

明 細 書

発明の名称： アクセス制御装置、制御方法、及びプログラム

技術分野

[0001] 本発明はデータの共有に関する。

背景技術

[0002] 複数の端末からアクセス可能な記憶装置にデータを格納することで、データの共有が行われている。このようなデータの共有に利用される記憶装置の1つとして、ブロックチェーン技術を利用して実現されるブロックチェーンストレージがある。例えば特許文献1は、端末で発生したイベントに関する情報をブロックチェーンストレージに格納して共有することが開示されている。

先行技術文献

特許文献

[0003] 特許文献1： 特開2018-081464号公報

発明の概要

発明が解決しようとする課題

[0004] ブロックチェーンストレージには、格納されたデータの改ざんが難しいという利点がある。一方で、ブロックチェーンストレージでは、格納されたデータを削除することも難しいため、データの持ち主が後に削除を望む可能性があるデータ（例えば個人情報）をブロックチェーンストレージ上に格納してしまうと、持ち主が削除を望んだ際の対処が難しくなってしまう。

[0005] 本発明は上記課題に鑑みてなされたものであり、その目的の一つは、データの削除を可能にしつつ、ブロックチェーンストレージを活用する技術を提供することである。

課題を解決するための手段

[0006] 本発明のアクセス制御装置は、1) 第1記憶装置に格納されているデータへのアクセスのリクエストを取得するリクエスト取得部と、2) 第1記憶装

置へのアクセスに関するアクセス権限を表す権限情報が格納されている第2記憶装置から権限情報を取得する権限情報取得部と、3) リクエストの主体である対象エンティティについての権限情報を用いて、アクセスが対象エンティティのアクセス権限の範囲内であるか否かを判定する権限判定部と、4) アクセスが対象エンティティのアクセス権限の範囲内であると判定された場合、アクセスを実行するアクセス実行部と、を有する。第2記憶装置はブロックチェーンストレージである。

[0007] 本発明の制御方法はコンピュータによって実行される。当該制御方法は、1) 第1記憶装置に格納されているデータへのアクセスのリクエストを取得するリクエスト取得ステップと、2) 第1記憶装置へのアクセスに関するアクセス権限を表す権限情報が格納されている第2記憶装置から権限情報を取得する権限情報取得ステップと、3) リクエストの主体である対象エンティティについての権限情報を用いて、アクセスが対象エンティティのアクセス権限の範囲内であるか否かを判定する権限判定ステップと、4) アクセスが対象エンティティのアクセス権限の範囲内であると判定された場合、アクセスを実行するアクセス実行ステップと、を有する。第2記憶装置はブロックチェーンストレージである。

[0008] 本発明のプログラムは、本発明の制御方法をコンピュータに実行させる。

発明の効果

[0009] 本発明によれば、データの削除を可能にしつつ、ブロックチェーンストレージを活用する技術が提供される。

図面の簡単な説明

[0010] [図1]実施形態1に係るアクセス制御装置の動作を概念的に例示する図である。

[図2]アクセス制御装置の機能構成を例示するブロック図である。

[図3]アクセス制御装置を実現するための計算機を例示する図である。

[図4]実施形態1のアクセス制御装置によって実行される処理の流れを例示するフローチャートである。

[図5]第2記憶装置に格納されている権限情報をテーブル形式で例示する図である。

[図6]実施例のアクセス制御装置を例示する図である。

発明を実施するための形態

[0011] 以下、本発明の実施の形態について、図面を用いて説明する。尚、すべての図面において、同様な構成要素には同様の符号を付し、適宜説明を省略する。また、特に説明する場合を除き、各ブロック図において、各ブロックは、ハードウェア単位の構成ではなく、機能単位の構成を表している。以下の説明において、特に説明しない限り、各種所定の値（閾値など）は、その値を利用する機能構成部からアクセス可能な記憶装置に予め記憶させておく。

[0012] [実施形態1]

<概要>

図1は、実施形態1に係るアクセス制御装置2000の動作を概念的に例示する図である。ここで、図1を用いて説明するアクセス制御装置2000の動作は、アクセス制御装置2000の理解を容易にするための例示であり、アクセス制御装置2000の動作を限定するものではない。アクセス制御装置2000の動作の詳細やバリエーションについては後述する。

[0013] アクセス制御装置2000は、エンティティに付与されたアクセス権に基づいて、エンティティからリクエストされた第1記憶装置30へのアクセスを制御する。ここでいうエンティティとは、第1記憶装置30に対するアクセスをリクエストする主体である。例えばエンティティは、ユーザや、ユーザのグループである。この場合、ユーザごとやユーザのグループごとにアクセス権が設定される。その他にも例えば、エンティティは、端末や、端末のグループである。この場合、端末ごとや端末のグループごとにアクセス権が設定される。なお、端末は、物理的なマシンであってもよいし、仮想的なマシンであってもよい。

[0014] 第1記憶装置30には、任意のデータが格納されている。例えば第1記憶装置30に格納されるのはユーザ認証に利用するユーザの認証情報や、ユー

ザの個人情報などである。

[0015] 各エンティティのアクセス権限を表す情報（権限情報70）は、第2記憶装置40に格納されている。第2記憶装置40は、ブロックチェーン技術を利用して構築されたストレージ（ブロックチェーンストレージ）である。なお、ブロックチェーンストレージを構築する技術には、既存の技術を利用することができる。以下、第2記憶装置40を、ブロックチェーンストレージ40とも表記する。ここで、第1記憶装置30はブロックチェーンストレージではない。

[0016] アクセス制御装置2000は、第1記憶装置30に格納されているデータへのアクセスのリクエストを受け付ける。以下、アクセス制御装置2000が受信したリクエストの主体であるエンティティを、対象エンティティ10と呼ぶ。アクセス制御装置2000は、対象エンティティ10の権限情報70を取得する。アクセス制御装置2000は、対象エンティティ10の権限情報70を利用して、リクエストされたアクセスが、対象エンティティ10に与えられたアクセス権限の範囲内であるか否かを判定する。

