

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7276539号
(P7276539)

(45)発行日 令和5年5月18日(2023.5.18)

(24)登録日 令和5年5月10日(2023.5.10)

(51)国際特許分類	F I
H 0 4 L 9/32 (2006.01)	H 0 4 L 9/32 2 0 0 Z
G 0 6 F 21/64 (2013.01)	G 0 6 F 21/64 3 5 0
G 0 6 Q 50/18 (2012.01)	G 0 6 Q 50/18 3 1 0

請求項の数 8 (全32頁)

(21)出願番号	特願2022-35326(P2022-35326)	(73)特許権者	000003207
(22)出願日	令和4年3月8日(2022.3.8)		トヨタ自動車株式会社
(62)分割の表示	特願2021-1450(P2021-1450)の分割		愛知県豊田市トヨタ町1番地
原出願日	令和3年1月7日(2021.1.7)	(74)代理人	110001195
(65)公開番号	特開2022-106690(P2022-106690 A)		弁理士法人深見特許事務所
(43)公開日	令和4年7月20日(2022.7.20)	(72)発明者	山室 直樹
審査請求日	令和4年3月8日(2022.3.8)		愛知県豊田市トヨタ町1番地 トヨタ自動車株式会社内
		(72)発明者	渡辺 淳也
			愛知県豊田市トヨタ町1番地 トヨタ自動車株式会社内
		(72)発明者	松本 茂樹
			愛知県豊田市トヨタ町1番地 トヨタ自動車株式会社内
		(72)発明者	竺原 慶和
			最終頁に続く

(54)【発明の名称】 データ管理装置およびデータ管理方法

(57)【特許請求の範囲】

【請求項1】

分散型台帳技術を用いてデータを管理するデータ管理装置であって、
分散型台帳を記憶する記憶装置と、
前記データの情報を含むトランザクションデータを前記分散型台帳に登録する制御装置と、
トラストサービスを提供する複数の認証局を選択可能に構成された通信装置とを備え、
前記複数の認証局の各々は、互いに異なる規格に基づく認証局であり、
前記制御装置は、

前記通信装置を介して、前記複数の認証局のうちの選択された少なくとも1つの認証局から提供されるトラストサービスにより得られる少なくとも1つの所定データを取得し、
前記少なくとも1つの所定データを前記分散型台帳に登録する、データ管理装置。

【請求項2】

前記複数の認証局の中から任意の認証局を選択することが可能に構成された入力装置をさらに備え、

前記制御装置は、前記通信装置を介して、前記入力装置への入力により選択された少なくとも1つの認証局から前記少なくとも1つの所定データを取得する、請求項1に記載のデータ管理装置。

【請求項3】

前記複数の認証局の各々は、秘密鍵および前記秘密鍵と対の公開鍵に対して電子証明書

を発行する鍵認証局であり、

前記電子証明書は、前記公開鍵の情報を含み、

前記少なくとも1つの所定データの各々は、電子証明書である、請求項1または請求項2に記載のデータ管理装置。

【請求項4】

前記記憶装置は、前記選択された少なくとも1つの鍵認証局が発行した少なくとも1つの前記電子証明書に対応する少なくとも1つの前記秘密鍵を記憶し、

前記制御装置は、前記少なくとも1つの秘密鍵を用いて少なくとも1つの電子署名を生成し、

前記生成された少なくとも1つの電子署名をトランザクションデータに含める、請求項3に記載のデータ管理装置。

【請求項5】

前記制御装置は、前記少なくとも1つの電子署名の各々を、対応する前記少なくとも1つの電子証明書に含まれる前記公開鍵の情報をを用いて復号し、

復号の結果に基づいて、前記少なくとも1つの電子署名の各々の有効性を検証する、請求項4に記載のデータ管理装置。

【請求項6】

前記データは、知的財産に関するデータである、請求項1から請求項5のいずれか1項に記載のデータ管理装置。

【請求項7】

分散型台帳技術を用いてデータを管理するデータ管理装置のデータ管理方法であって、

前記データ管理装置は、

分散型台帳を記憶する記憶装置と、

前記データの情報を含むトランザクションデータを前記分散型台帳に登録する制御装置と、

トラストサービスを提供する複数の認証局を選択可能に構成された通信装置とを備え、

前記複数の認証局の各々は、互いに異なる規格に基づく認証局であり、

前記データ管理方法は、

前記通信装置を介して、前記複数の認証局のうちの選択された少なくとも1つの認証局から提供されるトラストサービスにより得られる少なくとも1つの所定データを取得するステップと、

前記少なくとも1つの所定データを前記分散型台帳に登録するステップとを含む、データ管理方法。

【請求項8】

前記データ管理装置は、第1および第2のデータ管理装置を含み、

前記複数の認証局の各々は、秘密鍵および前記秘密鍵と対の公開鍵に対して電子証明書を発行する鍵認証局であり、

前記電子証明書は、前記公開鍵の情報を含み、

前記少なくとも1つの所定データの各々は、電子証明書であり、

前記第1のデータ管理装置は、前記選択された少なくとも1つの鍵認証局が発行した少なくとも1つの前記電子証明書に対応する少なくとも1つの前記秘密鍵を記憶し、

前記データ管理方法は、

前記第1のデータ管理装置が、前記少なくとも1つの秘密鍵を用いて少なくとも1つの電子署名を生成し、前記生成された少なくとも1つの電子署名をトランザクションデータに含めるステップと、

前記第2のデータ管理装置が、前記少なくとも1つの電子署名の各々を、対応する前記少なくとも1つの電子証明書に含まれる前記公開鍵の情報をを用いて復号し、復号の結果に基づいて、前記少なくとも1つの電子署名の各々の有効性を検証するステップとをさらに含む、請求項7に記載のデータ管理方法。

【発明の詳細な説明】

10

20

30

40

50

【技術分野】

【0001】

本開示は、分散型台帳技術を用いてデータを管理するデータ管理装置およびデータ管理方法に関する。

【背景技術】

【0002】

特開2019-46442号公報（特許文献1）には、特許等の知的財産に関するデータをブロックチェーン等の共用台帳に格納する知的財産管理システムが開示されている。この知的財産管理システムは、共用台帳のデータに基づいて公証データを生成し、当該公証データの公証を外部接続される公証サービスに依頼する。そして、知的財産管理システムは、公証日時を記録する。これにより、データの記録の正確性を保証している。

10

【先行技術文献】

【特許文献】

【0003】

【文献】特開2019-46442号公報

特表2019-521627号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

近年における事業の多国展開等に鑑み、複数の国や地域においてデータを記録した時刻の正確性を保証することが重要になってきている。しかしながら、ある国の認証サービスによる認証が、他の国においては公式に認められないというケースが起こり得る。そのため、たとえば、ある国の認証サービスによる認証を受けたデータは、当該認証サービスの属する国以外の国において、その認証により必ずしもデータを記録した時刻の正確性が保証されるものではない。複数の国や地域においてデータを記録した時刻の正確性を保証することができる仕組みが望まれている。

20

【0005】

本開示は、上記課題を解決するためになされたものであり、本開示の目的は、複数の国および／または地域において、データを記録した時刻の正確性を保証することである。

【課題を解決するための手段】

30

【0006】

（1）本開示のある局面に係るデータ管理装置は、分散型台帳技術を用いてデータを管理する。このデータ管理装置は、分散型台帳を記憶する記憶装置と、データの情報を含むトランザクションデータを分散型台帳に登録する制御装置と、複数の時刻認証局と通信可能に構成された通信装置とを備える。複数の時刻認証局の各々は、互いに異なる規格に基づく時刻認証局である。制御装置は、通信装置を介して、トランザクションデータを複数の時刻認証局のうちの選択された少なくとも1つの時刻認証局に送信して、当該選択された時刻認証局からトランザクションデータのタイムスタンプトークンを取得し、タイムスタンプトークンを分散型台帳に登録する。

【0007】

40

上記構成によれば、制御装置は、分散型台帳で管理する対象となるデータ（以下「対象データ」とも称する）の情報を含むトランザクションデータを、通信装置を介して複数の時刻認証局のうちの選択された少なくとも1つの時刻認証局に送信して、当該選択された時刻認証局からトランザクションデータのタイムスタンプトークンを取得する。そして、制御装置は、取得されたタイムスタンプトークンを分散型台帳に登録する。これにより、時刻認証局から取得したタイムスタンプトークンが分散型台帳で管理される。複数の時刻認証局の各々は、互いに異なる規格に基づく時刻認証局である。このような複数の時刻認証局からタイムスタンプトークンを取得して分散型台帳で管理することにより、複数の国および／または地域において、データを記録した時刻の正確性を保証することができる。

【0008】

50

(2) ある実施の形態においては、データ管理装置は、通信装置を介して、複数の時刻認証局の中から任意の時刻認証局を選択することが可能に構成された入力装置をさらに備える。制御装置は、入力装置への入力により選択された時刻認証局へトランザクションデータを送信する。

【0009】

たとえば、対象データの内容や属性等によって、複数の時刻認証局の全てからタイムスタンプトークンを取得する必要がない場合もある。上記構成によれば、データ管理装置のユーザは、タイムスタンプトークンを取得する時刻認証局を選択することができる。これにより、たとえば、タイムスタンプトークンを取得する必要がない時刻認証局からはタイムスタンプトークンを取得しないようにすることができるので、処理負荷を低減させることが可能となる。

【0010】

(3) ある実施の形態においては、制御装置は、通信装置を介して、トランザクションデータをハッシュ化して得られるハッシュ値を複数の時刻認証局のうちの選択された少なくとも1つの時刻認証局に送信して、当該選択された時刻認証局からハッシュ値のタイムスタンプトークンを取得し、タイムスタンプトークンを分散型台帳に登録する。

【0011】

上記構成によれば、制御装置は、対象データの情報を含むトランザクションデータのハッシュ値を、通信装置を介して複数の時刻認証局のうちの選択された少なくとも1つの時刻認証局に送信して、当該選択された時刻認証局からハッシュ値のタイムスタンプトークンを取得する。そして、制御装置は、取得されたタイムスタンプトークンを分散型台帳に登録する。これにより、時刻認証局から取得したタイムスタンプトークンが分散型台帳で管理される。このような構成によっても、複数の国および／または地域において、データを記録した時刻の正確性を保証することができる。

【0012】

(4) ある実施の形態においては、制御装置は、データを再度ハッシュ化し、再度ハッシュ化された値と、タイムスタンプトークンを取得したハッシュ値とを比較し、当該比較結果に基づいてデータの存在証明を検証する。

【0013】

上記構成によれば、データの存在証明を検証することができ、当該データがタイムスタンプトークンに含まれる時刻に存在していたこと、および、その時刻以降に当該データが改ざんされていないことを証明することができる。

【0014】

(5) ある実施の形態においては、データは、ID情報に紐付けられている。入力装置は、ID情報を選択可能に構成される。入力装置に対する操作により選択されたID情報に紐付けられた少なくとも1つのトランザクションデータを分散型台帳から読み出し、通信装置を介して、読み出された少なくとも1つのトランザクションデータを纏めてハッシュ化したハッシュデータを、複数の時刻認証局のうちの選択された少なくとも1つの時刻認証局に送信して、当該選択された時刻認証局からハッシュデータのタイムスタンプトークンを取得し、タイムスタンプトークンを分散型台帳に登録する。

【0015】

上記構成によれば、データ管理装置のユーザは、任意のタイミングでハッシュデータのタイムスタンプトークンを取得することができる。

【0016】

(6) ある実施の形態においては、制御装置は、ID情報に紐付けられた少なくとも1つのトランザクションデータを再度ハッシュ化し、再度ハッシュ化された値と、タイムスタンプトークンを取得したハッシュデータとを比較し、当該比較結果に基づいてデータの存在証明を検証する。

【0017】

上記構成によれば、ハッシュデータ単位でのデータの存在証明を検証することができる。

10

20

30

40

50

【0018】

(7) ある実施の形態においては、通信装置は、複数の鍵認証局と通信可能に構成される。複数の鍵認証局の各々は、互いに異なる規格に基づいて、秘密鍵および秘密鍵と対の公開鍵に対して電子証明書を発行する認証局である。電子証明書は、公開鍵の情報を含む。記憶装置は、複数の鍵認証局の各々に対応する秘密鍵、および、複数の鍵認証局の各々が発行した電子証明書を記憶する。制御装置は、複数の鍵認証局毎に秘密鍵を用いて電子署名を生成し、複数の鍵認証局毎の電子署名をトランザクションデータに含める。

【0019】

上記構成によれば、分散型台帳に登録される1つのトランザクションデータに、複数の認証局毎の電子署名が含まれる。電子署名の有効性は、規格の違いに起因して、国または地域によって異なり得る。規格の異なる複数の電子署名がトランザクションデータに含まれることにより、複数の国および／または地域でトランザクションデータに含まれた電子署名の有効性を証明することが可能となる。これにより、分散型台帳に登録されるデータの信頼性が高まり、第三者のなりすましやデータの改ざんを抑制することができる。

10

【0020】

(8) ある実施の形態においては、通信装置は、複数の鍵認証局と通信可能に構成される。複数の鍵認証局の各々は、互いに異なる規格に基づいて、秘密鍵および秘密鍵と対の公開鍵に対して電子証明書を発行する認証局である。電子証明書は、公開鍵の情報を含む。記憶装置は、複数の鍵認証局の各々に対応する秘密鍵、および、複数の鍵認証局の各々が発行した電子証明書を記憶する。制御装置は、複数の鍵認証局毎に秘密鍵を用いて電子署名を生成し、1つの処理に対して、複数の鍵認証局に対応する複数のトランザクションデータを分散型台帳に登録する。複数のトランザクションデータの各々には、対応した鍵認証局の電子署名が含まれる。

