

明 細 書

発明の名称： 情報処理方法、情報処理装置及びプログラム

技術分野

[0001] 本発明は、情報処理方法、情報処理装置及びプログラムに関する。

背景技術

[0002] 特許文献 1 には、患者情報、担当医療者情報、疾患・疾病における有害事象に関する質問と複数の回答とが組み合わされている複数の疾病診断用問合せ情報を用いて、異常を検出した場合に担当医療者へアラートを通知する疾病診断・治療・予防システムが開示されている。

先行技術文献

特許文献

[0003] 特許文献1：特開 2 0 2 0 - 0 6 4 4 3 5 号公報

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、特許文献 1 に係る発明は、医療研究者が患者の医療データを用いて医療を研究することができないという問題がある。

[0005] 一つの側面では、患者の医療データを適切に医療研究者に提供することが可能な情報処理方法等を提供することを目的とする。

課題を解決するための手段

[0006] 一つの側面に係る情報処理方法は、患者を特定する患者 ID、患者の属性、及び医療に関する質問に対する前記患者による回答を取得し、医師を特定する医師 ID を前記患者の患者端末装置により読み取らせることにより前記医師 ID を取得し、取得した前記医師 ID に対応する医師端末装置へ前記患者の患者 ID、属性及び回答を送信し、前記患者の患者 ID、属性及び回答が表示された前記医師端末装置を通じて、前記医師による前記患者に対する診療データの入力を受け付け、前記患者の属性、回答及び入力された診療データを含む医療データの送信要求を受け付け、前記医療データのハッシュ値

をブロックチェーンシステムに出力し、前記ブロックチェーンシステムに記録された前記医療データの開示要求を研究者の研究者端末装置を介して受け付け、前記研究者の開示要求に対する前記患者の承認を得た場合に、前記医療データを前記研究者端末装置に出力することを特徴とする。

発明の効果

[0007] 一つの側面では、患者の医療データを適切に医療研究者に提供することが可能となる。

図面の簡単な説明

[0008] [図1]医療データ管理システムの概要を示す説明図である。

[図2]サーバの構成例を示すブロック図である。

[図3]患者DB及び医師DBのレコードレイアウトの一例を示す説明図である。

[図4]質問DB及び医療データDBのレコードレイアウトの一例を示す説明図である。

[図5]研究者DB及び取引履歴DBのレコードレイアウトの一例を示す説明図である。

[図6]管理DBのレコードレイアウトの一例を示す説明図である。

[図7]ブロックチェーンのノードの構成例を示すブロック図である。

[図8]医師端末及び患者端末の構成例を示すブロック図である。

[図9]研究者端末の構成例を示すブロック図である。

[図10]電子署名付き医療データを作成する動作を説明する説明図である。

[図11]医療データをブロックチェーンに記録する処理を説明する説明図である。

[図12]医療データを研究者端末に出力する動作を説明する説明図である。

[図13]質問に対する回答の入力画面の一例を示す説明図である。

[図14]医療データの作成画面の一例を示す説明図である。

[図15]患者端末側での医療データの表示画面の一例を示す説明図である。

[図16]患者端末側での医療データの表示画面の一例を示す説明図である。

[図17]患者端末側での医療データの表示画面の一例を示す説明図である。

[図18]患者端末側での開示要求の応答画面の一例を示す説明図である。

[図19]患者端末側での医療データの取引履歴画面の一例を示す説明図である。

。

[図20]患者端末側での医療データの詳細画面の一例を示す説明図である。

[図21]研究者端末側での医療データ管理画面の一例を示す説明図である。

[図22]研究者端末側での取引履歴画面の一例を示す説明図である。

[図23]医療データを作成する際の処理手順を示すフローチャートである。

[図24]医療データを作成する際の処理手順を示すフローチャートである。

[図25]患者の承認を得た医療データを研究者端末に出力する際の処理手順を示すフローチャートである。

[図26]患者の承認を得た医療データを研究者端末に出力する際の処理手順を示すフローチャートである。

[図27]医療データを共有する際の処理手順を示すフローチャートである。

[図28]研究結果に関する情報を患者端末に出力する際の処理手順を示すフローチャートである。

[図29]研究者端末側での複数回の医療データの表示画面の一例を示す説明図である。

[図30]実施形態5における管理DBのレコードレイアウトの一例を示す説明図である。

[図31]承諾情報の受付画面の一例を示す説明図である。

[図32]患者の再承認を得た医療データを研究者端末に出力する際の処理手順を示すフローチャートである。

発明を実施するための形態

[0009] 以下、本発明をその実施の形態を示す図面に基づいて詳述する。

[0010] (実施形態1)

実施形態1は、患者の医療データを研究者（医療研究者）に提供する形態に関する。図1は、医療データ管理システムの概要を示す説明図である。本

実施形態のシステムは、情報処理装置 1、ブロックチェーンシステム 2、情報処理端末 3、情報処理端末 4 及び情報処理端末 5 を含み、各装置はインターネット等のネットワーク N を介して情報の送受信を行う。

[0011] 情報処理装置 1 は、種々の情報に対する処理、記憶及び送受信を行う情報処理装置である。情報処理装置 1 は、例えばサーバ装置、パーソナルコンピュータまたは汎用のタブレット PC（パソコン）等である。本実施形態において情報処理装置 1 はサーバ装置であるものとし、以下では簡潔のためサーバ 1 と読み替える。

[0012] ブロックチェーンシステム 2 とは、分散型台帳技術又は分散型ネットワークである。ブロックチェーンシステム 2 は、コンセンサス処理を実行する複数のノード 21 により構成される。ノード 21 の各々は、当該コンセンサス処理の実行を通じて、ブロックチェーンデータのコピーを保持する。ブロックチェーンシステム 2 は、ブロックと呼ばれるデータの単位を一定時間ごとに生成し、鎖のように連結していくことによりデータを保管する。

[0013] ブロックチェーンシステム 2 は、ピアツーピア（Peer to Peer）ネットワークと分散型タイムスタンプサーバの使用により自律的に管理される。鎖状に保存しているため、ブロック内のデータを一度記憶した場合、該データを遡及的に変更することが難しい。なお、ブロックチェーンシステム 2 は、パブリック型、プライベート型、コンソーシアム型のいずれであっても良い。データの単位はブロックではなく個々のトランザクションであっても良い。また、データの保存は鎖状以外にも有向非巡回グラフ等の保存形式であっても良い。以下では簡潔のため、ブロックチェーンシステム 2 をブロックチェーン 2 と読み替える。

[0014] 情報処理端末 3 は、患者の属性、医療に関する質問に対する患者による回答、及び医師による患者に対する診療データを含む医療データの作成、ならびに、医療データの電子署名等を行う端末装置である。情報処理端末 3 は、例えばスマートフォン、携帯電話、タブレット、パーソナルコンピュータ端末等の情報処理機器である。以下では簡潔のため、情報処理端末 3 を医師端

末3と読み替える。

[0015] 情報処理端末4は、患者の属性及び質問に対する回答の取得、電子署名付き医療データの取得、並びに、医療データの開示要求に対する承認情報の入力受付等を行う端末装置である。情報処理端末4は、例えばスマートフォン、携帯電話、アップルウォッチ（Apple Watch:登録商標）等のウェアラブルデバイス、タブレット、パーソナルコンピュータ端末等の情報処理機器である。以下では簡潔のため、情報処理端末4を患者端末4と読み替える。

[0016] 情報処理端末5は、医療データの開示要求の受付及び送信、ならびに、開示要求に対して承認を得た医療データの受信等を行う端末装置である。情報処理端末5は、例えばスマートフォン、携帯電話、タブレット、パーソナルコンピュータ端末等の情報処理機器である。以下では簡潔のため、情報処理端末5を研究者端末5と読み替える。

[0017] 本実施形態に係るサーバ1は、患者を特定する患者ID、患者の属性、及び医療に関する質問に対する前記患者による回答を取得する。サーバ1は、医師を特定する医師IDを患者端末4により読み取らせることにより医師IDを取得する。サーバ1は、取得した医師IDに対応する医師端末3へ患者の患者ID、属性及び回答を送信する。サーバ1は医師端末3を通じて、該医師による患者に対する診療データの入力を受け付ける。

[0018] サーバ1は、患者の属性、回答及び入力された診療データを含む医療データの送信要求を医師端末3から受け付けた場合、医療データのハッシュ値を算出する。サーバ1は、算出した医療データのハッシュ値をブロックチェーン2に出力する。サーバ1は研究者端末5を介して、ブロックチェーン2に記録された医療データの開示要求を受け付けた場合、受け付けた開示要求を、該医療データを提供した患者の患者端末4に送信する。サーバ1は、開示要求に対する患者の承認を得た場合、該医療データを研究者端末5に送信する。

[0019] 図2は、サーバ1の構成例を示すブロック図である。サーバ1は、制御部11、記憶部12、通信部13、入力部14、表示部15、読取部16及び

大容量記憶部 17 を含む。各構成はバス B で接続されている。

- [0020] 制御部 11 は CPU (Central Processing Unit)、MPU (Micro-Processing Unit)、GPU (Graphics Processing Unit) 等の演算処理装置を含み、記憶部 12 に記憶された制御プログラム 1P (プログラム製品) を読み出して実行することにより、サーバ 1 に係る種々の情報処理、制御処理等を行う。また制御プログラム 1P には、例えばイーサリアムの Geth (Go-Ethereum) 等のスマートコントラクトの生成・実行、仮想通貨の送金、アカウントの作成、マイニング等の処理を実行するプログラムが含まれる。
- [0021] また、制御部 11 は、ハッシュ値算出部 11a 及び電子署名作成部 11b を含む。ハッシュ値算出部 11a は、暗号学的ハッシュ関数を用いて各種情報のハッシュ値を算出する処理を行う。電子署名作成部 11b は、偽造又は改ざんを防止するため、公開鍵暗号方式に基づくデジタル認証用の署名を生成する。なお、図 2 では制御部 11 を単一のプロセッサであるものとして説明するが、マルチプロセッサであっても良い。
- [0022] 記憶部 12 は RAM (Random Access Memory)、ROM (Read Only Memory) 等のメモリ素子を含み、制御部 11 が処理を実行するために必要な制御プログラム 1P 又はデータ等を記憶している。また、記憶部 12 は、制御部 11 が演算処理を実行するために必要なデータ等を一時的に記憶する。通信部 13 は通信に関する処理を行うための通信モジュールであり、ネットワーク N を介して、ブロックチェーン 2 のノード 21、医師端末 3、患者端末 4 または研究者端末 5 等との間で情報の送受信を行う。
- [0023] 入力部 14 は、マウス、キーボード、タッチパネルまたはボタン等の入力デバイスであり、受け付けた操作情報を制御部 11 へ出力する。表示部 15 は、液晶ディスプレイ又は有機 EL (electroluminescence) ディスプレイ等であり、制御部 11 の指示に従い各種情報を表示する。
- [0024] 読取部 16 は、CD (Compact Disc) - ROM 又は DVD (Digital Versatile Disc) - ROM を含む可搬型記憶媒体 1a を読み取る。制御部 11 が読取部 16 を介して、制御プログラム 1P を可搬型記憶媒体 1a より読み取り

、大容量記憶部 17 に記憶しても良い。また、ネットワーク N 等を介して他のコンピュータから制御部 11 が制御プログラム 1 P をダウンロードし、大容量記憶部 17 に記憶しても良い。さらにまた、半導体メモリ 1 b から、制御部 11 が制御プログラム 1 P を読み込んでも良い。

[0025] 大容量記憶部 17 は、例えば HDD (Hard disk drive:ハードディスク)、SSD (Solid State Drive:ソリッドステートドライブ)等の記録媒体を備える。大容量記憶部 17 は、患者 DB (データベース: database) 171、医師 DB 172、質問 DB 173、医療データ DB 174、研究者 DB 175、取引履歴 DB 176 及び管理 DB 177 を含む。

[0026] 患者 DB 171 は、患者の属性を記憶している。医師 DB 172 は、医師の属性を記憶している。質問 DB 173 は、医療に関する質問に対する患者による回答を記憶している。医療データ DB 174 は、患者の医療データを記憶している。研究者 DB 175 は、研究者の属性を記憶している。取引履歴 DB 176 は、医療データの取引履歴を記憶している。管理 DB 177 は、医療データの管理情報を記憶している。

[0027] なお、本実施形態において記憶部 12 及び大容量記憶部 17 は一体の記憶装置として構成されていても良い。また、大容量記憶部 17 は複数の記憶装置により構成されていても良い。更にまた、大容量記憶部 17 はサーバ 1 に接続された外部記憶装置であっても良い。

[0028] なお、本実施形態では、サーバ 1 は一台の情報処理装置であるものとして説明するが、複数台により分散して処理させても良く、または仮想マシンにより構成されていても良い。

[0029] 図 3 は、患者 DB 171 及び医師 DB 172 のレコードレイアウトの一例を示す説明図である。患者 DB 171 は、患者 DID (Decentralized Identifier) 列、氏名列、生年月日列、郵便番号列、住所列、電話番号列、メールアドレス列及び登録日時列を含む。患者 DID 列は、各患者を識別するために、一意に特定される患者の DID を記憶している。DID は、ユーザが自分の属性情報に関するコントロール権を確保した上で、各データ保有者が

保有するユーザの属性情報のうち必要な情報を、ユーザの許可した範囲で連携し合う分散型アイデンティティ（非中央集権型ID）である。DIDは、ブロックチェーン2により構築された分散型システムを用いて、重複しない一意な識別子を実現することにより、不変性、または外部からの閲覧・改ざんに対する高い信頼性を維持することができる。なお、本実施形態では、患者IDが患者DIDである例を説明したが、これに限るものではない。患者IDは、患者を特定するための従来（既存）のID、顔または指紋による生体認証情報等であっても良い。

[0030] 氏名列は、患者の氏名を記憶している。生年月日列は、患者の生年月日を記憶している。郵便番号列は、患者の現住所に基づく郵便番号を記憶している。住所列は、患者の現住所を記憶している。電話番号列は、患者の電話番号を記憶している。メールアドレス列は、患者の電子メールアドレスを記憶している。登録日時列は、患者の属性を登録した日時情報を記憶している。

