(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7408277号
(P7408277)

(45)発行日　令和6年1月5日(2024.1.5)

(24)登録日　令和5年12月22日(2023.12.22)

(51)国際特許分類

		FI	
Ｇ０６Ｆ	*16/182 (2019.01)*	Ｇ０６Ｆ	16/182
Ｇ０６Ｆ	*16/00 (2019.01)*	Ｇ０６Ｆ	16/00
Ｇ０６Ｆ	*21/64 (2013.01)*	Ｇ０６Ｆ	21/64

請求項の数　2　（全15頁）

(21)出願番号　特願2018-220140(P2018-220140)
(22)出願日　平成30年11月26日(2018.11.26)
(65)公開番号　特開2020-86902(P2020-86902A)
(43)公開日　令和2年6月4日(2020.6.4)
審査請求日　令和3年5月20日(2021.5.20)
審判番号　不服2023-9024(P2023-9024/J1)
審判請求日　令和5年6月1日(2023.6.1)

(73)特許権者　517307061
リーガルテック株式会社
東京都港区虎ノ門５－１３－１
(74)代理人　100098729
弁理士　重信 和男
(74)代理人　100204467
弁理士　石川 好文
(74)代理人　100148161
弁理士　秋庭 英樹
(74)代理人　100195833
弁理士　林 道広
(72)発明者　佐々木 隆仁
東京都港区虎ノ門５－１－５ ＡＯＳリーガルテック株式会社内
(72)発明者　志田 大輔

最終頁に続く

(54)【発明の名称】　データ管理システム

(57)【特許請求の範囲】

【請求項１】

入力データ内にテキストデータに加えてイメージデータも含まれているか否かを判定する判定手段を備え、

前記判定手段の判定に基づき、前記入力データから前記イメージデータを抽出し所定の保管サーバである分散型ファイルシステムのＩＰＦＳに保管させ、保管時に前記保管サーバである分散型ファイルシステムのＩＰＦＳから返された前記イメージデータの保管に関する関連データであるイメージデータのハッシュ値を、前記テキストデータと統合する手段と、該統合されたデータをブロックチェーン上に保管させる保管指示手段とを備え、

データ管理システムを提供するインターネット上のサービスサーバを更に備え、

前記サービスサーバは、前記ブロックチェーン上からダウンロードされた前記データ内に前記イメージデータのハッシュ値があるか否かを判定し、該判定に基づき、前記保管サーバである分散型ファイルシステムのＩＰＦＳにて前記イメージデータのハッシュ値を用いて当該イメージデータのハッシュ値に対応するイメージデータを前記保管サーバである分散型ファイルシステムのＩＰＦＳのノードからダウンロードし、該イメージデータと前記データ内の前記テキストデータとを合わせて出力可能な出力手段とを有することを特徴とするデータ管理システム。

【請求項２】

前記統合する手段は、前記テキストデータに前記イメージデータのハッシュ値を統合する際、前記ハッシュ値に所定のタグを付与する付与手段を備えていることを特徴とする請求

項１に記載のデータ管理システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、入力データを解析可能に保管するデータ管理システムに関する。
【背景技術】
【０００２】
従来から、様々な業態においてサービスの提供者と被提供者間でのやり取り、例えば、医療機関では個人の診療録、金融機関では顧客の取引記録や取引履歴、法律関係機関では判例等が管理されている。このような管理資料は、後に参照可能に管理されており、個人単位や事件単位で履歴の参照や比較に用い、以降の診察や取引、裁判等に役立ててられている。近年では、これらの管理資料はコンピュータ等で入力されて電子データ化され、サーバ等の記憶媒体に集中管理方式にて保管されている。
【０００３】
また近年では、取引記録である入力データの改竄を防ぎやすい、例えばブロックチェーンのような分散型のデータ管理システムが現れている。このように高い改竄防止機能を備えたブロックチェーン上には、仮想通貨の取引記録以外の入力データも保管することができる。例えば、特許文献１では、取引記録である入力データをブロックチェーン上に保管することが提案されている。
【先行技術文献】
【特許文献】
【０００４】
【文献】特開２０１８－５１５８３３号公報（段落０００６、第１図）
【発明の概要】
【発明が解決しようとする課題】
【０００５】
特許文献１のデータ保管サーバは、入力データをブロックチェーン上に保管することで当該入力データの信憑性を保障可能としている。しかしながら、ブロックチェーンを取り扱うプラットフォームとして広く利用されているイーサリアム等は、テキストデータを保管することを念頭に開発されたプラットフォームである。そのため、例えば、イメージデータのようにテキストデータに比べて大容量のデータを含む入力データについては、規定以上の容量のデータに対してエラーを返す構成となっているものもあり、また仮に変換を行うプラットフォームであっても、ハッシュ値に変換する処理に多大な時間を要し実用に耐えず、このような大容量のデータを含む入力データの保管には適していなかった。
【０００６】
本発明は、このような問題点に着目してなされたもので、保管されたイメージデータを含む入力データの信憑性に優れるデータ管理システム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】
【０００７】
前記課題を解決するために、本発明のデータ管理システムは、
入力データ内にテキストデータに加えてイメージデータも含まれているか否かを判定する判定手段を備え、
前記判定手段の判定に基づき、前記入力データから前記イメージデータを抽出し所定の保管サーバである分散型ファイルシステムのＩＰＦＳに保管させ、保管時に前記保管サーバである分散型ファイルシステムのＩＰＦＳから返された前記イメージデータの保管に関する関連データであるイメージデータのハッシュ値を、前記テキストデータと統合する手段と、該統合されたデータをブロックチェーン上に保管させる保管指示手段とを備え、
データ管理システムを提供するインターネット上のサービスサーバを更に備え、
前記サービスサーバは、前記ブロックチェーン上からダウンロードされた前記データ内に前記イメージデータのハッシュ値があるか否かを判定し、該判定に基づき、前記保管サ

