

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7136339号
(P7136339)

(45)発行日 令和4年9月13日(2022.9.13)

(24)登録日 令和4年9月5日(2022.9.5)

(51)国際特許分類 F I
 G 0 6 Q 50/10 (2012.01) G 0 6 Q 50/10
 H 0 4 L 9/32 (2006.01) H 0 4 L 9/32 2 0 0 D

請求項の数 8 (全13頁)

(21)出願番号	特願2021-511704(P2021-511704)	(73)特許権者	000005223 富士通株式会社 神奈川県川崎市中原区上小田中4丁目1番1号
(86)(22)出願日	平成31年3月29日(2019.3.29)	(74)代理人	110001519 特許業務法人太陽国際特許事務所
(86)国際出願番号	PCT/JP2019/014209	(72)発明者	永井 功一 東京都港区東新橋一丁目5番2号 富士通Japan株式会社内
(87)国際公開番号	WO2020/202326	(72)発明者	島田 昌紘 東京都港区東新橋一丁目5番2号 富士通Japan株式会社内
(87)国際公開日	令和2年10月8日(2020.10.8)	審査官	松田 岳士
審査請求日	令和3年9月22日(2021.9.22)		

最終頁に続く

(54)【発明の名称】 情報処理プログラム、装置、及び方法

(57)【特許請求の範囲】

【請求項1】

要求元から書面データについての真偽確認の要求を受け付けた場合に、前記書面データの真偽確認を実行し、

前記真偽確認の照会結果を前記要求元に対して送信し、

前記要求元からの真偽確認の要求、又は前記真偽確認の照会結果の前記要求元への送信のいずれかに応じて、前記要求元の情報と前記書面データの識別情報とを対応付けて第1記憶部に記憶し、

第2記憶部に予め記憶された前記書面データの発行元に対し、前記書面データの識別情報と対応付けられた前記要求元の情報を通知する

ことを含む処理をコンピュータに実行させることを特徴とする情報処理プログラム。

【請求項2】

前記発行元が前記書面データを発行した場合に、前記書面データから計算されるハッシュ値と前記書面データの識別情報とを対応付けて前記第1記憶部に記憶する請求項1に記載の情報処理プログラム。

【請求項3】

前記真偽確認の要求として、前記書面データを受け付け、前記書面データから計算されるハッシュ値と、前記第1記憶部に記憶されたハッシュ値とを照合することにより、前記真偽確認を実行する請求項2に記載の情報処理プログラム。

【請求項4】

前記真偽確認の要求として、前記書面データ及び前記書面データの識別情報を受け付け、前記書面データから計算されるハッシュ値と、前記第1記憶部に記憶されたハッシュ値とを照合すると共に、受け付けた前記書面データの識別情報と、前記第1記憶部に記憶された前記書面データの識別情報とを照合することにより、前記真偽確認を実行する請求項2に記載の情報処理プログラム。

【請求項5】

受け付けた前記ハッシュ値及び前記書面データの識別情報と、前記第1記憶部に記憶された前記ハッシュ値及び前記書面データの識別情報とを照合した前記真偽確認の照会結果として、両方とも一致、前記書面データの識別情報のみ一致、前記ハッシュ値のみ一致、又は両方とも不一致であることを前記要求元へ送信する請求項4に記載の情報処理プログラム。

10

【請求項6】

第1記憶部及び第2記憶部はブロックチェーンデータベースであり、前記コンピュータはネットワークで接続された複数の他のコンピュータと共にブロックチェーンを構成する請求項1～請求項5のいずれか1項に記載の情報処理プログラム。

【請求項7】

要求元から書面データについての真偽確認の要求を受け付けた場合に、前記書面データの真偽確認を実行し、前記真偽確認の照会結果を前記要求元に対して送信し、前記要求元からの真偽確認の要求、又は前記真偽確認の照会結果の前記要求元への送信のいずれかに応じて、前記要求元の情報と前記書面データの識別情報とを対応付けて第1記憶部に記憶する実行部と、

20

第2記憶部に予め記憶された前記書面データの発行元に対し、前記書面データの識別情報と対応付けられた前記要求元の情報を通知する通知部と、

を含む情報処理装置。

【請求項8】

要求元から書面データについての真偽確認の要求を受け付けた場合に、前記書面データの真偽確認を実行し、前記真偽確認の照会結果を前記要求元に対して送信し、

前記要求元からの真偽確認の要求、又は前記真偽確認の照会結果の前記要求元への送信のいずれかに応じて、前記要求元の情報と前記書面データの識別情報とを対応付けて第1記憶部に記憶し、

30

第2記憶部に予め記憶された前記書面データの発行元に対し、前記書面データの識別情報と対応付けられた前記要求元の情報を通知する

ことを含む処理をコンピュータが実行することを特徴とする情報処理方法。

【発明の詳細な説明】

【技術分野】

【0001】

開示の技術は、情報処理プログラム、情報処理装置、及び情報処理方法に関する。

【背景技術】

【0002】

従来、公開者がネットワーク上で公開している資格情報の証明をオンラインで提供するシステムが提案されている。このシステムは、第1のネットワークとは異なる第2のネットワークに接続され、資格情報の証明を要求する証明要求を資格情報公開サーバからインタフェースを介して受信する。また、資格情報データベースにアクセスして証明要求の対象となる資格情報の申告識別子を取得する。そして、公開者識別子及び申告識別子の組み合わせに対応する資格保有者識別子及び証明書識別子の組み合わせが証明書データベースに保持されているか否かを証明サーバを介して問い合わせ、証明要求の対象となる資格情報の証明を行う。