[0017] アクセス制御装置2000は、リクエストされたアクセスが対象エンティティに与えられたアクセス権限の範囲内であると判定した場合、リクエストされたアクセスを実行する。一方、リクエストされたアクセスが対象エンティティに与えられたアクセス権限の範囲内でないと判定した場合、アクセス制御装置2000は、リクエストされたアクセスを実行しない。

[0018] <作用効果の一例>

本実施形態のアクセス制御装置2000によれば、第1記憶装置30へのアクセスのリクエストについて、リクエストされたアクセスの実行の許否が、ブロックチェーンストレージ40に格納されている権限情報70を利用して判定される。ここで、ブロックチェーンストレージには、格納されているデータの改ざんが難しいという利点がある。そのため、ブロックチェーンストレージ40上に格納されている権限情報70は改ざんが難しく、信頼度が高い情報であると言える。よって、アクセス制御装置2000によれば、正

当なアクセス権限を持たない対象エンティティ 10 によって第 1 記憶装置 30 に格納されているデータが不正にアクセスされてしまうことを防ぐことができる。

[0019] ここで、アクセス対象であるデータ自体をブロックチェーンストレージ 40 に格納するという方法も考えられる。しかしながら、ブロックチェーンストレージ上のデータは、改ざんだけでなく、削除することも難しい。そのため、ユーザが他者と共有するデータをブロックチェーンストレージに格納してしまうと、そのデータを当該ユーザが削除したいと思ったとしても、そのデータを削除することができなくなってしまう。例えばそのデータがユーザの個人情報であれば、GDPR (General Data Protection Regulation) の「忘れられる権利」を達成できないといった不都合も生じうる。

[0020] この点、アクセス制御装置 2000 では、アクセス権限を表す権限情報 70 についてはブロックチェーンストレージ 40 に格納される一方で、アクセス対象のデータについては、ブロックチェーンストレージではない第 1 記憶装置 30 に格納される。このようにすることで、ブロックチェーンストレージの利点を活かして、権限情報 70 が改ざんされてデータに対する不正なアクセスが発生してしまうことを防ぎつつ、データを削除することも可能となる。よって、データの削除を可能にしつつ、ブロックチェーンストレージの利点を活かしたセキュアなデータ共有を実現することができる。

[0021] 以下、アクセス制御装置 2000 についてより詳細に説明する。

[0022] <機能構成の例>

図 2 は、アクセス制御装置 2000 の機能構成を例示するブロック図である。アクセス制御装置 2000 は、リクエスト取得部 2020、権限情報取得部 2040、権限判定部 2060、及びアクセス実行部 2080 を有する。リクエスト取得部 2020 は、リクエスト 20 を取得する。リクエスト 20 は、対象エンティティ 10 による第 1 記憶装置 30 へのアクセスのリクエストである。権限情報取得部 2040 は、第 2 記憶装置 40 から、対象エンティティ 10 のアクセス権限を示す権限情報 70 を取得する。権限判定部 2

060は、権限情報70を利用して、リクエスト20に示されているアクセスが、対象エンティティ10のアクセス権限の範囲内であるか否かを判定する。アクセス権限の範囲内であると判定された場合、アクセス実行部2080は、リクエスト20に示されているアクセスを実行する。なお、第1記憶装置30はブロックチェーンストレージではなく、第2記憶装置40はブロックチェーンストレージである。

[0023] <アクセス制御装置2000のハードウェア構成の例>

アクセス制御装置2000の各機能構成部は、各機能構成部を実現するハードウェア（例：ハードワイヤードされた電子回路など）で実現されてもよいし、ハードウェアとソフトウェアとの組み合わせ（例：電子回路とそれを制御するプログラムの組み合わせなど）で実現されてもよい。以下、アクセス制御装置2000の各機能構成部がハードウェアとソフトウェアとの組み合わせで実現される場合について、さらに説明する。

[0024] 図3は、アクセス制御装置2000を実現するための計算機1000を例示する図である。計算機1000は、任意の計算機である。例えば計算機1000は、PC（Personal Computer）やサーバマシンなどといった、据え置き型の計算機である。その他にも例えば、計算機1000は、スマートフォンやタブレット端末などといった可搬型の計算機である。

[0025] 計算機1000は、アクセス制御装置2000を実現するために設計された専用の計算機であってもよいし、汎用の計算機であってもよい。後者の場合、例えば、計算機1000に対して所定のアプリケーションをインストールすることにより、計算機1000で、アクセス制御装置2000の各機能が実現される。上記アプリケーションは、アクセス制御装置2000の機能構成部を実現するためのプログラムで構成される。

[0026] 計算機1000は、バス1020、プロセッサ1040、メモリ1060、ストレージデバイス1080、入出力インタフェース1100、及びネットワークインタフェース1120を有する。バス1020は、プロセッサ1040、メモリ1060、ストレージデバイス1080、入出力インタフェ

ース１１００、及びネットワークインタフェース１１２０が、相互にデータを送受信するためのデータ伝送路である。ただし、プロセッサ１０４０などを互いに接続する方法は、バス接続に限定されない。

[0027] プロセッサ１０４０は、CPU (Central Processing Unit)、GPU (Graphics Processing Unit)、FPGA (Field-Programmable Gate Array) などの種々のプロセッサである。メモリ１０６０は、RAM (Random Access Memory) などを用いて実現される主記憶装置である。ストレージデバイス１０８０は、ハードディスク、SSD (Solid State Drive)、メモリカード、又は ROM (Read Only Memory) などを用いて実現される補助記憶装置である。

[0028] 入出力インタフェース１１００は、計算機１０００と入出力デバイスとを接続するためのインタフェースである。例えば入出力インタフェース１１００には、キーボードなどの入力装置や、ディスプレイ装置などの出力装置が接続される。

[0029] ネットワークインタフェース１１２０は、計算機１０００を通信網に接続するためのインタフェースである。この通信網は、例えば LAN (Local Area Network) や WAN (Wide Area Network) である。