ーバである分散型ファイルシステムのＩＰＦＳにて前記イメージデータのハッシュ値を用いて当該イメージデータのハッシュ値に対応するイメージデータを前記保管サーバである分散型ファイルシステムのＩＰＦＳのノードからダウンロードし、該イメージデータと前記データ内の前記テキストデータとを合わせて出力可能な出力手段とを有することを特徴としている。

この特徴によれば、データ管理システムは、クライアント側の端末から受信した入力データがテキストデータと大容量のデータであるイメージデータとが混在している場合には、イメージデータを抽出して保管サーバに保管し、そのイメージデータの保管に関する関連データ例えばハッシュ値のみをテキストデータに対応付けてブロックチェーン上に保管させるため、大容量のイメージデータは直接ブロックチェーン上に保管されない。これによれば、イーサリアム等のテキストデータを保管することを念頭に開発されたプラットフォームを用いた場合でも、テキストデータとイメージデータとが混在する入力データを上述のように保管することができ、かつ入力データの信憑性に優れるという効果を奏する。

【０００９】

前記統合する手段は、前記テキストデータに前記イメージデータのハッシュ値を統合する際、前記ハッシュ値に所定のタグを付与する付与手段を備えていることを特徴としている。

この特徴によれば、ブロックチェーン上に保管された入力データを参照する際に、当該入力データ内にイメージデータの保管に関する関連データの文字列が含まれていることを判断でき、処理効率を高めることができる。

【００１１】

前記サービスサーバは、前記保管サーバに保管された前記イメージデータの保管に関する関連データを前記テキストデータに統合し、統合された該データが前記ブロックチェーン上で保管される際に変換されたハッシュ値を、ユーザ識別情報に対応させて保持可能であることを特徴としている。

この特徴によれば、サービスサーバはユーザ識別情報に対応する入力データのみを出力させることが可能となるため、保管されたデータの漏洩を防止することができる。

【００１２】

前記保管サーバは分散型ファイルシステムを用いてイメージデータを保管するものであり、前記関連データはハッシュ値であることを特徴としている。

この特徴によれば、関連データとしてイメージデータを追加する際のハッシュ値を用いればよいので、既存のオープンソースの分散型ファイルシステムのプラットフォームを利用することができる。

【図面の簡単な説明】

【００１４】

【図１】本発明の実施例におけるデータ管理システムおよびデータ管理方法を示す概念図である。

【図２】ＡＰＩサーバから提供されてパソコンに表示される初期画面を示す図である。

【図３】同じくユーザーページを示す図である。

【図４】同じくデータ入力ページを示す図である。

【図５】変換前の診療録を示す図である。

【図６】タグの付与が完了したＸＭＬ形式のファイルを示す図である。

【図７】データ管理システムの保管までのフローを示す概念図である。

【図８】契約書類から変換されたＸＭＬ形式のファイルを示す図である。

【図９】任意の文字列に暗号化を設定できる表示画面を示す図である。

【図１０】出力された入力データを示す図である。

【図１１】電子契約の契約書類を保管する際のクライアント側のパソコンに表示される入力画面を示す図であり、契約者情報の入力を促すステップを示す。

【図１２】同じく契約内容の入力を促すステップを示す図である。

【図１３】同じく電子署名と印章の入力を促すステップを示す図である。

【図１４】同じく弁護士の選択を促すステップを示す図である。

【発明を実施するための形態】
【００１５】
本発明に係るデータ管理システムおよびデータ管理方法を実施するための形態を実施例に基づいて以下に説明する。
【実施例】
【００１６】
実施例に係るデータ管理システムおよびデータ管理方法につき、図１から図１４を参照して説明する。
【００１７】
データ管理システムは、様々な業態においてサービスの提供者と被提供者間でのやり取り、例えば、医療機関では個人の診療録（カルテ）、金融機関では顧客の取引履歴、法律関係機関では判例、遺言や不動産取引等の法務に関わる電子契約書類等を電子データ化し、後に参照できるようにサーバで管理するシステムである。本実施例では、診療録を病院単位で管理することを例に取り説明する。
【００１８】
図１は、本発明のデータ管理システムに係る実施形態を実現するための全体システム図を示し、符号１は管理会社（管理者）がデータ管理システムを提供するためのサービスサーバであり、符号２はクライアント及び出力手段としてのパーソナルコンピュータ（以下「パソコン」と略称する）、であり、これらはインターネットを通じて相互通信可能に接続されている。パソコン２には、入力手段としてのスキャナー３、キーボード４、マウス５等がそれぞれ接続されている。その他、入力手段としてはペンタブレットとスタイラスペン等も利用できる。
【００１９】
そして、上記各パソコン２は、ハードディスク等の図示省略の記録手段やＲＡＭ等に加え、電子化処理部を備えている。スキャナー３により撮像された紙媒体の管理書類は、電子化処理部にて記載された文字情報が文字認識され、文字情報がテキストに変換されたドキュメントが生成される。尚、管理書類に写真や図や動画等がある場合、これらはＰＮＧやＪＰＥＧやＡＶＩ等のイメージデータとしてテキストとともにドキュメントを構成する。
【００２０】
サービスサーバ１は、後述するブロックチェーンプラットフォームの動作環境及び分散型ファイルシステムの動作環境である複数のコンピュータ（記録手段）６とＡＰＩ（Application Program Interface）サーバ（記録手段）７と利用者管理サーバ（記録手段）８と処理サーバ（記録手段）９がネットワークで接続されて構成されており、クライアント側のパソコン２から管理書類のテキストデータである入力データを受信し、この入力データの管理を行う。
【００２１】
本実施例におけるデータ管理システムでは、入力データはブロックチェーンの技術を利用して保管される。サービスサーバ１を構成する複数のコンピュータ６は、ブロックチェーンのブロックを生成する複数のノードであり、分散型ファイルシステムを構成する分散サーバとしてのノードでもある。
【００２２】
ＡＰＩサーバ７は、データ管理システムを提供する管理会社が運用するサーバであり、クライアント側のパソコン２から受信した入力データをブロックチェーン上に保管するために必要なデータの変換や後に詳述するタグの付与をブロックチェーンや分散型ファイルシステムの知識を有していないクライアントでも簡単に利用することができるＡＰＩを提供するインターネット上のサーバである。尚、ＡＰＩサーバ７にて実装されてＡＰＩは、クライアント側のパソコン２で起動したウェブブラウザ上で動作する。
【００２３】
データ管理システムを利用するユーザは、データ管理システムの管理会社が公開するホームページにて、予め固有のユーザＩＤ（ユーザ識別情報）とパスワードとを登録してお

