(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4787077号
(P4787077)
(45)発行日　平成23年10月5日(2011.10.5)　(24)登録日　平成23年7月22日(2011.7.22)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 12/14　５１０F

請求項の数 4　(全 16 頁)

(21)出願番号　特願2006-156632(P2006-156632)
(22)出願日　平成18年6月5日(2006.6.5)
(62)分割の表示　特願2005-213302(P2005-213302)の分割
原出願日　平成17年7月22日(2005.7.22)
(65)公開番号　特開2007-35022(P2007-35022A)
(43)公開日　平成19年2月8日(2007.2.8)
審査請求日　平成20年7月18日(2008.7.18)

(73)特許権者　505277440
株式会社ソフィア
東京都杉並区天沼３－１－１関根ビル四階
(74)代理人　100105050
弁理士　鷲田　公一
(72)発明者　藤本　幸男
東京都多摩市豊ヶ丘１－５３－１０－２０３

審査官　小林　秀和

最終頁に続く

(54)【発明の名称】表計算ソフトの個人情報データ処理方法、プログラム及び記録媒体

(57)【特許請求の範囲】
【請求項１】
特定個人を識別できる識別情報と、前記特定の個人に関連する情報であって単独では特定の個人を識別することができない属性情報とを含む個人情報を記憶手段に保存し又は記憶手段から読み出す処理を、コンピュータに実行させる表計算ソフトの個人情報データ処理方法であって、
所定の分割規則を定めるデフォルト情報を取得するデフォルト情報取得ステップと、
前記デフォルト情報に従って、前記個人情報を、前記識別情報の列と前記属性情報の列とに分割する分割境界を表示するステップと、
表示された前記個人情報に対する前記分割境界の入力を受け付けるステップと、
受付けた前記分割境界の入力に従って前記個人情報を、前記識別情報の列と前記属性情報の列とに分割するステップと、
分割された前記識別情報を、複数の断片に分割する分割範囲を表示するステップと、
表示された前記分割範囲の入力を受け付けるステップと、
受け付けた前記分割範囲の入力に従って前記識別情報を、複数の断片に分割するステップと、
前記各断片の対応関係を示す連結鍵情報を生成するステップと、
前記各断片を異なるファイルに格納するステップと、
前記連結鍵情報と前記各断片とを異なる記憶領域に保管するステップと
を有する表計算ソフトの個人情報データ処理方法。

【請求項２】
前記記憶媒体領域に保管された前記連結鍵情報と、前記第１断片と前記第２断片とから元の識別情報を復元するステップと
をさらに有する請求項１記載の表計算ソフトの個人情報データ処理方法。
【請求項３】
特定個人を識別できる識別情報と、前記特定の個人に関連する情報であって単独では特定の個人を識別することができない属性情報とを含む個人情報を記憶手段に保存し又は記憶手段から読み出す処理を、コンピュータに実行させる表計算ソフトの個人情報データ処理方法であって、所定の分割規則を定めるデフォルト情報を取得するデフォルト情報取得ステップと、前記デフォルト情報に従って、前記個人情報を、前記識別情報の列と前記属性情報の列とに分割する分割境界を表示するステップと、表示された前記個人情報に対する前記分割境界の入力を受け付けるステップと、受付けた前記分割境界の入力に従って前記個人情報を、前記識別情報の列と前記属性情報の列とに分割するステップと、分割された前記識別情報を、複数の断片に分割する分割範囲を表示するステップと、表示された前記分割範囲の入力を受け付けるステップと、受け付けた前記分割範囲の入力に従って前記識別情報を、複数の断片に分割するステップと、前記各断片の対応関係を示す連結鍵情報を生成するステップと、前記各断片を異なるファイルに格納するステップと、前記連結鍵情報と前記各断片とを異なる記憶領域に保管するステップとをコンピュータに実行させるためのプログラム。
【請求項４】
特定個人を識別できる識別情報と、前記特定の個人に関連する情報であって単独では特定の個人を識別することができない属性情報とを含む個人情報を記憶手段に保存し又は記憶手段から読み出す処理を、コンピュータに実行させる表計算ソフトの個人情報データ処理方法であって、所定の分割規則を定めるデフォルト情報を取得するデフォルト情報取得ステップと、前記デフォルト情報に従って、前記個人情報を、前記識別情報の列と前記属性情報の列とに分割する分割境界を表示するステップと、表示された前記個人情報に対する前記分割境界の入力を受け付けるステップと、受付けた前記分割境界の入力に従って前記個人情報を、前記識別情報の列と前記属性情報の列とに分割するステップと、分割された前記識別情報を、複数の断片に分割する分割範囲を表示するステップと、表示された前記分割範囲の入力を受け付けるステップと、受け付けた前記分割範囲の入力に従って前記識別情報を、複数の断片に分割するステップと、前記各断片の対応関係を示す連結鍵情報を生成するステップと、前記各断片を異なるファイルに格納するステップと、前記連結鍵情報と前記各断片とを異なる記憶領域に保管するステップとをコンピュータに実行させるためのプログラムを記憶したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、個人情報保護を目的とする表計算ソフトの個人情報データ処理方法、プログラム及び記録媒体に関する。
【背景技術】
【０００２】
近年、インターネットに代表されるネットワークの普及とともに、電子メールやファイルの送受信がさかんに行われるようになってきた。それに伴い、セキュリティに対する不安も多くなっている。
【０００３】
ネットワークを通じて電子情報を交換すると、内容の改竄、書き換え、すり替えが可能で、しかもその痕跡が残らず事後に検知することが難しいという難点があった。また、通信路の途中で盗取して利用することも比較的容易であった。従来、このような場合に電子情報を暗号化して送付することにより安全を確保する方法が用いられてきた。しかし、暗号化方法は、送付したい電子情報の全てが通信データに含まれているため、通信が漏洩し

