(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
2013 年 6 月 27 日 (27.06.2013)

W 画P O ¦ P C T

(10) 国際公開番号
WO 2013/094018 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP201 1/0795 19

(22) 国際出願日: 201 1 年 12 月 20 日 (20. 12.201 1)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について):三菱電機株式会社 (Mitsubishi Electric Corporation) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 Tokyo (JP).

( ) 発明者 ;および

( ) 発明者/出願人 (米国についてのみ):市川 幸宏 (ICHIKAWA, Sachihiro) [—/JP]; 〒10083 10 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 松田 規 (MATSUDA, Nor り[—/JP]; 〒1008310 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 山中 忠和 (YAMANAKA, Tadakazu) [—/JP1; 〒10083 10 東京都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP). 高島 克幸 (TAKASHIMA, Katsuyuki) [—/JP]; 〒10083 10 東¾ 都千代田区丸の内二丁目7番3号 三菱電機株式会社内 Tokyo (JP)-

(74) 代理人 :溝井 章司, 外 (MIZOI, Shoji et al.) ; 〒2470056 神奈川県鎌倉市大船二丁目17番10号 NTA大船ビル3階 溝井国際特許事務所 Kanagawa (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

[続葉有]

(54) Title: ENCRYPTED DATA ADMINISTRATION DEVICE, ENCRYPTED DATA ADMINISTRATION METHOD, AND ENCRYPTED DATA ADMINISTRATION PROGRAM

(54) 発明の名称 :暗号化データ管理装置、暗号化データ管理方法及び暗号化データ管理プログラム

[図1]

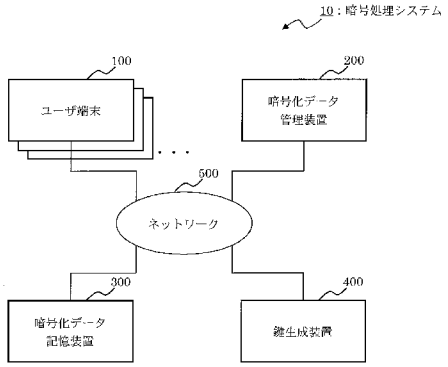


FIG. 1:
10 Encryption processing system
100 User terminal
200 Encrypted data administration device
300 Encrypted data storage device
400 Key generator device
500 Network

(57) Abstract: An objective of the present invention is to implement an invalidation protocol of a secret key which is usable even in a mathematical function encryption protocol. In an encryption processing system (10), an encryption protocol is used with which a secret key cannot be used to decrypt encrypted data when attribute information and key information which are set in the encrypted data do not correspond to attribute information and key information which are set in the secret key. An encrypted data administration device (200) is disposed which carries out a relay between a user terminal (100) which carries out data encryption and decryption and an encrypted data storage device (300) which stores the encrypted data. The encrypted data administration device (200) determines whether a user whose secret key is invalid is included among users who have attribute information which is set in the encrypted data wmch is acquired from the encrypted data storage unit (300), and sets to the encrypted data as the key information different values depending on the determination result. The encrypted data administration device (200) transmits to the user terminal (100) the encrypted data for which the key information is set.

(57) 要約 :

[続葉有]

WO 2013/094018 A1

添付公開書類：

- 国際調査報告 (条約第21条(3))

関数型暗号方式においても利用可能な秘密鍵の失効方式を実現する。暗号化データに設定された属性情報及び鍵情報と、秘密鍵に設定された属性情報及び鍵情報とが対応していない場合、暗号化データを秘密鍵で復号できない暗号化方式を用いる暗号処理システム10において、データの暗号化及ひ復号を行うユーザ端末100と、暗号化データを記憶する暗号化データ記憶装置300との間の中継を行う暗号化データ管理装置200を設ける。暗号化データ管理装置200は、暗号化データ記憶装置300から取得した暗号化データに設定された属性情報を有するユーザに、秘密鍵が失効しているユーザが含まれるか否かを判定し、判定結果によって異なる値を鍵情報として暗号化データに設定する。そして、暗号化データ管理装置200は、鍵情報を設定した暗号化データをユーザ端末100へ送信する。

明　細　書

発明の名称　：

暗号化データ管理装置、暗号化データ管理方法及び暗号化データ管理プログラム

技術分野

[0001] この発明は、秘密鍵の失効を実現する暗号化データの管理技術に関する。

背景技術

[0002] １９７６年にディフィーとヘルマンとが開発した公開鍵暗号方式は、様々な改良と機能拡張が行われている。２００１年には、ボネとフランクリンとにより、ペアリング演算に基づいたＩＤベース暗号と呼ばれる公開鍵暗号方式が開発された。近年ではペアリング演算に基づいた方式に関する研究が盛んに行われている。

ペアリングを用いた高機能な公開鍵暗号方式として、非特許文献１，２に記載された高い安全性を持つ暗号方式（以下、関数型暗号方式と呼ぶ）がある。関数型暗号方式は、従来の暗号とは異なり、復号が可能なユーザ（秘密鍵）を複数指定した暗号化を１つの公開鍵で行うことができる。

[0003] 公開鍵暗号方式を一般のユーザが利用するシステムに適用した場合には、ユーザが秘密鍵を紛失する恐れがある。この場合、紛失した秘密鍵が悪用されることを防止するため、紛失した秘密鍵を失効させることが必要になる。

秘密鍵を失効させる失効方式としては、特許文献１，２に記載された方式がある。

[0004] 特許文献１には、特定のユーザの秘密鍵を無効にするコマンドが入力された場合に、そのユーザの秘密鍵を無効にし、秘密鍵を再発行するコマンドが入力された場合に新規の暗号鍵及び秘密鍵の鍵ペアを生成する失効方式について記載されている。

[0005] 特許文献２には、アクセス要求とアクセス識別子とを受信したとき、無効にされた識別子のリストに記載された識別子とアクセス識別子とが一致する

かを確認し、一致する場合、アクセスを終了させる失効方式について記載されている。

先行技術文献

特許文献

[0006] 特許文献1 :特開２００５_５１６１４号公報

特許文献2 :特表２００３-５０６７８２号公報

非特許文献

[0007] 非特許文献1 :T. Okamoto, K. Takashima, "A geometric approach on pairings and hierarchical predicate encryption", In:Poster session, EUROCRYPT 2009.

非特許文献2 :T. Okamoto, K. Takashima, "Fully Secure Functional Encryption With General Relations from the Decisional Linear Assumption", CRYPTO 2010, Lecture Notes In Computer Science, 2010, Volume 6223/2010.

発明の概要

発明が解決しようとする課題

[0008] 関数型暗号方式は、従来と大きく異なる暗号方式であるため、従来の暗号方式に適用された秘密鍵の失効方式を適用することができない。また、関数型暗号方式は、従来の暗号方式と同様に、アルゴリズム自体では失効を考慮していない。そのため、関数型暗号方式は、一般のユーザが利用するシステムに適用した場合に発生する可能性の高い秘密鍵の紛失に対応できない。

[0009] 特許文献１に記載された失効方式では、秘密鍵が失効した場合に新しく鍵ペアを再発行する。そのため、この失効方式を関数型暗号方式に適用すると失効した秘密鍵で復号できるように暗号化した全てのデータを再暗号化しな

ければならない。したがって、過去に暗号化した多くデータを再暗号化することが必要となる恐れがあり、膨大なコストがかかってしまう恐れがある。

特許文献2に記載された失効方式を関数型暗号方式に適用した場合も同様に、失効した秘密鍵で復号できるように暗号化したデータを再暗号化しなければならない。

[001 0] この発明は、関数型暗号方式においても利用可能な秘密鍵の失効方式を実現することを主な目的とする。

課題を解決するための手段

[001 1] この発明に係る暗号化データ管理装置は、

暗号化データに設定された属性情報及び鍵情報と、秘密鍵に設定された属性情報及び鍵情報とが対応していない場合、前記暗号化データを前記秘密鍵で復号できない暗号化方式において、前記暗号化データを管理する暗号化データ管理装置であり、

属性情報が設定された暗号化データを記憶装置から取得するデータ取得部と、

前記データ取得部が取得した前記暗号化データに設定された前記属性情報を有するユーザに、秘密鍵が失効しているユーザが含まれるか否か判定する失効判定部と、

秘密鍵が失効しているユーザが含まれると前記失効判定部に判定されたか否かによって、異なる値を前記鍵情報として前記暗号化データに設定する鍵情報設定部と、

前記鍵情報設定部が鍵情報を設定した暗号化データをユーザ端末八送信するデータ送信部と

を備えることを特徴とする。

発明の効果

[001 2] この発明に係る暗号化データ管理装置は、暗号化データを復号可能なユーザに秘密鍵が失効しているユーザが含まれるか否かによって、異なる値を鍵情報として設定した上で、ユーザへ送信する。これにより、失効した秘密鍵

で暗号化データが復号されることを防止できる。

図面の簡単な説明

[001 3] [図1]実施の形態１に係る暗号処理システム１０の構成図。

[図2]実施の形態１に係るユーザ端末１００の構成図。

[図3]実施の形態１に係る暗号化データ管理装置２００の構成図。

[図4]実施の形態１に係る暗号化データ記憶装置３００の構成図。

[図5]実施の形態１に係る鍵生成装置４００の構成図。

[図6]実施の形態１に係る暗号化データ登録処理の流れを示すフローチャート。

[図7]実施の形態１に係る暗号化データ取得処理の流れを示すフローチャート。

[図8]実施の形態3に係る暗号化データ管理装置２００の構成図。

[図9]実施の形態3に係る暗号化データ記憶装置３００の構成図。

[図10]実施の形態3に係る暗号化データ登録処理の流れを示すフローチャート。

[図11]実施の形態3に係る暗号化データ取得処理の流れを示すフローチャート。

[図12]ユーザ端末１００、暗号化データ管理装置２００、暗号化データ記憶装置３００、鍵生成装置４００のハードウエア構成の一例を示す図。

発明を実施するための形態

[0014] 実施の形態１.

実施の形態１では、非特許文献１に記載された関数型暗号方式において、秘密鍵の失効方式を実現する方法を説明する。

[001 5] まず、非特許文献１に記載された関数型暗号方式について、この実施の形態の説明に必要な部分のみに簡略化して説明する。

非特許文献１に記載された関数型暗号方式には、Ｓｅｔｕｐアルゴリズム、ＫｅｙＧｅｎアルゴリズム、Ｅｎｃアルゴリズム、Ｄｅｃアルゴリズムがある。

[001 6] Ｓｅｔｕｐアルゴリズムは、公開パラメータｐｋとマスター秘密鍵ｓｋとを生成するアルゴリズムである。

Ｓｅｔｕｐアルゴリズムでは、双対ペアリングベクトル空間のパラメータｐａｒａｍと、ペアリング演算で関連付けられた双対正規直交基底である基底Ｂ及び基底Ｂ*とが生成される。そして、パラメータｐａｒａｍと基底Ｂとが公開パラメータｐｋとされ、基底Ｂ*がマスター秘密鍵ｓｋとされる。

なお、基底Ｂは、基底ベクトルｂい b_2，．．．，b_{n+2}を有し、基底Ｂ*は、基底ベクトル b^*_1，b^*_2，．．．，b^*_{n+2}を有する。つまり、基底Ｂ，Ｂ*は、それぞれのｎ＋２個（ｎは１以上の整数）の基底ベクトルを有する。

[001 7] ＫｅｙＧｅｎアルゴリズムは、ユーザ秘密鍵ｋ*を生成するアルゴリズムである。

ＫｅｙＧｅｎアルゴリズムでは、式１に示すように、マスター秘密鍵ｓｋに含まれる基底Ｂ*を用いて、ユーザ秘密鍵ｋ*が生成される。

<式１>

$k^* := \sigma(\nu_1 b^*_1 + \ldots + \nu_n b^*_n) + b^*_{n+1}$

ここで、σは、乱数値である。ν ,,．．．，ν_ηは、ユーザ秘密鍵ｋ*が与えられるユーザの属性情報等である。

[001 8] Ｅｎｃアルゴリズムは、暗号化データｃを生成するアルゴリズムである。

Ｅｎｃアルゴリズムでは、式２に示すように、公開パラメータｐｋに含まれる基底Ｂを用いて、暗号化データｃの要素ｃ ,が生成される。

<式２>

$c' := \omega(x_1 b_1 + \ldots + x_n b_n) + \zeta b_{n+1} + \phi b_{n+2}$

ここで、ω，ζ，φは、乱数値である。χ ,,．．．，χ_ηは、暗号化データｃを復号可能なユーザの属性情報等である。

また、Ｅｎｃアルゴリズムでは、式３に示すように、公開パラメータｐｋに含まれるパラメータｐａｒａｍを用いて、暗号化データｃの要素 c_2が生成される。

<式３>

$c_2 := e(g, g)^{\zeta} \cdot m$

ここで、gは、パラメータparamに含まれる情報であり、双対ペアリングベクトル空間を構成する群Gの要素である。mは、メッセージである。$e(g, g)$は、要素gと要素gとについてのペアリング演算である。

[0019] Decアルゴリズムは、暗号化データcをユーザ秘密鍵k^*で復号するアルゴリズムである。

Decアルゴリズムでは、式4に示す計算が実行され、暗号化データcがユーザ秘密鍵k^*で復号されて、m'が抽出される。

< 式4 >

$m' := c_2 / e(c_1, k)$

ここで、$e(c_1, k^*)$は、要素c,とユーザ秘密鍵k^*とについてのペアリング演算である。

[0020] Decアルゴリズムでは、ユーザ秘密鍵k^*における基底ベクトル$b^*_1, \ldots, b^*_n$に設定された属性情報等$(v_1, \ldots, v_n)$と、要素C_Iにおける基底ベクトル$b_1, \ldots, b_n$に設定された属性情報等$(x_1, \ldots, x_n)$とが対応する場合、抽出されたm' = mとなる。

属性情報等$(v_1, \ldots, v_n)$と属性情報等$(x_1, \ldots, x_n)$とが対応するとは、$\sum_{i=1}^{n} v_i \cdot x_i = 0$となることである。

[0021] ペアリング演算$e(sg, tg) = e(g, g)^{st}$である。そのため、$e(c_1, k^*) = e(g, g)^{Y}$となる。ここで、$Y = \omega\sigma(x_1 \cdot v_1 + \ldots \chi_\eta \cdot v_\eta) + \zeta$である。したがって、$\sum_{i=1}^{n} v$に$\chi_i = 0$であれば、$Y = \zeta$であり、$e(c_1, k^*) = e(g, g)^{\zeta}$である。

式3に示すように、$c_2 := e(g, g)^{\zeta} \cdot m$であるから、式4の計算を実行すれば、$\sum_{i=1}^{n} v$に$x_i = 0$の場合には、m' = mとなる。

[0022] 以下の説明では、説明を簡単にするため、n = 4として説明する。

[0023] 図1は、実施の形態1に係る暗号処理システム10の構成図である。

暗号処理システム10は、非特許文献1，2等に記載された関数型暗号方式に基づく暗号処理を実現する。暗号処理システム10は、複数のユーザ端

末１００、暗号化データ管理装置２００、暗号化データ記憶装置３００、鍵生成装置４００を備える。各ユーザ端末１００、暗号化データ管理装置２００、暗号化データ記憶装置３００、鍵生成装置４００は、それぞれ、インターネット等のネットワーク５００を介して接続されている。

[0024] 図２は、実施の形態１に係るユーザ端末１００の構成図である。

ユーザ端末１００は、ユーザが使用する端末であり、データの暗号化、復号を行う。ユーザ端末１００は、暗号化データ生成部１１０、データ送信部１２０、データ受信部１３０、復号部１４０、鍵管理部１５０を備える。

[0025] 図３は、実施の形態１に係る暗号化データ管理装置２００の構成図である。

暗号化データ管理装置２００は、ユーザ端末１００と暗号化データ記憶装置３００との間で、暗号化データの管理をする。暗号化データ管理装置２００は、データ受信部２１０（データ取得部）、失効判定部２２０、鍵情報設定部２３０、データ送信部２４０、失効情報管理部２５０、鍵管理部２６０を備える。

[0026] 図４は、実施の形態１に係る暗号化データ記憶装置３００の構成図である。

暗号化データ記憶装置３００は、暗号化データを記憶する。暗号化データ記憶装置３００は、データ受信部３１０、データ操作部３２０、データ送信部３３０、暗号化データ管理部３４０を備える。

[0027] 図５は、実施の形態１に係る鍵生成装置４００の構成図である。

鍵生成装置４００は、ユーザ秘密鍵ｋ*、マスター秘密鍵ｓｋ、公開パラメータｐｋを生成する。鍵生成装置４００は、指示受信部４１０、鍵生成部４２０、鍵送信部４３０、マスター鍵記憶部４４０を備える。

[0028] 暗号処理システム１０の主な処理には、暗号化データ登録処理と、暗号化データ取得処理とがある。暗号化データ登録処理は、ユーザ端末１００が暗号化データを暗号化データ記憶装置３００に登録する処理である。暗号化データ取得処理は、ユーザ端末１００が暗号化データを暗号化データ記憶装置

３００から取得する処理である。

また、暗号化データ登録処理と暗号化データ取得処理とには、３つの前提条件がある。

そこで、３つの前提条件を説明した上で、暗号化データ登録処理と、暗号化データ取得処理とを説明する。

[0029] <前提条件１>

ユーザ端末１００が、関数型暗号方式におけるユーザ秘密鍵ｋ*を取得している必要がある。

鍵生成装置４００の指示受信部４１０は、ユーザ端末１００等から鍵の生成指示を受信する。すると、鍵生成装置４００の鍵生成部４２０は、処理装置により、Ｓｅｔｕｐアルゴリズムを実行して、公開パラメータｐｋとマスター秘密鍵ｓｋとを生成し、マスター鍵記憶部４４０に記憶する。また、鍵生成部４２０は、処理装置により、ＫｅｙＧｅｎアルゴリズムを実行して、マスター秘密鍵ｓｋに含まれる基底Ｂ*を用いて、ユーザ秘密鍵ｋ*を生成する。

そして、鍵送信部４３０は、公開パラメータｐｋとユーザ秘密鍵ｋ*とをユーザ端末１００へ送信する。ユーザ端末１００のデータ受信部１３０は、公開パラメータｐｋとユーザ秘密鍵ｋ*とを受信して、鍵管理部１５０に記憶する。また、鍵送信部４３０は、公開パラメータｐｋを暗号化データ管理装置２００へ送信する。暗号化データ管理装置２００のデータ受信部２１０は、公開パラメータｐｋを受信して、鍵管理部２６０に記憶する。

