

【特許請求の範囲】**【請求項 1】**

紙文書を読み取ることにより画像データを生成する文書電子化装置であって、

ネットワークを介して接続するタイムスタンプサービスに、複数の前記画像データに対して一つのタイムスタンプの生成を要求するタイムスタンプ要求手段を有することを特徴とする文書電子化装置。

【請求項 2】

前記紙文書ごとに読み取られた複数の画像データのそれぞれについて第一のメッセージダイジェストを生成する第一のメッセージダイジェスト生成手段と、

前記第一のメッセージダイジェスト生成手段によって生成されたそれぞれのメッセージダイジェストを結合したデータについて第二のメッセージダイジェストを生成する第二のメッセージダイジェスト生成手段とを有し、

前記タイムスタンプ要求手段は、前記第二のメッセージダイジェストに対するタイムスタンプの生成を前記タイムスタンプサービスに要求することを特徴とする請求項 1 記載の文書電子化装置。

【請求項 3】

当該文書電子化装置に固有の秘密鍵を用いて前記画像データに対する第一の電子署名を生成する第一の電子署名生成手段を有することを特徴とする請求項 1 又は 2 記載の文書電子化装置。

【請求項 4】

前記第一の電子署名生成手段は、前記第一のメッセージダイジェスト生成手段によって生成されたそれぞれのメッセージダイジェストを前記秘密鍵によって暗号化することにより前記第一の電子署名を生成することを特徴とする請求項 3 記載の文書電子化装置。

【請求項 5】

前記画像データに基づくメッセージダイジェストを IC カードに送信することにより、前記 IC カードに固有の秘密鍵によって前記画像データに対する第二の電子署名を生成させる第二の電子署名生成手段を有することを特徴とする請求項 1 乃至 4 いずれか一項記載の文書電子化装置。

【請求項 6】

前記第二の電子署名生成手段は、前記第二のメッセージダイジェストを前記 IC カードに送信することを特徴とする請求項 5 記載の文書電子化装置。

【請求項 7】

前記タイムスタンプ要求手段は、一定の周期で前記タイムスタンプの生成を要求することを特徴とする請求項 1 乃至 6 いずれか一項記載の文書電子化装置。

【請求項 8】

前記タイムスタンプ要求手段が前記タイムスタンプの生成を要求する時期をユーザに入力させる入力手段を有することを特徴とする請求項 1 乃至 7 いずれか一項記載の文書電子化装置。

【請求項 9】

紙文書を読み取ることにより画像データを生成する文書電子化装置における文書電子化方法であって、

ネットワークを介して接続するタイムスタンプサービスに、複数の前記画像データに対して一つのタイムスタンプの生成を要求するタイムスタンプ要求手順を有することを特徴とする文書電子化方法。

【請求項 10】

前記紙文書ごとに読み取られた複数の画像データのそれぞれについて第一のメッセージダイジェストを生成する第一のメッセージダイジェスト生成手順と、

前記第一のメッセージダイジェスト生成手順において生成されたそれぞれのメッセージダイジェストを結合したデータについて第二のメッセージダイジェストを生成する第二のメッセージダイジェスト生成手順とを有し、

10

20

30

40

50

前記タイムスタンプ要求手順は、前記第二のメッセージダイジェストに対するタイムスタンプの生成を前記タイムスタンプサービスに要求することを特徴とする請求項 9 記載の文書電子化方法。

【請求項 11】

当該文書電子化装置に固有の秘密鍵を用いて前記画像データに対する第一の電子署名を生成する第一の電子署名生成手順を有することを特徴とする請求項 9 又は 10 記載の文書電子化方法。

【請求項 12】

前記第一の電子署名生成手順は、前記第一のメッセージダイジェスト生成手順において生成されたそれぞれのメッセージダイジェストを前記秘密鍵によって暗号化することにより前記第一の電子署名を生成することを特徴とする請求項 11 記載の文書電子化方法。 10

【請求項 13】

前記画像データに基づくメッセージダイジェストを IC カードに送信することにより、前記 IC カードに固有の秘密鍵によって前記画像データに対する第二の電子署名を生成させる第二の電子署名生成手順を有することを特徴とする請求項 9 乃至 12 いずれか一項記載の文書電子化方法。

【請求項 14】

前記第二の電子署名生成手順は、前記第二のメッセージダイジェストを前記 IC カードに送信することを特徴とする請求項 13 記載の文書電子化方法。

【請求項 15】 20

紙文書を読み取ることにより画像データを生成する文書電子化装置に、

ネットワークを介して接続するタイムスタンプサービスに、複数の前記画像データに対して一つのタイムスタンプの生成を要求するタイムスタンプ要求手順を実行させるための文書電子化プログラム。

【請求項 16】

前記紙文書ごとに読み取られた複数の画像データのそれぞれについて第一のメッセージダイジェストを生成する第一のメッセージダイジェスト生成手順と、

前記第一のメッセージダイジェスト生成手順において生成されたそれぞれのメッセージダイジェストを結合したデータについて第二のメッセージダイジェストを生成する第二のメッセージダイジェスト生成手順とを有し、 30

前記タイムスタンプ要求手順は、前記第二のメッセージダイジェストに対するタイムスタンプの生成を前記タイムスタンプサービスに要求することを特徴とする請求項 15 記載の文書電子化プログラム。

【請求項 17】

当該文書電子化装置に固有の秘密鍵を用いて前記画像データに対する第一の電子署名を生成する第一の電子署名生成手順を有することを特徴とする請求項 15 又は 16 記載の文書電子化プログラム。

【請求項 18】

前記第一の電子署名生成手順は、前記第一のメッセージダイジェスト生成手順において生成されたそれぞれのメッセージダイジェストを前記秘密鍵によって暗号化することにより前記第一の電子署名を生成することを特徴とする請求項 17 記載の文書電子化プログラム。 40

【請求項 19】

前記画像データに基づくメッセージダイジェストを IC カードに送信することにより、前記 IC カードに固有の秘密鍵によって前記画像データに対する第二の電子署名を生成させる第二の電子署名生成手順を有することを特徴とする請求項 15 乃至 18 いずれか一項記載の文書電子化プログラム。

