

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] 電子文書等の電子コンテンツに対して、改変が無いことを証明すること等を目的として、電子署名を行う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管理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] しかしながら、特許文献1の電子署名管理システムにおいて生成される署名値には、例えば署名者が任意に入力した事項を署名値に含めることはできない。そのため、電子文書に対して当事者がどのような意図をもって電子署名を行うかを把握することは困難である。

[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、署名者による電子署名の意図を確認することが可能な管理装置、管理装置の制御方法、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

[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と、該署名の内容を示す情報である署名内容情報とを取得する指示取得部と、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であって、署名

内容情報を含む電子証明書を生成する電子証明書生成部と、電子証明書を所定の記憶部に格納する格納部と、を備える。

[0007] これにより、署名指示に応じて電子コンテンツに対して電子署名が付与される場合、電子コンテンツに対する署名の内容を示す情報である署名内容情報を含む電子証明書が所定の記憶部に格納される。これにより、電子証明書において、署名内容情報が記録されるため、電子証明書を確認することにより、署名者による電子署名の意図を確認することが可能となる。

発明の効果

[0008] 本発明によれば、署名者による電子署名の意図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]実施形態に係るユーザ端末4の構成を示すブロック図である。

[図6A]実施形態に係る電子署名管理システム100が実行する動作処理の一例を示すシーケンス図である。

[図6B]実施形態に係る電子署名管理システム100が実行する動作処理の他の一例を示すシーケンス図である。

[図6C]実施形態に係る電子署名管理システム100が実行する動作処理の更に他の一例を示すシーケンス図である。

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、電子証明書データベース3、及び複数のユーザ端末4等を含む。管理装置1は、電子コンテンツデータベース2及び電子証明書データベース3それぞれに対して、これらデータベースに格納される情報を管理（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、複数のユーザ端末と互いに情報を送受信可能に接続される。

[0013] ここで、本実施形態では、例えば、ユーザは、商品・役務の提供を受注する受注企業と、受注企業に対して商品・役務を発注する発注企業と、受注企業及び発注企業間の受発注に係る債権に対してファクタリングを行うファクタリング企業と、ファクタリングにおける譲渡代金の収納を代行する収納代行企業とを含む。また、例えば、複数のユーザ端末4は、受注企業が利用するユーザ端末4Aと、発注企業が利用するユーザ端末4Bと、ファクタリング企業が利用するユーザ端末4Cと、収納代行企業の担当者が利用するユーザ端末4Dとを含む。

[0014] 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。

[0015] 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。

[0016] 管理装置1は、図1に示すように、電子証明書データベース3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の電子証明書を電子証明書データベース3に格納する。電子証明書データベース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電子証明書データベース3に格納する。

[0017] 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。

[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、電子証明書データベース3に保持された電子証明書に含まれる情報を取得し、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、電子証明書格納部17と、送受信部18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、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。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。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、電子証明書データベース 3 に記憶される。

[0026] 電子証明書格納部 17 は、生成された電子証明書を、電子証明書データベース 3 に格納する。

[0027] 図 4 は、電子証明書データベース 3 に記憶され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 つずつ電子証明書データベース 3 に追加されていく。

[0028] 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。

[0029] 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。

[0030] 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。

[0031] 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ことを示す情報）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。

[0032] 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。

[0033] 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。

- [0034] 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。
- [0035] 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。
- [0036] なお、上述した電子証明書はあくまでも例示であって、本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。
- [0037] 送受信部18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18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18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。
- [0038] 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。

[0039] (2-2) ユーザ端末4

図5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44と、整合性確認部45と、出力部46と、操作受付部47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。

[0040] 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。

[0041] 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。

[0042] ハッシュ値算出部44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44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44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44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。

[0043] 整合性確認部45は、管理装置1に記憶された電子証明書に基づいて、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45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44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45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に改変が無いかな否かを判定してもよい。また、整合性確認部45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に改変が無いかな否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、電子証明書データベース 3 に記憶されたハッシュ値（原文ハッシュ値、署名前ハッシュ値、及び署名後ハッシュ値）と照会等を行うことで、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、電子証明書データベース 3 による照会により判定が行われてもよい。

