

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号  
特許第7514766号  
(P7514766)

(45)発行日 令和6年7月11日(2024.7.11)

(24)登録日 令和6年7月3日(2024.7.3)

(51)国際特許分類 F I  
 G 0 6 F 21/62 (2013.01) G 0 6 F 21/62 3 4 5  
 H 0 4 L 9/32 (2006.01) H 0 4 L 9/32 2 0 0 Z

請求項の数 13 (全30頁)

(21)出願番号	特願2020-559269(P2020-559269)	(73)特許権者	514136668 パナソニック インテレクチュアル プロパティ コーポレーション オブ アメリカ Panasonic Intellectual Property Corporation of America アメリカ合衆国 9 0 5 0 4 カリフォルニア州, トーランス, スイート 4 5 0 , ウェスト 1 9 0 ストリート 2 0 5 0
(86)(22)出願日	令和1年12月11日(2019.12.11)	(74)代理人	100109210 弁理士 新居 広守
(86)国際出願番号	PCT/JP2019/048391	(74)代理人	100137235 弁理士 寺谷 英作
(87)国際公開番号	WO2020/122095	(74)代理人	100131417 弁理士 道坂 伸一
(87)国際公開日	令和2年6月18日(2020.6.18)		
審査請求日	令和4年10月4日(2022.10.4)		
(31)優先権主張番号	62/777,922		
(32)優先日	平成30年12月11日(2018.12.11)		
(33)優先権主張国・地域又は機関	米国(US)		

最終頁に続く

(54)【発明の名称】 制御方法、情報管理システム、および、プログラム

(57)【特許請求の範囲】

【請求項 1】

管理サーバとサーバとを備える情報管理システムにおける制御方法であって、

前記サーバは、

前記管理サーバにより管理されているユーザ情報であって、第一ユーザに関する情報であるユーザ情報に対応付けられた識別情報と、前記ユーザ情報の第二ユーザへの提供の許否を示す許否情報とを含む第一ランザクションデータを前記管理サーバから受信し、

受信した前記第一ランザクションデータに含まれている前記許否情報が、前記第一ユーザが設定した許否情報である設定許否情報と整合しているいか否かを判定し、

前記許否情報が前記設定許否情報と整合していると判定した場合に、受信した前記第一ランザクションデータを分散台帳に格納する

制御方法。

【請求項 2】

前記制御方法は、さらに、

前記識別情報、又は、前記第一ユーザが属する属性を示す属性情報を含み、前記識別情報または前記属性情報に適合する前記ユーザ情報の利用を求めることを示す第二ランザクションデータを前記第二ユーザの端末から受信し、

受信した前記第二ランザクションデータを前記分散台帳に格納する

請求項 1 に記載の制御方法。

【請求項 3】

10

20

前記ユーザ情報は、1以上のユーザ情報を含み、

前記許否情報は、前記1以上のユーザ情報のうち、前記第二ユーザへの提供が許可されるユーザ情報の条件を含み、

前記第二トランザクションデータは、さらに、前記識別情報に対応付けられた前記第一ユーザ、又は、前記属性情報により示される前記属性に属する前記第一ユーザに関するユーザ情報であって、前記第二ユーザが提供を求めるユーザ情報を示す要求情報を含み、

前記制御方法は、さらに、

前記第二トランザクションデータに含まれる前記要求情報が、前記許否情報に含まれる前記条件に適合するか否かを判定し、

前記要求情報が前記条件に適合すると判定した場合に限り、受信した前記第二トランザクションデータを前記分散台帳に格納する

請求項2に記載の制御方法。

【請求項4】

前記制御方法は、さらに、

前記第二トランザクションデータを受信したことに基づいて、前記第二ユーザの端末に前記ユーザ情報が送信された場合に、送信された前記ユーザ情報に係る前記識別情報又は前記属性情報を含む第三トランザクションデータを受信し、

受信した前記第三トランザクションデータを前記分散台帳に格納する

請求項2又は3に記載の制御方法。

【請求項5】

前記制御方法は、さらに、

前記第二ユーザの端末に前記ユーザ情報が送信されてから所定時間が経過した場合に、提供された前記ユーザ情報の利用が制限されることを示す制限情報を含む第四トランザクションデータを受信し、

受信した前記第四トランザクションデータを前記分散台帳に格納する

請求項3又は4に記載の制御方法。

【請求項6】

前記制御方法は、さらに、

前記情報管理システムにおいて管理されていて削除されたユーザ情報を示す識別子と、前記ユーザ情報が削除されたことを示す削除情報とを含む第五トランザクションデータを受信し、

受信した前記第五トランザクションデータを前記分散台帳に格納する

請求項1～5のいずれか1項に記載の制御方法。

【請求項7】

前記第一トランザクションデータを受信したときには、前記第一ユーザにトークンを付与する提供情報を含む第六トランザクションデータを取得し、

取得した前記第六トランザクションデータを前記分散台帳に格納する

請求項1～6のいずれか1項に記載の制御方法。

【請求項8】

前記許否情報は、前記ユーザ情報の提供を許可する期間、前記ユーザ情報の提供が許可されるユーザ、又は、前記ユーザ情報の再提供の許否を示す情報を含む

請求項1～7のいずれか1項に記載の制御方法。

【請求項9】

前記1以上のユーザ情報のそれぞれには、当該ユーザ情報の種別を示す種別情報が紐付けられており、

前記許否情報は、前記ユーザ情報の提供を許可する種別情報を含む

請求項3に記載の制御方法。

【請求項10】

前記管理サーバは、前記第一ユーザの端末から前記ユーザ情報と前記設定許否情報を取得して記録し、

10

20

30

40

50

前記サーバは、前記第一ランザクションデータに含まれる前記許否情報が、前記管理サーバに記録された前記設定許否情報と整合している場合に、受信した前記第一ランザクションデータを分散台帳に格納する。

請求項 1 に記載の制御方法。

【請求項 1 1】

前記第一ランザクションデータに含まれる前記許否情報が前記設定許否情報と整合しないと判定した場合、前記整合しなかったことを示す情報を含めたランザクションデータを生成し前記分散台帳に格納する、

請求項 1 に記載の制御方法。

【請求項 1 2】

管理サーバとサーバとを備える情報管理システムであって、

前記管理サーバは、

前記管理サーバにより管理されているユーザ情報であって、第一ユーザに関する情報であるユーザ情報に対応付けられた識別情報と、前記ユーザ情報の第二ユーザへの提供の許否を示す許否情報とを含む第一ランザクションデータを前記サーバに送信し、

前記サーバは、

前記管理サーバが送信した前記第一ランザクションデータを受信し、

受信した前記第一ランザクションデータに含まれている前記許否情報が、前記第一ユーザが設定した許否情報である設定許否情報と整合しているいか否かを判定し、

前記許否情報が前記設定許否情報と整合していると判定した場合に、受信した前記第一ランザクションデータを分散台帳に格納する処理部を備える情報管理システム。

【請求項 1 3】

請求項 1 ~ 1.1 のいずれか 1 項に記載の制御方法をコンピュータによって実行するためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、制御方法、サーバ、プログラム、および、データ構造に関する。

【背景技術】

【0002】

個人のデータを管理するとともに、そのデータを第三者に提供する情報銀行（情報利用信用銀行ともいう）が利用されている（非特許文献 1 参照）。

【先行技術文献】

【非特許文献】

【0003】

【文献】内閣官房IT総合戦略室、「AI、IoT時代におけるデータ活用ワーキンググループ中間とりまとめの概要」、[online]、[令和元年 1 1 月 2 5 日検索]、インターネット URL:[https://www.kantei.go.jp/jp/singi/it2/senmon\\_bunka/data\\_ryutsuseibi/ai2/siryoku1.pdf](https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/ai2/siryoku1.pdf)

【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、個人のデータの利用の都度に当該個人と情報銀行との間で利用の承諾に関わる情報交換のための通信が発生し得るとい問題がある。

【0005】

そこで、本発明は、情報管理システムにおいて、個人のデータの利用の際に発生し得る通信を抑制する制御方法などを提供する。

【課題を解決するための手段】

【0006】

10

20

30

40

50

本発明の一態様に係る制御方法は、分散台帳を保有している複数のサーバを備える情報管理システムにおいて、当該複数のサーバのうちの一のサーバが実行する制御方法であって、前記情報管理システムにより管理されているユーザ情報であって、第一ユーザに関する情報であるユーザ情報に対応付けられた識別情報と、前記ユーザ情報の第二ユーザへの提供の許否を示す許否情報とを含む第一トランザクションデータを受信し、受信した前記第一トランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する。

【 0 0 0 7 】

なお、これらの包括的または具体的な態様は、システム、装置、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なCD-ROMなどの記録媒体で実現されてもよく、システム、装置、集積回路、コンピュータプログラムおよび記録媒体の任意な組み合わせで実現されてもよい。

10

【発明の効果】

【 0 0 0 8 】

本発明の制御方法は、情報管理システムにおいて、個人のデータの利用の際に発生し得る通信を抑制することができる。

【図面の簡単な説明】

【 0 0 0 9 】

【図 1】図 1 は、実施の形態における情報管理システムの構成を模式的に示すブロック図である。

20

【図 2】図 2 は、実施の形態におけるサーバの構成を模式的に示すブロック図である。

【図 3】図 3 は、実施の形態における登録トランザクションデータのデータ構造を模式的に示す説明図である。

【図 4】図 4 は、実施の形態における利用要求トランザクションデータのデータ構造を模式的に示す説明図である。

【図 5】図 5 は、実施の形態における提供トランザクションデータのデータ構造を模式的に示す説明図である。

【図 6】図 6 は、実施の形態における利用制限トランザクションデータのデータ構造を模式的に示す説明図である。

【図 7】図 7 は、実施の形態における削除トランザクションデータのデータ構造を模式的に示す説明図である。

30

【図 8】図 8 は、実施の形態におけるトークン付与トランザクションデータのデータ構造を模式的に示す説明図である。

【図 9】図 9 は、実施の形態におけるサーバが実行するユーザ情報の登録に係る処理を示すフロー図である。

【図 10】図 10 は、実施の形態における、ユーザ情報の登録に係る情報管理システム全体の処理を示すシーケンス図である。

【図 11】図 11 は、実施の形態におけるサーバが実行するユーザ情報の利用要求に係る処理を示すフロー図である。

【図 12】図 12 は、実施の形態におけるサーバが実行するユーザ情報の提供に係る処理を示すフロー図である。

40

【図 13】図 13 は、実施の形態における、ユーザ情報の利用要求および提供に係る情報管理システム全体の処理を示すシーケンス図である。

【図 14】図 14 は、実施の形態におけるサーバが実行するデータの利用制限に係る処理を示すフロー図である。

【図 15】図 15 は、実施の形態における、ユーザ情報の利用制限に係る情報管理システム全体の処理を示すシーケンス図である。

【図 16】図 16 は、実施の形態におけるサーバが実行するユーザ情報の削除に係る処理を示すフロー図である。

【図 17】図 17 は、実施の形態における、ユーザ情報の削除に係る情報管理システム全

50

体の処理を示すシーケンス図である。

【図 18】図 18 は、実施の形態の変形例におけるサーバの処理を示すフロー図である。

【図 19】図 19 は、実施の形態の変形例におけるサーバの構成を模式的に示すブロック図である。

【図 20】図 20 は、ブロックチェーンのデータ構造を示す説明図である。

【図 21】図 21 は、トランザクションデータのデータ構造を示す説明図である。

【発明を実施するための形態】

【0010】

(本発明の基礎となった知見)

