(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年6月18日(18.06.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/122095 A1

(51) 国際特許分類:
H04L 9/32 (2006.01) *G06F 21/62* (2013.01)

(21) 国際出願番号： PCT/JP2019/048391

(22) 国際出願日： 2019年12月11日(11.12.2019)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(30) 優先権データ：
62/777,922 2018年12月11日(11.12.2018) US

(71) 出願人: 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**) [US/US]; 90503 カリフォルニア州トーランス, スイート ２００, マリナー アベニュー ２００００ California (US).

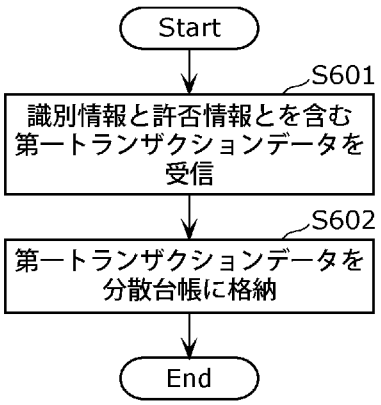
(72) 発明者: 道山 淳児(**MICHIYAMA, Junji**). 添田 純一郎(**SOEDA, Junichiro**). 廣瀬 雄揮(**HIROSE, Yuuki**). 渕上 哲司(**FUCHIKAMI, Tetsuji**). 大森 基司(**OHMORI, Motoji**). 海上 勇二(**UNAGAMI, Yuji**); 〒5718501 大阪府門真市大字門真１００６番地 パナソニック株式会社内 Osaka (JP).

(74) 代理人: 新 居 広 守, 外 (**NII, Hiromori** et al.); 〒5320011 大阪府大阪市淀川区西中島５丁目３番１０号タナカ・イトーピア新大阪ビル６階新居国際特許事務所内 Osaka (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,

(54) **Title:** CONTROL METHOD, SERVER, PROGRAM, AND DATA STRUCTURE

(54) 発明の名称： 制御方法、サーバ、プログラム、および、データ構造



S601 Receive first transaction data including identification information and permission information
S602 Store first transaction data in distributed ledger

(57) **Abstract:** In an information management system comprising a plurality of servers holding a distributed ledger, the control method of the present invention, which is executed by one of said plurality of servers, carries out the following steps: receiving first transaction data that includes identification information associated with user information managed by the information management system, said user information relating to a first user, and includes permission information that indicates permission to provide the user information to a second user (S601); and storing the received first transaction data in the distributed ledger that each of the plurality of servers comprises (S602).

WO 2020/122095 A1

［続葉有］

MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一　国際調査報告（条約第21条(3)）

(57) 要約：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し（Ｓ６０１）、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（Ｓ６０２）。

明　細　書

発明の名称 ：

制御方法、サーバ、プログラム、および、データ構造

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] 非特許文献1：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１１月２５日検索］、インターネット<URL:https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/dai2/siryou1.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う問題がある。

[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] 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。

[0007] 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。

発明の効果

[0008] 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

[0009] [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。

[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。

[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。

[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。

[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許否情報が含めら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。

[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] 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こ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。

[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。

[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。

[0021] 例えば、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。

[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。

[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。

[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。

[0036] 上記態様により、上記制御方法と同様の効果を奏する。

[0037] 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。

[0038] 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。

[0039] 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。

[0040] 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。

[0041] （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。

[0042] 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。

[0043] 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。

[0044] 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。

[0045] 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１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１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。

[0046] 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、複数であればよい。また、サーバ１０Ａ等同士は、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 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る。

[0064] （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Ｕ１がユーザ情報を管理サーバ２０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Ｕ１がユーザ情報を管理サーバ２０に登録したときに、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。

[0065] 登録トランザクションデータは、ユーザＵ１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Ｕ２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。

[0066] 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Ｕ２、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。

[0067] 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。

[0068] 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。

[0069] 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。

[0070] 情報アドレスは、管理サーバ２０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。

[0071] 利用条件は、管理サーバ２０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２０に登録されたユーザ情報のうち、ユーザＵ２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。

[0072] 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。

[0073] 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。

[0074] 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「ａ００１」であり、アドレス「ａｄｄ１」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、「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。

[0075] （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Ｕ２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。利用要求トランザクションデータは、ユーザＵ２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Ｕ２の端末４２によって生成され、サーバ１０Ａ等に送信される。

[0076] 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Ｕ１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ることを示す第二トランザクションデータに相当する。

[0077] 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。

[0078] 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。

[0079] 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。

[0080] 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、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Ｕ１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（２０代、３０代、４０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。

[0081] 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。

[0082] 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。

[0083] 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。

[0084] 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「ｂ００１」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」の情報の利用を利用者「ｕ００２」が求めていることを示している。生成日時は、「２０１８年１１月１１日　１６時００分００秒」であり、署名は、ユーザＵ２の電子署名である。ここで、ユーザＵ２の利用者ＩＤを「ｕ００２」とした。

[0085] （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２０からユーザＵ２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２０からユーザＵ２にユーザ情報を提供したときに、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。

[0086] 提供トランザクションデータは、管理サーバ２０からユーザＵ２の端末４２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。

[0087] 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。

[0088] 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。

[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。

[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。

[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。

[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] 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。

[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。

[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。

[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。

[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等に送信される。

[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。

[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。

[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。

[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。

[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] ステップＳ１０２において、制御部１３は、利用条件の整合性の検証を行う。具体的には、制御部１３は、ステップＳ１０１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Ｕ１のユーザ情報に対してユーザＵ１が設定した利用条件と整合しているか否かを検証する。

[0129] ステップＳ１０３において、制御部１３は、ステップＳ１０２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Ｓ１０３でＹｅｓ）には、ステップＳ１０４に進み、そうでない場合（ステップＳ１０３でＮｏ）には、ステップＳ１１１に進む。

[0130] ステップＳ１０４において、制御部１３は、ステップＳ１０１で受信した登録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、上記登録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。

[0131] ステップＳ１０５において、制御部１３は、管理サーバ２０からユーザＵ１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。

[0132] ステップＳ１０６において、制御部１３は、ステップＳ１０５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。

[0133] ステップＳ１１１において、制御部１３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。

[0134] ステップＳ１１２において、制御部１３は、ステップＳ１１１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。

[0135] ステップＳ１０６又はＳ１１２を終えたら、図９に示される一連の処理を終了する。

[0136] 図１０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１０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１０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Ｓ１０３でＹｅｓ）を示している。

[0137] ステップＳ１３１において、端末４１は、ユーザＵ１による操作に基づいてユーザＵ１のユーザ情報を、その利用条件とともに管理サーバ２０に送信する。管理サーバ２０は、端末４１からユーザ情報及び利用条件を受信する。

