

明 細 書

発明の名称：管理装置、管理装置の制御方法、及びプログラム

技術分野

[0001] 本開示は、管理装置、管理装置の制御方法、及びプログラムに関する。

背景技術

[0002] 従来から、電子文書等の電子コンテンツのデータが真正のものであることを保証するために、電子署名が用いられる。例えば、特許文献1には、署名対象データに電子署名を行うための電子署名管理システムが開示されている。また、例えば、特許文献2には、分散型台帳システムであるブロックチェーンを利用した本人認証方法として、電子署名が施された本人識別情報ハッシュ値を当該ブロックチェーンに保存しておく方法が提案されている。

先行技術文献

特許文献

[0003] 特許文献1：特開2018-067807号公報

特許文献2：特開2024-077561号公報

発明の概要

発明が解決しようとする課題

[0004] 電子署名に関する事項を証明するための証明書（電子証明書）を、ブロックチェーン等の台帳システムに記憶させることが考えられるが、台帳システムに記憶した情報自体が改ざんされる可能性もあるため、電子署名の信頼性の更なる向上が望まれていた。

[0005] そこで本発明は、上記従来の実状に鑑みてなされたものであり、電子署名の信頼性を向上させることを目的とする。

課題を解決するための手段

[0006] 本発明の実施形態に係る管理装置は、電子コンテンツに対する電子署名を管理するための管理装置であって、電子コンテンツに対する署名の指示を取得する取得部と、指示に応じて電子署名を生成する署名生成部と、生成され

た電子署名を電子コンテンツに付与する付与部と、電子署名に関する電子証明書を生成する電子証明書生成部と、複数の台帳システムの各台帳システムに、電子証明書に含まれる情報である電子証明書情報を格納するための処理を実行する電子証明書情報格納部と、複数の台帳システムのそれぞれに、各台帳システムに格納されている電子証明書情報の要求を送信することにより、要求に対する複数の台帳システムのそれぞれからの出力である複数の回答を取得する回答取得部と、複数の回答に含まれる同一の回答毎に、該回答を出力した台帳システムに対応付けられた係数を集計することにより、複数の回答に含まれる同一の回答のそれぞれの集計値を算出する集計値算出部と、集計値に基づいて、複数の回答のうち1つの回答を電子証明書情報に一致する回答として決定する決定部と、1つの回答を出力する出力部と、を備える。

[0007] これにより、電子署名に関する電子証明書の少なくとも一部である電子証明書情報が、複数の台帳システムの各台帳システムに格納された上で、複数の台帳システムのそれぞれから、電子証明書情報の要求に対する回答が取得され、同一の回答毎に、該回答を出力した台帳システムに対応付けられた係数を集計することにより集計値が算出され、集計値に基づいて、複数の回答のうち1つの回答が電子証明書情報に一致する回答として決定され、これが出力される。よって、電子証明書情報の改ざんの可能性が低減されるため、電子署名の信頼性を向上させることが可能となる。

発明の効果

[0008] 本発明によれば、電子署名の信頼性を向上させることが可能となる。

図面の簡単な説明

[0009] [図1]実施形態に係る管理装置1を用いた電子署名管理システム100の概要を示す概略図である。

[図2]実施形態に係る管理装置1によって生成された電子署名Sを付した電子文書Dを示す概略図である。

[図3]実施形態に係る管理装置1の構成を示すブロック図である。

[図4]実施形態に係る電子証明書のデータ構造の一例を示す概略図である。

[図5]実施形態に係る台帳システムテーブルのデータ構造の一例を示す概略図である。

[図6]実施形態に係るユーザ端末4の構成を示すブロック図である。

[図7]実施形態に係る電子署名管理システム100が実行する電子署名及び電子証明書の生成等の動作処理の一例を示すシーケンス図である。

[図8]実施形態に係る管理装置1が実行する、電子証明書情報の照会処理の一例を示す動作フロー図である。

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] (1) 概要

図1は、実施形態に係る管理装置1を用いた電子署名管理システム100の概要を示す概略図である。

[0012] 図1に示すとおり、電子署名管理システム100は、例えば、管理装置1、電子コンテンツデータベース2、複数の台帳システム3、及び複数のユーザ端末4等を含む。図1に示す例では、台帳システム3は、第1台帳システム3A、第2台帳システム3B、及び第3台帳システム3Cを含む。なお、実施形態に係る台帳システム3は、3つに限らず、2つ又は4つ以上の数の台帳システム3を含んでもよい。管理装置1は、電子コンテンツデータベース2及び台帳システム3それぞれに対して、情報を管理（格納、削除、変更等）可能に接続される。また、管理装置1は、インターネット等の通信ネットワークNを介して、複数のユーザ端末4と互いに情報を送受信可能に接続される。

[0013] 管理装置1は、例えば、サーバ等のコンピュータ（情報処理装置）であり、CPU等の処理部とメモリ等の記憶部とを有する。管理装置1は、ユーザの契約書等の電子コンテンツDに対して、電子署名Sを生成する装置である

。電子コンテンツDは、例えば、電子コンテンツデータベース2に保存されている。すなわち、管理装置1は、ユーザの電子コンテンツDに付与する電子署名Sを生成する機能を有する装置である。管理装置1は、例えば、電子署名Sを電子コンテンツDに視認可能に付与することで、電子コンテンツDへの同意等を示した電子コンテンツDを作成してもよい。

[0014] なお、以下の実施形態において、「電子コンテンツ」は、「電子文書」を含んでもよいし、「電子画像」を含んでもよい。「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、署名簿等の任意の文書であって、電子的に作成された文書を含んでもよい。また、「電子画像」は、静止画像であってもよいし、時系列的に連続した複数の静止画像から構成される動画（映像）であってもよい。動画は、音声と組み合わせられていてもよい。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コンテンツDに対して電子的に実施する処理を含んでもよい。また、「電子証明書」とは、電子署名に関する事項を証明するための証明書であってよく、例えば、利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明するために作成する電磁的記録を含んでもよい。

