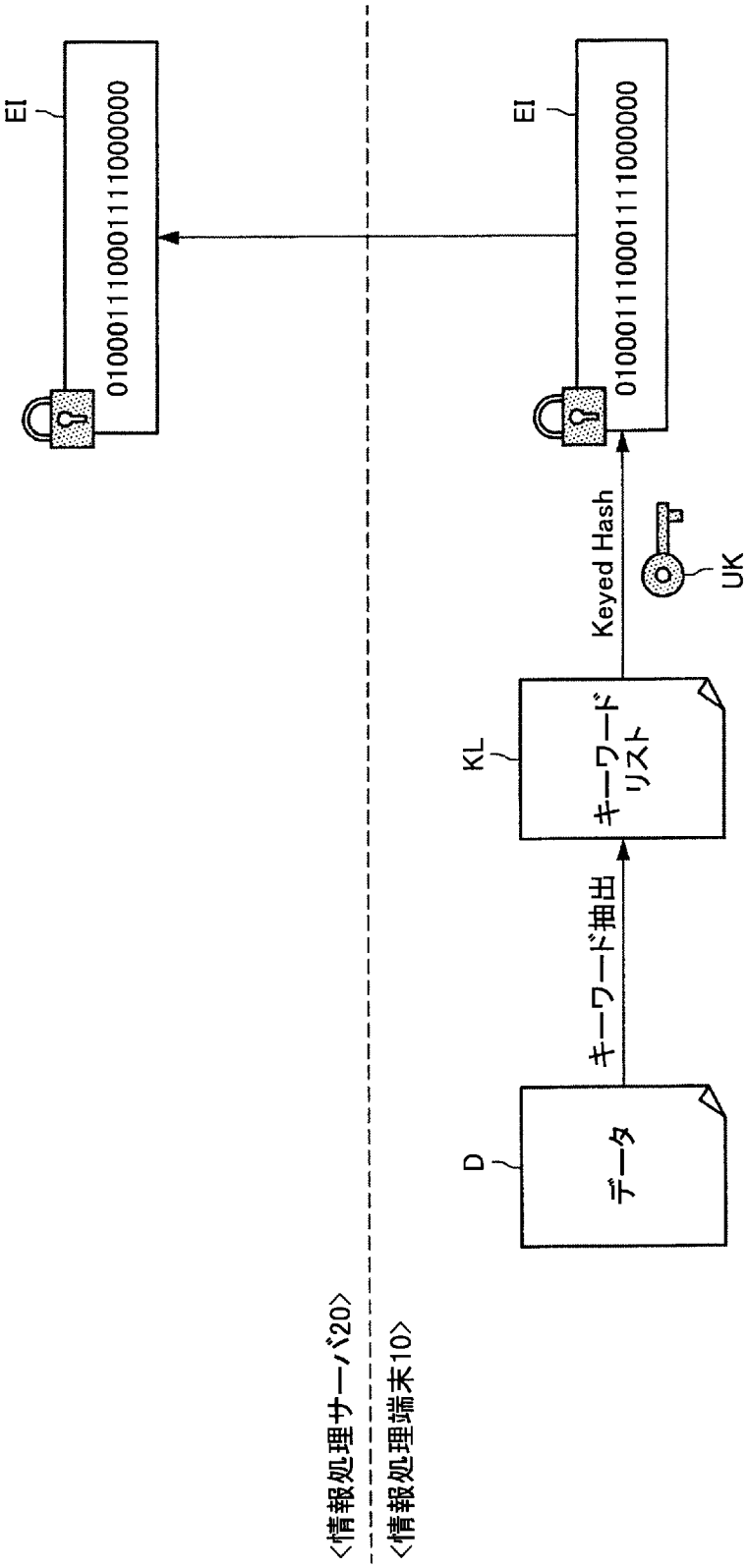
[図4]


20
情報処理サーバ
30
10b
情報処理端末
10
情報処理端末
160
表示部
150
復号部
170
通信部
120
入力部
130
暗号化部
140
秘密分散処理部
110
ユーザ鍵管理部

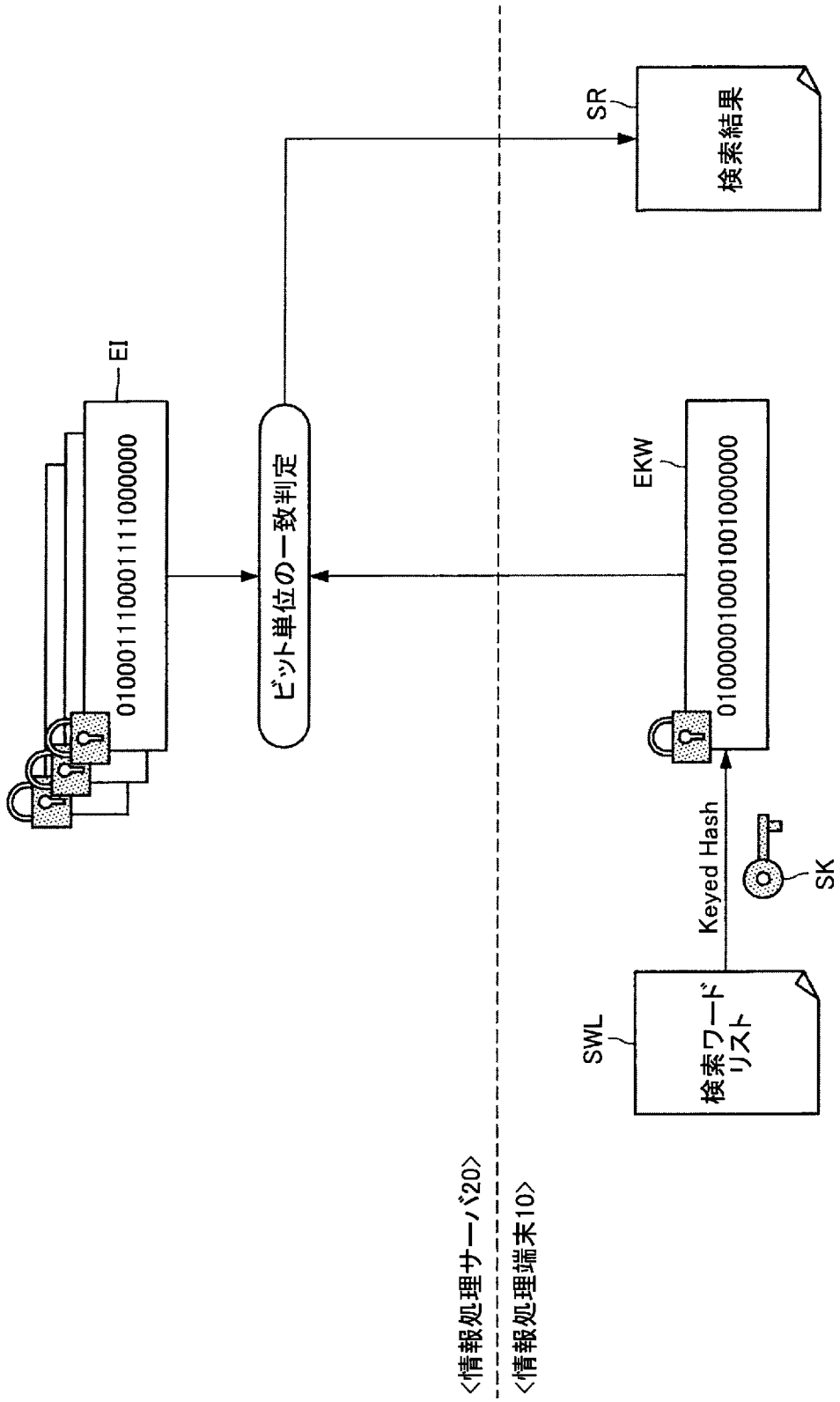
[図5]