本発明者は、「背景技術」の欄において記載した、情報銀行に関する技術に関し、以下の問題が生じることを見出した。

【0011】

情報銀行は、個人のデータを管理するとともに、そのデータを第三者に提供する機能を有する。情報銀行は、個人のデータの活用に関する契約を個人との間で結び、個人のデータを管理するとともに、第三者に提供する事業である。

【0012】

情報銀行に管理されている個人のデータの利用の都度に当該個人と情報銀行との間で利用の承諾に関わる情報交換のための通信が発生し得る。そのため、情報銀行に管理されるデータが多くなると通信量が増大し得るという問題がある。

【0013】

そこで、本発明は、情報管理システムにおいて、個人のデータの利用の際に発生し得る通信を抑制する制御方法などを提供する。

【0014】

このような問題を解決するために、本発明の一態様に係る制御方法は、分散台帳を保有している複数のサーバを備える情報管理システムにおいて、当該複数のサーバのうちの一のサーバが実行する制御方法であって、前記情報管理システムにより管理されているユーザ情報であって、第一ユーザに関する情報であるユーザ情報に対応付けられた識別情報と、前記ユーザ情報の第二ユーザへの提供の可否を示す可否情報とを含む第一トランザクションデータを受信し、受信した前記第一トランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する。

【0015】

上記態様によれば、サーバは、情報管理システムにより管理されているユーザ情報の利用に関する可否情報が含まれた第一トランザクションデータを分散台帳に格納する。そのため、サーバは、個人のデータの利用の都度に利用の承諾に関わる情報交換をする必要がなくなり、当該情報交換のための通信を抑制することができる。

【0016】

また、分散台帳に格納されたトランザクションデータの改ざんが実質的に不可能であることから、情報管理システムにより管理されているユーザ情報の利用に関する可否情報が適切に管理される。仮に、利用の承諾についての情報交換において個人と情報銀行との間、または、個人のデータを利用する企業と情報銀行との間で齟齬があると、個人のデータが適切に利用されるとはいえない。本発明の一態様に係る制御方法によれば、可否情報が分散台帳に格納され、改ざんが実質的に不可能となるので、上記の齟齬が生ずることが抑制される効果もある。

【0017】

例えば、前記制御方法は、さらに、前記識別情報、又は、前記第一ユーザが属する属性を示す属性情報を含み、前記識別情報または前記属性情報に適合する前記ユーザ情報の利用を求めることを示す第二トランザクションデータを前記第二ユーザの端末から受信し、受信した前記第二トランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する。

【0018】

10

20

30

40

50

上記態様によれば、サーバは、情報管理システムにより管理されているユーザ情報の利用を求めると示す第二ランザクションデータを分散台帳に格納する。そのため、利用の要求がなされたという事実を示す情報が、実質的に改ざんされることなく適切に管理される。よって、サーバは、ユーザ情報の利用の求めがあったという事実を示す情報を適切に管理しながら、個人のデータの利用の際に発生し得る通信を抑制することができる。

【0019】

例えば、前記ユーザ情報は、1以上のユーザ情報を含み、前記許否情報は、前記1以上のユーザ情報のうち、前記第二ユーザへの提供が許可されるユーザ情報の条件を含み、前記第二ランザクションデータは、さらに、前記識別情報に対応付けられた前記第一ユーザ、又は、前記属性情報により示される前記属性に属する前記第一ユーザに関するユーザ情報であって、前記第二ユーザが提供を求めるユーザ情報を示す要求情報を含み、前記制御方法は、さらに、前記第二ランザクションデータに含まれる前記要求情報が、前記許否情報に含まれる前記条件に適合するか否かを判定し、前記要求情報が前記条件に適合すると判定した場合に限り、受信した前記第二ランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する。

10

【0020】

上記態様によれば、サーバは、第二ユーザによって利用を求められたユーザ情報について、許否情報に含まれる条件に基づいて利用を許可するか否かを判定する。許否情報は、第一ユーザの判断に基づいて生成され分散台帳に格納されたものであるため、実質的に改ざんされることなく適切に管理されている。よって、サーバは、第一ユーザによる判断に従ってユーザ情報を第二ユーザに利用させる際に、個人のデータの利用の際に発生し得る通信を抑制することができる。

20

【0021】

例えば、前記制御方法は、さらに、前記第二ランザクションデータを受信したことに基づいて、前記第二ユーザの端末に前記ユーザ情報が送信された場合に、送信された前記ユーザ情報に係る前記識別情報又は前記属性情報を含む第三ランザクションデータを受信し、受信した前記第三ランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する。

【0022】

上記態様によれば、サーバは、第二ユーザにユーザ情報を送信したことを示す第三ランザクションデータを分散台帳に格納する。そのため、第二ユーザにユーザ情報を送信したという事実を示す情報が、実質的に改ざんされることなく適切に管理される。よって、サーバは、第二ユーザにユーザ情報を送信したという事実を示す情報を適切に管理しながら、個人のデータの利用の際に発生し得る通信を抑制することができる。また、第一ユーザが、自身のユーザ情報がどの企業によってどのように利用されたかを知ることができる利点がある。

30

【0023】

例えば、前記制御方法は、さらに、前記第二ユーザの端末に前記ユーザ情報が送信されてから所定時間が経過した場合に、提供された前記ユーザ情報の利用が制限されることを示す制限情報を含む第四ランザクションデータを受信し、受信した前記第四ランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する。

40

【0024】

上記態様によれば、サーバは、第二ユーザにユーザ情報を提供してから所定時間が経過したことによって、提供したユーザ情報の利用の制限がなされたことを示す第四ランザクションデータを分散台帳に格納する。そのため、利用制限がなされたという事実を示す情報が、実質的に改ざんされることなく適切に管理される。よって、サーバは、ユーザ情報の利用制限がなされたという事実を示す情報を適切に管理しながら、個人のデータの利用の際に発生し得る通信を抑制することができる。

【0025】

例えば、前記制御方法は、さらに、前記情報管理システムにおいて管理されていて削除

50

されたユーザ情報を示す識別子と、前記ユーザ情報が削除されたことを示す削除情報とを含む第五トランザクションデータを受信し、受信した前記第五トランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する。

【0026】

上記態様によれば、サーバは、ユーザ情報が削除されたことを示す第五トランザクションデータを分散台帳に格納する。そのため、ユーザ情報が削除されたという事実を示す情報が、実質的に改ざんされることなく適切に管理される。よって、サーバは、ユーザ情報が削除されたという事実を示す情報を適切に管理しながら、個人のデータの利用の際に発生し得る通信を抑制することができる。

【0027】

例えば、前記第一トランザクションデータを受信したときには、前記第一ユーザにトークンを付与する提供情報を含む第六トランザクションデータを取得し、取得した前記第六トランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する。

【0028】

上記態様によれば、サーバは、ユーザ情報の提供の許否情報が分散台帳に格納された第一ユーザにトークンを付与する。トークンは、分散台帳によって管理される価値情報であり、例えば金銭の価値の代替として用いられ得る。これにより、情報管理システムによってユーザ情報を管理することが促進され、管理対象であるユーザ情報の活用が促進される効果がある。

【0029】

例えば、前記許否情報は、前記ユーザ情報の提供を許可する期間、前記ユーザ情報の提供が許可されるユーザ、又は、前記ユーザ情報の再提供の許否を示す情報を含む。

【0030】

上記態様によれば、サーバは、ユーザ情報の提供を許可する期間、ユーザ情報の提供が許可されるユーザ、又は、ユーザ情報の再提供の許否を示す情報を、実質的に改ざんされることなく適切に管理する。これにより、サーバは、個人のデータの利用の都度に利用の承諾に関わる上記の情報の交換をする必要がなくなり、当該情報交換のための通信を抑制することができる。

【0031】

例えば、前記1以上のユーザ情報のそれぞれには、当該ユーザ情報の種別を示す種別情報が紐付けられており、前記許否情報は、前記ユーザ情報の提供を許可する種別情報を含む。

【0032】

上記態様によれば、サーバは、ユーザ情報の提供を許可する種別情報を、実質的に改ざんされることなく適切に管理する。これにより、サーバは、個人のデータの利用の都度に利用の承諾に関わる上記の情報の交換をする必要がなくなり、当該情報交換のための通信を抑制することができる。

【0033】

また、本発明の一態様に係るサーバは、分散台帳を保有している複数のサーバを備える情報管理システムにおいて、当該複数のサーバのうちの一のサーバであって、前記情報管理システムにより管理されているユーザ情報であって、第一ユーザに関する情報であるユーザ情報に対応付けられた識別情報と、前記ユーザ情報の第二ユーザへの提供の許否を示す許否情報とを含む第一トランザクションデータを受信し、受信した前記第一トランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する処理部を備える。

【0034】

上記態様により、上記制御方法と同様の効果を奏する。

【0035】

また、本発明の一態様に係るプログラムは、上記の制御方法をコンピュータに実行させるためのプログラムである。

10

20

30

40

50

## 【 0 0 3 6 】

上記態様により、上記制御方法と同様の効果を奏する。

## 【 0 0 3 7 】

また、本発明の一態様に係るデータ構造は、分散台帳を保有している複数のサーバを備える情報管理システムにおいて分散台帳に記録されるデータ構造であって、前記データ構造は、前記情報管理システムにより管理されているユーザ情報であって、第一ユーザに関する情報であるユーザ情報に対応付けられた識別情報と、前記ユーザ情報の第二ユーザへの提供の許否を示す許否情報とを含む第一トランザクションデータを含み、前記第一トランザクションデータは、前記複数のサーバそれぞれが備える前記分散台帳に記録される、データ構造である。

10

## 【 0 0 3 8 】

なお、これらの包括的または具体的な態様は、システム、装置、集積回路、コンピュータプログラムまたはコンピュータ読み取り可能なCD-ROMなどの記録媒体で実現されてもよく、システム、装置、集積回路、コンピュータプログラムまたは記録媒体の任意な組み合わせで実現されてもよい。

