(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2005-151358
(P2005-151358A)
(43)公開日　平成17年6月9日(2005.6.9)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/32	H04L 9/00	675Z	5B017
G06F 12/14	G06F 12/14	310Z	5J104

審査請求 未請求　請求項の数 8　ＯＬ　（全 20 頁）

(21)出願番号　特願2003-388414 (P2003-388414)
(22)出願日　平成15年11月18日 (2003.11.18)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100081880
弁理士　渡部　敏彦
(72)発明者　阿武　純
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

Ｆターム(参考)　5B017 AA02　CA16
5J104 AA11　MA01

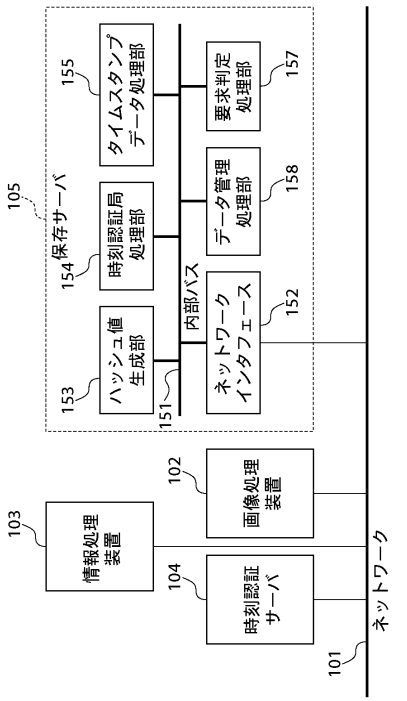
(54)【発明の名称】データ保存装置およびデータ保存方法

(57)【要約】

【課題】　保存されているデータの時刻認証を簡単に行うことができるデータ保存装置を提供する。

【解決手段】　保存サーバ１０５は、保存されているデジタルデータを、ネットワーク１０１経由で、ユーザの情報処理装置１０３に表示する。ユーザがデータを選択し、その時刻認証を要求すると、保存サーバ１０５はネットワーク１０１経由で時刻認証サーバ１０４に時刻認証を要求し、時刻認証の結果、受信したタイムスタンプをデジタルデータに埋めんで編集不可能なデータを作成して保存する。ユーザから、選択されたデータ、編集可能なデータあるいは編集不可能なデータのデータ形式が選択されると、選択されたデータ形式でデータをユーザの情報処理装置１０３に送信する。ユーザは所望のデータ形式でデータをダウンロードできる。

【選択図】　図２



【特許請求の範囲】
【請求項１】
編集可能なデータを保存するデータ保存装置において、
前記編集可能なデータの中から選択されたデータの時刻認証を要求し、該時刻認証の結果、得られた時刻情報を取得する時刻認証要求手段と、
前記時刻認証要求手段により取得した時刻情報を前記選択されたデータに付加して編集不可能なデータを作成する作成手段と、
時刻認証されたデータを要求された場合、前記作成手段により作成された編集不可能なデータを送信する送信手段とを備えたことを特徴とするデータ保存装置。
【請求項２】
保存された編集可能なデータまたは保存された編集不可能なデータの一覧を表示するデータ表示手段と、
前記データ表示手段により表示された一覧の中のデータの選択を受け付ける選択手段とを備え、
前記送信手段は、前記選択されたデータを送信することを特徴とする請求項１記載のデータ保存装置。
【請求項３】
前記データ表示手段は、前記時刻情報が付加された編集不可能なデータであるか否かの識別を併せて表示することを特徴とする請求項２記載のデータ保存装置。
【請求項４】
保存された編集不可能なデータの一覧を表示するデータ表示手段と、
前記データ表示手段により表示された一覧の中のデータの選択を受け付ける選択手段と、
前記選択された編集不可能なデータに付加された時刻情報の検証を要求し、該検証結果を取得する時刻認証確認手段と、
前記時刻認証確認手段により取得した検証結果を表示する検証結果表示手段とを備えたことを特徴とする請求項１乃至３のいずれかに記載のデータ保存装置。
【請求項５】
前記検証結果、前記編集不可能なデータの保存先情報、または前記検証結果を基に有効と判定された編集不可能なデータのいずれかの印刷指示を受け付ける印刷指示手段を備え、該印刷指示に従った印刷を要求することを特徴とする請求項４記載のデータ保存装置。
【請求項６】
編集可能なデータをデータ記憶装置に保存するデータ保存方法において、
前記編集可能なデータの中から選択されたデータの時刻認証を要求し、該時刻認証の結果、得られた時刻情報を取得する時刻認証要求ステップと、
前記時刻認証要求ステップで取得した時刻情報を前記選択されたデータに付加して編集不可能なデータを作成する作成ステップと、
時刻認証されたデータを要求された場合、前記作成ステップで作成された編集不可能なデータを送信する送信ステップとを有することを特徴とするデータ保存方法。
【請求項７】
保存された編集可能なデータまたは保存された編集不可能なデータの一覧を表示するデータ表示ステップと、
前記データ表示ステップで表示された一覧の中のデータの選択を受け付ける選択ステップとを有し、
前記送信ステップでは、前記選択されたデータを送信することを特徴とする請求項６記載のデータ保存方法。
【請求項８】
保存された編集不可能なデータの一覧を表示するデータ表示ステップと、
前記データ表示ステップで表示された一覧の中のデータの選択を受け付ける選択ステップと、

前記選択された編集不可能なデータに付加された時刻情報の検証を要求し、該検証結果を取得する時刻認証確認ステップと、
前記時刻認証確認ステップで取得した検証結果を表示する検証結果表示ステップとを有することを特徴とする請求項６または７記載のデータ保存方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、保存されているデータの時刻認証を提供するデータ保存装置およびデータ保存方法に関する。
【背景技術】
【０００２】
従来、プリンタ、ファクシミリ装置、複合機等のデータ処理装置には、時計が搭載されており、データの作成時刻やジョブの処理時刻として、この時計によって刻まれる時刻が付けられていた（例えば、特許文献１参照）。そして、このような時刻が付けられたデータは、データ保存装置に保存されていた。
【特許文献１】特開平１１－１７５２７３号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
しかしながら、上記従来のデータ保存装置には、以下に掲げる問題があった。すなわち、データ処理装置に搭載された時計が刻む時刻は、データ処理装置の管理者や使用者によって自由に設定可能であり、実際の時刻とは別の時刻に設定されるような事態を防止することができなかった。つまり、データ処理装置の制御ソフトウェアによって付けられる時刻は、第三者から見て信頼するに足るものとは言えず、データ保存装置から読み出したデータの時刻情報が正確なものであるとは限らなかった。
【０００４】
また、データ保存装置に保存されているデータが、時刻情報を付加した後に変更されたものであったり、改竄されたものであるおそれがあった。
【０００５】
そこで、本発明は、保存されているデータの時刻認証をより簡単に行うことができ、時刻認証後のデータの変更・改竄を防止できるデータ保存装置およびデータ保存方法を提供することを目的とする。
【０００６】
または、本発明は、保存されているデータを、編集可能なデータ形式で送信したり、編集不可能なデータ形式で送信することができるデータ保存装置およびデータ保存方法を提供することを他の目的とする。または、本発明は、保存されているデータの時刻認証を簡単に検証できるデータ保存装置およびデータ保存方法を提供することを他の目的とする。
【課題を解決するための手段】
【０００７】
上記目的を達成するために、本発明のデータ保存装置は、編集可能なデータを保存するデータ保存装置において、前記編集可能なデータの中から選択されたデータの時刻認証を要求し、該時刻認証の結果、得られた時刻情報を取得する時刻認証要求手段と、前記時刻認証要求手段により取得した時刻情報を前記選択されたデータに付加して編集不可能なデータを作成する作成手段と、時刻認証されたデータを要求された場合、前記作成手段により作成された編集不可能なデータを送信する送信手段とを備えたことを特徴とする。
【０００８】
本発明のデータ保存方法は、編集可能なデータをデータ記憶装置に保存するデータ保存方法において、前記編集可能なデータの中から選択されたデータの時刻認証を要求し、該時刻認証の結果、得られた時刻情報を取得する時刻認証要求ステップと、前記時刻認証要求ステップで取得した時刻情報を前記選択されたデータに付加して編集不可能なデータを