[0138] ステップＳ１４１において、管理サーバ２０は、端末４１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。

[0139] ステップＳ１４２において、管理サーバ２０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１０Ａ等に送信する。

[0140] 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。

[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。

[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。

[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。

[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。

[0151] ステップＳ３０２において、制御部１３は、ステップＳ３０１で受信した提供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、上記提供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。

[0152] ステップＳ３０３において、制御部１３は、ユーザＵ１のユーザ情報をユーザＵ２又は端末４２が正規に保有していることを証明する証明書を、ユーザＵ２に送信する。

[0153] ステップＳ３０３を終えたら、図１２に示される一連の処理を終了する。

[0154] 図１３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１３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１１のステップＳ２０２でＹｅｓ）を示している。

[0155] ステップＳ２６１において、端末４２は、ユーザＵ１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１０Ａ等に送信する。

[0156] サーバ１０Ａ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２０に通知する（ステップＳ２０１～Ｓ２０４）。

[0157] ステップＳ２４１において、管理サーバ２０は、鍵発行依頼を鍵管理装置３０に送信する。鍵発行依頼は、ユーザＵ１のユーザ情報をユーザＵ２の端末４２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。

[0158] ステップＳ２５１において、鍵管理装置３０は、ステップＳ２４１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３０は、生成した暗号化鍵を管理サーバ２０に送信し、生成した復号鍵を端末４２に送信する。管理サーバ２０は、鍵管理装置３０が送信した暗号化鍵を受信する。端末４２は、鍵管理装置３０が送信した復号鍵を受信する。

[0159] ステップＳ２４２において、管理サーバ２０は、ステップＳ２５１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４２に送信する。これにより、管理サーバ２０は、ユーザＵ１のユーザ情報をユーザＵ２に提供する。端末４２は、送信されたユーザ情報を受信し、ステップＳ２５１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。

[0160] ステップＳ２４３において、管理サーバ２０、ユーザＵ１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１０Ａ等に送信する。

[0161] この後、サーバ１０Ａ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４２に証明書を送信する（ステップＳ３０１～Ｓ３０３）。

[0162] （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。

[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。

[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。

[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ことに基づいて、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）。

[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、削除トランザクションデータを受信するまでステップＳ５０１で待機状態をとる。

[0173] ステップＳ５０２において、制御部１３は、ステップＳ５０１で受信した削除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、上記削除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

。

[0174] ステップＳ５０３において、制御部１３は、ユーザ情報の削除がなされたことを端末４２に通知する。端末４２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４２は、削除されたユーザ情報を利用することができない。

[0175] ステップＳ５０３を終えたら、図１６に示される一連の処理を終了する。

[0176] 図１７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。

[0177] ステップＳ５３１において、端末４１は、ユーザＵ１による操作に基づいて、管理サーバ２０に登録されているユーザＵ１のユーザ情報を削除する削除要求を管理サーバ２０に送信する。管理サーバ２０は、削除要求を受信する。

[0178] ステップＳ５４１において、管理サーバ２０は、管理しているユーザＵ１のユーザ情報を削除する。

[0179] ステップＳ５４２において、管理サーバ２０は、ステップＳ５４１でユーザＵ１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１０Ａ等に送信する。

[0180] この後、サーバ１０Ａ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１０Ａ等は、端末４２に削除の通知をする（ステップＳ５０１～Ｓ５０３）。

[0181] なお、上記の実施の形態では、ユーザ情報は、端末４１から管理サーバ２０に送信され、管理サーバ２０が保有しているとして説明したが、その代わりに、端末４１が保有していてもよい。その場合、登録トランザクションデータは、端末４１によって生成され、サーバ１０Ａ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４１の電子署名である。

[0182] 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２０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４２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４１によりサーバ１０Ａ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Ｕ２の端末４２の電子署名である。

[0183] （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。

[0184] 図１８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。

[0185] 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めら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。

[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こ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。

[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。

[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。

[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。

[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。

[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制御方法を実行させるプログラムである。

[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。

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

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

請求の範囲

[請求項1] 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

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

請求項１に記載の制御方法。

[請求項3] 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

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

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

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

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

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] 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

