

(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
2024年12月12日(12.12.2024)



(10) 国際公開番号

WO 2024/252559 A1

(51) 国際特許分類:

G06F 21/45 (2013.01) H04L 9/32 (2006.01)
G06F 21/31 (2013.01)

(21) 国際出願番号: PCT/JP2023/021160

(22) 国際出願日: 2023年6月7日(07.06.2023)

(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: 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 Tokyo (JP).

(72) 発明者: 井上 智紀 (INOUE, Tomoki); 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP).

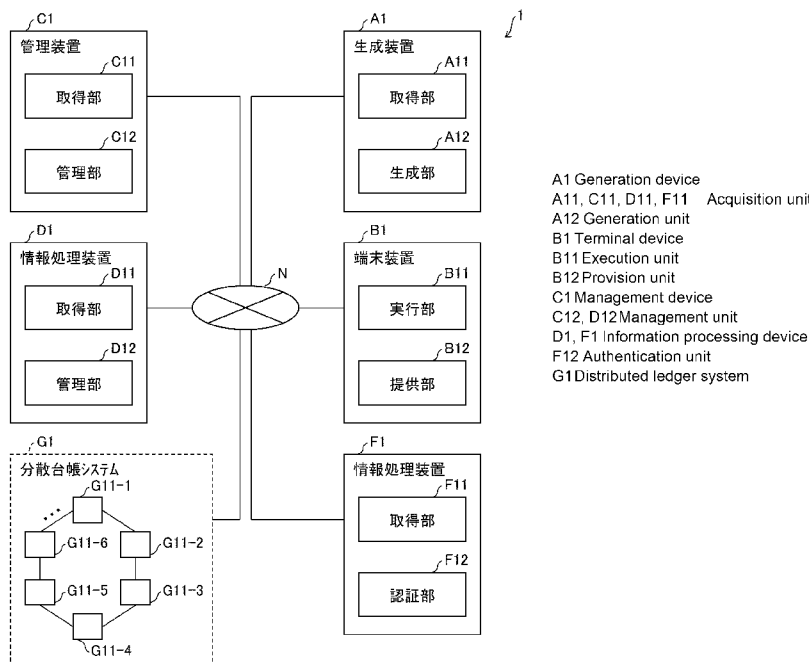
(74) 代理人: 弁理士法人 H A R A K E N Z O W O R L D P A T E N T & T R A D E M A R K (HARAKENZO WORLD PATENT & TRADEMARK); 〒5300041 大阪府大阪市北区天神橋2丁目北2番6号 大和南森町ビル Osaka (JP).

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK,

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

(54) 発明の名称: 管理装置、生成装置、端末装置、情報処理装置、管理方法、生成方法、情報処理方法、及びプログラム

図 1



(57) Abstract: This management device is provided with an acquisition means that acquires an existence confirmation result, which is the result of confirming the existence of a subject, and a management means that associates and manages the existence confirmation result with a non-fungible token.

SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, WS, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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:

— 国際調査報告 (条約第21条(3))

(57) 要約: 管理装置は、対象者の実存性に関する確認結果である実存性確認結果を取得する取得手段と、前記実存性確認結果を非代替トークンと関連付けて管理する管理手段とを備えている。

明 細 書

発明の名称：

管理装置、生成装置、端末装置、情報処理装置、管理方法、生成方法、情報処理方法、及びプログラム

技術分野

[0001] 本発明は、管理装置、生成装置、端末装置、情報処理装置、管理方法、生成方法、情報処理方法、及びプログラムに関する。

背景技術

[0002] 指紋認証、虹彩認証、顔認証など、人間の生体情報を利用して本人認証を行う技術である生体認証技術が知られている（例えば特許文献1）。これらの技術は、個人の生体情報を用いるため、パスワードを使った認証よりも高い認証性を持っている。また、一度登録した生体情報を使って、複数のサービスで利用することができるため、パスワードによる認証よりも利便性が高いとされている。

先行技術文献

特許文献

[0003] 特許文献1：特表2022-544411号公報

発明の概要

発明が解決しようとする課題

[0004] ユーザの生体情報やそれに対応づけられたユーザの個人情報は、本来、ユーザ自身が管理することが望ましい。しかしながら、特許文献1のように、特定企業がプラットフォームを提供するサービスの場合、特定企業がユーザの生体情報や個人情報を掌握し、それらの情報がどのように利用されるのかわからないという課題がある。

[0005] 本発明の一態様は、上記の問題に鑑みてなされたものであり、その目的の一例は、公平かつ透明性の高い認証システムを提供することにある。

課題を解決するための手段

- [0006] 本開示の一側面に係る管理装置は、対象者の実存性に関する確認結果である実存性確認結果を取得する取得手段と、前記実存性確認結果を非代替トークンと関連付けて管理する管理手段とを備えている。
- [0007] 本開示の一側面に係る情報処理装置は、対象者の実存性に関する確認結果である実存性確認結果に関連付けられた非代替トークンを特定する特定情報を取得する取得手段と、前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照した認証処理を実行する認証手段とを備えている。
- [0008] 本開示の一側面に係る管理方法は、管理装置が、対象者の実存性に関する確認結果である実存性確認結果を取得することと、前記実存性確認結果を非代替トークンと関連付けて管理することとを含んでいる。
- [0009] 本開示の一側面に係るプログラムは、コンピュータを管理装置として機能させるプログラムであって、前記プログラムは、前記コンピュータに、対象者の実存性に関する確認結果である実存性確認結果を取得することと、前記実存性確認結果を非代替トークンと関連付けて管理することとを実行させる。

発明の効果

- [0010] 本発明の一態様によれば、公平かつ透明性の高い認証システムを提供することができる。

図面の簡単な説明

- [0011] [図1]例示的实施形態1に係る認証システムの構成を示すブロック図である。
- [図2]例示的实施形態1に係る非代替トークンの例を示す図である。
- [図3]例示的实施形態1に係る情報処理方法の流れを示すフロー図である。
- [図4]例示的实施形態1に係る情報処理方法の流れを示すフロー図である。
- [図5]例示的实施形態1に係る情報処理方法の流れを示すフロー図である。
- [図6]例示的实施形態2に係る生成装置の構成を示すブロック図である。
- [図7]例示的实施形態2に係る生成装置による処理の対象となるデータの例を示す図である。

[図8]例示的实施形態2に係る端末装置の構成を示すブロック図である。

[図9]例示的实施形態2に係る端末装置が実行する実存性確認テストを説明するための図である。

[図10]例示的实施形態2に係る管理装置の構成を示すブロック図である。

[図11]例示的实施形態2に係る非代替データの構成例を示す図である。

[図12]例示的实施形態2に係る非代替データの構成例を示す図である。

[図13]例示的实施形態2に係る分散台帳システムを説明するための図である。

[図14]例示的实施形態2に係る情報処理装置の構成を示すブロック図である。

[図15]例示的实施形態2に係る表示用データの表示例を示す図である。

[図16]例示的实施形態2に係る情報処理装置の構成を示すブロック図である。

[図17]各例示的实施形態に係る各装置として機能するコンピュータの構成を示すブロック図である。

発明を実施するための形態

[0012] 〔例示的实施形態1〕

本発明の第1の例示的实施形態について、図面を参照して詳細に説明する。本例示的实施形態は、後述する例示的实施形態の基本となる形態である。

[0013] <認証システム1の概要>

本例示的实施形態に係る認証システム1は、ユーザの実存性確認結果を非代替データ（NFD: Non Fungible Data）として登録すると共に、当該非代替データをユーザの認証に利用するシステムである。ここで、「非代替データ」との文言は、あるユーザの非代替データを、他のユーザのデータによって代替することができないことを指す。ただし、「非代替データ」との文言は、当該あるユーザの非代替データが、当該あるユーザのデータによって更新されることを排除しない。

[0014] 非代替データの登録は、特定企業に依存しないよう、一例として、非中央

集権的な分散台帳システムを用いて行われる。また、本例示的实施形態に係る認証システム 1 では、そのような分散台帳システムとして、改ざん耐性が高く、かつ、データを外部から閲覧可能なシステムを用いるので、公平かつ透明性の高い認証システムを提供することができる。

[0015] 本例示的实施形態に係るユーザの実存性確認結果には、一例として、ユーザの生体認証結果が含まれる。また、本例示的实施形態に係る生体認証結果には、一例として

- ・顔認証
- ・光彩認証
- ・指紋認証
- ・静脈認証
- ・声や会話による認証

等の各種の技術の少なくとも何れかを利用した認証結果のデータが含まれる。ただし、上述した実存性確認結果の具体例は本例示的实施形態を限定するものではなく、ユーザの実存性に関する確認結果であればどのようなデータを用いてもよい。

[0016] <認証システム 1 の構成>

認証システム 1 の構成について図 1 を参照して説明する。図 1 は、本例示的实施形態に係る認証システム 1 の構成を示すブロック図である。図 1 に示すように、認証システム 1 は、生成装置 A 1、端末装置 B 1、管理装置 C 1、情報処理装置 D 1、情報処理装置 F 1、及び分散台帳システム G 1 を備えている。なお、本例示的实施形態に係る認証システム 1 は、これらすべての装置やシステムを備えることが必須ではなく、これらの装置及びシステムの一部のみを備えるシステムも、本例示的实施形態に係る認証システム 1 の一例である。

[0017] 認証システム 1 における生成装置 A 1、端末装置 B 1、管理装置 C 1、情報処理装置 D 1、情報処理装置 F 1、及び分散台帳システム G 1 の概要を説明すれば以下の通りである。ただし、以下に記載する各処理の全てが各装置

において必須のものというわけではなく、各装置は以下に記載する各処理の一部のみを実行する構成であってもよい。

[0018] (生成装置 A 1 の概要)

- ・ 端末装置 B 1 と連携して、実存性確認テストを実行し、実存性確認結果を生成する。
- ・ 管理装置 C 1 と連携して、非代替データに認証マークを付与したり、当該非代替データを更新したりする。

[0019] (端末装置 B 1 の概要)

- ・ 実存性確認のためのアプリケーションを実行し、管理装置 C 1 による非代替データの発行（ミント）のタイミング、及びその他の任意のタイミングで実存性確認テストを実行する。
- ・ 実存性確認テストに対するユーザからの応答を示す応答情報を取得する。
- ・ 情報処理装置 D 1 が管理する非代替データと関連付いた処理を実行する。
- ・ 実存性確認テストとして、冗長性を有するテスト（複数の認証テストを含むテスト）を実行する。

[0020] (管理装置 C 1 の概要)

- ・ 生成装置 A 1 及び端末装置 B 1 と連携して、非代替データの発行（ミント）と、当該非代替データに含まれる実存性確認結果の更新を行う。
- ・ 非代替データを、分散台帳システム G 1 に登録する。

[0021] (情報処理装置 D 1 の概要)

- ・ 非代替データを特定するための特定情報を取得し、当該非代替データを管理する。
- ・ 上記特定情報を用いて情報処理装置 F 1 にアクセスし、情報処理装置 F 1 からサービスの提供を受ける。

[0022] (情報処理装置 F 1 の概要)

- ・ 非代替データを参照した認証処理を実行し、認証結果に応じて、当該非代替データを管理する情報処理装置 D 1 にサービスを提供する。

[0023] (生成装置 A 1 の構成)

続いて、図 1 を参照して生成装置 A 1 の構成について説明する。生成装置 A 1 は、図 1 に示すように、取得部 A 1 1 と生成部 A 1 2 とを備えている。

[0024] (取得部 A 1 1)

取得部 A 1 1 は、対象者（対象ユーザ）の実存性を確認するための参照情報を取得する。一例として、取得部 A 1 1 は、対象者の実存性確認テストを実施する端末装置 B 1 から、当該実存性確認テストに対する前記対象者による応答情報として、前記参照情報を取得する。

[0025] (生成部 A 1 2)

生成部 A 1 2 は、前記対象者の実存性に関する確認結果である実存性確認結果であって非代替トークン（NFT: Non Fungible Token）への関連付けの対象である実存性確認結果を、前記参照情報を参照して生成する。生成部 A 1 2 によって生成された実存性確認結果は、一例として、前記実存性確認結果を非代替トークンと関連付けて管理する管理装置 C 1 に提供される。

[0026] このように、生成装置 A 1 は、対象者の実存性を確認するための参照情報を取得し、当該参照情報を参照して、対象者の実存性確認結果を生成する。ここで、生成装置 A 1 が生成する実存性確認結果は、非代替トークンに関連付けられ、非代替的に管理される情報である。したがって、上記の構成によれば、公平かつ透明性の高い認証システムを提供することができる。

[0027] (端末装置 B 1 の構成)

続いて、図 1 を参照して端末装置 B 1 の構成について説明する。端末装置 B 1 は、図 1 に示すように、実行部 B 1 1 と提供部 B 1 2 とを備えている。端末装置 B 1 は、一例として対象者（ユーザ）によって操作される端末であるが、これは本例示的实施形態を限定するものではない。

[0028] (実行部 B 1 1)

実行部 B 1 1 は、対象者の実存性確認のための確認テスト（実存性確認テスト）を実行する。一例として、実行部 B 1 1 は、生体の認証に関するテストを含む確認テストを実行する。

[0029] (提供部 B 1 2)

提供部 B 1 2 は、前記対象者の実存性に関する確認結果である実存性確認結果であって、非代替トークンへの関連付けの対象である実存性確認結果を生成する生成装置 A 1 に、前記確認テストに対する前記対象者の応答情報を提供する。

[0030] このように、端末装置 B 1、対象者の実存性確認のための実存性確認テストを実行し、当該実存性確認テストに対する前記対象者の応答情報を、生成装置 A 1 に提供する。また、当該応答情報は、実存性確認結果を生成するために生成装置 A 1 によって参照される。ここで、生成装置 A 1 が生成する実存性確認結果は、非代替トークンに関連付けられ、非代替的に管理される情報である。したがって、上記の構成によれば、公平かつ透明性の高い認証システムを提供することができる。

[0031] (管理装置 C 1)

続いて、図 1 を参照して管理装置 C 1 の構成について説明する。管理装置 C 1 は、図 1 に示すように、取得部 C 1 1 と管理部 C 1 2 とを備えている。

[0032] (取得部 C 1 1)

取得部 C 1 1 は、対象者の実存性に関する確認結果である実存性確認結果を取得する。一例として、取得部 C 1 1 は、生成装置 A 1 が生成した実存性確認結果を取得する。

[0033] (管理部 C 1 2)

管理部 C 1 2 は、前記実存性確認結果を非代替トークンと関連付けて管理する。ここで、管理部 C 1 2 による具体的な管理方法は本例示の実施形態を限定するものではないが、一例として、管理部 C 1 2 による管理には、

- ・ 前記実存性確認結果と非代替トークンとを含む非代替データ、又は
 - ・ 前記実存性確認結果を含む非代替トークンである非代替データ
- を、分散台帳システム G 1 に登録する処理が含まれる。

[0034] 図 2 は、管理部 C 1 2 が管理する対象である上記非代替データ N F D のデータ構造例を示す図である。図 2 に示すように、非代替データ N F D には、非代替トークン N F T を指定するトークン I D、及び当該トークン I D に関

連付けられた実存性確認結果が含まれている。ここで、図2に示す例では、

- ・非代替データNFDに、トークンIDによって指定される非代替トークンNFTと、当該トークンIDに関連付けられた実存性確認結果とが含まれている

と捉えることもできるし、

- ・トークンIDによって指定される非代替トークンNFTに、当該トークンIDに関連付けられた実存性確認結果が含まれており、当該非代替トークンNFTが非代替データNFDを構成している

と捉えることもできる。このように、図2に示す非代替データNFDは、

- ・対象者の実存性に関する確認結果である実存性確認結果を示す情報、及び
- ・前記実存性確認結果を示す情報に関連付けられた非代替トークン

を含んでいると表現することができる。

[0035] また、図2に示すように、非代替データNFDに含まれる実存性確認結果は、一例として、対象者が実存性確認テストに合格したか否か（実存性確認テストが成功したか否か）（図2に示すOK又はNG）、及び、当該実存性確認テストのスコアを含んでいる。ただし当該構成は本例示的实施形態を限定するものではない。

[0036] このように、管理装置C1は、対象者の実存性に関する確認結果である実存性確認結果を取得し、前記実存性確認結果を非代替トークンと関連付けて管理する。したがって、上記の構成によれば、公平かつ透明性の高い認証システムを提供することができる。

[0037] （情報処理装置D1）

続いて、図1を参照して情報処理装置D1の構成について説明する。情報処理装置D1は、図1に示すように、取得部D11と管理部D12とを備えている。情報処理装置D1は、一例として対象者（ユーザ）によって操作される装置であるが、これは本例示的实施形態を限定するものではない。

[0038] （取得部D11）

取得部D11は、対象者の実存性に関する確認結果である実存性確認結果

を示す情報と、前記実存性確認結果を示す情報に関連付けられた非代替トークンとを含む非代替データを特定するための特定情報を取得する。一例として、取得部D 1 1は、上記非代替データを特定するための特定情報として、上記非代替トークンのIDであるトークンIDを取得する。

[0039] (管理部D 1 2)

管理部D 1 2は、前記非代替データを管理する。管理部D 1 2による具体的な処理は本例示的实施形態を限定するものではないが、一例として、管理部D 1 2は、

- ・トークンIDと秘密鍵とを管理する
- ・秘密鍵を用いた暗号化を用いて、非代替トークンのトークンIDや非代替データNFD等を外部の装置に送信する

等の処理が含まれ得る。なお、管理部D 1 2が行う各処理は、いわゆるウォレットが行う処理を含むと捉えることもできるが、これは本例示的实施形態を限定するものではない。

[0040] このように、情報処理装置D 1は、対象者の実存性に関する確認結果である実存性確認結果を示す情報と、前記実存性確認結果を示す情報に関連付けられた非代替トークンとを含む非代替データを特定するための特定情報を取得し、前記非代替データを管理する。したがって、上記の構成によれば、公平かつ透明性の高い認証システムを提供することができる。

[0041] (情報処理装置F 1)

続いて、図1を参照して情報処理装置F 1の構成について説明する。情報処理装置F 1は、図1に示すように、取得部F 1 1と認証部F 1 2とを備えている。

[0042] (取得部F 1 1)

