(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5771822号
(P5771822)
(45)発行日　平成27年9月2日(2015.9.2)　(24)登録日　平成27年7月10日(2015.7.10)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675D
H04L 9/00 675Z

請求項の数 2　(全 33 頁)

(21)出願番号　特願2010-277346(P2010-277346)
(22)出願日　平成22年12月13日(2010.12.13)
(65)公開番号　特開2012-34329(P2012-34329A)
(43)公開日　平成24年2月16日(2012.2.16)
審査請求日　平成25年12月13日(2013.12.13)
(31)優先権主張番号　特願2010-94841(P2010-94841)
(32)優先日　平成22年4月16日(2010.4.16)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2010-148292(P2010-148292)
(32)優先日　平成22年6月29日(2010.6.29)
(33)優先権主張国　日本国(JP)

(73)特許権者　500481732
株式会社メキキ
東京都渋谷区渋谷１－１７－８
(74)代理人　100103872
弁理士　柏川　敏夫
(72)発明者　出口　光
東京都渋谷区渋谷１－１７－８　松岡渋谷ビル３Ｆ

審査官　打出　義尚

最終頁に続く

(54)【発明の名称】デジタルデータ内容証明システム

(57)【特許請求の範囲】
【請求項１】
ユーザ端末から送信されたデジタルデータからなる原本データを受信して証明を行うデータ証明装置と、
前記データ証明装置によって作成された中間ファイルに対して、ハッシュ値及び日時情報を包含する日時保証情報を付与するタイムスタンプ付与装置と、
を有してなるデジタルデータの内容証明システムであって、
前記データ証明装置は、
ユーザの個人情報をユーザ識別情報と対応づけて格納するユーザ情報記憶手段と、
前記ユーザ端末からユーザ識別情報とともに送信された原本データを受信する原本データ受付手段と、
内容証明日時とユーザ名を含む証明事項を記載する第１のエリアと、任意のファイルを添付する第２のエリアと、日時保証情報を添付する第３のエリアを備えたフォーマットを有するファイルを作成し、原本データ名と、前記ユーザ情報記憶手段からユーザ識別情報に基づいて抽出したユーザ名と、内容証明日時とを少なくとも含む証明事項を前記第１のエリアに記載するとともに、前記第２のエリアに前記受信した状態から変更がない原本データを複製可能な状態で添付して中間ファイルを作成する中間ファイル作成手段と、
前記中間ファイルを前記タイムスタンプ付与装置に送信するタイムスタンプ要求手段と、
前記タイムスタンプ付与装置から前記中間ファイルのハッシュ値及び日時情報を包含する日時保証情報を受信する日時保証情報取得手段と、

受信した日時保証情報を前記中間ファイルの第３のエリアに添付することで証明済ファイルを作成する証明済ファイル作成手段と、
この証明済ファイルを前記ユーザ端末に送信する証明済ファイル送信手段と、を有し、
前記タイムスタンプ付与装置は、
前記データ証明装置から受信した中間ファイルから所定のハッシュ関数に基づいて算出したハッシュ値と、日時情報とを包含する日時保証情報を生成する生成手段と、
前記生成した日時保証情報を、前記データ証明装置に送信する通信手段と、を有してなる、ことを特徴とする
デジタルデータの内容証明システム。
【請求項２】
前記タイムスタンプ要求手段は、前記中間ファイルのハッシュ値を算出して該ハッシュ値を前記タイムスタンプ付与装置に送信し、
前記生成手段は、前記データ証明装置から受信したハッシュ値と、日時情報とを包含する日時保証情報を生成する、
請求項１記載のデジタルデータの内容証明システム。
【発明の詳細な説明】
【技術分野】
【０００１】
顧客のデジタルデータの内容を証明するために、先ず所定の事項を記したファイルを作成して、これに前記原本であるデジタルデータもしくはそのハッシュ値を添付させ、更に日時保証情報を添付することによって最終的な内容証明とするデジタルデータ内容証明システムに関するものである。
【背景技術】
【０００２】
紙媒体がある時点で存在していたことを客観的に証明するために公証役場の確定日付を利用することが行われる。これは、紙媒体の持ち主が存在を主張しても、本人の主張では信頼性に欠けるので、やはり第三者機関の介在が必要になってくるからである。
ところで、昨今は、各種書類をパソコンなどの情報処理装置で作成することが多くなり、作成されたデジタルデータの作成時期と内容を第三者によって証明してもらおうとする需要は増加の一途を辿っている。このような現状のもと、特許文献１には電子公証サービスを実現するための技術が開示されている。
特許文献１の項目〔００２８〕では、公証サービスを希望する電子データ（１３０）に対して、公証サービス享受者のデジタル署名（１３１）と付加情報（１３２）を加え、これに公証センターの承認者のデジタル署名（１３３）を加え一体となった状態のデータを公証済電子データ（１４１）とする。このように、原本である電子データ（１３０）はデジタル署名（１３１）等が加えられることにより、元の電子データとは同一ではなくなっている。証明が必要とされているのは変更前の元データであるので、証明のために変更せざるを得ないのでは本末転倒である。また、付加情報（１３２）には、日付や承認者、承認内容等が含まれており、電子データ（１３０）の証明書の役割をなすものであるが、本来証明書というものは、それが証明する対象とは相互に独立のはずであり、対象となるデータに付加されるものではない。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００２－４９５９０号公報（項目〔００１６〕〔００２８〕、図６など）
【発明の概要】
【発明が解決しようとする課題】
【０００４】
紙媒体への刻印による証明法の特徴は、原本データ部分と証明書部分とが独立であり、

かつ両者の改変は不可能であり、かつ両者の対応に疑義が生じる余地はない、という点にある。本発明は、原本がデジタルデータの場合にも、このような証明法を実現することを目的とする。
以下、証明対象となるデジタルデータを「原本データ」という。
【課題を解決するための手段】
【０００５】
上記の目的を達成するために、本発明は、
ユーザ端末から送信されたデジタルデータからなる原本データ若しくは原本データのハッシュ値を受信して証明を行うデータ証明装置と、前記データ証明装置によって作成された中間ファイルに対して、ハッシュ値及び日時情報を包含する日時保証情報を付与するタイムスタンプ付与装置と、を有してなるデジタルデータの内容証明システムであって、請求項１～４に係る４つの態様がある。
【０００６】
請求項１に係る発明では、
前記データ証明装置は、
ユーザ情報記憶手段と、原本データ受付手段と、中間ファイル作成手段と、タイムスタンプ要求手段と、日時保証情報取得手段と、証明済ファイル作成手段と、証明済ファイル送信手段と、を有することを特徴とする。
ユーザ情報記憶手段は、ユーザの個人情報（ユーザ名、メールアドレス、所属などの属性情報）をユーザ識別情報と対応づけて格納する。
原本データ受付手段は、ユーザ端末からユーザ識別情報とともに送信された原本データを受信する。
中間ファイル作成手段は、まず、原本データ名と原本データの受信日時ユーザ名を含む証明事項を記載する第１のエリアと、任意のファイルを添付する第２のエリアと、日時保証情報を添付する第３のエリアを備えたフォーマットを有するファイルを作成する。次に、原本データ名と、ユーザ情報記憶手段からユーザ識別情報に基づいて抽出したユーザ名と、原本データの受信日時とを少なくとも含む証明事項を第１のエリアに記載するとともに、第２のエリアに前記受信した状態から変更がない原本データを複製可能な状態で添付して中間ファイルを作成する。
タイムスタンプ要求手段は、中間ファイルをタイムスタンプ付与装置に送信する。あるいは中間ファイルの代りに、中間ファイルのハッシュ値を算出して該ハッシュ値を送信してもよい。ハッシュ値を送信するようにすれば、中間ファイルのサイズが大きい場合でも遅滞なく処理することが出来る。
日時保証情報取得手段は、タイムスタンプ付与装置から中間ファイルのハッシュ値及び日時情報を包含する日時保証情報を受信する。
証明済ファイル作成手段は、受信した日時保証情報を中間ファイルの第３のエリアに添付することで証明済ファイルを作成する。
証明済ファイル送信手段は、この証明済ファイルをユーザ端末に送信する。
前記タイムスタンプ付与装置は、
前記データ証明装置から受信したハッシュ値或いは受信した中間ファイルから所定のハッシュ関数に基づいて算出したハッシュ値と、日時情報とを包含する日時保証情報を生成する生成手段と、
前記生成した日時保証情報を、前記データ証明装置に送信する通信手段と、を有してなる。
【０００７】
「中間ファイル」は、証明事項が記載された、タイムスタンプ付与装置に送信することを目的に作成される一時的なファイルである。
中間ファイルに原本データが添付された場合、この原本データには一切変更がない。このことは、内容証明を目的とするシステムにとっては本質的なことである。また、１ファイルに添付される原本データは複数あってもよい。従って例えば、表計算ソフトで作成した

データ、ワープロソフトで作成したデータ、描画ソフトで作成したデータなどを１のファイルに添付できる。これにより利便性は格段に増す。
「証明済ファイル」は、「中間ファイル」に日時保証情報を添付したファイルであって、後日必要になる場合に備えて、通常はユーザ端末側で保存される。
なお、中間ファイルおよび証明済ファイルのフォーマットとして現時点（出願時である２０１０年）ではＰＤＦ（Portable Document Format）を念頭においている。ＰＤＦ文書には、ファイルを添付できる機能（http://www.adobe.com/jp/designcenter/acrobat/articles/acr7sdreaderattach.html参照）があり、この機能を利用して原本データを添付する。また、ＰＤＦ文書に複数人が複数回の署名ができる機能（http://help.adobe.com/ja_JP/Reader/8.0/help.html?content=WS58a04a822e3e50102bd615109794195ff-7d48.html）があるので、この署名フィールドを日時保証情報の書き込みのために使用することにする。
「日時保証情報を添付」とは、署名フィールドに日時保証情報を書き込むことをいうものとする。
「日時情報」とは、原本データについての内容証明の要求が受け付けられた等の日時を示す情報である。
「日時保証情報」には、日時情報とハッシュ値が含まれ、他に必要に応じて付加情報も含まれる。日時保証情報に含まれる日時情報によって原本データの存在していた時期が証明でき、又ハッシュ値によって少なくともこの時期以降は原本データ及び該原本データに関する証明事項が改ざんされていないことが証明できる。
【０００８】
ところで、データ証明装置が作成する中間ファイルおよび証明済ファイルはＰＤＦのような一体管理型のフォーマットを利用したファイルであり、証明すべき原本を封入し、表側に証明事項が記載されている封筒に例えることができる。封筒の内部に入れられた原本は一切変更がない。証明済ファイルは、この原本入り封筒に公証人の印が押されていることに例えられる。この押印は、封筒内の原本と封筒の表面の証明事項の双方を同時に証明する役割を果たしているが、本発明の日時保証情報も、原本データと証明事項とを同時に証明するものである。
タイムスタンプ付与装置は、原本データ自体ではなく中間ファイルのハッシュ値を算出する。これにより、原本データと証明事項との改ざんの有無を同時に証明することが可能となる。
もし、原本データと証明事項の改ざんの有無が別々に証明されるとするならば、原本データと証明事項との関連性を別途証明しなくてはならない。しかし本発明では、両者の対応に疑義が生じる余地はない。
【０００９】
請求項２に係る発明のデータ証明装置は、
ユーザ端末から原本データ自体の代わりに原本データのハッシュ値が送信され、
中間ファイルには原本データの代りに原本データのハッシュ値が添付される点で、請求項１に係る発明と相違する。
　データ証明装置に対して原本データを送信する場合、送信データのセキュリティや大ファイル送信時のサーバや通信の負荷に配慮しなくてはならないが、ハッシュ値であれば安心して送信できる。
【００１０】
請求項３に係る発明のデータ証明装置は、
ユーザ端末から原本データ自体の代わりに原本データのハッシュ値が送信され、
中間ファイルには原本データの代りに原本データのハッシュ値が添付される点で、請求項２に係る発明と共通するが、
タイムスタンプ付与装置には原本データのハッシュ値を送信して、このハッシュ値及び日時情報を包含する日時保証情報を受信する点で請求項２と相違する。
　請求項１および２に係る発明では、原本データと証明事項の両者に対して同時に内容証明を受けることができるのに対して、請求項３に係る発明では、原本データ（正確にはハ

ッシュ値）に対してのみ内容証明が受けられる。
【００１１】
請求項４に係る発明のデータ証明装置は、
ユーザ端末から原本データ自体の代わりに原本データのハッシュ値が送信される点で請求項２および３に係る発明と共通する。しかし、証明事項は記載されているが原本データに関する情報（原本データ自体或いはハッシュ値）を添付していない中間ファイル或いは中間ファイルのハッシュ値をタイムスタンプ付与装置に送信して、中間ファイルのハッシュ値及び日時情報を包含する日時保証情報を受信する点、及び中間ファイルに日時保証情報と原本データのハッシュ値を添付して証明済ファイルを作成する点で請求項２あるいは３と相違する。
このように請求項４に係る発明では、証明事項に対してのみ内容証明が受けられる。
ユーザによっては、原本データのみ、あるいは証明事項にのみ内容証明を受けることを希望することも考えられるので、請求項３および４はこのようなニーズに応えるものである。
【００１２】
請求項５に係る発明は、請求項１～４のいずれか１に係る発明において、
中間ファイルに日時保証情報を添付する代りに、中間ファイルと同様のフォーマットを有するファイルを新規に作成し、この作成されたファイルには中間ファイルと日時保証情報を添付することで証明済ファイルを作成することを特徴とする。つまり、原本データと証明事項とを封入した封筒をさらに別の封筒に封入し、この別の封筒にタイムスタンプを押すことにたとえることができる。
【００１３】
請求項６に係る発明は、請求項１～４のいずれか１に係る発明において、
中間ファイルに日時保証情報を添付する代りに、受信した日時保証情報を格納する日時保証情報ファイルを作成し、
証明済ファイル送信手段は、中間ファイルを証明済ファイルとして送信するとともに、日時保証情報ファイルも送信することを特徴とする。
【００１４】
請求項７に係る発明は、請求項１～６のいずれか１に係る発明において、
ユーザ情報記憶手段には、本人確認書類（運転免許証、パスポート、住基カード、健康保険証等の本人であることを確認しうる書類）の画像データあるいは記載事項も格納し、証明済ファイルに記載される証明事項には、前記本人確認書類の画像データあるいは記載事項も含まれることを特徴とする。
【００１５】
請求項８に係る発明は、請求項１～７のいずれか１に係る発明において、
前記デジタルデータからなる原本データは原本作成者端末から前記ユーザ端末へ送信されたものであり、前記ユーザ端末は前記データ証明装置から受信した前記証明済ファイルを前記原本作成者端末に送信することを特徴とする。
　これにより、契約のように関与する人間が複数であっても、デジタルデータである原本の内容証明を本発明のシステムで行うことができる。
【００１６】
請求項９に係る発明は、請求項１～７のいずれか１に係る発明において、
前記原本データは、紙媒体の書類をスキャナで画像として読み取ったデジタルデータであることを特徴とする。
　これにより、請求書や領収証などの紙で取り交わされることが多い書類も、本発明のシステムによる証明の対象となる。
請求項１０に係る発明は、請求項９に係る発明において、
前記ユーザ端末は、前記原本データとともに、前記紙媒体の書類に記載されている事項を送信し、この送信された事項は、前記第１のエリアに記載されることを特徴とする。
　紙媒体の書類には日付や金額などが手書きされ、伝票番号などスタンプが押されている