た時には極めて能力の高い侵害者ならば電子情報の解読や改竄も可能である。
【０００４】
また、個人情報保護法の施行により、個人情報を扱う組織・団体はその管理に膨大な労力とコストをかけることを余儀なくされている。個人情報を扱う以上、万が一の事故に対して重大な社会的責任を負わなければならないからである。しかし、どれほど厳重に管理されていても個人情報に関する事故は後を絶たない。
【０００５】
個人情報を保護する技術は、以下のように大別される。
（１）ユーザ認証　　情報へのアクセスに際して、その入口で正規ユーザを確認するシステム。代表的な例としてＩＤ、パスワードによる認証方式がある。指紋、静脈、アイリスなど人の身体的特徴を利用した生体認証の技術もこれに含まれる。この技術は、情報の入口で不法な侵入を防ぐもので、一旦不正な進入が図られた場合、個人情報そのものは保護されない。また、生体認証の偽造は困難であるが、コスト高になることなどの難点がある。
（２）情報の暗号化　　復号の鍵を有するもの以外情報の内容を窺い知ることができないシステム。個人情報は暗号化されていた場合でも情報として一体をなしており、紛失、盗難に際して情報漏洩の可能性を残す。
（３）シンクライアント　　個人情報を含む情報漏洩を防ぐ目的で、最初から端末のパソコンにハードディスク（ＨＤ）を搭載せず、業務に必要なデータやソフトウェアはＬＡＮなどを経由してアクセスする。
（４）情報分散　　一つの情報を複数の分散情報に分割して管理する。複数の分散情報を１つ１つ個別に見ても情報全体は見えない。個人情報を分割によって断片化しネットワーク上の複数のデータ格納端末に格納することで、個人情報の機密性や安全性を確保しようとする、特許文献１に記載の情報管理システムはこの技術である。
【０００６】
また、特許文献２に記載の個人情報分散管理方法及びシステムは、ネットワーク上で複数の端末に分散配置された個人情報及び通知先情報を、各端末間で相互に送受信する方法を提供する。
【特許文献１】特開２００３－２７１７８２号公報
【特許文献２】特開２００４－１７８５１７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００７】
しかしながらこのような従来の個人情報管理装置にあっては、以下のような解決課題があった。
【０００８】
ユーザ認証や暗号化による情報保護は、不正な第三者の侵入の可能性を残す。情報の内容はあくまで個人情報として存在するので、一旦不正な進入を許した場合、情報全体の漏洩は必至である。したがって、紛失や盗難などの事故に際して管理者の責任は免れない。
【０００９】
また、シンクライアントでは、いちいち情報をダウンロードして使用することになる。この端末は、記憶媒体と一体になったパソコンではないため、大きな情報を処理するためには不便である。また、個人情報がそのままの形でネットワーク上を移動する際のリスクも免れない。特許文献１記載の個人情報管理システムにおける「情報分散」は、情報の意味と内容を基準にした分割ではない。したがって、（ａ）機械的に分割された情報の断片には、原理的に個人情報の一部が紛れ込む可能性がある。また、（ｂ）情報のそれぞれの断片に連結情報が含まれていることから、断片自体からもとの情報が復元される可能性が残る。
【００１０】
本発明は、かかる点に鑑みてなされたものであり、個人情報の漏洩や喪失に対する高い

安全性を確保することができる表計算ソフトの個人情報データ処理方法、プログラム及び記録媒体を提供することを目的とする。

【００１１】

また、本発明は、高い安全性を確保しつつ、データ処理の効率化を図ることができる表計算ソフトの個人情報データ処理方法、プログラム及び記録媒体を提供することを別の目的とする。

【課題を解決するための手段】

【００１２】

本発明の表計算ソフトの個人情報データ処理方法は、特定個人を識別できる識別情報と、前記特定の個人に関連する情報であって単独では特定の個人を識別することができない属性情報とを含む個人情報を記憶手段に保存し又は記憶手段から読み出す処理を、コンピュータに実行させる表計算ソフトの個人情報データ処理方法であって、所定の分割規則を定めるデフォルト情報を取得するデフォルト情報取得ステップと、前記デフォルト情報に従って、前記個人情報を、前記識別情報の列と前記属性情報の列とに分割する分割境界を表示するステップと、表示された前記個人情報に対する前記分割境界の入力を受け付けるステップと、受付けた前記分割境界の入力に従って前記個人情報を、前記識別情報の列と前記属性情報の列とに分割するステップと、分割された前記識別情報を、複数の断片に分割する分割範囲を表示するステップと、表示された前記分割範囲の入力を受け付けるステップと、受け付けた前記分割範囲の入力に従って前記識別情報を、複数の断片に分割するステップと、前記各断片の対応関係を示す連結鍵情報を生成するステップと、前記各断片を異なるファイルに格納するステップと、前記連結鍵情報と前記各断片とを異なる記憶領域に保管するステップとを有する。

本発明は、特定個人を識別できる識別情報と、前記特定の個人に関連する情報であって単独では特定の個人を識別することができない属性情報とを含む個人情報を記憶手段に保存し又は記憶手段から読み出す処理を、コンピュータに実行させる表計算ソフトの個人情報データ処理方法であって、所定の分割規則を定めるデフォルト情報を取得するデフォルト情報取得ステップと、前記デフォルト情報に従って、前記個人情報を、前記識別情報の列と前記属性情報の列とに分割する分割境界を表示するステップと、表示された前記個人情報に対する前記分割境界の入力を受け付けるステップと、受付けた前記分割境界の入力に従って前記個人情報を、前記識別情報の列と前記属性情報の列とに分割するステップと、分割された前記識別情報を、複数の断片に分割する分割範囲を表示するステップと、表示された前記分割範囲の入力を受け付けるステップと、受け付けた前記分割範囲の入力に従って前記識別情報を、複数の断片に分割するステップと、前記各断片の対応関係を示す連結鍵情報を生成するステップと、前記各断片を異なるファイルに格納するステップと、前記連結鍵情報と前記各断片とを異なる記憶領域に保管するステップとをコンピュータに実行させるためのプログラムである。

本発明は、特定個人を識別できる識別情報と、前記特定の個人に関連する情報であって単独では特定の個人を識別することができない属性情報とを含む個人情報を記憶手段に保存し又は記憶手段から読み出す処理を、コンピュータに実行させる表計算ソフトの個人情報データ処理方法であって、所定の分割規則を定めるデフォルト情報を取得するデフォルト情報取得ステップと、前記デフォルト情報に従って、前記個人情報を、前記識別情報の列と前記属性情報の列とに分割する分割境界を表示するステップと、表示された前記個人情報に対する前記分割境界の入力を受け付けるステップと、受付けた前記分割境界の入力に従って前記個人情報を、前記識別情報の列と前記属性情報の列とに分割するステップと、分割された前記識別情報を、複数の断片に分割する分割範囲を表示するステップと、表示された前記分割範囲の入力を受け付けるステップと、受け付けた前記分割範囲の入力に従って前記識別情報を、複数の断片に分割するステップと、前記各断片の対応関係を示す連結鍵情報を生成するステップと、前記各断片を異なるファイルに格納するステップと、前記連結鍵情報と前記各断片とを異なる記憶領域に保管するステップとをコンピュータに実行させるためのプログラムを記憶したコンピュータ読み取り可能な記録媒体である。