[0015] 図2は、実施形態に係る管理装置1によって生成された電子署名Sを付した電子文書Dを示す概略図である。特に、管理装置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を付与してもよい。管理装置1は、例えば、個々のユーザに対応した電子署名Sを視認可能に付与してもよい。管理装置1は、例えば、電子コンテンツDに、QRコード（登録商標）として示される電子署名Sを付与してもよい。なお、管理装置1は、電子コンテンツとしての電子画像に電子署名Sを付与する場合は、電子画像が含む少なくともいずれかの静止画像の一部に電子署名Sを重畳させてもよいし、電子画像が有するメタデータに電子署名Sを付与してもよい。

[0016] 管理装置1は、図1に示すように、台帳システム3（第1台帳システム3A、第2台帳システム3B、及び第3台帳システム3C）に接続される。管

理装置 1 は、電子署名 S を付与した電子コンテンツ D の電子証明書を作成する。管理装置 1 は、作成した電子コンテンツ D の電子証明書の少なくとも一部（電子証明書情報）を第 1 台帳システム 3 A、第 2 台帳システム 3 B、及び第 3 台帳システム 3 C のそれぞれに格納する。各台帳システム 3 は、分散型台帳システムであってよい。台帳システム 3 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（ノード）を含んで構成されてもよい。ブロックチェーンの形式は、特に限定されないが、例えばパブリック型、コンソーシアム型、及びプライベート型のいずれかのプライベートブロックチェーンとして構成されてもよい。管理装置 1 は、例えば、電子証明書を当該ブロックチェーン等として構成される第 1 台帳システム 3 A、第 2 台帳システム 3 B、及び第 3 台帳システム 3 C に格納する。

[0017] 管理装置 1 は、所定のタイミングにおいて、電子署名管理システム 100 が備える複数の台帳システム 3 に対して、所望の電子証明書情報を照会する処理（照会処理）を実行する。管理装置 1 は、複数の台帳システム 3 のそれぞれに、各台帳システム 3 に格納されている電子証明書情報を要求し、要求に対する各台帳システム 3 からの回答を取得する。ここで、台帳システム 3 の少なくともいずれかにおいて、電子証明書情報の改ざんがあった場合、複数の台帳システム 3 から取得した複数の回答に、複数の異なる回答が含まれ得ることとなるが、実施形態に係る管理装置 1 では、複数の台帳システム 3 によって電子証明書情報を管理するため、真正な電子証明書情報を担保することが可能となる。すなわち、管理装置 1 は、各台帳システム 3 から取得した回答に含まれる同一の回答毎に、該回答を出力した前記台帳システムに対応付けられた係数を集計することにより、複数の回答に含まれる同一の回答のそれぞれの集計値を算出する。管理装置 1 は、集計値に基づいて、複数の回答のうち 1 つの回答を電子証明書情報に一致する回答として決定し、当該 1 つの回答を出力する。このように、実施形態に係る電子署名管理システム 100 では、複数の台帳システム 3 に電子証明書情報を保存しておき、所定のタイミングにおいて、管理装置 1 が複数の台帳システム 3 に対して電子証

明書情報の照会処理を行うことにより、真正な電子証明書情報を決定し出力する。これにより、電子証明書情報の改ざんの可能性が低減され、ひいては電子署名の信頼性が向上する。

[0018] ユーザ端末4は、図1に示すように、例えば、管理装置1とは異なる装置として構成される。ユーザ端末4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コンピュータ（情報処理装置）であり、CPU等の処理部とメモリ等の記憶部とを有する。ユーザ端末4は、管理装置1によって生成された電子署名Sに基づいて、台帳システム3に保持された電子証明書に含まれる情報を、管理装置1を介して取得し、取得した当該情報に基づいて、電子コンテンツDの真正性を確認するための処理を実行する。また、ユーザ端末4は、取得した電子証明書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、ユーザ端末4は、電子コンテンツデータベース2において電子コンテンツ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、ユーザ端末4は、電子コンテンツDを電子コンテンツデータベース2から取得し、これを表示する。これにより、電子コンテンツDの真正性が担保される環境下で電子コンテンツDの内容を確認することが可能となる。更に、電子署名Sから電子コンテンツDの内容を確認できるので、ユーザは、電子コンテンツDのファイルではなく、電子コンテンツ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、（電子証明書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。

[0019] (2) 構成

(2-1) 管理装置1

図3は、実施形態に係る管理装置1の構成を示すブロック図である。管理装置1は、文書管理部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、電子証明書生成部16と、電子証明書情報格納部17と、回答取得部18と、集計値算出部19と、決定部20と、送受信部21と、を備える。これら各種の機能部は、管理装置1が有する

CPU等の処理部が動作することにより実現される。

- [0020] 文書管理部11は、例えば、CPUが動作することにより実現される。文書管理部11は、電子署名の対象となる電子コンテンツDの作成、取得、修正、記憶部への格納等を実行する。文書管理部11は、例えば、電子コンテンツデータベース2やユーザ端末4から電子コンテンツDを取得する。電子コンテンツDは、文書作成ソフトや画像作成ソフトにより作成された電子データであってもよいし、紙等の印刷物をスキャンしたデータであってもよい。また、文書管理部11は、ユーザ端末4から取得された指示に基づいて、電子コンテンツを作成・修正等してもよい。また、文書管理部11は、電子コンテンツを電子コンテンツデータベース2に格納してもよい。
- [0021] 指示取得部12は、署名対象となる、取得された電子コンテンツに対する署名の指示（署名指示）を取得する。指示取得部12は、例えば、ユーザ端末4から署名指示を取得する。
- [0022] 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、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、実施形態において、ユーザ情報取得部13は、電子署名Sを生成する際に、ユーザ端末4等からユーザ情報を取得する。ユーザ情報は、ユーザによって管理されるユーザに固有の任意の情報を含んでもよい。
- [0023] 署名生成部14は、電子証明書の識別子である電子証明書識別子がコード化された電子署名を生成する。なお、署名生成部14は、電子証明書識別子にユニークな文字列を含めてもよい。当該文字列は、例えば、電子署名S毎にユニークなものであってよい。電子証明書識別子は、例えば、電子コンテンツDに電子署名Sが付与されることにより生成（採番）される。
- [0024] 付与部15は、生成された電子署名Sを電子コンテンツDに付与する。付与部15は、例えば、電子署名Sを電子コンテンツDに視認可能に付与してもよい。これにより、電子コンテンツ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。付与部15は、例えば、図2に示すように、電子コンテンツ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生成された電子署名Sを付与してもよい。付与部15は、例えば、電子コンテンツ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を付与してもよい。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に併記してもよい。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、電子コンテンツD（電子文書）の表示面下方にユーザ名を併記する。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。

