

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7520472号
(P7520472)

(45)発行日 令和6年7月23日(2024.7.23)

(24)登録日 令和6年7月12日(2024.7.12)

(51)国際特許分類

F I

H 0 4 L 9/32 (2006.01)

H 0 4 L 9/32 2 0 0 Z

G 0 6 Q 20/38 (2012.01)

G 0 6 Q 20/38 3 1 0

請求項の数 14 (全20頁)

(21)出願番号	特願2022-560765(P2022-560765)	(73)特許権者	522357105
(86)(22)出願日	令和3年11月1日(2021.11.1)		東銀リースビジネスイノベーション株式
(86)国際出願番号	PCT/JP2021/040274		会社
(87)国際公開番号	WO2022/097608		東京都中央区新川二丁目27番1号
(87)国際公開日	令和4年5月12日(2022.5.12)	(74)代理人	100130111
審査請求日	令和5年12月19日(2023.12.19)		弁理士 新保 斉
(31)優先権主張番号	特願2020-184365(P2020-184365)	(72)発明者	長門 伸高
(32)優先日	令和2年11月4日(2020.11.4)		東京都中央区新川二丁目27番1号 東
(33)優先権主張国・地域又は機関	日本国(JP)		銀リースビジネスイノベーション株式会
早期審査対象出願		審査官	社内
前置審査			青木 重徳

最終頁に続く

(54)【発明の名称】 情報管理プラットフォームシステム及び、その処理方法

(57)【特許請求の範囲】

【請求項1】

ブロックチェーンを用いた情報管理プラットフォームシステムであって、
所望のデータの管理サービスを各管理サービスごとの会員に対して提供し、該会員のユーザ端末から送信されたデータを管理する複数のサービスサーバ装置と、
該サービスサーバ装置から該データのハッシュ値を含む登録情報を受理して、ブロックチェーンに登録及び照会して真正の認証を行うためのプラットフォームサーバ装置と
該サービスサーバ装置及び該プラットフォームサーバ装置とを接続する通信ネットワークから構成され、
該プラットフォームサーバ装置には、
該複数のサービスサーバ装置に対してAPI（Application Programming Interface）を提供し、該APIを通して該登録情報を受理する情報受理部と、
該登録情報の受理を契機として、該登録情報に係るトランザクションを発行するトランザクション発行部と、
該トランザクション発行部からのトランザクションに基づいてブロックチェーンへの該登録情報の記録を行うスマートコントラクト処理部と
該複数のサービスサーバ装置に対してAPIを提供し、該APIを通して該登録情報に関して少なくともハッシュ値を受理する照会受理部と、
該照会された該ハッシュ値のトランザクションがブロックチェーン上に記録されているか検索する検索処理部と、

検索された検索結果を該サービスサーバ装置に通知する結果通知部と
を備える構成であって、

該結果通知部から通知された検索結果に基づいて該サービスサーバ装置から該ユーザ端末に検索結果を送信することにより該データが認証されたことを表示可能にしたことを特徴とする情報管理プラットフォームシステム。

【請求項 2】

前記登録情報には、前記ハッシュ値と共に前記データに係る付加情報を含む
請求項 1 に記載の情報管理プラットフォームシステム。

【請求項 3】

前記サービスサーバ装置及び、前記プラットフォームサーバ装置はいずれも Web サーバ機能を有し、前記 API が Web API である
請求項 1 又は 2 に記載の情報管理プラットフォームシステム。

【請求項 4】

前記サービスサーバ装置において前記データを保存及び検索可能に管理する一方、
前記登録情報に、前記サービスサーバ装置で管理される該データを含まない
請求項 1 ないし 3 のいずれかに記載の情報管理プラットフォームシステム。

【請求項 5】

前記複数のサービスサーバ装置においてそれぞれ管理される各データが、該管理サービスを利用する会員情報と関連付けられる構成において、

前記プラットフォームサーバ装置において、

会員情報を統合して管理する会員情報共通処理部を備え、会員情報の管理機能を提供する
請求項 1 ないし 4 のいずれかに記載の情報管理プラットフォームシステム。

【請求項 6】

前記プラットフォームサーバ装置において、

前記複数のサービスサーバ装置の課金情報を統合して管理する課金情報共通処理部を備え、各会員に対する課金情報の管理機能を提供する

請求項 1 ないし 5 のいずれかに記載の情報管理プラットフォームシステム。

【請求項 7】

前記サービスサーバ装置が、文書の電子ファイルを前記データとして管理する管理サービスであって、

前記プラットフォームサーバ装置の前記情報受理部に対して、該電子ファイルから所定の計算式によって算出したハッシュ値と、該文書に対する署名情報とを前記 API を通して送信すると共に、

前記プラットフォームサーバ装置の前記照会受理部に対して、該ハッシュ値を前記 API を通して送信し、前記結果通知部からの検索結果を受信して、契約状態を表示する

請求項 1 ないし 6 のいずれかに記載の情報管理プラットフォームシステム。

【請求項 8】

前記サービスサーバ装置が、複数の IoT (Internet of Things) デバイスと接続され、前記データが、該 IoT デバイスとの通信履歴であって、

前記プラットフォームサーバ装置の前記情報受理部に対して、該通信履歴から所定の計算式によって算出したハッシュ値と、該通信履歴に関する付加情報とを前記 API を通して送信すると共に、

前記プラットフォームサーバ装置の前記照会受理部に対して、該ハッシュ値を前記 API を通して送信し、前記結果通知部からの検索結果を受信して、通信履歴の真正を表示する

請求項 1 ないし 7 のいずれかに記載の情報管理プラットフォームシステム。

【請求項 9】

ブロックチェーンを用いた情報管理プラットフォームシステムにおける情報処理方法であって、

該情報管理プラットフォームシステムが、複数のサービスサーバ装置と、プラットフォームサーバ装置と、該サービスサーバ装置及び該プラットフォームサーバ装置とを接続す

10

20

30

40

50

る通信ネットワークから構成されており、

各サービスサーバ装置は、所望のデータの管理サービスを各管理サービスごとの会員に対して提供し、該会員のユーザ端末から送信されたデータを管理するものであって、

該サービスサーバ装置から、該データのハッシュ値を含む登録情報を送信するステップ、
該プラットフォームサーバ装置の情報受理部が、API (Application Programming Interface) を通して該登録情報を受理するステップ、

該プラットフォームサーバ装置のトランザクション発行部が、該登録情報に係るトランザクションを発行するステップ、

該プラットフォームサーバ装置のスマートコントラクト処理部が、該トランザクション発行部からのトランザクションに基づいてブロックチェーンへの該登録情報の記録を行うステップ、

前記サービスサーバ装置から前記登録情報に関して少なくともハッシュ値を送信するステップ、

該プラットフォームサーバ装置の照会受理部が、API (Application Programming Interface) を通して該登録情報に関して少なくともハッシュ値を受理するステップ、

