(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4189496号
(P4189496)
(45)発行日　平成20年12月3日(2008.12.3)　(24)登録日　平成20年9月26日(2008.9.26)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A

請求項の数 11　(全 22 頁)

(21)出願番号　特願2005-96400(P2005-96400)
(22)出願日　平成17年3月29日(2005.3.29)
(65)公開番号　特開2006-279595(P2006-279595A)
(43)公開日　平成18年10月12日(2006.10.12)
審査請求日　平成17年8月9日(2005.8.9)

(73)特許権者　504145320
国立大学法人福井大学
福井県福井市文京３丁目９番１号
(74)代理人　100111855
弁理士　川崎　好昭
(72)発明者　田村　信介
福井県福井市文京３－９－１　国立大学法人福井大学工学部内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】情報処理システム及びそのプログラム

(57)【特許請求の範囲】
【請求項１】
複数のクライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置から情報を受信して処理するサーバ装置とを備えている情報処理システムであって、
前記クライアント装置は、当該装置が管理する情報に関連するＩＤ情報及びパスワード情報を記憶する記憶手段と、サーバ装置から受信した第一暗号キーにより暗号化された複数のパスワード情報に基づいて前記記憶手段に記憶されたパスワード情報を用いて前記複数のパスワード情報の暗号化処理に用いた暗号キーを算出した後サーバ装置から受信した第二暗号キーを用いて当該暗号キーを暗号化処理するパスワード処理手段と、サーバ装置から受信した前記第一暗号キーの第二暗号キーによる暗号化情報及び前記パスワード処理手段による前記暗号キーの暗号化情報に基づいてサーバ装置の正当性を判定すると共に正当性ありと判定された場合に前記暗号キーをクライアント検証情報としてサーバ装置に送信するサーバ判定手段とを備え、
前記サーバ装置は、前記クライアント装置のＩＤ情報を含む複数のＩＤ情報に対応するパスワード情報を抽出する抽出手段と、前記抽出手段により抽出された複数のパスワード情報を前記第一暗号キーを用いて暗号化処理してクライアント装置に送信する第一暗号化処理手段と、前記第一暗号キーを第二暗号キーを用いて暗号化処理して第二暗号キーとともにクライアント装置に送信する第二暗号化処理手段と、クライアント装置から送信された前記クライアント検証情報及び前記第一暗号キーに基づいてクライアント装置の正当性

を判定するクライアント判定手段とを備えていることを特徴とする情報処理システム。
【請求項２】
前記クライアント装置は、当該装置のＩＤ情報を含む複数のＩＤ情報を発生させてサーバ装置に送信するＩＤ情報処理手段を備え、前記サーバ装置の前記抽出手段は、前記クライアント装置から受信した複数のＩＤ情報に対応するパスワード情報を抽出することを特徴とする請求項１に記載の情報処理システム。
【請求項３】
複数のクライアント装置にネットワークを介してサーバ装置を接続して情報を処理する情報処理方法であって、
クライアント装置に記憶された利用者のＩＤ情報を含む複数のＩＤ情報を発生させてサーバ装置に送信し、送信された複数のＩＤ情報に対応するパスワード情報をサーバ装置において抽出し、抽出された複数のパスワード情報を第一暗号キーで暗号化処理するとともに第一暗号キーを第二暗号キーで暗号化処理して第二暗号キーとともにクライアント装置に送信し、暗号化された複数のパスワード情報に基づいてクライアント装置のパスワード情報を用いて前記複数のパスワード情報の暗号化に用いた暗号キーを算出した後第二暗号キーを用いて当該暗号キーを暗号化処理し、第一暗号キーの第二暗号キーによる暗号化情報及び前記暗号キーの暗号化情報に基づいてサーバ装置の正当性を判定し、サーバ装置の正当性ありと判定された場合に前記暗号キーをクライアント検証情報としてサーバ装置に送信し、クライアント装置から送信された前記クライアント検証情報及び第一暗号キーに基づいてクライアント装置の正当性を判定することを特徴とする情報処理方法。
【請求項４】
複数のクライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置から情報を受信して処理するサーバ装置とを備えている情報処理システムにおいて、該クライアント装置を機能させるためのプログラムであって、
前記クライアント装置を、
当該装置の利用者のＩＤ情報を含む複数のＩＤ情報を発生させてサーバ装置に送信する手段、
サーバ装置から受信した第一暗号キーにより暗号化された複数のパスワード情報に基づいてクライアント装置のパスワード情報を用いて前記複数のパスワード情報の暗号化に用いた暗号キーを算出した後サーバ装置から受信した第二暗号キーを用いて当該暗号キーを暗号化処理する手段、
サーバ装置から受信した前記第一暗号キーの第二暗号キーによる暗号化情報及び前記暗号キーの暗号化情報に基づいてサーバ装置の正当性を判定する手段、
サーバ装置の正当性ありと判定された場合に前記暗号キーをクライアント検証情報としてサーバ装置に送信する手段、
として機能させるためのプログラム。
【請求項５】
複数のクライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置から情報を受信して処理するサーバ装置とを備えている情報処理システムにおいて、該サーバ装置を機能させるためのプログラムであって、
前記サーバ装置を、
記憶された全利用者のＩＤ情報及びパスワード情報に基づいてクライアント装置から受信した複数のＩＤ情報に対応するパスワード情報を抽出する手段、
抽出された複数のパスワード情報を第一暗号キーを用いて暗号化処理してクライアント装置に送信する手段、
第一暗号キーを第二暗号キーを用いて暗号化処理して第二暗号キーとともにクライアント装置に送信する手段、
クライアント装置から送信されたクライアント検証情報及び前記第一暗号キーに基づいてクライアント装置の正当性を判定する手段、
として機能させるためのプログラム。

【請求項６】
Ｍ個の項目D_i（i=1,2,…,M）に対応するデータd_{ij}（i=1,2,…,M;j=1,2,…,N）を記憶するＮ個のデータ管理装置S_j（j=1,2,…,N）と、データ管理装置にネットワークを介して接続されるとともにデータd_{ij}を項目毎に集計するデータ集計装置とを備えている情報処理システムであって、
データ管理装置S_kは、係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及びＭ個のデータd_{ik}（i=1,2,…,M）を記憶する記憶手段と、データd_{ik}及び係数データa_{pq}を用いてＭ個の一次結合データv_{pk}（p=1,2,…,M）を以下の式（Ａ）
$$v_{pk}=a_{p1}d_{1k}+a_{p2}d_{2k}+\cdots+a_{pq}d_{qk}+\cdots+a_{pM}d_{Mk}\cdots(A)$$
により算出する結合計算手段と、一次結合データv_{pk}の順番別に全データ管理装置S_jで算出された値の集計を担当するデータ管理装置S_jを登録する登録手段と、登録された他のデータ管理装置S_jに集計に必要な順番の一次結合データv_{pk}を送信するとともに当該データ管理装置S_kが担当する順番の一次結合データv_{rj}（1≦r≦M;j=1,2,…,N）を他のデータ管理装置S_jから受信して全データ管理装置S_jの値を集計し集計された結合集計データをデータ集計装置に送信する結合集計手段とを備え、
データ集計装置は、前記係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）を記憶する記憶手段と、各データ管理装置S_jから受信した結合集計データを集計して結合集計データ及び前記係数データa_{pq}に基づいて項目D_i毎にデータd_{ij}の集計値を算出する集計データ算出手段とを備えていることを特徴とする情報処理システム。

【請求項７】
Ｍ個の項目D_i（i=1,2,…,M）に対応するデータd_{ij}（i=1,2,…,M;j=1,2,…,N）を記憶するＮ個のデータ管理装置S_j（j=1,2,…,N）にネットワークを介してデータ集計装置を接続してデータd_{ij}を項目毎に集計する情報処理方法であって、
データ管理装置S_kに記憶された係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及びＭ個のデータd_{ik}（i=1,2,…,M）を用いてＭ個の一次結合データv_{pk}（p=1,2,…,M）を以下の式（Ａ）
$$v_{pk}=a_{p1}d_{1k}+a_{p2}d_{2k}+\cdots+a_{pq}d_{qk}+\cdots+a_{pM}d_{Mk}\cdots(A)$$
により算出し、一次結合データv_{pk}の順番別に全データ管理装置S_jで算出された値の集計を担当する他のデータ管理装置S_jに集計に必要な順番の一次結合データv_{pk}を送信し、当該データ管理装置S_kが担当する順番の一次結合データv_{rj}（1≦r≦M;j=1,2,…,N）を他のデータ管理装置S_jから受信して全データ管理装置S_jの値を集計し集計された結合集計データをデータ集計装置に送信し、データ集計装置においてデータ管理装置S_jから受信した結合集計データ及び前記係数データa_{pq}に基づいて項目D_i毎にデータd_{ij}の集計値を算出することを特徴とする情報処理方法。

【請求項８】
Ｍ個の項目D_i（i=1,2,…,M）に対応するデータd_{ij}（i=1,2,…,M;j=1,2,…,N）を記憶するＮ個のデータ管理装置S_j（j=1,2,…,N）と、データ管理装置にネットワークを介して接続されるとともにデータd_{ij}を項目毎に集計するデータ集計装置とを備えている情報処理システムにおいて、データ管理装置S_kを機能させるためのプログラムであって、
前記データ管理装置S_kを、
係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及びＭ個のデータd_{ik}（i=1,2,…,M）を用いてＭ個の一次結合データv_{pk}（p=1,2,…,M）を以下の式（Ａ）
$$v_{pk}=a_{p1}d_{1k}+a_{p2}d_{2k}+\cdots+a_{pq}d_{qk}+\cdots+a_{pM}d_{Mk}\cdots(A)$$
により算出する手段、
一次結合データv_{pk}の順番別に全データ管理装置S_jで算出された値の集計を担当する他のデータ管理装置S_jに集計に必要な順番の一次結合データv_{pk}を送信するとともに当該データ管理装置S_kが担当する順番の一次結合データv_{rj}（1≦r≦M;j=1,2,…,N）を他のデータ管理装置S_jから受信して全データ管理装置S_jの値を集計し集計された結合集計データをデータ集計装置に送信する手段、
として機能させるためのプログラム。