40

【0003】

また、ユーザが情報を入力する手間や窓口に出向く手間あるいは書類を郵送する手間を省くと共に、効率のよいユーザ認証を実現するシステムが提案されている。このシステム

50

では、端末が、記憶する身分証明書データを中継サーバに送信し、データ検証サーバにより身分証明書データが真正である場合に、検証済みの身分証明書データを耐タンパデバイスに書き込む。そして、ユーザが事業者からサービスを受ける場合に、事業者サーバが、端末にユーザの身分証明書データの属性情報の送信を要求し、端末が、身分証明書データを中継サーバに送信する。そして、データ検証サーバにより身分証明書データが真正であるときに、端末が、事業者サーバに、検証済みのユーザの身分証明書データの属性情報を送信し、事業者サーバが登録完了通知を端末に送信する。

【先行技術文献】

【特許文献】

【0004】

【文献】特開2010-278982号公報

特開2012-181800号公報

【発明の概要】

【発明が解決しようとする課題】

【0005】

従来、証明書等の書面の提出を受けた企業や学校等の機関が、その書面の真偽を確認する仕組みは存在する。しかし、書面を発行した発行元が、発行した書面のその後の利用状況を把握する仕組みがなく、発行元が効率的及び効果的なマーケティング活動を行えないという問題がある。

【0006】

一つの側面として、開示の技術は、書面を発行した発行元が、発行した書面の提出先の情報を取得することを目的とする。

【課題を解決するための手段】

【0007】

一つの態様として、開示の技術は、要求元から書面データについての真偽確認の要求を受け付けた場合に、前記書面データの真偽確認を実行し、前記真偽確認の照会結果を前記要求元に対して送信する。また、開示の技術は、前記要求元からの真偽確認の要求、又は前記真偽確認の照会結果の前記要求元への送信のいずれかに応じて、前記要求元の情報と前記書面データの識別情報とを対応付けて第1記憶部に記憶する。そして、開示の技術は、第2記憶部に予め記憶された前記書面データの発行元に対し、前記書面データの識別情報と対応付けられた前記要求元の情報を通知する。

【発明の効果】

【0008】

一つの側面として、書面を発行した発行元が、発行した書面の提出先の情報を取得することができる、という効果を有する。

【図面の簡単な説明】

【0009】

【図1】本実施形態に係る情報処理システムの概略構成を示すブロック図である。

【図2】本実施形態に係る情報処理システムにより提供されるサービスの概要を説明するための図である。

【図3】情報処理装置の機能ブロック図である。

【図4】処理情報DB(Database)の一例を示す図である。

【図5】機関情報DBの一例を示す図である。

【図6】本実施形態に係る情報処理装置として機能するコンピュータの概略構成を示すブロック図である。

【図7】登録処理の一例を示すフローチャートである。

【図8】照会処理の一例を示すフローチャートである。

【図9】参照処理の一例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】

【0010】

10

20

30

40

50

以下、図面を参照して、開示の技術に係る実施形態の一例を説明する。

【0011】

図1に示すように、本実施形態に係る情報処理システム100は、複数の情報処理装置10と、複数の発行元端末32と、複数のユーザ端末34と、複数の提出先端末36とを含んで構成される。なお、図1では、発行元端末32、ユーザ端末34、及び提出先端末36の各々は、それぞれ1つのみ図示している。発行元端末32、ユーザ端末34、提出先端末36、及び情報処理装置10の各々は、ネットワークを介してそれぞれ接続されている。

【0012】

発行元端末32は、証明書の発行元が利用する情報処理端末である。本実施形態では、発行元が、語学学校、専門学校、資格の認定及び運営を行う団体等の教育機関である場合について説明する。

10

【0013】

ユーザ端末34は、証明書が発行される対象のユーザが利用する情報処理端末である。本実施形態では、ユーザは、上記の教育機関を利用した学生等である。

【0014】

提出先端末36は、ユーザが証明書を提出する提出先が利用する情報処理端末である。本実施形態では、提出先は、例えば、ユーザが入学を希望する教育機関や、就労を希望する企業等である。

【0015】

発行元端末32、ユーザ端末34、及び提出先端末36の各々は、説明の都合上、異なる名称を付与して区別しているが、いずれも、例えば、パーソナルコンピュータ、タブレット端末、スマートフォン等で実現することができる。

20

【0016】

複数の情報処理装置10は、図2に示すように、本実施形態に係る情報処理システム100により提供されるサービスのプラットフォームであって、ブロックチェーンを活用した情報処理プラットフォーム38の各ノードとして機能する。

【0017】

ここで、図2を参照して、本実施形態に係る情報処理システム100により提供されるサービスの概要について説明する。

30

【0018】

発行元が対象のユーザに対して証明書を発行すると、証明書をPDF (Portable Document Format) などのフォーマットで電子データ化した証明書データが、発行元端末32からユーザ端末34へ送信される。この際、発行元端末32から情報処理プラットフォーム38へ、証明書データのユニークな識別情報である証明書番号、証明書データ、及び発行元の識別情報である発行元IDを含む登録要求を送信する。そして、情報処理プラットフォーム38が、証明書データに関する処理情報(詳細は後述)をブロックチェーン上に登録する。ユーザは、発行された証明書データを提出先に提出する。

