

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2006-279595
(P2006-279595A)

(43) 公開日 平成18年10月12日(2006.10.12)

(51) Int. Cl. F I テーマコード(参考)
H04L 9/32 (2006.01) H04L 9/00 675A 5J104

審査請求有 請求項の数 11 O L (全 21 頁)

(21) 出願番号	特願2005-96400 (P2005-96400)	(71) 出願人	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
(22) 出願日	平成17年3月29日(2005.3.29)	(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
		Fターム(参考)	5J104 AA07 KA02 KA04 PA07

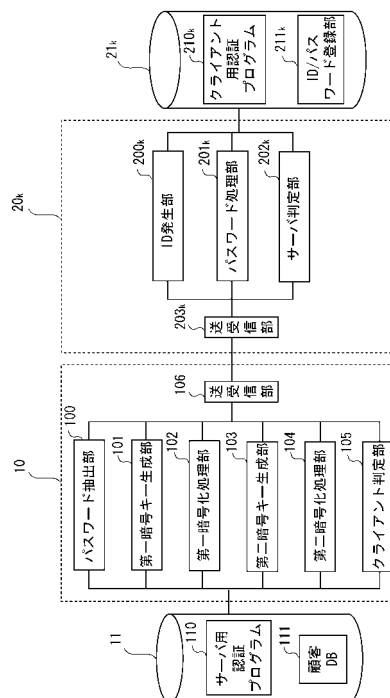
(54) 【発明の名称】 情報処理システム及びそのプログラム

(57) 【要約】

【課題】本発明は、互いに信用できない主体間において個別情報として特定されないように情報を送受信・処理・記録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。

【解決手段】クライアント装置2の利用者のIDを含む複数のIDを発生させて管理サーバ1に送信し、複数のIDに対応するパスワードを管理サーバ1で抽出するとともに暗号キーrを発生させ、抽出されたパスワードを暗号キーrとの排他的論理和xを計算して暗号化処理し、暗号キーKを発生させて暗号キーrを暗号化し暗号キーKとともにクライアント装置2に送信する。クライアント装置2では、利用者のパスワードと排他的論理和xとの排他的論理和を計算し暗号キーを復号化する。復号化した暗号キーを暗号キーKで暗号化して暗号キーrの暗号化情報と比較して管理サーバ1の正当性を判定する。一致した場合には復号化した暗号キーを管理サーバ1に送信してクライアント装置2の正当性を判定する。

【選択図】 図2



【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、

10

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。

20

【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。

30

40

【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

50

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、

10

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。

20

【請求項 6】

M 個の項目 D_i ($i=1, 2, \dots, M$) に対応するデータ d_{ij} ($i=1, 2, \dots, M; j=1, 2, \dots, N$) を記憶する N 個のデータ管理装置 S_j ($j=1, 2, \dots, N$) 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} ($p=1, 2, \dots, M; q=1, 2, \dots, M$) 及び M 個のデータ d_{ik} ($i=1, 2, \dots, M$) 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} ($p=1, 2, \dots, M$) を以下の式 (A)

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

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} ($1 \leq r \leq M; j=1, 2, \dots, N$) 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、

30

データ集計装置は、前記係数データ a_{pq} ($p=1, 2, \dots, M; q=1, 2, \dots, M$) 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】

40

M 個の項目 D_i ($i=1, 2, \dots, M$) に対応するデータ d_{ij} ($i=1, 2, \dots, M; j=1, 2, \dots, N$) を記憶する N 個のデータ管理装置 S_j ($j=1, 2, \dots, N$) 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} ($p=1, 2, \dots, M; q=1, 2, \dots, M$) 及び M 個のデータ d_{ik} ($i=1, 2, \dots, M$) を用いて M 個の一次結合データ v_{pk} ($p=1, 2, \dots, M$) を以下の式 (A)

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

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} ($1 \leq r \leq M; j=1, 2, \dots, N$)

50

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 ($i=1, 2, \dots, M$) に対応するデータ d_{ij} ($i=1, 2, \dots, M; j=1, 2, \dots, N$) を記憶する N 個のデータ管理装置 S_j ($j=1, 2, \dots, N$) 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、

10

係数データ a_{pq} ($p=1, 2, \dots, M; q=1, 2, \dots, M$) 及び M 個のデータ d_{ik} ($i=1, 2, \dots, M$) を用いて M 個の一次結合データ v_{pk} ($p=1, 2, \dots, M$) を以下の式 (A)

