(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4047573号
(P4047573)

(45)発行日　平成20年2月13日(2008.2.13)　(24)登録日　平成19年11月30日(2007.11.30)

(51)Int.Cl.			F I		
H04L	9/14	(2006.01)	H04L	9/00	641
G09C	1/00	(2006.01)	G09C	1/00	310
H04L	9/08	(2006.01)	H04L	9/00	601C
H04L	9/32	(2006.01)	H04L	9/00	673D

請求項の数 7　(全 19 頁)

(21)出願番号　特願2001-341037(P2001-341037)
(22)出願日　平成13年11月6日(2001.11.6)
(65)公開番号　特開2003-143131(P2003-143131A)
(43)公開日　平成15年5月16日(2003.5.16)
審査請求日　平成16年11月5日(2004.11.5)

(73)特許権者　301063496
東芝ソリューション株式会社
東京都港区芝浦一丁目１番１号
(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊

最終頁に続く

(54)【発明の名称】電子情報管理装置及びプログラム

(57)【特許請求の範囲】

【請求項１】

管理サーバ装置に接続され、電子情報を管理する電子情報管理装置であって、

入力された電子情報を書込処理する際に、複数の暗号化アルゴリズムのうちのいずれかの暗号化アルゴリズムに基づいて前記電子情報を暗号化し、暗号化電子情報を得る情報暗号化手段と、

前記情報暗号化手段により得られた暗号化電子情報を複数のフラグメントに分割する分割手段と、

前記分割手段により分割された各フラグメントをそれぞれランダムな物理位置情報を指定して書込処理するフラグメント書込手段と、

前記フラグメント書込手段で用いた各物理位置情報及び前記暗号化手段で用いた暗号化アルゴリズム名を含む対応テーブルを作成する対応テーブル作成手段と、

前記対応テーブル作成手段により作成された対応テーブルを暗号化し、得られた暗号化対応テーブルを物理位置情報を指定して書込処理する暗号化対応テーブル書込手段と、

前記暗号化対応テーブル書込手段で用いた物理位置情報を前記管理サーバ装置に送信するテーブル位置送信手段と、

を備えたことを特徴とする電子情報管理装置。

【請求項２】

請求項１に記載の電子情報管理装置において、

前記テーブル位置送信手段により送信された物理位置情報を前記管理サーバ装置から取

得するテーブル位置取得手段と、
前記テーブル位置取得手段により取得された物理位置情報に基づいて、前記暗号化対応テーブルを読出処理する暗号化対応テーブル読出手段と、
前記暗号化対応テーブルにより読出処理された暗号化対応テーブルを復号し、対応テーブルを得る対応テーブル復号手段と、
前記対応テーブル復号手段により得られた対応テーブルに基づいて、各フラグメントを読出すフラグメント読出手段と、
前記フラグメント読出手段により読出された各フラグメントを結合する結合手段と、
前記結合手段により結合された各フラグメントからなる暗号化電子情報を前記対応テーブルに記述された暗号化アルゴリズム名の暗号化アルゴリズムに基づいて復号し、得られた電子情報を出力する情報復号手段と、
を備えたことを特徴とする電子情報管理装置。
【請求項３】
管理サーバ装置に接続され、電子情報を管理する電子情報管理装置に用いられるプログラムであって、
前記電子情報管理装置のコンピュータを、
入力された電子情報を書込処理する際に、複数の暗号化アルゴリズムのうちのいずれかの暗号化アルゴリズムに基づいて前記電子情報を暗号化し、暗号化電子情報を得る情報暗号化手段、
前記情報暗号化手段により得られた暗号化電子情報を複数のフラグメントに分割する分割手段、
前記分割手段により分割された各フラグメントをそれぞれランダムな物理位置情報を指定して書込処理するフラグメント書込手段、
前記フラグメント書込手段で用いた各物理位置情報及び前記暗号化手段で用いた暗号化アルゴリズム名を含む対応テーブルを作成する対応テーブル作成手段、
前記対応テーブル作成手段により作成された対応テーブルを暗号化し、得られた暗号化対応テーブルを物理位置情報を指定して書込処理する暗号化対応テーブル書込手段、
前記暗号化対応テーブル書込手段で用いた物理位置情報を前記管理サーバ装置に送信するテーブル位置送信手段、
として機能させるためのプログラム。
【請求項４】
請求項３に記載のプログラムにおいて、
前記電子情報管理装置のコンピュータを、
前記テーブル位置送信手段により送信された物理位置情報を前記管理サーバ装置から取得するテーブル位置取得手段、
前記テーブル位置取得手段により取得された物理位置情報に基づいて、前記暗号化対応テーブルを読出処理する暗号化対応テーブル読出手段、
前記暗号化対応テーブルにより読出処理された暗号化対応テーブルを復号し、対応テーブルを得る対応テーブル復号手段、
前記対応テーブル復号手段により得られた対応テーブルに基づいて、各フラグメントを読出すフラグメント読出手段、
前記フラグメント読出手段により読出された各フラグメントを結合する結合手段、
前記結合手段により結合された各フラグメントからなる暗号化電子情報を前記対応テーブルに記述された暗号化アルゴリズム名の暗号化アルゴリズムに基づいて復号し、得られた電子情報を出力する情報復号手段、
として機能させるためのプログラム。
【請求項５】
請求項３に記載のプログラムにおいて、
前記電子情報管理装置のコンピュータを、
前記暗号化対応テーブル書込手段及び前記テーブル位置送信手段に代えて、

前記対応テーブル作成手段により作成された対応テーブルを暗号化し、得られた暗号化対応テーブルを前記管理サーバ装置に送信するテーブル送信手段、
として機能させるためのプログラム。
【請求項６】
請求項５に記載のプログラムにおいて、
前記電子情報管理装置のコンピュータを、
前記テーブル送信手段により送信された暗号化対応テーブル、又はこの暗号化対応テーブルから復号により得られる対応テーブルが前記管理サーバ装置により暗号化されてなる別の暗号化対応テーブルを前記管理サーバ装置から取得するテーブル取得手段、
前記テーブル取得手段により取得された暗号化対応テーブルを復号し、対応テーブルを得る対応テーブル復号手段、
前記対応テーブル復号手段により得られた対応テーブルに基づいて、各フラグメントを読出すフラグメント読出手段、
前記フラグメント読出手段により読出された各フラグメントを結合する結合手段、
前記結合手段により結合された各フラグメントからなる暗号化電子情報を前記対応テーブルに記述された暗号化アルゴリズム名の暗号化アルゴリズムに基づいて復号し、得られた電子情報を出力する情報復号手段、
として機能させるためのプログラム。
【請求項７】
請求項４又は請求項６に記載のプログラムにおいて、
前記電子情報管理装置のコンピュータを、
前記分割手段により分割された各フラグメントをそれぞれ圧縮し、第１の圧縮値を得る圧縮手段、
前記フラグメント読出手段により読出された各フラグメントをそれぞれ圧縮し、得られた第２の圧縮値と、前記圧縮手段により得られた第１の圧縮値とを比較し、両者が一致したとき、前記結合手段による結合を許可する検証手段、
として機能させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、電子情報を安全に記憶及び管理する電子情報管理装置及びプログラムに関する。
【０００２】
【従来の技術】
電子情報を扱う電子計算機には、悪意の第三者による電子情報の不正な閲覧及び改ざんや、同一の電子計算機を共有するユーザによる誤った操作等から電子情報を保護するための電子情報管理システムが広く用いられている。
【０００３】
この種の電子情報管理システムは、オペレーティング・システム（ＯＳ）などにより、電子情報を安全に記憶装置に保存して管理する方式が多い。しかしながら、ＯＳによる管理方式は、記憶装置の盗難及び／又は解析等により、記憶装置内の電子情報が盗まれる可能性がある。
【０００４】
また、電子情報を盗難から保護するように、ファイル暗号化ツールなどのツール群を用いる方式がある。しかしながら、ファイル暗号化ツールを用いる方式では、暗号化方式が既知である上、解読の手掛かりとなる鍵情報などが記憶装置に保存されている場合があり、依然として電子情報が盗まれる可能性が残る。
【０００５】
一方、記憶装置の盗難を防ぐ観点から、鍵情報などをＩＣカード（スマートカード）などの携帯装置に記憶してユーザが携帯する方式が考えられる。しかしながら、鍵情報を携帯

