

明 細 書

発明の名称： 情報処理装置、方法、及びプログラム

技術分野

[0001] 本開示は、情報処理装置、方法、及びプログラムに関する。

背景技術

[0002] 紙の契約書を用いるのに代えて、デジタルデータを用いる試みがなされている。デジタルデータでは、改変が無いことを証明することを目的として、電子署名を用いることが知られている。例えば、署名対象データに電子署名を行う電子署名システムが提案されている（例えば、特許文献1 参照）。

先行技術文献

特許文献

[0003] 特許文献1：特開2018-067807号公報

発明の概要

発明が解決しようとする課題

[0004] 特許文献1の電子署名システムでは、電子署名に含まれるデジタルデータのハッシュ値と、閲覧時におけるデジタルデータのハッシュ値とを比較する。比較の結果、ハッシュ値の値が異なる場合に、デジタルデータが改変されたと判断する。これにより、デジタルデータの改変を検出することができる。

[0005] 一方、特許文献1の電子署名システムでは、秘密鍵を用いて電子署名をするため、秘密鍵を管理する必要や、対応する公開鍵を取得する必要がある。また、電子署名は、通常不可視であるため、電子署名が用いられているのか否かを直感的に判断することができなかった。そして、電子署名が真正であることが確認できても、電子文書の内容を確認することができなかった。

[0006] 本発明は、上記従来の実状に鑑みてなされたものであり、電子文書の真正性が担保される環境下で電子文書の内容を確認することが可能な情報処理装置、方法、及びプログラムを提供することを目的とする。

課題を解決するための手段

[0007] 本発明の実施形態に係る情報処理装置は、ユーザの電子文書に付与された電子署名に基づいて、電子文書のハッシュ値を含む第1管理ファイルを識別するための第1管理ファイル識別子を取得する第1管理ファイル識別子取得部と、取得した第1管理ファイル識別子に基づいて、第1管理ファイルを取得する第1管理ファイル取得部と、第1管理ファイルに含まれるハッシュ値に基づいて、ハッシュ値と電子文書が記憶された記憶領域を特定するためのURLとを含む第2管理ファイルを取得する第2管理ファイル取得部と、URLを出力するURL出力部と、を備える。

発明の効果

[0008] 本発明によれば、電子文書の真正性が担保される環境下で電子文書の内容を確認することが可能となる。

図面の簡単な説明

[0009] [図1]実施形態に係る署名生成装置を用いた電子署名システムの概要を示す概略図である。

[図2]実施形態に係る署名生成装置によって生成された電子署名を付した電子文書を示す概略図である。

[図3]実施形態に係る署名生成装置1の構成を示すブロック図である。

[図4]実施形態に係る閲覧装置100の構成を示すブロック図である。

[図5]実施形態に係る管理ファイルのデータ構造の一例を示す概略図である。

[図6]実施形態に係る閲覧装置100が実行する処理の一例を示す動作フロー図である。

[図7]実施形態に係る第1画面G1の一例を示す概略図である。

[図8]実施形態に係る第2画面G2の一例を示す概略図である。

[図9]実施形態に係る第3画面G3の一例を示す概略図である。

発明を実施するための形態

[0010] 添付図面を参照して、本発明の好適な実施形態について説明する。（なお

、各図において、同一の符号を付したものは、同一又は同様の構成を有する。
。)

[0011] <概要>

図1は、実施形態に係る署名生成装置を用いた電子署名システムの概要を示す概略図である。図2は、実施形態に係る署名生成装置によって生成された電子署名を付した電子文書を示す概略図である。

[0012] 図1に示すとおり、電子署名システムは、例えば、署名生成装置1、電子文書データベース2、閲覧装置100、及び外部ネットワークN等を含む。

[0013] 署名生成装置1は、例えば、サーバ等の情報処理装置である。署名生成装置1は、ユーザ（例えば、法人等）の契約書等の電子文書Dに対して、電子署名Sを生成する装置である。電子文書Dは、例えば、電子文書データベース2に保存されている。すなわち、署名生成装置1は、ユーザの電子文書Dに付与する電子署名Sを生成する装置である。署名生成装置1は、例えば、電子署名Sを電子文書Dに視認可能に付与することで、電子文書Dへの同意を示した電子文書Dを作成する。以下の実施形態では、署名生成装置1は、秘密鍵を用いずに電子署名Sを作成することにより、秘密鍵の漏洩を抑制して容易に電子文書Dの証明をすることができる。

[0014] なお、以下の実施形態において、「電子文書」とは、契約書、見積書、申込書、注文書、納品書、請求書、領収書、送り状、議事録、稟議書、申請書等のうち、電子的に作成された文章をいう。また、「電子署名」とは、紙の契約書等に押印をする行為を電子文書Dに対して電子的に実施する処理をいう。