該プラットフォームサーバ装置の検索処理部が、照会された該ハッシュ値のトランザクションがブロックチェーン上に記録されているか検索するステップ、

該プラットフォームサーバ装置の結果通知部が、検索された検索結果を該サービスサーバ装置に通知するステップ、

該サービスサーバ装置から該ユーザ端末に対して該検索結果を送信するステップ、
を有する情報処理方法。

【請求項 10】

前記登録情報には、前記ハッシュ値と共に前記データに係る付加情報を含む

請求項 9 に記載の情報処理方法。

【請求項 11】

前記サービスサーバ装置及び、前記プラットフォームサーバ装置はいずれも Web サーバ機能を有し、前記 API が Web API である

請求項 9 又は 10 に記載の情報処理方法。

【請求項 12】

前記サービスサーバ装置において前記データをを保存及び検索可能に管理する一方、

前記登録情報に、前記サービスサーバ装置で管理される該データを含まない

請求項 9 ないし 11 のいずれかに記載の情報処理方法。

【請求項 13】

前記サービスサーバ装置が、文書の電子ファイルを前記データとして管理するサービスであって、

前記プラットフォームサーバ装置の前記情報受理部に対して、該電子ファイルから所定の計算式によって算出したハッシュ値と、該文書に対する署名情報とを前記 API を通して送信すると共に、

前記プラットフォームサーバ装置の前記照会受理部に対して、該ハッシュ値を前記 API を通して送信し、前記結果通知部からの検索結果を受信して、契約状態を表示する

請求項 9 に記載の情報処理方法。

【請求項 14】

前記サービスサーバ装置が、複数の IoT (Internet of Things) デバイスと接続され、前記データが、該 IoT デバイスとの通信履歴であって、

前記プラットフォームサーバ装置の前記情報受理部に対して、該通信履歴から所定の計算式によって算出したハッシュ値と、該通信履歴に関する付加情報とを前記 API を通して送信すると共に、

前記プラットフォームサーバ装置の前記照会受理部に対して、該ハッシュ値を前記 API を通して送信し、前記結果通知部からの検索結果を受信して、通信履歴の真正を表示する

10

20

30

40

50

請求項 9 ないし 13 のいずれかに記載の情報処理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ブロックチェーンを用いた情報管理プラットフォームシステムとその処理方法に係り、特に様々なサービスに対してブロックチェーンによる認証を容易に導入できる技術に関する。

【背景技術】

【0002】

近年、ブロックチェーンを用いた情報の記録方法が知られている。ネットワーク上の複数のコンピュータで分散的に構築し、一定期間のコントラクトをブロック単位にまとめ、コンピュータ同士で検証し合いながら鎖（チェーン）上に記録していくことで改ざんを防止可能な技術である。連結されたブロックは、1つ前のハッシュ値を持っているため、その連続性が確保される。

【0003】

従来、ブロックチェーンを用いた技術としては、仮想通貨の取引時にその取引データをブロックチェーン上に記録することで、データを改ざんし、不正取引を行っても、ブロックチェーンの分散型台帳に記録されたデータの多数決によって取引データの信頼性を保っている。例えば仮想通貨の取引システムは、特許文献 1 に開示されている。

【0004】

また、特許文献 2 では、契約の合意の記録として適用するものであって、1つのトランザクションに1つの電子署名という形態を保持しつつ、多人数であっても効率的に契約の証跡をブロックチェーンに残す技術が開示されている。本開示では、複数の装置が、それぞれ、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を記憶部に記憶し、記憶部に記憶されたブロックチェーンに合意対象の契約に対応する共有の契約用アドレス宛てのトランザクションが含まれるか否かを監視し、契約用アドレス宛てのトランザクションを検知した場合、契約に合意するか否かの証跡と、自装置ユーザの電子署名とを含む、契約用アドレス宛てのトランザクションを生成し、ネットワークへブロードキャストする手順が開示されている。

【0005】

特許文献 3 では、ネットワークに接続された装置の認証方法に適用する例であり、認証要求装置は分散台帳に認証要求トランザクションを発行し、認証応答装置は分散台帳に認証要求トランザクションを読み取り且つ認証する技術が開示されている。

【0006】

特許文献 4 では、分散形ネットワークを用い、所望の著作物に対して、簡易かつ安価に時刻認証を行うことができる著作物保護支援装置が開示されている。本装置には、通信部と、通信部を用いて、時刻認証を要求する旨の情報が付された著作物を取得する取得部と、取得部により取得された、時刻認証を要求する旨の情報が付された著作物に基づく情報を、送受信された情報が時刻情報と共に保持される分散型ネットワークに対して発信するように、通信部を制御する処理部とを備えている。

【0007】

これら複数の先行技術のようにブロックチェーン技術に対する様々なアプリケーションが提案されているものの、いずれもブロックチェーンに対する格納はそれぞれのシステムでトランザクションを生成し記録する構成であって、共通のプラットフォームとなるような技術は提案されていない。

【0008】

また、従来のブロックチェーン上に情報を記録するサービスは、記録するデータ自体をサービス側で取り扱うため、記憶領域や回線速度などサーバとしての負荷が高まるだけでなく、漏洩や外部からの攻撃に対するリスクを負う問題があり、結果としてコストアップや、導入の困難性につながっていた。

【先行技術文献】

【特許文献】

【0009】

【文献】特許第6776396号

【文献】特開2017-220710号

【文献】特開2020-178344号

【文献】特開2016-208347号

【発明の概要】

【発明が解決しようとする課題】

【0010】

本発明は、上記従来技術の課題を解決するために創出されたものであり、ブロックチェーンを用いた情報の管理を様々なサービスに対して簡便に提供する情報管理プラットフォーム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】

【0011】

上記課題を解決するため、本発明は次のような情報管理プラットフォームシステムを提供する。

すなわち、本発明の第1の実施態様によれば、ブロックチェーンを用いた情報管理プラットフォームシステムであって、所望のデータの管理サービスを提供する複数のサービスサーバ装置と、サービスサーバ装置からデータのハッシュ値を含む登録情報を受理して、ブロックチェーンに登録及び照会して真正の認証を行うためのプラットフォームサーバ装置とサービスサーバ装置及びプラットフォームサーバ装置とを接続する通信ネットワークから構成され、プラットフォームサーバ装置には、複数のサービスサーバ装置に対してAPI (Application Programming Interface) を提供し、APIを通して登録情報を受理する情報受理部と、登録情報の受理を契機として、登録情報に係るトランザクションを発行するトランザクション発行部と、トランザクション発行部からのトランザクションに基づいてブロックチェーンへの登録情報の記録を行うスマートコントラクト処理部と複数のサービスサーバ装置に対してAPIを提供し、APIを通して登録情報に関して少なくともハッシュ値を受理する照会受理部と、照会されたハッシュ値のトランザクションがブロックチェーン上に記録されているか検索する検索処理部と、検索結果をサービスサーバ装置に通知する結果通知部とを備えることを特徴とする。

【0012】

本発明の第2の実施態様によれば、前記登録情報には、前記ハッシュ値と共に前記データに係る付加情報を含む構成でもよい。

【0013】

本発明の第3の実施態様によれば、前記サービスサーバ装置及び、前記プラットフォームサーバ装置はいずれもWebサーバ機能を有し、前記APIがWeb APIであってもよい。

【0014】

本発明の第4の実施態様によれば、前記サービスサーバ装置において前記データを保存及び検索可能に管理する一方、前記登録情報に、前記サービスサーバ装置で管理されるデータを含まないのである。

【0015】

本発明の第5の実施態様によれば、前記複数のサービスサーバ装置においてそれぞれ管理される各データが、管理サービスを利用する会員情報と関連付けられる構成において、前記プラットフォームサーバ装置において、会員情報を統合して管理する会員情報共通処理部を備え、会員情報の管理機能を提供することもできる。