[0031] 医師DB172は、医師DID列、氏名列、医療機関名称列及び診療科名称列を含む。医師DID列は、各医師を識別するために、一意に特定される医師のDIDを記憶している。なお、本実施形態では、医師IDが医師DIDである例を説明したが、これに限るものではない。医師IDは、医師を特定するための従来（既存）のID、顔または指紋による生体認証情報等であっても良い。氏名列は、医師の氏名を記憶している。医療機関名称列は、医師が勤務している医療機関の名称を記憶している。診療科名称列は、精神科、皮膚科または外科等の診療科の名称を記憶している。

[0032] 図4は、質問DB173及び医療データDB174のレコードレイアウトの一例を示す説明図である。

[0033] 質問DB173は、患者DID列、質問種類列及び質問データ列を含む。患者DID列は、患者を特定する患者DIDを記憶している。質問種類列は、医療に関する質問の種類を記憶している。質問の種類は、例えばPDQ（Parkinson's Disease Questionnaire）-39、MDS-UPDRS（Movement Disorder Society-sponsored revision of the Unified Parkinson's Disease Questionnaire）-39、H-Y（Hoehn-Yahr）スケール、MMSE（Mini-Mental State Examination）等である。

ase Rating Scale) または E Q - 5 D (EuroQOL 5 Dimensions) 等を含む。
なお、上述した質問の種類は一例であり、これに限るものではない。質問データ列は、医療に関する質問、及び各質問に対する患者による回答を記憶している。

- [0034] 医療データ D B 1 7 4 は、医療データ I D 列、患者 D I D 列、医療データ列、ハッシュ値列、医師 D I D 列、署名日時列、B C へ記録日時列及び状態列を含む。医療データ I D 列は、各医療データを識別するために、一意に特定される医療データの I D を記憶している。患者 D I D 列は、患者を特定する患者 D I D を記憶している。
- [0035] 医療データ列は、医療データ I D に対応付けて患者の医療データを記憶している。医療データ列には、患者の属性、医療に関する質問に対する患者による回答、及び医師による患者に対する診療データを含む医療データが記憶されている。医療データは、例えば J S O N (JavaScript(登録商標) Object Notation) 形式のファイル、または X M L (Extensible Markup Language) 形式のファイル等である。ハッシュ値列は、医療データのハッシュ値を記憶している。
- [0036] 医師 D I D 列は、医師を特定する医師 D I D を記憶している。署名日時列は、医療データを電子署名した日時情報を記憶している。B C へ記録日時列は、ブロックチェーン 2 に医療データを記録した日時を記憶している。状態列は、医療データの状態を記憶している。医療データの状態は、例えば「下書き保存」、「サブミット済み」、「署名済み」または「B C へ記録済み」等を含む。「下書き保存」状態は、患者の属性及び質問に対する患者による回答を下書き保存した状態である。「サブミット済み」状態は、患者の属性及び質問に対する患者による回答をサーバ 1 にサブミット（送信）済みであることを示す状態である。「署名済み」状態は、患者の属性、質問に対する回答及び医師による患者に対する診療データを含む医療データに署名済みであることを示す状態である。「B C へ記録済み」状態は、医療データをブロックチェーン 2 に記録済みであることを示す状態である。

[0037] 図5は、研究者DB175及び取引履歴DB176のレコードレイアウトの一例を示す説明図である。研究者DB175は、研究者ID列、研究機関ID列、氏名列、生年月日列、郵便番号列、住所列、電話番号列、メールアドレス及び登録日時列を含む。研究者ID列は、各研究者を識別するために、一意に特定される研究者のIDを記憶している。なお、本実施形態では、研究者IDが研究者IDである例を説明したが、これに限るものではない。研究者IDは、研究者を特定するための従来のID、顔または指紋による生体認証情報等であっても良い。

[0038] 研究機関ID列は、研究者が所属する研究機関を特定するための研究機関IDを記憶している。研究機関は、研究、試験または鑑定等を行うための組織（機関）、またはその施設である。氏名列は、研究者の氏名を記憶している。生年月日列は、研究者の生年月日を記憶している。郵便番号列は、研究者の現住所に基づく郵便番号を記憶している。住所列は、研究者の現住所を記憶している。電話番号列は、研究者の電話番号を記憶している。メールアドレス列は、研究者の電子メールアドレスを記憶している。登録日時列は、研究者の属性を登録した日時情報を記憶している。

[0039] 取引履歴DB176は、研究機関ID列、医療データID列、患者ID列、研究者ID列及び取引日時列を含む。研究機関ID列は、研究機関を特定する研究機関IDを記憶している。医療データID列は、医療データを特定する医療データIDを記憶している。患者ID列は、患者を特定する患者IDを記憶している。研究者ID列は、研究者を特定する研究者IDを記憶している。取引日時列は、患者と研究者との間に医療データの取引日時を記憶している。

[0040] 図6は、管理DB177のレコードレイアウトの一例を示す説明図である。管理DB177は、管理ID列、医療データID列、患者ID列、研究者ID列、要求状況列、要求日時列、患者承認日時列、承認種別列、患者否認日時列及び患者撤回日時列を含む。管理ID列は、各管理データを識別するために、一意に特定される管理データのIDを記憶している。医療デー

タID列は、医療データを特定する医療データIDを記憶している。患者DID列は、患者を特定する患者DIDを記憶している。研究者DID列は、研究者を特定する研究者DIDを記憶している。

[0041] 要求状況列は、医療データの開示要求に対する患者の応答状況を記憶している。要求状況列には、「データ未請求」、「承認待ち」、「承認済み」、「撤回済み」または「保留中」等が記憶される。要求日時列は、医療データの開示要求を受け付けた日時情報を記憶している。患者承認日時列は、患者が医療データの利用を承認した日時情報を記憶している。

[0042] 承認種別列は、医療データに対する承認種別を記憶している。承認種別は、医療データの開示要求に対する第1承認、及び、第1承認と、医療データの開示要求に対して第1承認を得た医療データを、他の研究者に共有することを求める共有要求に対する患者の第2承認とを含む承認を有する。以下では簡潔のため、第1承認を「開示のみ」と読み替え、第1承認と第2承認とを含む承認を「開示&共有」と読み替える。患者否認日時列は、患者が医療データの利用を否認した日時情報を記憶している。患者撤回日時列は、承認済みの医療データに対し、患者が承認を撤回した日時情報を記憶している。

[0043] なお、上述した各DBの記憶形態は一例であり、データ間の関係が維持されていれば、他の記憶形態であっても良い。

[0044] 図7は、ブロックチェーン2のノード21の構成例を示すブロック図である。ブロックチェーン2のノード21は、制御部211、記憶部212、通信部213、受付部214、出力部215、ブロック生成部216、ブロック検証部217及びブロック共有部218を含む。各構成はバスBで接続されている。

[0045] 制御部211は、他ノード21（端末）の制御部と自律分散的に協調して、常に最新のブロックチェーン（台帳：ブロックチェーンデータのコピー）を記憶部212に保持する。記憶部212には、分散型のネットワークへブロードキャストされたトランザクションが含まれたブロックチェーン（台帳）、及びブロック内の情報の検証処理に必要となる情報等が記憶される。

- [0046] 通信部 213 は、通信に関する処理を行うための通信モジュールである。
受付部 214 は、外部ノードから、ブロックチェーン 2 が管理するブロックチェーンである分散型のネットワークに記録する情報を受け付ける。出力部 215 は、外部ノードからの要求に応じて、自身が保持するブロックチェーンの情報を出力する。
- [0047] ブロック生成部 216 は、受付部 214 が受け付けた情報を基に、ブロックチェーンに追加するブロックを生成する。ブロック生成部 216 は、前ブロックに基づく情報と受付部 214 が受け付けた情報とを含むブロックを生成する。また、ブロック生成部 216 は、自身が生成したブロックまたは後述するブロック共有部 218 を介して他のブロックチェーンのノード 21 が生成したブロックに対して、所定のコンセンサス処理として、例えば、ノンスを探索する処理や署名を付与する処理を行った上で、自身が管理するブロックチェーン（台帳）にブロックを追加する。なお、ブロック生成部 216 が生成したブロックに対して、複数のノード 21 が所定のコンセンサス処理を行って得られたものが、最終的にブロックチェーン 2 に追加されるブロックとなる。
- [0048] ブロック検証部 217 は、自身が保持するブロックチェーンにブロックを追加する際に、該ブロック内の情報の検証を行う。通常、追加対象とされるブロックは、自ノードを含むノード 21 群において最も早く規則が満たされたブロックであるが、悪意のあるノード 21 が含まれていた場合等を考慮して、実際に規則が満たされているか等を検証しても良い。
- [0049] ブロック共有部 218 は、ブロックチェーン 2 に属するノード 21 間で情報交換を行う。ブロック共有部 218 は、より具体的には、受付部 214 が受け付けた情報、ブロック生成部 216 が生成したブロック、及び他のノード 21 から受け付けたブロック等を、適宜他のノード 21 に送信する。これにより、可能な限り全てのノード 21 でこれらの情報および最新のブロックチェーン 2 を共有する。
- [0050] なお、図 7 の構成はあくまで一例であって、ブロックチェーンのノード 2

1 は、改ざんが困難なブロックチェーン 2 を複数のノードが共有して管理するための所定のコンセンサス処理を実行可能であり、外部ノードからの要求に応じて分散型のネットワークへの情報追加、及び分散型のネットワークに記録された情報の参照が可能なノードであれば、具体的な構成は問わない。

[0051] なお、サーバ 1 は、ブロックチェーン 2 のノード 2 1 であっても良い。

[0052] 図 8 は、医師端末 3 及び患者端末 4 の構成例を示すブロック図である。

医師端末 3 は、制御部 3 1、記憶部 3 2、通信部 3 3、入力部 3 4 及び表示部 3 5 を含む。各構成はバス B で接続されている。

[0053] 制御部 3 1 は CPU、MPU 等の演算処理装置を含み、記憶部 3 2 に記憶された制御プログラム 3 P（プログラム製品）を読み出して実行することにより、医師端末 3 に係る種々の情報処理、制御処理等を行う。また、制御部 3 1 は、ハッシュ値算出部 3 1 a 及び電子署名作成部 3 1 b を含む。ハッシュ値算出部 3 1 a は、暗号学的ハッシュ関数を用いて、ウォレットアドレス等を算出する処理を行う。また制御プログラム 3 P には、例えばイーサリアムの Geth 等のスマートコントラクトの生成・実行、仮想通貨の送金、アカウントの作成、マイニング等の処理を実行するプログラムが含まれる。電子署名作成部 3 1 b は、偽造又は改ざんを防止するため、公開鍵暗号方式に基づくデジタル認証用の署名を生成する。

[0054] なお、図 8 では制御部 3 1 を単一のプロセッサであるものとして説明するが、マルチプロセッサであっても良い。記憶部 3 2 は RAM、ROM 等のメモリ素子を含み、制御部 3 1 が処理を実行するために必要な制御プログラム 3 P 又はデータ等を記憶している。また、記憶部 3 2 は、制御部 3 1 が演算処理を実行するために必要なデータ等を一時的に記憶する。通信部 3 3 は通信に関する処理を行うための通信モジュールであり、ネットワーク N を介して、サーバ 1 等と情報の送受信を行う。入力部 3 4 は、キーボード、マウスまたは表示部 3 5 と一体化したタッチパネルでも良い。表示部 3 5 は、液晶ディスプレイ又は有機 EL ディスプレイ等であり、制御部 3 1 の指示に従い各種情報を表示する。

- [0055] 患者端末4は、制御部41、記憶部42、通信部43、入力部44、表示部45及び撮影部46を含む。各構成はバスBで接続されている。なお、患者端末4の制御部41、記憶部42、通信部43、入力部44及び表示部45に関しては、医師端末3の制御部31、記憶部32、通信部33、入力部34及び表示部35と同様であるため、説明を省略する。撮影部46は、例えばCCD (Charge Coupled Device)カメラ、CMOS (Complementary Metal Oxide Semiconductor) カメラ等の撮影装置である。なお、撮影部46は患者端末4の中に内蔵せず、外部で直接患者端末4と接続し、撮影可能な構成としても良い。
- [0056] 図9は、研究者端末5の構成例を示すブロック図である。研究者端末5は、制御部51、記憶部52、通信部53、入力部54及び表示部55を含む。各構成はバスBで接続されている。なお、研究者端末5の制御部51、記憶部52、通信部53、入力部54及び表示部55に関しては、医師端末3の制御部31、記憶部32、通信部33、入力部34及び表示部35と同様であるため、説明を省略する。
- [0057] 図10は、電子署名付き医療データを作成する動作を説明する説明図である。まず、患者の属性を予め登録する処理を説明する。患者の属性は、患者の氏名、性別、年齢、生年月日、郵便番号、住所、電話番号、メールアドレス、既往歴、投薬歴または血液型等を含む。なお、患者の属性には、生体が発する種々の生理学的・解剖学的情報である生体データ（例えば、血圧、心電、心音またはX線の吸収率）が含まれても良い。
- [0058] 具体的には、患者端末4は、患者の属性の入力を受け付け、受け付けた患者の属性をサーバ1に送信する。サーバ1は、患者端末4から送信された患者の属性を受信して患者DIDを発行する。例えばサーバ1は、Ethereum（登録商標）のERC725／735、またはSovrin Network等のプラットフォームを利用することにより、患者を特定する患者DIDを発行する。
- [0059] サーバ1は、発行した患者DIDに対応付け、受信した患者の属性を患者

DB171に記憶する。具体的には、サーバ1は患者DIDに対応付け、患者の氏名、生年月日、郵便番号、住所、電話番号、メールアドレス及び登録日時を一つのレコードとして患者DB171に記憶する。

[0060] 次に、医療に関する質問に対する患者による回答を予め登録する処理を説明する。医療に関する質問は、例えばパーキンソン病において、パーキンソン病患者を対象とした疾患特異的QOL (Quality of Life) 質問票であるPDQ-39が利用されても良い。具体的には、患者端末4は、患者による質問の種類（例えば、PDQ-39、MDS-UPDRSまたはEQ-5D）の選択を受け付ける。患者端末4は、受け付けた質問の種類に応じて、該当する質問を記憶部または外部装置から取得して画面に表示する。