[0044] 出力部 4 6 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 4 6 は、電子証明書データベース 3 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 6 は、整合性確認部 4 5 による整合性の確認結果を出力する。

[0045] 操作受付部 4 7 は、ユーザの各種の操作を受け付ける。操作受付部 4 7 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 7 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。

[0046] 送受信部 4 8 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 8 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 8 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。

[0047] （3）動作例

図 6 A～図 6 C は、実施形態に係る電子署名管理システム 1 0 0 が実行する動作処理の一例を示すシーケンス図である。以下では、発注企業から受注企業に対して、受注企業が提供する商品・役務の発注があったため、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D0の作成は、ユーザ端末4A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D0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4Aが、ユーザ端末4A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、本実施形態に係る電子署名管理システム100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。

[0048] (3-1) 債権発生

図6Aは、債権発生に関するシーケンス図である。受注企業の担当者が利用するユーザ端末4Aは、受注企業の担当者による電子文書D0に対する署名指示の操作を受け付けると、電子文書D0に対する署名指示を管理装置1に送信する(S101)。管理装置1は、電子文書D0に対する署名指示をユーザ端末4Aから受信する(S102)。

[0049] 電子文書D0に対する署名指示は、例えば、電子文書D0のデータ自体を含んでもよいし、或いは、電子文書データベース2やユーザ端末4Aがアクセス可能な記憶部等に格納された電子文書D0を特定するための情報(シリーズID等)を含んでもよい。また、署名指示は、例えば、電子証明書データベース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。

[0050] 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S1を生成し、また、電子証明書を生成する(S103)。電子証明書の生成に関して、管理装置1は、電子署名S1を付与する直前の電子文書D0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）を、電子証明書データベース 3 に格納する（S 1 0 4）。

[0051] 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。

[0052] 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。

[0053] 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）。

[0054] 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、電子証明書データベース 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。

[0055] 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S2を生成し、また、電子証明書を生成する(S110)。電子証明書の生成に関して、管理装置1は、電子署名S2を付与する直前の電子文書D1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S2を付与した後の電子文書D2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D0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)を、電子証明書データベース3に格納する(S111)。

[0056] 管理装置1は、電子文書D1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S2の付与対象である電子文書D1の内容が、1つ前の電子署名S1が付与された直後における電子文書D1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比較した上で、両者が一致していれば、電子文書D1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D1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4B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S2を行うに際して、対象となる電子文書D1の内容の連続性を確認することが可能となる。

[0057] 管理装置1は、生成された電子署名S2を電子文書D1に付与することにより、電子文書D2を生成する。そして、管理装置1は、生成された電子文書D2をユーザ端末4Bに送信する(S112)。ユーザ端末4Bは、受信した電子文書D2を、ユーザ端末4Bがアクセス可能な記憶部に格納してもよい。

[0058] 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。

[0059] （3－2）債権譲渡

図6 Bは、債権譲渡に関するシーケンス図である。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 2が示す債権に関する譲渡条件の入力の操作を受け付ける（S 2 0 1）。譲渡条件の内容は特に限定されず、債権に関する任意の項目（金額及び期日等）を含んでもよい。入力された譲渡条件は、ユーザ端末4 Aから管理装置1に送信され、管理装置1は、これを電子文書データベース2に検索可能に記録する。

[0060] ファクタリング企業の担当者が利用するユーザ端末4 Cは、ファクタリング企業の担当者による操作に応じて、債権の検索の処理を実行する（S 2 0 2）。例えば、ユーザ端末4 Cは、ファクタリング企業の担当者が入力した金額等の譲渡条件を含む検索要求を、管理装置1に送信する。管理装置1は、ユーザ端末4 Cから受信した検索要求に応じて、当該検索要求に含まれる譲渡条件をキーとして債権を検索し、検索結果をユーザ端末4 Cに送信する。