20

【0021】

上記構成によれば、1つの処理に対して、複数の鍵認証局に対応した複数のトランザクションデータが分散型台帳に登録される。上述のとおり、電子署名の有効性は、規格の違いに起因して、国または地域によって異なり得るが、1つの処理に対して、異なる規格に基づいた電子署名が含まれる複数のトランザクションデータが分散型台帳に登録されることにより、複数の国および／または地域で電子署名の有効性を証明することが可能となる。これにより、分散型台帳に登録されるデータの信頼性が高まり、第三者のなりすましやデータの改ざんを抑制することができる。

30

【0022】

(9) ある実施の形態においては、制御装置は、複数の鍵認証局毎の電子署名を、対応する複数の鍵認証局毎の電子証明書に含まれる公開鍵を用いて復号し、復号の結果に基づいて、複数の鍵認証局毎の電子署名の有効性を検証する。

【0023】

上記構成によれば、トランザクションデータに含まれる複数の電子署名、あるいは、トランザクションデータ毎に含まれる電子署名の有効性を検証することができる。

【0024】

(10) ある実施の形態においては、データは、知的財産に関するデータである。

40

知的財産に関するデータにおいては、先使用权等の観点から、そのデータを記録した時刻の正確性を保証することが重要であるが、上記構成によれば、知的財産に関するデータを記録した時刻の正確性を保証することができる。

【0025】

(11) 本開示の他の局面に係るデータ管理方法は、分散型台帳技術を用いてデータを管理するデータ管理装置のデータ管理方法である。データ管理装置は、分散型台帳を記憶する記憶装置と、データの情報を含むトランザクションデータを分散型台帳に登録する制御装置と、複数の時刻認証局と通信可能に構成された通信装置とを備える。複数の時刻認証局の各々は、互いに異なる規格に基づく時刻認証局である。データ管理方法は、トランザクションデータを複数の時刻認証局のうちの選択された少なくとも1つの時刻認証局に

50

送信するステップと、選択された時刻認証局からトランザクションデータのタイムスタンプトークンを取得するステップと、タイムスタンプトークンを分散型台帳に登録するステップとを含む。

【発明の効果】

【0026】

本開示によれば、複数の国および／または地域において、データを記録した時刻の正確性を保証することができる。

【図面の簡単な説明】

【0027】

【図1】実施の形態1に係るデータ管理システムの概略的な構成を示す図である。

10

【図2】DAGデータを説明するための図である。

【図3】トランザクションデータの生成を説明するための制御装置の機能ブロック図である。

【図4】存在証明の申請（タイムスタンプトークンの取得）の概要を説明するための図である。

【図5】DAGデータの作成から存在証明の申請（タイムスタンプトークンの取得）までの流れを説明するためのシーケンス図である。

【図6】存在証明の申請（タイムスタンプトークンの取得）をするためのインターフェース画面を説明するための図である。

【図7】図6の「存在証明の発行」のボタンを選択した場合に表示されるインターフェース画面を説明するための図である。

20

【図8】存在証明の申請（タイムスタンプトークンの取得）を説明するための制御装置の機能ブロック図である。

【図9】存在証明の検証の流れを説明するためのシーケンス図である。

【図10】存在証明の検証をするためのインターフェース画面を説明するための図である。

【図11】存在証明の検証を説明するための制御装置の機能ブロック図である。

【図12】電子署名の有効性の検証を説明するための制御装置の機能ブロック図である。

【図13】トランザクションデータを生成する処理の手順を示すフローチャートである。

【図14】発明情報の存在証明の申請をする処理の手順を示すフローチャートである。

【図15】存在証明を検証する処理の手順を示すフローチャートである。

30

【図16】電子署名の有効性を検証する処理の手順を示すフローチャートである。

【図17】実施の形態2に係るデータ管理システムの概略的な構成を示す図である。

【図18】ブロックチェーンデータを説明するための図である。

【図19】存在証明の申請（タイムスタンプトークンの取得）の概要を説明するための図である。

【発明を実施するための形態】

【0028】

以下、本開示の実施の形態について、図面を参照しながら詳細に説明する。実施の形態1では、分散型台帳技術を用いてデータを管理するデータ管理システムにおいて、DAG (Directed Acyclic Graph) を用いた分散型台帳技術が適用される例を説明する。実施の形態2では、分散型台帳技術を用いてデータを管理するデータ管理システムにおいて、ブロックチェーンを用いた分散型台帳技術が適用される例を説明する。なお、データ管理システムには、上記のDAGを用いた分散型台帳技術およびブロックチェーンを用いた分散型台帳技術以外の他の分散型台帳技術を適用することも可能である。なお、図中同一または相当部分には同一符号を付して、その説明は繰り返さない。

40

【0029】

〔実施の形態1〕

＜データ管理システムの全体構成＞

図1は、実施の形態1に係るデータ管理システム1の概略的な構成を示す図である。本実施の形態に係るデータ管理システム1は、複数の企業間でネットワークを形成して、特

50

許等の知的財産に関するデータを管理するためのシステムである。なお、データ管理システム1で管理されるデータは、知的財産に関するデータに限られるものではなく、種々のデータであってよい。

【0030】

図1を参照して、データ管理システム1は、4台のデータ管理装置100と、認証局群300と、時刻認証局群400とを備える。4台のデータ管理装置100の各々は、異なる企業（たとえば、A企業、B企業、C企業およびD企業）に帰属するデータ管理装置である。図1では、A企業のデータ管理装置100をデータ管理装置100と表記し、B企業、C企業およびD企業のデータ管理装置100をデータ管理装置100Aと表記するものとする。以下においては、A企業のデータ管理装置100について代表的に説明するが、データ管理装置100Aも同様の機能を有する。

10

【0031】

4台のデータ管理装置100、100Aは、ネットワークNWを形成している。実施の形態1に係るデータ管理システム1には、DAGを用いた分散型台帳技術が適用される。DAGを用いた分散型台帳（以下、単に「DAG」とも称する）には、特許等の知的財産に関するデータの記録の履歴等を含む種々の情報（記録情報）が含まれている。DAGには、データ管理システム1の運用が開始されてから現在までのすべての記録情報が記憶されている。なお、本実施の形態に係るデータ管理システム1においては、4台のデータ管理装置がネットワークNWを形成する例について説明するが、ネットワークNWを形成するデータ管理装置の台数は、任意であり、たとえば、4台未満であってもよいし、5台以上であってもよい。

20

【0032】

データ管理装置100は、たとえば、デスクトップ型のPC（Personal Computer）、ノート型のPC、タブレット端末、スマートフォン、または、通信機能を有するその他の情報処理端末である。データ管理装置100は、制御装置110と、ROM（Read Only Memory）120と、RAM（Random Access Memory）130と、通信装置140と、記憶装置150と、入力装置160と、表示装置170とを含む。制御装置110、ROM120、RAM130、通信装置140、記憶装置150、入力装置160、および表示装置170は、バス180に接続されている。また、データ管理装置100には、管理サーバ200が通信可能に接続されている。

30

【0033】

制御装置110は、たとえば、CPU（Central Processing Unit）を含む集積回路によって構成される。制御装置110は、ROM120に格納されている各種プログラムをRAM130に展開して実行する。各種プログラムには、オペレーティングシステム等が含まれる。RAM130は、ワーキングメモリとして機能し、各種プログラムの実行に必要な各種データを一時的に格納する。制御装置110は、複数の規格（たとえば、日本の規格、中国の規格、米国の規格およびEUの規格、等）に準拠して、それぞれの規格に準拠した秘密鍵（たとえば、後述の第1～第4秘密鍵）および公開鍵（たとえば、後述の第1～第4公開鍵）を生成する機能を有する。

【0034】

通信装置140は、外部の機器との通信が可能に構成される。外部の機器は、たとえば、データ管理装置100A、管理サーバ200、認証局群300および時刻認証局群400等を含む。通信装置140と外部の機器との通信は、インターネット、ワイドエリアネットワーク（WAN）、ローカルエリアネットワーク（LAN）、イーサネット（登録商標）ネットワーク、パブリックネットワーク、プライベートネットワーク、有線ネットワークまたは無線ネットワーク等、あるいは、これらの組み合わせを用いて行なわれる。

40

【0035】

記憶装置150は、たとえば、ハードディスクまたはフラッシュメモリ等の記憶媒体を含んで構成される。記憶装置150は、DAGデータ152を記憶する。なお、DAGデータ152が記憶されるのは、記憶装置150に限定されるものではなく、ROM120

50

、RAM 130、または、管理サーバ200に記憶されてもよい。DAGデータ152の詳細については、後述する。また、記憶装置150は、制御装置110により生成された秘密鍵および公開鍵を記憶する。また、記憶装置150は、認証局群300に含まれる複数の認証局の各々から発行された電子証明書を記憶する。なお、秘密鍵、公開鍵および電子証明書が記憶されるのは、記憶装置150に限定されるものではなく、ROM 120、RAM 130、または、管理サーバ200に記憶されてもよい。

【0036】

入力装置160は、入力デバイスを含む。入力デバイスは、たとえば、マウス、キーボード、タッチパネル、および／または、ユーザの操作を受け付けることが可能なその他の装置である。

【0037】

表示装置170は、ディスプレイを含む。表示装置170は、制御装置110からの制御信号に従って、ディスプレイに各種の画像を表示させる。ディスプレイは、たとえば、液晶ディスプレイ、有機EL (Electro Luminescence) ディスプレイ、または、その他の表示機器である。

【0038】

管理サーバ200は、特許等の知的財産に関するデータを記憶する。管理サーバ200は、データ管理装置100からの制御信号に従って知的財産に関するデータを記憶する。なお、知的財産に関するデータは、記憶装置150に記憶されてもよい。

【0039】

認証局群300は、複数の認証局を含む。認証局は、電子証明書を発行する認証機関に帰属するサーバを含む。電子証明書の申請者（本実施の形態においては、データ管理装置100）は、秘密鍵および公開鍵を生成し、生成された公開鍵を認証局に送信する。認証局は、申請者から受けた公開鍵に対して電子証明書を生成し、電子証明書を申請者に発行する。あるいは、認証局は、申請者（本実施の形態においては、データ管理装置100）の求めに応じて、秘密鍵および公開鍵、ならびに、電子証明書を生成し、これらを申請者に発行してもよい。認証局は、たとえば、公開鍵の情報を電子証明書に含めて発行する。認証局群300に含まれている複数の認証局の各々は、互いに異なる規格に準拠した電子証明書を発行する。本実施の形態においては、認証局群300には、第1認証局310、第2認証局320、第3認証局330および第4認証局340の4つの認証局が含まれている。なお、認証局群300に含まれる認証局の数は任意であり、たとえば4つ未満であってもよいし、5つ以上であってもよい。

【0040】

第1認証局310は、たとえば、日本の規格に準拠した電子証明書を発行する認証機関に帰属するサーバを含む。申請者は、日本の規格に準拠した第1秘密鍵および第1公開鍵を生成し、生成された第1公開鍵を第1認証局310に送信する。第1認証局310は、申請者から受けた第1公開鍵に対して第1電子証明書を生成し、第1電子証明書を申請者に発行する。なお、第1認証局310が第1秘密鍵および第1公開鍵を生成する場合には、第1認証局310は、申請者の求めに応じて、第1秘密鍵および第1公開鍵を生成し、第1秘密鍵、および、第1公開鍵を含めた第1電子証明書を申請者に発行する。第2認証局320は、たとえば、中国の規格に準拠した電子証明書を発行する認証機関に帰属するサーバを含む。申請者は、中国の規格に準拠した第2秘密鍵および第2公開鍵を生成し、生成された第2公開鍵を第2認証局320に送信する。第2認証局320は、申請者から受けた第2公開鍵に対して第2電子証明書を生成し、第2電子証明書を申請者に発行する。なお、第2認証局320が第2秘密鍵および第2公開鍵を生成する場合には、第2認証局320は、申請者の求めに応じて、第2秘密鍵および第2公開鍵を生成し、第2秘密鍵、および、第2公開鍵を含めた第2電子証明書を申請者に発行する。第3認証局330は、たとえば、米国の規格に準拠した電子証明書を発行する認証機関に帰属するサーバを含む。申請者は、米国の規格に準拠した第3秘密鍵および第3公開鍵を生成し、生成された第3公開鍵を第3認証局330に送信する。第3認証局330は、申請者から受けた第3

10

20

30

40

50

公開鍵に対して第3電子証明書を生成し、第3電子証明書を申請者に発行する。なお、第3認証局330が第3秘密鍵および第3公開鍵を生成する場合には、第3認証局330は、申請者の求めに応じて、第3秘密鍵および第3公開鍵を生成し、第3秘密鍵、および、第3公開鍵を含めた第3電子証明書を申請者に発行する。第4認証局340は、たとえば、EUの規格に準拠した電子証明書を発行する認証機関に帰属するサーバを含む。申請者は、EUの規格に準拠した第4秘密鍵および第4公開鍵を生成し、生成された第4公開鍵を第4認証局340に送信する。第4認証局340は、申請者から受けた第4公開鍵に対して第4電子証明書を生成し、第4電子証明書を申請者に発行する。なお、第4認証局340が第4秘密鍵および第4公開鍵を生成する場合には、第4認証局340は、申請者の求めに応じて、第4秘密鍵および第4公開鍵を生成し、第4秘密鍵、および、第4公開鍵を含めた第4電子証明書を申請者に発行する。

10

【0041】

本実施の形態では、第1秘密鍵、第1電子証明書、第2秘密鍵、第2電子証明書、第3秘密鍵、第3電子証明書、第4秘密鍵、および、第4電子証明書は、記憶装置150に記憶される。なお、認証局群300に含まれている第1認証局310、第2認証局320、第3認証局330および第4認証局340の各々は、本開示に係る「鍵認証局」の一例に相当する。

