

(19)日本国特許庁(JP)

(12)公 開 特 許 公 報(A)

(11)特許出願公開番号
特開2022-65010
(P2022-65010A)

(43)公開日
令和4年4月26日(2022. 4. 26)

(51)Int. Cl.
H 0 4 L 9/32 (2006. 01)
G 0 6 F 21/33 (2013. 01)

F I
H 0 4 L 9/32 1 0 0 B
G 0 6 F 21/33

テーマコード (参考)

審査請求 有 請求項の数 19 O L 公開請求 (全 201 頁)

(21)出願番号	特願2022-16773(P2022-16773)	(71)出願人	714009083
(22)出願日	令和4年2月5日(2022. 2. 5)		西沢 克弥
(62)分割の表示	特願2021-205792(P2021-205792) の分割	(72)発明者	西沢 克弥
原出願日	令和3年1月15日(2021. 1. 15)		長野県上田市吉田 5 1 5 番地 2

最終頁に続く

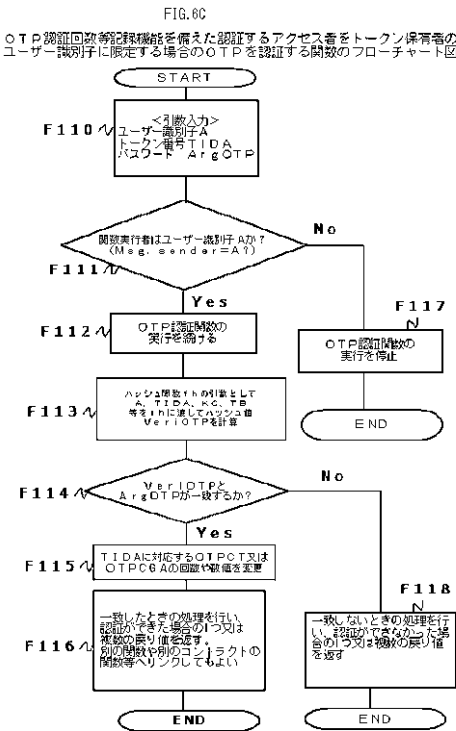
(54)【発明の名称】 認証装置および認証システム、認証処理方法

(57)【要約】 (修正有)

【課題】 O T P 生成をスマートコントラクトで行い、サービス提供端末で O T P 認証を行わせ、認証時にアクセス者を限定可能にする認証装置およびシステム及び方法を提供する。

【解決手段】 O T P 認証において分散型台帳システムを用いる系を利用し、 O T P 認証関数にアクセス者の秘密鍵由来のユーザ識別子を判定する処理部を備えさせ、 O T P 認証関数の処理部にユーザ識別子の判定部を備えさせる。分散型台帳システムとスマートコントラクトとサービス提供端末を用いる系において O T P トークンを或るユーザ識別子に対応付けて O T P 認証する。認証する関数部にアクセスできる秘密鍵を持つユーザ識別子を限定し、 O T P 認証において前記関数を実行又は動作させる際に秘密鍵及びユーザ識別子を必須にすることで、 O T P 認証に必要な前記トークンの個数や秘密鍵及びユーザ識別子を持たない不特定のユーザ端末が前記関数を実行させることを防止する。

【選択図】 図 6 C



【特許請求の範囲】

【請求項 1】

分散型台帳システムを含むネットワークにおいて、ある時刻において変化する変数 TB を用いる動的なパスワード VP をワンタイムパスワード OTP として生成する OTP 生成関数を備えた OTP トークンのスマートコントラクトを備える分散型台帳システムのノードとなる端末と、前記パスワード VP の認証を行う OTP 認証関数を備える OTP 認証端末と、前記ユーザ端末を前記ネットワークを介して接続させたコンピュータネットワークシステムにおいて、

前記 OTP 認証関数は前記スマートコントラクトの前記 OTP 生成関数にて計算される前記 OTP と同じ OTP を計算する処理部を備えており、前記ユーザ端末が前記 OTP 生成関数より前記 OTP を生成又は取得し、前記 OTP を前記 OTP 認証関数に入力することにより OTP 認証を行うコンピュータネットワークシステムであって、

前記 OTP 生成関数と前記 OTP 認証関数のパスワード VP の計算をハッシュ関数 f_h を用いて行う場合に、前記ハッシュ関数 f_h の引数にトークン番号 $TIDA$ と、前記 OTP 生成関数と前記 OTP 認証関数を備える端末に記憶された変数 KC と、ある時刻において分散型台帳システムにおいて変更される変数 TB と、ユーザ端末の秘密鍵もしくはシードとなる情報から分散型台帳システムに設定された方法で計算されるユーザ識別子 A のうち 3 つ以上の変数を基にして、前記ハッシュ関数 f_h の引数に利用するキー値もしくはシード値として備えハッシュ値を計算し前記 OTP の算出に用いるコンピュータネットワークシステムであって、

前記パスワード VP の計算を $VP = f_h(A, TIDA, KC, TB)$ または $VP = f_h(TIDA, KC, TB)$ または $VP = f_h(A, KC, TB)$ として行うことの出来る前記 OTP 生成関数と前記 OTP 認証関数を備え、

前記パスワード VP の計算に用いる計算処理方法を前記 OTP 生成関数と前記 OTP 認証関数の間で一致させる機能を前記スマートコントラクトまたは前記サービス提供端末に備え、

或る時刻 T において分散型台帳システムの変数 TB が変化することを利用して動的なパスワード VP により OTP 認証を行うことを特徴とするコンピュータネットワークシステム。

【請求項 2】

請求項 1 に記載の前記コンピュータネットワークシステムにおいて、スマートコントラクトの管理を行う権限をもつ管理者端末に記録された管理者用秘密鍵情報を用いて計算されるユーザ識別子 C のユーザのみがアクセスできるセッターとなる関数 f_{scb} または変数変更手段 f_{scb} と、前記関数 f_{scb} を用い任意の時刻またはブロック番号において書き換えることの出来る変数 KC または変数 BC を前記 OTP 生成関数を備える端末と前記 OTP 認証関数を備える端末に備え、

前記パスワード VP の計算を行う時に前記 OTP 生成関数と前記 OTP 認証関数の前記ハッシュ関数 f_h の引数に前記変数 KC または前記変数 BC を前記変数 TB の代わりに用い、任意の時刻またはブロック番号において、前記変数 KC または前記変数 BC を前記変数変更手段 f_{scb} または前記関数 f_{scb} を用いて変更し更新することによって、前記パスワード VP を生成し OTP 認証を行うコンピュータネットワークシステム。

【請求項 3】

請求項 1 に記載の前記コンピュータネットワークシステムにおいて、前記分散型台帳システムはブロックチェーンを用い、前記パスワード VP の計算を行う時に前記 OTP 生成関数と前記 OTP 認証関数の前記ハッシュ関数 f_h の引数にブロックチェーンの最新のブロック番号 B_n またはブロックナンバー B_n を前記変数 TB の代わりに用い、時間が変化することによって前記ブロック番号 B_n が変化することにより前記動的なパスワード VP を生成し OTP 認証を行うコンピュータネットワークシステム。

【請求項 4】

請求項 3 に記載のコンピュータネットワークシステムにおいて、前記パスワード VP の計算に用いる変数に前記変数 K C と前記変数 B C を備え、
前記関数 $f s c b$ または前記変数変更手段 $f s c b$ を用いて前記変数 K C または前記変数 B C を 1 つ以上書換えることができる、前記動的なパスワード VP を生成し O T P 認証を行うコンピュータネットワークシステム。

【請求項 5】

請求項 1 と請求項 4 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、前記変数 T B または前記ブロック番号 B n を前記パスワード VP の計算に用いる場合について、整数の変数 M を前記 OTP 生成関数を備える端末と前記 OTP 認証関数を備える端末に備え、前記変数 B n もしくは前記変数 T B を変数 M で割った剰余 r 、すなわち $r = B n \bmod M$ を計算し、前記 B n または前記変数 T B から r を減算することで算出される値 B n r を前記 T B または前記 B n の代わりに用いパスワード VP を計算するコンピュータネットワークシステム。

10

【請求項 6】

請求項 1 と請求項 2 と請求項 3 と請求項 4 と請求項 5 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、前記パスワード VP を符号なし整数に型変換した値 m を被除数 m とし、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 を整数値のパスワード VPr として用いるコンピュータネットワークシステム。

【請求項 7】

請求項 1 と請求項 2 と請求項 3 と請求項 4 と請求項 5 と請求項 6 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、前記パスワード VP の生成と認証を行う OTP 生成関数または OTP 認証関数の関数実行時に用いる変数として、
前記 O T P 生成関数の実行回数もしくは前記 O T P 認証関数の実行回数を記録するトークン番号を検索のキーとする変数、又は前記 O T P 生成関数の実行回数もしくは前記 O T P 認証関数の実行回数、又は前記 O T P 生成関数もしくは前記 O T P 認証関数の関数実行により変化する変数をスマートコントラクトに備え、
前記 O T P 生成関数もしくは前記 O T P 認証関数のいずれかもしくは両方について前記関数が実行されるたびに前記実行回数を記録する変数の値を増加もしくは減少させる処理を行うことの出来るコンピュータネットワークシステム。

20

30

【請求項 8】

請求項 3 と請求項 4 と請求項 5 と請求項 6 と請求項 7 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、前記分散型台帳システムを構成するノード間で、データブロックを連結する際にブロックチェーンまたは分散型台帳システムを構成するノード間で利用される変数を、ノード間の投票または合意により決定する際に、前記投票または合意により決定した変数 V を前記パスワード VP を計算するシード値に用い、前記パスワード VP を計算するコンピュータネットワークシステム。

【請求項 9】

請求項 8 に記載のコンピュータネットワークシステムにおいて、前記変数 V はブロックチェーンのデータブロックのデータサイズである変数 B S Z、または B l o c k G a s L i m i t であるコンピュータネットワークシステム。

40

【請求項 10】

請求項 1 から請求項 9 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ついて、トークン送信関数 $t f$ を備えるスマートコントラクトにおいて、前記関数 $t f$ を実行する際に必要な変数を備え、前記関数 $t f$ を実行する際に必要な変数は管理者の端末に記録された管理者用秘密鍵情報を用いてアクセス出来るセッターとなる関数または変数変更手段より変更され、前記関数 $t f$ を実行する際に必要な変数の値によって前記送信関数 $t f$ の実行は制御され、ユーザー識別子 A とユーザー識別子 B の異なるユーザー識別子間で前記 O T P トークンの送信と譲渡を前記管理者が停止または許可できる機能を持つ前記スマートコントラクトを用いることを特徴とするコンピュータネットワークシステム。

50

【請求項 1 1】

請求項 1 から請求項 1 0 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、前記 OTP 生成関数を備えた前記 OTP トークンのスマートコントラクトから前記 OTP を計算して生成し前記ユーザー端末の記憶装置に取得し、前記記憶装置に記憶され取得された前記 OTP と前記ユーザー識別子または前記トークン番号またはその両方を、ログインサービスを提供するサービス提供端末が提供するウェブサービスプログラムに含まれる前記 OTP 認証関数もしくは前記ウェブサービスプログラムからアクセス又は参照できるスマートコントラクトに含まれる前記 OTP 認証関数へ入力し、前記 OTP 認証関数を実行し、OTP 認証を行うコンピュータネットワークシステム。

【請求項 1 2】

請求項 2 に記載のコンピュータネットワークシステムにおいて、前記ユーザ識別子 A、前記トークン番号 T I D A、前記パスワード VP を文字列または二次元バーコードとして紙等あるいはユーザ端末のディスプレイといった記録手段に記録・表示させ、あるいは認証用データである前記ユーザー識別子 A と前記トークン番号 T I D A と前記パスワード VP の情報をユーザーの所持する磁気ストライプカードまたは IC カード端末や NFC 端末 (NFC タグ) やスマートフォン端末もしくはウェアラブルコンピュータ端末を含む前記ユーザー端末といったデータとして記憶または記録する記録手段に記憶または記録させて、前記記録手段を製造し、

前記記録手段が紙等あるいはユーザ端末のディスプレイといった記録手段または有価紙葉の形態で用いられる場合には、前記記録手段に記録された変数を、サービスを提供するサービス提供端末の備えるカメラもしくはスキャナを用いて読み取り、前記 OTP 認証関数を含む前記スマートコントラクトもしくは前記サービス提供端末の前記 OTP 認証関数の引数に入力し、前記 OTP 認証関数を実行させ、前記 OTP 認証関数の前記戻り値 C T A U を得て、ユーザーに対しサービス提供を行うコンピュータネットワークシステムであり、

前記記録手段が前記データとして記憶または記録する記録手段の場合には、前記サービス提供端末を用いて前記記録手段に記録された認証用データとして読み取り、前記サービス提供端末に備えられた前記 OTP 認証関数の引数に入力し、前記 OTP 認証関数を実行させ、前記 OTP 認証関数の戻り値 C T A U を得て、ユーザーに対しサービス提供を行う、コンピュータネットワークシステム。

【請求項 1 3】

請求項 1 から請求項 1 0 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、前記 OTP 認証関数から得られる前記戻り値 C T A U を暗号化データを復号するための鍵情報に用いて暗号化されたデータを復号するソフトウェア C R H N をユーザー端末に備えるコンピュータネットワークシステム。

【請求項 1 4】

請求項 1 から請求項 1 3 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、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 と前記トークン番号 T I D A またはその両方と、前記ユーザ端末の IP アドレスまたは位置情報または端末識別子または端末センサ値、もしくは前記 IP アドレスまたは前記位置情報または前記端末識別子または前記端末センサ値のハッシュ値、もしくは前記 IP アドレスまたは前記位置情報または前記端末識別子または前記端末センサ値の何れかを直接もしくは仮名化または匿名化して含む値 IPV、もしくは前記 IP アドレスまたは前記位置情報または前記端末識別子または前記端末センサ値の何れかを直接もしくは仮名化または匿名化して含む値 IPV のハッシュ値 IPV を、前記ユーザ端末より前記サービス提供端末に収集し記録させ、同一のユーザー識別子 A もしくはトークン番号 T I D A もしくはその両方に対し、異なる前記 IP アドレスまたは前記位置情報または前記端末識別子または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、もしくは前記値 IPV のハッシュ値からのアクセ

10

20

30

40

50

スが行われたか否かを検出する制御部と記憶部をサービス提供端末に備えるコンピュータネットワークシステムであって、

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備えセンサとして利用するコンピュータネットワークシステムであって、

前記モーションセンサーには加速度センサ（加速度計）またはジャイロセンサ（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またはにおいセンサを備えるコンピュータネットワークシステム、

