(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
2022年12月29日(29.12.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/269914 A1

(51) 国際特許分類:
G06F 21/32 (2013.01)

(21) 国際出願番号： PCT/JP2021/024182

(22) 国際出願日： 2021年6月25日(25.06.2021)

(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: 日本電気株式会社 (**NEC CORPORATION**) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者: 森 健吾(**MORI, Kengo**); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 一色 寿幸(**ISSHIKI, Toshiyuki**); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 中川 紗菜美(**NAKAGAWA, Sanami**); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 田宮 寛人(**TAMIYA, Hiroto**); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP). 奈良 成泰(**NARA, Masahiro**); 〒1088001 東京都港区芝五丁目７番１号 日本電気株式会社内 Tokyo (JP).

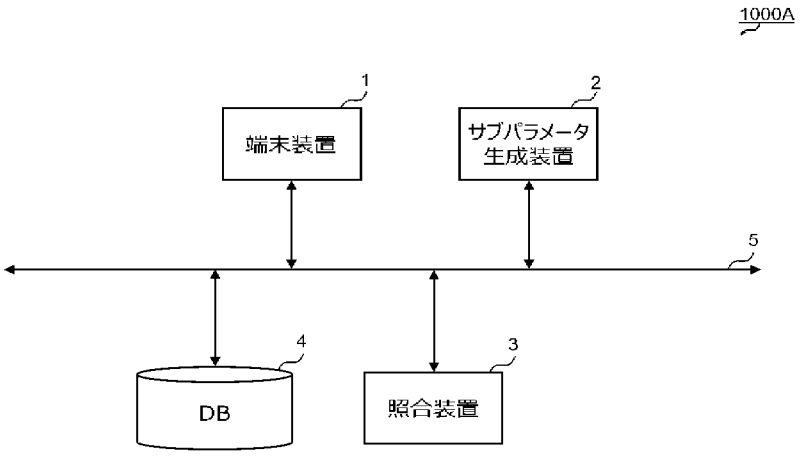
(74) 代理人: 梶田 邦之 (**KAJITA, Kuniyuki**); 〒2110005 神奈川県川崎市中原区新丸子町９１５ 武蔵小杉フコク生命ビル４階 Kanagawa (JP).

(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,

(54) **Title:** TERMINAL DEVICE, ENCRYPTED INFORMATION CONVERSION DEVICE, COLLATION SYSTEM, INPUT INFORMATION ENCRYPTION METHOD, ENCRYPTED INFORMATION CONVERSION METHOD, COLLATION METHOD, INPUT INFORMATION ENCRYPTION PROGRAM, AND ENCRYPTED INFORMATION CONVERSION PROGRAM

(54) 発明の名称： 端末装置、暗号化情報変換装置、照合システム、入力情報暗号化方法、暗号化情報変換方法、照合方法、入力情報暗号化プログラム、及び暗号化情報変換プログラム

Fig. 1



1 Terminal device
2 Sub-parameter generation device
3 Collation device

(57) **Abstract:** [Probem] To achieve encryption processing that can suppress degradation of collation precision and reduce the risk of information leakage. [Solution] A terminal device (1A) that encrypts input information that is inputted for

WO 2022/269914 A1

[続葉有]

BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

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

添付公開書類:

— 国際調査報告(条約第21条(3))

collation: performs conversion parameter generation processing that generates a conversion parameter on the basis of a first parameter that is stored in a storage area and a second parameter that is different from the first parameter; and generates encrypted input information by using the conversion parameter to encrypt the input information that is inputted for collation.

(57) 要約:【課題】照合精度の劣化の抑制と情報の漏洩リスクの低減とを両立可能な暗号化処理を実現する。【解決手段】照合のために入力される入力情報を暗号化する端末装置(１Ａ)であって、記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行い、照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成する。

明　細　書

発明の名称 ：

端末装置、暗号化情報変換装置、照合システム、入力情報暗号化方法、暗号化情報変換方法、照合方法、入力情報暗号化プログラム、及び暗号化情報変換プログラム

技術分野

[0001] 本発明は、端末装置、暗号化情報変換装置、照合システム、入力情報暗号化方法、暗号化情報変換方法、照合方法、入力情報暗号化プログラム、及び暗号化情報変換プログラムに関する。

背景技術

[0002] 近年、ユーザ認証方式のひとつとして、指紋、静脈、虹彩、及び顔画像等の生体情報を照合することにより認証を行う生体認証技術が広く用いられている。生体認証技術においては、ユーザの生体情報から特徴量を抽出して登録情報として保存し、認証に際し入力されたユーザの生体情報の特徴量と登録情報とを照合して認証可否が判断される。

[0003] 生体認証技術は、ＩＣカード等を利用した認証技術と比較して、紛失及び盗難のリスクが少ないといった利点がある一方で、生体情報が漏洩した場合であっても、生体情報の破棄及び更新を行うことができない。つまり、生体情報の漏洩は、漏洩した生体情報に係る生体の個人情報に関する問題だけではなく、漏洩した生体情報に係る生体の生体情報を用いる認証システムのセキュリティ性を損なうという問題がある。

[0004] このような問題に対して、ユーザの生体情報の保護を目的として、登録情報を無効化することが可能な「キャンセラブルバイオメトリクス」と呼ばれる技術が提案されている。

[0005] キャンセラブルバイオメトリクスでは、生体情報から抽出した特徴量の要素を、秘密鍵を用いて並び替えることにより暗号化し、登録情報を生成する。また、認証時に入力された生体情報から抽出された特徴量の要素に対して

も、登録時と同じ秘密鍵を用いて暗号化を行うことにより照合情報を生成する。つまり、登録情報を作り変える際には、異なる秘密鍵を用いることにより、生成済みの登録情報を無効化することが可能となる。キャンセラブルバイオメトリクスにおける暗号化は、このような登録情報の性質から、「キャンセラブル変換」と称される。キャンセラブル変換として、例えば、非特許文献１には、指紋等から得られた特徴点の画像をブロック分割して、秘密鍵を用いて分割した画像の並びを入れ替えることにより、登録情報及び照合情報を生成する方法が提案されている。

先行技術文献

非特許文献

[0006] 非特許文献1：Ｎ．Ｋ．Ｒａｔｈａ，ｅｔ　ａｌ．，“Ｅｎｈａｎｃｉｎｇ　ｓｅｃｕｒｉｔｙ　ａｎｄ　ｐｒｉｖａｃｙ　ｉｎ　ｂｉｏｍｅｔｒｉｃｓ－ｂａｓｅｄ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｓｙｓｔｅｍｓ”，ＩＢＭ　Ｓｙｓｔｅｍｓ　Ｊｏｕｒｎａｌ　４０（３），６１４－６３４，２００１

発明の概要

発明が解決しようとする課題

[0007] 上述したように、キャンセラブル変換では、登録時と照合時とにおいて同じ秘密鍵を用いて、生体情報から抽出した特徴量の要素の変換が行われる。したがって、生体情報の漏洩リスクを低減するには、キャンセラブル変換されたままの状態で登録情報と照合情報とを照合することが望ましい。また、登録情報と照合情報とを照合する場合に、従来の生体認証技術と同程度の照合精度が得られるように、キャンセラブル変換を行うことが望ましい。

[0008] 本発明の目的は、上記課題を鑑みてなされたものであり、照合精度の劣化の抑制と情報の漏洩リスクの低減とを両立可能な暗号化処理を実現する端末装置、暗号化情報変換装置、照合システム、入力情報暗号化方法、暗号化情報変換方法、照合方法、入力情報暗号化プログラム、及び暗号化情報変換プ

ログラムを提供することである。

課題を解決するための手段

[0009] 本発明の端末装置は、照合のために入力される入力情報を暗号化する端末装置であって、第１パラメータを記憶する端末側記憶領域と、第２パラメータを取得する端末側取得部と、前記第１パラメータと前記第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行う変換パラメータ生成部と、前記変換パラメータを用いて前記入力情報を暗号化することにより暗号化入力情報を生成する暗号化情報生成部と、を備える。

[0010] 本発明の暗号化情報変換装置は、照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換装置であって、前記第１パラメータを記憶する変換側記憶領域と、前記暗号化入力情報を生成するために用いられた前記第２パラメータと、前記第２パラメータとは異なる第３パラメータとを取得する変換側取得部と、前記第１パラメータ、前記第２パラメータ、及び前記第３パラメータを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成する暗号変換パラメータ生成部と、前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成する更新情報生成部と、を備える。

[0011] 本発明の暗号化情報変換装置は、照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換装置であって、前記第１パラメータを含む複数のマスタパラメータを記憶する変換側記憶領域と、前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得する変換側取得部と、複数の前記マスタパラメータと、前記第２パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成する暗号変換パラメータ生成部と、前記暗号変換パラメータを用いて前記暗号化入力情報を変換すること

により、前記更新暗号化入力情報を生成する更新情報生成部と、を備える。

[0012] 本発明の照合システムは、照合のために入力される入力情報を暗号化する端末装置であって、第１パラメータを記憶する端末側記憶領域と、第２パラメータを取得する端末側取得部と、前記第１パラメータと前記第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行う変換パラメータ生成部と、前記変換パラメータを用いて前記入力情報を暗号化することにより暗号化入力情報を生成する暗号化情報生成部とを備える端末装置と、照合のために前記端末装置に入力される第１入力情報を、前記暗号化情報生成部が前記変換パラメータを用いて暗号化することにより生成される第１暗号化入力情報と、照合のために前記端末装置に入力される前記第１入力情報とは異なる第２入力情報を暗号化することにより生成される第２暗号化入力情報とに基づいて、前記第１入力情報と前記第２入力情報とを照合する照合処理を行う照合処理部と、を備える。

[0013] 本発明の照合システムは、照合のために入力される入力情報を暗号化する端末装置であって、第１パラメータを記憶する端末側記憶領域と、第２パラメータを取得する端末側取得部と、前記第１パラメータと前記第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行う変換パラメータ生成部と、前記変換パラメータを用いて前記入力情報を暗号化することにより暗号化入力情報を生成する暗号化情報生成部と、を備える端末装置と、照合のために前記端末装置に入力される第３入力情報を、前記暗号化情報生成部が前記変換パラメータを用いて暗号化することにより生成される第３暗号化入力情報と、照合のために前記端末装置に入力される前記第３入力情報とは異なる第４入力情報を暗号化することにより生成される第４暗号化入力情報とに基づいて、前記第３入力情報と前記第４入力情報とを照合する照合処理を行う照合処理部と、を備える。

[0014] 本発明の入力情報暗号化方法は、記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、照合のために入力さ

れる入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、を備える。

[0015] 本発明の暗号化情報変換方法は、照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換方法であって、前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、前記第２パラメータとは異なる第３パラメータを取得することと、記憶領域に記憶されている前記第１パラメータと、取得した前記第２パラメータ及び前記第３パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、を備える。

[0016] 本発明の暗号化情報変換方法は、照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換方法であって、前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、記憶領域に記憶されている前記第１パラメータ以外のマスタパラメータと、前記第２パラメータとを用いて、前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、を備える。

[0017] 本発明の照合方法は、端末装置の記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、照合のための第１入力情報を、前記変換パラメータを用いて暗号化することにより生成される第１暗号化入力情報と、照合のために入力される前記第１入力情報とは異なる第２入力情報を暗号化する

ことにより生成される第２暗号化入力情報とに基づいて、前記第１入力情報と前記第２入力情報とを照合する照合処理を行うことと、を備える。

[0018] 本発明の照合方法は、端末装置の記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、照合のために入力される第３入力情報を、前記変換パラメータを用いて暗号化することにより生成される第３暗号化入力情報と、照合のために入力される前記第３入力情報とは異なる第４入力情報を暗号化することにより生成される第４暗号化入力情報とに基づいて、前記第３入力情報と前記第４入力情報とを照合する照合処理を行うことと、を備える。

[0019] 本発明の入力情報暗号化プログラムは、記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、をプロセッサに実行させる。

[0020] 本発明の暗号化情報変換プログラムは、照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換プログラムであって、前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、前記第２パラメータとは異なる第３パラメータを取得することと、記憶領域に記憶されている前記第１パラメータと、取得した前記第２パラメータ及び前記第３パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、をプロセッサに実行させる。

[0021] 本発明の暗号化情報変換プログラムは、照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換プログラムであって、前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、記憶領域に記憶されている前記第１パラメータ以外のマスタパラメータと、前記第２パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、をプロセッサに実行させる。

発明の効果

[0022] 本発明によれば、照合精度の劣化の抑制と情報の漏洩リスクの低減とを両立可能な暗号化処理を実現する端末装置、暗号化情報変換装置、照合システム、入力情報暗号化方法、暗号化情報変換方法、照合方法、入力情報暗号化プログラム、及び暗号化情報変換プログラムを提供することができる。なお、本発明により、当該効果の代わりに、又は当該効果とともに、他の効果が奏されてもよい。

図面の簡単な説明

[0023] [図1]図１は、第１の実施形態に係る照合システムの運用形態を例示した図である。

[図2]図２は、第１の実施形態に係る照合システムに含まれる情報処理装置のハードウェア構成を例示したブロック図である。

[図3]図３は、キャンセラブルバイオメトリクスの概要を示す図である。

[図4]図４は、第１の実施形態に係る端末装置の機能構成を示す機能ブロック図である。

[図5]図５は、第１の実施形態に係る変換処理部における情報の暗号化を説明するための説明図である。

[図6]図６は、第１の実施形態に係るサブパラメータ生成装置の機能構成を示

す機能ブロック図である。

[図7]図７は、第１の実施形態に係る照合装置の機能構成を示す機能ブロック図である。

[図8]図８は、第１の実施形態に係る更新情報生成部が暗号化入力情報を変換する過程を説明するための説明図である。

[図9]図９は、第１の実施形態に係る特徴量データを暗号化する処理の流れを示すシーケンス図である。

[図10]図１０は、第１の実施形態に係るデータベースに記憶される情報の構成を例示した図である。

[図11]図１１は、第１の実施形態の実施例１に係る暗号化情報を照合する処理の流れを示すシーケンス図である。

[図12]図１２は、第１の実施形態に係る暗号化データ変換処理の流れを示すシーケンス図である。

[図13]図１３は、第１の実施形態に係る暗号変換パラメータを生成する処理の流れを示すフローチャートである。

[図14]図１４は、第１の実施形態の実施例２に係る暗号化情報を照合する処理の流れを示すシーケンス図である。

[図15]図１５は、第１の実施形態の変形例１におけるハミング距離マスクによるキャンセラブル変換を説明するための説明図である。

[図16]図１６は、第１の実施形態の変形例２に係る暗号変換パラメータを生成する処理の流れを示すフローチャートである。

[図17]図１７は、第１の実施形態の変形例３に係る端末装置の機能構成を示す機能ブロック図である。

[図18]図１８は、第２の実施形態に係る照合システムの運用形態の一例を示す図である。

[図19]図１９は、第２の実施形態に係る判定装置の機能構成を示す機能ブロック図である。

[図20]図２０は、第２の実施形態に係る照合処理部の内部構成を示す機能ブ

ロック図である。

[図21]図２１は、第２の実施形態に係る照合システムにおける準同型演算処理を用いた照合処理の概要を示すモデル図である。

[図22]図２２は、第３の実施形態に係る端末装置の概略的な構成を例示するブロック図である。

[図23]図２３は、第３の実施形態に係る暗号化情報変換装置の概略的な構成を例示するブロック図である。

[図24]図２４は、第３の実施形態に係る照合システムの概略的な構成を示す図である。

発明を実施するための形態

[0024] 以下、添付の図面を参照して本発明の実施形態を詳細に説明する。なお、本明細書及び図面において、同様に説明されることが可能な要素については、同一の符号を付することにより重複説明が省略され得る。

[0025] 以下に説明される各実施形態は、本発明を実現可能な構成の一例に過ぎない。以下の各実施形態は、本発明が適用される装置の構成や各種の条件に応じて適宜に修正又は変更することが可能である。以下の各実施形態に含まれる要素の組合せの全てが本発明を実現するに必須であるとは限られず、要素の一部を適宜に省略することが可能である。したがって、本発明の範囲は、以下の各実施形態に記載される構成によって限定されるものではない。相互に矛盾のない限りにおいて、実施形態内に記載された複数の構成を組み合わせた構成も採用可能である。

[0026] 説明は、以下の順序で行われる。

１．本発明の実施形態の概要

２．第１の実施形態

２．１．照合システムの運用形態の概要

２．２．情報処理装置のハードウェア構成

２．３．キャンセラブルバイオメトリクスの概要

２．４．端末装置の機能構成

[0027] ＜１．本発明の実施形態の概要＞

まず、本発明の実施形態の概要を説明する。

[0028] （１）技術的課題

近年、ユーザ認証技術のひとつとして、指紋、静脈、虹彩、及び顔画像等の生体情報を照合することにより認証を行う生体認証技術が広く用いられている。生体認証技術においては、ユーザの生体情報から特徴量を抽出して登録情報として保存し、認証に際し入力されたユーザの生体情報の特徴量と登録情報とを照合して認証可否が判断される。

[0029] 生体認証技術は、ＩＣカード等を利用した認証技術と比較して、紛失及び盗難のリスクが少ないといった利点がある一方で、生体情報が漏洩した場合であっても、生体情報の破棄及び更新を行うことができない。つまり、生体情報の漏洩は、漏洩した生体情報に係る生体の個人情報に関する問題だけではなく、漏洩した生体情報に係る生体の生体情報を用いる認証システムのセキュリティ性を損なうという問題がある。

[0030] このような問題に対して、ユーザの生体情報の保護を目的として、登録情報を無効化することが可能な「キャンセラブルバイオメトリクス」と呼ばれる技術が提案されている。

[0031] キャンセラブルバイオメトリクスでは、生体情報から抽出した特徴量の要素を、秘密鍵を用いて並び替えることにより暗号化し、登録情報を生成する。また、認証時に入力された生体情報から抽出された特徴量の要素に対しても、登録時と同じ秘密鍵を用いて暗号化を行うことにより照合情報を生成する。つまり、登録情報を作り変える際には、異なる秘密鍵を用いることにより、生成済みの登録情報を無効化することが可能となる。キャンセラブルバイオメトリクスにおける暗号化は、このような登録情報の性質から、「キャンセラブル変換」と称される。キャンセラブル変換として、例えば、指紋等から得られた特徴点の画像をブロック分割して、秘密鍵を用いて分割した画像の並びを入れ替えることにより、登録情報及び照合情報を生成する方法が提案されている。

[0032] 上述したように、キャンセラブル変換では、登録時と照合時とにおいて同じ秘密鍵を用いて、生体情報から抽出した特徴量の要素の変換が行われる。したがって、生体情報の漏洩リスクを低減するには、キャンセラブル変換されたままの状態で登録情報と照合情報とを照合することが望ましい。また、登録情報と照合情報とを照合する場合に、従来の生体認証技術と同程度の照合精度が得られるように、キャンセラブル変換を行うことが望ましい。

[0033] 以上の事情に鑑み、本実施形態では、照合精度の劣化の抑制と情報の漏洩リスクの低減とを両立可能な暗号化処理を実現する端末装置、暗号化情報変換装置、照合システム、入力情報暗号化方法、暗号化情報変換方法、照合方法、入力情報暗号化プログラム、及び暗号化情報変換プログラムを提供することを目的とする。

[0034] （２）技術的特徴

本発明の実施形態では、照合のために入力される入力情報を暗号化する端末装置が、第１パラメータを記憶する端末側記憶領域と、第２パラメータを

取得する端末側取得部と、前記第１パラメータと前記第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行う変換パラメータ生成部と、前記変換パラメータを用いて前記入力情報を暗号化することにより暗号化入力情報を生成する暗号化情報生成部と、を備える。

[0035] また、本発明の実施形態では、照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換装置が、前記第１パラメータを記憶する変換側記憶領域と、前記暗号化入力情報を生成するために用いられた前記第２パラメータと、前記第２パラメータとは異なる第３パラメータとを取得する変換側取得部と、前記第１パラメータ、前記第２パラメータ、及び前記第３パラメータを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成する暗号変換パラメータ生成部と、前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成する更新情報生成部と、を備える。

[0036] これにより、照合精度の劣化の抑制と情報の漏洩リスクの低減とを両立可能な暗号化処理を実現する端末装置、暗号化情報変換装置、照合システム、入力情報暗号化方法、暗号化情報変換方法、照合方法、入力情報暗号化プログラム、及び暗号化情報変換プログラムを提供することができる。なお、上述した技術的特徴は本発明の実施形態の具体的な一例であり、当然ながら、本発明の実施形態は上述した技術的特徴に限定されない。

[0037] ＜２．第１の実施形態＞

以下、図１から図１５を参照して、本発明の第１の実施形態を説明する。本実施形態においては、指紋、静脈、虹彩、及び顔画像等のユーザの生体情報を用いた照合システムについて説明する。

[0038] ＜２．１．照合システムの運用形態の概要＞

図１は、本発明の第１の実施形態に係る照合システム１０００Ａの運用形態の一例を示す図である。図１に示すように、照合システム１０００Ａは、

端末装置１、サブパラメータ生成装置２、照合装置３、及びデータベース（Ｄａｔａ　Ｂａｓｅ、以後「ＤＢ」と称する場合がある）４がネットワーク５を介して接続されて構成されている。照合システム１０００Ａに入力される入力情報とは、例えば、指紋、静脈、虹彩、及び顔画像等のユーザの生体情報である。また、高い機密性及びセキュリティ性が求められるデータを含む情報も入力情報のひとつである。

[0039] 端末装置１は、照合システム１０００Ａに入力される入力情報を暗号化するプログラムがインストールされたコンピュータ又はサーバ等の情報処理装置である。端末装置１は、例えば、スマートフォン等の可搬型情報処理端末、ＡＴＭ（Ａｕｔｏｍａｔｉｃ　Ｔｅｌｌｅｒ　Ｍａｃｈｉｎｅ）、生体情報を検知するセンサが接続されたＰＣ（Ｐｅｒｓｏｎａｌ　Ｃｏｍｐｕｔｅｒ）等によって実現される。端末装置１が情報を暗号化する処理の詳細については後述する。端末装置１によって暗号化された入力情報（以後、「暗号化入力情報」と記載する場合がある）は、ＤＢ４に記憶される。

[0040] サブパラメータ生成装置２は、ユーザの生体情報を暗号化する際に用いられる変換パラメータを生成するためのサブパラメータを生成するプログラムがインストールされた情報処理装置である。サブパラメータ生成装置２は、サブパラメータとして、例えば、乱数を生成するための第２乱数シード、暗号化パラメータ等を生成する。また、サブパラメータ生成装置２は、ユーザによってサブパラメータ生成装置２に入力される文字列に基づいてサブパラメータを生成してもよい。サブパラメータ生成装置２は、生成したサブパラメータを、ネットワーク５を介して端末装置１及び照合装置３に送信する。サブパラメータ生成装置２は、本実施形態のパラメータ送信装置の一例である。

[0041] 照合装置３は、端末装置１が生成した暗号化情報に基づいて照合システム１０００Ａの入力情報を照合するプログラムがインストールされた情報処理装置である。照合装置３は、例えば、生体認証技術において、ＤＢ４が記憶しているユーザの生体情報の特徴量と、端末装置１から取得したユーザの生

体情報の特徴量とを照合する。また、照合装置３は、サブパラメータ生成装置２から受信したサブパラメータに基づいて暗号変換パラメータを生成し、生成した暗号変換パラメータを用いてＤＢ４に記憶されている暗号化入力情報を変換する。つまり、照合装置３は、本実施形態の暗号化情報変換装置の一例である。照合装置３によって変換された暗号化入力情報（以後、「更新暗号化入力情報」と記載する場合がある）を、ＤＢ４に記憶するようにしてもよい。なお、照合システム１０００Ａは、照合装置３が行う照合処理の結果に基づいて、ユーザの認証を行ってもよい。

[0042] ＤＢ４は、情報を記憶する記憶媒体であり、例えば、端末装置１が生成した暗号化入力情報、照合装置３が生成した更新暗号化入力情報等を記憶する。図１では、照合装置３とＤＢ４とをそれぞれ独立した要素として示しているものの、照合装置３が備えるＨＤＤ（Ｈａｒｄ　Ｄｉｓｋ　Ｄｒｉｖｅ）等の記憶媒体にＤＢ４を実装してもよい。

[0043] なお、図１では、サブパラメータ生成装置２がネットワーク５に接続されている例を示しているが、必ずしもネットワーク５に接続される必要はない。例えば、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）等によって、サブパラメータ生成装置２が、端末装置１、及び照合装置３に接続されていてもよい。また、端末装置１は、暗号化入力情報をＤＢ４に送信するときにＤＢ４に接続されていればよい。さらに、照合装置３は、通信を行う際に、端末装置１又はＤＢ４に接続されていればよい。さらに、サブパラメータ生成装置２は、サブパラメータを送信する際に端末装置１又は照合装置３と接続されていればよい。照合システム１０００Ａは、端末装置１と同じ要素を備える他の情報処理装置を備えていてもよい。

[0044] ＜２．２．情報処理装置のハードウェア構成＞

続いて、図２を参照して、本実施形態に係る端末装置１、サブパラメータ生成装置２、及び照合装置３等の情報処理装置のハードウェア構成について説明する。図２は、情報処理装置のハードウェア構成を示すブロック図である。

[0045] 情報処理装置は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１１、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１２、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１３、記憶媒体１４、及びインタフェース（Ｉ／Ｆ）１５がバス１６を介して相互に接続されている。また、Ｉ／Ｆ１５には、入力部１７、表示部１８、センサ１９及びネットワーク５が接続されている。なお、入力部１７、表示部１８、及びセンサ１９は、省略可能である。

[0046] ＣＰＵ１１は、演算手段であり、情報処理装置全体の動作を制御する。ＲＡＭ１３は、情報の高速な読み書きが可能な揮発性の記憶媒体であり、ＣＰＵ１１が情報を処理する際の作業領域として用いられる。ＲＯＭ１２は、読み出し専用の不揮発性記憶媒体であり、ファームウェア等のプログラムが格納されている。記憶媒体１４は、ＨＤＤ等の情報の読み書きが可能な不揮発性の記憶媒体であり、ＯＳ（Ｏｐｅｒａｔｉｎｇ Ｓｙｓｔｅｍ）や各種の制御プログラム、アプリケーション・プログラム等の情報が格納されている。

[0047] Ｉ／Ｆ１５は、バス１６と各種のハードウェアやネットワーク５等とを接続し制御する。入力部１７は、ユーザが情報処理装置に情報を入力するためのキーボードやマウス等の入力装置である。表示部１８は、ユーザが情報処理装置の状態を確認するためのＬＣＤ（Ｌｉｑｕｉｄ Ｃｒｙｓｔａｌ Ｄｉｓｐｌａｙ）等の表示装置である。

[0048] センサ１９は、指紋や静脈、顔画像等、ユーザの生体情報を取得するモジュールである。なお、センサ１９は省略可能である。この場合、端末装置１は、ネットワーク５又はＩ／Ｆ１５に接続されている情報処理装置を介してユーザの生体情報を取得してもよい。

[0049] このようなハードウェア構成において、端末装置１のＲＯＭ１２に格納されたプログラムや、端末装置１の記憶媒体１４から端末装置１のＲＡＭ１３にロードされたプログラムに従って端末装置１のＣＰＵ１１が演算を行うことにより、端末装置１のソフトウェア制御部が構成される。

[0050] 以上のようにして構成されたソフトウェア制御部と、ハードウェアとの組み合わせによって、本実施形態に係る端末装置１のコントローラ１００（図４参照）の機能を実現する機能ブロックが構成される。

