(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7145706号
(P7145706)

(45)発行日　令和4年10月3日(2022.10.3)

(24)登録日　令和4年9月22日(2022.9.22)

(51)国際特許分類

		FI		
G06F 16/735 (2019.01)		G06F	16/735	
G06F 16/78 (2019.01)		G06F	16/78	
H04L 9/32 (2006.01)		H04L	9/32	200Z

請求項の数　7　（全22頁）

(21)出願番号　特願2018-173262(P2018-173262)
(22)出願日　平成30年9月18日(2018.9.18)
(65)公開番号　特開2020-46795(P2020-46795A)
(43)公開日　令和2年3月26日(2020.3.26)
審査請求日　令和3年9月9日(2021.9.9)

(73)特許権者　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(74)代理人　110001807弁理士法人磯野国際特許商標事務所
(72)発明者　梶田 海成
東京都世田谷区砧一丁目１０番１１号
日本放送協会放送技術研究所内
(72)発明者　大竹 剛
東京都世田谷区砧一丁目１０番１１号
日本放送協会放送技術研究所内
(72)発明者　小川 一人
東京都世田谷区砧一丁目１０番１１号
日本放送協会放送技術研究所内
審査官　齊藤 貴孝

最終頁に続く

(54)【発明の名称】　ユーザ情報管理装置、ユーザ情報登録装置、ユーザ情報取得装置およびそれらのプログラム

(57)【特許請求の範囲】

【請求項１】

属性が予め定めたポリシーを満たす場合のみ検索対象を検索可能な属性ベース検索可能暗号方式で検索対象履歴データを暗号化した暗号化検索対象履歴データとユーザ情報とを対応付けた暗号化データベースを用いて、サービス事業者が提供するサービスと当該サービスを享受するユーザとをマッチングさせるユーザ情報管理装置であって、

ユーザ側のユーザ情報登録装置から、前記ユーザの属性と前記ユーザの履歴データに含まれるキーワードとにより生成された前記属性ベース検索可能暗号方式のユーザ用検索トークンとユーザ情報とを登録要求として受信する登録要求受信手段と、

前記ユーザの属性が前記ポリシーを満たす場合に、前記暗号化データベースにおいて、前記ユーザ用検索トークンに対応する前記暗号化検索対象履歴データを検索し、対応するレコードに、前記ユーザ情報を登録する登録手段と、

サービス事業者側のユーザ情報取得装置から、前記サービス事業者の属性と指定したキーワードとにより生成された前記属性ベース検索可能暗号方式の事業者用検索トークンを検索要求として受信する検索要求受信手段と、

前記サービス事業者の属性が前記ポリシーを満たす場合に、前記暗号化データベースにおいて、前記事業者用検索トークンに対応する前記暗号化検索対象履歴データを検索し、対応するレコードから前記ユーザ情報を読み出す検索手段と、

前記暗号化データベースから読み出した前記ユーザ情報を、前記ユーザ情報取得装置に送信する検索結果送信手段と、

を備えることを特徴とするユーザ情報管理装置。
【請求項２】
前記検索対象履歴データは、放送番組の番組情報であって、前記履歴データは、前記ユーザが視聴した放送番組の番組情報であることを特徴とする請求項１に記載のユーザ情報管理装置。
【請求項３】
請求項１または請求項２に記載のユーザ情報管理装置に、ユーザ情報の登録を要求するユーザ情報登録装置であって、
ユーザの属性と履歴データに含まれるキーワードとを含んだ属性ベース検索可能暗号方式のユーザ用検索トークンを生成する検索トークン生成手段と、
前記ユーザ用検索トークンとユーザ情報とを登録要求として前記ユーザ情報管理装置に送信する登録要求送信手段と、
を備えることを特徴とするユーザ情報登録装置。
【請求項４】
請求項１または請求項２に記載のユーザ情報管理装置から、指定されたキーワードに対応するユーザ情報を取得するユーザ情報取得装置であって、
サービス事業者の属性と前記指定されたキーワードとを含んだ属性ベース検索可能暗号方式の事業者用検索トークンを生成する検索トークン生成手段と、
前記事業者用検索トークンを検索要求として前記ユーザ情報管理装置に送信する検索要求送信手段と、
前記検索要求に対する検索結果として、前記キーワードに対応するユーザ情報を前記ユーザ情報管理装置から受信する検索結果受信手段と、
を備えることを特徴とするユーザ情報取得装置。
【請求項５】
コンピュータを、請求項１または請求項２に記載のユーザ情報管理装置として機能させるためのユーザ情報管理プログラム。
【請求項６】
コンピュータを、請求項３に記載のユーザ情報登録装置として機能させるためのユーザ情報登録プログラム。
【請求項７】
コンピュータを、請求項４に記載のユーザ情報取得装置として機能させるためのユーザ情報取得プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザの個人情報を保護して、サービス事業者が提供するサービスと当該サービスを享受したいユーザとをマッチングさせるユーザ情報管理装置、ユーザ情報登録装置、ユーザ情報取得装置およびそれらのプログラムに関する。
【背景技術】
【０００２】
現在、放送と通信とを融合させた放送通信連携サービスにより、様々な機器（ＩｏＴ〔Internet of Things〕機器等）がテレビと繋がり、新しいサービスを提供することが可能になっている。例えば、２０１３年９月よりＨｙｂｒｉｄｃａｓｔ(登録商標)と呼ばれる放送通信連携サービスが開始されている（非特許文献１参照）。
この放送通信連携サービスの１つとして、例えば、ユーザの視聴した放送番組の視聴履歴に基づいて、サービス事業者が、ユーザの嗜好に合わせたお勧め番組等をレコメンドとして提供するレコメンドサービスがある。
【０００３】
このようなサービスを実用化するための重要な課題の一つが、視聴履歴（履歴データ）等の個人情報の保護である。

個人情報の保護は、ＣＲＹＰＴＲＥＣ（Cryptography Research and Evaluation Committees）が推奨する公開鍵暗号方式のＲＳＡ暗号、共通鍵暗号方式のＡＥＳ等の暗号アルゴリズムを用いて個人情報を暗号化することで実現することができる。

【０００４】

しかし、これらの暗号アルゴリズムを用いた場合、ユーザとサービス事業者とが１対１に対応し、同一システム上において、１つの暗号化鍵に対して暗号文を復号する復号鍵は１つとなる。その場合、サービス事業者は、ユーザごとに異なる鍵を所有しなければならないため、大容量のストレージが必要となる。また、サービス事業者は、ユーザごとに鍵を使い分ける必要があるため、効率が悪いという問題がある。

【０００５】

そこで、近年では、サービス事業者側で鍵を使い分ける必要がなく、視聴者のプライバシを保護したままで、個人情報を利用または活用する暗号方式が種々提案されている。

例えば、データ（個人情報等）を暗号化したままでキーワードによる検索を可能とし、検索結果の正当性を検証することが可能な属性ベース検索可能暗号（ＶＡＢＫＳ：Verifiable Attribute-Based Keyword Search）方式である（非特許文献２参照）。このＶＡＢＫＳ方式は、属性ベース暗号（ＡＢＥ：Attribute-Based Encryption）方式が元となっており（非特許文献３参照）、秘密鍵や暗号文にユーザの属性（居住地、性別、年齢、会員種別等）を関連付け、復号条件（ポリシー）を満たすユーザのみが暗号文を復号することが可能な暗号方式である。

【０００６】

さらに、ＶＡＢＫＳ方式の暗号化処理の一部をクラウドサーバに委託したＶＡＢＫＳ委託方式が提案されている（非特許文献４参照）。

また、検索結果の正当性を検証する機能を有していない属性ベース検索可能暗号（ＡＢＫＳ：Attribute-Based Keyword Search）方式（非特許文献２参照）、ＡＢＫＳ方式の暗号化処理の一部をクラウドサーバに委託したＡＢＫＳ委託方式等も提案されている（非特許文献４参照）。

【先行技術文献】

【非特許文献】

【０００７】

【文献】IPTVFJ STD-0010 STD-0011. http://www.iptvforum.jp/download/.

Q. Zheng, S. Xu, and G. Ateniese, “VABKS: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data”, Proc. of IEEE Infocom’14, pp. 522-530, 2014.

J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption”, Proc. of IEEE S&P, pp. 321-334, 2007.

G. Ohtake, R. Safavi-Naini, and L. F. Zhang, “Outsourcing of veriable attribute-based key-word search”. In Nordic Conference on Secure IT Systems (2017), Springer, pp. 18-35.