[0015] 署名生成装置1は、図1に示すように、外部ネットワークNに接続される。署名生成装置1は、電子署名Sを付与した電子文書Dの管理ファイルを作成する。署名生成装置1は、作成した電子文書Dの管理ファイルを外部ネットワークNに保持する。外部ネットワークNは、例えば、ブロックチェーンを記憶する複数のノードコンピュータから構成されてもよい。ブロックチェーンの形式は、特に限定されないが、例えばコンソーシアム型のプライベート

トブロックチェーンとして構成されてもよい。署名生成装置 1 は、例えば、管理ファイルを当該ブロックチェーン等として構成される外部ネットワーク N に保持する。電子文書 D について、保存された管理ファイルと電子文書 D に書き込まれた電子署名 S との同一性を確認することにより、電子文書 D の改ざんが無いことを確認することができる。

[0016] 特に、署名生成装置 1 は、図 2 に示すように、電子文書 D に対して視認可能な電子署名 S を付与する。署名生成装置 1 は、例えば、2 名のユーザ（契約者）それぞれに対応した電子署名 S を視認可能に付与する。署名生成装置 1 は、例えば、電子文書 D に、QR コード（登録商標）として示される電子署名 S を付与する。

[0017] 閲覧装置 100 は、例えば、署名生成装置 1 とは異なる装置として構成される。閲覧装置 100 は、例えば、撮像機能を有するスマートフォン、タブレット端末、パーソナルコンピュータ等の情報処理装置である。閲覧装置 100 は、署名生成装置 1 によって生成された電子署名 S に基づいて、外部ネットワーク N に保持された管理ファイルを取得し、取得した管理ファイルに含まれる情報に基づいて、電子文書 D の真正性を確認するための認証処理を実行する。また、閲覧装置 100 は、取得した管理ファイルに含まれる情報に基づいて、各種の情報の表示処理を実行する。特に、閲覧装置 100 は、電子文書データベース 2 において電子文書 D が記憶された記憶領域を特定するための URL を表示する。ユーザが当該 URL を選択すると、閲覧装置 100 は、電子文書 D を電子文書データベース 2 から取得し、これを表示する。これにより、電子文書 D の真正性が担保される環境下で電子文書 D の内容を確認することが可能となる。更に、電子署名 S から電子文書 D の内容を確認できるので、ユーザは、電子文書 D のファイルではなく、電子文書 D をプリントアウトした紙等を保管することによっても、（管理ファイル上の情報による裏付けのある）証拠力を保持することが可能となる。

[0018] <構成>

<<署名生成装置 1>>

図3は、実施形態に係る署名生成装置1の構成を示すブロック図である。署名生成装置1は、文書取得部11と、指示取得部12と、ユーザ情報取得部13と、署名生成部14と、付与部15と、算出部16と、保持部17と、電子文書出力部18と、修正部19とを備える。

[0019] 文書取得部11は、例えば、CPUが動作することにより実現される。文書取得部11は、電子文書Dを取得する。文書取得部11は、例えば、契約書等の電子データを電子文書Dとして取得する。文書取得部11は、例えば、電子文書Dとして、紙のデータをスキャンしたデータ、ブラウザ又はアプリケーションを用いて作成されたデータ等を取得する。また、文書取得部11は、例えば、修正版の電子文書Dを取得する。

[0020] 指示取得部12は、例えば、CPUが動作することにより実現される。指示取得部12は、署名対象となる、取得された電子文書Dに対する署名の作成指示を取得する。指示取得部12は、例えば、契約対象となるユーザから電子署名Sの作成指示を取得する。また、例えば、指示取得部12は、修正対象となるオリジナルの電子文書Dを識別する情報を識別情報として取得する。また、指示取得部12は、電子文書Dの修正指示を取得する。

[0021] ユーザ情報取得部13は、例えば、CPUが動作することにより実現される。ユーザ情報取得部13は、ユーザの情報をユーザ情報として取得する。また、本実施形態において、ユーザ情報取得部13は、予め発行されるユーザのユーザIDとユーザ名とを取得する。ここで、ユーザ情報取得部13は、ユーザ情報として、契約者（利用者）同士のユーザID及びユーザ名を取得する。また、本実施形態において、ユーザ情報取得部13は、2法人のユーザのそれぞれから、電子署名Sを生成する際に、ユーザ情報を取得する。

[0022] 署名生成部14は、例えば、CPUが動作することにより実現される。署名生成部14は、署名時刻を示す時刻情報とユーザを識別する識別情報とを含むコード化された電子署名Sを生成する。署名生成部14は、例えば、時刻情報及びユーザ情報（ユーザID）を含むQRコードを生成する。また、署名生成部14は、取得された作成指示に基づいて、ユニークな文字情報を