サーバ。

[請求項11] 請求項１～９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。

[請求項12] 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、

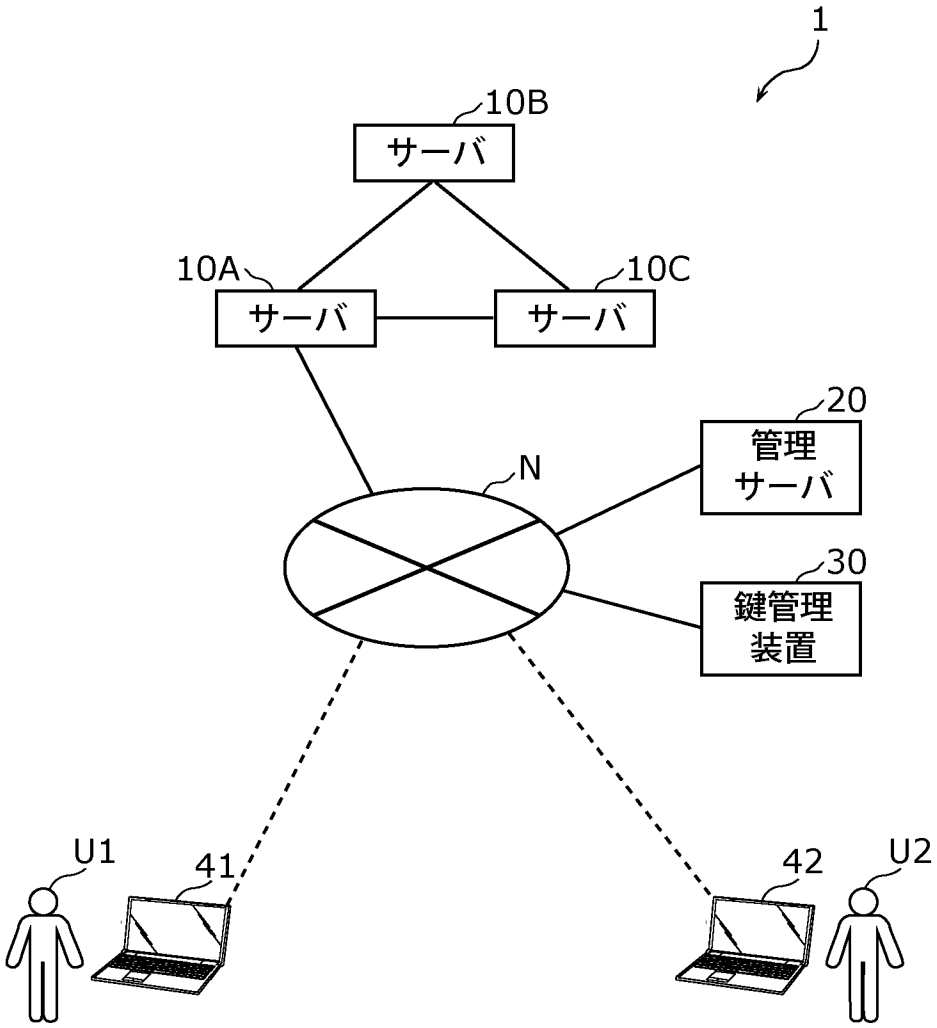
前記情報管理システムにより管理されているユーザ情報であって、

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、

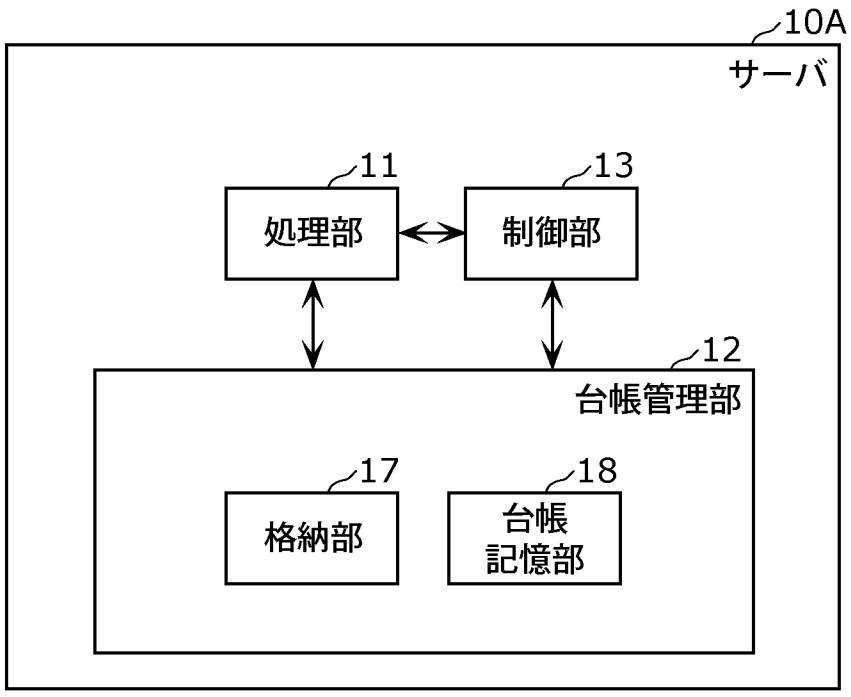
前記第一トランザクションデータは、前記複数のサーバそれぞれが備える前記分散台帳に記録される

データ構造。

[図1]


1
10B
サーバ
10A
サーバ
10C
サーバ
20
管理
サーバ
N
30
鍵管理
装置
U1
41
42
U2

[図2]


10A
サーバ
11
処理部
13
制御部
12
台帳管理部
17
格納部
18
台帳
記憶部

[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...

[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...

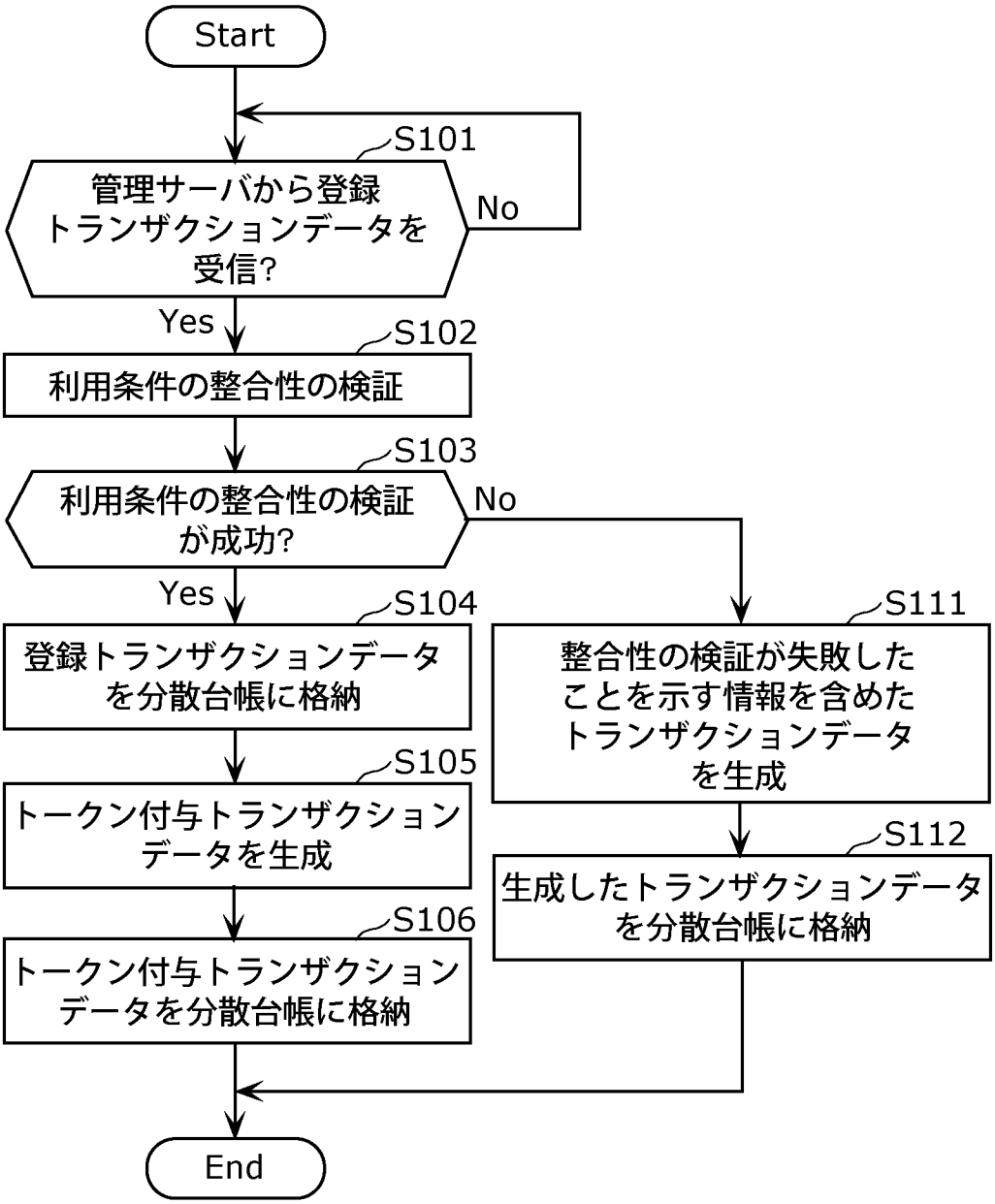
[図7]

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...