【0016】

本発明の第6の実施態様によれば、前記プラットフォームサーバ装置において、前記複数のサービスサーバ装置の課金情報を統合して管理する課金情報共通処理部を備え、各会

10

20

30

40

50

員に対する課金情報の管理機能を提供してもよい。

【0017】

本発明の第7の実施態様によれば、前記サービスサーバ装置が、文書の電子ファイルを前記データとして管理する管理サービスであって、前記プラットフォームサーバ装置の前記情報受理部に対して、電子ファイルから所定の計算式によって算出したハッシュ値と、文書に対する署名情報とを前記APIを通して送信すると共に、前記プラットフォームサーバ装置の前記照会受理部に対して、ハッシュ値を前記APIを通して送信し、前記結果通知部からの検索結果を受信して、契約状態を表示する構成でもよい。

【0018】

本発明の第8の実施態様によれば、前記サービスサーバ装置が、複数のIoT (Internet Of Things) デバイスと接続され、前記データが、IoT デバイスとの通信履歴であって、前記プラットフォームサーバ装置の前記情報受理部に対して、通信履歴から所定の計算式によって算出したハッシュ値と、通信履歴に関する付加情報とを前記APIを通して送信すると共に、前記プラットフォームサーバ装置の前記照会受理部に対して、ハッシュ値を前記APIを通して送信し、前記結果通知部からの検索結果を受信して、通信履歴の真正を表示することもできる。

【0019】

本発明は、ブロックチェーンを用いた情報管理プラットフォームシステムにおける情報処理方法として提供することもできる。

すなわち、第9の実施態様によれば、情報管理プラットフォームシステムが、複数のサービスサーバ装置と、プラットフォームサーバ装置と、サービスサーバ装置及びプラットフォームサーバ装置とを接続する通信ネットワークから構成されており、所望のデータの管理サービスを提供するサービスサーバ装置から、データのハッシュ値を含む登録情報を送信するステップ、プラットフォームサーバ装置の情報受理部が、API (Application Programming Interface) を通して登録情報を受理するステップ、プラットフォームサーバ装置のトランザクション発行部が、登録情報に係るトランザクションを発行するステップ、プラットフォームサーバ装置のスマートコントラクト処理部が、トランザクション発行部からのトランザクションに基づいてブロックチェーンへの登録情報の記録を行うステップを有する情報処理方法を提供する。

【0020】

本発明の第10の実施態様によれば、前記サービスサーバ装置から前記登録情報に関して少なくともハッシュ値を送信するステップ、プラットフォームサーバ装置の照会受理部が、API (Application Programming Interface) を通して登録情報に関して少なくともハッシュ値を受理するステップ、プラットフォームサーバ装置の検索処理部が、照会されたハッシュ値のトランザクションがブロックチェーン上に記録されているか検索するステップ、プラットフォームサーバ装置の結果通知部が、検索結果をサービスサーバ装置に通知するステップ、サービスサーバ装置において、検索結果を表示するステップを有する構成でもよい。

【0021】

本発明の第11の実施態様によれば、前記登録情報には、前記ハッシュ値と共に前記データに係る付加情報を含むこともできる。

【0022】

本発明の第12の実施態様によれば、前記サービスサーバ装置及び、前記プラットフォームサーバ装置はいずれもWebサーバ機能を有し、前記APIがWeb APIであってもよい。

【0023】

本発明の第13の実施態様によれば、前記サービスサーバ装置において前記データをを保存及び検索可能に管理する一方、前記登録情報に、前記サービスサーバ装置で管理されるデータを含まないこともできる。

【0024】

本発明の第14の実施態様によれば、前記サービスサーバ装置が、文書の電子ファイルを前記データとして管理するサービスであって、前記プラットフォームサーバ装置の前記情報受理部に対して、電子ファイルから所定の計算式によって算出したハッシュ値と、文書に対する署名情報とを前記APIを通して送信すると共に、前記プラットフォームサーバ装置の前記照会受理部に対して、ハッシュ値を前記APIを通して送信し、前記結果通知部からの検索結果を受信して、契約状態を表示する構成でもよい。

【0025】

本発明の第15の実施態様によれば、前記サービスサーバ装置が、複数のIoT (Internet Of Things)デバイスと接続され、前記データが、IoTデバイスとの通信履歴であって、前記プラットフォームサーバ装置の前記情報受理部に対して、通信履歴から所定の計算式によって算出したハッシュ値と、通信履歴に関する付加情報とを前記APIを通して送信すると共に、前記プラットフォームサーバ装置の前記照会受理部に対して、ハッシュ値を前記APIを通して送信し、前記結果通知部からの検索結果を受信して、通信履歴の真正を表示することもできる。

【発明の効果】

【0026】

本発明は上記構成により次のような効果を奏する。

すなわち、文書やIoTデバイスとの通信履歴といったさまざまなデータを、データの内容に全く限定されることなくサービスサーバ装置の運営者が管理しながら、プラットフォームサーバ装置ではそのデータの内容に関与することなく、ハッシュ値だけをブロックチェーン上に記録することで、データの認証サービスを提供することができる。

【0027】

これによりブロックチェーン技術を簡便に利用することができ、データの管理サービスの信頼性の向上が図られると同時に、低コスト化にも寄与する。

【0028】

加えて、会員情報や課金情報の管理をプラットフォーム側で担うこともできるので、データ本体と、会員情報、課金情報とを別個の管理にして情報管理の安全性を高めることができる。

【0029】

ビジネス文書を交換する際に、電子データ交換(EDI)に標準化されたプロトコルを用いなくても、独自フォーマットの交換を安全かつ簡便に行うことができる。

【図面の簡単な説明】

【0030】

【図1】本発明に係る情報管理プラットフォームシステムの全体図である。

【図2】本発明のプラットフォームサーバ装置の構成図である。

【図3】本発明のサービスサーバ装置の構成図である。

【図4】情報管理プラットフォームシステムによるサービスの提供態様を説明する図である。

【図5】本発明の情報処理方法(文書登録)のフローチャートである。

【図6】本発明の情報処理方法(署名)のフローチャートである。

【図7】本発明の情報処理方法(データ照会)のフローチャートである。

【図8】情報管理プラットフォームシステムを用いて押印情報を登録する例の説明図である。

【図9】情報管理プラットフォームシステムを用いてIoTデバイスとの通信履歴を登録する例の説明図である。

【発明を実施するための形態】

【0031】

以下、本発明の実施形態を、図面に示す実施例を基に説明する。なお、実施形態は下記に限定されるものではない。

図1は、本発明に係る情報管理プラットフォームシステム(1)の全体図である。本シ

10

20

30

40

50

ステム（１）は所望のデータの管理サービスを提供する複数のサービスサーバ装置（２０）と、サービスサーバ装置（２０）からデータのハッシュ値を含む登録情報を受理して、ブロックチェーン（３０）に登録及び照会して真正の認証を行うためのプラットフォームサーバ装置（１０）とサービスサーバ装置（２０）及びプラットフォームサーバ装置（１０）とを接続するインターネット等の通信ネットワーク（４０）から構成される。