生成するとともに、電子署名Sに、生成された文字情報を署名情報として含む電子署名Sを生成する。これにより、署名生成部14は、電子署名Sの生成ごとに異なる文字情報を生成する。また、例えば、署名生成部14は、修正版の電子文書Dに対して、新たな電子署名Sを作成する。署名生成部14は、例えば、新たなユニークな文書情報を含む電子署名Sを作成する。なお、電子署名Sが含むユニークな文字情報は、後述する第1管理ファイル識別子に含まれる。

[0023] 付与部15は、例えば、CPUが動作することにより実現される。付与部15は、生成された電子署名Sを電子文書Dに視認可能に付与する。付与部15は、例えば、図2に示すように、電子文書Dに記載されているユーザの情報である法人名及び代表者の氏名に対して、並べて表示される位置に作成された電子署名Sを付与する。付与部15は、例えば、電子文書Dのうち、記載されているユーザの情報に対応する電子署名Sであることがわかる位置に、電子署名Sを記載する。本実施形態において、付与部15は、取得されたユーザ情報に含まれるユーザの名前を電子署名Sに併記する。付与部15は、例えば、図2に示すように、対応するユーザの電子署名S（QRコード）に対して、電子文書Dの表示面下方にユーザ名を併記する。また、付与部15は、全てのユーザに対する電子署名Sの付与の後に、電子文書Dに対してタイムスタンプを付与する。また、付与部15は、例えば、修正後の電子文書Dに対して、新たに生成された電子署名Sを書き込む。また、付与部15は、例えば、修正後の電子文書Dに対して、新たに生成された電子署名Sの署名時刻を示す時刻情報を書き込む。

[0024] 算出部16は、例えば、CPUが動作することにより実現される。算出部16は、電子文書Dのハッシュ値を算出する。算出部16は、例えば、全てのユーザに電子署名Sを付与した後の電子文書Dについて、ハッシュ値を算出する。また、算出部16は、例えば、修正後の電子文書Dのハッシュ値を算出する。

[0025] 保持部17は、例えば、CPUが動作することにより実現される。保持部

17は、署名情報及び時刻情報について、電子文書Dを管理する管理ファイルとして保持する。保持部17は、例えば、ユーザID、ユーザ名、署名情報、署名の日時、及び電子文書Dのハッシュ値について、電子文書Dとは別の管理ファイルとして保持する。具体的には、保持部17は、契約者それぞれのユーザID及びユーザ名、署名情報、署名の日時、並びに電子文書Dのハッシュ値について、電子文書Dとは別の管理ファイルとして保存する。保持部17は、外部ネットワークNに、管理ファイルを保持する。本実施形態において、保持部17は、ブロックチェーンに管理ファイルを保持する。保持部17は、例えば、識別子によって示されるアドレスの位置に管理ファイルを保持する。また、保持部17は、管理ファイルに、少なくとも算出されたハッシュ値を保持する。保持部17は、例えば、ユーザID、ユーザ名、新たな署名情報、時刻情報、及びハッシュ値について、電子文書Dを管理する管理ファイルに保持する。保持部17は、例えば、修正前の管理ファイルに紐づけて、修正後の管理ファイルを保持する。

[0026] 電子文書出力部18は、例えば、CPUが動作することにより実現される。電子文書出力部18は、書き込まれた署名情報及び時刻情報を含む電子文書Dを出力する。電子文書出力部18は、例えば、ディスプレイ等の表示装置（図示せず）に、署名情報及び時刻情報を含む電子文書Dを出力する。また、電子文書出力部18は、所定の記憶装置に、電子署名Sの付与された電子文書Dを格納する。

[0027] 修正部19は、例えば、CPUが動作することにより実現される。修正部19は、電子文書Dの内容を修正する。修正部19は、修正版の電子文書Dに基づいて、識別された電子文書Dを修正する。修正部19は、例えば、管理ファイルに保持されているユーザID、ユーザ名、電子署名S、及び署名の日時によって修正対象の電子文書Dを識別する。

[0028] 署名生成装置1による電子署名Sの生成処理は、例えば次のように実行される。まず、文書取得部11は、電子文書データベース2から電子文書Dを取得する。次いで、ユーザ情報取得部13は、ユーザ情報を取得する。次い

で、指示取得部 12 は、電子署名 S の作成指示を取得する。次いで、署名生成部 14 は、電子署名 S を生成する。次いで、付与部 15 は、電子署名 S 及び署名時刻を電子文書 D に書き込む。そして、保持部 17 は、契約者それぞれのユーザ ID 及びユーザ名、署名情報、署名の日時、並びに電子文書 D のハッシュ値について、電子文書 D とは別の管理ファイルとして保存する。以上で、電子署名 S の生成処理が終了する。

