(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
2019年10月10日(10.10.2019)

WIPO | PCT

(10) 国際公開番号
WO 2019/193820 A1

(51) 国際特許分類:
G06F 21/62 (2013.01) *G06F 21/55* (2013.01)
G06F 12/00 (2006.01) *H04L 9/32* (2006.01)

(21) 国際出願番号： PCT/JP2019/002741

(22) 国際出願日： 2019年1月28日(28.01.2019)

(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：
特願 2018-070788 2018年4月2日(02.04.2018) JP

(71) 出願人: ソニー株式会社 (**SONY CORPORATION**) [JP/JP]; 〒1080075 東京都港区港南１丁目７番１号 Tokyo (JP).

(72) 発明者: 高橋 恒樹 (**TAKAHASHI, Koki**); 〒1410031 東京都品川区西五反田二丁目１１番１７号 株式会社ソニー・グローバルエデュケーション内 Tokyo (JP). 渡邊 一弘(**WATANABE, Kazuhiro**); 〒1410031 東京都品川区西五反田二丁目１１番１７号 株式会社ソニー・グローバルエデュケーション内 Tokyo (JP). 礒津 政明 (**ISOZU, Masaaki**); 〒1410031 東京都品川区西五反田二丁目１１番１７号 株式会社ソニー・グローバルエデュケーション内 Tokyo (JP).

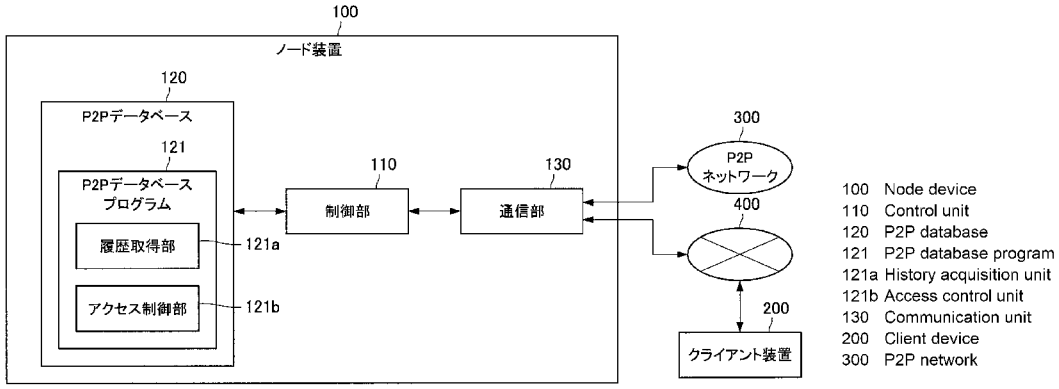
(74) 代理人: 特許業務法人酒井国際特許事務所 (**SAKAI INTERNATIONAL PATENT OFFICE**); 〒1000013 東京都千代田区霞が関３丁目８番１号 虎の門三井ビルディング Tokyo (JP).

(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, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,

(54) **Title:** INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD, AND PROGRAM

(54) 発明の名称： 情報処理装置、情報処理方法、およびプログラム

[図5]



(57) **Abstract:** [Problem] To allow access to a P2P database to be more appropriately controlled. [Solution] Provided is an information processing device comprising an access control unit that, on the basis of history information regarding access to a P2P database by an arbitrary subject, controls new access to the P2P database by the subject.

(57) 要約：【課題】Ｐ２Ｐデータベースへのアクセスをより適切に制御することを可能にする。【解決手段】任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御するアクセス制御部を備える、情報処理装置が提供される。

WO 2019/193820 A1

[続葉有]

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))

明　細　書

発明の名称 ： 情報処理装置、情報処理方法、およびプログラム

技術分野

[0001] 本開示は、情報処理装置、情報処理方法、およびプログラムに関する。

背景技術

[0002] 近年、ブロックチェーンデータをはじめとしたピアツーピアデータベースを使用するサービスが盛んに開発されている。例えば、仮想通貨のやり取りにブロックチェーンデータを使用するBitcoin等が挙げられる。ブロックチェーンデータをはじめとしたピアツーピアデータベースは、登録データの改ざん等を防ぎ、複数事業者によるノードの相互監視効果によって登録データを高い信頼度で保存することができる。

[0003] 特許文献１には、資格情報（アクセス資格認定資料）に基づいてピアツーピアデータベースへのアクセス制御を行う技術が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特開２００８－７２７１０号公報

発明の概要

発明が解決しようとする課題

[0005] ここで、特許文献１に記載の技術等によっては、ピアツーピアデータベースへのアクセスを適切に制御できない場合があった。より具体的には、ピアツーピアデータベースは基本的に登録データを削除できないため、あるユーザが大量のデータを登録すると、ピアツーピアデータベースのリソースが圧迫されてしまい、他のユーザがデータを登録できなくなる恐れがある。また、複数のノード装置間でコンセンサス（合意）が形成された後にピアツーピアデータベースへのデータ登録を行うという登録方式においては、一般的なリレーショナルデータベース等と比較してデータの登録により長い時間を要する。そのため、あるユーザが大量のデータの登録を要求した場合に、他の

ユーザがデータを登録できなくなる恐れがある。ここで、特許文献１に記載の技術等が用いられることで、資格情報（アクセス資格認定資料）に基づいてピアツーピアデータベースへアクセス可能なユーザが限定されたとしても、ピアツーピアデータベースへアクセス可能なユーザが大量のデータを登録した場合には、他のユーザがデータを登録できなくなる恐れがある。

[0006] そこで、本開示は、上記事情に鑑みてなされたものであり、ピアツーピアデータベースへのアクセスをより適切に制御することが可能な、新規かつ改良された情報処理装置、情報処理方法、およびプログラムを提供する。

課題を解決するための手段

[0007] 本開示によれば、任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御するアクセス制御部を備える、情報処理装置が提供される。

[0008] また、本開示によれば、任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御することを有する、コンピュータにより実行される情報処理方法が提供される。

[0009] また、本開示によれば、任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御することを、コンピュータに実現させるためのプログラムが提供される。

発明の効果

[0010] 以上説明したように本開示によれば、ピアツーピアデータベースへのアクセスをより適切に制御することが可能になる。

[0011] なお、上記の効果は必ずしも限定的なものではなく、上記の効果とともに、または上記の効果に代えて、本明細書に示されたいずれかの効果、または本明細書から把握され得る他の効果が奏されてもよい。

図面の簡単な説明

[0012] [図1]ピアツーピアデータベースの一種であるブロックチェーンデータの概要について説明する図である。

[図2]ピアツーピアデータベースの一種であるブロックチェーンデータの概要について説明する図である。

[図3]ピアツーピアデータベースの一種であるブロックチェーンデータの概要について説明する図である。

[図4]第１の実施形態に係る情報処理システムの構成例について説明する図である。

[図5]第１の実施形態に係るノード装置１００の機能構成例を示すブロック図である。

[図6]第１の実施形態に係るクライアント装置２００の機能構成例を示すブロック図である。

[図7]第１の実施形態に係る、Ｐ２Ｐデータベース１２０へのアクセス制御に関する処理の流れの一例を示すフローチャートである。

[図8]第２の実施形態に係るノード装置１００の機能構成例を示すブロック図である。

[図9]第２の実施形態に係る、Ｐ２Ｐデータベース１２０へのアクセス制御に関する処理の流れの一例を示すフローチャートである。

[図10]第１の実施形態、または第２の実施形態に係るノード装置１００、またはクライアント装置２００を実現する情報処理装置９００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

[0013] 以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

[0014] なお、説明は以下の順序で行うものとする。

１．ピアツーピアデータベースの概要

[0015] ＜１．ピアツーピアデータベースの概要＞

本開示の実施形態について説明する前に、まず、ピアツーピアデータベースの概要について説明する。

[0016] 本実施形態に係る情報処理システムでは、ピアツーピアネットワークに流通している分散型のピアツーピアデータベースが利用される。なお、ピアツーピアネットワークは、ピアツーピア型分散ファイルシステムと呼ばれる場合もある。以下では、ピアツーピアネットワークを「Ｐ２Ｐネットワーク」、ピアツーピアデータベースを「Ｐ２Ｐデータベース」と示す場合がある。Ｐ２Ｐデータベースの例として、Ｐ２Ｐネットワークに流通しているブロックチェーンデータが挙げられる。よって最初に、一例として、ブロックチェーンシステムの概要について説明する。

[0017] 図１に示すように、ブロックチェーンデータは、複数のブロックがあたかも鎖のように連なって含まれるデータである。それぞれのブロックには、１または２以上の対象データが、トランザクション（取引）として格納されうる。

[0018] ブロックチェーンデータとしては、例えば、Bitcoin等の仮想通貨のデータ

のやり取りに用いられるブロックチェーンデータが挙げられる。仮想通貨のデータのやり取りに用いられるブロックチェーンデータには、例えば、直前のブロックのハッシュと、ナンスと呼ばれる値が含まれる。直前のブロックのハッシュは、直前のブロックから正しく連なる、「正しいブロック」であるか否かを判定するために用いられる情報である。ナンスは、ハッシュを用いた認証においてなりすましを防ぐために用いられる情報であり、ナンスを用いることによって改ざんが防止される。ナンスとしては、例えば、文字列、数字列、あるいは、これらの組み合わせを示すデータ等が挙げられる。

[0019] また、ブロックチェーンデータでは、各トランザクションのデータに暗号鍵を用いた電子署名が付与されることによって、なりすましが防止される。また、各トランザクションのデータは公開され、Ｐ２Ｐネットワーク全体で共有される。なお、各トランザクションのデータは暗号鍵を用いて暗号化されてもよい。

[0020] 図２は、ブロックチェーンシステムにおいて、対象データがユーザＡによって登録される様子を示す図である。ユーザＡは、ブロックチェーンデータに登録する対象データに対して、ユーザＡの秘密鍵を用いて生成された電子署名を付する。そしてユーザＡは、電子署名が付された対象データを含むトランザクションをＰ２Ｐネットワーク上にブロードキャストする。これによって、対象データの保有者がユーザＡであることが担保される。

[0021] 図３は、ブロックチェーンシステムにおいて、対象データがユーザＡからユーザＢに移行される様子を示す図である。ユーザＡは、ユーザＡの秘密鍵を用いて生成した電子署名をトランザクションに付し、当該トランザクションにユーザＢの公開鍵を含める。これにより、対象データがユーザＡからユーザＢに移行されたことが示される。また、ユーザＢは、対象データの取引に際して、ユーザＡの公開鍵をユーザＡから取得し、電子署名が付された、または暗号化された対象データを取得してもよい。

[0022] また、ブロックチェーンシステムでは、例えばサイドチェイン技術を利用することによって、Bitcoinのブロックチェーンデータ等の、既存の仮想通貨

のデータのやり取りに用いられるブロックチェーンデータに、仮想通貨とは異なる他の対象データを含めることも可能である。

[0023] ＜２．第１の実施形態＞

上記では、Ｐ２Ｐデータベースの概要について説明した。続いて、本開示の第１の実施形態について説明する。

[0024] （２．１．概要）

まず、本開示の第１の実施形態の概要について説明する。

[0025] 上記のとおり、近年、ブロックチェーンデータをはじめとしたＰ２Ｐデータベースを使用するサービスが盛んに開発されている。そして、Ｐ２Ｐデータベースは、登録データの改ざん等を防ぎ、複数事業者によるノードの相互監視効果によって登録データを高い信頼度で保存することができる。

[0026] しかし、特許文献１に記載の技術等によっては、Ｐ２Ｐデータベースへのアクセスを適切に制御できない場合があった。例えば、特許文献１に記載の技術等によっては、Ｐ２Ｐデータベースへのデータの登録、およびＰ２Ｐデータベースからのデータの取得を含むＰ２Ｐデータベースへのアクセスの回数等を適切に制限することはできなかった。

[0027] ここで、Ｐ２Ｐデータベースは基本的に登録データを削除できないため、あるユーザが大量のデータを登録すると、Ｐ２Ｐデータベースのリソースが圧迫されてしまい、他のユーザがデータを登録できなくなる恐れがある。また、複数のノード装置間でコンセンサス（合意）が形成された後にＰ２Ｐデータベースへのデータ登録を行うという登録方式においては、一般的なリレーショナルデータベース等と比較してデータの登録により長い時間を要する。そのため、あるユーザが大量のデータの登録を要求した場合に、他のユーザがデータを登録できなくなる恐れがある。

[0028] そこで、本件の開示者は、上記事情に鑑みて本開示に係る技術を創作するに至った。本開示は、任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、当該主体によるＰ２Ｐデータベースへの新たなアクセスを制御することができる。以降では、本開示について詳細に説明し

ていく。

[0029] （２．２．システム構成例）

上記では、本実施形態の概要について説明した。続いて、図４を参照して、本実施形態に係る情報処理システムの構成例について説明する。

[0030] 図４に示すように、本実施形態に係る情報処理システムは、複数のノード装置１００（図中では、ノード装置１００ａ～ノード装置１００ｄ）と、クライアント装置２００と、を備える。また、複数のノード装置１００は、それぞれＰ２Ｐネットワーク３００に接続している。さらに、複数のノード装置１００のうちの一台（図中では、ノード装置１００ａ）とクライアント装置２００がネットワーク４００によって接続されている。