【0042】

時刻認証局群400は、複数の時刻認証局(TSA: Time Stamp Authority)を含む。時刻認証局は、タイムスタンプトークンを発行する認証機関に帰属するサーバを含む。時刻認証局は、申請者(本実施の形態においては、データ管理装置100)からのタイムスタンプ発行要求に応じて、タイムスタンプトークンを発行する。より具体的には、時刻認証局は、申請者(本実施の形態においては、データ管理装置100)から受信したデータ(ハッシュ値)に、国際標準時に追跡性がある時刻源に基づく時刻情報を結合させたタイムスタンプトークンを、申請者に送信する。データ管理装置100から時刻認証局に送信されるデータは、たとえば、トランザクションデータ(後述)のハッシュ値であってもよいし、ある発明のID(発明ID)に紐付けられた少なくとも1つのトランザクションデータを纏めてハッシュ化したハッシュ値(発明ハッシュ(後述))であってもよい。トランザクションデータの詳細は後述するが、トランザクションデータは、管理サーバ200に記憶された知的財産に関するデータのハッシュ値を含むデータである。ハッシュ値は、ハッシュ関数を用いてデータをハッシュ化した結果として得られる数値である。

20

30

【0043】

本実施の形態においては、時刻認証局群400は、第1時刻認証局410、第2時刻認証局420、第3時刻認証局430および第4時刻認証局440の4つの時刻認証局が含まれている。なお、時刻認証局群400に含まれる時刻認証局の数は任意であり、たとえば4つ未満であってもよいし、5つ以上であってもよい。

【0044】

第1時刻認証局410、第2時刻認証局420、第3時刻認証局430および第4時刻認証局440の各々は、国または地域で互いに異なる規格に基づく時刻認証局である。第1時刻認証局410は、たとえば、日本の規格に準拠したタイムスタンプを発行する時刻認証機関に帰属するサーバを含む。第2時刻認証局420は、たとえば、中国の規格に準拠したタイムスタンプを発行する時刻認証機関に帰属するサーバを含む。第3時刻認証局430は、たとえば、米国の規格に準拠したタイムスタンプを発行する時刻認証機関に帰属するサーバを含む。第4時刻認証局440は、たとえば、EUの規格に準拠したタイムスタンプを発行する時刻認証機関に帰属するサーバを含む。

40

【0045】

<DAGデータ>

図2は、DAGデータ152を説明するための図である。図2に示されるように、DAGデータ152は、1つのトランザクションデータを一方向に、かつ、複数に、かつ、巡回しないように繋いだ構成となっている。トランザクションデータは、トランザクション

50

を示すデータであり、その詳細は後述する。DAGデータ152には、データ管理システム1の運用が開始されてから現在までの、ネットワークNWを形成するデータ管理装置100、100Aにおける知的財産に関するデータ等の記録の履歴が記憶されている。DAGデータ152は、ネットワークNWを形成する全てのデータ管理装置100、100Aに記憶されている。これにより、仮にDAGデータ152があるユーザによって改ざんされたとしても、他の複数のユーザのDAGデータ152を基準として改ざんが防止される。
【0046】

図2に示す、本実施の形態に係るDAGデータ152の例においては、トランザクションデータは、当該トランザクションデータが対応するトランザクションよりも過去に発生した2つのトランザクションのトランザクションデータと繋がっている。これは、トランザクションデータが、当該トランザクションデータが対応するトランザクションよりも過去に発生した2つのトランザクションのトランザクションデータのハッシュ値を含む構成となっていることを示している。具体的に、トランザクションデータ153cをDAGデータ152に追加する場合を例として、本実施の形態に係る合意形成アルゴリズムを説明する。

【0047】

新たな知的財産に関するデータを登録する場合、データ管理装置100は、新たに登録する知的財産に関するデータ（たとえばドキュメント）を管理サーバ200に記憶させると、この処理を示すトランザクションのデータ（トランザクションデータ）153cを生成して、トランザクションデータ153cをネットワークNWへ送信する。このトランザクションデータ153cには、上記知的財産に関するデータ（ドキュメント）のハッシュ値が含まれる。このハッシュ値は、知的財産に関するデータを、ハッシュ関数を用いてハッシュ化し、ハッシュ化の結果として得られた数値である。さらに、このトランザクションデータ153cには、トランザクションデータ153cが対応するトランザクション（上記知的財産に関するデータの管理サーバ200への記憶）よりも過去に発生した2つのトランザクションのトランザクションデータ153a、153bのそれぞれのハッシュ値が含まれる。トランザクションデータ153cにトランザクションデータ153a、153bのそれぞれのハッシュ値が含まれていることは、トランザクションデータ153cの生成時にデータ管理装置100が、トランザクションデータ153a、153bを承認したことを示している。

【0048】

データ管理装置100は、トランザクションデータ153cを生成する場合に、DAGデータ152に含まれる過去のトランザクションデータから2つのトランザクションデータ153a、153bを選択する。そして、データ管理装置100は、選択されたトランザクションデータ153a、153bを承認するために、選択されたトランザクションデータ153a、153bの内容を検証する。さらに、データ管理装置100は、トランザクションデータ153a、153bが直接的または間接的に承認しているトランザクションデータを遡って検証し、不正なトランザクションデータを承認していないことを検証してもよい。直接的に承認しているとは、そのトランザクションデータのハッシュ値を含んでいることであり、たとえば、トランザクションデータ153a、153cを例にすれば、トランザクションデータ153cは、トランザクションデータ153aを直接的に承認している。間接的に承認しているとは、直接的に承認しているトランザクションデータが、そのトランザクションデータを直接的または間接的に承認していることであり、たとえば、トランザクションデータ153a、153c、153fを例にすれば、トランザクションデータ153fは、トランザクションデータ153aを直接的に承認しているトランザクションデータ153cのハッシュ値を含んでおり、トランザクションデータ153aを間接的に承認している。

【0049】

検証の手法は、たとえば、トランザクションデータに含まれる電子署名を用いた検証手法でもよいし、他の公知の検証手法であってもよい。トランザクションデータの内容の検

10

20

30

40

50

証を終えると、データ管理装置 100 は、検証したトランザクションデータ 153a, 153b をそれぞれハッシュ化し、これらのハッシュ値をトランザクションデータ 153c に含める。なお、2つのトランザクションデータ 153a, 153b の選択方法は、過去のトランザクションデータの中からランダムに選択する方法であってもよいし、たとえばマルコフ連鎖モンテカル口法のような選択アルゴリズムを用いた選択方法であってもよい。

【0050】

データ管理装置 100 からネットワーク NW へ送信されたトランザクションデータ 153c は、後にデータ管理装置 100A または／およびデータ管理装置 100 によって、上記の説明と同様にして承認される。たとえば、トランザクションデータ 153c は、トランザクションデータ 153d, 153f に承認されている。

10

【0051】

さらに、トランザクションデータの承認においては、トランザクションデータに対する荷重が考慮されてもよい。トランザクションデータには、当該トランザクションデータを直接的または間接的に承認しているトランザクションデータの荷重の総和である累積荷重が設定される。すなわち、累積荷重は、その値が大きいほど当該トランザクションデータを承認しているトランザクションデータが多いことを示す。換言すれば、累積荷重が大きいほど、トランザクションデータが有効である確率が高くなる。荷重は、トランザクションデータを生成した本人（たとえばデータ管理装置 100）が承認した場合と、他人（たとえばデータ管理装置 100A）が承認した場合とで、異なるように設定されてもよい。

【0052】

20

＜トランザクションデータ＞

トランザクションデータには、たとえば、発明 ID の情報、対象データ（知的財産に関するデータ：たとえばドキュメント）のハッシュ値、当該トランザクションデータをネットワーク NW へ向けてブロードキャストする（ネットワーク NW へ送信する）時刻情報、当該トランザクションデータの送信者情報、上述の過去のトランザクションデータのハッシュ値、および、電子署名、等が含まれる。トランザクションデータに含まれる知的財産に関するデータは、発明 ID に関連するデータである。発明 ID の情報および知的財産に関するデータのハッシュ値の詳細については、後に説明する。なお、トランザクションデータに含まれる時刻情報は、トランザクションデータが対応する処理（たとえば、対象データを管理サーバ 200 への記録する処理）の発生時刻を示す時刻情報であってもよい。

30

【0053】

トランザクションデータの送信者情報は、たとえば、データ管理装置 100 がネットワーク NW へ送信したトランザクションデータであれば、A 企業を示す情報である。なお、トランザクションデータの送信者情報は、さらに詳細に、ネットワーク NW へトランザクションデータを送信する操作を実行した部署（A 企業の一部門）を示す情報であってもよいし、ネットワーク NW へトランザクションデータを送信する操作を実行した個人（A 企業の従業員）を示す情報であってもよい。

【0054】

＜トランザクションデータの生成＞

図 3 は、トランザクションデータの生成を説明するための制御装置 110 の機能ブロック図である。図 3 を参照して、制御装置 110 は、情報取得部 1101 と、トランザクションデータ生成部 1103 と、電子署名部 1105 と、トランザクションデータ送信部 1107 とを含む。制御装置 110 は、たとえば、ROM 120 に記憶されたプログラムを実行することにより、情報取得部 1101、トランザクションデータ生成部 1103、電子署名部 1105、および、トランザクションデータ送信部 1107 として機能する。なお、情報取得部 1101、トランザクションデータ生成部 1103、電子署名部 1105、および、トランザクションデータ送信部 1107 は、たとえば、専用のハードウェア（電子回路）により実現されてもよい。

40

【0055】

情報取得部 1101 は、入力装置 160 を介して、ユーザからの要求情報を取得する。

50

要求情報は、たとえば、知的財産に関するデータの記録等の要求を含む。たとえば、データ管理装置100のユーザが、入力装置160を操作して、知的財産に関するデータを管理サーバ200に保存（登録）すると、知的財産に関するデータの記録等の要求が情報取得部1101に入力される。また、詳細は後述するが、情報取得部1101は、通信装置140を介して、時刻認証局群400からタイムスタンプトークンを取得する。情報取得部1101は、要求情報またはタイムスタンプトークンを取得すると、要求情報またはタイムスタンプトークンをトランザクションデータ生成部1103に出力する。

【0056】

トランザクションデータ生成部1103は、ネットワークNWへ送信するためのトランザクションデータを生成する。たとえば、知的財産に関するデータを記録する要求情報を情報取得部1101から取得した場合、トランザクションデータ生成部1103は、管理サーバ200から当該知的財産に関するデータ（対象データ）を読み出して、ハッシュ関数を用いて対象データをハッシュ化する。そして、トランザクションデータ生成部1103は、ハッシュ化された対象データをDAGデータ152に含めるためのトランザクションデータを生成する。また、たとえば、タイムスタンプトークンを情報取得部1101から取得した場合、トランザクションデータ生成部1103は、ハッシュ関数を用いてタイムスタンプトークン（対象データ）をハッシュ化して、ハッシュ化されたタイムスタンプトークンをDAGデータ152に含めるためのトランザクションデータを生成する。

【0057】

また、トランザクションデータ生成部1103は、電子署名部1105から電子署名を受ける。トランザクションデータ生成部1103は、電子署名をトランザクションデータに含める。

【0058】

電子署名部1105は、第1～第4秘密鍵を記憶装置150から読み出す。電子署名部1105は、第1秘密鍵を用いて、第1電子署名を生成する。たとえば、電子署名部1105は、トランザクションデータ生成部1103からハッシュ化された対象データを取得し、第1秘密鍵を用いて、当該ハッシュ化された対象データを暗号化することで第1電子署名を生成する。電子署名部1105は、生成された第1電子署名をトランザクションデータ生成部1103に出力する。また、電子署名部1105は、上述した第1電子署名の生成手順と同様の手順で、第2～第4秘密鍵を用いて、第2～第4電子署名をそれぞれ生成する。そして、電子署名部1105は、第2～第4電子署名をトランザクションデータ生成部1103に出力する。

【0059】

トランザクションデータ生成部1103は、4つの電子署名（第1電子署名、第2電子署名、第3電子署名、第4電子署名）をトランザクションデータに含める。そして、トランザクションデータ生成部1103は、当該トランザクションデータをトランザクションデータ送信部1107へ出力する。なお、トランザクションデータが、電子署名を1つしか含めることができないデータ構造である場合には、たとえば、任意のデータを含むことができるトランザクションデータのデータ領域に残りの3つの電子署名を含めるようにしてもよい。

【0060】

トランザクションデータ送信部1107は、トランザクションデータをネットワークNWへ送信するための制御信号を通信装置140に出力する。これにより、通信装置140を介して、トランザクションデータがネットワークNWに送信される。

【0061】

ある国の認証局で発行された電子証明書が、認証局が準拠する規格の違い等に起因して、他国においては、その有効性が認められないというケースが起こり得る。本実施の形態においては、トランザクションデータに複数の電子署名（第1電子署名、第2電子署名、第3電子署名、第4電子署名）が含まれる。それゆえに、複数の国や地域において、トランザクションデータに付された電子署名の有効性を担保することが可能となる。

【0062】

＜存在証明の申請（タイムスタンプトークンの取得）＞

特許等の知的財産に関するデータにおいては、たとえば、先使用权等の観点から、そのデータが記録された時刻が重要になる場合がある。本実施の形態に係るデータ管理装置100は、管理サーバ200にデータ（対象データ）を保存するとともに、時刻認証局から当該対象データに対するタイムスタンプトークンを取得してDAGデータ152に含める。これにより、対象データの存在証明が可能となる。さらに、時刻認証局が準拠する規格の違い等に起因して、ある国の時刻認証局のタイムスタンプトークンが、他の国においては公式に認められないことがあることから、本実施の形態に係るデータ管理装置100は、複数の時刻認証局から対象データに対するタイムスタンプトークンを取得してDAGデータ152に含める。これにより、複数の国や地域において、対象データの存在証明が可能となる。

