(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号
特許第7007077号
(P7007077)
(45)発行日　令和4年1月24日(2022.1.24)　(24)登録日　令和4年1月11日(2022.1.11)

(51)Int.Cl.		F I		
G06F 21/31	*(2013.01)*	G06F	21/31	360
G09C 1/00	*(2006.01)*	G09C	1/00	640E
H04L 9/32	*(2006.01)*	H04L	9/32	200B

請求項の数 3　(全 194 頁)

(21)出願番号　特願2021-121886(P2021-121886)
(22)出願日　令和3年7月26日(2021.7.26)
(62)分割の表示　特願2021-4788(P2021-4788)の分割
原出願日　令和3年1月15日(2021.1.15)
審査請求日　令和3年7月27日(2021.7.27)

(73)特許権者　714009083
西沢　克弥
長野県上田市吉田５１５番地２
(72)発明者　西沢　克弥
長野県上田市吉田５１５番地２

審査官　小林　秀和

(56)参考文献　特開２００５－３２１９２８（ＪＰ，Ａ）
特開２００７－０４３４１６（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】鍵情報を持つ端末の環境に由来するデータを収集する不正アクセス防止システム

(57)【特許請求の範囲】
【請求項１】
サービス提供端末に対してネットワークを介して接続されたユーザ端末がサービス提供端末にアクセスした際に、
前記ユーザ端末に記憶されたユーザーUAの秘密鍵に基づくユーザ識別子Ａと、
前記ユーザ端末の備えるセンサがある時刻Tにおいて前記ユーザー端末の置かれた物理環境より計量した端末センサ値を、
ある時刻Tにおいて前記ユーザー端末の置かれた環境により一意に決定する数値として直接サービス提供端末に収集し記録させ、
もしくは前記ユーザ識別子Ａと前記端末センサ値をハッシュ関数によりハッシュ化または匿名化して得られたハッシュ値をある時刻Tにおいて前記ユーザー端末の置かれた環境により一意に決定する数値として直接サービス提供端末に収集し記録させ、
もしくは前記ユーザ識別子Ａと前記端末センサ値または前記ハッシュ値
を含む値ＩＰＶをある時刻Tにおいて前記ユーザー端末の置かれた環境により一意に決定する数値として直接収集しサービス提供端末に記録させ、
前記サービス提供端末に前記ユーザ端末のログイン時刻Tまたはアクセス時刻Tまたは閲覧時刻Ｔと、ログイン履歴情報またはアクセス履歴情報または閲覧履歴情報Ｃｎｔをサービス提供端末に記録させ、
前記サービス提供端末に前記ユーザー識別子と前記端末センサ値
または前記端末センサ値をハッシュ関数によりハッシュ化して得られたハッシュ値

または前記端末センサ値を含むIPV値とを対またはペアにして前記ユーザー識別子ごとに記憶させたデータ構造について、
前記ユーザ識別子Ａに対し、異なる前記端末センサ値もしくは前記ハッシュ値もしくは前記端末センサ値または前記ハッシュ値を含む値ＩＰＶからのアクセスが行われたか否かを記録し監視する制御部と記憶部を前記サービス提供端末に備え、
ユーザＵＡの秘密鍵から計算される前記ユーザ識別子Ａについて複数の異なる前記端末センサ値もしくは前記ハッシュ値もしくは前記値ＩＰＶを持つ前記ユーザ端末から前記サービス提供端末へアクセスが行われている場合には、
前記ユーザーＵＡの登録した電子メールアドレスや電話番号へ不正使用を通知させ又は前記ユーザーUAの秘密鍵から計算されるユーザー識別子Aに向け不正使用通知型トークンまたは通知データを分散型台帳システムまたはサービス提供端末の記憶装置に記憶させユーザーへ通知する不正アクセス監視機能と不正アクセス通知機能を備えた前記サービス提供端末とセンサを備えた前記ユーザー端末を用いる、
秘密鍵情報の不正利用を検出し通知することの出来るコンピューターネットワークシステム。
【請求項２】
請求項１に記載のコンピューターネットワークシステムにおいて、
ユーザー端末の入力装置のセンサが検出し測定した物理量の数値を、前記ユーザーの端末のセンサが測定する地磁気や重力加速度または加速度または角速度の物理情報や温度や気圧または照度の物理的な値から測定される前記ユーザーの端末の置かれた環境に依存する１つ以上のセンサ情報を前記ユーザー端末に特有の識別情報に用いる特徴を持ち、
前記ユーザー端末がサービス提供端末にアクセスし、サービスの利用時に前記サービス提供端末に前記ユーザー端末のセンサが測定したセンサ値を収集させ同一時刻TにユーザーＵＡの秘密鍵から計算されるユーザー識別子Ａに対し、サービス提供端末にアクセスしている複数のユーザー端末が存在しているか監視し、
複数のユーザー端末が存在する際には、前記ユーザー識別子Aを計算する基になる秘密鍵がユーザ端末のログイン時刻またはアクセス時刻または閲覧時刻Ｔにおいて複数のユーザー端末に秘密鍵を共有されまたは前記秘密鍵を使い回される形で不正アクセスが行われている恐れを通知する不正アクセス監視機能と不正アクセス通知機能を備えたサービス提供端末を用いるシステムであって、
前記ユーザー端末の入力装置のセンサにモーションセンサまたは位置センサまたは環境センサを一つまたは複数を備え、
前記モーションセンサーには加速度センサまたは加速度計またはジャイロセンサまたは角速度センサを備え、前記位置センサには地磁気センサまたは加速度計を備え、
前記環境センサには温度センサまたは湿度センサまたは光センサまたは照度センサまたは気圧センサまたは圧力センサを備え、
前記センサの種類のうち一つまたは複数の種類のセンサのある時刻Ｔにおける測定値を秘密鍵の不正利用の検出と通知に用いる事を特徴にするコンピューターネットワークシステム。
【請求項３】
　請求項１から請求項２の何れかに記載のコンピュータネットワークシステムにおいて、
ユーザー識別子のデータサイズDtAdは秘密鍵のデータサイズDtKyと等しい又はDtKyより小さいという条件すなわちDtKy≧DtAdの関係を満たす特徴を持ったコンピューターネットワークシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は利用者の認証を行うシステムや装置に関するものである。
【背景技術】
【０００２】

＜次に参考として原出願にある明細の内容を記載する。＞
インターネットの普及に伴い商取引から電子商取引、対面の銀行取引からインターネットバンキング（ネットバンキング）へと、現実空間のサービスをコンピュータとネットワークを用いたデジタル空間で行う事が可能となっている。電子メールの閲覧、動画音楽サイトの閲覧、ソーシャル・ネットワーキング・サービス、ネットバンキング、電子商取引サイトへのログインへのログインなど認証によるログインを伴ったウェブサービスは拡大している。
インターネットサービスにおいてを用いて顧客にウェブサイトでサービスを提供する際に、サービスに登録した顧客へ電話番号あるいはユーザーＩＤ（あるいはユーザのニックネーム）、電子メールアドレスとパスワードを登録させ、ウェブサイトにログインさせる。ここでウェブサイトにログインしたのち、より価値の高いデータを操作する場合がある。
例えばインターネットバンキングにおいて他者の銀行口座に振り込むときに、ログインに利用したパスワードとは異なる認証法を持ちいて、ログインしている者が利用者本人かどうかの確認をする必要がある。パスワードのみではその情報が他者に漏洩し悪用された場合に、インターネットバンキングに不正にアクセスされ資産の移動を支持され資産を悪意のある者に奪われかねない。
【０００３】
そこでユーザー本人を確認する方法にパスワード以外の方法を組み合わせる必要がある。本人を確認し認証する方法として多く分けて、１．本人が知る知識、２．本人の持つ所有物、３．本人の生体特徴の３つがある。例として次の例が挙げられる。
１．本人が知る知識は合言葉、パスワード、４桁の暗証番号などである。
パスワードは静的である。攻撃者がパスワードを不正入手したりパスワード総当たり攻撃などを行う事も想定される。パスワード総当たり攻撃に対しては本人が定期的に異なる時刻において更新し動的なパスワードとする必要がある。4桁の暗証番号に関しては００００から９９９９までの暗証番号を総当たりで入力する総当たり攻撃が行われることが想定される。
それに対抗するために認証が成功しない回数を記録し、連続で3回から5回程度認証の失敗が生じた場合認証を行わせなくする方法がとられる。暗証番号による認証を実行した回数を記録し、それが成功した場合に回数をゼロに戻し、回数が一定数を超えると認証の実行そのものを行えなくする処理を行うことが考えられる例えば日本国において利用されている個人番号カードにおいて暗証番号は3回から5回間違えると利用が停止される。
２．本人の持つ所有物は動的パスワード生成器やＩＣキャッシュカード、個人番号カードである。（電子計算機の分野の外では木材や金属等で作製された鍵や印鑑なども認証に使う所有物に属する。）
本発明では一般の人間が記憶できないほど長くランダム性のあるパスワード、例えば公開鍵暗号に２５６ビットの秘密鍵データを使う場合、その秘密鍵は紙などに印刷するかデジタル機器に記録して利用するので所有とみなす。またＩＣカードのうち個人番号カードは電子証明書のデータを含んでおり、個人番号カードのＩＣチップに記録された秘密鍵のデータ・情報は外部に取り出すことができないので所有とみなせる。
一般に人間が記憶できる数字や文字の個数は７プラスマイナス２とされている（注１）。７を超える数、例えば２５６ビットで２の２５６乗の数を表現できる３２バイトの秘密鍵や、個人番号カードに採用される２０４８ビットの秘密鍵は人間が記憶できず、秘密鍵のデータ（秘密鍵情報）を紙などに印刷もしくは板材などに刻印するか、レコード盤や磁気テープに記録するか光ディスク、磁気ディスク、半導体メモリなどのデジタル機器に記憶させる必要があり、本人の知る知識というよりは本人の所有するものである。
秘密鍵は印鑑や金属製の鍵と同じくそれを表すデータが漏洩した場合には複製されるリスクがある。その一方で生体認証情報のように更新不可能ではなく利用者の求めに応じて、不正利用されている秘密鍵の利用を停止し、新たな秘密鍵を利用者に割り当てて、対応付けをして、秘密鍵の切り替えを行うことができる。秘密鍵の情報は一つに定めなくても

よい。
秘密鍵や動的パスワード生成器はセキュリティを向上させるため、利用者とサービス提供者の間で定期的に更新することができる。動的パスワード生成器や秘密鍵の更新はそれに対応したサービスに対応する認証手段を提供する個人や法人が行う。動的パスワードの他、顧客に番号表を送付しその番号表に従った正しい数値文字の入力がログイン後のウェブサイトで行えるか調べる認証法も存在する。
これらの方法においてサービスを行うもの（銀行など）とユーザーの間で合意形成が続くことが重要であり、合意形成を助ける手段に本発明も含むデジタルな認証手段は利用される。本発明はＴＯＴＰトークンや紙の有価紙葉や金属の鍵などのようにあくまで道具であり、それらを使いサービスを受けられるかはユーザーとサービス提供者の合意や各国の法に基づく。
（注１）Miller, G. A. (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. Psychological Review , 63(2) , 81 - 97.
３．本人の生体特徴は指紋や顔、虹彩、声、静脈パターン情報、遺伝子情報など身体情報と、筆跡や歩行、話者認証など行動的特徴を利用するものがある。
生体認証は利用者の備える情報を用いるので、認証の鍵となる情報はその利用者の身体が健在であれば利用者と共にあり、金属の鍵などと比べると紛失する可能性が低い。この特性を用いてコンピュータ端末機器などのソフトウェアにおいて簡易なログインに用いる。
一方で生体情報の変更は困難である。生体情報が流出した場合、金属の鍵やパスワードのように変更することが困難である。生体認証を行う鍵である生体データをもとに偽の生体的特徴を複製して錠となる認証用のセンシング装置を誤認させ突破することも考えられる。
また指紋などは利用者がログインをしたいという意志がなくとも機器を解除できてしまう。すなわち攻撃者が利用者の意志が明確でないときに利用者の身体を使い無理やり認証を行う恐れもある。
生体認証では認証する装置に本人のデータが伝えられたことがわかるのであって、本人の意志によるものかの断定はさらなる要素が必要になる。したがって生体特徴を認証に使う場合は知識、もしくは所有物による認証と組み合わせ多要素認証とすることが好ましい。
銀行の提供するインターネットバンキングのサービスなど資産を扱う場合には生体認証などをログインパスワードの代わりに用い、さらに本人の持つ所有物を認証に使う手段（パスワード生成器）を併用し多要素、多段階の認証を行いセキュリティを高めている。
【０００４】
ここで本人の持つ所有物を認証に使う手段の一つにハードウェア型の動的パスワード生成器が挙げられる。動的パスワードの生成アルゴリズムとしてＲＦＣ６２３８規格が知られる。ＲＦＣ６２３８規格では時刻に基づいて生成される動的に変化する一度限りのパスワードを利用している。このような時間によって変化する一度限りの使い捨てパスワードを時間ベースのワンタイムパスワード（ＴＯＴＰ、Ｔｉｍｅ－Ｂａｓｅｄ－Ｏｎｅ－Ｔｉｍｅ－Ｐａｓｓｗｏｒｄ）という。ＴＯＴＰはハードウェア型及びソフトウェア型のワンタイムパスワード表示器に利用できる。ある決められた時間ごとにＴＯＴＰは変化する。
ＴＯＴＰを用いて本人宛てに送付したワンタイムパスワード（ＯＴＰ、Ｏｎｅ－Ｔｉｍｅ－Ｐａｓｓｗｏｒｄ）表示器に表示された７から６桁数字のパスワードを、インターネットバンキングのウェブサイトやスマートフォンのアプリ等に入力しＴＯＴＰ認証を行いウェブサイトでの操作を実行することで、本人確認が行われたとみなし、指示されたプログラムを動作させ、他行の他者の銀行口座への振込など重要な処理を行う。
本人の持つワンタイムパスワード生成器と本人が知る知識のパスワードとを併用し二要素認証を実現でき、セキュリティを向上させることができる。
【０００５】

一方で既存のワンタイムパスワード生成器にも課題があった。例としてインターネットバンキング等のサービスを行う既存のハードウェア型ワンタイムパスワード表示器（ハードウェア型ＴＯＴＰトークン）では、銀行のサーバ端末とパスワード表示器との時刻を同期させる必要があり、ハードウェア型ＴＯＴＰトークンが備える時計としての機能を維持し時刻を同期するために利用する電池については電池消耗が起きるため、定期的に電池交換を行うことが必要となり、ワンタイムパスワードの更新する際に顧客に新たなハードウェア型ＴＯＴＰトークンを郵送ないし配達する必要があり、送料が掛かるという課題があった。（ただしハードウェアＴＯＴＰトークンは印鑑と同じく所有できる物でありネットワークに接続されないため、ＴＯＴＰの計算に用いる秘密にすべきキー情報がネットワーク経由で漏洩しにくいことも期待できる）

またＲＦＣ６２３８規格（非特許文献３）によればパスワードはハッシュ関数の引数に時間Ｔと、秘密にする必要のあるキー情報Ｋ（シード値ＫまたはシークレットＫ）を用いてハッシュ値を計算するが、Ｋについての情報が漏洩した場合にはユーザーのハードウェア型ＴＯＴＰトークンをすべて更新する必要がある。そこで漏洩の有無に限らずＫを定期的な電池交換の際にトークンごと更新することセキュリティを保つともできる。
また既知のハードウェアＴＯＴＰトークンの認証用パスワードの表示整数が６桁から７桁であるが、ワンタイムパスワード（ＯＴＰ）トークンの総当たり攻撃を行う計算機の処理能力が増加する場合には表示整数の桁数を増加させ１２ケタなどに更新し変更できてもよく、表示する際の時刻も更新し変更できれば良いかもしれないと発明者は考えた。（発明者は将来に既知の計算機を凌駕する処理力を持つ計算機端末による総当たり攻撃に対抗するためにＯＴＰトークン表示桁数を増減し表示時間も増減できれば良いと考えた。）

【０００６】

また発明者はウェブサイトでのＯＴＰトークンによるログイン方法を暗号化されたファイルで行う手段を探索していた。ある特定の個人法人や団体に対して伝えたい平文のデータファイルを暗号化してそのアクセス権となる鍵を用い復号できれば機密情報やコンテンツの配布におおいに役立つと考えた。

暗号化したファイルの閲覧に固定式のパスワードを利用することが一般的であるが、これをＴＯＴＰを用いて暗号化を解除し復号後に閲覧・実行・利用出来るようにして、暗号化を解くことの出来る鍵となる閲覧権をハードウェアトークンのようにトークン化してやり取りし、機密情報の取引やあるコミュニティ内部での情報、電子書籍のような利用、事務処理ソフトウェア等の復号、閲覧、利用を行うソフトウェアを備えた装置を提供したいという課題があった。さらにコンテンツを災害時などオフライン時でも閲覧できるようにすることも必要と考えた。

ファイルの閲覧に加えて、ネットバンキングサイト等ウェブサイトへのログインシステム、現実世界でのチケットとその読み取りシステムや施錠部の解錠システムや乗り物や装置や計算機端末の始動システムも必要と考えた。そして現実世界とウェブサービス及びデジタル世界の双方で利用できるアクセス制御システムを使用できるようにしたいと考えた。

【０００７】

ここで非特許文献１や非特許物件２のようにブロックチェーン型もしくは有向非巡回グラフ型のデータ構造を持ち、分散された端末間で改ざん困難な分散型台帳システムＤＬＳを用いて暗号資産の発行や譲渡取引の記録、ＤＬＳ上でのトランザクションにプログラムコードを記録させブロックチェーンなどの改ざん困難なデータ構造の中に保存して運用するスマートコントラクト（コントラクト）という技術が利用可能となった。

特許文献１は音楽の権利に関するブロックチェーンまたは分散型台帳技術ＤＬＴの利用例の一つであり、特許文献２も分散型台帳の１つのコントラクトで複数のファイル管理システムの情報を管理するシステムの例である。コントラクトを用いコントラクトに属する変数や関数といったプログラム情報が改ざんされずに分散型台帳に記録されネットワークを介してノードとなる端末が世界中に分散可能であって、前記のノードで構成される分散型台帳システムＤＬＳにコントラクトというプログラムを世界中に展開（デプロイ）し国

境を越えてサービスを提供しうる事が分散型台帳技術および分散型台帳システムの特徴である。

【先行技術文献】

【特許文献】

【０００８】

【特許文献１】特許第６７５７０４２号

【特許文献２】特開２０２０－１４４５８６公報

【非特許文献】

【０００９】

【非特許文献１】Vitalik Buterin、「Ethereum White Paper A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM」、［online］、［西暦2020年、令和２年１１月１６日検索］、インターネット〈URL：https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf〉

【非特許文献２】ＩＯＴＡ財団、「Differences between the Tangle and blockchain」、［online］、［西暦2020年、令和２年１１月１６日検索］、インターネット〈URL：https://docs.iota.org/docs/getting-started/1.1/the-tangle/tangle-vs-blockchain

【非特許文献３】Internet Engineering Task Force (IETF)、「TOTP: Time-Based One-Time Password Algorithm」、［online］、［西暦2020年、令和２年１１月１６日検索］、インターネット〈URL：https://tools.ietf.org/html/rfc6238〉

【発明の概要】

【発明が解決しようとする課題】

【００１０】

解決しようとする問題点は、既知のハードウェア型ＴＯＴＰトークンが電池交換が必要でトークンのキー情報Kをサービス提供者またはトークンの管理者が更新できないという点である。また暗号化された書籍などのコンテンツをＯＴＰをもちいて閲覧できる方法が少ないということが問題であった。さらにそれら問題を解決したＯＴＰトークンを例えばウェブサイトのログイン用チケットや改札、映画館などの入場口への入場チケットや、設備及び建物の施錠および解錠システムに提供されていないという点も課題であった。

【課題を解決するための手段】

【００１１】

本発明は、ＴＯＴＰの生成においてＴの値に主に分散型台帳システムにおいてブロックチェーンのブロック番号Ｂｎを用いること、またはブロックチェーン等分散型台帳システムにおいてＫやＴをスマートコントラクトの管理者が変更することで動的なパスワードを生成可能にすることを大きな特徴とする。

Ｔの値はある時刻に変化する値ＴｍまたはＴＢであって、Ｔｍが分散型台帳システムの時刻変化（時間変化）により自動的に変わるブロック番号Ｂｎを用いるか、スマートコントラクト（コントラクト）の管理者が手動にてＴｍやＫを変えるためのデータ値変更のトランザクションを分散型台帳システムに送信することで変更し更新するかの違いがある。コントラクト管理者が手動にてトランザクションを分散型台帳システムに送信することでＫを変更し更新することはＴＯＴＰトークンのＫを更新することにつながるため本発明では必要な要素である。

（本発明ではコントラクト管理者が手動にてトランザクションを分散型
台帳システムに送信することで変更し更新する事を前提とするが、そのほかにＯＴＰトークンの持ち主のユーザーが設定した送信したトランザクションやＯＴＰトークンの持ち主でもないユーザーの送信したトランザクションによるデータ値を用いてもＴＯＴＰのＫ値を変えることができる場合もある。）

【００１２】

本発明を説明する。本発明ではブロックチェーンのブロックナンバーに着目した。説明

のためブロックナンバーを本発明ではブロック番号Ｂｎと言い換える。ブロック番号ＢｎをＴＯＴＰで用いる時間による数値Ｔに用いることを本発明では考案した。本発明ではその方式を及びワンタイムパスワードをＢｎＴＯＴＰと呼称する。（本発明の実施例ではブロックチェーン型のデータ構造を用いる分散型台帳システムの一つであるイーサリアムを用いておりイーサリアムではブロック番号Ｂｎはブロックナンバーと呼称される。）
この名称はブロックチェーンが最初のブロックデータ（ブロック番号が0番目の場合）から数えてＢｎ番目にある時の番号Ｂｎを時刻や時間の変化を表す変数Ｂｎとして用いＴＯＴＰを動作させているためＢｎＴＯＴＰと呼称する。なおＢｎはＢｎＴＯＴＰの計算の基になる数字でありそれを加工した値（Ｂｎを基にあるハッシュ関数によりハッシュ値を求めＢｎに応じて変わる変数）を利用してＢｎＴＯＴＰを生成してもよい。

またＴＯＴＰのような時間に基づいて動的なワンタイムパスワード（ＯＴＰ）トークンを生成することに加え、任意の時間にブロックチェーンにアクセスしブロックチェーンにデプロイされたＯＴＰを計算するコントラクトの変数のうちキー情報Ｋを変更することで時間Ｔによる情報を用いなくてもＯＴＰトークンのシード値を更新することで動的なパスワードＯＷＰ（ＯｗｎｅｒＰａｓｓｗｏｒｄ）が利用できることに着目し、ＴＯＴＰ（ＢｎＴＯＴＰ）とＯＷＰの双方を用いる認証システムを考案し実施する。

本発明ではＯＷＰはブロック番号等のブロックチェーンの最新の時刻に関する情報を用いないが、その認証システムのブロックチェーン上のコントラクトを管理するコントラクト管理者がコントラクトの内部変数の状態を任意時刻に書き換えることでコントラクトに帰属するすべてのＯＷＰ方式のＯＴＰトークンのパスワード生成値が更新される動的パスワードの方式をＯＷＰと呼称する。
ＴＯＴＰ（ＢｎＴＯＴＰ）とＯＷＰの双方においてコントラクトの内部変数は一つのコントラクトに限らず異なるコントラクトから呼び出されたものでもよい。

ＢｎＴＯＴＰはブロック番号Ｂｎがブロックチェーン上で時計の自動的に変化することを計算に利用し、ＯＷＰはブロックチェーン上の変数がある任意の時刻に管理者や一般のユーザーがアクセスし書き換えることで変化させられることを利用する。

ＯＷＰにおいて管理者のユーザーがユーザー端末において定期的にブロックチェーンに署名済みトランザクションを送付することでシード値を更新できるとき、ＯＷＰはＢｎＴＯＴＰやＴＯＴＰと同じように運用できる。ただしＢｎＴＯＴＰではシード値変更のトランザクションは不要であるのに対しＯＷＰではトランザクションが必要である。ＯＷＰとＢｎＴＯＴＰを例えば６０秒ごとに更新されるパスワード生成器として用いる場合はＯＷＰの場合は６０秒ごとに手動又は自動化してトランザクションデータを送信する必要がありブロックチェーン上に蓄積するデータ量はＢｎＴＯＴＰよりも増大しブロックチェーンのノードとなる端末の記憶装置の記憶域を占有する。そのため本発明では用途に応じてＢｎＴＯＴＰとＯＷＰを使い分ける。

ＢｎＴＯＴＰはネットワークを介して数十秒ごとにＢｎＴＯＴＰ値を更新することを望むネットワークに接続されるウェブサービス等に用い、ＯＷＰはネットワークから切断されている場合や長期間（数カ月から数年）にわたり同一のＯＷＰ値となってもよいウェブサービスや紙やＮＦＣタグなどを用いた有価紙葉や施錠を解錠する鍵用途に用いる。

【００１３】

なお本発明ではブロックチェーン基盤の一つであるイーサリアム（Ｅｔｈｅｒｅｕｍ、非特許文献１）を用いてブロックチェーンとスマートコントラクトを用いＢｎＴＯＴＰやＯＷＰを生成し認証させるＯＴＰトークンとそのコントラクトを用いた認証システムを考案し実施した。本発明はイーサリアムを基盤として開発を行っておりブロックチェーンを構成するノードとなる端末の説明やユーザー端末の説明の一部は非特許文献１ の解説のとおりであり、本特許願には詳細を記述していない。
そして本特許願に記述された説明や図表はイーサリアムを用いることの出来る基盤での説明であってイーサリアムに実行に必要な説明のすべては記載されておらず、イーサリアムの分散型台帳システムとしての動作に関しては既知の非特許文献１を主として説明される。図９Ａはイーサリアムのブロックチェーン上での本発明のコントラクトの動作を説明す

る。図９Ｂは有向非巡回グラフ型の分散型台帳システムにおける本発明の動作の説明図である。

図９Ａと図９ＢではＯＷＰ型パスワードの動作がスマートコントラクトから可能となる。図９Ａのブロックチェーンにある最新のデータブロックのブロック番号やブロックデータに由来する情報があるのでＴＯＴＰの算出に用いることができるが、図９Ｂにおいても有向非巡回グラフ型の分散型台帳システムが各データのブロック（チャンク）においてハッシュ値やタイムスタンプなどを記入しており最新のデータチャンクから時刻情報が取得できるもしくは分散型台帳のシステムに時刻情報を持たせられる場合にはＢｎＴＯＴＰ型もしくはＴＯＴＰ型のパスワードが生成可能である。

本発明ではＯＷＰ型パスワードを利用する事を主要な特徴とする。ブロックチェーン上においてＯＴＰトークンのコントラクト内部のＫを変更することでそのＯＴＰトークンのコントラクトで発行されたトークンの表示するパスワードをすべて変えることができる。ＯＷＰ型パスワードをある時刻づつ変更する事を行えば疑似的なＴＯＴＰが実現可能となる。

一方でＯＷＰ型パスワードではトランザクションを分散型台帳システムに送信しなければならない。分散型台帳上でＴＯＴＰを実現するためにコントラクトの管理者などがトランザクションを分散型台帳システムに送信するとネットワークのトラフィックが増大しかねない。またトランザクションデータが増え、ノード端末の記憶装置の容量が増大しかねない。

そこで必要な場合もしくは必要な時（数週間や数カ月や数年に１度の頻度で）にＯＷＰを更新したいときににコントラクト管理者がＫ値を変更できるＯＷＰ型のパスワードと、６０秒間隔など頻繁にパスワードを更新したいＴＯＴＰの用途では主にブロック番号を用いＢｎＴＯＴＰ型のパスワードと、ＢｎＴＯＴＰ型のパスワードにＫ値を変更できるＯＷＰ型パスワードを組み合わせたＢｎＴＯＴＰ型パスワードを用い、動的なパスワードを生成認証させることでネットワークのトラフィック軽減や記憶装置のブロックチェーン部の使用容量の低減に役立つ。したがって本発明はＢｎＴＯＴＰ型とＯＷＰ型の両方の形式をどちらかまたは両方用いることを特徴とする。

【００１４】

本発明は、電池交換が不要でトークンのキー情報をサービス提供者が更新できるように、ハードウェア型ＴＯＴＰトークンではなくブロックチェーンとそのネットワークに基づいたソフトウェアＴＯＴＰトークンとして、ある時刻におけるブロックチェーン上のブロックデータにおいて変更される変数を時間に基づいた変数ＴｍをＲＦＣ６２３８規格における時間によって変化する変数Tとした認証システムであることを最も主要な特徴とする。

さらにブロックチェーン上の最新のブロックデータについてそのブロック番号の変数ＢｎをＴＯＴＰトークンのＲＦＣ６２３８規格における時間によって変動する変数Tに用いた認証システムであることを主要な特徴とする。

【００１５】

本発明は、ＲＦＣ６２３８規格のキー情報Ｋについてその一部またはすべてをトークンの管理者のみが任意の時間にアクセスし変更できる変数と、その変数を変更できる関数などの手段を備え、キー情報Ｋを管理者が更新できることを主要な特徴とする。

ここでキー情報Kが管理者によって変更できる場合において、ＲＦＣ６２３８規格の変数Ｔが設定されていないもしくは時刻により変化しない定数であっても、管理者が任意の時刻に指示し変更する値Ｋを変数Ｔとしてもよい。（本発明においてキー情報Ｋを更新できるものは管理者が好ましいが、管理者ではないユーザーがブロックチェーン上のコントラクトのKを変えても構わない。トークンにかかわるユーザー全員が任意の時間に各々の指示する値をブロックチェーンに入力し、投票するような形となっても本発明の認証システムはユーザーの投票した値に応じて動的なパスワード生成トークンとして動作しうる。）

【００１６】

ブロックチェーンといった分散型台帳システムを用いたソフトウェア型パスワード生成器のトークン（ＯＴＰトークン）と認証システムを用い、ユーザーにブロックチェーン式のトークン（ＯＴＰトークン）を発行し、そのＯＴＰトークンを例えば暗号化されたデータの復号の鍵となるトークンとして用いたり、ウェブサイトのログイン用途や、改札及び映画館などの入場チケット、入退場口の通行用許可証や有価紙葉及びＮＦＣタグに用い、設備及び建物の施錠および解錠を行う認証システムおよびアクセス制御システムであることを主要な特徴とする。

【００１７】

また本発明ではブロックチェーン上にてＯＴＰトークンの所有者を変え、異なるユーザー間でＯＴＰトークンの譲渡を行うことも可能である。ある文章や書籍・音声・動画・ソフトウェアのコンテンツを暗号化したデータを復号できるようにするＯＴＰトークンを異なるユーザー間でＯＴＰトークンの譲渡を行うことも可能である。

ただし本発明においてＯＴＰトークンのコントラクトは譲渡機能を制限する機能を持っていてもよく、コントラクト管理者の望みに応じて任意の時間にＯＴＰトークンの譲渡を可能にしたり不可能にする制御部をもつＯＴＰトークンを用いた認証システムであることを主要な特徴とする。

前記のＯＴＰトークンのコントラクトの備える譲渡機能を制限する機能は暗号化されたデータの復号時に得られるコンテンツの権利者によっては情報の流通を制御したいと考える場合も想定され、他には譲渡制限のあるチケットや銀行のインターネットバンキング用ハードウェア型ワンタイムパスワードカードのように譲渡そのものを禁じる用途も想定されるためである。サービスの利用規約に反しＯＴＰトークンが譲渡されないようＯＴＰトークンのコントラクトのプログラムに譲渡制限機能を組み込むことができる。

本発明では譲渡制限を行う制御部を設定でき、本発明の利用者であるサービスの提供者の望みによっては任意の時間（現在時刻）にＯＴＰトークンの譲渡を制限し譲渡を行えなくすることや譲渡できるようにする機能を備える事を特徴とする。また本発明では譲渡制限を行う制御部を設定でき、本発明の利用者であるサービスの提供者の望みによっては制御部をなくし、常にＯＴＰトークンの譲渡を不可能にすることできる。

【００１８】

本発明では譲渡制限に加え、サービス提供者の規約に違反した利用者のトークンを利用者のブロックチェーン上での識別子との対応関係を強制的に解除し、ユーザーからワンタイムパスワードトークンを除去できる制御部をもつ認証システムに利用できることも特徴とする。ただしこの機能はイーサリアムのＥＲＣ７２１規格において実現しうる機能であり既知の技術である。

またこのＯＴＰトークン除去機能はコントラクトの管理者があるユーザーの秘密鍵から計算されるユーザー識別子の持つあるトークン番号のＯＴＰトークンを強制的に除去できるため、ユーザーとサービス提供者・ＯＴＰトークンのコントラクトの管理者との合意が必要であり通常は使用されないことを想定する。

ユーザー間でＯＴＰトークンの譲渡制限を行い、あるユーザーに対しＯＴＰトークンの発行と除去を行うことでユーザーはＯＴＰトークンによる本発明のＯＴＰの生成とＯＴＰの認証が行える一方でＯＴＰトークンの実質的な所有権の保管や管理や流通はコントラクトの管理者が行うという形になるＯＴＰトークンの保管振替が可能となる。ＯＴＰトークンの保管振替などＯＴＰトークンの保管を行う資格のある第三者によるＯＴＰトークン保管振替を行う用途に利用されることを想定する。

保管振替の概念は証券保管振替機構の証券の集中保管や名義書き換えの概念と似ており既知の概念かもしれないがそれをＥＲＣ７２１規格にてブロックチェーン上で実現する形態の一つが譲渡制限とトークンの発行と除去を組わせたもので実現でいるかもしれないと考え本発明で採用できるものとした。

【発明の効果】

【００１９】

本発明の認証システムは世界中に設置可能なノードとなるサーバ端末（図３Ａの端末３

Ａや図３Ｂの端末３Ｂ）に構築されたブロックチェーン部をネットワーク２０で接続し分散してソフトウェアワンタイムパスワードトークンの情報を保有している。分散型台帳を用いるため、ある地域において災害が生じた場合も世界中の他の地域のサーバ端末からデータの普及が可能になる。また世界中とＯＴＰトークンの認証システムに対応したサービスの流通が可能になりうる。

本発明のワンタイムパスワードのプログラムであるスマートコントラクトはバイトコード等の形でコントラクト管理者の端末からトランザクションとしてブロックチェーン等分散型台帳システムに送信されブロックチェーンのあるブロックデータに格納され過去のブロックデータの連結体であるブロックチェーンと連結されブロックチェーンの特徴から改ざん困難・イミュータブルとなり、攻撃者によるワンタイムパスワードプログラム（コントラクト）の改ざんや、そのコントラクトに帰属したＯＴＰトークンとＯＴＰトークンのトークン番号に対するユーザー識別子との対応関係、ＯＴＰトークンの所有状態について改ざん困難になるという利点がある。

【００２０】

またユーザーとユーザー端末がアクセスに使う秘密鍵とブロックチェーンのノード端末（ノード端末の接続されたネットワーク）さえあればＯＴＰトークンを紛失しづらい。これはハードウェアトークンや既存のコンピュータ又はスマートフォンにインストールして利用するソフトウェアトークンよりも紛失がしづらく、世界中でアクセス可能であるとともにノード端末を分散させて管理できる利点がある。

【００２１】

ハードウェアトークンは時刻・時間を同期するために電池を必要としており、電池残量が減ると時刻がずれユーザーは時刻合わせをする必要があった。これに対し本発明で用いるブロックチェーンは世界中に分散したサーバがノードとなり時刻を同期させながら駆動しており、時刻同期が不要であるという利点がある。

ブロックチェーンにおいて時間が流れることは新たなトランザクションなどを含むブロックが一定の時間ごとにもとのブロックチェーンに連結されていくことに相当し、連結された最新のブロックにおける時刻を反映した情報ＴｍをＴＦＣ６２３８規格のＴＯＴＰを算出するシード変数Ｔに用いることで、時刻同期が不要である。

【００２２】

またハードウェアトークンではシード値のうちＫを変えることは困難で装置ごと使い捨てであったが、本発明のブロックチェーンを用いたパスワード生成器ではＫを更新できるようになっている利点がある。Ｋを更新するトランザクションをブロックチェーンに送信すればそのＫに関与する全てのＯＴＰトークンのＫ値を書き換えて更新することができる。

Ｋが更新されることでＯＴＰ計算に用いるシード値が変わり将来のＯＴＰの計算結果の出方が一新される。

【００２３】

本発明ではＯＴＰトークンと対応するサービス提供者が許可する場合にＯＴＰトークンの譲渡が可能である。またコントラクトに含まれるＯＴＰトークンについてユーザー間で譲渡を禁じることも許可することもできる。暗号化したコンテンツとその復号閲覧に利用できるトークンを国内国外に向け送付できる。これは本や音声動画、会員サイトやソフトウェアなどのデータの利用権を譲渡制限しながら海外に販売することが容易になるかもしれない。譲渡制限機能を持ちつつも電子書籍などをデータで所有しつつその権利、もしくは書籍そのものとしてユーザー間で販売されるようになる。

【００２４】

譲渡制限機能に加えトークンの除去機能を実装した場合には不法な転売や、販売を控えるべき国にトークンが渡らないように制御し管理できる。また秘密鍵を紛失、漏洩しトークンを正常に利用できなくなった場合に関してトークンの管理者にユーザーが届け出て新たなユーザーの秘密鍵から計算されるユーザー識別子にトークンを割り当てるトークン振替が行える。

（本発明では国内から国外に容易にコンテンツとトークンを譲渡可能になるので譲渡制限やトークン除去機能について記載している。トークン管理者とトークンのユーザーがトークンの利用規約などに合意できた場合について利用されることが好ましい。）

【図面の簡単な説明】

【００２５】

【図１】図１はブロックチェーンを用いたワンタイムパスワードの生成と認証の実施方法を示した説明図である。

【図１Ａ】図１Ａは本発明のブロックチェーンを用いたワンタイムパスワード（ＯＴＰ）の生成と認証の方法をサーバ端末に利用する際の概念を示した説明図である。

【図１Ｂ】図１Ｂは本発明のブロックチェーンを用いたＯＴＰ認証システムを通じて暗号化されたデータを復号する方法の概念を示した説明図である。

【図２Ａ】図２Ａは本発明の認証システムを用いて認証を行うユーザーＵＡの端末ＤＡの説明図である。

【図２ＡＡ】図２ＡＡは本発明の認証システムを用いて認証を行うユーザーの端末ＤＡの記憶部（記憶装置）や制御部（制御装置）入出力装置などの説明図である

【図２Ｂ】図２Ｂは図２Ａとは異なるユーザーＵＢの端末ＤＢの説明図である。端末ＤＡと端末ＤＢの機能は同等である。秘密鍵情報が異なる。

【図２Ｃ】図２Ｃはブロックチェーン部にコントラクトをデプロイし管理するユーザーＵＣの端末ＤＣの説明図である。端末ＤＡと端末ＤＣの機能は同等である。秘密鍵情報が異なる。

【図３Ａ】図３Ａは分散型台帳システムＤＬＳを構成するブロックチェーン部を持ちネットワーク２０に接続されるブロックチェーンのノードとなるサーバ端末３Ａの説明図である。

【図３ＡＡ】図３ＡＡは図３Ａの端末３Ａの制御部と記憶部および記憶部に記録されたブロックチェーン部のスマートコントラクト（コントラクト）の説明図である。

【図３ＡＢ】図３ＡＢは図３Ａの端末３Ａの記憶部に記録されたブロックチェーン部のコントラクトの説明図の一つである。

【図３ＡＣ】図３ＡＣは図３Ａの端末３Ａの記憶部に記録された譲渡制限機能やＯＴＰの文字数・桁数とＯＴＰの認証待受時間を変更可能なブロックチェーン部のコントラクトの具体例の説明図である。

【図３Ｂ】図３Ｂは図３Ａのサーバ Ｐ（３Ａ）と同じブロックチェーン部を持ちネットワーク２０上で分散型台帳システムＤＬＳを構成するノードとなる端末３Ｂの説明図である。

【図３Ｃ】図３Ｃはウェブサイト（ウェブページ、ウェブアプリ）へのログイン等で本発明の認証を行う場合のサービスを行うサーバ端末３Ｃの説明図である。

【図３Ｄ】図３Ｄは印刷物や表示画面及びＮＦＣタグに記録された本発明の認証情報を記録した有価紙葉や鍵を読み取り認証を行いサービスを行う端末３Ｄの説明図である

【図３ＤＡ】図３ＤＡは図３Ｄに記載のサーバＳＶＬｏｇ（端末３Ｄ）の記憶部（記憶装置、３０Ｄ）と入出力装置（３４Ｄ、３５Ｄ）に関する説明図である。

【図３Ｅ】図３ＥはＯＴＰトークンの購入または紙及びＮＦＣタグに対しＯＴＰ認証情報を出力しチケットや有価紙葉や鍵等を発券するサービスを行うサーバ端末３Ｅの説明図である

【図３Ｆ】図３Ｆはユーザ端末に対しサーバ Ｐ（３Ａ）に記録されたブロックチェーン情報からトランザクション情報やＯＴＰトークン情報を検索・監視・通知を行うサーバ端末３Ｆの説明図である。

【図４Ａ】図４Ａは本発明の認証システムを用いて暗号化データを復号し閲覧視聴または利用する端末（４Ａ）の説明図である。

【図４Ｂ】図４Ｂは本発明の認証システムを用いて暗号化データを復号し閲覧視聴または利用する端末（４Ａ）の記憶装置に関する説明図（実施の例）である。

【図４Ｃ】図４Ｃは図４Ｂにおいて端末４Ａの記憶装置に平文データ４０３５Ａが暗号化

もしくは難読化されてソフトウェア４０３Ａの４０３０Ａに内蔵されるときの説明図である。
【図５Ａ】図５Ａは本発明の認証システムを用いて暗号化データを復号し閲覧視聴または利用する端末（４Ａ）に広告を配信するサーバ端末の説明図である。
【図５Ｂ】図５Ｂは本発明の認証システムを用いて暗号化データを復号し閲覧視聴または利用する端末（４Ａ）に暗号化データをネットワークを通じて配信するサーバ端末５Ｂの説明図である。
【図５Ｃ】図５Ｃは本発明の認証システムを用いて暗号化データを復号し閲覧視聴または利用する端末（４Ａ）に暗号化データを放送によって送付するサーバ端末５Ｃの説明図である。
【図６Ａ】図６Ａは本発明においてＯＴＰトークンの保有者にＯＴＰを生成する関数の処理を示したフローチャート図である。基礎的なＯＴＰ生成関数である。
【図６Ｂ】図６Ｂは本発明においてＯＴＰトークンの保有者にＯＴＰ生成回数記録機能を備えたＯＴＰを生成する関数の処理を示したフローチャート図である。
【図６Ｃ】図６Ｃは本発明においてＯＴＰ認証回数等記録機能を備えた認証するアクセス者をトークン保有者のユーザー識別子に限定する場合のＯＴＰを認証する関数のフローチャート図である。
【図６Ｄ】図６Ｄは本発明においてＯＴＰ認証回数等記録機能を備えた認証するアクセス者を限定しない場合のＯＴＰを認証する関数のフローチャート図である。
【図６Ｅ】図６Ｅは本発明において図６ＣからＯＴＰ認証回数等記録機能を除いた場合のＯＴＰを認証する関数のフローチャート図である。
【図６Ｆ】図６Ｆは本発明において認証するアクセス者を限定しない場合のＯＴＰを認証する関数のフローチャート図である。基礎的なＯＴＰ認証関数である。
【図６Ｇ】図６Ｇは本発明においてＯＴＰ認証回数等記録機能を備えたＯＴＰトークンの保有者のアクセスか判断してＯＴＰを認証する関数の処理を示したフローチャート図である。
【図６Ｈ】図６Ｈは本発明においてＯＴＰトークンの保有者のアクセスか判断してＯＴＰを認証する関数の処理を示したフローチャート図である。
【図６Ｘ】図６Ｘは本発明の認証システムを利用してサービスを行うサーバ端末（３Ｃ，３Ｄ，３Ｅ，３Ｆ，５Ａ，５Ｂ）にユーザ端末（１Ａや４Ａ）がアクセスした際に記録されるデータ構造を示す図表である。
【図７Ａ】図７Ａは本発明の認証システムを説明するシーケンス図の一つである（ＴＢには主にブロック番号Ｂｎを用いる。ＢｎＴＯＴＰ型パスワードの説明図でもある）。
【図７Ｂ】図７Ｂは本発明においてパスワードＯＷＰを算出するシード値となるコントラクトの内部変数ＫＣやＢＣをコントラクトの管理者が関数ｆｓｃｂを用いて変更できる際の認証のシーケンス説明図である。
【図７ＣＡ】図７ＣＡは本発明において暗号化されたデータを復号して復号された平文データを閲覧・視聴・プログラムとして実行する際のシーケンス図である。
【図７ＣＢ】図７ＣＢは本発明において平文データを暗号化し暗号化データを配布・配信する際のシーケンス説明図である。
【図７ＣＣ】図７ＣＣは本発明において閲覧済みの暗号化データをネットワークに接続されていないオフライン状態で復号し平文データとして閲覧する際のシーケンス説明図である。
【図７Ｄ】図７Ｄは本発明においてウェブサイト・ウェブアプリ等ウェブベースのサービスにログインする際の認証システムの動作を説明するシーケンス図である。
【図７Ｅ】図７Ｅは本発明において例として有価紙葉またはＮＦＣタグを用いてパスワードＯＷＰにより認証しサービスの入場・解錠・始動を行うことを説明するシーケンス図である。
【図８Ａ】図８Ａはウェブサイトログイン時の端末の接続を説明する図である。（実施例１、実施形態１）

【図８Ｂ】図８Ｂは印刷物及びＮＦＣタグによる有価紙葉または鍵の利用時の端末の接続を説明する図である。（実施例２、実施形態２）
【図８Ｃ】図８Ｃは通信ネットワークを通じて暗号化データを配信（配布）する場合においてソフトウェアＣＲＨＮ（４０３Ａ）を利用する端末の接続を説明する図である。（実施例３、実施形態３）
【図８Ｄ】図８Ｄはデータ放送により暗号化データを放送する場合においてソフトウェアＣＲＨＮ（４０３Ａ）を利用する端末の接続を説明する図である。（実施形態３の他の実施例）
【図９Ａ】分散型台帳システムＤＬＳ（分散型台帳システムＤＬＳ）にブロックチェーン型のデータ構造を用いたＯＴＰトークンによる認証システムの概要を説明する図である。
【図９Ｂ】分散型台帳システムＤＬＳ（分散型台帳システムＤＬＳ）に有向非巡回グラフ型のデータ構造を用いたＯＴＰトークンによる認証システムの概要を説明する図である。
【発明を実施するための形態】
【００２６】
本発明はいくつかの要素によって成り立つ。代表的な説明図は図１である。図１に用いる端末の接続の説明図は図８Ａ、図８Ｂ、図８Ｃ、図８Ｄに記載する。本発明で用いるサーバ端末やユーザー端末などのコンピューター端末（電子計算機端末）はコンピュータの五大装置として制御演算装置（制御装置、演算装置）と記憶装置と入力装置と出力装置を備える。そして端末内で制御演算装置と記憶装置と入力装置と出力装置はパターニングされた導体による回路や電線といった配線により接続される。また前記制御演算装置（制御装置、演算装置）と記憶装置と入力装置と出力装置の接続は有線（電気的なケーブルもしくは光ファイバ）や無線による接続をされていてもよい。端末は無線もしくは有線による通信制御装置（通信装置を）を備えネットワーク２０や外部端末等と接続される他、外部記憶装置や入出力装置とも接続されうる。端末は電源装置を備え電子計算機端末を駆動する電力を供給する。
電子計算機ではなく何らかの量子を用いた計算機や、電力や電子の移動を用いず機械的なエネルギーを用いる歯車など機械を用いた古典な計算機、すなわち電子計算機の枠組みにとらわれないコンピュータ端末であっても本発明で説明する紙の印刷情報や半導体メモリ磁気ディスク光ディスクといった記憶装置とハッシュ関数と分散型台帳を用いるものであれば本発明の説明の範囲内であるかもしれない。
１．ユーザーＵＡの端末ＤＡ（端末１Ａ）
本発明のＯＴＰトークンを用い、ＯＴＰを表示または認証を行うコンピュータ端末ＤＡまたは端末１Ａ（図１および図２Ａ、図２ＡＡの端末１Ａ）を備えたユーザーＵＡとその端末１Ａ。
端末１Ａは記憶装置にブロックチェーンのサーバ３Ａ等にアクセスするプログラム、アクセス先となるサーバＰ（図３Ａのサーバ３Ａ）などを示すＵＲＩ、ブロックチェーンへのアクセス時に利用する秘密鍵ＰＲＶＡ（図２ＡＡの秘密鍵情報１０１Ａ）を備える。端末１Ａは通信装置１２Ａを持ちネットワーク２０を介してサーバ３Ａにアクセスする。
サーバ３ＡにＯＴＰの生成を求めてアクセスする際には図６Ａや図６ＢのＯＴＰ生成関数のフローチャートに記載するように秘密鍵ＰＲＶＡ１０１Ａと１０１Ａから計算されるユーザー識別子Ａに対して割り当てられた本発明のトークン番号ＴＩＤＡをもつＯＴＰトークンが必要である。ＯＴＰの認証を求めるときも秘密鍵ＰＲＶＡ１０１Ａと１０１Ａから計算されるユーザー識別子Ａに対して割り当てられた本発明のトークン番号ＴＩＤＡをもつＯＴＰトークンが必要とすることもでき（図６Ｃ、図６Ｅ、図６Ｇ、図６Ｈ）、また図６Ｆや図６ＤのＯＴＰ認証関数のフローチャートの様にユーザー識別子Ａやユーザー識別子ＡにＯＴＰトークンが割り当てられており所有しているかどうか判定するプロセスを必要としないこともできる。
端末１ＡのユーザーＵＡに加え端末１ＢのユーザーＵＢ、端末１ＣのユーザーＵＣ、端末４ＡのユーザーＵＰも存在する。端末４Ａは端末１Ａと同じく本認証システムを行うユーザー端末の1つの形態である。本発明ではユーザーＵＰとユーザーＵＡは同じ人物であり

秘密鍵１０１Ａと秘密鍵４０１Ａは同じものであるが説明のため記号を変えているときがある。

【００２７】

２．サーバＰ（サーバ３Ａ）

＜実施例等における具体的な前提＞

本発明において図１に示すようにブロックチェーン等分散型台帳システムＤＬＳを構成するブロックチェーン部を備えたノードとなるサーバＰ（３Ａ）やサーバＢ（３Ｂ）等が暗号化も可能なネットワーク２０を通じて相互に接続されている。ブロックチェーン等分散型台帳システムＤＬＳにはイーサリアムを用いた。既知のイーサリアムはおおよそ１５秒ごと（１５秒という値はイーサリアムなどのブロックチェーンの作成時に設定される値であって、ブロックチェーンの作成者が１５秒や４秒などの任意の秒数で作成できる）に新しいブロックがブロックチェーンに連結され、ブロック番号がゼロの時刻よりおおむねブロック番号Ｂｎ×１５秒だけ経過している。

イーサリアムのメインネット及びテストネットにおいてブロックチェーンに新たなデータブロックを連結を行うための端末３Ａや３Ｂなどのブロックチェーンを構成するノード間の合意形成・コンセンサスアルゴリズムにプルーフ・オブ・ワーク型（ＰｏＷ型、Proof of Work、作業による証明）もしくはプルーフ・オブ・オーソリティ型（ＰｏＡ型、Proof of Authority、権威による証明）もしくはプルーフ・オブ・ステーク型（ＰｏＳ型、Proof of Stake）が存在し、他のブロックチェーン型分散型台帳システムではプラクティカル・ビザンティン・フォルト・トレランス型（ＰＢＦＴ型、Practical Byzantine Fault Tolerance）等も存在する。本発明を実施する為には電力消費の少なく、処理できるトランザクションの多いことが期待できるプルーフ・オブ・オーソリティ型、プラクティカル・ビザンティン・フォルト・トレランス型、 プルーフ・オブ・ステーク型を用いてよい。

本発明は低消費電力かつトランザクションの処理速度が速い合意形成方法を用いることが好ましく、そのためには中央集権的な分散型台帳の管理方法に近い合意形成アルゴリズムを用いてもよい。本発明は分散型台帳システムの合意形成アルゴリズムに関する発明ではないので合意形成に関しては深く触れないが、本発明の実施例ではプルーフ・オブ・ワーク型もしくはプルーフ・オブ・オーソリティ型を利用するイーサリアムのテストネットを用いて本発明の開発と実施を行った。

ここで本発明ではサーバＰ（３Ａ）の制御部（３１Ａ）および記憶部（３０Ａ）にブロックチェーン部にブロックチェーン基盤の一つであるイーサリアムを形成し処理できる設備を備えていることを前提とする。本発明願においてイーサリアムを用いたブロックチェーンシステムを実行するすべての要素については記述しないが、本発明においてユーザー端末（図１Ａ及び図１Ｂの１Ａや４Ａ）およびサーバ端末３Ａや３Ｂ、３Ｃ、３Ｄ、３Ｅ、３Ｆ、５Ａ、５Ｂ、５Ｃなどはイーサリアムのノードとなることの出来るブロックチェーン制御部とブロックチェーンデータの記録部を持っていてもよい。サーバＰ（３Ａ）は通信装置３２Ａを通じてネットワーク２０に接続されネットワーク２０を介して別のブロックチェーンのノード端末３Ｂおよび複数の３Ｂに相当する端末群と接続され分散型台帳型システムを構成する。

【００２８】

ユーザーのコンピュータ端末ＤＡ（端末１Ａ）や端末ＤＣ（端末１Ｃ）はネットワークＮＴ（ネットワーク２０）を通じてブロックチェーン部を持つサーバ３Ａにアクセスする（図１Ａ）。

サーバ３Ａはオペレーティングシステムやウェブブラウザソフトがインストールされ、ＥＣＭＡＳｃｒｉｐｔ（ISO/IEC 16262）等が実行できることを前提とする。そしてイーサリアムのノードとなるイーサリアムクライアントソフトウェアのｇｅｔｈ（Go Ethereum、https://github.com/ethereum/go-ethereum、２０２１年１月３日閲覧。）等のクライアントソフトウェアをインストールしクライアントソフトウェアを実行して動作している。そして例としてイーサリアムのブロックチェーンを記録部に記録している。

イーサリアムではユーザーアカウント（ＥＯＡ：Externally Owned Account ）とコントラクトアカウント(Contract account)の２種類のアカウントがある。本発明ではユーザーアカウントＥＯＡをユーザ識別子と呼称し、コントラクトアカウントをスマートコントラクトのアドレスとしてコントラクト識別子と呼称する。

本発明ではブロックチェーンの基盤にイーサリアムを用い、コントラクトはＥＲＣ７２１規格のノンファンジブルトークンに関するスマートコントラクトの規格を基にした。ＥＲＣ７２１規格の参考文献として次の３つが挙げられる。１．イーサリアム財団、https://eips.ethereum.org/EIPS/eip-721、2020年12月11日閲覧、２．0penZeppelin、https://docs.openzeppelin.com/contracts/3.x/erc721、2020年12月11日閲覧、３．0xcert.org、https://github.com/0xcert/ethereum-erc721、2020年12月11日閲覧。

イーサリアムではＥＲＣ７２１規格のスマートコントラクトにおいて、そのコントラクトの管理者（秘密鍵１０１Ｃから計算されるユーザー識別子Ｃをもつ）が1つの単位でトークンを発行しユーザーとなるユーザー識別子ＡやＢに送信する。ＥＲＣ７２１規格のトークンは符号なし整数型変数にて表現されるトークンＩＤとその保持者にするユーザ識別子Ａを対応付けて、ユーザー識別子Ａにトークンを発行される。

ここで本発明ではＥＲＣ７２１規格におけるトークンＩＤをトークン番号と呼称する。ユーザー識別子Ａがトークン番号ＴＩＤＡを所有していることの情報はコントラクトに記録される。

例えば図３ＡＣの３０１４Ａのようにユーザー識別子ＡにはＴＩＤＡの番号を持つトークンの所有情報（３０１５Ａ）、ユーザー識別子ＢにはＴＩＤＢの番号を持つトークンの所有情報（３０１６Ａ）が記録されている。ある識別子に対しコントラクトからトークンが発行されていたり、異なるユーザー識別子間で譲渡されるなどした最終的な所有情報が記録されている。

ブロックチェーン上ではコントラクト作成や譲渡記録やコントラクトの内部変数の変更に関するトランザクションは改ざん困難な状態で記録されており過去のトークンの保有履歴情報は消去できない。一度ブロックチェーンに記録されデプロイされたコントラクトのプログラムも改ざんが行われない。

【００２９】

＜本発明に用いた分散型台帳上でのトークン＞

本発明では実施する際にイーサリアムをブロックチェーンの基盤として用いた。またイーサリアムで用いられるＥＲＣ７２１規格のトークンはイーサリアム上でのＯＴＰを備えたノンファンジブルトークンの発行に利用できると考えて本発明を実施する際に採用した。

そしてＥＲＣ７２１規格のトークンにワンタイムパスワード（ＯＴＰ）に関するプログラムを備えさせたスマートコントラクト（コントラクト）を本発明の認証システムのＯＴＰトークンのコントラクトに利用した。ここで実施する際にＥＲＣ７２１規格を用いたが、これは本発明の実施例の一つであり分散型台帳上にて本発明のＯＴＰトークンの機能を提供できるスマートコントラクトならば本発明は実施できる。本発明のＯＴＰトークンはＥＲＣ７２１規格やそれに類似したトークンおよびトークンのスマートコントラクトに限定されない。

本発明ではＯＴＰトークンもしくはＯＴＰ生成トークン・ＯＴＰ生成コントラクトは、ＯＴＰを生成するトークンの所有権やそのトークン発行処理、トークン送信処理、トークンの名称等情報の表示といった処理を行うコントラクトを示す。ＯＴＰ認証コントラクトまたはＯＴＰ認証コントラクト内部のＯＴＰ認証関数は、ＯＴＰ生成コントラクトのＯＴＰ生成関数と一致したＯＴＰを計算するための変数と処理部を持ち、ＯＴＰの生成と認証の処理を行うことができる。図３ＡＡや図３ＡＢや図３ＡＣがそのコントラクト説明図であり、認証関数を端末３Ａでなく端末３Ｄに持つときの例は図３ＤＡである。

ブロックチェーン部を持つサーバ群（３Ａ、３Ｂ等）とブロックチェーン部に接続する端末（１Ａ、１Ｃなど）を説明する図表では、実施例で用いたイーサリアムのブロックチェーンとコントラクトを実行できる制御部（処理部）と記憶部（記録部）を備えている事

を前提としている。
制御部や記憶部の詳細はイーサリアムの仕様に準拠し、その類似のブロックチェーン基盤を持つシステムにも適用される。本発明ではＥＲＣ７２１規格のトークンにＯＴＰ生成関数を備えさせ、ＥＲＣ７２１型のＯＴＰ生成トークンを発行できるコントラクト（ＯＴＰ生成コントラクト）とした。そしてＯＴＰ生成コントラクトのＯＴＰ生成に用いるシード値と同じ値にさせることのできるＯＴＰ認証関数を ＯＴＰ生成コントラクトに備えさせるか、または別途ＯＴＰ認証コントラクトを作成し、ＯＴＰ認証コントラクトに ＯＴＰ認証関数を備えさせ、
ＯＴＰ生成関数で生成されたＯＴＰをユーザ端末１Ａや４Ａなどに出力させ、出力されたＯＴＰとＯＴＰ認証に必要な情報をユーザー端末１Ａや４ＡからＯＴＰ認証にかかわるコントラクトのＯＴＰ認証関数もしくは端末３Ｄに搭載されたＯＴＰ認証関数に入力して正しいＯＴＰか検証し認証させ、正しいＯＴＰの場合には認証できた場合の戻り値データをユーザー端末の処理部に送信する。
このようにＥＲＣ７２１規格にＯＴＰ生成機能を備えさせたものが本発明のＯＴＰ生成トークンであり、インターネットバンキング（ネットバンキング）のサービスへログイン等に用いるヒトの手で所有できるハードウェアＴＯＴＰトークンをブロックチェーンなどの分散型台帳にて所有し利用できるようにしたものである。
【００３０】
＜ＥＲＣ７２１規格のノンファンジブルトークンのトークン番号とトークン発行＞
本発明のワンタイムパスワード生成関数及びそれを含むコントラクトではＥＲＣ７２１規格のトークンについて、あるユーザー識別子Ａのユーザーにトークン番号ＴＩＤＡが一つ発行（ｍｉｎｔ）される。トークン発行にはコントラクト内部の発行関数（図３ＡＣの３０４２Ａ）が利用される。３０４２Ａは原則としてコントラクトの管理者の秘密鍵ＰＲＶＣ（図１Ｃの１０１Ｃ）でないとトークン発行の操作できない。
【００３１】
＜トークンの譲渡と譲渡制限＞
ＥＲＣ７２１規格では異なるユーザ識別子間にてトークンの送信・譲渡は自由に行える。本発明のＯＴＰを生成するトークン（ＯＴＰトークン）はＥＲＣ７２１規格に準拠しているのでトークン番号ＴＩＤＡはユーザー識別子Ａのユーザーが望む場合にユーザー識別子Ｂなどのユーザーに送付することが可能である。トークンの送信は図３ＡＣのトークン送信関数（図３ＡＣの３０４０Ａ）を用いて行う。なおＥＲＣ７２１規格ではトークンの送信をコントラクト管理者が禁止する機能は存在しないが、本発明では譲渡制限用変数及び関数（３０４１Ａ）を用いて３０４０Ａの実行を停止させることも許可することもできる。
本発明では銀行のワンタイムパスワードトークンや譲渡禁止されたチケットや会員権など、譲渡を制限または譲渡を行わせないトークンとすることも必要であったので、ＥＲＣ７２１規格においてトークンの送信関数群（ｔｒａｎｓｆｅｒ関数）、送信の許可にかかわる関数群（ａｐｐｒｏｖｅ関数）の実行を制御する譲渡制限処理部３０４１Ａを設け、譲渡制限処理部はコントラクトの管理者（Ｏｗｎｅｒ）の端末１Ｃのみが変更できる変数によって処理を変更できるようにして譲渡制限できるようにした。
具体的には ｔｒａｎｓｆｅｒ関数の実行を制御する真偽値の変数と、ａｐｐｒｏｖｅ関数の実行を制御する真偽値の変数をコントラクトに設定し（コントラクト内部のすべての関数からアクセスできるグローバル関数として真偽値の変数を設定して）、コントラクトの管理者の識別子Ｃ（Ｃは端末１Ｃの１０１Ｃから計算される）のみがアクセスできるセッターとなる関数ｔａｆを備え、ｔａｆによりｔｒａｎｓｆｅｒ関数の実行を制御する真偽値の変数と、ａｐｐｒｏｖｅ関数の実行を制御する真偽値の変数を書き換えることで譲渡できる状態と譲渡できない状態の切り替えを可能にした。
（トークンの譲渡制限は異なるユーザ識別子間でのトークンの所有情報の書き換えを制限する。ユーザ識別子はユーザの秘密鍵に対応しておりトークンの譲渡制限は実態としては異なる秘密鍵間でのトークンのやり取りを制限する。）

【００３２】
＜ワンタイムパスワードにかかわるコントラクト（スマートコントラクト）＞
本発明においてブロックチェーン上にワンタイムパスワードトークン（ＯＴＰトークン）のユーザーへの発行（トークンの割り当て、対応付け）やトークンの送信（トークンのユーザー間での譲渡）、レーティング情報の取得、トークンの名前情報の取得、トークンのＵＲＩ情報の取得等が行える。そしてシークレット値ＫＣや時刻により変わる変数ＴＢ（本発明ではブロック番号ＢｎをＴＢとして用いる）、トークン番号ＴＩＤＡ、ユーザー識別子Ａを基にして生成されたシード値Ｓをハッシュ関数ｆｈの引数に用いてハッシュ値を得てそれをワンタイムパスワードとして戻り値にするワンタイムパスワード生成関数を備えたワンタイムパスワード生成コントラクト（図３ＡＡ、図３ＡＢ、図３ＡＣに記載の３００８Ａまたは３００８ＡＧ）がある。
また本発明のワンタイムパスワードを認証する関数もしくは認証するコントラクトでは、ワンタイムパスワードを生成する関数で用いるシード値Ｓとハッシュ関数ｆｈがワンタイムパスワードを認証する関数において引数に入力された関数の検証に用いるシード値とハッシュ関数と同期できていれば、正しいパスワードであるとき一致していることを確認できる。（ワンタイムパスワードＯＴＰ生成関数３００９Ａの処理を説明するフローチャートを図６Ａおよび図６Ｂに示す。ワンタイムパスワードＯＴＰ認証関数３０１８Ａの処理を説明するフローチャートを図６Ｃと図６Ｄと図６Ｅと図６Ｆと図６Ｇと図6Hに示す。）
ＯＴＰ認証関数はＯＴＰ生成関数を含むＯＴＰ生成コントラクトに内蔵されていてもよいし、ＯＴＰ生成コントラクトとＯＴＰ認証関数を分けて保存するためにＯＴＰ認証関数をＯＴＰ認証コントラクトに内蔵してＯＴＰ生成コントラクトとＯＴＰ認証コントラクトを分離してブロックチェーン上の同一のブロック番号もしくは異なるブロック番号のブロックデータに記録されていてもよい。
またＯＴＰ認証関数がネットワークとは接続されていない端末３ＤにありＯＴＰ生成関数がネットワーク上の端末３Ａにあって端末１Ａが端末３Ａで取得したＯＴＰを端末３Ｄで認証に用いてもよい。
認証関数と生成関数がそれぞれ異なる他のブロックチェーンにコントラクトが記録されており二つのブロックチェーン間でＯＴＰの生成と認証を分けて分担するシステムでもよいが、その場合は二つのブロックチェーンに分けて記録されたＯＴＰ生成関数とＯＴＰ認証関数のパスワード計算に用いる計算方法やハッシュ関数ｆｈやシード値Ｓが一致しなければいけない。
例として図６ＡのＯＴＰ生成関数と図６ＦのＯＴＰ認証関数のフローチャートで利用する関数の引数のシード値Ａ,ＴＩＤＡ,ＫＣ,Ｂｎとハッシュ関数ｆｈおよびそれらを用いた計算手順が一致し、ＯＴＰ生成関数とＯＴＰ認証関数で同じＯＴＰを計算できることが必要であり、また図６ＡのＦ１０７でシード値とハッシュ関数からハッシュ値を求めた後にハッシュ値をＯＴＰとせずに１０のＮ乗で割った剰余をＮ桁の符号なし整数のＯＴＰとする場合はＯＴＰ認証関数でも同じように剰余を求め、１０のＮ乗で割った剰余をＮ桁の符号なし整数のＯＴＰを計算できるようにＯＴＰ認証関数とＯＴＰ生成関数で計算されたＯＴＰが一致し同期しなければいけない。
シード値の内ＡやＴＩＤＡはＯＴＰトークンの保有者や保有するトークンのシリアル番号に相当するトークン番号であってユーザー由来の変数であるが、ＫＣはコントラクト管理者が更新できる値であるのでＫＣ値をＯＴＰ生成関数とＯＴＰ認証関数で一致できるようにした手段を備えなければいけない。
またシード値ＢｎやＢＣなどのある時刻Ｔにおいてかわる変数Ｔｍも一致していなければならず、ＢＣはコントラクトの管理者が一致させる必要のある変数であるがＴｍやＢｎについてもＯＴＰ認証関数とＯＴＰ生成関数で一致しないような現象が生じる場合には一致させる手段を備える必要がある。
同一のブロックチェーン（同一のブロックチェーン識別子、分散型台帳システム識別子）においてデプロイされたＯＴＰ認証関数とＯＴＰ生成関数をもつコントラクトは同じＢｎ

を用いることができるが、異なるブロックチェーン識別子間でＯＴＰ認証関数とＯＴＰ生成関数をもつコントラクトを分けて運用する際には、ブロックチェーン識別子間で異なるＢｎに補正値を加算減算して運用する場合に、Ｂｎが一致しなくなる場合にはＢｎが一致するようセッター関数など一致できるようにする手段を備える必要がある。

【００３３】

＜ワンタイムパスワードの算出＞

ユーザＵＡの端末ＤＡ（端末１Ａ）のアクセスに応じて端末３Ａは処理を行う。端末１Ａの記憶装置に記録された秘密鍵ＰＲＶＡ（秘密鍵１０１Ａ）からユーザー識別子Ａを算出する。

補足としてイーサリアムでは秘密鍵から公開鍵を算出し、公開鍵のハッシュ値をハッシュ関数を用いて計算し、そのハッシュ値を切り取りユーザー識別子とする。具体的にはイーサリアムではSecp256k1という楕円曲線を基にした方法で３２バイトの秘密鍵から６４バイトの公開鍵を作成する。また署名などに用いる（楕円曲線電子署名、ＥＣＤＳＡ、Elliptic Curve Digital Signature Algorithm）。そして６４バイトの公開鍵に対してKeccak-256というＳＨＡ－３と類似のハッシュ関数を用いて３２バイトのハッシュ値を求めその一部を取り除くことで残る情報をユーザー識別子（匿名化された識別子）とする。

サーバＰ（端末３Ａ）のブロックチェーン部、ブロックチェーン記録部のデータに従い、ブロックチェ―ン内部にプログラムされた本発明のコントラクトにおいて、ＯＴＰ生成関数は関数の実行者であるユーザー識別子Ａがコントラクトで発行されたワンタイムパスワードトークン（ＯＴＰトークン）を保有しているか確認し、トークン保有者にはトークンの番号ＴＩＤＡとコントラクトのシークレット変数のＫＣ値３０１１Ａ（図３ＡＡや図３ＡＢや図３ＡＣに記載の内部変数ＫＣ　３０１１Ａ）と、ある時刻Ｔにおいてブロックチェーン上で変動する変数ＴＢをパスワード生成のキー値（キー値、シード値）としてハッシュ関数ｆｈ（図３ＡＡや図３ＡＢや図３ＡＣに記載のハッシュ関数ｆｈ　３０１０Ａ）の引数として利用する。計算例はＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＴＢ）である。ＯＴＰ認証関数の実行時にユーザー識別子ＡやＯＴＰトークンの保有を確認する場合も同様である。

ここで実施例ではキー値にユーザー識別子Ａを追加し、本発明においてＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＴＢ）として計算される。

そして前記ＴＢに最新のブロック番号Ｂｎ（図３ＡＡに記載の３００１Ａがブロック番号Ｂｎ）を用いるブロック番号に基づいたワンタイムパスワードＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）を利用する事を特徴とするＯＴＰの計算方法を用いたＯＴＰトークンを本発明では用いる。

Ｔｍ（またはＴＢ）にＢｎを用いるときはＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＴＢ）でもＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＴＢ）でもよい。具体的にはＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）でもＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎ）でもよい。

ここでＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＴＢ）でもよい理由としては、例として短時間の６０秒ごとに更新されるＯＴＰの場合は保有するユーザーが変更されてもＢｎが６０秒ごとに変わるので６０秒前の過去に計算されたＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎ）は無効とできるためである。本発明の実施例ではユーザー識別子Ａ（およびユーザー識別子Ａを計算する秘密鍵１０１Ａ）をウェブサービスへのログイン等で秘密鍵の不正利用時の監視に用いる狙いもありＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＴＢ）を好ましくは用いた。

また前記ＴＢにＯＴＰ生成トークンのコントラクトの内部変数ＢＣ値３０１３Ａ（図３ＡＡや図３ＡＢや図３ＡＣに記載の内部変数ＢＣ３０１３Ａ）を用い、前記３０１３Ａはコントラクトの管理者端末１Ｃの秘密鍵１０１Ｃを用いてブロックチェーンへアクセスし３０１３Ａを書き換えることの出来るセッター関数３０１２Ａを用いて任意時間に任意の値に変更することで、ワンタイムパスワードＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）として管理者の設定するＢＣ値に応じてパスワードを変えられることを特徴とするＯＴＰの計算方法を用いたＯＴＰトークンを本発明で用いる。

Ｔｍ（またはＴＢ）にＢＣを用いるときはＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＴＢ）よりもＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＴＢ）が好ましいかもしれない。具体的にはＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＢＣ）よりもＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）が好ましいかもしれない。

ここでＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＴＢ）よりもＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＴＢ）が好ましい理由としては、例としてＫＣやＢＣはコントラクト管理者が任意の時間に変更できコントラクト管理者の判断によっては数年を超え長期間もしくは一度も変更されない恐れがあり、前記ＫＣやＢＣが長期間もしくは一度も更新されないときＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＢＣ）の場合はトークン譲渡により保有するユーザー識別子が変更されたときにトークン番号に固有だがユーザー識別子に固有ではないＯＴＰを生成・認証するので、ＯＴＰを取得してきたユーザーたちが次々とＯＴＰトークンを譲渡してＯＴＰを取得してＯＴＰの値ＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＢＣ）を共有し複製し記録できる問題（金属製の鍵における合鍵の複製に似た問題）があり、それに対しＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）というＯＴＰを計算することでユーザー識別子及びトークン番号に固有のＯＴＰを生成・認証できるので適しており本発明の実施例では好ましくは用いた。

そしてＢＣ値３０１３Ａと同じくＫＣ値３０１１Ａもコントラクトの管理者端末１Ｃの秘密鍵１０１Ｃを用いてブロックチェーンへアクセスし３０１１Ａを書き換えることの出来るセッター関数３０１２Ａを用いて任意時間に任意の値に変更することでワンタイムパスワードＢｎＴＯＴＰおよびＯＷＰの双方のシークレット変数ＫＣを変えることでコントラクトに属するＯＴＰトークン全てのキー値ＫＣを任意時間に任意数値で更新できることを特徴とする。変更できるＢＣ値とＫＣ値は同じものとみなすこともでき、ＢＣ値とＫＣ値を同じものとみなし１つの変数としてＯＴＰ計算することもできるほか、ＢＣ値とＫＣ値をそれぞれ複数個用意して利用することやユーザー識別子またはトークン番号に固有のＫＣ値（後述のマッピング変数ＫＣＡ）を設定しそれらＫＣ値にもちいてもよい。

【００３４】

＜ｎ桁の整数からなるワンタイムパスワードの算出＞

インターネットを用いたネットバンキングなどの銀行取引等で利用される7桁から6桁の整数のパスワードとするためにハッシュ関数で算出した情報ＢｎＴＯＴＰを符号なし整数に型変換し、その整数値をｎで割ったときの剰余を求めｎ桁の整数パスワードとすることもできる。

ここでｎは６から７の値をとってもよい。コントラクトにおいて変数ｎがコントラクトの管理者のみによって書き換えできるセッターとなる関数ｆＯＴＰＮが設定されている場合には（変数ｎと関数ｆＯＴＰＮが３０３１Ａに記録されている場合には）、ｎを６として設定してコントラクトをブロックチェーンに記録・展開（デプロイ）したのち、総当たり攻撃に必要な計算力を増加させるために、ｎを６から１２に引き上げ、１２桁のパスワードにすることも可能である。これはハードウェアＴＯＴＰトークンでは実現困難な方法である。セキュリティ上好ましくはないが、桁数が少なくてもよい場合はコントラクトを作成後にｎを６から３に変更し表示するＯＴＰの桁数を３桁にすることもできる。

またコントラクトには複数のＯＴＰ生成関数と認証関数を備えさせ、重要な操作を行う（例として高額な振り込みや決済を銀行で行う）場合のＯＴＰ認証関数及びＯＴＰ生成関数と、重要度は低いものの認証を必要とするＯＴＰ認証関数及びＯＴＰ生成関数をコントラクト内もしくは端末３Ｄに備えることができる。前記において重要な操作を行う場合はｎの値を大きくし、重要度が低い操作を行う場合はｎの値を小さくすることで入力時の桁数を変更させ、ＯＴＰ認証に要する入力文字数の労力を加減させ、ヒトが手などで端末の入力装置から入力しやすくすることもできる。

ＯＴＰ認証関数及びＯＴＰ生成関数でシード値が一致するように生成コントラクトと認証コントラクト（または認証関数）で同一の３０３１Ａを設定し、コントラクトをブロックチェーンにデプロイした後も、３０３０Ａの値を変更するときは生成コントラクトと認証コントラクト側で一致させるようコントラクトの管理者である端末１Ｃが設定変更のト

ランザクションを３Ａに送付し変数などの書換を行う必要がある。
本発明のワンタイムパスワードは符号なし整数で表現することも１６進数で表現することもできる。パスワードには数字、英字、記号などが利用されうる。
【００３５】
＜ブロック番号に関する処理＞
ブロックチェーンは例えば１５秒、１０分等のある時間ごとに新たなブロックが連結されブロック番号Ｂｎが1つずつ増えていく。ユーザーＵＡがサーバＰ（３Ａ）から端末１ＡにＯＴＰを生成して呼び出し表示して認証する時間（ＯＴＰ認証の待受け時間）が短すぎる時、例えばインターネットバンキングサイトなどウェブページに端末ＤＡ（１Ａ）のディスプレイに表示されたＯＴＰを入力したいが、15秒ごとにＯＴＰが更新されることによってヒトの手入力が追い付かずＯＴＰが入力できないことが想定される。実際に本発明の開発時においてはブロック番号が１５秒ごとに代わるイーサリアムのテストネットワークにあるブロックチェーンを用いたが、発明者の手では入力が困難になることが時折確認された。
そこでブロック番号Ｂｎを基に表示する間隔を増やす変数ｎを用い、Ｂｎ　ｍｏｄ　ｎとして、Ｂｎのｎで割った余りｍを求め、ＢｎからｍをＢｎｒとして（Ｂｎ－ｍ＝Ｂｎｒとして）、Ｂｎの代わりにＢｎｒをＯＴＰを算出するハッシュ関数の引数に利用した。たとえばブロック番号が15秒でｎを2にした時、ブロック番号Ｂｎが奇数または偶数のときパスワードが変更されるようになりパスワードの表示時間を15秒から30秒に増やせる。ｎを２から３、４、５、と増やしていけば、表示時間と認証時間を更に増やすことができる。このＯＴＰを生成し認証し表示を行い入力待ちを行える時間を増やす関数や変数は図３ＡＣの３０３０Ａに示す。なおｎは１以上の符号なし整数である。ｎ＝０とすることはできない。
認証関数及び生成関数でシード値が一致するように生成コントラクトと認証コントラクト（または認証関数）で同一の３０３０Ａを設定し、コントラクトをブロックチェーンにデプロイした後も、３０３０Ａの値を変更するときは生成コントラクトと認証コントラクト側で一致させるようコントラクトの管理者である端末１Ｃが設定変更のトランザクションを３Ａに送付し変数などの書換を行う必要がある。
【００３６】
＜ブロックチェーンにて決まる値を用いたＯＴＰ＞
実施例ではイーサリアムのテストネットで実施例となるＥＥＲＣ７２１規格に本発明のＯＴＰ認証用部分を追加したスマートコントラクトの形でワンタイムパスワードＯＴＰトークン発行部、ＯＴＰトークンとユーザーの所有関係記録部、ＯＴＰ生成部と、生成されたパスワードを検証し認証する認証部をブロックチェーンのコントラクトに設けた。ブロックチェーン部ではブロック番号Ｂｎが利用できる。
イーサリアムではブロックチェーンを構成するノード間でＧａｓＬｉｍｉｔ値（ＢｌｏｃｋＧａｓＬｉｍｉｔ値）に関する投票が行われる。そしてイーサリアムにはＧａｓＬｉｍｉｔ値によってブロックサイズが可変になる特徴がある。この投票で決まるＶ値３００４Ａやブロックサイズ ＢＳＺ値３００５Ａに関しても本発明ではブロックチェーンのシード値に用いる。例えばすべてを実施する場合はワンタイムパスワードＢｎＴＯＴＰはＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，Ｖ）、またはＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＳＺ）、またはＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，ＢＳＺ）のようにＯＴＰを生成するシード値となる引数を複数用いてＯＴＰを生成できる。またＯＴＰを擬似乱数とみなして擬似乱数生成器とすることもできる。
単にイーサリアム上でブロック番号Ｂｎを用いたＴＯＴＰベースの擬似乱数生成器用スマートコントラクトに用いるときはＢｎＴＯＴＰ＝ｆｈ（ＫＣ，Ｂｎ）やＢｎＴＯＴＰ＝ｆｈ（Ｂｎ）やＢｎＴＯＴＰ＝ｆｈ（ｆｈ（Ｂｎ））でもよく、本発明ではブロック番号Ｂｎを用いたＴＯＴＰベースの擬似乱数生成器が実施できることを確認した後、その擬似乱数生成器をＯＴＰ認証システムに応用している経緯がある。擬似乱数として用いるときはトークン番号ＴＩＤＡや後述するユーザー側の投票値のマッピング変数ＶＵをシード値

に用いてもよい。

【００３７】

実施例にあるイーサリアムにはｗｅｂ３．ｊｓといったブロックチェーン部とユーザー端末のウェブブラウザを結ぶＥＣＭＡＳｃｒｉｐｔモジュールがある。前記ＥＣＭＡＳｃｒｉｐｔモジュールを用いユーザーの秘密鍵や指定したユーザー識別子、コントラクト識別子、ブロックチェーン識別子、トークンの名前を用い、ウェブブラウザ上でイーサリアムのブロックチェーンにアクセスし本発明のＯＴＰ生成関数やＯＴＰ認証関数を操作し、ＯＴＰ等や認証結果の戻り値ＣＴＡＵを得て、ウェブサイトへのログオン（図８Ａ）、紙のチケット１８Ａまたは近距離無線通信（ＮＦＣ）タグ１９Ａによる入場や、ＮＦＣタグによる施錠の電子的な解錠鍵に用いてもよい（図８Ｂ）。

さらに本発明のＯＴＰ認証システムにおいてソフトウェアＣＲＨＮ（図４Ａの４０３Ａ）を用い、ＯＴＰ認証関数を実行し、認証結果が正しい時に得られた戻り値のデータＣＴＡＵ（ＣＴＡＵは図３ＡＡ等に記載のブロックチェーンのコントラクトに記録された３０２１Ａと、図３ＡＡの３０２１ＡをＯＴＰ認証取得し端末４Ａに記憶させた図４Ｂの４０３１Ａを示す）を用いることを特徴として、ブロックチェーンの外部から得られた鍵データＡＫＴＢ（図４Ｂの４０３２Ａ）や４０３Ａ内部に記録されたソフトウェアの秘密鍵データＣＲＫＹ（図４Ｂの４０３０２Ａ）を用いて４０３Ａのプログラムに従って共通鍵暗号化（対称鍵暗号化）を行う鍵データＴＴＫＹ（図４Ｂの４０３３Ａ）と、その鍵データＴＴＫＹ（図４Ｂの４０３３Ａ）にて暗号化されたデータ４０３５Ａを流通させ、アクセス権をワンタイムパスワード認証機能付きのＥＲＣ７２１型トークンとして与えられているユーザーの手で復号出来る暗号化データの流通と復号を行うシステムに本発明のＯＴＰ認証システムを用いることができる。

ＯＴＰ認証関数３０１８Ａや３０１８Ａや３０１８ＤＡの戻り値ＣＡＴＵ３０２１Ａはコントラクトの管理者が変更する手段を備え変更してもよく、１つ又は複数の戻り値ＣＴＡＵ３０２１Ａを返してもよく、さらにユーザー識別子Ａやトークン番号ＴＩＤＡをキーとするマッピング変数ＣＡＴＵ３０２１Ａ（ＣＴＡＵ［ＴＩＤＡ］やＣＴＡＵ［Ａ］というマッピング変数３０２１Ａ）と前記変数についてトークン番号やユーザー識別子をキーとして変数の値を変更するセッター関数を備えてもよい。

【００３８】

３．ネットワーク

通信経路であるネットワーク２０においてユーザーＵＡのコンピュータＤＡ（端末１Ａ）とサーバーＰ（端末３Ａ）の通信は暗号化されていることが好ましい。本発明ではワンタイムパスワードを端末１Ａとサーバ端末３Ａの間でやり取りするが、その際に端末１Ａと端末３Ａをネットワーク２０結ぶ通信経路が暗号化されていることが好ましい。もし暗号化されてなければネットワーク２０を介したブロックチェーンとのやり取りが読み取られてしまう恐れがある。

またブロックチェーンの基盤にトランザクションやコントラクトの処理内容やコントラクトの変数の情報を秘匿できる方法があることが好ましい。

ネットワークを構成する際は有線及び無線による通信方法を用いてもよい。ワンタイムパスワードの生成と認証を行う際に本発明のトークンを用いる場合は双方向の通信が必要である。しかし利用形態によってはワンタイムパスワードの生成のみを双方向通信で行い、認証は紙のチケットや施錠・解錠用のＮＦＣタグを読み取る端末３Ｄ（３Ｄの利用形態は図８Ｂに記載）にて認証させることができる。

また暗号化データを復号する用途では一対複数の放送で得られた暗号化データを生成されたＯＴＰに従って本発明の認証システムで認証し復号する事が可能である。放送する局が宇宙にある局５Ｃでそれを操作する局５ＣＣはネットワーク２を用いて無線通信を行い通信する。双方向のデータ通信により暗号化データを復号する用途ではネットワーク２０等を用いる。

【００３９】

４．パスワードを使うサービス

４Ａ．ウェブサイトのログイン用途
＜ログイン処理＞
本発明の認証システムでウェブサイトのログインや操作に利用する場合、サーバＳＶＬｏｇｉｎ（図８Ａの端末３Ｃ）を用いてログイン処理を行う。図８Ａに端末の接続図を示す。ネットワーク２０を介して端末１Ａと端末３Ａと端末３Ｃが接続されている。サーバ端末３Ｃは実機のサーバ端末３Ｃでもよいし仮想のサーバ端末３Ｃでもよいし仮想機械である端末３Ｃでもよい。
サーバ端末３Ｃの記憶装置データを端末１Ａに記憶させサーバ端末３Ｃを仮想機械として端末１Ａに構築し、端末１Ａ内部で端末１Ａと端末３Ｃを通信させつつ端末１Ａをネットワーク２０を介して端末３Ａと接続させることで端末１Ａに構築された仮想機械端末３Ｃにログインすることが可能となる。例えば端末３Ｃはサービスが終了したログインが必要な電子書籍サービスやオンラインゲームサーバのサービスであってもよい。
端末３ＣにおいてＥＣＭＡＳｃｒｉｐｔ等でサーバ３Ａのブロックチェーン部とユーザーの端末１Ａが通信してやり取りできるウェブアプリ、ウェブサイトデータをユーザーに送信し表示させ、ユーザーが持つ秘密鍵１０１Ａの情報を持ったウォレットソフトウェアを用い（ウォレットソフトウェアがない場合は秘密鍵情報１０１Ａそのものをウェブサイトに入力、記述、出力させ）ウェブサイトデータにユーザーが所持するサーバ端末３Ｃのログインに利用できるトークン番号を入力し、その情報とウォレットソフトの情報からワンタイムパスワード生成コントラクトのワンタイムパスワード生成関数よりユーザー識別子Ａ、トークン番号ＴＩＤＡを引数としてブロック番号ベースのワンタイムパスワードＢｎＴＯＴＰ生成し、ＢｎＴＯＴＰをウェブサイトに入力した際に、入力値をワンタイムパスワード認証コントラクトのワンタイムパスワード認証関数で認証処理を行う。
ＯＴＰの認証関数及び生成関数で計算されるＢｎＴＯＴＰはハッシュ関数ｆｈとコントラクト内部変数ＫＣと前記のＡ、ＴＩＤＡを用いてＢｎＴＯＴＰ＝ｆｈ（Ａ,ＴＩＤＡ,ＫＣ,Ｂｎ）という引数と関数で表される。
ここでウォレットソフトウェアは秘密鍵情報と秘密鍵から計算されるユーザー識別子情報を計算でき、ある保有秘密鍵とユーザー識別子におけるＥＲＣ７２１トークンの保有数を表示できるものもある。（ウォレットソフトウェアの例としてhttps://metamask.ioのブラウザ拡張ソフトウェア型ウォレットソフトウェアのMetamaskなど。秘密鍵を記録するハードウェアウォレットＤＷＡＬＴ１６０３Ａと通信できるものもある。）
認証結果が正しい時、サーバ３Ａにアクセスしてきたユーザー識別子Ａやトークン番号ＴＩＤＡといったブロックチェーンに関する情報と、端末１ＡのＩＰアドレスまたは位置情報や端末１Ａに固有の装置ＩＤ（デバイスＩＤ）または端末１Ａの入力装置１４Ａのセンサ１４４Ａのセンサ値を端末の環境値ＩＰＶとして図６Ｘで示すデータ構造でサーバ３Ａに保存し不正アクセスがあるかどうかを監視することもできる。
端末１Ａのセンサ１４４Ａのセンサ値は主にセンサ１４４Ａ、環境センサ１４４０Ａ、位置センサ１４４１Ａ、モーションセンサ１４４２Ａ、生体認証センサ１４４３Ａのセンサ値をユーザーの同意を得て利用する。プライバシー上好ましくないがやむを得ない場合は１４０Ａや１４１Ａ、１４３Ａ、１４２Ａといった入力装置１４Ａの入力そのものでも良い。１４３Ａや１４２Ａや１４１Ａ、１４０Ａといった入力装置をセンサ値として用いる場合はユーザーの情報提供の同意が無ければ利用できない。
ここで 環境センサ１４４０Ａは温度センサまたは湿度センサまたは気圧センサまたは圧力センサまたは照度センサまたは光センサ、化学センサ、においセンサといった端末周囲の環境にかかわる情報を物理的な手段を用いて測定できるできるセンサである。
位置センサ１４４１Ａは磁気センサまたは地磁気センサまたは加速度計を含み、加速度や磁気を物理量として測定し、重力加速度を用いた端末の向き、地磁気などに対する向きを示す磁気コンパス機能にも利用される位置を測定するセンサである。モーションセンサ１４４２Ａは加速度計またはジャイロセンサ（角速度センサ）のいずれか両方を含み、端末の加速度といった動きを検出するセンサであり、端末の動きを測定する。
生体認証センサ１４４３Ａは端末１Ａがカメラやサーモグラフィといった画像センサを

持ち前記画像センサを用いて顔の構造に由来する認証をするときのセンサであったり、スキャナを用いた指紋認証を行う指紋センサであったり、耳の構造に由来する認証を行うときのセンサであったり、歩行する際などに生じる装着された端末の感じるモーションや圧力信号を用いて認証する際のセンサである。生体認証は既知の方法を用いることができる。

【００４０】

＜ログイン実行と実行後の処理＞

端末３Ｃから端末１Ａにログイン後のウェブサイト、ウェブアプリデータを送付する。またログイン後のページにてユーザーが端末１Ａの入力装置を用いて入力した値をネットワークを通じてサーバ端末ＳＶＬｏｇｉｎ端末３Ｃが記録し、また入力した値によってユーザーデータの操作を行う。この例として具体的にはインターネットバンキングにおけるログイン後の振り込み処理や会員サイトでのデータの記録・変更や投票などの処理、オンライン株主総会での投票処理、オンラインゲームでの処理が挙げられる。ＯＴＰ認証後の処理に応じてはブロックチェーンにユーザー及びユーザー端末１Ａをアクセスさせ、処理を行わせた際にＯＴＰの生成関数を実行させＯＴＰを取得したのち取得したＯＴＰを引数に用いて認証関数を実行させたとき、３０１７Ａや３０１７ＡＡといった変数を変更させる。

ここでウェブサイト等の認証とログインに用いるとき３０１７Ａや３０１７ＡＡはサービスを利用出来る会員のポイントもしくは通貨残高が記録されており、本発明のログイン権や電子チケット等の情報をサービス提供時に提示したときにその残高がサービスに対応されるポイントもしくは通貨の数量だけ差し引かれていく形でもよい。会員ポイントや会員権専用の数値、通貨残高の他、オンラインゲーム等のデータについて改ざんされたくない重要なデータを記録してもよい。３０１７Ａや３０１７ＡＡはコントラクト内の他のユーザーやコントラクト管理者の指示によりその残高を変更し、あるユーザーの残高の一部を別のユーザーの残高に加算するという振込・振替処理を行えてもよい。

（ここで紙及び電子チケットやログイン権となりうる端末を端末３Ｄといったサービス提供機器に提示し認証するときも３０１７ＤＡにサービスを利用出来る会員のポイントもしくは通貨残高が記録されており、本発明の電子チケット、紙チケットの情報をサービス提供時に提示したときにその残高がサービスに対応されるポイントもしくは通貨の数量だけ差し引かれていく形でもよい。端末３Ｄ内の記憶装置のデータのうち、他のユーザーや端末３Ｄの管理者の指示によりその残高を変更し、あるユーザーの残高の一部を別のユーザーの残高に加算するという振込・振替処理を行えてもよい。端末３Ｄが端末３Ｃと同じくネットワーク２０に接続しノード端末３Ａや端末３Ｆや３Ｅと接続できる場合には端末３Ｄは端末３Ｃと同等とみなし端末３Ｃと同じ処理が行るものとみなす）

３０１７Ａや３０１７ＡＧはトークン番号に対応したＯＴＰトークンが持つ資産残高やデータ量を意味しており、認証関数実行後にそれらを操作してもよい。ＯＴＰ認証関数３０１８Ａの実行時に認証関数３０１８Ａ実行中に含まれる処理（もしくは認証関数の処理後にリンクされて別途行われる処理）として図３ＡＢの３０２１Ａ、３０２２Ａ、３０２３Ａがあってもよい。

前記３０１８Ａ、３０２１Ａ、３０２２Ａ、３０２３Ａは具体的にはインターネットバンキングの認証コントラクトがあり、そのコントラクトでは顧客の資産残高の記録が行われており、認証関数３０１８Ａに続いてコントラクト内にある別のユーザートークン番号（トークン番号と銀行口座番号が対応付けられていると想定）へ振り込み元のユーザーが３０１７ＡＡに記録された残高の範囲内で振り込み先にＯＴＰ認証関数が一致した際に振り込む処理をもつ３０２２Ａがあってもよい。

３０２２Ａは振り込み処理や定期預金、振り込み限度額設定といった設定を行う処理でもよい。そして銀行用途に限らず証券や保険など金融分野、私的または公的の公共又は民間の会員サイトなどでの投票などの意思表示・重要事項の変更、あるいはオンラインゲームなどで重要なユーザーのデータを記録させることに利用されうる。

【００４１】

＜不正ログインの検知＞

本発明ではログインしたユーザのＩＰアドレス（ＩＰアドレスのハッシュ化または加工した値）、または位置情報（位置情報をハッシュ化または加工した値）、またはコンピュータの装置ＩＤ（またはハッシュ値）と、トークン番号、ユーザー識別子をＳＶＬｏｇｉｎ（図３Ｃの端末３Ｃ）の記憶装置３０Ｃの３０１１Ｃに図６Ｘに示すデータ構造もしくはデータの形式で記録し、ログインしたユーザのＩＰアドレス（ＩＰアドレスのハッシュ化または加工した値）、または位置情報（位置情報をハッシュ化または加工した値）、またはコンピュータの装置ＩＤ（またはハッシュ値）を監視する処理部（図３Ｃの３１１０Ｃ、３１１１Ｃ、３１１２Ｃ、３１１３Ｃ）を端末３Ｃは備え、あるトークン番号やユーザー識別子に対して異なるＩＰアドレス、異なる位置情報、異なる装置ＩＤからアクセスしているか随時判断し、異なる場合にはユーザーに通知し、さらにはアクセスを遮断する機能を処理部（図３Ｃの３１１０Ｃ、３１１１Ｃ、３１１２Ｃ、３１１３Ｃ）を備える。

ここでコンピュータの装置ＩＤについては、デバイスＩＤなどのコンピュータ製造ＩＤやオペレーティングソフトウェアのＩＤ、ウェブブラウザのＩＤに加えて、端末１Ａに搭載された加速度センサや磁気センサ、圧力センサ（気圧センサ）、温度センサなどを含めた端末１Ａのセンサ１４４Ａ（図１４４Ａの１４４０Ａや１４４１Ａや１４４２Ａや１４４３Ａに記載のセンサ）情報を含むＩＰＶ値（図６Ｘに記載のデータ構造）やＩＰＶをハッシュ化したものを用いてもよい。この方法は本発明の他の利用例４Ｂ．４Ｃ．４Ｔに利用してもよい。

例えば端末１Ａが１４４Ａの位置センサ１４４１Ａに磁気センサを備え、地磁気を測定可能である３次元方向の磁気を検出可能な磁気センサーを搭載したスマートフォンであるとき、スマートフォン内蔵の磁気センサーの向きはユーザー端末の向きによって変わる。正常なアクセスであれば磁気センサーの値に対応するユーザー端末からのアクセス情報は１つしかないが、もしほかのユーザーが秘密鍵を不正に入手しログインしようとしても、攻撃者は離れた地球上のある位置にいるユーザーのコンピュータの磁気センサーの値と一致させなければならずなりすましは困難である。センサは一つだけでなく複数利用でき、例として地磁気センサと温度センサ、あるいは温度と気圧センサ（温度と圧力センサ）のように組み合わせる等が可能である。ＩＰアドレス（およびＩＰアドレスのハッシュ値または匿名化された値）とセンサ値を併用できると好ましい。

ここで端末１Ａに内蔵されるセンサについても説明する。全てのセンサを端末に内蔵している必要はなく、１つ以上のセンサを採用していれば好ましい。

１４４０Ａの環境センサは温度センサ、気圧センサ（圧力センサ）、湿度センサ、照度センサを含み前記４種のセンサの測定値を個別に端末１Ａに入力できる。

１４４１Ａの位置センサは磁気を検出する磁気センサと加速度を検出する加速度計を含み、端末の位置を検出できるセンサ。磁気センサや加速度計のセンサの測定値を個別に端末１Ａに入力できる。

１４４２Ａのモーションセンサは加速度計と角速度を検出するジャイロセンサを含み、端末の動きを検出できるセンサ。加速度計（加速度センサ）とジャイロセンサの測定値を個別に端末１Ａに入力できる。

１４４３Ａの生体認証センサは、例として顔やまばたきの情報であればカメラ１４２Ａを用い、指紋であれば指紋のスキャナを用い、静脈のパターン虹彩や耳の構造などはそれらを検出するセンサを用い、歩行に関する情報であれば端末１Ａの１４４２Ａや端末１Ａの通信装置１２Ａと通信できる外部端末の加速度センサと対応した靴型のモーションセンサデバイスや衣服に取り付けたモーションセンサ群を用いて測定してもよい。音声認証にてマイク・音センサ１４３Ａを備える端末では、端末周囲の音声を端末が感じることの出来る固有の音響情報として、前記音響情報をハッシュ化し個人のプライバシーを守りつつＩＰＶ値に用いることも出来うる。生体認証やプライバシーにかかわる情報を図６Ｘの情報に用いる場合はセンサが取得した情報をハッシュ化し、加工し、匿名化してを用いることが好ましいかもしれない。

ただし、銀行や証券など金融用途などでは防犯上ＩＰアドレスといった情報はそのまま記

録されることが好ましいかもしれない。

【００４２】

＜複数の秘密鍵を用いた不正アクセス対策＞

本発明の認証システムにおける実施形態では単一の秘密鍵１０１Ａを用いてもよいし秘密鍵１０１Ａ２といった１０１Ａとは異なる秘密鍵を用い、２つ以上の秘密鍵を用いてユーザー端末１Ａや１Ｂ、コントラクト管理者端末１Ｃなどからブロックチェーン部を持つサーバ３Ａのコントラクトの関数や変数へのアクセスを行ってもよいし、サービスを提供する端末３Ｃや端末３Ｄにアクセスしてもよい。本発明の認証システムを用いて暗号化されたデータを復号する用途に用いてもよい。

端末１Ａの秘密鍵１０１Ａを用いて１０１Ａに対応付けられたＯＴＰトークンのトークン番号がＴＩＤＡのときＯＴＰの認証関数及び生成関数で計算されるＢｎＴＯＴＰはハッシュ関数ｆｈとコントラクト内部変数ＫＣと前記のＡ、ＴＩＤＡを用いてＢｎＴＯＴＰ－１＝ｆｈ（Ａ,ＴＩＤＡ,ＫＣ,Ｂｎ）という引数と関数で表される。

ここで端末１Ａに搭載された秘密鍵１０１Ａのほかに１０１Ａ２という２番目の秘密鍵があり、その秘密鍵１０１Ａ２から計算されるユーザー識別子Ａ２とそれに対応付けられて発行されたＯＴＰトークンのトークン番号ＴＩＤＡ２があったとき2つ目のＢｎＴＯＴＰ－２＝ｆｈ（Ａ２,ＴＩＤＡ２,ＫＣ,Ｂｎ）が計算できる。

ＯＴＰ生成関数でＢｎＴＯＴＰ－１とＢｎＴＯＴＰ－２を生成した後、認証関数を持つコントラクト内の認証関数において関数の引数に、Ａ，ＴＩＤＡ，ＢｎＴＯＴＰ－１，Ａ２，ＴＩＤＡ２，ＢｎＴＯＴＰ２－２という形で、２つの秘密鍵１０１Ａと１０１Ａ２から計算されるユーザー識別子とＯＴＰトークンのトークン番号とＯＴＰ（ここではＢｎＴＯＴＰ－１およびＢｎＴＯＴＰ－２を例として示したが、ＯＷＰの場合はＯＷＰ－１とＯＷＰ－２といった形式も考えられる。）を用いて認証関数を実行させ認証を行ってもよい。前記のように２つの秘密鍵を用いることで２つの秘密鍵のうち１つが漏洩した場合、たとえば１０１Ａが漏洩し悪用され利用されているときは、もう片方の秘密鍵１０１Ａ２が漏洩しなければ関数の引数であるＢｎＴＯＴＰ－２（ＯＷＰの場合はＯＷＰ－２）が攻撃者にとっては不明であるので認証関数が実行できず、不正アクセスを防止する効果が期待される。

ここで秘密鍵を複数用いてＯＴＰトークンの認証に用いるときは、ＯＴＰトークンの認証を行うコントラクトにて秘密鍵１０１Ａから計算されるユーザ識別子Ａと秘密鍵１０１Ａ２から計算されるユーザー識別子Ａ２をユーザーＵＡが利用するユーザー識別子であるとコントラクト内部の変数もしくはサービス提供者・サービス提供者のデータベースに登録する必要がある。ユーザー識別子のほかにトークン番号ＴＩＤＡとＴＩＤＡ２が同一のユーザーＵＡに配布されていることをＯＴＰ認証関数を含むコントラクトに登録する部分を持っていてもよい。秘密鍵は２つに限定されず３個以上の複数個でもよい。

【００４３】

サーバ端末３Ｃや３Ｄなどの本発明においてサービス提供側となる端末にＵＡの二つの識別子ＡとＡ２もしくはトークン番号ＴＩＤＡとＴＩＤＡ２を登録し、ウェブサイトにログインするときにＡとＴＩＤＡとＢｎＴＯＴＰ－１の入力を求める認証を行った後、Ａ２とＴＩＤＡ２とＢｎＴＯＴＰ－２の入力を求める認証を行ってもよい。

ブロックチェーンではなくウェブサイトログイン先のサーバ端末３Ｃや３ＤにおいてＢｎＴＯＴＰ－１＝ｆｈ（Ａ,ＴＩＤＡ,ＫＣ,Ｂｎ）とＢｎＴＯＴＰ－２＝ｆｈ（Ａ２,ＴＩＤＡ２,ＫＣ,Ｂｎ）を別々にサーバ３Ｃが配信するウェブサイトのログイン画面にて認証処理を行い複数のＯＴＰトークンのＯＴＰ入力と認証をサーバ端末３Ｃや３Ｄで求めることもできる。この場合３Ｃや３ＤはユーザーＵＡの複数の秘密鍵に由来するユーザー識別子ＡとＡ２やＴＩＤＡとＴＩＤＡ２の対応付けを行って３Ｃや３Ｄの記録装置に記録されている必要がある。

サーバ端末３Ｃや３Ｄを用いて複数の秘密鍵によるＯＴＰトークンの認証に用いるときは、ＯＴＰトークンの認証を行うサーバ端末３Ｃおよび３Ｄで秘密鍵１０１Ａから計算されるユーザ識別子Ａと秘密鍵１０１Ａ２から計算されるユーザー識別子Ａ２をユーザーＵ

Ａが利用するユーザー識別子であると登録する必要がある。もしくはトークン番号ＴＩＤＡとＴＩＤＡ２が同一のユーザーＵＡに配布されていることをＯＴＰ認証関数を含むサーバ端末３Ｃや３Ｄに登録する部分を備えていてもよい。ＯＴＰトークンのコントラクト識別子が異なる場合も記録する必要がある。秘密鍵は２つに限定されずでなく３個以上の複数個でもよい。
複数の秘密鍵とそれに対し発行されたＯＴＰトークンの対応関係のデータベースはサーバ端末のみあるいブロックチェーン上のコントラクトのみまたはその両方に記録されていてもよい。サーバ端末３Ｃや３Ｄとブロックチェーン上のコントラクト双方に複数の秘密鍵を利用してアクセスする形態も考えられる。