[0051] また、上述のハードウェア構成において、サブパラメータ生成装置２のＲＯＭ１２に格納されたプログラムや、サブパラメータ生成装置２の記憶媒体１４からサブパラメータ生成装置２のＲＡＭ１３にロードされたプログラムに従って、サブパラメータ生成装置２のＣＰＵ１１が演算を行うことにより、サブパラメータ生成装置２のソフトウェア制御部が構成される。

[0052] 以上のようにして構成されたソフトウェア制御部と、ハードウェアとの組み合わせによって、本実施形態に係るサブパラメータ生成装置２のコントローラ２００（図６参照）の機能を実現する機能ブロックが構成される。

[0053] また、上述のハードウェア構成において、照合装置３のＲＯＭ１２に格納されたプログラムや、照合装置３の記憶媒体１４から照合装置３のＲＡＭ１３にロードされたプログラムに従って、照合装置３のＣＰＵ１１が演算を行うことにより、照合装置３のソフトウェア制御部が構成される。

[0054] 以上のようにして構成されたソフトウェア制御部と、ハードウェアとの組み合わせによって、本実施形態に係る照合装置３のコントローラ３００（図７参照）の機能を実現する機能ブロックが構成される。

[0055] ＜２．３．キャンセラブルバイオメトリクスの概要＞

続いて、図３を参照して、登録情報を無効化することが可能なキャンセラブルバイオメトリクスの概要について説明する。図３は、キャンセラブルバイオメトリクスの概要を示す図である。

[0056] 生体認証技術においては、指紋、静脈、虹彩、及び顔画像等、ユーザの生体情報を予め登録しておき、認証に際し入力されたユーザの生体情報との比較結果に基づいて認証可否が判断される。しかし、生体情報が漏洩してしまうと、漏洩した生体情報に係る生体の個人情報に関する問題だけではなく、漏洩した生体情報に係る生体の生体情報を用いる認証システムのセキュリティ性を損なうという問題がある。

[0057] このような問題に対して、ユーザの生体情報の保護を目的として、生体情報を秘匿した登録情報を用いて認証を行い、登録情報が漏洩した場合には漏洩した登録情報を無効化することが可能な「キャンセラブルバイオメトリクス」と呼ばれる手法が用いられている。

[0058] ここで、図３を参照して、キャンセラブルバイオメトリクスの概要について説明する。まず、生体情報を登録する際には、生体情報から特徴量が抽出される。ここでは、説明のために、生体情報から、ベクトルである特徴量データ

[数1]

$$\boldsymbol{x} = (x_1, x_2, \cdots, x_{n-1}, x_n)$$

が抽出されたと仮定する。以後、ベクトルである特徴量データｘを単に「特徴量データｘ」と記載する場合がある。続いて、置換鍵

[数2]

$$\boldsymbol{K}$$

を用いて一方向変換することにより、特徴量データｘを暗号化する（式１－１）。以後、ベクトルである置換鍵Ｋを単に「置換鍵Ｋ」、ベクトルである暗号化データＴを単に「暗号化データＴ」と記載する場合がある。置換鍵Ｋは、ランダムに生成される暗号鍵に相当する。また、変換関数Ｆは、入力されたデータ（ここでは、特徴量データｘ）を一方向変換（不可逆変換）する関数である。

[数3]

$$\boldsymbol{T} \leftarrow F_{\boldsymbol{K}}(\boldsymbol{x}) \quad \cdots \quad (式1-1)$$

（式１－１）に示すように暗号化データＴは、置換鍵Ｋを用いた変換関数Ｆ

により、特徴量データｘが変換されたデータに相当する。また、暗号化データＴは、照合に際し用いられる登録情報のひとつであり、ＤＢ４等の記憶装置に記憶される。

[0059] 続いて、認証時の処理について説明する。認証に際し、生体情報から特徴量が抽出される。ここでは、説明のために、認証のために入力された生体情報から、ベクトルである特徴量データ

[数4]

$$\boldsymbol{y} = (y_1, y_2, \cdots, y_{n-1}, y_n)$$

が抽出されたと仮定する。ベクトルである特徴量データｙが、本実施形態の入力情報、第２入力情報、及び第４入力情報の一例である。以後、ベクトルである特徴量データｙを単に「特徴量データｙ」と記載する場合がある。続いて、置換鍵Ｋを用いて一方向変換することにより、特徴量データｙを暗号化する（式１－２）。以後、ベクトルである暗号化データＴ´を単に「暗号化データＴ´」と記載する場合がある。

[数5]

$$\boldsymbol{T'} \leftarrow F_{\boldsymbol{K}}(\boldsymbol{y}) \cdot \cdot \cdot \ (式1-2)$$

（式１－２）に示すように暗号化データＴ´は、暗号化データＴと同じ置換鍵Ｋを用いた変換関数Ｆにより、特徴量データｙが変換されたデータに相当する。また、暗号化データＴ´が、暗号化データＴに対して照合される情報に相当する。なお、キャンセラブルバイオメトリクスでは、特徴量データｘが暗号化された暗号化データＴと、特徴量データｙが暗号化された暗号化データＴ´とを、暗号化したままの状態で照合する。

[0060] （式１－１）及び（式１－２）に示すように、キャンセラブルバイオメトリクスでは、登録時及び認証時において、同じ置換鍵Ｋを用いた変換関数Ｆによって特徴量データの暗号化を行う。つまり、特徴量データｘと特徴量デ

ータｙとの類似度は、置換鍵Ｋを用いた変換関数Ｆによる変換後も保存されることとなる。

[0061] 生体情報として同一人物の右手中指の指紋から特徴量データｘと、特徴量データｘに近い特徴量データｙとを抽出したと仮定する。この場合、暗号化データＴは、特徴量データｘを変換することにより生成され、暗号化データＴ´は、特徴量データｘに近い特徴量データｙを変換することにより生成される。したがって、暗号化データＴと暗号化データＴ´との類似度は、特徴量データｘと特徴量データｙとの類似度に等しいため、暗号化データＴと暗号化データＴ´とは、互いに近いデータである。

[0062] ここで、同じ特徴量データｘに対して、置換鍵

[数6]

$$K_1$$

と、置換鍵

[数7]

$$K_2$$

とを用いて変換関数Ｆによる変換を行ったと仮定する。以後、ベクトルである置換鍵K_1を単に「置換鍵K_1」、ベクトルである置換鍵K_2を単に「置換鍵K_2」と記載する場合がある。なお、置換鍵K_1≠置換鍵K_2とする。この場合、特徴量データｘからは、

[数8]

$$T_1 \leftarrow F_{K_1}(x)$$

[数9]

$$T_2 \leftarrow F_{K_2}(x)$$

変換鍵Ｋ$_1$を用いた変換関数Ｆにより、ベクトルであるデータＴ$_1$を、また、変換鍵Ｋ$_2$を用いた変換関数Ｆにより、ベクトルであるデータＴ$_2$を生成することができる。以後、ベクトルであるデータＴ$_1$を単に「データＴ$_1$」、ベクトルであるデータＴ$_2$を単に「データＴ$_2$」と記載する場合がある。

[0063] 上述したように、変換関数Ｆは、入力されたデータを一方向変換する関数である。つまり、置換鍵Ｋ$_1$≠置換鍵Ｋ$_2$である場合、特徴量データｘに対して、置換鍵Ｋ$_1$を用いたときに変換関数Ｆが出力するデータＴ$_1$は、置換鍵Ｋ$_2$を用いたときに変換関数Ｆが出力するデータＴ$_2$とは異なることとなる。なお、上述したように、キャンセラブルバイオメトリクスでは、照合の際に、置換鍵Ｋ$_1$及び置換鍵Ｋ$_2$に関する情報を用いない。

[0064] そして、データＴ$_1$に対してデータＴ$_2$を照合すると、いずれのデータも特徴量データｘを変換して生成されたデータであるにも関わらず、データＴ$_1$とデータＴ$_2$との類似度は、特徴量データｘ同士の類似度とは一致しない。このように、キャンセラブルバイオメトリクスでは、同じデータに対して、それぞれが異なる置換鍵Ｋ$_1$及び置換鍵Ｋ$_2$を用いることにより、それぞれが異なるデータＴ$_1$とデータＴ$_2$が生成される。このような特性を用いて、キャンセラブルバイオメトリクスでは、置換鍵Ｋを変更することにより、データベース等に記憶された登録情報を無効化することができる。以後の説明において、キャンセラブルバイオメトリクスにおけるデータの変換手法を、「キャンセラブル変換」と称する場合がある。

[0065] ＜２．４．端末装置の機能構成＞

続いて、端末装置１の機能構成について説明する。図４は、端末装置１の機能構成を示す機能ブロック図である。図４に示すように、端末装置１は、コントローラ１００、及びコントローラ１００がネットワーク５を介して他の機器と情報をやり取りするためのインタフェースであるネットワークＩ／

Ｆ１０１を含む。

[0066] コントローラ１００は、ネットワークＩ／Ｆ１０１を介して取得した情報を暗号化するための処理を行う。コントローラ１００は、専用のソフトウェア・プログラムが端末装置１等の情報処理装置にインストールされることによって実現されている。コントローラ１００は、サブパラメータ取得部１１０、特徴量算出部１２０、記憶領域１３０、パラメータ生成部１４０、及び変換処理部１５０を含む。

[0067] サブパラメータ取得部１１０は、ネットワークＩ／Ｆ１０１を介して、サブパラメータ生成装置２が生成したサブパラメータ（例えば、サブパラメータｖｐｉ１又はサブパラメータｖｐｉ２）を取得する。サブパラメータ取得部１１０は、本実施形態の端末側取得部の一例である。また、サブパラメータｖｐｉ１が第２パラメータの一例である。

[0068] 特徴量算出部１２０は、端末装置１のセンサ１９が取得したユーザの生体情報から特徴量を抽出する処理を行う。なお、ユーザの生体情報に関する特徴量の情報を端末装置１に入力してもよい。この場合、特徴量算出部１２０を省略してもよい。

[0069] 記憶領域１３０は、サブパラメータとは異なるパラメータであって、サブパラメータと共に変換パラメータｖｐを生成するために用いられるマスタパラメータ（例えば、マスタパラメータｖｐｍ１）を記憶している。本実施形態においてマスタパラメータとは、端末装置１に対してユニークに定められているパラメータである。マスタパラメータｖｐｍ１が、本実施形態の第１パラメータの一例である。記憶領域１３０は、マスタパラメータとして、乱数を生成するための第１乱数シードを記憶してもよい。また、記憶領域１３０は、マスタパラメータとして、暗号化パラメータを復号するための秘密鍵を記憶してもよい。記憶領域１３０は、本実施形態の端末側記憶領域の一例である。

[0070] なお、端末装置１に相当する要素を備える他の情報処理装置が照合システム１０００Ａに含まれている場合、端末装置１と他の情報処理装置とにおい

て、共通のマスタパラメータ（例えば、マスタパラメータｖｐｍ１）を記憶するようにしてもよい。さらに、マスタパラメータは、端末装置１の製品出荷又は端末装置１のアクティベーションを行う際に記憶領域１３０に記憶するようにしてもよい。

[0071] パラメータ生成部１４０は、記憶領域１３０に記憶されているマスタパラメータ（例えば、マスタパラメータｖｐｍ１）と、サブパラメータ生成装置２から取得したサブパラメータとに基づいて、端末装置１に入力された情報を暗号化するための変換パラメータを生成する変換パラメータ生成処理を行う。パラメータ生成部１４０が変換パラメータを生成する処理の具体的な態様については、後述する。パラメータ生成部１４０は、本実施形態の変換パラメータ生成部の一例である。

[0072] なお、パラメータ生成部１４０が生成した変換パラメータは、記憶領域１３０に記憶するようにしてもよい。このようにすることにより、サブパラメータ生成装置２との通信を行うことなく、記憶領域１３０に記憶されている変換パラメータによって、端末装置１に入力される入力情報（例えば、特徴量データｘ又は特徴量データｙ）を暗号化することができる。

[0073] 変換処理部１５０は、パラメータ生成部１４０が生成した変換パラメータを用いて、端末装置１に入力された情報を暗号化することにより、暗号化入力情報を生成する。変換処理部１５０は、本実施形態の暗号化情報生成部の一例である。また、暗号化データＴ及び暗号化データＴ´は、本実施形態の暗号化入力情報の一例である。ネットワークＩ／Ｆ１０１は、変換処理部１５０が生成した暗号化入力情報を、照合装置３に送信する。

[0074] なお、照合のために、端末装置１のユーザの生体情報等を照合システム１０００Ａに登録する場合、ネットワークＩ／Ｆ１０１は、変換処理部１５０が生成した暗号化入力情報をＤＢ４に送信する。ＤＢ４は、端末装置１から受信した暗号化入力情報と、ユーザを識別可能なユーザＩＤ等の識別情報とを関連付けて記憶する。ユーザを識別可能なユーザＩＤ等の識別情報とは、ユーザ又は端末装置１ごとに予め設定されている識別子等の情報に相当する

。

[0075] ここで、図５を参照して、変換処理部１５０が端末装置１に入力された情報を暗号化するときの具体的な態様について説明する。図５は、変換処理部１５０における情報の暗号化を説明するための説明図である。図５では、端末装置１に特徴量データｘが入力されたと仮定して説明を行う。特徴量データｘが本実施形態の入力情報、第１入力情報、及び第３入力情報の一例である。また、図５においては、（式２－１）に示すように、特徴量データｘが、ｄ次元（次元数がｄ）のデータセットであると仮定する。

[数10]

$$\boldsymbol{x} = (x[0], x[1], \cdots, x[d-2], x[d-1])$$

・・・（式２－１）

[0076] 本実施形態において、変換処理部１５０は、パラメータ生成部１４０が生成した変換パラメータｖｐに基づいて特徴量データｘを暗号化する。本実施形態において、パラメータ生成部１４０は、変換パラメータｖｐとして、特徴量データｘに含まれる各次元の要素の並び順を一方向変換する置換鍵Ｋを生成する。

[0077] 置換鍵Ｋには、例えば、特徴量データｘの０次元目の要素（ｘ［０］）をｄ－１次元目に並べ、特徴量データｘの１次元目の要素（ｘ［１］）をｄ－２次元目に並べ、特徴量データｘのｄ－２次元目の要素（ｘ［ｄ－２］）を１次元目に並べ、特徴量データｘのｄ－１次元目の要素（ｘ［ｄ－１］）を、０次元目に並べるためのパラメータが定義されている。

[0078] 変換処理部１５０は、置換鍵Ｋを用いて特徴量データｘを暗号化することにより、暗号化データ

[数11]

$$\boldsymbol{T} = (x'[0], x'[1], \cdots, x'[d-2], x'[d-1])$$

・・・（式２－２）

を生成する。暗号化データＴが、本実施形態の暗号化入力情報の一例である。

[0079] つまり、変換処理部１５０は、特徴量データｘの０次元目の要素（ｘ［０］）は、暗号化データＴのｄ－１次元目（ｘ´［ｄ－１］）に並び替える。また、変換処理部１５０は、特徴量データｘの１次元目の要素（ｘ［１］）は、暗号化データＴのｄ－２次元目（ｘ´［ｄ－２］）に並び替える。また、変換処理部１５０は、特徴量データｘのｄ－２次元目の要素（ｘ［ｄ－２］）は、暗号化データＴの１次元目（ｘ´［１］）に並び替える。また、変換処理部１５０は、特徴量データｘのｄ－１次元目の要素（ｘ［ｄ－１］）は、暗号化データＴの０次元目（ｘ´［０］）に並び替える。換言すると、変換処理部１５０は、置換鍵Ｋを用いて特徴量データｘをパーミュテーションすることにより、暗号化データＴを生成する。

[0080] なお、本実施形態において、特徴量算出部１２０、記憶領域１３０、パラメータ生成部１４０、及び変換処理部１５０は、端末装置１が備える保護領域１０２に設けられている。保護領域１０２とは、Ａｒｍ社のＴｒｕｓｔＺｏｎｅ（登録商標）やＲＩＳＣ－Ｖ財団のＫｅｙＳｔｏｎｅ等の技術によって、端末装置１のメモリ（ＲＯＭ１２やＲＡＭ１３）空間上においてコントローラ１００上の通常領域とは隔離して構築された、コントローラ１００上の通常領域よりもセキュアな空間（Ｓｅｃｕｒｅ　Ｗｏｒｌｄ）を指す。端末装置１に構築された保護領域１０２に機密情報を配置したり、セキュリティ処理を実装したりすることにより、機密情報の流出や端末装置１で行われる各種の処理の改ざんを防止することができる。

[0081] また、コントローラ１００上の通常領域は、非セキュア空間であるため、

コントローラ１００上の通常領域に設けられている要素は、セキュア空間である保護領域１０２に直接アクセスすることができない。そこで、本実施形態では、コントローラ１００上に保護領域１０２を設け、保護領域１０２に特徴量算出部１２０、記憶領域１３０、パラメータ生成部１４０、及び変換処理部１５０を実装することにより、端末装置１のマスタパラメータｖｐｍ１、パラメータ生成部１４０が生成した変換パラメータｖｐ、及び暗号化データＴ等の情報の漏洩をより抑制することが可能となる。

[0082] ＜２．５．サブパラメータ生成装置の機能構成＞

続いて、図６を参照して、サブパラメータ生成装置２の機能構成について説明する。図６は、サブパラメータ生成装置２の機能構成を示す機能ブロック図である。図６に示すように、サブパラメータ生成装置２は、コントローラ２００、及びコントローラ２００がネットワーク５を介して他の機器と情報をやり取りするためのインタフェースであるネットワークＩ／Ｆ２０１を含む。

[0083] コントローラ２００は、サブパラメータ（例えば、サブパラメータｖｐｉ１、又はサブパラメータｖｐｉ２）を生成し、ネットワークＩ／Ｆ１０１を介して端末装置１及び照合装置３に送信するための処理を行う。コントローラ２００は、専用のソフトウェア・プログラムがサブパラメータ生成装置２等の情報処理装置にインストールされることによって実現されている。コントローラ２００は、サブパラメータ生成部２１０、サブパラメータ送信部２２０、及びサブパラメータ記憶部２３０を含む。

[0084] サブパラメータ生成部２１０は、端末装置１が変換パラメータｖｐを生成するためのサブパラメータｖｐｉ１を生成する。サブパラメータ生成部２１０は、例えば、サブパラメータｖｐｉ１として、乱数を生成するための第２乱数シードを生成する。なお、サブパラメータ生成部２１０は、サブパラメータｖｐｉ１とは異なるサブパラメータ（例えば、サブパラメータｖｐｉ２）を生成することも可能である。

[0085] サブパラメータ送信部２２０は、サブパラメータ生成部２１０が生成した

サブパラメータｖｐｉ１（又はサブパラメータｖｐｉ２）を、ネットワークＩ／Ｆ２０１を介して端末装置１及び／又は照合装置３に送信する。

[0086] サブパラメータ記憶部２３０は、サブパラメータ生成部２１０が生成したサブパラメータｖｐｉ１及びサブパラメータｖｐｉ２等のサブパラメータを記憶する。なお、サブパラメータ記憶部２３０は、サブパラメータｖｐｉ１（又はサブパラメータｖｐｉ２）の宛先となった端末装置１を識別する識別情報、もしくはサブパラメータｖｐｉ１（又はサブパラメータｖｐｉ２）の宛先となった端末装置１に生体情報を入力したユーザを識別するための識別情報を、サブパラメータｖｐｉ１に関連付けて記憶してもよい。

[0087] ＜２．６．照合装置の機能構成＞

続いて、図７を参照して、照合装置３の機能構成について説明する。図７は、照合装置３の機能構成を示す機能ブロック図である。図７に示すように、照合装置３は、コントローラ３００、及びコントローラ３００がネットワーク５を介して他の機器と情報をやり取りするためのインタフェースであるネットワークＩ／Ｆ３０１を含む。

[0088] コントローラ３００は、ネットワークＩ／Ｆ１０１を介して取得した情報を照合するための処理を行う。コントローラ３００は、専用のソフトウェア・プログラムが照合装置３等の情報処理装置にインストールされることによって実現されている。コントローラ３００は、サブパラメータ取得部３１０、記憶領域３２０、パラメータ生成部３３０、更新情報生成部３４０、及び照合処理部３５０を含む。

[0089] サブパラメータ取得部３１０は、ネットワークＩ／Ｆ３０１を介して、サブパラメータ生成装置２が生成したサブパラメータ（例えば、サブパラメータｖｐｉ１及びサブパラメータｖｐｉ２）を取得する。サブパラメータ取得部３１０は、本実施形態の変換側取得部の一例である。

[0090] 記憶領域３２０は、サブパラメータｖｐｉ１及びサブパラメータｖｐｉ２とは異なるパラメータであって、変換パラメータｖｐを生成するために端末装置１において用いられたマスタパラメータと同じパラメータ（例えば、マ

スタパラメータｖｐｍ１）を記憶している。上述したように、マスタパラメータｖｐｍ１は、端末装置１に対してユニークに定められているパラメータである。本実施形態において、記憶領域３２０には、照合装置３に接続される可能性のある端末装置１が記憶しているマスタパラメータを記憶する。つまり、照合装置３に対して、端末装置１及び端末装置１に相当する要素を備える他の情報処理装置が接続されている場合、記憶領域３２０は、端末装置１のマスタパラメータｖｐｍ１を含む複数のマスタパラメータを記憶してもよい。記憶領域３２０は、本実施形態の変換側記憶領域の一例である。

[0091] パラメータ生成部３３０は、記憶領域３２０に記憶されているマスタパラメータｖｐｍ１と、サブパラメータ生成装置２から取得したサブパラメータｖｐｉ１及びサブパラメータｖｐｉ２とに基づいて、端末装置１から受信した暗号化入力情報を変換するための暗号変換パラメータｖｐ´を生成する。具体的に、パラメータ生成部３３０は、記憶領域３２０に記憶されているマスタパラメータｖｐｍ１と、サブパラメータ生成装置２から受信したサブパラメータｖｐｉ１と、サブパラメータｖｐｉ１とは異なるサブパラメータ（例えば、サブパラメータｖｐｉ２）とを用いて、暗号変換パラメータｖｐ´を生成する。パラメータ生成部３３０が暗号変換パラメータｖｐ´を生成する処理の具体的な態様については、後述する。パラメータ生成部３３０は、本実施形態の暗号変換パラメータ生成部の一例である。

[0092] 更新情報生成部３４０は、端末装置１から受信した暗号化入力情報を、パラメータ生成部３３０が生成した暗号変換パラメータｖｐ´を用いて変換することにより、更新暗号化入力情報を生成する。ここで、図８を参照して、更新情報生成部３４０が端末装置１から取得した暗号化入力情報を暗号化するときの具体的な態様について説明する。

[0093] 図８は、更新情報生成部３４０が暗号化入力情報を変換する過程を説明するための説明図である。図８では、更新情報生成部３４０が変換パラメータｖｐを用いて暗号化データＴを変換すると仮定して説明を行う。また、図８においては、（式３－１）に示すように、特徴量データｘが、５次元（次元

数が５）のデータセットであると仮定する（図８、左側の最上段参照）。

[数12]

$$\boldsymbol{x} = (x[0], x[1], x[2], x[3], x[4])$$

$$\cdots \quad (式3-1)$$

[0094] 上述したように、変換処理部１５０は、変換パラメータｖｐを用いて特徴量データｘを暗号化することにより、暗号化データＴを生成する。本実施形態において、パラメータ生成部１４０は、変換パラメータｖｐとして、特徴量データｘに含まれる各次元の要素の並び順を一方向変換する置換鍵Ｋを生成する。

[0095] 置換鍵Ｋには、例えば、特徴量データｘの０次元目の要素（ｘ［０］）を４次元目に並べ、特徴量データｘの１次元目の要素（ｘ［１］）を１次元目に並べ替え、特徴量データｘの２次元目の要素を（ｘ［２］）を０次元目に並べ替え、特徴量データｘの３次元目の要素（ｘ［３］）を４次元目に並べ替え、特徴量データｘの４次元目の要素（ｘ［４］）を２次元目に並べ替えるためのパラメータが定義されている。

[0096] 端末装置１においては、変換処理部１５０が、置換鍵Ｋを用いて特徴量データｘを暗号化することにより、暗号化データ

[数13]

$$\boldsymbol{T} = (x[2], x[1], x[4], x[0], x[3])$$

$$\cdots \quad (式3-2)$$

を生成する（図８、左側の上から２段目参照）。そして、端末装置１は、暗号化データＴを照合装置３に送信する。

[0097] ここで、暗号化データＴを特徴量データｘに復号すると仮定する。この場合、置換鍵Ｋを用いて暗号化データＴを逆変換することにより、（式３－２

）に示す暗号化データＴから（式３－１）に示す特徴量データｘを得ることができる（図８、左側の上から３段目参照）。

[0098] また、特徴量データｘに対して、置換鍵Ｋとは異なる置換鍵Ｋ´（例えば、パラメータｖｐｘ）を用いてキャンセラブル変換を行うとする。特徴量データｘに対して置換鍵Ｋ´を用いたキャンセラブル変換を行うことにより、暗号化データ

[数14]

$$T'' = (x[1], x[3], x[0], x[4], x[2])$$

・・・（式３－３）

を生成することができる（図８、左側の最下段参照）。以後、ベクトルである暗号化データＴ´´を単に「暗号化データＴ´´」と記載する場合がある。

[0099] （式３－２）及び（式３－３）に示すように、特徴量データｘに対して置換鍵Ｋ´を用いて生成した暗号化データＴ´´の要素の並び順は、特徴量データｘに対して置換鍵Ｋを用いて生成した暗号化データＴの要素の並び順とは異なる。このようにすることにより、キャンセラブル変換では、特徴量データｘに対して置換鍵Ｋを用いて生成した暗号化データＴを、特徴量データｘに対して置換鍵Ｋ´を用いて生成した暗号化データＴ´´によって無効化することが可能である。

[0100] しかしながら、暗号化データＴを置換鍵Ｋによって逆変換することにより、暗号化されていないデータである特徴量データｘが漏洩するリスクが増大してしまう。このような問題に対して、本実施形態は、更新情報生成部３４０において暗号化データＴを特徴量データｘに逆変換することなく、暗号化データＴを変換することが可能である。

[0101] 本実施形態において、記憶領域１３０及び記憶領域３２０は、マスタパラ

メータｖｐｍ１を記憶している。マスタパラメータｖｐｍ１は、端末装置１で変換パラメータｖｐを生成するために用いられるパラメータである。また、サブパラメータ取得部３１０は、サブパラメータｖｐｉ１をサブパラメータ生成装置２から受信する。サブパラメータｖｐｉ１は、変換パラメータｖｐを生成するためにサブパラメータ生成装置２から端末装置１に送信されたパラメータである。

[0102] なお、サブパラメータ生成装置２は、サブパラメータｖｐｉ１とは異なるサブパラメータ（例えば、サブパラメータｖｐｉ２）を照合装置３に送信することができる。パラメータ生成部３３０は、マスタパラメータｖｐｍ１と、サブパラメータｖｐｉ１と、サブパラメータｖｐｉ２とを用いて、暗号変換パラメータｖｐ´を生成する。暗号変換パラメータｖｐ´は、暗号化データＴを更新暗号化データＴ３に変換するためのパラメータである。

[0103] 更新情報生成部３４０は、暗号変換パラメータｖｐ´を用いて暗号化データＴ（図８、右側の上段参照）を変換することにより、更新暗号化データＴ３を生成する（図８、右側の下段参照）。更新暗号化データＴ３が、本実施形態の更新暗号化入力情報の一例である。図８に示すように、更新暗号化データＴ３に含まれる要素の並び順は、暗号化データＴ´´に含まれる要素の並び順と同じである。