【0019】

提出先は、その証明書データの真偽確認を行うために、提出先端末36から、証明書データ、その証明書データの証明書番号、及び提出先の識別情報である提出先IDを含む照会要求を情報処理プラットフォーム38へ送信する。情報処理プラットフォーム38は、証明書データの真偽確認を行うと共に、照会要求を行った提出先の情報、及び真偽確認を行った照会結果をブロックチェーン上に記憶し、照会結果を提出先に返却する。また、情報処理プラットフォーム38は、照会があった場合又は照会結果の返却を行った場合に、対象の証明書データを発行した発行元に、その旨を通知する。

40

【0020】

発行元は、通知を受けて、発行元端末32から、証明書番号を含む参照要求を情報処理プラットフォーム38へ送信する。情報処理プラットフォーム38は、参照要求に応じて、該当の証明書データが提出された提出先の情報、及び真偽確認の照会結果を発行元端末

50

3 2 へ送信する。

【 0 0 2 1 】

以下、情報処理プラットフォーム 3 8 として機能するブロックチェーンを構成する情報処理装置 1 0 の機能構成について詳述する。なお、複数の情報処理装置 1 0 の構成は同様であるため、1 つの情報処理装置 1 0 について説明する。

【 0 0 2 2 】

図 3 に示すように、情報処理装置 1 0 は、機能的には、登録部 1 2 と、実行部 1 4 と、通知部 1 6 とを含む。また、ブロックチェーンを構成する複数の情報処理装置 1 0 の各々の所定の記憶領域は、ブロックチェーンデータベースとして機能し、処理情報 D B (Data base) 2 0 及び機関情報 D B 2 2 が記憶される。

10

【 0 0 2 3 】

登録部 1 2 は、発行元端末 3 2 から送信された証明書番号、証明書データ、及び発行元 I D を含む登録要求を受け付ける。登録部 1 2 は、受け付けた登録要求に含まれる証明書データからハッシュ値を計算し、受け付けた登録要求に含まれる証明書番号及び発行元 I D と、処理種別（詳細は後述）及び処理日時と共に、処理情報として処理情報 D B 2 0 に記憶する。

【 0 0 2 4 】

図 4 に、処理情報 D B 2 0 の一例を示す。図 4 の例では、各行（各レコード）が 1 つの処理情報に相当する。各処理情報は、「証明書番号」、「ハッシュ値」、「処理種別」、「処理者」、「処理日時」、「処理結果」等の項目を含む。

20

【 0 0 2 5 】

「処理種別」は、証明書データに関連したどのような種別の処理が行われたかを示す情報である。例えば、証明書データに関する情報を処理情報 D B 2 0 に記憶する場合、すなわち、登録部 1 2 により記憶される処理情報の「処理種別」は「登録」とすることができる。また、証明書データの真偽確認を実行した場合、すなわち、後述する実行部 1 4 により記憶される処理情報の処理種別は「照会」とすることができる。また、「登録」及び「照会」以外にも、「削除」、「参照」等の他の処理種別を設定してもよい。

【 0 0 2 6 】

「処理者」は、証明書データに関する情報について、「処理種別」で示される処理を要求した機関を特定する情報である。例えば、証明書データに関する情報を処理情報 D B 2 0 に記憶する場合、すなわち、登録部 1 2 により記憶される処理情報の「処理者」には、登録部 1 2 が受け付けた登録要求に含まれる発行元 I D が記憶される。また、証明書データの真偽確認を実行した場合、すなわち、後述する実行部 1 4 により記憶される処理情報の「処理者」には、実行部 1 4 が受け付けた照会要求に含まれる提出先 I D が記憶される。

30

【 0 0 2 7 】

「処理結果」は、「処理種別」で示される処理を実行した結果であり、例えば、証明書データの真偽確認を実行した場合、その真偽確認の照会結果が記憶される。

【 0 0 2 8 】

処理情報 D B 2 0 に記憶される処理情報に含まれる項目は上記の項目に限定されず、証明書データの内容、例えば、その証明書データに関連する教育課程の履修コース、資格試験の成績等の情報を含んでいてもよい。

40

【 0 0 2 9 】

実行部 1 4 は、提出先端末 3 6 から送信された証明書データ、証明書番号、及び提出先 I D を含む照会要求を受け付ける。実行部 1 4 は、受け付けた照会要求に含まれる証明書データからハッシュ値を計算する。実行部 1 4 は、受け付けた照会要求に含まれる証明書番号及び計算したハッシュ値と、処理情報 D B 2 0 に記憶されている証明書番号及びハッシュ値とを照合し、照会要求の対象の証明書データの真偽確認を実行する。

【 0 0 3 0 】

具体的には、実行部 1 4 は、受け付けた照会要求に含まれる証明書番号及び計算したハッシュ値と一致する証明書番号及びハッシュ値が処理情報 D B 2 0 に記憶されている場合

50

には、真偽確認の照会結果を「真」とする。また、実行部 14 は、一致する証明書番号は処理情報 DB 20 に存在するものの、対応付けて記憶されたハッシュ値が一致しない場合には、真偽確認の照会結果を「偽（ハッシュ値不一致）」とする。また、一致する証明書番号も、一致するハッシュ値も処理情報 DB 20 に存在しない場合には、真偽確認の照会結果を「偽（該当なし）」とする。さらに、実行部 14 は、一致するハッシュ値は処理情報 DB 20 に存在するものの、対応付けて記憶された証明書番号が一致しないなど、イレギュラーな場合には、真偽確認の照会結果を「その他」とする。