する方式は、ユーザ毎に異なる暗号化鍵を設定することから、ユーザ間での情報共有が困難となってしまう。

【０００６】

【発明が解決しようとする課題】

以上説明したように電子情報管理システムでは、ＯＳによる管理方式やファイル暗号化ツールを用いる方式の場合、記憶装置の盗難及び／又は解析により、電子情報が盗まれる可能性がある。

【０００７】

また、ユーザ毎に暗号化鍵を設定する場合、異なるユーザ間での情報共有が困難となってしまう。

【０００８】

本発明は上記実情を考慮してなされたもので、記憶装置を解析されても、記憶内容の解読を阻止でき、安全性を向上し得る電子情報管理装置及びプログラムを提供することを目的とする。

【０００９】

また、本発明の他の目的は、ユーザ毎に暗号化鍵を設定する場合でも、各ユーザ間での情報共有を容易化し得る電子情報管理装置及びプログラムを提供することにある。

【００１０】

【課題を解決するための手段】

第１の発明は、管理サーバ装置に接続され、電子情報を管理する電子情報管理装置であって、入力された電子情報を書込処理する際に、複数の暗号化アルゴリズムのうちのいずれかの暗号化アルゴリズムに基づいて前記電子情報を暗号化し、暗号化電子情報を得る情報暗号化手段と、前記情報暗号化手段により得られた暗号化電子情報を複数のフラグメントに分割する分割手段と、前記分割手段により分割された各フラグメントをそれぞれランダムな物理位置情報を指定して書込処理するフラグメント書込手段と、前記フラグメント書込手段で用いた各物理位置情報及び前記暗号化手段で用いた暗号化アルゴリズム名を含む対応テーブルを作成する対応テーブル作成手段と、前記対応テーブル作成手段により作成された対応テーブルを暗号化し、得られた暗号化対応テーブルを物理位置情報を指定して書込処理する暗号化対応テーブル書込手段と、前記暗号化対応テーブル書込手段で用いた物理位置情報を前記管理サーバ装置に送信するテーブル位置送信手段と、を備えた電子情報管理装置である。

【００１１】

これにより、電子情報は、情報暗号化手段で暗号化され、分割手段で各フラグメントに分割されて、フラグメント書込手段により、ランダムな物理位置に書込まれる。

【００１２】

ここで、電子情報の読出に必要な物理位置情報と、暗号化に用いた暗号化アルゴリズムの名称とを含む対応テーブルは、暗号化されて書込まれている。このため、各フラグメントの物理位置情報や、暗号化に用いた暗号アルゴリズムの特定が困難となる。

【００１３】

また、暗号化対応テーブルを解読するとしても、暗号化対応テーブルの物理位置情報が管理サーバ装置で管理されているので、解読以前に暗号化対応テーブルの特定が困難となっている。

【００１４】

従って、電子情報管理装置の記憶装置を解析されても、記憶内容の解読を阻止でき、安全性を向上させることができる。

【００１５】

また、ユーザ毎に暗号化鍵を設定する場合でも、管理サーバ側でユーザのアクセス権限に応じて対応テーブル取得情報を送信することにより、各ユーザ間での情報共有を容易化することができる。

【００１６】

第２の発明は、第１の発明において、前記テーブル位置送信手段により送信された物理位置情報を前記管理サーバ装置から取得するテーブル位置取得手段と、前記テーブル位置取得手段により取得された物理位置情報に基づいて、前記暗号化対応テーブルを読出処理する暗号化対応テーブル読出手段と、前記暗号化対応テーブルにより読出処理された暗号化対応テーブルを復号し、対応テーブルを得る対応テーブル復号手段と、前記対応テーブル復号手段により得られた対応テーブルに基づいて、各フラグメントを読出すフラグメント読出手段と、前記フラグメント読出手段により読出された各フラグメントを結合する結合手段と、前記結合手段により結合された各フラグメントからなる暗号化電子情報を前記対応テーブルに記述された暗号化アルゴリズム名の暗号化アルゴリズムに基づいて復号し、得られた電子情報を出力する情報復号手段と、を備えた電子情報管理装置である。

【００１７】

これにより、第１の発明の作用に加え、読出処理の際には、電子情報を容易且つ確実に読み出すことができる。

【００２０】

なお、上記各発明は、「装置」として表現したが、これに限らず、「プログラム」、「方法」又は「システム」といった別の表現により表してもよい。

【００２１】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照して説明する。

（第１の実施形態）

図１は本発明の第１の実施形態に係る電子情報管理システムの構成を示す模式図であり、図２は同システムで管理される各電子情報の記憶形態を示す模式図である。また、図３は各電子情報の管理用の対応テーブルの構成を示す模式図であり、図４は対応テーブルの管理用の対応テーブル取得情報の構成を示す模式図である。

【００２２】

この電子情報管理システムは、図１に示すように、記憶装置１に接続されたクライアント装置２がインターネット及び／又は専用線などの通信回線３を介して管理サーバ４に接続されている。

【００２３】

ここで、記憶装置１は、クライアント装置２から読出／書込可能に、電子情報Ｅの各フラグメントｅ、及び対応テーブルＴが記憶されるものであり、図１の如き接続された形態に限らず、クライアント装置２に内蔵されていてもよく、又は着脱自在な小型の記憶媒体であってもよい。

【００２４】

電子情報Ｅは、図２に示すように、クライアント装置２内で暗号化により暗号化電子情報Ｅ’に変換された後に各フラグメントｅに分割された状態で、記憶装置１内の格納領域１ａに記憶される。なお、フラグメントｅは、暗号化電子情報Ｅ’を固定長又はランダムなサイズに分割した単位である。なお、フラグメントは、信頼性向上の観点から、シークレット・シェアリングや誤り訂正符号などの方法により、冗長性を付加させてもよい。