【請求項 20】

前記第二の電子署名生成手順は、前記第二のメッセージダイジェストを前記 IC カードに送信することを特徴とする請求項 19 記載の文書電子化プログラム。 50

【請求項 2 1】

請求項 1 5 乃至 2 0 いずれか一項記載の文書電子化プログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】**【技術分野】****【0 0 0 1】**

本発明は、文書電子化装置、文書電子化方法、文書電子化プログラム及び記録媒体に関し、特に紙文書を読み取ることにより画像データを生成する文書電子化装置、文書電子化方法、文書電子化プログラム及び記録媒体に関する。

【背景技術】

10

【0 0 0 2】

社会の高度情報化が進展するにつれ、従来は紙で保存が義務付けられていた書類も、電子的（電子文書として）に保存できるようにすることが求められている。しかし、電子文書は紙文書に比較して、痕跡を残さない改ざんが可能である、不可視である、長期保存性が劣る等といった問題があるため、これらの問題が解決されなければ電子文書のまま原本として保存することは法的に許可されないという状況であった。この問題を解決する方法として、電子文書について紙文書と同等の原本性を確保するシステムが提案されており、普及の兆しを見せている。

【特許文献 1】特開 2 0 0 0 - 2 1 5 3 7 9 号公報

【特許文献 2】特開 2 0 0 2 - 2 3 0 2 0 2 号公報

20

【特許文献 3】特開 2 0 0 3 - 2 2 4 7 2 8 号公報

【特許文献 4】特開 2 0 0 3 - 3 1 8 8 8 5 号公報

【特許文献 5】特開 2 0 0 3 - 2 9 6 2 9 号公報

【特許文献 6】特開 2 0 0 1 - 3 3 9 5 4 3 号公報

【発明の開示】**【発明が解決しようとする課題】****【0 0 0 3】**

しかし、かかるシステムはパーソナルコンピュータなどのデジタル機器によって生成されたデジタルデータに対して紙文書と同等の原本性を確保するためのものである。元々紙が原本であったものを電子的なデータに置き換えるためには、電子的なデータの内容が紙文書の内容と同じあることを保証しなくてはならない。紙文書がスキャンされた後に画像データが改ざんされたり、他のデータにすりかえられたりする可能性や、紙文書がスキャンされる際に紙文書自体に細工が加えられてその内容が変更されたり、紙文書そのものがすりかえられたりする可能性があるからである。従って、紙文書がスキャンされることによって生成される画像データは証拠としての証明力が低い。

30

【0 0 0 4】

そこで、紙文書がスキャンされることによって生成される画像データに対してタイムスタンプを付すことにより当該画像データの証拠性を担保することが考えられる。特に第三者機関が運営するタイムスタンプサービスによるタイムスタンプの付加は、客観的な証拠として高い信頼性が期待できる。

40

【0 0 0 5】

しかし、タイムスタンプサービスは、一回のタイムスタンプごとに課金する形態で提供されることが多い。したがって、紙文書をスキャンするたびにタイムスタンプサービスの利用を行うのは処理効率の観点からだけでなく、経済的にも非常に効率が悪いという問題がある。

【0 0 0 6】

本発明は、上記の点に鑑みてなされたものであって、タイムスタンプサービスを効率よく利用することにより、紙文書に基づいて生成される画像データの証拠性を低コストで高めることのできる文書電子化装置、文書電子化方法、文書電子化プログラム及び記録媒体の提供を目的とする。

50

【課題を解決するための手段】

【0007】

そこで上記課題を解決するため、本発明は、紙文書を読み取ることにより画像データを生成する文書電子化装置であって、ネットワークを介して接続するタイムスタンプサービスに、複数の前記画像データに対して一つのタイムスタンプの生成を要求するタイムスタンプ要求手段を有することを特徴とする。

【0008】

このような文書電子化装置では、画像データごとにタイムスタンプサービスを利用する必要はない。したがって、タイムスタンプサービスを効率よく利用することにより、紙文書に基づいて生成される画像データの証拠性を低コストで高めることができる。

10

【0009】

また、上記課題を解決するため、本発明は、上記文書電子化装置における文書電子化方法、前記文書電子化方法を前記文書電子化装置に実行させるための文書電子化プログラム、又は前記文書電子化プログラムを記録した記録媒体としてもよい。

【発明の効果】

【0010】

本発明によれば、タイムスタンプサービスを効率よく利用することにより、紙文書に基づいて生成される画像データの証拠性を低コストで高めることのできる文書電子化装置、文書電子化方法、文書電子化プログラム及び記録媒体を提供することができる。

【発明を実施するための最良の形態】

20

【0011】

以下、図面に基づいて本発明の実施の形態を説明する。図1は、第一の実施の形態におけるスキャナ装置の機能構成例を示す図である。図1に示されるようにスキャナ装置10は、スキャン部101、ユーザインタフェース部102、タイムスタンプ部103、データ保存部104及び保存データ配信部105等より構成されている。

【0012】

スキャン部101は、紙文書30上の濃淡情報（紙情報）を電子化する。すなわち、スキャン部101は、紙情報を光学的手法により読み取ることにより当該紙情報をデジタル化し、デジタル化された情報に対して画像フォーマット変換を施すことにより、JPG、TIFF、PDF等の所定の形式による画像データを生成する。

30

【0013】

ユーザインタフェース部102は、ユーザからの指示を受け付けるための各種の入力手段や、操作画面等から構成される。

【0014】

データ保存部104は、スキャン部101によって電子化された画像データを保存すると共に、保存されている画像データに対しハッシュ関数によるメッセージダイジェスト（MD）103を生成し、そのMD（画像データ）に対するタイムスタンプの生成をタイムスタンプ部に要求する。

【0015】

タイムスタンプ部103は、スキャナ装置10とインターネット等のネットワークを介して接続するタイムスタンプサービス60に、データ保存部104によって生成されたMDに対するタイムスタンプの生成を要求する。タイムスタンプサービス60は、例えば、信頼できる第三者機関が運営する、タイムスタンプサービスを提供するシステム又はコンピュータを表現したものである。