[0061] 患者端末4は、画面に表示されている質問に対する患者による回答を受け付け、受け付けた回答を患者DIDに対応付けてサーバ1に送信する。サーバ1は、患者端末4から送信された患者DID及び質問に対する回答を受信し、受信した患者DID及び回答を質問DB173に記憶する。具体的には、サーバ1は、受信した患者DIDに対応付け、質問の種類、質問及び該質問に対する回答を含む質問データを一つのレコードとして質問DB173に記憶する。

[0062] なお、患者の属性及び質問に対する回答のほか、血圧、心拍数、呼吸数または体温など計測を可能にするウェアラブルデバイス、またはバイタルセンサを搭載した端末などにより計測されたバイタルデータ（生体データ）がサーバ1に登録されても良い。例えば、端末2はウェアラブルデバイスを介して、血圧、心拍数、呼吸数または体温などを含むバイタルデータを取得する。端末2は、取得したバイタルデータを、患者の属性及び質問に対する回答と共にサーバ1に登録する。

[0063] 続いて、電子署名付き医療データを作成する処理を説明する。医療データは、患者の属性、質問に対する回答及び医師による該患者に対する診療データを含む。

[0064] 医師の医師端末3は、コードを生成するライブラリを利用し、医師を識別

する医師D I Dを記述したコードを生成する。コードは、一次元コード又は二次元コードを含む。一次元コードは、例えば縞模様状の線の太さによって数値または文字を表すバーコード (Barcode) であっても良い。二次元コードは、例えば横方向にしか情報を持たない一次元コードに対し、水平方向と垂直方向に情報を持つ表示方式のQRコード (登録商標) であっても良い。以下では、二次元コードの例を説明する。医師D I Dは、例えばE t h e r e u mのERC725/735、またはSovrin Network等のプラットフォームを利用して発行されても良い。

[0065] 医師端末3は、生成した二次元コードを画面に表示する。患者が医師の診断を受けた場合、患者端末4は、医師端末3上で表示されている二次元コードを読み取る。患者端末4は、二次元コードの解析ライブラリを利用し、読み取った二次元コードから医師D I Dを取得する。なお、本実施形態では、二次元コードを用いる例を挙げたが、これに限るものではない。例えば、ICタグ(Integrated Circuit Tag)、RFタグ(Radio Frequency Tag)、またはRFID(Radio Frequency Identifier)チップ (マイクロチップ) 等に記憶された医師D I DをRFリーダで読み取る形態であっても良く、または、バーコードに記憶された医師D I Dを読み取る形態であっても良い。更にまた、医師D I Dが手動入力で受け付けられても良い。

[0066] 患者端末4は、取得した医師D I Dと患者D I Dとをサーバ1に送信する。サーバ1は、患者端末4から送信された医師D I D及び患者D I Dを受信する。サーバ1は、受信した患者D I Dに基づいて患者の属性及び質問に対する回答を取得する。具体的には、サーバ1は、患者D I Dに基づいて患者DB171から患者の属性を取得する。サーバ1は、患者D I Dに基づいて質問DB173から質問に対する回答を取得する。

[0067] サーバ1は、患者D I Dと、取得した患者の属性及び質問に対する回答とを、受信した医師D I Dに対応する医師端末3に送信する。医師端末3は、サーバ1から送信された患者D I D、患者の属性及び質問に対する回答を受信する。医師端末3は、医師による患者に対する診療データの入力を受け付け

ける。例えばパーキンソン病などの疾患の重症度分類、処方情報（薬剤の成分名、剤型または用量等）、血圧または脈拍等が診療データに含まれる。

[0068] 医師端末3は、患者の属性、質問に対する回答及び診療データを含む医療データに対する電子署名の指示を受け付けた場合、該医療データに対して電子署名処理（暗号化）を行う。電子署名処理とは、与えられたデータに対し秘密鍵を用いた電子署名を行う機能である。通常は与えられたデータを暗号学的ハッシュ関数で変換したハッシュ値を暗号化する。暗号学的ハッシュ関数は、デジタル文書の改ざんを検出する一方向の暗号処理方法であり、出力値は常に16進数表記として64桁と固定されている。ハッシュ関数は何を用いても良く、例えば、SHA（Secure Hash Algorithm）-1またはSHA-256を用いることができる。なお、電子署名の対象となるデータのサイズが小さい場合には、ハッシュ値ではなく、データそのものを暗号化したものを電子署名として用いても良い。

[0069] なお、本実施形態では、医師により医療データに対して電子署名を行ったが、これに限るものではない。例えば、臨床検査技師、理学療法士または介護士等の医療関連の有資格者により医療データに対して電子署名を行っても良い。

[0070] 医師端末3は、患者DID及び医師DIDに対応付け、電子署名付き医療データをサーバ1に送信する。サーバ1は、医師端末3から送信された患者DID、医師DID及び電子署名付き医療データを受信する。サーバ1は、公開鍵を用いて電子署名付き医療データを復号する。サーバ1は、医療データを特定する医療データIDを作成する。例えばサーバ1は、Ethereumの一つのスマートコントラクト規格であるERC721を利用し、「価値」を証明することができる非代替性トークン（NFT）を医療データIDとして作成しても良い。ERC721規格を用いれば、ブロックチェーン2上の全ての医療データIDを開示しているが、改ざんすることはできないため、所有者または帰属情報等を付けることが可能となる。

[0071] サーバ1は、作成した医療データIDに対応付け、患者DID、復号した

医療データ、医師D I D、電子署名日時及び「署名済み」となった状態を一つのレコードとして医療データDB 174に記憶する。サーバ1は、医療データを患者端末4に送信する。患者端末4は、サーバ1から送信された医療データを受信して画面に表示する。患者端末4は、患者から該医療データをブロックチェーン2に出力（記録）する指示を受け付けた場合、ブロックチェーン2への出力指示をサーバ1に送信する。出力指示には、患者D I D及び医療データI Dが含まれる。サーバ1は、患者端末4から送信されたブロックチェーン2への出力指示を受信し、受信した出力指示に応じて該医療データのハッシュ値をブロックチェーン2に出力する。

[0072] 具体的には、サーバ1は、暗号的ハッシュ関数を用いて医療データのハッシュ値を算出する。例えばサーバ1は、SHA 2-256アルゴリズムを用いたハッシュ関数を採用し、医療データのハッシュ値を算出する。なお、ハッシュ関数に限らず、他の暗号化方式であっても良い。サーバ1は、患者D I D、医師D I D及び医療データI Dに対応付け、算出した医療データのハッシュ値をブロックチェーン2のいずれかのノード21に送信する。ブロックチェーン2のノード21は、サーバ1から送信された患者D I D、医師D I D、医療データI D及び医療データのハッシュ値を受信して記録する。サーバ1は、医療データI Dに対応付け、医療データのハッシュ値、ブロックチェーン2への記録日時、及び「BCへ記録済み」となった状態を医療データDB 174に記憶する。

[0073] 図11は、医療データをブロックチェーン2に記録する処理を説明する説明図である。ブロックチェーン2の一つのノード21は、サーバ1から送信された取引データ（トランザクション）を受信する。図示のように、患者D I D、医師D I D、医療データI D及び医療データのハッシュ値が取引データに含まれる。ノード21は、受信した取引データに含まれている患者D I D、医師D I D、医療データI D及び医療データのハッシュ値と、自身が管理しているブロックチェーンの情報とを基に作成した前ブロック管理情報とを少なくとも含むブロックを生成する。

- [0074] そして、ブロックチェーン2の各々のノード21は、所定のコンセンサスアルゴリズムに従った処理を実行する。例えばビットコイン（登録商標）に係るブロックチェーン技術を本システムに応用した場合、ノード21、ノード21、ノード21…は、P o W（Proof of Work）と呼ばれる演算処理を実行し、ブロックチェーン2を更新するノード21を決定する。P o Wは、新たに生成するブロックの一つ前のブロックに予め格納されたハッシュ値から、ある正解値を探索する（マイニング）演算処理である。
- [0075] ノード21は、新たにブロックを生成する場合、当該ブロックの一つ前のブロックに格納されたハッシュ値及び取引データをハッシュ化したハッシュ値を生成し、最新のブロックに格納する。例えば図11に示すように、ブロック3を生成する場合、ノード21は、ブロック2に格納されているハッシュ値と、複数の取引データとをハッシュ化してハッシュ値を生成し、ブロック3に格納する。例えばビットコインの例では、ノード21は演算処理の難易度を上げる目的で、取引データのほかにナンス値をヘッダに挿入してハッシュ値を生成する。ナンス値は、ハッシュ値のヘッダにゼロが所定数連続するような値であり、ナンス値に係るゼロの数を適切な数に設計することで、演算処理の処理負荷が調整される。
- [0076] 各ノード21は、最新のブロックを生成する場合、前のブロックに含まれる当該ハッシュ値から正解値（ビットコインの例ではナンス値）を探索するという探索問題を解く。例えば図11に示すように、ブロック3を新たに生成する場合、各ノード21は、ブロック2のブロックに格納されているハッシュ値から正解値を探索する。1回の演算処理で正解値を探し当てる確率は低く、例えばビットコイン等の仮想通貨に係るブロックチェーン技術を応用した場合、平均して10分程度の時間を要する。各ノード21は一斉に探索問題の演算処理を実行し、正解値を探索する。そして、最も早く正解値を探し当てたノード21に、最新のブロックを生成する権限が与えられる。不正者がブロックチェーンのデータを書き換えようとする場合、善意の検証者（ノード21）全ての演算処理速度を上回る速度でブロックを生成する必要が

あり、実際に不正な書き換えを行うことは極めて難しくなっている。

[0077] 探索に成功した場合、ノード21は、検証した取引データ（患者DID、医師DID、医療データID及び医療データのハッシュ値）を格納した最新のブロックを生成し、当該ブロックに係るデータを他のノード21、21、21…に通知する。この場合、上述の如くノード21は、一つ前のブロックに格納されているハッシュ値及び取引データからハッシュ値を生成し、当該ハッシュ値を新たなブロックに格納した上で各ノード21に通知する。

[0078] 例えば図11に示すように、ノード21は、ブロック2に格納されているハッシュ値及び取引データをハッシュ化したハッシュ値を生成し、新たなブロック3に格納して他のノード21、21、21…に通知する。新たなブロックに格納されたハッシュ値は、一つ前のブロックのハッシュ値を含むことから、ブロックチェーンを構成する各ブロックは時系列的に関連付けられている。他のノード21、21、21…は、通知されたブロックのデータの正当性を確認した後、取引データを記憶部212に記憶する。これにより、各ノード21、21、21…の記憶部212には、同一のブロックチェーンに係るデータが複製されて記憶される。

[0079] なお、探索に成功したノード21の管理者（マイナー）には、探索に成功した報酬が与えられる。すなわち、探索に成功したノード21の管理者に、当該ブロックに格納されている各取引の手数料が支払われる。これにより、管理者にはノード21という計算資源を投入するインセンティブが与えられる。

[0080] なお、上記ではブロックチェーンの更新権限を決定する手法としてPoWを用いたが、本実施の形態はこれに限定されるものではなく、例えばPOI（Proof of Importance）、POS（Proof of Stake）等を用いても良い。また、上記ではビットコイン技術を応用したシステムについて説明したが、本実施の形態はこれに限定されるものではない。例えばビットコイン以外に、イーサリアム、ハイパーレジャー・ファブリック（Hyperledger Fabric）等に係るブロックチェーン技術を応用しても良い。

- [0081] 続いて、ブロックチェーン2に記録された医療データを用いて医療を研究する研究者からの医療データの開示要求に応じて、該医療データを研究者端末5に出力する処理を説明する。
- [0082] 図12は、医療データを研究者端末5に出力する動作を説明する説明図である。なお、研究者の属性が予め登録される。研究者の属性は、研究者の氏名、生年月日、郵便番号、住所、電話番号、メールアドレス、プロフィールまたは研究目的等を含む。なお、研究者の登録処理に関しては、患者の登録処理と同様であるため、説明を省略する。
- [0083] 研究者端末5は、研究者による医療データの開示要求を受け付けた場合、受け付けた開示要求を、研究者DID及び医療データIDに対応付けてサーバ1に送信する。サーバ1は、研究者端末5から送信された研究者DID、医療データID及び開示要求を、該医療データを提供した患者の患者端末4に送信する。なお、開示要求と共に研究者のメッセージまたはプロフィールが患者端末4に送信されても良い。この場合、患者端末4は、研究者のメッセージまたはプロフィールを開示要求と共に画面に表示する。
- [0084] 患者端末4は、サーバ1から送信された開示要求に応じて、医療データの開示要求に対する承認情報を受け付けた場合、受け付けた承認情報をサーバ1に送信する。サーバ1は、患者端末4から送信された承認情報に応じて、研究者から患者へ所定のトークンを支払うトランザクションを作成する。トランザクションとは、ブロックチェーン2における取引記録であり、ブロックチェーン2の参加者間での各種の情報及び価値の移転を記憶している。作成されたトランザクションは、研究者のウォレットアドレス、患者のウォレットアドレス、支払ったトークン数量及び取引日時を含む。
- [0085] ウォレットアドレスは、取引ごとに作成された仮想通貨用の口座番号であり、文字列又はQRコードとして表示する。ウォレットアドレスは、ブロックチェーン2で利用されている公開鍵暗号を基にして、数学的に導出されたアドレスである。また、送信元と送信先のウォレットアドレスは、ブロックチェーン2のノード21に記録され、ブロックチェーン2のシステムが維持