【００３２】

サービスサーバ装置は、それぞれが何らかのデータを管理する管理サービスを提供するものであって、一般的には当該管理サービスを利用する会員のユーザ端末（５０）や、接続されるデバイス（５１）（５１）から送信されたデータを管理する。

【００３３】

本発明において、データの管理とは、データを保存し格納しておくことや、要求に従ってデータを検索し、抽出し、送信すること、さらにデータの真正を認証すること、タイムスタンプを参照して作成された日付や、その後の更新の有無などの情報を提供することなど、データに関する様々な処理を包括して定義する。

【００３４】

対象とするデータは任意であり、後日の客観的な証明、認証、公証が必要ないかなる情報を対象とすることができ、テキストデータ、画像・映像データ、音声データ、暗号化済みのデータなどいかなるデータを扱うこともできる。

認証する目的として、存在証明、取引日時証明、合意形成事実の証明、非改ざん証明、真正性証明などに用いることが好適である。

【００３５】

図２は、プラットフォームサーバ装置（１０）の構成図である。

プラットフォームサーバ装置（１０）には、複数のサービスサーバ装置（２０）に対してＡＰＩ（Application Programming Interface）を提供する。ここでプラットフォームサーバ装置（１０）は公知のＷｅｂサーバの機能を備え、ＡＰＩとしては汎用性の高いＷｅｂ ＡＰＩを実装することが好ましい。すなわち、本発明の実施において必要なデータをサービスサーバ装置（２０）から受理するＡＰＩによって、様々なサービスサーバ装置（２０）の上位サービスに柔軟に対応することができる。

【００３６】

プラットフォームサーバ装置（１０）は、公知のネットワークに配置されるサーバ装置の一般的な構成を備えており、サーバ、パーソナルコンピュータやワークステーションなど任意のコンピュータによって構成することができる。これらのハードウェアについては公知であるので説明を省略する。

【００３７】

プラットフォームサーバ装置（１０）のＣＰＵ（１１）により様々な処理を行う処理部を実装する。すなわち、ＡＰＩを通して登録情報を受理する情報受理部（１１１）、登録情報の受理を契機として、登録情報に係るトランザクションを発行するトランザクション発行部（１１２）と、トランザクション発行部（１１２）からのトランザクションに基づいてブロックチェーンへの登録情報の記録を行うスマートコントラクト処理部（１１３）が、ブロックチェーンに登録情報を記録するための最低限必要な処理部である。

【００３８】

また、ブロックチェーン（３０）に登録する際に、時刻認証局（図示しない）から取得したタイムスタンプを合わせて登録することによって、登録されたデータの時刻や変更の有無などを認証することができるようになる。このために時刻認証局からタイムスタンプを取得する時刻認証取得部（１１４）を備えてもよい。

【００３９】

さらに、ブロックチェーン（３０）に格納したデータを検索するために、ＣＰＵ（１０）には、複数のサービスサーバ装置（２０）に対してＡＰＩを提供し、ＡＰＩを通して登録情報に関して少なくともハッシュ値を受理する照会受理部（１１５）と、照会されたハッシュ値のトランザクションがブロックチェーン上に記録されているか検索する検索処理

10

20

30

40

50

部（１１６）と、検索結果をサービスサーバ装置に通知する結果通知部（１１７）とを備える。

【００４０】

ブロックチェーン（３０）については公知の技術であるので詳細な説明は省略するが、インターネット等のネットワーク上において各ブロックのような複数のブロックをチェーン状に連ね、前のブロックの情報を高度に複雑な計算をしたハッシュ値を次のブロックが持つことで、改ざんを極めて難しくする技術である。

【００４１】

ブロックチェーン（３０）は仮想通貨の取引等に用いられることが多いため、格納されるデータを一般的に取引記録と呼んでいるが、本発明ではこれを様々なデータから算出したハッシュ値の格納に適用し、このハッシュ値を記録の塊である各ブロックに時系列的に格納する。個々のブロックにはハッシュ値に加えて、１つ前に生成されたブロックのハッシュ値を格納する。

【００４２】

仮に、過去に生成したブロック内の情報を改ざんしようと試みた場合、変更したブロックから算出されるハッシュ値は以前と異なることになるため、後続するすべてのブロックのハッシュ値も変更しなければならない。ブロックチェーンのブロックはネットワーク上に分散して配置され、真正を多数決で決めることから、そうした変更は事実上困難であり、結果として改ざんを許さないシステムが実現される。

【００４３】

図３は、本発明のサービスサーバ装置（２０）の構成図である。サービスサーバ装置（２０）も上記同様、公知のコンピュータによって構成される。

ＣＰＵ（２１）には、管理サービスを利用する会員のログイン処理を行うログイン処理部（２１１）、ユーザ端末や接続機器からアップロードされるデータを受理するアップロード受理部（２１２）、データから所定の計算式によってハッシュ値を算出するハッシュ算出部（２１３）、少なくとも算出されたハッシュ値を登録情報としてプラットフォームサーバ装置（１０）に送信する登録情報送信部（２１５）などを備える。

【００４４】

また、ブロックチェーン（３０）に格納したデータを検索するために、プラットフォームサーバ装置（１０）が提供するＡＰＩにより、登録情報に関するハッシュ値を登録情報照会部（２１６）から送信する。そして、プラットフォームサーバ装置（１０）においてブロックチェーン（３０）上のハッシュ値を検索した結果を表示する。例えば、複数のデータを一括検索して一覧表示する一覧生成部（２１７）を備えることもできる。

【００４５】

サービスサーバ装置（２０）では、提供するサービスの会員を管理するために会員情報ＤＢ（２２）を備え、ＩＤやパスワードによって管理してもよい。上記ログイン処理部（２１１）は会員がユーザ端末で入力したＩＤとパスワードを会員情報ＤＢ（２２）を参照してログインの認証処理を行うことができる。

【００４６】

また、ハードディスク等の記憶手段（２３）に、ユーザ端末や接続機器から送信されたデータ（２３１）、ＩＤやその他の情報である付加情報（２３２）、ハッシュ算出部（２１３）で算出されたハッシュ値（２３３）を格納することができる。

これによって、会員はログインしてからデータを参照したり、登録情報照会部（２１６）はハッシュ値（２３３）を抽出して処理を行うことができる。

【００４７】

プラットフォームサーバ装置（１０）とサービスサーバ装置（２０）にはそれぞれネットワークアダプタ（１５）（２４）を備えて通信ネットワーク（４０）を介して互いに追伸する。また、プラットフォームサーバ装置（１０）は通信ネットワーク（４０）を介してブロックチェーン（３０）と、サービスサーバ装置（２０）は通信ネットワーク（４０）を介してユーザ端末や接続機器と通信を行うこともできる。

【0048】

以上のようなブロックチェーンを用いた情報管理プラットフォームシステム（１）によって、従来には無い新しいサービス提供の形態を創出することができる。図４は情報管理プラットフォームシステムによるサービスの提供態様を説明する図である。

ここでは、プラットフォームサーバ装置（１０）を運営する運営者と、サービスサーバ装置（２０）を運営する運営者、さらにサービスサーバ装置（２０）が提供する様々な管理サービスを利用するエンドユーザに分けられる。

【0049】

プラットフォームサーバ装置（１０）は、ハッシュや付加情報を受けてブロックチェーンにスマートコントラクトを行う機能を担い、このような認証処理に係る利用料をサービスサーバ装置運営者から受けとることができる。サービスサーバ装置運営者としても、ブロックチェーンにアクセスするシステムを準備することなく、簡便かつ低コストでブロックチェーンを使用した認証を導入することができる。

