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

特許第4266412号
(P4266412)

(45)発行日　平成21年5月20日(2009.5.20)　(24)登録日　平成21年2月27日(2009.2.27)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	12/14	560C
G09C 1/00	(2006.01)	G09C	1/00	640B
G11B 20/10	(2006.01)	G09C	1/00	660D
		G11B	20/10	H

請求項の数 5　(全 12 頁)

(21)出願番号　特願平10-304109
(22)出願日　平成10年10月26日(1998.10.26)
(65)公開番号　特開2000-132459(P2000-132459A)
(43)公開日　平成12年5月12日(2000.5.12)
審査請求日　平成17年6月15日(2005.6.15)

(73)特許権者　000000376
オリンパス株式会社
東京都渋谷区幡ヶ谷２丁目４３番２号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100084618
弁理士　村松　貞男
(74)代理人　100100952
弁理士　風間　鉄也
(74)代理人　100097559
弁理士　水野　浩司
(72)発明者　近藤　隆
東京都渋谷区幡ヶ谷２丁目４３番２号　オリンパス光学工業株式会社内

最終頁に続く

(54)【発明の名称】データ保存システム

(57)【特許請求の範囲】

【請求項１】

ファイル管理機能を用いて保存媒体に対してデータの保存、削除等を行なうデータ保存装置を備えたデータ保存システムであって、

前記データ保存装置に固有の秘密情報を格納する格納手段と、

前記格納手段に格納された秘密情報と、保存すべきデータとを用いて所定の暗号化処理を行うことにより前記保存すべきデータの改竄防止用データである第１の電子署名データを生成する生成手段と、

前記保存すべきデータと前記第１の電子署名データとを対応させて前記保存媒体に記録する第１の記録手段と、

前記保存媒体に予め記録されている媒体管理用データファイルに、前記第１の電子署名データを、前記保存すべきデータのファイルを識別する情報と対応させて記録する第２の記録手段と、

前記格納手段に格納されている秘密情報と、前記媒体管理用データファイルを用いて所定の暗号化処理を行うことにより、前記媒体管理用データファイルの改竄防止用データである第２の電子署名データを作成し、該第２の電子署名データと前記媒体管理用データファイルとを対応させて、前記保存媒体に記録する第３の記録手段と、

を具備するデータ保存システムにおいて、

前記保存媒体に記録されている媒体管理用データファイルからメッセージダイジェストを抽出し、前記媒体管理用データファイルの前記第２の電子署名データを、前記格納手段

に格納された復号鍵を用いて第２のコードに変換し、前記メッセージダイジェストと前記第２のコードとを比較することによって、前記媒体管理用データファイルが改竄されているか否かを検知する第１の検知手段と、

前記媒体管理用データファイルに登録されているファイルを全て、前記保存媒体上に存在しているか否かを確認する確認手段と、

前記媒体管理用データファイルのレコードに登録されているデータファイルの前記第１の電子署名データと、保存媒体上に前記データファイルと対応させて記録されている前記データファイルの前記第１の電子署名データとが一致するかどうかを検知する第２の検知手段と、

前記保存媒体に保存された前記保存すべきデータからメッセージダイジェストを抽出し、対応する前記第１の電子署名データを、前記格納手段に格納されている復号鍵を用いて第１のコードに変換し、前記メッセージダイジェストと前記第１のコードとを比較することによって、前記保存すべきデータが改竄されているか否かを検知する第３の検知手段と、

を具備することを特徴とするデータ保存システム。

【請求項２】

前記保存すべきデータは、通信回線を介して外部装置から送られてきたデータか、あるいは、前記データ保存装置のデータ入力機能を用いて入力されたデータであることを特徴とする請求項１に記載のデータ保存システム。

【請求項３】

前記保存媒体を初期化するとき、あるいは初めてファイルを記録するときに、前記媒体管理用データファイルを前記保存媒体に記録する手段を有することを特徴とする請求項１または２記載のデータ保存システム。

【請求項４】

前記ファイル管理機能は、前記保存媒体上のデータファイルを削除するときに、前記媒体管理用データファイルから消去するデータファイルのレコードも削除する機能を持つことを特徴とする請求項１または２記載のデータ保存システム。

【請求項５】

前記保存媒体は、前記データ保存装置に着脱自在な可搬型保存媒体か、あるいは、前記データ保存装置内に配置された固定型保存媒体であることを特徴とする請求項１から４のいずれか１つに記載のデータ保存システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はデータ保存システムに関するものである。

【０００２】

【従来の技術】

例えば光磁気ディスクやＣＤ－Ｒ，ＤＶＤ，ＤＡＴ等の可搬型保存媒体に、テキストファイルや画像ファイル等のデジタルデータを保存した場合には、悪意あるユーザが、当該デジタルデータを全く形跡を残すことなく改竄したり、不正に他のファイルと差し替えたり、不正に消去することが可能である。