取得部F 1 1は、対象者の実存性に関する確認結果である実存性確認結果に関連付けられた非代替トークンを特定する特定情報を取得する。

[0043] (認証部F 1 2)

認証部F 1 2は、前記実存性確認結果及び前記非代替トークンの少なくとも

も何れかを参照した認証処理を実行する。

[0044] 情報処理装置 F 1 は、一例として、認証部 F 1 2 による認証結果に応じて、前記対象者に対するサービスを選択し、選択したサービスを提供する。ここで、情報処理装置 F 1 が提供するサービスの具体例は本例示的实施形態を限定するものではないが、一例として、ゲーム、金融サービス、ビジネスサポート、情報発信、及び人事サービス等のサービスを挙げることができる。情報処理装置 F 1 は、認証部 F 1 2 による認証結果に応じて、これらのサービスに関連するデータ等を、ユーザが所有する端末（端末装置 B 1 や情報処理装置 D 1 等）に提供する。

[0045] このように、情報処理装置 F 1 は、対象者の実存性に関する確認結果である実存性確認結果に関連付けられた非代替トークンを特定する特定情報を取得し、前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照した認証処理を実行する。したがって、上記の構成によれば、公平かつ透明性の高い認証システムを提供することができる。

[0046] （分散台帳システム G 1）

続いて、図 1 を参照して分散台帳システム G 1 の構成について説明する。分散台帳システム G 1 は、図 1 に示すように、複数のノード G 1 1-1、G 1 1-2、・・・を備えて構成される。

[0047] ここで、複数のノード G 1 1-1、G 1 1-2、・・・各々は、分散台帳の一例としてのブロックチェーンを保管している。また、当該ブロックチェーンが備える複数のブロックの少なくとも何れかには、上述した管理装置 C 1 等が管理する非代替データ N F D が、トランザクションデータとして格納されている。ブロックチェーンは、改ざん耐性が高く、かつ、データを外部から閲覧可能なシステムを用いるので、分散台帳システム G 1 を用いることにより、公平かつ透明性の高い認証システム 1 を提供することができる。

[0048] （認証システム 1 が備える各装置による処理の流れ）

続いて、図 3～図 4 を参照して、認証システム 1 が備える各装置による処理の流れについて説明する。

[0049] (生成装置 A 1 による処理の流れ)

図 3 に示す S A 1 は、生成装置 A 1 による処理の流れを示すフロー図である。図 3 に示すように、生成装置 A 1 は、対象者の実存性に関する確認結果である実存性確認結果を取得し（ステップ S A 1 1）、前記実存性確認結果を非代替トークンと関連付けて管理する（S A 1 2）。

[0050] (端末装置 B 1 による処理の流れ)

図 3 に示す S B 1 は、端末装置 B 1 による処理の流れを示すフロー図である。図 3 に示すように、端末装置 B 1 は、対象者の実存性確認のための確認テストを実行し（ステップ S B 1 1）、前記対象者の実存性に関する確認結果である実存性確認結果であって、非代替トークンへの関連付けの対象である実存性確認結果を生成する生成装置に、前記確認テストに対する前記対象者の応答情報を提供する（ステップ S B 1 2）。

[0051] (管理装置 C 1 による処理の流れ)

図 3 に示す S C 1 は、管理装置 C 1 による処理の流れを示すフロー図である。図 3 に示すように、管理装置 C 1 は、対象者の実存性に関する確認結果である実存性確認結果を取得し（ステップ S C 1 1）、前記実存性確認結果を非代替トークンと関連付けて管理する（ステップ S C 1 2）。

[0052] (情報処理装置 D 1 による処理の流れ)

図 4 に示す S D 1 は、情報処理装置 D 1 による処理の流れを示すフロー図である。図 4 に示すように、情報処理装置 D 1 は、対象者の実存性に関する確認結果である実存性確認結果を示す情報と、前記実存性確認結果を示す情報に関連付けられた非代替トークンとを含む非代替データを特定するための特定情報を取得し（ステップ S D 1 1）、前記非代替データを管理する（ステップ S D 1 2）。

[0053] (情報処理装置 F 1 による処理の流れ)

図 4 に示す S F 1 は、情報処理装置 F 1 による処理の流れを示すフロー図である。図 4 に示すように、情報処理装置 F 1 は、対象者の実存性に関する確認結果である実存性確認結果に関連付けられた非代替トークンを特定する

特定情報を取得し（ステップS F 1 1）、前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照した認証処理を実行する（ステップS F 1 2）。

[0054] （認証システム1全体による処理の流れ）

図5は、認証システム1全体による処理の流れを示すフロー図である。

[0055] （ステップS B 0 1～S B 1 2）

まず、端末装置B 1は、実存性確認実行指示を取得する（ステップS B 0 1）。続いて、端末装置B 1は、実存性確認テストを実行する（ステップS B 1 1）。そして、端末装置B 1は、実存性確認テストに対する対象者の応答情報を、生成装置A 1に提供する（ステップS B 1 2）。

[0056] （ステップS A 1 1～S A 1 2）

続いて、生成装置A 1は、端末装置B 1から上記応答情報を取得する（ステップS A 1 1）。そして、生成装置A 1は、当該応答情報を参照して、実存性確認結果を生成する（ステップS A 1 2）。

[0057] （ステップS C 1 1～S C 1 2）

続いて、管理装置C 1は、生成装置A 1から実存性確認結果を取得する（ステップS C 1 1）。そして、管理装置C 1は、実存性確認結果を非代替トークンと関連付けて管理する（ステップS C 1 2）。

[0058] （ステップS D 1 1～S D 1 2）

続いて、情報処理装置D 1は、管理装置C 1から、上記非代替トークンを特定するための特定情報を取得する（ステップS D 1 1）。そして、情報処理装置D 1は、当該特定情報によって特定される非代替トークンを含む非代替データを管理する（ステップS D 1 2）。

[0059] （ステップS F 1 1～S F 1 2）

続いて、情報処理装置F 1は、情報処理装置D 1から、上記非代替トークンを特定するための特定情報を取得する（ステップS F 1 1）。そして、情報処理装置F 1は、当該特定情報によって特定される非代替トークンを含む非代替データを参照した認証処理を実行する（ステップS F 1 2）。

[0060] 以上のような処理を行う認証システム 1 によれば、非代替トークンと当該非代替トークンに関連付けられた実存性確認結果とを含む非代替データを管理し、当該非代替データを参照した認証処理を実行するので、公平かつ透明性の高い認証システムを提供することができる。

[0061] 〔例示的实施形態 2〕

本発明の第 2 の例示的实施形態について、図面を参照して詳細に説明する。なお、例示的实施形態 1 にて説明した構成要素と同じ機能を有する構成要素については、同じ符号を付し、その説明を適宜省略する。

[0062] 本例示的实施形態に係る認証システムは、例示的实施形態 1 において説明したように、生成装置 A 1、端末装置 B 1、管理装置 C 1、情報処理装置 D 1、情報処理装置 F 1、及び分散台帳システム G 1 を備えている。以下、本例示的实施形態に係る認証システムが備える各装置の具体的構成について説明する。

[0063] (生成装置 A 1)

図 6 は、生成装置 A 1 の構成を示すブロック図である。図 6 に示すように、生成装置 A 1 は、制御部 A 1 0、記憶部 A 2 0、及び通信部 A 3 0 を備えている。

[0064] 通信部 A 3 0 は、生成装置 A 1 の外部の装置と通信を行う。一例として通信部 A 3 0 は、端末装置 B 1、管理装置 C 1、及び本例示的实施形態に係る認証システムが備える他の装置の少なくとも何れかの装置と通信を行う。また、通信部 A 3 0 は、制御部 A 1 0 から供給されたデータを上記外部の装置に送信したり、上記外部の装置から受信したデータを制御部 A 1 0 に供給したりする。

[0065] (記憶部 A 2 0)

記憶部 A 2 0 には、制御部 A 1 0 によって参照される各種の情報、及び制御部 A 1 0 によって導出された各種の情報が格納されている。一例として、記憶部 A 2 0 には、

- ・ 端末装置 B 1 によって実行された第 1 の実存性確認テストに対する対象者

の応答内容を示す第 1 の応答情報 R 1 1

- ・ 端末装置 B 1 によって実行された第 2 の実存性確認テストに対する対象者の応答内容を示す第 2 の応答情報 R 1 2

- ・ 上記第 1 の応答情報 R 1 1, 及び上記第 2 の応答情報 R 1 2 の少なくとも何れかを参照して、生成部 A 1 2 が生成（導出）した当該対象者に関する実存性確認結果 E C R

- ・ 上記第 1 の実存性確認テスト及び上記第 2 の実存性確認テストの少なくとも何れかが実行された日時を示す時刻情報 T 1、

- ・ 上記第 1 の実存性確認テスト及び上記第 2 の実存性確認テストの少なくとも何れかが実行された位置（場所）を示す位置情報 P 1、

- ・ 上記対象者が保有する非代替トークンのトークン I D

が格納されている。

[0066] (制御部 A 1 0)

制御部 A 1 0 は、図 6 に示すように、取得部 A 1 1、生成部 A 1 2、及び提供部 A 1 3 を備えている。

[0067] (取得部 A 1 1)

取得部 A 1 1 は、対象者の実存性を確認するための参照情報を取得する。一例として、取得部 A 1 1 は、上記参照情報として、端末装置 B 1 から、当該端末装置 B 1 が実行した第 1 の実存性確認テストに対する対象者の応答内容を示す第 1 の応答情報 R 1 1 を取得する。また、取得部 A 1 1 は、更なる参照情報として、端末装置 B 1 から、当該端末装置 B 1 が実行した第 2 の実存性確認テストに対する対象者の応答内容を示す第 2 の応答情報 R 1 2 を取得してもよい。なお、端末装置 B 1 が実行する実存性確認テストの具体例については後述する。

[0068] また、取得部 A 1 1 は、端末装置 B 1 から、

- ・ 上記第 1 の実存性確認結果及び上記第 2 の実存性確認結果の少なくとも何れかが実行された日時を示す時刻情報 T 1、

- ・ 上記第 1 の実存性確認テスト及び上記第 2 の実存性確認テストの少なくと

も何れかが実行された位置（場所）を示す位置情報 P I

を取得し、取得した時刻情報 T I 及び位置情報 P I を、対応する実存性確認テストに関連付けて記憶部 A 2 0 に格納してもよい。

[0069] また、取得部 A 1 1 は、上記対象者が保有する非代替トークンのトークン I D を、一例として、管理装置 C 1、情報処理装置 D 1、及び端末装置 B 1 の少なくとも何れかから取得し、取得したトークン I D を記憶部 A 2 0 に格納してもよい。ここで言うトークン I D とは、具体的には、例えば、E R C 7 2 1 のコントラクトアドレスと発行番号の組み合わせから導出される一意な値のことを言う。

[0070] （生成部 A 1 2）

生成部 A 1 2 は、前記対象者の実存性に関する確認結果である実存性確認結果であって非代替トークンへの関連付けの対象である実存性確認結果を、前記参照情報を参照して生成（導出）する。一例として、生成部 A 1 2 は、取得部 A 1 1 が取得した第 1 の応答情報 R I 1 を参照して対象者に関する実存性確認結果を生成する。また、生成部 A 1 2 は、取得部 A 1 1 が取得した第 2 の応答情報 R I 2 を更に参照して上記実存性確認結果を生成してもよい。生成部 A 1 2 が生成した実存性確認結果 E C R は、一例として記憶部 A 2 0 に格納される。

[0071] 生成部 A 1 2 による実存性確認結果の導出処理の具体例は本例示的实施形態を限定するものではないが、一例として、生成部 A 1 2 は、第 1 の応答情報 R I 1 に含まれる対象者の応答内容と所定の応答内容との合致度に応じた実存性確認結果を導出してもよい。

[0072] 一例として、生成部 A 1 2 は、第 1 の応答情報 R I 1 に含まれる対象者の応答内容と所定の応答内容との合致度が所定の閾値以上であった場合に、第 1 の実存性確認テストに合格した旨の実存性確認結果を生成してもよい。また、生成部 A 1 2 は、当該第 1 の応答情報 R I 1 に含まれる対象者の応答内容と所定の応答内容との合致度を示すスコアを、前記実存性確認結果に含める構成としてもよい。

[0073] 同様に、生成部 A 1 2 は、第 2 の応答情報 R 1 2 に含まれる対象者の応答内容と所定の応答内容との合致度が所定の閾値以上であった場合に、第 2 の実存性確認テストに合格した旨の実存性確認結果を生成してもよい。また、生成部 A 1 2 は、当該第 2 の応答情報 R 1 2 に含まれる対象者の応答内容と所定の応答内容との合致度を示すスコアを、前記実存性確認結果に含める構成としてもよい。

[0074] (提供部 A 1 3)

提供部 A 1 3 は、前記実存性確認結果 E C R を非代替トークンと関連付けて管理する装置である管理装置 C 1 に、前記実存性確認結果 E C R を提供する。一例として、提供部 A 1 3 は、実存性確認結果 E C R を、当該実存性確認結果 E C R と関連付けられる非代替トークンのトークン I D と共に管理装置 C 1 に提供する。また、提供部 A 1 3 は、前記非代替トークンへの関連付けの対象である時刻情報を前記管理装置に提供してもよい。一例として、提供部 A 1 3 は、上述した時刻情報 T 1 を、前記非代替トークンへの関連付けの対象である時刻情報として前記管理装置 C 1 に提供してもよい。

[0075] また、提供部 A 1 3 は、前記非代替トークンへの関連付けの対象である位置情報を前記管理装置に提供してもよい。一例として、提供部 A 1 3 は、上述した位置情報 P 1 を、前記非代替トークンへの関連付けの対象である位置情報として前記管理装置 C 1 に提供してもよい。

[0076] また、提供部 A 1 3 は、

- ・ 上述した第 1 の実存性確認テストを実行するために参照される第 1 のテスト情報 T E 1、
- ・ 上述した第 2 の実存性確認テストを実行するために参照される第 2 のテスト情報 T E 2

を端末装置 B 1 に提供する構成としてもよい。第 1 のテスト情報 T E 1 及び第 2 のテスト情報 T E 2 は、一例として端末装置 B 1 によって第 1 の実存性確認テスト及び第 2 の実存性確認テストを実行するために参照される。

[0077] (提供部 A 1 3 が提供するデータの例)

図 7 は、提供部 A 1 3 が管理装置 C 1 に提供するデータの例を示している。図 7 に示すように、提供部 A 1 3 が提供するデータには、一例として、

- ・対象者の氏名 (User Name)
- ・対象者のメールアドレス (Email Address)
- ・対象者の生年月日 (Birthdate)
- ・対象者の居住国 (Country)
- ・対象者の収入 (Income)
- ・実存性確認テストを実行した日時を示す時刻情報 T I (Time stamp)
- ・実存性確認テストを実行した位置 (場所) を示す位置情報 P I (Position)

- ・実存性確認結果 E C R

が互いに関連付けられて含まれている。また、図 7 に示すように、実存性確認結果 E C R には、一例として、

- ・対象者が実存性確認テストに合格したか否か (実存性確認テストの一例としての生体認証に成功 (Success) したか失敗 (Failure) したか) (Biometric Result) 、及び
- ・実存性確認テストのスコアの一例としての生体認証スコア (Biometric Score)

が含まれている。

[0078] このように、生成装置 A 1 は、対象者の実存性を確認するための参照情報を取得し、当該参照情報を参照して、対象者の実存性確認結果を生成する。ここで、生成装置 A 1 が生成する実存性確認結果は、非代替トークンに関連付けられ、非代替的に管理される情報である。したがって、上記の構成によれば、公平かつ透明性の高い認証システムを提供することができる。

[0079] (端末装置 B 1)

図 8 は、端末装置 B 1 の構成を示すブロック図である。図 8 に示すように、端末装置 B 1 は、制御部 B 1 0、記憶部 B 2 0、通信部 B 3 0、及び入出力部 B 4 0 を備えている。

[0080] 通信部B30は、端末装置B1の外部の装置と通信を行う。一例として通信部B30は、生成装置A1、管理装置C1、及び本例示的实施形態に係る認証システムが備える他の装置の少なくとも何れかの装置と通信を行う。また、通信部B30は、制御部B10から供給されたデータを上記外部の装置に送信したり、上記外部の装置から受信したデータを制御部B10に供給したりする。

[0081] 入出力部B40は、一例として、キーボード、マウス、ディスプレイ、プリンタ、タッチパネル、カメラ、スピーカ等の少なくとも何れかの入出力デバイスを備えている。また、入出力部B40は、これらの入出力デバイスを備える代わりに、例えばUSB (Universal Serial Bus) などのインタフェースを備えてもよい。そして、当該インタフェースにこれらの少なくとも何れかの入出力デバイスが接続される構成としてもよい。

[0082] 入出力部B40は、上記少なくとも何れかの入出力デバイスから端末装置B1に対する各種の情報の入力を受け付ける。また、入出力部B40は、制御部B10の制御の下、当該少なくとも何れかの入出力デバイスに各種の情報を出力する。

[0083] (記憶部B20)

記憶部B20には、制御部B10によって参照される各種の情報、及び制御部B10によって導出された各種の情報が格納されている。一例として、記憶部B20には、

- ・生成装置A1から提供された第1のテスト情報TE1、及び第2のテスト情報TE2
- ・第1のテスト情報を参照して実行された第1の実存性確認テストに対する対象者の応答内容を示す第1の応答情報R11、
- ・第2のテスト情報を参照して実行された第2の実存性確認テストに対する対象者の応答内容を示す第2の応答情報R12、
- ・上記第1の実存性確認テスト及び上記第2の実存性確認テストの少なくとも何れかが実行された日時を示す時刻情報T1、

- ・ 上記第 1 の実存性確認テスト及び上記第 2 の実存性確認テストの少なくとも何れかが実行された位置（場所）を示す位置情報 P 1、
 - ・ 上記対象者が保有する非代替トークンのトークン I D
- が格納されている。