なお、Ｓｅｔｕｐアルゴリズムは一度だけ実行されればよく、ユーザ秘密鍵ｋ*を生成する度に実行する必要はない。

また、鍵送信部４３０がユーザ秘密鍵ｋ*をユーザ端末１００へ送信する場合、ユーザ認証を行い、正当なユーザの端末であることを確認する。また、鍵送信部４３０がユーザ秘密鍵ｋ*をユーザ端末１００へ送信する場合、盗聴と改ざんを防ぐため、ＳＳＬ（Ｓｅｃｕｒｅ Ｓｏｃｋｅｔ Ｌａｙｅｒ）等を用いた安全な通信路を使用する。つまり、ユーザ秘密鍵ｋ*が悪意ある第

三者に不正に利用されないようにする。

[0030] ここでは、鍵生成部４２０は、式５に示すようにユーザ秘密鍵ｋ＊を生成する。

＜式５＞

$$k^* = \sigma!(v_1 b^*_1 + v_2 b^*_2) + \sigma_2 (v_3 b^*_3 + v_4 b^*_4) + b^*_5$$

ここで、ひい σ_2は、乱数値である。ν ,, v_2は、鍵情報である。ここでは、鍵情報として、新たな鍵の発行毎に値がインクリメントされる世代番号を用いる。v_3, v_4は、ユーザ秘密鍵ｋ＊が与えられるユーザの属性情報である。

世代番号の値をＰとし、属性情報の値をαとした場合、ここでは、式６に示すようにユーザ秘密鍵ｋ＊は生成される。

＜式６＞

$$k^* = \sigma!(p b^*_1 + b^*_2) + \sigma_2 (\alpha b^*_3 + b^*_4) + b^*_5$$

つまり、ソ ,:ニジ, v_2 :＝１, v_3 :＝α, Ｖ４ :＝１である。

[0031] 鍵生成部４２０は、あるユーザに対して、初めにユーザ秘密鍵ｋ＊を生成する場合には、世代番号の値を１とする。そのュ－ザがュ－ザ秘密鍵ｋ＊を紛失して、再びュ－ザ秘密鍵ｋ＊を生成する場合には、世代番号の値をインクリメントして２とする。以降、ユーザ秘密鍵ｋ＊を紛失して再生成する場合には、インクリメントした世代番号の値を用いる。

[0032] ＜前提条件２＞

ユーザ端末１００が、ドメイン公開鍵ｄｐｋを取得している必要がある。

ドメイン公開鍵ｄｐｋとは、暗号化データ管理装置２００の秘密鍵（ドメイン秘密鍵ｄｓｋ）に対応する公開鍵である。なお、ドメイン秘密鍵ｄｓｋとドメイン公開鍵ｄｐｋとの鍵ペアは、関数型暗号方式における鍵ペアでなく、他の公開鍵暗号方式における鍵ペアであってもよい。

鍵生成部４２０は、ドメイン秘密鍵ｄｓｋとドメイン公開鍵ｄｐｋとの鍵ペアを生成し、鍵送信部４３０は、ドメイン公開鍵ｄｐｋをユーザ端末１００へ送信し、ドメイン秘密鍵ｄｓｋを暗号化データ管理装置２００へ送信す

る。ユーザ端末１００のデータ受信部１３０は、ドメイン公開鍵ｄｐｋを受信し、鍵管理部１５０に記憶する。また、暗号化データ管理装置２００のデータ受信部２１０は、ドメイン公開鍵ｄｐｋを受信し、鍵管理部２６０に記憶する。

鍵送信部４３０がドメイン秘密鍵ｄｓｋを暗号化データ管理装置２００へ送信する場合、盗聴と改ざんを防ぐため、ＳＳＬ等を用いた安全な通信路を使用する。

[0033] <前提条件３>

暗号化データ管理装置２００が、失効情報を取得している必要がある。

失効情報とは、ユーザ秘密鍵ｋ*を紛失したユーザの識別情報と、紛失したユーザ秘密鍵ｋ*の世代番号とを示す情報である。

ユーザがユーザ秘密鍵ｋ*を紛失した場合、ユーザ端末１００のデータ送信部１２０は、ユーザ秘密鍵ｋ*を紛失したユーザの識別情報と、紛失したユーザ秘密鍵ｋ*の世代番号とを失効情報として暗号化データ管理装置２００へ送信する。暗号化データ管理装置２００のデータ受信部２１０は、失効情報を受信し、失効情報管理部２５０に記憶する。

なお、データ受信部２１０は、失効情報を受信する場合、ユーザ認証を行し、失効を届け出たユーザが本人であることを確認する。

[0034] <暗号化データ登録処理>

図６は、実施の形態１に係る暗号化データ登録処理の流れを示すフローチャートである。

（Ｓ１１ :暗号化処理）

ユーザ端末１００の暗号化データ生成部１１０は、Ｅｎｃアルゴリズムを実行して暗号化データｃを生成する。

[0035] ここでは、暗号化データ生成部１１０は、処理装置により、式７に示すように、鍵管理部１５０に記憶した公開パラメータｐｋに含まれる基底Ｂを用いて、暗号化データｃの要素ｃ ,を生成する。

<式７>

$c_1 := \omega_1 (r_1 b_1 + r_2 b_2) + \omega_2 (x_3 b_3 + x_4 b_4) + \zeta b_5 + \phi b_6$

ここで、ω_1, ω_2, r_1, r_2, ζ, ϕは、乱数である。x_3, x_4は、暗号化データcを復号可能なユーザの属性情報が設定される。

属性情報の値をαとした場合、ここでは、式8に示すように暗号化データcは生成される。

< 式8 >

$c_1 := \omega_1 (r_1 b_1 + r_2 b_2) + \omega_2 (b_3 - \alpha b_4) + \zeta b_5 + \phi b_6$

つまり、$\chi_3 := 1$, $\chi_4 := -\alpha$である。

[0036] また、暗号化データ生成部１１０は、処理装置により、式9に示すように、鍵管理部１５０に記憶した公開パラメータpkに含まれるパラメータparamを用いて、暗号化データcの要素c_2を生成する。

< 式9 >

$c_2 := e(g, g)^m$

[0037] また、暗号化データ生成部１１０は、処理装置により、鍵管理部１５０に記憶したドメイン公開鍵dpにで、ω_1 r_1を暗号化したE (ω_1 r_1) と、ω_1 r_2を暗号化したE (ω_1 r_2) とを生成する。

また、暗号化データ生成部１１０は、要素c_1に設定した属性情報が示すユーザの識別情報をユーザリストulとして生成する。

[0038] （Ｓ１２：第1データ送信処理）

ユーザ端末１００のデータ送信部１２０は、通信装置により、暗号化データ生成部１１０が生成した要素c_1, c_2, E (ω_1, r_1), E (ω_1, r_2), ulを含む暗号化データcを、暗号化データ管理装置２００へ送信する。

[0039] （Ｓ１３：第2データ送信処理）

暗号化データ管理装置２００のデータ受信部２１０は、通信装置により、暗号化データcをユーザ端末１００から受信する。暗号化データ管理装置２００のデータ送信部２４０は、暗号化データcに関連情報rを添付して、暗号化データ記憶装置３００へ送信する。なお、関連情報rとは、暗号化データcの作成者や、暗号化データcの受信日時等であり、後に暗号化データc

を検索する際に利用される情報である。

[0040] （Ｓ１４：データ記憶処理）

暗号化データ記憶装置３００のデータ受信部３１０は、通信装置により、暗号化データｃと関連情報ｒとを暗号化データ管理装置２００から受信する。暗号化データ記憶装置３００のデータ操作部３２０は、暗号化データｃと関連情報ｒとを関連付けて、暗号化データ管理部３４０に記憶する。

[0041] （Ｓ１５：結果送信処理）

暗号化データ記憶装置３００のデータ送信部３３０は、通信装置により、暗号化データｃの記憶が成功したか否かを示す結果情報を、暗号化データ管理装置２００へ送信する。

[0042] （Ｓ１６：結果転送処理）

暗号化データ管理装置２００のデータ受信部２１０は、通信装置により、結果情報を暗号化データ記憶装置３００から受信する。暗号化データ管理装置２００のデータ送信部２４０は、通信装置により、結果情報をユーザ端末１００へ送信する。

[0043] （Ｓ１７：結果受信処理）

ユーザ端末１００のデータ受信部１３０は、通信装置により、結果情報を暗号化データ管理装置２００から受信する。

[0044] ＜暗号化データ取得処理＞

図７は、実施の形態１に係る暗号化データ取得処理の流れを示すフローチャートである。

（Ｓ２１：キーワード送信処理）

ユーザ端末１００のデータ送信部１２０は、通信装置により、暗号化データｃを特定可能なキーワードを、暗号化データ管理装置２００へ送信する。

[0045] （Ｓ２２：キーワード転送処理）

暗号化データ管理装置２００のデータ受信部２１０は、通信装置により、キーワードをユーザ端末１００から受信する。暗号化データ管理装置２００のデータ送信部２４０は、通信装置により、キーワードを暗号化データ記憶

装置３００へ送信する。

[0046] （Ｓ２３ :データ検索処理）

暗号化データ記憶装置３００のデータ受信部３１０は、通信装置により、キーワードを暗号化データ管理装置２００から受信する。暗号化データ記憶装置３００のデータ操作部３２０は、処理装置により、キーワードと一致する関連情報ｒを有する暗号化データｃを暗号化データ管理部３４０から抽出する。

[0047] （Ｓ２４ :第１データ送信処理）

暗号化データ記憶装置３００のデータ送信部３３０は、通信装置により、抽出した暗号化データｃを暗号化データ管理装置２００へ送信する。

[0048] （Ｓ２５ :世代番号付け代え処理）

暗号化データ管理装置２００のデータ受信部２１０は、通信装置により、暗号化データｃを暗号化データ記憶装置３００から受信する。

暗号化データ管理装置２００の失効判定部２２０は、処理装置により、暗号化データｃのユーザリストｕｌに含まれるユーザの識別情報が、失効情報管理部２５０が記憶する失効情報に含まれているか否か判定する。鍵情報設定部２３０は、処理装置により、暗号化データｃの要素ｃ ,における乱数値ｒ$_{1}$, ｒ$_{2}$を、失効判定部２２０の判定結果に応じて異なる値に設定し直し、要素○パ を生成する。

具体的には、鍵情報設定部２３０は、以下のように乱数値ｒいｒ$_{2}$を設定し直す。なお、ここでは、式８に示す要素ｃ ,における乱数値ｒいｒ$_{2}$を設定し直した要素ｃ$_{1}$’ を示す。

[0049] ユーザリストｕｌに含まれるユーザの識別情報が、失効情報管理部２５０が記憶する失効情報に含まれていない場合、鍵情報設定部２３０は、式１０に示すように、要素ｃ ,' を生成する。

< 式１０ >

$$c' := \omega'(b' - b_2) + \omega_2 (b_3 - \alpha b_4) + \zeta b_5 + \phi b_6$$

つまり、 门 を１に設定し直し、 「$_{2}$を_ １に設定し直す。ｒ$_{2}$を設定し直し

た_ 1は、_ 1 X世代番号の初期値である。

なお、式１１に示す計算をすることにより、式8 に示す要素ｃ ,から式１０に示す要素ｃ ;' を得ることができる。

< 式１１>

ｃ ⁉ := ｃ !— (ω 1 ｒ 1 ｂ 1 + ω 1 ｒ 2 ｂ 2) + (u>1 ｂ 1 — ω 1 ｂ 2)

ここで、ω ,r ,, ω 1 。は、暗号化データｃの要素Ｅ (ω 1 ｒ 1) , Ｅ (ω 1 ｒ 2) を、鍵管理部２６０に記憶したドメイン秘密鍵ｄｓｋで復号することにより得られる。また、ｂ 1, ｂ 2は、公開パラメータｐｋに含まれる基底Ｂから得られる。

[0050] ユーザリストｕｌに含まれるユーザの識別情報が、失効情報管理部２５０が記憶する失効情報に含まれている場合、鍵情報設定部２３０は、式１２に示すように、要素 。パ を生成する。

< 式１２>

ｃ ⁉ := ω !(ｂ !- ｐ !ｂ 2) + ω 2 (ｂ 3 _ α ｂ 4 リ + ζ ｂ 5 + ø ｂ 6

つまり、ｒ 1を1に設定し直し、ｒ 2を一ｐ ,に設定し直す。ｒ 2を設定し直した—ρ 1は、— 1 X (失効したユーザ秘密鍵ｋ*の世代番号の値+ 1) である。つまり、ユーザリストｕｌにユーザＡが含まれており、失効したユーザＡのユーザ秘密鍵ｋ*の世代番号として1が失効リストに含まれている場合、—ｐ ,は、－1 X (1 + 1) = —2 となる。

なお、式１３に示す計算をすることにより、式8 に示す要素ｃ ,から式１２に示す要素ｃ ;' を得ることができる。

< 式１３>

ｃ ⁉ := ｃ !— (ω 1 ｒ 1 ｂ 1 + ω 1 ｒ 2 ｂ 2) + (ω 1 ｂ 1 — ω 1 ρ 1 ｂ 2)

[0051] (Ｓ２６ :第２データ送信処理)

暗号化データ管理装置２００のデータ送信部２４０は、通信装置により、暗号化データｃの要素ｃ ,を要素ｃパ に置き換えた暗号化データｃ' を、ユ—ザ端末１００へ送信する。

[0052] (Ｓ２７ :復号処理)

ユーザ端末１００の暗号化データ生成部１１０は、通信装置により、暗号化データc'を暗号化データ管理装置２００から受信する。ユーザ端末１００の復号部１４０は、Ｄｅｃアルゴリズムを実行することにより、暗号化データc'をユーザ秘密鍵k*で復号する。

ここでは、復号部１４０は、処理装置により、式１４に示す計算を実行することにより、暗号化データc'をユーザ秘密鍵k*で復号して、メッセージm'を抽出する。

<式１４>

m' := c$_2$／e（c !, k つ

[0053] 上述したように、ユーザ秘密鍵k*における基底ベクトルb* ,, . . . , b*$_n$に設定された属性情報等（v$_I$, . . . , v$_n$）と、要素C$_I$における基底ベクトルb$_1$, . . . , b$_n$に設定された属性情報等（x$_I$, . . . , x$_n$）とが対応する場合、抽出されたm' = mとなる。そして、ここでは、属性情報等（v$_1$, . . . , v$_n$）と属性情報等（x$_I$, . . . , x$_n$）とが対応するとは、$\Sigma_{i=1}^{n} v_i \cdot x_i = 0$となることである。

[0054] ユーザ端末１００は、初めに生成され、世代番号の値として1が付されたユーザ秘密鍵k*を有しているとする。つまり、ユーザ端末１００は、式６のPに1が設定された、式１５に示すユーザ秘密鍵k*を有しているとする。

<式１５>

k* = σ !（b*$_1$+ b*$_2$）+ σ$_2$（a b*$_3$+ b*$_4$）+ b*$_5$

また、Ｓ１１において、暗号化データcの要素c ,は、式１６（＝式８）に示すように生成されているとする。

<式１６>

c ! := ω !ｲ ibi+ r$_2$b$_2$）+ ω$_2$（b$_3$_ α b$_4$ﾘ+ ζ b$_5$+ ø b$_6$

[0055] ユーザリストuＩに含まれるユーザの識別情報が失効情報に含まれていない場合、式１７（＝式１０）に示すように、要素c$_1$'は生成される。

<式１７>

c !' := ω !（b !- b$_2$）+ ω$_2$（b$_3$_ α b$_4$）+ ζ b$_5$+ ø b$_6$

この場合、$v_1 = 1$, $v_2 = 1$, $v_3 = \alpha$, $v_4 = 1$であり、$x_1 = 1$, $x_2 = -1$, $x_3 = 1$, $x_4 = -\alpha$であるから、$\sum_{i=1}^{4} v_i \cdot x_i = 1 - 1 + \alpha - \alpha = 0$となる。したがって、S26で抽出されたメッセージm'は、S11で暗号化データcの要素c_2に設定されたメッセージmと等しい。

つまり、ユーザ秘密鍵k^*で、暗号化データcを復号することができる。

[0056] 一方、ユーザリストulに含まれるユーザの識別情報が失効情報に含まれている場合、式18に示すように、要素c_1'は生成される。ここでは、世代番号がの値が1のユーザ秘密鍵k^*が失効していたとする。

<式18>

$$c_1' = \omega^{r'}(D - 2b_2) + \omega_2(b_3 - \alpha b_4) + \alpha b_5 + 0 b_6$$

この場合、ユーザ秘密鍵k^*において、基底ベクトル$b^*_1, \ldots, b^*_4$の係数に設定された$v_1, \ldots, v_4$は、$v_1 = 1$, $v_2 = 1$, $v_3 = \alpha$, $v_4 = 1$である。また、要素c_1'において、基底ベクトル$b_1, \ldots, b_4$の係数に設定された$x_1, \ldots, x_4$は、$x_1 = 1$, $x_2 = -2$, $x_3 = 1$, $x_4 = -\alpha$であるから、$\sum_{i=1}^{4} v_i \cdot x_i = 1 - 2 + \alpha - \alpha \neq 0$となる。したがって、S26で抽出されたメッセージm'は、S11で暗号化データcの要素c_2に設定されたメッセージmと等しくない。

つまり、失効しているユーザ秘密鍵k^*では、暗号化データcを復号することはできない。

[0057] しかし、ユーザ端末100は、鍵生成装置400にユーザ秘密鍵k^*を再生成してもらい、世代番号の値として2が付されたユーザ秘密鍵k^*を取得したとする。つまり、ユーザ端末100は、式6のpに2が設定された、式19に示すユーザ秘密鍵k^*を取得したとする。

<式19>

$$k^* = \sigma^{r}(2b^*_1 + b^*_2) + \sigma_2(ab^*_3 + b^*_4) + b^*_5$$

この場合、$v_1 = 2$, $v_2 = 1$, $v_3 = \alpha$, $v_4 = 1$であり、$x_1 = 1$, $x_2 = -2$, $x_3 = 1$, $x_4 = -\alpha$であるから、$\sum_{i=1}^{4} v_i \cdot x_i = 2 - 2 + \alpha - \alpha = 0$となる。したがって、S26で抽出されたメッセージm'は、S11で暗

号化データｃの要素c_2に設定されたメッセージｍと等しい。

つまり、ユーザ秘密鍵ｋ*を紛失した場合、ユーザ秘密鍵ｋ*を再生成してもらうことで、暗号化データｃの復号が可能となる。

[0058] また、ユーザ端末１００が、暗号化データ管理装置２００を介すことなく、暗号化データ記憶装置３００から暗号化データｃを取得することも考えられる。しかし、この場合、暗号化データｃの要素ｃ,は、式２０（＝式８）に示す通りである。

＜式２０＞

$$c_! := \omega_! \{ i b_i + r_2 b_2) + \omega_2 (b_3 - \alpha b_4 \} + \zeta b_5 + \phi b_6$$