【００２５】

対応テーブルＴは、記憶装置１内の各フラグメントｅを復号するためのデータの集合であり、図３に示すように、共通情報Ｃ及び格納領域情報Ｍを含んでおり、管理サーバ４の公開鍵により暗号化された状態（以下、暗号化対応テーブルＴ’ともいう）で記憶装置１内の格納領域に記憶される。

【００２６】

なお、対応テーブルＴは、規定されたアクセス・ルールに従って分類された電子情報群毎にまとめられ、それぞれの対応テーブルＴ毎に異なる公開鍵が使用されて暗号化され、暗号化対応テーブルＴ’として記憶装置１に記憶される。

【００２７】

共通情報Ｃは、保存する電子情報Ｅを同定するための同定情報ｃ１、暗号化に使用した暗

号化アルゴリズム名ｃ２、使用した暗号化アルゴリズムに対応した復号鍵ｃ３、を含んで構成されている。

【００２８】

同定情報ｃ１は、例えばファイル名やハッシュ値といった識別子などのように、電子情報Ｅを同定可能な任意の情報が使用可能である。

【００２９】

暗号化アルゴリズム名ｃ２及び復号鍵ｃ３は、基本的には任意であるが、高速な処理の観点から、本実施形態では共通鍵暗号方式に対応したものが使用される。これに伴い、以下の説明では復号鍵ｃ３を共通鍵ｃ３ともいう。

【００３０】

格納領域情報Ｍは、各フラグメントｅ毎に、結合順番ｍ１、サイズｍ２、記憶装置１内の物理位置情報ｍ３、及び圧縮値ｍ４を含んで構成されている。

【００３１】

なお、格納領域情報Ｍは、記憶装置１内における各フラグメントｅの格納場所を示すものであれば、任意の情報が使用可能である。例えば、物理位置情報ｍ３としては、物理アドレスやポインタなどが使用可能である。また、サイズｍ２は省略してもよい。

【００３２】

圧縮値ｍ４は、各フラグメントｅの検証用のデータであり、各フラグメントｅをハッシュ関数などの一方向性関数で処理して得た値である。

【００３３】

一方、クライアント装置２は、通信インタフェース１０、オペレーティングシステム（以下、ＯＳという）２０及び情報管理モジュール３０を備えており、情報管理モジュール３０が記憶装置１に接続されている。

【００３４】

通信インタフェース１０は、通信回線３と情報管理モジュール３０との間のインターフェースである。

ＯＳ２０は、通常のＯＳの機能に加え、情報管理モジュール３０を管理し、情報管理モジュール３０を介して記憶装置１内の電子情報にアクセスする機能をもっている。

【００３５】

情報管理モジュール３０は、相互認証部３１、対応テーブル管理部３２、乱数生成部３３、アルゴリズム選択部３４、鍵生成部３５、暗復号部３６、入出力部３７及び保存／読取部３８を備えている。

【００３６】

ここで、相互認証部３１は、管理サーバ４との相互認証処理を実行する認証部３１ａと、管理サーバ４との間での通信処理を実行する通信部３１ｂとを備え、認証部３１ａによる相互認証結果が正当のとき、通信部３１ｂにより、管理サーバ４から送信された対応テーブル取得情報Ｇを対応テーブル管理部３２に送出し、また、対応テーブル管理部３２から受けた対応テーブル名及び物理位置情報を通信インタフェース１０を介して通信回線３上の管理サーバ４に通信するものである。

【００３７】

なお、相互認証部３１では、相互認証方式として、公開鍵暗号方式に基づくチャレンジ・アンド・レスポンス方式や公開鍵基盤を利用した認証など、任意の認証方式が使用可能である。鍵交換方法も同様に任意の方式が使用可能である。

【００３８】

対応テーブル管理部３２は、管理サーバ４との認証成立後に、相互認証部３１からの対応テーブル取得情報Ｇに基づいて、保存／読取部３８を介して記憶装置１から暗号化対応テーブルＴ’を読出して復号する機能と、記憶装置１からの読出の際に、復号で得た対応テーブルＴに基づいて、保存／読取部３８を制御して記憶装置１内の各フラグメントｅを暗復号部３６に送出させる機能とをもっている。

【００３９】

また一方、対応テーブル管理部３２は、記憶装置１への書込の際に、各部３６～３８から受ける各情報に基づいて対応テーブルＴを作成又は更新する機能と、対応テーブルＴを暗号化して暗号化対応テーブルＴ’を得る機能と、暗号化対応テーブルＴ’を保存／読取部３８を介して記憶装置１に書込む機能と、記憶装置１内の暗号化対応テーブルＴ’の物理位置情報及び対応テーブル名を含む対応テーブル保存情報を管理サーバ４宛に相互認証部３１に送出する機能とをもっている。

【００４０】

対応テーブル取得情報Ｇは、図４に示すように、対応テーブル名ｇ１、対応テーブルＴを復号可能な管理サーバ４の秘密鍵ｇ２、及び対応テーブル格納領域情報ｇ３を含んで構成されている。

【００４１】

対応テーブル名ｇ１は、暗号化対応テーブルＴ’の名称であり、対応テーブルの名称に対応する。対応テーブル格納領域情報ｇ３は、記憶装置１内における暗号化対応テーブルＴ’の物理位置を示す物理位置情報である。

【００４２】

乱数生成部３３は、ＯＳ２０による入出力部３７へのアクセス時に乱数を生成し、得られた乱数を暗号アルゴリズム選択部３４及び鍵生成部３５に送出する機能をもっている。

【００４３】

アルゴリズム選択部３４は、乱数生成部３３から送出された乱数により、複数の共通鍵暗号方式の暗号アルゴリズムのうち、いずれか１つの暗号アルゴリズムを選択し、選択結果を鍵生成部３５及び暗復号部３６に送出する機能をもっている。

【００４４】

鍵生成部３５は、アルゴリズム選択部３４が選択した暗号アルゴリズムに使用可能な共通鍵を、乱数生成部３３から送出された乱数に基づいてランダムに生成し、得られた共通鍵ｃ３を暗復号部３６に送出する機能をもっている。

【００４５】

暗復号部３６は、情報暗号化部３６１、分割部３６２、圧縮部３６３、検証部３６４、結合部３６５及び情報復号部３６６を備えている。

情報暗号化部３６１は、入出力部３７から入力された電子情報Ｅを、暗号アルゴリズム選択部３４により選択された暗号アルゴリズムと鍵生成部３５により生成された共通鍵ｃ３とに基づいて暗号化し、得られた暗号化電子情報Ｅ’を分割部３６２に送出する機能をもっている。また、情報暗号化部３６１は、暗号化に使用した暗号アルゴリズムの名称ｃ２及び共通鍵ｃ３を対応テーブル管理部３２に送出する機能をもっている。

【００４６】

分割部３６２は、情報暗号化部３６１から送出された暗号化電子情報Ｅ’を分割して複数のフラグメントｅを作成し、各フラグメントｅ及びその結合順番ｍ１（とサイズｍ２）を圧縮部３６３に送出する機能をもっている。なお、サイズｍ２は、全て同一値の場合又は結合順番ｍ１毎に一定の場合などのように、別途、得られる場合には省略してもよい。