し続ける限り改ざんされない。ウォレットアドレスは計算で生成されるため、オンライン又はオフラインでも作成することが可能となる。

[0086] サーバ1は、ブロックチェーン2のいずれかのノード21に、作成したトランザクションを送信する。ブロックチェーン2のノード21は、トランザクションを受信してトークンの支払処理を実行する。なお、本実施形態では、研究者が医療データを提供した患者にトークンを支払ったが、これに限るものではない。例えば、研究者が医療データに電子署名した医師のみに所定のトークンを支払っても良い。または、研究者が医療データを提供した患者と、該医療データに電子署名した医師との両方に所定のトークンを支払っても良い。更にまた、研究者の開示要求にもかかわらず、医師が医療データに電子署名した場合、例えばスポンサーまたはシステム運営者が該医師に所定のトークンを支払っても良い。

[0087] なお、本実施形態では、トークンの一種である仮想通貨（暗号資産）の例を説明したが、これに限るものではない。例えば、電子マネー、クーポンまたはポイント等の他の種類のトークンにも同様に適用することができる。

[0088] ノード21は、トークンの支払処理を実行した後に、医療データIDに基づいて該医療データのハッシュ値を取得する。ノード21は、取得した医療データのハッシュ値をサーバ1に送信する。サーバ1は、ノード21から送信された医療データのハッシュ値を受信する。サーバ1は、医療データIDに基づいて該医療データのハッシュ値を医療データDB174から取得する。サーバ1は、ノード21から送信された医療データのハッシュ値と、医療データDB174に記憶された医療データのハッシュ値とを照合する。サーバ1は、両者が一致していると判定した場合、該医療データのハッシュ値に対応する医療データを医療データDB174から取得する。サーバ1は、取得した医療データを研究者端末5に送信する。研究者端末5は、サーバ1から送信された医療データを受信して画面に表示する。

[0089] なお、上述したトークンの支払処理に限らず、スマートコントラクトを利用しても良い。スマートコントラクトは、事前に執行条件及び契約内容の定

義がプログラム化されてトランザクションに組み込まれ、執行条件及び契約内容に合致した取引が発生した場合、自動的に契約が履行される仕組みである。サーバ1は、医療データの取引処理を行うための必要な執行条件、患者及び研究者のウォレットアドレス等が記述されたスマートコントラクトのコードを生成する。サーバ1は、生成したスマートコントラクトのコードを含むトランザクションをブロックチェーン2のいずれかのノード21に送信する。ブロックチェーン2のノード21は、受信したスマートコントラクトを含むトランザクションを記録する。

[0090] スマートコントラクトのコードの内容は、例えば研究者の開示要求に対する患者の承認を得た場合、研究者のウォレットアドレス宛から患者のウォレットアドレス宛に所定のトークンを支払う契約をコードで定義している。トランザクションは、スマートコントラクトのコード、患者及び研究者の電子署名を含む。ブロックチェーン2のノード21は、研究者の開示要求に対する患者の承認を得た執行条件に合致した場合、契約内容上で決められた所定のトークンを研究者のウォレットアドレス宛から患者のウォレットアドレス宛に支払う。

[0091] なお、本実施形態では、研究者が患者にトークンを支払う例を説明したが、これに限らず、例えばスポンサーまたはシステム運営者が患者に所定のトークンを支払っても良い。

[0092] 図13は、質問に対する回答の入力画面の一例を示す説明図である。該画面は、回答入力欄11a、保存ボタン11b及びサブミットボタン11cを含む。回答入力欄11aは、医療に関する質問に対する患者による回答の入力を受け付ける入力欄である。保存ボタン11bは、質問に対する回答を下書き保存するボタンです。サブミットボタン11cは、質問に対する回答をサーバ1に送信（サブミット）するボタンである。

[0093] なお、図13では、質問の種類がPDQ-39である例を説明するが、他の質問の種類にも同様に適用される。患者端末4は、PDQ-39をサーバ1の記憶部12または外部装置から取得する。患者端末4は、取得したPD

Q-39を回答入力欄11aに表示する。患者端末4は、回答入力欄11aの入力操作を受け付けた場合、質問に対する患者による回答を受け付ける。患者端末4は、保存ボタン11bのタッチ（クリック）操作を受け付けた場合、回答入力欄11aにより入力された回答を下書き保存する。患者端末4は、サブミットボタン11cのタッチ操作を受け付けた場合、回答入力欄11aにより入力された回答と患者の属性とを患者DIDに対応付けてサーバ1に送信する。

[0094] 図14は、医療データの作成画面の一例を示す説明図である。該画面は、QRコード生成ボタン12a、患者からデータ取得ボタン12b、QRコード表示欄12c、患者属性表示欄12d、閲覧ボタン12e、診療データ受付欄12f、署名送信ボタン12g及び結果表示欄12hを含む。

[0095] QRコード生成ボタン12aは、医師DIDを記述したQRコードを生成するボタンである。患者からデータ取得ボタン12bは、患者から患者の属性及び質問に対する回答を取得するボタンである。QRコード表示欄12cは、QRコードを表示する表示欄である。患者属性表示欄12dは、患者の属性を表示する表示欄である。

[0096] 閲覧ボタン12eは、質問に対する回答を表示するボタンである。なお、閲覧ボタン12eの数が、質問の種類に基づいて設けられても良い。図示のように、「PDQ-39」、「MDS-UPDRS」及び「EQ-5D」それぞれの閲覧ボタン12eが設けられる。医師端末3は、質問に対する回答をサーバ1から取得したと判定した場合、該当する閲覧ボタン12eのタイトルを「閲覧」に設定し、閲覧ボタン12eを操作可能なアクティブ（活性）状態に設定する。また、医師端末3は、質問に対する回答をサーバ1から取得していないと判定した場合、該当する閲覧ボタン12eのタイトルを「データなし」に設定し、閲覧ボタン12eを操作不可能な非アクティブ（非活性）状態に設定する。

[0097] 診療データ受付欄12fは、医師が患者を診断した診療データの入力を受け付ける受付欄である。署名送信ボタン12gは、患者の属性、質問に対する

る回答及び診療データを含む医療データを電子署名して送信するボタンである。結果表示欄12hは、医療データに対する電子署名及び送信処理の結果を表示する表示欄である。

[0098] 医師端末3は、QRコード生成ボタン12aのクリック（タッチ）操作を受け付けた場合、二次元コードを生成するライブラリを利用し、医師DIDを記述したQRコードを生成する。医師端末3は、生成したQRコードをQRコード表示欄12cに表示する。患者端末4は、医師端末3上で表示されているQRコードを読み取ることにより医師DIDを取得する。

[0099] 患者端末4は、取得した医師DIDと患者DIDとをサーバ1に送信する。サーバ1は、患者端末4から送信された医師DID及び患者DIDを受信し、受信した患者DIDに基づいて患者の属性及び質問に対する回答を患者DB171及び質問DB173から取得する。サーバ1は、取得した患者の属性及び質問に対する回答を、受信した医師DIDに対応する医師端末3に送信する。

[0100] また、患者からデータ取得ボタン12bにより患者の属性及び質問に対する回答を取得することができる。具体的には、医師端末3は、患者からデータ取得ボタン12bのクリック操作を受け付けた場合、患者DIDの入力を受け付けるためのサブ画面を生成する。医師端末3は、生成したサブ画面に患者DIDの入力を受け付け、受け付けた患者DIDをサーバ1に送信する。その後、上述した処理と同様に、患者の属性及び質問に対する回答がサーバ1から取得される。

[0101] 医師端末3は、サーバ1から送信された患者の属性及び質問に対する回答を受信する。医師端末3は、受信した患者の属性を患者属性表示欄12dに表示する。医師端末3は、閲覧ボタン12eのクリック操作を受け付けた場合、該当する質問に対する回答をサブ画面に表示する。例えば、医師端末3は、「PDQ-39」に対応する閲覧ボタン12eのクリック操作を受け付けた場合、質問に対する回答を表示するためのサブ画面を生成する。医師端末3は、受信した質問に対する回答から「PDQ-39」に対する回答を取

得し、取得した「PDQ-39」に対する回答をサブ画面に表示する。

- [0102] 医師端末3は、診療データ受付欄12fの入力操作を受け付ける。診療データは、診断データ、治療データ及び検査データを含む。診断データは、病状情報及び疾患情報（例えば、医師により決定された疾患名）等の診断に関するデータである。治療データは、患者の疾患に対する治療方針、治療法、手術情報または薬剤情報等の治療に関するデータである。検査データは、疾患の有無またはその程度を調べるために、患者が受けた各種の検査（例えば、血液検査）に関するデータである。
- [0103] 図示のように、医師端末3は、重症度分類を含む診断データ、処方情報（薬剤の成分名、剤型または用量等）を含む治療データ、並びに、医療診断画像、嗅覚検査、血圧及び脈拍を含む検査データの入力を診療データ受付欄12fにより受け付ける。医療診断画像は、例えばMRI(Magnetic Resonance Image)、DAT(Dopamine transporter) Scan、Cardiac MIBG(123I-metaiodobenzylguanidine) ScintigraphyまたはBrain Perfusion SPECT(Single Photon Emission Computed Tomography)等の検査により得られた画像である。なお、図14では、パーキンソン病の検査項目の例を説明したが、これに限らず、他の種類の疾患の検査項目にも同様に適用される。
- [0104] 医師端末3は、署名送信ボタン12gのクリック操作を受け付けた場合、患者の属性、質問に対する回答及び診療データを含む医療データを電子署名し、電子署名付き医療データを患者DID及び医師DIDに対応付けてサーバ1に送信する。医師端末3は、医療データに対する電子署名及び送信処理の結果を結果表示欄12hに表示する。図示のように、「署名&送信に成功しました」が結果表示欄12hに表示される。
- [0105] 図15は、患者端末4側での医療データの表示画面の一例を示す説明図である。なお、図15は電子署名未取得の医療データの例示である。該画面は、医療データID表示欄13a、状態アイコン13b、日時表示欄13c、医師表示ボタン13d、開示要求表示欄13e、開示請求ボタン13f及び取引履歴表示ボタン13gを含む。

- [0106] 医療データID表示欄13aは、医療データIDを表示する表示欄である。状態アイコン13bは、医療データの状態を示すアイコンである。日時表示欄13cは、医療データの各状態の更新日時を表示する表示欄である。医師表示ボタン13dは、医療データを電子署名した医師の属性を表示する表示欄である。開示要求表示欄13eは、開示要求に関する情報を表示する表示欄である。開示請求ボタン13fは、後述の開示要求の応答画面（図18）に遷移するためのボタンである。取引履歴表示ボタン13gは、後述の取引履歴画面（図19）に遷移するためのボタンである。
- [0107] 患者端末4は患者DIDに基づいて、医療データに関する情報をサーバ1の管理DB177から取得する。医療データに関する情報は、医療データID、医療データの状態（下書き保存、サブミット済み、署名済み及びBCへ記録済み）、及び各状態の更新日時を含む。患者端末4は、医療データIDごとに医療データに関する情報を画面に表示する。
- [0108] 具体的には、患者端末4は、医療データIDを医療データID表示欄13aに表示する。患者端末4は、医療データの状態に応じて該当するアイコンを状態アイコン13bに表示する。図示のように、患者端末4は、医療データの状態が「サブミット済み」とであると判定した場合、「サブミット済み」状態を示すアイコンを状態アイコン13bに表示し、医師表示ボタン13dを操作不可能な非アクティブ状態に設定する。
- [0109] 患者端末4は、各状態の更新日時を日時表示欄13cに表示する。図示のように、「下書き保存」の日時、「サブミット済み」の日時、「署名済み」の日時及び「BCへ記録済み」の日時が日時表示欄13cに表示される。なお、医師からの電子署名を未取得の状態であるため、「署名済み」の日時の代わりに、「医師に署名を依頼してください」となる提示情報が日時表示欄13cに表示される。また、該医療データがブロックチェーン2に記録されていないため、「BCへ記録済み」の日時の代わりに、「－」が日時表示欄13cに表示される。
- [0110] 患者端末4は、医療データの状態に応じて開示請求ボタン13f及び取引

履歴表示ボタン 13 g のアクティブ状態を設定する。具体的には、患者端末 4 は、医療データの状態が「下書き保存」、「サブミット済み」または「署名済み」であると判定した場合、開示請求ボタン 13 f 及び取引履歴表示ボタン 13 g を操作不可能な非アクティブ状態に設定する。患者端末 4 は、医療データの状態が「ＢＣへ記録済み」であると判定した場合、開示請求ボタン 13 f 及び取引履歴表示ボタン 13 g を操作可能なアクティブ状態に設定する。

[0111] 図 1 6 は、患者端末 4 側での医療データの表示画面の一例を示す説明図である。なお、図 1 6 は電子署名取得済みの医療データの例示である。なお、図 1 5 と重複する内容については同一の符号を付して説明を省略する。

[0112] 患者端末 4 は患者 ＤＩＤ に基づいて、医療データに関する情報をサーバ 1 の管理 ＤＢ 1 7 7 から取得する。医療データに関する情報は、医療データ ＩＤ、医療データの状態、各状態の更新日時、医療データを電子署名した医師の医師 ＤＩＤ 及び属性を含む。

[0113] 患者端末 4 は、医療データの状態が「署名済み」であると判定した場合、「署名済み」状態を示すアイコンを状態アイコン 13 b に表示し、医師による署名済みの日時を日時表示欄 13 c に表示する。患者端末 4 は、医師表示ボタン 13 d を操作可能なアクティブ状態に設定する。患者端末 4 は、医師表示ボタン 13 d のタッチ操作を受け付けた場合、医療データ ＩＤ をサーバ 1 に送信する。サーバ 1 は、患者端末 4 から送信された医療データ ＩＤ に基づいて該医療データを署名した医師の医師 ＤＩＤ を医療データ ＤＢ 1 7 4 から取得する。

[0114] サーバ 1 は、取得した医師 ＤＩＤ に基づいて医師の属性を医師 ＤＢ 1 7 2 から取得する。医師の属性は、医師の氏名、及び医師が所属する医療機関の名称を含む。サーバ 1 は、取得した医師 ＤＩＤ 及び医師の属性を患者端末 4 に送信する。患者端末 4 は、サーバ 1 から送信された医師 ＤＩＤ 及び医師の属性を受信し、受信した医師 ＤＩＤ 及び医師の属性を日時表示欄 13 c (「署名済み」の日時と「ＢＣへ記録済み」の日時との間の領域) に表示し、医