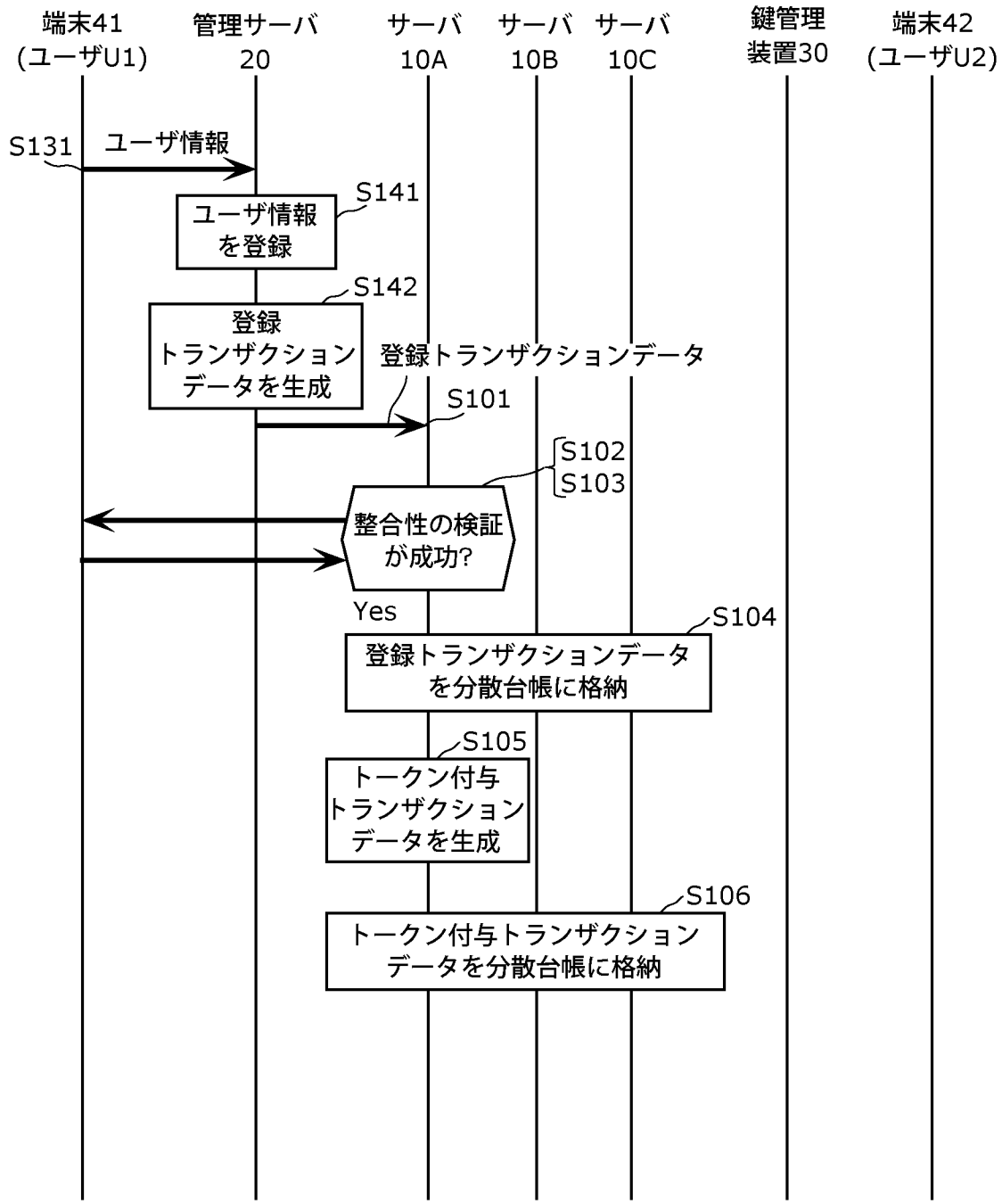
[図8]

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...

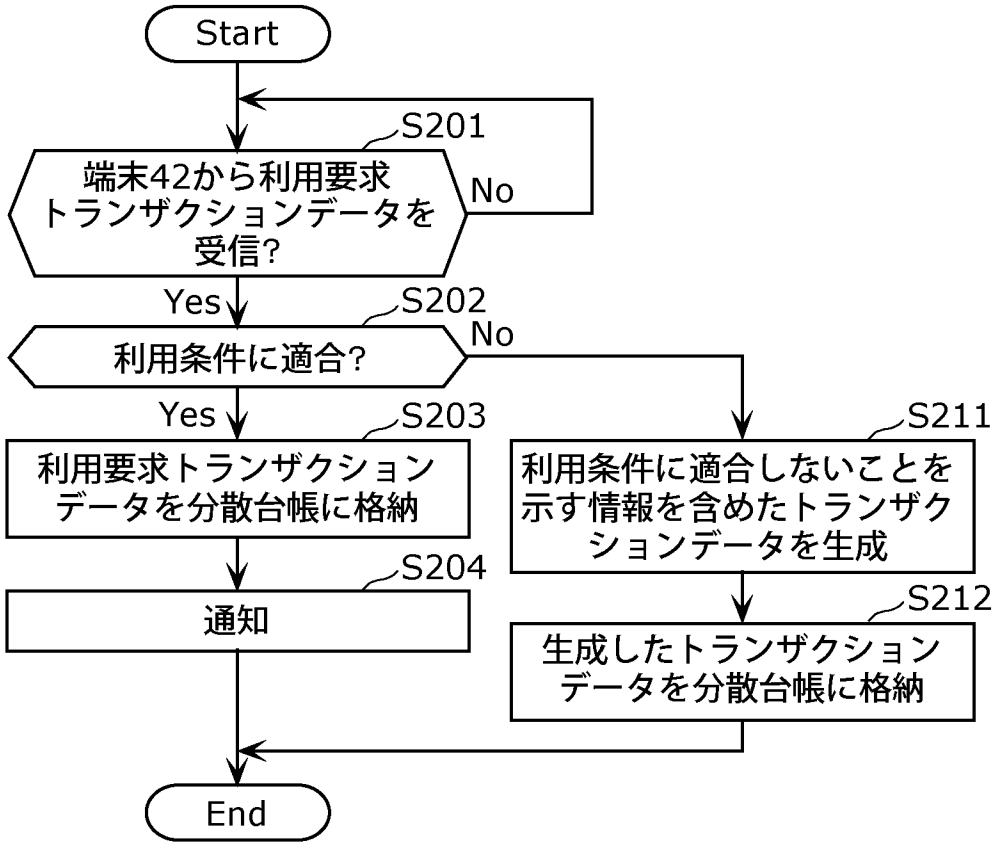
[図9]