【００４７】

圧縮部３６３は、分割部３６２により送出された各フラグメントｅ、結合順番ｍ１及びサイズｍ２を保存／読取部３８に転送する機能と、各フラグメントｅを圧縮して得た圧縮値ｍ４を対応テーブル管理部３２に送出する機能とをもっている。

【００４８】

検証部３６４は、保存／読取部３８により読取られた各フラグメントｅを圧縮部３６３と同一処理により圧縮して得た圧縮値と、対応テーブルＴ内の該当する圧縮値ｍ４とを比較し、両圧縮値が一致したときのみ各フラグメントｅを結合部３６５に送出する機能をもっている。

【００４９】

結合部３６５は、検証部３６４から送出された各フラグメントｅを結合して暗号化電子情報Ｅ’を作成し、得られた暗号化電子情報Ｅ’を情報復号部３６６に送出する機能をもっ

ている。
【００５０】
情報復号部３６６は、結合部３６５から受けた暗号化電子情報Ｅ’を、対応テーブルＴの暗号化アルゴリズム名ｃ２及び共通鍵ｃ３に基づいて復号し、得られた電子情報Ｅを入出力部３７に送出する機能をもっている。
【００５１】
入出力部３７は、入力部３７ａ及び出力部３７ｂを備えている。
入力部３７ａは、ＯＳ２０から受けた電子情報Ｅとその同定情報及び書込要求のうち、電子情報Ｅを情報暗号化部３６１に入力する機能と、書込要求の送出により乱数生成部３３を起動する機能と、同定情報を対応管理テーブル３２に送出する機能とをもっている。
【００５２】
出力部３７ｂは、情報復号部３６６から受けた電子情報ＥをＯＳ２０に出力する機能をもっている。
【００５３】
保存／読取部３８は、保存部３８ａ及び読取部３８ｂを備えている。
保存部３８ａは、圧縮部３６３から受けた各フラグメントｅを記憶装置１に保存する機能と、保存の際に、乱数生成部３３から受けた乱数に基づいて格納領域を調整する機能と、各フラグメントｅを保存した格納領域を示す物理位置情報ｍ３及び各フラグメントの結合順番ｍ１を対応テーブル管理部３２に送出する機能とをもっている。
【００５４】
ここで、格納領域を調整する機能は、例えば、既存の各フラグメントｅを別の格納領域に移動させる移動方式や、既存の各フラグメントｅをそのまま保持しつつ、新たな各フラグメントｅを新たな格納領域に格納する新規追加方式などが適宜、使用可能となっている。
【００５５】
また、保存部３８ａは、各フラグメントｅを保存した格納領域を示す物理位置情報ｍ３、各フラグメントｅの結合順番ｍ１及びサイズｍ２を対応テーブル管理部３２に送出する機能をもっている。
【００５６】
読取部３８ｂは、対応テーブル管理部３２の制御により、記憶装置１から暗号化対応テーブルＴ’を読み出して対応テーブル管理部３２に送出する機能と、対応テーブルＴを復号して得た対応テーブル管理部３２による制御により、記憶装置１内の各フラグメントｅを読み出して検証部３６４に送出する機能とをもっている。
【００５７】
一方、管理サーバ４は、クライアント装置２からのログイン要求及びログオフ要求をそれぞれ処理する機能をもっている。
ログイン要求を処理する機能としては、クライアント装置２との間で相互認証を行なう機能と、相互認証の結果が正当なとき、ユーザの認証情報を認証する機能と、ユーザの認証結果が正当なとき、所定のアクセスルール及びクライアント装置２から送信された読出要求に基づいて、予め記憶した対応テーブル取得情報Ｇをクライアント装置２に送信する機能とをもっている。なお、ユーザの認証機能は省略してもよい。
【００５８】
ログオフ要求を処理する機能としては、クライアント装置２からのログオフ要求に基づいて、自装置４の公開鍵をクライアント装置２に送信する機能と、クライアント装置２から送信された対応テーブル保存情報に基づいて、対応テーブル取得情報Ｇを生成して自装置４に記憶する機能とをもっている。
【００５９】
なお、クライアント装置２、情報管理モジュール３０及び管理サーバ４は、それぞれソフトウェア構成及び／又はハードウェア構成により実現可能となっている。ソフトウェア構成で実現される場合、予め各装置２，４の機能を実現するためのプログラムが記憶媒体又はネットワーク等から各装置２，４にインストールされている。

【００６０】
次に、以上のように構成された電子情報管理システムの動作を図５のシーケンス図、図６と図８の模式図、及び図７と図９のフローチャートを用いて説明する。
【００６１】
（ログイン時、時刻ｔ１～ｔ４、ＳＴ１）
クライアント装置２は、ユーザの操作により、ログインされたとする。
クライアント装置２の情報管理モジュール３０は、相互認証部３１により、図５に示すように、管理サーバ４にログイン要求を送信し（時刻ｔ１）、管理サーバ４との間で相互に自己の正当性を認証する相互認証処理を実行する（時刻ｔ２）。
【００６２】
装置２，４間の相互認証が成立すると、ユーザの認証情報を管理サーバ４にて認証する。ユーザの認証成立後、情報管理モジュール３０と管理サーバ４とは相互３０，４の間で安全な通信路を確立する。
【００６３】
相互認証とユーザ認証の完了後、管理サーバ４は、予め設定されたアクセス・ルールに従って、認証したユーザのアクセス権限に対応する対応テーブル取得情報Ｇをクライアント装置２に送信する（時刻ｔ３）。以後、管理サーバ４は、ログオフ完了まで、他のユーザに対応テーブル取得情報Ｇを送信せず、排他処理を行なう。
【００６４】
クライアント装置２においては、対応テーブル管理部３２がこの対応テーブル取得情報Ｇに基づいて、保存／読出部３８を介して記憶装置１から暗号化対応テーブルＴ’を読み出し（時刻ｔ４）、この暗号化対応テーブルＴ’を対応テーブル取得情報Ｇ内の秘密鍵ｇ２で復号し、対応テーブルＴを取得する（ＳＴ１）。
【００６５】
（読出処理；時刻ｔ５，ＳＴ２～ＳＴ５）
次に、読取処理について図６及び図７を用いて説明する。
いま、ＯＳ２０から読取要求が入力部３７ａを介して対応テーブル管理部３２に入力されたとする。対応テーブル管理部３２は、読取要求の対象となる電子情報の同定情報に基づいて、対応テーブルＴに記述された各情報を同定する。
【００６６】
続いて、対応テーブル管理部３２は、格納領域情報Ｍに基づいて、読取部３８ｂを制御する。読取部３８ｂは、記憶装置１内の該当する各フラグメントｅを読み出して検証部３６４に送出する（ＳＴ２）。
【００６７】
検証部３６４は、送出された各フラグメントｅを圧縮部３６３と同一処理により圧縮して得た圧縮値と、対応テーブル管理部３２から受ける対応テーブルＴ内の該当する圧縮値ｍ４とを比較し、改ざんされてない旨（両圧縮値の一致）を検証すると（ＳＴ３）、各フラグメントｅを結合部３６５に送出する。
【００６８】
結合部３６５は、これら各フラグメントｅを結合して暗号化電子情報Ｅ’を作成し（ＳＴ４）、得られた暗号化電子情報Ｅ’を情報復号部３６６に送出する。
【００６９】
一方、対応テーブル管理部３２は、対応テーブルＴ内の共通鍵ｃ３を情報復号部３６６に送出すると共に、対応テーブルＴ内の暗号アルゴリズム名ｃ２に該当する暗号アルゴリズムを暗号アルゴリズム選択部３４を介して情報復号部３６６に送出する。
【００７０】
情報復号部３６６は、結合部３６５からの暗号化電子情報Ｅ’をこれら共通鍵ｃ３及び暗号アルゴリズムに基づいて復号し（ＳＴ５）、得られた電子情報Ｅを出力部３７ｂに送出する。
【００７１】