[0025] 電子証明書生成部16は、電子署名Sに関する各種の電子証明書を生成する。電子証明書は、例えば、台帳システム3に記憶される。

[0026] 図4は、実施形態に係る電子証明書のデータ構造の一例を示す概略図である。図4に示す各行が1つの電子証明書に相当する。電子証明書は、例えば、電子コンテンツに対して電子署名が付与される度に、1つずつ台帳システム3に追加されていく。

[0027] 電子証明書は、例えば、発行者名、発行番号、発行日時、有効期間満了日、シリーズID、枝番、ユーザID、ユーザ所属組織、ユーザ役職、ユーザ氏名、署名内容、原文ハッシュ値、署名前ハッシュ値、署名後ハッシュ値、電子コンテンツ公開用URL、及びパスワードを含んでもよい。

[0028] 発行者名は、電子証明書の発行者の名称であり、例えば、管理装置1の管理者の名称であってもよい。発行番号は、管理装置1によって発行される電子証明書識別子（電子証明書を識別するための識別子）である。発行日時は、電子証明書が発行された日時であって、署名の時刻情報であってもよい。発行日時は、電子署名の順位を示す順位情報（電子署名が付与される度に、

当該電子署名が一連の電子署名のうちいずれの順位であるかを示す情報）の一例である。有効期間満了日は、電子証明書の有効期間が満了する日である。

[0029] シリーズIDは、電子コンテンツDの系統を識別するための識別情報である系統識別情報の一例である。シリーズIDは、電子コンテンツDに対して電子署名Sが1つ又は複数付与されても変化しない、電子コンテンツD（の系統）について固有の識別情報であってよい。換言すれば、シリーズIDは、電子コンテンツDが表す内容（修正されたものも含んでもよい）に対して与えられる識別情報である。これにより、電子コンテンツDに対して連続的に電子署名Sが付与される場合、当該電子コンテンツDや、一連の電子署名Sをシリーズとして管理することや、一連の電子署名Sのうちいずれの電子署名Sが最新であるか、所持している電子コンテンツDに付された電子署名Sが最新のものであるかなどを確認することなどが可能となる。

[0030] 枝番は、電子署名Sの順位を示す順位情報（電子署名Sが付与される度に、当該電子署名Sが一連の電子署名Sのうちいずれの順位であるかを示す情報）の一例である。図4に示す例では、枝番として、1、2、3などの自然数が用いられているが、順位を示すことが可能であれば、記号や符号等によって任意に枝番（順位情報）が構成されてもよい。

[0031] ユーザIDは、ユーザの識別情報である。ユーザ所属組織は、ユーザが所属する組織を示す情報である。ユーザ役職は、ユーザの当該組織における役職を示す情報である。ユーザ氏名は、ユーザの氏名（各企業の担当者の氏名）である。

[0032] 署名内容は、電子署名Sに付随する情報であって、ユーザが任意に入力したテキスト形式のデータであってもよい。署名内容は、例えば、電子署名に付随するユーザの意思を表明したものであってもよいし、署名対象の電子コンテンツに対して修正を行った場合は、修正があることを示す情報や修正の内容を示す情報であってもよい。これにより、電子証明書を確認することによって、電子署名に対するユーザの意思や、電子コンテンツに対する修正の

有無及びその内容等を確認することが可能となる。

- [0033] 原文ハッシュ値、署名前ハッシュ値、及び署名後ハッシュ値は、例えば、電子コンテンツDに関する整合性の確認処理等において用いられる。整合性の確認処理については、後述する。原文ハッシュ値は、いずれの電子署名も含まない電子コンテンツD（原文）のハッシュ値である。署名前ハッシュ値は、最新の電子署名Sを付与する直前の電子コンテンツD（当該電子署名Sよりも順位が前である電子署名Sを含む電子コンテンツD）のハッシュ値である。署名後ハッシュ値は、最新の電子署名Sを付与した電子コンテンツDのハッシュ値である。
- [0034] 電子コンテンツ公開用URLは、電子コンテンツDが保存された記憶領域を特定するためのURL（例えば、電子コンテンツデータベース2における電子コンテンツDのURL）であってよい。電子コンテンツ公開用URLには、有効期限が設定されていてもよい。パスワードは、ファイル公開用URLにアクセスして電子コンテンツDを閲覧する際に必要となるパスワードであってよく、任意またはシステムによって付与されてもよい。
- [0035] なお、上述した電子証明書はあくまでも例示であって、実施形態における電子証明書は、上述した項目の任意の項目を含まなくてもよく、また、上述した項目以外の項目を含んでもよい。
- [0036] 電子証明書情報格納部17は、生成された電子証明書の少なくとも一部（電子証明書情報）を、台帳システム3（第1台帳システム3A、第2台帳システム3B、及び第3台帳システム3C）に格納する。電子証明書情報の少なくとも一部である電子証明書情報は、例えば、図4に示した情報のうちの少なくとも一部を含んでもよい。
- [0037] 回答取得部18は、各台帳システム3から、各台帳システム3に格納されている電子証明書情報を取得する。具体的には、回答取得部18は、例えば、各台帳システム3に、各台帳システム3に格納されている電子証明書情報の要求を送信する。台帳システム3は、管理装置1から電子証明書情報の要求を受信すると、当該要求に応じて、台帳システム3に格納された電子証明

書情報を出し、出力した電子証明書情報を、当該要求に対する回答として管理装置 1 に送信する。回答取得部 18 は、各台帳システム 3 からの当該回答を取得する。回答取得部 18 による回答の取得処理が実行されるタイミングは、任意のタイミングであってもよいが、例えば、ユーザ端末 4 等から電子証明書情報の照会の要求を受け付けたときであってもよいし、電子文書に対する電子署名を新たに生成するときであってもよい。

[0038] 集計値算出部 19 は、回答取得部 18 により複数の台帳システム 3 から取得した複数の回答に含まれる同一の回答毎に、該回答を出力した台帳システム 3 に対応付けられた係数を集計することにより、複数の回答に含まれる同一の回答のそれぞれの集計値を算出する。すなわち、集計値は、同一の回答を出力した少なくとも 1 つの台帳システム 3 それぞれの係数の合計値であってよい。また、集計値は、電子証明書情報の回答に対応付けて算出される値であり、改ざんされていない真正な電子証明書情報を選択するためのスコアと言える。