【０００３】

データの改竄検知に関しては、保存するデータファイルに電子署名を付ける方法が一般的である（例えば、特開平７－２２１７５１号公報や特開平７－１３１４４９号公報等）。電子署名法は暗号技術を用いた方法であり、基本的にはデータに公知の処理を施してあるコードを抽出し、そのコードを本人しか知らない暗号鍵を用いて暗号化したものを改竄防止用のコード（電子署名）として、オリジナルのデータファイルに対応させて保存することからなる。改竄の有無を検知するには、まず、検知するデータに上記の公知の処理を施してコード１を抽出する。また、電子署名データを復号用の鍵を用いて復号してコード２を取り出す。その後、コード１とコード２を比較することで、両者が一致した場合には改

竄がなかった、一致しない場合は改竄があったことがわかる。

【０００４】

電子署名を用いる通常の方法では、データファイル作成者以外の第３者がデータ内容を改竄するとそれを検知することができる。しかし、この方法では、データファイル作成者はいつでもデータから電子署名を作成できるため、本物の書類作成後、何時でもデータファイルを作成しなおし、自分しか知らない暗号鍵を用いて、そのデータファイルがあたかも本物であるかのように、電子署名を付与することが可能である。例えば、３年前に作成した公文書（デジタルデータ）の内容を、時間を３年遅らせたＰＣを用いて改竄し、自分しか知らない暗号鍵を用いて電子署名を付与することで、あたかも３年前に作成した公文書で内容は３年前から改竄されていないように見せかけることができてしまう。問題となるのは、改竄防止用のコードである電子署名を作成する手段（暗号鍵）を、ユーザが自由に使用できるという点である。

【０００５】

上記のような問題を克服するためには、データファイルの改竄防止用コード作成のための暗号鍵を、ユーザではなく、ハードウェア及びソフトウェア的に安全性が確保されたデータ保存装置が管理し、改竄防止コードはユーザが自由に作成できないようにすることで実現できる。

【０００６】

【発明が解決しようとする課題】

しかし、上記の方法を用いた場合でも、可搬型保存媒体からデータファイルを消去するという改竄は検知することができない。また、ユーザが上記のデータ保存装置を用いて不正に作成したデータファイルと本物のデータファイルを差し替えるという改竄も検知することができない。つまり、データ作成時に予め本物のデータファイルと偽りの内容を記録している偽物のデータファイルとを上記データ保存装置で作成し、それぞれ別の可搬型保存媒体１，２上に同名のファイルで格納する（この場合、第３者は、偽物を格納した可搬型保存媒体の存在を知らない）。どちらも、データ保存装置の電子署名を持っており、データファイルとしては改竄されていないことが示される。その後、汎用のＰＣなどを用いて、可搬型保存媒体２上の偽物のデータファイルを、可搬型保存媒体１上の本物のデータファイルに上書きすることで、データファイルを不正の痕跡を残さずに差し替えることができてしまう。

【０００７】

本発明は、このような課題に着目してなされたものであり、その目的とするところは、汎用の保存媒体上に格納するデータファイルに対して、上述したような消去や差し替えを含む改竄がなされたことを検知できるデータ保存システムを提供することを目的とする。

【０００８】

【課題を解決するための手段】

上記の目的を達成するために、本発明の第１の態様に係るデータ保存システムは、ファイル管理機能を用いて保存媒体に対してデータの保存、削除等を行なうデータ保存装置を備えたデータ保存システムであって、前記データ保存装置に固有の秘密情報を格納する格納手段と、前記格納手段に格納された秘密情報と、保存すべきデータとを用いて所定の暗号化処理を行うことにより前記保存すべきデータの改竄防止用データである第１の電子署名データを生成する生成手段と、前記保存すべきデータと前記第１の電子署名データとを対応させて前記保存媒体に記録する第１の記録手段と、前記保存媒体に予め記録されている媒体管理用データファイルに、前記第１の電子署名データを、前記保存すべきデータのファイルを識別する情報と対応させて記録する第２の記録手段と、前記格納手段に格納されている秘密情報と、前記媒体管理用データファイルを用いて所定の暗号化処理を行うことにより、前記媒体管理用データファイルの改竄防止用データである第２の電子署名データを作成し、該第２の電子署名データと前記媒体管理用データファイルとを対応させて、前記保存媒体に記録する第３の記録手段と、を具備するデータ保存システムにおいて、前記保存媒体に記録されている媒体管理用データファイルからメッセージダイジェストを抽

