

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2020年10月8日(08.10.2020)



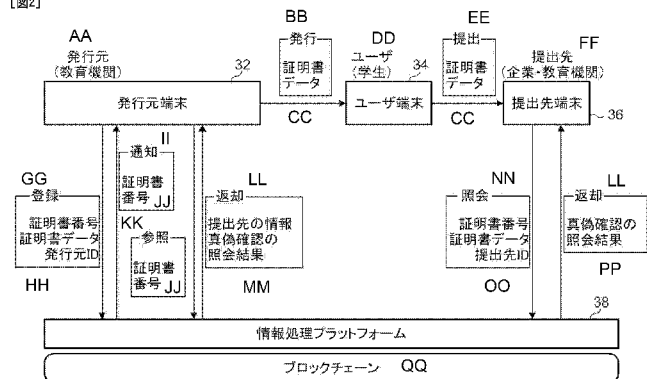
(10) 国際公開番号
WO 2020/202326 A1

- (51) 国際特許分類: *G06Q 50/10* (2012.01) *H04L 9/32* (2006.01) 川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP).
- (21) 国際出願番号: PCT/JP2019/014209 (74) 代理人: 中島 淳, 外 (NAKAJIMA, Jun et al.); 〒160022 東京都新宿区新宿4丁目3番17号 H K 新宿ビル7階 太陽国際特許事務所 Tokyo (JP).
- (22) 国際出願日: 2019年3月29日(29.03.2019)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人: 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 Kanagawa (JP).
- (72) 発明者: 永井 功一 (NAGAI, Koichi); 〒2118588 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内 Kanagawa (JP). 島田 昌紘 (SHIMADA, Masahiro); 〒2118588 神奈
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,

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

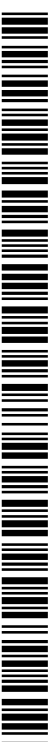
(54) 発明の名称: 情報処理プログラム、装置、及び方法

[図2]



- 32 Issuer terminal
- 34 User terminal
- 36 Recipient terminal
- 38 Information processing platform
- AA Issuer (Educational organization)
- BB Issuance
- CC Certificate data
- DD User (Student)
- EE Submission
- FF Recipient (Business corporation, educational organization)
- GG Registration
- HH Certificate no., certificate data, issuer ID
- II Notification
- JJ Certificate no.
- KK Reference
- LL Return
- MM Recipient information, inquiry result of authenticity confirmation
- NN Inquiry
- OO Certificate no., certificate data, recipient ID
- PP Inquiry result of authenticity confirmation
- QQ Blockchain

(57) Abstract: The purpose of the present invention is for an issuer which has issued certificate data to acquire information pertaining to a recipient to which the issued certificate data is submitted. When the issuer issues a certificate to a user to whom the certificate is to be issued, digitized certificate data into which the certificate is converted is transmitted from an issuer terminal (32) to a user terminal (34); in addition, the issuer terminal (32) transmits a registration request, and an information processing platform (38) registers processing information relating to the certificate data in a blockchain. A recipient terminal (36) to which the user has submitted the certificate data transmits an inquiry request for confirmation of the authenticity of the certificate data, and the information processing platform (38) stores the inquiry result of authenticity confirmation and recipient information in the blockchain and returns the inquiry result to the recipient, as well as notifies the issuer to the effect that there was an inquiry. The issuer refers to the stored processing information and acquires information pertaining to the recipient to which the certificate data was submitted and the inquiry result of authenticity



WO 2020/202326 A1

NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

- 一 国際調査報告 (条約第21条(3))

confirmation.

(57) 要約：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を目的とする。発行元が対象のユーザに対して証明書を発行すると、電子データ化された証明書データが、発行元端末(32)からユーザ端末(34)へ送信されると共に、発行元端末(32)が登録要求を送信し、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をブロックチェーン上に登録する。ユーザが、証明書データを提出した提出先の提出先端末(36)が証明書データの真偽確認の照会要求を送信し、情報処理プラットフォーム(38)が真偽確認を行った照会結果及び提出先の情報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と共に、発行元に照会があった旨を通知する。発行元は、記憶された処理情報を参照して、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取得する。

明 細 書

発明の名称： 情報処理プログラム、装置、及び方法

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。

[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] 特許文献1：特開2010-278982号公報

特許文献2：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] 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。