【請求項９】
クライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置との間で情報を送受信して処理するサーバ装置と、クライアント装置とサーバ装置との間の情報の処理過程で生成あるいは利用した特定情報に関するデータを記憶するデータ記憶装置とを備えている情報処理システムであって、
前記クライアント装置は、係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）を記憶する記憶手段と、前記特定情報に関するM個のデータd_i（i=1,2,…,M）及び係数データa_{pq}を用いてM個の一次結合データv_p（p=1,2,…,M）を以下の式（B）
$$v_p = a_{p1}d_1 + a_{p2}d_2 + \cdots + a_{pq}d_i + \cdots + a_{pM}d_M \quad \cdots \text{（B）}$$
により算出して算出されたM個の一次結合データv_pを前記データ記憶装置に送信する算出手段と、前記データ記憶装置に記憶された一次結合データv_pを読み出してデータd_iを集計するとともに集計値を前記サーバ装置に送信する集計手段とを備え、
前記サーバ装置は、前記クライアント装置から受信した集計値を登録処理する集計処理手段を備え、
前記データ記憶装置は、前記クライアント装置から受信した一次結合データv_pを記憶する登録処理手段と、前記クライアント装置に対して記憶された一次結合データv_pを送信する読出処理手段とを備えていることを特徴とする情報処理システム。
【請求項１０】
クライアント装置と、クライアント装置にネットワークを介して接続されたサーバ装置との間の情報の処理過程で生成あるいは利用した特定情報に関するデータをデータ記憶装置に記憶して当該特定情報に関するデータを集計する情報処理方法であって、
前記クライアント装置に記憶された係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及び前記特定情報に関するM個のデータd_i（i=1,2,…,M）を用いてM個の一次結合データv_p（p=1,2,…,M）を以下の式（B）
$$v_p = a_{p1}d_1 + a_{p2}d_2 + \cdots + a_{pq}d_i + \cdots + a_{pM}d_M \quad \cdots \text{（B）}$$
により算出して算出されたM個の一次結合データv_pを前記データ記憶装置に送信し、前記データ記憶装置において前記クライアント装置から受信した一次結合データv_pを記憶し、前記クライアント装置に対して記憶された一次結合データv_pを送信し、前記クライアント装置において前記データ記憶装置に記憶された一次結合データv_pを読み出してデータd_iを集計するとともに集計値を前記サーバ装置に送信し、前記サーバ装置において前記クライアント装置から受信した集計値を登録処理することを特徴とする情報処理方法。
【請求項１１】
クライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置との間で情報を送受信して処理するサーバ装置と、クライアント装置とサーバ装置との間の情報の処理過程で生成あるいは利用した特定情報に関するデータを記憶するデータ記憶装置とを備えている情報処理システムにおいて、前記クライアント装置を機能させるためのプログラムであって、
前記クライアント装置を、
前記特定情報に関するM個のデータd_i（i=1,2,…,M）及び係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）を用いてM個の一次結合データv_p（p=1,2,…,M）を以下の式（B）
$$v_p = a_{p1}d_1 + a_{p2}d_2 + \cdots + a_{pq}d_i + \cdots + a_{pM}d_M \quad \cdots \text{（B）}$$
により算出して算出されたM個の一次結合データv_pをデータ記憶装置に送信する手段、
データ記憶装置に記憶された一次結合データv_pを読み出してデータd_iを集計するとともに集計値を前記サーバ装置に送信する集計手段、
として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理システムにおいて、当該システムに関係する個人や物に密接に関連

付けられる個別情報が特定されないように保護する情報処理システム及びそのプログラムに関する。

【背景技術】

【０００２】

インターネット等のネットワークシステムが急速に普及するにつれて、様々な情報がネットワーク上で送受信されている。しかしながら、ネットワーク上でやりとりされる情報は、常に悪意を持った第三者に不正に取得されたり改変される危険性がある。そのため、安全対策として様々な暗号化処理技術が開発されており、ネットワーク上で送受信される情報を暗号化することで情報の不正利用や改変を防止するようにしている。

【０００３】

こうした通信情報の暗号化処理技術は、通信時の不正取得や改変には有効であるが、暗号化処理された情報が正当に取得されて復号化された後の情報の悪用には対応することができない。

【０００４】

すなわち、特定の個人がサービス提供会社にＩＤ及びパスワードを暗号化して送信し、サービス提供会社からサービスを受けた場合、その個人の受けたサービス内容は、ＩＤとともにサービス提供会社に蓄積され、その個人の関連情報として記憶されていく。このように蓄積された個別情報は、サービス提供会社で厳格な情報管理がなされていたとしても不正流用されるおそれがある。特に、情報処理システムの高度化に伴って大量の情報を簡単に処理することができるようになり、その危険性は大きくなっている。例えば、インターネットで様々な商品の販売を行うサービスが提供されているが、個人ごとの購買実績データは、販売促進を行う際の基礎データとして流用されるおそれがある。一方、サービス提供を行う会社にとっても、個別情報の漏洩は社会的信用の低下を招くため、個別情報を厳格に管理することがますます強く求められるようになり、管理負担が増大するようになる。

【０００５】

また、アンケート調査や選挙といった選択又は記入内容が個人と密接に関連付けられる個別情報の場合についても、情報を送信する際にいかに厳重に暗号化処理していたとしても復号化した後に集計されたデータベースが外部に流出してしまうと、大量の個別情報が公にされてしまうおそれがある。

【０００６】

なお、本明細書において、「個別情報」とは、個人、会社等の法人及び個別に特定されて取り扱われる物（以下「個人等」という。）に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人等を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人等を識別することができることとなるものを含む。）を意味する。

【０００７】

インターネット等のネットワークシステムにおいて上述したような個別情報を送受信する場合に、個別情報が流出するおそれがあるという仮定の下に安全対策を検討する必要がある。こうした個別情報の流出を防止するための１つの方法として、個人が特定されないように情報を送受信する方法が提案されている。例えば、特許文献１では、グループ署名方式を用いた匿名認証システムが記載されている。グループ署名方式では、グループのメンバが署名に用いる鍵情報とは別にグループごとに用いられる単一のグループ公開鍵で検証できる署名方式で、メンバごとの鍵情報を使用しないで認証が行われるため、メンバごとのサービス利用状況といった個別情報が特定されることがなくなり、サービス提供会社に個別情報が蓄積されることがなくなる。

【０００８】

また、特許文献２では、ユーザ端末及びサービス提供サーバの間でゼロ知識証明やブラインド署名方式を用いて匿名認証を行う装置が記載されている。また、特許文献３では、同一符号に復号できる見かけ上異なる値を示す符号を生成する暗号化手順を使って、ユー

ザに対してその都度可変に見える識別子を割り当てて、この可変識別子の持つ性質に従ってユーザ情報を検索できるようにし、ユーザの識別に用いる固定識別子とユーザの行動履歴とが深く結びつく事態を防止する点が記載されている。また、特許文献４では、サービス提供サーバが同一内容を保証した互いに異なる複数の仮デジタル署名を生成してユーザ装置に送信し、ユーザ装置では受信した仮デジタル署名から複数の電子証明書を取得し、そのうちの任意の１つの電子証明書により認証を行うことで、ユーザの属性情報を提供せずに匿名認証を行う点が記載されている。

【特許文献１】特開２００４－３２０５６２号公報
【特許文献２】特開２００５－５７７８号公報
【特許文献３】特開２００４－３６２２０１号公報
【特許文献４】特開２００４－２４２１９５号公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】

上述した特許文献１では、利用者の個別情報は、サービス提供会社に蓄積されないものの属性発行管理サーバにより管理されており、属性発行管理サーバからの個別情報の流出の危険性が依然として存在することになる。また、特許文献２から４では、ユーザの属性情報は用いずに認証を行うようになっているが、属性情報から完全に切り離されて認証を行うことはなく、認証に用いる情報がユーザと関連付けられる可能性は排除できないため、送受信される情報が個別情報として特定される可能性がある。

【００１０】

このように、個別情報として特定される可能性がある場合、互いに信用できない多数の主体同士がネットワークで接続されて情報を送受信される環境下では、安心して情報を送受信することができない。例えば、今後本格化するユビキュタス・コンピューティングでは、個人のあらゆる情報がコンピュータにより記録されてネットワークを介して送受信されるようになることが想定されるが、こうした個別情報に対する保護をどのように行うのか対策を立てておく必要がある。

【００１１】

そこで、本発明は、互いに信用できない主体間において個別情報のように個人や物に密接に関連付けられる情報がそれと特定されないように情報を送受信することができる情報処理システムを提供することを目的とするものである。