[0031] （ノード装置１００）

ノード装置１００は、Ｐ２Ｐネットワーク３００に接続しており、Ｐ２Ｐデータベースを保持している情報処理装置である。そして、ノード装置１００は、任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、当該主体によるＰ２Ｐデータベースへの新たなアクセスを制御することができる。例えば、ノード装置１００は、当該履歴情報に基づいて、Ｐ２Ｐデータベースへの新たなアクセスの可否を判断することができる。

[0032] ここで、「任意の主体」とは、ユーザ（例えば、本情報処理システムを利用するユーザ）、複数人のユーザによって構成されるグループ（例えば、組織、または団体等）、ユーザ等に使用されるクライアント装置２００、クライアント装置２００以外の外部装置、複数台の外部装置（またはクライアント装置２００）によって構成されるシステム、または外部装置（またはクライアント装置２００）によって用いられるソフトウェアのいずれかであることを想定しているが、これらに限定されない。例えば、「任意の主体」には、Ｐ２Ｐデータベースに対して何らかの処理を行うことができる有体物、または無体物が含まれ得る。以降では、主に、「任意の主体」がクライアント装置２００を使用するユーザである場合を一例として説明する。

[0033] また、「Ｐ２Ｐデータベースへのアクセス」とは、Ｐ２Ｐデータベースへ

のデータの登録、またはＰ２Ｐデータベースからのデータの取得のいずれかであることを想定しているが、これらに限定されない。より具体的には、「Ｐ２Ｐデータベースへのアクセス」には、Ｐ２Ｐデータベースに対して行われる何らかの処理が含まれ得る。

[0034] また、「Ｐ２Ｐデータベースへのアクセスに関する履歴情報」とは、過去に行われたＰ２Ｐデータベースへのアクセスの合計回数、所定の長さの期間（例えば１日間）におけるＰ２Ｐデータベースへのアクセスの合計回数（アクセスの頻度）、過去にＰ２Ｐデータベースへ登録されたデータ（または、過去にＰ２Ｐデータベースから取得されたデータ）の合計サイズ、または所定の長さの期間（例えば１日間）においてＰ２Ｐデータベースへ登録されたデータの合計サイズ（または、所定の長さの期間においてＰ２Ｐデータベースから取得されたデータの合計サイズ）のいずれかであることを想定しているが、これらに限定されない。なお、以降では便宜的に、「Ｐ２Ｐデータベースへのアクセスに関する履歴情報」を「アクセス履歴情報」とも呼称する。

[0035] ノード装置１００によるＰ２Ｐデータベースへのアクセス制御に関する処理については、後段でより詳細に説明する。

[0036] ここで、ノード装置１００がＰ２Ｐデータベースへアクセスする場合（すなわち、データの取得、または登録等を行う場合）には、ノード装置１００は、基本的に、Ｐ２Ｐデータベースに設けられ、Ｐ２Ｐデータベース上で実行される所定のプログラム（以降、便宜的に「Ｐ２Ｐデータベースプログラム」と呼称する）を用いる。Ｐ２Ｐデータベースプログラムが用いられることによって、例えば、Bitcoin等のような仮想通貨の取引を含む様々な処理が所定のルールに従って実現される。また、Ｐ２Ｐデータベースプログラムが Ｐ２Ｐデータベースに設けられることによって、当該プログラムが不正に改変されるリスクが低減される。

[0037] Ｐ２Ｐデータベースプログラムは、ハイパーレッジャー（Hyperledger）におけるチェーンコードであるが、これに限定されない。例えば、Ｐ２Ｐデー

タベースプログラムは、スマートコントラクトを指してもよい。なお、ノード装置１００は、適宜、Ｐ２Ｐデータベースプログラム以外のプログラムを用いて、Ｐ２Ｐデータベースへのアクセスを実現してもよい。

[0038] また、本実施形態では、複数のノード装置１００が同一の機能を有している場合を想定して説明するが、各ノード装置１００は、互いに異なる機能を有していてもよい。例えば、Ｐ２Ｐデータベースへのデータの登録を承認するノード装置１００（例えば、Endorsing Peer等）、承認後に各ノード装置１００に対して登録を指示するノード装置１００（例えば、Ordering Peer等）、Ｐ２Ｐデータベースにデータを登録するノード装置１００（例えば、Committing Peer等）が設けられてもよい。

[0039] なお、上記で説明したノード装置１００の処理内容は適宜変更され得る。また、ノード装置１００が備えるＰ２Ｐデータベースに登録されているデータの内容は特に限定されない。さらに、ノード装置１００の種類は特に限定されない。例えば、ノード装置１００は、汎用コンピュータ、ＰＣ（Personal
Computer）、またはタブレットＰＣ等を含む任意の装置であってよい。

[0040] （クライアント装置２００）

クライアント装置２００は、ノード装置１００に対してＰ２Ｐデータベースへのアクセスを要求するユーザが使用する情報処理装置である。例えば、ユーザは、Ｐ２Ｐデータベースへのデータの登録、またはＰ２Ｐデータベースからのデータの取得等を要求する旨の入力操作をクライアント装置２００に対して行う。すると、クライアント装置２００は、当該入力操作に基づいて要求信号を生成し、当該信号をノード装置１００へ送信することで、Ｐ２Ｐデータベースへのデータの登録、またはＰ２Ｐデータベースからのデータの取得を実現する。

[0041] また、クライアント装置２００は、要求に基づく処理の結果に関する情報（以降、便宜的に「要求結果情報」とも呼称する）をノード装置１００から受信した場合、当該情報をユーザに提供することができる。より具体的には

、クライアント装置２００は、ユーザインタフェースとして機能する出力部（例えば、ディスプレイ等の表示装置、スピーカ等の音声出力装置、ランプ等の光源装置、またはアクチュエータ等の触覚提示装置等）を介して、要求結果情報をユーザへ提供することができる。

[0042] なお、上記で説明したクライアント装置２００の処理内容は適宜変更され得る。また、ノード装置１００と同様に、クライアント装置２００の種類は特に限定されない。また、クライアント装置２００は、ノード装置１００と通信可能な任意の外部装置（例えば、サーバ装置等）に置き換えられてもよい。

[0043] （Ｐ２Ｐネットワーク３００）

Ｐ２Ｐネットワーク３００は、Ｐ２Ｐデータベースが流通しているネットワークである。上記のとおり、各ノード装置１００は、Ｐ２Ｐネットワーク３００に接続することで、他のノード装置１００が保持するＰ２Ｐデータベースと整合性を保ちながら、Ｐ２Ｐデータベースを更新することができる。

[0044] なお、Ｐ２Ｐネットワーク３００の種類は特に限定されない。例えば、Ｐ２Ｐネットワーク３００は、複数組織によって運営されるコンソーシアム型、単一組織によって運営されるプライベート型、または、参加者を特に限定しないパブリック型のうちのいずれの種類であってもよい。

[0045] なお、Ｐ２Ｐネットワーク３００に用いられる通信方式、または回線の種類等は特に限定されない。例えば、Ｐ２Ｐネットワーク３００は、ＩＰ－ＶＰＮ（Internet Protocol-Virtual Private Network）等の専用回線網で実現されてもよい。また、Ｐ２Ｐネットワーク３００は、インターネット、電話回線網、衛星通信網などの公衆回線網で実現されてもよい。また、Ｐ２Ｐネットワーク３００は、Ｅｔｈｅｒｎｅｔ（登録商標）を含む各種のＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等で実現されてもよい。さらに、Ｐ２Ｐネットワーク３００は、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）等の無線通信網で実現されてもよい。

[0046] （ネットワーク４００）

ネットワーク４００は、ノード装置１００、およびクライアント装置２００間を接続するネットワークである。なお、Ｐ２Ｐネットワーク３００と同様に、ネットワーク４００に用いられる通信方式、または回線の種類等は特に限定されない。

[0047] 以上、本実施形態に係る情報処理システムの構成例について説明した。なお、図４を参照して説明した上記の構成はあくまで一例であり、本実施形態に係る情報処理システムの構成は係る例に限定されない。例えば、ノード装置１００の機能の全部または一部が、クライアント装置２００に備えられてもよい。より具体的には、ノード装置１００の機能の全部または一部を提供するソフトウェアがクライアント装置２００上で実行されてもよい。また、逆に、クライアント装置２００の機能の全部または一部が、ノード装置１００に備えられてもよい。また、情報処理システムを構成する各装置の台数は適宜変更されてもよい。また、本実施形態に係る情報処理システムが提供可能なサービスの内容は特に限定されない。本実施形態に係る情報処理システムの構成は、仕様や運用に応じて柔軟に変形可能である。

[0048] （２．３．ノード装置１００の機能構成例）

上記では、本実施形態に係る情報処理システムの構成例について説明した。続いて、図５を参照して、ノード装置１００の機能構成例について説明する。

[0049] 図５に示すように、ノード装置１００は、制御部１１０と、Ｐ２Ｐデータベース１２０と、通信部１３０と、を備える。

[0050] （制御部１１０）

制御部１１０は、ノード装置１００が行う処理全般を統括的に制御する機能構成である。例えば、制御部１１０は、制御信号を用いて出力部（図示なし）、または通信部１３０等の起動や停止を制御することができる。また、制御部１１０は、Ｐ２Ｐデータベース１２０へのアクセスについての要求結果情報を含む応答信号（なお、クライアント装置２００からの要求の内容が、Ｐ２Ｐデータベース１２０からのデータの取得である場合には、取得され

たデータも応答信号に含まれる）を生成し、通信部１３０を介して当該信号をクライアント装置２００へ送信する。なお、制御部１１０の制御内容はこれらに限定されない。例えば、制御部１１０は、各種サーバ、汎用コンピュータ、ＰＣ、またはタブレットＰＣ等において一般的に行われる処理を制御してもよい。

[0051] （Ｐ２Ｐデータベース１２０）

Ｐ２Ｐデータベース１２０は、ノード装置１００に保持されるデータベースであり、例えば、ブロックチェーンデータである。上記のとおり、Ｐ２Ｐデータベース１２０には、真正性の担保が求められるようなより重要度の高いデータが登録される。Ｐ２Ｐデータベース１２０に登録される各種データは、暗号鍵を用いて生成された電子署名を付されたり、または暗号鍵を用いて暗号化されたりしてもよい。なお、上記のとおり、Ｐ２Ｐデータベース１２０に登録されるデータの内容は特に限定されない。例えば、Ｐ２Ｐデータベース１２０へのデータの登録、またはＰ２Ｐデータベース１２０からのデータの取得の際に課金が行われる場合には、Ｐ２Ｐデータベース１２０には、各ユーザが有する資産（例えば、Bitcoinにおけるコイン等）に関するデータが登録されていてもよい。また、図５に示すように、Ｐ２Ｐデータベース１２０は、Ｐ２Ｐデータベースプログラム１２１を備える。

[0052] （Ｐ２Ｐデータベースプログラム１２１）

Ｐ２Ｐデータベースプログラム１２１は、Ｐ２Ｐデータベース１２０に備えられ、Ｐ２Ｐデータベース１２０上で実行される所定のプログラムである。上記のとおり、Ｐ２Ｐデータベースプログラム１２１が用いられることによって、例えば、Bitcoin等のような仮想通貨の取引を含む様々な処理が所定のルールに従って一貫性を保ちつつ実現される。また、Ｐ２Ｐデータベースプログラム１２１がＰ２Ｐデータベース１２０に設けられることによって当該プログラムが不正に改変されるリスクが低減される。また、上記のとおり、Ｐ２Ｐデータベースプログラム１２１は、ハイパーレッジャー（Hyperledger）におけるチェーンコードであってもよいが、スマートコントラクトであ

ってもよい。

[0053] Ｐ２Ｐデータベースプログラム１２１は、Ｐ２Ｐデータベース１２０に対して行われる処理全般を実現することができる。例えば、図５に示すように、Ｐ２Ｐデータベースプログラム１２１は、履歴取得部１２１ａと、アクセス制御部１２１ｂと、を備え、これらを制御することでＰ２Ｐデータベース１２０へのアクセスに関する処理全般を実現することができる。なお、Ｐ２Ｐデータベースプログラム１２１によって実現される処理はこれに限定されない。また、Ｐ２Ｐデータベースプログラム１２１の開発言語、またはＰ２Ｐデータベース１２０上に設けられるＰ２Ｐデータベースプログラム１２１の個数等は特に限定されない。

[0054] （履歴取得部１２１ａ）

履歴取得部１２１ａは、Ｐ２Ｐデータベース１２０へのアクセス制御に用いられるアクセス履歴情報を取得する機能構成である。より具体的には、クライアント装置２００からのＰ２Ｐデータベース１２０へのアクセスを要求する要求信号が受信された場合、その都度、履歴取得部１２１ａは、過去に当該ユーザによって行われたＰ２Ｐデータベース１２０へのアクセスについてのアクセス履歴情報を集計する。例えば、履歴取得部１２１ａは、当該ユーザの識別情報（例えば、ユーザＩＤ、または公開鍵情報等）に基づいてＰ２Ｐデータベース１２０に登録されているデータの中から、過去に当該ユーザによって登録されたデータを抽出し、登録回数を集計することで登録回数の合計値を出力する。ここで、過去に行われたＰ２Ｐデータベース１２０への複数回のアクセスそれぞれに関する履歴情報（アクセス履歴情報）を「第１の履歴情報」とも呼称し、第１の履歴情報を集計することで得られたアクセス履歴情報を「第２の履歴情報」とも呼称する。すなわち、本実施形態に係る履歴取得部１２１ａは、クライアント装置２００からの要求信号が受信される都度、Ｐ２Ｐデータベース１２０に登録されているデータに基づいて第１の履歴情報を抽出し、第１の履歴情報を用いて第２の履歴情報を出力する。