## 【 0 0 3 9 】

以下、実施の形態について、図面を参照しながら具体的に説明する。

## 【 0 0 4 0 】

なお、以下で説明する実施の形態は、いずれも包括的または具体的な例を示すものである。以下の実施の形態で示される数値、形状、材料、構成要素、構成要素の配置位置及び接続形態、ステップ、ステップの順序などは、一例であり、本発明を限定する主旨ではない。また、以下の実施の形態における構成要素のうち、最上位概念を示す独立請求項に記載されていない構成要素については、任意の構成要素として説明される。

20

## 【 0 0 4 1 】

(実施の形態)

本実施の形態において、情報管理システムにおいて、個人のデータの利用の際に発生し得る通信を抑制する制御方法などについて説明する。

## 【 0 0 4 2 】

図1は、本実施の形態における情報管理システム1の構成を模式的に示すブロック図である。

30

## 【 0 0 4 3 】

図1に示されるように、情報管理システム1は、サーバ10A、10B及び10Cと、管理サーバ20と、鍵管理装置30とを備える。情報管理システム1が備える各装置及びサーバは、ネットワークNを介して互いに通信可能に接続されている。ネットワークNは、どのような通信回線又はネットワークから構成されてもよく、例えば、インターネット、携帯電話のキャリアネットワークなどを含む。サーバ10A、10B及び10Cを「サーバ10A等」ともいう。

## 【 0 0 4 4 】

また、情報管理システム1には、ネットワークNを介して、ユーザU1の端末41と、ユーザU2の端末42とが接続されている。

40

## 【 0 0 4 5 】

サーバ10Aは、情報管理システム1によってなされる情報管理に関する記録を行う複数のサーバ10A、10B及び10Cのうちの一つである。サーバ10Aは、分散台帳を保有している複数のサーバ10A、10B及び10Cのうちの一つである。サーバ10Aが保有している分散台帳には、情報管理システム1によって管理されている情報の登録、利用要求、提供、利用制限および削除、ならびに、トークン付与に関する各種トランザクションデータが格納される。

## 【 0 0 4 6 】

サーバ10B及び10Cは、それぞれ、サーバ10Aと同じ機能を有する装置であり、サーバ10Aとは独立に動作する。なお、サーバの台数は、3に限られず、複数であれば

50

よい。また、サーバ10A等とは、通信可能に接続されており、ネットワークNを介して接続されていてもよい。

【0047】

なお、ここでは、サーバ10Aが各種トランザクションデータまたは各種情報の送受信を行う場合を例として説明するが、サーバ10Bまたは10Cが行ってもよい。

【0048】

管理サーバ20は、ユーザ情報の管理をする情報管理サーバである。管理サーバ20は、ユーザU1の端末41からユーザ情報の提供を受け、提供されたユーザ情報を保有している。管理サーバ20は、一般の情報銀行に相当する。

【0049】

管理サーバ20は、保有しているユーザ情報についてユーザU2から利用の要求がなされたときには、その要求に応じてユーザ情報をユーザU2の端末42に提供する。管理サーバ20は、ユーザ情報をユーザU2の端末42に提供してから所定時間が経過すると、提供したユーザ情報の利用を制限する。管理サーバ20は、管理しているユーザ情報について削除の指示を受けたときには、当該ユーザ情報を削除する。管理サーバ20は、ユーザ情報をユーザU2の端末42に提供するときには、ユーザ情報を暗号化する。暗号化に用いられる鍵は、鍵管理装置30により提供される。

【0050】

鍵管理装置30は、データの暗号化および復号に用いる鍵情報を生成して提供する鍵管理装置である。具体的には、鍵管理装置30は、ユーザ情報が管理サーバ20からユーザU2の端末42に提供されるときに、暗号化鍵と復号鍵とをペアで生成し、生成した暗号化鍵を管理サーバ20に提供するとともに、生成した復号鍵をユーザU2の端末42に提供する。なお、暗号化鍵と復号鍵とは同一であってもよい。

【0051】

端末41は、ユーザU1が保有する端末装置である。ユーザU1は、情報管理システム1に自身のユーザ情報を登録するユーザの一例である。ここで、ユーザ情報とは、ユーザU1の個人情報（すなわち、氏名、生年月日または住所などユーザU1の個人を特定し得る情報）、並びに、パーソナルデータ（すなわち、移動履歴または購買履歴などユーザU1と関係を有するデータ）を含む電子データである。端末41は、ユーザU1のユーザ情報を管理サーバ20に登録し、その登録がなされたという事実を示す情報がサーバ10A等によって管理される。端末41は、ユーザ情報とともに、そのユーザ情報の利用条件を管理サーバ20に登録してもよい。端末41は、例えばパーソナルコンピュータ、スマートフォンまたはタブレットなどである。

【0052】

端末42は、ユーザU2が保有する端末装置である。ユーザU2は、情報管理システム1により管理されているユーザ情報を利用するユーザの一例であり、個人であることもあるし、企業などの団体であることもある。端末42は、ユーザU1のユーザ情報を管理サーバ20から提供される。端末42によるユーザ情報の利用の要求、又は、提供があったことがサーバ10A等によって管理される。端末42が取得したユーザ情報は、例えば、ユーザU2によって、認証またはデータ分析などのために利用されることが想定される。端末42は、例えばパーソナルコンピュータ、スマートフォンまたはタブレットなどである。

【0053】

以降において、情報管理システム1が備えるサーバ10A等の構成について詳細に説明する。

【0054】

図2は、本実施の形態におけるサーバ10Aの構成を模式的に示すブロック図である。

【0055】

図2に示されるように、サーバ10Aは、処理部11と、台帳管理部12と、制御部13とを備える。サーバ10Aが備える上記機能部は、例えばCPU（Central Processing

10

20

30

40

50

Unit) がメモリを用いてプログラムを実行することで実現され得る。

【0056】

処理部11は、分散台帳によって各種情報の管理を行う処理部である。処理部11は、情報管理システム1内の装置からトランザクションデータを受信した、又は、制御部13が生成したトランザクションデータを取得した場合に、受信又は取得したトランザクションデータを台帳管理部12に提供することで分散台帳に格納する。トランザクションデータには、ユーザ情報の登録、利用要求、提供、利用制限および削除、ならびに、トークン付与に関する各種トランザクションデータが含まれる。各種トランザクションデータについては後で詳しく説明する。

【0057】

台帳管理部12は、分散台帳を管理している処理部である。台帳管理部12は、処理部11から提供されたトランザクションデータを分散台帳に格納する。分散台帳には、過去から現在までのトランザクションデータが格納される。分散台帳に記録された情報の改ざんが困難であるという特性に基づいて、上記トランザクションデータが改ざんされないように管理されている。

【0058】

台帳管理部12は、格納部17と、台帳記憶部18とを有する。

【0059】

格納部17は、分散台帳に格納すべき新しいトランザクションデータを台帳記憶部18に格納する処理部である。格納部17は、分散台帳の種別に応じた方式で新しいトランザクションデータを台帳記憶部18に格納する。また、格納部17は、サーバ10A等のうちの他のサーバの格納部17と通信データを送受信し、他のサーバの台帳記憶部18にも上記新しいトランザクションデータを格納させる。例えば、格納部17は、分散台帳がブロックチェーンである場合には、新しいトランザクションデータを含むブロックを生成し、生成したブロックをサーバ10A等の間で同期をとったうえで、上記ブロックを台帳記憶部18に格納する。

【0060】

台帳記憶部18は、分散台帳を記憶している記憶装置である。台帳記憶部18に格納されている分散台帳は、1以上のトランザクションデータを記憶しており、ハッシュ値などの特性を用いて改ざんが困難であるように管理されている(後述)。

【0061】

なお、分散台帳は、例えばブロックチェーンであり、この場合を例として説明するが、他の方式の分散台帳(例えば、IOTA又はハッシュグラフ等)を採用することも可能である。なお、分散台帳は、新しいデータの格納の際にコンセンサスアルゴリズム(例えば、PBFT(Practical Byzantine Fault Tolerance)、PoW(Proof of Work)又はPoS(Proof of Stake))を実行するものであってもよいし、実行しないものであってもよい。コンセンサスアルゴリズムを実行しない分散台帳技術の一例としてHyperledger fabricがある。

【0062】

制御部13は、各種の情報処理を制御する処理部である。具体的には、制御部13は、登録トランザクションデータを受信した場合に、登録トランザクションデータに含まれるユーザ情報の整合の検証の処理を実行する。また、制御部13は、利用要求トランザクションデータを受信した場合に、利用要求が利用条件を満たすか否かについて判定の処理を実行する。

【0063】

以降において、処理部11が分散台帳に格納する各種トランザクションデータである、(1)登録トランザクションデータ、(2)利用要求トランザクションデータ、(3)提供トランザクションデータ、(4)利用制限トランザクションデータ、(5)削除トランザクションデータ、および、(6)トークン付与トランザクションデータについて説明す

10

20

30

40

50

る。

【 0 0 6 4 】

( 1 ) 登録トランザクションデータ

図 3 は、本実施の形態における登録トランザクションデータのデータ構造を模式的に示す説明図である。登録トランザクションデータは、ユーザ U 1 がユーザ情報を管理サーバ 2 0 に登録したという事実を示すトランザクションデータである。登録トランザクションデータは、ユーザ U 1 がユーザ情報を管理サーバ 2 0 に登録したときに、管理サーバ 2 0 によって生成され、サーバ 1 0 A 等に送信される。

【 0 0 6 5 】

登録トランザクションデータは、ユーザ U 1 に関する情報であるユーザ情報に対応付けられた識別情報と、ユーザ情報のユーザ U 2 への提供の許否を示す許否情報とを含む第一トランザクションデータに相当する。

10

【 0 0 6 6 】

許否情報は、例えば、ユーザ情報の提供を許可する期間、ユーザ情報の提供が許可されるユーザ U 2、又は、ユーザ情報の再提供の許否を示す情報を含む。また、ユーザ情報のそれぞれに、当該ユーザ情報の種別を示す種別情報が紐付けられている場合には、許否情報は、ユーザ情報の提供を許可する種別情報を含んでもよい。

【 0 0 6 7 】

以降では、許否情報が、ユーザ情報の提供を許可する種別情報を含む場合を例として説明する。

20

【 0 0 6 8 】

図 3 に示されるように、登録トランザクションデータは、トランザクション ID と、情報アドレスと、利用条件と、生成日時と、署名とを含む。

【 0 0 6 9 】

トランザクション ID は、当該登録トランザクションデータを一意に特定し得る識別子である。

【 0 0 7 0 】

情報アドレスは、管理サーバ 2 0 に登録されたユーザ情報のアドレスを示す情報である。情報アドレスは、ユーザ情報に対応付けられた識別情報に相当する。

【 0 0 7 1 】

利用条件は、管理サーバ 2 0 に登録されたユーザ情報の利用の条件を示す情報である。利用条件は、例えば、管理サーバ 2 0 に登録されたユーザ情報のうち、ユーザ U 2 への提供が許可されるユーザ情報の種別を示す条件である。利用条件は、上記種別情報に相当し、単に条件ともいう。