10

【請求項 15】

請求項 2 に記載のパスワード V P を用いたコンピュータネットワークシステムで用いる前記パスワード V P を含む前記 O T P 認証関数の引数となる認証情報を、紙面または有価紙葉や N F C タグ端末といった記録手段に記録させ物のタグまたはデータのタグとして添付又は貼付又は記録し、もしくは物の表面に添付して、前記物のタグに記録されたパスワード V P を前記 O T P 認証関数に入力し認証するコンピュータネットワークシステム。

【請求項 16】

請求項 3 から請求項 10 の何れかに記載のパスワード V P を含む前記 O T P 認証関数の引数となる認証情報を、データ通信端末または配信端末および放送局端末の放送又は配信又は送信するデータに添付し、前記放送又は配信又は送信するデータに添付されたパスワード V P を前記 O T P 認証関数に入力し認証し、

20

または、前記パスワード V P の取得時のブロック番号 B n p と前記パスワード V P を含む前記 O T P 認証関数の引数となる認証情報を、物のタグまたはデータのタグとして添付又は貼付又は記録し、前記タグに記録された前記パスワード V P と前記ブロック番号 B n p を前記 O T P 認証関数入力し認証するコンピュータネットワークシステム。

【請求項 17】

請求項 16 に記載のコンピュータネットワークシステムについて、前記放送するデータが全球測位衛星システム（G N S S）衛星端末より放送される測位用信号または測位用データであるコンピュータネットワークシステム。

【請求項 18】

30

請求項 3 から請求項 15 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、トークン番号 T I D A の前記 O T P トークンを付与されたユーザ識別子 A のユーザが設定または書換または変更出来るシード値 V U [T I D A] を前記パスワード V P の前記ハッシュ関数 f h の引数に利用するコンピュータネットワークシステム。

【請求項 19】

請求項 1 から請求項 18 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、O T P トークンを或るユーザ識別子に対応付けて O T P 認証する場合に、前記 O T P 認証関数を実行できる秘密鍵を持つユーザ識別子を限定する処理部を備えるコンピュータネットワークシステム。

【発明の詳細な説明】

40

【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】

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

50

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（あるいはユーザーのニックネーム）、電子メールアドレスとパスワードを登録させ、ウェブサイトログインさせる。ここでウェブサイトログインしたのち、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。

10

【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。

20

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。

30

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。

40

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。

50

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。

【 0 0 0 4 】

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RFC 6238規格が知られる。RFC 6238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。

【 0 0 0 5 】

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

10

20

30

40

50

ウェア型TOTPトークンを郵送ないし配達する必要がある、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変数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

10

20

30

40

50

【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>

10

【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>

8

【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。

20

【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B_n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。

30

Tの値はある時刻に変化する値T_mまたはTBであって、T_m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B_n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T_m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。)

40

【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B_nと言い換える。ブロック番号B_n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B_nTOTP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B_n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

50

ら数えて B_n 番目にある時の番号 B_n を時刻や時間の変化を表す変数 B_n として用い $TOTP$ を動作させているため B_nTOTP と呼称する。なお B_n は B_nTOTP の計算の基になる数字でありそれを加工した値 (B_n を基にあるハッシュ関数によりハッシュ値を求め B_n に応じて変わる変数) を利用して B_nTOTP 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 ($Owner Password$) が利用できることに着目し、 $TOTP$ (B_nTOTP) と OWP の双方を用いる認証システムを考案し実施する。

10

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。

$TOTP$ (B_nTOTP) 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。

B_nTOTP はブロック番号 B_n 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。

20

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 B_nTOTP や $TOTP$ と同じように運用できる。ただし B_nTOTP 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 B_nTOTP 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 B_nTOTP 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 B_nTOTP と OWP を使い分ける。

B_nTOTP はネットワークを介して数十秒ごとに B_nTOTP 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 (数力月から数年) 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。

30

【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 B_nTOTP 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。

40

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 9 A 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 9 B 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 9 A と図 9 B 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 9 A 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 9 B 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

50

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B n T O T P型もしくはT O T P型のパスワードが生成可能である。

本発明ではO W P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O T P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O T P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。O W P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T O T Pが実現可能となる。

一方でO W P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T O T P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O W Pを更新したいときにコントラクト管理者がK値を変更できるO W P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T O T Pの用途では主にブロック番号を用いB n T O T P型のパスワードと、B n T O T P型のパスワードにK値を変更できるO W P型パスワードを組み合わせたB n T O T P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B n T O T P型とO W P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T O T P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型T O T P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T mをR F C 6 2 3 8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B nをT O T PトークンのR F C 6 2 3 8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、R F C 6 2 3 8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、R F C 6 2 3 8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（O T P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（O T Pトークン）を発行し、そのO T P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N F C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。

【 0 0 1 7 】

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。

10

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ができる。

20

【 0 0 1 8 】

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す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。

30

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合わせたもので実現して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。

40

【 発明の効果 】

【 0 0 1 9 】

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3A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

50

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。

10

【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 T_m を $TF6238$ 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。

20

【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。

30

【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。

40

（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

50

を示した説明図である。

【図 1 A】図 1 A 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 1 B】図 1 B 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 2 A】図 2 A は本発明の認証システムを用いて認証を行うユーザー U A の端末 D A の説明図である。

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

【図 2 C】図 2 C 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 U C の端末 D C の説明図である。端末 D A と端末 D C の機能は同等である。秘密鍵情報が異なる。

【図 3 A】図 3 A は分散型台帳システム D L S を構成するブロックチェーン部を持ちネットワーク 2 0 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 3 A の説明図である。

【図 3 A A】図 3 A A は図 3 A の端末 3 A 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 3 A B】図 3 A B は図 3 A の端末 3 A 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 3 A C】図 3 A C は図 3 A の端末 3 A 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 3 B】図 3 B は図 3 A のサーバ P（3 A）と同じブロックチェーン部を持ちネットワーク 2 0 上で分散型台帳システム D L S を構成するノードとなる端末 3 B の説明図である。

【図 3 C】図 3 C 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 3 C の説明図である。

【図 3 D】図 3 D は印刷物や表示画面及び N F C 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 3 D の説明図である

【図 3 D A】図 3 D A は図 3 D に記載のサーバ S V L o g（端末 3 D）の記憶部（記憶装置、3 0 D）と入出力装置（3 4 D、3 5 D）に関する説明図である。

【図 3 E】図 3 E は OTP トークンの購入または紙及び N F C 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 3 E の説明図である

【図 3 F】図 3 F はユーザ端末に対しサーバ P（3 A）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 3 F の説明図である。

【図 4 A】図 4 A 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（4 A）の説明図である。

【図 4 B】図 4 B 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（4 A）の記憶装置に関する説明図（実施の例）である。

【図 4 C】図 4 C は図 4 B において端末 4 A の記憶装置に平文データ 4 0 3 5 A が暗号化もしくは難読化されてソフトウェア 4 0 3 A の 4 0 3 0 A に内蔵されるとき説明図である。

【図 5 A】図 5 A 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（4 A）に広告を配信するサーバ端末の説明図である。

【図 5 B】図 5 B 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（4 A）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 5 B の

10

20

30

40

50

説明図である。

【図 5 C】図 5 C 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（4 A）に暗号化データを放送によって送付するサーバ端末 5 C の説明図である。

【図 6 A】図 6 A は本発明において O T P トークンの保有者に O T P 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 O T P 生成関数である。

【図 6 B】図 6 B は本発明において O T P トークンの保有者に O T P 生成回数記録機能を備えた O T P 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 6 C】図 6 C は本発明において O T P 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 O T P を認証する関数のフローチャート図である。

10

【図 6 D】図 6 D は本発明において O T P 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 O T P を認証する関数のフローチャート図である。

【図 6 E】図 6 E は本発明において図 6 C から O T P 認証回数等記録機能を除いた場合の O T P を認証する関数のフローチャート図である。

【図 6 F】図 6 F 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 O T P を認証する関数のフローチャート図である。基礎的な O T P 認証関数である。

【図 6 G】図 6 G は本発明において O T P 認証回数等記録機能を備えた O T P トークンの保有者のアクセスか判断して O T P 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。

20

【図 6 H】図 6 H は本発明において O T P トークンの保有者のアクセスか判断して O T P 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 6 X】図 6 X 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（3 C , 3 D , 3 E , 3 F , 5 A , 5 B）にユーザ端末（1 A や 4 A）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 7 A】図 7 A 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（T B には主にブロック番号 B n を用いる。B n T O T P 型パスワードの説明図でもある）。

【図 7 B】図 7 B は本発明においてパスワード O W P を算出するシード値となるコントラクトの内部変数 K C や B C をコントラクトの管理者が関数 f s c b 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。

30

【図 7 C A】図 7 C A 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 7 C B】図 7 C B 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 7 C C】図 7 C C 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 7 D】図 7 D 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 7 E】図 7 E は本発明において例として有価紙葉または N F C タグを用いてパスワード O W P 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。

40

【図 8 A】図 8 A 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 8 B】図 8 B は印刷物及び N F C 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 8 C】図 8 C 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 C R H N（4 0 3 A）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 8 D】図 8 D 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

50

C R H N (4 0 3 A) 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 9 A】分散型台帳システム D L S (分散型台帳システム D L S) にブロックチェーン型のデータ構造を用いた O T P 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 9 B】分散型台帳システム D L S (分散型台帳システム D L S) に有向非巡回グラフ型のデータ構造を用いた O T P 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 8 A、図 8 B、図 8 C、図 8 D 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ン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(電氣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。

10

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。

20

1. ユーザー U A の端末 D A (端末 1 A)

本発明の O T P トークンを用い、O T P を表示または認証を行うコンピュータ端末 D A または端末 1 A (図 1 および図 2 A、図 2 A A の端末 1 A) を備えたユーザー U A とその端末 1 A。

端末 1 A は記憶装置にブロックチェーンのサーバ 3 A 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 3 A のサーバ 3 A) などを示す U R I、ブロックチェーンへのアクセス時に利用する秘密鍵 P R V A (図 2 A A の秘密鍵情報 1 0 1 A) を備える。端末 1 A は通信装置 1 2 A を持ちネットワーク 20 を介してサーバ 3 A にアクセスする。

30

サーバ 3 A に O T P の生成を求めてアクセスする際には図 6 A や図 6 B の O T P 生成関数のフローチャートに記載するように秘密鍵 P R V A 1 0 1 A と 1 0 1 A 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 T I D A をもつ O T P トークンが必要である。O T P の認証を求めるときも秘密鍵 P R V A 1 0 1 A と 1 0 1 A 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 T I D A をもつ O T P トークンが必要とすることもでき(図 6 C、図 6 E、図 6 G、図 6 H)、また図 6 F や図 6 D の O T P 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 O T P 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。

40

端末 1 A のユーザー U A に加え端末 1 B のユーザー U B、端末 1 C のユーザー U C、端末 4 A のユーザー U P も存在する。端末 4 A は端末 1 A 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 U P とユーザー U A は同じ人物であり秘密鍵 1 0 1 A と秘密鍵 4 0 1 A 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 3 A)

<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 D L S を構成

50

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 $B_n \times 15$ 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(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(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(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。E

10

20

30

40

50

R C 7 2 1 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 . OpenZeppelin、<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 E R C 7 2 1 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 1 0 1 C 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。E R C 7 2 1 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ー識別子 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 E R C 7 2 1 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 T I D A 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。

10

例えば図 3 A C の 3 0 1 4 A のようにユーザー識別子 A には T I D A の番号を持つトークンの所有情報（3 0 1 5 A）、ユーザー識別子 B には T I D B の番号を持つトークンの所有情報（3 0 1 6 A）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。

20

【 0 0 2 9 】

< 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 E R C 7 2 1 規格のトークンはイーサリアム上での O T P 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 E R C 7 2 1 規格のトークンにワンタイムパスワード（O T P）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 O T P 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 E R C 7 2 1 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 O T P 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 O T P トークンは E R C 7 2 1 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。

30

本発明では O T P トークンもしくは O T P 生成トークン・O T P 生成コントラクトは、O T P 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。O T P 認証コントラクトまたは O T P 認証コントラクト内部の O T P 認証関数は、O T P 生成コントラクトの O T P 生成関数と一致した O T P を計算するための変数と処理部を持ち、O T P の生成と認証の処理を行うことができる。図 3 A A や図 3 A B や図 3 A C がそのコントラクト説明図であり、認証関数を端末 3 A でなく端末 3 D に持つときの例は図 3 D A である。

40

ブロックチェーン部を持つサーバ群（3 A、3 B 等）とブロックチェーン部に接続する端末（1 A、1 C 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 E R C 7 2 1 規格のトークンに O T P 生成関数を備えさせ、E R C 7 2 1 型の O T P 生成トークンを発行できるコントラクト（O T P 生成コントラクト）とした。そして O T P 生成コントラクトの O T P 生成に用いるシード値と同じ値にさせることのできる O T P 認証関数を O T P 生成コントラクトに備えさ

50

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を検証し認証させ、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）のサービスヘ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OTP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。

10

【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、あるユーザ識別子Aのユーザにトークン番号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はユーザ識別子Aのユーザが望む場合にユーザ識別子Bなどのユーザ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。

20

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。

30

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。

40

（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

50

(本発明ではブロック番号 B_n 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 f_h の引数に用いてハッシュ値を得てそれをワнтаイムパスワードとして戻り値にするワнтаイムパスワード生成関数を備えたワнта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нта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нта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 f_h がワнта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нта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нта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。)

10

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。

20

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 f_h 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 、 B_n とハッシュ関数 f_h 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。

30

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 B_n や BC などのある時刻 T においてかわる変数 T_m も一致していなければならないが、 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 T_m や B_n 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。

40

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 B_n 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 B_n に補正値を加算減算して運用する場合に、 B_n が一致しなくなる場合には B_n 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нтаイムパスワードの算出>

50

ユーザU Aの端末D A (端末1 A) のアクセスに応じて端末3 Aは処理を行う。端末1 Aの記憶装置に記録された秘密鍵P R V A (秘密鍵1 0 1 A) 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3 2バイトの秘密鍵から6 4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、E C D S A、E l l i p t i c C u r v e D i g i t a l S i g n a t u r e A l g o r i t h m) 。そして6 4バイトの公開鍵に対してKeccak-256というS H A - 3と類似のハッシュ関数を用いて3 2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。

10

サーバP (端末3 A) 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、ブロックチェー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、O T P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 (O T P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T I D Aとコントラクトのシークレット変数のK C値3 0 1 1 A (図3 A Aや図3 A Bや図3 A Cに記載の内部変数K C 3 0 1 1 A) 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T B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f h (図3 A Aや図3 A Bや図3 A Cに記載のハッシュ関数f h 3 0 1 0 A) の引数として利用する。計算例は $O T P = f h (T I D A , K C , T B)$ である。O T P認証関数の実行時にユーザー識別子AやO T Pトークンの保有を確認する場合も同様である。

