

明 細 書

発明の名称：

認証コード発行システム、認証コード発行方法、端末装置、及び、認証コード利用方法

技術分野

[0001] 本発明は、認証コード発行システム、認証コード発行方法、端末装置、及び、認証コード利用方法などに関する。

背景技術

[0002] 近年、WWW (w o r l d w i d e w e b) を介したインターネットバンクサービス又はオンラインストア等のサービスにおいて、所謂、なりすましに代表される不正使用が急増している。

[0003] そこで、最近では、取引先又は取引元の位置情報を用いて取引元又は取引先の真正性を判定し、当該電子商取引の承認をする承認処理を実行する構成を有している（例えば、特許 7 3 2 1 4 1 8 号公報）。

発明の概要

発明が解決しようとする課題

[0004] しかしながら、特許文献 1 のシステムであっては、承認処理を行う際に、個人情報の取得に配慮しつつも、本人認証と匿名性の確保の相反する目的効果に関しては改良の余地がある。

[0005] 本発明は、上記課題を解決するためになされたものであり、その目的は、簡易な構成によって匿名性を担保しつつも本人認証としての信頼性が担保された認証コードを発行することが可能な認証コード発行システムなどを提供することにある。

[0006] また、本発明は、上記課題を解決するためになされたものであり、その目的は、このような特性を有する認証コードを用いることによって匿名性を担保して信頼性が高く、かつ、かつ、ネットワークサービスを利用した仮想空間におけるユーザの経済活動などの各種の活動を実空間と遜色なく実現する

ことが可能な端末装置などを提供することにある。

課題を解決するための手段

- [0007] (1) 本発明の第1の態様に係る認証コード発行システムは、
仮想空間におけるユーザの識別情報に実空間における当該ユーザの存在を示す実体情報を対応付けた固有の認証コードを発行する認証コード発行システムであって、
前記仮想空間内のユーザの識別情報を仮想識別情報として取得する仮想識別情報取得手段と、
前記ユーザが保持する端末装置から当該端末装置の現在位置を示す現在位置情報と、当該現在位置を特定した際の時刻を示す時刻情報と、を取得する位置情報取得手段と、
前記取得された仮想識別情報と、前記実体情報としての前記取得された現在位置情報及び時刻情報と、を対応付けて、前記ユーザ固有の識別情報のコードであって、所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードを発行する認証コード発行手段と、
前記発行された認証コードを前記ユーザに帰属させた上で所与のデータベースに登録する登録手段と、
を備える、構成を有している。
- [0008] (2) また、本発明の第2の態様に係る端末装置は、
仮想空間におけるユーザの識別情報に実空間における当該ユーザの存在を示す実体情報を対応付けた固有の認証コードを利用する端末装置であって、
前記仮想空間内のユーザの識別情報を仮想識別情報として受け付ける受付手段と、
現在位置を特定するとともに、当該現在位置を特定した際の時刻を特定する特定手段と、
前記受け付けられた仮想識別情報と、前記実体情報としての前記特定された現在位置を示す現在位置情報及び当該現在位置を特定した時刻を示す時刻

情報と、を対応付けて、サーバシステムに所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードの発行を要求する要求手段と、

前記発行要求に基づいて発行され、かつ、前記ユーザに帰属させた上で所与のデータベースに登録された認証コードを用いて、前記ネットワークサービスに関連するサービス関連処理を実行するサービス関連処理実行手段と、を備える、構成を有している。

[0009] (3) また、本発明の第3の態様に係る認証コード利用方法は、

仮想空間におけるユーザの識別情報に実空間における当該ユーザの実在することを示す実体情報を対応付けた固有の認証コードを利用する認証コード利用方法であって、

前記仮想空間内のユーザの識別情報を仮想識別情報として受け付けをし、現在位置を特定するとともに、当該現在位置を特定した際の時刻を特定し、

前記受け付けられた仮想識別情報と、前記実体情報としての前記特定された現在位置を示す現在位置情報及び当該現在位置を特定した時刻を示す時刻情報と、を対応付けて、サーバシステムに所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードの発行を要求し、

前記発行要求に基づいて発行され、かつ、前記ユーザに帰属させた上で所与のデータベースに登録された認証コードを用いて、前記ネットワークサービスに関連するサービス関連処理を実行する、構成を有している。

[0010] (4) また、本発明の第4の態様に係る認証コード発行方法は、

仮想空間におけるユーザの識別情報に実空間における当該ユーザの実在することを示す実体情報を対応付けた固有の認証コードを発行する認証コード発行方法であって、

前記仮想空間内のユーザの識別情報を仮想識別情報として取得し、

前記ユーザが保持する端末装置から当該端末装置の現在位置を示す現在位置情報と、当該現在位置を特定した際の時刻を示す時刻情報と、を取得し、

前記取得された仮想識別情報と、前記実体情報としての前記取得された現在位置情報及び時刻情報と、を対応付けて、前記ユーザ固有の識別情報のコードであって、所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードを発行し、及び、

前記発行された認証コードを前記ユーザに帰属させた上で所与のデータベースに登録すること、

を含む、構成を有している。

図面の簡単な説明

[0011] [図1]図1は、一実施形態におけるネットワーク型本人認証システムの構成を示すシステム構成図である。

[図2]図2は、一実施形態のトークン発行用サーバ装置の構成を示す機能ブロック図の一例である。

[図3]図3は、一実施形態の端末装置の構成の一例を示す機能ブロック図である。

[図4]図4は、一実施形態のトークン発行用サーバ装置において実行される認証コード発行処理及び端末装置によって実行される認証コード発行要求処理について説明するための図である。

[図5]図5は、一実施形態の本実施形態の端末装置によって実行される認証コード発行要求処理の動作を示すフローチャートである。

[図6]図6は、一実施形態の本実施形態の端末装置によって実行される認証コード発行要求処理の動作を示すフローチャートである。

[図7]図7は、一実施形態のトークン発行用サーバ装置によって実行される認証コード発行処理の動作を示すフローチャートである。

[図8]図8は、一実施形態の変形例2におけるネットワーク型本人認証システムの構成を示すシステム構成図である。

[図9]図9は、一実施形態の変形例2における情報処理サーバ装置において実行されるユーザのモーションキャプチャ処理について説明するための図である。

[図10]図10は、一実施形態の変形例2におけるトークン発行用サーバ装置において実行されるユーザのモーションキャプチャー処理について説明するための図である。

発明を実施するための形態

[0012] (1) 本発明の一実施の形態は、

仮想空間におけるユーザの識別情報に実空間における当該ユーザの実在することを示す実体情報を対応付けた固有の認証コードを発行する認証コード発行システムであって、

前記仮想空間内のユーザの識別情報を仮想識別情報として取得する仮想識別情報取得手段と、

前記ユーザが保持する端末装置から当該端末装置の現在位置を示す現在位置情報と、当該現在位置を特定した際の時刻を示す時刻情報と、を取得する位置情報取得手段と、

前記取得された仮想識別情報と、前記実体情報としての前記取得された現在位置情報及び時刻情報と、を対応付けて、前記ユーザ固有の識別情報のコードであって、所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードを発行する認証コード発行手段と、

前記発行された認証コードを前記ユーザに帰属させた上で所与のデータベースに登録する登録手段と、を備える、構成を有している。

[0013] この構成により、本発明の一実施の形態は、認証コードを介して仮想空間内の識別情報（すなわち、ID）に実空間においての実体を証明すべき情報を対応付けることができるので、仮想空間内におけるユーザの活動であっても、当該認証コードを用いることによって実在性を担保することができる。

[0014] すなわち、本発明の一実施の形態は、匿名性を担保しつつも本人認証としての信頼性が担保された認証コードを発行することができるので、匿名性を担保して本人認証としての信頼性が高く、かつ、ネットワークサービスを利用した仮想空間におけるユーザの経済活動などの各種の活動を実現することができる。

- [0015] なお、「本人確認用の非代替性の認証コード」とは、例えば、S B T (Soul Bound Token) などの一身帰属性のトークンであってもよいし、電子証明書的なデジタルコードであってもよい。
- [0016] また、「ユーザに帰属させた上で」とは、ネットワークで利用可能でありつつも、他人に譲渡不能であることを示す。
- [0017] (2) また、本発明の一実施の形態は、
前記認証コード発行手段が、
使用期間に制限のある前記認証コードを発行する、構成を有している。
- [0018] この構成により、本発明の一実施の形態は、例えば、1時間又は1日など発行後に短時間で認証コードを使用不可にすることができるので、認証コードが発行される毎に、ユーザの最新の位置を認識することができるとともに、その結果、ユーザが実在するか否かを定期的に認識することができる。
- [0019] また、本発明の一実施の形態は、ユーザの位置又はユーザの身体的な一部の部位をトレースすることによってユーザの活動範囲が適正か否か、又は、本人確認が継続的に行われているかをも判定することができるので、ユーザの真正性を証明すること、又は、継続的に真正性を証明することができる。
- [0020] (3) また、本発明の一実施の形態は、
前記登録手段が、
前記認証コードを暗号化し、当該暗号化された認証コードをネットワーク上の複数の前記データベースに分散登録する、構成を有している。
- [0021] この構成により、本発明の一実施の形態は、例えば、ブロックチェーンなどの改ざんが困難な分散型台帳技術を用いて任所コードを複数のデータベースに登録することができるので、本人認証としての信頼性を向上させることができる。
- [0022] なお、「暗号化された認証コードをネットワーク上の複数のデータベースに分散登録する」とは、例えば、ブロックチェーン技術などを用いて中央集権的ではなく、改ざんを防ぎ、分散管理されることを示す。
- [0023] (4) また、本発明の一実施の形態は、