作成する作成ステップと、時刻認証されたデータを要求された場合、前記作成ステップで作成された編集不可能なデータを送信する送信ステップとを有することを特徴とする。

【発明の効果】

【０００９】

本発明の請求項１に係るデータ保存装置によれば、編集可能なデータの中から選択されたデータの時刻認証を要求し、該時刻認証の結果、得られた時刻情報を取得し、前記取得した時刻情報を前記選択されたデータに付加して編集不可能なデータを作成し、時刻認証されたデータを要求された場合、前記作成された編集不可能なデータを送信するので、保存されているデータの時刻認証をより簡単に行うことができ、時刻認証後のデータの変更・改竄を防止できる。

【００１０】

請求項２に係るデータ保存装置によれば、保存されているデータを、編集可能なデータ形式で送信したり、編集不可能なデータ形式で送信することができる。請求項４に係るデータ保存装置によれば、保存されているデータの時刻認証を簡単に検証できる。

【発明を実施するための最良の形態】

【００１１】

本発明のデータ保存装置およびデータ保存方法の実施の形態について、図面を参照しながら説明する。

【００１２】

［システム構成］

図１は実施の形態における時刻認証システムの構成を示す図ある。この時刻認証システムは、画像処理装置１０２、情報処理装置１０３、時刻認証サーバ１０４および保存サーバ１０５がネットワーク１０１を介して相互に通信可能に接続された構成を有する。

【００１３】

画像処理装置としての複合機（ＭＦＰ）１０２は、紙原稿をスキャンしたり、情報処理装置１０３から送られてきた印刷ジョブを処理して印刷したり、情報処理装置１０３からＦＴＰプロトコルで送られた印刷データを処理したり、紙原稿をスキャンしその画像をＰＤＦデータに変換してメールに添付した上で情報処理装置１０３や保存サーバ１０５に送信する機能等を有する。

【００１４】

情報処理装置１０３は、ＭＳ－Ｗｏｒｄ（米国マイクロソフト社の登録商標）等のアプリケーションによってデジタルデータを作成したり、そのデジタルデータのハッシュ値を計算して時刻認証サーバ１０４に送信したり、その後、時刻認証サーバ１０４からタイムスタンプを受信する機能の他、デジタルデータを保存サーバ１０５にアップロードする機能等を有する。

【００１５】

時刻認証サーバ１０４は、規格に準拠して正確な時間を刻む時計を有しており、それに基づいて時刻認証を行い、そのタイムスタンプを生成し、画像処理装置１０２、情報処理装置１０３、保存サーバ１０５などの要求に従って、そのタイムスタンプを送信したり、作成したタイムスタンプを検証する機能を有する。

【００１６】

保存サーバ１０５は、画像処理装置１０２、情報処理装置１０３、時刻認証サーバ１０４などの要求に応じて、デジタルデータを受信して保存したり、保存されたデジタルデータを送信する他、後述するように、保存したデジタルデータの時刻認証を要求する等の機能を有する。

【００１７】

尚、図１では、画像処理装置、情報処理装置、時刻認証サーバおよび保存サーバがそれぞれ１台しかネットワーク１０１に接続されていないが、複数台接続されてもよいことは勿論である。また、このネットワーク１０１は、ローカルエリアネットワーク（ＬＡＮ）で構成されているが、複数のコンピュータがネットワークに接続可能である限り、ＷＡＮ

など他のネットワークでもよい。また、フロアやビル内のオフィスのＬＡＮでは、コンピュータを接続するために、イーサネット（登録商標）（米国ゼロックス社）がよく使われる。また、ネットワークは、イントラネット、インターネットのどちらでもよく、インターネット上に時刻認証局および保存サーバが存在する場合、イントラネット上に存在する場合のどちらでも実現可能である。また、インターネットへの接続方式としては、電話機のダイアルアップによるナローバンド接続、ｘＤＳＬや光ファイバによるブロードバンド接続など、特に限定されない。

【００１８】

［保存サーバの構成］

図２は保存サーバ１０５の構成を示す図である。保存サーバ１０５は、内部バス１５１を介してネットワークインタフェース１５２、ハッシュ値生成部１５３、時刻認証局処理部１５４、タイムスタンプデータ処理部１５５、要求判定処理部１５７およびデータ管理処理部１５８を有する。

【００１９】

上記構成を有する保存サーバ１０５では、ユーザが情報処理装置１０３から指示を行うと、その指示がネットワーク１０１経由で保存サーバ１０５のデータ管理処理部１５８に送られる。これにより、保存サーバ１０５は指示されたデジタルデータの時刻認証を開始する。

【００２０】

まず、保存サーバ１０５は、データ管理処理部１５８で管理されているデジタルデータに対し、ハッシュ値生成部１５３により一方向性関数を用いてハッシュ値を生成する。このとき用いられる一方向性関数とそのパラメータは、時刻認証局処理部１５４が予めネットワーク１０１経由で時刻認証サーバ１０４とネゴシエーションを行い、時刻認証サーバ１０４によって指定された一方向性関数とそのパラメータを認識し、その情報を時刻認証局処理部１５４内に保存しておくことで、用意されている。ハッシュ値生成部１５３は、この情報を用いてハッシュ値を生成する。

【００２１】

本実施形態では、どの時刻認証サーバを用いてもよい。一般に運用上のメリットから、保存サーバ１０５が連携・契約している時刻認証サーバが用いられる。また、いくつかの時刻認証サーバと連携・契約している場合、ユーザにその選択肢を提示し、ユーザの選択に従うようにしてもよい。時刻認証サーバが決まると、用いるべき一方向性関数とそのパラメータは一意に決定される。この場合、時刻認証局処理部１５４が複数の時刻認証サーバの管理を行うことになる。

【００２２】

保存サーバ１０５は、ハッシュ値を生成した後、生成したハッシュ値をネットワーク１０１経由で時刻認証サーバ１０４に送信し、時刻認証を要求する。時刻認証サーバ１０４は、正確な時刻を刻む時計を有しており、そこから正確な時刻を取得する。また、時刻認証サーバ１０４は、保存サーバ１０５から送信されたハッシュ値を受信すると、その時刻情報と送られたハッシュ値に対し、時刻認証サーバ１０４が持つ秘密鍵で持って電子署名を生成し、それをタイムスタンプとして保存サーバ１０５に返信する。

【００２３】

尚、この時刻認証シーケンスのプロトコルとして、時刻認証サーバによって指定されたものが用いられる。一般に、このプロトコルは標準化されており、それに従ってタイムスタンプの取得が行われる。また、このシーケンスは、インターネット上の時刻認証局の場合、イントラネット上の時刻認証サーバの場合のいずれの場合でも、変わらない。

【００２４】

［ＭＦＰ１０２および保存サーバ１０５の構成］

図３はネットワーク１０１を介して接続されるＭＦＰ１０２および保存サーバ１０５の電気的構成を示す図である。ＭＦＰ１０２は、画像読み取りを行うスキャナユニット２５１、そのスキャン画像データを処理するスキャナＩＰ部２５２、ファクシミリなどに代表

される電話回線を利用した画像の送受信を行うＦＡＸ部２５３、ネットワークを利用して画像データや装置情報をやり取りするＮＩＣ（ネットワークインターフェイスカード）２５４、および送られてきたページ記述言語（ＰＤＬ）を画像データに展開するＰＤＬ部２５５を有する他、コア部２５６、プリンタＩＰ部２５７、ＰＷＭ部２５８、プリンタ（部）２６０およびフィニッシャ（部）２６１を有する。ＭＦＰ１０２の使い方に応じて、コア部２５６は、画像データを一時保存したり、経路を決定する。

【００２５】

コア部２５６から出力された画像データは、プリンタＩＰ部２５７で画像処理された後、画像形成のために、ＰＷＭ部２５８を経由してプリンタ２６０に送られる。プリンタ２６０でプリントアウトされたシートは、フィニッシャ２６１に送り込まれると、シートの仕分け処理やシートの仕上げ処理が行われる。また、表示操作パネル２５９は、画像をプリントアウトせずに画像の内容を確認したり、プリントアウトする前に画像の様子を確認する、いわゆるプレビューを行う。

【００２６】

つづいて、時刻認証サーバ１０４、保存サーバ１０５および情報処理装置１０３の構成を示す。これらの装置は、汎用のＰＣから構成され、ほぼ同様の構成を有するので、ここでは代表して保存サーバ１０５についてだけ説明する。なお、保存サーバ１０５は、大量の画像データを記憶可能な大容量のディスクを有しており、この点で、時刻認証サーバ１０４および情報処理装置１０３と構成を異にする。また、時刻認証サーバ１０４は、正確な時を刻む時計を有する点で、保存サーバ１０５および情報処理装置１０３と構成を異にする。