ことが多い。これらの手書き文字などをユーザ端末からデータ証明装置に送信するならば、本発明の証明済ファイルの第１のエリアに、証明事項として記載することが可能となる。

【００１７】

請求項１１に係る発明は、請求項１～１０のいずれか１に係る発明において、
前記データ証明装置は、
前記データ証明装置の運営主体と、前記ユーザと、承認業務を行う第三者のいずれかが有する電子証明書に関する情報を記憶する電子証明書記憶手段と、
電子署名を生成する電子署名生成手段とを、さらに有するとともに、
前記中間ファイル作成手段が作成するファイルのフォーマットには電子署名を添付するための電子署名エリアがさらに備えられ、
前記証明済ファイル作成手段は、受信した日時保証情報を中間ファイルの第３のエリアに添付するとともに、電子署名エリアに電子署名を添付して証明済ファイルを作成することを特徴とする。
このように、内容証明の対象となる電子データには日時保証情報（いわゆるタイムスタンプに相当）に電子署名も付加されるので、一層の客観性が確保される。

【００１８】

上記のデータ証明装置の機能は、ユーザ端末に持たせてもよい。
請求項１２に係る発明は、ユーザ端末にデータ証明装置の機能を担わせるためのコンピュータプログラムである。
このコンピュータプログラムをインストールすることにより、ユーザ端末は、中間ファイル作成手段と、タイムスタンプ要求手段と、日時保証情報取得手段と、証明済ファイル作成手段と、を有することになる。ただし、請求項１に係る発明等のような原本データ受付手段、証明済ファイル送信手段は必要としていない。なぜなら、原本データは通常ユーザ端末に備えられている記憶手段に格納されており、証明済ファイルはこの記憶手段に格納されるからである。いわば、個々のユーザ専用のデータ証明装置であり、そのための利便性を重視したものである。

【００１９】

請求項１３～１７に係る発明は、原本証明装置の機能も兼ね備えたユーザ端末が、タイムスタンプ付与装置と、データ証明管理装置と接続して構成されることを特徴とするシステムである。
証明対象である原本データの持ち主であるユーザが自分の端末で証明済ファイルを作成するのであれば、第三者的な立場にあるデータ証明装置が証明済ファイルを作成する場合と比べ、客観性が疑問視されないとも限らない。
そこで、データ証明管理装置に、ユーザ端末から送信されるユーザアカウントおよびパスワードが登録されていることをもって正当なユーザか否かを判定するユーザ認証手段と、正当なユーザと判定されたユーザ端末から原本データあるいは中間ファイルを受信後、該ユーザ端末に電子証明書を送信する電子証明書配送手段とを備えさせることとした。

【００２０】

請求項１８に係る発明は、紙媒体の帳簿関係書類を読み取りデジタル画像データ化する画像読取手段を備えたユーザ端末と、
前記デジタル画像データが貼り付けられた中間ファイルにハッシュ値及び日時情報を包含する日時保証情報と、電子署名とを付与して証明済ファイルを作成するとともに、前記デジタル画像データに含まれる文字情報データと前記証明済ファイルとを対応づけて記憶手段に格納するタイムスタンプ付与装置と、
前記ユーザ端末から受信したデジタル画像データが貼り付けられた中間ファイルを作成して、前記ユーザ端末に送信するデータ証明装置とを有してなり、
前記ユーザ端末が前記タイムスタンプ付与装置に対して中間ファイルを送信し証明済ファイルの作成を依頼するシステムである。
これにより、紙媒体の帳票類を画像データ化してタイムスタンプと電子署名とにより証

明を受けることができる。証明済のファイルおよび文字情報データはタイムスタンプ付与装置側で保存し管理されるのでデータ証明装置の負担が軽減される。

なお、ユーザ端末が「画像読取手段を備えた」とは、外部の画像読取装置と接続し、読み取った画像を取得できる場合も含む意味である。また、ユーザ端末から送信される中間ファイルに文字情報データが含まれていないときは、中間ファイルと文字情報データがそれぞれタイムスタンプ付与装置に送信される。

【発明の効果】

【００２１】

原本データとその証明事項と日時保証情報（タイムスタンプ、原本データ及び該原本データに関する証明事項のハッシュ値を含む）とが一体化されているので、証明対象の原本データと証明事項とを同時に検証できる。さらに、次の点でユーザへの利便性が高い。第１に、原本データそのものでなく原本データのハッシュ値のみをデータ証明装置に送ってもよい。第２に、必要であれば、原本データのみ或いは証明事項のみにタイムスタンプを受けることも可能である。第３に、データ証明装置にユーザ登録をしておくならば、原本データの送信の都度ユーザ個人情報を送信しなくても必要な証明事項が記載された証明済ファイルを得ることができる。第４に、必要であれば、証明済ファイルには第三者即ち利害関係を有しない人間若しくは団体の電子署名も付与されるので、証明書としての客観性が増す。第５に、手書きの領収書やメモ書きなどの紙の書類も、スキャナを利用してデジタルデータ化することにより、原本データとして扱われて証明の対象となる。第６に、原本データの所有主の端末に、証明済ファイルを作成するコンピュータプログラムをインストールすることにより、外部の装置との通信を減らすことができる。

【図面の簡単な説明】

【００２２】

【図１】第１の実施形態のシステムのシステム構成例を示す図である。

【図２】第１の実施形態のシステムのデータ証明装置の機能ブロック例を示す図である。

【図３】第１の実施形態のシステムの処理概要を説明するフロー図である。

【図４】第１の実施形態のシステムの中間ファイルおよび証明済ファイルの構成を示す図である。

【図５】第１の実施形態のシステムにおいて、証明済ファイルが作成される手順を説明する図である。

【図６】第１の実施形態の変形例の証明済ファイルの構成を示す図である。

【図７】第２の実施形態のシステムの処理概要を説明するフロー図である。

【図８】第２の実施形態のシステムの中間ファイルおよび証明済ファイルの構成を示す図である。

【図９】第３の実施形態のシステムの処理概要を説明するフロー図である。

【図１０】第４の実施形態のシステムの処理概要を説明するフロー図である。

【図１１】第４の実施形態のシステムの中間ファイルおよび証明済ファイルの構成を示す図である。

【図１２】第６の実施形態のシステムのシステム構成例を示す図である。

【図１３】第６の実施形態のシステムの処理概要を説明するフロー図である。

【図１４】第７の実施形態のシステムのデータ証明装置の機能ブロック例を示す図である。

【図１５】第７の実施形態のシステムの処理概要を説明するフロー図である。

【図１６】第７の実施形態のシステムの中間ファイルおよび証明済ファイルの構成を示す図である。

【図１７】第８の実施形態のシステムのシステム構成例を示す図である。

【図１８】第８の実施形態のシステムのデータ証明装置の機能ブロック例を示す図である。

【図１９】第８の実施形態のシステムの処理概要を説明するフロー図である。

【図２０】第８の実施形態のシステムの中間ファイルおよび証明済ファイルの構成を示す

図である。
【図２１】第９の実施形態のシステムのシステム構成、ユーザ端末及びデータ証明管理装置の機能ブロック例を示す図である。
【図２２】第９の実施形態のシステムの処理概要を説明するフロー図である。
【図２３】第１０の実施形態の処理概要を説明するフロー図である。
【図２４】第１０の実施形態の願書記載項目入力画面を例示する図である。
【図２５】第１０の実施形態のファイル選択画面を例示する図である。
【図２６】第１１の実施形態のシステムのシステム構成例および装置の機能ブロック例を示す図である。
【図２７】第１１の実施形態のシステムの中間ファイルおよび証明済ファイルの構成を示す図である。
【図２８】第１１の実施形態のシステムの処理概要を説明するフロー図である。
【発明を実施するための形態】
【００２３】
《第１の実施形態》
この実施形態のシステム構成例を図１に示す。
インターネットＮを介して、データ証明装置１がユーザ端末２及びタイムスタンプ付与装置３と接続している。
【００２４】
ユーザ端末２は、この実施形態のシステムを利用してデジタルデータ（原本データ）について内容証明を受けようとするユーザが利用するものであり、インターネット接続機能があれば携帯電話でもＰＤＡでもよい。ただし、原本データの作成や更新を行うことが想定されるので、画像処理用プログラムや文書作成用プログラムがインストールされているパソコンが望ましい。ユーザ端末２は、図１には１台しかないが、台数に制限はない。
【００２５】
タイムスタンプ付与装置３は、データ証明装置１からの要求に対して日時保証情報を生成し、これをデータ証明装置１に返信する情報処理装置である。この実施形態のシステムでは、タイムスタンプ付与サービスを提供している既存の業者がいれば、その業者のサービスを利用するので、タイムスタンプ付与装置３はその業者がサービス提供にあたり利用する情報処理装置である。タイムスタンプ付与装置３は、データ証明装置１から中間ファイルを受信し、この中間ファイルから所定のハッシュ関数に基づいて算出したハッシュ値と、日時情報とを包含する日時保証情報を生成する生成手段と、生成した日時保証情報を、データ証明装置１に送信する通信手段を備えている。
【００２６】
データ証明装置１は、先ず証明対象の原本データを添付し、証明事項を記載した中間ファイルを作成し、この中間ファイルのハッシュ値を含む日時保証情報を添付して証明済ファイルを作成する情報処理装置である。図１では、１台しか記載がないが、１台でその処理を実行するとは限らず、複数の情報処理装置が連携してその処理を実行してもよい。
【００２７】
次に、図２のブロック図に従い、データ証明装置１の構成を説明する。
データ証明装置１は、記憶部４、処理部５を含む。
記憶部４は、ユーザ情報記憶手段６を含む。また、記憶部４は、コンピュータをデータ証明装置１として機能させるためのコンピュータプログラムや、処理の経過に伴う作業用データ、パラメータ類、Ｗｅｂデータなどを記憶する。このシステムを利用できるのは登録しているユーザに限る場合などは、登録ユーザの個人情報なども適宜記憶するものとする。
ユーザ情報記憶手段６には、データ証明装置１による内容証明サービスを受けようとするユーザが予めデータ証明装置１に送信した個人情報を、ユーザ管理や課金処理などのために登録する。登録される情報として、ユーザ名、ユーザの所属する会社や団体名、メールアドレス、住所などがある。

【００２８】
処理部５は、ユーザ情報管理手段７と、原本データ受付手段８と、中間ファイル作成手段９と、タイムスタンプ要求手段１０と、日時保証情報取得手段１１と、証明済ファイル作成手段１２と、証明済ファイル送信手段１３と、その他の処理手段を含む。
ただし、これらの各手段の分類は、あくまで説明の便宜上にすぎない。各手段は、その機能に応じて、ハードウェア、ソフトウェアで実装される。ソフトウェアによる場合は、ＲＯＭやハードディスクなどの記憶手段に格納されているコンピュータプログラムを、ＣＰＵが実行する。これらは、公知の事柄であるので説明を省略する。
また、データ証明装置１は、キーボードやディスプレイ等の入出力手段及びドライバ類、通信ネットワークを介したユーザ端末２やタイムスタンプ付与装置３との通信を可能とする通信インターフェース部１４も備える。
【００２９】
ユーザ情報管理手段７は、ユーザ端末２からユーザ名などの個人情報を受信してユーザ情報記憶手段６に格納したり更新したりするとともに、ユーザから内容証明の要求が送られてきたときに、ユーザ情報記憶手段６から当該ユーザに関する情報を取り出す。
原本データ受付手段８は、証明対象の１以上任意個数の原本データをユーザ端末２から受信する。
中間ファイル作成手段９は、先ずＰＤＦなどの一体管理型フォーマットのファイルを作成する。次にこのファイルに受信した原本データを変更することなくそのまま添付するとともに、証明事項を記載して中間ファイルを作成する。証明事項の記載はファイルの受信日時（タイムスタンプ付与装置３から日時保証情報を取得した日時すなわち内容証明日時と同じとみなして差し支えない）やファイル名などの必要と考えられる項目があれば、書式はどのようなものでもよい。
タイムスタンプ要求手段１０は、中間ファイルをタイムスタンプ付与装置３に送信する。
日時保証情報取得手段１１は、タイムスタンプ付与装置３から日時保証情報を受信する。
証明済ファイル作成手段１２は、受信した日時保証情報を中間ファイルに添付して証明済ファイルを作成する。
　証明済ファイル送信手段１３は、作成された証明済ファイルをユーザ端末２に送信する。
【００３０】
次に、図３を参照しながら、この実施形態のシステムの動作について詳しく説明する。
　原本データ受付手段８は、インターネットＮおよびインターフェース部１４を介してユーザ端末２から、原本データＤを受信する（ステップＳ１）。ここでユーザ識別情報も受信する。
【００３１】
中間ファイル作成手段９は、ＰＤＦファイルＦ１を作成する。ファイルＦ１は図４に示すように、第１のエリアＡ１、第２のエリアＡ２、第３のエリアＡ３を有する。第１のエリアＡ１には、原本データ名、原本データＤの受信日時などの証明事項Ｂが記載される。また、証明事項には、ユーザ情報記憶手段６からユーザ識別情報に基づいて抽出したユーザ名、メールアドレス、所属なども含まれる。
さらにファイルＦ１の第２のエリアＡ２に原本データＤを添付して中間ファイルＦ２を作成する（ステップＳ２）。
【００３２】
タイムスタンプ要求手段１０は、中間ファイルＦ２をタイムスタンプ付与装置３に送信する（ステップＳ３）。データ証明装置１は、予めタイムスタンプ付与装置３の提供するサービスを受けるために登録などの所定の手続きをしているものとする。なお、データ証明装置１は、タイムスタンプ付与装置３から見れば複数いるユーザの中の１ユーザであるから、両者の間には何らかの認証手段が確立されていなければならない。
【００３３】
　タイムスタンプ付与装置３は、受信した中間ファイルＦ２に付与する日時保証情報Ｃを