[0055] なお、第２の履歴情報は、上記とおり、過去に行われたＰ２Ｐデータベース１２０へのアクセスの合計回数、所定の長さの期間（例えば１日間）におけるＰ２Ｐデータベース１２０へのアクセスの合計回数（またはアクセスの頻度）、過去にＰ２Ｐデータベース１２０へ登録されたデータ（または、過去にＰ２Ｐデータベース１２０から取得されたデータ）の合計サイズ、または所定の長さの期間（例えば１日間）においてＰ２Ｐデータベース１２０へ登録されたデータの合計サイズ（または、所定の長さの期間においてＰ２Ｐデータベース１２０から取得されたデータの合計サイズ）のいずれかであることを想定しているが、これらに限定されない。

[0056] なお、上記では、履歴取得部１２１ａが、Ｐ２Ｐデータベース１２０に登録されているデータに基づいて第１の履歴情報を抽出する旨を説明したが、第１の履歴情報の抽出方法はこれに限定されない。例えば、第１の履歴情報を管理している記憶部、または外部装置等が存在する場合には、履歴取得部１２１ａは、当該記憶部、または外部装置等から第１の履歴情報を取得してもよい。

[0057] 履歴取得部１２１ａは、出力した第２の履歴情報をアクセス制御部１２１ｂへ提供することで、アクセス制御部１２１ｂが第２の履歴情報を用いて、当該ユーザによるＰ２Ｐデータベース１２０への新たなアクセスを制御することを可能にする。なお、履歴取得部１２１ａは、第１の履歴情報をアクセス制御部１２１ｂへ提供してもよい。

[0058] （アクセス制御部１２１ｂ）

アクセス制御部１２１ｂは、アクセス履歴情報に基づいて、Ｐ２Ｐデータベース１２０への新たなアクセスを制御する機能構成である。例えば、アクセス制御部１２１ｂは、アクセス履歴情報に基づいてＰ２Ｐデータベース１２０への新たなアクセスの可否を判断する。

[0059] より具体的に説明すると、クライアント装置２００からのＰ２Ｐデータベース１２０へのアクセスを要求する要求信号が受信された場合、アクセス制御部１２１ｂは、履歴取得部１２１ａから提供された第２の履歴情報と所定

の閾値とを比較すること等によってＰ２Ｐデータベース１２０への新たなアクセスの可否を判断する。例えば、アクセス制御部１２１ｂは、第２の履歴情報である、所定の長さの期間（例えば１日間）におけるＰ２Ｐデータベース１２０へのアクセスの合計回数と、所定の閾値とを比較することで、当該閾値を超えるアクセスを禁止することができる。

[0060] また、アクセス制御部１２１ｂは、Ｐ２Ｐデータベース１２０へのアクセス（データの登録、またはデータの取得等）の対象となるデータの種別、またはアクセスを行うユーザ（または主体）の種別等に応じて、Ｐ２Ｐデータベース１２０への新たなアクセスを制御してもよい（換言すると、アクセス制御部１２１ｂは、データの種別、またはユーザの種別に応じてＰ２Ｐデータベース１２０への新たなアクセスの制御ロジックを変更してもよい）。

[0061] ここで、「データの種別」とは、Ｐ２Ｐデータベース１２０へのアクセスの対象となるデータのカテゴリ、内容、用途、または当該データの取得装置等であることを想定しているが、必ずしもこれらに限定されない。例えば、「データの種別」とは、データに関する何らかのメタ情報等を含む。これによって、アクセス制御部１２１ｂは、例えば、カテゴリが「温度データ」であるデータと「脈拍データ」であるデータとで、登録可能な回数を異なる値にしてもよい。また、アクセス制御部１２１ｂは、例えば、装置Ａにより取得されたデータと装置Ｂにより取得されたデータとで、登録可能な回数を異なる値にしてもよい。

[0062] また、「ユーザ（主体）の種別」とは、Ｐ２Ｐデータベース１２０へのアクセスを要求しているユーザ（主体）が有する権限（例えば、管理者権限、プレミアムユーザ権限、または一般ユーザ権限等）、役割（例えば、投稿者、読者、先生、または生徒等）、属性（例えば、年齢、性別、または職業等）、またはユーザに対する評価等（例えば、成績等）であることを想定しているが、必ずしもこれらに限定されない。例えば、「ユーザ（主体）の種別」とは、ユーザ（主体）に関する何らかのメタ情報等を含む。これによって、アクセス制御部１２１ｂは、例えば、「プレミアムユーザ権限」を有する

ユーザからのデータと「一般ユーザ権限」を有するユーザからのデータとで、登録可能な回数を異なる値にしてもよい。上記によって、アクセス制御部１２１ｂは、Ｐ２Ｐデータベース１２０へのアクセスをより細かく制御することができる。

[0063] なお、アクセス制御部１２１ｂによるアクセス制御の方法は上記に限定されず、アクセス制御部１２１ｂは、様々な制御ロジックを用いてＰ２Ｐデータベース１２０へのアクセス制御を行うことができる。例えば、アクセス制御部１２１ｂは、Ｐ２Ｐデータベース１２０へのアクセス状況に基づいてアクセス制御のための制御ロジックを変更してもよい。より具体的には、アクセス制御部１２１ｂは、所定の方法でＰ２Ｐデータベース１２０へのアクセスの混雑状況等を認識し、アクセスが多い場合ほど、アクセスをより制限するように制御ロジックを変更してもよい（例えば上記で説明した所定の閾値を変更する等）。

[0064] また、アクセス制御部１２１ｂは、第２の履歴情報ではなく、第１の履歴情報（すなわち集計前のアクセス履歴情報）を用いてＰ２Ｐデータベース１２０へのアクセス制御を行ってもよい。また、アクセス制御部１２１ｂは、Ｐ２Ｐデータベース１２０へのアクセス制御に関する処理の全部または一部を、公知の機械学習技術または人工知能を用いて実現してもよい。

[0065] （通信部１３０）

通信部１３０は、クライアント装置２００との各種通信を行う機能構成である。例えば、通信部１３０は、Ｐ２Ｐデータベース１２０へのデータの登録を要求する要求信号をクライアント装置２００から受信し、要求結果情報等を含む応答信号をクライアント装置２００へ送信する。また、通信部１３０は、Ｐ２Ｐデータベース１２０からのデータの取得を要求する要求信号をクライアント装置２００から受信し、Ｐ２Ｐデータベース１２０から取得されたデータ、および要求結果情報等を含む応答信号をクライアント装置２００へ送信する。

[0066] また、通信部１３０は、ノード装置１００との各種通信も行う。例えば、

通信部１３０は、他のノード装置１００との通信において、Ｐ２Ｐデータベース１２０の更新に用いられる情報等（例えば、合意形成に用いられる情報等）を適宜送受信する。なお、通信部１３０が通信するデータ、および通信するケースはこれらに限定されない。

[0067] 以上、ノード装置１００の機能構成例について説明した。なお、図５を用いて説明した上記の機能構成はあくまで一例であり、ノード装置１００の機能構成は係る例に限定されない。例えば、ノード装置１００は、図５に示す構成の全てを必ずしも備えなくてもよい。また、Ｐ２Ｐネットワーク３００に接続している複数のノード装置１００は、互いに異なる機能構成を備えていてもよい。また、上記で説明した履歴取得部１２１ａ、またはアクセス制御部１２１ｂは、Ｐ２Ｐデータベースプログラム１２１以外に備えられてもよい。例えば、履歴取得部１２１ａ、またはアクセス制御部１２１ｂは、制御部１１０に備えられてもよい。また、図５には示していないが、ノード装置１００は、Ｐ２Ｐデータベース１２０以外の記憶部を別途備えていてもよい。そして、当該記憶部は、ノード装置１００の各機能構成によって使用されるプログラム、またはパラメータ等を記憶できてもよい。なお、当該記憶部が記憶する情報の内容はこれらに限定されない。ノード装置１００の機能構成は、仕様や運用に応じて柔軟に変形可能である。

[0068] （２．４．クライアント装置２００の機能構成例）

上記では、ノード装置１００の機能構成例について説明した。続いて、図６を参照して、クライアント装置２００の機能構成例について説明する。

[0069] 図６に示すように、クライアント装置２００は、制御部２１０と、入力部２２０と、出力部２３０と、記憶部２４０と、通信部２５０と、を備える。

[0070] （制御部２１０）

制御部２１０は、クライアント装置２００が行う処理全般を統括的に制御する機能構成である。例えば、制御部２１０は、制御信号を用いて入力部２２０、出力部２３０、または通信部２５０等の起動や停止を制御することができる。また、制御部２１０は、Ｐ２Ｐデータベース１２０へのアクセスを

要求する要求信号を生成する。また、要求結果情報等を含む応答信号がノード装置１００から提供された場合には、制御部２１０は当該情報の出力を制御する。なお、制御部２１０の制御内容はこれらに限定されない。例えば、制御部２１０は、各種サーバ、汎用コンピュータ、ＰＣ、またはタブレットＰＣ等において一般的に行われる処理を制御してもよい。

[0071] （入力部２２０）

入力部２２０は、ユーザによる入力を受ける機能構成である。例えば、入力部２２０はマウス、キーボード、タッチパネル、ボタン、スイッチ、またはマイクロフォン等の入力装置を備えており、ユーザがこれらの入力装置を用いることによって、Ｐ２Ｐデータベース１２０へのアクセスの要求等のための入力操作を行うことができる。例えば、ユーザは、これらの入力装置を用いることで、Ｐ２Ｐデータベース１２０へ登録するためのデータを作成することができる。なお、入力部２２０が備える入力装置は特に限定されない。

[0072] （出力部２３０）

出力部２３０は、制御部２１０によって制御されることで各種情報の出力を行う機能構成である。例えば、出力部２３０は、ディスプレイ等の表示装置、スピーカ等の音声出力装置、ランプ等の光源装置、またはアクチュエータ等の触覚提示装置等を備えており、制御部２１０による制御に基づいて、ノード装置１００から提供された要求結果情報等をユーザへ出力する。すなわち、出力部２３０はユーザインタフェースとして機能する。なお、出力部２３０が備える出力装置はこれらに限定されない。

[0073] （記憶部２４０）

記憶部２４０は、各種情報を記憶する機能構成である。例えば、記憶部２４０は、Ｐ２Ｐデータベース１２０へ登録される対象のデータ、Ｐ２Ｐデータベース１２０から取得されたデータ、または要求結果情報等を記憶したり、クライアント装置２００の各機能構成によって使用されるプログラム、またはパラメータ等を記憶したりする。なお、記憶部２４０が記憶する情報は

これらに限定されない。

[0074] （通信部２５０）

通信部２５０は、ノード装置１００との各種通信を行う機能構成である。例えば、通信部２５０は、Ｐ２Ｐデータベース１２０へのデータの登録を要求する要求信号をノード装置１００へ送信し、要求結果情報等を含む応答信号をノード装置１００から受信する。また、通信部２５０は、Ｐ２Ｐデータベース１２０からのデータの取得を要求する要求信号をノード装置１００へ送信し、Ｐ２Ｐデータベース１２０から取得されたデータ、および要求結果情報等を含む応答信号をノード装置１００から受信する。なお、通信部２５０が通信するデータ、および通信するケースはこれらに限定されない。

[0075] 以上、クライアント装置２００の機能構成例について説明した。なお、図６を用いて説明した上記の機能構成はあくまで一例であり、クライアント装置２００の機能構成は係る例に限定されない。例えば、クライアント装置２００は、図６に示す構成の全てを必ずしも備えなくてもよい。また、クライアント装置２００の機能構成は、仕様や運用に応じて柔軟に変形可能である。

[0076] （２．５．処理の流れ）

上記では、クライアント装置２００の機能構成例について説明した。続いて、図７を参照して、Ｐ２Ｐデータベース１２０へのアクセス制御に関する処理の流れについて説明する。図７は、Ｐ２Ｐデータベース１２０へのデータ登録の際に行われるアクセス制御に関する処理の一例を示すフローチャートである。

[0077] ステップＳ１０００では、ノード装置１００の通信部１３０が、Ｐ２Ｐデータベース１２０へのデータの登録を要求する要求信号をクライアント装置２００から受信する。ステップＳ１００４では、履歴取得部１２１ａがアクセス履歴情報（第２の履歴情報）を取得する。ステップＳ１００８では、アクセス制御部１２１ｂが、アクセス履歴情報に基づいてＰ２Ｐデータベース１２０へのデータ登録の可否を判断する。例えば、アクセス制御部１２１ｂ