10

【0063】

図4は、存在証明の申請（タイムスタンプトークンの取得）の概要を説明するための図である。図4を参照して、データ管理装置100は、知的財産に関するデータ（図4では発明元データ）を管理サーバ200に保存すると、当該知的財産に関するデータをハッシュ化して、ハッシュ値を含めたトランザクションデータをネットワークNWへ送信し、DAGデータ152に含める。たとえば、ある発明に関する、複数の知的財産に関するデータが管理サーバ200およびDAGデータ152に溜まった時点で、存在証明の申請が行なわれる。図4においては、トランザクションデータ153（c）がDAGデータ152に追加された時点で存在証明の申請が行なわれている。存在証明の申請が行なわれると、ある発明に関するトランザクションデータ（図4では、トランザクションデータ153（a）～（c））を纏めてハッシュ化した発明ハッシュが生成されて、発明ハッシュが時刻認証局群400に送信される。そして、各時刻認証局は、発明ハッシュに国際標準時に追跡性がある時刻源に基づく時刻情報を結合させたタイムスタンプトークンを生成する。このタイムスタンプトークンにより、その時刻にDAGデータ152に含まれているデータが存在していることを証明することができる。なお、図4では、ある発明に関するトランザクションデータが連続してDAGデータ152（コンソーシアム分散型台帳）に記憶されている例を示しているが、ある発明に関するトランザクションデータがDAGデータ152に連続して記憶されるとは限らない。ある発明に関するトランザクションデータが連続せずにDAGデータ152に記憶される場合もある。このような場合には、たとえば、トランザクションデータに含まれる発明IDにより、ある発明に関するトランザクションデータを特定し、これらを纏めてハッシュ化して発明ハッシュを生成すればよい。なお、「発明ハッシュ」は、本開示に係る「ハッシュデータ」の一例に相当する。

20

30

【0064】

図5は、DAGデータ152の作成から存在証明の申請（タイムスタンプトークンの取得）までの流れを説明するためのシーケンス図である。本実施の形態においては、図5に示す（1）から（6）の順に、存在証明の申請の処理が進められる。なお、（0）に示す電子証明書を発行する処理は、たとえば、データ管理装置100のネットワークNWへの参加時等に行なわれ、認証局（第1認証局310～第4認証局340）に対する申請により電子証明書が発行される。

40

【0065】

図5を参照して、（1）データ管理装置100のユーザが、入力装置160を介して、発明IDの発行のための操作を行なう。発明IDは、知的財産に関するデータを管理するためのIDであり、本実施の形態においては、1つの発明に対して、1つの発明IDが割り当てられる。この発明IDに、当該発明に関連する複数の知的財産に関するデータ（図5ではドキュメントファイル）が紐づけられることにより、発明が管理される。発明IDの発行のための操作が行なわれると、データ管理装置100の制御装置110は、発明IDを発行して、たとえば記憶装置150に記憶するとともに、このトランザクションを発生させるためのトランザクションデータを生成してネットワークNWに送信する。これに

50

より、DAGデータ152に、発明IDが格納される。ここでは、発明ID「A001」が発行されたものとする。なお、発明IDは、本開示に係る「ID情報」の一例に相当する。

【0066】

次いで、(2)データ管理装置100のユーザが、入力装置160を介して、ドキュメントファイル(知的財産に関するデータ)を登録するための操作を行なう。このドキュメントファイルが、発明ID「A001」に紐づけて登録されるように、ユーザは操作を行なう。当該操作により、制御装置110は、発明ID「A001」に紐づけて、Web(管理サーバ200)にドキュメントファイルを記憶する。図5に示す例では、発明ID「A001」に紐づいて、2つのドキュメントファイル「000001」,「000002」が管理サーバ200に記憶される。なお、発明IDに紐づけられたデータ(たとえばドキュメントファイル)を総称して、「発明情報」とも称する。

10

【0067】

そして、(3)制御装置110は、ドキュメントファイルをハッシュ化し、そのハッシュ値をDAGデータ152に登録するためのトランザクションデータを生成して、通信装置140を介して、トランザクションデータをネットワークNWに送信する。具体的には、ドキュメントファイル「000001」が管理サーバ200に記憶されると、制御装置110は、ドキュメントファイル「000001」のハッシュ値を含むトランザクションデータを生成して、通信装置140を介して、当該トランザクションデータをネットワークNWに送信する。これにより、DAGデータ152に、ドキュメントファイル「000001」のハッシュ値を含むトランザクションデータが記憶される。また、ドキュメントファイル「000002」が管理サーバ200に記憶されると、制御装置110は、ドキュメントファイル「000002」のハッシュ値を含むトランザクションデータを生成して、通信装置140を介して、当該トランザクションデータをネットワークNWに送信する。これにより、DAGデータ152に、ドキュメントファイル「000002」のハッシュ値を含むトランザクションデータが記憶される。なお、トランザクションデータが発明ID「A001」の情報を含むことにより、当該トランザクションデータが発明ID「A001」に紐付けられる。

20

【0068】

コンソーシアム分散型台帳の欄には、存在証明の申請(タイムスタンプトークンの取得)をする時点((4)の時点)におけるDAGデータ152のステートが概略的に示されている。図5においては、発明ID「A001」に2つのトランザクションデータ(ドキュメントファイル「000001」,「000002」のハッシュ値をそれぞれ含む)が紐づいている状態が示されている。

30

【0069】

(4)データ管理装置100のユーザが、入力装置160を介して、存在証明の申請(タイムスタンプトークンの取得)をするための操作を行なう。存在証明の申請(タイムスタンプトークンの取得)をするための操作が行なわれると、制御装置110は、ハッシュ関数を用いて、発明ID「A001」に紐づいているトランザクションデータ(ドキュメントファイル「000001」のハッシュ値を含むトランザクションデータ,ドキュメントファイル「000002」のハッシュ値を含むトランザクションデータ)を纏めてハッシュ化する。このときに得られる数値(ハッシュ値)が「発明ハッシュ」である。

40

【0070】

存在証明の申請をするための操作は、ユーザの任意のタイミングで行なうことが可能である。

【0071】

(5)制御装置110は、発明ハッシュを時刻認証局群400に送信する。このとき、制御装置110は、通信装置140を介して、時刻認証局群400のうち、後述するインターフェース画面において選択された時刻認証局に発明ハッシュを送信する。

【0072】

50

(6) 発明ハッシュを受信した時刻認証局は、発明ハッシュに国際標準時に追跡性がある時刻源に基づく時刻情報を結合させたタイムスタンプトークン(TST)をデータ管理装置100に返信する。時刻認証局からタイムスタンプトークンを受信すると、制御装置110は、タイムスタンプトークンをDAGデータ152に登録するためのトランザクションデータを生成し、通信装置140を介して、トランザクションデータをネットワークNWに送信する。これにより、タイムスタンプトークンがDAGデータ152に登録される。このようにして、存在証明(タイムスタンプトークン)が取得される。

【0073】

制御装置110は、発明ハッシュおよびタイムスタンプトークンを、たとえば記憶装置150に記憶しておく。また、制御装置110は、第1～第4電子証明書を付帯させた発明証明書をネットワークNWに送信する。発明証明書には、発明ID、当該発明IDに紐づけられたトランザクションデータ、第1～第4電子署名およびタイムスタンプトークンが含まれる。発明証明書は、後述の存在の検証および電子署名の有効性の検証で用いられる。なお、発明証明書に付帯される電子証明書は、存在証明の申請を行なった(タイムスタンプトークンを取得した)時刻認証局に対応した電子証明書のみであってもよい。

【0074】

図6は、存在証明の申請(タイムスタンプトークンの取得)をするためのインターフェース画面を説明するための図である。図6に示されるインターフェース画面は、表示装置170のディスプレイに表示される。

【0075】

インターフェース画面は、選択領域171と、第1表示領域172と、第2表示領域173と、第3表示領域174とを含む。

【0076】

選択領域171には、「発明情報管理」と「存在証明検証」とのタブが選択可能に表示されている。たとえば、マウス等の入力装置160により「発明情報管理」と「存在証明検証」とのいずれかのタブを選択することで、インターフェース画面の表示内容を切り替えることができる。図6は、「発明情報管理」が選択されている場合のインターフェース画面である。「存在証明検証」が選択された場合には、後述の図10に示されるインターフェース画面が、表示装置170のディスプレイに表示される。

【0077】

第1表示領域172には、登録されている発明プロジェクトが表示される。発明プロジェクトは、複数の発明IDを含む。図6に示す例においては、A001からA004の4つの発明IDが登録されている。「発明プロジェクトを追加」の表示を選択することにより、発明プロジェクト、すなわち新たな発明IDを発行して追加することができる。図6においては、発明ID「A001」が選択されている。

【0078】

第2表示領域173には、選択されている発明IDのバージョン情報が表示される。バージョン情報は、たとえば、ドキュメントファイルが新たに記憶されたり、発明ID「A001」に関する何らかの更新があった場合に追加される。

【0079】

第3表示領域174には、発明のタイトルの表示欄、発明IDの表示欄、発明の説明の表示欄、ドキュメントの表示欄、および、存在証明の表示欄が含まれる。発明のタイトルの表示欄には、その発明のタイトルが表示される。発明IDの表示欄には、発明のIDが表示される。図6に示す例においては、発明ID「A001」が表示されている。発明の説明の表示欄には、その発明に関する説明が表示される。

【0080】

ドキュメントの表示欄には、発明IDに紐づけて記憶されているドキュメントファイルが表示される。図6に示す例においては、発明ID「A001」に紐づけられているドキュメントファイル「000001」、「000002」が表示されている。「ファイルを追加」のボタン(表示)を選択することにより、新たなドキュメントを発明ID「A00

10

20

30

40

50

1」に紐づけて保存することができる。

【0081】

存在証明の表示欄には、発明ID「A001」に関して存在証明（タイムスタンプトークン）を発行した国および／または地域の情報と、そのタイムスタンプトークンに含まれる時刻の情報と、時刻認証局の情報（トラストサービス名）とが含まれる。図6においては、中国（第2時刻認証局420）、EU（第4時刻認証局440）および日本（第1時刻認証局410）で存在証明を発行していることが示されている。以下に説明するように、存在証明の発行を行なうと、その結果が存在証明の表示欄に表示される。

【0082】

存在証明の表示欄には、さらに、「存在証明の発行」のボタン（表示）が含まれる。「存在証明の発行」のボタンを選択することにより、発明ID「A001」についての存在証明を発行（申請）することができる。「存在証明」のボタンを選択することにより、制御装置110が、その時点における発明ハッシュを生成する。

【0083】

図7は、図6の「存在証明の発行」のボタンを選択した場合に表示されるインターフェース画面を説明するための図である。図7に示されるように、「存在証明の発行」のボタンを選択すると、存在証明を発行する国および／または地域を選択するためのポップアップ画面179が表示される。すなわち、存在証明を発行する時刻認証局を選択するためのポップアップ画面179が表示される。図7に示す例においては、第1時刻認証局410（日本）、第2時刻認証局420（中国）、および、第4時刻認証局440（EU）が選択されている。上記を選択した状態で、図7に示されている「存在証明の発行」のボタン（表示）を選択することにより、選択された時刻認証局に発明ハッシュが送信される。これにより、選択した時刻認証局からタイムスタンプトークンを取得することができる。選択した時刻認証局から取得したタイムスタンプトークンの情報が、図6の存在証明の表示欄に表示される。

【0084】

図8は、存在証明の申請（タイムスタンプトークンの取得）を説明するための制御装置110の機能ブロック図である。図8を参照して、制御装置110は、入力取得部1111と、表示制御部1113と、選択判定部1115と、発明ハッシュ生成部1117と、送信部1119と、受信部1121とを含む。制御装置110は、たとえば、ROM120に記憶されたプログラムを実行することにより、入力取得部1111、表示制御部1113、選択判定部1115、発明ハッシュ生成部1117、送信部1119、および、受信部1121として機能する。なお、入力取得部1111、表示制御部1113、選択判定部1115、発明ハッシュ生成部1117、送信部1119、および、受信部1121は、たとえば、専用のハードウェア（電子回路）により実現されてもよい。

【0085】

入力取得部1111は、入力装置160を介して、存在証明を申請（発行）するための操作が行なわれたことを検知する。具体的には、入力取得部1111は、入力装置160から、表示装置170のインターフェース画面（図6）に表示された「存在証明の発行」のボタンが選択されたことを示す情報を取得する。入力取得部1111は、当該情報を取得すると、ポップアップ表示を指示する制御信号を表示制御部1113に出力するとともに、発明ハッシュの生成を指示する制御信号を発明ハッシュ生成部1117に出力する。

【0086】

表示制御部1113は、入力取得部1111からポップアップ表示を指示する制御信号を取得すると、存在証明を発行する時刻認証局を選択するためのポップアップ画面（図7）を表示装置170に表示させる。

【0087】

選択判定部1115は、ポップアップ画面において選択された時刻認証局を判定する。ポップアップ画面に表示された「存在証明の発行」のボタンが選択されると、選択判定部1115は、選択された時刻認証局を特定するための情報である送信情報を送信部111

9に出力する。

【0088】

発明ハッシュ生成部1117は、入力取得部1111から発明ハッシュの生成を指示する制御信号を取得すると、選択されている発明IDに紐づけられているトランザクションデータを纏めてハッシュ化し、発明ハッシュを生成する。発明ハッシュ生成部1117は、生成された発明ハッシュを送信部1119に出力する。

【0089】

送信部1119は、選択判定部1115から受けた送信情報により特定される時刻認証局に発明ハッシュを送信するための制御信号を、通信装置140に出力する。これにより、通信装置140を介して、選択された時刻認証局に発明ハッシュが送信される。

10

【0090】

発明ハッシュを受信した時刻認証局の各々は、データ管理装置100へタイムスタンプトークンを返信する。

【0091】

受信部1121は、通信装置140を介して、発明ハッシュを送信した時刻認証局からタイムスタンプトークンを受信する。これにより、存在証明の申請の対象となる発明IDの発明情報の存在証明を取得することができる。

【0092】

<存在証明の検証>

図9は、存在証明の検証の流れを説明するためのシーケンス図である。本実施の形態においては、図9に示す(1)から(5)の順に、存在証明の検証の処理が進められる。

20

【0093】

まず、(1)データ管理装置100のユーザが、入力装置160を介して、任意の発明(発明ID)を選択し、その存在証明を検証するための操作を行なう。

【0094】

図10は、存在証明の検証をするためのインターフェース画面を説明するための図である。図10に示されるインターフェース画面は、表示装置170のディスプレイに表示される。インターフェース画面は、選択領域171と、第4表示領域175と、第5表示領域176と、第6表示領域177とを含む。選択領域171は、図6で説明した存在証明の申請をするためのインターフェース画面と共通である。選択領域171に表示される「発明情報管理」のタブを選択することで図6のインターフェース画面を表示させることができ、「存在証明検証」のタブを選択することで図10のインターフェース画面を表示させることができる。