師表示ボタン 13 d のタイトルを「医師非表示」に変更する。

[0115] 図 17 は、患者端末 4 側での医療データの表示画面の一例を示す説明図である。なお、図 17 はブロックチェーン 2 への記録済みの医療データの例示である。なお、図 15 及び図 16 と重複する内容については同一の符号を付して説明を省略する。

[0116] 患者端末 4 は患者 D I D に基づいて、医療データに関する情報及び開示要求に関する情報をサーバ 1 から取得する。医療データに関する情報は、医療データ I D、医療データの状態、各状態の更新日時、医療データを電子署名した医師の医師 D I D 及び属性を含む。開示要求に関する情報は、医療データに対する開示要求の数量、承認待ちの数量、「開示のみ」で承認済みの数量、及び「開示 & 共有」で承認済みの数量を含む。

[0117] 具体的には、患者端末 4 は、患者 D I D をサーバ 1 に送信する。サーバ 1 は、患者端末 4 から送信された患者 D I D を受信する。サーバ 1 は、受信した患者 D I D に基づいて医療データに関する情報を管理 D B 177 から取得する。サーバ 1 は、患者 D I D 及び医療データ I D に基づいて、医療データの開示要求に関する情報を管理 D B 177 から取得する。

[0118] サーバ 1 は、取得した医療データに関する情報及び開示要求に関する情報を患者端末 4 に送信する。患者端末 4 は、サーバ 1 から送信された医療データに関する情報及び開示要求に関する情報を受信して画面に表示する。なお、医療データに関する情報の表示処理に関しては、図 16 と同様であるため、説明を省略する。患者端末 4 は、受信した開示要求に関する情報を開示要求表示欄 13 e に表示する。図示のように、医療データに対する開示要求の数量、承認待ちの数量、「開示のみ」で承認済みの数量、及び「開示 & 共有」で承認済みの数量が開示要求表示欄 13 e に表示される。

[0119] 患者端末 4 は、医療データの状態が「BC へ記録済み」とであると判定した場合、「BC へ記録済み」状態を示すアイコンを状態アイコン 13 b に表示し、「BC へ記録済み」の日時を日時表示欄 13 c に表示し、開示請求ボタン 13 f 及び取引履歴表示ボタン 13 g を操作可能なアクティブ状態に設定

する。患者端末4は、開示請求ボタン13fのタッチ操作を受け付けた場合、後述の開示要求の応答画面（図18）に遷移する。患者端末4は、取引履歴表示ボタン13gのタッチ操作を受け付けた場合、後述の医療データの取引履歴画面（図19）に遷移する。

[0120] 図18は、患者端末4側での開示要求の応答画面の一例を示す説明図である。なお、図15～図17と重複する内容については同一の符号を付して説明を省略する。該画面は、開示要求表示欄14a、承認ボタン14b、否認ボタン14c、撤回ボタン14d及び承認種別設定ダイアログ14eを含む。

[0121] 開示要求表示欄14aは、医療データの開示要求に関する情報を表示する表示欄である。承認ボタン14bは、医療データの開示要求に応じて承認処理を行うためのボタンである。否認ボタン14cは、医療データの開示要求に応じて否認処理を行うためのボタンである。撤回ボタン14dは、承認済みの医療データに対して承認の撤回処理を行うためのボタンである。承認種別設定ダイアログ14eは、医療データに対する承認種別の設定を受け付けるダイアログ（子画面）である。

[0122] 患者端末4は、医療データIDに基づいて該医療データの開示要求に関する情報をサーバ1から取得する。患者端末4は、取得した開示要求に関する情報を開示要求表示欄14aに表示する。図示のように、研究者ID、申請日時及び要求状況（例えば、承認待ち）が開示要求表示欄14aに表示される。なお、開示要求に関する情報は、上記の項目に限らず、例えば研究者の氏名及びメールアドレス等を含んでも良い。

[0123] 患者端末4は、承認ボタン14bのタッチ操作を受け付けた場合、承認種別設定ダイアログ14eを生成して画面に表示する。承認種別設定ダイアログ14eは、承認種別設定ラジオボタン14f及びダイアログ内承認ボタン14gを含む。承認種別設定ラジオボタン14fは、医療データに対する承認種別（「開示のみ」または「開示&共有」）を受け付けるラジオボタンである。ダイアログ内承認ボタン14gは、承認種別に応じて医療データの承

認処理を行うためのボタンである。

- [0124] 患者端末4は、承認種別設定ラジオボタン14fのタッチ操作を受け付けた場合、承認種別の設定を受け付ける。患者端末4は、ダイアログ内承認ボタン14gのタッチ操作を受け付けた場合、承認種別設定ラジオボタン14fにより設定された承認種別を医療データIDに対応付けてサーバ1に送信する。
- [0125] 患者端末4は、否認ボタン14cのタッチ操作を受け付けた場合、医療データIDに対応付け、該医療データの利用を否認したことを示す否認情報をサーバ1に送信する。患者端末4は、撤回ボタン14dのタッチ操作を受け付けた場合、医療データIDに対応付け、該承認済みの医療データを承認撤回したことを示す承認撤回情報をサーバ1に送信する。
- [0126] 図19は、患者端末4側での医療データの取引履歴画面の一例を示す説明図である。なお、図15～図17と重複する内容については同一の符号を付して説明を省略する。該画面は、取引履歴表示欄15aを含む。取引履歴表示欄15aは、医療データの取引履歴を表示する表示欄である。
- [0127] 患者端末4は、患者DID及び医療データIDをサーバ1に送信する。サーバ1は、患者端末4から送信されたDID及び医療データIDを受信する。サーバ1は、受信した患者DID及び医療データIDに基づいて、医療データの取引履歴を取引履歴DB176から取得する。サーバ1は、取得した取引履歴を患者端末4に送信する。患者端末4は、サーバ1から送信された取引履歴を受信して取引履歴表示欄15aに表示する。図示のように、研究者DID、患者DID、取引履歴日時及び医療データのハッシュ値を含む取引履歴が取引履歴表示欄15aに表示される。
- [0128] 図20は、患者端末4側での医療データの詳細画面の一例を示す説明図である。なお、図15～図17と重複する内容については同一の符号を付して説明を省略する。該画面は、医療データ表示欄16aを含む。医療データ表示欄16aは、医療データの詳細情報を表示する表示欄である。
- [0129] 患者端末4は、患者DID及び医療データIDをサーバ1に送信する。サ

サーバ1は、患者端末4から送信されたD I D及び医療データ I Dを受信する。サーバ1は、受信した患者D I D及び医療データ I Dに基づいて、患者の属性、医療に関する質問に対する患者による回答（例えば、PDQ-39に対する回答）、及び医師による患者に対する診療データ（例えば、血圧、処方情報または脈拍）を含む医療データを医療データDB174から取得する。サーバ1は、取得した医療データを患者端末4に送信する。患者端末4は、サーバ1から送信された医療データを受信して医療データ表示欄16aに表示する。

[0130] 図21は、研究者端末5側での医療データ管理画面の一例を示す説明図である。該画面は、研究者表示欄17a、管理情報表示欄17b、アクションボタン17c及び患者D I Dリンク17dを含む。研究者表示欄17aは、研究者の氏名を表示する表示欄である。管理情報表示欄17bは、医療データの管理情報を表示する表示欄である。

[0131] アクションボタン17cは、医療データに対するアクションを受け付けるボタンである。アクションは、「データ請求」及び「閲覧」を含む。「データ請求」アクションは、医療データを提供した患者に該医療データの開示要求を送信するアクションである。「閲覧」アクションは、医療データを閲覧（表示）するアクションである。なお、本実施形態では、アクションが「データ請求」及び「閲覧」を含む例を説明したが、これに限るものではない。例えば、アクションには「再承認」または「再請求」が含まれても良い。「再承認」アクションは、研究者の開示要求に応じて一旦開示が拒否された医療データに対し、再び承認の要求を送信するアクションである。「再請求」アクションは、医療データに対して開示可能な期間（例えば、一年）が設けられた場合、開示可能な期間を過ぎた後に、医療データを提供した患者に該医療データの開示要求を再送信するアクションである。患者D I Dリンク17dは、後述の医療データの表示画面（図29）に遷移するためのボタンである。

[0132] 研究者端末5は、研究者D I Dをサーバ1に送信する。サーバ1は、研究

者端末5から送信された研究者D I Dを受信し、受信した研究者D I Dに基づいて研究者の氏名及び研究機関I Dを研究者DB 175から取得する。サーバ1は研究者D I Dに基づいて、患者D I D、開示要求に関する情報及び医師による医療データの署名日時を管理DB 177から取得する。サーバ1は、取得した研究者の氏名、研究機関I D、患者D I D、開示要求に関する情報及び医師による医療データの署名日時を研究者端末5に送信する。

[0133] 研究者端末5は、サーバ1から送信された研究者の氏名、研究機関I D、患者D I D、開示要求に関する情報及び医療データの署名日時を受信する。研究者端末5は、受信した研究者の氏名を研究者表示欄17aに表示し、研究機関I D、患者D I D、開示要求に関する情報及び医療データの署名日時を管理情報表示欄17bに表示する。開示要求に関する情報は、データ種類、開示要求状況、開示要求日時、承認日時、否認日時及び承認撤回日時を含む。開示要求状況は、データ未請求、承認済（閲覧&共有）、承認済（閲覧のみ）、撤回済及び保留中を含む。

[0134] 図示のように、研究機関I D、患者D I D（データ所有者）、データ種類、開示要求（リクエスト）状況、開示要求状況に応じて生成されたアクションボタン17c、医師署名日時、研究者の開示要求（リクエスト）日時、患者の承認日時、患者の否認日時及び患者の承認撤回日時が管理情報表示欄17bに表示される。

[0135] 研究者端末5は、開示要求状況に応じて、アクションボタン17cのタイトル及びアクティブ状態を設定する。具体的には、研究者端末5は、開示要求状況が「データ未請求」とであると判定した場合、アクションボタン17cのタイトルを「データ請求」に設定し、アクションボタン17cを操作可能なアクティブ状態に設定する。研究者端末5は、開示要求状況が「撤回済」または「保留中」とであると判定した場合、アクションボタン17cのタイトルを「データ請求」に設定し、アクションボタン17cを操作不可能な非アクティブ状態に設定する。研究者端末5は、開示要求状況が「承認済（閲覧&共有）」または「承認済（閲覧のみ）」であると判定した場合、アクショ

ンボタン 17c のタイトルを「閲覧」に設定し、アクションボタン 17c を操作可能なアクティブ状態に設定する。

- [0136] 研究者端末 5 は、タイトルが「データ請求」であるアクションボタン 17c のタッチ操作を受け付けた場合、研究者 D I D 及び医療データ I D をサーバ 1 に送信する。サーバ 1 は、研究者端末 5 から送信された研究者 D I D 及び医療データ I D を受信し、受信した研究者 D I D 及び医療データ I D に基づいて該医療データの開示要求を作成する。サーバ 1 は、作成した開示要求を患者端末 4 に送信する。
- [0137] 研究者端末 5 は、タイトルが「閲覧」であるアクションボタン 17c のタッチ操作を受け付けた場合、医療データ I D に基づいて医療データをサーバ 1 の医療データ D B 174 から取得する。研究者端末 5 は、取得した医療データを画面に表示する。患者が一度研究者に医療データの開示を承認した場合、該医療データを継続して閲覧することができる。または、医療データに対して開示可能な期間が設けられても良い。例えば、所定期間（例えば、一年）内に、研究者が該医療データを繰り返して閲覧することができる。
- [0138] 研究者端末 5 は、患者 D I D リンク 17d のクリック操作を受け付けた場合、開示要求状況を判定する。研究者端末 5 は、開示要求の状況が「承認済（閲覧＆共有）」または「承認済（閲覧のみ）」であると判定した場合、該患者 D I D に対応する患者が所有している医療データの表示画面（図 29）に遷移する。
- [0139] 図 22 は、研究者端末 5 側での取引履歴画面の一例を示す説明図である。該画面は、取引履歴表示欄 18a を含む。取引履歴表示欄 18a は、取引履歴を表示する表示欄である。研究者端末 5 は、研究者 D I D をサーバ 1 に送信する。サーバ 1 は、研究者端末 5 から送信された研究者 D I D を受信し、受信した研究者 D I D に基づいて該研究者の医療データの取引履歴を取引履歴 D B 176 から取得する。サーバ 1 は、取得した取引履歴を研究者端末 5 に送信する。
- [0140] 研究者端末 5 は、サーバ 1 から送信された取引履歴を受信して取引履歴表

示欄 18 a に表示する。図示のように、研究者が所属する研究機関の研究機関 ID、医療データ ID、取引日時、患者 D I D、研究者 D I D 及び医療データのハッシュ値を含む医療データの取引履歴が取引履歴表示欄 18 a に表示される。なお、単一の取引履歴の表示を例示したがこれに限定せず、複数の取引履歴を列挙しても良い。

[0141] なお、上述した医療データの取引履歴が医師端末 3 または患者端末 4 に送信され、取引履歴画面が医師端末 3 側または患者端末 4 側で表示されても良い。

[0142] 図 2 3 及び図 2 4 は、医療データを作成する際の処理手順を示すフローチャートである。医師端末 3 の制御部 3 1 は、二次元コードを生成するライブラリを利用し、医師 D I D を記述した二次元コード（例えば、QR コード）を生成する（ステップ S 3 1 1）。制御部 3 1 は、生成した二次元コードを表示部 3 5 により表示する（ステップ S 3 1 2）。患者端末 4 の制御部 4 1 は、医師端末 3 上で表示されている二次元コードを撮影部 4 6 により読み取る（ステップ S 4 1 1）。

[0143] 制御部 4 1 は、二次元コードの解析ライブラリを利用し、読み取った二次元コードから医師 D I D を取得する（ステップ S 4 1 2）。制御部 4 1 は通信部 4 3 を介して、患者の属性及び医療に関する質問に対する患者による回答をサーバ 1 から取得する（ステップ S 4 1 3）。具体的には、制御部 4 1 は患者 D I D に基づいて、患者の属性をサーバ 1 の大容量記憶部 1 7 の患者 D B 1 7 1 から取得し、質問に対する回答をサーバ 1 の大容量記憶部 1 7 の質問 D B 1 7 3 から取得する。なお、制御部 4 1 は、患者による質問に対する回答の入力を入力部 4 4 により受け付けても良い。