【００４４】

本発明の実施において利用したイーサリアムでは１つのユーザー識別子あたり２５６ｂｉｔの秘密鍵を用いるが、それを本発明のＯＴＰ認証システムの実施形態で秘密鍵を２つ用いれば５１２ｂｉｔの秘密鍵となり、Ｎ個用いれば２５６×Ｎ［ｂｉｔ］の秘密鍵によりＯＴＰ認証することが可能となり、秘密鍵の実質的なデータ長を拡張可能となる。

データ長を増やすことで不正アクセスを行おうとする者の攻撃に対する耐性を高めることもできる。例として秘密鍵を３つ用いるよう設定した場合には、３つの内１つの秘密鍵が漏洩しても残り２つが漏洩していなければコントラクトの関数や変数へアクセスしないようにする事ができる。複数のうち過半数の秘密鍵が入手できなければ、それら秘密鍵に割り当てられたＯＴＰトークンの認証が行えないのでサービスの提供を阻止する事ができる。これは一種のマルチシグ技術である。（マルチシグ：複数の秘密鍵を用いた複数署名。）

複数の秘密鍵を組み合わせてＯＴＰ認証を行うことで秘密鍵身元確認に関する運用ができるかもしれない。例えば２つ秘密鍵があり、片方は第三者機関と共有する身元確認のできている秘密鍵１０１Ａ２でもう片方はユーザーが端末１Ａ内部で生成した秘密鍵１０１Ａであるとき、かつ秘密鍵の利用を開始した直後におそらく秘密鍵の漏洩が無いと思われるときに、１０１Ａ２と１０１Ａの双方の秘密鍵で計算されるユーザー識別子Ａ２とＡを第三者機関やそれらをユーザー識別子と実在する人物ＵＡとの対応付けを行う第三者機関などのサーバ端末３ＣにＴＩＤＡとＴＩＤＡ２のトークンを用いて第三者機関第三者機関や対応付けを行う団体のウェブサイトにＯＴＰ認証してログインなどして登録する。

ＡとＡ２もしくはＡとＡ２に割り当てられたトークン番号ＴＩＤＡとＴＩＤＡ２のＯＴＰトークンによって、端末３Ｃの管理者はユーザーＵＡに伝えたＡ２の秘密鍵１０１Ａ２を知るＵＡが、Ａというユーザー識別子Ａを使うことと、Ａに対応した秘密鍵１０１Ａを持っていることが分かる。このときＡとＡ２とユーザーＵＡが紐づけられ簡易に本人確認できたとする。そしてＡに対し、ユーザーＵＡの所有する秘密鍵に対応するユーザ識別子であると判断し、ユーザー識別子Ａをトークンなどの送付先アドレスとして、例えばある会員サイトへのログイン権やある会場への入場券・施解錠する鍵、そして暗号化データを復号するＯＴＰトークンの発行や配布を行えるようになるかもしれない。

本発明のＯＴＰトークンを発行する際にユーザー識別子ＡやＡ２が実在するユーザーＵＡの識別子であるか確認する必要があり、ユーザー識別子Ａの入力ミスにより秘密鍵１０１Ａとは全く異なる秘密鍵にＯＴＰトークンが発行されることも考えられ、ＯＴＰトークンの送付先ユーザー識別子がユーザーＵＡやＵＢ、ＵＣといった実際のユーザーのが秘密鍵を記録して利用できている者かどうかを確認する必要があり、本人確認が必要と考えるため、前記本人確認法を示した。ただし１つの形態であって、本発明の実施時に必ず複数の秘密鍵を用いたＯＴＰトークンによる本人確認を行うわけではない。本人確認方法は他の既知の方法を用いてもよい。

【００４５】

＜レイティングやコントラクト管理者への連絡先を含むコントラクトの看板となる情報＞
看板変数３０２４Ａ（図３ＡのＫＮＢＮ、３０２４Ａ）にはレイティング情報のほかにコントラクトが提供するサービスの名前、トークンの名前、説明事項を変数に記録させ看板となる情報としてパブリック変数として公開してもよい。また看板となる情報はコント

ラクト管理者が書き換えることができてもよい。
具体的には、インターネットバンキングの場合は３０２４Ａに銀行の名称、郵便番号、銀行の本店の住所、法人番号、代表等電話番号（ファクシミリ番号）、銀行を所管する最寄りの省庁への連絡先など営業に関する必要事項をコントラクトの変数に記入しパブリック変数として公開してよい。サービスを提供する際に法律的に必要な事項をワンタイムパスワード生成トークンのコントラクトやワンタイムパスワード認証コントラクトに記入し、そのコントラクト管理者が書き換えられるようコントラクトをプログラムしてよい。
看板となる情報３０２４Ａは本発明のコントラクトに必要に応じて記入し、コントラクト管理者が書換できてもよい。３０２４Ａにはコントラクト管理者の端末１Ｃの秘密鍵１０１Ｃのみがアクセス可能となる書き換えに必要なセッター関数が含まれていてもよい。

【００４６】
＜レイティング＞
サービス対象年齢等を示すため、ワンタイムパスワード生成トークンのコントラクトにはレイティング情報が記録される。看板となるパブリック変数ＫＮＢＮ（図３ＡＡから図３ＡＣに記載の３０２４Ａ）にレイティング情報が記載される。３０２４Ａに書かれたレイティング情報はＯＴＰトークンのサービスの対象者を記述する。例として自動車の鍵に本発明を用いるとき、免許を受けたある年齢以上のユーザーが利用するはずのサービスであるのでその旨が記載される。未成年を対象とするか成人を対象とするか、免許など資格が必要かはサービスによって変わる。
ここでレイティング情報を格納したコントラクトの変数は全てのユーザーから閲覧できるパブリック変数であることが好ましい。またレイティングはコントラクト管理者が書き換えることができてもよい。

【００４７】
４Ｂ．入場口や建物設備への紙又はＩＣ式入場券、利用券、解錠鍵としての利用
チケットや入場券、建物設備の施錠と解錠に使う場合にはサーバＳＶＬｏｇ（図８Ｂや図３Ｄに記載のサーバ端末３Ｄ）を用いる。図８Ｂに端末の接続図を示す。サーバＳＶＬｏｇ（端末３Ｄ）は入場等の処理するユーザーが少ない場合には必ずしもサーバである必要はなくサーバより計算能力や記憶装置の容量、物理的な大きさの小さいコンピュータＳＶＬｏｇ（端末３Ｄ）でもよい。そして端末３Ｄは建物の施錠装置や自動車の施錠装置・原動機の始動装置を動作させる組み込み型の端末でもよい。３Ｄは組み込みシステム用のＭＣＵを持つ端末（Micro Control Unit、マイクロコントロールユニット、マイクロコントローラ、マイコン）でもよい。
本発明ではＮＦＣなどの通信機能を備えたＩＣタグ・ＩＣカード型のチケット１９Ａまたは紙のチケット１８Ａ（および紙のチケット１８Ａと同じＯＴＰ認証情報を表示させたディスプレイの表示面１５００Ａ）の記録情報にブロックチェーンから生成されたパスワードＯＷＰを利用する（ここでＩＣはIntegrated circuitであり集積回路のこと）。

【００４８】
１９Ａは非接触のＮＦＣタグや、接触型端子を持つＩＣカードであり、１９Ａの利用者ではないユーザーに不正使用させないように１９Ａに利用者がパスワードとしてＰＩＮ等を設定してもよい。１９Ａと端末３Ｄとの通信を行いＯＷＰなどの認証情報を伝達する際に、１９Ａに設定されたＰＩＮによるパスワード認証を求め、パスワード認証ができた場合にＮＦＣタグの情報を端末３Ｄの通信装置３２Ｄを通じて端末３Ｄに伝達してもよい。

【００４９】
ここでＰＩＮは個人識別番号（Personal identification number）の略であり、ＰＩＮは例えば４桁の整数のパスワードである。１９ＡのＰＩＮは１９Ａを用いてサービスを利用する際の最終的な利用意思確認手段として用いる。１９Ａは無線により通信するため１９Ａを所有するユーザーが知らぬ間に１９Ａの情報が端末３Ｄに伝達されないようにＰＩＮを用いてもよい。１９Ａは３Ｄと無線もしくは有線方式の通信を行う際に通信内容を暗号化してもよい。ＰＩＮなどを用いて１９Ａに記録されたＯＷＰを用いる認証情報を暗号

化してもよい（ＯＷＰを、ＰＩＮを鍵として共通鍵暗号化などの手段をもちいて暗号化してもよい）。１８Ａや１５００Ａはそれらを持つユーザの利用する意思がヒトの手で提示されることで確認できるが、１９Ａは無線通信などである程度離れていても決済ができてしまう恐れがあるのでＰＩＮコードを設定出来てもよい。

ＰＩＮを用いることで１９Ａのセキュリティ性は向上するが、サービスを認証するたびにＰＩＮの入力を必要とすることはＰＩＮ入力の時間をユーザーに要求しユーザーの利便性を下げることにつながることもあるかもしれない。そこで１９Ａと１９Ａの無線通信信号を読み取るＮＦＣ通信装置３４１Ｄ（前記通信装置は３４１Ｄまたは３２Ｄ）が非接触ではあるが通信距離が１０ｃｍ（具体的には１３．５６ ＭＨｚといった周波数を利用する通信距離１０ｃｍ程度の既知の近距離無線通信技術）であり、サービス提供者が１９Ａについて前記条件（通信距離１０ｃｍ程度の１９Ａであること）を示し、ＰＩＮが無くともＮＦＣタグ１９Ａによる本発明の認証システムを用いた認証結果に応じてサービスを提供することを許容する場合にはＰＩＮなどを設定せず、１９Ａを３Ｄの３２Ｄもしくは３４１ＤにかざすだけでＯＴＰ認証を行い認証結果に応じてサービスを提供する形で本発明を実施してもよい。（１９Ａにはセキュリティの為にＰＩＮを設定することもできる。そして１９ＡにはＰＩＮの設定をしないで利用することもでき、ＰＩＮを設定しない場合は入場口や改札などでの決済速度を向上させ、使いやすさ、ユーザビリティ、利便性を優先して利用することもできる。）

自動車のキーレスエントリー、リモート（通信距離が１０ｃｍを超え１ｍを超える）での自動車ドアの解錠用途に用いる施解錠鍵１９Ａや建物のドアのリモート（通信距離が１０ｃｍを超え１ｍを超える）での解錠用途に用いる施解錠鍵１９ＡでもＰＩＮを用いることが必要な用途と必要でない用途がある。通信距離が１０ｃｍを超え１ｍを超える自動車用途では１９ＡにＰＩＮは不要かもしれない。

通信距離が１０ｃｍを超え１ｍを超える建物や金庫・金庫室の施解錠用途では施解錠にもＰＩＮを用いたほうが好ましいかもしれない。

【００５０】

パスワードＯＷＰはハッシュ関数ｆｈとユーザ識別子Ａとトークン番号ＴＩＤＡとコントラクト内部シークレット変数ＫＣ値３０１１Ａとコントラクト管理者が変更できる変数ＢＣ値３０１３Ａを用いてＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）として計算される。ＯＷＰは前記ハッシュ関数ｆｈと引数を用いてＯＴＰ生成関数３００９Ａで計算され生成される。３００９Ａはこの利用例ではＯＴＰ＝ＯＷＰとしてＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）と表現できる計算処理を含む。

紙のチケット１８Ａは本発明のワンタイムパスワードＯＷＰの生成関数３００９Ａを用いて取得したＯＷＰ情報を紙などに印刷し製造される。１８Ａに記録される情報は少なくともユーザー識別子Ａとトークン番号ＴＩＤＡとパスワードＯＷＰを含む。１８Ａに記載の情報は１５００Ａで表示できる。１８Ａや１５００Ａを読み取るカメラなどの装置がサービス提供端末３Ｄに備えられている場合にはチケットなど有価紙葉のようよのほかに施解錠を行う金庫・金庫室や建物のドア、入退場口、自動車など乗り物や電子計算機端末に認証情報を読み取らせることができ、入退場や施解錠ができる。

ＮＦＣタグ１９は、端末１Ａが保有するユーザー識別子Ａとトークン番号ＴＩＤＡとパスワードＯＷＰを含む認証情報を端末１Ａの通信装置１２Ａを経由して１９Ａに記憶させることで１９Ａを製造でき、チケットなど有価紙葉や入退場用のタグや施解錠の鍵あるいはアクセス制御を解除するものとして用いられる。

図８Ｂに示すように前記ＡとＴＩＤＡとＯＷＰを記録したＮＦＣタグ１９Ａや、ＡとＴＩＤＡとＯＷＰを表示する端末１Ａのディスプレイ画面１５００Ａ、そしてその画面１５００Ａを印刷した紙のチケット１８Ａでもよい。

【００５１】

図８Ｂに示すように１８Ａと１５００Ａは端末３Ｄのカメラ・スキャナ３４０Ｄによって読み取られる。この時１８Ａと１５００ＡはＡとＴＩＤＡとＯＷＰを連結した文字列情報を表示していてもよいしバーコード情報（１次元及び２次元のバーコード）を表示して

いてもよい。
図８Ｂに示すように１９Ａは端末３Ｄの３２Ｄと通信しＡとＴＩＤＡとＯＷＰを連結した文字列情報を伝達してもよい。１９Ａと３２Ｄの通信にはＮＦＣを用いることを想定する。
１５００Ａ、１８Ａ、１９ＡからＡとＴＩＤＡとＯＷＰを受け取った端末３Ｄの制御部及び記憶部（３１Ｄおよび３０Ｄ）に備えられたパスワードＯＷＰの認証関数３０１８ＤＡ（図３ＤＡの３０１８ＤＡ））は図６Ｆや図６ＤのＯＴＰ認証関数の処理に関するフローチャートに従い、入力されたＯＷＰ（ＡｒｇＯＷＰ）が端末３Ｄに記録されたＫＣやＢＣ値を用いて計算されるＶｅｒｉＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）と一致するか検証し、一致した際には認証ができたと判断し、端末３Ｄは端末３Ｄが組み込まれた装置の開閉装置３５０Ｄまたは施錠装置３５０Ｄ（施解錠装置３５０Ｄ）または始動装置３５０Ｄまたはアクセス制御装置３５０Ｄを操作して、改札口や入場口の入場処理または施錠された建物や自動車など乗物と金庫など容器の解錠を行い、乗物や電子計算機、機械、設備の始動を行う。
【００５２】
認証関数３０１８ＤＡは図６Ｆや図６ＤのＯＴＰ認証関数の処理に関するフローチャートに従い１５００Ａや１８Ａや１９Ａの情報からＯＷＰ（ＯＷＰ＝ＡｒｇＯＷＰとして）とＡとＴＩＤＡとを引数として受け取る。そして図３ＤＡに示す３ＤのＫＣ値３０１１ＤＡやＢＣ値３０１３ＤＡ、ハッシュ関数３０１０ＤＡを用いてＶｅｒｉＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）を計算する。ここでＶｅｒｉＯＷＰとＡｒｇＯＷＰの計算に用いたハッシュ関数ｆｈとＫＣ値とＢＣ値は、ブロックチェーン上で１８Ａや１９Ａのためのの ＯＷＰを生成する端末３Ａとサービスを行う端末３Ｄのシード値ＫＣ、ＢＣ及びハッシュ関数ｆｈ等がすべて一致しなければならない。
認証関数３０１８ＤＡの関数の戻り値が認証結果の正しい時の値ならば端末３Ｄは３５０Ｄの開閉装置を開いたり施錠装置（施解錠装置）を解錠したり装置を始動させることができ、認証が失敗するときは開閉装置を閉じ、施錠装置（施解錠装置）の操作を行わず、装置を始動は行わない。
（ブロックチェーン上の３ＡでＯＷＰを計算する際に用いる変数と手順が端末３ＤでＯＷＰを計算する際に用いる変数と手順に一致しなければ、正しく生成されたＯＷＰを含む１５００Ａや１８Ａや１９Ａを端末３Ｄに提示しても誤った認証結果が計算され入場処理や解錠処理などを行えない。具体的には正しい認証情報を含むＮＦＣタグ１９Ａを持つユーザーＵＡが誤った３０１１ＤＡや３０１３ＤＡを記録した端末３Ｄに提示しても端末３Ｄは誤った３０１１ＤＡや３０１３ＤＡを用いて誤った認証関数３０１８ＤＡによってＯＷＰの検証を行い、認証関数の実行結果から１９Ａを不正なもの、入場や施錠の解錠を行えないものと判定し開閉装置や施錠装置を閉じたままにし、あるいは警告用のブザーなどを鳴らしてしまう。）
【００５３】
コントラクトの管理者とサービスおよび端末３Ｄの管理者は、ブロックチェーンのノード端末３Ａのハッシュ関数３０１０Ａと端末３Ｄの３０１０ＤＡを一致させ、端末３ＡのＫＣ値３０１１Ａと端末３Ｄの３０１１ＤＡを一致させ、端末３ＡのＢＣ値３０１３Ａと端末３Ｄの３０１３ＤＡを一致させ、ほかに変数や関数をＯＷＰの計算に用いる場合にはそれらを一致させ、端末３Ａと端末３ＤでのＯＷＰ型ＯＴＰの計算方法と計算に用いる変数を一致させ同期させなければならない。ＯＴＰの計算方法と計算に用いる変数を一致させることで１５００Ａや１８Ａや１９Ａを用いた紙やＮＦＣタグによる現実世界での本発明のＯＴＰ認証サービスが可能になる。
端末３Ｄが建物の扉や金庫に組み込まれた施錠を管理する端末であるときに、シークレット値ＫＣやＢＣの変更が生じたとき、端末３Ｄが組み込まれた扉や金庫等の利用者が施錠された設備の解錠後にアクセスできる位置（具体例として金庫の扉の裏側もしくは建物の扉の裏側、建物の扉の屋内側）に備えられた施錠管理端末３Ｄの通信装置３２Ｄに有線式もしくは無線式の方法でアクセスし、端末３Ｄの製造元の提供するソフトウェアなどに

従い３２ＤのＫＣ値３０１１ＤＡやＢＣ値３０１３ＤＡを更新できてもよい。
【００５４】
本発明を金属製の鍵と比較すると、ＯＷＰ＝ＡｒｇＯＷＰとして、ＡとＴＩＤＡとＡｒｇＯＷＰの情報が鍵であり、ＡとＴＩＤＡとＶｅｒｉＯＷＰの情報が錠に対応する。本発明では鍵と錠の情報は可変であり鍵と錠の情報が同期できず鍵を計算する条件と錠を計算する条件が一致しなければ認証を行うことができない。（参考に、ウェブサイトのログインなどに用いる想定のＢｎＴＯＴＰの場合はＡとＴＩＤＡとＡｒｇＢｎＴＯＴＰの情報が鍵であり、ＡとＴＩＤＡとＶｅｒｉＢｎＴＯＴＰの情報が錠に対応する。）
ブロックチェーンに鍵となるＯＴＰトークンとＯＴＰトークンが生成するＯＷＰ型のパスワードは分散型台帳技術で共有され改ざん困難な状態で保存可能であるが、３Ｄが３Ａと接続できない場面において本発明の実施を行う場合には、端末３Ｄの管理者が錠となる情報を最新の情報に更新する、もしくは端末１ＡのＯＷＰ型のパスワードとユーザー識別子Ａとトークン番号ＴＩＤＡを１５００Ａや１８Ａや１９Ａで認証できる情報を設定することが求められる。
【００５５】
端末３Ｄと端末３Ａで計算されるＯＷＰを一致させるために、ＫＣ値３０１１Ａ・３０１１ＤＡやＢＣ値３０１３Ａ・３０１３ＤＡをコントラクトのデプロイした後は変更しないという利用形態も考えられる。前記利用形態ではパスワードの更新は行われずセキュリティ上問題はあるものの、例えば少人数の限られたコミュニティで利用するある行事の一度限りの入場券などで利用する用途が想定される。ＫＣ値やＢＣ値の変更は可能だが実際は変更しないという利用形態のほうがサービス提供者の労力を抑えることができ本発明を利用しやすくするかもしれない。
この場合はＯＴＰトークンに有効期限や保証期限を明記する事が好ましい。簡易の金庫や錠前などの製品に用いるとき製品保証期間を設けそれを超える期間のコントラクトの管理は一切行わないという方法を使い、使い捨てのコントラクトという形でサービスを提供する形態もあるかもしれない。
【００５６】
限られたコミュニティの行事で利用する入場券として１５００Ａや１８Ａや１９Ａを利用する場合には、ユーザー識別子ＡとトークンＩＤＡとＯＷＰの３つの必須情報に加え１５００Ａや１８Ａや１９Ａを製造または作製した時刻や有効期限、入場券を利用できる場所の住所、入場券を発行しサービスを提供する責任者の名称と連絡先などを１５００Ａや１８Ａや１９Ａに記録してもよくそれら情報は文字列情報として１５００Ａや１８Ａに表示印刷され１９Ａの場合は端末１Ａのディスプレイに文字列として表示するなどしてヒトが有価紙葉の情報を目視で確認できることが好ましい。
ユーザー識別子ＡとトークンＩＤＡとＯＷＰの３つの必須情報は２次元バーコードとして表示しカメラやスキャナで読み取れるようにする事で認証に必要な情報を３Ｄの３４０Ｄに読み取らせることができる。またＯＷＰは読み取られると不正利用されうるため、ユーザー識別子やトークン番号を文字列で記載し、別途認証用にユーザー識別子ＡとトークンＩＤＡとＯＷＰの３つの必須情報は２次元バーコードとして印刷または表示または記録したＯＷＰのみは二次元バーコードとして記録される形態の１５００Ａや１８Ａがあってもよい。
１５００ＡについてはＯＷＰ以外の情報については目視または音声による読み上げを行いトークン番号やユーザー識別子、サービスの有効期限やサービスの提供先の情報についてユーザーに知らせる機能を端末１Ａが持っていてもよい。セキュリティが保たれた場合においては１８Ａを読み上げる画像認識端末があってもよい。
（ＯＷＰはサービス提供端末３Ｄ以外には入力してはいけない秘密情報である。セキュリティ上問題のあるソフトウェアを用いてＯＷＰの含まれた１８Ａや１５００Ａを読み取り、読み上げ、撮影、画像認識したり、ＰＩＮなどで保護されていない１９Ａの情報を読み取られた場合はＯＷＰなどが漏洩し不正利用される恐れがある。）
【００５７】

＜入場時のＯＴＰトークンを利用済みにする処理等＞
端末３Ｄまたはブロックチェーン上のコントラクトにて認証関数３０１８Ａ（または３０１８ＤＡ）の実行回数記録部分３０１７Ａや３０１７ＡＡ（または３０１７ＤＡ）にチケットをユーザーが本発明のＯＴＰ認証を行い認証関数を実行し認証ができてサービスを利用したか否か、チケットが有効か否かの真偽値、もしくはチケットの利用回数の整数値を記録してもよいし、３０１７Ａや３０１７ＡＧ（または３０１７ＤＡ）にチケットのサービスを利用出来るポイントもしくは通貨残高がチャージされており、本発明の電子チケット１９Ａ、紙チケット１８Ａ、画面表示型チケット１５００Ａの情報をサービス提供時に提示したときにその残高がサービスに対応されるポイントもしくは通貨の数量だけ差し引かれていく形でもよい。
ウェブサイトのログイン処理で利用する場合と同じく、ＯＴＰ認証関数３０１８Ａ（または３０１８ＤＡ）の実行時に認証関数３０１８Ａ（または３０１８ＤＡ）実行中に含まれる処理として図３ＡＢの３０２１Ａ、３０２２Ａ、３０２３Ａ（または図３ＤＡの３０２１ＤＡ、３０２２ＤＡ、３０２３ＤＡ）を行ってもよい。
利用済みにする機能はサービス提供者とユーザーが合意して利用するＯＴＰトークンにおいては、コントラクトの管理者がユーザーの要請を受けもしくはユーザーが不正な利用などをした場合にその数値を端末１Ｃと秘密鍵１０１Ｃを用いてコントラクトに設定されたセッター関数より３０１７Ａや３０１７ＡＡ（または３０１７ＤＡ）を書換えてもよい。
例えば改札やサービス提供窓口などで３０１７Ａや３０１７ＡＡ（または３０１７ＤＡ）の数値を入場の有無を示す真偽値やその回数を示す整数に加えて前記変数３０１７Ａや３０１７ＡＡ（または３０１７ＤＡ）に通貨を前払式決済手段のように残高をチャージさせ、チャージされた通貨の数値に応じて変数３０１７Ａや３０１７ＡＡ（または３０１７ＤＡ）を増加させるための処理を管理者端末１ＣがユーザーＵＡの端末１ＡからアクセスできるＯＴＰトークンに付与できる。
そしてサービスの利用金額に応じて金銭相当額の数値がチャージされた３０１７Ａや３０１７ＡＡ（または３０１７ＤＡ）の残高よりサービス料金額相当分を減少させることが可能である。この場合には認証関数３０１８Ａ（または３０１８ＤＡ）において図６Ｄのフローチャートの Ｆ１１５やＦ１１６において３０１７Ａや３０１７ＡＡ（または３０１７ＤＡ）の残高値がサービスの料金の数値よりも高いかどうか判定し、残高不足であるときは認証関数の実行を停止し、残高の再チャージを促す処理や、サービス提供者へ連絡するなどの処理が必要となる。
【００５８】
＜正常もしくは不正な入場を検出し知らせる機能＞
秘密鍵ＰＲＶＡ（端末１Ａの１０１Ａ）が漏洩し不正にサービスが利用されているかどうか調べ判定するために、ＳＶＬｏｇ（端末３Ｄ）に記録する１５００Ａや１８Ａや１９Ａによる認証を行ったときのトークン番号やユーザー識別子に対してその風貌を防犯カメラ３４２Ｄで撮影し保存してもよい。風貌は好ましくは顔、体格、体型、モーション、歩行など生体情報であると好ましい。前記生体情報を利用する意図は例えばサービスを提供する会場で不正な入場を防止するためである。ここで同じＯＷＰ認証情報とユーザー識別子ＡとトークンＩＤＡを含む１５００Ａや１８Ａや１９ＡをコピーしてコピーしてＯＷＰを複製し使い回すことにより異なる人間が同じ認証情報（ＡとＴＩＤＡとＯＷＰ）を用いて入場することの監視も同様に行う。
ユーザーの風貌を記録する監視カメラ３４２Ｄ（図８Ｂの３４２Ｄ）は生体情報を記録する場合の一例として図８Ｂに示している。ただし、生体情報を記録することは本発明にとって必須の機能ではなく駅の改札や入場口の入場処理などにおいて必要な機能であって、大型の金庫や金庫室では防犯カメラ３４２Ｄを内蔵することもできるが、端末３Ｄの電源部３７Ｄに用いる電池容量の制約や経済性の兼ね合いから小型の金庫や手提金庫などの容器に端末３Ｄを組み込む場合は防犯カメラ３４２Ｄは利用が困難であったり必要ない場合がある。３４２Ｄは用途・実施形態により搭載できるかどうか決めることができる。

また同じく自動車の施錠や建物の施錠装置に端末３Ｄを用いる際もプライバシーに配慮して３４２Ｄを搭載しないこともある。プライバシーを犠牲にしつつ防犯のため３４２Ｄを搭載することもある。例えばタクシー、バスといった用途や自動車の貸し借り・レンタカー・カーシェアリングなどの用途では防犯カメラがあることが好ましいかもしれない。サービスに応じて防犯カメラといったユーザーの存在を記録する手段の利用をサービス提供時や契約時にユーザーに知らせることが必要である。

【００５９】

３Ｄについて防犯カメラ３４２Ｄを用いないとき場合に防犯上利用可能な機能として、図８Ｂのランプなどの発光素子３５１Ｄまたはブザー等発音素子３５２Ｄを利用し音や光にてＯＷＰを用いた認証が成功したときの動作と失敗したときの動作を設定し利用する。具体的には金庫などの容器に端末３Ｄを備えて使用する場合にはＮＦＣタグ１９Ａに認証に用いる情報記録され、１９Ａを金庫内部の端末３Ｄが通信装置３２Ｄを用いてＮＦＣタグ１９Ａの情報を読み取り認証結果が正しければ金庫の施錠を解錠し、正しくない場合にはブザーで警告音を出すということができる。ブザーの代わりに通信装置３２Ｄで無線により周囲に電波のビーコン、無線標識を出してもよい。

防犯カメラ３４２Ｄとランプなどの発光素子３５１Ｄまたはブザー等発音素子３５２Ｄを併用して利用してもよい。

例として駅の改札において用いる１５００Ａや１８Ａや１９Ａが認証済みで利用済みかつ無効となったトークン番号を再度提示して認証を行おうとしたユーザーＵＡが現れたとき改札の開閉装置３５０Ｄは閉じた状態にしてＵＡをその場に留め、防犯カメラ３４２Ｄとランプなどの発光素子３５１Ｄまたはブザー等発音素子３５２Ｄを併用して周囲に知らせ、駅の従業員に知らせてトークンが不正利用されているかどうかをそのユーザーＵＡに尋ねることができる。

【００６０】

端末３Ｄが金庫等の容器である場合に限らず、端末３Ｄが改札・入場口や自動車・建物においても認証結果の出力に応じて発光素子３５１Ｄや発音素子３５２Ｄを動作させ認証結果が正しいか否かを端末３Ｄの周囲（周囲とは３５１Ｄや３５２Ｄや３２Ｄが信号をユーザーや端末に伝達できる距離の範囲内）やサービスの提供者に知らせることに利用される。なお発光素子３５１Ｄは電球などランプの他に発光ダイオード等の電流を流すことで光を発する半導体素子でもよい。

【００６１】

＜認証の回数と認証を行った人物を検知する場合＞

１．改札や入場口において端末３Ｄがインターネットワークに接続されサーバ３Ａと接続している場合。

秘密鍵ＰＲＶＡが漏洩し本来の利用権を持つユーザーＵＡが、１５００Ａや１８Ａや１９Ａを３Ｄの入力装置もしくは通信装置に読み取らせて提示し、改札や入場口を通る前に、別の人物ＵＢが秘密鍵ＰＲＶＡ（１０１Ａ）を何らかの手段で入手し自身の端末に複製して記録させ不正利用して入場口を通過することが想定される。もしくはＯＷＰの流出と使い回しによる不正利用も考えられる。

不正利用の際にＵＢの容姿を記録することで本人確認や本人の追跡を可能にする画像データ、認証決済時の時刻と認証端末の位置や端末番号（改札では駅名等）、歩行の様子等を得る。そして認証が起きたことをブロックチェーン上の認証用コントラクトの認証関数３０１８Ａの実行回数を記録する変数３０１７Ａや３０１７ＡＡをインクリメント等することで記録する。

またユーザーＵＡに対しあるサービスのある入場口でサービスを利用したことを電子メールなどで通知する。ユーザーＵＡがサービス提供者に対しチケットが不正利用されたと申し立て、不正に入場したＵＢの顔、体系、歩行情報等と照らし合わせ、ユーザーＵＡが不正に入場していないか判断することに利用できる。

ここでサーバ３Ｄがサーバ３Ａと同じくブロックチェーンのノードとなるときは３Ｄは３Ａと同じ機能を持つので３Ｄのブロックチェーン部（３００Ｄおよび３１０Ｄ）に認証

関数３０１８Ａが記録されており、３Ａではなく３Ｄのブロックチェーン部にユーザーＵＡの端末１Ａがアクセスして認証関数３０１８Ａを実行してもよい。

不正利用時はユーザーＵＡのＯＴＰトークンの利用を停止させ不正利用の被害の拡大を限定することが必要かもしれない。そこでユーザーＵＡのＯＴＰトークンの利用をサービス提供者が端末１Ｃを用いて停止できる変数を端末３ＡのＯＴＰトークンのコントラクトに備え、セッター関数を用いて変更できてもよい。もしくは改札などでサービス提供者のメインサーバ端末がトークンごとの残高をブロックチェーンとは別に管理している場合はそのメインサーバ端末の顧客ごとの設定を変えることで対応する。

【００６２】

２．改札や入場口において端末３Ｄがローカルエリアネットワーク（ＬＡＮ）に接続されサーバ３Ａと接続している場合。

ある駅や施設のローカルエリアネットワークに接続されインターネットワーク２０とは切断されている場合、端末３Ｄの記憶装置には１５００Ａや１８Ａや１９Ａを生成するのに用いたハッシュ関数３０１０Ａと３０１０ＤＡと一致させ、ＫＣ値３０１１Ａと３０１１ＤＡを一致させ、ＢＣ値３０１３Ａと３０１３ＤＡを一致させ、ほかに変数や関数をＯＷＰの計算に用いる場合にはそれらを一致させ、端末３Ａと端末３ＤでのＯＷＰ型ＯＴＰの計算方法と計算に用いる変数を一致させ、同期させなければならない。そして認証関数３０１８Ｄにより認証し認証できた回数もしくは認証時に変更を加えたデータを３０１７ＤＡに記録したり、あるいは３０１６Ｄに記録してもよい。

映画館や駅などの施設内のＬＡＮを通じて、施設の職員等が端末３Ｄへのアクセス権を持つ端末を持ちいて端末３Ｄのデータベース３１１６Ｄ（３１１４Ｄや３１１５Ｄを含む）にアクセスしユーザー識別子やトークン番号をキーとしてそのトークン番号のＯＴＰトークンに対するサービスの提供状況を検索し把握することが可能である。また１８Ａに印刷された紙の有価紙葉が認証に必要な情報が読み取れない場合にはユーザー識別子やトークン番号を１８Ａから得て３１１６Ｄの顧客情報と照合し、ＯＴＰトークンの購入履歴がありサービスを提供することの出来るユーザーか判断する（この手続きを行う場合には身分証が必要かもしれない）。

【００６３】

３．端末３Ｄがネットワークに接続せずオフラインの時。

改札や入場口、もしくは自動車の施錠装置、建物の施錠装置、金庫など容器の施錠装置に組み込まれている端末３Ｄがネットワーク２０と接続されていないときも、端末３Ｄの記憶装置には１５００Ａや１８Ａや１９Ａを生成するのに用いたハッシュ関数３０１０Ａと３０１０ＤＡを一致させ、ＫＣ値３０１１Ａと３０１１Ｄが一致させ、ＢＣ値３０１３Ａと３０１３ＤＡを一致させ、ほかに変数や関数をＯＷＰの計算に用いる場合にはそれらを一致させ、端末３Ａと端末３ＤでのＯＷＰ型ＯＴＰの計算方法と計算に用いる変数を一致させ同期させなければならない。そして認証関数３０１８ＤＡにより認証し認証できた回数もしくは認証時に変更を加えたデータを３０１７ＤＡに記録したり、あるいは３０１６Ｄに記録してもよい。

施錠の解錠をした後にアクセスできる部分に端末３Ｄがあり、３Ｄの通信装置３２Ｄが有線通信用のコネクタや端子あるいはアクセス可能な端末を限定できる無線通信装置を備え、利用者もしくは管理者の端末（１Ａや１Ｃ）の通信装置から端末３Ｄの通信装置３２Ｄを経て記憶装置３０ＤのＫＣ値３０１１ＤＡまたはＢＣ値３０１３ＤＡの変更またはハッシュ関数ｆｈの変更を行い、端末３ＡのＯＴＰ生成関数３００９Ａの生成するＯＷＰと認証関数３０１８ＤＡが生成するＯＷＰが同じものとなるよう変更できる手段を備える。ＯＷＰの算出に用いるＫＣ値３０１１ＤＡまたはＢＣ値３０１３ＤＡを更新できる余地を残すことで、例えば自動車や建物の施錠装置の解錠鍵となるデータを定期的に更新でき、自動車や建物の施錠装置の鍵を更新できる。

【００６４】

＜ワンタイムパスワードの生成と認証の回数を検知する場合＞

本発明ではワンタイムパスワードの生成と認証がコントラクトの同一の関数で行われな

い。生成時、認証時にそれぞれのＯＴＰ生成関数やＯＴＰ認証関数の実行回数をカウントしインクリメント（増加）する変数と処理部を備えることができ、それら実行回数３０１７Ａや３０１７ＡＧや３０１７ＡＡはブロックチェーンを用いることで改ざんされにくくなる。実行回数をカウントする変数のうち生成時に利用する変数３０１７Ａや３０１７ＡＧを監視することで不正利用を防ぐことにつなげられる。（ブロックチェーン上にはないが端末３Ｄの３０１７ＤＡもカウントする変数である）

【００６５】

例えば紙のチケットとしてＯＷＰ（１８Ａ）を生成する際にブロックチェーン上でＯＷＰの生成回数をインクリメントする機能がある場合には、ＯＷＰを含む紙のチケットのデータ（もしくはディスプレイの表示画面データ１５００Ａ）が不正に入場口にて使用され認証される前に通知を受け取ることもできる。その際にはＳＶＬｏｇ（端末３Ｄ）などにブロックチェーンを監視する処理部を３１１１Ｄを設け、サービスを提供するユーザーのトークン番号ＴＩＤＡのトークンのワンタイムパスワード生成回数の記録変数３０１７ＡＧ（呼び出し回数）、あるいは認証回数の記録変数３０１７ＡＡもしくは３０１７ＤＡの変化を検出し、トークンの持ち主であるユーザーにネットワークを経由した電子メールや通知アプリ、電話回線などで連絡する必要がある。電子メール以外にもワンタイムパスワード生成関数を利用したことを示すノンファンジブルトークンをトークン番号ＴＩＤＡの持ち主であるユーザー識別子Ａに送付してもよい。

【００６６】

ユーザーがメールアドレスを持たないときにはユーザー識別子Ａに向けワンタイムパスワードの生成又は認証があったことを示すＯＴＰトークンとは異なるノンファンジブルトークン（不正使用通知型トークン、通知葉書型トークン）を送付することもできる。この場合ノンファンジブルトークンは利用状態を示すレシートのように働く。（この不正利用通知型トークンは本発明のほかの実施形態や用途に利用できる。ウェブサイトログイン、紙もしくはＮＦＣタグによるチケット・有価紙葉、後述する暗号化データの復号用途。なおオフライン時の自動車や金庫などに内蔵された端末３Ｄは不正利用の通知は困難である。この場合は端末３Ｄが無線によるビーコンを発して周囲に知らせることは可能かもしれない。）

改札や施設の入場口の大人数かつ高速に提供するサービスにおいては、防犯カメラなどによる風貌の撮影に加え、サービス提供者が不正な入場者を引きとめ、個人番号カードや旅券などの身分証の提示や生年月日等の個人情報を確認し認証することも想定される。少人数を収容し行うイベントあるいはホテルなど宿泊施設の宿泊券として利用する場合は受付窓口で本人の名前等を記入したうえで１５００Ａや１８Ａや１９Ａを確認し認証してサービスの提供・利用ができるかもしれない。

【００６７】

＜レイティング及び看板情報＞

サーバ端末３Ｃを用いたサービスと同じく、紙もしくはＮＦＣタグを用いた有価紙葉とそれを認証する端末３Ｄを用いた認証システムにおいても、ユーザーの対象年齢等を示すため、ワンタイムパスワード生成トークンのコントラクトにはレイティング情報が３０２４Ａが記録される。またＯＴＰトークンのコントラクトの看板情報３０２４Ａも同様に設定される。例として自動車や船舶、重機といった乗物や設備・装置の利用者に求められる資格・免許情報といったレイティング情報であったり、映画館のレイティング情報等である。

また商品に１８Ａ、１９Ａを貼り付けるなどして添付する場合はその商品に基づいたレイティング情報となる。例えば１８Ａを貼り付けて酒類の流通を管理する場合は成人のみが飲用できるといったレイティング情報を記録してもよい。

【００６８】

４Ｃ．暗号化データおよびファイルの復号と閲覧

暗号化されたデータを本発明のブロックチェーンを用いたＯＴＰ認証システムを用いて復号するソフトウェアＣＲＨＮ（ソフトウェア４０３Ａ）を利用できる。ここでソフトウ

ェアＣＲＨＮは図４Ｂのソフトウェア４０３Ａである。図８Ｃに端末の接続図を示す。
暗号化されたファイルなどのデータ４０３４Ａ（図４Ｂの４０３４Ａ）を復号し閲覧する場合にはユーザーＵＰが利用するコンピュータＤＰ（図４Ａの端末４Ａ）を用いてサーバ端末３Ａにアクセスし端末４Ａの秘密鍵４０１Ａに割り当てられたＯＴＰトークンを用いてＢｎＴＯＴＰの生成と認証を行いＯＴＰ認証関数３０１８Ａの戻り値ＣＴＡＵ４０３１Ａを得て、戻り値４０３１Ａとあらかじめ設定されたパスワード値ＡＫＴＢ４０３２Ａとソフトウェア４０３Ａの内部で指定される秘密鍵ＣＲＫＹ４０３０２Ａ等とソフトウェア４０３Ａ計算方法に基づいてファイル暗号化及び復号を行える共通鍵ＴＴＫＹ４０３３Ａを生成しファイルの暗号化や復号を行うソフトウェア４０３Ａと前記ソフトウェア４０３Ａを用いた情報を閲覧、視聴、印刷出力等を行う暗号化データの復号と利用を行うことの出来る認証システムを本発明では利用できる。
なお復号にはＣＴＡＵ４０３１ＡとＡＫＴＢ４０３２Ａから算出されるＴＴＫＹ４０３３Ａのほかに、ＣＴＡＵ４０３１ＡとＡＫＴＢ４０３２Ａとソフトウェアに内蔵され難読化もしくは暗号化された鍵ＣＲＫＹ４０３０２Ａから算出されたＴＴＫＹ４０３３Ａを好ましくは用いる。
さらに前記鍵情報に加え、ＴＴＫＹ４０３３Ａの特定を困難にするようソフトウェアＣＲＨＮに記録されたプログラムに従って端末３Ａなどのブロックチェーンのノードとなる端末に記録されたコントラクト識別子ＡＰＫＹ４０３０１Ａのコントラクトから入手する鍵ＣＡＰＫＹ４０３０３Ａを用いてよいし、４０３３Ａの特定を困難にするよう処理を複雑にしそれらプログラムを難読化・暗号化してもよい。
この時、本発明は暗号化されたデータに含まれるコンテンツへのアクセスコントロール技術として機能する。

【００６９】

＜暗号化データの流通＞

暗号化データ４０３４ＡはＳＶＣＲＨＮｄｒｉｖｅというサーバ端末５Ｂからネットワーク２０を通じてコンピュータ端末４Ａに配信され記憶装置４０Ａに記憶される。サーバ端末５Ｂは実機のサーバでもよいし仮想のサーバ、仮想機械端末でもよい。クラウド型のデータストレージサービスでもよい。またバージョンを管理する機能を備え、暗号化データの更新歴や暗号化データのハッシュ値を記録し、ユーザーに表示できる機能を持っていてもよい。
端末５ＢはユーザーがＢＯＴＰ生成トークンによって復号できる暗号化データがあるか検索する機能を備えていてもよい。またトークンの発行者（発行者は個人、法人、出版社、ソフトウェア会社を想定）について、発行者が提示したキーワード（データの名前、作成時刻、キーワード、本等はその分類、レイティング情報）を用いてＯＴＰトークンのコントラクト識別子やそれに対応する暗号化データを検索出来る機能を備えてもよい。
電子商取引のウェブサイトまたはウェブアプリにおいて書籍や音声動画、ソフトウェアを顧客の端末４Ａの秘密鍵から計算されるユーザ識別子Ａに対しＯＴＰトークンを発行する形で顧客に販売することのできる機能を端末５Ｂに備えていてもよい。電子商取引を行う際に顧客ユーザがＯＴＰトークンとＯＴＰトークンに対応した暗号化データ検索機能、ＡＫＴＢ４０３２Ａの通知及び暗号化データのダウンロード機能、トークンを購入した場合の顧客の氏名やメールアドレス・ユーザー識別子・電話番号といったＯＴＰトークン購入者の個人情報及び連絡先情報を登録し保存するデータベースを備えていてもよい。端末５Ｂはユーザーの住所を記録し、信書の郵便配達などの形でＡＫＴＢ４０３２Ａの通知やＯＴＰトークン購入の事実を通知してもよい。

【００７０】

そして前記データベースに記録された顧客のユーザー氏名、メールアドレス・住所情報・ユーザー識別子といった連絡先情報を用いて、４０３２Ａと４０３１Ａと４０３０２Ａと４０３Ａで暗号化したファイル４０３４Ａを復号するのに必要な任意の鍵情報ＡＫＴＢ４０３２Ａについて、４０３２Ａと４０３１Ａと４０３０２Ａと４０３Ａで暗号化したフ

ファイル４０３４Ａと共に電子メールにて送付してもよい。
あるいは電子メールにて４０３２Ａと４０３１Ａと４０３０２Ａと４０３Ａで暗号化したファイル４０３４Ａを送付し、ＡＫＴＢ４０３２Ａはブロックチェーンや電子メールではない手段（４０３２Ａを記録した文章を信書として郵送配達する、電話番号のＳＭＳにてメッセージとして送付する・ファクシミリなどで送付する、あるいは秘密鍵４０１Ａを用いてＯＴＰトークンの存在するブロックチェーンとは異なるブロックチェーン基盤のブロックチェーンでＡＫＴＢ３０４２Ａを記述したトランザクションを受け取る等）にてＡＫＴＢ４０３２Ａをユーザー端末４Ａのユーザー ＵＰに伝達し、ＵＰは４Ａの４０３Ａに４０３２Ａを入力することでＯＴＰトークンが戻り値４０３１Ａとソフトウェア４０３Ａの鍵情報４０３０２Ａと４０３Ａの計算手順からＴＴＫＹ４０３Ａを算出し暗号化ファイル４０３４Ａを復号し復号された平文ファイル４０３５Ａを得て４０３５Ａのデータを閲覧や実行などして利用できる。

【００７１】

＜暗号化データを復号するトークンの流通制限機能＞

トークンの流通はトークンの管理者である権利者によって譲渡制限されることがある。トークンは実施例ではイーサリアムのＥＲＣ７２１規格によって他者への譲渡などが可能であるが、譲渡する際に権利者がその譲渡機能（送信関数３０４０Ａ）の実行を制御する変数や処理３０４１Ａが追加される。本発明のＯＴＰトークンは譲渡されないインターネットバンキング用のＴＯＴＰトークンをブロックチェーン上で利用する過程で発明されたものであって、基本的には譲渡を制限する機能が搭載されることを特徴とする。ＯＴＰトークンに対応したサービスの提供者あるいはコンテンツの提供者が本発明のＯＴＰトークンの異なるユーザー識別子間での譲渡を許可しない場合にはＯＴＰトークンのコントラクトの譲渡制限用変数および関連関数３０４１Ａは送信関数３０４０Ａの実行を阻止する変数の値をとる。

ＯＴＰトークンに対応したデータやファイルのコンテンツの権利者がコントラクトの管理者であるとき（又はコントラクトの管理を権利者がコントラクト管理者に委託しているとき）コントラクトの送信関数３０４０Ａの実行を停止させている状態から実行可能な状態になるようコントラクトの変数の値３０４１Ａを変更した場合は、異なるユーザー識別子のユーザー間で譲渡可能となる。

【００７２】

ＯＴＰトークンの譲渡の例を示す。ユーザーＵＰ（端末４Ａの利用者）とユーザーＵＢ（端末１Ｂの利用者）がネットワーク２０とサーバーＰ（サーバ端末３Ａ）を介してブロックチェーン上でＯＴＰトークンの情報をやり取りすることもできる。ＵＰからＵＢにＯＴＰトークンを送信関数３０４０Ａを用いて譲渡することもできる。

ＵＰからＯＴＰを送信されたＵＢは（実際には３Ａにて４Ａから秘密鍵４０１Ａを用いてアクセスを受けＯＴＰトークンのコントラクトにおけるＯＴＰトークンとユーザー識別子の対応関係を記したデータベースまたは台帳３０１４Ａについて３０４０Ａによりユーザ ＵＡからＵＢに所有者情報を書換えたもの）、端末５Ｂから暗号化ファイルをダウンロードするか、トークンの持ち主であったＵＰが端末１Ａに持つ暗号化データを複製して利用するか、ネットワーク上に流通している暗号化ファイルを入手して暗号化データの復号が可能である。

ここで暗号化ファイルの暗号化時にＡＫＴＢ４０３２Ａが利用されている場合はユーザーＵＰから４０３２Ａを入手する必要がある。ＡＫＴＢ４０３２Ａが設定されていないコンテンツでは暗号化ファイル４０３４ＡとＯＴＰトークンの認証で得られるＣＴＡＵ４０３１Ａと、ソフトウェア４０３Ａとソフトウェア内部の秘密鍵４０３０２Ａで復号できる。ユーザーＵＢがユーザーＵＰからＯＴＰトークンの譲渡とＡＫＴＢの通知、暗号化データと暗号データを閲覧できるソフトウェア４０３Ａを入手することでＵＰが閲覧していたコンテンツデータをＵＢが閲覧できるようになるとともにその閲覧権もしくは所有権を手に入れることができる。

本発明の実施例では暗号化データの復号にはＣＴＡＵ４０３１Ａ、ＡＫＴＢ４０３２Ａ

、閲覧ソフトウェア４０３Ａ内部の秘密鍵ＣＲＫＹ４０３０２Ａ、ソフトウェア４０３Ａなどを基にファイル暗号化及び復号鍵ＴＴＫＹ４０３３Ａを生成出来るとき、ＴＴＫＹ４０３３Ａで暗号化されたファイルの復号を行える。

【００７３】

本発明の譲渡制限機能を用いたＯＴＰトークンの譲渡機能は暗号化データの復号用トークンに限らず、本発明のすべてのＯＴＰ生成関数を持つコントラクトに帰属するＯＴＰトークンに用いる事ができ、図８Ａに記載の端末３Ｃのウェブサイトのログイン用ＯＴＰトークン、図８Ｂに記載の紙やＮＦＣタグ式チケットや有価紙葉及び解錠等の鍵を作成するパスワードＯＷＰの生成を行うＯＷＰトークンに用いることができる。

コントラクトのプログラム上ではＯＴＰトークンは譲渡可能であるが、ＯＴＰトークンが対応するサービスによってはサービスの権利者による利用制限や、国内国外の法や規制を受けることが想定される。譲渡制限を行う際の３０４１Ａの変更はコントラクト管理者が行う。

【００７４】

＜暗号化データのバージョン管理＞

ブロックサイズやトランザクションのデータ上限値が極めて大きく取れるブロックチェーン基盤においてそのブロックデータにトランザクションにデータやファイルを添付して分散型台帳へ記録させるいわゆるブロックチェーン型ストレージを暗号化ファイル配信サーバ端末５Ｂに備えてもよい。ブロックチェーンに限らずバージョン管理ができる改ざん困難なストレージステムでもよい。（端末５Ｂに含まれると好ましい機能を実施する既存の技術及びサービスの具体例として、米国Ｇｉｔｈｕｂ．　Ｉｎｃ．、ギットハブ・ジャパン合同会社のＧｉｔｈｕｂといったソフトウェア開発及びバージョン管理を行うプラットフォームなどが挙げられる）。

端末５Ｂはユーザー端末のアクセスを受けユーザー端末の求める検索のキー情報に応じて対応した暗号化ファイルやＯＴＰトークンを表示し、そのＯＴＰトークンを電子商取引機能により、あるコントラクト識別子のＯＴＰトークンを発行する発行送付宛先のユーザー識別子を端末５Ｂや該当するコントラクト識別子のコントラクト管理者端末１Ｃに提示し、購入代金などの決済などを行いＯＴＰトークンの購入とＯＴＰトークン購入者のユーザ識別子に対するトークン発行の指示、ＡＫＴＢ４０３２Ａが必要な場合にはＡＫＴＢ４０３２Ａを暗号化時に利用して暗号化ファイル４０３４Ａを作成し配布してもよい。

前記の４０３４Ａ配布する際にユーザーの電子メールにＡＫＴＢ４０３２Ａとコンテンツの暗号化ファイルを添付して送付してもよい。もしくはＡＫＴＢ４０３４Ａを電子メールにてユーザーに通知し、それに対応する暗号化ファイルは５Ｂなどの端末にアクセスできるダウンロード専用のＵＲＩからダウンロードするようにしてもよく、ＵＲＩは電子メールに記述するか５Ｂがログイン機能などを備えた会員サイトでもある場合はログイン後のユーザー専用表示画面にてＵＲＩを表示してユーザーに伝達してもよい。

【００７５】

改ざんが検知もしくはバージョン管理が行えるオンラインストレージにおいて、暗号化データ４０３４Ａが大衆に向け公開し販売している書籍であり、書籍のデータを改訂し、異なる版を流通させる必要が出るかもしれない。この場合、改訂前の版のデータを改ざんされないよう残しつつ、改訂版を暗号化されたデータとしてバージョン管理機能のある５Ｂにアップロードし流通させることができる。

このとき改訂版の新しい暗号化データを既存の版の古い暗号化ファイルを復号できる旧版のＯＴＰトークンで復号できる。これは例えば書籍ではなくコンピュータゲームなどで不具合のあるプログラムなどがあったときにそれを改善するために改訂版を流通させたいときに旧版のＯＴＰトークンにて復号できることが好ましく、暗号化されたコンピュータソフトウェアのデータを復号する用途での利用を想定する。この場合は新しい版とふるい版では同一のコントラクト識別子のままである。

あるいは、新しい版には古い版とは別の新しい版のトークンで復号できるよう暗号化して暗号化データを流通させつつ、ふるい版のトークンを権利者が販売することもできる。

これは例えば紙の書籍において、印刷され流通したふるい版の書籍と改訂された新しい版の書籍の双方が書店や古書店でモノとして販売されていうことに対応する。新しい版のトークンとふるい版のトークンには異なるコントラクト識別子のＯＴＰトークンのコントラクトがデプロイされユーザに通知される。新しい版のＯＴＰトークンを購入するかどうかは消費者の判断による。（コンピュータソフトウェアにおいても版ごとにＯＴＰトークンのコントラクトをデプロイしていくこともできる）

【００７６】

＜コンテンツのレイティング＞

暗号化データの情報を閲覧するのに適した年齢等を示すため、ワンタイムパスワード生成トークンのコントラクトにはそのトークンで復号を解除できる暗号化ファイルのコンテンツのレイティング情報３０２４Ａが記録される。図４Ｂの４０３５１Ａや４０３５２Ａにレイティングが記録されてもよい。

ブロックチェーン上にコンテンツのレイティングが記録され他者がそのレイティングをブロックチェーンに直接アクセスするか５Ｂや３Ｆといったサーバ端末から検索して閲覧しトークンの購入等を検討できる。

＜コンテンツの証明書＞

暗号化データの暗号化を復号したとき、その平文に悪意のあるプログラムが含まれていない事を示す第三者からの証明書があると好ましい。図４Ｂの４０３５１Ａや４０３５２Ａに記載の情報である。

これはコンテンツのレイティングとも関連し、コンテンツの平文データを第三者に検閲させそのプログラムの動作に問題が無いか調査される必要があるかもしれない。

【００７７】

＜コンテンツの閲覧実行環境＞

コンテンツの証明書を用いても、第三者機関が意図せず悪意のあるプログラムの存在を見逃してコンテンツの証明書（図４Ｂの４０３５１Ａや４０３５２Ａ）を発行してしまうこともあるかもしれない。そこでソフトウェア４０３Ａの実行環境は仮想機械環境の中で実行されることが好ましいかもしれない。

【００７８】

＜ある時刻に複数の環境からの閲覧の検知する機能（不正アクセス検知機能）＞

本発明ではこのソフトウェアＣＲＨＮにおいて暗号化コンテンツを復号し閲覧したとき、またはソフトウェアＣＲＨＮを閲覧したときに、

広告サーバーＣＲＨＮｃｍ（図５Ａのサーバ端末５Ａ）への接続を行うプログラムが実行され、端末５Ａから広告が配信されるとともにコンテンツの閲覧またはソフトウェアを実行したユーザの

ＩＰアドレス（ＩＰアドレスのハッシュ化または加工した値）、

位置情報（位置情報をハッシュ化または加工した値）、コンピュータのデバイス情報（またはそのハッシュ値）、端末のセンサ値（またはそのハッシュ値）、

そしてトークン番号とユーザー識別子を図６Ｘのようなデータとして端末５Ａに記録し、あるトークン番号やユーザー識別子に対して、

異なるＩＰアドレス、異なる位置情報、異なる装置ＩＤ、異なる端末付属の入力装置のセンサ情報にてアクセスしているかどうかを随時判断する処理部を備えることができる。

ここでコンピュータのデバイス情報、コンピュータの装置ＩＤについては、デバイスＩＤなどのコンピュータ製造ＩＤやオペレーティングソフトウェアのＩＤ、ウェブブラウザのＩＤに加えて、端末４Ａに搭載された加速度センサーや磁気センサー、圧力センサー、温度センサーなどの測定値や測定値をハッシュ化したものを用いてもよい。

これは広告サーバーが簡易なコンテンツの不正利用を監視するサーバーとして利用されることを想定している。しかしソフトウェア４０３Ａや暗号化コンテンツをの配布元である権利者がコンテンツの不正利用監視機能を要望する場合に限り利用される。

ソフトウェア４０３Ａを閲覧したときに、サーバ端末５Ａへの接続を行うプログラムを実行しなくとも本発明のＯＴＰ認証システムにより暗号化データの復号ができる。そして

実施形態において、本発明のソフトウェア４０３Ａの権利者や暗号化データの平文データの権利者が５Ａへの接続を行うプログラムを記録させ、ソフトウェア４０３Ａやコンテンツの利用者が同意する場合にサーバ端末５Ａへの接続を行うプログラムが実行されうる。（ここで権利者とは主にソフトウェアやコンテンツの著作権等利者である。平文データは著作権を初めとする知的財産権の観点から保護される。また法人の営業秘密等の機密情報である場合は知的財産権として保護される。個人の創作した平文データは著作権にて保護される。）

【００７９】

また５Ａを用いた広告機能は例えば発売前の製品の設計図などの機密情報を本発明のソフトウェアにて暗号化、復号し社内文章の暗号化ツールとして扱うといった場合においては必要とされない恐れがあり、前記社団に本ソフトウェアを提供する場合には広告の表示機能や広告配信サーバを用いたコンテンツの不正利用監視機能を利用しない形態も考えられうる。　個人が趣味等で利用する場合には広告表示機能と広告によるコンテンツの不正利用監視機能を権利者が搭載でき、個人や法人のビジネス用途ではその広告機能を搭載せず本発明のソフトウェアと装置として利用できる。

【００８０】

また端末４ＡのソフトウェアＣＲＨＮ（４０３Ａ）によりデータやファイルは復号され実行されその結果が出力装置であるディスプレイ画面４５０Ａに表示され、音声情報が含まれていればスピーカー４５１Ａで音として出力する。

ソフトウェアＣＲＨＮの表示画面でソフトウェア的に画像をスクリーンキャプチャされにくくしたり（この場合はディスプレイ４５０Ａを銀塩又はデジタルカメラにより複写される場合は複写できる）、コンテンツとなるファイルやソフトウェア側からプリンターによる印刷を許可しない設定にすることができる。コンテンツの権利者の要請によっては印刷を不可能にすることも可能にすることもできる。コンテンツのプレイヤー画面に常に閲覧者のユーザー識別子を表示できる。

【００８１】

＜オフライン時におけるデータの閲覧＞

本発明では災害などでオフラインとなり、インターネットワークから切断され隔離された場合についても、端末４Ａのソフトウェア４０３Ａを用いて閲覧したいデータがあることが考えられえる。たとえば災害において避難経路、災害に役立つ百科事典などの書籍のファイルを利用したいことも想定される。ブロックチェーンそのものは世界中に分散可能なサーバによるデータベースであり、局所的な災害に対しては耐性がある。しかし災害の被災者のデバイスはネットワークに接続できず手元にあるソフトウェア４０３Ａはブロックチェーンに接続できないので暗号化されたファイルの復号ができなくなることが想定された。

そこで本発明ではオンライン時、災害が起きる前に予めソフトウェア４０３Ａでファイルの復号を行ったときに、閲覧済みの証明書データ４０３６Ａ（図４Ｂに記載の４０３６Ａ。ブックマークデータ、本文章中ではＯＦＢＫＭＫ）を作成し、その証明書データ内部に記録されたユーザー秘密鍵ＰＲＶＰ（図４Ｂの４０１Ａ）にて暗号化された鍵情報を復号して閲覧する鍵として利用する。この場合も、本発明はコンテンツへのアクセスコントロール技術として機能する。

【００８２】

＜オフライン時に利用する閲覧済みの証明書データ＞

本発明の実施例では、

まずファイルの暗号化及び復号のための鍵情報ＴＴＫＹ４０３３Ａを算出し、ユーザーの秘密鍵４０１Ａまたはそれに基づく鍵情報を用いてＴＴＫＹ４０３３Ａを暗号化しＣＴＴＫＹ４０３６１Ａとし、４０３６１Ａをソフトウェア４０３Ａに内蔵する秘密鍵４０３０２Ａを用いて暗号化しＡＣＴＴＫＹ４０３６０Ａとする。

次に端末４ＡがＯＴＰ認証してデータを復号し閲覧できた時点でのブロック番号等ブロックチェーン情報やワンタイムパスワード生成および認証コントラクトのコントラクト識別

子を一つのオブジェクトデータまたはファイルとしてまとめ４０３６２Ａとする。
次に秘密鍵４０３０２ＡをＨＭＡＣのキー情報とし、４０３６０Ａと４０３６２Ａを連結したデータをＨＭＡＣのメッセージとして、ＨＭＡＣによりＭＡＣ値４０３６３Ａを求める。
そして４０３６０Ａと４０３６２Ａと４０３６３Ａを連結したデータを閲覧済みの証明書データＯＦＢＫＭＫ４０３６Ａとして利用する。
【００８３】
＜オフライン時の閲覧＞
閲覧済みの証明書データＯＦＢＫＭＫ４０３６Ａ、ユーザの秘密鍵４０１Ａ、ソフトウェア４０３Ａ内部のキー情報４０３０２Ａを用いて復号しＴＴＫＹ４０３３Ａを得る。
具体的には、ソフトウェア４０３ＡはＯＦＢＫＭＫ４０３６Ａに記述されたＡＣＴＴＫＹ４０３６０Ａを４０３０２Ａを用いて復号しＣＴＴＫＹ４０３６１Ａを得る。そしてＣＴＴＫＹ４０３６１Ａを４０１Ａを用いて復号し、ＴＴＫＹ４０３３Ａを得て、ＴＴＫＹを用いて暗号化されたデータやファイルを復号し閲覧可能とする。４０３６Ａの内部にある情報の暗号化は共通鍵暗号化と公開鍵暗号化等の暗号化が利用されうるが好ましくは共通鍵暗号化を用いてもよい。
ここで災害時において閲覧に制限は不要かもしれないが、ネットワークが切断された時に切断の理由が災害なのかユーザー都合なのか区別がつかない事と、災害時においても閲覧制限をしたいファイルがあるかもしれないので閲覧時間などに制限を設ける機能をソフトウェア４０３Ａが備えていてもよい。
【００８４】
ユーザーの中には端末４Ａがネットワーク２０から切断されたオフライン時の４０３６Ａを用いた閲覧機能を悪用しようとする人もいるかもしれない。そこで権利者のコンテンツを守るうえで閲覧済みの証明書データをもちいてオフラインで閲覧する利用者に利用制限をかけることが好ましい時がある。（なおコンテンツの権利者の判断では閲覧制限を設けない４０３６Ａの利用形態も考えられる。）
その具体的な対策例及び実施例として、ソフトウェア４０３Ａはオフライン時の利用において４０３Ａがインストールされたコンピュータやスマートフォンの時刻情報と証明書データＯＦＢＫＭＫ４０３６Ａの認証およびコンテンツを閲覧できた時刻を検出し、４０３６Ａの時刻が現在のスマートフォン等コンピュータ端末の時刻よりも過去にあることを確認してから、４０３６Ａの情報に含まれる情報を復号して４０３３Ａを得て、暗号化データやファイル４０３４Ａを復号し、４０３４Ａを４０３６Ａを用いて復号して閲覧などを行った時刻（４０３６Ａで閲覧を始めた現在時刻）を記録し、前記４０３６Ａで閲覧を始めた現在時刻よりある指定時刻だけ未来にある時刻まで間に限り閲覧を許可する。ある指定時刻だけ時間が経過した際には閲覧を停止する処理を行ったりソフトウェア４０３Ａを停止させ、平文データ４０３５Ａの利用を停止する。
【００８５】
ここでコンピュータ端末４Ａの内、スマートフォン型の端末４Ａは多くが位置情報の測位用に全球測位衛星システムＧＮＳＳからの無線信号受信装置４２２Ａもしくは４２３Ａを備え、時刻が更新されるのでこの機能を提供しやすい。ＧＮＳＳからの信号には時刻情報が含まれる。ＧＮＳＳなど時刻情報を得る手段を取り外し困難な状態で内蔵していないコンピュータでは、オフラインでコンピュータのＢＩＯＳ（Basic Input Output System）などで時刻を本来の時刻と異なる値に設定し、ソフトウェア４０３Ａが正しい現在時刻を取得するのを妨げ、閲覧を停止すべき時刻になってもソフトウェア４０３Ａが閲覧を許してしまう恐れがある。
ソフトウェア４０３Ａにおいて閲覧済みの証明書データＯＦＢＫＭＫ４０３６Ａを用いて閲覧するにはＮＩＴＺ（Ｎｅｔｗｏｒｋ　ＩＤ　ａｎｄ　Ｔｉｍｅ　Ｚｏｎｅ、ネットワークIDおよびタイムゾーン）、ＪＪＹ、ＧＮＳＳなどの災害時においても時刻を伝える放送局から受信できることが好ましい。またその時刻情報を受信できる装置が取り外し困難であることが好ましい。例えば端末の無線通信装置４２２Ａもしくは放送受信装置４２

３Ａと制御演算部４１Ａおよび４３ＡにあるＣＰＵ（Central Processing Unit）を金属製のシールドで封印し、シールドに無線機器としての認証番号（日本国の無線機器の工事設計認証、アメリカ合衆国の連邦通信委員会ＦＣＣの無線機器の認証ＩＤなど）を刻印するしてもよいし、半導体パッケージとして封止してもよいし、透明な接着剤などで内部の部品が視認できる形で封止してもよい。

４１Ａや４３Ａを含むＣＰＵとＧＮＳＳまたはＪＪＹまたはＮＩＴＺの受信装置４２２Ａもしくは４２３Ａを同じ半導体パッケージもしくは同じ半導体基板に搭載し、そのＣＰＵやシステムオンチップ（ＳｏＣ）となった装置を端末に制御部や制御演算部として搭載することが好ましい。（２０２０年時点で販売されたスマートフォンやタブレット型端末に搭載されたＳｏＣチップの中にはＣＰＵとＮＩＴＺを送信する無線通信局へのモデムとＧＮＳＳ（米国ＧＰＳや日本国ＱＺＳＳ）の無線信号を受信するモデムを内蔵したものが存在している。例として米国クアルコム社などのＳｏＣ。）
ＳｏＣでは一つの半導体チップであるが、ＳＩＰ（System in Package）という複数のＩＣチップを１つのパッケージに搭載し封止などを行った半導体部品でもよい。

また携帯電話及びスマートフォンなどの基地局を用いるＮＩＴＺ（Network Identity and Time Zone、ネットワークIDおよびタイムゾーン）は災害時に携帯電話用基地局が被災し、停止すると機能しない恐れもあるので、被災地から離れた地上の無線局の時刻データ（日本国ではＪＪＹ等）やＧＮＳＳ等の宇宙空間にある無線局の時刻データを用いて時刻補正できることが好ましい。
放送を用いるシステムの内ＧＮＳＳやＪＪＹの他、衛星放送により時刻を取得することも可能かもしれない。静止軌道にある気象観測衛星や放送衛星から送信された時刻情報がユーザー端末にて受信される事を想定する。月面などに時刻を放送する無線局５Ｃがあってもよい。

【００８６】

ユーザー端末の記憶装置のうちプログラム４０３Ａの秘密鍵情報を４０３Ａの実行時に記録する揮発性のＲＡＭや、ユーザーの秘密鍵情報を記録できるＲＯＭもしくは不揮発性メモリＮＶＲＡＭをＣＰＵと共にＳｏＣ等に搭載しパッケージとして封止してよい。これは端末を分解し、端末を構成する部品をはんだなどで接合した部分などから記憶装置の信号のやり取りを電気信号の測定装置を用いて測定し４０３Ａの秘密鍵などを実行する場合に読み取られかねず、部品の端子部の電気信号の測定とリバースエンジニアリングによる攻撃を防ぐことを意図する。記憶装置と制御演算装置の間の接続経路でのリバースエンジニアリングを防ぐために本発明で用いる記憶部と処理部を同じ基板形成しもしくは同じパッケージの中に封止することが好ましい。（この要件は端末１Ａや端末４Ａや端末３Ｄにもかかわる。）

記憶装置と制御装置の信号処理部に対するアクセスを行う事が困難にして、アクセスを行うと端末の記憶装置と制御装置が破壊される恐れがあることが好ましい。端末の制御部と記憶部を封止樹脂や接着材で封止してもよいし、端末を分解して記憶部や制御部へできないように封止樹脂や接着剤で封じてもよい。
ただし、前記記憶装置の内、ソフトウェアの動作に必要な情報の容量に該当する記憶装置を封止できればよく、端末の処理や利便性の向上のために例えば暗号化データ４０３４Ａを収録できる記憶容量を増やすために不揮発性の半導体メモリを増設してもよい。外部記憶装置としてハードディスクドライブなど磁気ディスクや光ディスクを用いてもよい。また４０３４Ａを記録した記憶装置は端末４Ａから取り外して他者に手渡しして配布できてもよい。

【００８７】

＜コンテンツの印刷、複写の制限と許可＞

暗号化データおよびファイル等のコンテンツ権利者に許可に応じて、コンテンツ権利者が暗号データ４０３４Ａから復号した平文データ４０３５Ａや４０３Ａに許可を行う旨の情報を記載し、かつ個人使用に限り、４０３Ａはコンテンツを出力装置のプリンターを用いて印刷できる。４０３Ａは印刷する際に印刷時に各ページごとに印刷を行ったユーザー

識別子やトークン番号、印刷時刻、コンテンツの名称、コントラクト識別子、印刷時のブロック番号とＴＯＴＰ等をタイムスタンプのように印字することができる。これは印刷された文章の印刷時刻や印刷者を確認するためである。印刷者はユーザ識別子で表される。

【００８８】

端末４Ａのディスプレイ画面に表示された暗号化データを復号したコンテンツは銀塩カメラ・フイルムカメラ・撮像素子を用いたデジタルカメラ、デジタルカメラを搭載したスマートフォンなど端末を用いて画像や動画として複写することができるかもしれない。

そこで端末４Ａのディスプレイ画面に表示された暗号化データを復号したコンテンツは銀塩カメラ・撮像素子をデジタルカメラを搭載したスマートフォンなど端末を用いて画像や動画として複写することを簡易的に防ぐ場合にはヘッドマウントディスプレイ４５３Ａ（頭部装着ディスプレイ４５３Ａ）を使用する。なお本発明は必ずヘッドマウントディスプレイ４５３Ａを用いるわけではなく従来のデスクトップ型端末やラップトップ及びノート型端末そして携帯電話機やスマートフォン端末に搭載されるディスプレイ４５０Ａを用いてもよい。

ここでヘッドマウントディスプレイ４５３Ａを装着したときに顔認証や虹彩認証、耳の構造に由来する認証、照度センサまたは光センサ、体温分布のサーモグラフィ画像などによる生体認証機能をヘッドマウントディスプレイ４５３Ａのセンサ４５３０Ａを利用して行ってもよい。前記認証機能では４５３Ａを実在する生体が装着しているかどうかを確認することが第一の目的であり、それに付属して個人の生体情報を取得して生体認証を行うことにつなげることもできる。

【００８９】

ソフトウェア４０３Ａは復号したデータを出力する出力装置４５Ａを限定してよい。具体的にはディスプレイ画面を銀塩カメラやデジタルカメラを用いて画像や動画として複写することを簡易的に防ぐ場合には４５３Ａを用いる。一方で複数人とディスプレイ画面のコンテンツを共有して視聴し、その場面においてディスプレイ画面の撮影を許容する場合には４５０Ａを用いるという形である。これら出力の方法を限定することは暗号データに含まれるコンテンツの権利者が決定でき、暗号データを復号した際の平文データに出力方法がプログラム等で記載され、そのプログラムを実行して閲覧する際に復号されたデータを出力する装置を限定する。ヘッドマウントディスプレイ４５３Ａやディスプレイ４５０Ａのようなディスプレイ装置・表示装置、４５２Ａのプリンター、４５１Ａのスピーカーを例として、出力装置ごとに復号のデータ・ファイル・コンテンツの出力は制限されうる。

【００９０】

４５３Ａを用いる場合であっても画面を複製することが必要な場合はソフトウェア４０３Ａの製造者が別途４５３Ａのほかに４５０Ａに出力させることもある。例えば暗号化データの内容にかかわる紛争の解決のための証拠取得などの手段で複製する場合は４５３Ａで出力することを指定していても４５０Ａで出力できるようソフトウェアの設定情報を捜査機関に開示し閲覧できるようにする。例えヘッドマウントディスプレイ４５３Ａを用いて複写を制限する場合でも、要請に応じてソフトウェア４０３Ａの提供者は、画面の複写できる版の（バージョンの）４０３Ａを紛争の起きている人々の解決に役立てるよう提供できる。

例えばディスプレイに表示する情報が法令等に反している情報（例として肖像権を侵害している情報など）でその情報による被害者がいる場合に、捜査当局や弁護士等へ情報を提供する際に４０３Ａの内ヘッドマウントディスプレイ４５３Ａのみで利用できるとしたデータを通常のディスプレイ４５０Ａで表示し紛争の解決のために情報を共有できるようにしてもよい。

【００９１】

情報を保持するという観点からはオフラインであっても閲覧済みの証明書データを持つユーザーはその個人利用の範囲内でデータを紙等に記録できることが好ましいかもしれない。本発明で用いるコンピュータや記憶装置そしてブロックチェーン等の技術は、紙や粘

土板及び石板といった過去に発明された記録手段のように長い実績を持った情報記録媒体ではないので、本発明を用いた情報のうち情報の権利者が望む場合には本発明で用いたデータやトークンの所有に関する情報を紙などに記録出来ることが好ましい。音楽映像データやソフトウェアデータもまた平文ファイルで磁気テープや磁気ディスク等の記憶装置に記憶することができるほうが情報が残り続けるかもしれない。

本発明は実際の紙の保存年月と同じくらいの年月、すなわち１００年を超え数世紀以上機能すると仮定し設計される。本発明のソフトウェアは今ある現代の文化や生活のデータを保持する観点を持って、データの所有、コンテンツ権利者保護、情報の記録を重視し設計を行っており、情報を後世に伝えることを考えている。

本発明では暗号化ファイルの形で世界中にファイルを配布することを可能とし、ＯＴＰトークンという鍵を用いて暗号化データを復号するという情報の流通形態を取るが、暗号化データの配布元である権利者は暗号化データの原本である平文のデータを責任を持って保存することが好ましい。世界中に販売した書籍のデータがあるからといって原本の保全をしなくなってしまうことを発明者は意図していない。

また発行したＯＴＰトークンとそれに対応した暗号データ４０３４Ａやソフトウェア４０３ＡとＡＫＴＢ４０３２Ａなどの復号の鍵となる情報をまとめて書籍や映像音声情報として図書館などに収録することで本発明の手段による書籍が長い年月にわたり保存され易くするかもしれない。

【００９２】

４Ｔ．放送での利用（双方向でない暗号化データの流通）

図８Ｃの応用として暗号化データ放送の用途がある。図８Ｄに端末の接続図を示す。図８Ｄ示すように、暗号化されたデータは1対複数の無線放送によって放送される音声動画の暗号化されたデータでもよく、ラジオ放送やテレビ放送（テレビジョン放送）のデータを暗号化し放送局５Ｃ（図８Ｄの５Ｃ）から送信し、ユーザーＵＰの端末１Ａに内蔵された無線受信機４２３Ａにより受信した暗号化データを復号し音声や映像を視聴することにも応用できる。

テレビ放送などによるコンテンツの配信は、図８Ｃに示すコンピュータとコンピュータネットワークによる双方向通信かつオンデマンド配信でのデータおよびファイルでのコンテンツのやり取りを、図８Ｄに示す放送局サーバ端末５Ｃと複数の受信機端末４Ａ（受信機付きテレビジョン）でのライブ放送・ライブ配信としたものである。

ここで複数の受信機４Ａ（放送受信機付きテレビジョン型コンピュータ端末４Ａ）は本発明ではインターネットに接続でき、本発明のワンタイムパスワードによる認証システムと暗号化コンテンツの閲覧機能を備えると好ましい。受信機がインターネットおよびグローバルなブロックチェーンに接続できない場合には、受信機に内蔵されたシークレットキー情報とは別に、放送局が放送データに時刻情報及びブロック番号Ｂｎやワンタイムパスワード認証、コンテンツの復号に必要なキー情報の一部を送信する必要がある。

この方式では複数のユーザーに対し一つの放送局からデータを送信できる一対複数のデータ送信が可能である。通信経路となる電波を独自に確保できていればスマートフォンやコンピュータネットワーク２０の混雑などを気にせず情報を公衆に伝達でき、新聞や官報や教科書籍データ等の公共性のあるデータ情報や、音声や動画などを送付するには利点がある。（既存の日本国の衛星及び地上波のデジタル放送においてもＩＣカードを利用し、共通鍵暗号化を用いたアクセスコントロールが行われている。）

【００９３】

本発明のＯＴＰトークンを放送の視聴権として用い放送データの暗号化を復号して閲覧する方式を応用した場合、ＩＣカードがない場合でも秘密鍵と、秘密鍵に割り当てられたトークンを用いてアクセスコントロールが可能になる。ＩＣカードの再交付をしなくともトークンの追加交付・追加発行を行い、コントラクト側で暗号化に利用するキー情報を変更できる。

ただし暗号化されたデータ（コンテンツ）は放送局から1対複数の形でデータ送信されるが、ＯＴＰの取得と認証、認証関数の戻り値の取得はインターネットワーク２０を通じ

て行う。従ってこの方式の放送データ視聴用端末４Ａは放送局からの無線受信装置とインターネットとの通信装置の両方を備えることが望ましい。本発明では通信機能を持つテレビジョン端末４Ａもしくはスマートフォン端末４Ａもしくはタブレット型の携帯端末４Ａについて図８Ｄに示す端末４Ａのような実施形態を想定する。

【００９４】

端末４Ａをスマートフォンなど携帯端末に限定せず、ヒトが携帯できないような大画面のテレビジョン端末４Ａであることも想定される。前記テレビジョン型端末４Ａを用いる場合は外部記録装置４６Ａに秘密鍵を記録し４０１Ａとして利用させてもよい。この実施形態は既存のアクセスコントロール機能を備えたＩＣカード読み取り装置つきのテレビジョン装置と同様である。

もしくはテレビジョン端末４Ａの記憶装置４０に秘密鍵４０１Ａを記録させ利用させることもできる。しかしこの場合は端末４Ａを廃棄もしくは譲渡する際に秘密鍵４０１Ａの情報を別途異なる記憶装置に記録した後、４０１Ａを４０Ａから消去することが必要かもしれない。本発明ではハードウェアウォレットやＩＣカード（個人番号カードのような秘密鍵を持つＩＣカード・ＮＦＣカード）のような秘密鍵を保存する記憶装置を用いずに端末１Ａや端末４Ａに記憶した秘密鍵がある場合には、端末の廃棄時もしくは譲渡時に秘密鍵を新しい端末や記録媒体に複製した後に端末の記憶装置のデータを消去することが必要である。

【００９５】

＜ネットワークに接続されていない受信端末について＞

図８Ｄにおいて端末４Ａがインターネットに接続されていないが、端末４Ａにはスマートフォン型端末１Ａと連携する無線通信装置があるとき、端末４Ａは端末１Ａを通じてインターネット２０に接続してもよい。

【００９６】

インターネットへの接続手段を備えておらず、またインターネットに接続できる端末とも通信できない場合、次のＡとＢの方法がある。

Ａ．図８Ｂで示したＯＷＰを用いる方法を用いる場合。

例として端末１ＡにてＯＷＰを生成するＯＴＰトークンを取得し、前記ＯＴＰトークン用いて端末３ＡにアクセスしながらパスワードＯＷＰを生成する。生成したパスワードＯＷＰとトークン番号とユーザー識別子をテレビジョン端末４Ａに入力するかもしくはそのパスワードの記録されたＮＦＣタグ１９Ａを４２０Ａに読み取らせ、認証ができたときは、端末４Ａの認証関数に記録された戻り値ＣＴＡＵを用いて放送された暗号データの復号を行い、復号できた場合にはコンテンツを視聴させる。

Ｂ．図８Ｂに類似し、放送データにシード値が含まれており、そのシード値に変化に応じて復号パスワードを生成するとき

Ａに示した例では復号を行うＴＴＫＹ４０３３Ａの元になる情報はＣＴＡＵ４０３１Ａのみとなる。そこでＡＫＴＢ４０３２Ａに該当する情報を端末４Ａに入力し、さらにデータ放送中の暗号データの中にＴＴＫＹ４０３３Ａの算出に利用する鍵を放送してもよい。放送される鍵情報は４０３Ａのみが解読できるよう秘匿化もしくは暗号化されていてもよい。

【００９７】

無線受信装置のみ備えるテレビジョン端末４Ａ等の場合には、放送局５Ｃの送信情報に時刻情報、あるいは５Ｃが３Ａ等から読み取ったブロック番号Ｂｎを付与し、テレビジョン端末４Ａ側でＢｎを受信させ、端末４Ａが備える認証関数と認証関数に用いる内部シークレット変数からＯＴＰの生成と認証、暗号化データの復号に必要な鍵の生成を行い、放送された暗号化データを随時復号してもよい。放送データに放送データ内部の暗号化コンテンツを復号する鍵の情報の一部が含まれていても良い。

【００９８】

放送されたデータは暗号化された形で受信機（テレビジョン受信機）の記憶装置（テレビジョン装置の録画端末に該当）に記録でき、再度視聴したい場合には復号に必要なＯＴ

Ｐトークンによる認証後の戻値ＣＴＡＵの取得を行い、ＡＫＴＢなどの情報を入力し、復号用の鍵ＴＴＫＹ４０３３Ａの算出を行い、４０３３Ａを使い録画録音された暗号化データのコンテンツを復号して閲覧できる。

【００９９】

＜テレビジョン型コンピュータ、テレビジョン型ゲーム機、テレビジョンと接続したコンピュータおよびゲーム機＞

ここで受信機端末４Ａがテレビジョン装置である場合、家庭などで家族に情報を共有し娯楽などに利用できる装置である。大画面であるテレビジョン装置はヘッドマウントディスプレイ４５３Ａと比べ複数人と情報を共有するのに適する。インターネット接続できるテレビジョン視聴機能を備えたコンピュータ端末４Ａである場合も想定できる。その場合はソフトウェア４０３Ａに暗号化されたテレビジョン用放送データの閲覧と暗号化されたデータという形でコンピュータゲームソフトウェアの実行が同一の端末で実行されうる。

放送の視聴権利とコンピュータゲームのプレイ権利、ウェブサイトログイン権利が割り当てられたＯＴＰトークンに対応する秘密鍵４０１Ａが端末４Ａに記録されており、ＯＴＰトークンを暗号化されたテレビジョン放送の視聴・暗号化されたゲームソフトウェアの実行・暗号化された書籍データの復号による新聞雑誌の閲覧等ができ、またＯＴＰトークンを用いたオンラインゲームサーバ端末３Ｃへのログインできるマルチメディア端末４Ａを提供することも考えられる。

【０１００】

＜放送局の設置場所と形態＞

端末５Ｃは有線放送と無線放送のどちらでも利用可能であるがこの項目では無線により複数の受信者に対し一方向にて情報を配信するサービスを好ましくは想定する。

【０１０１】

放送局５Ｃの設置場所は地上や空中を問わず宇宙空間の人工衛星でもよい。衛星の軌道は静止軌道でもよい。ある軌道に沿って動く衛星でもよい。能動的に推進剤などを用いて推力にて動く人工衛星でもよい。ＪＪＹのような時刻情報を放送する無線局やＧＮＳＳのような時刻情報を含む測位衛星システムに利用されてもよい。月面など衛星上でもよい。地球など惑星上でもよい。

【０１０２】

＜ワンタイムパスワードを簡易なタイムスタンプとして用いるブロックチェーン内蔵ＧＮＳＳ用放送局＞

放送局５Ｃもしくは５Ｃに３Ａのようなブロックチェーンノードとなる機能を持った人工衛星型端末５Ｃであり、かつ放送用のデータが全球測位衛星システムＧＮＳＳの測位データの内の暗号データ部分やタイムスタンプ部分に利用される場合も考えられる。前記測位用もしくは時刻放送用の端末５Ｃはある軌道に沿って動く衛星端末でもよいし月面など自然の天体に設置された端末でもよい。

この場合、放送局５Ｃは原子時計など時刻を算出する時計を持ち、時計に従った時刻データないしローカルなブロックチェーンを人工衛星内のサーバーに持ち、そのコントラクトに記録された本発明のブロックチェーン式ワンタイムパスワードを用い、時刻情報とＴＢ及びＫＣ値を用いて計算したハッシュ値を添付しＧＮＳＳ測位用の信号を含む電波として送信できる。また位置情報に加え独自の暗号化されたデータやタイムスタンプ情報を送付することもできる。このＧＮＳＳ放送局となった端末５Ｃから端末４Ａは時刻情報を受け取ることもできるかもしれない。

ＧＮＳＳ用の放送局５Ｃが放送する測位用の航法データにＢｎＴＯＴＰやメッセージ認証符号ＭＡＣ値を添付することで測位情報の流通時に３Ａを用いてＯＴＰ認証を行い測位情報の真贋を調べる事にもつながる。本発明のＢｎＴＯＴＰやＯＷＰを測位信号や測位用航法データに添付することで測位用航法データの改ざんを防ぎ、測位信号のなりすましによる誤った位置情報の算出や誤った位置情報による正しくないナビゲーションを防ぐことにつながりうる。前記の方法で端末４Ａは認証された位置情報と時刻情報を知ることができる。

５Ｃが宇宙にある場合、別の放送局５ＣＣが双方向通信を行い、５Ｃのブロックチェーンのキー情報Ｋの一部を５ＣＣの指示により変えることも出来る。

【０１０３】

＜レイティング＞

もしレイティングが必要な場合はコントラクトに明記しコントラクトからユーザーにトークンを発行する。

本発明ではレイティング情報をコントラクトに記述できる変数ＫＮＢＮをコントラクトに備える。

【０１０４】

５．サービス提供者、トークン管理者（Ｏｗｎｅｒ）

サービスを提供する資格のあるユーザーＵＡ（例えばインターネットバンキングを行うウェブサイト・ウェブアプリへのログイン権限を持つＯＴＰトークンの契約を行った銀行口座保有者を想定）とその端末１Ａに向けてその秘密鍵１０１Ａから端末３Ａのブロックチェーン部より計算されるユーザーの識別子Ａに管理者ＵＣは端末１Ｃ（端末ＤＣ）よりネットワーク２０（ネットワークＮＴ）を通じてブロックチェーンのノードであるサーバＰ（端末３Ａ）にＯＴＰ生成トークンを発行する。

ＯＴＰ生成トークンはスマートコントラクトとしてブロックチェーン上に記録される。スマートコントラクト（コントラクト）は修復及び改ざん困難なプログラムのとしてふるまい、一度端末３Ａや３ＢといったブロックチェーンシステムｄＬＳのブロックチェーン部にコントラクトが展開（デプロイ）されるとセッター関数などを用いて変更できる変数のほかは改ざん、変更、修正、消去ができない。サービス管理者はコントラクト内部に備えた内部変数を変更するセッターとなる関数ｆｓｃｂ３０１２Ａを通じてコントラクトのＫＣ値３０１１ＡやＢＣ値３０１３Ａの数値を変える。

コントラクトの関数は実行する権限のあるユーザー識別子や条件をプログラムすることができる。本発明では管理者のみが実行できるＯＴＰを計算するための内部シード値（内部シークレット変数）ＫＣ値３０１１ＡやＢＣ値３０１３Ａと、管理者のみがＫＣ３０１１ＡまたはＢＣ３０１３Ａにアクセスできる関数ｆｓｃｂ３０１２Ａを設定し、コントラクトの管理者のみがコントラクトのＯＴＰをを算出するシークレットキー情報を書き換え更新することができる。関数ｆｓｃｂ３０１２ＡはＫＣ値３０１１ＡとＢＣ値３０１３Ａの双方に個別に存在してもよいし、ＫＣ値３０１１ＡとＢＣ値３０１３Ａを同時に書き換える関数であってもよい。

本発明ではＯＴＰトークンの生成するパスワードのシークレット値のＫＣ値３０１１ＡまたはＢＣ値３０１３Ａを更新することでユーザーに動的なパスワードＯＷＰを提供する。そしてブロック番号Ｂｎを用いたワンタイムパスワードＢｎＴＯＴＰにおいてもシード値のＫＣ値３０１１Ａの更新を行うことを特徴とするので関数ｆｓｃｂとｆｓｃｂで書き換えられるシード値ＫＣ３０１１ＡやＢＣ３０１３Ａがコントラクトに備えられていることを特徴とする。

【０１０５】

トークンのコントラクト管理者はトークン発行時にトークン番号とは別にトークン固有のＵＲＩもしくは文字列情報をトークン番号をキーとしたマッピング変数などの形で設定し文字列情報をあるトークン番号のトークンに付与することもできる。ＵＲＩ情報からトークンを扱うソフトウェア上でＯＴＰトークンの製造番号を一次元バーコード等の形で表示できる。

このＵＲＩ情報はＥＲＣ７２１に準拠するのもであり既知の機能である。ＵＲＩもしくは文字列情報にトークンのシリアル番号やトークンに固有の画像情報のＵＲＩ（画像情報のあるウェブサーバの画像ファイルのＵＲＬ）等を記載することができる。

【０１０６】

＜コントラクト管理者の秘密鍵が漏洩することに備えた対策＞

サービス管理者は他のユーザーと同じくブロックチェーン部へアクセスするための秘密鍵１０１Ｃを持っており、前記コントラクト管理者ＵＣの端末１Ｃ（端末ＤＣ）に記録さ

れた秘密鍵１０１Ｃ（秘密鍵ＰＲＶＣ）が漏洩した場合、ＯＴＰトークンを管理するコントラクトが攻撃され、変更可能なコントラクト内部変数の書き換えやＯＴＰトークンの悪意ある発行が行われかねない。そこでコントラクトの変数を書き換える際に複数の秘密鍵によってコントラクトの実行を制御する部分がコントラクトに含まれていてもよい。

コントラクトに秘密鍵１０１Ｃ以外の秘密鍵を用いてアクセスを制御する技術を行ってもよい。１０１Ｃのみではなくて、１０１Ｃと１０１Ｃとは違う秘密鍵を1つ以上用いてコントラクトに管理者がのみが利用できる関数へアクセスし変数の閲覧や書き換えなどを行えるするマルチシグ技術を用いてもよい。

【０１０７】

あるいは、セキュリティ性を高めるためにＯＴＰを管理するコントラクトの内部変数やトークン発行関数などのＯＴＰトークンの運用にあたって重要度の高い実行する際に、関数の実行を行うには秘密鍵１０１Ｃから計算されるユーザー識別子Ｃと、ユーザー識別子Ｃ以外のユーザ識別子ＤとＥとＦとＧを持つ秘密鍵からアクセスし設定できるコントラクト内部変数が存在し、トークン発行関数やＫＣ値３０１１ＡやＢＣ値３０１３Ａの変更を行う関数を実行する際に、ユーザー識別子ＤとＥとＦとＧが設定できる変数が実行できる値かどうか判断し、ＤとＥとＦとＧの設定した値の内いずれか一つが関数の実行を停止させる（妨げる）変数値であった際には、トークン発行関数やＫＣ値・ＢＣ値のセッター関数やそのほかコントラクトの状態を変えるコントラクト管理者のみが変更できる関数の実行を中断させる機能が考えられる。

【０１０８】

前記のユーザー識別子Ｃと、ユーザー識別子Ｃ以外のユーザ識別子ＤとＥとＦとＧを持つ秘密鍵からアクセスし設定するという概念は、既存の装置に例えると複数のダイヤル及び鍵を備え全てのダイヤルと鍵を解錠できたときにのみ開けることの出来る金庫や金庫室の考えと同じである。金庫では複数のダイヤルや金属製の鍵と錠をもち、それら複数の要素が正しく解除されないと施錠された金庫が解錠されないように、ユーザー識別子Ｃの秘密鍵１０１Ｃを入手してもほかのユーザーの識別子ＤとＥとＦとＧの秘密鍵による複数の要素のロックを解除できないとコントラクトの内部変数を操作できない（複数の秘密鍵がそろわないと攻撃者はコントラクト変数の書き換えを行うセッター関数やトークン発行関数などの重要な操作を行う関数のロックを解除できない）。

コントラクト管理者の秘密鍵１０１Ｃ（１０１Ｃはユーザ識別子Ｃを示す）に加えて他のユーザー（監査役のユーザー識別子ＤやＥやＦやＧ）の持つ秘密鍵が１つ以上あり、それらすべてが個別にアクセスして設定できる真偽値を持っていて、ユーザー識別子Ｄ、Ｅ、Ｆ、Ｇの設定する真の値をとらなければコントラクト管理者用の関数を実行しないようにすることができる。これは図３ＡＣにおける３００８Ａ、３００８ＡＧ、３００８ＡＡにおいて、３０４２Ａのような変数又は処理部の記憶部である。

【０１０９】

またユーザ識別子ＤとＥとＦとＧのすべてが同意し変数を真偽値の真の値にする形ではなくて、例として１１人の監査人ユーザーを設定しそれらユーザーと対応したマッピング型の真偽値変数を備え、マッピング型変数の真の数（真か偽かの投票数）を集計し、１１のユーザーのうち過半数に達しない場合には管理者が操作できるコントラクトの関数の実行を停止するようプログラムできる（この場合も図３ＡＣにおける３００８Ａ、３００８ＡＧ、３００８ＡＡにおいて、３０４２Ａのような変数又は処理部の記憶部である）。

＜コントラクト管理者の秘密鍵が漏洩することに備えた簡易の対策＞

具体例ではユーザーＣとＤとＥとＦとＧの５つの秘密鍵を用いる例を示したが、不正アクセス時に簡易にコントラクトの操作を不可能にするために２つの異なる秘密鍵を用いてコントラクト管理者としてアクセスしてもよい。コントラクト管理者の秘密鍵１０１Ｃと、１０１Ｃが漏洩した際にＯＴＰトークンの発行等を停止するための秘密鍵１０１Ｂを用意し、１０１Ｂのみアクセスできる関数実行停止変数とそのセッター変数を備え、関数実行停止変数が真であるときに関数を実行し、偽であるときに関数を実行しないようにする処理をＯＴＰトークンの発行関数やコントラクト内部変数（図３ＡＣにおける３０４２Ａ

や３０４３Ａや３０２４Ａ、３０３０Ａ、３０３１Ａ、３０１１Ａ、３０１３Ａ）について設定できる。
秘密鍵漏洩が起きない条件、もしくは漏洩しても構わない場合には単一の秘密鍵１０１Ｃのみを用いてＯＴＰトークンのコントラクトにアクセスしコントラウトの状態を変えるようにしてもよい。
しかし何らかの複数の秘密鍵を用いて、コントラクト管理者の秘密鍵が漏洩した際の対策を行うことが好ましい。
【０１１０】
６．ＯＴＰトークンに関する補足
トークンのＵＲＩ情報を用い、ＵＲＩ情報から記号や模様を作り出すこともできる。ＥＲＣ７２１規格に準拠した32バイトのＵＲＩ情報のうち、先頭から1バイトずつ区切りその1バイトに数値を持たせそれをカードゲームの番号などに利用できるようにしている。
ウェブサイトのログインチケットとして利用する場合、ウェブサイトへログインしたのちトークンのＵＲＩ情報に従ってウェブサイトが動作を変えてもよい。チケットとしてトークンを用いる場合にＵＲＩバーコードをディスプレイに表示させ印字させてもよい。またＵＲＩ部分にはトークン発行時の備考情報が書かれていてもよい。ＵＲＩ情報はＥＲＣ７２１規格にある文字列情報でもよいし３２バイトの１６進数の情報であってもよい。ＵＲＩのデータ長が可変でもよい。
紙のチケットとして印刷する際に、印刷に用いるアプリケーションソフトウェアにおいて、サービス名とコントラクト識別子、ユーザー識別子、トークン番号、パスワード情報、印刷日時（必要によっては利用者名、連絡先）などの必要な情報に加え、チケットの紙面の印刷デザインの一部をトークンのＵＲＩ情報に応じて変えて印刷してもよい。
【０１１１】
＜ブロック番号Ｂｎを用いた時間に基づいたワンタイムパスワードの生成と呼び出し＞
本発明におけるワンタイムパスワードの生成と認証の基本的な動作を説明する。図１に示すシステムでＢｎＴＯＴＰを用いた認証方法について説明する。
ＯＴＰ生成とそれを認証するにはユーザー端末１Ａ、サーバ端末３Ａ、ネットワーク２０を利用する。ユーザー端末１Ａにおいて、秘密鍵１０１Ａと、指定したブロックチェーンのノードとしてサーバ端末３Ａのネットワーク２０でのＵＲＩ等と、指定したＯＴＰを生成するＯＴＰトークンのコントラクト識別子３０１９Ａ、秘密鍵１０１Ａからブロックチェーン部の処理によって算出されるユーザー識別子Ａ、指定したコントラクト識別子３０１９Ａにおいてユーザー識別子Ａに割り当てられた指定したトークン番号ＴＩＤＡを引数とする、図３ＡＡや図３ＡＢや図３ＡＣに記載のＯＴＰ生成関数３００９Ａを１Ａのブロックチェーンアクセスプログラムを通じて、ネットワーク２０を通じサーバ３Ａのブロックチェーン部にアクセスし関数呼び出しを行う。端末１Ａは端末３Ａのブロックチェーン部にアクセスし、ブロックチェーン部に記録されたコントラクトのＯＴＰ生成関数３００９Ａのプログラムに応じて処理を行う。
図１の実施例においてＯＴＰの生成にブロック番号Ｂｎを用いる時、図３ＡＡや図３ＡＢや図３ＡＣに記載のＯＴＰ生成関数３００９Ａでは、図６Ａに示すフロチャート図のＦ１００からＦ１０５に従い、ＴＩＤＡ、ＫＣ、Ｂｎ、Ａの4つを基にしてハッシュ関数ｆｈの引数とした後に引数をハッシュ関数に渡してＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）としてハッシュ値ＢｎＴＯＴＰを生成し、ＯＴＰ認証関数３００９Ａ又は３００９ＡはＢｎＴＯＴＰを関数３００９Ａの戻り値として端末１Ａに伝える。端末１Ａの入力した引数や関数呼び出しするユーザーがＦ１０１の条件に一致しない場合はＯＴＰ生成関数の実行を停止する。ハッシュ関数ｆｈは例えばＳＨＡ－２のＳＨＡ２５６である。
フローチャートの処理Ｆ１００ではＯＴＰ生成関数３００９Ａの引数入力にてユーザー識別子Ａ、トークン番号ＴＩＤＡの２つの引数を受け取る。なお用途に応じて第３や第４など複数の引数をとっても良い。
ここでＦ１０４にて生成されたＢｎＴＯＴＰを戻り値として利用しない場合、Ｆ１０７

に示すようにＢｎＴＯＴＰを符号なし整数として型変換しｎ桁のパスワードとして１０のｎ乗で割ったあまりをｎ桁数字のパスワードＢｎＴＯＴＰ－ｎとして伝えることもでき、ｎを７として７桁の整数値のＯＴＰとしてＯＴＰ生成関数３００９Ａの戻り値とすることもできるが、その場合はＯＴＰ認証関数３０１８Ａや３０１８ＤＡでも同じ計算を行いＯＴＰの検証を行うようにＯＴＰ認証関数をプログラムする必要がある。

実施例にはＦ１００からＦ１０５の処理を用いる３２バイトのＯＴＰを生成するＯＴＰ生成関数とＦ１００からＦ１０７までの処理を用いるｎ桁の符号なし整数のＯＴＰを生成するＯＴＰ生成関数を同一のコントラクトに備えたＯＴＰ生成を行うＯＴＰトークンのコントラクトを作成でき、通常はｎ桁（桁数は少なくともよい）のＯＴＰ生成関数とそれに対応するＯＴＰ認証関数で認証を行い、重要度の高い操作をするときはデータ量より大きな３２バイト（整数では最大２の２５６乗の数であり総当たり攻撃が困難と想定される）のＯＴＰ生成関数とそれに対応するＯＴＰ認証関数を用いて認証を行うこともできる。

【０１１２】

本発明の実施形態ではブロックチェーン基盤にイーサリアムを用い、ハッシュ関数ｆｈにハッシュ値が３２バイトの戻り値を出力するＳＨＡ２５６関数を用い、Ｆ１０４の選択肢をＯＴＰ生成関数の処理プログラムに設けずに、ＢｎＴＯＴＰ＝ｆｈ（ Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）として３２バイトのＯＴＰを算出するＯＴＰ生成関数（図６ＡにおいてはＦ１００、Ｆ１０１、Ｆ１０２、Ｆ１０３、Ｆ１０４、Ｆ１０５の順にフロチャートを経て動作する関数。あるいは図６ＢにおいてＦ１００，Ｆ１０８，Ｆ１０１、Ｆ１０２、Ｆ１０３、Ｆ１０４、Ｆ１０５の順にフロチャートを経て動作する関数。）と、

前記ＢｎＴＯＴＰを符号なし整数として型変換し１０の７乗で割った剰余である７桁数字のＯＴＰを算出するＯＴＰ生成関数（図６ＡのＦ１００、Ｆ１０１、Ｆ１０２、Ｆ１０３、Ｆ１０４、Ｆ１０７の順にフロチャートを経て動作する関数。あるいは図６ＢにおいてＦ１００，Ｆ１０８，Ｆ１０１、Ｆ１０２、Ｆ１０３、Ｆ１０４、Ｆ１０７の順にフロチャートを経て動作する関数。）の二通りのＯＴＰ生成関数をＯＴＰ生成トークンのコントラクトに備える形で実施した。

ここで図６Ａと図６Ｂの違いは、ＯＴＰ生成関数３００９Ａの実行を記録する回数などを保存する変数３０１７Ａや３０１７ＡＧに対して関数３００９Ａの実行回数の記録や増加処理もしくは関数３００９Ａの実行に必要な数値残高の増減等の変更処理Ｆ１０８の有無である。

Ｆ１０１では入力された引数からＯＴＰトークンのＯＴＰ生成関数３００９Ａを実行する関数実行者のユーザー識別子（関数の実行者、メッセージ送信者、ｍｓｇ．ｓｅｎｄｅｒのユーザー識別子）がトークン番号ＴＩＤＡのＯＴＰトークンが対応付けられ所有しているユーザーの識別子（ここではユーザー識別子Ａ）と一致するか判定する。この処理Ｆ１０１がなければＯＴＰトークンの持ち主でないユーザーがＯＴＰ関数を実行できてしまうため、メッセージ送信者が３００９Ａを実行する際にはそのメッセージ送信者がＯＴＰトークンの保有者であるかを判定する処理が必要である。

Ｆ１００ではＴＩＤＡのみを入力して処理を行うこともできるが、実際にはＦ１０１にて関数実行者のユーザー識別子（関数の実行者、メッセージ送信者ｍｓｇ．ｓｅｎｄｅｒのユーザー識別子）を関数実行処理時にｍｓｇ．ｓｅｎｄｅｒのユーザー識別子をＡとしてＯＴＰ生成関数に入力するので、Ａを引数として利用しているとみなし、Ｆ１０１に記載した。

（注）ＯＴＰトークンの生成の条件文Ｆ１０１ではＯＴＰトークンの保有者かどうかを判定するが、この部分をあるユーザー識別子のＯＴＰトークンの保有数とし保有数が１つ以上のＯＴＰトークンの数量を持つときトークン番号を引数としてＯＴＰを生成するということも可能であるが、この場合も関数実行者のトークンの保有数を調べる際にｍｓｇ．ｓｅｎｄｅｒというユーザー識別子を用いそのユーザー識別子（実行者がユーザー識別子Ａならばｍｓｇ．ｓｅｎｄｅｒ＝Ａ）のトークンのバランス（残数）を調べるので関数実行にはユーザー識別子を用いていると見てもよいかもしれない。あくまでここに記述することは実施例である。