【課題を解決するための手段】

【００１２】

本発明に係る情報処理システムは、複数のクライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置から情報を受信して処理するサーバ装置とを備えている情報処理システムであって、前記クライアント装置は、当該装置が管理する情報に関連するＩＤ情報及びパスワード情報を記憶する記憶手段と、サーバ装置から受信した第一暗号キーにより暗号化された複数のパスワード情報に基づいて前記記憶手段に記憶されたパスワード情報を用いて前記複数のパスワード情報の暗号化処理に用いた暗号キーを算出した後サーバ装置から受信した第二暗号キーを用いて当該暗号キーを暗号化処理するパスワード処理手段と、サーバ装置から受信した前記第一暗号キーの第二暗号キーによる暗号化情報及び前記パスワード処理手段による前記暗号キーの暗号化情報に基づいてサーバ装置の正当性を判定すると共に正当性ありと判定された場合に前記暗号キーをクライアント検証情報としてサーバ装置に送信するサーバ判定手段とを備え、前記サーバ装置は、前記クライアント装置のＩＤ情報を含む複数のＩＤ情報に対応するパスワード情報を抽出する抽出手段と、前記抽出手段により抽出された複数のパスワード情報を前記第一暗号キーを用いて暗号化処理してクライアント装置に送信する第一暗号化処理手段と、前記第一暗号キーを第二暗号キーを用いて暗号化処理して第二暗号キーとともにクライアント装置に送信する第二暗号化処理手段と、クライアント装置から送信された前記クライアント検証情報及び前記第一暗号キーに基づいてクライアント装置の正当性を判定

するクライアント判定手段とを備えていることを特徴とする。さらに、前記クライアント装置は、当該装置のＩＤ情報を含む複数のＩＤ情報を発生させてサーバ装置に送信するＩＤ情報処理手段を備え、前記サーバ装置の前記抽出手段は、前記クライアント装置から受信した複数のＩＤ情報に対応するパスワード情報を抽出することを特徴とする。

【００１３】

本発明に係る情報処理方法は、複数のクライアント装置にネットワークを介してサーバ装置を接続して情報を処理する情報処理方法であって、クライアント装置に記憶された利用者のＩＤ情報を含む複数のＩＤ情報を発生させてサーバ装置に送信し、送信された複数のＩＤ情報に対応するパスワード情報をサーバ装置において抽出し、抽出された複数のパスワード情報を第一暗号キーで暗号化処理するとともに第一暗号キーを第二暗号キーで暗号化処理して第二暗号キーとともにクライアント装置に送信し、暗号化された複数のパスワード情報に基づいてクライアント装置のパスワード情報を用いて前記複数のパスワード情報の暗号化に用いた暗号キーを算出した後第二暗号キーを用いて当該暗号キーを暗号化処理し、第一暗号キーの第二暗号キーによる暗号化情報及び前記暗号キーの暗号化情報に基づいてサーバ装置の正当性を判定し、サーバ装置の正当性ありと判定された場合に前記暗号キーをクライアント検証情報としてサーバ装置に送信し、クライアント装置から送信された前記クライアント検証情報及び第一暗号キーに基づいてクライアント装置の正当性を判定することを特徴とする。

【００１４】

本発明に係るプログラムは、複数のクライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置から情報を受信して処理するサーバ装置とを備えている情報処理システムにおいて、該クライアント装置を機能させるためのプログラムであって、前記クライアント装置を、当該装置の利用者のＩＤ情報を含む複数のＩＤ情報を発生させてサーバ装置に送信する手段、サーバ装置から受信した第一暗号キーにより暗号化された複数のパスワード情報に基づいてクライアント装置のパスワード情報を用いて前記複数のパスワード情報の暗号化に用いた暗号キーを算出した後サーバ装置から受信した第二暗号キーを用いて当該暗号キーを暗号化処理する手段、サーバ装置から受信した前記第一暗号キーの第二暗号キーによる暗号化情報及び前記暗号キーの暗号化情報に基づいてサーバ装置の正当性を判定する手段、サーバ装置の正当性ありと判定された場合に前記暗号キーをクライアント検証情報としてサーバ装置に送信する手段、として機能させる。

【００１５】

本発明に係るプログラムは、複数のクライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置から情報を受信して処理するサーバ装置とを備えている情報処理システムにおいて、該サーバ装置を機能させるためのプログラムであって、前記サーバ装置を、記憶された全利用者のＩＤ情報及びパスワード情報に基づいてクライアント装置から受信した複数のＩＤ情報に対応するパスワード情報を抽出する手段、抽出された複数のパスワード情報を第一暗号キーを用いて暗号化処理してクライアント装置に送信する手段、第一暗号キーを第二暗号キーを用いて暗号化処理して第二暗号キーとともにクライアント装置に送信する手段、クライアント装置から送信されたクライアント検証情報及び前記第一暗号キーに基づいてクライアント装置の正当性を判定する手段、として機能させる。

【００１６】

本発明に係る別の情報処理システムは、Ｍ個の項目D_i（i=1,2,…,M）に対応するデータd_{ij}（i=1,2,…,M;j=1,2,…,N）を記憶するＮ個のデータ管理装置S_j（j=1,2,…,N）と、データ管理装置にネットワークを介して接続されるとともにデータd_{ij}を項目毎に集計するデータ集計装置とを備えている情報処理システムであって、データ管理装置S_kは、係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及びＭ個のデータd_{ik}（i=1,2,…,M）を記憶する記憶手段と、データd_{ik}及び係数データa_{pq}を用いてＭ個の一次結合データv_{pk}（p=1,2,…,M）を以下の式（Ａ）

$v_{pk}=a_{p1}d_{1k}+a_{p2}d_{2k}+\cdots+a_{pq}d_{qk}+\cdots+a_{pM}d_{Mk}$・・・（Ａ）
により算出する結合計算手段と、一次結合データv_{pk}の順番別に全データ管理装置S_jで算出された値の集計を担当するデータ管理装置S_jを登録する登録手段と、登録された他のデータ管理装置S_jに集計に必要な順番の一次結合データv_{pk}を送信するとともに当該データ管理装置S_kが担当する順番の一次結合データv_{rj}（$1\leqq r\leqq M$;j=1,2,…,N）を他のデータ管理装置S_jから受信して全データ管理装置S_jの値を集計し集計された結合集計データをデータ集計装置に送信する結合集計手段とを備え、データ集計装置は、前記係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）を記憶する記憶手段と、各データ管理装置S_jから受信した結合集計データを集計して結合集計データ及び前記係数データa_{pq}に基づいて項目D_i毎にデータd_{ij}の集計値を算出する集計データ算出手段とを備えていることを特徴とする。

【００１７】

本発明に係る別の情報処理方法は、Ｍ個の項目D_i（i=1,2,…,M）に対応するデータd_{ij}（i=1,2,…,M;j=1,2,…,N）を記憶するＮ個のデータ管理装置S_j（j=1,2,…,N）にネットワークを介してデータ集計装置を接続してデータd_{ij}を項目毎に集計する情報処理方法であって、データ管理装置S_kに記憶された係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及びＭ個のデータd_{ik}（i=1,2,…,M）を用いてＭ個の一次結合データv_{pk}（p=1,2,…,M）を以下の式（Ａ）

$v_{pk}=a_{p1}d_{1k}+a_{p2}d_{2k}+\cdots+a_{pq}d_{qk}+\cdots+a_{pM}d_{Mk}$・・・（Ａ）
により算出し、一次結合データv_{pk}の順番別に全データ管理装置S_jで算出された値の集計を担当する他のデータ管理装置S_jに集計に必要な順番の一次結合データv_{pk}を送信し、当該データ管理装置S_kが担当する順番の一次結合データv_{rj}（$1\leqq r\leqq M$;j=1,2,…,N）を他のデータ管理装置S_jから受信して全データ管理装置S_jの値を集計し集計された結合集計データをデータ集計装置に送信し、データ集計装置においてデータ管理装置S_jから受信した結合集計データ及び前記係数データa_{pq}に基づいて項目D_i毎にデータd_{ij}の集計値を算出することを特徴とする。

【００１８】

本発明に係る別のプログラムは、Ｍ個の項目D_i（i=1,2,…,M）に対応するデータd_{ij}（i=1,2,…,M;j=1,2,…,N）を記憶するＮ個のデータ管理装置S_j（j=1,2,…,N）と、データ管理装置にネットワークを介して接続されるとともにデータd_{ij}を項目毎に集計するデータ集計装置とを備えている情報処理システムにおいて、データ管理装置S_kを機能させるためのプログラムであって、前記データ管理装置S_kを、係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及びＭ個のデータd_{ik}（i=1,2,…,M）を用いてＭ個の一次結合データv_{pk}（p=1,2,…,M）を以下の式（Ａ）

$v_{pk}=a_{p1}d_{1k}+a_{p2}d_{2k}+\cdots+a_{pq}d_{qk}+\cdots+a_{pM}d_{Mk}$・・・（Ａ）
により算出する手段、一次結合データv_{pk}の順番別に全データ管理装置S_jで算出された値の集計を担当する他のデータ管理装置S_jに集計に必要な順番の一次結合データv_{pk}を送信するとともに当該データ管理装置S_kが担当する順番の一次結合データv_{rj}（$1\leqq r\leqq M$;j=1,2,…,N）を他のデータ管理装置S_jから受信して全データ管理装置S_jの値を集計し集計された結合集計データをデータ集計装置に送信する手段、として機能させる。

【００１９】

本発明に係るさらに別の情報処理システムは、複数のクライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置との間で情報を送受信して処理するサーバ装置と、クライアント装置とサーバ装置との間の情報の処理過程で生成あるいは利用した特定情報に関するデータを記憶するデータ記憶装置とを備えている情報処理システムであって、前記クライアント装置は、係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）を記憶する記憶手段と、前記特定情報に関するＭ個のデータd_i（i=1,2,…,M）及び係数データa_{pq}を用いてＭ個の一次結合データv_p（p=1,2,…,M）を以下の式（Ｂ）

$v_p=a_{p1}d_1+a_{p2}d_2+\cdots+a_{pq}d_i+\cdots+a_{pM}d_M$・・・（Ｂ）
により算出して算出されたＭ個の一次結合データv_pを前記データ記憶装置に送信する算