10a
情報処理端末
30
10b
情報処理端末
20
情報処理サーバ
240
端末通信部
210
分散鍵管理部
220
データ管理部
230
処理部

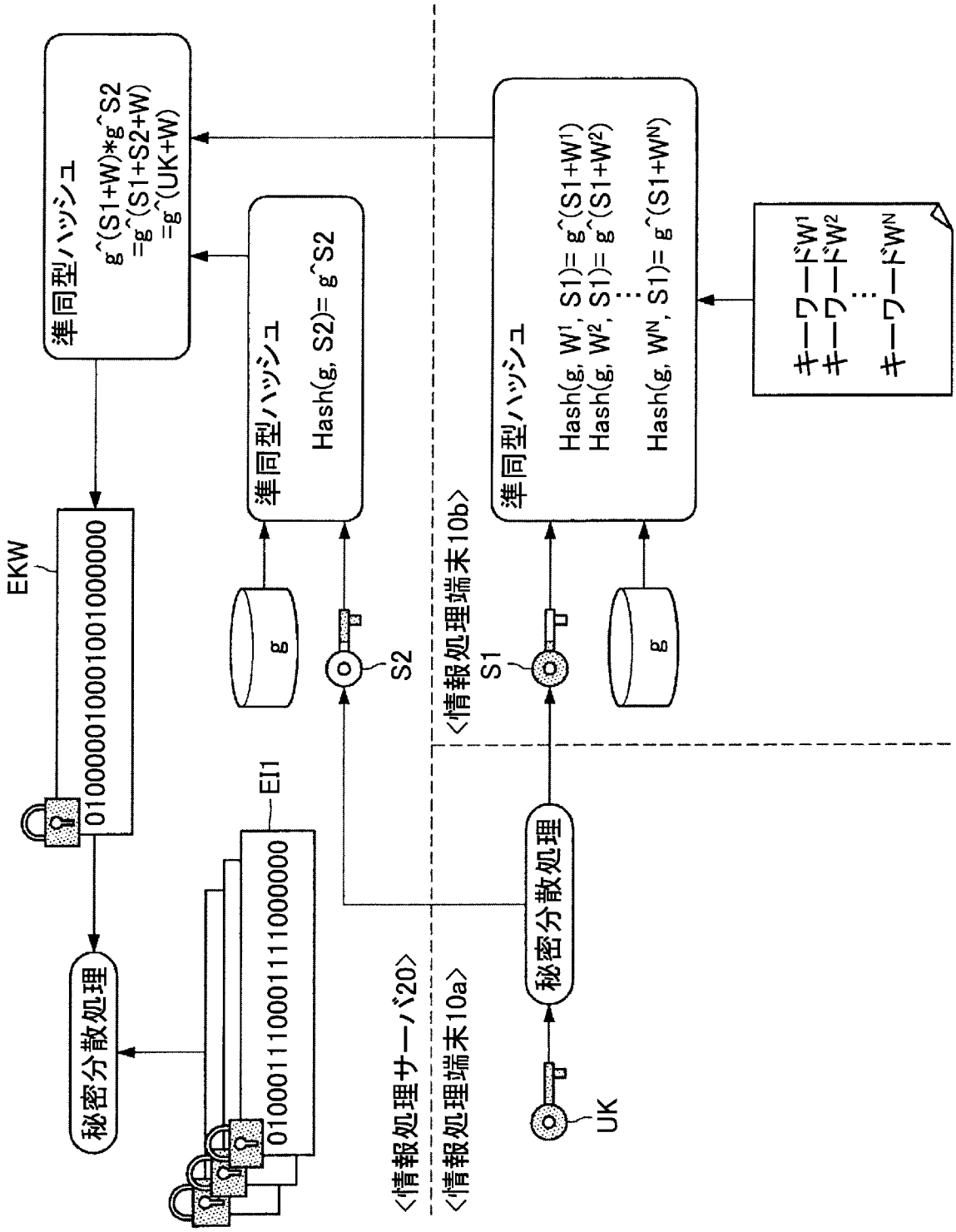
[図6]


EI
0100011100011111000000
EI
0100011100011111000000
Keyed Hash
UK
KL
キーワード
リスト
キーワード抽出
D
データ
<情報処理サーバ20>
<情報処理端末10>

[図7]


SR
検索結果
EI
0100011100011111000000
ビット単位の一致判定
EKW
0100000100010010000000
Keyed Hash
SK
SWL
検索ワードリスト
<情報処理サーバ20>
<情報処理端末10>