30

【 0 0 7 2 】

生成日時は、当該登録トランザクションデータが生成された日時を示す情報である。

【 0 0 7 3 】

署名は、当該登録トランザクションデータを生成した装置又は人が付した電子署名である。

【 0 0 7 4 】

図 3 に示される登録トランザクションデータは、トランザクション ID が「 a 0 0 1 」であり、アドレス「 a d d 1 」にユーザ情報が登録されたことを示している。また、登録されたユーザ情報のうち、「住所と氏名を利用可」という利用条件が設定されている。生成日時は、「 2 0 1 8 年 1 0 月 1 0 日 1 5 時 0 0 分 0 0 秒」であり、署名は、管理サーバ 2 0 の電子署名である。

40

【 0 0 7 5 】

( 2 ) 利用要求トランザクションデータ

図 4 は、本実施の形態における利用要求トランザクションデータのデータ構造を模式的に示す説明図である。利用要求トランザクションデータは、ユーザ U 2 がユーザ情報を利用することを求めたという事実を示すトランザクションデータである。利用要求トランザ

50

クシオンデータは、ユーザU 2がユーザ情報を利用するための利用要求を送信するときに、ユーザU 2の端末4 2によって生成され、サーバ1 0 A等に送信される。

【0 0 7 6】

利用要求トランザクションデータは、識別情報、又は、ユーザU 1が属する属性を示す属性情報を含み、識別情報または属性情報に適合するユーザ情報の利用を求めことを示す第二トランザクションデータに相当する。

【0 0 7 7】

図4に示されるように、利用要求トランザクションデータは、トランザクションIDと、利用者IDと、情報アドレスと、利用内容と、生成日時と、署名とを含む。

【0 0 7 8】

トランザクションIDは、当該利用要求トランザクションデータを一意に特定し得る識別子である。

【0 0 7 9】

利用者IDは、ユーザ情報を利用する利用者を一意に特定し得る識別子である。

【0 0 8 0】

情報アドレスは、管理サーバ2 0に登録されたユーザ情報であって、利用者が利用を求めるユーザ情報のアドレスを示す情報である。なお、情報アドレスの代わりに、ユーザU 1が属する属性を示す属性情報を用いることもできる。属性情報とは、例えば、年代(2 0代、3 0代、4 0代など)、性別または住所の都道府県などである。以降でも同様とする。

【0 0 8 1】

利用内容は、利用者が利用を求めるユーザ情報の内容を示す情報である。利用内容は、例えば、ユーザ情報が1以上存在する場合には、1以上のユーザ情報のうち利用を求めるユーザ情報を示す情報である。

【0 0 8 2】

生成日時は、当該利用要求トランザクションデータが生成された日時を示す情報である。

【0 0 8 3】

署名は、当該利用要求トランザクションデータを生成した装置又は人が付した電子署名である。

【0 0 8 4】

図4に示される利用要求トランザクションデータは、トランザクションIDが「b 0 0 1」であり、アドレス「a d d 1」に登録されているユーザ情報のうち、「住所と氏名」の情報の利用を利用者「u 0 0 2」が求めていることを示している。生成日時は、「2 0 1 8年1 1月1 1日 1 6時0 0分0 0秒」であり、署名は、ユーザU 2の電子署名である。ここで、ユーザU 2の利用者IDを「u 0 0 2」とした。

【0 0 8 5】

(3) 提供トランザクションデータ

図5は、本実施の形態における提供トランザクションデータのデータ構造を模式的に示す説明図である。提供トランザクションデータは、管理サーバ2 0からユーザU 2にユーザ情報を提供したという事実を示すトランザクションデータである。提供トランザクションデータは、管理サーバ2 0からユーザU 2にユーザ情報を提供したときに、管理サーバ2 0によって生成され、サーバ1 0 A等に送信される。

【0 0 8 6】

提供トランザクションデータは、管理サーバ2 0からユーザU 2の端末4 2にユーザ情報が送信された場合に、送信されたユーザ情報に係る識別情報又は属性情報と、種別情報とを含む第三トランザクションデータに相当する。

【0 0 8 7】

図5に示されるように、提供トランザクションデータは、トランザクションIDと、利用者IDと、情報アドレスと、提供内容と、生成日時と、署名とを含む。

【0 0 8 8】

10

20

30

40

50

トランザクションIDは、当該提供トランザクションデータを一意に特定し得る識別子である。

【0089】

利用者IDは、ユーザ情報を提供した宛先である利用者を一意に特定し得る識別子である。

【0090】

情報アドレスは、管理サーバ20に登録されたユーザ情報であって、管理サーバ20が利用者に提供したユーザ情報のアドレスを示す情報である。

【0091】

提供内容は、管理サーバ20が利用者に提供したユーザ情報の内容を示す情報である。提供内容は、例えば、ユーザ情報が1以上存在する場合には、1以上のユーザ情報のうち利用者に提供したユーザ情報を示す情報である。

10

【0092】

生成日時は、当該提供トランザクションデータが生成された日時を示す情報である。

【0093】

署名は、当該提供トランザクションデータを生成した装置又は人が付した電子署名である。

【0094】

図5に示される提供トランザクションデータは、トランザクションIDが「c001」であり、アドレス「add1」に登録されているユーザ情報のうち、「住所と氏名」のユーザ情報を利用者「u002」に提供したことを示している。生成日時は、「2018年11月11日 17時00分00秒」であり、署名は、管理サーバ20の電子署名である。

20

【0095】

#### (4) 利用制限トランザクションデータ

図6は、本実施の形態における利用制限トランザクションデータのデータ構造を模式的に示す説明図である。利用制限トランザクションデータは、ユーザU2に提供されたユーザ情報の利用が制限されるという事実を示すトランザクションデータである。利用制限トランザクションデータは、管理サーバ20からユーザU2にユーザ情報を提供してから所定時間経過したことによって、提供されたユーザ情報の利用を制限するとき、管理サーバ20によって生成され、サーバ10A等へ送信される。

30

【0096】

利用制限トランザクションデータは、提供されたユーザ情報の利用が制限されることを示す制限情報を含む第四トランザクションデータに相当する。

【0097】

図6に示されるように、利用制限トランザクションデータは、トランザクションIDと、利用者IDと、情報アドレスと、制限内容と、生成日時と、署名とを含む。

【0098】

トランザクションIDは、当該利用制限トランザクションデータを一意に特定し得る識別子である。

【0099】

利用者IDは、ユーザ情報を提供した宛先である利用者を一意に特定し得る識別子である。

40

【0100】

情報アドレスは、管理サーバ20が利用者に提供したユーザ情報であって、利用が制限されるユーザ情報のアドレスを示す情報である。

【0101】

制限内容は、利用が制限されるユーザ情報の内容を示す情報である。制限内容は、例えば、ユーザ情報が1以上存在する場合には、1以上のユーザ情報のうち利用が制限されるユーザ情報を示す情報である。制限内容は、制限情報に相当する。

【0102】

50

生成日時は、当該利用制限トランザクションデータが生成された日時を示す情報である。

【0103】

署名は、当該利用制限トランザクションデータを生成した装置又は人が付した電子署名である。

【0104】

なお、ユーザ情報の情報アドレスと制限内容とを指定する代わりに、当該ユーザ情報が提供されたときの提供トランザクションデータのトランザクションID（図6参照）を指定してもよい。

【0105】

図6に示される利用制限トランザクションデータは、トランザクションIDが「d001」であり、アドレス「add1」に登録されているユーザ情報のうち、利用者「u002」に提供された「住所と氏名」のユーザ情報の利用が制限されることを示している。生成日時は、「2019年5月11日 17時00分00秒」であり、署名は、管理サーバ20の電子署名である。

10

【0106】

(5) 削除トランザクションデータ

図7は、本実施の形態における削除トランザクションデータのデータ構造を模式的に示す説明図である。削除トランザクションデータは、管理サーバ20に登録されたユーザ情報が削除されたという事実を示すトランザクションデータである。削除トランザクションデータは、管理サーバ20に登録されたユーザ情報が削除されたときに、管理サーバ20によって生成され、サーバ10A等に送信される。

20

【0107】

削除トランザクションデータは、情報管理システム1において管理されていて削除されたユーザ情報を示す識別子と、ユーザ情報が削除されたことを示す削除情報とを含む第五トランザクションデータに相当する。

【0108】

図7に示されるように、削除トランザクションデータは、トランザクションIDと、情報アドレスと、削除情報と、生成日時と、署名とを含む。

【0109】

トランザクションIDは、当該削除トランザクションデータを一意に特定し得る識別子である。

30

【0110】

情報アドレスは、管理サーバ20に登録されていて、削除されたユーザ情報のアドレスを示す情報である。

【0111】

削除情報は、当該削除トランザクションデータがユーザ情報の削除に係ることを示す情報である。

【0112】

生成日時は、当該削除トランザクションデータが生成された日時を示す情報である。

【0113】

署名は、当該削除トランザクションデータを生成した装置又は人が付した電子署名である。

40

【0114】

図7に示される削除トランザクションデータは、トランザクションIDが「e001」であり、アドレス「add1」に登録されていたユーザ情報が削除されたことを示している。生成日時は、「2019年5月11日 17時00分00秒」であり、署名は、管理サーバ20の電子署名である。

【0115】

(6) トークン付与トランザクションデータ

図8は、本実施の形態におけるトークン付与トランザクションデータのデータ構造を模

50

式的に示す説明図である。トークン付与トランザクションデータは、ユーザ間でのトークンの授受を示すトランザクションデータであり、ユーザ情報を提供したユーザU1へのトークンの付与に用いられる。トークン付与トランザクションデータは、管理サーバ20にユーザ情報が登録されたときに、管理サーバ20によって生成され、サーバ10A等へ送信される。

【0116】

トークン付与トランザクションデータは、第一ユーザにトークンを付与する提供情報を含む第六トランザクションデータに相当する。

【0117】

図8に示されるように、トークン付与トランザクションデータは、トランザクションIDと、提供元アドレスと、提供先アドレスと、生成日時と、署名とを含む。提供元アドレスと提供先アドレスとは、提供情報に相当する。

10

【0118】

トランザクションIDは、当該トークン付与トランザクションデータを一意に特定し得る識別子である。

【0119】

提供元アドレスは、トークン付与において、トークンを提供する元（つまり提供元）であるユーザを示すアドレスを示す情報である。提供元は、例えば、管理サーバ20である。

【0120】

提供先アドレスは、トークン付与において、トークンを提供する先（つまり提供先）であるユーザを示すアドレスを示す情報である。提供先は、例えば、ユーザU1である。

20

【0121】

生成日時は、当該トークン付与トランザクションデータが生成された日時を示す情報である。

【0122】

署名は、当該トークン付与トランザクションデータを生成した装置又は人が付した電子署名である。

【0123】

図8に示されるトークン付与トランザクションデータは、トランザクションIDが「f001」であり、提供元アドレス「add5」に示されるユーザ（例えば管理サーバ20）から、提供先アドレス「add6」に示されるユーザ（例えば、ユーザU1）にトークン付与が行われることを示している。生成日時は、「2018年10月10日 15時00分00秒」であり、署名は、管理サーバ20の電子署名である。