出手段と、前記データ記憶装置に記憶された一次結合データv_pを読み出してデータd_iを集計するとともに集計値を前記サーバ装置に送信する集計手段とを備え、前記サーバ装置は、前記クライアント装置から受信した集計値を登録処理する集計処理手段を備え、前記データ記憶装置は、前記クライアント装置から受信した一次結合データv_pを記憶する登録処理手段と、前記クライアント装置に対して記憶された一次結合データv_pを送信する読出処理手段とを備えていることを特徴とする。

【００２０】

本発明に係るさらに別の情報処理方法は、クライアント装置と、クライアント装置にネットワークを介して接続されたサーバ装置との間の情報の処理過程で生成あるいは利用した特定情報に関するデータをデータ記憶装置に記憶して当該特定情報に関するデータを集計する情報処理方法であって、前記クライアント装置に記憶された係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及び前記特定情報に関するＭ個のデータd_i（i=1,2,…,M）を用いてＭ個の一次結合データv_p（p=1,2,…,M）を以下の式（Ｂ）

$$v_p = a_{p1}d_1 + a_{p2}d_2 + \cdots + a_{pq}d_i + \cdots + a_{pM}d_M \cdots （Ｂ）$$

により算出して算出されたＭ個の一次結合データv_pを前記データ記憶装置に送信し、前記データ記憶装置において前記クライアント装置から受信した一次結合データv_pを記憶し、前記クライアント装置に対して記憶された一次結合データv_pを送信し、前記クライアント装置において前記データ記憶装置に記憶された一次結合データv_pを読み出してデータd_iを集計するとともに集計値を前記サーバ装置に送信し、前記サーバ装置において前記クライアント装置から受信した集計値を登録処理することを特徴とする。

【００２１】

本発明に係るさらに別のプログラムは、複数のクライアント装置と、クライアント装置にネットワークを介して接続されるとともにクライアント装置との間で情報を送受信して処理するサーバ装置と、クライアント装置とサーバ装置との間の情報の処理過程で生成あるいは利用した特定情報に関するデータを記憶するデータ記憶装置とを備えている情報処理システムにおいて、前記クライアント装置を機能させるためのプログラムであって、前記クライアント装置を、前記特定情報に関するＭ個のデータd_i（i=1,2,…,M）及び係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）を用いてＭ個の一次結合データv_p（p=1,2,…,M）を以下の式（Ｂ）

$$v_p = a_{p1}d_1 + a_{p2}d_2 + \cdots + a_{pq}d_i + \cdots + a_{pM}d_M \cdots （Ｂ）$$

により算出して算出されたＭ個の一次結合データv_pをデータ記憶装置に送信する手段、データ記憶装置に記憶された一次結合データv_pを読み出してデータd_iを集計するとともに集計値を前記サーバ装置に送信する集計手段、として機能させる。

【発明の効果】

【００２２】

本発明に係る情報処理システム及び情報処理方法は、クライアント装置に記憶された利用者のＩＤ情報を含む複数のＩＤ情報を発生させてサーバ装置に送信し、送信された複数のＩＤ情報に対応するパスワード情報をサーバ装置において抽出し、抽出された複数のパスワード情報を第一暗号キーで暗号化処理するとともに第一暗号キーを第二暗号キーで暗号化処理して第二暗号キーとともにクライアント装置に送信し、暗号化された複数のパスワード情報に基づいてクライアント装置のパスワード情報を用いて複数のパスワード情報の暗号化に用いた暗号キーを算出した後第二暗号キーを用いて当該暗号キーを暗号化処理し、第一暗号キーの第二暗号キーによる暗号化情報及び暗号キーの暗号化情報に基づいてサーバ装置の正当性を判定するので、サーバ装置では利用者のＩＤ情報を特定することはできないが、クライアント装置ではサーバ装置の正当性を判定することができる。

【００２３】

また、サーバ装置の正当性ありと判定された場合には、クライアント装置は、暗号キーをクライアント検証情報としてサーバ装置に送信し、クライアント装置から送信されたクライアント検証情報及び第一暗号キーに基づいてクライアント装置の正当性を判定するので、サーバ装置においてもクライアント装置の正当性を判定することができる。

【００２４】
このように、どの利用者がアクセスしてきているのかサーバ装置で特定できないので、クライアント装置との間で送受信される情報は個別情報として特定されることはなく、また、クライアント装置及びサーバ装置が互いに正当性を判定できるので、互いに信用できない主体間でも正当性を確認して情報を送受信することが可能となる。
【００２５】
本発明に係る別の情報処理システム及び情報処理方法は、データ管理装置S_kに記憶された係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及びM個のデータd_{ik}（i=1,2,…,M）を用いてM個の一次結合データv_{pk}（p=1,2,…,M）を上記の式（Ａ）により算出し、一次結合データv_{pk}の順番別に全データ管理装置S_jで算出された値の集計を担当する他のデータ管理装置S_jに集計に必要な順番の一次結合データv_{pk}を送信するとともに当該データ管理装置S_jが担当する順番の一次結合データv_{rj}（1≦r≦M;j=1,2,…,N）を他のデータ管理装置S_jから受信して全データ管理装置S_jの値を集計するようにしているので、集計を担当するデータ管理装置S_jには一部の順番の一次結合データv_{pk}のみ集計され、他のデータ管理装置のデータｄを求めることはできない。すなわち、各データ管理装置は、共通の係数データa_{pq}を用いて一次結合データv_{pk}を算出しているので、すべての一次結合データv_{pk}を得ることができれば、M個のデータを変数として係数データa_{pq}を用いたM個の連立一次方程式を解くことによりデータｄを得ることができるが、一次結合データv_{pk}が一部しかない場合には連立一次方程式を解くことができない。このように、各データ管理装置では、互いにデータｄを特定されることなく一次結合データv_{pk}を順番別に全データ管理装置について集計することが可能となる。
【００２６】
そして、データ集計装置は、データ管理装置S_jから受信した集計データ及び前記係数データa_{pq}を得ることで項目D_i毎にデータd_{ij}の集計値を算出することができる。すなわち、データ管理装置で順番別に一次結合データv_{rs}（1≦r≦M;s=1,2,…,N）を集計した結合集計データV_rは、以下のとおりとなる。
$V_r=v_{r1}+v_{r2}+\cdots+v_{rs}+\cdots+v_{rN}=a_{r1}\Sigma d_{1s}+a_{r2}\Sigma d_{2s}+\cdots+a_{rq}\Sigma d_{is}+\cdots+a_{rM}\Sigma d_{Ms}$
したがって、M個の結合集計データV_rをデータ集計装置が得ることで、M個のΣd_{ij}を変数として係数データa_{pq}を用いたM個の連立一次方程式を解くことによりデータ項目D_i別の集計値Σd_{ij}を得ることができる。その際に、データ集計装置は、集計データV_rしか得ることがないので、各データｄを特定することはできない。そのため、データ管理装置から個別情報を特定されることなく集計データを外部に送信することで、個別情報の集計を行うことができるようになる。
【００２７】
また、本発明に係るさらに別の情報処理システムは、サーバ装置との間の処理過程で生成あるいは利用した情報に関するM個のデータd_iを係数データa_{pq}を用いてM個の一次結合データv_p（p=1,2,…,M）を以下の式（Ｂ）
$v_p=a_{p1}d_1+a_{p2}d_2+\cdots+a_{pq}d_i+\cdots+a_{pM}d_M$・・・（Ｂ）
により算出して変換することで、一次結合データv_pの形で外部に送信してもデータd_iを特定されることはない。そして、一次結合データv_pをサーバ装置とは別のデータ記憶装置に記憶して管理するようにすれば、サーバ装置がデータd_iに関与するのを防止することができる。そして、クライアント装置がデータ記憶装置に記憶された一次結合データv_pを読み出してデータd_iを集計して集計値をサーバ装置に送信するようにすれば、サーバ装置には集計値のみが送信されて個別の情報に対応するデータd_iが特定されることを防止できる。
【発明を実施するための最良の形態】
【００２８】
以下、本発明に係る実施形態について詳しく説明する。なお、以下に説明する実施形態は、本発明を実施するにあたって好ましい具体例であるから、技術的に種々の限定がなさ

れているが、本発明は、以下の説明において特に本発明を限定する旨明記されていない限り、これらの形態に限定されるものではない。

【００２９】

図１は、本発明に係る情報処理システムに関する実施形態の構成を示す概略図である。管理サーバ１は、インターネット等のネットワーク４を介してＮ個のクライアント装置２$_1$、・・・、２$_N$と接続されている。管理サーバ１は、情報処理部１０及び記憶部１１を備えており、情報処理部１０が記憶部１１に記憶されたデータ及びプログラムを読み出してデータ処理を行い、クライアント装置２とデータの送受信を行うようになっている。クライアント装置２は、それぞれ情報処理部２０$_1$、・・・、２０$_N$及び記憶部２１$_1$、・・・、２１$_N$を備えており、情報処理部２０が記憶部２１に記憶されたデータ及びプログラムを読み出してデータ処理を行い、管理サーバ１とデータの送受信を行うようになっている。管理サーバ１及びクライアント装置２における個別情報処理に関する機能は、予め記録媒体やネットワークを用いてインストールされるプログラムにより実現される。

【００３０】

図２は、管理サーバ１及びクライアント装置２$_k$との間で互いに正当性を判定するための機能ブロック図を示している。管理サーバ１の情報処理部１０は、パスワード抽出部１００、第一暗号キー生成部１０１、第一暗号化処理部１０２、第二暗号キー生成部１０３、第二暗号化処理部１０４、クライアント判定部１０５及び送受信部１０６を備えており、こうした機能は、記憶部１１に記憶されたサーバ用認証プログラム１１０により実現される。記憶部１１に記憶された顧客ＤＢ１１１には、クライアント装置を利用する全利用者のＩＤ、パスワード、氏名、住所といった顧客の属性情報が登録されている。