40

【0016】

保存データ配信部107は、データ保存部104に保存されている画像データを所定の配信先、例えば、外部装置20へ配信する機能である。配信とは、例えば、ネットワークを通じたファイル転送又はメール転送等が相当する。保存データ配信部107は、画像データと共に当該画像データに対するタイムスタンプ等を配信先に配信する。

【0017】

50

外部装置 20 は、例えば、スキャナ装置 10 において紙文書 30 に基づいて生成された画像データ等を利用者に対して公開するためのファイルサーバ等が相当する。

【0018】

なお、上記各部（タイムスタンプ部 103、データ保存部 104 及び保存データ配信部 105 等）は、スキャナ装置 10 にインストールされたプログラムに基づいて実現される。当該プログラムは、スキャナ装置 10 の出荷時等に予めインストールされていてもよいし、例えば CD-ROM や SD カード等の記録媒体 50 よりスキャナ装置 10 にインストールされてもよい。また、ネットワークを介してダウンロードされてもよい。

【0019】

図 2 は、第一の実施の形態におけるデータの流れを説明するための図である。図 2 において、画像データ 301、302、及び 303 は、それぞれ異なる非図示の紙文書 31、32、33 より読み取られた画像データである。

【0020】

まず、各画像データに対して所定のハッシュ関数（メッセージダイジェスト（MD）関数）が適用され、それぞれの画像データのメッセージダイジェスト（MD）が生成される（S11、S12、S13）。図中では、画像データ 301、302、303 のそれぞれに基づいて MD1、MD2、MD3 が生成されている。続いて、複数の MD が一つのデータとして結合され MD リスト 300 とされる（S14）。続いて、MD リスト 300 のメッセージダイジェストとして MD301 が生成される（S15）。続いて、MD301 に対するタイムスタンプの生成がタイムスタンプサービス 60 に対して要求される（S16）。続いて、タイムスタンプサービス 60 において MD301 に対するタイムスタンプが生成され、生成されたタイムスタンプ TS61 が返信される（S17）。続いて、画像データ 301、302 及び 303 と、MD リスト 300 と、TS61 とが外部装置 20 に送信され、外部装置 20 において管理される（S18）。

【0021】

第一の実施の形態では画像データに基づく MD301 に対してタイムスタンプを付与することにより、画像データの存在した時間と画像データが改ざんされていないことを保証することができ、画像データの証拠性を高めることができる。すなわち、外部装置 20 より画像データ群とタイムスタンプ TS61 と MD リスト 300 とを入手した者は、まず、それぞれの画像データに対する MD を生成し、その MD を結合したデータに対して更に MD を生成する。続いて、生成された MD と、タイムスタンプ TS61 をタイムスタンプサービス 60 の公開鍵で復号したデータとを比較することにより両者が一致すれば、複数の画像データのいずれもが改ざんされていないこと、またタイムスタンプ TS61 によって示される時刻に画像データが存在していたことを検証することができる。

【0022】

また、タイムスタンプサービスは一回のタイムスタンプごとに課金する形態で提供されていることが多い。しかし、第一の実施の形態では画像データごとにタイムスタンプを要求するのではなく、複数の画像データに基づいて一つの MD（MD301）を生成し、その MD301 に対するタイムスタンプを要求する。したがって、タイムスタンプの取得に関する時間的及び経済的なコストを低減させることができる。

【0023】

なお、タイムスタンプによって、スキャンで得られた画像データ群の改ざん検知と時刻保証を行うことはできるが、外部装置 20 に保管しておく情報が画像データ群とタイムスタンプだけでは（すなわち、MD リスト 300 を保管しないと）、一部の画像データが改ざんされた場合、改ざんされた画像データ特定することはできず、一連の画像データの全ての有効性が失われる。そこで、MD リスト 300 も同時に保管しておくことで、改ざんされた画像データを特定できるようにしておくことが望ましい。すなわち、それぞれの画像データの MD を生成し、その各 MD と MD リスト 300 に含まれている各 MD とを比較することで、画像データごとに改ざん検知を行うことができるからである。

【0024】

10

20

30

40

50

図 2 に示したデータフローを実現するスキャナ装置 10 による処理について説明する。図 3 は、第一の実施の形態におけるスキャナ装置の処理手順を説明するためのシーケンス図である。

【0025】

ユーザは、紙文書を ADF (Auto Document Feeder) 等にセットしスキャンの実行を指示する (S101)。その際、紙文書が複数ある場合の、複数の紙文書間の区切りに関し設定等を行う。

【0026】

紙文書間の区切りについて説明する。各紙文書は、必ずしもそれぞれ 1 ページより構成されることが限らない。したがって、例えば 2 ページずつからなる 10 文書 (計 20 枚) を一度にスキャンして 10 個の画像データを生成する、といったようなケースも考えられる。また、例えば 3 ページ、20 ページ、1 ページといったページ数の異なる 3 つの紙文書を一度にスキャンして 3 つの画像データを生成する、というようなケースも考えられる。このような場合、次のような方法で紙文書間の区切りを検出してもよい。

【0027】

a) 単位ページ数をあらかじめスキャナ装置 10 に指示しておく方法。特に、同じページ数の紙文書を複数スキャンする場合に有効となる。図 4 (a) 及び (b) は、ユーザインタフェース部 102 によって表示された、各紙文書のページ数を入力させる表示画面を示す。同じページ数の紙文書を複数スキャンする場合には、図 4 (a) のように、部数とページ数を入力するだけで、紙文書間の区切りを入力できる。また、各紙文書のページ数が異なる場合には、図 4 (b) のように、各紙文書毎にページ数を入力することができる。

【0028】

b) 文書間の区切りに、文書の区切りを示す特殊な紙 (以下、区切り用紙という) を挟み、スキャン部 101 が区切り用紙を判別して紙文書間の区切りを検出する方法。多様な紙文書を一度にスキャンする場合に対応できる。図 5 は、紙文書間の区切りに区切り用紙を挟んだ複数の紙文書の一例を示す。図 5 のように、スキャン部 101 が区切り用紙 35 を検出することで、スキャナ装置 10 が紙文書を区切ることができる。

