(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
2015 年 7 月 23 日(23.07.2015)

WIPO | PCT

(10) 国際公開番号
WO 2015/107641 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2014/050626

(22) 国際出願日: 2014 年 1 月 16 日(16.01.2014)

(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: 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).

(72) 発明者: 伊藤 隆(**ITO, Takashi**); 〒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). 市川 幸宏(**ICHIKAWA, Sachihiro**); 〒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). 森 拓海(**MORI, Takumi**); 〒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). 川合 豊(**KAWAI, Yutaka**); 〒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). 高島 克幸(**TAKASHIMA, Katsuyuki**); 〒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).

(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).

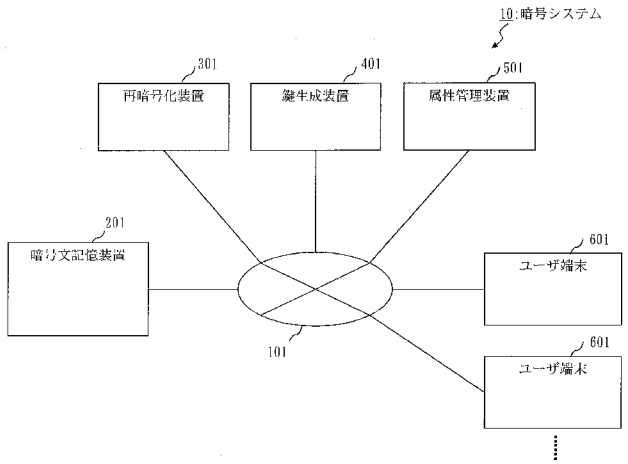
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, 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, 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).

[続葉有]

(54) **Title**: ENCRYPTION SYSTEM, KEY GENERATING DEVICE, RE-ENCRYPTION DEVICE, AND USER TERMINAL

(54) 発明の名称 : 暗号システム、鍵生成装置、再暗号化装置及びユーザ端末



10 Encryption system
201 Encrypted text storage device
301 Re-encryption device
401 Key generating device
501 Attribute management device
601 User terminal

(57) **Abstract**: This encryption system (10) uses an encryption protocol which, when two instances of information mutually correspond, is capable of decrypting an encrypted text, whereupon one of the instances of information is set, with a decryption key whereupon the other of the instances of information is set. A key generating device (401) generates a user secret key whereupon is set one of mutually corresponding instances of key information (u, y), and a re-encryption key which converts an encrypted text which may be decrypted with an attribute secret key whereupon is set one of mutually corresponding instances of user attribute information (x, v) to a re-encrypted text whereupon the other instance of key information (u, y) is set. An encrypted text storage device (201) stores the encrypted text whereupon the other instance of user attribute information (x, v) is set. A re-encryption device (301) re-encrypts with the re-encryption key the encrypted text which the encrypted text storage device stores and generates a re-encrypted text. A user terminal (601) decrypts the re-encrypted text with the user secret key.

(57) 要約: 暗号システム（１０）は、２つの情報が互いに対応している場合に一方の情報が設定された暗号文を他方の情報が設定された復号鍵により復号可能な暗号方式を用いる。鍵生成装置（４０１）は、互いに対応する鍵情報ｕ，ｙの一方が設定されたユーザ秘密鍵と、互いに対応するユーザ属性情報ｘ，ｖの一方が設定された属性秘密鍵で復号可能な暗号文を鍵情報ｕ，ｙの他方が設定された再暗号文に変換する再暗号化鍵とを生成する。暗号文記憶装置（２０１）は、ユーザ属性情報ｘ，ｖの他方が設定された暗号文を記憶する。再暗号化装置（３０１）は、再暗号化鍵で、暗号文記憶装置が記憶する暗号文を再暗号化して再暗号文を生成する。ユーザ端末（６０１）は、ユーザ秘密鍵で再暗号文を復号する。

WO 2015/107641 A1

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

暗号システム、鍵生成装置、再暗号化装置及びユーザ端末

技術分野

[0001] この発明は、鍵の失効を実現する暗号システムに関する。

背景技術

[0002] クラウドサービスの普及により、個人や企業のデータを外部のクラウドサーバに保管する機会が増えている。個人情報や企業機密が漏洩することを避けるため、暗号化したデータをクラウドサーバに保管することが多い。

[0003] データを暗号化する際に復号条件を指定でき、復号条件を満たすユーザのみが暗号文を復号できる関数型暗号がある。関数型暗号を用いると、データ作成者がアクセス権をコントロールすることができる。そのため、機密度や公開範囲の異なる様々なデータを扱う企業等がクラウドサービスを利用する際に都合がよい。

[0004] 企業等では、ユーザの異動や退職に伴ってアクセス権が変化するケースや、例えば社員証に格納された秘密鍵を紛失するケース等が考えられる。この際に、ユーザや鍵の失効処理、すなわち「それまで読めていたデータを読めなくする処理」が必要となる。

特にクラウドサーバを共有ファイルサーバのように使う場合、クラウドサーバには過去から現在に至るまでの全てのデータが保管される可能性がある。そのため、漏えいした秘密鍵から過去の全てのデータが漏れる危険性があり、何らかの対策が必須である。

[0005] 単純な失効処理の方式としては、企業等がクラウドサーバの全ての暗号文を復号し、失効した鍵では読めないようにデータを暗号化し直した後に、クラウドサーバに保管し直すものが考えられる。しかし、失効処理が発生するたびに大量データの送受信及び暗号処理を行う必要があり、効率が悪い。

[0006] 特許文献１には、クラウドサーバの暗号文を直接ユーザに渡すのではなく

、暗号文を暗号化したままで宛先を変更できる「再暗号化鍵」を利用し、個別のユーザ用暗号文に変換（再暗号化）してユーザに渡すことについて記載されている。特許文献１に記載された技術を応用すれば、再暗号化鍵の管理により失効処理を実現できる。

先行技術文献

特許文献

[0007] 特許文献1：特開２０１２－１６９９７８号広報

非特許文献

[0008] 非特許文献1：川合豊、高島克幸著、「代理人再暗号化機能を持つ関数型暗号」、２０１３年暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１３）、２０１３年１月２２日発行

発明の概要

発明が解決しようとする課題

[0009] 特許文献１では、ＲＳＡ暗号やＩＤベース暗号等、公開鍵と秘密鍵とが１対１の関係にある公開鍵暗号における再暗号化の仕組みを利用している。

そのため、企業等で１ユーザが複数のグループに属している場合、１ユーザに対して複数個の再暗号化鍵を管理する必要がある。例えば、所属が「総務部」で、役職が「課長」で、入社年度が「２０００年」であるユーザの場合、「総務部宛ての暗号文をユーザＡ宛てに再暗号化するための再暗号化鍵」と、「課長宛ての暗号文をユーザＡ宛てに再暗号化するための再暗号化鍵」と、「２０００年入社の人宛ての暗号文をユーザＡ宛てに再暗号化するための再暗号化鍵」との３個の再暗号化鍵を管理する必要がある。

また、アクセス権をグループのＡＮＤ条件として設定したい場合、ＡＮＤ条件に相当するグループについても再暗号化鍵を管理する必要がある。例えば、「総務部の課長」だけが読めるように暗号化したい場合、「総務部の課長宛ての暗号文をユーザＡ宛てに再暗号化するための再暗号化鍵」を管理する必要がある。そのため、ＡＮＤ条件やＯＲ条件を組み合わせた柔軟なアク

セス権を設定するには、多くの再暗号化鍵を管理する必要があり、実現することが難しい。

[0010] 非特許文献１には関数型暗号における再暗号化の仕組みが記載されている。しかし、ＲＳＡ暗号やＩＤベース暗号では公開鍵と秘密鍵とが１対１の関係にあるのに対し、関数型暗号の公開鍵と秘密鍵とは多対多の関係にある点が異なっているため、非特許文献１の方式を特許文献１の方式に単純に適用することはできない。

[0011] この発明は、関数型暗号等の柔軟なアクセス制御が可能な暗号方式における、ユーザや鍵の失効処理を効率的に実行可能とすることを目的とする。

課題を解決するための手段

[0012] この発明に係る暗号システムは、

２つの情報が互いに対応している場合に一方の情報が設定された暗号文を他方の情報が設定された復号鍵により復号可能な暗号方式を用いた暗号システムであり、

互いに対応する鍵情報ｕ，ｙの一方が設定されたユーザ秘密鍵と、互いに対応するユーザ属性情報ｘ，ｖの一方が設定された属性秘密鍵で復号可能な暗号文を前記鍵情報ｕ，ｙの他方が設定された再暗号文に変換する再暗号化鍵とを生成する鍵生成装置と、

前記ユーザ属性情報ｘ，ｖの他方が設定された暗号文を記憶する暗号文記憶装置と、

前記鍵生成装置が生成した前記再暗号化鍵で、前記暗号文記憶装置が記憶する前記暗号文を再暗号化して再暗号文を生成する再暗号化装置と、

前記鍵生成装置が生成した前記ユーザ秘密鍵で、前記再暗号化装置が再暗号化した前記再暗号文を復号するユーザ端末と

を備えることを特徴とする。

発明の効果

[0013] この発明に係る暗号システムでは、関数型暗号等の暗号方式の柔軟なアクセス制御を利用しつつ、再暗号化技術を取り入れることで、ユーザや鍵の失

効処理を効率的に実行できる。

図面の簡単な説明

[0014] [図1]実施の形態１に係る暗号システム１０の構成図。

[図2]実施の形態１に係る暗号文記憶装置２０１の構成図。

[図3]暗号文記憶部２１１が記憶する情報の一例を示す図。

[図4]実施の形態１に係る再暗号化装置３０１の構成図。

[図5]公開パラメータ記憶部３１１が記憶する情報の一例を示す図。

[図6]再暗号化鍵記憶部３１２が記憶する情報の一例を示す図。

[図7]実施の形態１に係る鍵生成装置４０１の構成図。

[図8]マスタ鍵情報記憶部４１１が記憶する情報の一例を示す図。

[図9]鍵情報記憶部４１２が記憶する情報の一例を示す図。

[図10]認証情報記憶部４１３が記憶する情報の一例を示す図。

[図11]実施の形態１に係る属性管理装置５０１の構成図。

[図12]属性情報記憶部５１１が記憶する情報の一例を示す図。

[図13]認証情報記憶部５１２が記憶する情報の一例を示す図。

[図14]実施の形態１に係るユーザ端末６０１の構成図。

[図15]公開パラメータ記憶部６１１が記憶する情報の一例を示す図。

[図16]ユーザ秘密鍵記憶部６１２が記憶する情報の一例を示す図。

[図17]システム全体の初期設定の流れを示すフローチャート。

[図18]ユーザ登録処理の流れを示すフローチャート。

[図19]データ登録処理の流れを示すフローチャート。

[図20]データ取得処理の流れを示すフローチャート。

[図21]ユーザ秘密鍵更新処理の流れを示すフローチャート。

[図22]鍵情報記憶部４１２が記憶する情報の一例を示す図。

[図23]ユーザ秘密鍵記憶部６１２が記憶する情報の一例を示す図。

[図24]再暗号化鍵記憶部３１２が記憶する情報の一例を示す図。

[図25]ユーザ属性更新処理の流れを示すフローチャート。

[図26]属性情報記憶部５１１が記憶する情報の一例を示す図。

[図27]鍵情報記憶部４１２が記憶する情報の一例を示す図。

[図28]再暗号化鍵記憶部３１２が記憶する情報の一例を示す図。

[図29]実施の形態１に示した暗号文記憶装置２０１、再暗号化装置３０１、鍵生成装置４０１、属性管理装置５０１、ユーザ端末６０１のハードウェア構成の例を示す図。

発明を実施するための形態

[0015] 実施の形態１.

以下の説明では、暗号方式として、関数型暗号における再暗号化方式（非特許文献１参照）を用いる。関数型暗号における再暗号化方式は、関数型暗号で暗号化されたデータを、暗号化したままで宛先を変更できる方式である。

[0016] 関数型暗号における再暗号化方式は、以下の（１）（２）の特徴を持つ。

（１）暗号化鍵と復号鍵とは、それぞれ情報ｘと情報ｖとが設定されている。そして、情報ｘと情報ｖとが対応する場合に限り、復号鍵dk_vは暗号化鍵ek_xで暗号化された暗号文を復号することができる。

（２）暗号化鍵と復号鍵とに情報ｘと情報ｖとがそれぞれ設定されていることに加え、再暗号化鍵は２つの情報（ｕ，ｖ）が設定されている。そして、情報ｘと情報ｖとが対応する場合に限り、再暗号化鍵$rk_{(u,v)}$は、暗号化鍵ek_xで暗号化された暗号文を、暗号化鍵ek_uで暗号化された暗号文に変更することができる。

ここで、情報ｘと情報ｖとは、例えば、一方がポリシー（復号条件）で、他方がポリシーに対する入力値である。この場合、情報ｘと情報ｖとが対応するとは、入力値がポリシーを満たすということである。

[0017] 関数型暗号における再暗号化方式には、暗号文にポリシーを設定した暗号文ポリシー型の方式と、復号鍵にポリシーを設定した鍵ポリシー型の方式とがある。

例えば、暗号文ポリシー型の方式の場合、暗号文に「総務部、または部長のみが復号可能」のようにユーザの属性に関する復号条件が設定され、復号

鍵に「所属＝総務部、役職＝課長、入社年度＝２０００年」のようにユーザの属性情報が設定される。一方、鍵ポリシー型の方式の場合、暗号文に「所属＝総務部、役職＝課長、入社年度＝２０００年」のようにユーザの属性情報が設定され、復号鍵に「総務部、または部長のみが復号可能」のようにユーザの属性に関する復号条件が設定される。

ここでは、暗号文ポリシー型の方式を用いて説明を行う。しかし、単に暗号化鍵と復号鍵とに設定する情報を入れ替えることで、鍵ポリシー型の方式を用いた方式とすることができる。

[0018] なお、暗号文に設定された復号条件を復号鍵に設定された属性情報が満たす場合に、暗号文を復号鍵で復号可能な暗号化方式における再暗号化方式であれば、非特許文献１に記載された以外の再暗号化方式を用いてもよい。