【００３１】

パスワード抽出部１００は、クライアント装置から受信した複数のＩＤからなるＩＤリストに対応する複数のパスワードｐを記憶部１１の顧客ＤＢ１１１より抽出し、ＩＤリストの配列順序に対応したパスワードリストを作成する。

【００３２】

第一暗号キー生成部１０１は、第一暗号化処理部１０２で用いる第一暗号キーとしてパスワードｐと同じ長さのランダムビットパターンｒを生成する。第一暗号化処理部１０２は、第一暗号キーｒとパスワード抽出部１００で作成されたパスワードリストのパスワードｐとの排他的論理和ｘ

ｘ＝ｐＸＯＲｒ

をｐの暗号化情報として算出し、パスワードリストに対応した暗号パスワードリストを作成する。

【００３３】

第二暗号キー生成部１０３は、第二暗号キーＫを生成し、第二暗号化処理部１０４は、第二暗号キーＫにより第一暗号キーｒを暗号化した暗号化情報Ｋ（ｒ）を算出し、Ｋ（ｒ）及びＫをサーバ検証情報とする。暗号パスワードリスト及び暗号化情報Ｋ（ｒ）は、第二暗号キーＫとともに送受信部１０６を介してクライアント装置に送信される。第二暗号化処理部１０４では、暗号化キー及び復号化キーが異なる暗号方式を用いればよく、例えば、ＲＳＡ等の公知の暗号方式を用いて暗号化処理するようにすればよい。

【００３４】

クライアント判定部１０５は、クライアント装置からクライアント検証情報として受信したランダムビットパターンと第一暗号キー生成部１０１で生成した第一暗号キーであるランダムビットパターンｒとを照合してクライアント装置の正当性を判定する。送受信部１０６は、クライアント装置とデータの送受信を行う。

【００３５】

クライアント装置２$_k$の情報処理部２０$_k$は、ＩＤ発生部２００$_k$、パスワード処理部２０１$_k$、サーバ判定部２０２$_k$及び送受信部２０３$_k$を備えており、こうした機能は、記憶部２１$_k$に記憶されたクライアント用認証プログラム２１０$_k$により実現される。記憶部２１$_k$は、クライアント装置を利用する利用者のＩＤ$_k$及びパスワードｐ$_k$を記憶するＩＤ／

パスワード登録部２１１$_k$を備えている。

【００３６】

ＩＤ発生部２００$_k$は、記憶部２１$_k$のＩＤ／パスワード登録部２１１$_k$に登録されたＩＤ$_k$を含む複数のＩＤを発生させてＩＤリストを作成する。当該利用者のＩＤ$_k$以外のＩＤについては、全利用者のＩＤ数に基づいてランダムに発生させるようにする。

【００３７】

パスワード処理部２０１$_k$は、管理サーバ１から受信した暗号パスワードリストの中のＩＤ／パスワード登録部２１１$_k$に登録されたＩＤ$_k$の位置に相当する暗号パスワードｘとＩＤ／パスワード登録部２１１$_k$に登録されたパスワードｑとの排他的論理和ｙ

ｙ＝ｘＸＯＲｑ

を計算して、さらに、ｙを管理サーバ１から受信した第二暗号キーＫを用いて第二暗号化処理部１０４と同一の暗号方式で暗号化しＫ（ｙ）とする。

【００３８】

ここで、パスワード処理部２０１$_k$では、管理サーバ１から受信した暗号パスワードｘは、

ｘ＝ｐＸＯＲｒ

であるので、ｑ＝ｐならば、

ｙ＝ｘＸＯＲｑ＝ｐＸＯＲｒＸＯＲｐ＝ｒ・・・（Ｃ）

となり、元の第一暗号キーｒが復号化される。例えば、

ｐ＝００１１００

ｒ＝０１１０００

である場合

ｘ＝０１０１００

となる。したがって、

ｘＸＯＲｐ＝０１１０００＝ｒ

となる。

【００３９】

サーバ判定部２０２$_k$は、管理サーバ１から受信した暗号化されたランダムビットパターンＫ（ｒ）及びパスワード処理部２０１$_k$で計算したＫ（ｙ）をパターン比較して一致するか否か判定する。一致すると判定された場合には、管理サーバ１は正当なものとしてパスワード処理部２０１$_k$で計算したランダムビットパターンｙ（＝ｒ）を管理サーバ１に送信し、一致しない場合には、管理サーバ１は不正なものとしてランダムビットパターンは送信しない。

【００４０】

図３は、管理サーバ１及びクライアント装置２$_k$との間で互いに正当性を判定する処理フローを示している。まず、クライアント装置２$_k$は、認証処理を行う場合、全利用者のＩＤからランダムに（Ｎ－１）個のＩＤを発生させる（Ｓ１００）。複数のＩＤを発生させる場合、例えば、予め記憶部２１$_k$に全利用者のＩＤ総数が記憶されており、ＩＤ総数の連続番号の中からランダムに選択するようにすればよい。そして、クライアント装置２$_k$に登録された利用者のＩＤ$_k$を記憶部２１$_k$から読み出して、発生させた複数のＩＤとともにランダムに配列させてＮ個のＩＤからなるＩＤリストを作成する（Ｓ１０１）。図４は、ＩＤリストの一例を示す。この例では、ｔ番目に利用者のＩＤ$_k$が設定されている。

【００４１】

作成されたＩＤリストを管理サーバ１に送信して、リスト中のＮ個のＩＤに対応するパスワードを記憶部１１から抽出する（Ｓ１０２）。そして、抽出したパスワードをＩＤリストの配列に従って配列してパスワードリストを作成する（Ｓ１０３）。図５は、図４のＩＤリストに基づいて作成されたパスワードリストを示している。パスワードリストのｔ番目には、利用者のパスワードｐ$_k$がリストアップされている。

【００４２】

次に、第一暗号キーであるランダムビットパターンｒを発生させて（Ｓ１０４）、パス

ワードリストのパスワードとランダムビットパターンｒとの排他的論理和ｘを算出する（Ｓ１０５）。パスワードリストの各パスワードについて排他的論理和ｘを算出したら、パスワードリストの配列に従って配列して暗号パスワードリストを作成する（Ｓ１０６）。図６は、図５のパスワードリストに基づいて作成された暗号パスワードリストを示している。暗号パスワードリストのｔ番目の排他的論理和$ｘ_k$が利用者のパスワード$ｐ_k$に対応する。

【００４３】

ここで、利用者が$ｐ_k$以外のパスワードを直接知るのを防ぐ目的で、パスワードリストの各パスワードをランダムビットパターンｒとの排他的論理和ｘを計算する前又は後で、暗号化しておいてもよい。ただし、この場合には、クライアント装置２_kが$ｐ_k$あるいは$ｐ_k$及びｒの排他的論理和ｘを暗号化した情報が計算できるように、クライアント装置２_kでも管理サーバ１と同じ暗号キーと暗号化機構を備える必要がある。この場合の暗号化方式は、当然暗号キーと復号キーとが異なるものでなければならない。

【００４４】

次に、第二暗号キー生成部１０３において第二暗号キーＫを生成し（Ｓ１０７）、第二暗号キーＫを用いてランダムビットパターンｒを暗号化処理して（Ｓ１０８）、第二暗号キーＫ、暗号化されたランダムビットパターンＫ（ｒ）及び暗号パスワードリストをクライアント装置２_kに送信する（Ｓ１０９）。

【００４５】

クライアント装置２_kでは、受信した暗号パスワードリストの中からｔ番目の排他的論理和$ｘ_k$を抽出して（Ｓ１１０）、記憶部２１_kに登録された利用者のパスワード$ｐ_k$との排他的論理和を算出する（Ｓ１１１）。ステップＳ１１１での算出処理により、式（Ｃ）に示すように、ランダムビットパターンｙが算出されるので、算出されたランダムビットパターンを第二暗号キーＫを用いて暗号化処理する（Ｓ１１２）。暗号化されたランダムビットパターンＫ（ｙ）を管理サーバ１から受信したランダムビットパターンＫ（ｒ）と比較して（Ｓ１１３）管理サーバ１の正当性を判定する。一致する場合には、管理サーバ１がクライアント装置２_kから受信したＩＤリストのすべてのＩＤとランダムビットパターンｒとの排他的論理和を正しく計算したことになり、正当な管理サーバであると判定することができる。そこで、ステップＳ１１１で算出したランダムビットパターンｙを管理サーバ１に送信する（Ｓ１１４）。ステップＳ１１３において両者が一致しない場合には管理サーバは不正なものであると判定してランダムビットパターンｙを送信せず終了する。

【００４６】

管理サーバ１は、受信したランダムビットパターンｙをステップＳ１０４で発生させたランダムビットパターンｒと比較して（Ｓ１１５）クライアント装置２_kの正当性を判定する。一致する場合には、管理サーバ１から送信した暗号パスワードリストに含まれるパスワードを用いてクライアント装置２_kが処理したと認証できるため、クライアント装置２_kに対してサービス提供を開始する。一致しない場合には、クライアント装置２_kは、暗号パスワードリストに含まれるパスワードを用いて処理していないことから、不正なものとしてエラーメッセージを送信して（Ｓ１１６）終了する。

【００４７】

以上の処理では、クライアント装置２_kからＩＤリストを送信しているので、管理サーバ１ではどのＩＤの利用者がアクセスしてきているのか特定することはなく、利用者の正当性を確認できる。そして、クライアント装置２_kでは、管理サーバ１から送信されたランダムビットパターンＫ（ｒ）と自身が計算したＫ（ｙ）とが一致することを確かめることにより、管理サーバ１が正しく処理していることを確認することができる。この場合、クライアント装置に他の利用者のパスワードが送信されるが、パスワード若しくはパスワードとランダムビットパターンとの排他的論理和も暗号キーと復号キーとが異なる暗号方式によって暗号化することで、復号化には別のキーが必要となるので、クライアント装置での不正な利用は簡単に防止できる。同様に、管理サーバ１で用いたランダムビットパタ