【発明の効果】
【００１３】
本発明によれば、個人情報の漏洩や喪失に対する高い安全性を確保することができる。また、データ保存プログラムとして、表計算ソフトなどのパッケージソフトなどに適用して好適である。また、特別な部材は不要で部品点数の増加もないので、低コストでしかも実施が容易でありパソコン等の情報処理装置に幅広く適用することができる。
【発明を実施するための最良の形態】
【００１４】
以下、本発明の実施の形態について図面を参照して詳細に説明する。
【００１５】
（本発明の基本的な考え方）
本発明は、個人情報保護を主たる目的としたデータベースのデータ管理装置、データ管理方法、データ処理方法及びデータ保存方法を提供する。
【００１６】
まず、個人情報の定義と分類について説明する。
【００１７】
「個人情報」とは、個人情報の保護に関する法律　第１章第２条によれば、生存する個人に関する情報であって、当該の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を識別することが出来るもの（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を識別することができることとなるものを含む。）をいう。以下に述べる個人情報は、上記定義に従うものとする。
【００１８】
本発明者は、上記個人情報を、特定の個人を識別できる機能を持つ識別情報と、前記識別情報と結びつくと個人情報となるが単独では個人情報とはならない属性情報とに分けることができることを見出した。
【００１９】
識別情報は、具体的には、氏名であり、属性情報は、具体的には、住所、電話番号、生年月日、年齢、性別、身長、体重、血液型、年収、学歴、家族構成、趣味、嗜好、購読雑誌などである。また、識別情報に準ずる情報として、単独では特定の個人を認識することはできないが、特定の個人を結びつける情報と照合することで容易に個人を特定できる情報がある。具体的には、お客様番号、会員番号、ＩＤ番号である。
【００２０】
図１は、本発明の基本概念を説明する図である。
【００２１】
<ステージ１>
個人情報分割手段１により個人情報を識別情報と属性情報とに人為的に分割する。この分割は、個人情報が、特定の個人を識別することができる機能を失うところ、すなわち個人情報としての意味を消失させるところで人為的に分割する。上記個人情報、識別情報及び属性情報は、所定の記憶媒体からなる各データファイルに保存される。
【００２２】
また、連結鍵<１>情報生成手段２により、分割した識別情報と属性情報とを元の個人情報に復元するための連結鍵<１>情報を生成し、生成した連結鍵<１>情報を連結鍵<１>情報保管手段３により前記各データファイルとは異なる場所の記憶媒体に連結鍵<１>ファイルとして保管する。
【００２３】
<ステージ２>
個人情報分割／並替手段４により、上記個人情報を分割した識別情報を、さらに複数の断片に分割するとともに、分割した断片をランダムに並べ替えを行って、所定の記憶媒体からなる各データファイルに保存する。識別情報が氏名の場合、断片は例えば名字（第１断片）と名前（第２断片）である。また、識別情報が氏名に準ずるＩＤの場合、断片は例

えばハイフン又は文字数などを基準に分割作成される。

【００２４】

また、連結鍵<２>情報生成手段５により、分割した断片を元の識別情報に復元するための連結鍵<２>情報を生成し、生成した連結鍵<２>情報を連結鍵<２>情報保管手段６により前記各データファイルとは異なる場所の記憶媒体に連結鍵<２>ファイルとして保管する。

【００２５】

さらに、データ処理実行手段７は、個人情報分割／並替手段４により分割された複数の断片及び／又は属性情報に対してデータ処理を実行する。

【００２６】

このように、本発明は、単にファイルを機械的に分割／保存するのではなく、個人情報を識別情報と属性情報とに分割し、その識別情報をさらに第１断片（例えば氏）と第２断片（例えば名前）に分割することによって、それぞれの断片を個人情報として意味をなさないものに変化させる。すなわち、識別情報を再分割することで、再分割された識別情報からは識別機能が殆ど完全に消失する。また、連結鍵情報は、断片及び属性情報とは別の記憶媒体に保管される。したがって、個人情報ではなくなったデータが、各データファイルに保存される。各データファイルに保存されたデータは個人を特定できないデータの集合体に過ぎないため、個人情報を保護することができる。一方、個人情報を分割した属性情報は、個人識別機能を持たないため単独で各種データ処理に利用することができる。また、連結鍵情報が入手できないと元の個人情報を復元できないことから個人情報の保護の実効を図ることができる。

【００２７】

（実施の形態１）

図２は、上記基本的な考え方に基づく本発明の実施の形態１に係るデータ管理装置の構成を示す図である。本実施の形態は、データ管理装置として、パーソナルコンピュータ等の情報処理装置（データ処理装置）に適用した例である。

【００２８】

図２において、データ管理装置１００は、ＣＰＵ１０１（指定手段の一部，第１分割手段，第２分割手段，連結鍵生成手段，並替手段）、制御プログラムや固定データ等を記憶するＲＯＭ１０２、ＣＰＵ１０１の実行・作業用記憶領域であるＲＡＭ１０３、電気的に書換可能な不揮発性メモリであるＥＥＰＲＯＭ（electrically erasable programmable ROM），電源バックアップされたＲＡＭ等からなる不揮発性補助記憶装置１０４（第２記憶媒体，保管手段）、キーボード及びマウス等のポインティングデバイスからなる入力装置１０５（指定手段）、ＬＣＤディスプレイ等からなる表示装置１０６、ハードディスクドライブ（ＨＤＤ）,ＤＶＤ等の外部記憶装置１０７（第１記憶媒体，格納手段）、入出力インターフェース（Ｉ／Ｆ）１０８、及び通信装置１０９を備えて構成される。

【００２９】

通信装置１０９は、モデムポート等からなり、インターネット又は専用回線からなるインターネット網１５０を経由して各種サーバ１６０，ｗｅｂ端末１７０に接続される。

【００３０】

サーバ１６０は、情報提供データなどの各種データをデータベースとして蓄積する商用サーバ等である。

【００３１】

ＣＰＵ１０１は、データ管理装置１００全体の制御を行うとともに、個人情報を特定の個人を識別できる識別情報と、単独では特定の個人を識別することができない属性情報とに分割する分割範囲のユーザ指定を受け付け、ユーザにより指定された分割範囲に従って個人情報を識別情報と属性情報とに第１分割し、第１分割した識別情報を、データ処理可能な複数の断片に第２分割し、さらに分割した識別情報、属性情報、及び複数の断片を元の個人情報に復元するための連結鍵情報を生成し、識別情報及び属性情報を外部記憶装置１０７に、連結鍵情報を不揮発性補助記憶装置１０４に保管するデータ保存処理を実行する。