出し、前記媒体管理用データファイルの前記第２の電子署名データを、前記格納手段に格納された復号鍵を用いて第２のコードに変換し、前記メッセージダイジェストと前記第２のコードとを比較することによって、前記媒体管理用データファイルが改竄されているか否かを検知する第１の検知手段と、前記媒体管理用データファイルに登録されているファイルを全て、前記保存媒体上に存在しているか否かを確認する確認手段と、前記媒体管理用データファイルのレコードに登録されているデータファイルの前記第１の電子署名データと、保存媒体上に前記データファイルと対応させて記録されている前記データファイルの前記第１の電子署名データとが一致するかどうかを検知する第２の検知手段と、前記保存媒体に保存された前記保存すべきデータからメッセージダイジェストを抽出し、対応する前記第１の電子署名データを、前記格納手段に格納されている復号鍵を用いて第１のコードに変換し、前記メッセージダイジェストと前記第１のコードとを比較することによって、前記保存すべきデータが改竄されているか否かを検知する第３の検知手段と、を具備する。

【０００９】

また、本発明の第２の態様に係るデータ保存システムは、第１の態様に係るデータ保存システムにおいて、前記保存すべきデータは、通信回線を介して外部装置から送られてきたデータか、あるいは、前記データ保存装置のデータ入力機能を用いて入力されたデータである。

【００１０】

また、本発明の第３の態様に係る発明は、第２の態様に係る発明において、前記保存媒体を初期化するとき、あるいは初めてファイルを記録するときに、前記媒体管理用データファイルを前記保存媒体に記録する手段を有する。

【００１１】

また、本発明の第４の態様に係るデータ保存システムは、第１または第２の態様に係るデータ保存システムにおいて、前記ファイル管理機能は、前記保存媒体上のデータファイルを削除するときに、前記媒体管理用データファイルから消去するデータファイルのレコードも削除する機能を持つ。

【００１２】

また、本発明の第５の態様に係るデータ保存システムは、第１から第４のいずれか１つの態様に係るデータ保存システムにおいて、前記保存媒体は、前記データ保存装置に着脱自在な可搬型保存媒体か、あるいは、前記データ保存装置内に配置された固定型保存媒体である。

【００１５】

【発明の実施の形態】

まず、図１及び図２を参照して本発明の実施形態の概略を説明する。本実施形態のデータ保存システムを用いて保存媒体にデータを記録するときには、まず、図１に示すように、データ保存装置内の秘密情報を用いてデータファイルから改竄防止用データ（ここでは電子署名）を作成し（ステップＳ１）、この作成した電子署名を当該データファイルと対応付けて可搬型保存媒体に記録する（ステップＳ２）。

【００１６】

次に、記録したデータファイルの改竄防止用データ（電子署名）をデータファイルの識別情報と共にレコードとして、可搬型保存媒体上の保存媒体管理用の管理ファイル（以下、媒体管理用データファイルと呼ぶ）に記録する（ステップＳ３）。

【００１７】

次に、上記媒体管理用データファイルに対しても改竄防止用データ（電子署名）を作成して（ステップＳ４）、可搬型保存媒体上に記録する（ステップＳ５）。

【００１８】

次に上記のようにして記録されたデータが不正な第３者によって改竄されたかどうかを検証する方法を図２を参照して説明する。改竄検証の要求があったときには、まず媒体管理用データファイルの改竄を検証する（ステップＳ１０）。次に登録されている全てのデー

タファイルの存在を確認し（ステップＳ１１）、媒体管理用データファイルのレコード中の改竄防止用データと、対応するデータファイルの改竄防止用データ（電子署名）とを比較する（ステップＳ１２）。このようにして全てのデータファイルに対して改竄を検証する（ステップＳ１３）。

【００１９】

すなわち、媒体管理用データファイルは、可搬型保存媒体に必ず１つずつ存在するはずなので、当該ファイルが存在しない場合には、可搬型保存媒体に対して不正な処理がなされたことを検知できる。また、媒体管理用データファイルの改竄防止用データ（電子署名）から、媒体管理用データが改竄されたことが検知された場合にも、可搬型保存媒体に何らかの不正な処理がなされたことを検知することができる。

【００２０】

また、媒体管理用データファイル中のレコードに記録されている改竄防止用データと対応するデータファイルの改竄防止用データが異なる場合には、不正な差し替えが行われたことが検知できる。

【００２１】

また、媒体管理用データファイル中のレコードに存在するファイルが、可搬型保存媒体上に存在しない場合には、不正な消去が行われたことが検知できる。

また、データファイルと、このデータファイルの改竄防止用データを用いることで、通常の電子署名と同様の方法で、データファイルが改竄されているかどうかを調べることができる。この処理は、保存媒体上のすべてのデータファイルに対して行なう。

【００２２】

以下に、上記した概略を後述する第１～第３実施形態によりさらに詳細に説明する。ここでは改竄防止用データとして電子署名を用いた場合について説明するが、データの改竄を検知できるコードであるならば電子署名以外のコードであってもよいことは勿論である。