[0019] 図１は、実施の形態１に係る暗号システム１０の構成図である。

暗号システム１０は、ネットワーク１０１を介して、暗号文記憶装置２０１と、再暗号化装置３０１と、鍵生成装置４０１と、属性管理装置５０１と、複数のユーザ端末６０１とが接続されている。

[0020] 図２は、実施の形態１に係る暗号文記憶装置２０１の構成図である。

暗号文記憶装置２０１は、暗号文を保持し、ユーザ端末６０１からの要求に応じて暗号文の送受信を行う。暗号文記憶装置２０１は、暗号文記憶部２１１、通信部２３１を備える。

[0021] 暗号文記憶部２１１は、図３に示すように、暗号文を、対応するデータＩＤと関連付けて記憶する記憶装置である。暗号文の例としては、文書や画像等のファイルを暗号化したもの、氏名等の文字列を暗号化したもの、年齢等の数値を暗号化したもの等が挙げられる。暗号文記憶部２１１は、１つのデータＩＤに対して複数個・複数種類の暗号文を記憶してもよい。また、暗号文記憶部２１１は、暗号文を、検索用のキーワード等と関連付けて記憶してもよい。

[0022] 通信部２３１は、ユーザ端末６０１等と通信を行う。

[0023] 図４は、実施の形態１に係る再暗号化装置３０１の構成図である。

再暗号化装置３０１は、復号条件が設定された暗号文を受信し、受信した暗号文を特定のユーザ向けに再暗号化してユーザ端末６０１に送信する。再暗号化装置３０１は、公開パラメータ記憶部３１１、再暗号化鍵記憶部３１２、再暗号化部３２１、通信部３３１を備える。

[0024] 公開パラメータ記憶部３１１は、図５に示すように、データの再暗号化に必要な、関数型暗号の公開パラメータを記憶する記憶装置である。

[0025] 再暗号化鍵記憶部３１２は、図６に示すように、復号条件が設定された暗号文を、特定のユーザ向けに再暗号化するための再暗号化鍵を、対応するユーザＩＤと関連付けて記憶する記憶装置である。

[0026] 再暗号化部３２１は、復号条件が設定された暗号文を、再暗号化鍵記憶部３１２が記憶した再暗号化鍵で再暗号化し、特定のユーザ向けの暗号文を出力する。再暗号化処理は、既存の暗号技術（ここでは、非特許文献１に記載された暗号技術）を用いて実現される。

[0027] 通信部３３１は、属性管理装置５０１やユーザ端末６０１等と通信を行う。

[0028] 図７は、実施の形態１に係る鍵生成装置４０１の構成図である。

鍵生成装置４０１は、データの暗号化・復号に必要な、関数型暗号の鍵（公開パラメータ及び秘密鍵）と、データの再暗号化に必要な、関数型暗号の再暗号化鍵とを生成する。鍵生成装置４０１は、マスタ鍵情報記憶部４１１、鍵情報記憶部４１２、認証情報記憶部４１３、鍵生成部４２１、認証部４２２、通信部４３１を備える。

[0029] マスタ鍵情報記憶部４１１は、図８に示すように、関数型暗号におけるマスタ秘密鍵と公開パラメータとを記憶する記憶装置である。

[0030] 鍵情報記憶部４１２は、図９に示すように、各ユーザの属性に対応する秘密鍵（以降、属性秘密鍵と記す）と、各ユーザ向けの暗号文を復号するための秘密鍵（以降、ユーザ秘密鍵と記す）のＩＤ（ユーザ秘密鍵ＩＤ）とを、対応するユーザＩＤと関連付けて記憶する記憶装置である。

[0031] 認証情報記憶部４１３は、図１０に示すように、属性管理装置５０１との

認証処理に必要な情報（ここでは、属性管理装置５０１のＩＤ（属性管理装置ＩＤ）とパスワード）を記憶する記憶装置である。

[0032] 鍵生成部４２１は、関数型暗号の鍵と、再暗号化鍵とを生成する。鍵の生成処理は、既存の暗号技術（ここでは、非特許文献１に記載された暗号技術）を用いて実現される。

[0033] 認証部４２２は、属性管理装置５０１との間で認証処理を実行する。認証処理は、既存の認証技術を用いて実現される。

[0034] 通信部４３１は、属性管理装置５０１等と通信を行う。

[0035] 図１１は、実施の形態１に係る属性管理装置５０１の構成図である。

属性管理装置５０１は、各ユーザの属性を管理し、管理する属性に基づいてユーザ秘密鍵と再暗号化鍵との生成を鍵生成装置４０１に依頼する。属性管理装置５０１は、属性情報記憶部５１１、認証情報記憶部５１２、認証部５２１、登録部５２２、通信部５３１を備える。

[0036] 属性情報記憶部５１１は、図１２に示すように、各ユーザの属性を、対応するユーザＩＤと関連付けて記憶する記憶装置である。

[0037] 認証情報記憶部５１２は、図１３に示すように、鍵生成装置４０１との認証処理に必要な情報（ここでは、属性管理装置５０１のＩＤ（属性管理装置ＩＤ）とパスワード）を記憶する記憶装置である。

[0038] 認証部５２１は、鍵生成装置４０１との間で認証処理を実行する。認証処理は、既存の認証技術を用いて実現される。

[0039] 登録部５２２は、ユーザの属性情報の登録を行う。登録処理は、例えば、管理者が入力画面等を操作することにより行われる。

[0040] 通信部５３１は、再暗号化装置３０１や鍵生成装置４０１やユーザ端末６０１と通信を行う。

[0041] 図１４は、実施の形態１に係るユーザ端末６０１の構成図である。

ユーザ端末６０１は、暗号文を暗号文記憶装置２０１に記憶し、必要に応じて暗号文記憶装置２０１からの暗号文を取得して復号する。ユーザ端末６０１は、公開パラメータ記憶部６１１、ユーザ秘密鍵記憶部６１２、暗号化

部６２１、復号部６２２、通信部６３１を備える。

[0042] 公開パラメータ記憶部６１１は、図１５に示すように、データの暗号化や復号に必要な、関数型暗号の公開パラメータを記憶する記憶装置である。

[0043] ユーザ秘密鍵記憶部６１２は、図１６に示すように、データの復号に必要なユーザ秘密鍵を、ユーザＩＤと関連付けて記憶する記憶装置である。

[0044] 暗号化部６２１は、復号条件を設定してデータを暗号化する。暗号化処理は、既存の暗号技術（ここでは、非特許文献１に記載された暗号技術）を用いて実現される。

[0045] 復号部６２２は、再暗号化装置３０１から受信した再暗号文をユーザ秘密鍵で復号する。復号処理は、既存の暗号技術（ここでは、非特許文献１に記載された暗号技術）を用いて実現される。

[0046] 通信部６３１は、暗号文記憶装置２０１や再暗号化装置３０１や属性管理装置５０１等と通信を行う。

[0047] 暗号システム１０の動作について説明する。暗号システム１０の動作は、（１）システム全体の初期設定、（２）ユーザ登録処理、（３）データ登録処理、（４）データ取得処理、（５）ユーザ秘密鍵更新処理、（６）ユーザ属性更新処理、に大別される。

なお、以下の説明では、非特許文献１に記載された暗号技術を単に関数型暗号と記す。

[0048] （１）システム全体の初期設定

システム全体の初期設定は、暗号システム１０の運用で必要になる初期情報を準備する処理である。システム全体の初期設定は、暗号システム１０の運用開始前に実行される。

[0049] 図１７は、システム全体の初期設定の流れを示すフローチャートである。

（Ｓ１０１）

鍵生成装置４０１の鍵生成部４２１は、関数型暗号の初期設定を行い、マスタ秘密鍵と公開パラメータとを生成し、マスタ鍵情報記憶部４１１に格納する。

これにより、マスタ鍵情報記憶部４１１は、図８に示す情報を記憶した状態になる。

[0050] （Ｓ１０２）

鍵生成装置４０１と属性管理装置５０１とは、認証に必要な情報を共有し、それぞれ認証情報記憶部４１３と認証情報記憶部５１２とに格納する。ここでは、属性管理装置ＩＤとパスワードの組を共有する。

これにより、認証情報記憶部４１３は、図１０に示す情報を記憶した状態になり、認証情報記憶部５１２は、図１３に示す情報を記憶した状態になる。

[0051] （Ｓ１０３）

属性管理装置５０１の通信部５３１は、鍵生成装置４０１から公開パラメータを取得し、再暗号化装置３０１に送信する。再暗号化装置３０１の通信部３３１は、公開パラメータを受信し、公開パラメータ記憶部３１１に格納する。

これにより、公開パラメータ記憶部３１１は、図５に示す情報を記憶した状態になる。

[0052] （２）ユーザ登録処理

ユーザ登録処理は、暗号システム１０を利用するユーザを登録する処理である。ユーザ登録処理は、（１）システム全体の初期設定の直後、及び、暗号システム１０を利用するユーザが増える度に実行される。ここでは、１ユーザを登録する処理について説明する。したがって、複数ユーザを登録する場合には、登録する人数分、以下に説明する処理を繰り返す必要がある。なお、以下の説明において、一部の例では、複数のユーザが登録された後の状態を示している。

[0053] 図１８は、ユーザ登録処理の流れを示すフローチャートである。

（Ｓ２０１）

属性管理装置５０１の登録部５２２は、登録するユーザに対し、一意となるユーザＩＤを割り当てる。登録部５２２は、関数型暗号の秘密鍵生成に必

要なユーザ属性を設定する。そして、登録部５２２は、ユーザＩＤとユーザ属性とを関連付けて属性情報記憶部５１１に格納する。

これにより、属性情報記憶部５１１は、図１２に示す情報を記憶した状態となる。図１２では、複数のユーザが登録された後の状態を示している。図１２では、例えば、総務部の課長である佐藤花子氏に対し、ユーザＩＤとしてｕｉｄ$_2$が割り当てられ、ユーザ属性として「所属＝総務部、役職＝課長、氏名＝佐藤花子」が設定されている。

[0054] （Ｓ２０２）

属性管理装置５０１の認証部５２１と、鍵生成装置４０１の認証部４２２とが、認証情報記憶部５１２と認証情報記憶部４１３とに格納されている認証情報を用いて認証処理を行う。ここでは、属性管理装置ＩＤとパスワードによる認証処理が行われる。

[0055] （Ｓ２０３）

認証処理が成功すると、属性管理装置５０１の通信部５３１は、登録するユーザのユーザＩＤとユーザ属性とを鍵生成装置４０１に送信し、鍵の発行を依頼する。

先の例では、ユーザＩＤとしてｕｉｄ$_2$が、ユーザ属性として「所属＝総務部、役職＝課長、氏名＝佐藤花子」が送信される。

[0056] （Ｓ２０４）

鍵生成装置４０１の鍵生成部４２１は、マスタ鍵情報記憶部４１１に格納されているマスタ秘密鍵及び公開パラメータと、受信したユーザ属性とを入力として、関数型暗号の秘密鍵生成処理を行う。これにより、ユーザ属性（ユーザ属性情報の一方）が設定された属性秘密鍵が生成される。

先の例では、ユーザＩＤがｕｉｄ$_2$である佐藤花子氏に関して、ユーザ属性「所属＝総務部、役職＝課長、氏名＝佐藤花子」を入力として、属性秘密鍵ｓｋ$_2$が生成される。

[0057] （Ｓ２０５）

鍵生成装置４０１の鍵生成部４２１は、鍵情報記憶部４１２の中で一意と

なるユーザ秘密鍵ＩＤ（鍵情報の一方）を生成する。ここでは、ｕｋｉｄ$_i$が生成されたとする。鍵生成部４２１は、マスタ秘密鍵及び公開パラメータと、属性「ユーザ秘密鍵ＩＤ＝ｕｋｉｄ$_i$」とを入力として、関数型暗号の秘密鍵生成処理を行う。これにより、ユーザ秘密鍵ＩＤが設定されたユーザ秘密鍵が生成される。

先の例では、ユーザＩＤがｕｉｄ$_2$である佐藤花子氏に関して、ユーザ秘密鍵ＩＤとしてｕｋｉｄ$_2$を生成した上で、属性「ユーザ秘密鍵ＩＤ＝ｕｋｉｄ$_2$」を入力として、ユーザ秘密鍵ｕｋ$_2$が生成される。

[0058] （Ｓ２０６）

鍵生成装置４０１の鍵生成部４２１は、公開パラメータと、属性秘密鍵と、復号条件「ユーザ秘密鍵ＩＤ＝ｕｋｉｄ$_i$」（鍵情報の他方）とを入力として、関数型暗号の再暗号化鍵生成処理を行う。これにより、再暗号化鍵が生成される。

先の例では、ユーザＩＤがｕｉｄ$_2$である佐藤花子氏に関して、属性秘密鍵ｓｋ$_2$と、復号条件「ユーザ秘密鍵ＩＤ＝ｕｋｉｄ$_2$」とを入力として、再暗号化鍵ｒｋ$_2$が生成される。

なお、ここで生成される再暗号化鍵は、入力された属性秘密鍵で復号可能な暗号文を、入力されたユーザ秘密鍵ＩＤが設定されたユーザ秘密鍵で復号できる暗号文に再暗号化する鍵である。

[0059] （Ｓ２０７）

鍵生成装置４０１の鍵生成部４２１は、ユーザＩＤと、属性秘密鍵と、ユーザ秘密鍵ＩＤとを関連付けて、ステータスを「有効」に設定して鍵情報記憶部４１２に格納する。

これにより、鍵情報記憶部４１２は、図９に示す情報を記憶した状態となる。図９では、複数のユーザが登録された後の状態を示している。

[0060] （Ｓ２０８）

鍵生成装置４０１の通信部４３１は、公開パラメータと、ユーザ秘密鍵と、再暗号化鍵とを属性管理装置５０１に送信する。

先の例では、ユーザ秘密鍵としてuk_2が、再暗号化鍵としてrk_2が送信される。

[0061] （Ｓ２０９）

属性管理装置５０１の通信部５３１は、公開パラメータと、ユーザＩＤと、ユーザ秘密鍵とを、ユーザＩＤに対応するユーザ端末６０１に送信する。これらを受信したユーザ端末６０１の通信部６３１は、公開パラメータを公開パラメータ記憶部６１１に、ユーザＩＤとユーザ秘密鍵とをユーザ秘密鍵記憶部６１２に格納する。