出力部３７ｂは、この電子情報ＥをＯＳ２０に送出する。
（書込処理；時刻ｔ５、ＳＴ１１～ＳＴ１６）
次に、書込処理について図８及び図９を用いて説明する。いま、ＯＳ２０から電子情報Ｅが入力部３７ａを介して情報暗号化部３６１に入力されると共に、ＯＳ２０から電子情報Ｅの同定情報ｃ１及び書込要求が入力部３７ａを介して対応テーブル管理部３２に入力され、また、ＯＳ２０から書込要求が入力部３７ａを介して乱数生成部３３に入力されたとする。
【００７２】
乱数生成部３３は、この書込要求を受けると、乱数を生成し、得られた乱数を暗号アルゴリズム選択部３４及び鍵生成部３５に送出する。
【００７３】
アルゴリズム選択部３４は、この乱数により、複数の共通鍵暗号方式の暗号アルゴリズムのうち、いずれか１つの暗号アルゴリズムを選択し、選択結果を鍵生成部３５及び暗復号部３６に送出する。
【００７４】
鍵生成部３５は、選択された暗号アルゴリズムに使用可能な共通鍵を、乱数成部３３から受けた乱数に基づいてランダムに生成し（ＳＴ１１）、得られた共通鍵ｃ３を暗復号部３６に送出する。
【００７５】
情報暗号化部３６１は、入力部３７ａからの電子情報Ｅを、送出された暗号アルゴリズム及び共通鍵ｃ３に基づいて暗号化し、得られた暗号化電子情報Ｅ’を分割部３６２に送出する一方、暗号化に使用した暗号アルゴリズムの名称ｃ２及び共通鍵ｃ３を対応テーブル管理部３２に送出する。
【００７６】
分割部３６２は、情報暗号化部３６１から受けた暗号化電子情報Ｅ’を複数のフラグメントｅに分割し（ＳＴ１２）、各フラグメントｅ、その結合順番ｍ１及びサイズｍ２を圧縮部３６３に送出する。
【００７７】
圧縮部３６３は、分割部３６２により送出された各フラグメントｅを個別に圧縮して各々の圧縮値ｍ４を生成し（ＳＴ１３）、得られた各圧縮値ｍ４を対応テーブル管理部３２に送出する一方、各フラグメントｅ、結合順番ｍ１及びサイズｍ２を保存部３８ａに転送する。
【００７８】
保存部３８ａは、乱数生成部３３から受けた乱数に基づいて記憶装置１の物理位置をランダムに決定し（ＳＴ１４）、この決定した物理位置に各フラグメントｅを保存する（ＳＴ１５）。
【００７９】
しかる後、保存部３８ａは、各フラグメントｅを保存した格納領域を示す物理位置情報ｍ３、各フラグメントｅの結合順番ｍ１及びサイズｍ２を対応テーブル管理部３２に送出する。
【００８０】
対応テーブル管理部３２は、入力部３７ａからの同定情報ｃ１、情報暗号化部３６１からの暗号アルゴリズム名ｃ２及び共通鍵ｃ３、圧縮部３６３からの圧縮値ｍ４、保存部３８ａからの結合順番ｍ１、サイズｍ２及び物理位置情報ｍ３に基づいて、対応テーブルＴを作成又は更新する（ＳＴ１６）。
【００８１】
（ログオフ時、時刻ｔ６～ｔ９）
クライアント装置２は、ユーザの操作により、ログオフされたとする。
クライアント装置２の情報管理モジュール３０は、通信部３１ｂにより、管理サーバ４にログオフ要求を送信し（時刻ｔ６）、管理サーバ４から対応テーブルＴの暗号化用の公開

鍵を取得する（時刻ｔ７）。

【００８２】

対応テーブル管理部３２は、得られた対応テーブルＴをこの公開鍵で暗号化して暗号化対応テーブルＴ’を得ると、この暗号化対応テーブルＴ’及び公開鍵を保存部３８ａを介して記憶装置１に書込む（時刻ｔ８）。

【００８３】

また、対応テーブル管理部３２は、記憶装置１内の暗号化対応テーブルＴ’の物理位置情報及び対応テーブル名を保存部３８ａから受けると、これら物理位置情報及び対応テーブル名を含む対応テーブル保存情報を通信部３１ｂ及び通信インタフェース１０を介して管理サーバ４宛に送信する（時刻ｔ９）。

【００８４】

管理サーバ４は、クライアント装置２に送信した公開鍵に対応する秘密鍵ｇ２と、クライアント装置２より取得した物理位置情報及び対応テーブル名ｇ１から対応テーブル取得情報Ｇを生成し、自装置４で管理する。

【００８５】

上述したように本実施形態によれば、暗号化した電子情報Ｅを分割して記憶装置１内にランダムに書込み、且つ読出と復号に必要な対応テーブルＴを隠蔽し、且つ対応テーブル取得情報Ｇを管理サーバ４側に管理させる構成により、記憶装置１を解析されても記憶内容の解読を阻止することができる。

【００８６】

詳しくは、電子情報Ｅは、情報暗号化部３６１で暗号化され、分割部３６２で各フラグメントｅに分割されて、保存部３８ａにより、記憶装置１のランダムな物理位置に書込まれる。

【００８７】

しかしながら、電子情報Ｅの読出に必要な物理位置情報ｍ３と、暗号化に用いた暗号化アルゴリズムの名称ｃ２とを含む対応テーブルＴは、暗号化されて書込まれている。このため、各フラグメントｅの特定や、暗号化に用いた暗号アルゴリズムの特定が困難となる。

【００８８】

例えば各フラグメントｅへの分割により、暗号化した電子情報Ｅを解読しようとすると、分割された全てのフラグメントｅを収集する必要が生じる。

【００８９】

しかしながら、記憶装置１が複数の物理ディスクを仮想的に統合した仮想記憶装置などの場合、各フラグメントｅが各物理ディスクに分散されるので、全てのフラグメントｅを収集することが極めて困難となる。