【０１１３】
ハッシュ関数ｆｈは実施例ではＳＨＡ－２のＳＨＡ２５６やＳＨＡ－３であり、他にＭＤ５やＲＩＰＥＭＤ，ＳＨＡ－１、ＳＨＡ－２、ＳＨＡ－３が利用できる。ｆｈは暗号学的ハッシュ関数であればよい。例えば、ｆｈがＳＨＡ２５６のとき、ＢｎＴＯＴＰ＝ＳＨＡ２５６（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）である。実施例では引数の順に変数をエンコードし結合しそのデータのハッシュ値をＳＨＡ２５６関数などで求めている。
具体例としてＳＨＡ２５６（　ＥｎｃｏｄｅＰａｃｋｅｄ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）　）のような処理である。ここで関数ＥｎｃｏｄｅＰａｃｋｅｄ（Ｗ．Ｘ．Ｙ，Ｚ）は変数Ｗ，Ｘ，Ｙ，Ｚの順に包み込んで（梱包して）エンコードしメッセージＭｅｓを出力する関数もしくはライブラリや処理方法である。
ＥｎｃｏｄｅＰａｃｋｅｄ 関数により引数を梱包する順番が変わればデータが変わり内部のメッセージＭｅｓが変わり、ＳＨＡ２５６（Ｍｅｓ）の引数値が変わるのでそこから計算されるハッシュ値も変化する。たとえば、ＳＨＡ２５６（　ＥｎｃｏｄｅＰａｃｋｅｄ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）　）と、ＳＨＡ２５６（　ＥｎｃｏｄｅＰａｃｋｅｄ（ＴＩＤＡ，Ａ，ＫＣ，Ｂｎ）　）は異なるハッシュ値ＢｎＴＯＴＰを生成する。
【０１１４】
ここに述べる実施例では引数にＴＩＤＡ、ＫＣ、Ｂｎ、Ａの4つを基にしていることを特徴としている。ＴＩＤＡ、ＫＣ、Ｂｎ、Ａに基づいてそれぞれハッシュ値などを行い加工された４つの変数がＯＴＰ生成関数内部で加工された後にハッシュ関数ｆｈの引数として利用されてもよい。すなわちＯＴＰを計算する関数の引数は例としてＴＩＤＡ、ＫＣ、Ｂｎ、Ａの場合には前記4つに由来していればよい。
ＴＩＤＡやＡは個人情報につながる恐れがあり、それらを使うことをサービス提供者とユーザーの間で合意していればＡ、ＴＩＤＡを利用できるが、そうでない場合、もしくは法令によって個人情報の取り扱いを厳重にすべき場合はＡとＴＩＤＡを匿名化してＯＴＰの認証関数の引数として利用する必要が生じるかもしれない。（Ａ、ＴＩＤＡはイーサリアムではＥＯＡやトークンナンバーとして直接利用することが必要であり、現状のイーサリアムを基盤に用いたブロックチェーンではその要求に答えられない恐れがある。）
またブロックチェーン基盤もＯＴＰの購入や発行などといった際にブロックチェーンに送信されるトランザクションが一部の人以外からは分からない等の形で秘匿されていることが個人情報保護の観点から好ましい。イーサリアムではユーザ識別子やあるコントラクト識別子のトークン番号は世界中から閲覧可能であり、その識別子とユーザーの個人情報を結びつけることでどのユーザーがどのＯＴＰトークンのサービスの利用者か推測されかねない点がある。ユーザー識別子Ａやトークン番号ＴＩＤＡおよび前記ＯＴＰトークンのコントラクト識別子はサーバ端末３Ｆで検索できる。
既知の例では端末３Ｆに相当するサービスはイーサスキャン(Etherscan)などのブロックチェーン検索サービスおよびそれを行うブロックチェーン検索用サーバ端末として提供される。端末３Ｆではプライバシーの保護などで検索に制限をかける機能を搭載してもよい。たとえばユーザー識別子Ａが３Ｆにアクセスし検索する場合はＡに関連するコントラクト識別子やトランザクション情報を表示できるようにし、また公開を許可したトランザクションやコントラクト識別子の情報を閲覧できるようにするなどである。
本発明をイーサリアムといったすべてのトランザクションが公開されたパブリックネットワークのブロックチェーンシステムで行う場合は、サービス提供者はユーザー識別子のユーザーの本人確認をする際はユーザー識別子ＡとユーザーＵＡといった対応関係の記録を外部に漏洩しないように情報を管理することがサービス提供者やＯＴＰトークンの発行者に求められるかもしれない。
顧客情報とサービスはサービス提供者が持ち、ＯＴＰトークンの発行はＯＴＰトークンの管理団体が行い、サービス提供者とユーザーのみがＯＴＰトークンのトークン番号とユーザーの個人情報の対応関係をしているようにして両者が情報を開示しないことで個人情報を保護できるかもしれない。
【０１１５】

＜ＯＴＰ生成用端末とＯＴＰ認証用端末の分離＞
本発明ではＯＴＰ生成用端末とＯＴＰ認証用端末を同じ端末１Ａで行うこともできる。またＯＴＰ生成用端末とＯＴＰ認証用端末に分けて利用することができる。すなわちＯＴＰを生成し表示できる出力装置を持つ通信可能なハードウェア型ＯＴＰ生成用携帯端末１Ａとウェブサイトログイン用のＯＴＰ入力装置を備えるログイン認証用端末４Ａといった利用形態もできる。
ＯＴＰ生成を行う端末１Ａおよび端末１ＡにＯＴＰトークンによるＯＴＰを生成させるブロックチェーン部を持つ３Ａと、ウェブサイトなどのサービスを扱う端末３Ｃにアクセスできる端末４Ａがあり、端末１Ａと端末３Ａと端末３Ｃと端末４Ａがネットワーク２０に接続されており、１ＡがＯＴＰ生成関数を実行しＯＴＰを生成し端末１Ａの出力装置１５Ａに出力した後、ユーザーＵＡはそれを目視してヒトの手で端末４Ａの入力装置に入力し端末４Ａは入力されたＯＴＰを用いてＯＴＰ認証を行いその結果を端末３Ｃと通信しやり取りし、認証結果に応じて端末４Ａをログインさせサービスを提供させることができる。

【０１１６】
＜ブロック番号Ｂｎを用いた時間に基づいたワンタイムパスワードの認証と認証結果呼び出し＞
図３ＡＡや図３ＡＢや図３ＡＣに記載のＯＴＰを検証し認証するＯＴＰ認証関数３０１８Ａの動作はＯＴＰ生成関数３００９Ａと似ており、認証関数３０１８Ａ内部でＴＩＤＡ、ＫＣ、Ｂｎ、Ａをハッシュ関数ｆｈを用いてＶｅｒｉＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）を求め、ユーザーがサーバ３Ａにアクセスする際にワンタイムパスワード認証関数の引数に入力するＴＩＤＡ、Ａ、入力されたＡｒｇＢｎＴＯＴＰのうち、ＩＦ文などによる条件式で、ＡｒｇＢｎＴＯＴＰがＶｅｒｉＢｎＴＯＴＰと一致するか判定し、一致した場合にはＯＴＰ認証できたときの戻り値を端末１Ａに返す。また認証できた時の処理を行うこともできる。
一致しない場合には認証できないときの戻り値を端末１Ａに返し認証できなかった時の処理を行う。ここで前記ＢｎＴＯＴＰでは実施例で３２バイトのＯＴＰが生成されるが、ＢｎＴＯＴＰをを入力ｎ桁数字のパスワードＢｎＴＯＴＰ－ｎとして読み替えて、ｎ＝７の７桁の整数パスワードとしたとしたときも同様である。図６Ｃから図６Ｈに認証関数３０１８Ａの処理に関するフローチャートを示す。
端末の代表的な接続図は図１Ａや図１Ｂである。

【０１１７】
図６Ｃから図６Ｈに示す認証関数３０１８Ａのフローチャートついて説明する。フローチャートの処理Ｆ１１０ではＯＴＰ認証関数３０１８Ａの引数入力にてユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＡｒｇＯＴＰの３つの引数を受け取る。なおＯＴＰ認証関数は用途に応じて第４や第５など複数の引数をとっても良い。

【０１１８】
図６Ｆは認証関数３０１８Ａの実施例の一つであり、基本的な処理例である。図６Ｆに示す処理を用いた認証は端末３Ｃや端末３Ｄおよび暗号されたデータの復号用途に用いることができる。Ｆ１１０で認証関数の引数としてユーザー識別子Ａとトークン番号ＴＩＤＡを受け取り、Ｆ１１３にて引数からＶｅｒｉＯＴＰを計算する。このときブロック番号ＢｎとシークレットＫＣ値を用いる。ＶｅｒｉＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）を計算し、Ｆ１１４にて入力された引数のＯＴＰであるＡｒｇＯＴＰとＶｅｒｉＯＴＰが一致するか比較する。一致する場合は認証ができたと判断し、Ｆ１１６の処理を行い、一致しない場合はＦ１１８の処理を行う。図６Ｆを用いる端末の接続例は図８Ａ、図８Ｂ、図８Ｃ、図８Ｄである。
図６ＦのＯＴＰ認証関数の形態は端末３Ｃや端末３Ｄにおいて利用できる。

【０１１９】
図６Ｄは図６Ｆの処理に用いる真偽値や整数などの変数３０１７Ａや３０１７ＡＡや３０１７ＤＡに対し、ＯＴＰ認証関数３０１８Ａの実行後の真偽値もしくは整数値などの書

き換えを行う処理Ｆ１１５を追加したものである。３０１７Ａや３０１７ＡＡや３０１７ＤＡは真偽値、整数、文字列などのデータである。３０１７Ａや３０１７ＡＡや３０１７ＤＡはトークン番号をキーとして真偽値型、符号なし整数型、文字列型などのデータ型を持つマッピング変数である。マッピング変数は一つの例であって、トークン番号をキーとして結びつけられたデータを記録できれば良い。図６Ｄを用いる端末の接続例は図８Ａ、図８Ｂ、図８Ｃ、図８Ｄである。

【０１２０】

図６Ｃは暗号化データの復号やウェブサイトへのログイン用途に用いることを想定した処理例である。図６Ｃは図６Ｄの処理に、Ｆ１１１の処理を追加したものである。Ｆ１１１では認証関数３０１８Ａの実行者はユーザー識別子Ａかを判断し、異なる場合には処理をＦ１１７に示すように処理を中断する。Ｆ１１１にて認証関数３０１８Ａの実行者がユーザー識別子Ａの場合には、Ｆ１１２の認証関数の処理を続行し、入力されたＯＴＰ＝ＡｒｇＯＴＰが問題ない場合にはＦ１１３、Ｆ１１４、Ｆ１１５、Ｆ１１６、Ｆ１１６と処理が行われる。Ｆ１１４にてＡｒｇＯＴＰがＶｅｒｉＯＴＰと一致しないときはＦ１１８の示すように処理を中断する。図６Ｅは図６Ｃの処理Ｆ１１５を取り除いたフローチャートである。図６Ｅおよび図６Ｃを用いる端末の接続例は図８Ａ、図８Ｃ、図８Ｄであり、図８Ｂは端末３Ｄがネットワーク２０に接続ができ端末３Ａに接続できる用途において利用できる。

【０１２１】

図６Ｃと図６Ｅに示す処理方法は３ＡのＯＴＰトークンに関するコントラクトにある所有者情報３０１４Ａを用いるため、３Ａなどブロックチェーン上の端末と３Ｄが接続され３０１４Ａの情報が同期され共有されなければ図６Ｃと図６Ｅに記載の認証方法は端末３Ｄでは利用できない。端末３Ｄが駅の改札や入場口などの処理端末でありネットワーク２０を介して端末３Ａに接続されるか端末３Ａと同じブロックチェーン記録部及び制御部を持つ場合には３Ｄにおいても図６Ｃ及び図６Ｅと図６Ｇと図６Ｈの処理は利用出来うる。

端末３Ｄが金庫など容器や自動車などで、端末に備えられた電池等電源装置の制限や、端末を搭載する移動体が電波などの届かない環境にあり通信装置が制限されることによりネットワーク２０に接続ができない場合には、図６Ｃ及び図６Ｅと図６Ｇと図６Ｈの処理を行うことは困難である。

端末３Ｄの用途に応じて図６Ｃ及び図６Ｅと図６Ｇと図６Ｈは利用されることも利用されないこともある。図６Ｃ及び図６Ｅと図６Ｇと図６Ｈは利用形態の例である。

【０１２２】

図６Ｃと図６Ｅは認証関数３０１８Ａの実行者（ｍｓｇ．ｓｅｎｄｅｒ）がユーザー識別子Ａであるかを判定する処理Ｆ１１１をもつ。この処理を持つことで、ウェブサイトへのログイン処理時にユーザーがもつ秘密鍵１０１Ａによって計算されるユーザー識別子Ａがメッセージを送信し実行しているかを判定し、秘密鍵を持たない認証関数の実行者による関数実行を中断させる。図６Ｃと図６Ｅの違いは認証ができた際の３０１７Ａや３０１７ＡＡや３０１７ＤＡを変更する処理Ｆ１１５の有無である。図６ＣにはＦ１１５が有り図６ＥにはＦ１１５が無い。

【０１２３】

図６Ｇと図６Ｈは認証関数３０１８Ａの実行者がＯＴＰトークンの保有者かを判定する処理Ｆ１１９をもつ。この処理はＯＴＰ生成関数時の図６Ａや図６Ｂのフローチャートに記載された処理Ｆ１０１と同様の処理である。処理Ｆ１１９によってウェブサイトへのログイン処理時にユーザーがもつ秘密鍵１０１Ａによってブロックチェーンのノードである端末３Ａにメッセージを送信したとき、そのユーザーがトークン番号ＴＩＤＡのＯＴＰトークンを保有するかＦ１１９にて判定し、ＯＴＰトークンを持たない実行者による認証関数の実行を中断させる。図６Ｇと図６Ｈの違いは認証ができた際の３０１７Ａや３０１７ＡＡや３０１７ＤＡを変更する処理Ｆ１１５の有無である。図６ＧにはＦ１１５があり図６ＨにはＦ１１５が無い。

【０１２４】

＜コントラクトから他のコントラクトの関数の呼び出し＞
本発明で用いるコントラクトはあるブロック番号において記録された一つのスマートコントラクトのみで完結していてもいいし、同一ブロック番号に記録された他のコントラクト識別子のスマートコントラクトや他のブロック番号に記録された他のコントラクト識別子のスマートコントラクトに処理内容が分けて記述されていてもよい。例えばコントラクトＸからコントラクトＹの関数等を呼び出して利用してもよい。
例えば図６ＦのＦ１１６において図３ＡＢの３０２２Ａや３０２３Ａの処理を行うためにＯＴＰトークンの認証コントラクト３００８ＡＡとは違うコントラクト識別子をもつコントラクトＸにアクセスし前記コントラクトＸの関数Ｙを実行させたあと認証関数３０１８Ａの戻り値３０２１Ａを端末１Ａに出力してもよい。
もしくは他の例としてＯＴＰ生成や認証を行うコントラクトＸのハッシュ関数ｆｈ等の関数をほかのコントラクトＹに定義してライブラリの様に選択して呼び出せるようにしてもよい。
暗号学的ハッシュ関数ｆｈが計算機端末の性能の向上によって単一のハッシュ値に対し複数のメッセージデータが計算され、ハッシュ値の衝突を起こせるようになる事態に備え、より強度の高いハッシュ関数ｆｈとＯＴＰの計算に用いることができるようコントラクトＹのハッシュ関数ｆｈを更新し、コントラクトＸはコントラクトＹのｆｈを利用できてもよい。
【０１２５】
＜認証結果呼び出しを用いたサービスの提供＞
ＯＴＰ認証関数を呼び出してＯＴＰやＡやＴＩＤＡを入力し、その結果得られた認証結果の戻り値ＣＴＡＵ３０２１Ａを用いてサービスの提供を行う。
ここでは４Ａ．ウェブサイトのログイン用途、４Ｂ．入場口や建物設備への紙又はＩＣ式入場券、利用券、解錠鍵としての利用、４Ｃ．暗号化データおよびファイルの復号と閲覧、４Ｔ．放送での利用（１対不ｋ数の放送による暗号化データの流通）について順に説明する。
【０１２６】
＜４Ａ．ウェブサイトのログイン用途＞
ウェブサイトなどのログインにはブロックチェーンのある時刻において変更されうる変数ＴＢのうち、ブロック番号Ｂｎを基にしたＴＯＴＰ型ワンタイムパスワードトークンを用いる。ＴＢにブロックチェーン上の最新のタイムスタンプ３００２Ａがある場合にはそれをＴＢとして用いることもできる。
【０１２７】
ＴＢにはブロックハッシュＢｈ（３００３Ａ）を用いることもできるが、ブロックハッシュを用いる場合、イーサリアムとそのスマートコントラクトのプログラミング言語Ｓｏｌｉｄｉｔｙでは最新のブロック番号から数えて２５６番目までのブロック番号のブロックハッシュ値を呼び出すことができるが、その際にはブロック番号Ｂｎを引数に計算していると考えられる。Ｂｎを引数にＢｈを計算していると考えたとき、ブロックハッシュＢｈを用いる方法もブロック番号Ｂｎを用いる方法と変わりない。
Ｓｏｌｉｄｉｔｙ言語で式として表現するとＢｎＴＯＴＰ＝（Ａ，ＴＩＤＡ，ＫＣ，Ｂｈ）、Ｂｈ＝Ｂｌｏｃｋｈａｓｈ（Ｂｎ） であるのでＢｎＴＯＴＰ＝（Ａ，ＴＩＤＡ，ＫＣ，Ｂｈ＝Ｂｌｏｃｋｈａｓｈ（Ｂｎ））であり、ブロックハッシュＢｈを用いるときもブロック番号Ｂｎを用いているため、 ＢｎＴＯＴＰ＝（Ａ，ＴＩＤＡ，ＫＣ，Ｂｈ）とＢｎＴＯＴＰ＝（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）は引数の観点では類似した計算方法であるといえる。前記のようにブロックハッシュ値Ｂｈを用いる方法もブロック番号Ｂｎを用いる方法の異なる形態であると本発明では考える。
ブロックハッシュをＴＢとして用いることも出来うる。ただしブロックハッシュはノードを構成する端末の管理者により操作されうるので注意が必要である。またあるブロック番号Ｂｎのブロックデータのハッシュ値であって時刻に対し動的ではあるが時刻を表現する値ではない。

【０１２８】
ブロックハッシュＢｈをＴＯＴＰのブロック番号に用いる場合はイーサリアムといったブロックチェーンの基盤や、ブロックハッシュを異なるサーバ端末やブロックチェーンに記録し、そのブロックハッシュ値をＴＯＴＰを計算するコントラクトから参照できるようにする必要があるかもしれない。またブロックハッシュは例としてイーサリアムでは１５秒毎に代わる値であり、ブロック番号ではなくブロックハッシュを用いる場合はＯＴＰを生成し認証する時間間隔を延長したい場合の計算が複雑になる。
ブロックハッシュＢｈではなくブロック番号Ｂｎであれば、Ｂｎを基に表示する間隔を増やす変数ｎを用い、Ｂｎ　ｍｏｄ　ｎ　として、Ｂｎのｎで割った余りｍを求め、Ｂｎからｍを減算しＢｎｒとして（Ｂｎ－ｍ＝Ｂｎｒとして）、Ｂｎの代わりにＢｎｒをＯＴＰを算出するハッシュ関数の引数に利用し、ＯＴＰの生成と認証を行える時間を１５秒、３０秒、４５秒、６０秒とｎの数を増大させることで延長でき、本発明では演算の簡単さからブロック番号Ｂｎを好ましく用いた。
【０１２９】
ブロックハッシュＢｈにおいてもＢｈはＢｎを引数として用いて過去のブロックハッシュＢｈを求めることができるが、その計算ではＢｎが必要になりうることは先に述べたとおりである。ブロックハッシュ値Ｂｈそのものはあるブロック番号Ｂｎのデータに対応するハッシュ値であって、ブロック番号は時間によりその数値が増えていく変数であり、ブロック番号Ｂｎの増加は時間の経過を表せるが、ブロックハッシュ値の変化・増加が起きてもそのハッシュ値がいつの時間のデータであったかを示すことが出来ない。
本発明ではＢｎを使ったほうが良い場合とＢｈを使ってもよい場合があるかもしれない。ＯＴＰ生成関数とＯＴＰ認証関数の計算で用いるシード値がすべて記録されていれば生成関数で取得したＯＴＰを認証関数で認証する余地がある。
Ｂｎは時刻データに比例するためサービスに時刻の要素を必要とするもの、例えばタイムスタンプ的な要素を用いる場合には好ましく利用される。一方Ｂｎに加え、もしくはＢｈを用いてよりランダムさを増したＯＴＰを生成しウェブサイトのログインなどで利用したい場合はＢｈを利用することも好ましい。
ＯＴＰトークンを擬似乱数生成器として用いる場合は後述するＤＬＳのノード端末間の投票で決まる値Ｖと共にＢｈをＯＴＰ計算のシード値に利用することでよりランダムさを持たせることもできる。
【０１３０】
Ｂｈをタイムスタンプに用いるときはＢｈとブロックデータとブロック番号のデータベースがサービスを提供する端末になければ、どの時刻のブロックハッシュＢｈか分からない。またブロックハッシュ値が衝突する頻度は限りなく低いと考えられるが、あるブロックハッシュ値Ｂｈについて２つ以上のブロック番号があるとき場合、生成されたＢｎＴＯＴＰがどちらのブロック番号の時刻のデータであったかが分からなくなる。ブロックハッシュ値を算出するブロックチェーンの基盤が利用するハッシュ関数がハッシュ値の衝突を起こしやすいものである場合はこの問題が生じかねないという点もある。
【０１３１】
サーバ端末３Ｃを利用し、図３ＡＢにあるようにＯＴＰ生成関数をもつコントラクト３００８ＡＧとＯＴＰ認証関数を持つコントラクト３００８ＡＡを用いてＢｎＴＯＴＰをＯＴＰとして用いるウェブサイトのログインを例を示す。ＯＴＰ生成関数を含むトークンのコントラクト識別子ＣＰＧＴ３０１９Ａと、ＯＴＰ認証関数を含むコントラクト識別子ＣＰＡＴ３０２０Ａを用いてブロックチェーンにアクセスし、ＣＰＧＴ３０１９Ａから取得したＢｎＴＯＴＰを用いて認証関数を含むコントラクトＣＰＡＴ３０２０Ａにて認証し、認証関数戻り値をウェブサイトのログインや操作に利用する場合に、サーバ端末３Ｃ（ＳＶＬｏｇｉｎ）を用いてログイン処理を行う。
ここでＢｎＴＯＴＰ＝（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）でもよいし、前期ＢｎＴＯＴＰの引数に投票で決まる値Ｖや、コントラクト管理者が変更できる値ＢＣを加えたＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，Ｖ）でもよいし、またはブロックサイズＢ

ＳＺを加えたＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＳＺ）でもよい。ネットワーク２０を介して図８Ａの様に端末１Ａ、１Ｃ、３Ａ、３Ｃが接続されているとき、ブロックチェーンのノード３Ａやノード３Ｂ等ノード群の間で決定される値Ｖやブロックサイズ ＢＳＺは疑似的なランダム要素として用いることができる。またブロックハッシュ値Ｂｈなども用いることができ、例えば本発明の実施例で用いるＢｎＴＯＴＰの式はＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，Ｖ，Ｂｈ）である。
ＢＳＺはＶに応じて変わるときはＶ＝ＢＳＺとみなしＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，ＢＳＺ，Ｂｈ）である。

【０１３２】

本発明のハッシュ関数ｆｈの引数はＡとＴＩＤＡ、ＫＣ、ＢｎやＢＣ、そしてＶやＢｈが用いられるが、例えばＫＣやＢＣあるいはＶやＢｈを基にハッシュ関数でそれらのハッシュ値を算出し加工してＢｎＴＯＴＰの算出方法の推測を難しくするよう計算方法をとってもよい。関数の処理を行う上で必要な引数や内部変数にＡ，ＴＩＤＡ，ＫＣ，ＢｎやＡ，ＴＩＤＡ，ＫＣ，ＢＣを持つことを本発明では特徴とし、さらに Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，Ｖ，Ｂｈといった変数を用いることができることを特徴とする。

【０１３３】

さらにユーザーが保有するトークン番号ＴＩＤＡをキーとしたマッピング変数ＶＵ（ＶＵ［ＴＩＤＡ］）をシード値として含むＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，Ｖ，ＶＵ［ＴＩＤＡ］）でもよい。ユーザー側が設定できる投票によるシード値となる引数ＶＵ［ＴＩＤＡ］については別途説明する。

【０１３４】

認証関数の戻り値を端末１Ａが取得し、１Ａはその戻り値を３Ｃ（ＳＶＬｏｇｉｎ）で動作するウェブサイトのプログラムに従って処理し、または３Ｃに戻り値を渡し、認証結果が正しい時３Ｃ内部のサービスを提供しコンテンツを閲覧し操作させる。例としてインターネットバンキングや会員サイトなどを想定する。認証結果が正しくない場合にはログインを行わせない。
またログイン時にユーザーの許可を得た上でＣＰＧＴ３０１９Ａや、ＴＩＤＡ、Ｂｎ、ユーザ識別子Ａなどのブロックチェーン情報と、ログイン時刻情報と、
ＩＰアドレスもしくはＩＰアドレスのハッシュ値などＩＰアドレスに基づく識別子や、位置情報、端末１Ａに固有のＩＤ、端末１Ａの入力装置１４Ａのセンサ１４４Ａ等のセンサ値をＩＰＶ値として
３Ｃの記憶装置に図６Ｘの形でユーザー識別子ＡやトークンＩＤＡとＩＰＶ値を対応づけて、表などで表現できる形でデータベースに保持する。図６Ｘは例であり、トークン番号やユーザー識別子に対し複数のＩＰＶにて３Ｃにアクセスされている事を記録できる台帳データ、データベースであればよい。ここで前記情報はユーザーの合意の上収集し、また合意の上一部またはすべてを仮名化（暗号化）もしくは匿名化して保存する。

【０１３５】

図６Ｘに記載する例のように、同一の秘密鍵１０１Ａに由来するユーザー識別子から異なるＩＰＶ値、すなわち異なる環境からアクセスがあった場合に、異なる環境からのアクセスを不正アクセスと推測し、ユーザーＵＡの秘密鍵が漏洩しユーザー識別子Ａとトークン番号ＴＩＤＡの組み合わせに対し、端末３Ｃに記録されたデータベースのユーザー識別子Ａまたはトークン番号ＴＩＤＡとそれに対応する連絡先情報に不正アクセスの疑いがあることを通知し、ユーザの許可に応じてアクセスを禁止する機能を端末３Ｃは持つことができる。不正アクセスを禁止する用途はインターネットバンキングなどユーザーにとって重要な情報へのアクセスと情報の操作を行う場合を想定する。

【０１３６】

なお、サーバ端末３Ｃはサービス用途によっては、図６Ｘのようなデータベースを構築しユーザーへの不正アクセスの通知機能を提供しない端末３Ｃも実施形態として存在しうる。例えば簡易の会員サイトもしくは簡単なオンラインゲームサイトなどであるときなどは、サービスを行う処理部と記憶部を備えたサーバ端末３Ｃでは、図６Ｘのようなユーザ

ーからのアクセスを監視するデータベースを作成することは端末３Ｃの計算資源や記憶装置の容量を増大させかねないことが想定される。そしてサーバ端末３Ｃの利用コストが高くなる恐れがある。

またサーバ端末３Ｃにて個人情報の保護や管理を行うことに対するコストが高く、あえてアクセス者の個人情報を端末３Ｃに収集しないことで、管理を行うためのコストを低減しつつ、本発明のＯＴＰ認証システムを用いたログインサービスを提供したいという要望もあるかもしれない。それらの要望に沿うために図６Ｘのようなデータベースを構築しユーザーへの不正アクセスの通知機能を提供しない端末３Ｃも実施形態として存在する。

【０１３７】

３Ｃにおいて図６Ｘの形式でのアクセス情報の記録と不正アクセスの監視はＯＴＰ認証システムとしては必須の機能ではなく、サーバ３Ｃのサービス提供者と端末１Ａのユーザー ＵＡが図６Ｘの形でアクセスを記録されるかどうか同意したのちに利用できる機能である。図６Ｘの形式でアクセス情報の記録と不正アクセスの監視を行わなくとも本発明の実施はできる。ただしＯＴＰ認証システムにおいて秘密鍵１０１Ａが複数の端末に記録され利用された場合には図６Ｘのような複数のことなる環境からのアクセスを検知する機能があることがセキュリティ上好ましい。

【０１３８】

図８Ａの利用例としてインターネットバンキングがある。その際にウェブサイトや顧客データを管理する端末３Ｃと、端末３Ａのブロックチェーン上のコントラクトデータの両方を操作することもできる。

ＯＴＰの生成コントラクト（図３ＡＢの３００８ＡＧ）において顧客がＯＴＰを生成し、そのＯＴＰ（主にＢｎＴＯＴＰ、定期的に更新できるならばＯＷＰも）とユーザー識別子とトークン番号ＴＩＤＡを用いて認証関数３０１８Ａを引数に用い、実行した認証の回数をコントラクト内部の変数として保持できる。さらに３０１８Ａの実行後に識別子Ａもしくはトークン番号ＴＩＤＡをキーとしたマッピング変数３０２３Ａを備え、３０２３Ａにあるユーザー識別子Ａやトークン番号ＴＩＤＡに対応する資産やポイント等数値、評価値、投票の結果値をコントラクトに書き込み保存する関数３０２２Ａを持っていてもよい。そして３０２３Ａと３０２２Ａが認証コントラクト３００８ＡＡや３００８Ａに含まれ、認証関数３０１８Ａで認証できた場合に操作できるようプログラムされて３００８ＡＡや３００８Ａに備えられていてもよい。

具体的にはインターネットバンキングや会員サイト等において、ユーザー識別子Ａや前記識別子Ａが保有するＯＴＰトークンのトークン番号ＴＩＤＡに対する資産残高やポイント等の値３０２３Ａと、３０２３Ａをコントラクトに書き込み保存する関数３０２２Ａを持っていてもよい。

【０１３９】

＜ウェブサイトのログイン時に認証関数を実行した回数を記録する処理＞

本発明のＯＴＰ（ＢｎＴＯＴＰおよびＯＷＰ）の生成時または認証時にコントラクトへＯＴＰ生成関数及び認証関数の実行回数を内部変数３０１７Ａまたは３０１７ＡＧまたは３０１７ＡＡに記録させることができる。ここで内部変数３０１７Ａまたは３０１７ＡＧまたは３０１７ＡＡはトークン番号と対応した値を持つ変数である。実施例として変数３０１７Ａはトークン番号をキーとしたマッピング型の変数であり、マッピング型のほかにも構造体やクラスなどのデータ型でトークン番号と対応付けられている変数であれば本発明に利用できる。

（マッピング型は実施例において利用されるイーサリアムのスマートコントラクトプログラミング言語Ｓｏｌｉｄｉｔｙにおいて利用できる型の一つである。）

【０１４０】

ＯＴＰの認証回数もしくは生成回数をブロックチェーンのコントラクトの内部変数３０１７Ａまたは３０１７ＡＧまたは３０１７ＡＡに記録することで、ユーザーＵＡの端末１Ａの秘密鍵１０１Ａが漏洩し、ユーザーＵＡが知らぬ間に攻撃者がブロックチェーンに秘密鍵１０１Ａを用いてアクセスしＯＴＰ生成関数を実行しＯＴＰを生成した場合には、Ｏ

ＴＰ生成関数を不正に実行されて取得された事実が３０１７Ａや３０１７ＡＧに記録される。

ユーザーＵＡがＯＴＰ取得のために実行したはずのないＯＴＰ生成関数の実行回数が増えたことで（もし３０１７ＡがＯＴＰを生成するのに必要な料金のようなポイントの場合はその残高が減る事で）ユーザーＵＡは秘密鍵１０１Ａが不正利用されているかどうか察知することができる。もしくは１０１Ａの秘密鍵に対応するユーザー識別子のトランザクションの取引履歴に不正利用時のトランザクションが追加される。

前記の不正利用の察知にはＯＴＰトークンのサービスを提供するサーバ３Ｃやサーバ３Ｄやブロックチェーンのトランザクション等検索機能を備えた３Ｆ、ＯＴＰトークンをチケットなどで販売する３Ｅ、広告配信サーバ５Ａや暗号データ配信サーバ５Ｂなどに、ブロックチェーンのノードとなる端末３Ａや３Ｂのブロックチェーン部の変化を監視し、秘密鍵１０１から計算されるユーザー識別子ＡやＯＴＰトークンのコントラクト識別子に帰属するトランザクションの変化を検出しユーザーＵＡの連絡先に通知する機能が必要である。

ＯＴＰ生成関数の実行に限らずＯＴＰ認証関数の実行を行い実行ができた場合にも、前記の３Ｃや３Ｄや、３Ｅや３Ｆやからユーザーの通知先電子メールアドレスや電話番号、ＳＭＳ（ＳＭＳ、Short Message Service）、ユーザー識別子Ａに対する連絡を送るブロックチェーン上のトランザクションなどで通知することができる。

【０１４１】

実施例１ではＯＴＰ生成関数の実行回数は記録しないものの、ＯＴＰ認証関数の実行回数は記録する方式を検討した。これはブロックチェーンに生成及び認証の回数を変更するトランザクションを送ることを考えたとき、パスワードの生成はカウントせず何度でも出来たほうが良く、認証時のみその回数を記録できた方がトランザクションが少なくなり、ブロックチェーンのリソースや、それらを記憶し制御するサーバーの記憶装置や通信装置への負荷を低減できると考えたためである。ただしセキュリティを考えた場合はワンタイムパスワード生成関数の実行回数は記録することが好ましい。

重要度の低い操作を行うＯＴＰ生成関数と認証関数は図６Ａと図６Ｆに示すようにＯＴＰ生成関数・ＯＴＰ認証関数の実行回数を記録せず、重要度の大きい操作を行うＯＴＰ生成関数とＯＴＰ認証関数は図６Ｂと図６Ｄのように実行回数を記録したほうが良く、それらを使い分けてもよい。

図６Ｃや図６Ｄや図６ＧのＦ１１５はＯＴＰ認証関数を実行し認証結果が正しいときに行う処理であり、図６ＢのＦ１０８はＯＴＰ生成関数の実行回数を記録する関数である。

図には記載していないが、図６Ｂと対応して、図６Ｃや図６Ｄや図６ＧのＦ１１５とは別に図６ＢのＦ１０８に類似したＯＴＰ認証関数を実行した回数のみを記録する処理がＯＴＰ認証関数に含まれていてもよく、認証時にＦ１１５にて実行回数を変更するのではなくＯＴＰ認証関数が実行されＦ１１０にて引数が渡されたときに、Ｆ１１０とＦ１１１の間にＦ１１５のプロセスを設置してもよい。

ＯＴＰ生成関数とＯＴＰ認証関数の関数の実行回数をブロックチェーン上に改ざん困難・イミュータブルに記録するできるとよい。

【０１４２】

本発明ではＯＴＰ生成関数と認証関数の両方にその関数の実行回数を記録できることが好ましい。生成関数の実行回数を記録できる方が不正アクセスを未然に検知できる。ＯＴＰ生成関数を実行し、ＢｎＴＯＴＰやＯＷＰといったパスワードを生成し、それを用いてに認証関数を実行する。前記の手順を踏む場合に、ユーザーＵＡの秘密鍵１０１Ａが漏洩してしまい攻撃者が不正にアクセスしようとした場合には最初に生成関数を動作させることが推測される。

ブロックチェーンにアクセスしブロックチェーン上のトランザクションを監視できるサーバ端末３Ｆ等（例としてネットワーク２０に接続しサーバ端末３Ａのブロックチェーン部に対しアクセスできる端末３Ｃや端末３Ｄ、端末３Ｅや端末３Ｆ、端末５Ａや端末５Ｂ）に、ユーザー識別子Ａのブロックチェーン上の生成関数の実行回数の変化や、ユーザー

識別子Ａのトランザクションの変化またはイーサリアムなどで利用される内部トークンの変化をユーザーの電話番号やメールアドレスなどを用いて通知し、認証関数を実行させる前に、不正アクセスを知らせる必要がある。不正アクセスがあるとき、ユーザーＵＡは端末３Ｃや端末３Ｄのサービス提供者に通知させサービスの利用を停止する。

【０１４３】

端末３Ｄはネットワーク２０にアクセスできない場合がある。その場合はＯＷＰを攻撃者の端末が端末３ＡにアクセスしてＯＴＰ生成関数で生成する際に実行される３０１７Ａや３０１７ＡＧが変化するので、前記変数の変化をユーザーＵＡに通知することでＯＴＰが攻撃者に取得され紙やＮＦＣタグに記録された恐れがあることが分かる。この場合にもサービス提供者に相談することができる。

端末３Ｄに記憶された認証回数記録部分も端末３Ｄへのユーザーのアクセスや認証の履歴をブロックチェーンの様にトランザクション毎にハッシュ値を付与させ連結して保存するなどして改ざん検知ができイミュータブルな記録部分とすることが好ましいかもしれない。ブロックチェーン型ではなくとも端末３Ｄのあるキーと認証のデータをメッセージとして定期的もしくは指定する認証回数ごとにＨＭＡＣによりＭＡＣ値を付与し記録できることが改ざんなどに対抗する手段として好ましいかもしれない。

このようにＯＴＰ認証関数とＯＴＰ生成関数のいづれかまたは両方に実行回数を記録する変数を設けることで、攻撃者はユーザーＵＡに知られないうちにユーザーのトークンを操作することを困難にさせ、不正アクセスを防止する。

【０１４４】

＜認証関数を含む関数が認証時にコントラクト内部の変数を操作する場合＞

認証関数を実行した回数を記録する処理に関連して、本発明では認証関数を含む関数が認証時にコントラクト内部の変数を操作する処理を含めることができる。

具体的には認証関数を内部に含むあるいは認証関数の後に続く処理３０２２Ａをコントラクトに設定し、３０２２Ａで認証関数が実行されワンタイムパスワードによる認証ができた場合にコントラクトの内部変数３０２３Ａを書き換えることができる。ここで内部変数３０２３Ａはユーザー識別子またはトークン番号と対応した値を持つ変数３０２３Ａである。変数３０２３Ａの例としてユーザー識別子もしくはトークン番号をキーとしたマッピング型変数であり、マッピング型のほかにも構造体やクラスなどのデータ型でユーザ識別子やトークン番号と対応づけられている変数であれば本発明に利用できる。

【０１４５】

＜インターネットバンキングでの処理例＞

認証関数を含む関数が認証時にコントラクト内部の変数を操作する場合の一例として、簡易なインターネットバンキングもしくはコントラクト内ポイント利用システムに利用可能である。認証コントラクト３００８ＡＡはこの場合ＯＴＰ認証機能と認証後の銀行口座残高情報の記録ができる。参考として次に例を示す。

【０１４６】

次に示す１から４に、インターネットバンキングもしくは認証コントラクト内ポイント利用システムのコントラクト内部で利用する顧客の変数を設定する。

１．銀行口座（ポイント口座）の識別子である銀行口座番号ＧＫＢＡ（またはポイント口座番号ＧＫＢＡ。ＧＫＢＡはトークン番号やユーザー識別子でもよい）。

２．口座ＧＫＢＡの名義を匿名化した値ＭＩＧＡ（秘匿されていないブロックチェーン基盤に名義匿名化などせずに記述することは好ましくない）。

３．ＧＫＢＡの資産の残高ＡＳＴＡ。ＧＫＢＡは３０２３Ａに記載の変数でトークン番号（またはユーザー識別子）をキーとしたマッピング変数ＡＳＴＡ［トークン番号］。

４．ＧＫＢＡに対応するトークン番号ＴＩＤＡもしくはユーザ識別子Ａを対応付けたデータベースＧＫＤＢ。

ＧＫＢＡやＭＩＧＡ、ＡＳＴＡはユーザー識別子やトークン番号をキーとするマッピング変数などで表現される。上記項目１から４の変数がＯＴＰ認証関数をもつコントラクト３００８ＡＡ（または３００８Ａ）に設置されており、ＯＴＰ認証関数もしくは認証処理

を含む、資産の別の銀行口座番号ＧＫＢＡへの振り替えを行う処理ができてもよい。
（このほか口座の種類、振り込み限度額、口座開設日もしくはそのブロック番号、本人確認情報を匿名化した値も必要となりうる。）
【０１４７】
ユーザー識別子Ａの持つトークン番号ＴＩＤＡのＯＴＰトークンに預けられた残高ＡＳＴＡ［ＴＩＤＡ］（ＴＩＤＡをキーとする３０２３Ａ）があって、
ユーザー識別子ＢもＴＩＤＡのＯＴＰトークンを持ち同様に残高ＡＳＴＡ［ＴＩＤＢ］を持つとき、ＡがＢのＴＩＤＢトークンにＡのＡＳＴＡから数値ｔｒｓを移動させたいとき、
ユーザー識別子Ａの持つトークン番号ＴＩＤＡのＯＴＰトークンに預けられた残高ＡＳＴＡ［ＴＩＤＡ］（ＴＩＤＡをキーとする３０２３Ａ）の一部をユーザーＵＡが指定し、
ユーザー識別子Ｂの持つトークン番号ＴＩＤＢのＯＴＰトークンに預けられた残高ＡＳＴＡ［ＴＩＤＢ］（ＴＩＤＢをキーとする３０２３Ａ）に振り込む関数もしくは処理３０２２Ａがあり、
ユーザー識別子Ａのユーザーがトークン番号ＴＩＤＡのＯＴＰトークンによりＯＴＰ認証を行い処理３０２２Ａと認証関数３０１８Ａの処理（３０２２Ａに３０１８を組み込んだ、もしくは３０１８Ａの後に３０２２Ａの処理を続けた処理）を実行し、ＯＴＰ関数の認証結果が正しい時、処理３０２２Ａは ＴＩＤＡをキーとするマッピング変数３０２３Ａからｔｒｓを引いてＡＳＴＡ［ＴＩＤＡ］－ｔｒｓとした後、 ＴＩＤＢをキーとするマッピング変数３０２３ＡへＴＩＤＡの持ち主であるユーザー識別子の指定する数値ｔｒｓを足した数値ＡＳＴＡ［ＴＩＤＢ］＋ｔｒｓに変更することで、数値を変更でき、数値ｔｒｓの振り込みができる。
このように本発明のＯＴＰ認証システムを用いてＯＴＰ認証関数を含む金融業務を行うコントラクトや会員サイトにおいてポイントのやり取りを行うコントラクトが実施されうる。
【０１４８】
関数３０２２Ａや資産残高を示す３０２３Ａは顧客がコントラクトにダイレクトにアクセスすることで閲覧や関数実行を行うことも想定される。
【０１４９】
また銀行がサーバ３Ｃに顧客をアクセスさせたうえで銀行側がコントラクトの顧客の資産残高などを操作することも考えられる。その場合はユーザーではなく銀行が顧客の資産の数値数量を顧客のログイン時ウェブアプリウェブサイトなどでの認証後の指示に従って取引指示を受け、残高を書き換える関数を用い振り込み手続きなどを行う。
【０１５０】
インターネットバンキングにおける資産残高をサーバ３Ｃと認証コントラクトのいずれかまたは両方に記録できる。前記についてはインターネットバンキングに限らず会員サイトや会員による投票サイト、オンラインゲームサイトなども同じように数値数量データの運用ができる。
【０１５１】
＜会員サイトへのログイン用ＯＴＰトークンの有効・無効の判定を行う手段＞
ウェブサイトへのログインの利用用途として会員サイト、インターネットバンキングなど金融取引、ウェブメール、オンラインストレージ、電子商取引サイト（ＥＣサイト）、ソーシャルネットワーキングサービスＳＮＳ、音声動画配信サイト、オンラインゲーム、オンライン会議サイトなどが挙げられる。銀行の場合と同じくサーバ端末３Ｃに顧客をアクセスさせることができる。ここでログインする権利が期間や回数で制限されていることが考えられる。本発明の実施形態として次の３つを示す。
【０１５２】
１．ブロック番号を用いてワンタイムパスワード表示可能な期限を設定する方法
　顧客がトークンを発行されてから指定したブロック番号を超えた場合にＯＴＰトークンのＯＴＰ生成を行えなくすることもできる。これはある一定期間以内にトークン有効期限

が切れる様にする場合にＯＴＰ生成部分に期限を設定することが必要になる場合もあり設定される。

具体例を次に示す。あるトークン番号のトークン発行時のブロック番号ＢｎＭｉｎｔをトークン番号をキーとしたマッピング型変数としてＯＴＰを生成するコントラクトに記録し、ＯＴＰを生成する関数に、実行時の最新のブロック番号Ｂｎが数値が表示したい期間に相当するブロック番号ＢｎＶａｌｉｄ＋ＢｎＭｉｎｔ以内であればＯＴＰを生成できるようにする。

例えばＯＴＰを生成する関数の実行時に、現在のブロック番号Ｂｎが、数式Ｂｎ＜ＢｎＭｉｎｔ＋ＢｎＶａｌｉｄ　であるかどうか判定させ、ブロック番号Ｂｎが数値が表示したい期間に相当する場合はＯＴＰを生成できるようＯＴＰ生成関数部分をプログラムすることで指定したブロック番号を超えた場合にＯＴＰトークンのＯＴＰ生成を行えなくする。

【０１５３】

２．コントラクトの管理者が、ユーザーのトークン番号に対応した有効、無効の判定に利用できる変数を書き換えられる場合。

ある顧客ＵＡのトークン番号ＴＩＤＡに対し、規約等に従って有効期限やサービスの提供が終了した場合にＴＩＤＡに対応付けられたトークンの無効・有効を示すマッピング型変数ＶＡＬＩＤ［ＴＩＤＡ］をコントラクトの管理者が変更し、トークンが有効から向こうに切り替わったことを持ってトークンデータとしては無効にすることができる。この処理は改札で紙等の切符を切る動作に該当する。あるいは入場券に判を押したり、券を切り半券にする動作に該当する。ＯＴＰトークンの有効無効を真偽値で示してもよいし、そのトークンにチャージされた電子マネー的な数値でもよい。電子マネー的な利用方法では残高に数値を加算したり減算したりできる。

ここで本発明のブロックチェーン上のトークンは現実世界での書籍やコンテンツ、紙の有価証券や金属の鍵の代替物であって、ユーザーとサービス提供者が合意しなければ法的な紛争が起きる可能性は残る。権限の集中を避けるため、コントラクト管理者とサービス提供者は別の団体とし、端末３Ｃや３Ｄを管理するサービス提供者の要求に応じて端末１Ｃを管理するコントラクト管理者がＶＡＬＩＤ［ＴＩＤＡ］を書き換えることでＯＴＰトークンを無効にしたり有効にすることもできる。ＶＡＬＩＤ［ＴＩＤＡ］が整数であれば数値の大きさを、ＶＡＬＩＤ［ＴＩＤＡ］が文字列であれば文字の形で変更できる。

【０１５４】

３．ユーザーがトークンの利用の意志を示せる場合

トークンの持ち主である顧客ＵＡがその利用権を放棄したいとき、もしくは一時的に利用を止めたいと示すときに、ユーザーの秘密鍵１０１Ａを用いてユーザー識別子Ａに帰属するコントラクト識別子のＯＴＰトークンのトークン番号ＴＩＤＡに対応する意思表示欄をマッピング型変数ＮＯＴＥ［ＴＩＤＡ］にその意志を設定し表示することができる。

前記変数ＮＯＴＥ［ＴＩＤＡ］については、秘密鍵１０１Ａを記録し１０１Ａにトークン番号ＴＩＤＡのＯＴＰトークンが割り当てられたユーザー識別子Ａのユーザーのみからアクセスし変更できるセッター関数によってＮＯＴＥ［ＴＩＤＡ］は変更される。

意思表示は真偽型変数や数値、文字列変数で行われることが想定される。またＮＯＴＥ［ＴＩＤＡ］は文字列型の場合、自由な文字列を記録できるものの、トランザクションデータ量が増える事と、誤って誤字などのある文章を書いてしまう恐れがある。ブロックチェーン、ＤＡＧ等の分散型台帳では一度連結されたブロックのブロックデータ内部のトランザクションデータは書き換えと改ざんが出来ないので、任意の文字列よりは真偽型変数や数字による選択肢方式で意思表示することが好ましい場合がある。

【０１５５】

＜会員サイトなどへの投票権としての利用＞

例えば投票を行うにおいては本発明のトークンを用い、あるウェブサイトやウェブアプリに本発明のトークンとワンタイムパスワード認証システムを用いてログインし、そのコンピュータ画面で投票したい候補者の識別子に投票し、ブロックチェーン上のワンタイム

パスワードを生成し認証するトークンのコントラクトの変数に投票内容を記録できる。ただし投票機能を実装するには認証関数を内蔵したコントラクトにユーザー識別子Ａがトークン番号ＴＩＤＡのトークンを所持することを確認し、所持する場合に限り投票先となる変数に値を入力するセッター関数が必要である。
秘密鍵１０１Ａそしてユーザー識別子Ａに帰属するコントラクト識別子のＯＴＰトークンのトークン番号ＴＩＤＡに対応する意思表示欄をマッピング型変数ＶＯＴＥ［ＴＩＤＡ］として設定し、変数ＶＯＴＥ［ＴＩＤＡ］は１０１Ａをもちユーザー識別子Ａとしてアクセスできるユーザーのみからアクセスされ、ユーザーが投票の値を投じることができる。
投票の内容を秘密にしつつ多数決などをとる場合は場合はＶＯＴＥ［ＴＩＤＡ］をプライベート変数にしたうえで秘匿化できるブロックチェーン基盤にて投票を行わせ、ＯＴＰトークンのコントラクト内でＶＯＴＥ［ＴＩＤＡ］の結果を集計すればよい。例えば選択肢が０から３しかない場合、それらの数字０から３以内までの整数を受け付けるようＶＯＴＥ［ＴＩＤＡ］のセッター関数をプログラムし、数字が０、１、２、３に該当する選択肢のＯＴＰトークンによる投票数は何票あるか（つまりＯＴＰトークンの票数が何票あるか）を集計すれば０から３の整数の選択肢の内どれが指示されているか調べることができる。ＯＴＰトークンのコントラクト内でＶＯＴＥ［ＴＩＤＡ］を集計せずに端末３Ｃや端末３Ｆを用いてＥＣＭＡＳｃｒｉｐｔを用いて、ノード３Ａや３Ｂのブロックチェーン部を読み込むことでＶＯＴＥ［ＴＩＤＡ］のデータを集計するプログラムを利用してもよい。

【０１５６】
＜ユーザー側が設定できる投票によるシード値ＶＵ［ＴＩＤＡ］＞
ＯＴＰトークンの生成するＢｎＴＯＴＰをログイン先のサービスで擬似乱数生成に利用する方法として、ユーザー側が設定できる投票によるシード値ＶＵ［ＴＩＤＡ］を用いることもできる。
例えば端末１Ａにて、ユーザー識別子Ａにトークン番号ＴＩＤＡというＯＴＰトークンが発行されており、ユーザー側が設定できる投票によるシード値ＶＵ［ＴＩＤＡ］を引数をＢｎＴＯＴＰのシード値に加え、例えばＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，Ｖ，Ｂｈ，ＶＵ［ＴＩＤＡ］）というＯＴＰを計算させることでＯＴＰの生成と認証とウェブサイトログインを行うＯＴＰトークンとして利用できるとともに、ウェブサイトのログイン先で前記ＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，Ｖ，Ｂｈ，ＶＵ［ＴＩＤＡ］）を簡易の擬似乱数生成器として用いることができる。ここでＶは投票で決まる値Ｖ（イーサリアムではＢｌｏｃｋＧａｓＬｉｍｉｔ値をＶとして用いる）、ＢｈはブロックハッシュＢｈである。

【０１５７】
前記のユーザー側が設定できる投票によるシード値ＶＵ［ＴＩＤＡ］を用いたＯＴＰトークンを用いる認証システム及び擬似乱数生成器は、ウェブサイト・ウェブアプリなどへのログインを要求するオンラインゲーム（オンラインコンピュータゲーム）などに利用できるかもしれない。ＶＵ［ＴＩＤＡ］を用いたＯＴＰトークンのＯＴＰのランダムさを応用し、ＯＴＰトークンの生成したＯＴＰをさらにハッシュ化あるいは加工してそれをゲーム内のランダムさを決定する変数に利用することができる。ゲーム以外の用途にも利用できる。

【０１５８】
例えばシード値ＫＣ値（およびＢＣ値）は端末３Ｃのゲーム管理者がコントラクトの管理者で端末１Ｃを操作できる場合は書き換えることができるが、ゲーム内でユーザーに対しランダムさを与えるＯＴＰトークンのＯＴＰを擬似乱数として利用しているとき、ユーザーのＯＴＰトークンの生成するＯＴＰデータの将来の現れ方をを悪意を持って制御しようとコントラクトの管理者がＫＣやＢＣを書き換えようとするかもしれない。
そこでコントラクト管理者が制御できない変数ＶＵ［ＴＩＤＡ］をトークン番号ＴＩＤＡのユーザーに書き換えさせるセッター関数と共にコントラクトに備えることで、ユーザーが自由意思により値を書き換えられる変数ＶＵ［ＴＩＤＡ］を設定することができる。

ここで外部のユーザーが設定できるシード値ＶＵ［ＴＩＤＡ］を設定することで、ＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，Ｖ，Ｂｈ，ＶＵ［ＴＩＤＡ］）などといったＯＴＰ計算方法となり、コントラクト管理者のＫＣ値のみならずＶＵ［ＴＩＤＡ］が存在し、ユーザーのみが制御可能でコントラクト管理者が制御できない変数がＯＴＰ（ＢｎＴＯＴＰ）に含まれるようになるため、ユーザーの指定するＶＵ［ＴＩＤＡ］の値を尊重した（ユーザーの送信したトランザクションの投票値による意思を尊重した）ＯＴＰあるいは擬似乱数を生成でき、ＯＴＰ認証システムや擬似乱数を用いたサービスに利用できる。
ＶＵ［ＴＩＤＡ］を利用するにはトークン番号ＴＩＤＡのトークンを持つユーザーのみがＶＵ［ＴＩＤＡ］を変更できるセッターとなる関数が必要である。
（前記会員サイトで利用する投票用変数ＶＯＴＥ［ＴＩＤＡ］と前記ＶＵ［ＴＩＤＡ］はユーザが設定できる変数としては同じ扱いである。）

【０１５９】
具体的に実施する場合、１つの例として以下の式でハッシュ関数にＳＨＡ－２のＳＨＡ２５６を用いてＢｎＴＯＴＰｒｎｖとするハッシュ値は表現される。
ＢｎＴＯＴＰｒｎｖ　＝　ＳＨＡ２５６（　ＥｎｃｏｄｅＰａｃｋｅｄ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，Ｖ，ＶＵ［ＴＩＤＡ］）　）。
ここで、ユーザー識別子Ａ、トークン番号ＴＩＤＡ、シークレット変数ＫＣ、パスワードの生成及び認証時の最新のブロック番号Ｂｎ、
ブロックチェーンノード間の投票により決まる値Ｖ、ユーザーが保有し利用する番号ＴＩＤＡのトークンの投票できるシード値ＶＵ［ＴＩＤＡ］である。
ＢｎＴＯＴＰｒｎｖはオンラインゲームのログイン用ワンタイムパスワードや、ログイン後のオンラインゲーム内での疑似的なランダムさを決める数値に利用できる。

【０１６０】
前記ＶＵ［ＴＩＤＡ］を引数に持ったワンタイムパスワードＢｎＴＯＴＰはオンラインゲームの管理者の制御の及ばない変数であり、管理者が不正に書き換えてゲームプレイヤーに対し不利になるような値を設定することはできない。

【０１６１】
補足として管理者がプレイヤーを欺いて、管理者もＶＵ［ＴＩＤＡ］を変更できる様に関数をコントラクトのデプロイ時に設定できてしまうとこの前提は崩れる。ログイン及び擬似乱数生成用のトークンを管理するものとゲームの管理者を分けることが好ましい。またコントラクトは秘匿化されていることが好ましく、さらに好ましくは秘匿化されている変数とその変数を変えるトランザクション以外はコントラクトの処理内容が公開できると好ましい。ユーザーの設定したＶＵ［ＴＩＤＡ］に関するトランザクションも設定したユーザー以外には閲覧できないようにすること（投票した値の秘密を保持する事、秘密投票できること）が好ましい。
本発明を端末３Ｃのコンピュータゲームサーバのログイン権および擬似乱数生成器に用いる場合、あるいは端末４Ａで暗号データを復号して実行できるコンピュータゲームの所有権及び擬似乱数生成器に用いる場合や、オンラインゲームを配信する端末３Ｃについてその乱数制御部を一部オープンソースとすることもあってもよい。

【０１６２】
補足として本発明の実施例で利用したイーサリアムではメインネットとテストネットを問わずすべてのコントラクト内部変数と関数や処理の内容、トランザクションが外部のユーザーから閲覧できるため、コントラクトの管理者はコントラクトの処理内容を隠すことが困難である。
投票によって決まる変数ＶやＶＵ［ＴＩＤＡ］を設定する理由の一つとして、イーサリアムのように全てのトランザクション、コントラクトの変数と処理内容が公開されており、あるユーザーのワンタイムパスワードのシード値が算出できそうであっても、ノード間の投票で決まる値としてＢｌｏｃｋＧａｓＬｉｍｉｔ値をＶとして採用し、さらにＶＵ［ＴＩＤＡ］をユーザーが任意の時間任意の値に変えうるようにすることで、攻撃者が将来

のパスワードの予想を困難にする狙いがある。
なお本発明を好ましく実施するにはコントラクトやトランザクションが秘匿化されたブロックチェーンが好ましい。
銀行など金融分野では秘匿化されたブロックチェーンなど分散型台帳システムにおいて本発明の認証システムと認証装置を構築することがおおいに好ましい。
【０１６３】
補足として分散型台帳記録部３００Ａのデータの連結構造にブロックチェーン型ではなくＤＡＧ型を用いる場合、Ｂｎが利用出来ない場合にはＢｎのかわりにコントラクト管理者が変更できるＢＣをＯＴＰ計算のシード値に用い、時刻の経過に応じて定期的にＢＣの数値をインクリメントするなどしてスマートコントラクト内部のシード値の変数を変更することができる。
またＶＵ［ＴＩＤＡ］をＢＣと同じくＯＴＰ計算のシード値に用いることができる。オンラインゲームに限らず、ログイン後のサービスがランダムさを求める場合には本発明のスマートコントラクトにおいて生成されるワンタイムパスワードを基に疑似的なランダム値を利用できる。
【０１６４】
＜４Ｂ．入場口や建物設備への紙又はＩＣ式入場券、利用券、解錠鍵としての利用＞
紙などに情報を固定された形で印刷し入場等に利用するパスワードを生成させるにはブロック番号Ｂｎに同期するワンタイムパスワードでは認証の実施が困難になる恐れがあった。そこで各トークン番号もしくは各ユーザー識別子に対応した時刻には同期しないが任意の時間に変えることの出来る半固定式のパスワードＯＷＰを利用する。図８Ｂに端末や装置の接続例を記載する。ここで説明のため主に図８Ｂや図３ＡＡと図３ＡＢと図３ＡＣと図３Ｄと図３ＤＡを説明に用いる。
【０１６５】
具体的にはブロックチェーンのある時刻において変更されうる変数ＴＢのうち、ブロック番号Ｂｎの代わりに、コントラクトの管理を行う権限をもつ端末１Ｃの秘密鍵１０１Ｃから計算されるユーザー識別子Ｃのユーザーのみがアクセス出来るセッターとなる関数ｆｓｃｂ３０１２Ａを備え、ユーザー識別子Ｃであるコントラクト管理を行うユーザーのみがブロックチェーン上で任意の時刻において書き換えることの出来る変数ＢＣ値３０１３Ａを備え、ＢＣをブロック番号Ｂｎの代わりに用いるパスワードＯＷＰを入場口や建物設備への紙又はＩＣ式入場券、利用券、解錠鍵としての利用する。
ここでＯＷＰは管理者変更型ワンタイムパスワードであり、管理者が変更しない場合には固定されたパスワードとなる。ＯＷＰは管理者が定期的（６０秒ごと１０分毎など）に更新する場合はＴＯＴＰに近づく動的なパスワードになりうる。ＢＣはＯＷＰをＴＯＴＰ的（ＢｎＴＯＴＰ的）に扱うときは管理者や指定したユーザーもしくはすべてのユーザーが書き換えることができてもよい。
しかしＯＷＰをＴＯＴＰ的にではなく紙のチケット１８Ａや金庫や自動車の鍵１９Ａに用いる場合はＢＣをＴＯＴＰ（ＢｎＴＯＴＰ）の様に短期間で書き換えられてしまうとＯＷＰによる認証ができないのでコントラクトの管理者がＢＣを変更するかどうか決定しある時刻に変更する。
なおＢｎＴＯＴＰを用いてＯＷＰを再現するときはブロック番号Ｂｎを符号なし整数の変数Ｍで割った剰余ｒを用い、Ｂｎをからｒを減算しＢｎｒとして（Ｂｎ－ｍ＝Ｂｎｒとして）Ｂｎｒを求め、前記ＢｎｒをＢｎの代わりにＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎｒ）として計算する際に、変数Ｍを著しく増大させ、Ｍを操作することで数週間、数カ月、数年といった時間にわたり同一の値のＢｎＴＯＴＰを生成・表示・認証させることもできる。
前記のＢｎＴＯＴＰではある月数や年数が過ぎて設定されたブロック番号を超えるとＢｎｒが変化し自動的にＢｎＴＯＴＰが変化する。ただしこの場合でもＢｎＴＯＴＰを設定するＫＣなどが漏洩した場合に備えＫＣをコントラクトの管理者が設定できるようにするというＯＷＰ式と似た機能は必要になる。また端末３Ｄがブロックチェーンと接続できず正

しいブロック番号や時刻が測定できない場合はＢｎＴＯＴＰ方式は利用が困難であり端末３Ｄに設定されたＯＴＰ認証関数３０１８ＤＡを用いるＯＷＰ方式を利用することが好ましいかもしれない。

【０１６６】

前記パスワードＯＷＰを計算するには少なくとも以下の4つの変数をハッシュ関数ｆｈの引数に利用しパスワードＯＷＰを生成する。

ワンタイムパスワード生成にはトークン番号ＴＩＤＡ、

コントラクトに記録されたシークレットキー情報ＫＣ、

コントラクト管理者がある時刻に変えることの出来る変数ＢＣの３つの変数を必ず用いる。

そして端末１Ａの秘密鍵１０１Ａから計算されるユーザー識別子Ａを4番目の変数に加え、ユーザーＵＡのトークン番号ＴＩＤＡのＯＴＰトークンに固有のパスワードにできる。

ＴＩＤＡ、ＫＣ、ＢＣ、Ａの4つをハッシュ関数ｆｈの引数として、パスワードＯＷＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＢＣ，Ａ）としてハッシュ値ＯＷＰを生成し、ＯＴＰ生成関数はそれを戻り値として端末１ＡにＯＷＰを伝える。ここでＯＷＰを符号なし整数として型変換し、例えば7桁のパスワードとして１０の７乗で割ったあまりを7桁数字のパスワードＯＷＰ－ｎ７として伝えることもできる。ここで７桁ではなくｎ桁の場合はＯＷＰ－ｎと表記する。ハッシュ関数は実施例ではＳＨＡ２５６やＳＨＡ－３である。

実施例では引数の順に変数をエンコードし結合しそのデータのハッシュ値をＳＨＡ２５６関数などで求めている。エンコード順によりメッセージ情報は変わるので、引数をどのような順番でエンコードするかによってハッシュ値も変化する。

本発明ではパスワードＯＷＰになるハッシュ値を生成する変数がＴＩＤＡ、ＫＣ、ＢＣ、Ａの4つに由来していればよい。すなわちＴＩＤＡ、ＫＣ、ＢＣ、Ａを演算し、変数のデータの一部を省略し、またはハッシュ関数によってハッシュ化し加工し匿名化されたデータを引数としてもよい。

【０１６７】

重要な点としてユーザー識別子Ａを変数に加えた場合はトークンを譲渡するとハッシュ値を算出するシード値（ＯＴＰを計算するハッシュ関数の引数）のうちユーザー識別子部分が変化するため異なるパスワードＯＷＰが生成される。

例えば、ユーザー識別子ＡとＢとＣではそれぞれ識別子が異なるため引数にユーザー識別子を用いるＯＷＰを生成するＯＴＰトークンをＡからＢに譲渡できたとき、ユーザー識別子ＢがＯＴＰ生成関数で生成したＯＴＰとＡがＯＴＰ生成関数で生成したＯＴＰは異なる値となる。

一方で、ユーザー識別子をハッシュ関数ｆｈの引数に利用しない場合は、異なるユーザー識別子のユーザーにトークンを送信し譲渡すると半固定式パスワードＯＷＰの内容が変わらないため、同じパスワード値を共有してしまう。

例えると固定された秘密にされるべき暗証番号の書かれた紙や複製容易な金属製の鍵を譲渡するのと同じであり、紙に書かれた情報を複製したり、金属製鍵の形状をもとに合鍵が作製されていき、トークンが流通している場合にはその流通の途中で解錠可能な合鍵が無数に複製できてしまう。前記の鍵情報の複製を防ぐためユーザー識別子ＡをＯＴＰを計算するハッシュ関数ｆｈの引数に含めたり、もしくはユーザー識別子を含めない場合でもコントラクトの管理者が関数ｆｓｃｂ３０１２Ａを用いて手動である時刻ごとにＢＣ値３０１３Ａを書き換えていくことが求められる。

変数ＢＣをあるおおよその時刻、おおよその時間間隔で、手動もしくはコントラクトＣの管理者が自動化プログラムを用いてアクセスし変更する場合にはパスワードＯＷＰはＴＯＴＰに近いものになる。例としてコントラクトＣの管理者が擬似乱数を用いた自動化プログラムを用いておおよそ1日ごと、1週間ごと、1カ月ごと、数年ごとに定期更新することもでき、定期更新時の具体な日付の決定は擬似乱数を利用しながら決定しシード値を変えることも想定される（大まかにシード値の変更時期は決定しているがその詳細な変更時刻はランダム値やヒトの意志により決める）。これによりランダムさを伴った疑似的なＴＯ

ＴＰによる認証システムが提供できる。
【０１６８】
＜パスワードＯＷＰの認証と認証結果呼び出し＞
パスワードＯＷＰはウェブサイトでのログイン処理に用いたＢｎＴＯＴＰと同じく認証することもできる。ユーザー端末１Ａは端末３ＡのＯＷＰ型のＯＴＰトークンのＯＴＰ生成関数を含むコントラクトにアクセスしＯＷＰ型のＯＴＰを生成関数にて生成させる。そして生成関数で生成したＯＷＰとユーザー識別子Ａとトークン番号ＴＩＤＡをサービスを提供する３Ｄ（アクセス制御端末３Ｄ）にアクセスしＯＴＰ認証関数３０１８ＤＡの引数に入力する。
次にＯＴＰ認証関数の引数に入力されたＡ、ＴＩＤＡ、引数に入力されたＡｒｇＯＷＰ（またはｎ桁の整数値パスワードＡｒｇＯＷＰ－ｎ）から、ＯＴＰ認証関数３０１８Ａ内部でＴＩＤＡ、ＫＣ、ＢＣ、Ａをハッシュ関数ｆｈを用いてＶｅｒｉＯＷＰ（またはｎ桁の整数値パスワードＶｅｒｉＯＷＰ－ｎ）を求め、ＩＦ文などによる条件式で、ＡｒｇＯＷＰ（またはＡｒｇＯＷＰ－ｎ）がＶｅｒｉＯＷＰ（またはＶｅｒｉＯＷＰ－ｎ）と一致するか判定し、一致した場合には認証できた時の処理を行うこともできる。一致しない場合には認証できなかった時の処理を行う。
この処理は端末３Ｃの配信するウェブサイトへＢｎＴＯＴＰを用いてログインするときと似ているが、ネットワークに接続される端末３Ｃの配信するウェブサイトへＢｎＴＯＴＰを用いてログインするとき時はノード端末３ＡのＯＴＰ認証関数３０１８Ａや３０１８ＡＡを用いているが、ネットワーク２０から切断されうる端末３ＤにＯＷＰを提示するときはＯＴＰ認証関数３０１８ＤＡを用いるという違いがある。
（端末３Ｄがネットワーク２０に接続しノード３Ａと接続できるときは３０１８Ａや３０１８ＡＡを用いることもできる。）
【０１６９】
＜ＯＷＰを用いた紙製のチケット等の有価紙葉１８Ａの製造と利用、ＩＣタグ１９Ａ等デジタル機器による認証＞
ネットワーク２０を通じて端末１Ａとサーバ３Ａを用いてブロックチェーン上のＯＴＰ生成コントラクトからパスワードＯＷＰをＯＴＰ生成関数３００９Ａから生成する。そして生成されたパスワードＯＷＰとユーザー識別子Ａ、トークン番号ＴＩＤＡを文字列またはバーコードまたはその両方をプリンターなどを用いて紙等に印刷し、紙のチケットもしくは有価紙葉１８Ａを製造する。この時、印刷された１８ＡにはＯＴＰ生成コントラクト識別子やＯＴＰ生成トークンと対応するサービスの名称、印刷日時、有価紙葉の有効期限、サービス提供者の名称と連絡先、誤り訂正符号やＭＡＣ値等のサービスを提供するために必要な情報が印刷されていてもよい。
また有価紙葉１８Ａのバーコードに含まれる情報やＩＣタグ１９Ａに含まれる文字列情報のデータはＯＷＰ、Ａ、ＴＩＤＡの各変数を区切るための区切り文字を含んでいてもよい。またバーコードのデータを一部またはすべて、認証するサービス提供者のみが暗号化の鍵を知る形で暗号化していてもよい。
【０１７０】
有価紙葉１８Ａに含まれるＯＷＰ、Ａ、ＴＩＤＡの各変数をバーコードとして表示して印刷する場合は好ましくは２次元バーコードであり、複数または一つの１次元バーコードでもよく、カメラ等光学撮像素子４３０Ｄにて認証に用いる１８Ａに印刷もしくは印字されたバーコードとそのバーコードが含む数値や文字列情報を読み取ることができればよい。
【０１７１】
有価紙葉１８Ａに含まれるＯＷＰ、Ａ、ＴＩＤＡの各変数をバーコードとして表示して１Ａのディスプレイ１５０Ａの画面１５００Ａに表示してもよい。１５００Ａの表示内容を印刷し１８Ａとしてもよい。
１５００Ａのディスプレイ画面と１５００Ａの表示画面を印刷した１８Ａは端末３Ｄの３４０Ｄにバーコード（あるいは文字列）を読み取らせることで端末３Ｄへユーザー識別

子Ａとトークン番号ＴＩＤＡとパスワードＯＷＰを伝えてもよい。
【０１７２】
有価紙葉１８Ａに記録するユーザー識別子Ａとトークン番号ＴＩＤＡとパスワードＯＷＰの情報はＮＦＣタグ１９Ａ（ＩＣタグ・ＩＣカード１９Ａ）の記録装置に記録されていてもよい。そして１９Ａはサービスを提供する端末３Ｄの通信装置３２Ｄや３４１Ｄを介して端末３Ｄと通信しユーザー識別子Ａとトークン番号ＴＩＤＡとパスワードＯＷＰを端末３Ｄに伝えてもよい。
【０１７３】
有価紙葉１８Ａを端末３Ｄのカメラ・スキャナ装置３４０Ｄに提示し、あるいはＮＦＣタグ１９Ａを３４１Ｄおよび３２Ｄに提示したユーザーＵＡに対し、
端末３Ｄが１８Ａに記載されたユーザー識別子Ａやトークン番号ＴＩＤＡとパスワードＯＷＰの情報を３４０Ｄを経由して読み取り端末３Ｄの記憶装置３０Ｄの認証関数３０１８ＤＡ（図３ＤＡの３０１８ＤＡ）の引数ＴＩＤＡ、ユーザー識別子Ａ、パスワードＡｒｇＯＷＰとして変数を渡し、
ＯＴＰ認証関数３０１８ＤＡ内部ではフローチャート図６Ｆあるいは図６Ｄの処理に従い、ＡｒｇＯＷＰに対し端末３Ｄに記録されたＫＣなどのシークレット変数のシード値と３０１８ＤＡの引数であるユーザー識別子Ａやトークン番号ＴＩＤＡを用いてＶｅｒｉＯＷＰを計算し、３０１８ＤＡに入力されたＡｒｇＯＷＰとＶｅｒｉＯＷＰが一致するか判定し、
一致するときにはＯＴＰ認証が成功したときの戻り値３０２１ＤＡを関数の戻り値ＣＴＡＵとして返し、３０２１ＤＡを返す前に３０２２ＤＡを実行するときは実行させる。
また３０１８ＤＡに入力されたＡｒｇＯＷＰとＶｅｒｉＯＷＰが一致するか判定し、一致しないときにはＯＴＰ認証が失敗したときの戻り値３０２１ＤＡを関数の戻り値として返す。
【０１７４】
端末３Ｄは３０１８ＤＡの関数の戻り値３０２１ＤＡや３０２２ＤＡに従って、ＯＴＰ認証が成功した場合の３０２１ＤＡを得たとき、有価紙葉１８Ａをカメラ３４０Ｄに提示もしくはＮＦＣタグ１９Ａを３４１Ｄおよび３２Ｄに提示したユーザーＵＡに対して、アクセス制御装置または始動装置または開閉装置もしくは施錠及び解錠を行う施解錠装置３５０Ｄを操作する。
３０２１ＤＡがＯＴＰ認証が成功した場合の値であるとき、端末３Ｄは開閉や施錠等のアクセス制御を行う部分３５０Ｄに対し制御を行い、改札や入場口ではユーザーＵＡが入場・退場出来るようゲート装置を開閉する。施錠等のアクセス制御を行う部分３５０Ｄが建物の扉や自動車のドア、自動車の原動機や電子計算機の始動装置である場合はその施錠を解錠し、装置や施設や設備の利用を可能にする。施錠された部分３５０Ｄが金庫など容器であるときは金庫の施錠を解錠する。
【０１７５】
３０２１ＤＡがＯＴＰ認証が成功した場合の値であるとき、端末３Ｄは施錠された部分３５０Ｄを解錠するとともに３５１Ｄや３５２Ｄを用いて光や音にてユーザーＵＡや端末３Ｄの周囲に解錠ができたことを知らせることができる。
３０２１ＤＡがＯＴＰ認証が失敗し入場できない場合の値の場合、３５１Ｄや３５２Ｄを用いてＯＴＰ認証が失敗した場合の光や音もしくは無線標識を発して認証が失敗したユーザーの存在を周囲に知らせることができる。
さらに防犯カメラ等３４２Ｄを利用できる端末３Ｄでは１８Ａや１９Ａを端末３Ｄに提示したユーザーＵＡの風貌の撮影などもできる。３４２Ｄを用いる用途として大型金庫・金庫室やコンピュータ端末・産業用の加工装置など装置や設備、建物の扉など施錠装置、自動車の施錠装置、改札や入場口（入場口・退場口、入退場口）である。
３４２Ｄを用いるのが困難であり、用いないこともある例としては電源の制約やプライバシーに配慮した建物や自動車の施錠装置や入場口であり、電池電源の制約があって３４２Ｄの大きさの制約から搭載することが困難な金庫（一部の家庭用金庫、手提げ金庫）な

ど容器の施錠装置や、錠前型の施錠装置（南京錠型、ワイヤーロック型などの小型の錠前）である。
３４２Ｄを用いたカメラによる監視は本発明において必須ではないが、改札や入場口など防犯上必要である用途には利用されることが好ましい。
【０１７６】
端末３Ｄに施錠を解除する装置３５０Ｄがなく、例えば入場口・退場口や改札口がヒトの手で警備され入退場を管理する場合においては３０２１ＤＡがＯＴＰ認証が成功した場合の値であるとき、３５１Ｄや３５２Ｄを用いて光や音にてユーザーＵＡや端末３Ｄの周囲のユーザーや警備を行う者に解錠ができたことを知らせることができる。
また３０２１ＤＡがＯＴＰ認証が失敗し入場できない場合の値の場合も、３５１Ｄや３５２Ｄを用いてＯＴＰ認証が成功した時とは異なる失敗した場合に専用の光や音を発して認証が失敗したユーザーの存在を周囲に知らせることができる。
さらに防犯カメラ等３４２Ｄを利用できる端末３Ｄではユーザーの風貌の撮影などもできる。
【０１７７】
ユーザーＵＡの風貌を記録する防犯カメラ３４２Ｄ（図８Ｂの３４２Ｄ）は駅の改札や入場口の入場処理などにおいて必要な機能であって、金庫などの容器に端末３Ｄを組み込む場合は防犯カメラ３４２Ｄは必要ない場合がある。また同じく自動車の施錠や建物の施錠装置に端末３Ｄを用いる際もプライバシーに配慮して搭載しないこともある。
【０１７８】
端末３Ｄはサービスの提供状況をユーザ識別子Ａ及びトークン番号ＴＩＤＡとサービス提供時刻Ｔ、サービスを行った回数３０１７ＤＡ（もしくはサービスを行った回数とそのサービスの価格値、防犯カメラ３４２Ｄを用いるときはユーザーの風貌情報）とを対応付けて記録するデータベースもしくは台帳部３１１６Ｄを端末３Ｄを備えることが好ましい。
サービス提供時刻を正しく記録する場合にはＪＪＹやＧＮＳＳ、ＮＩＴＺ等を受信させ、あるいはヒトの手で端末３Ｄの時刻を補正する必要がある。端末３Ｄが電池で動作する場合は、電力の制限から時刻情報が使えないという理由でサービス提供時刻Ｔの記録を行わない形態も考えられる。金庫などに内蔵する端末３Ｄは時刻情報が使えない場合もありうる。
【０１７９】
ただしデータベースまたは台帳部３１１６Ｄは家庭用金庫や手提金庫あるいは錠前といった用途に用いる場合は、端末３Ｄの制御装置・記憶装置の容量と価格などの経済性を考慮して３１１６Ｄを搭載しないことがある。
また電子計算機や自動車や建物の施錠装置もしくは金庫等容器に備えられた端末３Ｄの３１１６Ｄの情報から、何回解錠処理・始動処理を行ったか、あるいはどの時刻に何回解錠処理を行ったかを端末１Ａの有線通信装置（無線通信装置でも可）を用いて端末３Ｄにアクセスすることで端末１Ａの利用者が知ることができるかもしれない。有線通信のほかに端末１Ａと端末３Ｄの間で暗号化された無線通信を行い３Ｄの状態や解錠処理の履歴を調べることができる。３１１６Ｄといった端末３Ｄの解錠履歴から１Ａのユーザー以外のユーザーがＯＷＰを用いたＮＦＣタグ１９Ａを用いて不正に解錠されていたかどうかを知ることができる。
端末３Ｄに紙等による解錠鍵１８Ａを読み取るカメラが備えられている場合は紙等による解錠鍵１８Ａを用いて解錠されたかどうかが分かる。
【０１８０】
端末３Ｄは改札や入場口の端末として利用される際に、端末３Ｄがネットワーク２０に接続され端末３Ａと接続できるとき、端末３Ｃのウェブサイトへのログイン監視部と同じく不正なアクセスおよび入場を監視する機能を３０１Ｃや３１１Ｃの内部に備えることもできる。
また３Ｃや３Ｄはネットワーク２０に接続している場合にノードとなる端末としての装置を備えているときに３Ａや３Ｂと同じくブロックチェーンのノードとなることができ、

その際にはブロックチェーンに関する記録部と制御部（３００Ｄや３００Ｃと３１０Ｄや３１０Ｃ）を持つこともできる。

【０１８１】

端末３Ｄは改札や入場口として利用される際に、３Ｄが改札や入場口を持つ施設内のローカルエリアネットワークに接続されるとき、

端末３Ａのブロックチェーンに関する記録部と制御部と同じブロックチェーン基盤を用いた３Ａや３Ｂに記載されるブロックデータとは異なるブロックチェーン部３００Ｄと３１０Ｄを持ち、

前記３００Ｄの内部には、ネットワーク２０上で端末１Ａが端末３ＡにアクセスしＯＷＰを生成するのに用いるハッシュ関数ｆｈやシード値ＫＣやＢＣなどをもつ認証関数３０１８ＤＡを持つ３００８ＡＡに類似の認証コントラクトを備えていてもよい。

端末３ＡにＯＴＰ生成トークンのコントラクト３００８ＡＧをデプロイし、端末３Ｄに３００８ＡＧと同じ方法でＯＴＰの計算を行い認証するＯＴＰ認証関数３０１８ＤＡを備えた認証コントラクトをデプロイし前記二つのコントラクトのシード値を同期させ１５００Ａや１８Ａや１９Ａの認証を行い入場などの処理を行ってもよい。

【０１８２】

＜ＩＣタグ等デジタル機器による認証＞

ＮＦＣタグ１９Ａは近距離無線通信装置（ＮＦＣ装置）としてユーザー識別子、トークン番号、パスワードＯＷＰを書き込むことの出来る接触式ＩＣカード、非接触式ＩＣタグ（ＲＦＩＤタグ）、非接触式ＩＣカード（ＲＦＩＤカード）が利用できる。

【０１８３】

ＮＦＣタグ１９Ａは自動車等に使われうる。自動車に対し１９Ａを用いてリモートコントロールにて自動車に搭載された端末３ＤにＯＷＰ認証情報を暗号化された無線通信により送信し３ＤでＯＷＰの認証を行い自動車の施錠装置３５０を解錠しあるいは原動機を始動させる用途に用いる場合、１９Ａは電池を備え、解錠もしくは施錠またはその両方を入力できる押しボタン等の入力装置を備え、ボタンを押したときに無線にて通信していること（および電池が消耗しているかどうか）を示す出力装置として発光ダイオード等の発光素子を備える。ここで自動車の鍵は１９Ａの一つの例であり建物の扉や金庫あるいは設備にも利用されうる。

端末３Ｄが自動車の施錠や始動を管理する端末である場合を例とすると、前記端末３Ｄは電気自動車のドアの施錠を解除し電気自動車のモータを動作させるモータ駆動回路を制御する端末でもよいし、エンジン車（熱機関を用いる自動車）のドアの施錠を解除しセルモータなど電動によりエンジンを始動させる装置の制御端末でもよいし、エンジンを減速もしくは徐々に停止させる制御を行える電子計算機端末でもよい。モータもしくはエンジンを航続距離や速度に応じて制御する端末３Ｄであって本発明の認証システムを用いて認証できたときに航続距離や速度上限といった制限をなくすことができてもよい。

【０１８４】

ＮＦＣタグ１９Ａは電池や入出力装置を備えない形態も考えられる。例として１９ＡはＩＳＯ１４４４３タイプＢに準拠したカード型デバイスまたはタグ型デバイスであることも考えられる。

既知の技術としてＩＳＯ１４４４３タイプＢという非接触ＩＣカード技術では、カード型もしくはタグ型デバイスに通信および電力受信用のアンテナコイルが形成されている。電力の供給は電磁誘導によりＮＦＣタグのリーダー・ライター（端末３Ｄにおいては３Ｄの通信装置３２ＤもしくはＮＦＣタグの信号受信部３４１Ｄ）からＮＦＣタグ１９Ａのアンテナコイルを通じてＮＦＣタグ１９Ａに供給されるので電池を利用しない。

【０１８５】

ＮＦＣ１９Ａは本発明のＯＴＰ認証のほかに別途必要な情報を備えていてもよい。具体的にはＮＦＣタグ１９Ａに秘密鍵１０１Ａ２を持ち、ＯＷＰ型のＯＴＰ認証を行い自動車のドアの解錠後に原動機始動時にＮＦＣにて通信し端末３Ｄが１０１Ａ２を用いてインターネットワーク２０と接続し、ブロックチェーンのノード３Ａにて、１０１Ａ２に割り当

てられたＢｎＴＯＴＰ型のＯＴＰトークンを用いてＴＯＴＰによる認証を行い、ウェブサイトへのログインと同じく自動車のオペレーティングシステムにログインすることでを始動させ、自動車を起動させてもよい。前記の場合はネットワーク２０に常時接続できることが条件となる。インターネットワーク２０に接続される自動車において利用されうる。

自動車がＢｎＴＯＴＰ型の認証を行い原動機を始動させる場合に、ネットワーク２０が利用できない場合（通信障害や災害等の発生時）においてもユーザーＵＡがＮＦＣタグ１９Ａを用いて自動車を動かせるようにする必要がある。そこでＮＦＣタグ１９Ａに記憶されたユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰをもちいてＯＷＰ型のＯＴＰ認証を行い、予め自動車製造者により設定された航続可能距離にしたがって自動車の走行させるといった制限を与えて原動機を始動させてもよい。

【０１８６】

ＮＦＣ１９Ａは本発明のＯＴＰ認証のほかに別途必要な装置や処理部を備えていてもよい。例としてＩＳＯ１４４４３タイプＢとして動作させる装置や、自動車のキーレスエントリーシステムを実現するための無線通信装置および無線信号の暗号化などの処理は用途に応じて別途追加され利用される。

【０１８７】

本発明において近距離無線通信装置が用いる無線の周波数は本発明では特に制限しない。近距離無線通信装置は既知の無線通信技術によれば１３０ｋＨｚ帯、１３．５６ＭＨｚ帯、４３３ＭＨｚ帯、９００ＭＨｚ帯、２，４ＧＨｚ帯等を利用できる。無線周波数について具体的には１３．５６ＭＨｚ帯を用いて非接触型のＩＣタグ、ＮＦＣタグとして利用されるが、１３．５６ＭＨｚ以外の無線周波数でもよい。例えば２．４ＧＨｚ帯を利用してもよい。

ＮＦＣにかかわる規格の具体例として１３．５６ＭＨｚ帯の規格としてISO/IEC18092、ISO14443タイプA、ISO14443タイプＢ等がある。２．４ＧＨｚ帯ではＩＥＥＥ（Institute of Electrical and Electronics Engineers ）の８０２．１１系や８０２．１５．１系の既知の無線通信規格がありそれらを本発明で利用することもできる。

【０１８８】

本発明のＮＦＣタグ１９Ａは実施形態では１３．５６ＭＨＺ帯と２．４ＧＨｚ帯が利用されうる。ＮＦＣタグ１９ＡはＩＳＯ１４４４３タイプＢに準拠して１０ｃｍ程度の距離で３Ｄの通信装置３２Ｄおよび３４１Ｄと通信できる。しかしＮＦＣタグ１９Ａが無線パーソナルエリアネットワーク（無線ＰＡＮ、Wireless Personal Area Network）を用いる場合は通信距離は１０ｃｍを超えることもある。

【０１８９】

ＮＦＣタグ１９Ａがウェアラブルコンピュータ（Wearable Computer）端末に含まれていてもよい。もしくは１９Ａの機能をもつウェアラブルコンピュータ端末であってもよい。

例としてコンピュータ端末１Ａとウェアラブルコンピュータ端末１ＢとＮＦＣタグ１９Ａがあるとき、

ＮＦＣタグ１９Ａがウェアラブルコンピュータ端末１Ｂの１６Ｂの外部記憶装置として接続され、１６Ｂの代わりに１９Ａが１２Ｂと接続され、

ＮＦＣタグ１９Ａの記憶装置に端末１Ａが通信装置１Ｂを介してアクセスし、

ＯＷＰを用いた認証に必要なユーザー識別子、トークン番号、パスワードＯＷＰを書き込む事が出来てもよい。

もしくはウェアラブルコンピュータ端末１Ｂがインターネットワーク２０を介してサーバ端末３Ａにアクセスし ＯＷＰを生成した後、

前期パスワードＯＷＰ、ユーザー識別子、トークン番号を書き込むことが出来てもよい。

【０１９０】

本発明で用いるウェアラブルコンピュータ（wearable computer）端末の種類（利用用途及び形状）に制限はないが主に腕輪型および腕時計型（腕輪もしくは型端末であるスマートウォッチにＮＦＣタグ１９Ａの機能が備えられたもの）、指輪型（指輪もしくは指輪

型端末にＮＦＣタグ１９Ａが備えられたもの）、ベルト型（ベルトにＮＦＣタグ１９Ａが備えられたもの）、衣服型（衣服にＮＦＣタグ１９Ａが貼り付けもしくは編み込まれたもの、縫い付けられたもの）、靴型（履物の表面にＮＦＣタグ１９Ａが備えらたもの、もしくは靴のインソール部分にＮＦＣタグ１９Ａが備え付けられたもの）などである。

【０１９１】

例として、ヒトの頭部に関係するウェアラブルコンピュータとして帽子型・ヘルメット型、眼鏡型・ヘッドマウントディスプレイ型、補聴器・イヤホン型、マスク型、装身具型（ペンダント、首飾り、懐中時計型など）があり、装身具の例として社員証などの身分証となるＮＦＣタグ１９Ａを入れたカードケースをペンダントのように身に着けるストラップを組み合わせた身分証型ネックストラップがある。

ヒトの手に関係するウェアラブルコンピュータとしてブレスレット型、腕時計型、手袋・グローブ型の１９Ａがある。

ヒトの足に関係するウェアラブルコンピュータとしてアンクレット型、靴下型、履物のインソール型、履物の表面にＮＦＣタグ１９Ａを備えた履物型の１９Ａがある。

ヒトの衣服に用いる衣服型や身体の一部に巻くことで身に着けることができベルト型の１９Ａがある。身体の素肌や衣服に張り付けるシールもしくはテープ型の型のＮＦＣタグ１９Ａでもよい。

【０１９２】

ウェアラブルとは言えないが身に着けられる装置という観点から見た場合にＮＦＣタグ１９Ａを備えたスマートフォン型やタブレット型の携帯型コンピュータ端末４Ａでもよいし、社員証でもあるＮＦＣタグ１９Ａや財布型ＮＦＣタグ１９Ａ、鞄型ＮＦＣタグ１９Ａでもよい。１９Ａをある装置やモノの内部に搭載することで認証に利用できる。もしくは粘着性のテープや接着剤を備えたＮＦＣタグ１９Ａをある装置やモノの表面に張り付けられたＮＦＣタグ１９Ａとして利用できる。

（例として紙のチケット１８Ａに、１８Ａと同じ情報を記録させたシール型・フィルム型１９Ａを粘着性のある両面テープや接着剤で張り付けることで、ヒトの目による目視、カメラによる読み取り、ＮＦＣによる読み取りに対応した紙のチケットを製作できる。）

【０１９３】

ウェアブルコンピュータ端末は電源装置に電池を用いなくてもよいし、一次電池を用いてもよいし、充電可能な二次電池を用いていてもよい。充電については充電元からの有線による充電でもよいし、ワイヤレス電力伝送によって充電してもよい。端末に備えられた環境発電機能を用いて充電できてもよい。

【０１９４】

ＮＦＣタグ１９Ａは電源装置に電池を用いなくてもよいし、一次電池を用いてもよいし、充電可能な二次電池を用いていてもよい。充電については充電元からの有線による充電でもよいし、ワイヤレス電力伝送によって充電してもよい。１９Ａに付属の環境発電機能を用いて充電できてもよい。

【０１９５】

ＮＦＣタグ１９Ａは記憶装置に記録したパスワードＯＷＰ、ユーザー識別子、トークン番号を消去しすることができる。そして最新のパスワードＯＷＰ、ユーザー識別子、トークン番号を記録してもよい。

ただしＮＦＣタグ１９Ａがサービス提供者に配布される形式の場合は記録装置の内容の書き換えを禁止してもよい。

【０１９６】

＜有価紙葉１８Ａの製造＞

１８Ａの製造に関してはユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰを認証に用いるとき、識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰを区切り文字などを添えつつ連結して二次元バーコードもしくは複数の一次元バーコードに変換し紙に印刷する。この時、紙にはバーコードのほかにバーコードに変換する前の文字列データを可読可能な状態でバーコードと共に印刷してもよい。

またバーコードの内容はサービス提供者のみが復号する鍵を知る形で暗号化していてもよい。実施例では特許２９３８３３８等に記載の二次元バーコードを用い、紙のチケットのバーコード部分を形成し、レーザープリンターもしくはインクジェットプリンターにて印刷し、紙のチケットを製造した。

【０１９７】

１８Ａの印刷に用いるプリンタ１５２Ａの印刷方式やメディアとなる紙などの種類は問わず、バーコードがカメラやスキャナを用いてユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰとして読み取れることが必要である。１５２Ａがサーマルプリンタの場合は紙は感熱紙などを用いネットワークと接続された現金自動預け払い機ＡＴＭなどの感熱紙を利用する装置においても本発明の紙製チケットを印刷、印字して製造することもできる。また店舗などに備え付けのネットワークと接続された複写機や電話回線網と接続されたファクシミリにおいても、チケットの印刷データを記録した外部記録装置を接続しチケットデータを読み込むことができれば印刷可能である。

チケットデータを店舗などに設置されたコンピュータとしての機能を備える複写機やファクシミリ等で暗号化されたネットワークを通じてインターネット経由でチケットを発行し、またはユーザーが店舗の装置に持ち込んだ外部記録装置からデータを読み込んで印刷してもよい。

【０１９８】

＜デジタル機器が無い、または使えない環境への対応＞

ＯＷＰを用いる利用例（主に図８Ｂの利用例）において、デジタル機器を持たないユーザーに対してはトークンの発行をサービスを行う法人や発券を行う法人等が有価紙葉１８ＡもしくはＮＦＣタグ１９Ａの製造をユーザーの代わりに行い、ユーザーへ１８Ａをファクシミリや郵送にて送付できる。また１９Ａを郵送配達できる。１８Ａや１９Ａを送付された顧客は端末３Ｄの備えられたサービス提供窓口や装置を１８Ａや１９Ａを提示することで利用できる。

【０１９９】

例として、顧客がインターネットワーク２０とコンピュータ端末１Ａ、端末１Ａに接続できるプリンタを持たず電話回線とファクシミリ装置のみを備える場合には、サービスの提供者が秘密保持を約束し、顧客のパスワードＯＷＰ等の本発明の紙チケット作成に必要なデータを顧客から問い合わせて、顧客のファクシミリ番号を基にチケットデータを送付しファクシミリにて紙のチケットを出力することもできる。

【０２００】

＜デジタル機器がない時の１８Ａや１９Ａの作製依頼＞

ユーザーがデジタル機器を持たず装置１Ａやプリンターを持たない顧客の場合には、顧客のトークンを管理することの出来るサービスの提供者が郵送や電話などで契約する。ここでサービス提供者（またはサービス提供者とは独立したトークン保管会社）がユーザーの秘密鍵の文字列、ユーザ識別子等を信書にて送付してもよい。そしてチケットの販売とトークンの交付の秘密鍵への発行をサービス提供者が行い、サービス提供者（またはサービス提供者とは独立したトークン保管会社）はユーザーがトークンのパスワードＯＷＰ等を印刷した紙のチケットのデータを作成し、ユーザのファクシミリ番号に送信し、ユーザーのファクシミリで紙のチケットを製造できる。ファクシミリがなく電話番号のみの場合は郵送または手渡しにて紙チケット（もしくはＩＣカードやＩＣタグ式のチケット）を信書の形で渡す。

（トークンがチケットの場合は、トークンおよびそこから生成されるパスワードＯＷＰを印刷した紙は有価物でありそれを管理する資格が必要になる恐れがある。また秘密鍵をサービス提供者とユーザーの間で共有することになりうる場合も資格が必要になる恐れがある。）

【０２０１】

具体的に説明する。サービス提供者の端末３Ｄに提示する１８Ａや１９ＡをユーザーＵＡ入手したいとき、ユーザーＵＡが端末１Ａや４Ａなどを持たず、電話回線も持たず、ネ

ットワーク２０とも接続できない時がありうる。前記の場合、ユーザーＵＡは秘密鍵１０１Ａを信頼できる第三者ＵＢに発行させ、その第三者ＵＢに秘密鍵１０１Ａを信託させ、１０１Ａの保管と運用を依頼し、さらにサービスに対応したトークン番号ＴＩＤＡのＯＴＰトークンを１０１Ａのユーザー識別子Ａに当てて発行させる。

そして第三者ＵＢは前記ユーザー識別子Ａに発行されたＯＴＰトークン用いてサーバ３Ａのブロックチェーンにアクセスし ＯＴＰ生成関数からＯＷＰを取得し１８Ａや１９Ａを製造してユーザーＵＡの指定する住所や指定する場所へ郵送配達してもよい。郵送配達する際に１９Ａや１８Ａと共に１０１Ａを記録した信書を添付してもよい。第三者ＵＢが店舗でユーザーＵＡに直接１８Ａや１９Ａを提供してもよい。（この運用形態は技術的な問題はないが、秘密鍵１０１Ａを信託できる第三者ＵＢは法令で規制され資格が必要となるかもしれない。）

【０２０２】

また、第三者１０１Ｂがユーザー識別子Ｂを名義としてトークン番号ＴＩＤＡのＯＴＰトークンを発行し、前記トークンのＯＷＰから１８Ａや１９Ａを発行しユーザーＵＡの指定する住所や指定する場所へ郵送配達してもよい。第三者ＵＢが店舗でユーザーＵＡに直接１８Ａや１９Ａを提供してもよい。（この運用形態も技術的には問題はないが、ユーザーＵＡのトークン番号ＴＩＤＡのＯＴＰトークンを預かる第三者ＵＢは法令で規制され資格が必要となるかもしれない。）

【０２０３】

１５００Ａを表示することの出来る１Ａを、有価紙葉１８ＡやＮＦＣタグ１９Ａを郵送配達することの代わりに郵送配達配布できる。端末１Ａといった装置を持たないを持たない顧客が、電話や店舗での会話を基に第三者ＵＢ（ここでは通信会社やコンピュータまたはスマートフォン製造販売会社を含む）に端末１Ａの購入と何かに基づくＯＴＰトークンの購入を同時に契約し、第三者ＵＢは１５００Ａを表示できる端末１Ａをユーザーに販売し、１５００Ａを表示できる端末１ＡをユーザーＵＡの住所や指定する住所もしくは店舗の窓口での直接渡してもよい。

【０２０４】

＜店舗における発券装置＞

ネットワークと接続された現金自動預け払い機ＡＴＭ端末や印刷装置の備え付けられた端末が設置される店舗（例としてコンビニエンスストア等）にて、デジタル装置を持たないユーザーに対してＯＴＰトークンの購入及び発行とチケット等有価紙葉１８Ａの製造ができてもよい。

具体的には店舗などでチケットなどの料金の支払いが行われた後に顧客情報（ＯＴＰトークンの発行先であるユーザー識別子Ａ）を入力しブロックチェーンへの秘密鍵１０１Ａやユーザー識別子Ａの文字列情報、パスワードＯＷＰ等の紙チケットに必要な文字列およびバーコード情報を紙のチケットを印刷しユーザーに出力する。

次回に再度その端末を使ってチケットを作る場合は、端末のカメラもしくはスキャナにユーザー識別子Ａの情報が記録された紙や端末１Ａのディスプレイ部分をバーコードの形で読み込ませるか手入力してトークンの発行先のユーザー識別子を指定して新たなチケットのトークン発行を行う。

（なおＡＴＭ端末がユーザーＵＡを識別できＯＴＰトークンを発行するユーザー識別子Ａが決まっている場合にはＡＴＭ端末が備える顔認証などの生体認証手段をもちいてＯＴＰトークン及び１８Ａを発行することもできる。ただしその場合は生体認証を用いるのでだれがどのサービスに対応するＯＴＰトークンを利用しているか分からないよう配慮し、個人情報の匿名化などを行う必要があるかもしれない。）

【０２０５】

ここでサービス提供端末の処理の自動化・高速化を行い、入退場口や改札で取り扱いできるチケットの処理数を増やすという観点からは、秘密鍵１０１Ａとユーザー識別子Ａといった情報をカメラ・スキャナ等４３０Ｄで撮影する方式よりは、ＩＣカードに記録しＮＦＣタグ１９Ａなどを用いて無線通信を用いて非接触で行える事が好ましいかもしれない

。ＩＣカード１９Ａにはクレジットカード、デビットカード、プリペイドカードなどの決済に関する機能を備えていてもよく、非接触にて決済できるＮＦＣを用いるＩＣ式クレジットカード等でもよい。１９Ａが個人番号カードのようなＮＦＣをもちいた身分証カードでもよい。

【０２０６】

１９Ａは秘密鍵１０１Ａを記録していてもよい。ただし、１９Ａに秘密鍵１０１Ａを記録する場合には店舗や店舗内の他の顧客、あるいはＮＦＣを介してに秘密鍵１０１Ａが漏洩しないことが必要である。１９ＡをＰＩＮにより暗号化することで秘密鍵１０１Ａを暗号化して記録させ、１０１Ａを他者に読み取られないようにする事が必要である。

【０２０７】

そこでＩＣカード１９ＡもしくはＮＦＣタグ１９Ａに秘密鍵１０１Ａは搭載せず、秘密鍵から公開鍵を経て生成されるユーザー識別子Ａのみを搭載する方法も考えられる。この場合は紙等にブロックチェーン基盤の形式に沿って生成させた秘密鍵１０１Ａとユーザー識別子Ａを記録させ、ユーザー識別子Ａのみをカード発行装置または発行会社にバーコードの形で読み取らせ、ユーザー識別子Ａを記録したクレジットカード・プリペイドカード機能を持つＩＣカード等１９Ａを発行し、これを用いて店舗等のＡＴＭもしくはそれに類する端末においてＯＷＰを生成するＯＴＰトークン発行と、ＯＴＰトークンによるパスワードＯＷＰを含む紙のチケット等有価紙葉１８Ａの印刷及び発券が、非接触ＩＣカードを端末にかざして端末からアクセスさせた後に入力画面から行えるようになる。
チケットに限らず紙の券など有価紙葉１８Ａの形で本発明の認証を用いてサービス、役務の提供ができるものであれば適用できる。

【０２０８】

＜有価紙葉１８ＡとＮＦＣタグ１９Ａの利用と用途＞

有価紙葉１８Ａに記録される二次元バーコードはカメラなどを用いたスキャンを行いサービス提供者がカメラを用いてバーコードからユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰの３つの変数を検出し、前記3つの変数を端末３Ｄに入力し端末３Ｄに内蔵された認証関数３０１８ＤＡを用いて認証する。

あるいは端末３Ｄがネットワーク２０を介してノード端末３Ａに接続できるときは前記3つの変数をウェブアプリなどに入力し、ウェブアプリからブロックチェーンのコントラクトに問い合わせを行い認証関数３０１８Ａに3つの引数を入力する。
ここで端末３Ｄにおいて３０１８ＤＡもしくは３０１８Ａの認証関数によって認証処理を行い認証する工程において、二次元バーコードを用いる理由は二次元バーコードをカメラなどで認識させ３つの認証用変数の入力を端末３Ｄに行わせることで認証結果を得られるように自動化（および高速化）するためのものである。

【０２０９】

文字列のみを記した１８ＡをＡ４紙サイズのイメージスキャナ装置にてスキャンし、そのスキャンされた情報から文字列を画像認識し、ユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰを識別できれば二次元バーコードが無くとも端末３Ｄに入力することができうる。

【０２１０】

サービスを提供しなければいけないユーザーの総数が少ない場合には、バーコードが無く、文字列のみ書かれたチケットを提示されたとしても、対応するサービス提供者の労働力が十分であればヒトの手作業でユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰを端末３Ａや端末３Ｄの認証関数の引数に代入させ認証することができる。（また二次元バーコードの印字部分が読み取れなくなってしまった紙のチケットに対しても文字列が併記されていればサービス提供者の手で認証作業ができる。）

【０２１１】

有価紙葉１８Ａに印刷の形でユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰといった情報を記録することができほか、磁気ストライプを１８Ａに備えさせ、１８Ａの磁気ストライプにユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰを保

存してもよい。同様にカード型のＮＦＣタグ１９ＡまたはＮＦＣカード１９Ａにも磁気ストライプを備え、ユーザー識別子Ａ、トークン番号ＴＩＤＡ、パスワードＯＷＰといった情報を記録してもていてもよい。

【０２１２】

端末３Ｄが建物の扉や自動車の施錠装置もしくは金庫など容器の施錠装置であってその装置の利用者であるユーザーＵＡのユーザー識別子Ａや施錠装置端末３Ｄの製造番号やシリアル番号等に対応するＯＴＰトークンのトークン番号ＴＩＤＡを端末３Ｄに記録してもよい。

【０２１３】

端末３Ｄの記憶装置３０ＤにユーザーＵＡのユーザー識別子Ａやトークン番号ＴＩＤＡを記録させ、それを用いて、３０１８ＤＡを用いて認証処理を行う前に入力されたユーザー識別子情報やトークン番号と一致するか調べることで、本来利用されるべき３０Ｄに記録されたユーザーＵＡのユーザー識別子もしくはトークン番号のＯＷＰのみを受け付けるようにすることができる。