【００３２】
また、本実施の形態では、データ管理装置１００は、パーソナルコンピュータ等のデータ処理装置に適用しており、ＣＰＵ１０１は、アプリケーションプログラムの実行によりデータベースに格納されたデータにアクセスして表計算などのデータ処理を行うデータ処理実行手段としての機能を有する。この場合、ＣＰＵ１０１は、分割した複数の断片又は属性情報に対して計算表処理や統計処理などのデータ処理を実行する。
【００３３】
不揮発性補助記憶装置１０４は、電源ＯＦＦ以降、次回電源ＯＮまで保持しなければならない作業データ、補助プログラムなどのほか、生成された連結鍵情報ファイルが保管される。この不揮発性補助記憶装置１０４は、本体から取り外しが可能なＵＳＢ（Universal Serial Bus）メモリやカード型外部拡張記憶媒体であってもよい。この記憶媒体は、例えば小型ハードディスクドライブ（ＨＤＤ）等のディスク装置のほか、電源バックアップにより書き込まれた情報を保持するＳＲＡＭ（Static RAM）カードや電源バックアップが不要なフラッシュメモリ等からなるコンパクトフラッシュ（登録商標）（ＣＦ）、ＳＤメモリ（登録商標）、スマートメディア（登録商標）、メモリスティック等である。
【００３４】
入力装置１０５は、キーボード及びポインティングデバイスであるマウス等であり、個人情報入力や個人情報を識別情報と属性情報とに分割する分割範囲を指定する。
【００３５】
外部記憶装置１０７は、個人情報を蓄積する個人情報データベース１１０、各種情報及び分割された断片を格納するデータファイル１１１を備える。なお、個人情報データベース１１０は権限ある管理者のみがアクセスできる。
【００３６】
入出力Ｉ／Ｆ１０８は、ＩｒＤＡ（Infrared Data Association）による赤外線データ通信やＵＳＢなどを使用した有線通信により外部周辺機器と通信を行う。
【００３７】
通信装置１０９は、インターネット網１５０に接続されたサーバ１６０や他のｗｅｂ端末１７０と通信を行うとともに、それら機器との間でデータを送受信する。
【００３８】
インターネット網１５０は、移動体通信網、公衆電話網、ＬＡＮやインターネットなどから構成するネットワークであり、有線系又は無線系などネットワークの種類とプロトコルの種類は特に問わない。また、ネットワークのアクセス回線としてはＦＴＴＨ（Fiber To The Home）、ＨＦＣ（Hybrid Fiber Coax：光同軸ケーブル）、及びＡＤＳＬ（Asymmetric Digital Subscriber Line）／ＶＤＳＬ（Very high data rate Digital Subscriber Line）等の大容量回線が利用可能である。無線系には、専用回線であるキャリア網を経由してキャリアサーバに接続されるキャリアは勿論のこと、キャリア以外の電波を送受信して無線通信を行うBluetooth、ＵＷＢ（Ultra Wideband）、無線ＬＡＮでもよい。
【００３９】
以下、上述のように構成されたデータ管理装置の動作を説明する。
【００４０】
図３は、データ管理装置のデータ保存方法を示すフローチャートであり、本フローは、ＣＰＵ１０１により実行される。例えば、アプリケーションソフトウェア実行時にデータ保存プログラムとして呼び出され実行される。図中、Ｓはフローの各ステップを示す。
【００４１】
まず、ステップＳ１で個人情報データベース（ＤＢ）１１０から個人情報を読み出す。図４は、個人情報データベースに蓄積される個人情報の一例を示す図である。ここでは、保護の対象となる個人情報として個人の年齢、体重、身長及び血糖値のデータがある。
【００４２】
ステップＳ２で本データ保存方法によって情報が既に分割保存されているか否かを判別する。情報が既に分割保存されている場合には、本フローをそのまま終了する。情報が分

割保存されていない場合には、ステップＳ３で個人情報を識別情報と属性情報とに第１分割する分割範囲（分割箇所）が設定されているか否かを判別する。個人情報の分割範囲が設定されていなければ、ステップＳ４で個人情報としての意味を消失する境界となる分割範囲をユーザが設定する。この設定は、ユーザが個人情報データベースから読み出した個人情報を表示装置１０６で確認しながら適当な箇所で入力装置１０５により指定する。この場合、氏名を識別情報とし、それ以外を属性情報とすることが好ましい旨のガイダンスを表示する、識別情報と属性情報との間に分割推奨マークを表示する、あるいはデフォルトで氏名の後に分割範囲を表示しユーザの確認指示だけを待つなどの態様を採ることが好ましい。上記個人情報を識別情報と属性情報とに分割する第１分割処理は、以下の処理で識別情報を再度分割するために、前もって識別情報を個人情報から峻別するための予備的作業（前処理作業）としての分割処理である。

【００４３】

次いで、ステップＳ５でユーザ設定された分割範囲で個人情報を識別情報と属性情報とに分割し、ステップＳ６で分割された識別情報と属性情報とを連結する連結鍵情報を生成する。分割手順と連結鍵情報の生成の詳細については、図５及び図６により後述する。

【００４４】

次いで、ステップＳ７で分割した識別情報と属性情報とをデータファイルに格納し、ステップＳ８で生成した連結鍵情報をデータファイルとは異なる場所の記憶媒体に連結鍵<１>ファイルとして保管する。

【００４５】

ステップＳ９では、識別情報を複数の断片に分割するか否かを判別する。この設定についてもユーザが表示装置１０６に表示されたガイダンス（例えば「断片化しますか」）に従って入力装置１０５により指示する。この場合、デフォルトで識別情報を断片に分割する態様を採っても良い。例えば、名字と名前の間のスペース、ハイフン、文字数などで分割する。また、氏名のデータベースを検索して名字と名前の分割箇所を得ることも可能である。識別情報を断片に分割しない場合は、本フローを終了する。

【００４６】

識別情報を複数の断片に分割する場合には、ステップＳ１０でユーザ設定された分割範囲で識別情報を複数の断片に第２分割し、ステップＳ１１で分割された複数の断片同士を連結する連結鍵情報を生成する。分割手順と連結鍵情報の生成の詳細については、上記個人情報の分割と連結鍵情報生成と同様に作成できる。

【００４７】

次いで、ステップＳ１２で分割した複数の断片をデータファイルに格納し、ステップＳ１３で生成した連結鍵情報をデータファイルとは異なる場所の記憶媒体に連結鍵<２>ファイルとして保管して本フローを終了する。

【００４８】

上記第２分割処理により、個人情報の特殊性に鑑みて、第１分割処理により個人情報を識別情報と属性情報に分割したその識別情報を、識別機能が殆ど消失した複数の断片に再分割することができる。これにより、個人情報としての意味を喪失した各断片と、同じく識別情報を持たない属性情報とを得ることができる。

【００４９】

図５は、情報分割及び連結鍵情報生成の詳細を示すフローチャートであり、図３のステップＳ６及びステップＳ１１の詳細ステップである。また、図６は、図５のフローで処理される情報分割処理及び連結鍵情報生成の一例を示す図である。