【００９０】

また、各フラグメントｅの長さをランダムにして分割した場合、記憶装置１内のフラグメント群が一つの暗号文にまとめられた状態でしか判断できず、個々のフラグメントｅの抽出が困難となる。

【００９１】

ここで、各フラグメントｅの直接的な収集を止めて、暗号化対応テーブルＴ’を解読するとしても、暗号化対応テーブルＴ’の物理位置情報が管理サーバ４で管理されているので、解読以前に暗号化対応テーブルＴ’の特定が困難となっている。

【００９２】

従って、いずれにしろ、クライアント装置２の記憶装置１を解析されても、記憶内容の解読を阻止でき、安全性を向上させることができる。

【００９３】

また、管理サーバ４が、クライアント装置２のユーザのアクセス権限に応じて対応テーブル取得情報Ｇを送信するので、異なるユーザ間での情報共有を容易に行うことができる。

【００９４】

特に、機密性の高い情報を扱う電子計算機などにおいて、ユーザに過度の負担をかけずに

、より安全な電子情報管理を行うことができる。
【００９５】
一方、読出処理の際には、対応テーブルＴに基づいて、電子情報を容易且つ確実に読み出すことができる。また、検証部３６４が圧縮部３６３による圧縮値と、読み出した各フラグメントによる圧縮値とを比較するので、各フラグメントが改ざんされた場合を検出することができる。
【００９６】
（第２の実施形態）
図１０は本発明の第２の実施形態に係る電子情報管理システムの構成を示す模式図であり、前述した図面と同一部分は同一符号を付してその詳しい説明を省略し、ここでは異なる部分について主に述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。
【００９７】
すなわち、本実施形態は、暗号化対応テーブルＴ’を記憶装置１に保存した第１の実施形態とは異なり、暗号化対応テーブルＴ’を管理サーバ４ｘに保存する構成となっている。
【００９８】
これに伴い、対応テーブル管理部３２ｘは、前述した対応テーブル取得情報Ｇ及び対応テーブル保存情報に関する機能に代えて、管理サーバ４との認証成立後に、相互認証部３１からの暗号化対応テーブルＴ’を自己の秘密鍵により復号して対応テーブルを得る機能と、記憶装置１に更新した対応テーブルＴを管理サーバ４ｘの公開鍵で暗号化して暗号化対応テーブルＴ”を得る機能と、暗号化対応テーブルＴ”を管理サーバ４宛に相互認証部３１に送出する機能と、暗号化対応テーブルＴ”の送出後、クライアント環境の対応テーブルＴを消去する機能とをもっている。
【００９９】
一方、管理サーバ４ｘは、前述した対応テーブル取得情報Ｇ及び対応テーブル保存情報に関する機能に代えて、図１１に示すように、ログイン要求を処理する機能において、相互認証及びユーザ認証の後に、クライアント装置２に送信する内容が暗号化対応テーブルＴ’となっている（時刻ｔ３ｘ）。
【０１００】
また、ログオフ要求を処理する機能において、クライアント装置２から送信された暗号化対応テーブルＴ”（時刻ｔ９）を自己の秘密鍵で復号して対応テーブルＴを得ると、この対応テーブルＴをクライアント装置２の公開鍵で暗号化して得られた暗号化対応テーブルＴ’を自装置４に記憶する機能となっている。
【０１０１】
以上のような構成により、対応テーブルＴをクライアント装置２ｘが持たずに管理サーバ４ｘ側で管理した状態であっても、第１の実施形態と同様の効果を得ることができる。
【０１０２】
なお、本実施形態は、対応テーブルＴを管理サーバ４ｘ側で管理する内容であればよい。例えば、クライアント装置２ｘと管理サーバ４ｘとの間において、暗号化対応テーブルＴ’，Ｔ”を通信せずに、平文状態の対応テーブルＴを通信する構成に変形しても、同様の効果を得ることができる。
【０１０３】
（第３の実施形態）
図１２は本発明の第３の実施形態に係る電子情報管理システムの構成を示す模式図である。
【０１０４】
本実施形態は、管理サーバ４ｘ側で対応テーブルＴを管理する第２の実施形態の変形例であり、記憶装置１及びクライアント装置２ｘを小型化して内蔵した携帯型電子計算機４０と、管理サーバ４ｘを小型化して内蔵した演算機能付きの情報格納装置５０とから構成されている。

【０１０５】
ここで、携帯型電子計算機４０は、例えば携帯情報端末ＰＤＡ又は携帯電話などで実現可能となっており、自己の記憶装置１の電子情報Ｅを読出す場合、情報格納装置５０の対応テーブルＴを取得し、第２の実施形態と同様に電子情報Ｅを読出可能となっている。また、自己の記憶装置１の電子情報Ｅを書込む場合も第２の実施形態と同様に、電子情報Ｅを書込んだ後、対応テーブルＴを情報格納装置５０に送信可能となっている。
【０１０６】
情報格納装置５０は、耐タンパー性メモリを有するＩＣカード（スマートカード）のような小型デバイスであり、生体識別及び／又はＰＩＮ(personal identification number、例、パスワード)等の本人確認情報に基づく個人識別機能を有している。なお、個人識別機能として生体識別装置を備えた場合、生体識別装置の一部としての生体識別情報読取装置は、携帯型電子計算機４０に配置されてもよい。また、ユーザ・ログイン時の初期認証は、装置間４０，５０の相互認証の後、指紋、声紋又は虹彩といった生体識別情報を情報格納装置５０にて照合し、情報格納装置５０の使用権限を取得すればよい。
【０１０７】
以上のような構成によれば、電子情報Ｅを読み出すための対応テーブルＴが情報格納装置５０に保存されるので、第２の実施形態の効果に加え、携帯型電子計算機の開発ツールなどを用いた電子情報の不正な操作を防ぐことができる。
【０１０８】
また、生体識別情報に基づく個人識別結果が正当のときに、情報格納装置５０の使用権限を取得させるので、より安全な電子情報管理を行なうことができる。
【０１０９】
また、本実施形態の変形例としては、情報格納装置５０は、全てのメモリが耐タンパー性である必要はなく、例えば耐タンパー性メモリが、少なくとも対応テーブルＴ（又は暗号化対応テーブル）の記憶に用いられ、好ましくは、対応テーブルＴの他に、生体識別情報及び／又はＰＩＮ情報の記憶に用いられればよい。この場合、耐タンパー性のない通常のメモリは、対応テーブルＴ等といった機密性の高い情報以外の（機密性の低い）情報の記憶に用いればよい。このような変形例により、コストの高い耐タンパー性メモリの記憶容量を必要最小限に抑制できるので、コストの低減を図ることができる。
【０１１０】
（第４の実施形態）
図１３は本発明の第４の実施形態に係る電子情報管理システムの構成を示す模式図である。
【０１１１】
本実施形態は、クライアント装置２側で対応テーブルＴを管理する第１の実施形態の変形例であり、記憶装置１及びクライアント装置２を小型化して内蔵した携帯型電子計算機４０ｙと、管理サーバ４を小型化して内蔵した演算機能付きの情報格納装置５０ｙとから構成されている。
【０１１２】
ここで、携帯型電子計算機４０ｙは、前述同様に、例えば携帯情報端末ＰＤＡ又は携帯電話などで実現可能となっており、好ましくは、内蔵した記憶装置１のうちの全記憶領域又は対応テーブルＴの記憶領域に耐タンパー性メモリが使用される。
【０１１３】
情報格納装置５０ｙは、前述同様に、耐タンパー性メモリを有するＩＣカードのような小型デバイスであり、生体識別及び／又はＰＩＮ等の個人識別機能を有している。また同様に、情報格納装置５０ｙは、好ましくは、内蔵した記憶装置（図示せず）のうちの全記憶領域又は対応テーブル取得情報Ｇの記憶領域に耐タンパー性メモリが使用される。
【０１１４】
以上のような構成としても、電子情報Ｅを読み出すための対応テーブルＴが携帯型電子計算機４０ｙに保存されるので、携帯型電子計算機４０ｙ及び情報格納装置５０ｙからなる