この場合、乱数値 冂 ，r_2が用いられているため、ユーザ秘密鍵ｋ*に設定された世代番号の値がいくつであっても、$\sum_{i=1}^{4} v_i \cdot x_i \neq 0$となり、復号できない。

[0059] 以上のように、実施の形態１に係る暗号処理システム１０では、ユーザ秘密鍵ｋ*を紛失した場合には、紛失したユーザ秘密鍵ｋ*では暗号化データｃを復号できない状態とし、再生成されたユーザ秘密鍵ｋ*では暗号化データｃを復号できる状態とすることができる。特に、この際、既に暗号化データ記憶装置３００に記憶された暗号化データｃに対して、再暗号化等の処理を行う必要はない。

[0060] また、実施の形態１に係る暗号処理システム１０では、仮に、ユーザ端末１００が、暗号化データ管理装置２００を介すことなく、暗号化データ記憶装置３００から暗号化データｃを取得した場合にも、暗号化データｃを復号できない。

したがって、実施の形態１に係る暗号処理システム１０では、暗号化データ記憶装置３００を第三者に委託し、暗号化データ記憶装置３００から暗号化データｃが漏洩する可能性がある場合であっても、安全性を保つことができる。

[0061] つまり、実施の形態１に係る暗号処理システム１０では、ユーザ秘密鍵ｋ*に、ユーザの属性情報と、その鍵の世代番号とを設定しておく。また、暗号

化データｃに、復号できる条件として、復号可能なユーザの属性情報の条件と、復号可能な鍵の世代番号の条件とをＡＮＤ条件で設定しておく。

また、実施の形態１に係る暗号処理システム１０では、ユーザ端末１００と暗号化データ記憶装置３００との間の処理を中継する暗号化データ管理装置２００を設置する。そして、ユーザ端末１００が暗号化データｃを取得する場合、暗号化データ管理装置２００が暗号化データ記憶装置３００から暗号化データｃを取得して、ユーザ端末１００へ送信する。この際、暗号化データ管理装置２００は、暗号化データｃを復号可能なユーザにユーザ秘密鍵ｋ＊を失効したユーザが含まれるか否かに応じて、暗号化データｃの世代番号を異なる値に設定し直す。具体的には、失効したユーザが含まれない場合には、世代番号の値に初期値を設定し、失効したユーザが含まれる場合には、世代番号の値に失効していない世代番号の値を設定する。

これにより、実施の形態１に係る暗号処理システム１０は、暗号化データｃの再暗号化をすることなく、紛失したユーザ秘密鍵ｋ＊では暗号化データｃを復号できず、再生成されたユーザ秘密鍵ｋ＊では暗号化データｃを復号できる状態とする。

[0062] なお、上記説明では、式５に示すようにユーザ秘密鍵ｋ＊を生成するとした。つまり、鍵情報と属性情報とに、異なる乱数値ひぃ σ$_2$を乗じていた。しかし、式２１に示すように、鍵情報と属性情報とに同一の乱数値σを乗じて、ユーザ秘密鍵ｋ＊を生成してもよい。

＜式２１＞

$$k^* = \sigma (v\ ,b^*\ ,+ v_2 b^*_2 + v_3 b^*_3 + v_4 b^*_4) + b^*_5$$

[0063] また、上記説明では、式７に示すように暗号化データｃの要素ｃ ,を生成するとした。つまり、鍵情報と属性情報とに、異なる乱数値ω ,, ω$_2$を乗じていた。しかし、式２２に示すように、鍵情報と属性情報とに同一の乱数値ωを乗じて、要素ｃ ,を生成してもよい。

＜式２２＞

$$c\ ! := \omega (r_1 b_{1+} r_2 b_{2+} x_3 b_{3+} x_4 b_4) + \zeta b_{5+} 0\ b_6$$

[0064] また、式２３に示すように、乱数値ω ,を用いず、要素ｃ ,を生成してもよし。これは、ｒ ,, r_2自身が乱数値であり、さらに乱数値を掛けなくてもよいためである。

< 式２３ >

$Ci := ri\,bi + r_2 b_2 + \omega_2 (x_3 b_3 + x_4 b_4) + \zeta b_5 + \text{ø}\, b_6$

[0065] また、式２４に示すように、鍵情報を設定する一部の基底ベクトル (式２４ではb_1）の係数を０とし、要素ｃ ,を生成してもよい。これは、基底ベクトルb_1, b_2は、暗号化データ管理装置２００によって値を付け直しされるので、どちらか１つの基底ベクトルの係数に乱数値を設定しておけばよいためである。

< 式２４ >

$c' := r_2 b_2 + \omega_2 (x_3 b_3 + x_4 b_4) + \zeta b_5 + \text{ø}\, b_6$

[0066] また、式２５に示すように、鍵情報を設定する基底ベクトルに乱数値を設定せず、他の部分をドメイン公開鍵で暗号化して、要素ｃ ,を生成してもよい。鍵情報を設定する基底ベクトルに乱数値を設定することにより、ユーザ端末１００が暗号化データ記憶装置３００から直接暗号化データｃを取得した場合に、復号できない状態としていた。しかし、他の部分をドメイン公開鍵で暗号化しておくことで、同様の効果が得られるためである。

< 式２５ >

$c' := E(\omega_2 (x_3 b_3 + x_4 b_4) + \zeta b_5 + \text{ø}\, b_6)$

[0067] また、上記説明では、説明を簡単にするため、αが属性情報の値として設定されたユーザ秘密鍵ｋ*と暗号化データｃとを用いて説明した。

しかし、実際には、ユーザＵの所属するＡ会社を示す値α いＢ部を示す値α_2、Ｃ課を示す値α_3、ユーザＵを示すα_4が属性情報の値として設定されたユーザ秘密鍵ｋ*を用いることがある。例えば、式２６に示すユーザ秘密鍵ｋ*を用いることがある。なお、ここでは、世代番号の値として１を設定している。また、この場合、ｎ＝１０である。

< 式２６ >

$k^* = \sigma_1 (b^*_1 + b^*_2) + \sigma_2 (\alpha_1 b^*_3 + b^*_4 + \alpha_2 b^*_5 + b^*_6 + \alpha_3 b^*_7 + b^*_8 + \alpha_4 b^*_9 + b^*_{10}) + b^*_{11}$

また、A会社のB部に所属するユーザであれば誰でも復号可能であるように、A会社を示す値α_1、B部を示す値α_2が属性情報の値として設定された暗号化データcを用いることがある。例えば、式27に示す暗号化データcを用いることがある。

<式27>

$c' := \omega' (r_1 b_1 + r_2 b_2) + \omega_2 (b_3 - \alpha_1 b_4 + b_5 - \alpha_2 b_6) + \zeta b_{11} + \phi b_{12}$

[0068] ユーザリストuIに含まれるユーザの識別情報が失効情報に含まれている場合、式28に示すように、要素c_1'は生成される。

<式28>

$c' := \omega' (b' b_2) + \omega_2 (b_3 - \alpha_1 b_4 + b_5 - \alpha_2 b_6) + \zeta b_{11} + \phi b_{12}$

この場合、$v_1 = 1$, $v_2 = 1$, $v_3 = \alpha_1$, $v_4 = 1$, $v_5 = \alpha_2$, $v_6 = 1$, $v_7 = \alpha_3$, $v_8 = 1$, $v_9 = \alpha_4$, $v_{10} = 1$であり、$\chi_1 = 1$, $\chi_2 = -1$, $\chi_3 = 1$, $\chi_4 = -\alpha_1$, $\chi_5 = 1$, $\chi_6 = -\alpha_2$, $\chi_7 = 0$, $\chi_8 = 0$, $\chi_9 = 0$, $\chi_{10} = 0$であるから、$\Sigma_{i=1}^{1} v_i' \chi_i = \sigma_1 \omega_1 (1-1) + \sigma_2 \omega_2 (\alpha_1 - \alpha_1 + \alpha_2 - \alpha_2 + 0 + 0 + 0 + 0) = 0$となる。したがって、S26で抽出されたメッセージm'は、S11で暗号化データcの要素c_2に設定されたメッセージmと等しい。

[0069] 一方、ユーザリストuIに含まれるユーザの識別情報が失効情報に含まれている場合、式29に示すように、要素c_1'は生成される。ここでは、世代番号がの値が1のユーザ秘密鍵k*が失効していたとする。

<式29>

$c' := \omega' (D' - 2 b_2) + \omega_2 (b_3 - \alpha_1 b_4 + b_5 - \alpha_2 b_6) + \zeta b_{11} + \phi b_{12}$

なお、B部に所属する1人のユーザU'がユーザ秘密鍵k*を紛失すると、

B部に所属する他のユーザU_2が暗号化データcを取得する場合にも、要素c,は式28に示す要素cパではなく、式29に示す要素C_I'に変換される。したがって、ユーザU_1だけでなく、ユーザU_2等のB部に所属する他のユーザもユーザ秘密鍵k*を再作成してもらわなければ、暗号化データcを復号することはできなくなる。

[0070] 実施の形態2.

実施の形態2では、非特許文献2に記載された関数型暗号方式において、秘密鍵の失効方式を実現する方法を説明する。

[0071] まず、非特許文献2に記載された関数型暗号方式について、この実施の形態の説明に必要な部分のみに簡略化して説明する。特に、非特許文献2に記載された関数型暗号方式で用いられるスパンプログラムや秘密分散等については、省略、あるいは簡略化して説明する。

非特許文献2に記載された関数型暗号方式には、非特許文献1に記載された関数型暗号方式と同様に、Setupアルゴリズム、KeyGenアルゴリズム、Encアルゴリズム、Decアルゴリズムがある。

[0072] Setupアルゴリズムは、公開パラメータpkとマスター秘密鍵skとを生成するアルゴリズムである。

Setupアルゴリズムでは、双対ペアリングベクトル空間のパラメータparamと、t=0,...,d(dは1以上の整数)の各tについての正規直交基底である基底B_t及び基底B^*_tとが生成される。そして、パラメータparamと基底B_tとが公開パラメータpkとされ、基底B^*_tがマスター秘密鍵skとされる。

なお、基底B_0は、基底ベクトル$b_{0,1}$,い$b_{0,2}$,...,$b_{0,5}$を有し、基底B^*_0は、基底ベクトル$b^*_{0,1}$,$b^*_{0,2}$,...,$b^*_{0,5}$を有する。つまり、基底B_0,B^*_0は、それぞれ5個の基底ベクトルを有する。また、t=1,...,dの各tについての基底B_tは、基底ベクトルレ$b_{t,1}$,レ$b_{t,2}$,...,$b_{t,3nt+1}$を有し、基底B^*_tは、基底ベクトル$b^*_{t,1}$,い$b^*_{t,2}$,...,$b^*_{t,3nt+1}$を有する。つまり、基底B_t,B^*_tは、それぞれ3nt+1

個 (ｎｔは１以上の整数）の基底ベクトルを有する。

但し、厳密には、係数として必ず０が割り当てられる基底ベクトルは公開パラメータｐｋやマスター秘密鍵ｓｋに含める必要がない。そのため、公開パラメータｐｋに含める基底Ｂ。は、基底ベクトルb_{0}，い $b_{0,3}$，$b_{0,5}$のみを有し、マスター秘密鍵ｓｋに含める基底B^{*}_{0}は、基底ベクトルb^{*}_{0}，い $b^{*}_{o,3}$，$b^{*}_{0,4}$のみを有するとしてもよい。また、ｔ＝１，．．．，ｄの各ｔについて、公開パラメータｐｋに含める基底B_{t}は、基底ベクトルb_{t}，，，．．．，$b_{t,nt}$，$b_{t,3nt+1}$のみを有し、マスター秘密鍵ｓｋに含める基底B^{*}_{t}は、基底ベクトルb^{*}_{t}，レ．．．，$b^{*}_{t,nt+1}$，$b^{*}_{t,2nt+1}$，．．．，$b^{*}_{t,3nt}$のみを有するとしてもよい。

[0073] ＫｅｙＧｅｎアルゴリズムは、ユーザ秘密鍵ｋ＊を生成するアルゴリズムである。

ＫｅｙＧｅｎアルゴリズムでは、式３０に示すように、マスター秘密鍵ｓｋに含まれる基底B^{*}_{t}を用いて、要素k^{*}_{0}と、ｔ＝１，．．．，ｄの各ｔについての要素k^{*}_{t}とを有するユーザ秘密鍵ｋ＊が生成される。

＜式３０＞

$k^{*}_{0} := (8, 0, 1, \phi 0, 0) B^{*}o$

$k^{*}_{t} := (\delta \vec{v}_{t}, 0^{nt}, 0\rightarrow_{t}, 0) B^{*}_{t}$

ここで、δ，ϕ_{O}，$0\rightarrow t := 0t,i, \ldots, \phi_{t,nt}$は、乱数値である。$\vec{v}t := v_{t,1}, \ldots, v_{t,nt}$は、ユーザ秘密鍵ｋ＊が与えられるユーザの属性情報等である。

また、（ｚい．．．，z_{N}）$B^{*}_{t} := \Sigma_{i=1}{}^{N} z_{i} b^{*}_{t}$，;である。つまり、$k^{*}_{0} := \{8, 0, 1, \phi o, 0) B^{*}_{O} := \delta b^{*}_{0,1} + b^{*}_{0,3} + 0_{o} b^{*}_{o,4}$である。また、$k^{*}_{t} := (\delta \vec{v}_{t}, 0^{nt}, 0\rightarrow_{t}, 0) B^{*}_{t} := \Sigma i_{=1}{}^{nt} \delta v_{t,i} b^{*}_{t,i} + \Sigma_{i=1}{}^{nt} \phi_{t,i} b^{*}_{t,2nt+i}$である。

[0074] Ｅｎｃアルゴリズムは、暗号化データｃを生成するアルゴリズムである。

Ｅｎｃアルゴリズムでは、式３１に示すように、公開パラメータｐｋに含まれる基底Ｂを用いて、暗号化データｃの要素ｃ。と、ｔ＝１，．．．，Ｌ（

Lは、d以下の整数）の各tについての要素c_tとが生成される。

<式3 1>

$c_0 := (-s_0, 0, \zeta, 0, \eta_0) B_0$

$c_t := (s_t \vec{e}_{t,1} + \Theta_t \vec{x}_t, 0^{nt}, 0^{nt}, \eta_t) B_t$

ここで、$\vec{e}_{t,}$,は、nt個の要素を持ち、先頭要素が1で残りの要素が0であるベクトルである。また、$s_0 = \Sigma_{i=1}^{L} s_i$である。$\zeta$, Θ_t, η_o, η_tは、乱数値である。x_t, ,,. . . ,$x_{t,nt}$は、暗号化データcを復号可能なユーザの属性情報等である。

また、 (z い . . . ,z_N) B_t :=$\Sigma_{i=}$に$z_i b_{t,i}$である。つまり、co := (-so, 0, ζ, 0, 刀。) B_0 := _ $s_o b_o$, ,+ $\zeta b_{o,3} + \eta_o b_{o,5}$である。また、$c_t := (s_t \vec{e}_{t,1} + \theta_t \vec{X}_t, O^{nt}, O^{nt}, \eta_t) B_t$:= $\Sigma_{i=1}^{nt} (s_t \vec{e}_{t,1} + \Theta_t x_{t,i}) b_{t,i} + \eta_t b_{3nt+1}$である。

[0075] また、Encアルゴリズムでは、式3 2に示すように、公開パラメータpkに含まれるパラメータparamを用いて、暗号化データcの要素c_{d+1}が生成される。

<式3 2>

$c_{d+i} := e(g, g)^{\iota} m$

ここで、gは、パラメータparamに含まれる情報であり、双対ペアリングベクトル空間を構成する群Gの要素である。mは、メッセージである。e（g，g）は、要素gと要素gとについてのペアリング演算である。

[0076] Decアルゴリズムは、暗号化データcをユーザ秘密鍵k*で復号するアルゴリズムである。

Decアルゴリズムでは、式3 3に示す計算が実行され、暗号化データcがユーザ秘密鍵k*で復号されて、m' が抽出される。

<式3 3>

$m' := c_{d+} iZ (e(c_o, k^*_0) - \Pi_{t=1}^{L} e(c_t, k^*_t))$

ここで、e（c_0，k^*_0）は、要素c。とユーザ秘密鍵k^*_0とについてのペアリング演算であり、e（C_t，k^*_t）は、要素c_tとユーザ秘密鍵kつとに

ついてのペアリング演算である。

[0077] Ｄｅｃアルゴリズムでは、ｔ＝１，．．．，Ｌの各ｔについて、ユーザ秘密鍵ｋ*における要素ｋ*$_t$に設定された属性情報等（$v\vec{}_t$）と、暗号化データｃにおける要素ｃ$_t$に設定された属性情報等（$x\vec{}_t$）とが対応する場合、抽出されたｍ'＝ｍとなる。

属性情報等（$v\vec{}_t$）と属性情報等（$x\vec{}_t$）とが対応するとは、$v\vec{}_t \cdot x\vec{}_t = \sum_{i=1}^{n_t} v_{t,i} \cdot x_{t,i} = 0$となることである。

[0078] ペアリング演算ｅ（ｓｇ，ｔｇ）＝ｅ（ｇ，ｇ）stである。そのため、ｅ（ｃ$_0$，ｋ*$_0$）＝ｅ（ｇ，ｇ）^{Y1}となる。ここで、Ｙ１＝_ｓ$_0$＋《である。また、$\prod_{t=1}^{L}$ｅ（ｃ$_t$，ｋ*$_t$）＝（ｇ，ｇ）^{Y2}となる。ここで、$Y2 = \sum_{i=1}^{L}(s_i + v\vec{}_t - x\vec{}_t) = \sum_{i=1}^{L}(S_i) + \sum_{i=1}^{L} v\vec{}_i \cdot \chi\vec{}_i$である。したがって、$\sum_{i=1}^{L} v\vec{}_i \cdot x\vec{}_i = 0$であれば、$Y2 = \sum_{i=1}^{L}(S_i)$である。

そして、ｅ（ｃｏ，ｋ*ｏ）・$\prod_{t=1}^{L}$ｅ（ｃ$_t$，ｋ*$_t$）＝ｅ（ｇ，ｇ）^{Y3}となり、$\sum_{i=1}^{L} v\vec{}_i \cdot x\vec{}_i = 0$であれば、Ｙ３＝_ｓ$_o$＋《＋$\sum_{i=1}^{L}(s_i)$である。そして、上述した通り、ｓ$_o$＝$\sum_{i=1}^{L} s_i$であるから、Ｙ３＝《である。つまり、ｅ（ｃ$_o$，ｋ*ｏ）・$\prod_{t=1}^{L}$ｅ（ｃ$_t$，ｋ*$_t$）＝ｅ（ｇ，ｇ）$^{\zeta}$である。