[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。

[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。

[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。

[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 32 へ送信する。

- [0021] 以下、情報処理プラットフォーム38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10の機能構成について詳述する。なお、複数の情報処理装置10の構成は同様であるため、1つの情報処理装置10について説明する。
- [0022] 図3に示すように、情報処理装置10は、機能的には、登録部12と、実行部14と、通知部16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10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DB(Database)20及び機関情報DB22が記憶される。
- [0023] 登録部12は、発行元端末32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。登録部12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ID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DB20に記憶する。
- [0024] 図4に、処理情報DB20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。
- [0025] 「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DB20に記憶する場合、すなわち、登録部12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14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。
- [0026] 「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DB20に記憶する場合、すなわち、登録部12により

記憶される処理情報の「処理者」には、登録部12が受け付けた登録要求に含まれる発行元ID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14により記憶される処理情報の「処理者」には、実行部14が受け付けた照会要求に含まれる提出先IDが記憶される。

[0027] 「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。

[0028] 処理情報DB20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。

[0029] 実行部14は、提出先端末36から送信された証明書データ、証明書番号、及び提出先IDを含む照会要求を受け付ける。実行部14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14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DB20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。

[0030] 具体的には、実行部14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DB20に記憶されている場合には、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DB20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DB20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DB20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。

- [0031] 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。
- [0032] 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。
- [0033] 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。
- [0034] 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。
- [0035] 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。
- [0036] 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。

- [0037] 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。
- [0038] 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 へ送信してもよい。この場合、発行元端末 32 からの参照要求は不要となる。
- [0039] 情報処理装置 10 は、例えば図 6 に示すコンピュータ 40 で実現することができる。コンピュータ 40 は、CPU (Central Processing Unit) 41 と、一時記憶領域としてのメモリ 42 と、不揮発性の記憶部 43 とを備える。また、コンピュータ 40 は、入力部、表示部等の入出力装置 44 と、記憶媒体 49 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 45 とを備える。また、コンピュータ 40 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) 46 を備える。CPU 41、メモリ 42、記憶部 43、入出力装置 44、R/W 部 45、及び通信 I/F 46 は、バス 47 を介して互いに接続される。
- [0040] 記憶部 43 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 43 には、コンピュータ 40 を、情報処理装置 10 として機能させるための情報処理プログラム 50 が記憶される。情報処理プログラム 50 は、登録プロセス 52 と、実行プロセス 54 と、通知プロセス 56 とを有する。また、記憶部 43 は、処理情報 DB 20 及び機関情報 DB 22 の各々を構成する情報が

記憶される情報記憶領域60を有する。

[0041] CPU41は、情報処理プログラム50を記憶部43から読み出してメモリ42に展開し、情報処理プログラム50が有するプロセスを順次実行する。CPU41は、登録プロセス52を実行することで、図3に示す登録部12として動作する。また、CPU41は、実行プロセス54を実行することで、図3に示す実行部14として動作する。また、CPU41は、通知プロセス56を実行することで、図3に示す通知部16として動作する。また、CPU41は、情報記憶領域60から情報を読み出して、処理情報DB20及び機関情報DB22の各々をメモリ42に展開する。これにより、情報処理プログラム50を実行したコンピュータ40が、情報処理装置10として機能することになる。なお、プログラムを実行するCPU41はハードウェアである。

[0042] なお、情報処理プログラム50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。

[0043] 次に、本実施形態に係る情報処理装置10の作用について説明する。発行元端末32から登録要求が送信されると、情報処理装置10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36から照会要求が送信されると、情報処理装置10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32から参照要求が送信されると、情報処理装置10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。

[0044] まず、図7に示す登録処理について説明する。

[0045] ステップS12で、登録部12が、発行元端末32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。

[0046] 次に、ステップS14で、登録部12が、上記ステップS12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。

[0047] 次に、ステップS16で、登録部12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S14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DB20に記憶する。そして、登録処理は終了する。

[0048] 次に、図8に示す照会処理について説明する。

[0049] ステップS22で、実行部14が、提出先端末36から送信された証明書データ、証明書番号、及び提出先IDを含む照会要求を受け付ける。

[0050] 次に、ステップS24で、実行部14が、上記ステップS22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。

[0051] 次に、ステップS26で、実行部14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DB20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14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。