先の例では、ユーザＩＤがuid_2である佐藤花子氏に対応するユーザ端末６０１に情報が送信される。そして、佐藤花子氏に対応するユーザ端末６０１の公開パラメータ記憶部６１１は、図１５に示す情報を記憶した状態となり、ユーザ秘密鍵記憶部６１２は、図１６に示す情報を記憶した状態となる。

[0062] （Ｓ２１０）

属性管理装置５０１の通信部５３１は、ユーザＩＤと再暗号化鍵とを再暗号化装置３０１に送信する。これらを受信した再暗号化装置３０１の通信部３３１は、ユーザＩＤと再暗号化鍵とを関連付けて再暗号化鍵記憶部３１２に格納する。

先の例では、再暗号化鍵としてrk_2が送信され、再暗号化鍵記憶部３１２は、図６に示す情報を記憶した状態となる。図６では、複数のユーザが登録された後の状態を示している。

[0063] ここでのポイントは、関数型暗号の属性として、ユーザ端末６０１がデータ登録処理（手続き（３）で後述）の際に復号条件として利用しない、仮想的な属性「ユーザ秘密鍵ＩＤ」を導入し、同じ関数型暗号の枠組みの中で属性秘密鍵とユーザ秘密鍵とを使い分けるようにしたことである。これにより、単一の鍵生成装置４０１及び単一の公開パラメータで鍵発行や再暗号化が実現できるようになる。

[0064] なお、図９の例では鍵生成装置４０１の鍵情報記憶部４１２は、ユーザＩ

Ｄ、属性秘密鍵、ユーザ秘密鍵ＩＤ、ステータスを記憶している。しかし、鍵情報記憶部４１２は、手続きの途中で受信あるいは生成したユーザ属性、ユーザ秘密鍵、再暗号化鍵も記憶するようにしてもよい。また、鍵情報記憶部４１２は、属性秘密鍵を記憶せず、必要時にユーザ属性から再生成するようにしてもよい。

[0065] また、属性管理装置５０１は、安全上の観点からユーザ秘密鍵や再暗号化鍵を記憶しないが、公開パラメータだけは記憶するようにしてもよい。また、ユーザ秘密鍵や再暗号化鍵をユーザ端末６０１や再暗号化装置３０１に送信する際に、属性管理装置５０１を介さずに、鍵生成装置４０１から直接送信するようにしてもよい。

[0066] また、ユーザ端末６０１のユーザ秘密鍵記憶部６１２がユーザ属性を記憶するようにしてもよい。

[0067] （３）データ登録処理

データ登録処理は、データを暗号文記憶装置２０１に登録する処理である。データ登録処理は、ユーザ端末６０１がデータを登録する度に実行される。

データ登録処理では、ユーザ端末６０１がデータを暗号文記憶装置２０１に登録する場合、権限を持つユーザだけがデータを閲覧できるよう、関数型暗号で暗号化したデータを暗号文記憶装置２０１に送信する。これによって、権限を持たないユーザはもちろん、暗号文記憶装置２０１に対してもデータを秘匿することができる。

なお、以下の説明において、一部の例では、複数のデータが登録された後の状態を示している。

[0068] 図１９は、データ登録処理の流れを示すフローチャートである。

（Ｓ３０１）

ユーザ端末６０１の暗号化部６２１は、登録するデータに対し、一意となるデータＩＤを割り当てる。

[0069] （Ｓ３０２）

ユーザ端末６０１の暗号化部６２１は、公開パラメータ記憶部６１１に格納されている公開パラメータと、登録するデータと、復号可能なユーザ属性を指定した復号条件（ユーザ属性情報の他方）とを入力として、関数型暗号の暗号化処理を行う。これにより、データが暗号化された暗号文が生成される。

復号条件の例としては、「所属＝総務部」（総務部のユーザのみが復号可能）、「所属＝総務部　ＡＮＤ　役職＝部長」（総務部の部長のみが復号可能）、「所属＝総務部　ＯＲ　役職＝部長」（総務部のユーザ、もしくは各部の部長のみが復号可能）等が挙げられる。また、利用する関数型暗号の方式によっては、ＡＮＤ条件とＯＲ条件だけでなく、「ＮＯＴ（所属＝総務部）　ＡＮＤ　役職＝部長」（総務部以外の部の部長のみが復号可能）のように、ＮＯＴ条件を用いることも可能である。

[0070] （Ｓ３０３）

ユーザ端末６０１の通信部６３１は、データＩＤと暗号文とを、暗号文記憶装置２０１に送信する。これらを受信した暗号文記憶装置２０１は、データＩＤと暗号文とを関連付けて暗号文記憶部２１１に格納する。

これにより、暗号文記憶部２１１は、図３に示す情報を記憶した状態となる。図３では、複数のデータが登録された後の状態を示している。

[0071] なお、データの暗号化の際、データを直接関数型暗号で暗号化するのではなく、他の暗号方式（例えばＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）等の共通鍵暗号方式）でデータを暗号化し、暗号化に用いた鍵を関数型暗号で暗号化するようにしてもよい。この場合、復号の際にも関数型暗号と他の暗号方式を併用することになる。

[0072] また、図３の例では暗号文記憶装置２０１の暗号文記憶部２１１がデータＩＤ、暗号文を記憶しているが、暗号文記憶装置２０１はユーザ端末６０１から復号条件も受信し、これも暗号文記憶部２１１に記憶するようにしてもよい。復号条件は、ユーザ端末６０１が暗号文記憶装置２０１から必要な情報を検索するための補助情報として利用することができる。

[0073] （４）データ取得処理

データ取得処理は、ユーザ端末６０１が暗号文記憶装置２０１から暗号文を読み出す処理である。データ取得処理は、ユーザ端末６０１が暗号文記憶装置２０１から暗号文を読み出す度に実行される。

暗号システム１０では、ユーザや鍵の失効管理を実現するため、暗号文記憶装置２０１に保管されている暗号文が、ユーザ端末６０１単体では復号できないようになっている。暗号システム１０では、暗号文記憶装置２０１から取得した暗号文は、再暗号化装置３０１に送信され、再暗号化装置３０１で個別のユーザ向けに再暗号化される。

[0074] 図２０は、データ取得処理の流れを示すフローチャートである。

（Ｓ４０１）

ユーザ端末６０１の通信部６３１は、取得したいデータのデータＩＤを暗号文記憶装置２０１に送信する。これを受信した暗号文記憶装置２０１は、暗号文記憶部２１１からデータＩＤに関連付けられた暗号文を取得し、ユーザ端末６０１に送信する。

[0075] ここで、暗号文には復号条件としてユーザ属性が指定されているため、暗号文を復号するには、その復号条件を満たすユーザ属性が設定された属性秘密鍵が必要である。ユーザ端末６０１のユーザ秘密鍵記憶部６１２に記憶されているのはユーザ秘密鍵であるため、ユーザ端末６０１は暗号文を復号することができない。

例えば、暗号文c_1が復号条件「所属＝総務部」で暗号化されているとする。そして、図１２に示すユーザＩＤがuid_2である佐藤花子氏が暗号文c_1を取得したとする。佐藤花子氏の所属は総務部であるので、本来暗号文c_1を復号できるはずである。しかし、佐藤花子氏が持つユーザ秘密鍵uk_2は、属性「ユーザ秘密鍵ＩＤ＝uid_2」を入力として生成おり、ユーザ秘密鍵uk_2に設定された属性と復号条件とが対応しておらず、このままでは復号できない。

[0076] （Ｓ４０２）

ユーザ端末６０１の通信部６３１は、ユーザＩＤと暗号文とを再暗号化装置３０１に送信し、データの再暗号化を依頼する。これらを受信した再暗号化装置３０１は、再暗号化鍵記憶部３１２からユーザＩＤに関連付けられた再暗号化鍵を取得する。

先の例では、通信部６３１がユーザＩＤとしてuid_2を受信し、これに関連付けられた再暗号化鍵rk_2を取得する。上述したように、rk_2は、属性「所属＝総務部、役職＝課長、氏名＝佐藤花子」から生成された属性秘密鍵sk_2で復号可能な暗号文を、復号条件「ユーザ秘密鍵ＩＤ＝uid_2」となるよう再暗号化するための再暗号化鍵である。

[0077] （Ｓ４０３）

再暗号化装置３０１の再暗号化部３２１は、公開パラメータ記憶部３１１に格納されている公開パラメータと、再暗号化鍵記憶部３１２から取得した再暗号化鍵と、受信した暗号文とを入力として、関数型暗号の再暗号化処理を行う。これにより、ユーザ秘密鍵で復号可能となる暗号文（再暗号文）が生成される。

先の例では、暗号文c_1が再暗号化鍵rk_2で再暗号化され、復号条件が「ユーザ秘密鍵ＩＤ＝uid_2」である暗号文C_1が生成される。

[0078] （Ｓ４０４）

再暗号化装置３０１の通信部３３１は、再暗号化によって生成された暗号文をユーザ端末６０１に送信する。但し、再暗号化処理が失敗した場合は、その旨をユーザ端末６０１に送信する。

[0079] （Ｓ４０５）

暗号文を受信したユーザ端末６０１の復号部６２２は、公開パラメータ記憶部６１１に格納されている公開パラメータと、ユーザ秘密鍵記憶部６１２に格納されているユーザ秘密鍵と、受信した暗号文とを入力として、関数型暗号の復号処理を行う。これにより、最初に指定したデータＩＤに対応するデータを得ることができる。

先の例では、ユーザ端末６０１が暗号文C_1を受信し、これをユーザ秘密鍵

ｕｋ$_2$で復号する。すると、属性「ユーザ秘密鍵ＩＤ＝ｕｋｉｄ$_2$」と復号条件「ユーザ秘密鍵ＩＤ＝ｕｋｉｄ$_2$」が適合するため、求めるデータｄ$_1$を得ることができる。

[0080] 以上のように、正当なユーザ端末６０１は暗号文記憶装置２０１上のデータを（自分の権限の範囲で）閲覧することができる。

[0081] （５）ユーザ秘密鍵更新処理

ユーザ秘密鍵更新処理は、あるユーザが持つユーザ秘密鍵を紛失もしくは漏洩した場合等に、当該ユーザに対してユーザ秘密鍵を再発行する処理である。ユーザ秘密鍵更新処理は、ユーザ秘密鍵を再発行する際に実行される。

ユーザ秘密鍵を再発行することにより、ユーザが暗号システム１０を引き続き利用できるようになる。しかし、さらに、紛失・漏えいしたユーザ秘密鍵から暗号文記憶装置２０１に記憶されたデータが漏れることを防止する必要がある。ユーザ秘密鍵更新処理では、再暗号化装置３０１が記憶する再暗号化鍵を更新することでこれを実現する。

[0082] 図２１は、ユーザ秘密鍵更新処理の流れを示すフローチャートである。

（Ｓ５０１）

属性管理装置５０１の認証部５２１と、鍵生成装置４０１の認証部４２２とが、認証情報記憶部５１２と認証情報記憶部４１３とに格納されている認証情報を用いて認証処理を行う。ここでは、属性管理装置ＩＤとパスワードによる認証処理が行われる。

[0083] （Ｓ５０２）

認証処理が成功すると、属性管理装置５０１の通信部５３１は、ユーザ秘密鍵更新を行うユーザのユーザＩＤを鍵生成装置４０１に送信し、鍵の再発行を依頼する。

（２）ユーザ登録処理で例として挙げた、ユーザＩＤがｕｉｄ$_2$である佐藤花子氏が持っていたユーザ秘密鍵ｕｋ$_2$を更新する場合、ユーザＩＤとしてｕｉｄ$_2$が送信される。

[0084] （Ｓ５０３）

鍵生成装置４０１の鍵生成部４２１は、鍵情報記憶部４１２からユーザＩＤに関連付けられた属性秘密鍵を取得する。

先の例で、鍵情報記憶部４１２が図９に示す情報を記憶している場合、属性秘密鍵sk_2が取得される。

[0085] （Ｓ５０４）

鍵生成装置４０１の鍵生成部４２１は、鍵情報記憶部４１２の中で一意となるユーザ秘密鍵ＩＤを新たに生成する。ここでは、$ukid_i$が生成されたとする。鍵生成部４２１は、マスタ鍵情報記憶部４１１に格納されているマスタ秘密鍵及び公開パラメータと、属性「ユーザ秘密鍵ＩＤ＝$ukid_i$」とを入力として、関数型暗号の秘密鍵生成処理を行う。これにより、新たに生成されたユーザ秘密鍵ＩＤが設定されたユーザ秘密鍵が生成される。

先の例では、ユーザ秘密鍵ＩＤとして例えば$ukid_{102}$を生成した上で、属性「ユーザ秘密鍵ＩＤ＝$ukid_{102}$」を入力として、ユーザ秘密鍵uk_{102}が生成される。

[0086] （Ｓ５０５）

鍵生成装置４０１の鍵生成部４２１は、公開パラメータと、属性秘密鍵と、Ｓ５０３で新たに生成したユーザ秘密鍵ＩＤを用いた復号条件「ユーザ秘密鍵ＩＤ＝$ukid_i$」とを入力として、関数型暗号の再暗号化鍵生成処理を行う。これにより、再暗号化鍵を生成する。

先の例では、ユーザＩＤがuid_2である佐藤花子氏に関して、属性秘密鍵sk_2と復号条件「ユーザ秘密鍵ＩＤ＝$ukid_{102}$」とを入力として、再暗号化鍵rk_{102}が生成される。

[0087] （Ｓ５０６）

鍵生成装置４０１の鍵生成部４２１は、鍵情報記憶部４１２からユーザＩＤに関連付けられたレコードを検索し、該当するレコードのステータスを「失効」に更新する。

[0088] （Ｓ５０７）

鍵生成装置４０１の鍵生成部４２１は、ユーザＩＤと、属性秘密鍵と、新

たに生成したユーザ秘密鍵ＩＤとを関連付けて、ステータスを「有効」に設定して鍵情報記憶部４１２に格納する。

これにより、鍵情報記憶部４１２は、図９に示す情報を記憶した状態から、図２２に示す情報を記憶した状態に更新される。

[0089] （Ｓ５０８）

鍵生成装置４０１の通信部４３１は、新たに生成したユーザ秘密鍵と、新たに生成した再暗号化鍵とを属性管理装置５０１に送信する。

先の例では、ユーザ秘密鍵としてuk_{102}が、再暗号化鍵としてrk_{102}が送信される。

[0090] （Ｓ５０９）

属性管理装置５０１の通信部５３１は、ユーザ秘密鍵を、ユーザＩＤに対応するユーザ端末６０１に送信する。これを受信したユーザ端末６０１の通信部６３１は、ユーザ秘密鍵記憶部６１２に記憶されたユーザ秘密鍵を、受信したユーザ秘密鍵に更新する。