[0030] ストレージデバイス１０８０は、アクセス制御装置２０００の各機能構成部を実現するプログラム（前述したアプリケーションを実現するプログラム）を記憶している。プロセッサ１０４０は、このプログラムをメモリ１０６０に読み出して実行することで、アクセス制御装置２０００の各機能構成部を実現する。

[0031] <処理の流れ>

図４は、実施形態１のアクセス制御装置２０００によって実行される処理の流れを例示するフローチャートである。リクエスト取得部２０２０は、リクエスト２０を取得する（Ｓ１０２）。権限情報取得部２０４０は、対象エンティティ１０の権限情報７０を取得する（Ｓ１０４）。権限判定部２０６０は、リクエスト２０で要求されているアクセスが、対象エンティティ１０のアクセス権限の範囲内であるか否かを判定する（Ｓ１０６）。アクセス権

限の範囲内である場合（S 1 0 6 : Y E S）、アクセス実行部 2 0 8 0 は、リクエスト 2 0 で要求されているアクセスを実行する（S 1 0 8）。

[0032] アクセス権限の範囲内でない場合（S 1 0 6 : N O）、図 4 の処理は終了する。ただし、アクセス制御装置 2 0 0 0 は、この場合にも何らかの処理を行ってもよい。例えば後述するように、アクセス制御装置 2 0 0 0 は、リクエストされたアクセスがアクセス権限の範囲内でないことを表す通知を出力する。

[0033] <権限情報 7 0 について>

第 1 記憶装置 3 0 へのアクセス権限は、権限情報 7 0 によって表される。権限情報 7 0 は、アクセスの主体と客体の組み合わせに対して定められる。前述したように、アクセスの主体はエンティティである。例えば、「エンティティ A、客体 B」という組み合わせに対して定められている権限情報 7 0 は、エンティティ A が客体 B へのアクセスについて持つアクセス権限を表す。

[0034] アクセスの客体は、様々な方法で表すことができる。例えばアクセスの客体は、第 1 記憶装置 3 0 に格納されているデータで表される。この場合、「エンティティ識別情報、データの識別情報（データ識別情報）」の組み合わせに対して、アクセス権限が設定される。この方法によれば、データ単位でアクセス権限を設定することができる。

[0035] ここで、データ識別情報としては、データを互いに識別できる任意の情報を利用することができる。例えばデータがファイルとして管理されている場合、データ識別情報は、ファイル名やパスである。その他にも例えば、データがテーブルで管理されている場合、データ識別情報は、テーブル内のデータを特定するための情報である。

[0036] その他にも例えば、アクセスの客体は、第 1 記憶装置 3 0 に格納されているデータのグループで表される。この場合、「エンティティ識別情報、データグループの識別情報（データグループ識別情報）」の組み合わせに対して、アクセス権限が設定される。この方法によれば、データのグループ単位でアクセス権限を設定することができる。

- [0037] その他にも例えば、アクセスの客体は、第1記憶装置30内の部分的な記憶領域（以下、部分領域）で表されてもよい。この場合、「エンティティ識別情報、部分領域の識別情報（領域識別情報）」の組み合わせに対して、アクセス権限が設定される。この方法によれば、部分領域単位でアクセス権限を設定することができる。
- [0038] 例えば部分領域は、特定のユーザに対して割り当てられる。ユーザは、割り当てられた部分領域にデータを格納する。部分領域単位でアクセス権限を設定できるようにすることで、ユーザは、自分に割り当てられた部分領域へのアクセスを、特定のエンティティのみに許可することが可能になる。
- [0039] なお、アクセス権限の設定方法（すなわち、権限情報70の生成方法）については後述する。
- [0040] 図5は、第2記憶装置40に格納されている権限情報70をテーブル形式で例示する図である。図5のテーブルを、テーブル100と呼ぶ。テーブル100は、エンティティ識別情報102、客体識別情報104、及び権限情報70という3つの列を有する。エンティティ識別情報102は、エンティティの識別情報を示す。客体識別情報104は、客体の識別情報（データ識別情報、データグループ識別情報、又は領域識別情報）を示す。権限情報70は、対応するエンティティ識別情報102によって特定されるエンティティが、対応する客体識別情報104によって特定される客体に対して有する権限を表す。図5の権限情報70では、「read」は読み出し権限を有することを示し、「write」は書き込み権限を有することを示し、「read, write」は読み出しと書き込みの両方の権限を有することを示している。なお、読み出し権限と書き込み権限の他に、実行権限が設定可能であってもよい。
- [0041] ここで、アクセス権限の設定（すなわち、テーブル100のレコードの登録）は、アクセス制御装置2000を介して行われてもよいし、アクセス制御装置2000を介さずに行われてもよい。前者の場合、例えばアクセス制御装置2000は、アクセス権限の設定を受け付けるウェブサイトなどをユーザに対して提供する。ユーザは、当該ウェブサイトに必要な情報を入力す

ることにより、アクセス権限の設定を行う。アクセス制御装置 2000 は、ユーザによって指定されたアクセス権限（テーブル 100 のレコード）を、ブロックチェーンストレージ 40 に格納する。なお、ブロックチェーンストレージにデータを格納する技術には、既存の技術を利用することができる。

[0042] <リクエスト 20 の取得：S102>

リクエスト取得部 2020 は、リクエスト 20 を取得する。例えばリクエスト 20 は、アクセス制御装置 2000 と通信可能に接続されている任意の端末から送信される。この場合、アクセス制御装置 2000 は、ユーザによって操作させる端末と通信可能に接続されているサーバマシンなどで実現される。その他にも例えば、リクエスト取得部 2020 は、アクセス制御装置 2000 に接続されている入力デバイスを用いたリクエスト 20 の入力を受け付けてもよい。この場合、アクセス制御装置 2000 は、ユーザによって操作される端末などで実現される。