【００２３】

図３は本発明の第１実施形態に係るデータ保存システムの構成を示す図であり、データ保存装置３０と、このデータ保存装置３０に着脱自在な可搬型保存媒体２とからなり、保存すべきデータは通信回線３を介してホストコンピュータ１から供給される。データ保存装置３０としては、ハードウェア的にはコンピュータの本体部分だけを使い、本体外壁を強固にパッケージ化したような構成を用いる。また、可搬型保存媒体２としては、光ディスクや可搬型ハードディスク、ＤＡＴ，ＰＣＭＣＩＡカード型メモリ、コンパクトフラッシュメモリなどの汎用の記録媒体を用いる。同様に、記録媒体を駆動する装置としても汎用の媒体駆動装置が用いられる。

【００２４】

図３に示すように、データ保存装置３０は、通信回線３に接続可能な通信ポート１１と、コマンド処理部１２と、ＣＰＵ２１と、ＣＰＵ作業用メモリ２２と、プログラム格納用ＲＯＭ２３と、暗号鍵格納用メモリ２４と、ファイル管理部２５と、暗号・復号処理部２６と、可搬型保存媒体２を駆動可能な可搬型保存媒体駆動装置２７とを備えている。

【００２５】

また、本実施形態では、ユーザは他のパソコン等の情報機器（図１ではホストコンピュータ１）から通信回路３を通してしか、データ保存装置３０及び可搬型保存媒体２内のデータにアクセスできないようになっている。つまり、ユーザがデータ保存装置３０にデータを保存するためには、ホストコンピュータ１から、コマンド、データ及び必要な各種属性値を通信回線３を通してデータ保存装置３０へ送る。データ保存装置３０側では、受け取ったコマンドが正当な処理要求である場合にのみ保存の処理を行う。このような、従来のデータ保存システムとしては、原本性保証電子保存システム（“原本性保証電子保存システムの開発－システムの構築”、ＭＥＤＩＣＡＬ　ＩＭＡＧＩＮＧ　ＴＥＣＨＮＯＬＯＧＹ，Ｖｏｌ．１６　ＮＯ．４，ｐ４０１－４０２，Ｊｕｌｙ　１９９８）がある。

【００２６】

まず、可搬型保存媒体２を初期化する方法を説明する。ここで説明する初期化の方法は後

述する第２、第３実施形態に対しても同様に適用することができる。
まず、ファイル管理部２５の機能を用いて、可搬型保存媒体２にファイルが含まれているかどうかを調べる。ファイルが可搬型保存媒体２中に存在する場合には、初期化の処理は行わない。可搬型保存媒体２上にファイルが存在しない場合には、以下の手順で可搬型保存媒体２を初期化する。
【００２７】
可搬型保存媒体２に対して必要に応じて論理フォーマットを施す。その後、可搬型保存媒体２上に媒体管理用データファイルを生成する。初期化時には媒体管理用データファイルに、データを初期化した時間や初期化したユーザに関する情報などを書き込む。次に、暗号鍵格納用メモリ２４から電子署名作成用の暗号鍵データを読み出し、媒体管理用データファイルのデータと読み出した暗号鍵データから暗号・復号処理部２６の機能を用いて改竄防止用データとしてデータ保存装置３０の電子署名のデータを求めて、媒体管理用データファイルと対応づけて可搬型保存媒体２上に保存する。
【００２８】
次に、第１実施形態におけるデータ保存方法を説明する。データを保存するときには、ホストコンピュータ１から通信回線３を通してデータを保存するためのコマンド、データ及び必要な各種属性値を受け取る。ここで、各種属性とは、ファイル名、ユーザのアカウント名、ファイルサイズ、ファイル生成時刻等のファイル属性値などがある。次に、暗号鍵格納用メモリ２４から電子署名作成用の暗号鍵データを読み出し、前記暗号鍵データと上記データから暗号・復号処理部２６の機能を用いて改竄防止用データとしてデータ保存装置３０の電子署名を求めて、データファイルと対応付けて保存する。
【００２９】
図４は可搬型保存媒体２に、保存するデータ１のファイル１０１と、データ１の電子署名１０２を対応付けて記録した状態を示している。その他のデータがある場合にはデータ２、データ３、…が電子署名２、３、…とそれぞれ対応付けて記録される。
【００３０】
次に、データ保存装置３０の電子署名のデータを、保存すべきデータファイルのファイル名などのファイル識別子とともに、媒体管理用データファイル１０３中にレコードとして保存する。
【００３１】
図４は可搬型保存媒体２の媒体管理用データファイル１０３に、識別子１と電子署名１とを対応付けてデータファイル１のレコード１０５として記録した状態を示している。データ２、３、…がある場合には識別子２、３、…と電子署名２、３、…とが対応付けて記録される。
【００３２】
その後、この媒体管理用データファイル１０３が改竄されないように、前記暗号鍵データを用いて媒体管理用データファイル１０３から、暗号・復号処理部２６の機能を用いて媒体管理用データファイル１０３に対する改竄防止用コードであるデータ保存装置３０の電子署名１０４を求め、媒体管理用データファイル１０３と対応させて可搬型保存媒体２上に保存する。なお、図中には示していないが媒体管理用データファイル１０３内には、前述した保存媒体初期化時の初期化データも記録されている。図４は可搬型保存媒体２上に媒体管理用データファイル１０３の電子署名１０４を記録した状態を示している。
【００３３】
図５は本発明の第２実施形態に係るデータ保存システムの構成を示す図であり、データ保存装置として、デジタルカメラのような画像入力装置を用いた場合の例である。図中、図３と同じ番号のモジュールは図３と同じ機能を果たすことを意味する。
【００３４】
データは、画像撮像部３０にて図示していないレンズ系、ＣＣＤ素子、Ａ／Ｄ変換器、ファイルフォーマット作成部等を経て、画像データとしてＣＰＵ作業用メモリ２２に蓄積される。その後、ユーザがデジタルカメラ４０のユーザインタフェース２９を通して、上記