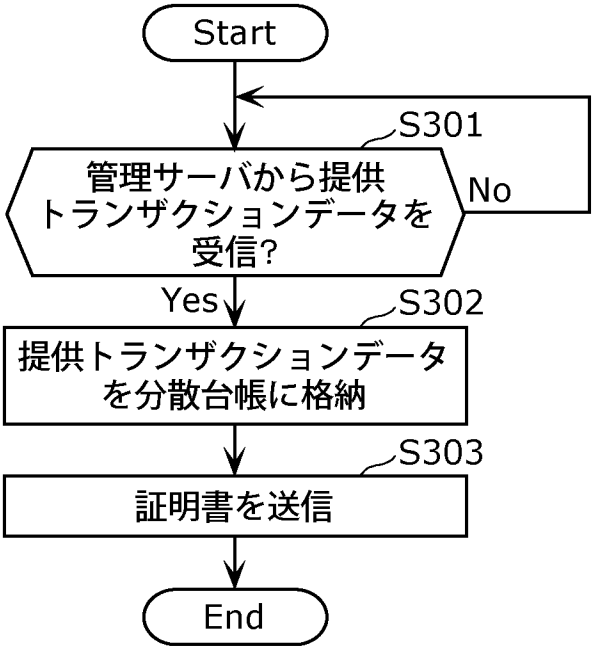
[図10]


端末41
(ユーザU1)
管理サーバ
20
サーバ
10A
サーバ
10B
サーバ
10C
鍵管理
装置30
端末42
(ユーザU2)
S131
ユーザ情報
S141
ユーザ情報
を登録
S142
登録
トランザクション
データを生成
登録トランザクションデータ
S101
S102
S103
整合性の検証
が成功?
Yes
S104
登録トランザクションデータ
を分散台帳に格納
S105
トークン付与
トランザクション
データを生成
S106
トークン付与トランザクション
データを分散台帳に格納

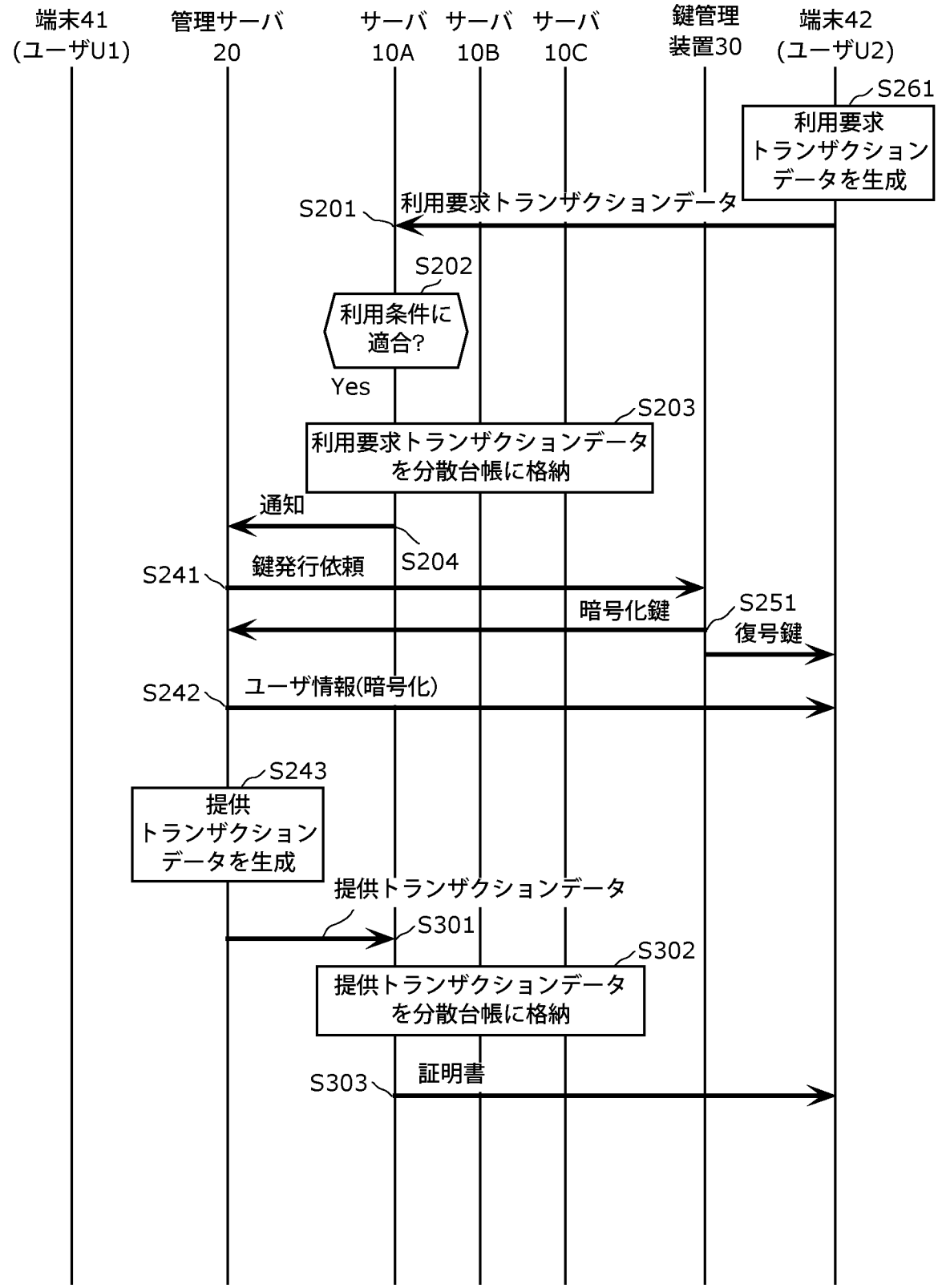
[図11]


Start
S201
端末42から利用要求トランザクションデータを受信?
No
Yes
S202
利用条件に適合?
No
Yes
S203
利用要求トランザクションデータを分散台帳に格納
S204
通知
S211
利用条件に適合しないことを示す情報を含めたトランザクションデータを生成
S212
生成したトランザクションデータを分散台帳に格納
End