[0029] 署名生成装置 1 による電子文書 D の修正処理は、例えば次のように実行される。まず、文書取得部 11 が修正版の電子文書 D を取得した場合、指示取得部 12 は、修正指示を取得する。次いで、修正部 19 は、電子文書 D を修正する。次いで、付与部 15 は、電子署名 S 及び署名時刻を電子文書 D に書き込む。次いで、算出部 16 は、修正された電子文書 D のハッシュ値を算出する。次いで、保持部 17 は、修正された電子文書 D に関するユーザ ID、ユーザ名、署名情報、署名時刻、及びハッシュ値を管理ファイルに保持する。以上で、電子文書 D の修正処理が終了する。

[0030] 署名生成装置 1 に含まれる各構成は、ハードウェア、ソフトウェア又はこれらの組み合わせによりそれぞれ実現することができる。ここで、ソフトウェアによって実現されるとは、コンピュータがプログラムを読み込んで実行することにより実現されることを意味する。プログラムは、様々なタイプの非一時的なコンピュータ可読媒体 (non-transitory computer readable medium) を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体 (tangible storage medium) を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体 (例えば、フレキシブルディスク、磁気テープ、ハードディスクドライブ)、光磁気記録媒体 (例えば、光磁気ディスク)、CD-ROM (Read Only Memory)、CD-R、CD-R/W、半導体メモリ (例えば、マスク ROM、PROM (Programmable ROM)、EPROM (Erasable PROM)、フラッシュ ROM、RAM (ra

ndom access memory)) を含む。また、表示プログラムは、様々なタイプの一時的なコンピュータ可読媒体 (transitory computer readable medium) によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。

[0031] 以上、本実施形態に係る署名生成装置 1 及びプログラムによれば、以下の効果を奏する。(1) ユーザの電子文書 D に付与する電子署名 S を生成する署名生成装置 1 であって、電子文書 D を取得する文書取得部 11 と、取得された電子文書 D に対する署名の作成指示を取得する指示取得部 12 と、署名時刻を示す時刻情報とユーザを識別する識別情報とを含むコード化された電子署名 S を生成する署名生成部 14 と、生成された電子署名 S を電子文書 D に視認可能に付与する付与部 15 と、を備える。

(2) また、ユーザの電子文書 D に付与する電子署名 S を生成する署名生成装置 1 としてコンピュータを動作させるプログラムであって、コンピュータを、電子文書 D を取得する文書取得部 11、取得された電子文書 D に対する署名の作成指示を取得する指示取得部 12、署名時刻を示す時刻情報とユーザを識別する識別情報とを含むコード化された電子署名 S を生成する署名生成部 14、生成された電子署名 S を電子文書 D に視認可能に付与する付与部 15、として機能させる。

これにより、電子署名 S を視認可能に電子文書 D に付与することができる。したがって、電子文書 D に電子署名 S が付与されていることを容易に識別することができる。また、電子署名 S をコード化することで、電子署名 S に含まれる各種情報を容易に取り出すことができるようになる。したがって、電子署名 S を容易に扱うことが可能となる。

[0032] (3) 署名生成装置 1 は、電子文書 D のハッシュ値を算出する算出部 16 と、時刻情報及びハッシュ値について、電子文書 D を管理する管理ファイルに

保持する保持部 17 と、をさらに備え、管理ファイルにおいて、電子文書 D に付与された時刻情報及び電子文書 D のハッシュ値を示す管理ファイルを識別する識別子を含む電子署名 S を生成する。これにより、電子署名 S から管理ファイルを識別することができるので、管理ファイルの検索を容易にすることができる。また、電子文書 D と管理ファイルとの対比を容易にすることができる。したがって、電子文書 D の改ざんの有無を容易に確認することができる。

[0033] (4) 署名生成装置 1 は、ユーザの情報をユーザ情報として取得するユーザ情報取得部 13 をさらに備え、署名生成部 14 は、取得されたユーザ情報を含む電子署名 S を生成する。これにより、ユーザごとに電子文書 D を管理することができる。

[0034] (5) 付与部 15 は、取得されたユーザ情報に含まれるユーザの名前を電子署名 S に併記する。これにより、コード化された電子署名 S について、いずれのユーザの電子署名 S かを明確にすることができる。また、コード化された電子署名 S に併記されることで、コードを印影のように扱うことができるので、紙への印鑑の捺印のような視覚的な効果を得ることができる。

[0035] (6) 保持部 17 は、管理ファイルを外部ネットワーク N に保持する。これにより、署名生成装置 1 が保持する場合に比べ、管理ファイルが喪失されることを抑制できる。したがって、電子文書 D と管理ファイルとの照合が不能になることを抑制できる。

[0036] (7) 署名生成装置 1 は、電子文書 D の内容を修正する修正部 19 をさらに備え、文書取得部 11 は、電子文書 D の修正内容を取得し、付与部 15 は、修正後の電子文書 D に対して、署名情報と修正後の署名時刻を示す時刻情報とを修正後の電子文書 D に書き込み、算出部 16 は、修正後の電子文書 D のハッシュ値を算出し、保持部 17 は、管理ファイルに、少なくとも算出されたハッシュ値を保持する。これにより、算出されたハッシュ値と、修正後の電子文書 D との同一性を担保することができる。したがって、修正があった後でも、改変の有無を判断可能にすることができる。