[0144] 制御部 4 1 は通信部 4 3 を介して、取得した患者の属性及び質問に対する回答を、患者 D I D 及び医師 D I D に対応付けてサーバ 1 に送信する（ステップ S 4 1 4）。サーバ 1 の制御部 1 1 は通信部 1 3 を介して、患者端末 4 から送信された患者 D I D、医師 D I D、患者の属性及び回答を受信し（ステップ S 1 1 1）、受信した患者 D I D、医師 D I D、患者の属性及び回答

を医師端末3に送信する(ステップS112)。医師端末3の制御部31は、サーバ1から送信された患者DID、医師DID、患者の属性及び回答を通信部33により受信する(ステップS313)。制御部31は、受信した患者の属性及び回答を表示部35により表示する(ステップS314)。

[0145] 制御部31は、医師による患者に対する診療データの入力を入力部34により受け付ける(ステップS315)。制御部31は、患者の属性、質問に対する回答及び診療データを含む医療データに対する電子署名の指示を入力部34により受け付け(ステップS316)、制御部31の電子署名作成部31bは、医師の秘密鍵を用いて、該医療データに対して電子署名処理を行う(ステップS317)。制御部31は、患者DID及び医師DIDに対応付けて電子署名付き医療データを通信部33によりサーバ1に送信する(ステップS318)。

[0146] サーバ1の制御部11は、医師端末3から送信された患者DID、医師DID及び署名付き医療データを通信部13により受信する(ステップS113)。制御部11は公開鍵を用いて、受信した電子署名付き医療データを復号する(ステップS114)。制御部11は、例えばEthereumの一つのスマートコントラクト規格であるERC721を利用し、医療データを特定する医療データIDを作成する(ステップS115)。制御部11は、作成した医療データIDに対応付け、患者DID、医療データ、医師DID、電子署名日時及び「署名済み」となった医療データの状態を一つのレコードとして医療データDB174に記憶する(ステップS116)。

[0147] 制御部11は、医療データを通信部13により患者端末4に送信する(ステップS117)。患者端末4の制御部41は、サーバ1から送信された医療データを通信部43により受信し(ステップS415)、受信した医療データを表示部45により表示する(ステップS416)。制御部41は、患者から該医療データをブロックチェーン2に記録する指示を入力部44により受け付けた場合(ステップS417)、ブロックチェーン2への記録指示を通信部43によりサーバ1に送信する(ステップS418)。

- [0148] サーバ1の制御部11は、患者端末4から送信されたブロックチェーン2への記録指示を通信部13により受信する（ステップS118）。制御部11のハッシュ値算出部11aは、暗号的ハッシュ関数を用いて医療データのハッシュ値を算出する（ステップS119）。制御部11は、算出した医療データのハッシュ値を医療データIDに対応付けて医療データDB174に記憶する（ステップS120）。制御部11は、算出した医療データのハッシュ値を患者ID及び医師IDに対応付けてトランザクションを作成する（ステップS121）。作成されたトランザクションは、患者ID、医師ID及び医療データのハッシュ値を含む。
- [0149] 制御部11は、トランザクションデータを分散して管理するブロックチェーン2のいずれかのノード21に、作成したトランザクションを通信部13により送信する（ステップS122）。ブロックチェーン2のノード21の制御部211は、サーバ1から送信されたトランザクションを通信部213により受信する（ステップS211）。ノード21の制御部211は、受信したトランザクションに基づいて、医療データのハッシュ値を患者ID及び医師IDに関連付けて記録する（ステップS212）。
- [0150] 具体的には、トランザクションを受信したノード21の制御部211は、ブロック生成部216を介して、受信したトランザクションに含まれた患者ID、医師ID及び医療データのハッシュ値と、自身が管理しているブロックチェーン（台帳）の情報とを基に作成した前ブロック管理情報とを少なくとも含むブロックを生成する。そして、ブロックチェーン2のノード21各々の制御部211は、所定のコンセンサス処理をブロック生成部216により実行する。ブロックチェーンは、ブロックとよばれる所定のデータ構造を有するデータ群を時系列に並べたものであり、取引内容を記した台帳としての役割を有する。各ブロックは、取引内容等の当該ブロックに記録したいデータの他に、一つ以上前のブロック（以下、前ブロックという）の情報と、改ざんの有無を検知するための情報（ノンスまたは署名等）とを含む。ノンスは、あるデータ領域に対して、その領域内のデータを一方向性関数に

より処理したときに得られる値が予め決められた規則を満たすように設定される、当該データ領域内の値である。

- [0151] ブロックチェーン2には、2台以上のノードが参加する所定のコンセンサスアルゴリズムに従った処理を経て新たなブロックが追加される。例えば、コンセンサスアルゴリズムの一つであるP o Wでは、前ブロックの情報とノンスとを含む各ブロック（データ群）に対して、「ブロックのH a s h値が閾値以下であること」といった規則が予め決められており、ブロックを追加する際に、そのような規則を満たすようなノンスを複数のノードが同時並列的に探索する処理がブロック検証部217により行われる。なお、P o W以外にもB F T（Byzantine fault tolerance）等のコンセンサスアルゴリズムがある。ブロックチェーン2のノード21各々の制御部211は、所定のコンセンサス処理を実行した後に、ブロック共有部218を介して、ブロック生成部216が生成したブロックを記憶部212に記憶（追加）する。
- [0152] なお、本実施形態では、ブロックチェーン2への記録処理をサーバ1側で実行したが、これに限らず、患者端末4側で実行しても良い。
- [0153] 図25及び図26は、患者の承認を得た医療データを研究者端末5に出力する際の処理手順を示すフローチャートである。研究者端末5の制御部51は、ブロックチェーン2に記録された医療データの開示要求を入力部54により受け付ける（ステップS531）。制御部51は通信部53を介して、研究者D I D及び医療データI Dに対応付け、受け付けた開示要求をサーバ1に送信する（ステップS532）。サーバ1の制御部11は、研究者端末5から送信された研究者D I D、医療データI D及び開示要求を通信部13により受信する（ステップS131）。制御部11は、受信した研究者I D、医療データI D及び開示要求を、該医療データを提供した患者の患者端末4に送信する（ステップS132）。
- [0154] 患者端末4の制御部41は、サーバ1から送信された研究者I D、医療データI D及び開示要求を通信部43により受信する（ステップS431）。制御部41は、受信した開示要求に応じて、医療データに対する承認情報を

受け付け（ステップS 4 3 2）、受け付けた承認情報を通信部 4 3 によりサーバ 1 に送信する（ステップS 4 3 3）。承認情報は、医療データが開示可能であるか否かを示す情報、及び医療データに対する承認種別（「開示のみ」、または「開示&共有」）を含む。

[0155] サーバ 1 の制御部 1 1 は、患者端末 4 から送信された承認情報を通信部 1 3 により受信する（ステップS 1 3 3）。制御部 1 1 は、受信した承認情報に基づいて、開示要求の対象となる医療データが開示可能であるか否かを判定する（ステップS 1 3 4）。制御部 1 1 は、該医療データが開示不可能であると判定した場合（ステップS 1 3 4 でNO）、開示不可の旨を含む通知を通信部 1 3 により研究者端末 5 に送信する（ステップS 1 3 5）。研究者端末 5 の制御部 5 1 は、サーバ 1 から送信された開示不可通知を通信部 5 3 により受信し（ステップS 5 3 3）、受信した開示不可通知を表示部 5 5 により表示する（ステップS 5 3 4）。

[0156] 制御部 1 1 は、該医療データが開示可能であると判定した場合（ステップS 1 3 4 でYES）、研究者から患者へ所定のトークンを支払うトランザクションを作成する（ステップS 1 3 6）。トランザクションは、研究者のウォレットアドレス、患者のウォレットアドレス、支払ったトークン数量及び取引日時を含む。制御部 1 1 は、ブロックチェーン 2 のいずれかのノード 2 1 に、作成したトランザクションを通信部 1 3 により送信する（ステップS 1 3 7）。

[0157] ブロックチェーン 2 のノード 2 1 は、サーバ 1 から送信されたトランザクションを通信部 2 1 3 により受信し（ステップS 2 3 1）、受信したトランザクションを実行する（ステップS 2 3 2）。ノード 2 1 の制御部 2 1 1 は、医療データ ID に基づいて該医療データのハッシュ値を取得する（ステップS 2 3 3）。ノード 2 1 の制御部 2 1 1 は、取得した医療データのハッシュ値を通信部 2 1 3 によりサーバ 1 に送信する（ステップS 2 3 4）。

[0158] サーバ 1 の制御部 1 1 は、ブロックチェーン 2 から送信された医療データのハッシュ値を通信部 1 3 により受信する（ステップS 1 3 8）。制御部 1

1 は、医療データ I D に基づいて該医療データのハッシュ値を大容量記憶部 1 7 の医療データ D B 1 7 4 から取得する（ステップ S 1 3 9）。制御部 1 1 は、取得した医療データのハッシュ値と、ノード 2 1 から送信された医療データのハッシュ値とを照合し、両者が一致しているか否かを判定する（ステップ S 1 4 0）。

[0159] 制御部 1 1 は、両者が一致していないと判定した場合（ステップ S 1 4 0 で N O）、不正な医療データである旨を含むエラーメッセージを通信部 1 3 により研究者端末 5 に送信する（ステップ S 1 4 1）。研究者端末 5 の制御部 5 1 は、サーバ 1 から送信されたエラーメッセージを通信部 5 3 により受信し（ステップ S 5 3 5）、受信したエラーメッセージを表示部 5 5 により表示する（ステップ S 5 3 6）。

[0160] 制御部 1 1 は、両者が一致していると判定した場合（ステップ S 1 4 0 で Y E S）、該医療データのハッシュ値に対応する医療データを大容量記憶部 1 7 の医療データ D B 1 7 4 から取得する（ステップ S 1 4 2）。制御部 1 1 は、取得した医療データを通信部 1 3 により研究者端末 5 に送信する（ステップ S 1 4 3）。研究者端末 5 の制御部 5 1 は、サーバ 1 から送信された医療データを通信部 5 3 により受信し（ステップ S 5 3 7）、受信した医療データを表示部 5 5 により表示し（ステップ S 5 3 8）、処理を終了する。

[0161] 本実施形態によると、医師による電子署名付き医療データを作成することが可能となる。

[0162] 本実施形態によると、研究者が、医療データを提供した患者に所定のトークンを支払うことにより、医療データの提供を積極的に進めることが可能となる。

[0163] 本実施形態によると、研究者がブロックチェーン 2 に記録された医療データを用いて医療を研究することにより、新しい治療法の研究、健康寿命の延伸、医療サービスの質の向上または医療費または介護費の抑制等に貢献することが可能となる。

[0164] （実施形態 2）

実施形態 2 は、研究者により医療データを共有する形態に関する。なお、実施形態 1 と重複する内容については説明を省略する。

- [0165] 研究者は、患者により設定された医療データの承認種別に基づき、医療データを利用する。医療データの承認種別が「開示のみ」である場合、開示要求を行った研究者に該医療データを開示することができるが、他の研究者に共有することができない。医療データの承認種別が「開示 & 共有」である場合、開示要求を行った研究者に該医療データを開示することができ、かつ、他の研究者に共有することができる。
- [0166] 図 27 は、医療データを共有する際の処理手順を示すフローチャートである。なお、図 27 のフローチャートでは説明の便宜上、共有元の研究者端末 5 を符号 5 a で表し、共有先の研究者端末 5 を符号 5 b で表す。
- [0167] 研究者端末 5 a の制御部 5 1 は、医療データ ID を通信部 5 3 によりサーバ 1 に送信する（ステップ S 5 5 1）。サーバ 1 の制御部 1 1 は、研究者端末 5 a から送信された医療データ ID を通信部 1 3 により受信する（ステップ S 1 5 1）。制御部 1 1 は、受信した医療データ ID に基づいて、該医療データの承認種別を大容量記憶部 1 7 の医療データ DB 1 7 4 から取得する（ステップ S 1 5 2）。制御部 1 1 は、取得した承認種別を通信部 1 3 により研究者端末 5 a に送信する（ステップ S 1 5 3）。
- [0168] 研究者端末 5 a の制御部 5 1 は、サーバ 1 から送信された承認種別を通信部 5 3 により受信する（ステップ S 5 5 2）。制御部 5 1 は、受信した承認種別が「開示 & 共有」であるか否かを判定する（ステップ S 5 5 3）。制御部 5 1 は、承認種別が「開示 & 共有」でないと判定した場合（ステップ S 5 5 3 で NO）、処理を終了する。制御部 5 1 は、承認種別が「開示 & 共有」と判定した場合（ステップ S 5 5 3 で YES）、共有先の研究者 ID の入力を入力部 5 4 により受け付ける（ステップ S 5 5 4）。
- [0169] 制御部 5 1 は、医療データ ID、及び受け付けた共有先の研究者 ID を通信部 5 3 によりサーバ 1 に送信する（ステップ S 5 5 5）。サーバ 1 の制御部 1 1 は、研究者端末 5 a から送信された医療データ ID 及び共有先の研

研究者D I Dを通信部13により受信する（ステップS154）。制御部11は、受信した医療データI Dに基づいて医療データを大容量記憶部17の医療データDB174から取得する（ステップS155）。制御部11は、取得した医療データを通信部13により研究者端末5bに送信する（ステップS156）。研究者端末5bの制御部51は、サーバ1から送信された医療データを通信部53により受信し（ステップS556）、受信した医療データを表示部55により表示し（ステップS557）、処理を終了する。

[0170] なお、上述した共有処理に限るものではない。例えば、承認種別が「開示&共有」である医療データを研究者に開示した場合、該研究者が所属する研究機関内の他の研究者に、該医療データを自動的に共有しても良い。