[0084] （制御部 B 1 0）

制御部 B 1 0 は、図 8 に示すように、取得部 B 1 3、実行部 B 1 1、及び提供部 B 1 2 を備えている。

[0085] （取得部 B 1 3）

取得部 B 1 3 は、

- ・ 第 1 の実存性確認テストを実行するために参照する第 1 のテスト情報 T E 1
- ・ 第 2 の実存性確認テストを実行するために参照する第 2 のテスト情報 T E 2

を、一例として生成装置 A 1 から取得し、取得した第 1 のテスト情報 T E 1 及び第 2 のテスト情報 T E 2 を記憶部 B 2 0 に格納する。

[0086] また、取得部 B 1 3 は、一例として管理装置 C 1 から、

- ・ 第 1 のテスト情報 T E 1 及び第 2 のテスト情報 T E 2 の少なくとも何れかを参照して生成装置 A 1 が生成する実存性確認結果が関連付けられる非代替トークンを特定する特定情報（トークン I D）を取得し、取得したトークン I D を記憶部 B 2 0 に格納してもよい。

[0087] （実行部 B 1 1、提供部 B 1 2）

実行部 B 1 1 は、対象者の実存性確認のための確認テストを実行する。一例として、実行部 B 1 1 は、第 1 のテスト情報 T E 1 を参照して第 1 の実存性確認テストを実行する。また、実行部 B 1 1 は、第 2 のテスト情報 T E 2 を参照して第 2 の実存性確認テストを更に実行してもよい。

[0088] 提供部 B 1 2 は、前記対象者の実存性に関する確認結果である実存性確認結果であって、非代替トークンへの関連付けの対象である実存性確認結果を生成する生成装置 A 1 に、前記確認テストに対する前記対象者の応答情報を

提供する。一例として、提供部B 1 2は、上述した第1の応答情報R 1 1、及び上記第2の応答情報R 1 2を生成装置A 1に提供する。また、提供部B 1 2は、上記実存性確認結果と共に、上述した時刻情報T 1及び位置情報P 1の少なくとも何れかを生成装置A 1に提供してもよい。提供部B 1 2は、上記実存性確認結果に関連付けて、上述したトークンIDを生成装置A 1に提供してもよい。当該トークンIDは、生成装置A 1において上記実存性確認結果に関連づけられる。

[0089] なお、端末装置B 1による当該端末装置の位置情報P 1の特定処理は本例示的实施形態を限定するものではないが、一例として、当該端末装置B 1が備える測位装置により特定された位置情報、当該端末装置B 1による近距離無線通信により特定された位置情報、及び当該端末装置B 1が備えるカメラによる撮像画像の解析によって特定された位置情報等を用いることができる。

[0090] また、実行部B 1 1が実行する実存性確認テストの具体例は本例示的实施形態を限定するものではないが、一例として、

- ・顔認証
- ・光彩認証
- ・指紋認証
- ・静脈認証
- ・声や会話による認証

等の各種の生体認証技術の少なくとも何れかを利用した実存性確認テストを挙げることができる。

[0091] 図9は、実行部B 1 1が実行する第1の実存性確認テストの具体例を説明するための図である。

[0092] 図9に示す例は、顔の向きを対象者の認証に用いるための第1の実存性確認テストを示している。図9に示す例では、4通りの確認テスト（チャレンジと呼ぶこともある）（画像A、画像B、画像C、音声）が種類毎に分類され、同じ種類のチャレンジが関連付けられている。その種類毎に、識別子で

ある「コード」が付与され、また、名称である「種別」が付与されている。例えば、コードが「FD02」であり、かつ、種別が「左向き」である種類の4つのチャレンジのうち、画像Aは左向きの顔の鏡像反転を表すアイコン画像である。画像Bは「左を向いてください」という文字列を表す画像である。画像Cは、左を向くように指示する矢印アイコン画像である。音声は、左を向くように指示する音声データである。

[0093] 図9に示す例では、取得部B13は、第1のテスト情報TE1として、上述した画像A、画像B、画像C、音声を示すデータを取得する。また、図9に示す例では、実行部B11は、上述した画像A、画像B、画像C、音声の少なくとも何れかを用いた第1の実存性確認テストを実行する。

[0094] 一例として、実行部B11は、何れかの種別の画像Aを、入出力部B40が備えるディスプレイを介して対象者に提示し、当該画像Aに対する対象者の応答内容を、第1の応答情報R11として取得する。第1の応答情報R11には、画像Aが提示されたタイミングで入出力部B40が備えるカメラによって撮像された対象者の顔を含む撮像データが含まれ得る。当該撮像データを含む第1の応答情報R11は、提供部B12により、一例として生成装置A1に提供される。

[0095] 他の例として、実行部B11は、第1のテスト情報TE1に含まれる音声データを、入出力部B40が備えるスピーカを介して対象者に提示し、当該画像Aに対する対象者の応答内容を、第1の応答情報R11として取得する。第1の応答情報R11には、当該音声提示されたタイミングで入出力部B40が備えるカメラによって撮像された対象者の顔を含む撮像データが含まれ得る。当該撮像データを含む第1の応答情報R11は、提供部B12により、一例として生成装置A1に提供される。

[0096] 生成装置A1の生成部A12は、所定の顔認証アルゴリズムを用いて、第1の応答情報R11に含まれる上記撮像データが示す対象者の顔が、予め登録された顔と同じであるか否かを判定する。また、上記撮像データが示す対象者の顔の向きが、所定の向きであるか否かを判定する。そして生成部A1

2は、上記判定結果に応じた実存性確認結果を生成する。当該生成部A 1 2は、

- ・上記撮像データが示す対象者の顔と予め登録された顔との合致度、及び、

- ・上記撮像データが示す対象者の顔の向きと、所定の向きとの合致度

を示すスコアを算出し、当該スコアを実存性確認結果に含めてもよい。実存性確認結果の一例は、図7を参照して説明した通りである。

[0097] 実行部B 1 1が上述したような第1の実存性確認テストを行う場合、当該実行部B 1 1は、第2の実存性確認テストとして、光彩認証、指紋認証、静脈認証、及び声や会話による認証の少なくとも何れかの認証テストを実行してもよい。

[0098] 一例として、実行部B 1 1は、入出力部B 4 0を介して、対象者に自身の光彩を撮像するよう促してもよい。そして、入出力部B 4 0が備えるカメラによって撮像された対象者の光彩を含む撮像データを、第2の応答情報R 1 2として取得してもよい。対象者の光彩の撮像データを含む第2の応答情報R 1 2は、提供部B 1 2によって生成装置A 1に提供される。

[0099] そして、生成装置A 1の生成部A 1 2は、第2の応答情報R 1 2に含まれる上記撮像データが示す光彩の画像が、所定の構造を有しているか否かを判定し、判定結果に応じた実存性確認結果を生成する。当該生成部A 1 2は、上記撮像データが示す対象者の光彩の構造と、予め登録されている対象者の光彩の構造との合致度を示すスコアを算出し、当該スコアを実存性確認結果に含めてもよい。

[0100] なお、上述の実存性確認テストを実行部B 1 1が実行するタイミングは本例示的实施形態を限定するものではないが、一例として、実行部B 1 1は、実存性確認結果と非代替トークンとを関連付けて管理する管理装置C 1からの指示に基づき、前記実存性確認テストを実施する構成としてもよい。

[0101] 一例として、管理装置C 1は、非代替トークンを発行（ミント）するタイミングで端末装置B 1に、上記実存性確認テストを実行するよう指示を行い、実行部B 1 1は当該タイミングで上記実存性確認テストを実行してもよい。

。

[0102] (管理装置C1)

図10は、管理装置C1の構成を示すブロック図である。図10に示すように、管理装置C1は、制御部C10、記憶部C20、及び通信部C30を備えている。

[0103] 通信部C30は、端末装置B1の外部の装置と通信を行う。一例として通信部C30は、生成装置A1、端末装置B1、情報処理装置D1、及び本例示の実施形態に係る認証システムが備える分散台帳システムG1等の他の装置やシステムの少なくとも何れかと通信を行う。また、通信部C30は、制御部C10から供給されたデータを上記外部の装置に送信したり、上記外部の装置から受信したデータを制御部C10に供給したりする。

[0104] (記憶部C20)

記憶部C20には、制御部C10によって参照される各種の情報、及び制御部C10によって導出された各種の情報が格納されている。一例として、記憶部C20には、

- ・ 1又は複数の実存性確認結果ECR
- ・ 各実存性確認結果ECRに関連付けられた時刻情報TI
- ・ 各実存性確認結果ECRに関連付けられた位置情報PI
- ・ 上記1又は複数の実存性確認結果ECRに関連付けられた非代替トークンのトークンID
- ・ 上記非代替トークンに関連付けられた表示用データDD

が格納されている。ここで、図10に示すように、管理装置C1においては、複数の実存性確認結果ECRを1つのトークンIDに関連付けてもよい。一例として、

- ・ 時刻情報TI1及び位置情報PI1に関連付けられた実存性確認結果ECR1と、
- ・ 時刻情報TI2及び位置情報PI2に関連付けられた実存性確認結果ECR2と

を同一のトークンIDに関連付けてもよい。これら複数の実存性確認結果は、一例として、同一の対象者による、異なった日時及び異なった場所での実存性確認テストの結果を示す。

[0105] あるいは、管理装置C1においては、1つの実存性確認結果ECRに、複数の時刻情報と、複数の位置情報とを関連付けてもよい。このような構成とすることで、管理装置C1が管理する非代替データNFDは、対象者の位置の経時的な変化を証明するためのデータとして用いることができる。

[0106] （制御部C10）

制御部C10は、図10に示すように、取得部C11、管理部C12、及び提供部C13を備えている。

[0107] （取得部C11）

取得部C11は、対象者の実存性に関する確認結果である実存性確認結果を取得する。一例として、取得部C11は、生成装置A1が生成した実存性確認結果ECRを取得する。また、取得部C11は、前記実存性確認結果に関連付けられた時刻情報T1及び位置情報P1の少なくとも何れかを取得してもよい。これらの時刻情報T1及び位置情報P1は、前記実存性確認結果を導出するための実存性確認テストが実行された日時及び位置（場所）を示す情報である。

[0108] （管理部C12）

管理部C12は、前記実存性確認結果を非代替トークンと関連付けて管理する。一例として、取得部C11は、前記実存性確認結果ECRを、非代替トークンのトークンIDと関連付けて管理する。また、管理部C12は、前記実存性確認結果と、取得部C11が取得した上記時刻情報T1及び上記位置情報P1の少なくとも何れかを関連付けて管理してもよい。また、管理部C12は、上記非代替トークンを発行（ミント）する発行部としても機能する。一例として、管理部C12は、新たな非代替トークンを特定する特定情報として新たなトークンIDを決定してもよい。

[0109] また、取得部C11は、より新しい時刻情報に関連付けられた更新用の実

存性確認結果を取得し、管理部C 1 2は、前記更新用の実存性確認結果を用いて、前記非代替トークンに関連付けられた実存性確認結果を更新する構成としてもよい。

[0110] 管理部C 1 2が管理するデータは、一例として、トランザクションデータとしてブロックチェーンに登録される。このため、管理部C 1 2は当該データを非代替的に管理するものであると表現することもできる。

[0111] また、管理部C 1 2は、上記非代替トークンに関連付けられた表示用データD Dを生成する表示用データ生成部としても機能する。換言すれば、管理部C 1 3は、前記非代替トークンの表示用データであって、前記実存性確認結果に応じた表示オブジェクトを含む表示用データを生成する。

[0112] なお、管理部C 1 2は、上記非代替トークンを、譲渡不可能に設定されたトークン（Soul Bound Token）として管理してもよい。一例として、管理部C 1 2は、提供部C 1 3を介して、上記非代替トークンを、譲渡不可能な設定でトランザクションデータとしてブロックチェーンに登録する構成としてもよい。

[0113] （提供部C 1 3）

提供部C 1 3は、実存性確認結果E C Rと、当該実存性確認結果に関連付けられた非代替トークンN F Tとを含むデータ（非代替データN F Dとも呼ぶ）を、トランザクションデータとして、分散台帳システムG 1が管理するブロックチェーンに登録する。ここで、当該非代替データには、上述した時刻情報T I及び位置情報P Iが含まれていてもよい。

[0114] また、提供部C 1 3は、上記非代替トークンのトークンI Dを、本例示の実施形態に係る認証システムが備える他の装置（例えば、情報処理装置D 1、生成装置A 1、及び端末装置B 1等）に提供してもよい。

[0115] また、提供部C 1 3は、任意のタイミングにて、端末装置B 1又は生成装置A 1に対して、実存性確認テストを実行するよう指示してもよい。一例として、提供部C 1 3は、管理部C 1 2が、上記非代替トークンをミントするタイミングで、端末装置B 1又は生成装置A 1に対して、実存性確認テスト

を実行するよう指示してもよい。また、提供部C 1 3は、管理部C 1 2が、上記非代替トークンを更新するタイミングで、端末装置B 1又は生成装置A 1に対して、実存性確認テストを実行するよう指示してもよい。

[0116] (非代替データの構成例)

図1 1は、管理部C 1 2によって管理され、提供部C 1 3によってトークンIDが提供される非代替データの構成例1を示している。当該構成例では、

- ・ 非代替トークンのトークンID (NFT ID)
- ・ 時刻情報TI (Time Stamp)
- ・ 実存性確認結果ECR
- ・ 位置情報PI (Position)

が互いに関連付けられている。また、図1 1に示すように、実存性確認結果ECRには、

- ・ 対象者が実存性確認テストに合格したか否か（実存性確認テストの一例としての生体認証に成功 (Success) したか失敗 (Failure) したか） (Biometric Result)、及び
- ・ 実存性確認テストのスコアの一例としての生体認証スコア (Biometric Score)

が含まれている。

[0117] また、図1 1に示す例は、

- ・ 非代替データNFDに、トークンIDによって指定される非代替トークンNFTと、当該トークンIDに関連付けられた実存性確認結果とが含まれている

と捉えることができる。換言すれば、図1 1に示す非代替データは、

- ・ 対象者の実存性に関する確認結果である実存性確認結果を示す情報、及び
 - ・ 前記実存性確認結果を示す情報に関連付けられた非代替トークン
- を含んでいると表現することができる。

[0118] 図1 2は、管理部C 1 2によって管理され、提供部C 1 3によってトークン

ンIDが提供される非代替データの構成例2を示している。当該構成例では、非代替トークンNFTに、

- ・トークンID、及び
- ・ロケーション情報LI

が含まれており、

上記ロケーション情報LIによって指定される格納先に、格納用データBIとして

- ・時刻情報TI (Time Stamp)
- ・実存性確認結果ECR
- ・位置情報PI (Position)

が互いに関連付けられて格納されている。ここで、当該格納先は、分散的な格納先であってもよい。当該例では、非代替トークンNFTが、ブロックチェーンのトランザクションデータとして登録され（オンチェーンとして登録され）、上記ロケーション情報LIによって指定される格納先は、一例として上記ブロックチェーン以外（オフチェーン）の格納先を示している。

[0119] このように、図12に示す非代替データNFDは、

- ・対象者の実存性に関する確認結果である実存性確認結果を示す情報をオフチェーン情報として含み、
- ・前記実存性確認結果を示す情報に関連付けられた非代替トークンをオンチェーン情報として含んでいると表現することができる。

[0120] なお、図11及び図12に示すように、本例示的实施形態に係る非代替データNFDは

- ・対象者の氏名 (User Name)
- ・対象者のメールアドレス (Email Address)
- ・対象者の生年月日 (Birthdate)
- ・対象者の居住国 (Country)
- ・対象者の収入 (Income)

を含んでいない。このような構成とすれば、トークンIDを参照しても、当

該トークンIDに関連付けられた対象者に関する上記の情報が判明することはない。したがって、上記の構成によれば、分散台帳システムを用いて認証用データをオープンに管理しつつ、対象者のプライバシーを秘匿することができるという利点がある。

[0121] また、上述のように、管理部C12は、同一のトークンIDに関連付ける実存性確認結果（及び時刻情報及び位置情報）を逐次更新可能に構成されている。このため、管理部C12は、対象者の認証用データとして、最新の实存性確認結果を含む非代替データを管理することができる。このような構成は、対象者の実存性確認結果を動的NFT（Dynamic NFT）として管理するものであると表現することもできるが、これは本例示的实施形態を限定するものではない。

[0122] （分散台帳システムG1）

続いて、本例示的实施形態に係る分散台帳システムG1について説明する。本例示的实施形態に係る分散台帳システムG1は、例示的实施形態1と同様に、複数のノードG11-1、G11-2、・・・を備えて構成される。

[0123] ここで、複数のノードG11-1、G11-2、・・・各々は、分散台帳の一例としてのブロックチェーンを保管している。また、当該ブロックチェーンが備える複数のブロックの少なくとも何れかには、上述した管理装置C1等が管理する非代替データNFDが、トランザクションデータとして格納されている。

[0124] 図13は、トランザクションデータを含むブロックが各ノードによって登録されたブロックチェーンBCを示す図である。図13に示すように、ブロックチェーンBCには、複数のブロック（・・・、Block1、Block2、Block3）が含まれており、各ブロックは、ブロックヘッダ、及びトランザクションデータを含んでいる。図13に示すように、ブロックヘッダには、一例として、前ブロックのブロックヘッダのハッシュ値、当該ブロックのトランザクションデータのハッシュ値、及びナンス値が含まれている。各ブロックが直前のブロックのハッシュ値を含むことにより、ブロック

間の順序関係が規定される。

[0125] 分散台帳システム G 1 のノードは、ブロックチェーン B C にブロックを登録するために一例として以下の処理を行う。

- ・ブロックに追加すべきトランザクションデータを特定し、特定したトランザクションデータのハッシュ値を算出する。
- ・前ブロックのハッシュ値を算出する
- ・所定条件を満たすナンス値を算出する。

[0126] そして、当該ノードは、トランザクションデータのハッシュ値、前ブロックのハッシュ値、及びナンス値を含むブロックヘッダを生成し、生成したブロックヘッダとトランザクションデータとを含むブロックを生成する。当該ノードは、生成したブロックを、分散台帳システム G 1 の他のノードにブロードキャストする。そして、他のノードによって、当該ブロックが所定のコンセンサスアルゴリズムに基づき承認された場合に、当該ノードは、当該ブロックをブロックチェーン B C に登録する。