[0037] <<閲覧装置 100>>

図4は、実施形態に係る閲覧装置100の構成を示すブロック図である。

閲覧装置100は、撮像部101と、識別子取得部102と、保持情報取得部103と、ハッシュ値算出部104と、整合性確認部105と、出力部106と、操作受付部107を備える。

[0038] 撮像部101は、いわゆるカメラを含む撮像機構である。撮像部101は、例えば、電子文書Dに付与されている電子署名Sを撮像する。撮像部101は、例えば、他の端末の表示部（図示せず）に表示されている電子文書Dに含まれる電子署名Sを撮像する。

[0039] 識別子取得部102は、例えば、CPUが動作することにより実現される。識別子取得部102は、電子署名S（QRコード）の撮像により、電子署名Sに含まれるユニークな文字情報を少なくとも含む第1管理ファイル識別子（第1管理ファイルを識別するための識別子）を取得する。

[0040] 保持情報取得部103は、例えば、CPUが動作することにより実現される。保持情報取得部103は、外部ネットワークNから、各種の管理ファイル（第1管理ファイル、第2管理ファイル、及び第3管理ファイル等）を取得する。

[0041] ハッシュ値算出部104は、例えば、CPUが動作することにより実現される。ハッシュ値算出部104は、電子署名Sを含む電子文書Dのハッシュ値を算出する。

[0042] 整合性確認部105は、例えば、CPUが動作することにより実現される。整合性確認部105は、取得されたハッシュ値と算出されたハッシュ値との整合性を確認する。取得されたハッシュ値と算出されたハッシュ値とが整合した場合、電子文書Dの真正性が一定程度、担保され得る。

[0043] 出力部106は、例えば、CPUが動作することにより実現される。出力部106は、電子文書Dに関する各種の情報を出力する。例えば、出力部106は、外部ネットワークNから取得された各種の管理ファイルの情報を出力する。また、例えば、出力部106は、整合性確認部105による整合性

の確認結果を出力する。

[0044] 操作受付部107は、ユーザの各種の操作を受け付ける。操作受付部107は、例えば、電子文書Dの真正性の確認処理を行うことの選択を受け付ける。また、操作受付部107は、例えば、電子文書Dに関する情報を表示する各種の画面の遷移や、リンクの選択等を受け付ける。

[0045] <<管理ファイル>>

図5は、実施形態に係る管理ファイルのデータ構造の一例を示す概略図である。管理ファイルは、例えば、外部ネットワークNに保持され、より具体的には、例えば、外部ネットワークNが記憶するブロックチェーンに記憶されてもよい。図5に示すとおり、管理ファイルは、第1管理ファイル、第2管理ファイル、及び第3管理ファイルを含む。これら第1管理ファイル、第2管理ファイル、及び第3管理ファイルは、所定の階層構造を構成してもよい。

[0046] 第1管理ファイルは、第1管理ファイル識別子によって特定され、例えば、第1管理ファイル識別子をキーとした検索によって取得される。第1管理ファイル識別子は、第1管理ファイルの場所を示すアドレス(URL)であってもよい。第1管理ファイル識別子は、例えば、電子署名Sに埋め込まれたユニークな文字情報を含んでもよく、撮像等を介して電子署名S(QRコード)を復号することにより取得され得る。第1管理ファイルは、例えば、署名時刻、署名者の名称、ユーザID、及び電子文書Dのハッシュ値を含む。なお、第1管理ファイルは、他のユーザ情報を含んでもよい。

[0047] 第2管理ファイルは、電子文書Dのハッシュ値によって特定され、例えば、電子文書Dのハッシュ値をキーとした検索によって取得される。第2管理ファイルは、例えば、電子文書Dのハッシュ値、署名者の情報、URL、及びトランザクションハッシュ値を含む。署名者の情報は、電子署名Sを行った全ての署名者に関する任意の情報であってよい。図5には、一例として、電子文書Dに電子署名Sを行った署名者A及び署名者Bそれぞれの情報が示されている。URLは、例えば、電子文書データベース2の電子文書Dが保

存された記憶領域を示すURLであってよい。ユーザは、当該URLに基づいて、電子文書データベース2から、電子文書Dを取得することが可能である。トランザクションのハッシュ値は、ブロックチェーンにおいて当該管理ファイルが含まれるトランザクションのハッシュ値である。

[0048] 第3管理ファイルは、トランザクションのハッシュ値によって特定され、例えば、トランザクションのハッシュ値をキーとした検索によって取得される。第3管理ファイルは、例えば、管理ファイルが含まれるトランザクションのステータス、当該トランザクションが含まれるブロックの情報、トランザクションのタイムスタンプ等を含む。なお、第3管理ファイルは、トランザクションに関する他の任意の情報を含んでもよい。