【００５０】

まず、ステップＳ２１で分割される個人情報のデータ行列をカウントする。例えば、図４に示す個人情報を例に採ると、この表データの行数をカウントする。図４では、氏名（識別情報）とそれ以外の年齢等の属性情報とからなるデータ列において、行数をカウントする。いま、データは１行目（山田太郎）からｎ行目（佐藤元）まで行数はｎ個ある。次いで、ステップＳ２２で乱数を発生させて（ｎ×２）個の乱数表（図６（ａ）参照）を作

成し、ステップＳ２３で作成した乱数表からリンクテーブル（図６（ｂ）参照）を作成する。乱数表の作成条件は、例えば何れの数も０で始まらない（条件１）、同じ数が重複しない（条件２）である。図６（ｂ）に示すように、図６（ａ）に示す（１からｎまでの数列）と（ｎ＋１からｎ×２までの数列）の対列からなるリンクテーブルを作成する。この対列からなるリンクテーブルが連結鍵情報となる。

【００５１】

ステップＳ２４では、元データの分割基準を決定する。本フローが図３のステップＳ６で呼び出された場合は、個人情報を個人情報を識別情報とに分割する設定を読み込む。また、本フローが図３のステップＳ１１で呼び出された場合は、識別情報を断片に分割する設定を読み込む。次いで、ステップＳ２５で設定された分割範囲（分割箇所）に従って個人情報を個人情報と識別情報とに分ける。具体的には、新たな作業用データファイルに個人情報からなる列グループと識別情報とからなる列グループをコピーする。次いで、ステップＳ２６で上記ステップＳ２３で作成したリンクテーブルの隣接する列に上記ステップＳ２５でコピーした列グループを貼り付ける。図６（ｃ）に示すように、個人情報からなる列グループと識別情報とからなる列グループとの間にリンクテーブル（図６（ｂ）参照）が貼り付けられる。

【００５２】

次いで、ステップＳ２７でリンクテーブルを貼り付けた作業用データファイルを対列部分で二つに分け（図６（ｄ）参照）、ステップＳ２８で分割されたそれぞれのファイルのデータ行について乱数を用いてソートする。これにより、ファイルのデータ同士の前後の関連性が失われ、個人情報がより一層保護される。次いで、ステップＳ２９でそれぞれのファイルを別々のデータファイルとしてＨＤＤ等に記憶するとともに、リンクテーブルは連結鍵情報として各データファイルとは別の記憶媒体（例えば、着脱可能なＵＳＢメモリやＳＤカード）に保存して本フローを終了する。

【００５３】

以上、設定された分割範囲に従って個人情報を個人情報と識別情報とに分ける場合を例に採り説明したが、識別情報を複数の断片に分ける場合も同様である。この場合は、ステップＳ１４の分割基準で、例えば名字と名前の間のスペース、ハイフン、文字数などで分割指定し同様の処理を行えばよい。

【００５４】

上述した各フローを実行することにより、具体的には以下の動作が実現される。

【００５５】

図７は、データ保存時の手順を示すフローチャートであり、パッケージソフト上に組み込まれた場合の手順の一例を示す。パッケージソフトとして表計算ソフトを例に採る。

【００５６】

いま、表計算ソフト上でデータ保存を実行する。

（１）ソフトウェアによるダイヤログ表示などにより「個人情報を分割保存して無意味化しますか?」を表示する。ユーザ指示により個人情報の分割保存が指示されたかった場合は通常の保存を行う。

（２）ユーザ指示により個人情報の分割保存が指示された場合、「分割する範囲（識別情報と属性情報）を指定して下さい。」を表示し、ユーザ指示を待つ。

（３）ユーザ入力により二つのブロックの境界が指定されると、「元の情報が識別情報と属性情報に分割されました。識別情報をさらに分割して情報を完全に無意味化します。」を表示する。

（４）「識別情報の列を分割する基準を選択して下さい。空白で分割（例：山田　太郎、Michael　Jackson）／ハイフンで分割（例：ID4527-5608）／文字数を指定して分割」を表示する。

（５）「分割が完了しました。新たに生成された連結鍵ファイルと分割された断片ファイルを格納する場所をそれぞれ指定して下さい。Ｃドライブ／Ｄドライブ／フロッピー（登録商標）ディスク／ＵＳＢメモリ（外部記憶装置）」を表示し、ユーザ指示を待つ。

（６）ユーザ指示により指定された場所にデータが格納され、「元の個人情報は、無意味化されて保存されました。連結鍵ファイルは、断片ファイルとは別に管理して下さい。」を表示する。本例では、連結鍵ファイルと分割された断片ファイルとを同じ場所に格納しようとすると警告（メッセージ表示／報知音）を行う。

【００５７】

以下、想定される具体的な使用例について説明する。

１．分割された断片情報はいずれも個人情報としての意味を消失している。この断片情報と属性情報（又はその断片）は、元の個人情報から見た場合には情報の断片でありながら単独では完結したデータである。したがって、安全性を維持しながらデータベースを構成するあるいは表計算などのアプリケーションソフトによるデータ処理が可能である。例えば、アンケートの集計結果から氏名などの識別情報を伴わない属性情報の断片を作成し、ノートパソコンに格納して自宅に持ち帰り、数値の統計処理を施してグラフを作成する。この例のように、個人情報漏洩の危険を冒さずにデータベース処理を行い、必要に応じて断片の再結合をするなどの使用方法が考えられる。なお、この利用方法は従来の機械的分割では成立しない。

２．個人ユーザの場合

ａ．無意味化された個人情報の「断片ファイル」をノートパソコンのハードディスク上に別々に格納する。

ｂ．「連結鍵情報ファイル」はＵＳＢメモリなどの外部記憶装置に保存してノートパソコンとは分離して携帯する。

ｃ．出先で「連結鍵情報ファイル」が格納されたＵＳＢメモリなどの外部記憶装置をノートパソコンに挿入して作業をする。作業後はＵＳＢメモリなどの外部記憶装置をはずして管理する。

３．大規模ユーザの場合

ａ．無意味化された個人情報の「断片ファイル」と「連結鍵情報ファイル」は、社内のネットワーク上にばらばらに格納する。

ｂ．社員は、無意味化された個人情報の「断片ファイル」と「連結鍵情報ファイル」をネットワーク上からダウンロードして使用する。

４．ハードディスクの紛失、盗難、廃棄に際して情報管理者がなすべきこと。

【００５８】

ハードディスクには「無意味化された個人情報の断片」しか入っていない。これらの断片は仮に第三者に覗かれても情報としての意味を構成しない。したがって、ハードディスクから情報が漏洩する可能性は皆無である。この性質は、ハードディスクが紛失、盗難、廃棄される場合、「個人情報保護法案」の規定に対してきわめて有効に働く。また、盗難、紛失の場合は、当該情報に対応する「連結鍵情報ファイル」を速やかに凍結することで、「個人情報」の遺漏を効果的に防ぐことができる。これは、情報の断片がＣＤ，ＤＶＤなどの記憶媒体に保存されている場合も同様である。