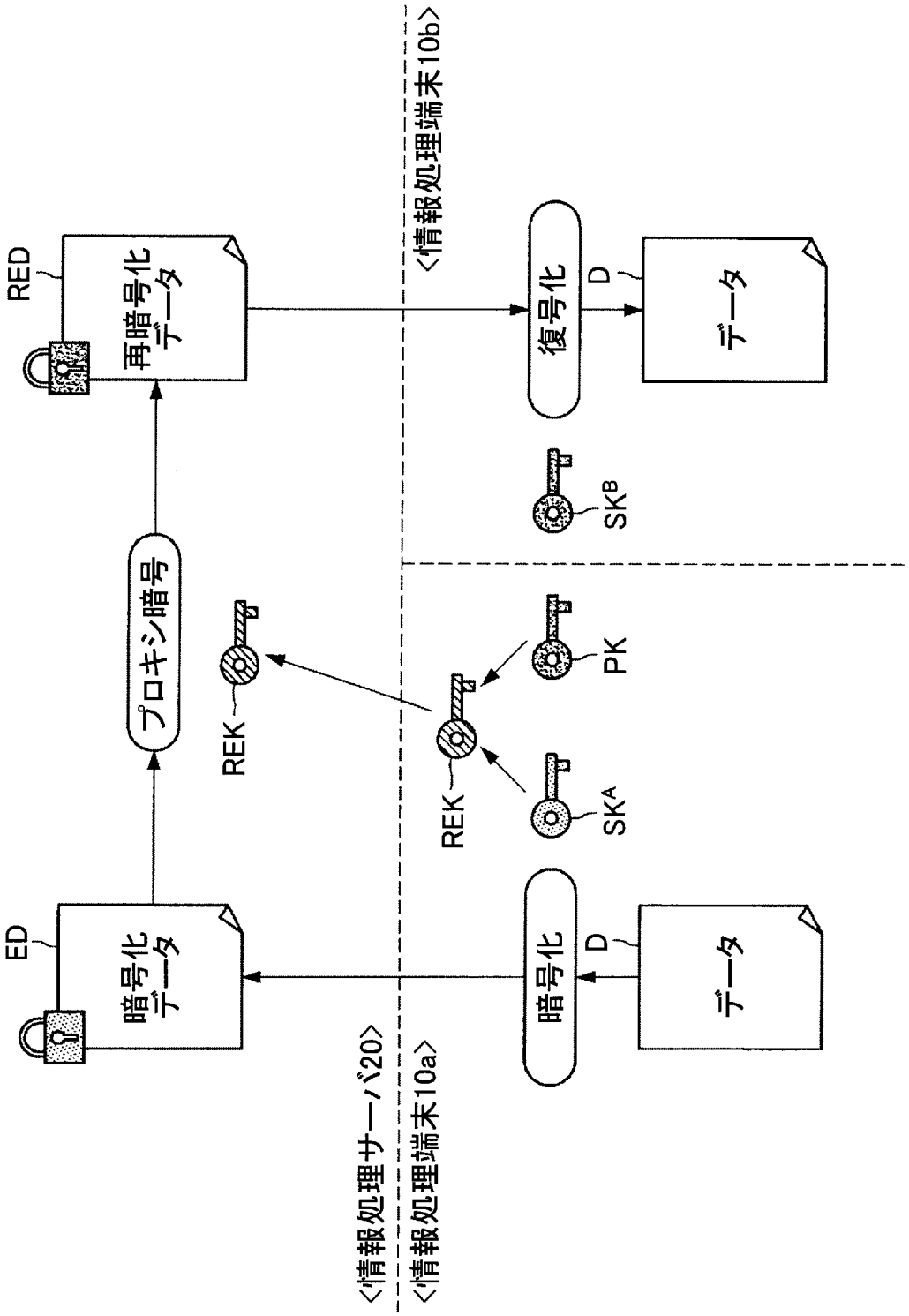
[図8]


準同型ハッシュ
g^(S1+W)*g^S2
=g^(S1+S2+W)
=g^(UK+W)
準同型ハッシュ
Hash(g, S2)= g^S2
準同型ハッシュ
Hash(g, W1, S1)= g^(S1+W1)
Hash(g, W2, S1)= g^(S1+W2)
Hash(g, WN, S1)= g^(S1+WN)
キーワードW1
キーワードW2
キーワードWN
EKW
0100000100010010000000
EI1
0100011100011110000000
秘密分散処理
秘密分散処理
g
g
S2
S1
UK
<情報処理サーバ20>
<情報処理端末10a>
<情報処理端末10b>

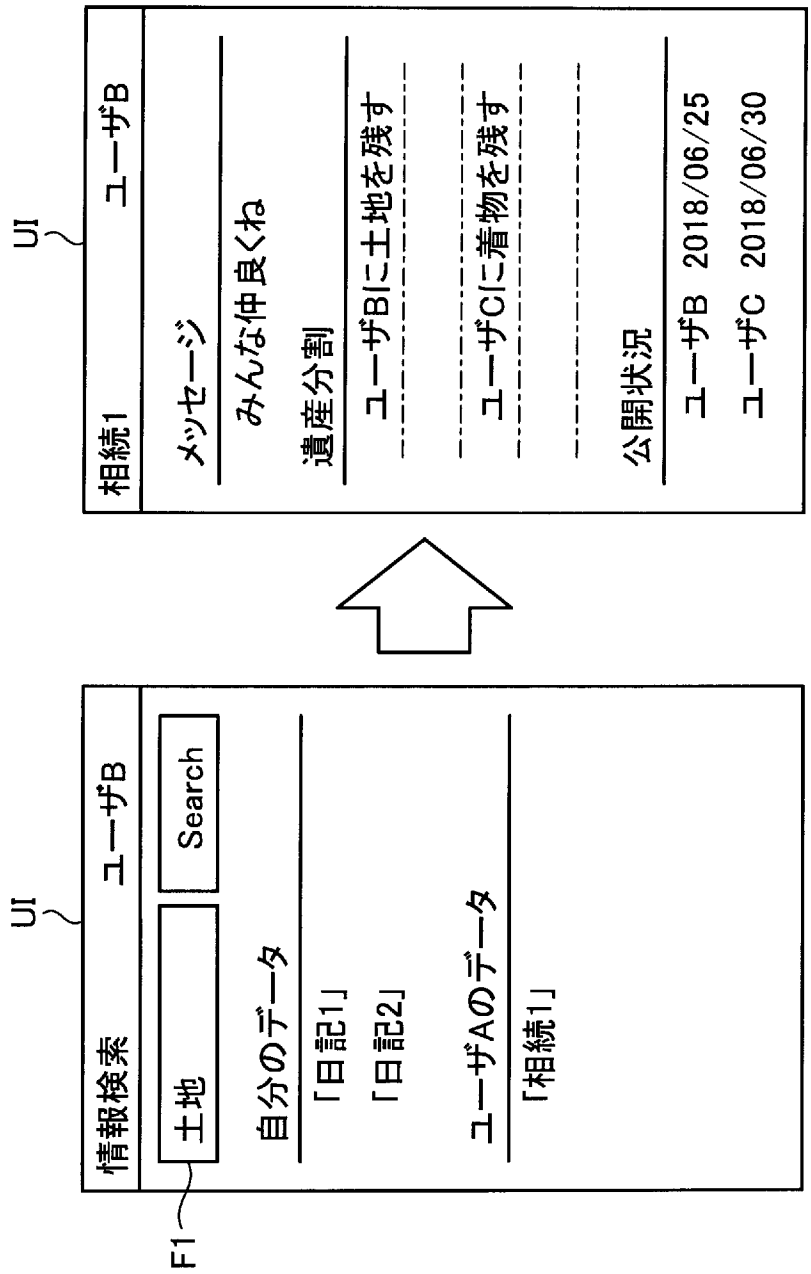
[図9]