[0061] ここでは、検索結果として電子文書D 2がヒットし、当該電子文書D 2に関する情報が管理装置1からユーザ端末4 Cに送信されたものとする。ファクタリング企業の担当者は、電子文書D 2に関する情報を確認した上で、当該電子文書D 2に係る債権を買い取ることを決定すると、ユーザ端末4 Cに、当該債権の買取の申請を入力する。ユーザ端末4 Cは、買取の申請を、原債権者である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 2

03)。なお、当該送信処理は、管理装置1を介して実行されてもよい。

[0062] 原債権者である受注企業の担当者は、ファクタリング企業の担当者による買取の申請を確認し、債権を譲渡することを決定した場合、ユーザ端末4Aに、電子文書D2に対する、債権譲渡の承諾のための署名指示を入力する。ユーザ端末4Aは、当該操作に応じて、電子文書D2に対する署名指示を管理装置1に送信する(S204)。管理装置1は、電子文書D2に対する署名指示をユーザ端末4Aから受信する(S205)。

[0063] 電子文書D2に対する署名指示は、例えば、電子文書D2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4Aがアクセス可能な記憶部等に格納された電子文書D2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、電子証明書データベース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「本請求書に記載の請求権を譲渡した」との署名内容が示されている。

[0064] 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S3を生成し、また、電子証明書を生成する(S206)。電子証明書データの生成に関して、管理装置1は、電子署名S3を付与する直前の電子文書D2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S3を付与した後の電子文書D3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D0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3行目の電子証明書)を、電子証明書データベース3に格納する(S207)。

[0065] 管理装置1は、電子文書D2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S3の付与対象である電子文書D2

の内容が、1つ前の電子署名S2が付与された直後における電子文書D2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2行目の電子証明書の署名後ハッシュ値と、3行目の電子証明書の署名前ハッシュ値とを比較した上で、両者が一致していれば、電子文書D2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D2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4Aに送信する等して出力してもよい。これにより、受注企業の担当者は、電子署名S3を行うに際して、対象となる電子文書D2の内容の連続性を確認することが可能となる。

[0066] 管理装置1は、生成された電子署名S3を電子文書D2に付与することにより、電子文書D3を生成する。そして、管理装置1は、生成された電子文書D3をユーザ端末4Cに送信する(S208)。ユーザ端末4Cは、受信した電子文書D3を、ユーザ端末4Cがアクセス可能な記憶部に格納してもよい。

[0067] ユーザ端末4Cは、電子文書D3を表示し、ファクタリング企業の担当者は、電子文書D3の内容を確認する(S209)。ユーザ端末4Cは、ファクタリング企業の担当者が譲渡代金の入金操作を行うと、当該操作を受け付け、譲渡代金の入金処理を実行する(S210)。譲渡代金の入金処理により、例えば、ファクタリング企業の口座から収納代行企業の口座へ、譲渡代金が送金される。収納代行企業の担当者が利用するユーザ端末4Dは、収納代行企業の担当者の操作に応じて、ユーザ端末4Cから受け付けた譲渡代金の入金確認処理を実行する(S211)。

[0068] 新債権者であるファクタリング企業の担当者は、譲渡代金の支払及び受領を確認した上で、ユーザ端末4Cに、電子文書D3に対する、債権譲受の登録のための署名指示を入力する。ユーザ端末4Cは、当該操作に応じて、電子文書D3に対する署名指示を管理装置1に送信する(S212)。管理装置1は、電子文書D3に対する署名指示をユーザ端末4Cから受信する(S213)。

- [0069] 電子文書D 3に対する署名指示は、例えば、電子文書D 3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等に格納された電子文書D 3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、電子証明書データベース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、ファクタリング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、「本請求書に記載の請求権を譲受した」との署名内容が示されている。
- [0070] 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 4を生成し、また、電子証明書を生成する（S 2 1 4）。電子証明書の生成に関して、管理装置1は、電子署名S 4を付与する直前の電子文書D 3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 4を付与した後の電子文書D 4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4行目の電子証明書）を、電子証明書データベース3に格納する（S 2 1 5）。
- [0071] 管理装置1は、電子文書D 3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 4の付与対象である電子文書D 3の内容が、1つ前の電子署名S 3が付与された直後における電子文書D 3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3行目の電子証明書の署名後ハッシュ値と、4行目の電子証明書の署名前ハッシュ値とを比較した上で、両者が一致していれば、電子文書D 3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 3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 Cに送信する等して出力してもよい。これにより、ファクタリング企業の担当者は、電子署名S 4を行うに際して、対象となる電子文書D 3の内容の連続性を確