【０２１４】

端末３Ｄの記憶装置３０ＤにユーザーＵＡのユーザー識別子Ａやトークン番号ＴＩＤＡをユーザーＵＡが端末３Ｄに記録させ、それを用いて、３０１８ＤＡを用いて認証処理を行う前に入力されたユーザー識別子情報やトークン番号と一致するか調べることで、ＯＴＰトークンがユーザーＵＢからＵＡに譲渡されたとしても、譲渡前のユーザーＵＢの知るユーザー識別子ＢとトークンＴＩＤＡとＯＷＰから作成されたＮＦＣタグ１９Ａでは解錠できなくなるようにする事もできる。

【０２１５】

建物の扉や金庫などの容器を解錠した際に端末３Ｄにアクセスできる通信装置３２Ｄの有線通信端子があって、３２Ｄを介して有線通信によりユーザーＵＡの端末１Ａからユーザー識別子Ａやトークン番号ＴＩＤＡを端末３Ｄの記録部３０Ｄに記憶させた後、端末３ＤにユーザーＡやトークン番号ＴＩＤＡとパスワードＯＷＰを記録させたＮＦＣタグ１９Ａをかざし、１９Ａに記録されたユーザー識別子Ａとトークン番号ＴＩＤＡとパスワードＯＷＰを３０Ｄに記録されたユーザー識別子Ａやトークン番号ＴＩＤＡと照合し、ユーザー識別子Ａまたはトークン番号ＴＩＤＡが３０Ｄに記録された値と一致する場合には認証関数３０１８ＤＡを動作させ、ユーザー識別子ＡとトークンＴＩＤＡとパスワードＯＷＰを３０１８ＤＡを用いてＯＷＰが正しいか検証し、正しい場合には施錠を解錠させる。

前記３２Ｄの有線通信端子からユーザー識別子やトークン番号を自由に設定でき、前記有線通信端子を備えた端末３Ｄを備えた解錠された金庫などをユーザーＵＡがＵＢに譲渡した場合はトークン番号ＴＩＤＡのトークンをＵＢの端末１Ｂに譲渡し、ＵＢは解錠された金庫の有線通信端末部分を用いてユーザー識別子ＢとトークンＴＩＤＡを設定することで、ユーザー識別子ＢとトークンＴＩＤＡと前記ＢとＴＩＤＡより生成されたＯＷＰを用いて端末３Ｄを解錠するようにできる。ここで端末３Ｄは元の持ち主であるユーザーＵＡのユーザー識別子Ａは受け付けなくなりユーザーＵＡの端末１Ａの保有する（記憶する）ＯＷＰは利用できなくなる。

【０２１６】

端末３Ｄの３０Ｄに記録されたトークン番号は認証関数３０１８ＤＡを動作させるための施錠装置では防犯上、トークン番号は施錠装置の製造番号に対応していてもよい。

その例として自動車の場合には自動車の製造番号とトークン番号を対応させ、端末３Ｄの記憶装置３２Ｄの一度しか書き込めないＲＯＭに自動車製造番号と対応したトークン番号を記録させ、ＲＯＭに記録されたトークン番号を読み出して３０１８ＤＡの認証関数の引数のトークン番号として常に利用させるようプログラムしてもよい。

ここでＲＯＭは端末３Ｄの記憶装置３２Ｄとして原動機や自動車を制御する端末として一体化され樹脂などで封止・封印し悪意のある攻撃者によってＲＯＭの情報やＲＯＭそのものを取り換えられないようにする事が好ましい。ＯＴＰトークンのトークン番号と自動

車の製造番号が常に一致することで自動車の流通管理や防犯に役立つかもしれない。
【０２１７】
端末３Ｄは施錠された装置に組み込まれている場合、施錠を解錠してアクセスできる部分に通信装置３２Ｄまたは入力装置や出力装置を備える。３Ｄの記憶装置にはユーザー識別子、トークン番号、シークレット変数ＫＣやＢＣが記録されており、施錠を解錠してアクセスできる部分に通信装置または入力装置からユーザー識別子、トークン番号、シークレット変数ＫＣやＢＣを書き換えることができると好ましい。
【０２１８】
端末３Ｄは施錠された装置に組み込まれている場合、施錠を解錠してアクセスできない部分（金庫においてはテンキー式、プッシュ式金庫などのキー入力ボタンの設置面）にＮＦＣタグ１９Ａとの通信装置（またはカメラによる読み取り装置）及び出力装置を備えてもよい。
【０２１９】
本発明のＮＦＣタグ１９Ａと端末３Ｄによる施錠装置は既知の施錠方式と組み合わせてもよい。具体例として本発明を金庫に用いる場合は本発明のＮＦＣタグ１９Ａと端末３Ｄによる施錠と、ダイアル錠または鍵とシリンダー錠を用いた施錠方式、またはテンキー式プッシュ式ボタンによる暗証番号結果を用いる施錠方式、または端末３Ｄに生体認証センサを用いた生体認証を用いる施錠方式を組み合わせてもよい。金庫のみならず他の実施形態においても既知の施錠方式と組み合わせてもよい。
例として自動車においても金属製の鍵と組み合わせてもよい。その場合自動車の金属製の鍵では原動機始動後の航続可能距離の設定を行い、ＮＦＣタグ１９Ａを用いたときのほうが金属製の鍵よりも航続可能距離が長くなくなる、もしくは航続可能な距離の制限がなくなるなどの措置をとってもよい。
ネットワーク２０に接続できる場合にはＢｎＴＯＴＰによるウェブサイトへのログインのような認証ができたときに航続距離の制限を無くし１９Ａで施錠を解錠した際には例として１００ｋｍの走行を許可し金属製の鍵で解錠した際には５０ｋｍの走行を許可するといった設定も考えられる。
【０２２０】
用途の例として自動車や金庫の施錠のみならず飛行機、船舶、農業機械、林業機械、重機の施錠に用いてもよい。建物の扉、保管庫や倉庫の施錠、加工装置・産業設備・電子計算機端末の施錠及び始動装置に用いてもよい。アクセスコントロールを行うための端末３Ｄを組み込める機械や装置または施設や設備と容器に対し利用されうる。
【０２２１】
＜ＩＣ型タグ型の解錠鍵とそれを用いて解錠される建物及び設備＞
建物や金庫室、自動車等の電源を備える物に対し、本発明の ＩＣタグ等デジタル機器による認証システムを利用し、端末３Ｄは防犯カメラなど入出力装置や記憶装置を多用し解錠するユーザーを監視しつつ解錠操作をユーザーに行わせることができる。端末３Ｄの電源に容量の限られる電池を用いる場合、例えば家庭用金庫や手提金庫や錠前に電池を備える場合その電池容量によって運用に制限が生じうる。
なお端末３Ｄが金庫などの容器である時を例にすると、端末３Ｄの電源装置３７Ｄに電池を用いて駆動されるときは一次電池及び二次電池といった蓄電装置を用いることができる。二次電池を用いる場合は施錠された部分を解錠して端末３Ｄにアクセスできる部分に充電することの出来る充電用端子やワイヤレス電力伝送によって充電できる部分を備えていてもよい。あるいは施錠された端末３Ｄを持つ金庫の庫内にアクセスできない場合であってもワイヤレス電力伝送によって施錠された面から内部の端末３Ｄに充電してもよい。そして端末に接続されるハンドル式の手回し発電などの発電機能や環境発電機能を用いて充電できてもよい。
さらに端末３Ｄに充電のみ行う機能を持つ端子を施錠された面（アクセス制御されていない面）に備えてもよい。端末３Ｄに充電のみ行う機能を持つ端子を施錠された面に備える場合は充電端子に交流の電力や高電圧などを印加されたとしても端末３Ｄの動作に影響し

ないようにする保護回路を充電機能と共に持たせた電源装置３７Ｄを持たせてもよい。
【０２２２】
ここで建物や自動車等設備の錠と錠を制御する端末３Ｄはネットワーク２０に接続できていると好ましい。ネットワーク２０経由で端末３Ｄの認証関数３０１８ＤＡのＯＷＰ計算を行うＫＣやＢＣを変更できるためである。ＫＣやＢＣは建物等の定期検査や自動車の車検時などに変更されていもよい。錠を制御するコンピュータ端末３Ｄのシード値と鍵１９Ａに用いるＯＷＰを生成するワンタイムパスワード生成トークンのシード値が合うように運用される。
【０２２３】
＜インターネットワーク２０から切断された端末３ＤにおいてＯＴＰ認証を行う手段＞
ネットワーク２０に接続できなくとも、ブロックチェーンのブロック番号Ｂｎを放送できる地上局や人工衛星局（例として人工衛星型端末である放送局端末５Ｃ）があって、放送局端末５Ｃからのブロック番号Ｂｎ（もしくはブロックタイムスタンプ）またはＢＣ値や暗号化されたＫＣ値などの放送データを端末３Ｄと端末１Ａが受け取り、端末１Ａと端末３Ｄの間でＢｎＴＯＴＰ型およびＯＷＰ型の認証を行ってもよい。この場合は端末１ＡにＯＴＰ生成関数３００９Ａに相当する関数を利用できるソフトウェアがあり、端末３ＤにはＯＴＰ認証関数３０１８ＤＡが備えられている。 ブロック番号Ｂｎが放送されている場合、放送を受信できる地域にある錠を制御するコンピュータはブロック番号ベースのワンタイムパスワードＢｎＴＯＴＰにて認証を行い施錠を解除することや装置を駆動することが可能となる。
【０２２４】
端末１Ａと端末３Ｄがブロック番号ＢｎもしくはＢＣを用い、端末３Ｄや端末１Ａに記録された鍵情報を用いてＫＣ値を復号し、ＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）またはＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）を端末１Ａにて生成させ、端末１Ａと端末３Ｄの通信装置を介して端末３ＤにＡやＴＩＤＡとＯＷＰまたはＢｎＴＯＴＰを入力し、３Ｄの認証関数３０１８ＤＡの引数として入力させることでＯＷＰの検証および認証を行う余地がある。
【０２２５】
ＮＩＴＺ，ＪＪＹ、ＧＮＳＳ、ラジオ局、テレビジョン放送局からの時刻信号など、無線局からブロック番号や時刻情報および暗号化されたＫＣ値を得ることも想定される。ユーザーはスマートフォン端末１Ａを保有しているが自動車などには必ずしもスマートフォンと同等の通信機能を搭載できないことも想定されるので自動車側はＧＮＳＳやＪＪＹ等から時刻情報を得ることができてもよく、それを端末３Ｄに通信装置を用いて伝えてもよい。ＧＮＳＳなどの時刻情報を用いる場合、ＧＮＳＳの時刻情報データＴｍに基づいてワンタイムパスワードに利用することも考えられる。その場合ワンタイムパスワード生成及び認証時にＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）をＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｔｍ）に変えることが必要となる。
しかし、ＧＮＳＳやＪＪＹ、ＮＩＴＺといった放送局もしくは無線通信局から得られる時刻Ｔｍを用いる場合であってもユーザー識別子Ａやトークン番号ＴＩＤＡは必要である。ＯＴＰトークンは原則として端末３Ａなどのブロックチェーンのノードに接続することでＯＴＰトークンの発行や譲渡等とＯＴＰ生成関数を行うことが本来の運用方法である。
【０２２６】
＜時刻情報受信機付きワンタイムパスワード施錠設備＞
また設備に本発明のワンタイムパスワード認証機能を採用する場合にも設備内の施錠装置に付属する電池などの消耗を抑える必要がある。常時ネットワークに接続するのは電池の容量上困難であり、その場合は施錠を解除する設備内の放送受信機とコンピュータ端末を動かし、ＧＮＳＳなどの時刻データや無線局のブロックチェーンのＴＢに関するデータ、例えば先に述べたブロック番号Ｂｎをデータ放送により端末１Ａを含む複数の端末に伝え、端末１Ａにブロック番号Ｂｎを受信させ端末３Ｄに伝える形で、ＢｎＴＯＴＰ型のワンタイムパスワードの認証を行わせることができる（ただしＫＣ値の更新は手動による更

新または放送データにより更新する必要がある）。
【０２２７】
＜ワンタイムパスワード取得時のブロック番号Ｂｎｐを認証関数の引数に追加する場合＞
ＧＮＳＳなどの時刻データの送信局や通信装置を持たない場合においてもワンタイムパスワードＢｎＴＯＴＰを利用する方法がある。
ブロック番号Ｂｎに基づくワンタイムパスワード認証関数にはトークン番号ＴＩＤＡ、ワンタイムパスワードＢｎＴＯＴＰの二つが少なくとも必要である。認証関数３０１８ＤＡを備え認証処理を行う処理部を含む建物設備等の施錠装置や入場窓口等装置について、インターネットワーク２０やＧＮＳＳ等からのブロック番号Ｂｎや時刻情報を受信できない場合が考えられる。
【０２２８】
インターネットへの通信やＧＮＳＳ等からのブロック番号や時刻情報を受信できない場合に対応するため、ワンタイムパスワード生成関数にてワンタイムパスワードＢｎＴＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎｐ）として生成した際に、パスワード取得時のブロック番号Ｂｎｐ、トークン番号ＴＩＤＡ、ワンタイムパスワードＢｎＴＯＴＰを有価紙葉１８ＡもしくはＮＦＣタグ１９Ａにバーコードもしくは文字列情報として記録させる。
１８Ａのバーコードの場合は３Ｄのカメラ等３４０Ｄで読み取り、ＮＦＣタグ１９Ａの場合は１９Ａの３Ｄの通信装置３２Ｄや３４１Ｄにて読み取り、文字列の場合はキーボード等を施錠された設備にコンピュータの入出力装置として備え、出力装置のディスプレイ等で認証関数に用いる引数の入力を求める。
認証関数３０１８ＤＡに Ｂｎｐ、ＴＩＤＡ、ＢｎＴＯＴＰを入力し、それら引数が認証関数で検証され引数に入力されたＢｎＴＯＴＰと認証関数で計算されるワンタイムパスワードと一致した場合に、認証結果が正しい時の戻り値をコンピュータ端末３Ｄ内部の解錠に用いるプログラム（解錠プログラム）の認証関数３０１８ＤＡに渡し３０１８ＤＡにて認証した結果、正しいＢｎＴＯＴＰとＴＩＤＡとＢｎｐの場合に施錠装置に解錠の信号を送付し施錠を解除する。
【０２２９】
なお、ここでＢｎＴＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎｐ）として生成した場合について述べたが、ハッシュ関数ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎｐ）の引数にユーザー識別子Ａを加えＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎｐ）として計算し、紙１８ＡやＮＦＣタグ１９Ａなどにユーザー識別子Ａ、ブロック番号Ｂｎｐ、トークン番号ＴＩＤＡ、ワンタイムパスワードＢｎＴＯＴＰとして出力し記録させ、それら１８Ａと１９Ａを端末３Ｄへの認証に用いてもよい。認証関数３０１８ＤＡに Ｂｎｐ、Ａ，ＴＩＤＡ、ＢｎＴＯＴＰを入力させ、認証を行なってもよい。１８Ａの代わりにＢｎｐも記録し表示する１５００Ａを用いてもよい。
【０２３０】
ＢｎＴＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎｐ）やＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎｐ）として計算する場合、Ｂｎｐの値でのブロック番号ではＯＴＰトークンはユーザー識別子ＡのＴＩＤＡによりＯＴＰ生成が行われたことが分かるが、そのＢｎｐの番号が最新のブロック番号Ｂｎよりも著しく小さく古いブロック番号値であって、ユーザーがＯＴＰトークンを誰かに譲渡する前に、過去のＢｎｐの時にＢｎＴＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎｐ）やＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎｐ）として計算しユーザー識別子Ａ、ブロック番号Ｂｎｐ、トークン番号ＴＩＤＡ、ワンタイムパスワードＢｎＴＯＴＰを出力させ１８Ａや１９Ａを製造した後、譲渡制限の解除されていたＯＴＰトークンを譲渡していたとする。
この場合譲渡後のユーザーＵＡはＯＴＰトークン（ＯＴＰトークンというアクセス権もしくはブロックチェーン上での自動車の鍵や所有権情報）が無いにもかかわらず自動車などの施錠が解除出来る恐れがある。そこで前記方法を用いる場合は、ＧＮＳＳなどの時刻情報Ｔｍや放送されたブロック番号ＢｎとＢｎｐが、ＢｎＴＯＴＰを生成した推定時刻Ｔｐについて、ある閾値Ｌを基に比較を行い、ＴｍとＴｐの差分がＬよりも大きい時、また

は放送されるＢｎとＢｎｐの値が閾値Ｌよりも大きい時、そのＢｎｐ値とＢｎＴＯＴＰ値による認証を受け付けないよう認証関数３０１８ＤＡや端末３Ｄの記録部にプログラムとして保存できる。

また端末３Ｄの内部にＧＮＳＳで受信した時刻情報を記録する書換回数の多い不揮発メモリ（フラッシュメモリや強誘電体メモリ、磁気抵抗メモリ、相変化メモリ、抵抗変化型メモリといった不揮発性のメモリ）を端末３Ｄの記憶装置に内蔵し、前記抵抗変化メモリや強誘電体メモリといった読み書き回数の多い不揮発メモリをＧＮＳＳの時刻情報の記録装置に用い、悪意ある攻撃者が端末３Ｄの時刻情報を記録したメモリ部分の情報にアクセスし改ざんできぬよう封止等を行うことが求められる。

【０２３１】

＜ユーザー識別子もしくはトークンごとに異なるマッピング型シークレット変数ＫＣＡを設定する場合＞

ネットワーク２０に接続されていない設備に内蔵された端末３Ｄのシークレットキー変数ＫＣは更新を行う場合、ユーザーもしくはサービスの提供者が端末３Ｄの無線及び有線通信装置にアクセスして個別にＫＣ値を更新する必要がある。放送による時刻情報およびＫＣ値の受信やネットワーク２０に接続ができない端末３Ｄの場合コントラクトのオーナーは任意の時刻に変更することは困難である。

コントラクトに含まれるＯＴＰトークンとＯＴＰトークンに対応する全ての施錠用端末３Ｄに単一のＫＣ値を使っていた場合、ＫＣの情報が漏洩した場合には、オフラインの施錠装置全てのＫＣを個別に書き換える必要が生じる恐れがある。

これを防ぐには、ＫＣについてトークン番号やユーザー識別子に応じて複数の値を設定することが想定できる。例としてトークン番号ＴＩＤＡに固有のシークレットキー変数ＫＣＡを設定することが可能である。具体例としてトークン番号ＴＩＤＡをキーとするマッピング型変数ＫＣＡ［ＴＩＤＡ］等がある。またマッピング型以外にもＴＩＤＡをキーとしてＫＣＡを設定できる型であればよい。

ＯＴＰ生成及び認証においてハッシュ関数ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎ）の引数ＫＣをＫＣＡに置き換え、ＢｎＴＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣＡ［ＴＩＤＡ］，Ｂｎ）としてＯＴＰの生成と認証に用いてもよいし、ＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣＡ［ＴＩＤＡ］，Ｂｎ）のようにユーザー識別子を追加してもよい。ＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣＡ［ＴＩＤＡ］，ＢＣ）でもよい。

トークンごとに異なるＫＣＡを設定する場合の注意点としてブロックチェーンのコントラクトに発行したトークンの数量に応じてシークレット変数ＫＣＡを記録しなければならない。これはブロックチェーン上に多くのトランザクションを生成させ、ブロックチェーンのデータ総量を増大させる恐れがある。

ＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣＡ［ＴＩＤＡ］，Ｂｎ）のようにユーザー識別子を追加してもよい。ＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣＡ［ＴＩＤＡ］，ＢＣ）の形態は端末３Ｄでの利用例に限らず本発明の他の実施形態でも利用できる。例として端末３Ｃへのアクセスにも用いることができるほか端末４Ａにおける暗号化データをソフトウェア４０３Ａを用いて復号する用途にも用いられる。ＫＣと同じくトークン番号をキーとしたマッピング変数ＫＣＡもコントラクトの管理者がセッターとなる関数を用いてＯＴＰ生成関数やＯＴＰ認証関数の計算に利用する或るトークン番号のＫＣＡ値を変更・更新してもよい。

【０２３２】

＜シークレット変数ＫＣを更新することの出来るオフライン型施錠装置＞

ＫＣの更新においては、建物や設備の施錠に用いる本発明の認証システムを備える端末３Ｄに接触型または非接触型の通信装置を備えさせ、施錠装置を操作する端末３Ｄ内部にＫＣを更新させる情報を入力させることが考えられる。ここで更新作業を行うのは施錠装置を購入したユーザーを想定する。ユーザーの端末１Ａ等により施錠装置とそのコンピュータ端末３Ｄにアクセスし３Ｄの製造元から配布されたＫＣ値（暗号化され配布されたＫＣ値をインストールするなどして）を更新する方法が考えられる。

【０２３３】
＜ユーザー識別子Ａのないｏｗｐトークン＞
ＢｎＴＯＴＰ型のトークンではユーザー識別子ＡがＯＴＰ計算を行うハッシュ関数の引数に無い場合はＢｎＴＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎ）であり、前記ＢｎＴＯＴＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，Ｂｎ）はＢｎが１５秒などの定期的な間隔で更新されるので利用は可能である。それに対しＯＷＰ型のトークンでユーザー識別子Ａがハッシュ関数の引数にない時はＯＷＰ＝ｆｈ（ＴＩＤＡ，ＫＣ，ＢＣ）の内ＢＣがコントラクトの管理者等により定期的に変更されなければＯＴＰトークンの流通時にＯＷＰ値が多くの人に知れ渡ることが想定される。
本発明でＯＷＰを生成する場合にユーザー識別子を利用しない場合の危険性を認識したうえで識別子Ａを一切利用しないケースも考えられる（つまりユーザー識別子は含まずトークン番号のみでワンタイムパスワードの生成と認証を行う本発明の実施例）。サービス提供者の望みに応じては個人情報保護のためユーザー識別子Ａは使わずトークン番号ＴＩＤＡのみ利用し、譲渡され流通する中でＯＷＰが漏洩する形で本発明が提供されることもあるかもしれない。
この場合本発明の紙製チケットの所持者は改札や入場窓口の人員の助けを借りブロックチェーン上での所有を確認できなければなければ入場できないが、サービス提供者が規約などで許可しトークン流通の途中でＯＷＰを知ったものにサービスを提供すると契約している場合には、入場あるいはサービスを受けることが出来る（この時、トークンはチケットもしくは回覧板、広告の散らしのようなものであり、そのクーポンコードＯＷＰｃｐを複数のユーザーが回し見て、ユーザーたちがＯＷＰｃｐをサービス提供者の店舗などに提示し特典を受けるサービスを想定する。あるいは試供品や試し読みなどの用途への利用を想定する）。
本発明はサービス提供者とユーザーの間で認証し合意してサービスを行うことに役立てる事を意図したものであるので、ＯＷＰが漏洩しやすくなる条件であってもサービス提供者の望みに応じて提供される。またカスタマイズされうる。
一方でサービス提供者はブロックチェーン上のコントラクトを利用する際にユーザーに提供する変数のうちトークン番号やユーザー識別子などユーザーに帰属する情報のうちどのような変数を利用しているか開示し表示する必要がある。
【０２３４】
なお本発明は認証装置としての端末３Ｄに関してであり、認証装置ではなく施錠装置そのものの機構を破壊するなどして開錠される恐れは残り、一方でその手段を用いて本発明に必要な秘密鍵１０１Ａや解錠用のＯＴＰデータを失ったユーザーがコントラクト管理者や業者に依頼し設備や金庫、建物などを開錠する余地は残されている。
【０２３５】
＜発券サーバ端末＞
発券サーバ端末３Ｅは店舗のＡＴＭ等端末や端末１Ａ、端末１Ｂ、管理者端末１Ｃ、端末４Ａ、ブロックチェーンノード端末３Ａ、３Ｂ、ブロックチェーン検索サーバ３Ｆとネットワーク２０を介して接続されている。ここで端末３Ｄもネットワーク２０に接続されることがあるが、端末３Ｄは常時接続を想定しない。
【０２３６】
発券サーバ３Ｅは、ユーザーＵＡが店舗のＡＴＭ等端末や端末１Ａを操作し、サービスに対応したＯＴＰトークンを検索し前記ＯＴＰトークンを電子商取引機能を用いて購入し、ユーザーＵＡが指示するユーザー識別子Ａに対しＯＴＰトークンの発行を依頼する。
そして発券サーバ３Ｅはコントラクトの管理者ＵＣとコントラクト管理者端末１ＣにＵＡが購入したサービスに対応するＯＴＰトークンについて、ユーザー識別子Ａに対し、あるブロックチェーン識別子のあるコントラクト識別子のＯＴＰトークンのコントラクトについて、トークン番号ＴＩＤＡのＯＴＰトークンの発行を指示する。（トークン番号ＴＩＤＡはコントラクト管理者が決めてもよい。）
コントラクト管理者端末１Ｃは発券サーバ３Ｅの指示に従いノード端末３Ａのブロック

チェーン部にコントラクト管理者の秘密鍵１０１Ｃを用いてアクセスし、ＯＴＰトークンのコントラクトのトークン発行関数にユーザー識別子Ａとトークン番号ＴＩＤＡとその他ＯＴＰトークンの情報（ＯＴＰトークンのＵＲＩ情報やシリアル番号、有効無効の真偽値、備考など）を引数に入力し、ＯＴＰトークン発行関数の実行トランザクションを署名後に３Ａのブロックチェーン部に送信し、トランザクションがブロックデータにまとめられブロックチェーンに連結されることでトークン番号ＴＩＤＡのＯＴＰトークンがユーザ識別子Ａに発行される。

コントラクト管理者端末１Ｃもしくは発券サーバ３Ｅを通じてＯＴＰトークンを発行したユーザーに対し電子メールや電話番号ＳＭＳまたは郵送配達によりトークン番号ＴＩＤＡのＯＴＰトークン発行を行ったことを通知する。

【０２３７】

＜４Ｃ．暗号化データおよびファイルの復号と利用＞

図１Ｂに示すように本発明では、図８Ａや図８Ｂに示す本発明のＯＴＰ認証システムを応用し、端末５Ｂなどから配布された暗号化されたデータ４０３４Ａを持つ端末４Ａがネットワーク２０を通じて端末３Ａに接続し本発明のブロックチェーンを用いたＯＴＰ認証システムを用いて認証の戻り値４０３１Ａを取得し、ソフトウェア４０３Ａ（図４Ｂに記載の４０３Ａ、４０３ＡはソフトウェアＣＲＨＮ）は少なくとも４０３１Ａを用い、好ましくは４０３２Ａや４０３０２Ａといった複数の鍵情報を基にソフトウェア４０３Ａのプログラムの処理に従って暗号化データの復号及び平文データの暗号化を行う共通鍵（対称鍵）４０３３Ａを算出し暗号化データを復号し平文データの利用を可能にする。

【０２３８】

本発明のＯＴＰ認証システムはアクセスコントロール技術であり、図１Ｂおよび図８Ｃや図８Ｄに示す実施形態は図８Ａや図８Ｂとは異なる実施形態である。

図１Ａ及び図８Ａや図８Ｂにおいては端末３Ｃや端末３ＤがＯＴＰ認証を行いアクセスする対象であった。しかし図１Ｂや図８Ｃや図８ＤにおいてはＯＴＰ認証を行いアクセスする対象が端末ではなく暗号化されたデータであり、端末３Ｃや３Ｄが存在せず、端末４Ａとブロックチェーンのノードとなるサーバ端末３Ａとネットワーク２０があって、端末４Ａの記録装置に暗号化データ４０３４Ａとソフトウェア４０３Ａ とＯＴＰ認証後の戻り値４０３１Ａと４０３２Ａや４０３０２Ａといった複数の鍵情報を基にソフトウェア４０３Ａのプログラムの処理に従って暗号化データの復号及び平文データの暗号化を行う鍵情報４０３３Ａを算出し暗号化データを平文データに復号できる。４０３４Ａは４０３３Ａを共通鍵暗号（対象鍵暗号）の共通鍵（対象鍵）として用い復号され４０３５Ａを求めることができる。４０３Ａで用いる暗号化方式は好ましくは共通鍵暗号化を用いる。

【０２３９】

暗号化データ４０３４Ａは平文データ４０３５Ａを暗号化できるバージョンの（版の）４０３Ａを用いることで作成される（４０３Ａで用いる暗号化方式とＴＴＫＹ４０３３Ａを算出できるならば４０３Ａを用いなくても暗号化することはできる。）。

図５Ｂの端末５Ｂといったネットワーク２０を用いてユーザー端末４Ａのアクセスに応じ、端末４Ａが端末５Ｂの持つデータベース検索機能により５Ｂ内部に収蔵された複数の暗号化データから端末４Ａが検索し探索させた暗号データ４０３４Ａを端末４Ａにネットワーク２０を介して配信する機能を持つ。また端末５Ｂを用いずとも、既知のクラウドストレージやデータ共有サービスを利用し４０３４Ａを配信・配布できる。

さらにネットワーク２０を用いずとも暗号化されたデータ４０３４Ａを記録させた光ディスク（光学ディスク、オプティカルディスク）や半導体メモリ、磁気ディスク、磁気テープおよびそれらを読み取りできる外部記録装置を物流などを通じて流通させ、ユーザーＵＰと端末４Ａの元へ４０３４Ａの記録された外部記録装置を届けることができる。あるいは街頭もしくは店舗などで４０３４Ａの記録された外部記録装置を配布してもよい。後述する図８Ｄに示す端末５Ｃにより放送の形で端末４Ａを含む複数の端末に暗号データ４０３４Ａを配信・放送してもよい。

【０２４０】

図８Ｃや図８Ｄに示す形態の暗号化データは、解錠できる鍵情報４０３３Ａを紛失すると復号できなくなり失われる恐れがある。図８Ｂに示される例としての金庫の施錠装置のように、端末３Ｄそのもののハードウェアや施錠用の機械的機構が正常に動作しなくなって解錠ができない場合は施錠装置そのものを破壊し開錠することにより金庫内の物品を回収できることに対し、暗号化データではそのような開錠はできず、復号が困難となった暗号化データに含まれる平文データは失われてしまう恐れがある。

【０２４１】

実施例では電子書籍や音楽映像情報を視聴し閲覧する権利をＯＴＰ生成トークンとして表し、ＯＴＰ生成関数３００９ＡとＯＴＰ認証関数３０１８ＡとＯＴＰトークン所有情報３０１４ＡとＯＴＰトークン発行関数３０４３Ａ等を含む図３ＡＣのコントラクト３００８ＡをＯＴＰ認証システムで用いる場合に呼び出す。

ソフトウェア４０３Ａを利用するＯＴＰトークンのコントラクトは図３ＡＢに示すようなＯＴＰ生成関数を含むコントラクト３００８ＡＧとＯＴＰ認証関数を含むコントラクト３００８ＡＡもしくは端末３Ｄに記録されるＯＴＰ認証関数３０１８ＤＡのようにＯＴＰ生成関数を含むコントラクトとＯＴＰ認証関数を含むコントラクトに分離していても認証を行えないわけではないが、
ソフトウェア４０３Ａを用いる場合には好ましくは図３ＡＣに示すように同一のコントラクトにＯＴＰ生成関数３００９ＡとＯＴＰ認証関数３０１８ＡとＫＣ値３０１１ＡやＢＣ値３０１３Ａとそのセッター関数３０１２Ａを記述する事が好ましい。

４０３Ａはネットワーク２０と分散型台帳システムノード端末３Ａがあってその端末３Ａのコントラクト３００８ＡでＯＴＰの生成と認証を完結できることが望ましく、コントラクトの管理者はＫＣ値３０１１ＡやＢＣ値３０１３Ａ、３０３０Ａや３０３１Ａや３０４１Ａや３０４２Ａといったコントラクトの変数や関数を一つのコントラクト３００８Ａだけ変更等管理すればよい。

一つのコントラクト３００８Ａだけ変更等管理することで、ＫＣ値などの設定変数を異なるＯＴＰ生成及び認証を行うコントラクト間や端末３ＤのＯＴＰ認証関数３０１８ＤＡ間で一致するよう設定する労力を無くすことができる。

端末３Ｃのサービスで用いる可能性のある３００８ＡＧと３００８ＡＡに分離したコントラクト間でのシード値３０１１ＡやＢＣ値３０１３ＡやＯＴＰ計算法に関わるブロック番号剰余変数３０３０ＡやＯＴＰ桁数調整用整数３０３１Ａの同期のための変更等管理作業や、端末３Ｄのサービスで用いる３００８Ａや３００８ＡＧと３０１８ＤＡをもつ端末３Ｄの記録部の間での変更等管理作業が、ソフトウェア４０３Ａの用途では不要になることがある。

ユーザー端末が用いるＯＴＰ生成コントラクトと端末３Ｃや３Ｄなどで用いつＯＴＰを認証する関数やコントラクトを分離すると、そのシード値を変更する際にそれぞれのコントラクトまたは関数のＫＣ値等数値を同じ値に変更させ同期させる必要があり、コントラクトやサービス管理者の労力を要求する。一方で図３ＡＣに示すように同一のコントラクトにＫＣ値３０１１ＡやＢＣ値３０１３Ａとそのセッター関数３０１２Ａを記述することでＯＴＰ生成関数とＯＴＰ認証関数の計算に用いるＫＣ値３０１１Ａなど数値が同一コントラクトにある場合は、そのコントラクトのセッター関数３０１２Ａを一度操作するのみで済み、シード値の更新と同期を行う際に労力が少なくなる利点がある。そこでソフトウェア４０３Ａを用いる実施形態では図３ＡＣに示すようにＯＴＰの生成関数と認証関数を用いるコントラクトを利用した。

【０２４２】

実施例においては、ＯＴＰ認証時に認証関数３０１８Ａを実行し認証結果を戻り値ＣＴＡＵ（図３ＡＣの３０２１Ａと図４Ｂの４０３１Ａ）として受け取ったとき、戻り値４０３１Ａが複数あって、第一の戻り値が真偽値変数ＣＴＡＵｔｆ（真偽値型変数ＣＴＡＵｔｆ、ブーリアン型変数ＣＴＡＵｔｆ、ブール型変数ＣＴＡＵｔｆ）で第二の戻り値が認証コントラクトに内蔵された変数に記録された鍵情報ＣＴＡＵｋｅｙであった時、認証結果のうち真偽値ＣＴＡＵｔｆを用いてアプリケーションソフトウェア４０３Ａ内部の次の処

理の実行を決定させる。４０３１Ａに含まれる第１の戻り値ＣＴＡＵｔｆが真ならば認証結果が正しいと定義する時、ソフトウェア４０３ＡはＣＴＡＵｔｆの結果が真であるか判定し、偽の値の場合は処理を中断する。

ＣＴＡＵｔｆが真の値である時、４０３１Ａに含まれる第２戻り値のＣＴＡＵｋｅｙを受け取り、そのＣＴＡＵｋｅｙとソフトウェア４０３Ａに内蔵された鍵４０３０２Ａと必要に応じて外部で設定された４０３２Ａを鍵を生成する情報に用いて共通鍵４０３３Ａ（ＴＴＹ４０３３Ａ、タイトルキー４０３３Ａ）をソフトウェア４０３Ａのプログラムに従って計算し、４０３３Ａを共通鍵に用いてＡＥＳ(Advanced Encryption Standard)方式等の共通鍵暗号で暗号化されたデータやファイルを復号して閲覧し利用する事が可能である。

ここで本発明の実施例や実施形態では閲覧・視聴可能なファイルは文章ファイル、音声ファイル、動画ファイルなどが可能である。主にＨＴＭＬ５とＥＣＭＡＳｃｒｉｐｔに対応するウェブブラウザにおいて表示可能なファイル拡張子のファイルを用いた。

【０２４３】

本発明を実施する際にはソフトウェア４０３Ａにおける共通鍵暗号に用いたＡＥＳ方式の鍵長は１２８ｂｉｔおよび１９２ｂｉｔを用いた。本発明の実施例で用いたＡＥＳ方式は具体的にはＡＥＳ－ＣＢＣ暗号であり明示的初期ベクトル（Initialization Vector：IV）を伴う暗号ブロック連鎖（CBC）モードを用いた。ソフトウェア４０３Ａには鍵のデータ長とＣＢＣモードや初期ベクトルＩＶを設定する。

【０２４４】

ソフトウェア４０３Ａの実施例として、文章形式では米国アドビ社のＰＤＦ形式、音声ではＭＰ３形式、動画形式ではＭＰ４形式などウェブブラウザで利用できるファイルの形式に対応する。また著作権に関するコンテンツを含むファイルのみならず、例えば外部に漏洩することを防ぎ漏洩したとしても暗号化などで復号されないようにしたい法人の顧客等個人情報（例としてある株式会社の顧客名簿、学校法人の学生名簿など）や、個人・法人・団体の内部で閲覧するべき機密文章や、製作中の音声画像動画情報、製品の設計図、製品のＣＡＤデータ（３Ｄプリンタに利用可能な３ＤＣＡＤデータも含む）、電子回路データ（プログラムロジックデバイスで利用できる設計データを含む）、半導体のフォトマスクデータなどといった多様な研究所や工場などの機密情報などを暗号化し復号して伝達する際にも本発明は利用できる。

【０２４５】

本発明の実施例ではＡＥＳ方式の共通鍵暗号で暗号化されたファイルをソフトウェア４０３Ａを用いて作成または復号するための鍵４０３３Ａを生成する際に、ソフトウェア４０３Ａは少なくとも鍵情報ＣＴＡＵ４０３１Ａを利用する。そしてソフトウェア４０３Ａに内蔵された鍵４０３０２Ａ（ＣＲＫＹ４０３０２Ａ、ＣＲＨＮソフトウェア秘密鍵４０３０２Ａ）を用い、さらにブロックチェーン（分散型台帳システム）及びソフトウェア４０３Ａに含まれない鍵４０３２Ａ（ＡＫＴＢ４０３２Ａ、合言葉４０３２Ａ、外部パスワード４０３２Ａ）を用いる。４０３２Ａはブロックチェーンを用いないことにしているがそれは推奨であって実際には４０３Ａを利用するブロックチェーン基盤とは異なるブロックチェーン基盤からのトランザクションで通知されてもよく、４０３２Ａの通知方法は暗号化するユーザーの方針による。

【０２４６】

１．ブロックチェーンのコントラクトに記録された認証関数の戻り値４０３１Ａ

鍵情報を持つ変数４０３１ＡはＯＴＰ認証コントラクトの認証関数に利用される変数に内蔵されているが、ＯＴＰ生成コントラクトに認証関数と共に内蔵していてもよい。４０３１Ａは認証関数３０１８Ａを実行したときに認証結果が正しい場合の戻り値ＣＡＴＵとして設定される。ここでＯＴＰトークンの発行等ＥＲＣ７２１規格のノンファンジブルトークンとしての処理とＯＴＰの生成・認証を行うコントラクト３００８Ａの関数や変数の内容は秘匿化されていることが好ましい。

また鍵情報４０３１Ａをコントラクトの作成者・管理者が変更できるセッター関数を持っ

ていてもよい。コントラクトの作成者・管理者は暗号化されたファイルの著作権等の権限を持つ権利者の個人法人を想定する。

４０３ＡとＯＴＰトークンと４０３１Ａが対象にするサービスが定期購読型の雑誌や新聞、定期視聴型の放送データであるとき、暗号化に用いる鍵４０３３Ａは数カ月もしくは数年毎に更新することが好ましく、コントラクトの４０３１Ａをコントラクト管理者が定期的に変更することで４０３３Ａも更新される。変更された４０３３Ａで平文データを暗号化して流通させる。

その場合、４０３１Ａを知らないユーザーは４０３３Ａを算出できず暗号化データの復号が困難もしくは不可能になる。この場合は４０３Ａが出来事を記録するために新聞の記事の一部を個人利用用に切取り保存できた方が文化や時事の記録に役立つほか複写なども許可すべきかもしれない。後述する証明書４０３６Ａと同様に電子署名やＨＭＡＣなどの手段を用いて新聞など公共性のある情報から個人利用のために切り抜いたデータに時刻情報やブロックチェーンのブロック番号とそれらメッセージのＭＡＣ値を添付して改ざん検知できる新聞等書籍の記録として保存してもよい（新聞等書籍の権利者が切り取りなどを許可しない場合は４０３Ａにおいて切取して保存する機能は停止される）。

別の方法として４０３１Ａを固定されたデータ値とし、４０３２Ａをあらかじめ新聞や雑誌の契約時にユーザー識別子へのトランザクションやもしくは電子メールなどで通知しておき、数カ月もしくは数年ごとに４０３２Ａを更新し４０３３Ａを更新しながら暗号化データを作成しユーザーへ暗号化データを流通させつつ、ユーザーへ更新後の４０３２Ａを通知しさせる。ユーザーに電子メールなどで更新後の４０３２Ａと前記４０３２Ａを用いて４０３３Ａを算出し鍵に用いて暗号化した暗号化データを配布してもよい。４０３２Ａを伝達する方法として電子メールの代わりに４０３Ａがあるウェブサイトやウェブアプリと接続しＡＫＴＢ４０３２Ａを自動的に取得してもよい。

任意ではあるが４０３２Ａを顧客・ユーザーごとに変えて４０３３Ａも同じく顧客ごとに変えて暗号化したデータを作成して配布してよい。ただし、データ流通時にその暗号化データは対象となる読者にユニークなデータやハッシュ値を持つため誰がどの出版社の雑誌や新聞を購読しているかがトラッキングされる恐れもあるので、暗号化された電子メールやクラウドストレージなどの通信手段で暗号データを出版社とユーザー間でユーザー専用の暗号化データのやり取りをすることが好ましい。４０３２Ａと４０３２Ａを用いて作製した４０３３Ａを記録した光ディスク等の記録媒体を通信ではなく郵便や配達の形で配布する事もできる。

新聞・雑誌などは単一の４０３３Ａで暗号化され無線による放送データの形で取得できるとき、だれがどのようなデータを購読しているかはトラッキングしづらいかもしれない。

【０２４７】

ＯＴＰトークンと対応するデータやコンテンツを提供する権利者の要請に応じ、コントラクト３００８Ａには譲渡制限を行う３０４１Ａが設定され、３０４１Ａのデータ値に応じてトークン送信関数３０４０Ａの実行が中断されるようにしてもよい。

【０２４８】

例として、機密情報などを団体で扱う場合にはデータのアクセス権であるＯＴＰトークンを譲渡する必要が無く、譲渡制限機能を利用したいときには３０４１Ａにて譲渡を禁止する変数値を設定する。

一方、ＯＴＰトークンに対応するコンテンツが例として書籍データであって、その書籍データは紙の書籍と同じく古物として法令に従って流通することをコンテンツの権利者が許可するとき、コントラクト３００８Ａには譲渡制限を行う３０４１Ａが設定されるものの、３０４１Ａのデータ値はコンテンツの権利者が鍵情報４０３１Ａをコントラクトの作成者・管理者が変更できるセッター関数により任意の時刻に書き換えることで３０４１Ａが譲渡可能な状態の場合にＯＴＰトークンを紙の書籍の代替物とみなして異なる秘密鍵を持つユーザー（例として１０１Ａを持つユーザー識別子Ａと１０１Ｂを持つユーザー識別子Ｂのユーザー）の間で送信関数３０４０Ａを用いて譲渡することが可能になる。さらに

、コンテンツの権利者が許可する場合、譲渡制限を行う３０４１Ａが設定されず、ＥＲＣ７２１規格に準拠してトークンが流通させることもできる。

【０２４９】

２．合言葉もしくはパスワードを使う鍵４０３２Ａ。

この情報はブロックチェーン上のＯＴＰ生成及び認証コントラクトやソフトウェア４０３Ａには含まれない情報であり、それらとかかわりのない通信経路を用いて鍵４０３２Ａをユーザーに伝える。ここで伝達の仕方は任意であり、電子メール、電話、ＳＭＳ、コントラクト作成者のウェブサイトなどや、封書をユーザー宛てに郵送するなどの手段を利用できる。（ここで鍵４０３２ＡをＯＴＰ生成トークンを保有するユーザーに伝達する場合にパブリックなブロックチェーンによるトランザクションやソフトウェア４０３Ａを用いるのは推奨されない。秘匿化されたプライベートなブロックチェーンではトランザクションに４０３２Ａを記録してユーザーの識別子に送付できるかもしれないが、ブロックチェーンに依存せず電子メールや電話、信書の郵送配達といった形で送付してもよい。）

【０２５０】

４０３２Ａには空欄を記入することも可能である。すなわち暗号化の鍵のデータ値が４０３１Ａだけになる場合もあるが、攻撃者にとっては４０３Ａのソースコードとブロックチェーン以外の経路から伝達された鍵を推測する必要が生じるので、その鍵の特定が必要となり、暗号化を復号する事を困難にさせる、暗号解読に取り組む意欲を削ぐ狙いがある。４０３２Ａはデータを暗号化したいユーザーが、データを暗号化によりどの程度保護したいかに応じて設定する変数である。好ましくは値４０３２Ａは空欄ではなく、ある数の数字や文字列であるとよい。値４０３２Ａはソフトウェア４０３Ａの許す限り長い文字列のデータ値をとることもできる。４桁のＰＩＮでもよい。もしくは１文字の英数字記号でもよい。

【０２５１】

ここで４０３２ＡはユーザーＵＡの電子メールアドレスなどに伝達されるが、メールアドレスごとに（送付先ごとに）異なる値４０３２Ａとし（例えばユーザー識別子Ａを由来として数々の演算やハッシュ化、情報の切り取りなどの加工した値とし、コントラクトに内蔵された一つの戻り値４０３１Ａとユーザー識別子毎に異なる値４０３２Ａを基にユーザー識別子毎に異なるファイル暗号化鍵ＴＴＫＹ４０３３Ａを生成してコンテンツファイルの暗号化を行い、暗号化ファイルをユーザーに別途メールやウェブサービスで伝達することもできる。このとき、ファイルを流通させるサーバ５Ｂにおいてユーザーごとのメールアドレス毎に異なるＡＥＳ暗号化鍵でコンテンツを暗号化し送信する処理部と記憶部が必要である。

【０２５２】

一方で、ユーザーの区別なく簡易なセキュリティとして社内などに配布したい資料のファイルの暗号化に用いる場合などでは４０３２Ａは社内で決めた文字列にして、単一の４０３２Ａのみを用い、社内のメールや紙の回覧板、社内郵便などで通知させ、同一のダイジェスト値（ハッシュ値）を持つ暗号化ファイル４０３４Ａを社内に接続されたユーザーの端末に配布することも考えられる。

この場合、ネットワーク２０に接続されたサーバ５Ｂは不要であり、社外のサーバーを使わないことはコストの低減につながる。社内に限らず個人同士やある団体で文章やソフトウェアといったコンテンツを流通させたい場合にも利用できる。社内のデータを暗号化し、万一暗号化データが漏洩した際も平文データの形で閲覧されることを防ぐ。

【０２５３】

ハッシュ値の異なる同一の平文データ・コンテンツを含む暗号化ファイルを各々のユーザー識別子のユーザーに配布する場合は、配布先のユーザー数が多いほど個別に暗号して作成する４０３４Ａが増え、端末５Ｂの計算資源と記憶領域を消費する恐れがある。さらにＯＴＰトークンの譲渡制限がない場合、ユーザーはＯＴＰトークンを譲渡し合えるが、ＯＴＰトークンと対応した鍵４０３２Ａと、４０３２Ａを用いて暗号化したデータ４０３４Ａを譲渡時に譲渡元のユーザーから引き継ぐ必要がある。もしくは端末５ＢにＯＴＰト

ークンの譲渡があったことを通知し、５Ｂ譲渡先のユーザーのために新たに生成した４０３２Ａと４０３２Ａを用いて暗号化したデータ４０３４Ａを配信・配布されてもよい。

【０２５４】

ハッシュ値の異なる同一の平文データ・コンテンツを含む暗号化ファイル４０３４Ａを各々のユーザー識別子のユーザーに配布する場合は、オーダーメードされた暗号化データ４０３４Ａの流通をネットワーク２０上でトラッキングすることで不正なデータの流通を監視出来るかもしれないが、暗号化データ４０３４Ａの流通をネットワーク２０上で追跡することでどのような新聞や書籍がどのようなユーザーに読まれているかを補足することが容易になる恐れもある。

プライバシーの保護とコンテンツ管理者の保護を両立できるよう４０３２Ａを用いた暗号化データ４０３４Ａの生成と流通を行うことが望ましい。また計算資源、記憶領域、暗号化データの保存性を考慮することが好ましい。発明者としては４０３２Ａは個人間や団体内、社内で決めた単一の文字列（合言葉としての外部パスワード）として、同一のダイジェスト値（ハッシュ値）を持つ暗号化ファイル４０３４Ａを配布することが好ましいと考える。

【０２５５】

さらに次に示す3番目、4番目の鍵情報を追加できる。

【０２５６】

３．ソフトウェア４０３Ａの例として４０３ＡのＥＣＭＡＳｃｒｉｐｔ等のソースコードに記述されたソフトウェア４０３Ａに設定された鍵情報４０３０２Ａ（図４ＢのＣＲＫＹ、４０３０２Ａ）。ここでソフトウェア４０３Ａのソースコードは難読化されることが好ましい。またソースコードは暗号化することもできる。もし４０３０２Ａが漏洩した場合には４０３０２Ａの値を変更した新たな版のソフトウェア４０３Ａを配布する際に利用する。

４０３３Ａの算出には４０３１Ａと４０３２Ａと４０３０２Ａを含む４０３Ａが必要である。新しい版の４０３Ａのユーザーは過去の書籍の暗号データ４０３４Ａに対応する版の４０３Ａを同じ場所に記録して保存することが好ましい。

【０２５７】

４．ブロックチェーン上の端末３Ａをはじめとするノードに記録されるＯＴＰ生成および認証コントラクトとは異なる鍵管理コントラクトから読み取る鍵情報４０３０３Ａを用いてもよい。

４０３０３Ａは攻撃者によるソフトウェア４０３Ａの鍵４０３３Ａの計算方法の解読を困難にする目的で導入される一つの例である。

ソフトウェア４０３Ａには鍵管理コントラクトのコントラクト識別子４０３０１Ａが記述され、ソフトウェア４０３ＡのＥＣＭＡＳｃｒｉｐｔで指定された処理に応じて、鍵管理コントラクトから鍵４０３０３Ａを手に入れるゲッター関数を動作させ、関数の戻り値として４０３０３Ａを得る。４０３０１Ａ、４０３０２Ａ、４０３０３ＡはソフトウェアＣＲＨＮごとに決定される。もし４０３０３Ａが漏洩した場合には４０３０３Ａの値を変更したソフトウェアＣＲＨＮを配布する際に利用する。ここでコントラクトの関数や変数の内容は秘匿化されていることが好ましい。

【０２５８】

整理すると、本発明の実施例では４つの鍵情報を用いた。端末４Ａにおいて、端末３Ａなどのブロックチェーンノードから得られる鍵情報は４０３１Ａ、４０３０３Ａであり、ソフトウェア４０３Ａから得られる鍵情報は４０３０２Ａであり、そのどちらにも属さない経路で伝達される鍵情報は４０３２Ａである。４０３１Ａ、４０３０３Ａ、４０３０２Ａ、４０３２Ａの４つの鍵を用い、４つの鍵情報を変数としたソフトウェア４０３Ａの鍵計算関数（鍵計算処理部）を用いてファイルを暗号化及び復号を行う共通鍵ＴＴＫＹ４０３３Ａを生成する。

【０２５９】

鍵４０３２Ａは情報が設定されない場合は空欄を入力したものとみなす。すなわち４０

３２Ａが空欄であることを伝達されたと解釈し４０３Ａのプログラムはファイルの復号を試みる。また平文のファイルがありそれを暗号化する処理をユーザーが選択した場合には４０３２Ａを空欄の場合は空欄として扱い暗号化を行う。

【０２６０】

本発明の実施例及び実施形態で、このような４つの鍵を利用する方式をとる理由、とくにＡＫＴＢ４０３２Ａを用いる理由としてファイルを攻撃者が開錠し復号する際に仮にブロックチェーン上の４０３１Ａ，４０３０３Ａはイーサリアムでは鍵情報が解読可能な状態であり、なおかつソフトウェア４０３Ａもソースコードを難読化し暗号化などをしても攻撃者が鍵を見破る恐れがある。

そこでブロックチェーン及びソフトウェア４０３Ａに存在しないＡＫＴＢという変数４０３２Ａを設定しファイルを暗号化、復号を行う。４０３２Ａを設定することで攻撃者へ対応する。４０３２Ａの変数の個数は一つとは限らず複数設定できる。

【０２６１】

ここでイーサリアムでなく、エンタープライズイーサリアムアライアンス（ＥＥＡ）の提供するＱｕｏｒｕｍのような 取引（トランザクション）の秘匿化やネットワークへのアクセス制御などの機能が追加されたパーミッション型（許可型）のブロックチェーンを用いればコントラクトに記録された４０３１Ａ、４０３０３Ａは秘匿化されうるため、前記の取引（トランザクション）の秘匿化が可能なブロックチェーン基盤を用いることが好ましい。

Ｑｕｏｒｕｍのような 取引（トランザクション）の秘匿化やネットワークへのアクセス制御などの機能が追加されたパーミッション型（許可型）のブロックチェーンは図１、図１Ａ、図１Ｂ、図８Ａ、図８Ｂ、図８Ｃ、図８Ｄの実施例でも利用されることが好ましい。端末３Ｃの銀行のインターネットバンキングへのウェブサイトへのログイン用途および金融や価値のある情報を扱うウェブサービスへのログイン用途、端末３Ｄでの金庫や金庫室と自動車や建物などを施錠し解錠する用途、そしてソフトウェア４０３Ａを用いる暗号化データの復号用途にも利用されることが好ましい。

【０２６２】

＜暗号化データの分散された保管＞

４０３１Ａ、４０３０３Ａ、４０３０２Ａ、４０３２Ａと併用し、それら4つの変数を基に算出された単一の暗号化鍵ＴＴＫＹ４０３３Ａにてコンテンツを暗号化し、暗号化されたファイルのハッシュ値が一つのみとなる形でコンテンツを暗号化して流通させることが想定される。一方で先に説明したことと同じであるが、ユーザーごとに４０３１Ａや４０３２Ａを変更させてＴＴＫＹ４０３３Ａの違う暗号化ファイルを流通させることもできる。

ここで情報の保存のため、単一のＴＴＫＹ４０３３Ａで暗号化されたファイルを流通させることも考える。施錠された金庫などの設備等の例で示した解錠の手段を無くした場合でも施錠を破壊すればよいという考え方はコンテンツなどを含む暗号化データでは適用できない。コンテンツの権利者が配布した暗号化データが複数のコンピュータに保存され閲覧され続けて欲しい場合は単一のＴＴＫＹ４０３３Ａで暗号化されたファイルを流通させるほうが好ましいかもしれない。

本発明ではＴＴＫＹ４０３３Ａを算出する方法を紛失した場合、暗号化データを復元する事は不可能になる。４０３１Ａや４０３２Ａの値を単一の値にすることでＯＴＰトークンを持つユーザーであればソフトウェア４０３Ａにて復号できるとともに、ＯＴＰトークン持つユーザーが単一の４０３１Ａや４０３２Ａで復号できる暗号化ファイルを世界中に分散させて保有できることにつながり、世界中で利用される暗号化データは後世に保存されやすくなるかもしれない。

先に述べたことは発明者の考え方であって、最終的な暗号化の方法はデータの権利者が決定する。データの権利者の要請に応じ４０３１Ａと４０３２Ａと４０３０２Ａとその他の鍵値を設定し４０３Ａにそれらを入力させ処理を行い暗号化及び復号に用いる鍵４０３３Ａを用いて平文データの暗号化と暗号化データの復号ができる。

情報を閲覧制限しながら後世に紙の書籍のように保存するという考えから、権利者が許可する場合に４０３Ａを用いた本発明のシステムから文章データなど等を紙や外部記憶装置等に保存する手段を持たせることができる。
また需要などの問題で世界中に流通することのなかった暗号化データがある事が想定され、流通後に問題が生じ平文データの閲覧が出来ない事も想定されるので、権利者が自身の創作したコンテンツのデータの平文もしくは暗号化データとその復号を行う鍵情報を保存し管理する必要がある。

【０２６３】

＜広告等の表示または不正アクセスの監視ができるシステム＞

ここでソフトウェア４０３Ａや暗号化されたデータを復号して得られる平文データ４０３５Ａには広告を表示するＵＲＩが記録され、ソフトウェア４０３ＡはそのＵＲＩ情報に従ってサーバ端末５Ａが配信する広告等を表示させるプログラムを備えていてもよい。端末５Ａは広告のほかソフトウェア４０３Ａの取扱説明書情報や４０３Ａの版情報（バージョン情報）に関する通知を行う。
広告は端末５Ａにアクセスしてきた端末４Ａに対し端末５Ａの記憶部５０５Ａまたは５０６Ａと制御部５１５Ａまたは５１６Ａに従って端末５Ａから端末４Ａへネットワーク２０を経由して（介して）配信する。

ソフトウェア４０３Ａと端末５Ａによる広告表示方法は、紙の新聞や雑誌を読む際に紙面に広告を印刷しているのと類似しており、書籍の著作者や出版社、版権元、アプリの開発元へユーザーがソフトウェア４０３Ａやコンテンツを閲覧した回数などに応じて広告を表示したことによる報酬を分配できるようにするためである。

また紙の媒体での広告と異なり、ソフトウェア４０３Ａや暗号化されたコンテンツに記述されたリンク先ＵＲＩの端末５Ａが端末４Ａにネットワーク２０を介して配信するウェブサイトによる広告情報は動的に広告内容を変えることができる。

【０２６４】

端末５Ａとソフトウェア４０３Ａを用いた広告に関する部分は、電子書籍や音声動画の再生に関して利用し、機密情報の暗号化及び復号用途には利用しないことが好ましい。機密データを会社や団体及び個人間で秘密裏にやり取りする場合は広告の表示機能を省いたソフトウェア４０３Ａの業務用版（業務用バージョンのソフトウェア４０３Ａ）を別途用意することが好ましい。

【０２６５】

広告の表示機能による広告ウェブサイトへの接続と連携を自動的に行うのは企業間での秘密保持等の面で好ましくない可能性があり、広告の表示先に端末５Ａが広告を作成した会社から入手したデータ内部にユーザーのコンピュータにとって意図しない有害な動作をするプログラムが含まれている場合があり、セキュリティを低下させる恐れがあるため端末５Ａへ接続できる広告配信機能を省略したソフトウェア４０３Ａも用意できることが好ましい。用途に応じてソフトウェア４０３Ａを動作させるためのＯＴＰトークンがあってもよい。４０３Ａのアプリケーションソフトウェアにログインするトークンがあってもよい。

【０２６６】

端末５Ａは法人などで運用されうること、官公庁や企業間の機密情報を考慮すると、前記利用者の情報を奪うためにソフトウェア４０３Ａや広告を作成し販売するすべての関係者の中に攻撃者がいないことは保証できない。そのためソフトウェア４０３Ａは端末４Ａのオペレーティングシステム環境下で仮想機械環境やサンドボックス環境で利用されることが好ましいかもしれない。暗号化データ４０３４ＡをＯＴＰ認証システムと鍵情報で復号し平文情報４０３５Ａとして４０３５Ａを実行したとき、もしくは４０３Ａを実行したときにその挙動を調べることが好ましい。
ソフトウェア４０３Ａの実行可能なファイル形式（ファイル拡張子）が音楽ファイルや動画ファイル、書籍ファイルに限られている場合に、そのファイルを信頼する場合は仮想機械環境を省いて実行出来るかもしれない。

【０２６７】
　また広告等の情報はソフトウェア４０３ＡやＯＴＰトークンのレイティング情報に基づいていることが必要である。本発明のワンタイムパスワードトークンのコントラクトにはレイティングなどを記録した看板となる変数ＫＮＢＮ３０２４Ａを備えることができ、３０２４Ａに書かれたレイティング情報をソフトウェア４０３Ａは読み取って広告に対して動作を変える事が可能である。（例として端末５Ａが配信する広告に酒類など成人の嗜好品に関する情報が含まれるとき、未成年向けのレイティングのトークンについては広告を表示せず、広告の表示部分にはソフトウェア４０３Ａの開発元のページなどや、ソフトウェア４０３Ａの取扱説明サイトしか表示できないようにすることもできる。）
【０２６８】
ここで本発明のワンタイムパスワード認証システムを用いてソフトウェア４０３Ａを用いる場合は、
１．ソフトウェア４０３Ａ、
２．ソフトウェア４０３Ａを記録装置に記録し、ブロックチェーンとコントラクトへのアクセス情報と秘密鍵４０１Ａが記録（入力）されたスマートフォン端末４Ａまたはコンピュータ端末４Ａ、
３．暗号化できる通信経路ネットワーク２０（例としてＴＬＳ等の暗号化で通信は暗号化されている）、
４．ブロックチェーンを構成しワンタイムパスワードの生成と認証を行うサーバ３Ａ（ワンタイムパスワードの生成関数と認証関数を含むコントラクトがブロックチェーンに記録されている。）、
５．ユーザーのアクセスを受け広告を表示するサーバ５Ａ（広告のほかにユーザーへの情報通知やユーザーのアクセスを監視する複数の役割も行えるウェブサイトを展開するサーバ）、
６．ソフトウェア４０３Ａのプログラムに内蔵された広告を表示させるサーバ５ＡへのＵＲＩ情報
７．暗号化されたデータもしくはファイル４０３４Ａ
８．暗号化されたデータ４０３４Ａに含まれる広告を表示させるサーバ５ＡへのＵＲＩ情報
９．暗号化されたデータ４０３４Ａを通信経路ネットワーク２０を通じてユーザーの端末４Ａに届けるサーバ５Ｂ
が必要になる。端末４Ａは平文データの閲覧や利用の出来る端末であればよく、タブレット端末やヘッドマウントディスプレイと接続されたコンピュータ端末でもよい。
【０２６９】
　ソフトウェア４０３Ａもしくは暗号化データを復号し得られる４０３５Ａに広告を表示させるサーバ端末５ＡのＵＲＩが設定されており、前記ソフトウェア４０３Ａは広告を表示させるサーバ端末５ＡのＵＲＩに従ってサーバ５Ａにアクセスする。このとき、サーバ５Ａは５ＡにアクセスしてきたユーザーＵＰの端末４Ａ、あるいはユーザーＵＡの端末１Ａ、ユーザーＵＢの端末１Ｂといった複数の端末について、アクセス情報を図６Ｘのように記録できる。
【０２７０】
　図６Ｘではサービスを提供しているＯＴＰトークンのコントラクト識別子やブロックチェーン識別子は省略されているが、図６Ｘにコントラクト識別子ＣＰＧＴやブロックチェーン識別子（分散型台帳システムの識別子）をユーザー識別子やトークン番号と対応付けて記録してもよい。
【０２７１】
端末５Ａが端末４Ａのソフトウェア４０３Ａのアクセスを受け、端末４Ａのアクセス情報を５０１Ａに記録し、広告を記憶部５０５Ａまたは５０６Ａと制御部５１５Ａまたは５１６Ａに従って配信する。
端末４Ａのアクセス情報ブロックチェーンの識別子と、ＯＴＰ生成を行うＯＴＰトークン

のコントラクト識別子ＣＰＧＴとを記録した後、図６Ｘに示すユーザーの識別子Ａと、トークン番号ＴＩＤＡと、端末４ＡのＩＰアドレスまたは位置情報またはコンピュータの装置に固有のＩＤ情報または端末４Ａの入力装置４２Ａのセンサ値から計算される値ＩＰＶと、閲覧時刻Ｔや閲覧履歴情報Ｃｎｔ（Ｃｎｔはアクセス回数）等のログイン状態データをサーバ端末５Ａが記録装置のデータベース５０１Ａに記録することができる。

【０２７２】

端末５Ａの記録装置５０Ａ及び処理装置５１Ａにおいて、コントラクト識別子ＣＰＧＴ、ユーザー識別子Ａ、トークン番号ＴＩＤＡ、値ＩＰＶ、閲覧時刻Ｔや閲覧履歴情報Ｃｎｔ（Ｃｎｔはアクセス回数）等のログイン状態データの対応関係を保存し、図６Ｘと似た表の形式で表示できるよう保存する。

ここで表の形式やデータベースの方式は必ずしも図６Ｘの形式でなくともよい。図６Ｘは表を用いて、あるユーザー識別子・トークン番号に対し複数のＩＰＶ値（３軸の地磁気センサ、３軸の磁気コンパスセンサに異なるＺの値がある場合を示している）が存在し不正アクセスが疑われる場合を検知する際の説明図である。同一の秘密鍵やＯＴＰトークンのトークン番号について異なるＩＰＶ値によるアクセスがあるかどうかを検出できれば良い。図６Ｘは説明図である。図６Ｘのそのままの形式ではなく本発明から逸脱しない限りにおいて図６Ｘの一部を変えてデータを記録してアクセス者の監視に用いてもよい。

【０２７３】

端末５Ａの記録装置５０Ａ及び処理装置５１Ａにおいて、トークン番号ＴＩＤＡについて異なるＩＰＶ値によるアクセスが端末５Ａに対し行われたかどうか検出できる処理部をサーバ端末５Ａに備え、

同一のユーザー識別子Ａの秘密鍵４０１Ａに割り当てられたトークン番号ＴＩＤＡについて、複数のＩＰアドレスや位置情報、位置情報、端末のセンサ値の結合したデータＩＰＶからをもつ装置からの閲覧があったことを検知し、ユーザー識別子Ａに対応するユーザーＵＡに連絡することができる不正アクセス監視機能（図５Ａの５１１Ａ、５１２Ａ、５１３Ａ）を備える。

プログラム４０３Ａに端末５Ａへ接続するＵＲＩを記録することで広告表示機能と共に図６Ｘのような不正アクセス監視機能を持たせることが出来る。前記不正アクセス監視機能を用いて顧客に秘密鍵が不正利用されているか通知することも端末５Ａに備えさせることができる。

平文データ４０３５Ａについても端末５Ａへ接続するＵＲＩを記録させ端末５Ａにアクセスさせ広告の配信機能と図６Ｘのような不正アクセス監視機能を持たせることができる。

ただしソフトウェア４０３Ａにおける端末５Ａを用いた不正アクセス監視機能や広告配信機能は必須の要素ではなく、不正アクセス監視機能や広告配信機能を用いない４０３Ａがあってもよい。

プライバシー保護の観点から不正アクセス防止機能や広告配信機能を使用しない４０３Ａがあってもよい。一方で不正アクセス監視機能や広告配信機能機能は秘密鍵の不正利用を防止し、ＯＴＰトークンの保有者やＯＴＰトークンと対応した暗号化データのコンテンツとその権利者を保護することにつながる。

平文データ４０３５Ａにおける端末５Ａを用いた不正アクセス監視機能や広告配信機能は平文データの権利者が利用を決定する機能であり、コンテンツの保護やコンテンツの権利者が広告による収益を上げること役立つと考えられる。広告へのＵＲＩは平文データ４０３５ＡにＨＴＭＬ言語などで記述され埋め込まれたＵＲＩ（リンクタグ）であったりするため４０３５ＡのＵＲＩ（およびＵＲＩのリンク先の広告コンテンツ）もコンテンツの一部であるかもしれない。

平文データ４０３５Ａにおける端末５Ａを用いた不正アクセス監視機能や広告配信機能はコンテンツの権利者によって利用され、コンテンツの権利者によっては前記機能を利用しないこともある。

【０２７４】

＜不正アクセスの監視ができるシステムへのユーザー連絡先の登録＞
端末５Ａではソフトウェア４０３Ａを利用する際にユーザー登録をし、その際に不正アクセス監視機能において不正アクセスが検知された際の通知先・連絡先を登録する顧客情報データベース管理部５１４Ａと顧客情報を記録する５０４Ａを備える。不正アクセス監視機能（図５Ａの５１１Ａ、５１２Ａ、５１３Ａ）にて不正アクセスが検知された場合５０４Ａに記録された連絡先を用いて不正アクセス通知部５１３Ａが連絡先に不正アクセスの起きた時刻、ユーザー識別子、トークン番号、ＯＴＰトークンのコントラクト識別子とその他サービス提供に必要な情報を通知する。
【０２７５】
＜暗号化されたデータが視聴可能なデータである場合＞
ユーザーは暗号化データ４０３４Ａをソフトウェア４０３ＡとＯＴＰ認証システムを用いて復号し閲覧視聴できる。
【０２７６】
＜暗号化されたデータを復号し編集した後、再度暗号化する場合＞
ユーザーは暗号化データ４０３４Ａをソフトウェア４０３ＡとＯＴＰ認証システムを用いて復号し平文データを閲覧し編集したのち、ブロック番号や閲覧に用いたＯＴＰトークンのＢｎＴＯＴＰとタイムスタンプなどを記録し、改ざん検知用の電子署名やＨＭＡＣを添付したデータを再度暗号化して保存できる。
例えばある団体の職員ＵＰが文章ファイルや音声動画ファイル、表計算ファイルや設計図ファイルなどに修正を加えた後ブロック番号やＢｎＴＯＴＰとタイムスタンプなどを記録し、文章や動画データ改ざん検知用の電子署名またはＨＭＡＣのＭＡＣ値を添付したデータを再度暗号化して保存し、それを団体内の別の職員ＵＡに向けて配布した後、職員ＵＡに復号用の４０３２Ａ等鍵情報と暗号化に用いたソフトウェア４０３ＡとＯＴＰトークンを配布することで、ＵＡは職員ＵＰが再度暗号化されたデータを受けとり、復号し、ＵＰが追記・変更した内容を閲覧しＵＡの手で追記変更し、ブロック番号やＢｎＴＯＴＰとタイムスタンプなどを記録し、文章や動画データ改ざん検知用の電子署名またはＨＭＡＣのＭＡＣ値を添付したのち暗号化して保存することが可能になる。
このようにしてある団体のＵＰやＵＡ、ＵＢ、ＵＣといった複数ユーザー間で機密文書に追記しタイムスタンプやＨＭＡＣのＭＡＣ値または電子署名をデータに添付して施しながら文章のやり取りが出来うる。
【０２７７】
＜暗号化されたデータが３次元の設計図情報である場合＞
暗号化されたデータを復号して得られる３次元のＣＡＤデータ（立体の設計図情報）から、３Ｄプリンタにより造形し、多軸加工機等により母材を加工することで設計図に示された３次元の物体を製作する。ただし平文データのレイティングや出力設定によっては出力できない。銃刀法などの法令に違反する立体物の出力をソフトウェア４０３Ａは禁止するべきであり、平文データのレイティング情報に記述された情報から４０３Ａは立体の出力の可否を判断する。３次元ＣＡＤデータ情報をヘッドマウントディスプレイ４５３Ａで閲覧することもできうる。２次元のＣＡＤデータであっても同様に閲覧や出力や利用ができる。例として産業用印刷機やプロッタなどの加工機に用いる設計図データでもよい。
１次元、２次元または３次元のある物体や装置の製造にかかわる設計図データを本発明の方法で暗号データとして保存し、ＯＴＰ認証システムを利用して復号することで製造に用いる情報に利用してもよい。
【０２７８】
＜暗号化されたデータが回路等の設計図である場合＞
暗号化されたデータが回路の設計図でもよい。例えばプログラマブルロジックデバイスの設計図データでもよい。ＦＰＧＡ（Field Programmable Gate Array）は、プログラマブルロジックデバイスの一種であり、現場で構成可能な回路配列を備えた、デバイス内の電子制御機能を変更できる半導体ＩＣである。本発明の実施例では前記ＦＰＧＡを構成もしくは再構成するための回路のデータを暗号化データとして受信し復号して利用する事

を可能にする。プログラマブルロジックデバイスは産業用機器や放送通信用機器に用いられうる他、ユーザー端末１Ａやサーバ端末３Ａに利用されることも想定される。

再構成可能コンピューティングを可能にする回路情報を暗号化データとして流通させＯＴＰトークンにより復号させてもよい。再構成可能コンピューティングを可能とする暗号化された回路情報はＧｉｔＨｕｂ社のＧｉｔＨｕｂのようなバージョン管理およびコードリポジトリに保存され利用者端末からダウンロードされ配信・配布されてもよい。プログラマブルロジックデバイスの回路情報が改ざんされていないかバージョン管理を行いつつＯＴＰトークンによりその利用権を得て復号しプログラマブルロジックデバイスに設計図に従った回路を動的に構築する事を意図する。

設計図情報をＦＰＧＡなどに展開する際に、仮想機械環境（サンドボックス環境）にて復号データの挙動や悪意あるプログラムの調査を行うことが好ましい。もしくは初回のみＯＴＰ認証システムで暗号データを復号した際に仮想機械環境でデータを調査し悪質でないと判断したのち証明書を発行し、前記証明書のある場合に仮想機械環境を用いずにＦＰＧＡに設計図データをＦＰＧＡなどに展開してもよい。

ＦＰＧＡの例を用いて具体例に説明したがＣＰＵやＳｏＣやＭＰＵといった電子計算機の制御を行う回路の記憶部分に本発明の方法で復号されたデータを記憶させ前記制御演算装置の振る舞いを変えてもよい。あるいは電子計算機端末のファームウェアやＢＩＯＳといったハードウェアに近い証明書付きのプログラムを暗号化し配布しインストールさせるときに利用してもよい。

ある団体の内部で流通させる目的で、電気機器・電子機器の回路基板情報や半導体を半導体基板から最終的なＣＰＵやＳｏＣ、ＭＰＵを製造する装置や回路及び半導体部品製造ラインがあって、その製造にかかわるデータを本発明の方法で暗号化データとして保存し、ＯＴＰ認証システムを利用して復号することで半導体製品の製造に用いる情報に利用してもよい。電子機器に限らず、ある製品の製造データや機密情報に応用してもよい。

【０２７９】

＜４Ｔ．放送での利用（双方向でない暗号化データの流通、ライブ配信）＞

暗号化されたデータやファイル４０３４Ａをネットワーク２０を通じてユーザー端末４Ａに届けるサーバ端末５Ｂは双方向通信が可能な機器であるが、端末５Ｂの代わりに１対複数の放送が行える放送局端末５Ｃ（図５Ｃの５Ｃ、ＳＶＣＲＨＮｂｒｏａｄｃａｓｔｅｒ）を利用できる。前記放送局５Ｃは一対複数の放送による通信経路ＮＴＢ（通信ネットワーク２１、無線放送においては電波の帯域、有線放送においては放送用ケーブル）を用いて、放送を受け取れる受信機４２３Ａを持つユーザー端末４Ａに対し、単一の暗号鍵ＴＴＫＹ４０３３ＡでＡＥＳ暗号化などの共通鍵暗号化を施した暗号化データ４０３４Ａを放送する。前記放送局５Ｃは地上に設置されていてもよいし、移動する局でもよいし、衛星に設置されていてもよい。地上に設置されていてもよいし、宇宙空間に設置されていてもよい。

【０２８０】

＜端末５Ｃが端末３Ａと同じブロックチェーンのノードでありＢｎＴＯＴＰを放送できるとき＞

放送局５Ｃは３Ａと同じ機能を持ちうる。放送局５Ｃは放送局５Ｃを制御する端末５ＣＣと通信経路２（通信網２）を介して接続される。そして端末５Ｃが端末３Ａと同じくブロックチェーン部を持つことの出来る記憶装置を持ち、端末５Ｃを制御する制御端末５ＣＣを介してネットワーク２０と接続され、端末５Ｃと端末３Ａをネットワーク２０と通信経路３で接続できるとき端末５Ｃは端末３Ａと同じブロックチェーン部を持つことができる。そして端末５Ｃは端末３Ａのブロックチェーン部にあるブロック番号Ｂｎやブロックデータ、ブロックハッシュ値、タイムスタンプ・時刻情報、端末５Ｃの時計による時刻情報を放送することができる。端末５Ｃは地上局でも人工衛星の放送局でもよい。

【０２８１】

＜端末５Ｃが全球測位衛星システム用の衛星用端末であって全球測位衛星システム用の信号の認証のためにＢｎＴＯＴＰを測位情報と共に放送できるとき＞

端末５Ｃが宇宙空間にある人工衛星であって、原子時計などを備え、全球測位衛星システム（ＧＮＳＳ）用の測位用人工衛星である場合も考えられる。端末５Ｃがブロックチェーン部を持ち無線によるネットワーク２を介してブロックチェーンのノード端末３Ａと接続される。

そして端末３Ａおよび端末５Ｃに記録されたブロックチェーン部のＯＴＰトークン生成コントラクトを用いてブロック番号Ｂｎに基づいたＯＴＰであるＢｎＴＯＴＰを算出し端末５Ｃの放送信号に原子時計等による時刻情報とＢｎとＢｎＴＯＴＰとトークン番号とユーザー識別子を添付することで、前記信号を受信する端末４ＡにおいてＧＮＳＳ衛星の放送信号を認証できる。

ここで送信メッセージとメッセージのＨＭＡＣによるＭＡＣ値の２つを連結し放送してもよい。１つの測位用データとＢｎとＢｎＴＯＴＰを含むメッセージデータのＨＭＡＣによるＭＡＣ値を、１つの測位用データとＢｎとＢｎＴＯＴＰを含むメッセージデータに添付して放送することにより放送メッセージの改ざんも検知できる。

【０２８２】

端末５Ｃは５Ｃが持つＯＴＰトークンのコントラクトを含むブロックチェーン部の情報と、ブロック番号Ｂｎ及び時刻情報や放送局５Ｃ専用に設定されたＯＴＰトークンのＢｎＴＯＴＰとそれらメッセージのＨＭＡＣのＭＡＣ値を連結して放送することができる。端末５Ｃは時刻情報ＢｎとＢｎＴＯＴＰとトークン番号とユーザー識別子を含む信号を放送し、前記放送を端末４Ａ等は受信する。４つ以上のＧＮＳＳ衛星端末５Ｃからの放送を受信した端末４Ａは全球測位衛星システムＧＮＳＳによる位置の測位を行う。また端末４Ａは端末５Ｃから受け取ったＢｎＴＯＴＰ値とトークン番号とユーザー識別子とブロック番号Ｂｎ（さらに必要に応じてＯＴＰトークンのコントラクト識別子やブロックチェーンＩＤも加え）やＭＡＣ値により時刻情報とその信号の真偽・真贋を検証し、放送されたデータを認証する。

測位用信号をＧＮＳＳ衛星５Ｃから端末１Ａや端末４Ａに測位用の無線による信号を放送し、既知の位置情報を測位するのに必要な時刻情報などに加え、ブロック番号Ｂｎとブロック番号Ｂｎの時間変化により動的に変わる認証用パスワードＢｎＴＯＴＰが信号に添付されていることによりＧＮＳＳの測位放送データの真贋を確認することの出来る手段を備えた、複数の放送局衛星５Ｃにより測位を行う測位システム、測位装置、測位方法に利用されうる。

【０２８３】

ＧＮＳＳ衛星に本発明のＢｎＴＯＴＰによるＯＴＰを添付する意図とねらいは、ＧＮＳＳ衛星の信号がなりすまし（スプーフィング）の偽の信号情報であるか、真のＧＮＳＳ用信号情報であるかを時刻情報とＢｎとＢｎＴＯＴＰとトークン番号とユーザー識別子を添付することで判別することである。ＧＮＳＳ信号のなりすまし・ハッキングに対抗する際に本発明のＯＴＰ認証システムが利用されうる。本発明のこのような利用形態は飛行機や船舶や自動車、無人機、無人飛行機などのナビゲーションにおけるセキュリティ向上のために利用されうるかもしれない。

【０２８４】

ＧＮＳＳ用途に用いる人工衛星５Ｃに秘密鍵５０１ＣとＢｎＴＯＴＰとブロック番号と５Ｃ専用のＯＴＰトークン番号と５Ｃの記録装置に記録されたシークレット値ＫＣ３０１１Ａがあり、それらの内、ＢｎＴＯＴＰとブロック番号Ｂｎとユーザー識別子トークン番号を端末５Ｃは放送する。

【０２８５】

ユーザー識別子は５Ｃの秘密鍵５００から計算される。トークン番号もＧＮＳＳ管理者が設定する。トークン番号には端末５Ｃの人工衛星識別番号・機体番号・製造番号等を割り当て、ユーザ識別子にはＧＮＳＳサービスを行う事業者の管理する秘密鍵から計算されるユーザー識別子が利用されうる。人工衛星毎に異なる秘密鍵とユーザー識別子をもっていてもよいし、事業者が保有する単一の秘密鍵を持っていてそれらを複数の人工衛星の記憶装置に記録させ利用させてもよい。ＧＮＳＳで測位に用いる４つ以上の人工衛星それぞ

れに異なるトークン番号のＯＴＰトークンを割り当て、衛星間で異なるＢｎＴＯＴＰを生成させ放送データに添付することが必要である。

例としてある一つの測位用人工衛星型端末５Ｃの秘密鍵が１０１Ａと同じもので、かつトークン番号ＴＩＤＡのＯＴＰトークンであるとき、ＢｎＴＯＴＰ＝ｆｈ（ユーザ識別子Ａ、機体番号兼トークン番号ＴＩＤＡ、ＫＣ値、ブロック番号Ｂｎ）として計算されうる。ＫＣ値はＧＮＳＳ衛星端末５Ｃの管理者が端末３Ａのブロックチェーン部にＫＣ変更を指示するトランザクションを送信し、端末３Ａと接続された端末５Ｃのブロックチェーンのコントラクトの ＫＣ値も変化する。

ＢｎＴＯＴＰ＝ｆｈ（ Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）を用いたワンタイムパスワードコードＢｎＴＯＴＰを放送局端末５Ｃのブロックチェーン部（５０００Ｃと５１００Ｃ）でＯＴＰ生成関数３００９Ａを実行させＯＴＰとしてＢｎＴＯＴＰを生成し、もしくはネットワーク２やネットワーク２０からブロックチェーンノード３ＡのＯＴＰトークンのコントラクトのＯＴＰ生成関数３００９Ａを実行することで取得し、放送・配信するデータに本体データと時刻情報とブロック番号とＢｎＴＯＴＰを添付することで配信又は放送された情報・データの真偽や真贋を確認することができる。

【０２８６】

ここでＧＮＳＳの放送にＢｎＴＯＴＰを利用する実施形態を示したが、ＢｎＴＯＴＰのかわりにＯＷＰ＝ｆｈ（ Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）を放送・配信するデータに添付してもよい（この場合はＢＣを放送してもよい）。ただしＢｎＴＯＴＰであれば例えば１５秒・１８０秒などで新しいデータブロックがブロックチェーンに連結されＢｎが自動的に更新されるが、ＯＷＰの場合はコントラクトの管理者が任意の時間にＫＣ値やＢＣ値を変更する必要がある。

ＢｎＴＯＴＰに用いるブロック番号の更新時間は１５秒に限らず３０秒でも６０秒でも６００秒（１０分）でもよく、ある時刻に定期的にＢｎが増加すればよい（ブロックチェーンの基盤において新たなトランザクションを含むブロックデータの連結時間を任意の秒数で変更できる）。ＯＷＰを用いるときもコントラクトの管理者が定期的にＫＣ値やＢＣ値の変更を行えばよい。ＧＮＳＳ専用に１０分毎にブロック番号が変化するブロックチェーンを構築すると好ましいかもしれない。

【０２８７】

複数のＧＮＳＳ放送局５Ｃ、具体的には４基の測位用衛星端末５Ｃがあって、それらには異なるユーザー識別子・トークン番号もしくは同一のユーザー識別子・トークン番号が設定され、４つの端末５Ｃは既知のＧＮＳＳによる測位法の測位用情報に加え、ＢｎＴＯＴＰ（ＢｎＴＯＴＰを算出する際に用いたユーザー識別子・トークン番号も添付してもよいし、予め端末４ＡのＧＮＳＳを利用する情報に記録させてもよい）やブロック番号Ｂｎ、そして必要に応じて放送メッセージのＨＭＡＣによるＭＡＣ値を添付し放送する。放送はブロック番号が変化する間に１回以上放送できれば良く、例としてブロック番号Ｂｎが１８０秒で変化するときはＧＮＳＳ衛星５Ｃが１８０秒以内に一回から数回送るなどしてもよい。

ＧＮＳＳのメッセージデータの長さが足りない場合には、ＧＮＳＳに対応させるブロックチェーン部のブロック番号Ｂｎが変わる時間を増加させ、例として１８０秒ではなく６００秒でブロック番号Ｂｎが変わるとき、測位情報の航法メッセージデータ送信の後、３０秒にわたって本発明のＯＴＰ認証データ（ユーザー識別子、トークン番号、ブロック番号、ＢｎＴＯＴＰ、ＨＭＡＣのＭＡＣ値）を放送し、再度航行メッセージデータを放送し、を交互に放送することで放送の途中に認証情報を添付してもよい。

【０２８８】

ＧＮＳＳの既知の例として米国のＧＰＳ（Global Positioning System）に本発明を利用することを仮に想定するとき、位置情報を測定するための４つ以上のＧＰＳ衛星端末５Ｃ（スペースセグメント）を宇宙空間のそれぞれの衛星の軌道に配置され、地上管制局５ＣＣ（コントロールセグメント）とＧＰＳ受信機端末４Ａ（ユーザーセグメント）が存在し、また端末５Ｃや端末５ＣＣと端末４Ａはネットワーク２０を通じてブロックチェーン

のノード端末３Ａや端末３Ｂ等と接続させ端末５Ｃのブロックチェーン部を同期させる。もしくは正確である端末５Ｃの原子時計を頼りにしてＢｎがすべてのＧＮＳＳ衛星端末５Ｃで一致すると考えて３００秒ごとにブロック番号Ｂｎを増やすよう設定し１年に数回地上管制局５ＣＣと衛星端末５Ｃで同期を行い正しく時刻やＢｎが増加できているか確認しＫＣ値などの変更と更新を行った場合はそのデータをすべてのＧＮＳＳ衛星局５Ｃと共有しブロックチェーン部を同期させる。

このとき端末４Ａは端末５Ｃから受信した放送に含まれるＢｎＴＯＴＰをブロックチェーンのノード端末３Ａの認証関数３０１８Ａを用いて認証し、正しいＢｎＴＯＴＰが記録された４つのＧＰＳ衛星の放送データを用いて端末４Ａの位置を測位できる。

【０２８９】

ＧＰＳにおいては、例として、航法メッセージデータ１５００ｂｉｔを３０秒、 認証用データは１つの変数が２５６ｂｉｔで5つある場合は１２８０ｂｉｔなので３０秒以内、両者を連結して順に放送する場合は２７８０ｂｉｔを６０秒にわたり放送する。ブロック番号Ｂｎが６００秒で変化するブロックチェーンをＧＮＳＳ衛星用に構築したとき、１０回にわたり同じＢｎＴＯＴＰデータを送付させることができ、この１０回のうちどれかをユーザー端末４Ａが検出し、ＢｎＴＯＴＰを認証関数で検証し認証結果を求めることで受信した衛星５Ｃのデータが正しいデータであったか、なりすまし等の疑いのあるデータであるか否かが分かる。

もしくは毎回の航法メッセージデータに前記認証データを添付しないことも考えられる。６００秒でＢｎが一つ増えるブロックチェーンを用いるとき６００秒で３０秒放送される航法データは２０回放送されるが、その２０回の航法データの放送枠の内、たとえば４回程度を１２８０ｂｉｔ３０秒の認証用データの放送枠として放送してもよいかもしれない。６００秒の間に４回放送される認証データ付き航法メッセージデータを受信しＯＴＰ認証できれば認証された位置と時刻が測定できうる。

【０２９０】

衛星端末５Ｃと端末４Ａがネットワーク２０から切断されている場合は、端末５Ｃが搭載する原子時計などの時計と記憶部に持つＯＴＰ生成関数３００９Ａを基に、ブロック番号ＢｎとＢｎＴＯＴＰを算出し、ＢｎとＢｎＴＯＴＰとメッセージデータとそれらのＭＡＣ値を添付して端末４Ａ等ユーザーセグメント端末に放送する。

次に端末４Ａには予めＢｎＴＯＴＰ＝ｆｈ（ Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）の計算の出来る認証関数３０１８ＡとＫＣ値が記録されたソフトウェア、もしくはＢｎＴＯＴＰ＝ｆｈ（ Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）を計算できる認証関数３０１８Ａ、３０１８ＡとＫＣ値が記録された端末３Ｃの機能がＧＮＳＳ信号を受信する通信装置４２Ａの４２３Ａに備えられていてもよい。

ＢｎＴＯＴＰの代わりにＯＷＰを用いるときはＯＷＰ＝ｆｈ（ Ａ，ＴＩＤＡ，ＫＣ，Ｂ Ｃ）を計算のできる認証関数３０１８ＡとＫＣ値が記録されたソフトウェア、もしくはＯＷＰ＝ｆｈ（ Ａ，ＴＩＤＡ，ＫＣ，Ｂ Ｃ）を計算できる認証関数３０１８ＤＡとＫＣ値が記録された端末３Ｄの機能がＧＮＳＳ信号を受信する通信装置４２Ａの４２３Ａに備えられていてもよい。

認証関数３０１８Ａ・３０１８ＤＡとＫＣ値が記録されたソフトウェアはソフトウェア４０３Ａに備えられていてもよい。

【０２９１】

ユーザー端末４Ａは複数（４つ以上）の衛星端末５Ｃが放送する測位用信号を端末４Ａの４２Ａの４２３Ａもしくは４２２Ａを用いて受信し、受信信号を処理して衛星と受信機間の距離を測定し，これより位置を計算する。そして既知のＧＮＳＳによる測位法の測位用情報を基に算出した位置に従い現在位置を一時的に仮定する（この段階までは既存のＧＮＳＳと同じであり、本発明のＯＴＰ認証システムが利用できない場合はこの段階の位置情報が利用される）。その後端末５Ｃの放送するＢｎＴＯＴＰのＯＴＰ認証処理に移行する。

【０２９２】

端末５Ｃの放送するＢｎＴＯＴＰのＯＴＰ認証処理では、端末４Ａが受信している人工衛星端末５Ｃの送付する測位用情報に添付されたブロック番号ＢｎとＢｎＴＯＴＰ（またはＢｎＴＯＴＰを算出する際に用いたユーザー識別子・トークン番号も添付されているときは、ユーザー識別子・トークン番号を用いて）をＯＴＰ認証関数３０１８Ａを用いて認証させ、認証関数の戻り値から端末５Ｃの放送したデータの真偽・真贋を判断する。

【０２９３】

端末４Ａにおいて端末５Ｃから受信した測位情報が正しいものか判断するためにネットワーク２０を介して端末３Ａの端末５Ｃの管理者が設定した認証関数３０１８ＡにＢｎＴＯＴＰを算出する際に用いたユーザー識別子・トークン番号とブロック番号Ｂｎ、ＢｎＴＯＴＰを引数として渡して３０１８Ａを実行させ、その戻り値がＯＴＰが正しい時の戻り値であったとき（ＢｎＴＯＴＰが真の値であったとき）、放送局５Ｃの放送が正しいことが期待されることを端末４Ａに記録し、ユーザーに通知・表示させる。

３０１８Ａの戻り値が正しくない戻り値であったとき（ＢｎＴＯＴＰが偽りの値であったとき）その放送局５Ｃに関連する測位情報はＯＴＰ認証のできない偽の情報であることをユーザーに通知・表示させる。

端末５Ｃの放送したデータ情報がＯＴＰ認証できず誤りの時、その後の処理は本発明の認証機能付きＧＮＳＳを用いるサービスやソフトウェアに委ねられるが、位置情報が重要な自動車やその運転に関する分野では認証された位置情報が利用できない旨を伝え、誤った放送を行う端末５Ｃとは異なる新規のＧＮＳＳ放送用衛星５Ｃの信号を受信するよう待機し、新規の端末５Ｃから受信した信号を認証し、認証された端末５Ｃを増やした上で測位を行うようにする等が考えられる。

受信した信号の認証結果が正しくない場合（なりすまし信号である場合）であっても公道を走る自動車を急停止させ別の進路に切り替える等は危険であり、運転や飛行や航行の判断を運転や操縦を行う利用者に委ね、利用者に測位信号に認証できない信号があることを表示して伝えた上で運転や操縦を操縦者など利用者に行わせる必要があるかもしれない。

【０２９４】

＜放送局５Ｃの放送データを認証された位置情報と時間情報データの作成地の位置と時刻を添付する場合＞

ユーザー端末４Ａは４つ以上の端末５Ｃから４Ａの本発明のＯＴＰ認証により認証された位置情報と時刻情報と４つの５Ｃの放送するブロック番号ＢｎおよびＢｎＴＯＴＰに平文データに記録し、秘密鍵４０１Ａ等を用いて改ざん検知用の電子署名やＨＭＡＣを平文データに行い、電子署名またはＭＡＣ値を作成し平文データに添付し、平文データを作成した時刻と位置について認証がなされた状態で保存できる。

【０２９５】

ユーザー端末４Ａは４つ以上の端末５Ｃから４Ａの本発明のＯＴＰ認証により認証された位置情報と時刻情報と４つの５Ｃの放送するブロック番号ＢｎおよびＢｎＴＯＴＰを平文データ（平文のコンテンツデータもしくは原稿データ）に記録し、秘密鍵４０１Ａ等を用いて改ざん検知用の電子署名やＨＭＡＣを平文データに行い、電子署名またはＭＡＣ値を作製し平文のコンテンツデータに添付し、平文データ４０３５Ａを作成した時刻と位置について認証がなされた状態で保存された電子署名またはＭＡＣ値つきの改ざん検知可能な平文データ４０３５Ａとして作成できてもよく、前記４０３５Ａを秘密鍵４０１Ａに割り当てられたＯＴＰトークンによってソフトウェア４０３Ａを用いて暗号化する事が出来てもよい。

平文データ４０３５Ａは取材に関する録音・音声データや録画・動画データでもよい。平文データ４０３５Ａの原稿文章・原稿データ（写真や設計図など画像や録画動画・録画音声）の作成地・作成位置情報と作成時刻を本発明のＯＴＰ認証システムにより簡易に証明する。

前記の４０３５Ａに記入するブロック番号ＢｎはＢｎｐであって、ＢｎｐはＢｎＴＯＴＰを取得したときのＢｎであり原稿となる平文データに記入され平文データの印刷や外部記

憶装置への記憶し配布するか、ネットワーク２０等を用いた配信等で出版され端末の外部に出力されうる。

ＯＴＰ認証コントラクトのＯＴＰ認証関数３０１８Ａや認証を検証する端末３Ｄの認証関数３０１８ＤＡにはＢｎＴＯＴＰ＝ｆｈ（ Ａ，ＴＩＤＡ，ＫＣ，Ｂｎｐ）の形で認証するための認証関数を備え、４０３５Ａにはユーザー識別子Ａとトークン番号ＴＩＤＡが記入されていてもよい。

出版された４０３５Ａの暗号化データ４０３４Ａは流通し、それを復号するトークン番号ＴＩＤＢのＯＴＰトークンとＡＫＴＢとソフトウェア４０３Ａを持つ顧客ユーザーＵＢがいる場合には平文データ４０３５Ａが閲覧などされる。そして顧客ユーザーは平文データ４０３５Ａに記録されたＢｎｐとＢｎＴＯＴＰとトークン番号ＴＩＤＡを用い、さらにユーザー識別子Ａが記入されていればそれを用い、記入されてなければ原稿を作成したユーザーに問い合わせてユーザー識別子Ａを得て、ＯＴＰ認証関数にてＢｎＴＯＴＰ＝ｆｈ（ Ａ，ＴＩＤＡ，ＫＣ，Ｂｎｐ）の形で計算を行えるようＡとＴＩＤＡとＢｎｐを認証関数の引数に渡し認証関数を実行し認証結果を得て作成された時刻や位置情報を得ることができる。作成された位置情報はＧＮＳＳなどを用いた正確な緯度経度を記したものでもよいし、プライバシー保護のため緯度経度情報から地図情報を基に都道府県や市町村（海外では州や省と市町村名）まで分かるようにし詳細な位置ではなくおおよその位置を記載する事もできる。

【０２９６】

＜放送局５Ｃからのデータファイルの放送＞

放送局５Ｃが地上局または人工衛星局であって、アマチュア局および業務用の放送局であり、新聞や雑誌など文章やソフトウェアのデータを放送するデータ放送局や、音声を放送するラジオ放送局や、音声動画を放送するテレビジョン放送局であってもよい。マスメディアとして放送可能なデータを放送できる放送局５Ｃであってもよい。

【０２９７】

ここで文章、音声、動画ファイルの配信に放送局５Ｃを用いる狙いは、ＯＴＰトークンを持つ閲覧権利を持つユーザーに動画データ（書籍データよりもデータ容量が大きい傾向のある音声動画データ）について暗号化データ４０３４Ａをライブ（生放送で）で配信する際に、公共の双方向型ネットワーク２０にかかる通信容量的な負荷をかけないようにすることである。

ただし災害など緊急時は、公共性のある放送局５ＣはソフトウェアＡ４０３Ａといった音声のラジオ放送視聴ソフトウェアや音声映像のテレビビジョン閲覧ソフトウェアに対し暗号化を解除する旨の信号と平文データ４０３５Ａの放送データを放送できることが必要である。

また重複するコンテンツ情報（人気のある楽曲や映像作品などの情報）を双方向のネットワーク２０でユーザーに伝えるよりも放送により１対複数の形でデータを伝えたほうがネットワーク２０の負荷を抑えることにつながり、双方向通信を必要とするブロックチェーンのノード間の通信、電子メール、インターネットバンキングサービス（金融サービス）、ウェブサイトを用いる会員サービスを初めとするサービスに通信の容量を振り向けることができる。

【０２９８】

具体的に本発明をラジオ放送やテレビジョン放送といった音声、動画ファイルの放送に利用すると仮定した場合について述べる。放送に用いる無線機、無線局５Ｃは業務用でもよいしアマチュア用でもよい。広域に、多くの地域に放送する場合について、ある一つの放送局無線機の電磁波が到達する範囲は有限であり、地域ごとに異なる放送局５Ｃ、送信所５Ｃなどの形で設置されている。ユーザー端末４Ａは最寄りの無線局５Ｃの暗号データ放送を閲覧するＯＴＰ生成トークンを取得する。

【０２９９】

放送局５Ｃは放送局５Ｃに固有の共通鍵ＴＴＫＹ４０３３Ａでラジオやテレビジョン番組のデータを暗号化し４０３４Ａとして、電波が届く最寄りのユーザー端末４Ａに放送局

５Ｃが暗号データ４０３４Ａ送信する。そして放送された暗号化データ４０３４Ａを復号し閲覧するソフトウェア４０３Ａにて、サーバー端末３Ａと端末４Ａをネットワーク２０を介して接続させＢｎＴＯＴＰの生成・認証を行い認証関数の戻り値ＣＴＡＵ４０３１Ａを得る。

ここでＢｎＴＯＴＰでなくＯＷＰを取得できるＯＴＰトークンを用いてソフトウェア４０３ＡにてＯＷＰの生成と認証を行い戻り値ＣＴＡＵ４０３１Ａを得てもよい。４０３１Ａと必要に応じて４０３２Ａと４０３Ａ内部の鍵情報４０３０２Ａを用いてＴＴＫＹ４０３３Ａを生成し、ＴＴＫＹ４０３３Ａにて暗号化された放送データを復号し視聴できる。

【０３００】

ＯＷＰを用いる場合はコントラクトの管理者が放送局の指示に従い毎年１年ごとなどある時期にＯＷＰを生産するＫＣ値やＢＣ値を更新する旨の連絡を放送の受信者に行い、受信契約を更新できるユーザーにＫＣ値やＢＣ値を更新した後のＯＷＰを、ネットワーク２０を用いずに郵送で通知させることができる。郵送で通知したＯＷＰをテレビジョン型などの端末４Ａのソフトウェア４０３Ａに入力し認証結果が正しければ放送されるデータの復号ができる。このとき更新されたＫＣ値やＢＣ値は放送データの中に含まれており４Ａが放送データを受信する際に自動的に更新されてもよい。ＯＷＰを用いるときはネットワークに端末４Ａを接続できないユーザーを対象にする。

ネットワーク２０に接続されたユーザー端末４Ａはソフトウェア４０３Ａを利用してブロックチェーン端末３Ａに接続しＯＷＰの生成と認証を行えるため郵送によるＯＷＰの通知は不要である。またネットワーク２０に常時接続されているときはＯＷＰもＢｎＴＯＴＰも用いることもできる。

放送の視聴権であるＯＴＰトークンのコントラクトのＣＴＡＵ４０３１Ａを放送を行う事業者の指示によりコントラクトの管理者端末１Ｃが書き換えることでコンテンツを暗号化または復号するＴＴＫＹ４０３３Ａを変更することができる。例えば１年ごとにＯＷＰのＢＣ値とＣＴＡＵ４０３１Ａを更新することで放送の視聴権を持つユーザーは閲覧を継続でき、視聴権を持たないユーザーは閲覧できないようにする事もできる。

【０３０１】

視聴権を持たないユーザーに閲覧できないようにするためにはＯＴＰトークンのＯＴＰ生成関数がＯＴＰトークンの有効無効を判定するマッピング変数等をトークン番号をキーとしてあって、そのマッピング変数が有効ならばＯＷＰを表示させ、無効ならばＯＷＰを表示させないようにコントラクトの管理者が端末１Ｃを通じて書き換えることができると好ましい。

もしくは放送専用のブロックチェーン部を構築し、毎年ＯＴＰトークンのコントラクトを新規にデプロイする方法も考えられる。毎年ＯＴＰトークンのコントラクトを新規にデプロイする際にＫＣ値を変更することでソフトウェア４０３Ａを用いて暗号化を行うＴＴＫＹ４０３３Ａが変更される。ＯＴＰトークンは契約ができているユーザー識別子（それに対応する秘密鍵４０１Ａに対し）にＯＴＰトークンを配布し閲覧できるようにする。

【０３０２】

パスワードＯＷＰを用いる理由はネットワーク２０が通信障害や災害などで切断された状態ではサーバ３Ａにユーザ端末４Ａが一時的に接続できない恐れがあり、そのような場合において１年ごとに契約が更新される方式であるならば災害が起こった瞬間であってもＢｎＴＯＴＰのようにパスワードがブロック番号Ｂｎによって変化することはないこと、そしてＯＷＰが郵送などで通知でき、ネットワークを利用できない人でも入手できることから災害（１週間から１カ月程度で対応できるもの）に対応できる可能性がある。

【０３０３】

ブロックチェーンのノード３Ａとネットワーク２０を介して同期できる端末５ＣＣとＧＮＳＳなどの人工衛星放送局５Ｃが存在するとき、端末５Ｃの放送データにブロック番号Ｂｎを含み、ソフトウェア４０３Ａ内部にＫＣ値やＣＴＡＵ４０３１Ａといったの生成と認証を行う部分が難読化・暗号化・秘匿化され記録・搭載されている場合はソフトウェア４０３ＡによりブロックＢｎとＣＴＡＵ４０３１ＡからＴＴＫＹ４０３３Ａを

算出し暗号化されたデータ放送を受信できるかもしれない。

【０３０４】

具体例を示す。あるアマチュア局が開局申請を行い、アマチュア局が放送する暗号化データ放送を視聴できる会員権式トークンを本発明のシステムにてＯＴＰトークンとその生成認証コントラクトとしてサーバ３Ａのブロックチェーン上で発行し、ＯＴＰトークンをユーザー間で流通させることができる。トークンを持つ人に対し見ることの出来るＯＷＰとそれを用いて認証やデータの復号と視聴を行うソフトウェアＣＲＨＮ４０３Ａがあればデータの復号と視聴ができる。

これは音声や動画データの放送も可能であり、新聞や雑誌、法令に関する本、教科書、コンピュータソフトウェア（教育用ソフトウェア、オペレーティングソフトウェア、オフィスソフトウェア、ゲームソフトウェア）のような出版の形で用いる形態のデータも送信できる。ユーザーは暗号化されたデータを受信し録画もしくは録音、書物やソフトウェアデータの記録を行い、本発明の認証システムにて復号し閲覧や視聴、ソフトウェアのインストールなどができる。暗号化されたコンテンツデータを放送を受信する形でダウンロードして利用することができる。

【０３０５】

この利用形態において懸念されることとして、天候不順などで通信障害が起こり放送局５Ｃからの無線による信号が端末４Ａに届かないことが考えられる。また放送機材の不良で放送データにノイズなどが混じる恐れがある。動画や音声データの場合はノイズを含んでいても放送番組として成立する事がある（成立させざるを得ないことがある）。しかし雑誌や新聞またはコンピュータプログラムデータの場合はノイズにより閲覧ができなくなるもしくはソフトウェア等が動作しない恐れがある。その対処策として同じ内容の放送を別の日時に複数回行うこと（再放送）、衛星放送の場合は衛星放送の通信速度（通信容量、キャパシティ）を増加させるハイスループット衛星等を利用する、誤り訂正技術が利用する、などの対策をとることが好ましい。

【０３０６】

先の例ではアマチュア局一つの暗号化放送データ４０３４Ａに対しＴＴＫＹ４０３３Ａが一つの場合について述べた。同じ平文のデータまたはコンテンツデータ４０３５Ａであっても異なるアマチュア局の数に対応してトークンとＯＷＰが割り当てられＴＴＫＹ４０３３Ａで暗号化されデータ送信される。