分散鍵ID	共有先ユーザID	共有元ユーザID	分散鍵
1	ユーザID^{A}	ユーザID^{A}	分散鍵^{AA}
2	ユーザID^{A}	ユーザID^{B}	分散鍵^{AB}
3	ユーザID^{A}	ユーザID^{C}	分散鍵^{AC}
4	ユーザID^{B}	ユーザID^{B}	分散鍵^{BB}
5	ユーザID^{B}	ユーザID^{A}	分散鍵^{BA}
6	ユーザID^{B}	ユーザID^{D}	分散鍵^{BD}

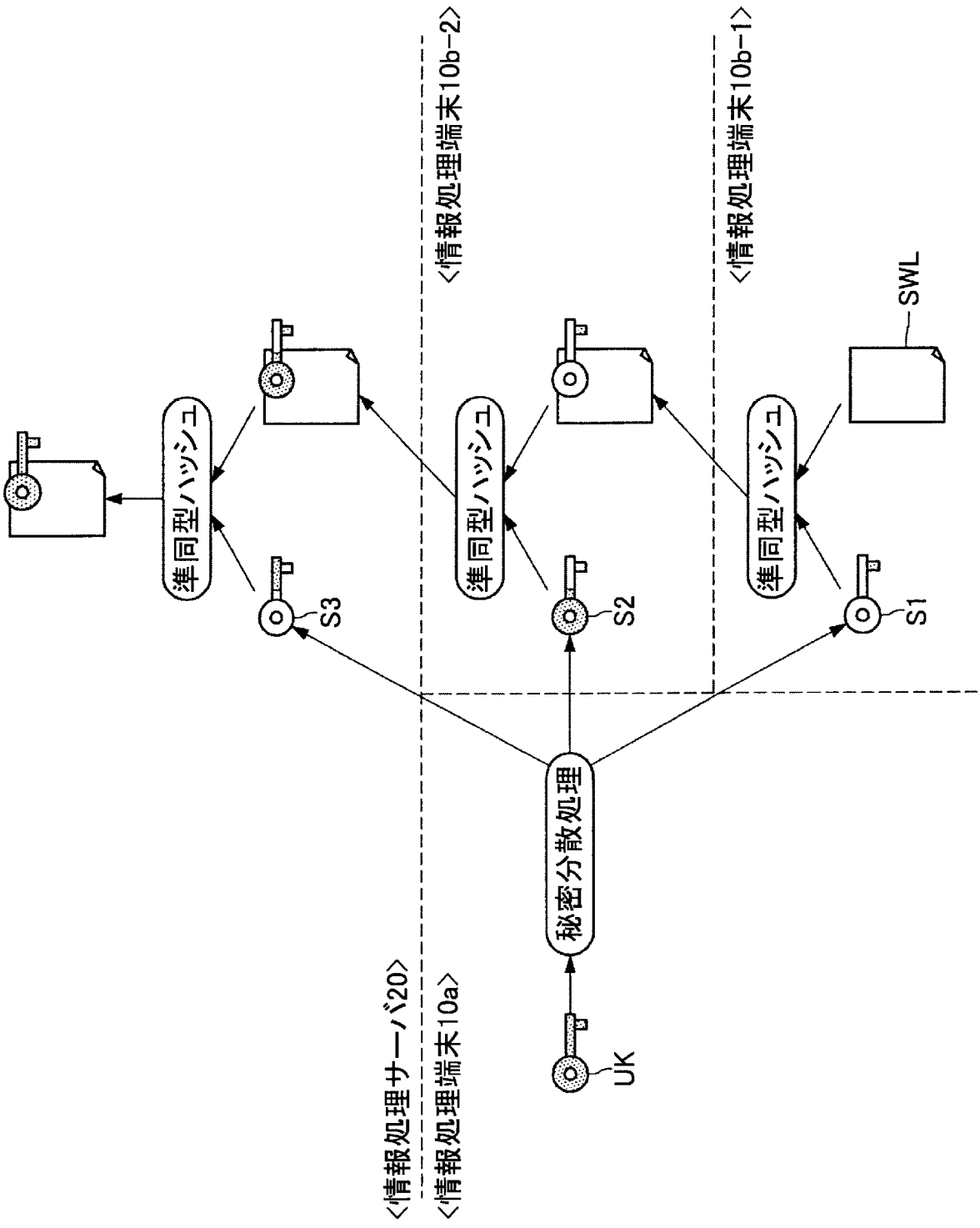
[図10]


RED
再暗号化データ
ED
暗号化データ
プロキシ暗号
REK
REK
SK^A
PK
SK^B
復号化
暗号化
D
D
データ
データ
<情報処理端末10b>
<情報処理サーバ20>
<情報処理端末10a>

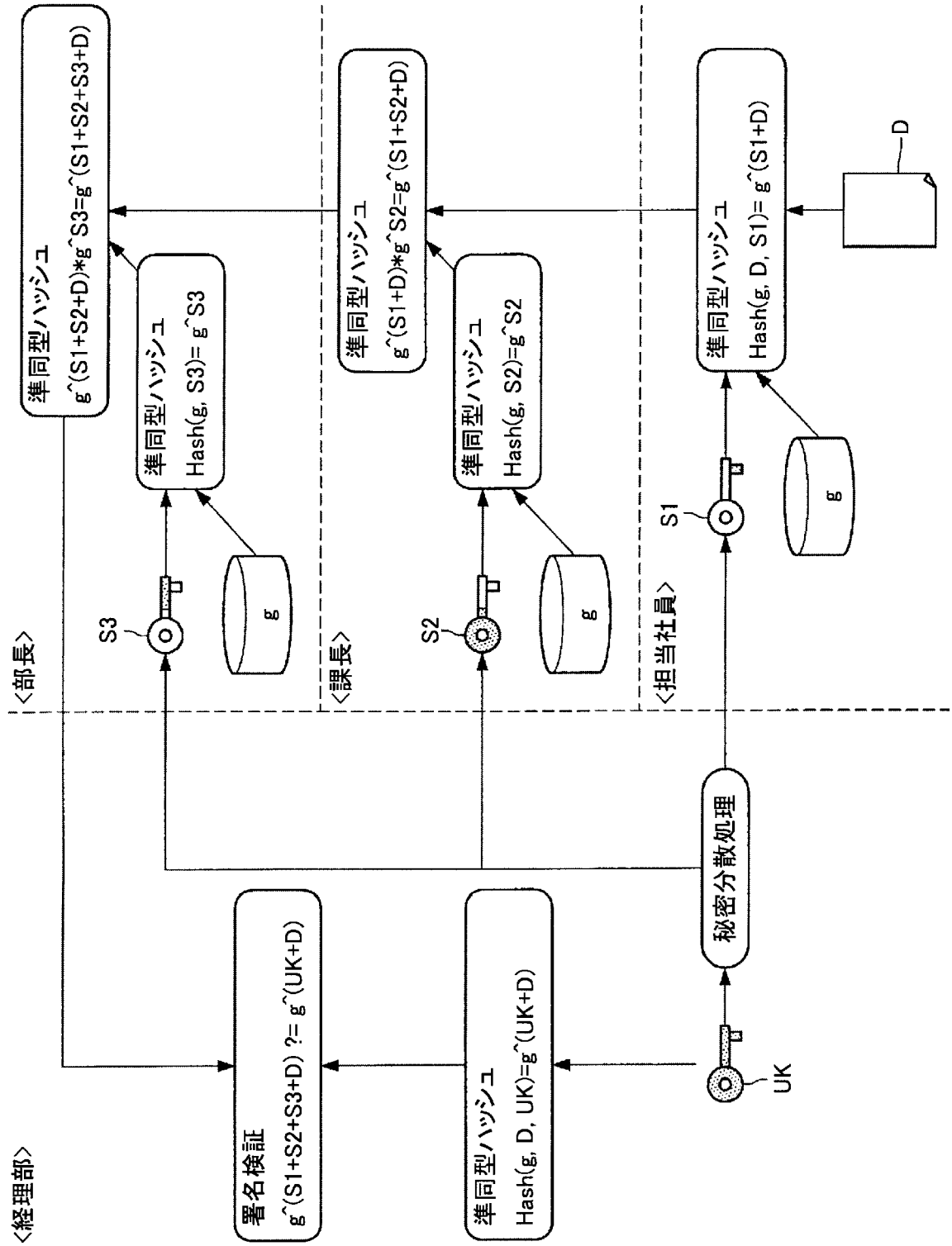
[図11]