30

【0124】

以上のように構成されたサーバ10A等および情報管理システム1の処理を以下で説明する。

【0125】

以降において、(1)ユーザ情報の登録、(2)ユーザ情報の利用要求と提供、(3)ユーザ情報の利用制限、および(4)ユーザ情報の削除の際の処理について順に説明する。

【0126】

(1)ユーザ情報の登録

図9は、本実施の形態におけるサーバ10A等が実行するユーザ情報の登録に係る処理を示すフロー図である。

40

【0127】

ステップS101において、処理部11は、管理サーバ20から登録トランザクションデータを受信したか否かを判定する。登録トランザクションデータを受信したと判定した場合（ステップS101でYes）には、ステップS102に進み、そうでない場合（ステップS101でNo）には、ステップS101を再び実行する。つまり、処理部11は、登録トランザクションデータを受信するまでステップS101で待機状態をとる。

【0128】

50

ステップ S 1 0 2 において、制御部 1 3 は、利用条件の整合性の検証を行う。具体的には、制御部 1 3 は、ステップ S 1 0 1 で受信した登録トランザクションデータに含まれる利用条件が、ユーザ U 1 のユーザ情報に対してユーザ U 1 が設定した利用条件と整合しているか否かを検証する。

【 0 1 2 9 】

ステップ S 1 0 3 において、制御部 1 3 は、ステップ S 1 0 2 において、利用条件の整合性の検証が成功したか否かを判定する。検証が成功した場合（ステップ S 1 0 3 で Y e s ）には、ステップ S 1 0 4 に進み、そうでない場合（ステップ S 1 0 3 で N o ）には、ステップ S 1 1 1 に進む。

【 0 1 3 0 】

ステップ S 1 0 4 において、制御部 1 3 は、ステップ S 1 0 1 で受信した登録トランザクションデータを台帳管理部 1 2 に提供することで、分散台帳に格納する。また、制御部 1 3 は、上記登録トランザクションデータを他のサーバ 1 0 B 等に送信し、すべてのサーバ 1 0 A 等の分散台帳に格納させる。

【 0 1 3 1 】

ステップ S 1 0 5 において、制御部 1 3 は、管理サーバ 2 0 からユーザ U 1 に対してトークンを付与するためのトークン付与トランザクションデータを生成する。

【 0 1 3 2 】

ステップ S 1 0 6 において、制御部 1 3 は、ステップ S 1 0 5 で生成したトークン付与トランザクションデータを台帳管理部 1 2 に提供することで、分散台帳に格納する。また、制御部 1 3 は、上記トークン付与トランザクションデータを他のサーバ 1 0 B 等に送信し、すべてのサーバ 1 0 A 等の分散台帳に格納させる。

【 0 1 3 3 】

ステップ S 1 1 1 において、制御部 1 3 は、利用条件の整合性の検証が成功しなかった（つまり失敗した）ことを示す情報を含めたトランザクションデータ（不図示）を生成する。

【 0 1 3 4 】

ステップ S 1 1 2 において、制御部 1 3 は、ステップ S 1 1 1 で生成したトランザクションデータを台帳管理部 1 2 に提供することで、分散台帳に格納する。また、制御部 1 3 は、上記トークン付与トランザクションデータを他のサーバ 1 0 B 等に送信し、すべてのサーバ 1 0 A 等の分散台帳に格納させる。

【 0 1 3 5 】

ステップ S 1 0 6 又は S 1 1 2 を終えたら、図 9 に示される一連の処理を終了する。

【 0 1 3 6 】

図 1 0 は、本実施の形態における、ユーザ情報の登録に係る情報管理システム 1 全体の処理を示すシーケンス図である。なお、図 1 0 において、図 9 のフロー図と同じ処理を示すものは、図 9 と同じ符号を付し詳細な説明を省略する。なお、図 1 0 では、利用条件の整合性の検証が成功する場合（図 9 のステップ S 1 0 3 で Y e s ）を示している。

【 0 1 3 7 】

ステップ S 1 3 1 において、端末 4 1 は、ユーザ U 1 による操作に基づいてユーザ U 1 のユーザ情報を、その利用条件とともに管理サーバ 2 0 に送信する。管理サーバ 2 0 は、端末 4 1 からユーザ情報及び利用条件を受信する。

【 0 1 3 8 】

ステップ S 1 4 1 において、管理サーバ 2 0 は、端末 4 1 から受信したユーザ情報と利用条件とを、管理対象の情報として登録する。

【 0 1 3 9 】

ステップ S 1 4 2 において、管理サーバ 2 0 は、ユーザ情報を登録したことを示す登録トランザクションデータを生成し、生成した登録トランザクションデータをサーバ 1 0 A 等に送信する。

【 0 1 4 0 】

10

20

30

40

50

この後、サーバ10A等は、ステップS142で送信された登録トランザクションデータを受信し、登録トランザクションデータの分散台帳への格納およびトークンの付与等の処理を行う(ステップS101~S112)。

【0141】

(2) ユーザ情報の利用要求と提供

図11は、本実施の形態におけるサーバ10A等が実行するユーザ情報の利用要求に係る処理を示すフロー図である。

【0142】

ステップS201において、処理部11は、ユーザU2の端末42から利用要求トランザクションデータを受信したか否かを判定する。利用要求トランザクションデータを受信したと判定した場合(ステップS201でYes)には、ステップS202に進み、そうでない場合(ステップS201でNo)には、ステップS201を再び実行する。つまり、処理部11は、利用要求トランザクションデータを受信するまでステップS201で待機状態をとる。

10

【0143】

ステップS202において、制御部13は、ステップS201で受信した利用要求トランザクションデータに含まれているユーザ情報および利用内容が、管理サーバ20が管理しているユーザ情報の利用条件に適合するか否かを判定する。適合していると判定した場合(ステップS202でYes)には、ステップS203に進み、そうでない場合(ステップS202でNo)には、ステップS211に進む。

20

【0144】

ステップS203において、制御部13は、ステップS201で受信した利用要求トランザクションデータを台帳管理部12に提供することで、分散台帳に格納する。また、制御部13は、上記利用要求トランザクションデータを他のサーバ10B等に送信し、すべてのサーバ10A等の分散台帳に格納させる。

【0145】

ステップS204において、制御部13は、ユーザU1のユーザ情報について、ユーザU2から利用要求がなされたことを管理サーバ20に通知する。この通知を受信した管理サーバ20は、管理対象であるユーザU1のユーザ情報をユーザU2の端末42に送信する。

30

【0146】

ステップS211において、制御部13は、利用内容が利用条件に適合しなかったことを示す情報を含めたトランザクションデータ(不図示)を生成する。

【0147】

ステップS212において、制御部13は、ステップS211で生成したトランザクションデータを台帳管理部12に提供することで、分散台帳に格納する。また、制御部13は、上記トークン付与トランザクションデータを他のサーバ10B等に送信し、すべてのサーバ10A等の分散台帳に格納させる。

【0148】

ステップS204又はS212を終えたら、図11に示される一連の処理を終了する。

40

【0149】

図12は、本実施の形態におけるサーバ10A等が実行するユーザ情報の提供に係る処理を示すフロー図である。

【0150】

ステップS301において、処理部11は、管理サーバ20からユーザU2の端末42にユーザU1のユーザ情報が提供されたことを示す提供トランザクションデータを管理サーバ20から受信したか否かを判定する。提供トランザクションデータを受信したと判定した場合(ステップS301でYes)には、ステップS302に進み、そうでない場合(ステップS301でNo)には、ステップS301を再び実行する。つまり、処理部11は、提供トランザクションデータを受信するまでステップS301で待機状態をとる。

50

## 【 0 1 5 1 】

ステップ S 3 0 2 において、制御部 1 3 は、ステップ S 3 0 1 で受信した提供トランザクションデータを台帳管理部 1 2 に提供することで、分散台帳に格納する。また、制御部 1 3 は、上記提供トランザクションデータを他のサーバ 1 0 B 等に送信し、すべてのサーバ 1 0 A 等の分散台帳に格納させる。

## 【 0 1 5 2 】

ステップ S 3 0 3 において、制御部 1 3 は、ユーザ U 1 のユーザ情報をユーザ U 2 又は端末 4 2 が正規に保有していることを証明する証明書を、ユーザ U 2 に送信する。

## 【 0 1 5 3 】

ステップ S 3 0 3 を終わったら、図 1 2 に示される一連の処理を終了する。

10

## 【 0 1 5 4 】

図 1 3 は、本実施の形態における、ユーザ情報の利用要求および提供に係る情報管理システム 1 全体の処理を示すシーケンス図である。なお、図 1 3 では、利用要求トランザクションデータに含まれているユーザ情報および利用内容が利用条件に適合する場合（図 1 1 のステップ S 2 0 2 で Yes）を示している。

## 【 0 1 5 5 】

ステップ S 2 6 1 において、端末 4 2 は、ユーザ U 1 のユーザ情報の利用の要求のための利用要求トランザクションデータを生成し、生成した利用要求トランザクションデータをサーバ 1 0 A 等に送信する。

## 【 0 1 5 6 】

サーバ 1 0 A 等は、送信された利用要求トランザクションデータを受信し、利用条件に適合することを判定した上で利用要求トランザクションデータを分散台帳に格納し、管理サーバ 2 0 に通知する（ステップ S 2 0 1 ~ S 2 0 4）。

20

## 【 0 1 5 7 】

ステップ S 2 4 1 において、管理サーバ 2 0 は、鍵発行依頼を鍵管理装置 3 0 に送信する。鍵発行依頼は、ユーザ U 1 のユーザ情報をユーザ U 2 の端末 4 2 に送信する際にユーザ情報の暗号化および復号に用いる鍵を発行することを依頼する情報である。

## 【 0 1 5 8 】

ステップ S 2 5 1 において、鍵管理装置 3 0 は、ステップ S 2 4 1 で送信された鍵発行依頼を受信すると、ユーザ情報の暗号化に用いる暗号化鍵と、当該ユーザ情報の復号に用いる復号鍵とをペアで生成する。そして、鍵管理装置 3 0 は、生成した暗号化鍵を管理サーバ 2 0 に送信し、生成した復号鍵を端末 4 2 に送信する。管理サーバ 2 0 は、鍵管理装置 3 0 が送信した暗号化鍵を受信する。端末 4 2 は、鍵管理装置 3 0 が送信した復号鍵を受信する。