【発明の概要】

【発明が解決しようとする課題】

【０００８】

従来提案されているＶＡＢＫＳ方式の暗号方式を用いた手法は、個人情報を暗号化したままでキーワードによる検索を可能とし、そのキーワードに合致したユーザにサービスを提供することができる。

例えば、従来の手法は、あるユーザの個人情報である履歴データ（視聴履歴）を暗号化した状態で取得し、商品名（キーワード）でその商品が登場した番組の視聴の有無を検索することができる。そして、従来手法は、ユーザがその商品が登場した番組を視聴した場合に、ユーザに当該商品に関連するレコメンド情報を提供することができる。

【０００９】

このように、従来の手法では、個人情報を暗号化したままでキーワード検索が可能であ

るが、サービス事業者は、複数のユーザを対象としてサービスを提供するためには、すべてのユーザの履歴データから、当該サービスに関心のあるユーザを特定しなければならず、極めて効率が悪い。

そのため、サービス事業者が提供するサービスと当該サービスを享受したいユーザとを効率よくマッチングさせる手法が望まれていた。

【００１０】

本発明は、このような問題や要望に鑑みてなされたものであり、個人情報である履歴データを保護しつつ、サービス事業者が提供するサービスと当該サービスを享受したいユーザとを効率よくマッチングさせるユーザ情報管理装置、ユーザ情報登録装置、ユーザ情報取得装置およびそれらのプログラムを提供することを課題とする。

【課題を解決するための手段】

【００１１】

前記課題を解決するため、本発明に係るユーザ情報管理装置は、属性が予め定めたポリシーを満たす場合のみ検索対象を検索可能な属性ベース検索可能暗号方式で検索対象履歴データを暗号化した暗号化検索対象履歴データとユーザ情報とを対応付けた暗号化データベースを用いて、サービス事業者が提供するサービスと当該サービスを享受するユーザとをマッチングさせるユーザ情報管理装置であって、登録要求受信手段と、登録手段と、検索要求受信手段と、検索手段と、検索結果送信手段と、を備える構成とした。

【００１２】

かかる構成において、ユーザ情報管理装置は、登録要求受信手段によって、ユーザ側のユーザ情報登録装置から、ユーザの属性とユーザの履歴データに含まれるキーワードとにより生成された属性ベース検索可能暗号方式のユーザ用検索トークンとユーザ情報とを登録要求として受信する。ユーザの属性は、検索条件を示すポリシーに対応したユーザを区分するための個別情報である。また、履歴データは、ユーザの番組の視聴履歴、商品の購入履歴等の番組や商品を示すキーワードであって、番組名、出演者、商品名等である。

そして、ユーザ情報管理装置は、登録手段によって、ユーザの属性がポリシーを満たす場合に、暗号化データベースにおいて、ユーザ用検索トークンに対応する暗号化検索対象履歴データを検索し、対応するレコードに、ユーザ情報を登録する。これによって、ユーザ情報管理装置は、ユーザの履歴データを暗号化したままで検索して、対応する履歴データのレコードにユーザ情報を追加登録することができる。

【００１３】

また、ユーザ情報管理装置は、検索要求受信手段によって、サービス事業者側のユーザ情報取得装置から、サービス事業者の属性と指定したキーワードとにより生成された属性ベース検索可能暗号方式の事業者用検索トークンを検索要求として受信する。サービス事業者の属性は、検索条件を示すポリシーに対応したサービス事業者を区分するための個別情報である。

そして、ユーザ情報管理装置は、検索手段によって、サービス事業者の属性がポリシーを満たす場合に、暗号化データベースにおいて、事業者用検索トークンに対応する暗号化履歴対象データを検索し、対応するレコードからユーザ情報を読み出す。これによって、ユーザ情報管理装置は、ユーザの履歴データを暗号化したままで検索して、対応するユーザ情報を暗号化データベースから読み出すことができる。

【００１４】

そして、ユーザ情報管理装置は、検索結果送信手段によって、暗号化データベースから読み出したユーザ情報を、サービス事業者側のユーザ情報取得装置に送信する。

これによって、ユーザ情報管理装置は、履歴データを保護しつつ、検索の属性を有するサービス事業者にキーワードに対応するユーザ情報を提供することができる。

【００１５】

また、前記課題を解決するため、本発明に係るユーザ情報登録装置は、ユーザ情報管理装置に、ユーザ情報の登録を要求するユーザ情報登録装置であって、検索トークン生成手段と、登録要求送信手段と、を備える構成とした。

【００１６】
かかる構成において、ユーザ情報登録装置は、検索トークン生成手段によって、ユーザの属性と履歴データに含まれるキーワードとを含んだ属性ベース検索可能暗号方式のユーザ用検索トークンを生成する。これによって、ユーザ用検索トークンには、暗号化データベースを検索するための属性とキーワードとが含まれる。
そして、ユーザ情報登録装置は、登録要求送信手段によって、ユーザ用検索トークンとユーザ情報とを登録要求としてユーザ情報管理装置に送信する。
これによって、ユーザ情報登録装置は、暗号化データベースにおいて、履歴データに対応してユーザ情報を登録することができる。
【００１７】
また、前記課題を解決するため、本発明に係るユーザ情報取得装置は、ユーザ情報管理装置から、指定されたキーワードに対応するユーザ情報を取得するユーザ情報取得装置であって、検索トークン生成手段と、検索要求送信手段と、検索結果受信手段と、を備える構成とした。
【００１８】
かかる構成において、ユーザ情報取得装置は、検索トークン生成手段によって、サービス事業者の属性と指定されたキーワードとを含んだ属性ベース検索可能暗号方式の事業者用検索トークンを生成する。これによって、事業者用検索トークンには、暗号化データベースを検索するための属性とキーワードとが含まれる。
そして、ユーザ情報取得装置は、検索要求送信手段によって、事業者用検索トークンを検索要求としてユーザ情報管理装置に送信する。
そして、ユーザ情報取得装置は、検索結果受信手段によって、検索要求に対する検索結果として、キーワードに対応するユーザ情報をユーザ情報管理装置から受信する。
これによって、ユーザ情報取得装置は、履歴データを介して、サービス事業者が提供するサービスに、関心や興味を持つユーザ情報を取得することができる。
【００１９】
なお、ユーザ情報管理装置、ユーザ情報登録装置およびユーザ情報取得装置は、それぞれ、コンピュータを、前記した各手段として機能させるためのプログラムで動作させることができる。
【発明の効果】
【００２０】
本発明は、以下に示す優れた効果を奏するものである。
本発明によれば、サービス事業者が指定する履歴データと合致する履歴を持つユーザを特定することができ、履歴データを介して効率的に、サービス事業者が提供するサービスと当該サービスを享受したいユーザとをマッチングさせることができる。
また、本発明によれば、属性ベース検索可能暗号方式で履歴データを暗号化したまま検索することができるため、個人情報である履歴データを保護することができる。
【図面の簡単な説明】
【００２１】
【図１】本発明の実施形態に係るマッチングシステムの全体構成を示すシステム構成図である。
【図２】図１のマッチングシステムのクラウドサーバを構成するデータ記憶装置およびユーザ情報管理装置の各構成を示すブロック図である。
【図３】暗号化データベースの構造を示すデータ構造図である。
【図４】図１のユーザ情報登録装置の構成を示すブロック図である。
【図５】図１のユーザ情報取得装置の構成を示すブロック図である。
【図６】本発明の実施形態に係るマッチングシステムの視聴履歴によるユーザ情報の登録動作を示すフローチャートである。
【図７】本発明の実施形態に係るマッチングシステムのユーザ情報の取得動作を示すフローチャートである。

【図８】本発明の実施形態に係るマッチングシステムの他の構成を示すシステム構成図である。
【発明を実施するための形態】
【００２２】
以下、本発明の実施形態について図面を参照して説明する。
［マッチングシステムの構成］
まず、図１を参照して、本発明の実施形態に係るマッチングシステムＳの構成について説明する。
【００２３】
マッチングシステムＳは、ユーザの個人情報である履歴データ（ここでは、視聴履歴）を保護して、サービス事業者が提供するサービスとユーザとをマッチングさせるものである。
このマッチングシステムＳは、視聴履歴により、ユーザが視聴した番組に固有のユーザ情報であるユーザＩＤを対応付ける。そして、マッチングシステムＳは、サービス事業者が提供するサービスに関連する番組の視聴ユーザのユーザＩＤをサービス事業者が取得することで、サービスとユーザとをマッチングさせる。
【００２４】
ここでは、マッチングシステムＳは、鍵生成装置１と、暗号化装置２と、データ記憶装置３と、ユーザ情報管理装置４と、ユーザ情報登録装置５と、ユーザ情報取得装置６と、を備える。なお、これらの各装置は、図示を省略したネットワークを介して接続される。また、ここでは、説明を簡略化するため、ユーザ側の装置であるユーザ情報登録装置５、および、サービス事業者側の装置であるユーザ情報取得装置６を、それぞれ１台だけ図示しているが、複数台ネットワークに接続することとしてもよい。
【００２５】
このマッチングシステムＳは、個人情報であるユーザの視聴履歴を保護するための暗号化処理として、データを暗号化したままでキーワードによる検索が可能で検索結果の正当性を検証することが可能な属性ベース検索可能暗号方式（検証可能属性ベース検索可能暗号方式〔ＶＡＢＫＳ方式〕）を用いることとする。
【００２６】
（鍵生成装置）
鍵生成装置１は、ＶＡＢＫＳ方式の暗号化処理に用いる公開鍵および秘密鍵を生成するものである。この鍵生成装置１は、マッチングシステムＳを管理するシステム管理者の装置である。
【００２７】
公開鍵は、暗号化装置２、ユーザ情報管理装置４、ユーザ情報登録装置５およびユーザ情報取得装置６に対して公開される共通の情報である。ここでは、鍵生成装置１は、ネットワークを介して、暗号化装置２、ユーザ情報管理装置４、ユーザ情報登録装置５およびユーザ情報取得装置６に公開鍵を送信する。
秘密鍵は、ユーザ情報登録装置５およびユーザ情報取得装置６に対してそれぞれの秘密情報として送信される個別の情報である。
【００２８】
ここでは、鍵生成装置１は、ユーザ情報登録装置５から通知される属性から公開鍵と秘密鍵とを生成し、ユーザ情報登録装置５に送信する。
ユーザ情報登録装置５から通知される属性は、ユーザを区分するための個別情報であって、例えば、サービスを有料とした場合、料金を支払った会員であるか否かを示す会員種別の情報である。なお、ユーザ情報登録装置５に送信する秘密鍵には、個々のユーザに対応して、検索トークン（ユーザ用検索トークン）を生成するためのトークン生成鍵が含まれる。
【００２９】
また、鍵生成装置１は、ユーザ情報取得装置６から通知される属性から公開鍵と秘密鍵