UI
情報検索
ユーザB
土地
Search
自分のデータ
「日記1」
「日記2」
ユーザAのデータ
「相続1」
F1
UI
相続1
ユーザB
メッセージ
みんな仲良くね
遺産分割
ユーザBに土地を残す
ユーザCに着物を残す
公開状況
ユーザB 2018/06/25
ユーザC 2018/06/30

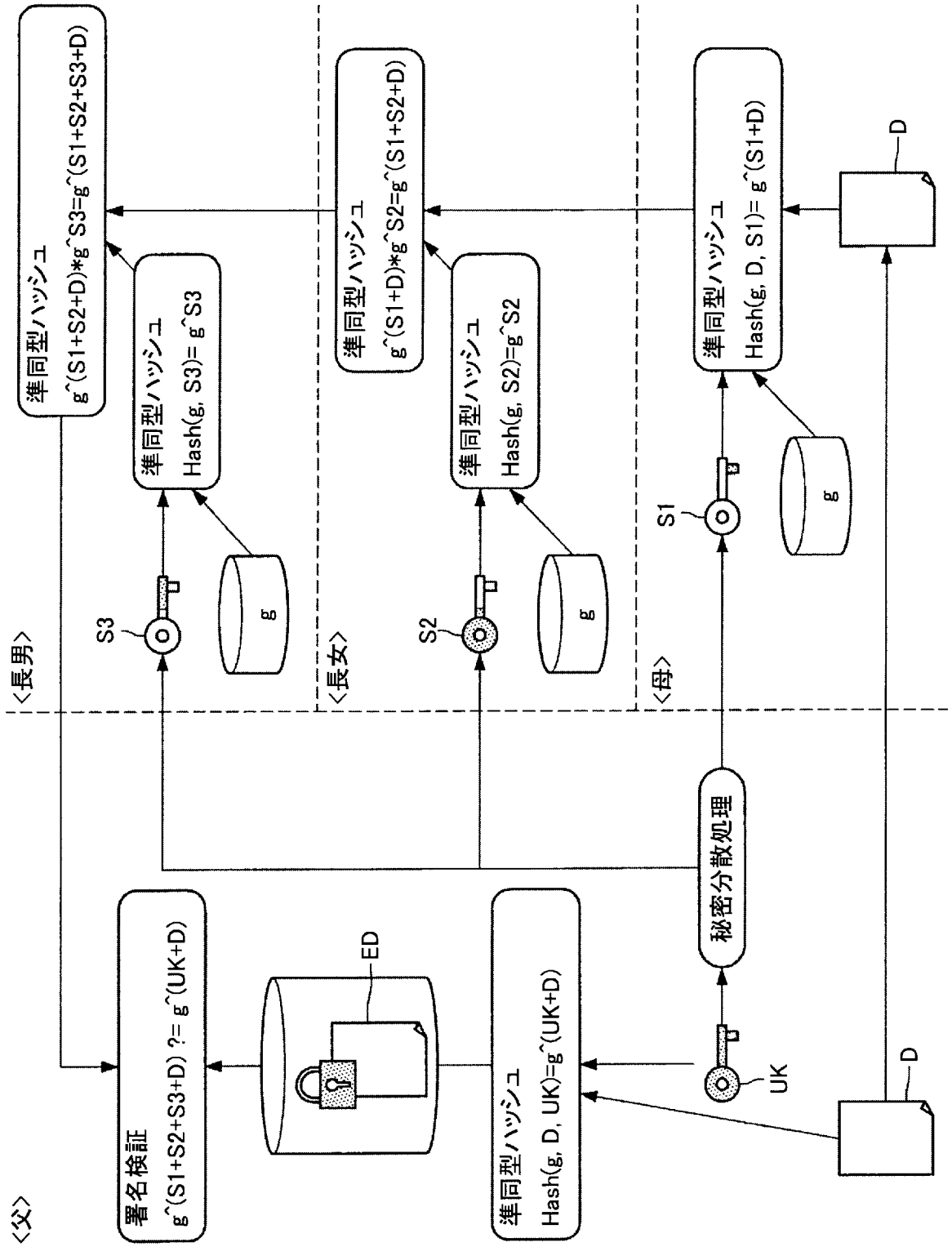
[図12]


〈情報処理サーバ20〉
〈情報処理端末10a〉
〈情報処理端末10b-2〉
〈情報処理端末10b-1〉
秘密分散処理
準同型ハッシュ
準同型ハッシュ
準同型ハッシュ
UK
S3
S2
S1
SWL