ーンｒの暗号化も暗号キーと復号キーとが異なる暗号方式によって行われるので、暗号化されたランダムビットパターンＫ（ｒ）を直接復号化して管理サーバに送信するといった不正な処理も防止される。すなわち、真正なパスワードがないとクライアント装置ではランダムビットパターンｒを復号化することができない。

【００４８】

そして、暗号パスワードリストでは共通のランダムビットパターンｒを用いてパスワードを処理しているので、暗号パスワードリストの何番目のパスワードが復号化されたかについても管理サーバ１では特定されない。また、管理サーバ１では、クライアント装置2_kから受信したランダムビットパターンｙにより正当性を判定するので、利用者を特定することなく認証を行うことができる。

【００４９】

図７は、図１の情報処理システムを用いて個別情報を集計するためのシステムに関する機能ブロック図を示している。Ｎ個のクライアント装置2_1、・・・、2_Nがそれぞれデータ管理装置S_1、・・・、S_Nとして機能し、管理サーバ１がデータ集計装置Ｃとして機能する。

【００５０】

各データ管理装置は、情報処理部20_1、・・・、20_N及び記憶部21_1、・・・、21_Nを備えており、情報処理部２０は、データ抽出部、結合計算部及び結合集計部として機能し、こうした機能は、各記憶部21_kにそれぞれ記憶されたデータ管理プログラムにより実現される。各記憶部21_kには、係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）及び各データ管理装置が集計を担当する順番を登録した担当データテーブルがそれぞれ記憶されている。また、記憶部21_1には、Ｍ個のデータ項目D_i（i=1,2,…,M）に対応する数値化された個人データd_{i1}（i=1,2,…,M）が記憶されており、同様に記憶部21_2には、個人データd_{i2}（i=1,2,…,M）、・・・、記憶部21_kには、個人データd_{ik}（i=1,2,…,M）、・・・、記憶部21_Nには、個人データd_{iN}（i=1,2,…,M）がそれぞれ記憶されている。

【００５１】

情報処理部20_kの機能について説明すると、データ抽出部は、記憶部21_kから必要に応じて係数データa_{pq}及び個人データd_{ik}を抽出する。結合計算部は、抽出された個人データd_{ik}及び係数データa_{pq}を用いてＭ個の一次結合データv_{pk}（p=1,2,…,M）を以下の式（Ａ）により計算する。

$$v_{pk}=a_{p1}d_{1k}+a_{p2}d_{2k}+\cdots+a_{pq}d_{qk}+\cdots+a_{pM}d_{Mk} \quad \cdots（A）$$

結合集計部は、全データ管理装置の結合計算部で計算したＭ×Ｎ個の一次結合データv_{ps}（p=1,2,…,M;s=1,2,…,N）を順番ｐ別に全データ管理装置で算出された値の集計を行う。どの順番の一次結合データv_{ps}の集計をどのデータ管理装置で担当するかは担当データテーブルに予め登録されている。１つのデータ管理装置が複数の順番の一次結合データを担当してもよい。そして、結合集計部は、担当データテーブルのデータに基づいて当該装置の担当の順番以外のデータを他のデータ管理装置に送信すると共に担当の順番のデータを他のデータ管理装置から受信して集計を行う。順番ｒの一次結合データv_{rs}（1≦r≦M;s=1,2,…,N）を集計する場合、結合集計データV_rは、以下のとおりとなる。

$$V_r=v_{r1}+v_{r2}+\cdots+v_{rs}+\cdots+v_{rN}=a_{r1}\Sigma d_{1s}+a_{r2}\Sigma d_{2s}+\cdots+a_{rq}\Sigma d_{qs}+\cdots+a_{rM}\Sigma d_{Ms}$$

したがって、結合集計データV_rは、各データ項目D_i（i=1,2,…,M）別の集計値Σd_{ij}を変数とし係数データa_{pq}を用いた連立一次方程式の右辺値になる。結合集計部は、こうして算出された結合集計データV_p（p=1,2,…,M）をデータ集計装置Ｃに送信する。

【００５２】

データ集計装置Ｃは、情報処理部１０及び記憶部１１を備えており、情報処理部１０は、結合データ集計部及び集計データ算出部として機能し、こうした機能は、記憶部１１に記憶されたデータ集計プログラムにより実現される。また、記憶部１１には、係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）が記憶されている。

【００５３】
情報処理部１０の結合データ集計部は、各データ管理装置からＭ個の結合集計データ$Ｖ_{p}$を受信する。集計データ算出部は、受信されたＭ個の結合集計データ$Ｖ_{p}$及び記憶部１１に記憶された係数データ$ａ_{pq}$に基づいて、Ｍ個の$Σｄ_{ij}$を変数として係数データ$ａ_{pq}$を用いたＭ個の連立一次方程式を解くことによりデータ項目$Ｄ_{i}$別の集計値$Σｄ_{ij}$を算出することができる。
【００５４】
したがって、データ集計装置Ｃは、データ項目$Ｄ_{i}$別の集計値$Σｄ_{ij}$を用いて平均値を算出するといった統計処理を行うことができる。また、データ項目として個人データの２乗値を加えることで、分散及び共分散といった処理を行うことも可能となる。さらに、データが所定範囲に含まれる場合に１、含まれない場合に０とするようなデータ項目を設定することで、特定範囲の出現頻度を計算することもできる。
【００５５】
また、アンケート調査の回答項目を数値化すれば、アンケート結果の集計を行うことも容易に行うことができる。さらに、選挙の投票票数の集計にも用いることが可能である。
【００５６】
そして、データ集計装置Ｃは、結合集計データ$Ｖ_{p}$しか得ることがないので、個人データ$ｄ_{ij}$を特定することはできない。そのため、データ管理装置から個別情報を特定されることなく集計データを外部に送信することが可能となり、個別情報が特定されることなくその集計を行うことができる。また、各データ管理装置は、他のデータ管理装置の一部の一次結合データしか得ることができないため、他のデータ管理装置の個人データを知ることはできない。すなわち、各データ管理装置には、係数データ$ａ_{pq}$が記憶されているものの一次結合データをすべて得ることができないと、個人データを変数とする連立一次方程式を解くことができないため、個人データが特定されることはない。
【００５７】
図８は、図１の情報処理システムを用いて、図２に示す管理サーバ１及びクライアント装置２_{k}との間で互いに正当性を判定するための機能を持たせるとともに、両者の間で取引される情報を図７で説明した手法を利用してクライアント装置２_{k}に関する個別の取引情報が管理サーバ１に特定されないように取引情報を集計するためのシステムに関する機能ブロック図を示している。図８では、図１に示す情報処理システムに、データ記憶装置３がネットワークに接続されている。
【００５８】
管理サーバ１の情報処理部１０は、アクセス処理部１０７、取引処理部１０８、集計処理部１０９及び送受信部１０６を備えており、こうした機能は、記憶部１１に記憶されたサーバ用取引処理プログラム１１２により実現される。記憶部１１に記憶された顧客ＤＢ１１１には、クライアント装置を利用する全利用者のＩＤ、パスワード、氏名、住所といった顧客の属性情報が登録されている。記憶部１１に記憶された取引集計登録部１１３には、クライアント装置２_{k}から受信した個々の取引情報に関する集計値が登録されている。
【００５９】
アクセス処理部１０７は、図２において説明した互いの正当性を判定するための管理サーバ１の各処理部の機能を備えるもので、図２と同一の機能であるから説明は省略する。そして、アクセス処理部１０７は、正当性ありと判定された場合に後述するデータ記憶装置３に対して書き込み許可を指示する。
【００６０】
取引処理部１０８は、クライアント装置２_{k}との間で取引に関する情報処理を行い、個別の取引情報をクライアント装置２_{k}に対して送信する。
【００６１】
集計処理部１０９は、所定期間又は所定取引回数毎にクライアント装置２_{k}に集計指示信号を送信するとともにデータ記憶装置３に対して読出し許可を指示する。そして、クラ

イアント装置2_kから送信される集計値を処理して取引集計登録部１１３に記憶する。

【００６２】

クライアント装置2_kの情報処理部20_kは、アクセス処理部204_k、取引処理部205_k、結合計算部206_k、取引集計部207_k及び送受信部203_kを備えており、こうした機能は、記憶部21_kに記憶されたクライアント用取引処理プログラム212_kにより実現される。記憶部21_kは、管理サーバ１との間で取引処理された個別の取引情報を示す複数のデータd_i及び後述する係数データa_{pq}を記憶する個別取引登録部213_kを備えている。個別の取引情報を示す複数のデータd_iとしては、例えば、取引日時、取引相手、取引量、取引金額といったものが挙げられる。そして、こうした情報は、０と１の２進数としてデータ化されている。

【００６３】

アクセス処理部204_kは、図２において説明した互いの正当性を判定するためのクライアント装置2_kの各処理部の機能を備えるもので、図２と同一の機能であるから説明は省略する。

【００６４】

取引処理部205_kは、管理サーバ１との間で取引に関する情報処理を行い、個別の取引情報を示す複数のデータd_iを個別取引登録部213_kに登録する。

【００６５】

結合計算部206_kは、個別取引登録部213_kに登録された個別の取引情報を示すM個のデータd_i（i=1,2,…,M）及び係数データa_{pq}（p=1,2,…,M;q=1,2,…,M）を用いてM個の一次結合データv_p（p=1,2,…,M）を以下の式（Ｂ）

$$v_p = a_{p1}d_1 + a_{p2}d_2 + \cdots + a_{pq}d_i + \cdots + a_{pM}d_M \cdots (B)$$