【 0 0 3 1 】

このように、真偽確認の照会結果を分類することで、単純に真又は偽とする場合に比べ、多くの情報を得ることができる。例えば、照会結果「偽（ハッシュ値不一致）」の場合には、正規の証明書データに対して改ざんが行われていると予想することができる。また、照会結果「偽（該当なし）」の場合は、証明書データ自体が偽造されていると予想することができる。

10

【 0 0 3 2 】

実行部 14 は、提出先端末 36 から受け付けた照会要求に含まれる証明書番号及び提出先 ID と、計算したハッシュ値と、真偽確認の照会結果と、処理種別「照会」及び処理日時とを、処理情報として処理情報 DB 20 に記憶する。また、実行部 14 は、照会要求を送信した提出先端末 36 へ、真偽確認の照会結果を返却する。

【 0 0 3 3 】

通知部 16 は、処理種別「照会」の処理情報が処理情報 DB 20 に記憶されると、その処理情報の「証明書番号」が示す証明書データを発行した発行元へ、照会があった旨を通知する。

20

【 0 0 3 4 】

具体的には、通知部 16 は、処理情報 DB 20 に記憶された処理種別「照会」の処理情報の「証明書番号」、すなわち、真偽確認が行われた証明書データの証明書番号を取得する。そして、通知部 16 は、情報処理システム 100 が提供するサービスを利用する機関に関する情報が記憶された機関情報 DB 22 を参照して、取得した証明書番号に対応する発行元のアドレスを取得する。

【 0 0 3 5 】

図 5 に、機関情報 DB 22 の一例を示す。図 5 の例では、機関毎に、発行元 ID 又は提出先 ID を示す「機関 ID」、機関 ID が示す機関の名称である「機関名」、「区分」、「アドレス」、「証明書番号」等の情報が対応付けて記憶されている。「区分」は機関が発行元か提出先かを示す情報であり、「アドレス」は、例えば、発行元端末 32 又は提出先端末 36 の IP アドレスや発行元端末 32 又は提出先端末 36 で利用されるメールアドレス等である。

30

【 0 0 3 6 】

通知部 16 は、取得した発行元端末 32 のアドレスに、真偽確認が行われた証明書データの証明書番号を送信することにより、発行元に、発行元が発行した証明書データに対する照会があった旨を通知する。

【 0 0 3 7 】

また、通知部 16 は、通知に応じて、発行元端末 32 から送信された証明書番号を含む参照要求を受け付けると、処理情報 DB 20 から、受け付けた参照要求に含まれる証明書番号と、処理種別「照会」とを含む処理情報を取得して、発行元端末 32 へ送信する。これにより、発行元は、自身が発行した証明書データが提出された提出先の情報を取得することができる。また、真偽確認の照会結果から、証明書データの改ざんや偽造の有無を確認することができる。

40

【 0 0 3 8 】

また、通知部 16 は、提出先の情報として、処理情報に含まれる提出先 ID に対応する機関名を機関情報 DB 22 から取得して、処理情報と共に送信してもよい。また、通知部 16 は、照会があった旨の通知として、該当の処理情報自体を発行元端末 32 へ送信して

50

もよい。この場合、発行元端末 3 2 からの参照要求は不要となる。

【 0 0 3 9 】

情報処理装置 1 0 は、例えば図 6 に示すコンピュータ 4 0 で実現することができる。コンピュータ 4 0 は、CPU (Central Processing Unit) 4 1 と、一時記憶領域としてのメモリ 4 2 と、不揮発性の記憶部 4 3 とを備える。また、コンピュータ 4 0 は、入力部、表示部等の入出力装置 4 4 と、記憶媒体 4 9 に対するデータの読み込み及び書き込みを制御する R / W (Read/Write) 部 4 5 とを備える。また、コンピュータ 4 0 は、インターネット等のネットワークに接続される通信 I / F (Interface) 4 6 を備える。CPU 4 1、メモリ 4 2、記憶部 4 3、入出力装置 4 4、R / W 部 4 5、及び通信 I / F 4 6 は、バス 4 7 を介して互いに接続される。

10

【 0 0 4 0 】

記憶部 4 3 は、HDD (Hard Disk Drive)、SSD (Solid State Drive)、フラッシュメモリ等によって実現できる。記憶媒体としての記憶部 4 3 には、コンピュータ 4 0 を、情報処理装置 1 0 として機能させるための情報処理プログラム 5 0 が記憶される。情報処理プログラム 5 0 は、登録プロセス 5 2 と、実行プロセス 5 4 と、通知プロセス 5 6 とを有する。また、記憶部 4 3 は、処理情報 DB 2 0 及び機関情報 DB 2 2 の各々を構成する情報が記憶される情報記憶領域 6 0 を有する。

【 0 0 4 1 】

CPU 4 1 は、情報処理プログラム 5 0 を記憶部 4 3 から読み出してメモリ 4 2 に展開し、情報処理プログラム 5 0 が有するプロセスを順次実行する。CPU 4 1 は、登録プロセス 5 2 を実行することで、図 3 に示す登録部 1 2 として動作する。また、CPU 4 1 は、実行プロセス 5 4 を実行することで、図 3 に示す実行部 1 4 として動作する。また、CPU 4 1 は、通知プロセス 5 6 を実行することで、図 3 に示す通知部 1 6 として動作する。また、CPU 4 1 は、情報記憶領域 6 0 から情報を読み出して、処理情報 DB 2 0 及び機関情報 DB 2 2 の各々をメモリ 4 2 に展開する。これにより、情報処理プログラム 5 0 を実行したコンピュータ 4 0 が、情報処理装置 1 0 として機能することになる。なお、プログラムを実行する CPU 4 1 はハードウェアである。