く。利用者管理サーバ８は、ホームページにて入力されたユーザＩＤとパスワードと当該ユーザＩＤのユーザに割り当てられたブロックチェーンへのリンク情報との対応関係を保有する対応テーブルを備えている。

【００２４】

図７は、データ管理システムにおける入力データのアップロードからブロックチェーン上、分散型ファイルシステム上での保管までのフローを示す概念図であり、以下、要所に図７の矢印に付された番号を説明に用いることがある。

【００２５】

ユーザがデータ管理システムに入力データを入力する際には、まずパソコン２で起動したウェブブラウザを用いて管理会社が公開するホームページにアクセスする。図２に示されるように、ホームページの初期画面１０には、ユーザＩＤの入力欄１１とパスワードの入力欄１２と、ログインボタン１３とが表示され、アクセスしてきたユーザに対して、ユーザＩＤとパスワードの入力が求められる。

【００２６】

ユーザは、これらユーザＩＤの入力欄１１とパスワードの入力欄１２に入力し、ログインボタン１３を選択する。ログインボタン１３が選択されると、入力されたユーザＩＤとパスワードとは利用者管理サーバ８（図１参照）に送られ、入力されたユーザＩＤとパスワードとの組み合わせが対応テーブルを参照して正しいことが判断できたことに基づき、図３に示されるユーザーページ１４が表示される。

【００２７】

ユーザーページ１４には、データ入力ボタン１５とデータ参照ボタン１６とが選択可能に表示される。ユーザは新たに診療録のドキュメントをアップロードする際には、データ入力ボタン１５を選択し、既に管理されている診療録の電子データを参照する際には、データ参照ボタン１６を選択する。

【００２８】

データ入力ボタン１５が選択されると、図４に示されるデータ入力ページ１７が表示される。データ入力ページ１７には、ファイル選択ボタン１８とアップロードボタン１９とが表示される。ユーザがファイル選択ボタン１８を選択すると、クライアント側のパソコン２の記憶媒体に記憶された診療録のドキュメントを選択可能なウィンドウが表示され、アップロードボタン１９の選択（図７矢印１参照）により、当該選択した診療録の電子データが処理サーバ９に送信される（図７矢印２参照）。

【００２９】

処理サーバ９では、まず診療録のドキュメントをファイル形式に基づく判断材料やそのデータの中身を読み込むことで、当該ドキュメントが全文検索可能なテキストのみのファイルであるか否か判定する（判定手段）。テキストのみのファイルであれば、タグを付与するステップ（付与手段）に移る。一方、テキストに加えてイメージデータ等のテキストデータに比べて大きなファイルサイズのデータが貼り込まれている場合には、タグを付与するステップの前に、ドキュメントを当該大きなファイルサイズのデータとテキストデータとに分ける分割処理に移る。テキストデータに比べて大きなファイルサイズのデータは、本実施例ではＣＴ画像２０（イメージデータ・図５参照）として説明する。

【００３０】

分割処理では、分けられたテキストデータとイメージデータとに共通するメタデータをそれぞれ付与し、後の処理の準備状態として保持する。

【００３１】

処理サーバ９は、複数のコンピュータ６にて動作する分散型ファイルシステムに対して、入力データから取り出したイメージデータを保管するように指示を行う（図７矢印３参照）。この分散型ファイルシステムはＩＰＦＳ（Inter Planetary File System）であり、イメージデータが保管されるノードをネットワーク上で参照にするハッシュ値を処理サーバ９に返す（図７矢印４参照）。

【００３２】

分散型ファイルシステムからイメージデータのハッシュ値を受信した処理サーバ９は、イメージデータと分けられた後のテキストデータを全文検索し、予め設定した所定の付与条件で名詞等の文字データ（例えば、項目名である既往歴等）をテキストデータから発見し、これらテキストデータの文字列にタグを付与したＸＭＬ形式のファイルに変換する。

【００３３】

例えば、図５の診療録の電子データから項目を示す「既往歴」という単語の文字データと、この「既往歴」という単語の近傍の単語である「インフルエンザ」と「硬膜下血腫」という文字データとが発見されると、「インフルエンザ」と「硬膜下血腫」とが「既往歴」に該当するものと判断する。そして、図６のＸＭＬ形式のファイルにおいて、＜既往歴＞と＜／既往歴＞の間に「インフルエンザ」と「硬膜下血腫」の文字データをそれぞれ配置する。

【００３４】

このように、「既往歴」「インフルエンザ」「硬膜下血腫」等の単語を認識することと、これら「インフルエンザ」「硬膜下血腫」が「既往歴」に対応することは、所定のタグの付与条件として、予め管理会社とユーザとで処理サーバ９に設定されている。

【００３５】

加えて、本実施例におけるＡＰＩは、タグの付与条件として、「インフルエンザ」という文字データが「呼吸器」の疾患であり、「硬膜下血腫」という文字データが「脳」の疾患であると判定することができる付与条件も備えている。そして、ＸＭＬ形式のファイルにおいて「インフルエンザ」を挟むように＜呼吸器＞と＜／呼吸器＞のタグを、「硬膜下血腫」を挟むように＜脳＞と＜／脳＞のタグを、それぞれ配置する。つまり、「インフルエンザ」という文字データには、下位のサブタグである＜呼吸器＞＜／呼吸器＞のタグと、上位のメインタグである＜既往歴＞＜／既往歴＞というタグが付与され、これら複数のタグが階層で分けられて判定可能となっている。なお、一つの文字データに複数のタグが付与されるようになっていてもよい。例えば「インフルエンザ」という文字列に「呼吸器」と「ウィルス」という２つのタグが付与されるようになっていてもよい。