[0127] 図 1 3 は、第 1 の対象者の実存性確認結果に関連付けられた非代替トークンのトークン I D (N F T 1) と、第 2 の対象者の実存性確認結果に関連付けられた非代替トークンのトークン I D (N F T 2) とを含むトランザクションデータを含むブロック (B l o c k 3) を示している。当該ブロックには、トークン I D に加えて、当該トークン I D に関連付けられた実存性確認結果 E C R、時刻情報 T I、及び位置情報 P I を更に含む構成としてもよい。

[0128] なお、分散台帳システム G 1 の各ノードには、本例示的实施形態に係る認証システムが備える各装置の各機能を実行するためのプログラム（各機能に対応するスマートコントラクトを実行するプログラム）をデプロイしてもよい。また、本例示的实施形態に係る認証システムは、当該プログラムにより各機能を実現する構成とすることができるが、これは本例示的实施形態を限定するものではない。

[0129] 分散台帳システム G 1 が管理するブロックチェーンは、改ざん耐性が高く

、かつ、データを外部から閲覧可能なシステムを用いるので、分散台帳システムG1を用いることにより、公平かつ透明性の高い認証システムを提供することができる。

[0130] (情報処理装置D1)

図14は、情報処理装置D1の構成を示すブロック図である。図14に示すように、情報処理装置D1は、制御部D10、記憶部D20、通信部D30、及び入出力部D40を備えている。情報処理装置D1は、一例として対象者（ユーザ）によって操作される装置であるが、これは本例示の実施形態を限定するものではない。

[0131] 通信部D30は、情報処理装置D1の外部の装置と通信を行う。一例として通信部D30は、端末装置B1、管理装置C1、及び本例示の実施形態に係る認証システムが備える他の装置（例えば情報処理装置F1）の少なくとも何れかの装置と通信を行う。また、通信部D30は、制御部D10から供給されたデータを上記外部の装置に送信したり、上記外部の装置から受信したデータを制御部D10に供給したりする。

[0132] 入出力部D40は、一例として、キーボード、マウス、ディスプレイ、プリンタ、タッチパネル、カメラ、スピーカ等の少なくとも何れかの入出力デバイスを備えている。また、入出力部D40は、これらの入出力デバイスを備える代わりに、例えばUSB（Universal Serial Bus）などのインタフェースを備えてもよい。そして、当該インタフェースにこれらの少なくとも何れかの入出力デバイスが接続される構成としてもよい。

[0133] 入出力部D40は、上記少なくとも何れかの入出力デバイスから情報処理装置D1に対する各種の情報の入力を受け付ける。また、入出力部D40は、制御部D10の制御の下、当該少なくとも何れかの入出力デバイスに各種の情報を出力する。

[0134] (記憶部D20)

記憶部D20には、制御部D10によって参照される各種の情報、及び制御部D10によって導出された各種の情報が格納されている。一例として、

記憶部D20には、

- ・トークンIDを暗号化するための鍵情報K1
- ・トークンID
- ・トークンIDに関連付けられた表示用データDD
- ・後述する情報処理装置F1から提供されたサービスデータ群DG

等が格納されている。

[0135] (制御部D10)

制御部D10は、図14に示すように、取得部D11、管理部D12、及び提供部D13を備えている。

[0136] (取得部D11)

取得部D11は、対象者の実存性に関する確認結果である実存性確認結果を示す情報と前記実存性確認結果を示す情報に関連付けられた非代替トークンとを含む非代替データを特定するための特定情報を取得する。一例として、取得部D11は、上記特定情報として上記非代替トークンのトークンIDを取得し、取得したトークンIDを記憶部D20に格納する。

[0137] ここで、当該非代替トークンに関連付けられた実存性確認結果ECRには、上述したように、

- ・当該実存性確認結果ECRに関連付けられた時刻情報T1
- ・当該実存性確認結果ECRに関連付けられた位置情報P1
- ・実存性確認テストのスコア

の少なくとも何れかを含んでいる。また、当該実存性確認結果ECRは、後述する情報処理装置F1による認証処理において参照され、当該情報処理装置F1は、当該認証処理の結果に応じて、前記対象者にサービスを提供する。

[0138] (管理部D12)

管理部D12は、上記非代替データを管理する。一例として、管理部D12は、上記非代替データに関連付けられた非代替トークンのトークンIDを管理する。管理部D12が管理するトークンIDは、一例として、管理装置

C 1 から提供されたものである。また、管理部 D 1 2 が管理するトークン I D が示す非代替トークンは、一例として譲渡不可能に設定されたトークンである。また、管理部 D 1 2 は、管理装置 C 1 によって生成され、トークン I D に関連付けられた表示用データ D D を管理する。

[0139] なお、管理部 D 1 2 は、実存性確認結果を含む上記非代替データに含まれる非代替トークン以外の非代替トークンも管理する構成としてもよい。

[0140] (提供部 D 1 3)

提供部 D 1 3 は、前記非代替トークンを特定する特定情報を提供する。一例として、提供部 D 1 3 は、上記特定情報として、トークン I D を、後述する情報処理装置 F 1 に提供する。

[0141] ここで、提供部 D 1 3 による特定情報の具体的な提供処理は本例示的实施形態を限定するものではないが、一例として、提供部 D 1 3 は、上述した鍵情報 K I を用いて暗号化したトークン I D を情報処理装置 F 1 又は本例的实施形態に係る認証システムが備える他の装置に提供する。また、提供部 D 1 3 による具体的な暗号化処理は本提示的实施形態を限定するものではないが、一例として、提供部 D 1 3 は、

- ・ 鍵情報 K I として秘密鍵を管理し、
- ・ 所定のアルゴリズムによって上記秘密鍵から公開鍵を生成し、
- ・ 生成した公開鍵を情報処理装置 F 1 又は他の装置に提供し、
- ・ 秘密鍵を用いて暗号化したトークン I D を情報処理装置 F 1 又は他の装置に提供する

という構成と採用することができる。情報処理装置 D 1 又は上記他の装置は公開鍵を用いてトークン I D を復号したり、当該トークン I D の正当性を確認したりすることができる。

[0142] なお、管理部 D 1 2 及び提供部 D 1 3 が行う処理の一部は、いわゆるウォレットの機能の一部であると表現することもできるが、これは本例示的实施形態を限定するものではない。

[0143] (表示用データ D D の例)

図 1 5 は、管理装置 C 1 によって生成され、管理部 D 1 2 によって管理される表示用データ D D の例を示す図である。図 1 5 に示すように、当該表示用データ D D には、一例として、

- ・当該表示用データ D D に関連付けられたデータが非代替データであることを示す文字列（図 1 5 の例では「P A S S P O R T」）、及び
- ・当該表示用データ D D に関連付けられた非代替データの最新の更新日時（図 1 5 の例では「Last Updated: 2023/mm/dd」）
- ・当該表示用データ D D に関連付けられた非代替データに付与されたレベル（図 1 5 の例では「Level:★★★★★」）

等が含まれる。管理装置 C 1 は、一例として、非代替データの更新日時が現在日時により近い場合に、当該非代替データに対してより高いレベルを付与する構成としてもよい。また、このような構成の場合、更新日時の新しさを、レベルで表現することができるので、表示用データ D D は、更新日時（Last Updated: 2023/mm/dd）を含まない代わりに、レベル（Level:★★★★★）を含む構成としてもよい。なお、上記の例では、レベルの値を星の数を用いて表現しているが、これは本例示的实施形態を限定するものではなく、レベルを数字を用いて表現してもよい。

[0144] また、他の例として、管理装置 C 1 は、非代替データに含まれるスコアの値がより大きい場合に、当該非代替データに対してより高いレベルを付与する構成としてもよい。このような構成とすれば、当該スコアをユーザに対して効果的に提示することができる。

[0145] また、表示用データ D D は、上述した更新日時やレベルに代えて、又はそれらと共に、アイコン（図像）を含む構成としてもよい。ここで当該アイコンは、一例として、更新日時やレベルを、当該アイコン（図像）の色や形や大きさ等を用いてユーザに識別可能に提示できるよう構成されてもよい。

[0146] （情報処理装置 F 1）

図 1 6 は、情報処理装置 F 1 の構成を示すブロック図である。図 1 6 に示すように、情報処理装置 F 1 は、制御部 F 1 0、記憶部 F 2 0、通信部 F 3

0、及び入出力部F 4 0を備えている。情報処理装置F 1は、一例として対象者（ユーザ）にサービスを提供する装置であるが、これは本例示的实施形態を限定するものではない。

[0147] 通信部F 3 0は、情報処理装置F 1の外部の装置と通信を行う。一例として通信部F 3 0は、情報処理装置D 1、分散台帳システムG 1、及び本例示的实施形態に係る認証システムが備える他の装置の少なくとも何れかの装置と通信を行う。また、通信部F 3 0は、制御部F 1 0から供給されたデータを上記外部の装置に送信したり、上記外部の装置から受信したデータを制御部F 1 0に供給したりする。

[0148] 入出力部F 4 0は、一例として、キーボード、マウス、ディスプレイ、プリンタ、タッチパネル、カメラ、スピーカ等の少なくとも何れかの入出力デバイスを備えている。また、入出力部F 4 0は、これらの入出力デバイスを備える代わりに、例えばU S B（Universal Serial Bus）などのインタフェースを備えてもよい。そして、当該インタフェースにこれらの少なくとも何れかの入出力デバイスが接続される構成としてもよい。

[0149] 入出力部F 4 0は、上記少なくとも何れかの入出力デバイスから情報処理装置F 1に対する各種の情報の入力を受け付ける。また、入出力部F 4 0は、制御部F 1 0の制御の下、当該少なくとも何れかの入出力デバイスに各種の情報を出力する。

[0150] （記憶部F 2 0）

記憶部F 2 0には、制御部F 1 0によって参照される各種の情報、及び制御部F 1 0によって導出された各種の情報が格納されている。一例として、記憶部F 2 0には、

- ・ 情報処理装置D 1から提供されたトークンIDを復号するための鍵情報F K I
 - ・ 情報処理装置D 1に提供するための提供用サービスデータ群S D G
- が格納されている。

[0151] （制御部F 1 0）

制御部 F 1 0 は、図 1 6 に示すように、取得部 F 1 1、管理部 F 1 2、及び提供部 F 1 3 を備えている。

[0152] (取得部 F 1 1)

取得部 F 1 1 は、対象者の実存性に関する確認結果である実存性確認結果に関連付けられた非代替トークンを特定する特定情報を取得する。一例として、取得部 F 1 1 は、上記特定情報として、上記非代替トークンのトークン ID を取得する。取得部 F 1 1 による特定情報の具体的な取得処理は本例示の実施形態を限定するものではないが、一例として、取得部 F 1 1 は、

- ・ 情報処理装置 D 1 において秘密鍵を用いて暗号化されたトークン ID を取得し、
 - ・ 取得したトークン ID を公開鍵を用いて復号する
- という処理を行ってもよい。

[0153] また、取得部 F 1 1 は、上記トークン ID に関連付けられた実存性確認結果に対応する時刻情報 T 1 及び位置情報 P 1 の少なくとも何れかを更に取得してもよい。

[0154] (認証部 F 1 2)

認証部 F 1 2 は、前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照した認証処理を実行する。また、認証部 F 1 2 は、取得部 F 1 1 が取得した時刻情報 T 1 及び位置情報 P 1 の少なくとも何れかを更に参照した認証処理を実行してもよい。また、前記実存性確認結果が、当該実存性確認に関するスコアを含んでおり、認証部 F 1 2 が、前記スコアを更に参照した認証処理を実行する構成としてもよい。

[0155] (提供部 F 1 3)

提供部 F 1 3 は、認証部 F 1 2 による前記認証処理の結果に応じて、前記対象者に対するサービスを提供する。ここで、提供部 F 1 3 が提供するサービスの具体例は本例示の実施形態を限定するものではないが、一例として、ゲーム、金融サービス、ビジネスサポート、情報発信、医療・ヘルスケア及び人事サービス等のサービスを挙げることができる。提供部 F 1 3 は、認証

部 F 1 2 による認証結果に応じて、これらのサービスに関連するデータ等を、ユーザが所有する端末（端末装置 B 1 や情報処理装置 D 1 等）に提供する。

[0156] （認証処理及び提供処理の例）

以下では、認証部 F 1 2 による認証処理及び提供部 F 1 3 による提供処理の例について説明する。

[0157] （例 1）

認証部 F 1 2 が、

- ・取得部 F 1 1 が取得したトークン I D によって特定される非代替トークンに関連付けられている対象者の実存性確認結果に含まれるスコアが 6 0 点以上である

- ・上記実存性確認結果に関連付けられている時刻情報 T 1 が、1 日以上前のものではない

と判定した場合に、提供部 F 1 3 は、トークン I D の提供元である情報処理装置 D 1 からのログインを許可し、当該情報処理装置 D 1 に対してソーシャルネットワーキングサービスの提供を行う。

[0158] （例 2）

認証部 F 1 2 が、

- ・取得部 F 1 1 が取得したトークン I D によって特定される非代替トークンに関連付けられている対象者の実存性確認結果に含まれるスコアが 5 0 点以上である

- ・上記実存性確認結果に関連付けられている時刻情報 T 1 が、1 年以内のものである

- ・対象者がサービスの運営元が発行した他の非代替トークンを保持していると判定した場合に、提供部 F 1 3 は、トークン I D の提供元である情報処理装置 D 1 からのログインを許可し、当該情報処理装置 D 1 に対してゲームデータの提供を行う。

[0159] （例 3）

認証部 F 1 2 が、

- ・ 取得部 F 1 1 が取得したトークン I D によって特定される非代替トークンに関連付けられている対象者の実存性確認結果に含まれるスコアが 9 0 点以上である

- ・ 上記実存性確認結果に関連付けられている時刻情報 T I が、3 時間以内のものである

と判定した場合に、提供部 F 1 3 は、トークン I D の提供元である情報処理装置 D 1 からのログインを許可し、当該情報処理装置 D 1 に対して金融サービスの提供を行う。

[0160] (例 4)

認証部 F 1 2 が、

- ・ 取得部 F 1 1 が取得したトークン I D によって特定される非代替トークンに関連付けられている時刻情報 T I 及び位置情報 P I が、対象者（端末装置 B 1）が所定のタイミングで所定の経路に沿って移動したことを示していると判定した場合に、提供部 F 1 3 は、情報処理装置 D 1 に対して、スタンプラリー終了時のサービスの提供を行う。

[0161] (例 5)

認証部 F 1 2 が、

- ・ 取得部 F 1 1 が取得したトークン I D によって特定される非代替トークンに関連付けられている時刻情報 T I 及び位置情報 P I が、対象者が所定の日時（時間帯）に所定の場所に存在していたことを示している

と判定した場合に、提供部 F 1 3 は、勤怠管理装置（又は出欠確認装置）に対して、当該対象者が当該日時に勤務（又はレクチャー等に参加）していたことを通知する。

[0162] (例 6)

認証部 F 1 2 が、

- ・ 取得部 F 1 1 が取得したトークン I D によって特定される非代替トークンに関連付けられている時刻情報 T I 及び位置情報 P I が、対象者が所定の時

間内に、所定の経路に沿って場所Aから場所Bに移動したことを示していると判定した場合に、提供部F 13は、場所Aから場所Bまでの当該経路における交通機関の交通料金を対象者に対して請求する。

[0163] このように、情報処理装置F 1は、対象者の実存性に関する確認結果である実存性確認結果に関連付けられた非代替トークンを特定する特定情報を取得し、前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照した認証処理を実行する。したがって、上記の構成によれば、公平かつ透明性の高い認証システムを提供することができる。

[0164] なお、情報処理装置F 1は、上述の認証処理を事前に定められたルールに従って行うことができる。または、情報処理装置F 1は、認証処理の基準を動的に切り替えてもよい。以下、認証処理の切り替え方法の一例を説明する。

[0165] ユーザが実存性確認を頻繁に行うことで、ユーザに対する信頼度が高まるという利点がある。しかしながら、頻繁な更新や高すぎる認証スコアの要求は、ユーザに繰り返し認証を行う負担を与え、ユーザの満足度低下に繋がる可能性もある。

[0166] 情報処理装置F 1は、既存の機械学習技術や最適化手法を用いて、認証基準を切り替えるようにしてもよい。一例として、情報処理装置F 1は、ユーザの実存性確認に関連するスコアや時刻情報を入力として受け取り、当該ユーザがボット（またはロボット、自動化されたプログラム）であるか否かを判断する機械学習モデルを用いてもよい。このような機械学習モデルは、ユーザの実存性確認に関連するスコアや時刻情報と、当該ユーザがボット（またはロボット、自動化されたプログラム）であるか否かを示す正解ラベルとを含む学習用データを用いて予め学習させておくことができる。

[0167] 情報処理装置F 1は、このような機械学習モデルを利用して、ボットの排除率を一定の閾値以上を満たす範囲内で、簡易な認証処理の基準を探索（最適化）することができる。換言すれば、情報処理装置F 1の制御部F 10は、対象者の実存性確認結果とラベル（正解ラベル）との関係を学習した機械

学習モデルに基づいて認証処理の条件を最適化するという構成としてもよい。

[0168] このように、情報処理装置F 1は、過去のデータから作成された機械学習モデルを用いることで、可能な限りユーザの負担が少なく、かつボットを排除可能な認証基準を設定することができる。

[0169] [ヘルスケアサービスへの応用例]

また、情報処理装置F 1は、ウォレットで管理されている、特定の情報を有するN F Tのデータを利用してもよい。

[0170] 具体的には、本実施形態の技術によれば、ユーザが保有するウォレットの信頼性を担保することができる。サービスを提供する事業者は、このように高い信頼性を有するウォレットに格納されている情報を利用することでサービスを提供してもよい。

[0171] 例えば、情報処理装置F 1は、心拍数等、診断に必要なデータを登録したN F T（ヘルスケアトークンと呼ぶ）に関する情報をウォレットから取得するようにしてもよい。サービス提供者は、信頼できるウォレットに格納されたヘルスケアトークンのデータを活用することで、ユーザに対してさまざまなヘルスケアサービスを提供できる。これにより、個人の健康情報の安全性とプライバシーを保護しつつ、効率的かつ正確なサービス提供が実現できる。