20

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 $O T P = f h (A , T I D A , K C , T B)$ として計算される。

そして前記T Bに最新のブロック番号B n (図3 A Aに記載の3 0 0 1 Aがブロック番号B n) 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 $B n T O T P = f h (A , T I D A , K C , B n)$ を利用する事を特徴とするO T Pの計算方法を用いたO T Pトークンを本発明では用いる。

T m (またはT B) にB nを用いるときは $O T P = f h (A , T I D A , K C , T B)$ でも $O T P = f h (T I D A , K C , T B)$ でもよい。具体的には $O T P = f h (A , T I D A , K C , B n)$ でも $O T P = f h (T I D A , K C , B n)$ でもよい。

30

ここで $O T P = f h (T I D A , K C , T B)$ でもよい理由としては、例として短時間の6 0秒ごとに更新されるO T Pの場合は保有するユーザーが変更されてもB nが6 0秒ごとに変わるので6 0秒前の過去に計算された $O T P = f h (T I D A , K C , B n)$ 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1 0 1 A) 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 $O T P = f h (A , T I D A , K C , T B)$ を好ましくは用いた。

また前記T BにO T P生成トークンのコントラクトの内部変数B C値3 0 1 3 A (図3 A Aや図3 A Bや図3 A Cに記載の内部変数B C 3 0 1 3 A) を用い、前記3 0 1 3 Aはコントラクトの管理者端末1 Cの秘密鍵1 0 1 Cを用いてブロックチェーンへアクセスし3 0 1 3 Aを書き換えることの出来るセッター関数3 0 1 2 A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 $O W P = f h (A , T I D A , K C , B C)$ として管理者の設定するB C値に応じてパスワードを変えられることを特徴とするO T Pの計算方法を用いたO T Pトークンを本発明で用いる。

40

T m (またはT B) にB Cを用いるときは $O T P = f h (T I D A , K C , T B)$ よりも $O T P = f h (A , T I D A , K C , T B)$ が好ましいかもしれない。具体的には $O T P = f h (T I D A , K C , B C)$ よりも $O T P = f h (A , T I D A , K C , B C)$ が好ましいかもしれない。

ここで $O T P = f h (T I D A , K C , T B)$ よりも $O T P = f h (A , T I D A , K C , T B)$ が好ましい理由としては、例としてK CやB Cはコントラクト管理者が任意の

50

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。

10

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BnOTP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】

20

<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BnOTP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OTP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。

30

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。

40

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

50

れブロック番号 B_n が1つずつ増えていく。ユーザー U_A 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つかず 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 B_n を基に表示する間隔を増やす変数 n を用い、 $B_n \bmod n$ として、 B_n の n で割った余り m を求め、 B_n から m を減算し B_{n-r} として ($B_n - m = B_{n-r}$ として)、 B_n の代わりに B_{n-r} 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 B_n 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の実施例となる $EERC721$ 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нта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 B_n 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нтаイムパスワード B_nTOTP は $B_nTOTP = fh(A, TIDA, KC, B_n, BC, V)$ 、または $B_nTOTP = fh(A, TIDA, KC, B_n, BSZ)$ 、または $B_nTOTP = fh(A, TIDA, KC, B_n, BC, BSZ)$ 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 B_n 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 $B_nTOTP = fh(KC, B_n)$ や $B_nTOTP = fh(B_n)$ や $B_nTOTP = fh(fh(B_n))$ でもよく、本発明ではブロック番号 B_n 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TTY(図4Bの4033A)と、その鍵データTTY(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。

10

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。

20

【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。

30

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。

40

【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

50

ある端末 3 C でもよい。

サーバ端末 3 C の記憶装置データを端末 1 A に記憶させサーバ端末 3 C を仮想機械として端末 1 A に構築し、端末 1 A 内部で端末 1 A と端末 3 C を通信させつつ端末 1 A をネットワーク 20 を介して端末 3 A と接続させることで端末 1 A に構築された仮想機械端末 3 C にログインすることが可能となる。例えば端末 3 C 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 3 C において E C M A S c r i p t 等でサーバ 3 A のブロックチェーン部とユーザーの端末 1 A 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 101 A 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 101 A 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 3 C 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 T I D A 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 B n T O T P 生成し、B n T O T P 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。

O T P の認証関数及び生成関数で計算される B n T O T P はハッシュ関数 f h とコントラクト内部変数 K C と前記の A、T I D A を用いて $B n T O T P = f h (A, T I D A, K C, B n)$ 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 E R C 7 2 1 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 D W A L T 1 6 0 3 A と通信できるものもある。）

認証結果が正しい時、サーバ 3 A にアクセスしてきたユーザー識別子 A やトークン番号 T I D A といったブロックチェーンに関する情報と、端末 1 A の I P アドレスまたは位置情報や端末 1 A に固有の装置 I D （デバイス I D ）または端末 1 A の入力装置 14 A のセンサ 144 A のセンサ値を端末の環境値 I P V として図 6 X で示すデータ構造でサーバ 3 A 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 1 A のセンサ 144 A のセンサ値は主にセンサ 144 A、環境センサ 1440 A、位置センサ 1441 A、モーションセンサ 1442 A、生体認証センサ 1443 A 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 140 A や 141 A、143 A、142 A といった入力装置 14 A の入力そのものでも良い。143 A や 142 A や 141 A、140 A 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 1440 A 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センサである。

位置センサ 1441 A 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 1442 A 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 1443 A は端末 1 A 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。

< ログイン実行と実行後の処理 >

端末 3 C から端末 1 A 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 1 A 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 S V L o g i n 端末 3 C 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。O T P 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 1 A をアクセスさせ、処理を行わせた際に O T P の生成関数を実行させ O T P を取得したのち取得した O T P を引数に用いて認証関数を実行させたとき、3 0 1 7 A や 3 0 1 7 A A といった変数を変更させる。

10

ここでウェブサイト等の認証とログインに用いるとき 3 0 1 7 A や 3 0 1 7 A A 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。3 0 1 7 A や 3 0 1 7 A A 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。

20

(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 3 D といったサービス提供機器に提示し認証するときも 3 0 1 7 D A 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 3 D 内の記憶装置のデータのうち、他のユーザーや端末 3 D 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 3 D が端末 3 C と同じくネットワーク 2 0 に接続しノード端末 3 A や端末 3 F や 3 E と接続できる場合には端末 3 D は端末 3 C と同等とみなし端末 3 C と同じ処理が行うものとみなす)

3 0 1 7 A や 3 0 1 7 A G はトークン番号に対応した O T P 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进行操作してもよい。O T P 認証関数 3 0 1 8 A の実行時に認証関数 3 0 1 8 A 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 3 A B の 3 0 2 1 A、3 0 2 2 A、3 0 2 3 A があってもよい。

30

前記 3 0 1 8 A、3 0 2 1 A、3 0 2 2 A、3 0 2 3 A 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 3 0 1 8 A 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 3 0 1 7 A A に記録された残高の範囲内で振り込み先に O T P 認証関数が一致した際に振り込む処理をもつ 3 0 2 2 A があってもよい。

3 0 2 2 A 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。

40

【 0 0 4 1 】

< 不正ログインの検知 >

本発明ではログインしたユーザの I P アドレス(I P 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 I D (またはハッシュ値)と、トークン番号、ユーザー識別子を S V L o g i n (図 3 C の端末 3 C) の記憶装置 3 0 C の 3 0 1 1 C に図 6 X 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 I P アドレス(I P アドレスのハッシュ

50

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

10

20

30

40

50

サーバ 3 A 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 3 C や端末 3 D 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 1 A の秘密鍵 1 0 1 A を用いて 1 0 1 A に対応付けられた O T P トークンのトークン番号が T I D A のとき O T P の認証関数及び生成関数で計算される $B n T O T P$ はハッシュ関数 $f h$ とコントラクト内部変数 $K C$ と前記の A 、 $T I D A$ を用いて $B n T O T P - 1 = f h (A, T I D A, K C, B n)$ という引数と関数で表される。

ここで端末 1 A に搭載された秘密鍵 1 0 1 A のほかに 1 0 1 A 2 という 2 番目の秘密鍵があり、その秘密鍵 1 0 1 A 2 から計算されるユーザー識別子 $A 2$ とそれに対応付けられて発行された O T P トークンのトークン番号 $T I D A 2$ があったとき 2 つ目の $B n T O T P - 2 = f h (A 2, T I D A 2, K C, B n)$ が計算できる。

O T P 生成関数で $B n T O T P - 1$ と $B n T O T P - 2$ 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 、 $T I D A$ 、 $B n T O T P - 1$ 、 $A 2$ 、 $T I D A 2$ 、 $B n T O T P 2 - 2$ という形で、2 つの秘密鍵 1 0 1 A と 1 0 1 A 2 から計算されるユーザー識別子と O T P トークンのトークン番号と O T P (ここでは $B n T O T P - 1$ および $B n T O T P - 2$ を例として示したが、O W P の場合は O W P - 1 と O W P - 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 1 0 1 A 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 1 0 1 A 2 が漏洩しなければ関数の引数である $B n T O T P - 2$ (O W P の場合は O W P - 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 O T P トークンの認証に用いるときは、O T P トークンの認証を行うコントラクトにて秘密鍵 1 0 1 A から計算されるユーザ識別子 A と秘密鍵 1 0 1 A 2 から計算されるユーザー識別子 $A 2$ をユーザー $U A$ 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 $T I D A$ と $T I D A 2$ が同一のユーザー $U A$ に配布されていることを O T P 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 3 C や 3 D などの本発明においてサービス提供側となる端末に $U A$ の二つの識別子 A と $A 2$ もしくはトークン番号 $T I D A$ と $T I D A 2$ を登録し、ウェブサイトログインするときに A と $T I D A$ と $B n T O T P - 1$ の入力を求める認証を行った後、 $A 2$ と $T I D A 2$ と $B n T O T P - 2$ 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 3 C や 3 D において $B n T O T P - 1 = f h (A, T I D A, K C, B n)$ と $B n T O T P - 2 = f h (A 2, T I D A 2, K C, B n)$ を別々にサーバ 3 C 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 O T P トークンの O T P 入力と認証をサーバ端末 3 C や 3 D で求めることもできる。この場合 3 C や 3 D はユーザー $U A$ の複数の秘密鍵に由来するユーザー識別子 A と $A 2$ や $T I D A$ と $T I D A 2$ の対応付けを行って 3 C や 3 D の記録装置に記録されている必要がある。

サーバ端末 3 C や 3 D を用いて複数の秘密鍵による O T P トークンの認証に用いるときは、O T P トークンの認証を行うサーバ端末 3 C および 3 D で秘密鍵 1 0 1 A から計算されるユーザ識別子 A と秘密鍵 1 0 1 A 2 から計算されるユーザー識別子 $A 2$ 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 $T I D A$ と $T I D A 2$ が同一のユーザー $U A$ に配布されていることを O T P 認証関数を含むサーバ端末 3 C や 3 D に登録する部分を備えていてもよい。O T P 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 O T P 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 $256 \times N$ [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ることで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て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ー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る、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秘密鍵を記録して利用できている者がどうかを確認する必要がある、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3AC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、

10

20

30

40

50

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 3 0 2 4 A は本発明のコントラクトに必要な応じて記入し、コントラクト
管理者が書換できてよい。3 0 2 4 A にはコントラクト管理者の端末 1 C の秘密鍵 1 0
1 C 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。

【 0 0 4 6 】

< 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 K N B N (図 3 A A から図 3
A C に記載の 3 0 2 4 A) にレイティング情報が記載される。3 0 2 4 A に書かれたレイ
ティング情報は O T P 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。

10

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
えることができてよい。

【 0 0 4 7 】

4 B . 入場口や建物設備への紙又は I C 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 S V L o g (図 8 B や
図 3 D に記載のサーバ端末 3 D) を用いる。図 8 B に端末の接続図を示す。サーバ S V L
o g (端末 3 D) 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 S
V L o g (端末 3 D) でもよい。そして端末 3 D 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。3 D は組み込みシステム用の
M C U 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。

20

本発明では N F C などの通信機能を備えた I C タグ・ I C カード型のチケット 1 9 A ま
たは紙のチケット 1 8 A (および紙のチケット 1 8 A と同じ O T P 認証情報を表示させた
ディスプレイの表示面 1 5 0 0 A) 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 O W P を利用する (ここで I C は Integrated circuit であり集積回路のこと) 。

30

【 0 0 4 8 】

1 9 A は非接触の N F C タグや、接触型端子を持つ I C カードであり、1 9 A の利用者
ではないユーザーに不正使用させないように 1 9 A に利用者がパスワードとして P I N 等
を設定してもよい。1 9 A と端末 3 D との通信を行い O W P などの認証情報を伝達する際
に、1 9 A に設定された P I N 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 N F C タグの情報を端末 3 D の通信装置 3 2 D を通じて端末 3 D に伝達してもよい。

【 0 0 4 9 】

ここで P I N は個人識別番号 (Personal identification number) の略であり、P I N
は例えば 4 桁の整数のパスワードである。1 9 A の P I N は 1 9 A 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。1 9 A は無線により通信するため 1
9 A を所有するユーザーが知らぬ間に 1 9 A の情報が端末 3 D に伝達されないように P I
N を用いてもよい。1 9 A は 3 D 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。P I N などを用いて 1 9 A に記録された O W P を用いる認証情報を暗号
化してもよい (O W P を、P I N 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) 。1 8 A や 1 5 0 0 A 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、1 9 A 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 P I N コードを設定出来てもよい。

40

P I N を用いることで 1 9 A 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 P I N の入力が必要とすることは P I N 入力の時間をユーザーに要求しユーザーの利便

50

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13.56MHz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の設定をしなくても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。）

10

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。

20

【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。

30

NFCタグ19は、端末1Aが保有するユーザ識別子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。

40

【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3018D

50

A (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

10

20

30

40

50

ンなどに用いる想定の本 n T O T P の場合は A と T I D A と A r g B n T O T P の情報が鍵であり、A と T I D A と V e r i B n T O T P の情報が錠に対応する。))

ブロックチェーンに鍵となる O T P トークンと O T P トークンが生成する O W P 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、3 D が 3 A 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 3 D 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 1 A の O W P 型のパスワードとユーザー識別子 A とトークン番号 T I D A を 1 5 0 0 A や 1 8 A や 1 9 A で認証できる情報を設定することが求められる。

【 0 0 5 5 】

端末 3 D と端末 3 A で計算される O W P を一致させるために、K C 値 3 0 1 1 A ・ 3 0 1 1 D A や B C 値 3 0 1 3 A ・ 3 0 1 3 D A 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。K C 値や B C 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 O T P 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。