20

【 0 0 4 2 】

なお、情報処理プログラム 5 0 により実現される機能は、例えば半導体集積回路、より詳しくはASIC (Application Specific Integrated Circuit) 等で実現することも可能である。

30

【 0 0 4 3 】

次に、本実施形態に係る情報処理装置 1 0 の作用について説明する。発行元端末 3 2 から登録要求が送信されると、情報処理装置 1 0 において、図 7 に示す登録処理が実行される。また、提出先端末 3 6 から照会要求が送信されると、情報処理装置 1 0 において、図 8 に示す照会処理が実行される。また、発行元端末 3 2 から参照要求が送信されると、情報処理装置 1 0 において、図 9 に示す参照処理が実行される。なお、登録処理、照会処理、及び参照処理は、開示の技術の情報処理方法の一例である。

【 0 0 4 4 】

まず、図 7 に示す登録処理について説明する。

40

【 0 0 4 5 】

ステップ S 1 2 で、登録部 1 2 が、発行元端末 3 2 から送信された証明書番号、証明書データ、及び発行元 ID を含む登録要求を受け付ける。

【 0 0 4 6 】

次に、ステップ S 1 4 で、登録部 1 2 が、上記ステップ S 1 2 で受け付けた登録要求に含まれる証明書データからハッシュ値を計算する。

【 0 0 4 7 】

次に、ステップ S 1 6 で、登録部 1 2 が、受け付けた登録要求に含まれる証明書番号及び発行元 ID (「処理者」と)、上記ステップ S 1 4 で計算したハッシュ値と、処理種別「登録」と、処理日時とを、処理情報として処理情報 DB 2 0 に記憶する。そして、登録

50

処理は終了する。

【 0 0 4 8 】

次に、図 8 に示す照会処理について説明する。

【 0 0 4 9 】

ステップ S 2 2 で、実行部 1 4 が、提出先端末 3 6 から送信された証明書データ、証明書番号、及び提出先 I D を含む照会要求を受け付ける。

【 0 0 5 0 】

次に、ステップ S 2 4 で、実行部 1 4 が、上記ステップ S 2 2 で受け付けた照会要求に含まれる証明書データからハッシュ値を計算する。

【 0 0 5 1 】

次に、ステップ S 2 6 で、実行部 1 4 が、受け付けた照会要求に含まれる証明書番号及び計算したハッシュ値と、処理情報 D B 2 0 に記憶されている証明書番号及びハッシュ値とを照合する。実行部 1 4 は、証明書番号及びハッシュ値の一致又は不一致に応じて、真偽確認の照会結果「真」、「偽（ハッシュ値不一致）」、「偽（該当なし）」、又は「その他」を決定する。

【 0 0 5 2 】

次に、ステップ S 2 8 で、実行部 1 4 が、照会要求を送信した提出先端末 3 6 へ、上記ステップ S 2 6 で決定した真偽確認の照会結果を返却する。

【 0 0 5 3 】

ステップ S 3 0 で、実行部 1 4 が、照会要求に含まれる証明書番号及び提出先 I D（「処理者」と、計算したハッシュ値と、決定した真偽確認の照会結果（「処理結果」と、処理種別「照会」と、処理日時とを、処理情報として処理情報 D B 2 0 に記憶する。

【 0 0 5 4 】

次に、ステップ S 3 2 で、処理種別「照会」の処理情報が処理情報 D B 2 0 に記憶されたこと、すなわち、証明書データの真偽確認の照会があった旨を、その処理情報の「証明書番号」が示す証明書データを発行した発行元へ通知する。そして、照会処理は終了する。

【 0 0 5 5 】

次に、図 9 に示す参照処理について説明する。

【 0 0 5 6 】

ステップ S 4 2 で、通知部 1 6 が、発行元端末 3 2 から送信された証明書番号を含む参照要求を受け付ける。

【 0 0 5 7 】

次に、ステップ S 4 4 で、通知部 1 6 が、処理情報 D B 2 0 から、上記ステップ S 4 2 で受け付けた参照要求に含まれる証明書番号と、処理種別「照会」とを含む処理情報を取得して、発行元端末 3 2 へ送信する。そして、参照処理は終了する。

【 0 0 5 8 】

以上説明したように、本実施形態に係る情報処理システムによれば、情報処理装置が、証明書データの提出先から、証明書データの真偽確認の照会要求があった場合、又は照会結果を返却した場合に、その旨を証明書データの発行元へ通知する。そして、発行元へ提出先の情報及び照会結果を送信する。これにより、証明書データを発行した発行元が、発行した証明書データの提出先の情報を取得することができる。また、真偽確認の照会結果から、証明書データの改ざんや偽造の有無を確認することができる。

【 0 0 5 9 】

例えば、発行元が資格検定に関する機関である場合、証明書データの提出先を把握することで、受験者数増に向けた効率的かつ効果的なマーケティングが可能となる。また、資格検定の認定又は合格証の証明書データが偽造されて利用された場合には、その資格検定の信頼性やブランドを損なうおそれがある。本実施形態のように、発行元が、証明書データの改ざんや偽造の有無等を把握することで、ウェブ上や提出先の機関への注意喚起を行うなどの対策を早期にとることができる。また、改ざんや偽造が困難となるように、証明書データのデザインを改めたり、電子透かしを埋め込んだりなどの対策をとることも