[0039] 決定部 20 は、例えば、集計値算出部 19 が算出した集計値に基づいて、各台帳システム 3 から取得した複数の回答のうち 1 つの回答を、電子証明書情報に一致する回答として決定する。決定部 20 は、例えば、複数の台帳システム 3 から取得した回答のうち集計値が最も高い回答を、電子証明書情報に一致する回答であると決定してもよい。

[0040] 送受信部 21 は、ユーザ端末 4 との間で各種の情報を送受信する。送受信部 21 は、例えば、ユーザ端末 4 から電子コンテンツ D に対する署名指示を受信する。また、送受信部 21 は、例えば、電子コンテンツ D（電子署名 S が付与されたものを含む）を、ユーザ端末 4 に送信する。また、送受信部 21 は、出力部の一例であって、決定部 20 により電子証明書情報に一致する回答として決定された回答を出力する。ここで、回答を出力する処理は、例えば、ユーザ端末 4 等の他の外部装置に当該回答を送信する処理であってもよいし、当該回答を任意の表示装置に表示させる処理であってもよい。

[0041] 管理装置 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（`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。

[0042] 図5は、実施形態に係る台帳システムテーブルのデータ構造の一例を示す概略図である。台帳システムテーブルは、例えば、管理装置1が備える記憶部等の、管理装置1がアクセス可能な記憶部に記憶されてもよい。台帳システムテーブルは、電子署名管理システム100が備える各台帳システム3に関する情報を含んでもよい。図5に示す例においては、台帳システムテーブルは、台帳システム3毎に、台帳システム3の係数及び特性情報が含まれている。

[0043] 係数は、各台帳システム3に対応付けられた数値であり、例えば、電子証

明書情報の照会処理時において、集計値を算出する基となる。換言すれば、当該係数は、当該台帳システム3に電子証明書情報として格納されている情報が、真正な電子証明書情報に一致する可能性や尤度を示した数値であってよい。

[0044] 台帳システムテーブルは、各台帳システム3の特性を示す特性情報を含んでもよい。特性情報は、例えば、台帳システム3のタイプを示す情報であってよい。台帳システム3のタイプは、例えば、分散型か非分散型かの別や、分散型の場合の型（パブリック型、コンソーシアム型、及びプライベート型等）等であってよい。また、特性情報は、例えば、アルゴリズムタイプを含んでもよい。アルゴリズムタイプは、台帳システム3が採用する、情報を記憶するためのアルゴリズム（コンセンサスアルゴリズム等）のタイプを示す情報である。具体的には、アルゴリズムタイプは、ブロックチェーン、イーサリアム、及び他のアルゴリズムを含んでもよい。また、特性情報は、例えば、ノード数を含んでもよい。ノード数は、台帳システム3を構成するノードの数であってよい。なお、図5に示した特性情報はあくまで一例であって、台帳システムテーブルは、台帳システム3の特性を示す任意の特性情報を含んでもよい。

[0045] 管理装置1は、各台帳システム3の特性を示す特性情報に基づいて、係数を算出及び更新してもよい。管理装置1は、全ての台帳システム3の係数が等しくなるように係数を算出してもよい。この場合、実質的に、複数の台帳システム3による多数決によって、1つの回答が電子証明書情報に一致する回答として決定されることとなる。或いは、管理装置1は、例えば、台帳システム3の特性情報が改ざんの可能性の小さいものであるほど、当該台帳システム3の係数が大きくなるように、係数を算出してもよい。具体的には、例えば、台帳システム3が非分散型よりも分散型の場合に、より係数が大きくなるようにしてもよい。また、例えば、分散型台帳システム3のタイプがパブリック型、コンソーシアム型、及びプライベート型の順に、係数が大きくなるようにしてもよい。また、台帳システム3のノード数が大きい程、係

数が大きくなるようにしてもよい。

[0046] (2-2) ユーザ端末4

図6は、実施形態に係るユーザ端末4の構成を示すブロック図である。ユーザ端末4は、撮像部41と、識別子取得部42と、保持情報取得部43と、ハッシュ値算出部43と、整合性確認部44と、出力部45と、操作受付部46と、を備える。これら各種の機能部は、ユーザ端末4が有するCPU等の処理部が動作することにより実現される。

[0047] 撮像部41は、いわゆるカメラを含む撮像機構である。撮像部41は、例えば、電子コンテンツDに付与されている任意の電子署名Sを撮像する。撮像部41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コンテンツDに含まれる任意の電子署名Sを撮像する。

[0048] 識別子取得部42は、電子署名S(QRコード)の撮像により、撮像された電子署名Sに含まれる電子証明書識別子を取得する。

[0049] ハッシュ値算出部43は、電子コンテンツDに基づいて、各種のハッシュ値を算出する。ハッシュ値算出部43は、例えば、最新の電子署名Sを含む電子コンテンツDのハッシュ値(署名後ハッシュ値)を算出してもよい。また、ハッシュ値算出部43は、例えば、最新の電子署名Sのみを含まない電子コンテンツDのハッシュ値(署名前ハッシュ値)を算出してもよい。また、ハッシュ値算出部43は、例えば、いずれの電子署名Sも含まない原文としての電子コンテンツDのハッシュ(原文ハッシュ値)を算出してもよい。

[0050] 整合性確認部44は、台帳システム3に記憶された電子証明書を管理装置1を介して取得した上で、これに基づいて、電子コンテンツDに関する電子コンテンツDの整合性の確認処理を実行する。電子コンテンツDの整合性の確認処理により、電子コンテンツDが真正であるか否かを判定することが可能となる。例えば、整合性確認部44は、電子コンテンツDに含まれるいずれかの電子署名Sの撮像により取得された電子証明書識別子に基づいて、管理装置1から電子証明書を取得した上で、当該取得された電子証明書に含まれるハッシュ値(原文ハッシュ値、署名前ハッシュ値、及び/又は署名後ハ