式３２に示すように、$c_{d+1} = e(g,g)^{m}$であるから、式３３の計算を実行すれば、$\sum_{i=1}^{L} v\vec{}_i \cdot x\vec{}_i = 0$の場合には、ｍ'＝ｍとなる。

[0079] 以下の説明では、説明を簡単にするため、ｄ＝２，Ｌ＝２とし、ｎ１＝２，ｎ２＝２として説明する。

[0080] 実施の形態２に係る暗号処理システム１０の構成は、図１に示す実施の形態１に係る暗号処理システム１０の構成と同じである。実施の形態２に係るユーザ端末１００、暗号化データ管理装置２００、暗号化データ記憶装置３００、鍵生成装置４００の構成は、図２_５に示す実施の形態１に係るユーザ端末１００、暗号化データ管理装置２００、暗号化データ記憶装置３００、鍵生成装置４００の構成と同じである。

[0081] 実施の形態２に係る暗号処理システム１０の主な処理には、実施の形態１

に係る暗号処理システム１０と同様に、暗号化データ登録処理と、暗号化データ取得処理とがあり、暗号化データ登録処理と暗号化データ取得処理とには、３つの前提条件がある。

[0082] ３つの前提条件は、前提条件１において生成されるユーザ秘密鍵ｋ＊の構成を除き、実施の形態１と同じである。

[0083] ここでは、鍵生成部４２０は、式３４に示すようにユーザ秘密鍵ｋ＊を生成する。

＜式３４＞

$k^*_0 := (8, 0, 1, \phi 0, 0) B^*o$

$k^*_1 := (\delta v^{\rightarrow}_1, 0^{\eta 1}, \phi^{\rightarrow}_1, 0) B^*_1$

$k^*_2 := (\delta v^{\rightarrow}_2, 0^{\eta 2}, \phi^{\rightarrow}_2, 0) B^*_2$

ここで、δ，０o，$\Phi^{\rightarrow}_1$，$0^{\rightarrow}_2$は、乱数値である。$ソ^{\rightarrow}_1 := ソし_1, V_{1,2}$は、鍵情報である。ここでは実施の形態１と同様に、鍵情報として、新たな鍵の発行毎に値がインクリメントされる世代番号を用いる。$v^{\rightarrow}_2 := V_2$，，，$v_{2,2}$は、ユーザ秘密鍵ｋ＊が与えられるユーザの属性情報等である。

世代番号の値をＰとし、属性情報の値をａとした場合、ここでは、式３５に示すようにユーザ秘密鍵ｋ＊は生成される。

＜式３５＞

$k^*_0 := (\delta, 0, 1, \Phi_0, 0) B^*_0$

$k^*_1 := (\delta (P, 1), o^{\eta 1}, 0^{\rightarrow}_1, 0) B^*_1$

$k^*_2 := (\delta (\alpha, 1), o^{\eta 2}, 0^{\rightarrow}_2, 0) B^*_2$

つまり、$v_{1,1} = P$，$v_{1,2} := 1$，$v_{2,1} := ¼$，$V_{2,2} := 1$である。

[0084] ＜暗号化データ登録処理＞

図６を用いて、実施の形態２に係る暗号化データ登録処理について、実施の形態１に係る暗号化データ登録処理と異なる部分を中心に説明する。

（Ｓ１１：暗号化処理）

ユーザ端末１００の暗号化データ生成部１１０は、Ｅｎｃアルゴリズムを

実行して暗号化データcを生成する。

[0085] ここでは、暗号化データ生成部１１０は、処理装置により、式３６に示すように、鍵管理部１５０に記憶した公開パラメータpkに含まれる基底Bを用いて、暗号化データcの要素c_0，c_1，c_2を生成する。

<式３６>

$c_0 := (-s_0, 0, \zeta, 0, \eta_0) B_0$

$c_1 := (s_1 e^{\rightarrow}_1, \theta_1(1, r), 0^{\eta 1}, 0^{\eta 1}, \eta_1) B_1$

$c_2 := (s_2 e^{\rightarrow}_{2,1} + \theta_2 x^{\rightarrow}_{2,\circ}, 0^{\eta 2}, 0^{\eta 2}, \eta_2) B_2$

ここで、$s_0 = s_1 + s_2$である。ζ，θ_1，θ_2，v_0，η_1，η_2，rは、乱数値である。$\chi_{2,1}$，，$\chi_{2,2}$は、暗号化データcを復号可能なユーザの属性情報等である。

属性情報の値をaとした場合、ここでは、式３７に示すように暗号化データcは生成される。

<式３７>

$c_0 := (-s_0, 0, \zeta, 0, \eta_0) B_0$

$c_1 := (s_1 e^{\rightarrow}_1, \theta_1(1, r), 0^{\eta 1}, 0^{\eta 1}, \eta_1) B_1$

$c_2 := (s_2 e^{\rightarrow}_{2,1} + \theta_2(1, -\alpha), 0^{\eta 2}, 0^{\eta 2}, \eta_2) B_2$

つまり、$\chi_{2,1} := 1$，$\chi_{2,2} := -\alpha$である。

[0086] また、暗号化データ生成部１１０は、処理装置により、式３８に示すように、鍵管理部１５０に記憶した公開パラメータpkに含まれるパラメータparamを用いて、暗号化データcの要素c_{d+1}を生成する。

<式３８>

$c_{d+1} := e(g, g)^{\zeta} \cdot m$

[0087] また、暗号化データ生成部１１０は、処理装置により、鍵管理部１５０に記憶したドメイン公開鍵dpにで、rを暗号化したE（r）と、θを暗号化したE（Θ_1）とを生成する。

また、暗号化データ生成部１１０は、要素c，に設定した属性情報が示すユーザの識別情報をユーザリストulとして生成する。

[0088] （Ｓ１２　:第１データ送信処理）

データ送信部１２０は、通信装置により、暗号化データ生成部１１０が生成した要素c_0，c_1，c_2，c_{d+1}，Ｅ（ｒ），Ｅ（ｒ），ｕｌを含む暗号化データｃを、暗号化データ管理装置２００へ送信する。

[0089] Ｓ１３からＳ１７までの処理は、実施の形態１と同じである。

[0090] ＜暗号化データ取得処理＞

図７を用いて、実施の形態２に係る暗号化データ取得処理について、実施の形態１に係る暗号化データ取得処理と異なる部分を中心に説明する。

Ｓ２１からＳ２４までの処理は、実施の形態１と同じである。

[0091] （Ｓ２５　:世代番号付け代え処理）

Ｓ２５も、原則として実施の形態１と同様である。しかし、暗号化データｃの要素ｃ　,における乱数値ｒを設定し直す方法が異なる。

具体的には、鍵情報設定部２３０は、以下のように乱数値ｒを設定し直す。なお、ここでは、式３７に示す要素ｃ　,における乱数値ｒを設定し直した要素c_1'を示す。

[0092] ユーザリストｕｌに含まれるユーザの識別情報が、失効情報管理部２５０が記憶する失効情報に含まれていない場合、鍵情報設定部２３０は、式３９に示すように、要素。パを生成する。

＜式３９＞

$$c_1' := (S_1 e_{\to 1,1} + \theta_1 (1, -1), \bigcirc_{n1}, \bigcirc_{n1}, \eta_1) B_1$$

つまり、ｒを_１に設定し直す。ｒを設定し直した－１は、_１Ｘ世代番号の初期値である。

なお、式４０に示す計算をすることにより、式３７に示す要素ｃ　,から式３９に示す要素ｃ；を得ることができる。

＜式４０＞

$$c_1' := c_i \_ \theta_{irbi,2} \_ \theta_{ibi,2}$$

ここで、ｒ，ん は、暗号化データｃの要素Ｅ（ｒ），Ｅ（Θ_1）を、鍵管理部２６０に記憶したドメイン秘密鍵ｄｓｋで復号することにより得られる

。また、ヒしぃ $b_{1,2}$ は、公開パラメータpkに含まれる基底Bから得られる。

[0093] ユーザリストulに含まれるユーザの識別情報が、失効情報管理部250が記憶する失効情報に含まれている場合、鍵情報設定部230は、式41に示すように、要素c ¦ を生成する。

< 式41 >

$$c_1' := (s\ !e^{\rightarrow}{}_1,\ !+\Theta\ !(1,-P_{;)},\ O^{n1},\ 0"^1,\ \eta_{;)}\ B_1$$

つまり、rを一ρ_1に設定し直す。rを設定し直した一p ,は、_1X（失効したユーザ秘密鍵k*の世代番号の値+1）である。つまり、ユーザリストulにユーザAが含まれており、失効したユーザAのユーザ秘密鍵k*の世代番号として1が失効リストに含まれている場合、－ρ_1は、—1X（1+1）=_2となる。

なお、式42に示す計算をすることにより、式37に示す要素c ,から式41に示す要素。パ を得ることができる。

< 式42 >

$$c_1' := Ci\_\theta i\ r\ bi,_2\_\theta i\ Pi\ bi,_2$$

[0094] S26は、実施の形態1と同じである。

[0095] S27も、原則として実施の形態1と同様である。しかし、復号の方法が異なる。

ここでは、復号部140は、処理装置により、式43に示す計算を実行することにより、暗号化データc'をユーザ秘密鍵k*で復号して、メッセージm'を抽出する。

< 式43 >

$$m' := c_{d+1}Z\ (e\ (co,\ k^*{}_0)\ -\Pi_{t=1}{}^{L}e\ (c_t,\ k^*{}_t))$$

[0096] 上述したように、t=1,...,Lの各tについて、ユーザ秘密鍵k*における要素$k^*{}_t$に設定された属性情報等（$v^{\rightarrow}{}_t$）と、暗号化データcにおける要素c_tに設定された属性情報等（$x^{\rightarrow}{}_t$）とが対応する場合、抽出されたm ,=mとなる。そして、ここでは、属性情報等（$v^{\rightarrow}{}_t$）と属性情報等（$x^{\rightarrow}{}_t$

) とが対応するとは、$\vec{v}_t \cdot \vec{x}_t = \sum_{i=int} v_{t,r} \cdot \chi_{t,i} = 0$ となることである。

[0097] ユーザ端末１００は、初めに生成され、世代番号の値として1が付されたユーザ秘密鍵k*を有しているとする。つまり、ユーザ端末１００は、式35のPに1が設定された、式44に示すユーザ秘密鍵k*を有しているとする。

< 式44 >

$k^*_0 := (8, 0, 1, \phi 0, 0)\ B^*_0$

$k^*_1 := (8\ (1, 1), 0\eta^1, \vec{\phi}_1, 0)\ B^*_1$

$k^*_2 := (\delta\ (a, 1), 0\eta^2, 0\vec{}_2, 0)\ B^*_2$

また、Ｓ１１において、暗号化データcの要素c ,は、式45 (= 式37)に示すように生成されているとする。

< 式45 >

$c_0 := (-s0, 0, \zeta, 0, \eta 0)\ B_0$

$c_! := (s_! e\vec{}_1, !+\theta_!(1, r), O''^1, O\eta^1, \eta_1)\ B_1$

$c_2 := (s_2 e\vec{}_{2,1} + \theta 2\ (1, -\alpha), 0\eta^2, 0\eta^2, \eta_2)\ B_2$

[0098] ユーザリストuIに含まれるユーザの識別情報が失効情報に含まれていない場合、式46 (= 式39)に示すように、要素c_1'は生成される。

< 式46 >

$c_1' := (s_! e\vec{}_1, !+\Theta_!(1, -1), O''^1, 0''^1, \eta_1)\ B_1$

この場合、ユーザ秘密鍵k*において、基底B* ,の基底ベクトルb*しいb*し2の係数に設定されたVしいv ,,2は、ソし ,二し Vし2= 1である。また、要素c1' において、基底B ,の基底ベクトルbしいb1,2の係数に設定されたXしいx1,2は、乂し ,二し Xし2= _ 1である。そのため、$\vec{v}_1 - \vec{x}_1 = \sum_{i=1}^{2} v_{I,i} \cdot x_{I,i} = 1 - 1 = 0$ となる。また、ユーザ秘密鍵k*において、基底B*2の基底ベクトルb*2,いb*2,2の係数に設定されたV2,1, V2,2は、V2,1= ℄, V2,2= 1でめる。また、要素C ! におして、基底B2の基底ベクトルb2,1, b2,2の係数に設定されたx2,1? x2,2まX2,1= 1, X2,2= −αである。そのにめ、$\vec{v}_2 - \vec{x}_2 = \sum_{i=1}^{2} v_{2,i}$

・$x_{2,i} = \alpha\_\alpha = 0$ となる。したがって、Ｓ２６で抽出されたメッセージm' は、Ｓ１１で暗号化データc の要素c_{d+1}に設定されたメッセージm と等しい。

つまり、ユーザ秘密鍵k * で、暗号化データc を復号することができる。

[0099] 一方、ユーザリストu l に含まれるユーザの識別情報が失効情報に含まれている場合、式４７に示すように、要素c_1' は生成される。ここでは、世代番号がの値が１のユーザ秘密鍵k * が失効していたとする。

< 式４７ >

$c_1' := (s\ !e^{\rightarrow}_1, !+\Theta !(1, -2), O"^1, 0"^1, \eta_1) B_1$

この場合、ソし 1= １，ｖし$_2$= １であり、$x_{1,l}$＝１，$x_{1,2}$＝—２であるから、$v^{\rightarrow}$,・$x^{\rightarrow}_1$ニ匚ぃノソし ;・$x_{l,i}$＝１_２≠０となる。したがって、Ｓ２６で抽出されたメッセージm' は、Ｓ１１で暗号化データc の要素c_{d+1}に設定されたメッセージm と等しくない。

つまり、失効しているユーザ秘密鍵k * では、暗号化データc を復号することはできない。

[0100] しかし、ユーザ端末１００は、鍵生成装置４００にユーザ秘密鍵k * を再生成してもらい、世代番号の値として２が付されたユーザ秘密鍵k * を取得したとする。つまり、ユーザ端末１００は、式３５のp に２が設定された、式４８に示すユーザ秘密鍵k * を取得したとする。

< 式４８ >

$k^*_0 := (8, 0, 1, \phi 0, 0)\ B^*_0$

$k^*_1 := (\delta (2, 1), 0\eta^1, 0^{\rightarrow}_1, 0)\ B^*_1$

$k^*_2 := (8 (a, 1), 0"_2, 0^{\rightarrow}_2, 0)\ B^*_2$

この場合、ｖ】,i＝２，ｖし$_2$＝１であり、$x_{1,l}$＝１，$x_{1,2}$＝—２であるから、$v^{\rightarrow}$,・$x^{\rightarrow}_1 = \Sigma_{i=1}{}^2 v_{1,}$;・x】,i＝２—２＝０となる。また、$v^{\rightarrow}_2 \cdot x^{\rightarrow}_2 = \Sigma_{i=1}{}^2 v_{2,i} \cdot x_{2,i} = \alpha\_\alpha = 0$ である。したがって、Ｓ２６で抽出されたメッセージm' は、Ｓ１１で暗号化データc の要素c_{d+1}に設定されたメッセージm と等しい。

つまり、ユーザ秘密鍵k^*を紛失した場合、ユーザ秘密鍵k^*を再生成してもらうことで、暗号化データcの復号が可能となる。

[0101] また、ユーザ端末100が、暗号化データ管理装置200を介すことなく、暗号化データ記憶装置300から暗号化データcを取得することも考えられる。しかし、この場合、暗号化データcの要素$c_{,}$は、式49(=式37)に示す通りである。

<式49>

$$c_{,} := (s_{,}\vec{e}_1, +\Theta_{,}(1, r), \sigma_1, \eta_1)B_1$$

この場合、乱数値rが用いられているため、ユーザ秘密鍵k^*に設定された世代番号の値がいくつであっても、$\Sigma_{i=1}^{2} v_{1,i} \cdot x_{1,i} \neq 0$となり、復号できない。

[0102] 以上のように、実施の形態2に係る暗号処理システム10では、実施の形態1に係る暗号処理システム10と同様の効果を得ることができる。

[0103] なお、上記説明では、式36に示すように暗号化データcの要素$c_{,}$を生成するとした。しかし、式50に示すように、乱数値$\theta_{,}$を用いず、要素$c_{,}$を生成してもよい。これは、r自身が乱数値であり、さらに乱数値を掛けなくてもよいためである。

<式50>

$$c_{,} := (s_{,}\vec{e}_1, +(1, r), \sigma_1, \eta_1)B_1$$

[0104] また、式51に示すように、鍵情報を設定する基底ベクトルに乱数値を設定せず、要素c_I全体をドメイン公開鍵で暗号化して、要素c_Iを生成してもよい。鍵情報を設定する基底ベクトルに乱数値を設定することにより、ユーザ端末100が暗号化データ記憶装置300から直接暗号化データcを取得した場合に、復号できない状態としていた。しかし、他の部分をドメイン公開鍵で暗号化しておくことで、同様の効果が得られるためである。

<式51>

$$c_{,} := E(s_{,}\vec{e}_1, {}_1, \sigma_1, 0, \eta_{,})B_1$$

[0105] 実施の形態3.