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

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} ($1 \leq r \leq M; j=1, 2, \dots, N$) 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、

20

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} ($p=1, 2, \dots, M; q=1, 2, \dots, M$) 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 ($i=1, 2, \dots, M$) 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 ($p=1, 2, \dots, M$) を以下の式 (B)

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

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、

30

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、

40

前記クライアント装置に記憶された係数データ a_{pq} ($p=1, 2, \dots, M; q=1, 2, \dots, M$) 及び前記特定情報に関する M 個のデータ d_i ($i=1, 2, \dots, M$) を用いて M 個の一次結合データ v_p ($p=1, 2, \dots, M$) を以下の式 (B)

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

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

50

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 ($i=1,2,\dots,M$)及び係数データ a_{pq} ($p=1,2,\dots,M; q=1,2,\dots,M$)を用いてM個の一次結合データ v_p ($p=1,2,\dots,M$)を以下の式(B)

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

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、当該システムに係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。

10

【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。

20

【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

30

【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。

40

【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

50

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。

10

20

【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。

30

【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

40

50

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。

10

【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 ($i=1,2,\dots,M$)に対応するデータ d_{ij} ($i=1,2,\dots,M; j=1,2,\dots,N$)を記憶するN個のデータ管理装置 S_j ($j=1,2,\dots,N$)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} ($p=1,2,\dots,M; q=1,2,\dots,M$)及びM個のデータ d_{ik} ($i=1,2,\dots,M$)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} ($p=1,2,\dots,M$)を以下の式(A)

20

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

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} ($1 \leq r \leq M; j=1,2,\dots,N$)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} ($p=1,2,\dots,M; q=1,2,\dots,M$)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。

30

【0017】

本発明に係る別の情報処理方法は、M個の項目 D_i ($i=1,2,\dots,M$)に対応するデータ d_{ij} ($i=1,2,\dots,M; j=1,2,\dots,N$)を記憶するN個のデータ管理装置 S_j ($j=1,2,\dots,N$)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} ($p=1,2,\dots,M; q=1,2,\dots,M$)及びM個のデータ d_{ik} ($i=1,2,\dots,M$)を用いてM個の一次結合データ v_{pk} ($p=1,2,\dots,M$)を以下の式(A)

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

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} ($1 \leq r \leq M; j=1,2,\dots,N$)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。

40

【0018】

本発明に係る別のプログラムは、M個の項目 D_i ($i=1,2,\dots,M$)に対応するデータ d_{ij} ($i=1,2,\dots,M; j=1,2,\dots,N$)を記憶するN個のデータ管理装置 S_j ($j=1,2,\dots,N$)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

50

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} ($p=1,2,\dots,M$; $q=1,2,\dots,M$) 及び M 個のデータ d_{ik} ($i=1,2,\dots,M$) を用いて M 個の一次結合データ v_{pk} ($p=1,2,\dots,M$) を以下の式 (A)

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

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} ($1 \leq r \leq M$; $j=1,2,\dots,N$) 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。

10

【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} ($p=1,2,\dots,M$; $q=1,2,\dots,M$) 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 ($i=1,2,\dots,M$) 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 ($p=1,2,\dots,M$) を以下の式 (B)

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

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。

20

【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} ($p=1,2,\dots,M$; $q=1,2,\dots,M$) 及び前記特定情報に関する M 個のデータ d_i ($i=1,2,\dots,M$) を用いて M 個の一次結合データ v_p ($p=1,2,\dots,M$) を以下の式 (B)

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

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。

40

【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 ($i=1,2,\dots,M$) 及び係数データ a_{pq} ($p=1,2,\dots,M$; $q=1,2,\dots,M$) を用いて M 個の一次結合データ v_p ($p=1,2,\dots,M$) を以下の式 (B)

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

50

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。

10

【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。

20

【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} ($p=1,2,\dots,M; q=1,2,\dots,M$)及びM個のデータ d_{ik} ($i=1,2,\dots,M$)を用いてM個の一次結合データ v_{pk} ($p=1,2,\dots,M$)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} ($1 \leq r \leq M; j=1,2,\dots,N$)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。