ッシュ値)と、ハッシュ値算出部43により電子コンテンツDから算出されたハッシュ値(原文ハッシュ値、署名前ハッシュ値、及び／又は署名後ハッシュ値)との整合性を確認する。整合性確認部44は、例えば、対象となる電子コンテンツDから得られる原文ハッシュ値が、電子証明書に含まれる原文ハッシュ値に一致するか否かを判定することにより、原文としての電子コンテンツDに改変が無いかなかを判定してもよい。また、整合性確認部44は、例えば、対象となる電子コンテンツDから得られる署名前ハッシュ値(最新の電子署名のみを除いて得られる電子コンテンツに基づいて算出されるハッシュ値)が、順位が1つ前の電子証明書に含まれる署名後ハッシュ値に一致するか否かを判定することにより、1つ前の電子署名Sがなされてから最新の電子署名Sがなされる期間において電子コンテンツDに改変が無いかなかを判定してもよい。具体的な動作例は以下のとおりである。すなわち、ユーザは、例えば、紙に出力した(手交、交付等された)電子コンテンツDの電子署名Sをユーザ端末4で撮像することで、管理装置1(の電子コンテンツデータベース2等)に保存されている電子コンテンツD(原本)にアクセスし、電子コンテンツDをユーザ端末4に表示させることが可能である。管理装置1はアクセスを受けた電子コンテンツDについてハッシュ値を算出し、台帳システム3に対してハッシュ値(原文ハッシュ値、署名前ハッシュ値、及び署名後ハッシュ値)の照会を行うことで、電子コンテンツDが真正であるかを判定しても良い。手交・交付された電子コンテンツDについては、ユーザは、例えば、電子コンテンツDが真正であるかについて、手交・交付された電子コンテンツDを、管理装置1に記憶されている電子コンテンツDをユーザ端末4に表示させたものと目視で比較すること等により確認することが可能である。また、管理装置1に記憶されている電子コンテンツDが真正であるかについては、例えば、台帳システム3に対する照会により判定が行われてもよい。

[0051] 出力部45は、電子コンテンツDに関する各種の情報を出力する。例えば、出力部45は、管理装置1から取得された各種の電子証明書の情報を出力

する。また、例えば、出力部 4 5 は、整合性確認部 4 4 による整合性の確認結果を出力する。

[0052] 操作受付部 4 6 は、ユーザの各種の操作を受け付ける。操作受付部 4 6 は、例えば、電子コンテンツ D に関する整合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 4 6 は、例えば、電子コンテンツ 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。

[0053] 送受信部 4 7 は、管理装置 1 や他のユーザ端末 4 との間で各種の情報を送受信する。送受信部 4 7 は、例えば、電子コンテンツに対する署名指示を管理装置 1 に送信する。また、送受信部 4 7 は、例えば、電子コンテンツ D（電子署名 S が付与されたものを含む）や電子証明書を、管理装置 1 から受信する。

[0054] （３）動作例

（３－１）電子署名及び電子証明書の生成等

図 7 は、実施形態に係る電子署名管理システム 1 0 0 が実行する電子署名及び電子証明書の生成等の動作処理の一例を示すシーケンス図である。以下では、ユーザの一例である発注企業からユーザの他の一例である受注企業に対して、受注企業が提供する商品・役務の発注があった場合を例に説明する。受注企業が利用するユーザ端末 4 をユーザ端末 4 A とし、発注企業が利用するユーザ端末 4 をユーザ端末 4 B とする。この場合において、受注企業の担当者が当該商品・役務の発注企業に対する請求書としての電子文書 D 0 を作成した状態にあるものとする。なお、電子文書 D 0 の作成は、ユーザ端末 4 A が、管理装置 1 が提供する電子文書の作成サービスを利用して作成されたものでもよいし、そのような作成サービスを用いない一般的な文書作成ソフト等を利用して作成されたものでもよい。また、作成された電子文書 D 0 は、管理装置 1 が、電子文書データベース 2 に格納しておいてもよいし、ユーザ端末 4 A が、ユーザ端末 4 A がアクセス可能な記憶部に格納しておいてもよい。なお、当該シーケンス図は、実施形態に係る電子署名管理システム 1 0 0 が電子コンテンツとしての電子文書を扱う場合を例としているが、電

子文書に限らず、電子画像等の他の電子コンテンツに対しても適用可能である。

[0055] 受注企業の担当者が利用するユーザ端末4 Aは、受注企業の担当者による電子文書D 0に対する署名指示の操作を受け付けると、電子文書D 0に対する署名指示を管理装置1に送信する（S 1 0 1）。管理装置1は、電子文書D 0に対する署名指示をユーザ端末4 Aから受信する（S 1 0 2）。

[0056] 電子文書D 0に対する署名指示は、例えば、電子文書D 0のデータ自体を含んでいてもよいし、或いは、電子文書データベース2やユーザ端末4 Aがアクセス可能な記憶部等に格納された電子文書D 0を特定するための情報（シリーズID等）を含んでいてもよい。また、署名指示は、例えば、台帳システム3に記録される任意の項目（受注企業の担当者に関する項目等）を含んでもよい。また、署名指示は、例えば、受注企業の担当者が入力した署名内容を含んでもよい。図4に示す例では、受注企業の担当者が入力した「請求する」との署名内容が示されている。

[0057] 管理装置1は、署名指示に基づいて、受注企業の担当者による電子署名S 1を生成し、また、電子証明書を生成する（S 1 0 3）。電子証明書の生成に関して、管理装置1は、電子署名S 1を付与する直前の電子文書D 0のハッシュ値を生成し、これを署名前ハッシュ値として電子証明書に含める。また、管理装置1は、電子署名S 1を付与した後の電子文書D 1のハッシュ値を生成し、これを署名後ハッシュ値として電子証明書に含める。また、管理装置1は、いずれの電子署名Sも含まない電子文書D 0のハッシュ値を生成し、これを原文ハッシュ値として電子証明書に含める。管理装置1は、生成した電子証明書（例えば、図4に示す1行目の電子証明書）の少なくとも一部を、第1台帳システム3 A、第2台帳システム3 B、及び第3台帳システム3 Cに格納する（S 1 0 4）。

[0058] 管理装置1は、生成された電子署名S 1を電子文書D 0に付与することにより、電子文書D 1を生成する。そして、管理装置1は、生成された電子文書D 1をユーザ端末4 Aに送信する（S 1 0 5）。ユーザ端末4 Aは、受信