[0104] また、特徴量データｙが特徴量データｘに近いデータである場合において、特徴量データｙを置換鍵Ｋ´によってキャンセラブル変換したと仮定する。この場合、特徴量データｙと特徴量データｘとが相互に近いデータであるため、特徴量データｙは、置換鍵Ｋ´により暗号化データＴ´´に変換される。この場合においても、更新暗号化データＴ３に含まれる要素の並び順は、置換鍵Ｋ´を用いて特徴量データｙをキャンセラブル変換して生成される暗号化データＴ´´に含まれる要素の並び順と同じとなる。

[0105] つまり、更新情報生成部３４０は、暗号変換パラメータｖｐ´を用いて暗号化データＴを変換することにより、更新暗号化データＴ３を生成することができる。上述したように、更新暗号化データＴ３は、置換鍵Ｋ´（つまり

、変換パラメータｖｐｘ）を用いて特徴量データｘを暗号化した暗号化データＴ´´に相当するデータセットである（図８参照）。このようにすることにより、本実施形態では、照合装置３において暗号化データＴを特徴量データｘに復号することなく、暗号化データＴを無効化することが可能である。

[0106] 照合処理部３５０は、ＤＢ４に記憶されている暗号化入力情報と、端末装置１から取得した暗号化データ（例えば、暗号化データＴ´、又は暗号化データＴ´´）とを照合する照合処理を行う。上述したように、端末装置１は、記憶領域１３０に記憶しているマスタパラメータｖｐｍ１と、サブパラメータ生成装置２から受信したサブパラメータｖｐｉ１とに基づいて変換パラメータｖｐを生成する。本実施形態では、照合システム１０００Ａのメンテナンスやバージョン変更等により、サブパラメータ生成装置２が、サブパラメータｖｐｉ１とは異なるサブパラメータ（例えば、サブパラメータｖｐｉ２）を、端末装置１に送信する場合がある。このような場合において、端末装置１に入力される情報を暗号化する際には、記憶領域１３０に記憶しているマスタパラメータｖｐｍ１と、サブパラメータ生成装置２から受信したサブパラメータｖｐｉ２とに基づいて生成された変換パラメータ（例えば、変換パラメータｖｐｘ）が用いられる。

[0107] 上述したように、端末装置１において用いられるサブパラメータが、サブパラメータｖｐｉ１からサブパラメータｖｐｉ２に変更された場合であっても、パラメータ生成部３３０は、サブパラメータｖｐｉ１及びサブパラメータｖｐｉ２と、記憶領域３２０に記憶しているマスタパラメータｖｐｍ１とを用いて暗号変換パラメータｖｐ´を生成する。このようにすることにより、更新情報生成部３４０は、暗号化データＴを更新暗号化データＴ３に変換することができる。

[0108] 照合処理部３５０は、端末装置１から、特徴量データｙを暗号化したデータ（暗号化データＴ´又は暗号化データＴ´´）を取得し、暗号化データＴと照合する。上述したように、端末装置１において同じ置換鍵Ｋを用いて暗号化を行う限り、特徴量データｘに近いデータ（例えば、同一人物の右手中

指の指紋から抽出された特徴量データｙ）を置換鍵Ｋによって暗号化したデータ（暗号化データＴ´）と、暗号化データＴとの類似度は、特徴量データｘと特徴量データｙとの類似度に一致する。

[0109] また、一方で、端末装置１において、置換鍵Ｋとは異なる置換鍵Ｋ´を用いて特徴量データｙを暗号化したと仮定する。このような場合、特徴量データｙを置換鍵Ｋ´によって暗号化したデータ（つまり、暗号化データＴ´´に相当するデータ）と、暗号化データＴとの類似度は、特徴量データｘと特徴量データｙとの類似度に一致しない。

[0110] 照合処理部３５０は、ＤＢ４から取得した暗号化データ（例えば、暗号化データＴ）と、端末装置１から受信した暗号化データ（例えば、暗号化データＴ´又は暗号化データＴ´´）とを照合する照合処理を行う。また、照合処理部３５０は、照合処理の結果を出力する。照合処理部３５０による照合処理の結果とは、例えば、暗号化データＴと暗号化データＴ´との類似度、又は暗号化データＴと暗号化データＴ´´との類似度を示す情報に相当する。

[0111] なお、本実施形態において、記憶領域３２０、パラメータ生成部３３０、更新情報生成部３４０、及び照合処理部３５０は、照合装置３が備える保護領域３０２に設けられている。保護領域３０２とは、保護領域１０２と同様に、Ａｒｍ社のＴｒｕｓｔＺｏｎｅやＲＩＳＣ－Ｖ財団のＫｅｙＳｔｏｎｅ等の技術によって、照合装置３のメモリ（ＲＯＭ１２やＲＡＭ１３）空間上においてコントローラ３００上の通常領域とは隔離して構築された、コントローラ３００上の通常領域よりもセキュアな空間（Ｓｅｃｕｒｅ　Ｗｏｒｌｄ）を指す。照合装置３に構築された保護領域３０２に機密情報を配置したり、セキュリティ処理を実装したりすることにより、機密情報の流出や照合装置３で行われる各種の処理の改ざんを防止することができる。

[0112] また、コントローラ３００上の通常領域は、非セキュア空間であるため、コントローラ３００上の通常領域に設けられている要素は、セキュア空間である保護領域３０２に直接アクセスすることはできない。そこで、本実施形

態では、コントローラ３００上に保護領域３０２を設け、保護領域３０２に記憶領域３２０、パラメータ生成部３３０、更新情報生成部３４０、及び照合処理部３５０を実装することにより、照合装置３のマスタパラメータ、パラメータ生成部３３０が生成した暗号変換パラメータｖｐ´、暗号化データＴ、暗号化データＴ´、及び暗号化データＴ´´等の情報の漏洩をより抑制することが可能となる。

[0113] また、照合処理部３５０を、照合装置３とは異なる情報処理装置の保護領域に実装するようにしてもよい。

[0114] ＜２．７．照合システムにおける特徴量データを暗号化する処理の流れ＞

続いて、図９を参照して、特徴量データｘを暗号化する処理の流れを説明する。図９は、特徴量データｘを暗号化する処理の流れを示すシーケンス図である。図９では、サブパラメータ生成装置２がサブパラメータｖｐｉ１を端末装置１に送信する例を示しているが、サブパラメータ生成装置２は、サブパラメータｖｐｉ１以外のサブパラメータ（サブパラメータｖｐｉ２）を生成して端末装置１に送信してもよい。

[0115] ステップＳ１１において、サブパラメータ生成部２１０は、サブパラメータｖｐｉ１を生成する。ステップＳ１２において、サブパラメータ送信部２２０は、端末装置１にサブパラメータｖｐｉ１を送信する。

[0116] ステップＳ１３において、サブパラメータ取得部１１０は、サブパラメータ生成装置２からサブパラメータｖｐｉ１を取得する。端末装置１は、サブパラメータ生成装置２からサブパラメータｖｐｉ１を取得することにより、特徴量データｘを暗号化することが可能になる。また、サブパラメータ生成装置２は、端末装置１にサブパラメータｖｐｉ１を送信する際にオンラインとなっていればよい。

[0117] ステップＳ１４において、パラメータ生成部１４０は、サブパラメータｖｐｉ１と、記憶領域１３０に記憶されているマスタパラメータｖｐｍ１とに基づいて、変換パラメータｖｐを生成する。

[0118] マスタパラメータｖｐｍ１が第１乱数シードであり、かつサブパラメータ

ｖｐｉ１が第２乱数シードである場合、パラメータ生成部１４０は、第１乱数シードと第２乱数シードを用いて乱数を生成する。パラメータ生成部１４０が生成する乱数は、変換パラメータｖｐの一例である。

[0119] マスタパラメータｖｐｍ１が秘密鍵であり、かつサブパラメータｖｐｉ１が暗号化パラメータである場合、パラメータ生成部１４０は、秘密鍵により暗号化パラメータを復号する。パラメータ生成部１４０によって復号された暗号化パラメータは、変換パラメータｖｐの一例である。

[0120] ステップＳ１５において、変換処理部１５０は、変換パラメータｖｐを用いて特徴量データｘを暗号化することにより、暗号化データＴを生成する。ステップＳ１４において、パラメータ生成部１４０が変換パラメータｖｐとして乱数を生成している場合、変換処理部１５０は、パラメータ生成部１４０が生成した乱数を用いて特徴量データｘを暗号化する。

[0121] 本実施形態において、特徴量データｘは、照合のために端末装置１に入力される入力情報の一例である。また、本実施形態において、暗号化データＴは、暗号化入力情報の一例である。

[0122] ステップＳ１６において、ネットワークＩ／Ｆ１０１は、特徴量データｘを抽出したときの端末装置１のユーザを識別可能な識別情報と暗号化データＴとをＤＢ４に送信する。ステップＳ１７において、ＤＢ４は、端末装置１から受信した暗号化データＴと特徴量データｘを抽出したときの端末装置１（又は、端末装置１のユーザ）を識別可能な識別情報とを関連付けて記憶する。暗号化データＴは、照合装置３が照合を行うための第１暗号化入力情報、及び第３暗号化入力情報の一例である。

[0123] 図１０は、ＤＢ４に記憶される情報の構成を例示した図である。図１０に示すように、ＤＢ４のＮｏ．１のデータには、バージョン情報として“ｖ１”を示す情報と、暗号化データとして“暗号化データＴ”と、識別情報として“ＥｗＦｓｉｈ”を示す情報とが関連付けて記憶されている。また、ＤＢ４のＮｏ．２のデータには、バージョン情報として“ｖ２”を示す情報と、暗号化データとして“暗号化データＴＲ”と、識別情報として“ｕ１ＷＬＭ

ｏ”を示す情報とが関連付けて記憶されている。

[0124] バージョン情報は、図１０のＮｏ．１のデータでは、サブパラメータｖｐｉ１を用いて暗号化データＴを生成したことを示す“ｖ１”を、バージョン情報として記憶している。

[0125] 識別情報は、暗号化データを生成するために用いた特徴量データを抽出した端末装置を識別するための情報である。図１０のＮｏ．１のデータでは、端末装置１を用いて暗号化データＴを生成したことを示す“ＥｗＦｓｉｈ”を、識別情報として記憶している。

[0126] 端末装置１は、照合のために端末装置１に入力される特徴量データｙに対して、変換パラメータｖｐを用いてステップＳ１５の処理を行うことにより、暗号化データＴ´を生成する。

[0127] なお、特徴量データｙを暗号化するに際し、パラメータ生成部１４０は、サブパラメータｖｐｉ１とは異なるサブパラメータｖｐｉ２を取得してステップＳ１４の処理を行うことにより、変換パラメータｖｐｘを生成する場合がある。この場合、端末装置１は、照合のために端末装置１に入力される特徴量データｙに対して、変換パラメータｖｐｘを用いてステップＳ１５の処理を行うことにより、暗号化データＴ´´を生成する。変換パラメータｖｐｘが、本実施形態の端末側更新変換パラメータの一例である。

[0128] ＜２．８．照合システムにおいて照合を行う処理の流れ＞

＜２．８．１．実施例１＞

続いて、照合システム１０００Ａにおいて照合を行う処理の流れの一例について説明する。実施例１として、照合装置３において暗号化データＴを更新暗号化データＴ３に変換しない、つまり、端末装置１において、変換パラメータｖｐを用いて特徴量データｘ及び特徴量データｙを暗号化したときの処理の流れについて説明する。

[0129] 暗号化データＴ´が、実施例１の照合装置３が照合を行うための第２暗号化入力情報、及び第４暗号化入力情報の一例である。また、特徴量データｘが、実施例１の第１入力情報、及び第３入力情報の一例であり、特徴量デー

タｙが、実施例１の第２入力情報、及び第４入力情報の一例である。

[0130] 図１１を参照して、実施例１において暗号化データＴと暗号化データＴ´とを照合する処理の流れについて説明する。図１１は、照合システム１００ＯＡにおいて暗号化データＴと暗号化データＴ´とを照合する処理の流れを示すシーケンス図である。なお、上述したように、暗号化データＴ´は、サブパラメータｖｐｉ１から生成された変換パラメータｖｐを用いて特徴量データｙを暗号化したデータに相当する。また、特徴量データｘ及び特徴量データｙを抽出したときの端末装置１のユーザを識別する識別情報は、同じであると仮定する。

[0131] ステップＳ２１において、ネットワークＩ／Ｆ１０１は、暗号化データＴ´と、特徴量データｙを抽出したときの端末装置１のユーザを識別する識別情報とを照合装置３に送信する。ステップＳ２２において、ネットワークＩ／Ｆ３０１は、端末装置１が送信した暗号化データＴ´と、特徴量データｙを抽出したときの端末装置１のユーザを識別する識別情報とを受信する。

[0132] ステップＳ２３において、照合処理部３５０は、暗号化データＴをＤＢ４から取得する。暗号化データＴは、ステップＳ２２において、暗号化データＴ´と共に受信した端末装置１のユーザを識別する識別情報に対応する情報に相当する。

[0133] ステップＳ２４において、照合処理部３５０は、ステップＳ２２で受信した暗号化データＴ´と、ステップＳ２３で取得した暗号化データＴとを照合する。ステップＳ２５において、照合処理部３５０は、ステップＳ２５の照合処理の結果を端末装置１に送信する。

[0134] 上述したように、端末装置１では、変換パラメータｖｐを用いて特徴量データｘ及び特徴量データｙを暗号化して、暗号化データＴ及び暗号化データＴ´を生成する。特徴量データｘと特徴量データｙとは、互いに近いデータである。この場合、照合処理部３５０は、暗号化データＴ及び暗号化データＴ´が近いデータであるとの照合結果を端末装置１に送信する。端末装置１は、照合装置３から受信した照合処理の結果に基づいて、端末装置１のユー

ザの認証を行ってもよい。

[0135] 続いて、本実施例において、メンテナンスやバージョン変更により、端末装置１がサブパラメータｖｐｉ２を用いて変換パラメータｖｐｘを生成して暗号化を行うときの照合システム１０００Ａにおける暗号化データ変換処理の流れについて説明する。図１２は、暗号化データ変換処理の流れを示すシーケンス図である。

[0136] ステップＳ３１において、サブパラメータ生成装置２は、照合装置３に対して、サブパラメータｖｐｉ１、及びサブパラメータｖｐｉ２を送信する。なお、端末装置１は、マスタパラメータｖｐｍ１及びサブパラメータｖｐｉ１に基づいて変換パラメータｖｐを生成する。また、端末装置１は、マスタパラメータｖｐｍ１及びサブパラメータｖｐｉ２に基づいて変換パラメータｖｐｘを生成する。

[0137] ステップＳ３２において、照合装置３は、サブパラメータｖｐｉ１、サブパラメータｖｐｉ２及びマスタパラメータｖｐｍ１に基づいて、暗号変換パラメータｖｐ´を生成する。

[0138] ここで、図１３を参照して、暗号変換パラメータｖｐ´を生成する処理の流れについて説明する。図１３は、暗号変換パラメータｖｐ´を生成する処理の流れを示すフローチャートである。

[0139] ステップＳ４１において、サブパラメータ取得部３１０は、ネットワークＩ／Ｆ３０１を介して、サブパラメータ生成装置２からサブパラメータｖｐｉ１、及びサブパラメータｖｐｉ２を取得する。

[0140] ステップＳ４２において、パラメータ生成部３３０は、マスタパラメータｖｐｍ１及びサブパラメータｖｐｉ１から、パラメータｖｐ１を生成する。第１の実施形態において、端末装置１及び照合装置３が用いるマスタパラメータｖｐｍ１は、共通化されている。つまり、ステップＳ４２において生成されるパラメータｖｐ１は、変換パラメータｖｐに相当するパラメータである。

[0141] ステップＳ４３において、パラメータ生成部３３０は、マスタパラメータ

ｖｐｍ１及びサブパラメータｖｐｉ２から、パラメータｖｐ２を生成する。パラメータｖｐ２は、パラメータｖｐ２を用いて特徴量データｘを暗号化することにより、暗号化データＴ´´を生成することができるパラメータ（置換鍵Ｋ´）に相当する（図８参照）。パラメータｖｐ２が、本実施形態の更新変換パラメータの一例である。

[0142] ステップＳ４４において、パラメータ生成部３３０は、パラメータｖｐ１とパラメータｖｐ２とを合成して、暗号変換パラメータｖｐ´を生成する。具体的に、パラメータ生成部３３０は、パラメータｖｐ１を逆変換したパラメータと、パラメータｖｐ２とを合成することにより、暗号変換パラメータｖｐ´を生成する。

[0143] 図１２のシーケンス図に戻って説明を続ける。ステップＳ３３において、更新情報生成部３４０は、暗号化データＴをＤＢ４から取得する。暗号化データＴは、ステップＳ４１において受信したサブパラメータｖｐｉ１を示すバージョン情報に関連つけられている暗号化データに相当する（図１０参照）。

[0144] ステップＳ３４において、更新情報生成部３４０は、暗号変換パラメータｖｐ´を用いて暗号化データＴを変換することにより、更新暗号化データＴ３を生成する。

[0145] ステップＳ３５において、更新情報生成部３４０は、更新暗号化データＴ３をＤＢ４に送信する。ステップＳ３６において、ＤＢ４は、更新暗号化データＴ３により暗号化データＴを上書きしてもよい、又は、暗号化データＴと更新暗号化データＴ３とを、端末装置１の識別情報に関連付けて記憶してもよい。

[0146] ＜２．８．２．実施例２＞

続いて、照合システム１０００Ａにおいて照合を行う処理の流れの他の例について説明する。実施例２として、照合装置３において暗号化データＴを更新暗号化データＴ３に変換する、つまり、端末装置１において、変換パラメータｖｐを用いて特徴量データｘを暗号化し、かつ、変換パラメータｖｐ

ｘを用いて特徴量データｙを暗号化したときの処理の流れについて説明する。

[0147] なお、暗号化データＴ´´が、実施例２の照合装置３が照合を行うための第２暗号化入力情報、及び第４暗号化入力情報の一例である。また、特徴量データｘが、実施例２の第１入力情報、及び第３入力情報の一例であり、特徴量データｙが、実施例２の第２入力情報、及び第４入力情報の一例である。

[0148] 図１４を参照して、実施例２において暗号化データＴと暗号化データＴ´´とを照合する処理の流れについて説明する。図１４は、照合システム１００Ａにおいて暗号化データＴと暗号化データＴ´´とを照合する処理の流れを示すシーケンス図である。なお、上述したように、暗号化データＴ´´は、サブパラメータｖｐｉ２から生成された変換パラメータｖｐｘを用いて特徴量データｙを暗号化したデータに相当する。また、特徴量データｘ及び特徴量データｙを抽出したときの端末装置１のユーザを識別する識別情報は、同じであると仮定する。

[0149] ステップＳ５１において、ネットワークＩ／Ｆ１０１は、暗号化データＴ´´と、特徴量データｙを抽出したときの端末装置１のユーザを識別する識別情報とを照合装置３に送信する。ステップＳ５２において、ネットワークＩ／Ｆ３０１は、端末装置１が送信した暗号化データＴ´´と、特徴量データｙを抽出したときの端末装置１のユーザを識別する識別情報とを受信する。

[0150] ステップＳ５３において、照合処理部３５０は、暗号化データＴをＤＢ４から取得する。暗号化データＴは、ステップＳ５２において、暗号化データＴ´´と共に受信した端末装置１のユーザを識別する識別情報に対応する情報に相当する。

[0151] 続いて、ステップＳ５４において、サブパラメータ生成装置２は、照合装置３に対して、サブパラメータｖｐｉ１、及びサブパラメータｖｐｉ２を送信する。

[0152] ステップＳ５５において、照合装置３は、サブパラメータｖｐｉ１、サブパラメータｖｐｉ２及びマスタパラメータｖｐｍ１に基づいて、暗号変換パラメータｖｐ´を生成する。ステップＳ５５の工程は、ステップＳ３２と同様の工程であるため、重複する説明を省略する。

[0153] ステップＳ５６において、更新情報生成部３４０は、暗号変換パラメータｖｐ´を用いて暗号化データＴを変換することにより、更新暗号化データＴ３を生成する。

[0154] ステップＳ５７において、照合処理部３５０は、ステップＳ５２で受信した暗号化データＴ´´と、ステップＳ５６で生成した更新暗号化データＴ３とを照合する。

[0155] 図８において説明したように、更新暗号化データＴ３に含まれる要素の並び順は、暗号化データＴ´´に含まれる要素の並び順と同じであり、更新暗号化データＴ３は、暗号化データＴ´´に相当するデータである。この場合、ステップＳ５６において、照合処理部３５０は、暗号化データＴ及び暗号化データＴ´´が近いデータであるとの照合結果を端末装置１に送信する。

[0156] なお、端末装置１は、照合装置３から受信した照合処理の結果に基づいて、端末装置１のユーザの認証を行ってもよい。

[0157] ステップＳ５９において、更新情報生成部３４０は、更新暗号化データＴ３をＤＢ４に送信する。なお、暗号化データＴ´と更新暗号化データＴ３とが近いデータである場合に、ステップＳ５９の処理を行うようにしてもよい。また、ＤＢ４は、更新暗号化データＴ３により暗号化データＴを上書きしてもよい、又は、暗号化データＴと更新暗号化データＴ３とを、端末装置１のユーザの識別情報に関連付けて記憶してもよい。

[0158] なお、実施例２において、ステップＳ５７の照合処理とステップＳ５６の暗号化データＴを変換する処理との順番を入れ替えてもよい。つまり、照合装置３は、暗号化データＴと暗号化データＴ´´との照合処理の結果に基づいて暗号化データＴを変換する処理の実行可否を判断するようにしてもよい。

[0159] なお、ステップＳ５７の照合処理とステップＳ５６の暗号化データＴを変換する処理との順番を入れ替えた場合、暗号化データＴの生成に用いられた変換パラメータｖｐと、暗号化データＴ´´の生成に用いられた変換パラメータｖｐｘとが異なるため、暗号化データＴ´´は、暗号化データＴに対して近いデータではない。ステップＳ５７の照合処理において、特徴量データｘ及び特徴量データｙを抽出したときの端末装置１のユーザを識別する識別情報が同じ場合であって、かつ、暗号化データＴ´´が、暗号化データＴに対して近いデータではない場合に、更新情報生成部３４０がステップＳ５６の処理を行うようにしてもよい。

[0160] ＜２．８．３．第１の実施形態のまとめ＞

以上説明したように、本実施形態において、端末装置１は、サブパラメータｖｐｉ１とマスタパラメータｖｐｍ１とを用いて、入力情報を暗号化するための変換パラメータｖｐを生成する。マスタパラメータｖｐｍ１は、端末装置１の保護領域１０２に記憶されているため、ネットワークを介した置換鍵の送受信に比べてマスタパラメータｖｐｍ１が漏洩するリスクが少ない。また、実施例１においては、端末装置１が用いたサブパラメータｖｐｉ１とマスタパラメータｖｐｍ１に関する情報が無くとも照合装置３が照合を行うことができるため、情報が漏洩するリスクをより低減することができ、かつ照合精度の劣化の抑制することが可能である。

[0161] さらに、実施例２では、サブパラメータｖｐｉ１の代わりにサブパラメータｖｐｉ２を用いて変換パラメータｖｐｘを生成することにより、変換パラメータｖｐ１によって変換した暗号化データＴを無効化するため、セキュリティ性をより高めることが可能である。

[0162] さらに、実施例２において、照合装置３は、暗号変換パラメータｖｐ´を用いて暗号化データＴを変換することにより、暗号化データＴを特徴量データｘに復号することなく更新暗号化データＴ３に変換することができる。更新暗号化データＴ３は、変換パラメータｖｐｘによって特徴量データｘを暗号化した暗号化データＴ´´に相当するデータセットであるため、照合処理

の精度を維持することができる。このようにすることにより、本実施形態では、照合精度の劣化の抑制と情報の漏洩リスクの低減とを両立可能な暗号化処理を実現することが可能である。

[0163] ＜３．第１の実施形態の変形例＞

＜３．１．変形例１＞

続いて、第１の実施形態の変形例１について、図１５を参照して説明する。図１５は、第１の実施形態の第１の変形例としてのハミング距離マスクによるキャンセラブル変換を説明するための説明図である。

[0164] 照合システム１０００Ａにおけるキャンセラブル変換として、特徴量データｘに含まれる要素を並び変える手法（図５及び図８参照）以外にも、例えば、ハミング距離マスクと呼ばれる手法により、特徴量データｘを暗号化してもよい。ハミング距離マスクによるキャンセラブル変換において、変換処理部１５０は、特徴量データ

[数15]

$$\boldsymbol{x} = (0,1,0,1,1,1,0)$$

の各次元の要素に対し、ランダムなビット列からなるデータセットであるマスク配列

[数16]

$$\boldsymbol{r} = (1,1,0,0,0,1,1) \cdots \quad (式4-1)$$

の各次元の要素の論理的排他和を計算することにより、暗号化データＴを生成する（図１５、右側上段参照）。

[0165] ハミング距離マスクによるキャンセラブル変換では、特徴量データｘの各次元の特徴量データの要素をマスクするランダムなビット列からなるマスク配列ｒが、本変形例の変換パラメータｖｐの一例である。また、特徴量データｙの各次元の要素に対しても、ランダムなビット列からなるマスク配列ｒ

の論理的排他和を計算することにより暗号化データＴ´を生成する。

[0166] 特徴量データｘに対する特徴量データｙのハミング距離は、暗号化データＴ及び暗号化データＴ´のハミング距離と一致するため、本変形例のキャンセラブル変換においても、照合処理の精度を維持することが可能である。

[0167] なお、照合装置３において、暗号化データＴを更新暗号化データＴ３に変換する際には、（式４－１）とは異なる配列を持つランダムなビット列からなるデータセットであるマスク配列ｒ´を暗号変換パラメータｖｐ´として用いるとよい。このようにすることにより、暗号化データＴを特徴量データｘに復号することなく、暗号化データＴを更新暗号化データＴ３に変換することが可能である。なお、この場合において、端末装置１においては、特徴量データｙに対してマスク配列ｒ´の論理的排他和を計算することにより、暗号化データＴ´´が生成されているものとする。

[0168] ＜３．２．変形例２＞

続いて、第１の実施形態の変形例２について、図１６を参照して説明する。図１６は、第１の実施形態の第２の変形例に係る暗号変換パラメータｖｐ´を生成する処理の流れを示すフローチャートである。

[0169] 照合システム１０００Ａにおいて暗号変換パラメータｖｐ´を生成する態様として、第１の実施形態では、サブパラメータｖｐｉ１及びサブパラメータｖｐｉ２と、マスタパラメータｖｐｍ１とを用いる例について説明を行った。

[0170] 本変形例では、照合装置３に、端末装置１及び端末装置１に相当する要素を備える他の情報処理装置が接続されている場合において、記憶領域３２０に記憶されている複数のマスタパラメータ（例えば、マスタパラメータｖｐｍ１及びマスタパラメータｖｐｍ２）を用いて暗号変換パラメータｖｐ´を生成する例について図１６を参照して説明を行う。また、マスタパラメータｖｐｍ２が、端末装置１に相当する要素を備える他の情報処理装置の保護領域に記憶されていると仮定する。

[0171] なお、図１６のフローチャートは、図１２のステップＳ３２において行わ

れる処理である。また、図１６のフローチャートにおいて、照合装置３は、ステップＳ３１の工程において、サブパラメータｖｐｉ１をサブパラメータ生成装置２から受信したと仮定して説明を行う。

[0172] ステップＳ６１において、サブパラメータ取得部３１０は、ネットワークＩ／Ｆ３０１を介して、サブパラメータ生成装置２からサブパラメータｖｐｉ１を取得する。

