(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7556397号
(P7556397)

(45)発行日　令和6年9月26日(2024.9.26)

(24)登録日　令和6年9月17日(2024.9.17)

(51)国際特許分類

Ｈ０４Ｌ　9/32　(2006.01)	Ｈ０４Ｌ	9/32	２００Ｂ
Ｇ０６Ｆ　21/16　(2013.01)	Ｇ０６Ｆ	21/16	
Ｇ０６Ｆ　21/64　(2013.01)	Ｇ０６Ｆ	21/64	

ＦＩ

請求項の数　7　（全15頁）

(21)出願番号　特願2022-558654(P2022-558654)
(86)(22)出願日　令和2年10月28日(2020.10.28)
(86)国際出願番号　PCT/JP2020/040340
(87)国際公開番号　WO2022/091233
(87)国際公開日　令和4年5月5日(2022.5.5)
審査請求日　令和5年4月21日(2023.4.21)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100103894
弁理士　家入 健
(72)発明者　宮坂 信
東京都港区芝五丁目７番１号 日本電気株式会社内
審査官　児玉 崇晶

最終頁に続く

(54)【発明の名称】　データ取引管理装置、データ取引管理方法、及びプログラム

(57)【特許請求の範囲】

【請求項１】

第１の端末との間でデータを提供するための取引を行う取引部と、

加工前の前記データの識別情報、加工に使用するアプリケーションの識別情報、及び前記取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する署名部と、

前記アプリケーションを使用して、秘密計算により前記データを加工する加工部と、

加工後の前記データを前記第１の端末に提供する提供部と、

前記取引情報の署名を含む証明書を発行する発行部と、

前記証明書を公開する公開部と、

を備え、

前記取引情報は、前記第１の端末を使用する利用者の識別情報をさらに含み、

前記公開部は、前記第１の端末又は第２の端末から、前記取引情報の署名を指定した前記取引の照会要求を受信した場合、前記第１の端末又は前記第２の端末に対し、前記取引情報に含まれる、加工前の前記データの識別情報、前記アプリケーションの識別情報、及び前記利用者の識別情報を提供する、

データ取引管理装置。

【請求項２】

前記提供部は、加工後の前記データに前記証明書を添付し、前記証明書が添付された加工後の前記データを、前記第１の端末に提供する、

請求項１に記載のデータ取引管理装置。

【請求項３】
前記署名部は、加工後の前記データを暗号基盤により暗号化して、加工後の前記データの署名を生成し、
前記提供部は、加工後の前記データ及び加工後の前記データの署名を、前記第１の端末に提供する、
請求項１又は２に記載のデータ取引管理装置。
【請求項４】
データ取引管理装置が行うデータ取引管理方法であって、
第１の端末との間でデータを提供するための取引を行う取引ステップと、
加工前の前記データの識別情報、加工に使用するアプリケーションの識別情報、及び前記取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する第１の署名ステップと、
前記アプリケーションを使用して、秘密計算により前記データを加工する加工ステップと、
加工後の前記データを前記第１の端末に提供する提供ステップと、
前記取引情報の署名を含む証明書を発行する発行ステップと、
前記証明書を公開する公開ステップと、
を含み、
前記取引情報は、前記第１の端末を使用する利用者の識別情報をさらに含み、
前記公開ステップでは、前記第１の端末又は第２の端末から、前記取引情報の署名を指定した前記取引の照会要求を受信した場合、前記第１の端末又は前記第２の端末に対し、前記取引情報に含まれる、加工前の前記データの識別情報、前記アプリケーションの識別情報、及び前記利用者の識別情報を提供する、
データ取引管理方法。
【請求項５】
前記提供ステップでは、加工後の前記データに前記証明書を添付し、前記証明書が添付された加工後の前記データを、前記第１の端末に提供する、
請求項４に記載のデータ取引管理方法。
【請求項６】
加工後の前記データを暗号基盤により暗号化して、加工後の前記データの署名を生成する第２の署名ステップをさらに含み、
前記提供ステップでは、加工後の前記データ及び加工後の前記データの署名を、前記第１の端末に提供する、
請求項４又は５に記載のデータ取引管理方法。
【請求項７】
コンピュータに、
第１の端末との間でデータを提供するための取引を行う取引手順と、
加工前の前記データの識別情報、加工に使用するアプリケーションの識別情報、及び前記取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する署名手順と、
前記アプリケーションを使用して、秘密計算により前記データを加工する加工手順と、
加工後の前記データを前記第１の端末に提供する提供手順と、
前記取引情報の署名を含む証明書を発行する発行手順と、
前記証明書を公開する公開手順と、
を実行させるためのプログラムであって、
前記取引情報は、前記第１の端末を使用する利用者の識別情報をさらに含み、
前記公開手順では、前記第１の端末又は第２の端末から、前記取引情報の署名を指定した前記取引の照会要求を受信した場合、前記第１の端末又は前記第２の端末に対し、前記取引情報に含まれる、加工前の前記データの識別情報、前記アプリケーションの識別情報、及び前記利用者の識別情報を提供する、
プログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、データ取引管理装置、データ取引管理方法、及びコンピュータ可読媒体に関する。
【背景技術】
【０００２】
近年、データ提供者が、任意のデータを登録し、データ提供者とは別のデータ利用者が、その登録されたデータを取引で取得できるデータ流通市場が注目を集めている。データを流通させるためのシステムも、例えば、特許文献１に開示されている。
【０００３】
しかし、データ提供者は、需要が見込めるデータを持っている場合でも、データに秘密にしておきたい情報が含まれていると、データ流通市場にデータを提供できなくなり、データ流通市場内を流通するデータの量や種類が少なくなってしまう。
【０００４】
データ流通市場内を流通するデータの量や種類が少なくなるという問題は、秘密計算と呼ばれる技術を使用することで、解消できると考えられる。秘密計算とは、計算処理する際に、計算処理中のプログラム以外からは、処理内容を、メモリの内容も含めて、参照できなくする技術である。秘密計算の例としては、ＴＥＥ（Trusted Execution Environment）やＭＰＣ（Multi-Party Computation）等が挙げられる。
【０００５】
データに秘密にしておきたい情報が含まれている場合、アプリケーションを使用して、秘密計算により、元のデータを非公開のままにして、秘密にしておきたい情報を削除する加工をする。これにより、データ流通市場からデータを取得したデータ利用者に、その情報を秘密にすることが可能になる。
【先行技術文献】
【特許文献】
【０００６】
【文献】特開２０１６－１９５４４０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
上述したように、アプリケーションを使用して、秘密計算によりデータを加工することにより、データに含まれている、秘密にしておきたい情報を、公開することなく、加工後のデータを作成することができる。
【０００８】
ただし、加工後のデータは加工前のデータとは異なり、加工前のデータは公開されていない。そのため、加工後のデータを取得したデータ利用者は、加工後のデータが、加工前の意図したデータを加工したものであるか否かを確認したいという要求がある。
しかし、特許文献１等の関連技術では、データ利用者や第三者が、加工前のデータや、加工に使用したアプリケーションを確認する方法が存在しなかった。
【０００９】
そこで本開示の目的は、上述した課題を解決し、アプリケーションを使用して、秘密計算によりデータを加工した場合であっても、加工前のデータや、加工に使用したアプリケーションを確認できるデータ取引管理装置、データ取引管理方法、及びコンピュータ可読媒体を提供することにある。
【課題を解決するための手段】
【００１０】
一態様によるデータ取引管理装置は、
第１の端末との間でデータを提供するための取引を行う取引部と、