とを生成し、ユーザ情報取得装置６に送信する。
　ユーザ情報取得装置６から通知される属性は、サービス事業者を区分するための個別情報であって、例えば、認定を受けたサービス事業者であるか否かを示す事業者種別の情報である。なお、ユーザ情報取得装置６に送信する秘密鍵には、個々のサービス事業者に対応して、検索トークン（事業者用検索トークン）を生成するためのトークン生成鍵と、暗号化ユーザＩＤ（暗号化されたユーザ情報）を復号するための復号鍵とが含まれる。
【００３０】
　鍵生成装置１は、マッチングシステムＳを構築する際に、最初に、公開鍵を生成し、ユーザを登録する際に、ユーザごとに秘密鍵を生成し、サービス事業者を登録する際に、サービス事業者ごとに秘密鍵を生成する。
　なお、鍵生成装置１における公開鍵および秘密鍵の生成手法は、従来のＶＡＢＫＳ方式と同じであるため、ここでは説明を省略する。
【００３１】
（暗号化装置）
　暗号化装置２は、ＶＡＢＫＳ方式により、番組データ(放送番組の番組情報）と、当該番組データを検索するためのインデックスとを、ポリシーを用いて暗号化するものである。この暗号化装置２は、放送番組の各種情報を所有する番組データ所有者（例えば、放送局等）の装置である。
【００３２】
　番組データは、過去に放送した番組の情報である。例えば、番組データは、○月○日○時、番組名○○、出演者○○、…といった番組を特定する情報、番組の内容を記載した情報等である。
　インデックスは、番組データを検索するための情報（キーワード）である。例えば、インデックスは、番組データに含まれる番組名、出演者等である。
　なお、番組データおよびインデックスは、検索対象の履歴データ（検索対象履歴データ）となる情報である。
【００３３】
　ポリシーは、暗号化された番組データ（暗号化番組データ）を復号ための条件や、履歴データを検索するための条件を示す情報である。すなわち、ポリシーは、ある属性のユーザおよびサービス事業者に対して復号、検索の許可を与えるか否かを示す情報である。例えば、属性が、料金を支払った会員であるユーザ、または、認定を受けたサービス事業者である場合に、そのユーザまたはサービス事業者に対して復号、検索の許可を示す情報である。
【００３４】
　なお、マッチングシステムＳでは、暗号化装置２が暗号化番組データを生成する際に設定するポリシーと、ユーザ情報登録装置５（ユーザＩＤ暗号化手段５５）が暗号化ユーザＩＤを生成する際に設定するポリシーとの２種類を用いる。
　暗号化装置２が設定するポリシーは、暗号化番組データを復号する必要はないため、検索条件を示すもの（検索ポリシー）とする。ユーザ情報登録装置５（ユーザＩＤ暗号化手段５５）が設定するポリシーは、暗号化ユーザＩＤを検索する必要はないため、復号条件を示すもの（復号ポリシー）とする。
【００３５】
　暗号化装置２は、検索対象履歴データ（番組データ、インデックス）を暗号化して、暗号化検索対象履歴データ（暗号化番組データ、暗号化インデックス）を生成する。
　すなわち、暗号化装置２は、公開鍵とポリシーとにより、番組データを暗号化して、暗号化番組データを生成する。この暗号化番組データにはポリシーが含まれる。
　また、暗号化装置２は、公開鍵とポリシーとにより、インデックスを暗号化して、暗号化インデックスを生成するとともに、検索結果の検証を行うための検証鍵と検証用データとを生成する。この暗号化インデックスにはポリシーが含まれる。
【００３６】

また、暗号化装置２は、暗号化番組データに電子署名を付加し、ユーザ情報取得装置６に、電子署名を検証するための検証鍵を送信する。
なお、暗号化装置２における暗号化手法は、従来のＶＡＢＫＳ方式と同じであるため、ここでは説明を省略する。
この暗号化装置２は、番組ごとに生成した暗号化番組データ、暗号化インデックスおよび検証用データを、ネットワークを介して、クラウドサーバ上のデータ記憶装置３に送信する。

【００３７】

（データ記憶装置およびユーザ情報管理装置）

データ記憶装置３およびユーザ情報管理装置４は、クラウドサーバ上の装置である。なお、ここでは、データ記憶装置３およびユーザ情報管理装置４は、ローカルに接続されているものとする。

【００３８】

データ記憶装置３は、暗号化装置２で生成された番組ごとの暗号化検索対象履歴データ（暗号化番組データ、暗号化インデックス）および検証用データを、暗号化データベースＤＢとして記憶する。暗号化データベースＤＢは、ユーザ情報管理装置４によって、番組データが暗号化されたままで検索される。また、暗号化データベースＤＢは、ユーザ情報管理装置４によって、番組を視聴したユーザを示す暗号化ユーザＩＤ（ユーザ情報）が暗号化検索対象履歴データに対応して記録される。

【００３９】

ユーザ情報管理装置４は、ユーザが視聴した番組をデータ記憶装置３から検索し、対応する暗号化検索対象履歴データに暗号化ユーザＩＤ（ユーザ情報）を登録するとともに、サービス事業者が要求する番組を視聴したユーザの暗号化ユーザＩＤを検索するものである。

【００４０】

ここで、図２を参照して、クラウドサーバ（データ記憶装置３およびユーザ情報管理装置４）の構成について説明する。

（データ記憶装置）

図２に示すように、データ記憶装置３は、データ受信手段３０と、記憶手段３１と、を備える。

【００４１】

データ受信手段３０は、暗号化装置２で生成された暗号化検索対象履歴データ（暗号化番組データ、暗号化インデックス）および検証用データを受信するものである。ここでは、データ受信手段３０は、ネットワークを介して、暗号化検索対象履歴データおよび検証用データを受信し、記憶手段３１に書き込み記憶する。

【００４２】

記憶手段３１は、データ受信手段３０で受信した暗号化検索対象履歴データ（暗号化番組データ、暗号化インデックス）および検証用データを暗号化データベースＤＢとして記憶するものである。

【００４３】

暗号化データベースＤＢは、暗号化装置２で生成された暗号化検索対象履歴データ（暗号化番組データ、暗号化インデックス）および検証用データ、ならびに、番組を視聴したユーザの暗号化ユーザＩＤ（ユーザ情報）を番組ごとに記憶したデータベースである。
暗号化データベースＤＢは、図３に示すように、レコードＲ１，Ｒ２，…Ｒｎ（ｎは１以上の整数）ごとに、番組情報としての暗号化番組データ、暗号化インデックスおよび検証データ、ならびに、ユーザ情報としての暗号化ユーザＩＤが記録される。なお、レコードＲ１，Ｒ２，…Ｒｎは、暗号化ユーザＩＤの登録数に応じた可変長レコードである。
この暗号化データベースＤＢは、ユーザ情報管理装置４の登録手段４３および検索手段４４によって、番組情報が検索され、登録手段４３によって暗号化ユーザＩＤ（ユーザ情報）が登録される。

【００４４】
（ユーザ情報管理装置）
図２に示すように、ユーザ情報管理装置４は、公開鍵受信手段４０と、公開鍵記憶手段４１と、要求受信手段４２と、登録手段４３と、検索手段４４と、検索結果送信手段４５と、を備える。
【００４５】
公開鍵受信手段４０は、鍵生成装置１で生成されたＶＡＢＫＳ方式の公開鍵を受信するものである。ここでは、公開鍵受信手段４０は、ネットワークを介して、公開鍵を受信し、受信した公開鍵を公開鍵記憶手段４１に書き込み記憶する。
【００４６】
公開鍵記憶手段４１は、公開鍵受信手段４０で受信した公開鍵を記憶するものである。この公開鍵記憶手段４１は、半導体メモリ等の一般的な記憶媒体で構成することができる。この公開鍵記憶手段４１に記憶された公開鍵は、登録手段４３および検索手段４４によって読み出される。
【００４７】
要求受信手段４２は、ユーザ情報登録装置５から送信される登録要求、および、ユーザ情報取得装置６から送信される検索要求を、ネットワークを介して受信するものである。
ユーザ情報登録装置５から送信される登録要求には、暗号化データベースＤＢの番組情報を検索するための履歴データ（具体的には、番組データのインデックス）をキーワードとした検索トークン（ユーザ用検索トークン）と、登録用の暗号化ユーザＩＤが含まれている。
ユーザ情報取得装置６から送信される検索要求には、暗号化データベースＤＢの番組情報を検索するための履歴データ（具体的には、番組データのインデックス）をキーワードとした検索トークン（事業者用検索トークン）が含まれている。
【００４８】
ユーザ用検索トークンは、ＶＡＢＫＳ方式において、秘密鍵と、公開鍵と、キーワードと、ユーザの属性とにより生成されるものである。すなわち、ユーザ用検索トークンには、キーワードおよびユーザの属性を示す情報が含まれている。
事業者用検索トークンは、ＶＡＢＫＳ方式において、秘密鍵と、公開鍵と、キーワードと、サービス事業者の属性とにより生成されるものである。すなわち、事業者用検索トークンには、キーワードおよびサービス事業者の属性を示す情報が含まれている。
要求受信手段４２は、ユーザ情報登録装置５から登録要求を受信した場合、当該登録要求に含まれるユーザ用検索トークンおよび暗号化ユーザＩＤを登録手段４３に出力する。
また、要求受信手段４２は、ユーザ情報取得装置６から検索要求を受信した場合、当該検索要求に含まれる事業者用検索トークンを検索手段４４に出力する。
【００４９】
登録手段４３は、ユーザ用検索トークンに対応する番組を暗号化データベースＤＢにおいて検索し、検索したレコードに暗号化ユーザＩＤ（ユーザ情報）を追加登録するものである。ここでは、登録手段４３は、番組検索手段４３０と、ユーザＩＤ追加手段４３１と、を備える。
【００５０】
番組検索手段４３０は、暗号化データベースＤＢにおいてユーザ用検索トークンに対応する番組を検索するものである。
この番組検索手段４３０は、暗号化データベースＤＢの番組（レコード）ごとに、暗号化インデックスに含まれるポリシーと、ユーザ用検索トークンに含まれるユーザの属性とにより、ユーザが検索可能なユーザであるか否かを判定する。
そして、番組検索手段４３０は、ユーザの属性がポリシーを満たすと判定された番組（レコード）について、ユーザ用検索トークン（キーワード）に対応する番組を検索する。なお、番組検索手段４３０は、公開鍵を用いて、ＶＡＢＫＳ方式による検索を行うことで、番組データを暗号化したままで、キーワードによる検索を行うことができる。

