(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第6962629号
(P6962629)
(45)発行日　令和3年11月5日(2021.11.5)　(24)登録日　令和3年10月18日(2021.10.18)

(51)Int.Cl.		F I		
G09C 1/00	(2006.01)	G09C	1/00	650Z
H04L 9/30	(2006.01)	H04L	9/00	663Z
G06F 21/60	(2013.01)	G06F	21/60	320
G06F 21/62	(2013.01)	G06F	21/62	318

請求項の数 9　(全 31 頁)

(21)出願番号　特願2021-48066(P2021-48066)
(22)出願日　令和3年3月23日(2021.3.23)
審査請求日　令和3年3月26日(2021.3.26)

早期審査対象出願

(73)特許権者　518334141
ＥＡＧＬＹＳ株式会社
東京都渋谷区千駄ヶ谷５－２７－３　やまとビル７Ｆ
(74)代理人　100210815
弁理士　西田　聡子
(72)発明者　今林　広樹
東京都渋谷区代々木１丁目５５－１４　内海ビル３０１号室　ＥＡＧＬＹＳ株式会社内

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】データ共有システム、データ共有方法、およびデータ共有プログラム

(57)【特許請求の範囲】
【請求項１】
複数のデータ提供装置と、鍵管理装置と、プロキシ装置と、演算装置と、を備えるデータ共有システムであって、
前記鍵管理装置は、システム公開鍵およびシステム秘密鍵の鍵対であるシステム鍵を管理する鍵管理部を有し、
前記複数のデータ提供装置は、
機微データを取得する第１の機微データ取得部と、
前記システム鍵とは異なる、ユーザ公開鍵およびユーザ秘密鍵の鍵対であるユーザ鍵を生成する鍵生成部と、
前記ユーザ公開鍵を用いて、前記機微データを完全準同型暗号方式で暗号化する暗号化部を有し、
前記プロキシ装置は、
前記複数のデータ提供装置から、前記暗号化された機微データを取得する第２の機微データ取得部と、
前記取得した機微データを、前記システム公開鍵および前記ユーザ秘密鍵に基づいて生成される再暗号化鍵を用いて、完全準同型暗号方式で暗号化することで、所定の暗号化空間における機微データに変換する変換部と、
を有し、
前記演算装置は、前記変換された機微データに基づいて、秘密計算として、機械学習に

よるモデル学習および推論を実行する実行部を有し、
前記鍵管理装置は、前記再暗号化鍵の生成を行わない、データ共有システム。
【請求項２】
前記データ提供装置は、
前記鍵管理装置の前記鍵管理部から前記システム公開鍵を取得するシステム鍵取得部をさらに有し、
前記鍵生成部は、前記ユーザ秘密鍵および前記システム公開鍵を用いて再暗号化鍵を生成し、
前記プロキシ装置は、前記データ提供装置から前記再暗号化鍵を取得する再暗号化鍵取得部をさらに有する、請求項１に記載のデータ共有システム。
【請求項３】
前記プロキシ装置は、
前記鍵管理装置の前記鍵管理部から前記システム公開鍵を取得するシステム鍵取得部と、
前記データ提供装置から前記ユーザ秘密鍵を取得するユーザ鍵取得部と、
前記ユーザ秘密鍵および前記システム公開鍵を用いて再暗号化鍵を生成する鍵生成部と、をさらに有する、請求項１に記載のデータ共有システム。
【請求項４】
複数のデータ提供装置と、鍵管理装置と、プロキシ装置と、演算装置と、を備えるデータ共有システムであって、
前記鍵管理装置は、システム鍵を管理する鍵管理部を有し、
前記複数のデータ提供装置は、
機微データを取得する第１の機微データ取得部と、
前記システム鍵とは異なるユーザ鍵を用いて前記機微データを所定の暗号方式で暗号化する暗号化部を有し、
前記プロキシ装置は、
前記複数のデータ提供装置から、前記暗号化された機微データを取得する第２の機微データ取得部と、
標準実行環境から保護される仮想実行環境を構築し、前記仮想実行環境において、前記取得した機微データを、前記システム鍵に基づいて所定の暗号化空間における機微データに変換する変換部と、
を有し、
前記演算装置は、前記変換された機微データに基づいて秘密計算を実行する実行部を有し、
前記仮想実行環境は、
前記暗号化された機微データを取得する仮想実行環境データ取得部と、
前記暗号化された機微データを復号するユーザ鍵と、前記システム鍵と、を取得する仮想実行環境鍵取得部と、
前記ユーザ鍵を用いて復号した前記機微データを、前記システム鍵を用いて暗号化することにより、前記変換を行う仮想実行環境変換部と、
を含む、データ共有システム。
【請求項５】
前記データ提供装置の前記暗号化部は、前記機微データに含まれる属性項目の少なくとも一部の属性値を所定の暗号方式で暗号化し、
前記プロキシ装置の前記変換部は、前記機微データの、所定の暗号方式で暗号化された前記属性値を、当該所定の暗号方式に応じた暗号方式で前記変換を行う、請求項４に記載のデータ共有システム。
【請求項６】
前記機微データは、第１の暗号方式で暗号化された第１の属性値、および第１の暗号方式と異なる第２の暗号方式で暗号化された第２の属性値を含む、請求項５に記載のデータ

共有システム。
【請求項７】
前記演算装置は、複数の前記変換された機微データを統合して、前記秘密計算を実行する、請求項１から請求項６のいずれか一項に記載のデータ共有システム。
【請求項８】
複数のデータ提供装置と、鍵管理装置と、プロキシ装置と、演算装置と、を備えるシステムにおけるデータ共有方法であって、
前記鍵管理装置は、システム公開鍵およびシステム秘密鍵の鍵対であるシステム鍵を管理するステップを実行し、
前記複数のデータ提供装置は、
機微データを取得するステップと、
前記システム鍵とは異なる、ユーザ公開鍵およびユーザ秘密鍵の鍵対であるユーザ鍵を生成するステップと、
前記ユーザ公開鍵を用いて、前記機微データを完全準同型暗号方式で暗号化するステップと、
を実行し、
前記プロキシ装置は、
前記複数のデータ提供装置から、前記暗号化された機微データを取得するステップと、
前記取得した機微データを、前記システム公開鍵および前記ユーザ秘密鍵に基づいて生成される再暗号化鍵を用いて、完全準同型暗号方式で暗号化することで、所定の暗号化空間における機微データに変換するステップと、
を実行し、
前記演算装置は、前記変換された機微データに基づいて、秘密計算として、機械学習によるモデル学習および推論を実行するステップを実行し、
前記鍵管理装置は、前記再暗号化鍵を生成するステップを実行しない、
データ共有方法。
【請求項９】
複数のデータ提供装置と、鍵管理装置と、プロキシ装置と、演算装置と、を備えるシステムに実行させるデータ共有プログラムであって、
前記鍵管理装置は、システム公開鍵およびシステム秘密鍵の鍵対であるシステム鍵を管理するステップを実行し、
前記複数のデータ提供装置は、
機微データを取得するステップと、
前記システム鍵とは異なる、ユーザ公開鍵およびユーザ秘密鍵の鍵対であるユーザ鍵を生成するステップと、
前記ユーザ公開鍵を用いて、前記機微データを完全準同型暗号方式で暗号化するステップと、
を実行し、
前記プロキシ装置は、
前記複数のデータ提供装置から、前記暗号化された機微データを取得するステップと、
前記取得した機微データを、前記システム公開鍵および前記ユーザ秘密鍵に基づいて生成される再暗号化鍵を用いて、完全準同型暗号方式で暗号化することで、所定の暗号化空間における機微データに変換するステップと、
を実行し、
前記演算装置は、前記変換された機微データに基づいて、秘密計算として、機械学習によるモデル学習および推論を実行するステップを実行し、
前記鍵管理装置は、前記再暗号化鍵を生成するステップを実行しない、
データ共有プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、データ共有システム、データ共有方法、およびデータ共有プログラムに関する。
【背景技術】
【０００２】
インターネット上で提供される電子商取引サービスや、ＩｏＴ（Internet of Things）の進展により、自社保有のデータはもとより、社外（他者）のデータをも活用した大量のデータに対する統計分析や機械学習を行う技術が求められている。例えば、特許文献１には、異なる公開鍵を用いて暗号化された暗号データに対して、暗号化したまま統計処理を行う暗号化統計処理システムが開示されている。当該システムでは、所定の公開鍵を用いて暗号化された暗号化データを、その公開鍵とは異なる公開鍵に対応する秘密鍵を用いて復号できる暗号データに変換するためのプロキシ鍵を生成し、プロキシ鍵に基づいて暗号化されたデータから暗号化統計データ（処理結果）を生成する。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】国際公開第２０１２／１６９１５３号
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、特許文献１に記載のシステムは、複数のサービス提供装置の公開鍵及び秘密鍵を用いて対話的に全体公開鍵を生成し、全体公開鍵と各サービス提供装置の秘密鍵とに基づいて個々のプロキシ鍵を生成するため、自身が保有するデータを暗号化したまま利活用するには、システムに参加する他者の公開鍵及び秘密鍵が必要となり、各サービス提供装置間の通信量が膨大になってしまう。
【０００５】
また、昨今は、機械学習や人工知能技術の広まりから、情報漏洩や不正利用等の情報セキュリティ上の問題を考慮しながら、膨大なデータを扱うことができる技術が望まれているところ、特許文献１に記載のシステムは、一部のサービス提供装置から提供されるデータに基づいた部分統計処理に基づく統計処理であり、複数のサービス提供者の各データを統合して行うことでより高い予測精度が期待される全体統計や機械学習などの処理を行うものではない。
【０００６】
そこで、本開示は、上記課題を解決すべくなされたものであって、その目的は、各者が保有するデータを、データの詳細を他者に開示することなく、安全に活用することができるデータ共有システムを提供することである。
【課題を解決するための手段】
【０００７】
上記目的を達成するため、本開示に係るデータ共有システムは、複数のデータ提供装置と、鍵管理装置と、プロキシ装置と、演算装置と、を備えるシステムであって、鍵管理装置は、システム鍵を管理する鍵管理部を有し、複数のデータ提供装置は、機微データを取得する第１の機微データ取得部と、システム鍵とは異なるユーザ鍵を用いて機微データを所定の暗号方式で暗号化する暗号化部を有し、プロキシ装置は、複数のデータ提供装置から、暗号化された機微データを取得する第２の機微データ取得部と、取得した機微データを、システム鍵に基づいて所定の暗号化空間における機微データに変換する変換部と、を有し、演算装置は、変換された機微データに基づいて秘密計算を実行する実行部を有する。
【０００８】

上記目的を達成するため、本開示に係るデータ共有方法は、複数のデータ提供装置と、鍵管理装置と、プロキシ装置と、演算装置と、を備えるシステムにおける方法であって、鍵管理装置は、システム鍵を管理するステップを実行し、複数のデータ提供装置は、機微データを取得するステップと、システム鍵とは異なるユーザ鍵を用いて機微データを所定の暗号方式で暗号化するステップと、を実行し、プロキシ装置は、複数のデータ提供装置から、暗号化された機微データを取得するステップと、取得した機微データを、システム鍵に基づいて所定の暗号化空間における機微データに変換するステップと、を実行し、演算装置は、変換された機微データに基づいて秘密計算を実行するステップを実行する。

【０００９】

また、上記目的を達成するため、本開示に係るデータ共有プログラムは、複数のデータ提供装置と、鍵管理装置と、プロキシ装置と、演算装置と、を備えるシステムに実行させるプログラムであって、鍵管理装置は、システム鍵を管理するステップを実行し、複数のデータ提供装置は、機微データを取得するステップと、システム鍵とは異なるユーザ鍵を用いて機微データを所定の暗号方式で暗号化するステップと、を実行し、プロキシ装置は、複数のデータ提供装置から、暗号化された機微データを取得するステップと、取得した機微データを、システム鍵に基づいて所定の暗号化空間における機微データに変換するステップと、を実行し、演算装置は、変換された機微データに基づいて秘密計算を実行するステップを実行する。

【発明の効果】

【００１０】

本開示によれば、データ共有システムにおいて、各者が保有するデータの内容を他者に開示することなく、安全に活用することができる。

【図面の簡単な説明】

【００１１】

【図１】データ共有システム１の構成を示す図である。
【図２】実施形態１に係る処理の概念図である。
【図３】データ提供サーバ１００の機能構成の一例を示す機能ブロック図である。
【図４】鍵管理サーバ２００の機能構成の一例を示す機能ブロック図である。
【図５】プロキシサーバ３００の機能構成の一例を示す機能ブロック図である。
【図６】演算サーバ４００の機能構成の一例を示す機能ブロック図である。
【図７】端末装置５００の機能構成の一例を示す機能ブロック図である。
【図８】機微データのデータ構造の一例を示した図である。
【図９】暗号化された機微データのデータ構造の一例を示す図である。
【図１０】統合データのデータ構造の一例を示す図である。
【図１１】実施形態１に係る処理の一例を示すフローチャートである。
【図１２】プロキシサーバ３００のハードウェア構成を示すブロック図である。
【図１３】実施形態２に係る処理の概念図である。
【図１４】データ提供サーバ６００の機能構成の一例を示す機能ブロック図である。
【図１５】プロキシサーバ７００の機能構成の一例を示す機能ブロック図である。
【図１６】実施形態２に係る処理の一例を示すフローチャートである。