[0172] [ソフトウェアによる実現例]

生成装置A 1、端末装置B 1、管理装置C 1、情報処理装置D 1、情報処理装置F 1、ノードG 1 1の一部又は全部の機能は、集積回路（I Cチップ）等のハードウェアによって実現してもよいし、ソフトウェアによって実現してもよい。

[0173] 後者の場合、生成装置A 1、端末装置B 1、管理装置C 1、情報処理装置D 1、情報処理装置F 1、ノードG 1 1は、例えば、各機能を実現するソフトウェアであるプログラムの命令を実行するコンピュータによって実現される。このようなコンピュータの一例（以下、コンピュータCと記載する）を図1 7に示す。コンピュータCは、少なくとも1つのプロセッサC 1と、少

なくとも1つのメモリC2と、を備えている。メモリC2には、コンピュータCを生成装置A1、端末装置B1、管理装置C1、情報処理装置D1、情報処理装置F1、ノードG11として動作させるためのプログラムPが記録されている。コンピュータCにおいて、プロセッサC1は、プログラムPをメモリC2から読み取って実行することにより、生成装置A1、端末装置B1、管理装置C1、情報処理装置D1、情報処理装置F1、ノードG11の各機能が実現される。

[0174] プロセッサC1としては、例えば、CPU (Central Processing Unit)、GPU (Graphic Processing Unit)、DSP (Digital Signal Processor)、MPU (Micro Processing Unit)、FPU (Floating point number Processing Unit)、PPU (Physics Processing Unit)、TPU (Tensor Processing Unit)、量子プロセッサ、マイクロコントローラ、又は、これらの組み合わせなどを用いることができる。メモリC2としては、例えば、フラッシュメモリ、HDD (Hard Disk Drive)、SSD (Solid State Drive)、又は、これらの組み合わせなどを用いることができる。

[0175] なお、コンピュータCは、プログラムPを実行時に展開したり、各種データを一時的に記憶したりするためのRAM (Random Access Memory) を更に備えていてもよい。また、コンピュータCは、他の装置との間でデータを送受信するための通信インタフェースを更に備えていてもよい。また、コンピュータCは、キーボードやマウス、ディスプレイやプリンタなどの入出力機器を接続するための入出力インタフェースを更に備えていてもよい。

[0176] また、プログラムPは、コンピュータCが読み取り可能な、一時的でない有形の記録媒体Mに記録することができる。このような記録媒体Mとしては、例えば、テープ、ディスク、カード、半導体メモリ、又はプログラマブルな論理回路などを用いることができる。コンピュータCは、このような記録媒体Mを介してプログラムPを取得することができる。また、プログラムPは、伝送媒体を介して伝送することができる。このような伝送媒体としては、例えば、通信ネットワーク、又は放送波などを用いることができる。コン

ピュータCは、このような伝送媒体を介してプログラムPを取得することもできる。

[0177] 〔付記事項１〕

本発明は、上述した実施形態に限定されるものでなく、請求項に示した範囲で種々の変更が可能である。例えば、上述した実施形態に開示された技術的手段を適宜組み合わせ得られる実施形態についても、本発明の技術的範囲に含まれる。

[0178] 〔付記事項２〕

上述した実施形態の一部又は全部は、以下のようにも記載され得る。ただし、本発明は、以下の記載する態様に限定されるものではない。

[0179] （付記Ｃ１）

対象者の実存性に関する確認結果である実存性確認結果を取得する取得手段と、

前記実存性確認結果を非代替トークンと関連付けて管理する管理手段とを備えている管理装置。

[0180] （付記Ｃ２）

前記管理手段は、前記非代替トークンを発行する発行手段を備えている付記Ｃ１に記載の管理装置。

[0181] （付記Ｃ３）

前記取得手段は、前記実存性確認結果に関連付けられた時刻情報を取得し、

前記管理手段は、前記前記実存性確認結果に時刻情報を関連付けて管理する

付記Ｃ１又はＣ２に記載の管理装置。

[0182] （付記Ｃ４）

前記取得手段は、位置情報を取得し、

前記管理手段は、前記前記実存性確認結果に前記位置情報を関連付けて管理する

付記 C 1 から C 3 の何れか 1 項に記載の管理装置。

[0183] (付記 C 5)

前記実存性確認結果には、当該実存性確認に関するスコアが含まれる
付記 C 1 から C 4 の何れか 1 項に記載の管理装置。

[0184] (付記 C 6)

前記取得手段は、更新用の実存性確認結果を取得し、
前記管理手段は、前記更新用の実存性確認結果を用いて、前記非代替トークンに関連付けられた実存性確認結果を更新する
付記 C 1 から C 5 の何れか 1 項に記載の管理装置。

[0185] (付記 C 7)

前記管理手段は、
前記非代替トークンの表示用データであって、前記実存性確認結果に応じた表示オブジェクトを含む表示用データを生成する
付記 C 1 から C 6 の何れか 1 項に記載の管理装置。

[0186] (付記 C 8)

前記非代替トークンは、譲渡不可能に設定されたトークンである
付記 C 1 から C 7 の何れか 1 項に記載の管理装置。

[0187] (付記 A 1)

対象者の実存性を確認するための参照情報を取得する取得手段と、
前記対象者の実存性に関する確認結果である実存性確認結果であって非代替トークンへの関連付けの対象である実存性確認結果を、前記参照情報を参照して生成する生成手段と
を備えている生成装置。

[0188] (付記 A 2)

前記取得手段は、対象者の実存性確認テストを実施する端末装置から、当該実存性確認テストに対する前記対象者による応答情報として、前記参照情報を取得する
付記 A 1 に記載の生成装置。

[0189] (付記 A 3)

前記実存性確認結果を非代替トークンと関連付けて管理する管理装置に、
前記実存性確認結果を提供する提供手段を備える
付記 A 1 又は A 2 に記載の生成装置。

[0190] (付記 A 4)

前記提供手段は、前記非代替トークンへの関連付けの対象である時刻情報
を前記管理装置に提供する
付記 A 3 に記載の生成装置。

[0191] (付記 A 5)

前記提供手段は、前記非代替トークンへの関連付けの対象である位置情報
を前記管理装置に提供する
付記 A 3 又は A 4 に記載の生成装置。

[0192] (付記 A 6)

前記実存性確認結果には、当該実存性確認に関するスコアが含まれる
付記 A 1 から A 5 の何れか 1 項に記載の生成装置。

[0193] (付記 A 7)

前記取得手段は、更なる参照情報を取得し、
前記生成手段は、当該更なる参照情報を参照して、前記実存性確認結果を
生成する
付記 A 1 から A 6 の何れか 1 項に記載の生成装置。

[0194] (付記 B 1)

対象者の実存性確認のための確認テストを実行する実行手段と、
前記対象者の実存性に関する確認結果である実存性確認結果であって、非
代替トークンへの関連付けの対象である実存性確認結果を生成する生成装置
に、前記確認テストに対する前記対象者の応答情報を提供する提供手段と
を備えている端末装置。

[0195] (付記 B 2)

前記確認テストには、生体の認証に関するテストが含まれる

付記 B 1 に記載の端末装置。

[0196] (付記 B 3)

前記提供手段は、前記確認テストを実行した時刻を示す時刻情報を、前記生成装置に提供する

付記 B 1 又は B 2 に記載の端末装置。

[0197] (付記 B 4)

前記提供手段は、当該端末装置の位置情報を、前記生成装置に提供する
付記 B 1 から B 3 の何れか 1 項に記載の端末装置。

[0198] (付記 B 5)

前記実行手段は、対象者の実存性確認のための更なる確認テストを実行し、

前記提供手段は、前記更なる確認テストに対する前記対象者の応答情報を提供する

付記 B 1 から B 4 の何れか 1 項に記載の端末装置。

[0199] (付記 B 6)

前記実行手段は、実存性確認結果と非代替トークンとを関連付けて管理する管理装置からの指示に基づき、前記確認テストを実施する

付記 B 1 から B 5 の何れか 1 項に記載の端末装置。

[0200] (付記 B 7)

前記実存性確認結果が関連付けられる非代替トークンを特定する特定情報を取得する取得手段を更に備え、

前記提供手段は、前記特定情報を、前記生成装置に提供する

付記 B 1 から B 6 の何れか 1 項に記載の端末装置。

[0201] (付記 D 1)

対象者の実存性に関する確認結果である実存性確認結果を示す情報と、前記実存性確認結果を示す情報に関連付けられた非代替トークンとを含む非代替データを特定するための特定情報を取得する取得手段と、

前記非代替データを管理する管理手段を備えている情報処理装置。

[0202] (付記 D 2)

前記非代替トークンを特定する特定情報を提供する提供手段を備えている
付記 D 1 に記載の情報処理装置。

[0203] (付記 D 3)

前記非代替データは、前記実存性確認結果に関連付けられた時刻情報を含
んでいる
付記 D 1 又は D 2 に記載の情報処理装置。

[0204] (付記 D 4)

前記非代替データは、位置情報を含んでいる
付記 D 1 から D 3 の何れか 1 項に記載の情報処理装置。

[0205] (付記 D 5)

前記実存性確認結果は、当該実存性確認に関するスコアを含んでいる
付記 D 1 から D 4 の何れか 1 項に記載の生成装置。

[0206] (付記 D 6)

前記実存性確認結果は、情報処理装置による認証処理において参照され、
当該情報処理装置は、当該認証処理の結果に応じて、前記対象者にサービス
を提供する
付記 D 1 から D 5 の何れか 1 項に記載の生成装置。

[0207] (付記 D 7)

前記非代替トークンは、譲渡不可能に設定されたトークンである
付記 D 1 から D 6 の何れか 1 項に記載の管理装置。

[0208] (付記 F 1)

対象者の実存性に関する確認結果である実存性確認結果に関連付けられた
非代替トークンを特定する特定情報を取得する取得手段と、
前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照し
た認証処理を実行する認証手段と
を備えている情報処理装置。

[0209] (付記 F 2)

前記取得手段は、前記実存性確認結果に関連付けられた時刻情報を更に取り得し、

前記認証手段は、前記時刻情報を更に参照した認証処理を行う
付記 F 1 に記載の情報処理装置。

[0210] (付記 F 3)

前記取得手段は、前記実存性確認結果に関連付けられた位置情報を更に取り得し、

前記認証手段は、前記位置情報を更に参照した認証処理を行う
付記 F 1 又は F 2 に記載の情報処理装置。

[0211] (付記 F 4)

前記実存性確認結果は、当該実存性確認に関するスコアを含んでおり、
前記認証手段は、前記スコアを更に参照した認証処理を実行する
付記 F 1 から F 3 の何れか 1 項に記載の情報処理装置。

[0212] (付記 F 5)

前記認証処理の結果に応じて、前記対象者に対するサービスを提供する提供手段を更に備えている
付記 F 1 から F 4 の何れか 1 項に記載の情報処理装置。

[0213] (付記 F 6)

前記対象者の実存性確認結果とラベルとの関係を学習した機械学習モデルに基づいて、前記認証処理の条件を最適化する
付記 F 1 から F 5 の何れか 1 項に記載の情報処理装置。

[0214] (付記 E 1)

対象者の実存性に関する確認結果である実存性確認結果を示す情報と、
前記実存性確認結果を示す情報に関連付けられた非代替トークンと
を含む非代替データのデータ構造。

[0215] (付記 E 2)

前記非代替データは、前記実存性確認結果に関連付けられた時刻情報を含んでいる

付記 E 1 に記載の情報処理装置。

[0216] (付記 E 3)

前記非代替データは、位置情報を含んでいる

付記 E 1 又は E 2 に記載の情報処理装置。

[0217] (付記 E 4)

前記実存性確認結果は、当該実存性確認に関するスコアを含んでいる

付記 E 1 から E 3 の何れか 1 項に記載の生成装置。

[0218] (付記 E 5)

前記実存性確認結果は、情報処理装置による認証処理において参照され、当該情報処理装置は、当該認証処理の結果に応じて、前記対象者にサービスを提供する

付記 E 1 から E 4 の何れか 1 項に記載の生成装置。

[0219] (付記 E 6)

前記非代替トークンは、譲渡不可能に設定されたトークンである

付記 E 1 から E 5 の何れか 1 項に記載の管理装置。

[0220] (付記 S C 1)

管理装置が、

対象者の実存性に関する確認結果である実存性確認結果を取得することと、

前記実存性確認結果を非代替トークンと関連付けて管理することとを含んでいる管理方法。

[0221] (付記 S A 1)

生成装置が、

対象者の実存性を確認するための参照情報を取得することと、

前記対象者の実存性に関する確認結果である実存性確認結果であって非代替トークンへの関連付けの対象である実存性確認結果を、前記参照情報を参照して生成することと

を含んでいる生成方法。

[0222] (付記 S B 1)

端末装置が、

対象者の実存性確認のための確認テストを実行することと、

前記対象者の実存性に関する確認結果である実存性確認結果であって、非代替トークンへの関連付けの対象である実存性確認結果を生成する生成装置に、前記確認テストに対する前記対象者の応答情報を提供することとを含んでいる情報処理方法。

[0223] (付記 S D 1)

情報処理装置が、

対象者の実存性に関する確認結果である実存性確認結果を示す情報と、前記実存性確認結果を示す情報に関連付けられた非代替トークンとを含む非代替データを特定するための特定情報を取得することと、

前記非代替データを管理することと

を含んでいる情報処理方法。

[0224] (付記 S F 1)

情報処理装置が、

対象者の実存性に関する確認結果である実存性確認結果に関連付けられた非代替トークンを特定する特定情報を取得することと、

前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照した認証処理を実行することと

を含んでいる情報処理方法。

[0225] (付記 P C 1)

コンピュータを管理装置として機能させるプログラムであって、

前記プログラムは、前記コンピュータに、

対象者の実存性に関する確認結果である実存性確認結果を取得することと

、

前記実存性確認結果を非代替トークンと関連付けて管理することと

を実行させるプログラム。

[0226] (付記 P A 1)

コンピュータを生成装置として機能させるプログラムであって、
前記プログラムは、前記コンピュータに、
対象者の実存性を確認するための参照情報を取得することと、
前記対象者の実存性に関する確認結果である実存性確認結果であって非代替トークンへの関連付けの対象である実存性確認結果を、前記参照情報を参照して生成することと
を実行させるプログラム。

[0227] (付記 P B 1)

コンピュータを端末装置として機能させるプログラムであって、
前記プログラムは、前記コンピュータに、
対象者の実存性確認のための確認テストを実行することと、
前記対象者の実存性に関する確認結果である実存性確認結果であって、非代替トークンへの関連付けの対象である実存性確認結果を生成する生成装置に、前記確認テストに対する前記対象者の応答情報を提供することと
を実行させるプログラム。

[0228] (付記 P D 1)

コンピュータを端末装置として機能させるプログラムであって、
前記プログラムは、前記コンピュータに、
対象者の実存性に関する確認結果である実存性確認結果を示す情報と、前記実存性確認結果を示す情報に関連付けられた非代替トークンとを含む非代替データを特定するための特定情報を取得することと、
前記非代替データを管理することと
を実行させるプログラム。

[0229] (付記 P F 1)

コンピュータを情報処理装置として機能させるプログラムであって、
前記プログラムは、前記コンピュータに、
対象者の実存性に関する確認結果である実存性確認結果に関連付けられた

非代替トークンを特定する特定情報を取得することと、

前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照した認証処理を実行することと

を実行させるプログラム。

[0230] 〔付記事項 3〕

上述した実施形態の一部又は全部は、更に、以下のように表現することもできる。

[0231] （付記 C C 1）

少なくとも 1 つのプロセッサを備え、前記プロセッサは、

対象者の実存性に関する確認結果である実存性確認結果を取得する取得処理と、

前記実存性確認結果を非代替トークンと関連付けて管理する管理処理とを実行する管理装置。

[0232] （付記 A A 1）

少なくとも 1 つのプロセッサを備え、前記プロセッサは、

対象者の実存性を確認するための参照情報を取得する取得処理と、

前記対象者の実存性に関する確認結果である実存性確認結果であって非代替トークンへの関連付けの対象である実存性確認結果を、前記参照情報を参照して生成する生成処理と
を実行する生成装置。

[0233] （付記 B B 1）

少なくとも 1 つのプロセッサを備え、前記プロセッサは、

対象者の実存性確認のための確認テストを実行する実行処理と、

前記対象者の実存性に関する確認結果である実存性確認結果であって、非代替トークンへの関連付けの対象である実存性確認結果を生成する生成装置に、前記確認テストに対する前記対象者の応答情報を提供する提供処理と
を実行する端末装置。

[0234] （付記 D D 1）

少なくとも1つのプロセッサを備え、前記プロセッサは、
対象者の実存性に関する確認結果である実存性確認結果を示す情報と、前記実存性確認結果を示す情報に関連付けられた非代替トークンとを含む非代替データを特定するための特定情報を取得する取得処理と、
前記非代替データを管理する管理処理と
を実行する情報処理装置。

[0235] (付記 F F 1)

少なくとも1つのプロセッサを備え、前記プロセッサは、
対象者の実存性に関する確認結果である実存性確認結果に関連付けられた非代替トークンを特定する特定情報を取得する取得処理と、
前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照した認証処理を実行する認証処理と
を実行する情報処理装置。

[0236] (付記 P P C 1)

コンピュータを管理装置として機能させるプログラムが格納された非一時的な記録媒体であって、
前記プログラムは、前記コンピュータに、
対象者の実存性に関する確認結果である実存性確認結果を取得することと
、
前記実存性確認結果を非代替トークンと関連付けて管理することと
を実行させる非一時的な記録媒体。

[0237] (付記 P P A 1)

コンピュータを生成装置として機能させるプログラムが格納された非一時的な記録媒体であって、
前記プログラムは、前記コンピュータに、
対象者の実存性を確認するための参照情報を取得することと、
前記対象者の実存性に関する確認結果である実存性確認結果であって非代替トークンへの関連付けの対象である実存性確認結果を、前記参照情報を参