は、アクセス履歴情報である、所定の長さの期間（例えば１日間）におけるＰ２Ｐデータベース１２０へのデータ登録の合計回数と所定の閾値とを比較することで、新たなデータ登録の可否を判断する。

[0078] アクセス履歴情報に基づいてＰ２Ｐデータベース１２０へのデータ登録の条件が満たされていると判断された場合（ステップＳ１０１２／Ｙｅｓ）、ステップＳ１０１６にて、アクセス制御部１２１ｂが、Ｐ２Ｐデータベース１２０へデータを登録する。ステップＳ１０２０では、制御部１１０が、データ登録に成功した旨の要求結果情報を含む応答信号を生成し、通信部１３０を介して当該信号をクライアント装置２００へ送信することで一連の処理が終了する。なお、ステップＳ１０１２にて、アクセス履歴情報に基づいてＰ２Ｐデータベース１２０へのデータ登録の条件が満たされていないと判断された場合（ステップＳ１０１２／Ｎｏ）、データ登録が行われることなく、ステップＳ１０２０にて、制御部１１０が、データ登録に失敗した旨の要求結果情報を含む応答信号を生成し、通信部１３０を介して当該信号をクライアント装置２００へ送信する。

[0079] なお、図７のフローチャートにおける各ステップは、必ずしも記載された順序に沿って時系列に処理される必要はない。すなわち、フローチャートにおける各ステップは、記載された順序と異なる順序で処理されても、並列的に処理されてもよい。

[0080] ＜３．第２の実施形態＞

上記では、本開示の第１の実施形態について説明した。続いて、本開示の第２の実施形態について説明する。

[0081] 本開示の第１の実施形態に係るノード装置１００は、クライアント装置２００からの要求信号が受信された場合、その都度、過去に行われたＰ２Ｐデータベース１２０へのアクセスを集計することで第２の履歴情報を出力していた。一方、本開示の第２の実施形態に係るノード装置１００は、過去に行われたＰ２Ｐデータベース１２０へのアクセスを事前に集計することで第２の履歴情報を出力し、当該第２の履歴情報をＰ２Ｐデータベース１２０に登

録しておく。そして、ノード装置１００は、クライアント装置２００からの要求信号を受信した場合、事前に出力されＰ２Ｐデータベース１２０に登録されている第２の履歴情報を用いて、Ｐ２Ｐデータベース１２０への新たなアクセスを制御する。これによって、ノード装置１００は、クライアント装置２００からの要求信号が受信されてからＰ２Ｐデータベース１２０へのアクセス制御を行う（アクセスの可否を判断する）までに要する時間を短縮することができる。

[0082] （３．１．ノード装置１００の機能構成例）

続いて、図８を参照して、本実施形態に係るノード装置１００の機能構成例について説明する。なお、以降では、第１の実施形態に係る機能構成と同様の内容についての説明を省略する。また、クライアント装置２００の機能構成は、上記で説明した第１の実施形態に係る機能構成と同様であり得るため説明を省略する。

[0083] 図８に示すように、本実施形態に係るノード装置１００のＰ２Ｐデータベースプログラム１２１は、第１の実施形態に係る機能構成と比較して、新たに履歴登録部１２１ｃを備える。

[0084] （履歴取得部１２１ａ）

第１の実施形態に係る履歴取得部１２１ａは、クライアント装置２００からの要求信号が受信される都度、過去に行われたＰ２Ｐデータベース１２０へのアクセスについての履歴情報（第１の履歴情報）を集計することで第２の履歴情報を出力していた。一方、本実施形態に係る履歴取得部１２１ａは、クライアント装置２００からの要求信号の受信に先立って事前に第２の履歴情報を出力しておく。

[0085] 履歴取得部１２１ａが第２の履歴情報を出力するタイミング、またはトリガは特に限定されない。例えば、履歴取得部１２１ａは、同一のユーザ（主体）による直前のアクセス発生時に第２の履歴情報を出力してもよい。より具体的には、履歴取得部１２１ａは、Ｐ２Ｐデータベース１２０へのアクセスが発生した場合に、過去に出力した第２の履歴情報を次のアクセスの発生

に備えて更新してもよい。また、履歴取得部１２１ａは、定期的に第２の履歴情報を出力してもよい。また、履歴取得部１２１ａは、ノード装置１００の管理者からの入力操作（指示）をトリガに第２の履歴情報を出力してもよい。

[0086] 履歴取得部１２１ａは、出力した第２の履歴情報を履歴登録部１２１ｃへ提供する。

[0087] （履歴登録部１２１ｃ）

履歴登録部１２１ｃは、第２の履歴情報をＰ２Ｐデータベース１２０へ登録する機能構成である。より具体的には、履歴登録部１２１ｃは、履歴取得部１２１ａから第２の履歴情報を提供された場合に、当該第２の履歴情報をＰ２Ｐデータベース１２０へ登録する。これによって、第２の履歴情報の真正性が担保される。

[0088] なお、履歴登録部１２１ｃは、履歴取得部１２１ａから第２の履歴情報を提供された場合に、必ずしも、当該第２の履歴情報をＰ２Ｐデータベース１２０へ登録しなくてもよい。例えば、履歴登録部１２１ｃは、履歴取得部１２１ａから提供された第２の履歴情報を分析することで、対象のユーザ（主体）によるＰ２Ｐデータベース１２０への新たなアクセスが制限される条件を満たしたと判断した場合にのみ、当該第２の履歴情報をＰ２Ｐデータベース１２０へ登録してもよい。これによって、履歴登録部１２１ｃは、Ｐ２Ｐデータベース１２０へのアクセス可否の判断に影響を及ぼさない履歴情報がＰ２Ｐデータベース１２０へ登録されることを防ぐことができる。

[0089] （３．２．処理の流れ）

上記では、本実施形態に係るノード装置１００の機能構成例について説明した。続いて、図９を参照して、本実施形態における、Ｐ２Ｐデータベース１２０へのアクセス制御に関する処理の流れについて説明する。図９は、Ｐ２Ｐデータベース１２０へのデータ登録の際に行われるアクセス制御に関する処理の一例を示すフローチャートである。

[0090] ステップＳ１１００では、履歴取得部１２１ａが、過去に行われたＰ２Ｐ

データベース１２０へのアクセスを事前に集計することでアクセス履歴情報（第２の履歴情報）を出力する。ステップＳ１１０４では、履歴登録部１２１ｃが当該アクセス履歴情報をＰ２Ｐデータベース１２０に登録しておく。

[0091] その後、ステップＳ１１０８にて、通信部１３０が、Ｐ２Ｐデータベース１２０へのデータの登録を要求する要求信号をクライアント装置２００から受信すると、ステップＳ１１１２にて、履歴取得部１２１ａがアクセス履歴情報をＰ２Ｐデータベース１２０から取得する。ステップＳ１１１６では、アクセス制御部１２１ｂが、アクセス履歴情報に基づいてＰ２Ｐデータベース１２０へのデータ登録の可否を判断する。

[0092] アクセス履歴情報に基づいてＰ２Ｐデータベース１２０へのデータ登録の条件が満たされていると判断された場合（ステップＳ１１２０／Ｙｅｓ）、ステップＳ１１２４にて、アクセス制御部１２１ｂが、Ｐ２Ｐデータベース１２０へデータを登録する。ステップＳ１１２８では、制御部１１０が、データ登録に成功した旨の要求結果情報を含む応答信号を生成し、通信部１３０を介して当該信号をクライアント装置２００へ送信することで一連の処理が終了する。なお、ステップＳ１１２０にて、アクセス履歴情報に基づいてＰ２Ｐデータベース１２０へのデータ登録の条件が満たされていないと判断された場合（ステップＳ１１２０／Ｎｏ）、データ登録が行われることなく、ステップＳ１１２８にて、制御部１１０が、データ登録に失敗した旨の要求結果情報を含む応答信号を生成し、通信部１３０を介して当該信号をクライアント装置２００へ送信する。

[0093] なお、図９のフローチャートにおける各ステップは、必ずしも記載された順序に沿って時系列に処理される必要はない。すなわち、フローチャートにおける各ステップは、記載された順序と異なる順序で処理されても、並列的に処理されてもよい。

[0094] ＜４．ハードウェア構成例＞

上記では、本開示の第２の実施形態について説明した。続いて、図１０を参照して、各装置のハードウェア構成について説明する。

[0095] 図１０は、第１の実施形態、または第２の実施形態に係るノード装置１００、またはクライアント装置２００のハードウェア構成の一例を示すブロック図である。これらの装置は、図１０に示す情報処理装置９００によって具現され得る。

[0096] 情報処理装置９００は、例えば、ＭＰＵ９０１と、ＲＯＭ９０２と、ＲＡＭ９０３と、記録媒体９０４と、入出力インタフェース９０５と、操作入力デバイス９０６と、表示デバイス９０７と、通信インタフェース９０８とを備える。また、情報処理装置９００は、例えば、データの伝送路としてのバス９０９で各構成要素間を接続する。

[0097] ＭＰＵ９０１は、例えば、ＭＰＵなどの演算回路で構成される、１または２以上のプロセッサや、各種処理回路などで構成され、ノード装置１００の制御部１１０、またはクライアント装置２００の制御部２１０として機能する。なお、これらの機能構成は、上記で説明した各種処理を実現可能な専用の（または汎用の）回路（例えば、ＭＰＵ９０１とは別体のプロセッサなど）で構成されていてもよい。

[0098] ＲＯＭ９０２は、ＭＰＵ９０１が使用するプログラムや演算パラメータなどの制御用データなどを記憶する。ＲＡＭ９０３は、例えば、ＭＰＵ９０１により実行されるプログラムなどを一時的に記憶する。

[0099] 記録媒体９０４は、ノード装置１００のＰ２Ｐデータベース１２０、またはクライアント装置２００の記憶部２４０として機能し、各実施形態に係る情報処理に関するデータや各種プログラムなど様々なデータを記憶する。ここで、記録媒体９０４としては、例えば、ハードディスクなどの磁気記録媒体や、フラッシュメモリなどの不揮発性メモリが挙げられる。また、記録媒体９０４は、情報処理装置９００から着脱可能であってもよい。

[0100] 入出力インタフェース９０５は、例えば、操作入力デバイス９０６や、表示デバイス９０７を接続する。ここで、入出力インタフェース９０５としては、例えば、ＵＳＢ（Universal Serial Bus）端子や、ＤＶＩ（Digital Visual Interface）端子、ＨＤＭＩ（High-Definition Multimedia Inter

face）（登録商標）端子、各種処理回路などが挙げられる。

[0101] また、操作入力デバイス９０６は、例えば、情報処理装置９００上に備えられ、情報処理装置９００の内部で入出力インタフェース９０５と接続される。操作入力デバイス９０６としては、例えば、キーボード、マウス、キーパッド、タッチパネル、マイクロホン、操作ボタン、方向キーまたはジョグダイヤルなどの回転型セレクタ、あるいは、これらの組み合わせなどが挙げられる。操作入力デバイス９０６は、クライアント装置２００の入力部２２０として機能する。

[0102] また、表示デバイス９０７は、例えば、情報処理装置９００上に備えられ、情報処理装置９００の内部で入出力インタフェース９０５と接続される。表示デバイス９０７としては、例えば、液晶ディスプレイ（Liquid Crystal Display）や有機ＥＬディスプレイ（Organic Electro-Luminescence Display）などが挙げられる。表示デバイス９０７は、クライアント装置２００の出力部２３０として機能する。

[0103] なお、入出力インタフェース９０５が、情報処理装置９００の外部の操作入力デバイスや外部の表示デバイスなどの外部デバイスと接続することも可能であることは、言うまでもない。また、表示デバイス９０７は、例えばタッチパネルなど、表示とユーザ操作とが可能なデバイスであってもよい。

[0104] 通信インタフェース９０８は、情報処理装置９００が備える通信手段であり、ノード装置１００の通信部１３０、またはクライアント装置２００の通信部２５０として機能する。また、通信インタフェース９０８は、任意のネットワークを介して（あるいは、直接的に）、例えば、サーバなどの任意の外部装置と、無線または有線で通信を行う機能を有していてもよい。ここで、通信インタフェース９０８としては、例えば、通信アンテナおよびＲＦ（Radio Frequency）回路（無線通信）や、ＩＥＥＥ８０２．１５．１ポートおよび送受信回路（無線通信）、ＩＥＥＥ８０２．１１ポートおよび送受信回路（無線通信）、あるいはＬＡＮ（Local Area Network）端子および送受信回路（有線通信）などが挙げられる。

[0105] なお、情報処理装置９００のハードウェア構成は、図１０に示す構成に限られない。例えば、情報処理装置９００は、接続されている外部の通信デバイスを介して通信を行う場合には、通信インタフェース９０８を備えていなくてもよい。また、通信インタフェース９０８は、複数の通信方式によって通信を行うことが可能な構成であってもよい。また、情報処理装置９００は、例えば、操作入力デバイス９０６または表示デバイス９０７等を備えなくてもよい。また、例えば、図１０に示す構成の一部または全部は、１または２以上のＩＣ（Integrated Circuit）で実現されてもよい。

[0106] ＜５．備考＞

上記では、ノード装置１００が、アクセス履歴情報に基づいてユーザ（すなわち主体）によるＰ２Ｐデータベース１２０へのアクセスを制御する旨について説明してきた。ここで、仮に、ユーザがＰ２Ｐデータベース１２０へのアクセスを許可されなかった場合の対応について説明する。