【発明を実施するための形態】

【００１２】

以下、本開示の実施形態について図面を参照して説明する。実施形態を説明する全図において、共通の構成要素には同一の符号を付し、繰り返しの説明を省略する。なお、以下の実施形態は、特許請求の範囲に記載された本開示の内容を不当に限定するものではない。また、実施形態に示される構成要素のすべてが、本開示の必須の構成要素であるとは限らない。

【００１３】

＜発明の概要＞

近年、顧客情報などの大量の機微データを保有する組織が増加している。これにより、

自組織だけでなく、他組織が保有する機微データも活用して統計的な分析処理や機械学習等を行い、ビジネス上の新たな知見や、サービスにつなげるようなクラウドサービスが普及しつつある。しかしながら、機微データは、セキュリティへの配慮や、プライバシーの保護などデータの取り扱いに細心の注意が求められるため、自組織の保有する機微データの情報漏洩を防ぎつつ、検索や集計分析、統計、機械学習など、精度の高い検知、予測に資するようなデータ処理を行うことが求められる。

【００１４】

不正なアクセス等による情報漏洩を防ぎながら、データ処理を実現する技術として、データを暗号化したまま演算を行う「秘密計算」が知られている。「秘密計算」の実現方式の一つとして、例えば、準同型暗号がある。準同型暗号は、準同型性を有する暗号方式であり、ある公開鍵を用いて暗号化された暗号データに対して、暗号化したまま、数値計算等の演算を行うことができる。準同型暗号を用いて、複数の暗号データを対象としたデータ処理を現実的な処理性能で可能とするためには、これらの暗号データが同一の暗号化空間にある、すなわち、同一の公開鍵により暗号化されている必要がある。

【００１５】

そこで、本発明に係るデータ共有システムは、暗号データを同一の暗号化空間に変換するためのシステム鍵を管理する鍵管理装置を備える。また、当該システムに参加する各組織等に対応するデータ提供装置は、システム鍵とは異なる、当該組織に対応するユーザ鍵を用いて機微データを所定の暗号方式で暗号化し、プロキシ装置に送信する。プロキシ装置は、取得した暗号化された機微データを、システム鍵に基づいて、所定の暗号化空間に変換する。そして、演算装置は、変換された機微データに基づいて秘密計算を実行する。システム鍵（暗号鍵に対応）に基づいて所定の暗号化空間に変換された機微データに対する秘密計算の実行結果は、システム鍵（復号鍵に対応）により復号することができる。なお、以下、本明細書において、「秘密計算」とは、データを暗号化状態のまま演算を行う処理のことをいい、「演算」とは、加減乗除に関する計算、検索、分析、機械学習に関する計算を含む。

【００１６】

＜実施形態１＞

本実施形態では、プロキシサーバ３００が、各データ提供サーバ１００において暗号化された機微データを復号することなく、再暗号化鍵により同一の暗号化空間に変換する。

【００１７】

（データ共有システム１の構成）

図１は、本実施形態に係るデータ共有システム１の構成を示す図である。図１を参照して、実施形態１に係るデータ共有システム１の構成について説明する。

【００１８】

データ共有システム１は、データ提供サーバ１００－１，１００－２，…，１００－Ｎ（Ｎは自然数）と、鍵管理サーバ２００と、プロキシサーバ３００と、演算サーバ４００と、端末装置５００と、を備える。図１において、データ提供サーバ１００－１，１００－２，…，１００－Ｎと、鍵管理サーバ２００と、プロキシサーバ３００と、演算サーバ４００と、端末装置５００とは、ネットワークＮＷを介して通信可能に接続される。ネットワークＮＷは、例えば、ＷＡＮ（Wide Area Network）、ＬＡＮ（Local Area Network）、光回線網、イントラネット等であるが、任意のネットワークから構成されてもよい。データ共有システム１は、当該システムに参加する各組織が、それぞれの組織が保有するデータを、他組織にデータの詳細な内容を開示することなく利用できるプラットフォームである。なお、組織とは、企業や団体に限られず、役割ごとに区切られた部門、課、グループ、チーム等の集団であってもよい。

【００１９】

以下の説明では、データ提供サーバ１００－１，１００－２，…，１００－Ｎは、特に区別する必要のない限り、データ提供サーバ１００と記載する。

【００２０】

データ提供サーバ１００は、プラットフォームに参加する組織と関連付けられており、組織が保有する機微データを暗号化し、鍵管理サーバ２００に送信する。図１において、例えば、データ提供サーバ１００－１は「会社Ａ」、データ提供サーバ１００－２は「会社Ｂ」、データ提供サーバ１００－Ｎは「会社Ｘ」に関連付けられている。

【００２１】

データ提供サーバ１００は、システム鍵（後述）とは異なるユーザ鍵を用いて機微データを所定の暗号方式で暗号化し、プロキシサーバ３００に送信する。なお、データ提供サーバ１００は、ユーザ鍵を自サーバ内で記憶して管理してもよいし、他の情報処理装置に記憶させて管理（例えば、ＫＭＳ(Key Management Service：鍵管理システム）に管理を委託）してもよい。また、データ提供サーバ１００は、システム鍵およびユーザ鍵に基づいて再暗号化鍵を生成し、プロキシサーバ３００に送信する。

【００２２】

機微データは、例えば、属性項目（カラム）ごとの属性値を含むデータであってもよい。機微データのデータ構造については後述する。また、データ提供サーバ１００は、機微データの一部の属性値を所定の暗号方式で暗号化するようにしてもよい。

【００２３】

鍵管理サーバ２００は、システム鍵を管理する。鍵管理サーバ２００は、例えば、暗号データを復号する復号鍵が適切な方法で管理されている信頼された機関であるが、プロキシサーバ３００に内包されるように構成されてもよい。すなわち、プロキシサーバ３００が、システム鍵を管理する機能を備えてもよい。

【００２４】

プロキシサーバ３００は、各データ提供サーバ１００から暗号化された機微データおよび再暗号化鍵を取得し、当該再暗号化鍵により、取得した機微データを所定の暗号化空間における機微データに変換する。

【００２５】

演算サーバ４００は、プロキシサーバ３００において変換された機微データについて、秘密計算を実行する。演算サーバ４００は、秘密計算として、例えば、検索、統合、分析、データマイニング、および機械学習によるモデル学習および推論を行う。例えば、モデル学習および推論は、統計的手法もしくは深層学習等の解析アルゴリズムによって行われてもよい。また、演算サーバ４００は、例えば、複数の変換された機微データを統合し、統合した機微データについて秘密計算を実行してもよい。秘密計算の実行結果は、システム鍵（復号鍵に相当）で復号することができる。

【００２６】

端末装置５００は、データ共有システム１のユーザが用いる情報処理装置である。端末装置５００は、例えば、ＰＣ（Personal Computer）、スマートフォン、タブレット端末である。また、ヘッドマウントディスプレイ等のウェアラブル端末、ＡＲ（Augmented Reality）／ＶＲ（Virtual Reality）／ＭＲ（Mixed Reality）装置等であってもよい。ユーザは、例えば、会社Ａの社員など、プラットフォームに参加し、機微データを提供する組織の従業員であってもよく、この場合、情報処理装置は、ユーザが所属する組織のデータ提供サーバ１００と紐づけられた構成としてもよい。

【００２７】

端末装置５００は、演算サーバ４００に対し、各データ提供サーバ１００から提供される機微データを対象としたデータ処理の処理要求を行う。データ処理は、例えば、検索・集計処理および／または統計処理を含む。また、データ処理は、機微データを統合する処理を含む。データ処理の処理要求（処理クエリ）は、例えば、ＳＱＬ文などのＣＬＩ（Command Line Interface)もしくはＧＵＩ（Graphical User Interface）によって記載される。

【００２８】

以下、上述したデータ共有システム１を構成する各サーバ等の機能構成、処理について説明する。なお、各機能構成を示す機能ブロックや処理ブロックは、１つ、または複数の

装置、コンピュータプロセッサ、コンピュータプロセッサの分散グループによって実現されてもよい。例えば、鍵管理サーバ２００、プロキシサーバ３００、演算サーバ４００が行う機能は、１つの装置で実現されてもよい。

【００２９】

図２は、実施形態１に係る処理の概念図である。図２を参照して、データ共有システム１における処理の概要について説明する。

【００３０】

実施形態１は「プロキシ再暗号化方式」を用いるものであって、プロキシサーバ３００は、データ提供サーバ１００において暗号化された機微データを復号することなく、所定の暗号化空間に変換する。図２では、公開鍵暗号方式をベースとした方式を説明するが、共通鍵暗号方式を用いても当該変換は実現可能である。

【００３１】

（１）鍵生成ステップ

鍵管理サーバ２００は、システム鍵として、システム公開鍵Pkxおよびシステム秘密鍵Skxの鍵対を生成する。

各データ提供サーバ１００は、ユーザ鍵として、それぞれ自身のユーザ公開鍵pkおよびユーザ秘密鍵skの鍵対を生成する。ユーザ鍵およびシステム鍵は、例えば、公知の鍵生成アルゴリズム等により生成される。

【００３２】

また、各データ提供サーバ１００は、鍵管理サーバ２００からシステム公開鍵Pkxを取得し、ユーザ秘密鍵skおよびシステム公開鍵Pkから再暗号化鍵rkを生成する。生成した再暗号化鍵rkは、プロキシサーバ３００へ送信する。再暗号化鍵rkは、例えば、ユーザ秘密鍵skとシステム公開鍵Pkに基づいて、鍵生成アルゴリズムにより生成されてもよいし、ユーザ秘密鍵skをシステム公開鍵Pkで暗号化して生成するようにしてもよい。プロキシサーバ３００は、各データ提供サーバ１００と対応付けて再暗号化鍵rkを記憶する。

【００３３】

なお、図２において、再暗号化鍵rkは、データ提供サーバ１００で生成されるが、プロキシサーバ３００で生成するよう構成してもよい。例えば、プロキシサーバ３００とデータ提供サーバ１００との間でセキュアな通信チャンネルを確立し、プロキシサーバ３００が各データ提供サーバ１００から、ユーザ秘密鍵skをそれぞれ取得する。プロキシサーバ３００は、鍵管理サーバ２００からシステム公開鍵Pkxを取得し、各データ提供サーバ１００に対応するユーザ秘密鍵skとシステム公開鍵Pkxとを用いて各再暗号化鍵rkを生成し、それぞれデータ提供サーバ１００と対応付けて記憶するようにしてもよい。

【００３４】

（２）登録ステップ

データ提供サーバ１００は、機微データをユーザ公開鍵pkで暗号化し、暗号文Mを生成する。生成された暗号文Mは、プロキシサーバ３００に送信される。プロキシサーバ３００は、各暗号文Mをデータ共有システム１に参加する組織から提供されたデータとして登録（記憶）する。

【００３５】

（３）データ処理ステップ

演算サーバ４００は、例えば、端末装置５００（図２において不図示）からの処理要求に応じて、プロキシサーバ３００に対し、処理要求の対象となる機微データを要求する。

【００３６】

プロキシサーバ３００は、データ処理の対象となる暗号文Mを、暗号文Mを送信したデータ提供サーバ１００において生成された再暗号化鍵rkで暗号化し、再暗号化文Mを生成する。プロキシサーバ３００は、再暗号化文Mを、演算サーバ４００に送信する。演算サーバ４００は、再暗号化文について秘密計算を実行する。この際、演算サーバ４００は、プロキシサーバ３００から取得した各再暗号化文Mを統合して、秘密計算を実行するよう

にしてもよい。データの統合については後述する。

【００３７】

秘密計算の実行結果は、データ処理を要求した端末装置５００に送信される。また、実行結果を利用する権限を有するユーザに使用する端末装置５００は、鍵管理サーバ２００からシステム秘密鍵Skxを取得することができる。端末装置５００は、システム秘密鍵Skxを用いて実行結果を復号することにより、データ処理の結果を利用することができる。

【００３８】

また、秘密計算の実行結果は、プロキシサーバ３００を介して、データ処理を要求した端末装置５００に送信されてもよい。例えば、演算サーバ４００は、プロキシサーバ３００に実行結果を送信する。プロキシサーバ３００は鍵管理サーバ２００からシステム秘密鍵Skxを取得し、演算サーバ４００から送信された実行結果を復号する。そして、プロキシサーバ３００は、プロキシサーバ３００と端末装置５００との間で確立されたセキュアな通信路で用いられるセッション鍵で上記復号した実行結果を暗号化し、端末装置５００に送信する。端末装置５００は、セッション鍵を用いて実行結果を復号することにより、データ処理の結果を利用することができる。