先の例では、ユーザＩＤがuid_2である佐藤花子氏に対応するユーザ端末６０１のユーザ秘密鍵記憶部６１２は、図１６に示す情報を記憶した状態から、図２３に示す情報を記憶した状態に更新される。

[0091] （Ｓ５１０）

属性管理装置５０１の通信部５３１は、ユーザＩＤと、新たに生成された再暗号化鍵とを再暗号化装置３０１に送信する。これらを受信した再暗号化装置３０１の通信部３３１は、再暗号化鍵記憶部３１２からユーザＩＤに関連付けられたレコードを検索し、該当するレコードの再暗号化鍵を、受信した再暗号化鍵に更新する。

先の例では、再暗号化鍵記憶部３１２は、図６に示す情報を記憶した状態から、図２４に示す情報を記憶した状態に更新される。

[0092] 以上のように、ユーザ秘密鍵を更新する場合、ユーザ秘密鍵に合わせて再暗号化鍵も更新される。そのため、更新された再暗号化鍵によって再暗号化された暗号文は、更新されたユーザ秘密鍵で復号できる。したがって、ユー

ザ秘密鍵の再発行を受けたユーザ端末６０１が、ユーザ秘密鍵更新処理の前に閲覧できていたデータを引き続き閲覧できる。

また、更新された再暗号化鍵によって再暗号化された暗号文は、更新前の古いユーザ秘密鍵で復号できない。そのため、古いユーザ秘密鍵では、暗号文記憶装置２０１に記憶されたデータを一切閲覧できない。

つまり、本手続きを実施することで、ユーザ秘密鍵の紛失・漏えいに伴う失効処理が実現される。

[0093] なお、ここではユーザ秘密鍵を失効させ、再発行する更新処理について説明しているが、ユーザの退職時等に、ユーザ秘密鍵の失効だけを行い、再発行を行わないことも可能である。この場合、再暗号化装置３０１が記憶した再暗号化鍵の削除だけを行えばよい。

[0094] （６）ユーザ属性更新処理

ユーザ属性更新処理は、企業内の異動等に伴い、あるユーザの属性（例えば、所属や役職）に変更が生じた場合に、当該ユーザが新しい属性に応じてデータを閲覧できるようにする処理である。

例えば、（２）ユーザ登録処理で例として挙げた、ユーザＩＤがuid_2である佐藤花子氏が、総務部から経理部へと異動した場合、経理部宛てのデータを閲覧できるようにしなければならない。同時に、異動後は、総務部宛てのデータを一切閲覧できないようにしたいケースがある（但し、総務部宛てのデータを引き続き閲覧できるようにしたい場合も考えられる）。ユーザ属性更新処理では、再暗号化装置３０１が記憶する再暗号化鍵を更新することでこれを実現する。

[0095] 図２５は、ユーザ属性更新処理の流れを示すフローチャートである。

（Ｓ６０１）

属性管理装置５０１の登録部５２２は、ユーザ属性の更新を行うユーザについて、属性情報記憶部５１１が記憶したユーザ属性を更新する。

先の例では、属性情報記憶部５１１は、図１２に示す情報を記憶した状態から、図２６に示す情報を記憶した状態に更新する。

[0096] （Ｓ６０２）

属性管理装置５０１の認証部５２１と、鍵生成装置４０１の認証部４２２とが、認証情報記憶部５１２および認証情報記憶部４１３に格納されている認証情報を用いて認証処理を行う。ここでは、属性管理装置ＩＤとパスワードによる認証処理が行われる。

[0097] （Ｓ６０３）

属性管理装置５０１の通信部５３１は、ユーザ属性更新を行うユーザのユーザＩＤと新しいユーザ属性とを鍵生成装置４０１に送信し、鍵の再発行を依頼する。

先の例では、ユーザＩＤとしてuid_2が、新しいユーザ属性として「所属＝経理部、役職＝課長、氏名＝佐藤花子」が送信される。

[0098] （Ｓ６０４）

鍵生成装置４０１の鍵生成部４２１は、マスタ鍵情報記憶部４１１に格納されているマスタ秘密鍵及び公開パラメータと、受信した新しいユーザ属性とを入力として、関数型暗号の秘密鍵生成処理を行う。これにより、新しいユーザ属性が設定された属性秘密鍵が生成される。

先の例では、ユーザＩＤがuid_2である佐藤花子氏に関して、新しいユーザ属性「所属＝経理部、役職＝課長、氏名＝佐藤花子」を入力として、新しい属性秘密鍵sk_{202}が生成される。

[0099] （Ｓ６０５）

鍵生成装置４０１の鍵生成部４２１は、鍵情報記憶部４１２からユーザＩＤに関連付けられたユーザ秘密鍵ＩＤを取得する。但し、ユーザＩＤに関連付けられたレコードが複数ある場合、鍵生成部４２１は、ステータスが「有効」であるレコードから取得する。ここでは、$ukid_i$が取得されたとする。

先の例では、ユーザＩＤがuid_2である佐藤花子氏に関して、図９に示す情報から、ユーザ秘密鍵ＩＤとして$ukid_2$が取得される。

[0100] （Ｓ６０６）

鍵生成装置４０１の鍵生成部４２１は、公開パラメータと、新しい属性秘密鍵と、Ｓ６０５で取得したユーザ秘密鍵ＩＤを用いた復号条件「ユーザ秘密鍵ＩＤ＝ｕｋｉｄ$_i$」とを入力として、関数型暗号の再暗号化鍵生成処理を行う。これにより、再暗号化鍵を生成する。

先の例では、ユーザＩＤがｕｉｄ$_2$である佐藤花子氏に関して、新しい属性秘密鍵ｓｋ$_{202}$と復号条件「ユーザ秘密鍵ＩＤ＝ｕｋｉｄ$_2$」とを入力として、再暗号化鍵ｒｋ$_{202}$が生成される。

[0101] （Ｓ６０７）

鍵生成装置４０１の通信部４３１は、鍵情報記憶部４１２が記憶したユーザ秘密鍵ＩＤがｕｋｉｄ$_i$であるレコードについて、属性秘密鍵を、新しい属性秘密鍵に更新する。

これにより、鍵情報記憶部４１２は、図９に示す情報を記憶した状態から、図２７に示す情報を記憶した状態に更新される。

[0102] （Ｓ６０８）

鍵生成装置４０１の通信部４３１は、新たに生成した再暗号化鍵を属性管理装置５０１に送信する。

先の例では、再暗号化鍵としてｒｋ$_{202}$が送信される。

[0103] （Ｓ６０９）

属性管理装置５０１の通信部５３１は、ユーザＩＤと、新たに生成された再暗号化鍵とを再暗号化装置３０１に送信する。これらを受信した再暗号化装置３０１の通信部３３１は、再暗号化鍵記憶部３１２からユーザＩＤに関連付けられたレコードを検索し、該当するレコードの再暗号化鍵を、受信した再暗号化鍵に更新する。

先の例では、再暗号化鍵記憶部３１２は、図６に示す情報を記憶した状態から、図２８に示す情報を記憶した状態に更新される。

[0104] 以上のように、ユーザ属性の変更があると、属性秘密鍵が更新されるとともに、属性秘密鍵に合わせて再暗号化鍵も更新される。そのため、更新された再暗号化鍵によって再暗号化できる暗号文は、更新されたユーザ属性で閲

覧可能な暗号文である。したがって、ユーザ属性の変更があったユーザのユーザ端末６０１が、新しい属性に応じたデータを閲覧できる。

また、更新された再暗号化鍵では、古い属性のみで閲覧可能であった（更新されたユーザ属性で閲覧できない）暗号文は、再暗号化できない。そのため、古い属性のみで閲覧可能であったデータを閲覧できない。

つまり、本手続きを実施することで、ユーザ属性の変更に伴う失効処理が実現される。

[0105] 以上のように、実施の形態１に係る暗号システム１０は、（１）～（６）の処理によって、暗号文記憶装置２０１が記憶した暗号文を、ユーザ端末６０１が必要に応じて取得し、権限のあるユーザのみがデータを復号・閲覧できるシステムを実現する。

また、実施の形態１に係る暗号システム１０は、（５）～（６）の処理で説明した通り、ユーザ秘密鍵の紛失・漏えいや、ユーザ属性変更に伴う失効処理を、暗号文記憶装置２０１が記憶した暗号文を更新することなく、再暗号化装置３０１が記憶した再暗号化鍵を更新することで実現できる。そのため、大規模な企業等、失効処理が頻繁に必要となる環境でも効率的に動作させることが可能である。

[0106] また、実施の形態１に係る暗号システム１０は、再暗号化装置３０１が持つ再暗号化鍵が１ユーザあたり１個で済む。したがって、失効処理における再暗号化鍵更新の負荷が小さい。また、実施の形態１に係る暗号システム１０は、関数型暗号の柔軟なアクセス制御を利用することもできる。

[0107] また、実施の形態１に係る暗号システム１０は、暗号文記憶装置２０１と再暗号化装置３０１とを分ける構成をとっている。そのため、失効したユーザ（もしくは、失効したユーザ秘密鍵を入手した攻撃者）と暗号文記憶装置２０１とが結託した場合においても、暗号文記憶装置２０１が記憶した暗号文を復号することはできない。

[0108] なお、上記説明では、属性管理装置５０１やユーザ端末６０１を持つ単一の企業が暗号システム１０を利用する例を示した。しかし、暗号文記憶装置

２０１、再暗号化装置３０１、鍵生成装置４０１の一部または全部を共用し、複数の企業が暗号システム１０を利用できるようにしてもよい。この場合、暗号システム１０の各装置は、企業を一意に識別するための企業ＩＤを別途管理することになる。

[0109] また、上記説明では、各装置の認証や、通信路の暗号化については（一部を除き）記述していないが、必要に応じてこれらを実行するようにしてもよい。これには、パスワードやＰＫＩ（公開鍵基盤）を用いた既存の認証技術や、ＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）通信等の既存の暗号技術が利用できる。

[0110] また、上記説明では、（４）データ取得処理で、暗号文記憶装置２０１が暗号文をユーザ端末６０１に送信する際に、データＩＤに関連付けられた暗号文を無条件に送信した。

しかし、暗号文記憶部２１１が各暗号文の復号条件を記憶しておき、ユーザ端末６０１がデータＩＤとともにユーザ属性を送信するようにしてもよい。そして、暗号文記憶装置２０１が、復号条件とユーザ属性とに基づき、暗号文の復号可否を判定し、復号可能な暗号文のみをユーザ端末６０１に送信するようにしてもよい。但しこの場合、暗号文記憶装置２０１に対して、復号条件やユーザ属性といった余分な情報が開示されることになるため、注意する必要がある。

[0111] また、上記説明では、（４）データ取得処理で、再暗号化装置３０１が再暗号化を行う際に、ユーザ端末６０１を介して暗号文を再暗号化装置３０１に送信した。

しかし、ユーザ端末６０１を介さずに、暗号文記憶装置２０１から再暗号化装置３０１へ暗号文を直接送信するようにしてもよい。さらにこの場合、効率性を高めるために、暗号文記憶装置２０１と再暗号化装置３０１とを１つの装置にまとめることも可能である。但し、これらをまとめることによって、失効したユーザと暗号文記憶装置２０１（及び再暗号化装置３０１）の結託で、暗号文記憶装置２０１が記憶した暗号文を不正に復号できるように

なるため、注意する必要がある。

[0112] また、属性管理装置５０１と再暗号化装置３０１とを１つの装置にまとめることで効率化を図ってもよい。また、属性管理装置５０１と鍵生成装置４０１とを１つの装置にまとめることで効率化を図ってもよい。

[0113] また、上記説明では、運用容易性の観点から、関数型暗号から、（公開パラメータも含め）同一の関数型暗号への再暗号化を行った。

しかし、関数型暗号から、異なる関数型暗号、もしくは関数型暗号以外への再暗号化を行うこともできる。例えば、関数型暗号から、ＩＤベース暗号への再暗号化を行ってもよい。この場合、鍵生成装置４０１は、２種類の暗号の鍵生成機能を持つ（もしくは、鍵生成装置４０１を２個用意する）ことになる。

[0114] また、上記説明では、ユーザ端末６０１がデータ登録とデータ取得との両方の機能を持っていた。

しかし、データ登録のみ行うユーザ装置と、データ取得のみ行うユーザ装置とに分けてもよい。データ登録のみ行うユーザ装置には、ユーザ秘密鍵記憶部６１２は不要である。

[0115] また、上記説明では、ユーザ端末６０１のユーザ秘密鍵記憶部６１２がユーザ秘密鍵を記憶していた。しかし、ユーザ秘密鍵を外部装置（例えばＩＣカード）に記憶し、必要に応じてユーザ端末６０１が外部装置からユーザ秘密鍵を取得するようにしてもよい。また、外部装置が暗号化部や復号部を備え、外部装置側でユーザ秘密鍵を用いた暗号化処理や復号処理を行うようにしてもよい。

[0116] また、上記説明では、関数型暗号として「暗号文ポリシー型の関数型暗号」を利用する場合について説明した。しかし、上述した通り、「鍵ポリシー型の関数型暗号」を利用することも可能である。

例えば、鍵ポリシー型の関数型暗号では、暗号文に属性「所属＝総務部、作成年度＝２０１２年」を設定し、これを復号するための秘密鍵にポリシー（復号条件）「（所属＝総務部　ＡＮＤ　作成年度＝２０１２年）ＯＲ（所

属＝経理部　ＡＮＤ　作成年度＝２０１３年）」を設定することができる。この例では、この秘密鍵を用いて「２０１２年に総務部で作成されたデータ」、及び、「２０１３年に経理部で作成されたデータ」を復号することができる。そのため、ユーザが在籍した時期に対応した文書のみ閲覧可能とする等、ユーザ所属の変更に伴う、より柔軟なアクセス制御が可能となる。