【００３６】

更に処理サーバ９は、分散型ファイルシステムから返されたハッシュ値（関連データ）を、ＸＭＬ形式のファイル内に記入する。詳しくは、イメージデータに関連するハッシュ値は、その文字列がイメージデータのハッシュ値であることを示すタグ情報＜ｉｍｇ＞＜／ｉｍｇ＞の間に記入される。尚、ＸＭＬ形式のファイルには、イメージデータの位置情報を示すタグ情報やイメージデータの配置及び表示サイズ等の情報を配置してもよい。

【００３７】

処理サーバ９は、イメージデータに関連するハッシュ値とテキストデータとが統合されたＸＭＬ形式のファイルを、複数のコンピュータ６にて動作するブロックチェーンプラットフォームにて保管するように指示を行うステップ（保管指示手段）に移る（図７矢印５参照）。ブロックチェーンプラットフォームはイーサリアムであり、統合されたＸＭＬ形式のファイルは、ハッシュ値に変換されてブロックチェーン上で保管される。

【００３８】

すなわち、ＸＭＬ形式のファイルは、サービスサーバ１を構成するいずれかのコンピュータ６にてブロックチェーンの形式に沿ってハッシュ値化（図７矢印６参照）され、前述の対応テーブルにて照会されたユーザＩＤに対応するブロックチェーンへのリンクを用いて複数のブロックチェーンの中から該当するブロックチェーンを特定し、サービスサーバ１を構成する複数のノードとして機能するコンピュータ６の環境において動作するブロックチェーン上に保管される。また、利用者管理サーバ８の対応テーブルでは、ブロックチェーン上に保管されたハッシュ値とユーザＩＤとの対応関係を保持（図１）しており、後述する出力時には、ユーザはログイン時に表示される複数のハッシュ値から任意のものを選択することで、入力データ単位で内容を確認可能に出力できる。処理サーバ９は、ブロックチェーンへの入力データの保管が完了したことをＡＰＩの表示等を用いてクライアント側のパソコン２に対して通知する（図７矢印７，８参照）。

【００３９】
　また、図８に示される契約書類のように、クレジットカード番号等の秘匿性の高い文字列がＸＭＬ形式のファイルに記載されている場合がある。サービスサーバ１が提供するデータ管理システムでは、ＸＭＬ形式のファイルにおいて、ユーザが必要に応じてテキストデータの暗号化を行うことができる機能を備えている。
【００４０】
　処理サーバ９はＸＭＬ形式のファイルのタグの付与が完了すると、秘匿処理ステップを行う。詳しくは、ＡＰＩを用いて図９に示されるような任意の文字列に暗号化を設定できる表示画面を表示させる。ユーザは、マウス５等を用いて文字列をドラッグ（選択）することで、秘匿したい部分を指定できる（図９では２箇所を指定する例を示している。）。ＡＰＩはドラッグされた文字列を認識し、表示画面では当該文字列にマスキングを掛け、かつ処理サーバ９に当該文字列の暗号化を指示する。
【００４１】
　処理サーバ９は、選択された文字列を変数にて一見して内容が判断できない文字列に変換（暗号化）する。このとき処理サーバ９は、暗号化に用いた変数を対応テーブル（図１参照）にてユーザＩＤに紐づけて保存する。
【００４２】
　また、処理サーバ９は、暗号化を行った部分を判別できるようにタグをＸＭＬ形式のファイルに付与する。図９では、＜クレジットカード番号＞＜／クレジットカード番号＞がタグ付けされた文字列と、＜ｉｍｇ＞＜／ｉｍｇ＞がタグ付けされた文字列、すなわちイメージデータのハッシュ値の文字列とに暗号化を行うため、最下端に＜Ｅｎｃ＞＜／Ｅｎｃ＞のタグで＜クレジットカード番号＞＜／クレジットカード番号＞と＜ｉｍｇ＞＜／ｉｍｇ＞のタグを挟んで記載している。
【００４３】
　尚、処理サーバ９は、タグに基づき秘匿すべきと判断した文字列を、暗号化を設定できる表示画面においてフリッカ表示、ハイライト表示等の強調表示をする等してユーザに示すアシスト機能を備えていてもよい。
【００４４】
　また、文字列の暗号化に限らず、各タグを選択してタグ自体を暗号化できる仕様としてもよい。これによれば、タグに挟まれた文字列が何に対応するのかを判別不能にできる。また、タグとタグに挟まれた文字列を共に暗号化することも可能である。
【００４５】
　また、イメージデータについても、暗号化可能な仕様としてもよい。
【００４６】
　処理サーバ９は、ブロックチェーン上に保管された複数の入力データを参照する機能（出力手段）を有する。ユーザは、パソコン２で起動したウェブブラウザを用いて管理会社が公開するホームページにアクセスしログインを行う。
【００４７】
　ユーザは、ログイン後にクライアント側のパソコン２に表示されるユーザーページ１４（図３参照）のデータ参照ボタン１６を選択する。処理サーバ９は、データ参照ボタン１６の選択に基づき、入力データを参照するステップを開始する。
【００４８】
　詳しくは、処理サーバ９はユーザがログイン時に受信したユーザＩＤを対応テーブルで参照し、対応するブロックチェーンへのリンクを用いて、入力データ保管されている当該ブロックチェーン上を特定し、当該ブロックチェーンプラットフォームに該ユーザＩＤ対応するハッシュ値を送信する。
【００４９】
　ついでブロックチェーンプラットフォームは、ハッシュ値をＸＭＬ形式のファイルに復号し、処理サーバ９にＸＭＬ形式のファイルを返信する。更に、処理サーバ９ではＸＭＬ形式のファイルを読み込み、内部にイメージデータに関連するハッシュ値があるか否かを