【0029】

区切り用紙 35 は、スキャン部 101 が、「区切りを示す用紙」であることを認識できる用紙であればよい。例えば、全面黒い紙を区切り用紙としておき、明暗の階調が 256 段階で評価される場合に、スキャン結果の画像データの 95% 以上が 5 階調未満であれば区切りとみなす、というルールを設定しておく。これにより、通常 of 原稿と区切り用紙との区別をすることができる。この場合、紙文書としてスキャンしたい原稿中に、区切り用紙の条件を満たしてしまうものがあると、区切り用紙として誤認識されてしまうケースが考えられるので、区切り用紙の判定条件を複数用意しておき、ユーザがどの区切り用紙を使用するのか、ユーザインタフェース部 102 によって選択できるようにしておくことが好適である。

【0030】

c) その他、紙文書間の区切りを検出する方法はいかなる方法であってもよい。例えば、紙文書の欄外に、1 つの紙文書の最初のページと最後のページを表す所定のマークを付し、スキャン部 101 が該マークを検出することで自動的に紙文書間の区切りを判定するようにしてもよい。また、紙文書の欄外に付されたページ番号を読み取ることで、紙文書間の区切りを検出してもよい。

【0031】

紙文書間の区切りの設定が終了し、スキャンの開始が指示されると、ユーザインタフェース部 102 はスキャン部 101 にスキャン要求を行う (S102)。スキャン部 101 は、紙文書 31 の第 1 ページからスキャンを開始し、上述した紙文書間の区切りまで (紙文書 31 のスキャンが終了するまで) スキャンを実行する (S103)。紙文書 31 のスキャンが終了したら、スキャン部 101 はデータ保存部 104 に画像データ 301 を出力

10

20

30

40

50

し (S 1 0 4)、データ保存部 1 0 4 は紙文書 3 1 の画像データ 3 0 1 を記憶する (S 1 0 5)。データ保存部 1 0 4 は、紙文書 3 1 の記憶が成功したら、成功を示す信号をスキャン部 1 0 1 に出力する (S 1 0 6)。

【 0 0 3 2 】

紙文書 3 1 の画像データ 3 0 1 がデータ保存部 1 0 4 に記憶されたら、データ保存部 1 0 4 は、紙文書 3 1 の画像データのメッセージダイジェスト M D 1 を生成し (S 1 0 7)、生成された M D 1 を保持しておく (S 1 0 8)。以降は、A D F にセットされた他の紙文書 3 2 ~ 紙文書 3 n のスキャンが終了するまでスキャンが実行され、更にデータ保存部 1 0 4 に記憶された画像データの M D 2 ~ M D n が順次生成され、保持される (S 1 0 9 ~ S 1 1 7)。

10

【 0 0 3 3 】

全ての紙文書のスキャンが終了すると、スキャン部 1 0 1 は、データ保存部 1 0 4 に対してスキャンの完了を通知する (S 1 1 8)。データ保存部 1 0 4 は、スキャンの完了通知に応じ、これまでに保持されている M D 1 ~ M D n を連結して、M D リスト 3 0 0 を生成する (S 1 1 9)。更に、データ保存部 1 0 4 は、M D リスト 3 0 0 のメッセージダイジェスト M D 3 0 1 を生成する (S 1 2 0)。続いて、データ保存部 1 0 4 は、M D 3 0 1 をタイムスタンプ部 1 0 3 に出力し、M D 3 0 1 に対するタイムスタンプの生成を要求する (S 1 2 1)。

【 0 0 3 4 】

タイムスタンプ部 1 0 3 が、M D 3 0 1 を伴ってタイムスタンプサービス 6 0 に対してタイムスタンプの生成を要求すると (S 1 2 2)、タイムスタンプサービス 6 0 は、例えば、M D 3 0 1 と現在時刻を示すデータとをタイムスタンプサービス 6 0 の秘密鍵で暗号化することにより電子署名 (タイムスタンプ T S 6 1) を生成し (S 1 2 3)、生成したタイムスタンプ T S 6 1 をタイムスタンプ部 1 0 3 に対して返信する (S 1 2 4)。タイムスタンプ部 1 0 3 は、返信されたタイムスタンプ T S 6 1 をデータ保存部 1 0 4 に出力する (S 1 2 5)。

20

【 0 0 3 5 】

データ保存部 1 0 4 が、タイムスタンプ T S 6 1 と、紙文書 3 1 ~ 3 n に対するそれぞれの画像データと、M D リスト 3 0 0 との配信を保存データ配信部 1 0 5 に要求すると (S 1 2 6)、保存データ配信部 1 0 5 はそれらを外部装置 2 0 に対して送信する (S 1 2 7)。外部装置 2 0 は、受信したタイムスタンプ T S 6 1 と、紙文書 3 1 ~ 3 n に対するそれぞれの画像データと、M D リスト 3 0 0 とを関連付けて保存すると (S 1 2 8)、保存に成功した旨を返信する (S 1 2 9)。画像データ等の保存に成功した旨は、保存データ配信部 1 0 5、データ保存部 1 0 4 及びスキャン部 1 0 1 を介してユーザインタフェース部 1 0 2 に通知され (S 1 3 0、S 1 3 1、S 1 3 2)、ユーザインタフェース部 1 0 2 が操作パネルにメッセージを表示させることにより、ユーザに通知される (S 1 3 3)。

30

【 0 0 3 6 】

次に、第二の実施の形態について説明する。図 6 は、第二の実施の形態におけるスキャナ装置の機能構成例を示す図である。図 6 中、図 1 と同一部分には同一符号を付し、その説明は省略する。

40

【 0 0 3 7 】

図 6 においては、機器署名部 1 0 6 が新たに追加されている。機器署名部 1 0 6 は、データ保存部 1 0 4 において画像データごとに生成される M D 1 ~ M D n のそれぞれを、スキャナ装置 1 0 固有の暗号鍵 (秘密鍵) (以下「機器秘密鍵」という。) によって暗号化 (例えば R S A 暗号) することにより画像データの電子署名を生成する機能である。なお、機器署名部 1 0 6 によって生成される画像データごとの電子署名を以下「機器署名」という。