30

## 【 0 1 5 9 】

ステップ S 2 4 2 において、管理サーバ 2 0 は、ステップ S 2 5 1 で受信した暗号化鍵でユーザ情報を暗号化し、暗号化されたユーザ情報を端末 4 2 に送信する。これにより、管理サーバ 2 0 は、ユーザ U 1 のユーザ情報をユーザ U 2 に提供する。端末 4 2 は、送信されたユーザ情報を受信し、ステップ S 2 5 1 で受信した復号鍵でユーザ情報を復号することで、ユーザ情報を取得する。端末 4 2 が取得したユーザ情報は、例えば、ユーザ U 2 によって、認証またはデータ分析などのために利用されることが想定される。

40

## 【 0 1 6 0 】

ステップ S 2 4 3 において、管理サーバ 2 0、ユーザ U 1 のユーザ情報を提供したことを示す提供トランザクションデータを生成し、生成した提供トランザクションデータをサーバ 1 0 A 等に送信する。

## 【 0 1 6 1 】

この後、サーバ 1 0 A 等は、送信された提供トランザクションデータを受信し、受信した提供トランザクションデータを分散台帳に格納するとともに、端末 4 2 に証明書を送信する（ステップ S 3 0 1 ~ S 3 0 3）。

## 【 0 1 6 2 】

50

### (3) ユーザ情報の利用制限

図14は、本実施の形態におけるサーバが実行するデータの利用制限に係る処理を示すフロー図である。

#### 【0163】

ステップS401において、処理部11は、ユーザU1のユーザ情報の利用制限がかかったことを示す利用制限トランザクションデータを管理サーバ20から受信したか否かを判定する。利用制限トランザクションデータを受信したと判定した場合(ステップS401でYes)には、ステップS402に進み、そうでない場合(ステップS401でNo)には、ステップS401を再び実行する。つまり、処理部11は、利用制限トランザクションデータを受信するまでステップS401で待機状態をとる。

10

#### 【0164】

ステップS402において、制御部13は、ステップS401で受信した利用制限トランザクションデータを台帳管理部12に提供することで、分散台帳に格納する。また、制御部13は、上記利用制限トランザクションデータを他のサーバ10B等に送信し、すべてのサーバ10A等の分散台帳に格納させる。

#### 【0165】

ステップS403において、制御部13は、ユーザ情報の利用制限がなされたことを端末42に通知する。端末42は、利用制限の通知を受信すると、ユーザ情報の利用を制限する。その後、端末42は、利用制限されているユーザ情報を利用することができない。

#### 【0166】

ステップS403を終えたら、図14に示される一連の処理を終了する。

20

#### 【0167】

図15は、本実施の形態における、ユーザ情報の利用制限に係る情報管理システム1全体の処理を示すシーケンス図である。なお、図15では、管理サーバ20が端末42にユーザ情報を提供してから所定時間が経過した場合を示している。

#### 【0168】

ステップS441において、管理サーバ20は、端末42にユーザ情報を提供してから所定時間が経過したか否かを判定する。所定時間が経過したと判定した場合(ステップS441でYes)には、ステップS442に進み、そうでない場合には、ステップS441を再び実行する。つまり、管理サーバ20は、所定時間が経過するまでステップS441で待機状態をとる。

30

#### 【0169】

ステップS442において、管理サーバ20は、ステップS441で所定時間が経過したと判定したに基づいて、端末42に提供したユーザ情報の利用を制限することを示す利用制限トランザクションデータを生成し、生成した利用制限トランザクションデータをサーバ10A等に送信する。

#### 【0170】

この後、サーバ10A等は、送信された利用制限トランザクションデータを受信し、受信した利用制限トランザクションデータを分散台帳に格納する。また、サーバ10A等は、端末42に利用制限の通知をする(ステップS401~S403)。

40

#### 【0171】

### (4) ユーザ情報の削除

図16は、本実施の形態におけるサーバ10A等が実行するユーザ情報の削除に係る処理を示すフロー図である。

#### 【0172】

ステップS501において、処理部11は、管理サーバ20において、ユーザU1のユーザ情報が削除されたことを示す削除トランザクションデータを管理サーバ20から受信したか否かを判定する。削除トランザクションデータを受信したと判定した場合(ステップS501でYes)には、ステップS502に進み、そうでない場合(ステップS501でNo)には、ステップS501を再び実行する。つまり、処理部11は、削除トラン

50

ザクションデータを受信するまでステップ S 5 0 1 で待機状態をとる。

【 0 1 7 3 】

ステップ S 5 0 2 において、制御部 1 3 は、ステップ S 5 0 1 で受信した削除トランザクションデータを台帳管理部 1 2 に提供することで、分散台帳に格納する。また、制御部 1 3 は、上記削除トランザクションデータを他のサーバ 1 0 B 等に送信し、すべてのサーバ 1 0 A 等の分散台帳に格納させる。

【 0 1 7 4 】

ステップ S 5 0 3 において、制御部 1 3 は、ユーザ情報の削除がなされたことを端末 4 2 に通知する。端末 4 2 は、削除の通知を受信すると、ユーザ情報を削除する。その後、端末 4 2 は、削除されたユーザ情報を利用することができない。

10

【 0 1 7 5 】

ステップ S 5 0 3 を終えたら、図 1 6 に示される一連の処理を終了する。

【 0 1 7 6 】

図 1 7 は、本実施の形態における、ユーザ情報の削除に係る情報管理システム 1 全体の処理を示すシーケンス図である。

【 0 1 7 7 】

ステップ S 5 3 1 において、端末 4 1 は、ユーザ U 1 による操作に基づいて、管理サーバ 2 0 に登録されているユーザ U 1 のユーザ情報を削除する削除要求を管理サーバ 2 0 に送信する。管理サーバ 2 0 は、削除要求を受信する。

【 0 1 7 8 】

ステップ S 5 4 1 において、管理サーバ 2 0 は、管理しているユーザ U 1 のユーザ情報を削除する。

20

【 0 1 7 9 】

ステップ S 5 4 2 において、管理サーバ 2 0 は、ステップ S 5 4 1 でユーザ U 1 のユーザ情報を削除したことを示す削除トランザクションデータを生成し、生成した削除トランザクションデータをサーバ 1 0 A 等に送信する。

【 0 1 8 0 】

この後、サーバ 1 0 A 等は、送信された削除トランザクションデータを受信し、受信した削除トランザクションデータを分散台帳に格納する。また、サーバ 1 0 A 等は、端末 4 2 に削除の通知をする（ステップ S 5 0 1 ~ S 5 0 3 ）。

30

【 0 1 8 1 】

なお、上記の実施の形態では、ユーザ情報は、端末 4 1 から管理サーバ 2 0 に送信され、管理サーバ 2 0 が保有しているとして説明したが、その代わりに、端末 4 1 が保有しているもよい。その場合、登録トランザクションデータは、端末 4 1 によって生成され、サーバ 1 0 A 等に送信される。その場合、登録トランザクションデータ内の署名は、端末 4 1 の電子署名である。

【 0 1 8 2 】

なお、上記の実施の形態では、利用制限トランザクションデータは、管理サーバ 2 0 により所定時間が経過したことに基づいて生成されると説明したが、その代わりに、端末 4 2 により所定時間が経過したことに基づいて生成されてもよい。その場合、利用制限トランザクションデータは、端末 4 1 によりサーバ 1 0 A 等に送信される。利用制限トランザクションデータの電子署名は、ユーザ U 2 の端末 4 2 の電子署名である。

40

【 0 1 8 3 】

（実施の形態の変形例）

なお、上記実施の形態の情報管理システムの制御方法は、以下のようにも記載され得るが、これに限定されない。

【 0 1 8 4 】

図 1 8 は、本変形例におけるサーバの処理（サーバの制御方法ともいう）を示すフロー図である。

【 0 1 8 5 】

50

図18に示される一連の処理は、分散台帳を保有している複数のサーバを備える情報管理システムにおいて、当該複数のサーバのうちの一のサーバが実行する制御方法である。

【0186】

ステップS601において、サーバは、情報管理システムにより管理されているユーザ情報であって、第一ユーザに関する情報であるユーザ情報に対応付けられた識別情報と、ユーザ情報の第二ユーザへの提供の許否を示す許否情報とを含む第一トランザクションデータを受信する。

【0187】

ステップS602において、サーバは、ステップS601で受信した第一トランザクションデータを複数のサーバそれぞれが備える分散台帳に格納する。

【0188】

図19は、本変形例における情報管理システムが備える複数のサーバのうちの一のサーバの構成を模式的に示すブロック図である。

【0189】

図19に示されるサーバ60は、処理部61を備える。なお、サーバ60は、実施の形態におけるサーバ10Aに相当する。

【0190】

処理部61は、情報管理システムにより管理されているユーザ情報であって、第一ユーザに関する情報であるユーザ情報に対応付けられた識別情報と、ユーザ情報の第二ユーザへの提供の許否を示す許否情報とを含む第一トランザクションデータを受信する。そして、処理部61は、受信した第一トランザクションデータを複数のサーバそれぞれが備える分散台帳に格納する。

【0191】

これにより、情報管理システムにおいて、個人のデータの利用の際に発生し得る通信を抑制することができる。

【0192】

上記実施の形態、又は、変形例におけるブロックチェーンについて補足的に説明する。

【0193】

図20は、ブロックチェーンのデータ構造を示す説明図である。

【0194】

ブロックチェーンは、その記録単位であるブロックがチェーン（鎖）状に接続されたものである。それぞれのブロックは、複数のトランザクションデータと、直前のブロックのハッシュ値とを有している。具体的には、ブロックB2には、その前のブロックB1のハッシュ値が含まれている。そして、ブロックB2に含まれる複数のトランザクションデータと、ブロックB1のハッシュ値とから演算されたハッシュ値が、ブロックB2のハッシュ値として、ブロックB3に含められる。このように、前のブロックの内容をハッシュ値として含めながら、ブロックをチェーン状に接続することで、記録されたトランザクションデータの改ざんを有効に防止する。

【0195】

仮に過去のトランザクションデータが変更されると、ブロックのハッシュ値が変更前と異なる値になり、改ざんしたブロックを正しいものとみせかけるには、それ以降のブロックすべてを作り直さなければならず、この作業は現実的には非常に困難である。この性質を使用して、ブロックチェーンに改ざん困難性が担保されている。

【0196】

図21は、トランザクションデータのデータ構造を示す説明図である。

【0197】

図21に示されるトランザクションデータは、トランザクション本体P1と、電子署名P2とを含む。トランザクション本体P1は、当該トランザクションデータに含まれるデータ本体である。電子署名P2は、トランザクション本体P1のハッシュ値に対して、当該トランザクションデータの作成者の署名鍵で署名する、より具体的には、作成者の秘密

10

20

30

40

50

鍵で暗号化することで生成されたものである。

【0198】

トランザクションデータは、電子署名P2を有するので、改ざんが実質的に不可能である。これにより、トランザクション本体の改ざんが防止される。

【0199】

以上のように、上記の実施の形態および変形例に係る制御方法によれば、サーバは、情報管理システムにより管理されているユーザ情報の利用に関する許否情報が含まれた第一トランザクションデータを分散台帳に格納する。そのため、サーバは、個人のデータの利用の都度に利用の承諾に関わる情報交換をする必要がなくなり、当該情報交換のための通信を抑制することができる。