前記認証コード発行手段が、

少なくとも前記現在位置情報を前記ユーザの生体情報として利用して前記本人確認用の認証コードを発行する、構成を有している。

[0024] この構成により、本発明の一実施の形態は、現在位置情報を用いて的確に本人認証を行うことができる。

[0025] なお、「ユーザの生体情報として利用して」とは、ユーザの位置そのものだけでなく、例えば、位置情報を用いることによってユーザの特徴的な動き（モーション）を認識し、当該認識したユーザの動きを生体情報として利用することも含む。

[0026] （５）また、本発明の一実施の形態は、

記憶手段に記憶されている前記ユーザ毎に該当するユーザに関するユーザ情報を管理する手段であって、前記ユーザの身体の一部の部位の動きの特徴を示すモーション特徴情報を、当該ユーザ情報として、管理する情報管理手段を更に備え、

前記認証コード発行手段が、

複数の前記現在位置情報に基づいて前記ユーザの身体の一部の部位の軌道を部位軌道情報として検出し、当該検出された部位軌道情報に基づいて前記ユーザの身体の動きを示すモーション情報を特定し、

前記認証コードの発行要求したユーザの前記モーション特徴情報と、前記取得されたモーション情報と、に基づいて、当該対象ユーザの身体的な部位の動きの同一性を判定する判定処理を実行し、

前記判定処理において、前記モーション特徴情報によって示される部位の動きと、前記モーション情報によって示される対象ユーザの身体的な部位の動きと、が同一又は同一とみなされる動きであると判定された場合に、前記対象ユーザの本人認証を行う認証処理を実行し、

前記認証処理によって前記本人認証が成功の場合に、前記本人確認用の認証コードを発行する、構成を有している。

[0027] この構成により、本発明の一実施の形態は、位置情報を用いることによっ

てユーザの特徴的な動き（モーション）を認識し、当該認識したユーザの動きを生体情報として利用することができるので、匿名性を担保しつつも本人認証としての信頼性が担保された認証コードを発行することができる。

[0028] したがって、本発明の一実施の形態は、匿名性を担保して本人認証としての信頼性が高く、かつ、ネットワークサービスを利用した仮想空間におけるユーザの経済活動などの各種の活動を実現することができる。

[0029] なお、「モーション特徴情報」とは、身体的な部位の動きに関する特徴情報を示し、例えば、例えば、手足・頭部・上体などの可動範囲、若しくは、左右差、又は、癖などの変則的な動き若しくは部位の位置などが示される。

[0030] また、「ユーザの身体の一部の部位」には、例えば、手首、足首、頭頂部、額、肘及び膝の他に、各関節などの身体において主に可動する部位、又は、可動にあたり基準（中心）となる部位が含まれる。

[0031] そして、「部位軌道情報」とは、0.1秒から1.0秒などの所定のタイミング毎に取得した位置情報を実空間において連続的な位置変化として軌道化した情報を示す。

[0032] さらに、「身体の動き」には、例えば、腕（左右双方又は片方）を回す（種々の回し方含む。）・上げる・下げる、手掌（左右双方又は片方）を振る、頭部を振る（前後、左右）・回す、足（左右どちらか）を上げる（種々の上げ方）・下げる、又は、上体を左右に動かす・曲げるなどの各部位又は複合的な部位の動きだけでなく、歩く、ジャンプする、姿勢を変える（しゃがむ、起こす、横たわるなど）動きなどの身体全体の動きも含まれる。

[0033] （6）また、本発明の一実施の形態は、

仮想空間におけるユーザの識別情報に実空間における当該ユーザの実在することを示す実体情報を対応付けた固有の認証コードを利用する端末装置であって、

前記仮想空間内のユーザの識別情報を仮想識別情報として受け付ける受付手段と、

現在位置を特定するとともに、当該現在位置を特定した際の時刻を特定す

る特定手段と、

前記受け付けられた仮想識別情報と、前記実体情報としての前記特定された現在位置を示す現在位置情報及び当該現在位置を特定した時刻を示す時刻情報と、を対応付けて、サーバシステムに所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードの発行を要求する要求手段と、

前記発行要求に基づいて発行され、かつ、前記ユーザに帰属させた上で所与のデータベースに登録された認証コードを用いて、前記ネットワークサービスに関連するサービス関連処理を実行するサービス関連処理実行手段と、を備える、構成を有している。

[0034] この構成により、本発明の一実施の形態は、認証コードを介して仮想空間内の識別情報（すなわち、ID）に実空間においての実体を証明すべき情報を対応付けることができるので、仮想空間内におけるユーザの活動であっても、当該認証コードを用いることによって実在性を担保することができる。

[0035] すなわち、本発明の一実施の形態は、匿名性を担保しつつも本人認証としての信頼性が担保された認証コードを利用してネットワークサービスを楽しむことができるので、仮想空間におけるユーザの経済活動などの各種の活動を実空間と遜色なく実現することができる。

[0036] （7）また、本発明の一実施の形態は、

前記認証コードが使用期限を経過しているか否かを判定する使用期限判定処理を実行する判定手段を更に備え、

前記要求手段が、

前記使用期限判定処理の結果、前記認証コードの使用期限が経過していると判定された場合には、再取得した現在位置情報及び時刻情報に基づいて、前記サーバシステムに認証コードの発行を要求する、構成を有している。

[0037] この構成により、本発明の一実施の形態は、使用期限を設けることにより所定の期間毎にユーザの正規性を証明することができるので、情報の漏洩又はなりすましなどの不正利用を的確に防止することができる。

[0038] (8) また、本発明の一実施の形態は、

前記サービス関連処理実行手段が、

所与のデータベースとして、ネットワーク上の複数のデータベースに暗号化して分散登録された認証コードを用いて、前記ネットワークサービスに関連するサービス関連処理を実行する、構成を有している。

[0039] この構成により、本発明の一実施の形態は、例えば、ブロックチェーンなどの改ざんが困難な分散型台帳技術を用いて認証コードを複数のデータベースに登録することができるので、本人認証としての信頼性を向上させることができる。

[0040] (9) また、本発明の一実施の形態は、

仮想空間におけるユーザの識別情報に実空間における当該ユーザの実在することを示す実体情報を対応付けた固有の認証コードを利用する認証コード利用方法であって、

前記仮想空間内のユーザの識別情報を仮想識別情報として受け付けし、

現在位置を特定するとともに、当該現在位置を特定した際の時刻を特定し

、
前記受け付けられた仮想識別情報と、前記実体情報としての前記特定された現在位置を示す現在位置情報及び当該現在位置を特定した時刻を示す時刻情報と、を対応付けて、サーバシステムに所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードの発行を要求し、

前記発行要求に基づいて発行され、かつ、前記ユーザに帰属させた上で所与のデータベースに登録された認証コードを用いて、前記ネットワークサービスに関連するサービス関連処理を実行する、
構成を有している。

[0041] この構成により、本発明の一実施の形態は、認証コードを介して仮想空間内の識別情報（すなわち、ID）に実空間においての実体を証明すべき情報を対応付けることができるので、仮想空間内におけるユーザの活動であっても、当該認証コードを用いることによって実在性を担保することができる。

- [0042] すなわち、本発明の一実施の形態は、匿名性を担保しつつも本人認証としての信頼性が担保された認証コードを利用してネットワークサービスを享受することができるので、仮想空間におけるユーザの経済活動などの各種の活動を実空間と遜色なく実現することができる。
- [0043] 特に、本発明の一実施の形態は、身元確認情報についてユーザ本人以外によってアクセスすることができないように登録すれば、認証コード発行システムを含めて他者に身元確認情報を知られることなく、本人確認することができるので、その匿名性を担保することができる。
- [0044] (10) また、本発明の一実施の形態は、
仮想空間におけるユーザの識別情報に実空間における当該ユーザの実在することを示す実体情報を対応付けた固有の認証コードを発行する認証コード発行方法であって、
前記仮想空間内のユーザの識別情報を仮想識別情報として取得し、
前記ユーザが保持する端末装置から当該端末装置の現在位置を示す現在位置情報と、当該現在位置を特定した際の時刻を示す時刻情報と、を取得し、
前記取得された仮想識別情報と、前記実体情報としての前記取得された現在位置情報及び時刻情報と、を対応付けて、前記ユーザ固有の識別情報のコードであって、所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードを発行し、
前記発行された認証コードを前記ユーザに帰属させた上で所与のデータベースに登録する、
構成を有している。
- [0045] この構成により、本発明の一実施の形態は、認証コードを介して仮想空間内の識別情報（すなわち、ID）に実空間においての実体を証明すべき情報を対応付けることができるので、仮想空間内におけるユーザの活動であっても、当該認証コードを用いることによって実在性を担保することができる。
- [0046] すなわち、本発明の一実施の形態は、匿名性を担保しつつも本人認証としての信頼性が担保された認証コードを発行することができるので、匿名性を

担保して本人認証としての信頼性が高く、かつ、ネットワークサービスを利用した仮想空間におけるユーザの経済活動などの各種の活動を実現することができる。

[0047] 以下、本発明に係る実施形態について、図面を参照しながら説明する。

[0048] なお、以下に説明する実施の形態は、身元確認事業者によって身元確認済みで、かつ、位置情報を取得していることを前提に一身帰属性のトークン（認証コード）としてS B T（Soul Bound Token）を発行するトークン発行用サーバ装置と、当該S B Tを利用して所与の取引を行う端末装置とを有するネットワーク型本人認証システムに対して本願の認証コード発行システム又は端末装置などを適用した場合の実施形態である。

[0049] また、本実施形態においては、本人認証を行うデジタルコードとしてS B Tを用いて説明するが、N F T（Non Fungible Token）などの本人認証済みの譲渡不能な固有の認証コードであれば、これに限られない。