【００２７】

保存サーバ１０５は、ＣＰＵ１３１、ＲＡＭ１３２、ＣＲＴ１３３、キーボード１３４、ポインティングデバイス１３５、ＲＯＭ１３６、ハードディスク（ＤＩＳＫ）１３７およびＮＩＣ１５２がシステムバス１４０を介して相互に接続された構成を有する。ここで、ハードディスク１３７はデータ管理処理部１５８に含まれるものである。また、保存サーバ１０５を制御するプログラムは、記憶媒体であるハードディスク（ＤＩＳＫ）１３７に格納されており、必要に応じてＲＡＭ１３２に読み出され、ＣＰＵ１３１によって実行される。そして、図２の各部は、ＣＰＵ１３３がハードディスク１３７に格納された制御プログラムを実行することにより実現される。また、ＣＰＵ１３１は、ＣＲＴ１３３によって各種情報の表示を行い、キーボード１３４およびポインティングデバイス１３５からユーザの指示を受け付ける。さらに、ＣＰＵ１３１は、ＮＩＣ１５２およびネットワーク１０１を通じて外部の情報処理装置１０３、時刻認証サーバ１０４、ＭＦＰ１０２等と通信を行う。

【００２８】

［時刻認証取得時の保存サーバの内部動作］

図４は時刻認証取得時における保存サーバ１０５の動作処理手順を示すフローチャートである。この処理プログラムは、保存サーバ１０５内のハードディスク１３７に格納されており、ＣＰＵ１３１によって実行される。まず、データ管理処理部１５８で管理され、ハードディスク１３７に記憶されている画像データ（デジタルデータ）を読み出し、ネットワークインタフェース１５２およびネットワーク１０１を経由してユーザの情報処理装置１０３に表示する（ステップＳ１）。

【００２９】

ユーザによってデジタルデータが選択され、その時刻認証の取得が指示されたか否かを判別する（ステップＳ２）。指示されていない場合、ステップＳ２の処理を繰り返す。一方、ユーザによって指示されると、その指示がネットワーク１０１経由で保存サーバ１０５のデータ管理処理部１５８に送られる。これにより、保存サーバ１０５はそのデジタルデータの時刻認証処理を開始する。

【００３０】

まず、保存サーバ１０５は、データ管理処理部１５８で管理されているデジタルデータ

に対し、ハッシュ値生成部１５３により、一方向性関数を用いてハッシュ値を生成する（ステップＳ３）。このとき用いられる一方向性関数とそのパラメータは、時刻認証局処理部１５４が予め時刻認証サーバ１０４とネットワーク１０１経由でネゴシエーションを行い、時刻認証サーバ１０４によって指定された一方向性関数とそのパラメータを認識し、内部に保存したものである。ハッシュ値生成部１５３は、この情報を基にハッシュ値を生成する。

【００３１】

尚、本実施形態では、いずれの時刻認証サーバであっても構わない。一般に運用上の利点から、保存サーバ１０５と連携・契約している時刻認証サーバが用いられる。また、複数の時刻認証サーバと連携・契約している場合、ユーザにその選択肢を示し、ユーザの選択に従うようにしてもよい。これにより、時刻認証に用いられる時刻認証サーバが選択されるので、用いるべき一方向性関数とそのパラメータは一意に決定される。この場合、複数の時刻認証サーバの管理は、時刻認証局処理部１５４によって行われる。

【００３２】

保存サーバ１０５は、ハッシュ値を生成した後、生成したハッシュ値をネットワーク１０１経由で時刻認証サーバ１０４に送信し、時刻認証の取得を要求する（ステップＳ４）。そして、保存サーバ１０５は、ネットワークインタフェース１５２によりネットワーク１０１経由で時刻認証サーバ１０４から送られてきたタイムスタンプを受信するまで待機する（ステップＳ５）。タイムスタンプを受信すると、受信したタイムスタンプは、保存サーバ１０５内のデータ管理処理部１５８に送られ、ハードディスク１３７に保存される。

【００３３】

このとき、データ管理処理部１５８は、時刻認証したデジタルデータとそのタイムスタンプとを関連付けて管理する。具体的な関連付けの方法としては、種々考えられるが、例えば、１つのデジタルデータ毎に１つのフォルダを用意し、その中に対となるデジタルデータとタイムスタンプを保存する方法や、ＸＭＬなどの記述言語を用いたデータによって対となるデジタルデータとタイムスタンプを特定する方法などが挙げられる。さらに、デジタルデータとタイムスタンプを１つのデジタルデータに合体し、編集できない属性を有するデータに変換して管理する方法もある。

【００３４】

例えば、Ａｄｏｂｅ社のアプリケーションであるＡｃｒｏｂａｔの時刻認証プラグインによる管理が知られている。これを用いた場合、タイムスタンプデータ処理部１５５は、データ管理処理部１５８で管理されているデジタルデータをＰＤＦデータに変換する。この後、時刻認証サーバ１０４から送られ、データ管理処理部１５８に保存されているタイムスタンプをタイムスタンプデータ処理部１５５に送る。そして、タイムスタンプデータ処理部１５５はＰＤＦデータにタイムスタンプを埋め込む。さらに、Ａｃｒｏｂａｔの暗号化機能を用いて編集できない属性を有するＰＤＦデータとする。この方法は、既にＡｃｒｏｂａｔによって実現されているので、この方法をそのまま使うことで、タイムスタンプが埋められた変更不可能なデジタルデータの管理方法を取得できる。

【００３５】

具体例として、時刻認証された「２００２．０９．２１＿ｍｅｅｔｉｎｇ＿ｍｅｍｏ．ｄｏｃ」のデジタルデータと、そのタイムスタンプである「２００２．０９．２１＿ｍｅｅｔｉｎｇ＿ｍｅｍｏ．ｔｍｓ」のデジタルデータが存在している場合を想定する。「２００２．０９．２１＿ｍｅｅｔｉｎｇ＿ｍｅｍｏ．ｄｏｃ」のデジタルデータをＰＤＦファイルに変換してタイムスタンプを埋め込んだものが、「２００２．０９．２１＿ｍｅｅｔｉｎｇ＿ｍｅｍｏ．ｐｄｆ」のＰＤＦデータである。このＰＤＦデータは、時刻認証されたファイルの内容を示す上、タイムスタンプも内蔵しているので、このＰＤＦデータだけで時刻認証の検証を行うことが可能である。

【００３６】

即ち、保存サーバ１０５は、ファイルを保存する際、ファイルそのものと、時刻認証し

た場合、そのタイムスタンプと、そのデータおよびタイムスタンプが一体化された編集不可能なファイルとの３種類のファイルを保存することになる。これらのファイルは、データ管理処理部１５８によって管理されている。

【００３７】

図５は時刻認証取得時における時刻認証サーバ１０４の動作処理手順を示すフローチャートである。この処理プログラムは、時刻認証サーバ１０４内の記憶媒体に格納されており、ＣＰＵ（図示せず）によって実行される。前述したように、時刻認証サーバ１０４は、正確な時刻を刻む時計を持っており、そこから正確な時刻を得ることができる。

【００３８】

まず、保存サーバ１０５から送信されたハッシュ値を受信するのを待ち（ステップＳ１１）、ハッシュ値を受信すると、その時の正確な時刻情報を取得する（ステップＳ１２）。そして、時刻認証サーバ１０４は、その時の時刻情報と送られたハッシュ値に対し、時刻認証サーバ１０４が持つ秘密鍵で電子署名を生成し（ステップＳ１３）、それをタイムスタンプとして保存サーバ１０５に返信する（ステップＳ１４）。この後、本処理を終了する。

【００３９】

この時刻認証シーケンスにおけるプロトコルとして、時刻認証サーバが指定したものが用いられる。一般に、このプロトコルは標準化されており、それに従ってタイムスタンプの取得が行われる。このシーケンスは、インターネット上の時刻認証局の場合、イントラネット上の時刻認証サーバの場合のいずれであっても、変わらない。

【００４０】

［時刻認証確認時の保存サーバの内部動作］

図６は時刻認証確認時における保存サーバ１０５の動作処理手順を示すフローチャートである。この処理プログラムは、保存サーバ１０５内のハードディスク１３７に格納されており、ＣＰＵ１３１によって実行される。まず、データ管理処理部１５８で管理され、ハードディスク１３７に記憶されている画像データ（デジタルデータ）を読み出し、ネットワークインタフェース１５２およびネットワーク１０１を経由してユーザの情報処理装置１０３に表示する（ステップＳ２１）。