[0052] 次に、ステップS28で、実行部14が、照会要求を送信した提出先端末36へ、上記ステップS26で決定した真偽確認の照会結果を返却する。

[0053] ステップS30で、実行部14が、照会要求に含まれる証明書番号及び提出先ID（「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DB20に記憶する。

[0054] 次に、ステップS32で、処理種別「照会」の処理情報が処理情報DB20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。

[0055] 次に、図9に示す参照処理について説明する。

[0056] ステップS42で、通知部16が、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。

[0057] 次に、ステップS44で、通知部16が、処理情報DB20から、上記ステップS42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32へ送信する。そして、参照処理は終了する。

[0058] 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。

[0059] 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できることで、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できることで、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できる。

[0060] 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。

[0061] 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。

[0062] 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。

[0063] 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。

[0064] 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。

[0065] 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。

[0066] 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。

[0067] 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

- [0068] 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

- 3 6 提出先端末
- 3 8 情報処理プラットフォーム
- 4 0 コンピュータ
- 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

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知照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に送信する請求項4に記載の情報処理プログラム。

[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、

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] 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記憶部に記憶する登録部を更に含む請求項7に記載の情報処理装置。

[請求項9] 前記実行部は、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8に記載の情報処理装置。

[請求項10] 前記実行部は、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 8 に記載の情報処理装置。

[請求項11] 前記実行部は、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に送信する請求項 10 に記載の情報処理装置。

[請求項12] 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、前記情報処理装置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 7 ～請求項 11 のいずれか 1 項に記載の情報処理装置。

[請求項13] 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知照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。

[請求項14] 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 13 に記載の情報処理方法。

[請求項15] 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 1

4 に記載の情報処理方法。

[請求項16] 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14に記載の情報処理方法。

[請求項17] 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に送信する請求項16に記載の情報処理方法。

[請求項18] 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13～請求項17のいずれか1項に記載の情報処理方法。

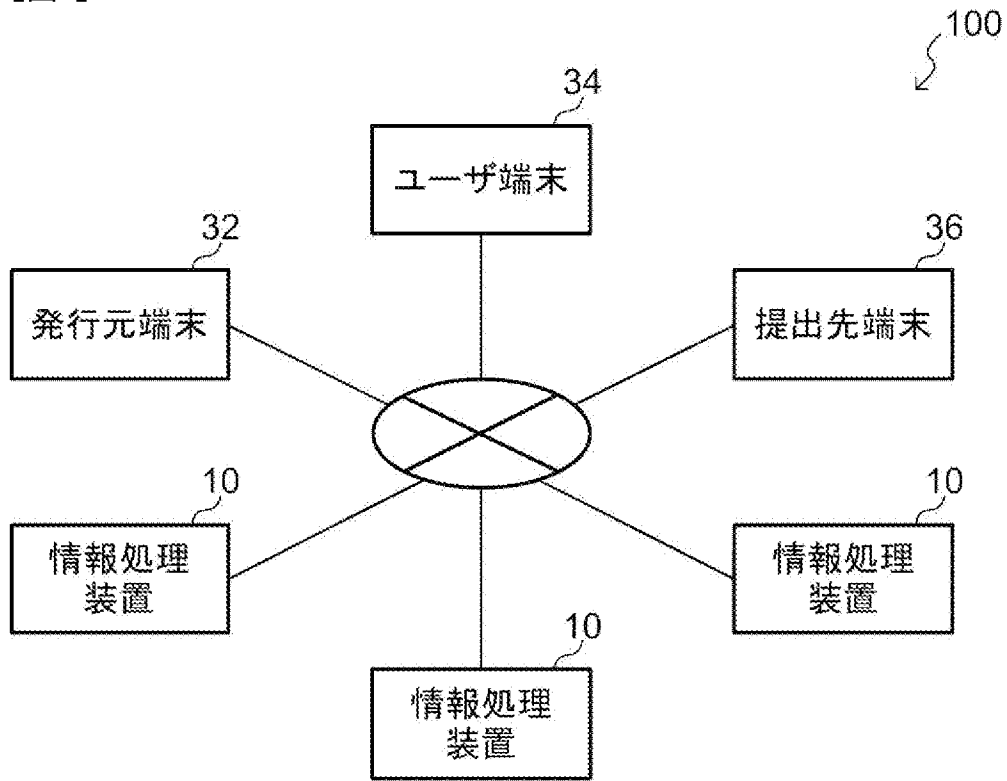
[請求項19] 要求元から書面データについての真偽確認の要求を受け付けた場合に、前記書面データの真偽確認を実行し、前記真偽確認の照会結果を前記要求元に対して送信し、