[0050] [1] ネットワーク型本人認証システムの概要

まず、図 1 を用いて本実施形態のネットワーク型本人認証システム S の概要及びシステム構成について説明する。

[0051] なお、図 1 は、本実施形態におけるネットワーク型本人認証システム S の構成を示すシステム構成図である。

[0052] また、図が煩雑になることを防止するために、図 1 においては、一部のユーザによって利用される端末装置 2 0 のみを示している。すなわち、実際のネットワーク型本人認証システム S においては、図 1 に示しているよりも多数の端末装置 2 0 が存在している。

[0053] （システム概要）

本実施形態のネットワーク型本人認証システム S は、図 1 に示すように、仮想空間におけるユーザの識別情報に実空間における当該ユーザの存在することを示す実体情報を対応付けた固有の認証コードとしてS B Tを発行し、当該発行されたS B Tを用いてユーザの本人認証を含む各種のネットワークサービスを適切に享受することが可能なシステムである。

[0054] 特に、ネットワーク型本人認証システムSは、S B Tを介して仮想空間内の識別情報（すなわち、I D）に実空間においての実体を証明すべき情報（具体的には、現在位置情報とそれを特定した際の時刻情報）を対応付けることによって、仮想空間内におけるユーザの活動であっても、当該認証コードを用いることによって実在性を担保することが可能な構成を有している。

[0055] （システム構成）

本実施形態のネットワーク型本人認証システムSは、図1に示すように、S B Tを発行するトークン発行用サーバ装置10と、インターネットなどのネットワークを介してトークン発行用サーバ装置10に接続され、GPS衛星70から送信された衛星信号に基づいて現在位置を特定する端末装置20（例えば、端末装置20A、20B、20C）と、身元確認事業者によって管理され、身元確認を行う際に用いる身元確認用サーバ装置30と、ブロックチェーン技術を用いて各ユーザのS B Tが登録される複数のデータベース40と、所与のネットワークサービスを管理するための各種の処理を実行するサービス管理サーバ装置50と、から構成される。

[0056] トークン発行用サーバ装置10は、例えば、API（アプリケーションプログラミングインタフェース）や所定のプラットフォーム等を利用してS B Tの発行に関する各種の処理を実行する情報処理装置である。

[0057] 特に、トークン発行用サーバ装置10は、端末装置20と連動し、仮想空間における各ユーザの識別情報（具体的には、仮想空間用I D）と、当該端末装置20から送信された当該端末装置20の現在位置を示す現在位置情報及び当該現在位置を特定した際の時刻を示す時刻情報と、に対応付けて前記ユーザ固有の識別情報のコードであって、所与のネットワークサービスを利用するための本人確認用の非代替性の認証コード（すなわち、S B T）を発行する。

[0058] また、トークン発行用サーバ装置10は、1つの（装置、プロセッサ）で構成されていてもよいし、複数の（装置、プロセッサ）で構成されていてもよい。

- [0059] 端末装置20は、ユーザによって利用されるPC（パーソナルコンピュータ）、タブレット型情報通信端末装置、スマートフォン、携帯型電話器、又は、HMDなどの情報処理装置によって構成される通信端末装置である。
- [0060] また、端末装置20は、インターネット（WAN）やLANなどのネットワークを介してトークン発行用サーバ装置10に接続可能な装置であり、トークン発行用サーバ装置10と有線又は無線によって通信回線を確立して各種のデータの授受を行う構成を有している。
- [0061] また、端末装置20は、ユーザによって入力された入力情報などのトークン発行用サーバ装置10との通信を行うための通信制御機能、端末装置20の現在位置（すなわち、現在位置情報）を取得する機能、身元確認用サーバ装置30と連動して身元確認に関する処理（以下、「身元確認処理」という。）を実行する機能、身元確認情報をデータベース40に登録する機能、及び、トークン発行用サーバ装置10から送信されたSBTを用いてサービス管理サーバ装置50又は他の端末装置20とのサービスを享受し、又は、所与の取引を実行するための機能を備える構成を有している。
- [0062] 特に、端末装置20は、GPS（Global Positioning System）を含む、GNSS（Global Navigation Satellite System）などのGPS衛星70との通信、携帯型電話器用の基地局BSとの通信、又は、Wi-Fiなどの無線ルータとの近距離無線通信などを用いた高精度の測位を行うシステムと連動し、端末装置20の現在位置情報を取得する構成を有している。
- [0063] 身元確認用サーバ装置30は、端末装置20によって提供された身元確認情報に基づいてユーザの身元確認を行う身元確認処理を実行し、当該身元確認処理によって身元確認が成功している場合には、身元確認済み情報を該当するユーザの端末装置20、又は、トークン発行用サーバ装置10に提供する構成を有している。
- [0064] 各データベース40は、ネットワークに接続可能なハードディスクドライブなどの各種のデータベース（広義には記憶装置、メモリ）によって構成されていてもよいし、PC（パーソナルコンピュータ）又はサーバ装置などの

ネットワークNに接続される情報処理装置とともに形成されているものであってもよい。

[0065] サービス管理サーバ装置50は、例えば、API（アプリケーションプログラミングインタフェース）や所定のプラットフォーム等を利用して各種のネットワークサービス、電子商取引に関する各種の処理、又は、ネットワークサービス若しくは電子商取引を管理する情報処理装置である。

[0066] また、サービス管理サーバ装置50は、1つの（装置、プロセッサ）で構成されていてもよいし、複数の（装置、プロセッサ）で構成されていてもよい。

[0067] [2] トークン発行用サーバ装置

次に、図2を用いて本実施形態のトークン発行用サーバ装置10について説明する。

[0068] なお、図2は、本実施形態のトークン発行用サーバ装置10の構成を示す機能ブロック図の一例である。

[0069] 本実施形態のトークン発行用サーバ装置10は、図2に例示するように、処理部100と、記憶部170と、情報記憶媒体180と、通信部196と、を有している。

[0070] なお、トークン発行用サーバ装置10は、図2の各部を全て含む必要はなく、その一部を省略した構成としてもよい。

[0071] 記憶部170は、処理部100などのワーク領域となるもので、その機能はRAM（VRAM）などのハードウェアにより実現できる。

[0072] 具体的には、記憶部170は、各種の処理を実行する際に用いるワークエリアとして使用される主記憶部171と、発行されたSBTに関する情報が記憶されたSBT関連情報記憶部172と、を含む。

[0073] 特に、SBT関連情報記憶部172には、各ユーザのユーザIDに対応付けて、発行されたSBTに関する情報（履歴情報を含む。）が記憶される。

[0074] なお、本実施形態の記憶部170は、主記憶部171及びSBT関連情報記憶部172などの構成の一部を省略する構成としてもよい。

- [0075] 情報記憶媒体 180 は、コンピュータにより読み取り可能であり、この情報記憶媒体 180 にはプログラムやデータなどが格納されている。すなわち、情報記憶媒体 180 には、本実施形態の各部としてコンピュータを機能させるためのプログラム（各部の処理をコンピュータに実行させるためのプログラム）が記憶される。
- [0076] なお、処理部 100 は、この情報記憶媒体 180 に格納されるプログラム（データ）から読み出されたデータに基づいて本実施形態の種々の処理を行うことができる。
- [0077] 例えば、情報記憶媒体 180 は、光ディスク（CD、DVD）、光磁気ディスク（MO）、磁気ディスク、ハードディスク、ソリッドステートドライブ等のフラッシュメモリ、磁気テープ、メモリ（ROM）、又は、メモリカード等である。
- [0078] 通信部 196 は、外部（例えば、端末装置 20）との間で通信を行うための各種制御を行うものであり、その機能は、各種プロセッサ又は通信用 ASIC などのハードウェアや、プログラムなどによって構成される。
- [0079] 処理部 100 は、記憶部 170 に格納されるプログラム（データ）に基づいて本実施形態の種々の処理を行う。
- [0080] なお、本実施形態の処理部 100 が、情報記憶媒体 180 に格納されているプログラムやデータを読み出し、読み出したプログラムやデータを一時的に記憶部 170 に格納し、そのプログラムやデータに基づいて処理を行ってもよい。
- [0081] また、処理部 100（プロセッサ）は、記憶部 170 内の主記憶部 171 をワーク領域として各種処理を行う。そして、処理部 100 の機能は各種プロセッサ（CPU、DSP 等）などのハードウェアや、プログラムにより実現できる。
- [0082] 具体的には、処理部 100 は、通信制御部 101、データ管理部 102、トークン発行管理部 103、トークン登録管理部 104、タイマ管理部 110、及び、情報提供部 111 を含む。

- [0083] 通信制御部１０１は、ネットワークを介して端末装置２０などと通信回線を確立し、相互に通信を行う。
- [0084] データ管理部１０２は、通信制御部１０１と連動し、通信部１９６を介して各端末装置２０から送信された仮想空間内のユーザの識別情報（以下、「仮想識別情報」という。）、現在位置情報及び身元確認済み情報を取得する。
- [0085] トークン発行管理部１０３は、ユーザ毎に、ユーザの仮想空間内の識別情報と、当該ユーザの実空間における位置を示す位置情報及び当該位置を特定する際の時刻を示す時刻情報と、に基づいて、本人確認用の認証コードとしてのＳＢＴを発行する。
- [0086] トークン登録管理部１０４は、トークン発行管理部１０３によって発行された認証コードとしてのＳＢＴをユーザに帰属させた上での各データベース４０に分散登録する。
- [0087] タイマ管理部１１０は、現在日時や所定のタイミングからの計測を行う機能を有しており、所定のタイミングが到来した場合に、現在時刻や計測結果を出力する。
- [0088] 情報提供部１１１は、ＳＢＴが発行されてデータベース４０に登録された旨（ＳＢＴのアクセス位置）及び登録したＳＢＴへのアクセスするためのアクセス位置の情報を該当する端末装置２０に提供する。
- [0089] [３] 端末装置
- 次に、図３を用いて、端末装置２０の機能について説明する。なお、図３は、本実施形態の端末装置２０の構成の一例を示す機能ブロック図である。
- [0090] 本実施形態の端末装置２０は、図３に示すように、処理部２００と、現在位置検出部２５０、タッチパネル等で構成される操作入力部２６０と、記憶部２７０と、情報記憶媒体２８０と、液晶パネル等の表示素子によって構成される表示部２９０と、通信部２９６と、音出力部２９２と、を有している。
- [0091] 現在位置検出部２５０は、所定のタイミング毎に端末装置２０の現在位置