加工前の前記データの識別情報、加工に使用するアプリケーションの識別情報、及び前記取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する署名部と、
前記アプリケーションを使用して、秘密計算により前記データを加工する加工部と、
加工後の前記データを前記第１の端末に提供する提供部と、
前記取引情報の署名を含む証明書を発行する発行部と、
前記証明書を公開する公開部と、
を備える。
【００１１】
一態様によるデータ取引管理方法は、
データ取引管理装置が行うデータ取引管理方法であって、
第１の端末との間でデータを提供するための取引を行う取引ステップと、
加工前の前記データの識別情報、加工に使用するアプリケーションの識別情報、及び前記取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する署名ステップと、
前記アプリケーションを使用して、秘密計算により前記データを加工する加工ステップと、
加工後の前記データを前記第１の端末に提供する提供ステップと、
前記取引情報の署名を含む証明書を発行する発行ステップと、
前記証明書を公開する公開ステップと、
を含む。
【００１２】
一態様によるコンピュータ可読媒体は、
コンピュータに、
第１の端末との間でデータを提供するための取引を行う取引手順と、
加工前の前記データの識別情報、加工に使用するアプリケーションの識別情報、及び前記取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する署名手順と、
前記アプリケーションを使用して、秘密計算により前記データを加工する加工手順と、
加工後の前記データを前記第１の端末に提供する提供手順と、
前記取引情報の署名を含む証明書を発行する発行手順と、
前記証明書を公開する公開手順と、
を実行させるためのプログラムが格納される非一時的なコンピュータ可読媒体である。
【発明の効果】
【００１３】
上述の態様によれば、アプリケーションを使用して、秘密計算によりデータを加工した場合であっても、加工前のデータや、加工に使用したアプリケーションを確認できるデータ取引管理装置、データ取引管理方法、及びコンピュータ可読媒体を提供できるという効果が得られる。
【図面の簡単な説明】
【００１４】
【図１】実施の形態に係るデータ取引管理装置を含むデータ取引管理システムの構成例を示す図である。
【図２】実施の形態に係るデータ取引管理装置におけるデータ及びアプリケーションの登録時の動作例を説明する図である。
【図３】実施の形態に係るデータ取引管理装置におけるデータ取引時の動作例を説明する図である。
【図４】実施の形態に係るデータ取引管理装置におけるデータ提供時の動作例を説明する図である。
【図５】実施の形態に係るデータ取引管理装置における取引照会時の動作例を説明する図である。
【図６】実施の形態に係るデータ取引管理装置の動作のフロー例を説明するフロー図であ