[0043] リクエスト 20 は、少なくとも、対象エンティティ 10 のエンティティ識別情報と、アクセスの内容を表す情報（以下、アクセス内容情報）を含む。エンティティ識別情報は、エンティティ同士を互いに識別するために利用される情報である。例えばユーザをエンティティとして扱う場合、エンティティ識別情報には、ユーザの識別情報や、ユーザが属するユーザグループの識別情報などを利用することができる。端末をエンティティとして扱う場合、エンティティ識別情報には、端末の識別情報（IP アドレスや MAC アドレスなどのアドレス情報など）や、端末が属する端末グループの識別情報（ネットワークグループの識別情報など）などを利用することができる。

[0044] アクセス内容情報は、リクエスト 20 によってリクエストされるアクセスの内容を表す。例えばアクセス内容情報は、アクセスされるデータのデータ識別情報と、そのデータに対するアクセスの種類を含む。アクセスの種類は、読み出しや書き込みなどである。また、アクセスの種類が書き込みである場合、アクセス内容情報には、書き込みの内容がさらに含まれる。

[0045] なお、前述したように、権限情報 70 は、データのグループや部分領域に

対応付けられていることもある。そこで、アクセス権限の有無の判定に、データのグループや部分領域の識別情報を利用してもよい。この場合、アクセス内容情報は、アクセスされるデータが属するグループのグループ識別情報や、アクセスされるデータが格納されている部分領域の領域識別情報をさらに示す。グループや部分領域についてのアクセス権限をチェックすることにより、その中に含まれる複数のデータにアクセスする際に、アクセス権限の有無の判定に要する時間を短くすることができる。

[0046] <権限情報 70 の取得 : S 104>

権限情報取得部 2040 は権限情報 70 を取得する (S 104)。前述したように、権限情報 70 は、アクセスの主体 (エンティティ) と客体の組み合わせに対して定められる。そこで権限情報取得部 2040 は、リクエスト 20 に示されている主体と客体の識別情報の組み合わせに対応する権限情報 70 を取得する。

[0047] リクエスト 20 において、アクセスの主体の識別情報は、対象エンティティのエンティティ識別情報である。一方、アクセスの客体の識別情報は、例えば、アクセス内容情報に含まれるデータ識別情報である。ただし前述したように、リクエスト 20 には、データグループ識別情報や領域識別情報が含まれていてもよい。この場合、アクセスの客体の識別情報として、データグループ識別情報や領域識別情報を利用する。

[0048] <<権限情報 70 の取得元について>>

前述したように、権限情報 70 はブロックチェーンストレージ 40 に格納されている。そこで例えば、権限情報取得部 2040 は、リクエスト 20 に示されている主体と客体の識別情報の組み合わせに対応する権限情報 70 を、ブロックチェーンストレージ 40 から取得する。

[0049] ただし、権限情報取得部 2040 は、ブロックチェーンストレージ 40 に格納されている情報の一部又は全てを予め別の記憶装置 (以下、第 3 記憶装置) にコピーしておき、リクエスト 20 に応じて取得する権限情報 70 については、この第 3 記憶装置から取得するようにしてもよい。アクセス制御装

置 2 0 0 0 から第 3 記憶装置へのアクセスは、アクセス制御装置 2 0 0 0 からブロックチェーンストレージ 4 0 へのアクセスよりも高速に行えることが好ましい。このように、高速にアクセスできる記憶装置に予め権限情報 7 0 をコピーしておくことにより、アクセス権限の判定をより高速に行えるようになる。例えば第 3 記憶装置は、アクセス制御装置 2 0 0 0 内に設けられている記憶装置である。

[0050] 権限情報取得部 2 0 4 0 は、第 3 記憶装置とブロックチェーンストレージ 4 0 の内容を同期させておく。なお、2 つの記憶装置の内容を同期させる具体的な技術には、既存の技術を利用することができる。

[0051] <アクセス権限の判定：S 1 0 6>

権限判定部 2 0 6 0 は、権限情報 7 0 を利用して、リクエスト 2 0 でリクエストされているアクセスが、対象エンティティ 1 0 のアクセス権限の範囲内であるか否かを判定する (S 1 0 6)。より具体的には、権限判定部 2 0 6 0 は、アクセス内容情報に示されている種類のアクセスが、取得した権限情報 7 0 において許可されているか否かを判定する。許可されている場合、対象エンティティ 1 0 のアクセス権限の範囲内であると判定される。一方、許可されていない場合、対象エンティティ 1 0 のアクセス権限の範囲内でないとして判定される。

[0052] ここで前述したように、リクエスト 2 0 は、アクセス権限を判定するための客体として、データグループや部分領域の識別情報を示していてもよい。この場合、データグループや部分領域の識別情報に対応する権限情報 7 0 が取得される。そこで例えば、権限判定部 2 0 6 0 は、アクセス内容情報によって示される「データ、そのデータへのアクセスの種類」のペアについて、1) そのデータがアクセス権限の判定に利用されたデータグループ又は部分領域に属するか否か、及び 2) その種類のアクセスが権限情報 7 0 において許可されているか否かという 2 つを判定する。

[0053] アクセス内容情報によって示されるデータがアクセス権限の判定に利用されたデータグループ又は部分領域に属しており、なおかつ、アクセス内容情

報によって示される種類のアクセスが権限情報 70 において許可されている場合、権限判定部 2060 は、リクエストされたアクセスが対象エンティティ 10 のアクセス権限の範囲内であると判定する。一方、アクセス内容情報によって示されるデータがアクセス権限の判定に利用されたデータグループ又は部分領域に属していない場合や、アクセス内容情報によって示される種類のアクセスが権限情報 70 において許可されていない場合、権限判定部 2060 は、リクエストされたアクセスが対象エンティティ 10 のアクセス権限の範囲内でないと判定する。

[0054] なお、権限判定部 2060 では 1) の判定を行わず、アクセス実行部 2080 が第 1 記憶装置 30 からアクセス対象のデータを探す範囲を、アクセス権限の判定に利用されたデータグループや部分領域に限定するようにしてもよい。このようにすることで、アクセス内容情報によって示されるデータが、アクセス権限の判定が行われたデータグループに属していない場合や、アクセス権限の判定が行われた部分領域に格納されていない場合、アクセス実行部 2080 はそのデータを見つけることができないため、そのデータにアクセスできない。よって、この方法でも、アクセス権限の範囲内でないアクセスが行われることを防ぐことができる。