により算出する。こうして算出されたM個の一次結合データv_pは、係数データa_{pq}が知られない限り、M個のデータd_iを知ることはきわめて困難なため、一次結合データv_pを外部に送信しても個別の取引情報の内容を知られることが防止できる。算出された一次結合データv_pは、データd_iに代えてデータ記憶装置３に送受信部203_kを介して送信されて記憶される。

【００６６】

取引集計部207_kは、所定期間又は所定の取引回数毎にデータ記憶装置３に記憶された一次結合データv_pを読み出して個別の取引情報であるデータd_iを集計して、管理サーバ１に送信する。集計する場合、N個の取引情報に対応する一次結合データv_{ps}（p=1,2,…,M；s=1,2,…,N）の順番ｒの一次結合データv_{rs}（1≦r≦M;s=1,2,…,N）を集計して結合集計データV_rを算出する。結合集計データV_rは、以下のとおりとなる。

$$V_r = v_{r1} + v_{r2} + \cdots + v_{rs} + \cdots + v_{rN} = a_{r1}\Sigma d_{1s} + a_{r2}\Sigma d_{2s} + \cdots + a_{rq}\Sigma d_{qs} + \cdots + a_{rM}\Sigma d_{Ms}$$

したがって、結合集計データV_rは、データd_{is}（i=1,2,…,M；s=1,2,…,N）の集計値Σd_{is}を変数とし係数データa_{pq}を用いた連立一次方程式の右辺値になる。取引集計部207_kは、個別取引登録部213_kに登録された係数データa_{pq}を読み出し、算出されたM個の結合集計データV_p（p=1,2,…,M）に基づいて連立一次方程式を解き、集計値Σd_{is}を求める。そして、例えば、取引金額及び取引量に関する集計値を管理サーバ１に送受信部203_kを介して送信する。

【００６７】

データ記憶装置３の情報処理部３０は、登録処理部３０１、読出処理部３０２及び送受信部３０３を備えており、記憶部３１には、結合情報登録部３１０が記憶されている。登録処理部３０１は、管理サーバ１から書き込み許可を受けて、クライアント装置2_kから送信された一次結合データv_pを結合情報登録部３１０に登録処理する。読出処理部３０２は、管理サーバ１から読出し許可の指示を受けて、所定期間又は所定取引回数毎の一次結合データv_pをクライアント装置2_kに送信する。

【００６８】

データ記憶装置３は、管理サーバ１から書き込み許可及び読み出し許可を受けてクライ

アント装置2_kとの間で登録処理や読出し処理を行なうものの、管理サーバ１との間ではデータの読出し処理ができないようにされている。また例え不正に読み出した場合でもその内容は係数データa_{pq}を知っていなければわからない。したがって、管理サーバ１は、データ記憶装置３とクライアント装置2_kとの間でのデータのやり取りには関与できないようになっている。

【００６９】

図９は、クライアント装置2_kに関する取引情報をデータ記憶装置３に記憶するための処理フローを示している。まず、管理サーバ１とクライアント装置2_kとの間で互いの正当性を判定するためのアクセス処理が行われる（Ｓ２００、Ｓ２０１）。このアクセス処理は、図３と同様であるので、説明は省略する。互いに正当性ありと判定されると、クライアント装置2_kは、取引処理依頼を管理サーバ１に対して送信し（Ｓ２０２）、管理サーバ１は取引処理を行う（Ｓ２０３）。管理サーバ１は、取引処理が終了すると取引情報を生成してクライアント装置2_kに送信する（Ｓ２０４）。クライアント装置2_kは、受信した取引情報をいったん個別取引登録部213_kに登録し（Ｓ２０５）、取引情報を示すデータd_iに基づいて一次結合データv_pを算出する（Ｓ２０６）。一方、管理サーバ１は、書き込み許可をデータ記憶装置３に送信し、データ記憶装置３は、書き込み許可に従いクライアント装置2_kから送信された一次結合データv_pを記憶する（Ｓ２０８）。

【００７０】

図１０は、データ記憶装置３から一次結合データv_pを読み出して集計を行なうための処理フローを示している。まず、管理サーバ１は、クライアント装置2_kに対して集計指示を送信し（Ｓ３００）、データ記憶装置３に対して読出し許可を送信する（Ｓ３０１）。クライアント装置2_kは、集計指示を受信するとデータ記憶装置３に対して一次結合データの読出し依頼を送信する（Ｓ３０２）。データ記憶装置３は、読出し許可を受けクライアント装置2_kから読出し依頼を受けて所定期間又は所定取引回数の間の取引情報に対応する一次結合データv_pを読み出してクライアント装置2_kに送信する（Ｓ３０３）。クライアント装置2_kは、受信した一次結合データv_pに基づいて上述したように結合集計データV_rを算出して集計値Σd_{is}を求めて管理サーバ１に送信する（Ｓ３０４）。管理サーバ１は、受信した集計値Σd_{is}を取引集計登録部１１３に登録し、以後集計データに基づいて課金処理等を行なう。

【００７１】

以上のように、データ記憶装置３に一次結合データv_pに変換して取引情報を示すデータd_iを記憶しておくことで、クライアント装置2_kの個別の取引情報が外部に知られることなく、クライアント装置2_kの取引情報として特定されることもない。また、データ記憶装置３は、管理サーバ１により書き込み及び読出しを管理されているので、クライアント装置2_kが勝手にデータ記憶装置３にアクセスしてデータを改ざんすることを防止できる。

【００７２】

なお、クライアント装置2_kが偽りの取引情報を登録するといった不正行為を防止するために、クライアント装置2_kの取引累積回数や取引時刻といった情報も取引情報に組み合せておき、必要に応じて取引内容をチェックできるようにしてもよい。

【産業上の利用可能性】

【００７３】

このように、本発明に係る情報処理システムは、互いに信用できない主体同士が個別情報を送受信する際に、その個別情報が特定されないように送受信されるので、情報を送信する側にとっては安心して外部に情報を出すことができ、情報を受信する側にとっては情報を厳格に管理する負担が軽減される。

【００７４】

特に、今後ユキュビタス・コンピューティングの進展により企業のみならず家庭内にもネットワークが普及してくることが想定されるが、本発明に係る情報処理システムでは、複雑なシステム構成を用いることなく個別情報が特定できないようにすることができ、ユ

キュビタス・コンピューティングに用いられる様々な情報機器に適用することが可能となる。

【００７５】

また、ある業種に所属する複数の企業における従業員の給与の全体平均値を計算する場合、特定の母集団の特定の病気の感染数を調査したい場合、特定の母集団の身長、体重の分布を調査したい場合などには、これまで統計調査を行う団体に個人の給与、病歴情報又は身体情報を開示する必要があったが、本発明に係る個別情報処理システムでは、こうした個別情報が特定されることなく統計処理を容易に行うことができる。

【図面の簡単な説明】

【００７６】

【図１】本発明に係る情報処理システムに関する実施形態の構成を示す概略図である。

【図２】管理サーバ及びクライアント装置の間の正当性を判定するための機能ブロック図である。

【図３】管理サーバ及びクライアント装置の間の正当性を判定するための処理フローである。

【図４】ＩＤリストに関する説明図である。

【図５】パスワードリストに関する説明図である。

【図６】暗号パスワードリストに関する説明図である。

【図７】個別情報を集計するための情報処理システムに関する機能ブロック図である。

【図８】個別の取引情報が管理サーバに特定されないように取引情報を集計するための情報処理システムに関する機能ブロック図である。

【図９】個別の取引情報が管理サーバに特定されないように取引情報を登録するための処理フローである。

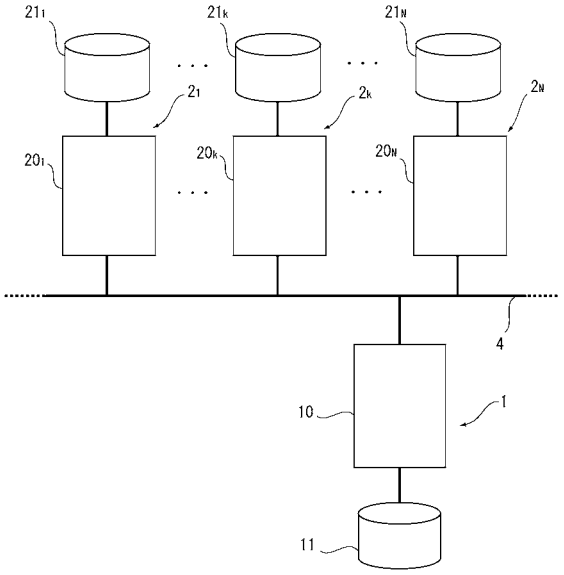
【図１０】個別の取引情報が管理サーバに特定されないように取引情報を集計するための処理フローである。

【符号の説明】

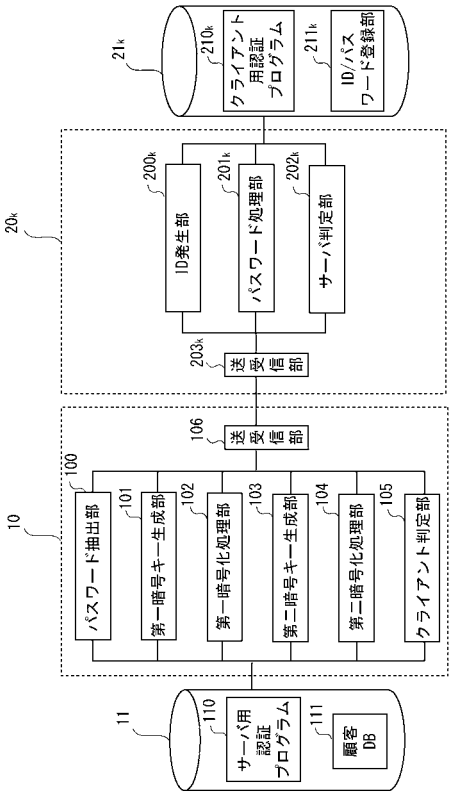
【００７７】

１　管理サーバ
２　クライアント装置
３　データ記憶装置
４　ネットワーク
10　情報処理部
11　記憶部
20　情報処理部
21　記憶部
30　情報処理部
31　記憶部