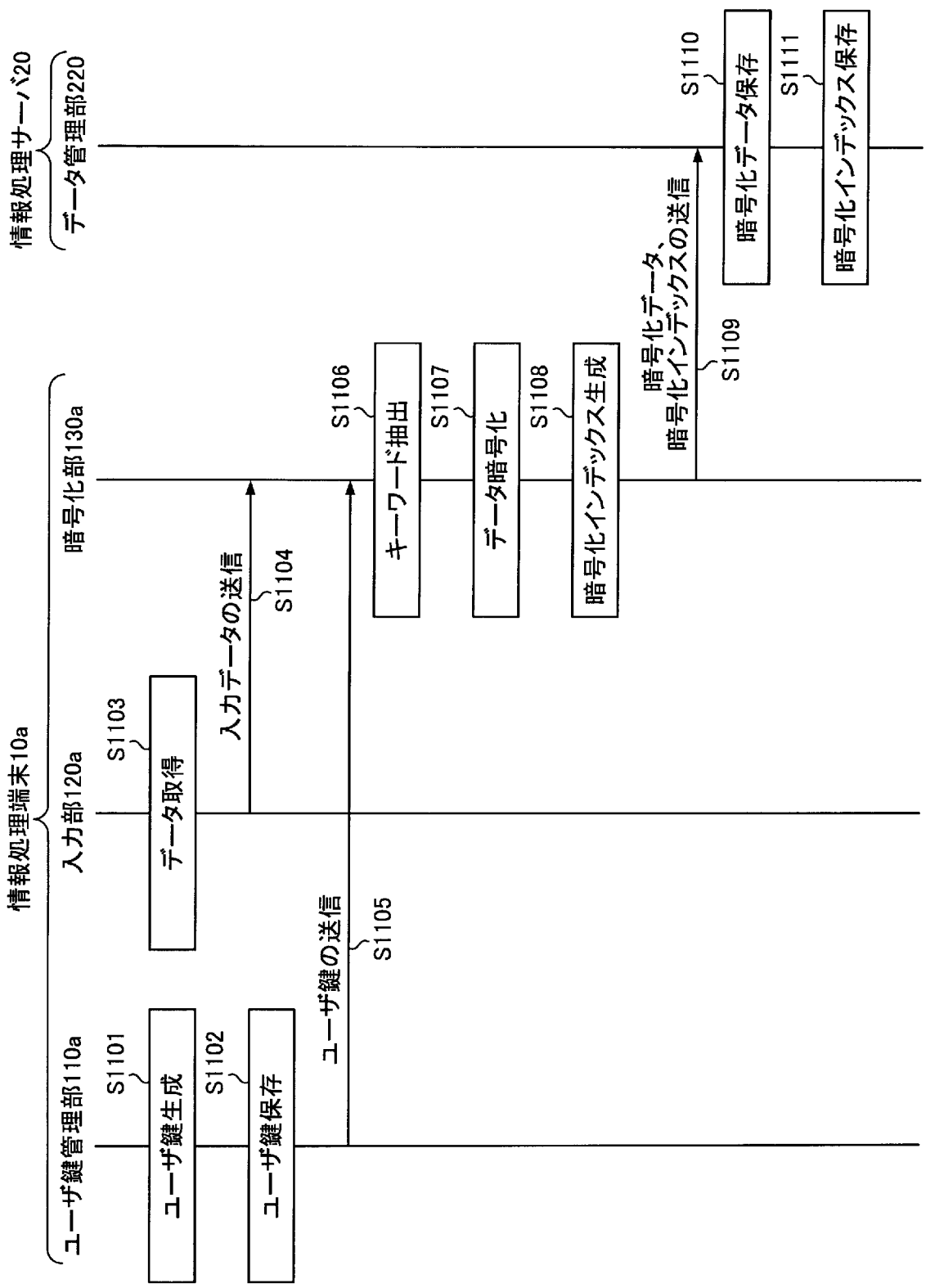
[図13]


〈部長〉
〈課長〉
〈担当社員〉
〈経理部〉
準同型ハッシュ
g^(S1+S2+D)*g^S3=g^(S1+S2+S3+D)
準同型ハッシュ
Hash(g, S3)= g^S3
準同型ハッシュ
g^(S1+D)*g^S2=g^(S1+S2+D)
準同型ハッシュ
Hash(g, S2)=g^S2
準同型ハッシュ
Hash(g, D, S1)= g^(S1+D)
S3
S2
S1
UK
g
D
秘密分散処理
署名検証
g^(S1+S2+S3+D) ?= g^(UK+D)
準同型ハッシュ
Hash(g, D, UK)=g^(UK+D)

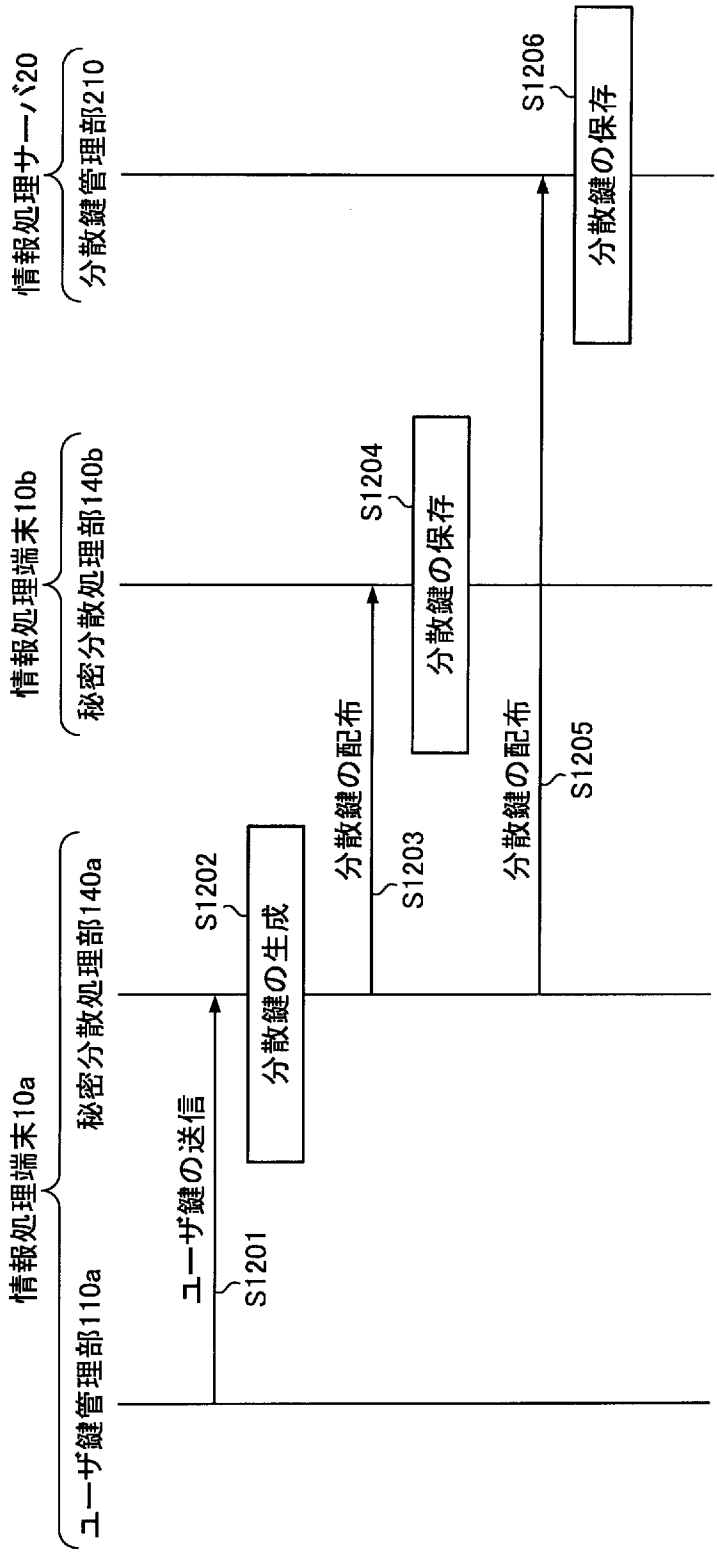
[図14]