30

【0095】

第4表示領域175には、存在証明の検証を行なう発明を検索するための入力領域が表示されている。たとえば、入力領域に発明ID「A001」を入力することで、発明ID「A001」の情報を第5表示領域176に表示させることができる。図10には、発明ID「A001」が検索された表示画面が示されている。

【0096】

第5表示領域176には、検索された発明ID(「A001」)の情報が表示される。第6表示領域177には、「存在証明の検証」のボタン(表示)が含まれる。「存在証明の検証」のボタンを選択することにより、第5表示領域176に表示されている発明IDの発明情報の存在証明の検証が開始される。

40

【0097】

再び図9を参照して、(2)データ管理装置100の制御装置110は、選択された発明IDに紐づけられたトランザクションデータを纏めてハッシュ化して発明ハッシュを生成する。

【0098】

(3)制御装置110は、記憶装置150からタイムスタンプトークンを読み出す。そして、制御装置110は、タイムスタンプトークンに含まれている発明ハッシュを読み出

50

す。

【0099】

(4) 制御装置110は、生成した発明ハッシュと、タイムスタンプトークンに含まれている発明ハッシュとを比較し、両者が一致することを確認する。両者が一致することが確認されることにより、タイムスタンプトークンが発行されてから現在までの間に、発明ID(図9に示す例では「A001」)の発明情報が改ざんされていないことを証明することができる。

【0100】

(5) 制御装置110は、存在証明の検証の結果を、たとえば表示装置170のディスプレイに表示させる。

【0101】

図11は、存在証明の検証を説明するための制御装置110の機能ブロック図である。図11を参照して、制御装置110は、入力取得部1131と、発明ハッシュ生成部1133と、読み出し部1135と、比較部1137と、出力部1139とを含む。制御装置110は、たとえば、ROM120に記憶されたプログラムを実行することにより、入力取得部1131、発明ハッシュ生成部1133、読み出し部1135、比較部1137、および、出力部1139として機能する。なお、入力取得部1131、発明ハッシュ生成部1133、読み出し部1135、比較部1137、および、出力部1139は、たとえば、専用のハードウェア(電子回路)により実現されてもよい。

【0102】

入力取得部1131は、入力装置160を介して、存在証明を検証するための操作が行われたことを検知する。具体的には、入力取得部1131は、入力装置160から、表示装置170に表示された「存在証明の検証」のボタンが選択されたことを示す情報を取得する。入力取得部1131は、当該情報を取得すると、発明ハッシュの生成を指示する制御信号を発明ハッシュ生成部1133に出力するとともに、タイムスタンプトークンの読み出しを指示する制御信号を読み出し部1135に出力する。

【0103】

発明ハッシュ生成部1133は、入力取得部1131から発明ハッシュの生成を指示する制御信号を取得すると、選択されている発明IDに紐づけられているトランザクションデータを纏めてハッシュ化し、発明ハッシュを生成する。発明ハッシュ生成部1133は、生成された発明ハッシュを比較部1137に出力する。

【0104】

読み出し部1135は、入力取得部1131からタイムスタンプトークンの読み出しを指示する制御信号を取得すると、記憶装置150に記憶された、選択されている発明IDのタイムスタンプトークンを読み出す。読み出し部1135は、読み出されたタイムスタンプトークンから発明ハッシュを読み出し、読み出された発明ハッシュを比較部1137に出力する。

【0105】

比較部1137は、発明ハッシュ生成部1133から受けた発明ハッシュと、読み出し部1135から受けた発明ハッシュとを比較する。両者が一致した場合には、比較部1137は、タイムスタンプトークンが発行されてから現在までの間に、発明IDの発明情報が改ざんされていないと判定する。両者が一致しない場合には、比較部1137は、タイムスタンプトークンが発行されてから現在までの間に、発明IDの発明情報が改ざんされたと判定する。比較部1137は、比較結果を出力部1139に出力する。

【0106】

出力部1139は、比較結果を、たとえば、表示装置170に出力する。これにより、選択されている発明IDの存在証明の検証結果が表示装置170に表示される。

【0107】

<電子署名の有効性の検証>

再び図9を参照して、(1)の処理、すなわち、発明IDを選択して、その存在証明を

10

20

30

40

50

検証するための操作が行なわれると、データ管理装置 100 の制御装置 110 は、上述の存在証明の検証と並列に、あるいは、存在証明の検証の前後に、電子署名の有効性の検証を行なう。

【0108】

まず、制御装置 110 は、発明 ID（図 9 に示す例では「A001」）に紐づけられたトランザクションデータの電子署名（第 1～第 4 電子署名）を、発明証明書に付帯されている第 1～第 4 電子証明書に含まれる第 1～第 4 公開鍵を用いてそれぞれ復号する。上述のとおり、発明証明書には、発明 ID、当該発明 ID に紐づけられたトランザクションデータ、第 1～第 4 電子署名およびタイムスタンプトークンが含まれているため、制御装置 110 は、たとえば、選択された発明 ID と発明証明書に含まれる発明 ID とを照合させることにより、用いるべき発明証明書を特定することができる。

10

【0109】

制御装置 110 は、第 1～第 4 電子署名を第 1～第 4 公開鍵を用いて、それぞれ復号する。制御装置 110 は、電子署名毎に、復号した値を発明 ID に紐づけられたトランザクションデータに含まれる対象データ（ドキュメント）のハッシュ値と比較し、両者が一致することを確認する。両者が一致することが確認されることにより、電子署名の有効性が認められる。

【0110】

なお、制御装置 110 は、存在証明の検証の対象となる国または地域に対応する電子署名の有効性を検証し、存在証明の検証の対象とならない国または地域に対応する電子署名の有効性を検証しないようにしてもよい。存在証明の検証の対象となる国または地域とは、存在証明の申請において選択された（図 7 で選択された）国または地域である。たとえば、選択された発明 ID の存在証明の検証の対象となる国または地域が日本、中国および EU である場合、つまり、第 1 時刻認証局 410、第 2 時刻認証局 420 および第 4 時刻認証局 440 でタイムスタンプトークンが取得されている場合には、制御装置 110 は、第 1 電子署名、第 2 電子署名および第 4 電子署名の有効性を検証し、第 3 電子署名の有効性の検証を省略してもよい。これにより、存在証明の検証の対象となる国または地域に対応する電子署名の有効性に加えて、存在証明の検証の対象とならない国または地域に対応する電子署名の有効性も検証する場合に比べて、処理負荷を低減させることができる。

20

【0111】

図 12 は、電子署名の有効性の検証を説明するための制御装置 110 の機能ブロック図である。図 12 を参照して、制御装置 110 は、入力取得部 1141 と、読み出し部 1143 と、選択部 1145 と、復号部 1147 と、判定部 1149 と、出力部 1151 とを含む。制御装置 110 は、たとえば、ROM 120 に記憶されたプログラムを実行することにより、入力取得部 1141、読み出し部 1143、選択部 1145、復号部 1147、判定部 1149、および、出力部 1151 として機能する。なお、入力取得部 1141、読み出し部 1143、選択部 1145、復号部 1147、判定部 1149、および、出力部 1151 は、たとえば、専用のハードウェア（電子回路）により実現されてもよい。

30

【0112】

入力取得部 1141 は、入力装置 160 を介して、存在証明を検証するための操作が行なわれたことを検知する。具体的には、入力取得部 1141 は、入力装置 160 から、表示装置 170 に表示された「存在証明の検証」のボタンが選択されたことを示す情報を取得する。入力取得部 1141 は、当該情報を取得すると、対象となる発明 ID を特定し、特定された発明 ID、および、当該発明 ID に紐づけられたトランザクションデータの読み出しを指示する制御信号を読み出し部 1143 に出力する。

40

【0113】

読み出し部 1143 は、入力取得部 1141 から、発明 ID および当該発明 ID に紐づけられたトランザクションデータの読み出しを指示する制御信号を取得すると、発明 ID に紐づけられたトランザクションデータを記憶装置 150 から読み出す。さらに、読み出し部 1143 は、発明 ID に対応する発明証明書を記憶装置 150 から読み出す。読み出

50

し部 1 1 4 3 は、読み出された発明証明書を選択部 1 1 4 5 に出力するとともに、読み出されたトランザクションデータおよび発明証明書を復号部 1 1 4 7 に出力する。

【 0 1 1 4 】

選択部 1 1 4 5 は、有効性を検証する電子署名を選択する。選択部 1 1 4 5 は、たとえば、発明証明書に含まれるタイムスタンプトークンから、存在証明の検証の対象となる国または地域を特定する。そして、選択部 1 1 4 5 は、特定した国または地域に対応する電子署名を選択する。具体的には、たとえば、発明証明書に、第 1 時刻認証局 4 1 0、第 2 時刻認証局 4 2 0 および第 4 時刻認証局 4 4 0 が発行したタイムスタンプトークンが含まれている場合には、選択部 1 1 4 5 は、第 1 時刻認証局 4 1 0、第 2 時刻認証局 4 2 0 および第 4 時刻認証局 4 4 0 がそれぞれ対応する国または地域の認証局である、第 1 認証局 3 1 0、第 2 認証局 3 2 0、および第 4 認証局 3 4 0 に対応する第 1 電子署名、第 2 電子署名および第 4 電子署名を、有効性を検証する電子署名として選択する。選択部 1 1 4 5 は、選択された電子署名、すなわち、復号の対象となる電子署名を示す信号を復号部 1 1 4 7 に出力する。

10

【 0 1 1 5 】

復号部 1 1 4 7 は、発明証明書に付帯された電子証明書を用いて、復号の対象となる電子署名を復号する。具体的には、復号部 1 1 4 7 は、入力取得部 1 1 4 1 から受けたトランザクションデータに付された電子署名のうち、復号の対象となる電子署名（ここでは、第 1 電子署名、第 2 電子署名および第 4 電子署名）を、第 1 電子証明書（第 1 公開鍵）、第 2 電子証明書（第 2 公開鍵）および第 4 電子証明書（第 4 公開鍵）でそれぞれ復号する。復号部 1 1 4 7 は、復号された値（復号値）の各々を判定部 1 1 4 9 に出力する。また、復号部 1 1 4 7 は、読み出し部 1 1 4 3 から受けたトランザクションデータを判定部 1 1 4 9 に出力する。なお、トランザクションデータは、読み出し部 1 1 4 3 から判定部 1 1 4 9 に送られる構成であってもよい。

20

【 0 1 1 6 】

判定部 1 1 4 9 は、復号部 1 1 4 7 から受けた復号値の各々を、復号値毎に、トランザクションデータに含まれるドキュメントファイルのハッシュ値と比較する。両者が一致した場合には、判定部 1 1 4 9 は、電子署名が有効なものであると判定する。両者が一致しない場合には、判定部 1 1 4 9 は、電子署名が有効なものでないと判定する。判定部 1 1 4 9 は、判定結果を出力部 1 1 5 1 に出力する。

30

【 0 1 1 7 】

出力部 1 1 5 1 は、判定結果を、たとえば、表示装置 1 7 0 に出力する。これにより、電子署名の有効性の検証結果が表示装置 1 7 0 に表示される。

【 0 1 1 8 】

<制御装置で実行される処理>

<<トランザクションデータの生成>>

図 1 3 は、トランザクションデータを生成する処理の手順を示すフローチャートである。図 1 3 に示すフローチャートの処理は、入力装置 1 6 0 を介した入力操作が行なわれる毎に、あるいは、時刻認証局群 4 0 0 からタイムスタンプトークンを取得する毎に制御装置 1 1 0 によって実行される。入力操作は、たとえば、知的財産に関するデータを新たに保存する操作である。なお、図 1 3 および後述する図 1 4、1 5、1 6 に示すフローチャートの各ステップ（以下ステップを「S」と略す）は、制御装置 1 1 0 によるソフトウェア処理によって実現される場合について説明するが、その一部あるいは全部が制御装置 1 1 0 内に作製されたハードウェア（電子回路）によって実現されてもよい。

40

【 0 1 1 9 】

S 1 において、制御装置 1 1 0 は、対象データをハッシュ化する。具体的には、知的財産に関するデータを記録する場合には、制御装置 1 1 0 は、管理サーバ 2 0 0 から当該知的財産に関するデータ（対象データ）を読み出して、ハッシュ関数を用いて対象データをハッシュ化する。あるいは、タイムスタンプトークンを記録する場合には、制御装置 1 1 0 は、ハッシュ関数を用いてタイムスタンプトークン（対象データ）をハッシュ化する。

50

【0120】

S3において、制御装置110は、第1～第4秘密鍵を記憶装置150から読み出す。そして、制御装置110は、第1～第4秘密鍵を用いて、ハッシュ化された対象データを暗号化して、第1～第4電子署名をそれぞれ生成する。

【0121】

S5において、制御装置110は、対象データのハッシュ値と、4つの電子署名（第1電子署名、第2電子署名、第3電子署名、第4電子署名）とを含めて、トランザクションデータを生成する。なお、制御装置110は、上記の他に、発明IDの情報、トランザクションデータをネットワークNWへ向けてブロードキャストする時刻情報（トランザクションデータが対応する処理の発生時刻を示す時刻情報であってもよい）、および、トランザクションデータの送信者情報をトランザクションデータに含める。さらに、制御装置110は、過去に発生した2つのトランザクションのトランザクションデータを承認し、これらのトランザクションデータのハッシュ値をトランザクションデータに含める。