暗号文ポリシー型属性ベース暗号、鍵ポリシー型属性ベース暗号のどちらを利用するのが適しているかは、データ管理システムの用途や、利用する企業の組織構成等に依存する。

[0117] また、「暗号文ポリシー型の関数型暗号」と「鍵ポリシー型の関数型暗号」とを組み合わせたＵｎｉｆｉｅｄポリシー型の関数型暗号を利用することも可能である。Ｕｎｉｆｉｅｄポリシー型の関数型暗号では、暗号文に属性１とポリシー２とが設定され、復号鍵に属性１に対応するポリシー１とポリシー２に対応する属性２とが設定される。これにより、「暗号文ポリシー型の関数型暗号」と「鍵ポリシー型の関数型暗号」との両方の利点を享受することができる。

[0118] 図２９は、実施の形態１に示した暗号文記憶装置２０１、再暗号化装置３０１、鍵生成装置４０１、属性管理装置５０１、ユーザ端末６０１のハードウェア構成の例を示す図である。

暗号文記憶装置２０１、再暗号化装置３０１、鍵生成装置４０１、属性管理装置５０１、ユーザ端末６０１は、コンピュータである。暗号文記憶装置２０１、再暗号化装置３０１、鍵生成装置４０１、属性管理装置５０１、ユーザ端末６０１の各要素をプログラムで実現することができる。

暗号文記憶装置２０１、再暗号化装置３０１、鍵生成装置４０１、属性管理装置５０１、ユーザ端末６０１のハードウェア構成としては、バスに、演算装置９０１、外部記憶装置９０２、主記憶装置９０３、通信装置９０４、入出力装置９０５が接続されている。

[0119] 演算装置９０１は、プログラムを実行するＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）等である。外部記憶装置９０２は、例えばＲ

ＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）やフラッシュメモリ、ハードディスク装置等である。主記憶装置９０３は、例えばＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等である。通信装置９０４は、例えば通信ボード等である。入出力装置９０５は、例えばマウス、キーボード、ディスプレイ装置等である。

[0120] プログラムは、通常は外部記憶装置９０２に記憶されており、主記憶装置９０３にロードされた状態で、順次演算装置９０１に読み込まれ、実行される。

プログラムは、通信部２３１、再暗号化部３２１、通信部３３１、鍵生成部４２１、認証部４２２、通信部４３１、認証部５２１、登録部５２２、通信部５３１、暗号化部６２１、復号部６２２、通信部６３１として説明している機能を実現するプログラムである。

更に、外部記憶装置９０２にはオペレーティングシステム（ＯＳ）も記憶されており、ＯＳの少なくとも一部が主記憶装置９０３にロードされ、演算装置９０１はＯＳを実行しながら、上記プログラムを実行する。

また、実施の形態１の説明において、暗号文記憶部２１１、公開パラメータ記憶部３１１、再暗号化鍵記憶部３１２、マスタ鍵情報記憶部４１１、鍵情報記憶部４１２、認証情報記憶部４１３、属性情報記憶部５１１、認証情報記憶部５１２、公開パラメータ記憶部６１１、ユーザ秘密鍵記憶部６１２が記憶すると説明した情報やデータや信号値や変数値が主記憶装置９０３にファイルとして記憶されている。

[0121] なお、図２９の構成は、あくまでも暗号文記憶装置２０１、再暗号化装置３０１、鍵生成装置４０１、属性管理装置５０１、ユーザ端末６０１のハードウェア構成の一例を示すものであり、暗号文記憶装置２０１、再暗号化装置３０１、鍵生成装置４０１、属性管理装置５０１、ユーザ端末６０１のハードウェア構成は図２９に記載の構成に限らず、他の構成であってもよい。

符号の説明

[0122] １０　暗号システム、１０１　ネットワーク、２０１　暗号文記憶装置、

２１１　暗号文記憶部、２３１　通信部、３０１　再暗号化装置、３１１　公開パラメータ記憶部、３１２　再暗号化鍵記憶部、３２１　再暗号化部、３３１　通信部、４０１　鍵生成装置、４１１　マスタ鍵情報記憶部、４１２　鍵情報記憶部、４１３　認証情報記憶部、４２１　鍵生成部、４２２　認証部、４３１　通信部、５０１　属性管理装置、５１１　属性情報記憶部、５１２　認証情報記憶部、５２１　認証部、５２２　登録部、５３１　通信部、６０１　ユーザ端末、６１１　公開パラメータ記憶部、６１２　ユーザ秘密鍵記憶部、６２１　暗号化部、６２２　復号部、６３１　通信部。

請求の範囲

[請求項1] ２つの情報が互いに対応している場合に一方の情報が設定された暗号文を他方の情報が設定された復号鍵により復号可能な暗号方式を用いた暗号システムであり、

互いに対応する鍵情報ｕ，ｙの一方が設定されたユーザ秘密鍵と、互いに対応するユーザ属性情報ｘ，ｖの一方が設定された属性秘密鍵で復号可能な暗号文を前記鍵情報ｕ，ｙの他方が設定された再暗号文に変換する再暗号化鍵とを生成する鍵生成装置と、

前記ユーザ属性情報ｘ，ｖの他方が設定された暗号文を記憶する暗号文記憶装置と、

前記鍵生成装置が生成した前記再暗号化鍵で、前記暗号文記憶装置が記憶する前記暗号文を再暗号化して再暗号文を生成する再暗号化装置と、

前記鍵生成装置が生成した前記ユーザ秘密鍵で、前記再暗号化装置が再暗号化した前記再暗号文を復号するユーザ端末と

を備えることを特徴とする暗号システム。

[請求項2] 前記鍵生成装置は、前記ユーザ秘密鍵を失効させる場合、互いに対応する新しい鍵情報ｕ’，ｙ’の一方が設定された新しいユーザ秘密鍵と、前記属性秘密鍵で復号可能な暗号文を前記鍵情報ｕ’，ｙ’の他方が設定された再暗号文に変換する新しい再暗号化鍵とを生成し、

前記再暗号化装置は、前記新しい再暗号化鍵が生成された後は、前記新しい再暗号化鍵で、前記暗号文記憶装置が記憶する暗号文を再暗号化して再暗号文を生成する

ことを特徴とする請求項１に記載の暗号システム。

[請求項3] 前記鍵生成装置は、ユーザの属性が変更された場合、互いに対応する新しいユーザ属性情報ｘ’，ｖ’の一方が設定された新しい属性秘密鍵で復号可能な暗号文を前記鍵情報ｕ，ｙの他方が設定された再暗号文に変換する新しい再暗号化鍵を生成し、

前記再暗号化装置は、前記新しい再暗号化鍵が生成された後は、前記新しい再暗号化鍵で、前記暗号文記憶装置が記憶する暗号文を再暗号化して再暗号文を生成する

ことを特徴とする請求項１に記載の暗号システム。

[請求項4] 前記鍵生成装置は、ユーザ毎に、前記ユーザ秘密鍵と前記再暗号化鍵とを生成し、

前記再暗号化装置は、前記ユーザ端末からユーザの識別情報を受信すると、受信した識別情報が示すユーザに対応する再暗号化鍵で、前記暗号文記憶装置が記憶する暗号文を再暗号化する

ことを特徴とする請求項１に記載の暗号システム。

[請求項5] ２つの情報が互いに対応している場合に一方の情報が設定された暗号文を他方の情報が設定された復号鍵により復号可能な暗号方式を用いた暗号システムにおける鍵生成装置であり、

互いに対応する鍵情報ｕ，ｙの一方が設定されたユーザ秘密鍵と、互いに対応するユーザ属性情報ｘ，ｖの一方が設定された属性秘密鍵で復号可能な暗号文を前記鍵情報ｕ，ｙの他方が設定された再暗号文に変換する再暗号化鍵とを生成する鍵生成部と、

前記鍵生成部が生成したユーザ秘密鍵をユーザ端末へ送信するとともに、前記鍵生成部が生成した再暗号化鍵を再暗号化装置へ送信する通信部と

を備えることを特徴とする鍵生成装置。

[請求項6] ２つの情報が互いに対応している場合に一方の情報が設定された暗号文を他方の情報が設定された復号鍵により復号可能な暗号方式を用いた暗号システムにおける再暗号化装置であり、

ユーザの識別情報毎に、互いに対応するユーザ属性情報ｘ，ｖの一方が設定された属性秘密鍵で復号可能な暗号文を互いに対応する鍵情報ｕ，ｙの一方が設定された再暗号文に変換する再暗号化鍵を記憶する再暗号化鍵記憶部と、

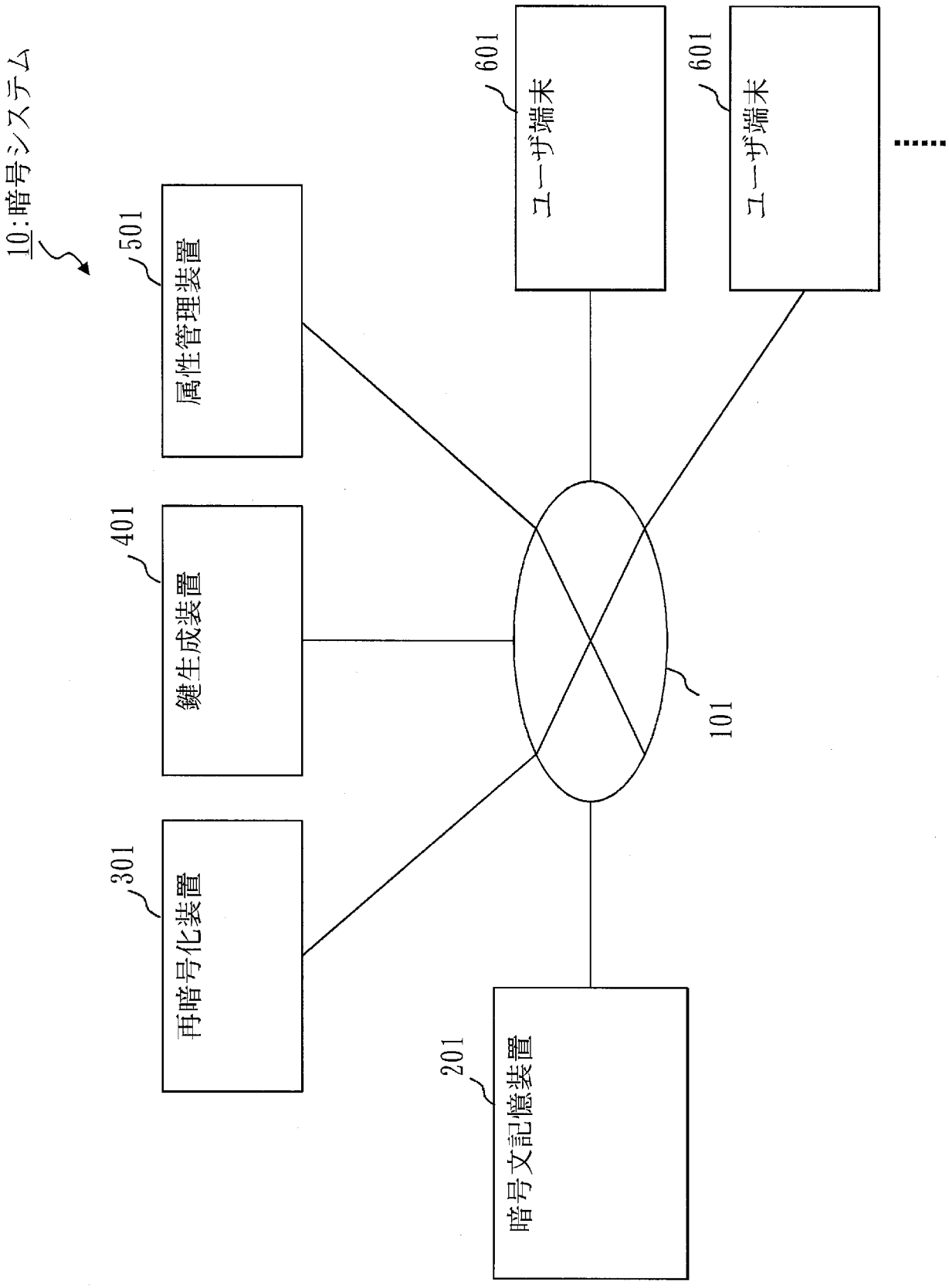
ユーザの識別情報と暗号文とを受信すると、受信したユーザの識別情報に対応して前記再暗号化鍵記憶部が記憶した再暗号化鍵で、受信した暗号文を再暗号化して再暗号文を生成する再暗号化部と
を備えることを特徴とする再暗号化装置。

[請求項7] ２つの情報が互いに対応している場合に一方の情報が設定された暗号文を他方の情報が設定された復号鍵により復号可能な暗号方式を用いた暗号システムにおけるユーザ端末であり、

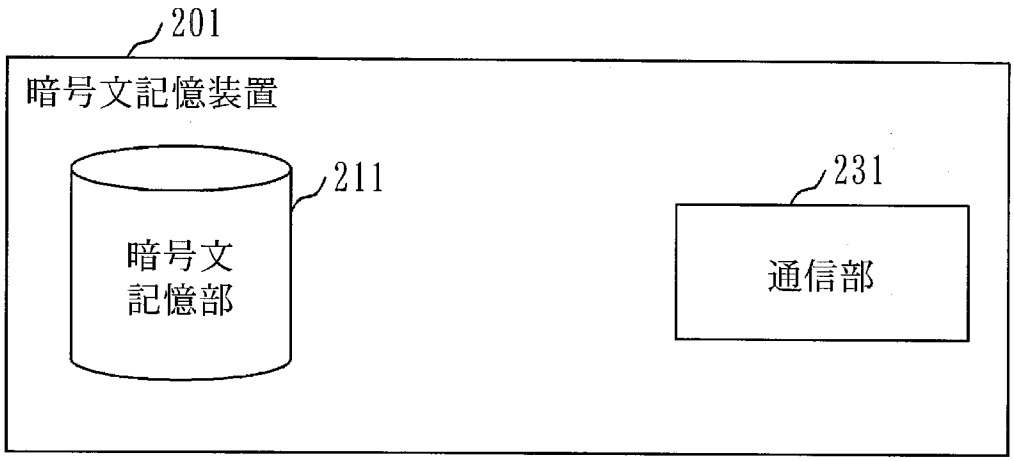
互いに対応するユーザ属性情報ｘ，ｖの一方が設定された暗号文が再暗号化された再暗号文であって、互いに対応する鍵情報ｕ，ｙの一方が設定された再暗号文を受信する通信部と、

前記鍵情報ｕ，ｙの他方が設定されたユーザ秘密鍵で、前記通信部が受信した再暗号文を復号する復号部と
を備えることを特徴とするユーザ端末。

[図1]


10:暗号システム
501
属性管理装置
401
鍵生成装置
301
再暗号化装置
201
暗号文記憶装置
101
601
ユーザ端末
601
ユーザ端末
.....