この番組検索手段４３０は、検索した番組（レコード）を識別する番号（レコード番号）と暗号化ユーザＩＤとをユーザＩＤ追加手段４３１に出力する。
なお、番組検索手段４３０は、検索結果が複数のレコードである場合、そのすべてのレコード番号をユーザＩＤ追加手段４３１に出力する。

【００５１】

ユーザＩＤ追加手段４３１は、番組検索手段４３０で検索された暗号化データベースＤＢのレコードに、暗号化ユーザＩＤを追加するものである。
これによって、登録手段４３は、暗号化データベースＤＢにおいて、ユーザ用検索トークンに対応する番組を暗号化したままで検索し、暗号化ユーザＩＤを追加することができ、ユーザの視聴履歴を暗号化データベースＤＢに反映することができる。

【００５２】

検索手段４４は、事業者用検索トークンに対応する番組を暗号化データベースＤＢにおいて検索し、検索したレコードに登録されている暗号化ユーザＩＤ（ユーザ情報）を取得するものである。ここでは、検索手段４４は、番組検索手段４４０と、ユーザＩＤ読出手段４４１と、を備える。

【００５３】

番組検索手段４４０は、暗号化データベースＤＢにおいて事業者用検索トークンに対応する番組を検索するものである。
この番組検索手段４４０は、暗号化データベースＤＢの番組（レコード）ごとに、暗号化インデックスに含まれるポリシーと、事業者用検索トークンに含まれるサービス事業者の属性とにより、サービス事業者が検索可能なサービス事業者であるか否かを判定する。
そして、番組検索手段４４０は、サービス事業者の属性がポリシーを満たすと判定された番組（レコード）について、サービス事業者用検索トークン（キーワード）に対応する番組を検索する。なお、番組検索手段４４０は、公開鍵を用いて、ＶＡＢＫＳ方式による検索を行うことで、番組データを暗号化したままで、キーワードによる検索を行うことができる。
この番組検索手段４４０は、検索した番組（レコード）の識別番号（レコード番号）をユーザＩＤ読出手段４４１に出力する。
なお、番組検索手段４４０は、検索結果が複数のレコードである場合、そのすべてのレコード番号をユーザＩＤ読出手段４４１に出力する。

【００５４】

ユーザＩＤ読出手段４４１は、番組検索手段４４０で検索された暗号化データベースＤＢのレコードから、暗号化ユーザＩＤを読み出すものである。
なお、ここでは、ユーザＩＤ読出手段４４１は、暗号化ユーザＩＤ以外にも、暗号化番組データおよび検証用データを暗号化データベースＤＢのレコードから読み出すこととする。暗号化番組データおよび検証用データは、ユーザ情報取得装置６において、検索結果が、事業者用検索トークンに対応するものであることを検証するためのデータである。
ユーザＩＤ読出手段４４１は、読み出した暗号化番組データ、検証用データおよび暗号化ユーザＩＤを、検索結果送信手段４５に出力する。
これによって、検索手段４４は、暗号化データベースＤＢにおいて、事業者用検索トークンに対応する番組を暗号化したままで検索し、暗号化ユーザＩＤを読み出すことができる。

【００５５】

検索結果送信手段４５は、検索手段４４で検索された検索結果である暗号化番組データ、検証用データおよび暗号化ユーザＩＤを、ネットワークを介して、事業者検索トークンを送信したユーザ情報取得装置６に送信するものである。

【００５６】

以上説明したようにデータ記憶装置３およびユーザ情報管理装置４を構成することで、ユーザ情報管理装置４は、ユーザ情報登録装置５からの登録要求によって、データ記憶装置３に記憶されている暗号化データベースＤＢを検索し、番組に対応するレコードにユー

ザの暗号化ユーザＩＤを登録することができる。
　また、ユーザ情報管理装置４は、ユーザ情報取得装置６からの検索要求によって、サービス事業者が指定した番組に対応する暗号化データベースＤＢに登録されている暗号化ユーザＩＤを検索し、ユーザ情報取得装置６に送信することができる。
　このとき、ユーザ情報管理装置４は、ＶＡＢＫＳ方式により、番組データを暗号化したままで検索することができるため、ユーザの個人情報を保護することができる。
　なお、ユーザ情報管理装置４は、コンピュータを前記した各手段として機能させるためのユーザ情報管理プログラムで動作させることができる。
　図１に戻って、マッチングシステムＳの構成について説明を続ける。
【００５７】
（ユーザ情報登録装置）
　ユーザ情報登録装置５は、ユーザが視聴した番組の履歴データから、クラウドサーバ上の暗号化データベースＤＢに、視聴した番組に対応付けてユーザ情報を登録するものである。
　このユーザ情報登録装置５は、ユーザが保持する装置であって、例えば、多機能端末（スマートフォン等）、テレビ受像機等、放送番組の視聴履歴を収集可能な装置である。
　ここで、図４を参照して、ユーザ情報登録装置５の構成について説明する。図４に示すように、ユーザ情報登録装置５は、属性送信手段５０と、鍵情報受信手段５１と、鍵情報記憶手段５２と、視聴履歴記憶手段５３と、検索トークン生成手段５４と、ユーザＩＤ暗号化手段５５と、登録要求送信手段５６と、を備える。
【００５８】
　属性送信手段５０は、ユーザの属性を、ネットワークを介して、鍵生成装置１に送信するものである。この属性送信手段５０は、ユーザの属性（例えば、サービスの料金を支払った会員を示す情報）を鍵生成装置１に送信する。
【００５９】
　鍵情報受信手段５１は、属性送信手段５０で送信された属性に基づいて鍵生成装置１で生成されたＶＡＢＫＳ方式の秘密鍵と公開鍵とを、ネットワークを介して受信するものである。なお、秘密鍵には、検索トークン（ユーザ用検索トークン）を生成するためのトークン生成鍵が含まれている。
　この鍵情報受信手段５１は、受信した秘密鍵と公開鍵とを、鍵情報記憶手段５２に書き込み記憶する。
【００６０】
　鍵情報記憶手段５２は、鍵情報受信手段５１で受信した秘密鍵と公開鍵とを記憶するものである。この鍵情報記憶手段５２は、半導体メモリ等の一般的な記憶媒体で構成することができる。この鍵情報記憶手段５２に記憶された秘密鍵と公開鍵とは、検索トークン生成手段５４と、ユーザＩＤ暗号化手段５５とによって読み出される。
【００６１】
　視聴履歴記憶手段５３は、ユーザが視聴した放送番組の履歴を記憶するものである。この視聴履歴記憶手段５３は、半導体メモリ等の一般的な記憶媒体で構成することができる。この視聴履歴記憶手段５３に記憶する視聴履歴は、図示を省略した放送受信手段が放送番組を受信する際に、電子番組表（ＥＰＧ：Electronic Program Guide）に記載されている番組データを抽出して、視聴履歴記憶手段５３に記憶したものである。
【００６２】
　検索トークン生成手段５４は、視聴履歴の番組データに含まれるキーワードにより、クラウドサーバの暗号化データベースＤＢにおいて、当該番組データのレコードを検索するための検索トークン（ユーザ用検索トークン）を生成するものである。
　なお、検索トークン生成手段５４が用いるキーワードは、番組データを特定するものであって、例えば、番組名である。
　検索トークン生成手段５４は、視聴履歴記憶手段５３に記憶されている視聴履歴（履歴データ）に含まれるキーワードと、鍵情報記憶手段５２に記憶されている公開鍵と、秘密

鍵（トークン生成鍵を含む）とから、ＶＡＢＫＳ方式の検索トークンを生成する。秘密鍵にはユーザの属性を示す情報が含まれる。すなわち、ユーザ用検索トークンは、キーワードおよびユーザの属性を示す情報が含まれた情報である。

この検索トークン生成手段５４は、生成した検索トークン（ユーザ用検索トークン）を、登録要求送信手段５６に出力する。

【００６３】

ユーザＩＤ暗号化手段５５は、ＡＢＥ暗号方式により、予め定めたユーザＩＤ（ユーザ情報）を、ポリシーを用いて暗号化するものである。なお、ユーザＩＤは、マッチングシステムＳで一意に特定できるユーザの識別情報であれば何でもよい。例えば、放送番組の視聴履歴に対応した視聴者を識別するＩＤ等である。なお、ポリシーは、あるサービス事業者に対して、そのサービス事業者の属性に応じて暗号化ユーザＩＤを復号する許可を与えるか否かを示す情報である。

ＡＢＥ暗号方式では、鍵情報記憶手段５２に記憶されている公開鍵を用いて暗号化を行う。ＡＢＥ暗号方式による暗号化は従来手法と同じであるため暗号化の詳細は省略する。

ユーザＩＤ暗号化手段５５は、生成した暗号化ユーザＩＤを登録要求送信手段５６に出力する。

【００６４】

登録要求送信手段５６は、検索トークン生成手段５４で生成されたユーザ用検索トークンと、ユーザＩＤ暗号化手段５５で生成された暗号化ユーザＩＤとを、登録要求として、ユーザ情報管理装置４に送信するものである。