[0055] <判定結果に基づくアクセスの制御：S108>

リクエストされたアクセスが対象エンティティ 10 のアクセス権限の範囲内であると判定された場合 (S106: YES)、アクセス実行部 2080 は、リクエストされたアクセスを実行する (S108)。一方、リクエストされたアクセスが対象エンティティ 10 のアクセス権限の範囲内でないと判定された場合 (S106: NO)、アクセス実行部 2080 は、リクエスト 20 によって示されているアクセスを実行しない。

[0056] 後者の場合、例えばアクセス実行部 2080 は、アクセス権限が無いためにリクエストされたアクセスを実行することができない旨を示す通知を出力する。リクエスト 20 が他の端末からアクセス制御装置 2000 へ送信されたものである場合、アクセス制御装置 2000 は、その端末へ通知を送信す

る。一方、リクエスト20が入力デバイス等を用いてアクセス制御装置2000へ入力されたものである場合、アクセス制御装置2000は、アクセス制御装置2000に接続されているディスプレイ装置などに通知を出力する。

[0057] なお、アクセス実行部2080は、リクエストされたアクセスを実行できた場合にも、所定の通知（アクセスを完了した旨の通知など）を出力してもよい。通知の出力先は、リクエストされたアクセスが実行されなかった場合の通知と同様である。

[0058] [実施例]

例えばアクセス制御装置2000は、所定のサービスを利用しようとしているユーザの本人確認に利用することができる。以下、アクセス制御装置2000の実施例として、本人確認に利用されるアクセス制御装置2000について説明する。ただし、以下の説明はあくまで例示であり、アクセス制御装置2000の利用方法は、ユーザの本人確認に限定されない。

[0059] 図6は、実施例のアクセス制御装置2000を例示する図である。この例では、ユーザ110が、保険会社Cによって提供されている保険に加入する手続を行う。この際、保険会社Cは、ユーザ110の正当な個人情報（氏名や住所など）を取得する必要がある。そこで例えば、保険会社Cは、店舗Sにおいてユーザ110から個人情報の提供を受け、なおかつ、その個人情報がユーザ110の正当な個人情報であることの確認（すなわち、本人確認）を行う。言い換えれば、ユーザ110が虚偽の個人情報を提供していないかどうかの確認が行われる。

[0060] アクセス制御装置2000を利用した本人確認を実現するため、ユーザの本人確認に利用できる情報を、予め第1記憶装置30に格納しておく。具体的には、ユーザの個人情報を、ユーザの認証情報と対応づけて第1記憶装置30に格納しておく。ユーザの認証情報は、ユーザ認証に利用できる任意の情報であり、例えば、顔画像などの生体情報や、アカウント情報（ユーザ名とパスワードのペア）などである。図6の例では、生体情報の一種である顔

画像が認証情報として利用されている。

- [0061] 例えば第1記憶装置30において、ユーザの認証情報と個人情報、そのユーザに割り当てられた部分領域32に格納される。言い換えれば、同一の部分領域32に格納された認証情報と個人情報は、互いに対応づけられたものである。権限情報70は、部分領域32の識別情報に対応付けて定められる。
- [0062] 保険会社Cを利用するユーザ110は、予め、ユーザ110の部分領域32への読み出し権限を、保険会社Cに対して与えておく。すなわち、「主体＝保険会社C、客体＝ユーザ110の部分領域32」という組み合わせに対応付けて、読み出し許可を示す権限情報70を、ブロックチェーンストレージ40に格納しておく。
- [0063] 例えばユーザ110の本人確認は、以下の流れで行われる。まず、ユーザ110は、保険会社Cの店舗Sへ行く。そして、ユーザ110は、店舗Sの店舗端末120に対し、ユーザ110の認証情報と、ユーザ110の部分領域32の領域識別情報とを提供する。図6の例では、店舗端末120に設けられているカメラでユーザ110の顔を撮像することにより、店舗端末120に対してユーザ110の顔画像が提供される。
- [0064] 店舗端末120は、アクセス制御装置2000へリクエスト20を送信する。このリクエスト20は、対象エンティティ10のエンティティ識別情報として保険会社Cの識別情報を示し、アクセス内容情報として「顔画像の読み出し」を示す。また、アクセス権限の判定のために、ユーザ110の部分領域32の領域識別情報を示す。
- [0065] 権限情報取得部2040は、「主体＝保険会社Cの識別情報、客体＝ユーザ110の部分領域32の領域識別情報」に対応する権限情報70を取得する。権限判定部2060は、取得した権限情報70において読み出しが許可されているか否かを判定することにより、リクエストされたアクセスが保険会社Cのアクセス権限の範囲内であるか否かを判定する。
- [0066] 前述したように、ユーザ110は、予め保険会社Cに対し、ユーザ110

の部分領域 32 への読み出し権限を与えておく。そのため、リクエストされたアクセスは保険会社 C のアクセス権限の範囲内であると判定される。そこでアクセス実行部 2080 は、ユーザ 110 の部分領域 32 から、ユーザ 110 の顔画像を読み出す。

[0067] アクセス制御装置 2000 は、店舗端末 120 から取得した顔画像（店舗 S でユーザ 110 を撮像することによって得られた顔画像）と、部分領域 32 から取得した顔画像とを照合する（これらが同一個人のものであるか否かを判定する）。これらが同一個人のものであると判定された場合、部分領域 32 に格納されている個人情報、ユーザ 110 の正当な個人情報であると言える。そこでアクセス制御装置 2000 は、ユーザ 110 の部分領域 32 からユーザ 110 の個人情報を取得し、店舗端末 120 へ提供する。一方、これらが同一個人のものでないと判定された場合、アクセス制御装置 2000 は、認証に失敗した旨のエラー通知を店舗端末 120 へ送信する。なお、2 つの顔画像が同一個人のものであるか否かを判定する方法には、既存の方法を利用できる。例えば制御装置 2000 は、2 つの顔画像の類似度を算出し、その類似度を所定の閾値と比較する。類似度が所定の閾値以上である場合には、2 つの顔画像が同一個人のものであると判定され、類似度が所定の閾値未満である場合には、2 つの顔画像が同一個人のものでないと判定される。