【００４１】

ユーザによってデジタルデータが選択され、その時刻認証確認の指示を受け付けるまで待つ（ステップＳ２２）。つまり、ユーザが情報処理装置１０３に対して指示を行うと、その指示がネットワーク１０１経由で保存サーバ１０５のデータ管理処理部１５８に送られる。これにより、保存サーバ１０５はそのデジタルデータの時刻認証の確認処理を開始する。

【００４２】

そして、保存サーバ１０５は、前述したように、その内部管理テーブルあるいは別のＸＭＬなどで記述されたリンクファイルによって、指定されたデジタルデータに対応するタイムスタンプを検索する（ステップＳ２３）。検索したタイムスタンプをタイムスタンプデータ処理部１５５によって処理し、時刻認証を行った時刻認証サーバ１０４を特定する。保存サーバ１０５は、特定された時刻認証サーバ１０４に対し、データ管理処理部１５８によって管理されているタイムスタンプをネットワークインタフェース１５２およびネットワーク１０１経由で送信し、時刻認証の確認要求を行う（ステップＳ２４）。尚、このタイムスタンプの構造は標準規格に規定されているので、時刻認証サーバの特定方法は既知であり、その詳細については省略する。

【００４３】

保存サーバ１０５は、ネットワークインタフェース１５２により、ネットワーク１０１経由で時刻認証サーバ１０４から送られてきた時刻認証の確認結果を受信するまで待ち（ステップＳ２５）、時刻認証の確認結果を受信すると、これをタイムスタンプデータ処理部１５５に送る。タイムスタンプデータ処理部１５５は、その結果をデータ管理処理部１５８に通知する。データ管理処理部１５８は、デジタルデータやタイムスタンプの存在と

共に、その結果をユーザの情報処理装置１０３に通知して表示する（ステップＳ２６）。この後、本処理を終了する。

【００４４】

図７は時刻認証確認時における時刻認証サーバ１０４の動作処理手順を示すフローチャートである。この処理プログラムは、時刻認証サーバ１０４内の記憶媒体に格納されており、ＣＰＵ（図示せず）によって実行される。

【００４５】

まず、時刻認証サーバ１０４は、タイプスタンプを受信するまで待つ（ステップＳ３１）。タイムスタンプを受信して確認要求があると、時刻認証サーバ１０４のみが持つ秘密鍵によってタイムスタンプ内の電子署名を復号化し、改竄があったか否かを判定し（ステップＳ３２）、その判定結果と埋め込まれている時刻情報を取り出す（ステップＳ３３）。これらの結果を保存サーバ１０５に返信する（ステップＳ３４）。この後、本処理を終了する。この認証確認シーケンスにおけるプロトコルとして、時刻認証サーバが指定したものが用いられる。一般に、このプロトコルは標準化されており、それに従ってタイムスタンプの取得が行われる。

【００４６】

［デジタルデータのダウンロード時の保存サーバの内部動作］

図８はデジタルデータのダウンロード時における保存サーバ１０５の動作処理手順を示すフローチャートである。この処理プログラムは、保存サーバ１０５内のハードディスク１３７に格納されており、ＣＰＵ１３１によって実行される。まず、データ管理処理部１５８で管理され、ハードディスク１３７に記憶されている画像データ（デジタルデータ）を読み出し、ネットワークインタフェース１５２およびネットワーク１０１を経由してユーザの情報処理装置１０３に表示する（ステップＳ４１）。ユーザは、保存サーバ１０５に対して、編集可能なデータ形式（可変な形）でダウンロードするのか、あるいは時刻認証された編集不可能なデータ形式（変更不可の形）でダウンロードするのかを明示し、ダウンロードを指示する。

【００４７】

そして、ダウンロードの指示を受け付けたか否かを判別する（ステップＳ４２）。つまり、ユーザの指示がネットワーク１０１経由で保存サーバ１０５のデータ管理処理部１５８に送られたか否かを判別する。ユーザの指示が送られていない場合、ダウンロードの指示を受け付けるまで待ち、ダウンロードの指示を受け付けると、ダウンロードの指示を判定する（ステップＳ４３）。つまり、保存サーバ１０５内の要求判定処理部１５７は、その指示内容を判断し、編集可能なデータ形式（可変な形）のダウンロードであるか、あるいは時刻認証された編集不可能なデータ形式（変更不可の形）のダウンロードであるかを判定する。要求判定処理部１５７は、その判定結果をデータ管理処理部１５８に通知する。

【００４８】

そして、ダウンロードの指示判定結果を基に、対応するデジタルデータを検索し（ステップＳ４４）、見つかった対応するデジタルデータをユーザの情報処理装置１０３に送信する（ステップＳ４５）。この後、本処理を終了する。つまり、データ管理処理部１５８は、要求判定処理部１５７からの通知に基づき、適切なデータをユーザに送信する。具体的に、編集可能なデータ形式（可変な形）のダウンロード要求である場合、データ管理処理部１５８は、管理しているデータのうち、ユーザがアップロードしたデジタルデータそのものを選択する。一方、時刻認証された編集不可能なデータ形式（変更不可の形）のダウンロード要求である場合、データ管理処理部１５８は、管理しているデータのうち、タイムスタンプが埋められた編集不可能なデータ形式（変更不可）のデジタルデータを選択する。

【００４９】

データ管理処理部１５８は、ユーザのダウンロード要求に従って選択したデータを、ネットワークインタフェース１５２により、ネットワーク１０１経由で送信する。これによ

り、保存サーバ１０５は、その内部に保存されているデジタルデータのうち、編集可能なデータ形式（可変な形）で保存されているデジタルデータであるのか、それとも時刻認証された編集不可能なデータ形式（変更不可の形）で保存されているデジタルデータであるのかを識別可能に表示して、ユーザの情報処理装置１０３にダウンロードを行わせることができる。

【００５０】

［デジタルデータの作成から保存サーバへのアップロード時のユーザ操作］

つぎに、デジタルデータを作成し、保存サーバにアップロードする際の動作を示す。まず、ユーザは、ＰＣ（パーソナルコンピュータ）に代表される情報処理装置１０３において、ＭＳ－Ｗｏｒｄ（米国マイクロソフト社の登録商標）などのアプリケーションを用いてデータを作成する。データの作成が完了すると、それをデジタルデータとして保存する。ユーザは、他人が再編集できるように、このデジタルデータを共有したいと考えた場合、ネットワーク１０１上の保存サーバ１０５にアップロードし、このデジタルデータを保存サーバ１０５に保存する。

【００５１】

また、コピーおよび複合機（ＭＦＰ）に代表される画像処理装置１０２によってデジタルデータが作成される場合も考えられる。この場合、ユーザは、画像処理装置１０２に装備されているスキャナに紙原稿をセットし、原稿の読み取りを開始させる。画像処理装置１０２は、紙原稿をスキャンしてそのイメージを読み取り、それをＴＩＦＦやＪＰＥＧ等のデジタルデータに変換し、さらにマルチＴＩＦＦやＰＤＦ等のファイル形式に変換する。そして、変換されたデジタルデータを画像処理装置１０２から保存サーバ１０５に直接アップロードしたり、一旦、そのデジタルデータを情報処理装置１０３に転送した後、保存サーバ１０５にアップロードする。その後、保存サーバ１０５は、デジタルデータを受信して保存する。

【００５２】

図９は保存サーバ１０５の保存サービスにログインした場合の操作画面を示す図である。この操作画面は情報処理装置１０３の表示部に表示される。画面の１行目には、この操作画面で選択可能なコマンドのメニューバー２０１が設けられている。ここでは、ファイル２０２、コマンド２０３、ヘルプ２０４が設定されている。

【００５３】

画面の２行目２０５には、保存サーバ１０５にログインしたユーザ名が表示されている。ここでは、ログイン名は「××××　ＵＳＥＲ００５６５６」である。画面の３行目２０６には、保存サーバ１０５にログインした後、そのユーザがアクセス可能なトップディレクトリ名が表示されている。その左下側のフォルダ一覧画面２０７には、その配下にあるフォルダの一覧が表示されている。

【００５４】

一方、右下側のデジタルデータ一覧画面２０９には、フォルダ一覧画面２０７で選択されたフォルダ（ここでは、Ｐｅｒｓｏｎａｌ２０８）内のデジタルデータが一覧表示されている。４つのデジタルデータが保存されており、そのデジタルデータ名２１２、デジタルデータサイズ２１３、作成日２１４、代表頁のサムネール画像２１１、タイムスタンプ欄２１５などが表示されている。フォルダ名とその日付から所望のデジタルデータにアクセスすることが可能である。