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、

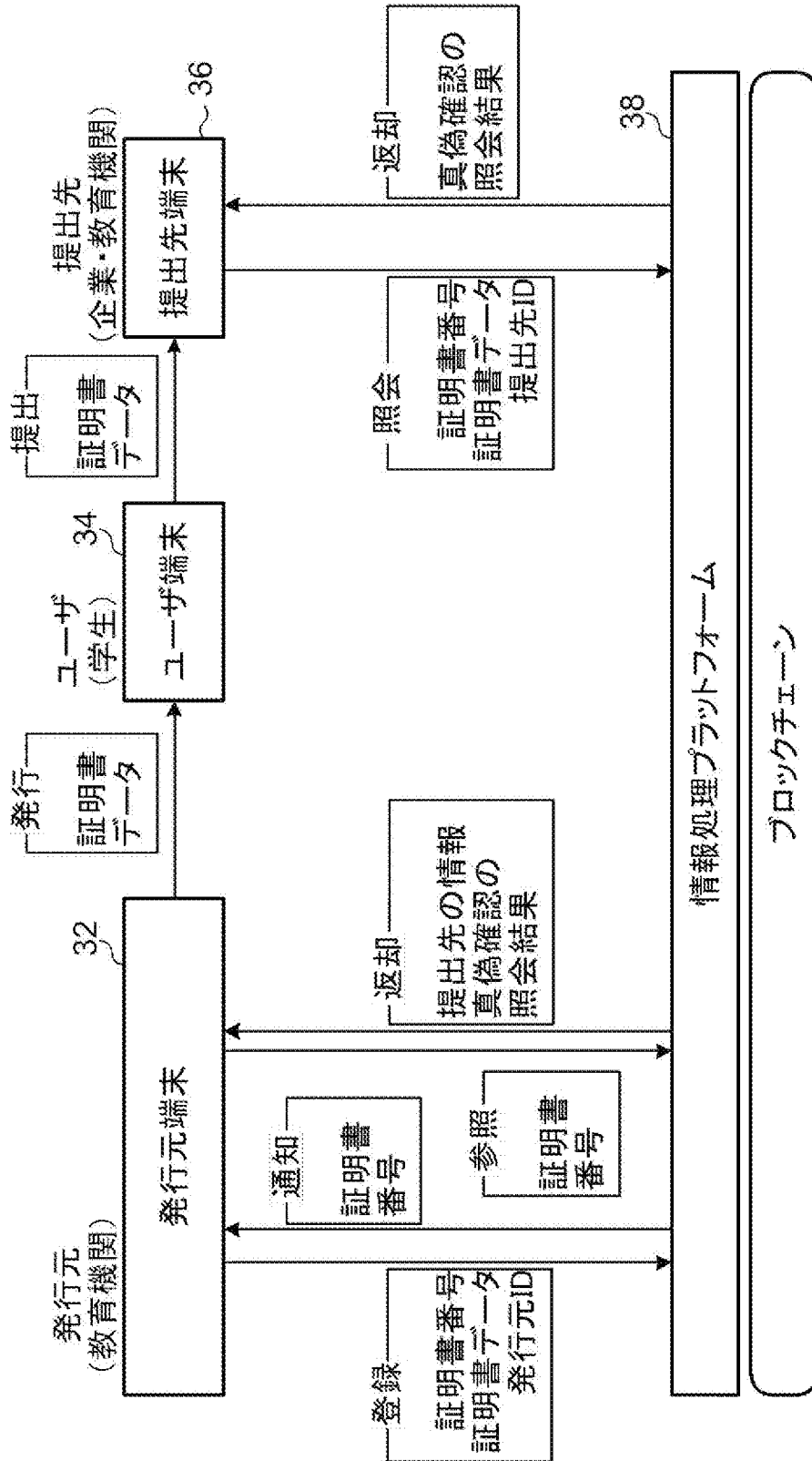
第2記憶部に予め記憶された前記書面データの発行元に対し、前記書面データの識別情報と対応付けられた前記要求元の情報とを通知する