10

【0050】

プラットフォームサーバ装置（１０）には多数のサービスサーバ装置運営者が契約すると共に、提供する上位サービスのエンドユーザに対して、認証機能を使ったサービスを提供する。もちろん、このサービスの対価として、利用料がエンドユーザからサービスサーバ装置運営者に対して支払われる。

【0051】

従来、ブロックチェーンを利用して認証システムでは、データを保管すると共にハッシュ値を計算し、スマートコントラクトを実行してブロックチェーンに記録する処理を一貫して行っていたが、本システムは別個の運営者によって同様の認証処理をエンドユーザに提供する新しいシステムを提供することができる。

20

【0052】

また、改ざん不可能な認証機能を提供することで管理サービスの付加価値が向上し、エンドユーザからサービスサーバ装置運営者への利用料や、ひいてはサービスサーバ装置運営者からプラットフォームサーバ装置への利用料についても価値を高めることができる。

【0053】

このようにサービスサーバ装置（２０）は、さまざまなデータの管理を行うことができるが、本実施例では、データの例として文書の電子ファイルを扱う場合について説明する。例えば契約文書について、その文書の存在と、その当事者について管理するサービスを想定している。

30

【0054】

図５は、文書登録を行う際の処理方法を示す。

まず、ログイン処理部（２１１）が、会員のユーザ端末（５０）から公知のログイン方法によってログイン処理（Ｓ１０）を行う。会員情報ＤＢ（２２）を参照して、会員と確認ができた場合にユーザ端末（５０）がログイン状態となる。

なお、本発明においてサービスサーバ装置（２０）はかならずしも会員のみがサービスを利用できる態様に限らず、ログイン処理（Ｓ１０）を行わなくてもよい。

【0055】

40

ログイン状態で、会員は例えば契約書などの文書をアップロード（Ｓ１１）する。具体的には、ユーザ端末（５０）内に保存されている電子ファイルを指定し、送信を行うことでサービスサーバ装置（２０）のアップロード受理部（２１２）が受信し、記憶手段（２３）にデータ（２３１）として保存（Ｓ１２）される。

【0056】

この段階で、当事者が署名を行う処理を行ってもよいし、すぐにブロックチェーンに記録する処理に進んでもよい。本実施例は後者の例であり、ハッシュ値算出部（２１３）が電子ファイルを所定のハッシュ関数を用いてハッシュ値を算出（Ｓ１３）する。ハッシュ関数は任意に決めることができるが、例えばSHA256やRIPEMD160などが良く知られている。

50

算出したハッシュ値は、記憶手段（２３）のハッシュ値データ（２３３）に文書に係るデータ（２３１）と関連づけて保存される。

【００５７】

サービスサーバ装置（２０）では、ユーザに対して文書の管理サービスを提供するために文書の電子ファイルやハッシュ値だけでなく、さまざまなデータを関連付けて保存している。表１はその一例である。

【００５８】

【表１】

管理番号	登録日付	文書のハッシュ値	署名状態	ファイル名	取引年月日	取引金額
1	2020/4/1	1234abc	aaa@hoge.com.jp bbb@example.com	agreement0401.pdf	2020/4/15	¥1,000,000
2	2020/5/6	def5678	aaa@hoge.com.jp	contract0506.doc		

10

【００５９】

表１において、左から順にデータの通し番等として管理番号、文書が登録された日付、算出されたハッシュ値、署名状態、電子ファイルのファイル名、取引を行った場合の取引年月日、取引金額である。サービスサーバ装置（２０）の付加情報生成部（２１４）が、各情報を生成して記録する。

署名状態に入力されているのは、その文書について署名した当事者のメールアドレスである。

【００６０】

ブロックチェーンに記録する際に、このような様々な付加情報（２３２）の中から適宜付加情報を選択することができる。本実施例では署名状態に含まれるメールアドレスを登録情報として含む。すなわち、登録情報送信部（２１５）がプラットフォームサーバ装置（１０）に送信（Ｓ１４）するのは、ハッシュ値"1234abc"と署名"aaa@hoge.com.jp/bbb@example.com"となる。

30

【００６１】

プラットフォームサーバ装置（１０）の情報受理部（１１１）が提供するＡＰＩを通して登録情報を受信すると、トランザクション発行部（１１２）が、登録情報に係るトランザクションを発行（Ｓ１５）する。さらに、スマートコントラクト処理部（１１５）が、トランザクション発行部からのトランザクションに基づいてブロックチェーン（３０）への登録情報の記録（Ｓ１６）を行う。

【００６２】

この一連の流れによって、サービスサーバ装置（２０）に格納されている文書のハッシュ値と署名状態がブロックチェーン（３０）に記録されることから、例えば文書の内容や署名者を変更することはできなくなる。

40

同時に、プラットフォームサーバ装置（１０）ではハッシュ値と署名者の情報を一時的に受信するだけであるので、データ保管のコストやリスクを負うことがなく、サーバはごく低負荷で運用することができる。

【００６３】

合わせて、文書のハッシュ値と署名状態が合わせてブロックチェーン（３０）上に記録されることで、いわゆる電子署名と同等の作用を及ぼすことができる。上記のように署名状態にメールアドレスを格納するだけでも、改ざんが不可能な情報として記録されるので、取引が真正に成立したことを保存することができる。

50

【0064】

なお、取引年月日はプラットフォームサーバ装置（10）の時刻認証取得部（114）が時刻認証局からタイプスタンプを取得して合わせてブロックチェーン（30）に格納してもよい。あるいは、サービスサーバ装置（20）が登録情報として署名された日付を含めてプラットフォームサーバ装置（10）に送信し、ブロックチェーン（30）上に記録する構成でもよい。

【0065】

日本の電子帳簿保存法によれば、電子取引情報に付与するタイムスタンプには、時刻認証業務認定事業者発行のタイムスタンプが含まれており、例えば同法が対象とする請求書をメールで送る場合にもこれに適合したタイムスタンプが必要となる。請求書を電子送付するサービス事業者が個別にタイムスタンプを取得し、検証可能なサービスを準備する必要があるが、本発明ではプラットフォーム側でサービスを提供することができる。

10

【0066】

具体的には、プラットフォームサーバ装置（10）からデータのハッシュ値をネットワークを介して時刻認証業務認定事業者（TSA）の時刻認証サーバ装置に送信し、当該データに対するタイムスタンプを作成させる。時刻認証サーバ装置からタイムスタンプデータの送信を受けて、このタイムスタンプデータを上記データのハッシュ値や署名（メールアドレス）と共にブロックチェーン（30）に記録する。

【0067】

合わせて、プラットフォームサーバ装置（10）においてタイムスタンプの検証を行うAPIを提供することもできる。サービスサーバ装置（20）から照会受理部（115）がAPIを通して登録情報に関して少なくともハッシュ値を受信すると、図示しないタイムスタンプ照会処理部が時刻認証サーバ装置にタイムスタンプの検証処理を実施し、その結果を受信した上で、結果通知部（117）からサービスサーバ装置（20）に回答することもできる。