【００５９】

以上のように、本実施の形態のデータ管理装置１００は、ユーザ指定により個人情報を特定の個人を識別できる識別情報と、単独では特定の個人を識別することができない属性情報とに分割する分割範囲を設定し、ＣＰＵ１０１はユーザにより指定された分割範囲に従って個人情報を識別情報と属性情報とに第１分割するとともに、第１分割した識別情報を、データ処理可能な複数の断片に第２分割し、さらに分割した識別情報、属性情報、及び複数の断片を元の個人情報に復元するための連結鍵情報を生成し、識別情報、属性情報及び複数の断片を外部記憶装置１０７に、連結鍵情報を不揮発性補助記憶装置１０４に保管するデータ保存処理を実行するので、個人情報の漏洩や喪失に対する高い安全性を確保することができる。すなわち、情報分割は、機械的に行われるのではなく、「個人情報」の特性を踏まえて「個人情報」としての意味を消失させ、第三者による不正な情報使用を阻止することを目的として行われる。個人情報は、第一段階で主に氏名からなる「識別情報」と「属性情報」に分割される。次に、「識別情報」である氏名を、「名字」と「名前

」の二つの別のファイルに分割する。分割された断片を連結する情報は、断片の中に書き込まれるのではなく、第三の連結鍵情報として新たに生成されるファイルの中に保存される。この「連結鍵情報」の生成が、情報の一元管理に際して有効に機能することは上述した使用例に示す通りである。

【００６０】

特に、本実施の形態は、単にファイルを機械的に分割／保存するのではなく、識別情報と属性情報に分割し、その識別情報をさらに「名字」と「名前」に分割することによって、それぞれの断片を個人情報として意味をなさないものに変化させる点に特徴がある。

【００６１】

分割された断片情報はいずれも個人情報としての意味を消失しているので、安全性を維持しながらデータベースを構成するあるいは表計算などのアプリケーションソフトによるデータ処理が可能である。すなわち、分割された各情報は個人情報を喪失しているだけで、データ行列等のデータ構造自体はユーザが一見して分かる配列であるため、ユーザは通常のデータ処理作業をそのまま続ける感覚であり、作業効率の向上が期待できる。データを暗号化してしまう態様では、取り扱うデータが暗号化されたデータとなるため同等の作業性を求めることは難しい。さらに、データを暗号化してしまう態様では、一旦データ暗号化が破られてしまうと個人情報データは無防備になってしまうが、本実施の形態では、分割された断片情報はそれ自体が個人情報としての意味を消失しているので、個人情報保護の観点について言えば極めて強靭なデータ保護機能がある。

【００６２】

また、情報の断片を繋ぐ連結鍵情報は、断片とは隔離されて格納される。個人情報の保護は、連結鍵情報ファイルの管理に依存するので、個人情報の厳正な一元集中管理が効果的に達成できる。また、膨大な量の情報を破棄する場合も連結鍵情報ファイルを破棄することで完了する。

【００６３】

ここで、情報の大部分を占める属性情報は、識別情報と隔離されることにより、個人情報ではなくなる。したがって、ハードディスクなどに格納して持ち運びが可能である。持ち運びに際して情報遺漏の危険を伴わないという利点は、従来技術のシンクライアントの不便さを解消するものである。

【００６４】

さらに、暗号化情報との違いについて説明する。本データ保存方法は、復号化の手がかりを与えない構造である。機械的に暗号化された情報においては、無数の組み合わせの中に突出して有意義な組み合わせが必ず含まれる。この突出して有意義な組み合わせを手がかりにすれば、「暗号化された情報」は、理論的には何れ必ず解読される。これに対して、本実施の形態では、識別情報は、名字と名前の断片に分割され、この名字と名前は乱数表を使ってランダムに並べ替えられ保存される。名字と名前の断片を再び組み合わせて出来た氏名は、すべての組み合わせが同じ程度に意味を持つ。すべての組み合わせが有意義さの程度において等価であるといえる。同様に、属性情報と識別情報の組み合わせも有意義さの程度において等価であるといえる。したがって、情報を復元する手がかりをそれ自身に持たない点で卓越した個人情報保護を図ることが可能になる。

【００６５】

（実施の形態２）

実施の形態１は、個人情報を識別情報と属性情報とに第１分割するとともに、第１分割した識別情報を、データ処理可能な複数の断片に第２分割し、さらに分割した識別情報、属性情報、及び複数の断片を元の個人情報に復元するための連結鍵情報を生成するものである。実施の形態２は、個人情報を含むデータの他の分割例である。

【００６６】

ハード的構成は、図２と同様であるため説明を省略する。

【００６７】

図８は、本発明の実施の形態２に係るデータ管理装置の個人情報を含むデータの分割処

理の別の態様を説明する図である。実施の形態１では、図８（ａ）に示すように、個人情報を識別情報（氏名）と属性情報（Ａ，Ｂ，…）とに第１分割するとともに（ａ．参照）、第１分割した識別情報（氏名）を、データ処理可能な複数の断片である氏と名に第２分割する（ｂ．参照）。そして、分割した氏と名とをランダムに並べ替えるとともに（ｃ．参照）、属性情報データ列についてもランダムに並べ替える（ｄ．参照）。

【００６８】

しかしながら個人情報を含むデータの分割は、上述した例に限定されるものではない。例えば、第１分割及び第２分割は時間的に同時であってもよく、個人情報を含むデータを任意の複数の断片情報に分割することも可能である。これを図８（ｂ）により説明する。図８（ｂ）に示すように、個人情報を含むデータを任意の箇所で分割する。ここでは、個人情報を識別情報（氏名）及び属性情報（Ａ）と属性情報（Ｂ，…）とに分割する。個人情報を含むデータの分割はここで終了してもよいし、さらに繰り返し分割してもよい。そして、分割した識別情報（氏名）及び属性情報（Ａ）と属性情報（Ｂ，…）とをランダムに並べ替える（ｂ．参照）。これにより、図８（ｂ）のハッチングに示す属性情報（Ａ）の該当データ列は、属性情報（Ｃ）の該当データ列に、図８（ｂ）のハッチングに示す氏名の該当データ列は、属性情報（Ｄ）の該当データ列に対応することになる。したがって、本実施の形態にあっても個人情報を含むデータを、識別機能が殆ど消失した複数の断片に再分割することができ、安全性を維持しながらデータベースを構成するあるいは表計算などのアプリケーションソフトによるデータ処理が可能になる。