る。
【図７】実施の形態に係るデータ取引管理装置を実現するコンピュータのハードウェア構成例を示すブロック図である。
【発明を実施するための形態】
【００１５】
以下、図面を参照して本開示の実施の形態について説明する。なお、以下の記載及び図面は、説明の明確化のため、適宜、省略及び簡略化がなされている。また、以下の各図面において、同一の要素には同一の符号が付されており、必要に応じて重複説明は省略されている。
【００１６】
＜実施の形態＞
まず、図１を参照して、本実施の形態に係るデータ取引管理装置１０を含むデータ取引管理システムの構成例について説明する。
【００１７】
図１に示されるように、本実施の形態に係るデータ取引管理装置１０は、データ取引管理システムに組み込まれて使用される。データ取引管理装置１０は、データ取引市場において、データ取引を管理するための装置である。
【００１８】
図１に示されるデータ取引管理システムは、データ取引管理装置１０を備える他、データ提供者端末２０、アプリケーション提供者端末３０、データ利用者端末４０、及び第三者端末５０を備えている。なお、データ利用者端末４０は、第１の端末の一例であり、第三者端末５０は、第２の端末の一例である。
【００１９】
データ提供者端末２０は、データ提供者が、秘密計算により加工する加工前のデータを提供するために使用する端末である。
アプリケーション提供者端末３０は、アプリケーション提供者が、秘密計算による加工に使用するアプリケーションを提供するために使用する端末である。
【００２０】
データ利用者端末４０は、データ利用者が、秘密計算により加工した加工後のデータを取得（購入）するために使用する端末である。
第三者端末５０は、第三者が、データ利用者が加工後のデータの権利を持っていることや、加工前のデータや加工に使用したアプリケーションを確認するために使用する端末である。
【００２１】
データ取引管理装置１０は、取引部１１、署名部１２、加工部１３、提供部１４、発行部１５、公開部１６、情報蓄積ＤＢ（Data Base。以下、同じ）１７、及び署名蓄積ＤＢ１８を備えている。
【００２２】
取引部１１は、データ利用者端末４０との間で、データを提供するための取引を行う。取引においては、取引部１１は、データ利用者端末４０から、提供するデータが指定され、課金等の処理を行う。
【００２３】
署名部１２は、後述する加工部１３が加工する加工前及び加工後のデータの署名、その加工に使用するアプリケーションの署名を生成する。さらに、署名部１２は、取引によりデータを提供するデータ利用者端末４０を使用するデータ利用者の識別情報（例えば、ユーザ名等）、加工前のデータの識別情報（例えば、データ名等）、加工に使用するアプリケーションの識別情報（例えば、アプリケーション名等）、及び取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する。
【００２４】
加工部１３は、データ利用者端末４０から指定された加工前のデータを、アプリケーシ

ョンを使用して、秘密計算により加工する。例えば、加工部１３は、加工前のデータから、データ提供者が秘密にしておきたい情報を削除する加工を行う。なお、加工に使用するアプリケーションは、データ提供者端末２０が指定しても良いし、データ利用者端末４０が指定しても良い。

【００２５】

提供部１４は、加工部１３が加工した加工後のデータをデータ利用者端末４０に提供する。このとき、提供部１４は、加工後のデータに対し、署名部１２が生成した加工後のデータの署名や、加工後のデータを復号するための鍵や、後述する発行部１５が発行する証明書を添付しても良い。

【００２６】

発行部１５は、取引情報の署名を含む証明書を発行する。

公開部１６は、発行部１５が発行した証明書を公開する。また、公開部１６は、第三者端末５０から、取引情報の署名が指定された取引の照会要求を受信した場合、第三者端末５０に対し、取引情報に含まれる、データ利用者の識別情報、加工前のデータの識別情報、及びアプリケーションの識別情報を提供する。なお、公開部１６は、データ利用者端末４０から照会要求を受信した場合にも、同様の動作を行う。

【００２７】

情報蓄積ＤＢ１７は、加工前のデータ、加工後のデータ、アプリケーション、及び取引情報を蓄積する。

署名蓄積ＤＢ１８は、加工前のデータの署名、加工後のデータの署名、アプリケーションの署名、及び取引情報の署名を蓄積する。

【００２８】

なお、情報蓄積ＤＢ１７及び署名蓄積ＤＢ１８は、データ取引管理装置１０において必須の構成要素ではなく、データ取引管理装置１０の外部に設けても良い。すなわち、データ取引管理装置１０は、取引部１１、署名部１２、加工部１３、提供部１４、発行部１５、及び公開部１６からなる最小構成で実現しても良い。

【００２９】

続いて、図２～図５を参照して、本実施の形態に係るデータ取引管理装置１０の動作例について説明する。以下では、データ取引管理装置１０の動作を、データ及びアプリケーションの登録時の動作（図２）、データ取引時の動作（図３）、データ提供時の動作（図４）、及び取引照会時の動作（図５）に分けて、それぞれについて説明する。なお、以下では、データ提供者端末２０、アプリケーション提供者端末３０、データ利用者端末４０、及び第三者端末５０は、事前に、データ取引管理装置１０を利用可能となるための設定がなされているものとする。また、図２～図５においては、説明の明確化のため、データ取引管理装置１０内の取引部１１、署名部１２、加工部１３、提供部１４、発行部１５、及び公開部１６の図示は省略している。