10

【0200】

また、分散台帳に格納されたトランザクションデータの改ざんが実質的に不可能であることから、情報管理システムにより管理されているユーザ情報の利用に関する許否情報が適切に管理される。仮に、利用の承諾についての情報交換において個人と情報銀行との間、または、個人のデータを利用する企業と情報銀行との間で齟齬があると、個人のデータが適切に利用されるとはいえない。本発明の一態様に係る制御方法によれば、許否情報が分散台帳に格納され、改ざんが実質的に不可能となるので、上記の齟齬が生ずることが抑制される効果もある。

【0201】

また、サーバは、情報管理システムにより管理されているユーザ情報の利用を求めるとを示す第二トランザクションデータを分散台帳に格納する。そのため、利用の要求がなされたという事実を示す情報が、実質的に改ざんされることなく適切に管理される。よって、サーバは、ユーザ情報の利用の求めがあったという事実を示す情報を適切に管理しながら、個人のデータの利用の際に発生し得る通信を抑制することができる。

20

【0202】

また、サーバは、第二ユーザによって利用を求められたユーザ情報について、許否情報に含まれる条件に基づいて利用を許可するか否かを判定する。許否情報は、第一ユーザの判断に基づいて生成され分散台帳に格納されたものであるので、実質的に改ざんされることなく適切に管理されている。よって、サーバは、第一ユーザによる判断に従ってユーザ情報を第二ユーザに利用させる際に、個人のデータの利用の際に発生し得る通信を抑制することができる。

30

【0203】

また、サーバは、第二ユーザにユーザ情報を送信したことを示す第三トランザクションデータを分散台帳に格納する。そのため、第二ユーザにユーザ情報を送信したという事実を示す情報が、実質的に改ざんされることなく適切に管理される。よって、サーバは、第二ユーザにユーザ情報を送信したという事実を示す情報を適切に管理しながら、個人のデータの利用の際に発生し得る通信を抑制することができる。また、第一ユーザが、自身のユーザ情報がどの企業によってどのように利用されたかを知ることができる利点がある。

【0204】

また、サーバは、第二ユーザにユーザ情報を提供してから所定時間が経過したことによって、提供したユーザ情報の利用の制限がなされたことを示す第四トランザクションデータを分散台帳に格納する。そのため、利用制限がなされたという事実を示す情報が、実質的に改ざんされることなく適切に管理される。よって、サーバは、ユーザ情報の利用制限がなされたという事実を示す情報を適切に管理しながら、個人のデータの利用の際に発生し得る通信を抑制することができる。

40

【0205】

また、サーバは、ユーザ情報が削除されたことを示す第五トランザクションデータを分散台帳に格納する。そのため、ユーザ情報が削除されたという事実を示す情報が、実質的に改ざんされることなく適切に管理される。よって、サーバは、ユーザ情報が削除されたという事実を示す情報を適切に管理しながら、個人のデータの利用の際に発生し得る通信

50

を抑制することができる。

【0206】

また、サーバは、ユーザ情報の提供の許否情報が分散台帳に格納された第一ユーザにトークンを付与する。トークンは、分散台帳によって管理される価値情報であり、例えば金銭の価値の代替として用いられ得る。これにより、情報管理システムによってユーザ情報を管理することが促進され、管理対象であるユーザ情報の活用が促進される効果がある。

【0207】

また、サーバは、ユーザ情報の提供を許可する期間、ユーザ情報の提供が許可されるユーザ、又は、ユーザ情報の再提供の許否を示す情報を、実質的に改ざんされることなく適切に管理する。これにより、サーバは、個人のデータの利用の都度に利用の承諾に関わる上記の情報の交換をする必要がなくなり、当該情報交換のための通信を抑制することができる。

10

【0208】

また、サーバは、ユーザ情報の提供を許可する種別情報を、実質的に改ざんされることなく適切に管理する。これにより、サーバは、個人のデータの利用の都度に利用の承諾に関わる上記の情報の交換をする必要がなくなり、当該情報交換のための通信を抑制することができる。

【0209】

なお、上記実施の形態において、各構成要素は、専用のハードウェアで構成されるか、各構成要素に適したソフトウェアプログラムを実行することによって実現されてもよい。各構成要素は、CPUまたはプロセッサなどのプログラム実行部が、ハードディスクまたは半導体メモリなどの記録媒体に記録されたソフトウェアプログラムを読み出して実行することによって実現されてもよい。ここで、上記実施の形態のコンテンツ管理システムなどを実現するソフトウェアは、次のようなプログラムである。

20

【0210】

すなわち、このプログラムは、コンピュータに、分散台帳を保有している複数のサーバを備える情報管理システムにおいて、当該複数のサーバのうちの一のサーバが実行する制御方法であって、前記情報管理システムにより管理されているユーザ情報であって、第一ユーザに関する情報であるユーザ情報に対応付けられた識別情報と、前記ユーザ情報の第二ユーザへの提供の許否を示す許否情報とを含む第一ランザクションデータを受信し、受信した前記第一ランザクションデータを前記複数のサーバそれぞれが備える前記分散台帳に格納する制御方法を実行させるプログラムである。

30

【0211】

以上、一つまたは複数の態様に係る制御方法、サーバおよび情報管理システムなどについて、実施の形態に基づいて説明したが、本発明は、この実施の形態に限定されるものではない。本発明の趣旨を逸脱しない限り、当業者が思いつく各種変形を本実施の形態に施したもののや、異なる実施の形態における構成要素を組み合わせて構築される形態も、一つまたは複数の態様の範囲内に含まれてもよい。

【産業上の利用可能性】

【0212】

本発明は、ユーザ情報を管理する情報管理システムに利用可能である。

40

【符号の説明】

【0213】

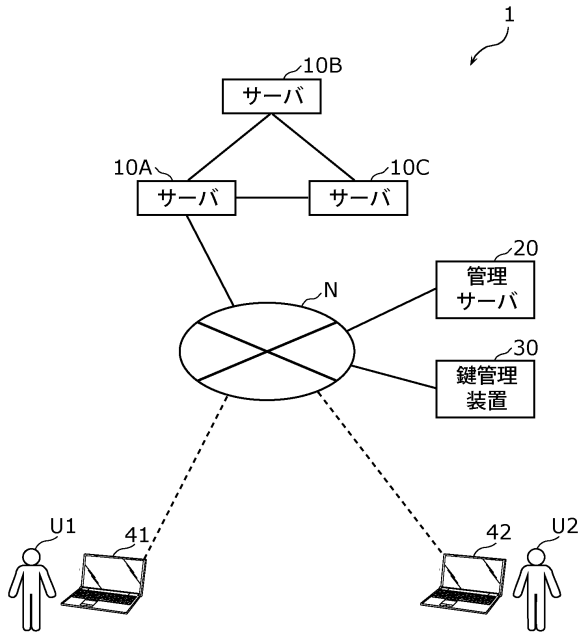
- 1 情報管理システム
- 10A、10B、10C、60 サーバ
- 11、61 処理部
- 12 台帳管理部
- 13 制御部
- 17 格納部
- 18 台帳記憶部

50

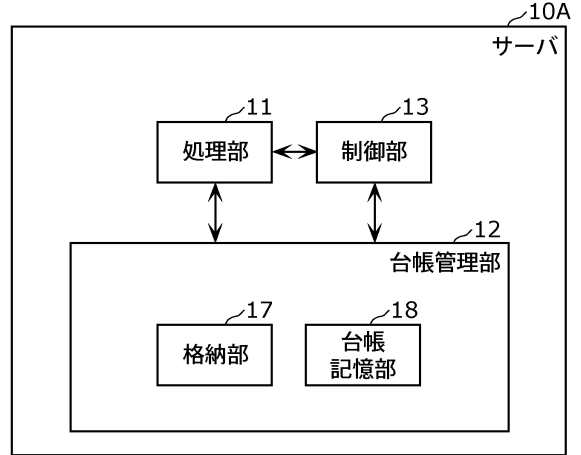
- 20 管理サーバ
- 30 鍵管理装置
- 41、42 端末
- B0、B1、B2、B3 ブロック
- N ネットワーク
- P1 トランザクション本体
- P2 電子署名
- U1、U2 ユーザ

【図面】

【図1】



【図2】



10

20

30

40

50

【 図 3 】

トランザクションID	情報アドレス	利用条件	生成日時	署名
a001	add1	住所と氏名を利用可	2018.10.10 15:00:00	89ag...

【 図 4 】

トランザクションID	利用者ID	情報アドレス	利用内容	生成日時	署名
b001	u002	add1	住所と氏名	2018.11.11 16:00:00	78ba...

10

20

【 図 5 】

トランザクションID	利用者ID	情報アドレス	提供内容	生成日時	署名
c001	u002	add1	住所と氏名	2018.11.11 17:00:00	5ab3...

【 図 6 】

トランザクションID	利用者ID	情報アドレス	制限内容	生成日時	署名
d001	u002	add1	住所と氏名	2019.5.11 17:00:00	da12...

30

40

50

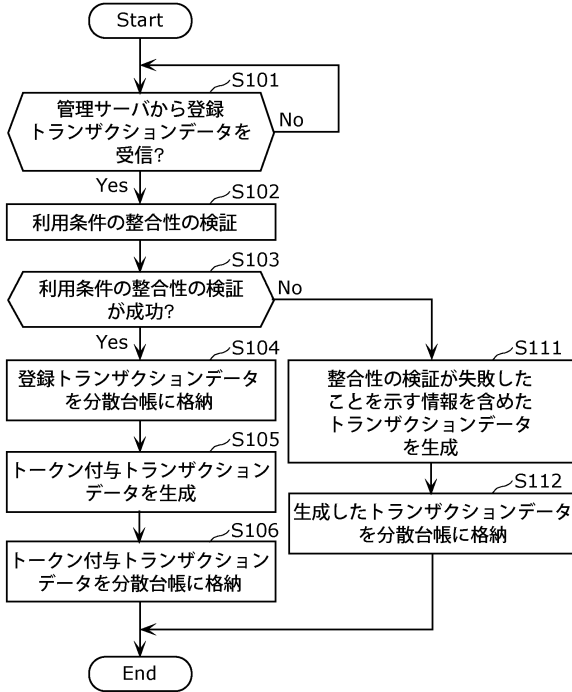
【 図 7 】

トランザクションID	情報アドレス	削除情報	生成日時	署名
e001	add1	削除	2019.5.11 17:00:00	c492...