30

40

【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} ($1 \leq r \leq M; s=1,2,\dots,N$)を集計した結合集計データ V_r は、以下のとおりとなる。

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

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 d_{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

50

i 別の集計値 d_{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 ($p=1, 2, \dots, M$) を以下の式 (B)

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

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 、
 \dots 、 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 、 \dots 、 20_N 及び記憶部 21_1 、 \dots 、
 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1
00、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

$$x = p \text{ XOR } r$$

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。

10

【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。

20

【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

$$y = x \text{ XOR } q$$

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。

30

【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、

$$x = p \text{ XOR } r$$

であるので、 $q = p$ ならば、

$$y = x \text{ XOR } q = p \text{ XOR } r \text{ XOR } p = r \cdots (C)$$

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、

$$x \text{ XOR } p = 011000 = r$$

となる。

40

【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

50

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よければよい。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。

10

【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。

20

【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。

30

【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る、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

40

50

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。

10

【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認することにより、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。

20

【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。

30

【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 、 \dots 、 2_N がそれぞれデータ管理装置 S_1 、 \dots 、 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 、 \dots 、 20_N 及び記憶部 21_1 、 \dots 、 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} ($p=1,2,\dots,M; q=1,2,\dots,M$)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 ($i=1,2,\dots,M$)に対応する数値化された個人データ d_{i1} ($i=1,2,\dots,M$)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} ($i=1,2,\dots,M$)、 \dots 、記憶部 21_k には、個人データ d_{ik} ($i=1,2,\dots,M$)、 \dots 、記憶部 21_N には、個人データ d_{iN} ($i=1,2,\dots,M$)がそれぞれ記憶されている。

40

【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} ($p=1,2,\dots,M$)を以下の

50

式 (A) により計算する。

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

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 $M \times N$ 個の一次結合データ V_{ps} ($p=1, 2, \dots, M; s=1, 2, \dots, N$) 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} ($1 \leq r \leq M; s=1, 2, \dots, N$) 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。

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

したがって、結合集計データ V_r は、各データ項目 D_i ($i=1, 2, \dots, M$) 別の集計値 d_{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 ($p=1, 2, \dots, M$) 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} ($p=1, 2, \dots, M; q=1, 2, \dots, M$) 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 d_{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 d_{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 d_{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ができない。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

10

20

30

40

50

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 ($i=1,2,\dots,M$)及び係数データ a_{pq} ($p=1,2,\dots,M; q=1,2,\dots,M$)を用いてM個の一次結合データ v_p ($p=1,2,\dots,M$)を以下の式(B)

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

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

10

20

30

40

50

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} ($p=1, 2, \dots, M; s=1, 2, \dots, N$) の順番 r の一次結合データ v_{rs} ($1 \leq r \leq M; s=1, 2, \dots, N$) 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。

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

したがって、結合集計データ V_r は、データ d_{is} ($i=1, 2, \dots, M; s=1, 2, \dots, N$) の集計値 d_{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 ($p=1, 2, \dots, M$) に基づいて連立一次方程式を解き、集計値 d_{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。

10

【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。

20

【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)。

30

【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毎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 d_{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 d_{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。

40

【0071】

50

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わせておき、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。

10

【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、今後ユキュピタス・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、ユキュピタス・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。