した電子文書D 1 を、ユーザ端末4 Aがアクセス可能な記憶部に格納してもよい。

[0059] ユーザ端末4 Aは、受注企業の担当者による操作に応じて、電子文書D 1 を、発注企業の担当者が利用するユーザ端末4 Bに送信する（S 1 0 6）。なお、電子文書D 1 のユーザ端末4 Bへの送信は、管理装置1を介して行われてもよい。ユーザ端末4 Bは、電子文書D 1を受信する（S 1 0 7）。ユーザ端末4 Bは、受信した電子文書D 1 を、ユーザ端末4 Bがアクセス可能な記憶部に格納してもよい。

[0060] 発注企業の担当者は、受信された電子文書D 1の内容（請求書の内容）を適宜確認した上で、発注企業の担当者による電子文書D 1に対する署名指示の操作を行う。ユーザ端末4 Bは、当該操作を受け付けると、電子文書D 1に対する署名指示を管理装置1に送信する（S 1 0 8）。管理装置1は、電子文書D 1に対する署名指示をユーザ端末4 Bから受信する（S 1 0 9）。

[0061] 電子文書D 1に対する署名指示は、例えば、電子文書D 1のデータ自体を含んでいてもよいし、或いは、電子文書データベース2やユーザ端末4 Bがアクセス可能な記憶部等に格納された電子文書D 1を特定するための情報（シリーズID等）を含んでいてもよい。また、署名指示は、例えば、台帳システム3に記録される任意の項目（発注企業の担当者に関する項目等）を含んでもよい。また、署名指示は、例えば、発注企業の担当者が入力した署名内容を含んでもよい。図4に示す例では、発注企業の担当者が入力した「請求内容通りに支払う」との署名内容が示されている。

[0062] 管理装置1は、署名指示に基づいて、発注企業の担当者による電子署名S 2を生成し、また、電子証明書を生成する（S 1 1 0）。電子証明書の生成に関して、管理装置1は、電子署名S 2を付与する直前の電子文書D 1のハッシュ値を生成し、これを署名前ハッシュ値として電子証明書に含める。また、管理装置1は、電子署名S 2を付与した後の電子文書D 2のハッシュ値を生成し、これを署名後ハッシュ値として電子証明書に含める。また、管理装置1は、いずれの電子署名Sも含まない電子文書D 0のハッシュ値を生成

し、これを原文ハッシュ値として電子証明書に含める。管理装置 1 は、生成した電子証明書（例えば、図 4 に示す 2 行目の電子証明書）の少なくとも一部を、第 1 台帳システム 3 A、第 2 台帳システム 3 B、及び第 3 台帳システム 3 C に格納する（S 1 1 1）。

[0063] 管理装置 1 は、電子文書 D 1 の内容が改変されていないかを判定してもよい。すなわち、管理装置 1 は、電子署名 S 2 の付与対象である電子文書 D 1 の内容が、1 つ前の電子署名 S 1 が付与された直後における電子文書 D 1 の内容から改変されていないかを判定してもよい。例えば、管理装置 1 は、図 4 に示す 1 行目の電子証明書の署名後ハッシュ値と、2 行目の電子証明書の署名前ハッシュ値とを、台帳システム 3 に対して照会した上で、これらを比較し、両者が一致していれば、電子文書 D 1 は改変していないと判定し、両者が一致していなければ、電子文書 D 1 は改変していると判定する。管理装置 1 は、判定結果を、ユーザ端末 4 B に送信する等して出力してもよい。これにより、発注企業の担当者は、電子署名 S 2 を行うに際して、対象となる電子文書 D 1 の内容の連続性を確認することが可能となる。

[0064] 管理装置 1 は、生成された電子署名 S 2 を電子文書 D 1 に付与することにより、電子文書 D 2 を生成する。そして、管理装置 1 は、生成された電子文書 D 2 をユーザ端末 4 B に送信する（S 1 1 2）。ユーザ端末 4 B は、受信した電子文書 D 2 を、ユーザ端末 4 B がアクセス可能な記憶部に格納してもよい。

[0065] ユーザ端末 4 B は、発注企業の担当者による操作に応じて、電子文書 D 2 を、受注企業の担当者が利用するユーザ端末 4 A に送信する（S 1 1 3）。なお、電子文書 D 2 のユーザ端末 4 A への送信は、管理装置 1 を介して行われてもよい。ユーザ端末 4 A は、電子文書 D 2 を受信する（S 1 1 4）。なお、ユーザ端末 4 B からユーザ端末 4 A へ、管理装置 1 を介し又は介さず、支払を承諾する旨の通知が送信されてもよい。ユーザ端末 4 A は、受信した電子文書 D 2 を、ユーザ端末 4 A がアクセス可能な記憶部に格納してもよい。

[0066] (3-2) 電子証明書情報の照会

図8は、実施形態に係る管理装置1が実行する、電子証明書情報の照会処理の一例を示す動作フロー図である。電子証明書情報の照会処理は、電子署名管理システム100が備える複数の台帳システム3に対して、所望の電子証明書情報を照会する処理である。電子証明書情報の照会処理は、任意のタイミングで実行されてもよいが、例えば、ユーザ端末4等から電子証明書情報の照会の要求を受け付けたときであってもよいし、電子文書に対する電子署名を新たに生成するとき（例えば、上述したステップS110等のタイミング）であってもよい。

[0067] 回答取得部18は、例えば、各台帳システム3に、各台帳システム3に格納されている電子証明書情報の要求を送信し、各台帳システム3から、当該要求に対する回答として各台帳システム3が出力した電子証明書情報を取得する（S201）。回答取得部18は、当該処理を、ユーザ端末4から電子証明書情報の照会の要求があったことに応じて実行してもよい。

[0068] 集計値算出部19は、回答取得部18により複数の台帳システム3から取得した複数の回答に含まれる同一の回答毎に、該回答を出力した台帳システム3に対応付けられた係数を集計することにより、複数の回答に含まれる同一の回答のそれぞれの集計値を算出する（S202）。

[0069] 決定部20は、例えば、集計値算出部19が算出した集計値に基づいて、各台帳システム3から取得した複数の回答のうち1つの回答を、電子証明書情報に一致する回答として決定する（S203）。