一つの国、もしくは世界規模で、例えば無線を用い衛星放送用い暗号データを送付する場合はコンテンツの権利者が許可する場合に限り、共通のＯＴＰトークン、ＯＷＰ、ＴＴＫＹ４０３３Ａを用いて暗号化しユーザーに送信することもできる。（ただし世界規模で同一のＴＴＫＹ４０３３Ａを用い暗号化する場合はＴＴＫＹ４０３３Ａが漏洩したときに世界中で保存された暗号化データが視聴可能になる恐れがある。そのため局ごと、放送網ごと、地域ごと、国ごとにＯＴＰトークン、ソフトウェア４０３の版、ＯＷＰ・ＢｎＴＯＴＰ、ＴＴＫＹ４０３３Ａを使い分けることが好ましいかもしれない。）

【０３０７】

＜双方向通信暗号化データの流通とライブ配信＞

ウェブミーティングソフト、オンラインゲーム等のライブ配信要素（生放送配信要素）を持つコンテンツの暗号化が可能である。なおソフトウェア４０３Ａを使ってミーティングなどのライブ配信の配信データの収録と暗号化を行いネットワーク２０を介して流通させ配信先に暗号化データを伝えて復号させ視聴させても良いし、配信サイトとして端末３Ｃ（サーバ端末ＳＶＬｏｇｉｎ）を用いてウェブサイト・ウェブアプリにログインする形でもよい。

【０３０８】

ソフトウェア４０３Ａや端末３Ｃを用いて暗号データを配信する際に暗号データの暗号化方式はブロック暗号方式とストリーム暗号方式を用いてもよい。ブロック暗号方式とストリーム暗号方式共に共通鍵暗号による暗号化を平文データに行い暗号化データを生成する。テレビジョンの放送に用いる既知のブロック暗号方式では特許２７６０７９９がある

。またＡＥＳ方式も利用されうる。端末５Ｃからの放送によるライブ配信も同様に暗号化方式はブロック暗号方式とストリーム暗号方式を用いてもよい。

【０３０９】

＜インターネット通信網でやり取りするデータの暗号化、暗号化されていない通信経路において＞

本発明のＯＴＰ認証用コードをＴＬＳによる暗号化通信（ＴＬＳ・ＳＳＬによる暗号化通信）の代わりにウェブサイト通信用のデータ暗号化の鍵に用いる場合について述べる。ソフトウェア４０３Ａで暗号データを例えばユーザーＵＣからユーザーＵＡへ配布することを示したが、それをユーザーＵＡからＵＣに行い、ＵＡとＵＣが相互に暗号化データを行うことで暗号化通信に用いる事につながる。

ここでＴＬＳは Transport Layer Security ProtocolのTransport Layer Securityの略でＲＦＣ８４４６規格。ＳＳＬはSecure Socket Layerの略。

【０３１０】

具体的な例としてウェブページの閲覧において、ある本発明のスマートコントラクトがあり、そのコントラクトではＯＴＰトークンのトークン番号ＴＩＤＡについてユーザーＵＡとコントラクトの管理者ＵＣがワンタイムパスワードＢｎＴＯＴＰを生成し認証できるよう関数が設定され、ＵＣがＵＡのトークン番号ＴＩＤＡのＢｎＴＯＴＰを手に入れられる時（ＵＣがＵＡのＯＴＰ生成関数を呼び出してＢｎＴＯＴＰを見て共有できる）を考える。

【０３１１】

通常、ＯＴＰ生成関数は図６Ａと図６Ｂのフローチャートに記載した通りにＯＴＰトークンの持ち主のユーザー識別子とその秘密鍵から呼び出せるように設計されるが、用途に応じてはコントラクトの管理者であるサービス提供者も管理者端末１Ｃの秘密鍵１０１Ｃを用いてＯＴＰ生成関数を呼び出せるようにしてもよい。ただし、顧客のＯＴＰトークンのＯＴＰ生成関数をコントラクトの管理者が呼び出せるようにする場合はＯＴＰトークンの発行の契約をする際にサービスの規約などに明記することが必要であり、ＯＴＰトークンのＫＮＢＮ変数３０２４Ａに明示して記載することも必要である。

本発明のＯＴＰトークンは端末３Ｃのウェブサイトへのログイン権、端末３Ｄに提示する入場券１８Ａや施錠の解錠鍵１９Ａ、ソフトウェア４０３Ａを用いる暗号化データの復号を行える閲覧・利用・所有権ではあるユーザーが所有することを意図しており、主にＯＴＰトークンを割りあてられた秘密鍵を持つユーザー１人のみがＯＴＰ生成関数を呼び出すことを基本および原則にしている。

ＯＴＰ生成関数を２つ以上の秘密鍵から呼び出せることは通常の実施形態ではないが、実施することもできる。

【０３１２】

次に、ＵＣが運営するウェブサイトにおいてＵＡに対しＢｎＴＯＴＰをＡＥＳ方式などの共通鍵暗号の鍵に用いてウェブページを暗号化し、暗号化されたデータＣＲＹＰＴＷＥＢＰＡＧＥを生成する。そして前記暗号化されたデータＣＲＹＰＴＷＥＢＰＡＧＥを暗号化されていない経路があるネットワーク２２を通じてユーザーＵＡのコンピュータ端末１Ａに送付する。ここでＵＣはＵＡの通信暗号用ＯＴＰトークンのトークン番号ＴＩＤＡがＯＴＰ生成関数３００９Ａにて生成するＢｎＴＯＴＰ値（ＯＷＰ値）を閲覧できることとする。

ユーザーＵＡはトークン番号ＴＩＤＡのＢｎＴＯＴＰ（ＯＷＰ値）を用いて暗号化データＣＲＹＰＴＷＥＢＰＡＧＥを復号し平文のウェブページを閲覧することもできる。同様にＵＣに対してメッセージを送信するときはユーザーＵＡはトークン番号ＴＩＤＡのＢｎＴＯＴＰをＯＴＰ生成関数から取得し暗号化に用い暗号化データＣＲＹＰＴＷＥＢＰＡＧＥをネットワーク２２を通じＵＣのウェブサイトのサーバ端末に送信する。

ＵＣは送付された暗号化データＣＲＹＰＴＷＥＢＰＡＧＥをＵＡの通信暗号用ＯＴＰトークンのトークン番号ＴＩＤＡがＯＴＰ生成関数３００９Ａにて生成するＢｎＴＯＴＰ値（ＯＷＰ値）を呼び出して前記ＢｎＴＯＴＰを復号する鍵として用い暗号化データＣＲＹ

ＰＴＷＥＢＰＡＧＥを復号しＵＡの平文のメッセージを得ることでＵＡとＵＣがネットワーク２２にて暗号化通信を行う。このように暗号化通信分野にも本発明は応用されうる。（ただしこの場合でもＵＡとＵＣがブロックチェーンよりＢｎＴＯＴＰを手に入れる過程での通信は別途暗号化・秘匿化されていなければならない。ＵＡとＵＣが最初にブロックチェーンよりＢｎＴＯＴＰを手に入れる過程での通信はＵＡとＵＣが持つ秘密鍵を用いた公開鍵暗号を基にした暗号化が必要となるかもしれない。秘匿化されたブロックチェーン基盤も必要である。）

【０３１３】

＜不正アクセス情報の監視機能＞

本発明の認証システムにおいて、端末１Ａの秘密鍵１０１Ａ（端末４Ａの秘密鍵４０１Ａ）が流出し不正にサーバ端末３Ｃや端末５Ａ等にアクセスされているか調べる際に、サービスを提供する端末３Ｃや端末５Ａにアクセスする端末１ＡのＩＰアドレスや位置情報、端末１Ａ固有のＩＤ情報をサーバ３Ｃや５Ａ等に保存し監視する機能において、

端末１Ａに固有のＩＤ情報に、１Ａが備える入力装置１４Ａにおいてセンサ１４４Ａに含まれうる加速度計、ジャイロセンサ、磁気センサ、気圧センサ、温度センサ、照度センサを備えさせ、

それらセンサ群のうち1つまたは複数のセンサが測定した物理量に由来する測定値を基にサーバーに保存させる方法が考えられる。

【０３１４】

マイクなど音センサやカメラ、ポインティングデバイス、キーボードといった入力装置の情報も１４４Ａに含まれてもよいセンサとなりうるが、これらを利用することはプライバシーの侵害や個人情報の過度な収集につながりかねず、発明者は推奨しない。キーボードやポインティングデバイス情報を読み取り収集することは入力データを読み取ることにつながりかねないので推奨しない。

【０３１５】

ＩＰアドレスや位置情報は個人の特定につながる恐れがあるが、気圧センサ、温度センサの情報、磁気センサ（磁気コンパス）の情報などはそれぞれのユーザーと端末のいる位置や環境に由来する物理情報であり、これを秘密鍵の不正検出に用いる。（ＩＰアドレスや端末の装置ＩＤやオペレーティングシステムおよびウェブブラウザなど端末のソフトウェア情報については金融用途など重要な取引を行う場合に、顧客の資産を守るために図６Ｘといったデータを記録する際に収集し利用する必要があるかもしれない。）

【０３１６】

漏洩した秘密鍵１０１Ａを用いて不正利用しようとする攻撃者は先に述べたサーバ３Ｃ（ＳＶＬｏｇｉｎ）やサーバ５Ａ（ＳＶＣＲＨＮｃｍ）といった秘密鍵が流出し不正にアクセスされているか調べる処理部と図６Ｘに記載のアクセス情報のデータベースを持たせたサーバーに対し、ユーザーがどのようなセンサの数値でアクセスを行っているか調べなければセンサの数値、センサの検出する物理量を真似してなりすましによる不正アクセスを行うことができない。

前記のように装置１Ａの入力装置のセンサに由来する測定値を本発明の認証システムの不正アクセス検知用の変数に利用することで、不正アクセスを防ぎつつ、ＩＰアドレスや位置情報などの個人情報を基にしない形で不正利用を検知する。

【０３１７】

この利用方法ではユーザーのスマートフォンなどコンピュータ端末のセンサ値をサービスを行うサーバが記録し、同じ時刻に一致しないセンサ値でアクセスされたかどうかを検出するものであるので、センサの測定値と測定値のハッシュ値や匿名化した値を監視に用いることができる。センサの値を使う場合は個人情報の一部を収集してしまうもののサーバーの管理者はユーザーの状態を見守りしやすい。センサの値を基にハッシュ化や各種演算による加工を行った数値を使う場合は個人情報の保護に役立つ。

【０３１８】

もしユーザーが１人だけならばサービスを提供するサーバ（３Ｃや５Ａなど）のユーザ

ー識別子とユーザーのＯＴＰトークンのトークン番号とＩＰアドレスや位置情報と端末ＩＤと端末センサの値の結合値ＩＰＶのリストについて、ある時刻Ｔに対して1つのセンサ値もしくはＩＰＶ値をもったユーザー識別子とユーザーのＯＴＰトークンのアクセス情報が記録されることが正常なアクセスとみなされる。そしてユーザーと不正アクセス者が同じ時刻にアクセスした際には図６Ｘの※２の様にユーザー識別子とユーザーのＯＴＰトークンの情報について異なるセンサ値やＩＰＶ値のアクセス情報が記録される。

前記アクセス情報をサービスを提供するサーバは検出し、トークンの持ち主であるユーザーに異常を通知することができ同じ時刻に異なるセンサ値のアクセスが続く場合にはアクセスを遮断する制御部を持ってもよい。またアクセスデータを保存する記録部を持ってもよい。

【０３１９】

例として同じ時刻に、温度気圧が２５℃、９８７ｈＰａ、地磁気センサが北向きの値を示す秘密鍵１０１Ａを持つ正当なアクセス権を持つ端末１Ａと、３０℃、１０１０ｈＰａ、地磁気センサが東向きの値を示す不正なアクセスを試みる秘密鍵１０１Ａを不正に入手した端末１Ｂからアクセスがあったとき、サーバは異なる環境からアクセスがあったと判断できる。また温度センサ、気圧センサの数値の変化以外にもログイン後の加速度計とジャイロセンサからデータ又はサービスを閲覧するスマートフォンの端末の向きや重力加速度の変化、モーション変化、照度や温度・気圧・湿度といった環境の変化を追跡できる。

センサとしては他に、カメラなどの撮像素子の情報、音センサー（マイク、マイクロフォン）の入力データや測定値も利用可能であるが、利用者にとってはプライバシーが問題になるため推奨はしない。ただし技術的にはカメラなどの撮像素子の情報、音センサーもセンサとして本発明のＩＰＶ値に利用できる。もし利用せざるを得ない場合には、利用者の同意を得た撮像素子や音センサー、マイクの情報も利用する。カメラやマイクの測定値を不正アクセス検知に利用する場合はハッシュ化などを行うことが特に好ましい。

本発明では装置１Ａの入力装置のうちカメラやマイク、キーボード、ポインティングの情報を利用できる。しかし本特許に基づいて実際の業務においてサーバへのユーザの不正アクセス監視用途にユーザーの端末１Ａのカメラ、マイク、キーボード、ポインティングデバイスの入力情報は個人情報やユーザーの出力するＰＩＮ番号などの情報であったり秘密鍵情報の不正な取得に利用されかねないため、利用しないことが好ましい。

【０３２０】

端末１Ａが備える入力装置においてセンサ群のうち1つまたは複数のセンサが測定した物理量に由来する測定値を基にサーバ３Ｃや端末５Ａに保存させる方法では次に示すセンサの利用が考えられる。センサはモーションセンサ、位置センサ、環境センサがあり、モーションセンサには加速度センサ（加速度計）、ジャイロセンサ（角速度センサ）を用いることができる。位置センサには地磁気センサまたは加速度計を用いることができる。環境センサには湿度センサ、光センサ、照度センサ、気圧センサ、圧力センサ、温度センサを用いることができる。

そして認証時にサーバ端末３Ｃ（ＳＶＬｏｇｉｎ）、端末５Ａ（ＳＶＣＲＨＮｃｍ）といった秘密鍵の不正利用を監視する処理部を持ったサーバについて、ユーザーの識別子Ａとトークン番号ＴＩＤＡと、閲覧している時刻Ｔ、閲覧履歴情報Ｃｎｔ、そしてコンピュータの装置に備え付けられたセンサが検出した値から計算される値ＩＰＶを、サーバの記録装置に記録し、異なるＩＰＶからのアクセスを監視するサーバとしたシステムである。閲覧履歴情報Ｃｎｔは金融用途の端末３Ｃの場合は異なる環境からのアクセスかどうか記録するためユーザー端末がログアウトした後も記録し続けることが好ましく、再度ユーザー端末がログインするときに端末３Ｃはユーザー端末が過去に記録した閲覧履歴情報Ｃｎｔと類似する条件でログインしているかどうか判定し大きく異なる環境からログインした場合にはユーザーの連絡先に通知しＯＴＰ認証やあらかじめ設定した第２の秘密鍵（例としてマルチシグ技術用の第一の秘密鍵１０１Ａと第二の秘密鍵１０１Ａ２）に由来するＯＴＰトークンによるＯＴＰ認証を行うようにしてもよい。

（異なるＩＰアドレスやオペレーティングソフトウェアおよびウェブブラウザソフトウェ

アの環境からのアクセスがあることをウェブサービスで表示・通知するのは既知の技術である。）

【０３２１】

＜ブロックチェーン上のコントラクトの管理＞

ＯＴＰトークンのコントラクト管理者ＵＣは端末１Ｃの秘密鍵１０１Ｃによりブロックチェーンノード３Ａにアクセスしサービスを提供する資格のあるユーザーに向けてそのユーザーの識別子にトークンを発行する。

またコントラクト３００８Ａや３００８ＡＧや３００８ＡＡや３００８ＤＡのＯＴＰ生成関数３００９ＡやＯＴＰ認証関数３０１８Ａや３０１８ＤＡのＯＴＰ計算に用いるシークレットキー情報Ｋ値のＫＣ値３０１１ＡやＢＣ値３０１３Ａを関数３０１２Ａや３０１２ＤＡといった手段を用いて書き換えて更新することもできる。他に看板（ＫＮＢＮ）となる変数３０２４Ａを変更できる。

注意するべきこととして本発明のワンタイムパスワード生成関数と認証関数において同一のキー値ＫとＴ値を使用しなければ認証が行えない。

端末１Ａがサーバ端末３Ｃにアクセスするサービスやソフトウェア４０３Ａを用いる暗号化データの復号用途では、端末１Ａは４０３Ａのプログラムに従いネットワーク２０を介してブロックチェーンのノード端末３Ａにアクセスしてワンタイムパスワード（ＯＷＰ、ＢｎＴＯＴＰ）を取得できる。

管理者端末１Ｃのアクセスを端末３Ａが受け付け、ＫＣ値３０１１Ａの変更のトランザクションを端末３Ａは受信しブロックチェーンに連結することでＫＣ値の変更が行え、端末３Ａにアクセスする端末１Ａは端末１Ｃが書き換えたＫＣ値を反映したＯＴＰによる認証ができる。一方で端末３Ｄを用いるサービスではＫ値はＫＣ値３０１１ＤＡやＢＣ値３０１３ＤＡを書き換え更新する手段をコントラクト管理者ＵＣは提供する。

【０３２２】

例としてユーザーＵＡが秘密鍵１０１Ａを用いてアクセスするＯＴＰ生成関数とＯＴＰ認証関数について、ＯＴＰ生成関数とＯＴＰ認証関数が利用するワンタイムパスワードのシード値ＴＩＤＡ、ＫＣ、Ｂｎ、Ａの場合にはＫＣ値３０１１Ａを、ＯＴＰ生成関数とＯＴＰ認証関数ともに同じ値、もしくは同じデータとなるように設定し同期させなければいけない。同期していない場合、生成するパスワードと認証関数内部で計算されるパスワードが一致せず、ワンタイムパスワード認証が行えなくなる。

【０３２３】

ＫＣ値３０１１Ａはコントラクトがブロックチェーンのあるブロックに記録した際に書き込まれ、その後一切書換を行わないようにコントラクトをプログラムすることもできる。またＫＣ値３０１１Ａはコントラクトの管理者のみが変更することもできる。ＫＣ値３０１１Ａの取り扱いはコントラクトの管理者による。ＫＣ値３０１１Ａがコントラクトの管理者によって任意の時刻に変更される場合はパスワードＯＷＰの算出などで用いるＢＣ値３０１３Ａと同じ役割を持つ変数とみなせる。

【０３２４】

ＫＣ値３０１１Ａは本発明を用いるほかのスマートコントラクトとＯＴＰトークンのＯＴＰの値と衝突しにくくするために、例えばＯＴＰ生成コントラクトの識別子やサービス名、書籍等コンテンツの場合にはコンテンツの名前ＩＳＢＮ等に基づいて計算されるＫＣ値３０１１Ａを使うことが好ましい。

ＫＣ値が似通ったもの、例えば２５６ｂｉｔ（符号なし整数値では２の２５６乗の０を含む符号なし整数数値を表現できる）の容量を持つＫＣ値に対し、大きな数値を設定するのが面倒であるなどの理由で０から２５５（２の８乗まで）、さらには０から１０までといった小さい整数の範囲でＫＣ値を記録するなどの運用を複数のＯＴＰトークンのコントラクトで行われてしまうとＯＴＰ値が衝突する恐れがある。

具体例について述べる。ある会員サイトのログインサービスのユーザー識別子Ａのトークン番号９８７６のＯＴＰトークンにおいて、異なるインターネットバンキングのログイン用ＯＴＰトークンの番号９８７６であった時、両サービスのＯＴＰトークンのコントラ

クトのＫＣ値が１２３などと設定されハッシュ関数もＳＨＡ－１を用い同じブロックチェーン識別子のブロックチェーンにデプロイされていた時、ＯＴＰはＢｎＴＯＴＰ＝ｆｈ（共通のＡ，ＴＩＤＡ＝９８７６，ＫＣ＝１２３，共通のＢｎ）として計算され、結果として二つの異なるサービス用のＯＴＰトークン間で一致したＯＴＰが算出されてしまう。

これはウェブサイトログイン用のＢｎＴＯＴＰのみならず施錠用のＯＷＰでも同様のことが起きうる。そこでサービスの異なるＯＴＰトークンのＯＴＰ値の一致・衝突を避けるためにＫＣ値をユニークな値にする必要がありその手段の一つとしてコントラクト識別子情報を含むもしくはコントラクト識別子情報を加工などして匿名化してＫＣ値の一部に用いることが望ましい。

ＫＣ値を複雑にしてＯＴＰトークンのＯＴＰ値が一致しないようにするために、複数のＫＣ値を設定してよい。ＫＣ値は一つでなく複数あってもよく、例として第一のＫＣ値はコントラクト管理者が任意の値（擬似乱数生成器で生成された値やそれを加工したもの、もしくは管理者が思いついた値など）に設定し、第二のＫＣ値はコントラクト管理者がＯＴＰトークンのコントラクト識別子（またはそれを加工し匿名化した値）を設定し、第三のＫＣ値はキー値の更新に用いるＢＣ値と同じ変数型の値であってもよい。

【０３２５】

ＫＣ値やＢＣ値はデータ型を制限しない。符号なし整数型でもよく文字列型でもよく、ＫＣ値やＢＣ値に当たる変数が複数コントラクトに含まれＯＴＰの計算に用いられてもよい。

【０３２６】

本発明ではハッシュ関数ｆｈはＳＨＡ－２のＳＨＡ２５６というハッシュ関数を用いた。ＳＨＡ２５６ハッシュ関数はユーザー識別子Ａとトークン番号ＴＩＤＡとシークレット変数ＫＣとブロック番号Ｂｎやコントラクト管理者の変更するＢＣを基に作成されたメッセージについて３２バイトのハッシュ値ＢｎＴＯＴＰまたはＯＷＰを求め、前記ＢｎＴＯＴＰまたはＯＷＰをＯＴＰに用いる。ハッシュ値ＢｎＴＯＴＰまたはＯＷＰをそのままＯＴＰに用いても良いし、そのハッシュ値をさらに任意の方法で計算・加工してＯＴＰとしてもよい。

【０３２７】

ＯＴＰの計算においてハッシュ関数の衝突が発見されている（もしくは疑いのある）ＳＨＡ－１等のハッシュ関数の使用は推奨されない。そして将来のある時点で既知のハッシュ関数ｆｈの脆弱性が発見された場合、そのハッシュ関数の脆弱性に対する対策をＯＴＰトークンのコントラクトやブロックチェーンの基盤に施すことが必要になるかもしれない。

ブロックチェーンの基盤においてブロックハッシュＢｈの算出に用いるハッシュ関数（例としてイーサリアムではKeccak-256をハッシュ関数に用いる）に問題が生じてしまうときはブロックチェーンの基盤の切り替えが必要になってしまう事もないとは言い切れない。

前記の問題が生じたときはＯＴＰトークンのコントラクトをもちいてＯＴＰの生成と認証を行う方法とＯＴＰトークンの保有者情報を、脆弱性のないハッシュ関数を用いたブロックチェーンあるいは有方向非巡回グラフを用いる新たな分散型台帳システムにＯＴＰトークンのコントラクトとＯＴＰトークンの保有者情報を転記させる必要が生じるかもしれない。

【０３２８】

ＯＴＰトークンの生成と認証を行うハッシュ関数ｆｈをコントラクトの管理者によって任意の種類に変更できてもよい。例えばハッシュ関数ｆｈをＳＨＡ－２のＳＨＡ２－２５６からＳＨＡ－３のＳＨＡ３－２５６にコントラクトのデプロイ後に変更できてもよい。この時もＫＣ値などの時と同じくＯＴＰ生成関数とＯＴＰ認証関数に用いるハッシュ関数ｆｈの種類を一致させなければＯＴＰ認証は行えなくなる。

【０３２９】

＜ＲＦＣ６２３８規格と本発明とのワンタイムパスワード算出に関する処理内容の比較＞
ＲＦＣ６２３８規格ではワンタイムパスワードとの算出にキー値Ｋと時刻により変化するＴ値をハッシュ関数の引数に用いハッシュ値を求めワンタイムパスワードの生成、認証に利用する。前記ＲＦＣ６２３８規格によるとＨＭＡＣに基づくＨＯＴＰ方式のワンタイムパスワード規格においてカウンターＣを時刻Ｔに基づくカウンターに置き換えたものである。次にＴＯＴＰを算出する式を示す。
ＴＯＴＰ　＝　ＨＯＴＰ（Ｋ，Ｔ）
　　＝　Ｔｒｕｎｃａｔｅ（ＨＭＡＣ－ＳＨＡ－１（Ｋ．Ｔ））
ここでＴｒｕｎｃａｔｅ は端数処理である。本発明ではＲＦＣ６２３８にあるＨＭＡＣと組み合わせたハッシュ関数に限らない。本発明ではハッシュ関数もしくはＨＭＡＣと組み合わせたハッシュ関数のいずれかを利用できる。
具体的にはブロックチェーンの基盤で用いるハッシュ関数（イーサリアムで用いるKeccak-256）の他、ＳＨＡ－３、ＨＭＡＣ－ＳＨＡ３、ＳＨＡ－２（ＳＨＡ２５６，ＳＨＡ３８４、ＳＨＡ５１２）、ＲＩＰＥＭＤ－１２８／１６８、ＭＤ５、ＳＨＡ－１等と、ＨＭＡＣ－ＳＨＡ－３、ＨＭＡＣ－ＳＨＡ－２（ＨＭＡＣ－ＳＨＡ２５６、ＨＭＡＣ－ＳＨＡ－３８４、ＨＭＡＣ－ＳＨＡ－５１２）、 ＨＭＡＣ－ＲＩＰＥＭＤ－１２８／１６８、ＨＭＡＣ－ＭＤ５、ＨＭＡＣ－ＳＨＡ－１などである。前記の具体的な関数群はＨＭＡＣを用いている場合もハッシュ関数に基づいており、ハッシュ関数の一方向関数という性質を利用し、引数のメッセージデータ（もしくはキー情報）ごとに異なり衝突しにくい固有のものとみなせるダイジェスト値が計算でき、それをパスワードに利用するという機能に変わりはない。
【０３３０】
本発明ではＲＦＣ６２３８規格を参考とし、その規格で用いるＫ値とＴ値についてブロックチェーン上の時刻において変化する変数ＴＢ（好ましくはブロック番号Ｂｎやある時刻にコントラクト管理者が変更できるＢＣを用いる）とＫ値（シークレットキーＫＣ値、トークン番号ＴＩＤＡ、ユーザー識別子Ａなど）、ハッシュ関数ｆｈを用いてブロックチェーンのコントラクトにアクセスしコントラクトにおいて対応づけられたユーザー識別子の保有するトークン番号ＴＩＤＡのＯＴＰトークンを利用しＯＴＰの生成と認証を行うブロックチェーンベースの時間に基づいて変化するＯＴＰ認証システムに用いることを特徴とする。
本発明のワンタイムパスワードＢｎＴＯＴＰの算出式は以下のようになる。またｎ桁の整数のパスワードＢｎＴＯＴＰ－Ｎも次に示す。
ＢｎＴＯＴＰ　＝　ｆｈ（Ｋ，Ｔ）
　　＝　ｆｈ（ＫＣ，ＴＩＤＡ，Ａ，Ｂｎ）　※具体例。
ＢｎＴＯＴＰ－Ｎ　＝　Ｔｒｕｎｃａｔｅ（ｆｈ（Ｋ．Ｔ））
　　＝　Ｕｉｎｔ（　ｆｈ（ＫＣ，ＴＩＤＡ，Ａ，Ｂｎ）　）　ｍｏｄ　１０^{n}　※具体例、ＢｎＴＯＴＰを符号無し整数化して１０のｎ乗で割り算しその余りをパスワードとする場合。
ここでＵｉｎｔ（Ｘ）は引数Ｘを符号なし整数に型変換する関数。
【０３３１】
＜ＢｎＴＯＴＰとパスワードＯＷＰの算出に関する処理内容の比較＞
時刻により変化するＴ値をＴｍ値として、本発明のブロック番号ＢｎをＴｍとして用いるワンタイムパスワードＢｎＴＯＴＰの算出式の一つの例は次のようになる。ＴｍはＴＢと同じである。
ＢｎＴＯＴＰ　＝　ｆｈ（Ｋ，Ｔｍ）
　　＝　ｆｈ（ＫＣ，ＴＩＤＡ，Ａ，Ｂｎ）　※例
一方、Ｔｍ値をある時刻にコントラクト管理者が変更できるＢＣ値（またはＢＣを変更できる権限のあるユーザーが書き換えることの出来るＢＣの値）を用いて本発明のパスワードＯＷＰの算出式の一つの例は次のようになる。
ＯＷＰ　＝　ｆｈ（Ｋ，Ｔｍ）

＝　ｆｈ（ＫＣ，ＴＩＤＡ，Ａ，ＢＣ）　※例

【０３３２】

ｎ桁の整数のパスワードＯＷＰ－ＮとＢｎＴＯＴＰ－Ｎを次に示す。

ＢｎＴＯＴＰ－Ｎ　＝　Ｕｉｎｔ（　ｆｈ（ＫＣ，ＴＩＤＡ，Ａ，Ｂｎ）　）　ｍｏｄ　10^{n}

ＯＷＰ－Ｎ　＝　Ｕｉｎｔ（　ｆｈ（ＫＣ，ＴＩＤＡ，Ａ，ＢＣ）　）　ｍｏｄ　10^{n}

ＯＷＰ－ＮとＢｎＴＯＴＰ－Ｎは剰余ｒを用いるのでＯＷＰｒやＢｎＴＯＴＰｒやそれらを総称したＯＴＰｒと言い換えることができる。

ここで１０のｎ乗で割り算する例を示したが、１０のｎ乗ではなくＹのＮ乗で割り算して剰余を求めるときを考える。ＯＷＰやＢｎＴＯＴＰといったＯＴＰを符号なし整数に型変換した値ｍを被除数ｍとし、１０のほかに２や３や１１といった２以上の符号なし整数Ｙを１以上の符号なし整数ＮでＮ乗した整数を除数ｎとして、被除数ｍを除数ｎで割った際の剰余ｒを算出し前記ｒを整数値のＯＴＰｒとして用いる処理部と記憶部をコントラクトに備えさせることもできる。ＯＴＰを符号なし整数に変換し剰余を求めたときの整数値ｒをＯＴＰｒとしたとき次のような式となる。

ＯＴＰｒ　＝　ｍ－ｑｎ

ただしｎ＝Y^{N}で、好ましくはＹは２以上の符号なし整数であってＮは１以上の符号なし整数、ｑは商、ｎは除数、ｍは被除数、ｒは剰余。

ＯＴＰとして実用的に用いるにはＹは１０以上かつＮは６から７以上が好ましい。しかし用途に応じてＹが１０かつＮは２や４であってもよい。

明確な注意点としてＹが２かつＮが１の場合、ＯＴＰｒは奇数か偶数かを示す０か１の値を擬似乱数的に出力することとなり、０と１の擬似乱数生成器としては利用できるかもしれないが、ウェブサイトログイン用などのワンタイムパスワードＯＴＰの用途には０と１のどちらかを当ててしまえばログインなどができてしまうので実用的ではない。

そこで、例としてＯＴＰｒで４桁の整数のＰＩＮ番号を表現する場合を考えると、Ｙは２以上Ｎは14以上として除数ｎ＝2^{14}＝１６３８４とする必要がある。

Ｙが１０かつＮが７や６であれば、７桁や６桁のＯＴＰを生成でき、コントラクト管理者にとって整数のＯＴＰの算出や桁数の変更がイメージしやすいため本発明の実施例では１０のＮ乗の剰余をＮ桁のＯＴＰ（ＯＴＰｒ）として用いた。

【０３３３】

＜ブロックチェーン基盤について＞

本発明を運用する中でブロックチェーン部分は技術的もしくは記憶容量などの制限でからある年数ごとにブロックチェーン部を更新したり、新たに作成し直すことが考えられる。ブロックチェーン部のブロックハッシュ算出を行うハッシュ関数を変更する必要も生じることでブロックチェーン部を更新する必要があるかもしれない。

そこで本発明のブロックチェーンを用いたＯＴＰ認証システムではコントラクトに記録されたＯＴＰ生成トークンのコントラクトとＯＴＰ認証コントラクトのプログラム情報、シード値ＫＣやＢＣの情報を管理者が定期的に端末に記録することが特に好ましい。

そしてＯＴＰトークンの持ち主となるユーザー識別子Ａやそのトークンのトークン番号とＯＴＰトークンに付帯するＵＲＩなどのＯＴＰトークンの状態情報を記録し、ＯＴＰトークンの状態情報も保存されたＯＴＰトークンの保有者名簿情報を作成し端末３Ｃや端末３Ｅや端末３Ｆや端末５Ａや端末５Ｂや端末１Ｃ、そしてユーザー端末１Ａの記憶装置に保管することが特に好ましい。ユーザー端末においても保有するＯＴＰトークンの所有する一覧情報を保持することが好ましい。

【０３３４】

本発明ではブロックチェーンを用いて改ざん困難な関数や変数を持つプログラムを実施する形態としてスマートコントラクトを用い、ブロックチェーン上である時刻に変化する値Ｔｍを用いてパスワードを生成し前期パスワードを端末３Ｃや端末３Ｄへ用いることで認証を行うものである。

しかしブロックチェーンは長い時間、例えば１００年を超えて維持される場合には、最新のブロック番号に対して５０年もしくは１００年前にブロックチェーンに記録されたコントラクトのデータについて、１００年間蓄積したトランザクションを含めコントラクトの関数を実行する必要が生じる恐れがある。

【０３３５】

本発明の問題だけでなく分散型台帳技術の課題としてあるトランザクションがあるコントラクトに対し、人の一生を超える年月にわたりトランザクションが蓄積した時の応答が不明である。また計算資源や端末の材料資源、ネットワーク資源、システムを駆動する電力源も持続可能なものでなければならない。

実施例で用いたイーサリアムのブロックチェーン基盤としての稼働実績は本文章作成時においては５年程度であり、紙のように１００年以上にわたり利用され、かつ１００年にわたり情報を記録しうる媒体であるかは未知な点がある。イーサリアムは１００年にわたりあるコントラクトにトランザクションが蓄積しながら運用できた実績はなく、１００年を超えトランザクションが集積された分散型台帳データベースでスマートコントラクトが遅延なく問題なく動作するか不明である。

しかし紙とは異なりまた既存のサーバ端末とも異なる改ざん困難で時刻に関するタイムスタンプやタイムスタンプに対応したブロック番号が刻々と記録されるコントラクト内蔵型データベースシステムを構築できる点に特徴がある。

ＧＮＳＳ衛星端末５Ｃにおいて放送データに認証用情報を添付する例で示したように物やデータに本発明の認証システムによるタグをつけてそのものやデータの真贋を判定したり、デジタルと現実の両方で利用出来うるＯＷＰ型のパスワードを表示させ入場用のチケットや施解錠の鍵に用いられる有価仕様やタグに用いることの出来るＯＴＰトークンや、ウェブサイトへのログインや暗号化データの復号用途に用いることの出来るＢｎＴＯＴＰ型のＯＴＰトークンが実施できる。

【０３３６】

発明者が懸念する点として、１００年を超えブロックチェーン（あるいは有方向非巡回グラフなどを用い改ざん耐性を備えつつスマートコントラクトを実行できるシステム）が運用される際にブロックチェーン基盤において、マークルパトリシア木を代表とするデータ構造があって、計算量0(log(n))でキーと値のペアを検索し挿入削除を行うが、年月の経過とともにブロックチェーンのデータ量が大きくなり端末３Ａや３Ｂといったノードの記憶域を消費するようになる恐れがある。マークルパトリシア木のデータベースに関するデータ検索時間・データ探索時間がより多くかかるなどの恐れがある。より昔、より小さいブロック番号でデプロイされたコントラクト（及びそれに含まれるＯＴＰ生成関数・ＯＴＰ認証関数）ほどブロックチェーン部から読み取りにくくなる、もしくは読み取って関数を実行させる場合に想定以上に時間がかかるのではないかという懸念である。

計算力が高い電子計算機端末や、量子力学に基づいたデータ探索用の計算機端末が産み出され、高速かつ大容量なＲＡＭやＲＯＭといった記憶装置があるとき問題を解決できるかもしれないが、そうならないとき、ブロックチェーン基盤を更新し、過去の分散型台帳システムの分散型台帳をアーカイブし、新たな分散型台帳基盤に過去の分散型台帳で需要のあるコントラクトを転記しブロックチェーン基盤の更新を行うことが求められるかもしれない。

【０３３７】

トランザクションが蓄積したコントラクトを含むブロックチェーンにおいてステートツリーが５年ではなく１００年あるいはそれ以上になるときの計算量0(log(n))がどのようになるか不明である。（イーサリアムはマークルパトリシア木型のステートツリー（状態木）をもちいる。）

ブロックチェーンを構成するデータベースに含まれるトランザクションが増大することで、ステートツリーもしくはブロックチェーンのブロックの長さが大きくなることで、ＯＴＰ生成関数やＯＴＰ認証関数を検索するにの必要な計算量が増え、データ探索時間に必要な計算量が増える恐れがある。そして本発明においてはＯＴＰを生成するコントラクト

のＯＴＰ生成関数やＯＴＰ認証関数の実行に必要な時間が増大する恐れがある。
【０３３８】
そこで、利用者の多いコントラクトをブロックチェーン部が検知し、サーバ３Ａの記憶部の内主記憶装置のＲＡＭ等の計算機端末内で最も高速な読み取りと書き換えを行うことの出来る記憶装置に配置できればコントラクトにアクセスするユーザーはＯＴＰの生成や認証処理の速度を向上させることができる。
【０３３９】
また、本発明では仮にＯＴＰ生成関数やＯＴＰ認証関数の実行に必要な時間が意図せず増大する場合においても、コントラクトの管理者が３０３０ＡによりＢｎＴＯＴＰの表示時間と認証可能な時間（ＯＴＰ認証可能な待ち受け時間）を増大することができ、ＯＷＰを用いるときにはコントラクト管理者がＯＷＰのシード値ＫＣを変更する場合には更新の時間間隔を変えることで処理の遅延などが生じてもＢｎＴＯＴＰやＯＷＰをブロックチェーンより取得し認証させることができる。
【０３４０】
＜ブロックチェーン基盤とＯＴＰコントラクトの更新＞
長い年月の中で技術的な課題や新たな計算機によって公開鍵暗号用の秘密鍵１０１Ａのデータ長などの仕様を変更し、データ長を拡張する必要も生じるかもしれない。ブロックチェーン基盤に用いる公開鍵暗号など暗号化形式やハッシュ関数の安全性に問題が生じる恐れもあるかもしれない。その結果としてブロックチェーン基盤の問題もしくはデータ量の問題からブロックチェーンの基盤を数十年ごとに更新する必要があるかもしれない。
【０３４１】
ブロックチェーン部やブロックチェーン基盤を含めたブロックチェーン部の更新時に、端末３Ａが保有するブロックチェーン部のデータを保存し磁気テープ・磁気ディスクなど半導体メモリ型のＲＡＭよりは低速な読み書き速度ではあるが安価で不揮発性の大容量な外部記憶装置に記録し保存できることも好ましい。
ノード３Ａが記録する更新前のブロックチェーンのフルノードデータを記録することで、トランザクションが外部記録装置に複製されて記録できる。外部記録装置に記録された更新前のブロックチェーンデータは未来のある時点で取引に問題が生じていたことが分かったとき、個人や法人もしくは捜査機関が捜査を行うときに役立つ。
【０３４２】
１００年を超えて運用されるサービスであっても、分散型台帳技術における課題や、想定できない課題により、ブロックチェーンのブロック番号の大きさ、ブロックチェーンのブロックの長さが１００年ではなく２５年といった期間に区切りながら保存することが必要になることも想定される。その事態を想定し、端末３Ａから端末３Ｅや端末３ＦがＯＴＰトークンのコントラクトに関する情報を各コントラクト識別子やユーザー識別子ごとにとりまとめ、新たなブロックチェーンにコントラクト識別子やユーザー識別子に対応した最新の情報を移植もしくは更新できるようにすることも必要になるかもしれない。
【０３４３】
ブロックチェーンの更新、ブロックチェーンのコントラクトの更新に関連し、３Ａに３Ｃや３Ｅや３Ｆや５Ａや５ＢがアクセスしユーザーＵＡらのＯＴＰトークンの資産残高やＯＴＰトークンのＵＲＩなどＯＴＰトークン情報を各々の端末の顧客データベースに記録し３Ａに３Ｃや３Ｅや３Ｆや５Ａや５Ｂがデータベース情報よりユーザーＵＡらの資産残高情報を収集し電子署名やＨＭＡＣを行った残高通帳もしくは残高明細書あるいは残高データをユーザＵＡらの端末に発行できることが好ましい。
【０３４４】
ブロックチェーンの更新が無くとも、サービス提供者やＯＴＰトークンのユーザーの要望によっては３Ａに３Ｃや３Ｅや３Ｆや５Ａや５ＢがアクセスしユーザーＵＡらのＯＴＰトークンの資産残高やＯＴＰトークンのＵＲＩなどＯＴＰトークン情報をデータベースに記録し、ユーザーＵＡらに電子署名やＨＭＡＣを行った残高通帳もしくは残高明細書あるいはＯＴＰトークンの残高・残数データをユーザＵＡらの端末に発行できることが好まし

い。

【０３４５】

サービス提供者の意志に応じてＯＴＰトークンのコントラクトを作り直す場合には顧客のユーザー識別子とトークン番号とトークンに含まれるデータを用いて元のＯＴＰトークンとは異なるコントラクト識別子にＯＴＰトークンのコントラクトを新規にデプロイし、元のＯＴＰトークンのコントラクトに含まれる顧客のユーザー識別子とトークン番号とトークンに含まれるデータに従ってＯＴＰトークンを再発行することでコントラクトの更新を行う。

【０３４６】

＜本発明のＯＴＰ認証システムを実施する形態＞

本発明ではネットワーク２０に接続されたブロックチェーンなど分散型台帳システムＤＬＳのノードとなるサーバ端末３ＡにＯＴＰトークンとＯＴＰを生成するコントラクトを管理者端末１Ｃの秘密鍵１０１Ｃを用いたトランザクションによってデプロイさせて備えさせ、前記ＯＴＰトークンを生成するコントラクトを備えるサーバ端末３Ａにユーザー端末１Ａおよび４Ａが秘密鍵１０１Ａまたは４０１Ａを用いてＯＴＰトークンのＯＴＰを生成する関数３００９Ａを呼び出し、ＯＴＰを生成させ、生成されたＯＴＰを３Ｃや３Ｄ、もしくはソフトウェア４０３Ａのプログラムに従って入力し、認証先が３Ｃや４０３Ａの場合はサーバ端末３ＡのＯＴＰ認証関数３０１８Ａを用いてＯＴＰを認証し、認証先が３Ｄの場合は３Ｄに内蔵された認証関数３０１８ＤＡを用いてＯＴＰを認証し、認証結果の戻り値３０２１Ａが認証結果の正しい時の値であるとき、ＯＴＰ認証が行えたと判断しサービスの提供を行うシステムを実現する。

ブロックチェーンなど分散型台帳システムＤＬＳ上で動作するスマートコントラクトという改ざん困難なプログラムを用いることでＯＴＰトークンの生成関数３００９Ａや認証関数３０１８Ａ、３０１８ＤＡの実行時にその実行結果を改ざん困難な状態で保存でき、またＯＴＰ認証関数やＯＴＰ生成関数およびＯＴＰトークンの所有者情報やＯＴＰを計算するシード値となるＫＣ値３０１１Ａ等といったコントラクトの内部変数も改ざん困難な分散型台帳として記録されるため改ざん困難かつ分散して記録できるブロックチェーンベースのＯＴＰトークンとそれを用いた認証システムと前記システムに用いる装置や端末を実現した。そしてＯＴＰを計算する際に用いるキー値ＫやＫＣをコントラクト管理者の管理者端末の秘密鍵１０１Ｃを用いたトランザクションによって変更しコントラクトに属するすべてのユーザーのＯＴＰトークンのキー値を変え更新できる認証システムと認証システムに用いる装置や端末を実現した。

キー値ＫやＫＣの更新の他にＯＴＰ認証に用いるＯＴＰの桁数やＯＴＰ認証を行える時間間隔をコントラクト管理者の管理者端末の秘密鍵１０１Ｃを用いたトランザクションによって変更可能とした。

秘密鍵の不正利用を検出するためにユーザー端末の環境値や環境値を匿名化した情報をユーザー識別子もしくはトークン番号の値もしくは匿名化した値と対応させ、漏洩した秘密鍵や使い回された秘密鍵による同一時刻へのアクセスを検知できる手段も備えることができる。

【実施例１】

【０３４７】

図８Ａは本発明のワンタイムパスワード認証システム（ＯＴＰ認証システム）においてウェブサイトにログインする際の基本的な認証システム図である。

図８Ａにおいてユーザ端末１Ａ（図２Ａの１Ａ）とサーバ端末３Ａ（図３Ａの３Ａ）とコントラクト管理者端末１Ｃ（図２Ｃの１Ｃ）とログイン先となるウェブサイトを管理するサーバ端末３Ｃ（図３Ｃ）がネットワーク２０を通じて（介して）接続されている。図８Ａから省略しているが図１Ａに示したサーバ端末３Ａと同様のブロックチェーン部を持つサーバ端末３Ｂや端末１Ａとは異なるユーザー端末３Ｂが存在できる。

図７ＤはＯＴＰ認証システムを用いてウェブサイトへログインする際のシーケンスの説明図である。図７Ｄは図７Ａと類似する。

図６Ａと図６Ｂと図６Ｃと図６Ｄと図６Ｅと図６Ｆは図8Aのサーバ端末３Ａの記憶部３０Ａに記録された分散型台帳記録部３００Ａとしてブロックチェーン型のデータ構造を用いたブロックチェーン部３００Ａのブロックチェーン全体部３００６Ａに記録され展開された（デプロイされた）本発明で用いるワンタイムパスワード生成および認証スマートコントラクト（コントラクト）３００８Ａと３００８ＡＧと３００８ＡＡにおけるＯＴＰ生成処理やＯＴＰ認証処理を説明するフローチャートの説明図である。

参考として図９Ａは分散型台帳システムＤＬＳにブロックチェーン型のデータ構造を用いた分散型台帳記録部３００Ａを用いるときのＯＴＰトークンによる認証システムの概要を説明しており、図９Ｂは分散型台帳システムＤＬＳに有向非巡回グラフ型（ＤＡＧ型）のデータ構造を用いた分散型台帳記録部３００Ａを用いるときのＯＴＰトークンによる認証システムの概要を説明する図である。

図７Ａでは端末１ＣはＳ１１０からＳ１１３にかけて端末３ＡのＤＬＳにコントラクトをデプロイしサービスにコントラクトを設定する。Ｓ１１４とＳ１１５ではサービス（主に常時ネットワーク接続される前提である端末３Ｃやソフトウェア４０３Ａによる暗号データの復号の用途等で、ネットワーク２０と切断される恐れがある端末３Ｄもネットワーク２０に接続できるときは図７Ａの形で認証するようプログラムされうる。）から指示を受けた端末１ＣがＯＴＰトークンをユーザー識別子Ａにトークン番号ＴＩＤＡとしてトークンを発行し、また１Ｃまたはサービスはユーザー端末１Ａにトークン番号やトークン発行結果を知らせることができる。

Ｓ１１６ではユーザー端末１Ａがサービスにアクセスし、図６Ｘに示すようにアクセス情報をサービス側が記録することもできるし記録しないこともできる。次にサービスは１ＡにＯＴＰ認証を求め端末１Ａは端末３Ａにアクセスし Ｓ１１７からＳ１１９のシークエンスでＯＴＰ生成関数３００９ＡからＯＴＰを取得する。ＯＴＰはハッシュ関数にＳＨＡ２５６を用いたときは３２バイト（符号なし整数にして２の２５６乗－１）のデータとして計算され出力される。

（３００９Ａと３０１８ＡにＳＨＡ２５６を用いたデータを符号なし整数値に型変換し、ある整数ｎで割ったときの剰余をある桁数の整数値のＯＴＰとしてもよい。例として３２バイトのデータを符号なし整数に型変換しその１０のＮ乗の剰余ＯＴＰｒをＮ桁の符号なし整数のＯＴＰとして用いてもよい。前記の様に実施例１のみならず実施例１や実施例３でもハッシュ関数から出力されたデータを符号なし整数等に型変換してある桁数や文字数にして本発明の認証システムを構築する際はＯＴＰ生成関数３００９ＡとＯＴＰ認証関数３０１８Ａや端末３Ｄに搭載する３０１８ＤＡも対となるＯＴＰ生成関数と同じようにＯＴＰの計算を行い剰余によるパスワードＯＴＰｒを計算できなければ認証できない。）

そしてＳ１２０ではサービスが接続中の１Ａのアクセス状況や挙動を収集し記録することもできるし収集や記録をしないこともできる。Ｓ１２０ではＯＴＰ認証を端末１Ａに要求しする。端末１ＡはＳ１２１からＳ１２３にかけてＳ１１７からＳ１１９で取得した値とユーザー識別子とＯＴＰトークンのトークン番号をＯＴＰ認証関数３０１８Ａに入力し認証関数３０１８Ａを実行させＳ１２３にて認証結果３０１８Ａ等の戻り値ＣＴＡＵを端末３Ａから得てサービスに認証関数の戻り値ＣＴＡＵを入力・出力する。端末１Ａの出力した認証関数の戻り値ＣＴＡＵがＯＴＰ認証結果が正しい時の値であればウェブサイトへのログインやウェブサイトの操作・ウェブサービスの操作を行わせる。

Ｓ１２５ではログイン後も端末１Ａのアクセス情報をサービス側は収集し不正アクセスがないかどうか、秘密鍵の多重利用による同一のＯＴＰトークン番号ＴＩＤＡとユーザー識別子Ａに対し異なるＩＰアドレスや位置情報や端末のＩＤ値そして端末のセンサ値が図６Ｘに示すように記録されないかどうか監視し記録された時は不正アクセスをユーザーに通知できる。しかし実施時には図６Ｘのように記録することがプライバシー侵害や端末の計算資源を不要に利用してしまい経済の費用対応化に見合わない恐れもあるので必ず行わなくともよい。

本発明においては、例として暗号化データの復号によるコンテンツ閲覧利用やインターネットバンキング用のログインや銀行口座残高の操作といった金銭的価値・重要なものを扱

うＯＴＰトークンが割り当てられた分散型台帳システムへのアクセス用秘密鍵の漏洩や使い回しを検知する手段として図６Ｘのデータ収集と監視を行いたいのであり、本発明を用いて例えば簡易に世界規模で匿名性を生かした会員サイトや投票サイトなどを計算力の低い端末をサーバとして作りたいといった用途に用いる場合には図６Ｘのデータ収集と監視を行わない。図６Ｘによるサービスへの不正アクセスの監視は本発明の利用形態に応じて用いる。

【０３４８】

実施例１（実施形態１）では、図６Ａと図６Ｂと図６Ｃと図６Ｄと図６Ｅと図６Ｆに記載のＯＴＰ生成およびＯＴＰ認証を行うＯＴＰの計算はハッシュ関数ｆｈと、そのｆｈの引数に、

ブロックチェーン部へのユーザー識別子Ａと、

Ａに対応図けられたトークン番号ＴＩＤＡ、

コントラクト内部のシークレット変数ＫＣ、ブロック番号Ｂｎの4つを用い、

さらにコントラクト管理者が変更可能なシークレット変数ＢＣと、

ブロックチェーンのシステムを構成するノードの投票値で決まる値ＧａｓＬｉｍｉｔ値をＶとして、

ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，ＢＣ，Ｖ）を計算させＯＴＰを算出させることで、

ユーザー識別子およびトークン番号によって異なる専用のＯＴＰを生成させ、

Ｖ値によって疑似的なランダム性を備えさせ、シークレット変数ＫＣとＢＣのうちＢＣ値を更新できるＯＴＰ認証システムを構築した。

【０３４９】

実施例１では図８Ａのサーバ端末３Ａのブロックチェーン上のコントラクト３００８Ａと３００８ＡＧと３００８ＡＡは、コントラクト内部の変数ＫＣ（図３ＡＣの３０１１Ａ）またはＢＣ（図３ＡＣの３０１３Ａ）と内部変数ＫＣまたはＢＣまたはその両方を書き換えて更新できるセッター関数ｆｓｃｂ（図３ＡＣの３０１２Ａ）を備えている。

前記セッター関数ｆｓｃｂ（図３ＡＣの３０１２Ａ）はコントラクト管理者の端末１Ｃが備える秘密鍵ＰＲＶＣ（図２Ｃの１０１Ｃ）によってブロックチェーンにアクセスされるときに限り変数ＫＣ（図３ＡＣの３０１１Ａ）またはＢＣ（図３ＡＣの３０１３Ａ）と内部変数ＫＣまたはＢＣまたはその両方を書き換えて更新できるよう関数ｆｓｃｂ（３０１２Ａ）はプログラムされる。

コントラクト内部変数値は秘匿化されていることが好ましい。

３００８Ａは同一のコントラクトに内部変数ＫＣ値やＢＣ値が記録されているが、３００８ＡＧと３００８ＡＡの二つのコントラクトを用いる場合にはＯＴＰの計算に用いる変数ＫＣ（３０１１Ａ）、変数ＢＣ（３０１３Ａ）を関数ｆｓｃｂ（３０１２Ａ）で書換更新し３００８ＡＧと３００８ＡＡのＫＣ値及びＢＣ値を一致させ同期させ、同期した状態を保つ必要がある。ＫＣやＢＣの変数の個数やデータ型等は限定しないが、設定したＫＣやＢＣに該当するデータの個数や量に応じて一致させるべき数値も増える。前記のＫＣやＢＣのほかにＯＴＰ認証の待受け時間を変える関数及び変数３０３０ＡやＯＴＰｒを求めるためのＯＴＰｒ桁数変更用関数及び変数３０３１Ａも３００８ＡＧと３００８ＡＡの間で同期させて一致させなければいけない。また変数の他ＯＴＰを計算するために必要なハッシュ関数ｆｈの関数の種類を一致させなければならない。

ここで端末３Ｃでは３００８ＡＧと３００８ＡＡを用いるが、端末３Ｄでは３００８Ａまたは３００８ＡＧと端末３Ｄの認証関数３０１８ＤＡを用いるので端末３ＤにＫＣ値やＢＣ値や３０３０Ａや３０３１Ａを設定する場合には３００８Ａまたは３００８ＡＧの変数・関数の記憶部と端末３Ｄの変数・関数の記憶部を一致させ同期しなければいけない。

【０３５０】

またコントラクトの管理者はその端末１ＣからコントラクトにＯＴＰトークンの名前やサービスの名称、サービス提供者の住所連絡先、レイティング情報などサービスを提供するうえで必要な情報を示した看板変数とその変数を変更書換できる関数ＫＮＢＮ（３０２４Ａ）をコントラクトに記録させ設定できる。ここで看板として記録する変数の数や配列

、構造体、マッピング型など型を問わない。変数３０２４Ａはブロックチェーンにアクセスするすべてのユーザーが読み取る事のみできる（ＫＮＢＮの書換は端末１Ｃの秘密鍵ＰＲＶＣ（１０１Ｃ）を用いて行われる）。

【０３５１】

実施例1に限らず実施例２や３にも起きうる問題として管理者端末１Ｃの秘密鍵ＰＲＶＣ（秘密鍵１０１Ｃ）が管理すべきユーザーの手から漏洩し、別のユーザーが秘密鍵１０１Ｃ情報を入手し、その情報を複製し、端末からコントラクト３００８Ａなどに不正アクセスし、サービスを受けさせる権限である本発明のＯＴＰトークンを不正アクセス者が望むユーザー識別子に無制限に発行することが可能になりうる。そして看板情報３０２４Ａや内部変数３０１１Ａおよび３０１３Ａにアクセスする可能性が考えられる。

このような事態が起きないよう、コントラクト内部にあるトークン発行関数（図３０４３Ａ）や関数ｆｓｃｂ（３０１２Ａ）や３０２４Ａ等に含まれるセッター関数を実行する際に秘密鍵１０１Ｃとは異なる秘密鍵に由来するユーザー識別子の同意がなければ関数関数を実行させないようにするコントラクト管理者秘密鍵漏洩対策部分３０４２Ａを備えることができる。

【０３５２】

＜コントラクト管理者の秘密鍵が漏洩することに備えた対策例＞

コントラクト管理者秘密鍵漏洩対策部分３０４２Ａについて説明する。

ＯＴＰを管理するコントラクトの内部変数やトークン発行を関数として実行する際に、関数の実行を行うには秘密鍵ＰＲＶＣのユーザー識別子Ｃのコントラクト管理者以外の1つまたは複数のユーザ識別子が個別に設定できるマッピング変数または配列、構造体、それらと同等の複数変数があり、ユーザー識別子と対応したブーリアン型（真偽型）の変数値において真か偽かを記録させる。

そしてユーザー識別子に対応した真偽値が真であるとき実行でき、偽であるとき実行しないとする。ここで全てのユーザー識別子に対しユーザー識別子に対応した真偽値が真であるときＯＴＰトークンの発行やコントラクト内部変数の操作を行い、全てのユーザー識別子のうち1つでも真偽値が偽になっている場合関数の実行を停止する場合が考えられる。この応用として全てのユーザー識別子に対しユーザー識別子に対応した真偽値の真もしくは偽の数を数え、全ユーザー識別子数の過半数（あるいは設定した割合）を超えたときに関数の実行を行うこともできる。

３０４２Ａにはユーザー識別子に対応した真偽値をもつマッピング変数とその変数の真偽値から処理を実行させるか停止させるか判断する処理部を持ち３０４２Ａはトークン発行関数３０４３Ａや関数３０１２Ａ等のコントラクトの状態を限定したアクセス者に対して読取または書き換えを行う関数の処理部に記述（設定）することができる。

【０３５３】

＜コントラクト管理者の秘密鍵が漏洩することに備えた簡易の対策＞

例えば二つの異なる秘密鍵を用いてコントラクト管理者としてアクセスしてもよい。コントラクト管理者の秘密鍵の鍵ＰＲＶＣとＰＲＶＣが漏洩した際にＯＴＰトークンの発行等を停止するための秘密鍵ＰＲＶＢを用意し、ＰＲＶＣ２のみアクセスできる関数実行停止変数とそのセッター変数を備え、関数実行停止変数が真であるときに関数を実行し、偽であるときに関数を実行しないようにする処理をＯＴＰトークンの発行関数やコントラクト内部変数（図３ＡＣにおける３０４３Ａや３０２４Ａ、３０３０Ａ、３０３１Ａ、３０１１Ａ、３０１３Ａ）について設定できる。

本発明に記載の方法以外にも一般にマルチシグ技術と呼ばれるものを用いて複数の秘密鍵を設定し、秘密鍵の流出に対応してもよい。

【０３５４】

サービス提供者が秘密鍵を漏洩したこと、攻撃を受けている事、攻撃を受けた時刻をコントラクト識別子３０１９Ａとともに自社のウェブページ等に掲載し、ユーザーに周知し、漏洩した秘密鍵とは異なる新たな秘密鍵でコントラクトをデプロイしＯＴＰトークンの再発行をすることもできる。ブロックチェーンを含む分散型台帳システムにおいて技術的

に問題が生じ、新たなブロックチェーン等へトークンを移転させるるために再発行を行うことも考えられる。
本発明は改ざん困難なブロックチェーン上でＯＴＰを流通させＯＴＰトークンをもちいてサービスの提供を自動化したり記録するものであって、サービスを提供するかどうかは最終的にはサービスを購入した時の契約内容や、法による制限、そしてサービス提供者とユーザーとの合意により決まる。
サービスの提供が困難な場合にユーザーに連絡先を伝えたいとき、あるいはサービスの提供者に連絡を取りたい場合には看板情報ＫＮＢＮ（３０２４Ａ）にて連絡先を掲示することが必要である。サービスのレイティング（サービスに年齢制限があるか、サービスが自動車の鍵である場合は運転免許証が必要か等の制限情報）も３０２４に記入される。
本発明ではトークンは電子商取引を用いて購入する形で発行することを意図している。電子商取引ではクレジットカードなどの情報を用いるがその場合は成人が対象となる。本サービスを未成年のコンピュータゲームサイトやウェブアプリへのログインそして暗号化された書籍データの復号用とする場合は秘密鍵を記録した端末を家族用として購入し、その端末を未成年に買い与えるといった考え方が必要かもしれない。
端末１Ａを持たないユーザーＵＡがＯＷＰ型の１８Ａや１９Ａを入手したい場合は電話などでサービス提供者やチケット等発券者、コンビニエンスストア店舗などで代理でＯＴＰトークンとサービス用のＯＷＰつき１８Ａや１９Ａを発行させることもできる。
秘密鍵１０１Ａを記録させたＮＦＣタグ１９Ａや１６ＡをＵＡが所持し、コンビニエンスストアなど店舗に備え付けられた秘密鍵の無い端末１Ａに１９Ａや１６Ａの秘密鍵情報を読み取らせることでログインできるかもしれない。端末１Ａやインターネット回線を提供するインターネットカフェやホテル、民宿などの店舗でも利用出来うる。
【０３５５】
＜トークンの発行＞
図８Ａにおいて図７Ｄに記載のシーケンス図に従い、秘密鍵ＰＲＶＡ（図２ＡＡの１０１Ａ）と秘密鍵１０１Ａから計算されるユーザ識別子Ａに対しコントラクト３００８Ａまたは３００８ＡＧがトークン番号ＴＩＤＡのＯＴＰトークンを発行する。
本発明のすべての実施例ではブロックチェーン部にイーサリアム（Ethereum）のＥＲＣ７２１規格のトークンにＯＴＰを計算するシークレット変数（シード値）ＫＣ、ＢＣとＯＴＰの生成関数（図６Ａ，図６Ｂ）及び認証関数（図６Ｃ、図６Ｄ、図６Ｅ、図６Ｆ）を追加する形で、ブロックチェーン上にてワンタイムパスワード生成及び認証を行うコントラクトを構築した。トークンの所有関係（トークン番号とユーザ識別子との対応関係）はユーザ識別子Ａの秘密鍵ＰＲＶＡ（１０１Ａ）に対してブロックチェーン上のコントラクト内部に記録される。ＥＲＣ７２１規格ではトークンの発行、トークンの送信（譲渡）、トークンの除去などの機能があるがその説明は省略する。本発明ではＥＲＣ７２１規格においてトークン送信を制限する譲渡制限機能を搭載することができる。
これは本発明において譲渡を許可しないチケットや会員権やオンラインゲーム及びネットバンキング用のログイン用途のＯＴＰトークンとすることを意図しているためである。
コントラクトの管理者によってトークンの送信を制限する変数及びセッター関数３０４１Ａを用いてトークン送信関数３０４０Ａの実行を制御できる。３０４１Ａの変数が真であるときはトークン送信関数３０４０Ａの実行を続け３０４１Ａの変数が偽であるときはトークン送信関数３０４０Ａの実行を停止するというように３０４０Ａをプログラムすることができる。
譲渡制限ではなく譲渡を禁止したい用途ではトークンの契約者に譲渡を禁止することを伝えた上でトークンを発行することを前提とし、３０４１Ａの変数を偽に固定し、３０４１の変数を変更できるセッター関数を除いて、常にトークン送信関数３０４０Ａを実行できない様にプログラムしたＯＴＰトークンのコントラクト３００８Ａ及び３００８ＡＧであってもよい。またはトークン送信関数３０４０Ａそのものを除いたＯＴＰトークンのコントラクト３００８Ａ及び３００８ＡＧでもよい。
次に図７Ｄのシーケンス図を用いてコントラクトのデプロイからＯＴＰトークンの発行と

トークンを用いたサービスの提供を説明する。

【０３５６】

図７Ｄにおいてユーザー端末１Ａとブロックチェーンシステムｄｌｓをもつサーバ３Ａ（実際はイーサリアムのテストネット）、ウェブサイトログインサービス用サーバ３Ｃ、ＯＴＰトークン及びＯＴＰ認証システムに関するコントラクトをデプロイし管理しトークンの発行をすることの出来る秘密鍵１０１Ｃを記憶装置１０Ｃに備える管理者端末１Ｃがある。

【０３５７】

シークエンスＳ２１０において端末１ＣにてブロックチェーンにデプロイするＯＴＰトークンのシークレット変数ＫＣ（図３ＡＣの３０１１Ａ）またはＢＣ（図３ＡＣの３０１３Ａ）や看板情報３０２４Ａ、ＯＴＰを変更する時間（ブロック数）を変更するブロック番号剰余変数３０３０ＡやＯＴＰ桁数調整部３０３１Ａ等を設定する。そしてＯＴＰを生成認証するコントラクト３００８Ａ、ＯＴＰを生成するコントラクト３００８ＡＧ、ＯＴＰを認証するコントラクト３００８ＡＡを設定する。

実施例３ではＯＴＰの生成と認証ができるコントラクト３００８Ａを用いる。

実施例２ではＯＴＰの生成ができるコントラクト３００８Ａ又は３００８ＡＧとＯＴＰの認証ができる端末３ＤのＯＴＰ認証関数３０１８ＤＡ及び前記関数の変数や関数の記録部を用いる。３Ｄがネットワーク２０を通じてノード３Ａに接続し通信できる場合は３００８ＡＡや３００８Ａの認証関数３０１８Ａを利用できるようにしている。

実施例１ではＯＴＰの生成ができるコントラクト３００８Ａ又は３００８ＡＧとＯＴＰの認証ができるコントラクト３００８ＡＡを組み合わせて用いる。

【０３５８】

シークエンスＳ２１１でブロックチェーンにコントラクトをデプロイする。コントラクトのコード（イーサリアムバーチャルマシンの実行用バイトコード、バイトコード）をブロックチェーンにトランザクションとして送信し、ブロックデータに記録させる。ログイン用途では認証を行いログイン後に認証コントラクト３００８ＡＡにユーザーがトークンに紐図けられた値（トークンとユーザー識別子に対応した銀行口座残高のマッピング変数、残高からの送金処理、会員サイトでのポイントや投票値）の操作を行いたい場合がある。

そこでここでは図３ＡＣの３００８Ａ（図３ＡＢの３００８ＡＧでも実施可能）をＯＴＰ生成トークンを記録したＯＴＰ生成コントラクトとし図３ＡＢの３００８ＡＡをＯＴＰ認証コントラクトとして、ブロックチェーン上に別々にデプロイする。（図９Ａのようにブロックチェーンのブロックデータ Bd0から Bd7のうち、Bd1、Bd3、Bd4へデプロイされる。デプロイされたデータに端末１Ａがアクセスしてｏｔｐの生成と認証を行う。）

【０３５９】

シークエンスＳ２１２ではコントラクトがブロックチェーンに組み込まれた際に決定したコントラクト識別子（コントラクトアドレス）をブロックチェーン部から端末１Ｃの記録装置（１０Ｃ）に取得しウェブサイトにログインするサーバ３ＣのウェブサイトのＥＣＭＡＳｃｒｉｐｔなどのウェブページを動作させるプログラムに記録させ設定する。同時にウェブページを動作させるプログラム（フロントエンド、サーバーサイド、データベース、そして必要に応じてブロックチェーン部など含む）を設定する。

【０３６０】

シークエンスＳ２１３ではＯＴＰを生成するＯＴＰトークンの発行を行う。サービスの契約や購入を行ったユーザー識別子Ａに対し管理者端末１ＣはデプロイしたＯＴＰ生成トークンにアクセスしてトークン番号ＴＩＤＡのＯＴＰトークンを発行する。発行されるＯＴＰトークンは３００８Ａまたは３００８ＡＧに示すコントラクトであり実施例1ではＥＲＣ７２１規格の機能を持つ。ＯＴＰトークンは電子商取引などで決済手段を用いてログイン権として購入されるか、インターネットバンキングを代表とする銀行など金融分野のサービスや会員サイトのログインサービス、ソーシャルネットワーキングサービスＳＮＳのログインサービス、オンラインゲームなどのログインサービスに付属して発行される。

【０３６１】
本発明のＯＴＰ認証システムを提供する際に決済はブロックチェーン外で行われることを想定している。しかしイーサリアムではメインネットにおける暗号資産イーサの払い込みに応じて決済を用いてＯＴＰトークンを付与すること（つまり自動販売機のようにユーザーがイーサをコントラクトに硬貨の様に投入し、そのユーザーに対しＯＴＰトークンを送付する事）も可能である。ただしサービスによってはブロックチェーンの外で人員が契約や決済の有無、ＯＴＰトークンを付与するユーザーの実在性確認、本人確認、ＫＹＣ（Know Your Customer）をする必要があると考えられるのでブロックチェーンの内部通貨を用いた決済は必須としない。とくに銀行や証券などの金融分野では本人確認が必要であると考えられるので、本発明のＯＴＰトークンの契約や発行にはブロックチェーン外でユーザーを確認する人員や装置が必要である。
【０３６２】
シークエンスＳ２１４ではウェブページへのログインを行う。ＯＴＰトークンを付与されたユーザーは秘密鍵１０１Ａ（秘密鍵ＰＲＶＡ）を記憶装置１０Ａもしくは外部記録装置１６Ａに記録させた端末１Ａを用いてサーバ３Ｃ及びブロックチェーンシステムＤＬＳにアクセスする。端末１Ａのアクセスを受けたサーバ端末３Ｃは端末１Ａのアクセスに応じてウェブサイトまたはウェブアプリのデータを端末１Ａに配信する。
３Ｃはシークエンス Ｓ２１４では例としてログイン時のユーザー名とパスワードの入力を要求するウェブページデータを端末１Ａに配信し1段階目の認証を要求する。
ここでウェブブラウザの拡張機能にウォレットソフトウェアがあってウォレットソフトウェアに秘密鍵が搭載されているか判断するプログラムをウェブページデータに備えていてもよく、ウェブブラウザの拡張機能等に記録されたウォレットソフトウェアとウォレットソフトウェアに記憶された秘密鍵を用いてＯＴＰ生成を行いＯＴＰ認証を行えるようにしてもよい。また秘密鍵を記入し記録しブロックチェーンにアクセスしＯＴＰを表示させるソフトウェアを端末１Ａの記憶装置１０Ａの１０２Ａに搭載していてもよい。ユーザー名とパスワードが一致した場合に次のシーケンスに続く。（ユーザー名とパスワードは認証の１つの要素として用いる。ＯＴＰ認証と既存のユーザー名・パスワード認証を合わせて２要素または２段階認証とする。のユーザー名・パスワード認証のほかに用途によってはＰＩＮや生体認証でもよい。）
【０３６３】
シーケンスＳ２１５ではＯＴＰ認証を行うためのユーザー端末１Ａのアクセスをサーバ端末３Ｃが受けて、端末３Ｃから端末１ＡへＯＴＰの生成を行わせるウェブページを配信するとともに、そのユーザー端末１Ａのアクセスを不正なアクセスか否かを監視する。ウェブページ上でＯＴＰを生成するにはユーザー識別子とトークン番号の入力を要求し、ユーザーのユーザ識別子やトークン番号等の入力値と、ユーザー端末のＩＰアドレスや位置情報や端末の入力装置のセンサ値などを含むＩＰＶ値と、ログイン時刻やログイン回数やログイン状態について図６Ｘのように記録する。通常の端末３Ｃの利用において、同一時刻に１人の個人が1つの秘密鍵を１つの端末からサーバ端末３Ｃへアクセスする場合は、図６Ｘに記載の異なる複数のＩＰＶ値は記録されないはずである。
また端末３Ｃはウェブブラウザのバージョンなど端末に固有の情報とＩＰアドレスといった値を収集できる場合には、その情報を次回のユーザーＵＡの端末１Ａのログインまで端末３Ｃの記憶装置に記憶しておくこともできる。次回のログイン時に記憶されたアクセス情報を照らし合わせてアクセス環境の変化を検出してもよい。
【０３６４】
シーケンスＳ２１６及びＳ２１７ではＳ２１５で配信されたウェブページのＥＣＭＡＳｃｒｉｐｔ等プログラムに応じて、ユーザ識別子Ａとトークン番号ＴＩＤＡとユーザー端末１Ａに記録された秘密鍵１０１Ａを用いてブロックチェーンのノードの一つである端末３Ａにアクセスし、端末３Ａにデプロイされ たＯＴＰ生成コントラクト３００８Ａまたは３００８ＡＧのＯＴＰ生成関数（図３ＡＣの３００９Ａ）を実行する。
トークン番号ＴＩＤＡが秘密鍵１０１Ａから計算されるユーザー識別子Ａと対応づけられ

ていてＴＩＤＡの所有者がＯＴＰ生成関数３００９Ａの実行者である場合にＯＴＰ計算して生成し端末１ＡにＯＴＰを戻り値として返す。Ｓ２１８では端末３ＡのＯＴＰ生成コントラクト３００８Ａや３００８ＡＧに従って生成されたＯＴＰをＯＴＰ関数３００９Ａの戻り値としてユーザー端末１Ａが取得する。
３００９Ａの動作するフローチャートは図６Ａまたは図６Ｂ示すとおりであり、図６Ｂに示すようにＯＴＰ生成関数３００９Ａを実行した際にその実行回数を記録する変数ＯＴＰＣＴ（図３ＡＣの３０１７Ａ）またはＯＴＰＣＴＧ（図３ＡＢの３０１７ＡＧ）を増加または減少させることでブロックチェーンのコントラクト上の変数を変えることができ、ブロックチェーン上でＯＴＰを生成する計算を実行した回数が改ざんされずに記録される。
なおかつその変数３０１７Ａまたは３０１７ＡＧの変数変化をサーバ端末３Ｃの３１１４Ｃが検出し、不正利用があったことを通知するＯＴＰトークンとは別のノンファンジブルトークン（不正通知トークンを）をユーザー識別子に対し送信することや、顧客情報データベース３０１６Ｃに記載のユーザー識別子に対応する電子メールアドレスや携帯番号などの連絡先に対し不正アクセスの通知することができる。
ＯＴＰトークンの真のユーザー端末であっても不正に秘密鍵を入手したユーザー端末であってもＯＴＰを生成する際に３０１７Ａや３０１７ＡＧの数値の増加減少などの変化が発生し、サーバ端末３Ｃはそれを検出してユーザーに通知できるほか、３０１７Ａや３０１７ＡＧがパブリック変数である場合にはブロックチェーンにアクセスするすべての人がその数値変化を調べることができる。不正アクセスをするユーザーにとってはＯＴＰ認証を行うためのＯＴＰを生成する段階で改ざん困難なブロックチェーン上にＯＴＰの生成回数が記録されるため、不正アクセスの証拠を残さずに本発明の認証システムを通り抜けることは困難である。

【０３６５】

ここでＳ２１６及びＳ２１７においてユーザー端末がウェブブラウザの拡張機能等に秘密鍵を記録している、あるいは秘密鍵を管理しているほかのウェブサイトなどと連携している場合にはその秘密鍵情報を利用してＯＴＰ生成関数３００９Ａと認証関数３０１８Ａをユーザー端末１Ａに実行させる。この時、端末１Ａには秘密鍵を搭載したウェブブラウザ拡張機能等と端末１Ａに発行されたトークン番号ＴＩＤＡの情報が必要である。
端末１Ａからサーバ端末３Ｃへアクセスするために用いたトークン番号と、ユーザ識別子と、端末１ＡのＩＰアドレスや位置情報やセンサ情報などのＩＰＶ情報と、ログイン時刻やログイン回数やログイン状態については端末３Ｃの記憶部３０Ｃのアクセス検出及び監視用データベース３０１１Ｃに図６Ｘのようなデータが記録される。
また秘密鍵を記入し記録しブロックチェーンにアクセスしＯＴＰを表示させるソフトウェアを端末１Ａの記憶装置１０Ａの１０２Ａに搭載している場合は秘密鍵情報をログイントークン番号ＴＩＤＡの記入が必要である。（さらにコントラクト識別子やブロックチェーン識別子の記入も必要である。）

【０３６６】

シーケンスＳ２１９においてサーバ３Ｃは端末１Ａに対し、ＯＴＰトークンのトークン番号とユーザー識別子とＯＴＰの入力を求め、その際にサーバ３Ｃにログインに用いたトークン番号、ユーザ識別子、ＩＰアドレスや位置情報やセンサ情報などのＩＰＶ情報とログイン時刻、ログイン回数、ログイン状態を記録するとともに、端末３Ｃから端末１ＡへＯＴＰの認証を行わせるウェブページを配信するとともに、そのユーザー端末１Ａのアクセスを不正なアクセスか否かを監視する。ウェブページ上でＯＴＰを認証する際にユーザーのユーザ識別子やトークン番号等の入力値と、ユーザー端末のＩＰアドレスや位置情報や端末のセンサ値などを含むＩＰＶ値と、ログイン時刻やログイン回数やログイン状態について図６Ｘのように記録する。
この場合も通常利用で、同一時刻に１人の個人が1つの秘密鍵を１つの端末からサーバ端末３Ｃへアクセスする場合は、図６Ｘに記載の異なるＩＰＶ値は記録されないはずである。

【０３６７】

シーケンスＳ２２０及びＳ２２１ではＳ２１９で配信されたウェブページのＥＣＭＡＳｃｒｉｐｔ等プログラムに応じて、ユーザ識別子Ａとトークン番号ＴＩＤＡとユーザー端末１Ａに記録された秘密鍵１０１Ａを用いてブロックチェーンのノードの一つである３Ａにアクセスし、３Ａにデプロイされ
たＯＴＰ生成コントラクト３００８Ａまたは３００８ＡＡのＯＴＰ認証関数（図３ＡＣの３０１８Ａ）を実行する。
ＯＴＰ認証関数３０１８Ａはユーザー識別子Ａ、トークン番号ＴＩＤＡ、ＯＴＰを引数として、引数ＯＴＰをＡｒｇＯＴＰとして利用し、認証関数内で認証コントラクトに記録されたＫＣ値やＢＣ値と最新のブロック番号と引数で渡された値であるユーザ識別子Ａとトークン番号ＴＩＤＡを基にしてデータを作成しそのデータをハッシュ関数ｆｈでハッシュ化してＶｅｒｉＯＴＰを算出する。ＶｅｒｉＯＴＰとＡｒｇＯＴＰが一致するか検証し、一致する場合には認証ができたと判断し、認証ができたときの処理を行い認証結果を端末１Ａに戻り値ＣＴＡＵ（図３ＡＢの３０２１Ａ）として返し、一致しない場合は認証ができなかった場合の処理を行う（前記処理は図６Ｃ又は図６Ｄ又は図６Ｅ又は図６Ｆ又は図６Ｇ又は図６Ｈのフローチャート説明図に従って認証関数３０１８Ａは動作する）。

図６Ｃまたは図６Ｄに示すようにＯＴＰ認証関数３０１８Ａを実行した際に、３０１８Ａの処理内部にその実行回数を記録する変数ＯＴＰＣＴ（図３ＡＣの３０１７Ａ）またはＯＴＰＣＴＡ（図３ＡＢの３０１７ＡＡ）を増加または減少させ、ブロックチェーン上でＯＴＰを生成する計算を行った回数が改ざんされずに記録する処理を備えていてもよい。なおかつその変数３０１７Ａまたは３０１７ＡＡの変数の変化をサーバ端末３Ｃの３１１４Ｃが検出し、不正利用があったことを通知するＯＴＰトークンとは別のノンファンジブルトークン（不正通知トークンを）をユーザー識別子に対し送信することや、顧客情報データベース３０１６Ｃに記載のユーザー識別子に対応する電子メールアドレスや携帯番号などの連絡先に対し不正アクセスの通知することができる。

ＯＴＰ生成関数の場合と同じく、ＯＴＰ認証関数の場合においても、ＯＴＰトークンの真のユーザー端末と不正に秘密鍵を入手したユーザー端末の区別を問わず、ＯＴＰを生成する際に３０１７Ａや３０１７ＡＧの数値の増加減少などの変化が発生し、サーバー端末３Ｃはそれを検出してユーザーに通知できるほか、３０１７Ａや３０１７ＡＧがパブリック変数である場合にはブロックチェーンにアクセスするすべての人がその数値変化を調べることができる。不正アクセスをするユーザーにとってはＯＴＰ認証を行うときに改ざん困難なブロックチェーン上にＯＴＰの生成回数が記録されるため、不正アクセスの証拠を残さずに本発明の認証システムを通り抜けることは困難である。（またＢｎＴＯＴＰ生成回数が変わらずＢｎＴＯＴＰを生成し取得していないにもかかわらずＯＴＰ認証回数が変化し認証関数が実行された場合は不正利用が考えられるのでサービス提供者はその対抗策を講じることができ、ユーザーもＯＴＰ生成関数が未利用であることを主張し不正利用を受けたことを主張できる。）

【０３６８】

シークエンスＳ２２２では３０２１Ａ、３０２２Ａ、３０２３Ａのように認証後の１つまたは複数の戻り値ＣＴＡＵを定義し、認証後の処理内容、処理内容が操作するトークン番号に対応したデータベース（例として銀行口座残高や、口座残高を別の関数に送金する等といった処理）を実行できる。３０２２Ａや３０２３Ａはブロックチェーン上において顧客の口座残高やポイント、会員サイトでの投票結果などの価値のある変数を改ざんされないように記録するために設定できるものである。３０２２Ａ、３０２３Ａを設定しなくとも既存の銀行のインターネットバンキングと同様に銀行などのサーバ端末３Ｃの内部（サービス提供者の内部ネットワーク）で顧客の銀行口座情報を管理することもできるため、サービスを提供する個別のケースによっては３０２２Ａや３０２３Ａは利用されないことも考えられる。

【０３６９】

シークエンスＳ２２３では認証関数３０１８Ａの認証結果ＣＴＡＵ（３０２１Ａ）を端末１Ａが取得する。

【０３７０】

シークエンスＳ２２４では端末１Ａが取得したＣＴＡＵが認証結果が正しい時の値であるかどうか検証し、正しければログイン後のウェブサイト情報を配信しサービスを提供する。
シーケンスＳ２１５からＳ２２４までの処理は、トークン番号と秘密鍵がありユーザーの秘密鍵を漏洩しないよう配慮したウェブブラウザ環境であれば、トークン番号を入力するだけで（ＯＴＰの生成と認証をＥＣＭＡＳｃｒｉｐｔ等によるプログラムで自動的に行い、ＯＴＰの手動入力を省いて）ログインできる。ただしプログラム上は自動でログイン出来る場合であっても、シーケンス２１８で端末１Ａが入手したＯＴＰを１Ａのディスプレイ１５０Ａに表示させ、そのＯＴＰを手動で入力するなどしてユーザーとしてヒトが実在するかどうか確認するというシークエンスでもよい。

【０３７１】
シークエンスＳ２２５ではＳ２１５やＳ２１９と同じく端末３Ｃのログイン後のサービスにアクセスするユーザー端末１Ａのユーザ識別子、トークン番号、ＩＰアドレスや位置情報や端末のセンサ値などＩＰＶを含むアクセス情報を不正アクセス検出制御部３１１２Ｃにて監視し、図６Ｘにある不正アクセスがあった場合にはそのユーザー識別子に不正アクセス通知トークンをブロックチェーン上で送付するか、あらかじめ登録された連絡先に電子メール等で不正利用の疑いがあることを連絡する。
シークエンスＳ２２６ではユーザのアクセスに応じてサービスを提供する。例えばネットバンキングでは口座残高の確認や口座の取引履歴（ウェブ通帳の表示）等の処理を行う。そして振り込みなどパスワード認証やＯＴＰ認証が必要な処理ではＳ２１４のパスワード入力やＳ２１５からＳ２２４までのＯＴＰ認証を行いサービスを提供する。シークエンスＳ２２７はシークエンス２２５と同じ処理である。
ユーザーがログアウトを実行したり、一定時間端末１Ａから端末３Ｃへのアクセスが無い時は自動的にログアウトさせる。

【０３７２】
サーバ３Ｃは端末１Ａのアクセス時にＩＰアドレスなどの値を記録できる。本発明では銀行取引等金融分野などの重要な取引を扱う必要があるサービスにおいては個人情報の保護をしつつ、ユーザーが通常アクセスする端末の情報やＩＰアドレス、位置情報をユーザーの同意を得て収集し（またはＩＰアドレス等のハッシュ値や匿名化した値を求め収集し）、図６Ｘにあるデータの表に銀行口座番号や名義と電話番号または電子メールアドレスなどの連絡先情報を追記したデータベースを３Ｃの記録部に記録してもよい。そして端末１Ａのアクセス履歴に対し、ある時端末１Ａの秘密鍵１０１Ａを用いて異なるＩＰアドレス等の環境からアクセスを受けたとき、顧客に電話または電子メールで通常とは異なる環境から秘密鍵１０１に由来するユーザー識別子Ａにてアクセスがあったことを通知してもよい。

【実施例２】
【０３７３】
図８Ｂは本発明のワンタイムパスワード認証システム（ＯＴＰ認証システム）において有価紙葉の表示画面１５００Ａや紙のチケット等有価紙葉１８ＡやＮＦＣタグ１９Ａを用いて入場や改札、施錠された建物・乗物・設備・容器を解錠する際の基本的な認証システム図である。図８Ｂは実施例２（実施形態２）を説明する資料である。
実施例１と実施例２（実施形態２）の基本的な動作は類似している。チケットによる入場処理を行う場合は３Ｃと同様の機能を併せ持つ端末３Ｄでもよい（ウェブサイトにログインして入場する際に利用する端末は３Ｃであり、現実の入場口に入場する際に利用する端末は３Ｄである。３Ｄは入場口や改札などで入場処理を行うことを意図しているが端末３Ｄを入場口の改札機などに用いるほかに施錠された建物・乗物・設備・容器を解錠する用途にも応用できる。）
実施例２ではブロック番号Ｂｎ等ブロックチェーンの時刻情報を利用せずコントラクト管理者が任意時間に変数ＫＣ（図３ＡＣの３０１１Ａ）またはＢＣ（図３ＡＣの３０１３Ａ）の数値を変更できる余地を持たせたパスワードＯＷＰを用いる。実施例で利用するＯ

ＷＰはＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）であり、前記関数ｆｈの引数には時刻によって変化するブロック番号Ｂｎといった変数を持たない。ただしＯＷＰはコントラクト管理者がある時刻にセッター関数ｆｓｃｂを用いてＢＣやＫＣを変更させた場合に変化することがある。

【０３７４】

図８Ｂにおいてユーザ端末１Ａ（図２Ａの１Ａ）とサーバ端末３Ａ（図３Ａの３Ａ）とコントラクト管理者端末１Ｃ（図２Ｃの１Ｃ）と入場口・改札又は施錠された建物・乗物・設備・容器に備え付けられた施錠の制御と本発明のＯＴＰ認証システムによる認証を行うことの出来る端末３Ｄ（図３Ｄの端末３Ｄ）とチケットなど有価紙葉をＯＴＰトークンとしてを発券するサーバ端末３Ｅがネットワーク２０を通じて接続されている。

【０３７５】

端末３Ｄはネットワークに接続されていてもよいし、接続されていなくてもよい。ここで端末３Ｄの記憶装置３０Ｄのブロックチェーン記録部３００Ｄまたは３０１０Ａには、端末３ＡのＯＴＰ生成コントラクトが生成するＯＷＰ型ＯＴＰを認証できる認証関数３０１８Ａ、３０１８ＤＡが記録されていてもよい。認証関数３０１８Ａ、３０１８ＤＡに用いるＫＣ値３０１１ＡやＢＣ値３０１３Ａや３０３０Ａや３０３１ＡといったＯＴＰ計算に必要な変数情報を端末３Ｄに記録していてもよい。

端末３Ｄはネットワーク２０には接続されていないがサーバ端末３ＡのＯＴＰ生成トークンに関するコントラクト３００８Ａまたは３００８ＡＧにて生成されたＯＴＰ（ＯＷＰ型ＯＴＰ、ＯＷＰ）を認証できる認証関数を３Ｄの記憶部３０Ｄの３００Ｄや３０１０Ｄに備え、ブロックチェーン部を持つ３Ａとネットワーク２０を通じて接続されていないオフライン状態であってもＯＷＰなどの認証情報を記録した紙のチケット等有価紙葉やＮＦＣタグを用いて認証を行い、入場や改札、施錠された建物・乗物・設備・容器を解錠出来てもよい。

特に自動車や建物、あるいは金庫等の容器は常にインターネットワークに接続できるオンライン状態であるとは限らず、災害時にはオフラインとなりブロックチェーンへアクセスできるネットワークに接続できない恐れがあり、ネットワーク２０等から端末３Ｄが切断された状態においても認証できることが求められうる。

そこで本発明ではＯＴＰトークンの発行・流通・ＯＷＰ型ＯＴＰの生成はオンラインにおいて端末１Ａと端末３Ａと端末３Ｅと端末１Ｃがネットワーク２０を介してブロックチェーン部にてトークンの発行を行い端末１Ａと端末３Ａ間でＯＷＰ型の生成を行い、生成されたＯＷＰとＯＷＰ生成に用いたトークン番号とユーザ識別子を端末１Ａのプリンタ１５２Ａにて紙に印刷・印字し印刷物１８Ａ（図２Ａまたは図８Ｂの１８Ａ）を製造し端末３Ｄのカメラ３４０Ｄに１８Ａや１５００Ａのイメージ情報を読み取らせて認証させる。また、通信装置１２ＡとＮＦＣタグ１９Ａ（図２Ａまたは図８Ｂの１９Ａ）を通信させＮＦＣタグ１９ＡにＯＷＰとＯＷＰ生成に用いたトークン番号とユーザ識別子を記録させ、前記ＮＦＣタグ１９Ａを電子的な入場券や解錠を行う鍵として端末３Ｄと通信させ認証を行い入場または解錠などを行う。

ここでタグ１９Ａは主に非接触式のＮＦＣタグを想定するが接触式のＩＣタグやＩＣカード、通信端子を備えた外部記録端末１９Ａでもよく、磁気ストライプを用いた１９Ａでもよく、１９Ａは非接触式または接触式の通信を端末３Ｄと行うことができる。

なお端末３Ｄがネットワークに接続されている場合は、３Ｄに記録された認証関数３０１８ＤＡに限らず、端末３Ａに存在するブロックチェーン部の認証関数３０１８Ａにアクセスし紙のチケットやＮＦＣタグに記録されたＯＷＰを含む認証情報をもちいて認証を行い、入場口や改札での入場処理や建物・乗物および設備や装置・電子計算機端末・保管庫・金庫など容器の施錠の解錠も可能である。

【０３７６】

＜紙のチケット等有価紙葉１８ＡまたはＮＦＣタグ１９Ａの製造と利用＞

オフライン状態にある端末３Ｄのカメラ３４０Ｄにて紙の有価紙葉１８Ａの印刷面のＯＷＰとＯＷＰ生成に用いたトークン番号とユーザ識別子情報を読取り、あるいは３ＤのＮ

ＦＣ通信装置３４１ＤにてＮＦＣタグ１９Ａ内部に記録されたＯＷＰとＯＷＰ生成に用いたトークン番号とユーザ識別子情報を読み取り、３Ｄの記録部３０Ｄの３００Ｄや３０１０Ｄに記録された認証関数３０１８ＤＡまたは３０１８Ａと同様の処理（図６Ｆのフローチャートも参照）に従って紙やＮＦＣタグのＯＷＰ型ＯＴＰをＡｒｇＯＴＰとして、ＶｅｒｉＯＴＰとＡｒｇＯＴＰが等しいか検証して一致すれば、開閉・ゲート・施錠・始動装置３５０Ａを操作して入場口や改札であれば入場を行い施錠装置であれば解錠を行い始動装置であれば始動を行う。同時に３５１Ｄと３５２Ｄを認証できた場合と認証できない場合に対応した動作を行わせてもよい。
端末３Ｄのカメラ３４０Ｄに対し紙の情報１８Ａの代わりに端末１Ａのディスプレイ１５０ＡのＯＷＰ等認証情報表示画面１５００Ａを提示し読み取ることで認証してもよい。

【０３７７】
＜プリンタによる１８Ａの製造＞
紙のチケット等の有価紙葉１８Ａを製造するプリンタは文字情報やバーコード情報を紙やプラスチックフィルム、板材など印刷できればよい。インクジェットプリンタ、レーザープリンタ（電子写真方式）、サーマルプリンタ（感熱紙）の利用が考えられる。ほかにチケットが紙でなく板や立体でもよい時はプロッターやプロッターに切削装置などを取りつけ母材に情報を切削・刻印できる2次元の加工機や、3次元の加工機、そして３Ｄプリンタなども利用できてもよい。ここでプリンタは認証先となる端末３Ｄのカメラやスキャナ３４０Ｄに文字列または1次元及び2次元のバーコード情報を読み込ませる事ができる加工を母材に施せる装置である。インクジェットプリンタやレーザープリンタ、プロッタを用いてエッチング用・パターニング用のパターンを作り、母材に対しパターンを基に加工する処理（サンドブラスト、エッチング、昇華転写など）も利用できる。
紙やフィルム材に限らず金属板、陶磁器、布など繊維製品にもＯＷＰ等の認証情報を印刷・パターニング・捺染・転写し有価紙葉１８Ａを製造できる。
インクはインクジェットプリンタでは目視で判読できる水性の顔料インク、染料インクが使えるほか、必要に応じてセキュリティ用の不可視インクや溶剤インクと溶剤インク用のフィルム材、紫外線硬化インクとそのインクに対応したフィルム材を利用できる。金券やチケット分野でチケット販売者がユーザーの代理で印刷などをしてユーザー住所に送付する場合には特殊なインクを用いてチケットに付加価値をつけることも想定される。またユーザーがインクジェットプリンタを保有し端末１Ａに接続して印刷できる場合はカラー印刷である場合にチケットの絵柄などを表現することが容易になる。チケットを印刷する際に多色で絵柄が印刷されることでどのような種類のチケットか判別しやすくなると思われる。（例として紙幣や金券は色が付けられ券種に応じて色や絵柄がありヒトの目で券種が判別しやすい事が挙げられる）
実施例２では１８Ａの製造に水性の染料インクを用いる家庭用インクジェットプリンタもしくはトナーを用いるレーザープリンタを用いた。トナーとレーザープリンタを用いた理由は印刷物の対候性が高いことと印刷速度が高く、また事業所やＣＶＳなどで広く流通しておりレーザープリンタは白と黒の色表現ができるためである。
サーマルプリンタと感熱紙は現金自動預け払い機ＡＴＭやＣＶＳや商店の店舗のレジスター等業務用機器に内蔵され広く流通している。本発明ではこれらのサーマルプリンタにおいても感熱紙にＯＷＰを含む認証に必要な情報を文字列または1次元及び2次元のバーコード情報として印刷しチケットなど有価紙葉とすることができる。ただしトナーによるものより印刷面・印字面の耐久性が低い傾向にあり、短期間のみ有効な期限付きのチケットや商品券に利用されうる。

【０３７８】
＜ＮＦＣタグ１９Ａの製造＞
ＮＦＣタグ１９Ａを用いる場合は端末１Ａの通信装置１２Ａと１９Ａが通信できれば良い。ＮＦＣタグでもよいしＮＦＣカードでもよい。１９ＡはＮＦＣタグの形状や形態と同等の機能を持つ形状の装置であればよい。ＮＦＣタグ１９Ａの機能を備えさせた眼鏡・ヘッドマウントディスプレイまたは補聴器・イヤホン・ヘッドホンまたは衣服または腕輪・

腕時計・腕時計型端末または指輪またはベルト・ベルト型端末または靴・靴の部品・靴型端末といった製品に組み込まれたＮＦＣタグ１９ＡもしくはＮＦＣタグ１９Ａの機能付きのウエアラブルコンピュータ端末であってもよい。
さらにスマートフォンなどの携帯電話機型端末や財布やキーホルダーなどの金銭の決済や金属鍵の管理に用いられてきた既知の製品にＮＦＣタグを内蔵してもよい。ＮＦＣタグ１９Ａは製品に組み込まれていても貼り付け等されていてもよい。
また端末１ＡがＮＦＣ機能をもち端末１Ａそのものが持ち運びの出来るＮＦＣタグ１９Ａとなっていてもよい。その場合、端末１Ａの通信装置１２Ａ（端末の電子回路を含む）にてＮＦＣタグ部分１９Ａと制御装置１１Ａや記憶装置１０Ａが有線方式で接続される。タグ１９Ａには有線通信用の接点や端子が備え付けられていてもよい。１９Ａに備えられた接点又は端子を用いて端末３Ｄに認証情報を読み込ませ３Ｄが制御する施錠装置や入場用の開閉装置等を動作させてもよい。
ＩＣを用いる１９Ａも１６Ａも端末１Ａと同じくコンピュータの五大装置として制御演算装置と記憶装置と入力装置・出力装置を備えるカードもしくはタグ型の小型電子計算機端末であり、電源装置や通信装置も備える。電源装置はワイヤレス給電システムや一次電池、二次電池、電池を利用する回路、電池を充電するシステムを含みうる。
【０３７９】
実施例２におけるＯＴＰの生成関数のフローチャートは図６Ａと図６Ｂに記載し、ＯＴＰの認証フローチャートは図６Ｄと図６Ｆに記載する。図６Ｄ及び図６Ｆでは引数となるユーザー識別子ＡとトークンＩＤＡとＯＷＰが紙に印刷された情報またはＮＦＣタグの記憶装置から送信された情報として入力されると、認証関数３０１８Ａ（もしくは３０１８ＤＡ）は入力された引数の情報に従い、認証関数３０１８Ａの属するコントラクト３００８ＡＡの内部シークレット変数ＫＣやＢＣと、引数として入力されたユーザ識別子ＡとトークンＩＤＡとＯＷＰ（ＯＷＰ＝ＡｒｇＯＴＰとして）から、検証用ＯＴＰであるＶｅｒｉＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）を計算し、ＶｅｒｉＯＴＰがＡｒｇＯＴＰと一致するか（つまりＶｅｒｉＯＴＰ＝ＡｒｇＯＴＰとなるか、ＶｅｒｉＯＴＰ＝ＯＷＰとなるか）を判定し、一致した場合には認証が正しい処理を行い、一致しない場合には認証できないときの処理を行う。認証関数は端末３Ｄに記録された認証関数３０１８ＤＡを用いることもできる。
【０３８０】
図７Ｅは図８Ｂに記載の装置とＯＴＰ認証システムを用いて端末３Ｄに対し認証を行う際のシーケンスの説明図である。図７Ｅでは例としてチケット及び会員権や自動車等の鍵または容器の鍵の用途を想定している。チケットや会員権は有効期限があり期限切れがある事、また自動車の鍵分野では車検などで定期的に施錠した物体がインターネットワーク等に接続され保守メンテナンスできることを想定する。
図７Ｅは図７Ｂと類似する。
図７ＢはパスワードＯＷＰを用いたＯＴＰトークンの一般的な発行時のシークエンス図でありＳ１３０からＳ１３５までの一連の流れでＯＴＰトークンをサービスに登録し、ブロックチェーン（または分散型台帳システムＤＬＳ）のノード端末３ＡのにＫＣ値をｋ１、ＢＣ値をｃ１としてＯＴＰ生成関数を含むＯＴＰトークンのコントラクト（生成コントラクト、ＯＴＰ生成コントラクト）のバイトコード等を含むトランザクションを送信しデプロイしＯＷＰによる認証をできるように準備した後にユーザー端末１Ａの秘密鍵１０１Ａのユーザー識別子Ａにトークン番号ＴＩＤＡのトークンを発行する。また同時にサービスを提供する端末３Ｄや３ＣにＯＴＰ認証関数３０１８ＤＡや３０１９ＡＡや３０１８ＡにＫＣ値をｋ１、ＢＣ値をｃ１としてＯＴＰ認証関数を設定しなければいけない。この時点では端末１ＡのユーザーはＯＷＰ＝ｆｈ（Ａ,ＴＩＤＡ,ｋ１,ｃ１）のパスワードＯＷＰを生成して取得し認証に用いることができる。
Ｓ１４４においてある時間が経過した後、Ｓ１４５にてＯＴＰトークンのＯＴＰ生成関数を含むコントラクトと認証関数３０１８ＤＡのＫＣ値をｋ２、ＢＣ値をｃ２へ書き換えることでユーザーのＯＴＰトークンの生成するＯＴＰを変えることができる。

端末１Ａのユーザーはブロックチェーンにアクセスするソフトウェアを用いてＯＷＰ生成ソフトウェアまたは専用のウェブサイトを用い、Ｓ１３７からＳ１３９までの一連の流れで端末３Ａのブロックチェーン部のＯＷＰ型のＯＴＰトークンのコントラクトからＯＴＰ生成関数を呼び出してＯＷＰ型のＯＴＰを取得する。その際のＯＷＰはＯＷＰ＝ｆｈ（Ａ,ＴＩＤＡ,ｋ２,ｃ２）で計算される。
端末３Ｃや端末３Ｄがネットワーク２０を介して３Ａと接続されているときＳ１４１からＳ１４３にてＯＴＰ認証関数３０１８Ａを呼び出し、もしくはＳ１４１からＳ１４３と同様の工程を３Ａではなく３ＤのＯＴＰ認証関数３０１８ＤＡを呼び出し行って認証結果の戻り値ＣＴＡＵを得て、前記認証の戻り値ＣＴＡＵが認証ができたときの値（データ）の時にＳ１４４にて端末３Ｄのサービス提供用内部プログラムに従い開閉装置または施錠装置または始動装置３５０Ｄを操作し開閉装置の場合はゲート装置や改札装置などを開き施錠装置の場合は施錠を解錠し始動装置の場合は原動機や電子計算機を始動させる。
ＯＷＰ生成ソフトウェアまたは専用のウェブサイトではユーザーの秘密鍵の不正利用を監視するためにＳ１３６やＳ１４０のプロセスにて図６Ｘに示すデータ構造の様に不正アクセスの有無を検出しユーザーに通知してもよいし、ＯＷＰを用いたＮＦＣタグ１９Ａを用いて施錠を行う扉や乗物や容器などの装置などで個人情報を守る必要があるとき、もしくは個人情報を収集するサーバ３Ｃ（およびネットワークに接続できる３Ｄ）や３Ｅや３Ｆや５Ａで情報流出する事により顧客が購入した端末３Ｄの設備やその所有者を危険にさらす恐れがあるときはＳ１３６やＳ１４０といった利用者からアクセス情報を収集する機能を利用しなくともよい。

Ｓ１４６ではＳ１４４と同じくある任意の時間経過したのちＳ１４５と同様に、端末１ＣがＯＴＰ生成側の３ＡとＯＴＰ認証及びサービス側の３Ｄや３ＣにてＫＣ値とＢＣ値を更新し一致させＯＴＰ計算ができるように設定することができる。ＫＣ値をｋ３、ＢＣ値をｃ３に書き換えることができ、その後も同様に任意の時間ごとにＫＣ値ＢＣ値を書き換えることができる。利用形態として自動車の鍵をＮＦＣタグ１９Ａで実現する場合には車検ごとに自動車の鍵となるＯＷＰを書き換え偽造されたＮＦＣタグ１９がある場合もそれを過去のもの（無効な物と）とできる。また有効期限のある利用券やチケット１８Ａを有効期限後に強制的に認証できないようにさせる事ができる。

【０３８１】
実施例２のＯＷＰはＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）として算出され、Ａ，ＴＩＤＡ，ＯＷＰの３つを記録させたＮＦＣタグ１９Ａ（およびＡ，ＴＩＤＡ，ＯＷＰの３つを印刷した有価紙葉１８Ａ）はＫＣ値やＢＣ値が変更されない限り認証を行うことができる。コントラクト３００８Ａおよび３００８ＡＧの生成関数と３Ｄに認証関数に対し同一のＫＣ値、ＢＣ値を設定した後にＫＣ値、ＢＣ値を変更しないサービスの運用も可能である。

【０３８２】
しかし長時間（ここでは数年、数十年）ＫＣ値ＢＣ値を変更しない場合、ＮＦＣタグ中のＡ、ＴＩＤＡ、ＯＷＰの3つの情報が漏洩しＯＷＰ情報を複製し不正に自動車の鍵を開錠し自動車を始動させる恐れがある。そこで自動車の鍵として数カ月単位、数年単位で定期的にＯＷＰを更新したいときがあるかもしれない。その場合にはＯＷＰを生成するＯＴＰトークンのコントラクトの管理者が数カ月、数年ごとにＫＣ値とＢＣ値をセッター関数ｆｓｃｂで書き換えることでＯＴＰトークンのシークレット変数を書き換え、ＯＷＰを任意の時間間隔で変更できる。更新された取得したＯＷＰは更新前の複製されていたかもしれないＯＷＰとは異なる。

ここではＮＦＣタグについて述べているが、紙のチケットなどでもＯＷＰが更新され、ＯＷＰの更新前に印刷した紙のチケットは無効となる。ＫＣ値ＢＣ値の更新を行うことで過去に製造された紙のチケットやＮＦＣのデータ値を無効にすることができる。無効になった紙のチケットなどに対しどう対応するかはサービス提供者に委ねられる。ＫＣ値やＢＣ値の変更の履歴を知るサービス提供者は紙のチケットがかつて存在したかどうか検証しその紙のチケット１８Ａを持つものに対して対応することができるかもしれない。１８Ａ