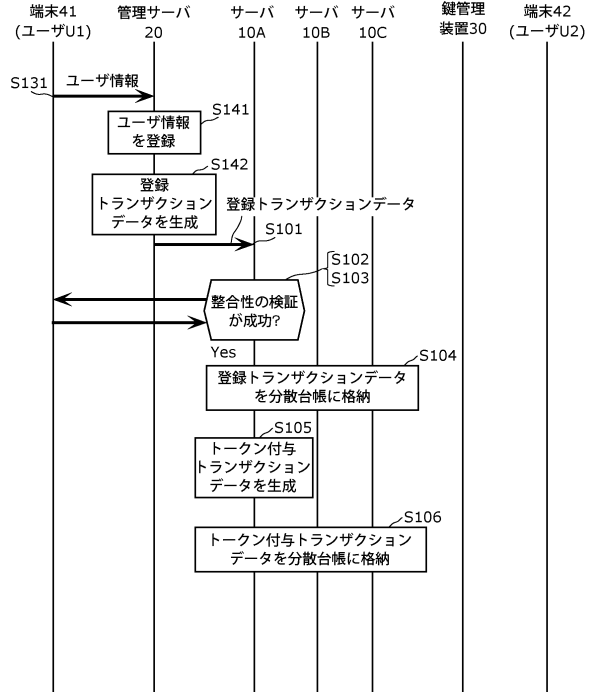
【 図 8 】

トランザクションID	提供元アドレス	提供先アドレス	生成日時	署名
f001	add5	add6	2018.10.10 15:00:00	3b44...

【 図 9 】



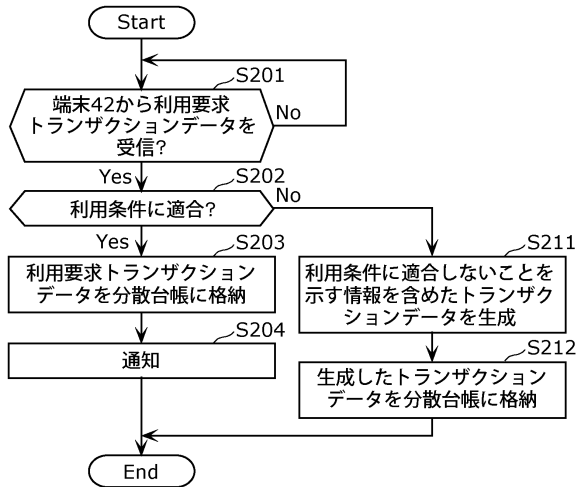
【 図 10 】



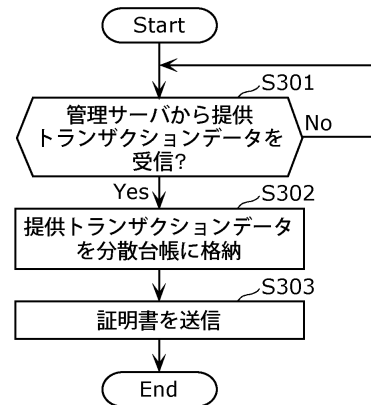
10

20

【 図 11 】



【 図 12 】

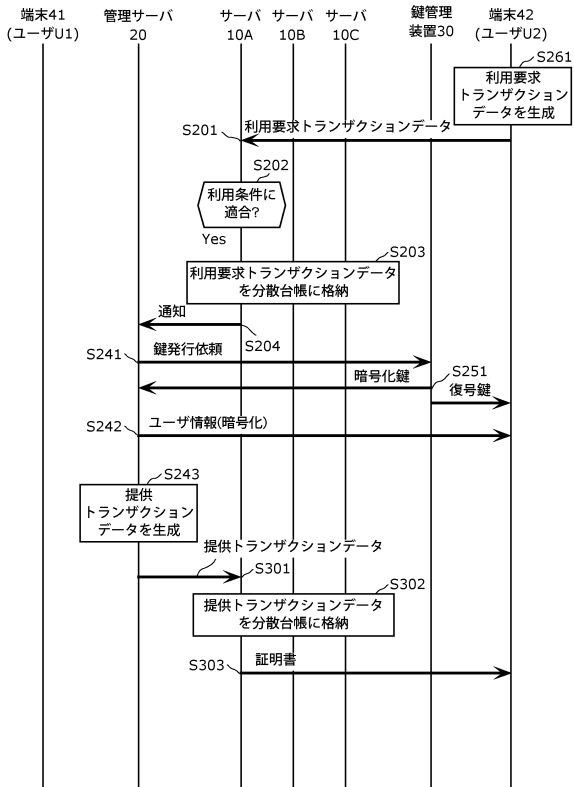


30

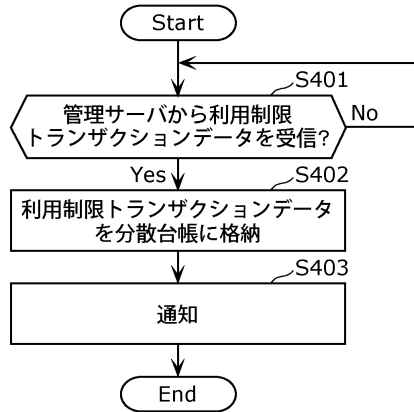
40

50

【図13】



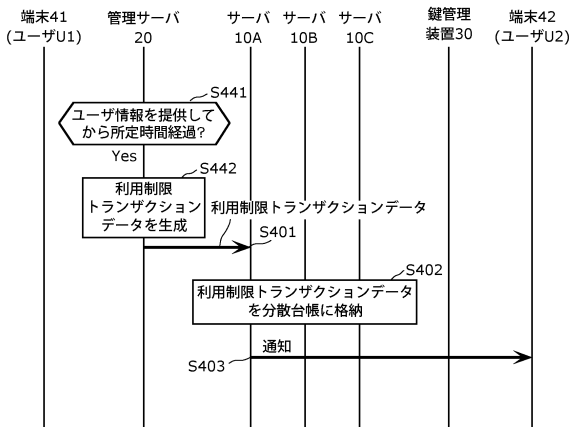
【図14】



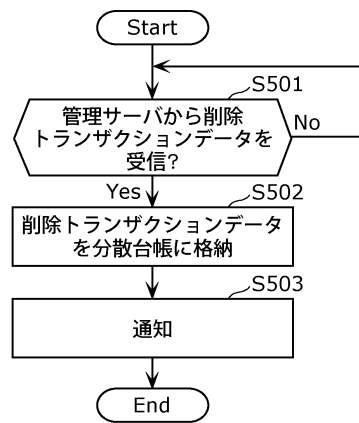
10

20

【図15】



【図16】

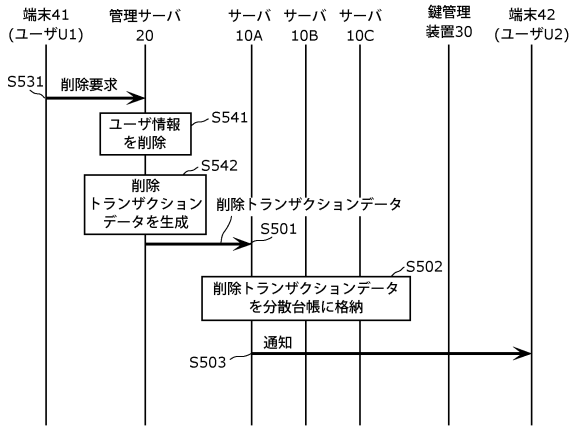


30

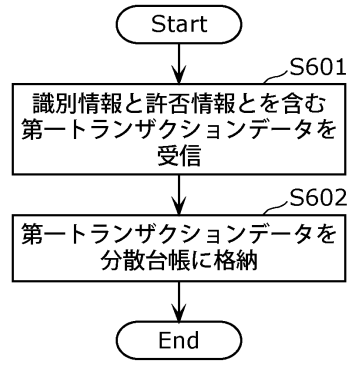
40

50

【図17】

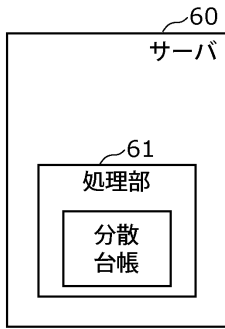


【図18】

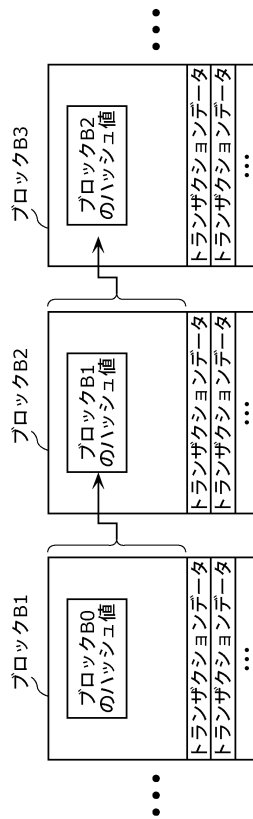


10

【図19】



【図20】



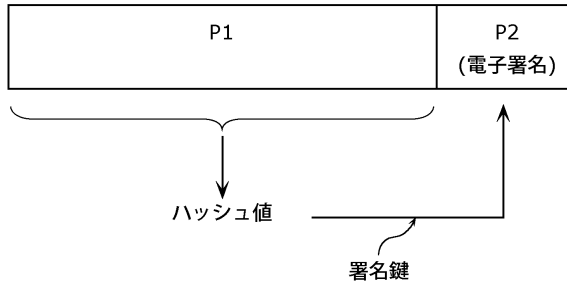
20

30

40

50

【図 2 1】



10

20

30

40

50

## フロントページの続き

- (72)発明者 海上 勇二  
日本国大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内
- (72)発明者 道山 淳児  
日本国大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内
- (72)発明者 添田 純一郎  
日本国大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内
- (72)発明者 廣瀬 雄揮  
日本国大阪府大阪府中央区城見 2 丁目 1 番 6 1 号 パナソニック I P マネジメント株式会社内
- (72)発明者 淵上 哲司  
日本国大阪府大阪府中央区城見 2 丁目 1 番 6 1 号 パナソニック I P マネジメント株式会社内
- (72)発明者 大森 基司  
日本国大阪府門真市大字門真 1 0 0 6 番地 パナソニック株式会社内
- 審査官 行田 悦資
- (56)参考文献 国際公開第 2 0 1 8 / 1 2 4 2 9 7 ( W O , A 1 )  
特開 2 0 1 6 - 0 9 1 0 6 7 ( J P , A )  
清本 晋作, 分散型ブロックチェーン基盤とデータ流通プラットフォームへの応用, 第 3 8 回医療情報学連合大会 ( 第 1 9 回日本医療情報学会学術大会 ) 論文集, 日本, 日本医療情報学会, 2018年11月22日, pp.174-176  
真野浩, 「オープンなデータ取引市場」実現の取り組み, 情報管理, 日本, 国立研究開発法人科学技術振興機構, 2017年09月01日, 第60巻, 第6号, pp.391-401
- (58)調査した分野 (Int.Cl., D B 名)  
G 0 6 F 2 1 / 6 2  
H 0 4 L 9 / 3 2