【００３０】

最初に、図２を参照して、データ取引管理装置１０におけるデータ及びアプリケーションの登録時の動作例について説明する。

図２に示されるように、データ提供者端末２０は、事前に、加工前のデータを情報蓄積ＤＢ１７に登録し、また、アプリケーション提供者端末３０は、事前に、加工に使用するアプリケーションを情報蓄積ＤＢ１７に登録する。この登録は、データ取引管理装置１０内の任意の構成要素（例えば、取引部１１等）を介して行えば良い。

【００３１】

次に、署名部１２は、情報蓄積ＤＢ１７に登録された加工前のデータ及びアプリケーションの各々の署名を生成する。この署名は、任意の方式で生成すれば良く、例えば、ハッシュ値を署名としても良い。次に、署名部１２は、生成した署名を署名蓄積ＤＢ１８に登録する。このとき、情報蓄積ＤＢ１７に登録された加工前のデータ及びアプリケーションと、署名蓄積ＤＢ１８に登録されたそれらの署名とは、例えば、取引の識別情報を付加して登録する等によって、互いに対応付けておく。

【００３２】
続いて、図３を参照して、データ取引管理装置１０におけるデータ取引時の動作例について説明する。
図３に示されるように、まず、取引部１１は、データ利用者端末４０との間で、データを提供するための取引を行う。この取引においては、取引部１１は、データ利用者端末４０から、提供するデータが指定される。次に、取引部１１は、取引の結果に基づいて、データ利用者端末４０を使用するデータ利用者の識別情報、加工前のデータの識別情報、加工に使用するアプリケーションの識別情報、及び取引を行った時刻を示すタイムスタンプを含む取引情報を、情報蓄積ＤＢ１７に登録する。
【００３３】
次に、署名部１２は、取引情報の署名を生成する。この署名も、任意の方式で生成すれば良く、例えば、ハッシュ値を署名としても良い。次に、署名部１２は、生成した署名を署名蓄積ＤＢ１８に登録する。このとき、情報蓄積ＤＢ１７に登録された取引情報と、署名蓄積ＤＢ１８に登録された取引情報の署名とは、例えば、取引の識別情報を付加して登録する等によって、互いに対応付けておく。
【００３４】
続いて、図４を参照して、データ取引管理装置１０におけるデータ提供時の動作例について説明する。なお、図４の動作は、図３の動作が終了したタイミングで開始される。
図４に示されるように、まず、加工部１３は、データ利用者端末４０から指定された加工前のデータ及びアプリケーションを、情報蓄積ＤＢ１７から取り出し、アプリケーションを使用して、秘密計算により加工前のデータを加工する。
【００３５】
次に、署名部１２は、加工部１３が加工した加工後のデータの署名を生成する。この署名は、ＰＫＩ（Public Key Infrastructure）方式で生成するのが好ましい。そのため、署名部１２は、加工後のデータのハッシュ値を秘密鍵で暗号化することにより、加工後のデータの署名を生成する。次に、署名部１２は、生成した署名を署名蓄積ＤＢ１８に登録する。このとき、情報蓄積ＤＢ１７に登録された加工後のデータと、署名蓄積ＤＢ１８に登録された加工後のデータの署名とは、例えば、取引の識別情報を付加して登録する等によって、互いに対応付けておく。
【００３６】
次に、提供部１４は、加工部１３が加工した加工後のデータに、加工後のデータの署名、加工後のデータを復号するための公開鍵、及び、署名蓄積ＤＢ１８から取り出した取引情報の署名を添付して、データ利用者端末４０に提供する。なお、公開鍵及び取引情報の署名は、発行部１５が発行する証明書の形式で、加工後のデータに添付しても良い。ただし、加工後のデータに取引情報の署名を添付することは、任意で行えば良い。また、加工部１３による秘密計算の基盤で鍵が提供される場合は、その鍵を利用することで秘密計算の処理をした基盤の証明も可能となる。
【００３７】
次に、発行部１５は、署名蓄積ＤＢ１８から取引情報の署名を取り出し、取り出した取引情報の署名を含む証明書を発行する。公開部１６は、発行部１５が発行した証明書を公開する。
【００３８】
このように、公開部１６は、取引情報の署名を含む証明書を公開する。これにより、第三者端末５０及びデータ利用者端末４０は、証明書に含まれる取引情報の署名を指定して、取引の照会要求を行うことができる。その結果、第三者端末５０及びデータ利用者端末４０は、取引情報に含まれる、データ利用者、加工前のデータ、アプリケーションを確認できるため、加工後のデータの権利をデータ利用者が持っていることや、加工前のデータや加工に使用したアプリケーションを確認できるようになる。
【００３９】
続いて、図５を参照して、データ取引管理装置１０における取引照会時の動作例につい