判定する。イメージデータに関連するハッシュ値があることが判定されると、処理サーバ９は分散型ファイルシステムにて当該ハッシュ値を用いて当該ハッシュ値に対応するイメージデータを分散ファイルシステムからダウンロードする。

【００５０】

そして、処理サーバ９によって、ＸＭＬ形式のファイル内のイメージデータに関連するハッシュ値以外のテキストデータとダウンロードしたイメージデータを用いて、図１０に示されるように、クライアント側のパソコン２のディスプレイに対して、ＸＭＬ形式のファイル中のテキストデータとイメージデータとを同時に閲覧できる出力画面を表示する。

【００５１】

このとき、処理サーバ９は、利用者管理サーバ８の対応テーブルから暗号化に用いた解読用の鍵としての変数（復号情報）を抽出し、当該変数を用いてＸＭＬ形式のファイル中の暗号化された文字列を復号化して表示する。

【００５２】

このように、所定の検索条件によって抽出されたテキストと、当該テキストに付与されたタグを用いることで、事業活動に有益な知識を得るためのデータ解析に利用することができる。例えば、医療の分野では、ユーザである一の病院の患者全ての診療録の入力データを解析することで、近似する既往歴の患者同士の診療録の入力データから、疾患傾向や有効な治療法の研究等に役立つ知識を得られる可能性がある。

【００５３】

以上説明したように、本発明のデータ管理システムは、処理サーバ９はクライアント側のパソコン２から受信した入力データを判定手段により判定し、テキストデータと大容量のデータであるイメージデータとが混在している場合には、イメージデータを抽出して分散型ファイルシステムにて保管させる。そして、分散型ファイルシステムから返されたイメージデータの保管に関する関連データであるハッシュ値のみをテキストデータに対応付けてブロックチェーン上に保管させる。これによれば、大容量のイメージデータは直接ブロックチェーン上に保管されず、イーサリアム等のテキストデータを保管することを念頭に開発されたプラットフォームを用いた場合でも、テキストデータとイメージデータとが混在する入力データをブロックチェーン上に保管することができ、かつ入力データの信憑性に優れるという効果を奏する。

【００５４】

また、処理サーバ９は、イメージデータのハッシュ値の文字列とテキストデータとを統合することで、これらを簡単かつ確実に対応付けてブロックチェーン上に保管させることができる。また、統合データが一つのブロックとしてブロックチェーン上に保管されることとなるので、保管された入力データを復号する際に、イメージデータの保管箇所とテキストデータの保管箇所とを対応付けたテーブルを必ずしも用意しておく必要がない。

【００５５】

また、処理サーバ９は、テキストデータに統合されたイメージデータのハッシュ値の文字列に対して、所定のタグを付与する付与手段を備えている。これによれば、処理サーバ９は、ブロックチェーン上に保管された入力データを参照する際に、当該入力データ内にイメージデータのハッシュ値の文字列が含まれていることを判断でき、出力や参照時の処理効率を高めることができる。更に、イメージデータはＩＰＦＳを用いて保管されており、ハッシュ値を用いて検索が行われるため、ＵＲＬを用いた検索よりも高速な検索、参照が可能である。

【００５６】

また、処理サーバ９は、入力データの出力を要求された場合には、分散型ファイルシステムからイメージデータを抽出し、ブロックチェーン上に保管されたハッシュ値から復号した対応するテキストデータと合わせて、クライアント側の端末から受信した入力データと同様の内容に復号させて出力することができる。

【００５７】

また、サービスサーバ１は、利用者管理サーバ８にてブロックチェーン上に保管された

ハッシュ値とユーザＩＤとを対応させて保持しており、ユーザＩＤに対応する入力データのみを出力させるため、保管されたデータの漏洩を防止することができる。

【００５８】

尚、データ管理システムにて管理できる書類は、前記実施例にて説明した診療録や契約書類に限らず、データ解析等のデータ活用には基本的に利用しないもの、例えば、遺言や不動産取引等の法務に関わる電子契約書類であってもよい。このような遺言書等の電子契約書類をブロックチェーン上で保管する場合には、弁護士のように公的に法律的な遺言書の効力を証明できる第三者の承認が必要となる。

【００５９】

このように弁護士の承認を必要とする入力データを保管するサービスを提供する場合について、図１１から図１４を用いて説明する。データ管理システムを提供するサービスサーバは、この承認作業を行う弁護士の承認ステップが実装されている。尚、ここでは不動産取引の電子契約について説明する。

【００６０】

図１１に示されるように、契約書類はＡＰＩが提供する入力画面がクライアント側のパソコン２に表示され、ユーザはこの入力画面から直接内容を入力することができる。入力画面のステップ１として、ユーザには契約書類のタイトルと契約者情報として契約者氏名、住所の入力が要求される。次いでステップ２として、ユーザには契約内容を入力する入力欄が表示され（図１２参照）、内容の入力が完了するとマウス等を用いて行う電子署名と、印章のアップロードが促される（図１３参照）。ユーザによる契約書類の入力が完了すると、クライアント側のパソコン２には図１４に示されるような、契約書類の入力データの承認を依頼する弁護士の選択を促す画面が表示される。

【００６１】

ユーザが弁護士を選択し認証依頼ボタンが操作されると、サービスサーバ１は予め連絡先が登録されている、選択された弁護士に対して入力データの内容確認の依頼を示すメッセージを送信する。弁護士は、ネットワークに接続されたパソコン等の端末を用いて、当該入力データを確認し、確認完了のメッセージをサービスサーバ１に送信する。この確認完了のメッセージとしては、例えば弁護士による電子署名であってもよい。

【００６２】

サービスサーバ１は、この承認完了のメッセージの受信に基づき、当該入力データの承認作業が完了したと見なし、当該入力データを上記したタグの付与及び署名、印章のイメージデータの抽出、ハッシュ値への変換等の作業を行い、ブロックチェーン上に保管する指示を行う。