には好ましくはＡ、ＴＩＤＡ、ＯＷＰのほかに印刷時のブロック番号Ｂｎや印刷時刻、サービス提供者の名称と連絡先、ＯＴＰトークンのコントラクト識別子を判読できる文字列の状態で記録することが好ましい。

【０３８３】

自動車は自動車検査時（車検時）に定期的にメンテナンスされるため、その際に自動車に内蔵された自動車の施錠や始動を制御する端末３Ｄをインターネットに接続させ認証関数のシード値を同期させることもでき、端末３Ｄに備えられた認証関数３０１８ＤＡと対応したＯＷＰ、ＴＩＤＡ、Ａを再度ＮＦＣタグ１９Ａに記録させる必要がある。自動車のＯＴＰトークンの管理者は年末など自動車検査が行われていない休日を狙いＫＣとＢＣを変えるトランザクションを端末３Ａを含むブロックチェーンシステムに送信することで、コントラクトに属するすべての自動車のＮＦＣタグのＯＷＰ情報を変更でき、年末の休日が終わった後からは新しい年のＫＣ，ＢＣ値を基に自動車の検査を行い自動車内部の端末３Ｄや顧客のＮＦＣタグの鍵を最新のＯＷＰを用いるように更新できる。

【０３８４】

自動車の鍵でなく建物や容器に搭載された端末３Ｄの場合は通信用端子や無線通信装置を備えておらずＫＣやＢＣの更新ができない恐れがあるので、３Ｄが通信手段を持たないときはコントラクトの管理者はＫＣ値ＢＣ値の変更を行わない。ただし、建物や容器に搭載された端末３Ｄが通信装置を持ちＫＣ値やＢＣ値を更新できる場合にはコントラクト管理者はＫＣ値とＢＣ値の変更を行うことができる。

端末３ＤのＫＣ値とＢＣ値を更新するには３Ｄの所有者が更新作業を行うか、３Ｄの製造者が更新作業を行うことになりヒトの手が必要になる。施錠を解錠した時に見える部分（施錠された扉の裏側に位置する施錠を解錠するレバーやスイッチおよび金庫においては施錠する端末３Ｄや施錠装置が取りつけられた面または庫内の面）に有線式の通信用端子を備えさせ、更新用のプログラムを通じてＫＣ値やＢＣ値を更新できると好ましい。
無線により３Ｄにアクセスできるようにすることもできるがその場合は端末３Ｄへのアクセス権が必要となる。ＯＴＰトークンを保有しているユーザー識別子Ａの端末１Ａに搭載された何らかのパスワードや秘密鍵を用いてアクセスすることが考えられる。

端末３Ａを含む施錠装置の形状および形態については金庫の施錠装置のほか、南京錠型の端末３Ｄやワイヤーロック型もしくはベルト型の端末３Ｄも考えられる。自転車等の施錠にはワイヤーロック型や自転車専用の鍵となる端末３Ｄも考えられる。

【０３８５】

入場口や改札などサービスを行う施設に設置された端末３Ｄの場合はインターネットワークまたはローカルエリアネットワークＬＡＮへの接続が容易である。有線または無線を用い入場口や改札でチケットの認証に用いる端末３Ｄの認証関数３０１８ＤＡに用いるＫＣ値ＢＣ値を遠隔地の端末１Ｃから更新できる。また３Ｄをネットワーク２０を通じてブロックチェーンのノードとなる端末３Ａに接続し３Ａのブロックチェーン部に記録された認証関数３０１８Ａを用いて認証してもよい。

【０３８６】

図７Ｅは図８Ｂ記載の装置とＯＴＰ認証システムを用いて端末３Ｄに対し認証を行う際のシーケンスの説明図について説明する。実施例２を説明する図７Ｅと実施例１を説明する図７Ｄには類似する箇所がある。シークエンスＳ２３０，Ｓ２３１は実施例１と同様である。Ｓ２３０ではＯＴＰを計算する際にｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）といった、ブロック番号Ｂｎを用いず代わりにコントラクト管理者が変更できる変数ＫＣや変数ＢＣを書き換えられるようにする。実施例２ではコントラクト管理者が変更できるシークレット変数ＢＣやＫＣを採用したパスワードＯＷＰについてＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）として計算する。ここでＡはユーザ識別子Ａであり、ＴＩＤＡはトークン番号ＴＩＤＡである。

【０３８７】

Ｓ２３２ではコントラクト識別子をチケットなど有価紙葉の発券に利用するサーバ端末３Ｅとサーバ端末３Ｄに登録または設定する。３Ｄがネットワーク２０と接続されずに利

用される場合は３Ｄの記録部３０Ｄのブロックチェーン部３００Ｄや基礎プログラム部３０１０Ｄに認証関数３０１８Ａや３０１８Ａを含む認証コントラクト３００８ＡＡを記憶させ、制御部３１Ｄで認証関数３０１８Ａが実行出来るようにする。

【０３８８】

端末１Ａと端末３Ｅがあるサービスに対応したトークンの発行を契約した事を確認し、端末３Ｅが管理者端末１Ｃにトークンの発行を依頼する。シークエンスＳ２３３では１Ｃは１Ａのユーザー識別子Ａに対しトークン番号ＴＩＤＡのトークンを発行する。

【０３８９】

＜有価紙葉の製造＞

ＳＳ２３４からＳ２４０までの一連のシークエンスでは、端末１Ａに発行されたトークン番号ＴＩＤＡと端末１Ａに記録された秘密鍵１０１Ａを基に、発券サイト３Ｅもしくは端末１Ａの記憶装置に記録された発券ソフトウェアを用いて１Ａをブロックチェーンシステムの０ＴＰ生成コントラクト３００８Ａにアクセスさせ、Ｓ２３０にて３００８Ａ設定されたＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）をＯＴＰとして生成させる処理を開始する。

そしてＯＷＰを３Ｅや発券ソフトウェアに記録されたチケットの図柄情報、サービス提供者の連絡先や住所、チケットなど有価紙葉の有効期限など、サービスに応じて必要な情報と共に印刷用のＯＷＰ等認証情報表示画面１５００Ａを１Ａ表示させ、また必要であれば１５００Ａの画面情報を端末１Ａのプリンタ１５２Ａを用いて印刷させ、ＯＷＰとＡとＴＩＤＡを記入した有価紙葉１８Ａを製造させる。

またＯＷＰとＡとＴＩＤＡを記入したＮＦＣタグ１９Ａを製造させる。ＮＦＣタグ１９Ａについても有価紙葉１８Ａと同様に、ＯＷＰとＡとＴＩＤＡとサービス提供者の連絡先や住所、チケットなど有価紙葉の有効期限など、サービスに応じて必要な情報を１９Ａの記録装置に記録させることができる。

【０３９０】

シークエンスＳ２３５では発券サーバ３Ｅにアクセスし１５００Ａや１８Ａに発券を行う際に図６Ｘにあるようなアクセス者の情報を取得し不正アクセスが行われていないか監視できる。ただし必須の機能ではない。

不正アクセスの監視に関してはＳ２４２やＳ２４４にて１５００Ａや１８Ａや１９Ａをサービス提供端末３Ｄに提示した際に図８Ｂの３４２Ｄの防犯カメラ等の入場者を監視するシステムがあると好ましい。（３４２Ｄを備えると好ましいが物理的なあるいは経済的な理由で防犯カメラを備えることに利点が少ない用途、例えば小型金庫や南京錠型の施錠機器などでは監視カメラを搭載しなくともよい。自動車や建物を施錠する用途などでは防犯カメラを搭載することは可能であるが搭乗者のプライバシーを考慮し３４２Ｄを搭載しない場合も本発明では考えられる。）

【０３９１】

シークエンスＳ２３６、Ｓ２３７、Ｓ２３８で端末１Ａは端末３Ａの０ＴＰ生成コントラクトにＯＴＰを生成する関数を呼び出し実行させ取得する。サーバ端末３Ｅのウェブサイトでチケットを発行している場合にはＳ２３９にて有価紙葉の情報１５００Ａを表示し、１５００Ａの印刷を許可し有価紙葉１８Ａを印刷させＮＦＣタグ１９Ａに有価紙葉の情報を記録させる。また１Ａに記録し実行している発券ソフトウェアから発券している場合にはＳ２４０にてソフトウェアを通じて有価紙葉の情報１５００Ａを表示し、１５００Ａの印刷を許可し有価紙葉１８Ａを印刷させＮＦＣタグ１９Ａに有価紙葉の情報を記録させる。

【０３９２】

＜有価紙葉の使用＞

シークエンスＳ２４１では１５００Ａを表示できる端末１Ａもしくは０Ｓ２４０で製造した紙チケット１８Ａ又はＮＦＣタグ１９をサービス提供の場へ持参し提示し改札や入場口または施錠された建物・乗物・容器の端末３Ｄへ提示し入場や解錠を試みる。このとき１５００Ａまたは紙チケット１８Ａを端末３Ｄのカメラ３４０Ｄに読取させる。またＮＦＣ

タグ１９ＡのＯＷＰの認証に必要なを入場口又は施錠設備の端末３Ｄの通信装置３２Ｄを通じて読取させる。

【０３９３】

シークエンスＳ２４２では提示された紙又はディスプレイの表示面印刷面を読み取り、あるいはＮＦＣタグチケットのデータ読み取り、

端末３Ｄがネットワーク２０と接続されていない場合（オフラインの場合）、Ｓ２４２にてサービス部の端末装置３Ｄ内部の３００Ｄや３０１０Ｄに記録された認証関数３０１８ＤＡにてＯＷＰの検証、認証処理を行い認証関数から認証結果の戻り値ＣＴＡＵを得る。

端末３Ｄがネットワーク２０と接続されている場合（オンラインの場合）、Ｓ２４３にてＤＬＳ上の認証関数３０１８Ａにアクセスしで ＯＷＰを認証し認証関数から認証結果の戻り値ＣＴＡＵを得る。Ｓ２４３では認証時に認証回数の増減やチケットを利用済みにする処理を設定できる。

ここで端末３Ｄがオフラインの場合の例として小型の金庫、南京錠型施錠装置、無線通信が困難な環境が想定される自動車や農業機械・林業機械・船舶・重機などの乗物や建物の施錠部分が想定される。オフラインで利用されることが前提の端末３Ｄでは保守点検用に３Ｄの３００Ｄや３０１０Ｄに記録された認証関数３０１８ＤＡに用いる変数ＫＣやＢＣを変更できる通信用の端子や無線通信装置、ＮＦＣ装置を備えていると好ましい。

端末３Ｄがオンラインの場合の例として駅の改札や映画館など商業施設の入場口が挙げられる。ただし災害時にはネットワークが切断される恐れがあるのでオンラインの場合であってもオフラインになっても認証ができるようにした方が好ましく、そのサービスを提供する会社のローカルエリアネットワークを経由しインターネットワーク上の３Ａのブロックチェーン部を複製し同期させつつ、インターネットワークから遮断された場合でも端末３Ｄにブロックチェーン部３００Ｄを構築できていることが好ましい。

【０３９４】

シークエンスＳ２４４では端末３Ｄは認証関数から認証結果の戻り値ＣＴＡＵが正しいか判断し、正しい場合には認証ができたと判断し、入場処理や施錠を解錠するため３５０Ｄを操作する。認証結果の戻り値ＣＴＡＵが正しく無い場合には再度認証を行うまで待機する。Ｓ２４４にて３５０Ｄを操作すると同時に３５１Ｄと３５２Ｄを認証できた場合と認証できない場合に対応した動作を行わせてもよい。

またＳ２４４において入場口や駅の改札の端末３Ｄなどの時に開閉装置３５０Ｄが無く人員によって入場者の制止などを行う場合は３５０Ｄを備えていなくてもよく、３５０Ｄの代わりに人員が音や光で入場させるユーザーを区別する際に役立つよう３５１Ｄと３５２Ｄを認証できた場合と認証できない場合に対応した動作を行わせてもよい。

【０３９５】

シークエンスＳ２４５ではコントラクト管理者端末１Ｃがブロックチェーンのノード端末３Ａにアクセスし、ＯＴＰ生成コントラクトのシークレット変数ＫＣ値やＢＣ値を変更し、さらに端末３Ｄの記憶装置の３００Ｄや３０１０Ｄに記録された認証関数のＫＣ値ＢＣ値を変更することで、ＯＷＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ）のシード値が変更されパスワードＯＷＰが変更される。ネットワークに接続されていない端末３Ｄは端末３Ｄとユーザー端末との間で通信を行うことの出来る端子や無線通信装置、ＮＦＣ装置が必要である。端末３Ｄが金庫や自動車ではその所有者や整備又は保守を行う者がシークレット変数ＫＣ値やＢＣ値を変更する必要がある。

【０３９６】

シークエンスＳ２４５において端末３Ａと端末３ＤのＫＣやＢＣを変更すると、ユーザーが製造したＮＦＣタグや印刷物のチケットなど有価紙葉は認証できなくなり無効にさせることもできる。例えばある期日までに（１１月30日から12月30日まで有効など）使用期限が設定されている商品券では有効期限後にＫＣ値やＢＣ値を変更すると流通していた商品券（紙、ディスプレイ表示情報、ＮＦＣタグ）は認証できなくなり利用できなくさせることもできる。

【０３９７】
シークエンスＳ２３２、Ｓ２３３に関連して端末３Ｄを用いて解錠できるトークン番号をあらかじめ決定し、そのトークン番号を端末３ＤのＲＯＭとなる記憶装置に記録させてもよい。端末３Ｄの認証関数はＡ，ＴＩＤＡ，ＯＷＰをＮＦＣタグより読み取り認証を行うが、自動車や建物・金庫など容器といった異なる製造番号を持ちうる製品に端末３Ｄを設定する際には、製品の製造番号（製品の個体識別番号）に対応したトークン番号を製品の製造時に端末３Ｄに組み込むことができる。
【０３９８】
＜自動車の鍵＞
例として仮にＯＴＰトークンとそのトークンが生成するＯＷＰ型のパスワード等をＮＦＣタグに記録させた自動車の鍵である場合、ある車種に対応するＯＴＰトークンのコントラクト識別子が設定され、その車種の製造番号に対応するトークン番号を記録した端末３Ｄが製造番号に対応する自動車の施錠装置の端末３Ｄや始動制御装置端末３Ｄあるいは自動車のメインコンピュータ端末３Ｄに搭載されうる。
自動車を所有している事はＤＬＳ上に記録され、仮にほかの人（他のユーザー識別子Ｂ）に自動車を譲渡した場合、ＯＷＰを生成する引数がＡからＢに変更され、ユーザー識別子Ｂをもつユーザーはユーザー識別子Ａのユーザーとは異なるＯＷＰを生成しＮＦＣタグに搭載させ利用することができる。ここでユーザーＡは更新前のＡ，ＴＩＤＡ，ＯＷＰを持つＮＦＣタグを持っており自動車を解錠できるユーザーはＡとＢの２人がいる事になってしまう。そこでシークエンスＳ２４５において定期的に３Ａを含むブロックチェーンシステムと自動車の端末３ＤのＫＣ，ＢＣを変更させ更新させる。
また端末３Ｄがユーザー識別子ＡやＢを記録できるようにしてもよい。ユーザー識別子Ａからユーザー識別子Ｂのユーザーに譲渡された時ユーザー識別子Ｂのユーザーはユーザー識別子Ｂを解錠された自動車のドア内部からアクセスできる通信端子を経由して端末３Ｄに書き込んでもよい。前記の例ではユーザー識別子Ｂが内部で端末３Ｄに書き込まれてＯＴＰ認証関数３０１８ＤＡの引数に固定されていれば端末３Ｄは解錠時にユーザー識別子Ｂに由来するＯＷＰのみ認証できる。（この作業は名義の書き換えに似ている。）
自動車の端末３Ｄがインターネットワークに接続できる場合には端末３Ｄとサーバ端末３ＡでのＫＣ，ＢＣの更新と同期は容易であるが、インターネットワーク２０に接続困難な場合は自動車を整備できる工場や自動車の譲渡売買に対応する古物商の元でＫＣ，ＢＣの更新の対応ができうる。また定期的な自動車検査の段階で自動車の端末３Ｄの認証関数とそれを動かすＮＦＣタグ１９Ａを更新することもできる。他に農業機械、重機、船舶などに搭載された端末３Ｄもユーザーの求めに応じて保守点検や譲渡時にＫＣをＢＣを書換えてＮＦＣタグと端末３Ｄの状態を更新することができる。工作機械などの産業用設備や装置も施錠できる。
トークン番号を一回のみ書き込みできるＲＯＭの形で（自動車などの製品製造者がトークン番号を一度書き込むと攻撃者から書き換えされないＲＯＭの形で）端末３Ｄの記録装置に記録させ製品の製造番号と対応づけることで、自動車等の製品の保有者の履歴情報、流通情報やメンテナンス履歴の記録に役立つかもしれない。自動車に限らず乗物や設備、製品の流通状況を調べることに利用できる。
【０３９９】
＜建物の扉の鍵、金庫など容器の鍵の鍵＞
建物の鍵、金庫など容器の鍵の鍵については、自動車の製造時と同じくトークン番号を金庫や施錠機能付き扉の製品ごとに製造時に割り当て、製品に内蔵した端末３Ｄに固有のトークン番号を端末３Ｄの記憶装置３０ＤのＲＯＭに記録させ、ユーザーのもとへ端末３Ｄを含む製品を流通させることができる。一方で３０ＤのＲＯＭに製品の製造番号に対応したトークン番号を割り当てることは製品の製造工程において時間や労力費用を必要とする恐れがある。（例として大量生産される小型の錠前型端末３Ｄに個別にトークン番号を割り当てるのは小型の錠前の製造コストの増加につながりかねない）
そこで３０Ｄにトークン番号を記録させる際にＲＯＭではなく不揮発性のＲＡＭを用い

、顧客が施錠機能付き扉や金庫等の容器を購入した際にユーザーの手でＮＦＣタグの認証に利用するトークン番号を記録する方式が考えられる。ユーザーが例として端末３Ｄを備えた金庫を購入し、またトークンの発行を依頼しトークン番号ＴＩＤＡのトークンが発行される。購入した金庫は施錠されておらず、金庫の扉の裏に設置された端末３Ｄへの接続用端子やＮＦＣ等通信部を用いて、ユーザー端末１Ａなどから記憶装置３０Ｄにアクセスし、金庫のトークン番号をユーザー識別子Ａが保有しているトークン番号ＴＩＤＡに設定する。そして端末１Ａの持っている秘密鍵１０１Ａを用いてサーバ３ＡよりＯＷＰを生成し、ＯＷＰとユーザー識別子Ａ（そしてトークン番号ＴＩＤＡ）をＮＦＣタグ１９に記録させ、前記認証情報を記録したＮＦＣタグ１９にて端末３ＤでＯＷＰによるＯＴＰ認証を行い認証結果が一致した際には金庫を解錠する（施錠または解錠する）。
金庫等に搭載する端末３Ｄにおいても自動車の場合と同じくユーザー識別子を端末３Ｄに記録させてもよい。（装置にユーザー識別子という形でユーザーの名義を記入してもよい。）

【０４００】

＜ＮＦＣタグの電源および入出力装置＞

ＮＦＣタグ１９Ａには電源装置の中に一次電池または二次電池を含んでいてもよい。１９Ａには入力装置として一つ以上の押しボタン式スイッチ（またはタッチセンサ）を備えていてもよい。自動車の鍵の用途では自動車のドアの施錠をＮＦＣなどの無線通信により遠隔地から解錠することを実行する押しボタンと、解錠されたドアを再度施錠するための施錠ボタンの二つを１９Ａは備え、なおかつ１９ＡのＯＷＰなどを記録した記憶装置、制御演算装置、入出力装置、無線通信を含む電子計算機を動作させるための電源として一次電池または二次電池が必要となる。

ここで１９Ａの入力装置はＮＦＣ機能付きのＩＣカードやタグであるときは、入力装置がＮＦＣタグとしての無線通信によるものだけの場合もある。
また入力装置は押しボタン式やタッチセンサを具体例として述べたがその方式は特に指定はしない。（例えば音センサによる音声入力のようにセンサの種類に応じて多様な入力形態が考えられるためである）。１９ＡにはＮＦＣ機能も含む無線の入力装置やその他センサによる入力装置を備えている。

さらに可能であればＮＦＣタグ１９Ａは入力装置を操作した際（入力装置が動作している際に）に入力装置が操作されたことを光や音で知らせるための出力装置を備えていてもよい。１９Ａは発光ダイオードなどの発光装置またはブザーを備えていてもよい。

【実施例３】

【０４０１】

＜暗号化されたデータを復号する用途＞

図８Ｃ及び図８Ｄは本発明のワンタイムパスワード認証システム（ＯＴＰ認証システム）において暗号化されたデータを復号し閲覧する際の装置の接続図である。図８Ｃはネットワーク２０を経由して双方向に通信できるよう端末４Ａ、端末１Ｃ、端末３Ａ、端末５Ａ，端末５Ｂが接続されている。図８Ｄは端末４Ａ（および４Ａと同等の複数端末）が放送局端末５Ｃから暗号化データ放送を受信し、受信した暗号化データを復号する場合の装置の接続図である。

端末４Ａの記録部にはソフトウェアＣＲＨＮの情報４０３Ａが記録され、４０３Ａのプログラムを実行しソフトウェアＣＲＨＮを動作させ暗号化されたデータＥｎｃＤａｔａ（図４Ｂの４０３４Ａ）を本発明の認証システムから得られた鍵情報ＣＴＡＵ４０３１Ａや外部の鍵情報ＡＫＴＢ４０３２Ａを用いて復号に用いる鍵情報ＴＴＫＹ４０３３Ａを作成し、４０３３Ａを用いて４０３４Ａを復号し復号されたデータＤｅｃＤａｔａ（図４Ｂの４０３５Ａ）を得て４０３５Ａを閲覧または視聴し、４０３５Ａがプログラムの場合は実行する。図８Ｃと図８Ｄは実施例３（実施形態３）を説明する資料である。

【０４０２】

実施例３（実施形態３）の動作は実施例１と似ている。実施例１ではウェブサイトにログインしサービスにアクセスする用途で用いるが、実施例３ではログインする対象が暗号

化されたデータを復号してアクセスすることに代わる。実施例３ではブロック番号Ｂｎ等ブロックチェーンの時刻情報を利用したＢｎＴＯＴＰを用いる。実施例で利用するＢｎＴＯＴＰはＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）またはＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，Ｖ）またはＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ，Ｂｎ，Ｖ）であり、変数ＫＣとＢＣはコントラクト管理者によって関数ｆｓｃｂにより変更され更新されることがある。

【０４０３】

図７ＣＡに配信または記録媒体の配布または放送を受信して得られた暗号化されたデータを復号するシークエンスを示す。図７ＣＢに平文のデータの暗号化を行い作成された暗号化データを配信または配布または放送するシークエンスを示す。図７ＣＣにネットワークからユーザー端末の通信が切断されたオフライン状態において閲覧済み証明書ＯＦＢＫＭＫを用いて暗号化ファイルを復号し閲覧する例を示す。

【０４０４】

＜暗号化されたデータの作成＞

まずソフトウェアＣＲＨＮ４０３Ａを用いて暗号化されたファイルを作成する手順から述べる。

図７ＣＢのシークエンスＳ１８０で平文データ（コンテンツデータ、コンテンツファイル）を用意する。Ｓ１８１では平文データに添付する電子証明書ＤｅｃＣｅｒｔなど（電子証明書とコンテンツデータをある秘密鍵で電子署名した情報を含む）を取得する。これは必須ではないが、暗号化データを復号した際に平文ファイルの作成者が誰かを知り、電子証明書の発行者がソフトウェアＣＲＨＮに広告などを掲載するサーバーに登録された発行者であると分かっていれば悪意のあるプログラムではないと判断し、そのデータを実行できる。

通常、ソフトウェアＣＲＨＮが電子書籍や音楽動画の再生ソフトウェアとして利用されるのみの場合、音楽・動画・書籍ファイルであればファイル名に拡張子がついておりその拡張子に従ってファイルを処理しドキュメントファイルの表示や音楽映像ファイルの再生ができるので、悪意のあるファイルを実行する可能性は低いかもしれない。しかしファイル名に拡張子が無くあらゆるデータを実行できるようソフトウェアＣＲＨＮをプログラムする場合には悪意のあるプログラムデータに対する対抗手段が必要となり、その手段の一つとして平文のファイルや暗号化された後のファイルに登録された電子証明書と電子署名を付与することが望ましい。

【０４０５】

Ｓ１８１では平文データが雑誌であったり新聞であったり週間誌等であることも想定される。紙の新聞や雑誌には紙面に広告などが印刷されているように、平文ファイルに広告データや広告を配信するサイトをもつ広告配信用サーバ端末５Ａ（ＣＲＨＮｃｍ）にリンクし接続させるための広告配信サイトのＵＲＩを埋め込むことができる。

この端末５Ａの広告配信サイトへのＵＲＩを平文データに埋め込むことによるによる機能を利用するかどうかは平文データの権利者の判断によるが、サーバ５Ａには不正アクセス防止機能が備えることができ、また広告の表示と、平文データに由来して広告が表示されたことによる平文データの権利者への広告収入の還元も期待できるため搭載することが望ましいかもしれない。前記機能はコンテンツの権利者がユーザー端末によって権利者の暗号化データをソフトウェア４０３Ａを用いて復号し閲覧されるたびに広告収入を得て収益を得ることにつながる収益化機能となる。

トークン番号ごとに異なる広告配信サイトのＵＲＩを設定することもできる（基本的なＵＲＩにユーザー識別子やトークン番号に由来する値を設定しそのＵＲＩに対応する広告データを設定するなど）。

ここで設定するＵＲＩからは配信する広告などは平文データやそれに対応するＯＴＰトークンに記載のレイティング情報に応じた広告を配信する必要がある。一度暗号化しネットワーク２０を通じて世界中に配布し流通した暗号化ファイルに含まれる平文データに記載されたＵＲＩは変更出来ない。

【０４０６】
端末５Ａが配信する広告配信サイトへ接続するためのＵＲＩはソフトウェアＣＲＨＮ４０３Ａにも設定でき、端末４Ａで４０３Ａを実行させた際に広告を表示させることができる。広告を表示させると同時に不正アクセスの有無を４０３Ａが調べることもできる。広告に加えソフトウェアＣＲＨＮ４０３Ａのソフトウェア情報の更新の案内もできる。ただし、コンテンツの閲覧専用ではなく個人または法人の業務用に設計された４０３Ａは広告へ接続するＵＲＩを持たないこともある。
【０４０７】
Ｓ１８２ではＳ１８１で作成し登録や広告用のＵＲＩを埋め込んだ平文データを暗号化及び復号するＯＴＰトークンのコントラクトをプログラムする。実施例１や実施例２と同様な工程である。看板となる変数３０２４Ａにコンテンツの名前や権利者名、権利者の連絡先、レイティング等の情報を記録する。またＯＴＰ認証関数の戻り値またはデータＣＴＡＵ（図３ＡＡやＡＢやＡＣの３０２１Ａ）あるいはＯＴＰ処理時の処理内容３０２２Ａや３０２２Ａで操作される情報のデータベース３０２３Ａといった変数を必要に応じて設定する。
ここで実施例３を実施する際に必要な変数は認証関数の戻り値ＣＴＡＵであり、ＣＴＡＵは認証したときにブロックチェーン上に記録された情報ＣＴＡＵを認証結果が正しいアクセス者に返し、そうでない場合にはＣＴＡＵではない情報（認証ができないときの情報）を返す。実施例３において暗号化データを復号するための共通鍵暗号の共通鍵ＴＴＫＹはＣＴＡＵを基に計算されるので、コントラクトの作成者および管理者はＣＴＡＵの設定を行う必要がある。
３０２１ＡのＣＴＡＵに関する情報はＣＴＡＵを変更する権限のあるユーザー識別子からのアクセスを受けてＣＴＡＵを変更させるセッター関数を備えていてもよい。トークン番号に異なるＣＴＡＵ（マッピング変数として表現する場合ＣＴＡＵ［ＴＩＤＡ］）を設定することも可能である。ただしその場合も各ユーザー毎にＣＴＡＵ［ＴＩＤＡ］を設定する必要がある。さらにユーザーのＣＴＡＵ［ＴＩＤＡ］毎にコンテンツを暗号化して配信する必要がある（そしてブロックチェーン上でのトランザクションが増加する）。
３０２１ＡのＣＴＡＵは端末３Ａにおいての値であり、ＯＴＰ認証後に端末４Ａに４０３１Ａとして記録される。３０２１Ａと４０３１Ａは同じ値である。
【０４０８】
実施例３では簡易にブロックチェーン上から入手できる鍵として単一のＣＴＡＵをコントラクトに記録させ、認証関数の戻り値とした。本発明では好ましくはＣＴＡＵデータ３０２１Ａの情報が秘匿できるブロックチェーンの基盤（または分散型台帳システムＤＬＳの基盤）を用いることが好ましい。コントラクトのデプロイ時のトランザクションやＫＣ値ＢＣ値といったシークレット変数、シード値とともにＣＴＡＵデータ３０２１Ａも秘匿化されるか許可を受けたアクセスやまたは限定されたアクセス者のみ閲覧できるようにすることが好ましい。
【０４０９】
本発明の実施例３を行う中で、コントラクトやトランザクション内容が世界中に公開されたイーサリアムを用いたため、ＣＴＡＵ（３０２１Ａ）はブロックチェーン上に公開せざるを得ない。そのため３０２１Ａ以外の鍵を用いて暗号化する事が必要となった。そしてブロックチェーンとは異なる経路で得られる鍵ＡＫＴＢ（図４Ｂの４０３２Ａ）とコントラクトのＣＴＡＵ（３０２１Ａ）を用いてデータを暗号化する共通鍵ＴＴＫＹとすることで暗号化を行った。
【０４１０】
さらにソフトウェアＣＲＨＮ（４０３Ａ）内部に難読化または暗号化したソースコード―内部にソフトウェア用の秘密鍵ＣＲＫＹ（図４Ｂの４０３０２Ａ）を加え、ＣＴＡＵ（３０２１Ａまたは４０３１Ａ）とＡＫＴＢ（４０３２Ａ）とＣＲＫＹ（４０３０２）より共通鍵暗号に用い平文ファイルの暗号化と復号を行う鍵ＴＴＫＹ（４０３３Ａ）を生成させた。

また実際にはこのほかにＴＴＫＹを解読されぬよう４０３２Ａを複数用いたり、難読化されたソフトウェアＣＲＨＮのソースコード内にソフトウェアＣＲＨＮに関する鍵情報を管理するブロックチェーン上の専用スマートコントラクト（コントラクト識別子ＡＰＫＹ、図４Ｂの４０３０１）にアクセスさせ、鍵情報ＣＡＰＫＹ（図４Ｂ４０３０３Ａ）を取得させ、ＣＴＡＵとＡＫＴＢとＣＲＫＹにを加えたＣＡＰＫＹの4つ変数を用いてＴＴＫＹ（４０３３Ａ）を生成する方法を考案した。実施例３ではＣＴＡＵとＡＫＴＢとＣＲＫＹの３つの変数を使い、共通鍵暗号に用いるＴＴＫＹ（４０３３Ａ）を算出させた。なお前記３つの変数そのまま結合させて共通鍵とするわけでななく、ハッシュ化や変数値の一部の切り取りを行って４０３３Ａを算出を行う。４０３３Ａを算出する計算方法や処理方法を含むプログラムはソフトウェア４０３Ａに記録される。

【０４１１】

実施例３ではＣＴＡＵ（３０２１Ａ）とＡＫＴＢ（４０３２Ａ）を基にＣＲＫＹ（４０３０２Ａ）やＣＡＰＫＹ（４０３０３Ａ）利用してＴＴＫＹ（４０３３Ａ）を計算しているが本発明をコンテンツの権利者が利用し暗号化されたコンテンツの配布に用いるときは少なくともブロックチェーン上のコントラクトにおいて認証関数を実行した際のＯＴＰ認証結果を含むＣＴＡＵ（３０２１）に由来する共有鍵暗号の共有鍵４０３３Ａを利用する。

【０４１２】

ＣＴＡＵ（３０２１Ａまたは４０３１Ａ）に加えＡＫＴＢ（４０３２Ａ）が利用できる。４０３２Ａは具体的はある書籍や音声映像データをＯＴＰトークンとして購入した人に対し、そのトークン番号に対応したパスワード値をＡＫＴＢとして電子メールや郵便などの手段で送信し、かつ電子メールで送信したＡＫＴＢとコントラクトで共通のＣＴＡＵから計算されるＴＴＫＹ（４０３３Ａ）にて平文を共通鍵暗号化（または対称鍵暗号化）し、その暗号化データをクラウドストレージや電子メール、磁気テープ・磁気ディスク・光学ディスク・半導体メモリなどで配布し、ＯＴＰトークンを購入したユーザーが４０３３Ａを用いて配布された暗号化データについて、
ユーザーは端末４Ａの記憶装置４０Ａに記憶されたソフトウェアＣＲＨＮ４０３Ａと、
ＯＴＰトークンの割り当てられたユーザーの秘密鍵４０１Ａと、
ＯＴＰトークンのコントラクト識別子と
ＯＴＰトークン番号ＴＩＤＡと、
４０３Ａで４０１Ａとトークン番号ＴＩＤＡを用いてＯＴＰ認証して得られるＣＴＡＵ（３０２１Ａまたは４０３１Ａ）と
電子メールなどで通知された鍵ＡＫＴＢ（４０３２Ａ）
を用いて暗号化されたデータを復号することができる。

【０４１３】

管理者端末１Ｃは暗号化データの復号に利用できるある値のＣＴＡＵ（３０２１Ａ）をコントラクトの認証関数の戻り値に利用できるよう設定し、ＯＴＰの計算に用いるＫＣ値、ＢＣ値を設定しＯＴＰをＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）またはＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，Ｖ）またはＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ，Ｂｎ，Ｖ）で計算するようプログラムしたＯＴＰ生成関数と認証関数を含むコントラクトを作成し、Ｓ１８３にてＳ１８２で作成したコントラクトをブロックチェーンシステムＤＬＳのノードとなるサーバ端末３Ａにアクセスしてデプロイする。

【０４１４】

Ｓ１８４ではＳ１８３で端末１ＣがＤＬＳにデプロイしたコントラクトの識別子３０１９Ａを取得する。

Ｓ１８５ではサービスにコントラクト識別子やコントラクトの名前、作成者名、作成日、レイティング等をサーバ５Ａやサーバ５Ｂの記憶部および記憶部のデータベースや制御部に設定する。また暗号化データの登録ができるようになる。

サーバ端末５Ｂは端末４Ａからアクセスを受け、サーバ５Ｂが電子書籍や音声動画コン

ピュータソフトウェアなどコンテンツの販売、電子商取引用のサーバを兼ねている場合には４Ａが購入する商品の権利者名レイティング情報等と商品名とそれに対応する暗号化データを復号するためのＯＴＰトークンのコントラクト識別子とソフトウェアＣＲＨＮを対応付けておくことができる。サーバ５Ｂがある団体の機密データを暗号化し団体内で共有する用途である場合そのデータの名前、あるいはファイル名・データ作成者名・データ権利者名とＯＴＰトークンのコントラクト識別子を対応付けておくことができる。

【０４１５】

また、端末５Ｂは電子商取引に必要な顧客の氏名、生年月日等、電子メールアドレス、ログインパスワード、住所情報、電話番号等、ブロックチェーンへのアクセスに用いるユーザ識別子Ａ、保有している（または購入履歴のある）ＯＴＰトークンのコントラクト識別子とそれに応じた保有するトークンのトークン番号といった顧客の個人データを持つ。端末５Ｂは前記顧客の個人データを基に、顧客の支持を受けて外部のクレジットカードなど決済事業者及びそのサーバ等端末と連携して商品の購入と決済を行うことが出来る。

そして端末５Ｂは顧客の電子メールアドレス、電話番号、住所に対し電子メールや電話、信書の郵送などで通知された鍵ＡＫＴＢ（４０３２Ａ）を伝達できる。また本来はブロックチェーン上で行わないはずの４０３２Ａの伝達を４０３２Ａをユーザー識別子Ａに内容を秘匿化できるトランザクションを用いてＡＫＴＢ（４０３２Ａ）を送る事もできる。またはユーザ識別子Ａを計算できる端末４Ａの秘密鍵４０１Ａを基に別のブロックチェーン基盤を構築し秘密鍵４０１ＡＡからユーザー識別子Ａではなくユーザー識別子ＡＡが計算される場合にユーザー識別子ＡＡに向けて４０３２Ａを送ることも考えられる。

具体的にはイーサリアムというブロックチェーンの基盤でユーザ識別子Ａを、ハイパーレジャー（Hyperledger ）というブロックチェーンの基盤でユーザ識別子ＡＡを示す秘密鍵４０１Ａを用い、ＯＴＰトークンの発行はイーサリアムを用い、ＡＫＴＢ（４０３２Ａ）の通知はハイパーレジャーのトランザクションを持ちいることで、同一の秘密鍵を使いながら異なるブロックチェーンで本発明で暗号化されたデータの復号にかかわる操作が可能である。

【０４１６】

Ｓ１８５では広告機能を持つサーバ５Ａ（ＳＶＣＲＨＮｃｍ）に対してもコントラクトの識別子やコンテンツの情報を登録することができる。

【０４１７】

Ｓ１８６ではコントラクトの管理者端末１Ｃが顧客にトークンや暗号データを配布する前に、試験用および暗号化用としてＯＴＰトークンを端末１Ｃの秘密鍵１０１Ｃに対応するユーザ識別子Ｃに発行する。Ｓ１８６は端末１ＣにＯＴＰトークン発行し、平文コンテンツを暗号化した暗号化データを作成し端末１Ｃに記録し、記録した暗号化データを配布するためのシークエンスである。

後に後述するが、Ｓ１５５では端末５Ｂの電子商取引機能により決済を行いＯＴＰトークンの購入と暗号化データの閲覧権及び閲覧できるデータの所有権を得たユーザーのユーザー識別子Ａに対しＯＴＰトークンを発行する。ここで必ずしもＯＴＰトークンは端末５Ｂで購入される必要はなく、端末１Ｃが注文や依頼を受ければ発行できる。たとえば端末１ＣがＥＣサイトやＥＣ型の書店サイトなどと契約しており、ＥＣサイトが指定するユーザー識別子に対しトークン番号割り当てて発行していく形態が考えられる。

ここで重要なこととして本発明はトークンの送付先となるユーザ識別子が正しく知らされていないとＯＴＰトークンを正しい相手に送付できない。トークン発行には正しい送付先のユーザー識別子が必要である。

【０４１８】

Ｓ１８７ではソフトウェアＣＲＨＮ（４０３Ａ）を主に端末５Ｂから取得する。端末５Ｂ以外でも信頼できる４０３Ａの保存先から入手できる。暗号化データの配布者はそのデータを復号できる版の（バージョンの）４０３Ａを指定してユーザーに知らせなければならない。具体的に運用する場合は暗号化データの作成に用いたバージョンのソフトウェアＣＲＨＮ（４０３Ａ）を暗号化データと共に配布すればよい。

【０４１９】
Ｓ１８８では設定読込・入力等を行う。４０３Ａに秘密鍵を直接入力するか秘密鍵を管理する４０３Ａとは別のソフトウェアと連携させ秘密鍵情報を４０３Ａに入力する。
【０４２０】
Ｓ１９９では４０３Ａ起動時、あるいは秘密鍵（図７ＣＢでは端末１Ｃの秘密鍵１０１Ｃ）の情報が４０３Ａに入力された時にユーザー識別子が計算され生成され、４０３に埋め込まれた端末５Ａの広告配信用ＵＲＩへリンクさせることができ、このときコントラクト管理者１Ｃに対しても図６Ｘに示すような不正アクセスの監視を行うことができる。
【０４２１】
Ｓ１８９ではＡＫＴＢ（４０３２Ａ）を設定する。もしくはあらかじめ決めておいたＡＫＴＢ（４０３２Ａ）を端末１Ｃの記録装置に記憶させる。Ｓ１８９はＳ１８８と同時に行ってもよい。ＡＫＴＢ（４０３２Ａ）はトークンを配布したいユーザーに対応して設定される。
具体的にはある団体で年や月そして週や日ごとに異なるＡＫＴＢ（４０３２Ａ）を設定して団体に所属するユーザー同士がＡＫＴＢ（４０３２Ａ）を知っておりＯＴＰトークンを所有出来るユーザーにのみ暗号化したデータを復号できるようにしてもよい。
あるいは電子書籍型出版物を権利者が平文データとして、あるユーザー識別子に対応した固有のＡＫＴＢ（４０３２Ａ）を設定しメールアドレスなどでＡＫＴＢ（４０３２Ａ）を通知してから、権利者は平文データをＡに対応したＡＫＴＢ（４０３２Ａ）を用いて暗号化してもよい。
【０４２２】
暗号化に関して、ＣＴＡＵ（３０２１Ａまたは４０３１Ａ）と任意設定し配布先に通知されるＡＫＴＢ（４０３２Ａ）とソフトウェアＣＲＨＮ（４０３Ａ）と４０３Ａの秘密鍵ＣＲＫＹ（４０３０２Ａ）を利用してユーザー識別子Ａだけが知るＡＫＴＢ（４０３２Ａ）を使い復号できる暗号化データを作成し、Ａのメールアドレスに添付ファイルとして添付しては配布するかクラウドストレージサービスなどで配布するか、端末５Ｂのような本発明で利用されるサーバ端末を用いて配布できる。また配布時にネットワーク２０を使わなくとも磁気テープ、磁気ディスク、光学ディスク、半導体メモリなどの外部記憶装置を郵便や配達によってユーザーの住所に届けることで配布できる。
雑誌や書籍について顧客ごとに異なるＡＫＴＢ（４０３２Ａ）を設定し配布する場合はコンテンツの権利者の平文データの保護に役立つ一方でユーザーの人数に応じた平文データの暗号化処理を行いＡＫＴＢ（４０３２Ａ）の情報を対応する暗号化データをユーザーに配布する必要がある。
新聞や雑誌など放送と類似した1対多数のマスメディアなコンテンツ流通を行う書籍の場合には、ある期間（毎日・毎週）に我が国の何割かのユーザーごとに平文をユーザーの総数に応じて暗号化する必要が生じかねず電子計算機やネットワークのリソース（資源）を消費する恐れがある。
その場合、ある期間（毎週、毎月、毎年など）や地域（長野、大阪、東京など）によって代わるＡＫＴＢ（４０３２Ａ）をユーザーの電子メールや信書の郵便・配達の形で配布し、ＡＫＴＢ（４０３２Ａ）に応じた新聞の暗号化データを配布することで、新聞の閲覧権購入権となるＯＴＰトークンをブロックチェーンに所有し、ＡＫＴＢ（４０３２Ａ）を知り、ソフトウェアＣＲＨＮ（４０３Ａ）を持っているユーザがそのデータを入手できれば新聞を読めるようにすることもできる。
【０４２３】
配布された暗号化データはユーザの端末に記録され、ユーザー端末に暗号化データ（４０３４Ａ）をＯＴＰトークン（ＯＴＰトークンの認証時に得られるＣＴＡＵ（３０２１Ａ））とＡＫＴＢ（４０３２Ａ）とソフトウェアＣＲＨＮ（４０３Ａ）とＣＲＫＹ（４０３０２Ａ）と秘密鍵４０１Ａがある場合に復号し、復号データ・平文データ（４０３５Ａ）として閲覧できる。
閲覧時に暗号化データを復号できる鍵ＴＴＫＹ（４０３３Ａ）が算出されそれを秘密鍵

４０１Ａで暗号化しＣＴＴＫＹ（４０３６１Ａ）とし、ＣＴＴＫＹ（４０３６１Ａ）をソフトウェアＣＲＨＮ（４０３Ａ）に記録されたＣＲＫＹ（４０３０２Ａ）で暗号化しＡＣＴＴＫＹ（４０３６０Ａ）を得て、ＯＴＰ認証済み証明書４０３６Ａまたは閲覧済み証明書ＯＦＢＫＭＫ（４０３６Ａ）データ内部に記録する。ＯＦＢＫＭＫはソフトウェアＣＲＨＮの秘密鍵とユーザーの秘密鍵で暗号化されたコンテンツの復号用共通鍵ＴＴＫＹ（４０３３Ａ）を記録している。（ＯＦＢＫＭＫはオフライン・ブック・マーク）

ＯＦＢＫＭＫ４０３６Ａは閲覧時間などを制御した形でユーザーへのオフライン時のアクセスを許可する。

ＯＴＰトークンが譲渡制限機能が解除されており他者にトークンが送信されている場合、ＯＦＢＫＭＫ４０３６Ａは本の閲覧権や所有権が無い場合であるにもかかわらず本を読むことが可能になりかねない。

そこでコンテンツの権利者がＯＦＢＫＭＫ機能４０３６Ａは閲覧制限時間の時間数値がＯＴＰ認証を行う毎に最大となり、その時のタイムスタンプがＨＭＡＣや電子署名などを施された形でＯＦＢＫＭＫに記録されており、ＯＦＢＫＭＫに記載された認証時のタイムスタンプから遅くなるほどネットワーク２０から切断されオフライン時になった場合に閲覧可能な時間が減少するようソフトウェア４０３Ａプログラムできる。閲覧は時間は実施例３では１０分や３０分、数時間単位で設定した。

例として閲覧制限時間がＯＴＰ認証直後は３００分であった場合、本発明ではＯＦＢＫＭＫのタイムスタンプ時刻からｙ年経過するごとに年数で割った時刻だけ閲覧するなどができる。たとえばｙ＝１０年の時、タイムスタンプから１０年経過しており、３００分を１０年の１０で割り、３００［分］÷１０＝30［分］の間に限り、ソフトウェアＣＲＨＮ（４０３Ａ）にて閲覧可能などとすることができる。ここでユーザーがＯＴＰトークンを保有していればオンライン時にブロックチェーンにアクセスさせ認証させ、ＯＦＢＫＭＫを新規に作成し閲覧時間を３００分に再設定できる。

タイムスタンプと現在時刻の比較の処理において現在時刻はユーザー端末４Ａの時刻に基づく。ＧＮＳＳやＪＪＹ、ＮＩＴＺなどの時刻データ送信局があり正しい時刻データが端末で受信でき、端末の時刻データが正しく設定されていることが好ましい。なお平文データの権利者が許可する場合にはＯＦＢＫＭＫによる閲覧時間を設定しないこともできる。

ＯＦＢＫＭＡＫ４０３６Ａの機能は時間制限付きで閲覧できる暗号化データを平文化しその平文にアクセスできる機能であり、紙の書籍に例えると紙の書面を複写したデータ制限付きで閲覧できる証明書を保有しているような概念である。もしくは一度閲覧した書籍のイメージ図をヒトが記憶しており時間経過とともに閲覧した書籍のイメージ図を忘れて思い出しにくくなるような様子を基にしたものである。時間経過によって４０３６Ａを用いた復号時に平文データがぼやけて端末４Ａのディスプレイに表示されるなどの加工を４０３Ａが行ってもよい。

【０４２４】

紙の書籍であっても資料として複写するなどのケースはあり、コンテンツをディスプレイの撮影などから保護するなどしないと複写されることの危険性は残る。一方でコンテンツがオフラインになりうる災害時にも利用できる有益なものである場合、ユーザーが読むことができるほうが好ましいので本発明では閲覧済み証明書ＯＦＢＫＭＫ（４０３６Ａ）を採用した。

コンテンツをユーザー端末に残すことなく配信したい場合は実施例１のウェブサイトへのログイン方式を利用したほうが好ましい。ただし、その場合はログイン先のサーバーがサービス終了などをしてデータを無くしてしまえばユーザーが購読してきた書籍や音楽映像作品は閲覧できなくなってしまう。

紙の書籍、古文書、浮世絵などは数百年を超え後世に残され文化を伝えている。本発明ではデジタルデータであっても長い年数を経て後世に残されるべきデータに対しその所有権、閲覧権、利用権をＯＴＰトークンの形で記録しながら、そのトークンで閲覧できるデータを暗号化データとして流通させ、かつその暗号化データを災害時などネットワークが

切断されたオフラインにおいてもユーザーの手元のデータによって閲覧可能とした。ブロックチェーンにて閲覧や所有の権利となるＯＴＰトークンは管理されるがブロックチェーンは必ずしもアクセスできるとは限らず、本発明ではユーザーが購入した書籍をオフラインでも閲覧できるよう配慮した。

【０４２５】

コンテンツが新聞等であるときは、それが定期購読型のサービスである為、ＯＴＰトークンのコントラクトについてＣＴＡＵ（３０２１Ａ）値を定期更新する必要があるかもしれない。あるいはＣＴＡＵの代わりにＡＫＴＢ（４０３２Ａ）を定期更新する必要があるかもしれない。

ユーザーのＯＴＰトークン番号に対応した有効無効の変数（トークン番号をキーとした真偽値型のトークンの有効無効を表すマッピング変数）を用意して、認証関数（３０１８Ａ）の認証時にその変数が真か偽かを判断し、真であれば認証の戻り値ＣＴＡＵ（３０２１Ａ）を返し、偽であればＣＴＡＵ（３０２１Ａ）を返さないという処理も追加できる。

ここでユーザーのＯＴＰトークン番号に対応した有効無効の変数（トークン番号をキーとした真偽値型のトークンの有効無効を表すマッピング変数）コントラクト管理者の端末１Ｃがすべてのトークン番号に対し真か偽かを設定できるセッター関数を設定する必要がある。

（実施例１や実施例２においても入場やログインの閲覧権やチケットでは有効期限後に端末１Ｃから トークン番号をキーとした真偽値型のトークンの有効無効を表すマッピング変数を真から偽に書き換えることでＯＴＰの生成や認証を停止させることができてもよい。

またあるＯＴＰトークンが、ある本・書籍・音楽レコード・動画に関する暗号化データを復号するＯＴＰトークンで、有効期限が無期限で、ＯＴＰトークンを所持している限り有効な場合は、トークンの有効無効を表すマッピング関数やＯＴＰの生成認証を停止させる関数は不要である。）

新聞や雑誌ではインターネットに接続できる場合は実施例１のような新聞や雑誌の権利者サイトへのログイン権としてＯＴＰトークンを利用し、アクセスしたユーザーに閲覧制限などをかけながらコンテンツを適宜暗号化しながら配信するほうが好ましいかもしれない。ただし、紙の新聞と同じく、ユーザーの端末４Ａの手元に暗号化データを保存し、ネットワークに接続されていないオフラインでも閲覧したい場合には実施例３の方式をとることが本発明では可能である。新聞は過去の出来事を報じており、ユーザーの手元に残る方式のほうが出来事の記録を行うには適しているかもしれない。

【０４２６】

Ｓ１９０からＳ１９２までの一連のシークエンスは、ブロックチェーンシステムＤＬＳ（端末３Ａ）へ端末４Ａがアクセスし、ＤＬＳのＯＴＰトークンのコントラクトに備えられたＯＴＰ生成関数から端末４Ａの記憶装置にＯＴＰ取得する。ここでＯＴＰはＢｎＴＯＴＰ型のＯＴＰでもよいし、ＯＷＰ型のＯＴＰでもよい。実施例３ではＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ，Ｖ）またはＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，ＢＣ，Ｂｎ，Ｖ）を用いた。ＯＴＰ生成のシークエンスは実施例１や実施例２と同様である。

【０４２７】

Ｓ１９３からＳ１９５までの一連のシークエンスは、実施例１や実施例２と同じく取得したＯＴＰとＯＴＰトークンのトークン番号とユーザー識別子を引数としてＯＴＰ認証関数に入力し（Ｓ１９３，Ｓ１９４部分）、認証関数からの戻り値ＣＴＡＵ（３０２１Ａまたは４０３１Ａ）を得る（Ｓ１９５部分）ものである。

【０４２８】

Ｓ１９６ではＣＴＡＵ（３０２１Ａまたは４０３１Ａ）とＡＫＴＢ（４０３２Ａ）とＣＲＫＹ（４０３０２Ａ）から平文データを暗号化する鍵ＴＴＫＹ（４０３３Ａ）をソフトウェアＣＲＨＮ（４０３Ａ）のプログラムに沿って処理し生成する。ここで４０３Ａのプログラムにおいて４０３３Ａを生成計算する工程にハッシュ化や数値文字列の切り取り加

工などの処理を含んでもよく４０３Ａのプログラムもまた暗号化を復号する鍵となる要素である。

【０４２９】

Ｓ１９７ではＳ１９６で算出されたＴＴＫＹ（４０３３Ａ）を共通鍵に用いて共通鍵暗号化を平文データ（４０３５Ａ、ただし４０３５Ａは端末１Ｃの記憶装置にも存在可能であり端末４Ａの記憶装置にも存在できる）に行い、暗号化データＥｎｃＤａｔａ（４０３４Ａ、ただし４０３４Ａは端末１Ｃの記憶装置にも存在可能であり端末４Ａの記憶装置にも存在できる）を得る。共通鍵暗号化ではＡＥＳ（Advanced Encryption Standard）を用いた。実際にはＡＥＳの鍵のデータ長は１２８Ｂｉｔ、１９２Ｂｉｔ、２５６Ｂｉｔを利用した。

【０４３０】

Ｓ１９８では暗号化データ４０３４Ａをサーバ端末５Ｂ（ＳＶＣＲＨＮｄｒｉｖｅ）や、端末５Ｂ以外のクラウドストレージ、端末５Ｂとは異なるファイル保存・ファイル共有サーバーなどに保存させＯＴＰトークンを配布したユーザーが暗号化データ４０３４Ａを配信する。この過程で放送局となるサーバ端末５Ｃに暗号データ４０３４Ａを記録させ有線または無線にて放送させてもよい。光学ディスクなどの光学メディア、磁気テープや磁気ディスクなどの磁気メディア、半導体メモリ等に暗号化データ４０３４Ａ記録して配布してもよい。

そのほかに磁気や半導体を用いない記録媒体でもよい。暗号化したデータをマイクロフィルムに文字列に変換させ記録して保存し郵送などで配達して配布してもよい。多様な方法で暗号化データを配布し流通させる事ができる。マイクロフィルムと同様に暗号化したデータを文字列化したものを紙に印刷することもできうる。データの配布方法に制限は設けない。

【０４３１】

シークエンスＳ１９８でサーバ端末５Ｂではなく放送局サーバ端末５Ｃにデータを保管する際に、端末５Ｃが宇宙の人工衛星局である場合は端末５Ｃと相互通信するサーバ端末５ＣＣが必要である。また端末５Ｃが端末５ＣＣと専用の回線にて接続されている場合にも端末５ＣＣは必要である。暗号化されたデータ４０３４Ａをデータ放送に適した形に加工し（放送局からのデジタル放送用処理を行い）ユーザーのもとに送信する。デジタル放送用の処理は誤り訂正符号の追加やパケット化などがある。

無線式のデータのライブ放送の用途においては４０３３Ａを鍵として４０３５Ａから４０３４Ａを作成するときには天候などで電波がユーザの受信機に到達せずデータが途切れてしまう恐れがある。それに対処するため撮影録画されている映像や音声を随時４０３３Ａを鍵とした小さいデータのパケットとしてブロック暗号化を用いて配信したり、誤り訂正符号を添付したり、ストリーム暗号化を用いて配信することがある。

既存の例では地上波デジタル放送にはブロック暗号が利用されているが本発明では平文データに対しブロック暗号化に加えストリーム暗号化をソフトウェアＣＲＨＮ（４０３Ａ）が行うことができる。そしてストリーム暗号化された暗号化データを逐次放送することができる。また放送だけでなくネットワーク２０を介して双方向にストリーム暗号化データのやり取りを行いウェブ上での会議や音声動画の配信ができてもよい。

【０４３２】

＜暗号化されたデータの復号＞

次に暗号化されたデータを受け取ったユーザー端末４Ａが暗号化データの復号を行いデータの閲覧を行うシークエンスについて述べる。図７ＣＡにユーザー端末４Ａに配布された暗号化データの復号を行うシークエンスを示す。Ｓ１５０からＳ１５３までの一連のシークエンスは図７ＣＢのＳ１８２からＳ１８５までの一連のシークエンスと同じである。

【０４３３】

Ｓ１５４で端末１ＣはＯＴＰトークンの発行の指示を受ける。この時、端末４Ａのユーザーは購入したい暗号化データを購入可能なサーバ端末５Ｂや、端末５Ｂのほかに購入が可能な電子用取引サイトへＯＴＰトークンをユーザー識別子Ａを提示して注文し決済処理

を行った際に端末１Ｃはサーバー端末５Ｂや電子商取引サイトからユーザー識別子Ａに対し暗号化データが復号できるＯＴＰトークンに対応するコントラクト識別子を提示し、指定されたあるユーザー識別子にあるコントラクト識別子のＯＴＰトークンを発行するという指示を端末１Ｃは受ける。

ここでＯＴＰトークンの購入という表現があるが、これは暗号化データが雑誌や書籍や音声動画ソフトウェア放送等コンテンツで、コンテンツの権利者が存在し、暗号化データの閲覧権や所有権や利用権の販売を行う場合を想定している。会社などの団体や個人用途において例えば秘密にしたい情報を暗号化し、暗号化したデータを限られた団体の人々の間で共有するなどの場合にはＯＴＰトークンはＯＴＰトークンの購入ではなくＯＴＰトークンの使用許可を利用したいユーザー識別子に対して付与するという許可が必要になる。

【０４３４】

Ｓ１５５で端末１Ｃは端末１Ｃの秘密鍵１０１Ｃを用いてブロックチェーンシステムＤＬＳ（端末３Ａなど）のＯＴＰトークンのコントラクトにアクセスしトークン番号ＴＩＤＡのトークンをユーザー識別子Ａに発行する。端末４Ａには秘密鍵４０１Ａからユーザー識別子Ａが計算できる。端末４ＡはＯＴＰトークンのデータを保有していないが秘密鍵４０１Ａを持つことでＤＬＳ上のＯＴＰトークンにアクセスしそれを操作する所有権を持っている。

【０４３５】

Ｓ１５６では端末４ＡがＯＴＰトークンのデプロイされたＤＬＳとは異なるＤＬＳからのトランザクションや電子メールまたは電話やファクシミリや信書の郵送配達などの形でブロックチェーン外部からのパスワードＡＫＴＢ（　４０３２Ａ　）を入手し端末４Ａの記録装置４０Ａに記録している。（ＡＫＴＢは合言葉の略である。）

このパスワードＡＫＴＢを用いることでブロックチェーン上のスマートコントラクトにパスワードを個別に設定することを回避しあるユーザー識別子Ａに対しパスワードを任意に設定し送ることもでき、あるいはユーザー識別子Ａやユーザー識別子Ｂなどがの所属する会社などの団体において合言葉のように指定したパスワード値ＡＫＴＢを社内の各社員のメールアドレスに通知させることもできる。

ＡＫＴＢを設定した経緯は実施例１と実施例２と実施例３で用いたイーサリアムというブロックチェーン基盤はコントラクトの変数が公開されており攻撃者がＣＴＡＵ値を解析することが可能であったため、やむを得ず解決策としてＡＫＴＢを利用した。ＡＫＴＢとＣＴＡＵの２つ、さらにはソースコードが難読化・暗号化されたソフトウェアＣＲＨＮのＣＲＫＹを加えた３つを用いることでブロックチェーンと閲覧ソフトウェアとそれ以外の外部パスワードの３つ知らなければ暗号化データを復号することはできない。
コントラクトのＣＴＡＵ値（３０２１Ａ）は秘匿化されていることが好ましい。

【０４３６】

Ｓ１５７では暗号化データＥｎｃＤａｔａ（４０３４Ａ）と前記暗号化データ４０３４Ａの閲覧を行えるソフトウェアＣＲＨＮ（４０３Ａ）をＯＴＰトークンを購入したサーバ端末５Ｂや電子商取引サイトから配布されたデータを入手する。なお磁気ディスクや磁気テープ、光学ディスク、半導体メモリなどの外部記録装置に記憶された４０３４Ａや４０３Ａを端末４Ａの記憶装置に複製してもよい。

【０４３７】

Ｓ１５８でソフトウェアＣＲＨＮ（４０３Ａ）を実行し起動させ、暗号化データの復号に必要なＯＴＰトークンの秘密鍵４０１Ａに関する情報の入力とＯＴＰトークンのコントラクト識別子、ＯＴＰトークンのトークン番号ＴＩＤＡを入力する。実施例3ではさらにＯＴＰの生成と認証を行うために接続するノードとなるサーバ端末３Ａを指定するＵＲＩを設定した。（ウォレットソフトを用いて秘密鍵の保存と入力や接続先ノードのＵＲＩを設定してもよい。）秘密鍵４０１Ａの入力とその後のプログラム実行によってユーザ識別子Ａが計算され、秘密鍵４０１Ａとユーザー識別子Ａとトークン番号ＴＩＤＡがソフトウェア４０３Ａに記録される。ソフトウェア４０３Ａには利用するブロックチェーン識別子やそのブロックチェーンにアクセスするプログラムが含まれている。

【０４３８】
Ｓ１５９ではＳ１５８で入力された情報からユーザー識別子やトークン番号を用いてソフトウェアＣＲＨＮ（４０３Ａ）のプログラムに設定された広告など配信サイトへのＵＲＩに従って広告等配信サービスサーバ端末５Ａにアクセスする。この時、ユーザー識別子Ａとトークン番号ＴＩＤＡとユーザー端末４ＡのＩＰアドレスや位置情報、端末のＩＤや端末のセンサ値をユーザーの同意した情報に対しサーバー５Ａに記録し図６Ｘのようなアクセスの監視と不正アクセス防止に利用することができる。
実施する際はＳ１５９ではユーザー識別子や、ユーザー識別子を匿名化した情報を用いることが多いと推測される。
【０４３９】
Ｓ１６０からＳ１６５まではＯＴＰの生成と認証の一連のシークエンスでありＳ１９０からＳ１９５までの一連のシークエンスにおける説明と同様である。ＯＴＰの生成、ＯＴＰの取得、取得したＯＴＰによる認証といったＳ１６０からＳ１６５までのシークエンスはソフトウェアＣＲＨＮ（４０３Ａ）内部で自動的に行ってもよい。Ｓ１６２からＳ１６３のシークエンスにおいて生成関数から取得したＯＴＰの認証関数への入力と実行を自動的に行えるよう４０３Ａのプログラムを設定することで自動化できる。実施例ではコンテンツを見るためのＯＴＰ認証をする労力や閲覧に至るまでの時間を減らすためプログラム内で自動的に認証させた。
Ｓ１６２からＳ１６３のシークエンスにおいてユーザーによるＯＴＰの手動入力を望み、自動化したくないときは生成関数から取得したＯＴＰの認証関数への入力と実行を手動で行うように４０３Ａのプログラムを設定できる。
【０４４０】
Ｓ１６６は４０３ＡにてＣＴＡＵ（４０３１Ａ）とＡＫＴＢ（４０３２Ａ）とＣＲＫＹ（４０３０Ａ）からＥｎｃＤａｔａ（４０３４Ａ）を復号する鍵情報ＴＴＫＹ（４０３３Ａ）を生成する。
【０４４１】
Ｓ１６７はＳ１６６で生成された鍵情報ＴＴＫＹ（４０３３Ａ）を用いて暗号化データＥｎｃＤａｔａ（４０３４Ａ）を復号し、平文データＤｅｃＤａｔａ（４０３５Ａ）を得る。
【０４４２】
Ｓ１６８にてＳ１６７で４０３４Ａを復号して端末４Ａの記憶装置に得られた平文データ４０３５Ａについて、端末４Ａの出力装置４５Ａと入力装置４４Ａを用いて平文データ４０３５Ａの閲覧や音声動画の視聴やソフトウェアおよびプログラムの実行と操作を行い、ユーザーにコンテンツを利用させる。実施例３では暗号化データを復号し得られた平文データ４０３５Ａは一時的なデータであり平文データの閲覧や視聴等コンテンツの利用が終了すると記憶装置から削除されるようにした。
実施例３ではウェブブラウザソフトが対応するＨＴＭＬ５とＥＣＭＡＳｃｒｉｐｔで処理できる米国アドビ社の文章データを管理するＰＤＦ形式のファイル（拡張子は.pdf）、Fraunhofer IISらが発明した音声データを扱うＭＰ３ファイル（拡張子は.mp3）、ＩＳＯのMPEG-4 Part 14（ISO/IEC 14496-14:2003）による動画音声などマルチメディアデータを扱うＭＰ４ファイル（拡張子は.mp4）にて本発明の実施例３方法を用いＯＴＰトークンとソフトウェアＣＲＨＮを用いた暗号化と復号を実施しファイルのデータの閲覧視聴を行った。ここでＰＤＦ形式のファイルはアクセス制御されたファイルを設定することもできる。
アクセス制御を施したＰＤＦ形式の平文ファイルを作成し、本発明の暗号化を復号した平文ファイルにアクセスコントロールや印刷禁止または印刷許可の設定を行うこともできる。また前記ＰＤＦファイルの例にあるように、任意のファイル形式、ファイル拡張子のアクセス制御プログラムを内蔵した平文データを本発明の方法で暗号化して配布され、その暗号化データが本発明の方法で復号され閲覧や実行を行う際に、平文ファイル利用時にアクセス制御を行えるようデータにプログラムしてもよい。平文ファイルにはファイルに

固有の方法（それぞれのコンテンツファイルに対応した方法）でアクセス制御を行うプログラムが含まれていてもよい。）

アクセス制御はコンテンツの印刷や外部記録端末への平文ファイルの複製の可否、平文ファイル内容の変更の可否、音楽動画を再生できる機器の制限などを含む。平文データがある団体の機密情報の場合ではその書類の管理者の判断によっては紙に印刷し金庫などに保存出来たほうが運用しやすい場合はプリンタを用いた印刷が可能な事例が想定される。権利者の存在する音声動画ファイルでは権利者の指示に応じて平文のファイルを複製させないように指定できる事例が想定される。

【０４４３】

ファイルの形式等に応じてソフトウェアＣＲＨＮ（４０３Ａ）は平文データ４０３５Ａの内容を読み取り、権利者が４０３５Ａ設定したプログラムに応じてユーザーの端末４Ａでのプリンタ４５２Ａを用いた紙などへの閲覧情報の印刷の可否や、ディスプレイ４５０Ａやスピーカー４５１Ａヘッドマウントディスプレイ４５３Ａなどへの出力の可否などを、平文データ内に書き込まれた出力の設定に応じて決定し平文データを出力装置４５Ａから出力させる。また入力装置４４Ａから入力された内容に応じて閲覧させる。例として文章ファイル、音声動画データ、ソフトウェアであればソフトウェアを操作するキーや入力ボタンやポインティングデバイスや音声入力、各種センサ、コントローラなど入出力装置を用いて平文データを操作し閲覧・視聴・実行する。

スマートフォン端末や携帯電話端末に用いるディスプレイ４５０Ａに出力してもよいし、デスクトップ型パーソナルコンピュータ端末に用いる２２インチなどの大きさのディスプレイ４５０Ａでもよい。持ち運びのできるラップトップ型またはノート型パーソナルコンピュータ端末やタブレット型端末のディスプレイ４５０Ａでもよい。

本発明の実施においてヘッドマウントディスプレイ４５３Ａは用いず通常のディプレイ４５０Ａのみを用い暗号化データをソフトウェア４０３Ａと分散型台帳システムＤＬＳを用いたＯＴＰ認証システムにより復号し閲覧利用してもよい。

本発明はＤＬＳによるＯＴＰ認証とログイン、入退場、施錠の解錠、暗号化データの復号（暗号化データへのログイン）を主な発明とする。ヘッドマウントディスプレイによる生体認証やコンテンツの複写防止はコンテンツの保護の観点で用いるものである。

ヘッドマウントディスプレイ４５３Ａを用いる際は眼鏡型でもよく、両眼型、単眼型、非透過型、透過型の眼鏡もしくはゴーグル型装置でよい。仮想現実ＶＲ、拡張現実ＡＲを実現する際のＯＴＰ認証システムに用いてもよい。

またユーザーにコンテンツを利用させる際にそのコンテンツが擬似乱数を用いたいとき、本発明のＯＴＰトークンから計算されるＯＴＰを擬似乱数を実現する値に利用してもよい。例えばオンラインゲーム及びオフライン傾向（ブロックチェーンだけはオンラインだがゲームとしてはオフライン）のゲームにおいてゲーム内で何かのイベントが起きるときに擬似乱数を用いたいときに本発明のＢｎＴＯＴＰ型のＯＴＰ認証コードを用いてもよい。ＯＴＰを疑似ランダム用途に利用する場合はＯＴＰ認証に用いるよりも少ない桁数の値、例えば本来１０桁のＯＴＰであるときその下５桁の数字を用いて疑似ランダム値の生成に用いるなどを行うと好ましい。

【０４４４】

またＳ１６８においてデータが権利者の存在する書籍や雑誌などのコンテンツではなく暗号化した機密文章をある団体のユーザー間で共有したい場合があるかもしれない。ある１つの書類を示した暗号化データはユーザー間で各々書き換えを行い電子署名を付与して変更されていくかもしれない。

そこで、入力装置４４Ａを用いて平文データの書き換えを行い端末４Ａの秘密鍵４０１Ａで平文データの変更前後のデータのハッシュ値等を求め、ある時刻またはあるブロック番号Ｂｎにデータを変更・追記・改ざん・訂正したことをタイムスタンプやＨＭＡＣ等ＭＡＣあるいは電子証明書を用いた電子署名を行って記録し（電子署名用の秘密鍵は４０１Ａでもよいし社員証や個人番号カードに記録されたものでもよい）、データ変更後の電子署名追加済み平文データとしてユーザー端末４ＡのＯＴＰトークンを用いＣＴＡＵ（４０

３１Ａ）とＡＫＴＢ（４０３２Ａ）とＣＲＫＹ（４０３０Ａ）から前記データ変更後の電子署名追加済み平文データを鍵情報ＴＴＫＹ（４０３３Ａ）で暗号化した暗号化データとして、機密文章を送付したいユーザー（そのユーザーは送付元のユーザーと同じく暗号化と復号ができるＯＴＰトークンを保有する）に送付することもできる。そして２人以上のユーザー間である書類のファイルを書き足し又は変更される毎に書き足しや変更を行ったユーザーのＨＭＡＣのＭＡＣ値や電子署名が付与され暗号化されることをユーザー間で繰り返して行い暗号化されたデータとして保管しつつデータの変更を行った際には署名やタイムスタンプを記入できる。

前記の手続きのシークエンスは図７ＣＢと図７ＣＣを組み合わせたものである。ユーザーＵＡとユーザーＵＣがある団体に所属し機密文章をＨＭＡＣのＭＡＣ値や電子署名などを用いて相互に暗号化とデータ変更と復号と暗号化を繰り返しながらデータを作成し閲覧できる。この処理を行う業務用のソフトウェアＣＲＨＮ（４０３Ａ）は書籍や音楽動画といった権利者の存在する作品を復号して読み取りのみできる版とは異なる版である事が好ましいかもしれない。

【０４４５】

通常の紙の雑誌や新聞や本、教科書では購入したそれらにユーザーが筆記用具でメモなどを書くことがある。本発明が教育分野で利用される場合には教科書などにタッチセンサや電子的なタッチペンやマーカーで書き込むことができると好ましいかもしれない。音声音楽はレコード盤や光学ディスク、動画は映画フィルムや磁気テープや光学ディスクといった形で販売されそれらにユーザーが筆記用具などで書き込むことはあまりないが、書籍に関してはユーザーが筆記用具に書き込みメモや学習のために利用するというケースがある。

そこで本発明ではＳ１６８において、書籍データに対しタッチペンやペンタブレットといったペン型のポインティングデバイスと、タッチ型の指でなぞる形式のポインティングデバイスに対応し、４０３Ａで教科書などのデータを閲覧している際にペンで平文データを加工し、秘密鍵４０１Ａで加工した差分のデータに電子署名を付与して保存してもよい。または教科書そのものがすべて画像データで構成されていた場合には該当する頁の画像データにポインテイングデバイスで任意の色情報や画像的な効果の情報を付与し、その結果形成された新たな平文データを暗号化し保存できる。この手順も図７ＣＢと図７ＣＣを組み合わせて実現できる。

紙の教科書と比べＯＴＰトークン化した教科書のデータとすることで保存場所が少なくてよく（端末４Ａと秘密鍵さえ忘れなければよく）教科書への手書きの書き込み保存機能をＯＴＰトークンと同時に利用することで実現する。ユーザーがメモなどを書き込んだ教科書の暗号化データが紛失したり書き込みが増えすぎて見れなくなった場合には再度教科書の原本の暗号化データを入手して利用できる。書籍に書き込む事ができる用途のソフトウェアＣＲＨＮ（４０３）は音楽や動画といった権利者の存在する作品を復号い閲覧や視聴のみできる版（バージョンまたはソフトウェアの名称）とは異なる事が好ましいかもしれない。

紙の教科書は場所を取るために処分されてしまうこともあるが電子化された教科書であればデジタル装置に記憶でき成人後に教科書を読み直すことも容易である。

【０４４６】

Ｓ１６９においてコンテンツに内蔵されたＵＲＩに対応する広告等サーバ５Ａ（ＳＶＣＲＨＮｃｍ）に接続させることができる。これはソフトウェアＣＲＨＮ（４０３Ａ）に内蔵されたプログラムが、 Ｓ１６８にてＳ１６７で４０３４Ａを復号して端末４Ａの記憶装置に得られた平文データ４０３５Ａにおいて広告を表示させることのできる制御文が存在し、前記制御文に従って４０３Ａはサーバ５Ａに接続できるＵＲＩが記載されている場合にそのＵＲＩの接続先から広告の配信を受ける。ここでＵＲＩはコンテンツのレーティングに適したものであることが必要である。

広告機能が付与されていなくともよく、教科書などではこのような広告用ＵＲＩや広告に誘導するプログラムは記録されていないかもしれない。

Ｓ１６９において端末４Ａのユーザー識別子、保有しているトークン番号、ＩＰアドレスや位置情報、端末のＩＤやセンサ値などから図６Ｘのようにアクセスの監視を行い不正アクセスの有無を調べることもできる。広告は表示させずに広告表示サーバにアクセスさせ、アクセス情報のみサーバ５Ａに記録させることもできる。プライバシー保護のために５Ａまたは５Ａに準ずる広告配信サーバ端末にアクセスを行わないようにすることもできる。

Ｓ１６９ではサーバ５Ａに接続させる形で広告の配信を行わせることもできるし、広告主がアクセス管理だけはサーバ５Ａで行い、本来の広告は平文データの内部に言葉や絵図、動画や音声の形で記録させる形でもよい。またプライバシー保護のために広告の配信とアクセス管理をサーバ５Ａに行わせず、広告を文章や画像データとして平文データの中に記録させる形でもよい。（この場合、紙の雑誌などと同じく固定された広告の情報は後世に残ることが期待できる。）

【０４４７】

Ｓ１７０では閲覧済みの証明書データＯＦＢＫＭＫ（４０３６Ａ）を作成する。これはユーザーが暗号データを復号したときにソフトウェア４０３Ａにて行われる。Ｓ１７０Ａで証明書データ（４０３６Ａ）はＴＴＫＹ（４０３３Ａ）を暗号化もしくは難読化し、なおかつＯＴＰ認証を行い閲覧を開始した日付と時刻をタイムスタンプ情報として記録させ、難読もしくは暗号化された４０３３Ａとタイムスタンプの連結データに電子署名して改ざんの有無を検知出るようにしたものである。

何らかの形で４０３３Ａを難読化・暗号化し端末４Ａのユーザーからは復号されない（復号が困難な）鍵情報４０３６０Ａとする。ＯＴＰ認証時の時刻データ及びユーザー識別子等情報（４０３６２Ａ）と４０３６０Ａのデータを連結させ1つのメッセージとし、そのメッセージに対し端末４Ａの秘密鍵４０１Ａまたは秘密鍵ＣＲＫＹ（４０３０２Ａ）をキーとしたＨＭＡＣ（Hash-based Message Authentication Code、ハッシュ関数を用いた符号メッセージ認証、メッセージ符号認証）を用いてＨＭＡＣ値を算出し認証情報（４０３６３Ａ）とする。そして４０３６０Ａと４０３６２Ａと４０３６３Ａを連結し閲覧済み証明書データＯＦＢＫＭＫ（４０３６Ａ）とする

【０４４８】

Ｓ１７０では閲覧済みの証明書データＯＦＢＫＭＫ（４０３６Ａ）はネットワークから端末４Ａが切断されオフライン時にブロックチェーンが使えない場合、すなわちＣＴＡＵ値（４０３１Ａ）が入手できない場合において認証を可能とする機能である。閲覧済みの証明書データＯＦＢＫＭＫ（４０３６Ａ）には暗号データを復号するＴＴＫＹ（４０３３Ａ）の情報が含まれる。

４０３６Ａに４０３３Ａを記載してしまう事もできるが、その場合は４０３３Ａが漏洩すると配布された暗号化されたデータの暗号が無意味になってしまうので何らかの形で暗号化・難読化を施す必要がある。ソフトウェアＣＲＨＮ（４０３Ａ）のプログラムに内蔵された秘密鍵ＣＲＫＹ（４０３０２Ａ）のみを用い４０３３Ａを暗号化することも可能であるが、その場合は同じ４０３Ａを利用するユーザー間であるユーザーが閲覧した後の証明書データを配布しそれを異なるユーザーが端末に取り込み４０３Ａに暗号化データとともに読み込ませれば閲覧できる恐れがある。（ただしこの場合では４０３Ａが出力した４０３６Ａに記載のユーザー識別子と異なるユーザー識別子を生じる秘密鍵（ここでは仮に１０１Ｂ）であったとき４０３Ａはそれを検知して閲覧を実行させないこともできる。）

そこで４０３３Ａを端末４Ａの秘密鍵４０１Ａ（４０１Ａには端末４Ａの様々な有価なＯＴＰトークンが割り当てられている）を用いて暗号化しＣＴＴＫＹ（４０３６１Ａ）とする。続いてＣＴＴＫＹ（４０３６１Ａ）をソフトエアＣＲＨＮ（４０３Ａ）の秘密鍵（４０３０２Ａ）を用いて暗号化しＡＣＴＴＫＹ（４０３６０Ａ）とした。

秘密鍵４０１Ａの流出時や秘密鍵の不正な使いまわしは端末４Ａ等のユーザー端末が広告サーバ５Ａにアクセスした際に図６Ｘのような不正アクセス検知機構により検知される。

【０４４９】

なおここでは実施例であって、本発明では４０３６Ａは４０３３Ａの情報と閲覧したユ

ーザー識別子とユーザーが閲覧した時刻とそれらをメッセージをＨＭＡＣを用いて算出したＭＡＣ値を含むデータである。４０３６Ａは内部情報の改ざんを検知できるＨＭＡＣから計算されるＭＡＣ値を備えている。改ざん検知をさせる情報（４０３６３Ａ）には共通鍵やハッシュ関数に基づくＨＭＡＣではなく公開鍵暗号を用いた電子署名（デジタル署名）であってもよい。ただし本発明の実施例では４０３６Ａの改ざん検知ができれば良いのでＨＭＡＣを用いた。

【０４５０】

実施例３ではＴＴＫＹ（４０３３Ａ）を難読化もしくは暗号化し鍵情報４０３６０Ａにする方法として、４０３３Ａを端末４Ａの秘密鍵４０１Ａで暗号化した後ソフトウェアＣＲＨＮ（４０３Ａ）の秘密鍵ＣＲＫＹ（４０３０２Ａ）で暗号化させ、端末４Ａの秘密鍵４０１Ａとソフトウェアの秘密鍵４０３０２Ａが揃う場合でなければＴＴＫＹ（４０３３Ａ）を得て暗号データが復号できないようにした。

処理の方法としては、ＴＴＫＹ（４０３３Ａ）を秘密鍵４０１Ａを鍵に用いて共通鍵暗号化してＣＴＴＫＹ（４０３６１Ａ）を得る。（ここで共通鍵暗号化のほかに公開鍵暗号化も利用可能と思われるが、証明書データＯＦＢＫＭＫ（４０３６Ａ）はオフライン時の閲覧用データであり他者に送付・通知・共有・譲渡をさせるものではないので共通鍵暗号化を利用した。暗号化の手段は共通鍵暗号化や公開鍵暗号化に限らず暗号化／平文化できる鍵ＴＴＫＹ（４０３３Ａ）を暗号化もしくは難読化させそれを復号し再度ＴＴＫＹ（４０３３Ａ）として取得出来る方法であれば構わない。）

そしてＣＴＴＫＹ（４０３６１Ａ）をソフトウェアＣＲＨＮ（４０３Ａ）のプログラムに内蔵された秘密鍵ＣＲＫＹ（４０３０２Ａ）を鍵に用いて暗号化しＡＣＴＴＫＹ（４０３６０Ａ）として、ＡＣＴＴＫＹにブロック番号Ｂｎや端末の時刻とユーザー識別子やトークン番号とトークンおコントラクト識別子と暗号データおよびＯＴＰトークンの名称をまとめたデータとして、そのデータに秘密鍵４０１ＡとＨＭＡＣを利用し電子署名を行い証明書データＯＦＢＫＭＫ（４０３６Ａ）を作成する。ＨＭＡＣのハッシュ関数は例えばＳＨＡ－２のＳＨＡ２５６を利用できる。

【０４５１】

＜不正利用の対応＞

本発明の実施例１、実施例２、実施例３において共通している事として、秘密鍵４０１Ａが攻撃者により複製され漏洩してしまったときに悪意を持ったほかのユーザー端末に配布される恐れはある。もし悪意を持って流通された４０１Ａをほかの端末で利用した場合に、平文データのコンテンツ内に広告が設置されておりインターネットワークに接続されている場合にはサーバＳＶＣＲＨＮｃｍにＩＰアドレスや端末装置のシリアル番号、端末の入力装置４４Ａの入力センサ４４４Ａの情報が規約で同意されている場合はサーバ５Ａに通知されサーバ５Ａに図６Ｘに示すユーザー識別子とＯＴＰトークンのトークン番号とＩＰＶに収集され記憶され不正アクセスの有無の監視と通知を行う。実施例１では端末３Ｃ、実施例２では端末３Ｄ、実施例３では端末５Ａにアクセスする端末に対し図６Ｘに示すユーザー識別子とＯＴＰトークンのトークン番号とＩＰＶに収集され記憶される。

もしオフラインの場合はＧＮＳＳやＪＪＹ、ＮＩＴＺといった時刻情報を受信できる場合には、４０３６Ａに記載の時刻情報と照らし合わせて閲覧可能な時間を設定して表示する。

また４０３６Ａで復号せず、ネットワークにて悪意を持って４０１Ａを他のユーザーと共有し、多くの人が同じ秘密鍵に不正アクセスしてある書籍を読んでいる場合には、ソフトウェアＣＲＨＮ（４０３Ａ）や書籍のデータに埋め込まれた広告サイトへのＵＲＩを経由し端末５Ａに図６Ｘのような不正アクセスが多く（同一時刻に２人ではなく10人、100人など明らかに異常な件数で）記録されうる。

サービスの提供者の判断によるが、敢えてＩＰアドレスなどをハッシュ化しない様に規約を設定しＩＰアドレスを記録し図６Ｘのようなアクセスの監視を端末５Ａで行うことを規約に明記してＯＴＰトークンの販売を行うようにするとこれらの不正アクセス防止に役立つかもしれない。（発明者は４０３Ａやその復号したデータを利用する際に同一の秘密

鍵を用いて異なる端末での同一時刻でのアクセスによる利用は不正アクセスであると判断する。）

サービス提供者がこのような４０１Ａを共有した形での不正アクセスを許容するかどうかによるが、販売されるコンテンツであれば利用規約で秘密鍵の共有や売買は禁止するべきである。また秘密鍵をサービスのアカウントと見たとき名義貸しなどになりうるので通常は秘密鍵の使い回しは許可されない。本発明の秘密鍵は銀行のインターネットバンキングのＯＴＰトークンにも用いることが考えられ、その用途で利用する場合にはＯＴＰトークンの秘密鍵の共有・売買・名義貸しは利用規約の違反と共にマネーロンダリングなどに利用される恐れが生じかねず、法によって秘密鍵の不正利用が制限されうる。

秘密鍵の管理の視点では個人番号カードなどの秘密鍵を抜き出せないＩＣカード４６Ａ（ＮＦＣタグ４６Ａ）に記録させそれと端末４Ａを端子を経由した有線接続やＮＦＣなどで無線接続し、ＩＣカード経由でブロックチェーン上のコントラクトにアクセスさせるのが好ましいかもしれない。その場合はＩＣカード内の秘密鍵を管理する団体が必要になる。ＩＣカードの内部の秘密鍵情報をＩＣカード製造発行団体のあるデータベースに控えた上で、ＩＣカードの秘密鍵にアクセスできないように装置の設定を変更することが必要である。

【０４５２】

＜トークンの除去とトークンの保管振替＞

本発明ではＥＲＣ７２１規格に実施例１から3に示したＯＴＰ生成認証機能をもつＯＴＰトークンのコントラクトを用いている。ＥＲＣ７２１規格によればあるコントラクトの管理者の端末１Ｃがコントラクトにアクセスしトークン番号を除去する除去関数をコントラクトに備えることができる。このトークン除去関数と発行関数と譲渡制限機能を組み合わせることでＯＴＰトークンの保管振替操作がコントラクト管理者１Ｃから行える。この場合もユーザ端末４Ａの秘密鍵４０１Ａを用いユーザーがＯＴＰトークンを利用することが可能である。

譲渡制限機能と除去関数によりユーザーが秘密鍵を紛失したり不正に秘密鍵を他者と共有し、不正なアクセスが発生している場合はＯＴＰトークンを端末４Ａの秘密鍵４０１Ａ（及びその秘密鍵から計算されるユーザー識別子）から除去し、端末４Ａが別途指定するほかの秘密鍵のユーザー識別子に発行することで振り替えることが可能である。

それでも不正なアクセスが止まらない場合はトークンを除去することも考えられる。これはＯＴＰトークンの利用規約にトークンの除去関数の存在の明記や保管振替ができることを明記する必要がある。

保管振替操作が可能になるとユーザーが秘密鍵を紛失しまたは流出した際に異なる秘密鍵にＯＴＰトークンをコントラクトの管理者が振り替えることができる。そしてユーザーがＯＴＰトークンを誰かに譲渡したり相続する場合にその振替をコントラクトの管理者に依頼することで行える。もし振替機能が無い場合は秘密鍵が分からない場合ＯＴＰトークンの送信ができず、家族・親族間での相続はできなくなる。

他方、ＯＴＰトークンのコントラクト管理者はコントラクトに帰属するすべてのトークン番号のトークンについて発行と除去、保管振替ができるようになる。ユーザーの家族の依頼を受けコントラクト管理者が端末１Ｃで保管振替を行い相続ができるが、端末１Ｃに権限が集中するためコントラクト管理者の責任が大きくなる。顧客のトークンの除去関数を行う場合は利用規約などに記載してトークンの購入を提案するとともに顧客のＯＴＰトークンをカストディできるよう法令を遵守し外部から監査される必要があるかもしれない。また倉庫業や信託や銀行業、金融業や情報通信産業などにかかわる資格を取得した業者が管理することが好ましいかもしれない。

【０４５３】

ここで相続について触れたのはＯＴＰトークンが例えば高価もしくは親族にとってかけがえのない文章や書籍や音楽動画のデータであってそれを家族に相続させたいまたは家族の誰かが相続したいという問題が生じたときにそれに対しトークンの振り替えを行うには法人などの団体が端末１Ｃを操作し保管振替をするのが適しているかもしれないからであ

る。紙の書類は１００年を超えて存在し得るが本発明のＯＴＰトークンやブロックチェーンなどの分散型台帳システムと暗号化データや秘密鍵と暗号化データを復号するソフトウェアＣＲＨＮ、そしてそれらを動作させるデジタル機器の端末を用いて１００年以上にわたり運用する場合、人間の寿命を考慮して個人や法人がもつデジタル資産としてのＯＴＰトークンを考えた場合ＯＴＰトークンの相続について触れる必要があったためである。

【０４５４】

Ｓ１７１ではコントラクト管理者が端末１Ｃを用いてコントラクトのＫＣ値やＢＣ値といったＯＴＰを計算するシークレット値（シード値）を更新できる。実施例３では端末４Ａは本発明のＯＴＰ認証時にインターネットワークに接続されＢｎＴＯＴＰもしくはＯＷＰは常に最新のシード値を用いて認証が行える。またＯＴＰトークンの名前や連絡先などを記載した看板情報ＫＮＢＮ（３０２４Ａ）も書換えることができる。その利用例として、ＯＴＰトークンがある書籍のトークンであって、その書籍を出版する出版社が合併した際には存続会社の連絡先などをトークンのコントラクトに記載することができる。
実施例３ではＢｎＴＯＴＰのほかにＯＷＰを用いてもよい。

【０４５５】

＜ネットワークから切断された場合の暗号化されたデータの復号＞

紙の書籍はネットワーク２０の存在に頼らず読むことができる。コンピュータやサーバーなど電子計算機の端末に保存された書籍データは装置を動かす電源があれば、内蔵した機器の記憶装置に記録されたデータに従い情報を入出力装置に出力させそれが本の情報であれば読むことができる。ネットワーク２０の存在を前提としてネットワーク２０経由で書籍データを閲覧する場合はそのデータが端末に保存され読めるようになっていない場合は読むことができない。

本発明では災害などでネットワーク２０から切断された端末４Ａにおいて、端末４Ａに記録されたＯＴＰ認証を行って暗号化データを閲覧した時（シークエンスＳ１７０の時）に作成される証明書データＯＦＢＫＭＫ（４０３６Ａ）を利用し閲覧可能な制限時間内であれば閲覧できる方式を用いて書籍や動画・音声・ソフトウェアが閲覧利用できるようにした。図７ＣＣにネットワーク２０から端末４Ａが切断されたオフラインのときに暗号化コンテンツの閲覧を行うシークエンス図を示す。

本発明では実施例３において図７ＣＣに示すようにネットワーク２０に接続されていない端末４Ａにて暗号化データを復号して閲覧・視聴・利用するシークエンス実施できるが、証明書データ４０３６Ａに暗号化データの復号に用いるＴＴＫＹ（４０３３Ａ）が平文または難読化・暗号化された状態で含まれており、またＯＴＰ認証した際のブロック番号や時刻情報とユーザー識別子を記録した閲覧時刻と閲覧ユーザー識別子等情報４０３６２Ａを含み、４０３６Ａと４０３６２Ａを連結したメッセージデータとしたとき、メッセージデータをＨＭＡＣにてＭＡＣ値（４０３６３Ａ）を算出し４０３６Ａと４０３６２Ａと４０３６３Ａを連結して４０３６Ａとする事を利用した。

４０３６Ａに必要な情報は暗号化データの復号に用いるＴＴＫＹ（４０３３Ａ）の算出に結びつく情報と、ネットワーク２０に接続していた際に図７ＣＡのＳ１５６からＳ１７０においてＯＴＰ認証を行いＴＴＫＹ（４０３３Ａ）を算出し暗号化データを閲覧できた時の時刻等タイムスタンプ情報４０３６２Ａを結合し、端末４Ａの秘密鍵４０１ＡやソフトウェアｃＲＨＮ（４０３Ａ）に内蔵された秘密鍵（４０３０２Ａ）または４０３０２Ａ以外のソフトウェア内部変数を基にＨＭＡＣにて算出したＭＡＣ値（４０３６３Ａ）があれば本発明の証明書データを構成できる。

【０４５６】

＜暗号化データ４０３４Ａを用いず代わりに平文データを難読化・暗号化したソフトウェア４０３Ａの内部に持つ場合＞

実施例３の別の４０３６Ａの実施形態として図４Ｃに記載の端末４Ａのソースコードが難読化・暗号化されたソフトウェア４０３Ａの内部の４０３０Ａに平文データ４０３５Ａが内蔵されている実施例が実施できる。（４０３Ａの暗号化もしくは難読化したプログラムのソースコード４０３０Ａにソフトウェア用の秘密鍵４０３０２Ａと共に平文データ４

０３５Ａを組み込む場合である）。
この場合にはソフトウェア４０３Ａの秘密鍵４０３０２Ａとユーザー用秘密鍵４０１Ａがある時、ソフトウェア４０３Ａの４０３０Ａにあるシークレット変数Ｋ４０３（４０３０３ＫＡ）を用いて
４０１Ａから計算できるユーザー識別子Ａの情報とＯＴＰ認証時の時刻情報Ｔ４０３とＫ４０３を連結させた情報のハッシュ値ＨＴ４０３を求め、前記ハッシュ値ＨＴＫ４０３と可読可能なユーザー識別子Ａや認証時タイムスタンプ情報Ｔ４０３を含む証明書を構成する情報を連結し、証明書の本文データＣＨＴ４０３（４０３６２ＫＡ）として４０３６２ＫＡをメッセージとしユーザ秘密鍵４０１Ａをキーにして ＨＭＡＣによりＭＡＣ値４０３６３ＫＡを求め、４０３６２ＫＡとＭＡＣ値４０３６３Ａを連結し証明書データＯＦＢＫＭＫ（４０３６Ａ）としてもよい。

【０４５７】
前記の４０３６２ＫＡをメッセージとしユーザ秘密鍵４０１Ａをキーにして ＨＭＡＣによりＭＡＣ値４０３６３ＫＡを求め、４０３６２ＫＡとＭＡＣ値４０３６３Ａを連結し証明書データＯＦＢＫＭＫ（４０３６Ａ）とする場合、ＯＴＰ認証関数の戻り値ＣＴＡＵは単一の真偽値のみの戻り値でもよいし、2つ以上の戻り値を持ちその中に４０３Ａがユーザーに閲覧を許可する判定式の条件文に用いる変数を持っていてもよい。ＣＴＡＵが単一の真偽値だけでもよい理由は、ソフトウェア４０３の内部データが平文データを含めて暗号化もしくは難読化されておりプログラム実行時にブロックチェーン上のコントラクトにおいてＯＴＰ認証が行えたかどうかの真か偽かの真偽値を４０３Ａが確認し、もし真の値を返して認証できた場合にはＳ１７０の証明書データ４０３６Ａを４０３０３ＫＡとユーザーの秘密鍵４０１Ａを用いて算出出来るためである。

【０４５８】
ユーザー秘密鍵４０１Ａと証明書データ４０３６Ａをオフライン下で４０３Ａは読み込み、４０３６Ａに記述されたＭＡＣ値４０３６３Ａから４０３６Ａの改ざんが行われていないか４０１Ａを用いて確認し、４０３６Ａが改ざんされていない場合にはＣＨＴ４０３のＨＴＫ４０３の値をソフトウェア４０３は読み取り、ソフトウェア内部で計算される４０１Ａから計算できるユーザー識別子Ａの情報とＯＴＰ認証時の時刻情報とＫ４０３を連結させた情報のハッシュ値ＨＴ４０３と一致するか計算して検証し、４０３６Ａの情報と４０３Ａで計算される情報が一致した場合はプログラムに内蔵された平文データをユーザ端末４Ａの入出力装置を通じて閲覧視聴利用させる。一致しない場合は平文データを利用させない。

【０４５９】
ここで秘密鍵４０１Ａを共通鍵としてＨＭＡＣを用いた方式について述べたが、４０１Ａを公開鍵暗号の鍵に用いて電子署名（デジタル署名）により証明書を作成する方式も考えられる。ただし４０３６Ａは他者に送付することを意図しないデータであるのでＨＭＡＣを好ましくは利用した。オンライン時においてＯＴＰトークンを割り当てられた秘密鍵４０１Ａをキーとして ＨＭＡＣとソフトウェア内部のシークレット変数（Ｋ４０３）と認証時刻を用い認証証明データを作成し、オフライン時に読込してソフトウェア内のファイル閲覧可能とする。

【０４６０】
ソフトウェア４０３ＡはＨＭＡＣにより改ざん検知できる証明書の認証時刻データと端末４Ａの現在時刻からユーザーが連続して閲覧可能な時間を計算しその時間の間に入出力装置を通じて端末４Ａのユーザーにデータを閲覧・視聴・利用させる。認証時刻がより過去の時間となり、古い証明書データ（４０３６Ａ）であるほど、連続して閲覧可能な時間が短くなる。そしてユーザーは閲覧時間が短くなるために再度４０３Ａを起動しては４０３Ａが制限時間を超えたことを検知し終了してを繰り返しソフトウェア４０３を頻繁に再実行しなければいけなくなる。これを解消するにはオンライン時にブロックチェーンシステムを構成する３Ａにアクセスし、本発明の閲覧したい平文データに対応したＯＴＰトークンの割り当てられた秘密鍵４０１Ａを用いてＯＴＰ認証を再び行って平文データを閲覧

し新しい証明書データ（４０３６Ａ）を発行することができればよい。
【０４６１】
平文データをソフトウェア上で連続して閲覧可能な時刻の設定権限はデータの権利者にある。データの権利者はコンテンツのレイティングやそのデータが災害など非常事態においてどのように使われるかを考慮して閲覧可能な時間を設定することができる。
またデータの権利者が許可する場合にはオフラインにて４０３６Ａを用いてコンテンツを利用する際に制限時間を設定しないことも可能である。
【０４６２】
実施例３の用途ではオフライン時に端末４Ａの時間情報に基づいて時刻が計算される。端末４Ａの制御処理装置４１Ａに含まれるリアルタイムクロック（ＲＴＣ）の機能に従い、４Ａの電源装置４７Ａ（ＲＴＣ部を動かすことの出来る電池を含む）を用いオフラインの４Ａにおいても時刻情報を保持し続けることができるが、ＢＩＯＳで書き換えられてしまう恐れがある。（ここでＲＴＣは水晶振動子や発信回路などのＩＣで構成された時計機能を提供できる部品。）
本発明では好ましくはＢＩＯＳ等端末４Ａを制御するソフトウェアで端末の時間が書き換えられないようにすることや、端末４Ａに時刻情報を受信する装置がありＧＮＳＳやＪＪＹ、ＮＩＴＺといった情報源から正しいと思われる時刻情報を取得し、端末４Ａの時刻を国際原子時（ＴＡＩ）や協定世界時（ＵＴＣ）に近い値に設定できると好ましい。端末４Ａのハードウェア的な時刻情報の改ざんが可能であるときはソフトウェア４０３Ａは誤った時刻、あるいは悪意を持って設定された時刻に従うほかなく、４０３６Ａを用いた閲覧を出来る時間を制限する仕組みは成り立たなくなる。
【０４６３】
証明書データＯＦＢＫＭＫ（４０３６Ａ）の要件は本発明のＯＴＰ認証システムで認証しデータを閲覧したときの時刻情報４０３６２Ａと前記情報の改ざんが行われていないか検証するためのＭＡＣ値４０３６３Ａである。暗号化データ４０３４Ａがソフトウェア４０３Ａの外部にある場合は暗号化データを復号する鍵ＴＴＫＹ（４０３３Ａ）を計算するための情報４０３６０Ａや４０３６１Ａ等が必要になる。ＯＦＢＫＭＫ（４０３６Ａ）はユーザー秘密鍵４０１Ａに応じて発行される。同一のコンテンツでも秘密鍵が異なるときは異なった４０３６Ａが発行される。またさらにトークン番号が違う場合にも異なった４０３６Ａが発行される。
暗号化データ４０３４Ａがソフトウェア４０３Ａの内部にあり暗号化されているとき、つまり４０３０Ａの内部にあるソフトウェアの秘密鍵ＣＲＫＹ（４０３０２Ａ）のように難読化もしくは暗号化されている場合は平文データがプログラムのソースコードと共に暗号化されておりＴＴＫＹ（４０３３Ａ）が必要ないので、暗号化データを復号する鍵ＴＴＫＹ（４０３３Ａ）を計算するための情報４０３６０Ａや４０３６１Ａ等は不要である。ソフトウェア４０３Ａを実行し、ユーザーが秘密鍵４０１Ａと証明書データＯＦＢＫＭＫ（４０３６Ａ）を４０３Ａに読み込ませ、閲覧を希望すればオフラインであっても４０３Ａはソフトウェア内部の平文データを閲覧させることができる。
本発明では暗号化データ４０３４Ａを読み込むソフトウェア４０３Ａの版と平文データを内蔵したソフトウェア４０３Ａのどちらも４０３６Ａを作成でき、またそれらに対応するＯＴＰトークンを用い認証を行い暗号化データの復号を行える。
【０４６４】
図７ＣＣにネットワークに接続されていない場合において図４Ｂの構成の端末４Ａで秘密鍵４０１Ａと暗号化データ４０３４Ａとソフトウェア ＣＲＨＮ４０３Ａと証明書データ４０３６Ａを用いて暗号化データを復号する場合を示す。シークエンスＳ２００では図４Ｂの構成の端末４Ａで秘密鍵４０１Ａと暗号化データ４０３４Ａとソフトウェア ＣＲＨＮ４０３Ａと証明書データ４０３６Ａを用意する。
【０４６５】
Ｓ２０１ではソフトウェア４０３Ａを実行し起動させ、少なくとも秘密鍵４０１Ａと暗号化データ４０３４Ａを読み込ませ（あるいは４０１Ａと４０３４Ａのあるファイルのディ

レクトリとファイル名を指定し、あるいはファイルを示すＵＲＩを指定し）、他に設定入力が必要な場合は入力を行う。

【０４６６】

Ｓ２０２では証明書データ４０３６Ａを読み込ませる。この時４０３６Ａが改ざんされていないか調べるため、４０３６ＡのＭＡＣ値を秘密鍵を用いて検証する。

【０４６７】

Ｓ２０３では４０３６ＡのＡＣＴＴＫＹ４０３６０ＡをＣＲＫＹ４０３０２Ａ等にて復号しＣＴＴＫＹ４０３６１Ａを得る。

ＣＴＴＫＹ４０３６１Ａを端末４Ａの秘密鍵を用いて復号しＴＴＫＹ４０３３Ａを生成する。

【０４６８】

Ｓ２０４ではＴＴＫＹ４０３３Ａにて暗号化データ４０３４Ａを復号し平文データ４０３５Ａを得る。

【０４６９】

Ｓ２０５ではソフトウェアＣＲＨＮ４０３Ａのプログラムに従い、証明書データ４０３６に含まれる４０３６３Ａから証明書が改ざんされていないことを確認し、４０３６Ａに含まれるＯＴＰ認証時及び平文でたーの閲覧時刻情報４０３６２Ａの時刻情報を取得し、端末４Ａの時刻情報と４０３６２Ａの時刻情報から閲覧可能な時刻を算出する。

【０４７０】

Ｓ２０６では閲覧可能な時間を現在時刻に加算した時刻になるまでユーザーにデータを閲覧もしくは使用させる（時刻を取得するには端末ＤＡのＧＮＳＳ受信器や、ＮＩＴＺ、ＪＪＹなどの時刻受信機が備え付けられていると好ましい）。ここで閲覧可能な時刻の算出や制御の仕方は平文データの権利者の求めにより代わり、ソフトウェアＣＲＨＮ４０３Ａのプログラムや、平文データ４０３５Ａ内にその処理の仕方や処理に利用する変数が記載されるため具体的な時刻の計算方法や変数値は限定しない。Ｓ２０６では４０３６２Ａの時刻情報と現在時刻を基にしてユーザーが閲覧できる時間を計算して設定し時間が経過したときに４０３Ａの実行を停止することも可能な処理が含まれる。閲覧可能な時間の制限がない場合はそれに合わせて動作させる。

【０４７１】

Ｓ２０７ではＳ２０６で４０３６２Ａの時刻情報と現在時刻を基にしてユーザーが閲覧できる時間を計算した値よりも長い時間がユーザー端末４Ａで経過したときを示す。Ｓ２０８ではＳ２０７に示す時刻になったときソフトウェア４０３Ａは平文データの閲覧視聴利用を停止し、警告などを行った後、ユーザの意志にかかわらず強制的に終了する。

【０４７２】

また図７ＣＣのネットワークに接続されていない場合において、端末４Ａが図４Ｃに示す構成（ソフトウェア４０３Ａの４０３０Ａに平文データ４０３５が内蔵され暗号化もしくは難読化されている場合）ではＳ２０３やＳ２０４のシークエンスを除いたシークエンス図となる。

【０４７３】

実施例３のソフトウェアＣＲＨＮ（４０３Ａ）には、

１．ＥｎｃＤａｔａからＤｅｃＤａｔａへの変換のみができるものＣＲＨＮＲｅａｄｅｒ、

２．ＤｅｃＤａｔａからＥｎｃＤａｔａへの変換をするものＣＲＨＮＷｒｉｔｅｒ、

３．ＤｅｃＤａｔａとＥｎｃＤａｔａの相互変換を行えるものＣＲＨＮＲｅａｄｅｒＷｒｉｔｅｒ

の3種類が考えられる。

ＣＲＨＮＲｅａｄｅｒＷｒｉｔｅｒはある団体の文章を暗号化、復号するために書類等データの変更が行われる毎に文章の暗号化と復号を行う（ここでＥｎｃＤａｔａとして保持し、ユーザーがＥｎｃＤａｔａを復号して変更する際にＤｅｃＤａｔａを記憶装置内に内蔵する）。復号したデータを変更し暗号化して保存する際に書類へのタイムスタンプや