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を記憶した記憶媒体。

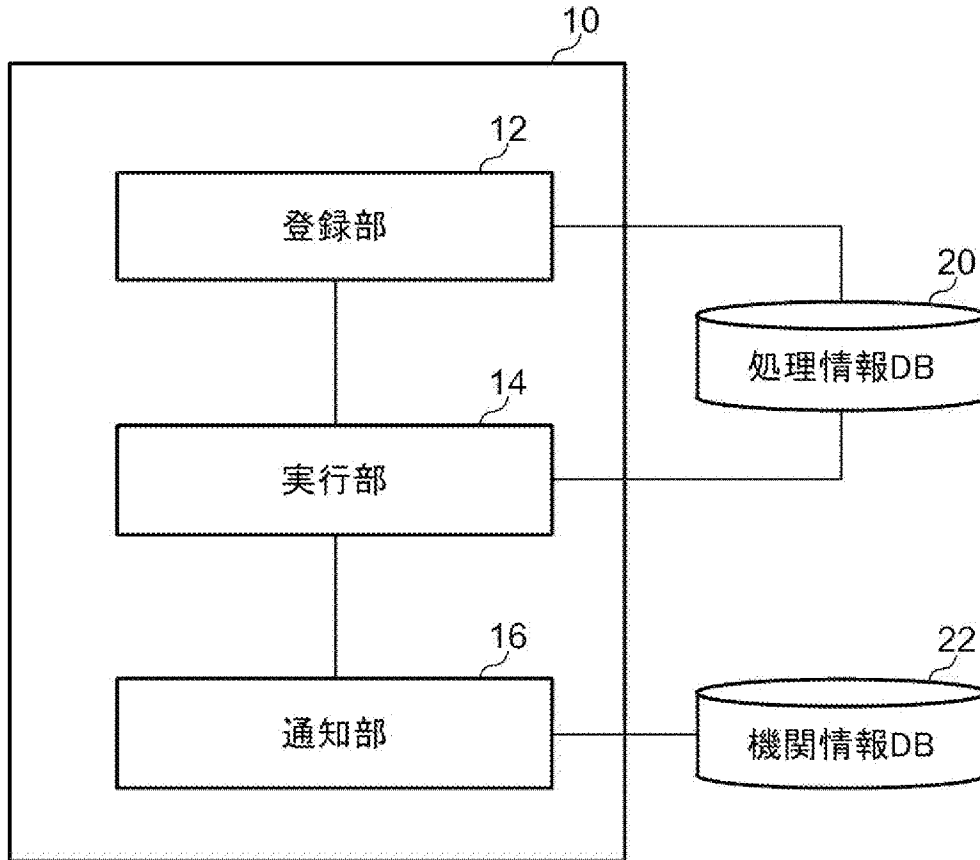
[図1]



[図2]



[図3]



[図4]