生成する（ステップＳ４）。図５に示すように、タイムスタンプ付与装置３は、所定のハッシュ関数に受信した中間ファイルＦ２を入力してハッシュ値Ｆｈを算出する。ここで、特徴的なのは、原本データＤのハッシュ値Ｄｈではなく、原本データＤおよび証明事項Ｂの両者を有する中間ファイルＦ２のハッシュ値Ｆｈを算出する点である。これにより、原本データＤと証明事項Ｂに対して同時に一の証明印を押すも同然となる。
あわせて、タイムスタンプ付与装置３は、所定の時刻認証局にタイムスタンプＴＳの発行を要求する。このタイムスタンプＴＳは中間ファイルＦ２を受信した時刻などに対応する。この実施形態のシステムのタイムスタンプＴＳは、請求項１にいう「日時情報」に相当し、これにハッシュ値Ｆｈと、その他付加情報を含めて日時保証情報Ｃを生成する。その他付加情報には、ハッシュ値Ｆｈのほかに時刻認証局やタイムスタンプ付与装置３などの証明書類（ＰＫＩの電子証明書も含む）も含まれ得る。なお、日時保証情報Ｃにはタイムスタンプ ＴＳとハッシュ値Ｆｈが最小限含まれていればよく、その他付加情報は必須ではないから、利便性等を考慮して決定すればよい。
ところで、日時保証情報は、タイムスタンプ付与装置３の暗号鍵によって暗号化されていることが望ましい。つまり、公開鍵方式も導入してセキュリティの強化を図るわけである。

【００３４】
タイムスタンプ付与装置３が日時保証情報Ｃを送信してくる（ステップＳ５）ので、日時保証情報取得手段１１はこれを受信する。

【００３５】
証明済ファイル作成手段１２は、中間ファイルＦ２の第３のエリアＡ３に日時保証情報Ｃを添付し、証明済ファイルＦ３を作成する（ステップＳ６）。
　続いて、証明済ファイル送信手段１３は、作成された証明済ファイルＦ３をユーザ端末２に送信する（ステップＳ７）。

【００３６】
このファイルＦ２およびＦ３の形式は、本発明の出願時点ではＰＤＦ形式が最適である。ＰＤＦ形式のファイルには、署名フィールド（第３のエリアが相当）に書き込んだデータを変更したり削除したりすることはできないという特徴がある。したがって、日時保証情報Ｃが後から変更されていないと信頼することができる。
さらに、ファイルＦ２では、１以上任意個数の原本データを添付できる。しかも、個々の原本データを格納するファイル形式は限定しないので、例えば、ＷＯＲＤ（マイクロソフト社の製品名）のようなワープロソフトで作成されたファイルとＧＩＦ形式などの画像ファイルとをファイル形式を変更することなく同一のファイルＦ２に添付できる。原本データのファイル形式を変更しなくても証明済ファイルＦ３の作成ができる点も本発明の特徴のひとつである。
以上が、第１の実施形態の構成及び動作の説明である。

【００３７】
証明済ファイルＦ３を受け取ったユーザは、添付の原本データＤについての内容証明が必要になったとき、どのような方法で検証を受けるかは、複数の方法が考えられる。ここでは、一例を挙げるにとどめる。
データ証明装置１あるいはタイムスタンプ付与装置３は証明済ファイルＦ３を検証するソフトウェアを予め作成しておき、データ証明装置１からユーザ端末２に証明済ファイルＦ３を送付するとき等にこのソフトウェアも送付する。このソフトウェアは、次のような機能を備えている。
すなわち、証明済ファイルＦ３から日時保証情報Ｃを削除した後のファイル（中間ファイルＦ２）のハッシュ値を計算する機能、この算出したハッシュ値と日時保証情報から取り出したハッシュ値Ｆｈとを比較する機能、ハッシュ値同士の比較結果を出力する機能である。
日時保証情報Ｃがタイムスタンプ付与装置３の秘密鍵で暗号化されている場合は、このソフトウェアには公開鍵を定数として持たせ、この公開鍵で復号化してハッシュ値を取り出

すものとする。
以上のソフトウェアによってハッシュ値が一致したときは、証明済ファイルＦ３の証明事項Ｂも添付の原本データＤも改ざんされていないと判断できる。
このようにして、原本データＤは何時内容証明を受けたのか、つまり何時の時点で既に存在していたかということ、証明済ファイルＦ３に記載されている証明事項Ｂと添付の原本データＤとの対応に間違いがないことを証明できる。
【００３８】
この実施形態では、原本データＤの受信日時やデータ名などを記した証明事項Ｂが記載されるので、次のような利点がある。すなわち、日時保証情報Ｃは、証明済ファイルＦ３の署名フィールドに暗号化されて添付されていることが多い。この場合、証明済ファイルＦ３の所有者もただちに日時を知ることはできない。しかし、証明済ファイルＦ３内のエリアＡ１に平文でも記述されているので、そこを参照すれば直ちに分かる。つまり、この実施形態では安全性も利便性も満たされているのである。
【００３９】
上記の第１の実施形態にはいろいろな変形例が考えられるが、以下３つを紹介する。
第１に、データ証明装置１側で中間ファイルＦ２のハッシュ値Ｆｈを算出し、タイムスタンプ付与装置３には中間ファイルＦ２の代わりに、ハッシュ値Ｆｈを送信してもよい。
【００４０】
第２の変形例は、図６に示すようなものである。日時保証情報Ｃを中間ファイルＦ２に添付する代りに、新たなＰＤＦフォーマットのファイルＦｎを作成し、このファイルＦｎの第２のエリアＡｎ２に中間ファイルＦ２を添付し、第３のエリアＡｎ３に日時保証情報Ｃを添付し、これを証明済ファイルＦ３としてユーザ端末２に送信する。なお、ファイルＦｎの第１のエリアＡｎ１は空欄でかまわない。証明事項Ｂを参照したいときは、第２のエリアＡｎ２から中間ファイルＦ２を取り出し、このファイルＦ２の第１のエリアＡ１を参照すればよいからである。
【００４１】
第３に、日時保証情報ＣをＰＤＦフォーマットのファイルの署名フィールドに添付する変わりに、日時保証情報Ｃのみを別ファイル（請求項６の「日時保証情報ファイル」）に格納してユーザ端末２に送信してもよい。格納するファイルのフォーマットは何でもよい。同時に中間ファイルＦ２をそのまま証明済ファイルＦ３としてユーザ端末２に送信する。ユーザ端末２側では、送信されたファイルＦ３と日時保証情報ファイルとを同一のフォルダに格納するとよい。
【００４２】
上記の第２および第３の変形例は、下記の第２～第５の実施形態についても変形例となりうる。
【００４３】
《第２の実施形態》
第２の実施形態は、ユーザ端末２からは原本データＤではなく、原本データＤのハッシュ値Ｄｈが送信される点で第１の実施形態と相違する。
第三者的機関による内容証明を希望するが、インターネット等の通信回線を介して重要な原本データを送信することは避けたいという要望に応えたり、大ファイル送信時の障害を回避するためである。
以下、第１の実施形態との相違点を中心に、図２のブロック図および図７のフロー図を参照しながら説明する。
【００４４】
原本データ受付手段８は、インターネットＮおよびインターフェース部１４を介してユーザ端末２から、原本データＤのハッシュ値Ｄｈを受信する（ステップＳ１１）。ここでユーザ識別情報と原本データ名も受信する。
【００４５】
中間ファイル作成手段９は、ＰＤＦファイルＦ１を作成する。ファイルＦ１は図８に示

すように、第１のエリアＡ１、第２のエリアＡ２、第３のエリアＡ３および第４のエリアＡ４を有する。第１のエリアＡ１には、原本データ名、原本データＤのハッシュ値Ｄｈの受信日時などの証明事項Ｂを記載し、第４のエリアＡ４に原本データＤのハッシュ値Ｄｈを添付して中間ファイルＦ２を作成する（ステップＳ１２）。

【００４６】

タイムスタンプ要求手段１０は、中間ファイルＦ２をタイムスタンプ付与装置３に送信する（ステップＳ１３）。タイムスタンプ付与装置３は、受信した中間ファイルＦ２に付与する日時保証情報Ｃを生成する（ステップＳ１４）。タイムスタンプ付与装置３は、所定のハッシュ関数に受信した中間ファイルＦ２を入力してハッシュ値Ｆｈを算出する。ここで、特徴的なのは、原本データＤのハッシュ値Ｄｈではなく、原本データＤのハッシュ値Ｄｈおよび証明事項Ｂの両者を有する中間ファイルＦ２のハッシュ値Ｆｈを算出する点である。これにより、原本データＤのハッシュ値Ｄｈ（ひいては原本データＤそのもの）と証明事項Ｂに対して同時に一の証明印を押すも同然となる。

あわせて、タイムスタンプ付与装置３は、所定の時刻認証局にタイムスタンプＴＳの発行を要求し、このタイムスタンプＴＳにハッシュ値Ｆｈと、その他付加情報を含めて日時保証情報Ｃを生成する。

【００４７】

タイムスタンプ付与装置３が日時保証情報Ｃを送信してくる（ステップＳ１５）ので、日時保証情報取得手段１１はこれを受信する。証明済ファイル作成手段１２は、図８に示すように、中間ファイルＦ２の第３のエリアＡ３に日時保証情報Ｃを添付し、証明済ファイルＦ３を作成する（ステップＳ１６）。この証明済ファイルＦ３の第２のエリアＡ２に添付されるファイルはない。ユーザ端末２から原本データ自体は送られなかったからである。

続いて、証明済ファイル送信手段１３は、作成された証明済ファイルＦ３をユーザ端末２に送信する（ステップＳ１７）。

上記のステップＳ１３では、中間ファイルＦ２を送信していたが、データ証明装置１で中間ファイルＦ２のハッシュ値Ｆｈを算出し、このハッシュ値Ｆｈを送信してもよい。

【００４８】

《第３の実施形態》

第３の実施形態は、ユーザ端末２からは原本データＤではなく、原本データＤのハッシュ値Ｄｈが送信される点で第１の実施形態と相違し、第２の実施形態と共通する。

以下、第１の実施形態との相違点を中心に、図２のブロック図および図９のフロー図を参照しながら説明する。

【００４９】

原本データ受付手段８は、インターネットＮおよびインターフェース部１４を介してユーザ端末２から、原本データＤのハッシュ値Ｄｈを受信する（ステップＳ２１）。ここでユーザ識別情報と原本データ名も受信する。

【００５０】

中間ファイル作成手段９は、ＰＤＦファイルＦ１を作成する。ファイルＦ１は、第２の実施形態と同様に（図８を参照）、第１のエリアＡ１、第２のエリアＡ２、第３のエリアＡ３および第４のエリアＡ４を有する。第１のエリアＡ１には、原本データ名、原本データＤのハッシュ値Ｄｈの受信日時などの証明事項Ｂを記載し、第４のエリアＡ４に原本データＤのハッシュ値Ｄｈを添付して中間ファイルＦ２を作成する（ステップＳ２２）。

【００５１】

タイムスタンプ要求手段１０は、原本データＤのハッシュ値Ｄｈをタイムスタンプ付与装置３に送信する（ステップＳ２３）。タイムスタンプ付与装置３は、受信したハッシュ値Ｄｈを含む日時保証情報Ｃを生成する（ステップＳ２４）。ここで、特徴的なのは、原本データＤのハッシュ値Ｄｈに対してのみ一の証明印を押すも同然ということである。この実施形態では、証明事項Ｂに対してタイムスタンプが付与されることはない。

【００５２】

タイムスタンプ付与装置３が日時保証情報Ｃを送信してくる（ステップＳ２５）ので、日時保証情報取得手段１１はこれを受信する。証明済ファイル作成手段１２は、中間ファイルＦ２の第３のエリアＡ３に日時保証情報Ｃを添付し、証明済ファイルＦ３を作成する（ステップＳ２６）。この証明済ファイルＦ３の第２のエリアＡ２に添付されるファイルはない。ユーザ端末２から原本データ自体は送られなかったからである。

続いて、証明済ファイル送信手段１３は、作成された証明済ファイルＦ３をユーザ端末２に送信する（ステップＳ２７）。

この実施形態は、原本データＤ（正確にはそのハッシュ値Ｄｈ）についてのみタイムスタンプを受けたいというニーズに応えるものである。第１または第２の実施形態のように原本データＤと証明事項Ｂとを一体としてタイムスタンプを受けるのか、この第３の実施形態のように原本データＤにのみタイムスタンプを受けるのか、あるいは下記の第４の実施形態のように証明事項Ｂにのみタイムスタンプを受けるのかは、ユーザ端末２から原本データＤあるいはハッシュ値Ｄｈを送信するときにユーザに選択させるようにしてもよい。

【００５３】

《第４の実施形態》

第４の実施形態は、ユーザ端末２からは原本データＤではなく、原本データＤのハッシュ値Ｄｈが送信される点で第１の実施形態と相違し、第２および第３の実施形態と共通する。

以下、第１の実施形態との相違点を中心に、図２のブロック図および図１０のフロー図を参照しながら説明する。

【００５４】

原本データ受付手段８は、インターネットＮおよびインターフェース部１４を介してユーザ端末２から、原本データＤのハッシュ値Ｄｈを受信する（ステップＳ３１）。ここでユーザ識別情報と原本データ名も受信する。

【００５５】

中間ファイル作成手段９は、ＰＤＦファイルＦ１を作成する。ファイルＦ１は図１１に示すように、第１のエリアＡ１、第２のエリアＡ２、第３のエリアＡ３および第４のエリアＡ４を有する。第１のエリアＡ１には、原本データ名、原本データＤのハッシュ値Ｄｈの受信日時などの証明事項Ｂを記載して中間ファイルＦ２を作成する（ステップＳ３２）。この中間ファイルＦ２はタイムスタンプ付与装置３によって証明事項に対する証明を受けるために作成されたものである。したがって、中間ファイルＦ２には原本データＤのハッシュ値Ｄｈを含めない。

【００５６】

タイムスタンプ要求手段１０は、中間ファイルＦ２をタイムスタンプ付与装置３に送信する（ステップＳ３３）。タイムスタンプ付与装置３は、所定のハッシュ関数に受信した中間ファイルＦ２を入力してハッシュ値Ｆｈを算出する。ここで、特徴的なのは、証明事項Ｂのみを有する中間ファイルＦ２のハッシュ値Ｆｈを算出する点である。これにより、証明事項Ｂに対してのみ一の証明印を押すも同然となる。

タイムスタンプ付与装置３は、所定の時刻認証局にタイムスタンプＴＳの発行を要求し、このタイムスタンプＴＳにハッシュ値Ｆｈと、その他付加情報を含めて日時保証情報Ｃを生成する（ステップＳ３４）。

【００５７】

タイムスタンプ付与装置３が日時保証情報Ｃを送信してくる（ステップＳ３５）ので、日時保証情報取得手段１１はこれを受信する。証明済ファイル作成手段１２は、中間ファイルＦ２の第３のエリアＡ３に日時保証情報Ｃを添付し、第４のエリアＡ４に原本データＤのハッシュ値Ｄｈを添付して証明済ファイルＦ３を作成する（ステップＳ３６）。この証明済ファイルＦ３の第２のエリアＡ２に添付されるファイルはない。ユーザ端末２から原本データ自体は送られなかったからである。