【 0 0 3 8 】

図 7 は、第二の実施の形態におけるデータの流れを説明するための図である。図 7 中、

50

図 2 と同一部分には同一符号を付し、その説明は適宜省略する。

【 0 0 3 9 】

第二の実施の形態では、画像データごとの MD 1 ~ n に基づいて機器署名 1 ~ n が生成され (S 1 9 、 S 2 0 、 S 2 1) 、外部装置 2 0 に保管される (S 2 2) 。したがって、第二の実施の形態によれば、時刻保証及び改ざん検知に加え、外部装置 2 0 に保管されている各画像データが特定のスキャナ装置 1 0 においてスキャンされたことを検証することができる。検証は、各機器署名をスキャナ装置 1 0 の公開鍵によって復号したものと、各画像データに基づく MD とを比較すればよい。両者が一致すれば、改ざんされていないこと及びスキャナ装置 1 0 においてスキャンされたことが検証されたことになる。

【 0 0 4 0 】

図 7 に示したデータフローを実現するスキャナ装置 1 0 による処理について説明する。図 8 は、第二の実施の形態におけるスキャナ装置の処理手順を説明するためのシーケンス図である。図 8 中、図 3 と同一ステップには同一符号を付し、その説明は省略する。

【 0 0 4 1 】

第二の実施の形態において、データ保存部 1 0 4 は、各画像データについて MD を生成するたびに、その MD を機器署名部 1 0 6 に出力し、機器署名の生成を要求する (S 2 0 1 、 S 2 0 4 、 S 2 0 7) 。機器署名部 1 0 6 は、機器秘密鍵でそれぞれの MD を暗号化することにより機器署名を生成し (S 2 0 2 、 S 2 0 5 、 S 2 0 8) 、生成された機器署名をデータ保存部 1 0 4 に出力する (S 2 0 3 、 S 2 0 6 、 S 2 0 9) 。

【 0 0 4 2 】

その後、ステップ S 1 2 7 において、保存データ配信部 1 0 5 が、タイムスタンプ T S 6 1 と、紙文書 3 1 ~ 3 n に対するそれぞれの画像データと、MD リスト 3 0 0 と、機器署名 1 ~ n とを外部装置 2 0 に対して送信すると、それらの情報が外部装置 2 0 において関連付けられて保存される (S 1 2 8) 。その他の処理については、第一の実施の形態と同様である。

【 0 0 4 3 】

次に、第三の実施の形態について説明する。図 9 は、第三の実施の形態におけるスキャナ装置の機能構成例を示す図である。図 9 中、図 6 と同一部分には同一符号を付し、その説明は省略する。

【 0 0 4 4 】

図 9 においては、カード入出力部 1 0 7 及びユーザ署名部 1 0 8 が新たに追加されている。カード入出力部 1 0 7 は、例えば、IC カードリーダライタとそのドライバソフトとを含み、スキャナ装置 1 0 と IC カード 4 0 とを物理的及び論理的に仲介する。IC カード 4 0 は、例えば、各ユーザに配布されている IC カードであり、内部のフラッシュ ROM 等に当該ユーザに固有 (すなわち、当該 IC カードに固有) の暗号鍵 (秘密鍵) (以下「ユーザ秘密鍵」という。) と、ユーザ秘密鍵に対する公開鍵証明書 (以下「ユーザ公開鍵証明書」という。) とが記録されている。ユーザ公開鍵証明書は、ユーザ秘密鍵に対する公開鍵 (以下「ユーザ公開鍵」という。) 等が含まれている情報であり、予め認証機関によって発行されているものである。

【 0 0 4 5 】

ユーザ署名部 1 0 8 は、ユーザ秘密鍵によって画像データごとの MD を暗号化することにより画像データの電子署名を生成する機能である。ユーザ署名部 1 0 5 によって生成された電子署名を以下「ユーザ署名」という。なお、厳密には、ユーザ署名部 1 0 5 は、ユーザ秘密鍵が記録されている IC カード 4 0 にユーザ署名の生成処理を行わせる。セキュリティ上の観点よりユーザ秘密鍵は IC カード 4 0 の外部に取り出すことができないように管理されているからである。

【 0 0 4 6 】

図 1 0 は、第三の実施の形態におけるデータの流れを説明するための図である。図 1 0 中、図 7 と同一部分には同一符号を付し、その説明は適宜省略する。

【 0 0 4 7 】

10

20

30

40

50

第三の実施の形態では、ＩＣカード４０によってＭＤ３０１に基づいてユーザ署名が生成され（Ｓ２３、Ｓ２４）、外部装置２０に保管される（Ｓ２５）。したがって、第三の実施の形態によれば、第一及び第二の実施の形態による効果に加え、画像データが特定のユーザの操作によってスキャンされたことを検証することができる。検証は、ユーザ署名をユーザ公開鍵によって復号したものと、各画像データに基づいて生成したＭＤの結合データのＭＤとを比較すればよい。両者が一致すれば、改ざんされていないこと及び特定のユーザによってスキャンされたことが検証されたことになる。

【００４８】

図１０に示したデータフローを実現するスキャナ装置１０による処理について説明する。図１１は、第三の実施の形態におけるスキャナ装置の処理手順を説明するためのシーケンス図である。図１１中、図８と同一ステップには同一符号を付し、その説明は省略する。

10

【００４９】

第三の実施の形態において、データ保存部１０４は、ユーザ署名部１０８にＭＤ３０１を出力すると共に、ユーザ署名の生成を要求する（Ｓ３０１）。ユーザ署名部１０８は、ＭＤ３０１を、カード入出力部１０７を介してＩＣカード４０に送信する。ＩＣカード４０は、内部に保持するユーザ秘密鍵でＭＤ３０１を暗号化してユーザ署名を生成し（Ｓ３０２）、ユーザ署名部１０８に送信する。ユーザ署名部１０８は、ユーザ署名をデータ保存部１０４に出力する（Ｓ３０３）。

【００５０】

その後、ステップＳ１２７において、保存データ配信部１０５が、タイムスタンプＴＳ６１と、紙文書３１～３ｎに対するそれぞれの画像データと、ＭＤリスト３００と、機器署名１～ｎと、ユーザ署名とを外部装置２０に対して送信すると、それらの情報が外部装置２０において関連付けられて保存される（Ｓ１２８）。その他の処理については、第二の実施の形態と同様である。