[0173] ステップＳ６２において、パラメータ生成部３３０は、マスタパラメータｖｐｍ１及びサブパラメータｖｐｉ１から、パラメータｖｐ３を生成する。マスタパラメータｖｐｍ１は、端末装置１に記憶されているマスタパラメータである。つまり、ステップＳ６２において生成されるパラメータｖｐ３は、変換パラメータｖｐに相当するパラメータである。

[0174] ステップＳ６３において、パラメータ生成部３３０は、マスタパラメータｖｐｍ２及びサブパラメータｖｐｉ１から、パラメータｖｐ４を生成する。マスタパラメータｖｐｍ２は、端末装置１に相当する要素を備える他の情報処理装置に記憶されているマスタパラメータである。つまり、ステップＳ６３において生成されるパラメータｖｐ４は、端末装置１に相当する要素を備える他の情報処理装置において特徴量データを暗号化するための変換パラメータに相当する。また、マスタパラメータｖｐｍ２は、本実施形態の第４パラメータの一例である。パラメータｖｐ４が、本実施形態の更新変換パラメータの一例である。

[0175] ステップＳ６４において、パラメータ生成部３３０は、パラメータｖｐ３とパラメータｖｐ４とを合成して、暗号変換パラメータｖｐ´を生成する。具体的に、パラメータ生成部３３０は、パラメータｖｐ３を逆変換したパラメータと、パラメータｖｐ４とを合成することにより、暗号変換パラメータｖｐ´を生成する。ステップＳ６４以降の処理は、第１の実施形態と同じである。

[0176] なお、第１の実施形態の実施例１を本変形例に対して適用する場合、ＤＢ４は、バージョン情報として、暗号化データを生成するために用いたマスタ

パラメータを識別するための情報を記憶するようにしてもよい（図１０参照）。

[0177] このように、本変形例の照合装置３は、端末装置１及び端末装置１に相当する要素を備える他の情報処理装置において、同一人物の生体情報が暗号化された場合であっても、マスタパラメータｖｐｍ１及びマスタパラメータｖｐｍ２と、サブパラメータｖｐｉ１とを用いて暗号変換パラメータｖｐ´を生成することができる。本変形例では、第１の実施形態と同様に照合精度の劣化の抑制と情報の漏洩リスクの低減とを両立可能な暗号化処理を実施可能である。さらに、本変形例では、端末装置１によって暗号化された生体情報に対し、端末装置１に相当する要素を備える他の情報処理装置に生体情報を入力することによる照合処理を行うことが可能である。

[0178] ＜３．３．変形例３＞

続いて、第１の実施形態の変形例３に係る端末装置１の構成について、図１７を参照して説明する。図１７は、第１の実施形態の変形例３に係る端末装置１の機能構成を示す機能ブロック図である。変形例３に係る端末装置１は、第１の実施形態のサブパラメータ生成部２１０に相当する要素、サブパラメータ記憶部２３０に相当する要素及びパラメータ生成部３３０に相当する要素を備える。なお、図１７において、図４に示す端末装置１の要素と同じ要素には同じ符号を付し、重複する説明を省略する。

[0179] 本変形例に係る端末装置１のコントローラ１００は、特徴量算出部１２０、変換処理部１５０、サブパラメータ生成部１６０、パラメータ生成部１７０、及び記憶領域１８０を備える。

[0180] サブパラメータ生成部１６０は、第１の実施形態に係るサブパラメータ生成部２１０に相当する要素である。つまり、サブパラメータ生成部１６０は、変換パラメータｖｐを生成するためのサブパラメータｖｐｉ１を生成する。サブパラメータ生成部１６０は、例えば、サブパラメータｖｐｉ１として、乱数を生成するためのサブ乱数シードを生成する。なお、サブパラメータ生成部１６０は、サブパラメータｖｐｉ１とは異なるサブパラメータｖｐｉ

２を生成することも可能である。

[0181] パラメータ生成部１７０は、第１の実施形態に係るパラメータ生成部１４０に相当する要素とパラメータ生成部３３０に相当する要素とを併せ持つ要素である。つまり、パラメータ生成部１７０は、記憶領域１８０に記憶されているマスタパラメータｖｐｍ１及びサブパラメータｖｐｉ１に基づいて、端末装置１に入力された情報を暗号化するための変換パラメータｖｐを生成する。また、パラメータ生成部１７０は、記憶領域１８０に記憶されているマスタパラメータｖｐｍ１と、サブパラメータｖｐｉ１と、サブパラメータｖｐｉ１とは異なるサブパラメータ（例えば、サブパラメータｖｐｉ２）とを用いて、暗号変換パラメータｖｐ´を生成する。なお、変換処理部１５０は、特徴量データｘを変換パラメータｖｐにより暗号化した暗号化データＴを、暗号変換パラメータｖｐ´を用いて変換することにより、更新暗号化データＴ３を生成することが可能である。

[0182] 記憶領域１８０は、第１の実施形態に係る記憶領域１３０に相当する要素とサブパラメータ記憶部２３０に相当する要素とを併せ持つ要素である。つまり、記憶領域１８０は、変換パラメータｖｐ又は暗号変換パラメータｖｐ´を生成するために用いられるマスタパラメータｖｐｍ１と、サブパラメータ生成部１６０が生成したサブパラメータｖｐｉ１及びサブパラメータｖｐｉ２等のサブパラメータを記憶する。記憶領域１８０は、端末装置１を識別する識別情報、又は端末装置１に生体情報を入力したユーザを識別するための識別情報を、サブパラメータｖｐｉ１及びサブパラメータｖｐｉ２等に関連付けて記憶してもよい。

[0183] 本変形例においては、照合装置３にマスタパラメータｖｐｍ１、サブパラメータｖｐｉ１及びサブパラメータｖｐｉ２を実装していない場合であっても端末装置１において暗号化データＴ´´を生成する処理、及び暗号化データＴを更新暗号化データＴ３に変換する処理を行うことが可能である。したがって、第１の実施形態と同様に本変形例においても、照合精度の劣化の抑制と情報の漏洩リスクの低減とを両立可能な暗号化処理を実現することが可

能である。

[0184] ＜４．第２の実施形態＞

続いて、図１８から図２１を参照して、本発明の第２の実施形態について説明する。図１８は、本実施形態の照合システム１０００Ｂの運用形態の一例を示す図である。なお、図１８の照合システム１０００Ｂにおいて、図１の照合システム１０００Ａと同じ構成には、同じ符号を付し、重複する説明を省略する。

[0185] 図１８に示すように、照合システム１０００Ｂは、判定装置６を備える点において照合システム１０００Ａと異なる。

[0186] 図１９は、判定装置６の機能構成を示す機能ブロック図である。判定装置６の機能構成は、図２において説明した要素と同様のハードウェア構成において、判定装置６のＲＯＭ１２に格納されたプログラムや、判定装置６の記憶媒体１４から判定装置６のＲＡＭ１３にロードされたプログラムに従って、判定装置６のＣＰＵ１１が演算を行うことにより、判定装置６のソフトウェア制御部が構成される。

[0187] 以上のようにして構成されたソフトウェア制御部と、ハードウェアとの組み合わせによって、本実施形態に係る判定装置６の機能を実現する機能ブロックが構成される。

[0188] 判定装置６は、復号処理部６１０、及び類似度判定部６２０を備える。復号処理部６１０は、暗号文復号パラメータｓｋ´´により、照合装置３から受信した照合処理の結果を復号する。類似度判定部６２０は、復号処理部６１０が復号した照合処理の結果に基づいて、特徴量データＲと特徴量データＳとの類似度を判定する。

[0189] 続いて、図２０を参照して、本実施形態に係る照合処理部３５０の内部構成について説明する。図２０は、照合処理部３５０の内部構成を示す機能ブロック図である。

[0190] 図２０に示すように、照合処理部３５０は、準同型演算処理部３５１、及び暗号文変換処理部３５２を備える。準同型演算処理部３５１は、暗号化さ

れた情報を暗号化されたままの状態で加減算及び乗算する、いわゆる準同型演算を行う。暗号文変換処理部３５２は、準同型演算処理部３５１の演算結果を、暗号文変換パラメータｓｋ´によって暗号化する。

[0191] 続いて、図２１を参照して、照合システム１０００Ｂにおける照合処理の概要について説明する。図２１は、照合システム１０００Ｂにおける準同型演算処理を用いた照合処理の概要を示すモデル図である。

[0192] 端末装置１では、暗号化パラメータｐｋを用いて、特徴量データＲ＝（ｘ，ｙ）及び特徴量データＳ＝（ｘ´，ｙ´）を暗号化する。なお、特徴量データＲ＝（ｘ，ｙ）及び特徴量データＳ＝（ｘ´，ｙ´）は、同一人物の顔画像であると仮定する。暗号化パラメータｐｋが、本実施形態の変換パラメータの一例である。

[0193] パラメータ生成部１４０は、サブパラメータ生成装置２から受信したサブパラメータｖｐｉ１とマスタパラメータｖｐｍ１とを用いて暗号化パラメータｐｋを生成する。特徴量データＲ＝（ｘ，ｙ）を暗号化パラメータｐｋによって暗号化したデータがＥｎｃｐｋ（Ｒ）である。また、特徴量データＳ＝（ｘ´，ｙ´）を暗号化パラメータｐｋによって暗号化したデータがＥｎｃｐｋ（Ｓ）である。Ｅｎｃｐｋ（Ｒ）は、端末装置１からＤＢ４に送信される。また、Ｅｎｃｐｋ（Ｓ）は、端末装置１から照合装置３に送信される。

[0194] 照合装置３は、ＤＢ４が記憶しているＥｎｃｐｋ（Ｒ）を取得する。続いて、準同型演算処理部３５１は、Ｅｎｃｐｋ（Ｒ）とＥｎｃｐｋ（Ｓ）とを準同型演算することにより、Ｅｎｃｐｋ（Ｒ）とＥｎｃｐｋ（Ｓ）との類似度

[数17]

$$Enc_{pk}((x-x')^2+(y-y')^2)$$

を算出する。

[0195] 暗号文変換処理部３５２は、Ｅｎｃｐｋ（Ｒ）とＥｎｃｐｋ（Ｓ）との類

似度を暗号文変換パラメータｓｋ´によって暗号化し、暗号文

[数18]

$$Enc_{pk''}((x-x')^2+(y-y')^2)$$

・・・（式５－１）

を判定装置６に送信する（式５－１）。暗号文変換処理部３５２は、本変形例の暗号化類似度情報生成部の一例である。（式５－１）に示す暗号文は、Ｅｎｃｐｋ（Ｒ）とＥｎｃｐｋ（Ｓ）との類似度を示す情報が暗号化された暗号化類似度情報に相当する。また、暗号文変換パラメータｓｋ´は、暗号化パラメータｐｋに依存するパラメータである。

[0196] 復号処理部６１０は、照合装置３から受信した（式５－１）のＥｎｃｐｋ（Ｒ）とＥｎｃｐｋ（Ｓ）との類似度を示す情報を、暗号文復号パラメータｓｋ´´により復号する。暗号文復号パラメータｓｋ´´により、（式５－１）のＥｎｃｐｋ（Ｒ）とＥｎｃｐｋ（Ｓ）との類似度を示す情報は、判定装置６において演算可能な平文

[数19]

$$\sqrt{(x-x')^2+(y-y')^2}$$

・・・（式５－２）

に復号することができる。なお、暗号文復号パラメータｓｋ´´は、暗号化パラメータｐｋに依存するパラメータである。

[0197] 類似度判定部６２０は、（式５－２）に基づいて特徴量データＲ＝（ｘ，ｙ）と特徴量データＳ＝（ｘ´，ｙ´）との類似度を判定する。照合システム１０００Ｂは、類似度判定部６２０の判定結果に基づいて、端末装置１のユーザの認証を行ってもよい。

[0198] なお、端末装置１は、特徴量データＳ＝（ｘ´，ｙ´）を暗号化する際に、サブパラメータｖｐｉ２とマスタパラメータｖｐｍ１とを用いて暗号化パラメータｐｋ´を生成する場合がある。このような場合、パラメータ生成部

３３０は、サブパラメータ生成装置２からサブパラメータｖｐｉ２とマスタパラメータｖｐｍ１とを受信し、サブパラメータｖｐｉ２及びマスタパラメータｖｐｍ１と、マスタパラメータｖｐｍ１とを用いて暗号変換パラメータｖｐ´を生成する。

[0199] そして、暗号変換パラメータｖｐ´を用いて変換したＥｎｃｐｋ（Ｒ）と、暗号化パラメータｐｋ´を用いて特徴量データＳ＝（ｘ´，ｙ´）を暗号化したＥｎｃｐｋ´（Ｓ）とを準同型演算することにより、特徴量データＲ＝（ｘ，ｙ）と特徴量データＳ＝（ｘ´，ｙ´）とを照合することが可能である。

[0200] 以上説明したように、本実施形態では、準同型演算によりＥｎｃｐｋ（Ｒ）とＥｎｃｐｋ（Ｓ）とを照合する場合においても、第１の実施形態と同様にＥｎｃｐｋ（Ｒ）を特徴量データＲ＝（ｘ，ｙ）に復号することなく、Ｅｎｃｐｋ（Ｒ）を無効化することが可能である。

[0201] ＜５．第３の実施形態＞

続いて、図２２から図２４を参照して、本発明の第３の実施形態を説明する。上述した第１の実施形態及び第２の実施形態は、具体的な実施形態であるが、第３の実施形態は、より一般化された実施形態である。

[0202] 図２２は、第３の実施形態に係る端末装置１Ａの概略的な構成を例示するブロック図である。端末装置１Ａは、端末側取得部１１０Ａ、端末側記憶領域１３０Ａ、変換パラメータ生成部１４０Ａ、及び暗号化情報生成部１５０Ａを備える。

[0203] 端末側取得部１１０Ａは、第２パラメータを取得する。端末側記憶領域１３０Ａは、第１パラメータを記憶する。変換パラメータ生成部１４０Ａは、第１パラメータと第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行う。暗号化情報生成部１５０Ａは、変換パラメータを用いて入力情報を暗号化することにより暗号化入力情報を生成する。

[0204] 図２３は、第３の実施形態に係る暗号化情報変換装置３Ａの概略的な構成を例示するブロック図である。暗号化情報変換装置３Ａは、変換側取得部３

１０Ａ、変換側記憶領域３２０Ａ、暗号変換パラメータ生成部３３０Ａ、及び更新情報生成部３４０Ａを備える。

[0205] 変換側取得部３１０Ａは、暗号化入力情報を生成するために用いられた第２パラメータと、第２パラメータとは異なる第３パラメータとを取得する。変換側記憶領域３２０Ａは、第１パラメータを記憶する。暗号変換パラメータ生成部３３０Ａは、第１パラメータ、第２パラメータ、及び第３パラメータを用いて暗号化入力情報を変換するための暗号変換パラメータを生成する。更新情報生成部３４０Ａは、暗号変換パラメータを用いて暗号化入力情報を変換することにより、更新暗号化入力情報を生成する。

[0206] なお、変換側取得部３１０Ａ、変換側記憶領域３２０Ａ、第１パラメータを含む複数のマスタパラメータを記憶する暗号変換パラメータ生成部３３０Ａ、及び更新情報生成部３４０Ａを以下のように構成してもよい。例えば、変換側取得部３１０Ａは、暗号化入力情報を生成するために用いられた第２パラメータを取得する。変換側記憶領域３２０Ａは、第１パラメータを含む複数のマスタパラメータを記憶する。暗号変換パラメータ生成部３３０Ａは、複数のマスタパラメータと、第２パラメータとを用いて暗号化入力情報を変換するための暗号変換パラメータを生成する。更新情報生成部３４０Ａは、暗号変換パラメータを用いて暗号化入力情報を変換することにより、更新暗号化入力情報を生成する。

[0207] 照合処理部３５０Ａは、照合のために端末装置１Ａに入力される第１入力情報を、暗号化情報生成部１５０Ａが変換パラメータを用いて暗号化することにより生成される第１暗号化入力情報と、照合のために端末装置１Ａに入力される第１入力情報とは異なる第２入力情報を暗号化することにより生成される第２暗号化入力情報とに基づいて、第１入力情報と第２入力情報とを照合する照合処理を行う。

[0208] なお、照合処理部３５０Ａを以下のように構成してもよい。例えば、照合処理部３５０Ａは、照合のために端末装置１Ａに入力される第３入力情報を、暗号化情報生成部１５０Ａが変換パラメータを用いて暗号化することによ

り生成される第３暗号化入力情報と、照合のために端末装置１Ａに入力される第３入力情報とは異なる第４入力情報を暗号化することにより生成される第４暗号化入力情報とに基づいて、第３入力情報と第４入力情報とを照合する照合処理を行う。

[0209] 図２４は、本発明の第３の実施形態に係る照合システム１０００Ｃの概略的な構成を例示するブロック図である。図２４に示すように、照合システム１０００Ｃは、端末装置１Ａ、及び照合処理部３５０Ａを備える。

[0210] －第１及び第２の実施形態との関係

一例として、第３の実施形態に係る端末装置１Ａが、第１又は第２の実施形態に係る端末装置１の動作を実行してもよい。同様に、一例として、第３の実施形態に係る暗号化情報変換装置３Ａが、第１又は第２の実施形態に係る照合装置３の動作を実行してもよい。同様に、一例として、第３の実施形態に係る照合システム１０００Ｃが、第１の実施形態に係る照合システム１０００Ａ又は第２の実施形態に係る照合システム１０００Ｂの動作を実行してもよい。以上の場合、第１の実施形態又は第２の実施形態についての説明が第３の実施形態にも適用可能である。なお、第３の実施形態は以上の例に限定されるものではない。

[0211] ＜６．その他の実施形態＞

以上、本発明の実施形態を説明したが、本発明はこれらの実施形態に限定されるものではない。これらの実施形態は例示にすぎないということ、及び、本発明のスコープ及び精神から逸脱することなく様々な変形が可能であるということは、当業者に理解されるであろう。

[0212] 例えば、本明細書に記載されている処理におけるステップは、必ずしもフローチャート及びシーケンス図に記載された順序に沿って時系列に実行されなくてよい。例えば、処理におけるステップは、フローチャート及びシーケンス図として記載した順序と異なる順序で実行されても、並列的に実行されてもよい。また、処理におけるステップの一部が削除されてもよく、さらなるステップが処理に追加されてもよい。

[0213] また、本明細書において説明した端末装置の構成要素（端末側記憶領域、端末側取得部、変換パラメータ生成部、及び／又は、暗号化情報生成部）を備える装置（例えば、登録情報生成装置を構成する複数の装置（又はユニット）のうちの１つ以上の装置（又はユニット）、又は上記複数の装置（又はユニット）のうちの１つのためのモジュール）が提供されてもよい。本明細書において説明した暗号化情報変換装置の構成要素（変換側記憶領域、変換側取得部、暗号変換パラメータ生成部、及び／又は、更新情報生成部）を備える装置（例えば、照合情報生成装置を構成する複数の装置（又はユニット）のうちの１つ以上の装置（又はユニット）、又は上記複数の装置（又はユニット）のうちの１つのためのモジュール）が提供されてもよい。また、上記構成要素の処理を含む方法が提供されてもよく、上記構成要素の処理をプロセッサに実行させるためのプログラムが提供されてもよい。また、当該プログラムを記録したコンピュータに読み取り可能な非一時的記録媒体（Non-transitory computer readable medium）が提供されてもよい。当然ながら、このような装置、モジュール、方法、プログラム、及びコンピュータに読み取り可能な非一時的記録媒体も本発明に含まれる。

[0214] 上記実施形態の一部又は全部は、以下の付記のようにも記載され得るが、以下には限られない。

[0215] （付記１）

照合のために入力される入力情報を暗号化する端末装置であって、

第１パラメータを記憶する端末側記憶領域と、

第２パラメータを取得する端末側取得部と、

前記第１パラメータと前記第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行う変換パラメータ生成部と、

前記変換パラメータを用いて前記入力情報を暗号化することにより暗号化入力情報を生成する暗号化情報生成部と、を備える、

端末装置。

[0216] （付記２）

前記第１パラメータは、第1乱数シードであり、

前記第２パラメータは、第２乱数シードであり、

前記変換パラメータ生成部は、

前記変換パラメータ生成処理として、前記第１乱数シード及び前記第２乱数シードを用いて乱数を生成し、

前記暗号化情報生成部は、

前記変換パラメータとして、前記乱数を用いて前記入力情報を暗号化する、

付記１に記載の端末装置。

[0217] （付記３）

前記第２パラメータは、前記変換パラメータが暗号化された暗号化パラメータであり、

前記第１パラメータは、前記暗号化パラメータを復号するための秘密鍵であり、

前記変換パラメータ生成部は、

前記変換パラメータ生成処理として、前記暗号化パラメータを前記秘密鍵によって復号することにより、前記変換パラメータを生成する、

付記１に記載の端末装置。

[0218] （付記４）

前記端末側記憶領域、前記変換パラメータ生成部、及び前記暗号化情報生成部は、前記端末装置の保護領域に実装されている、

付記１から３のいずれか１項に記載の端末装置。

[0219] （付記５）

前記変換パラメータは、

前記暗号化情報生成部による暗号化の対象となる情報に含まれる要素の並び順を置き換える置換鍵であり、

前記暗号化情報生成部は、

前記入力情報に含まれる要素の並び順を、前記置換鍵を用いて置き換える

ことにより、前記暗号化入力情報を生成する、

付記１から４のいずれか１項に記載の端末装置。

[0220] （付記６）

前記変換パラメータは、

前記暗号化情報生成部による暗号化の対象となる情報に含まれる要素に対応するランダムなビット列からなるデータセットであり、

前記暗号化情報生成部は、

前記入力情報と前記データセットとの論理的排他和を計算することにより、前記暗号化入力情報を生成する、

付記１から４のいずれか１項に記載の端末装置。

[0221] （付記７）

照合のために入力される入力情報を、第１パラメータ及び第２パラメータに基づいて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換装置であって、

前記第１パラメータを記憶する変換側記憶領域と、

前記暗号化入力情報を生成するために用いられた前記第２パラメータと、前記第２パラメータとは異なる第３パラメータとを取得する変換側取得部と、

前記第１パラメータ、前記第２パラメータ、及び前記第３パラメータを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成する暗号変換パラメータ生成部と、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成する更新情報生成部と、を備える、

暗号化情報変換装置。

[0222] （付記８）

前記暗号変換パラメータ生成部は、

前記第１パラメータ及び前記第２パラメータを用いて前記変換パラメータ

を生成し、

前記第１パラメータ及び前記第３パラメータを用いて前記変換パラメータとは異なる更新変換パラメータを生成し、

前記変換パラメータと前記更新変換パラメータとを合成することにより、前記暗号変換パラメータを生成する、

付記７に記載の暗号化情報変換装置。

[0223]（付記９）

前記変換パラメータは、

前記入力情報に含まれる要素の並び順を置き換える第１置換鍵であり、

前記暗号変換パラメータは、

前記暗号化入力情報に含まれる要素の並び順を置き換える第２置換鍵であり、

前記更新情報生成部は、

前記暗号化入力情報に含まれる要素の並び順を、前記第２置換鍵を用いて置き換えることにより、前記更新暗号化入力情報を生成する、

付記７又は８に記載の暗号化情報変換装置。

[0224]（付記１０）

前記変換パラメータは、

前記入力情報に含まれる要素に対応するランダムなビット列からなる第１データセットであり、

前記暗号変換パラメータは、

前記暗号化入力情報に含まれる要素に対応するランダムなビット列であって、かつ前記第１データセットとは異なる第２データセットであり、

前記更新情報生成部は、

前記暗号化入力情報と前記第２データセットとの論理的排他和を計算することにより、前記更新暗号化入力情報を生成する、

付記７又は８に記載の暗号化情報変換装置。

[0225]（付記１１）

前記変換側記憶領域、前記暗号変換パラメータ生成部、及び前記更新情報生成部は、前記暗号化情報変換装置の保護領域に実装されている、

付記７から１０のいずれか１項に記載の暗号化情報変換装置。

[0226] （付記１２）

照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換装置であって、

前記第１パラメータを含む複数のマスタパラメータを記憶する変換側記憶領域と、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得する変換側取得部と、

複数の前記マスタパラメータと、前記第２パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成する暗号変換パラメータ生成部と、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成する更新情報生成部と、を備える、

暗号化情報変換装置。

[0227] （付記１３）

前記暗号変換パラメータ生成部は、

前記第１パラメータ及び前記第２パラメータを用いて前記変換パラメータを生成し、

前記第１パラメータ以外の前記マスタパラメータと、前記第２パラメータとを用いて、前記変換パラメータとは異なる更新変換パラメータを生成し、

前記変換パラメータと、前記更新変換パラメータとを合成することにより、前記暗号変換パラメータを生成する、

付記１２に記載の暗号化情報変換装置。

[0228] （付記１４）

前記変換パラメータは、

前記入力情報に含まれる要素の並び順を置き換える第１置換鍵であり、

前記暗号変換パラメータは、

前記暗号化入力情報に含まれる要素の並び順を置き換える第２置換鍵であり、

前記更新情報生成部は、

前記暗号化入力情報に含まれる要素の並び順を、前記第２置換鍵を用いて置き換えることにより、前記更新暗号化入力情報を生成する、

付記１２又は１３に記載の暗号化情報変換装置。

[0229]（付記１５）

前記変換パラメータは、

前記入力情報に含まれる要素に対応するランダムなビット列からなる第１データセットであり、

前記暗号変換パラメータは、

前記暗号化入力情報に含まれる要素に対応するランダムなビット列であって、かつ前記第１データセットとは異なる第２データセットであり、

前記更新情報生成部は、

前記暗号化入力情報と前記第２データセットとの論理的排他和を計算することにより、前記更新暗号化入力情報を生成する、

付記１２又は１３に記載の暗号化情報変換装置。

[0230]（付記１６）

前記変換側記憶領域、前記暗号変換パラメータ生成部、及び前記更新情報生成部は、前記暗号化情報変換装置の保護領域に実装されている、

付記１２から１５のいずれか１項に記載の暗号化情報変換装置。

[0231]（付記１７）

付記１から６のいずれか１項に記載の端末装置と、

照合のために前記端末装置に入力される第１入力情報を、前記暗号化情報生成部が前記変換パラメータを用いて暗号化することにより生成される第１

暗号化入力情報と、照合のために前記端末装置に入力される前記第１入力情報とは異なる第２入力情報を暗号化することにより生成される第２暗号化入力情報とに基づいて、前記第１入力情報と前記第２入力情報とを照合する照合処理を行う照合処理部と、を備える、

照合システム。

[0232] （付記１８）

付記７から１１のいずれか１項に記載の暗号化情報変換装置を備える、

付記１７に記載の照合システム。

[0233] （付記１９）

前記暗号化情報変換装置は、前記照合処理部を有する、

付記１８に記載の照合システム。

[0234] （付記２０）

前記照合処理部は、前記暗号化情報変換装置が備える保護領域に実装されている、

付記１９に記載の照合システム。

[0235] （付記２１）

前記端末装置及び前記暗号化情報変換装置に前記第２パラメータ及び前記第３パラメータを送信するパラメータ送信装置を備える、

付記１８から２０のいずれか１項に記載の照合システム。

[0236] （付記２２）

前記パラメータ送信装置は、

前記第２パラメータと前記第３パラメータとを生成するパラメータ生成部を有する、

付記２１に記載の照合システム。

[0237] （付記２３）

前記変換パラメータ生成部は、

前記第１パラメータと、前記第３パラメータとに基づいて、前記変換パラメータとは異なる端末側更新変換パラメータを生成可能であり、

前記暗号化情報生成部は、

前記端末側更新変換パラメータを用いて、前記第２入力情報を暗号化することにより前記第２暗号化入力情報を生成する、

付記２１又は２２に記載の照合システム。

[0238]（付記２４）

前記暗号変換パラメータ生成部は、

前記第１パラメータ、前記第２パラメータ、及び前記第３パラメータを用いて前記暗号変換パラメータを生成し、

前記更新情報生成部は、

前記第１パラメータ、前記第２パラメータ、及び前記第３パラメータを用いて生成された前記暗号変換パラメータによって前記第１暗号化入力情報を前記更新暗号化入力情報に変換し、