10

20

30

40

50

できる。

【 0 0 6 0 】

また、本実施形態に係る情報処理システムによるサービスを提供する情報処理プラットフォームを、ブロックチェーンを活用して実現する。これにより、登録されたハッシュ値の改ざん防止、処理情報DBに記憶された情報の損失防止等が図れ、システムの信頼性を担保することができる。

【 0 0 6 1 】

なお、上記実施形態では、処理情報DBに、証明書データの真偽確認の照会結果を含む処理種別「照会」の処理情報が記憶された場合に、発行元にその旨を通知する場合について説明したが、これに限定されない。提出先から照会要求があった時点で、照会要求があったことを示す処理情報を処理情報DBに記憶し、その旨を発行元に通知するようにしてもよい。

10

【 0 0 6 2 】

また、上記実施形態では、書面データの一例として教育機関が発行する証明書データについて説明したが、これに限定されず、例えば、身分証等の他の証明書であってもよいし、領収書、各種帳票等の他の書面を電子データ化した書面データであってもよい。また、発行元も教育機関に限定されず、自治体や金融機関等であってもよい。

【 0 0 6 3 】

また、上記実施形態では、証明書番号とハッシュ値との組合せで、証明書データの真偽確認を実行する場合について説明したが、これに限定されない。照会要求に含まれるハッシュ値と一致するハッシュ値が処理情報DBに存在するか否かで照合してもよいし、証明書番号及びハッシュ値に、証明書データを発行されたユーザの識別情報も加えて照合してもよい。

20

【 0 0 6 4 】

また、上記実施形態において、ユーザ端末34から、ユーザが自身に発行された証明書データの真偽確認を照会したり、真偽確認の照会結果を参照したりできるようにしてもよい。

【 0 0 6 5 】

また、上記実施形態では、ブロックチェーンを活用した場合について説明したが、中央集権型システムや、他の分散型のシステムで実現してもよい。

30

【 0 0 6 6 】

また、上記実施形態では、情報処理プログラムが記憶部に予め記憶（インストール）されている態様を説明したが、これに限定されない。開示の技術に係るプログラムは、CD-ROM、DVD-ROM、USBメモリ等の記憶媒体に記憶された形態で提供することも可能である。

【 0 0 6 7 】

以上の実施形態に関し、更に以下の付記を開示する。

【符号の説明】

【 0 0 6 8 】

- 10 情報処理装置
- 12 登録部
- 14 実行部
- 16 通知部
- 20 処理情報DB
- 22 機関情報DB
- 32 発行元端末
- 34 ユーザ端末
- 36 提出先端末
- 38 情報処理プラットフォーム
- 40 コンピュータ

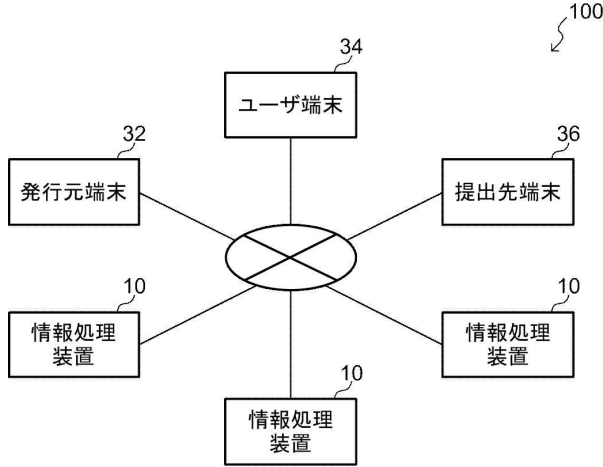
40

50

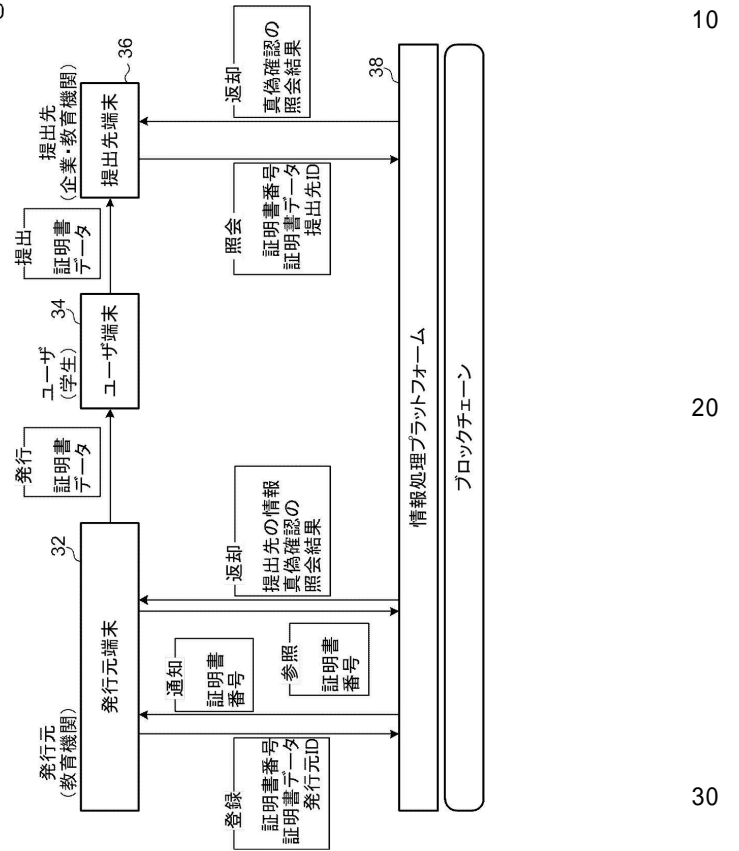
- 4 1 CPU
- 4 2 メモリ
- 4 3 記憶部
- 4 4 入出力装置
- 4 9 記憶媒体
- 5 0 情報処理プログラム
- 1 0 0 情報処理システム