20

【００５１】

なお、ユーザ署名は、画像データごとのＭＤ（ＭＤ１～ＭＤｎ）のそれぞれをユーザ秘密鍵で暗号化することにより、画像データごとに生成してもよい。但し、一般にＩＣカードに搭載されているＣＰＵの処理能力はそれほど高くないため、処理速度の高速化を考慮すると、第三の実施の形態において説明したように、ＭＤ３０１に基づいて複数の画像データに対して一つ生成するほうが好ましい。

30

【００５２】

ところで、画像データの存在を証明する時刻の正確さは必ずしも秒単位である必要はなく、日単位や月単位でも十分である場合が多い。したがって、タイムスタンプサービス６０に対するタイムスタンプの要求は、ユーザによるスキャン指示の際に即座に実行する必要は必ずしもなく、例えば、毎日一回又は毎月一回といったように定期的に行うようにしてもよい。

【００５３】

また、タイムスタンプの間隔をユーザに指定させるようにしてもよい。図１２は、タイムスタンプの間隔をユーザに指定させるための画面例を示す図である。図１２において、画面１０２３は、ボタン１０２３ａ、１０２３ｂ、１０２３ｃ、及び１０２３ｄのいずれかを選択させることにより、予め用意された候補（１時間、１日、１週間、１ヶ月）の中からタイムスタンプの間隔をユーザに選択させるための画面である。また、画面１０２４では、左右の矢印ボタン１０２４ｂの操作によって、タイムスタンプ間隔表示領域１０２４ａにおけるカーソルの位置が「月」、「日」、「時間」のいずれかに移動する。そして、テンキー１０２４ｃによって入力された値が、カーソルの位置する箇所に入力される。これによって、ユーザはタイムスタンプの間隔を任意に設定することができる。

40

【００５４】

また、毎日０：００といったように時刻を指定させるようにしてもよい。

【００５５】

50

なお、画面 1 0 2 3 及び 1 0 2 4 はいずれもユーザインタフェース部 1 0 2 によって表示される。但し、スキャナ装置 1 0 に液晶パネル等が無い場合は、例えばネットワーク経由で Web ブラウザ等から同様の設定を可能としてもよい。

【 0 0 5 6 】

設定された値はデータ保存部 1 0 4 によって管理される。データ管理部 1 0 4 は、時刻を監視し、設定された値に応じた時刻になるとそれまでにスキャンされたすべての画像データに基づく M D 3 0 1 に対するタイムスタンプの生成をタイムスタンプ部 1 0 3 に要求する。

【 0 0 5 7 】

以上、本発明の実施例について詳述したが、本発明は係る特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。

【図面の簡単な説明】

【 0 0 5 8 】

【図 1】第一の実施の形態におけるスキャナ装置の機能構成例を示す図である。

【図 2】第一の実施の形態におけるデータの流れを説明するための図である。

【図 3】第一の実施の形態におけるスキャナ装置の処理手順を説明するためのシーケンス図である。

【図 4】各紙文書のページ数を入力させる表示画面の一例である。

【図 5】紙文書間の区切りに区切り用紙を挟んだ複数の紙文書の一例である。

【図 6】第二の実施の形態におけるスキャナ装置の機能構成例を示す図である。

【図 7】第二の実施の形態におけるデータの流れを説明するための図である。

【図 8】第二の実施の形態におけるスキャナ装置の処理手順を説明するためのシーケンス図である。

【図 9】第三の実施の形態におけるスキャナ装置の機能構成例を示す図である。

【図 1 0】第三の実施の形態におけるデータの流れを説明するための図である。

【図 1 1】第三の実施の形態におけるスキャナ装置の処理手順を説明するためのシーケンス図である。

【図 1 2】タイムスタンプの間隔をユーザに指定させるための画面例を示す図である。

【符号の説明】

【 0 0 5 9 】

1 0	スキャナ装置
2 0	外部装置
3 0	紙文書
4 0	I C カード
5 0	記録媒体
6 0	タイムスタンプサービス
1 0 1	スキャン部
1 0 2	ユーザインタフェース部
1 0 3	タイムスタンプ部
1 0 4	データ保存部
1 0 5	保存データ配信部
1 0 6	機器署名部
1 0 7	カード入出力部
1 0 8	ユーザ署名部