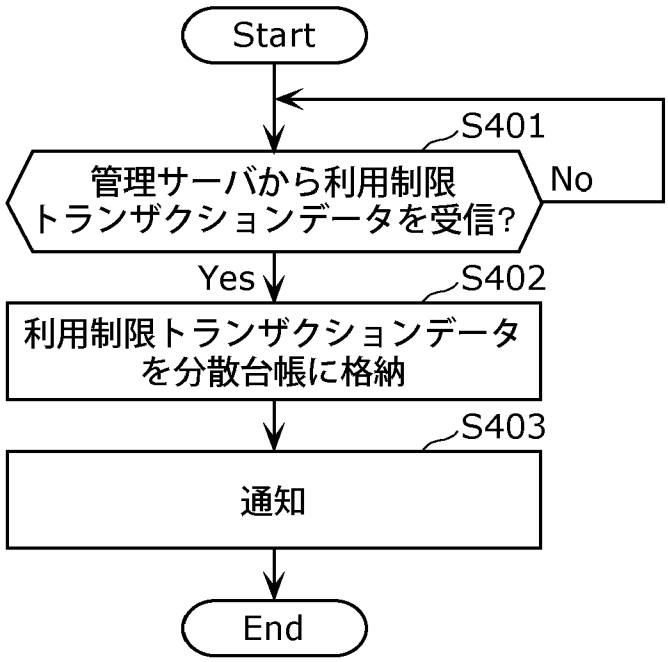
[図12]


Start
S301
管理サーバから提供トランザクションデータを受信?
No
Yes
S302
提供トランザクションデータを分散台帳に格納
S303
証明書を送信
End

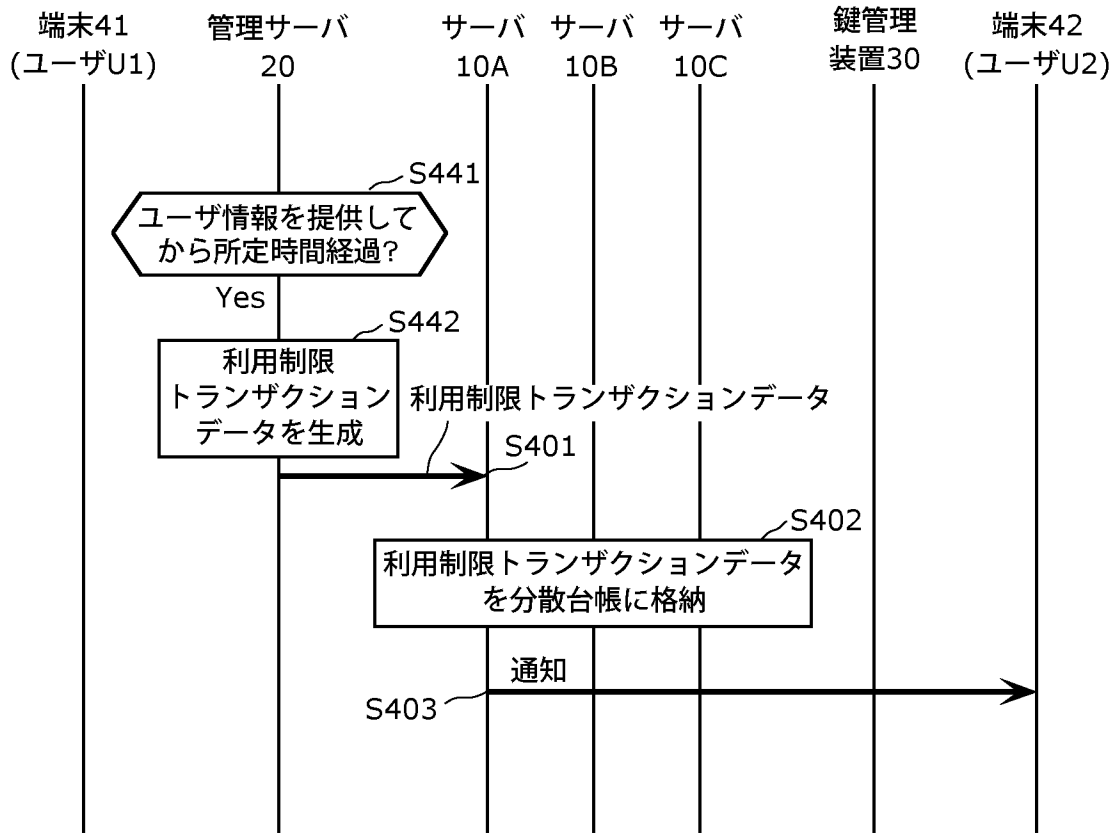
[図13]


端末41
(ユーザU1)
管理サーバ
20
サーバ
10A
サーバ
10B
サーバ
10C
鍵管理
装置30
端末42
(ユーザU2)
S261
利用要求
トランザクション
データを生成
S201
利用要求トランザクションデータ
S202
利用条件に
適合?
Yes
S203
利用要求トランザクションデータ
を分散台帳に格納
通知
S204
S241
鍵発行依頼
暗号化鍵
S251
復号鍵
S242
ユーザ情報(暗号化)
S243
提供
トランザクション
データを生成
提供トランザクションデータ
S301
S302
提供トランザクションデータ
を分散台帳に格納
S303
証明書

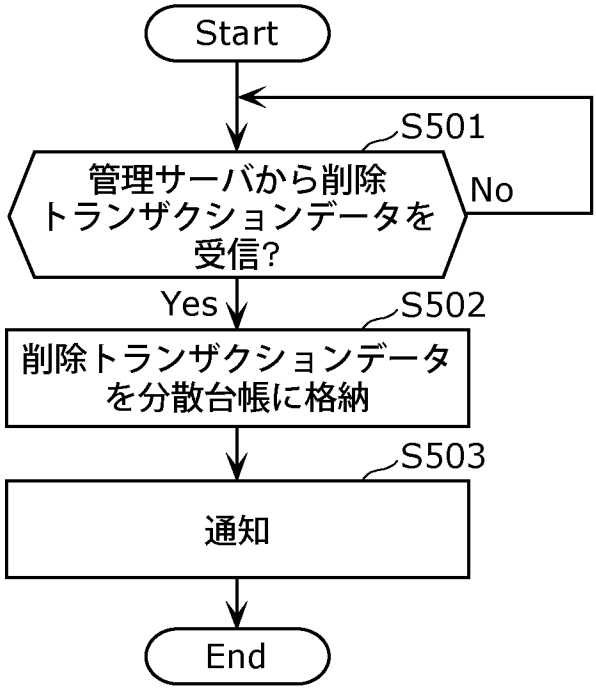
[図14]


Start
S401
管理サーバから利用制限
トランザクションデータを受信?
No
Yes
S402
利用制限トランザクションデータ
を分散台帳に格納
S403
通知
End