続いて、証明済ファイル送信手段１３は、作成された証明済ファイルＦ３をユーザ端末２に送信する（ステップＳ３７）。

上記のステップＳ３３では、中間ファイルＦ２を送信していたが、データ証明装置１で中間ファイルＦ２のハッシュ値Ｆｈを算出し、このハッシュ値Ｆｈを送信してもよい。

【００５８】

《第５の実施形態》

この実施形態は、証明事項Ｂに本人確認書類を含める点で第１の実施形態と相違する。

以下、第１の実施形態と相違する点を説明する。

ユーザ情報記憶手段６には、ユーザごとに本人確認書類を含める。本人確認書類としては免許証、パスポート、住基カード或いは健康保険証などの公的な証明書が適当である。この本人確認書類を複写した画像データをユーザ情報記憶手段６に格納してもよく、免許証番号や被保険者番号などの記載事項をテキストデータとして格納してもよい。

中間ファイルＦ２の第１のエリアＡ１に証明事項Ｂを記載するときに、あわせて本人確認書類の画像データ或いはテキストデータを記載するとよい。証明事項Ｂには登録者であるユーザ名が必須の記載事項であるが、同姓同名もいることから、証明事項Ｂに本人確認書類データを含めることは非常に意義がある。

第２～第４の実施形態においても、同様に本人確認データも含めたタイムスタンプを受けるならば、極めて信頼性の高い内容証明となる。

【００５９】

《第６の実施形態》

この実施形態は、図１２に示すように原本作成者端末２０を含める点で第１の実施形態と相違する。

以下、第１の実施形態と相違する点を中心に説明する。

原本作成者端末２０は、原本データを作成する者が使用する情報処理装置であり、インターネットＮなどの通信回線を介してユーザ端末２とデータの送受信が可能である。原本作成者端末２０が作成した原本データがユーザ端末２に送信され、ユーザ端末２からの送信によりこの原本データがデータ証明装置１によって証明される。また、データ証明装置１からユーザ端末２に送信された証明済ファイルは、ユーザ端末２から原本作成者端末２０に送信される。

【００６０】

この実施形態が適用される状況として考えられるのは、次のような場合である。すなわち、原本作成者は発注者であり、ユーザが受注者であって、発注者から受注者に送られる発注書が原本データに相当する。後日起こり得る係争として、発注した覚えはない、受注していない、発注内容が変わっている、などが考えられる。このような事態に備えるためにも発注書を添付した受注証明書を作成して、当事者双方がこの受注証明書を保存しておくならば、将来の係争を回避するうえで意義のあることである。

【００６１】

図１３に従い、この実施形態の動作について説明する。

原本作成者端末２０が作成した発注書Ｄのデジタルデータがユーザ端末２に送信される（ステップＦ１）。

原本データ受付手段８は、ユーザ端末２から、発注書データＤを受信する（ステップＳ１ｎ）。中間ファイル作成手段９は、ＰＤＦファイルＦ１を作成する。ファイルＦ１は第１のエリアＡ１、第２のエリアＡ２、第３のエリアＡ３を有し、第１のエリアＡ１には、受注書の名前、住所、発注者の名前、発注内容の概要、発注書の内容に同意した日時などの証明事項Ｂが記載される。同意した日時として、例えばデータ証明装置１がユーザ端末２から発注書データＤを受信した日時を用いればよい。

さらにファイルＦ１の第２のエリアＡ２に発注書データＤを添付して中間ファイルＦ２を作成する（ステップＳ２ｎ）。

タイムスタンプ要求手段１０は、中間ファイルＦ２をタイムスタンプ付与装置３に送信する（ステップＳ３ｎ）。

タイムスタンプ付与装置３は、受信した中間ファイルＦ２に付与する日時保証情報Ｃを生成する（ステップＳ４ｎ）。

タイムスタンプ付与装置３が日時保証情報Ｃを送信してくる（ステップＳ５ｎ）ので、日時保証情報取得手段１１はこれを受信する。
証明済ファイル作成手段１２は、中間ファイルＦ２の第３のエリアＡ３に日時保証情報Ｃを添付し、受注証明書ファイルＦ３を作成する（ステップＳ６ｎ）。
続いて、証明済ファイル送信手段１３は、作成された受注証明書ファイルＦ３をユーザ端末２に送信する（ステップＳ７ｎ）。
ユーザ端末２は、受注証明書ファイルＦ３を保存するとともに、受注証明書ファイルＦ３の複製ファイルＦ４を作成する（ステップＦ２）。
受注証明書ファイルＦ３の複製Ｆ４は、ユーザ端末２から原本作成者端末２０に送信される（ステップＦ３）。

【００６２】
上記のステップＳ１ｎからＳ７ｎまでの各処理の内容は、ステップＳ１ｎの記載内容を除き、第1の実施形態のステップＳ１からＳ７までの処理（図３参照）と変わるところはない。
つまり、この実施形態は、第１の実施形態にステップＦ１、Ｆ２、Ｆ３の処理を追加することにより、発注書のような相手方のいる書類の内容証明を簡便に行うことを目的とする。
なお、このような目的は、第２～第５の実施形態にステップＦ１、Ｆ２、Ｆ３の処理を追加することによっても実現可能である。

【００６３】
《第７の実施形態》
この実施形態は、受注証明書ファイルに電子署名を添付する点で第６の実施形態と相違する。
システム構成は第６の実施形態と同様であり（図１２参照）、データ証明装置の機能は、電子署名生成・添付の機能が追加された点を除き第１の実施形態のデータ証明装置１と同様である。

【００６４】
この実施形態のデータ証明装置３０の機能ブロックについて図１４に従い説明する。ここで、第１の実施形態と同様の機能については図２と同一の符号を用いるとともに、説明を省略する。
記憶部４には、電子証明書記憶手段３１も含まれる。電子証明書記憶手段３１には、データ証明装置３０が有する電子証明書に関する情報が記憶されている。電子証明書に関する情報としては、電子証明書の所有者（この実施形態ではデータ証明装置３０の運営主体）の名前と住所、秘密鍵と対をなす公開鍵、当該電子証明書を発行した認証局に関する情報と発行日時などがある。

【００６５】
処理部５には、電子署名生成手段３２も含まれる。
この実施形態の証明済ファイル作成手段３３は、受信した日時保証情報Ｃに加え、電子署名生成手段３２が生成した電子署名Ｅも中間ファイルＦ２に添付して証明済ファイルＦ３を作成する。

【００６６】
図１５に従い、この実施形態の動作について説明する。第６の実施形態と同一内容の処理ステップについては、図１３と同一の符号を付す。
原本作成者端末２０が作成した発注書Ｄのデジタルデータがユーザ端末２に送信される（ステップＦ１）。
原本データ受付手段８は、ユーザ端末２から、発注書データＤを受信する（ステップＳ１ｎ）。中間ファイル作成手段９は、ＰＤＦファイルＦ１を作成する。図１６に示すように、ファイルＦ１は第１のエリアＡ１、第２のエリアＡ２、第３のエリアＡ３および電子署名エリアＡ５を有し、第１のエリアＡ１には、受注書の名前、住所、発注者の名前、発注内容の概要、発注書の内容に同意した日時などの証明事項Ｂが記載される。同意した日

時として、例えばデータ証明装置１がユーザ端末２から発注書データＤを受信した日時を用いればよい。
さらにファイルＦ１の第２のエリアＡ２に発注書データＤを添付して中間ファイルＦ２を作成する（ステップＳ４０）。
タイムスタンプ要求手段１０は、中間ファイルＦ２をタイムスタンプ付与装置３に送信する（ステップＳ３ｎ）。
タイムスタンプ付与装置３は、受信した中間ファイルＦ２に付与する日時保証情報Ｃを生成する（ステップＳ４ｎ）。
タイムスタンプ付与装置３が日時保証情報Ｃを送信してくる（ステップＳ５ｎ）ので、日時保証情報取得手段１１はこれを受信する。

【００６７】
電子署名生成手段３２は電子署名Ｅを生成する（ステップＳ４１）。ここで電子署名の対象となるのは、証明事項Ｂが記載され原本データＤを添付したファイルＦ２である。ファイルＦ２を、予め定義したハッシュ関数に代入してハッシュ値を求め、このハッシュ値をデータ証明装置３０の運営主体の秘密鍵で暗号化して暗号文を得る。この暗号文に、公開鍵、認証機関情報などの暗号文を復号化するうえで必要な情報を付加したものが電子署名Ｅである。
証明済ファイル作成手段３３は、中間ファイルＦ２の第３のエリアＡ３に日時保証情報Ｃを添付し、電子署名エリアＡ５に電子署名Ｅを添付し図１６に示すように、受注証明書ファイルＦ３を作成する（ステップＳ４２）。
続いて、証明済ファイル送信手段１３は、作成された受注証明書ファイルＦ３をユーザ端末２に送信する（ステップＳ７ｎ）。
ユーザ端末２は、受注証明書ファイルＦ３を保存するとともに、受注証明書ファイルＦ３の複製ファイルＦ４を作成する（ステップＦ２）。
受注証明書ファイルの複製Ｆ４は、ユーザ端末２から原本作成者端末２０に送信される（ステップＦ３）。

【００６８】
以上の処理フローでは、中間ファイルＦ２を電子署名の対象としていたが、第３のエリアＡ３に日時保証情報Ｃを添付した後のファイルを電子署名の対象としてもよい。
重要なのは、受注証明書ファイルＦ３には日時保証情報（いわゆるタイムスタンプに相当）と電子署名とを添付したということである。

【００６９】
上記の第７の実施形態では、データ証明装置３０の運営主体の秘密鍵を用いて電子署名を付与していた。つまり、受注証明書の原本性をデータ証明装置３０の運営主体が保証したことになる。
しかし、原本性を保証するのは、行政書士や税理士などの第三者でもよい。この場合は、電子証明書記憶手段３１には、データ証明装置３０の運営主体に与えられた秘密鍵と公開鍵ではなく、当該第三者の秘密鍵と、この秘密鍵に対応する電子証明書に関する情報が記憶される。
あるいは、ユーザ（＝受注者）の秘密鍵を用いて電子署名を付与してもよい。この場合、ユーザは、自分の秘密鍵と電子証明書をデータ証明装置３０側に預託し、電子証明書記憶手段３１はこれを記憶する。

【００７０】
タイムスタンプとともに電子署名も添付し、印紙税が非課税となる電子契約書を作成するという目的は、第２～第５の実施形態に発注者とのファイルの送受信処理（図１５のステップＦ１、Ｆ２、Ｆ３の処理）を追加するとともに、電子署名の生成と証明書への添付処理を追加することによっても実現可能である。

【００７１】
《第８の実施形態》
この実施形態は、証明の対象が紙媒体の書類である点で、上記の第１～第７の実施形態と

相違する。電子帳簿保存法の施行により、従来は紙媒体で管理していた帳簿書類も、一定の要件を充たすことで、電子データで保存することが可能となった。この電子データとして保存される帳簿書類も原本データとして証明の対象にしようとするのが本実施形態である。

【００７２】

システム構成は図１７に示すように、ユーザ端末２にスキャナ４１が接続されている点で上記の各実施形態と相違する。スキャナ４１が必須であるのは、電子帳簿保存法の規定に従い電子データで保存するために、当該紙の書類をスキャナで読み取る必要があるからである。

なお、この実施形態の代表的なユーザとして、顧客から帳簿書類を預かった税理士等が考えられる。

【００７３】

この実施形態のデータ証明装置４０の機能ブロックについて図１８に従い説明する。ここで、第７の実施形態のデータ証明装置３０と同様の機能については図１４と同一の符号を用いるとともに、説明を省略する。

記憶部４の電子証明書記憶手段４２には、電子証明書に関する情報、即ち、電子証明書の所有者である税理士等の名前と住所、秘密鍵と対をなす公開鍵、当該電子証明書を発行した認証局に関する情報と発行日時などが記憶されている。この場合、税理士等は、自分の秘密鍵と電子証明書をデータ証明装置４０側に預託しているわけである。

【００７４】

処理部５の原本データ受付手段４３は、原本データとともに紙媒体の書類に記載されていた事項などの送信も受け付ける。また、中間ファイル作成手段４４は、送信された事項なども中間ファイルの第１のエリアに記載する。

【００７５】

図１９に従い、この実施形態の動作について説明する。

紙媒体の書類をスキャナ４１が読み取って、画像情報をデジタルデータ化する（ステップＳ５１）。このようにデジタルデータ化された画像情報が、データ証明装置４０に送信される原本データである。原本データが格納されるファイル形式は、ＴＩＦＦを初めとする画像ファイルでも、ＰＤＦファイルでも何でもよい。紙媒体の書類の画像が視認または印刷可能であればよい。

ユーザはユーザ端末２と接続しているキーボードなどの入力手段から紙媒体の書類に記載されている書類記載事項を入力する（ステップＳ５２）。書類記載事項としては、取引者名、取引金額、伝票番号、取引年月日など、手書きされていたりスタンプを押されたりしている事項がある。

原本データ受付手段４３は、ユーザ端末２から、原本データＤと書類記載事項を受信する（ステップＳ５３）。中間ファイル作成手段４４は、ＰＤＦファイルＦ１を作成する。図２０に示すように、ファイルＦ１は第１のエリアＡ１、第２のエリアＡ２、第３のエリアＡ３および電子署名エリアＡ５を有し、第１のエリアＡ１には、ユーザの名前・住所、取引者の名前・住所、帳簿などの書類名、取引金額、伝票番号、取引年月日などの証明事項Ｂが記載される。

さらにファイルＦ１の第２のエリアＡ２に原本データＤを添付して中間ファイルＦ２を作成する（ステップＳ５４）。

タイムスタンプ要求手段１０は、中間ファイルＦ２をタイムスタンプ付与装置３に送信する（ステップＳ５５）。

タイムスタンプ付与装置３は、受信した中間ファイルＦ２に付与する日時保証情報Ｃを生成する（ステップＳ５６）。

タイムスタンプ付与装置３が日時保証情報Ｃを送信してくる（ステップＳ５７）ので、日時保証情報取得手段１１はこれを受信する。

【００７６】

電子署名生成手段３２は電子署名Ｅを生成する（ステップＳ５８）。ここで電子署名の対

象となるのは、証明事項である書類記載事項Ｂが記載され原本データＤを添付したファイルＦ２である。ファイルＦ２を、予め定義したハッシュ関数に代入してハッシュ値を求め、このハッシュちを税理士等の秘密鍵で暗号化して暗号文を得る。この暗号文に、公開鍵、認証機関情報などの暗号文を復号化するうえで必要な情報を付加したものが電子署名Ｅである。電子署名に関しては公知の技術を利用するので、ここでは説明を省略する。
証明済ファイル作成手段３３は、中間ファイルＦ２の第３のエリアＡ３に日時保証情報Ｃを添付し、電子署名エリアＡ５に電子署名Ｅを添付し図２０に示すように、証明書ファイルＦ３を作成する（ステップＳ５９）。
続いて、証明済ファイル送信手段１３は、作成された証明書ファイルＦ３をユーザ端末２に送信する（ステップＳ６０）。