【 0 0 5 6 】

限られたコミュニティの行事で利用する入場券として 1 5 0 0 A や 1 8 A や 1 9 A を利用する場合には、ユーザー識別子 A とトークン番号 T I D A と O W P の 3 つの必須情報に加え 1 5 0 0 A や 1 8 A や 1 9 A 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 1 5 0 0 A や 1 8 A や 1 9 A に記録してもよくそれら情報は文字列情報として 1 5 0 0 A や 1 8 A に表示印刷され 1 9 A の場合は端末 1 A 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 とトークン番号 T I D A と O W P 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 3 D の 3 4 0 D に読み取らせることができる。また O W P 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 とトークン番号 T I D A と O W P 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 O W P のみは二次元バーコードとして記録される形態の 1 5 0 0 A や 1 8 A があってもよい。

1 5 0 0 A については O W P 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 1 A が持ってもよい。セキュリティが保たれた場合においては 1 8 A を読み上げる画像認識端末があってもよい。

(O W P はサービス提供端末 3 D 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 O W P の含まれた 1 8 A や 1 5 0 0 A を読み取り、読み上げ、撮影、画像認識したり、P I N などによって保護されていない 1 9 A の情報を読み取られた場合は O W P などが漏洩し不正利用される恐れがある。)

【 0 0 5 7 】

< 入場時の O T P トークンを利用済みにする処理等 >

端末 3 D 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 3 0 1 8 A (または 3 0 1 8 D A) の実行回数記録部分 3 0 1 7 A や 3 0 1 7 A A (または 3 0 1 7 D A) にチケットをユーザーが本発明の O T P 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、3 0 1 7 A や 3 0 1 7 A G (または 3 0 1 7 D A) にチケットのサ

10

20

30

40

50

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。

10

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。

20

【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とトークン番号TIDAを含む1500Aや18Aや19Aをコピーして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。

30

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。

40

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。

50

【 0 0 5 9 】

3 D について防犯カメラ 3 4 2 D を用いないとき場合に防犯上利用可能な機能として、図 8 B のランプなどの発光素子 3 5 1 D またはブザー等発音素子 3 5 2 D を利用し音や光にて O W P 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 3 D を備えて使用する場合には N F C タグ 1 9 A に認証に用いる情報記録され、1 9 A を金庫内部の端末 3 D が通信装置 3 2 D を用いて N F C タグ 1 9 A 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出来る。ブザーの代わりに通信装置 3 2 D 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 3 4 2 D とランプなどの発光素子 3 5 1 D またはブザー等発音素子 3 5 2 D を併用して利用してもよい。

10

例として駅の改札において用いる 1 5 0 0 A や 1 8 A や 1 9 A 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 U A が現れたとき改札の開閉装置 3 5 0 D は閉じた状態にして U A をその場に留め、防犯カメラ 3 4 2 D とランプなどの発光素子 3 5 1 D またはブザー等発音素子 3 5 2 D 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 U A に尋ねることができる。

【 0 0 6 0 】

端末 3 D が金庫等の容器である場合に限らず、端末 3 D 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 3 5 1 D や発音素子 3 5 2 D を動作させ認証結果が正しいか否かを端末 3 D の周囲（周囲とは 3 5 1 D や 3 5 2 D や 3 2 D 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 3 5 1 D 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。

20

【 0 0 6 1 】

< 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 3 D がインターネットワークに接続されサーバ 3 A と接続している場合。

秘密鍵 P R V A が漏洩し本来の利用権を持つユーザー U A が、1 5 0 0 A や 1 8 A や 1 9 A を 3 D 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 U B が秘密鍵 P R V A (1 0 1 A) 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 O W P の流出と使い回しによる不正利用も考えられる。

30

不正利用の際に U B 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 3 0 1 8 A の実行回数を記録する変数 3 0 1 7 A や 3 0 1 7 A A をインクリメント等することで記録する。

またユーザー U A 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 U A 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 U B の顔、体系、歩行情報等と照らし合わせ、ユーザー U A が不正に入場していないか判断することに利用できる。

40

ここでサーバ 3 D がサーバ 3 A と同じくブロックチェーンのノードとなるときは 3 D は 3 A と同じ機能を持つので 3 D のブロックチェーン部（3 0 0 D および 3 1 0 D ）に認証関数 3 0 1 8 A が記録されており、3 A ではなく 3 D のブロックチェーン部にユーザー U A の端末 1 A がアクセスして認証関数 3 0 1 8 A を実行してもよい。

不正利用時はユーザー U A の O T P 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 U A の O T P トークンの利用をサービス提供者が端末 1 C を用いて停止できる変数を端末 3 A の O T P 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

50

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。

【 0 0 6 2 】

2．改札や入場口において端末 3 D がローカルエリアネットワーク（LAN）に接続されサーバ 3 A 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 2 0 とは切断されている場合、端末 3 D の記憶装置には 1 5 0 0 A や 1 8 A や 1 9 A を生成するのに用いたハッシュ関数 3 0 1 0 A と 3 0 1 0 D A と一致させ、K C 値 3 0 1 1 A と 3 0 1 1 D A を一致させ、B C 値 3 0 1 3 A と 3 0 1 3 D A を一致させ、ほかに変数や関数を O W P の計算に用いる場合にはそれらを一致させ、端末 3 A と端末 3 D での O W P 型 O T P 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 3 0 1 8 D 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 3 0 1 7 D A に記録したり、あるいは 3 0 1 6 D に記録してもよい。

10

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 3 D へのアクセス権を持つ端末を持ちいて端末 3 D のデータベース 3 1 1 6 D（3 1 1 4 D や 3 1 1 5 D 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 O T P 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 1 8 A 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 1 8 A から得て 3 1 1 6 D の顧客情報と照合し、O T P 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）。

20

【 0 0 6 3 】

3．端末 3 D 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 3 D がネットワーク 2 0 と接続されていないときも、端末 3 D の記憶装置には 1 5 0 0 A や 1 8 A や 1 9 A を生成するのに用いたハッシュ関数 3 0 1 0 A と 3 0 1 0 D A を一致させ、K C 値 3 0 1 1 A と 3 0 1 1 D が一致させ、B C 値 3 0 1 3 A と 3 0 1 3 D A を一致させ、ほかに変数や関数を O W P の計算に用いる場合にはそれらを一致させ、端末 3 A と端末 3 D での O W P 型 O T P 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 3 0 1 8 D A 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 3 0 1 7 D A に記録したり、あるいは 3 0 1 6 D に記録してもよい。

30

施錠の解錠をした後にアクセスできる部分に端末 3 D があり、3 D の通信装置 3 2 D 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（1 A や 1 C）の通信装置から端末 3 D の通信装置 3 2 D を経て記憶装置 3 0 D の K C 値 3 0 1 1 D A または B C 値 3 0 1 3 D A の変更またはハッシュ関数 f h の変更を行い、端末 3 A の O T P 生成関数 3 0 0 9 A の生成する O W P と認証関数 3 0 1 8 D A が生成する O W P が同じものとなるよう変更できる手段を備える。O W P の算出に用いる K C 値 3 0 1 1 D A または B C 値 3 0 1 3 D A 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。

40

【 0 0 6 4 】

< 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ない。生成時、認証時にそれぞれの O T P 生成関数や O T P 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 3 0 1 7 A や 3 0 1 7 A G や 3 0 1 7 A A 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 3 0 1 7 A や 3 0 1 7 A G を監視することで不正利用を防ぐことにつながる。（ブロックチェーン上にはないが端末 3 D の 3 0 1 7 D A もカウントする変数である）

50

【 0 0 6 5 】

例えば紙のチケットとしてOWP (1 8 A) 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 1 5 0 0 A) 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 3 D) などにブロックチェーンを監視する処理部を 3 1 1 1 D 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нтаイムパスワード生成回数の記録変数 3 0 1 7 A G (呼び出し回数) 、あるいは認証回数の記録変数 3 0 1 7 A A もしくは 3 0 1 7 D A 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нта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。

10

【 0 0 6 6 】

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нта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 3 D は不正利用の通知は困難である。この場合は端末 3 D 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。)

20

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 1 5 0 0 A や 1 8 A や 1 9 A 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。

【 0 0 6 7 】

< レイティング及び看板情報 >

30

サーバ端末 3 C 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 3 D 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нта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 3 0 2 4 A 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 3 0 2 4 A 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 1 8 A 、 1 9 A 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 1 8 A 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。

40

【 0 0 6 8 】

4 C . 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 4 0 3 A) を利用できる。ここでソフトウェアCRHNは図 4 B のソフトウェア 4 0 3 A である。図 8 C 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 4 0 3 4 A (図 4 B の 4 0 3 4 A) 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 4 A の端末 4 A) を用いてサーバ端末 3 A にアクセスし端末 4 A の秘密鍵 4 0 1 A 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 3 0 1 8 A の戻り値CTAU 4 0 3 1 A を得て、戻り値 4 0 3 1 A とあらかじめ設定されたパスワード値AKTB 4 0 3 2 A

50

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TTY4033A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TTY4033Aのほかに、CTAU4031AとAKTB4032AとソフトウェアCRHN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TTY4033Aを好ましくは用いる。

さらに前記鍵情報に加え、TTY4033A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履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もよい。

端末5Bはユーザーが自身の保有する本発明のOTP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

10

20

30

40

50

ロックチェーンでA K T B 3 0 4 2 Aを記述したトランザクションを受け取る等)にてA K T B 4 0 3 2 Aをユーザー端末4 AのユーザーUPに伝達し、UPは4 Aの4 0 3 Aに4 0 3 2 Aを入力することでOTPトークンが戻り値4 0 3 1 Aとソフトウェア4 0 3 Aの鍵情報4 0 3 0 2 Aと4 0 3 Aの計算手順からT T K Y 4 0 3 Aを算出し暗号化ファイル4 0 3 4 Aを復号し復号された平文ファイル4 0 3 5 Aを得て4 0 3 5 A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。

10

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。

20

【0072】

OTPトークンの譲渡の例を示す。ユーザーUP(端末4 Aの利用者)とユーザーUB(端末1 Bの利用者)がネットワーク20とサーバーP(サーバ端末3 A)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3 Aにて4 A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UAからUBに所有者情報を書換えたもの)、端末5 B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1 A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。

30

ここで暗号化ファイルの暗号化時にA K T B 4 0 3 2 A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。A K T B 4 0 3 2 A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A K T B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。

40

本発明の実施例では暗号化データの復号にはCTAU4031A、A K T B 4 0 3 2 A、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T T K Y 4 0 3 3 Aを生成出来るとき、T T K Y 4 0 3 3 A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OTPt

50

ークンに用いる事ができ、図 8 A に記載の端末 3 C のウェブサイトのログイン用 O T P トークン、図 8 B に記載の紙や N F C 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 O W P の生成を行う O W P 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 O T P トークンは譲渡可能であるが、O T P 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 3 0 4 1 A の変更はコントラクト管理者が行う。

【 0 0 7 4 】

< 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 5 B 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システムでもよい。(端末 5 B 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 G i t h u b . I n c . 、ギットハブ・ジャパン合同会社の G i t h u b といい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 5 B 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 O T P トークンを表示し、その O T P 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 O T P 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 5 B 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 1 C に提示し、購入代金などの決済などを行い O T P トークンの購入と O T P トークン購入者のユーザー識別子に対するトークン発行の指示、 A K T B 4 0 3 2 A が必要な場合には A K T B 4 0 3 2 A を暗号化時に利用して暗号化ファイル 4 0 3 4 A を作成し配布してもよい。

前記の 4 0 3 4 A 配布する際にユーザーの電子メールに A K T B 4 0 3 2 A 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 A K T B 4 0 3 4 A 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 5 B などの端末にアクセスできるダウンロード専用の U R I からダウンロードするようにしてもよく、U R I は電子メールに記述するか 5 B 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 U R I を表示してユーザーに伝達してもよい。

【 0 0 7 5 】

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 4 0 3 4 A 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 5 B 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 O T P 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 O T P 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ることに対応する。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 O T P 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 O T P 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 O T P 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)

10

20

30

40

50

【 0 0 7 6 】

< 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 3 0 2 4 A が記録される。図 4 B の 4 0 3 5 1 A や 4 0 3 5 2 A 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 5 B や 3 F 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 4 B の 4 0 3 5 1 A や 4 0 3 5 2 A 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。

【 0 0 7 7 】

< コンテンツの閲覧実行環境 >

コンテンツの証明書をを用いても、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 4 B の 4 0 3 5 1 A や 4 0 3 5 2 A ）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 4 0 3 A 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。

【 0 0 7 8 】

< 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 C R H N 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 C R H N を閲覧したときに、

広告サーバー C R H N c m（図 5 A のサーバ端末 5 A）への接続を行うプログラムが実行され、端末 5 A 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

I P アドレス（I P 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 6 X のようなデータとして端末 5 A 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 I P アドレス、異なる位置情報、異なる装置 I D、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 I D については、デバイス I D などのコンピュータ製造 I D やオペレーティングソフトウェアの I D、ウェブブラウザの I D に加えて、端末 4 A 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 4 0 3 A 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 4 0 3 A を閲覧したときに、サーバ端末 5 A への接続を行うプログラムを実行しなくとも本発明の O T P 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 4 0 3 A の権利者や暗号化データの平文データの権利者が 5 A への接続を行うプログラムを記録させ、ソフトウェア 4 0 3 A やコンテンツの利用者が同意する場合にサーバ端末 5 A 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

10

20

30

40

50

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うる。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。

10

20

30

40

50

【 0 0 8 3 】

< オフライン時の閲覧 >

閲覧済みの証明書データ O F B K M K 4 0 3 6 A、ユーザの秘密鍵 4 0 1 A、ソフトウェア 4 0 3 A 内部のキー情報 4 0 3 0 2 A を用いて復号し T T K Y 4 0 3 3 A を得る。

具体的には、ソフトウェア 4 0 3 A は O F B K M K 4 0 3 6 A に記述された A C T T K Y 4 0 3 6 0 A を 4 0 3 0 2 A を用いて復号し C T T K Y 4 0 3 6 1 A を得る。そして C T T K Y 4 0 3 6 1 A を 4 0 1 A を用いて復号し、T T K Y 4 0 3 3 A を得て、T T K Y 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。4 0 3 6 A 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。

10

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 4 0 3 A が備えていてもよい。

【 0 0 8 4 】

ユーザーの中には端末 4 A がネットワーク 2 0 から切断されたオフライン時の 4 0 3 6 A 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 4 0 3 6 A の利用形態も考えられる。)

20

その具体的な対策例及び実施例として、ソフトウェア 4 0 3 A はオフライン時の利用において 4 0 3 A 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 O F B K M K 4 0 3 6 A の認証およびコンテンツを閲覧できた時刻を検出し、4 0 3 6 A 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、4 0 3 6 A の情報に含まれる情報を復号して 4 0 3 3 A を得て、暗号化データやファイル 4 0 3 4 A を復号し、4 0 3 4 A を 4 0 3 6 A を用いて復号して閲覧などを行った時刻(4 0 3 6 A で閲覧を始めた現在時刻)を記録し、前記 4 0 3 6 A 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 4 0 3 A を停止させ、平文データ 4 0 3 5 A の利用を停止する。