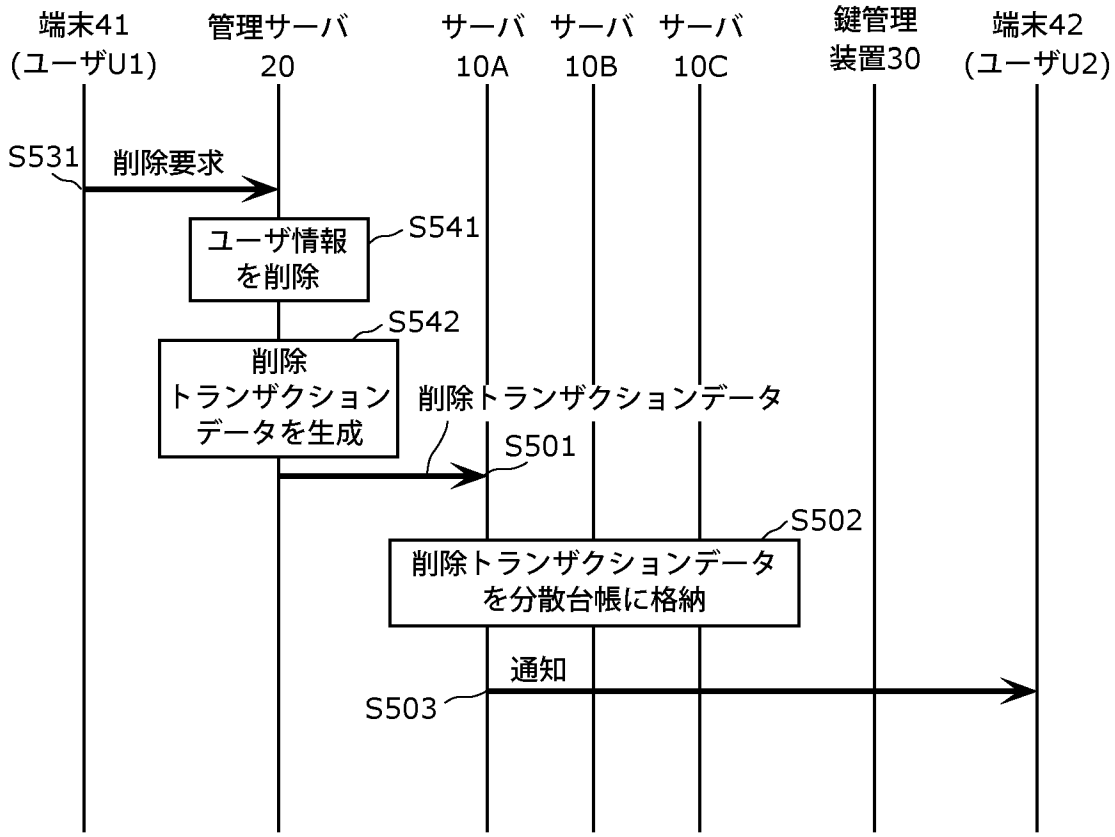
[図15]


端末41
(ユーザU1)
管理サーバ
20
サーバ
10A
サーバ
10B
サーバ
10C
鍵管理
装置30
端末42
(ユーザU2)
S441
ユーザ情報を提供して
から所定時間経過?
Yes
S442
利用制限
トランザクション
データを生成
利用制限トランザクションデータ
S401
S402
利用制限トランザクションデータ
を分散台帳に格納
通知
S403

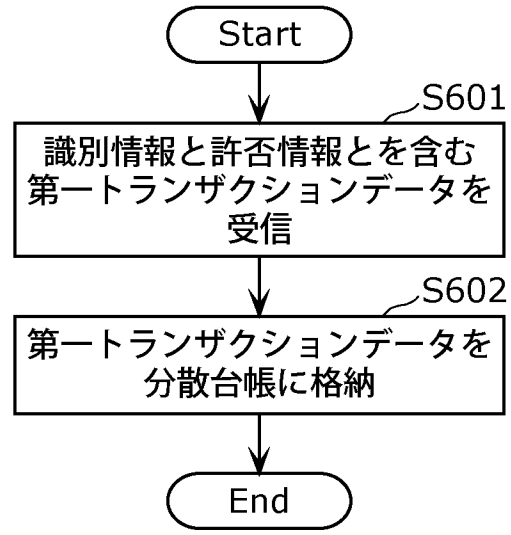
[図16]


Start
S501
管理サーバから削除トランザクションデータを受信?
No
Yes
S502
削除トランザクションデータを分散台帳に格納
S503
通知
End

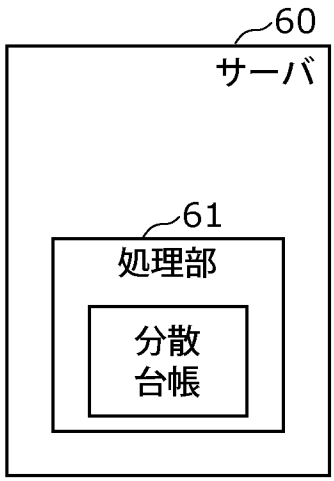
[図17]


端末41 (ユーザU1)
管理サーバ 20
サーバ 10A
サーバ 10B
サーバ 10C
鍵管理装置30
端末42 (ユーザU2)
S531
削除要求
ユーザ情報を削除
S541
S542
削除トランザクションデータを生成
削除トランザクションデータ
S501
S502
削除トランザクションデータを分散台帳に格納
通知
S503

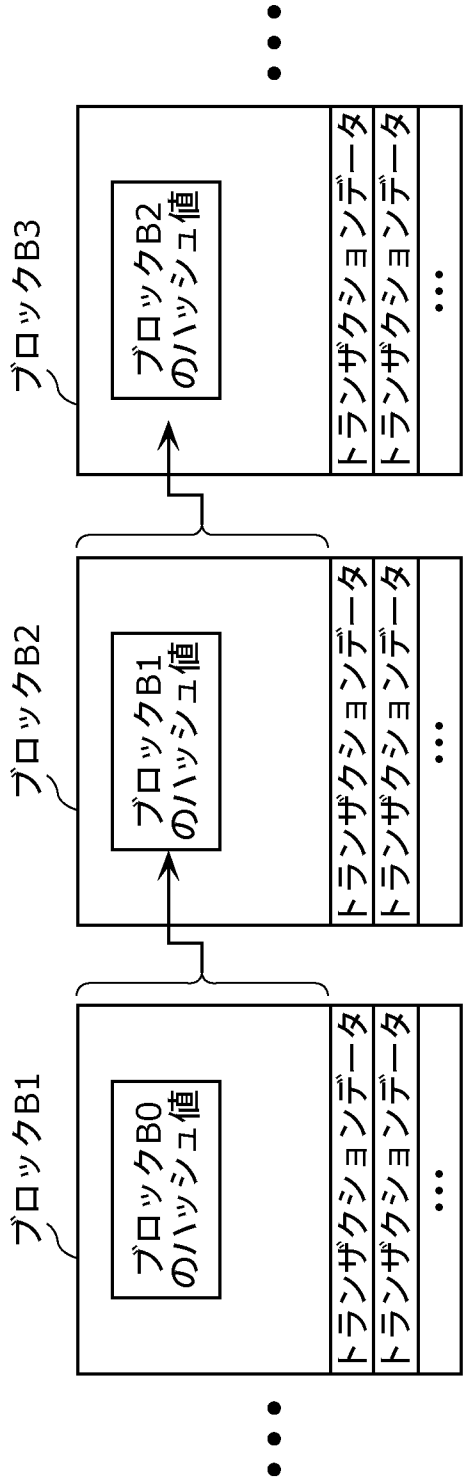
[図18]