【００７７】
以上の処理フローでは、中間ファイルＦ２を電子署名の対象としていたが、第３のエリアＡ３に日時保証情報Ｃを添付した後のファイルを電子署名の対象としてもよい。
上記の実施形態では、ユーザの秘密鍵を用いて電子署名を付与していた。つまり、保存証明書の原本性をユーザが保証したことになる。
この実施形態では、ユーザとして顧客に代わって帳簿類を保存する税理士等を想定しているが、原本性を保証するのは、データ証明装置４０の運営主体やユーザ以外の第三者でもよい。その場合は、データ証明装置４０の運営主体や、第三者の秘密鍵を用いて電子署名を付与することになる。

【００７８】
以上、第１～第８の実施形態をもとに本発明の説明をしてきた。これらの実施形態は、ユーザ端末がインターネットＮを介して外部のデータ証明装置の証明サービスを利用する場合の例示にすぎない。例えば、データ証明装置（１、３０，４０）とタイムスタンプ付与装置３との処理分担や処理の流れ等につき種々の変形例が考えられ、それらの変形例も本発明の範囲内にある。
例えば、上記の実施形態では、データ証明装置からユーザ端末２へ証明済ファイルＦ３を送信していた。しかし、必ずしもユーザ端末２へ送信しなくてもよい。ユーザ端末２がインターネットＮを介してアクセス可能な装置（データ証明装置が考えられるが、それに限らずデータ証明装置と通信可能かつユーザ管理を同期しているファイルサーバなどでもよい）に証明済ファイルＦ３を保存しておき、ユーザ端末２から要求がある度に、閲覧可能としてもよい。

【００７９】
前記の第１～第５の実施形態では証明済ファイルに電子署名が添付されていなかったが、日時保証情報とともに電子署名を添付してもよいことは言うまでもない。証明書としての客観性が高まるからである。

【００８０】
また、上記の説明では特に言及しなかったが、原本データには既にタイムスタンプを付与された証明済ファイルのデジタルデータも含みうる。データ証明装置やタイムスタンプ付与装置３が持っている電子証明書には有効期限が設定されているのが通常である。したがって、ユーザは、証明済ファイルの入手後、然るべき日時が経過してから該証明済ファイルあるいは該証明済ファイルのハッシュ値をデータ証明装置に送信し、再度証明を受ければ、内容証明が更新されたのも同然である。

【００８１】
《第９の実施形態》
この実施形態は、請求項１３に係る発明に対応するものであり、ユーザ端末５１自体がデータ証明の機能を備えている点で、上記の各実施形態と大きく相違する。自分で証明するわけであるから証明の客観性に疑義が生ずる可能性を考慮し、外部にデータ証明管理装置５２をおく。データ証明管理装置５２は、ユーザ認証と、電子署名者が所有する電子証明書のユーザ端末５１への配送とを担う。ユーザ端末５１は、この電子証明書を利用して生成した電子署名と、タイムスタンプ付与装置３からの日時保証情報とを同時に原本データ

に付加する。
【００８２】
図２１に示すように、ユーザ端末５１は、インターネットＮを介して、タイムスタンプ付与装置３及びデータ証明管理装置５２と接続している。データ証明管理装置５２は電子署名者の使用する端末（以下、「電子署名者端末」）５３とも接続している。
この実施形態は、データ証明の機能をデータ証明装置１が担っている第１の実施形態と対比されるものであり、タイムスタンプ付与装置３のように異なるところがないものは同一の符号を用いるとともに説明を省略する。
【００８３】
ユーザ端末５１は、この実施形態のシステムを利用して原本データについて内容証明済のファイルを生成しようとするユーザが利用するものであり、インターネット接続機能を有し、かつ、原本データの内容証明に必要なコンピュータプログラム（以下、「原本データ証明プログラム」）がインストールされていることを要する。
【００８４】
以下、図２１に従い、原本データ証明プログラムをインストールしたユーザ端末５１の構成を説明する。
ユーザ端末５１は、記憶部５４、処理部５５を備え、他に図示しないキーボードやディスプレイなどの入出力手段及びドライバ類、通信ネットワークを介したタイムスタンプ付与装置３などの外部の装置との通信を可能とする通信インターフェース部５６も備える。
記憶部５４は、原本データ証明プログラムや、処理の経過に伴う作業用データ、パラメータ類などを記憶する。また、ユーザ名、ユーザの所属する会社や団体名、メールアドレス、住所なども記憶し、原本データ証明プログラムによって適宜参照される。
【００８５】
処理部５５は、中間ファイル作成手段５７と、タイムスタンプ要求手段５８と、日時保証情報取得手段５９と、証明済ファイル作成手段６０とを含むと共に、ユーザ認証要求手段６１と、電子証明書取得手段６２と、電子署名生成手段６３と、電子証明書破棄手段６４とを、さらに含む。
これらの手段のうち、手段５７～６０は、第１～第８の実施形態ではデータ証明装置１に備えられていた。本実施形態は、データ証明装置１による処理をユーザの手許で実行させることによって、システムの簡素化と低コスト化を図るものである。
【００８６】
中間ファイル作成手段５７は、キーボードやマウスなどの入力手段によって、証明対象の原本データが指定されると、先ずＰＤＦなどの一体管理型フォーマットのファイルを作成する。次にこのファイルに指定された原本データを変更することなくそのまま添付するとともに、証明事項を記載して中間ファイルを作成する。証明事項の記載は原本データが格納されたファイルの指定日時（タイムスタンプ付与装置３から日時保証情報を取得した日時すなわち内容証明日時と同じとみなして差し支えない）やファイル名などの必要と考えられる項目があれば、書式はどのようなものでもよい。
タイムスタンプ要求手段５８は、中間ファイルをタイムスタンプ付与装置３に送信する。
日時保証情報取得手段５９は、タイムスタンプ付与装置３から日時保証情報を受信する。
証明済ファイル作成手段６０は、受信した日時保証情報を中間ファイルに添付して証明済ファイルを作成する。
【００８７】
ユーザ認証要求手段６１は、ユーザアカウントとパスワードをデータ証明管理装置５２に送信して認証を受ける。
電子証明書取得手段６２は、データ証明管理装置５２に対して、原本データおよび証明事項、あるいは両者を含む中間ファイル（以下、「原本データ或は中間ファイル」）を送信して、電子証明書を受信する。
電子署名生成手段６３は、受信した電子証明書を用いて電子署名を生成する。
電子証明書破棄手段６４は、電子署名の生成後に電子証明書を破棄する。

【００８８】
次に、データ証明管理装置５２について説明する。
データ証明管理装置５２は、正当なユーザからの要求があれば電子証明書を配送する情報処理装置であり、記憶部６５、処理部６６を含む。
【００８９】
記憶部６５は、ユーザ情報記憶手段６７と、電子証明書記憶手段６８を含む。また、記憶部６５は、コンピュータをデータ証明管理装置５２として機能させるためのコンピュータプログラムや、処理の経過に伴う作業用データ、パラメータ類、Ｗｅｂデータなどを記憶する。
ユーザ情報記憶手段６７は、本システムのユーザに関する情報、例えば、ユーザ名、住所、メールアドレス等をユーザアカウントおよびパスワードと関連付けて記憶する。
電子証明書記憶手段６８は、電子署名を行う者即ち電子署名者の名前、住所、メールアドレス等とともに、その電子署名者の電子証明書を記憶する。電子署名者とは、例えば行政書士である。
【００９０】
処理部６６は、ユーザ認証手段６９と、電子証明書配送手段７０と、電子署名者通知手段７１と、その他の処理手段を含む。
ユーザ認証手段６９は、ユーザ端末５１から送信されたユーザアカウントおよびパスワードがユーザ情報記憶手段６７に登録されていることをもって正当なユーザと判定する。
電子証明書配送手段７０は、正当なユーザと判定されたユーザ端末５１から原本データ或は中間ファイルを受信すると、ユーザ端末５１に電子証明書を送信する。電子証明書の送信の前に、この証明書の所有者である電子署名者の端末５３に、受信した原本データ或は中間ファイルを閲覧させて、電子署名者が了承した場合に限って、電子証明書を送信してもよい。
電子署名者通知手段７１は、電子署名者端末５３に通知をして原本データ或は中間ファイルの閲覧を促す。
ただし、これらの各手段の分類は、あくまで説明の便宜上にすぎない。各手段は、その機能に応じて、ハードウェア、ソフトウェアで実装される。ソフトウェアによる場合は、ＲＯＭやハードディスクなどの記憶手段に格納されているコンピュータプログラムを、ＣＰＵが実行する。これらは、公知の事柄であるので説明を省略する。
また、データ証明管理装置５２は、キーボードやディスプレイ等の入出力手段及びドライバ類、通信ネットワークを介したユーザ端末５１や電子署名者端末５３との通信を可能とする通信インターフェース部７２も備える。
【００９１】
電子署名者端末５３は、行政書士などの電子署名を行う者であって、データ証明管理装置５２に自分の電子証明書を預託している者が使用する情報処理装置である。
データ証明管理装置５２から、電子署名の対象となる原本データ或は中間ファイルの閲覧を促すメールを受信したり、データ証明管理装置５２にインターネットＮを介してアクセスし当該原本データ或は中間ファイルを閲覧したりする必要上、電子署名者端末５３はメール送受信機能およびインターネット接続機能を備えている。
【００９２】
次に、図２２を参照しながら、この実施形態のシステムの動作について詳しく説明する。
ユーザは、ユーザ端末５１の入力手段を介して、原本データ証明プログラムを起動する（ステップＳ６１）。なお、プログラムの起動は、画面上のアイコンのダブルクリック等の各種アプリケーションプログラムに共通の方法によるので、説明は省略する。
ユーザは、ユーザ端末５１の入力手段を介して、証明対象となる原本データを格納したファイルを指定する（ステップＳ６２）。ファイルの指定は、ディスプレイ上に表示されたダイアログボックスにおいてファイル一覧から所望のファイルを特定するといった方法による。このようなＧＵＩ（グラフィカルユーザインターフェース）の利用は、周知技術であるので、詳細は省略する。

【００９３】
ユーザ認証要求手段６１は、ユーザアカウントとパスワードをデータ証明管理装置５２に送信する（ステップＳ６３）。
データ証明管理装置５２のユーザ認証手段６９は、ユーザ端末５１から送信されたユーザアカウントおよびパスワードの組合せがユーザ情報記憶手段６７に登録されているか否かを検索し、登録されているならば正当なユーザと判定し（ステップＳ６４）、その判定結果をユーザ端末５１に送信する（ステップＳ６５）。
正当なユーザでなければ（ステップＳ６６で“ＮＧ”）、エラーメッセージを画面表示してエラー処理を行い、終了する。
【００９４】
正当なユーザであれば（ステップＳ６６で“ＯＫ”）、中間ファイル作成手段５７は、ＰＤＦファイルＦ１を作成する。ファイルＦ１は、第１のエリアＡ１、第２のエリアＡ２、第３のエリアＡ３を有する。第１のエリアＡ１には、原本データ名、原本データＤの指定日時などの証明事項Ｂが記載される。また、証明事項には、記憶部５４から抽出、あるいは入力手段から入力したユーザ名、メールアドレス、所属なども含まれる。
さらにファイルＦ１の第２のエリアＡ２に原本データＤを添付して中間ファイルＦ２を作成する（ステップＳ６７）。
【００９５】
電子証明書取得手段６２は、電子証明書の配送を受けるために、データ証明管理装置５２に原本データＤおよび証明事項Ｂ、あるいは両者を含む中間ファイルＦ２を送信する（ステップＳ６８）。
データ証明管理装置５２の電子署名者通知手段７１は、電子署名者端末５３に受信した中間ファイルＦ２などの閲覧を促す。中間ファイルＦ２などを電子署名者端末５３にメールで送信してもよく、データ証明管理装置５２が管理する所定のサイト（図示せず）のＵＲＬを通知し、当該サイト上で中間ファイルＦ２などを閲覧するように促してもよい。このように電子署名者の了承を得た後、当該電子署名者の電子証明書を電子証明書記憶手段６８から抽出して（ステップＳ６９）、ユーザ端末５１に送信する（ステップＳ７０）。
電子署名生成手段６３は、中間ファイルＦ２からハッシュ値を求め、受信した電子証明書を用いて電子署名を生成する（ステップＳ７１）。
【００９６】
タイムスタンプ要求手段５８は、中間ファイルＦ２をタイムスタンプ付与装置３に送信する（ステップＳ７２）。ユーザ端末５１は、予めタイムスタンプ付与装置３の提供するサービスを受けるために登録などの所定の手続きをしているものとする。なお、ユーザ端末５１は、タイムスタンプ付与装置３から見れば複数いるユーザの中の１ユーザであるから、両者の間には何らかの認証手段が確立されていることが望ましい。
タイムスタンプ付与装置３は、受信した中間ファイルＦ２に付与する日時保証情報Ｃを生成し（ステップＳ７３）、ユーザ端末５１に送信する（ステップＳ７４）。
ステップＳ７１の電子署名の生成は、このステップＳ７４の後に行ってもよい。
【００９７】
証明済ファイル作成手段６０は、中間ファイルＦ２の第３のエリアＡ３に日時保証情報Ｃとステップ７１で生成した電子署名を同時に添付し、証明済ファイルＦ３を作成する（ステップＳ７５）。作成された証明済ファイルＦ３は、記憶部５４やＵＳＢメモリなどの外部記憶媒体に適宜保存する。
電子証明書破棄手段６４は、ユーザ端末５１上から電子証明書を破棄する（ステップＳ７６）。この破棄の処理は、電子署名生成の直後に行ってもよい。この処理は、電子証明書を悪用されないようにするために必要な措置である。
【００９８】
このように第９の実施形態では、第三者の電子署名も添付された証明済ファイルＦ３が作成されるので、データ証明の客観性が確保できる。
なお、電子署名の主体は、データ証明管理装置５２の運営者であってもよい。その場合は