10

【0122】

なお、S5において、制御装置110は、対象データのハッシュ値と第1電子署名とを含めたトランザクションデータ、対象データのハッシュ値と第2電子署名とを含めたトランザクションデータ、対象データのハッシュ値と第3電子署名とを含めたトランザクションデータ、対象データのハッシュ値と第4電子署名とを含めたトランザクションデータの4つのトランザクションデータを生成してもよい。なお、この4つのトランザクションデータにも、発明IDの情報、トランザクションデータをネットワークNWへ向けてブロードキャストする時刻情報、トランザクションデータの送信者情報、および、過去に発生した2つのトランザクションのトランザクションデータのハッシュ値が含まれる。

20

【0123】

S7において、制御装置110は、生成されたトランザクションデータをネットワークNWへ送信するための制御信号を通信装置140に出力する。これにより、通信装置140を介して、トランザクションデータがネットワークNWに送信される。

【0124】

<<存在証明の申請>>

図14は、発明情報の存在証明の申請をする処理の手順を示すフローチャートである。図14に示すフローチャートの処理は、入力装置160を介して、存在証明を申請するための操作が行なわれる毎に、制御装置110によって実行される。本実施の形態においては、存在証明の申請は、発明ID単位に行なわれる。

30

【0125】

S11において、制御装置110は、存在証明を発行する時刻認証局を選択するためのポップアップ画面を表示装置170に表示させる。

【0126】

S13において、制御装置110は、ポップアップ画面において選択された時刻認証局を判定する。

【0127】

S15において、制御装置110は、存在証明の申請の対象である発明IDに紐づけられているトランザクションデータを纏めてハッシュ化し、発明ハッシュを生成する。なお、S15の処理は、S11の処理より前に行なわれてもよい。

40

【0128】

S17において、制御装置110は、選択された時刻認証局に発明ハッシュを送信するための制御信号を、通信装置140に出力する。これにより、通信装置140を介して、選択された時刻認証局に発明ハッシュが送信される。

【0129】

S19において、制御装置110は、通信装置140を介して、発明ハッシュを送信した時刻認証局からタイムスタンプトークンを受信する。これにより、存在証明の申請の対象である発明IDの発明情報の存在証明が取得される。

50

【0130】

<<存在証明の検証>>

図15は、存在証明を検証する処理の手順を示すフローチャートである。図15に示すフローチャートの処理は、入力装置160を介して、存在証明を検証するための操作が行なわれる毎に、制御装置110によって実行される。

【0131】

S21において、制御装置110は、存在証明を検証するための操作において選択された発明IDに紐づけられているトランザクションデータを纏めてハッシュ化し、発明ハッシュを生成する。

【0132】

S23において、制御装置110は、存在証明を検証するための操作において選択された発明IDのタイムスタンプトークンを記憶装置150から読み出す。そして、制御装置110は、読み出されたタイムスタンプトークンから発明ハッシュを読み出す。

【0133】

S25において、制御装置110は、S21において生成された発明ハッシュと、S23において読み出された発明ハッシュとを比較する。

【0134】

S27において、制御装置110は、S25における比較結果を、たとえば、表示装置170のディスプレイに表示させる。これにより、選択されている発明IDに関する存在証明の検証結果が表示装置170に表示される。

【0135】

<<電子署名の有効性の検証>>

図16は、電子署名の有効性を検証する処理の手順を示すフローチャートである。図16に示すフローチャートの処理は、入力装置160を介して、存在証明を検証するための操作が行なわれる毎に、制御装置110によって実行される。このフローチャートの処理は、図15のフローチャートの処理と並列に実行されてもよいし、図15のフローチャートの処理の実行前後で実行されてもよい。

【0136】

S31において、制御装置110は、存在証明を検証するための操作において選択された発明IDに紐づけられているトランザクションデータを記憶装置150から読み出す。また、制御装置110は、存在証明を検証するための操作において選択された発明IDの発明証明書を記憶装置150から読み出す。

【0137】

S33において、制御装置110は、有効性を検証する電子署名を選択する。制御装置110は、発明証明書に含まれるタイムスタンプトークンから、存在証明の検証の対象となる国または地域を特定する。

【0138】

S35において、制御装置110は、発明証明書に付帯された電子証明書を用いて、復号の対象となる電子署名を復号する。具体的には、制御装置110は、1つのトランザクションデータに含められた第1～第4電子署名のうち、有効性を検証する対象である電子署名（たとえば、第1電子署名、第2電子署名および第4電子署名）に対して、対応する電子証明書（たとえば、第1電子証明書、第2電子証明書および第4電子証明書）を用いた復号を行なう。S35の処理は、発明IDに紐づけられた全てのトランザクションデータに対して実行される。

【0139】

S37において、制御装置110は、復号を行なった値（復号値）毎に、復号値を、トランザクションデータに含まれるドキュメントファイルのハッシュ値と比較する。制御装置110は、両者が一致した場合には、当該電子署名が有効なものであると判定する。制御装置110は、両者が一致しない場合には、当該電子署名が有効なものでないと判定する。

10

20

30

40

50

【0140】

S39において、制御装置110は、S37における判定結果を、たとえば、表示装置170のディスプレイに表示させる。これにより、電子署名の有効性の検証結果が表示装置170に表示される。

【0141】

以上のように、本実施の形態に係るデータ管理システム1において、データ管理装置100は、発明情報を記録するにあたり、発明情報の発明ハッシュを時刻認証局群400に送信する。時刻認証局群400には、複数の時刻認証局（実施の形態においては第1～第4時刻認証局410～440）が含まれる。データ管理装置100は、複数の時刻認証局からタイムスタンプトークンを取得する。これにより、複数の国および地域において、上記発明情報を記録した時刻の正確性を保証することができる。

10

【0142】

また、本実施の形態に係るデータ管理システム1において、データ管理装置100は、時刻認証局群400の中から、タイムスタンプトークンを取得する時刻認証局を選択することができる。発明によっては、タイムスタンプトークンの取得が不要となる国または地域が存在し得る。タイムスタンプトークンを取得する時刻認証局を選択することにより、タイムスタンプトークンを取得する必要がない時刻認証局からはタイムスタンプトークンを取得しないようにすることができるので、データ管理システム1の処理負荷を低減させることができる。

20

【0143】

また、本実施の形態に係るデータ管理システム1において、データ管理装置100は、認証局群300に含まれる認証局の各々から、電子証明書を取得する。具体的には、データ管理装置100は、第1認証局310から第1電子証明書を、第2認証局320から第2電子証明書を、第3認証局330から第3電子証明書を、第4認証局340から第4電子証明書をそれぞれ取得する。データ管理装置100は、第1～第4電子証明書を発明証明書に付帯させてネットワークNWに送信する。データ管理装置100は、第1～第4秘密鍵を用いて第1～第4電子署名をそれぞれ生成し、これら4つの電子署名をトランザクションデータに含める。電子署名の有効性は、規格の違いに起因して、国または地域によって異なり得るが、トランザクションデータに第1～第4電子署名の4つの電子署名を含めておくことにより、複数の国および／または地域で電子署名の有効性を証明することが可能となる。これにより、ネットワークNWへ送信されるデータの信頼性が高まり、第三者のなりすましやデータの改ざんを抑制することができる。

30

【0144】

また、存在証明の検証の対象となる国または地域に対応する電子署名の有効性を検証し、存在証明の検証の対象とならない国または地域に対応する電子署名の有効性を検証しないようにしてもよい。これにより、存在証明の検証の対象となる国または地域に対応する電子署名の有効性に加えて、存在証明の検証の対象とならない国または地域に対応する電子署名の有効性も検証する場合に比べて、データ管理システム1の処理負荷を低減させることができる。

【0145】

40

[変形例]

実施の形態においては、1つのトランザクションデータに4つの電子署名（第1電子署名、第2電子署名、第3電子署名、第4電子署名）が含まれる例について説明した。しかしながら、電子署名の数に応じて、複数のトランザクションデータが生成されてもよい。すなわち、対象データに対する1つの処理に対して、第1電子署名を含むトランザクションデータ、第2電子署名を含むトランザクションデータ、第3電子署名を含むトランザクションデータ、および、第4電子署名を含むトランザクションデータの4つのトランザクションデータが生成されてもよい。このような構成であっても、対象データに対する1つの処理に対して、上記4つのトランザクションデータが生成されることにより、複数の国および／または地域で電子署名の有効性を証明することが可能となる。

50

【0146】

なお、変形例においては、存在証明の申請（タイムスタンプトークンの取得）の際に、時刻認証局へは当該時刻認証局に対応する認証局の電子署名を含むデータ（たとえば発明ハッシュ）を送信する。具体的には、第1時刻認証局410には、第1認証局310の第1電子署名を含むデータを送信する。第2時刻認証局420には、第2認証局320の第2電子署名を含むデータを送信する。第3時刻認証局430には、第3認証局330の第3電子署名を含むデータを送信する。第4時刻認証局440には、第4認証局340の第4電子署名を含むデータを送信する。これにより、存在証明を申請したデータに付された電子署名の有効性を適切に担保することが可能となる。

【0147】

変形例は、後述の実施の形態2に適用することも可能である。

〔実施の形態2〕

図17は、実施の形態2に係るデータ管理システム2の概略的な構成を示す図である。実施の形態2に係るデータ管理システム2は、複数の企業間でネットワークNW（ブロックチェーンネットワーク）を形成して、特許等の知的財産に関するデータを管理するためのシステムである。データ管理システム2には、ブロックチェーンを用いた分散型台帳技術が適用される。データ管理システム2は、実施の形態1に係るデータ管理システム1と基本的には同様の構成を備える。そのため、実施の形態2では、実施の形態1との相違点であるブロックチェーンに関する点について説明する。なお、実施の形態1に係るデータ管理システム1と同様の構成については、同じ符号を付し、その説明は繰り返さない。

【0148】

データ管理システム2は、4台のデータ管理装置500と、認証局群300と、時刻認証局群400とを備える。4台のデータ管理装置500の各々は、実施の形態1と同様、異なる企業（たとえば、A企業、B企業、C企業およびD企業）に帰属するデータ管理装置である。図17では、A企業のデータ管理装置500をデータ管理装置500と表記し、B企業、C企業およびD企業のデータ管理装置500をデータ管理装置500Aと表記するものとする。以下においては、A企業のデータ管理装置500について代表的に説明するが、データ管理装置500Aも同様の機能を有する。

【0149】

データ管理装置500は、たとえば、デスクトップ型のPC、ノート型のPC、タブレット端末、スマートフォン、または、通信機能を有するその他の情報処理端末である。データ管理装置500は、制御装置510と、ROM120と、RAM130と、通信装置140と、記憶装置550と、入力装置160と、表示装置170とを含む。制御装置510、ROM120、RAM130、通信装置140、記憶装置550、入力装置160、および表示装置170は、バス180に接続されている。また、データ管理装置500には、管理サーバ200が通信可能に接続されている。

【0150】

制御装置510は、たとえば、CPUを含む集積回路によって構成される。制御装置510は、ROM120に格納されている各種プログラムをRAM130に展開して実行する。制御装置510は、複数の規格（たとえば、日本の規格、中国の規格、米国の規格およびEUの規格、等）に準拠して、それぞれの規格に準拠した秘密鍵（たとえば、第1～第4秘密鍵）および公開鍵（たとえば、第1～第4公開鍵）を生成する機能を有する。

【0151】

記憶装置550は、たとえば、ハードディスクまたはフラッシュメモリ等の記憶媒体を含んで構成される。記憶装置550は、ブロックチェーンデータ552を記憶する。なお、ブロックチェーンデータ552が記憶されるのは、記憶装置550に限定されるものではなく、ROM120、RAM130、または、管理サーバ200に記憶されてもよい。また、記憶装置550は、制御装置510により生成された秘密鍵および公開鍵を記憶する。また、記憶装置550は、認証局群300に含まれる複数の認証局の各々から発行された電子証明書を記憶する。なお、秘密鍵、公開鍵および電子証明書が記憶されるのは、

10

20

30

40

50

記憶装置 550 に限定されるものではなく、ROM 120、RAM 130、または、管理サーバ 200 に記憶されてもよい。

【0152】

<ブロックチェーンデータ>

図 18 は、ブロックチェーンデータ 552 を説明するための図である。図 18 に示されるように、ブロックチェーンデータ 552 は、ひと繋ぎの複数のブロック 553 で構成される。ブロック 553 の各々には、知的財産に関するデータ等の種々の情報が含まれている。ブロックチェーンデータ 552 には、データ管理システム 2 の運用が開始されてから現在までの、ネットワーク NW を形成するデータ管理装置 500、500A における知的財産に関するデータ等の記録の履歴が記憶されている。

10

【0153】

ブロックチェーンデータ 552 は、ネットワーク NW を形成する全てのデータ管理装置 500、500A に記憶されている。これにより、仮にブロックチェーンデータ 552 があるユーザによって改ざんされたとしても、他の複数のユーザのブロックチェーンデータ 552 を基準として改ざんが防止される。

【0154】

具体的には、新たな知的財産に関するデータを登録する場合、データ管理装置 500 は、新たに登録する知的財産に関するデータを管理サーバ 200 に記憶させると、この処理を示すトランザクションのデータ（トランザクションデータ）を生成する。データ管理装置 500 は、当該知的財産に関するデータを、ハッシュ関数を用いてハッシュ化し、ハッシュ化の結果として得られる数値（ハッシュ値）を含むトランザクションデータを生成する。データ管理装置 500 は、生成されたトランザクションデータをネットワーク NW に送信する。このトランザクションデータは、新規のブロック 553（ B_{n+1} ）に纏められる。そして、一定の条件が満たされた場合に新規のブロック 553（ B_{n+1} ）がブロックチェーンデータ 552 に追加される。

20

【0155】

なお、トランザクションデータは、ネットワーク NW に流れただけでは有効なものとは認められない。トランザクションデータは、データ管理装置 500、500A の各々に保持されるブロックチェーンデータ 552 に追加されて初めて有効となる。未認証のトランザクションデータは、新規のブロック 553（ B_{n+1} ）に纏められ、たとえば、POW（Proof of Work）と呼ばれるマイニング処理によって新規のブロック 553（ B_{n+1} ）がブロックチェーンデータ 552 に追加される。