〈父〉
〈長男〉
〈長女〉
〈母〉
署名検証
g^(S1+S2+S3+D) ?= g^(UK+D)
ED
準同型ハッシュ
Hash(g, D, UK)=g^(UK+D)
秘密分散処理
UK
D
準同型ハッシュ
g^(S1+S2+D)*g^S3=g^(S1+S2+S3+D)
準同型ハッシュ
Hash(g, S3)= g^S3
S3
g
準同型ハッシュ
g^(S1+D)*g^S2=g^(S1+S2+D)
準同型ハッシュ
Hash(g, S2)=g^S2
S2
g
準同型ハッシュ
Hash(g, D, S1)= g^(S1+D)
S1
g
D

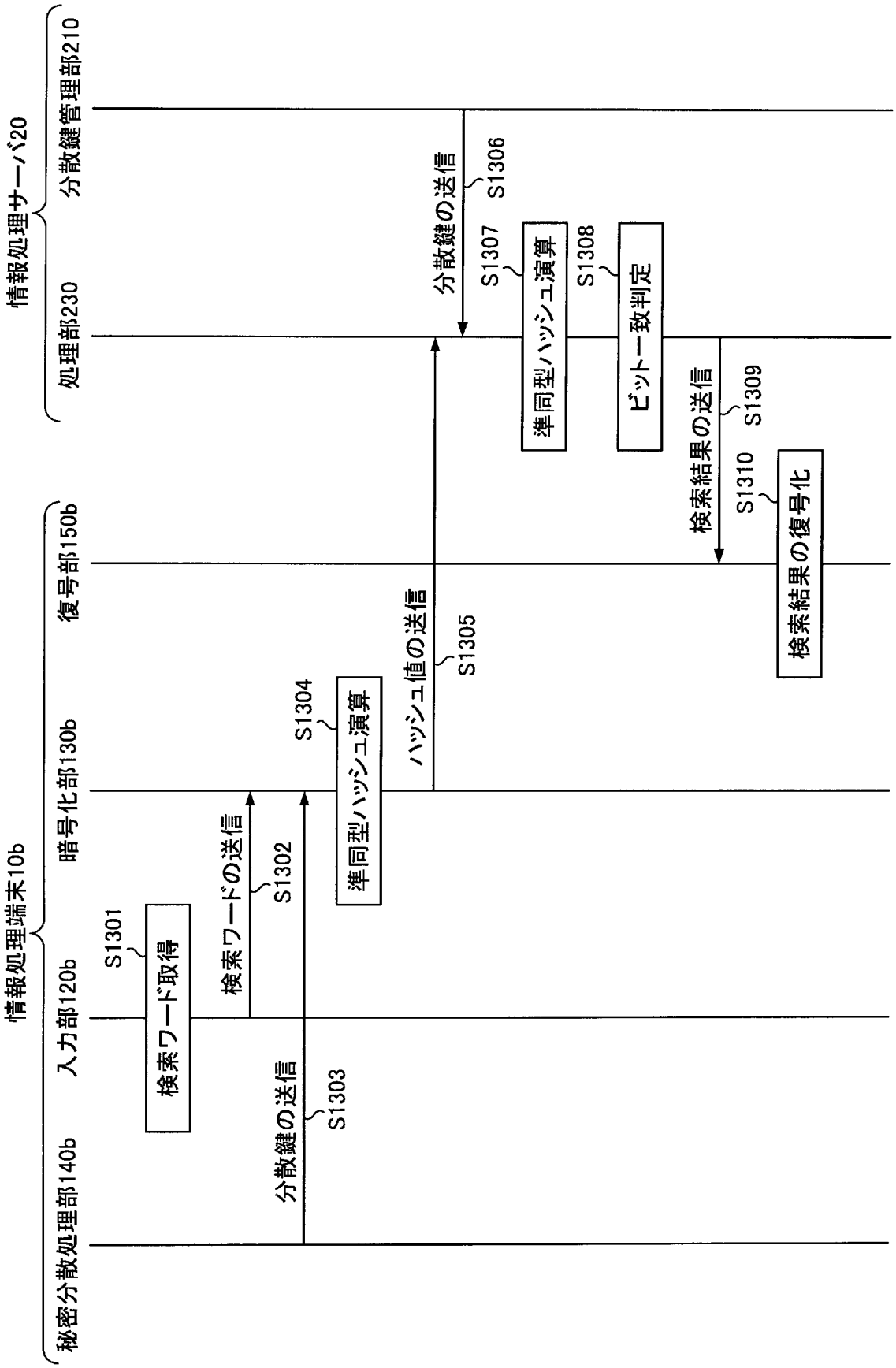
[図15]


情報処理端末10a
ユーザ鍵管理部110a
入力部120a
暗号化部130a
情報処理サーバ20
データ管理部220
S1101
ユーザ鍵生成
S1102
ユーザ鍵保存
S1103
データ取得
入力データの送信
S1104
ユーザ鍵の送信
S1105
S1106
キーワード抽出
S1107
データ暗号化
S1108
暗号化インデックス生成
暗号化データ、
暗号化インデックスの送信
S1109
S1110
暗号化データ保存
S1111
暗号化インデックス保存