[0068] アクセス制御装置 2000 からユーザ 110 の個人情報を取得した場合、店舗端末 120 は、ユーザ 110 から提供された個人情報と、アクセス制御装置 2000 から提供された個人情報（すなわち、ユーザ 110 の部分領域 32 から読み出された個人情報）とが一致するか否かを判定する。これらが一致した場合、店舗端末 120 は、店舗 S においてユーザ 110 から提供された個人情報が正当なものであると判定する。すなわち、保険会社 C の店舗 S を訪れたユーザ 110 が本人であることを確認することができる。

[0069] なお、店舗端末 120 は、必ずしも上述した個人情報の一致の確認を行わなくてもよい。例えば、個人情報の一致の確認は、アクセス制御装置 2000

０によって行われてもよい。この場合、店舗端末１２０は、ユーザ１１０から提供された個人情報もアクセス制御装置２０００へ送信する。そして、アクセス制御装置２０００は、店舗端末１２０から提供された個人情報（すなわち、店舗Ｓにおいてユーザ１１０から提供された個人情報）と、ユーザ１１０の部分領域３２から取得した個人情報とが一致するか否かの確認を行う。

[0070] また、店舗端末１２０は、ユーザ１１０から個人情報を取得しなくてもよい。例えばこの場合、ユーザ１１０は、個人情報を申込用紙などに記入する。そして、店舗Ｓの店員が、店舗端末１２０がアクセス制御装置２０００を経由して表示する、ユーザ１１０の部分領域３２の個人情報を参照し、申込用紙に記入された個人情報と比較することで、ユーザ１１０の本人確認をする。

[0071] その他にも例えば、保険会社Ｃは、ユーザ１１０に対して個人情報の入力や記入を求めず、店舗端末１２０が上述した流れでアクセス制御装置２０００から取得する個人情報を、ユーザ１１０の個人情報として利用してもよい。この場合、ユーザ１１０は、顔画像などの認証情報を提供すれば自動的に個人情報を提供することができる。そのため、ユーザによる個人情報の入力の手間が軽減される。また、個人情報の入力誤りが生じることを防ぐことができる。

[0072] 上述した流れで本人確認に成功した場合、アクセス制御装置２０００は、ユーザ１１０の認証情報と個人情報のペアの正当性が確認されたことを表す情報（以下、確認情報）を、ユーザ１１０の部分領域３２に格納してもよい。例えば確認情報には、本人確認を行った会社や政府の機関など（以下、会社等）の識別情報が含まれる。以下、本人確認を行った会社等を確認者とも表記する。

[0073] このような確認情報を格納することにより、その後にユーザ１１０が利用する他の会社等は、既にユーザ１１０について本人確認が行われている事実を利用して、ユーザ１１０へサービスを提供すべきかどうかの判断などを効

率的に行うことができる。例えば、１）パスポートを発行する機関が、ユーザの部分領域３２に格納されているパスポートのデータが正当であることを表す確認情報を部分領域３２に格納する、２）運転免許証を発行する機関が、ユーザの部分領域３２に格納されている運転免許証のデータが正当であることを表す確認情報を部分領域３２に格納する、３）決済サービスを提供する会社が、ユーザの部分領域３２に格納されている決済サービスについての情報（決済余力など）が正当であることを表す確認情報を部分領域３２に格納する、などといった例が挙げられる。

[0074] また、確認情報には、本人確認の後に行われた種々の手続等の結果を表す情報がさらに含まれてもよい。例えば前述した保険会社の例では、本人確認の後に締結された保険契約に関する情報を確認情報に含めることができる。

[0075] なお、本人確認が行われた情報がその後に書き換えられることを防ぐため、本人確認が行われた情報に対して確認者の電子署名が付されてもよい。例えば、ユーザ１１０の認証情報と個人情報のペアが正当であることが確認されたら、確認者の秘密鍵を利用して生成された電子署名が当該ペアに対して付される。具体的には、確認者の識別情報、及び上記電子署名付きのデータを含む確認情報が、ユーザ１１０の部分領域３２に格納される。

[0076] その後にユーザ１１０の認証情報及び個人情報を利用したい他の会社等は、ユーザ１１０の部分領域３２から上記確認情報を取得し、確認情報に示されている識別情報で特定される確認者の公開鍵を利用して、確認情報に含まれるデータに付されている電子署名の復号を行う。こうすることで、確認情報に含まれる電子署名付きのデータが、本人確認後に更新されていないこと、および他の確認者が当該個人情報の正当性を認めた事実を確認できる。なお、電子署名を利用してデータの書き換えが行われていないことを確認する具体的な方法については、既存の方法を利用することができる。

[0077] 以下、確認情報を利用する具体的なケースについて例示する。

[0078] <<確認情報を利用するケース１>>

例えばユーザ１１０が、レンタカーを利用するとする。この場合、ユーザ

１１０は予め、レンタカー会社Ｘが提供するウェブサイトで、レンタカーの予約をしておく。予約の際、ユーザ１１０は、認証情報や個人情報を提供する。その結果、ユーザの認証情報、ユーザの個人情報、予約日時、及び利用する車の種類などを含む予約情報が、レンタカー会社Ｘの予約管理サーバに保存される。また、ユーザ１１０は、ユーザ１１０の部分領域３２への読み出し権限を、レンタカー会社Ｘに与えておく。そして、レンタカーを利用する当日、ユーザ１１０は、レンタカー会社Ｘの店舗Ｙへ行く。