、ステップＳ６９において、電子署名者端末５３への通知と了承の処理は不要となる。
【００９９】
《第１０の実施形態》
この実施形態は、第１～第４のいずれか１の実施形態によって作成された証明済ファイルＦ３の利用に関するものであり、本発明のシステムが工夫次第でさまざまに応用できることの一例である。
【０１００】
この実施形態は、米国への仮出願のための書類を調整することを目的とする。
そのため、まず「米国への仮出願」ということについて簡単に説明する。
通常、特許出願をするためには所定の様式で、特許請求の範囲、明細書、図面などを含む書類を作成しなくてはならない。この書類、特に特許請求の範囲の検討と作成には手間と時間がかかり、そのために特許出願が遅れることもある。こうした事態を避けるのに好都合な制度として、米国には仮出願制度がある。仮出願制度では、厳格な書類の要件が課されておらず、特許請求の範囲の省略も可能であって、図面や実験記録や論文などを提出することにより出願しうる。１年以内に定められた書式の書類を揃えて正式な出願をしなくてはならないとはいえ、とりあえず出願日を確保できる。
　先願主義の日本とは異なり、米国は先発明主義を採用しているので、何時発明がなされたのかが重要な意味を持つ。それゆえ、仮出願時に提出する書類が何時作成されたのかを客観的に証明できることが望まれる。
この実施形態は、仮出願時に提出する書類の電子データが何時作成されたのかを本発明の証明済ファイルＦ３によって証明しようとするものである。
【０１０１】
　ユーザ端末２には、仮出願専用のソフトウェア（以下、「仮出願用プログラム」）がインストールされる。この仮出願用プログラムはユーザ端末２に接続する内蔵あるいは外付けの記憶媒体に記憶されており、ユーザ端末２が備えるマウスやキーボードなどの入力手段を介して起動の指示により、主記憶上に読み出されてＣＰＵが実行する。
仮出願用プログラムの機能は、次の３つに大別される。
（１）入力手段を介して指定されたファイルＤを、本発明のデータ証明装置１に送信して証明済ファイルＦ３を受信する機能（以下、「証明取得機能」）
（２）仮出願用の願書ファイルを自動生成する機能（以下、「願書生成機能」）
（３）入力手段を介して指定された１以上の証明済ファイルＦ３と、願書ファイルを１個のファイルに格納することで仮出願用データを生成する機能（以下、「出願用一式データ生成機能」）
【０１０２】
インストール済の仮出願用プログラムを起動しているユーザ端末２における処理を中心に、この実施形態の処理の流れを図２３に従い説明する。
仮出願用プログラムの証明取得機能により、仮出願時に提出するファイルＤをデータ証明装置１に送信する（ステップＳ８１）。このファイルＤとして想定されるのは、仮出願の願書とともに提出する図形データやテキストデータが格納されたファイルである。ファイルＤを受信したデータ証明装置１は、証明済ファイルＦ３を作成し（ステップＳ８２）、ユーザ端末２に送信する（ステップＳ８３）。このデータ証明装置１にアクセスして日時保証情報Ｃを添付した証明済ファイルＦ３を取得するステップＳ８１からＳ８３の処理は、上記の第１の実施形態そのものであり、したがって処理の詳細を説明することは省略する。
このステップＳ８１からＳ８３の処理は、証明を受けようとするファイルＤの個数分だけ繰り返される。
なお、証明済ファイルＦ３は複数のファイル（Ｄ１、Ｄ２，・・）を添付することができるので、同日に作成されたファイルであれば、ステップＳ８１で複数のファイルを送信してもよい。
仮出願の願書とともに提出したいファイルが作成されると、通常はその作成時点でデータ

証明装置１に送信され、証明済ファイルＦ３を取得することが望ましい。証明済ファイルＦ３に添付されている日時保証情報Ｃにより、願書とともに提出されているファイルＤが遅くとも何時の時点で存在していたかが証明可能であり、発明日の決定に意味を持つからである。

【０１０３】

願書に添付する個々のファイルＤについて証明済ファイルＦ３を取得したならば、次は仮出願のためのデータ一式を作成する。

仮出願用プログラムの図示しないメニュー画面などを利用して願書生成機能を選択すると、図２４に例示するような願書記載項目を入力するための画面が表示される。ユーザは入力手段を介して、発明者名、発明の名称、図面の枚数などを入力するだけで願書が自動生成される（ステップＳ８４）。ユーザは画面上で必要事項をキー入力等するだけでよく、仮出願用願書のフォーマットなどの知識は必要とされない。

【０１０４】

続いて、仮出願用プログラムの出願用一式データ生成機能を利用して、米国の特許庁へ提出するためのデータ一式を生成する。まず、図２５に例示するようなファイル選択画面が表示される。画面左側のファイル一覧から願書に添付したいファイルを選択する（ステップＳ８５）。このファイルは、当初のファイルＤではなく、ステップＳ８３を経て原ファイルＤおよび日時保証情報Ｃを添付した証明済ファイルＦ３である。

選択された１個以上のファイルＦ３は、ステップＳ８４で生成した願書ファイルとともに１個のファイル（以下、「出願用一式データ」）に格納される（ステップＳ８６）。

【０１０５】

仮出願を希望する者は、出願用一式データを米国の代理人に送ればよい（ステップＳ８７）。直接代理人宛に送信してもよいが、国内の代理人や社内の専門部署を介して送信してもよい。あるいは、データ証明装置１を介して送信してもよい。一旦データ証明装置１に送信すれば、データ証明装置１が米国への送信の履歴などを保存するからである。

【０１０６】

なお、出願用一式データを受信した米国の代理人は、格納されている各証明済ファイルＦ３に添付されているファイルＤを取り出し、これらのファイルＤを同時に格納されている願書ファイルの付属ファイルとして米国の特許庁へ提出すればよい。出願後に発明日について疑義が生じた場合などは、証明済ファイルＦ３の日時保証情報Ｃが証拠となる。

【０１０７】

この実施形態は、本発明のデジタルデータ内容証明システムの有用な応用例であるが、さまざまな変形が考えられる。

例えば、証明済ファイルＦ３の取得のためには、ファイル自体をデータ証明装置１に送信するのではなく、第２あるいは第３の実施形態のように当該ファイルのハッシュ値を代わりに送信してもよい。

また、願書の作成は証明済ファイルＦ３の選択後に行ってもよく、願書は自動生成によらず、別途ワープロソフトなどで作成してもよい。

さらに、図２４、図２５の画面は一例であり、適宜リファインされる。

要は、本発明は、さまざまな用途に活用でき、例えば、この実施形態のように米国への仮出願、さらに米国への正式の出願のためのデータを作成する際にも利用できるということが重要なのである。

【０１０８】

《第１１の実施形態》

この実施形態は、（請求項１８に係る発明に対応するもので、）タイムスタンプ付与装置に日時保証情報の生成機能以外に次の３つの機能が追加されている点で、上記の各実施形態と相違する。

【０１０９】

（追加機能１）電子署名を付与する機能

（追加機能２）アクセス可能に接続している記憶装置に証明済ファイルを格納するととも

に、検索に必要な文字情報データも対応づけて格納することにより、証明済ファイルのキーワード検索を可能とする機能
（追加機能３）所定のメールアドレス宛に、証明済ファイルを作成・保管した旨および作成したファイルの格納場所を通知する機能
【０１１０】
図２６に従い、この実施形態のシステム構成を説明する。
インターネットＮを介して、データ証明装置８０がユーザ端末８１及びタイムスタンプ付与装置８３と接続している。
【０１１１】
ユーザ端末８１は、画像読取装置８２と接続していることが必要である。画像読取装置８２としては、ＯＣＲ（Ｏｐｔｉｃａｌ　Ｃｈａｒａｃｔｅｒ　Ｒｅａｄｅｒ）が最適である。ＯＣＲであれば、紙媒体の書類を画像として読み取ることができると同時に、この画像に含まれる文字を識別して文字情報データに変換することもできるからである。
【０１１２】
タイムスタンプ付与装置８３は、ユーザ端末８１から中間ファイルが送信されてくると証明済ファイルを作成して証明済ファイル記憶装置８４に格納するとともに、所定のメールアドレス宛に証明済ファイルの格納場所を通知する情報処理装置である。この実施形態では、このようなサービスを提供している既存の業者がいれば、その業者のサービスを利用するので、タイムスタンプ付与装置８３はその業者がサービス提供にあたり利用する情報処理装置である。
タイムスタンプ付与装置８３は、ユーザ端末８１から中間ファイルを受信して日時保証情報と電子署名を付加して証明済ファイルを作成する証明済ファイル作成手段８５と、この証明済ファイルを記憶装置８４に格納するとともに、ユーザなどからの検索要求を受信すると検索したり閲覧に供したりする証明済ファイル管理手段８６と、証明済ファイルの格納場所を通知する通知メール送信手段８７を備えている。
タイムスタンプ付与装置８３が、その機能を実行するためにユーザ情報を記憶する手段、電子証明書を格納する記憶手段、通信ネットワークを介してデータ証明装置８０やユーザ端末８１と接続するための通信インターフェースなどを備えていることは言うまでもない。
証明済ファイル記憶装置８４は、タイムスタンプ付与装置８３に内蔵あるいは外付けのＨＤＤなどにより実装されてもよいが、タイムスタンプ付与装置８３とは別のコンピュータをファイルサーバとして利用してもよい。
【０１１３】
データ証明装置８０は、ユーザ端末８１から画像データを受信して、タイムスタンプ付与装置８３のデータ証明サービスに供するために当該画像データを所定フォーマットのファイルに貼り付けてユーザ端末８１に返送する情報処理装置である。
図２６に従い、データ証明装置８０の構成を説明する。なお、第１の実施の形態と同様の機能については同一の符号を用い説明を省略する。
【０１１４】
データ証明装置８０は、記憶部４、処理部８８、通信インターフェース部１４、その他キーボードやディスプレイ等の入出力手段及びドライバ類等を含む。
記憶部４は、ユーザ情報記憶手段６を含む。
処理部８８は、ユーザ情報管理手段７と、原本データ受付手段８９と、中間ファイル作成手段９０と、中間ファイル送信手段９１と、その他の処理手段を含む。
ただし、これらの各手段の分類は、あくまで説明の便宜上にすぎない。各手段は、その機能に応じて、ハードウェア、ソフトウェアで実装される。
【０１１５】
原本データ受付手段８９は、証明対象である画像データをユーザ端末８１から受信する。もし画像読取装置８２がＯＣＲであれば、画像データから識別した文字情報データも受信する。

中間ファイル作成手段９０は、先ずＰＤＦなどの一体管理型フォーマットのファイルを作成する。次にこのファイルに受信した画像データを貼り付けるとともに、文字情報データを添付して中間ファイルを作成する。中間ファイルには画像データのほか、画像データの受信日時やファイル名などの後日証明等が必要となる場合に参照されうる項目があれば記載してもよい。
中間ファイル送信手段９１は、中間ファイルをユーザ端末８１に送信する。この中間ファイルを受信したユーザ端末８１は、文字情報とともにタイムスタンプ付与装置８３に送信する。

【０１１６】

次に、図２７および図２８を参照しながら、この実施形態のシステムの動作について詳しく説明する。
ユーザ端末８１は、画像読取装置８２に紙媒体の帳票類を読み込ませ、デジタル画像データＦＩＬ１とこの画像データから識別した文字である文字情報データＦＩＬ２を取得する（ステップＳ９０）。図２７に示すように画像データＦＩＬ１は紙の帳票のイメージそのものであり、文字情報データＦＩＬ２は、帳票内の文字を取り込んだものである。
ユーザ端末８１は、画像データＦＩＬ１と文字情報データＦＩＬ２をデータ証明装置８０に送信する（ステップＳ９１）。ユーザを特定する名前やメールアドレス等の情報も同時に送信する。ユーザ情報記憶手段６にユーザ登録済であれば、ユーザＩＤなどの最小限の情報で足りる。

【０１１７】

データ証明装置８０の原本データ受付手段８９は、送信された画像データおよび文字情報データを受信して中間ファイル作成手段９０に渡す。本実施形態の原本データとは紙媒体の帳票類のイメージを格納した画像データである。中間ファイル作成手段９０は、ＰＤＦファイルＦＩＬ３を作成する。ファイルＦＩＬ３は図２７に示すように、第１のエリア（請求項１８の「証明対象エリア」）Ａ１、第２のエリアＡ２、第３のエリアＡ３および第４のエリアＡ４を有する。第１のエリアＡ１には、画像データＦＩＬ１を貼り付ける。さらに第２のエリアＡ２に文字情報データＦＩＬ２を添付する。これにより中間ファイルＦＩＬ３が加工されてＦＩＬ４となる（ステップＳ９２）。なお、原本である画像データ名（帳票名）、画像データの受信日時などは将来証拠として参照される可能性がある。そのため、これらの事項は第１のエリアＡ１の適宜の箇所に記載してもよい。

【０１１８】

中間ファイル送信手段９１は、作成した中間ファイルＦＩＬ４をユーザ端末８１に送信する（ステップＳ９３）。
ユーザ端末８１は、受信した中間ファイルＦＩＬ４をタイムスタンプ付与装置８３に送信する（ステップＳ９４）。同時にユーザを特定するために必要な情報も送信する。ユーザを特定する情報の一つにメールアドレスがある。証明済ファイルを作成し記憶装置８４に格納したならば、ユーザに通知するが、このメールアドレスが送信先となるからである。
ここで、文字情報データＦＩＬ２の扱いとして複数が考えられる。上記のステップＳ９２では第２のエリアＡ２に添付した（図２７参照）が、第１のエリアＡ１に画像データＦＩＬ１の前後に貼り付けてもよい。あるいは、文字情報データＦＩＬ２の内容を中間ファイルＦＩＬ４には含めず、ステップＳ９４においてユーザ端末８１が中間ファイルＦＩＬ４と文字情報データＦＩＬ２とをそれぞれ送信してもよい。これはタイムスタンプ付与装置８３の機能仕様に依存する。

【０１１９】

タイムスタンプ付与装置８３の証明済ファイル作成手段８５は、中間ファイルＦＩＬ４に日時保証情報Ｃと電子署名Ｅを添付する（ステップＳ９５）。まず、受信した中間ファイルＦＩＬ４に付与する日時保証情報Ｃを生成する。生成の仕方は第１の実施形態と同様なので説明は省略する。あわせて、タイムスタンプ付与装置８３の電子証明書を利用して電子署名Ｅも生成する。電子署名の生成の仕方は第７の実施形態と同様なので説明は省略する。

証明済ファイル作成手段８５は、中間ファイルＦＩＬ４の第３のエリアＡ３に日時保証情報Ｃを添付し、第４のエリアＡ４に電子署名Ｅを添付する。以上で証明済ファイルＦＩＬ５が完成する。

【０１２０】

続いて、証明済ファイル管理手段８６は、作成された証明済ファイルＦＩＬ５を文字情報データＦＩＬ２と対応づけて記憶装置８４に格納する（ステップＳ９６）。文字情報データＦＩＬ２も同時に格納するのは、ユーザからの検索要求に対応するためである。たとえば、図２７のＦＩＬ２のような項目が画像と対応づけて記憶されていれば、ユーザ「□山◎男」から「領収書　平成２２年」というキーワードが送られてきた場合、宛先が「□山◎男」、日付が「平成２２年」の領収書を検索することができる。

【０１２１】

タイムスタンプ付与装置８３の通知メール送信手段８７は、証明済ファイルＦＩＬ５の記憶装置８４への格納が完了した時点で、所定のメールアドレスに証明および格納処理の完了の旨、および格納場所をメールで通知する（ステップＳ９７）。所定のメールアドレスとは、ユーザとの契約に従うが、必ずしもユーザのメールアドレスに限らず、契約先のメールアドレスやデータ証明装置８０のメールアドレスであってもかまわない。格納場所の表わし方としては、例えば“http:／／ｗｗｗ．ｘｘｘ＊＊＊．ｊｐ／ｕｓｅｒＰＤＦ／□山／領収証１．ｐｄｆ”のようなＵＲＬがある。