10

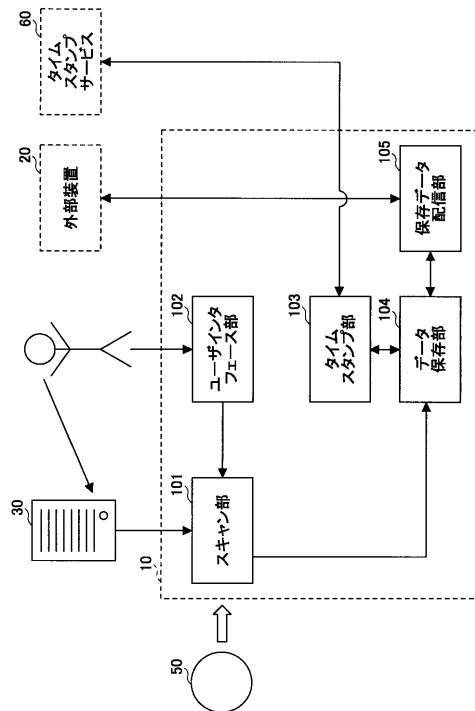
20

30

40

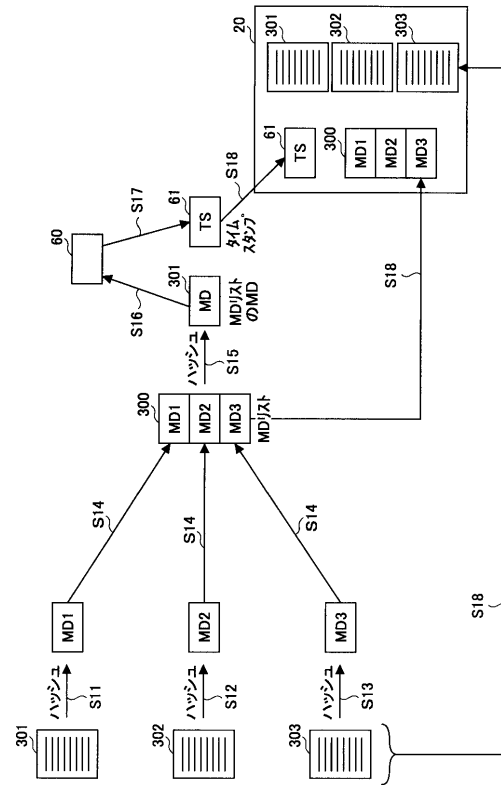
【図 1】

第一の実施の形態におけるスキャナ装置の機能構成例を示す図

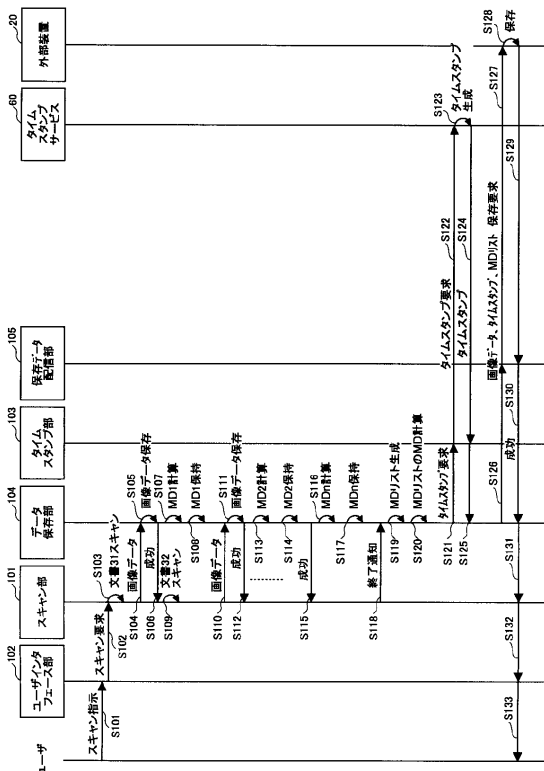


【図 2】

第一の実施の形態におけるデータの流れを説明するための図

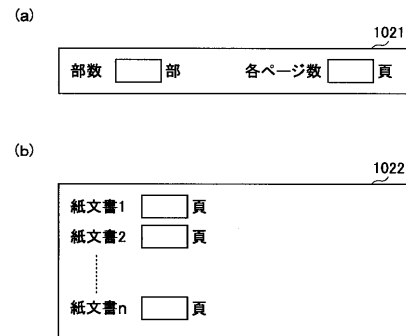


【図 3】

第一の実施の形態における
スキャナ装置の処理手順を説明するためのシーケンス図

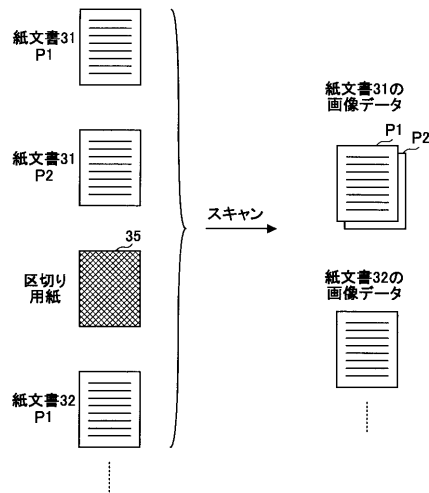
【図 4】

各紙文書のページ数を入力させる表示画面の一例



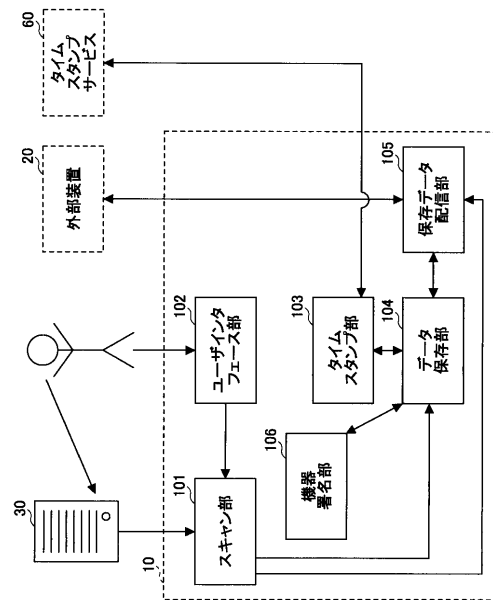
【 図 5 】

紙文書間の区切りに区切り用紙を挟んだ複数の紙文書の一例