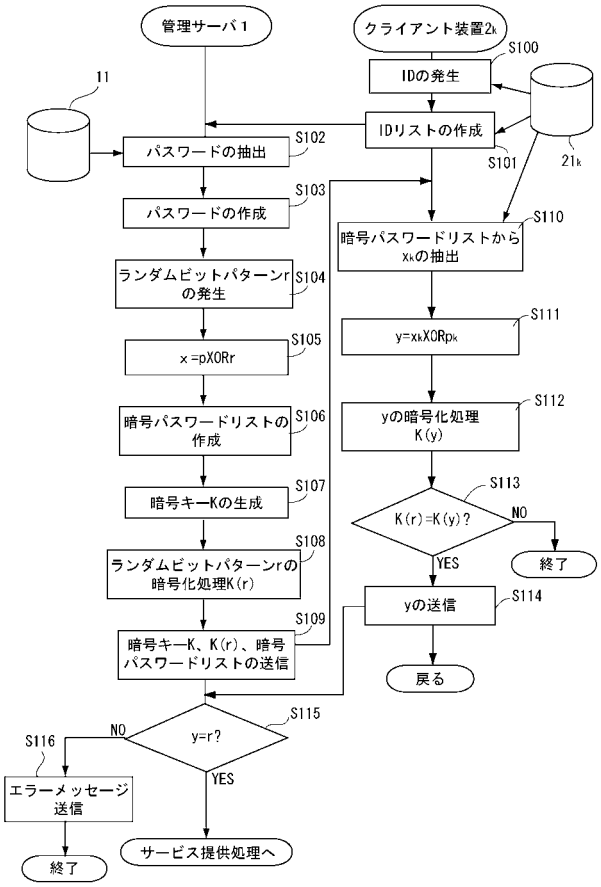
【図１】



【図２】



【図３】



【図４】

1	ID₁
2	ID₅
・	・
・	・
t	IDk
・	・
・	・
N	IDm

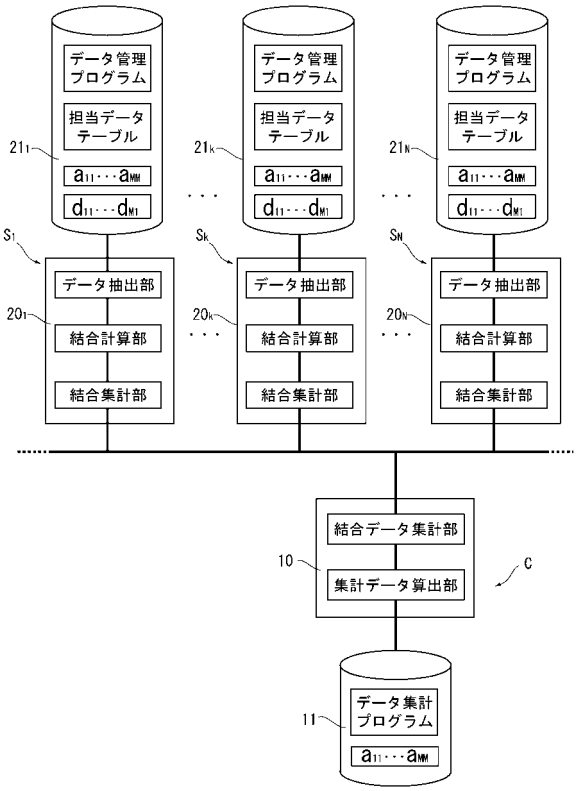
【図５】

1	p₁
2	p₅
・	・
・	・
t	pk
・	・
・	・
N	pm

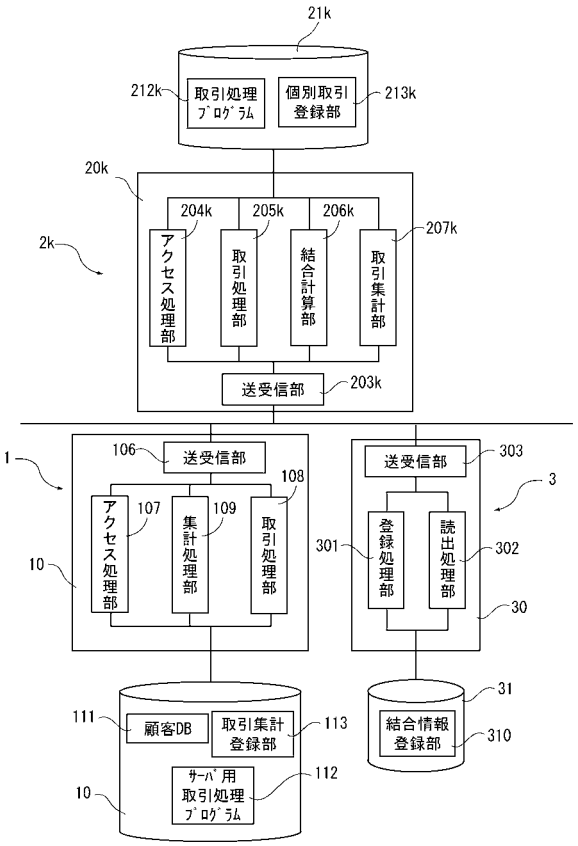
【図６】

1	x_1
2	x_5
・	・
・	・
・	・
t	x_k
・	・
・	・
・	・
N	x_m

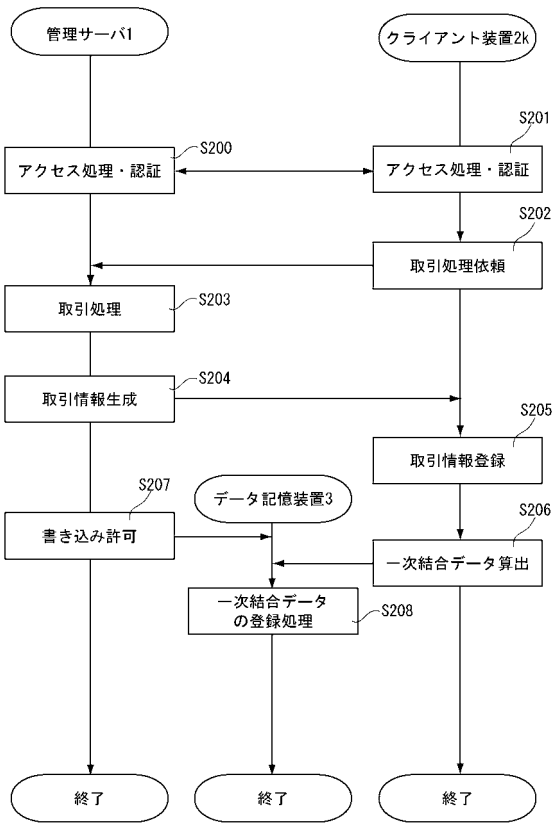
【図７】



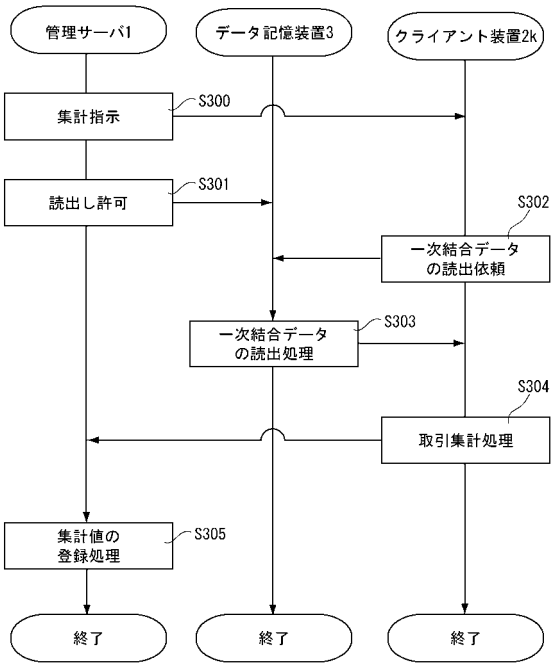
【図８】



【図９】



【図１０】


管理サーバ1
データ記憶装置3
クライアント装置2k
集計指示
S300
読出し許可
S301
S302
一次結合データ
の読出依頼
一次結合データ
の読出処理
S303
S304
取引集計処理
集計値の
登録処理
S305
終了
終了
終了

フロントページの続き

(56)参考文献 国際公開第２００４／０９５７７３（WO，Ａ２）
特開２００５－５７７８（ＪＰ，Ａ）
岡博文，北川隆，椙勇一，“大学における講義評価のための匿名アンケートシステムについて”，コンピュータセキュリティシンポジウム２００１論文集，日本，社団法人情報処理学会，２００１年１０月３１日，Ｖｏｌ．２００１，Ｎｏ．１５，ｐ．３６１－３６６
Shinsuke Tamura, Tatsuro Yanase, “Information Sharing among Untrustworthy Entities”, 電気学会論文誌Ｃ 電子・情報・システム部門誌，日本，社団法人電気学会，２００５年１１月 1日，Ｖｏｌ．１２５，Ｎｏ．１１ ２００５，ｐ．１７６７－１７７２
Shinsuke Tamura, Kazuya Kouro, and Tatsuro Yanase, “Expenditure Limits in Anonymous Credit Card Systems”, Systems, Man and Cybernetics, 2006.SMC '06. IEEE International Conference on, ２００６年１０月 8日, p.1238-1243, ＵＲＬ, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4274018

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２