20

【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】

30

【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。

40

【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】

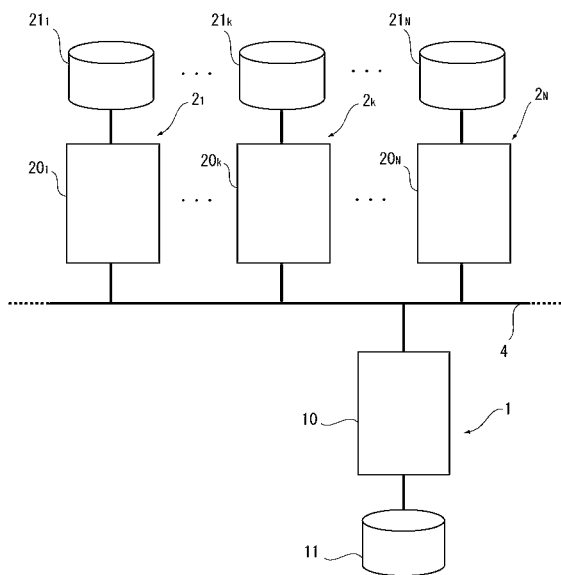
【0077】

- 1 管理サーバ
- 2 クライアント装置
- 3 データ記憶装置

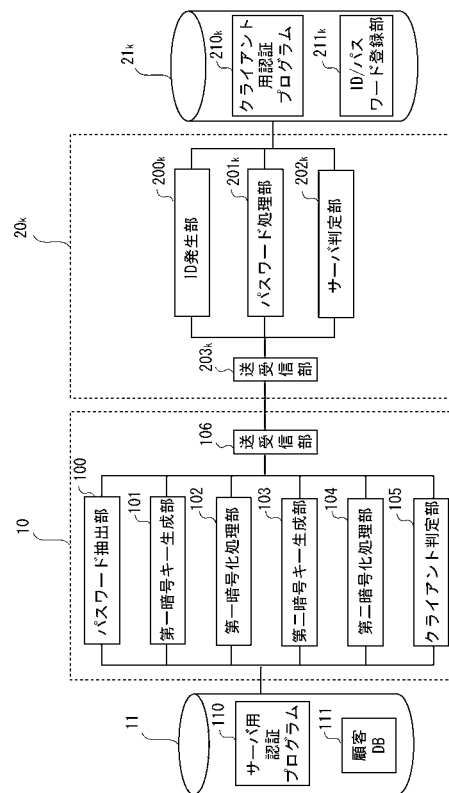
50

- 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