この通知メールを受信したユーザは、メールに記載されている登録場所にアクセスして証明済ファイルＦＩＬ５を閲覧したり、ダウンロードしたりすることができる。そのためにはもちろん、あらかじめ登録してあるユーザＩＤやパスワードなどで認証を受けねばならないし、閲覧出来るのもユーザ本人の証明済ファイルＦＩＬ５等許可されたファイルのみである。

【０１２２】

この第１１の実施形態にもさまざまな変形が考えられる。例えば、ＯＣＲの使用を前提としていたが、文字を認識する機能のないスキャナを使用するユーザもいる。その場合は、ユーザは自分で文字情報データＦＩＬ２を作成してもよい。あるいは、ユーザ端末からは画像データのみを送信し、データ証明装置８０側でソフトウェアを用いて、あるいは人手を介して文字情報データＦＩＬ２を作成してもよい。

【産業上の利用可能性】

【０１２３】

ユーザは、原本データについてデータを格納するファイル形式を問わず簡便に内容証明を受けることができる。今後各種書類は、従来の紙媒体からデジタルデータへの移行が進むと予想されるが、本発明はデジタルデータの内容証明を簡便かつ確実に行うシステム・方法として多くの需要が見込まれると期待される。また、紙媒体の書類であっても、スキャナで画像として読み取りデジタルデータ化すれば、本発明の原本データとして扱われて証明を受けることができる。なお「簡便」とは、単にユーザの作業の簡便性だけではなく、「運用のための大がかりな組織や、専用コンピュータおよびそのソフトウェアを必要としない」という意味も含まれる。

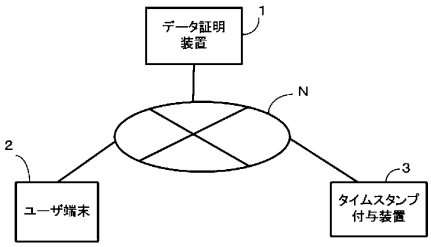
【符号の説明】

【０１２４】

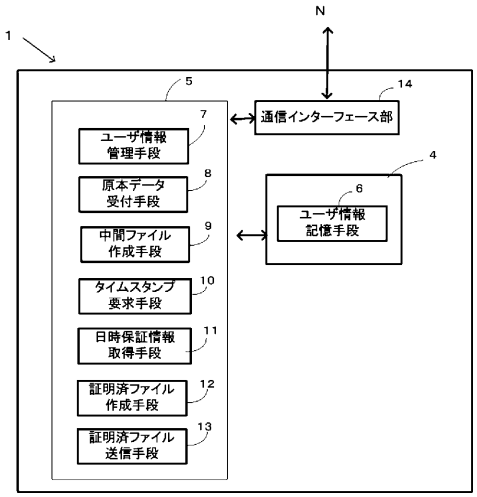
１：データ証明装置、２：ユーザ端末、３：タイムスタンプ付与装置、
６：ユーザ情報記憶手段、７：ユーザ情報管理手段、８：原本データ受付手段、
９：中間ファイル作成手段、１０：タイムスタンプ要求手段、１１：日時保証情報取得手段、１２：証明済ファイル作成手段、１３：証明済ファイル送信手段、
２０：原本作成者端末、
３０：データ証明装置、３１：電子証明書記憶手段、３２：電子署名生成手段、３３：証明済ファイル作成手段、
４０：データ証明装置、４１：スキャナ、４２：電子証明書記憶手段、４３：原本データ受付手段、４４：中間ファイル作成手段、

５１：ユーザ端末、５２：データ証明管理装置、
５７：中間ファイル作成手段、５８：タイムスタンプ要求手段、
５９：日時保証情報取得手段、６０：証明済ファイル作成手段、
６１：ユーザ認証要求手段、６２：電子証明書取得手段、６３：電子署名生成手段、６４：電子証明書破棄手段、
６７：ユーザ情報記憶手段、６８：電子証明書記憶手段、
６９：ユーザ認証手段、７０：電子証明書配送手段、７１：電子署名者通知手段、
８０：データ証明装置、８１：ユーザ端末、８２：画像読取装置、８３：タイムスタンプ付与装置、８４：証明済ファイル記憶装置、８９：原本データ受付手段、
９０：中間ファイル作成手段、９１：中間ファイル送信手段、
Ｎ：インターネット、
Ａ１～Ａ４：第１～４のエリア、Ａ５：電子署名エリア、Ｂ：証明事項、Ｃ：日時保証情報、Ｄ：原本データ、Ｄｈ：原本データのハッシュ値、Ｅ：電子署名、Ｆ１：ＰＤＦファイル、Ｆ２：中間ファイル、Ｆｈ：中間ファイルのハッシュ値、Ｆ３：証明済ファイル

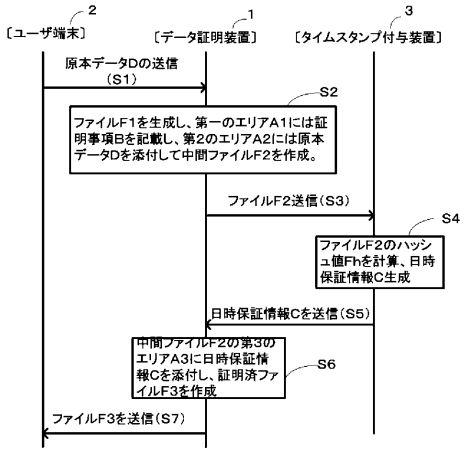
【図１】



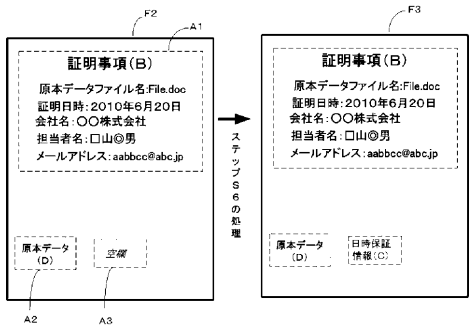
【図２】



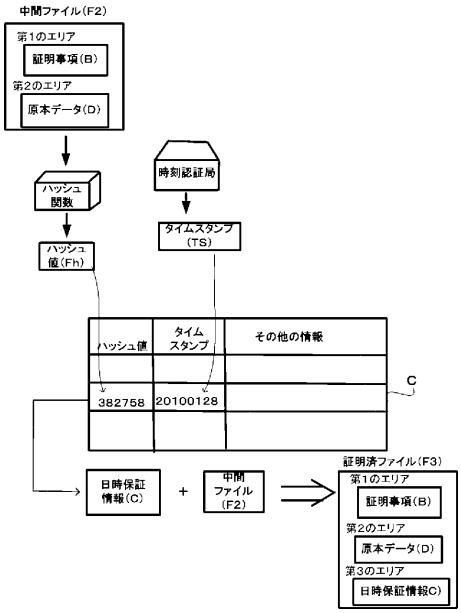
【図３】



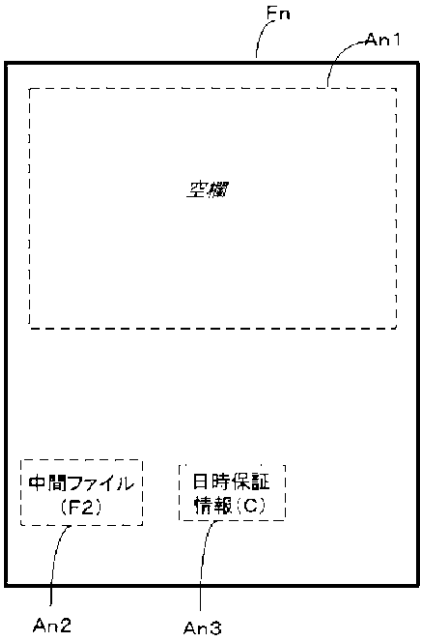
【図４】



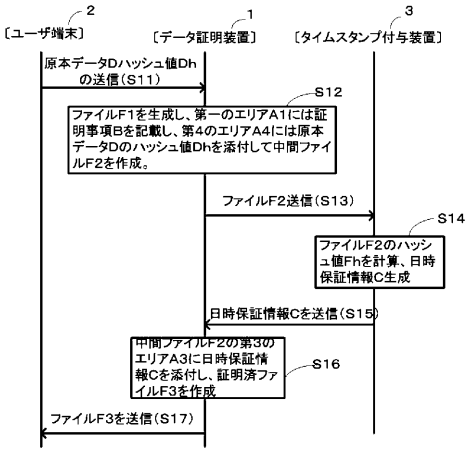
【図５】


中間ファイル(F2)
第1のエリア
証明事項(B)
第2のエリア
原本データ(D)
ハッシュ関数
ハッシュ値(Fh)
時刻認証局
タイムスタンプ(TS)
ハッシュ値
タイムスタンプ
その他の情報
382758
20100128
C
日時保証情報(C)
+
中間ファイル(F2)
証明済ファイル(F3)
第1のエリア
証明事項(B)
第2のエリア
原本データ(D)
第3のエリア
日時保証情報C)

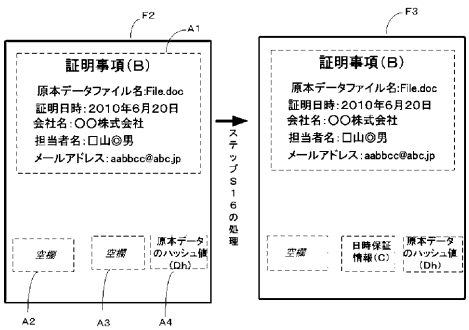
【図６】


Fn
An1
空欄
中間ファイル(F2)
日時保証情報(C)
An2
An3

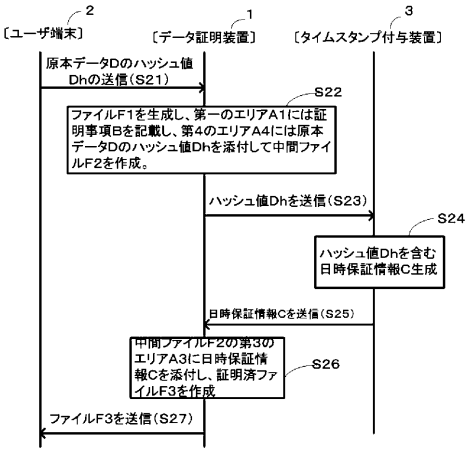
【図７】


2
〔ユーザ端末〕
1
〔データ証明装置〕
3
〔タイムスタンプ付与装置〕
原本データDハッシュ値Dhの送信(S11)
S12
ファイルF1を生成し、第一のエリアA1には証明事項Bを記載し、第4のエリアA4には原本データDのハッシュ値Dhを添付して中間ファイルF2を作成。
ファイルF2送信(S13)
S14
ファイルF2のハッシュ値Fhを計算、日時保証情報C生成
日時保証情報Cを送信(S15)
中間ファイルF2の第3のエリアA3に日時保証情報Cを添付し、証明済ファイルF3を作成
S16
ファイルF3を送信(S17)

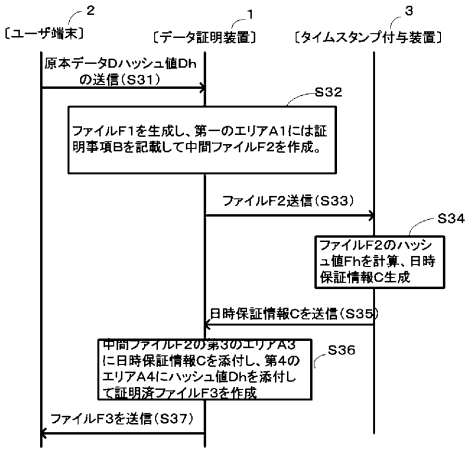
【図８】


F2
A1
証明事項(B)
原本データファイル名:File.doc
証明日時:2010年6月20日
会社名:○○株式会社
担当者名:口山◎男
メールアドレス:aabbcc@abc.jp
空欄
空欄
原本データのハッシュ値(Dh)
A2
A3
A4
ステップS16の処理
F3
証明事項(B)
原本データファイル名:File.doc
証明日時:2010年6月20日
会社名:○○株式会社
担当者名:口山◎男
メールアドレス:aabbcc@abc.jp
空欄
日時保証情報(C)
原本データのハッシュ値(Dh)

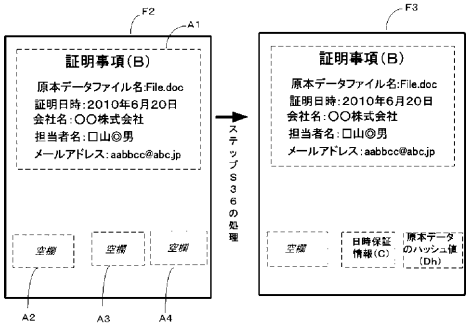
【図９】


2
〔ユーザ端末〕
1
〔データ証明装置〕
3
〔タイムスタンプ付与装置〕
原本データDのハッシュ値Dhの送信(S21)
S22
ファイルF1を生成し、第一のエリアA1には証明事項Bを記載し、第4のエリアA4には原本データDのハッシュ値Dhを添付して中間ファイルF2を作成。
ハッシュ値Dhを送信(S23)
S24
ハッシュ値Dhを含む日時保証情報C生成
日時保証情報Cを送信(S25)
中間ファイルF2の第3のエリアA3に日時保証情報Cを添付し、証明済ファイルF3を作成
S26
ファイルF3を送信(S27)