て説明する。図５は、第三者端末５０が取引の照会要求を行う場合の動作例である。

【００４０】

図５に示されるように、公開部１６は、第三者端末５０から、取引情報の署名が指定された取引の照会要求を受信した場合、まず、情報蓄積ＤＢ１７から、取引情報の署名に対応付けられた取引情報を取り出す。次に、公開部１６は、第三者端末５０に対し、取引情報に含まれる、データ利用者の識別情報、加工前のデータの識別情報、及びアプリケーションの識別情報を提供する。なお、公開部１６は、データ利用者端末４０から照会要求を受信した場合にも、同様の動作を行う。

【００４１】

続いて、図６を参照して、本実施の形態に係るデータ取引管理装置１０の動作のフロー例について説明する。なお、図６は、図３のデータ取引時の動作から、図４のデータ提供時の動作までに相当する動作を示している。

【００４２】

図６に示されるように、まず、取引部１１は、データ利用者端末４０との間で、データを提供するための取引を行う（ステップＳ１１）。この取引においては、取引部１１は、データ利用者端末４０から、提供するデータが指定される。

【００４３】

次に、取引部１１は、取引の結果に基づいて、データ利用者端末４０を使用するデータ利用者の識別情報、加工前のデータの識別情報、加工に使用するアプリケーションの識別情報、及び取引を行った時刻を示すタイムスタンプを含む取引情報を、情報蓄積ＤＢ１７に登録する（ステップＳ１２）。

【００４４】

次に、署名部１２は、取引情報の署名を生成し、生成した署名を署名蓄積ＤＢ１８に登録する（ステップＳ１３）。

次に、加工部１３は、データ利用者端末４０から指定された加工前のデータ及びアプリケーションを、情報蓄積ＤＢ１７から取り出し、アプリケーションを使用して、秘密計算により加工前のデータを加工する（ステップＳ１４）。

【００４５】

次に、署名部１２は、加工部１３が加工した加工後のデータの署名を生成し、生成した署名を署名蓄積ＤＢ１８に登録する（ステップＳ１５）。

次に、提供部１４は、加工部１３が加工した加工後のデータを、データ利用者端末４０に提供する（ステップＳ１６）。このとき、提供部１４は、加工後のデータに、加工後のデータの署名を添付しても良い。また、提供部１４は、加工後のデータを鍵で復号する必要があれば、加工後のデータに、鍵を添付しても良い。また、提供部１４は、加工後のデータに、取引情報の署名を添付しても良い。

【００４６】

その後、発行部１５は、署名蓄積ＤＢ１８から取引情報の署名を取り出し、取り出した取引情報の署名を含む証明書を発行し、公開部１６は、発行部１５が発行した証明書を公開する（ステップＳ１７）。

【００４７】

上述したように本実施の形態１によれば、取引部１１は、データ利用者端末４０との間で、データを提供するための取引を行う。署名部１２は、データ利用者の識別情報、加工前のデータの識別情報、加工に使用するアプリケーションの識別情報、及び取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する。加工部１３は、アプリケーションを使用して、秘密計算により加工前のデータを加工し、提供部１４は、加工後のデータをデータ利用者端末４０に提供する。発行部１５は、取引情報の署名を含む証明書を発行し、公開部１６は、その証明書を公開する。

【００４８】

これにより、第三者端末５０及びデータ利用者端末４０は、証明書に含まれる取引情報の署名を指定して、取引の照会要求を行うことができる。そのため、第三者端末５０及び

データ利用者端末４０は、加工後のデータの権利をデータ利用者が持っていることや、加工前のデータや加工に使用したアプリケーションを確認できるようになる。

【００４９】

＜その他の実施の形態＞

上述した実施の形態では、情報蓄積ＤＢ１７に加工前のデータ、アプリケーション、及び取引情報を登録しているが、これらの取引情報等は、一定期間保存して、再度署名を生成できる状態を維持しておくことが好ましい。情報蓄積ＤＢ１７から取引情報等を削除してしまうと、再度署名を生成できず、証明書の再現性を担保できない。そのため、情報蓄積ＤＢ１７に取引情報等を一定期間保存することで、証明書の再現性を担保し、加工前のデータ等を長期間証明することが可能となる。

【００５０】

また、上述した実施の形態では、データ取引市場において、データ取引を管理するデータ取引管理装置１０内の署名蓄積ＤＢ１８に署名を登録している。しかし、データ流通市場の内部で、署名の改ざんが行われる可能性もある。そのため、データ流通市場の内部における署名蓄積ＤＢ１８の改ざんを防止するため、署名蓄積ＤＢ１８に改ざん対策を行うことが好ましい。改ざん対策としては、ブロックチェーン方式で署名を蓄積する等が考えられる。又は、外部の認証局を利用して証明書を生成することも考えられる。

【００５１】

また、上述した実施の形態では、取引情報にデータ利用者の識別情報を含めていたが、これには限定されない。例えば、加工後のデータを取得したデータ利用者は、取引の識別情報から辿っていく等で、確認できる可能性がある。このように、加工後のデータを取得したデータ利用者については、その他の手段を使用しても確認できると考えられる。そのため、取引情報にデータ利用者の識別情報を含めることは、任意で行えば良い。