【００３９】

上述のように、図２では、公開鍵暗号方式により暗号文を同一の暗号化空間に変換する方法を説明したが、共通鍵暗号方式の場合は、例えば「ワンタイムパッド」を利用することで実現できる。同暗号は、平文をビット列とみなし、同じ長さのランダムなビット列（共通鍵）をビットごとに排他的論理和を行うことで暗号化を行う。復号するには、暗号化に用いたランダムなビット列と暗号文の排他的論理和を用いればよい。また、再暗号化鍵は、ユーザ共通鍵（ユーザ鍵）とシステム共通鍵（システム鍵）との排他的論理和により生成される。データ提供サーバ１００は、機微データとユーザ共通鍵との排他的論理和により暗号文Ｍを生成する。そして、プロキシサーバ３００は、暗号文Ｍと再暗号化鍵との排他的論理和より、再暗号化文Ｍを生成する。

【００４０】

なお、図２では、データ提供サーバ１００が再暗号化鍵を生成する場合を説明したが、上述したように、再暗号化鍵は、プロキシサーバ３００が生成してもよい。例えば、プロキシサーバ３００が、鍵管理サーバ２００から取得したシステム公開鍵と、データ提供サーバ１００から取得したユーザ秘密鍵とを用いて再暗号化鍵を生成する。ただし、プロキシサーバ３００において、各データ提供サーバ１００から取得したユーザ秘密鍵は、信頼できる環境で適切に管理される必要がある。

【００４１】

また、図２の説明では、演算サーバ４００が、端末装置５００からの処理要求に応じて、プロキシサーバ３００に対し、処理要求の対象となる機微データを要求し、プロキシサーバ３００において再暗号化文が生成されたが、プロキシサーバ３００が、定期的に再暗号化文を生成する処理を実行し、再暗号化文を記憶するようにしておいてもよい。このように構成することで、演算サーバ４００は、プロキシサーバ３００に対して処理要求の対象となる機微データを要求すると、その再暗号化文の生成処理が行われるのを待つことなく、再暗号化文を取得することができる。

【００４２】

（データ提供サーバ１００の機能構成）

図３は、データ提供サーバ１００の機能構成の一例を示す機能ブロック図である。図３を参照して、データ提供サーバ１００の機能構成の一例について説明する。

【００４３】

データ提供サーバ１００は、通信部１０１と、制御部１０２と、記憶部１０３と、鍵生成部１０４と、暗号化部１０５と、を備える。

【００４４】

通信部１０１は、データ提供サーバ１００がネットワークＮＷを介してサーバや装置等と所定の通信プロトコルに従って通信を行うための通信インタフェース回路を有する。所

定の通信プロトコルは、ＴＣＰ／ＩＰ(Transmission Control Protocol/Internet Protocol）等である。通信部１０１は、受信したデータを制御部１０２に送り、また、制御部１０２から受け取ったデータを、ネットワークＮＷを介してサーバや装置等に送信するが、通信部１０１は、データ提供サーバ１００内の制御部１０２以外の機能ブロックとデータのやり取りを行ってもよい。なお、通信部１０１は、ネットワークＮＷを介した装置やローカルに接続された装置等と、セキュリティが確保されたセキュアな通信チャンネルでデータを送受信する。セキュアな通信チャンネルの構築、通信方法は、共通鍵（セッション鍵など）や公開鍵等を用いた周知の技術であるため、説明を省略する。

【００４５】

通信部１０１は、第１の機微データ取得部に相当し、例えば、プラットフォームに参加する組織から、当該組織が保有する機微データを取得する。図１において、会社Ａと関連付けられるデータ提供サーバ１００－１は、会社Ａの社員が操作する端末装置５００から機微データを取得してもよい。本実施形態において、機微データは、例えば、個人に関する情報であって、年齢、性別、収入、居住地域、購買情報などの個人の属性を示す項目である属性項目（カラム）の属性値（文字列又は数値）である。また、機微データは、機微データを統合するための統合キーとなる識別子（文字列、数値、またはそれらの組み合わせ）を属性項目として含み、個人を一意に特定する共通ＩＤ等を識別子としてもよい。機微データは、識別子に基づいて統合されてもよい。機微データは、個人に関する情報に限られず、機器に関するログデータ等であってもよい。機微データ及び機微データのデータ構造の詳細については後述する。

【００４６】

また、通信部１０１は、システム鍵取得部に相当し、鍵管理サーバ２００から、システム鍵（システム公開鍵および／またはシステム共通鍵）を取得する。取得したシステム鍵は記憶部１０３に記憶させる。

【００４７】

制御部１０２は、データ提供サーバ１００の各機能を制御し、予め記憶部１０３に記憶されているプログラムに基づいて動作するＣＰＵ（Central Processing Unit）等のプロセッサである。なお、制御部１０２として、ＤＳＰ（digital signal processor）等が用いられてもよい。また、制御部１０２として、ＬＳＩ（large scale integration）、ＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field-Programmable Gate Array）等の制御回路が用いられてもよい。

【００４８】

記憶部１０３は、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等のメモリ装置、ハードディスク等の固定ディスク装置、又はフレキシブルディスク、光ディスク等の可搬用の記憶装置等を有する。また、記憶部１０３は、データ提供サーバ１００の各種処理に用いられるコンピュータプログラム、暗号プログラム、鍵等が格納される。コンピュータプログラムは、コンピュータ読み取り可能な可搬型記録媒体から公知のセットアッププログラム等を用いて記憶部１０３にインストールされてもよい。可搬型記録媒体は、例えばＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＤＶＤ－ＲＯＭ（Digital Versatile Disc Read Only Memory）等である。コンピュータプログラムは、所定のサーバ等からインストールされてもよい。

【００４９】

鍵生成部１０４は、ユーザ鍵を生成する。鍵生成部１０４は、例えば、暗号化部１０５の要求する暗号方式に応じた鍵を生成する。暗号方式が、例えば、暗号化状態のまま演算が可能な準同型暗号方式（Paillier方式等）の場合は、ユーザ公開鍵とユーザ秘密鍵の鍵対を生成する。

【００５０】

また、暗号方式が、暗号文の大小関係と対応する平文の大小関係が一致する順序保存暗号方式（OPE方式:Order Preserving Encryption）や、暗号化状態のまま平文の一致判定が可能な検索可能暗号方式の場合は、ユーザ共通鍵を生成する。このように、ユーザ鍵は

、ユーザ公開鍵とユーザ秘密鍵の鍵対である場合と、ユーザ共通鍵である場合とがある。なお、鍵生成アルゴリズムは、周知の技術であるので説明を省略する。

【００５１】

また、鍵生成部１０４は、ユーザ鍵とシステム鍵とに基づいて、再暗号化鍵を生成する。公開鍵暗号方式の場合は、ユーザ秘密鍵およびシステム公開鍵を用いて再暗号化鍵を生成する。また、共通鍵暗号方式の場合は、ユーザ共通鍵およびシステム共通鍵を用いて、再暗号化鍵を生成する。なお、再暗号化鍵は、ユーザ鍵およびシステム鍵を用いて鍵生成アルゴリズムにより生成するようにしてもよいし、ユーザ鍵をシステム鍵により暗号化することにより生成するようにしてもよい。

【００５２】

鍵生成部１０４は、生成した鍵や鍵生成のためのパラメータ等を、例えば、記憶部１０３に記憶させる。鍵生成部１０４は、生成した鍵と、暗号方式や、暗号化対象としたデータ（属性項目（カラム）等）、対応するデータ提供サーバ等とを対応付けて記憶部１０３に記憶させてもよい。

【００５３】

暗号化部１０５は、システム鍵とは異なるユーザ鍵を用いて機微データを所定の暗号方式で暗号化する。暗号化部１０５は、例えば、機微データに含まれる属性項目の少なくとも一部の属性値を所定の暗号方式で暗号化する。所定の暗号方式には、通信部１０１が取得した機微データの少なくとも一部の属性値を暗号化状態のまま演算可能な暗号方式を含み、例えば、準同型暗号方式、順序保存暗号方式、ＡＥＳ(Advanced Encryption Standard)、ＤＥＳ（Data Encryption Standard）、検索可能暗号、ＳＨＡ（Secure Hash Algorithm）、ＭＤ５（Message Digest algorithm 5）などである。なお、上述したように「演算」とは、加減乗除に関する計算、検索、分析に関する計算を含む。本実施形態では、暗号化部１０５は、機微データに含まれる属性項目の属性値のうち、データ形式が数値の場合（第１の属性値に相当）は、準同型暗号方式（Paillier方式、Lifted-Ellgamal方式、Somewhat Homomorphic Encryption方式、Fully Homomorphic Encryption方式等）および／または順序保存暗号方式（OPE方式）（第１の暗号方式に相当）を用いて暗号化する。なお、データ処理の内容に応じて、暗号方式により処理効率が異なるので、各属性項目は、準同型暗号方式で暗号化された属性値と、順序保存暗号方式で暗号化された属性値、後述する検索可能暗号方式で暗号化された属性値等、複数の暗号方式で保持しておいてもよい。

【００５４】

また、データ形式が文字列の場合（第２の属性値に相当）は、検索可能暗号方式、もしくは暗号文上で完全一致が可能なＡＥＳ暗号等（第２の暗号方式に相当）を用いて暗号化する。なお、データ形式ごとに適用する上記暗号方式は一例であって、どの属性項目の属性値について暗号化するか、また、どの暗号方式で暗号化するか等は、機微データを保有する組織が適宜決定してもよい。また、個人の意思に従って、機微データを暗号化するか否かを決定してもよい。

【００５５】

本実施形態において、属性項目として含まれる識別子は、暗号化の対象としない。これにより、演算サーバ４００は、再暗号化鍵による再暗号化により、同一の暗号化空間に変換された機微データを、識別子に基づいて統合したデータ（統合データ）を生成することができる。統合データについては後述する。暗号化アルゴリズムは、周知の技術であるので説明を省略する。なお、他の実施形態として、暗号化部１０５は、属性項目として含まれる識別子を暗号化の対象としてもよい。

【００５６】

（鍵管理サーバ２００の機能構成）

図４は、鍵管理サーバ２００の機能構成の一例を示す機能ブロック図である。図４を参照して、鍵管理サーバ２００の機能構成の一例について説明する。

【００５７】

鍵管理サーバ２００は、通信部２０１と、記憶部２１０と、鍵生成部２２０と、を備える。

【００５８】

通信部２０１は、鍵管理サーバ２００がネットワークＮＷを介して各サーバや装置等と所定の通信プロトコルに従って通信を行うための通信インタフェース回路を有する。通信部２０１は、鍵生成部２２０で生成されたシステム鍵を、ネットワークＮＷを介してサーバや装置等に送信する。なお、通信部２０１は、ネットワークＮＷを介した装置等と、セキュリティが確保されたセキュアな通信チャンネルでデータを送受信する。セキュアな通信チャンネルの構築、通信方法は、周知の技術であるため、説明を省略する。

【００５９】

記憶部２１０は、鍵生成部２２０で生成されたシステム鍵を管理する鍵管理部に相当する。記憶部２１０は、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等のメモリ装置、ハードディスク等の固定ディスク装置、又はフレキシブルディスク、光ディスク等の可搬用の記憶装置等を有する。また、記憶部２１０は、鍵管理サーバ２００の各種処理に用いられるコンピュータプログラム、データベース、テーブル等が格納される。コンピュータプログラムは、コンピュータ読み取り可能な可搬型記録媒体から公知のセットアッププログラム等を用いて記憶部２１０にインストールされてもよい。可搬型記録媒体は、例えばＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＤＶＤ－ＲＯＭ（Digital Versatile Disc Read Only Memory）等である。コンピュータプログラムは、所定のサーバ等からインストールされてもよい。

【００６０】

鍵生成部２２０は、システム鍵を生成する。鍵生成部２２０は、例えば、機微データに適用される暗号方式に応じた鍵を生成してもよい。暗号方式が公開鍵暗号方式、例えば、準同型暗号方式（Paillier方式）の場合は、システム公開鍵とシステム秘密鍵の鍵対を生成する。

【００６１】

また、暗号方式が共通鍵暗号方式、例えば、順序保存暗号方式や、検索可能暗号方式の場合は、ユーザ共通鍵を生成する。このように、システム鍵は、システム公開鍵とシステム秘密鍵の鍵対である場合と、システム共通鍵である場合とがある。なお、鍵生成アルゴリズムは、周知の技術であるので説明を省略する。

【００６２】

（プロキシサーバ３００の機能構成）

図５は、プロキシサーバ３００の機能構成の一例を示す機能ブロック図である。図５を参照して、プロキシサーバ３００の機能構成の一例について説明する。

【００６３】

プロキシサーバ３００は、通信部３０１と、記憶部３０２と、変換部３０３と、制御部３０４と、を備える。

【００６４】

通信部３０１は、複数のデータ提供サーバ１００から、暗号化された機微データを取得する第２の機微データ取得部に相当する。通信部３０１は、データ提供サーバ１００の通信部１０１と同様の機能を有し、プロキシサーバ３００がネットワークＮＷを介してサーバや装置等と所定の通信プロトコルに従って通信を行うための通信インタフェース回路を有する。