[0107] 当該対応については様々な態様が考えられるところ、例えば、Ｐ２Ｐデータベース１２０へのアクセスを許可されなかったユーザは、所定の方法でノード装置１００（または情報処理システム）の管理者から承認を得ることによってＰ２Ｐデータベース１２０へのアクセスを許可されてもよい。この場合、クライアント装置２００は、管理者から提供された許可情報を要求信号に含めることで、ノード装置１００は、当該許可情報に基づいてＰ２Ｐデータベース１２０へのアクセスを許可する。

[0108] また、Ｐ２Ｐデータベース１２０へのアクセスを許可されなかったユーザは、所定の料金を支払うことによってＰ２Ｐデータベース１２０へのアクセスを許可されてもよい。この場合、所定の料金の支払いは、Ｐ２Ｐデータベース１２０によって管理されているユーザの資産（例えば、Bitcoinにおけるコイン等）に関するデータによって実現されてもよい。

[0109] また、Ｐ２Ｐデータベース１２０へのアクセスが重要であり、かつ、急を要することを示すフラグ情報が設けられてもよい。より具体的には、Ｐ２Ｐデータベース１２０へのアクセスを許可されなかったユーザが、当該フラグ

情報を要求信号に含めることによって、例外的にＰ２Ｐデータベース１２０へのアクセスが許可されてもよい。例えば、この方式は、人命に関わる事件、または災害の発生時に有用であると考えられる。

[0110] また、ユーザによるＰ２Ｐデータベース１２０へのアクセスが許可されなかった場合、ノード装置１００は、アクセス可能な条件（例えば、アクセス可能なデータの種別、ユーザ（主体）の種別、データのサイズ、または次にアクセス可能なタイミング等）をユーザに対して通知してもよい。なお、仮に、ユーザによるＰ２Ｐデータベース１２０へのアクセスが許可された場合であっても、ノード装置１００は、その後のアクセスについての条件（例えば、許容されるアクセス回数の残存値（換言すると、あと何回アクセス可能か、という情報）等）をユーザに対して通知してもよい。なお、ノード装置１００は、これらの通知をクライアント装置２００に対して行うのではなく、クライアント装置２００以外の所定の外部装置（例えば所定のサーバ装置）に対して行ってもよい。これによって、当該外部装置によって提供される所定のサービスを介してこれらの通知が行われ得る。

[0111] また、ユーザによるＰ２Ｐデータベース１２０へのアクセスが許可されなかった場合、ノード装置１００は、当該ユーザがアクセス可能な状態になったときに自律的にＰ２Ｐデータベース１２０へのアクセスを行うことでユーザによる要求に関する処理（例えばデータの登録、またはデータの取得等）を行ってもよい。これによって、ユーザがクライアント装置２００を用いて要求信号をノード装置１００へ再度送信する必要がなくなる。

[0112] なお、上記で説明したノード装置１００による各種処理は、ノード装置１００の制御部１１０、またはＰ２Ｐデータベースプログラム１２１等によって実現され得るが、必ずしもこれに限定されない。例えば、上記で説明した各種処理は、ノード装置１００以外の所定のサーバ装置とノード装置１００が連携することによって実現されてもよい。

[0113] ＜６．まとめ＞

以上で説明してきたように、本開示に係るノード装置１００は、任意の主

体によるＰ２Ｐデータベース１２０へのアクセスに関する履歴情報（アクセス履歴情報）を集計し、集計後のアクセス履歴情報（第２の履歴情報）に基づいて当該主体によるＰ２Ｐデータベース１２０への新たなアクセスを制御することができる。例えば、本開示に係るノード装置１００は、集計後のアクセス履歴情報（第２の履歴情報）である、所定の長さの期間（例えば１日間）における、ある主体によるＰ２Ｐデータベース１２０へのデータ登録の合計回数と所定の閾値とを比較することで、当該主体によるＰ２Ｐデータベース１２０への新たなデータ登録の可否を判断することができる。

[0114] また、第２の実施形態に係るノード装置１００は、過去に行われたＰ２Ｐデータベース１２０へのアクセスを事前に集計することで第２の履歴情報を出力し、当該第２の履歴情報をＰ２Ｐデータベース１２０に登録しておく。これによって、第２の実施形態に係るノード装置１００は、クライアント装置２００からの要求信号が受信されてからＰ２Ｐデータベース１２０へのアクセス制御を行う（アクセスの可否を判断する）までに要する時間を短縮することができる。

[0115] 以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本開示の技術的範囲に属するものと了解される。

[0116] また、本明細書に記載された効果は、あくまで説明的または例示的なものであって限定的ではない。つまり、本開示に係る技術は、上記の効果とともに、または上記の効果に代えて、本明細書の記載から当業者には明らかな他の効果を奏しうる。

[0117] なお、以下のような構成も本開示の技術的範囲に属する。

（１）

任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基

づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御するアクセス制御部を備える、

情報処理装置。

（２）

前記アクセス制御部は、前記履歴情報に基づいて前記新たなアクセスの可否を判断する、

前記（１）に記載の情報処理装置。

（３）

前記アクセスは、前記Ｐ２Ｐデータベースへのデータの登録、または前記Ｐ２Ｐデータベースからのデータの取得のうちの少なくともいずれか一つを含む、

前記（１）または（２）に記載の情報処理装置。

（４）

前記アクセス制御部は、前記履歴情報として、過去に行われた前記アクセスの合計回数、所定の長さの期間において行われた前記アクセスの合計回数、過去に行われた前記アクセスにおける前記データの合計サイズ、または前記所定の長さの期間において行われた前記アクセスにおける前記データの合計サイズのうちの少なくともいずれか一つに基づいて前記新たなアクセスを制御する、

前記（３）に記載の情報処理装置。

（５）

前記アクセス制御部は、前記データの種別、または前記主体の種別に応じて前記新たなアクセスの制御ロジックを変更する、

前記（３）または（４）に記載の情報処理装置。

（６）

前記履歴情報は、前記主体によって過去に行われた複数回の前記アクセスそれぞれに関する第１の履歴情報を集計することで得られた第２の履歴情報を含む、

前記（１）から（５）のいずれか１項に記載の情報処理装置。

（７）

前記第２の履歴情報を前記Ｐ２Ｐデータベースに登録する履歴登録部をさらに備え、

前記アクセス制御部は、前記Ｐ２Ｐデータベースに登録された前記第２の履歴情報に基づいて前記新たなアクセスを制御する、

前記（６）に記載の情報処理装置。

（８）

前記主体は、ユーザ、複数人の前記ユーザによって構成されるグループ、所定の外部装置、複数台の前記外部装置によって構成されるシステム、または前記外部装置によって用いられるソフトウェアのうちの少なくともいずれか一つを含む、

前記（１）から（７）のいずれか１項に記載の情報処理装置。

（９）

前記アクセス制御部は、前記Ｐ２Ｐデータベースに設けられ、前記Ｐ２Ｐデータベース上で実行される所定のプログラムによって具現される、

前記（１）から（８）のいずれか１項に記載の情報処理装置。

（１０）

前記Ｐ２Ｐデータベースはブロックチェーンデータである、

前記（１）から（９）のいずれか１項に記載の情報処理装置。

（１１）

任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御することを有する、

コンピュータにより実行される情報処理方法。

（１２）

任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御

することを、

コンピュータに実現させるためのプログラム。

符号の説明

[0118]

１００	ノード装置
１１０	制御部
１２０	Ｐ２Ｐデータベース
１２１	Ｐ２Ｐデータベースプログラム
１２１ａ	履歴取得部
１２１ｂ	アクセス制御部
１２１ｃ	履歴登録部
１３０	通信部
２００	クライアント装置
２１０	制御部
２２０	入力部
２３０	出力部
２４０	記憶部
２５０	通信部
３００	Ｐ２Ｐネットワーク
４００	ネットワーク

請求の範囲

[請求項1] 任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御するアクセス制御部を備える、

情報処理装置。

[請求項2] 前記アクセス制御部は、前記履歴情報に基づいて前記新たなアクセスの可否を判断する、

請求項１に記載の情報処理装置。

[請求項3] 前記アクセスは、前記Ｐ２Ｐデータベースへのデータの登録、または前記Ｐ２Ｐデータベースからのデータの取得のうちの少なくともいずれか一つを含む、

請求項１に記載の情報処理装置。

[請求項4] 前記アクセス制御部は、前記履歴情報として、過去に行われた前記アクセスの合計回数、所定の長さの期間において行われた前記アクセスの合計回数、過去に行われた前記アクセスにおける前記データの合計サイズ、または前記所定の長さの期間において行われた前記アクセスにおける前記データの合計サイズのうちの少なくともいずれか一つに基づいて前記新たなアクセスを制御する、

請求項３に記載の情報処理装置。

[請求項5] 前記アクセス制御部は、前記データの種別、または前記主体の種別に応じて前記新たなアクセスの制御ロジックを変更する、

請求項３に記載の情報処理装置。

[請求項6] 前記履歴情報は、前記主体によって過去に行われた複数回の前記アクセスそれぞれに関する第１の履歴情報を集計することで得られた第２の履歴情報を含む、

請求項１に記載の情報処理装置。

[請求項7] 前記第２の履歴情報を前記Ｐ２Ｐデータベースに登録する履歴登録部をさらに備え、

前記アクセス制御部は、前記Ｐ２Ｐデータベースに登録された前記第２の履歴情報に基づいて前記新たなアクセスを制御する、

請求項６に記載の情報処理装置。

[請求項8] 前記主体は、ユーザ、複数人の前記ユーザによって構成されるグループ、所定の外部装置、複数台の前記外部装置によって構成されるシステム、または前記外部装置によって用いられるソフトウェアのうちの少なくともいずれか一つを含む、

請求項１に記載の情報処理装置。

[請求項9] 前記アクセス制御部は、前記Ｐ２Ｐデータベースに設けられ、前記Ｐ２Ｐデータベース上で実行される所定のプログラムによって具現される、

請求項１に記載の情報処理装置。

[請求項10] 前記Ｐ２Ｐデータベースはブロックチェーンデータである、

請求項１に記載の情報処理装置。

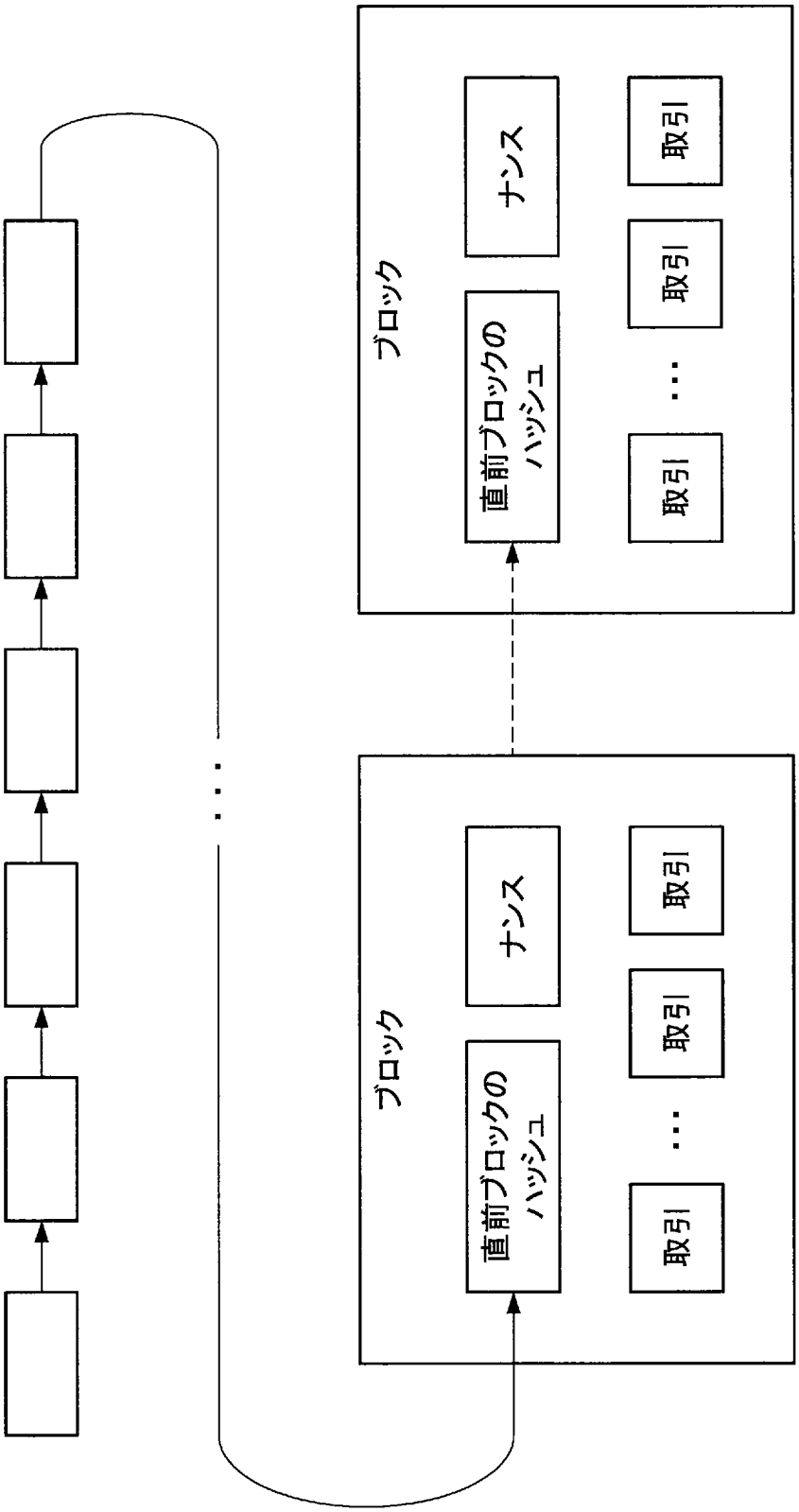
[請求項11] 任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御することを有する、