[0049] <動作例>

図6は、実施形態に係る閲覧装置100が実行する処理の一例を示す動作フロー図である。図6に示す処理は、電子署名Sに基づいた、各種の管理ファイルの情報の取得及び表示等の処理である。

[0050] (S10) まず、撮像部101が、電子文書Dに付与されている電子署名S(QRコード)を撮像すると、識別子取得部102は、電子署名Sに含まれるユニークな文字情報を少なくとも含む第1管理ファイル識別子を取得する。第1管理ファイル識別子は、例えば、第1管理ファイルの場所を示すアドレス(URL)として、外部ネットワークNに記憶されたブロックチェーンを参照するURL及び所定のパラメータを含んで構成されてもよい。

[0051] (S11) 次に、保持情報取得部103は、取得された第1管理ファイル識別子に基づいて、外部ネットワークNから第1管理ファイルを取得する。第1管理ファイルは、例えば、第1管理ファイル識別子をキーとする検索により特定される。

[0052] (S12) 次に、出力部106は、取得された第1管理ファイルに基づいて、第1画面G1を表示する。

[0053] 図7は、実施形態に係る第1画面G1の一例を示す概略図である。第1画面G1は、第1管理ファイルに含まれる各種の情報を含んでもよい。第1画

面G 1は、例えば、署名時刻と、署名者の名称と、署名者のユーザIDと、電子文書Dのハッシュ値とを含む。図7には、1人の署名者に関する情報のみしか示されていないが、これに限らず、第1画面G 1は、電子文書Dに電子署名を行った全ての署名者に関する情報が含まれてもよい。第1画面G 1では、電子文書Dのハッシュ値がリンクL 1として表示されている。

[0054] 閲覧装置100は、例えば、第1画面G 1に対するユーザの操作等に応じて、電子署名Sの整合性を確認する処理を実行してもよい。具体的には、ハッシュ値算出部104は、電子署名Sを含む電子文書Dのハッシュ値を算出する。次いで、整合性確認部105は、取得された第1管理ファイルに含まれる電子文書Dのハッシュ値と、ハッシュ値算出部104により算出されたハッシュ値とを比較する。整合性確認部105は、2つのハッシュ値が同じであるか否かを判断する。次いで、出力部106は、確認結果を出力する。出力部106は、例えば、2つのハッシュ値が同一であれば、改ざんなしを示す信号を出力する。一方、出力部106は、2つのハッシュ値が異なれば、改ざんありを示す信号を出力する。このように、第1管理ファイルに電子文書Dのハッシュ値が含まれるため、例えば、第1管理ファイルを取得することにより、電子文書Dの真正性を確認することが可能となる。

[0055] (S 13) 次いで、例えば、ユーザは、第1画面G 1に表示されたリンクL 1を選択する。これにより、操作受付部107は、ユーザによるリンクL 1の当該選択を受け付ける。

[0056] (S 14) 次いで、保持情報取得部103は、選択されたリンクL 1に対応する、電子文書Dのハッシュ値に基づいて、外部ネットワークNから第2管理ファイルを取得する。第2管理ファイルは、例えば、電子文書Dのハッシュ値をキーとする検索により特定される。

[0057] (S 15) 次いで、出力部106は、取得された第2管理ファイルに基づいて、第2画面G 2を表示する。

[0058] 図8は、実施形態に係る第2画面G 2の一例を示す概略図である。第2画面G 2は、第2管理ファイルに含まれる各種の情報を含んでもよい。第2画

面G 2は、例えば、電子文書Dのハッシュ値と、署名者の情報と、電子文書DのURLと、トランザクションのハッシュ値とを含む。電子文書Dのハッシュ値が選択されることにより、上述した、電子署名Sの整合性を確認する処理が実行されてもよい。署名者の情報は、電子文書Dに対して電子署名Sを行った全ての署名者の任意の情報であってよい。第2画面G 2では、トランザクションハッシュ値がリンクL 2として表示されている。

[0059] 図8に示すとおり、第2画面G 2では、電子文書データベース2の電子文書Dが保存された記憶領域を示すURLが表示される。閲覧装置100は、当該URLを選択するユーザの操作等に応じて、電子文書データベース2から、電子文書Dを取得した上で、電子文書Dの内容を表示してもよい。上述したとおり、第1画面G 1においては、電子文書Dのハッシュ値が表示され、閲覧装置100は当該ハッシュ値に基づいて、電子文書Dの整合性を確認する処理を実行することが可能であった。そして、第1画面G 1に含まれるリンクL 1の選択に基づいて表示される第2画面G 2には、電子文書DのURLが表示され、これに基づいて電子文書Dの内容が表示される。