30

【0156】

POW は、新規のブロック 553（ B_{n+1} ）の追加を複数のノード（管理装置 500、500A）間で競う仕組みである。POW に参加するノードは、一般的にマイナと呼ばれる。新規のブロック 553（ B_{n+1} ）を最も早く生成したマイナには、報酬が与えられる。このような仕組みを用いた合意形成アルゴリズムによって、ブロックチェーンデータ 552 の耐改ざん性が確保される。

【0157】

<トランザクションデータ>

トランザクションデータには、たとえば、発明 ID の情報、対象データ（知的財産に関するデータ：たとえばドキュメント）のハッシュ値、当該トランザクションデータをネットワーク NW へ向けてブロードキャストする時刻情報、当該トランザクションデータの送信者情報、および、電子署名、等が含まれる。なお、トランザクションデータに含まれる時刻情報は、トランザクションデータが対応する処理（たとえば、対象データを管理サーバ 200 への記録する処理）の発生時刻を示す時刻情報であってもよい。

40

【0158】

トランザクションデータの送信者情報は、たとえば、データ管理装置 500 がネットワーク NW へ送信したトランザクションデータであれば、A 企業を示す情報である。なお、トランザクションデータの送信者情報は、さらに詳細に、ネットワーク NW へトランザク

50

ションデータを送信する操作を実行した部署（A企業の一部門）を示す情報であってもよいし、ネットワークNWへトランザクションデータを送信する操作を実行した個人（A企業の従業員）を示す情報であってもよい。

【0159】

＜存在証明の申請（タイムスタンプトークンの取得）＞

図19は、存在証明の申請（タイムスタンプトークンの取得）の概要を説明するための図である。図19を参照して、データ管理装置500は、知的財産に関するデータ（図19では発明元データ）を管理サーバ200に保存すると、当該知的財産に関するデータをハッシュ化して、ハッシュ値を含めたトランザクションデータをネットワークNWへ送信し、ブロックチェーンデータ552に含める。たとえば、あるタイミングで、データ管理装置500のユーザが、ある発明IDについて存在証明の申請を行なう。そうすると、データ管理装置500は、当該発明IDに紐づけられたトランザクションデータを各ブロックから読み出して、これらを纏めてハッシュ化して発明ハッシュを生成する。そして、データ管理装置500は、発明ハッシュを時刻認証局群400（詳細には、選択された時刻認証局）に送信する。発明ハッシュを受けた各時刻認証局は、発明ハッシュに国際標準時に追跡性がある時刻源に基づく時刻情報を結合させたタイムスタンプトークンを生成する。このタイムスタンプトークンにより、その時刻にブロックチェーンデータ552に含まれているデータが存在していることを証明することができる。

10

【0160】

存在証明の検証および電子証明の有効性の検証については、実施の形態1と同様の手順で処理が行なわれるため、繰り返し説明しない。

20

【0161】

以上のように、データ管理システム2に、ブロックチェーンを用いた分散型台帳技術を適用しても実施の形態1と同様の効果を奏することができる。

【0162】

今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本開示の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【符号の説明】

30

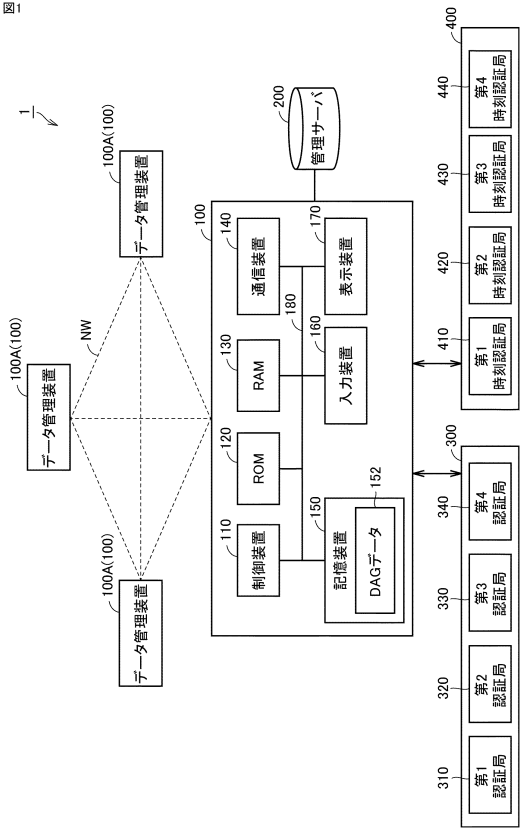
【0163】

1, 2 データ管理システム、100, 100A データ管理装置、110 制御装置、120 ROM、130 RAM、140 通信装置、150 記憶装置、152 DAG データ、160 入力装置、170 表示装置、171 選択領域、172 第1表示領域、173 第2表示領域、174 第3表示領域、175 第4表示領域、176 第5表示領域、177 第6表示領域、179 ポップアップ画面、180 バス、200 管理サーバ、300 認証局群、310 第1認証局、320 第2認証局、330 第3認証局、340 第4認証局、400 時刻認証局群、410 第1時刻認証局、420 第2時刻認証局、430 第3時刻認証局、440 第4時刻認証局、500, 500A データ管理装置、510 制御装置、550 記憶装置、552 ブロックチェーンデータ、1101 情報取得部、1103 トランザクションデータ生成部、1105 電子署名部、1107 トランザクションデータ送信部、1111 入力取得部、1113 表示制御部、1115 選択判定部、1117 発明ハッシュ生成部、1119 送信部、1121 受信部、1131 入力取得部、1133 発明ハッシュ生成部、1135 読み出し部、1137 比較部、1139 出力部、1141 入力取得部、1143 読み出し部、1145 選択部、1147 復号部、1149 判定部、1151 出力部、NW ネットワーク。