【００５５】

尚、図９の操作画面は専用アプリケーションの操作画面であるが、どのような操作画面であってもよい。この他、Ｗｅｂクライアントとして米国マイクロソフト社のインタネットエクスプローラやＨＴＴＰクライアント等であってもよい。

【００５６】

保存サーバ１０５へのアップロード時、デジタルデータ毎の整理を行うために、フォルダを作成する場合を示す。図９のメニューバー２０１からコマンド２０３を選択すると、コマンドとして用意されている機能が選択可能である。図１０はコマンドメニューを示す

図である。ここで、「フォルダの作成」４０６を選択すると、図１１（Ａ）に示すように、フォルダの名前付け画面３０１が表示される。図１１はフォルダの名前付け画面およびアップロード画面を示す図である。フォルダの名前付け画面３０１から、フォルダ名３０２を入力すると、図９のフォルダ一覧画面２０７に新しいフォルダが作成される。この後、新規に作成したフォルダを選択し、このフォルダ内にデジタルデータをアップロードすることを指示する。

【００５７】

また、メニューバー２０１からコマンド２０３を選択し、図１０のアップロード４０２を選択すると、図１１（Ｂ）に示すように、アップロードするデジタルデータの名前を入力する画面３０３が表示される。デジタルデータ名３０４を入力すると、図９のデジタルデータ一覧画面２０９には、アップロードされたデジタルデータが表示される。その画面には、そのデジタルデータ名２１２、デジタルデータサイズ２１３、作成日２１４、代表頁のサムネール画像２１１、タイムスタンプ欄２１５などが表示される。デジタルデータをアップロードした後、保存サーバ１０５にアクセスすると、保存サーバ１０５に保存されているデジタルデータを見ることができる。

【００５８】

［時刻認証取得時のユーザ操作］

つぎに、保存サーバ１０５に保存されているデジタルデータの時刻認証を取得する際の操作を示す。まず、ユーザは、保存サーバ１０５にログインし、所望のデジタルデータを特定する。この手順は前述したアップロードと同じである。ユーザは、デジタルデータを特定した後、保存サーバ１０５が提供する時刻認証サービスの実行を指示する。

【００５９】

図９の操作画面では、フォルダ一覧画面２０７内の所望のフォルダ名を選択すると、そのフォルダ内に保存されているデジタルデータが表示される。例えば、フォルダ一覧画面２０７内のＰｅｒｓｏｎａｌ２０８を選択すると、このフォルダ内に保存されている４つのデジタルデータがデジタルデータ一覧画面２０９に表示される。ここでは、「ｆｒｉｅｎｄ」、「ｍａｒｒｉａｇｅ」、「ｃａｒｄｓ」および「ｍａｐ」の４つのデジタルデータが表示される。

【００６０】

例えば、「ｃａｒｄｓ」という名前のデジタルデータの時刻認証を行う操作を示す。「ｃａｒｄｓ」のデジタルデータは、そのタイムスタンプ（Ｔｉｍｅ　ｓｔａｍｐ）欄２１５を見ると、「ｎｏｎｅ」と表示されており、これはそのデジタルデータが時刻認証されていないことを示している。デジタルデータ一覧画面２０９内のチェック（ｃｈｅｃｋ）欄２１０にある「ｃａｒｄｓ」のチェックボックスを選択（チェック）すると、チェックボックスが□から■に変化する。この後、コマンド２０３から「時刻認証を行う」４０８を実行する。そして、ユーザの確認画面が表示された後、保存サーバ１０５は「ｃａｒｄｓ」のデジタルデータの時刻認証を行う。

【００６１】

尚、保存サーバ１０５に保存されているデジタルデータの時刻認証を行う操作手順は上記の通りであるが、この手順は一例である。したがって、デジタルデータの選択手順や選択したデジタルデータの時刻認証を指示する手順は、ユーザが保存サーバ１０５に指示を行えるようになっている限り、特に限定されるものでなく、この画面を実現するアプリケーションやＯＳに依存して異なってもよい。

【００６２】

時刻認証サーバ１０４によって時刻認証が行われた後、保存サーバ１０５は、時刻認証サーバ１０４からタイムスタンプを受信する。受信したタイムスタンプは、時刻認証されたデジタルデータ（ここでは、「ｃａｒｄｓ」）と関連付けされた後、保存される。例えば、関連付けとしては、時刻認証されたデジタルデータとタイムスタンプを、保存サーバ１０５の同じフォルダ内に保存する方法が挙げられる。また、デジタルデータ一覧画面２０９では、「ｆｒｉｅｎｄ」のデジタルデータが時刻認証され、そのタイムスタンプが保

存されている状態であるので、そのタイムスタンプ欄２１５には、「ｄｏｎｅ」が表示されている。

【００６３】

［時刻認証確認時のユーザ操作］

つぎに、時刻認証の取得後、ユーザが時刻認証を検証する場合を示す。まず、ユーザは保存サーバ１０５にログインし、所望のデジタルデータを選択する。このデジタルデータの選択手順は、前述した時刻認証取得時と同様である。図９のデジタルデータ一覧画面２０９に表示されている４つのデジタルデータのうち、「ｆｒｉｅｎｄ」のデジタルデータは、そのタイムスタンプ欄２１５が「ｄｏｎｅ」となっているので、時刻認証され、そのタイムスタンプが保存されている状態を示す。そして、「ｆｒｉｅｎｄ」のデジタルデータを選択すると、そのチェック欄２１０の表示は□から■に変わる。

【００６４】

この後、コマンド２０３から「時刻認証を検証する」４０９を選択して実行する。ユーザの確認画面が表示された後、保存サーバ１０５は、「ｆｒｉｅｎｄ」のデジタルデータに対する時刻認証の検証を行う。そして、保存サーバ１０５は、時刻認証サーバ１０４から送られた検証の結果をユーザの情報処理装置１０３に表示する。図１２は時刻認証の結果を示す図である。同図（Ａ）は時刻認証の結果、有効である場合を示し、その結果表示欄１００２には、スタンプ時刻と「有効です」が表示されている。同図（Ｂ）は無効である場合を示し、その結果表示欄１００２には、「無効です」が表示されている。さらに、時刻認証サーバ１０４が検証した時刻も検証時刻欄１００３に表示される。

【００６５】

また、デジタルデータ一覧画面２０９では、「ｍａｒｒｉａｇｅ」のデジタルデータが時刻認証され、そのタイムスタンプが保存されている状態であり、かつ時刻認証サーバ１０４で検証され、それが有効である状態の場合、タイムスタンプ欄２１５には、「ｏｋ」が表示される。

【００６６】

また、検証結果の「有効です」は、タイムスタンプが時刻認証サーバ１０４で作成されたものであり、作成後から検証した時点までに改竄がないことを保証する。言い換えると、検証した以降は、改竄の保証がないので、将来に亘って有効であることを保証しない。しかし、ユーザにとっては、デジタルデータを見たときに有効であって欲しいという要望がある。この要望は、保存サーバ１０５にアクセスしたときに常に時刻認証の検証を行い、その結果を表示するようにすることで満たされる。図１３は時刻認証の検証時のオプション画面を示す図である。オプション画面１１０１には、「常に検証を行う」のチェックボックス１１０２および「ユーザの指示時に検証を行う」のチェックボックス１１０３が設けられている。いずれかのチェックボックスを選択することにより、時刻認証の検証時にオプションとして、常に検証するのか、あるいはユーザの指示時にのみ検証を行うのかを選択することができる。これにより、ユーザは、所望のデジタルデータに対し、タイムスタンプの存在とその正当性を簡単に認識できる。

【００６７】

つぎに、ユーザがその時刻認証の検証結果を印刷する場合を示す。図１２の検証結果の画面が表示され、ユーザが「ＯＫ」１００４を押下すると、その結果を印刷指示する画面５０１が表示される。図１４は検証結果の印刷指定画面を示す図である。この画面５０１では、印刷モードが選択可能である。画面５０１には、表紙印刷のチェックボックス５０２、リンク印刷のチェックボックス５０３、本文印刷のチェックボックス５０４、ＯＫボタン５０５およびＣａｎｃｅｌボタン５０６が表示されている。

【００６８】

表紙印刷モードとは、画面に表示されている内容に準じて、サムネール画像、名称、日付と共に、検証結果を印刷するモードである。リンク印刷モードとは、保存サーバ１０５に保存されているデジタルデータへのリンクを示すリンクデータを印刷するモードである。本文印刷モードとは、保存サーバ１０５に保存されている時刻認証されたデジタルデー