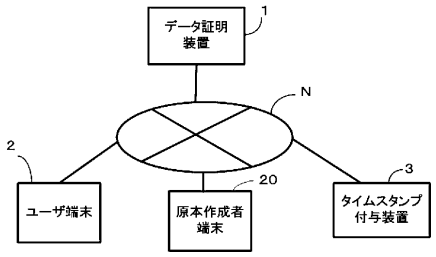
【図１０】



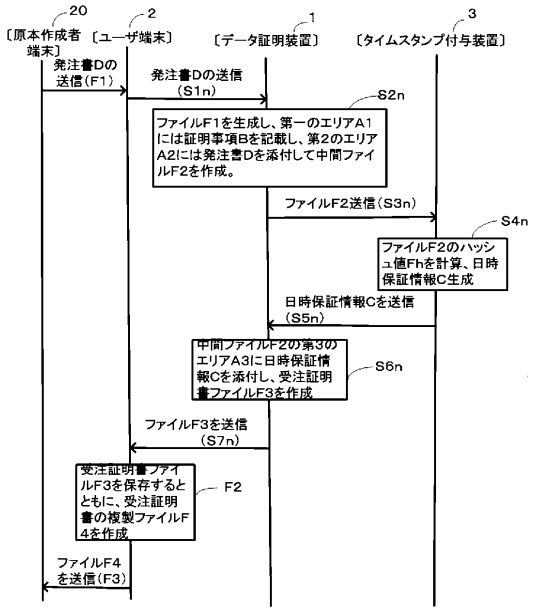
【図１１】



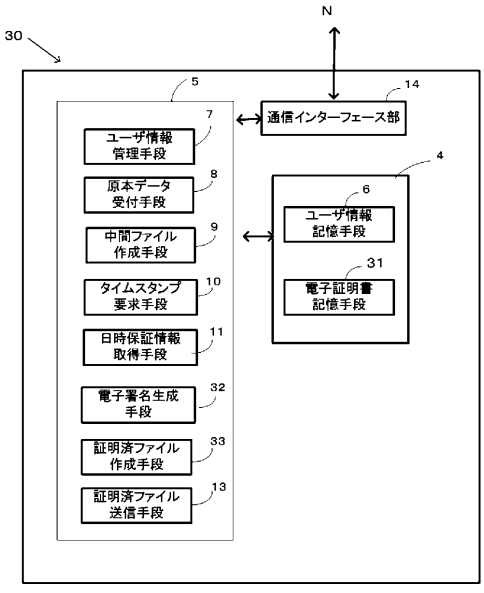
【図１２】



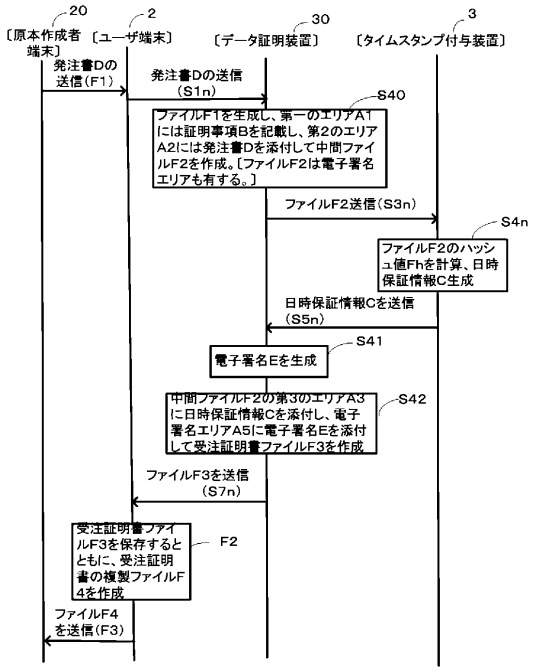
【図１３】



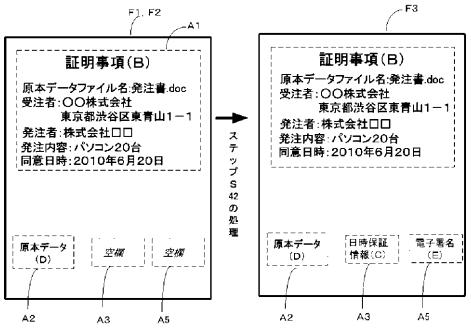
【図１４】



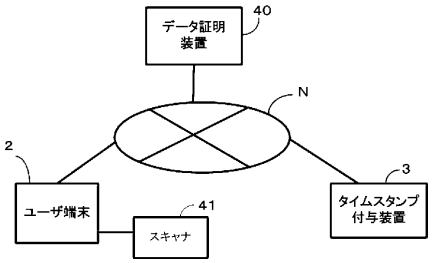
【図１５】



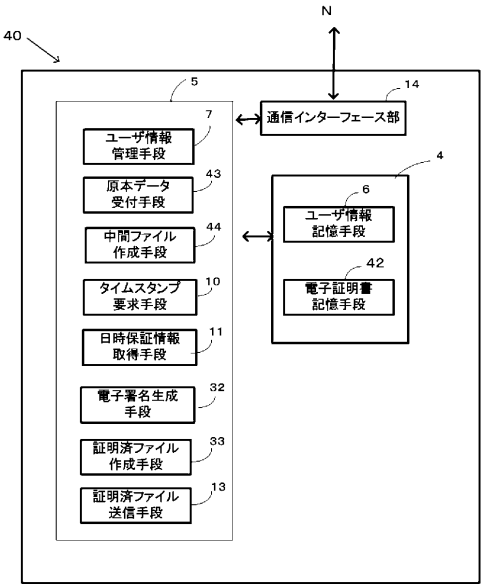
【図１６】



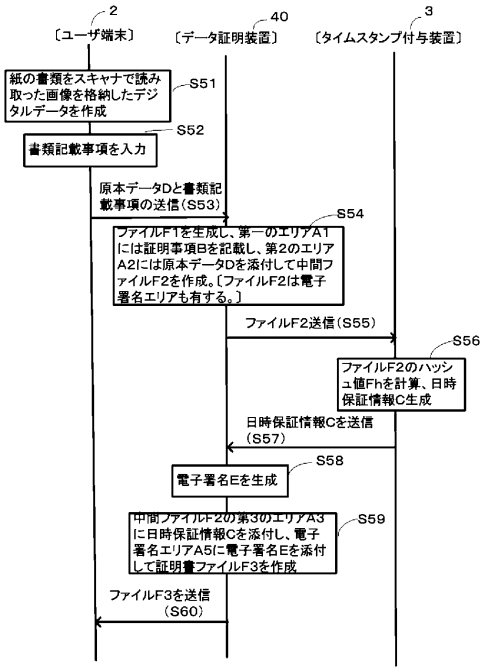
【図１７】



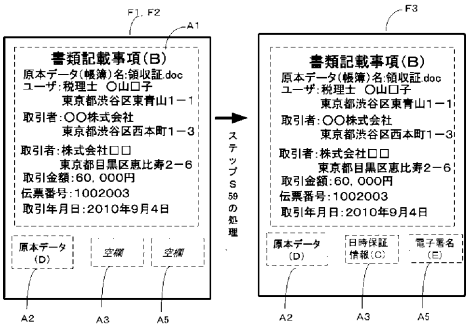
【図１８】



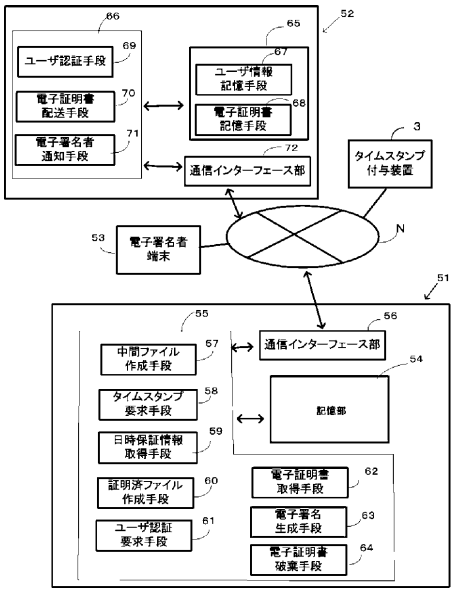
【図１９】



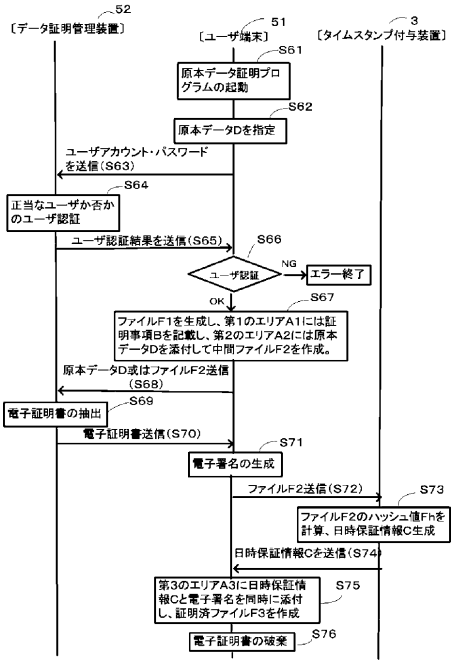
【図２０】



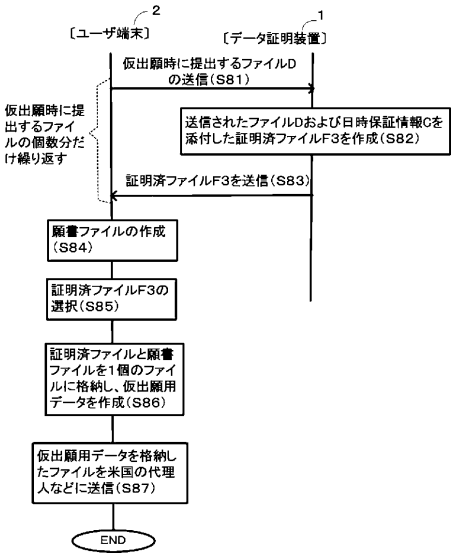
【図２１】



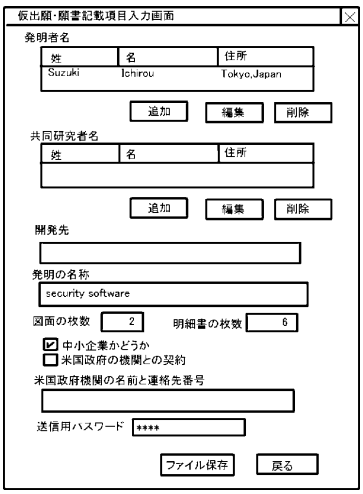
【図２２】



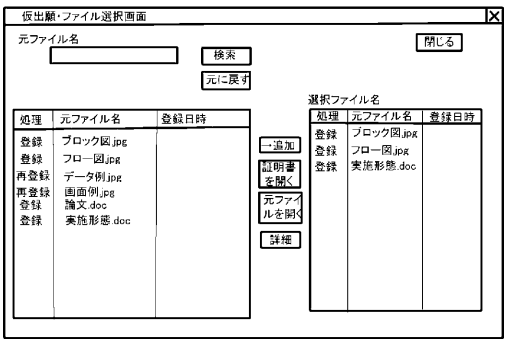
【図２３】



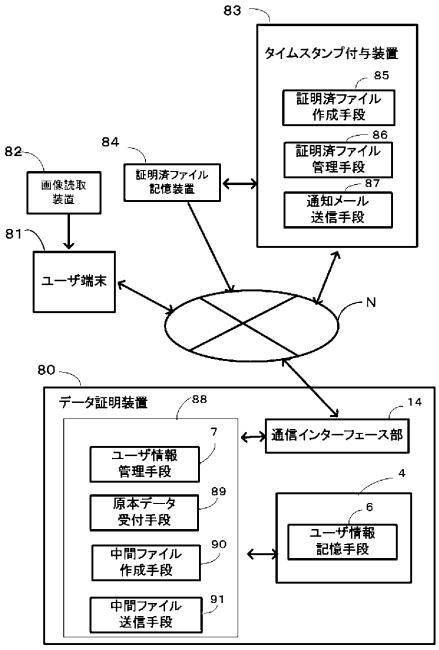
【図２４】



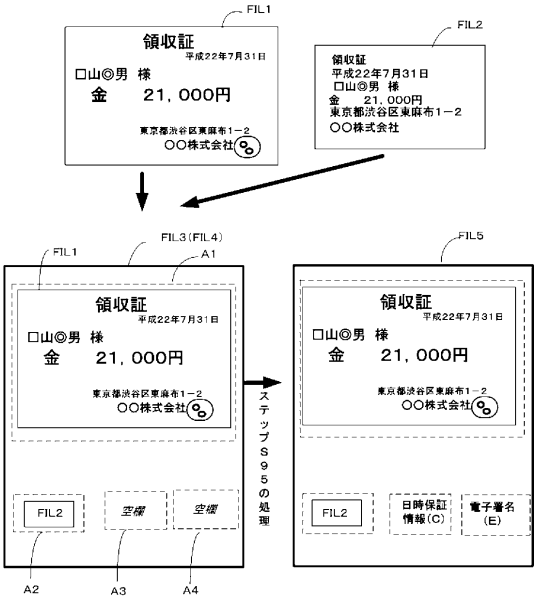
【図２５】



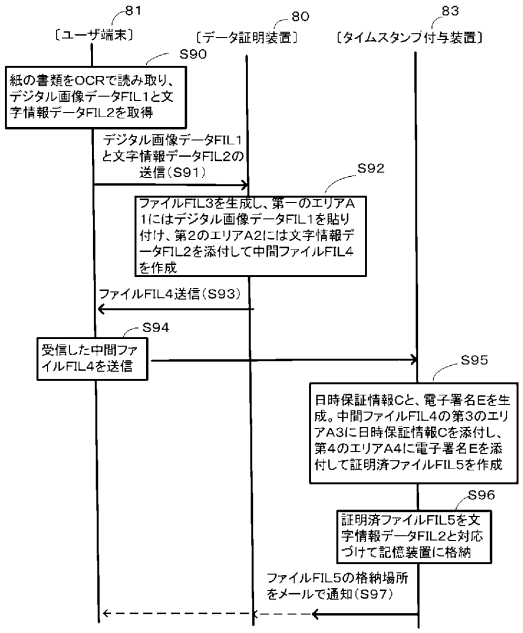
【図２６】


83
タイムスタンプ付与装置
85
証明済ファイル作成手段
86
証明済ファイル管理手段
87
通知メール送信手段
82
画像読取装置
84
証明済ファイル記憶装置
81
ユーザ端末
N
80
データ証明装置
88
14
通信インターフェース部
7
ユーザ情報管理手段
89
原本データ受付手段
90
中間ファイル作成手段
91
中間ファイル送信手段
4
6
ユーザ情報記憶手段

【図２７】


FIL1
領収証
平成22年7月31日
□山◎男 様
金 21，000円
東京都渋谷区東麻布1－2
○○株式会社
FIL2
領収証
平成22年7月31日
□山◎男 様
金 21，000円
東京都渋谷区東麻布1－2
○○株式会社
FIL3（FIL4）
FIL1
A1
領収証
平成22年7月31日
□山◎男 様
金 21，000円
東京都渋谷区東麻布1－2
○○株式会社
ステップS95の処理
FIL5
領収証
平成22年7月31日
□山◎男 様
金 21，000円
東京都渋谷区東麻布1－2
○○株式会社
FIL2
空欄
空欄
FIL2
日時保証情報（C）
電子署名（E）
A2
A3
A4

【図２８】


81
〔ユーザ端末〕
80
〔データ証明装置〕
83
〔タイムスタンプ付与装置〕
S90
紙の書類をOCRで読み取り、デジタル画像データFIL1と文字情報データFIL2を取得
デジタル画像データFIL1と文字情報データFIL2の送信（S91）
S92
ファイルFIL3を生成し、第一のエリアA1にはデジタル画像データFIL1を貼り付け、第2のエリアA2には文字情報データFIL2を添付して中間ファイルFIL4を作成
ファイルFIL4送信（S93）
S94
受信した中間ファイルFIL4を送信
S95
日時保証情報Cと、電子署名Eを生成。中間ファイルFIL4の第3のエリアA3に日時保証情報Cを添付し、第4のエリアA4に電子署名Eを添付して証明済ファイルFIL5を作成
S96
証明済ファイルFIL5を文字情報データFIL2と対応づけて記憶装置に格納
ファイルFIL5の格納場所をメールで通知（S97）

フロントページの続き

(56)参考文献 特開２０１０－０８１３７２（ＪＰ，Ａ）
特開２００４－２５２３８５（ＪＰ，Ａ）
特開２００３－０２２０１０（ＪＰ，Ａ）
特開２００８－３１２０６４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２