前記照合処理部は、

前記第１暗号化入力情報を変換して生成された前記更新暗号化入力情報と、前記端末側更新変換パラメータを用いて生成された前記第２暗号化入力情報とに基づいて前記照合処理を行う、

付記２３に記載の照合システム。

[0239]（付記２５）

前記照合処理部は、

前記第１暗号化入力情報と前記第２暗号化入力情報とを準同型演算することにより、前記第１入力情報と前記第２入力情報との類似度を暗号化した状態で出力する準同型演算処理部と、

暗号化した状態で出力された前記類似度を暗号化することにより暗号化類似度情報を生成する暗号化類似度情報生成部と、を有し、

前記照合システムは、

前記暗号化類似度情報を復号する復号処理部と、

復号された前記暗号化類似度情報に基づいて前記第１入力情報に対する前記第２入力情報の類似度を判定する類似度判定部と、を備える、

付記１７から２４のいずれか１項に記載の照合システム。

[0240]（付記２６）

付記１から６のいずれか１項に記載の端末装置と、

照合のために前記端末装置に入力される第３入力情報を、前記暗号化情報生成部が前記変換パラメータを用いて暗号化することにより生成される第３暗号化入力情報と、照合のために前記端末装置に入力される前記第３入力情報とは異なる第４入力情報を暗号化することにより生成される第４暗号化入力情報とに基づいて、前記第３入力情報と前記第４入力情報とを照合する照合処理を行う照合処理部と、を備える、

照合システム。

[0241]（付記２７）

付記７から１１のいずれか１項に記載の暗号化情報変換装置を備える、

付記２６に記載の照合システム。

[0242]（付記２８）

前記暗号化情報変換装置は、前記照合処理部を有する、

付記２７に記載の照合システム。

[0243]（付記２９）

前記照合処理部は、前記暗号化情報変換装置が備える保護領域に実装されている、

付記２８に記載の照合システム。

[0244]（付記３０）

前記端末装置及び前記暗号化情報変換装置に前記第２パラメータを送信するパラメータ送信装置を備える、

付記２７から２９のいずれか１項に記載の照合システム。

[0245]（付記３１）

前記パラメータ送信装置は、

前記第２パラメータを生成するパラメータ生成部を有する、

付記３０に記載の照合システム。

[0246]（付記３２）

前記端末装置は、

前記第１パラメータ及び前記第２パラメータとは異なる第４パラメータを、前記端末側記憶領域に記憶し、

前記変換パラメータ生成部は、

前記第２パラメータと、前記第４パラメータとに基づいて、前記変換パラメータとは異なる端末側更新変換パラメータを生成可能であり、

前記暗号化情報生成部は、

前記端末側更新変換パラメータを用いて、前記第４入力情報を暗号化することにより前記第４暗号化入力情報を生成する、

付記３０又は３１に記載の照合システム。

[0247]（付記３３）

前記暗号化情報変換装置は、

前記マスタパラメータとして、前記第４パラメータを記憶し、

前記暗号変換パラメータ生成部は、

前記第１パラメータ、前記第２パラメータ、及び前記第４パラメータを用いて前記暗号変換パラメータを生成し、

前記更新情報生成部は、

前記第４パラメータに基づいて生成した前記暗号変換パラメータを用いて前記第３暗号化入力情報を変換し、

前記照合処理部は、

前記更新情報生成部によって前記第３暗号化入力情報を変換して生成した前記更新暗号化入力情報と、前記端末装置において前記端末側更新変換パラメータを用いて生成された前記第４暗号化入力情報とに基づいて前記照合処理を行う、

付記３２に記載の照合システム。

[0248]（付記３４）

前記照合処理部は、

前記第３暗号化入力情報と前記第４暗号化入力情報とを準同型演算することにより、前記第３入力情報と前記第４入力情報との類似度を暗号化した状態で出力する準同型演算処理部と、

暗号化した状態で出力された前記類似度を暗号化することにより暗号化類似度情報を生成する暗号化類似度情報生成部と、を有し、

前記照合システムは、

前記暗号化類似度情報を復号する復号処理部と、

復号された前記暗号化類似度情報に基づいて前記第３入力情報に対する前記第４入力情報の類似度を判定する類似度判定部と、を備える、

付記２６から３３のいずれか１項に記載の照合システム。

[0249]（付記３５）

前記照合処理部は、

前記照合処理の結果を前記端末装置に送信する、

付記１７から３４のいずれか１項に記載の照合システム。

[0250]（付記３６）

記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、

照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、を備える、

入力情報暗号化方法。

[0251]（付記３７）

照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換方法であって、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、

前記第２パラメータとは異なる第３パラメータを取得することと、

記憶領域に記憶されている前記第１パラメータと、取得した前記第２パラメータ及び前記第３パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、を備える、

暗号化情報変換方法。

[0252]（付記３８）

照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換方法であって、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、

記憶領域に記憶されている前記第１パラメータ以外のマスタパラメータと、前記第２パラメータとを用いて、前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、を備える、

暗号化情報変換方法。

[0253]（付記３９）

端末装置の記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、

照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、

照合のための第１入力情報を、前記変換パラメータを用いて暗号化することにより生成される第１暗号化入力情報と、照合のために入力される前記第

１入力情報とは異なる第２入力情報を暗号化することにより生成される第２暗号化入力情報とに基づいて、前記第１入力情報と前記第２入力情報とを照合する照合処理を行うことと、を備える、

照合方法。

[0254]（付記４０）

端末装置の記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、

照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、

照合のために入力される第３入力情報を、前記変換パラメータを用いて暗号化することにより生成される第３暗号化入力情報と、照合のために入力される前記第３入力情報とは異なる第４入力情報を暗号化することにより生成される第４暗号化入力情報とに基づいて、前記第３入力情報と前記第４入力情報とを照合する照合処理を行うことと、を備える、

照合方法。

[0255]（付記４１）

記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、

照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、をプロセッサに実行させる、

入力情報暗号化プログラム。

[0256]（付記４２）

照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換プログラ

ムであって、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、

前記第２パラメータとは異なる第３パラメータを取得することと、

記憶領域に記憶されている前記第１パラメータと、取得した前記第２パラメータ及び前記第３パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、をプロセッサに実行させる、

暗号化情報変換プログラム。

[0257] （付記４３）

照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換プログラムであって、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、

記憶領域に記憶されている前記第１パラメータ以外のマスタパラメータと、前記第２パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、をプロセッサに実行させる、

暗号化情報変換プログラム。

産業上の利用可能性

[0258] 照合精度の劣化の抑制と情報の漏洩リスクの低減とを両立可能な暗号化処理を実現する端末装置、暗号化情報変換装置、照合システム、入力情報暗号

化方法、暗号化情報変換方法、照合方法、入力情報暗号化プログラム、及び暗号化情報変換プログラムを提供する。

符号の説明

[0259] １、１Ａ　端末装置

２　サブパラメータ生成装置

３　照合装置

３Ａ　暗号化情報変換装置

４　ＤＢ

５　ネットワーク

６　判定装置

１０２　保護領域

１１０　サブパラメータ取得部

１１０Ａ　端末側取得部

１２０　特徴量算出部

１３０　記憶領域

１３０Ａ　端末側記憶領域

１４０　パラメータ生成部

１４０Ａ　変換パラメータ生成部

１５０　変換処理部

１５０Ａ　暗号化情報生成部

１６０　サブパラメータ生成部

１７０　パラメータ生成部

１８０　記憶領域

２１０　サブパラメータ生成部

２２０　サブパラメータ送信部

２３０　サブパラメータ記憶部

３０２　保護領域

３１０　サブパラメータ取得部

３１０Ａ　変換側取得部

３２０　記憶領域

３２０Ａ　変換側記憶領域

３３０　パラメータ生成部

３３０Ａ　暗号変換パラメータ生成部

３４０、３４０Ａ　更新情報生成部

３５０、３５０Ａ　照合処理部

３５１　準同型演算処理部

３５２　暗号文変換処理部

６１０　復号処理部

６２０　類似度判定部

１０００Ａ、１０００Ｂ、１０００Ｃ　照合システム

請求の範囲

[請求項1] 照合のために入力される入力情報を暗号化する端末装置であって、

第１パラメータを記憶する端末側記憶領域と、

第２パラメータを取得する端末側取得部と、

前記第１パラメータと前記第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行う変換パラメータ生成部と、

前記変換パラメータを用いて前記入力情報を暗号化することにより暗号化入力情報を生成する暗号化情報生成部と、を備える、

端末装置。

[請求項2] 前記第１パラメータは、第1乱数シードであり、

前記第２パラメータは、第２乱数シードであり、

前記変換パラメータ生成部は、

前記変換パラメータ生成処理として、前記第１乱数シード及び前記第２乱数シードを用いて乱数を生成し、

前記暗号化情報生成部は、

前記変換パラメータとして、前記乱数を用いて前記入力情報を暗号化する、

請求項１に記載の端末装置。

[請求項3] 前記第２パラメータは、前記変換パラメータが暗号化された暗号化パラメータであり、

前記第１パラメータは、前記暗号化パラメータを復号するための秘密鍵であり、

前記変換パラメータ生成部は、

前記変換パラメータ生成処理として、前記暗号化パラメータを前記秘密鍵によって復号することにより、前記変換パラメータを生成する、

請求項１に記載の端末装置。

[請求項4] 前記端末側記憶領域、前記変換パラメータ生成部、及び前記暗号化情報生成部は、前記端末装置の保護領域に実装されている、

請求項１から３のいずれか１項に記載の端末装置。

[請求項5] 前記変換パラメータは、

前記暗号化情報生成部による暗号化の対象となる情報に含まれる要素の並び順を置き換える置換鍵であり、

前記暗号化情報生成部は、

前記入力情報に含まれる要素の並び順を、前記置換鍵を用いて置き換えることにより、前記暗号化入力情報を生成する、

請求項１から４のいずれか１項に記載の端末装置。

[請求項6] 前記変換パラメータは、

前記暗号化情報生成部による暗号化の対象となる情報に含まれる要素に対応するランダムなビット列からなるデータセットであり、

前記暗号化情報生成部は、

前記入力情報と前記データセットとの論理的排他和を計算することにより、前記暗号化入力情報を生成する、

請求項１から４のいずれか１項に記載の端末装置。

[請求項7] 照合のために入力される入力情報を、第１パラメータ及び第２パラメータに基づいて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換装置であって、

前記第１パラメータを記憶する変換側記憶領域と、

前記暗号化入力情報を生成するために用いられた前記第２パラメータと、前記第２パラメータとは異なる第３パラメータとを取得する変換側取得部と、

前記第１パラメータ、前記第２パラメータ、及び前記第３パラメータを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成する暗号変換パラメータ生成部と、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成する更新情報生成部と、を備える、

暗号化情報変換装置。

[請求項8] 前記暗号変換パラメータ生成部は、

前記第１パラメータ及び前記第２パラメータを用いて前記変換パラメータを生成し、

前記第１パラメータ及び前記第３パラメータを用いて前記変換パラメータとは異なる更新変換パラメータを生成し、

前記変換パラメータと前記更新変換パラメータとを合成することにより、前記暗号変換パラメータを生成する、

請求項７に記載の暗号化情報変換装置。

[請求項9] 前記変換パラメータは、

前記入力情報に含まれる要素の並び順を置き換える第１置換鍵であり、

前記暗号変換パラメータは、

前記暗号化入力情報に含まれる要素の並び順を置き換える第２置換鍵であり、

前記更新情報生成部は、

前記暗号化入力情報に含まれる要素の並び順を、前記第２置換鍵を用いて置き換えることにより、前記更新暗号化入力情報を生成する、

請求項７又は８に記載の暗号化情報変換装置。

[請求項10] 前記変換パラメータは、

前記入力情報に含まれる要素に対応するランダムなビット列からなる第１データセットであり、

前記暗号変換パラメータは、

前記暗号化入力情報に含まれる要素に対応するランダムなビット列であって、かつ前記第１データセットとは異なる第２データセットで

あり、

前記更新情報生成部は、

前記暗号化入力情報と前記第２データセットとの論理的排他和を計算することにより、前記更新暗号化入力情報を生成する、

請求項７又は８に記載の暗号化情報変換装置。

[請求項11] 前記変換側記憶領域、前記暗号変換パラメータ生成部、及び前記更新情報生成部は、前記暗号化情報変換装置の保護領域に実装されている、

請求項７から１０のいずれか１項に記載の暗号化情報変換装置。

[請求項12] 照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換装置であって、

前記第１パラメータを含む複数のマスタパラメータを記憶する変換側記憶領域と、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得する変換側取得部と、

複数の前記マスタパラメータと、前記第２パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成する暗号変換パラメータ生成部と、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成する更新情報生成部と、を備える、

暗号化情報変換装置。

[請求項13] 前記暗号変換パラメータ生成部は、

前記第１パラメータ及び前記第２パラメータを用いて前記変換パラメータを生成し、

前記第１パラメータ以外の前記マスタパラメータと、前記第２パラ

メータとを用いて、前記変換パラメータとは異なる更新変換パラメータを生成し、

前記変換パラメータと、前記更新変換パラメータとを合成することにより、前記暗号変換パラメータを生成する、

請求項１２に記載の暗号化情報変換装置。

[請求項14] 前記変換パラメータは、

前記入力情報に含まれる要素の並び順を置き換える第１置換鍵であり、

前記暗号変換パラメータは、

前記暗号化入力情報に含まれる要素の並び順を置き換える第２置換鍵であり、

前記更新情報生成部は、

前記暗号化入力情報に含まれる要素の並び順を、前記第２置換鍵を用いて置き換えることにより、前記更新暗号化入力情報を生成する、

請求項１２又は１３に記載の暗号化情報変換装置。

[請求項15] 前記変換パラメータは、

前記入力情報に含まれる要素に対応するランダムなビット列からなる第１データセットであり、

前記暗号変換パラメータは、

前記暗号化入力情報に含まれる要素に対応するランダムなビット列であって、かつ前記第１データセットとは異なる第２データセットであり、

前記更新情報生成部は、

前記暗号化入力情報と前記第２データセットとの論理的排他和を計算することにより、前記更新暗号化入力情報を生成する、

請求項１２又は１３に記載の暗号化情報変換装置。

[請求項16] 前記変換側記憶領域、前記暗号変換パラメータ生成部、及び前記更新情報生成部は、前記暗号化情報変換装置の保護領域に実装されてい

る、

請求項１２から１５のいずれか１項に記載の暗号化情報変換装置。

[請求項17] 請求項１から６のいずれか１項に記載の端末装置と、

照合のために前記端末装置に入力される第１入力情報を、前記暗号化情報生成部が前記変換パラメータを用いて暗号化することにより生成される第１暗号化入力情報と、照合のために前記端末装置に入力される前記第１入力情報とは異なる第２入力情報を暗号化することにより生成される第２暗号化入力情報とに基づいて、前記第１入力情報と前記第２入力情報とを照合する照合処理を行う照合処理部と、を備える、

照合システム。

[請求項18] 請求項７から１１のいずれか１項に記載の暗号化情報変換装置を備える、

請求項１７に記載の照合システム。

[請求項19] 前記暗号化情報変換装置は、前記照合処理部を有する、

請求項１８に記載の照合システム。

[請求項20] 前記照合処理部は、前記暗号化情報変換装置が備える保護領域に実装されている、

請求項１９に記載の照合システム。

[請求項21] 前記端末装置及び前記暗号化情報変換装置に前記第２パラメータ及び前記第３パラメータを送信するパラメータ送信装置を備える、

請求項１８から２０のいずれか１項に記載の照合システム。

[請求項22] 前記パラメータ送信装置は、

前記第２パラメータと前記第３パラメータとを生成するパラメータ生成部を有する、

請求項２１に記載の照合システム。

[請求項23] 前記変換パラメータ生成部は、

前記第１パラメータと、前記第３パラメータとに基づいて、前記変

換パラメータとは異なる端末側更新変換パラメータを生成可能であり、

前記暗号化情報生成部は、

前記端末側更新変換パラメータを用いて、前記第２入力情報を暗号化することにより前記第２暗号化入力情報を生成する、

請求項２１又は２２に記載の照合システム。

[請求項24] 前記暗号変換パラメータ生成部は、

前記第１パラメータ、前記第２パラメータ、及び前記第３パラメータを用いて前記暗号変換パラメータを生成し、

前記更新情報生成部は、

前記第１パラメータ、前記第２パラメータ、及び前記第３パラメータを用いて生成された前記暗号変換パラメータによって前記第１暗号化入力情報を前記更新暗号化入力情報に変換し、

前記照合処理部は、

前記第１暗号化入力情報を変換して生成された前記更新暗号化入力情報と、前記端末側更新変換パラメータを用いて生成された前記第２暗号化入力情報とに基づいて前記照合処理を行う、

請求項２３に記載の照合システム。

[請求項25] 前記照合処理部は、

前記第１暗号化入力情報と前記第２暗号化入力情報とを準同型演算することにより、前記第１入力情報と前記第２入力情報との類似度を暗号化した状態で出力する準同型演算処理部と、

暗号化した状態で出力された前記類似度を暗号化することにより暗号化類似度情報を生成する暗号化類似度情報生成部と、を有し、

前記照合システムは、

前記暗号化類似度情報を復号する復号処理部と、

復号された前記暗号化類似度情報に基づいて前記第１入力情報に対する前記第２入力情報の類似度を判定する類似度判定部と、を備える

、

請求項１７から２４のいずれか１項に記載の照合システム。

[請求項26] 請求項１から６のいずれか１項に記載の端末装置と、

照合のために前記端末装置に入力される第３入力情報を、前記暗号化情報生成部が前記変換パラメータを用いて暗号化することにより生成される第３暗号化入力情報と、照合のために前記端末装置に入力される前記第３入力情報とは異なる第４入力情報を暗号化することにより生成される第４暗号化入力情報とに基づいて、前記第３入力情報と前記第４入力情報とを照合する照合処理を行う照合処理部と、を備える、

照合システム。

[請求項27] 請求項７から１１のいずれか１項に記載の暗号化情報変換装置を備える、

請求項２６に記載の照合システム。

[請求項28] 前記暗号化情報変換装置は、前記照合処理部を有する、

請求項２７に記載の照合システム。

[請求項29] 前記照合処理部は、前記暗号化情報変換装置が備える保護領域に実装されている、

請求項２８に記載の照合システム。

[請求項30] 前記端末装置及び前記暗号化情報変換装置に前記第２パラメータを送信するパラメータ送信装置を備える、

請求項２７から２９のいずれか１項に記載の照合システム。

[請求項31] 前記パラメータ送信装置は、

前記第２パラメータを生成するパラメータ生成部を有する、

請求項３０に記載の照合システム。

[請求項32] 前記端末装置は、

前記第１パラメータ及び前記第２パラメータとは異なる第４パラメータを、前記端末側記憶領域に記憶し、

前記変換パラメータ生成部は、

前記第２パラメータと、前記第４パラメータとに基づいて、前記変換パラメータとは異なる端末側更新変換パラメータを生成可能であり、

前記暗号化情報生成部は、

前記端末側更新変換パラメータを用いて、前記第４入力情報を暗号化することにより前記第４暗号化入力情報を生成する、

請求項３０又は３１に記載の照合システム。

[請求項33] 前記暗号化情報変換装置は、

前記マスタパラメータとして、前記第４パラメータを記憶し、

前記暗号変換パラメータ生成部は、

前記第１パラメータ、前記第２パラメータ、及び前記第４パラメータを用いて前記暗号変換パラメータを生成し、

前記更新情報生成部は、

前記第４パラメータに基づいて生成した前記暗号変換パラメータを用いて前記第３暗号化入力情報を変換し、

前記照合処理部は、

前記更新情報生成部によって前記第３暗号化入力情報を変換して生成した前記更新暗号化入力情報と、前記端末装置において前記端末側更新変換パラメータを用いて生成された前記第４暗号化入力情報とに基づいて前記照合処理を行う、

請求項３２に記載の照合システム。

[請求項34] 前記照合処理部は、

前記第３暗号化入力情報と前記第４暗号化入力情報とを準同型演算することにより、前記第３入力情報と前記第４入力情報との類似度を暗号化した状態で出力する準同型演算処理部と、

暗号化した状態で出力された前記類似度を暗号化することにより暗号化類似度情報を生成する暗号化類似度情報生成部と、を有し、

前記照合システムは、

前記暗号化類似度情報を復号する復号処理部と、

復号された前記暗号化類似度情報に基づいて前記第３入力情報に対する前記第４入力情報の類似度を判定する類似度判定部と、を備える、

請求項２６から３３のいずれか１項に記載の照合システム。

[請求項35] 前記照合処理部は、

前記照合処理の結果を前記端末装置に送信する、

請求項１７から３４のいずれか１項に記載の照合システム。

[請求項36] 記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、

照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、を備える、

入力情報暗号化方法。

[請求項37] 照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換方法であって、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、

前記第２パラメータとは異なる第３パラメータを取得することと、

記憶領域に記憶されている前記第１パラメータと、取得した前記第２パラメータ及び前記第３パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、を備える、

暗号化情報変換方法。

[請求項38] 照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換方法であって、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、

記憶領域に記憶されている前記第１パラメータ以外のマスタパラメータと、前記第２パラメータとを用いて、前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、を備える、

暗号化情報変換方法。

[請求項39] 端末装置の記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、

照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、

照合のための第１入力情報を、前記変換パラメータを用いて暗号化することにより生成される第１暗号化入力情報と、照合のために入力される前記第１入力情報とは異なる第２入力情報を暗号化することにより生成される第２暗号化入力情報とに基づいて、前記第１入力情報と前記第２入力情報とを照合する照合処理を行うことと、を備える、

照合方法。

[請求項40] 端末装置の記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、

照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、

照合のために入力される第３入力情報を、前記変換パラメータを用いて暗号化することにより生成される第３暗号化入力情報と、照合のために入力される前記第３入力情報とは異なる第４入力情報を暗号化することにより生成される第４暗号化入力情報とに基づいて、前記第３入力情報と前記第４入力情報とを照合する照合処理を行うことと、を備える、

照合方法。

[請求項41] 記憶領域に記憶されている第１パラメータと前記第１パラメータとは異なる第２パラメータとに基づいて変換パラメータを生成する変換パラメータ生成処理を行うことと、

照合のために入力される入力情報を、前記変換パラメータを用いて暗号化することにより暗号化入力情報を生成することと、をプロセッサに実行させる、

入力情報暗号化プログラム。

[請求項42] 照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換プログラムであって、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、

前記第２パラメータとは異なる第３パラメータを取得することと、

記憶領域に記憶されている前記第１パラメータと、取得した前記第２パラメータ及び前記第３パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、をプロセッサに実行させる、

暗号化情報変換プログラム。

[請求項43] 照合のために入力される入力情報を、第１パラメータ及び第２パラメータを用いて生成した変換パラメータによって暗号化することにより生成される暗号化入力情報を、更新暗号化入力情報に変換する暗号化情報変換プログラムであって、

前記暗号化入力情報を生成するために用いられた前記第２パラメータを取得することと、

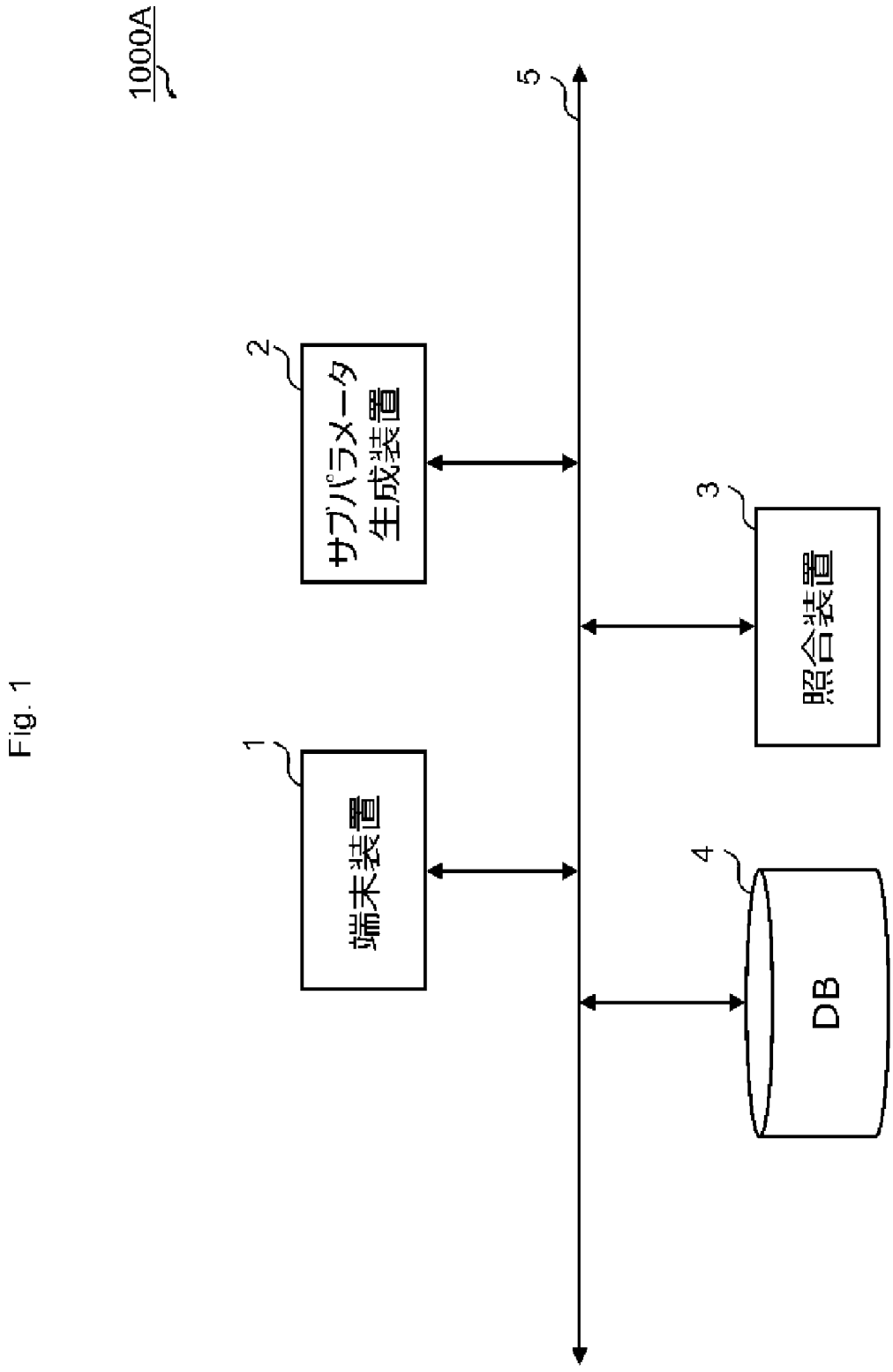
記憶領域に記憶されている前記第１パラメータ以外のマスタパラメータと、前記第２パラメータとを用いて前記暗号化入力情報を変換するための暗号変換パラメータを生成することと、