【００６５】

また、通信部３０１は、各データ提供サーバ１００から、再暗号化鍵を取得する再暗号化鍵取得部に相当し、取得した再暗号化鍵を、記憶部３０２に記憶させる。

【００６６】

また、通信部３０１は、演算サーバ４００からの要求に応じて、記憶部３０２に記憶される、変換された機微データを送信するようにしてもよいし、機微データが変換されたことに応じて演算サーバ４００に送信するようにしてもよい。

【００６７】
記憶部３０２は、データ提供サーバ１００の記憶部１０３と同様の機能を有する記憶装置であって、プロキシサーバ３００の各種処理に用いられるコンピュータプログラム、データベース、テーブル等が格納される。コンピュータプログラムは、コンピュータ読み取り可能な可搬型記録媒体から公知のセットアッププログラム等を用いて記憶部３０２にインストールされてもよい。
【００６８】
変換部３０３は、データ提供サーバ１００から取得した機微データを、対応する再暗号化鍵を用いて所定の暗号化空間における機微データに変換する。変換部３０３は、取得した機微データの暗号化方式に応じた暗号化方式により暗号化することで変換を行う。例えば、データ提供サーバ１００において準同型暗号方式で暗号化された機微データについては、同じ準同型暗号方式により当該データ提供サーバ１００から取得した再暗号化鍵を用いて再暗号化を行う。また、ＡＥＳで暗号化された機微データについては、同じＡＥＳにより再暗号化鍵を用いて再暗号化を行う。変換部３０３は、変換された機微データを記憶部３０２に記憶（登録）させる。
【００６９】
なお、上述したように、機微データの属性項目の属性値ごとに所定の暗号方式で暗号化されている場合は、当該属性項目の属性値について、当該所定の暗号方式に応じた暗号化を行う。したがって、同一のデータ提供サーバ１００が提供する機微データには、属性項目の属性値のデータ形式によって異なる暗号方式が含まれ得る。例えば、準同型暗号方式で再暗号化された属性値と、ＡＥＳで再暗号化された属性値とが含まれ得る。しかしながら、再暗号化には、鍵管理サーバ２００が管理するシステム鍵に基づいて生成される再暗号化鍵を用いるため、各属性項目の属性値は、所定の暗号方式ごとに、同一の暗号化空間に変換されている。
【００７０】
制御部３０４は、プロキシサーバ３００の各機能を制御し、予め記憶部３０２に記憶されているプログラムに基づいて動作するＣＰＵ（Central Processing Unit）等のプロセッサである。制御部３０４は、演算サーバ４００からの要求に応じて、記憶部３０２から変換された機微データを読み出し、通信部３０１に対して、演算サーバ４００に送信するよう制御する。
【００７１】
（演算サーバ４００の機能構成）
図６は、演算サーバ４００の機能構成の一例を示す機能ブロック図である。図６を参照して、演算サーバ４００の機能構成の一例について説明する。
【００７２】
演算サーバ４００は、通信部４０１と、記憶部４１０と、制御部４２０と、を備える。
【００７３】
通信部４０１は、演算サーバ４００がネットワークＮＷを介して各サーバや装置等と所定の通信プロトコルに従って通信を行うための通信インタフェース回路を有する。通信部４０１は、受信したデータを制御部４２０に送り、また、制御部４２０から受け取ったデータを、ネットワークＮＷを介してサーバや装置等に送信する。なお、通信部４０１は、ネットワークＮＷを介した装置等と、セキュリティが確保されたセキュアな通信チャンネルでデータを送受信する。セキュアな通信チャンネルの構築、通信方法は、周知の技術であるため、説明を省略する。
【００７４】
記憶部４１０は、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等のメモリ装置、ハードディスク等の固定ディスク装置、又はフレキシブルディスク、光ディスク等の可搬用の記憶装置等を有する。また、記憶部４１０は、演算サーバ４００の各種処理に用いられるコンピュータプログラム、データベース、テーブル等が格納される。コンピュータプログラムは、コンピュータ読み取り可能な可搬型記録媒体から公知のセット

アッププログラム等を用いて記憶部４１０にインストールされてもよい。可搬型記録媒体は、例えばＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＤＶＤ－ＲＯＭ（Digital Versatile Disc Read Only Memory）等である。コンピュータプログラムは、所定のサーバ等からインストールされてもよい。

【００７５】

また、記憶部４１０は、通信部４０１がプロキシサーバ３００から受信した、変換された機微データを記憶する。

【００７６】

制御部４２０は、全体制御部４２１と、統合データ生成部４２２と、実行部４２３と、を有する。全体制御部４２１は、演算サーバ４００の各機能を制御し、予め記憶部４１０に記憶されているプログラムに基づいて動作するＣＰＵ（Central Processing Unit）等のプロセッサである。なお、全体制御部４２１として、ＤＳＰ（digital signal processor）等が用いられてもよい。また、全体制御部４２１として、ＬＳＩ（large scale integration）、ＡＳＩＣ（Application Specific Integrated Circuit）、ＦＰＧＡ（Field-Programmable Gate Array）等の制御回路が用いられてもよい。

【００７７】

統合データ生成部４２２は、全体制御部４２１の制御により、通信部４０１を介してプロキシサーバ３００から受信し、記憶部４１０に記憶される変換された機微データを、機微データに属性項目として含まれる識別子（図８～図１１（後述）の例では共通ＩＤ）に基づいて統合して統合データを生成する。そして、統合データ生成部４２２は、生成した統合データを記憶部４１０に記憶させる。

【００７８】

実行部４２３は、変換された機微データに基づいて秘密計算を実行する。そして、実行部４２３は、実行結果を記憶部４１０に記憶させる。ここで、実行部４２３が実行する秘密計算とは、機械学習によるモデル学習および推論であって、統計的手法もしくは深層学習等の解析アルゴリズムが用いられてもよい。実行部４２３は、１つのデータ提供サーバ１００により提供された機微データについて秘密計算を実行してもよいし、統合データ生成部４２２が生成した統合データについて秘密計算を実行してもよい。統合された機微データは、上述のように、属性項目ごとに、準同型暗号方式、順序保存暗号方式や、検索可能暗号方式、暗号文上で完全一致が可能なＡＥＳ暗号等により、所定の暗号化空間における機微データに変換されているので、例えば、属性項目に対して、加減乗除に関する計算、検索、分析に関する計算である演算を暗号化状態のまま実行することができる。

【００７９】

（端末装置５００の機能構成）

図７は、端末装置５００の機能構成の一例を示す機能ブロック図である。図７を参照して、端末装置５００の機能構成の一例について説明する。

【００８０】

端末装置５００は、通信部５０１と、記憶部５０２と、入力部５０３と、出力部５０４と、制御部５０５と、を備える。端末装置５００は、上述したように、例えば、プラットフォーム（データ共有システム１）に参加する組織に所属するユーザが操作する情報処理装置であってもよい。

【００８１】

通信部５０１は、データ提供サーバ１００の通信部１０１と同様の機能を有し、端末装置５００がネットワークＮＷを介してサーバや装置等と所定の通信プロトコルに従って通信を行うための通信インタフェース回路を有する。通信部５０１は、受信したデータを制御部５０５に送り、また、制御部５０５から受け取ったデータを、ネットワークＮＷを介してサーバや装置等に送信する。また、端末装置５００を操作するユーザは、機微データに対する秘密計算の実行結果を利用する権限を有しており、鍵管理サーバ２００から、通信部５０１を介して、実行結果を復号できるシステム鍵（システム秘密鍵および／またはシステム共通鍵）を取得する。

【００８２】
記憶部５０２は、データ提供サーバ１００の記憶部１０３と同様の機能を有する記憶装置であって、端末装置５００の各種処理に用いられるコンピュータプログラム、データベース、テーブル等が格納される。コンピュータプログラムは、コンピュータ読み取り可能な可搬型記録媒体から公知のセットアッププログラム等を用いて記憶部５０２にインストールされてもよい。また、記憶部５０２は、演算サーバ４００から秘密計算の実行結果を復号するためのシステム鍵を記憶するようにしてもよい。
【００８３】
入力部５０３は、端末装置５００のユーザ入力を受け付けるインタフェースである。入力部５０３は、例えば、キーボードや、タッチパネル、音声入力を検出するマイクであるが、これらに限られない。ユーザは、入力部５０３を介して、データ処理の処理要求を入力する。
【００８４】
出力部５０４は、情報を出力してユーザに通知するインタフェースである。出力部５０４は、例えば、ディスプレイや、音声出力するスピーカであるが、これらに限られない。出力部５０４は、データ処理の実行結果をディスプレイに表示する等してユーザに提供する。
【００８５】
制御部５０５は、端末装置５００の各機能を制御し、予め記憶部５０２に記憶されているプログラムに基づいて動作するＣＰＵ（Central Processing Unit）等のプロセッサである。制御部５０５は、入力部５０３により入力されたデータ処理の処理要求を、通信部５０１を介して演算サーバ４００に送信する。また、制御部５０５は、通信部５０１を介して、秘密計算の実行結果を取得する。制御部５０５は、秘密計算の実行結果を、記憶部５０２に記憶されたシステム鍵により復号し、実行結果を取得する。
【００８６】
図８は、機微データのデータ構造の一例を示した図である。本実施形態において、機微データは、個人に関する情報であって、年齢、性別、収入、居住地域、購買情報などの属性項目（カラム：列）の属性値（文字列又は数値）である。また、機微データは、統合キーとして、個人を一意に特定できる識別子（共通ＩＤ）を属性項目として含んでよい。識別子は、数値、文字列またはそれらの組み合わせであってよい。なお、図８において、説明を簡略化するため、所定の属性項目を示しているが、これに加え、図示しない属性項目を機微データに含ませてもよい。また、機微データは、個人に関する情報に限られず、ＩｏＴ・ＮＷ機器、産業用機器などのシステムに関する機密情報（センシングデータやログデータ等）であってもよい。また、統合キーは個人を一意に特定できる識別子に限られず、複数のテーブルにおけるデータを一意に特定できる値であれば、任意の値を用いてもよい。
【００８７】
図８において、属性項目の属性値が格納されたテーブルＴ１，Ｔ２，Ｔ３が示されている。テーブルＴ１は、データ提供サーバ１００－１が提供する機微データ（すなわち、会社Ａが保有するデータ）を示している。テーブルＴ１において、機微データは、属性項目として、個人を一意に特定する識別子である「共通ＩＤ」、個人の年齢を示す「年齢」、個人の性別を示す「性別」、個人の収入を示す「収入」、個人の商品１に対する購買の有無を示す「購買フラグ１」を含む。テーブルＴ１において、属性項目「共通ＩＤ」，「年齢」，「収入」，「購買フラグ１」の属性値は数値である。なお、図８において「性別」の属性値はカテゴリ（文字列）であるが、性別と数値を対応させる等して、カテゴリを数値で表すようにしてもよい。
【００８８】
テーブルＴ１において、属性項目「共通ＩＤ」に対し属性値「１２３４５」、属性項目「年齢」に対し属性値「４５」、属性項目「性別」に対し属性値「女」、属性項目「収入」に対し属性値「４５０」、属性項目「購買フラグ１」に対し属性値「１」が格納されて

いる。これは、共通ＩＤが１２３４５である個人は、年齢が４５歳、性別が女、収入が４５０（万円）、商品１を購入済み、ということを意味している。同様に、属性項目「共通ＩＤ」の属性値「６７８９０」，「２３４５６」，「９０１２３」，「８９０１２」，「３４５６７」についても、各属性項目に対し属性値が格納される。

【００８９】

テーブルＴ２は、データ提供サーバ１００－２が提供する機微データ（すなわち、会社Ｂが保有するデータ）を示している。データ提供サーバ１００－２は、テーブルＴ１で示される機微データを保有する会社Ａとは異なる属性項目を含む機微データを提供する。

【００９０】

テーブルＴ２において、機微データは、属性項目として、個人を一意に特定する識別子である「共通ＩＤ」、個人の居住する地域を示す「居住地域」、個人の商品２に対する購買の有無を示す「購買フラグ２」，個人の商品３に対する購買の有無を示す「購買フラグ３」を含む。テーブルＴ２において、属性項目「共通ＩＤ」，「購買フラグ２」，「購買フラグ３」の属性値は数値であり、属性項目「居住地域」の属性値は文字列である。なお、図８において「居住地域」の属性値はカテゴリ（文字列）であるが、地域と数値を対応させる等して、カテゴリを数値で表すようにしてもよい。例えば、テーブルＴ２において、属性項目「共通ＩＤ」に対し属性値「６７８９０」、属性項目「居住地域」に対し属性値「東京」、属性項目「購買フラグ２」に対し属性値「１」、属性項目「購買フラグ３」に対し属性値「０」が格納されている。これは、共通ＩＤが６７８９０である個人は、居住する地域が東京、商品２を購入済み、商品３は未購入、ということを意味している。同様に、属性項目「共通ＩＤ」の属性値「２３４５６」，「８９０１２」，「１２３４５」，「９０１２３」，「３４５６７」についても、各属性項目に対し属性値が格納される。