コンピュータにより実行される情報処理方法。

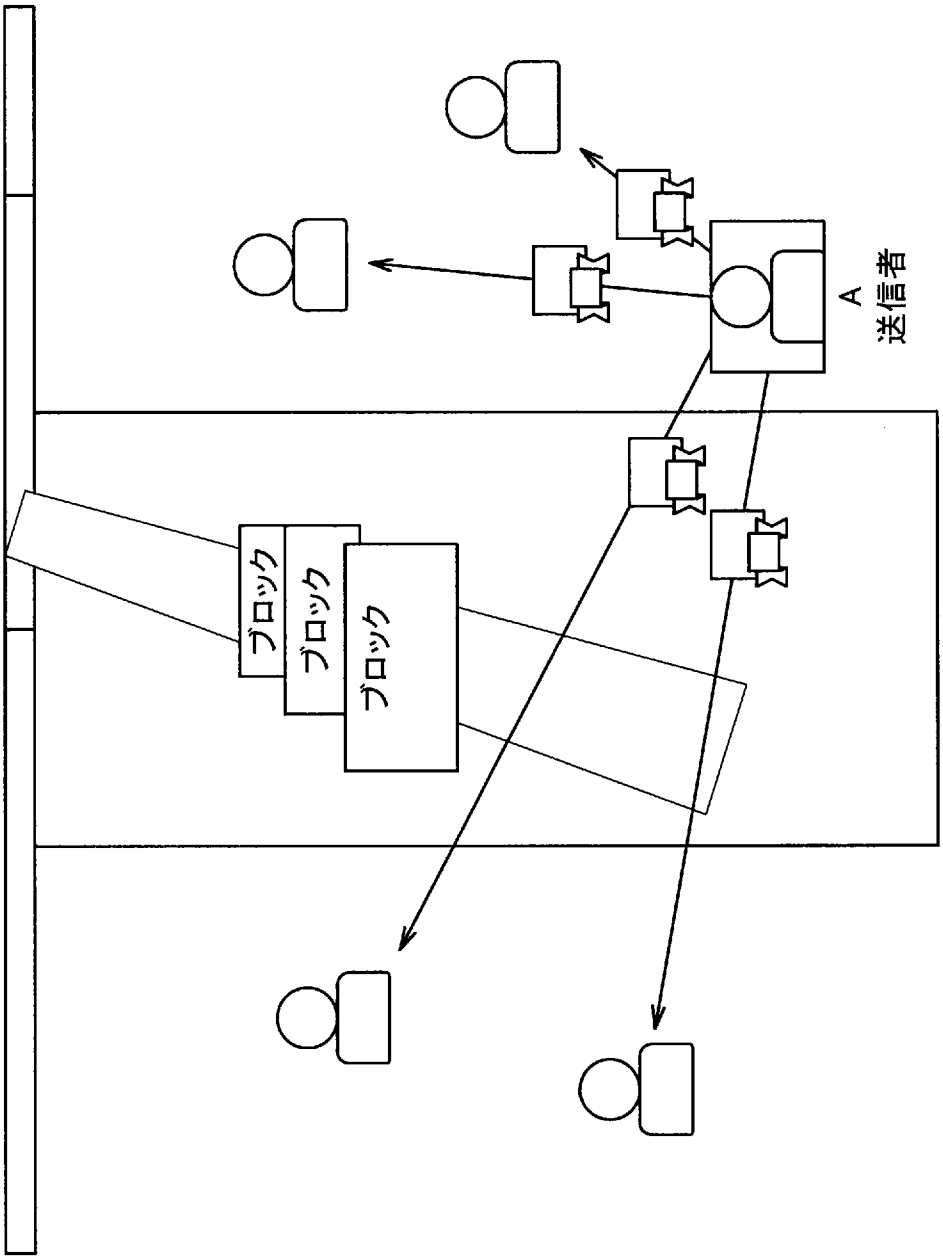
[請求項12] 任意の主体によるＰ２Ｐデータベースへのアクセスに関する履歴情報に基づいて、前記主体による前記Ｐ２Ｐデータベースへの新たなアクセスを制御することを、

コンピュータに実現させるためのプログラム。

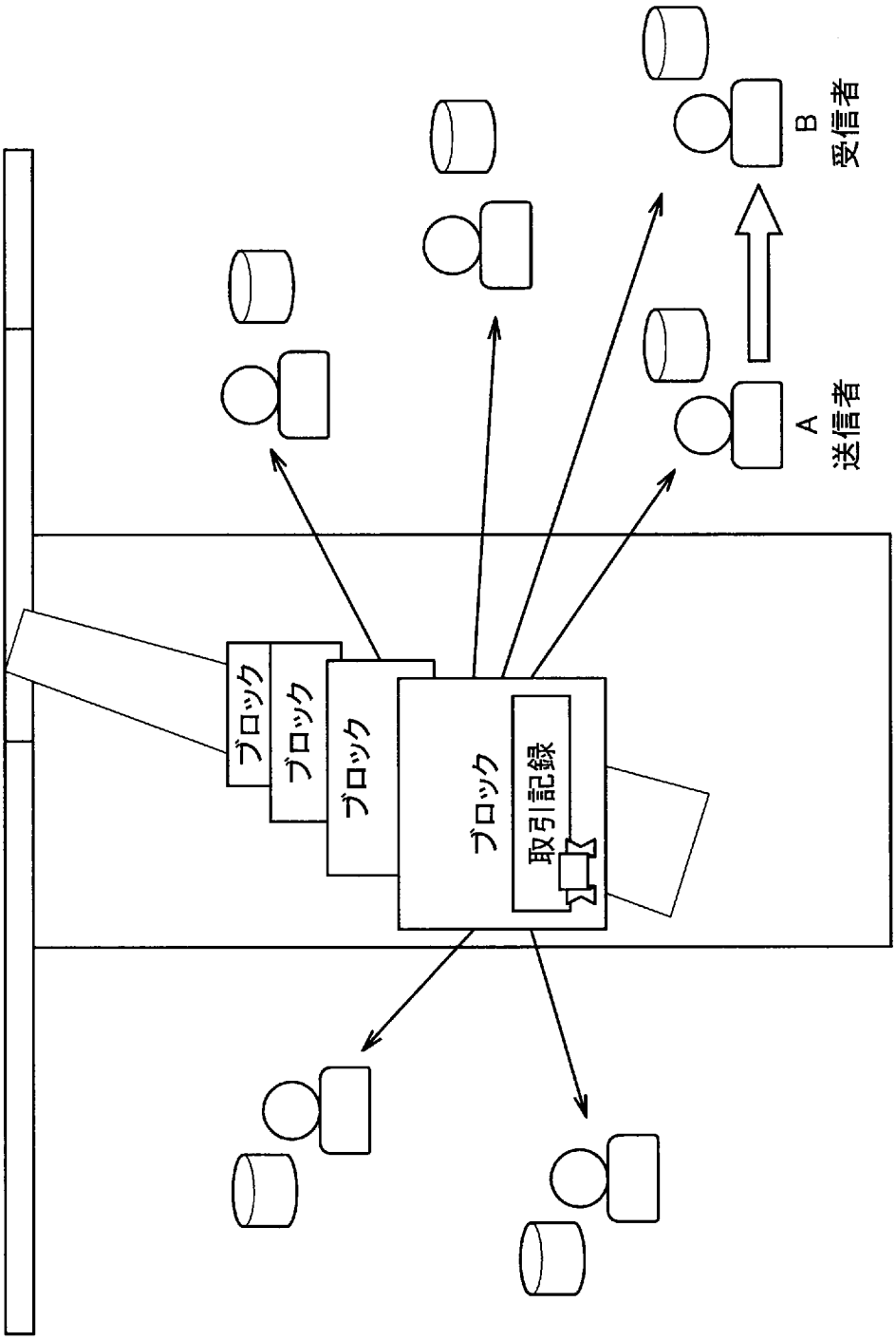
[図1]



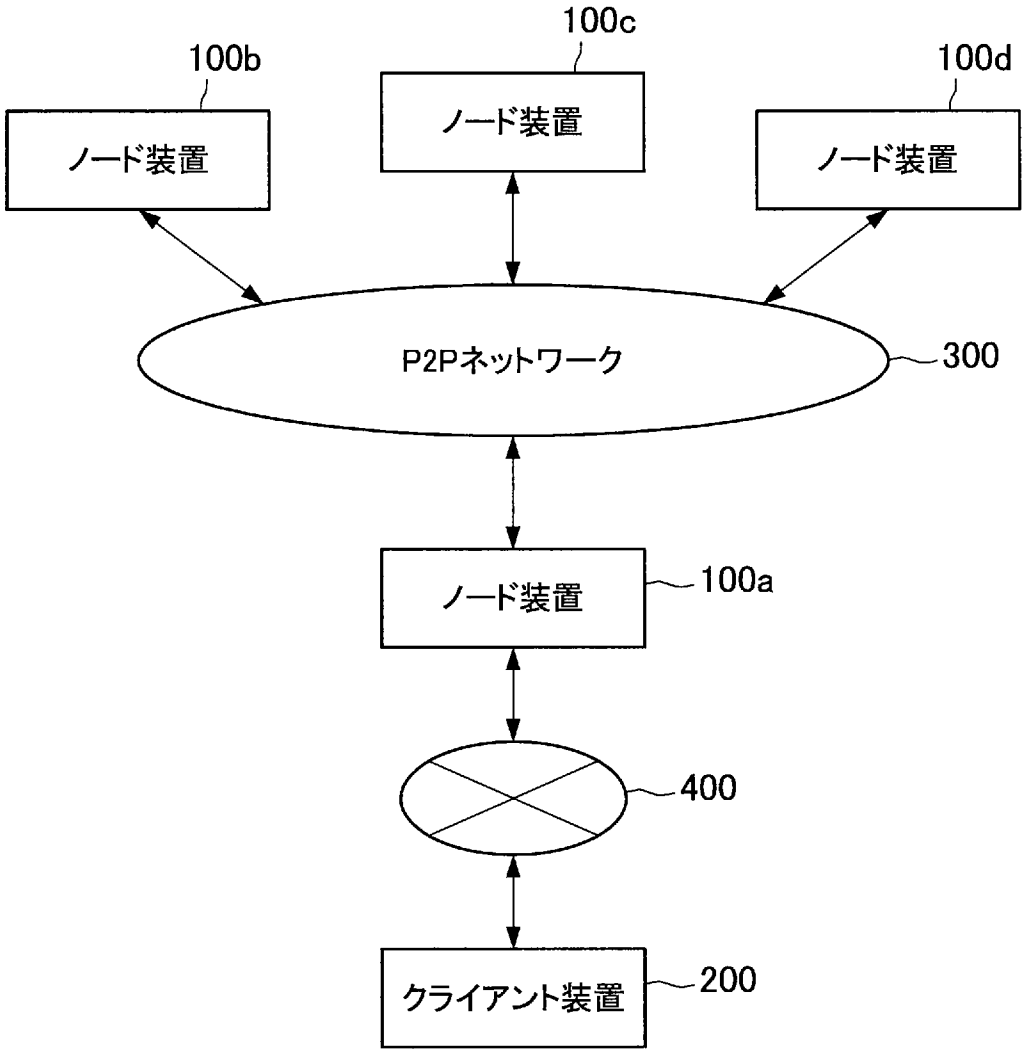
[図2]