【００６５】

以上説明したようにユーザ情報登録装置５を構成することで、ユーザ情報登録装置５は、ユーザの個人情報である視聴履歴を秘匿したままで、クラウドサーバ上の暗号化データベースＤＢにおいて、視聴した番組に対応するレコードに暗号化ユーザＩＤを登録することができる。

なお、ユーザ情報登録装置５は、コンピュータを前記した各手段として機能させるためのユーザ情報登録プログラムで動作させることができる。

図１に戻って、マッチングシステムＳの構成について説明を続ける。

【００６６】

（ユーザ情報取得装置）

ユーザ情報取得装置６は、サービス事業者が指定した番組の視聴ユーザのユーザ情報をクラウドサーバのユーザ情報管理装置４から取得するものである。

このユーザ情報取得装置６は、サービス事業者が保持する装置であって、パーソナルコンピュータ等の一般的なコンピュータで構成することができる。

ここで、図５を参照して、ユーザ情報取得装置６の構成について説明する。図５に示すように、ユーザ情報取得装置６は、属性送信手段６０と、鍵情報受信手段６１と、鍵情報記憶手段６２と、検索トークン生成手段６３と、検索要求送信手段６４と、検索結果受信手段６５と、検証鍵受信手段６６と、復号手段６７と、を備える。

【００６７】

属性送信手段６０は、サービス事業者の属性を、ネットワークを介して、鍵生成装置１に送信するものである。この属性送信手段６０は、サービス事業者の属性（例えば、認定を受けたサービス事業者であるか否かを示す情報）を鍵生成装置１に送信する。

【００６８】

鍵情報受信手段６１は、属性送信手段６０で送信された属性に基づいて鍵生成装置１で生成されたＶＡＢＫＳ方式の秘密鍵と公開鍵とを、ネットワークを介して受信するものである。なお、秘密鍵には、検索トークン（事業者用検索トークン）を生成するためのトークン生成鍵が含まれている。

この鍵情報受信手段６１は、受信した秘密鍵と公開鍵とを、鍵情報記憶手段６２に書き込み記憶する。

【００６９】

鍵情報記憶手段６２は、鍵情報受信手段６１で受信した秘密鍵と公開鍵とを記憶するものである。この鍵情報記憶手段６２は、半導体メモリ等の一般的な記憶媒体で構成することができる。この鍵情報記憶手段６２に記憶された秘密鍵と公開鍵とは、検索トークン生成手段６３と、復号手段６７とによって読み出される。

【００７０】

検索トークン生成手段６３は、サービス事業者が指定する番組データのキーワードとして、クラウドサーバの暗号化データベースＤＢにおいて、当該番組データのレコードを検索するための検索トークン（事業者用検索トークン）を生成するものである。

なお、サービス事業者が指定する番組データのキーワードには、例えば、サービス事業者が扱う商品が登場する番組名、関連する商品の名称等のサービス事業者が提供するサービスに関連するキーワードを用いる。

【００７１】

検索トークン生成手段６３は、指定されたキーワードと、鍵情報記憶手段６２に記憶されている公開鍵と、秘密鍵（トークン生成鍵を含む）とから、ＶＡＢＫＳ方式の検索トークンを生成する。秘密鍵にはサービス事業者の属性を示す情報が含まれる。すなわち、事業者検索トークンは、キーワードおよびサービス事業者の属性を示す情報が含まれた情報である。

この検索トークン生成手段６３は、生成した検索トークン（事業者用検索トークン）を、検索要求送信手段６４に出力する。

検索要求送信手段６４は、検索トークン生成手段６３で生成された事業者用検索トークンを、検索要求として、ユーザ情報管理装置４に送信するものである。

【００７２】

検索結果受信手段６５は、ユーザ情報管理装置４において、検索トークン（事業者用検索トークン）により検索された検索結果を、ネットワークを介して受信するものである。

この検索結果には、事業者用検索トークンで指定したキーワードに対応する番組の暗号化番組データ、検証用データおよび暗号化ユーザＩＤが含まれる。

この検索結果受信手段６５は、受信した検索結果を、復号手段６７に出力する。

【００７３】

検証鍵受信手段６６は、暗号化装置２から、暗号化番組データに付加されている電子署名を検証するための検証鍵を、ネットワークを介して受信するものである。この検証鍵受信手段６６は、受信した検証鍵を復号手段６７に出力する。

なお、検証鍵受信手段６６は、復号手段６７が検証鍵を参照するタイミングで、暗号化装置２に検証鍵を要求し取得する。

【００７４】

復号手段６７は、検索結果受信手段６５で受信した検索結果に含まれる暗号化ユーザＩＤを復号するものである。ここでは、復号手段６７は、検索結果検証手段６７０と、ユーザＩＤ復号手段６７１と、を備える。

【００７５】

検索結果検証手段６７０は、検索結果に含まれる検証用データに基づいて、検索結果（暗号化番組データ）が、要求した検索トークン（事業者用検索トークン）に対応する検索結果であるか否かを検証するものである。ここでは、検索結果検証手段６７０は、ＶＡＢＫＳ方式の検証を行う。

また、検索結果検証手段６７０は、暗号化番組データに付加されている電子署名を、検証鍵受信手段６６で受信した検証鍵で検証する。なお、署名方式は、暗号化装置２との間で予め共有しておく。

検索結果検証手段６７０は、検証（署名検証を含む）が正しく行われた場合、暗号化ユーザＩＤを、ユーザＩＤ復号手段６７１に出力する。

【００７６】

ユーザＩＤ復号手段６７１は、検索結果検証手段６７０で検証が正しく行われた暗号化ユーザＩＤを復号するものである。このユーザＩＤ復号手段６７１は、ユーザ情報登録装

置５のユーザＩＤ暗号化手段５５（図４参照）で使用した暗号化手法に対応した復号手法によって、暗号化ユーザＩＤを復号する。

【００７７】

すなわち、ユーザＩＤ復号手段６７１における復号手法は、ＡＢＥ暗号方式を用いる。

ユーザＩＤ復号手段６７１は、ユーザ情報登録装置５のユーザＩＤ暗号化手段５５で使用した公開鍵に対応する秘密鍵を、鍵情報記憶手段６２から取得し復号を行う。このとき、ＡＢＥ暗号方式の性質により、復号を行うサービス事業者が、ユーザが暗号化の際に設定したポリシーを満たさなければ復号することができない。また、サービス事業者の属性が、暗号化ユーザＩＤに予め設定されたポリシーを満たすとき、復号されたユーザＩＤを得ることができる。

このユーザＩＤ復号手段６７１は、復号したユーザＩＤを、図示を省略した表示装置、記憶装置等に出力する。

【００７８】

以上説明したようにユーザ情報取得装置６を構成することで、ユーザ情報取得装置６は、サービス事業者が指定したキーワードに対応するユーザ情報を取得することができ、サービス事業者が提供するサービスと、ユーザとをマッチングさせることができる。

なお、ユーザ情報取得装置６は、コンピュータを前記した各手段として機能させるためのユーザ情報取得プログラムで動作させることができる。

【００７９】

［マッチングシステムの動作］

次に、本発明の実施形態に係るマッチングシステムＳの動作について説明する。なお、ここでは、鍵生成装置１は、ＶＡＢＫＳ方式の公開鍵を生成してシステム上に公開しているものとする。また、ユーザ情報登録装置５は、ユーザの属性に応じて、鍵生成装置１から鍵情報（秘密鍵、公開鍵）を取得し、ユーザ情報取得装置６は、サービス事業者の属性に応じて、鍵生成装置１から鍵情報（秘密鍵、公開鍵）を取得しているものとする。さらに、暗号化装置２は、番組データおよびインデックスを、ポリシーを用いで暗号化し、データ記憶装置３は、その暗号化した番組データおよびインデックスと検証用データとを、暗号化データベースＤＢとして記憶しているものとする。

以下、ユーザ情報を番組に対応付けて暗号化データベースＤＢに登録する動作と、キーワードに応じたユーザ情報を暗号化データベースＤＢから取得する動作について説明する。

【００８０】

（視聴履歴によるユーザ情報登録動作）

図６を参照（構成については適宜図１，図２，図４参照）して、マッチングシステムＳにおいて、ユーザ情報登録装置５とユーザ情報管理装置４とにより、視聴履歴に応じてユーザのユーザＩＤを暗号化して暗号化データベースＤＢに登録する動作について説明する。

【００８１】

まず、ユーザ情報登録装置５は、以下のステップＳ１～Ｓ４の動作を行う。

ステップＳ１において、ユーザＩＤ暗号化手段５５は、予め定めたユーザＩＤを、サービス事業者のユーザ情報取得装置６が保持する秘密鍵に対応した、ＡＢＥ暗号方式の公開鍵を用いて暗号化する。

ステップＳ２において、検索トークン生成手段５４は、ユーザの視聴履歴をキーワードとして取得する。ここでは、検索トークン生成手段５４は、視聴履歴記憶手段５３に記憶されている視聴履歴の番組ごとの番組データ（例えば、番組名）をキーワードとして読み込む。

【００８２】

ステップＳ３において、検索トークン生成手段５４は、ステップＳ２で取得したキーワード（番組データ）と、鍵情報記憶手段５２に記憶されている公開鍵と、秘密鍵（トークン生成鍵を含む）とから、ＶＡＢＫＳ方式の検索トークン（ユーザ用検索トークン）を生成する。なお、ＶＡＢＫＳ方式により、ユーザ用検索トークンは、キーワード（番組データ）を暗号化した状態で含んでいる。