タの全頁を印刷するモードである。これらの印刷モードは、組み合わせて指定可能である。

【００６９】

ユーザは、印刷モードの指定後、ＯＫボタン５０５を押すことで、印刷を開始させる。これらの印刷モードを指定して印刷を行うと、時刻認証の検証結果としての有効、時刻認証された時刻、タイプスタンプを発行した時刻認証サーバ１０４の名前などのＩＤ情報、および時刻認証を検証した時刻からなる基本情報と共に、指定したオプションを印刷する。尚、無効である場合、その検証結果と共に指定したオプションを印刷する。また、キャンセルボタン５０６が押されると、印刷は行われない。

【００７０】

図１５は時刻認証の検証結果の印刷例を示す図である。図において、１２０１は基本情報が印刷された出力紙である。この出力紙１２０１には、基本情報として、デジタルデータ名１２０２（ここでは、「ｍａｒｒｉａｇｅ」）、検証結果１２０３（ここでは、「有効」）、認証時刻１２０４（ここでは、「２００３．０９．１５　１５：２３」に認証済み）、時刻認証を行った時刻認証サーバ名１２０５（ここでは、××××）、および時刻認証を検証した時刻１２０６（ここでは、「２００３．０９．１８　１８：０１」）が記載されている。

【００７１】

また、表紙印刷モードが指定された場合、出力紙１２１１が印刷される。この出力紙１２１１には、デジタルデータ名１２１２（ここでは、「ｍａｒｒｉａｇｅ」）、デジタルデータの作成日付１２１３（ここでは、「２００３．０９．１０　１０：１０」）、検証結果１２１４（ここでは、「有効」）、および代表ページのサムネール画像１２１５が記載されている。

【００７２】

また、リンク印刷モードが指定された場合、出力紙１２２１が印刷される。この出力紙１２２１には、デジタルデータ名１２２２（ここでは、「ｍａｒｒｉａｇｅ」）、およびデジタルデータへのリンク情報１２２３が記載されている。リンク情報１２２３として、リンク情報をバーコード化したものが印刷され、バーコードスキャナで呼び出すことで正確にリンク情報が入力できるようになっている。

【００７３】

また、本文印刷モードが指定された場合、出力紙１２３１が印刷される。この出力紙１２３１には、デジタルデータが印刷されている。これらの出力紙１２０１、１２１１、１２２１、１２３１は、それぞれの用紙に印刷されるばかりでなく、まとめて印刷されるようにしてもよい。

【００７４】

このような操作を行うことで、ユーザは、タイムスタンプ付きの認証時刻と時刻認証されたデジタルデータを得ることができ、時刻認証された出力紙を確認できる。

【００７５】

［保存サーバからデジタルデータのダウンロード時のユーザ操作］

つぎに、保存サーバ１０５に保存されているデジタルデータを取得する場合を示す。ダウンロードには、２通りの場合がある。すなわち、保存されているデジタルデータを編集するために、編集可能なデータ形式（可変な形）でダウンロードする場合と、時刻認証されたデジタルデータを第三者に送信して証明するために、時刻認証された編集不可能なデータ形式（変更不可の形）でダウンロードする場合である。それぞれの場合によって、ダウンロードされるデジタルデータは異なる。

【００７６】

そこで、ユーザは、保存サーバ１０５に対して編集可能なデータ形式（可変な形）のダウンロードであるか、あるいは時刻認証された編集不可能なデータ形式（変更不可の形）のダウンロードであるかを明示してダウンロードを指示する。その操作手順は以下の通りである。

【００７７】
まず、時刻認証されているデジタルデータを選択する。デジタルデータ一覧画面２０９に表示されているデジタルデータのうち、上２つが時刻認証されているデジタルデータであり、下２つが時刻認証されていないデジタルデータである。これらのデジタルデータの中から、ダウンロードしたいものを選択する。
【００７８】
そして、チェック（Ｃｈｅｃｋ）欄２１０のチェックボックスを選択すると、その表示が□から■に変わる。この後、コマンド２０３からダウンロードを実行する。前述したように、デジタルデータを編集するために、編集可能なデータ形式（可変な形）でダウンロードする場合、「可変形式でダウンロード」４０３を選択し、時刻認証されたデジタルデータを時刻認証された編集不可能なデータ形式（変更不可の形）でダウンロードする場合、「時刻認証でダウンロード」４０４を選択する。このような操作によって、ユーザが所望するデジタルデータの形式を保存サーバ１０５に通知する。ユーザは、保存サーバ１０５から所望のデータ形式のデジタルデータをダウンロードすることができる。
【００７９】
以上示したように、本実施形態によれば、保存サーバに保存されているデータの時刻認証を簡単に行うことができ、時刻認証後のデータの変更・改竄を防止できる。また、保存されているデータを、編集可能なデータ形式で送信したり、編集不可能なデータ形式で送信することができる。さらに、保存サーバに保存されているデータの時刻認証を簡単に検証できる。これにより、ユーザは、保存サーバに保存されているデジタルデータを編集するために、編集可能なデータ形式でダウンロードしたり、あるいは時刻認証されたデジタルデータを第三者に送信して証明するために、編集不可能なデータ形式でダウンロードすることができる。
【００８０】
この結果、以下のような問題が解決される。作成したデータが存在している時刻を公正明大な第三者に証明して貰う際、この証明を行う公正明大な第三者がいわゆる時刻認証局であり、精密な時計で刻まれる時刻に基づく時刻データ（タイムスタンプ）を付けて認証するサービスをインターネット上で行っている。この時刻認証局は、標準規格を満足する機能を備えているので、刻まれた時刻は他者から正しいと認識される。即ち、タイムスタンプを付けることを依頼するもの、付けられたタイムスタンプを確認するもの、どちらもこの時刻認証局を信じることで、そのタイムスタンプを信用することができる。しかし、この時刻認証局にタイムスタンプを付けるように依頼することと、付いたタイムスタンプを時刻認証局で確認することは、通常、ＰＣ（パーソナルコンピュータ）上で行われている。
【００８１】
具体的な手順は、次の通りである。ＰＣ上でデジタルデータを作成した後、そのデジタルデータのハッシュ値を計算し、時刻認証を受けたい時刻認証局を選択してそのハッシュ値を送付する。そして、時刻認証局で作成されたタイムスタンプを受信し、紙原稿のデジタルデータと受信したタイムスタンプとをセットにして管理する。さらに、そのタイムスタンプを時刻認証局で確認する場合、タイムスタンプを時刻認証局に送付し、時刻認証局で確認された結果を受信し、その結果をＰＣの画面上に表示する。こうして時刻認証とその確認が行われるが、この場合、時刻認証したデジタルデータとその時刻を証明するタイムスタンプとが別のファイルとして存在しており、管理が煩雑であった。
【００８２】
そこで、デジタルデータの保存を行う保存サーバにおいて時刻認証の生成・確認を行えると、その手間を大きく省くことができる。しかし、従来の保存サーバはアクセス制限を付けることができるが、一度、保存サーバからローカルのデジタルデータ処理装置にダウンロードした後、その変更を防止することはできない。時刻認証したタイムスタンプとそのデジタルデータは、時刻認証後は変更されないようにすべきであり、本実施形態の保存サーバでは、時刻認証後にデジタルデータが変更された場合、時刻認証したタイムスタン

プによって無効であると判定されるので、上記問題を解決できる。

【００８３】

以上が本発明の実施形態の説明であるが、本発明は、これら実施形態の構成に限られるものではなく、特許請求の範囲で示した機能、または実施形態の構成が持つ機能が達成できる構成であればどのようなものであっても適用可能である。

【００８４】

例えば、保存サーバに時刻認証サーバ機能を持たせることで、保存サーバがネットワークを介して時刻認証を行わなくて済むような構成とすることも可能である。この構成では、保存サーバで使われている時刻表示が正しいことが一般に認められるが、保存サーバから取り出されたデータの時刻属性が正しいことが常に証明されるわけではないので、時刻認証の必要性がなくなるわけではない。

【００８５】

また、ユーザが操作する操作画面を、保存サーバの表示部に表示してユーザの指示を受け付けるようにしてもよいし、ネットワーク１０１経由で保存サーバに接続された情報処理装置や画像処理装置（ＭＦＰ）の表示部に表示してユーザの指示を受け付け、ネットワーク１０１経由で保存サーバが受信するようにしてもよく、いずれの場合でも本発明は適用可能である。