照して生成することと
を実行させる非一時的な記録媒体。

[0238] (付記 P P B 1)

コンピュータを端末装置として機能させるプログラムが格納された非一時的な記録媒体であって、

前記プログラムは、前記コンピュータに、

対象者の実存性確認のための確認テストを実行することと、

前記対象者の実存性に関する確認結果である実存性確認結果であって、非代替トークンへの関連付けの対象である実存性確認結果を生成する生成装置に、前記確認テストに対する前記対象者の応答情報を提供することと
を実行させる非一時的な記録媒体。

[0239] (付記 P P D 1)

コンピュータを端末装置として機能させるプログラムが格納された非一時的な記録媒体であって、

前記プログラムは、前記コンピュータに、

対象者の実存性に関する確認結果である実存性確認結果を示す情報と、前記実存性確認結果を示す情報に関連付けられた非代替トークンとを含む非代替データを特定するための特定情報を取得することと、

前記非代替データを管理することと

を実行させる非一時的な記録媒体。

[0240] (付記 P P F 1)

コンピュータを情報処理装置として機能させるプログラムが格納された非一時的な記録媒体であって、

前記プログラムは、前記コンピュータに、

対象者の実存性に関する確認結果である実存性確認結果に関連付けられた非代替トークンを特定する特定情報を取得することと、

前記実存性確認結果及び前記非代替トークンの少なくとも何れかを参照した認証処理を実行することと

を実行させる非一時的な記録媒体。

[0241] なお、上述した装置及びシステムは、更にメモリを備えていてもよく、このメモリには、前記取得処理と、前記導出処理とを前記プロセッサに実行させるためのプログラムが記憶されていてもよい。また、このプログラムは、コンピュータ読み取り可能な一時的でない有形の記録媒体に記録されていてもよい。

符号の説明

[0242]	1	・・・認証システム
	A 1	・・・生成装置
	A 1 1	・・・取得部
	A 1 2	・・・生成部
	B 1	・・・端末装置
	B 1 1	・・・実行部
	B 1 2	・・・提供部
	C 1	・・・管理装置
	C 1 1	・・・取得部
	C 1 2	・・・管理部
	D 1	・・・情報処理装置
	D 1 1	・・・取得部
	D 1 2	・・・管理部
	F 1	・・・情報処理装置
	F 1 1	・・・取得部
	F 1 2	・・・認証部
	G 1	・・・分散台帳システム

請求の範囲

- [請求項1] 対象者の実存性に関する確認結果である実存性確認結果を取得する取得手段と、
前記実存性確認結果を非代替トークンと関連付けて管理する管理手段と
を備えている管理装置。
- [請求項2] 前記管理手段は、前記非代替トークンを発行する発行手段を備えている
請求項1に記載の管理装置。
- [請求項3] 前記取得手段は、前記実存性確認結果に関連付けられた時刻情報を取得し、
前記管理手段は、前記前記実存性確認結果に時刻情報を関連付けて管理する
請求項1又は2に記載の管理装置。
- [請求項4] 前記取得手段は、位置情報を取得し、
前記管理手段は、前記前記実存性確認結果に前記位置情報を関連付けて管理する
請求項1から3の何れか1項に記載の管理装置。
- [請求項5] 前記実存性確認結果には、当該実存性確認に関するスコアが含まれる
請求項1から4の何れか1項に記載の管理装置。
- [請求項6] 前記取得手段は、更新用の実存性確認結果を取得し、
前記管理手段は、前記更新用の実存性確認結果を用いて、前記非代替トークンに関連付けられた実存性確認結果を更新する
請求項1から5の何れか1項に記載の管理装置。
- [請求項7] 前記管理手段は、
前記非代替トークンの表示用データであって、前記実存性確認結果に応じた表示オブジェクトを含む表示用データを生成する

請求項 1 から 6 の何れか 1 項に記載の管理装置。

[請求項8] 前記非代替トークンは、譲渡不可能に設定されたトークンである
請求項 1 から 7 の何れか 1 項に記載の管理装置。

[請求項9] 対象者の実存性に関する確認結果である実存性確認結果に関連付け
られた非代替トークンを特定する特定情報を取得する取得手段と、
前記実存性確認結果及び前記非代替トークンの少なくとも何れかを
参照した認証処理を実行する認証手段と
を備えている情報処理装置。

[請求項10] 前記取得手段は、前記実存性確認結果に関連付けられた時刻情報を
更に取得し、
前記認証手段は、前記時刻情報を更に参照した認証処理を行う
請求項 9 に記載の情報処理装置。

[請求項11] 前記取得手段は、前記実存性確認結果に関連付けられた位置情報を
更に取得し、
前記認証手段は、前記位置情報を更に参照した認証処理を行う
請求項 9 又は 10 に記載の情報処理装置。

[請求項12] 前記実存性確認結果は、当該実存性確認に関するスコアを含んでお
り、
前記認証手段は、前記スコアを更に参照した認証処理を実行する
請求項 9 から 11 の何れか 1 項に記載の情報処理装置。

[請求項13] 前記認証処理の結果に応じて、前記対象者に対するサービスを提供
する提供手段を更に備えている
請求項 9 から 12 の何れか 1 項に記載の情報処理装置。

[請求項14] 前記対象者の実存性確認結果とラベルとの関係を学習した機械学習
モデルに基づいて、前記認証処理の条件を最適化する
請求項 9 から 13 の何れか 1 項に記載の情報処理装置。

[請求項15] 管理装置が、
対象者の実存性に関する確認結果である実存性確認結果を取得する

ことと、

前記実存性確認結果を非代替トークンと関連付けて管理することと
を含んでいる管理方法。

[請求項16]

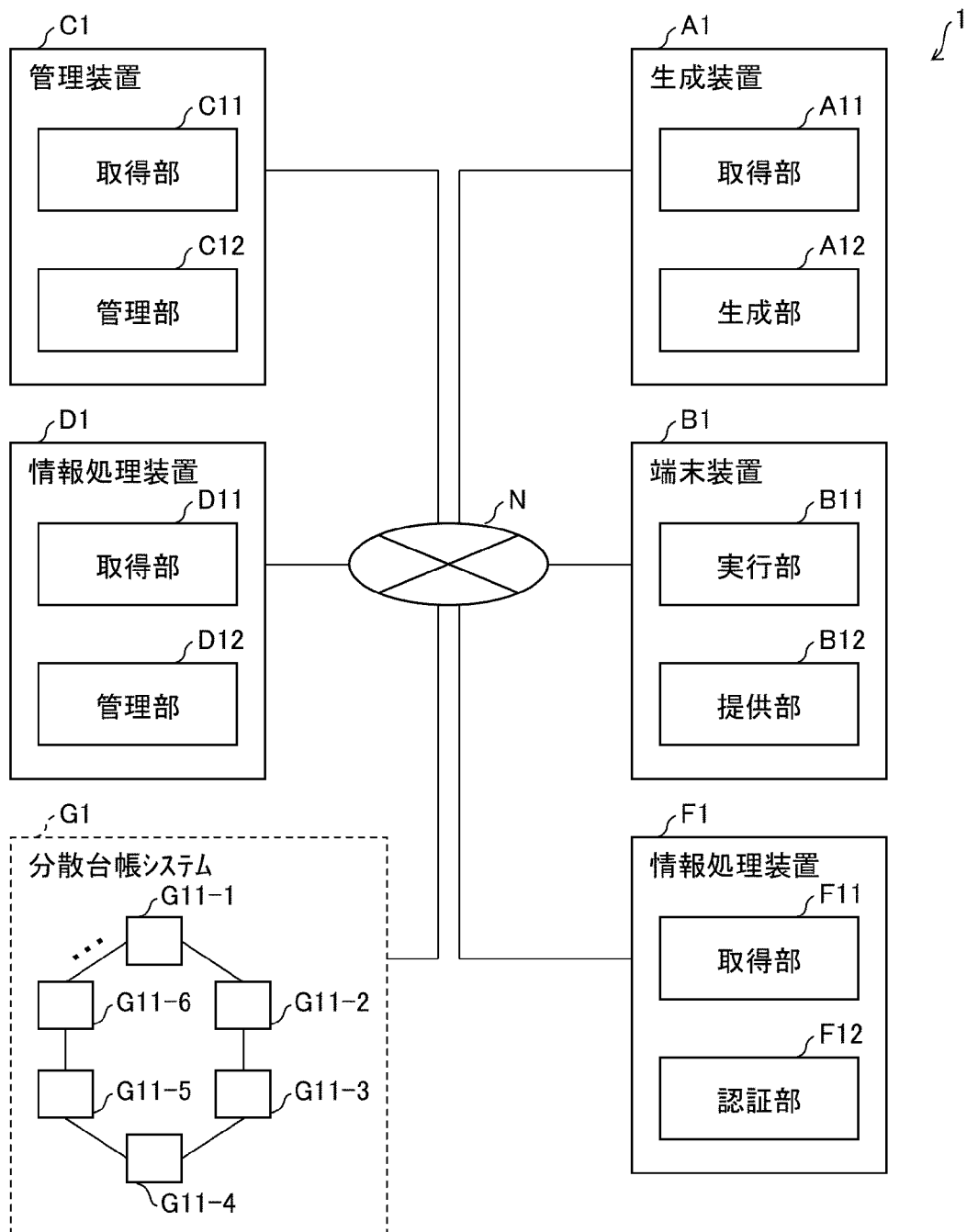
コンピュータを管理装置として機能させるプログラムであって、
前記プログラムは、前記コンピュータに、

対象者の実存性に関する確認結果である実存性確認結果を取得する
ことと、

前記実存性確認結果を非代替トークンと関連付けて管理することと
を実行させるプログラム。

[図1]

図 1



[図2]

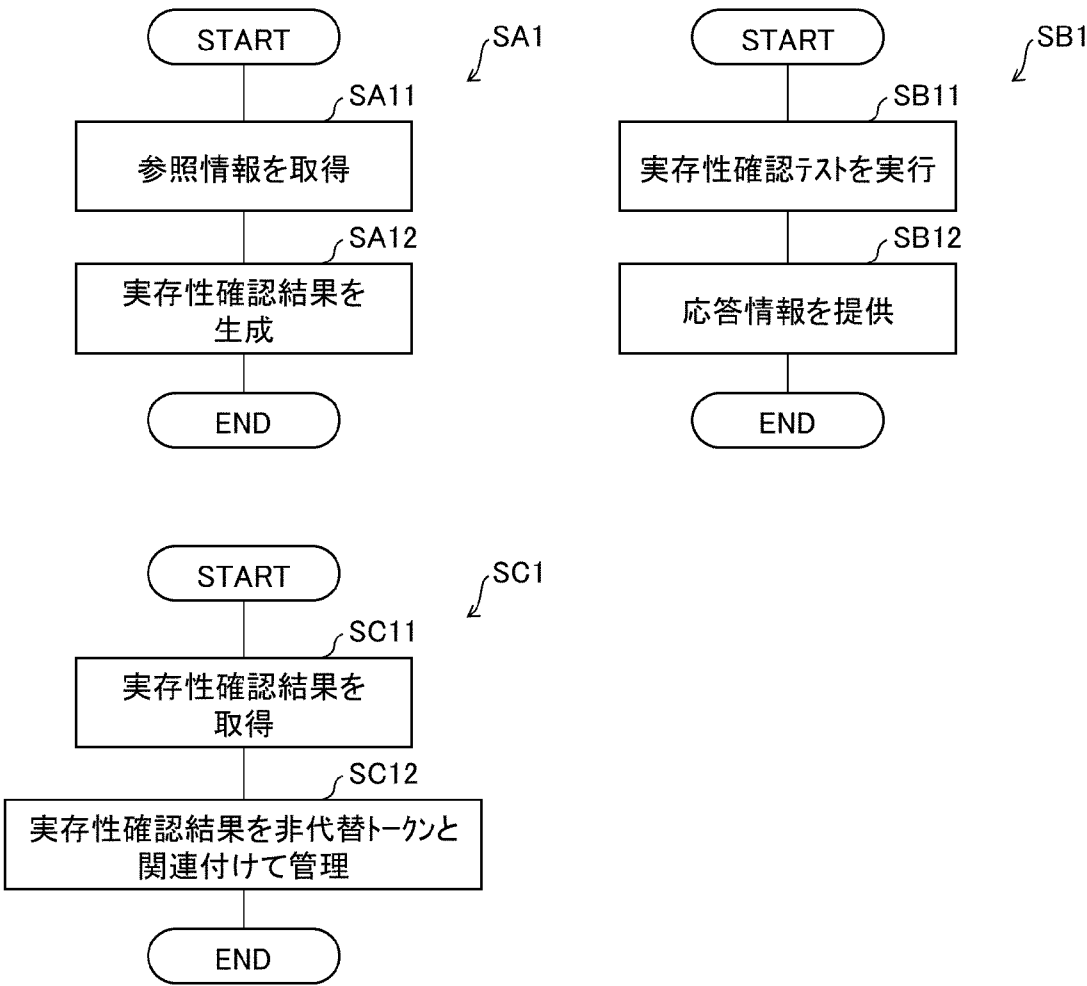
図 2

NFT(NFD)

トークンID	実存性確認結果
1	OK (score:70)
2	OK (score:90)
3	NG (score:20)
⋮	⋮

[図3]

図 3



[図4]

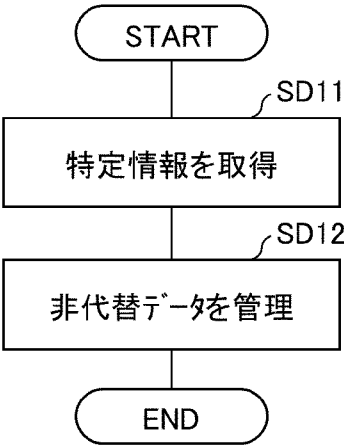
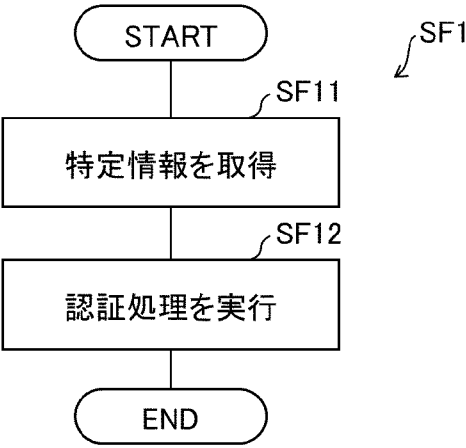
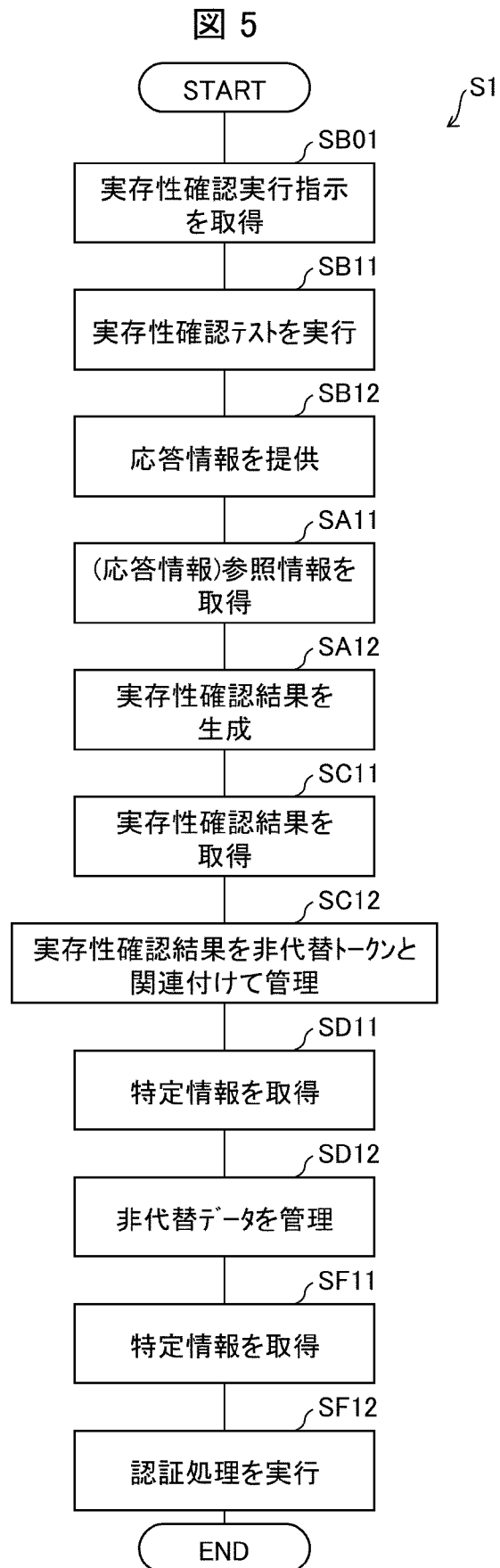