【００８３】
ステップＳ４において、登録要求送信手段５６は、ステップＳ３で生成したユーザ用検索トークンと、ステップＳ１で生成した暗号化ユーザＩＤとを、登録要求としてユーザ情報管理装置４に送信する。
なお、ユーザ情報登録装置５は、視聴履歴記憶手段５３に逐次番組データが記憶されるたびに、ステップＳ２～Ｓ４の動作を繰り返す。
以上の動作によって、ユーザ情報登録装置５は、ユーザの視聴履歴に応じて、ユーザＩＤを暗号化した状態で、ユーザ情報管理装置４に送信することができる。
【００８４】
次に、ユーザ情報管理装置４は、以下のステップＳ５～Ｓ９の動作を行う。
ステップＳ５において、要求受信手段４２は、ステップＳ４でユーザ情報登録装置５から送信されたユーザ用検索トークンを受信する。
ステップＳ６において、登録手段４３の番組検索手段４３０は、暗号化データベースＤＢに登録されている番組（レコード）ごとに、ユーザ用検索トークンに含まれるユーザの属性が、暗号化インデックスに含まれる検索ポリシーを満たすか否かを判定する。
ここで、ユーザの属性がポリシーを満たす場合（ステップＳ６でＹｅｓ）、ステップＳ７において、番組検索手段４３０は、ユーザ用検索トークンに含まれるキーワードが、暗号化インデックスに含まれるか否かを判定する。
【００８５】
ここで、キーワードが暗号化インデックスに含まれている場合（ステップＳ７でＹｅｓ）、ステップＳ８において、ユーザＩＤ追加手段４３１は、ステップＳ７でキーワードが含まれると判定された暗号化データベースＤＢのレコードに、ステップＳ５で受信した暗号化ユーザＩＤを追加する。そして、ユーザ情報管理装置４は、ステップＳ９に動作を進める。
また、ステップＳ６において、ユーザの属性がポリシーを満たさなかった場合（ステップＳ６でＮｏ）、ステップＳ７において、キーワードが暗号化インデックスに含まれていない場合（ステップＳ７でＮｏ）も、ユーザ情報管理装置４は、ステップＳ９に動作を進める。
【００８６】
ステップＳ９において、登録手段４３は、暗号化データベースＤＢのすべてのレコードにおいて検索を行ったか否かを判定する。
ここで、まだ、未検索のレコードが存在する場合（ステップＳ９でＮｏ）、ユーザ情報管理装置４は、ステップＳ６に戻って、次の番組（レコード）について、検索を継続する。一方、すべてのレコードにおいて検索を行った場合（ステップＳ９でＹｅｓ）、ユーザ情報管理装置４は、動作を終了する。
以上の動作によって、データ記憶装置３の暗号化データベースＤＢには、ユーザの視聴履歴に応じて、番組ごとに暗号化ユーザＩＤが登録される。
【００８７】
（キーワードによるユーザ情報取得動作）
次に、図７を参照（構成については適宜図１，図２，図５参照）して、マッチングシステムＳにおいて、ユーザ情報取得装置６とユーザ情報管理装置４とにより、サービス事業者が、キーワードにより、番組を視聴したユーザのユーザＩＤ（暗号化ユーザＩＤ）を取得する動作について説明する。
【００８８】
まず、ユーザ情報取得装置６は、以下のステップＳ１０～Ｓ１２の動作を行う。
ステップＳ１０において、検索トークン生成手段６３は、番組名等のキーワードを入力する。
ステップＳ１１において、検索トークン生成手段６３は、ステップＳ１０で取得したキーワードと、鍵情報記憶手段６２に記憶されている公開鍵と、秘密鍵（トークン生成鍵を含む）とから、ＶＡＢＫＳ方式の検索トークン（事業者用検索トークン）を生成する。な

お、ＶＡＢＫＳ方式により、事業者用検索トークンは、キーワードを暗号化した状態で含んでいる。
ステップＳ１２において、検索要求送信手段６４は、ステップＳ１１で生成した事業者用検索トークンを、検索要求としてユーザ情報管理装置４に送信する。
以上の動作によって、ユーザ情報取得装置６は、キーワードを含んだ番組を視聴したユーザのユーザＩＤを、ユーザ情報管理装置４に要求する。
【００８９】
次に、ユーザ情報管理装置４は、以下のステップＳ１３～Ｓ１８の動作を行う。
ステップＳ１３において、要求受信手段４２は、ステップＳ１２でユーザ情報取得装置６から送信された検索要求を受信する。
ステップＳ１４において、検索手段４４の番組検索手段４４０は、暗号化データベースＤＢに登録されている番組（レコード）ごとに、事業者用検索トークンに含まれるサービス事業者の属性が、暗号化インデックスに含まれる検索ポリシーを満たすか否かを判定する。
【００９０】
ここで、サービス事業者の属性がポリシーを満たす場合（ステップＳ１４でＹｅｓ）、ステップＳ１５において、番組検索手段４４０は、サービス事業者用検索トークンに含まれるキーワードが、暗号化インデックスに含まれるか否かを判定する。
ここで、キーワードが暗号化インデックスに含まれている場合（ステップＳ１５でＹｅｓ）、ステップＳ１６において、ユーザＩＤ読出手段４４１は、ステップＳ１５でキーワードが含まれると判定された暗号化データベースＤＢのレコードに登録されている暗号化番組データ、検証用データおよび暗号化ユーザＩＤを読み出す。
【００９１】
ステップＳ１７において、検索結果送信手段４５は、ステップＳ１６で読み出した暗号化番組データ、検証用データおよび暗号化ユーザＩＤを、検索結果としてユーザ情報取得装置６に送信する。そして、ユーザ情報管理装置４は、ステップＳ１８に動作を進める。
なお、ステップＳ１４において、サービス事業者の属性がポリシーを満たさない場合（ステップＳ１４でＮｏ）、ステップＳ１５において、キーワードが暗号化番組データに含まれていない場合（ステップＳ１５でＮｏ）も、ユーザ情報管理装置４は、ステップＳ１８に動作を進める。
【００９２】
ステップＳ１８において、検索手段４４は、暗号化データベースＤＢのすべてのレコードにおいて検索を行ったか否かを判定する。
ここで、まだ、未検索のレコードが存在する場合（ステップＳ１８でＮｏ）、ユーザ情報管理装置４は、ステップＳ１４に戻って、次の番組（レコード）について、検索を継続する。一方、すべてのレコードにおいて検索を行った場合（ステップＳ１８でＹｅｓ）、ユーザ情報管理装置４は、動作を終了する。
以上の動作によって、ユーザ情報管理装置４は、要求のあったキーワードをインデックスとして含む番組を視聴したユーザのユーザＩＤ（暗号化ユーザＩＤ）を、視聴履歴を暗号化したままで検索し、ユーザ情報取得装置６に送信することができる。
【００９３】
次に、ユーザ情報取得装置６は、以下のステップＳ１９～Ｓ２２の動作を行う。
ステップＳ１９において、検索結果受信手段６５は、ステップＳ１７でユーザ情報管理装置４から送信された検索結果（暗号化番組データ、検証データ、暗号化ユーザＩＤ）を受信する。
ステップＳ２０において、検証鍵受信手段６６は、暗号化装置２から、暗号化番組データに付加されている電子署名を検証するための検証鍵を取得する。
ステップＳ２１において、復号手段６７の検索結果検証手段６７０は、ステップＳ１９で受信した暗号化番組データに付加されている電子署名を、ステップＳ２０で取得した検証鍵で検証する。さらに、検索結果検証手段６７０は、ステップＳ１９で受信した検証用

データに基づいて、検証結果である暗号化番組データが、要求した検索トークン（事業者用検索トークン）に対応する検索結果であるか否かについて、ＶＡＢＫＳ方式の検証を行う。

【００９４】

ここで、検証に失敗した場合（ステップＳ２１でＮｏ）、ユーザ情報取得装置６は動作を終了する。

一方、検証に成功した場合（ステップＳ２１でＹｅｓ）、ステップＳ２２において、ユーザＩＤ復号手段６７１は、ステップＳ１９で受信した暗号化ユーザＩＤに含まれるポリシーについて、サービス事業者の属性が満たしているか否かを判定する。属性がポリシーを満たす場合（ステップ２２でＹｅｓ）、ステップＳ２３において、ユーザＩＤ復号手段６７１は、ステップＳ１９で受信した暗号化ユーザＩＤを、ステップＳ１（図６参照）で行った暗号化手法に対応する復号手法（ＡＢＥ暗号方式）で復号する。

ここで、サービス事業者の属性が、暗号化ユーザＩＤに含まれるユーザのポリシーを満たしていない場合（ステップＳ２２でＮｏ）、他に受信した暗号化ユーザＩＤがあれば、再度ステップＳ２２の処理を行う。一方、他に受信した暗号化ユーザＩＤがなければ、ユーザ情報取得装置６は動作を終了する。

以上の動作によって、ユーザ情報取得装置６は、ユーザの視聴履歴を保護した状態で、キーワードで指定した番組を視聴したユーザのユーザＩＤを取得することができ、サービス事業者が提供するサービスにマッチングしたユーザを特定することが可能になる。

【００９５】

以上、本発明の実施形態に係るマッチングシステムＳの構成および動作について説明したが、本発明は、この実施形態に限定されるものではない。

【００９６】

ここでは、マッチングシステムＳは、暗号化装置２における暗号化処理として、データを暗号化したままでキーワードによる検索が可能で検索結果の正当性を検証することが可能な検証可能属性ベース検索可能暗号方式（ＶＡＢＫＳ方式）を用いることとした。

しかし、この暗号化処理には、非特許文献３に記載されているような、暗号化処理の一部をクラウド上に委託する検証可能属性ベース検索可能暗号方式（ＶＡＢＫＳ委託方式）を用いてもよい。例えば、図８に示すように、マッチングシステムＳＢを構成する。