【００８６】

また、本発明の目的は、実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）が記憶媒体に格納されたプログラムコードを読み出して実行することによっても達成される。

【００８７】

この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００８８】

又、プログラムコードを供給するための記憶媒体としては、例えば、ＲＯＭ、フロッピー（登録商標）ディスク、ＰＣＭＣＩＡカードやコンパクトフラッシュ（登録商標）等のメモリカード、ハードディスク、マイクロＤＡＴ、光磁気ディスク、ＣＤ－ＲやＣＤ－ＲＷ等の光ディスク、ＤＶＤ等の相変化型光ディスク等で構成されてもよい。

【００８９】

また、コンピュータが読み出したプログラムコードを実行することにより、上記実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【００９０】

更に、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【００９１】

ここで、請求項２乃至５に記載のデータ保存装置は、ネットワーク１０１を介して接続された保存サーバ１０５および情報処理装置１０３に相当する。

【図面の簡単な説明】

【００９２】

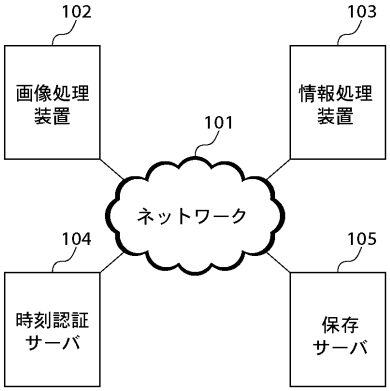
【図１】実施の形態における時刻認証システムの構成を示す図ある。

【図２】保存サーバ１０５の構成を示す図である。

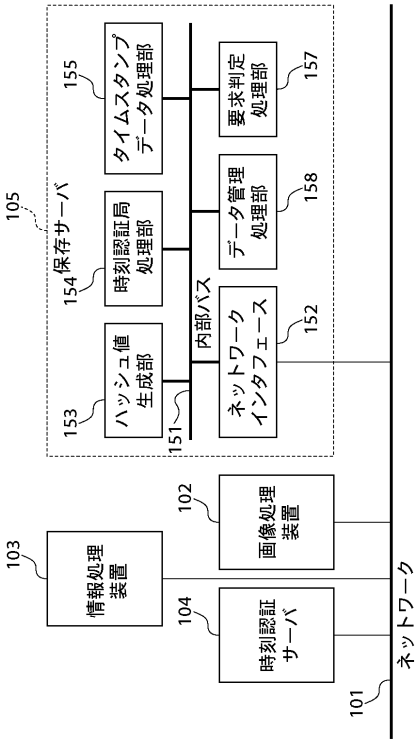
【図３】ネットワーク１０１を介して接続されるＭＦＰ１０２および保存サーバ１０５の

電気的構成を示す図である。
【図４】時刻認証取得時における保存サーバ１０５の動作処理手順を示すフローチャートである。
【図５】時刻認証取得時における時刻認証サーバ１０４の動作処理手順を示すフローチャートである。
【図６】時刻認証確認時における保存サーバ１０５の動作処理手順を示すフローチャートである。
【図７】時刻認証確認時における時刻認証サーバ１０４の動作処理手順を示すフローチャートである。
【図８】デジタルデータのダウンロード時における保存サーバ１０５の動作処理手順を示すフローチャートである。
【図９】保存サーバ１０５の保存サービスにログインした場合の操作画面を示す図である。
【図１０】コマンドメニューを示す図である。
【図１１】フォルダの名前付け画面およびアップロード画面を示す図である。
【図１２】時刻認証の結果を示す図である。
【図１３】時刻認証の検証時のオプション画面を示す図である。
【図１４】検証結果の印刷指定画面を示す図である。
【図１５】時刻認証の検証結果の印刷例を示す図である。
【符号の説明】
【００９３】
１０１　ネットワーク
１０３　情報処理装置
１０４　時刻認証サーバ
１０５　保存サーバ
１３１　ＣＰＵ
１３７　ハードディスク（ＤＩＳＫ）
１５４　時刻認証局処理部
１５５　タイムスタンプデータ処理部
１５７　要求判定処理部
１５８　データ管理処理部

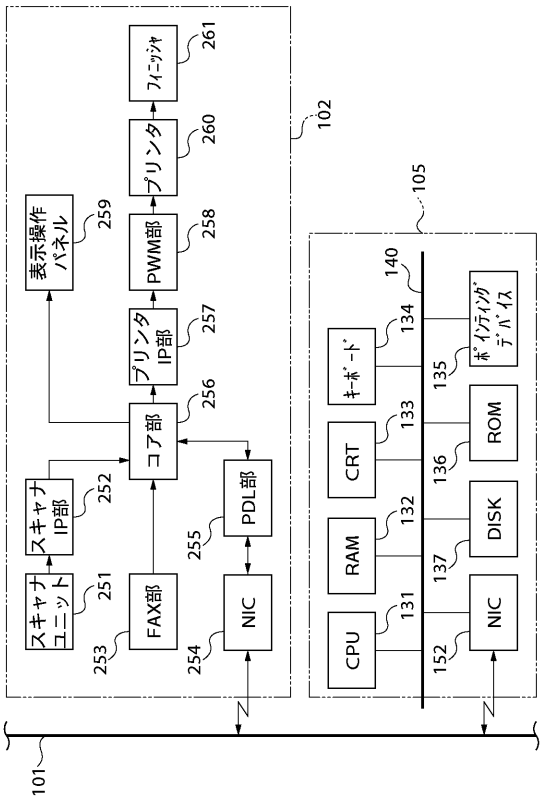
【図１】


102
画像処理装置
103
情報処理装置
101
ネットワーク
104
時刻認証サーバ
105
保存サーバ

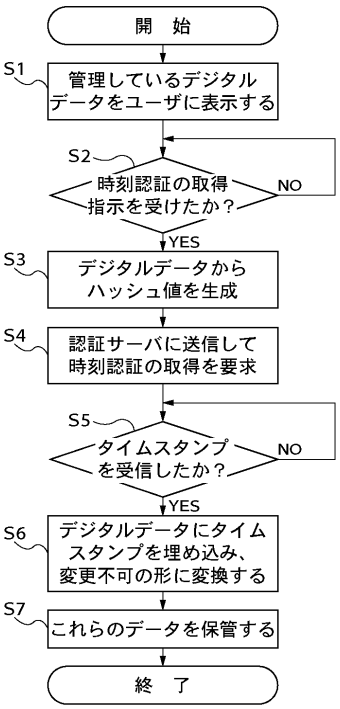
【図２】


105
保存サーバ
155
タイムスタンプデータ処理部
157
要求判定処理部
154
時刻認証局処理部
158
データ管理処理部
内部バス
153
ハッシュ値生成部
151
ネットワークインタフェース
152
102
画像処理装置
103
情報処理装置
104
時刻認証サーバ
ネットワーク
101

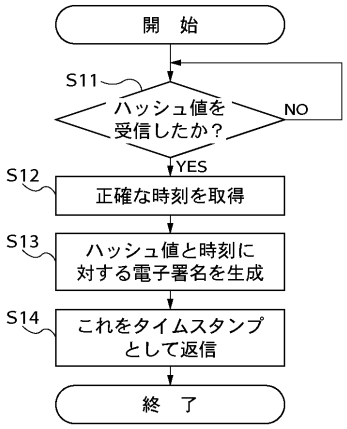
【図３】


102
261
フィニッシャ
260
プリンタ
259
表示操作パネル
258
PWM部
257
プリンタIP部
256
コア部
252
スキャナIP部
255
PDL部
251
スキャナユニット
253
FAX部
254
NIC
105
140
134
キーボード
135
ポインティングデバイス
133
CRT
136
ROM
132
RAM
137
DISK
131
CPU
152
NIC
101

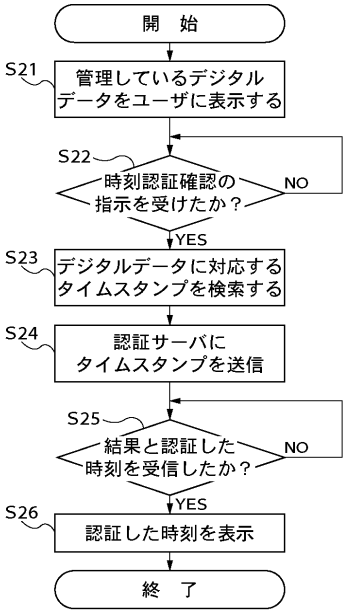
【図４】


開　始
S1
管理しているデジタルデータをユーザに表示する
S2
時刻認証の取得指示を受けたか？
NO
YES
S3
デジタルデータからハッシュ値を生成
S4
認証サーバに送信して時刻認証の取得を要求
S5
タイムスタンプを受信したか？
NO
YES
S6
デジタルデータにタイムスタンプを埋め込み、変更不可の形に変換する
S7
これらのデータを保管する
終　了