小型の電子情報管理システムであっても、第１の実施形態の効果を得ることができる。

【０１１５】

なお、上記各実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピー（登録商標）ディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、光磁気ディスク（ＭＯ）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【０１１６】

また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【０１１７】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【０１１８】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【０１１９】

また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【０１２０】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【０１２１】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１２２】

なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。

例えば、第１～第４の実施形態におけるクライアント装置２内の情報管理モジュール３０は、ボードとして実装してもよく、ソフトウェア上で実装してもよい。

【０１２３】

また、情報管理モジュール３０は、ＰＤＡ内のチップ又は回路として実装してもよく、カード状の情報管理モジュール３０をクライアント装置２のスロットに差し込む形態で実装してもよい。

【０１２４】

さらに、情報管理モジュール３０は、全体をソフトウェアとしてハードディスク上に実装してもよく、あるいは全体のうち、相互認証部３１を除く部分をソフトウェアとしてハードディスク上に実装し、相互認証部３１をソフトウェアとしてＯＳ２０上に実装してもよい。

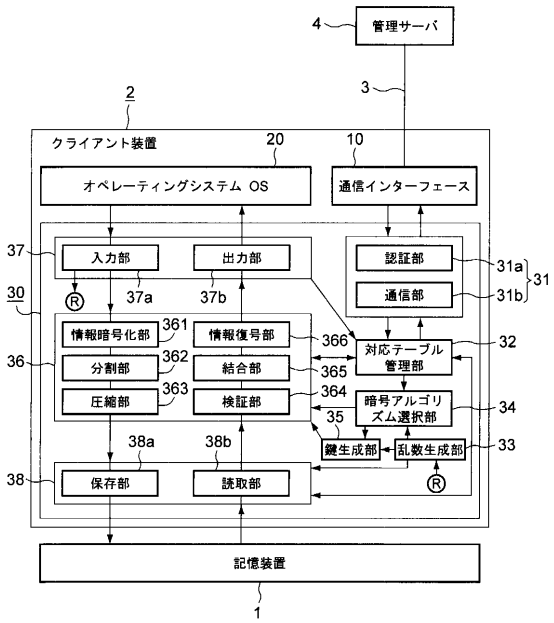
【０１２５】

また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成用件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

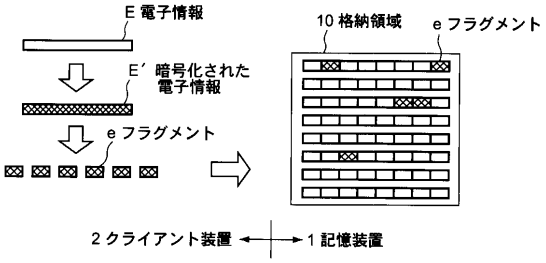
【０１２６】
その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。
【０１２７】
【発明の効果】
以上説明したように本発明によれば、記憶装置を解析されても、記憶内容の解読を阻止でき、安全性を向上できる。また、ユーザ毎に暗号化鍵を設定する場合でも、各ユーザ間での情報共有を容易化できる。
【図面の簡単な説明】
【図１】本発明の第１の実施形態に係る電子情報管理システムの構成を示す模式図
【図２】同実施形態における各電子情報の記憶形態を示す模式図
【図３】同実施形態における対応テーブルを示す模式図
【図４】同実施形態における対応テーブル取得情報の構成を示す模式図
【図５】同実施形態における動作を説明するためのシーケンス図
【図６】同実施形態における読出動作を説明するための模式図
【図７】同実施形態における読出動作を説明するためのフローチャート
【図８】同実施形態における書込動作を説明するための模式図
【図９】同実施形態における書込動作を説明するためのフローチャート
【図１０】本発明の第２の実施形態に係る電子情報管理システムの構成を示す模式図
【図１１】同実施形態における動作を説明するためのシーケンス図
【図１２】本発明の第３の実施形態に係る電子情報管理システムの構成を示す模式図
【図１３】本発明の第４の実施形態に係る電子情報管理システムの構成を示す模式図
【符号の説明】
１…記憶装置
２，２ｘ…クライアント装置
３…通信回線
４，４ｘ…管理サーバ
１０…通信インタフェース
２０…ＯＳ
３０…情報管理モジュール
３１…相互認証部
３１ａ…認証部
３１ｂ…通信部
３２，３２ｘ…対応テーブル管理部
３３…乱数生成部
３４…アルゴリズム選択部
３５…鍵生成部
３６…暗復号部
３６１…情報暗号化部
３６２…分割部
３６３…圧縮部
３６４…検証部
３６５…結合部
３６６…情報復号部
３７…入出力部
３７ａ…入力部
３７ｂ…出力部
３８…保存／読取部
３８ａ…保存部
３８ｂ…読取部
４０，４０ｙ…携帯型電子計算機

５０，５０ｙ…情報格納装置
Ｅ…電子情報
Ｅ’…暗号化電子情報
Ｔ…対応テーブル
Ｔ’，Ｔ”…暗号化対応テーブル
ｅ…フラグメント
Ｃ…共通情報
ｃ１…同定情報
ｃ２…暗号化アルゴリズム名
ｃ３…復号鍵，共通鍵
Ｍ…格納領域情報
ｍ１…結合順番
ｍ２…サイズ
ｍ３…物理位置情報
ｍ４…圧縮値
Ｇ…対応テーブル取得情報
ｇ１…対応テーブル名
ｇ２…秘密鍵
ｇ３…対応テーブル格納領域情報

【図１】



【図２】



【図３】

T

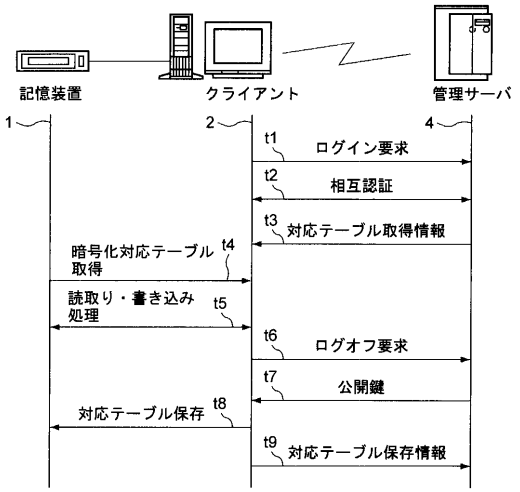
対応テーブル						
c1	c2	共通情報 C	c3	m1	m2	格納領域情報 M m3 m4
同定情報	暗号アルゴリズム名	復号鍵（共通鍵）		結合順番	サイズ	物理位置情報	圧縮値
File A	Algorithm A	xnsb094・・		1	1	aaa01	a4xdj・・
				・・・	・・・	・・・	・・・