30

【 0 0 8 5 】

ここでコンピュータ端末 4 A の内、スマートフォン型の端末 4 A は多くが位置情報の測位用に全球測位衛星システム G N S S からの無線信号受信装置 4 2 2 A もしくは 4 2 3 A を備え、時刻が更新されるのでこの機能を提供しやすい。G N S S からの信号には時刻情報が含まれる。G N S S 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 B I O S (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 4 0 3 A 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 4 0 3 A が閲覧を許してしまう恐れがある。

ソフトウェア 4 0 3 A において閲覧済みの証明書データ O F B K M K 4 0 3 6 A を用いて閲覧するには N I T Z (Network ID and Time Zone、ネットワークIDおよびタイムゾーン)、J J Y、G N S S 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 4 2 2 A もしくは放送受信装置 4 2 3 A と制御演算部 4 1 A および 4 3 A にある C P U (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 F C C 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。

40

4 1 A や 4 3 A を含む C P U と G N S S または J J Y または N I T Z の受信装置 4 2 2

50

A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TOP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・フィルムカメラ・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

10

20

30

40

50

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、それに付随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。例えば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

10

20

30

40

50

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 4 A であることも想定される。前記テレビジョン型端末 4 A を用いる場合は外部記録装置 4 6 A に秘密鍵を記録し 4 0 1 A 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付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 4 A の記憶装置 4 0 に秘密鍵 4 0 1 A 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 4 A を廃棄もしくは譲渡する際に秘密鍵 4 0 1 A の情報を別途異なる記憶装置に記録した後、4 0 1 A を 4 0 A 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 1 A や端末 4 A 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。

10

【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 8 D において端末 4 A がインターネットに接続されていないが、端末 4 A にはスマートフォン型端末 1 A と連携する無線通信装置があるとき、端末 4 A は端末 1 A を通じてインターネット 2 0 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。

20

A . 図 8 B で示した OWP を用いる方法を用いる場合。

例として端末 1 A にて OWP を生成する OTP トークンを取得し、前記 OTP トークンを用いて端末 3 A 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 4 A に入力するかもしれない。パスワードの記録された NFC タグ 1 9 A を 4 2 0 A に読み取らせ、認証ができたときは、端末 4 A の認証関数に記録された戻り値 C T A U 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 8 B 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 T T K Y 4 0 3 3 A の元になる情報は C T A U 4 0 3 1 A のみとなる。そこで A K T B 4 0 3 2 A に該当する情報を端末 4 A に入力し、さらにデータ放送中の暗号データの中に T T K Y 4 0 3 3 A 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 4 0 3 A 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。

30

【0097】

無線受信装置のみ備えるテレビジョン端末 4 A 等の場合には、放送局 5 C の送信情報に時刻情報、あるいは 5 C が 3 A 等から読み取ったブロック番号 B n を付与し、テレビジョン端末 4 A 側で B n を受信させ、端末 4 A 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。

40

【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 OTP トークンによる認証後の戻り値 C T A U の取得を行い、A K T B などの情報を入力し、復号用の鍵 T T K Y 4 0 3 3 A の算出を行い、4 0 3 3 A 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 >

50

ここで受信機端末 4 A 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 4 5 3 A 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 4 A である場合も想定できる。その場合はソフトウェア 4 0 3 A 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 O T P トークンに対応する秘密鍵 4 0 1 A が端末 4 A に記録されており、O T P 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 O T P トークンを用いたオンラインゲームサーバ端末 3 C へのログインできるマルチメディア端末 4 A を提供することも考えられる。

10

【 0 1 0 0 】

< 放送局の設置場所と形態 >

端末 5 C 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。

【 0 1 0 1 】

放送局 5 C 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。J J Y のような時刻情報を放送する無線局や G N S S 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。

20

【 0 1 0 2 】

< 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 G N S S 用放送局 >

放送局 5 C もしくは 5 C に 3 A 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 5 C であり、かつ放送用のデータが全球測位衛星システム G N S S 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 5 C 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。

30

この場合、放送局 5 C 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 T B 及び K C 値を用いて計算したハッシュ値を添付し G N S S 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 G N S S 放送局となった端末 5 C から端末 4 A は時刻情報を受け取ることもできるかもしれない。

G N S S 用の放送局 5 C が放送する測位用の航法データに B n T O T P やメッセージ認証符号 M A C 値を添付することで測位情報の流通時に 3 A を用いて O T P 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 B n T O T P や O W P 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 4 A は認証された位置情報と時刻情報を知ることができる。

40

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

【 0 1 0 3 】

< 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。

50

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 KNB_N 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。

10

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 $fs cb 3012A$ 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 $KC 3011A$ または $BC 3013A$ にアクセスできる関数 $fs cb 3012A$ 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 $fs cb 3012A$ 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。

20

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 B_n を用いたワンタイムパスワード $B_n TOTP$ 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 $fs cb$ と $fs cb$ で書き換えられるシード値 $KC 3011A$ や $BC 3013A$ がコントラクトに備えられていることを特徴とする。

30

【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の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 $ERC 721$ 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。

40

【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

50

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が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。

10

【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)。

20

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】

30

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。

40

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ク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

50

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。

10

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B_n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B_nTOTPを用いた認証方法について説明する。

20

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。

30

図1の実施例においてOTPの生成にブロック番号B_n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、B_n、Aの4つを基にしてハッシュ関数f_hの引数とした後に引数をハッシュ関数に渡してB_nTOTP = f_h(A, TIDA, KC, B_n)としてハッシュ値B_nTOTPを生成し、OTP認証関数3009A又は3009AはB_nTOTP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f_hは例えばSHA-2のSHA256である。

40

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B_nTOTPを戻り値として利用しない場合、F107に示すようにB_nTOTP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B_nTOTP - 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

50

生成関数と F 1 0 0 から F 1 0 7 までの処理を用いる n 桁の符号なし整数の O T P を生成する O T P 生成関数を同一のコントラクトに備えた O T P 生成を行う O T P 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 O T P 生成関数とそれに対応する O T P 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 3 2 バイト（整数では最大 2 の 2 5 6 乗の数であり総当たり攻撃が困難と想定される）の O T P 生成関数とそれに対応する O T P 認証関数を用いて認証を行うこともできる。

【 0 1 1 2 】

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 f h にハッシュ値が 3 2 バイトの戻り値を出力する S H A 2 5 6 関数を用い、F 1 0 4 の選択肢を O T P 生成関数の処理プログラムに設けずに、 $B n T O T P = f h (A , T I D A , K C , B n)$ として 3 2 バイトの O T P を算出する O T P 生成関数（図 6 A においては F 1 0 0、F 1 0 1、F 1 0 2、F 1 0 3、F 1 0 4、F 1 0 5 の順にフロチャートを経て動作する関数。あるいは図 6 B において F 1 0 0、F 1 0 8、F 1 0 1、F 1 0 2、F 1 0 3、F 1 0 4、F 1 0 5 の順にフロチャートを経て動作する関数。）と、

前記 $B n T O T P$ を符号なし整数として型変換し 1 0 の 7 乗で割った剰余である 7 桁数字の O T P を算出する O T P 生成関数（図 6 A の F 1 0 0、F 1 0 1、F 1 0 2、F 1 0 3、F 1 0 4、F 1 0 7 の順にフロチャートを経て動作する関数。あるいは図 6 B において F 1 0 0、F 1 0 8、F 1 0 1、F 1 0 2、F 1 0 3、F 1 0 4、F 1 0 7 の順にフロチャートを経て動作する関数。）の二通りの O T P 生成関数を O T P 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 6 A と図 6 B の違いは、O T P 生成関数 3 0 0 9 A の実行を記録する回数などを保存する変数 3 0 1 7 A や 3 0 1 7 A G に対して関数 3 0 0 9 A の実行回数の記録や増加処理もしくは関数 3 0 0 9 A の実行に必要な数値残高の増減等の変更処理 F 1 0 8 の有無である。

F 1 0 1 では入力された引数から O T P トークンの O T P 生成関数 3 0 0 9 A 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、 $m s g . s e n d e r$ のユーザー識別子）がトークン番号 T I D A の O T P 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 F 1 0 1 がなければ O T P トークンの持ち主でないユーザーが O T P 関数を実行できてしまうため、メッセージ送信者が 3 0 0 9 A を実行する際にはそのメッセージ送信者が O T P 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。

F 1 0 0 では T I D A のみを入力して処理を行うこともできるが、実際には F 1 0 1 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 $m s g . s e n d e r$ のユーザー識別子）を関数実行処理時に $m s g . s e n d e r$ のユーザー識別子を A として O T P 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、F 1 0 1 に記載した。

（注）O T P トークンの生成の条件文 F 1 0 1 では O T P トークンの保有者かどうかを判定するが、この部分があるユーザー識別子の O T P トークンの保有数とし保有数が 1 つ以上の O T P トークンの数量を持つときトークン番号を引数として O T P 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 $m s g . s e n d e r$ 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 $m s g . s e n d e r = A$ ）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。

【 0 1 1 3 】

ハッシュ関数 f h は実施例では S H A - 2 の S H A 2 5 6 や S H A - 3 であり、他に M D 5 や R I P E M D、S H A - 1、S H A - 2、S H A - 3 が利用できる。f h は暗号学的ハッシュ関数であればよい。例えば、f h が S H A 2 5 6 のとき、 $B n T O T P = S H A 2 5 6 (A , T I D A , K C , B n)$ 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 S H A 2 5 6 関数などで求めている。

具体例として $\text{SHA256}(\text{EncodePacked}(A, \text{TIDA}, \text{KC}, \text{Bn}))$ のような処理である。ここで関数 $\text{EncodePacked}(W, X, Y, Z)$ 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、 $\text{SHA256}(\text{Mes})$ 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、 $\text{SHA256}(\text{EncodePacked}(A, \text{TIDA}, \text{KC}, \text{Bn}))$ と、 $\text{SHA256}(\text{EncodePacked}(\text{TIDA}, A, \text{KC}, \text{Bn}))$ 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 f_h 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上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を行い、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。

10

20

30

40

50

OTP生成を行う端末1 Aおよび端末1 A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3 Aと、ウェブサイトなどのサービスを扱う端末3 Cにアクセスできる端末4 Aがあり、端末1 Aと端末3 Aと端末3 Cと端末4 Aがネットワーク2 0に接続されており、1 AがOTP生成関数を実行しOTPを生成し端末1 Aの出力装置1 5 Aに出力した後、ユーザーU Aはそれを目視してヒトの手で端末4 Aの入力装置に入力し端末4 Aは入力されたOTPを用いてOTP認証を行いその結果を端末3 Cと通信しやり取りし、認証結果に応じて端末4 Aをログインさせサービスを提供させることができる。

【0 1 1 6】

<ブロック番号B n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3 A Aや図3 A Bや図3 A Cに記載のOTPを検証し認証するOTP認証関数3 0 1 8 Aの動作はOTP生成関数3 0 0 9 Aと似ており、認証関数3 0 1 8 A内部でT I D A、K C、B n、Aをハッシュ関数f hを用いて $VeriBnOTP = fh(A, TIDA, KC, Bn)$ を求め、ユーザーがサーバ3 A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T I D A、A、入力された $ArgBnOTP$ のうち、I F文などによる条件式で、 $ArgBnOTP$ が $VeriBnOTP$ 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1 A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1 Aに返し認証できなかった時の処理を行う。ここで前記B n T O T Pでは実施例で3 2 バイトのOTPが生成されるが、B n T O T Pをを入力n桁数字のパスワードB n T O T P - 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きも同様である。図6 Cから図6 Hに認証関数3 0 1 8 A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1 Aや図1 Bである。

【0 1 1 7】

図6 Cから図6 Hに示す認証関数3 0 1 8 Aのフローチャートについて説明する。フローチャートの処理F 1 1 0ではOTP認証関数3 0 1 8 Aの引数入力にてユーザー識別子A、トークン番号T I D A、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。

【0 1 1 8】

図6 Fは認証関数3 0 1 8 Aの実施例の一つであり、基本的な処理例である。図6 Fに示す処理を用いた認証は端末3 Cや端末3 D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。F 1 1 0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T I D Aを受け取り、F 1 1 3にて引数から $VeriOTP$ を計算する。このときブロック番号B nとシークレット変数K C値を用いる。 $VeriOTP = fh(A, TIDA, KC, Bn)$ を計算し、F 1 1 4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、F 1 1 6の処理を行い、一致しない場合はF 1 1 8の処理を行う。図6 Fを用いる端末の接続例は図8 A、図8 B、図8 C、図8 Dである。

図6 FのOTP認証関数の形態は端末3 Cや端末3 Dにおいて利用できる。

【0 1 1 9】

図6 Dは図6 Fの処理に用いる真偽値や整数などの変数3 0 1 7 Aや3 0 1 7 A Aや3 0 1 7 D Aに対し、OTP認証関数3 0 1 8 A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F 1 1 5を追加したものである。3 0 1 7 Aや3 0 1 7 A Aや3 0 1 7 D Aは真偽値、整数、文字列などのデータである。3 0 1 7 Aや3 0 1 7 A Aや3 0 1 7 D A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6 Dを用いる端末の接続例は図8 A、図8 B、図8 C、図8 Dである。

10

20

30

40

50

【 0 1 2 0 】

図 6 C 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 6 C は図 6 D の処理に、F 1 1 1 の処理を追加したものである。F 1 1 1 では認証関数 3 0 1 8 A 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 F 1 1 7 に示すように処理を中断する。F 1 1 1 にて認証関数 3 0 1 8 A の実行者がユーザー識別子 A の場合には、F 1 1 2 の認証関数の処理を続行し、入力された O T P = A r g O T P が問題ない場合には F 1 1 3、F 1 1 4、F 1 1 5、F 1 1 6、F 1 1 6 と処理が行われる。F 1 1 4 にて A r g O T P が V e r i O T P と一致しないときは F 1 1 8 の示すように処理を中断する。図 6 E は図 6 C の処理 F 1 1 5 を取り除いたフローチャートである。図 6 E および図 6 C を用いる端末の接続例は図 8 A、図 8 C、図 8 D であり、図 8 B は端末 3 D がネットワーク 2 0 に接続ができ端末 3 A に接続できる用途において利用できる。

10

【 0 1 2 1 】

図 6 C と図 6 E に示す処理方法は 3 A の O T P トークンに関するコントラクトにある所有者情報 3 0 1 4 A を用いるため、3 A などブロックチェーン上の端末と 3 D が接続され 3 0 1 4 A の情報が同期され共有されなければ図 6 C と図 6 E に記載の認証方法は端末 3 D では利用できない。端末 3 D 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 2 0 を介して端末 3 A に接続されるか端末 3 A 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 3 D においても図 6 C 及び図 6 E と図 6 G と図 6 H の処理は利用出来る。