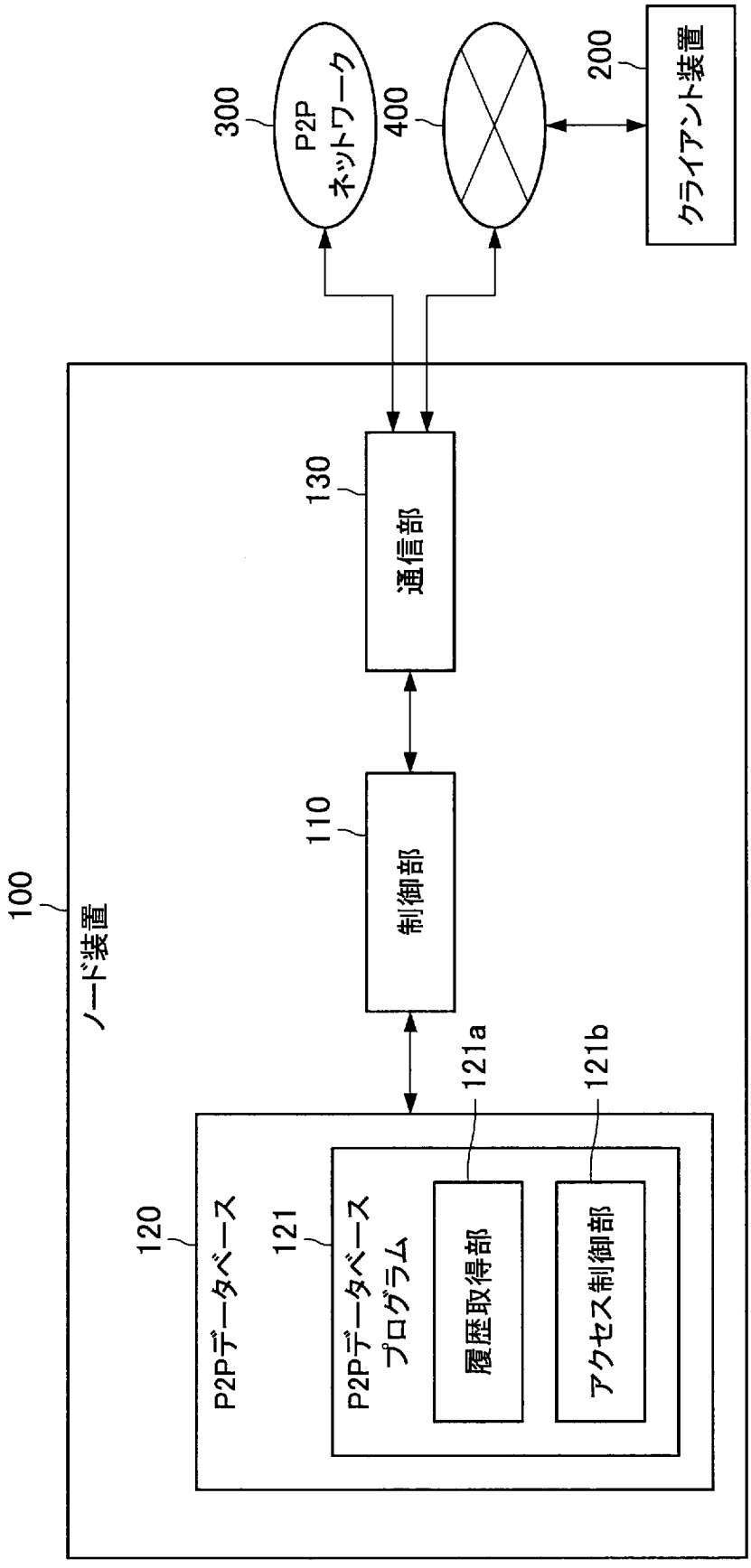
[図3]



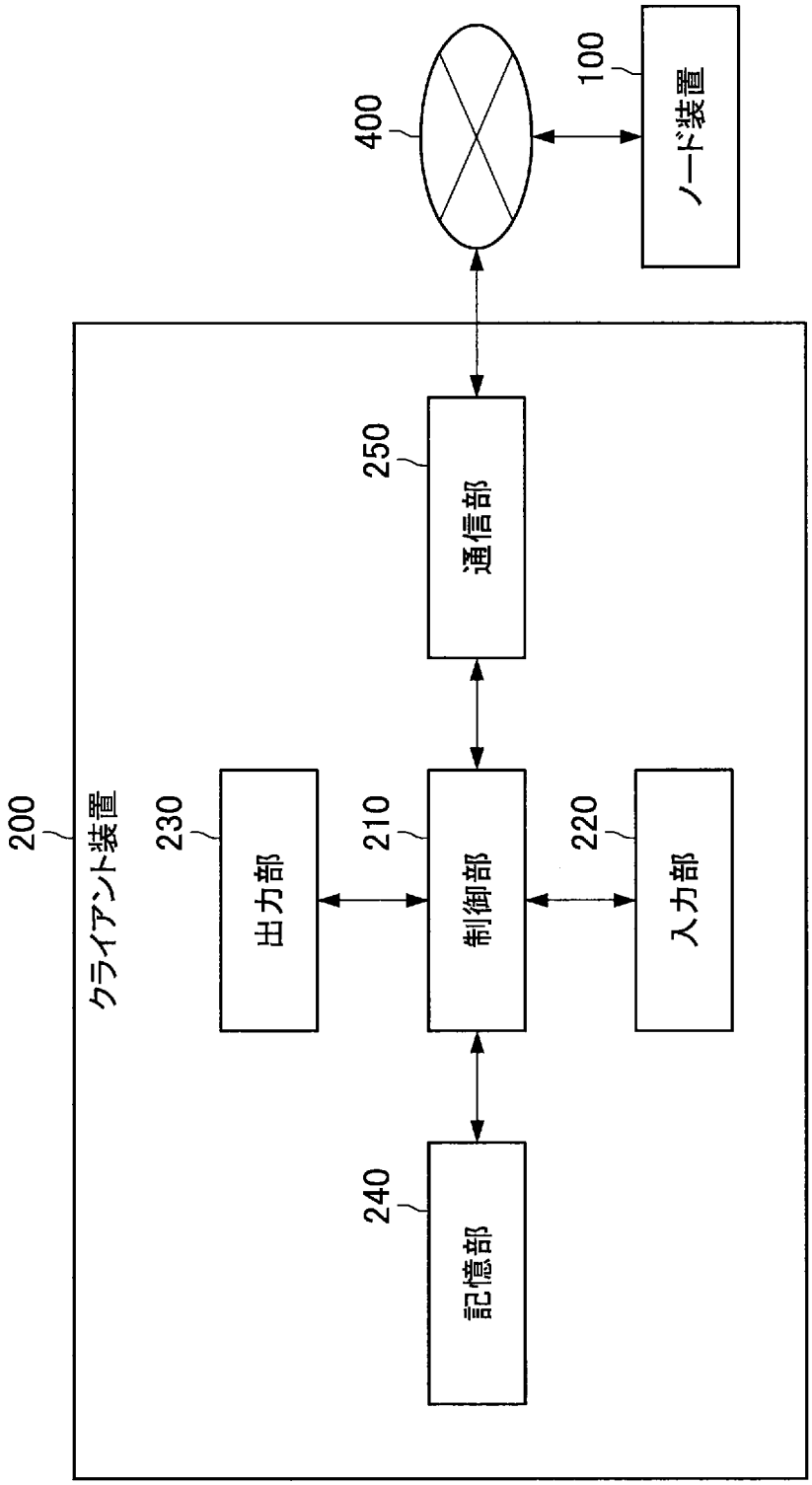
[図4]


100b
ノード装置
100c
ノード装置
100d
ノード装置
P2Pネットワーク
300
ノード装置
100a
400
クライアント装置
200

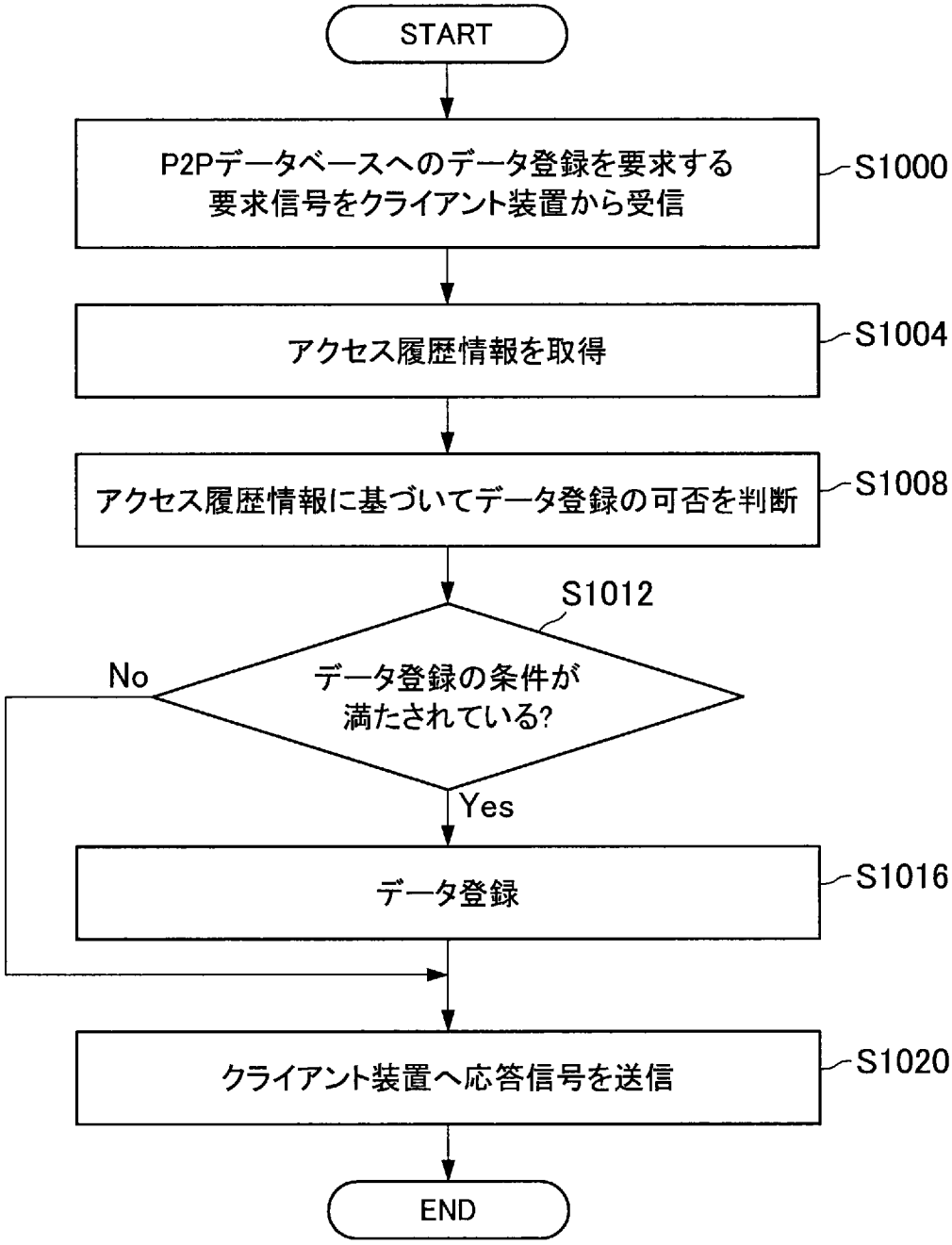
[図5]


300
P2P
ネットワーク
400
200
クライアント装置
130
通信部
110
制御部
100
ノード装置
121a
121b
120
P2Pデータベース
121
P2Pデータベース
プログラム
履歴取得部
アクセス制御部

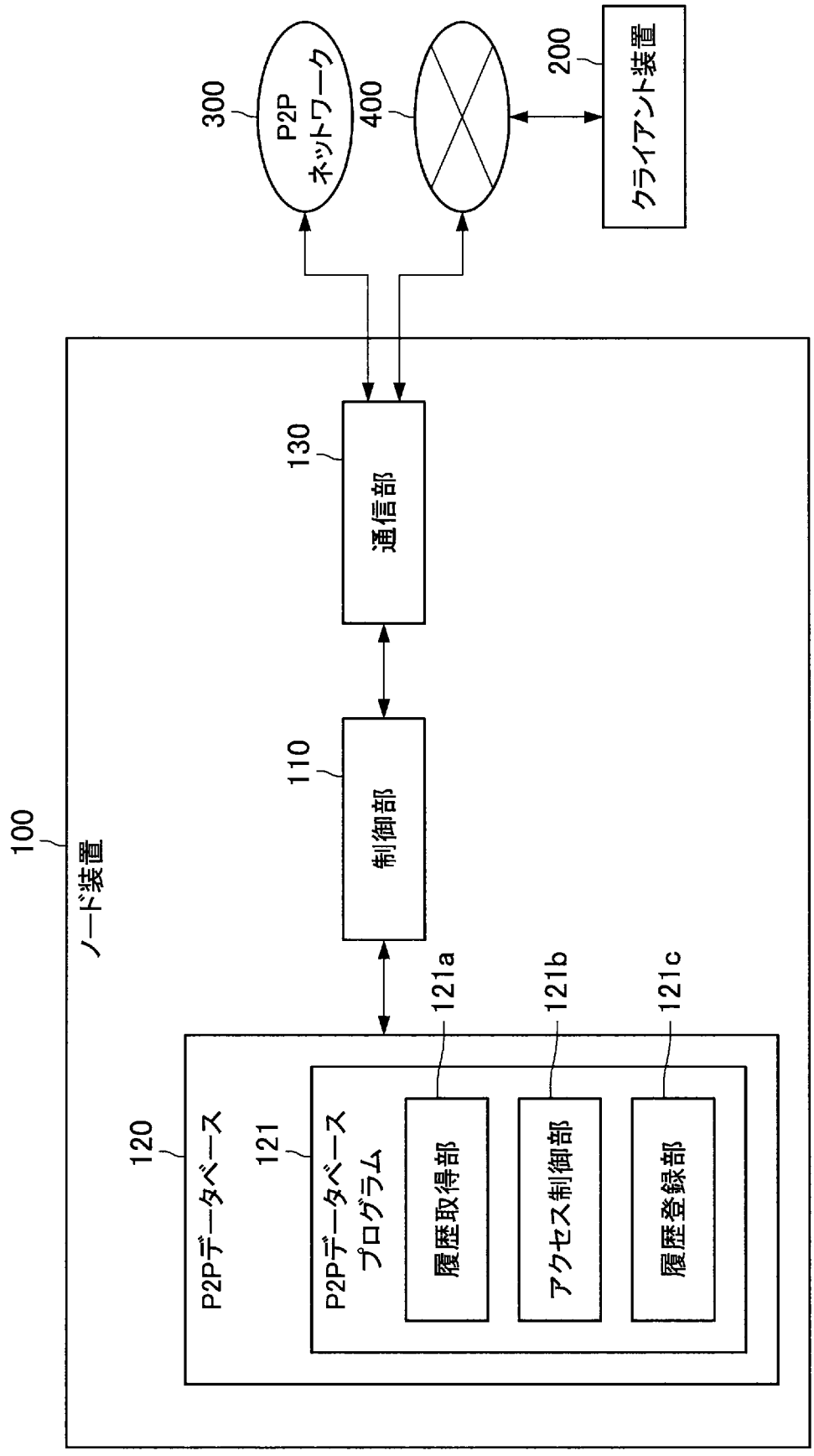
[図6]