20

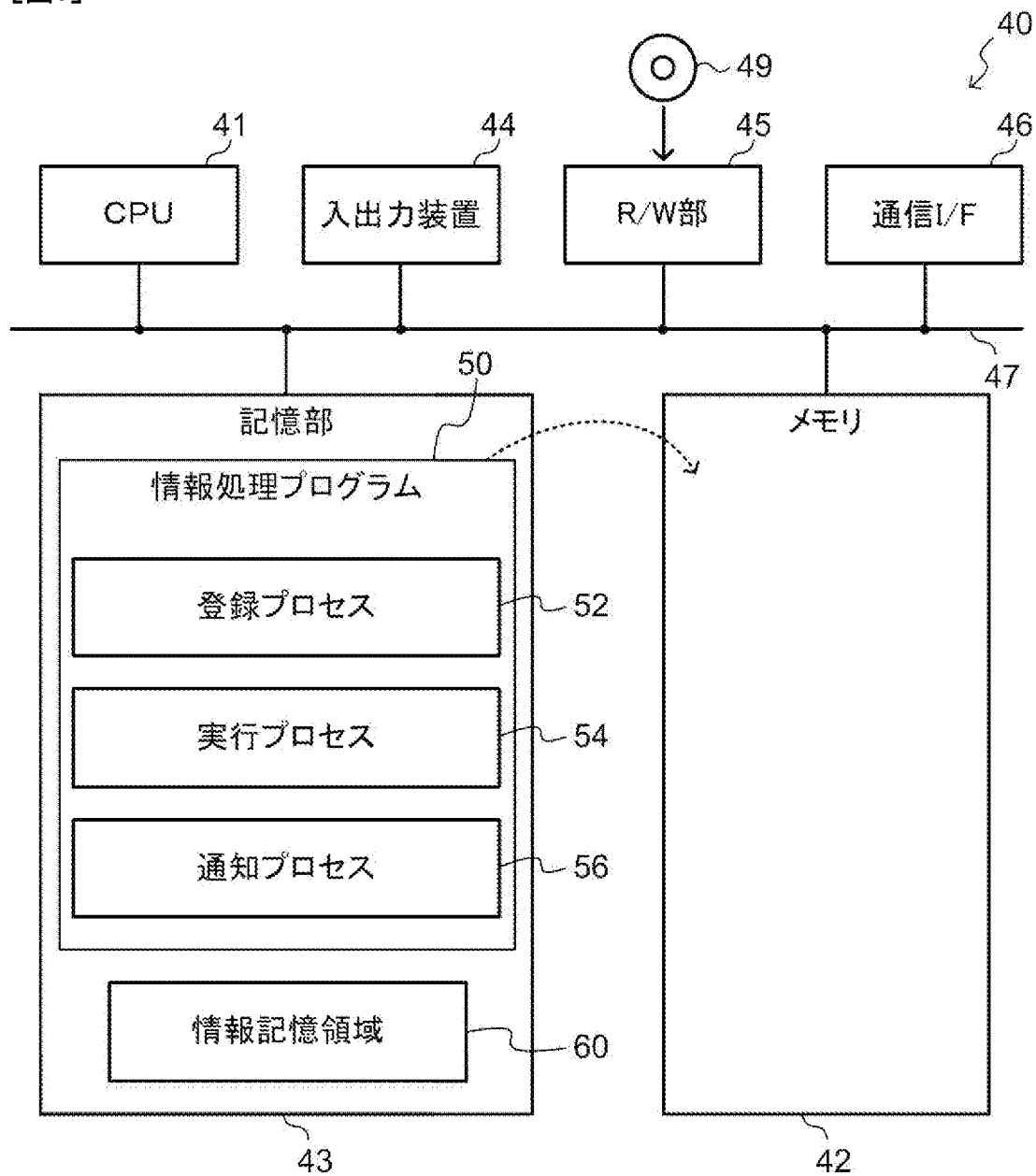
証明書番号	ハッシュ値	処理種別	処理者	処理日時	処理結果	...
A01001	21g6e94...	登録	A01	2019/03/10 15:30	—	
A01001	21g6e94...	照会	Z01	2019/03/20 13:00	真	
...						

[図5]