実施の形態１では、暗号化データｃの要素c_1における鍵情報が設定される基底ベクトルに乱数値ｒいr_2を設定すること等により、ユーザ端末１００が直接暗号化データ記憶装置３００から暗号化データｃを取得した場合の安全性を保っていた。同様に、実施の形態２では、暗号化データｃの要素ｃ,における鍵情報が設定される基底に乱数値ｒを設定すること等により、ユーザ端末１００が直接暗号化データ記憶装置３００から暗号化データｃを取得した場合の安全性を保っていた。

実施の形態３では、暗号化データｃの設定を簡略化しつつ、暗号化データ記憶装置３００へのアクセス制御を行うことにより、ユーザ端末１００が直接暗号化データ記憶装置３００から暗号化データｃを取得しようとした場合の安全性を保つ方法について説明する。

実施の形態３では、実施の形態１に係る処理を応用した場合について説明するが、実施の形態２に係る処理を応用した場合についても同様に実現可能である。

[01 06] 暗号処理システム１０の構成は、図１に示す実施の形態１に係る暗号処理システム１０の構成と同じである。ユーザ端末１００、鍵生成装置４００の構成は、図２，５に示す実施の形態１に係るユーザ端末１００、鍵生成装置４００の構成と同じである。

[01 07] 図８は、実施の形態３に係る暗号化データ管理装置２００の構成図である。

実施の形態３に係る暗号化データ管理装置２００は、図３に示す実施の形態１に係る暗号化データ管理装置２００の機能に加え、認証処理部２７０を備える。

[01 08] 図９は、実施の形態３に係る暗号化データ記憶装置３００の構成図である。

実施の形態３に係る暗号化データ記憶装置３００は、図４に示す実施の形態１に係る暗号化データ記憶装置３００の機能に加え、認証処理部３５０を備える。

[01 09] 3つの前提条件については、原則として実施の形態1と同じである。

但し、実施の形態1では公開パラメータpkに含まれていた基底Bの基底ベクトルbい b_2は、公開パラメータpkから除かれ、鍵生成装置400から暗号化データ管理装置200へのみ送信される。なお、この際、盗聴と改ざんを防ぐため、SSL等を用いた安全な通信路が使用される。

[01 10] <暗号化データ登録処理>

図10は、実施の形態3に係る暗号化データ登録処理の流れを示すフローチャートである。

(S31:暗号化処理)

ユーザ端末100の暗号化データ生成部110は、図6のS11と同様に、Encアルゴリズムを実行して暗号化データcを生成する。

[01 11] ここでは、暗号化データ生成部110は、処理装置により、式52に示すように暗号化データcの要素c,を生成する。

<式52>

$c_! := \omega(x_3 b_3 + x_4 b_4) + \zeta b_5 + \phi b_6$

ここで、ω, ζ, φは、乱数値である。χ_3, χ_4は、暗号化データcを復号可能なユーザの属性情報が設定される。

属性情報の値をaとした場合、ここでは、式53に示すように暗号化データcは生成される。

<式53>

$c_! := \omega(b_3 - \alpha b_4) + \zeta b_5 + \phi b_6$

つまり、$\chi_3 := 1$, $\chi_4 := -\alpha$である。

[01 12] 暗号化データ生成部110は、要素c2, E(ω_1 r_1), E(ω_1 r_2), ulについても、図6のS11と同様に生成する。

[01 13] (S32:第1認証情報送信処理)

ユーザ端末100のデータ送信部120は、通信装置により、認証情報として、ユーザの識別情報とパスワードとを暗号化データ管理装置200へ送信する。

[01 14] （Ｓ３３ :第１認証処理）

暗号化データ管理装置２００のデータ受信部２１０は、通信装置により、ユーザの識別情報とパスワードとをユーザ端末１００から受信する。

すると、暗号化データ管理装置２００の認証処理部２７０は、ユーザの識別情報とパスワードとに基づき、ユーザの認証を行う。例えば、認証処理部２７０は、ユーザ毎に識別情報とパスワードとを予め記憶しておき、受信した識別情報及びパスワードと、記憶された識別情報及びパスワードとが一致するか否かにより認証する。認証処理部２７０は、認証に成功した場合、処理をＳ３４へ進め、認証に失敗した場合、処理を終了する。

（Ｓ３４ :第１データ送信処理）

ユーザ端末１００のデータ送信部１２０は、図６のＳ１２と同様に、暗号化データｃを暗号化データ管理装置２００へ送信する。

[01 15] （Ｓ３５ :第２認証情報送信処理）

暗号化データ管理装置２００のデータ受信部２１０は、通信装置により、暗号化データｃをユーザ端末１００から受信する。すると、データ送信部２４０は、認証情報として、暗号化データ管理装置２００の識別情報とパスワードとを暗号化データ記憶装置３００へ送信する。

[01 16] （Ｓ３６ :第２認証処理）

暗号化データ記憶装置３００のデータ受信部３１０は、通信装置により、暗号化データ管理装置２００の識別情報とパスワードとをユーザ端末１００から受信する。

すると、暗号化データ記憶装置３００の認証処理部３５０は、暗号化データ管理装置２００の識別情報とパスワードとに基づき認証処理を行う。例えば、認証処理部３５０は、暗号化データ管理装置２００の識別情報とパスワードとを予め記憶しておき、受信した識別情報及びパスワードと、記憶された識別情報及び/《スワードとが一致するか否かにより認証する。認証処理部３５０は、認証に成功した場合、処理をＳ３７へ進め、認証に失敗した場合、処理を終了する。

[01 17] （Ｓ３７ :第２データ送信処理）

暗号化データ管理装置２００のデータ送信部２４０は、暗号化データｃに関連情報ｒを添付して、暗号化データ記憶装置３００へ送信する。

[01 18] Ｓ３８からＳ４１までの処理は、図６に示すＳ１４からＳ１７までの処理と同じである。

[01 19] < 暗号化データ取得処理>

図１１は、実施の形態３に係る暗号化データ取得処理の流れを示すフローチャートである。

（Ｓ５１ :第１認証情報送信処理）

ユーザ端末１００のデータ送信部１２０は、通信装置により、認証情報として、ユーザの識別情報とパスワードとを暗号化データ管理装置２００へ送信する。

[01 20] （Ｓ５２ :第１認証処理）

暗号化データ管理装置２００のデータ受信部２１０は、通信装置により、ユーザの識別情報とパスワードとをユーザ端末１００から受信する。

すると、暗号化データ管理装置２００の認証処理部２７０は、ユーザの識別情報とパスワードとに基づき、ユーザの認証を行う。例えば、認証処理部２７０は、Ｓ３３と同じ方法により認証を行う。認証処理部２７０は、認証に成功した場合、処理をＳ５３へ進め、認証に失敗した場合、処理を終了する。

[01 21] （Ｓ５３ :キーワード送信処理）

ユーザ端末１００のデータ送信部１２０は、通信装置により、暗号化データｃを特定可能なキーワードを、暗号化データ管理装置２００へ送信する。

[01 22] （Ｓ５４ :第２認証情報送信処理）

暗号化データ管理装置２００のデータ受信部２１０は、通信装置により、キーワードをユーザ端末１００から受信する。すると、データ送信部２４０は、認証情報として、暗号化データ管理装置２００の識別情報とパスワードとを暗号化データ記憶装置３００へ送信する。

[01 23] （Ｓ５５：第２認証処理）

暗号化データ記憶装置３００のデータ受信部３１０は、通信装置により、暗号化データ管理装置２００の識別情報とパスワードとをユーザ端末１００から受信する。

すると、暗号化データ記憶装置３００の認証処理部３５０は、暗号化データ管理装置２００の識別情報とパスワードとに基づき認証処理を行う。例えば、認証処理部３５０は、Ｓ３６と同じ方法より認証する。認証処理部３５０は、認証に成功した場合、処理をＳ５６へ進め、認証に失敗した場合、処理を終了する。

[01 24] （Ｓ５６：キーワード転送処理）

暗号化データ管理装置２００のデータ送信部２４０は、通信装置により、キーワードを暗号化データ記憶装置３００へ送信する。

[01 25] Ｓ５７からＳ５８までの処理は、図７に示すＳ２３からＳ２４までの処理と同じである。

[01 26] （Ｓ５９：権限判定処理）

暗号化データ管理装置２００のデータ受信部２１０は、通信装置により、暗号化データｃを暗号化データ記憶装置３００から受信する。

すると、暗号化データ管理装置２００の認証処理部２７０は、処理装置により、Ｓ５２で受信したユーザの識別情報が、暗号化データｃのユーザリストｕｌに含まれているか否かを判定する。認証処理部２７０は、含まれている場合、処理をＳ６０へ進め、含まれていない場合、処理を終了する。

[01 27] （Ｓ６０：世代番号付け代え処理）

暗号化データ管理装置２００の失効判定部２２０は、処理装置により、暗号化データｃのユーザリストｕｌに含まれるユーザの識別情報が、失効情報管理部２５０が記憶する失効情報に含まれているか否か判定する。鍵情報設定部２３０は、処理装置により、暗号化データｃの要素c_lに、失効判定部２２０の判定結果に応じて異なる値に設定し、要素c_l'を生成する。

具体的には、鍵情報設定部２３０は、以下のように要素c_lに値を設定する

。なお、ここでは、式５３に示す要素ｃ，に値を設定した要素ｃ，'を示す。

[0128] ユーザリストｕｌに含まれるユーザの識別情報が、失効情報管理部２５０が記憶する失効情報に含まれていない場合、鍵情報設定部２３０は、式５４（＝式１０）に示すように、要素C_l'を生成する。

＜式５４＞

$$c_l' := \omega_1(b_1 - b_2) + \omega_2(b_3 - \alpha b_4) + \zeta b_5 + \phi b_6$$

つまり、基底ベクトルｂ，の係数に１を設定し、基底ベクトルb_2の係数に－１を設定する。基底ベクトルb_2の係数に設定し直した—１は、＿１Ｘ世代番号の初期値である。

[0129] なお、式５５に示す計算をすることにより、式５３に示す要素ｃ，から式５４に示す要素c_1'を得ることができる。

＜式５５＞

$$c_l' := c_l + (\omega_1 b_1 - \omega_1 b_2)$$

[0130] ユーザリストｕｌに含まれるユーザの識別情報が、失効情報管理部２５０が記憶する失効情報に含まれている場合、鍵情報設定部２３０は、式５６（＝式１２）に示すように、要素C_l'を生成する。

＜式５６＞

$$c_l' := \omega_1(b_1 - p_1 b_2) + \omega_2(b_3 - \alpha b_4) + \zeta b_5 + \phi b_6$$

つまり、基底ベクトルｂ，の係数に１を設定し、基底ベクトルb_2の係数に$-\rho_1$を設定する。基底ベクトルb_2の係数に設定した—ｐ，は、—１Ｘ（失効したユーザ秘密鍵ｋ＊の世代番号の値＋１）である。

なお、式５７に示す計算をすることにより、式５３に示す要素ｃ，から式５６に示す要素ｃ，'を得ることができる。

＜式５７＞

$$c_l' := c_l + (\omega_1 b_1 - \omega_1 p_1 b_2)$$

[0131] Ｓ６１からＳ６２までの処理は、図７に示すＳ２６からＳ２７までの処理と同じである。

[0132] 以上のように、実施の形態３に係る暗号処理システム１０は、暗号化デー

タ管理装置２００と暗号化データ記憶装置３００とでそれぞれ認証を行う。これにより、ユーザ端末１００により直接暗号化データ記憶装置３００から暗号化データｃを取得されることを防止できる。そのため、暗号化データｃに乱数値を設定する等せずに、安全性を保つことができる。

[01 33] また、実施の形態３に係る暗号処理システム１０は、暗号化データ登録処理において、不正なデータを暗号化データ記憶装置３００に登録されることを防止できる。

[01 34] なお、上記説明では、暗号化データ管理装置２００と暗号化データ記憶装置３００とでそれぞれ認証を行った。しかし、暗号化データ管理装置２００では認証を行わず、暗号化データ記憶装置３００だけが認証を行うようにしてもよい。少なくとも暗号化データ記憶装置３００が認証を行うことで、ユーザ端末１００により直接暗号化データ記憶装置３００から暗号化データｃを取得されることや、不正なデータを暗号化データ記憶装置３００に登録されることを防止できる。

[01 35] また、上記説明では、実施の形態１に係る処理を応用した場合について説明した。実施の形態２に係る処理を応用した場合、処理の流れは実施の形態１に係る処理を応用した場合と同じである。しかし、Ｓ３１で生成される要素いと、Ｓ６０で生成される要素ｃ，'とが、実施の形態１に係る処理を応用した場合とは異なる。

実施の形態２に係る処理を応用した場合、Ｓ３１で生成される要素ｃ，は式５８のようになる。

< 式５８ >

$$c_1' := (s_1 e_1^{\rightarrow}, \text{い}\ O''^{1}, 0''^{1}, \eta_{;)}\ B_1$$

また、実施の形態２に係る処理を応用した場合、Ｓ６０で生成される要素c_1'は式３９や式４１のようになる。

また、実施の形態２では公開パラメータｐｋに含まれていた基底B_1は、公開パラメータｐｋから除かれ、鍵生成装置４００から暗号化データ管理装置２００へのみ送信される。なお、この際、盗聴と改ざんを防ぐため、ＳＳＬ

等を用いた安全な通信路が使用される。

[01 36] ここで、上記実施の形態におけるユーザ秘密鍵k*と暗号化データcとへの鍵情報や属性情報の割り当て方法は、一例であり他の方法であつてもよい。

例えば、実施の形態1では、属性情報がαであれば、ユーザ秘密鍵k*については、基底ベクトルb^*_3の係数としてα、基底ベクトルb^*_4の係数として1が設定された。また、暗号化データcの要素c ,については、基底ベクトルb_3の係数として1、基底ベクトルb_4の係数として_ αが設定された。しかし、例えば、ユーザ秘密鍵k*については、基底ベクトルb^*_3の係数として1、基底ベクトルb^*_4の係数としてαが設定され、暗号化データcの要素c ,については、基底ベクトルb_3の係数として—α、基底ベクトルb_4の係数として1が設定されてもよい。

また、このように単純に値を設定する基底ベクトルを変更するのではなく、全く別の方法により鍵情報や属性情報を割り当てるようにしてもよい。どのような割り当て方法であっても、上記実施の形態に係る失効方式を適用することは可能である。

[01 37] また、上記実施の形態では、鍵の失効方式を非特許文献1，2に記載された関数型暗号方式へ適用する方法について説明した。

しかし、上記実施の形態に係る鍵の失効方式は、非特許文献1，2に記載された関数型暗号方式に限らず、非特許文献1，2に記載された関数型暗号方式を応用した関数型暗号方式に適用することも可能である。

また、上記実施の形態に係る鍵の失効方式は、関数型暗号方式に限らず、他の暗号方式にも適用可能である。

[01 38] また、上記実施の形態では、関数型暗号方式を用いて、メッセージmを送信する場合について説明した。

公開鍵暗号方式を用いた暗号化では、通常、データを共通鍵で暗号化した後、その共通鍵をユーザの公開鍵で暗号化するいわゆるハイブリッド暗号方式を用いることが多い。ハイブリッド暗号方式では、暗号化したデータにユーザの公開鍵で暗号化された共通鍵が添付される。

ハイブリッド暗号方式では、暗号化された共通鍵を暗号化データから削除することで、共通鍵で暗号化されたデータを復号することができなくなる。しかし、関数型暗号方式は複数の秘密鍵で復号可能なデータを１つの公開鍵で暗号化する。そのため、仮に同じ仕組みで共通鍵を添付する場合、複数の秘密鍵に対して１つしか暗号化された共通鍵を付与しない。つまり、１人のユーザが失効すれば、従来通りの方式で対応すると再暗号化するしか方法がない。

しかし、上記実施の形態に係る鍵の失効方式を用いれば、関数型暗号方式を用いたハイブリッド暗号方式の場合であっても鍵の失効を実現することができる。なお、ハイブリッド暗号方式の場合、メッセージｍとして、コンテンッを暗号化するための共通鍵 (又は共通鍵の生成元データ)が設定される。

[01 39] 図１２は、ユーザ端末１００、暗号化データ管理装置２００、暗号化データ記憶装置３００、鍵生成装置４００のハードウエア構成の一例を示す図である。

図１２に示すように、ユーザ端末１００、暗号化データ管理装置２００、暗号化データ記憶装置３００、鍵生成装置４００は、プログラムを実行するＣＰＵ９１１(Ｃｅｎｔｒａｌ-Ｐｒｏｃｅｓｓｉｎｇ・Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう)を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４、ＬＣＤ９０１(Ｌｉｑｕｉｄ Ｃｒｙｓｔａｌ Ｄｉｓｐｌａｙ)、キーボード９０２(K/ B)、通信ボード９１５、磁気ディスク装置９２０と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置９２０(固定ディスク装置)の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。磁気ディスク装置９２０は、所定の固定ディスクインタフエースを介して接続される。

[0140] ＲＯＭ９１３、磁気ディスク装置９２０は、不揮発性メモリの一例である。ＲＡＭ９１４は、揮発性メモリの一例である。ＲＯＭ９１３とＲＡＭ９１

４と磁気ディスク装置９２０とは、記憶装置（メモリ）の一例である。また、キーボード９０２、通信ボード９１５は、入力装置の一例である。また、通信ボード９１５は、通信装置の一例である。さらに、ＬＣＤ９０１は、表示装置の一例である。

[0141] 磁気ディスク装置９２０又はＲＯＭ９１３などには、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

[0142] プログラム群９２３には、上記の説明において「暗号化データ生成部１１０」、「データ送信部１２０」、「データ受信部１３０」、「復号部１４０」、「データ受信部２１０」、「失効判定部２２０」、「鍵情報設定部２３０」、「データ送信部２４０」、「認証処理部２７０」、「データ受信部３１０」、「データ操作部３２０」、「データ送信部３３０」、「指示受信部４１０」、「鍵生成部４２０」、「鍵送信部４３０」等として説明した機能を実行するソフトウェアやプログラムやその他のプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。

ファイル群９２４には、上記の説明において「鍵管理部１５０」、「失効情報管理部２５０」、「鍵管理部２６０」、「暗号化データ管理部３４０」、「マスター鍵記憶部４４０」等に記憶される情報やデータや信号値や変数値やパラメータが、「ファイル」や「データベース」の各項目として記憶される。「ファイル」や「データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵ９１１の動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵ９１１の動作の間、情報やデータや信号値や変数値やパラメータは、

メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

[0143] また、上記の説明におけるフローチヤー トの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ９１４のメモリ、その他光ディスク等の記録媒体やＩＣチップに記録される。また、データや信号は、バス９１２や信号線ゃケーブルその他の伝送媒体や電波によりオンライン伝送される。

また、上記の説明において 「部」として説明するものは、 「回路」、 「装置」、 「機器」、 「手段」、 「機能」であってもよく、また、 「ステップ」、 「手順」、 「処理」であってもよい。また、 「装置」として説明するものは、 「回路」、 「機器」、 「手段」、 「機能」であってもよく、また、 「ステップ」、 「手順」、 「処理」であってもよい。さらに、 「処理」として説明するものは 「ステップ」であっても構わない。すなわち、 「部」として説明するものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトゥエアのみ、或いは、素子・デバイス・基板・配線などのハー ドウエアのみ、或いは、ソフトウェアとハー ドウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトゥエアは、プログラムとして、ＲＯＭ９１３等の記録媒体に記憶される。プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。すなわち、プログラムは、上記で述べた 「部」としてコンピュータ等を機能させるものである。あるいは、上記で述べた 「部」の手順や方法をコンピュータ等に実行させるものである。

符号の説明

[0144] １０ 暗号処理システム、１００ ユーザ端末、１１０ 暗号化データ生成部、１２０ データ送信部、１３０ データ受信部、１４０ 復号部、１５０ 鍵管理部、２００ 暗号化データ管理装置、２１０ データ受信部、２２０ 失効判定部、２３０ 鍵情報設定部、２４０ データ送信部、２５０ 失効情報管理部、２６０ 鍵管理部、２７０ 認証処理部、３００ 暗

号化データ記憶装置、３１０　データ受信部、３２０　データ操作部、３３０　データ送信部、３４０　暗号化データ管理部、３５０　認証処理部、４００　鍵生成装置、４１０　指示受信部、４２０　鍵生成部、４３０　鍵送信部、４４０　マスター鍵記憶部。