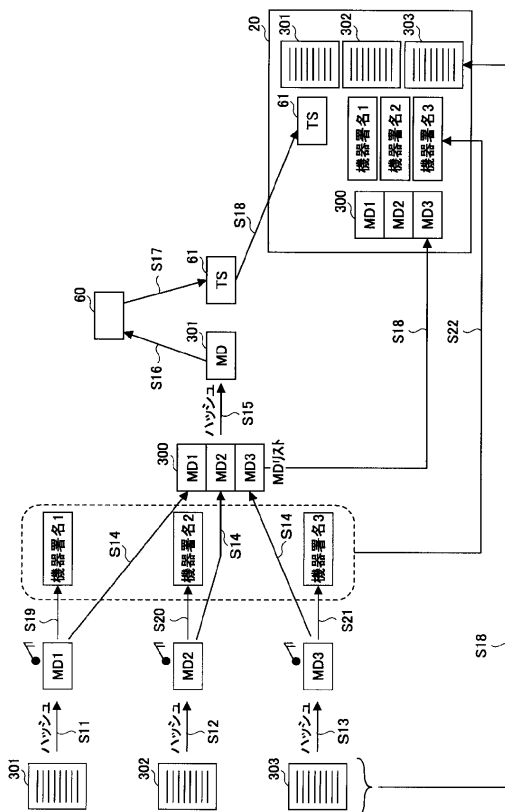
【 図 6 】

第二の実施の形態におけるスキャナ装置の機能構成例を示す図



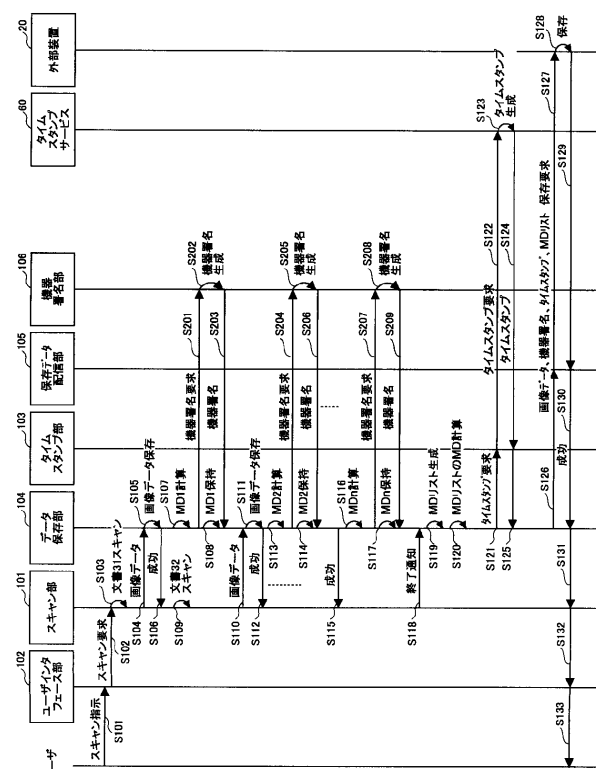
【圖 7】

第二の実施の形態におけるデータの流れを説明するための図



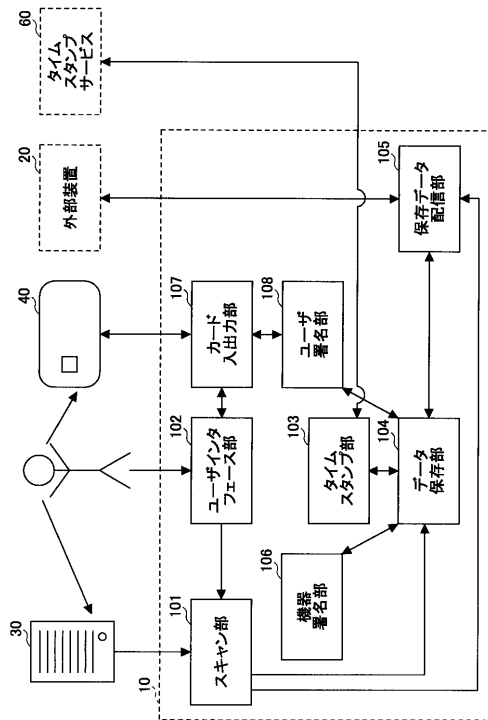
【圖 8】

第二の実施の形態における
スキャナ装置の処理手順を説明するためのシーケンス図



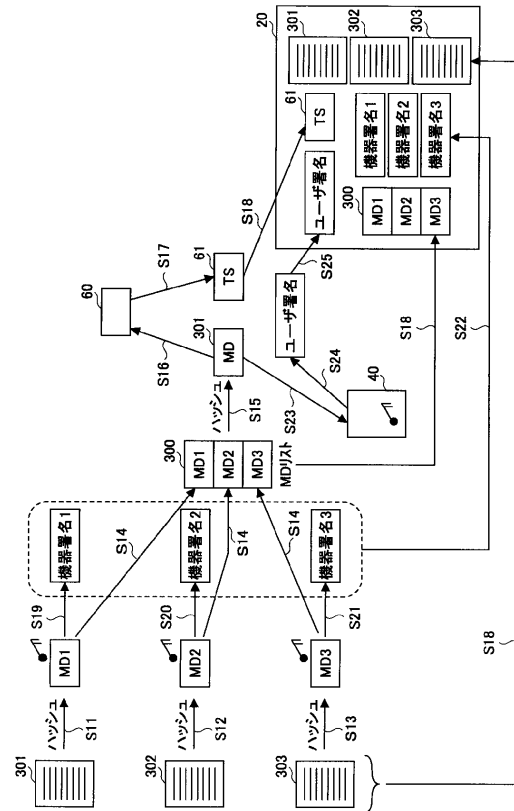
【図 9】

第三の実施の形態におけるスキャナ装置の機能構成例を示す図

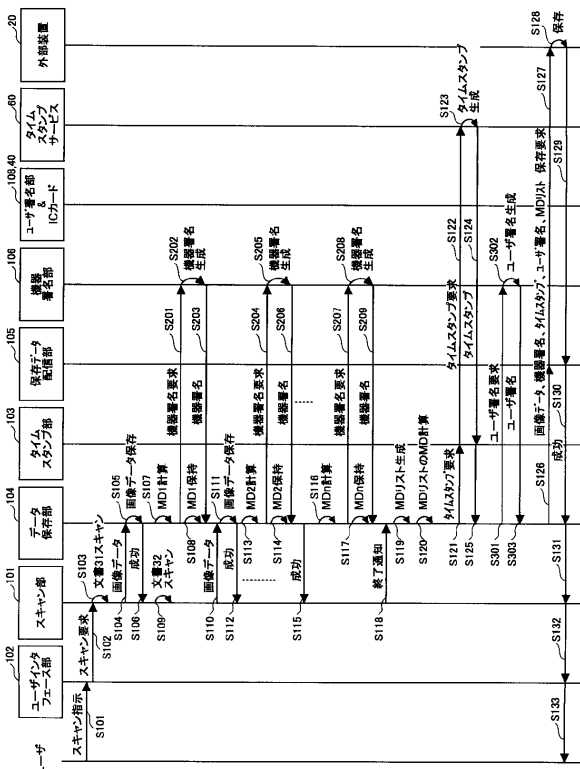


【図 10】

第三の実施の形態におけるデータの流れを説明するための図



【図 11】

第三の実施の形態における
スキャナ装置の処理手順を説明するためのシーケンス図

【図 12】

タイムスタンプの間隔をユーザに指定させるための画面例を示す図