[0079] ユーザ１１０は、店舗Ｙでレンタルの手続を行う。具体的には、まず、店舗Ｙの店舗端末Ｒが、ユーザ１１０に関する予約情報をサーバから読み出す。そのために、店舗端末Ｒは、ユーザ１１０から認証情報を取得し、予約管理サーバへ送信する。例えば予約管理サーバは、予約日時が当日である予約情報の中から、店舗端末Ｒから提供された認証情報とマッチする認証情報を示すものを特定し、店舗端末Ｒへ提供する。

[0080] また、店舗端末Ｒは、ユーザ１１０の本人確認を行う。具体的には、ユーザ１１０の部分領域３２からユーザ１１０の個人情報を取得もしくは参照し、その個人情報と予約情報に含まれる個人情報が一致するか否かを確認する。なお、ユーザ１１０の部分領域３２からユーザ１１０の個人情報を取得もしくは参照する処理の流れは、前述した保険会社Ｃのケースで説明した流れと同様である。

[0081] さらに今回のケースでは、前述した保険会社Ｃにより、ユーザ１１０の部分領域３２に確認情報が格納されている。この確認情報には、保険会社Ｃの識別情報に加えて、ユーザ１１０との間で締結された保険契約に関する情報も含むことができる。レンタカー会社Ｘは、この確認情報を利用して、ユーザ１１０が加入している保険について、保険会社Ｃによって正当性が保証されている情報を得ることができる。

[0082] 例えばレンタカー会社Ｘは、ユーザ１１０が加入している保険の情報を参照することにより、ユーザ１１０がレンタカーを利用するために一時的な保険へ加入する必要があるか否かをチェックするといったことが可能となる。

[0083] <<確認情報を利用するケース2>>

例えば確認情報は、キャッシュレス決済に利用することができる。そのために、ユーザ110は、第1記憶装置30に格納されている生体情報（認証情報）を利用し、決済サービスを提供する会社Z（例えばクレジットカード会社）に対し、決済サービスの申込みを行う。その結果、ユーザ110の部分領域32には、会社Zが提供する決済サービスの情報を含む確認情報が格納される。なお、ここでいう「決済サービスの申込み」は、会社Zが提供する決済サービスを新規に申し込むものであってもよいし、既に会社Zのクレジットカード等の媒体を利用している状況において、そのような媒体無しに生体情報のみで決済を行えるようにする追加の申込みであってもよい。

[0084] 決済サービスが利用可能になったら、ユーザ110は、その決済サービスを利用できる店舗で買い物をする。店舗の決済端末P1は、決済を行うために、ユーザ110の生体情報を取得する（例えばユーザ110の顔をカメラで撮像する）。決済端末P1は、その生体情報を含むリクエストをアクセス制御装置2000へ送信する。アクセス権限の確認後、アクセス制御装置2000は、ユーザ110の部分領域32から生体情報を取得し、決済端末P1から提供されたユーザ110の生体情報との照合を行う。

[0085] 決済端末P1から提供されたユーザ110の生体情報とユーザ110の部分領域32から取得した生体情報とが同一個人のものであると判定されたら（すなわち、認証に成功したら）、アクセス制御装置2000は、会社Zによって部分領域32に格納された確認情報を取得し、決済端末P1に提供する。決済端末P1は、確認情報に含まれる決済サービスの情報を利用して、決済を実行する。このような流れにより、ユーザ110は、現金やカードなどの媒体を提示することなく、決済を行うことができる。

[0086] なお、上述の決済サービスを実現するためには、上記決済端末P1からのリクエストに応じてユーザ110の部分領域32からデータを読み出すことができるように、アクセス権限を設定しておく必要がある。そこで例えば、会社Zから提供される決済サービスを受け入れる各店舗のグループを表すエ

ンティティを用意し、そのエンティティに対し、部分領域 32 への読み出しアクセスの権限を与えておく。会社 Z から提供される決済サービスを受け入れる各店舗の決済端末は、アクセス制御装置 2000 へリクエスト 20 を送信する際、上述したエンティティとしてリクエストを送信する。こうすることで、複数の店舗に対して一括でアクセス権限を設定できる。

[0087] <<確認情報を利用するケース 3>>

例えば確認情報は、MaaS (Mobility as a Service) を実現するために利用される。MaaS では、飛行機、電車、又はバスなどのように、それぞれ異なる事業者によって提供される交通手段を乗り継いで移動するようなケースにおいて、事業者を跨がって一括のサービスを受けることが可能となる。例えば、特定の範囲にある様々な交通手段を、一日定額で乗り放題にするといったサービスが提供される。

[0088] 例えばユーザ 110 は、前述した保険会社 C と保険の契約を締結する流れと同様の流れで、上述した MaaS のサービスの利用契約を行う。ここでいうサービスの利用契約とは、指定した期間に指定した範囲で提供される各交通手段を自由に利用できるようにするための契約である。サービスの契約が完了したら、ユーザ 110 の部分領域 32 に、ユーザが利用できるサービスの契約内容を含む確認情報が格納される。

[0089] 上記サービスを利用するために、ユーザ 110 は、乗り物 V に設置されている決済端末 P2 に対し、認証情報を提供する（決済端末 P2 がユーザ 110 の顔をカメラで撮像する）。決済端末 P2 は、取得した認証情報を含むリクエスト 20 を、アクセス制御装置 2000 に送信する。アクセス制御装置 2000 は、認証に成功すると、上述した確認情報を部分領域 32 から読み出して、決済端末 P2 に提供する。

[0090] 決済端末 P2 は、取得した確認情報に含まれているサービスの契約内容を参照し、乗り物 V の利用が契約の範囲内であるか否かを判定する。契約の範囲内である場合、決済端末 P2 は、ユーザ 110 に代金の支払いを求めることなく、ユーザ 110 に乗り物 V の利用を許可する（例えば、入り口のゲー