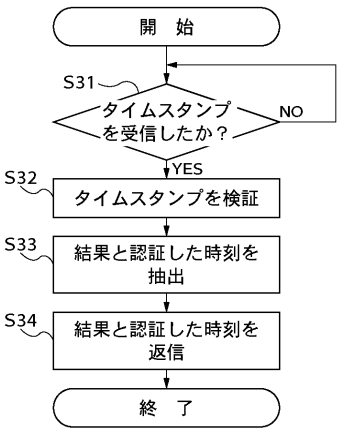
【図５】


開　始
S11
ハッシュ値を
受信したか？
NO
YES
S12
正確な時刻を取得
S13
ハッシュ値と時刻に
対する電子署名を生成
S14
これをタイムスタンプ
として返信
終　了

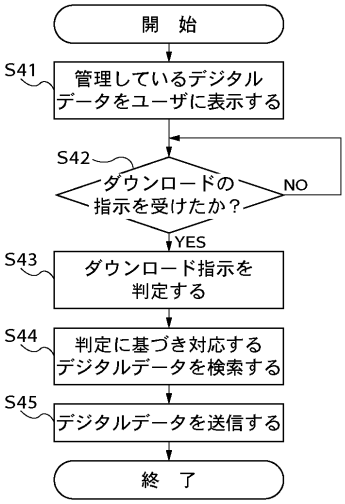
【図６】


開　始
S21
管理しているデジタル
データをユーザに表示する
S22
時刻認証確認の
指示を受けたか？
NO
YES
S23
デジタルデータに対応する
タイムスタンプを検索する
S24
認証サーバに
タイムスタンプを送信
S25
結果と認証した
時刻を受信したか？
NO
YES
S26
認証した時刻を表示
終　了

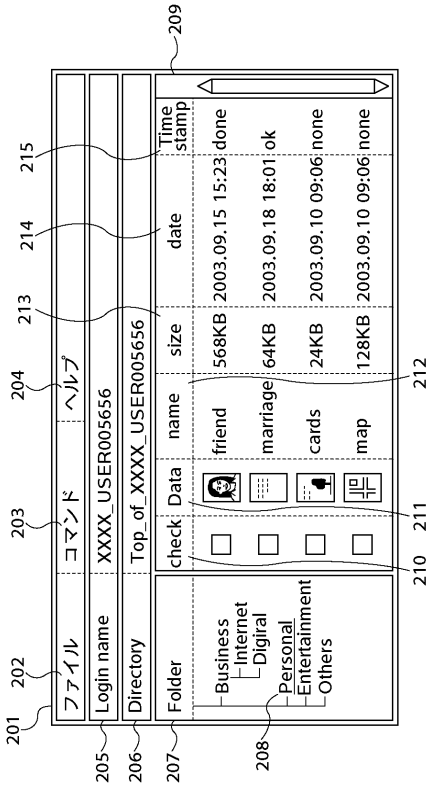
【図７】


開　始
S31
タイムスタンプ
を受信したか？
NO
YES
S32
タイムスタンプを検証
S33
結果と認証した時刻を
抽出
S34
結果と認証した時刻を
返信
終　了

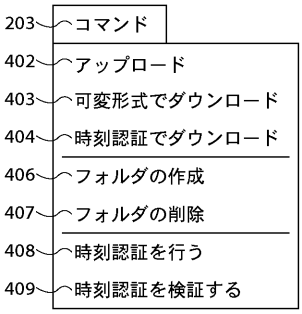
【図８】


開　始
S41
管理しているデジタル
データをユーザに表示する
S42
ダウンロードの
指示を受けたか？
NO
YES
S43
ダウンロード指示を
判定する
S44
判定に基づき対応する
デジタルデータを検索する
S45
デジタルデータを送信する
終　了

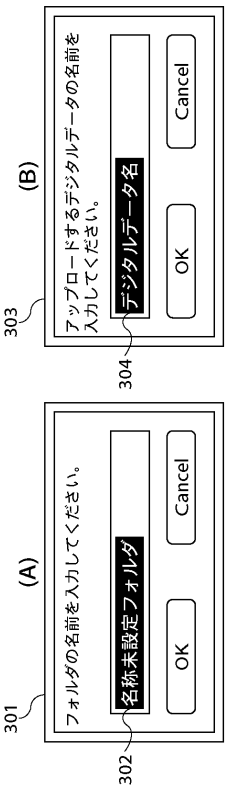
【図９】



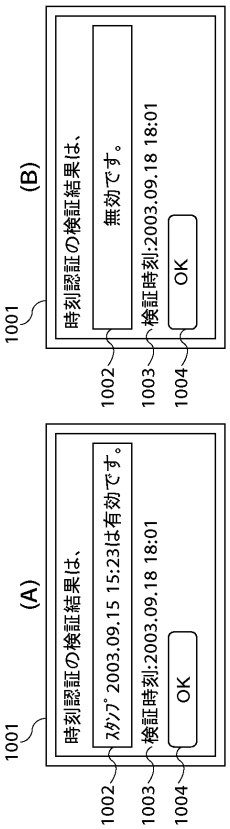
【図１０】



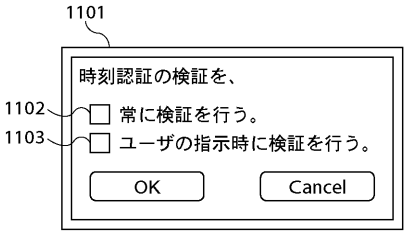
【図１１】



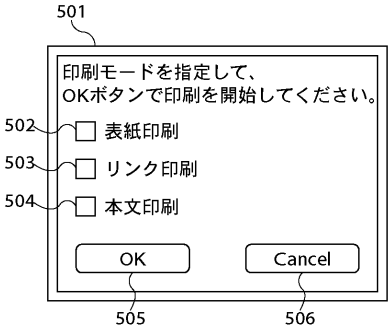
【図１２】



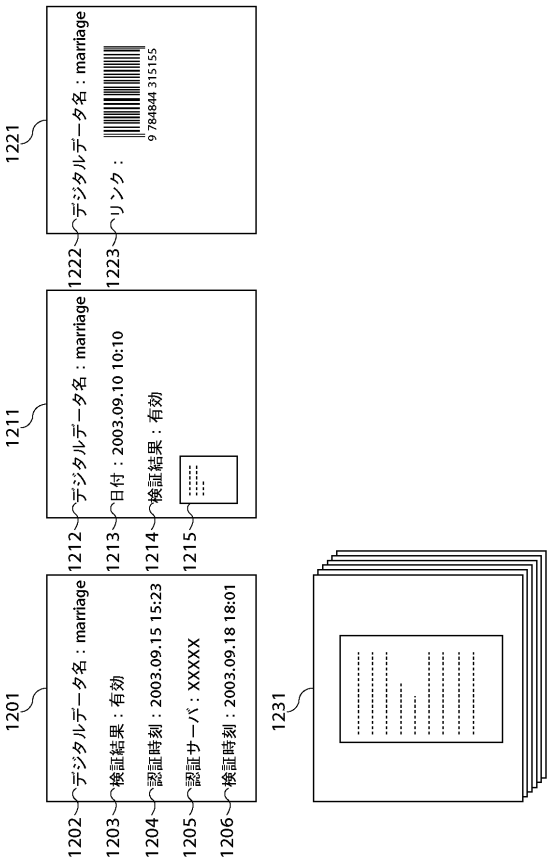
【図１３】


1101
時刻認証の検証を、
1102
常に検証を行う。
1103
ユーザの指示時に検証を行う。
OK
Cancel

【図１４】


501
印刷モードを指定して、
OKボタンで印刷を開始してください。
502
表紙印刷
503
リンク印刷
504
本文印刷
OK
Cancel
505
506

【図１５】


1221
デジタルデータ名：marriage
9 784844 315155
リンク：
1222
1223
1211
デジタルデータ名：marriage
日付：2003.09.10 10:10
検証結果：有効
1212
1213
1214
1215
1201
デジタルデータ名：marriage
検証結果：有効
認証時刻：2003.09.15 15:23
認証サーバ：XXXXX
検証時刻：2003.09.18 18:01
1202
1203
1204
1205
1206
1231