画像データを保存するという指示をデジタルカメラ４０に送ると、暗号鍵格納用メモリ２４から電子著名作成用の暗号鍵データを読み出し、暗号鍵と上記データから暗号・復号処理部２６の機能を用いて改竄防止用データとして電子署名を求めて、図４に示すようにデータファイル１０１と対応付けて保存する。

【００３５】

さらに、この時に電子署名のデータを、保存するデータファイルのファイル名などのファイル識別子とともに媒体管理用データファイル１０３中にレコード１０５として保存する。その後、この媒体管理用データファイル１０３が改竄されないように、前記暗号鍵データと媒体管理用データファイル１０３から、暗号・復号処理部２６の機能を用いて媒体管理用データファイル１０３の電子署名を求め、媒体管理用データファイル１０３と対応させて可搬型保存媒体２上に保存する。

【００３６】

図６は本発明の第３実施形態に係るデータ保存システムの構成を示す図であり、データ保存装置としてデジタル録音機のような音声入力装置を用いた場合の例である。図中、図３と同じ番号のモジュールは図３と同じ機能を果たすことを意味する。

【００３７】

データは、音声入力部５０にて図示していないマイク、Ａ／Ｄ変換器、ファイルフォーマット作成部等を経て、音声データとしてＣＰＵ作業用メモリ２２に蓄積される。その後、ユーザがデジタル録音機６０のユーザインタフェース２９を通して、上記音声データを保存するというコマンドを入力すると、暗号鍵格納用メモリ２４から電子署名作成用の暗号鍵データを読み出し、暗号鍵と上記データから暗号・復号処理部２６の機能を用いて改竄防止用データとして電子署名を求めて、図４に示すようにデータファイル１０１と対応付けて保存する。

【００３８】

さらに、この時に電子署名のデータを媒体管理用データファイル１０３中に、保存するデータファイルのファイル名などのファイル識別子とともにレコード１０５として保存する。その後、この媒体管理用データファイル１０３自体が改竄されないように、前記暗号鍵データと媒体管理用データファイル１０３のデータから、暗号・復号処理部２６の機能を用いて媒体管理用データファイル１０３の電子署名１０４を求め、媒体管理用データファイル１０３と対応させて可搬型保存媒体２上に保存する。

【００３９】

次に、本実施形態のデータ保存システムを用いて可搬型保存媒体２からデータファイルを正規の手続きで消去する方法について説明する。

第１実施形態の場合は、ホストコンピュータ１から送られてきたデータファイルを消去するコマンドに応じて、可搬型保存媒体２上の指定されたファイルを消去する。第２、第３実施形態の場合には、ユーザインタフェース２９を用いてユーザが入力したデータファイル消去要求に応じて、可搬型保存媒体２上の指定されたファイルを消去する。

【００４０】

データファイルを可搬型保存媒体２から消去する場合には、同時に媒体管理用データファイル１０３上の消去するデータファイルのレコードも削除する。その後、暗号鍵格納用メモリ２４から電子署名作成用の暗号鍵データを読み出し、媒体管理用データファイル１０３と暗号鍵データから暗号・復号処理部２６の機能を用いて改竄防止用データとしてデータ保存装置の電子署名１０４のデータを作成しなおし、媒体管理用データファイル１０３と対応づけて可搬型保存媒体２上に上書きにより保存する。

【００４１】

なお、レコードの削除は、媒体管理用データファイル１０３から実際に削除しても良いし、また、各レコードの先頭などに削除されたかどうかを示すフラグを設け、例えばそのレコードが存在するなら対応するフラグを１に、削除されたなら０にすることで、媒体管理用データファイル１０３からレコードを削除したことにしてもよい（後者を仮削除と呼ぶ）。なお、仮削除をする場合には、媒体管理用データファイル１０３に対応する電子署名