20

端末 3 D 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 2 0 に接続ができない場合には、図 6 C 及び図 6 E と図 6 G と図 6 H の処理を行うことは困難である。

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

【 0 1 2 2 】

図 6 C と図 6 E は認証関数 3 0 1 8 A の実行者 (m s g . s e n d e r) がユーザー識別子 A であるかを判定する処理 F 1 1 1 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 1 0 1 A 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 6 C と図 6 E の違いは認証ができた際の 3 0 1 7 A や 3 0 1 7 A A や 3 0 1 7 D A を変更する処理 F 1 1 5 の有無である。図 6 C には F 1 1 5 が有り図 6 E には F 1 1 5 が無い。

30

【 0 1 2 3 】

図 6 G と図 6 H は認証関数 3 0 1 8 A の実行者が O T P トークンの保有者かを判定する処理 F 1 1 9 をもつ。この処理は O T P 生成関数時の図 6 A や図 6 B のフローチャートに記載された処理 F 1 0 1 と同様の処理である。処理 F 1 1 9 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 1 0 1 A によってブロックチェーンのノードである端末 3 A 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 T I D A の O T P トークンを保有するか F 1 1 9 にて判定し、O T P 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 6 G と図 6 H の違いは認証ができた際の 3 0 1 7 A や 3 0 1 7 A A や 3 0 1 7 D A を変更する処理 F 1 1 5 の有無である。図 6 G には F 1 1 5 があり図 6 H には F 1 1 5 が無い。

40

【 0 1 2 4 】

< 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 の関数等と呼び出して利用してもよい。

50

例えば図 6 F の F 1 1 6 において図 3 A B の 3 0 2 2 A や 3 0 2 3 A の処理を行うために O T P トークンの認証コントラクト 3 0 0 8 A A 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 3 0 1 8 A の戻り値 3 0 2 1 A を端末 1 A に出力してもよい。

もしくは他の例として O T P 生成や認証を行うコントラクト X のハッシュ関数 f_h 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を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 f_h 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 f_h と O T P 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 f_h を更新し、コントラクト X はコントラクト Y の f_h を利用できてもよい。

10

【 0 1 2 5 】

< 認証結果呼び出しを用いたサービスの提供 >

O T P 認証関数を呼び出して O T P や A や T I D A を入力し、その結果得られた認証結果の戻り値 C T A U 3 0 2 1 A を用いてサービスの提供を行う。

ここでは 4 A . ウェブサイトのログイン用途、 4 B . 入場口や建物設備への紙又は I C 式入場券、利用券、解錠鍵としての利用、 4 C . 暗号化データおよびファイルの復号と閲覧、 4 T . 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。

20

【 0 1 2 6 】

< 4 A . 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 T B のうち、ブロック番号 B_n を基にした T O T P 型ワンタイムパスワードトークンを用いる。T B にブロックチェーン上の最新のタイムスタンプ 3 0 0 2 A がある場合にはそれを T B として用いることもできる。

【 0 1 2 7 】

T B にはブロックハッシュ B_h (3 0 0 3 A) 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 S o l i d i t y では最新のブロック番号から数えて 2 5 6 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 B_n を引数に計算していると考えられる。 B_n を引数に B_h を計算していると考えたとき、ブロックハッシュ B_h を用いる方法もブロック番号 B_n を用いる方法と変わらない。

30

S o l i d i t y 言語で式として表現すると $B_n T O T P = (A , T I D A , K C , B_h)$ 、 $B_h = B l o c k h a s h (B_n)$ であるので $B_n T O T P = (A , T I D A , K C , B_h = B l o c k h a s h (B_n))$ であり、ブロックハッシュ B_h を用いるときもブロック番号 B_n を用いているため、 $B_n T O T P = (A , T I D A , K C , B_h)$ と $B_n T O T P = (A , T I D A , K C , B_n)$ 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 B_h を用いる方法もブロック番号 B_n を用いる方法の異なる形態であると本発明では考える。

40

ブロックハッシュを T B として用いることも出来る。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 B_n 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。

【 0 1 2 8 】

ブロックハッシュ B_h を T O T P 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 T O T P 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 1 5 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 O T P を

50

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 B_h ではなくブロック番号 B_n であれば、 B_n を基に表示する間隔を増やす変数 n を用い、 $B_n \bmod n$ として、 B_n の n で割った余り m を求め、 B_n から m を減算し B_{n-r} として ($B_n - m = B_{n-r}$ として)、 B_n の代わりに B_{n-r} 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 B_n を好ましく用いた。

【0129】

ブロックハッシュ B_h においても B_h は B_n を引数として用いて過去のブロックハッシュ B_h を求めることができるが、その計算では B_n 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 B_h そのものはあるブロック番号 B_n 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 B_n 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 B_n を使ったほうが良い場合と B_h 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。

B_n 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 B_n に加え、もしくは B_h 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 B_h 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 B_h 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】

B_h をタイムスタンプに用いるときは B_h 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れば、どの時刻のブロックハッシュ B_h が分からない。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 B_h 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 B_n OTP 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 B_n OTP 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 B_n OTP 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 B_n OTP = (A, TIDA, KC, B_n) でもよいし、前期 B_n OTP 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 B_n OTP = $f_h(A, TIDA, KC, B_n, BC, V)$ でもよいし、またはブロックサイズ BSZ を加えた B_n OTP = $f_h(A, TIDA, KC, B_n, BSZ)$ 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 B_h 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 B_n OTP の式は B_n OTP = $f_h(A, TIDA, KC, B_n, BC, V, B_h)$ である。

B S ZはVに応じて変わるときは $V = B S Z$ とみなし $B n T O T P = f h (A , T I D A , K C , B n , B C , B S Z , B h)$ である。

【0132】

本発明のハッシュ関数 $f h$ の引数はAとT I D A、K C、B nやB C、そしてVやB hが用いられるが、例えばK CやB CあるいはVやB h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B n T O T P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、T I D A、K C、B nやA、T I D A、K C、B Cを持つことを本発明では特徴とし、さらにA、T I D A、K C、B n、B C、V、B h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T I D Aをキーとしたマッピング変数V U (V U [T I D A]) をシード値として含む $B n T O T P = f h (A , T I D A , K C , B n , B C , V , V U [T I D A])$ 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V U [T I D A]については別途説明する。

【0134】

認証関数の戻り値を端末1 Aが取得し、1 Aはその戻り値を3 C (S V L o g i n) 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3 Cに戻り値を渡し、認証結果が正しい時3 C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C P G T 3 0 1 9 Aや、T I D A、B n、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、

I PアドレスもしくはI Pアドレスのハッシュ値などI Pアドレスに基づく識別子や、位置情報、端末1 Aに固有のI D、端末1 Aの入力装置1 4 Aのセンサ1 4 4 A等のセンサ値をI P V値として

3 Cの記憶装置に図6 Xの形でユーザー識別子Aやトークン番号T I D AとI P V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6 X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I P Vにて3 C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6 Xに記載する例のように、同一の秘密鍵1 0 1 Aに由来するユーザー識別子から異なるI P V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U Aの秘密鍵が漏洩しユーザー識別子Aとトークン番号T I D Aの組み合わせに対し、端末3 C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T I D A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3 C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3 Cはサービス用途によっては、図6 X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3 Cも実施形態として存在する。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3 Cでは、図6 X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3 C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3 Cの利用コストが高くなる恐れがある。

またサーバ端末3 C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3 C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O T P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 6 X 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 3 C も実施形態として存在する。

【 0 1 3 7 】

3 C において図 6 X 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 O T P 認証システムとしては必須の機能ではなく、サーバ 3 C のサービス提供者と端末 1 A のユーザー U A が図 6 X 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 6 X 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 O T P 認証システムにおいて秘密鍵 1 0 1 A が複数の端末に記録され利用された場合には図 6 X 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。

10

【 0 1 3 8 】

図 8 A 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 3 C と、端末 3 A 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。

O T P の生成コントラクト (図 3 A B の 3 0 0 8 A G) において顧客が O T P を生成し、その O T P (主に B n T O T P 、定期的に更新できるならば O W P も) とユーザー識別子とトークン番号 T I D A を用いて認証関数 3 0 1 8 A 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 3 0 1 8 A の実行後に識別子 A もしくはトークン番号 T I D A をキーとしたマッピング変数 3 0 2 3 A を備え、3 0 2 3 A 20にあるユーザー識別子 A やトークン番号 T I D A 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 3 0 2 2 A を持っていてよい。そして 3 0 2 3 A と 3 0 2 2 A が認証コントラクト 3 0 0 8 A A や 3 0 0 8 A に含まれ、認証関数 3 0 1 8 A で認証できた場合に操作できるようプログラムされて 3 0 0 8 A A や 3 0 0 8 A に備えられていてもよい。

20

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 O T P トークンのトークン番号 T I D A に対する資産残高やポイント等の値 3 0 2 3 A と、3 0 2 3 A をコントラクトに書き込み保存する関数 3 0 2 2 A を持っていてよい。

【 0 1 3 9 】

< 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 >

30

本発明の O T P (B n T O T P および O W P) の生成時または認証時にコントラクトへ O T P 生成関数及び認証関数の実行回数を内部変数 3 0 1 7 A または 3 0 1 7 A G または 3 0 1 7 A A に記録させることができる。ここで内部変数 3 0 1 7 A または 3 0 1 7 A G または 3 0 1 7 A A 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 3 0 1 7 A 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 S o l i d i t y において利用できる型の一つである。)

【 0 1 4 0 】

40

O T P 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 3 0 1 7 A または 3 0 1 7 A G または 3 0 1 7 A A に記録することで、ユーザー U A の端末 1 A の秘密鍵 1 0 1 A が漏洩し、ユーザー U A が知らぬ間に攻撃者がブロックチェーンに秘密鍵 1 0 1 A を用いてアクセスし O T P 生成関数を実行し O T P を生成した場合には、O T P 生成関数を不正に実行されて取得された事実が 3 0 1 7 A や 3 0 1 7 A G に記録される。

ユーザー U A が O T P 取得のために実行したはずのない O T P 生成関数の実行回数が増えたことで (もし 3 0 1 7 A が O T P 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 U A は秘密鍵 1 0 1 A 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 1 0 1 A の秘密鍵に対応するユーザー識別子のトランザク

50

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UA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することが好ましい。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、BnT OTPやOWPといったパスワードを生成し、それを用いて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

10

20

30

40

50

者の端末が端末 3 A にアクセスして O T P 生成関数で生成する際に実行される 3 0 1 7 A や 3 0 1 7 A G が変化するので、前記変数の変化をユーザー U A に通知することで O T P が攻撃者に取得され紙や N F C 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 3 D に記憶された認証回数記録部分も端末 3 D 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 3 D 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 H M A C により M A C 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。

10

このように O T P 認証関数と O T P 生成関数のいず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 U A 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。

【 0 1 4 4 】

< 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続く処理 3 0 2 2 A をコントラクトに設定し、3 0 2 2 A 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 3 0 2 3 A を書き換えることができる。ここで内部変数 3 0 2 3 A 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 3 0 2 3 A である。変数 3 0 2 3 A 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。

20

【 0 1 4 5 】

< 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 3 0 0 8 A A はこの場合 O T P 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。

30

【 0 1 4 6 】

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 G K B A (またはポイント口座番号 G K B A 。 G K B A はトークン番号やユーザー識別子でもよい) 。
- 2 . 口座 G K B A の名義を匿名化した値 M I G A (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 . G K B A の資産の残高 A S T A 。 G K B A は 3 0 2 3 A 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 A S T A [トークン番号] 。
- 4 . G K B A に対応するトークン番号 T I D A もしくはユーザ識別子 A を対応付けたデータベース G K D B 。

40

G K B A や M I G A 、 A S T A 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 O T P 認証関数をもつコントラクト 3 0 0 8 A A (または 3 0 0 8 A) に設置されており、O T P 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 G K B A への振り替えを行う処理ができてよい。(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。)

【 0 1 4 7 】

ユーザー識別子 A の持つトークン番号 T I D A の O T P トークンに預けられた残高 A S T A [T I D A] (T I D A をキーとする 3 0 2 3 A) があって、

50

ユーザー識別子 B も T I D A の O T P トークンを持ち同様に残高 A S T A [T I D B] を持つとき、A が B の T I D B トークンに A の A S T A から数値 t r s 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 T I D A の O T P トークンに預けられた残高 A S T A [T I D A] (T I D A をキーとする 3 0 2 3 A) の一部をユーザー U A が指定し、ユーザー識別子 B の持つトークン番号 T I D B の O T P トークンに預けられた残高 A S T A [T I D B] (T I D B をキーとする 3 0 2 3 A) に振り込む関数もしくは処理 3 0 2 2 A があり、

ユーザー識別子 A のユーザーがトークン番号 T I D A の O T P トークンにより O T P 認証を行い処理 3 0 2 2 A と認証関数 3 0 1 8 A の処理 (3 0 2 2 A に 3 0 1 8 を組み込んだ、もしくは 3 0 1 8 A の後に 3 0 2 2 A の処理を続けた処理) を実行し、O T P 関数の認証結果が正しい時、処理 3 0 2 2 A は T I D A をキーとするマッピング変数 3 0 2 3 A から t r s を引いて A S T A [T I D A] - t r s とした後、T I D B をキーとするマッピング変数 3 0 2 3 A へ T I D A の持ち主であるユーザー識別子の指定する数値 t r s を足した数値 A S T A [T I D B] + t r s に変更することで、数値を変更でき、数値 t r s の振り込みができる。

このように本発明の O T P 認証システムを用いて O T P 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。

【 0 1 4 8 】

関数 3 0 2 2 A や資産残高を示す 3 0 2 3 A 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。

【 0 1 4 9 】

また銀行がサーバ 3 C 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。

【 0 1 5 0 】

インターネットバンキングにおける資産残高をサーバ 3 C 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。

【 0 1 5 1 】

< 会員サイトへのログイン用 O T P 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 (E C サイト)、ソーシャルネットワーキングサービス S N S、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 3 C 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。

【 0 1 5 2 】

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 O T P トークンの O T P 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 O T P 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 B n M i n t をトークン番号をキーとしたマッピング型変数として O T P を生成するコントラクトに記録し、O T P を生成する関数に、実行時の最新のブロック番号 B n が数値が表示したい期間に相当するブロック番号 B n V a l i d + B n M i n t 以内であれば O T P 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 B_n が、数式 $B_n < B_{n_{\text{Min}}t} + B_n \text{Valid}$ であるかどうか判定させ、ブロック番号 B_n 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、OTPT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 OTPTトークンによる投票数は何票あるか（つまり OTPT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。OTPT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。