【００９１】

テーブルＴ１とテーブルＴ２とでは、「共通ＩＤ」以外の属性項目は異なっているが、同一の「共通ＩＤ」で示されるレコードは同一の個人に対応する。例えば、テーブルＴ１の「共通ＩＤ」の属性値「６７８９０」によって特定されるレコード（個人）は、テーブルＴ２の「共通ＩＤ」の属性値「６７８９０」によって特定されるレコード（個人）と同一である。

【００９２】

テーブルＴ３は、データ提供サーバ１００－３が提供する機微データ（会社Ｃが保有するデータ）を示している。データ提供サーバ１００－３は、テーブルＴ１およびＴ２で示される機微データを保有する会社Ａおよび会社Ｂとは異なる機微データを提供する。

【００９３】

テーブルＴ３において、機微データは、属性項目として、個人を一意に特定する識別子である「共通ＩＤ」、配偶者の有無を示す「配偶者フラグ」、扶養家族の人数を示す「扶養人数」、個人の商品４に対する購買の有無を示す「購買フラグ４」を含む。テーブルＴ３において、属性項目「共通ＩＤ」，「配偶者フラグ」，「扶養人数」，「購買フラグ４」の属性値は数値である。例えば、テーブルＴ３において、属性項目「共通ＩＤ」に対し属性値「２３４５６」、属性項目「配偶者フラグ」に対し属性値「１」、属性項目「扶養人数」に対し属性値「３」、属性項目「購買フラグ４」に対し属性値「１」が格納されている。これは、共通ＩＤが２３４５６である個人は、配偶者を有し、扶養人数は３人であり、商品４を購入済み、ということを意味している。同様に、属性項目「共通ＩＤ」の属性値「９０１２３」，「５６７８９」，「３４５６７」，「７８９０１」，「１２３４５」についても、各属性項目に対し属性値が格納される。

【００９４】

テーブルＴ３と、テーブルＴ１及びＴ２とでは、「共通ＩＤ」以外の属性項目は異なっている。また、属性項目「共通ＩＤ」の属性値は、テーブルＴ３にのみ「５６７８９」および「７８９０１」が含まれている。すなわち、各テーブルには、同一のレコードの群ではなく、テーブルごとに異なるレコードを含む群であってもよい。なお、本実施形態においては、図８で示したように、各データ提供サーバが提供する機微データに含まれる属性

項目は、「共通ＩＤ」（識別子）以外は異なるものとしているが、他の実施形態として、同じ属性項目を含んでいてもよい。その場合、統合データとしてどのデータ提供サーバが提供する属性値を優先するかは、システム管理者等が適宜設定して決定することができる。

【００９５】

図９は、暗号化された機微データのデータ構造の一例を示す図である。図９において、「共通ＩＤ」以外の属性項目の属性値が暗号化されたテーブルＴ１ｅ，Ｔ２ｅ，Ｔ３ｅが示されている。

【００９６】

テーブルＴ１ｅは、データ提供サーバ１００－１（会社Ａ）が管理するユーザ鍵（ユーザ公開鍵またはユーザ共通鍵）に基づいて、テーブルＴ１の「共通ＩＤ」以外の属性値が暗号化されている。例えば、属性値が数値である属性項目「年齢」，「収入」，「購買フラグ１」については、準同型暗号方式および／または順序保存暗号方式で暗号化し、属性値が文字列である属性項目「性別」については、検索可能暗号方式で暗号化する。なお、テーブルＴ１ｅにおいて、説明を簡単にするため、属性値が数値のデータは、例えば、準同型暗号方式で暗号化された値を示している（以下、テーブルＴ２ｅ，Ｔ３ｅにおいても同様）。

【００９７】

テーブルＴ２ｅは、データ提供サーバ１００－２（会社Ｂ）が管理するユーザ鍵（ユーザ公開鍵またはユーザ共通鍵）に基づいて、テーブルＴ２の「共通ＩＤ」以外の属性値が暗号化されている。例えば、属性値が数値である属性項目「購買フラグ２」，「購買フラグ３」については、準同型暗号方式および／または順序保存暗号方式で暗号化し、属性値が文字列である属性項目「居住地域」については、検索可能暗号方式で暗号化する。

【００９８】

また、テーブルＴ３ｅは、データ提供サーバ１００－３（会社Ｃ）が管理するユーザ鍵（ユーザ公開鍵またはユーザ共通鍵）に基づいて、テーブルＴ３の「共通ＩＤ」以外の属性値が暗号化されている。例えば、属性値が数値である属性項目「配偶者フラグ」，「扶養人数」，「購買フラグ４」については、準同型暗号方式および／または順序保存暗号方式で暗号化する。

【００９９】

プロキシサーバ３００は、データ提供サーバ１００－１から暗号化された機微データとしてテーブルＴ１ｅを取得する。そして、データ提供サーバ１００－１に対応する再暗号化鍵でテーブルＴ１ｅの属性項目の暗号方式に応じた暗号方式で暗号化を行う。例えば、属性値が数値である属性項目「年齢」，「収入」，「購買フラグ１」については、準同型暗号方式や順序保存暗号方式等で暗号化されているため、同様に、再暗号化鍵（ユーザ秘密鍵およびシステム公開鍵に基づいて生成された鍵）を用いてそれぞれ準同型暗号方式や順序保存暗号方式等で暗号化する。また、属性値が文字列である属性項目「性別」については、ＡＥＳや検索可能暗号方式等で暗号化されているため、同様に、再暗号化鍵（ユーザ共通鍵およびシステム共通鍵に基づいて生成された鍵）を用いてＡＥＳや検索可能暗号方式等で暗号化する。

【０１００】

プロキシサーバ３００は、テーブルＴ１ｅと同様に、テーブルＴ２ｅ及びＴ３ｅについても再暗号化鍵で暗号化を行う。

【０１０１】

図１０は、統合データのデータ構造の一例を示す図である。図１０において、統合テーブルＴｍは、図９で示したテーブルＴ１ｅ，Ｔ２ｅ，Ｔ３ｅを再暗号化したテーブルに含まれる属性項目「共通ＩＤ」の属性値（識別子）を統合キーとして、統合されたテーブルである。すなわち、統合データは、属性項目として「共通ＩＤ」，「年齢」，「性別」，「収入」，「購買フラグ１」，「居住地域」，「購買フラグ２」，「購買フラグ３」，「配偶者フラグ」，「扶養人数」，「購買フラグ４」を含むテーブルであって、「共通ＩＤ

」以外の各属性項目の属性値は、図９において上述したように、再暗号化鍵により暗号化されている。

【０１０２】

統合テーブルＴｍにおいて、属性項目「年齢」，「性別」，「収入」，「購買フラグ１」（カラム）は、データ提供サーバ１００－１（会社Ａ）が提供する機微データである。属性項目「居住地域」，「購買フラグ２」，「購買フラグ３」（カラム）は、データ提供サーバ１００－２（会社Ｂ）が提供する機微データである。属性項目「配偶者フラグ」，「扶養人数」，「購買フラグ４」（カラム）は、データ提供サーバ１００－３（会社Ｃ）が提供する機微データである。

【０１０３】

テーブルＴ３に含まれ、テーブルＴ１およびＴ２には含まれていない「共通ＩＤ」の属性値「５６７８９」および「７８９０１」については、テーブルＴ１およびＴ２に含まれる属性項目の属性値は、ブランク（NULL）またはダミーの数値を格納するなど、演算サーバ４００の管理者等が適宜決定してもよい。または、統合データの属性項目「共通ＩＤ」以外の属性値が格納されていないレコードについては削除するようにしてもよい。

【０１０４】

すなわち、図１０の例では、図９のテーブルＴ１ｅ，Ｔ２ｅ，Ｔ３ｅの属性項目「共通ＩＤ」を統合キーとして、横方向へテーブルを統合（「属性項目」（カラム）の追加）及び、縦方向へのテーブルの統合（「レコード」の追加）を含む統合処理が行われている。

【０１０５】

属性項目「年齢」，「収入」，「購買フラグ１」，「購買フラグ２」，「購買フラグ３」，「配偶者フラグ」，「扶養人数」，「購買フラグ４」の属性値は、再暗号化鍵（ユーザ秘密鍵およびシステム公開鍵に基づいて生成された鍵）により準同型暗号方式や順序保存暗号方式等で暗号化され、同一の暗号化空間に変換されている。また、属性項目「性別」，「居住地域」の属性値は、再暗号化鍵（ユーザ共通鍵およびシステム共通鍵に基づいて生成された鍵）によりＡＥＳや検索可能暗号方式等で暗号化され、同一の暗号化空間に変換されている。これにより、演算サーバ４００では、同一の暗号化空間に変換された属性値について、秘密計算を実行することができる。なお、完全準同型暗号を活用する場合は、再暗号化鍵はデータ提供サーバ１００にてユーザ公開鍵情報およびユーザ秘密鍵情報に基づいて生成することができる。

【０１０６】

図１１は、実施形態１に係る処理の一例を示すフローチャートである。図１１を参照して、プラットフォーム（データ共有システム１）に参加する各組織が提供する機微データを、プロキシサーバ３００が再暗号化して所定の暗号化空間に変換し、秘密計算によりデータ処理される流れについて説明する。処理の流れは一例であり、図１１で示す順序に限られない。なお、以下では、説明を簡略にするため、暗号化された機微データを所定の暗号化空間に変換する方式は、公開鍵暗号方式をベースとした方式で説明する。

【０１０７】

ステップＳ１０１において、データ共有システム１では、鍵生成処理が実行される。鍵管理サーバ２００は、システム鍵（システム公開鍵とシステム秘密鍵の鍵対）を生成する。また、データ提供サーバ１００は、ユーザ鍵（ユーザ公開鍵とユーザ秘密鍵の鍵対）を生成する。さらに、データ提供サーバ１００は、鍵管理サーバ２００で生成されたシステム公開鍵を取得し、ユーザ秘密鍵およびシステム公開鍵に基づいて、再暗号化鍵を生成する。なお、完全準同型暗号を活用する場合は、再暗号化鍵は、基本的にユーザ公開鍵及びユーザ秘密鍵の生成を行うデータ提供サーバ１００で生成され、鍵管理サーバ２００は生成を行わない（当該鍵生成の委託を受けた場合はその限りでない）。鍵管理サーバ２００は、データ提供サーバ１００で生成された当再暗号化鍵を受け取り、必要に応じて鍵管理サーバ２００で管理を行う。

【０１０８】

ステップＳ１０２において、データ提供サーバ１００は、プラットフォームに参加する

組織等から取得した機微データを、ユーザ公開鍵を用いて所定の暗号方式で暗号化する。図１１では、例えば、準同型暗号方式で暗号化する。データ提供サーバ１００は、暗号化した機微データおよび再暗号化鍵をプロキシサーバ３００に送信する。

【０１０９】

ステップＳ１０３において、プロキシサーバ３００は、データ提供サーバ１００から受信した機微データを、当該データ提供サーバ１００から受信した再暗号化鍵で暗号化して、所定の暗号化空間における機微データに変換する。図１１の例では、ステップＳ１０２において、機微データは、準同型暗号方式により暗号化されているので、プロキシサーバ３００は、当該機微データの暗号方式に応じた準同型暗号方式により再暗号化鍵で暗号化する。

【０１１０】

ステップＳ１０４において、演算サーバ４００は、プロキシサーバ３００から変換された機微データを取得する。演算サーバ４００は、例えば、端末装置５００からのデータ処理要求に応じて、処理対象の機微データを送信するようプロキシサーバ３００に要求するようにしてもよい。プロキシサーバ３００は、演算サーバ４００の要求に応じ、所定の暗号化空間に変換された、処理対象の機微データを演算サーバ４００に送信する。

【０１１１】

ステップＳ１０５において、演算サーバ４００は、端末装置５００のデータ処理要求に応じた秘密計算を実行する。演算サーバ４００は、例えば、複数の機微データを統合して統合データを生成し、統合データについて機械学習によるモデル学習および推論を行う。なお、モデル学習等は、１つのデータ提供サーバ１００から提供された機微データに基づいて実行されてもよい。演算サーバ４００は、秘密計算の実行結果を、データ処理の要求をした端末装置５００に送信する。

【０１１２】

ステップＳ１０６において、端末装置５００は、秘密計算の実行結果をシステム秘密鍵により復号する。これにより、端末装置５００は、復号された実行結果を平文データとして利用することができる。なお、端末装置５００は、実行結果を利用する権限を有するユーザとして、鍵管理サーバ２００からシステム秘密鍵を予め付与されていてもよいし、データ処理要求の際に、認証されたユーザとしてシステム秘密鍵を取得させてもよい。以上のようにして、データ共有システム１では、データ処理が行われる。

【０１１３】

（ハードウェア構成図）

図１２は、プロキシサーバ３００のハードウェア構成を示すブロック図である。プロキシサーバ３００は、コンピュータ１００１に実装される。コンピュータ１００１は、ＣＰＵ１００２と、主記憶装置１００３と、補助記憶装置１００４と、インタフェース１００５と、を備える。