【００６３】

このように、弁護士による承認が完了した入力データのみがブロックチェーン上に保管されるため、ユーザは別途に電子証明書等を用意する必要がなく、またサービスサーバ１が提供するホームページから弁護士への承認要請を行うことができ、面倒な手続きを省略して、信憑性の高い電子契約の管理を行うことができる。

【００６４】

以上、本発明の実施例を図面により説明してきたが、具体的な構成はこれら実施例に限られるものではなく、本発明の要旨を逸脱しない範囲における変更や追加があっても本発明に含まれる。

【００６５】

例えば、前記実施例では、サービスサーバ１はＡＰＩサーバ７を備え、ＡＰＩを用いることで、視覚において直感的な操作によりブロックチェーン技術に関する知識を有していないユーザでも簡単にシステムを利用できるようになっているが、これに限らず、処理サーバ９への指示信号を送信できるウェブブラウザ上で動作するＡＰＩとは別のプログラムを利用する等してもよい。

【００６６】

また、前記実施例において、イメージデータは分散型ファイルシステムであるＩＰＦＳ

を用いて保管されているが、これに限らず、例えばテキストデータを保管するブロックチェーン以外の保管環境であれば、分散型ファイルシステムが用いられなくてもよいし、サーバやローカルサーバ等に保管されてもよい。また、この場合、イメージデータが保存されているＵＲＬやローカルドメイン等がイメージデータの保管に関する関連データとして、テキストデータと対応付けて保管される。

【００６７】

また、分散型ファイルシステムから返されたハッシュ値は、テキストデータに統合される仕様に限らず、例えばテキストデータはイメージデータのハッシュ値とは別途ハッシュ値化されてブロックチェーン上にそれぞれ別ブロックとして保管し、イメージデータのハッシュ値に対応するテキストデータの保管に関する関連データを付与した上で、ブロックチェーン上に別の単位で保管される仕様としてもよい。

【００６８】

また、前記実施例において、ＸＭＬ形式のファイル内の任意の文字列を秘匿する際に暗号化に利用した変数は、ユーザＩＤ毎に設定され保管される仕様で説明したが、これに限らず、例えばＸＭＬ形式のファイル毎に変数が設定され保管される仕様とすることで秘匿性を更に高める仕様としてもよい。

【００６９】

また、前記実施例におけるブロックチェーンは、管理会社が提供するサービスサーバ１を構成する複数のコンピュータ６上の環境で動作する、所謂プライベートチェーンで説明したが、パブリックチェーンの仕様であってもよい。分散型ファイルシステムの動作環境についても同様にプライベートな環境とパッブリックな環境のいずれであってもよい。

【００７０】

また、管理会社が提供するサービスサーバ１を構成するＡＰＩを備えるＡＰＩサーバ７と、対応テーブルを備える利用者管理サーバ８と処理サーバ９とは、それぞれの機能を兼ねる一台のコンピュータで構成されていてもよい。

【００７１】

また、ユーザが利用するクライアント側の端末は、パソコンに限らず、タブレットやスマートフォンでもよい。

【００７２】

また、前記実施例では、データ管理システムはサービスサーバ１により提供される構成で説明したが、これに限らず、例えばクライアント側のパソコン２上で、ＡＰＩを備えるＡＰＩサーバ７と、対応テーブルを備える利用者管理サーバ８と処理サーバ９の機能を備えたアプリケーションを動作させる構成としてもよく、この場合、パソコン２がデータ管理システムを構成することになる。

【００７３】

また、ブロックチェーンで変換されたハッシュ値やリンクは、対応テーブルで管理されずに、直接ユーザに送信される構成であってもよい。

【符号の説明】

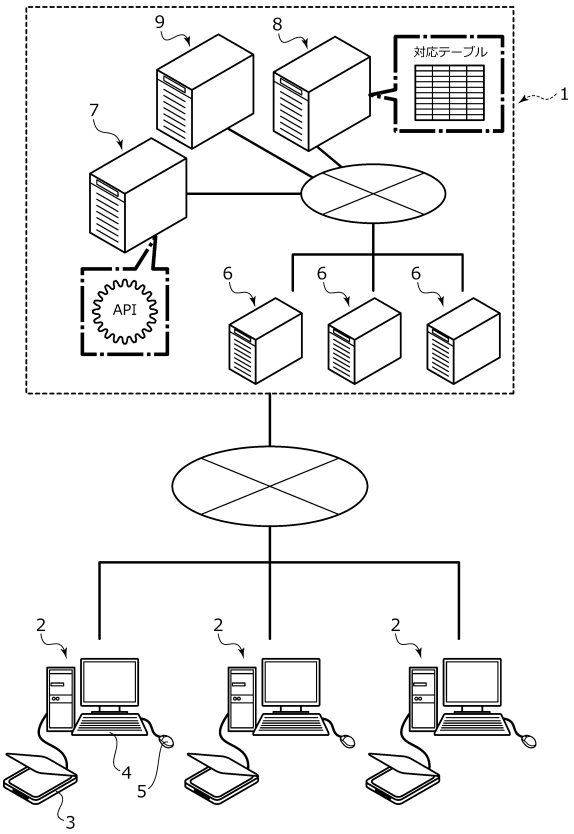
【００７４】

１	サービスサーバ
２	パソコン
３	スキャナー
４	キーボード
５	マウス
６	コンピュータ（保管サーバ）
７	ＡＰＩサーバ
８	利用者管理サーバ
９	処理サーバ
１０	初期画面
１４	ユーザーページ

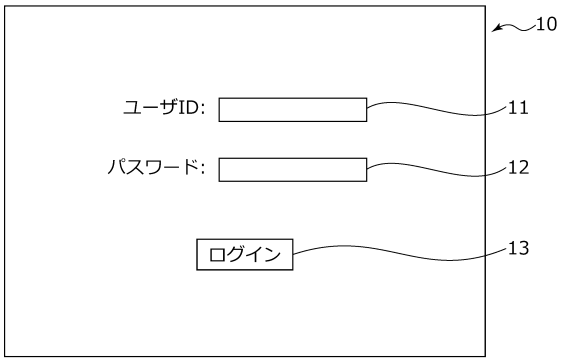
１５　　データ入力ボタン
１６　　データ参照ボタン
１７　　データ入力ページ
１８　　ファイル選択ボタン
１９　　アップロードボタン
２０　　ＣＴ画像（イメージデータ）