400
100
ノード装置
250
通信部
200
クライアント装置
230
出力部
210
制御部
220
入力部
240
記憶部

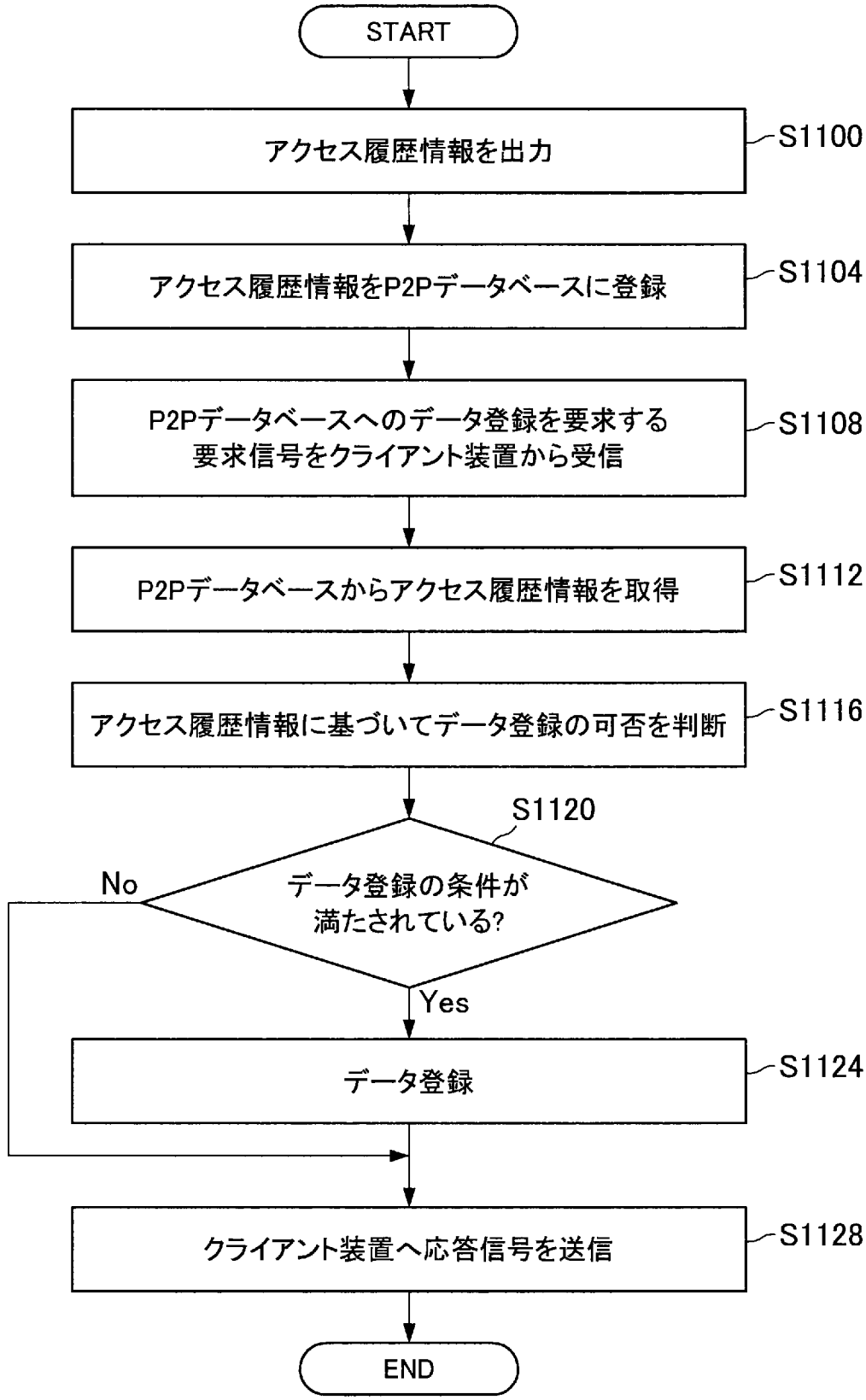
[図7]


START
P2Pデータベースへのデータ登録を要求する
要求信号をクライアント装置から受信
S1000
アクセス履歴情報を取得
S1004
アクセス履歴情報に基づいてデータ登録の可否を判断
S1008
S1012
データ登録の条件が
満たされている?
No
Yes
データ登録
S1016
クライアント装置へ応答信号を送信
S1020
END

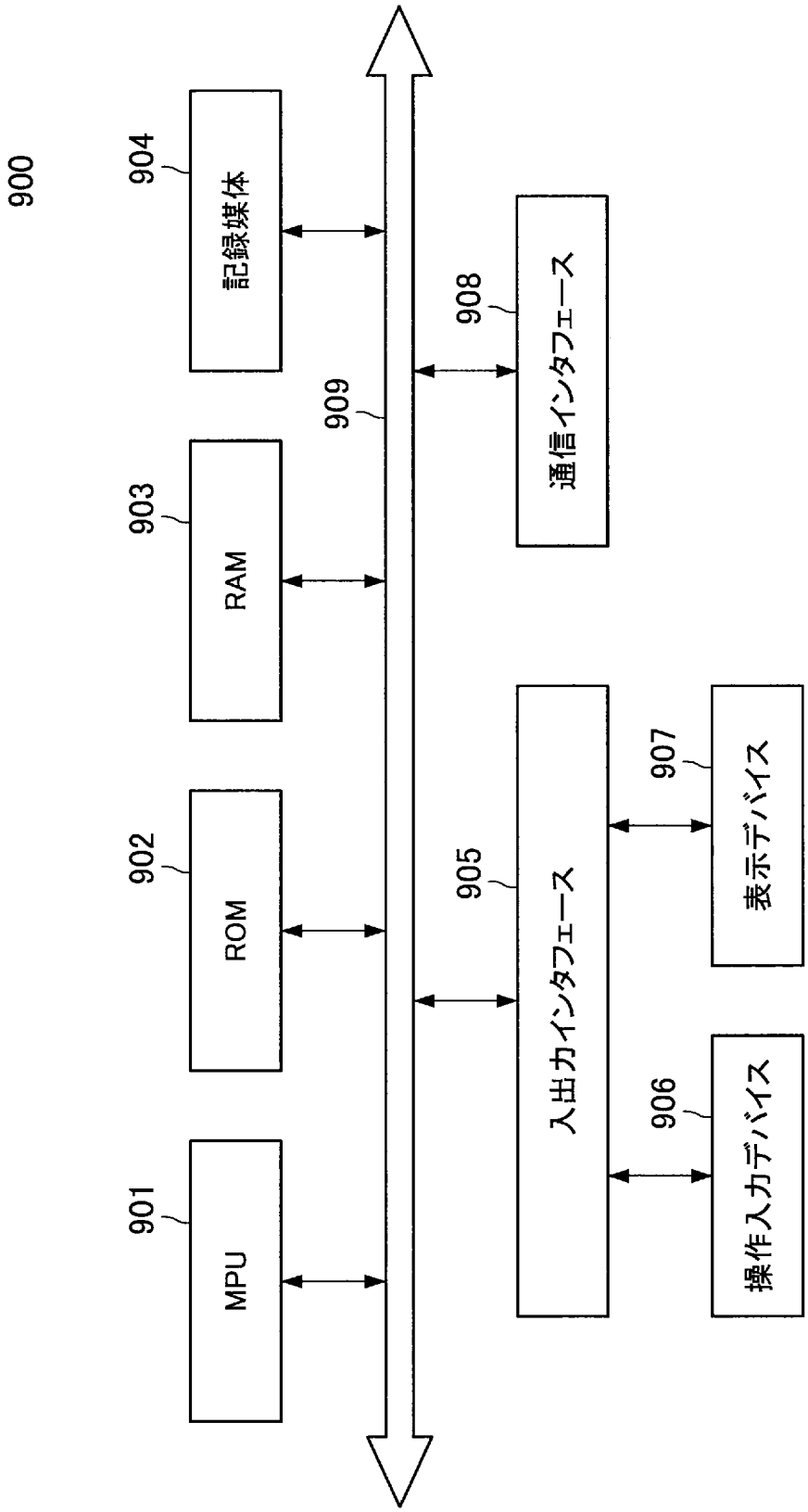
[図8]


300
P2P
ネットワーク
400
200
クライアント装置
130
通信部
110
制御部
100
ノード装置
121a
121b
121c
120
P2Pデータベース
121
P2Pデータベース
プログラム
履歴取得部
アクセス制御部
履歴登録部

[図9]


START
アクセス履歴情報を出力
S1100
アクセス履歴情報をP2Pデータベースに登録
S1104
P2Pデータベースへのデータ登録を要求する
要求信号をクライアント装置から受信
S1108
P2Pデータベースからアクセス履歴情報を取得
S1112
アクセス履歴情報に基づいてデータ登録の可否を判断
S1116
S1120
データ登録の条件が
満たされている?
No
Yes
データ登録
S1124
クライアント装置へ応答信号を送信
S1128
END

[図10]


900
MPU
901
ROM
902
RAM
903
記録媒体
904
入出力インタフェース
905
操作入力デバイス
906
表示デバイス
907
通信インタフェース
908
909

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/002741

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/62(2013.01)i, G06F12/00(2006.01)i, G06F21/55(2013.01)i, H04L9/32(2006.01)i

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. G06F21/62, G06F12/00, G06F21/55, H04L9/32

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	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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 A	JP 2008-299553 A (NATIONAL INSTITUTE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY) 11 December 2008, claim 1, paragraphs [0059], [0067]-[0077] (Family: none)	1-9, 11-12 10
Y A	村上陽平他, サービス指向集合知のためのサービスグリッドアーキテクチャ, 電子情報通信学会技術研究報告, 21 February 2011, vol. 110, no. 428, pp. 7-12, (MURAKAMI, Yohei et al., Service grid architecture for service-oriented collective intelligence, IEICE Technical Report)	1-9, 11-12 10
A	US 2017/0034197 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY) 02 February 2017, abstract & EP 3125489 A1 & CN 106407808 A	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 05.04.2019	Date of mailing of the international search report 16.04.2019
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

International application No.
PCT/JP2019/002741

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2017/170679 A1 (BITFLYER INC.) 05 October 2017, paragraphs [0040], [0056] & US 2019/0036702 A1, paragraphs [0048], [0066] & EP 3439231 A1 & CN 109219940 A	1-12
A	JP 2018-5818 A (NIPPON TELEGRAPH AND TELEPHONE CORPORATION) 11 January 2018, abstract (Family: none)	1-12

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／００２７４１

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/62(2013.01)i, G06F12/00(2006.01)i, G06F21/55(2013.01)i, H04L9/32(2006.01)i

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））

Int.Cl.　G06F21/62, G06F12/00, G06F21/55, H04L9/32

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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 A	JP 2008-299553 A (独立行政法人情報通信研究機構) 2008.12.11, 請求項 1, 段落[0059], [0067]-[0077] (ファミリーなし)	1-9, 11-12 10
Y A	村上陽平他, サービス指向集合知のためのサービスグリッドアーキテクチャ, 電子情報通信学会技術研究報告, 2011.02.21, 第 110 巻, 第 428 号, p. 7-p. 12	1-9, 11-12 10
A	US 2017/0034197 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY) 2017.02.02, ABSTRACT & EP 3125489 A1 & CN 106407808 A	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矛盾するものではなく、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
０５．０４．２０１９	１６．０４．２０１９

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　９５５５
宮司　卓佳
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　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
A	WO 2017/170679 A1（株式会社ｂｉｔＦｌｙｅｒ）2017.10.05, 段落[0040],[0056] & US 2019/0036702 A1,段落[0048],[0066] & EP 3439231 A1 & CN 109219940 A	1-12
A	JP 2018-5818 A（日本電信電話株式会社）2018.01.11, 要約 (ファミリーなし)	1-12