【００９７】

すなわち、図１で説明したマッチングシステムＳの暗号化装置２を、図８に示す部分暗号化装置２Ａと、委託暗号化装置２Ｂとで構成する。その場合、部分暗号化装置２Ａは、番組データおよびインデックスの暗号化処理を中間段階まで行い、部分暗号化番組データ、部分暗号化インデックスおよび検証用データを委託暗号化装置２Ｂに送信し、委託暗号化装置２Ｂが、最終段階まで暗号化処置を行う。

このように、部分暗号化装置２Ａを番組データ所有者の装置とし、委託暗号化装置２Ｂをクラウドサーバの装置とすることで、暗号化処理の一部をクラウドに委託することができる。

【００９８】

また、ここでは、暗号化装置２における暗号化方式として、検証可能属性ベース検索可能暗号方式（ＶＡＢＫＳ方式、ＶＡＢＫＳ委託方式）を例に説明した。しかし、暗号化方式は、検索結果の正当性を検証する機能を有していない属性ベース検索可能暗号方式（ＡＢＫＳ方式）、あるいは、ＡＢＫＳ方式の暗号化処理の一部をクラウドサーバに委託したＡＢＫＳ委託方式を用いて、簡易化して構成してもよい。その場合、マッチングシステムＳ，ＳＢから、検証用データを用いた検証の機能（図５の検証鍵受信手段６６、検索結果検証手段６７０）を省略すればよい。

【００９９】

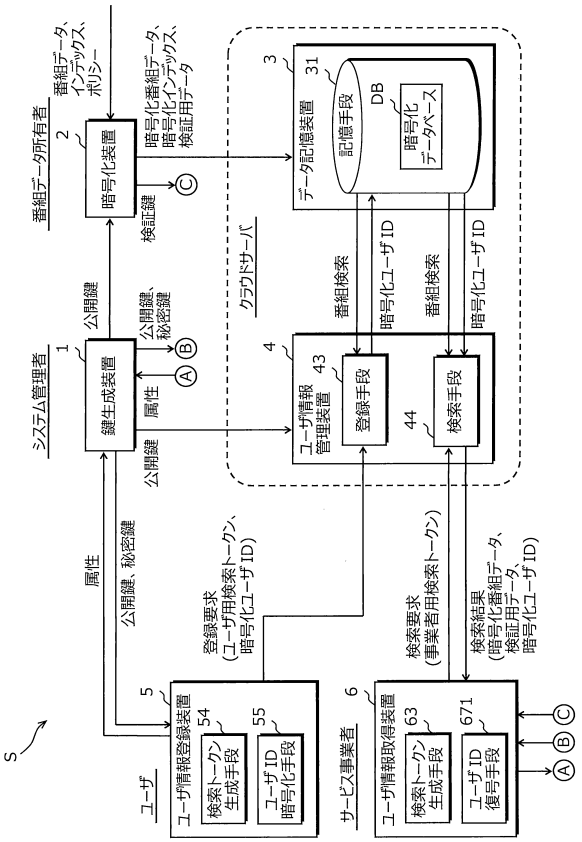
また、ここでは、ユーザＩＤを、ユーザ情報登録装置５のユーザＩＤ暗号化手段５５において暗号化し、ユーザ情報取得装置６のユーザＩＤ復号手段６７１において復号する構成とした。本実施形態では、ＡＢＥ暗号方式を採用することで、鍵配布・鍵管理のコスト

を抑えることができ、さらにユーザがサービス事業者に対してポリシーによるアクセス制御を可能とした。
　しかし、本発明において、個人情報である履歴情報を保護する目的を達成するためには、必ずしもユーザＩＤの暗号化および復号は必須ではない。
【０１００】
　また、ここでは、サービス事業者が提供するサービスと、ユーザ（ユーザＩＤ）とをマッチングさせるため、ユーザの番組の視聴履歴を用いた。
　しかし、このマッチングは、番組の視聴履歴に限定されるものではない。例えば、ユーザがインターネットで商品を購入した購入履歴を用いることとしてもよい。この場合、実施形態で説明した番組を商品、視聴履歴を購入履歴に置き換えて適用すればよい。
　これによって、ユーザは、自身の購入履歴を暗号化してクラウドに登録し、提供可能なサービス事業者（例えば、認定を受けたサービス事業者）のみに、ユーザ情報を提供することが可能になる。
【符号の説明】
【０１０１】
　Ｓ，ＳＢ　マッチングシステム
　１　　鍵生成装置
　２　　暗号化装置
　２Ａ　部分暗号化装置
　２Ｂ　委託暗号化装置
　３　　データ記憶装置
　３０　データ受信手段
　３１　記憶手段
　４　　ユーザ情報管理装置
　４０　公開鍵受信手段
　４１　公開鍵記憶手段
　４２　要求受信手段
　４３　登録手段
　４３０　番組検索手段
　４３１　ユーザＩＤ追加手段
　４４　検索手段
　４４０　番組検索手段
　４４１　ユーザＩＤ読出手段
　４５　検索結果送信手段
　５　　ユーザ情報登録装置
　５０　属性送信手段
　５１　鍵情報受信手段
　５２　鍵情報記憶手段
　５３　視聴履歴記憶手段
　５４　検索トークン生成手段
　５５　ユーザＩＤ暗号化手段
　５６　登録要求送信手段
　６　　ユーザ情報取得装置
　６０　属性送信手段
　６１　鍵情報受信手段
　６２　鍵情報記憶手段
　６３　検索トークン生成手段
　６４　検索要求送信手段
　６５　検索結果受信手段
　６６　検証鍵受信手段

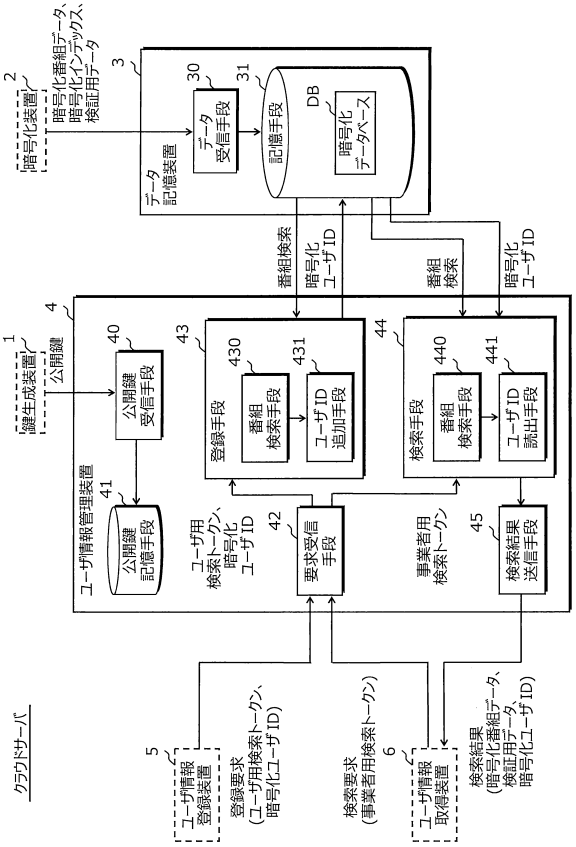
６７　　復号手段
６７０　検索結果検証手段
６７１　ユーザＩＤ復号手段
ＤＢ　　暗号化データベース