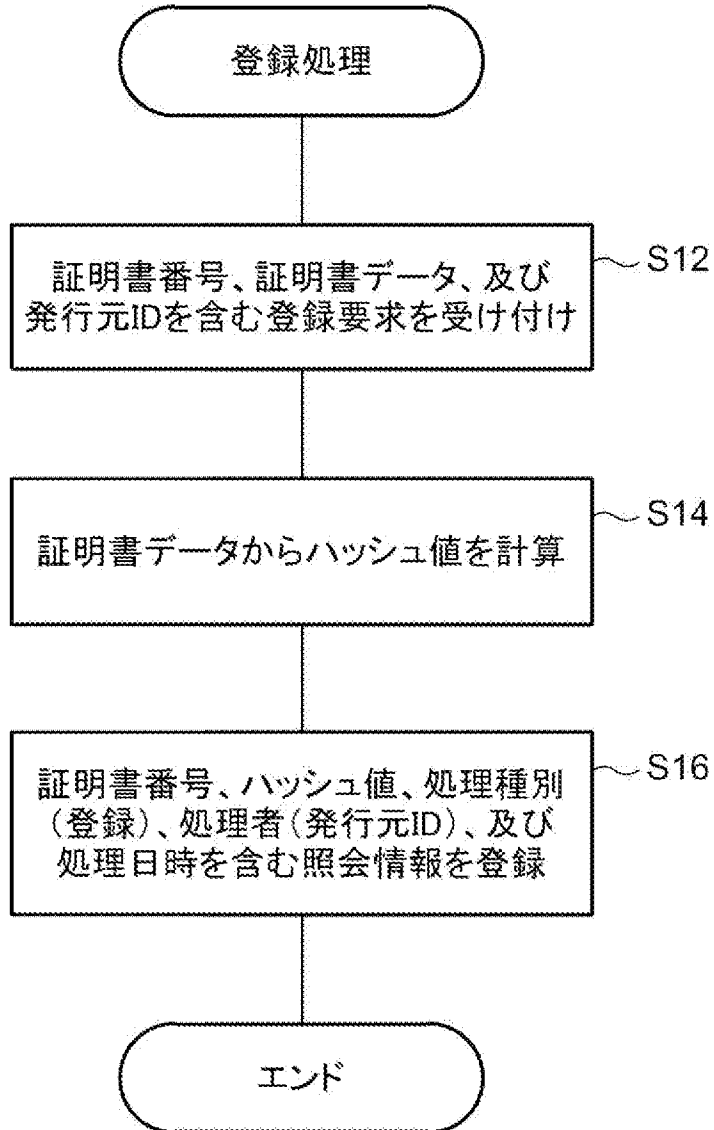
22

機関ID	機関名	区分	アドレス	証明書番号	...
A01	AAA	発行元	xxx.xxx.xx.xx	A01001, A01002, ...	
Z01	ZZZ	提出先	xxx.xxx.xx.xx		
...					

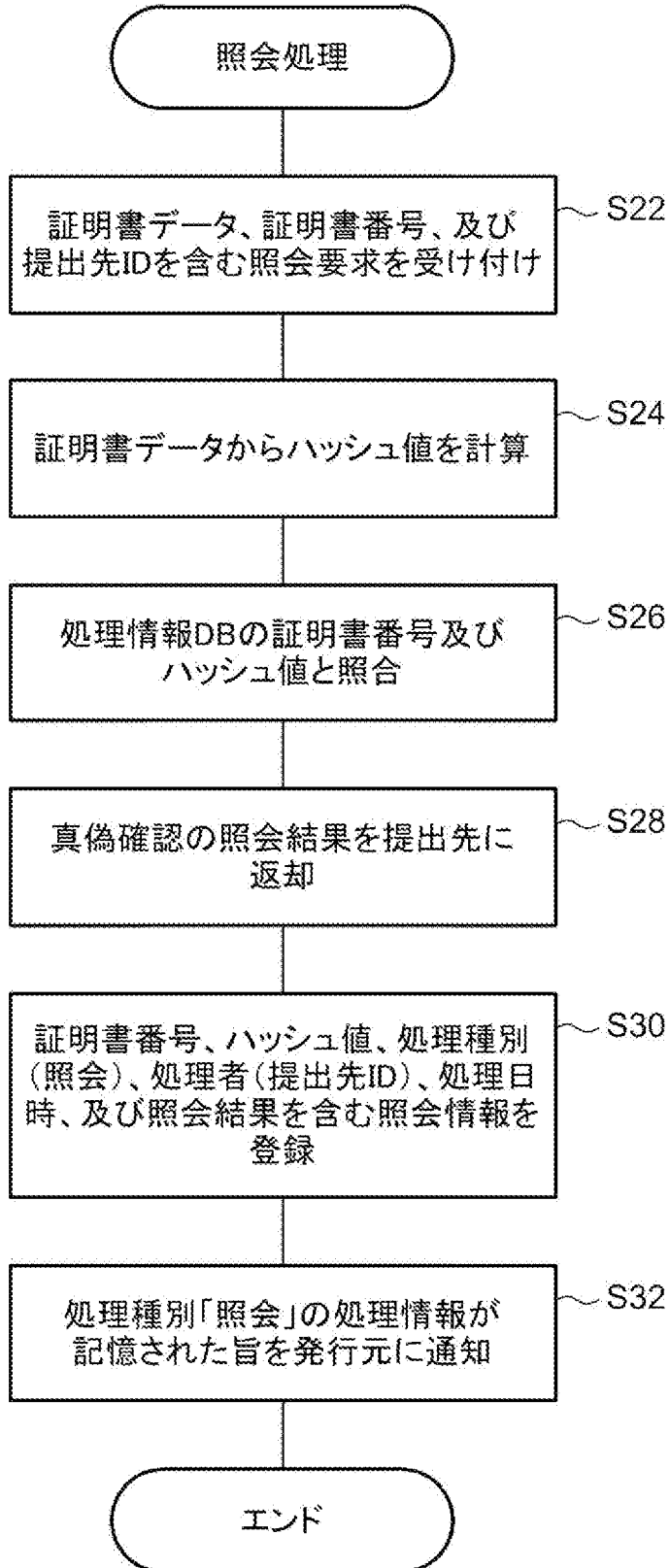
[図6]