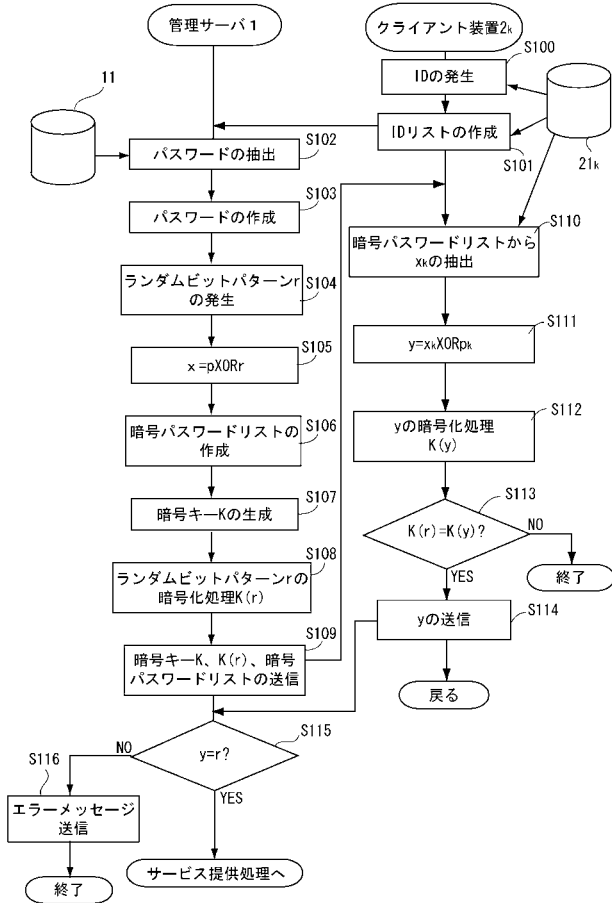
【図1】



【図2】



【 図 3 】



【 図 4 】

1	ID ₁
2	ID ₅
...	...
t	ID _k
...	...
N	ID _m

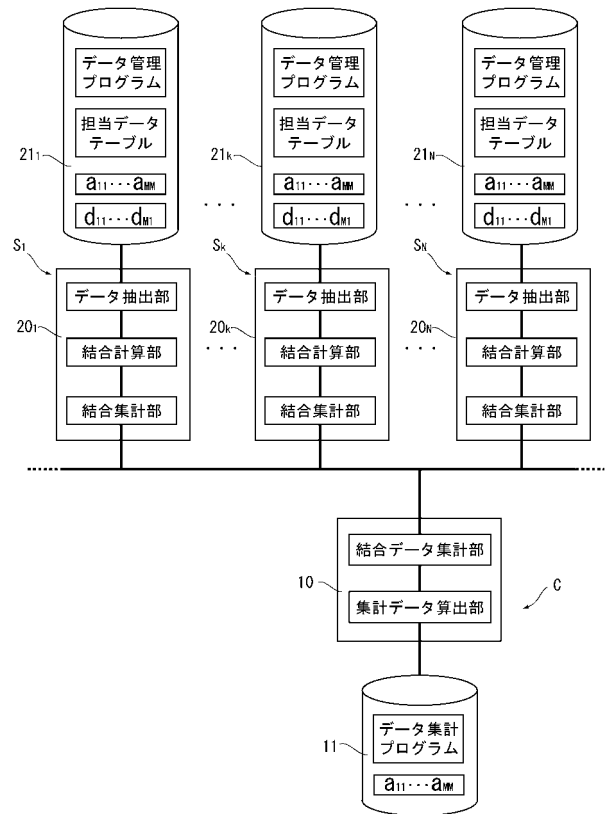
【 図 5 】

1	p ₁
2	p ₅
...	...
t	p _k
...	...
N	p _m

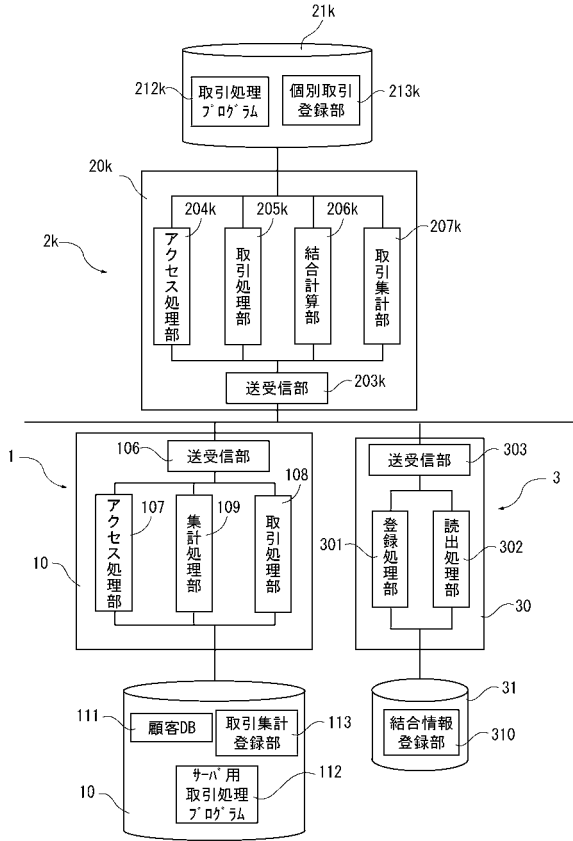
【 図 6 】

1	x ₁
2	x ₅
...	...
t	x _k
...	...
N	x _m

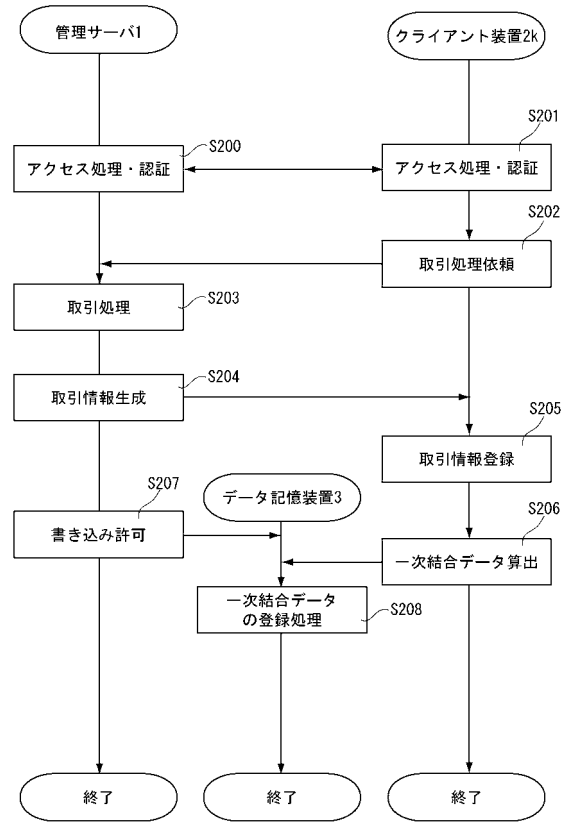
【 図 7 】



【 図 8 】



【 図 9 】



【 図 10 】