認することが可能となる。

[0072] 管理装置 1 は、生成された電子署名 S 4 を電子文書 D 3 に付与することにより、電子文書 D 4 を生成する。そして、管理装置 1 は、生成された電子文書 D 4 をユーザ端末 4 C に送信する (S 2 1 6)。

[0073] ユーザ端末 4 C は、電子文書 D 4 を表示し、ファクタリング企業の担当者はこれを確認する (S 2 1 7)。ユーザ端末 4 C は、ファクタリング企業の担当者が譲渡代金の支払依頼操作を行うと、当該操作を受け付け、譲渡代金の支払依頼を、収納代行企業の担当者が利用するユーザ端末 4 D に送信する (S 2 1 8)。収納代行企業の担当者が利用するユーザ端末 4 D は、ユーザ端末 4 C から譲渡代金の支払依頼を受信すると、収納代行企業の担当者による操作に応じて、譲渡代金の支払処理を実行する (S 2 1 9)。譲渡代金の支払処理により、例えば、収納代行企業の口座から受注企業の口座へ、譲渡代金が入金される。受注企業の担当者が利用するユーザ端末 4 A は、受注企業の担当者の操作に応じて、ユーザ端末 4 D から受け付けた譲渡代金の支払確認処理を実行する (S 2 2 0)。

[0074] (3-3) 債権消滅

図 6 C は、債権消滅に関するシーケンス図である。発注企業の担当者が利用するユーザ端末 4 B は、発注企業の担当者の操作に応じて、電子文書 D 4 に係る買掛金の支払処理を実行する (S 3 0 1)。買掛金の支払処理により、例えば、発注企業の口座から収納代行企業の口座へ、買掛金が送金される。収納代行企業の担当者が利用するユーザ端末 4 D は、収納代行企業の担当者の操作に応じて、ユーザ端末 4 B から受け付けた買掛金の入金確認処理を実行する (S 3 0 2)。収納代行企業の担当者が利用するユーザ端末 4 D は、収納代行企業の担当者による操作に応じて、買掛金の支払処理を実行する (S 3 0 3)。買掛金の支払処理により、例えば、収納代行企業の口座からファクタリング企業の口座へ、買掛金が入金される。ファクタリング企業の担当者が利用するユーザ端末 4 C は、ファクタリング企業の担当者の操作に応じて、ユーザ端末 4 D から受け付けた買掛金の支払確認処理を実行する (

S 3 0 4)。

[0075] 新債権者であるファクタリング企業の担当者は、買掛金の支払を確認した上で、ユーザ端末4 Cに、電子文書D 4に対する、債権消滅の登録のための署名指示を入力する。ユーザ端末4 Cは、当該操作に応じて、電子文書D 4に対する署名指示を管理装置1に送信する(S 3 0 5)。管理装置1は、電子文書D 4に対する署名指示をユーザ端末4 Cから受信する(S 3 0 6)。

[0076] 電子文書D 4に対する署名指示は、例えば、電子文書D 4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等に格納された電子文書D 4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、電子証明書データベース3に記録される任意の項目(ファクタリング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、ファクタリング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、「請求通りに支払われた」との署名内容が示されている。

[0077] 管理装置1は、署名指示に基づいて、ファクタリング企業の担当者による電子署名S 5を生成し、また、電子証明書を生成する(S 3 0 7)。電子証明書の生成に関して、管理装置1は、電子署名S 5を行う直前の電子文書D 4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 5を付与した後の電子文書D 5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5行目の電子証明書)を、電子証明書データベース3に格納する(S 3 0 8)。