【 図面 】

【 図 1 】



【 図 2 】



10

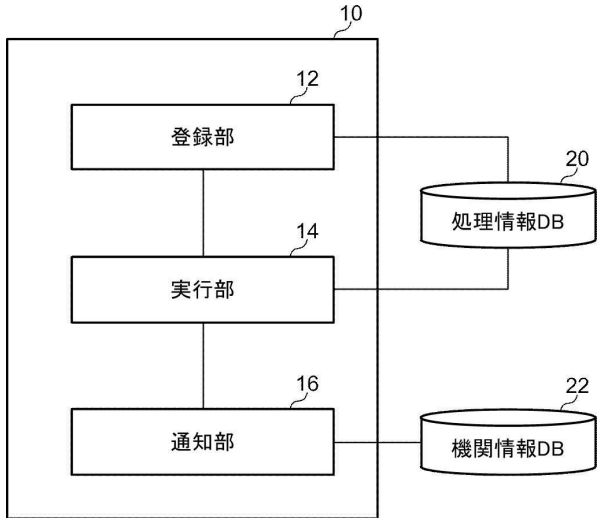
20

30

40

50

【図3】



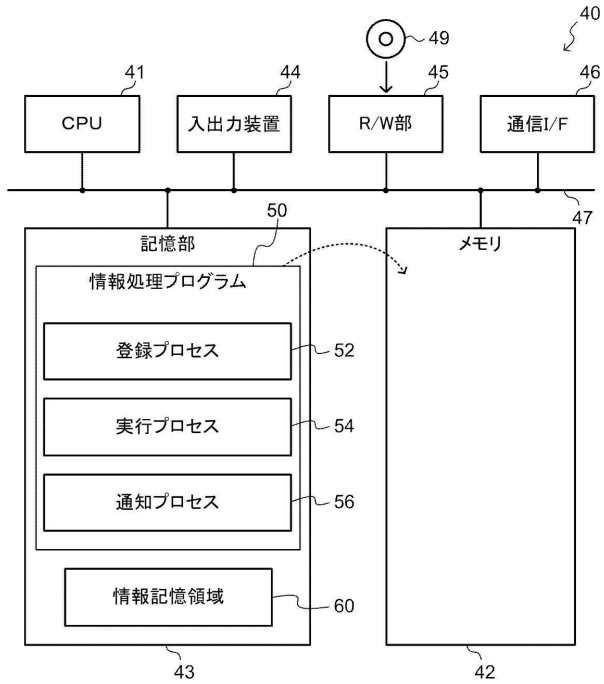
【図4】

証明書番号	A01001	21g6e94...	登録	A01	2019/03/10 15:30	-	...
	A01001	21g6e94...	照会	Z01	2019/03/20 13:00	真	
	...						

【図5】

機関ID	A01	AAA	発行元	xxx.xxx.xxx.xx	A01001, A01002,
	Z01	ZZZ	提出先	xxx.xxx.xxx.xx		
	...					