[図2]

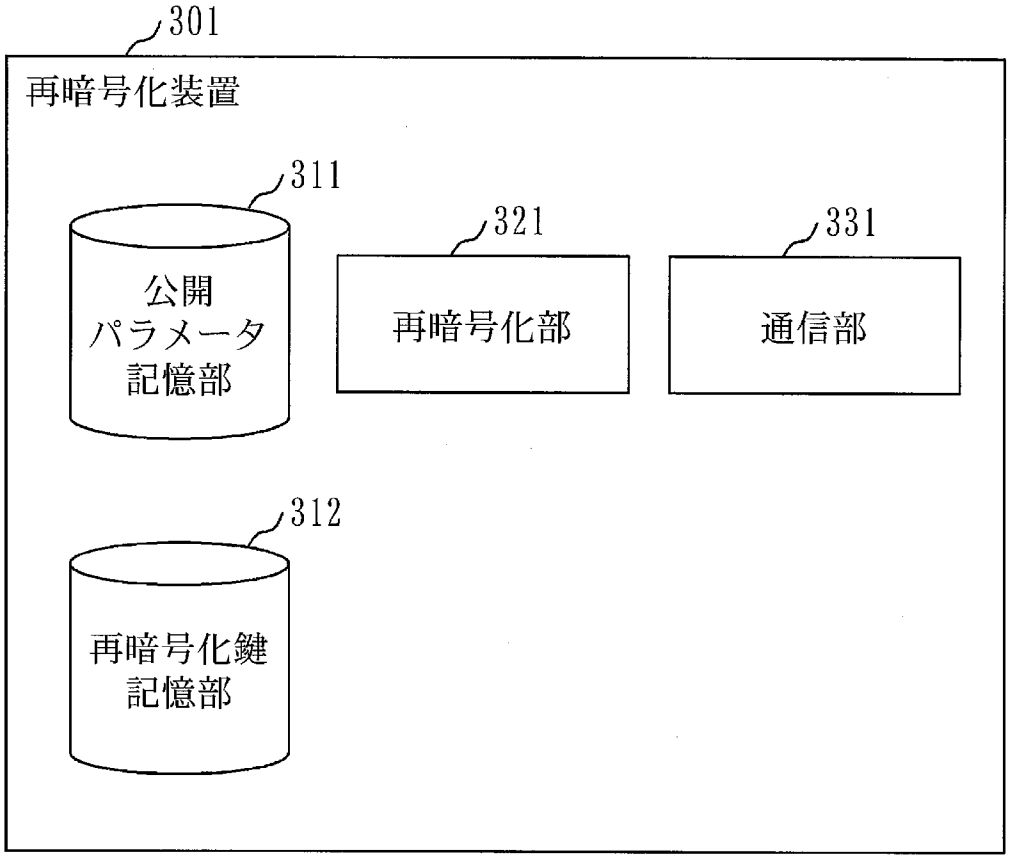


[図3]

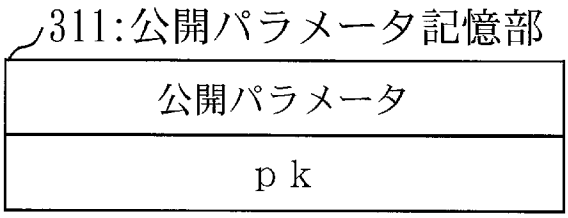
211:暗号文記憶部

データID	暗号化データ
did_1	c_1
did_2	c_2
did_3	c_3
did_4	c_4
did_5	c_5
:	:
:	:

[図4]


301
再暗号化装置
311
公開
パラメータ
記憶部
321
再暗号化部
331
通信部
312
再暗号化鍵
記憶部

[図5]

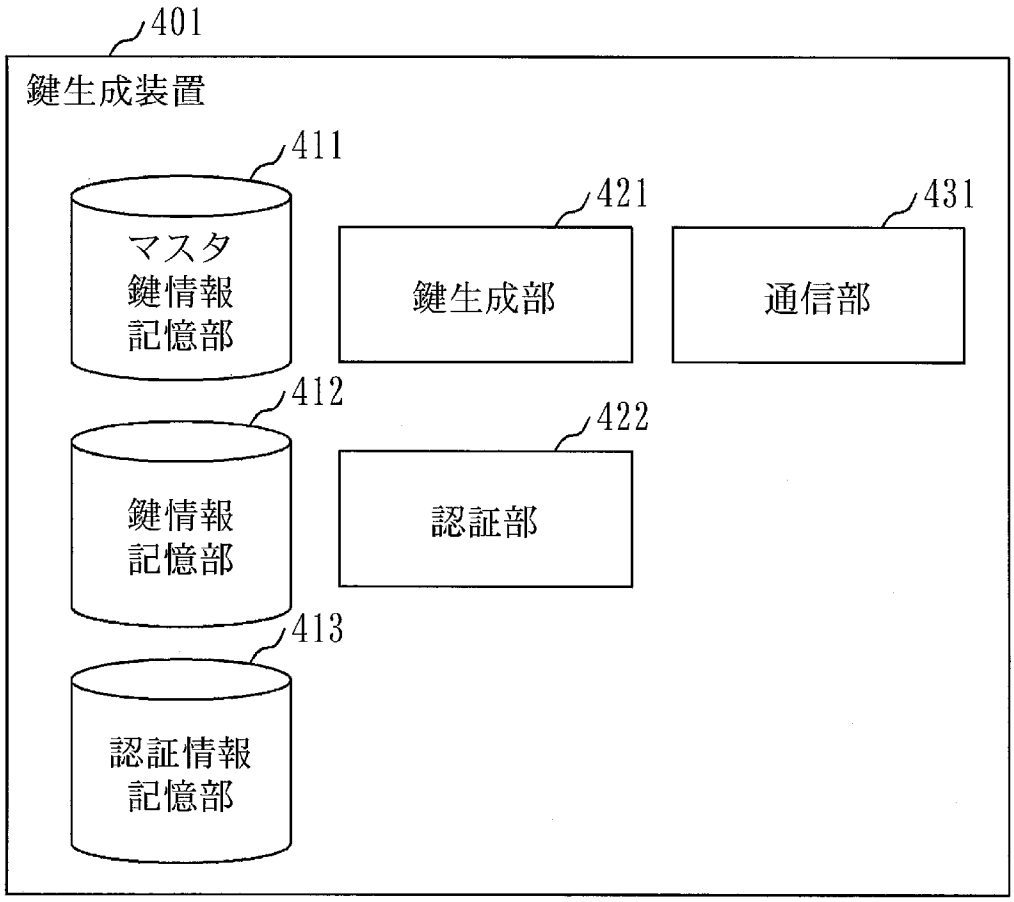

311:公開パラメータ記憶部
公開パラメータ
ｐｋ

[図6]

312:再暗号化鍵記憶部

ユーザID	再暗号化鍵
uid_1	rk_1
uid_2	rk_2
uid_3	rk_3
uid_4	rk_4
uid_5	rk_5
:	:
:	:

[図7]



[図8]

411:マスタ鍵情報記憶部

マスタ秘密鍵	公開パラメータ
ｍｓｋ	ｐｋ

[図9]

412:鍵情報記憶部

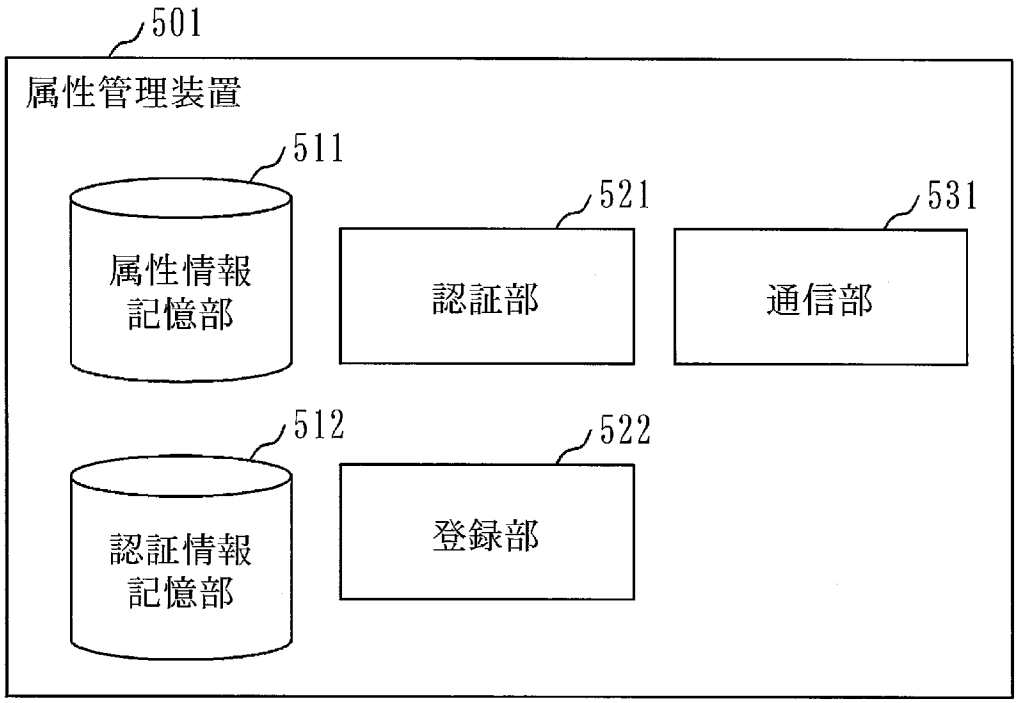
ユーザID	属性秘密鍵	ユーザ秘密鍵ID	ステータス
uid_1	sk_1	$ukid_1$	有効
uid_2	sk_2	$ukid_2$	有効
uid_3	sk_3	$ukid_3$	有効
uid_4	sk_4	$ukid_4$	有効
uid_5	sk_5	$ukid_5$	有効
:	:	:	:
:	:	:	:

[図10]

413:認証情報記憶部

属性管理装置ID	パスワード
ｄｅｖ＿ｉｄ	ｐａｓｓｗｄ

[図11]



[図12]

511:属性情報記憶部

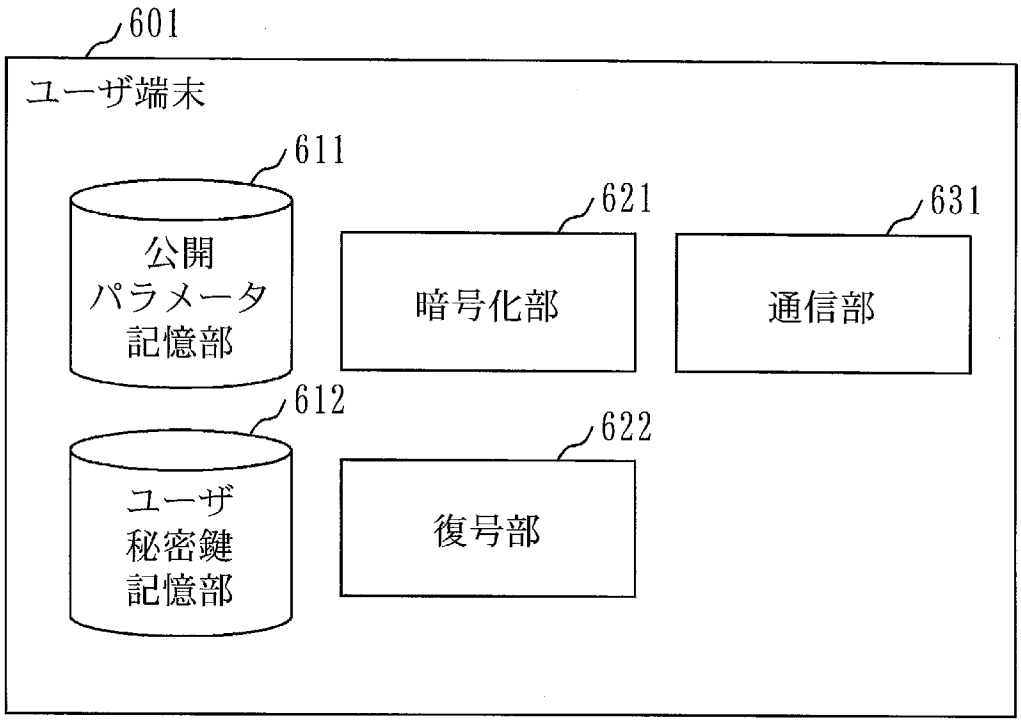
ユーザID	ユーザ属性
uid_1	所属＝総務部、役職＝部長、氏名＝高橋太郎
uid_2	所属＝総務部、役職＝課長、氏名＝佐藤花子
uid_3	所属＝総務部、役職＝担当、氏名＝田中正一
uid_4	所属＝経理部、役職＝部長、氏名＝佐藤和夫
uid_5	所属＝経理部、役職＝担当、氏名＝渡辺量子
:	:
:	:

[図13]

512:認証情報記憶部

属性管理装置ID	パスワード
dev_id	passwd

[図14]



[図15]