【図面】

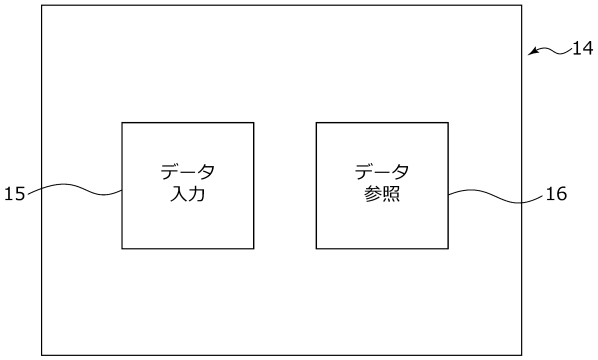
【図１】



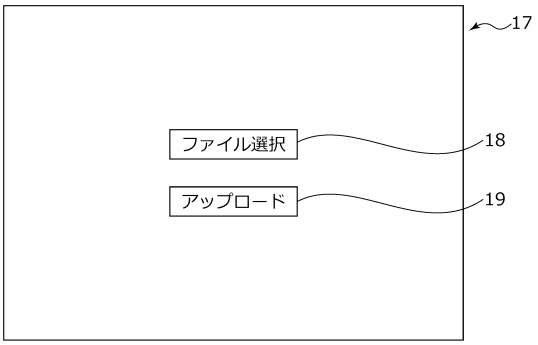
【図２】



【図３】



【図４】

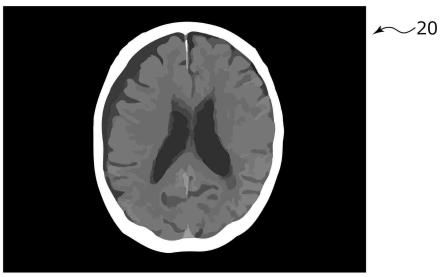


【図５】

受診者	氏名	○○　○○
	生年月日	昭和３３年３月３日　(男)・女
	住所	東京都△△△区△△△１－１－１ 電話：00-0000-0000

既往歴
インフルエンザ
硬膜下血腫

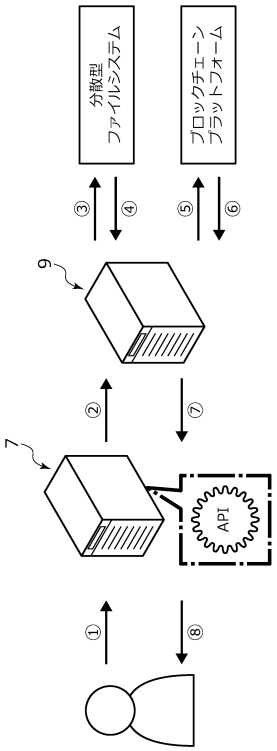
検査歴
赤血球
CT



【図６】

```
<患者情報>
 <受診者>
  <氏名>○○　○○</氏名>
  <生年月日>昭和３３年３月３日</生年月日>
  <性別>男</性別>
  <住所>
   <郵便番号>000-0000</郵便番号>
   <都道府県>東京都</都道府県>
   <町名>△△△区△△△</町名>
   <番地>１－１－１</番地>
   <電話>00-0000-0000</電話>
  </住所>
 </受診者>
 <既往歴>
  <呼吸器>インフルエンザ</呼吸器>
  <脳>硬膜下血腫</脳>
 </既往歴>
 <検査歴>
  <血液>インフルエンザ</血液>
  <放射線>CT</放射線>
 </検査歴>
</患者情報>
<img01>a03gt9x5by</img01>
```

【図７】



【図８】

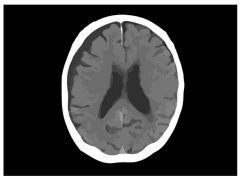
```
<顧客情報>
  <契約者>
    <氏名>□□ □□</氏名>
    <生年月日>昭和４０年１０月１０日</生年月日>
    <性別>男</性別>
    <住所>
      <郵便番号>000-0000</郵便番号>
      <都道府県>東京都</都道府県>
      <町名>△△△区△△△</町名>
      <番地>５－３－１</番地>
      <電話>03-XXXX-XXXX</電話>
    </住所>
  </契約者>
  <契約内容>
    <保険商品名>○×○×保険</保険商品名>
    <加入日>平成１０年３月５日</加入日>
  </契約内容>
  <支払情報>
    <ｸﾚｼﾞｯﾄｶｰﾄﾞ番号>5432-XXXX-XXXX</ｸﾚｼﾞｯﾄｶｰﾄﾞ番号>
  </支払情報>
</顧客情報>
<img01>2f64gw9q1t</img01>
```

【図９】

```
<顧客情報>
  <契約者>
    <氏名>□□ □□</氏名>
    <生年月日>昭和４０年１０月１０日</生年月日>
    <性別>男</性別>
    <住所>
      <郵便番号>000-0000</郵便番号>
      <都道府県>東京都</都道府県>
      <町名>△△△区△△△</町名>
      <番地>５－３－１</番地>
      <電話>03-XXXX-XXXX</電話>
    </住所>
  </契約者>
  <契約内容>
    <保険商品名>○×○×保険</保険商品名>
    <加入日>平成１０年３月５日</加入日>
  </契約内容>
  <支払情報>
    <ｸﾚｼﾞｯﾄｶｰﾄﾞ番号>5432-XXXX-XXXX</ｸﾚｼﾞｯﾄｶｰﾄﾞ番号>
  </支払情報>
</顧客情報>
<img01>2f64gw9q1t</img01>
<Enc><img01><ｸﾚｼﾞｯﾄｶｰﾄﾞ番号></Enc>
```