20

【0068】

ブロックチェーン（30）への登録情報の記録（S16）への登録結果、登録成功、登録失敗の情報はサービスサーバ装置（20）に送信（S17）され、さらにユーザ端末（50）に通知（S18）される。

【0069】

次に、すでに保存されている文書について署名を行う処理方法を図6を用いて説明する。文書をアップロードした会員に限らず、取引の相手方もサービスサーバ装置（20）上で、署名を行うことができる。

30

具体的には、アップロード時に相手方のメールアドレスを設定すると、メール送受信部（218）から相手方に登録内容が通知される。

【0070】

これに基づいて、取引の相手方もサービスサーバ装置（20）上で文書を確認し、「署名」の処理を行うことで、署名が送信（S20）される。上述したように電子署名ではなく、単にメールアドレスを送信するだけでよい。あるいはログイン状態である場合には、署名の信号を送信するだけで、サービスサーバ装置（20）が会員情報DB（22）を参照して、その会員のメールアドレスを取得することもできる。

40

【0071】

署名時に改めてデータ（231）から当該文書を読み込み（S21）、ハッシュ値を算出（S22）してもよいし、これらは省略してもよい。

そして、再びハッシュ値（233）と共に署名（メールアドレス）を登録情報としてプラットフォームサーバ装置（10）に送信（S23）する。この処理により、取引の当事者が順次署名を追加、更新することができる。

【0072】

プラットフォームサーバ装置（10）の情報受理部（111）が提供するAPIを通して更新された登録情報を受信すると、トランザクション発行部（112）が、登録情報に

50

係るトランザクションを発行（Ｓ２４）する。さらに、スマートコントラクト処理部（１１５）が、トランザクション発行部からのトランザクションに基づいてブロックチェーン（３０）への登録情報の記録（Ｓ２５）を行う。

【００７３】

ブロックチェーン（３０）への登録情報の記録（Ｓ２５）への登録結果、登録成功、登録失敗の情報はサービスサーバ装置（２０）に送信（Ｓ２６）され、さらにユーザ端末（５０）に通知（Ｓ２７）される。

【００７４】

次に、サービスサーバ装置（２０）上で管理されている管理データを照会する処理方法について図７を用いて説明する。

ユーザ端末（５０）からログイン（Ｓ３０）したログイン状態において、管理データを照会（Ｓ３１）を行う。具体的には、契約書一覧画面を開くことで照会をする、あるいは更新ボタンを押すことで照会する、などの手順が考えられる。

【００７５】

照会を受けるとサービスサーバ装置（２０）の登録情報照会部（２１６）が、例えば管理番号を索引として対応するハッシュ値を読み込み（Ｓ３２）、プラットフォームサーバ装置（１０）の照会受理部（１１５）に送信（Ｓ３３）する。ここでも送信されるのはハッシュ値だけであるので、プラットフォームサーバ装置（１０）側では取り扱うデータの内容には全く関与しない。

【００７６】

検索処理部（１１６）はブロックチェーン（３０）に対してハッシュ値を記録しているかどうか検索（Ｓ３４）する処理を行い、一致するものが発見された場合には合わせて記録されている署名と共に結果通知部（１１７）が検索結果として送信（Ｓ３５）する。

【００７７】

サービスサーバ装置（２０）では一覧生成部（２１７）において、ブロックチェーンによって情報の真正が認証された管理データの一覧が更新され、ユーザ端末（５０）に送信（Ｓ３６）される。

この結果は表１で示したものと同等と考えることができる。つまり、登録時に記録された管理データが、ブロックチェーン（３０）への検索を経て、認証された情報として表示（Ｓ３７）される。

【００７８】

本発明は、上記実施例のようにサービスサーバ装置（２０）においてデータ（２３１）を保存したり検索可能に管理する一方、プラットフォームサーバ装置（１０）に送信される登録情報にはデータを含まないことが好ましい。

しかし、データ（２３１）の一部又は全部をプラットフォームサーバ装置（１０）に格納してもよい。例えば上位サービスのデータベース（１４）を記憶手段に格納することもできる。

【００７９】

サービスサーバ装置（２０）は会員に対して提供するサービスの対価として課金処理を行ってもよい。課金処理方法は周知であるので説明を省略するが、例えば会員資格として月額の設定額制としたり、文書のアップロード回数に応じて、あるいは取引の成立回数に応じて課金をすることができる。課金処理のためにＣＰＵ（２０）に課金処理部（図示しない）と記憶手段（２３）に課金情報ＤＢ（図示しない）を備えてもよい。

【００８０】

本発明では、さらにこのような課金処理や、会員のログイン処理に係る処理をプラットフォームサーバ装置（１０）側で統合管理することも提案する。

【００８１】

すなわち、図２に示すようにプラットフォームサーバ装置（１０）に会員情報共通処理部（１１８）と会員情報ＤＢ（１２）を備え、ユーザ端末（５０）がログインを行おうとした場合、サービスサーバ装置（２０）はＩＤやパスワードをプラットフォームサーバ装

10

20

30

40

50

置（１０）に転送、あるいはログイン画面自体をプラットフォームサーバ装置（１０）にリダイレクトし、プラットフォームサーバ装置（１０）上でログインの認証処理を行う。

【００８２】

認証結果をプラットフォームサーバ装置（１０）からサービスサーバ装置（２０）が受信することによって、サービスサーバ装置（２０）におけるログイン状態とする。

プラットフォームサーバ装置（１０）が会員情報を管理することで、管理するデータ（２３１）と会員情報を分離して取り扱うことが可能となり、データ管理の安全性が向上する。

また、高度なログイン処理をプラットフォームサーバ装置（１０）が提供することで、サービスサーバ装置（２０）は低コストかつ簡便に優れたログイン技術を採用することができる。

10

【００８３】

ログイン処理と同様に、プラットフォームサーバ装置（１０）に課金情報共通処理部（１１９）と課金情報ＤＢ（１３）を備えることで、プラットフォームサーバ装置（１０）側でユーザ端末（５０）に対する課金処理を行うこともできる。例えばクレジットカードや電子マネーへのアクセスなど、高度な安全性を必要とする課金処理をプラットフォームサーバ装置（１０）に統合することで、上位サービスの提供において低コストかつ簡便に優れた課金処理を行うことができる。

【００８４】

言うまでもなくこの課金処理は、プラットフォームサーバ装置の運営者からサービスサーバ装置の運営者への手数料の課金処理も用いることもできる。

20

【００８５】

（別実施例１）

契約書への署名の別実施例として、電子印章具を用い紙ベースの契約手続をブロックチェーン上に記録することもできる。

図８は、本発明における情報管理プラットフォームシステムを用いて押印情報を登録する例の説明図である。

【００８６】

本発明で用いる電子印章具は、次のような構成である。すなわち、内部に印章と、印章が押印を検知する検知部と、検知部が検知した押印検知情報を有線又は無線の通信経路で送信する送信部とを備えた電子印章具（６０）、通信経路を通して押印検知情報を受信する受信部と、受信部の受信時における時刻情報及び位置情報を取得し、押印情報を生成する押印情報生成部とを備えた押印情報生成装置（６１）から構成される。