[0171] 本実施形態によると、医療データを他の研究者に共有することにより、医療データの活用に役立つことが可能となる。

[0172] （実施形態3）

実施形態3は、医療データを用いて研究した研究結果に関する情報を患者端末4に出力する形態に関する。なお、実施形態1～2と重複する内容については説明を省略する。研究結果は、例えば大量の患者の医療データに基づく学術論文、レポート、研究計画書、または治療に関する病気・症状・治療方法の動画等を含む。

[0173] 図28は、研究結果に関する情報を患者端末4に出力する際の処理手順を示すフローチャートである。研究者端末5の制御部51は、医療データを用いて研究した研究結果に関する情報を取得する（ステップS571）。具体的には、制御部51は、研究結果に関する情報を入力部54により受け付けても良く、または通信部53により外部装置から取得しても良い。例えば研究結果が論文である場合、研究結果に関する情報は、論文のタイトル、著者・編者、書誌番号、発表日時または内容等を含む。

[0174] 制御部51は通信部53を介して、研究者D I Dと取得した研究結果に関する情報とを、該研究結果に関連付けられた医療データI Dに対応付けてサーバ1に送信する（ステップS572）。サーバ1の制御部11は、研究者

端末5から送信された研究者D I D、研究結果に関する情報及び医療データ I Dを通信部13により受信する（ステップS 171）。制御部11は、受信した医療データ I Dに基づき、該医療データを提供した患者を特定する（ステップS 172）。具体的には、制御部11は、研究者D I D及び医療データ I Dに基づき、患者D I Dを大容量記憶部17の取引履歴DB 176から取得して患者を特定する。

[0175] 制御部11は、特定した患者の患者端末4に研究結果に関する情報を通信部13により送信する（ステップS 173）。患者端末4の制御部41は、サーバ1から送信された研究結果に関する情報を通信部43により受信し（ステップS 471）、受信した研究結果に関する情報を表示部45により表示し（ステップS 472）、処理を終了する。

[0176] 本実施形態によると、医療データを用いて研究した研究結果を、該医療データを提供した患者に共有（送信）することにより、患者から医療データの提供を積極的に進めることが可能となる。

[0177] （実施形態4）

実施形態4は、複数回の医療データを統合的に出力する形態に関する。なお、実施形態1～3と重複する内容については説明を省略する。本実施形態では、患者の属性、複数回の質問に対する患者による回答、及び、医師による初回診断時の診療データと、2回目以降の診断時の診療データとを統合した診療データを含む医療データを研究者端末5に出力する処理を説明する。

[0178] 図29は、研究者端末5側での複数回の医療データの表示画面の一例を示す説明図である。なお、図29では、パーキンソン病の検査項目の例を説明したが、これに限らず、他の種類の疾患の検査項目にも同様に適用される。

[0179] 該画面は、患者D I D表示欄19a、閲覧ボタン19b、重症度分類表示欄19c、診断画像表示オブジェクト19d、嗅覚検査表示欄19e、処方情報表示欄19f、血圧表示欄19g、脈拍表示欄19h及びダウンロードボタン19iを含む。患者D I D表示欄19aは、患者D I Dを表示する表示欄である。閲覧ボタン19bは、質問に対する回答を表示するボタンであ

る。なお、閲覧ボタン19bに関しては、図14の閲覧ボタン12eと同様であるため、説明を省略する。

[0180] 重症度分類表示欄19cは、複数回の重症度分類情報を表示する表示欄である。パーキンソン病において、重症度がI度（症状は片方の手足のみ）、II度（症状は両方の手足に）、III度（姿勢反射障害が加わってくる）、IV度（日常生活に部分的な介助が必要）及びV度（車いすでの生活または寝たきりとなる）に分類される。重症度分類情報は、重症度分類及び重症度の診断日時を含む。図示のように、「I：2012/06/08」、「II：2017/10/31」及び「III：2020/03/04」となった重症度分類情報が重症度分類表示欄19cに表示される。診断画像表示オブジェクト19dは、複数回の診断画像を表示するためのボタンである。なお、診断画像表示オブジェクト19dの数が、診断画像の種類に基づいて設けられても良い。図示のように、「MRI」、「DAT Scan」、「Cardiac MIBG Scintigraphy」及び「Brain Perfusion SPECT」それぞれの診断画像表示オブジェクト19dが設けられる。

[0181] 嗅覚検査表示欄19eは、複数回の嗅覚検査の結果を表示する表示欄である。処方情報表示欄19fは、複数回の処方情報を表示する表示欄である。血圧表示欄19gは、複数回の血圧検査結果を表示する表示欄である。脈拍表示欄19hは、複数回の脈拍の検査結果を表示する表示欄である。ダウンロードボタン19iは、医療データをダウンロードするボタンである。

[0182] 研究者端末5は、患者DID及び研究者DIDをサーバ1に送信する。サーバ1は、研究者端末5から送信された患者DID及び研究者DIDを受信し、受信した患者DID及び研究者DIDに基づいて該患者の複数回の医療データを取得する。具体的には、サーバ1は、患者DIDに基づいて、質問種類ごとにすべての質問に対する回答を質問DB173から取得する。サーバ1は、患者DID及び研究者DIDに基づいて、取引対象となった医療データの医療データIDを取引履歴DB176から抽出する。サーバ1は、抽出した医療データIDに基づいて、該当するすべての医療データを医療データDB174から取得する。

- [0183] サーバ1は、取得した複数回の医療データを研究者端末5に送信する。研究者端末5は、サーバ1から送信された複数回の医療データに対して統合する。研究者端末5は、統合した複数回の医療データを画面に表示する。具体的には、研究者端末5は、診断日時の新しい順に複数回の重症度分類を医療データから抽出し、抽出した複数回の重症度分類を重症度分類表示欄19cに表示する。
- [0184] 研究者端末5は、診断日時の古い順に複数回の嗅覚検査結果を医療データから抽出し、抽出した複数回の嗅覚検査結果に基づいて嗅覚検査の評点を示すグラフを生成する。研究者端末5は、生成したグラフを嗅覚検査表示欄19eに表示する。図示のように、患者におけるおいスティック (OSIT-J: odor Stick Identification Test for Japanese)を用いた嗅覚検査の評点を示すグラフが嗅覚検査表示欄19eに表示される。横軸は1回目、2回目、…と検査回数を示し、縦軸は嗅覚検査の評点を示す。なお、横軸は嗅覚検査の日付であっても良い。なお、複数の嗅覚検査法が利用された場合、研究者端末5はそれぞれの検査法に対応するグラフを生成して嗅覚検査表示欄19eに並びに表示しても良い。
- [0185] 研究者端末5は、診断日時の新しい順に複数回の処方情報を医療データから抽出し、抽出した複数回の処方情報を処方情報表示欄19fに表示する。研究者端末5は、診断日時の古い順に複数回の血圧（高血圧及び低血圧）検査結果を医療データから抽出し、抽出した複数回の血圧検査結果に基づいて血圧の値を示すグラフを生成する。研究者端末5は、生成したグラフを血圧表示欄19gに表示する。図示のように、横軸は1回目、2回目、…と検査回数を示し、縦軸は血圧の値を示す。なお、横軸は血圧検査の日付であっても良い。
- [0186] 研究者端末5は、診断日時の古い順に複数回の脈拍検査結果を医療データから抽出し、抽出した複数回の脈拍検査結果に基づいて脈拍数を示すグラフを生成する。研究者端末5は、生成したグラフを脈拍表示欄19hに表示する。図示のように、横軸は1回目、2回目、…と検査回数を示し、縦軸は脈

拍数を示す。なお、横軸は脈拍検査の日付であっても良い。

[0187] 研究者端末5は、閲覧ボタン19bのクリック（タッチ）操作を受け付けた場合、該当する質問に対する複数回の回答をサブ画面に表示する。例えば研究者端末5は、「PDQ-39」に対応する閲覧ボタン19bのクリック操作を受け付けた場合、質問に対する回答を表示するためのサブ画面を生成する。研究者端末5は、受信した医療データから「PDQ-39」に対する複数回の回答を抽出し、抽出した複数回の回答をサブ画面に表示する。

[0188] 研究者端末5は、診断画像表示オブジェクト19dのクリック操作を受け付けた場合、該当する複数回の診断画像をサブ画面に表示する。例えば研究者端末5は、「DAT Scan」に対応する診断画像表示オブジェクト19dのクリック操作を受け付けた場合、診断画像を表示するためのサブ画面を生成する。研究者端末5は、受信した医療データから「DAT Scan」に対する複数回の診断画像を抽出し、抽出した複数回の診断画像をサブ画面に表示する。なお、診断画像と、診断画像を撮影した日時との両方がサブ画面に表示されても良い。

[0189] 研究者端末5は、ダウンロードボタン19iのクリック操作を受け付けた場合、複数回の医療データに基づいて統合された医療データをExcel（登録商標）ファイルまたはPDF（Portable Document Format）ファイル等へ書き込む。研究者端末5は、医療データを書き込んだファイルを、指定されたフォルダにダウンロードする。

[0190] なお、図29では、複数回の医療データの表示例を説明したが、これに限らず、1回の医療データにも同様に適用される。

[0191] 本実施形態によると、複数回の医療データを統合的に出力することにより、長期的な経過観察及び治療効果の判定等に利用することができるため、医療研究に役立つことが可能となる。

[0192] （実施形態5）

実施形態5は、所定期間以降の第2期間における患者の医療データを再開示する形態に関する。なお、実施形態1～4と重複する内容については説明

を省略する。

[0193] 図30は、実施形態5における管理DB177のレコードレイアウトの一例を示す説明図である。なお、図6と重複する内容については同一の符号を付して説明を省略する。管理DB177には、承諾情報列及び再開示期間列が含まれる。

[0194] 承諾情報列は、患者の医療データの再開示に関する承諾情報（例えば、再開示可能または再開示不可）を記憶している。再開示期間列は、医療データの再開示期間を記憶している。再開示期間は、所定期間以降の第2期間である。例えば、所定期間が起算日から2年であり、第2期間が2年以降の20年であっても良い。起算日は、例えば医療データをブロックチェーン2のノード21に最初に登録した登録日であっても良く、または当該医療データの開示要求に対する患者の最初の承認を得た承認日であっても良い。なお、第2期間が予め再開示期間列に記憶されても良く、またはユーザによる設定が受け付けられても良い。

[0195] 患者端末4は、所定期間以降の第2期間における医療データの再開示に関する承諾情報を受け付けた場合、受け付けた承諾情報をサーバ1に送信する。医療データに対し承諾情報が得られた場合、第2期間における当該医療データを再開示することができる。サーバ1は、患者端末4から送信された承諾情報を医療データIDに対応つけて管理DB177に記憶する。

[0196] 第2期間において、研究者端末5は、研究者による医療データの再開示要求を受け付けた場合、受け付けた再開示要求を、研究者ID及び医療データIDに対応付けてサーバ1に送信する。サーバ1は、研究者端末5から送信された研究者ID、医療データID及び再開示要求を受信する。サーバ1は、受信した再開示要求に応じて、当該医療データを再開示可能であるか否かを判定する。

[0197] 具体的には、サーバ1は医療データIDに基づき、当該医療データに対応する承諾情報及び第2期間（再開示期間）を管理DB177から取得する。サーバ1は、取得した承諾情報及び第2期間に基づいて、当該医療データを

再開示可能であるか否かを判定する。例えば、第2期間において、承諾情報が「再開示可能」である場合、制御部11は当該医療データを再開示可能と判定する。または、第2期間において、承諾情報が「再開示不可」である場合、制御部11は当該医療データを再開示不可と判定する。

[0198] サーバ1は、当該医療データを再開示可能と判定した場合、サーバ1から送信された再開示要求、研究者DID及び医療データIDを、該医療データを提供した患者の患者端末4に送信する。患者端末4は、サーバ1から送信された再開示要求、研究者DID及び医療データIDを画面に表示する。なお、再開示要求と共に、過去の開示要求の履歴（研究者DID、開示要求日時または承認日時等）、研究者のメッセージまたはプロフィールが患者端末4に送信されても良い。この場合、患者端末4は、過去の開示要求の履歴、研究者のメッセージまたはプロフィールを開示要求と共に画面に表示する。

[0199] 患者端末4は、当該医療データの再開示要求に対する患者の再承認情報を受け付けた場合、受け付けた再承認情報をサーバ1に送信する。再承認情報は、医療データが再開示可能であるか否かを示す情報、及び医療データに対する承認種別（「開示のみ」、または「開示&共有」）を含む。サーバ1は、患者端末4から送信された再承認情報を受信する。サーバ1は、受信した再承認情報に応じて、医療データが再開示可能であるか否かを判定する。

[0200] サーバ1は、当該医療データが再開示可能であると判定した場合、ブロックチェーン2のノード21を経由して、研究者から患者へ所定のトークンを支払う。なお、支払処理に関しては、実施形態1と同様であるため、説明を省略する。なお、患者により当該医療データを無料で提供する等のサービスを有する場合には、トークンの支払処理を省略しても良い。

[0201] ブロックチェーン2のノード21は、トークンの支払処理を実行した後に、医療データIDに基づいて当該医療データのハッシュ値を取得する。ノード21は、取得した医療データのハッシュ値をサーバ1に送信する。サーバ1は、ノード21から送信された医療データのハッシュ値を受信する。サーバ1は、受信した医療データのハッシュ値と、医療データDB174に記憶

された医療データのハッシュ値とを照合する。

[0202] サーバ1は、両者が一致していると判定した場合、当該医療データのハッシュ値に対応する医療データを医療データDB174から取得する。サーバ1は、取得した医療データを研究者端末5に送信する。研究者端末5は、サーバ1から送信された医療データを受信して画面に表示する。

[0203] 図31は、承諾情報の受付画面の一例を示す説明図である。なお、図18と重複する内容については同一の符号を付して説明を省略する。

[0204] 承認種別設定ダイアログ14eは、承諾チェックボックス14hを含む。承諾チェックボックス14h■、所定期間（例えば、2年）以降の第2期間（例えば、20年）において、患者の医療データの再開示に関する承諾情報を受け付けるチェックボックスである。患者端末4は、承諾チェックボックス14h■チェック操作を受け付けた場合、受け付けた承諾情報（例えば、再開示可能または再開示不可）■取得する。なお、第2期間をユーザ（例えば、患者）が設定できるようにしても良い。