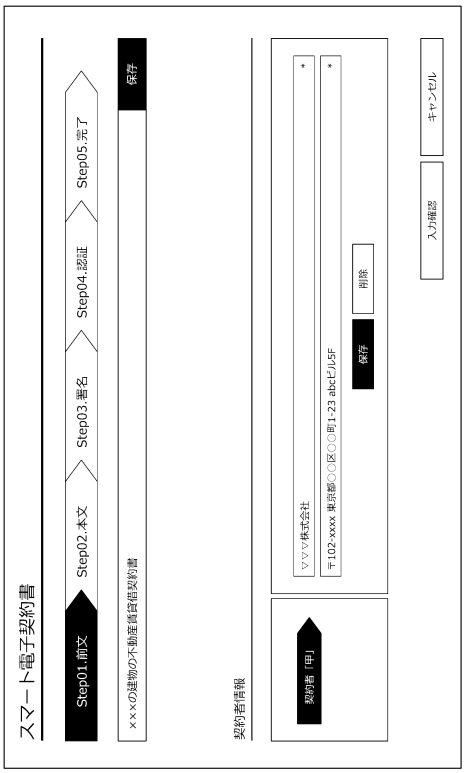
【図１０】

```
<患者情報>
  <受診者>
    <氏名>○○　○○</氏名>
    <生年月日>昭和３３年３月３日</生年月日>
    <性別>男</性別>
    <住所>
      <郵便番号>000-0000</郵便番号>
      <都道府県>東京都</都道府県>
      <町名>△△△区△△△</町名>
      <番地>１－１－１</番地>
      <電話>00-0000-0000</電話>
    </住所>
  </受診者>
  <既往歴>
    <呼吸器>インフルエンザ</呼吸器>
    <脳>硬膜下血腫</脳>
  </既往歴>
  <検査歴>
    <血液>インフルエンザ</血液>
    <放射線>CT</放射線>
  </検査歴>
</患者情報>
<img01>
```

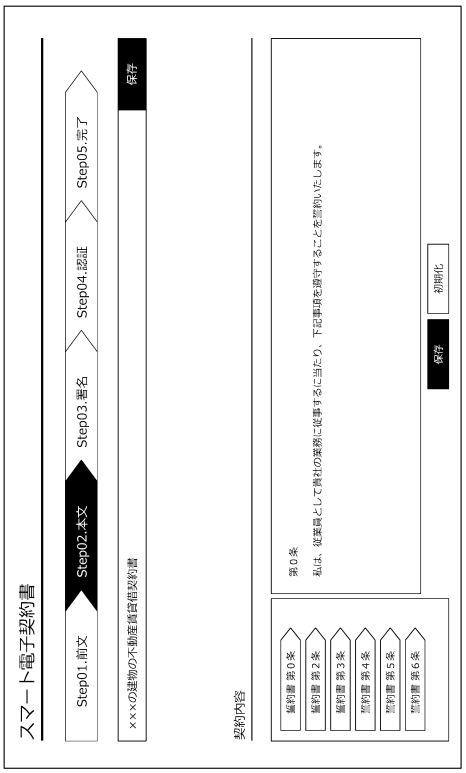


```
</img01>
```

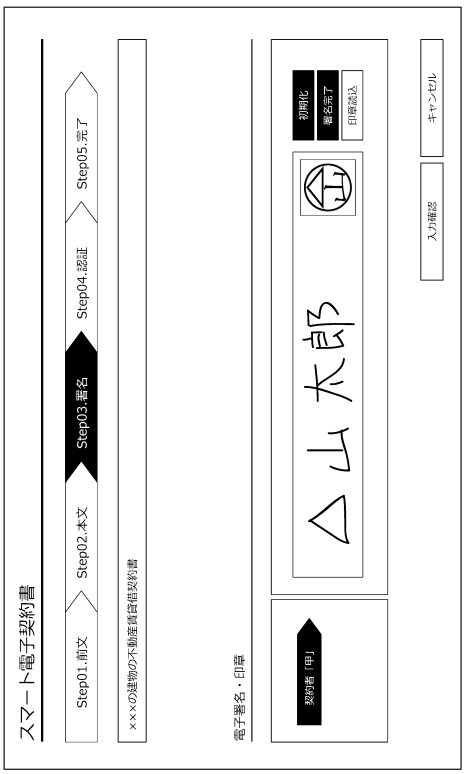
【図１１】



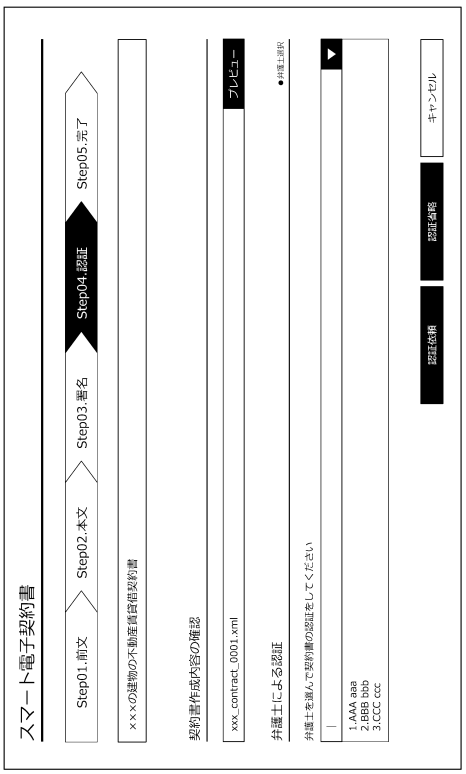
【図１２】



【図１３】



【図１４】



フロントページの続き

東京都港区虎ノ門５－１３－１ データテック株式会社内

合議体

審判長　須田 勝巳

審判官　打出 義尚

審判官　吉田 美彦

(56)参考文献　特開２０１８－１３３０５１（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)

G06F 16/00-16/958