30

【００８７】

押印情報生成装置（６１）は一般的なスマートフォンなどで構成することができる。そして、押印情報生成装置（６１）が文書の電子ファイルを印刷した紙媒体（６２）上に記載された２次元バーコード（ＱＲコード（登録商標））（６３）を読み込むのと合わせて、押印検知情報を取得することによって、サービスサーバ装置（２０）が押印されたこと、すなわち取引が成立したことを認識し、対応する電子ファイルのハッシュ値と共に押印情報生成装置（６１）から送信される押印者情報を署名としてプラットフォームサーバ装置（１０）に送信する。

40

【００８８】

このような構成によれば、押印情報をブロックチェーン上に記録することができるだけでなく、サービスサーバ装置（２０）に保存される文書の電子ファイルへの署名と連係させることができるため、電子契約と、紙媒体を利用した契約形態とを統合的に処理することができる。

【００８９】

（別実施例２）

本発明に係る情報管理プラットフォームシステム（１）は上記実施例で示したような文書の管理に限定されない。プラットフォームサーバ装置（１０）がサービスサーバ装置（

50

20) から受理するデータは任意であり、データベースのいかなるフィールドでも取り扱うことができる。

【0090】

一例として、サービスサーバ装置(20)が、複数のIoT(Internet Of Things)デバイス(70)(71)(72)と接続され、IoTデバイス(70)(71)(72)との通信履歴をブロックチェーン(30)上に記録することもできる。

通信履歴の具体的な内容は任意であり、例えばIoTデバイスのオンオフ情報、IoTデバイスのセンサの検知情報、IoTデバイスの動作結果情報などである。

【0091】

さらにIoTデバイス同士による契約の締結を通信履歴としてもよい。例えば、在庫が少なくなったことを検知するIoTデバイスから、追加発注の信号を送信し、受注を行う別のIoTデバイスがこの承諾を通知した場合に、その契約内容に関する情報のハッシュ値と当事者のIoTデバイスのシリアル番号をブロックチェーン(30)に記録する。

【0092】

各IoTデバイス(70)(71)(72)をIoTハブ(73)と通信し、IoTハブ(73)からサービスサーバ装置(20)にIoTデバイスのシリアル番号と共に通信履歴を通知する。通信履歴から所定の計算式によって算出したハッシュ値と、通信履歴に関する付加情報としてシリアル番号をAPIを通してプラットフォームサーバ装置(10)に送信し、スマートコントラクト処理部(113)がブロックチェーン上に記録する。

【0093】

本実施例におけるIoTデバイスはいかなるデバイスでもよく、IoTハブ(73)を用いなくてもよいし、ネットワーク上に広く分布するIoTデバイスを対象とするものである。

【0094】

本構成によれば、IoTデバイス(70)(71)(72)の動作に係る通信履歴を改ざん不可能にブロックチェーン上に保存することができる。タイムスタンプと共に記録すれば、さまざまなIoTデバイスの動作を後日検証可能に記録することができる。

【0095】

上記実施例と同じように、サービスサーバ装置(20)からハッシュ値を送信して、プラットフォームサーバ装置(10)の照会受理部(115)、検索処理部(116)、結果通知部(117)を経て、一覧生成部(217)が通信履歴の真正を表示することもできる。

【0096】

(その他の適用事例)

情報管理プラットフォームシステム(1)を用いた取り扱いデータの例を列挙する。

第1に、アプリケーションソフトから対応するサービスサーバ装置にコンテンツを送信し、そのコンテンツに係る認証を行うことが考えられる。

例えば、楽曲や描画のアプリケーションで作成されたコンテンツをサービスサーバ装置(20)が受信して、ハッシュ値とタイムスタンプをブロックチェーン(30)に記録することによって著作権の認証が可能である。

【0097】

また、Web会議のアプリケーションがその録音・録画コンテンツをサービスサーバ装置(20)に送信し、ハッシュ値とタイムスタンプをブロックチェーン(30)に記録することによって議事録の認証が可能である。

【0098】

発明の記録をアプリケーションソフト上で文書作成し、その文書コンテンツをサービスサーバ装置(20)に送信し、ハッシュ値とタイムスタンプをブロックチェーン(30)に記録することによって発明ノートの認証が可能である。

【0099】

第2に、任意のデバイスとサービスサーバ装置(20)を接続し、デバイスで生成され

10

20

30

40

50

たデータを認証することにも用いることができる。例えば、デジタルカメラから、撮影された写真のデータをサービスサーバ装置（２０）に送信し、そのハッシュ値とタイムスタンプをブロックチェーンに記録することにより、撮影日や非改ざんを証明できる機能を提供することができる。

【０１００】

自動車や、航空機、船舶、建設機械等に備えるＧＰＳデバイスの測位結果と、その識別情報をサービスサーバ装置（２０）に送信し、ブロックチェーンに記録することもできる。

【０１０１】

第３に、既存のオンライン上のストレージと組み合わせたサービスも考えられる。例えば、ストレージサービス事業者が、その保存された情報を電子帳簿保存法に準拠した保管サービスを提供することができる。

10

【０１０２】

第４に、クラウドソーシングサービスを提供する事業者が、参加する当事者間の契約条件の公証機能を提供することにも適用できる。例えば、クラウドソーシングの付加サービスとして、募集事業者と多数の個人事業主間の契約文書をブロックチェーンに記録し証明することができる。

【０１０３】

これらのように、本発明に係る情報管理プラットフォームシステムは、管理するデータを誰が作ったのか、データが作られたのはいつか、データが作られた時から改変されていないか、データに対し誰がいつどのような操作を行ったか、など管理データに係る様々な認証の場面で汎用的に用いることができる。

20

【符号の説明】

【０１０４】

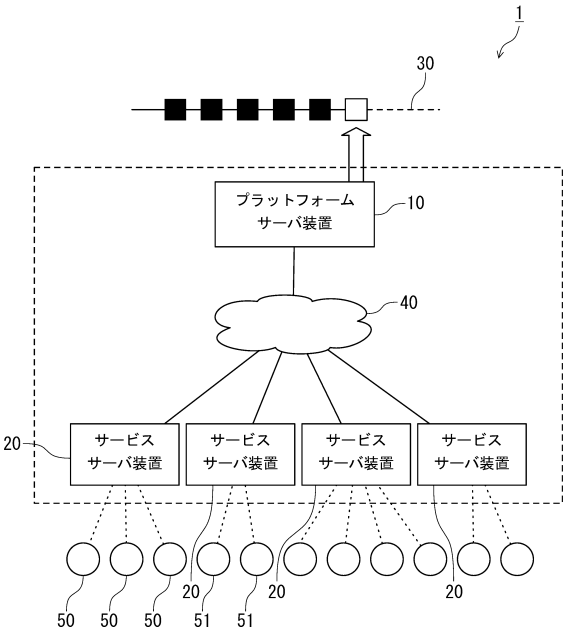
- １ 情報管理プラットフォームシステム
- １０ プラットフォームサーバ装置
- ２０ サービスサーバ装置
- ３０ ブロックチェーン
- ４０ 通信ネットワーク
- ５０ ユーザ端末
- ６０ 電子印章具