請求の範囲

[請求項1] 暗号化データに設定された属性情報及び鍵情報と、秘密鍵に設定された属性情報及び鍵情報とが対応していない場合、前記暗号化データを前記秘密鍵で復号できない暗号化方式において、前記暗号化データを管理する暗号化データ管理装置であり、

属性情報が設定された暗号化データを記憶装置から取得するデータ取得部と、

前記データ取得部が取得した前記暗号化データに設定された前記属性情報を有するユーザに、秘密鍵が失効しているユーザが含まれるか否か判定する失効判定部と、

秘密鍵が失効しているユーザが含まれると前記失効判定部に判定されたか否かによって、異なる値を前記鍵情報として前記暗号化データに設定する鍵情報設定部と、

前記鍵情報設定部が鍵情報を設定した暗号化データをユーザ端末へ送信するデータ送信部と

を備えることを特徴とする暗号化データ管理装置。

[請求項2] 前記データ取得部は、前記鍵情報として乱数値が設定された暗号化データを取得し、

前記鍵情報設定部は、前記データ取得部が取得した暗号化データに設定された鍵情報を前記異なる値に設定し直す

ことを特徴とする請求項1に記載の暗号化データ管理装置。

[請求項3] 前記暗号化データ管理装置は、さらに、

失効した秘密鍵の世代番号を管理する失効情報管理部

を備え、

前記鍵情報設定部は、秘密鍵が失効しているユーザが含まれないと判定された場合、前記世代番号の初期値を前記鍵情報として設定し、秘密鍵が失効しているユーザが含まれると判定された場合、前記失効情報管理部が管理する世代番号とは異なる値を前記鍵情報として設定

する

ことを特徴とする請求項１に記載の暗号化データ管理装置。

[請求項4] 前記データ取得部は、所定の基底Ｂにおける一部の基底ベクトルである基底ベクトルＡの係数に前記属性情報が設定された暗号化ベクトルを前記暗号化データとして取得し、

前記鍵情報設定部は、前記基底Ｂにおける前記基底ベクトルＡとは異なる基底ベクトルである基底ベクトルＫの係数に前記異なる値を設定する

ことを特徴とする請求項１に記載の暗号化データ管理装置。

[請求項5] 前記データ取得部は、前記基底ベクトルＫの係数に乱数値が設定された前記暗号化ベクトルと、前記乱数値が暗号化された暗号化乱数値とを含む暗号化データを取得し、

前記鍵情報設定部は、前記暗号化乱数値を復号して前記乱数値を得て、前記基底ベクトルＫの係数に前記乱数値を設定したベクトルを前記暗号化ベクトルから減算し、前記基底ベクトルＫの係数に前記異なる値を設定したベクトルを前記暗号化ベクトルに加算する

ことを特徴とする請求項４に記載の暗号化データ管理装置。

[請求項6] 前記データ取得部は、前記基底ベクトルＫの係数に０が設定された前記暗号化ベクトルを前記暗号化データとして取得し、

前記鍵情報設定部は、前記基底ベクトルＫの係数に前記異なる値を設定したベクトルを前記暗号化ベクトルに加算する

ことを特徴とする請求項４に記載の暗号化データ管理装置。

[請求項7] 前記データ取得部は、ｔ＝１，．．．，ｎ（ｎは２以上の整数）の各ｔについての基底Ｂ[t]の_部の基底である属性基底の基底ベクトルの係数に前記属性情報が設定された属性ベクトルと、前記基底Ｂ[t]における前記属性基底とは異なる基底である鍵情報基底の鍵情報ベクトルとを含む暗号化ベクトルを前記暗号化データとして取得し、

前記鍵情報設定部は、前記鍵情報基底の基底ベクトルの係数に前記

異なる値を設定したベクトルに前記鍵情報ベクトルをする
ことを特徴とする請求項1に記載の暗号化データ管理装置。

[請求項8] 前記データ取得部は、前記鍵情報基底の基底ベクトルのうちの所定の基底ベクトルKの係数に乱数値が設定されたベクトルを、前記鍵情報ベクトルとして含む前記暗号化ベクトルと、前記乱数値が暗号化された暗号化乱数値とを含む暗号化データを取得し、

前記鍵情報設定部は、前記暗号化乱数値を復号して前記乱数値を得て、前記基底ベクトルKの係数に前記乱数値を設定したベクトルを前記鍵情報ベクトルから減算し、前記基底ベクトルKの係数に前記異なる値を設定したベクトルを前記鍵情報ベクトルに加算する
ことを特徴とする請求項7に記載の暗号化データ管理装置。

[請求項9] 前記データ取得部は、前記鍵情報基底の基底ベクトルのうちの所定の前記基底ベクトルKの係数に0が設定された前記暗号化ベクトルを前記暗号化データとして取得し、

前記鍵情報設定部は、前記基底ベクトルKの係数に前記異なる値を設定したベクトルを前記鍵情報ベクトルに加算する
ことを特徴とする請求項7に記載の暗号化データ管理装置。

[請求項10] 暗号化データに設定された属性情報及び鍵情報と、秘密鍵に設定された属性情報及び鍵情報とが対応していない場合、前記暗号化データを前記秘密鍵で復号できない暗号化方式において、前記暗号化データを管理する暗号化データ管理方法であり、

通信装置が、属性情報が設定された暗号化データを記憶装置から取得するデータ取得ステップと、

処理装置が、前記データ取得ステップで取得した前記暗号化データに設定された前記属性情報を有するユーザに、秘密鍵が失効しているユーザが含まれるか否か判定する失効判定ステップと、

処理装置が、秘密鍵が失効しているユーザが含まれると前記失効判定ステップで判定されたか否かによって、異なる値を前記鍵情報とし

て前記暗号化データに設定する鍵情報設定ステップと、

通信装置が、前記鍵情報設定ステツプで鍵情報を設定した暗号化データをユーザ端末へ送信するデータ送信ステツプと

を備えることを特徴とする暗号化データ管理方法。

[請求項11] 暗号化データに設定された属性情報及び鍵情報と、秘密鍵に設定された属性情報及び鍵情報とが対応していない場合、前記暗号化データを前記秘密鍵で復号できない暗号化方式において、前記暗号化データを管理する暗号化データ管理プログラムであり、

属性情報が設定された暗号化データを記憶装置から取得するデータ取得処理と、

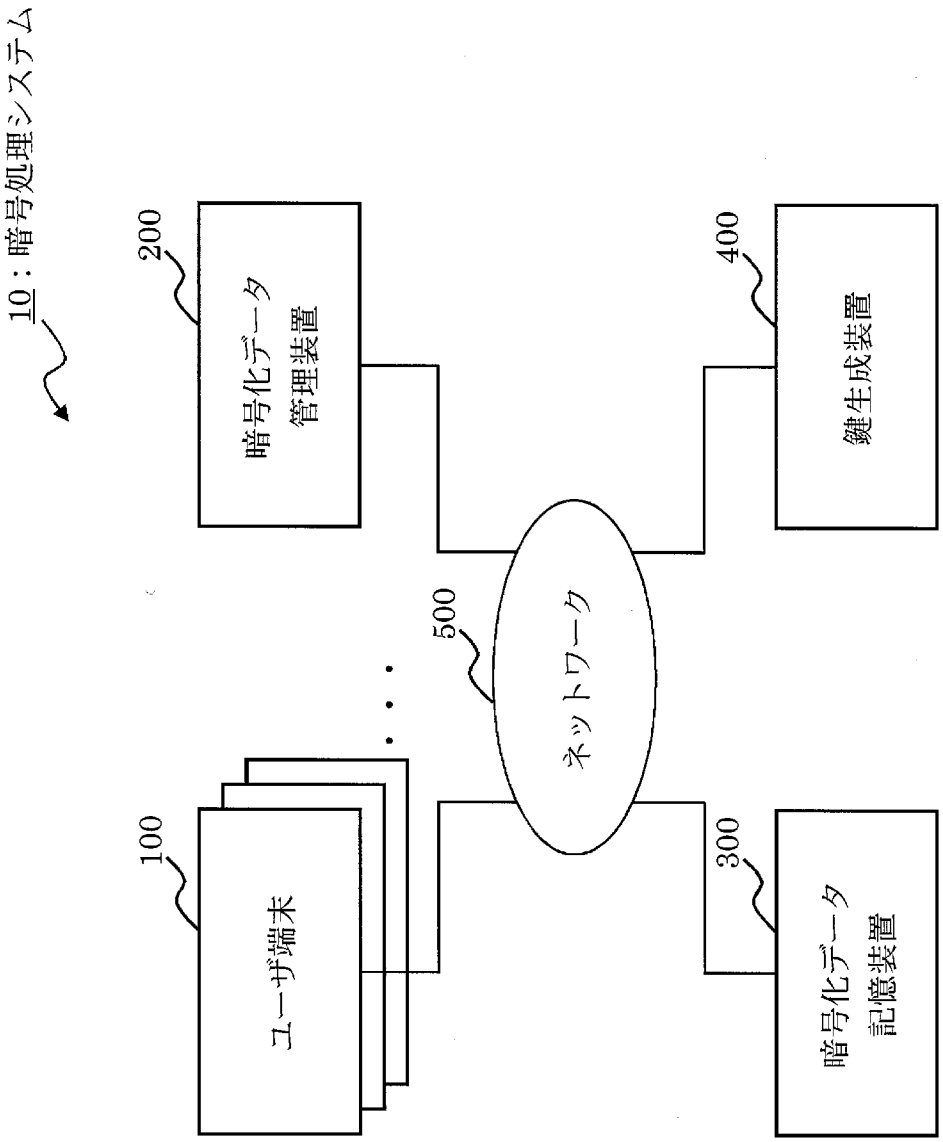
前記データ取得処理で取得した前記暗号化データに設定された前記属性情報を有するユーザに、秘密鍵が失効しているユーザが含まれるか否か判定する失効判定処理と、

秘密鍵が失効しているユーザが含まれると前記失効判定処理で判定されたか否かによって、異なる値を前記鍵情報として前記暗号化データに設定する鍵情報設定処理と、

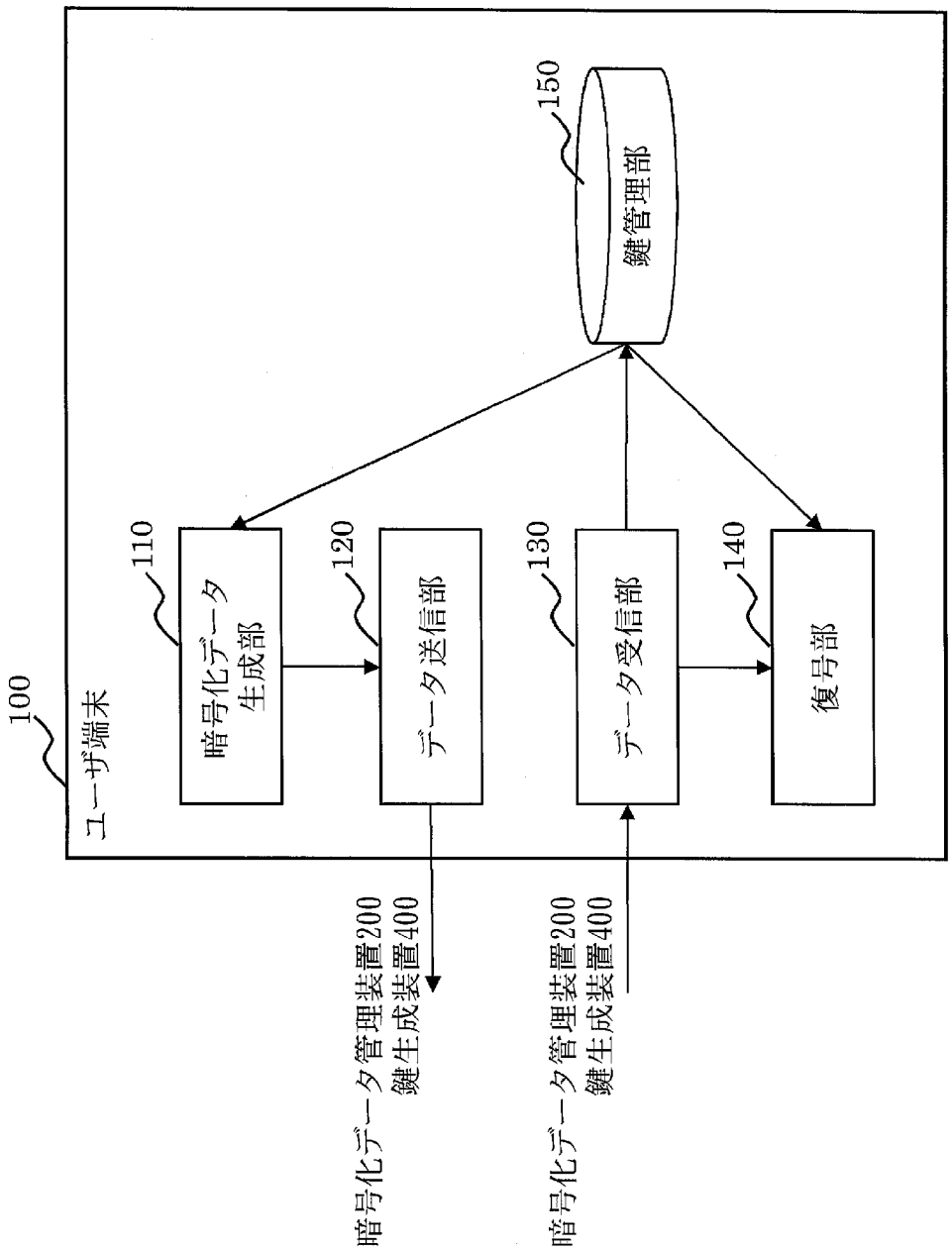
前記鍵情報設定処理で鍵情報を設定した暗号化データをユーザ端末八送信するデータ送信処理と

をコンピュータに実行させることを特徴とする暗号化データ管理プログラム。

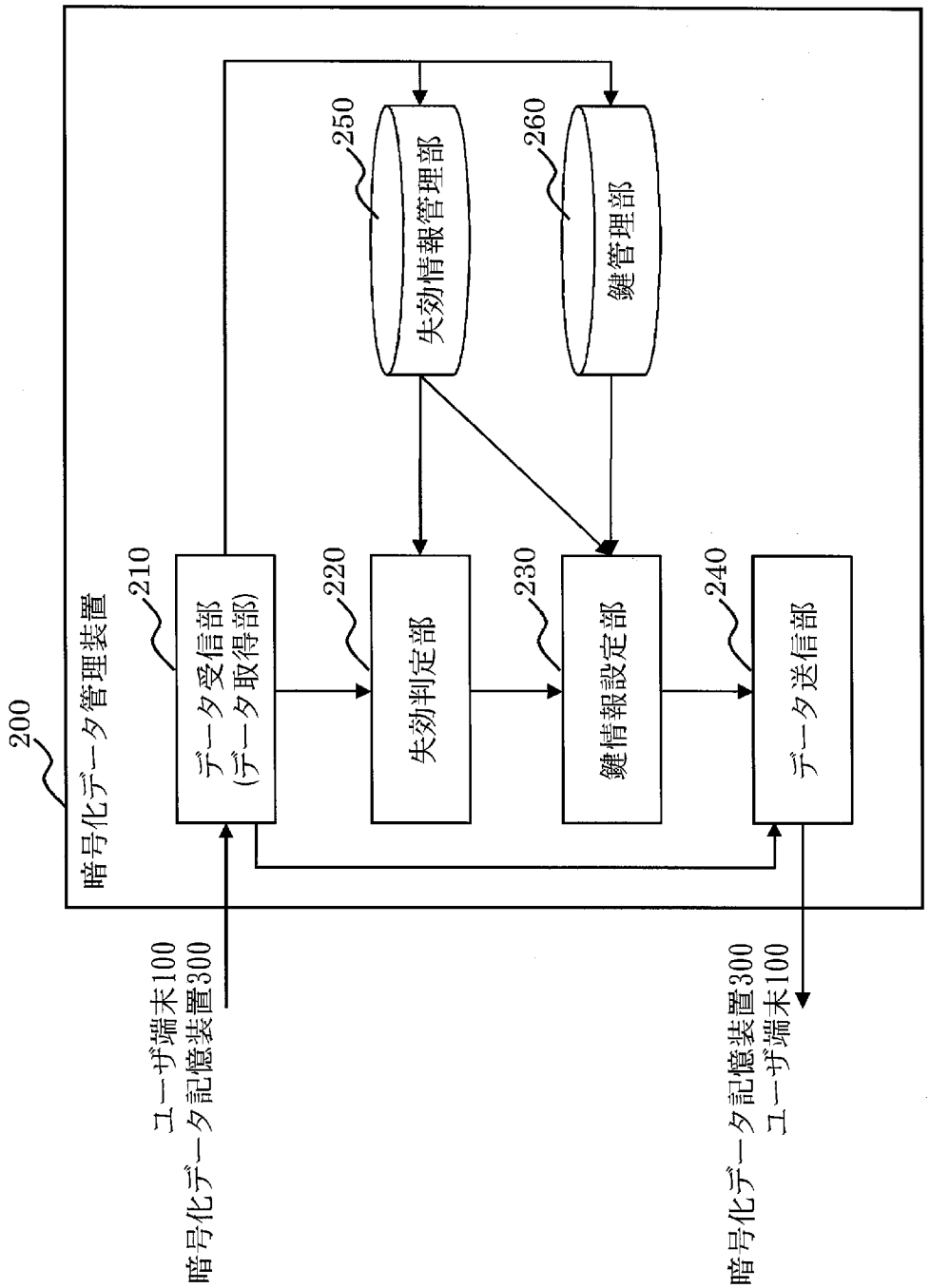
[図1]