【０１１４】

プロキシサーバ３００の各構成要素の動作は、プログラムの形式で補助記憶装置１００４に記憶されている。ＣＰＵ１００２は、プログラムを補助記憶装置１００４から読み出して主記憶装置１００３に展開し、当該プログラムに従って上記処理を実行する。また、ＣＰＵ１００２は、プログラムに従って、記憶領域を主記憶装置１００３に確保する。当該プログラムは、具体的には、コンピュータ１００１に、データ処理を行わせるプログラムである。

【０１１５】

なお、補助記憶装置１００４は、一時的でない有形の媒体の一例である。一時的でない有形の媒体の他の例としては、インタフェース１００５を介して接続される磁気ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、半導体メモリ等が挙げられる。また、このプログラムがネットワークを介してコンピュータ１００１に配信される場合、配信を受けたコンピュータ１００１が当該プログラムを主記憶装置１００３に展開し、処理を実行してもよい。

【０１１６】
また、当該プログラムは、前述した機能の一部を実現するためのものであってもよい。さらに、当該プログラムは、前述した機能を補助記憶装置１００４に既に記憶されている他のプログラムとの組み合わせで実現するもの、いわゆる差分ファイル（差分プログラム）であってもよい。なお、図１２に示したハードウェア構成は、データ提供サーバ１００，鍵管理サーバ２００，演算サーバ４００および端末装置５００も同様の構成としてもよい。これらの装置における各構成要素の動作も、上述のプロキシサーバ３００と同様に、補助記憶装置に記憶されたプログラムに従ったＣＰＵにより実現する。
【０１１７】
（効果の説明）
上述したように、本実施形態に係るデータ共有システムは、暗号データを同一の暗号化空間に変換するためのシステム鍵を管理する鍵管理サーバを備える。また、当該システムに参加する各組織等に対応するデータ提供サーバは、システム鍵とは異なる、当該組織に対応するユーザ鍵を用いて機微データを所定の暗号方式で暗号化し、プロキシサーバに送信する。プロキシサーバは、取得した暗号化された機微データを、ユーザ鍵とシステム鍵とに基づいて生成された再暗号化鍵に基づいて、所定の暗号化空間に変換する。そして、演算サーバは、変換された機微データに基づいて秘密計算を実行する。
【０１１８】
これにより、再暗号化鍵に基づいて所定の暗号化空間に変換された機微データに対する秘密計算の実行結果は、システム鍵により復号することができる。したがって、各データ提供サーバが保有する機微データの内容を他者に開示する（復号する）ことなく、データ処理を行うことができる。また、プロキシサーバと演算サーバとを備えることにより、機械学習やディープラーニング等のアルゴリズムやデータマイニングを秘密計算で実行する際に、プロキシサーバと演算サーバとが部分的に通信しながら協調して秘密計算を行うことができるようになるため、実行パフォーマンスを向上させることができる。
【０１１９】
また、本実施形態に係るデータ共有システムは、秘密計算の実行結果を復号することができるシステム鍵（システム秘密鍵および／またはシステム共有鍵）を鍵管理サーバで管理する。秘密計算の実行結果を利用する権限を実行する際に、各データ提供サーバの協力を必要とすることなく、鍵管理サーバで管理するシステム鍵の付与により行うことができるため、権限の管理が容易である。また、実行結果を利用するために各データ提供サーバの協力が必要となる場合よりも処理を高速に行うことができる。
【０１２０】
また、本実施形態に係るデータ共有システムは、暗号方式が異なる（例えば、暗号化状態のまま検索が可能な方式と、加算乗算が可能な準同型暗号方式など）属性値を含む機微データについて秘密計算を実行する。これにより、機微データについて、暗号化状態のまま、統計的手法もしくは、機械学習・深層学習等の解析アルゴリズムによるモデル学習および推論を行うことができ、セキュアに機微データを活用することができる。
【０１２１】
また、本実施形態に係るデータ共有システムは、変換された機微データを統合して、秘密計算を実行する。これにより、データ共有システムに参加する組織は、自組織が保有する機微データを、他組織に開示することなく統合データとして容易に利活用することができる。また、複数の組織から提供される機微データについてデータ処理を実行することができるため、モデル学習および推論の精度を向上させることができる。
【０１２２】
＜実施形態２＞
本実施形態では、プロキシサーバが、標準実行環境から保護される仮想実行環境を構築し、当該仮想実行環境において、各データ提供サーバにおいて暗号化された機微データを復号後、同一の暗号化空間に変換する。
【０１２３】

実施形態２に係るデータ共有システム２は、実施形態１に係るデータ共有システム１のデータ提供サーバ１００およびプロキシサーバ３００に代えて、データ提供サーバ６００およびプロキシサーバ７００を備える点で異なる。

【０１２４】

図１３は、実施形態２に係る処理の概念図である。図１３を参照して、データ共有システム２における処理の概要について説明する。

【０１２５】

実施形態２に係るプロキシサーバ７００は、標準実行環境から保護される仮想実行環境を構築し、当該仮想実行環境において、各データ提供サーバ６００において暗号化された機微データを復号後、同一の暗号化空間に変換する。仮想実行環境は、認証もしくは許可されたユーザしか標準実行環境からアクセスすることができない環境である。認証や許可は、予め条件が定義されている場合は自動的に行われ、定義されていない場合は、アクセスするごとに認証や許可に関する処理が行われるようにしてもよい。また、仮想実行環境は、標準実行環境から信頼された環境であってもよい。また、仮想実行環境は、短時間の構築であることが好ましい。これにより、仮想実行環境がサイバー攻撃を受けても、時間的にセキュリティ突破することが困難であるため、セキュリティ上の安全性を担保することができる。

【０１２６】

データ提供サーバ６００は、ユーザ鍵を生成し、ユーザ鍵により機微データを暗号化する。データ提供サーバ６００－１は、例えば、ユーザ公開鍵pk1およびユーザ秘密鍵sk1の鍵対を生成し、機微データＭ１を、ユーザ公開鍵pk1を用いて、任意の（公開鍵）暗号方式により暗号化する。データ提供サーバ６００－２は、例えば、ユーザ共通鍵ck2を生成し、機微データＭ２を、ユーザ共通鍵ck2を用いて、任意の（共通鍵）暗号方式により暗号化する。

【０１２７】

すなわち、各データ提供サーバ６００は、ユーザ鍵として、ユーザ公開鍵およびユーザ秘密鍵の鍵対、および／または、ユーザ共通鍵を生成する。また、機微データに含まれるデータ形式等に応じた暗号方式で暗号化してもよい。各データ提供サーバ６００は、機微データを復号することができる鍵（ユーザ秘密鍵、ユーザ共通鍵）をセキュアな経路を介してプロキシサーバ７００に送信する。

【０１２８】

鍵管理サーバ２００は、機微データを、所定の暗号化空間に変換するのに用いるシステム鍵を生成する。システム鍵は、システム公開鍵Pkxおよびシステム秘密鍵Skxの鍵対、および／または、システム共通鍵Ckx（不図示）であってよい。鍵管理サーバ２００は、プロキシサーバ７００にシステム鍵（システム公開鍵Pkxおよび／またはシステム共通鍵Ckx）を送信する。

【０１２９】

プロキシサーバ７００は、標準実行環境から保護される仮想実行環境を構築し、仮想実行環境において、ユーザ鍵を用いて暗号文Ｍを復号し、機微データＭを生成する。そして、復号された機微データについて、システム鍵を用いて、秘密計算が実行可能な暗号化方式で暗号化を行い、再暗号化文Ｍを生成する。例えば、システム公開鍵Pkxを用いて、準同型暗号方式により暗号化してもよいし、システム共通鍵Ckxを用いて、検索可能暗号方式により暗号化してもよい。また、機微データに含まれるデータ形式等に応じた暗号方式で暗号化してもよい。

【０１３０】

例えば、データ提供サーバ６００－１から送信された暗号文Ｍ１は、ユーザ秘密鍵sk1によって復号され、平文の機微データＭ１となる。次いで、システム公開鍵Pkxによって暗号化され、再暗号化文Ｍ１に変換される。また、例えば、データ提供サーバ６００－２から送信された暗号文Ｍ２は、ユーザ共通鍵ck2によって復号され、平文の機微データＭ２となる。次いで、システム公開鍵Pkxによって暗号化され、再暗号化文Ｍ２に変換され

る。
【０１３１】
演算サーバ４００は、再暗号化文Mについて秘密計算を実行する。複数の再暗号化文M１，M２…を図８～１１で述べたように、統合して統合データを生成し、統合データについて秘密計算を実行するようにしてもよい。
【０１３２】
秘密計算の実行結果は、システム鍵で復号することができる。例えば、システム公開鍵Pkxで暗号化された機微データに対する秘密計算の実行結果は、システム秘密鍵Skxで復号することができる。また、例えば、システム共通鍵Ckxで暗号化された機微データに対する秘密計算の実行結果は、システム共通鍵Ckxで復号することができる。
【０１３３】
標準実行環境から保護される仮想実行環境は、認証されないユーザからのアクセスを防ぐことができるため、暗号化された機微データを所定の暗号化空間に変換する処理を、セキュアに実行することができる。また、復号した機微データを所定の暗号方式で暗号化して所定の暗号化空間に変換するので、処理効率よくデータ処理を実行することができる。また、仮想実行環境は、短時間の構築であることが好ましい。これにより、仮想実行環境がサイバー攻撃を受けても、時間的にセキュリティ突破することが困難であるため、セキュリティ上の安全性を担保することができる。
【０１３４】
（データ提供サーバ６００の機能構成）
図１４は、データ提供サーバ６００の機能構成の一例を示す機能ブロック図である。図１４を参照して、データ提供サーバ６００の機能構成の一例について説明する。
【０１３５】
データ提供サーバ６００は、通信部６０１と、制御部６０２と、記憶部６０３と、鍵生成部６０４と、暗号化部６０５と、を備える。
【０１３６】
通信部６０１は、通信部１０１と同様の機能を有する。通信部６０１は、ネットワークNWを介した装置やローカルに接続された装置等と、セキュリティが確保されたセキュアな通信チャンネルでデータを送受信する。セキュアな通信チャンネルの構築、通信方法は、共通鍵（セッション鍵など）や公開鍵等を用いた周知の技術であるため、説明を省略する。
【０１３７】
制御部６０２は、制御部１０２と同様の機能を有し、データ提供サーバ６００の各機能を制御する。
【０１３８】
記憶部６０３は、記憶部１０３と同様の機能を有し、データ提供サーバ６００の各種処理に用いられるコンピュータプログラム、暗号プログラム、鍵等が格納される。
【０１３９】
鍵生成部６０４は、ユーザ鍵を生成する。ユーザ鍵は、ユーザ公開鍵とユーザ秘密鍵の鍵対、および／または、ユーザ共通鍵を含む。鍵生成部６０４は、例えば、暗号化部６０５の要求する暗号方式に応じた鍵を生成してもよい。ユーザ鍵は、通信部６０１を介して、セキュアな通信チャンネルを通して、プロキシサーバ７００に送信される。
【０１４０】
暗号化部６０５は、暗号化部１０５と同様の機能を有し、システム鍵とは異なるユーザ鍵を用いて機微データを所定の暗号方式で暗号化する。暗号化された機微データは、通信部６０１を介して、プロキシサーバ７００に送信される。
【０１４１】
（プロキシサーバ７００の機能構成）
図１５は、プロキシサーバ７００の機能構成の一例を示す機能ブロック図である。図１５を参照して、プロキシサーバ７００の機能構成の一例について説明する。

【０１４２】
プロキシサーバ７００は、通信部７０１と、記憶部７０２と、制御部７０３と、変換部７０４と、を備える。
【０１４３】
通信部７０１は、複数のデータ提供サーバ１００から、暗号化された機微データを取得する。また、通信部７０１は、鍵管理サーバ２００から、システム鍵（システム公開鍵および／またはシステム共通鍵）およびユーザ鍵（ユーザ秘密鍵および／またはユーザ共通鍵）を取得し、記憶部７０２に格納する。
【０１４４】
記憶部７０２は、プロキシサーバ３００の各種処理に用いられるコンピュータプログラム、データベース等が格納される。
【０１４５】
制御部７０３は、仮想実行環境構築部７１１と、仮想実行環境廃棄部７１２と、を有し、データ提供サーバ１００から取得した機微データを所定の暗号化空間に変換するための仮想実行環境を構築するよう制御する。
【０１４６】
仮想実行環境構築部７１１は、仮想実行環境を構築する。例えば、暗号化された機微データを受信するごとに仮想実行環境を構築するようにしてもよいし、演算サーバ４００からの要求に応じて、仮想実行環境を構築するようにしてもよい。仮想実行環境には、例えば、ＯＳ（不図示）が搭載され、当該ＯＳは、変換部７０４を備える。
【０１４７】
仮想実行環境廃棄部７１２は、上述の仮想実行環境を廃棄する（消滅させる）。仮想実行環境廃棄部７１２は、例えば、仮想実行環境を表す所定のデータを削除することで、仮想実行環境を廃棄する。仮想実行環境の廃棄は、例えば、機微データを所定の暗号化空間に変換した後に実行されてもよいし、認証したユーザからの指示に基づいて実行されてもよい。
【０１４８】
変換部７０４は、取得部７２１と、復号部７２２と、暗号化部７２３と、提供部７２４と、を含む。
【０１４９】
取得部７２１は、仮想実行環境データ取得部および仮想実行環境鍵取得部に相当し、記憶部７０２から暗号化された機微データおよび当該機微データに対応するユーザ鍵ならびにシステム鍵を取得する。
【０１５０】
復号部７２２は、暗号化された機微データを、当該機微データを暗号化したデータ提供サーバ６００に対応するユーザ鍵によって復号する。
【０１５１】
暗号化部７２３は、仮想実行環境変換部に相当し、復号された機微データをシステム鍵で暗号化する。暗号化部７２３は、暗号化された機微データの暗号方式に応じた暗号化を行う。例えば、データ提供サーバ１００において準同型暗号方式で暗号化された機微データについては、同じ準同型暗号方式により鍵管理サーバ２００から取得したシステム鍵を用いて再暗号化を行う。また、ＡＥＳで暗号化された機微データについては、同じＡＥＳによりシステム鍵を用いて再暗号化を行う。
【０１５２】
また、暗号化部７２３は、暗号化された機微データの処理目的に応じた暗号方式により暗号化してもよい。例えば、機微データについて高度なアルゴリズム計算処理を行う場合は、暗号化部７２３は、保管や簡易計算・検索等を目的とするのに適した暗号化方式で暗号化された機微データについて、高度なアルゴリズム計算処理を目的とするのに適した暗号化方式により再暗号化鍵を用いて再暗号化を行うようにしてもよい。より具体的には、順序保存暗号方式により暗号化された機微データについては、準同型暗号方式により再暗