を検出しつつ、当該現在位置を示す位置情報を生成する。

- [0092] 例えば、現在位置検出部250は、所定の期間毎（例えば、5秒毎）に図示しないGPS衛星の位置を認識しつつ、当該GPS衛星から送信された衛星信号（GPS信号）を検出する。
- [0093] そして、現在位置検出部250は、検出したGPS信号に基づいて自機の端末装置20の現在位置の座標値（例えば、緯度及び経度）を算出（すなわち、検出）し、当該座標値を現在位置情報として処理部200に提供する。
- [0094] なお、現在位置検出部250は、GPS信号に代えて、又は、加えて、WiFiを用いて、又は、携帯電話用の電波を用いて現在位置の座標を検出し、又は、当該座標の補正を実行してもよい。
- [0095] 操作入力部260は、ユーザからの入力情報を入力するための機器であり、ユーザの入力情報を処理部200に出力する。
- [0096] 本実施形態の操作入力部260は、ユーザの入力情報（入力信号）を検出する検出部262を備え、例えば、レバー、ボタン、マイク、タッチパネル型ディスプレイ、キーボード、マウスなどによって構成される。
- [0097] 記憶部270は、処理部200などのワーク領域となるもので、その機能はRAM（VRAM）などのハードウェアにより実現できる。
- [0098] そして、本実施形態の記憶部270は、ワーク領域として使用される主記憶部271と、最終的な表示画像等が記憶される画像バッファ272と、ユーザ情報が記憶されたユーザ情報記憶部273と、を含む。なお、これらの一部を省略する構成としてもよい。
- [0099] 情報記憶媒体280は、コンピュータにより読み取り可能であり、この情報記憶媒体280には各種のアプリ、OS（オペレーティングシステム）の他に、特に、本実施形態においては、当該端末装置20に対応するユーザのユーザIDを含む各種のデータが記憶されている。
- [0100] すなわち、情報記憶媒体280には、本実施形態の各部としてコンピュータを機能させるためのアプリ（各部の処理をコンピュータに実行させるためのアプリ）及びユーザIDが記憶される。

- [0101] 例えば、情報記憶媒体 280 は、光ディスク（CD、DVD）、光磁気ディスク（MO）、磁気ディスク、ハードディスクドライブ、フラッシュメモリ、磁気テープ、或いはメモリ（ROM）、メモリカード等である。
- [0102] 通信部 296 は、外部（例えば、他の端末装置 20、トークン発行用サーバ装置 10、身元確認用サーバ装置 30、データベース 40 又はサービス管理サーバ装置 50）との間で通信を行うための各種制御を行うものであり、その機能は、各種プロセッサ又は通信用 ASIC などのハードウェアや、プログラムなどによって構成される。
- [0103] 処理部 200 は、この情報記憶媒体 280 に格納されるアプリを読み出して実行することによって本実施形態の種々の処理を行うことができる。なお、情報記憶媒体 280 に記憶させておくアプリの種別については、任意である。
- [0104] 処理部 200 は、情報記憶媒体 280 に格納されるアプリに基づいて本実施形態の種々の処理を行う。なお、本実施形態の処理部 200 が、情報記憶媒体 280 に格納されているプログラムやデータを読み出し、読み出したプログラムやデータを一時的に記憶部 270 に格納し、そのプログラムやデータに基づいて処理を行ってもよい。
- [0105] また、処理部 200（プロセッサ）は、記憶部 270 内の主記憶部をワーク領域として各種処理を行う。そして、処理部 200 の機能は各種プロセッサ（CPU、DSP 等）などのハードウェアや、プログラムにより実現できる。
- [0106] 処理部 200 は、通信制御部 210、Web ブラウザ 211、現在位置管理部 212、表示制御部 213、入力受付処理部 214、身元確認処理部 216、ウォレット管理部 217、タイマ管理部 218、描画部 220、音処理部 230 を含む。なおこれらの一部を省略する構成としてもよい。
- [0107] 通信制御部 210 は、トークン発行用サーバ装置 10、身元確認用サーバ装置 30、データベース 40 又はサービス管理サーバ装置 50 とデータを送受信する処理を行う。

- [0108] また、通信制御部 210 は、トークン発行用サーバ装置 10、身元確認用サーバ装置 30、データベース 40 又はサービス管理サーバ装置 50 から送信されたデータを受信し、当該受信したデータを記憶部 270 に格納する処理、所与のデータを提供又は登録する処理、及び、その他のデータの送受信に関する制御処理等を行う。
- [0109] なお、通信制御部 210 は、トークン発行用サーバ装置 10、身元確認用サーバ装置 30、データベース 40 又はサービス管理サーバ装置 50 の宛先情報（IP アドレス、ポート番号）を情報記憶媒体 280 に記憶し、管理する処理を行うようにしてもよい。
- [0110] Web ブラウザ 211 は、Web ページ（認証用画面、身元確認処理用画面、身元情報登録用画面又はサービス享受用画面）を閲覧するためのアプリケーションプログラムであって、Web サーバ（トークン発行用サーバ装置 10、身元確認用サーバ装置 30 又はサービス管理サーバ装置 50）から、HTML ファイルや画像ファイル等をダウンロードし、レイアウトを解析して表示制御する。
- [0111] また、Web ブラウザ 211 は、入力フォーム（リンクやボタンやテキストボックス等）を用いてデータを Web サーバ（トークン発行用サーバ装置 10、身元確認用サーバ装置 30 又はサービス管理サーバ装置 50）に送信する。
- [0112] なお、端末装置 20 は、Web ブラウザ 211 によって、インターネットを介して URL によって指定された Web サーバ（トークン発行用サーバ装置 10、身元確認用サーバ装置 30 又はサービス管理サーバ装置 50）からの情報を表示させることができる。
- [0113] 例えば、端末装置 20 は、トークン発行用サーバ装置 10、身元確認用サーバ装置 30 又はサービス管理サーバ装置 50 から受信した各コンテンツ（HTML 等のデータ）を Web ブラウザ 211 によって表示させることができる。
- [0114] 現在位置管理部 212 は、現在位置検出部 250 から取得した所定の期間

毎の現在位置情報を取得し、主記憶部 271 に履歴情報として記憶する。

- [0115] また、現在位置管理部 212 は、S B T の発行要求時にトークン発行用サーバ装置 10 にユーザの現在位置情報を送信する。
- [0116] 表示制御部 213 は、表示部 290 に表示する処理を行う。例えば、表示制御部 213 は、W e b ブラウザ 211 を用いて表示してもよい。
- [0117] 入力受付処理部 214 は、ユーザによって操作入力部 260 から入力された入力情報を認識し、認識した情報に基づいて各種の処理を実行する。
- [0118] 身元確認処理部 216 は、身元確認用サーバ装置 30 と連動し、例えば、パスポート、保険証若しくは運転免許証などの本人確認書類の情報、又は、公的機関が発行する証明書などの公的機関が発行された本人確認書類の情報を、上記の身元確認情報に基づいて、当該ユーザの身元確認を実行する際の各種の処理を実行する。
- [0119] ウォレット管理部 217 は、他の端末装置 20 又はサービス管理サーバ装置 50 と連動し、各種のネットワークサービス、又は、電子商取引に関する各種の処理を実行する。
- [0120] 特に、ウォレット管理部 217 は、ユーザの S B T が発行されてブロックチェーン上に記録された場合（すなわち、データベース 40 上に暗号化されて分散登録された場合）に、記憶されている当該ユーザの S B T のデータへのアクセス権限を有している。
- [0121] そして、ウォレット管理部 217 は、固有のウォレットアドレスを有し、当該ウォレットアドレスと、S B T と、を用いてトランザクションの署名及び検証を行う。
- [0122] ウォレット管理部 217 は、ユーザの秘密鍵と公開鍵（ウォレットアドレスであってもよい。）を生成し、これらの鍵を用いてトランザクションの署名と検証を実行する。
- [0123] 例えば、ウォレット管理部 217 は、ユーザの秘密鍵を暗号化し、複数のデータベース 40（すなわち、分散ストレージ）に格納し、ユーザによる所与の認証プロセスを経てアクセスされ、ユーザのデータとアクションに関する

るトランザクションを署名及び検証を実行する。

[0124] タイマ管理部 218 は、現在日時や所定のタイミングからの計測を行う機能を有しており、所定のタイミングが到来した場合に、現在時刻や計測結果を出力する。

[0125] 描画部 220 は、処理部 200 で行われる種々の処理に基づいて描画処理を行い、これにより画像を生成し、表示制御部 213 によって表示部 290 に出力する。

[0126] 音処理部 230 は、処理部 200 で行われる種々の処理の結果に基づいて音処理を行い、BGM、効果音、又は音声などを生成し、音出力部 292 に出力する。

[0127] [4] 本実施形態の手法

[4.1] 概要

次に、図4を用いて本実施形態のトークン発行用サーバ装置10によって実行される認証コード発行処理及び端末装置20によって実行される認証コード発行要求処理について説明する。