10：暗号処理システム
200
暗号化データ
管理装置
400
鍵生成装置
500
ネットワーク
100
ユーザ端末
300
暗号化データ
記憶装置

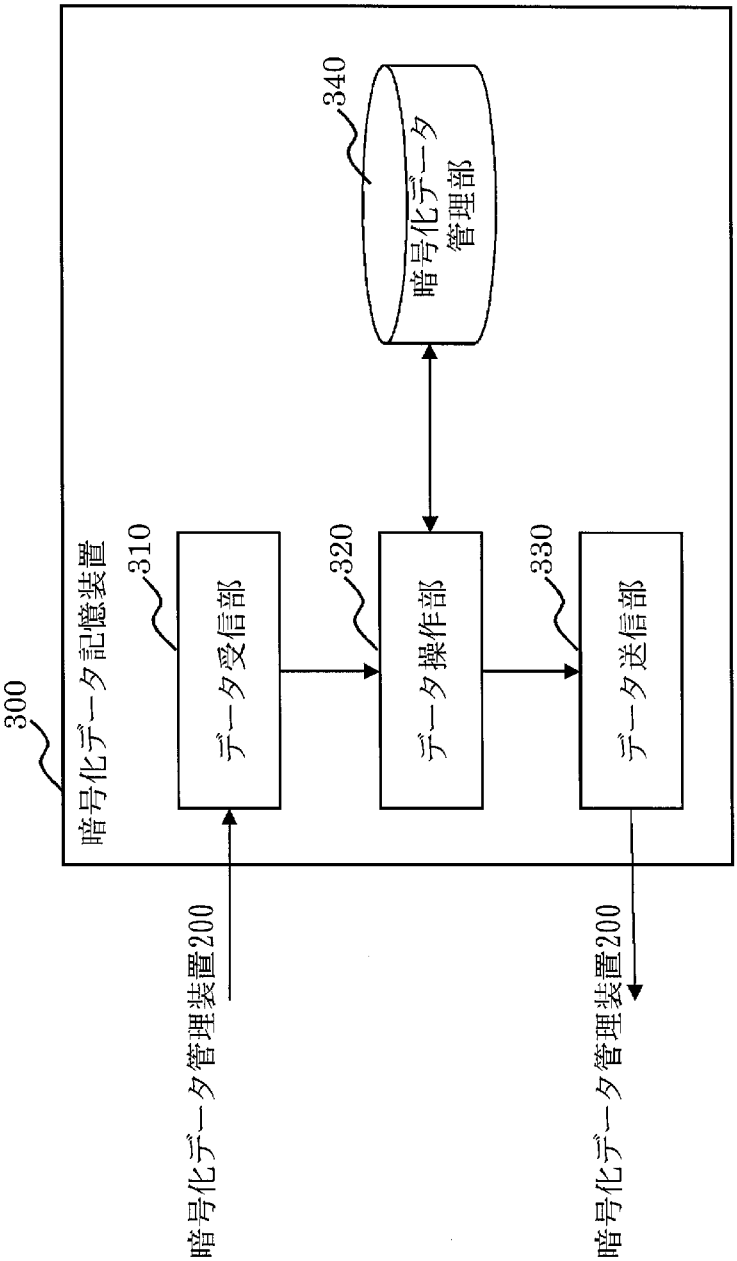
[図2]


100
ユーザ端末
110
暗号化データ生成部
120
データ送信部
130
データ受信部
140
復号部
150
鍵管理部
暗号化データ管理装置200
鍵生成装置400
暗号化データ管理装置200
鍵生成装置400

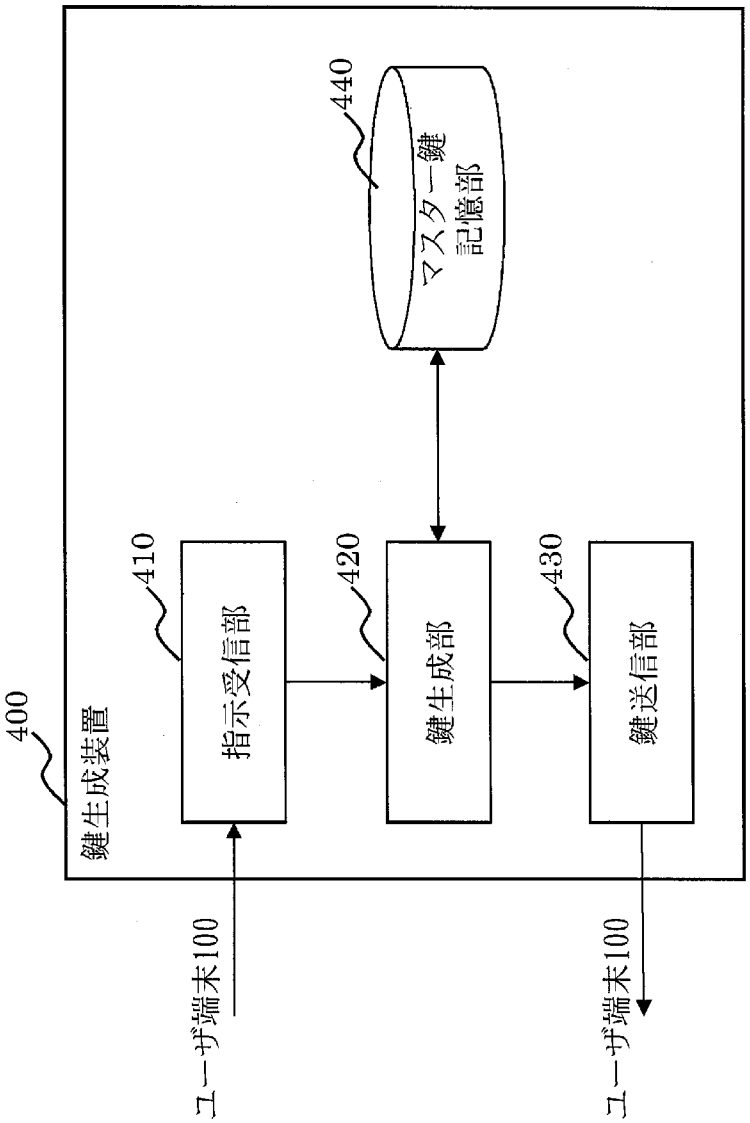
[図3]


200
暗号化データ管理装置
210
データ受信部
(データ取得部)
220
失効判定部
230
鍵情報設定部
240
データ送信部
250
失効情報管理部
260
鍵管理部
ユーザ端末100
暗号化データ記憶装置300
暗号化データ記憶装置300
ユーザ端末100

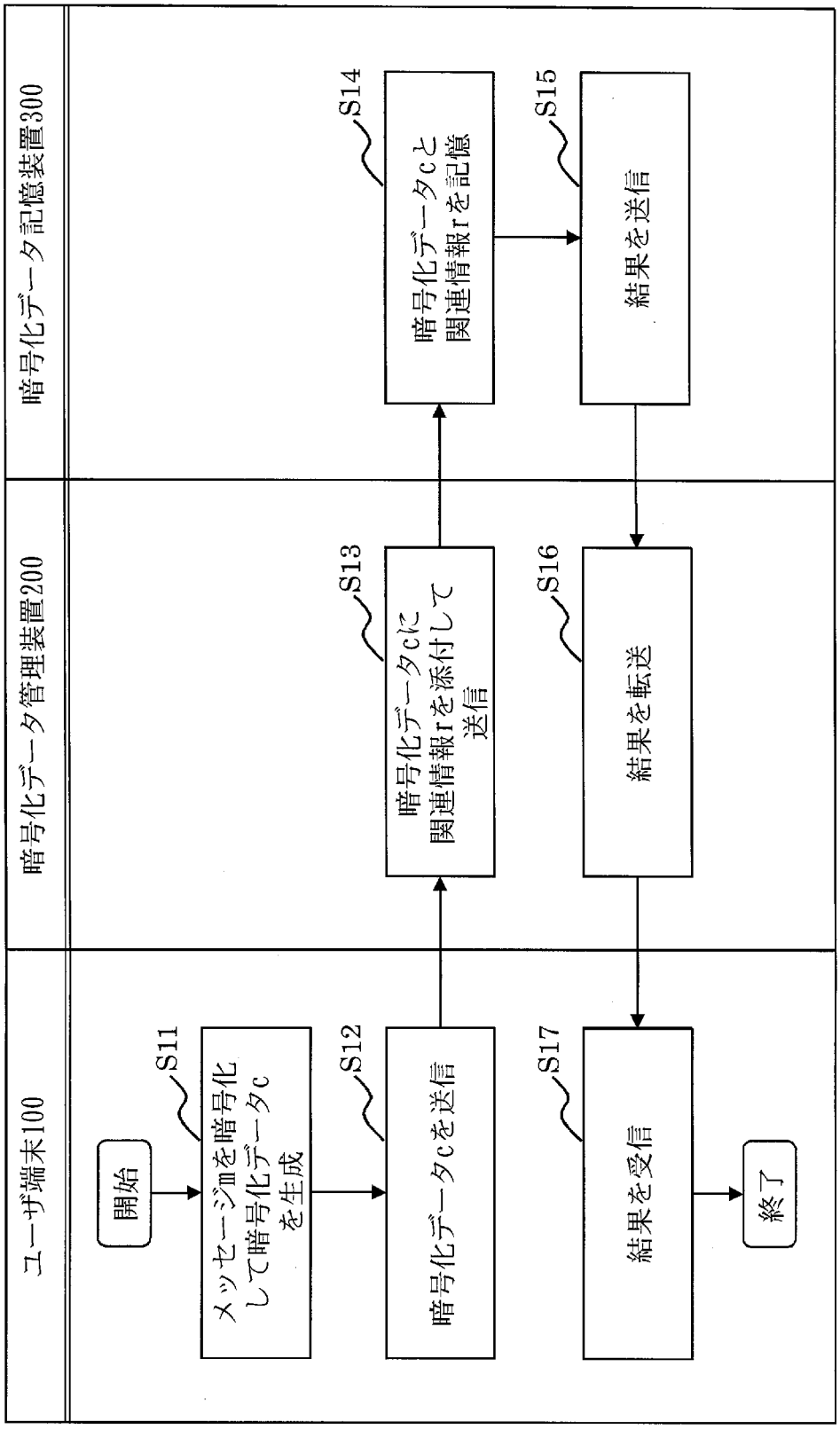
[図4]


300
暗号化データ記憶装置
310
データ受信部
320
データ操作部
330
データ送信部
340
暗号化データ
管理部
暗号化データ管理装置200
暗号化データ管理装置200

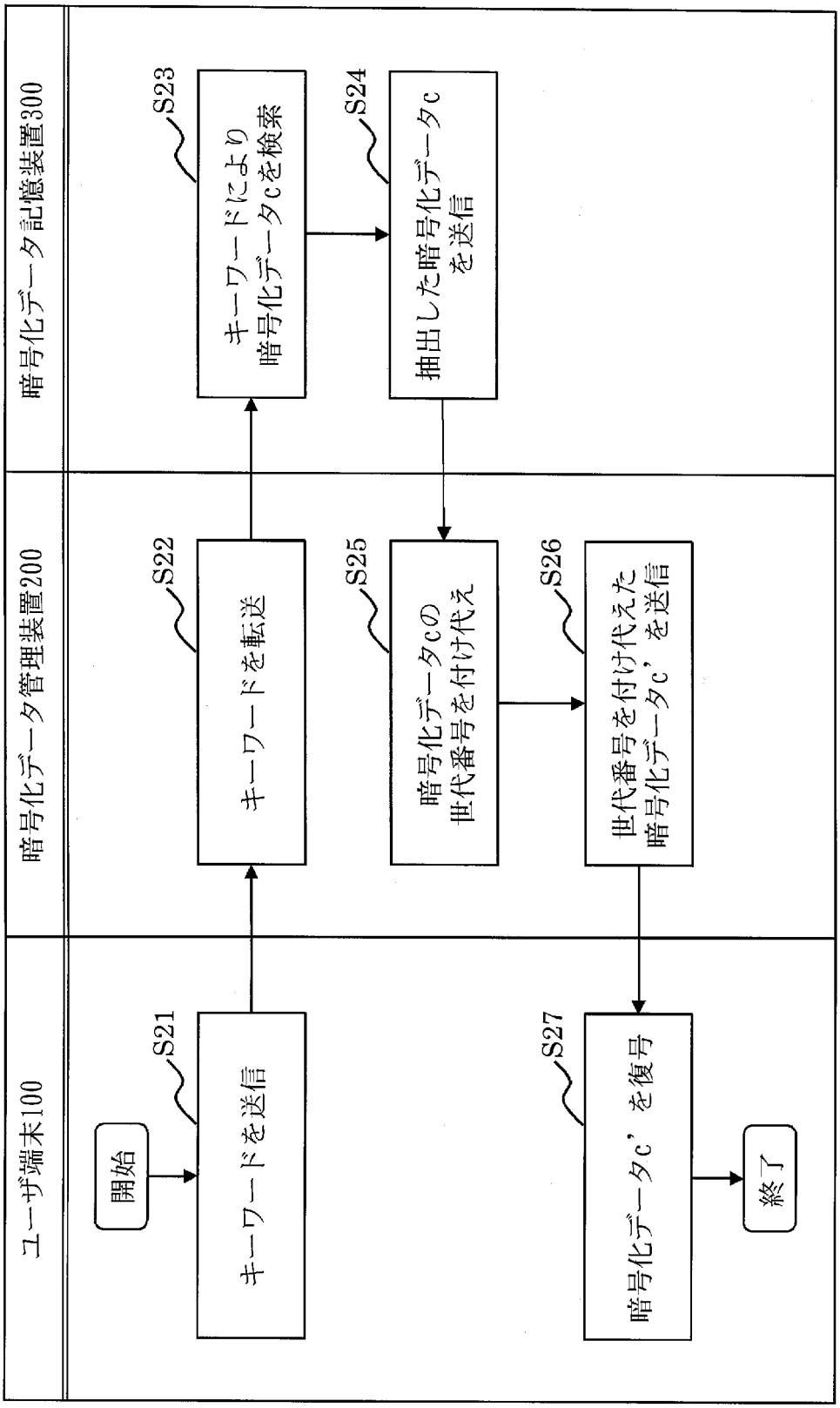
[図5]


400
鍵生成装置
410
指示受信部
420
鍵生成部
430
鍵送信部
440
マスター鍵
記憶部
ユーザ端末100
ユーザ端末100

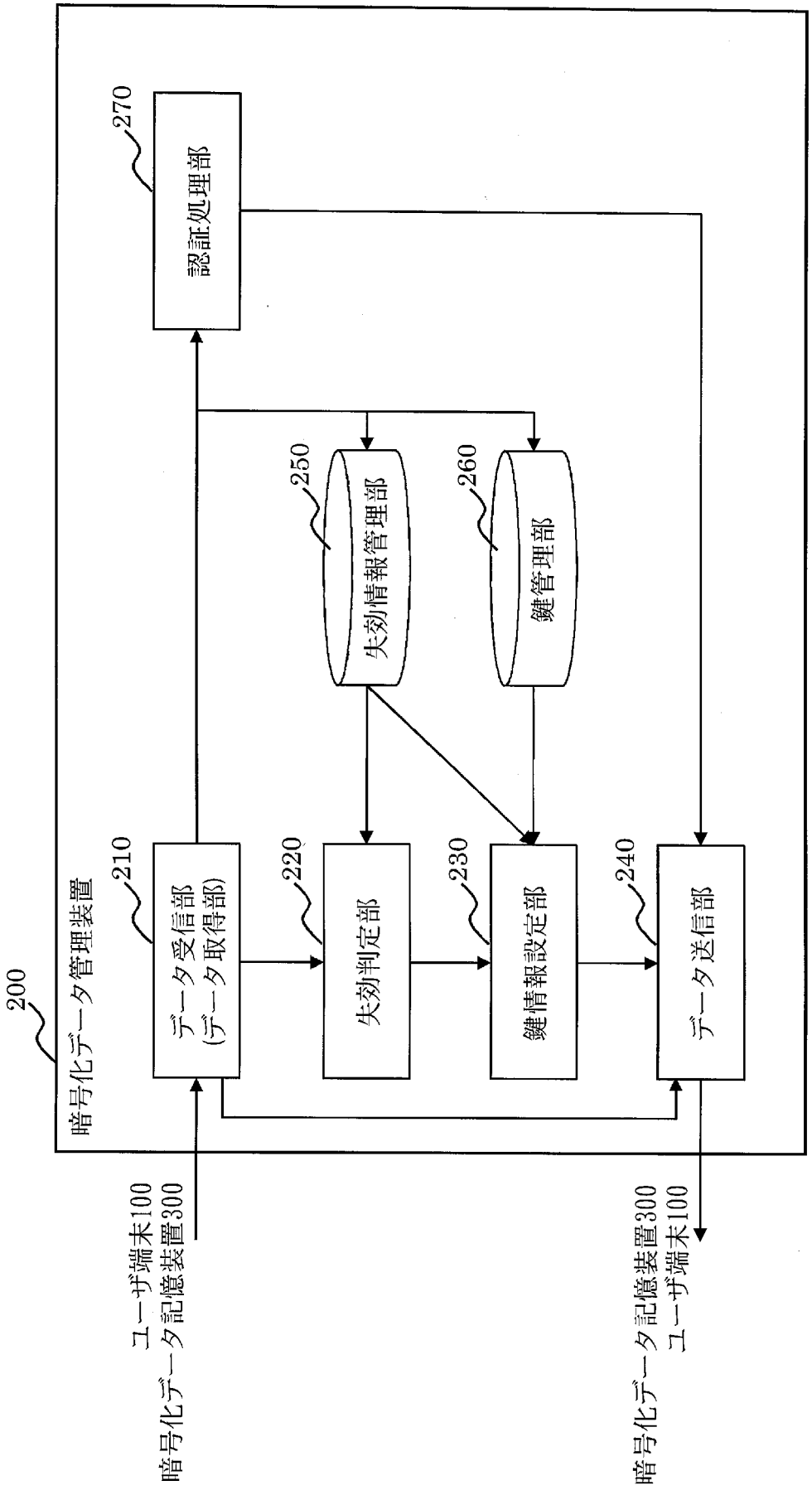
[図6]


ユーザ端末100
暗号化データ管理装置200
暗号化データ記憶装置300
開始
S11
メッセージmを暗号化して暗号化データcを生成
S12
暗号化データcを送信
S13
暗号化データcに関連情報rを添付して送信
S14
暗号化データcと関連情報rを記憶
S15
結果を送信
S16
結果を転送
S17
結果を受信
終了