【図面】

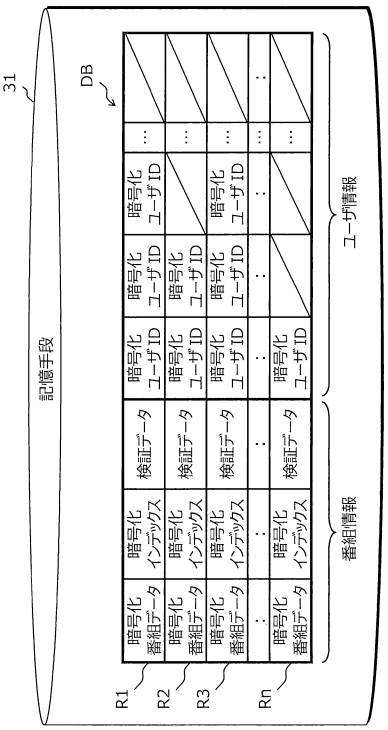
【図１】



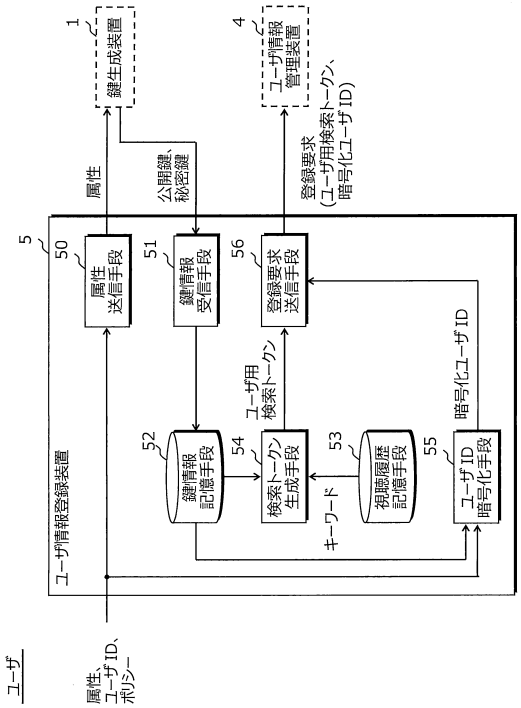
【図２】



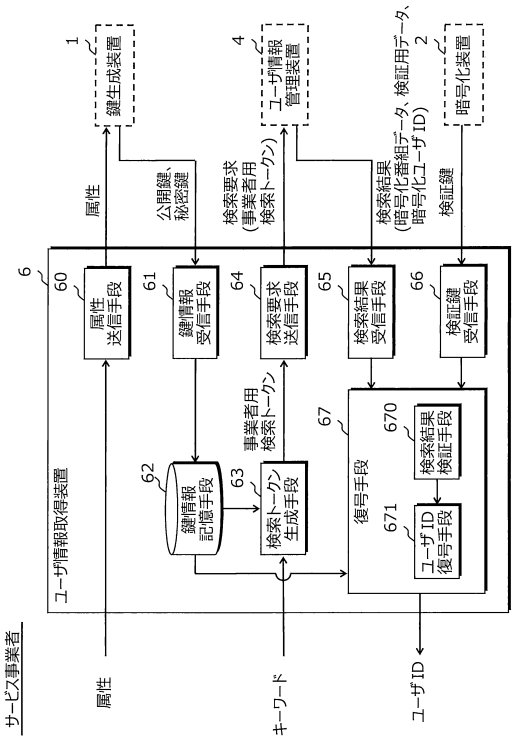
【図３】


31
記憶手段
DB
暗号化番組データ
暗号化インデックス
検証データ
暗号化ユーザID
…
R1
R2
R3
Rn
ユーザ情報
番組情報

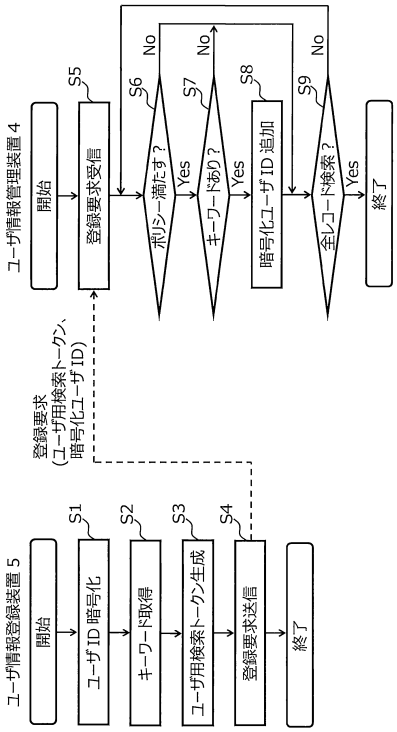
【図４】


1
鍵生成装置
4
ユーザ情報管理装置
属性
公開鍵、秘密鍵
登録要求（ユーザ用検索トークン、暗号化ユーザID）
5
ユーザ情報登録装置
50
属性送信手段
51
鍵情報受信手段
56
登録要求送信手段
52
鍵情報記憶手段
54
検索トークン生成手段
53
視聴履歴記憶手段
55
ユーザID暗号化手段
ユーザ用検索トークン
キーワード
暗号化ユーザID
ユーザ
属性、ユーザID、ポリシー

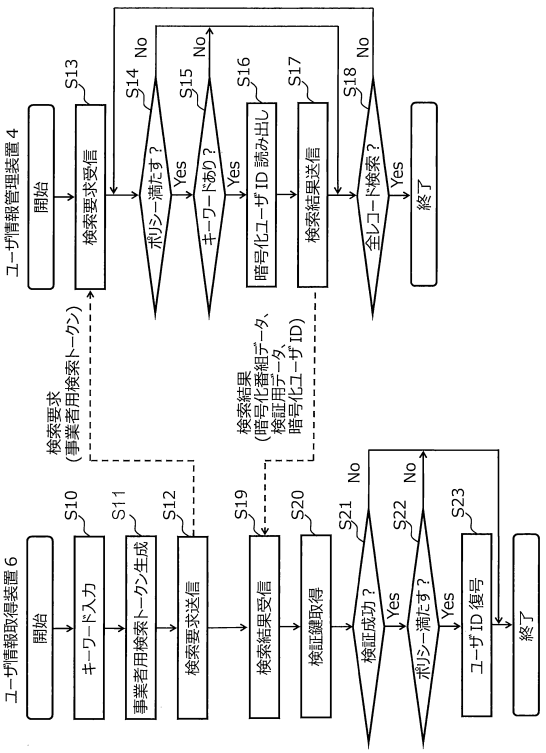
【図５】


サービス事業者
1
鍵生成装置
4
ユーザ情報管理装置
2
暗号化装置
属性
公開鍵、秘密鍵
検索要求（事業者用検索トークン）
検索結果（暗号化番組データ、検証用データ、暗号化ユーザID）
検証鍵
6
ユーザ情報取得装置
60
属性送信手段
61
鍵情報受信手段
64
検索要求送信手段
65
検索結果受信手段
66
検証鍵受信手段
62
鍵情報記憶手段
63
検索トークン生成手段
事業者用検索トークン
67
復号手段
670
検索結果検証手段
671
ユーザID復号手段
属性
キーワード
ユーザID

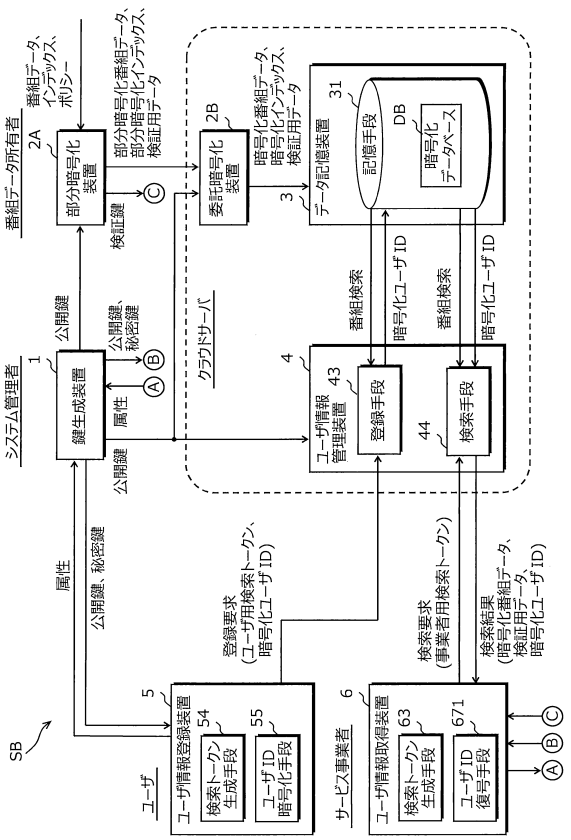
【図６】


ユーザ情報管理装置 4
開始
S5
登録要求受信
S6
ポリシー満たす？
No
Yes
S7
キーワードあり？
No
Yes
S8
暗号化ユーザID追加
S9
全レコード検索？
No
Yes
終了
登録要求（ユーザ用検索トークン、暗号化ユーザID）
ユーザ情報登録装置 5
開始
S1
ユーザID暗号化
S2
キーワード取得
S3
ユーザ用検索トークン生成
S4
登録要求送信
終了

【図７】


ユーザ情報取得装置 6
開始
S10
キーワード入力
S11
事業者用検索トークン生成
S12
検索要求送信
S19
検索結果受信
S20
検証鍵取得
S21
No
検証成功？
Yes
S22
No
ポリシー満たす？
Yes
S23
ユーザID 復号
終了
検索要求
(事業者用検索トークン)
検索結果
(暗号化番組データ、
検証用データ、
暗号化ユーザID)
ユーザ情報管理装置 4
開始
S13
検索要求受信
S14
No
ポリシー満たす？
Yes
S15
No
キーワードあり？
Yes
S16
暗号化ユーザID 読み出し
S17
検索結果送信
S18
No
全レコード検索？
Yes
終了

【図８】


番組データ所有者
2A
番組データ、
インデックス、
ポリシー
部分暗号化
装置
部分暗号化番組データ、
部分暗号化インデックス、
検証用データ
検証鍵
C
2B
委託暗号化
装置
暗号化番組データ、
暗号化インデックス、
検証用データ
3
データ記憶装置
31
記憶手段
DB
暗号化
データベース
システム管理者
1
鍵生成装置
公開鍵
公開鍵、
秘密鍵
A
B
属性
公開鍵
クラウドサーバ
4
ユーザ情報
管理装置
43
登録手段
44
検索手段
番組検索
暗号化ユーザID
番組検索
暗号化ユーザID
属性
公開鍵、秘密鍵
登録要求
(ユーザ用検索トークン、
暗号化ユーザID)
検索要求
(事業者用検索トークン)
検索結果
(暗号化番組データ、
検証用データ、
暗号化ユーザID)
SB
5
ユーザ情報登録装置
54
検索トークン
生成手段
55
ユーザID
暗号化手段
ユーザ
サービス事業者
6
ユーザ情報取得装置
63
検索トークン
生成手段
671
ユーザID
復号手段
A
B
C

フロントページの続き

(56)参考文献 再公表特許第２０１６／１２９２５９（ＪＰ，Ａ１）
特開２０１７－１６８１３０（ＪＰ，Ａ）
米国特許出願公開第２０１６／０１３２６９２（ＵＳ，Ａ１）
大竹 剛、外２名，委託可能な属性ベース検索可能暗号の実装評価，２０１８年 暗号と情報セキュリティシンポジウム（ＳＣＩＳ２０１８）予稿集 ［ＵＳＢ］ ２０１８年 暗号と情報セキュリティシンポジウム概要集，日本，一般社団法人電子情報通信学会，2018年02月13日，ｐ．１－８
大竹 剛、外２名，検証可能な属性ベース検索可能暗号の効率化に関する検討，電子情報通信学会技術研究報告，日本，一般社団法人電子情報通信学会，2017年03月02日，第１１６巻，第５０５号，ｐ．１９５－２０２
大竹 剛、外２名，委託先の攻撃に対して耐性のある委託可能な属性ベース暗号，ＳＣＩＳ２０１６，日本，電子情報通信学会，2016年01月19日，ｐ．１－８

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １６／００－１６／９５８
Ｈ０４Ｌ ９／３０－ ９／４０