[0060] (S 16) 次いで、例えば、ユーザは、第2画面G 2に表示されたリンクL 2を選択する。これにより、操作受付部107は、ユーザによるリンクL 2の当該選択を受け付ける。

[0061] (S 17) 次いで、保持情報取得部103は、選択されたリンクL 2に対応する、トランザクションのハッシュ値に基づいて、外部ネットワークNから第3管理ファイルを取得する。第3管理ファイルは、例えば、トランザクションのハッシュ値をキーとする検索により特定される。

[0062] (S 18) 次いで、出力部106は、取得された第3管理ファイルに基づいて、第3画面G 3を表示する。

[0063] 図9は、実施形態に係る第3画面G 3の一例を示す概略図である。第3画面G 3は、第3管理ファイルに含まれる各種の情報を含んでもよい。第3画面G 3は、例えば、管理ファイルが含まれるトランザクションのステータス、当該トランザクションが含まれるブロックの情報、トランザクションのタ

イムスタンプ等を含む。なお、第3画面G3は、トランザクションに関する他の任意の情報を含んでもよい。以上で、処理が終了する。なお、第1画面G1、第2画面G2、第3画面G3、及び他の任意の画面については、ユーザの操作等によりこれら画面間を任意に遷移可能であってよい。

[0064] 閲覧装置100に含まれる各構成は、ハードウェア、ソフトウェア又はこれらの組み合わせによりそれぞれ実現することができる。ここで、ソフトウェアによって実現されるとは、コンピュータがプログラムを読み込んで実行することにより実現されることを意味する。プログラムは、様々なタイプの非一時的なコンピュータ可読媒体（non-transitory computer readable medium）を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体（tangible storage medium）を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体（例えば、フレキシブルディスク、磁気テープ、ハードディスクドライブ）、光磁気記録媒体（例えば、光磁気ディスク）、CD-ROM（Read Only Memory）、CD-R、CD-R/W、半導体メモリ（例えば、マスクROM、PROM（Programmable ROM）、EPROM（Erasable PROM）、フラッシュROM、RAM（random access memory））を含む。また、表示プログラムは、様々なタイプの一時的なコンピュータ可読媒体（transitory computer readable medium）によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。

[0065] 以上、本発明の署名生成装置1、閲覧装置100、及びプログラムの好ましい各実施形態につき説明したが、本開示は、上述の実施形態に制限されるものではなく、適宜変更が可能である。

- [0066] 例えば、上記実施形態において、署名生成装置 1 は、例えば、ユーザの本人確認状況のレベルを確認レベルとして取得する確認レベル取得部（図示せず）をさらに備えてもよい。署名生成装置 1 は、例えば、法人であるユーザの担当者の名前、住所、株主構成、顔写真等まで確認できている場合を高い確認レベル、及び登記簿謄本のみを確認にとどまる場合を低い確認レベルとして数段階に分けられた確認レベルをユーザごとに取得する。署名生成部 14 は、取得された確認レベルに応じて、コードの色を変化させてもよい。署名生成部 14 は、例えば、最も高い確認レベルの場合に赤いコードを作成してもよい。また、署名生成部 14 は、最も低い確認レベルの場合に青いコードを作成してもよい。このように、コードの色を変更することにより、コードから各ユーザの本人確認レベルを確認することができる。したがって、より高い本人確認レベルを必要とする場合等に、その本人確認レベルを容易に確認することができる。
- [0067] また、上記実施形態において、署名生成部 14 は、ユニークな文字情報を生成するとしたが、これに制限されない。署名生成部 14 は、契約書の修正を不可とする場合には、ユニークな文字情報を生成しないようにしてもよい。
- [0068] また、上記実施形態において、電子文書出力部 18 は、電子署名 S を付与した電子文書 D を紙で出力してもよい。また、保持部 17 は、電子文書 D に含まれる契約の内容を管理ファイルに保持してもよい。これにより、認証時において、保持情報取得部 103 は、管理ファイルから契約内容を取得することができる。取得された契約内容と、電子文書 D の内容とが比較されることにより、改ざんの有無を判断することができる。
- [0069] また、上記実施形態において、ユーザごとにそれぞれ別のタイミングで電子署名 S の指示をしてもよい。すなわち、署名生成部 14 は、全てのユーザから指示を取得した時点で、電子署名 S イ及びタイムスタンプを作成してもよい。
- [0070] また、上記実施形態において、修正版の電子文書 D によりオリジナルが修

正される場合、過去の電子署名Sを電子文書Dにそのまま保持するようにしてもよい。また、保持部17は、管理ファイルに過去の電子署名Sを保持するようにしてもよい。これにより、修正履歴を容易に確認することができる。