【００５２】

また、上述した実施の形態では、署名部１２は、加工後のデータの署名を、ＰＫＩ方式で生成していたが、これには限定されない。署名部１２は、加工後のデータの署名を、任意の暗号基盤により暗号化して生成すれば良い。

【００５３】

また、上述した実施の形態では、データ提供者端末２０は、加工前のデータを暗号化せずに情報蓄積ＤＢ１７に登録することを想定していたが、これには限定されない。データ提供者端末２０は、加工前のデータを暗号化した上で、情報蓄積ＤＢ１７に登録しても良い。

【００５４】

また、上述した実施の形態では、データ提供者端末２０内の構成要素が１つの筐体に配置されることを想定していたが、これには限定されない。データ提供者端末２０内の構成要素は、複数の筐体に分散して配置されても良い。

【００５５】

＜実施の形態に係るデータ取引管理装置のハードウェア構成＞

続いて、図７を参照して、上述した実施の形態に係るデータ取引管理装置１０を実現するコンピュータ６０のハードウェア構成について説明する。なお、図７に示されるコンピュータ６０は、構成要素が１つの筐体に配置されるデータ取引管理装置１０を実現するものであるとする。

【００５６】

図７に示されるように、コンピュータ６０は、プロセッサ６０１、メモリ６０２、ストレージ６０３、入出力インタフェース（入出力Ｉ／Ｆ）６０４、及び通信インタフェース（通信Ｉ／Ｆ）６０５等を備える。プロセッサ６０１、メモリ６０２、ストレージ６０３、入出力インタフェース６０４、及び通信インタフェース６０５は、相互にデータを送受信するためのデータ伝送路で接続されている。

【００５７】

プロセッサ６０１は、例えばＣＰＵ（Central Processing Unit）やＧＰＵ（Graphics

Processing Unit）等の演算処理装置である。メモリ６０２は、例えばＲＡＭ（Random Access Memory）やＲＯＭ（Read Only Memory）等のメモリである。ストレージ６０３は、例えばＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）、またはメモリカード等の記憶装置である。また、ストレージ６０３は、ＲＡＭやＲＯＭ等のメモリであっても良い。

【００５８】

ストレージ６０３は、データ取引管理装置１０が備える構成要素の機能を実現するプログラムを記憶している。プロセッサ６０１は、これら各プログラムを実行することで、データ取引管理装置１０が備える構成要素の機能をそれぞれ実現する。ここで、プロセッサ６０１は、上記各プログラムを実行する際、これらのプログラムをメモリ６０２上に読み出してから実行しても良いし、メモリ６０２上に読み出さずに実行しても良い。また、メモリ６０２やストレージ６０３は、データ取引管理装置１０が備える構成要素が保持する情報やデータを記憶する役割も果たす。

【００５９】

また、上述したプログラムは、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（コンピュータ６０を含む）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（Compact Disc-ROM）、ＣＤ－Ｒ（CD-Recordable）、ＣＤ－Ｒ／Ｗ（CD-ReWritable）、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を含む。また、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良い。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。

【００６０】

入出力インタフェース６０４は、表示装置６０４１、入力装置６０４２、音出力装置６０４３等と接続される。表示装置６０４１は、ＬＣＤ（Liquid Crystal Display）、ＣＲＴ（Cathode Ray Tube）ディスプレイ、モニターのような、プロセッサ６０１により処理された描画データに対応する画面を表示する装置である。入力装置６０４２は、オペレータの操作入力を受け付ける装置であり、例えば、キーボード、マウス、及びタッチセンサ等である。表示装置６０４１及び入力装置６０４２は一体化され、タッチパネルとして実現されていても良い。音出力装置６０４３は、スピーカのような、プロセッサ６０１により処理された音響データに対応する音を音響出力する装置である。

【００６１】

通信インタフェース６０５は、外部の装置との間でデータを送受信する。例えば、通信インタフェース６０５は、有線通信路または無線通信路を介して外部装置と通信する。

【００６２】

以上、実施の形態を参照して本開示を説明したが、本開示は上述した実施の形態に限定されるものではない。本開示の構成や詳細には、本開示のスコープ内で当業者が理解し得る様々な変更をすることができる。