１０４を作成する際にフラグの情報も含める。

【００４２】

次に、本実施形態のデータ保存システムを用いて可搬型保存媒体２からデータファイルの識別子を正規の手続きで変更する手法について説明する。ファイル名の変更、ディレクトリの変更等、ファイル識別子を変更する場合には、同時に媒体管理用データファイル１０３上の対応するレコードのファイル識別子をも変更する。その後、暗号鍵格納用メモリ２４から電子署名作成用の暗号鍵データを読み出し、媒体管理用データファイル１０３と暗号鍵データから暗号・復号処理部２６の機能を用いて改竄防止用データとしてデータ保存装置３０の電子署名のデータを作成しなおし、媒体管理用データファイル１０３と対応づけて可搬型保存媒体２上に上書きにより保存する。

【００４３】

次に、第１実施形態の方法を用いて本実施形態のデータ保存システムの不正な消去を含むデータの改竄検知の方法を説明する。改竄検知の方法は、基本的に第２、第３実施形態においても同様である。第１実施形態の場合と異なる処理を行う必要のある部分については個々に説明する。

【００４４】

まず、可搬型保存媒体２上のデータファイルの改竄を検知するために、各々のデータファイル（媒体管理用データファイルを含む）のデータ及び、対応する電子署名と暗号鍵格納用メモリ２４から読み出した改竄検知用データとしての復号用の鍵から、暗号・復号処理部２６の機能を用いて個々のファイルの改竄検知を行う。改竄の有無を検知するには、まず、検知するデータに所定の処理を施してメッセージ・ダイジェストと呼ばれるコード（コード１と呼ぶ）を抽出する。また、データファイルの電子署名データを、暗号鍵格納用メモリ２４から読み出した復号用の鍵を用いて復号してコード（コード２と呼ぶ）を取り出す。

【００４５】

その後、前記所定の処理を施して得られたコード１と前記電子署名を復号化して得たコード２とを比較し、両者が一致している場合には改竄されていない、一致していない場合にはデータファイルが改竄されていると判断することで改竄検知の処理を行う。改竄されている場合には、第１実施形態の場合には通信回路３を介してホストコンピュータ１側に、第２、第３実施形態の場合にはユーザインタフェース２９を介してユーザに改竄があったことを通知する。

【００４６】

また、可搬型保存媒体２上のデータファイルの不正な消去を検知するには、ファイル管理部２５の機能を用いて媒体管理用データファイル１０３にレコードとして登録されているファイルが、すべて可搬型保存媒体２上に存在するかどうかを調べる。もし、ファイルが一つでも存在しない場合には、データファイルが不正に消去させていることになる。不正な消去があった場合には、第１実施形態の場合には通信回路３を介してホストコンピュータ１側に、第２、第３実施形態の場合にはユーザインタフェース２９を介してユーザに不正にデータが消去されたことを通知する。

【００４７】

また、可搬型保存媒体２上のデータファイルの不正な差し替えを検知するには、ファイル管理部２５の機能を用いて、保存されている全てのデータファイルの電子署名と媒体管理用データファイル１０３の対応するレコードに記録されている電子署名とを照合する。一致しないデータファイルがある場合には、そのファイルは不正に差し替えられたことになる。不正な差し替えがあった場合には、第１実施形態の場合には通信回線３を介してホストコンピュータ１側に、第２、第３実施形態の場合にはユーザインタフェース２９を介してユーザに不正にデータが消去されたことを通知する。

【００４８】

また、上記の処理を行っているときに、媒体管理用データファイル１０３にレコードが登録されていないファイルが可搬型保存媒体２上に存在した場合には、本実施形態のデータ

保存システム以外のシステムを用いてデータファイルが保存されたことになり、この場合にも不正があったとして、第１実施形態の場合には通信回線３を介してホストコンピュータ１側に、第２、第３実施形態の場合にはユーザインタフェース２９を介してユーザに不正にデータが保存されていることを通知する。

【００４９】

さらに、改竄防止用データ作成及び改竄検知の手段として、公開鍵暗号方式のように、改竄防止用データ作成時と改竄検知時で用いる情報（鍵）が異なるものを用いた場合、改竄防止用データ作成のための情報だけをデータ保存装置内に安全に格納すればよいので、改竄検知用の情報を公開することでデータ保存装置以外の汎用の装置でも改竄検知の処理を行うことができる。

【００５０】

なお、上記実施形態中では媒体管理データのレコード中には、データファイルの識別子とデータファイルの電子署名を記録するとしか記述しなかったが、ファイルに関する他の情報等をレコードの属性中に定義しても構わない。例えば、媒体管理データ中のレコードを検索で使えるようにするためにレコード中に、キーワードを含めるといった構成も考えられる。