トを開く)。一方、契約したサービスの範囲内でない場合、決済端末P2は、ユーザ110に対し、代金の支払いを請求する。

[0091] なお、上述の Maas のサービスを実現するためには、決済端末P2からのリクエストに応じてユーザ110の部分領域32からデータを読み出すことができるように、アクセス権限を設定しておく必要がある。そこで例えば、前述した MaaS のサービスに加入している各交通手段の事業者のグループを表すエンティティを用意し、そのエンティティに対し、部分領域32への読み出しアクセスの権限を与えておく。MaaS のサービスに加入している各交通手段の決済端末等は、アクセス制御装置2000へリクエスト20を送信する際、上述したエンティティとしてリクエストを送信する。こうすることで、複数の事業者に対して一括してアクセス権限を設定できる。

[0092] 上記の実施形態の一部又は全部は、以下の付記のようにも記載されうるが、以下には限られない。

1. 第1記憶装置に格納されているデータへのアクセスのリクエストを取得するリクエスト取得部と、

前記第1記憶装置へのアクセスに関するアクセス権限を表す権限情報が格納されている第2記憶装置から前記権限情報を取得する権限情報取得部と、

前記リクエストの主体である対象エンティティについての前記権限情報を用いて、前記アクセスが前記対象エンティティのアクセス権限の範囲内であるか否かを判定する権限判定部と、

前記アクセスが前記対象エンティティのアクセス権限の範囲内であると判定された場合、前記アクセスを実行するアクセス実行部と、を有し、

前記第2記憶装置はブロックチェーンストレージである、アクセス制御装置。

2. 前記第1記憶装置にはユーザの認証情報が格納されており、

前記リクエストが示すアクセスは、ユーザの認証情報の読み出しを含み、

前記リクエストには、認証対象のユーザの認証情報が含まれており、

前記アクセス実行部は、前記リクエストに含まれる認証情報と、前記第1

記憶装置に対するアクセスによって読み出した認証情報とを比較することにより、前記認証対象のユーザについて認証を行う、１．に記載のアクセス制御装置。

３． 前記認証情報は生体情報である、２．に記載のアクセス制御装置。

４． 前記アクセス実行部は、前記認証の結果を表す通知を出力し、
前記通知には、前記第１記憶装置から取得した認証情報が含まれない、２．又は３．に記載のアクセス制御装置。

５． 前記第１記憶装置において、ユーザごとに部分記憶領域が割り当てられており、

前記第２記憶装置において、エンティティの識別情報と前記部分記憶領域の識別情報の組み合わせに対応付けて、そのエンティティがその部分記憶領域に対して持つアクセス権限を表す前記権限情報が格納されている、１．から４いずれか一つに記載のアクセス制御装置。

６． 第１のユーザの前記部分記憶領域に、前記第１のユーザの認証情報と個人情報とが格納されており、

前記アクセス実行部は、前記第１のユーザの認証に成功し、かつ、前記第１のユーザの個人情報が正当であることが確認された場合に、当該確認の結果を表す確認情報を、前記部分記憶領域に格納する、５．に記載のアクセス制御装置。

７． コンピュータによって実行される制御方法であって、

第１記憶装置に格納されているデータへのアクセスのリクエストを取得するリクエスト取得ステップと、

前記第１記憶装置へのアクセスに関するアクセス権限を表す権限情報が格納されている第２記憶装置から前記権限情報を取得する権限情報取得ステップと、

前記リクエストの主体である対象エンティティについての前記権限情報を用いて、前記アクセスが前記対象エンティティのアクセス権限の範囲内であるか否かを判定する権限判定ステップと、

前記アクセスが前記対象エンティティのアクセス権限の範囲内であると判定された場合、前記アクセスを実行するアクセス実行ステップと、を有し、

前記第2記憶装置はブロックチェーンストレージである、制御方法。

8. 前記第1記憶装置にはユーザの認証情報が格納されており、

前記リクエストが示すアクセスは、ユーザの認証情報の読み出しを含み、

前記リクエストには、認証対象のユーザの認証情報が含まれており、

前記アクセス実行ステップにおいて、前記リクエストに含まれる認証情報と、前記第1記憶装置に対するアクセスによって読み出した認証情報とを比較することにより、前記認証対象のユーザについて認証を行う、7.に記載の制御方法。

9. 前記認証情報は生体情報である、8.に記載の制御方法。

10. 前記アクセス実行ステップにおいて、前記認証の結果を表す通知を出力し、

前記通知には、前記第1記憶装置から取得した認証情報が含まれない、8.又は9.に記載の制御方法。

11. 前記第1記憶装置において、ユーザごとに部分記憶領域が割り当てられており、

前記第2記憶装置において、エンティティの識別情報と前記部分記憶領域の識別情報の組み合わせに対応付けて、そのエンティティがその部分記憶領域に対して持つアクセス権限を表す前記権限情報が格納されている、7.から10.いずれか一つに記載の制御方法。

12. 第1のユーザの前記部分記憶領域に、前記第1のユーザの認証情報と個人情報が格納されており、

前記アクセス実行ステップにおいて、前記第1のユーザの認証に成功し、かつ、前記第1のユーザの個人情報が正当であることが確認された場合に、当該確認の結果を表す確認情報を、前記部分記憶領域に格納する、11.に記載の制御方法。

13. 7.から12.に記載の制御方法をコンピュータに実行させるプログ

ラム。

符号の説明

- [0093] 1 0 対象エンティティ
2 0 リクエスト
3 0 第1記憶装置
3 2 部分領域
4 0 第2記憶装置、ブロックチェーンストレージ
7 0 権限情報
1 0 0 テーブル
1 0 2 エンティティ識別情報
1 0 4 客体識別情報
1 1 0 ユーザ
1 2 0 店舗端末
1 0 0 0 計算機
1 0 2 0 バス
1 0 4 0 プロセッサ
1 0 6 0 メモリ
1 0 8 0 ストレージデバイス
1 1 0 0 入出力インタフェース
1 1 2 0 ネットワークインタフェース
2 0 0 0 アクセス制御装置
2 0 2 0 リクエスト取得部
2 0 4 0 権限情報取得部
2 0 6 0 権限判定部
2 0 8 0 アクセス実行部