[0078] 管理装置1は、電子文書D 4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 5の付与対象である電子文書D 4の内容が、1つ前の電子署名S 4が付与された直後における電子文書D 4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 4 行目の電子証明書の署名後ハッシュ値と、5 行目の電子証明書の署名前ハッシュ値とを比較した上で、両者が一致していれば、電子文書 D 4 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 4 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 C に送信する等して出力してもよい。これにより、ファクタリング企業の担当者は、電子署名 S 5 を行うに際して、対象となる電子文書 D 4 の内容の連続性を確認することが可能となる。

[0079] 管理装置 1 は、生成された電子署名 S 5 を電子文書 D 4 に付与することにより、電子文書 D 5 を生成する。そして、管理装置 1 は、生成された電子文書 D 5 をユーザ端末 4 C に送信する（S 3 0 9）。ユーザ端末 4 C は、電子文書 D 5 を表示し、ファクタリング企業の担当者はこれを確認する（S 3 1 0）。

[0080] （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 S 1 1 0、S 2 0 6、S 2 1 4、S 3 0 7）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。

[0081] 上述した電子署名管理システム 1 0 0 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。

[0082] 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、本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。

[0083] 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

[0084] 1…管理装置、2…電子コンテンツデータベース、3…電子証明書データベース、4、4 A、4 B、4 C、4 D…ユーザ端末、1 1…文書管理部、1 2…指示取得部、1 3…ユーザ情報取得部、1 4…署名生成部、1 5…付与部、1 6…電子証明書生成部、1 7…電子証明書格納部、1 8…送受信部、4 1…撮像部、4 2…識別子取得部、4 3…保持情報取得部、4 4…ハッシュ値算出部、4 5…整合性確認部、4 6…出力部、4 7…操作受付部、4 8…送受信部、N…通信ネットワーク、S…電子署名、D…電子コンテンツ、D 0、D 1、D 2、D 3、D 4、D 5…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つて、
- 前記電子コンテンツに対する署名の指示と、該署名の内容を示す情報である署名内容情報と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であつて、前記署名内容情報を含む電子証明書を生成する電子証明書生成部と、
- 前記電子証明書を所定の記憶部に格納する格納部と、
- を備える管理装置。
- [請求項2] 前記電子署名は、符号化された、前記電子証明書を識別するための識別子を含む、請求項1に記載の管理装置。
- [請求項3] 前記付与部は、前記電子署名を、前記電子コンテンツに視認可能に付与する、請求項1に記載の管理装置。
- [請求項4] 前記電子証明書生成部は、生成する前記電子証明書に、いずれの前記電子署名も含まない前記電子コンテンツのハッシュ値である原文ハッシュ値、前記電子署名が付与される前の前記電子コンテンツのハッシュ値である署名前ハッシュ値、及び、前記電子署名が付与された後の前記電子コンテンツのハッシュ値である署名後ハッシュ値の少なくともいずれかを更に含める、請求項1に記載の管理装置。
- [請求項5] 前記電子証明書生成部は、生成する前記電子証明書に、前記電子署名の順位を示す順位情報を更に含め、
- 前記管理装置は、
- 1つの前記電子証明書に含まれる前記署名後ハッシュ値と、前記1つの前記電子証明書に含まれる前記順位情報に次ぐ前記順位情報を含む前記電子証明書に含まれる署名前ハッシュ値とを比較する比較部

と、

前記比較部の比較結果を出力する出力部と、を更に備える、請求項4に記載の管理装置。

[請求項6] 前記電子コンテンツは、電子文書、又は画像である、請求項1に記載の管理装置。

[請求項7] 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の制御方法であって、

前記電子コンテンツに対する署名の指示と、該署名の内容を示す情報である署名内容情報と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であって、前記署名内容情報を含む電子証明書を生成するステップと、

前記電子証明書を所定の記憶部に格納するステップと、

を含む制御方法。

[請求項8] 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、

前記電子コンテンツに対する署名の指示と、該署名の内容を示す情報である署名内容情報と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であって、前記署名内容情報を含む電子証明書を生成する電子証明書生成部と、

前記電子証明書を前記所定の記憶部に格納する格納部と、

として機能させるためのプログラム。