電子署名が可能であり、ブロックチェーンのブロック番号とＢｎＴＯＴＰを固有のシークレットして記入し、書籍データをハッシュ化し書籍をブロックチェーンのように改ざん困難な形で保存させることもできる。（機密文章を管理する用途に向けたソフトウェアである。）

またＣＲＨＮＲｅａｄｅｒＷｒｉｔｅｒのもう一つの形態としては、１次創作物の権利者が許可する場合に限り１次創作物となるコンテンツの暗号化データを復号後にコンテンツの内容の一部に従いつつ変更をして２次的創作物となるコンテンツとして次のＯＴＰトークンの保有者に配布するといったことにも利用できる。この場合はコンテンツの利用権として、１次創作物となるコンテンツのＯＴＰトークンとは異なるコントラクトで発行・配布されるかもしれない。暗号化データが書換えられたのちも広告サーバ５Ａに接続されるＵＲＩの部分を変更出来ないようにＣＲＨＮＲｅａｄｅｒＷｒｉｔｅｒとなる４０３Ａにプログラムをすることで、１次創作者は２次またはｎ時の創作物に埋め込まれたＵＲＩ情報に接続・リンクされたサーバ５Ａの広告により収益を上げることもできる。

ＣＲＨＮＲｅａｄｅｒは暗号化された書籍、音声動画、ソフトウェア等データＥｎｃＤａｔａを復号して得られた平文データＤｅｃＤａｔａを閲覧・再生・起動する。書籍における付箋などの様に原本の平文データとは別に注釈などを記録する機能を備えてもよい。

ＣＲＨＮＷｒｉｔｅｒはＣＲＨＮＲｅａｄｅｒにて復号させる暗号化データＥｎｃＤａｔａを平文データＤｅｃＤａｔａから作成するためのものであり、書籍・音声動画・ソフトウェア等の平文データＤｅｃＤａｔａを暗号化する。

ソフトウェア４０３Ａの種類やバージョンに応じて、ソフトウェアアプリケーション専用の鍵を管理するコントラクトの識別子ＡＰＫＹ４０３０１Ａ、ソフトウェア４０３Ａの秘密鍵４０３０２Ａ、ブロックチェーンから取得した鍵管理コントラクトの戻り値ＣＡＰＫＹ４０３０３Ａ等が設定される。ＡＰＫＹ，ＣＲＫＹ、ＣＡＰＫＹをバージョンや種類の異なるソフトウェア４０３Ａ毎に固有の値として設定することでＣＲＨＮをＣＲＨＮＷｒｉｔｅｒとして動作させるのか、ＣＲＨＮＲｅａｄｅｒＷｒｉｔｅｒとして動作させるのかを切り替える情報として利用できる。また４０３Ａのソフトウェアのバージョンを例として数年ごとに変え、ＡＰＫＹ，ＣＲＫＹ、ＣＡＰＫＹを変えていくことができる。

【０４７４】

＜特殊な版のＣＲＨＮＲｅａｄｅｒＷｒｉｔｅｒによる原本への加筆とｎ次創作＞

ＣＲＨＮＲｅａｄｅｒＷｒｉｔｅｒの形態としては１次創作物となるコンテンツの暗号化データを復号後にコンテンツの内容の一部に従いつつ変更をして２次的創作物となるコンテンツとして次のＯＴＰトークンの保有者に配布することは知的財産権の１つである著作権におおいに関連する。

著作権者がコンテンツのｎ次利用を許可した場合にその許可された広告付きのコンテンツの原本と暗号化データとそれを復号するＯＴＰトークンとその用途のＣＲＨＮＲｅａｄｅｒＷｒｉｔｅｒを販売することができるかもしれない。コンテンツには文章書籍や画像と動画そして音声やゲームソフトウェアとプログラムソースコードが想定される。

例として無料のソフトウェアのプログラムのソースコードをフリーに近いライセンスにてオープンソースコードとしてコラボレーションを許可して配布する場合であっても、配布されたプログラムをコラボレーションして改良した２次創作者が前記の１次創作者のデータに対応した無料のＯＴＰトークンとそこに添付した広告ＵＲＩを２次創作物のプログラムに添付し、添付されたプログラムをエンドユーザーが利用する際に１次創作者と２次創作者の組み込んだ広告のタグに従い端末５Ａの広告配信サイトへ広告を呼び出す等で１次創作者及び２次創作者の双方に広告費が支払われるならばプログラマーの収益改善に寄与できるかもしれない。

＜世界各国の法律の権利によって保護されたものを権利トークン する場合の問題＞

前記のｎ次創作の著作権など知的財産権に関連し、本発明のＯＴＰトークンを株式や不動産所有権や知的財産権や特許権や商標権や著作権の所有権として利用することも考えられるが、本発明はあくまで情報処理を改ざん困難かつＯＴＰ認証などを行って権利の行使を行いやすくする手段であって（認証を自動化する方法であって）、その株式や不動産所

有権や知的財産権がその国の法令によって管理されることに留意すべきであり、各国の行政やＯＴＰトークンの発行体や発行体への監査、会社であれば公認会計士といった専門家、不動産ならば不動産取引法務の専門家や弁理士や弁護士など法で定められた資格を持つ専門家・専門家団体の仲介が分散型台帳システムの外で必要になる。

本発明では権利と対応したＯＴＰトークンの用途については、専門家の立合・監査・監視・判断・承認・証人がないときは法的な権利に関するＯＴＰトークンは紛争の元となったり存在しないもの（法の裏付けのない記録）になる恐れもあり、本発明の利用例で詳細な説明は行わなかった。しかし株式など有価証券では株主総会へのログインや株主投票などを行うウェブサイトへのログイン及び意思表示用のＯＴＰトークンとなること、そして株主がその株式に対応する株式会社のサービスの利用権となりうることから利用例を記載した。

また分散型台帳システムは国境を越えてＯＴＰトークンを発行できてしまう事から、仮に法で守られる権利をＯＴＰトークン化する際はＫＹＣされたユーザーにＯＴＰトークンを発行譲渡する事が好ましい。特許権や著作権など知的財産権を権利化したとき、前記権利を一般市民だけが所有するとは限らない。予期しない団体（テロリストなど）に権利の過半数を掌握されトークンの権利による収益を分配することを迫られるリスクがある。そこでこの場合はＯＴＰトークンに譲渡制限機能とトークン除去関数を用いた保管振替機能を持たせる事が好ましいと考える。

またＯＴＰトークンの売買によるユーザー間での金銭のやり取り又は暗号資産のやり取りを記録し、予期しない団体 への資金供与を抑えるとともに、ＯＴＰトークンなどの分散型台帳システム上のやり取りで生じた税に関する処理を自動で行わせるサーバー端末（端末３Ｅや３Ｆを拡張した物）があると好ましい。

ＯＴＰトークンの流通はＫＹＣされたユーザー間で取引されることが好ましい。

またユーザー識別子が間違って入力されていると本来送付したいユーザーにトークンを送付できないので、入力間違い減らし識別子検索を容易にするためにユーザー識別子をドメイン名とＩＰアドレスの対応づけをするドメインネームシステムと同じように分散型台帳システムでのユーザー識別子やコントラクト識別子などアドレスとドメイン名等のＵＲＬ・ＵＲＩを対応付けてサーバ３Ｆや３Ｅや５Ａや５Ｂ等に記録すると好ましいかもしれない。

＜模写などへの備考＞

ヘッドマウントディスプレイ４５３Ａによる銀塩カメラ・デジタルカメラ等による４５０Ａの複写の防止について述べたが、ヒトの目で見て手で書き残すことができれば記録する事ができる。ヒトの記憶に残る情報であればそれを基に２次創作されうる。完全に模写や模倣を制限することは困難である。２次創作者の記録したことが広まる形でｎ次創作・ｎ次利用も起きうる。

ただし、児童や学生が楽しみや勉強のためにコンテンツから学ぶ形で個人利用の範囲で記憶したことを用いて写し取ることまで禁じることは想定していない。

ＯＴＰトークンの利用例はコンテンツの権利者や法に従う。

【０４７５】

暗号化データを再生できるＣＲＨＮソフトウェアのバージョンでなければ暗号化データは再生できなくなる。これは固定のソフトウェア内部の暗号化を続けるのは攻撃者からソフトウェア内部の鍵が解読された場合にそのソフトウェアで暗号化されたデータの解読につながる恐れがあるため、定期的にソフトウェアＣＲＨＮとそれが含む鍵ＡＰＫＹ，ＣＲＫＹ、ＣＡＰＫＹを変えることで同じＡＰＫＹ，ＣＲＫＹ、ＣＡＰＫＹを利用しないようにするためである。

ほかにソフトウェアＣＲＨＮ（４０３Ａ）の実施できる形態として平文データＥｎｃＤａｔａを４０３０Ａに含め、平文データＥｎｃＤａｔａと４０３０Ａを暗号化ないし難読化したソフトウェアが考えられる。

【０４７６】

＜暗号化ファイルの復号時の注意＞

暗号化ファイル復号時に平文ファイルＤｅｃＤａｔａに悪質なプログラムが含まれることが想定される。
平文ファイルを作成する際に平文ファイルにファイル作成者以外の第三者が発行した電子証明書ＤｅｃＣｅｒｔを付与又は電子署名し、発行者を閲覧者が電子証明書を通じて確認できるようにする。さらに書籍や音声動画コンピュータソフトなどは外部の第三者が平文の監査を行い悪質なコンピュータウイルス等のプログラムが無いことと平文ファイルのコンテンツのレイティングを付与したことを示す監査証明書ＡｕｄｉｔＲａｔを付与することが好ましい。
なお個人や団体の機密文章を暗号化するビジネス用途ではＡｕｄｉｔＲａｔは付与しなくともよい。また顧客が悪質なプログラムが動作されることも許容して利用する場合はＤｅｃＣｅｒｔも利用されない。
暗号化ファイルにＥｎｃＤａｔａにそのデータのハッシュ値と内容を保証するＥｎｃＣｅｒｔを付与することもできる。
【０４７７】
＜暗号化ファイルの復号時の環境＞
現実の端末において仮想的に複数のコンピュータ環境を構築する仮想コンピュータ（仮想機械）技術方式がある。またオペレーティングシステム上に仮想環境を構築し、動作の不明なソフトの実行を監視するサンドボックスという環境がある。本発明のソフトウェアＣＲＨＮ４０３Ａはそのような仮想環境のシステムで構築されることが好ましい場合がある。
これはコンピュータウイルスなどが暗号化されたファイルの平文データに埋め込まれている場合の被害を最小にする手段の一つである。平文を監査する第三者機関の能力・処理量には限りがある可能性があり、本発明においてソフトウェアＣＲＨＮ４０３Ａで様々なデータが無数の個人法人で発行される場合には監査が行き届かず、悪意のあるソフトウェアが組み込まれているにもかかわらず監査証明書が発行される恐れもある。また未知のウイルスプログラムには監査が届かない恐れがあり、仮想的な環境で実行できる事が好ましい。４０３Ａを動作させる仮想環境には必要以上の個人情報や私的ファイルは保管しないことが望ましい。秘密鍵も趣味用の４０３用の物と、業務用の４０３用の物と、重要な金融用途の物に分けるなどすると好ましいかもしれない。
仮想環境を実現するために、ソフトウェアＣＲＨＮ４０３Ａが仮想環境などを構築できるウェブブラウザソフトウェアやウェブブラウザを内包したオペレーティングソフトウェアであってもよいし、ＣＲＨＮがコンピュータのＢＩＯＳに相当する基本ソフトウェア部分を持っていてもよい。
【０４７８】
本発明を実施するにあたり、実施例１や実施例２や実施例３においてブロックサイズがブロックガスリミット値の投票という形で可変になるイーサリアムのテストネットにて行った。またスマートコントラクトはプログラム言語Ｓｏｌｉｄｉｔｙで記述し、ブロックチェーンに記録させ、展開（デプロイ）した。
実施例1においてはスマートコントラクトの作成者であり管理者となるコンピュータ端末１Ｃ（図８Ａまたは図１の端末１Ｃ）とサーバーＰ（図８Ａまたは図１の端末３Ａ）をネットワーク２０（図８Ａまたは図１の２０）を用い、端末３Ａのブロックチェーン制御処理部３１０Ａとブロックチェーン記録部３００Ａ にアクセスしワンタイムパスワード生成及び認証を行うコントラクトをシークレット値ＫＣやコントラクト管理者のみが変更できるＢＣ値を設定し、コンパイルし、バイトコードに変換しブロック番号のブロックデータに記録させ展開させた。
実施例のイーサリアムのテストネットワークでは１５秒ごとに新しいブロックが連結されブロック番号Ｂｎが一つ増加する。ブロック番号Ｂｎは15秒後ごとに変動する、物理量である時間に比例する変数である。
本発明の実施例１では、ブロックチェーン上で時間を表現する変数としてブロック番号を用いた。あるブロック番号Ｂｎにおいてブロック番号がゼロのブロックチェーンが生み出

された状態から何秒経過しているか求めるには、Ｂｎ×１５［ｓｅｃ］として求められる。イーサリアムでは１５秒である必要はなく任意の時間間隔ｔ［ｓｅｃ］を設定してもよいが、今回はテストネットで決定されている15秒を利用して本発明を実施した。

【０４７９】

秘密鍵ＰＲＶＡ（１０１Ａ）はユーザーＵＡの記録装置１０Ａ、１０１Ａに記録される。しかし場合によっては無線ないし有線により端末１Ａと接続される外部記憶装置１６Ａの記録装置ＤＷＡＬＴ１６０３Ａに記録されていもよい。ＤＷＡＬＴ１６０３Ａは接触式ＩＣカード型、非接触式ＩＣカード型、接触式の記憶装置型（ハードウェアウォレット）、非接触式タグ型（ＮＦＣタグ型）でもよい。また紙や板などの記録された秘密鍵ＰＲＶＡ１６０８Ａでもよい。

【０４８０】

コントラクトでは生成トークンのトークン番号に対応付けされたユーザー識別子を調べることができる。前記トークン番号からその番号のトークンを保有するユーザー識別子のを調べ表示する機能を利用しブロックチェーン上でのコントラクトの全てのトランザクションデータに加え、いわゆる株主名簿のようなユーザーＵＡやＵＣがトークンの持ち主となるユーザー識別子の名簿を作り保存し、ブロック番号やユーザのＢｎＴＯＴＰなどを含ませる形で紙などに印刷し、または記録装置に保存することができる。トークンが書籍データを閲覧させるサービスであった場合には書籍の保持者の識別子と書籍のトークン番号（書籍のシリアル番号）を（これはブロックチェーンが万一世界中で利用できない場合でもトークンの保有者を調べるために利用される紙等の名簿になる）。
発行されたすべてのトークンの保有割合も名簿データから計算できる。これらはサーバーＰなどからサーバ端末３Ｆによりトランザクションデータが収集され集計され日常的に利用されうる。サーバ端末３Ｆを代表として端末３Ｅや端末５Ｂ等は、発行されたすべてのトークンの保有割合も名簿データから計算し記録しユーザーに通帳やトークンの資産残高台帳として通知させる役割を持つ端末となることもできる。

【０４８１】

＜ブロックチェーン検索機能、検索結果のデータベース構築機能＞

サーバ端末３Ｆの記憶部３０Ｆの３０１Ｆにはブロックチェーンに対する検索履歴や検索履歴に対応するブロックチェーン上のデータの対応関係などを３Ｆに記録し、ブロックチェーン上の検索される検索のキー情報と検索結果のブロックチェーンの情報の一部を３Ｆに記録することでデータベースを構築してもよい。

例として多くのユーザーが興味を持つＯＴＰトークンのコントラクト識別子やサービス名の情報とそのトランザクションを記録することでブロックチェーンのノードなる３Ａ等にアクセスが集中することなく３Ｆにて検索のアクセスを受け付けその情報を配信できる。３０１Ｆには３１１Ｆの記憶が書き込まれているとともに３０１Ｆは３１１Ｆにより制御される。

端末３Ｆがサーバ端末３Ａや３Ｂと同じくブロックチェーンのノードの1つとなっていて、ブロックチェーンの全情報を記録したうえで、そのブロックチェーンデータに記録されたコントラクト識別子やユーザー識別子やトランザクションに対し、ユーザー端末からどのような検索によるアクセスが行われているかを分析し、ユーザーに情報をより速く提供できるよう検索結果を保存できる

例えばデータの読み書き速度の速い主記憶装置やソリッドステートドライブ（ＳＳＤ）などに頻度の高いＯＴＰトークンの検索結果とブロックチェーン上のデータを記録して配置し、ハードディスクドライブや磁気テープといった高いデータ容量ではあるがアクセス速度が主記憶装置やＳＳＤよりも低速な記憶装置に頻度の低い検索されたデータのキャッシュを保存することで、ブロックチェーンへの世界中からのユーザーの検索によるアクセス情報を高速に記憶装置を用いて受け付けるとともに検索先の情報を保管できうる。

【０４８２】

＜ブロックチェーン上のデータを検索しＯＴＰトークンの流通に用いる例＞

ブロックチェーン上で需要がある出版社の書籍に関するコンテンツの閲覧権に対応した

本発明のＯＴＰトークンがあり、人々がそのＯＴＰトークンの名前やＯＴＰトークンの発行者（出版社名など）、ＯＴＰトークンの発行総数（書籍の販売総数）、所有しているユーザー識別子の総数（購入したユーザーアカウントの総数）、ＯＴＰトークンの複数所持の有無（それぞれのユーザー識別子につき何個購入されたか）、ＯＴＰトークンは譲渡制限があるかどうか、ＯＴＰトークンの看板情報ＫＮＢＮに記載のレーティング情報や出版社連絡先・ＯＴＰトークンの購入先・暗号化データの配布先などをユーザーが検索し、ユーザーはＯＴＰトークンの流通状況やＯＴＰトークンの購入先の情報を調べ、ＯＴＰトークンを購入するかどうかの判断材料として検索情報を利用できる。

【０４８３】

＜ブロックチェーン上のトランザクション監視機能＞

ほか、ユーザーが３Ｆの提供するサービスについて利用することを契約しユーザー登録をして、個人情報である電子メールアドレス等の連絡先を通知先データベース３０１３Ｆに通知先登録部３１１３Ｆを利用して登録した場合に、ユーザーが指定するコントラクト識別子やユーザ識別子についてトランザクションが発生した場合にはそれを３０１０Ｆと３１１０Ｆが監視し、新しいトランザクションが発生し状態が変化したことを３Ｆはブロックチェーン状態変化通知先データベース３０１３Ｆに登録された通知先となるユーザーの電子メールアドレス又は電話番号またはユーザー識別子に状態変化発生時刻と状態変化の内容を送付し通知する必要がある。

ＯＴＰ生成関数やＯＴＰ認証関数を実行した際にその実行回数をコントラクト内部変数３０１７Ａや３０１７ＡＧや３０１７ＡＡに記録できるとき、コントラクトに記録された３０１７Ａや３０１７ＡＧや３０１７ＡＡの変化を監視するようユーザーはサーバ端末３Ｆへ監視を依頼するコントラクト識別子、コントラクト識別子に対応するコントラクトのＯＴＰトークンのトークン番号、ユーザー識別子などを対応づけて３Ｆの３０１０Ｆに記録させる。

状態変化検出プログラム３０１１Ｆによって動作する状態変化検出部３１１１Ｆが指定したコントラクトの識別子やユーザー識別子のトランザクションの変化を検知し、ユーザーの指定したコントラクトに帰属するＯＴＰトークンのトランザクションやユーザー識別子のトランザクションが新たに生じてブロックチェーンの状態が変化したとき、状態変化検知部３１１１Ｆがブロックチェーンの状態変化を検出し、通知部３１１２Ｆが電子メールアドレスまたは電話番号や電話番号を用いたＳＭＳ（Short Message Service）によりトランザクションが新たに生じたことをユーザー端末を通じてユーザーに通知し、ユーザーに心当たりのあるトランザクションであるか通知する。

もし心当たりのない、ユーザーが操作していないにも関わらずトランザクションが発生している場合はＯＴＰトークンのコントラクト識別子に対応したサービスの提供者に不正利用があったことを伝え、ユーザーとサービス提供者両者にて相談して問題を解決する事が想定される。

３０１７Ａや３０１７ＡＧや３０１７ＡＡはブロックチェーンに記録されている情報であり改ざんが困難である。その情報を新たに変更するトランザクションをブロックチェーンに送付し、ブロックチェーンに連結されると変更や改ざんが困難である。不正に人の秘密鍵４０１Ａや１０１Ａなどを入手し、本発明のＯＴＰトークンにおいて３０１７Ａといった変数が設定されたＯＴＰ生成関数やＯＴＰ認証関数を操作すると、その記録は取り消すことができない。本発明において３Ａなどのブロックチェーンシステムを構成するサーバーに、防犯のためにＩＰアドレスや位置情報、デバイスＩＤといったアクセス情報を検知し記録する機能を機能備えており、またサーバ３Ｆのようにユーザーの意図しない不正利用を検知し通知する機能を組み合わせることで不正利用を試みようとする者の意欲を削ぐことができるかもしれない。

そのためにはサーバ３Ａといったブロックチェーン部にはサーバ３Ａへのアクセス者の情報を記録し、またサーバ３Ｃや広告サーバ５Ａといったサービス提供サーバ部についても図６Ｘのようなアクセス情報の監視機能を備え、なおかつそのアクセスデータを改ざんできないように、３Ａのブロックチェーン型のアクセスデータベースや３Ｃのブロックチ

ェーン型のアクセスデータベースを作り各サーバで保存する事もできるかもしれない。
【０４８４】
＜ブロックチェーンシステムＤＬＳからＯＴＰトークンなどの資産残高を改ざん検知できる証明書の形で配布する機能＞
ほか、ユーザーが３Ｆはブロックチェーン上のユーザー識別子とコントラクト識別子のトランザクションを取りまとめ、ユーザーの名前や住所など個人情報が記入された取引明細書（通帳）やＯＴＰトークンなどＤＬＳ上の資産残高証明書や取引報告書をユーザー識別子やコントラクト識別子を検索キーとして検索し検索結果を取りまとめてタイムスタンプや電子署名やＨＭＡＣなどを用い検索結果をあるタイムスタンプの時刻における残高や取引の明細書として、改ざん検知ができる形でユーザーに配布してもよい。
【０４８５】
＜トークンを未来のあるブロック番号までコントラクトに預けることを約束する機能＞
ＯＴＰトークンにある未来のブロック番号まで（ある未来の期間まで）ＯＴＰトークンを移動しないようにする定期トークン預け機能（ＯＴＰトークンのＴｉｍｅＤｅｐｏｓｉｔ機能、通貨における定期預金を本発明のＯＴＰトークンに形態）を本発明のＯＴＰトークンのトークンに組み込んで利用してよく、その機能によって ＯＴＰトークンのＴｉｍｅＤｅｐｏｓｉｔ機能が解除されるブロック番号を預け入れているＯＴＰトークンと対応付けられた備考欄に明記して電子署名やＨＭＡＣなどを用いて改ざん困難な資産残高証明書を作成してもよい。
ＴｉｍｅＤｅｐｏｓｉｔ機能は例えばＯＴＰトークンの譲渡制限が解除されていても、ユーザーがある時期（数年もしくは数十年）までは譲渡しようとは思わない書籍の暗号化データを復号するＯＴＰトークンを保管する際に用いられることを想定している。秘密鍵の流出による不正アクセスが仮にあってもＴｉｍｅＤｅｐｏｓｉｔ機能によりトークン送信関数によって譲渡されるのを防ぐことができる。
【０４８６】
＜ブロックチェーン上のコントラクトやコントラクトと対応したサービスなどを検索するサービス＞
サーバ端末３Ａが記録しているブロックチェーン部データからユーザーの求めに応じてコントラクト識別子やその識別子のコントラクトの看板情報ＫＮＢＮから情報にアクセスし、ユーザーが望む情報を提供できるようにするブロックチェーン検索監視のための記憶部３０１Ｆとブロックチェーン検索監視部３１１Ｆを備えたサーバ端末３Ｆが存在し、端末１Ａや端末４Ａから３Ｆに対しアクセスし、望みのＯＴＰトークンのコントラクト識別子やＯＴＰトークンのサービス名、ＯＴＰトークンを発行したユーザー識別子、検索数の多いＯＴＰトークンの情報、発行総数の多い／少ないＯＴＰトークンの情報などが検索できる。ここで３Ｆは既に既存のサービス例があるため説明を省略することもできるが、３Ｆの存在が無いとブロックチェーンを利用したＯＴＰトークンの流通やトランザクションの監視が出来ないのでここに記述する。
サーバ端末３Ｆ及びそれが提供する検索及び監視サービスはブロックチェーンエクスプローラー（ブロックチェーン上の情報を調査・閲覧・検索するシステム）であり、イーサスキャン（Etherscan）という団体による情報検索サイトEtherscanが既存の例として挙げられる（参考元、https://etherscan.io/　2020年12月8日閲覧）。本発明において端末３Ｆが存在することで秘密鍵を持たない端末や秘密鍵を持つ端末１Ａからアクセスを受け、端末３Ｆの設定に応じてブロックチェーン上のデータを調査・検索・閲覧可能にする。
端末３Ｆが無い場合、端末１Ａは端末３Ａにアクセスしブロックチェーンから望みの情報を独力で見つけ出さなければならなくなる。またブロックチェーンへのアクセスを行う秘密鍵（端末１Ａの１０１Ａ、端末１Ｂの１０１Ｂ、端末１Ｃの１０１Ｃ、端末４Ａの４０１Ａなど）が無いユーザーがブロックチェーン上で起きているデータのやり取りを見るためにもこのようなブロックチェーンの検索サービスサイトとそれを担う端末３Ｆが必要である。
【０４８７】

ブロックチェーンについて検索するサービスとして既存の例ではイーサスキャンが挙げられる。本発明ではブロックチェーン上の情報を検索し収集することは発明内容ではないので省略するが、本発明のサーバ３Ｆに加えサーバーＰ（図１の３Ａ）や端末１Ａ、端末１Ｂ、端末１Ｃ、端末４Ａ、サーバ端末３Ｃ、端末３Ｄ、端末５Ａ等はブロックチェーンにアクセスし任意のコントラクトのトランザクションデータを記録し、データベースを構築してコントラクトに関するデータを検索してもよい。なおイーサスキャンから検索する場合はＵＲＩで指定したユーザー識別子やコントラクト識別子のトランザクションを検索できる。

次に示す３つのＵＲＩは本発明の実施例において用いたコントラクト作成者および管理者の識別子に関するＵＲＩのトランザクション検索結果画面である。（１．https://ropsten.etherscan.io/address/0x0f398803BE4319B98F164cae47589797aC5cF906、２．https://rinkeby.etherscan.io/address/0x0f398803be4319b98f164cae47589797ac5cf906、３．https://goerli.etherscan.io/address/0x0f398803be4319b98f164cae47589797ac5cf906、2020年12月8日閲覧）

【０４８８】

本発明の認証システムにおけるコントラクトをブロックチェーン上にデプロイするときのトランザクションやコントラクト内部のコードを秘匿化すること、コントラクトのシークレット変数ＫＣ値やＢＣ値を変える場合のトランザクションを秘匿化することは重要であり、秘匿化されたデータは検索されても良いようにするか、もしくはトランザクションデータの閲覧を認めたユーザー識別子以外のユーザには開示しないシステム必要である。本発明の認証システムでは秘匿化できるブロックチェーン基盤を用いることが好ましい。

秘匿化されたブロックチェーン基盤をもちいてワンタイムパスワード生成および認証を行うコントラクトを生成し、ユーザーにワンタイムパスワードを表示させる権限としてあるトークン番号のトークンを発行しユーザーへワンタイムパスワード認証の手段を提供するとともに、コントラクトの管理者等がコントラクトにおいてワンタイムパスワードの計算に用いるシークレットキーとなる変数ＫＣまたはＢＣを書き換える指令と新たな変数の値などを記述したトランザクションを暗号化などで秘匿化してブロックチェーンに送付し記録させることが好ましい。

コントラクトの秘匿化のために複数のブロックチェーンを利用しそれらが連携するブロックチェーン基盤であってもよい。またブロックチェーンのノードがトランザクションマネージャー等を搭載しブロックチェーン上のトランザクションを秘匿化していてもよい。

本発明は秘匿化されたブロックチェーン基盤の構築に関する発明ではないので、秘匿化に関しては省略する。コントラクトのプログラムデータやシークレット変数ＫＣやＢＣ等を秘匿する方法は限定されない。

【０４８９】

＜有向非巡回グラフ系システム、その他スマートコントラクトを搭載したデータ構造のシステムへのＴＯＴＰ適用＞

本発明は実施例にデータ構造にブロックが単一のチェーンとして連結されるブロックチェーンを用いた。ブロックチェーンは改ざんに対し耐性があり、またブロックが１次元の鎖状に過去から未来のブロックへ結合しながら形成されていくので、ある時刻のブロックにおいてワンタイムパスワードの時刻に関する変数とワンタイムパスワードをトークン化しパスワードの生成と認証するスマートコントラクトが改ざんされにくい点で本発明を実施しやすい。本発明でブロックチェーンにはスマートコントラクトというブロックチェーン上でのトランザクションを基に動作する改ざん耐性のあるプログラムを搭載できるイーサリアムを利用している（非特許文献１）。

一方でブロックチェーンとは異なるデータ構造をとるシステムに有向非巡回グラフ（ＤＡＧ）を用いたものも存在する（非特許文献２）。ＤＡＧではトランザクションを一つのデータブロックとしている。本発明をＤＡＧ等に利用する場合にはブロック番号を用いて時刻を表現するのは困難であるかもしれない。

【０４９０】

ＤＡＧ型においてデータブロック（チャンク）にタイムスタンプを付してあればそのシステムで動作するＴＯＴＰトークンのコントラクトが構築できるかもしれない。ＤＡＧ型の分散型台帳システムにおいてある時刻Ｔを表す関数としてＤＡＧを形成している最新のブロック（チャンク）に記述された時刻データＴｍをワンタイムパスワードの生成と認証に用いる事が可能である。ＴｍにはＤＡＧを構成するデータブロックがあり、あるデータブロックに本発明で述べたワンタイムパスワード認証のスマートコントラクトが記録され、そのスマートコントラクトに対し、ＤＡＧシステム全体で同じ時刻を示せるデータが最新のＤＡＧのブロックもしくはＤＡＧシステムから入手できる場合において、ブロックチェーンと同じくスマートコントラクトが実行され、本発明の認証システムとすることができる。

【０４９１】

ここでＤＡＧを用いる場合は最新の時刻にトランザクションのデータブロック（チャンク）が複数存在するため、最新のトランザクションデータ全てに最新の時刻情報が記録されていることが必要かもしれない。本発明ではＴＯＴＰを算出するシード値をブロックチェーンの最新のブロック番号、最新のブロックの時刻データもしくはタイムスタンプ、最新のブロックデータのブロックハッシュを利用することが可能であった。しかし、ブロックチェーンでなくＤＡＧ型のデータ構造を持つ場合、もしくはＤＡＧのように現在の最新のデータブロックもしくはトランザクションデータが複数存在する場合にはブロックハッシュを用いてＴＯＴＰを生成することができない。また最新のトランザクションデータのブロックに時刻情報やブロック番号に相当する時刻を表現する数値情報が含まれていないとＴＯＴＰの生成が困難かもしれない。時刻を表現する数値情報が含まれている場合はＢｎＴＯＴＰのようなＴＯＴＰが利用できうる。

ブロックチェーン型のデータ構造を用いた分散型台帳では、ブロックデータのハッシュ値は最新のブロックが一つだけなので一つのみである。また過去のブロックハッシュはブロックチェーンの各ブロックデータを参照し、ブロック番号と対応し現在から過去に列挙していくことができる。一方でＤＡＧブロックチェーンのような複数の最新のトランザクションのブロックデータがある場合、それぞれに異なるブロックハッシュが計算されるので時刻によって唯一のブロック値が存在しないのでブロックハッシュをＴＯＴＰのシード値に用いるのは困難である。

【０４９２】

ＤＡＧを用いる場合に本発明を適用するにはブロックチェーン型における最新のブロック番号もしくはタイムスタンプに相当する変数をスマートコントラクトの実行に利用できる分散型台帳制御部が必要である。実施例のブロックチェーンの場合はブロックチェーン部にブロック番号やタイムスタンプを得る処理部が含まれている。

本発明はブロックチェーンやＤＡＧなどの改ざん耐性を備えさせた分散型台帳かつスマートコントラクトが動作する基盤において、過去から未来にトランザクション等のデータがブロック（塊）として連結される場合に、そのデータブロック連結体の内部にワンタイムパスワード認証にかかわる処理部をスマートコントラクトという改ざんされにくいプログラムに内蔵し、改ざん耐性を持たせ、かつデータブロック連結体の最新のブロックもしくはシステム状態で得られる時刻データＴｍをワンタイムパスワードの生成に用いることを特徴とする。Ｔｍが時刻情報でもよいし、Ｔｍの代わりにＢＣを用いてコントラクトの管理者がＢＣを任意時刻に書き換えてもよい。

【０４９３】

＜有向非巡回グラフ系システムにスマートコントラクトを搭載したシステムへのＯＷＰの適用＞

有向非巡回グラフ（ＤＡＧ）型システムまたはそれに含まれないデータ構造のスマートコントラクトが動作するシステムにおいて、コントラクトの管理者のユーザーが任意の時刻にワンタイムパスワード生成および認証を行うコントラクトにアクセスし、そのシークレット変数ＫＣやＢＣを書き換えるトランザクションを分散型台帳に記述し、ＫＣまたはＢＣの変化によりパスワードＯＷＰを生成させ認証に利用することが可能である。パスワ

ードＯＷＰの場合はブロックチェーンやＤＡＧの時刻情報によらず、コントラクトの管理者が任意の時刻に変数ＫＣやＢＣを変えることができるので、ＤＡＧのようなデータ構造においても適用できる。

本発明でコントラクトの管理者のユーザーが任意の時刻Ｔにシード値を書き換えて変化させることのできるパスワードＯＷＰはブロックチェーンとは異なるデータ構造のスマートコントラクトを動作させる基盤に対しても有効であり適用される。ＤＡＧではＯＷＰのシード値となるＫＣやＢＣをコントラクトの管理者の端末からある時刻ごとに変数の書き換えを行うことで、ＴＯＴＰと同様にある時間ごとに代わる動的なパスワードが生成できる。この場合、コントラクトの管理者の端末にコントラクトのＫＣ値とＢＣ値を指定した日時、時刻ごとに変えるプログラムを記憶装置と処理装置に持たせることで、ＫＣ値及びＢＣ値の更新作業を自動化させることもできる。（スマートコントラクトを備えるＤＡＧならば、ＴＯＴＰ型の実施が困難であってもＯＷＰとＯＷＰのシード値を変える自動化プログラムにより疑似的なＴＯＴＰによる認証システムを構築できる）

【０４９４】

本発明では実施例でイーサリアムを用いており、本発明はイーサリアムを基盤としたブロックチェーンとそれを用いたスマートコントラクトの実行システムで動作出来ることを検証しながら発明を行った。発明を行ったのは西暦２０２０年であり、その当時の最新の版であるイーサリアムと、プログラム言語Ｓｏｌｉｄｉｔｙを用いている。

【０４９５】

本発明においてスマートコントラクトを用いてブロックチェーンのある時間において変化する情報を動的なワンタイムパスワードのシード値として用いる事を、またその認証システムを用いて暗号化したデータの復号を行うシステムや、ウェブサイトへのログインシステム、さらにはデジタル機器を用いるＮＦＣタグ１９Ａもしくは紙等の有価紙葉１８Ａやディスプレイ１５００Ａなどの媒体でチケットや施錠を解錠する鍵などに用いる認証システムの説明を行った。

認証時にブロックチェーンにおける最新のブロックデータのブロック番号Ｂｎやブロックハッシュ値、タイムスタンプ値、コントラクトに帰属するトークンのトークン番号、ブロックチェーンのユーザー識別子、ＩＰアドレス、位置情報、コンピュータの装置情報、そしてコンピュータ内蔵の入力装置４４Ａのセンサ４４４Ａの環境センサ４４４０または位置センサ４４４１またはモーションセンサ４４４２Ａまたは生体認証用センサ４４４３Ａを用いて測定する物理量を利用することを特徴とし、ブロックチェーンで用いるユーザの秘密鍵の不正使用を監視し検出しユーザーへ通知可能な認証システムとした。前記の本発明の認証システムについて実施例、符号、図などを用いて説明を行った。

【０４９６】

ただし本発明はブロックチェーン基盤の発明ではないのでイーサリアムの詳細については省略している。実施例の前提として本発明はイーサリアムとイーサリアムのスマートコントラクトの動作する環境で動作する。さらにイーサリアム及びそのブロックチェーン上で動作するスマートコントラクトを用いるウェブアプリ、ｄＡｐｐｓ（分散型アプリケーションソフトウェア）、ウェブブラウザソフトウェア、ＥＣＭＡｓｃｒｉｐｔ、Ｓｏｌｉｄｉｔｉｙ、コンピュータのオペレーティングソフトウェア、ブロックチェーンのノード、ネットワーク、ノードとなるサーバーやコンピュータについてはイーサリアムが運用可能な環境を使用する。実施に関しては好ましくは秘匿化されたトランザクションやコントラクトを利用できるブロックチェーン基盤が好ましい。

【０４９７】

＜ネットワークの定義＞

本発明で示される通信網２に含まれる暗号化されたネットワーク２０（ネットワークＮＴ）、暗号化されていないネットワーク２２（ネットワークＮＴＰ）は光ファイバや電線のような有線ケーブルと無線設備等を用いた、地球規模の通信網であるインターネットワークでもよい。

ネットワークには接続の制限されたローカルエリアネットワークＬＡＮを用いたものでも

よい。
【０４９８】
＜インターネットワークとローカルエリアネットワーク上のコントラクトの連携＞
ここでインターネットワークと物理的に接続できないネットワークとは、団体の建物のみの中で利用されるネットワークや、ある建物と遠くに離れた建物を専用の回線で結んで形成されたネットワークのことを示し、その例として企業や公的機関、大学、研究機関、金融機関等が用いる専用回線で構築されたコンピュータネットワークである。
本発明においてワンタイムパスワード認証を行う際にパスワードを算出するハッシュ関数などの処理の内容と、その引数が一致できれば認証可能である。例えば紙のチケットでパスワードＯＷＰを生成する際は、ＯＷＰの生成はインターネット経由でブロックチェーンにアクセスして生成し紙に印刷し、紙のチケットの認証はサービスを提供する建物の入場口のチケット読み取り端末３Ｄは建物内のローカルエリアネットワーク（ＬＡＮ）に接続され、そのＬＡＮ上で動作する建物専用のブロックチェーンのコントラクトにアクセスし認証を行う。
ここで重要なこととしてインターネットと建物のＬＡＮ間でのブロックチェーンのコントラクトはＯＷＰを算出するハッシュ関数ｆｈなど処理内容とシード値ＫＣが一致していなければいけない。ＬＡＮのブロックチェーンにてＯＷＰの認証ができれば、ユーザーは建物に入場できる。
インターネットワークと物理的に接続できないネットワーク はＬＡＮの規模に限らない。大学の構内程度から一都市全域までをカバーするコンピューターネットワーク、もしくは遠隔地のＬＡＮを専用の回線で連携させたコンピューターネットワークでもよい。
【０４９９】
＜ローカルエリアネットワーク上でのコントラクトの連携＞
ワンタイムパスワードの生成と認証を行う関数等とシード値が一致しているならば、同一のＬＡＮ内や異なるＬＡＮで構築されたブロックチェーン上のコントラクトにてワンタイムパスワードの生成と認証が行える。具体的にはある研究機関で研究所内の実験データなどを本発明のソフトウェア４０３Ａを用いた暗号システムで暗号化する、または研究施設や設備を施錠するといった際に、インターネットワークに接続していないＬＡＮにブロックチェーンを形成し、研究所の職員に応じたアクセスレベルのワンタイムパスワードを社員のＩＣカード式社員証などに付与して、暗号化データの閲覧、実験で得られた平文データの暗号化、研究施設や設備の解錠に用いる。
【０５００】
＜記憶装置＞
本発明でユーザー端末１Ａやサーバ端末３Ａなどの記憶装置は読み取り専用メモリＲＯＭ（Read Only Memory）とランダムアクセスメモリＲＡＭ（Random Access Memory）がある。他に半導体メモリの一つであるフラッシュメモリで構成されたＳＳＤ（Solid State Drive）や磁気ディスクを用いるＨＤＤ（Hard Disk Drive）そして磁気テープも記憶装置に利用できる。他に光学ディスクも利用される。
【０５０１】
＜本発明の認証システムに用いる個人情報の管理＞
欧州連合ＥＵの 一般データ保護規則ＧＤＰＲ（参考元、 日本貿易振興機構「特集 ＥＵ 一般データ保護規則（GDPR）について」 https://www.jetro.go.jp/world/europe/eu/gdpr/ 閲覧日2020年12月8日）によれば個人情報の保護が必要となることも予想される。
個人の名前や住所、電子メールアドレス、電話番号、ＩＰアドレス、位置情報、端末１Ａや４Ａなどの装置に固有のＩＤ（デバイスＩＤ）や端末の入力装置４４Ａのセンサ４４４Ａの値とユーザー識別子とＯＴＰトークンのトークン番号を本発明では図６Ｘのように収集しサーバ３Ｃやサーバ５Ａといった端末で保持する際に、端末の所有者に同意を求め、どのような情報を取集し、不正アクセスの検知に用いるか説明し同意を求める機能を図６Ｘのデータ構造を持つ実施例１と実施例２と実施例３に述べたサービスで利用できる。
本発明ではユーザー端末の秘密鍵の不正利用を監視し検出する場合にユーザーの個人情報

であるユーザー識別子やトークン番号とＩＰアドレスや端末のセンサ値などを収集する。
本発明では個人情報を保護しつつ不正アクセスの検出を行うために、図６Ｘに示すユーザー識別子とトークン番号とＩＰアドレス、位置情報、端末１Ａや４Ａなどの装置に固有のＩＤ（デバイスＩＤ）や端末のセンサの値は、匿名化（不可逆的に識別を防止。ハッシュ化、ハッシュ化後にハッシュ値の一部を切取るなどの加工を行い）または仮名化（可逆的に仮名化したデータとそれを復号する鍵などを用いている場合。個人情報を暗号化して保存する場合）してサーバ端末３Ｃや端末５Ａといった端末へ図６Ｘのデータ形式で情報を記録し利用できる。

【０５０２】

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、本発明の認証システムが利用されるサービス・暗号化データ・装置・容器・乗物・建物ごとに法令を遵守した利用が行われ、それに応じてコンピュータ端末、ネットワーク、サーバ端末、記録装置、入出力装置を追加して利用されうる。本発明の認証システムを利用するユーザーの個人情報の保護を行いつつ、データやサービスへのアクセスコントロールを前提として本発明を適用したシステムは運用される。また実際に利用される形態ではスマートコントラクトに本発明の説明で述べた処理の内容の他に、ユーザーに対し様々な業種や種類のサービスを提供するために必要な変数や関数・処理を追加することが考えられる。

本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら新規な実施形態は、例としてイーサリアム等に限らずその他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行なうことができる。

【０５０３】

＜記号・用語＞

次に記号と用語について説明する。

ＤＬＴ　(Distributed Ledger Technology)　分散型台帳技術のこと。

ＤＬＳ　(Distributed Ledger System) 分散型台帳システム。本発明を適用するブロックチェーンシステムやＤＡＧ型システムの略号にＤＬＳを用いた。

ＵＲＩ　(Uniform Resource Identifier) インターネット上の情報の所在を指定する URL, URN などの総称。

ウォレットソフトウェア　　ＤＬＳで用いる秘密鍵を管理する。例としてパスワード付きのウェブブラウザ拡張機能等として利用される。記録された秘密鍵にてウェブページ・ＤＬＳにアクセスできる。

ハードウェアウォレット　　デジタル機器に秘密鍵を記録させた秘密鍵の外部記憶装置。ウォレットソフトウェアと連携できる装置もある。秘密鍵記憶装置の観点では個人番号カードとも類似する。

秘密鍵ＰＲＶＡ等　　ＤＬＳ上で利用する秘密鍵。秘密鍵とＤＬＳが無ければＯＴＰトークンによる認証やサービスが行えない。端末１Ａの１０１Ａと同じ。

ユーザー識別子Ａ　　秘密鍵１０１ＡからＤＬＳの処理に従い計算される。実施例においては秘密鍵、公開鍵、公開鍵のハッシュ値、ハッシュ値の一部データを切り取りユーザ識別子として利用する。

ＵＡ　　端末１Ａのユーザ。

ＵＢ　　端末１Ｂのユーザ。

ＵＣ　　端末１Ｃのユーザ。

ＵＰ　　端末４Ａのユーザ。

ＢｎＴＯＴＰ　　ブロックチェーンなどのＤＬＳ上でブロック番号Ｂｎとコントラクト内部のシード値ＫＣなどを基に計算する、ブロックチェーン上の時間に基づいたワンタイムパスワードの略称。

ＯＷＰ　　コントラクト管理者（Ｏｗｎｅｒ）が分散型台帳システムＤＬＳのコントラクト内部変数ＫＣやＢＣを任意時間、任意数位に書き換えることで、疑似的なＯ

ＴＰを生成する際のパスワードの略称。
　ＢＩＯＳ　Basic Input Output Systemの略。端末の記憶装置もしくは外部記録装置からオペレーティングシステムソフトウェアの読込、時刻情報の記録など基礎的な制御を行う。
　ＥＦＩ　Extensible Firmware Interfaceの略。特許出願時点で利用されている最新のＢＩＯＳの規格。
　ＲＯＭ　Read Only Memory。データの書き込み後、読取のみできる記憶装置。
　ＲＡＭ　Random Access Memory 。データの消去、書換が可能な記憶装置。
　ＣＰＵ　Central Processing Unit 。 電子計算機（コンピュータ）の中央処理装置であり、制御装置と演算装置を統合したもの。
　ＳｏＣ　System on Chip。 ＣＰＵとグラフィック処理装置、ＧＮＳＳなど無線信号の受信モデム、無線通信モデムといった複数の機能を１つチップに統合したもの。通信装置や制御演算装置を構成する。
　ＭＣＵ　Micro Control Unitの略称。マイクロコントロールユニット。
　ＮＦＣ　Near Field Communicationの略称。近距離無線通信。
　ＮＩＴＺ　ネットワークｉｄおよびタイムゾーン。
　ＧＮＳＳ　Global Navigation Satellite System / 全球測位衛星システム。
　ＪＪＹ　日本標準時を送信する放送局の名称。
【産業上の利用可能性】
【０５０４】
　ブロックチェーン等分散型台帳システムＤＬＳにおいて、ＤＬＳ上で最新の時刻Ｔにおいて変化する情報ＴＢ（もしくはＴｍ）のうち、ブロック番号Ｂｎなどの時刻によりブロックチェーン上の最新のブロックにおいて変化する変数を用いて時間に基づいてパスワードＢｎＴＯＴＰが動的に変化するワンタイムパスワード認証システムを実現した。
　またＤＬＳ上で最新の時刻Ｔにおいて変化する情報ＴＢをワンタイムパスワード認証システムに関与するコントラクトのシード値ＢＣやＫＣをコントラクトの管理者が任意の時間、任意の数値で変更することで、疑似的なワンタイムパスワードを実現し、コントラクト管理者がその値を変更するまで有効なトークン番号ＴＩＤＡのパスワードＯＷＰを用いたコントラクト管理者変更型ワンタイムパスワード認証システムを実現した。
　そして時間に基づいてパスワードＢｎＴＯＴＰについてシード値ＫＣ、ＢＣをコントラクトの管理者が任意の時間、任意の数値に変更し更新することを可能にした時間に基づいたワンタイムパスワード認証システムを実現した。
　さらにパブリックなブロックチェーンにおいて、ランダムなシード値をＢｎＴＯＴＰ計算に用いることがセキュリティ上必要と考え、ブロックチェーンを構成するノードの投票によって決まる値Ｖ、ブロックチェーンに連結するブロックデータサイズ値ＢＳＺを擬似乱数の元となる値としてＢｎＴＯＴＰの計算に利用するワンタイムパスワード認証システムを実現した。そしてＢｎＴＯＴＰを例としてウェブサイトへのログインや暗号化データの復号、現実世界でのオンラインなサービス提供会場においてウェブサイトなどにログインする形での入場を可能にする。
【０５０５】
＜ＢｎＴＯＴＰによる用途＞
　ウェブサイトへのログインは銀行や証券、保険、決済事業における多要素認証に利用できる。また会員制サイト、電子商取引、オンラインデータストレージ、電子メール、業務用オンラインソフトウェア、オンラインコンピュータゲームへのログインにも応用されうる。暗号化されたデータを復号する際に認証システムにて認証を行い、その戻り値を鍵の一つとして暗号化データの復号ができる。
＜ＯＷＰによる用途＞
チケットなど有価紙葉１８Ａや施錠を解錠するＮＦＣタグ１９Ａに用いられる。
　パスワードＯＷＰをユーザーに表示印刷させ、ユーザーにユーザー識別子Ａとトークン番号ＴＩＤＡとパスワードＯＷＰを紙などに文字列またはバーコードとして印刷し１８Ａ

とし、あるいはＮＦＣタグ１９Ａなどの非接触型デジタル機器に記録させ、紙及び電子式チケットを製造し、サービスを提供する現実世界の場において前期チケットよりパスワードＯＷＰ、ユーザー識別子Ａ、トークン番号ＴＩＤＡを読み取り認証を行うことでサービスを提供する認証システムが構築できる。紙は情報が印刷、印字できればよく、レーザープリンタ、インクジェットプリンタ、サーマルプリンタ等のデジタル印刷装置とそれに対応した紙、感熱紙、インク、トナー等を使用する。印刷方式は版の無い方式を用い、電子計算機から出力される指示に従って文字列やバーコードを紙やプラスチック、金属板などのメディアに記録できればよい。

カメラなどで認証用の情報が読み取り可能であれば紙にとどまらず金属板や石板などに情報は記録できる。カメラを使わない場合でも、文字列を人の手によって認証することは可能である。プリンタが無くともユーザーが手で紙や金属板に認証に必要な文字列を判読可能な状態で書き記し、それをチケットとしてサービスを提供する場に持ちこみ、文字列をサービス提供者に提示もしくは伝達し、サービス提供者が文字列を認証関数に手動で入力し認証を行うこともできる。しかしそれでは省力化・自動化できないので紙などに文字列またはそれを示すバーコードを印刷し、サービス提供者はその文字列バーコードをカメラやスキャナで読み取って認証する。

ＮＦＣタグ１９ＡにＯＷＰとユーザー識別子Ａとトークン番号ＴＩＤＡを記録した場合は、ＮＦＣタグ１９Ａを読み取ることの出来る施錠を管理する端末３ＤにＡとＴＩＤＡとＯＷＰを読み込ませ認証処理を端末３Ｄに行わせ認証結果が正しいときに施錠を解錠させることができる。

【０５０６】

＜ＯＷＰなどの認証情報を記録したＮＦＣタグ＞

紙よりも認証の高速化が期待できるのはＮＦＣタグ１９Ａなどデジタル機器による認証である。ＮＦＣタグ１９Ａは携帯可能な端末や身に着けることが容易な端末でもよく、スマートフォンなど携帯電話端末に内蔵したもの、財布型、ＩＣカード型、キーホルダー等タグ型、眼鏡型、補聴器・ヘッドホン・イヤホン型、ＮＦＣタグ１９Ａつき衣服型、時計型、腕輪型、ベルト型、靴型等である。（スマートフォンなど災害などの例外を除いてネットワーク２０に接続できる端末とＮＦＣ端末１９Ａが通信し合い連携している場合には不正アクセス検知も可能である）。ＮＦＣタグでなくとも、財布や衣服、靴などの服飾品にＯＷＰ等が印字された布・プラスチックフィルム・紙等のタグの形で利用することができる。

【０５０７】

＜ＯＷＰを用いたタグによる製品の真贋鑑定＞

本発明ではＯＷＰを用いたチケットについては、会員証・身分証・商品券・サービス券（有価紙葉）を想定している。それ以外にも商標権（立体商標権含む）を取得した衣服品などを流通させる際に真贋鑑定や認証を行う際に、衣料品の型番とＯＴＰトークンのコントラクト識別子、製造番号とＯＴＰトークン番号、商標権を持つ製品製造者のユーザー識別子、ＯＷＰコードを用いて認証に利用することができる。この場合は商標権などで保護された製品に内蔵されたＮＦＣタグか、製品の表面に目に見える形で取りつけられた布製・紙製等のバーコードの形で製品を正規流通品かどうか認証できる。

被服にＮＦＣタグを搭載した場合、自らどのようなＮＦＣタグで認証された正規の衣服製品かの真贋を判定できる。しかし同時に被服に内蔵のＮＦＣタグのデータを無線通信で読み取られる恐れもあり、タグを持つユーザーのプライバシーを侵害しかねない。

その一方でＮＦＣタグと比べ布などにＯＷＰ等が印刷もしくは捺染もしくは編み込まれる形で書かれた方式では、無線により読み取られることがないので個人情報を保護する事に役立つ。紙や布に書かれた認証情報であれば、普段人目につかない服のサイズなどを記すタグ部分に洗濯表示やサイズ情報、製造者情報の隣に製品のシリアル番号としてＯＷＰ認証用情報のタグをつけることができる。

被服を例として示したが、権利者によって守られている農林水産物のラベル、食品など生活必需品のラベル、ワイン・日本酒など酒類のラベル、衣服のラベル、皮革製品のラベ

ル、宝飾品のラベル・刻印、電気機器・電子機器のラベル、住居のラベル、自動車や機械設備等部品のラベル、模型・玩具、紙本、音楽・動画のディスクなど著作権者等の権利者のいる製品のラベル（およびタグ）にも本発明は応用可能であり製品の認証と真贋鑑定ができる。

半導体及び電子部品等の小型な製品においても半導体のパッケージや内蔵されたシリコンや素子に微細な文字列またはバーコードをパターニング、刻印、印字し、肉眼では判別不可能かつ顕微鏡などで判別可能なＯＷＰ等認証情報を記録させ、そのＯＷＰ情報を読み取り認証関数へ読み取った情報を代入することで製品が正規品かどうかの真偽を確かめることができる。ＯＷＰを使う場合は目視判別出来ないほど微小な印刷内容や刻印内容であっても、それを拡大して文字情報、画像情報として読み取ることが出来れば認証可能である。

ウエアラブルコンピュータ、腕時計、指輪、宝飾品や半導体チップ（パッケージ前のＩＣシリコン片）など小型な貴金属や半導体、石材など本発明を応用する場合は製品の母材の表面に微小なＯＷＰ等の情報を刻印などで記録させ真贋の鑑定に利用することも考えられる。指輪など装身具では宝石などを留める指輪本体部分の母材に刻印する。貴金属の宝飾品やインゴットなどの製品にも微細なＯＷＰ等の情報を複数記録させることで製品流通を管理できるかもしれない。プラスチックフィルムや紙でできた有価紙葉を流通させる場合も容易に読み取られないように微小なＯＷＰ等の情報を印刷して有価紙葉を製造できるかもしれない。

【０５０８】

＜ＯＷＰを用いたタグによる物流管理＞

物流用にＯＷＰを生成・認証するＤＬＳを構築し、前記物流用ＤＬＳにＯＴＰトークンを発行し、それに対応したＯＷＰ生成関数と認証時の認証を行った端末の位置情報やセンサ情報をＤＬＳ上に記録させる認証関数を用いることでＯＷＰでラベル付けされた物流容器の配送状況などの記録が可能になる。ＯＷＰにて容器を封じた際にその封印用ラベルに本発明のＯＷＰ等認証情報を印字し、封印ラベル１８Ａで封じられた荷物の流通を改ざんなどに耐性のあるブロックチェーン上で記録しつつ追跡できる。

【０５０９】

食品の物流用に本発明の１８Ａの情報を食品の包装に印刷し、食品の包装に印字される賞味・消費期限情報や製造工場情報などといった商品情報を記録し流通の過程で管理させ消費者が購入する際に店舗にてその二次元バーコードを読み取り、かつ消費者の決済情報や端末と関連付けることで、ある店舗で賞味・消費期限が何時までの食品を購入したか情報を記録できる。そして前記情報から購入済みの食品の消費期限切れによる食品廃棄ロスを減らせるかもしれない。１８Ａの流通情報や店舗における購入時に購入した商品の賞味・消費期限情報を端末１Ａなどの決済に用いるもしくは決済結果を閲覧できる端末に記録・表示させ、消費期限が近づいた際に端末１Ａに通知することで意図しない消費期限経過による食品廃棄を防ぐ。１８Ａの情報は冷蔵庫などの食品保管庫を制御する端末と連携していてもよい。

【０５１０】

食品に限らず家電製品や住宅設備、自動車部品と自動車、医薬品などの商品について、商品の製造販売元が消費者より回収を行う際に、店舗が販売した消費者の同意を得て製造販売元に情報開示できるとき、どの商品がどの消費者により購入されているかの調査に役立つかもしれない。

【０５１１】

＜ＯＷＰの認証＞

ここでパスワードＯＷＰを用いて１５００Ａや１８Ａや１９Ａにて認証する場合は、サービスを提供する場に持ち込まれた紙及び電子式のチケットが有効であるか判定する認証サーバ（認証端末３Ｄ）がある場合にはチケットの認証が可能であり、災害などでネットワークがオフラインになってもチケットの認証を行うことが可能である。チケットの発行と所持の観点ではブロックチェーン等ＤＬＳの持つ改ざんへの耐性や分散させることが特

性により世界中にサーバにトークンデータの記録を行われ、ユーザーが保有していたことを記録できる。チケットの他鍵としても利用されうる。

産業上の利用可能性を高めるためＯＷＰを用いたチケット１８Ａの譲渡を禁止することも、許可することも可能にし、かつ紙及びＮＦＣタグなどでの入場チケットを可能にするために、本発明ではＤＬＳと紙のチケットを結びつけるためにコントラクトの管理者であるオーナーが任意に任意変数を用いて変更できるオーナー型のワンタイムパスワードＯＷＰの概念を導入した。

【０５１２】

＜ＢｎＴＯＴＰとＯＷＰの関連性＞

ＯＷＰはコントラクト管理者がコントラクト内のワンタイムパスワード計算用シード値を書き換えることで、そのコントラクトに属するトークン番号のトークンが生成するパスワードを変更する。一方、ＢｎＴＯＴＰではブロック番号が自動的に増えてシード値は変更される。コントラクト管理者がシード値ＢＣ等をブロック番号Ｂｎのようにブロック番号が変わるごとに変更するようＤＬＳにトランザクションを送信しシード値を書き換えることで擬似的なＢｎＴＯＴＰをＯＷＰ方式でも実現できる。したがって、本発明ではＯＷＰのようにコントラクト管理者がＢｎＴＯＴＰの算出に用いるシード値を変更できることが好ましい。

ＤＬＳ上のスマートコントラクトにおいて、ＯＷＰ方式とＢｎＴＯＴＰ方式の考え方として、時計の秒針が自動で動く場合（ＢｎＴＯＴＰ）と手動で動かす場合（ＯＷＰ）が想像できる。カウンターである時計の秒針を動かすことが出来ればパスワードは変わり動的なパスワードはＤＬＳのスマートコントラクトで生成できる（ＤＬＳ由来のブロック番号等に由来する時間の変化によって変更される変数をカウンター変数に採用するか、スマートコントラクト経由でカウンターの変数を書き換えるトランザクションを送信して変更するかの違いである）。

ここでＢｎＴＯＴＰと比べＯＷＰはシード値の更新も含むので本発明では必要な要素である。

本発明ではＯＷＰを利用することで現実世界でのチケットなど有価紙葉によるサービスの提供とウェブサイトなどデジタル世界でのサービスの提供、暗号化データを復号するソフトウェアとそのソフトウェアへの広告配信サービス、秘密鍵の不正利用監視サービスが可能である。

ＯＷＰに加え、カウンターを手動で更新する必要のないブロックチェーンなどＤＬＳに利用されるブロック番号などのデータに着目しＯＷＰのパスワード算出を行うハッシュ関数の引数にブロック番号Ｂｎを追加して ＢｎＴＯＴＰとすることでワンタイムパスワードのシード値を手動にて変更できシード値の更新をＤＬＳにより自動で行わせることが可能になることを主張する。

【０５１３】

＜ＯＴＰトークンのスマートコントラクト上での利用可能性＞

図９Ａにブロックチェーン型の分散型台帳システム、図９Ｂに有方向非巡回ＤＡＧ型の分散型台帳システムを用いて本発明のスマートコントラクトや図６Ｘにおける秘密鍵の不正利用監視機能を用いる形態を示す。本発明は図９Ａの形態の他、図９Ｂの形態においても改ざん困難な分散型台帳システム上にスマートコントラクトのプログラムとして記録されるＯＴＰ生成関数とＯＴＰ認証関数を用い、ＯＴＰ認証システムを提供しうる。

【０５１４】

＜ＯＴＰトークンの利用可能性＞

本発明のＢｎＴＯＴＰもしくはＯＷＰを生成するＯＴＰ生成トークンを現実世界での鍵と同じようにブロックチェーン上のコントラクトでユーザーに発行したり、限定されたコミュニティまたは世界中のユーザー同士で譲渡し合うことが可能になる。

本発明のワンタイムパスワードトークンを現実及びデジタル分野での鍵もしくはログイン権、所有権、閲覧権、利用権、投票権などに利用することが可能になり、また暗号化されたデータを本発明によりワンタイムパスワードトークンを使い復号することも可能にな

る。本発明は紙のチケットにも電子的なチケットにもウェブサイトへのログインチケットにも適用でき、現実領域（物理的領域）とデジタル領域（データ領域）の両方で展開されるサービスに適用できる。

【０５１５】

＜ＯＴＰトークンのセキュリティトークンとしての用途＞

デジタルな空間におけるウェブサイトへのログインや暗号化データの復号、紙やＮＦＣタグでの現実世界でサービスを利用する場合の利用券として利用できる事について述べた。ここでＯＴＰトークンについてはユーティリティトークンとしての利用を想定するが、法で規制される有価証券の役割をＯＴＰトークンに持たせることも可能かもしれない。すなわち本発明のＯＴＰトークンをセキュリティ―トークン（電子記録移転権利、出典：日本証券業協会　https://www.jsda.or.jp/about/jishukisei/words/0326.html、２０２０年１２月１２日閲覧、）として用いることができるかもしれない。

セキュリティトークンの具体的な利用の形態の１つとしては本発明のＯＴＰ認証システムで用いるＯＴＰトークンと対応する株式会社の株式と結び付け、そのＯＴＰトークンのコントラクト管理者が譲渡制限や保管振替を行いつつ、株式会社の利益のうち配当金を証券会社や信託銀行等と連携しながらＯＴＰトークンの持ち主の証券口座などへ振り込むなどして分配する。

そして株主総会を行うウェブサイトへのログインをＯＴＰ認証システムで行い、株主総会における電磁的方法による議決権の行使を本発明のＯＴＰ認証システムを用いて投票などを通じて行うことができるかもしれない。１つのＯＴＰトークンに対し議決権を持たせそれを株主総会を行うウェブサイトでログイン及び議決権を行使した投票を行う処理に利用する。また株主が株式型のＯＴＰトークンを持つ場合に受けることの出来る権利（自社サービスの利用権、株主優待券など）の利用を行うときに端末１ＡのディスプレイなどでＢｎＴＯＴＰ型のＯＴＰを表示させてサービス提供者やサービス提供端末に提示しＯＴＰ認証結果が正しい時サービスなどを受けることができてもよい。

このように銀行や証券などの金融分野の利用券や証券として利用できるかもしれない。また建物の施錠に関連してや建物不動産の所有権と利用権に用いることも想定される。

【０５１６】

＜ＯＴＰトークンのＯＴＰを擬似乱数として用い、擬似乱数生成装置に用いる用途＞

くじ引きやサイコロを用いた遊戯など確率を基に何かを決定する事がある。例えば集客などの用途である商品の購入後にひくことの出来るくじ引きがあり本発明はその用途に利用できるかもしれない。遊戯用途ではオンラインゲームを含むコンピュータゲームにおいてＯＴＰをゲーム内で起きる物事の処理を決定する数に利用できるかもしれない。現実世界においても現物の賽子の代わりに賽子として利用するＯＴＰトークンのＯＴＰを表示させ、表示された番号によってカードゲーム等の遊具を用いた遊戯が可能になるかもしれない。

あるいは寺院や神社といった宗教的な施設に参拝し、お賽銭を投げ、あるいは金銭を支払い宗教的な施設に寄付をしておみくじを引くといった事例がありこの場合も本発明のＯＴＰ認証システムとＯＴＰトークンとその擬似乱数生成機能が利用できるかもしれない。

本発明はＯＴＰを生成させる機能があるが、これを疑似的な乱数として利用しつつ、ＯＴＰ認証を備えたウェブサイトにログインするＯＴＰトークンとして利用でき、ウェブサイトにログインした後もＯＴＰトークンからＯＴＰを生成し利用できることは先に述べたとおりである。そして寺院や神社といった宗教法人への寄付やおみくじをそのウェブサイトで行い通貨等で決済した際におみくじの結果をＯＴＰトークンのＯＴＰ値を寺院・神社のウェブサイトを配信する端末３Ｃでおみくじの結果を算出する引数として用い、おみくじの結果を計算してユーザーの端末１Ａに表示させてもよい。そして寺院や神社に訪れたユーザーに暗号化データの形でその縁起などを紹介するパンフレットのデータを配布し、ユーザーに閲覧できるようにしてもよい。

【０５１７】

ＯＴＰを擬似乱数生成に用いる際には、ＯＴＰ生成及び認証コントラクトにあるユーザ

ーのトークン番号ＴＩＤＡに対応したマッピング型変数ＫＣＵ［ＴＩＤＡ］（もしくはＶＵ［ＴＩＤＡ］）をＴＩＤＡのトークンの持ち主であるユーザー識別子Ａが変更できるセッター関数を備え、ＫＣＵ［ＴＩＤＡ］をユーザー識別子Ａのみが書き換えることができ、コントラクトの管理者１Ｃが書き換えることはできないがユーザーのみがアクセスし書き換えることでユーザーの保有するＯＴＰトークンの擬似乱数の計算に用いるシード値を変えることの出来る擬似乱数発生機を構築することもできる。

これはコントラクトの管理者が設定するシークレット変数ＫＣ値とは別に、ＯＴＰトークンの番号に応じてＯＴＰトークンの保有者が設定できるシークレット変数ＫＣＵ［ＴＩＤＡ］を設定し、それぞれのトークンに対しユーザーが設定したＫＣＵ［ＴＩＤＡ］をハッシュ関数ｆｈの引数に追加してＯＴＰを生成するものである。前記ＯＴＰの計算例はＢｎＴＯＴＰ型の場合はＢｎＴＯＴＰ＝ｆｈ（Ａ,ＴＩＤＡ,ＫＣ,Ｂｎ,ＫＣＵ［ＴＩＤＡ］）である。

ＫＣＵ［ＴＩＤＡ］、ＫＣＵ［ＴＩＤＢ］、ＫＣＵ［トークン番号］といったマッピング型変数（もしくは構造体型や配列型などの変数も可能、トークン番号をキーとしてＫＣＵのデータ配列を表現できれば可能）を擬似乱数を利用するユーザーが設定できることで、コントラクト管理者が定めたＫＣ値だけのくじ引き結果ではなく、ユーザーが定めたＫＣＵ［トークン番号］を加えたくじ引き結果を得ることができるのでコントラクト管理者の不正行為を防ぐことに役立つかもしれない。

前記コントラクト管理者の不正行為の例として、例えばオンラインゲームなどでゲームを管理する側がＫＣ値を含むシード値を全て知っていればある特定のユーザー識別子の特定のトークン番号のＯＴＰが未来のある時刻にどのようなＯＴＰ値が取れるかわかってしまい、それを予測してサーバ３Ｃのオンラインゲーム提供プログラムにユーザー識別子Ａなどを狙って悪意のある処理を組み込むことすら考えられる。

そこでユーザーが保有するＯＴＰトークンのシード値ＫＣＵ［トークン番号］が設定されていて変えることができる場合（なおかつＫＣＵ［ＴＩＤＡ］をユーザ識別子Ａが変更する際に送信するトランザクションが秘匿化できるブロックチェーン基盤であるとき）にはコントラクト管理者はユーザーの将来のＯＴＰ値を推測困難になる。そしてユーザーもまたコントラクト管理者の決定したＫＣ値を知らない場合にはユーザーの持つトークン番号ＴＩＤＡのＯＴＰトークンの生成するＯＴＰ値はわからないので疑似的な乱数発生装置として利用できる。コントラクト管理者はいつユーザーがＯＴＰのシード値ＫＣＵ［ＴＩＤＡ］を変更するかわからないので推測する意欲を削ぐかもしれない。

ここではオンラインゲームについて本発明を擬似乱数生成装置として利用したときの産業上の利用可能性について述べたが、オンラインゲームやくじ引き以外にも個人や団体、企業や公共団体にて何かを確率で決める際に利用できるかもしれない。

【０５１８】

＜ＯＴＰトークンをコンテンツとみなしデータ流通させる可能性＞

電子書籍や紙の書籍とも異なる分散型台帳システムを利用した暗号化データの流通を可能にする。譲渡制限が行われていない状態においてＯＴＰトークンと暗号化データとその復号用のソフトウェアＣＲＨＮ４０３Ａを別のユーザーに譲渡する事が可能になる。我が国で作成された著作物に由来するデータを海外に流通しやすくすることが可能になる。

データには小説、漫画、音楽、動画、コンピュータゲームソフトウェア、ビジネス用ソフトウェア、３ＤのＣＡＤデータ（及びその３ＤのＣＡＤデータを使い３Ｄプリンタから出力される模型等3次元物体）が含まれ広範なコンテンツをＯＴＰトークンという閲覧権・データ復号鍵として二次流通市場で取り扱われる可能性もある。また二次流通時にトークンの譲渡を任意の時間に制限し、または制限を解除する機能を持つため権利者の要望に沿った流通を行える。

ＯＴＰトークンと暗号化データの流通時にデータを復号した際に広告およびアクセス監視サーバーを設けることで、閲覧されているコンテンツの権利者に広告収益を分配することを意図している。また広告表示機能は不正アクセスの防止機能を兼ねており、ＯＴＰトークンの持ち主の秘密鍵の不正利用を検知することもできる。ソフトウェアＣＲＨＮ４０

３Ａにも広告等表示機能があり、不正アクセス防止と広告表示、ソフトウェア更新通知などを行う。

【０５１９】

＜ＯＴＰトークンをコンテンツのアクセス権や所有権およびコンテンツそのものとして流通させる可能性＞

本発明で暗号化データを復号する用途では、例えば書籍に関しては電子書籍や紙の書籍とも異なる分散型台帳システムを利用した暗号化データの流通とその所有権やアクセス権としてのＯＴＰトークンの流通を可能にする。またコンピュータソフトウェアにおいては業務用ソフトウェアやゲームソフトのソフトウェアにおいても所有権やアクセス権を表すＯＴＰトークンとして流通する。

ＯＴＰトークンのコントラクトに除去関数が内蔵されていない限り、ＯＴＰトークンはユーザーの持つ秘密鍵と対応したユーザー識別子に対応付けて改ざん困難なブロックチェーンに記録され保存されつづける。イーサリアムのようにユーザーもノード端末３Ａと同じ機能を持った端末を持ちブロックチェーンのノードとなることができればそのブロックチェーンを保持したいと考えるユーザーがいる限りＯＴＰトークンの所有情報は保存されうる。コンピュータソフトウェア販売者が配布するソフトウェアを暗号化したデータや暗号化前の平文データをソフトウェアＣＲＨＮに内蔵して配布している場合にはそのソフトウェアをユーザーの端末に記録し保持してソフトウェアを動作し続けることができる。

【０５２０】

＜ＯＴＰトークンを放送された暗号データの閲覧権として用いるとき＞

放送された暗号データ内部もしくはソフトウェア４０３Ａに視聴者が視聴するＯＴＰトークンのコントラクト識別子情報を図６Ｘのデータに併記することでユーザー識別子がどの放送事業者（もしくは放送サービス提供者）のコントラクト識別子のどのユーザー識別子のどのトークン番号のユーザーがアクセスして視聴しているかが把握できる。この機能は端末５Ａによる広告サーバ機能と不正アクセス防止機能を応用するものである。ユーザーのプライバシーに配慮しユーザー識別子やトークン番号を匿名化し図６Ｘのように端末５Ａに記録することが特に求められるかもしれない。

前記図６Ｘに示すアクセスデータを集計し放送の視聴者数に該当するユーザー識別子のアカウント数を集計することでは総視聴者数が得られ、放送時の視聴率などを求めたいときに応用できる。ただし放送受信者が地上波デジタル放送などの受信者数に匹敵するときは端末５Ａは複数の分散されたサーバ群にしなければ図６Ｘの形式でのアクセス管理を行う際に計算資源やネットワーク２０の通信可能な帯域を消費しかねないので、図６Ｘにおけるアクセス受付時間をトークン番号の末尾桁数時ごとに異なる時刻で視聴中か否かの情報を端末４Ａからネットワーク２０を介して端末５Ａのサーバ群に伝達できると好ましいかもしれない。

【０５２１】

＜ＯＴＰトークンを用いてＧＮＳＳの信号のデータの真偽を判定するとき＞

ブロックチェーンのノード端末３Ａと接続できるＧＮＳＳなどの測位用人工衛星端末５Ｃから放送されたＧＮＳＳ測位信号に、本発明のＢｎＴＯＴＰ信号を添付させ、地上局端末１Ａや端末４Ａでその受信した測位信号とデータをネットワーク２０を介してブロックチェーンのノード端末３Ａの認証関数３０１８Ａで認証することで放送局５Ｃの測位信号が正しいものか判断でき、ＧＮＳＳの測位信号のなりすましか否かを判断できる。

ＧＮＳＳ信号は自動車や航空機、船舶、携帯電話・スマートフォン端末、無人機が自身の位置を測位するための情報であり、ＧＮＳＳ信号の真贋を判定しなりすまし信号を判別できるようにする。位置情報と時刻情報はＢｎＴＯＴＰによる認証を用いることでブロックチェーン上のデータとリンクされそのＢｎＴＯＴＰを含む測位情報を受信した端末１Ａの位置情報と時刻情報とブロックチェーン情報を用いることでその端末１Ａがあるときにある場所にいたかを認証できるかもしれない。

そしてＢｎＴＯＴＰを含む測位情報を受信した端末１Ａの位置情報と時刻情報とブロックチェーン情報を用いることでその端末１Ａが入出力装置を通して記録している文章画像

情報や動画や音声といった情報にＢｎＴＯＴＰや時刻情報や位置情報を記録することで、入出力された情報や印刷物などに確かな位置情報付きタイムスタンプを付与できる。（前記データにＨＭＡＣのＭＡＣ値を付与してもよい。）
さらに自動車や船舶や航空機と無人機・無人航空機のナビゲーション用途で認証された位置情報によってより安全にそれらの機械を移動させることができるかもしれない。

【０５２２】

このＧＮＳＳ信号にＢｎＴＯＴＰを添付するという考え方は、ＯＷＰを用いたタグによる物流管理において１８Ａや１９Ａの形で物にＯＷＰを添付して流通を管理していた考え方を、端末５Ｃから放送されたデータの流通に応用したものであって、ＢｎＴＯＴＰを放送データに添付して放送データの流通を管理するものである。ＧＮＳＳ信号に限らず放送データや配信データにＢｎＴＯＴＰやＯＷＰを添付して認証し真贋を判定してもよい。

【０５２３】

＜ダウンロード販売プラットフォームとの関係＞

ダウンロード販売プラットフォームにより電子書籍や音声動画データ、コンピュータソフトウェア、コンピュータゲームソフトウェアが販売されることが増えている。しかしダウンロード販売プラットフォームはそれを運営する会社ごとに異なるアプリケーションソフトウェアをインストール必要があったり、そのソフトウェアを維持する会社が存続できなくなった場合にはサービスが終了する恐れがある。

例として電子書籍やコンピューターゲームは閲覧権やプレイする権利を購入していることがあり、紙の書籍やコンピュータゲーム端末に読み込ませるゲームソフトウェアの記憶された半導体メモリ式ＲＯＭカセットや光学ディスクの所有権を販売する形態とは異なる。

本発明では権利者が許可する場合に限りその所有権をＯＴＰトークンとして流通させ、ブロックチェーンシステム・ＯＴＰトークン・トークンの割り当てられた秘密鍵４０１Ａ・ソフトウェアＣＲＨＮ４０３Ａにて復号できる暗号化データの形でコンテンツを所持可能とする狙いがある。災害などでオフラインになるときはＯＴＰ認証し閲覧できた事を証明する証明書データと秘密鍵４０１Ａを用いて閲覧を可能とし、常にインターネットワークへの接続を必要とせずコンテンツを利用できる。

本発明においてもブロックチェーンを構成する３Ａ、３Ｂなどのノードがすべてなくなってしまう場合にはＯＴＰトークンを支えるブロックチェーンのハードウェアがなくなり、サービスが終了することは起きえる。しかし３Ａや３Ｂのような端末を構成したいと思ったサーバ管理者がいたときには公開されたオープンソースのソフトウェアに沿ってノード端末３Ａを維持できる。

ＯＴＰトークンに結びつけられたデータやサービスに価値を見出してデータやサービスに対応するＯＴＰトークンを維持するためにノード端末３Ａをユーザーが用意して用意した端末がブロックチェーンの１つのノードになることができれば、そのブロックチェーンがサービスを終了しにくくするかもしれない。

ブロックチェーンの場合にはある会社のアプリケーションとは異なり世界中でノードとなる端末が存在しネットワーク２０を用いて接続されていれば動作させることができる。ブロックチェーンのノードが世界中に分散していれば地球上の局所的な災害に強いデータベースシステムになりうる。

【０５２４】

＜仮想機械環境での稼働＞

本発明のブロックチェーンは仮想的なサーバのネットワークで処理されることも考えられる。パーソナルコンピュータやサーバなどの電子計算機の端末はハードウェア面およびソフトウェア面での変化が激しく、例えば本発明では100年以上ＯＴＰトークンとそれにより暗号データを復号する形でのデータとその権利の流通システムを想定するが、たとえばＢＩＯＳやＥＦＩといったオペレーティングソフトウェアを起動させるソフトウェアそのものが変更され既存のオペレーティングソフトやウェブブラウザやブロックチェーンのクライアントソフトウェアが動作させることができなくなる恐れがある。ブロックチェー

ン基盤の公開鍵暗号方式や暗号学的ハッシュ関数の更新、共通鍵暗号方式の更新の可能性も考えられる。

そこでサーバ３Ａのみならずサーバ３Ｃといった分散型台帳システムのノード端末やウェブサービス端末を仮想機械環境で稼働させてもよい。互換性の問題から、サーバ端末のオペレーティングソフトウェアでブロックチェーンのクライアントソフトウェアが動作させることができなくなった場合に備え、仮想的なコンピュータ上やサーバ上、複数のサーバー上で動作するようにすることが好ましいかもしれない。（互換性の問題の例はウェブサイトを閲覧するインターネットプロトコルの変化、ＥＣＭＡＳｃｒｉｐｔなどプログラム言語の変化）

【０５２５】

＜長期の稼働＞

長期にわたり現実または仮想機械環境で利用されることも考慮し、ブロックチェーンシステムの消費する電力量は少ないほうが好ましく、Proof of AuthorityやProof of Stake などのProof of Workよりも低い消費電力であることが期待されるブロックチェーンシステムの合意形成アルゴリズムを用いることが好ましい。端末やネットワークを動かす電源装置には持続可能なエネルギーを利用することが望ましい。

サービス提供者はブロックチェーン上からサーバ３Ｆなどを用いてサービスに対応したＯＴＰトークンの持ち主の名簿を持ち、ブロックチェーンのみに依存せず持ち主の情報を名簿のように記憶できていることが好ましい。通常、実施例１や実施例２に示したウェブサイトへのログインやイベントなどでのチケットの用途、自動車や建物の鍵などは有限の期限（イベントの開催期限、自動車の耐用年数、ウェブサイト運営会社のログイン方法の変更等）があり、ヒトの寿命を超える前にサービスを提供する法的な根拠が無くなる用途が多い。

一方で実施例３に示す暗号化データを復号する用途ではヒトの寿命を超えて後世に残されることが想定される。既存の紙と墨で書かれた古文書や版画の浮世絵はヒトの寿命を超えて過去の出来事を伝えている。もし本発明がそれらのように長い期間にわたる場合には、ＯＴＰトークンが無ければ閲覧しにくい文章、音楽レコード、動画情報、コンピュータゲームソフトウェアが発生すると予想され、これらＯＴＰトークンは古書店などで暗号化データや復号用の情報と共に紙の古文書などと同じく古物として販売されうるかもしれない。

【０５２６】

＜ユーザーがシード値を変更できる場合＞

コントラクトにいくつかのシード値となる変数があり、一部はコントラクト管理者のみがアクセスでき、ほかの変数は全くコントラクトに関係ないユーザーが書き換えることの出来る変数と、トークンの持ち主が書き換えることのできる変数を用意し、ユーザーが任意時間、任意数値に変更できることで疑似的なランダム値になり得る。ユーザーのトークン番号に対応したワンタイムパスワード生成シード値を設定しそれをオンラインゲームなどでの擬似乱数の生成要素にすることもできる。またランダムさを用いるサービスとしてくじ引きなどにも利用されうる。

【０５２７】

＜ＯＴＰトークンを機密情報の暗号化を復号する鍵として流通させる可能性＞

ある団体においてＯＴＰトークンを付与したユーザーにのみ閲覧させたい平文データを暗号化させ、暗号化データとして配布し閲覧させることが可能になる。本発明では分散型台帳だけで復号を行う他に、団体内部で通用する外部パスワードＡＫＴＢを設定している。例としてある会社の社内において試作品の乗物の部品や模型などを３ＤのＣＡＤデータとして暗号化されたデータとして配布し、それを復号できるソフトウェアＣＲＨＮ４０３ＡとＯＴＰトークン（およびＯＴＰトークンで認証したときの戻り値ＣＴＡＵ）と外部パスワードＡＫＴＢを持つことの出来る社員が復号を行い閲覧することができ、その３ＤのＣＡＤデータを基に部品や模型などを作製しうる。

機密情報のＯＴＰトークンはユーザー端末１Ａ（端末ＤＡ）の秘密鍵に紐づけられる。こ

こで端末１Ａ（または４Ａ）の外部記録装置１６Ａとして個人番号カードやＩＣカード型社員証・学生証などに割り当てられた秘密鍵を記録したＩＣカードを接続し通信させ、ＩＣカード内の秘密鍵により重要情報、個人情報、個人の記録、機密情報の暗号化を行うことも意図している。（この場合秘密鍵を記録したＩＣカードなどが破損・紛失した場合に秘密鍵を無くしてしまう恐れがあり、ＩＣカード発行者が秘密鍵を記憶装置に複製し、前記記憶装置をインターネットからアクセスされないデータセンターや金庫などに保管し管理することが必要になる恐れもある。）

【０５２８】

＜暗号化データ放送の復号を行う閲覧権としての販売＞

アマチュア無線・業務用無線などで放送や通信を行う際に本発明のトークンを用いて暗号化したラジオやテレビジョンの視聴権をＯＴＰトークンとしてやり取りできるかもしれない。地上波、衛星放送、有線放送、インターネット放送を含む分野で暗号化放送を復号して視聴することを可能とするＯＴＰ認証システムを提供できるかもしれない。例としてある国Ａと別の国Ｂで放送されている番組の視聴権を契約又は売買等して閲覧するということが可能になるかもしれない。またアマチュア無線の個人局、社団局においても無線情報を暗号化して放送できる。業務用に工場や会社の社屋内で通信する際にも利用できる。

【０５２９】

＜衛星放送において暗号化データ放送の復号を行うスクランブル放送閲覧権としての販売＞

地上における携帯電話機やスマートフォンといった無線通信機器の利用には電波帯の確保が必要かもしれない。衛星放送では宇宙空間より地上に向け放送するため人工衛星を宇宙空間に展開できれば地上の電波資源を消費せずに宇宙空間からデータ放送を行え、データ放送時に放送の閲覧権として利用できるかもしれない。

【０５３０】

＜衛星放送の閲覧権としてのＯＴＰトークンと電波資源の関係＞

宇宙空間に多数の人工衛星による通信および放送ネットワークがあって、地上において端末４Ａが人工衛星型の放送局５Ｃからの暗号化データを無線放送により取得できるとき、暗号化データ（雑誌・新聞等データ、ソフトウェアデータの情報等を含む）を放送し、それらデータを受信した端末４Ａの秘密鍵４０１Ａにデータの復号が可能なＯＴＰトークンがある場合に復号させ利用させるという形式も考えられる。なおこの時の暗号化の鍵ＴＴＫＹ（４０３３Ａ）は各放送コンテンツに対応するＯＴＰトークンごとに設定される。

具体的にはある新聞またはテレビジョンの暗号化データを放送するサービスに対応したＯＴＰトークンがありそれを所持する人が端末４Ａに備え付けた受信機にて暗号データ放送に対応した帯域（チャンネル）において受信した暗号データをＯＴＰトークンで復号し閲覧視聴する。ＯＴＰトークンはサブスクリプションサービスにより定期購読もしくは定期視聴の契約が行われる。定期契約の契約終了後にＯＴＰトークンは利用ができなくなるように設定される。地上波放送を災害時の放送を含め既存の放送を行いつつ、より高付加価値または大容量でなおかつ新しい用途の放送・通信を宇宙空間の人工衛星網で行うことも検討されうる。

地上の携帯電話やスマートフォン、パーソナルコンピュータ、ＩｏＴデバイスといった端末の利用に必要な電波資源の有効利用と既存の放送を両立しつつ、電波資源を災害や日常生活での必要性に照らして有効活用する必要性があるとき、本発明のような暗号化データのアクセスコントロール技術とそれを権利化したＯＴＰトークンによる視聴権の流通が利用できるかもしれない。

【０５３１】

＜衛星放送網の番組の枠の配信権または配信するコンテンツをＯＴＰトークンとして流通させる場合＞

ある民間の衛星へ個人がアップリンク用の無線局へデータを個人が配布したいデータ送信し、人工衛星にアップリンクして送信した後、人工衛星からダウンリンクして地上の端末へ放送するということも考えられる（これもその権利をＯＴＰトークン化してもよい）

。例えば動画視聴サイトにてデータ量の多い動画データが世界中で配信されているが、そのデータトラフィックは無視できないかもしれない。無線によるネットワーク２０は電波資源を消費し、有線によるネットワーク２０は増大するトラフィックに対応するため光ファイバ等の増設を必要とする。仮に動画視聴に必要なデータが多くの人に消費されているコンテンツである場合、そのあるデータを動画サイトで双方向通信ネットワークで通信するよりも衛星放送の暗号データとして受信して記録したほうがネットワーク２０に対する負荷が少なくなるかもしれない。

あるいは双方向通信時の動画配信データにおいても同一のデータを何度も異なる人に応じて送信するよりは暗号データとして配布し、それをソフトウェア４０３Ａ上で広告配信及び不正利用監視サーバ５Ａに接続しながら視聴したほうがネットワーク２０に対する負担は少なくなるかもしれない。ＯＴＰトークンを動画のライブ配信視聴権として流通させ人工衛星からの放送とネットワーク２０からの放送を組み合わせ通信障害に強い動画のライブ配信等で用いられるかもしれない。

ある民間等の衛星放送の受信範囲にある地域（複数の国家を対称として含む）において地域に住むユーザーに向けてＯＴＰトークンを販売配布したうえで暗号化データを放送するスクランブル放送が存在できるかもしれない。

【０５３２】

本発明ではヘッドマウントディスプレイ４５３Ａ に生体認証機能４５３０Ａ を備えさせ、暗号化されたデータを復号して閲覧させる際に暗号化させたデータを閲覧している人の生体データを直接またはハッシュ化などを行い間接的に取得し簡易に認証を行い閲覧可能となりうる。

ここでヘッドマウントディスプレイ４５３Ａは携帯端末やタブレットパソコン、テレビジョン視聴用ディスプレイよりも画面が小さく、携帯端末やデジタルカメラでは４５３Ａに映し出される復号したデータによるコンテンツ（映像、画像、文章）を撮影することが困難にする。端末４Ａにおいてソフトウェアｃｒｈｎ４０３Ａが４５３Ａが接続されている場合に限り動作するようプログラムし、暗号化データを復号して得られたコンテンツの撮影を防ぐ認証システム及び暗号化データ復号閲覧システムとすることもできる。

生体認証装置４５３０Ａでは温度センサを用いて体温を測定してもよく。点状、1次元、2次元のサーモグラフィを４５３Ａの装着者の頭部や目元から得て装着している人がいることと、その装着している人の特徴を検出する。また頭部の顔の形状に関する認証、目に関する生体認証、耳の構造に由来する生体認証、頭部の形状に由来する生体認証、まばたきに関する生体認証を用いてもよい。

【０５３３】

＜暗号化データソフトウェアを用いてネットワーク上の通信を暗号化する場合＞

ソフトウェアｃｒｈｎ４０３Ａのブロックチェーンを用いた平文データの暗号化機能と暗号化データの復号機能を用いてネットワーク２０に接続された端末間での通信を暗号化する事もできる。

【０５３４】

＜ＢｎＴＯＴＰをタイムスタンプとして使う場合＞

ＢｎＴＯＴＰを生成した場合のＫＣ値やＢＣ値を除くシード値の入力を求める認証関数を用いて、ＢｎＴＯＴＰによるとＯＴＰを生成した際にブロック番号Ｂｎとユーザ識別子Ａとトークン番号ＴＩＤＡが記録された箇所が果たしてそのブロック番号に固有のＯＴＰを記録したタイムスタンプとして機能しているか検証できる。ここで記録する箇所は認証を行う端末１Ａ記憶装置内のデータでもよいし端末１Ａが文章データを紙などに印刷する際に付加して印刷してもよい。このときサーバ端末３Ａのブロックチェーン部に存在するＯＴＰ生成コントラクトとＯＴＰ認証コントラクトは簡易なタイムスタンプサーバとして機能する。

【０５３５】

タイムスタンプの例の一つとして次のＢｎＴＯＴＰを計算してＯＴＰの生成と認証を行う場合を考える。

ＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）
それに対応する認証関数の引数は例として秘匿化されるシークレット変数ＫＣを除いて（Ａ，ＴＩＤＡ，Ｂｎ）となる。
この時、前記ＢｎＴＯＴＰはＫＣは秘匿化されており、ユーザ端末１ＡにてＯＴＰ生成関数を実行し、ＯＴＰ取得時のブロック番号Ｂｎとユーザー識別子Ａとトークン番号ＴＩＤＡと、秘密にされているＫＣから計算されるＢｎＴＯＴＰを取得する。そして端末１Ａは平文のデータにＡ，ＴＩＤＡ，Ｂｎ，ＢｎＴＯＴＰを記録しそのファイルに電子署名を行いデータの改ざん検知できるようにする。あるいは印刷用データにＡ，ＴＩＤＡ，Ｂｎ，ＢｎＴＯＴＰを付加して頁の下部などに書き込み簡易のタイムスタンプとし、印刷を実行し、ブロック番号Ｂｎの時刻に近い時に印刷されたと推測される印刷物を作成できる。電子署名に用いる秘密鍵はブロックチェーンにアクセスするための１０１Ａでもよいし公的機関や民間団体が発行した秘密鍵でもよい。この用途においてはＫＣ値を変更する事は好ましくないかもしれない。

【０５３６】
次に他のタイムスタンプの例として次のＢｎＴＯＴＰを計算してＯＴＰの生成と認証を行う場合を考える。
ＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ、Ｖ）
それに対応する認証関数の引数は例として秘匿化されるシークレット変数ＫＣを除いて（Ａ，ＴＩＤＡ，Ｂｎ，Ｖ）となる。
この時、前記ＢｎＴＯＴＰはＫＣは秘匿化されており、ユーザ端末１ＡにてＯＴＰ生成関数を実行し、ＯＴＰ取得時のブロック番号Ｂｎと投票によって決まる値Ｖとユーザー識別子Ａとトークン番号ＴＩＤＡと、秘密にされているＫＣから計算されるＢｎＴＯＴＰを取得する。そして端末１Ａは平文のデータにＡ，ＴＩＤＡ，Ｂｎ，Ｖ，ＢｎＴＯＴＰを記録しそのファイルに電子署名を行いデータの改ざん検知できるようにする。
あるいは印刷用データにＡ，ＴＩＤＡ，Ｂｎ，Ｖ，ＢｎＴＯＴＰの５つをタイムスタンプデータとして付加し頁の下部などに書き込み簡易のタイムスタンプとし、印刷を実行し、ブロック番号Ｂｎの時刻に近い時に印刷されたと推測される印刷物を作成できる。Ｖ値を疑似ランダム値およびタイムスタンプ値の一つにとして用いることでそのデータや文章が端末１ＡがＢｎＴＯＴＰを取得した時刻に存在して電子署名が行われている事が分かる。端末１Ａにプリンタが接続されている場合には印刷時にＡ，ＴＩＤＡ，Ｂｎ，Ｖの５つをタイムスタンプとして印刷することで印刷時の時刻が認証できる。
端末１Ａがプリンターに内蔵されたコンピュータである場合、プリンターそのものがネットワーク２０を通じてサーバ端末３ＡのブロックチェーンのＯＴＰ生成コントラクトにアクセスし、Ａ，ＴＩＤＡ，Ｂｎ，Ｖの５つを印刷する機能を備え、ユーザーの求めに応じてプリンター内部で印刷を行う度にＡ，ＴＩＤＡ，Ｂｎ，Ｖ，ＢｎＴＯＴＰの５つを印刷物の頁の最下部に記録させることもできる。ブロックチェーンのＯＴＰコントラクトと連携し簡易的なタイムスタンプを印刷物に付与しながら印刷できるタイムスタンプ機能付きプリンター端末１Ａを利用できる。この用途においてはＫＣ値を変更する事は好ましくないかもしれない。

【０５３７】
＜ＢｎＴＯＴＰを有価紙葉のタイムスタンプ及びＯＴＰ認証情報として使う場合＞
ＢｎＴＯＴＰを用いて簡易的なタイムスタンプをデータに負荷して記録したり、紙などに文章と共に印刷することについて述べたが、タイムスタンプに記載されるＡ，ＴＩＤＡ，Ｂｎ，ＢｎＴＯＴＰや、Ａ，ＴＩＤＡ，Ｂｎ，Ｖ，ＢｎＴＯＴＰの情報はＯＷＰを用いる紙のチケットに記入する情報Ａ，ＴＩＤＡ，ＯＷＰの３つの情報にブロック番号ＢｎやＶを加え、それを認証関数において認証関数の引数として読み取れるようにしたものである。
従ってＯＷＰ型以外にもＢｎＴＯＴＰ型の紙のチケットおよび有価紙葉を作成する事ができる。実施例２ではＯＷＰを用いて認証を行っている。それを変更しＯＴＰの計算式をＢｎＴＯＴＰ＝ｆｈ（Ａ，ＴＩＤＡ，ＫＣ，Ｂｎ）としたとき、生成関数から取得したＯＴ

ＰとブロックチェーンアドレスＢｎとユーザー識別子Ａとトークン番号ＴＩＤＡを端末１Ａの記憶装置１０Ａに記憶し、１０Ａに記録したＡ，ＴＩＤＡ，Ｂｎ，ＢｎＴＯＴＰの４つの情報をプリンタを用いて紙に文字列やバーコードとして印刷し記録させ有価紙葉１８Ａとして利用することもできる。あるいはＮＦＣタグ１９Ａに通信装置１２Ａを経由してＡ，ＴＩＤＡ，Ｂｎ，ＢｎＴＯＴＰの４つの情報を書き込んでもよい。

【符号の説明】

【０５３８】

１Ａ　ユーザーＵＡの端末となる端末ＤＡ、端末１Ａ（電子計算機ＤＡ、電子計算機１Ａ。）

１０Ａ　端末１Ａの記憶部　（記録装置、記録部、ＲＯＭやＲＡＭを含む）

１０１Ａ　端末１Ａに記録されたユーザーの秘密鍵ＰＲＶＡ

１０１Ａ２　端末１Ａに記録されたユーザーの秘密鍵ＰＲＶＡ２

１０２Ａ　端末１Ａがネットワークを介してサーバＰなどのブロックチェーン部に１０１Ａの秘密鍵ＰＲＶＡを用いてアクセスするためのブロックチェーンプログラム。

ここで１０２Ａのプログラムはブロックチェーンの識別子（ブロックチェーンの識別情報。ネットワークＩＤ、チェインＩＤ等を含む）と、

アクセス先ノードとなるサーバ端末３Ａを示すＵＲＩ情報を含むこともできる。

１１Ａ　端末１Ａの制御部

１１０Ａ　端末１Ａのブロックチェーンへアクセスする制御処理部

１２Ａ　端末１Ａの通信装置（入出力装置のうちの一つと考えることもできる）

１２０Ａ　端末１Ａの近距離無線通信（ＮＦＣ装置）

１２１Ａ　端末１Ａの無線通信装置

１２２Ａ　端末１Ａの有線通信装置（必要な場合）

１２３Ａ　端末１Ａの放送受信装置（必要な場合。ＧＮＳＳや、データ放送の受信装置を含む。無線の放送受信装置は無線通信装置に含まれていてもよい）

１３Ａ　端末１Ａの制御および演算装置

１４Ａ　端末１Ａの入力装置

１４０Ａ　端末１Ａキーボード

１４１Ａ　端末１Ａのポインティングデバイス（マウス、タッチパネルなど入力装置）

１４２Ａ　端末１Ａのカメラもしくはスキャナ（光子を検出する固体撮像素子、イメージセンサ）

１４３Ａ　端末１Ａのマイク　（音センサ）

１４４Ａ　端末１Ａのセンサ（加速度計、ジャイロセンサ、磁気センサは3次元の物理的な量を計測できてもよい。センサのうち一種類または複数種類を用いてもよい）

１４４０Ａ　端末１Ａの環境センサ（温度センサまたは湿度センサまたは気圧センサまたは圧力センサまたは照度センサまたは光センサ、化学センサ、においセンサ）

１４４１Ａ　端末１Ａの端位置センサ（磁気センサまたは地磁気センサ・磁気コンパスまたは加速度計）

１４４２Ａ　端末１Ａのモーションセンサ（加速度計またはジャイロセンサ）

１４４３Ａ　端末１Ａの生体認証センサ（必要な場合に利用。顔の情報、体温又はサーモグラフィ、声、耳の構造、手の構造、指紋、静脈等パターンを読み出せるセンサ。）

１５Ａ　端末１Ａの出力装置

１５０Ａ　端末１Ａのディスプレイ

１５００Ａ　端末１Ａのディスプレイに表示されたチケット、有価紙葉１８Ａの画像、ＯＴＰ認証用情報

１５１Ａ　端末１Ａのスピーカー

１５２Ａ　端末１Ａのプリンタ（プリンター）

１６Ａ　　端末１Ａの外部記憶装置および外部入出力装置、外部コンピュータ端末
１６００Ａ　端末１ＡのＩＣカードの読出し装置（接触式ＩＣカードリーダ、非接触式ＩＣカードリーダー）
１６０１Ａ　端末１Ａの接触式または非接触式のＩＣカード、非接触式ＩＣタグ
１６０２Ａ　端末１ＡのＩＣに内蔵された秘密鍵１０１Ａ等
１６０３Ａ　端末１Ａの無線ないし有線によりＤＡと接続される記録装置ＤＷＡＬＴ（外部接続型ハードウェアウォレットＤＷＡＬＴ、ＩＣカード型、ドングル型など含む）
１６０４Ａ　端末１ＡのＤＷＡＬＴ１６０３Ａ に記録された秘密鍵１０１Ａ、もしくは秘密鍵１０１Ａを含んだソフトウェア
１６０５Ａ　端末１ＡのＤＷＡＬＴ１６０３Ａ に記録された秘密鍵処理ソフトウェア
１６０６Ａ　端末１ＡのＤＷＡＬＴ１６０３Ａ の制御演算装置、処理装置（ＤＷＡＬＴを制御するＩＣチップ群、ＭＣＵなど）
１６０７Ａ　端末１ＡのＤＷＡＬＴ１６０３Ａ の入出力装置、通信装置
１６０８Ａ　プリンタもしくはヒトの手で紙や金属板などに印刷もしくは印字・刻印・記録された秘密鍵１０１Ａ。（文字列やバーコードの形で紙や金属板・石板などに記録されていてもよい。）
１７Ａ　　端末１Ａの電源装置（※本発明の装置について、前提としてコンピュータやサーバー端末、入出力装置、外部記憶装置、ネットワークは電源装置を持ち電力で駆動している。）
１８Ａ　　端末１Ａのプリンタで紙などに印刷されたチケット、有価紙葉
１８０Ａ　　１８Ａに記載の本発明のワンタイムタイムパスワード認証に必要なバーコードまたは文字列またはその両方の印刷情報
１８１Ａ　　１８Ａに記載バーコードまたは文字列またはその両方に含まれるトークン番号ＴＩＤＡの情報
１８２Ａ　　１８Ａに記載バーコードまたは文字列またはその両方に含まれるパスワードＯＷＰの情報
１８３Ａ　　１８Ａに記載バーコードまたは文字列またはその両方に含まれるユーザー識別子Ａの情報
１８４Ａ　　１８Ａに記載のチケットまたは有価紙葉として利用するために必要な情報、図柄等。
１９Ａ　　有線通信型又は近距離無線通信型のＩＣカード、ＩＣタグ型チケット等有価紙葉または施錠解錠等する鍵（主としてＮＦＴタグ、ＮＦＣカード型チケット）
１９０Ａ　　１９Ａに記載の記憶装置
１９１Ａ　　１９Ａに記載の制御処理装置
１９２Ａ　　１９Ａに記載の通信装置
１９３Ａ　　１９Ａに記載の制御演算装置
１９４Ａ　　１９Ａに記載の入力装置
１９５Ａ　　１９Ａに記載の出力装置
１９７Ａ　　１９Ａに記載の電源装置
１Ｂ　ユーザーＵＢの端末ＤＢ、端末１Ｂ。１Ｂはスマートフォン等の携帯可能な端末でもよい。端末ＤＢはＤＡと同様の機能を持ち、本発明の認証に用いるトークンを保有・利用するユーザー端末。
１０Ｂ　端末１Ｂの記憶装置
１０１Ｂ　端末１Ｂに記録されたユーザーの秘密鍵ＰＲＶＢ
１０２Ｂ　端末１Ｂがネットワークを介してサーバＰなどのブロックチェーン部に１０１Ａの秘密鍵ＰＲＶＢを用いてアクセスするためのプログラム。
　　ここで１０２Ｂのプログラムはブロックチェーンの識別子（ブロックチェーンの識別情報。ネットワークＩＤ、チェインＩＤ等を含む）と、

アクセス先ノードとなるサーバ端末３Ａを示すＵＲＩ情報を含むこともできる。
１１Ｂ　端末１Ｂの制御部
１１０Ｂ　端末１Ｂのブロックチェーンへアクセスする制御処理部
１２Ｂ　端末１Ｂの通信装置
１３Ｂ　端末１Ｂの制御および演算装置
１４Ｂ　端末１Ｂの入力装置（入力装置に環境センサ、モーションセンサ、位置センサを備えている。例として温度センサや地磁気センサ・磁気コンパス・デジタルな方位磁針装置を備えている。）
１５Ｂ　端末１Ｂの出力装置
１６Ｂ　端末１Ｂの外部記憶装置および外部入出力装置、外部コンピュータ
１７Ｂ　端末１Ｂの電源装置
１Ｃ　本発明のワンタイムパスワードに関するコントラクトを管理するユーザーＵＣのコンピュータ端末ＤＣ、端末１Ｃ
１０Ｃ　端末１Ｃの記憶装置
１０１Ｃ　端末１Ｃに記録されたユーザーの秘密鍵ＰＲＶＣ
１０１Ｃ2　端末１Ｃに記録されたユーザーＵＣの任意の第二の秘密鍵ＰＲＶＣ2
１０２Ｃ　端末１Ｃがネットワーク２０を介してサーバＰなどのブロックチェーン部に１０１Ｃの秘密鍵ＰＲＶＣを用いてアクセスするためのプログラム。
ここで１０２Ｃのプログラムはブロックチェーンの識別子（ブロックチェーンの識別情報。ネットワークＩＤ、チェインＩＤ等を含む）と、
アクセス先ノードとなるサーバ端末３Ａを示すＵＲＩ情報を含むこともできる。
１１Ｃ　端末１Ｃの制御部
１１０Ｃ　端末１Ｃブロックチェーンへアクセスする制御処理部
１２Ｃ　端末１Ｃの通信装置
１３Ｃ　端末１Ｃの制御および演算装置
１４Ｃ　端末１Ｃの入力装置
１５Ｃ　端末１Ｃの出力装置
１６Ｃ　端末１Ｃの外部記憶装置または外部コンピュータ（秘密鍵の記憶が可能なＩＣカード、ＩＣタグ、ＮＦＣカード、ＮＦＣタグでもよい。）
１７Ｃ　端末１Ｃの電源装置
２　通信網、ネットワーク
２０　暗号化通信を行える通信経路、ネットワークＮＴ　（有線又は無線式の双方向通信経路であり、サーバー及び端末が通信網を介して接続されている。暗号化を行う通信と暗号化しない通信を行える）
２１　放送による通信経路ＮＴＢ　（有線もしくは無線放送式の情報の送信経路であり、一対複数の一方向通信が行える。情報の送信者は放送局で複数のユーザーの受信機に情報をリアルタイムに送付する）
２２　暗号化されていないネットワークＮＴＰ（有線もしくは無線式の双方向通信経路。暗号化は行われていないので、必要に応じて平文のメッセージデータを暗号化しなければいけない。）
３Ａ　サーバＰ、サーバ端末３Ａ　（ユーザーの接続する分散型台帳システムのノードとなる端末。　他のノードと分散型台帳部を共有。ある端末内に構築された仮想サーバでもよい。）
３０Ａ　サーバ端末３Ａのサーバ記憶部（サーバＰの記憶装置）
３００Ａ　サーバ端末３Ａの分散型台帳記録部　（３００Ａはブロックチェーン型もしくはＤＡＧ型の分散型台帳もしくは分散型台帳の記録部となる）
３０００Ａ　３００Ａに記録された最新のブロックデータ
３００１Ａ　３００Ａに記録された最新のブロックにおけるブロック番号Ｂｎ