前記暗号変換パラメータを用いて前記暗号化入力情報を変換することにより、前記更新暗号化入力情報を生成することと、をプロセッサに実行させる、

暗号化情報変換プログラム。

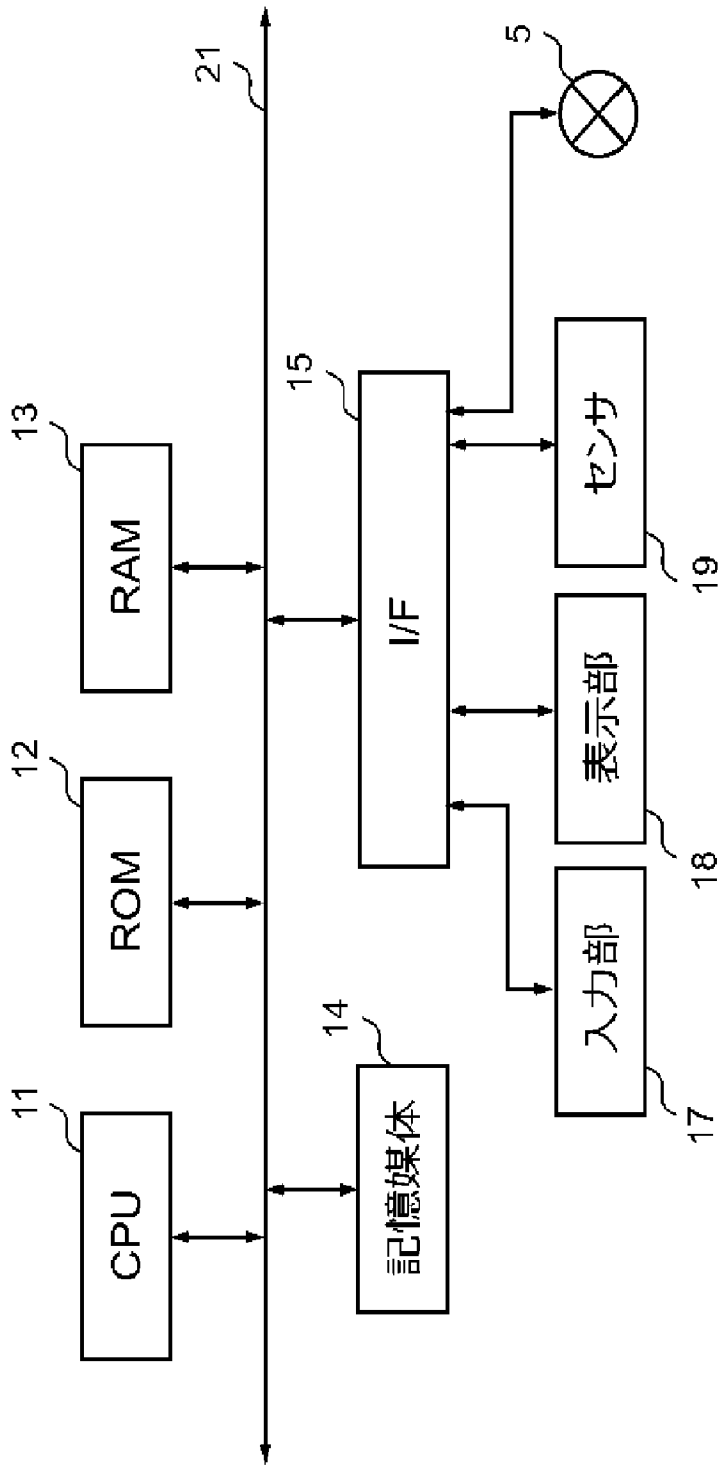
[図1]

Fig. 1



[図2]

Fig. 2



[図3]

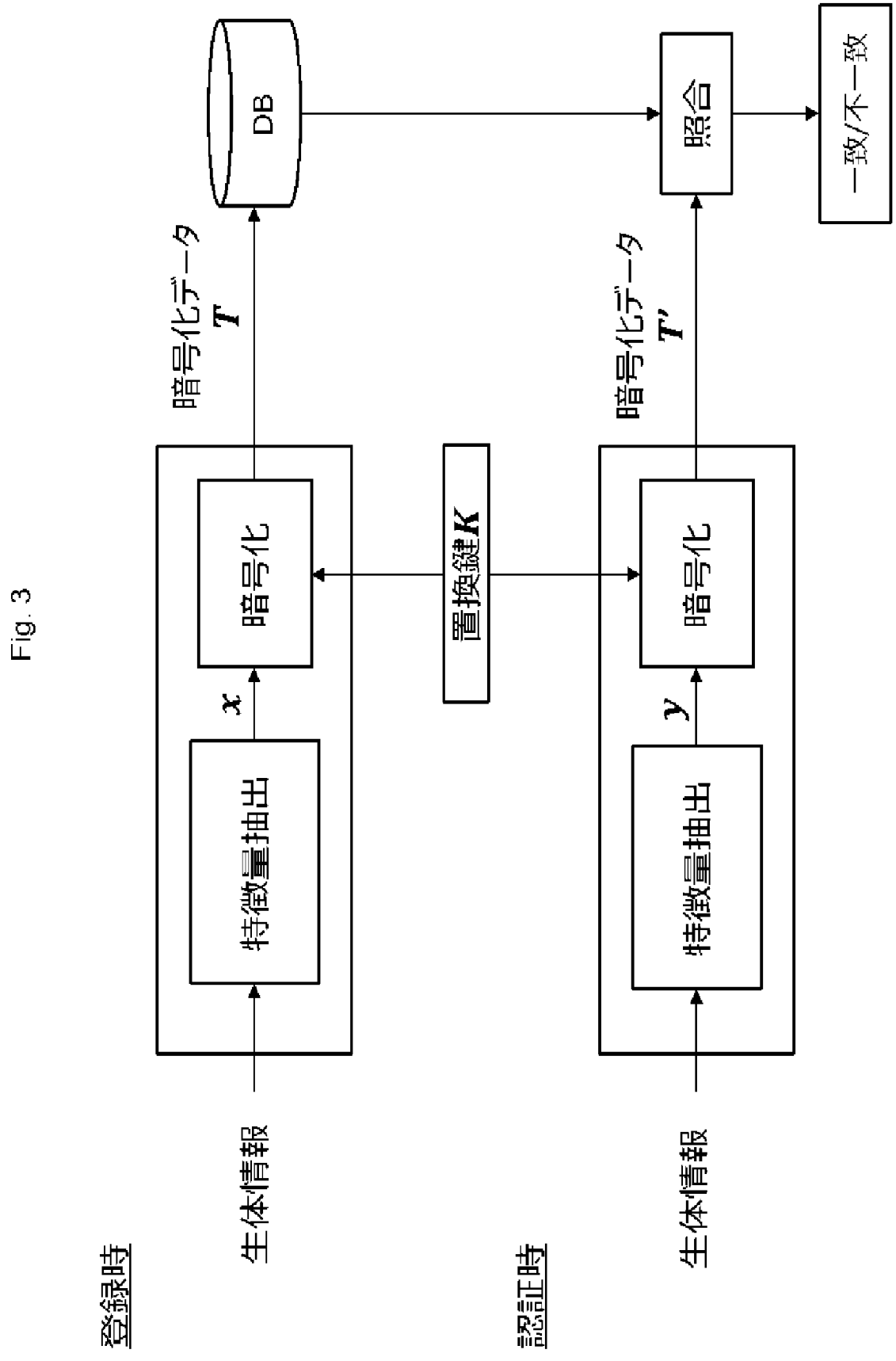
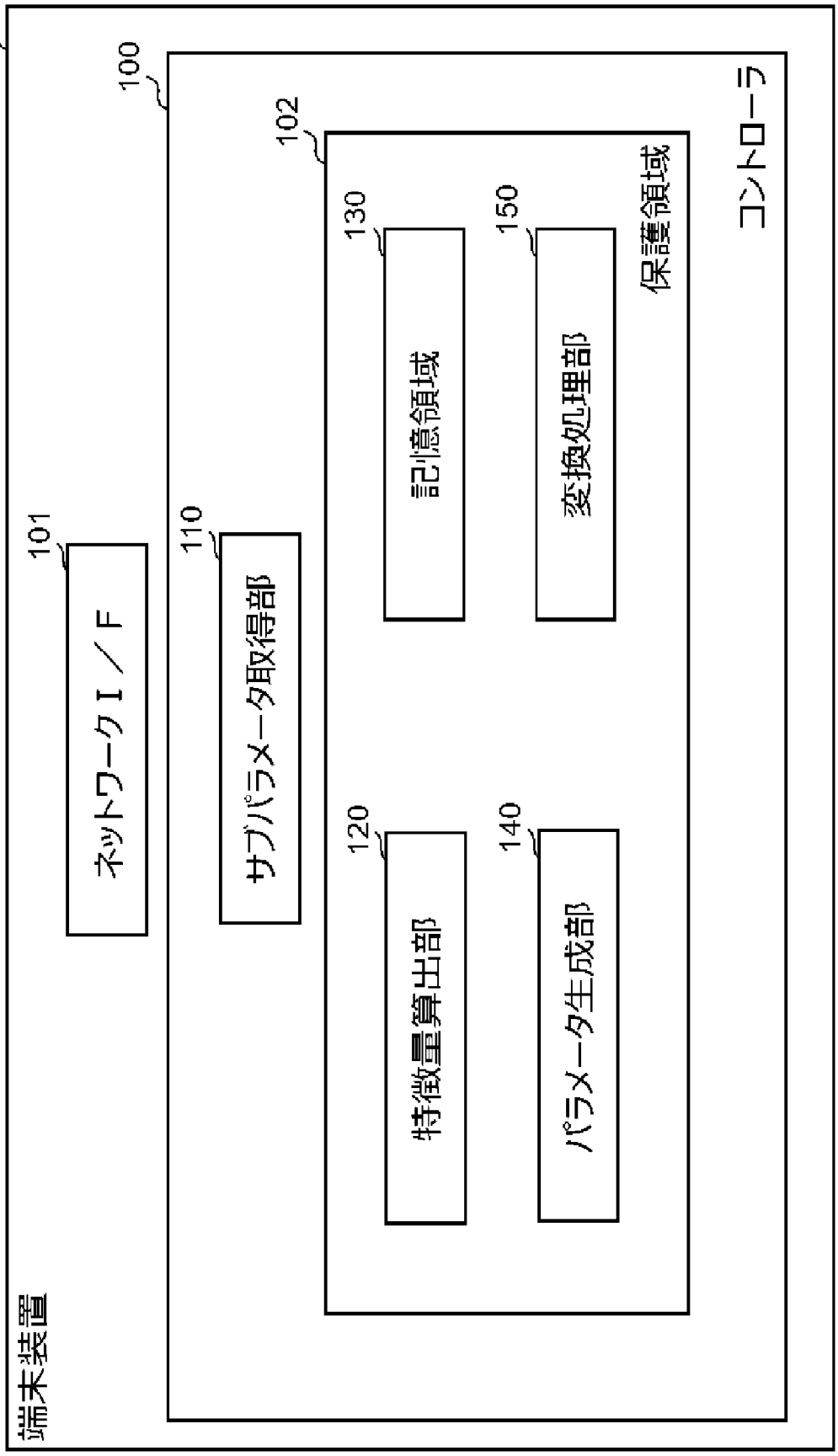

登録時
生体情報
特徴量抽出
x
暗号化
暗号化データ
T
DB
置換鍵K
認証時
生体情報
特徴量抽出
y
暗号化
暗号化データ
T'
照合
一致/不一致

Fig. 3

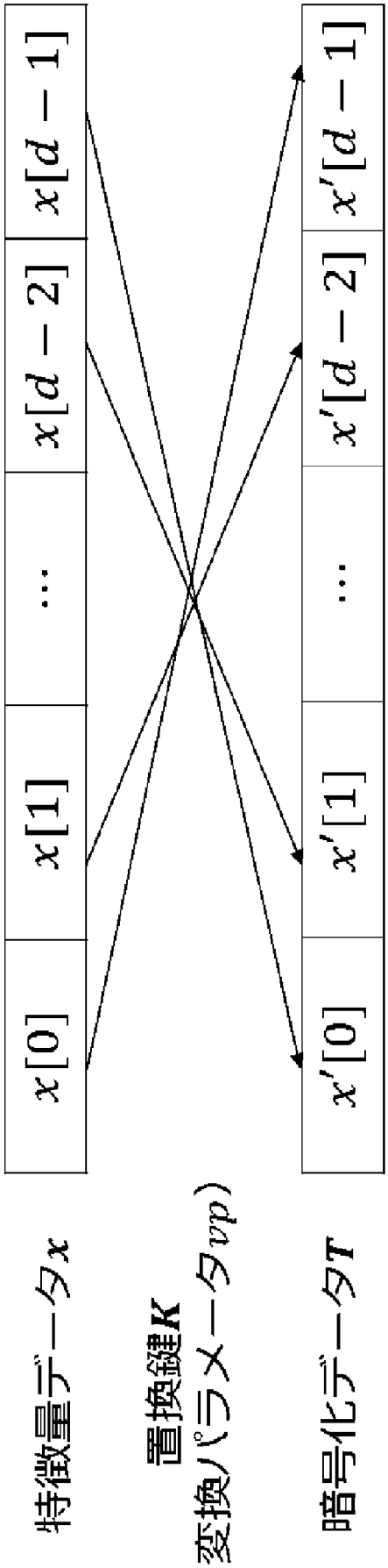
[図4]

Fig. 4


1
端末装置
100
コントローラ
101
ネットワークＩ／Ｆ
110
サブパラメータ取得部
102
保護領域
130
記憶領域
150
変換処理部
120
特徴量算出部
140
パラメータ生成部

[図5]

Fig. 5



[図6]

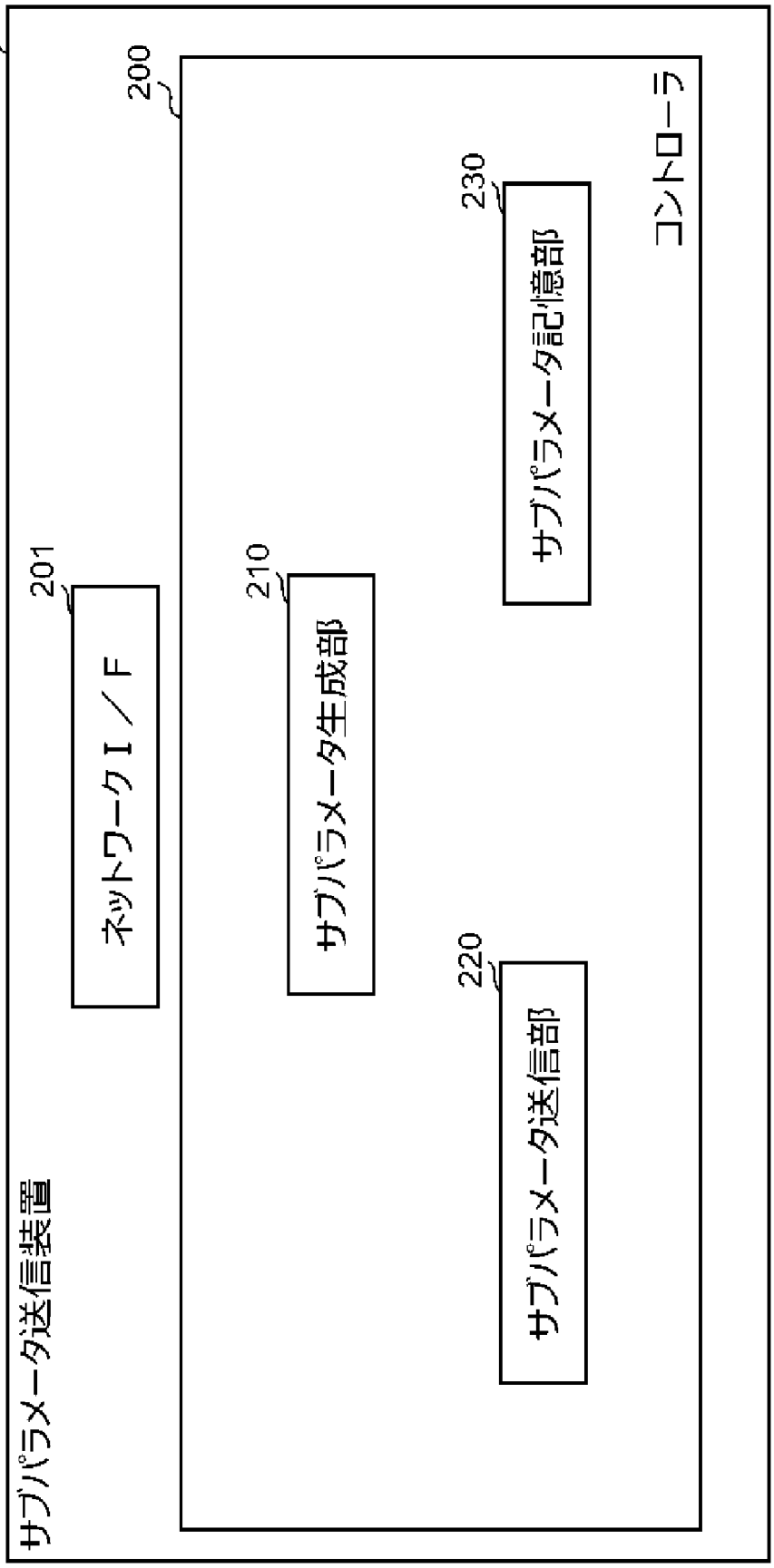
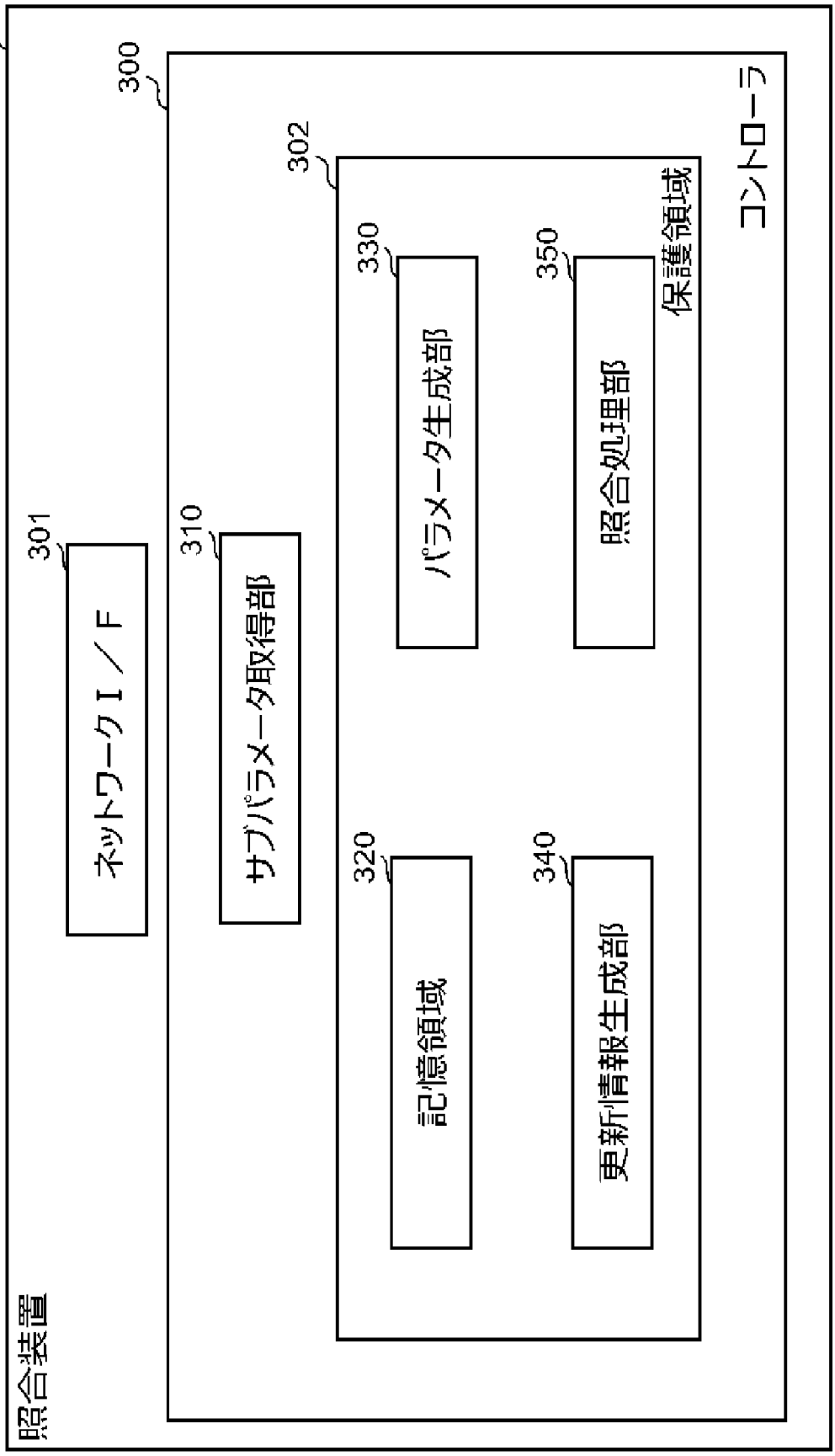

2
サブパラメータ送信装置
200
コントローラ
201
ネットワークＩ／Ｆ
210
サブパラメータ生成部
220
サブパラメータ送信部
230
サブパラメータ記憶部

Fig. 6

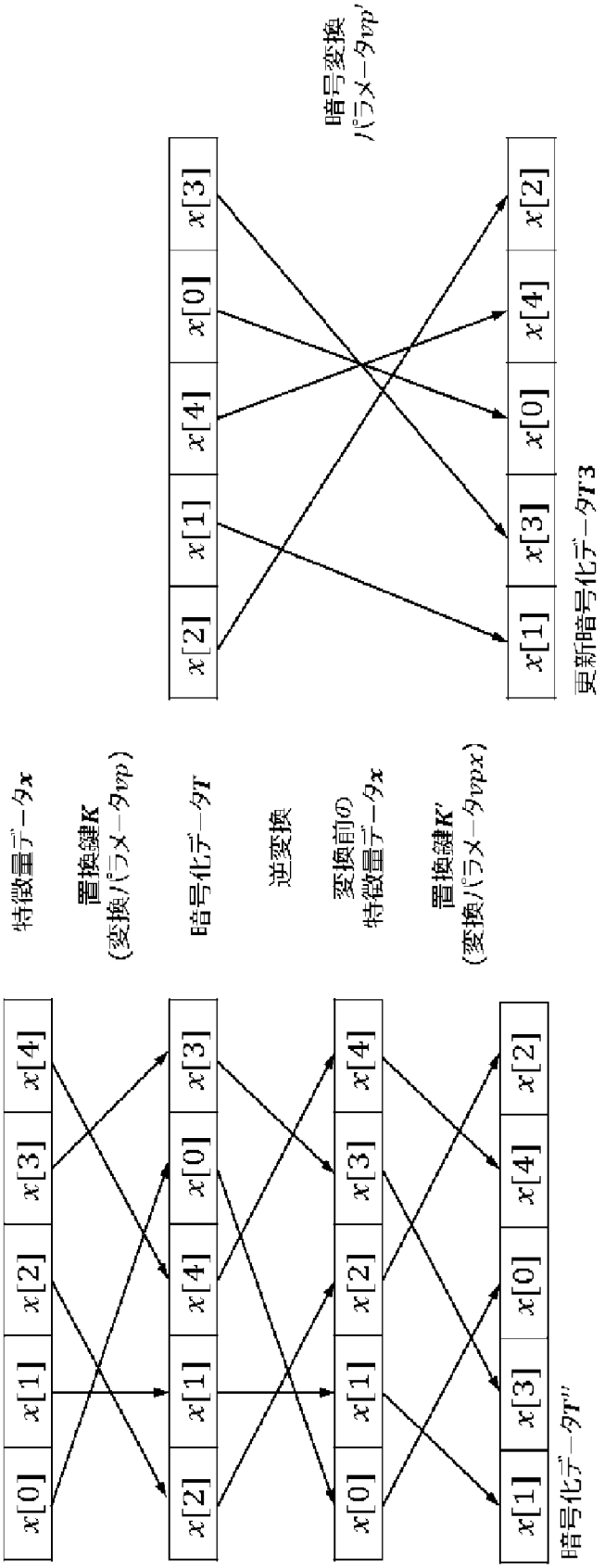
[図7]

Fig. 7


3
照合装置
300
コントローラ
301
ネットワークＩ／Ｆ
310
サブパラメータ取得部
302
保護領域
330
パラメータ生成部
350
照合処理部
320
記憶領域
340
更新情報生成部

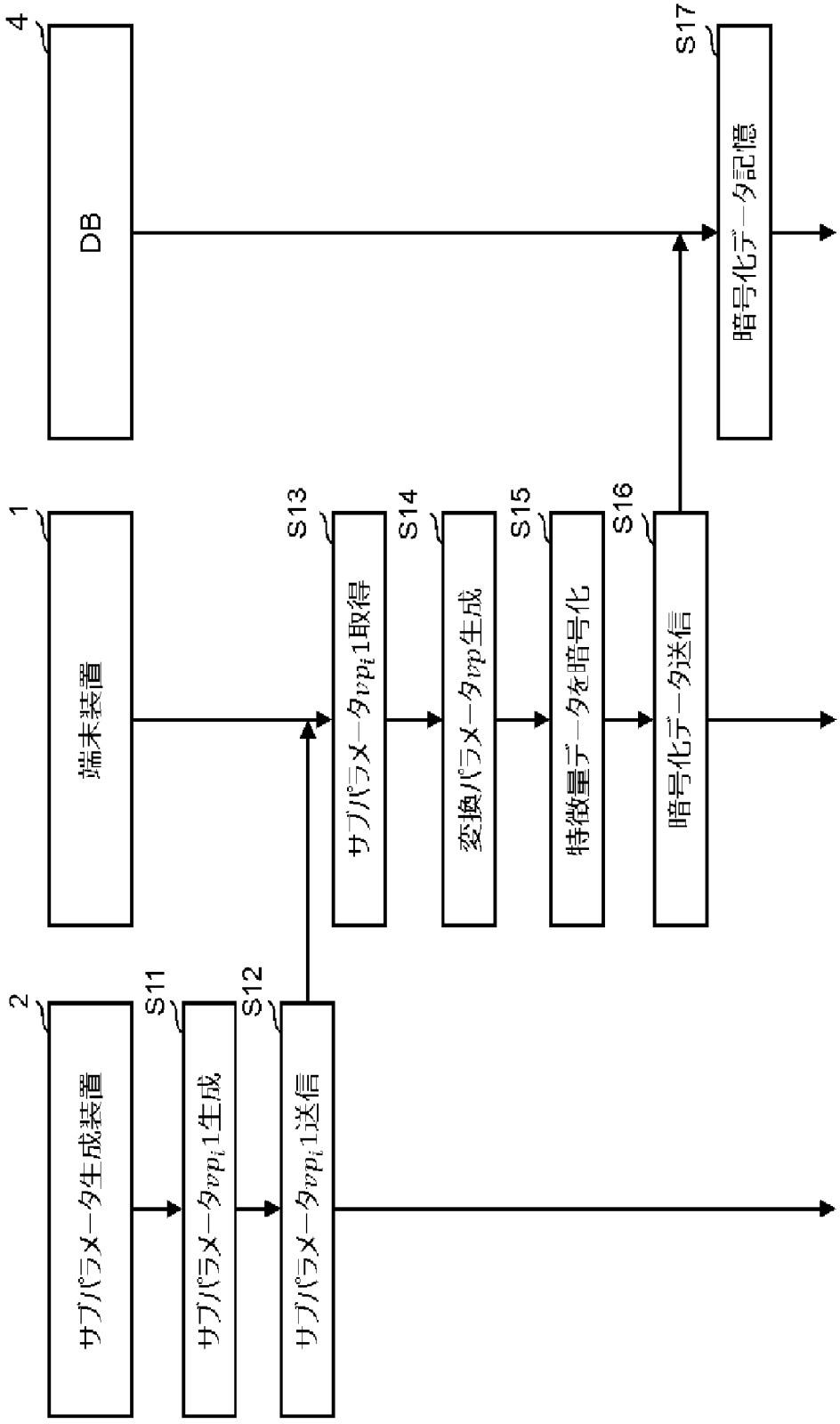
[図8]