30

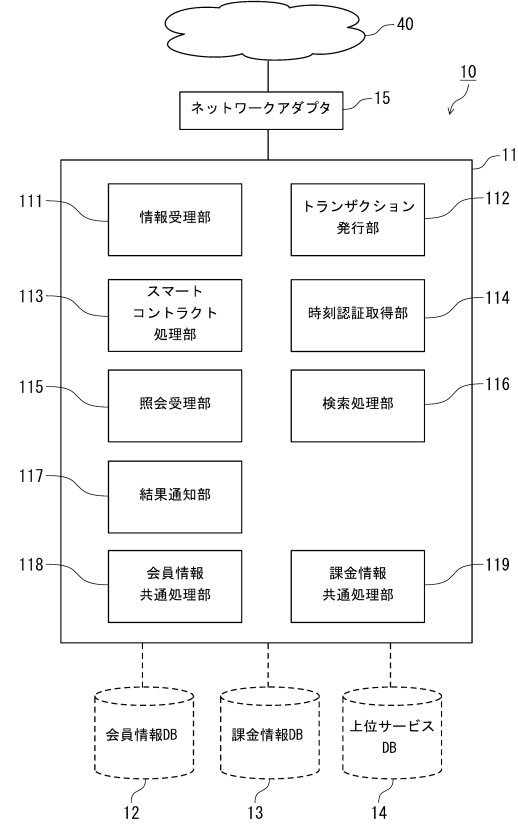
40

50

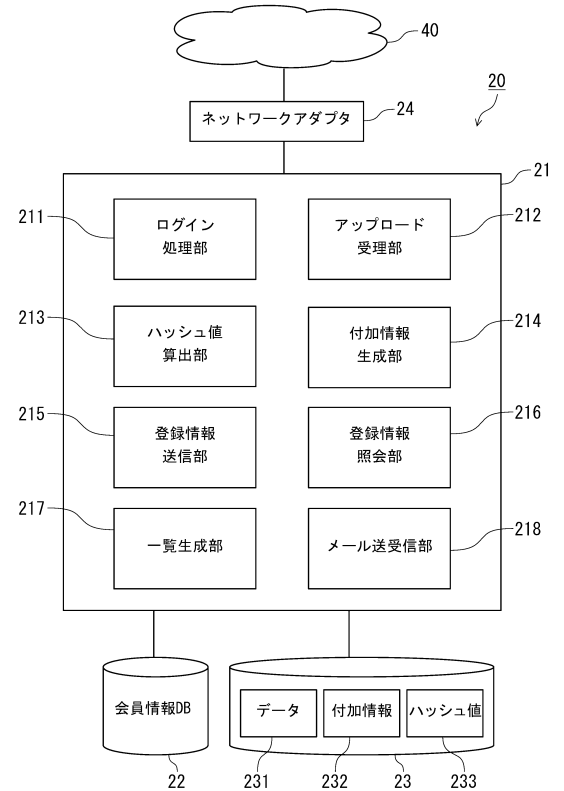
【図面】
【図 1】



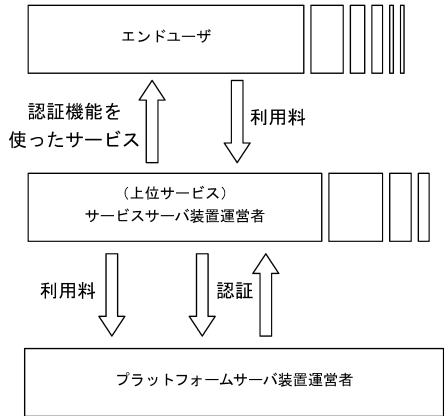
【図 2】



【図 3】



【図 4】



10

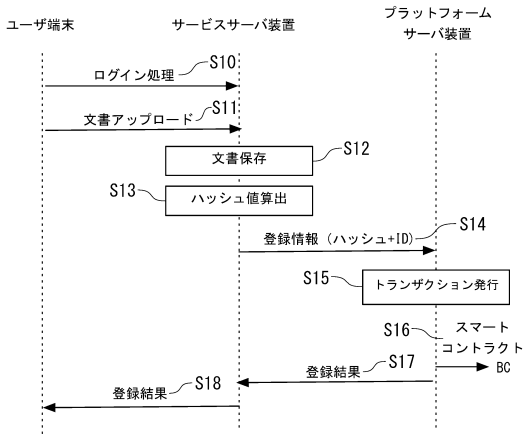
20

30

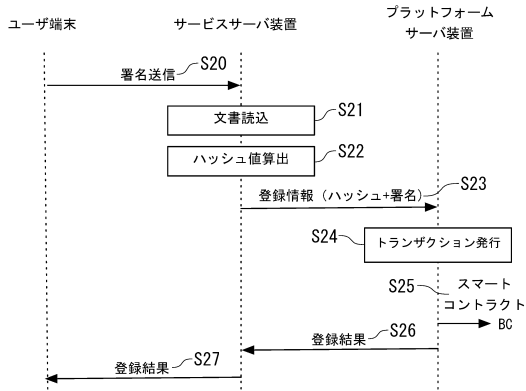
40

50

【図 5】

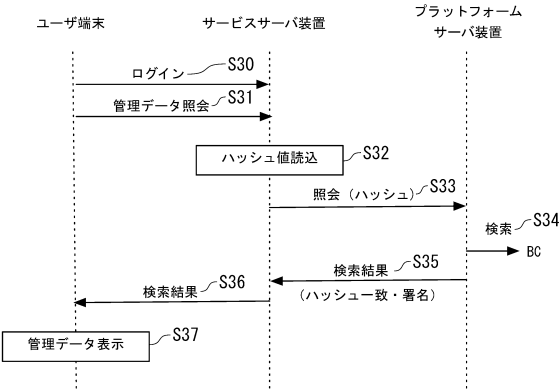


【図 6】

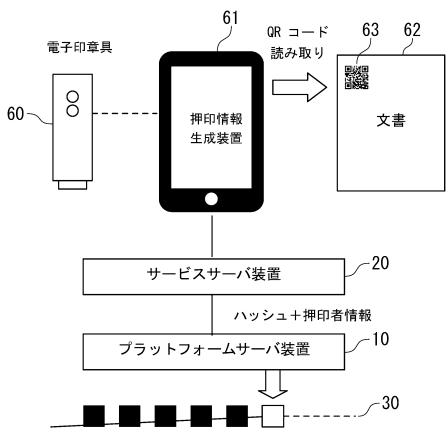


10

【図 7】



【図 8】



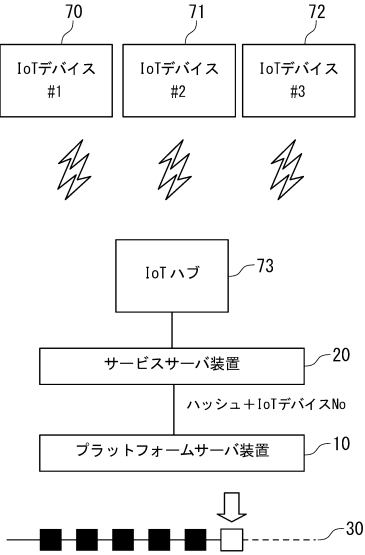
20

30

40

50

【図 9】



10

20

30

40

50

フロントページの続き

(56)参考文献 国際公開第2019/207655 (WO, A1)
 韓国公開特許第10-2020-0092210 (KR, A)
 特開2020-161092 (JP, A)
 米国特許第10826684 (US, B1)
 米国特許出願公開第2019/0386833 (US, A1)
 韓国公開特許第2020-0048440 (KR, A)
(58)調査した分野 (Int.Cl., DB名)
 H04L 9/32
 G06Q 20/38