【図6】



10

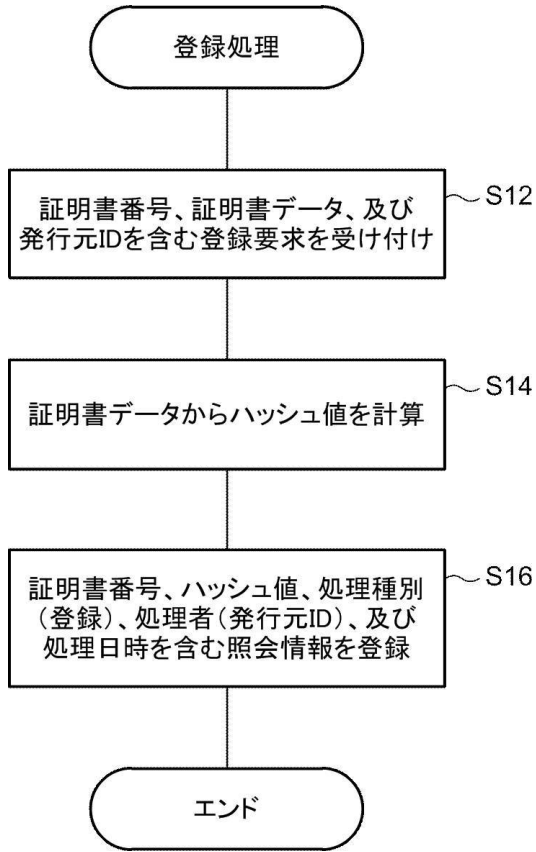
20

30

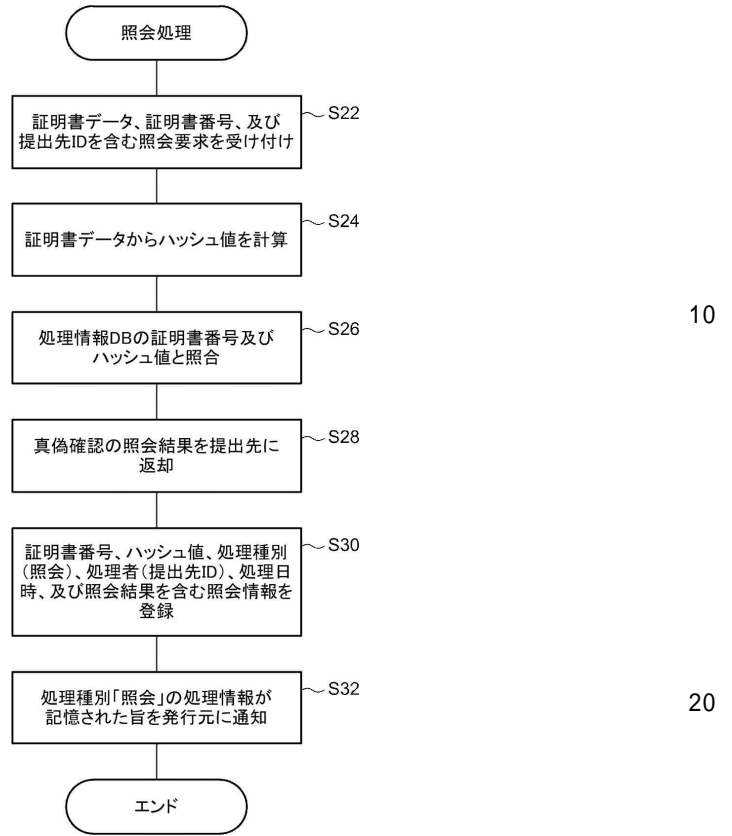
40

50

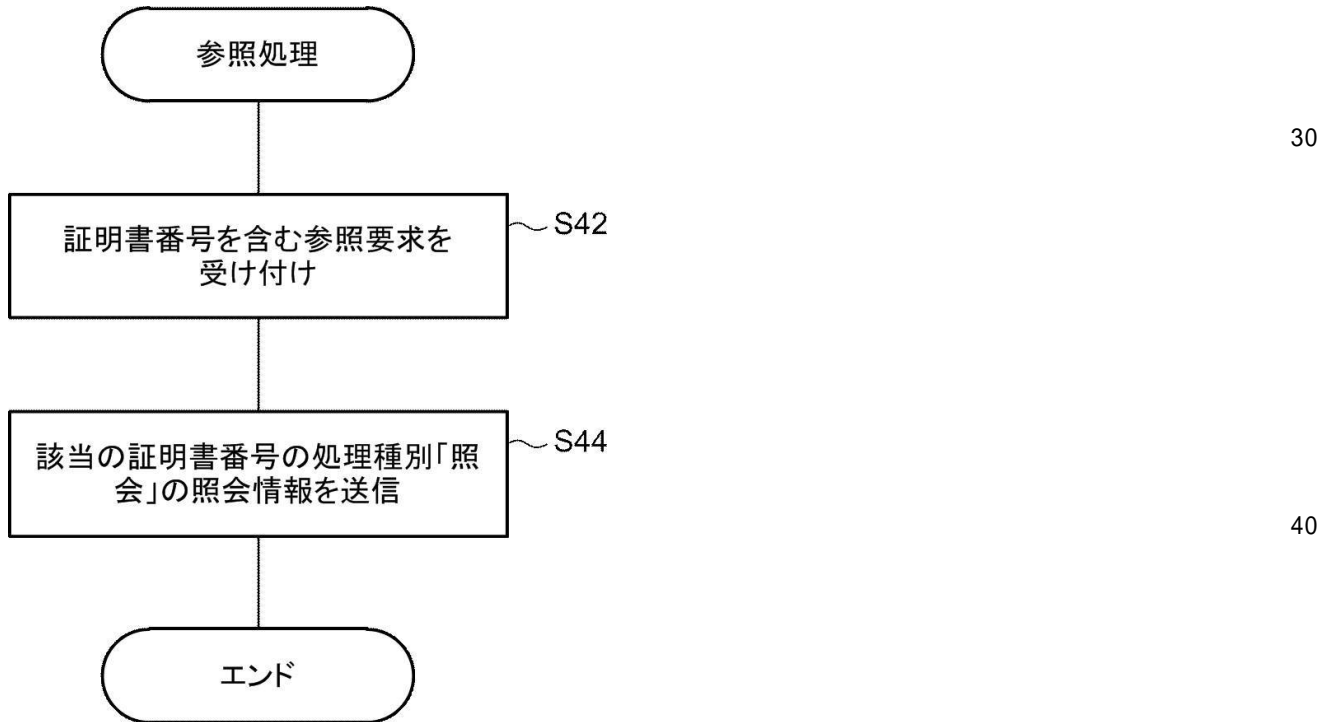
【 図 7 】



【 図 8 】



【 図 9 】



フロントページの続き

- (56)参考文献 特表2004-526235(JP,A)
特開2008-301463(JP,A)
国際公開第2017/136879(WO,A1)
- (58)調査した分野 (Int.Cl., DB名)
- | | |
|------|---------------|
| G06Q | 10/00 - 99/00 |
| G09C | 1/00 - 5/00 |
| H04K | 1/00 - 3/00 |
| H04L | 9/00 - 9/40 |