611:公開パラメータ記憶部

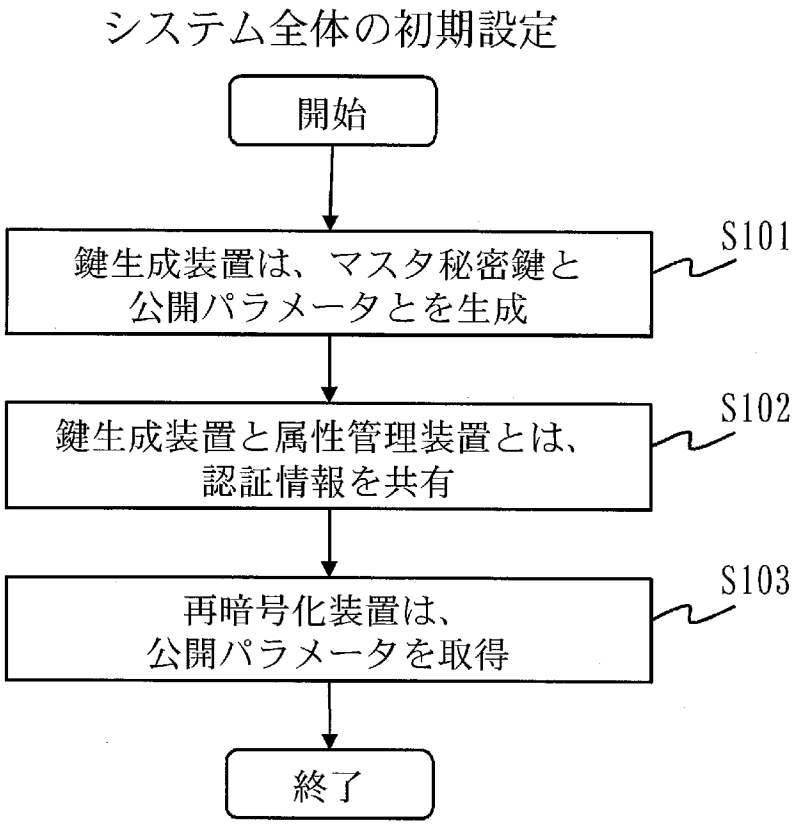
公開パラメータ
ｐｋ

[図16]

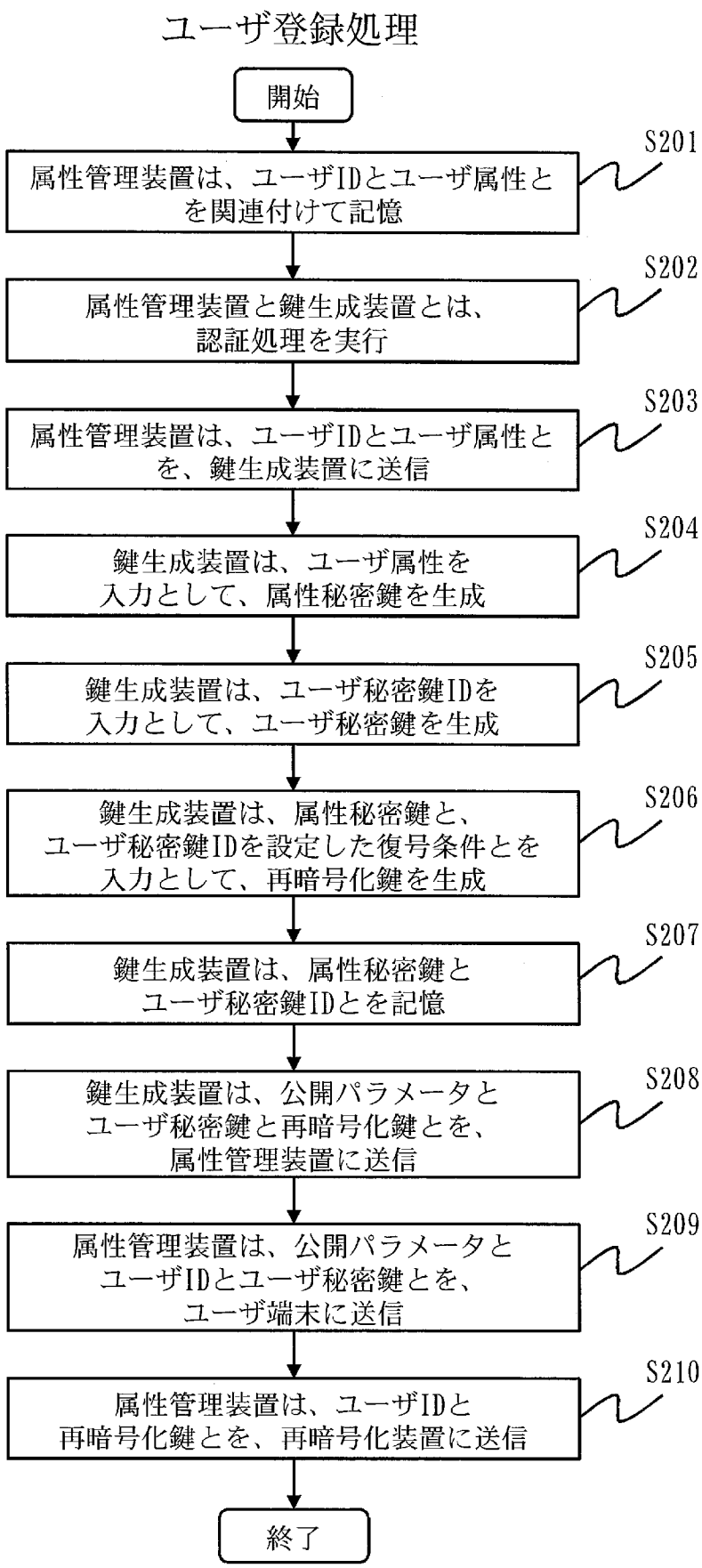
612:ユーザ秘密鍵記憶部

ユーザID	ユーザ秘密鍵
uid_2	uk_2

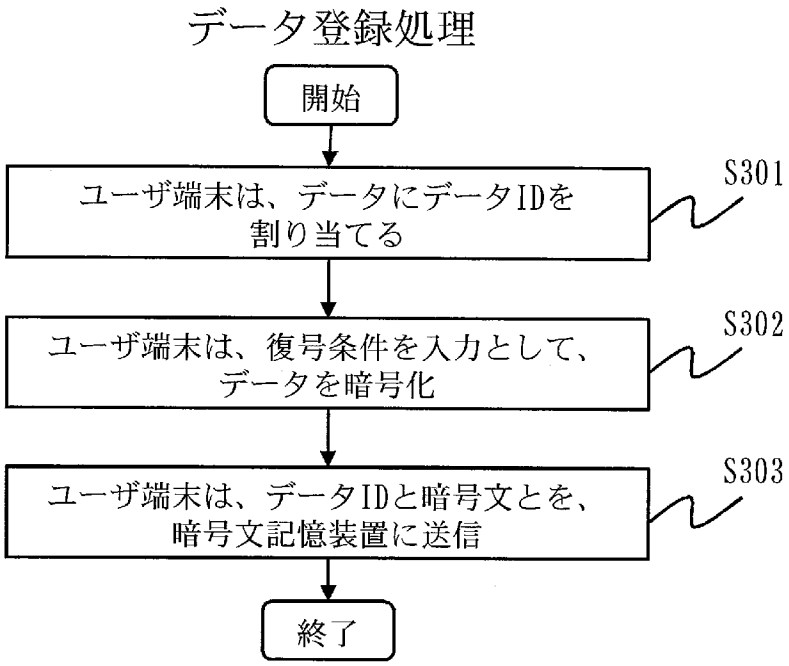
[図17]


システム全体の初期設定
開始
鍵生成装置は、マスタ秘密鍵と
公開パラメータとを生成
S101
鍵生成装置と属性管理装置とは、
認証情報を共有
S102
再暗号化装置は、
公開パラメータを取得
S103
終了

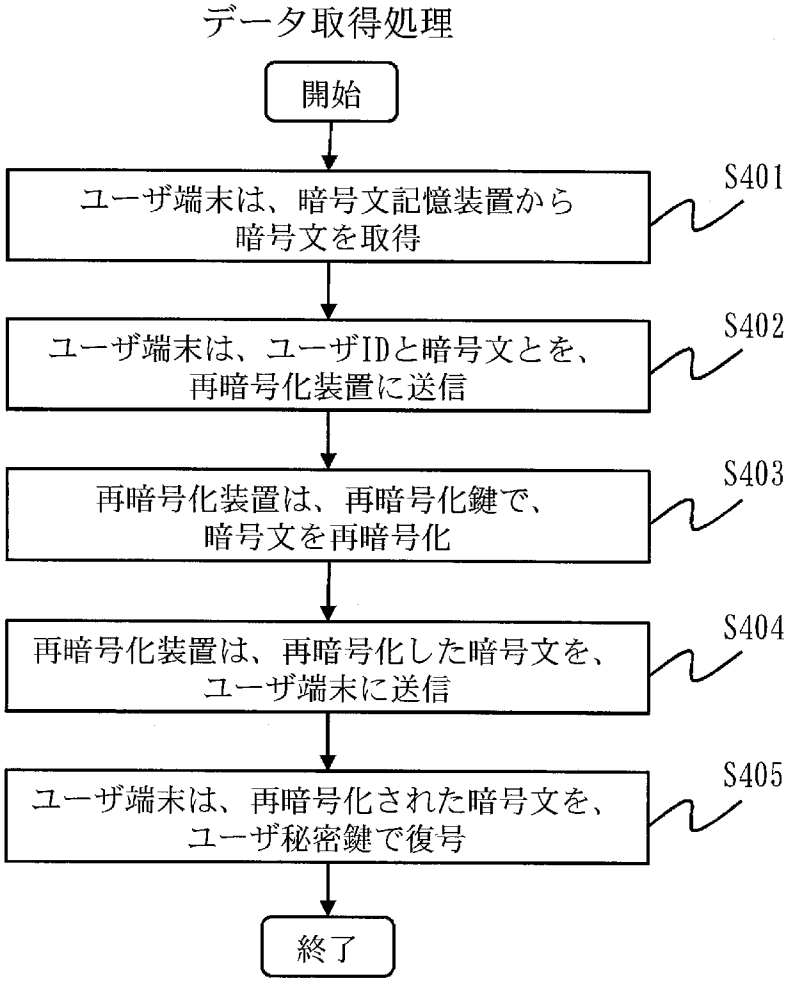
[図18]


ユーザ登録処理
開始
S201
属性管理装置は、ユーザIDとユーザ属性とを関連付けて記憶
S202
属性管理装置と鍵生成装置とは、認証処理を実行
S203
属性管理装置は、ユーザIDとユーザ属性とを、鍵生成装置に送信
S204
鍵生成装置は、ユーザ属性を入力として、属性秘密鍵を生成
S205
鍵生成装置は、ユーザ秘密鍵IDを入力として、ユーザ秘密鍵を生成
S206
鍵生成装置は、属性秘密鍵と、ユーザ秘密鍵IDを設定した復号条件とを入力として、再暗号化鍵を生成
S207
鍵生成装置は、属性秘密鍵とユーザ秘密鍵IDとを記憶
S208
鍵生成装置は、公開パラメータとユーザ秘密鍵と再暗号化鍵とを、属性管理装置に送信
S209
属性管理装置は、公開パラメータとユーザIDとユーザ秘密鍵とを、ユーザ端末に送信
S210
属性管理装置は、ユーザIDと再暗号化鍵とを、再暗号化装置に送信
終了

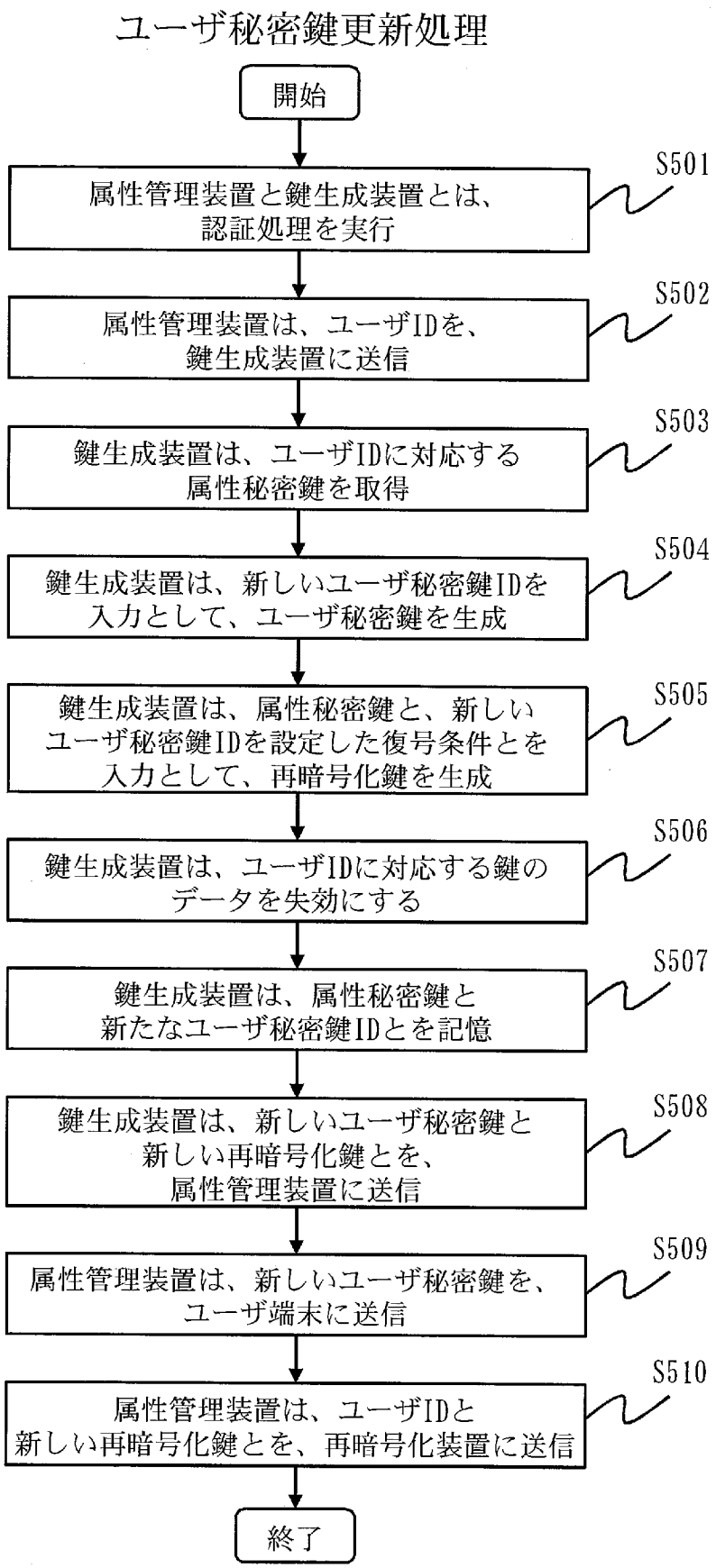
[図19]