Start
S601
識別情報と許否情報とを含む第一トランザクションデータを受信
S602
第一トランザクションデータを分散台帳に格納
End

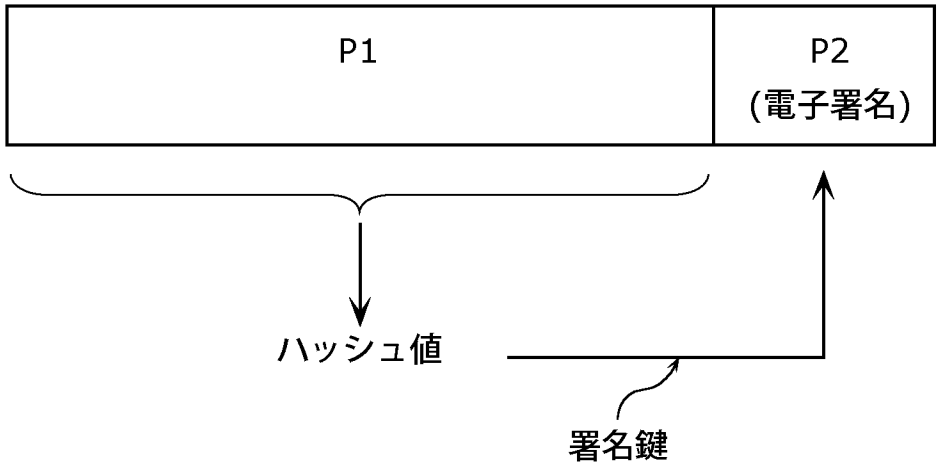
[図19]


60
サーバ
61
処理部
分散台帳

[図20]


ブロックB3
ブロックB2のハッシュ値
トランザクションデータ
トランザクションデータ
…
ブロックB2
ブロックB1のハッシュ値
トランザクションデータ
トランザクションデータ
…
ブロックB1
ブロックB0のハッシュ値
トランザクションデータ
トランザクションデータ
…

[図21]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/048391

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. H04L9/32(2006.01)i, G06F21/62(2013.01)i
FI: G06F21/62345, H04L9/00675Z
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl. H04L9/32, G06F21/62

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2020
Registered utility model specifications of Japan	1996-2020
Published registered utility model applications of Japan	1994-2020

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	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38回医療情報学連合大会（第19回日本医療情報学会学術大会）論文集，22 November 2018, pp. 174-176, particularly, sections 2, 3.1, (KIYOMOTO, Shinsaku, Distributed blockchain architecture and its application to data distribution platform), non-official translation (Proceedings of the 38th Joint Conference on Medical Informatics (The 19th Annual Meeting of Japan Association for Medical Informatics))	1-12
Y	WO 2018/124297 A1 (OKEIOS INC.) 05.07.2018 (2018-07-05), paragraphs [0050]-[0097]	1-12
Y	JP 2016-91067 A (SOFTBANK CORP.) 23.05.2016 (2016-05-23), paragraphs [0021]-[0079]	2-9
Y	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，01 September 2017, vol. 60, no. 6, pp. 391-401, particularly, section 4, (MANO, Hiroshi, Open data exchange market platform design, Journal of Information Processing and Management)	2-9
P, A	WO 2019/129582 A1 (NEWBANKING APS) 04.07.2019 (2019-07-04), page 13, line 30 to page 20, line 7	1-12

☐ Further documents are listed in the continuation of Box C.
☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10.02.2020	25.02.2020
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2019/048391

WO 2018/124297 A1	05.07.2018	EP 3564845 A1 paragraphs [0050]-[0097]
JP 2016-91067 A	23.05.2016	(Family: none)
WO 2019/129582 A1	04.07.2019	(Family: none)

国際調査報告

国際出願番号
PCT/JP2019/048391

A. 発明の属する分野の分類（国際特許分類（ＩＰＣ））

H04L 9/32(2006.01)i; G06F 21/62(2013.01)i
FI: G06F21/62 345; H04L9/00 675Z

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

H04L9/32; G06F21/62

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０２０年
日本国実用新案登録公報	１９９６－２０２０年
日本国登録実用新案公報	１９９４－２０２０年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	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３８回医療情報学連合大会（第１９回日本医療情報学会学術大会）論文集，2018.11.22，pp.174-176 特に、2節、3.1節	1-12
Y	WO 2018/124297 A1 (株式会社ＯＫＥＩＯＳ) 05.07.2018 (2018-07-05) 段落0050-0097	1-12
Y	JP 2016-91067 A (ソフトバンク株式会社) 23.05.2016 (2016-05-23) 段落0021-0079	2-9
Y	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，2017.09.01，第60巻，第6号，pp.391-401 特に、4節	2-9
P, A	WO 2019/129582 A1 (NEWBANKING APS) 04.07.2019 (2019-07-04) 13頁30行－20頁7行	1-12

☐ Ｃ欄の続きにも文献が列挙されている。

☑ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー
"A" 特に関連のある文献ではなく、一般的技術水準を示すもの
"E" 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
"L" 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
"O" 口頭による開示、使用、展示等に言及する文献
"P" 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
"T" 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの
"X" 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
"Y" 特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
"&" 同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
10.02.2020	25.02.2020

名称及びあて先
日本国特許庁(ISA/JP)
〒100-8915
日本国
東京都千代田区霞が関三丁目４番３号

権限のある職員（特許庁審査官）
行田　悦資 5S 6304
電話番号 03-3581-1101 内線 3546

国際調査報告
パテントファミリーに関する情報

国際出願番号
PCT/JP2019/048391

引用文献	公表日	パテントファミリー文献	公表日
WO 2018/124297 A1	05.07.2018	EP 3564845 A1 段落0050-0097	
JP 2016-91067 A	23.05.2016	（ファミリーなし）	
WO 2019/129582 A1	04.07.2019	（ファミリーなし）	