[0070] ここで、第1台帳システム3A、第2台帳システム3B、及び第3台帳システム3Cの3つの台帳システム3を有する電子署名管理システム100を例に、集計値の算出によって、1つの回答を電子証明書情報に一致する回答として決定する方法の具体例を説明する。

[0071]

[表1]

台帳システム	係数	回答
第1台帳システム3 A	1	123
第2台帳システム3 B	1	123
第3台帳システム3 C	1	456

[0072] 例えば、表1に示すとおり、所定の電子証明書情報の要求に対して、第1台帳システム3 Aからの回答が「1 2 3」、第2台帳システム3 Bからの回答が「1 2 3」、第3台帳システム3 Cからの回答が「4 5 6」であったものとする。第1台帳システム3 Aの係数、第2台帳システム3 Bの係数が、第3台帳システム3 Cの係数のいずれもが「1」である場合を想定する。

[0073] この場合、集計値算出部19は、回答「1 2 3」の集計値を、当該回答を出力した台帳システム3の係数の和、すなわち、第1台帳システム3 Aの係数「1」と、第2台帳システム3 Bの係数「1」との和である「2」として算出する。また、この場合、集計値算出部19は、回答「4 5 6」の集計値を、当該回答を出力した台帳システム3の係数の和、すなわち、第3台帳システム3 Cの係数「1」の和である「1」として算出する。そして、決定部20は、全ての回答（回答「1 2 3」及び回答「4 5 6」）それぞれの集計値のうち、回答「1 2 3」の集計値「2」が最も高いため、当該回答「1 2 3」を、電子証明書情報に一致する回答であると決定する。

[0074] なお、このように、第1台帳システム3 Aの係数、第2台帳システム3 Bの係数が、第3台帳システム3 Cの係数のいずれもが「1」である場合のように、全ての台帳システム3の係数が等しい場合は、実質的に、複数の台帳システム3による多数決によって、1つの回答が電子証明書情報に一致する回答として決定されることとなる。また、実施形態に係る電子署名管理システム100が有する台帳システム3の数が奇数である場合、原則として、集計値が最も高い回答の数は1つに絞られるため、電子証明書情報に一致する回答としての決定を効率的に行うことが可能となる。

[0075]

[表2]

台帳システム	係数	回答
第1台帳システム3 A	1	123
第2台帳システム3 B	1.5	123
第3台帳システム3 C	3	456

[0076] また、例えば、表2に示すとおり、所定の電子証明書情報の要求に対して、第1台帳システム3 Aからの回答が「1 2 3」、第2台帳システム3 Bからの回答が「1 2 3」、第3台帳システム3 Cからの回答が「4 5 6」であったものとする。第1台帳システム3 Aの係数が「1」、第2台帳システム3 Bの係数が「1. 5」、第3台帳システム3 Cの係数が「3」である場合を想定する。

[0077] この場合、集計値算出部19は、回答「1 2 3」の集計値を、当該回答を出力した台帳システム3の係数の和、すなわち、第1台帳システム3 Aの係数「1」と、第2台帳システム3 Bの係数「1. 5」との和である「2. 5」として算出する。また、この場合、集計値算出部19は、回答「4 5 6」の集計値を、当該回答を出力した台帳システム3の係数の和、すなわち、第3台帳システム3 Cの係数「3」の和である「3」として算出する。そして、決定部20は、全ての回答（回答「1 2 3」及び回答「4 5 6」）それぞれの集計値のうち、回答「4 5 6」の集計値「3」が最も高いため、当該回答「4 5 6」を、電子証明書情報に一致する回答であると決定する。

[0078] 送受信部21は、決定部20により電子証明書情報に一致する回答として決定された回答を、ユーザ端末4に送信する（S204）。

[0079] （4）付記

上述した実施形態では、電子文書（電子コンテンツ）の改変の有無の判定処理を、署名指示に応じて電子署名を生成するタイミング（ステップS110、S206、S214、S307）で行うものとした。しかしながら、当該改変の有無の判定処理は、これらタイミングに限られず、例えば、ユーザが任意のタイミングで、ユーザ端末4を介して管理装置1に判定を要求したタイミングに実行されてもよい。この際、ユーザ端末4は、例えば、ユーザ

が判定処理の対象として指定した電子署名の情報を受け付けて、当該情報を判定の要求に含めて管理装置 1 に送信してもよい。管理装置 1 は、指定された電子署名に係る署名前ハッシュ値と、指定された電子署名よりも 1 つ前の電子署名の署名後ハッシュ値とを比較し、両者が一致する場合には、指定された電子署名に際して電子文書（電子コンテンツ）は改変していないと判定し、両者が一致しない場合には、指定された電子署名に際して電子文書（電子コンテンツ）は改変していると判定してもよい。

[0080] 上述した電子署名管理システム 100 は、契約の締結後に、任意のユーザが契約内容の修正を行う場合にも適用可能である。すなわち、まず、例えば、ユーザは、締結済みの契約の内容（納期や金額など）の修正が必要になった場合、ユーザ端末 4 において、対象となる電子文書を取得する操作を行う。これにより、ユーザ端末 4 は、管理装置 1 を介して電子文書データベース 2 から対象となる電子文書を取得する。次に、ユーザ端末 4 は、ユーザの操作に応じて、電子文書を適宜、修正する。そして、ユーザ端末 4 は、ユーザの操作に応じて、修正された電子文書（修正電子文書）に対する署名指示を管理装置 1 に送信する。管理装置 1 は、修正電子文書に対する電子署名を生成し、これを修正電子文書に付与する。

[0081] 電子署名が付与された修正電子文書は、例えば、管理装置 1 から他のユーザ（契約の相手方等）が利用するユーザ端末 4 に送信されてもよい。そして、他のユーザは、ユーザ端末 4 に表示された修正電子文書の内容を確認した上で、修正電子文書に対する電子署名の操作をユーザ端末 4 に対して行う。ユーザ端末 4 は、署名指示を管理装置 1 に送信し、管理装置 1 は、他のユーザの電子署名を生成し、これを修正電子文書（上記ユーザの電子署名が付与されたもの）に更に付与する。これにより、例えば修正覚書を交わさずに同一の電子文書のファイルの上で、契約内容の修正が可能となる。従来の電子署名では、電子文書の内容やこれに基づくハッシュ値が変わることで、元の電子署名が不正になってしまう場合があった。一方、実施形態に係る電子署名管理システム 100 では、電子署名によって電子文書のハッシュ値が変化