データ登録処理
開始
ユーザ端末は、データにデータIDを割り当てる
S301
ユーザ端末は、復号条件を入力として、データを暗号化
S302
ユーザ端末は、データIDと暗号文とを、暗号文記憶装置に送信
S303
終了

[図20]


データ取得処理
開始
ユーザ端末は、暗号文記憶装置から暗号文を取得
S401
ユーザ端末は、ユーザIDと暗号文とを、再暗号化装置に送信
S402
再暗号化装置は、再暗号化鍵で、暗号文を再暗号化
S403
再暗号化装置は、再暗号化した暗号文を、ユーザ端末に送信
S404
ユーザ端末は、再暗号化された暗号文を、ユーザ秘密鍵で復号
S405
終了

[図21]


ユーザ秘密鍵更新処理
開始
属性管理装置と鍵生成装置とは、認証処理を実行
S501
属性管理装置は、ユーザIDを、鍵生成装置に送信
S502
鍵生成装置は、ユーザIDに対応する属性秘密鍵を取得
S503
鍵生成装置は、新しいユーザ秘密鍵IDを入力として、ユーザ秘密鍵を生成
S504
鍵生成装置は、属性秘密鍵と、新しいユーザ秘密鍵IDを設定した復号条件とを入力として、再暗号化鍵を生成
S505
鍵生成装置は、ユーザIDに対応する鍵のデータを失効にする
S506
鍵生成装置は、属性秘密鍵と新たなユーザ秘密鍵IDとを記憶
S507
鍵生成装置は、新しいユーザ秘密鍵と新しい再暗号化鍵とを、属性管理装置に送信
S508
属性管理装置は、新しいユーザ秘密鍵を、ユーザ端末に送信
S509
属性管理装置は、ユーザIDと新しい再暗号化鍵とを、再暗号化装置に送信
S510
終了

[図22]

412:鍵情報記憶部

ユーザＩＤ	属性秘密鍵	ユーザ秘密鍵ID	ステータス
uid_1	sk_1	$ukid_1$	有効
uid_2	sk_2	$ukid_2$	失効
uid_2	sk_2	$ukid_{102}$	有効
uid_3	sk_3	$ukid_3$	有効
uid_4	sk_4	$ukid_4$	有効
uid_5	sk_5	$ukid_5$	有効
:	:	:	:
:	:	:	:

[図23]

612:ユーザ秘密鍵記憶部

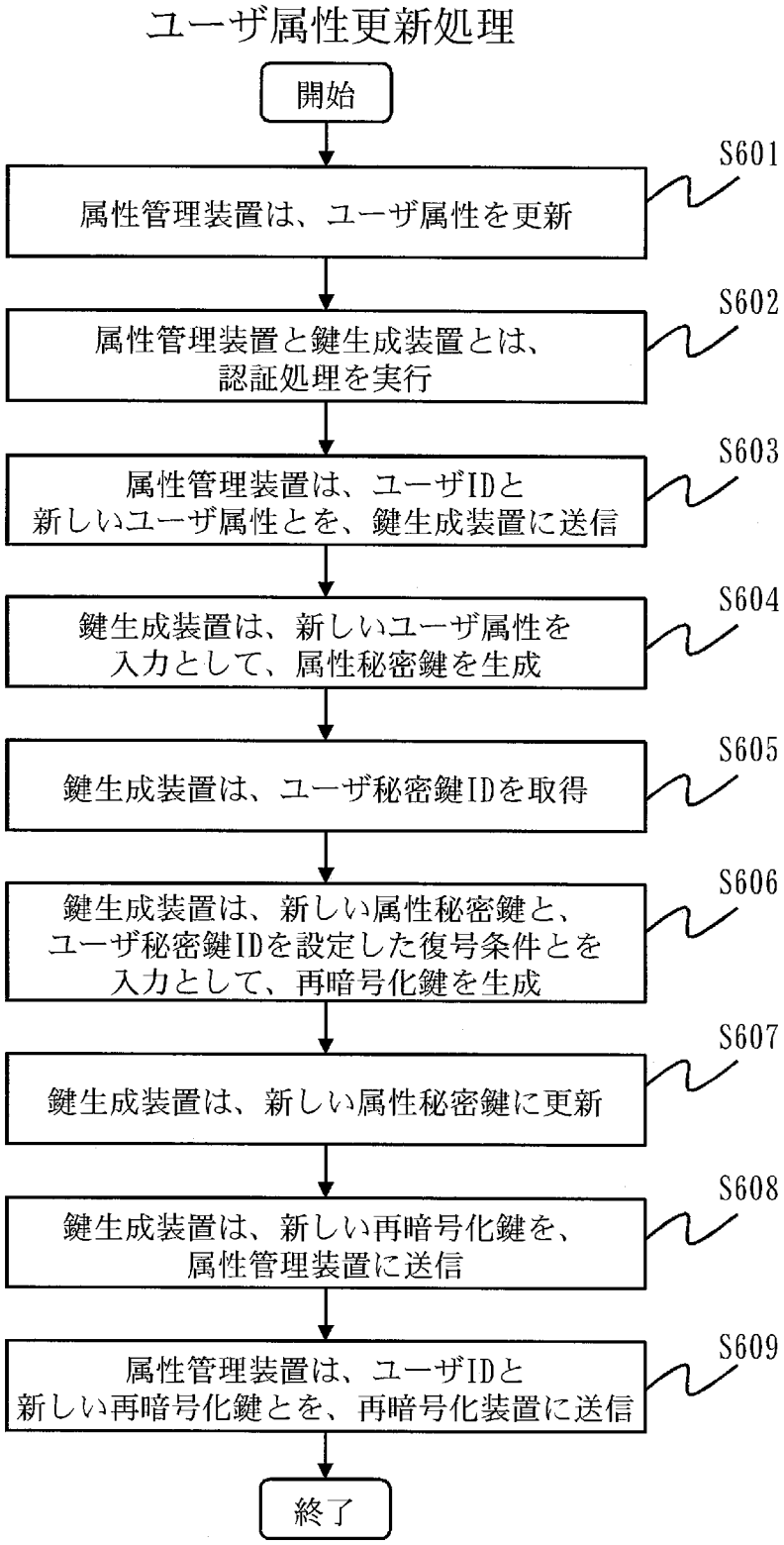
ユーザID	ユーザ秘密鍵
uid_2	uk_{102}

[図24]

312:再暗号化鍵記憶部

ユーザID	再暗号化鍵
uid_1	rk_1
uid_2	rk_{102}
uid_3	rk_3
uid_4	rk_4
uid_5	rk_5
:	:
:	:

[図25]


ユーザ属性更新処理
開始
S601
属性管理装置は、ユーザ属性を更新
S602
属性管理装置と鍵生成装置とは、
認証処理を実行
S603
属性管理装置は、ユーザIDと
新しいユーザ属性とを、鍵生成装置に送信
S604
鍵生成装置は、新しいユーザ属性を
入力として、属性秘密鍵を生成
S605
鍵生成装置は、ユーザ秘密鍵IDを取得
S606
鍵生成装置は、新しい属性秘密鍵と、
ユーザ秘密鍵IDを設定した復号条件とを
入力として、再暗号化鍵を生成
S607
鍵生成装置は、新しい属性秘密鍵に更新
S608
鍵生成装置は、新しい再暗号化鍵を、
属性管理装置に送信
S609
属性管理装置は、ユーザIDと
新しい再暗号化鍵とを、再暗号化装置に送信
終了

[図26]

511:属性情報記憶部

ユーザID	ユーザ属性
uid_1	所属＝総務部、役職＝部長、氏名＝高橋太郎
uid_2	所属＝経理部、役職＝課長、氏名＝佐藤花子
uid_3	所属＝総務部、役職＝担当、氏名＝田中正一
uid_4	所属＝経理部、役職＝部長、氏名＝佐藤和夫
uid_5	所属＝経理部、役職＝担当、氏名＝渡辺量子
:	:
:	:

[図27]

412:鍵情報記憶部

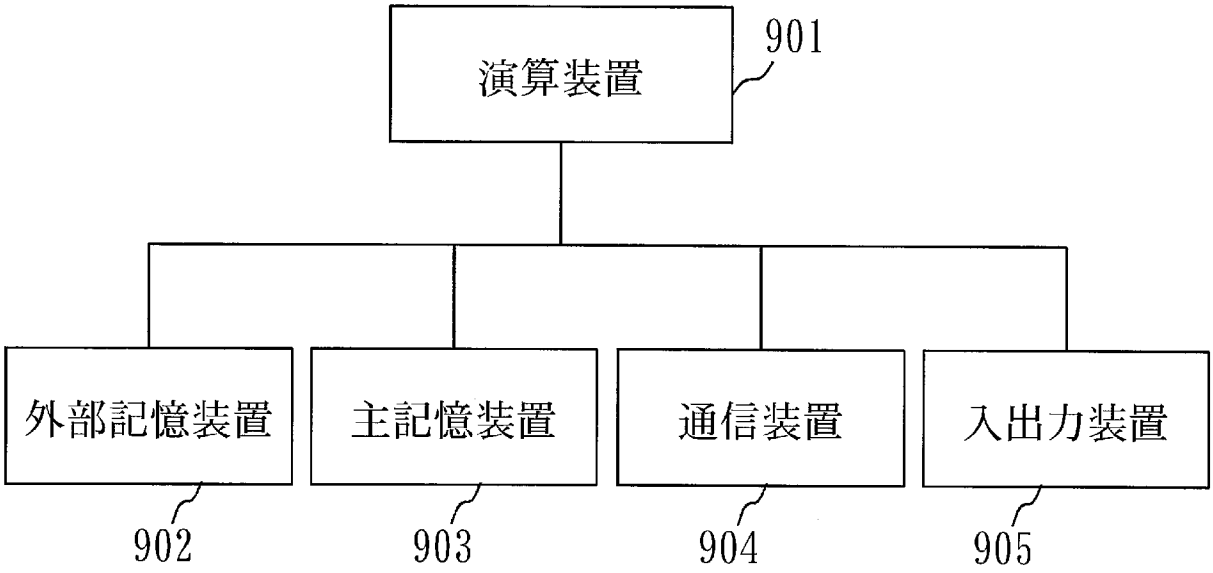
ユーザID	属性秘密鍵	ユーザ秘密鍵ID	ステータス
uid_1	sk_1	$ukid_1$	有効
uid_2	sk_{202}	$ukid_2$	有効
uid_3	sk_3	$ukid_3$	有効
uid_4	sk_4	$ukid_4$	有効
uid_5	sk_5	$ukid_5$	有効
:	:	:	:
:	:	:	:

[図28]

312:再暗号化鍵記憶部

ユーザID	再暗号化鍵
uid_1	rk_1
uid_2	rk_{202}
uid_3	rk_3
uid_4	rk_4
uid_5	rk_5
:	:
:	:

[図29]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/050626

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	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

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	Takeshi NARUSE, "Zenpo Hitokusei o Mitasu Zokusei Shikko Kino Tsuki Zokusei Base Ango", Symposium on Multimedia, Distributed, Cooperative and Mobile Systems (DICOMO213) Ronbunshu, IPSJ Symposium Series, vol.2013, no.2 [CD-ROM], 03 July 2013 (03.07.2013), pages 215 to 221	1-7
A	Yukihiro ICHIKAWA, "Shikko o Koryo shita Kansu-gata Ango System", 2012 Nen Symposium on Cryptography and Information Security Yokoshu [CD-ROM], 30 January 2012 (30.01.2012), pages 1 to 7	1-7

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

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

Date of the actual completion of the international search	Date of mailing of the international search report
07 March, 2014 (07.03.14)	18 March, 2014 (18.03.14)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/050626

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Takeshi NARUSE, "Koshin-yo no Zokusei Kagi to Proxy Sai Angoka ni yori Zokusei Shikko Shori o Bunsan saseru Zokusei Base Ango", Dai 75 Kai (Heisei 25 Nen) Zenkoku Taikai Koen Ronbunshu (3), 06 March 2013 (06.03.2013), pages 3-521 to 3-522	1-7
A	WO 2010/123122 A1 (Nippon Telegraph and Telephone Corp.), 28 October 2010 (28.10.2010), entire text; all drawings & JP 5253567 B & US 2012/0027210 A1 & EP 2424156 A1 & CN 102369687 A & KR 10-2011-0134900 A	1-7
A	WO 2013/094018 A1 (Mitsubishi Electric Corp.), 27 June 2013 (27.06.2013), entire text; all drawings (Family: none)	1-7

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１４／０５０６２６

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	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１４年
日本国実用新案登録公報	１９９６－２０１４年
日本国登録実用新案公報	１９９４－２０１４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	成瀬 猛，前方秘匿性を満たす属性失効機能付き属性ベース暗号，マルチメディア，分散，協調とモバイル（DICOMO213）シンポジウム論文集　情報処理学会シンポジウムシリーズ　Vol.2013　No.2 [CD-ROM]，2013.07.03，p.215-221	1-7
A	市川 幸宏，失効を考慮した関数型暗号システム，2012年 暗号と情報セキュリティシンポジウム予稿集 [CD-ROM]，2012.01.30，p.1-7	1-7

☑　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
０７．０３．２０１４	１８．０３．２０１４

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　９４６９
石田　信行
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	成瀬 猛, 更新用の属性鍵とプロキシ再暗号化により属性失効処理を分散させる属性ベース暗号, 第75回（平成25年）全国大会講演論文集（3）, 2013.03.06, p.3-521～3-522	1-7
A	WO 2010/123122 A1（日本電信電話株式会社）2010.10.28, 全文, 全図 & JP 5253567 B & US 2012/0027210 A1 & EP 2424156 A1 & CN 102369687 A & KR 10-2011-0134900 A	1-7
A	WO 2013/094018 A1（三菱電機株式会社）2013.06.27, 全文, 全図 (ファミリーなし)	1-7