【００６３】

また、上述した実施の形態の一部又は全部は、以下の付記のようにも記載されうるが、以下には限られない。

（付記１）

第１の端末との間でデータを提供するための取引を行う取引部と、

加工前の前記データの識別情報、加工に使用するアプリケーションの識別情報、及び前

記取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する署名部と、
前記アプリケーションを使用して、秘密計算により前記データを加工する加工部と、
加工後の前記データを前記第１の端末に提供する提供部と、
前記取引情報の署名を含む証明書を発行する発行部と、
前記証明書を公開する公開部と、
を備える、データ取引管理装置。
（付記２）
前記公開部は、前記第１の端末又は第２の端末から、前記取引情報の署名を指定した前記取引の照会要求を受信した場合、前記第１の端末又は前記第２の端末に対し、前記取引情報に含まれる、加工前の前記データの識別情報及び前記アプリケーションの識別情報を提供する、
付記１に記載のデータ取引管理装置。
（付記３）
前記取引情報は、前記第１の端末を使用する利用者の識別情報をさらに含み、
前記公開部は、前記第１の端末又は前記第２の端末から前記照会要求を受信した場合、前記第１の端末又は前記第２の端末に対し、前記取引情報に含まれる、加工前の前記データの識別情報、前記アプリケーションの識別情報、及び前記利用者の識別情報を提供する、
付記２に記載のデータ取引管理装置。
（付記４）
前記提供部は、加工後の前記データに前記証明書を添付し、前記証明書が添付された加工後の前記データを、前記第１の端末に提供する、
付記１から３のいずれか１項に記載のデータ取引管理装置。
（付記５）
前記署名部は、加工後の前記データを暗号基盤により暗号化して、加工後の前記データの署名を生成し、
前記提供部は、加工後の前記データ及び加工後の前記データの署名を、前記第１の端末に提供する、
付記１から４のいずれか１項に記載のデータ取引管理装置。
（付記６）
データ取引管理装置が行うデータ取引管理方法であって、
第１の端末との間でデータを提供するための取引を行う取引ステップと、
加工前の前記データの識別情報、加工に使用するアプリケーションの識別情報、及び前記取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する第１の署名ステップと、
前記アプリケーションを使用して、秘密計算により前記データを加工する加工ステップと、
加工後の前記データを前記第１の端末に提供する提供ステップと、
前記取引情報の署名を含む証明書を発行する発行ステップと、
前記証明書を公開する公開ステップと、
を含む、データ取引管理方法。
（付記７）
前記公開ステップでは、前記第１の端末又は第２の端末から、前記取引情報の署名を指定した前記取引の照会要求を受信した場合、前記第１の端末又は前記第２の端末に対し、前記取引情報に含まれる、加工前の前記データの識別情報及び前記アプリケーションの識別情報を提供する、
付記６に記載のデータ取引管理方法。
（付記８）
前記取引情報は、前記第１の端末を使用する利用者の識別情報をさらに含み、
前記公開ステップでは、前記第１の端末又は前記第２の端末から前記照会要求を受信した場合、前記第１の端末又は前記第２の端末に対し、前記取引情報に含まれる、加工前の

前記データの識別情報、前記アプリケーションの識別情報、及び前記利用者の識別情報を提供する、
付記７に記載のデータ取引管理方法。
（付記９）
前記提供ステップでは、加工後の前記データに前記証明書を添付し、前記証明書が添付された加工後の前記データを、前記第１の端末に提供する、
付記６から８のいずれか１項に記載のデータ取引管理方法。
（付記１０）
加工後の前記データを暗号基盤により暗号化して、加工後の前記データの署名を生成する第２の署名ステップをさらに含み、
前記提供ステップでは、加工後の前記データ及び加工後の前記データの署名を、前記第１の端末に提供する、
付記６から９のいずれか１項に記載のデータ取引管理方法。
（付記１１）
コンピュータに、
第１の端末との間でデータを提供するための取引を行う取引手順と、
加工前の前記データの識別情報、加工に使用するアプリケーションの識別情報、及び前記取引を行った時刻を示すタイムスタンプを含む取引情報の署名を生成する署名手順と、
前記アプリケーションを使用して、秘密計算により前記データを加工する加工手順と、
加工後の前記データを前記第１の端末に提供する提供手順と、
前記取引情報の署名を含む証明書を発行する発行手順と、
前記証明書を公開する公開手順と、
を実行させるためのプログラムが格納された非一時的なコンピュータ可読媒体。
【符号の説明】
【００６４】
１０　データ取引管理装置
１１　取引部
１２　署名部
１３　加工部
１４　提供部
１５　発行部
１６　公開部
１７　情報蓄積ＤＢ
１８　署名蓄積ＤＢ
２０　データ提供者端末
３０　アプリケーション提供者端末
４０　データ利用者端末
５０　第三者端末
６０　コンピュータ
６０１　プロセッサ
６０２　メモリ
６０３　ストレージ
６０４　入出力インタフェース
６０４１　表示装置
６０４２　入力装置
６０４３　音出力装置
６０５　通信インタフェース