[0071] また、上記第1実施形態において、付与部15は、例えば、複数のユーザ数に対して、それぞれのユーザからの署名指示に基づいて、それぞれのユーザの署名情報及び署名時刻を電子文書Dに書き込んでもよい。保持部17は、全てのユーザからの署名指示に基づいて署名情報及び署名時刻の書き込みを実施した後に、管理ファイルに全てのユーザのユーザID、ユーザ名、署名情報、署名時刻、及びハッシュ値を保持するようにしてもよい。

[0072] また、上記実施形態において、付与部15は、契約締結を確定して確定ファイルとするために、電子文書Dにタイムスタンプを押印してもよい。

[0073] また、上記第3実施形態において、ハッシュ値算出部104は、閲覧装置100とは異なる端末で算出されたハッシュ値を取得するようにしてもよい。ハッシュ値算出部104は、例えば、電子文書Dを表示する他の端末によって算出される電子文書Dのハッシュ値を取得してもよい。また、閲覧装置100は、認証する電子文書Dを取得してもよい。この場合、撮像部101に代えて、識別子取得部102が電子文書Dから電子署名Sの識別子を取得してもよい。

[0074] また、上記実施形態において、署名生成部14は、図2に示すように、コード化された電子署名Sに重ねてユーザ名等を付与してもよい。

符号の説明

- [0075]
- 1 署名生成装置
 - 11 文書取得部
 - 12 指示取得部
 - 13 ユーザ情報取得部
 - 14 署名生成部
 - 15 付与部

- 1 6 算出部
- 1 7 保持部
- 1 0 0 閲覧装置
- 1 0 3 保持情報取得部
- 1 0 4 ハッシュ値算出部
- 1 0 5 整合性確認部
- 1 0 6 出力部
- 1 0 7 操作受付部
- 2 電子文書データベース
- D 電子文書
- N 外部ネットワーク
- S 電子署名

請求の範囲

- [請求項1] コンピュータが、
- ユーザの電子文書に付与された電子署名に基づいて、前記電子文書のハッシュ値を含む第1管理ファイルを識別するための第1管理ファイル識別子を取得するステップと、
- 取得した前記第1管理ファイル識別子に基づいて、前記第1管理ファイルを取得するステップと、
- 前記第1管理ファイルに含まれる前記ハッシュ値に基づいて、前記ハッシュ値と前記電子文書が記憶された記憶領域を特定するためのURLとを含む第2管理ファイルを取得するステップと、
- 前記URLを出力するステップと、
- を実行する方法。
- [請求項2] 前記コンピュータが、
- 前記URLの選択を受け付けるステップと、
- 前記記憶領域から前記電子文書を取得するステップと、
- 前記電子文書を出力するステップと、を更に実行する、請求項1に記載の方法。
- [請求項3] 前記第1管理ファイル識別子は、少なくとも、前記電子署名が含むユニークな文字情報を含む、請求項1に記載の方法。
- [請求項4] 前記第1管理ファイル及び前記第2管理ファイルは、ブロックチェーンに記録される、請求項1に記載の方法。
- [請求項5] 前記第2管理ファイルは、更に、前記ブロックチェーンを構成するトランザクションであって、前記第1管理ファイル及び前記第2管理ファイルが含まれるトランザクションのハッシュ値を含み、
- 前記コンピュータが、前記トランザクションのハッシュ値に基づいて、前記トランザクションに関する情報を含む第3管理ファイルを前記ブロックチェーンから取得するステップ、を更に実行する、請求項4に記載の方法。

- [請求項6] 前記コンピュータが、
前記電子署名を含む前記電子文書のハッシュ値を算出するステップと、
と、
取得された前記ハッシュ値と算出された前記ハッシュ値との整合性を確認するステップと、
確認した結果を出力するステップと、を更に実行する、請求項1に記載の方法。
- [請求項7] コンピュータに、
ユーザの電子文書に付与された電子署名に基づいて、前記電子文書のハッシュ値を含む第1管理ファイルを識別するための第1管理ファイル識別子を取得するステップと、
取得した前記第1管理ファイル識別子に基づいて、前記第1管理ファイルを取得するステップと、
前記第1管理ファイルに含まれる前記ハッシュ値に基づいて、前記ハッシュ値と前記電子文書が記憶された記憶領域を特定するためのURLとを含む第2管理ファイルを取得するステップと、
前記URLを出力するステップと、
を実行させるためのプログラム。
- [請求項8] ユーザの電子文書に付与された電子署名に基づいて、前記電子文書のハッシュ値を含む第1管理ファイルを識別するための第1管理ファイル識別子を取得する第1管理ファイル識別子取得部と、
取得した前記第1管理ファイル識別子に基づいて、前記第1管理ファイルを取得する第1管理ファイル取得部と、
前記第1管理ファイルに含まれる前記ハッシュ値に基づいて、前記ハッシュ値と前記電子文書が記憶された記憶領域を特定するためのURLとを含む第2管理ファイルを取得する第2管理ファイル取得部と、
、
前記URLを出力するURL出力部と、

を備える情報処理装置。