号化するようにしてもよい。また、準同型暗号方式により暗号化された機微データについては、完全準同型暗号方式により再暗号化するようにしてもよい。なお、暗号化部７２３は、機微データのデータ形式（文字列や数字）等に応じた暗号方式で暗号化することで、機微データを所定の暗号化空間に変換してもよい。

【０１５３】

提供部７２４は、暗号化部７２３により所定の暗号化空間に変換された機微データを、標準実行環境等に提供する。例えば、変換された機微データは、記憶部７０２に格納される。

【０１５４】

また、復号部７２２が暗号化された機微データを復号する際に用いたユーザ鍵は、仮想実行環境廃棄部７１２が仮想実行環境を廃棄する際に廃棄するようにしてもよい。

【０１５５】

図１６は、実施形態２に係る処理の一例を示すフローチャートである。図１６を参照して、プラットフォーム（データ共有システム２）に参加する各組織が提供する機微データを、仮想実行環境で復号後に所定の暗号化空間に変換し、秘密計算によりデータ処理される流れについて説明する。処理の流れは一例であり、図１６で示す順序に限られない。なお、以下では、説明を簡略にするため、暗号化された機微データを所定の暗号化空間に変換する方式は、公開鍵暗号方式をベースとした方式で説明する。

【０１５６】

ステップＳ２０１において、データ共有システム２では、鍵生成処理が実行される。鍵管理サーバ２００は、システム鍵（システム公開鍵とシステム秘密鍵の鍵対）を生成し、システム公開鍵をプロキシサーバ７００に送信する。また、データ提供サーバ６００は、ユーザ鍵（ユーザ公開鍵とユーザ秘密鍵の鍵対またはユーザ共通鍵）を生成する。

【０１５７】

ステップＳ２０２において、データ提供サーバ６００は、プラットフォームに参加する組織等から取得した機微データを、ユーザ鍵を用いて所定の暗号方式で暗号化する。例えば、準同型暗号方式によりユーザ公開鍵を用いて暗号化してもよいし、ＡＥＳによりユーザ共通鍵を用いて暗号化してもよい。データ提供サーバ６００は、暗号化した機微データおよび当該機微データを復号するユーザ鍵（ユーザ秘密鍵および／またはユーザ共通鍵）をプロキシサーバ７００に送信する。

【０１５８】

ステップＳ２０３において、プロキシサーバ７００は、仮想実行環境を構築する。そして、データ提供サーバ６００から受信した機微データを、構築した仮想実行環境において、当該データ提供サーバ６００のユーザ鍵で復号後、システム公開鍵を用いて所定の暗号化空間における機微データに変換する。より具体的には、プロキシサーバ７００は、機微データを、例えば、暗号化状態のまま数値計算等を行うことができる準同型暗号方式や、順序保存暗号方式等により暗号化する。プロキシサーバ７００は、機微データの変換後、仮想実行環境を廃棄する。

【０１５９】

ステップＳ２０４において、演算サーバ４００は、プロキシサーバ７００から変換された機微データを取得する。演算サーバ４００は、例えば、端末装置５００からのデータ処理要求に応じて、処理対象の機微データを送信するようプロキシサーバ７００に要求する。プロキシサーバ７００は、演算サーバ４００の要求に応じ、所定の暗号化空間に変換された、処理対象の機微データを演算サーバ４００に送信する。

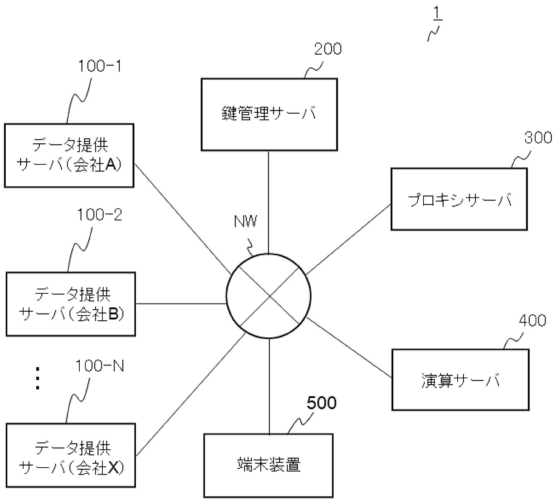
【０１６０】

ステップＳ２０５において、演算サーバ４００は、端末装置５００のデータ処理要求に応じた秘密計算を実行する。演算サーバ４００は、例えば、複数の機微データを統合して統合データを生成し、統合データについて機械学習によるモデル学習および推論を行う。なお、モデル学習等は、１つのデータ提供サーバ６００から提供された機微データに基づいて実行されてもよい。演算サーバ４００は、秘密計算の実行結果を、データ処理の要求

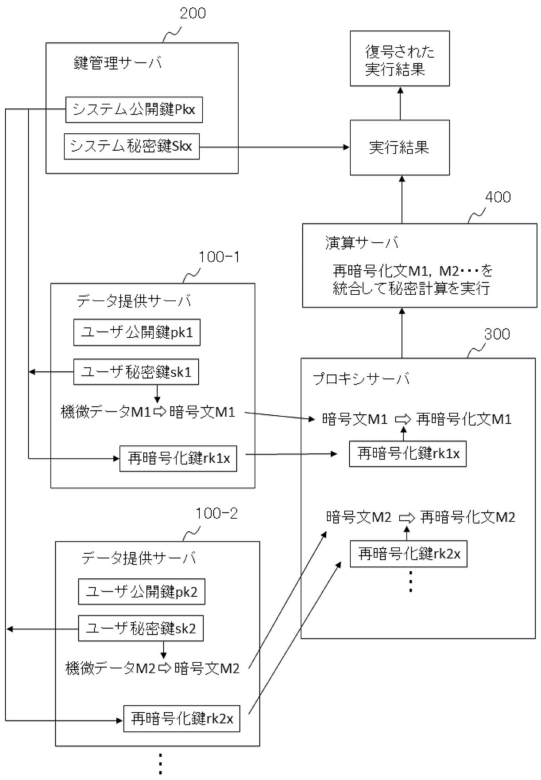
をした端末装置５００に送信する。
【０１６１】
ステップＳ２０６において、端末装置５００は、秘密計算の実行結果をシステム秘密鍵により復号する。これにより、端末装置５００は、復号された実行結果を平文データとして利用することができる。なお、端末装置５００は、実行結果を利用する権限を有するユーザとして、鍵管理サーバ２００からシステム秘密鍵を予め付与されていてもよいし、データ処理要求の際に、認証されたユーザとしてシステム秘密鍵を取得させてもよい。以上のようにして、データ共有システム２では、データ処理が行われる。
【０１６２】
（効果の説明）
上述したように、本実施形態に係るデータ共有システムは、暗号データを同一の暗号化空間に変換するためのシステム鍵を管理する鍵管理サーバを備える。また、当該システムに参加する各組織等に対応するデータ提供サーバは、システム鍵とは異なる、当該組織のユーザ鍵を用いて機微データを所定の暗号方式で暗号化し、プロキシサーバに送信する。プロキシサーバは、標準実行環境から保護される仮想実行環境を構築し、当該仮想実行環境において、取得した暗号化された機微データを復号後、システム鍵に基づいて、所定の暗号化空間に変換する。そして、演算サーバは、変換された機微データに基づいて秘密計算を実行する。
【０１６３】
標準実行環境から保護される仮想実行環境は、認証されないユーザからのアクセスを防ぐことができるため、暗号化された機微データを所定の暗号化空間に変換する処理を、セキュアに実行することができる。また、復号した機微データを所定の暗号方式で暗号化して所定の暗号化空間に変換するので、処理効率よく所定の暗号化空間に変換することができる。また、仮想実行環境は、短時間の構築であるため、仮想実行環境がサイバー攻撃を受けても、時間的にセキュリティ突破することが困難であり、セキュリティ上の安全性を担保することができる。
【０１６４】
＜実施形態２の変形例＞
仮想実行環境を構築し、仮想実行環境において、暗号化された機微データを所定の暗号化空間に変換する処理は、プロキシサーバ７００ではなく、演算サーバ４００が行うように構成してもよい。さらに、鍵管理サーバ２００が行う、システム鍵の管理についても、演算サーバ４００で行うように構成してもよい。
【０１６５】
これにより、通信チャンネルを介したデータの送受信処理を削減することができるため、セキュリティが向上し、また、コストの削減にもつなげることができる。
【０１６６】
上記実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれると同様に、特許請求の範囲に記載された発明とその均等の範囲に含まれるものとする。
【符号の説明】
【０１６７】
１，２　データ共有システム、１００，６００　データ提供サーバ、２００　鍵管理サーバ、３００，７００　プロキシサーバ、４００　演算サーバ、５００　端末装置、１０１，２０１，３０１，４０１，５０１，６０１，７０１　通信部、１０２，３０４，４２０，５０５，６０２，７０３　制御部、１０３，２１０，３０２，４１０，５０２，６０３，７０２　記憶部、１０４，２２０，６０４　鍵生成部、１０５，６０５，７２３　暗号化部、３０３，７０４　変換部、４２１　全体制御部、４２２　統合データ生成部、４２３　実行部、５０３　入力部、５０４　出力部、７１１　仮想実行環境部、７１２　仮想実行環境廃棄部、７２１　取得部、７２２　復号部、７２４　提供部。

【要約】
【課題】データ共有システムにおいて、各者が保有するデータの内容を他者に開示することなく、安全に活用すること。
【解決手段】本開示に係るデータ共有システムは、複数のデータ提供装置と、鍵管理装置と、プロキシ装置と、演算装置と、を備えるシステムであって、鍵管理装置は、システム鍵を管理する鍵管理部を有し、複数のデータ提供装置は、機微データを取得する第１の機微データ取得部と、システム鍵とは異なるユーザ鍵を用いて機微データを所定の暗号方式で暗号化する暗号化部を有し、プロキシ装置は、複数のデータ提供装置から、暗号化された機微データを取得する第２の機微データ取得部と、取得した機微データを、システム鍵に基づいて所定の暗号化空間における機微データに変換する変換部と、を有し、演算装置は、変換された機微データに基づいて秘密計算を実行する実行部を有する。
【選択図】図１