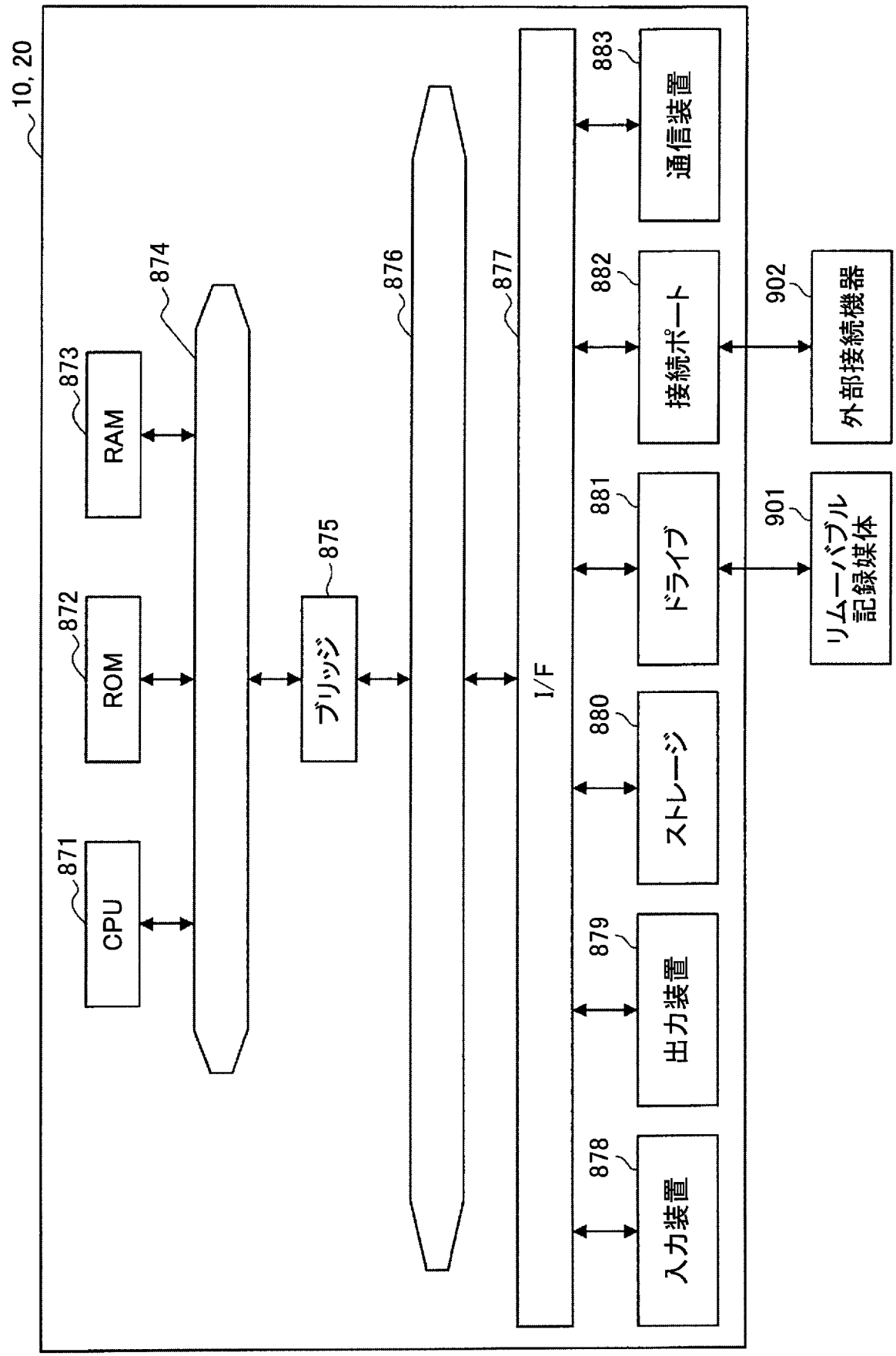
[図16]


情報処理端末10a
ユーザ鍵管理部110a
秘密分散処理部140a
情報処理端末10b
秘密分散処理部140b
情報処理サーバ20
分散鍵管理部210
ユーザ鍵の送信
S1201
S1202
分散鍵の生成
分散鍵の配布
S1203
S1204
分散鍵の保存
分散鍵の配布
S1205
S1206
分散鍵の保存

[図17]


情報処理端末10b
秘密分散処理部140b
入力部120b
暗号化部130b
復号部150b
情報処理サーバ20
処理部230
分散鍵管理部210
検索ワード取得
S1301
検索ワードの送信
S1302
分散鍵の送信
S1303
準同型ハッシュ演算
S1304
ハッシュ値の送信
S1305
分散鍵の送信
S1306
準同型ハッシュ演算
S1307
ビット一致判定
S1308
検索結果の送信
S1309
検索結果の復号化
S1310

[図18]


10, 20
CPU
871
ROM
872
RAM
873
874
ブリッジ
875
876
877
I/F
878
入力装置
879
出力装置
880
ストレージ
881
ドライブ
882
接続ポート
883
通信装置
901
リムーバブル記録媒体
902
外部接続機器

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/020337

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G09C1/00(2006.01)i, G06F16/28(2019.01)i, H04L9/08(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, G06F16/28, H04L9/08

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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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.
X A	JP 2014-60614 A (HITACHI SOLUTIONS, LTD.) 03 April 2014, paragraphs [0015]-[0035] (Family: none)	19-20 1-18
A	JP 2018-97034 A (HITACHI, LTD.) 21 June 2018, paragraphs [0175]-[0285] (Family: none)	1-20
A	JP 2013-26954 A (NEC CORP.) 04 February 2013, paragraphs [0044]-[0053] (Family: none)	1-20

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 16 August 2019 (16.08.2019)	Date of mailing of the international search report 27 August 2019 (27.08.2019)
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/JP2019/020337

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	清藤武暢，四方順司，高機能暗号を活用した情報漏えい対策「暗号化状態処理技術」の最新動向，金融研究，20 October 2014, vol. 33, no. 4, pp. 97-132, ISSN 0287-5306, in particular, pp. 105-111, 132, non-official translation (SEITO, Takenobu, SHIKATA, Junji, "Information leakage countermeasures using high-performance encryption, Latest Trends in 'Encryption State Processing Technology'", Financial Research)	1-20
A	US 2013/0275752 A1 (ZHANG, Xinwen et al.) 17 October 2013, paras. 0031-0042 & WO 2013/158798 A2 & CN 104521178 A	1-20

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０２０３３７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G09C1/00(2006.01)i, G06F16/28(2019.01)i, H04L9/08(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.　G09C1/00, G06F16/28, H04L9/08

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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
X A	JP 2014-60614 A（株式会社日立ソリューションズ）2014.04.03, 段落 0015-0035（ファミリーなし）	19-20 1-18
A	JP 2018-97034 A（株式会社日立製作所）2018.06.21, 段落 0175-0285（ファミリーなし）	1-20
A	JP 2013-26954 A（日本電気株式会社）2013.02.04, 段落 0044-0053（ファミリーなし）	1-20

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１６．０８．２０１９	２７．０８．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　４５３８
金沢　史明
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	清藤武暢，四方順司，高機能暗号を活用した情報漏えい対策「暗号化状態処理技術」の最新動向， 金融研究，2014.10.20，第33巻，第4号，pp. 97-132， ISSN 0287-5306，特にpp.105-111,132	1-20
A	US 2013/0275752 A1 (ZHANG, Xinwen et al.) 2013.10.17, paras. 0031-0042 & WO 2013/158798 A2 & CN 104521178 A	1-20