Fig. 8


特徴量データx
置換鍵K
(変換パラメータvp)
暗号化データT
逆変換
変換前の
特徴量データx
置換鍵K'
(変換パラメータvpx)
暗号化データT''
暗号変換
パラメータvp'
更新暗号化データ$T3$
x[0] x[1] x[2] x[3] x[4]
x[2] x[1] x[4] x[0] x[3]
x[0] x[1] x[2] x[3] x[4]
x[1] x[3] x[0] x[4] x[2]
x[2] x[1] x[4] x[0] x[3]
x[1] x[3] x[0] x[4] x[2]

[図9]

Fig. 9


4
DB
S17
暗号化データ記憶
1
端末装置
S13
サブパラメータvp_i1取得
S14
変換パラメータvp生成
S15
特徴量データを暗号化
S16
暗号化データ送信
2
サブパラメータ生成装置
S11
サブパラメータvp_i1生成
S12
サブパラメータvp_i1送信

[図10]

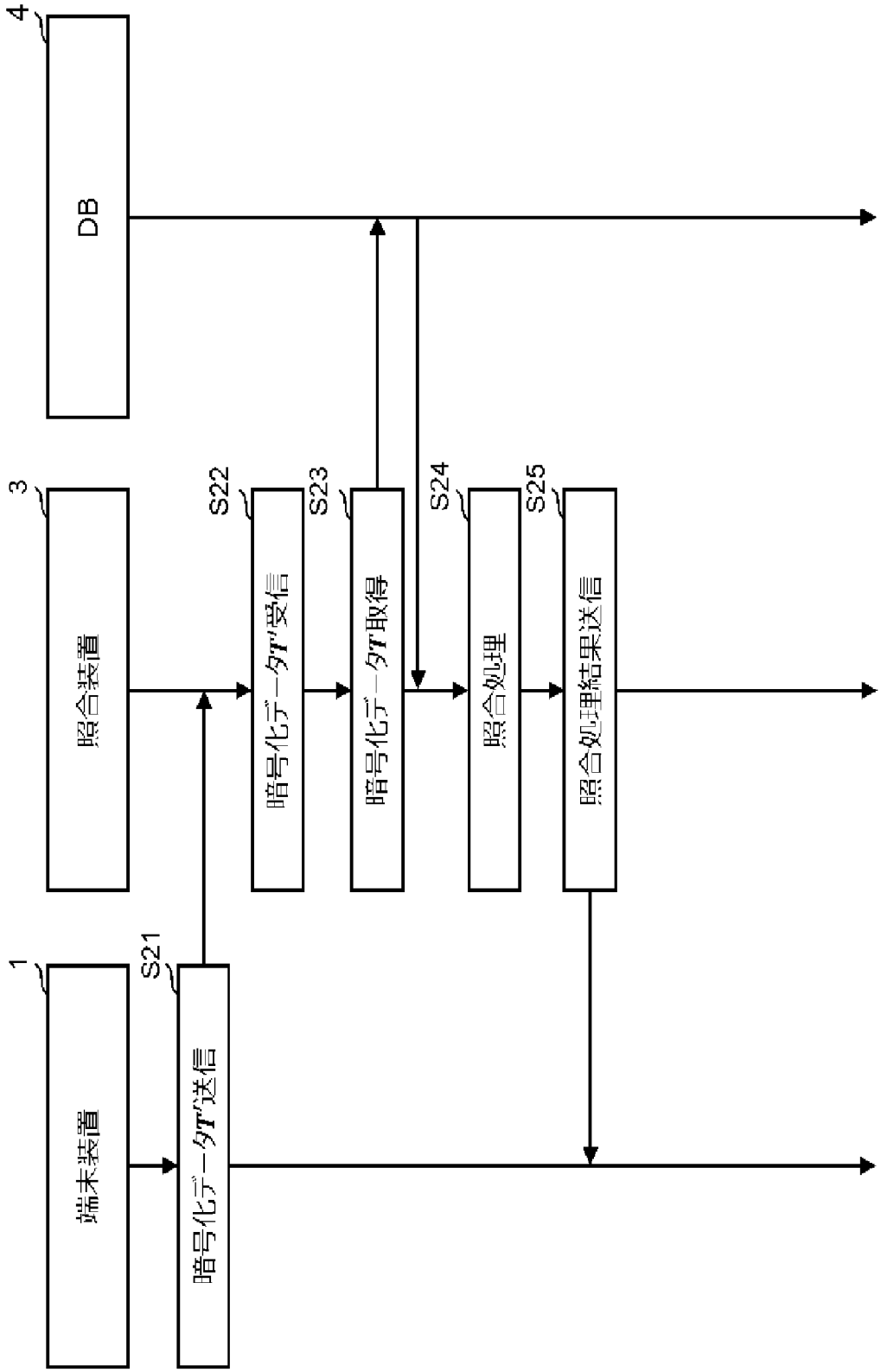
Fig. 10

4

No.	バージョン情報	暗号化データ	識別情報	
1	v1	暗号化データT	EwFsih	…
2	v2	暗号化データTR	u1WLMo	…
…	…	…	…	…

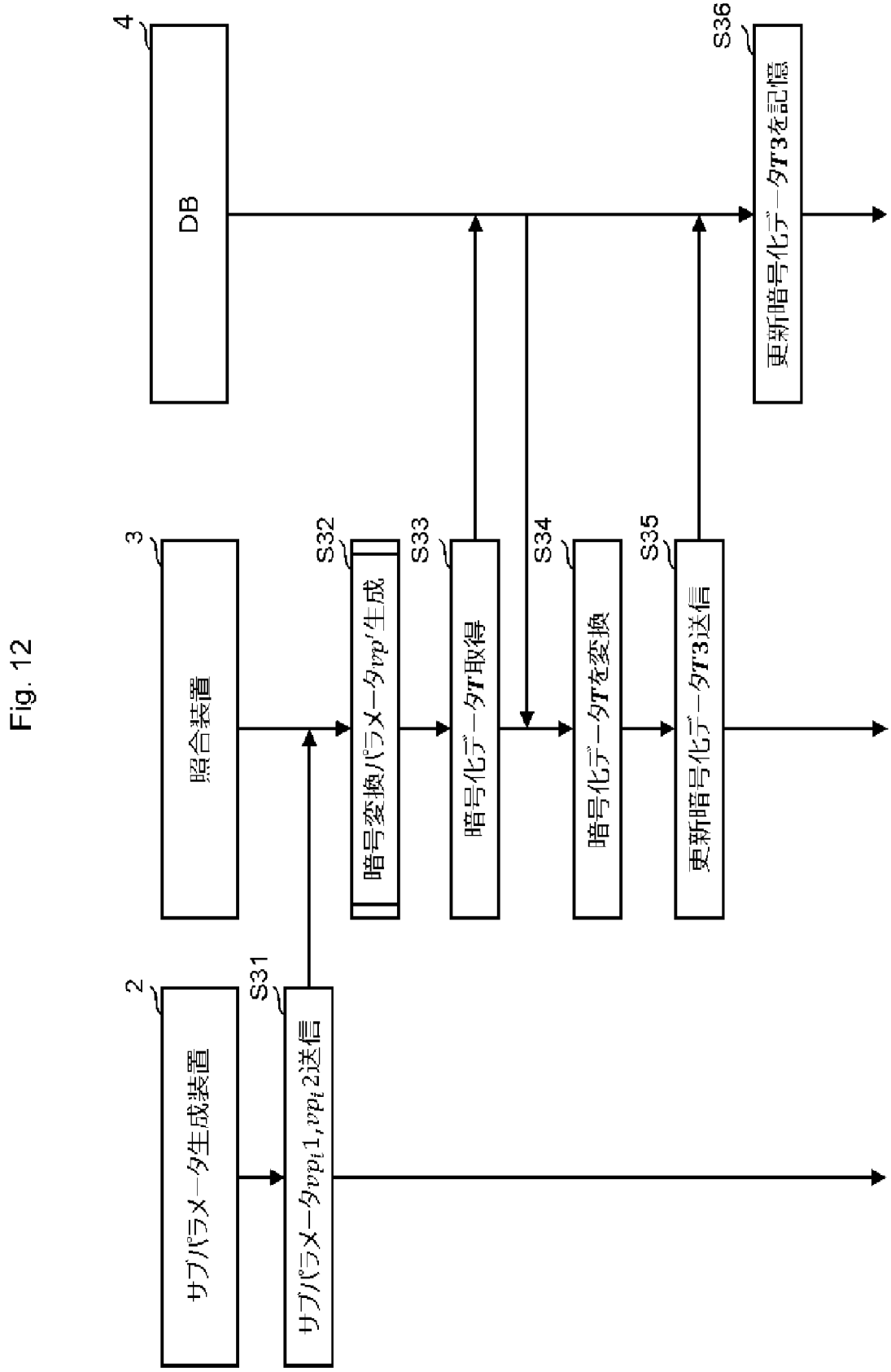
[図11]

Fig. 11


4
DB
3
照合装置
S22
暗号化データ受信
S23
暗号化データ取得
S24
照合処理
S25
照合処理結果送信
1
端末装置
S21
暗号化データ送信

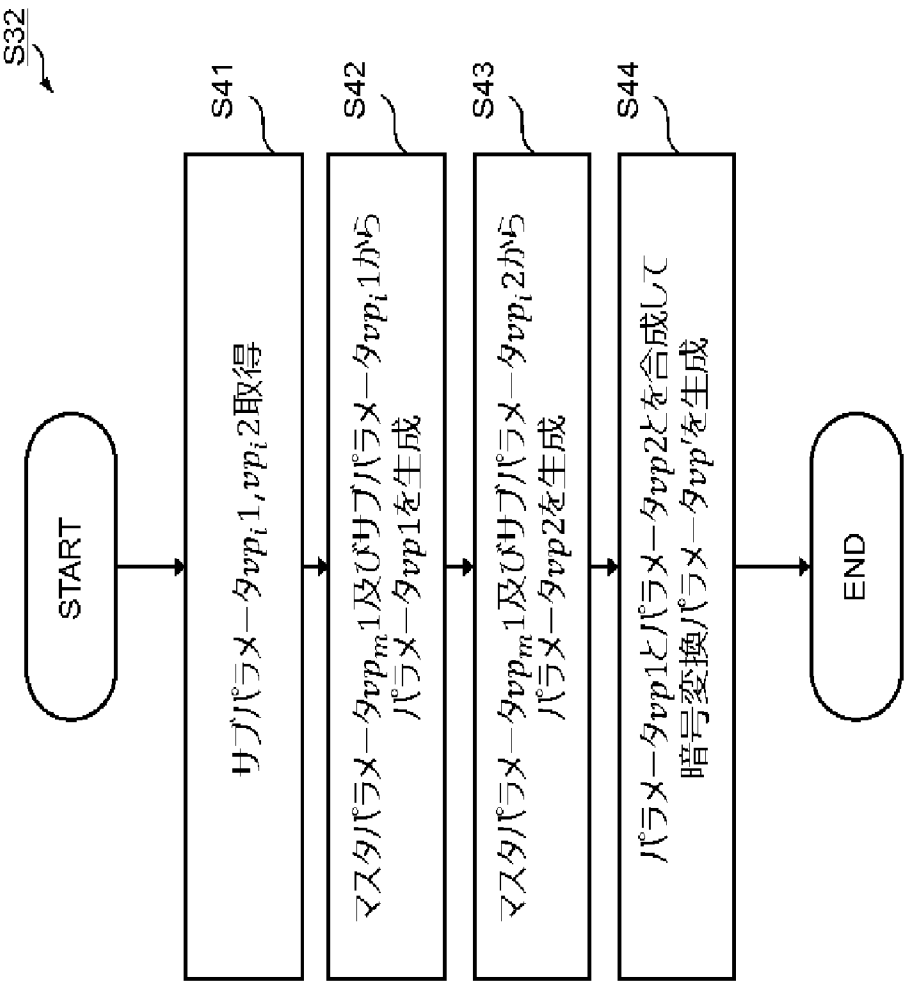
[図12]

Fig. 12


4
DB
S36
更新暗号化データ$DT3$を記憶
3
照合装置
S32
暗号変換パラメータvp'生成
S33
暗号化データDT取得
S34
暗号化データDTを変換
S35
更新暗号化データ$DT3$送信
2
サブパラメータ生成装置
S31
サブパラメータvp_i1, vp_i2送信

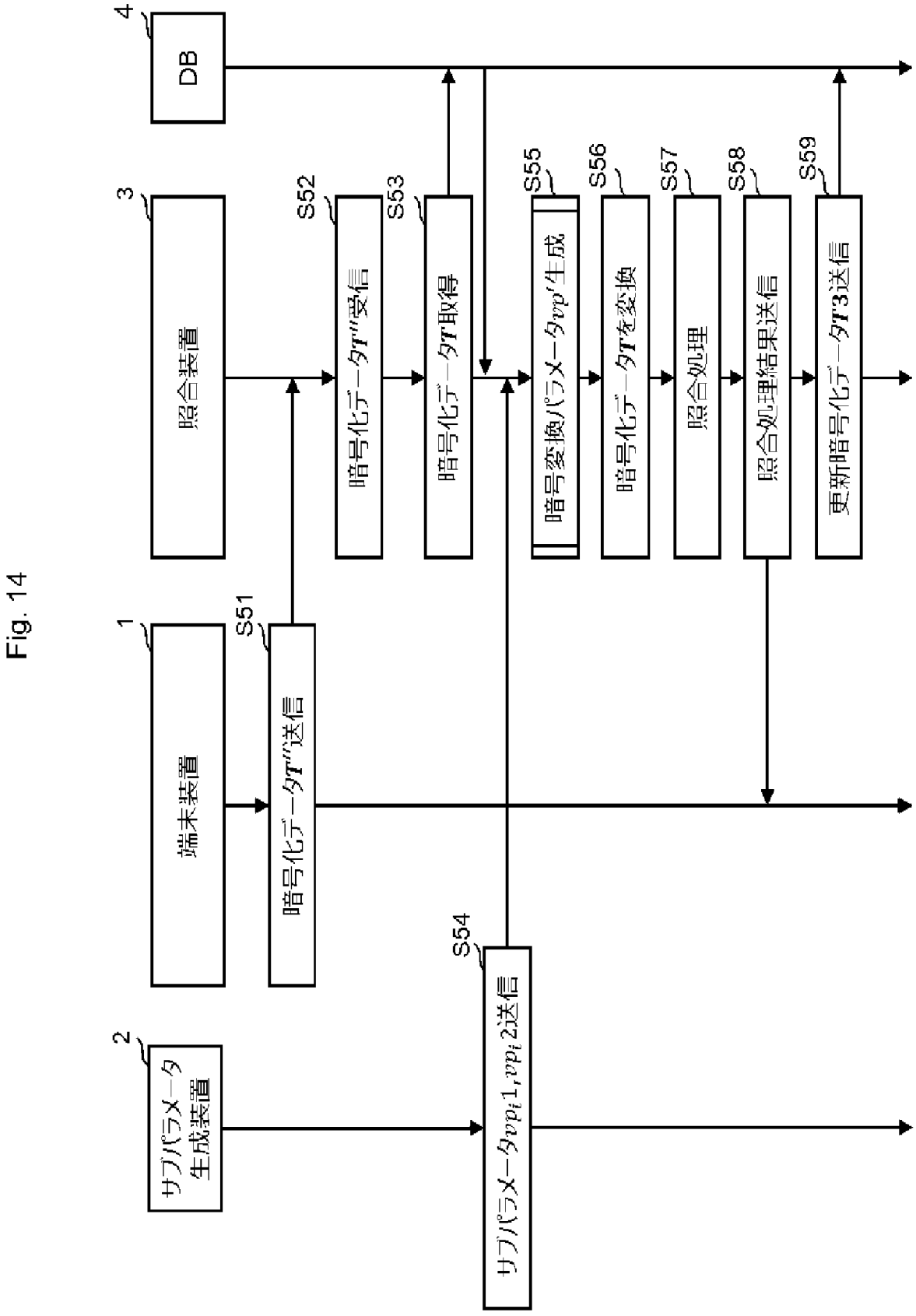
[図13]

Fig. 13


S32
START
S41
サブパラメータvp_i1, vp_i2取得
S42
マスタパラメータvp_m1及びサブパラメータvp_i1から
パラメータ$vp1$を生成
S43
マスタパラメータvp_m1及びサブパラメータvp_i2から
パラメータ$vp2$を生成
S44
パラメータ$vp1$とパラメータ$vp2$とを合成して
暗号変換パラメータvp'を生成
END

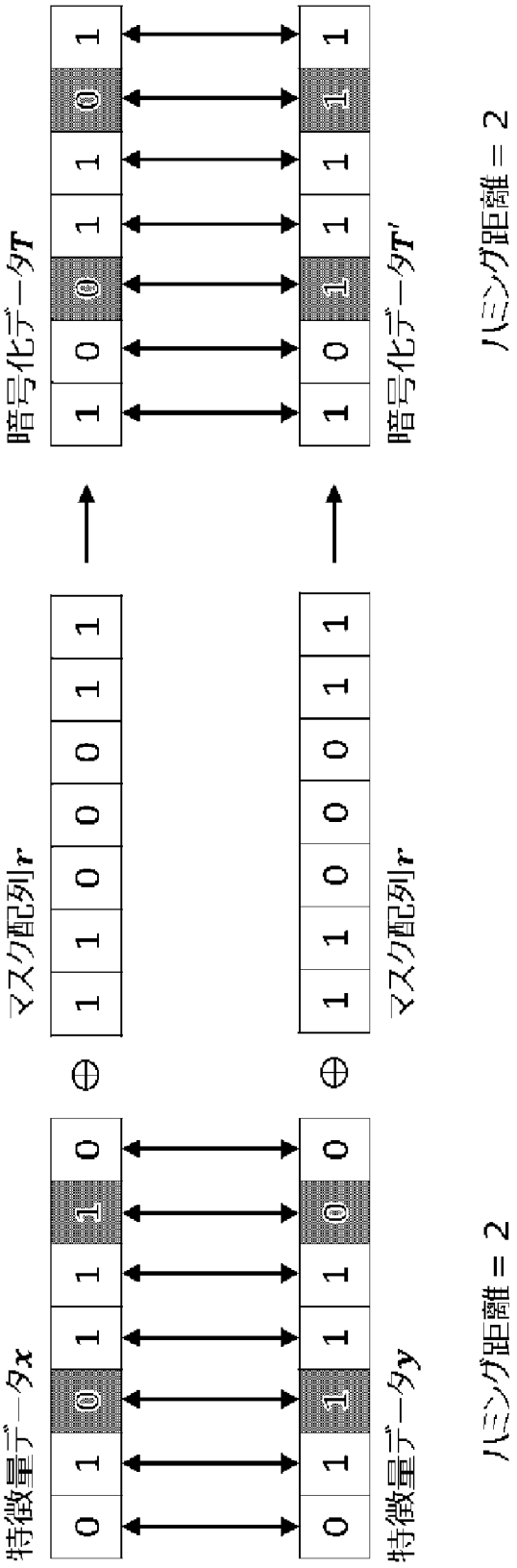
[図14]

Fig. 14


4
DB
3
照合装置
S52
暗号化データ$\mathbf{T}''$受信
S53
暗号化データ$\mathbf{T}$取得
S55
暗号変換パラメータvp'生成
S56
暗号化データ$\mathbf{T}$を変換
S57
照合処理
S58
照合処理結果送信
S59
更新暗号化データ$\mathbf{T}3$送信
1
端末装置
S51
暗号化データ$\mathbf{T}''$送信
2
サブパラメータ生成装置
S54
サブパラメータvp_i1, vp_i2送信

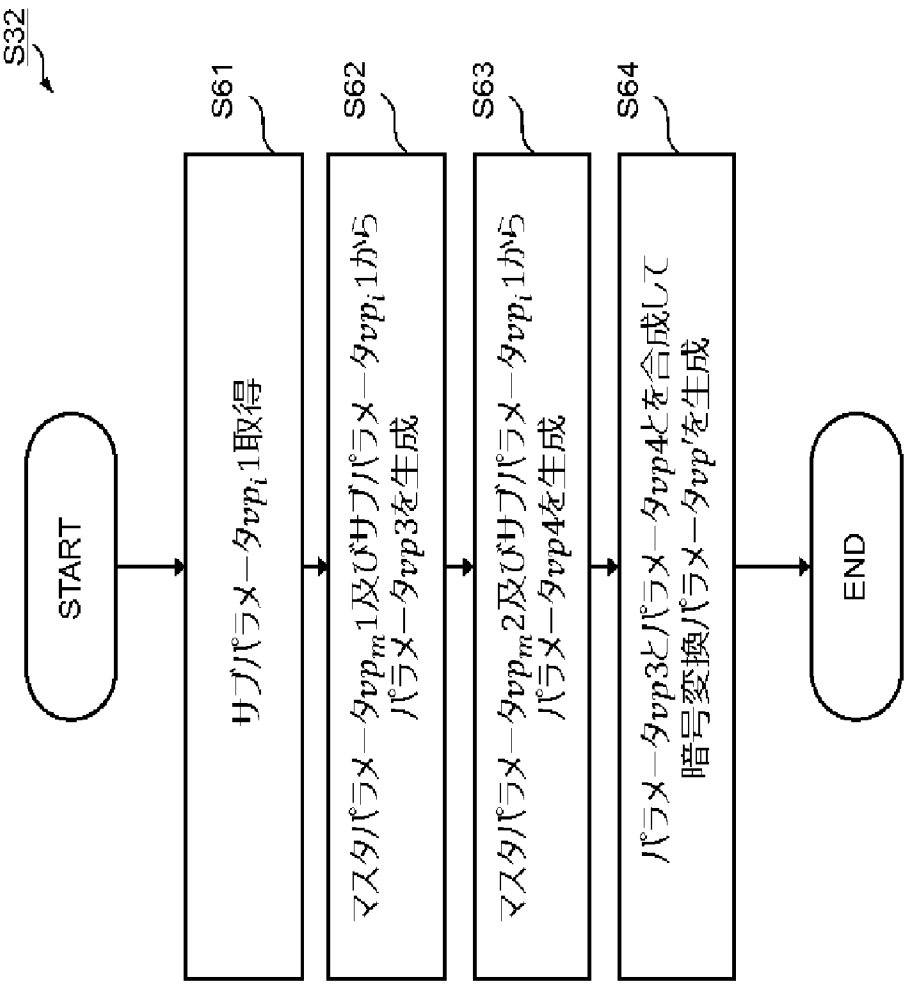
[図15]

Fig. 15


特徴量データx
0 1 0 1 1 1 0 0
⊕
マスク配列r
1 1 0 0 0 1 1 1
暗号化データT
1 0 0 1 1 1 0 1
ハミング距離 = 2
特徴量データy
0 1 1 1 1 1 0 0
⊕
マスク配列r
1 1 0 0 0 1 1 1
暗号化データT'
1 0 1 1 1 1 1 1
ハミング距離 = 2

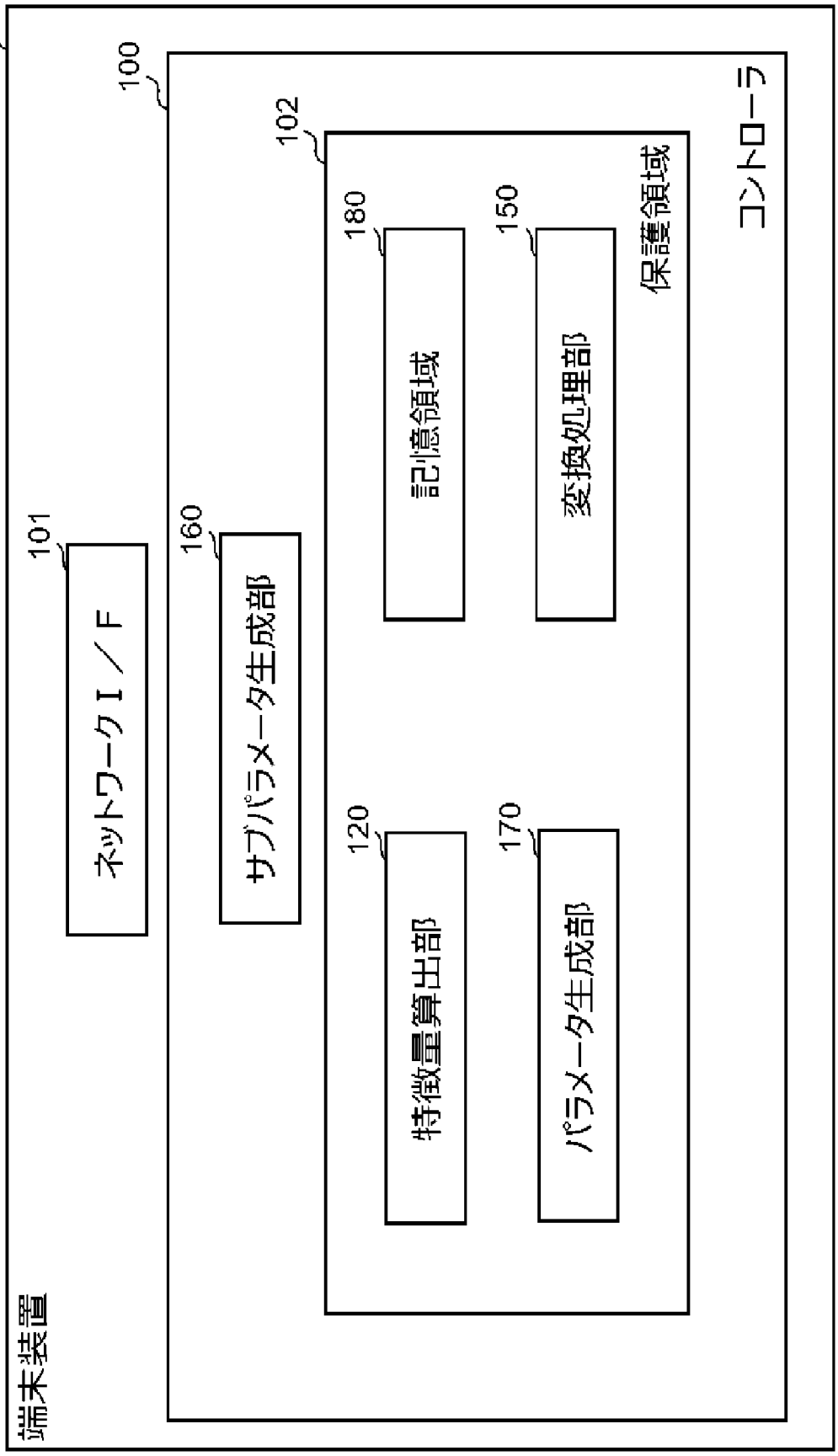
[図16]

Fig. 16


S32
START
S61
サブパラメータvp_i1取得
S62
マスタパラメータvp_m1及びサブパラメータvp_i1から
パラメータ$vp3$を生成
S63
マスタパラメータvp_m2及びサブパラメータvp_i1から
パラメータ$vp4$を生成
S64
パラメータ$vp3$とパラメータ$vp4$を合成して
暗号変換パラメータvp'を生成
END

[図17]

Fig. 17


1
端末装置
100
コントローラ
101
ネットワークＩ／Ｆ
160
サブパラメータ生成部
102
保護領域
180
記憶領域
150
変換処理部
120
特徴量算出部
170
パラメータ生成部

[図18]