【００６９】

なお、上記各実施の形態に係るデータ管理装置は、装置単体としては勿論のこと、パソコン等の情報処理装置やサーバに組み込まれた装置であってもよい。

【００７０】

また、図４、図６、図７及び図８のデータ処理は一例であり、どのようなデータ及び分割保存方法でも構わない。また、データ並べ替えも適応的に採用することが可能である。

【００７１】

また、本実施の形態ではデータ管理装置、データ管理方法及びデータ処理方法という名称を用いたが、これは説明の便宜上であり、情報処理装置、個人情報管理方法等であってもよいことは勿論である。

【００７２】

さらに、上記データ管理装置を構成する各回路部、例えば記憶装置等の種類、数及び接続方法などは前述した実施の形態に限られない。

【００７３】

以上説明したデータ管理装置、データ管理方法及びデータ処理方法は、このデータ管理装置、データ管理方法及びデータ処理方法を機能させるためのプログラムでも実現される。このプログラムはコンピュータで読み取り可能な記録媒体に格納されている。本発明では、この記録媒体として、メインメモリそのものがプログラムメディアであってもよいし、また外部記憶装置としてプログラム読み取り装置が設けられ、そこに記録媒体を挿入することで読み取り可能なプログラムメディアであってもよい。いずれの場合においても、格納されているプログラムはＣＰＵがアクセスして実行させる構成であってもよいし、あるいはいずれの場合もプログラムを読み出し、読み出されたプログラムは、図示されていないプログラム記憶エリアにダウンロードされて、そのプログラムが実行される方式であってもよい。このダウンロード用のプログラムは予め本体装置に格納されているものとする。

【００７４】

ここで、上記プログラムメディアは、本体と分離可能に構成される記録媒体であり、磁気テープやカセットテープ等のテープ系、フロッピー（登録商標）ディスクやハードディスク等の磁気ディスクやＣＤ－ＲＯＭ／ＭＯ／ＭＤ／ＤＶＤ等の光ディスクのディスク系、ＩＣカード／光カード等のカード系、あるいはマスクＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、フラッシュＲＯＭ等による半導体メモリを含めた固定的にプログラムを担持する媒体

であってもよい。

【００７５】

さらに、図示されていないが、外部の通信ネットワークとの接続が可能な手段を備えている場合には、その通信接続手段を介して通信ネットワークからプログラムをダウンロードするように、流動的にプログラムを担持する媒体であってもよい。なお、このように通信ネットワークからプログラムをダウンロードする場合には、そのダウンロード用プログラムは予め本体装置に格納しておくか、あるいは別な記録媒体からインストールされるものであってもよい。なお、記録媒体に格納されている内容としてはプログラムに限定されず、データであってもよい。

【産業上の利用可能性】

【００７６】

本発明に係る表計算ソフトの個人情報データ処理方法、プログラム及び記録媒体は、個人情報保護を目的とするデータベースの分散保存及び管理方法に有用である。また、プログラムとして、表計算ソフトなどのパッケージソフトなどに適用して好適である。また、特別な部材は不要で部品点数の増加もないので、低コストでしかも実施が容易でありパソコン等の情報処理装置に幅広く適用することができる。

