

【公報種別】特許法第 17 条の 2 の規定による補正の掲載  
 【部門区分】第 7 部門第 3 区分  
 【発行日】平成 19 年 8 月 9 日 (2007.8.9)

【公開番号】特開 2006-33198 (P2006-33198A)  
 【公開日】平成 18 年 2 月 2 日 (2006.2.2)  
 【年通号数】公開・登録公報 2006-005  
 【出願番号】特願 2004-206482 (P2004-206482)  
 【国際特許分類】

**H 0 4 L      9/08      (2006.01)**

**G 0 6 F      21/24      (2006.01)**

**G 0 6 K      17/00      (2006.01)**

**H 0 4 L      9/10      (2006.01)**

【F I】

H 0 4 L      9/00      6 0 1 B

G 0 6 F      12/14      5 6 0 C

G 0 6 K      17/00      D

H 0 4 L      9/00      6 0 1 E

H 0 4 L      9/00      6 2 1 A

H 0 4 L      9/00      6 0 1 A

【手続補正書】

【提出日】平成 19 年 6 月 21 日 (2007.6.21)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

コンピュータを、

ユーザ側端末からユーザ情報が送信されたときに、ユーザ情報の全部または一部を暗号化するための暗号鍵を生成し、前記暗号鍵を用いて前記ユーザ情報の全部または一部を暗号化するとともに、前記全部または一部が暗号化されたユーザ情報をユーザ識別符号とともにユーザ管理データベースに登録し、前記暗号鍵と前記ユーザ識別符号とをユーザ側の端末に送信するユーザ管理サーバ、

前記ユーザ管理サーバから送信された前記暗号鍵と前記ユーザ識別符号とを所定の記憶媒体に記憶させるユーザ側端末、及び

前記記憶媒体に記憶された前記ユーザ識別符号に基づき前記ユーザ管理データベースからユーザ情報を取得し、前記記憶媒体に記憶された暗号鍵によりユーザ情報の暗号化部分を復号し、該ユーザ情報によりデータベースから所定のデータを取得するデータアクセス端末、

として機能させることを特徴とするプログラム。

【請求項 2】

請求項 1 記載のプログラムにおいて、前記ユーザ管理サーバを、

前記ユーザ側端末からユーザ情報が送信された場合に、ユーザ情報の全部または一部を暗号化するための暗号鍵を生成する暗号鍵生成手段、

前記ユーザ情報の全部または一部を前記暗号鍵を用いて暗号化する暗号化手段、

前記暗号鍵からユーザ識別符号を生成するユーザ識別符号生成手段、

前記暗号化されたユーザ情報と前記ユーザ識別符号とを前記ユーザ管理データベースに

登録する登録管理手段、及び

前記暗号鍵と前記ユーザ識別符号とを前記ユーザ側端末に送信する通信手段、  
として機能させることを特徴とするプログラム。

【請求項 3】

請求項 1 または請求項 2 記載のプログラムにおいて、前記データアクセス端末を、  
前記記憶媒体から前記暗号鍵と前記ユーザ識別符号とを取得するデータ読取手段、  
前記ユーザ識別符号に基づき前記ユーザ管理データベースからユーザ情報を取得する情報取得手段、

前記取得したユーザ情報のうち暗号化されている部分を前記暗号鍵を用いて復号する復号化手段、及び

前記復号後のユーザ情報に基づきデータベースから所定のデータを取得するデータ取得手段、

として機能させることを特徴とするプログラム。

【請求項 4】

請求項 1 から請求項 3 のいずれか一項記載のプログラムにおいて、前記ユーザ識別符号は、前記暗号鍵からハッシュ関数を用いて求めたハッシュ値であることを特徴とするプログラム。

【請求項 5】

請求項 1 から請求項 4 のいずれか一項記載のプログラムにおいて、前記記憶媒体は、非接触式の IC カードであることを特徴とするプログラム。

【請求項 6】

ユーザ管理サーバが、ユーザ側端末からユーザ情報が送信されたときに、ユーザ情報の全部または一部を暗号化するための暗号鍵を生成し、前記暗号鍵を用いて前記ユーザ情報の全部または一部を暗号化するとともに、前記全部または一部が暗号化されたユーザ情報をユーザ識別符号とともにユーザ管理データベースに登録し、前記暗号鍵と前記ユーザ識別符号とをユーザ側の端末に送信し、

ユーザ側端末が、前記ユーザ管理サーバから送信された前記暗号鍵と前記ユーザ識別符号とを所定の記憶媒体に記憶させ、

データアクセス端末が、前記記憶媒体に記憶された前記ユーザ識別符号に基づき前記ユーザ管理データベースからユーザ情報を取得し、前記記憶媒体に記憶された暗号鍵によりユーザ情報の暗号化部分を復号し、該ユーザ情報によりデータベースから所定のデータを取得する、

ことを特徴とするデータ管理方法。

【請求項 7】

ユーザ側端末からユーザ情報が送信されたときに、ユーザ情報の全部または一部を暗号化するための暗号鍵を生成し、前記暗号鍵を用いて前記ユーザ情報の全部または一部を暗号化するとともに、前記全部または一部が暗号化されたユーザ情報をユーザ識別符号とともにユーザ管理データベースに登録し、前記暗号鍵と前記ユーザ識別符号とをユーザ側の端末に送信するユーザ管理サーバと、

前記ユーザ管理サーバから送信された前記暗号鍵と前記ユーザ識別符号とを所定の記憶媒体に記憶させるユーザ側端末と、

前記記憶媒体に記憶された前記ユーザ識別符号に基づき前記ユーザ管理データベースからユーザ情報を取得し、前記記憶媒体に記憶された暗号鍵によりユーザ情報の暗号化部分を復号し、該ユーザ情報によりデータ管理データベースからデータを取得するデータアクセス端末と、

を備えることを特徴とするデータ管理システム。