【図面】

【図１】

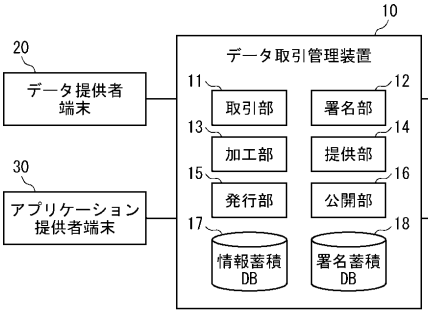

Fig. 1

【図２】

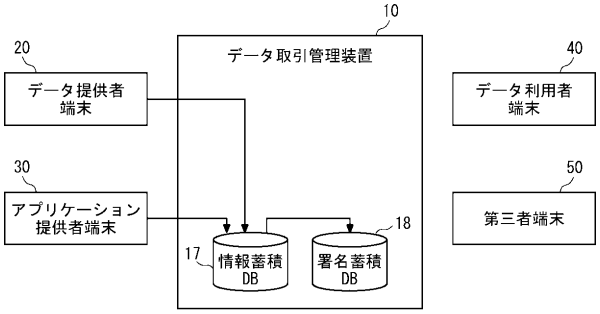

Fig. 2

【図３】

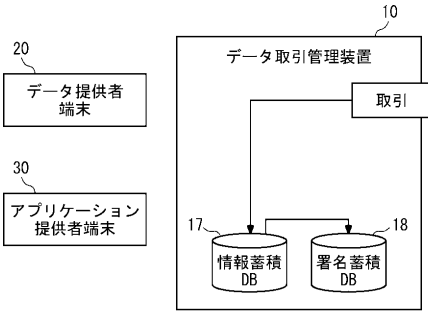

Fig. 3

【図４】

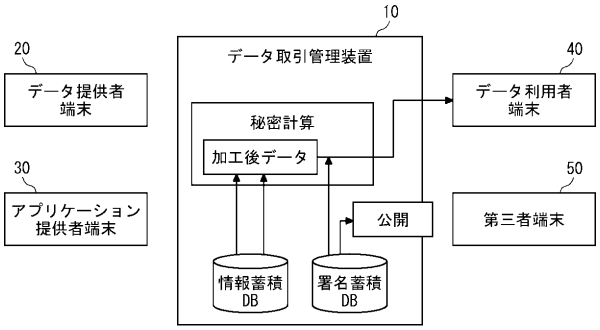

Fig. 4

【図５】

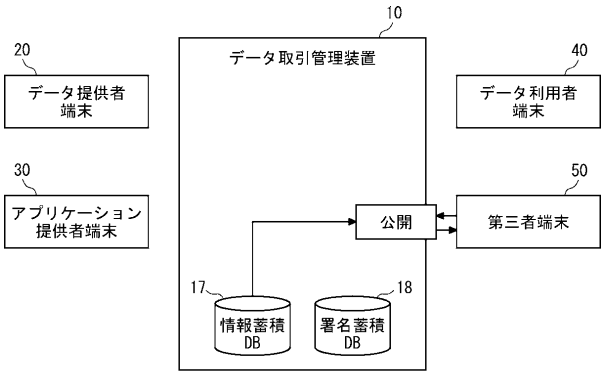

Fig. 5

【図６】

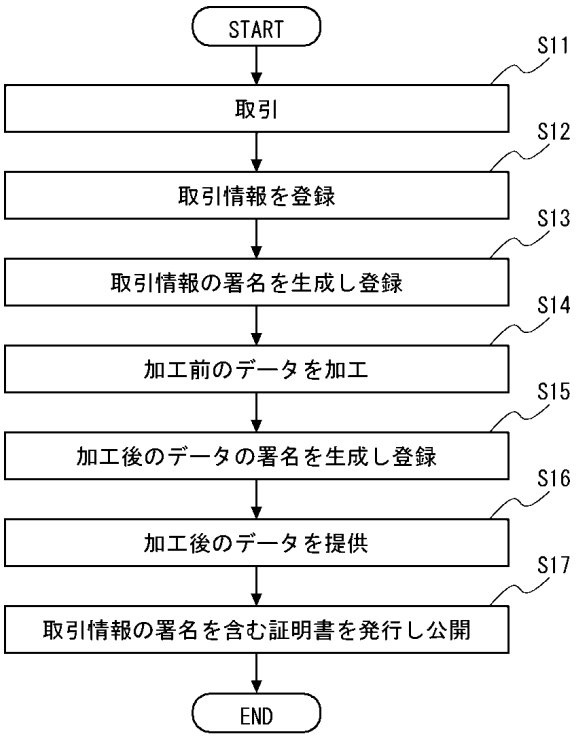

Fig. 6

【図７】

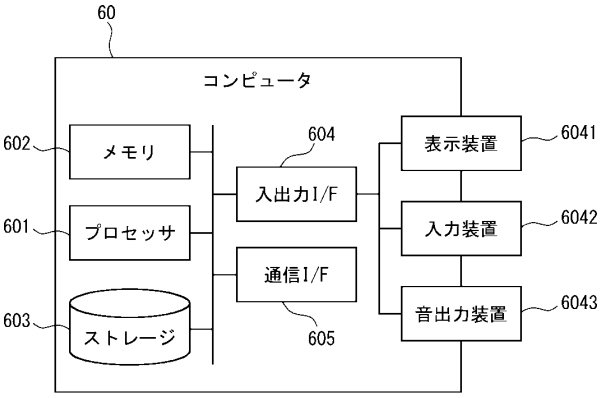

Fig. 7

フロントページの続き

(56)参考文献　特開２０２０－０４６９９３（ＪＰ，Ａ）
特開２０１３－０９７３５１（ＪＰ，Ａ）
特開２００８－１２４６６８（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０６Ｆ　２１／１６
Ｇ０６Ｆ　２１／６４