図 4

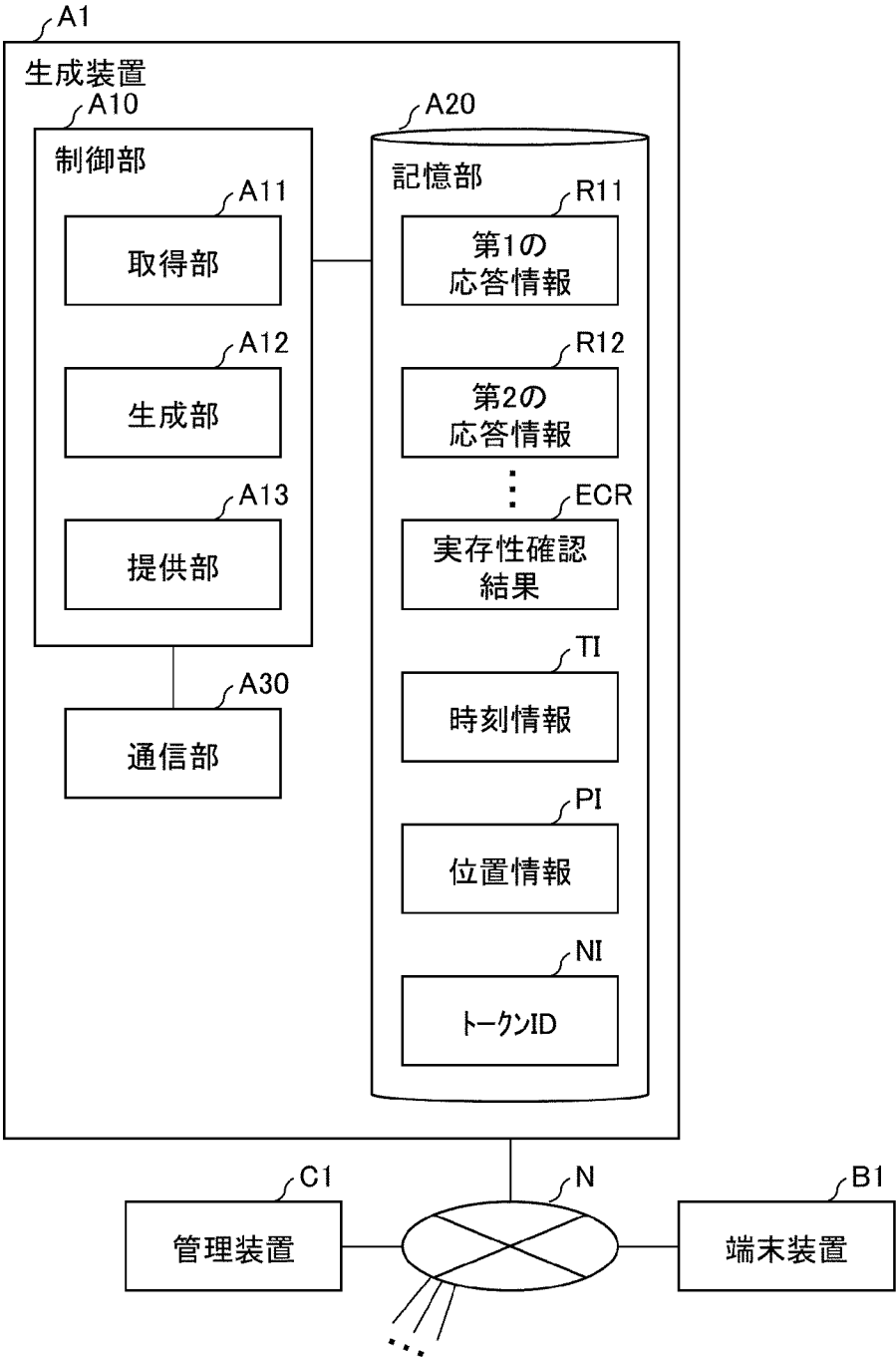


[図5]



[図6]

図 6

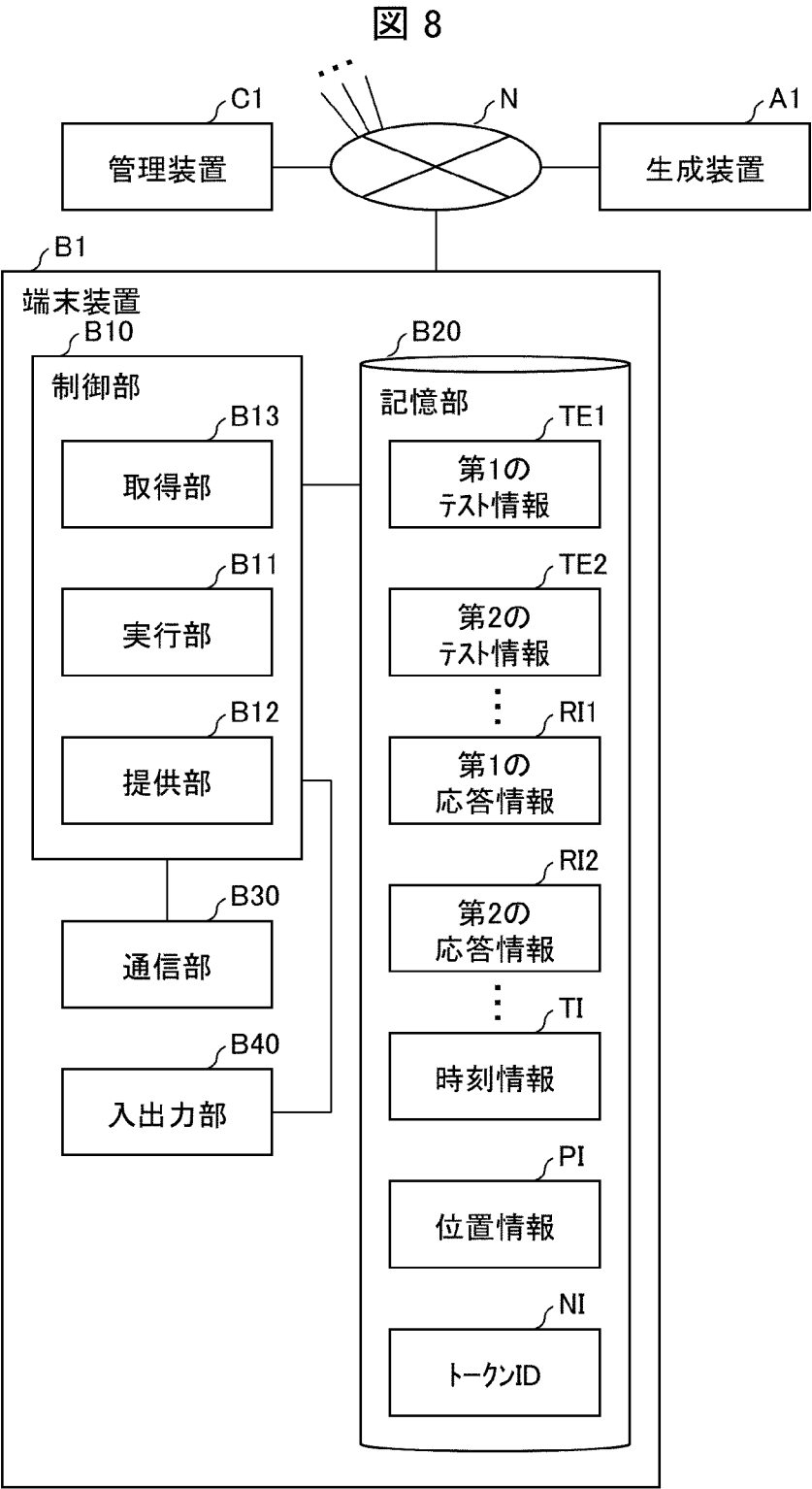


[図7]

図 7

User Name	Email Address	Birthdate	Country	income	TI		ECR		PI	
					Time_stamp	Biometric Result	Biometric Score	Position		
John XXX	john.xxx@example.com	1990-xx-xx	USA	2.5	2023-04-01	Success	97	Lat: xxx, Lon: xxx		
Jane YYY	jane.yyy@example.com	1985-yy-yy	Canada	1.8	2023-03-20	Success	95	Lat: yyy, Lon: yyy		
Mike ZZZ	mike.zzz@example.com	1997-zz-zz	UK	4	2023-02-28	Failure	20	Lat: zzz, Lon: zzz		
Alice WWW	alice.www@example.com	1992-ww-ww	Australia	3.2	2023-01-15	Success	99	Lat: www, Lon: www		

[図8]



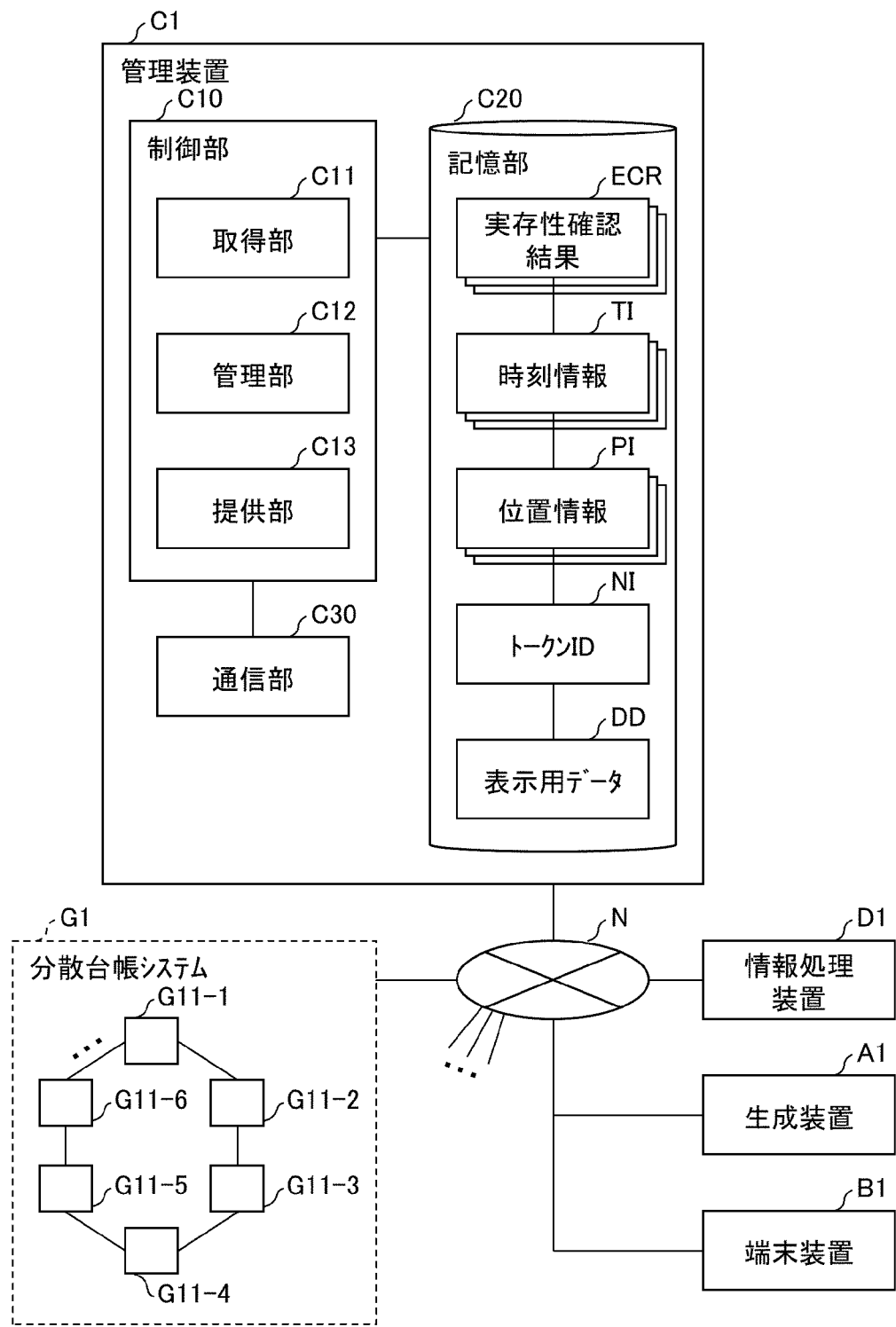
[図9]

図 9

コード	種別	テスト用データ			
		画像A	画像B	画像C	音声
FD01	正面		正面を 向ってください		“正面を向い てください”
FD02	左向き		左を 向ってください		“左を向いて ください”
FD03	右向き		右を 向ってください		“右を向いて ください”
FD04	上向き		上を 向ってください		“上を向いて ください”
FD05	下向き		下を 向ってください		“下を向いて ください”

[図10]

図 10



[図11]

図 11

非代替データの構成例1

NFT(NFD)

NI	TI	ECR		PI
NFT ID	Time_stamp	Biometric Result	Biometric Score	Position
NFT-001	2023-04-01	Success	97	Lat: xxx, Lon: xxx
NFT-002	2023-03-20	Success	95	Lat: yyy, Lon: yyy
NFT-003	2023-02-28	Failure	20	Lat: zzz, Lon: zzz
NFT-004	2023-01-15	Success	99	Lat: www, Lon: www

[図12]

図 12

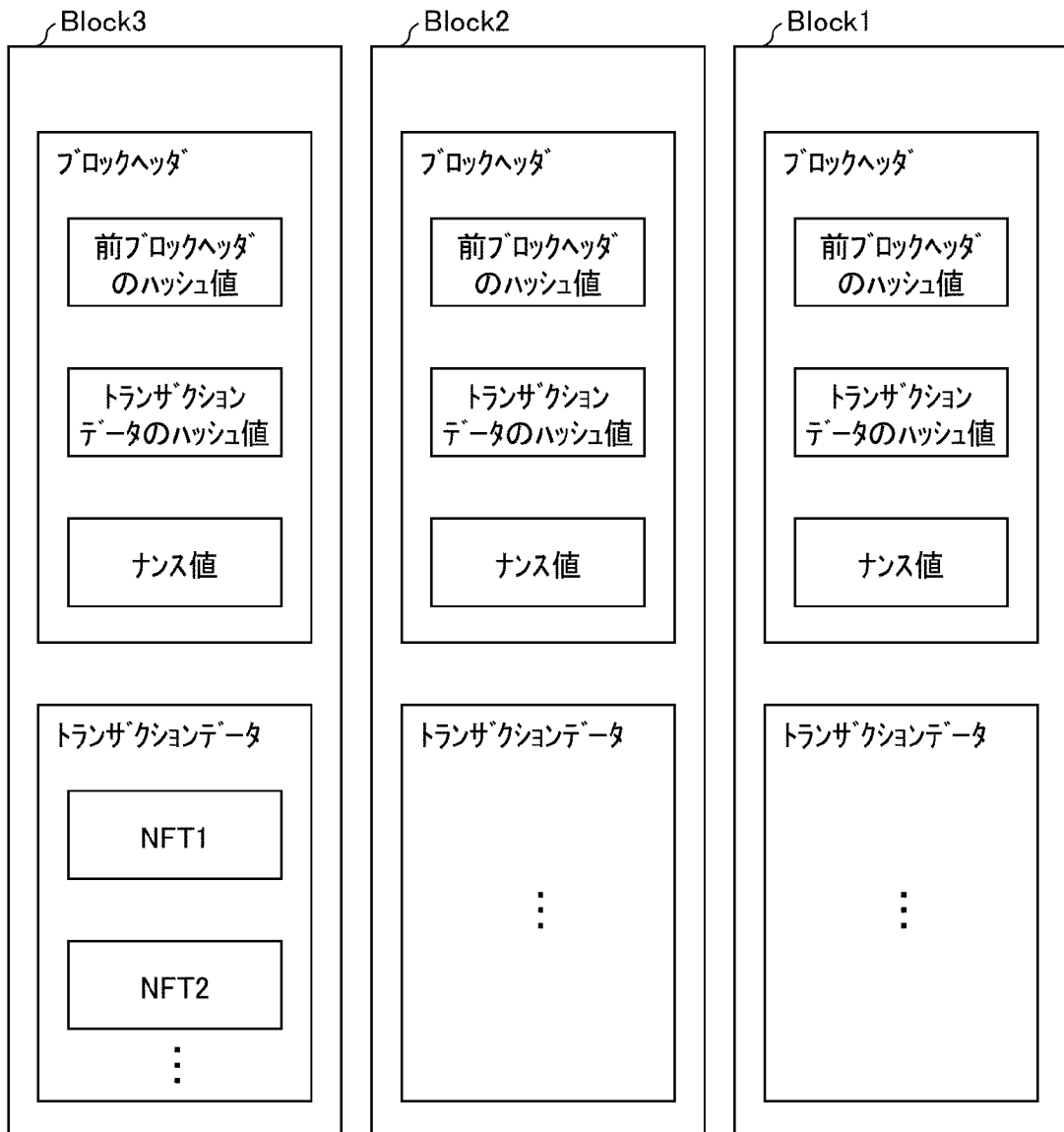
非代替データの構成例2

NI		LI		NFT	
NFT ID		location			
NFT-001		ipfs://xxxxx			
NFT-002		ipfs://yyyyy			
NFT-003		ipfs://zzzzz			
NFT-004		ipfs://wwwww			