40

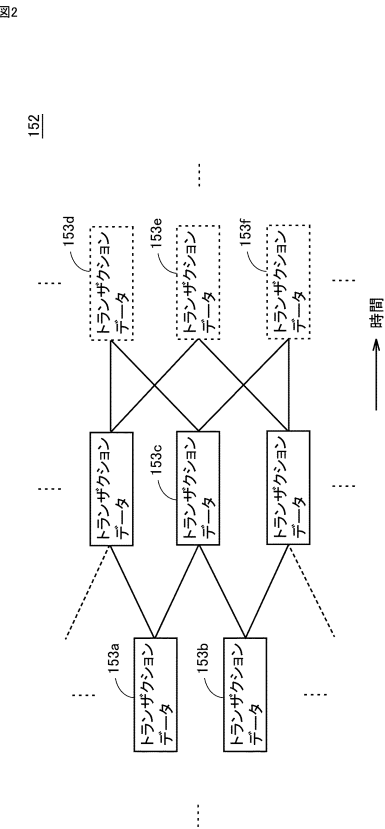
【図面】
【図 1】

図 1



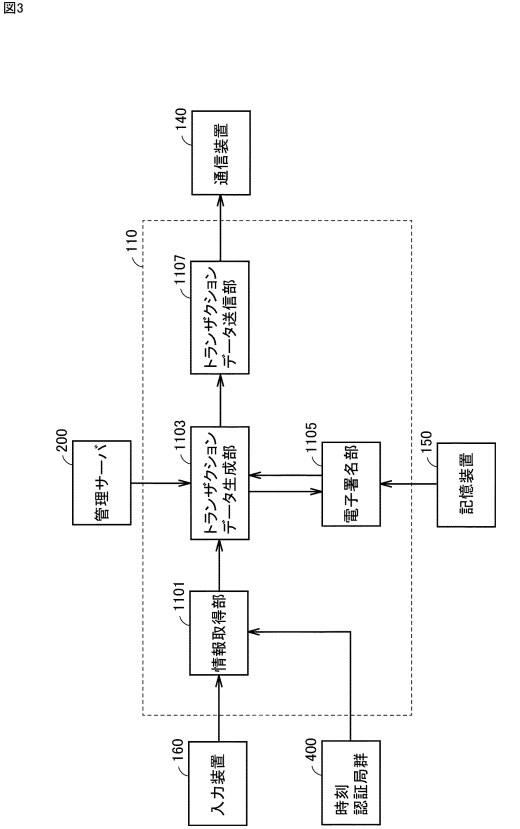
【図 2】

図 2



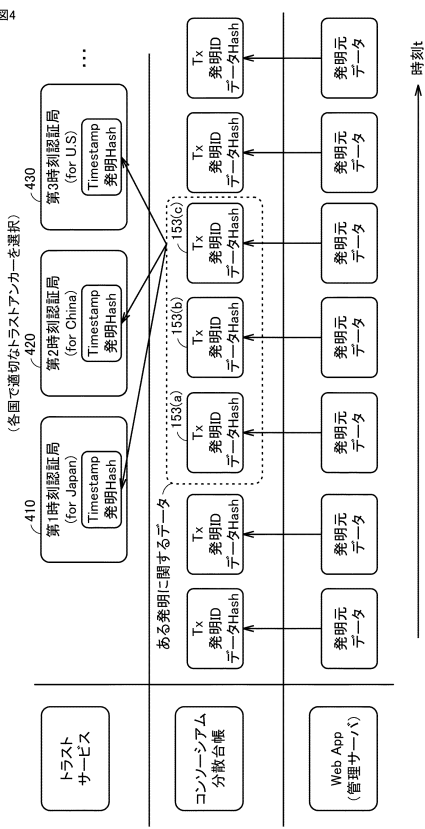
【図 3】

図 3



【図 4】

図 4



10

20

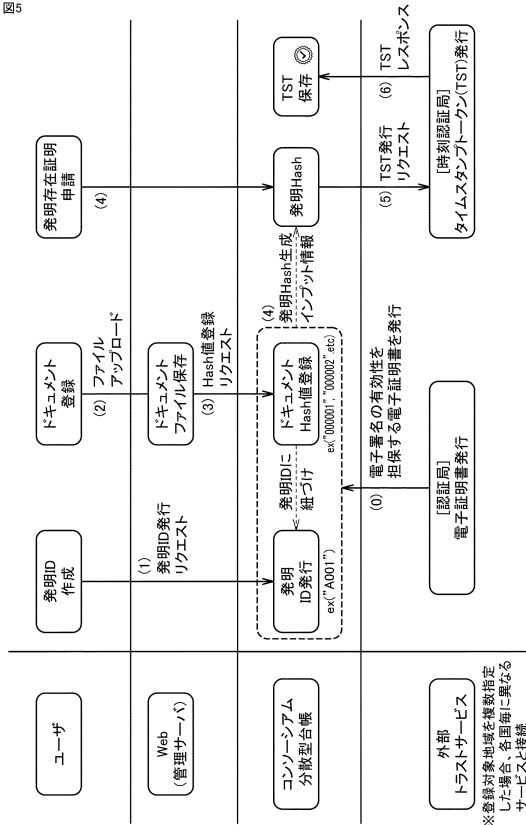
30

40

50

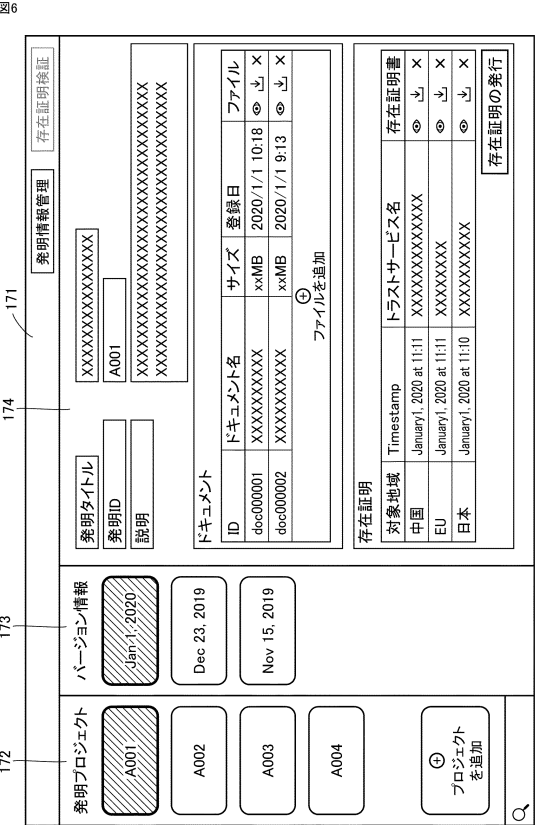
【図 5】

図5



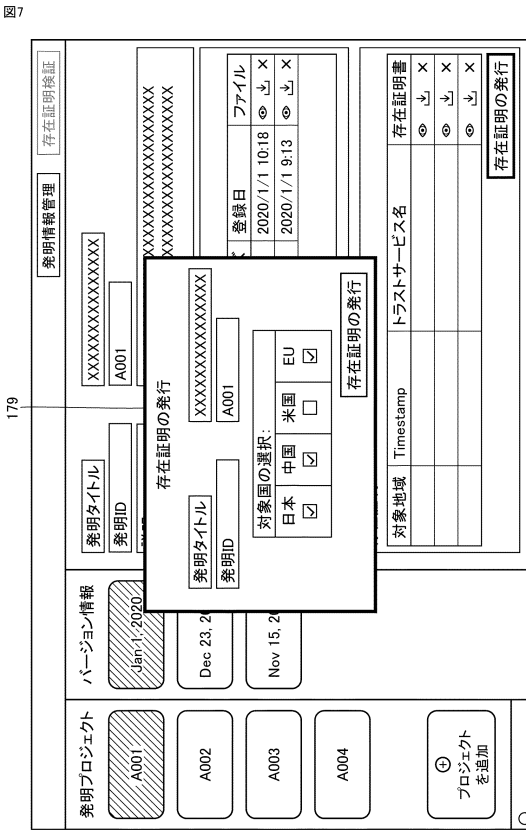
【図 6】

図6



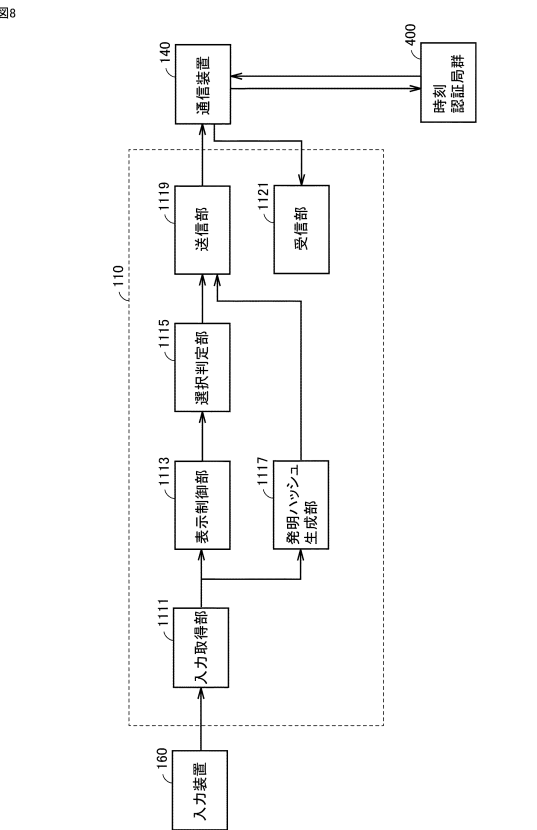
【図 7】

図7



【図 8】

図8



10

20

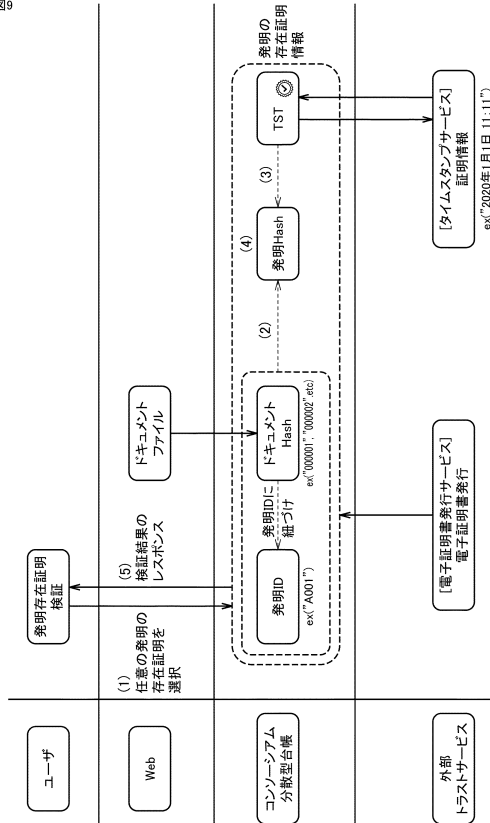
30

40

50

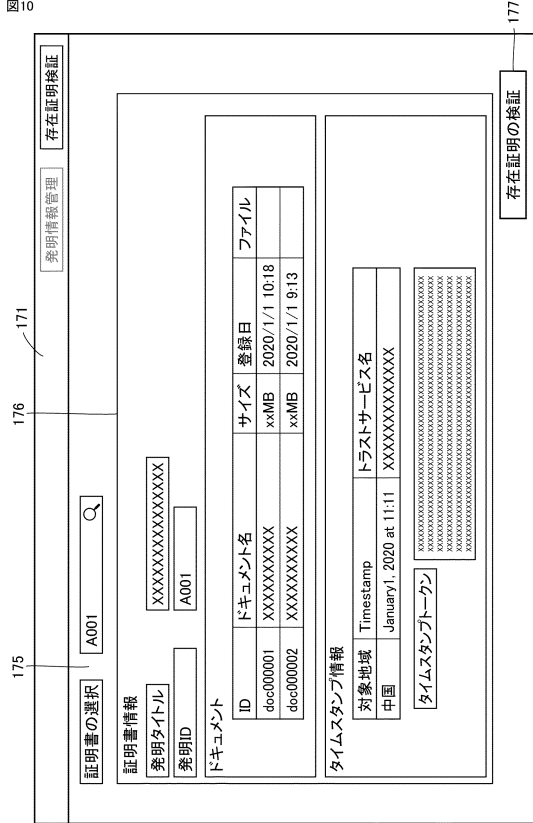
【図 9】

图9



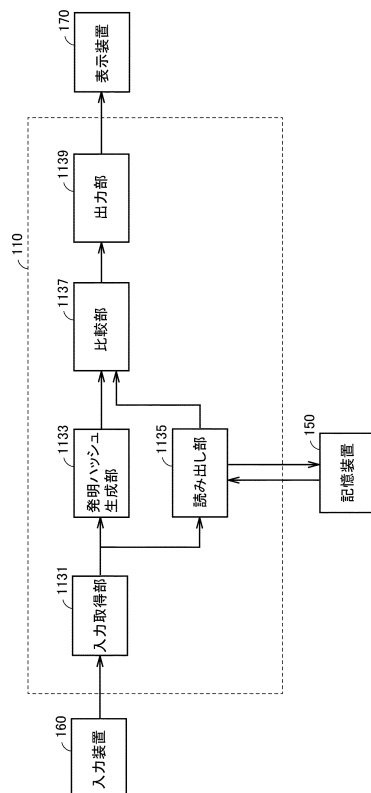
【図 10】

图 10



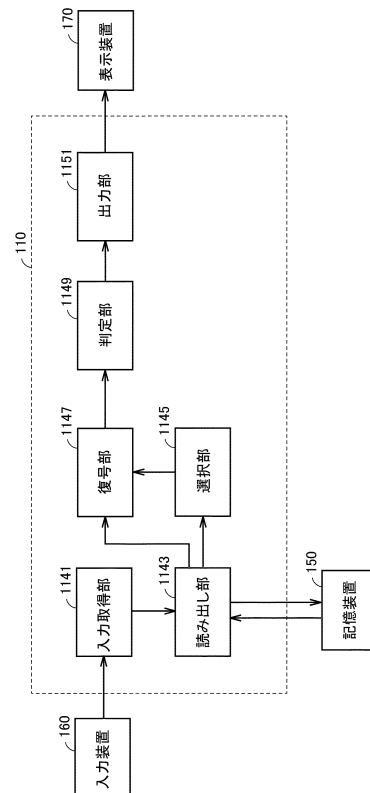
【図 1 1】

圖11



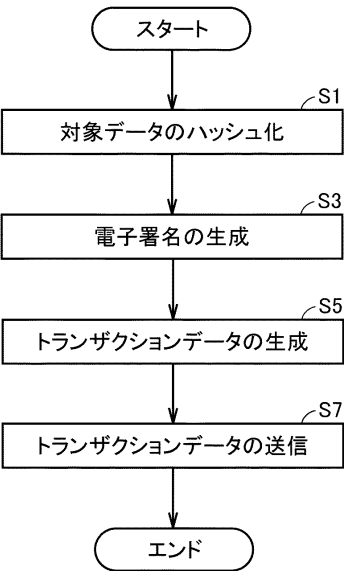
【図 12】

图12



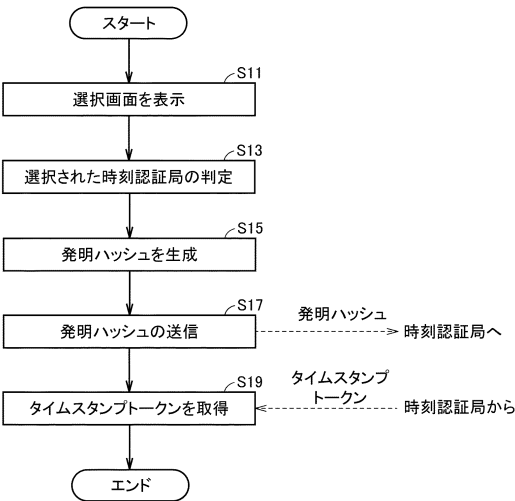
【図 1 3】

図13



【図 1 4】

図14

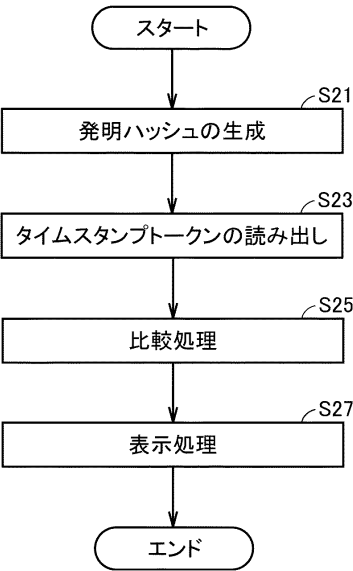


10

20

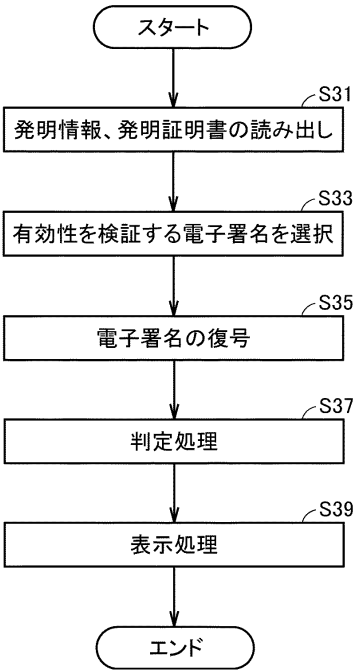
【図 1 5】

図15



【図 1 6】

図16



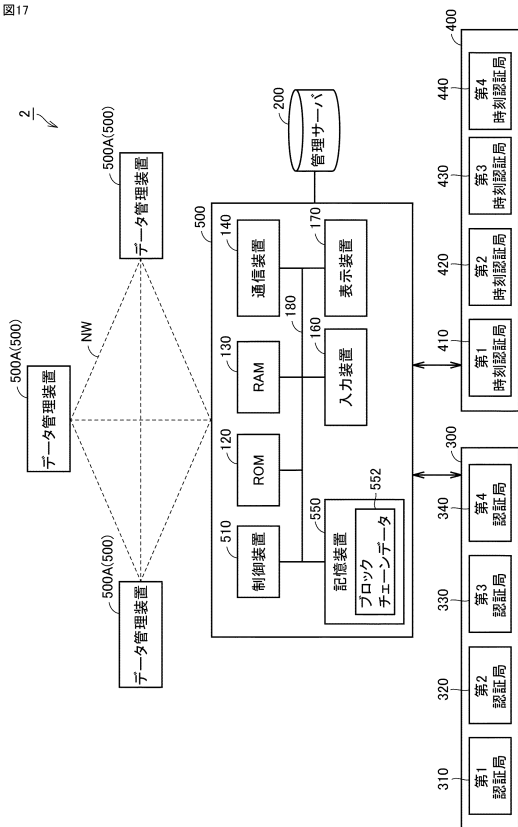
30

40

50

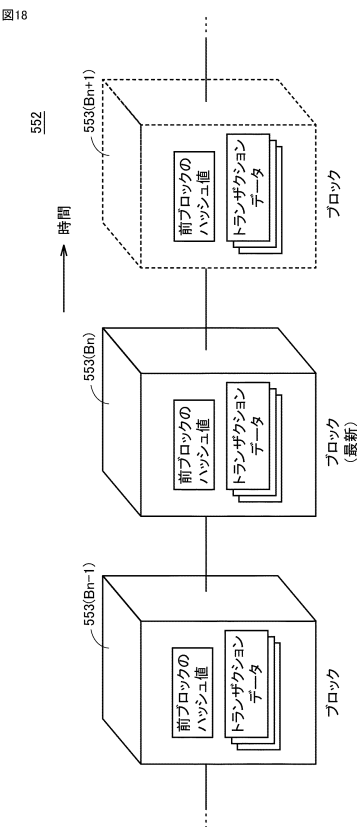
【図 17】

図 17



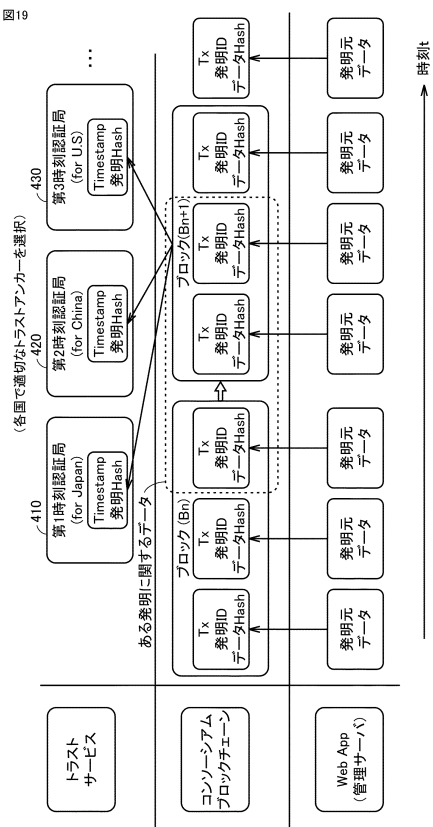
【図 18】

図 18



【図 19】

図 19



10

20

30

40

50

フロントページの続き

- 愛知県豊田市トヨタ町1番地 トヨタ自動車株式会社内
- (72)発明者 鈴木 竜太
愛知県名古屋市西区牛島町6番1号 名古屋ルーセントタワー トヨタファイナンシャルサービス株式会社内
- (72)発明者 山下 雄己
愛知県名古屋市西区牛島町6番1号 名古屋ルーセントタワー トヨタファイナンシャルサービス株式会社内
- (72)発明者 村上 仁
愛知県名古屋市西区牛島町6番1号 名古屋ルーセントタワー トヨタファイナンシャルサービス株式会社内
- 審査官 宮司 卓佳
- (56)参考文献 特表2020-512714 (JP, A)
特開2005-151358 (JP, A)
特開2012-028979 (JP, A)
特開2002-207427 (JP, A)
- (58)調査した分野 (Int.Cl., DB名)
H04L 9/32
G06F 21/64
G06Q 50/18