[0128] なお、図4は、本実施形態のトークン発行用サーバ装置10において実行される認証コード発行処理及び端末装置20によって実行される認証コード発行要求処理について説明するための図である。

[0129] (認証コード発行処理)

本実施形態のトークン発行用サーバ装置10は、ニックネーム、ハンドルネーム又はペンネームなどの仮想空間におけるユーザの識別情報に実空間における当該ユーザの実在することを示す実体情報を対応付けた固有の認証コードとして認証コード自体の所有者を他の所有者に変更することができないSBTを発行する構成を有している。

[0130] 特に、本実施形態のトークン発行用サーバ装置10は、SBTを介して仮想空間内の識別情報（すなわち、ID）に実空間においての実体を証明すべき情報を対応付けることによって、経済活動をはじめとする仮想空間内におけるユーザの活動であっても、その実在性を担保し、的確な本人認証するこ

とが可能な構成を有している。

- [0131] 具体的には、トークン発行用サーバ装置 10 は、図 4 に示すように、
- (A 1) 仮想空間内のユーザの識別情報を仮想識別情報として取得する仮想識別情報取得処理、
 - (A 2) ユーザが保持する端末装置 20 から当該端末装置 20 の現在位置を示す現在位置情報と、当該現在位置を特定した際の時刻を示す時刻情報と、を取得する現在位置情報取得処理、
 - (A 3) 取得された仮想識別情報と、実体情報としての取得された現在位置情報及び時刻情報と、を対応付けて、ユーザ固有の識別情報のコードであって、所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードとしての SBT を発行する SBT 発行処理、及び、
 - (A 4) 発行された認証コードとしての SBT をユーザに帰属させた上で各データベース 40 に登録する SBT 登録処理、
- を実行する構成を有している。

- [0132] なお、図 4 には、上記の各処理に加えて、トークン発行用サーバ装置 10 によって SBT が発行された場合に、SBT が発行されてデータベース 40 に登録された旨 (SBT のアクセス位置) の送信、及び、SBT を用いて商取引や決済などのトランザクションが実行された場合に、SBT 及びウォレットアドレスを用いた検証することが示されている。

- [0133] 本実施形態のトークン発行用サーバ装置 10 は、このような構成を有することによって、匿名性を担保しつつも本人認証としての信頼性が担保された認証コードを発行することができるので、匿名性を担保して本人認証としての信頼性が高く、かつ、ネットワークサービスを利用した仮想空間におけるユーザの経済活動などの各種の活動を実現することができるようになっている。

- [0134] 特に、本実施形態のトークン発行用サーバ装置 10 は、分散型インターネット (Web 3.0) 又は Dapps (Decentralized Applications) などのデータや情報を分散化して個人管理することが増大し、個人活動が仮想空

間においても活発化する状況において、ユーザの匿名性を担保しつつ、信頼性が高く、かつ、即時性の高い本人認証及びその結果に基づく取引認証を実現することができる。

[0135] なお、本実施形態において、ユーザの識別情報として実名とは異なるニックネームなどの匿名性を有する識別情報を用いているが、勿論、ユーザの識別情報に、ユーザの氏名などの実名を用いてもよい。ただし、この場合には、匿名性の担保という観点からはその効果は薄れるものの、本人認証としての信頼性を向上させ、なりすましなどのネットワークサービスの利用に対するセキュリティを向上させることができる。

[0136] (認証コード発行要求処理)

本実施形態の端末装置20は、所与のネットワークサービスを利用する際に、種々の本人確認を行うことなく、本人の真正性を証明するために、SBTの発行を要求し、かつ、当該発行されたSBTを用いる構成を有している。

[0137] すなわち、本実施形態の端末装置20は、仮想空間におけるユーザの識別情報に実空間における当該ユーザの実在することを示す実体情報を対応付けた固有の認証コードとしてのSBTを利用する構成を有している。

[0138] 特に、本実施形態の端末装置20は、仮想空間内の識別情報(すなわち、ID)に実空間においての実体を証明すべき情報を対応付けられたSBTの発行を要求し、それを利用することによって、経済活動をはじめとする仮想空間内におけるユーザの活動であっても、その実在性を担保し、的確な本人認証することが可能な構成を有している。

[0139] 具体的には、端末装置20は、

(B1) 仮想空間内のユーザの識別情報を仮想識別情報として受け付ける仮想識別情報受付処理、

(B2) 現在位置を特定するとともに、当該現在位置を特定した際の時刻を特定する現在位置特定処理、

(B3) 受け付けられた識別情報と、実体情報としての特定された現在位置

を示す現在位置情報及び当該現在位置を特定した時刻を示す時刻情報と、を対応付けて、サーバシステムに所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードとしてのS B Tの発行を要求するS B T発行要求処理、及び、

(B 4) S B Tの発行要求に基づいて発行され、かつ、ユーザに帰属させた上で各データベース4 0に登録されたS B Tを用いて、ネットワークサービスに関連する処理を実行するサービス関連処理、を実行する構成を有している。

[0140] なお、図4には、上記の各処理に加えて、身元確認用サーバ装置3 0に対する身元確認処理の要求及び身元証明情報の提供、並びに、当該身元確認用サーバ装置3 0における身元確認処理の実行が示されている。

[0141] 本実施形態のトークン発行用サーバ装置1 0は、このような構成を有することによって、匿名性を担保しつつも本人認証としての信頼性が担保された認証コードを利用してネットワークサービスを享受することができるので、仮想空間におけるユーザの経済活動などの各種の活動を実空間と遜色なく実現することができるようになっている。

[0142] [4. 2] 身元確認済み情報取得処理（認証コード発行処理の前提の処理）

次に、トークン発行用サーバ装置1 0によって実行される認証コード発行処理の前提の処理としての身元確認済み情報取得処理について説明する。

[0143] データ管理部1 0 2は、端末装置2 0から送信された認証コード発行要求を受信した場合には、図4に示すように、当該認証コード発行要求とともに当該端末装置2 0から送信された、身元確認事業者によってユーザが固有の身元証明情報に基づいて身元確認されたことを示す身元確認済み情報を取得する身元確認済み情報取得処理を実行する。

[0144] 特に、データ管理部1 0 2は、該当するユーザの端末装置2 0によって、身元確認用サーバ装置3 0と連動して、例えば、パスポート、保険証、運転免許証などの公的機関によって発行された本人確認書類の情報、又は、住民票などの公的機関が発行する証明書の情報などの身元証明情報に基づいて身

元確認をし、当該身元確認が成功していることを示す身元確認済み情報の取得の有無を判定する。

[0145] そして、データ管理部 102 は、身元確認が成功していることを示す身元確認済み情報を取得すると、認証コード発行処理を実行し、身元確認済み情報を取得することができない場合には、認証コード発行要求に基づく SBT の発行を中止する。

[0146] なお、身元確認事業者としては、例えば、政府又は政府から依頼若しくは許可された公共的、及び、法的要件によって拘束されている信頼度の高い事業者である。

[0147] [4. 3] 仮想識別情報の受付処理及び現在位置情報取得処理

次に、トークン発行用サーバ装置 10 によって実行される認証コード発行処理のうち仮想識別情報取得処理及び現在位置情報取得処理について説明する。

[0148] (仮想識別情報取得処理)

データ管理部 102 は、図 4 に示すように、端末装置 20 から送信された認証コード発行要求を受信した場合には、通信制御部 101 と連動し、通信部 196 を介して端末装置 20 から送信された仮想空間内のユーザの識別情報を仮想識別情報として取得する仮想識別情報取得処理を実行する。

[0149] 特に、データ管理部 102 は、端末装置 20 から送信された認証コード発行要求を受信すると、ユーザの匿名性を確保するために、端末装置 20 から送信されたニックネーム、ハンドルネーム又はペンネームなどの仮想空間におけるユーザの識別情報を仮想識別情報として取得する。

[0150] なお、仮想識別情報は、各ユーザの希望によって特定された情報であってもよいし、自動的に付与されてもよいが、固有の情報であり、他のユーザの仮想識別情報と識別されて付与されることが好ましい。

[0151] (現在位置情報取得処理)

データ管理部 102 は、仮想識別情報と同様に、端末装置 20 から送信された認証コード発行要求を受信した場合には、図 4 に示すように、通信制御

部 1 0 1 と連動し、通信部 1 9 6 を介して端末装置 2 0 から送信された現在位置情報を取得する現在位置情報取得処理を実行する。

[0152] 特に、データ管理部 1 0 2 は、端末装置 2 0 から送信された認証コード発行要求を受信した場合には、当該端末装置 2 0 から送信された情報であって、当該端末装置 2 0 の現在位置を示す現在位置情報と、当該現在位置を特定した際の時刻を示す時刻情報と、を取得する現在位置情報取得処理を実行する。

[0153] すなわち、データ管理部 1 0 2 は、ユーザが実在することを証明するためであり、かつ、ユーザの生体情報として利用して S B T を発行するために、認証コード発行要求を送信した端末装置 2 0 から、当該端末装置 2 0（すなわち、ユーザの）の現在位置情報及び当該現在位置を特定したときの時刻を示す時刻情報を取得する。

[0154] [4 . 4] S B T 発行処理及び S B T 登録処理（認証コード発行処理）

次に、トークン発行用サーバ装置 1 0 によって実行される認証コード発行処理のうち S B T 発行処理及び S B T 登録処理について説明する。

[0155] （ S B T 発行処理）

トークン発行管理部 1 0 3 は、認証コード発行要求とともに、仮想識別情報取得処理及び現在位置情報取得処理によって仮想識別情報、現在位置情報及び時刻情報を取得すると、図 4 に示すように、取得された仮想識別情報と、実体情報としての取得された現在位置情報及び時刻情報と、を対応付けて、ユーザ固有の識別情報のコードであって、所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードとしての S B T を発行する S B T 発行処理を実行する。