【図４】

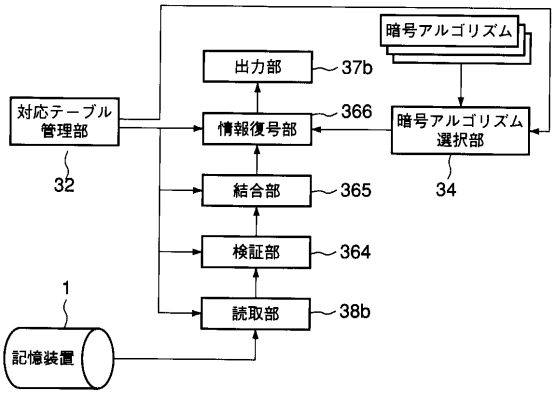
G

対応テーブル取得情報		
対応テーブル名	秘密鍵	対応テーブル格納領域情報
g1	g2	g3

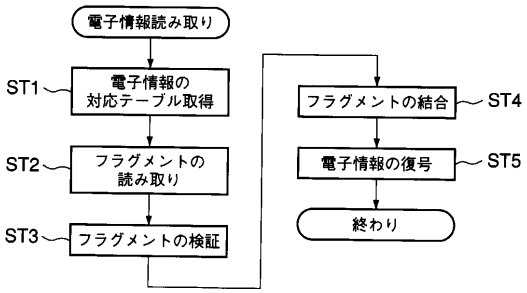
【図５】



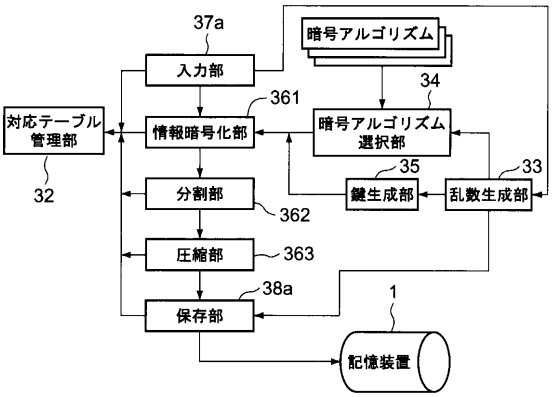
【図６】



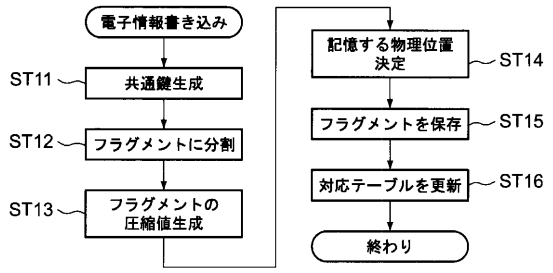
【図７】



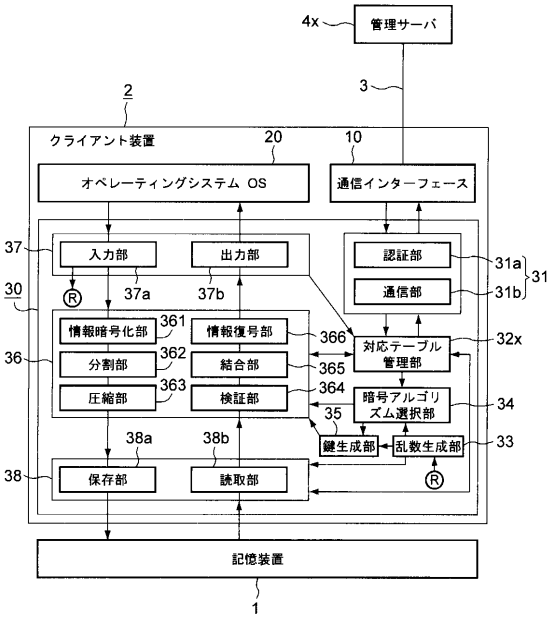
【図８】



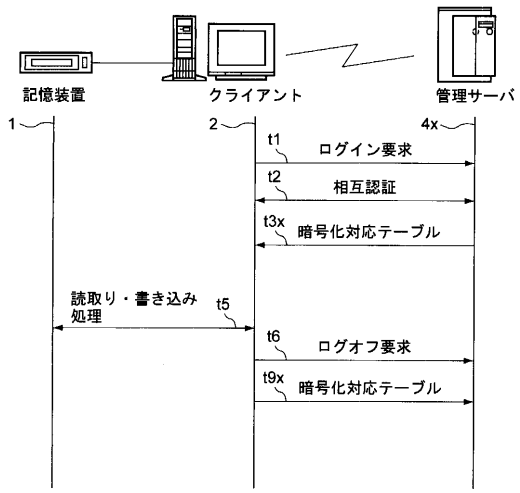
【図９】



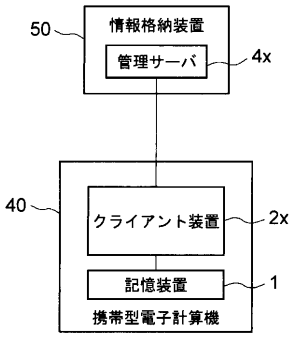
【図１０】



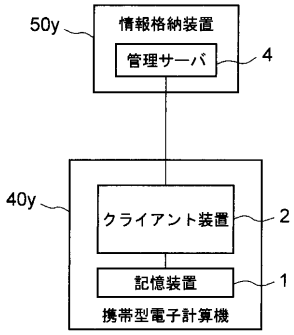
【図１１】


記憶装置
クライアント
管理サーバ
1
2
4x
t1
ログイン要求
t2
相互認証
t3x
暗号化対応テーブル
読取り・書き込み
処理
t5
t6
ログオフ要求
t9x
暗号化対応テーブル

【図１２】


50
情報格納装置
管理サーバ
4x
40
クライアント装置
2x
記憶装置
1
携帯型電子計算機

【図１３】


50y
情報格納装置
管理サーバ
4
40y
クライアント装置
2
記憶装置
1
携帯型電子計算機

フロントページの続き

(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 池田 竜朗
東京都府中市東芝町１番地 株式会社東芝府中事業所内
(72)発明者 森尻 智昭
東京都府中市東芝町１番地 株式会社東芝府中事業所内
(72)発明者 才所 敏明
東京都府中市東芝町１番地 株式会社東芝府中事業所内

審査官 速水 雄太

(56)参考文献 特開２００１－００５４９３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/14
G09C 1/00
H04L 9/08
H04L 9/32