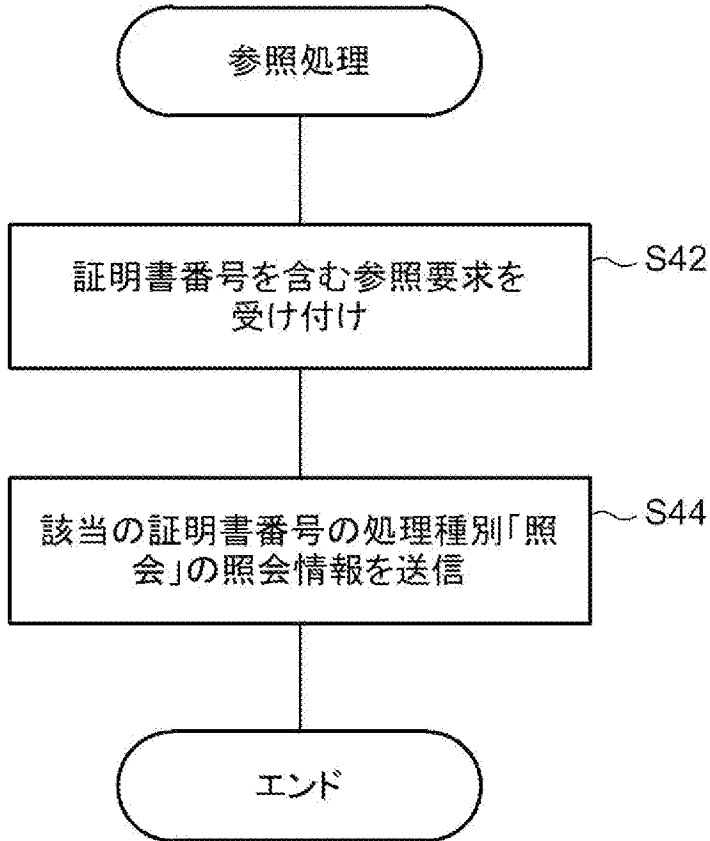
[図7]



[図8]



[図9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2019/014209

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. G06Q50/10 (2012.01) i, H04L9/32 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl. G06Q50/10, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2019

Registered utility model specifications of Japan 1996-2019

Published registered utility model applications of Japan 1994-2019

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2004-526235 A (KWON, Oh, Bong) 26 August 2004, entire text & US 2004/0049463 A1, entire text & WO 2002/061694 A1 & CN 1509457 A	1-19
A	JP 2008-301463 A (SAKAMOTO, Hironori) 11 December 2008, entire text (Family: none)	1-19
A	WO 2017/136879 A1 (MOLONEY, Lindsay) 17 August 2017, entire text & JP 2019-511758 A & US 2019/0044727 A1 & CA 3012870 A1 & KR 10-2018-0110670 A & CN 109075971 A	1-19

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
20.06.2019

Date of mailing of the international search report
02.07.2019

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl. G06Q50/10(2012.01)i, H04L9/32(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl. G06Q50/10, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2019年
日本国実用新案登録公報	1996-2019年
日本国登録実用新案公報	1994-2019年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2004-526235 A (ウォン、オー・ボン) 2004.08.26, 全文 & US 2004/0049463 A1, 全文 & WO 2002/061694 A1 & CN 1509457 A	1-19
A	JP 2008-301463 A (坂本 博則) 2008.12.11, 全文 (ファミリーなし)	1-19

C欄の続きにも文献が列挙されている。

パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」同一パテントファミリー文献

国際調査を完了した日

20.06.2019

国際調査報告の発送日

02.07.2019

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
 郵便番号 100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

松田 岳士

電話番号 03-3581-1101 内線 3562

5 L

3137

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	WO 2017/136879 A1 (MOLONEY, Lindsay) 2017.08.17, 全文 & JP 2019-511758 A & US 2019/0044727 A1 & CA 3012870 A1 & KR 10-2018-0110670 A & CN 109075971 A	1-19