10

【0156】

<ユーザー側が設定できる投票によるシード値 $VU[TIDA]$ >

OTPT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 OTPT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 OTPT を計算させることで OTPT の生成と認証とウェブサイトログインを行う OTPT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。

20

【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 OTPT 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 OTPT トークンの OTPT のランダムさを応用し、OTPT トークンの生成した OTPT 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。

30

【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 OTPT トークンの OTPT を擬似乱数として利用しているとき、ユーザーの OTPT トークンの生成する OTPT データの将来の現れ方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。

40

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 OTPT 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 OTPT（ $BnTOTP$ ）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）OT

50

P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。

$$BnTOTPrnv = SHA256(EncodePacked(A, TIDA, KC, Bn, V, VU[TIDA]))$$

10

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。

20

【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。

30

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。

40

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】

50

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、 B_n が利用出来ない場合には B_n 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】

10

< 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 B_n 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 B_n 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 $f_{scb3012A}$ 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 B_n 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。

20

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 ($B_n TOTP$ 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。

30

しかし OWP を $TOTP$ 的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 $TOTP$ ($B_n TOTP$) 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 $B_n TOTP$ を用いて OWP を再現するときはブロック番号 B_n を符号なし整数の変数 M で割った剰余 r を用い、 B_n をから r を減算し B_{nr} として ($B_n - m = B_{nr}$ として) B_{nr} を求め、前記 B_{nr} を B_n の代わりに $B_n TOTP = fh(A, TIDA, KC, B_{nr})$ 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 $B_n TOTP$ を生成・表示・認証させることもできる。

40

前記の $B_n TOTP$ 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 B_{nr} が変化し自動的に $B_n TOTP$ が変化する。ただしこの場合でも $B_n TOTP$ 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 $B_n TOTP$ 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。

50

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。

10

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】

20

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。

30

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 $fs_{cb3012A}$ 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 OTP 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、定期更新時の具体的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 OTP による認証システムが提供できる。

40

【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

50

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。

10

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>

20

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。

30

【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。

40

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

50

末 3 D に伝えてもよい。

【 0 1 7 3 】

有価紙葉 1 8 A を端末 3 D のカメラ・スキャナ装置 3 4 0 D に提示し、あるいは N F C タグ 1 9 A を 3 4 1 D および 3 2 D に提示したユーザー U A に対し、
端末 3 D が 1 8 A に記載されたユーザー識別子 A やトークン番号 T I D A とパスワード O W P の情報を 3 4 0 D を経由して読み取り端末 3 D の記憶装置 3 0 D の認証関数 3 0 1 8 D A (図 3 D A の 3 0 1 8 D A) の引数 T I D A 、ユーザー識別子 A 、パスワード A r g O W P として変数を渡し、
O T P 認証関数 3 0 1 8 D A 内部ではフローチャート図 6 F あるいは図 6 D の処理に従い、
A r g O W P に対し端末 3 D に記録された K C などのシークレット変数のシード値と 3 0 1 8 D A の引数であるユーザー識別子 A やトークン番号 T I D A を用いて V e r i O W P を計算し、3 0 1 8 D A に入力された A r g O W P と V e r i O W P が一致するか判定し、
一致するときには O T P 認証が成功したときの戻り値 3 0 2 1 D A を関数の戻り値 C T A U として返し、3 0 2 1 D A を返す前に 3 0 2 2 D A を実行するときは実行させる。
また 3 0 1 8 D A に入力された A r g O W P と V e r i O W P が一致するか判定し、一致しないときには O T P 認証が失敗したときの戻り値 3 0 2 1 D A を関数の戻り値として返す。

10

【 0 1 7 4 】

端末 3 D は 3 0 1 8 D A の関数の戻り値 3 0 2 1 D A や 3 0 2 2 D A に従って、O T P 認証が成功した場合の 3 0 2 1 D A を得たとき、有価紙葉 1 8 A をカメラ 3 4 0 D に提示もしくは N F C タグ 1 9 A を 3 4 1 D および 3 2 D に提示したユーザー U A 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錠装置 3 5 0 D を操作する。

20

3 0 2 1 D A が O T P 認証が成功した場合の値であるとき、端末 3 D は開閉や施錠等のアクセス制御を行う部分 3 5 0 D に対し制御を行い、改札や入場口ではユーザー U A 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 3 5 0 D 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 3 5 0 D が金庫など容器であるときは金庫の施錠を解錠する。

30

【 0 1 7 5 】

3 0 2 1 D A が O T P 認証が成功した場合の値であるとき、端末 3 D は施錠された部分 3 5 0 D を解錠するとともに 3 5 1 D や 3 5 2 D を用いて光や音にてユーザー U A や端末 3 D の周囲に解錠ができたことを知らせることができる。

3 0 2 1 D A が O T P 認証が失敗し入場できない場合の値の場合、3 5 1 D や 3 5 2 D を用いて O T P 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 3 4 2 D を利用できる端末 3 D では 1 8 A や 1 9 A を端末 3 D に提示したユーザー U A の風貌の撮影などもできる。3 4 2 D 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。

40

3 4 2 D 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 3 4 2 D 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。

3 4 2 D 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。

【 0 1 7 6 】

端末 3 D に施錠を解除する装置 3 5 0 D がなく、例えば入場口・退場口や改札口がヒト

50

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UAの風貌の撮影などでもできる。

【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。

10

【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。

20

【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。

30

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。

40

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

50

た 3 A や 3 B 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 3 0 0 D と 3 1 0 D を持ち、

前記 3 0 0 D の内部には、ネットワーク 2 0 上で端末 1 A が端末 3 A にアクセスし O W P を生成するのに用いるハッシュ関数 f_h やシード値 K_C や B_C などをもつ認証関数 3 0 1 8 D A を持つ 3 0 0 8 A A に類似の認証コントラクトを備えていてもよい。

端末 3 A に O T P 生成トークンのコントラクト 3 0 0 8 A G をデプロイし、端末 3 D に 3 0 0 8 A G と同じ方法で O T P の計算を行い認証する O T P 認証関数 3 0 1 8 D A 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 1 5 0 0 A や 1 8 A や 1 9 A の認証を行い入場などの処理を行ってもよい。

【 0 1 8 2 】

10

< I C タグ等デジタル機器による認証 >

N F C タグ 1 9 A は近距離無線通信装置 (N F C 装置) としてユーザー識別子、トークン番号、パスワード O W P を書き込むことの出来る接触式 I C カード、非接触式 I C タグ (R F I D タグ)、非接触式 I C カード (R F I D カード) が利用できる。

【 0 1 8 3 】

N F C タグ 1 9 A は自動車等に使われうる。自動車に対し 1 9 A 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 3 D に O W P 認証情報を暗号化された無線通信により送信し 3 D で O W P の認証を行い自動車の施錠装置 3 5 0 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、 1 9 A 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 1 9 A 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。

20

端末 3 D 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 3 D 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 3 D 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。

30

【 0 1 8 4 】

N F C タグ 1 9 A 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 1 9 A は I S O 1 4 4 4 3 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 I S O 1 4 4 4 3 タイプ B という非接触 I C 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 N F C タグのリーダー・ライター (端末 3 D においては 3 D の通信装置 3 2 D もしくは N F C タグの信号受信部 3 4 1 D) から N F C タグ 1 9 A のアンテナコイルを通じて N F C タグ 1 9 A に供給されるので電池を利用しない。

【 0 1 8 5 】

40

N F C 1 9 A は本発明の O T P 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 N F C タグ 1 9 A に秘密鍵 1 0 1 A 2 を持ち、 O W P 型の O T P 認証を行い自動車のドアの解錠後に原動機始動時に N F C にて通信し端末 3 D が 1 0 1 A 2 を用いてインターネット 2 0 と接続し、ブロックチェーンのノード 3 A にて、 1 0 1 A 2 に割り当てられた B n T O T P 型の O T P トークンを用いて T O T P 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 2 0 に常時接続できることが条件となる。インターネット 2 0 に接続される自動車において利用されうる。

自動車が B n T O T P 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 2 0 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 U A が N F C タグ 1

50

9 A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N F Cタグ1 9 Aに記憶されたユーザー識別子A、トークン番号T I D A、パスワードO W PをもちいてO W P型のO T P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。

【0 1 8 6】

N F C 1 9 Aは本発明のO T P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I S O 1 4 4 4 3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。

【0 1 8 7】

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1 3 0 k H z 帯、1 3 . 5 6 M H z 帯、4 3 3 M H z 帯、9 0 0 M H z 帯、2 , 4 G H z 帯等を利用できる。無線周波数について具体的には1 3 . 5 6 M H z 帯を用いて非接触型のI Cタグ、N F Cタグとして利用されるが、1 3 . 5 6 M H z 以外の無線周波数でもよい。例えば2 . 4 G H z 帯を利用してもよい。

N F Cにかかわる規格の具体例として1 3 . 5 6 M H z 帯の規格としてIS0/IEC18092、IS014443タイプA、IS014443タイプB等がある。2 . 4 G H z 帯ではI E E E (Institute o f Electrical and Electronics Engineers) の8 0 2 . 1 1系や8 0 2 . 1 5 . 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。

【0 1 8 8】

本発明のN F Cタグ1 9 Aは実施形態では1 3 . 5 6 M H z 帯と2 . 4 G H z 帯が利用されうる。N F Cタグ1 9 AはI S O 1 4 4 4 3タイプBに準拠して1 0 c m程度の距離で3 Dの通信装置3 2 Dおよび3 4 1 Dと通信できる。しかしN F Cタグ1 9 Aが無線パーソナルエリアネットワーク(無線P A N、Wireless Personal Area Network)を用いる場合は通信距離は1 0 c mを超えることもある。

【0 1 8 9】

N F Cタグ1 9 A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1 9 A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1 Aとウェアラブルコンピュータ端末1 BとN F Cタグ1 9 Aがあるとき、

N F Cタグ1 9 Aがウェアラブルコンピュータ端末1 Bの1 6 Bの外部記憶装置として接続され、1 6 Bの代わりに1 9 Aが1 2 Bと接続され、

N F Cタグ1 9 Aの記憶装置に端末1 Aが通信装置1 Bを介してアクセスし、O W P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O W P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1 Bがインターネットワーク2 0を介してサーバ端末3 AにアクセスしO W Pを生成した後、

前期パスワードO W P、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。

【0 1 9 0】

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N F Cタグ1 9 A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N F Cタグ1 9 Aが備えられたもの)、ベルト型(ベルトにN F Cタグ1 9 Aが備えられたもの)、衣服型(衣服にN F Cタグ1 9 A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N F Cタグ1 9 Aが備えられたもの、もしくは靴のインソール部分にN F Cタグ1 9 Aが備え付けられたもの) などである。

【0 1 9 1】

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

10

20

30

40

50

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。

10

【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、鞆型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。）

20

【0193】

ウェアラ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。

30

【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。

40

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

50

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T I D A、パスワードO W Pとして読み取れることが必要である。1 5 2 A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A T M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。

10

【0198】

<デジタル機器が無い、または使えない環境への対応>

O W P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N F Cタグ19Aの製造をユーザーの代わりに行き、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O W P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、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。

20

【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O W P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I CカードやI Cタグ式のチケット）を信書の形で渡す。

30

（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O W P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。）

40

【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U A入手したいとき、ユーザーU A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U Aは秘密鍵101Aを信頼できる第三者U Bに発行させ、その第三者U B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T I D AのO T P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U Bは前記ユーザー識別子Aに発行されたO T P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O T P生成関数からO W Pを取得し18Aや19Aを

50

製造してユーザーU A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19 Aや18 Aと共に101 Aを記録した信書を添付してもよい。第三者U Bが店舗でユーザーU Aに直接18 Aや19 A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101 Aを信託できる第三者U B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101 Bがユーザー識別子Bを名義としてトークン番号T I D AのO T Pトークンを発行し、前記トークンのO W Pから18 Aや19 Aを発行しユーザーU A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U Bが店舗でユーザーU Aに直接18 Aや19 A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U Aのトークン番号T I D AのO T Pトークンを預かる第三者U Bは法令で規制され資格が必要となるかもしれない。)

10

【0203】

1500 Aを表示することの出来る1 Aを、有価紙葉18 AやN F Cタグ19 A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1 A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U B(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1 Aの購入と何かに基づくO T Pトークンの購入を同時に契約し、第三者U Bは1500 Aを表示できる端末1 AをユーザーU Aに販売し、1500 Aを表示できる端末1 AをユーザーU A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。

20

【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A T M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O T Pトークンの購入及び発行とチケット等有価紙葉18 Aの製造ができてよい。

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(O T P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101 Aやユーザー識別子Aの文字列情報、パスワードO W P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。

30

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1 A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A T M端末がユーザーU Aを識別できO T P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A T M端末が備える顔認証などの生体認証手段をもちいてO T Pトークン及び18 A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O T Pトークンを利用しているか分からないよう配慮し、個人情報匿名化などを行う必要があるかもしれない。)

【0205】

40

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101 Aとユーザー識別子Aといった情報をカメラ・スキャナ等430 Dで撮影する方式よりは、I Cカードに記録しN F Cタグ19 A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。I Cカード19 A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N F Cを用いるI C式クレジットカード等でもよい。19 Aが個人番号カードのようなN F Cをもちいた身分証カードでもよい。

【0206】

19 Aは秘密鍵101 Aを記録していてもよい。ただし、19 Aに秘密鍵101 Aを記

50

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IC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

10

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。

【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

20

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る。

30

【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。）

40

【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

50

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とトークン番号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にユーザー識別子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とトークン番号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とトークン番号TIDAを設定することで、ユーザー識別子Bとトークン番号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

10

20

30

40

50

レット変数 K C や B C を書き換えることができると好ましい。

【0218】

端末 3 D 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 N F C タグ 1 9 A 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 N F C タグ 1 9 A と端末 3 D 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 N F C タグ 1 9 A と端末 3 D による施錠と、ダイヤ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
10 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 3 D 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、N F C タグ 1 9 A 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 2 0 に接続できる場合には B n T O T P 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 1 9 A で施錠を解錠した際には例として 1 0 0 k m の走行を許可し金属製の鍵で解錠した際には 5 0 k m の走行を許可するとい
20 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 3 D 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】

< I C 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 I C タグ等デジタル機器による認証システムを利用し、端末 3 D は防犯カメラなど入出力装置や記憶装置を多用し
30 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 3 D 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 3 D が金庫などの容器である時を例にすると、端末 3 D の電源装置 3 7 D 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 3 D 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 3 D を持つ金庫の庫内にアクセスできない場合であ
40 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 3 D 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 3 D 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 3 D 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 3 D 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 3 7 D 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 3 D はネットワーク 2 0 に接続できていると好ましい。ネットワーク 2 0 経由で端末 3 D の認証関数 3 0 1 8 D A の O W P 計算を行う K C や B C を変更できるためである。K C や B C 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 3 D のシード値と鍵 1
50