【図面の簡単な説明】

【００７７】

【図１】本発明の基本概念を説明する図である。

【図２】本発明の実施の形態１に係るデータ管理装置の構成を示す図

【図３】上記実施の形態１に係るデータ管理装置のデータ保存方法を示すフローチャート

【図４】上記実施の形態１に係るデータ管理装置の個人情報データベースに蓄積される個人情報の一例を示す図

【図５】上記実施の形態１に係るデータ管理装置の情報分割及び連結鍵情報生成の詳細を示すフローチャート

【図６】上記実施の形態１に係るデータ管理装置の情報分割処理及び連結鍵情報生成の一例を示す図

【図７】上記実施の形態１に係るデータ管理装置のデータ保存時の手順を示すフローチャート

【図８】本発明の実施の形態２に係るデータ管理装置の個人情報を含むデータの分割処理の別の態様を説明する図

【符号の説明】

【００７８】

１００　データ管理装置

１０１　ＣＰＵ（指定手段の一部，第１分割手段，第２分割手段，連結鍵生成手段，並替手段）

１０２　ＲＯＭ

１０３　ＲＡＭ

１０４　不揮発性補助記憶装置（第２記憶媒体，保管手段）

１０５　入力装置（指定手段）

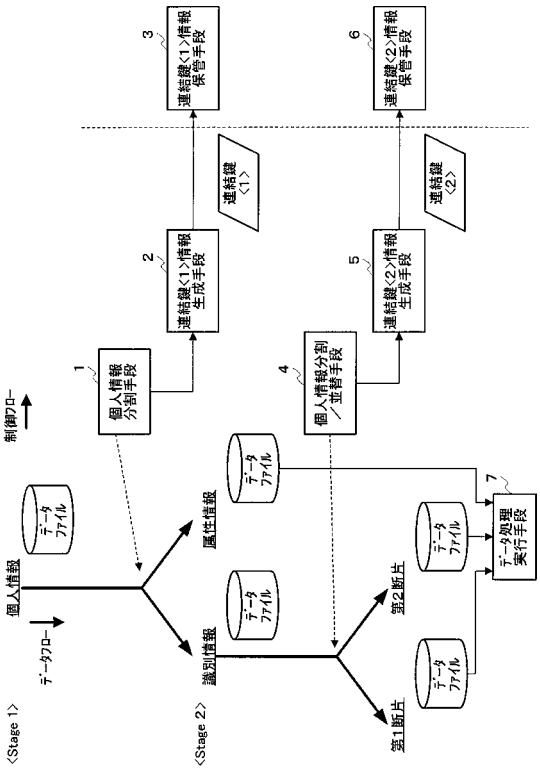
１０６　表示装置

１０７　外部記憶装置（第１記憶媒体，格納手段）

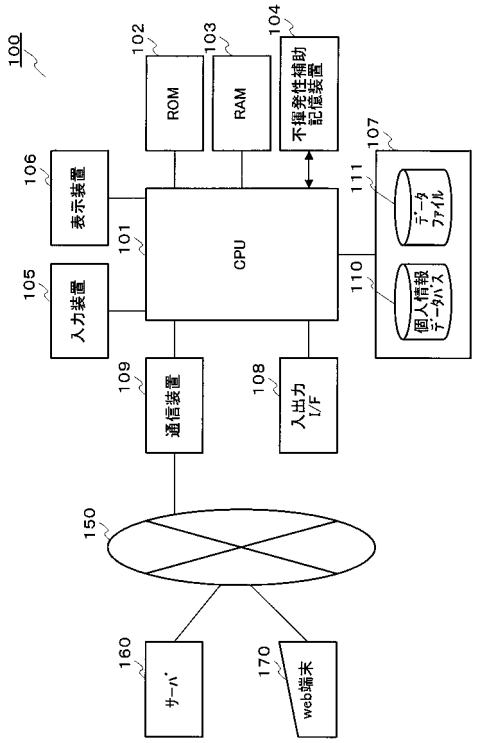
１０８　入出力インターフェース（Ｉ／Ｆ）

１０９　通信装置

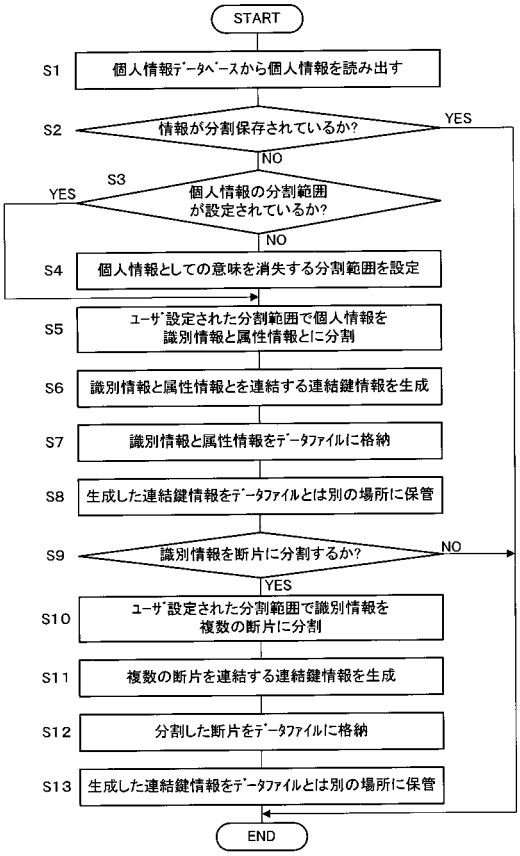
【図１】



【図２】



【図３】

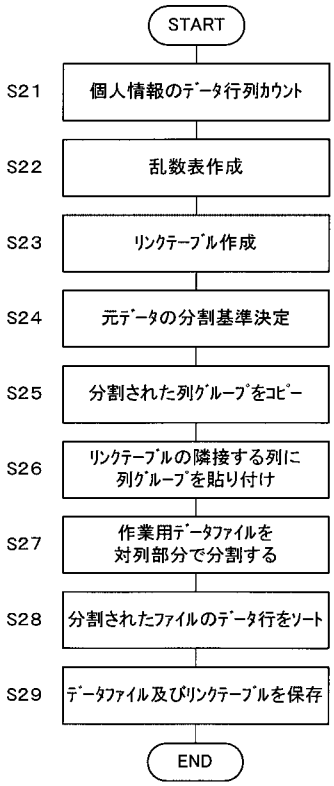


【図４】

分割される元のデータ

氏名	年齢	体重	身長	血糖値	
山田 太郎	55	74	175	98	1行目
鈴木 花子	45	48	160	120	2行目
・・・					
佐藤 元	34	58	175	136	n行目

【図５】



【図６】

(a)

5391
7308
6683
・ ・ ・
7138
3410

(n×2)個

(b)

5391	4628
7308	9462
6683	9321
・ ・ ・	・ ・ ・
7749	7138
9284	3410

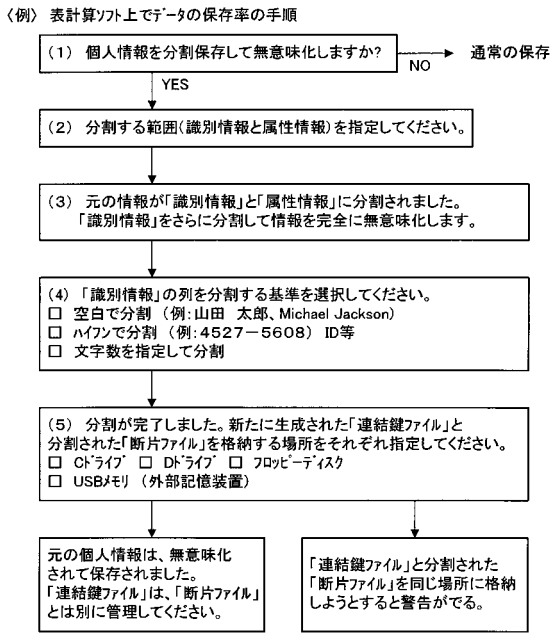
(c)

山田 太郎	5391	4628	55	74	175	98
鈴木 花子	7308	9462	45	48	160	120
・ ・ ・	・ ・ ・		・ ・ ・			
佐藤 元	9284	3410	34	58	175	136

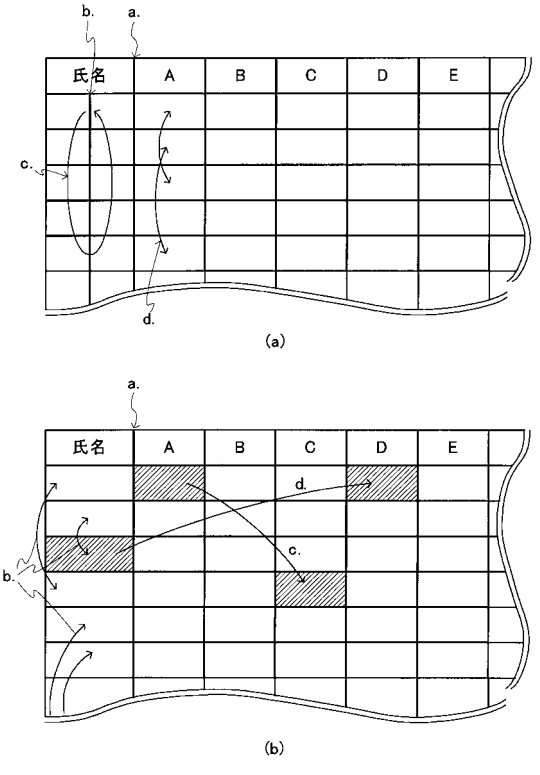
(d)

山田 太郎	5391	4628	55	74	175	98
鈴木 花子	7308	9462	45	48	160	120
・ ・ ・		・ ・ ・				
佐藤 元	9284	3410	34	58	175	136

【図７】



【図８】



フロントページの続き

(56)参考文献 特開２００２－３５９６１８（ＪＰ，Ａ）
特開２０００－１５５７９１（ＪＰ，Ａ）
特開２００４－２５２５０９（ＪＰ，Ａ）
伊藤 智，‘グリッド技術を利用したセキュアデータベース 分散ファイルシステム(Gfarm)で情報漏洩を防止する’，産総研TODAY，産業技術総合研究所，２００５年 7月 1日，第5巻 第7号，32頁-33頁
鈴木 英男，‘簡単で効果的な個人情報保護の方法 -データ保存法とデータ入力法-’，情報処理学会研究報告，日本，社団法人情報処理学会，２００３年１２月１８日，第2003巻 第126号，31頁-36頁

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２４