[0156] 特に、このとき、トークン発行管理部 1 0 3 は、該当する端末装置 2 0 からウォレットアドレスを取得する。

[0157] そして、トークン発行管理部 1 0 3 は、常に個人のウォレットアドレスに結び付けられ、他人に売却や譲渡が不能な一身帰属性の N F T （Non-Fungible Token：偽造不可な鑑定書・所有証明書付きのデジタルデータ）として、

S B T (Soul Bound Token) を発行する。

[0158] また、トークン発行管理部 103 は、所定のタイミング毎にユーザの実体性を確認するために、1 日毎又は 1 週間毎など、予め定められた使用期限を有する S B T を発行する。

[0159] なお、本実施形態においては、トークン発行管理部 103 は、Verifiable Credentials (以下、「検証可能な資格情報」という。)としての身元確認済み情報を取得していること(すなわち、身元確認が実行されていること)を前提に、仮想識別情報と、現在位置情報及び時刻情報と、に基づいて、他のユーザに譲渡不能な固有の認証コードとして、S B T を発行する。

[0160] (S B T 登録処理)

トークン登録管理部 104 は、トークン発行管理部 103 によって認証コードとしての S B T が発行されると、図 4 に示すように、当該発行された S B T をユーザに帰属させた上で複数のデータベース 40 に分散登録する。

[0161] 特に、トークン登録管理部 104 は、例えば、ブロックチェーン技術を用いて、発行された S B T を暗号化し、かつ、当該暗号化された S B T をネットワーク上の複数のデータベース 40 に分散登録する。

[0162] また、このとき、トークン登録管理部 104 は、S B T を該当するユーザのウォレットアプリに付与されたウォレットアドレスに対応付けて、ネットワークで利用可能でありつつも、他人に譲渡不能に複数のデータベース 40 に分散登録する。

[0163] そして、トークン登録管理部 104 は、S B T を登録すると、情報提供部 111 を介して、当該 S B T が登録された旨とともに、当該登録した S B T へのアクセスするためのアクセス位置の情報を該当する端末装置 20 に提供する。

[0164] なお、本実施形態においては、認証コードとして、一身帰属性のトークンである S B T を発行しているが、譲渡不能であれば、電子証明書的なデジタルコードであってもよい。

[0165] また、本実施形態においては、ブロックチェーン技術を用いて、認証コー

ドとしてのS B Tをウォレットアドレスに対応付けてユーザに帰属させた上での複数のデータベース40に分散登録しているが、ウォレットアドレスに代えて、仮想識別情報、端末装置20のID (UID) 又は端末装置20が携帯用電話機の機能を有している場合にその番号（いわゆる携帯電話番号）など、所与のネットワークサービスを享受するための端末装置20の唯一性を有する識別情報を用いてもよい。

[0166] [4. 5] 身元確認処理（認証コード発行要求処理の前提の処理）

次に、端末装置20によって実行される認証コード発行要求処理の前提の処理としての身元確認処理について説明する。

[0167] 身元確認処理部216は、認証コード発行要求を行う場合には、図4に示すように、身元確認用サーバ装置30と連動し、ユーザの身元を示す身元証明情報に基づいて身元確認を要求する身元確認要求処理を実行する。

[0168] 特に、身元確認処理部216は、身元確認情報として、氏名、住所、電話番号又はクレジットカード番号などの情報を提供するとともに、例えば、パスポート、保険証、運転免許証などの公的機関によって発行された本人確認書類の情報、又は、住民票などの公的機関が発行する証明書の情報などの身元証明情報に基づいて身元確認用サーバ装置30に身元確認を要求する。

[0169] なお、身元確認用サーバ装置30は、提供された身元確認情報及び身元証明情報などを用いて自動的に身元確認処理を実行してもよいし、人的リソースを利用して身元確認処理を実行してもよい。

[0170] 一方、身元確認処理部216は、身元確認用サーバ装置30によって身元確認処理が実行された場合において、当該身元確認処理が成功した旨を受信すると、身元確認済みであるとして、それを示す情報（すなわち、身元確認済み情報）をユーザ情報記憶部273に登録する。

[0171] そして、身元確認処理部216は、身元確認用サーバ装置30において、身元確認処理が失敗した旨を受信すると、表示制御部213と連動して表示部290にその旨を表示させる。

[0172] このとき、身元確認処理部216は、身元確認要求処理を再度実行しても

よいし、当該身元確認要求処理を強制終了させてもよい。

[0173] [4. 6] 仮想識別情報受付処理及び現在位置特定処理（認証コード発行要求処理）

次に、端末装置20によって実行される認証コード発行要求処理のうち仮想識別情報受付処理及び現在位置特定処理について説明する。

[0174] （仮想識別情報受付処理）

入力受付処理部214は、認証コード発行要求を行う場合には、図4に示すように、例えば、ユーザの操作入力部260への操作に基づいて、仮想空間内のユーザの識別情報を仮想識別情報として受け付ける。

[0175] 例えば、入力受付処理部214は、ニックネーム、ハンドルネーム又はペンネームなどの仮想空間において、他のユーザと識別するための識別情報を仮想識別情報として受け付ける。

[0176] （現在位置特定処理）

現在位置管理部212は、認証コード発行要求を行う場合には、図4に示すように、現在位置特定処理として、現在位置検出部250によって受信したGPS信号に基づいて、端末装置20の現在位置を特定するとともに、当該現在位置を特定した際の時刻を特定する。

[0177] 特に、現在位置管理部212は、GPS信号を用いて特定された位置情報を用いてもよいし、当該GPS信号に代えて、又は、加えて、WiFiを用いて、又は、携帯電話用の電波を用いて現在位置の座標又はその補正を実行してもよい。

[0178] [4. 7] SBT発行要求処理（認証コード発行要求処理）及びウォレット機能他

次に、端末装置20によって実行される認証コード発行要求処理のうちSBT発行要求処理、SBTの管理及び再発行、当該SBTを用いたウォレット機能、について説明する。

[0179] （SBT発行要求処理）

ウォレット管理部217は、認証コード発行要求を行う場合において、仮

想識別情報受付処理によって受け付けられた仮想識別情報と、実体情報としての特定された現在位置を示す現在位置情報及び当該現在位置を特定した時刻を示す時刻情報と、取得すると、図4に示すように、取得した仮想識別情報と、取得した現在位置情報及び時刻情報と、を対応付けて、トークン発行用サーバ装置10に所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードとしてのS B Tの発行を要求する。

[0180] (S B Tの管理及び再発行要求)

ウォレット管理部217は、所定のタイミングにおいて各データベース40に分散登録されているS B Tの使用期限を管理する。

[0181] 特に、S B Tには、使用期限が記憶されており、使用期限後には、利用不能になるため、ウォレット管理部217は、所定のタイミングとして、ウォレットの機能を使用するタイミング、又は、S B Tが発行された際に定まる使用期限を認識し、当該認識した使用期限に基づくタイミングに、S B Tの再発行の要求を行う。

[0182] 具体的には、ウォレット管理部217は、所定のタイミングにおいて各データベース40に対してウォレットアドレスに基づいて、該当するS B Tの情報から使用期限の情報を取得し、当該使用期限まで一定期間内、又は、使用期限日を徒過したか否かを判定する判定処理を実行する。

[0183] そして、ウォレット管理部217は、使用期限まで一定期間内（使用期限1日前）に、又は、使用期限日を徒過したことを検出した場合には、S B Tの再発行の要求を行う。

[0184] (ウォレット機能)

ウォレット管理部217は、デジタルウォレットとして、他のユーザのウォレットと識別するためのウォレットアドレスを有し、当該ウォレットアドレスを用いて、無線、Bluetooth（登録商標）、磁気機能を利用して、決済データを他の端末装置20又はサービス管理サーバ装置50に提供する機能を有するアプリケーションを管理する。

[0185] 特に、ウォレット管理部217は、ユーザのS B Tが発行されてブロック

チェーン上に記録されている場合（すなわち、データベース40上に暗号化されて分散登録されている場合）に、記憶されている当該ユーザのS B Tのデータへのアクセス権限を有している。

[0186] また、ウォレット管理部217は、データベース40に登録された認証コードとしてのS B Tを用いて、金融サービス又はECサイトなどのネットワークサービスに関連するサービス関連処理を実行する。

[0187] すなわち、ウォレット管理部217は、発行要求に基づいて発行され、かつ、ユーザに帰属させた上で所与のデータベースに登録されたS B Tを用いて、所与のネットワークサービスに関連するサービス関連処理を実行する。

[0188] 具体的には、ウォレット管理部217は、決済又は商取引などのトランザクションを実行する場合には、決済先又は商取引先のサービス管理サーバ装置50又は他の端末装置20によって当該トランザクションの検証を実行させるため、図4に示すように、決済先又は取引先に、ウォレットアドレスとともにS B Tの情報を提供する。

[0189] [5] 本実施形態における動作

[5.1] 認証コード発行要求処理

次に、図5及び図6を用いて本実施形態の端末装置20によって実行される認証コード発行要求処理の動作について説明する。

[0190] なお、図5及び図6を用いて本実施形態の端末装置20によって実行される認証コード発行要求処理の動作を示すフローチャートである。

[0191] まず、入力受付処理部214は、操作入力部260を介してユーザの認証コード発行指示を受信すると（ステップS101）、ユーザの指示に基づいて、最初の認証コードの発行か、又は、2回目以降の認証コードの発行かを判定する判定処理を実行する（ステップS102）。

[0192] このとき、入力受付処理部214は、最初の認証コードの発行であると判定すると、ステップS103の処理に移行し、最初の認証コードの発行でないと判定すると、ステップS111の処理に移行する。