【００５１】

また、媒体管理用データファイルとして、可搬型保存媒体２上の全てのファイルをまとめて１つのファイルとしたものを用いても、（このファイルを媒体管理用データファイル'と呼ぶ）、改竄検知に関しては同様の効果は得られる。しかし、この場合には媒体管理用データファイル'のサイズが非常に大きくなり、電子署名１０４を作成するために処理時間が非常に長くかかってしまう。しかも、電子署名１０４は可搬型保存媒体上のどのファイルを更新しても、必ず更新される必要があるため非常に効率の悪いデータ保存システムになってしまう。

【００５２】

一方、本実施形態で提案した手法では媒体管理用データファイルに記録されるデータは、前記媒体管理用データファイル'に比べ非常に小さくなる。媒体管理用データファイルのレコードのサイズは、ファイルの識別子とファイルに対応した電子署名のサイズの合計なのでせいぜい数百バイトであり、一方、通常のファイルのサイズは、数十キロ～数メガバイトである。したがって、媒体管理用データファイルは媒体管理用データファイル'に比べて１／１００～１／１００００程度小さくなる。そのため、提案した手法を用いることで電子署名１０４を更新するための処理時間は短くなる。

【００５３】

以上、上記した実施形態を要約すると以下のようになる。すなわち、データ保存システムを用いてデータファイルを保存するときには、データファイルの改竄防止用データ（電子署名）を作成して、データファイルと対応付けて可搬型保存媒体２上に保存するとともに、媒体管理用データファイル１０３にデータファイルの識別子と前記改竄防止用データをレコードとして記録し、さらに、媒体管理用データファイル１０３の改竄防止用データを作成して、可搬型保存媒体２上に保存する。

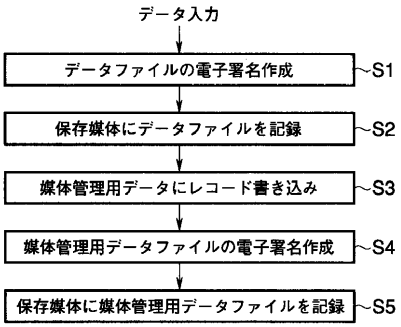
【００５４】

また、データ保存システムを用いて改竄を検知するときには、前記媒体管理用データファイル１０３と媒体管理用データファイル１０３の改竄防止用データ１０４を用いて改竄の有無を検証する。さらに、媒体管理用データファイル１０３のレコードに登録されているデータファイルが全て可搬型保存媒体２上に存在するかどうかを確認し、不正な消去が行われなかったか確認する。また、データファイルの改竄防止用データと、媒体管理用データファイル１０３のレコードに記録されているデータファイルの改竄防止用データを照合し、一致しているかどうかを調べることで、データファイルの不正な差し替えがなかったか否かを確認する。その後、可搬型保存媒体２上の各データファイルと対応する改竄防止用データを用いてデータファイルの改竄の有無を検証する。

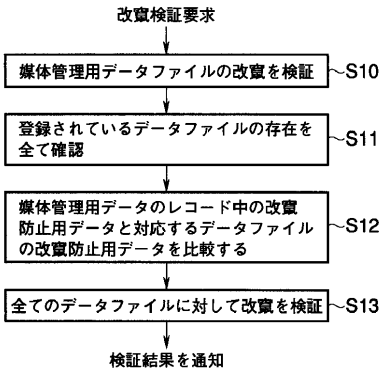
【００５５】

以上の処理において、不正を検知した場合には通信回線３、もしくはインタフェース２９を用いてユーザに不正があったことを通知する。
上記した実施形態によれば、データ保存装置以外には、可搬型保存媒体２にデータを保存するときに作成する改竄防止用データを作成できないようにすることが可能となる。また、可搬型保存媒体２に保存される全てのファイルの改竄防止用データは、可搬型保存媒体２上の媒体管理用データファイル１０３に登録され、媒体管理用データファイル１０３自体にも改竄防止用データが付けられる。以上の処理を行うことで、データファイルの不正消去、不正コピーを含む可搬型保存媒体２上のファイルの改竄を防止することが可能となる。
【００５６】
つまり、データファイルの改竄防止用データを調べることで、データファイルが本実施形態の保存システム以外のシステムを用いて不正に改竄されたかどうかを検知できる。また、媒体管理用データファイル１０３に登録されている改竄防止用データと、対応するデータファイルの改竄防止用データを比較することで、本実施形態の保存システム以外のシステムを用いて不正にデータファイルが消去、あるいはコピーされたかどうかを検知できる。このようにして、汎用の可搬型保存媒体を用いても、データファイルの不正な消去、コピーを含む改竄を防止できる。
【００５７】
なお、上記した実施形態ではデータ保存装置に着脱自在な可搬型保存媒体を用いたが、データ保存装置内に配置された固定型保存媒体を用いるようにしてもよい。
【図面の簡単な説明】
【図１】本発明の実施形態に係るデータ保存方法を説明するためのフローチャートである。
【図２】記録されたデータが不正な第３者によって改竄されたかどうかを検証する方法を説明するためのフローチャートである。
【図３】本発明の第１実施形態に係るデータ保存システムの構成を示す図である。
【図４】可搬型保存媒体に本実施形態の方法によりデータファイルを保存した状態を示す図である。
【図５】本発明の第２実施形態に係るデータ保存システムの構成を示す図である。
【図６】本発明の第３実施形態に係るデータ保存システムの構成を示す図である。
【符号の説明】
１…ホストコンピュータ、
２…可搬型保存媒体、
３…通信回線、
１１…通信ポート、
１２…コマンド処理部、
２１…ＣＰＵ、
２２…ＣＰＵ作業用メモリ、
２３…プログラム格納用ＲＯＭ、
２４…暗号鍵格納用メモリ、
２５…ファイル管理部、
２６…暗号・復号処理部、
２７…可搬型保存媒体駆動装置、
２８…ハードディスク、
１０１…保存するデータ１のファイル、
１０２…データ１の電子署名、
１０３…媒体管理用データファイル、
１０４…媒体管理用データファイルの電子署名、
１０５…データファイル１のレコード。