３００２Ａ　３００Ａに記録された最新のブロックまたはシステムにおけるタイムスタンプ値
３００３Ａ　３００Ａに記録された最新のブロックにおけるハッシュ値Ｂｈ
３００４Ａ　３００Ａに記録されたブロックチェーンを構成するノード間の投票で決まる値Ｖ
３００５Ａ　３００Ａに記録されたブロックチェーンのブロックサイズ値ＢＳＺ（実施例ではＢｌｏｃｋＧａｓＬｉｍｉｔ値）
３００６Ａ　３００Ａに記録されたブロックチェーンデータ部（３００Ａに記録された分散型台帳のデータ部。３００８Ａ・３００８ＡＧ・３００８ＡＡ等のコントラクトデータを記録した部分）
３００７Ａ　３００Ａに記録されたブロックチェーンの基礎情報（ブロックチェーンが何秒ごとに連結されるか記録したデータを含む）
３００８Ａ　３００Ａに記録された認証関数を持つＯＴＰ生成コントラクト（ワンタイムパスワード：ＯＴＰ）
３００８ＡＧ　３００Ａに記録されたＯＴＰ生成コントラクト
３００８ＡＡ　３００Ａに記録されたＯＴＰ認証コントラクト
３００９Ａ　３００Ａに記録されたＯＴＰ生成関数
３０１０Ａ　３００Ａに記録されたＯＴＰの生成と認証に用いるハッシュ関数ｆｈ
３０１１Ａ　３００Ａに記録されたシークレットキー変数ＫＣ
３０１２Ａ　３００Ａに記録された変数ＫＣと変数ＢＣのいずれかまたは両方を任意のブロック番号において利用できる関数ｆｓｃｂ
３０１３Ａ　３００Ａに記録されたコントラクト管理者であるユーザー識別子Ｃのみが変えることのできる変数ＢＣ
３０１４Ａ　３００Ａに記録された３００８において発行されるトークンのトークン番号とその持ち主であるユーザー識別子を対応付けたデータベース
３０１５Ａ　前記３０１４Ａにおいて、ユーザーＵＡの秘密鍵ＰＲＶＡ１０１Ａから計算されるユーザー識別子Ａとトークン番号ＴＩＤＡと対応付けられた情報
３０１６Ａ　前記３０１４Ａにおいて、ユーザーＵＢの秘密鍵ＰＲＶＢ１０１Ｂから計算されるユーザー識別子Ｂとトークン番号ＴＩＤＢと対応付けられた情報
３０１７Ａ　３００Ａに記録されたＯＴＰＣＴ（ＯＴＰ生成及び認証関数の実行回数等記録する部分。実施例ではトークン番号をキー、実行回数を値としたマッピング変数ＯＴＰＣＴを用いた）
３０１７ＡＧ　３００Ａに記録されたＯＴＰＣＴＧ（ＯＴＰ生成関数の実行回数記憶部・記録部。実施例ではトークン番号をキー、実行回数を値としたマッピング変数を用いた。）
３０１７ＡＡ　３００Ａに記録されたＯＴＰＣＴＡ（ＯＴＰ認証関数の実行回数記憶部・記録部。実施例ではトークン番号をキー、実行回数を値としたマッピング変数を用いた。）
３０１８Ａ　３００Ａに記録されたＯＴＰ認証関数
３０１９Ａ　３００Ａに記録されたＯＴＰ生成コントラクト識別子ＣＰＧＴ
３０２０Ａ　３００Ａに記録されたＯＴＰ認証コントラクト識別子ＣＰＡＴ
３０２１Ａ　３００Ａに記録されたＯＴＰ認証関数の戻り値またはデータ
３０２２Ａ　３００Ａに記録されたＯＴＰ認証関数実行時の処理内容、処理用関数など（例として銀行口座間での送金処理、会員サイトでの投票処理など）
３０２３Ａ　３００Ａに記録されたＯＴＰ認証関数で認証できた場合の処理に応じて書き換える変数またはデータベース（例として銀行口座の残高であって、銀行内の送金処理で書き換える口座残高）
３０２４Ａ　３００Ａに記録されたコントラクトの看板情報ＫＮＢＮ（コントラクト名、作成者情報、管理者情報と連絡先、レイティング等を含み、それらを変更するセッター関数を備える）

３０３０Ａ　３００Ａに記録されたブロック番号剰余変数ｍ及びそのセッター関数（ＯＴＰ認証期間延長用変数及び関数）
３０３１Ａ　３００Ａに記録されたＯＴＰ桁数調整用整数ｎ及びそのセッター関数（ＯＴＰ文字数・桁数の増減用変数及び関数）
３０４０Ａ　３００Ａに記録されたトークン送信関数（トークン譲渡用関数）
３０４１Ａ　３００Ａに記録された譲渡制限用変数ｔｆ、ａｆ及びそれらのセッター関数
３０４２Ａ　３００Ａに記録されたコントラクト管理者秘密鍵漏洩対策部分
３０１Ａ　サーバ端末３Ａのサーバの基礎的な制御プログラム記録部
３１Ａ　サーバ端末３Ａのサーバ制御部（サーバＰの制御装置）
３１０Ａ　サーバ端末３Ａの分散型台帳システム制御部（ブロックチェーン制御処理部もしくはＤＡＧ型分散型台帳制御処理部）
３１１Ａ　サーバ端末３Ａのサーバの基礎的な制御部
３２Ａ　サーバ端末３Ａの通信装置、通信制御装置（サーバＰの通信装置）
３３Ａ　サーバ端末３Ａの処理及び制御演算装置　（サーバＰの制御部、処理部、演算部装置）
３４Ａ　サーバ端末３Ａの入力装置（サーバＰの入力装置）
３５Ａ　サーバ端末３Ａの出力装置（サーバＰの出力装置）
３７Ａ　サーバ端末３Ａの電源装置（サーバＰの電源装置、サーバＰを動作させる動力源）
３Ｂ　サーバ端末３Ｂ（サーバ端末Ｂ）、およびサーバ端末３Ｂやサーバ端末３Ａと同じくブロックチェーンのノードになりうるサーバ群
３０Ｂ　サーバ端末３Ｂ のサーバの記憶部　（記憶部はサーバ３Ａと同じ３００Ａを持つ）
３１Ｂ　サーバ端末３Ｂ のサーバの制御部　（制御部はサーバ３Ａと同じ３１０Ａを持つ）
３２Ｂ　サーバ端末３Ｂ の通信装置
３３Ｂ　サーバ端末３Ｂ の制御および演算装置
３４Ｂ　サーバ端末３Ｂ の入力装置
３５Ｂ　サーバ端末３Ｂ の出力装置
３７Ｂ　サーバ端末３Ｂ の電源装置
３Ｃ　サーバＳＶＬｏｇｉｎ、サーバ端末３Ｃ（主にウェブサイトログインの場合に用いる端末。ウェブサイトなどウェブサービスを提供する端末。ある現実の端末内の仮想サーバ端末でもよい。）
３０Ｃ　サーバ端末３Ｃ の記録部
３００Ｃ　端末３Ｃ のブロックチェーン記録部（必要な場合。３００Ａと３００Ｃは同じ）
３０１Ｃ　端末３Ｃ のサービス用プログラム及び記録部
３０１０Ｃ　端末３Ｃ のＳＶＬｏｇｉｎの基礎プログラム（ウェブサイト等にブロックチェーンへ接続するプログラムを含む。銀行や電子商取引等のサービスに固有の機能を備えていてもよい）
３０１１Ｃ　端末３Ｃのアクセス検出及び監視用データベース（データ構造は図６Ｘ参照。ログイン時の時刻、ユーザー・トークン情報、ＩＰＶ値、現在のサービス状態を随時記憶し監視する。）
３０１２Ｃ　端末３Ｃの不正アクセス検出プログラム
３０１３Ｃ　端末３Ｃの不正アクセス通知プログラム（登録されたメールアドレスに連絡を行い、ユーザー識別子に対し専用通知トークンを送付する、トランザクションを送り異常を知らせる。）
３０１４Ｃ　端末３ＣのＯＴＰＣＴ変化検出部（必要な場合。ＯＴＰ生成または認証コントラクトの実行回数の変化を検出する部分）

３０１５Ｃ　端末３ＣのＯＴＰＣＴ変化通知部（必要な場合。ＯＴＰ生成または認証コントラクトの実行回数の変化を通知する部分）
３０１６Ｃ　端末３Ｃの顧客情報データベース（必要な場合。サービスの購入履歴等、利用資格のあるユーザー識別子やトークン番号を記録。）
３１Ｃ　端末３Ｃのサーバ制御部
３１０Ｃ　端末３Ｃのブロックチェーン制御部（必須ではない。３１０Ａと３１０Ｃは同じ）
３１１Ｃ　端末３Ｃのログイン及びサービス制御部
３１１０Ｃ　端末３ＣのＳＶＬｏｇｉｎの基礎プログラム制御部（ウェブサイトもしくはウェブアプリにブロックチェーンへ接続するプログラムを含む）
３１１１Ｃ　端末３Ｃのアクセス検出及び監視用データベース（データ構造は図６Ｘ参照。ログイン時の時刻、ユーザー・トークン情報、ＩＰＶ値、現在のサービス状態を随時記憶しモニタリングする。）
３１１２Ｃ　端末３Ｃの不正アクセス検出プログラム（同じユーザー識別子またトークン番号情報に対し異なるＩＰアドレスやセンサ値などＩＰＶ値によるアクセスがあるか検出する）
３１１３Ｃ　端末３Ｃの不正アクセス通知プログラム（登録されたメールアドレスに連絡を行い、ユーザー識別子に対し専用通知トークンを送付する、トランザクションを送り異常を知らせる。）
３１１４Ｃ　端末３ＣのＯＴＰＣＴ変化検出部（必要な場合。ＯＴＰ生成または認証コントラクトの実行回数の変化を検出する部分）
３１１５Ｃ　端末３ＣのＯＴＰＣＴ変化通知部（必要な場合。ＯＴＰ生成または認証コントラクトの実行回数の変化を通知する部分）
３１１６Ｃ　端末３Ｃの顧客情報データベース（必要な場合。サービスの購入履歴等、利用資格のあるユーザー識別子やトークン番号といった情報を記録。）
３２Ｃ　端末３Ｃの通信装置、通信制御装置
３３Ｃ　端末３Ｃの制御および演算装置
３４Ｃ　端末３Ｃの入力装置
３５Ｃ　端末３Ｃの出力装置
３７Ｃ　端末３Ｃの電源装置
３Ｄ　サーバＳＶＬｏｇ、端末３Ｄ　（１９Ａや１８Ａと１５００Ａを認証する端末。アクセス制御端末３Ｄ。３Ｄはサーバ端末もしくはコンピュータ端末または組み込みシステム型端末）
３０Ｄ　端末３Ｄのサーバ記憶部（３０ＤにはＯＴＰ認証関数とＯＴＰ認証関数の計算に用いる変数や関数が記録される）
３００Ｄ　端末３Ｄのブロックチェーン記録部（必要な場合。　３００Ａと３００Ｄは同じ）
３０１Ｄ　端末３Ｄのサービス用プログラム及び記録部
３０１０Ｄ　端末３ＤのＳＶＬｏｇの基礎プログラム（ウェブサイトもしくはウェブアプリにブロックチェーンへ接続するプログラムを含む）
３０１１Ｄ　端末３Ｄのアクセス検出及び監視用データベース（アクセス時の時刻またはアクセス回数またはユーザートークン情報または現在のサービス状態を随時記憶する）
３０１２Ｄ　端末３Ｄの不正アクセス検出プログラム（必要な場合。３０１１Ｄに入場者の風貌等情報や解錠者のＮＦＣタグ固有の装置ＩＤ番号等を含むとき、それを過去の情報と異なるか判断する）
３０１３Ｄ　端末３Ｄの不正アクセス通知プログラム（必要な場合。３Ｄを管理する人に異常を通知し、登録されたメールアドレス・ユーザー識別子に対し通知用トランザクションを送り異常を知らせる）
３０１４Ｄ　端末３ＤのＯＴＰＣＴ変化検出部（必要な場合。ＯＴＰ生成または認証

コントラクトの実行回数の変化を検出する部分。例として端末３Ｄの備えられた金庫や自動車では解錠の回数を記録する）
３０１５Ｄ　端末３ＤのＯＴＰＣＴ変化通知部（必要な場合。ＯＴＰ生成または認証コントラクトの実行回数の変化を通知する部分。３Ｄがオンラインの時ネットワークを介して解錠回数変化を知らせる）
３０１６Ｄ　端末３Ｄの顧客情報データベース（必要な場合。サービスの購入履歴等、利用資格のあるユーザー識別子やトークン番号を記録）
３０１０ＤＡ　３０Ｄに記録されたハッシュ関数ｆｈ
３０１１ＤＡ　３０Ｄに記録されたシークレット変数ＫＣ
３０１２ＤＡ　３０Ｄに記録された変数ＫＣまたは変数ＢＣのどちらかまたは両方を変更し更新するセッター関数ｆｓｃｂ（端末３Ｄの管理者によりアクセスされる）
３０１３ＤＡ　３０Ｄに記録されたコントラクト管理者によって変更される変数ＢＣ
３０１７ＤＡ　３０ＤにＯＴＰ認証関数の実行回数又は数値記録部（認証時のＯＴＰトークンの番号をキーとしたマッピング変数等で表現される。）
３０１８ＤＡ　端末３Ｄの３０Ｄに記録されたＯＴＰ認証関数（ノード端末３Ａで生成するＯＴＰと等しいＯＴＰを計算できる変数と関数と処理方法を備える）
３０２１ＤＡ　ＯＴＰ認証関数の戻り値又はデータＣＴＡＵ
３０２２ＤＡ　３０Ｄに記録されたＯＴＰ認証時の処理内容
３０２３ＤＡ　３０Ｄに記録されたＯＴＰ認証時の処理にて書き換える変数またはデータベース、
３１Ｄ　端末３Ｄのサーバ制御部
３１０Ｄ　端末３Ｄのブロックチェーン制御部（必須ではない。３１０Ａと３１０Ｄは同じ）
３１１Ｄ　端末３Ｄのログイン及びサービス制御部
３１１０Ｄ　端末３ＤのＳＶＬｏｇの基礎プログラム（ウェブサイトもしくはウェブアプリにブロックチェーンへ接続するプログラムを含む）
３１１１Ｄ　端末３Ｄのアクセス検出及び監視用データベース（データ構造は図６Ｘ参照。ログイン時の時刻、ユーザー情報、トークン番号、ＩＰＶ値、現在のサービス状態を随時記憶しモニタリングする。）
３１１２Ｄ　端末３Ｄの不正アクセス検出プログラム（必要な場合。）
３１１３Ｄ　端末３Ｄの不正アクセス通知プログラム（必要な場合。登録されたメールアドレスに連絡し、ユーザー識別子に対しトランザクションを送り異常を知らせる。）
３１１４Ｄ　端末３ＤのＯＴＰＣＴ変化検出部（必要な場合。ＯＴＰ生成または認証コントラクトの実行回数の変化を検出する部分）
３１１５Ｄ　端末３ＤのＯＴＰＣＴ変化通知部（必要な場合。ＯＴＰ生成または認証コントラクトの実行回数の変化を通知する部分）
３１１６Ｄ　端末３Ｄの顧客情報データベース（必要な場合。サービスの購入履歴等、利用資格のあるユーザー識別子やトークン番号を記録。）
３２Ｄ　端末３Ｄの通信装置、通信制御装置
３３Ｄ　端末３Ｄの制御および演算装置
３４Ｄ　端末３Ｄの入力装置
３４０Ｄ　端末３Ｄのカメラ等の文字列バーコード読取機（入場口、改札機等に設置しチケット等有価紙葉のバーコードもしくは文字列を読み取るカメラまたはスキャナ。光学撮像素子）
３４１Ｄ　端末３ＤのＮＦＣタグの信号受信部（３２Ｄと共有）
３４２Ｄ　端末３Ｄの入場者記録装置または入場者記録手段（防犯用カメラ等で入場または解錠者を記録する等。装置の代わりに人員を配置して入場者を観察し記録してもよい。）
３５Ｄ　端末３Ｄの出力装置
３５０Ｄ　端末３Ｄの開閉装置・ゲート装置・施錠装置・始動装置、施解錠装置、ア

クセス制御装置（施錠される対象は建物の扉、自動車等乗物、工作機械、金庫等の容器、電子計算機等装置を含む）
３５１Ｄ　端末３Ｄのランプなど発光素子、発光装置（認証後、入場できるユーザーには入場可能を示す色や文字を伝え、入場できない入場不可能であることを示す色や文字を光で伝える。）
３５２Ｄ　端末３Ｄのブザーなど発音素子、発音装置（認証後、入場できるユーザーには認証できた時の音を鳴らす。入場できないユーザーに対し、警告音を鳴らし、周囲に知らせる。）
３７Ｄ　端末３Ｄの電源装置
３Ｅ　サーバＳＶｔｋ、端末３Ｅ（端末１Ａが用いるチケット等１８Ａやチケット及び鍵となるＮＦＣタグ１９Ａのプレイガイド。端末４Ａが用いる４０３Ａ用の暗号化データのトークン等も販売可。）
３０Ｅ　端末３Ｅ のサーバの記憶部
３００Ｅ　端末３Ｅ のブロックチェーン記録部（必要な場合。３００Ａと３００Ｅは同じ）
３０１Ｅ　端末３Ｅ のトークン型チケット等発券情報（チケットを顧客に表示するウェブサイトもしくはアプリの情報や３００Ａ・３００Ｅを利用したトークンとサービスのデータベースを含む）
３１Ｅ　端末３Ｅ のサーバの制御部
３１０Ｅ　端末３Ｅ のブロックチェーン制御部（必要な場合。３００Ａと３１０Ｅは同じ）
３１１Ｅ　端末３Ｅ の発券処理制御部（ユーザの指示に応じてトークンを販売しブロックチェーンよりチケット等の券面情報を表示し印刷可能にする部分。３１２Ｅ、３１３Ｅ、３１４Ｅを内包。）
３１２Ｅ　端末３Ｅ のブロックチェーン部３００Ｅ及びサーバ３Ｅに設定されたチケットの有効期限や図柄や表示および印刷時刻、印刷時ブロック番号、タイムスタンプなどの情報を取得する部分
３１３Ｅ　端末３Ｅ の３１１Ｅ，３１２Ｅで処理された情報をアクセスを受けたユーザー識別子Ａのユーザーのディスプレイに描画しチケット等有価紙葉の画像もしくは文章データとする処理部
３１４Ｅ　端末３Ｅにアクセスするユーザ端末に３１３Ｅの画像もしくは文章データを紙１８Ａやタグ１９Ａなどに印刷記録する情報を送信またはウェブブラウザ等に印刷を許可し実行させる処理部
３２Ｅ　端末３Ｅ の通信装置
３３Ｅ　端末３Ｅ の制御および演算装置
３４Ｅ　端末３Ｅ の入力装置
３５Ｅ　端末３Ｅ の出力装置
３７Ｅ　端末３Ｅ の電源装置
３Ｆ　サーバＳＶｆｉｎｄ、端末３Ｆ（ブロックチェーン部のトランザクションやコントラクト及びユーザ識別子を検索し、利用を監視し通知可能な装置。）（ユーザーＯＴＰトークンの保有残高の検索確認・発行もでき、利用状態の検索と通知もできるブロックチェーン検索エンジン。）
３０Ｆ　端末３Ｆのサーバ記憶部
３００Ｆ　端末３Ｆのブロックチェーン記憶部（必要な場合。３００Ａと３００Ｆは同じ）
３０１Ｆ　端末３Ｆのブロックチェーン検索監視など基礎プログラム（検索やトランザクションなど監視、ユーザーの残高算出や出力等サービスを行うサービス提供用基礎部分。）（ウェブサイト等にブロックチェーンを接続するプログラムを含む。）

３０１０Ｆ　端末３Ｆのブロックチェーン監視部プログラム
３０１１Ｆ　端末３Ｆの状態変化検出部プログラム
３０１２Ｆ　端末３Ｆの状態変化通知部プログラム
３０１３Ｆ　端末３Ｆの状態変化通知先データベース
３０１４Ｆ　端末３Ｆのブロックチェーン検索プログラム
３０１５Ｆ　端末３Ｆのブロックチェーン検索情報表示プログラム
３０１６Ｆ　端末３Ｆのブロックチェーン検索情報データベース
３１Ｆ　端末３Ｆのサーバ制御部
３１０Ｆ　端末３Ｆのブロックチェーン制御部（必要な場合。３００Ａと３１０Ｆは同じ）
３１１Ｆ　端末３Ｆのブロックチェーン検索監視など基礎的な処理部・制御部
３１１０Ｆ　端末３Ｆの監視部
３１１１Ｆ　端末３Ｆの状態変化検出部
３１１２Ｆ　端末３Ｆの状態変化通知部
３１１３Ｆ　端末３Ｆの状態変化通知先登録部
３１１４Ｆ　端末３Ｆのブロックチェーン情報検索部
３１１５Ｆ　端末３Ｆのブロックチェーン検索情報表示部
３１１６Ｆ　端末３Ｆのブロックチェーン検索情報データベース処理部
３２Ｆ　端末３Ｆの通信装置
３３Ｆ　端末３Ｆの制御および演算装置
３４Ｆ　端末３Ｆの入力装置
３５Ｆ　端末３Ｆの出力装置
３７Ｆ　端末３Ｆの電源装置
４Ａ　ユーザーＵＰの端末となるコンピュータＤＰ、端末４Ａ（Ｐ：プレイヤー、再生機を備えたユーザー端末）
４０Ａ　端末４Ａの記録部　（コンピュータDPの記憶装置）
４０１Ａ　端末４Ａに記録されたユーザーの秘密鍵ＰＲＶＰ（ここでＰＲＶＰはＰＲＶＡと同じくユーザー識別子Ａを示す秘密鍵）
４０２Ａ　端末４Ａがブロックチェーンにアクセスするためのプログラム（ブロックチェーンのノード端末３ＡへアクセスするＵＲＩなどが記録されていてもよい）
４０３Ａ　端末４Ａの記録部４０Ａに記録された本発明を用いて暗号化ファイルを復号して閲覧するソフトウェアＣＲＨＮの情報、ソフトウェアＣＲＨＮのプログラムと関連データ。
４０３０Ａ　端末４Ａの４０３ＡのソフトウェアＣＲＨＮのプログラム情報（ソースコードが難読化または暗号化されている。４０３０Ａに含まれる変数も難読化または暗号化されている）
（ブロックチェーンのノード端末３ＡへアクセスするＵＲＩなどが４０３０Ａに記録されていてもよい）
（秘密鍵を直接入力する機能を備えてもよい。あるいはウォレットソフトウェア機能を備えてもよい）
４０３０１Ａ　４０３Ａに記載のソフトウェアアプリケーション専用の鍵を管理するコントラクトの識別子ＡＰＫＹ
４０３０２Ａ　４０３Ａに記載の内蔵した秘密鍵ＣＲＫＹ（ブロックチェーン部ＤＬＳにアクセスできる公開鍵暗号の秘密鍵でもよい。４０３０２Ａは４０３０Ａに内蔵され難読化または暗号化されている）
４０３０３Ａ　４０３Ａに記載のブロックチェーンから取得した鍵管理コントラクトの戻り値ＣＡＰＫＹ（必須ではないが、さらなるセキュリティ対策とするために設定できる）

４０３０３ＫＡ　４０３Ａに記載のソフトウェア内部のシークレット変数Ｋ４０３（Ｋ４０３は難読化または暗号化されている）
４０３１Ａ　ブロックチェーンから取得したＯＴＰ認証関数の戻り値ＣＴＡＵの端末４Ａにおける記憶部（ＣＴＡＵは認証関数の戻り値の管理者により変更されうる）
４０３２Ａ　ブロックチェーンおよびソフトウェアＣＲＨＮ４０３Ａの外部で設定されるパスワードＡＫＴＢの端末４Ａ内の記憶部（ＡＫＴＢは平文データ管理者により変更されうる）
４０３３Ａ　４０３Ａに記載の暗号化及び復号に用いる鍵情報ＴＴＫＹの記憶部（少なくともＣＴＡＵを含み、そしてＡＫＴＢを用い、さらにＣＲＫＹを用い算出される鍵情報。）
４０３４Ａ　４０３Ａに用いるソフトウェアＣＲＨＮで復号する暗号されたデータまたはファイルＥｎｃＤａｔａ（４０３４Ａは４０Ａに含まれていればよい。）
４０３４０Ａ　４０３４Ａの暗号化データ本体ＥｔＤａｔａ
４０３４１Ａ　４０３４Ａの平文データ発行者の暗号化データ４０３４Ａに対して付与した電子証明書ＥｎｃＣｅｒｔ（電子署名も含まれていてよい。ＭＡＣ値が含まれていてもよい。無くともよい。）
４０３５Ａ　４０３Ａに用いるソフトウェアＣＲＨＮで暗号化したい平文のデータまたはファイルＤｅｃＤａｔａ（４０３５Ａは４０Ａに含まれていればよい。ＤｅｃＤａｔａはアクセス制御される。）
４０３５０Ａ　４０３５Ａの平文データ本体ＣｔＤａｔａ
４０３５１Ａ　４０３５Ａの平文データ発行者の電子証明書ＤｅｃＣｅｒｔ（電子署名も含まれていてよい。無くともよい。）
４０３５２Ａ　４０３５Ａの平文データ監査証明書ＡｕｄｉｔＲａｔ（平文データが悪意のあるプログラムではないことを示す監査証明書。または第三者のレビュー結果とレイティング。あることが好ましい）
４０３６Ａ　４０Ａに記録された閲覧済みの証明書データＯＦＢＫＭＫ（ＯＴＰ認証済みのアクセス証明書データ。災害等オフライン時アクセス用データ。４０３６Ａは４０Ａに含まれていればよい。）
４０３６０Ａ　４０３６Ａに記録されたＣＴＴＫＹをＣＲＨＮのプログラムに内蔵した秘密鍵ＣＲＫＹ等で暗号化したＡＣＴＴＫＹ
４０３６１Ａ　４０３６Ａに記録されたＴＴＫＹを秘密鍵ＰＲＶＡで暗号化したデータＣＴＴＫＹ（４０３６Ａに含まれる情報。暗号化方式は公開鍵暗号化、共通鍵暗号化どちらでも可能。）
４０３６２Ａ　４０３６Ａに記録された閲覧時刻と閲覧ユーザー識別子などの情報
４０３６３Ａ　４０３６Ａに記録されたＨＭＡＣなど認証用情報
４０３６２ＫＡ　４０Ａに記録された証明書の本文データＣＨＴ４０３
４０３６３ＫＡ　４０Ａに記録された４０３６２ＫＡをメッセージとしたＨＭＡＣなど認証用情報
４０４Ａ　４０Ａに記録されたソフトウェアＣＲＨＮを動作させるオペレーティングシステム等管理プログラム
４０５Ａ　４０Ａに記録されたコンピュータＤＰの外部記録装置（不揮発メモリ、ハードディスク、光ディスクなど）
４１Ａ　端末４Ａの制御部
４１０Ａ　端末４Ａのブロックチェーンへアクセスする制御処理部
４１１Ａ　端末４ＡのソフトウェアＣＲＨＮの制御処理部
４２Ａ　端末４Ａの通信装置
４２０Ａ　通信装置４２Ａの近接無線通信装置（必要な場合）
４２１Ａ　通信装置４２Ａの無線通信装置
４２２Ａ　通信装置４２Ａの有線通信装置（必要な場合）
４２３Ａ　通信装置４２Ａの放送受信装置（必要な場合。時刻取得のためＮＩＴＺ、

ＪＪＹ、時刻及び位置情報測位用のＧＮＳＳの受信機、暗号化データ放送受信装置を含む。）
４３Ａ　端末４Ａの制御および演算装置
４４Ａ　端末４Ａの入力装置
４４０Ａ　端末４Ａのキーボード
４４１Ａ　端末４Ａのポインティングデバイス（マウスや接触画面等による入力装置）
４４２Ａ　端末４Ａのカメラもしくはスキャナ
４４３Ａ　端末４Ａのマイク
４４４Ａ　端末４Ａのセンサ（加速度計、ジャイロセンサ、磁気センサは3次元の物理的な量を計測できてもよい。センサのうち一種類または複数種類を用いてもよい）
４４４０Ａ　端末４Ａの環境センサ（温度センサまたは湿度センサまたは気圧センサまたは圧力センサまたは照度センサまたは光センサ、化学センサ、においセンサ）
４４４１Ａ　端末４Ａの位置センサ（磁気センサまたは地磁気センサまたは加速度計）
４４４２Ａ　端末４Ａのモーションセンサ（加速度計またはジャイロセンサ）
４４４３Ａ　端末４Ａの生体認証センサ（顔の構造、体温又はサーモグラフィ、目の構造、まばたき、声、耳の構造、手の構造、指紋、静脈等パターンを読み出せるセンサ）
４５Ａ　端末４Ａの出力装置
４５０Ａ　端末４Ａのディスプレイ（暗号化された動画データを表示する）
４５１Ａ　端末４Ａのスピーカー（暗号化された音楽データや動画データの音声を再生する）
４５２Ａ　端末４Ａのプリンタ（暗号化データのコンテンツ権利者の許可を得た場合には関連するデータを紙に二次元情報として印刷できる。プリンタの種類には立体を出力できる３Ｄプリンタも含む。）
４５３Ａ　端末４Ａのヘッドマウントディスプレイ（ＨＭＤ、頭部装着ディスプレイ。装着者に暗号化データのコンテンツを閲覧させたい場合に用いる。眼鏡型ディスプレイも可）
４５３０Ａ　端末４ＡのＨＭＤに付属の生体認証センサ。
４５３０Ａは装着者の複数の生体情報（顔の構造、体温又はサーモグラフィ、目の構造、まばたき、声、耳の構造、手の構造、目元静脈等パターン）を測定し、装着者の存在確認と生体認証を行う
４５３０Ａは４４４３Ａに記載のセンサと機能を共有していてもよい。
（ここで４５３０Ａのセンサは４５３Ａを補助する入力装置。装着者の存在を確認するためのセンサであり、生体認証機能は存在確認機能に付属するものである。）
（本発明では認証用途ではなく装着者の存在を確認する用途で、プライバシーに配慮するためにＨＭＤ装着者の目の周りの体温の測定やサーモグラフィー画像を用いることが想定される。）
（体温は赤外線温度センサをＨＭＤ内部に設置して、装着車の目や目の周りの皮膚温度を測定する。センサの測定点は1点でもよいし、2次元にセンサを配列させ線や画像の形で測定してもよい。）
（４５３０Ａのセンサは装着者の目元の温度分布、装着者の目の周りの顔のサーモグラフィーを測定してプライバシーに配慮した簡易な生体認証情報及び存在確認情報として利用する。）
（ＨＭＤのセンサが検出した温度等びそのハッシュ値は、装着者が許可する場合において、秘密鍵の不正アクセス検知の為端末５Ａ等のサービス用サーバに通知されることがある。）
４６Ａ　端末４Ａの外部記録装置（暗号化データを保存する磁気テープ、磁気ディスク、光学ディスク、半導体メモリを含む外部記録装置。秘密鍵が保存されていてもよい。

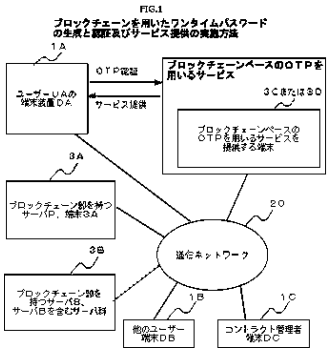
)
４７Ａ　端末４Ａの電源装置
５Ａ　端末５ＡのサーバＳＶＣＲＨＮｃｍ（暗号化ファイル復号閲覧ソフトにおける広告のアクセス先サーバ）
５０Ａ　端末５Ａのサーバ記録部
５００Ａ　端末５ＡのＳＶＣＲＨＮｃｍ動作プログラム（ソフトウェアＣＲＨＮに指定されたリンク用ＵＲＩの対象となる広告情報配信などサービス用プログラム。
ウェブサイトもしくはウェブアプリにブロックチェーンへ接続するプログラムを含む。）
５０１Ａ　端末５Ａのアクセス監視部データベース（ＳＶＣＲＨＮｃｍへアクセスしたユーザ端末とトークン番号関するデータベース。
ユーザー識別子またはトークン番号とＩＰアドレス又は位置情報又は端末ＩＤ又は端末センサ値とサービス利用状況を対応付けた情報。
アクセス者情報はハッシュ化などされて個人情報を保護するよう加工されて保存されてもよい。図６Ｘにデータ構造を示す図表を示す。）
５０２Ａ　端末５Ａの不正アクセス検出プログラム（ユーザー識別子またはトークン番号に対し、異なるＩＰアドレス又は位置情報又は端末ＩＤ又は端末センサ値を示す端末からのアクセスを検出）
５０３Ａ　端末５Ａの不正アクセス通知プログラム（５０２Ａにて不正アクセスの恐れがあるユーザー識別子へ通知用トークンの送付、または識別子に対応する電子メール・ＳＭＳ等に通知する）
５０４Ａ　端末５Ａの顧客情報データベース（必須ではない。ユーザー識別子に対応する連絡先を記録した台帳。）
（プライバシー配慮の為、顧客情報がない場合は不正アクセスを通知用トークンの送付にて通知する。）
（顧客に不正利用の通知を随時伝えたい場合は通知用トークンが送付されたとき端末ＤＰへトークンが送付されたことを知らせる常駐のプログラムが必要。）
５０５Ａ　端末５Ａの暗号化データに埋め込まれたＵＲＩ情報からアクセスされた際に配信する広告等情報（広告はトークンの看板情報や暗号化データ復号時の得られるレイティングにより内容を制御する。）
５０６Ａ　端末５Ａのソフトウェアに含まれる情報にリンクされた広告等情報（５０６ＡはソフトウェアＣＲＨＮのバージョン更新等の通知を配信する機能を含む）
５０００Ａ　端末５Ａの任意のブロックチェーン記憶部（必要な場合。３００Ａと５０００Ａは同じ）
５１Ａ　端末５Ａのサーバ制御部
５１０Ａ　端末５ＡのＳＶＣＲＨＮｃｍ制御部
５１１Ａ　端末５Ａのアクセス監視部及び制御部
５１２Ａ　端末５Ａの不正アクセス監視部
５１３Ａ　端末５Ａの不正アクセス通知部
５１４Ａ　端末５Ａの顧客情報データベース管理部
５１５Ａ　端末５Ａの暗号化データ用広告等配信部
５１６Ａ　端末５Ａのソフトウェア用広告等配信部
５１００Ａ　端末５Ａの任意のブロックチェーン制御部（必要な場合。３１０Ａと５１００Ａは同じ）
５２Ａ　端末５Ａの通信装置
５３Ａ　端末５Ａの制御および演算装置
５３Ａ　端末５Ａの入力装置
５４Ａ　端末５Ａの出力装置
５７Ａ　端末５Ａの電源装置

５Ｂ　サーバＳＶＣＲＨＮｄｒｉｖｅ、端末５Ｂ（暗号化データ及びファイルの配信、共有、検索、バージョン管理を行うサーバー用途。）
５０Ｂ　端末５Ｂのサーバ記録部
５００Ｂ　端末５Ｂのプログラム（ユーザーが望む暗号化データを配信するサーバの基本プログラム部）
５０１Ｂ　端末５Ｂに記録された暗号化ファイルデータベース（暗号化されたデータまたはファイルのハッシュ値、ファイル名、ファイルを復号できるワンタイムパスワード生成
及び認証にかかわるトークンのコントラクト識別子のデータベース。）
５０２Ｂ　端末５Ｂに記録された暗号化ファイル検索用データベース（データベースからユーザーが求める情報を検索しサーバからダウンロードするプログラム）
５０３Ｂ　端末５Ｂに記録された暗号化ファイル登録部（データベースへユーザーが暗号化ファイルをアップロードし、
それを復号するワンタイムパスワード生成及び認証コントラクトの識別子とファイル名、ハッシュ値などを登録するプログラム）
５０４Ｂ　端末５Ｂの鍵情報ＡＫＴＢ通知部（これは電子メールでもよいし、信書送付又は電話番号ＳＭＳサービスと連携してもよい。鍵通知は端末５Ｂの外で行ってもよい）
５０５Ｂ　端末５ＢのＡＫＴＢにより暗号化されたファイルのＵＲＩ等配信先の通知部（ＡＫＴＢを鍵の１つとして利用して生成した鍵ＴＴＫＹで暗号化されたファイルのＵＲＩを通知するメール通知部）
５０６Ｂ　端末５Ｂの電子商取引用プログラム（必要な場合。書籍や動画音声などコンテンツファイルを暗号化ファイルとそれに対応するＯＴＰ生成トークン共に販売する際に利用。決済機能と連携）
５０７Ｂ　端末５ＢのＯＴＰ生成及び認証用のＯＴＰトークン発行部（必要な場合。５０６Ｂの決済の完了を確認しデータの復号を行えるＯＴＰトークンを発行するプログラム。端末１Ｃに発行指示）
５０８Ｂ　端末５Ｂのアクセスユーザのデータベース（必要な場合。顧客ユーザのアクセスに関するデータベース。データ構造は図６Ｘと同じ。）
５０９Ｂ　端末５Ｂの不正アクセス検知部（暗号データを配信するだけの場合は必須ではない。電子商取引にて金銭を用いて暗号化データとＯＴＰトークンの売買をする際に５Ｂに搭載する事が好ましい。）
５０００Ｂ　端末５Ｂの任意のブロックチェーン記憶部（必要な場合。３００Ａと５０００Ｂは同じ）
５１Ｂ　端末５Ｂのサーバ制御部
５１０Ｂ　端末５Ｂのサービス制御部（プログラム５００Ｂ、５０１Ｂ、５０２Ｂ、５０３Ｂ、５０４Ｂ、５０５Ｂ、５０６Ｂ、５０７Ｂ、５０８Ｂ、５０９Ｂに従い制御する部分）
５１００Ｂ　端末５Ｂの任意のブロックチェーン制御部（必要な場合。３１０Ａと５１００Ｂは同じ）
５２Ｂ　端末５Ｂの通信装置
５３Ｂ　端末５Ｂの制御および演算装置
５３Ｂ　端末５Ｂの入力装置
５４Ｂ　端末５Ｂの出力装置
５７Ｂ　端末５Ｂの電源装置
５Ｃ　放送局となるサーバＳＶＣＲＨＮｂｒｏａｄｃａｓｔｅｒ、端末５Ｃ、放送局端末５Ｃ
５０Ｃ　端末５Ｃのサーバ記録部
５０１Ｃ　端末５Ｃのブロックチェーンアクセス用秘密鍵
５０２Ｃ　端末５Ｃの秘密鍵５０１Ｃを用いてブロックチェーンへアクセスするため

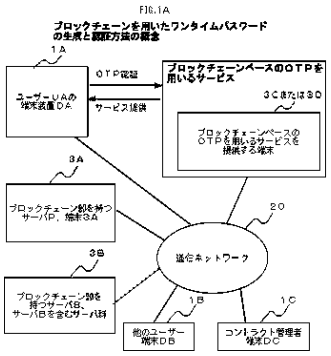
のプログラム
５０３Ｃ　端末５Ｃの放送用ソフトウェア（ソフトウェア４０３Ａを含んでいてもよい。ＧＮＳＳによる測位情報を放送するソフトウェアを含んでいてもよい。）
５０００Ｃ　端末５Ｃの任意のブロックチェーンの記憶部（必要な場合。３００Ａと５０００Ｃは同じ。特に人工衛星型端末５Ｃでは５０００Ｃを備えてもよい。）
５０３４Ｃ　端末５Ｃの放送する暗号化データ（５０３５Ｃを４０３Ａで復号できる鍵ＴＴＫＹで暗号化し放送するデータ）
５０３５Ｃ　端末５Ｃの放送する暗号化データの平文データ（通常は放送しない。ただし緊急時に暗号化を解除して放送する場合に備え、平文データそのものを記憶装置５０Ｃに保持してもよい。）
５１Ｃ　端末５Ｃのサーバ制御部
５１０Ｃ　端末５Ｃの制御部
５１００Ｃ　端末５Ｃの任意で備え付けられることの出来るブロックチェーンの制御部（必要な場合。３１０Ａと５１００Ｃは同じ）
５２Ｃ　端末５Ｃの通信装置
５２０Ｃ　端末５Ｃの放送用無線装置
５２１Ｃ　端末５Ｃの無線通信装置（５Ｃを制御する端末５ＣＣとの連絡用）
５２２Ｃ　端末５Ｃの有線通信装置（必要な場合。端末５Ｃが地上局の際には利用されうる。無線放送ではなく有線放送の場合は通信網への接続装置を兼ねる。）
５２００Ｃ　端末５Ｃの放送用空中線
５２１Ｃ　端末５Ｃの双方向通信装置（人工衛星の場合は地上局と無線により配信データの送信や放送局サーバの制御と管理を行う。地上局の場合は通信網を介して操作可能。）
５３Ｃ　端末５Ｃの制御および演算装置
５３Ｃ　端末５Ｃの入力装置
５４Ｃ　端末５Ｃの出力装置
５７Ｃ　端末５Ｃの電源装置（人工衛星の場合は二次電池や太陽電池を含む）、
５ＣＣ　端末５Ｃの放送局となるサーバ端末を制御する端末もしくは装置（例として５Ｃが人工衛星局の時、５ＣＣは地上局で５Ｃは５ＣＣと通信し５ＣＣ経由でネットワーク２０に接続されうる。）

【要約】　（修正有）
【課題】耐タンパー性の低い秘密鍵を用いる系において、秘密鍵を利用者が抜き出して使い回す場合もしくは秘密鍵が漏洩した場合に備える手段を見つける不正アクセス防止手段を備えるコンピューターネットワークシステムを提供する。
【解決手段】コンピューターネットワークシステムは、秘密鍵から計算されるユーザー識別子とユーザー端末の環境を反映したセンサのデータを対にしてサービス用サーバへ収集し、同一ユーザー識別子に対し異なるセンサの測定値をもつ複数の環境からのアクセスの有無を検知することで、秘密鍵情報の不正利用を検出し通知する。
【選択図】図３Ｃ

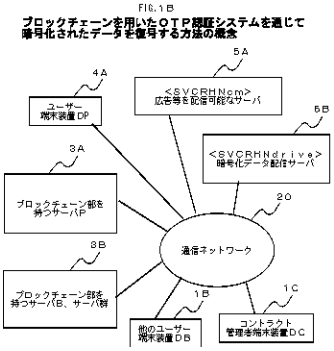
【図１】



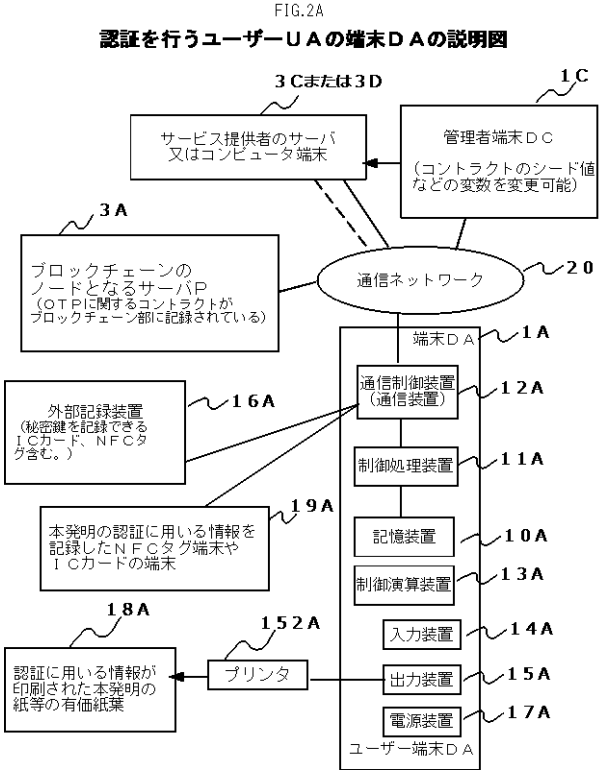
【図１Ａ】



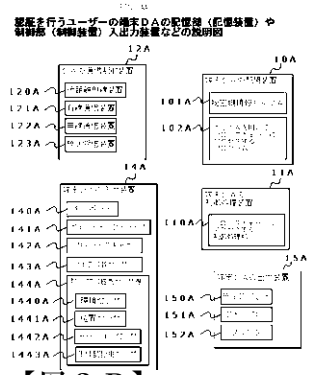
【図１Ｂ】



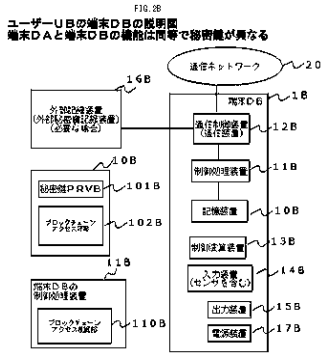
【図２Ａ】



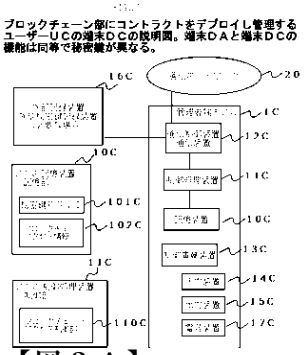
【図２ＡＡ】



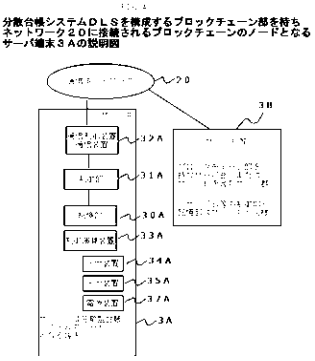
【図２Ｂ】



【図２Ｃ】



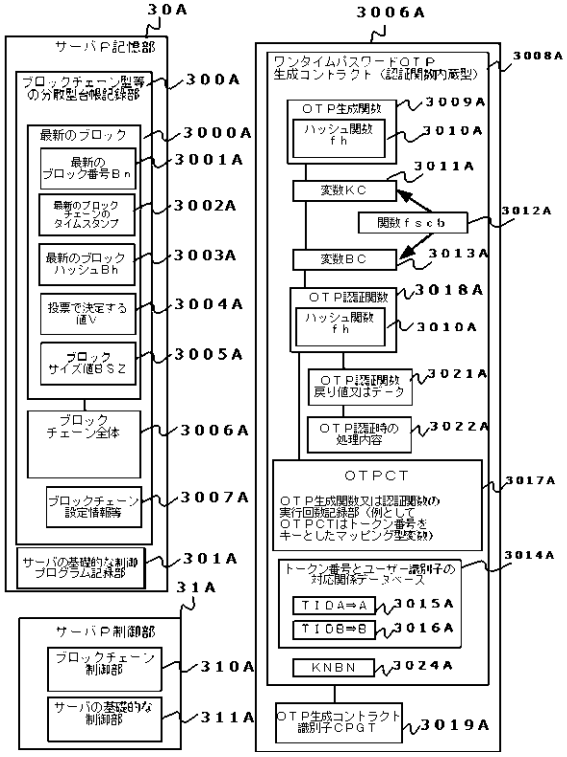
【図３Ａ】



【図３ＡＡ】

FIG.3AA

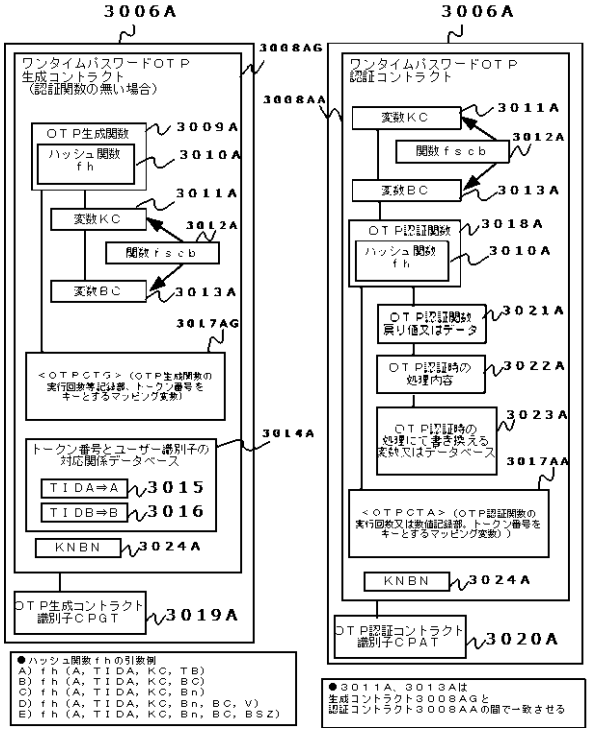
端末３Ａの制御部と記憶部およびスマートコントラクト（コントラクト）の説明図



【図３ＡＢ】

FIG.3AB

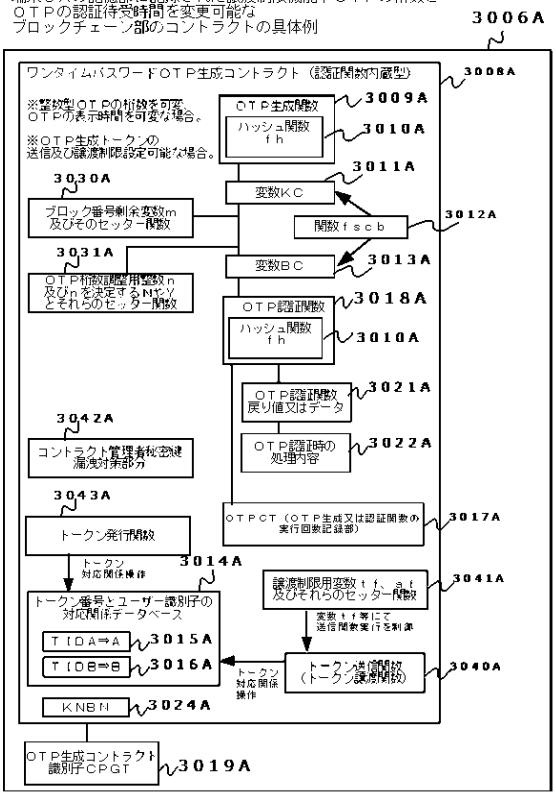
端末３Ａの記憶部に記録されたブロックチェーン部のコントラクトの説明図の一つ



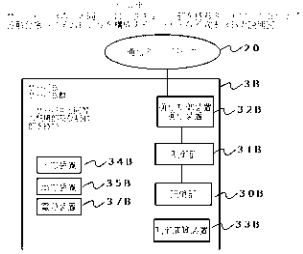
【図３ＡＣ】

FIG.3AC

端末３Ａの記憶部に記録された譲渡制限機能やＯＴＰの桁数とＯＴＰの認証待受時間を変更可能なブロックチェーン部のコントラクトの具体例



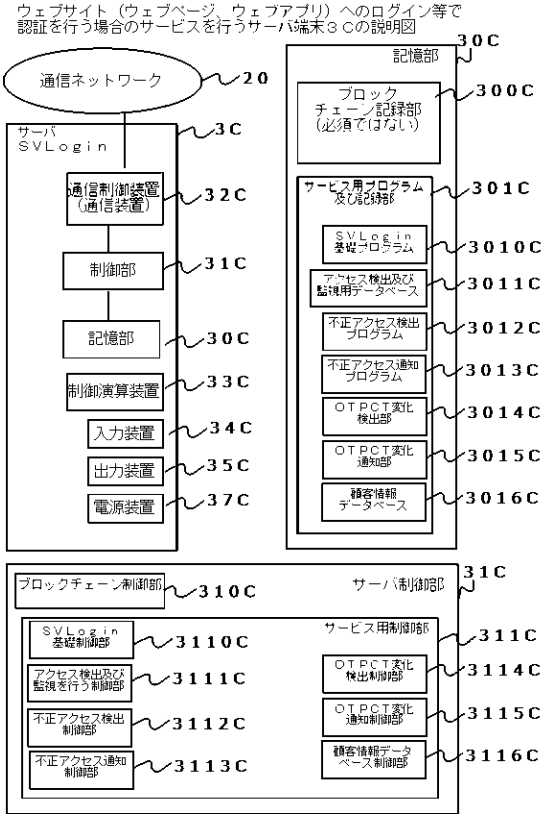
【図３Ｂ】



【図３Ｃ】

FIG.3C

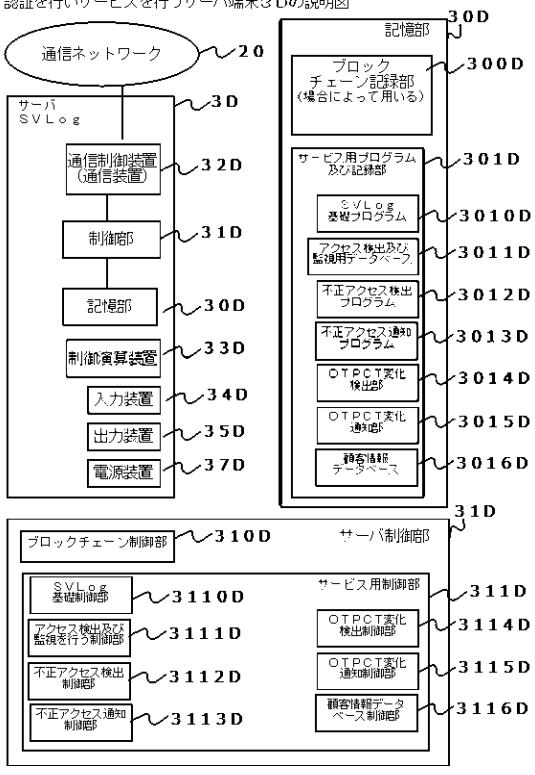
ウェブサイト（ウェブページ、ウェブアプリ）へのログイン等で
認証を行う場合のサービスを行うサーバ端末３Ｃの説明図



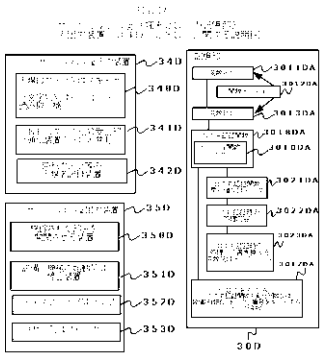
【図３Ｄ】

FIG.3D

印刷物や表示画面及びＮＦＣタグに記録された本発明の認証情報を読み取り
認証を行いサービスを行うサーバ端末３Ｄの説明図



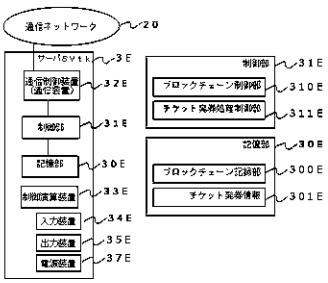
【図３ＤＡ】



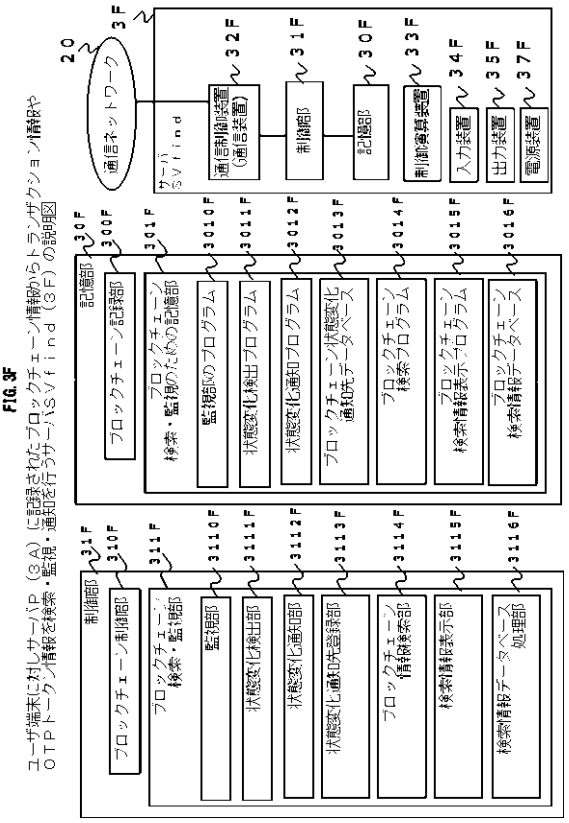
【図３Ｅ】

FIG.3E

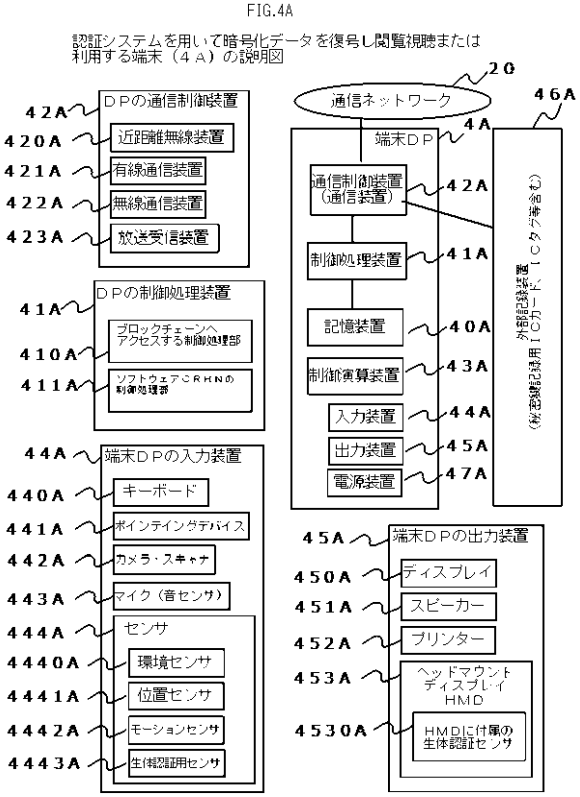
ＯＴＰトークンの購入または振込及びＮＦＣタグに対しＯＴＰ認証情報を出力し
有価証券を発券するサービスを行うサーバ端末３Ｅの説明図



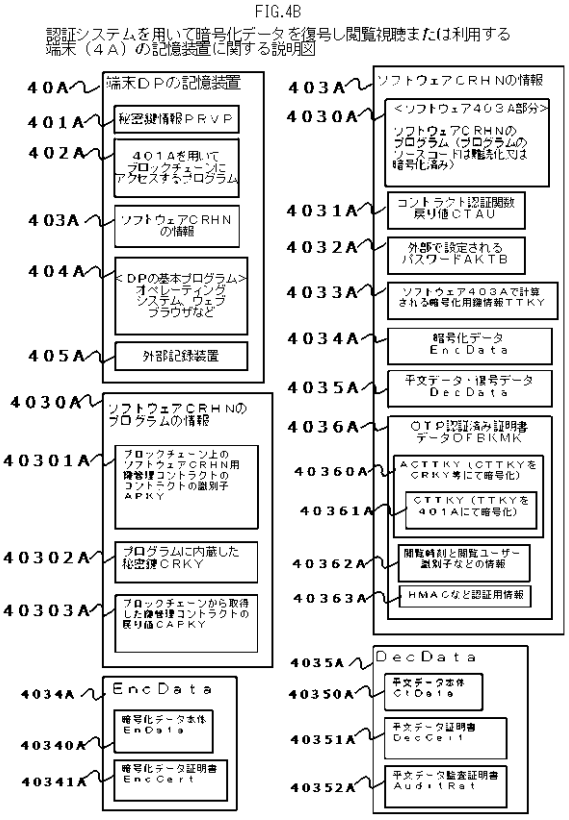
【図３Ｆ】



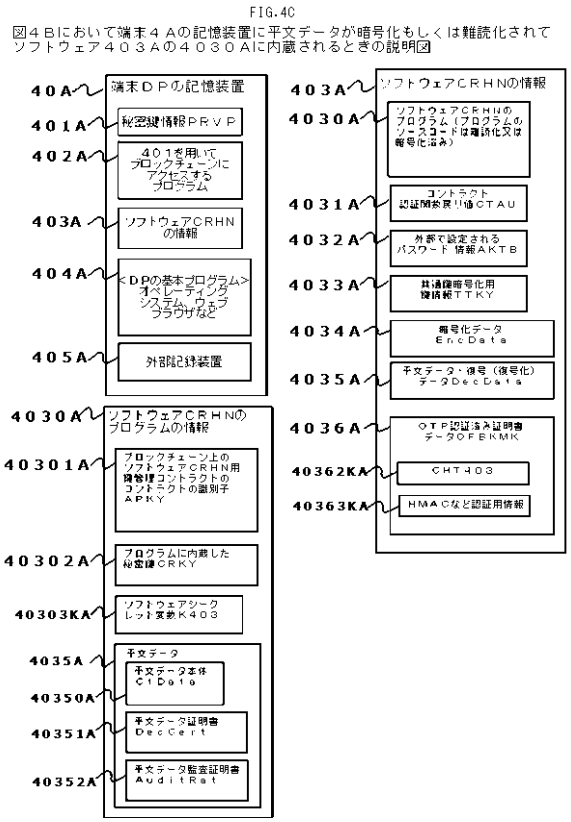
【図４Ａ】



【図４Ｂ】



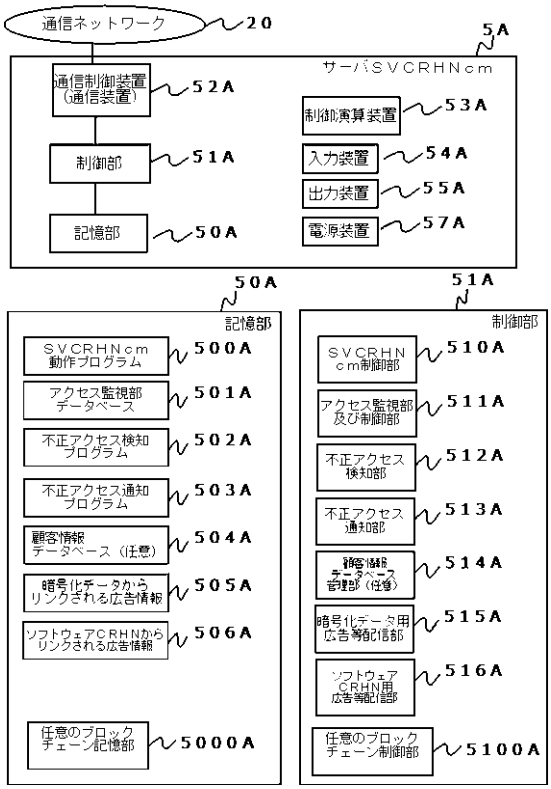
【図４Ｃ】



【図５Ａ】

FIG.5A

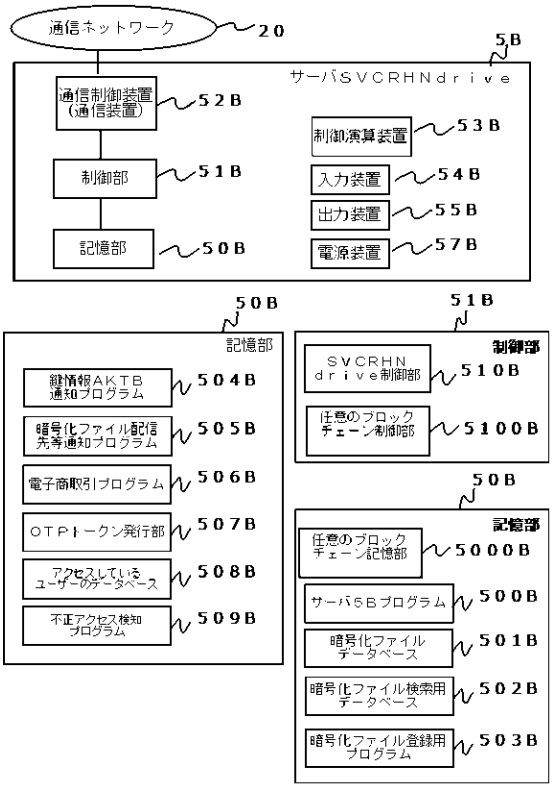
認証システムを用いて暗号化データを復号し閲覧視聴または利用する端末（４Ａ）に広告を配信するサーバ端末の説明図



【図５Ｂ】

FIG.5B

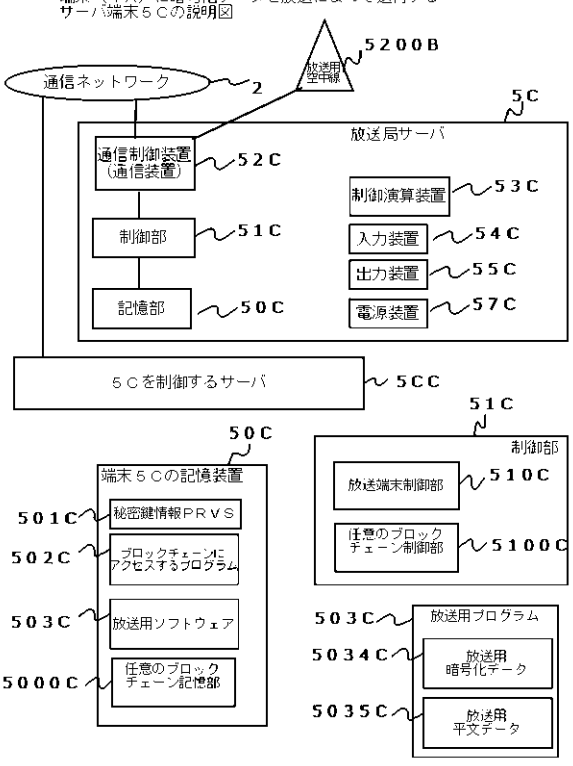
端末（４Ａ）に暗号化データをネットワークを通じて配信するサーバ端末５Ｂの説明図



【図５Ｃ】

FIG.5C

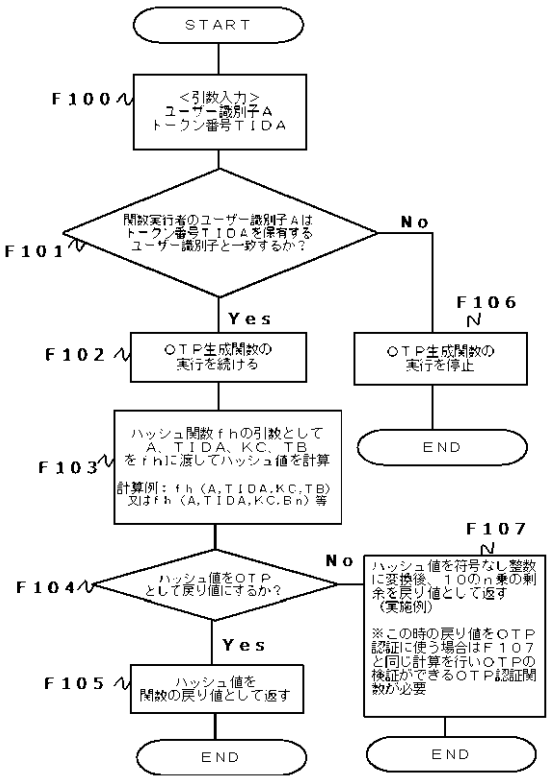
端末（４Ａ）に暗号化データを放送によって送付するサーバ端末５Ｃの説明図



【図６Ａ】

FIG.6A

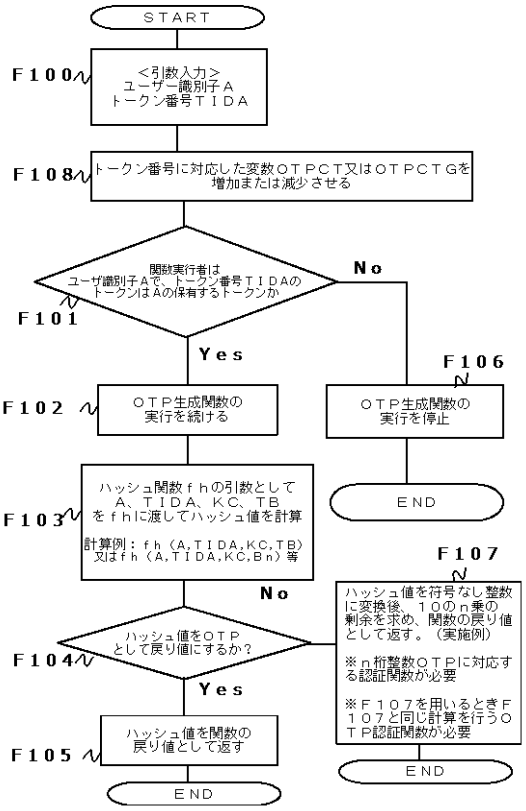
ＯＴＰを生成する関数の処理を示したフローチャート図



【図６Ｂ】

FIG.6B

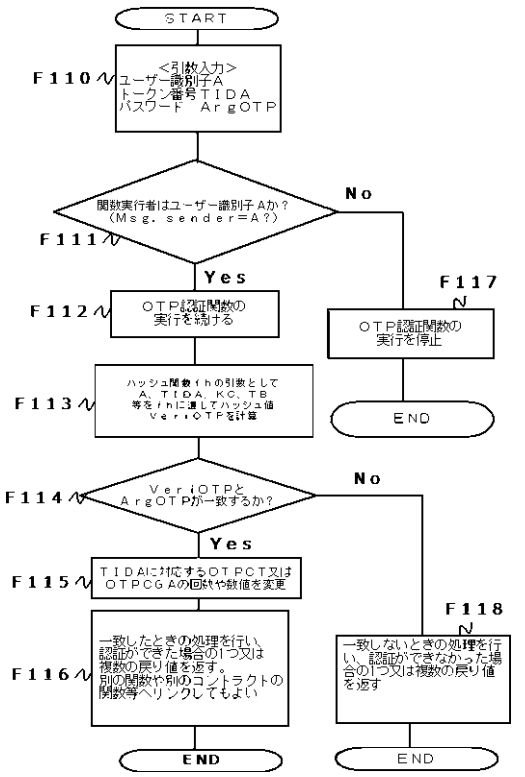
ＯＴＰ生成回数記録機能を備えたＯＴＰを生成する関数の処理を示したフローチャート図



【図６Ｃ】

FIG.6C

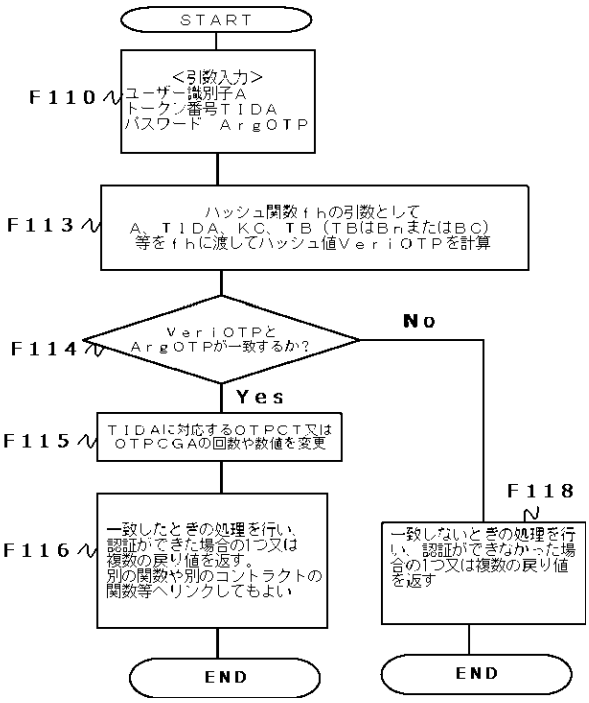
ＯＴＰ認証回数等記録機能を備えた認証するアクセス者をトークン保有者のユーザー識別子に限定する場合のＯＴＰを認証する関数のフローチャート図



【図６Ｄ】

FIG.6D

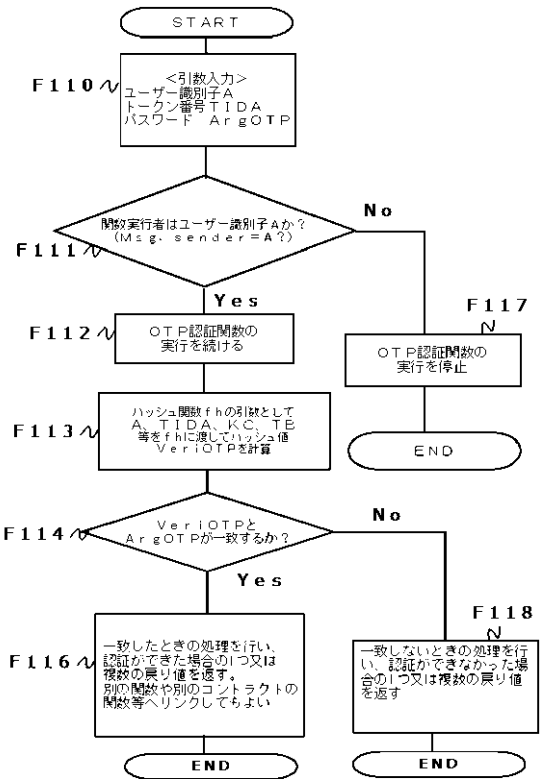
ＯＴＰ認証回数等記録機能を備えた認証するアクセス者を限定しない場合のＯＴＰを認証する関数のフローチャート図



【図６Ｅ】

FIG.6E

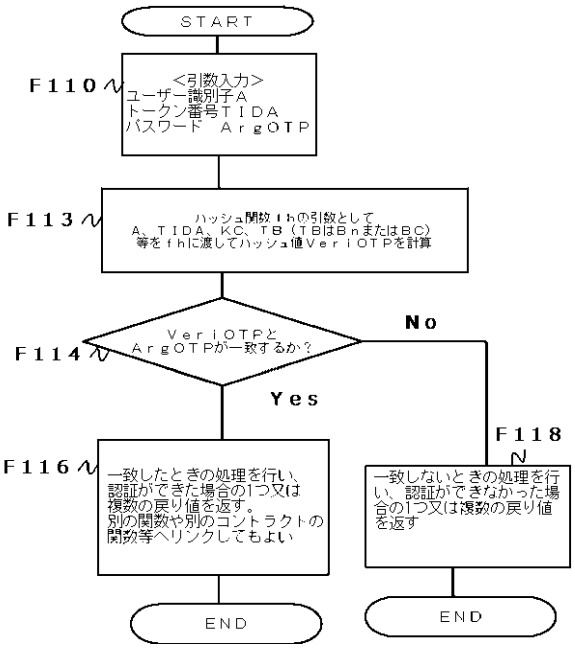
図６ＣからＯＴＰ認証回数等記録機能を除いた場合のＯＴＰを認証する関数のフローチャート図



【図６Ｆ】

FIG.6F

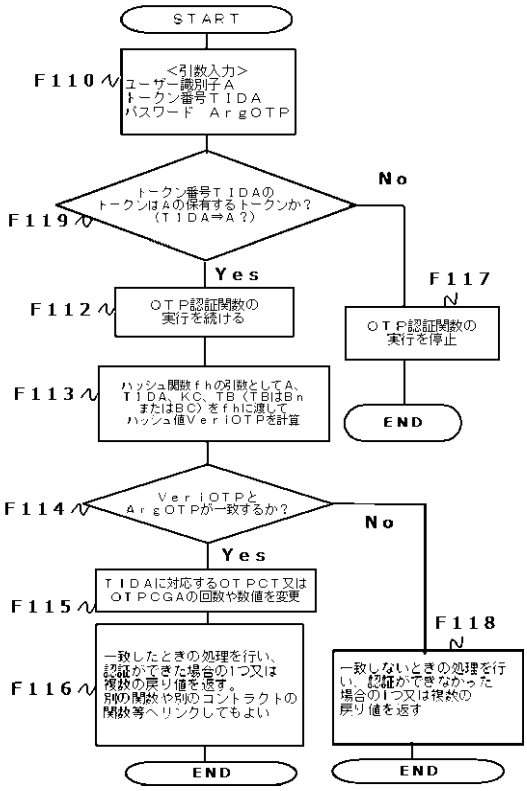
認証するアクセス者を限定しない場合の
ＯＴＰを認証する関数のフローチャート図



【図６Ｇ】

FIG.6G

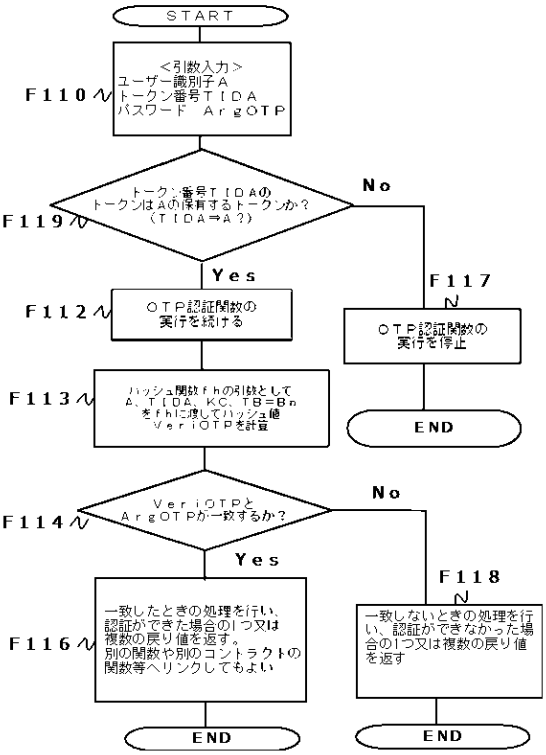
ＯＴＰ認証回数等記録機能を備えたＯＴＰトークンの保有者のアクセスか判断して認証する関数の処理を示したフローチャート図



【図６Ｈ】

FIG.6H

ＯＴＰトークンの保有者のアクセスか判断して
ＯＴＰを認証する関数の処理を示したフローチャート図



【図６Ｘ】

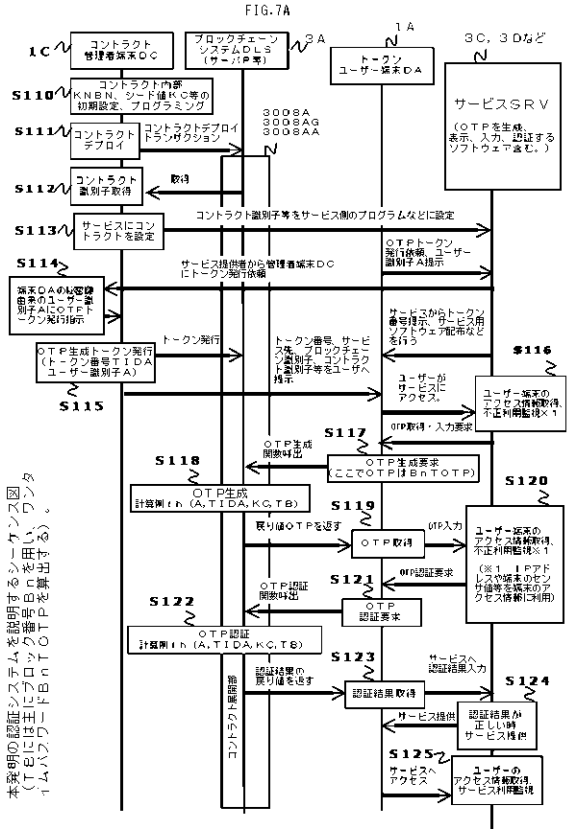
FIG.6X

本発明の認証システムを利用してサービスを行うサーバ端末（３Ｃ，３Ｄ，３Ｅ，３Ｆ，５Ａ，５Ｂ）にユーザ端末（ＤＡなど）がアクセスした際に記録されるデータ構造

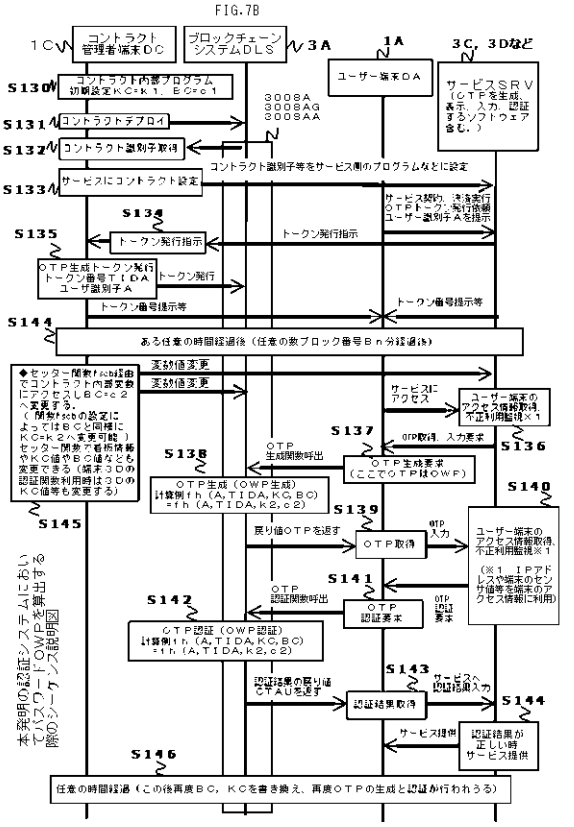
ユーザー識別子	トークン番号	ＩＰＶ値を構成する要素				正常アクセスか？	閲覧時刻Ｔ、閲覧履歴情報Ｃｎｔ（アクセス回数）等のログイン状態データ ※３
		ＩＰアドレス	位置情報	端末ＩＤ	端末センサ値 ※１		
0x714009083C ※４※５	12345	111.11.1.1	東経Ｆ１北緯Ｎ１	ＳＮ：１２３４５	X=123，Y=345，Z=567	正常	2020年11月11日11時11分ログイン、回数１２３、状態0x11AEFF…
0x71400908D0	12346	121.11.1.2	非開示	非開示	非開示	正常	2020年11月11日11時11分ログイン、回数234、状態0x51AFGF…
0x71400908EE	54321	131.11.3.3	西経Ｗ１南緯Ｓ１	ＩＤ：Ａ１２３ＢＣ	X=156，Y=345，Z=569	異常検知 ※２	2020年12月12日13時12分ログイン、回数345、状態0x506011…
0x714009 08EE	54321	131.11.3.3	西経Ｗ１南緯Ｓ１	ＩＤ：Ａ１２３ＢＣ	X=156，Y=345，Z=123	異常検知 ※２	2020年12月12日13時13分ログイン、回数346、状態0x506011…
0x714009 08FF	12347	非開示	非開示	非開示	温度２３℃、気圧９９０ｈＰａ	正常	2020年12月12日22時22分ログイン、回数1010、状態0x101011…
：	：	：	：	：	：	：	：

※１：3軸の地磁気センサまたは温度気圧湿度センサを想定
※２：同じユーザー識別子のアクセスデータにおいて端末センサ値のＺ値が異なる。
端末センサは地磁気センサを想定。温度や気圧センサでもよい。
※３：ログイン状態データは一例。サーバ３Ｃのウェブサイトのログインやソフトウェア４０３Ａにおける広告サーバ５Ａへのアクセスなど本発明において認証後に利用したいサーバへのアクセスに利用される。
※４：表に記載のユーザー識別子やトークン番号等の情報は個人情報保護のためハッシュ化や加工が行われサーバに記録されることもある。
※５端末センサ値、ＩＰアドレス、位置情報、端末ＩＤはＯＴＰトークン利用者の二重もしくは多重のアクセスを検知することに用いられる。多重アクセスが起きる場合は異なる端末から同一の秘密鍵を用いてアクセスしていることが推測される。

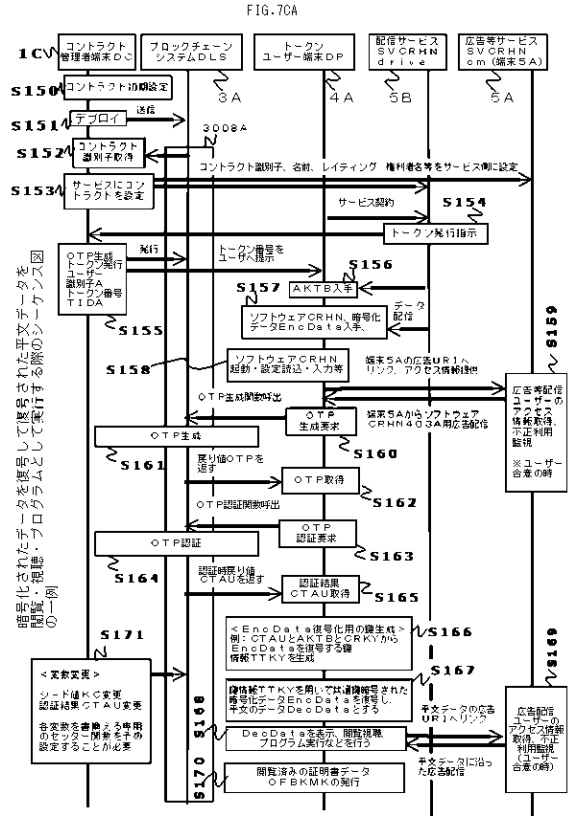
【図７Ａ】



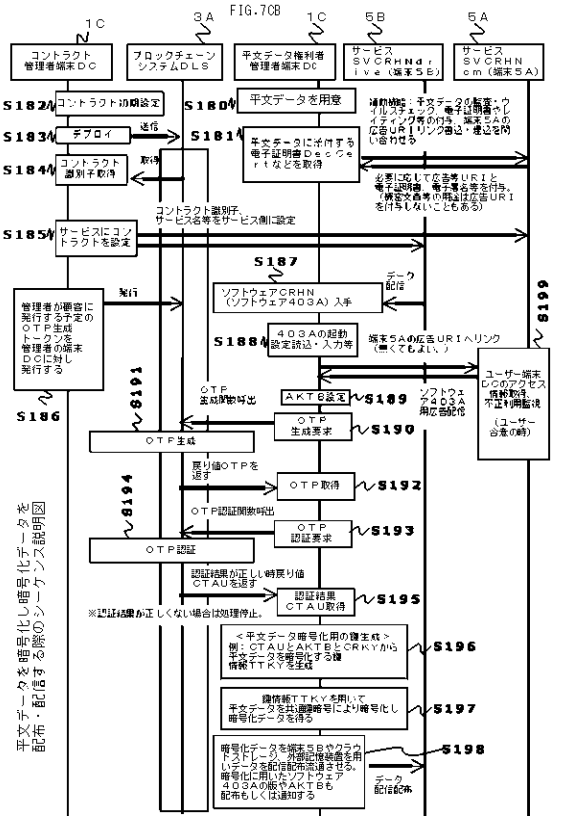
【図７Ｂ】



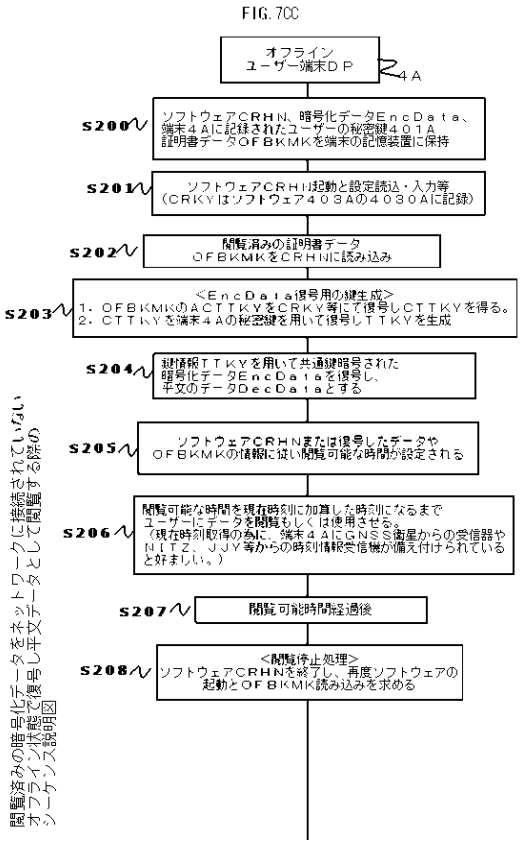
【図７ＣＡ】



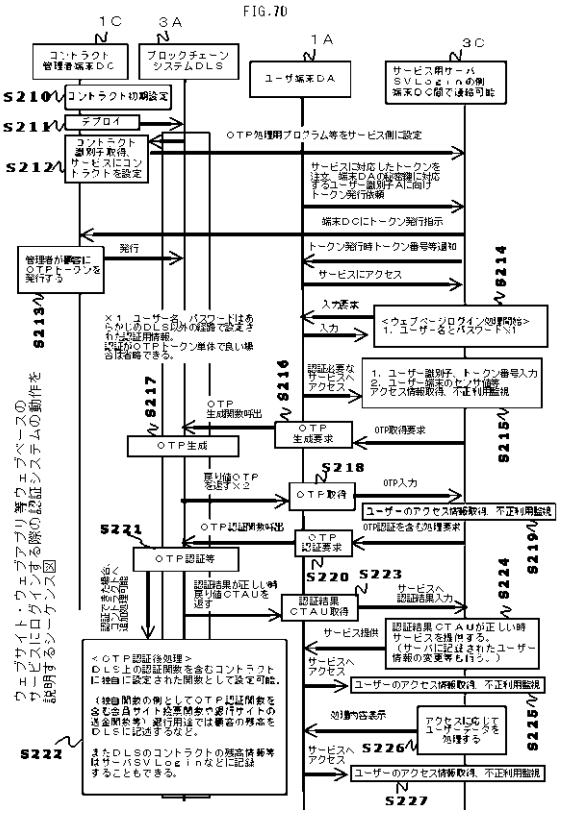
【図７ＣＢ】



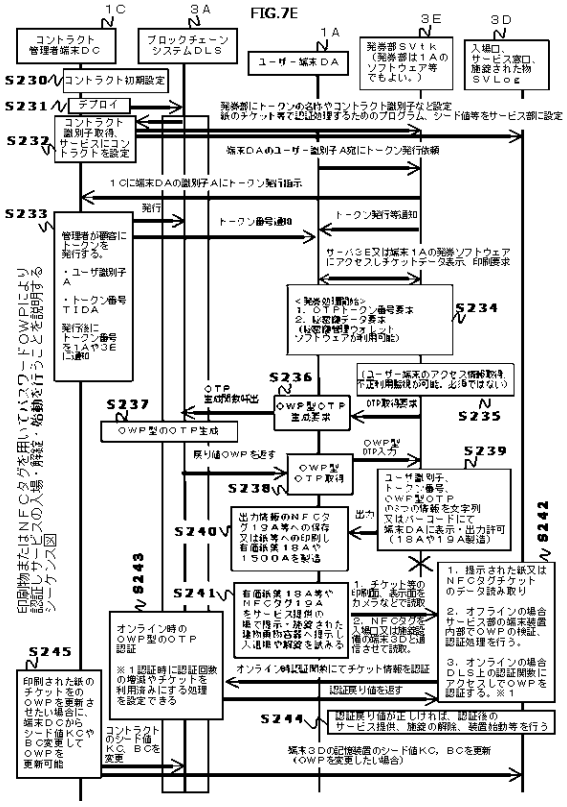
【図７ＣＣ】



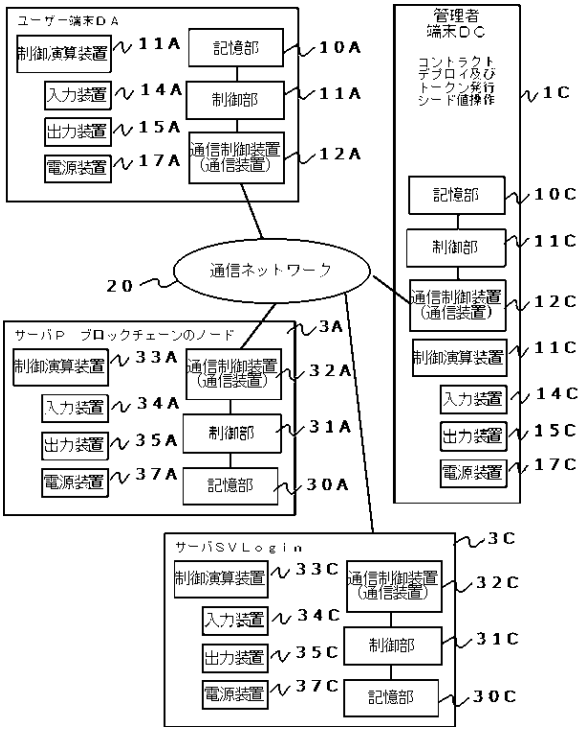
【図７Ｄ】



【図７Ｅ】



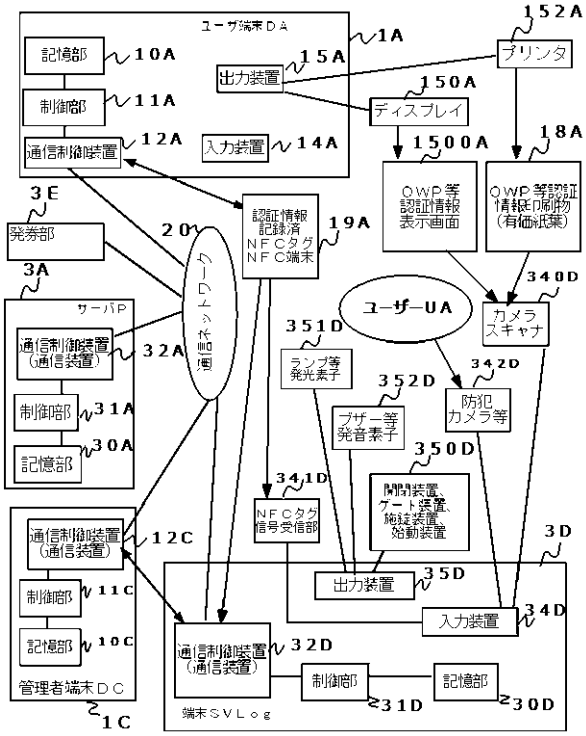
【図８Ａ】



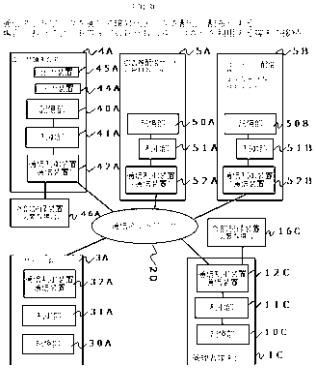
【図８Ｂ】

FIG.8B

印刷物及びＮＦＣタグによる有価紙葉または鍵利用時の端末の接続



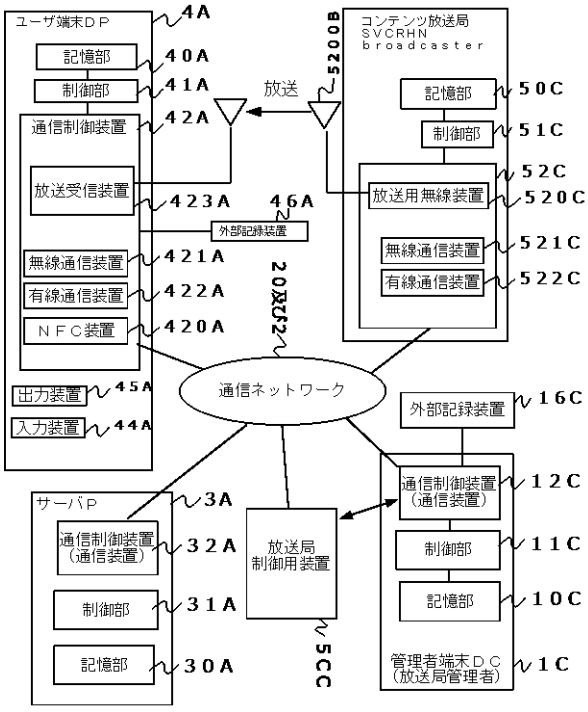
【図８Ｃ】



【図８Ｄ】

FIG.8D

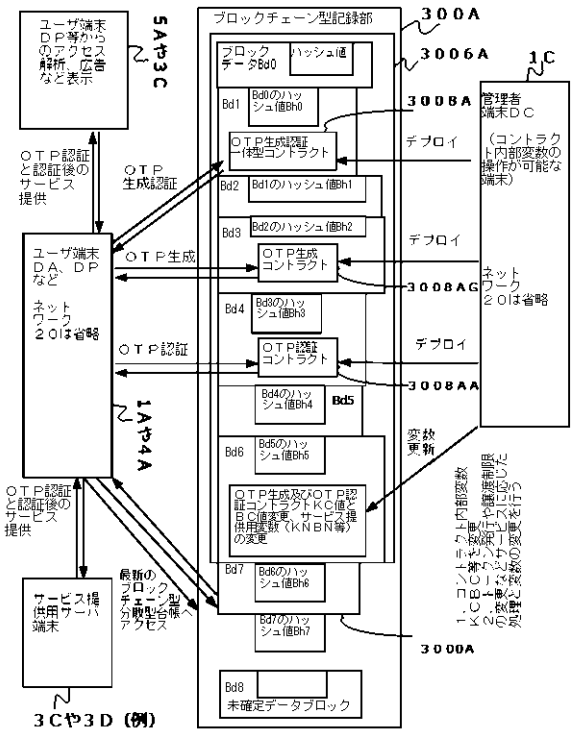
データ放送により暗号化データを放送する場合において
ソフトウェアＣＲＨＮ（４０３Ａ）を利用する端末の接続



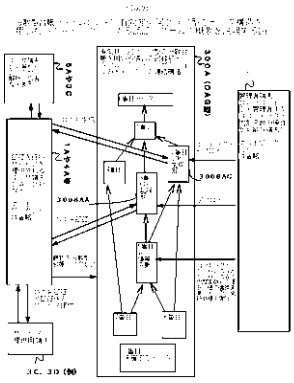
【図９Ａ】

FIG.9A

分散型台帳システムＤＬＳにブロックチェーン型のデータ構造を
用いたＯＴＰトークンによる認証システムの概要を説明する図



【図９Ｂ】



フロントページの続き

特許法第３０条第２項適用　令和２年２月２２日にｎｏｔｅ．ｃｏｍ（運営会社は東京都港区北青山３－１－２のｎｏｔｅ株式会社）にて出願番号の発明の発明者である西沢克弥はペンネーム槍建としや名義で掲載アドレス（ｈｔｔｐｓ：／／ｎｏｔｅ．ｃｏｍ／ｔｏｓｈｉｙａｓｉｎｇｕｌａｒ／ｎ／ｎ７ａ９ｅ０ｆｄ０ｆ７６７）にてブロックチェーンのブロック番号（ブロックナンバー）を用いたＴＯＴＰ及び疑似乱数生成器のアイデアを公開し、た。　そして令和２年２月２３日（ｈｔｔｐｓ：／／ｎｏｔｅ．ｃｏｍ／ｔｏｓｈｉｙａｓｉｎｇｕｌａｒ／ｎ／ｎ６ｃ４ｅ０８ｂ５７８ｅ５）及び２月２４日（ｈｔｔｐｓ：／／ｎｏｔｅ．ｃｏｍ／ｔｏｓｈｉｙａｓｉｎｇｕｌａｒ／ｎ／ｎ５５３６７ａｄ４ｄ１ｂｃ）に同じくｎｏｔｅ．ｃｏｍにてユーザー識別子を用いたＯＴＰトークンを用いるブロックチェーンのブロック番号を用いたＴＯＴＰ認証の概念やプログラムコードについて公開した。　さらに西沢克弥はＯＴＰ認証システムの開発と発明の実施を行い令和２年４月１７日にブロック番号ＢｎベースのＴＯＴＰの生成と認証に関するコントラクトをパブリックなブロックチェーンのイーサリアムのＲｏｐｓｔｅｎテストネットにデプロイし公開し、令和２年５月２６日にＧｉｔＨｕｂ．ｃｏｍ（運営会社はＧｉｔｈｕｂ．ｉｎｃ、米国カリフォルニア州サンフランシスコ市）においてウェブサイト上でＴＯＴＰ及びＯＴＰ認証プログラムの基礎的な公開をした。　（公開先はｈｔｔｐｓ：／／ｇｉｔｈｕｂ．ｃｏｍ／ＮＺＲＩ－ＡＺＲＩ／ＥＲＣ７２１ＬＴ－ＯＴＰ－ＧＥＮ－ＡＵＴＨ。）同年７月９日にもＯＴＰ認証システムのコントラクトとウェブサイト・ウェブアプリを公開した。さらにＯＴＰ認証システムを用いたウェブサイトログイン・紙のチケット・暗号化データ復号への用途の概念に関わる概念を令和２年７月１３日にｈｔｔｐｓ：／／ｇｉｔｈｕｂ．ｃｏｍ／ＮＺＲＩ－ＡＺＲＩ／ｃｒｙｈｏｎ及びｈｔｔｐｓ：／／ｇｉｔｈｕｂ．ｃｏｍ／ＮＺＲＩ－ＡＺＲＩ／ｃｒｙｈｏｎ／ｂｌｏｂ／ｍａｓｔｅｒ／Ｃｒｙｂｏｎ－ＥＲＣ７２１ＫＩ．ｐｄｆにて公開した。

特許法第３０条第２項適用　またＧｉｔＨｕｂを用いてソースコードを掲載しながら米Ｈｅｒｏｋｕ社のＨｅｒｏｋｕというウェブサイト開発プラットフォームにて、ＯＴＰ認証時にＩＰアドレスを収集する事を意図した番号ＢｎベースのＴＯＴＰ認証に関するウェブページを令和２年４月２６日にｈｔｔｐｓ：／／ｏｔｐ－ｒｏｐｓｔｅｎ－ｔｅｓｔ．ｈｅｒｏｋｕａｐｐ．ｃｏｍ／にて公開した。また同年７月２９日にはコンテンツ閲覧用サイトの例としてｈｔｔｐｓ：／／ｃｒｙｈｏｎ．ｈｅｒｏｋｕａｐｐ．ｃｏｍ／を公開している。　発明者の用いたコントラクトをブロックチェーンにデプロイするために用いたイーサリアムテストネットのアドレスは０ｘ０ｆ３９８８０３ＢＥ４３１９Ｂ９８Ｆ１６４ｃａｅ４７５８９７９７ａＣ５ｃＦ９０６と０ｘ７Ｅ８６ｅＦＥ６６０Ｄ７７ＦＡ８７４３３８ａＤＡｆ８ｂｅ８８ｆ８ｃＡＥＤ３ｃ２７と０ｘ８６９０４３３９Ｄ２３ＢＦ３４６Ｃ１ＦＦＦ３１Ｃｃ３Ｂｂ７２６２ｆａ５９ｄ８３７を用いており、前記イーサリアムアドレスについて本発明に関するトランザクションが記録され公開されている。次に１番目のアドレスの検索ＵＲＩを例として次に２つ示す。ｈｔｔｐｓ：／／ｒｏｐｓｔｅｎ．ｅｔｈｅｒｓｃａ．ｉｏ／ａｄｄｒｅｓｓ／０ｘ０ｆ３９８８０３ＢＥ４３１９Ｂ９８Ｆ１６４ｃａｅ４７５８９７９７ａＣ５ｃＦ９０６、ｈｔｔｐｓ：／／ｒｉｎｋｅｂｙ．ｅｔｈｅｒｓｃａｎ．ｉｏ／ａｄｄｒｅｓｓ／０ｘ０ｆ３９８８０３ＢＥ４３１９Ｂ９８Ｆ１６４ｃａｅ４７５８９７９７ａＣ５ｃＦ９０６　。

早期審査対象出願

(58)調査した分野(Int.Cl.，ＤＢ名)

Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　２１／５５
Ｇ０９Ｃ　１／００
Ｈ０４Ｌ　９／３２