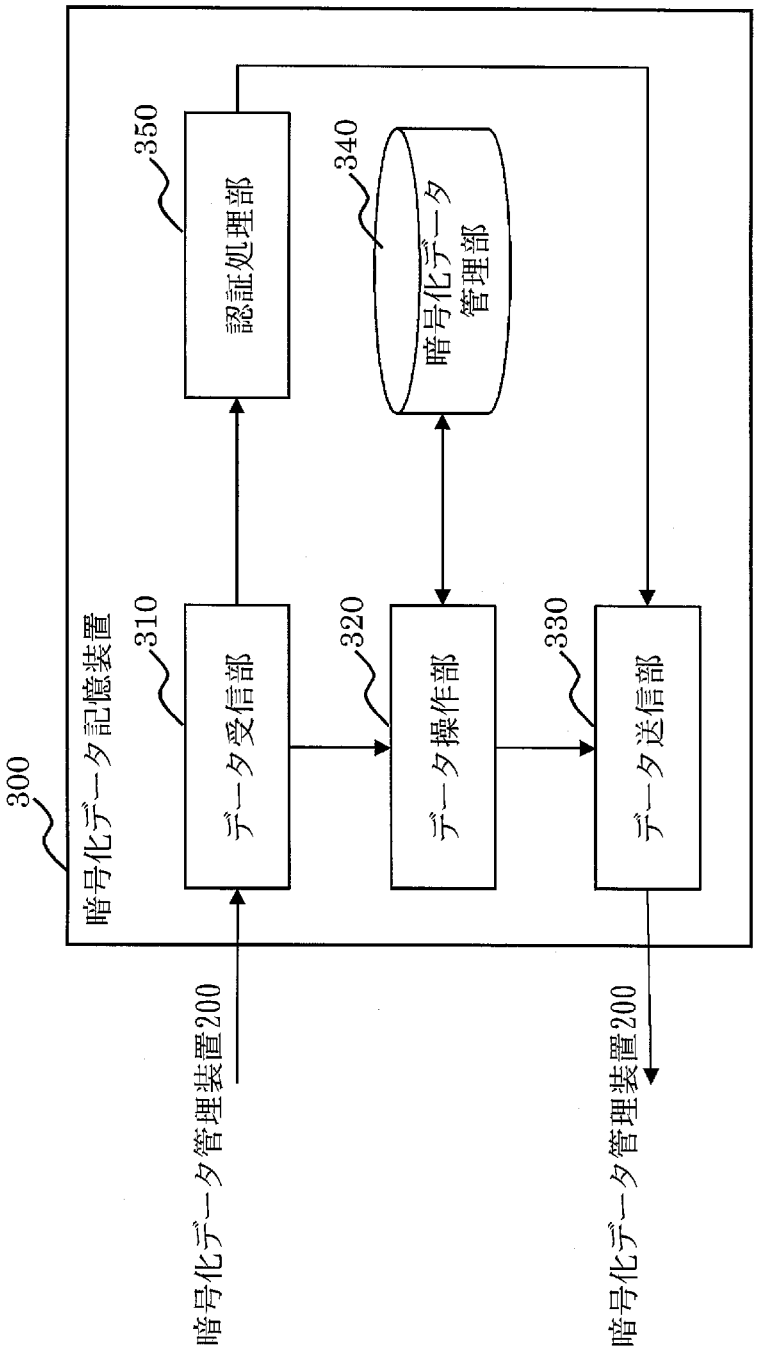
[図7]


ユーザ端末100
暗号化データ管理装置200
暗号化データ記憶装置300
開始
S21
キーワードを送信
S22
キーワードを転送
S23
キーワードにより
暗号化データcを検索
S24
抽出した暗号化データc
を送信
S25
暗号化データcの
世代番号を付け代え
S26
世代番号を付け代えた
暗号化データc'を送信
S27
暗号化データc'を復号
終了

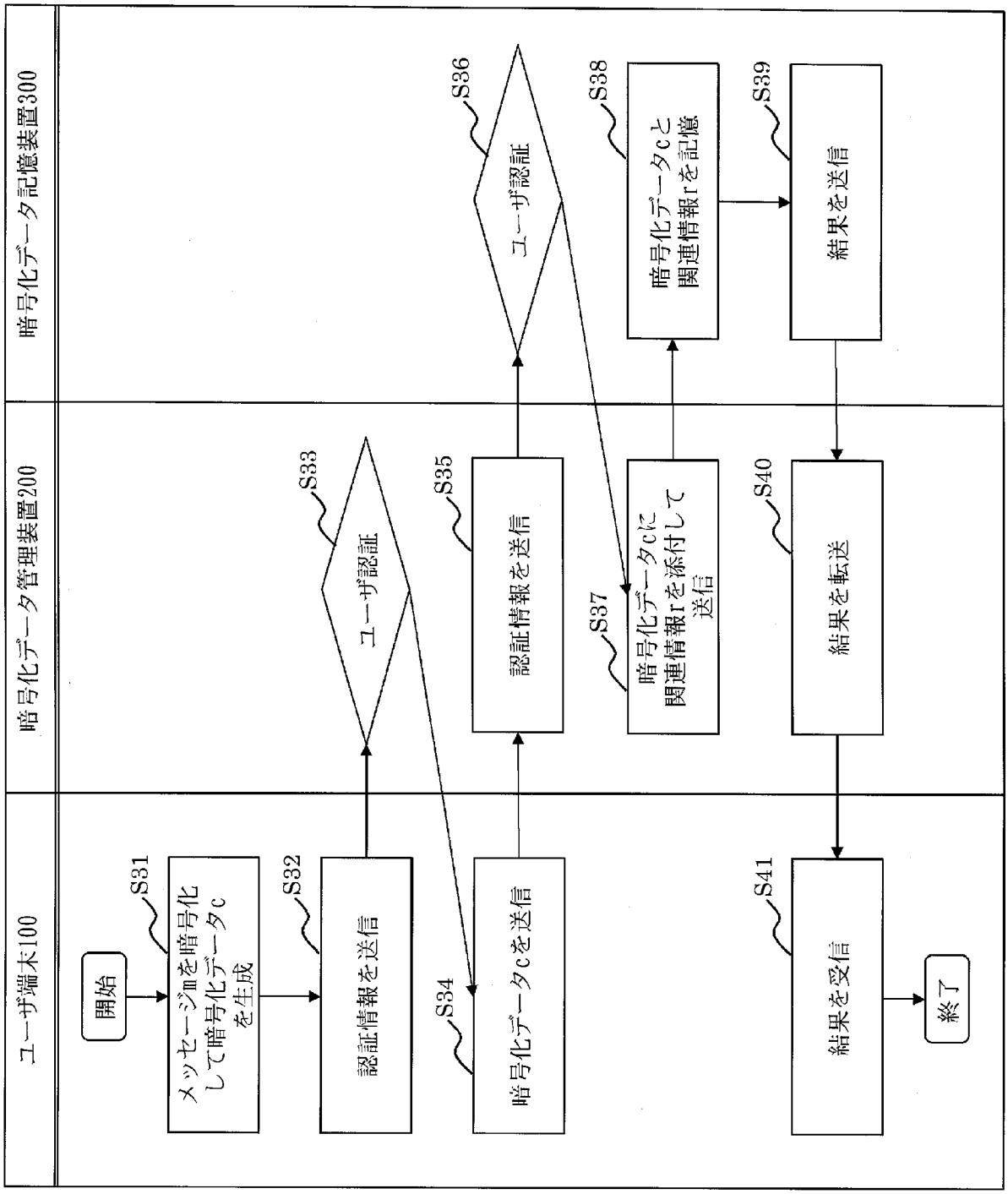
[図8]


200
暗号化データ管理装置
210
データ受信部
(データ取得部)
220
失効判定部
230
鍵情報設定部
240
データ送信部
250
失効情報管理部
260
鍵管理部
270
認証処理部
ユーザ端末100
暗号化データ記憶装置300
暗号化データ記憶装置300
ユーザ端末100

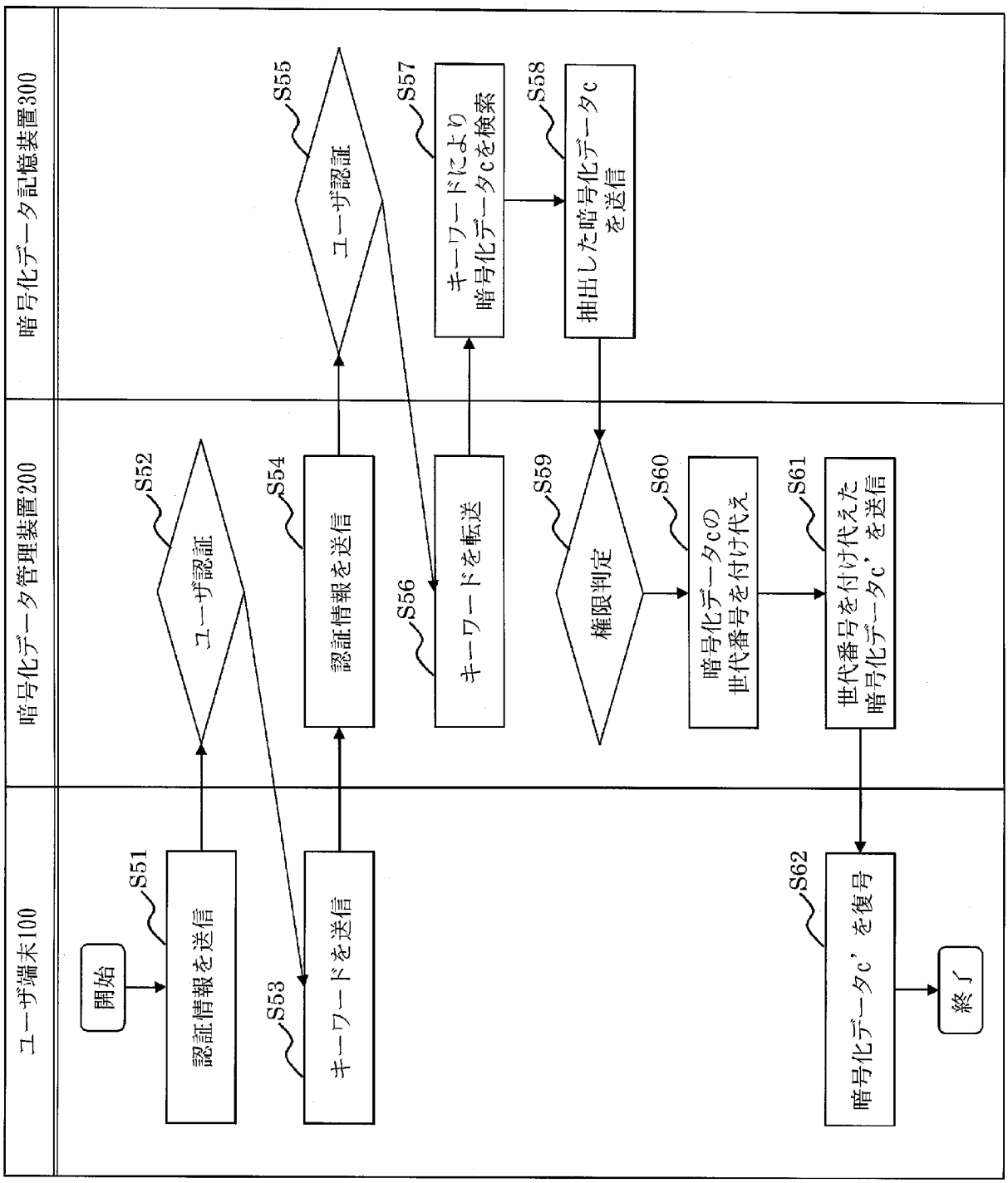
[図9]


300
暗号化データ記憶装置
310
データ受信部
320
データ操作部
330
データ送信部
340
暗号化データ管理部
350
認証処理部
暗号化データ管理装置200
暗号化データ管理装置200

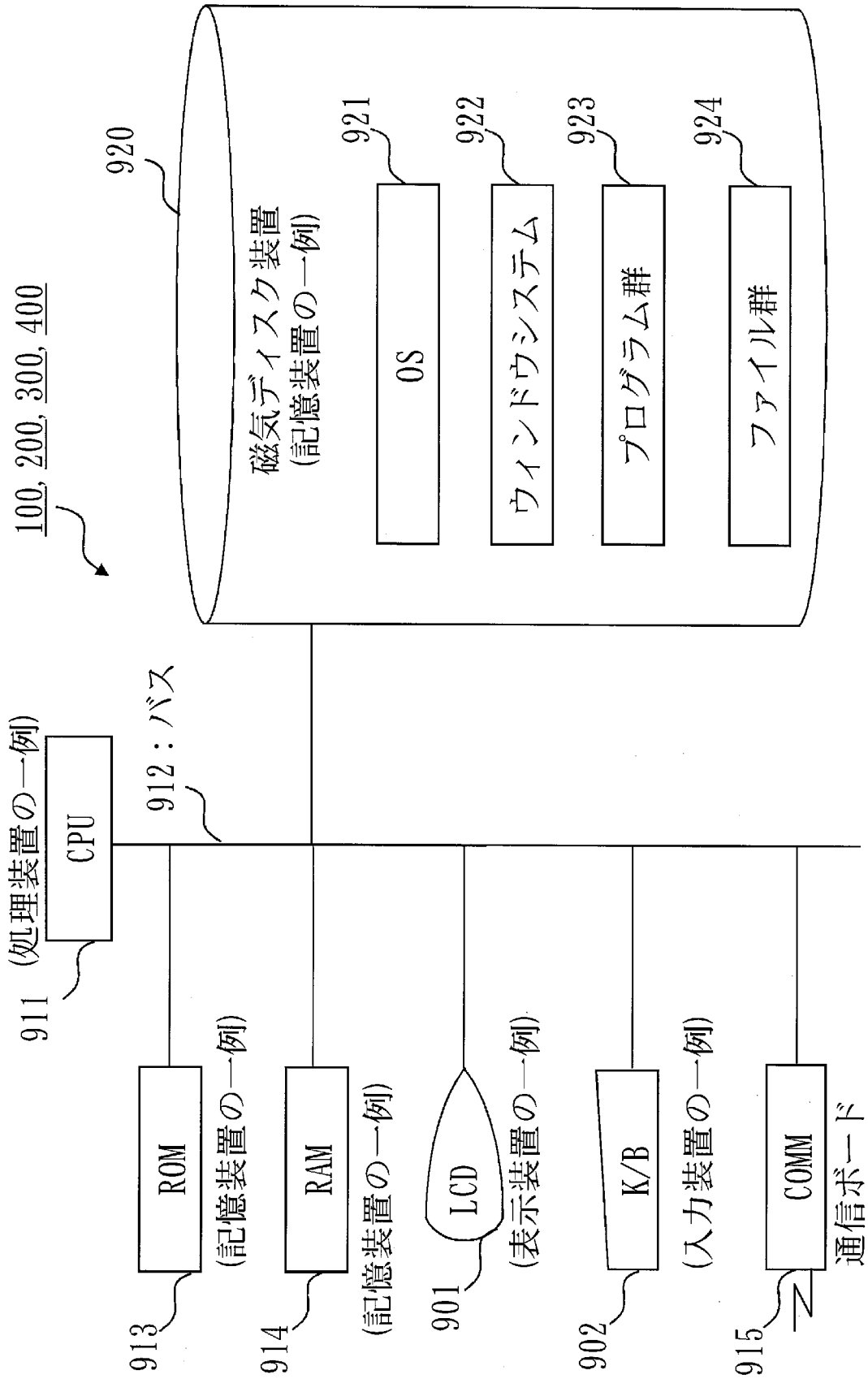
[図10]


ユーザ端末100
暗号化データ管理装置200
暗号化データ記憶装置300
開始
S31
メッセージmを暗号化して暗号化データcを生成
S32
認証情報を送信
S33
ユーザ認証
S34
暗号化データcを送信
S35
認証情報を送信
S36
ユーザ認証
S37
暗号化データcに関連情報rを添付して送信
S38
暗号化データcと関連情報rを記憶
S39
結果を送信
S40
結果を転送
S41
結果を受信
終了

[図11]


ユーザ端末100
暗号化データ管理装置200
暗号化データ記憶装置300
開始
S51
認証情報を送信
S52
ユーザ認証
S53
キーワードを送信
S54
認証情報を送信
S55
ユーザ認証
S56
キーワードを転送
S57
キーワードにより
暗号化データcを検索
S58
抽出した暗号化データc
を送信
S59
権限判定
S60
暗号化データcの
世代番号を付け代え
S61
世代番号を付け代えた
暗号化データc'を送信
S62
暗号化データc'を復号
終了

[図12]


100, 200, 300, 400
920
磁気ディスク装置
(記憶装置の一例)
921
OS
922
ウィンドウシステム
923
プログラム群
924
ファイル群
911
(処理装置の一例)
CPU
912：バス
913
ROM
(記憶装置の一例)
914
RAM
(記憶装置の一例)
901
LCD
(表示装置の一例)
902
K/B
(入力装置の一例)
915
COMM
通信ボード

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/079519

A. CLASSIFICATION OF SUBJECT MATTER
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)
H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2012
Kokai Jitsuyo Shinan Koho 1971-2012 Toroku Jitsuyo Shinan Koho 1994-2012

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JST Plus / JMEDPlus / JST7580 (JDreaml l)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Mitsuhiro Hatto riet al, Searchable Public-Key Encryption for Hierarchical Systems with Adaptive Join/Leave of Members, 2011 Nen Symposium on Cryptography and Information Security Yokoshu CD-ROM, 25 January 2011 (25.01.2011), 4C2-5	1-11
A	WO 2011/086668 A1 (Mitsubishi Electric Corp.), 21 July 2011 (21.07.2011), paragraph [0412] (Family: none)	1-11
A	Ken'ichiro MUTO et al., "Joho Kagi Ango ni Okeru Kagi Kanri Hoshiki no Kento", 2011 Nen Symposium on Cryptography and Information Security Yokoshu CD-ROM, 25 January 2011 (25.01.2011), 2F1-4	1-11

☒ 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, exhibnion 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 tiie invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 January, 2012 (13.01.12)	24 January, 2012 (24.01.12)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/079519

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Takuho MITSUNAGA, "Implementation and Evaluation of Attribute Based Encryption with Revocation Function", Dai 73 Kai (Heisei 23 Nen) Zenkoku Taikai Koen Ronbunshu (3) Network Security, 02 March 2011 (02.03.2011), pages 3-443 to 3-444	1-11

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１１／０７９５１９

A． 発明の属する分野の分類 (国際特許分類 (ＩＰＣ))

Int.Cl. 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. 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－
日本国公開実用新案公報	１９７１－２０１２年
日本国実用新案登録公報	１９９６－
日本国登録実用新案公報	１９９４－２０１２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)

JSTPlus/JMEDPlus/JST7580 (JDreamII)

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	Mitsuhiro Hattori et al, Searchable Public-Key Encryption for Hierarchical Systems with Adaptive Join/Leave of Members, 2011年 暗号と情報セキュリティシンポジウム予稿集 ＣＤ—ＲＯＭ, 2011. 01. 25, 4C2-5	1-11
A	WO 2011/086668 A1 (三菱電機株式会社) 2011. 07. 21, 段落【００４１】－【００４２】 (ファミリーなし)	1-11

☑ 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
１３．０１．２０１２	２４．０１．２０１２

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

特許庁審査官 (権限のある職員) 5S 3146
松平 英
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	武藤　健一郎　et al，情報鍵暗号における鍵管理方式の検討，2011年　暗号と情報セキュリティシンポジウム予稿集　CD—ROM，2011. 01. 25, 2F1-4	1-11
A	満永　拓邦　Takuho Mitsunaga,　鍵失効機能を持つ属性ベース暗号の実装評価，第73回(平成23年)全国大会講演論文集(3)　ネットワーク　セキュリティ，2011. 03. 02，ρ· 3-443 〜3-444	1-11