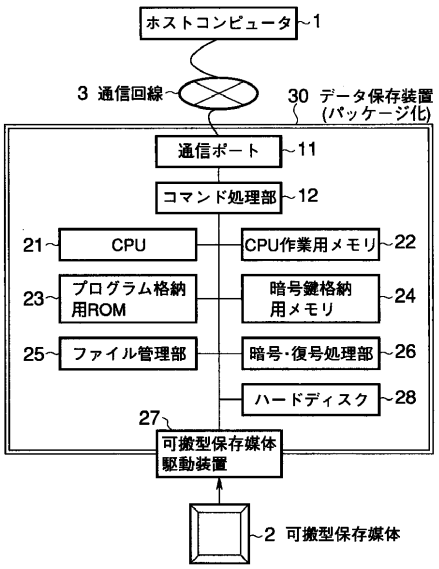
【図１】



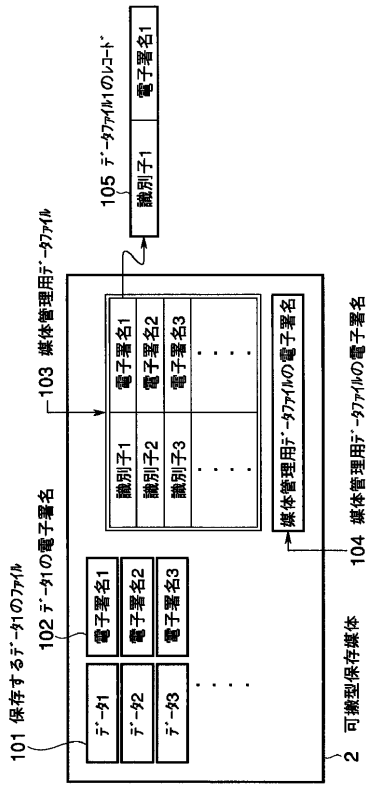
【図２】



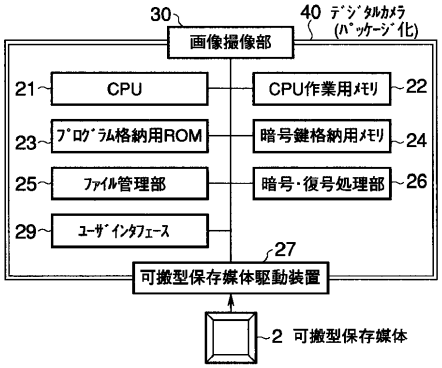
【図３】



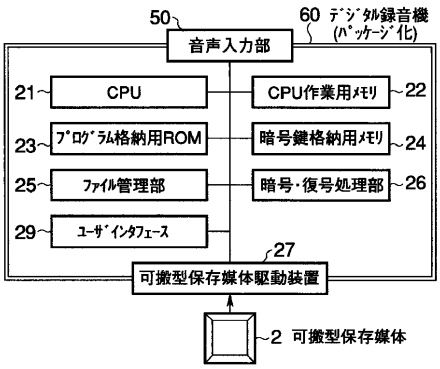
【図４】



【図５】



【図６】



フロントページの続き

審査官　平井　誠

(56)参考文献　特開平１０－２８３２６３（ＪＰ，Ａ）
欧州特許出願公開第００８４５７３３（ＥＰ，Ａ１）
特開平１０－３２６０７８（ＪＰ，Ａ）
特開平１０－２８３２６４（ＪＰ，Ａ）
特開平１０－０４０１００（ＪＰ，Ａ）
特開平０１－１６３８７１（ＪＰ，Ａ）
特開平０８－０８３０４６（ＪＰ，Ａ）
金井洋一，原本性保証電子保存システムについて，行政＆ＡＤＰ，社団法人行政情報システム研究所，１９９８年，１９９８年８月号，p.10-p.17

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/24