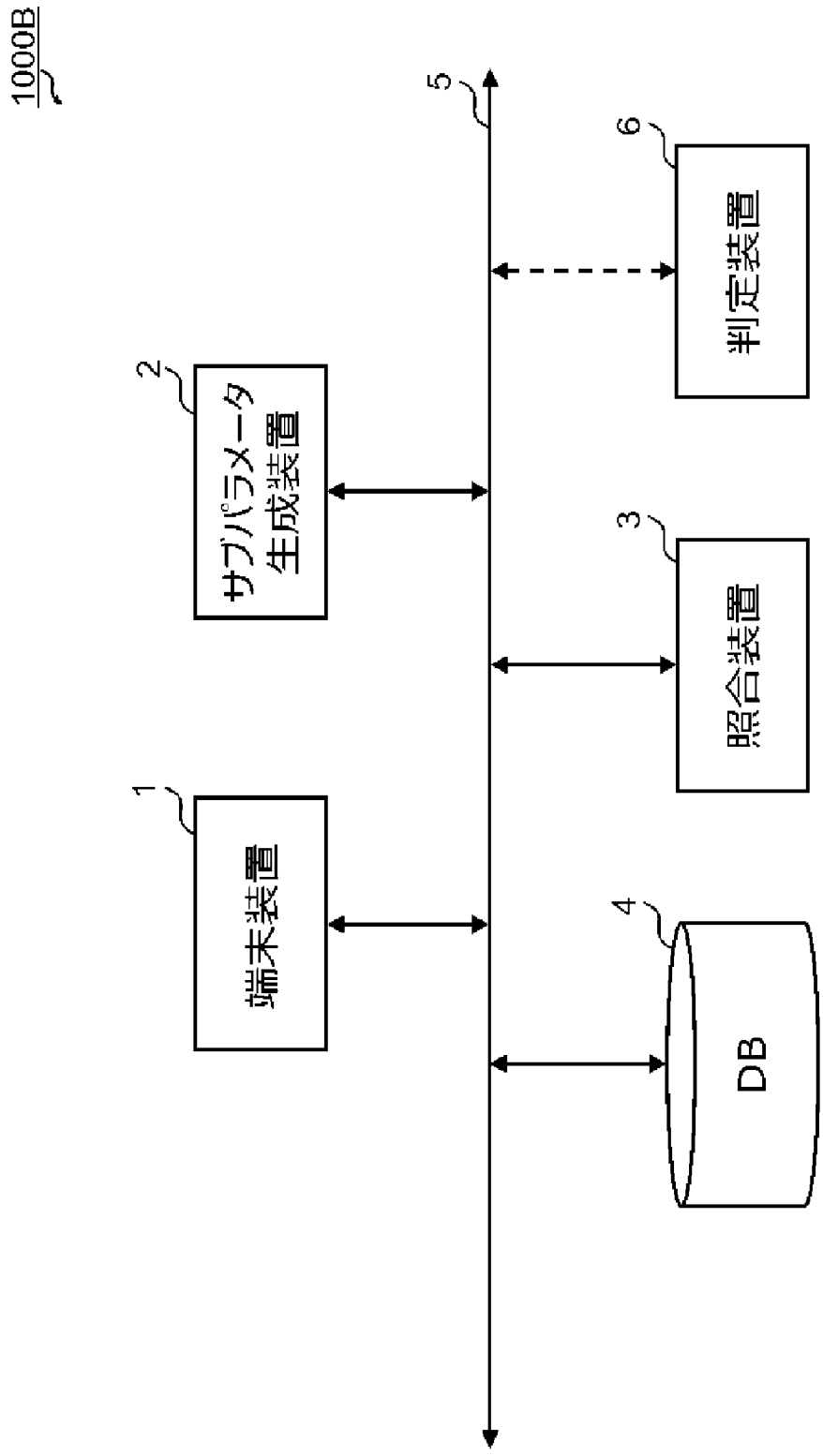
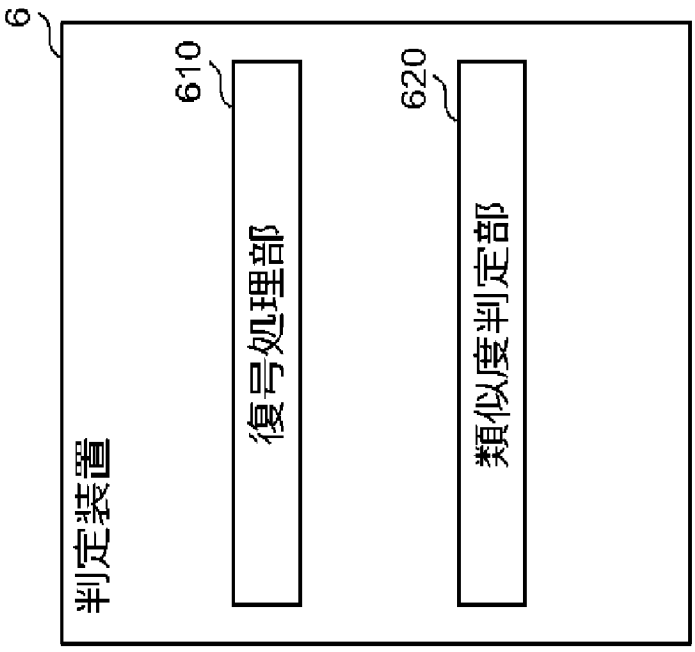


Fig. 18

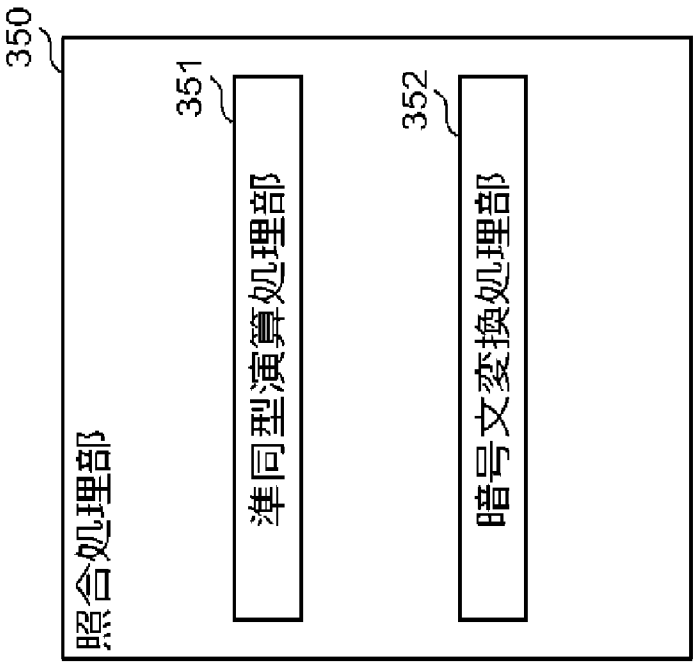
[図19]

Fig. 19



[図20]

Fig. 20



[図21]

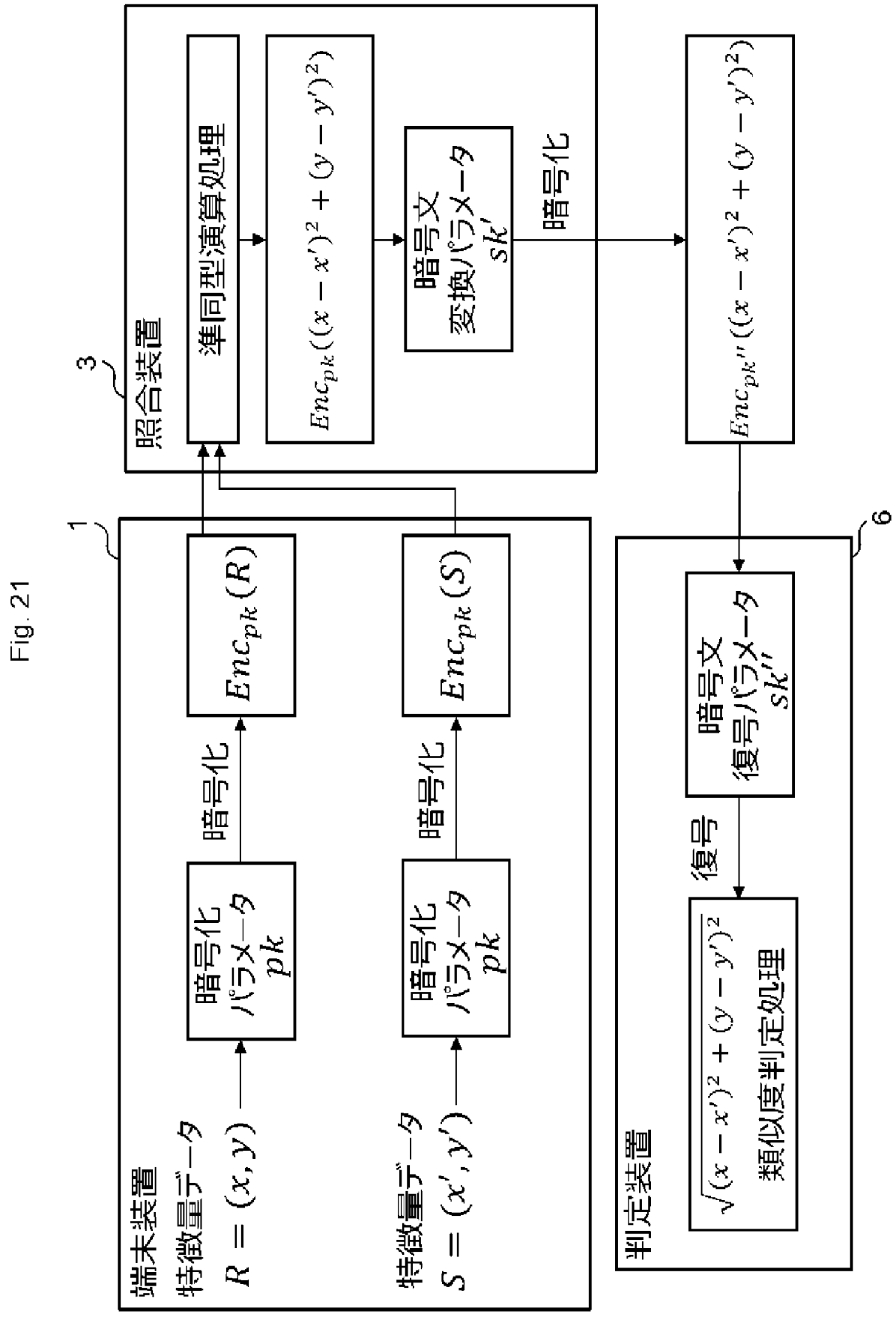

端末装置
特徴量データ
$R = (x, y)$
暗号化パラメータ
pk
暗号化
$Enc_{pk}(R)$
特徴量データ
$S = (x', y')$
暗号化パラメータ
pk
暗号化
$Enc_{pk}(S)$
1
照合装置
準同型演算処理
$Enc_{pk}((x-x')^2 + (y-y')^2)$
暗号文
変換パラメータ
sk'
暗号化
$Enc_{pk''}((x-x')^2 + (y-y')^2)$
3
判定装置
暗号文
復号パラメータ
sk''
復号
$\sqrt{(x-x')^2 + (y-y')^2}$
類似度判定処理
6

Fig. 21

[図22]

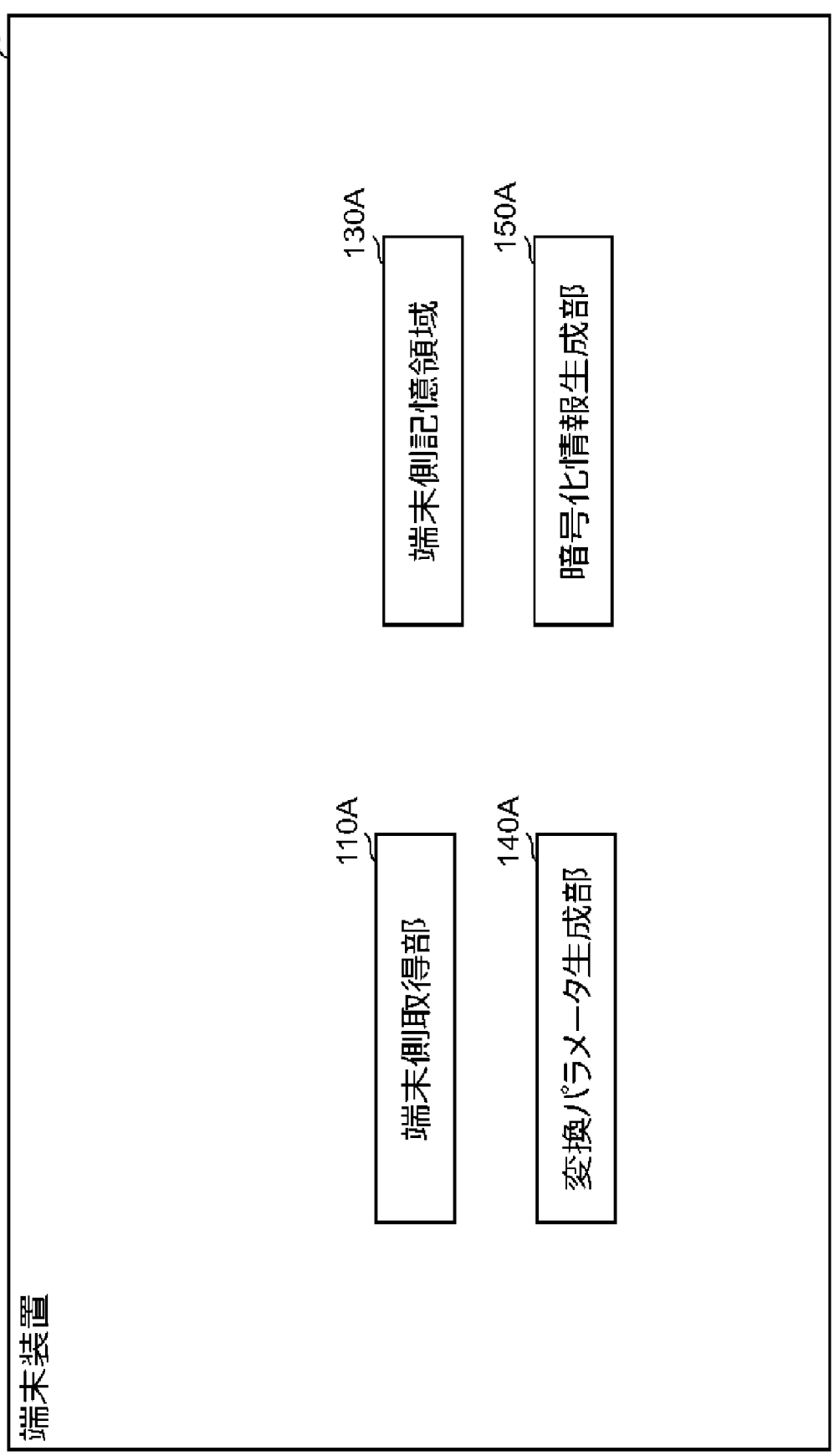

1A
端末装置
110A
端末側取得部
130A
端末側記憶領域
140A
変換パラメータ生成部
150A
暗号化情報生成部

Fig. 22

[図23]

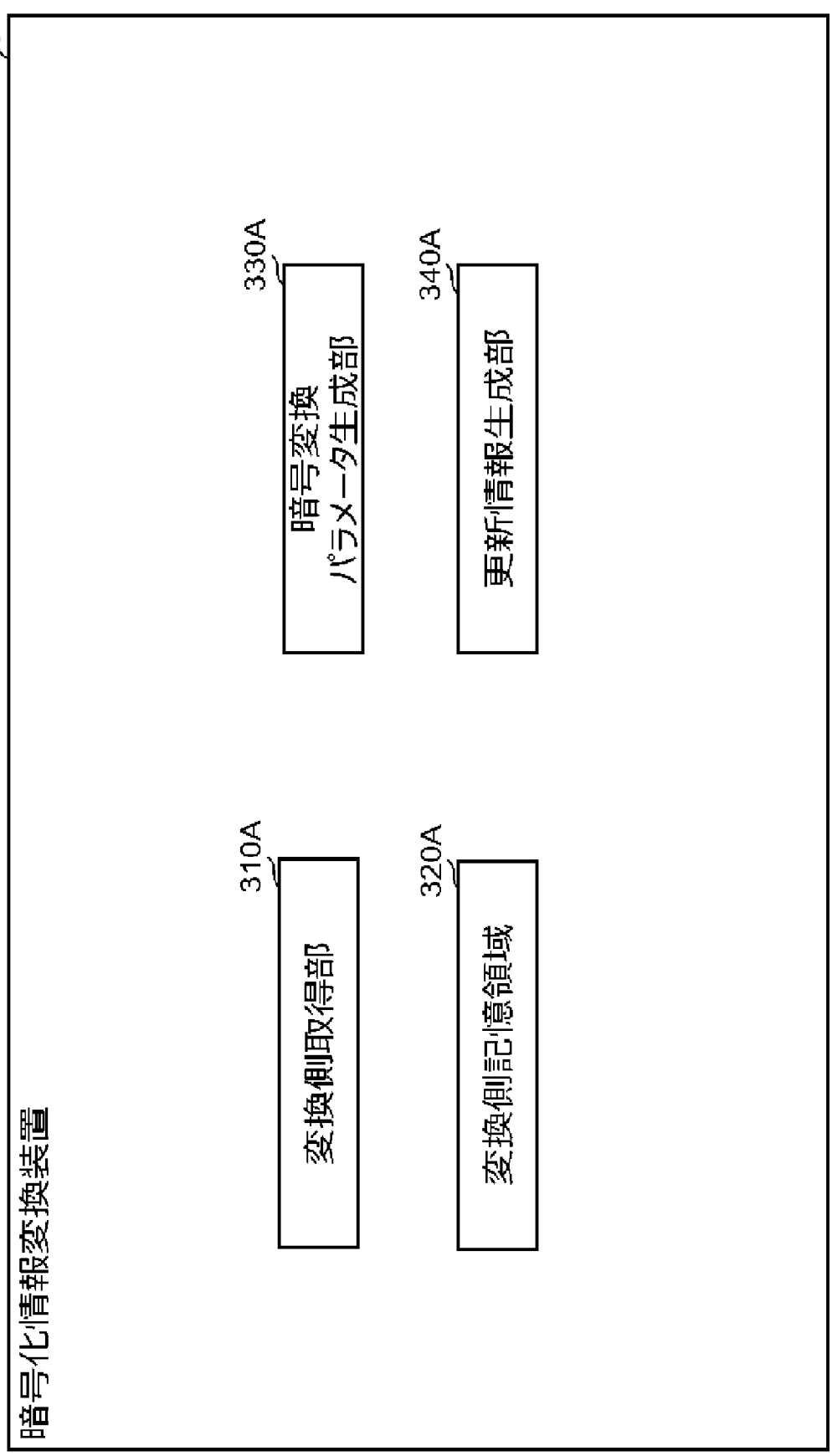

3A
暗号化情報変換装置
310A
変換側取得部
320A
変換側記憶領域
330A
暗号変換
パラメータ生成部
340A
更新情報生成部

Fig. 23

[図24]

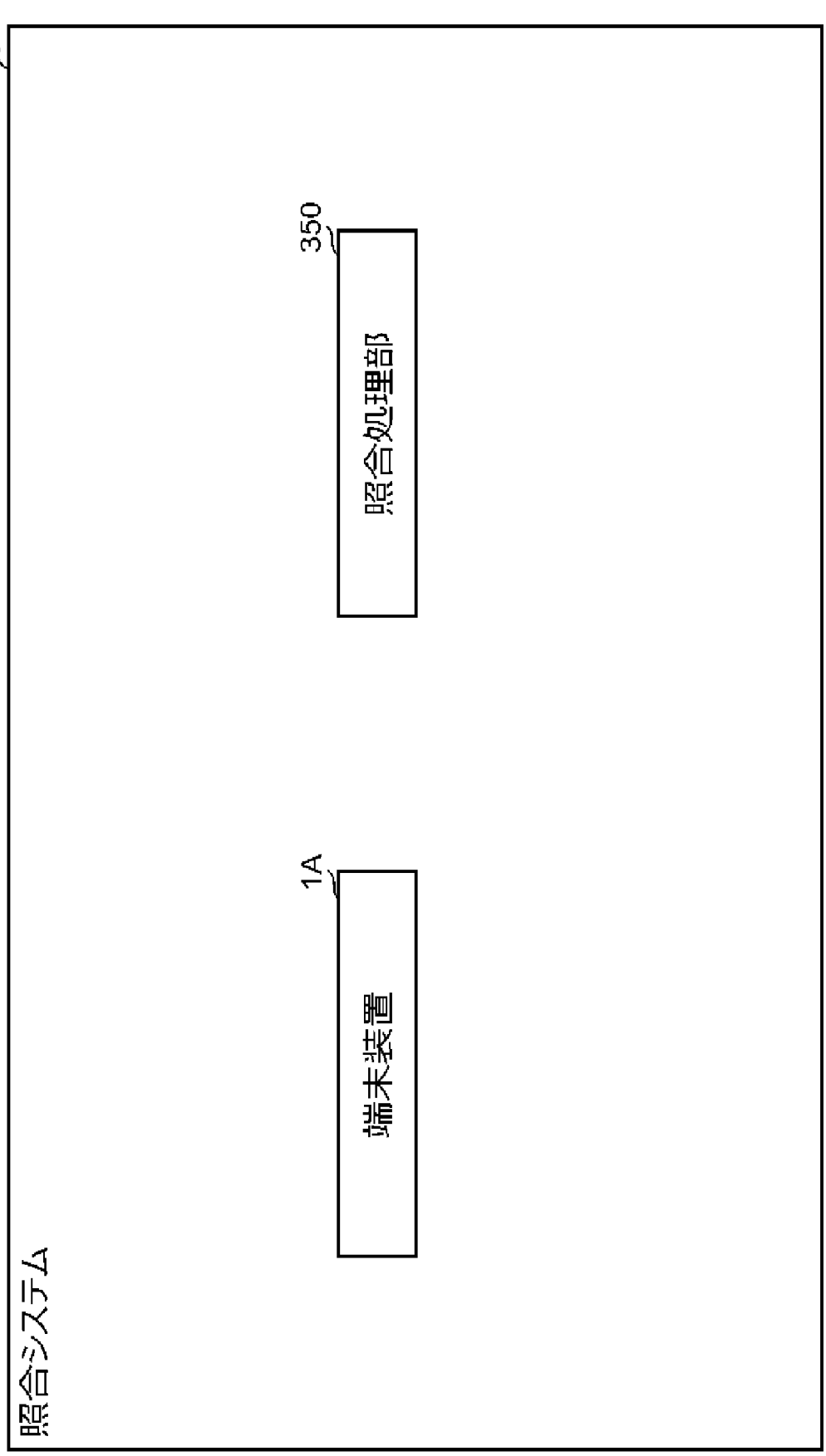


Fig. 24

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/024182

A. CLASSIFICATION OF SUBJECT MATTER
G06F 21/32(2013.01)i
FI: G06F21/32
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)
G06F21/32

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

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2021
Registered utility model specifications of Japan	1996-2021
Published registered utility model applications of Japan	1994-2021

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 Y A	JP 2011-248778 A (MITSUBISHI ELECTRIC CORP) 08 December 2011 (2011-12-08) paragraphs [0059]-[0062], [0064], [0066], [0072]-[0073], [0075]-[0078], [0092], [0094], [0125], [0127], fig. 7	1, 3-4, 36, 41 2, 5-6 7-35, 37-40, 42-43
Y	JP 2006-121215 A (FUJI ELECTRIC HOLDINGS CO LTD) 11 May 2006 (2006-05-11) paragraphs [0029]-[0030], fig. 4	2
Y	JP 2008-046151 A (SHARP CORP) 28 February 2008 (2008-02-28) paragraphs [0003]-[0004], [0013]	5-6
Y	WO 2010/070787 A1 (HITACHI, LTD) 01 July 2010 (2010-07-01) paragraphs [0030], [0037]-[0038], [0041], [0043]-[0044], [0075], [0089], [0093], [0095]-[0098], fig. 2, 8-10	17, 26, 35, 38-40, 43

☒ 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
11 August 2021 (11.08.2021)	24 August 2021 (24.08.2021)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2021/024182

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2010-186075 A (CHUGOKU ELECTRIC POWER CO INC) 26 August 2010 (2010-08-26) paragraph [0025]	17, 26, 35, 38-40, 43
Y	JP 2016-131335 A (FUJITSU LTD) 21 July 2016 (2016-07-21) paragraph [0041], fig. 1	17, 26, 35, 38-40, 43

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2021/024182

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
JP 2011-248778 A	08 Dec. 2011	(Family: none)	
JP 2006-121215 A	11 May 2006	(Family: none)	
JP 2008-046151 A	28 Feb. 2008	(Family: none)	
WO 2010/070787 A1	01 Jul. 2010	EP 2360615 A1 paragraphs [0028], [0035]-[0036], [0039], [0041]-[0042], [0073], [0087], [0091], [0093]-[0096], fig. 2, 8-10 US 2012/0005736 A1 CN 102132288 A	
JP 2010-186075 A	26 Aug. 2010	(Family: none)	
JP 2016-131335 A	21 Jul. 2016	EP 3046286 A1 paragraph [0040], fig. 1 US 2016/0204936 A1	

国際調査報告

国際出願番号
PCT/JP2021/024182

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

G06F 21/32(2013.01)i
FI: G06F21/32

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））

G06F21/32

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	１９７１－２０２１年
日本国実用新案登録公報	１９９６－２０２１年
日本国登録実用新案公報	１９９４－２０２１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	JP 2011-248778 A (三菱電機株式会社) 08.12.2011 (2011-12-08) 段落[0059]-[0062], [0064], [0066], [0072]-[0073], [0075]-[0078], [0092], [0094], [0125], [0127], 図7	1, 3-4, 36, 41
Y		2, 5-6
A		7-35, 37-40, 42-43
Y	JP 2006-121215 A (富士電機ホールディングス株式会社) 11.05.2006 (2006-05-11) 段落[0029]-[0030], 図4	2
Y	JP 2008-046151 A (シャープ株式会社) 28.02.2008 (2008-02-28) 段落[0003]-[0004], [0013]	5-6
Y	WO 2010/070787 A1 (株式会社日立製作所) 01.07.2010 (2010-07-01) 段落[0030], [0037]-[0038], [0041], [0043]-[0044], [0075], [0089], [0093], [0095]-[0098], 図2, 8-10	17, 26, 35, 38-40, 43
Y	JP 2010-186075 A (中国電力株式会社) 26.08.2010 (2010-08-26) 段落[0025]	17, 26, 35, 38-40, 43

☑ 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抵触するものではなく、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
11.08.2021	24.08.2021

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
小林　秀和 5S 3449

電話番号 03-3581-1101 内線 3546

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
Y	JP 2016-131335 A (富士通株式会社) 21.07.2016 (2016-07-21) 段落[0041], 図1	17, 26, 35, 38-40, 43

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2021/024182

引用文献	公表日	パテントファミリー文献	公表日
JP 2011-248778 A	08.12.2011	（ファミリーなし）	
JP 2006-121215 A	11.05.2006	（ファミリーなし）	
JP 2008-046151 A	28.02.2008	（ファミリーなし）	
WO 2010/070787 A1	01.07.2010	EP 2360615 A1 段落[0028], [0035]-[0036], [0039], [0041]-[0042], [0073], [0087], [0091], [0093]-[0096], 図2, 8-10 US 2012/0005736 A1 CN 102132288 A	
JP 2010-186075 A	26.08.2010	（ファミリーなし）	
JP 2016-131335 A	21.07.2016	EP 3046286 A1 段落[0040], 図1 US 2016/0204936 A1	