[0193] 次いで、入力受付処理部214によって最初の認証コードの発行であると

判定されると、入力受付処理部 2 1 4 及び操作入力部 2 6 0 と連動し、氏名、住所、電話番号又はクレジットカード番号などの予め定められた身元確認情報の入力を促しつつ、当該身元確認情報を取得する（ステップ S 1 0 3）。

[0194] なお、本実施形態においては、身元確認情報として、身元確認処理において提供する本人確認書類に記載されている情報が要求される。

[0195] 次いで、身元確認処理部 2 1 6 は、登録された身分確認情報とともに、例えば、パスポート、保険証、運転免許証若しくは公的機関が発行する証明書などの本人確認書類の情報を含めて身元確認用サーバ装置 3 0 に身元確認を要求する（ステップ S 1 0 5）。

[0196] 次いで、身元確認処理部 2 1 6 は、身元確認用サーバ装置 3 0 と連動し、ユーザの身元確認が完了（成功）したか否かを判定する判定処理を実行する（ステップ S 1 0 6）。

[0197] このとき、身元確認処理部 2 1 6 は、身元確認が成功しなかった（完了できなかった）と判定した場合には、身元確認が失敗した旨をユーザに告知して（ステップ S 1 0 7）ステップ S 1 0 3 の処理に移行する。ただし、身元確認処理部 2 1 6 は、ユーザの操作に基づいてこの時点で本動作を強制終了させてもよい。

[0198] 次いで、身元確認処理部 2 1 6 は、身元確認が成功した（完了できた）と判定した場合には、身元確認済み情報を受信し、当該受信した身元確認済み情報をユーザ情報記憶部 2 7 3 に登録する（ステップ S 1 0 8）。

[0199] なお、身元確認済み情報には、身元確認をした事業者名などの当該事業者に関する情報、登録した時刻、ユーザの ID などの各種の情報が含まれる。

[0200] 次いで、入力受付処理部 2 1 4 は、ユーザの操作入力部 2 6 0 への操作に基づいて、仮想空間内のユーザの識別情報を仮想識別情報として受け付ける（ステップ S 1 1 1）。

[0201] 次いで、現在位置管理部 2 1 2 は、GPS 信号に基づいて現在位置を検出するとともに、タイマ管理部 2 1 8 検出したタイミングにおける現在時刻を

取得する（ステップS 1 1 2）。

[0202] 次いで、ウォレット管理部2 1 7は、トークン発行用サーバ装置1 0に対して仮想識別情報と、認識された現在位置を示す現在位置情報（現在時刻情報を含む）及びその期の時刻情報とともに、認証コードであるS B Tの発行を要求する（ステップS 1 1 3）。

[0203] 次いで、ウォレット管理部2 1 7は、S B Tが発行されたことを認識すると（ステップS 1 1 4）、当該S B Tのデータベース4 0上のアクセス位置をユーザ情報記憶部2 7 3に登録して（ステップS 1 1 5）本動作を終了させる。

[0204] 次いで、ウォレット管理部2 1 7は、S B Tが発行されていないことを認識すると（ステップS 1 1 4）、当該S B Tの発行中止を表示部2 9 0に表示させて（ステップS 1 1 6）本動作を終了させる。

[0205] なお、ウォレット管理部2 1 7は、他の端末装置2 0又はサービス管理サーバ装置5 0からS B Tに基づく認証を要求された場合には、ウォレットアドレス及びS B Tのアクセス位置の情報を提供する。ただし、この場合において、S B Tの使用期限が経過している場合には、ウォレット管理部2 1 7は、ステップS 1 0 1の処理から本動作を開始させ、新たなS B Tの発行後にウォレットアドレス及び新たに発行されたS B Tのアクセス位置の情報を提供する。

[0206] [5 . 2] 認証コード発行処理

次に、図7を用いて本実施形態のトークン発行用サーバ装置1 0によって実行される認証コード発行処理の動作について説明する。

[0207] なお、図7を用いて本実施形態のトークン発行用サーバ装置1 0によって実行される認証コード発行処理の動作を示すフローチャートである。

[0208] まず、データ管理部1 0 2は、端末装置2 0から送信された認証コード発行要求を受信すると（ステップS 2 0 1）、当該認証コード発行要求に含まれる仮想識別情報、現在位置情報及び時刻情報を取得する（ステップS 2 0 2）。

[0209] 次いで、トークン発行管理部103は、仮想識別情報、現在位置情報及び現在時刻情報に基づいて、S B Tの発行の有無を判定する発行判定処理を実行する（ステップS203）。

[0210] 例えば、トークン発行管理部103は、身元確認済み情報も取得し、当該身元確認済み情報が正規な情報であることを判定しつつ、現在位置が実在する実空間の位置であること、及び、現在時刻が現在時刻を基準に所定の範囲内であることを判定する。

[0211] また、このとき、トークン発行管理部103は、S B Tを発行すると判定した場合には、S B Tを発行し（ステップS204）、発行したS B Tの複数のデータベースへの分散登録及び当該S B Tのデータベース40のアクセス位置を該当する端末装置20に送信して（ステップS205）本動作を終了させる。

[0212] 一方、トークン発行管理部103は、S B Tを発行しないと判定した場合には、情報提供部111と連動し、その旨を端末装置20に送信して（ステップS206）本動作を終了させる。

[0213] [6] 変形例

[6.1] 変形例1

次に、本実施形態の変形例1について説明する。

[0214] 本実施形態においては、ユーザの実在の有無に対して端末装置20の現在位置情報を用いているが、トークン発行用サーバ装置10は、例えば、日本人又は身元確認情報に含まれる住所などによってユーザ毎に活動エリアを登録し、検出された端末装置20の現在位置が予め登録された活動エリアであるか否かを判定し、検出された現在位置が活動エリア内の場合に、S B Tを発行してもよい。

[0215] [6.2] 変形例2

次に、図8～図10を用いて本実施形態の変形例2について説明する。

[0216] なお、図8は、本実施形態の変形例2におけるネットワーク型本人認証システムの構成を示すシステム構成図であり、図9は、本実施形態の変形例2

における情報処理サーバ装置において実行されるユーザのモーションキャプチャー処理について説明するための図である。

[0217] また、図10は、本実施形態の変形例2におけるトークン発行用サーバ装置において実行されるユーザのモーションキャプチャー処理について説明するための図である。

[0218] (システム概要及び構成)

本変形例は、認証コード発行処理を実行する際に用いる現在位置情報に基づいてユーザの身体的な動きを認識し、当該認識した動きを用いて本人認証を追加で実行する点に特徴がある。

[0219] 具体的には、本変形例のネットワーク型本人認証システムSは、図8に示すように、上記と同様に、トークン発行用サーバ装置10と、端末装置20(例えば、端末装置20A、20B、20C)と、身元確認用サーバ装置30と、複数のデータベース40と、サービス管理サーバ装置50と、から構成される。

[0220] また、本変形例のネットワーク型本人認証システムSは、図8に示すように、上記の構成に加えて、所定の期間毎の現在位置情報を利用しつつ、ネットワークを用いてユーザの身体的な動き(モーション)を認識し、当該認識したユーザの身体的な動きをモーション情報として出力するための、モーションキャプチャー処理を実行する情報処理サーバ装置60を有している。

[0221] なお、本変形例のネットワーク型本人認証システムSにおいて、上記実施形態と同一の部材については、同一の符号を付してその説明を省略する。

[0222] (情報処理サーバ装置)

本変形例の情報処理サーバ装置60は、図9に示すように、

(A1) ユーザPの身体的な特徴を示す情報を身体情報として取得する処理(すなわち、ユーザ情報を読み出す処理及び端末装置20を用いた入力サポートに基づく身体情報を特定して取得する処理を含む。)、

(A2) ユーザPの身体の一部の部位(すなわち、特定の部位)に対応付けて存在し、当該部位の動きに伴って移動する端末装置20の現在位置情報を

取得する処理（以下、「部位位置情報取得処理」という。）、

（Ａ３）端末装置２０の位置情報に基づいて、ユーザの身体の一部の部位の軌道を部位軌道情報として検出する処理（以下、「部位軌道情報検出処理」という。）、

（Ａ４）取得された身体情報と、検出された部位軌道情報と、に基づいて、ユーザの身体の動きを認識するモーション認識処理、及び、

（Ａ５）認識された身体的な動きをモーション情報としてトークン発行用サーバ装置１０に出力する出力制御処理、
を実行する構成を有している。

[0223] すなわち、情報処理サーバ装置６０は、現在位置情報を用いたユーザそのもの又はユーザの身体の一部の部位の動き（いわゆる、モーション）をデジタル的に取得するモーションキャプチャを実現する構成を有している。

[0224] （トークン発行用サーバ装置）

本変形例のトークン発行用サーバ装置１０は、図１０を示すように、

（Ｂ１）記憶されているユーザ毎に該当するユーザに関するユーザ情報であって、ユーザの身体の一部の部位の動きの特徴を示すモーション特徴情報を、当該ユーザ情報として、管理し、

（Ｂ２）情報処理サーバ装置６０から出力されたモーション情報の対象となるユーザ（以下、「対象ユーザ」という。）を特定し、

（Ｂ３）特定された対象ユーザのモーション特徴情報（すなわち、基準モーション情報）と、情報処理サーバ装置６０から出力されたモーション情報と（すなわち、認識モーション情報）、に基づいて、特定されたユーザの身体的な部位の動きの同一性を判定する判定処理を実行し、

（Ｂ４）判定処理において、モーション特徴情報によって示される部位の動きと、モーション情報によって示されるユーザの身体的な部位の動きと、が同一又は同一とみなされる動きであると判定された場合に、該当するユーザの本人認証を行う認証処理を実行し、