しても、シリーズID（系統識別情報）によって互いに対応付けられた一連の電子署名を確認することが可能であるため、契約内容の修正の管理も簡易に行うことが可能となる。

- [0082] 上述した電子署名管理システム100は、電子署名によって電子コンテンツのハッシュ値が変化しても、シリーズID（系統識別情報）によって互いに対応付けられた一連の電子署名を確認することが可能であるため、契約に限らず、電子署名が連続的に付与されることが想定されるものであれば任意の電子コンテンツについて適用可能である。例えば、電子署名管理システム100は、政治活動における署名運動等において、署名簿の電子文書に対して複数の署名者が順次に電子署名を行う場合にも適用可能である。

符号の説明

- [0083] 1…管理装置、2…電子コンテンツデータベース、3、3A、3B、3C…台帳システム、4、4A、4B、4C、4D…ユーザ端末、11…文書管理部、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、16…電子証明書生成部、17…電子証明書情報格納部、18…回答取得部、19…集計値算出部、20…決定部、21…送受信部、41…撮像部、42…識別子取得部、43…ハッシュ値算出部、44…整合性確認部、45…出力部、46…操作受付部、47…送受信部、100…電子署名管理システム、N…通信ネットワーク、S…電子署名、D…電子コンテンツ、D0、D1、D2…電子文書

請求の範囲

- [請求項1] 電子コンテンツに対する電子署名を管理するための管理装置であって、
- 電子コンテンツに対する署名の指示を取得する取得部と、
- 前記指示に応じて電子署名を生成する署名生成部と、
- 生成された前記電子署名を前記電子コンテンツに付与する付与部と、
- 、
- 前記電子署名に関する電子証明書を生成する電子証明書生成部と、
- 複数の台帳システムの各台帳システムに、前記電子証明書の少なくとも一部である電子証明書情報を格納するための処理を実行する電子証明書情報格納部と、
- 前記複数の台帳システムのそれぞれに、各台帳システムに格納されている前記電子証明書情報の要求を送信することにより、前記要求に対する前記複数の台帳システムのそれぞれからの出力である複数の回答を取得する回答取得部と、
- 前記複数の回答に含まれる同一の回答毎に、該回答を出力した前記台帳システムに対応付けられた係数を集計することにより、前記複数の回答に含まれる前記同一の回答のそれぞれの集計値を算出する集計値算出部と、
- 前記集計値に基づいて、前記複数の回答のうち1つの回答を前記電子証明書情報に一致する回答として決定する決定部と、
- 前記1つの回答を出力する出力部と、
- を備える管理装置。
- [請求項2] 前記決定部は、前記集計値が最も高い回答を、前記1つの回答に決定する、請求項1に記載の管理装置。
- [請求項3] 前記複数の台帳システムの少なくとも1つは、分散型台帳システムである、請求項1に記載の管理装置。
- [請求項4] 前記係数は、前記台帳システムの特性を示す特性情報に基づいて定

められる、請求項 1 に記載の管理装置。

[請求項5] 前記特性情報は、前記台帳システムがデータの格納に用いるアルゴリズム、及び前記台帳システムが含むノードの数、のうち少なくとも 1 つに基づいて定められる、請求項 4 に記載の管理装置。

[請求項6] 前記複数の台帳システムのそれぞれに対応付けられた前記係数は等しい、請求項 1 に記載の管理装置。

[請求項7] 前記複数の台帳システムの数 は奇数である、請求項 6 に記載の管理装置。

[請求項8] 前記電子コンテンツは、電子文書である、請求項 1 に記載の管理装置。

[請求項9] 前記電子証明書情報は、前記電子コンテンツに基づいて生成されるハッシュ値である、請求項 1 に記載の管理装置。

[請求項10] 電子コンテンツに対する電子署名を管理するための管理装置が実行する制御方法であって、

電子コンテンツに対する署名の指示を取得するステップと、

前記指示に応じて電子署名を生成するステップと、

生成された前記電子署名を前記電子コンテンツに付与するステップと、

前記電子署名に関する電子証明書を生成するステップと、

複数の台帳システムの各台帳システムに、前記電子証明書の少なくとも一部である電子証明書情報を格納するための処理を実行するステップと、

前記複数の台帳システムのそれぞれに、各台帳システムに格納されている前記電子証明書情報の要求を送信することにより、前記要求に対する前記複数の台帳システムのそれぞれからの出力である複数の回答を取得するステップと、

前記複数の回答に含まれる同一の回答毎に、該回答を出力した前記台帳システムに対応付けられた係数を集計することにより、前記複数の

の回答に含まれる前記同一の回答のそれぞれの集計値を算出するステップと、

前記集計値に基づいて、前記複数の回答のうち1つの回答を前記電子証明書情報に一致する回答として決定するステップと、

前記1つの回答を出力するステップと、
を含む制御方法。

[請求項11]

情報処理装置を、電子コンテンツに対する電子署名を管理するための管理装置として機能させるためのプログラムであって、前記管理装置を、

電子コンテンツに対する署名の指示を取得する取得部と、
前記指示に応じて電子署名を生成する署名生成部と、
生成された前記電子署名を前記電子コンテンツに付与する付与部と、
、

前記電子署名に関する電子証明書を生成する電子証明書生成部と、
複数の台帳システムの各台帳システムに、前記電子証明書の少なくとも一部である電子証明書情報を格納するための処理を実行する電子証明書情報格納部と、

前記複数の台帳システムのそれぞれに、各台帳システムに格納されている前記電子証明書情報の要求を送信することにより、前記要求に対する前記複数の台帳システムのそれぞれからの出力である複数の回答を取得する回答取得部と、

前記複数の回答に含まれる同一の回答毎に、該回答を出力した前記台帳システムに対応付けられた係数を集計することにより、前記複数の回答に含まれる前記同一の回答のそれぞれの集計値を算出する集計値算出部と、

前記集計値に基づいて、前記複数の回答のうち1つの回答を前記電子証明書情報に一致する回答として決定する決定部と、

前記1つの回答を出力する出力部と、

として機能させるためのプログラム。