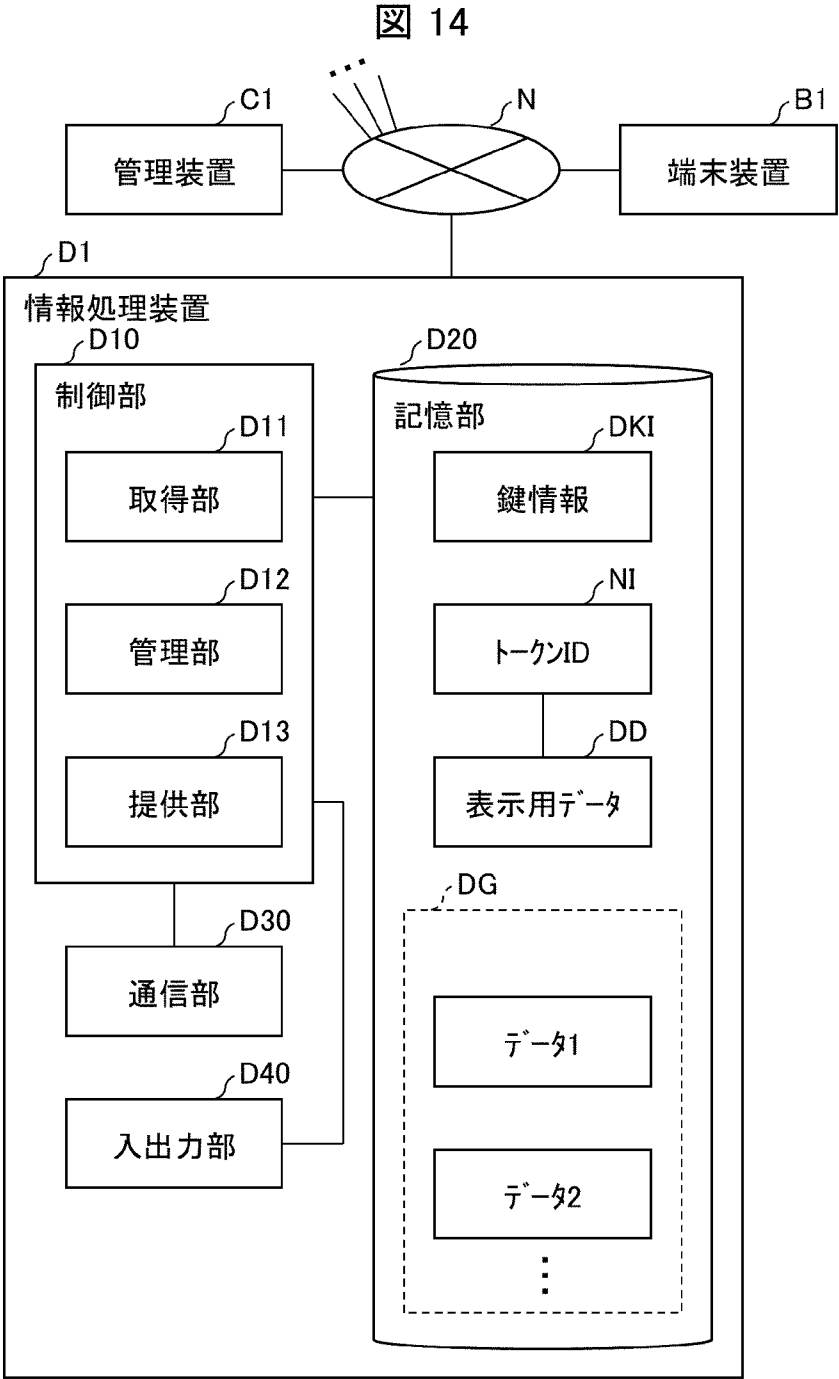
location ipfs://xxxxx	TI	ECR		PI	BI
	Time_stamp	Biometric Result	Biometric Score	Position	
	2023-04-01	Success	97	Lat: xxx, Lon: xxx	
location ipfs://yyyyy	Time_stamp	Biometric Result	Biometric Score	Position	
	2023-03-20	Success	95	Lat: yyy, Lon: yyy	
location ipfs://zzzzz	Time_stamp	Biometric Result	Biometric Score	Position	
	2023-02-28	Failure	20	Lat: zzz, Lon: zzz	
location ipfs://wwwww	Time_stamp	Biometric Result	Biometric Score	Position	
	2023-01-15	Success	99	Lat: www, Lon: www	

[図13]

図 13



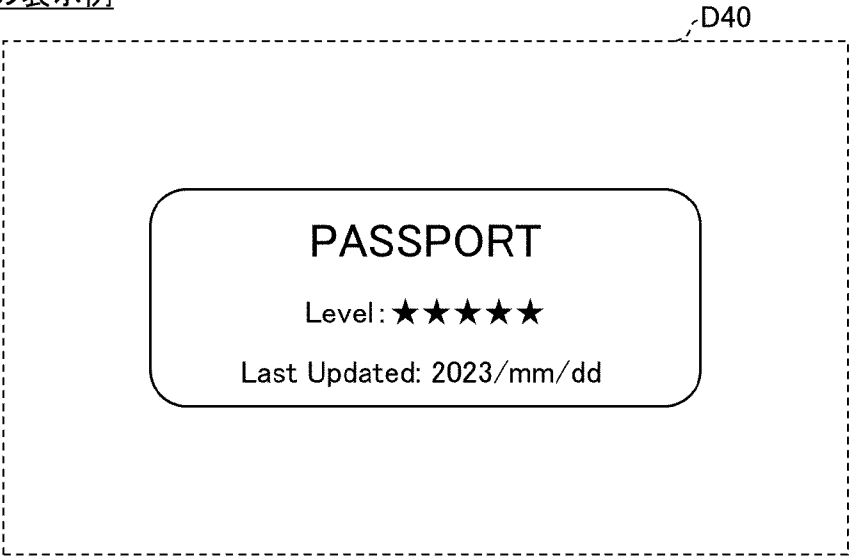
[図14]



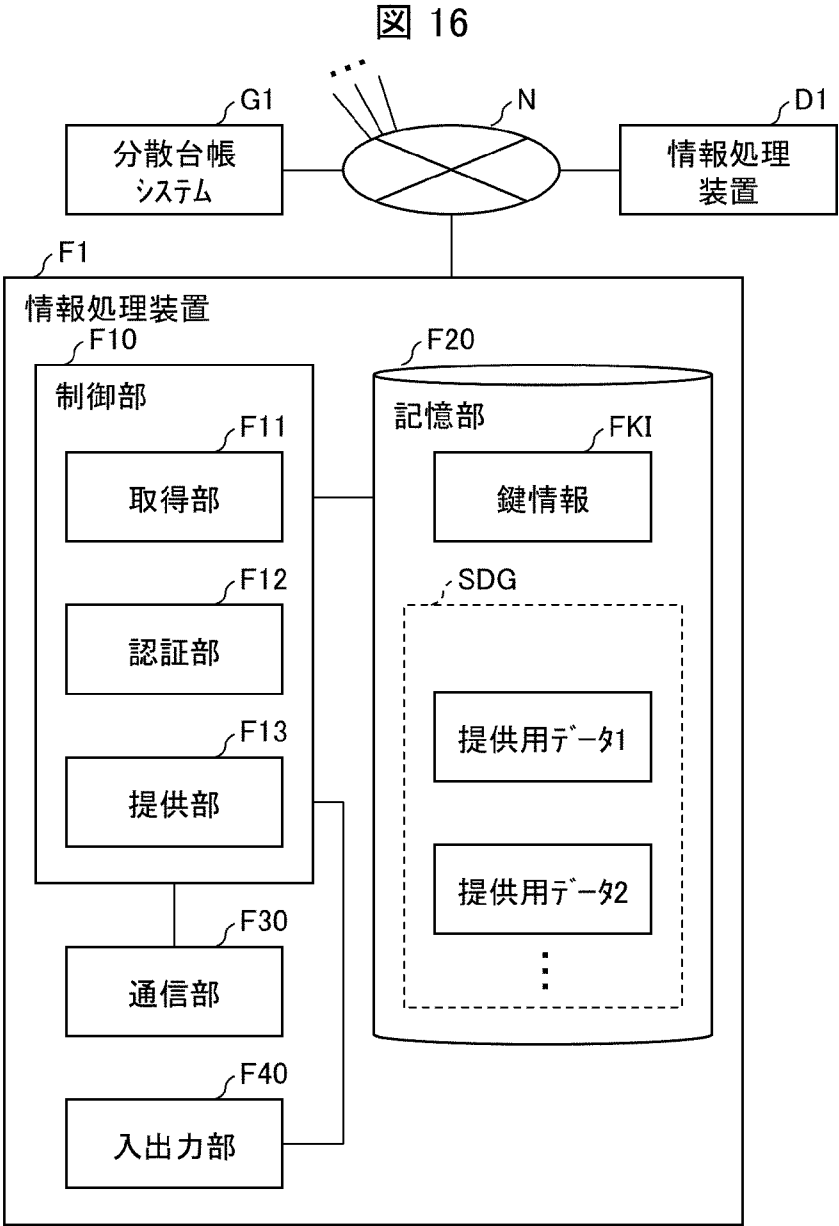
[図15]

図 15

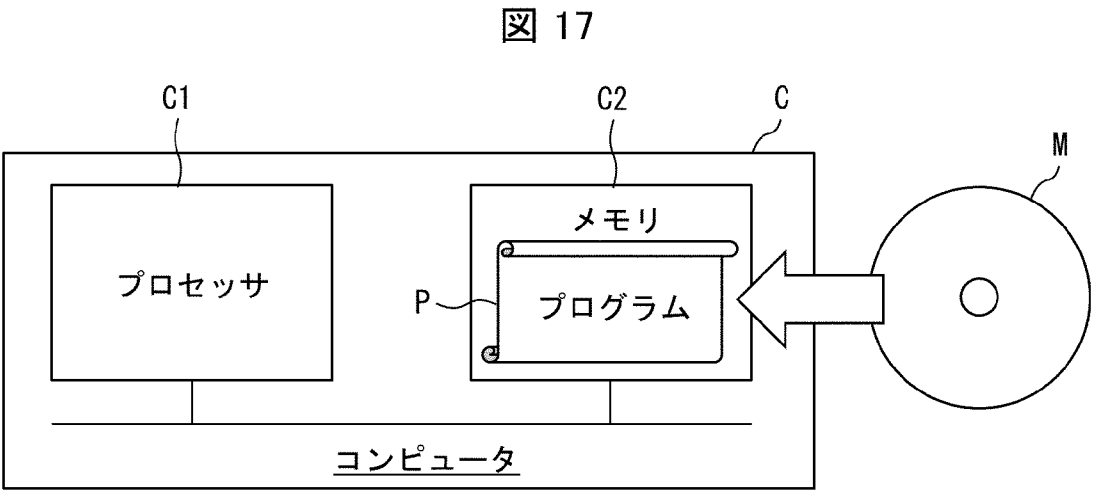
表示用データの表示例



[図16]



[図17]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/021160

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/45**(2013.01)i; **G06F 21/31**(2013.01)i; **H04L 9/32**(2006.01)i

FI: G06F21/45; G06F21/31; H04L9/32 200Z

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)

G06F21/45; G06F21/31; 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 1971-2023
 Registered utility model specifications of Japan 1996-2023
 Published registered utility model applications of Japan 1994-2023

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.
X	US 2023/0027380 A1 (SUTTON-SHEARER, D. et al.) 26 January 2023 (2023-01-26) paragraphs [0005], [0027], [0034], [0064], [0068]-[0069], [0073], [0076]-[0077], [0082], [0096], [0098], fig. 2-3	1-4, 9-11, 13, 15-16
Y		5, 8, 12
A		6-7, 14
Y	WO 2008/050765 A1 (IHC CORP.) 02 May 2008 (2008-05-02) abstract, paragraph [0063]	5, 12
Y	WO 2021/132483 A1 (SIVIRA INC.) 01 July 2021 (2021-07-01) paragraphs [0074]-[0077]	8
A	JP 2022-133057 A (NTT TECHNOCROSS CORP.) 13 September 2022 (2022-09-13) paragraph [0051]	6
A	JP 2023-058149 A (SQUARE ENIX CO., LTD.) 25 April 2023 (2023-04-25) paragraph [0136]	7

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“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)

“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

“T” 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

“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

“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

“&” document member of the same patent family

Date of the actual completion of the international search

16 August 2023

Date of mailing of the international search report

29 August 2023

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915
 Japan

Authorized officer

Telephone No.

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Document 1: US 2023/0027380 A1 (SUTTON-SHEARER, D. et al.) 26 January 2023 (2023-01-26), paragraphs [0005], [0027], [0034], [0064], [0068]-[0069], [0073], [0076]-[0077], [0082], [0096], [0098], fig. 2-3

The claims are classified into the following two inventions.

Invention 1: claims 1-5, 12, and the portions of claims 6-8 and 13-14 relating to the feature in which "an existence confirmation result regarding the existence of a subject and associated with a non-fungible token includes a score pertaining to said existence confirmation".

Claims 1-4 lack novelty in light of document 1 and thus do not have a special technical feature. However, claim 5 which depends from claim 1 has the special technical feature in which "an existence confirmation result regarding the existence of a subject and associated with a non-fungible token includes a score pertaining to said existence confirmation", and the portions of claims 6-8 that refer back to the abovementioned portion of claim 5, claim 12, and the portions of claims 13-14 that refer back to the abovementioned portion of claim 12 have the same special technical feature. Therefore, claims 1-5, 12, and the abovementioned portions in claims 6-8 and 13-14 are classified as invention 1.

Also, the portions other than the abovementioned in claims 6-8 depend from claim 1 and are inventively linked to claim 1, and thus are classified as invention 1.

Furthermore, claims 15-16 are substantially identical to or similarly closely related to claim 1, and thus are classified as invention 1.

Invention 2: claims 9-11 and the portions of claims 13-14 not classified as invention 1

Claims 9-11 and the abovementioned portions of claims 13-14 cannot be said to have the same or corresponding special technical feature as claim 5 classified as invention 1.

Also, claims 9-11 and the abovementioned portions of claims 13-14 do not depend from claim 1. Furthermore, claims 9-11 and the abovementioned portions of claims 13-14 are not substantially identical to or similarly closely related to any of the claims classified as invention 1.

Therefore, claims 9-11 and the abovementioned portions of claims 13-14 cannot be classified as invention 1.

Furthermore, claims 9-11 and the abovementioned portion of claim 13 lack novelty in light of document 1, and thus do not have a special technical feature. However, the abovementioned portion of claim 14 which depends from claim 9 has the special technical feature of an "information processing device comprising an acquisition means that acquires an existence confirmation result, which is a confirmation result regarding the existence of a subject, and a management means that manages the existence confirmation result in association with a non-fungible token, wherein a condition of the authentication processing is optimized on the basis of a machine learning model that has learned a relationship between the existence confirmation result of the subject and a label". Therefore, claims 9-11 and the abovementioned portions of claims 13-14 are classified as invention 2.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/021160

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/021160

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US	2023/0027380	A1	26 January 2023	(Family: none)	
WO	2008/050765	A1	02 May 2008	JP 2008-269556	A
WO	2021/132483	A1	01 July 2021	EP 4083806	A1
				paragraphs [0074]-[0077]	
				US 2023/0091451	A1
				CN 114902195	A
JP	2022-133057	A	13 September 2022	(Family: none)	
JP	2023-058149	A	25 April 2023	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 21/45(2013.01)i; G06F 21/31(2013.01)i; H04L 9/32(2006.01)i FI: G06F21/45; G06F21/31; H04L9/32 200Z		
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）） G06F21/45; G06F21/31; 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 1971-2023年 日本国実用新案登録公報 1996-2023年 日本国登録実用新案公報 1994-2023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
X	US 2023/0027380 A1 (SUTTON-SHEARER, Drake et al.) 26.01.2023 (2023-01-26) 段落[0005], [0027], [0034], [0064], [0068]-[0069], [0073], [0076]- [0077], [0082], [0096], [0098], 図2-3	1-4, 9-11, 13, 15-16
Y		5, 8, 12
A		6-7, 14
Y	WO 2008/050765 A1 (株式会社 IHC) 02.05.2008 (2008-05-02) [要約], 段落[0063]	5, 12
Y	WO 2021/132483 A1 (シビラ株式会社) 01.07.2021 (2021-07-01) 段落[0074]-[0077]	8
A	JP 2022-133057 A (NTTテクノクロス株式会社) 13.09.2022 (2022-09-13) 段落[0051]	6
A	JP 2023-058149 A (株式会社スクウェア・エニックス) 25.04.2023 (2023-04-25) 段落[0136]	7
☐ 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、一般的な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抵 触するものではなく、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 16.08.2023	国際調査報告の発送日 29.08.2023	
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 小林 秀和 5S 3449 電話番号 03-3581-1101 内線 3546	

第III欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるこの国際調査機関は認めた。

文献1：US 2023/0027380 A1 (SUTTON-SHEARER, Drake et al.) 26.01.2023(2023-01-26)
段落[0005], [0027], [0034], [0064], [0068]-[0069], [0073], [0076]-[0077],
[0082], [0096], [0098], 図2-3

請求の範囲は、以下の2つの発明に区分される。

（発明1）請求項1～5、12、及び請求項6～8、13～14のうち「非代替トークンと関連付けられた、対象者の実存性に関する実存性確認結果には、当該実存性確認に関するスコアが含まれる」ことに
関する部分

請求項1～4は、文献1により新規性が欠如しているため、特別な技術的特徴を有しない。しかしながら、請求項1の従属請求項である請求項5は、「非代替トークンと関連付けられた、対象者の実存性に関する実存性確認結果には、当該実存性確認に関するスコアが含まれる」という特別な技術的特徴を有しており、請求項6～8のうち、請求項5の上記部分を引用している部分、請求項12、及び請求項13～14のうち、請求項12の上記部分を引用している部分も、これと同一の特別な技術的特徴を有している。したがって、請求項1～5、12、及び請求項6～8、13～14における上記部分を発明1に区分する。

また、請求項6～8における上記以外の部分は、請求項1の従属請求項であり、請求項1に対して発明の連関を有しているので、発明1に区分する。

さらに、請求項15～16は、請求項1と実質同一又はそれに準ずる関係にあるので、発明1に区分する。

（発明2）請求項9～11、及び請求項13～14のうち発明1に区分されない部分

請求項9～11、及び請求項13～14の上記部分は、発明1に区分された請求項5と、同一の又は対応する特別な技術的特徴を有しているとはいえない。

また、請求項9～11、及び請求項13～14の上記部分は、請求項1の従属請求項ではない。さらに、請求項9～11、及び請求項13～14の上記部分は、発明1に区分されたいずれの請求項に対しても実質同一又はそれに準ずる関係にはない。

したがって、請求項9～11、及び請求項13～14の上記部分は発明1に区分できない。

さらに、請求項9～11、及び請求項13の上記部分は、文献1により新規性が欠如しているため、特別な技術的特徴を有しない。しかしながら、請求項9の従属請求項である請求項14の上記部分は、「対象者の実存性に関する確認結果である実存性確認結果を取得する取得手段と、前記実存性確認結果を非代替トークンと関連付けて管理する管理手段とを備え、前記対象者の実存性確認結果とラベルとの関係を学習した機械学習モデルに基づいて、前記認証処理の条件を最適化する、情報処理装置」という特別な技術的特徴を有している。したがって、請求項9～11、及び請求項13～14の上記部分を発明2に区分する。

第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

追加調査手数料の異議の
申立てに関する注意

- ☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。
- ☐ 追加調査手数料の納付はあったが、異議申立てはなかった。

国際調査報告
 パテントファミリーに関する情報

国際出願番号

PCT/JP2023/021160

引用文献			公表日	パテントファミリー文献	公表日
US	2023/0027380	A1	26.01.2023	(ファミリーなし)	
WO	2008/050765	A1	02.05.2008	JP 2008-269556	A
WO	2021/132483	A1	01.07.2021	EP 4083806	A1
				段落[0074]-[0077]	
				US 2023/0091451	A1
				CN 114902195	A
JP	2022-133057	A	13.09.2022	(ファミリーなし)	
JP	2023-058149	A	25.04.2023	(ファミリーなし)	