（Ｂ５）本人認証されたユーザに対して上記のようにＳＢＴを発行する、

構成を有している。

[0225] そして、トークン発行用サーバ装置 10 は、モーションキャプチャの処理によって得られたモーション情報を、生体情報として、利用しつつ、当該モーション情報に基づく生体認証として本人認証を実行するための構成を有している。

[0226] [6. 3] 変形例 3

次に、本実施形態の変形例 3 について説明する。

[0227] 上記実施形態においては、身元確認用サーバ装置 30 によって本人確認書類に基づく身元確認が成功していることを前提に、S B T の発行が実行されているが、当該身元確認が実行されていない場合であっても、端末装置 20 の位置情報、時刻情報及び仮想空間内の識別情報に基づいて、S B T を発行してもよい。

[0228] [6. 4] 変形例 4

次に、本実施形態の変形例 4 について説明する。

[0229] 上記実施形態においては、端末装置の実施例として、スマートフォンなどの情報端末装置を用いて説明したが、IoT センサなどの IoT デバイスに S B T を提供してもよい。

[0230] この場合には、IoT デバイスが発生するデータの真正性を担保することができるので、例えば、サプライチェーン関連のデータの監視、製品の出荷からエンドユーザまでの透明性を向上させること、及び、製品の品質、安全性、信頼性及び人権保護などの状況を検証又は分析可能になる。

[0231] [7] その他

本発明の一実施の形態は、上記実施形態で説明したものに限らず、種々の変形実施が可能である。例えば、明細書又は図面中の記載において広義や同義な用語として引用された用語は、明細書又は図面中の他の記載においても広義や同義な用語に置き換えることができる。

[0232] 本発明の一実施の形態は、実施形態で説明した構成と実質的に同一の構成（例えば、機能、方法及び結果が同一の構成、あるいは目的及び効果が同一

の構成)を含む。また、本発明は、実施形態で説明した構成の本質的でない部分を置き換えた構成を含む。また、本発明は、実施形態で説明した構成と同一の作用効果を奏する構成又は同一の目的を達成することができる構成を含む。また、本発明は、実施形態で説明した構成に公知技術を付加した構成を含む。

[0233] 上記のように、本発明の実施形態について詳細に説明したが、本発明の新規事項及び効果から実体的に逸脱しない多くの変形が可能であることは当業者には容易に理解できるであろう。したがって、このような変形例はすべて本発明の範囲に含まれるものとする。

符号の説明

[0234] S : ネットワーク型本人認証システム
10 : トークン発行用サーバ装置
20 : 端末装置
30 : 身元確認用サーバ装置
40 : データベース
50 : サービス管理サーバ装置
60 : 情報処理サーバ装置
70 : GPS衛星
100 : 処理部
101 : 通信制御部
102 : データ管理部
103 : トークン発行管理部
110 : タイマ管理部
111 : 情報提供部
170 : 記憶部
171 : 主記憶部
172 : SBT関連情報記憶部
180 : 情報記憶媒体

1 9 6	: 通信部
2 0 0	: 処理部
2 1 0	: 通信制御部
2 1 1	: W e b ブラウザ
2 1 2	: 現在位置管理部
2 1 3	: 表示制御部
2 1 4	: 入力受付処理部
2 1 5	: 身元確認情報管理部
2 1 6	: 身元確認処理部
2 1 7	: ウォレット管理部
2 1 8	: タイマ管理部
2 2 0	: 描画部
2 3 0	: 音処理部
2 5 0	: 現在位置検出部
2 6 0	: 操作入力部
2 6 2	: 検出部
2 7 0	: 記憶部
2 7 1	: 主記憶部
2 7 2	: 画像バッファ
2 7 3	: ユーザ情報記憶部
2 8 0	: 情報記憶媒体
2 9 0	: 表示部
2 9 2	: 音出力部
2 9 6	: 通信部

請求の範囲

- [請求項1] 仮想空間におけるユーザの識別情報に実空間における当該ユーザの
実在することを示す実体情報を対応付けた固有の認証コードを発行す
る認証コード発行システムであって、
 前記仮想空間内のユーザの識別情報を仮想識別情報として取得する
仮想識別情報取得手段と、
 前記ユーザが保持する端末装置から当該端末装置の現在位置を示す
現在位置情報と、当該現在位置を特定した際の時刻を示す時刻情報と
、を取得する位置情報取得手段と、
 前記取得された仮想識別情報と、前記実体情報としての前記取得さ
れた現在位置情報及び時刻情報と、を対応付けて、前記ユーザ固有の
識別情報のコードであって、所与のネットワークサービスを利用する
ための本人確認用の非代替性の認証コードを発行する認証コード発行
手段と、
 前記発行された認証コードを前記ユーザに帰属させた上で所与のデ
ータベースに登録する登録手段と、
 を備えることを特徴とする認証コード発行システム。
- [請求項2] 請求項1の認証コード発行システムにおいて、
 前記認証コード発行手段が、
 使用期間に制限のある前記認証コードを発行する、認証コード発
行システム。
- [請求項3] 請求項1の認証コード発行システムにおいて、
 前記登録手段が、
 前記認証コードを暗号化し、当該暗号化された認証コードをネッ
トワーク上の複数の前記データベースに分散登録する、認証コード発
行システム。
- [請求項4] 請求項1の認証コード発行システムにおいて、
 前記認証コード発行手段が、

少なくとも前記現在位置情報を前記ユーザの生体情報として利用して前記本人確認用の認証コードを発行する、認証コード発行システム。

[請求項5]

請求項4の認証コード発行システムにおいて、

記憶手段に記憶されている前記ユーザ毎に該当するユーザに関するユーザ情報を管理する手段であって、前記ユーザの身体の一部の部位の動きの特徴を示すモーション特徴情報を、当該ユーザ情報として、管理する情報管理手段を更に備え、

前記認証コード発行手段が、

複数の前記現在位置情報に基づいて前記ユーザの身体の一部の部位の軌道を部位軌道情報として検出し、当該検出された部位軌道情報に基づいて前記ユーザの身体の動きを示すモーション情報を特定し、

前記認証コードの発行要求したユーザの前記モーション特徴情報と、前記取得されたモーション情報と、に基づいて、当該対象ユーザの身体的な部位の動きの同一性を判定する判定処理を実行し、

前記判定処理において、前記モーション特徴情報によって示される部位の動きと、前記モーション情報によって示される対象ユーザの身体的な部位の動きと、が同一又は同一とみなされる動きであると判定された場合に、前記対象ユーザの本人認証を行う認証処理を実行し、

前記認証処理によって前記本人認証が成功の場合に、前記本人確認用の認証コードを発行する、認証コード発行システム。

[請求項6]

仮想空間におけるユーザの識別情報に実空間における当該ユーザの存在することを示す実体情報を対応付けた固有の認証コードを利用する端末装置であって、

前記仮想空間内のユーザの識別情報を仮想識別情報として受け付ける受付手段と、

現在位置を特定するとともに、当該現在位置を特定した際の時刻を特定する特定手段と、

前記受け付けられた仮想識別情報と、前記実体情報としての前記特定された現在位置を示す現在位置情報及び当該現在位置を特定した時刻を示す時刻情報と、を対応付けて、サーバシステムに所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードの発行を要求する要求手段と、

前記発行要求に基づいて発行され、かつ、前記ユーザに帰属させた上で所与のデータベースに登録された認証コードを用いて、前記ネットワークサービスに関連するサービス関連処理を実行するサービス関連処理実行手段と、
を備えることを特徴とする端末装置。

[請求項7]

請求項6の端末装置において、
前記認証コードが使用期限を経過しているか否かを判定する使用期限判定処理を実行する判定手段を更に備え、
前記要求手段が、
前記使用期限判定処理の結果、前記認証コードの使用期限が経過していると判定された場合には、再取得した現在位置情報及び時刻情報に基づいて、前記サーバシステムに認証コードの発行を要求する、
端末装置。

[請求項8]

請求項6の端末装置において、
前記サービス関連処理実行手段が、
所与のデータベースとして、ネットワーク上の複数のデータベースに暗号化して分散登録された認証コードを用いて、前記ネットワークサービスに関連するサービス関連処理を実行する、
端末装置。

[請求項9]

仮想空間におけるユーザの識別情報に実空間における当該ユーザの存在することを示す実体情報を対応付けた固有の認証コードを利用する認証コード利用方法であって、
前記仮想空間内のユーザの識別情報を仮想識別情報として受け付けをし、

現在位置を特定するとともに、当該現在位置を特定した際の時刻を特定し、

前記受け付けられた仮想識別情報と、前記実体情報としての前記特定された現在位置を示す現在位置情報及び当該現在位置を特定した時刻を示す時刻情報と、を対応付けて、サーバシステムに所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードの発行を要求し、

前記発行要求に基づいて発行され、かつ、前記ユーザに帰属させた上で所与のデータベースに登録された認証コードを用いて、前記ネットワークサービスに関連するサービス関連処理を実行する、ことを特徴とする認証コード利用方法。

[請求項10]

仮想空間におけるユーザの識別情報に実空間における当該ユーザの存在することを示す実体情報を対応付けた固有の認証コードを発行する認証コード発行方法であって、

前記仮想空間内のユーザの識別情報を仮想識別情報として取得し、

前記ユーザが保持する端末装置から当該端末装置の現在位置を示す現在位置情報と、当該現在位置を特定した際の時刻を示す時刻情報と、を取得し、

前記取得された仮想識別情報と、前記実体情報としての前記取得された現在位置情報及び時刻情報と、を対応付けて、前記ユーザ固有の識別情報のコードであって、所与のネットワークサービスを利用するための本人確認用の非代替性の認証コードを発行し、

前記発行された認証コードを前記ユーザに帰属させた上で所与のデータベースに登録する、ことを特徴とする認証コード発行方法。