[0205] 患者端末4は、ダイアログ内承認ボタン14gのタッチ操作を受け付けた場合、承認種別設定ラジオボタン14fにより設定された承認種別、及び承諾チェックボックス14hにより取得された承諾情報を医療データIDに対応付けてサーバ1に送信する。サーバ1は、患者端末4から送信された承認種別及び承諾情報を医療データIDに対応付けて管理DB177に記憶する。

[0206] 図32は、患者の再承認を得た医療データを研究者端末5に出力する際の処理手順を示すフローチャートである。なお、図25及び図26と重複する内容については同一の符号を付して説明を省略する。

[0207] 研究者端末5の制御部51は、ブロックチェーン2のノード21の記憶部212に記録された医療データの再開示要求を入力部54により受け付ける（ステップS581）。制御部51は通信部53を介して、研究者DID及び医療データIDに対応付け、受け付けた再開示要求をサーバ1に送信する（ステップS582）。サーバ1の制御部11は、研究者端末5から送信さ

れた研究者ID、医療データID及び再開示要求を通信部13により受信する（ステップS181）。

[0208] 制御部11は、受信した医療データIDに基づき、当該医療データに対応する承諾情報及び第2期間を大容量記憶部17の管理DB177から取得する（ステップS182）。制御部11は、取得した承諾情報及び第2期間に基づいて、当該医療データを再開示可能であるか否かを判定する（ステップS183）。

[0209] 制御部11は、当該医療データを再開示不可と判定した場合（ステップS183でNO）、再開示不可の旨を含む通知を通信部13により研究者端末5に送信する（ステップS184）。研究者端末5の制御部51は、サーバ1から送信された再開示不可通知を通信部53により受信し（ステップS583）、受信した再開示不可通知を表示部55により表示する（ステップS584）。

[0210] 制御部11は、当該医療データを再開示可能と判定した場合（ステップS183でYES）、制御部11は、受信した研究者ID、医療データID及び再開示要求を、当該医療データを提供した患者の患者端末4に送信する（ステップS185）。患者端末4の制御部41は、サーバ1から送信された研究者ID、医療データID及び再開示要求を通信部43により受信する（ステップS481）。制御部41は、受信した研究者ID、医療データID及び再開示要求を表示部45により表示する（ステップS482）。

[0211] 制御部41は、受信した再開示要求に応じて、医療データに対する患者の再承認情報を受け付けた場合（ステップS483）、受け付けた再承認情報を通信部43によりサーバ1に送信する（ステップS484）。再承認情報は、医療データが再開示可能であるか否かを示す情報、及び医療データに対する承認種別を含む。サーバ1の制御部11は、患者端末4から送信された再承認情報を通信部13により受信する（ステップS186）。

[0212] 制御部11は、受信した再承認情報に基づいて、当該医療データが再開示可能であるか否かを判定する（ステップS187）。制御部11は、当該医

療データが再開示不可能であると判定した場合（ステップS 1 8 7でNO）、ステップS 1 8 4の処理に戻る。制御部1 1は、当該医療データが再開示可能であると判定した場合（ステップS 1 8 7でYES）、ステップS 1 3 6の処理を実行する。

[0213] 本実施形態によると、患者の医療データの再開示に関する承諾情報に基づき、所定期間以降の第2期間において、当該医療データを再開示することが可能となる。

[0214] 本実施形態によると、医療データの再開示により、医療データを活用して医療技術の進歩を促すことが可能となる。

[0215] 今回開示された実施の形態はすべての点で例示であって、制限的なものではないと考えられるべきである。本発明の範囲は、上記した意味ではなく、請求の範囲によって示され、請求の範囲と均等の意味及び範囲内でのすべての変更が含まれることが意図される。

符号の説明

- [0216]
- | | |
|-------|-------------|
| 1 | 情報処理装置（サーバ） |
| 1 1 | 制御部 |
| 1 2 | 記憶部 |
| 1 3 | 通信部 |
| 1 4 | 入力部 |
| 1 5 | 表示部 |
| 1 6 | 読取部 |
| 1 7 | 大容量記憶部 |
| 1 7 1 | 患者DB |
| 1 7 2 | 医師DB |
| 1 7 3 | 質問DB |
| 1 7 4 | 医療データDB |
| 1 7 5 | 研究者DB |
| 1 7 6 | 取引履歴DB |

- 1 7 7 管理 D B
- 1 a 可搬型記憶媒体
- 1 b 半導体メモリ
- 1 P 制御プログラム
- 2 ブロックチェーンシステム（ブロックチェーン）
- 2 1 ノード
- 2 1 1 制御部
- 2 1 2 記憶部
- 2 1 3 通信部
- 2 1 4 受付部
- 2 1 5 出力部
- 2 1 6 ブロック生成部
- 2 1 7 ブロック検証部
- 2 1 8 ブロック共有部
- 3 情報処理端末（医師端末）
- 3 1 制御部
- 3 1 a ハッシュ値算出部
- 3 1 b 電子署名作成部
- 3 2 記憶部
- 3 3 通信部
- 3 4 入力部
- 3 5 表示部
- 3 P 制御プログラム
- 4 情報処理端末（患者端末）
- 4 1 制御部
- 4 2 記憶部
- 4 3 通信部
- 4 4 入力部

4 5	表示部
4 6	撮影部
5	情報処理端末（研究者端末）
5 1	制御部
5 2	記憶部
5 3	通信部
5 4	入力部
5 5	表示部

請求の範囲

- [請求項1] 患者を特定する患者ID、患者の属性、及び医療に関する質問に対する前記患者による回答を取得し、
- 医師を特定する医師IDを前記患者の患者端末装置により読み取らせることにより前記医師IDを取得し、
- 取得した前記医師IDに対応する医師端末装置へ前記患者の患者ID、属性及び回答を送信し、
- 前記患者の患者ID、属性及び回答が表示された前記医師端末装置を通じて、前記医師による前記患者に対する診療データの入力を受け付け、
- 前記患者の属性、回答及び入力された診療データを含む医療データの送信要求を受け付け、
- 前記医療データのハッシュ値をブロックチェーンシステムに出力し、
- 前記ブロックチェーンシステムに記録された前記医療データの開示要求を研究者の研究者端末装置を介して受け付け、
- 前記研究者の開示要求に対する前記患者の承認を得た場合に、前記医療データを前記研究者端末装置に出力する
- 情報処理方法。
- [請求項2] 前記医師の秘密鍵を用いて電子署名を行った電子署名付き医療データを前記医師端末装置から取得し、
- 取得した前記医療データを前記患者端末装置に出力する
- 請求項1に記載の情報処理方法。
- [請求項3] 前記医療データに対する前記ブロックチェーンシステムへの出力指示を前記患者端末装置から受け付けた場合に、前記医療データのハッシュ値を前記ブロックチェーンシステムに出力する
- 請求項1又は2に記載の情報処理方法。
- [請求項4] 前記医師IDを記述した二次元コードを前記患者端末装置により読

み取らせることにより前記医師IDを取得する

請求項1から3のいずれか一つに記載の情報処理方法。

[請求項5] 前記開示要求に対する前記患者の承認を得た場合に、前記研究者のウォレットアドレス宛から前記患者のウォレットアドレス宛へ、前記ブロックチェーンシステム経由で所定のトークンを支払う

請求項1から4のいずれか一つに記載の情報処理方法。

[請求項6] 前記医療データの開示要求に対する承認、または、前記承認と、前記医療データの開示要求に対して承認を得た前記医療データを、他の研究者に共有することを求める共有要求に対する前記患者の第2承認とを含む承認情報を前記患者端末装置から受け付け、

受け付けた前記承認情報を前記医療データに対応付けて記憶する

請求項1から5のいずれか一つに記載の情報処理方法。

[請求項7] 所定期間以降の第2期間における前記医療データの再開示に関する承諾情報を前記患者端末装置から受け付け、

前記第2期間において、前記承諾情報が得られた医療データの再開示要求を研究者の研究者端末装置を介して受け付けた場合、受け付けた再開示要求を前記患者端末装置に送信し、

前記再開示要求に対する前記患者の再承認を得た場合に、前記医療データを前記研究者端末装置に出力する

請求項1から6のいずれか一つに記載の情報処理方法。

[請求項8] 前記医療データを用いて研究した研究結果に関する情報を前記研究者端末装置から受け付け、

受け付けた前記研究結果に関する情報を、前記医療データを提供した患者の患者端末装置に出力する

請求項1から7のいずれか一つに記載の情報処理方法。

[請求項9] 前記医療データを特定する医療データID、前記医療データの取引日時、前記患者ID、前記研究者を特定する研究者ID及び前記医療データのハッシュ値を含む取引履歴を取得し、

取得した前記取引履歴を、前記研究者端末装置、前記医師端末装置または前記患者端末装置に送信する

請求項 2 から 8 のいずれか一つに記載の情報処理方法。

[請求項10] 前記患者 I D、前記開示要求に関する情報及び前記医師による医療データの署名日時を取得し、

取得した前記患者 I D、前記開示要求に関する情報及び前記医療データの署名日時を前記研究者端末装置に送信する

請求項 2 から 9 のいずれか一つに記載の情報処理方法。

[請求項11] 前記医療データに対する開示要求を前記研究者端末装置から受け付けた場合に、受け付けた前記開示要求を、前記医療データを提供した患者の患者端末装置に送信する

請求項 1 から 1 0 のいずれか一つに記載の情報処理方法。

[請求項12] 前記医療データ I D、前記開示要求に関する情報及び前記医師 I D を取得し、

取得した前記医療データ I D、前記開示要求に関する情報及び前記医師 I D を前記患者端末装置に送信する

請求項 1 から 1 1 のいずれか一つに記載の情報処理方法。

[請求項13] 前記医療データを記憶したが前記医師からの電子署名を未取得の状態であるか、前記医師から前記医療データの電子署名を取得済みの状態であるか、または前記医療データを前記ブロックチェーンシステムに記録済みの状態であることを示す前記医療データの状態を前記患者端末装置に送信し、

前記医療データの状態を示すオブジェクトを前記患者端末装置に表示させる

請求項 2 から 1 2 のいずれか一つに記載の情報処理方法。

[請求項14] 患者を特定する患者 I D、患者の属性、及び医療に関する質問に対する前記患者による回答を取得する第 1 取得部と、

医師を特定する医師 I D を前記患者の患者端末装置により読み取ら

せることにより前記医師IDを取得する第2取得部と、

取得した前記医師IDに対応する医師端末装置へ前記患者の患者ID、属性及び回答を送信する送信部と、

前記患者の患者ID、属性及び回答が表示された前記医師端末装置を通じて、前記医師による前記患者に対する診療データの入力を受け付ける第1受付部と、

前記患者の属性、回答及び入力された診療データを含む医療データの送信要求を受け付ける第2受付部と、

前記医療データのハッシュ値をブロックチェーンシステムに出力する第1出力部と、

前記ブロックチェーンシステムに記録された前記医療データの開示要求を研究者の研究者端末装置を介して受け付ける第3受付部と、

前記研究者の開示要求に対する前記患者の承認を得た場合に、前記医療データを前記研究者端末装置に出力する第2出力部と

を備える情報処理装置。

[請求項15]

患者を特定する患者ID、患者の属性、及び医療に関する質問に対する前記患者による回答を取得し、

医師を特定する医師IDを前記患者の患者端末装置により読み取らせることにより前記医師IDを取得し、

取得した前記医師IDに対応する医師端末装置へ前記患者の患者ID、属性及び回答を送信し、

前記患者の患者ID、属性及び回答が表示された前記医師端末装置を通じて、前記医師による前記患者に対する診療データの入力を受け付け、

前記患者の属性、回答及び入力された診療データを含む医療データの送信要求を受け付け、

前記医療データのハッシュ値をブロックチェーンシステムに出力し、

前記ブロックチェーンシステムに記録された前記医療データの開示要求を研究者の研究者端末装置を介して受け付け、

前記研究者の開示要求に対する前記患者の承認を得た場合に、前記医療データを前記研究者端末装置に出力する

処理をコンピュータに実行させるプログラム。

[請求項16]

患者を特定する患者IDを取得し、

患者の属性、及び医療に関する質問に対する前記患者による回答を受け付け、

医師を特定する医師IDを取得し、

取得した前記医師IDに対応付けて、前記患者の患者ID、属性及び回答を送信し、

前記患者の属性、回答及び前記医師による前記患者に対する診療データを含む医療データを受信し、

ブロックチェーンシステムに記録された前記医療データの研究者による開示要求を受信した場合に、前記研究者の開示要求に対する前記患者の承認を得たか否かを示す情報を送信する

処理をコンピュータに実行させるプログラム。

[請求項17]

前記医療データに対する前記ブロックチェーンシステムへの出力指示を受け付け、

受け付けた前記ブロックチェーンシステムへの出力指示を送信する処理を実行させる請求項16に記載のプログラム。

[請求項18]

前記医師IDを記述した二次元コードを読み取り、

読み取った前記二次元コードから前記医師IDを取得する

処理を実行させる請求項16又は17に記載のプログラム。

[請求項19]

前記医療データの開示要求に対する承認、または、前記承認と、前記医療データの開示要求に対して承認を得た前記医療データを、他の研究者に共有することを求める共有要求に対する前記患者の第2承認とを含む承認情報を受け付け、

受け付けた前記承認情報を、前記医療データを特定する医療データ
IDに対応付けて送信する

処理を実行させる請求項16から18のいずれか一つに記載のプロ
グラム。

[請求項20] 前記医療データを記憶したが前記医師からの電子署名を未取得の状
態であるか、前記医師から前記医療データの電子署名を取得済みの状
態であるか、または前記医療データを前記ブロックチェーンシステム
に記録済みの状態であることを示す前記医療データの状態を受信し、
受信した前記医療データの状態を示すオブジェクトを表示する
処理を実行させる請求項16から19のいずれか一つに記載のプロ
グラム。