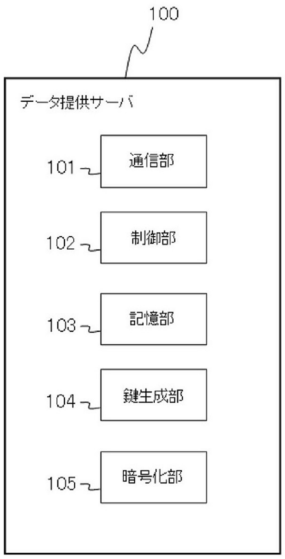
【図１】



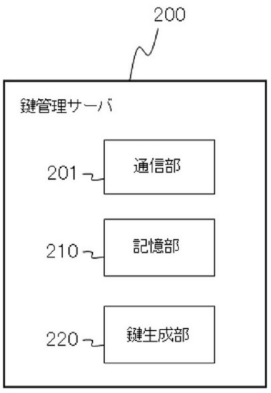
【図２】



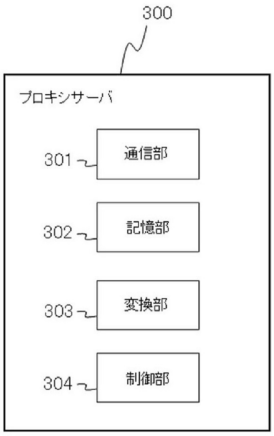
【図３】


100
データ提供サーバ
101
通信部
102
制御部
103
記憶部
104
鍵生成部
105
暗号化部

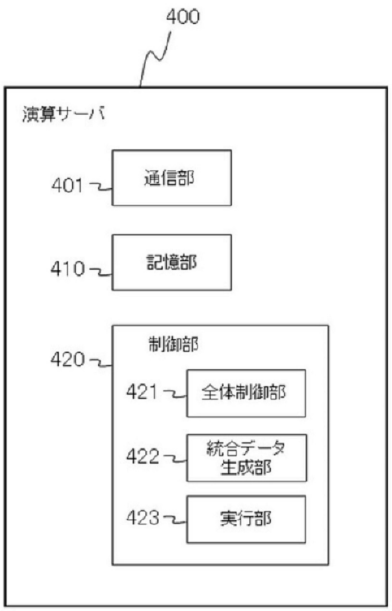
【図４】


200
鍵管理サーバ
201
通信部
210
記憶部
220
鍵生成部

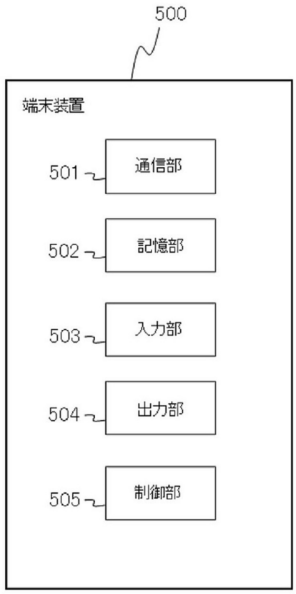
【図５】


300
プロキシサーバ
301
通信部
302
記憶部
303
変換部
304
制御部

【図６】


400
演算サーバ
401
通信部
410
記憶部
420
制御部
421
全体制御部
422
統合データ生成部
423
実行部

【図７】



【図８】

共通ID	年齢	性別	収入	購買フラグ1
12345	45	女	450	1
67890	28	男	500	0
23456	32	男	800	0
90123	34	女	900	1
89012	26	女	600	0
34567	55	男	600	1

T1
データ提供
サーバ100-1
(会社A)が提供

共通ID	居住地域	購買フラグ2	購買フラグ3
67890	東京	1	0
23456	神奈川	0	1
89012	東京	0	0
12345	名古屋	1	0
90123	大阪	1	1
34567	東京	0	1

T2
データ提供
サーバ100-2
(会社B)が提供

共通ID	配偶者フラグ	扶養人数	購買フラグ4
23456	1	3	1
90123	1	1	0
56789	0	0	0
34567	1	2	1
78901	0	2	1
12345	1	2	0

T3
データ提供
サーバ100-3
(会社C)が提供

【図９】

共通ID	年齢	性別	収入	購買フラグ1
12345	x22dc66…	adt3h54…	a66dc66…	dth54…
67890	s35ad54…	sdh2s3d…	d53ad54…	2dth5…
23456	af2weg6…	sdh2s3d…	3rfweg6…	2dth5…
90123	sd23c66…	adt3h54…	sw23c66…	dth54…
89012	cv45gw1…	adt3h54…	wr25gw1…	2dth5…
34567	vkf245a…	sdh2s3d…	wr25gw1…	dth54…

T1e
データ提供サーバ100-1
(会社A)のユーザ鍵で
暗号化
↓
再暗号化鍵で暗号化

共通ID	居住地域	購買フラグ2	購買フラグ3
67890	avf3h54…	23ds24…	45sfs2…
23456	sddfg3d…	45sfs2…	23ds24…
89012	avf3h54…	45sfs2…	45sfs2…
12345	hjk3h54…	23ds24…	45sfs2…
90123	adt3ert…	23ds24…	23ds24…
34567	avf3h54…	45sfs2…	23ds24…

T2e
データ提供サーバ100-2
(会社B)のユーザ鍵で暗号化
↓
再暗号化鍵で暗号化

共通ID	配偶者フラグ	扶養人数	購買フラグ4
23456	53ad54d…	66dc66a…	53ad54d…
90123	53ad54d…	53ad54d…	rfweg63…
56789	rfweg63…	rfweg63…	rfweg63…
34567	53ad54d…	2r25gw1…	53ad54d…
78901	rfweg63…	2r25gw1…	53ad54d…
12345	53ad54d…	2r25gw1…	rfweg63…

T3e
データ提供サーバ100-3
(会社C)のユーザ鍵で暗号化
↓
再暗号化鍵で暗号化

【図１０】

Tm

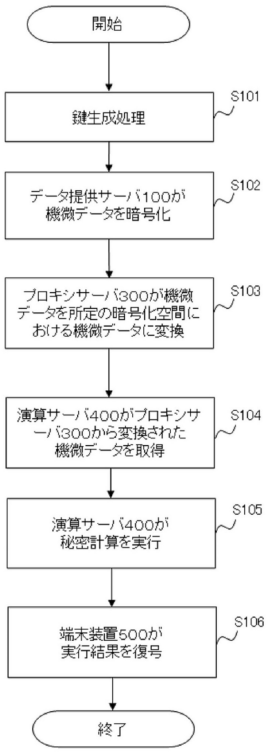
データ提供
サーバ100-1
(会社A)

データ提供
サーバ100-2
(会社B)

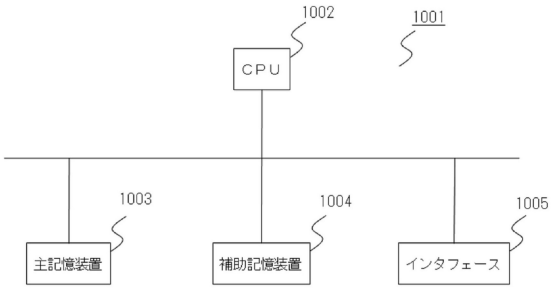
データ提供
サーバ100-3
(会社C)

共通ID	年齢	性別	収入	購買フラグ1	居住地域	購買フラグ2	購買フラグ3	配偶者フラグ	扶養人数	購買フラグ4
12345	x33dc66…	adth354…	a45dc66…	dth4…	hjk3h54…	2ds24…	45fs2…	53ad4d…	r25gw1…	rfwg63…
67890	s53ad54…	sdhs23d…	d35ad54…	2dh5…	avf3h54…	2ds24…	45fs2…	(NULL)	(NULL)	(NULL)
23456	a2fweg6…	sdhs23d…	3fnweg6…	2dh5…	sddfg3d…	45fs2…	2ds24…	53ad4d…	6dc66a…	53ad4d…
90123	s2d3c66…	adth354…	s2w3c66…	dth4…	adt3ert…	2ds24…	2ds24…	53ad4d…	5ad54d…	rfwg63…
89012	c4v5gw1…	adth354…	w2r5gw1…	2dh5…	avf3h54…	45fs2…	45fs2…	(NULL)	(NULL)	(NULL)
34567	vfk445a…	sdhs23d…	wr52gw1…	dth4…	avf3h54…	45fs2…	2ds24…	53ad4d…	r25gw1…	53ad4d…
56789	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	rfwg63…	rfwg63…	rfwg63…
78901	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	rfwg63…	r25gw1…	5ad54d…

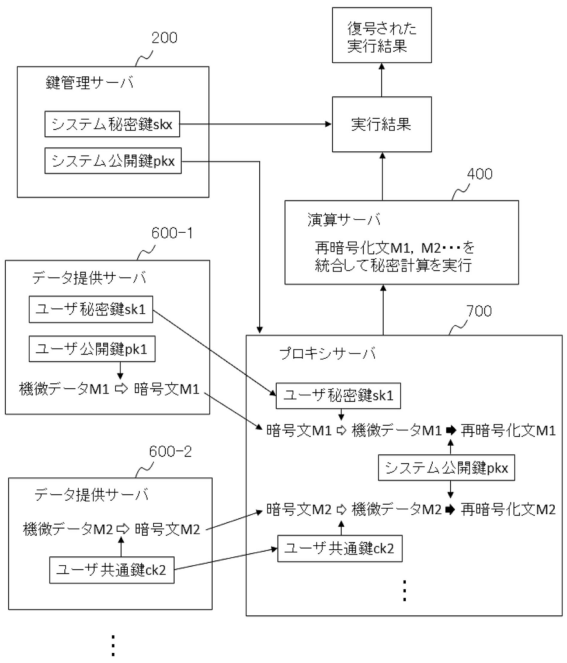
【図１１】



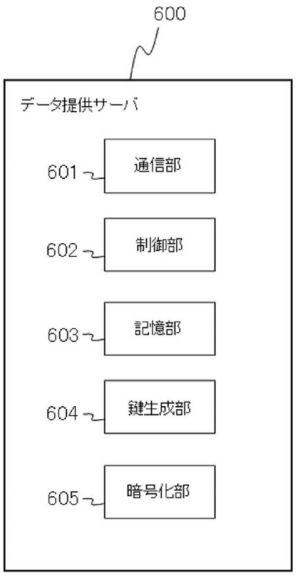
【図１２】



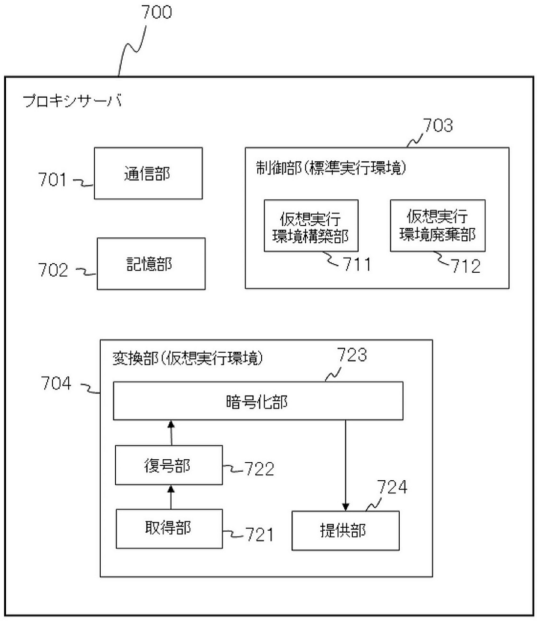
【図１３】



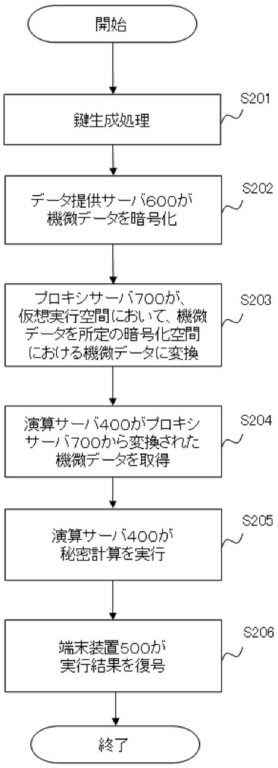
【図１４】



【図１５】


700
プロキシサーバ
703
701
通信部
制御部(標準実行環境)
仮想実行
環境構築部
仮想実行
環境廃棄部
711
712
702
記憶部
変換部(仮想実行環境)
723
704
暗号化部
復号部
722
724
取得部
721
提供部

【図１６】


開始
鍵生成処理
S201
データ提供サーバ600が
機微データを暗号化
S202
プロキシサーバ700が、
仮想実行空間において、機微
データを所定の暗号化空間
における機微データに変換
S203
演算サーバ400がプロキシ
サーバ700から変換された
機微データを取得
S204
演算サーバ400が
秘密計算を実行
S205
端末装置500が
実行結果を復号
S206
終了

フロントページの続き

(56)参考文献 国際公開第２０１９／１３０５２８（WO，Ａ１）
国際公開第２０１２／１４７８６９（WO，Ａ１）
特開２０１５－１１４６２９（ＪＰ，Ａ）
特表２０１３－５２８８７２（ＪＰ，Ａ）
特許第６６７１７０１（ＪＰ，Ｂ１）
特許第６８０３５９８（ＪＰ，Ｂ１）
国際公開第２０１２／１１１７１３（WO，Ａ１）
柴田 崇夫，松澤 智史，武田 正之，Proxy re-encryptionを用いたマルチユーザ向け完全準同型暗号の提案，2014年 情報科学技術フォーラム(FIT)講演論文集，2014年08月19日，第四分冊，pp.19-24
宇根正志，井上紫織，機械学習システムの脆弱性と対応策にかかる研究動向について Research Trends on Vulnerability and Count，コンピュータセキュリティシンポジウム２０１８論文集，2018年10月15日，pp.193-200
一色寿幸 他，準同型暗号を用いたプライバシー保護型統計演算のソフトウェア実装報告，電子情報通信学会技術研究報告，2012年02月23日，第111巻 第455号，pp.135-140
XIAO，L. et al.，An Efficient Homomorphic Encryption Protocol for Multi-User Systems，Cryptology ePrint Archive，Report 2012/193，[online]，2012年04月，pp.1-19，<URL:https://eprint.iacr.org/2012/193>，[2021年6月30日検索]

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　　１／００
Ｈ０４Ｌ　　９／３０
Ｇ０６Ｆ　２１／６０
Ｇ０６Ｆ　２１／６２