9 A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。

10

【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。

20

【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。

30

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）。

40

【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

50

ンタイムパスワード B_nTOTP 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 $GNS S$ 等からのブロック番号 B_n 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 $GNS S$ 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 $B_nTOTP = fh(TIDA, KC, B_np)$ として生成した際に、パスワード取得時のブロック番号 B_np 、トークン番号 $TIDA$ 、ワンタイムパスワード B_nTOTP 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。

10

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 B_np 、 $TIDA$ 、 B_nTOTP 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 B_nTOTP 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 B_nTOTP と $TIDA$ と B_np 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。

20

【0229】

なお、ここで $B_nTOTP = fh(TIDA, KC, B_np)$ として生成した場合について述べたが、ハッシュ関数 $fh(TIDA, KC, B_np)$ の引数にユーザー識別子 A を加え $B_nTOTP = fh(A, TIDA, KC, B_np)$ 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 B_np 、トークン番号 $TIDA$ 、ワンタイムパスワード B_nTOTP 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 B_np 、 A 、 $TIDA$ 、 B_nTOTP を入力させ、認証を行なってもよい。18A の代わりに B_np も記録し表示する 1500A を用いてもよい。

【0230】

30

$B_nTOTP = fh(TIDA, KC, B_np)$ や $B_nTOTP = fh(A, TIDA, KC, B_np)$ として計算する場合、 B_np 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 B_np の番号が最新のブロック番号 B_n 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 B_np の時に $B_nTOTP = fh(TIDA, KC, B_np)$ や $B_nTOTP = fh(A, TIDA, KC, B_np)$ として計算しユーザー識別子 A 、ブロック番号 B_np 、トークン番号 $TIDA$ 、ワンタイムパスワード B_nTOTP 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、 $GNS S$ などの時刻情報 T_m や放送されたブロック番号 B_n と B_np が、 B_nTOTP を生成した推定時刻 T_p について、ある閾値 L を基に比較を行い、 T_m と T_p の差分が L よりも大きい時、または放送される B_n と B_np の値が閾値 L よりも大きい時、その B_np 値と B_nTOTP 値による認証を受け付けないう認証関数 $3018DA$ や端末 3D の記録部にプログラムとして保存できる。

40

また端末 3D の内部に $GNS S$ 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

50

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。

10

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 $f_h(TIDA, KC, B_n)$ の引数KCをKCAに置き換え、 $B_nTOTP = f_h(TIDA, KCA[TIDA], B_n)$ としてOTPの生成と認証に用いてもよいし、 $B_nTOTP = f_h(A, TIDA, KCA[TIDA], B_n)$ のようにユーザー識別子を追加してもよい。 $OWP = f_h(A, TIDA, KCA[TIDA], BC)$ でもよい。

20

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。

$B_nTOTP = f_h(A, TIDA, KCA[TIDA], B_n)$ のようにユーザー識別子を追加してもよい。 $OWP = f_h(A, TIDA, KCA[TIDA], BC)$ 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KC値を変更・更新してもよい。

30

【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。

40

【0233】

<ユーザー識別子AのないOWPトークン>

B_nTOTP 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 $B_nTOTP = f_h(TIDA, KC, B_n)$ であり、前記 $B_nTOTP = f_h(TIDA, KC, B_n)$ は B_n 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

50

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らぬ入場できないが、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、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 トークンがユーザー識

10

20

30

40

50

別子 A に発行される。

コントラクト管理者端末 1 C もしくは発券サーバ 3 E を通じて O T P 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 S M S または郵送配達によりトークン番号 T I D A の O T P トークン発行を行ったことを通知する。

【 0 2 3 7 】

< 4 C . 暗号化データおよびファイルの復号と利用 >

図 1 B に示すように本発明では、図 8 A や図 8 B に示す本発明の O T P 認証システムを応用し、端末 5 B などから配布された暗号化されたデータ 4 0 3 4 A を持つ端末 4 A がネットワーク 2 0 を通じて端末 3 A に接続し本発明のブロックチェーンを用いた O T P 認証システムを用いて認証の戻り値 4 0 3 1 A を取得し、ソフトウェア 4 0 3 A (図 4 B に記載の 4 0 3 A 、 4 0 3 A はソフトウェア C R H N) は少なくとも 4 0 3 1 A を用い、好ましくは 4 0 3 2 A や 4 0 3 0 2 A といった複数の鍵情報を基にソフトウェア 4 0 3 A 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) 4 0 3 3 A 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。

【 0 2 3 8 】

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

図 1 A 及び図 8 A や図 8 B においては端末 3 C や端末 3 D が O T P 認証を行いアクセスする対象であった。しかし図 1 B や図 8 C や図 8 D においては O T P 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 3 C や 3 D が存在せず、端末 4 A とブロックチェーンのノードとなるサーバ端末 3 A とネットワーク 2 0 があって、端末 4 A の記録装置に暗号化データ 4 0 3 4 A とソフトウェア 4 0 3 A と O T P 認証後の戻り値 4 0 3 1 A と 4 0 3 2 A や 4 0 3 0 2 A といった複数の鍵情報を基にソフトウェア 4 0 3 A 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 4 0 3 3 A を算出し暗号化データを平文データに復号できる。 4 0 3 4 A は 4 0 3 3 A 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 4 0 3 5 A を求めることができる。 4 0 3 A 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。

【 0 2 3 9 】

暗号化データ 4 0 3 4 A は平文データ 4 0 3 5 A を暗号化できるバージョンの (版の) 4 0 3 A を用いることで作成される (4 0 3 A で用いる暗号化方式と T T K Y 4 0 3 3 A を算出できるならば 4 0 3 A を用いなくても暗号化することはできる。) 。

図 5 B の端末 5 B といったネットワーク 2 0 を用いてユーザー端末 4 A のアクセスに応じ、端末 4 A が端末 5 B の持つデータベース検索機能により 5 B 内部に収蔵された複数の暗号化データから端末 4 A が検索し探索させた暗号データ 4 0 3 4 A を端末 4 A にネットワーク 2 0 を介して配信する機能を持つ。また端末 5 B 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 4 0 3 4 A を配信・配布できる。

さらにネットワーク 2 0 を用いずとも暗号化されたデータ 4 0 3 4 A 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 U P と端末 4 A の元へ 4 0 3 4 A 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 4 0 3 4 A 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 8 D に示す端末 5 C により放送の形で端末 4 A を含む複数の端末に暗号データ 4 0 3 4 A を配信・放送してもよい。

【 0 2 4 0 】

図 8 C や図 8 D に示す形態の暗号化データは、解錠できる鍵情報 4 0 3 3 A を紛失すると復号できなくなり失われる恐れがある。図 8 B に示される例としての金庫の施錠装置のように、端末 3 D 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することに対し、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、

10

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ることができる。

20

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。

30

【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。

40

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(

50

T T Y 4 0 3 3 A、タイトルキー 4 0 3 3 A) をソフトウェア 4 0 3 A のプログラムに従って計算し、4 0 3 3 A を共通鍵に用いて A E S (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 H T M L 5 と E C M A S c r i p t 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。

【 0 2 4 3 】

本発明を実施する際にはソフトウェア 4 0 3 A における共通鍵暗号に用いた A E S 方式の鍵長は 1 2 8 b i t および 1 9 2 b i t を用いた。本発明の実施例で用いた A E S 方式は具体的には A E S - C B C 暗号であり明示的初期ベクトル (Initialization Vector : I V) 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 4 0 3 A には鍵のデータ長と C B C モードや初期ベクトル I V を設定する。

10

【 0 2 4 4 】

ソフトウェア 4 0 3 A の実施例として、文章形式では米国アドビ社の P D F 形式、音声では M P 3 形式、動画形式では M P 4 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 C A D データ (3 D プリンタに利用可能な 3 D C A D 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。

20

【 0 2 4 5 】

本発明の実施例では A E S 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 4 0 3 A を用いて作成または復号するための鍵 4 0 3 3 A を生成する際に、ソフトウェア 4 0 3 A は少なくとも鍵情報 C T A U 4 0 3 1 A を利用する。そしてソフトウェア 4 0 3 A に内蔵された鍵 4 0 3 0 2 A (C R K Y 4 0 3 0 2 A、C R H N ソフトウェア秘密鍵 4 0 3 0 2 A) 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 4 0 3 A に含まれない鍵 4 0 3 2 A (A K T B 4 0 3 2 A、合言葉 4 0 3 2 A、外部パスワード 4 0 3 2 A) を用いる。4 0 3 2 A 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 4 0 3 A 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、4 0 3 2 A の通知方法は暗号化するユーザーの方針による。

30

【 0 2 4 6 】

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 4 0 3 1 A
鍵情報を持つ変数 4 0 3 1 A は O T P 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、O T P 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。4 0 3 1 A は認証関数 3 0 1 8 A を実行したときに認証結果が正しい場合の戻り値 C A T U として設定される。ここで O T P トークンの発行等 E R C 7 2 1 規格のノンファンジブルトークンとしての処理と O T P の生成・認証を行うコントラクト 3 0 0 8 A 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。

40

また鍵情報 4 0 3 1 A 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。

4 0 3 A と O T P トークンと 4 0 3 1 A 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 4 0 3 3 A 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 4 0 3 1 A をコントラクト管理者が定期的に変更することで 4 0 3 3 A も更新される。変更された 4 0 3 3 A で平文データを暗

50

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り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において切り取り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・ユーザーごとに变えて4033Aも同じく顧客ごとに变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。

10

【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TTY4033A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。

20

【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は社内ですでに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。

30

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。

40

【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、オーダーメイ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

50

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】

10

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。

20

【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。

30

【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TTY4033Aを生成する。

40

【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4032A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プロ

50

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。

10

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。

20

【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TTY4033A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TTY4033A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TTY4033A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TTY4033A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。

30

本発明ではTTY4033A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トークンを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。

40

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

50

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。

10

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同様であり、書籍の著作者や出版社、著作権元、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。

20

【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OTPトークンがあってもよい。

30

【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。

40

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

50

品に関する情報が含まれるとき、未成年向けのレー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 5 A の記録装置 5 0 A 及び処理装置 5 1 A において、コントラクト識別子 C P G T、ユーザー識別子 A、トークン番号 T I D A、値 I P V、閲覧時刻 T や閲覧履歴情報 C n t (C n t 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 6 X 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 6 X の形式でなくともよい。図 6 X 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 I P V 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 O T P トークンのトークン番号について異なる I P V 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 6 X は説明図である。図 6 X 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 6 X 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。

10

【 0 2 7 3 】

端末 5 A の記録装置 5 0 A 及び処理装置 5 1 A において、トークン番号 T I D A について異なる I P V 値によるアクセスが端末 5 A 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 5 A に備え、

同一のユーザー識別子 A の秘密鍵 4 0 1 A に割り当てられたトークン番号 T I D A について、複数の I P 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 I P V 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 U A に連絡することができる不正アクセス監視機能 (図 5 A の 5 1 1 A、5 1 2 A、5 1 3 A) を備える。

20

プログラム 4 0 3 A に端末 5 A へ接続する U R I を記録することで広告表示機能と共に図 6 X 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。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 5 A に備えさせることができる。

平文データ 4 0 3 5 A についても端末 5 A へ接続する U R I を記録させ端末 5 A にアクセスさせ広告の配信機能と図 6 X 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 4 0 3 A における端末 5 A 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 4 0 3 A があってもよい。

30

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 4 0 3 A 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、O T P トークンの保有者や O T P 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 4 0 3 5 A における端末 5 A 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 U R I は平文データ 4 0 3 5 A に H T M L 言語などで記述され埋め込まれた U R I (リンクタグ) であったりするため 4 0 3 5 A の U R I (および U R I 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。

40

平文データ 4 0 3 5 A における端末 5 A 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。

【 0 2 7 4 】

< 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 5 A ではソフトウェア 4 0 3 A 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 5 1 4 A と顧客情報を記録する 5 0 4 A を備える。不正アクセス監視機能 (図 5 A の 5 1 1 A、5 1 2 A、5 1 3 A) にて不正アクセスが検知された場合 5 0 4 A に記録された連絡先を用いて不正アクセス通知部 5 1 3 A が連絡先に不正アクセス

50

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。

10

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。

20

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。鋸刃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。

30

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。

40

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

50

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 F P G A 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 F P G A に設計図データを F P G A などに展開してもよい。

F P G A の例を用いて具体例に説明したが C P U や S o C や M P U 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 B I O S 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 C P U や S o C 、 M P U 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。

【 0 2 7 9 】

< 4 T . 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 4 0 3 4 A をネットワーク 2 0 を通じてユーザー端末 4 A に届けるサーバ端末 5 B は双方向通信が可能な機器であるが、端末 5 B の代わりに 1 対複数の放送が行える放送局端末 5 C（図 5 C の 5 C、S V C R H N b r o a d c a s t e r）を利用できる。前記放送局 5 C は 1 対複数の放送による通信経路 N T B（通信ネットワーク 2 1、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 4 2 3 A を持つユーザー端末 4 A に対し、単一の暗号鍵 T T K Y 4 0 3 3 A で A E S 暗号化などの共通鍵暗号化を施した暗号化データ 4 0 3 4 A を放送する。前記放送局 5 C 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。

【 0 2 8 0 】

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

放送局 5 C は 3 A と同じ機能を持ちうる。放送局 5 C は放送局 5 C を制御する端末 5 C と通信経路 2（通信網 2）を介して接続される。そして端末 5 C が端末 3 A 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 5 C を制御する制御端末 5 C を介してネットワーク 2 0 と接続され、端末 5 C と端末 3 A をネットワーク 2 0 と通信経路 3 で接続できるとき端末 5 C は端末 3 A 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 5 C は端末 3 A のブロックチェーン部にあるブロック番号 B n 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 5 C の時計による時刻情報を放送することができる。端末 5 C は地上局でも人工衛星の放送局でもよい。

【 0 2 8 1 】

< 端末 5 C 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 B n T O T P を測位情報と共に放送できるとき>

端末 5 C 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（G N S S）用の測位用人工衛星である場合も考えられる。端末 5 C 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 3 A と接続される。

そして端末 3 A および端末 5 C 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 B n に基づいた OTP である B n T O T P を算出し端

10

20

30

40

50

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。

10

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。

20

【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。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かもしれない。

30

【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、ユーザー識別子には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。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るてもよいし、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。

40

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、 $BnTOTP = fh$ （ユーザー識別子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。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

50

指示するトランザクションを送信し、端末 3 A と接続された端末 5 C のブロックチェーンのコントラクトの K C 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 5 C 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 3 A 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 GNS 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。GNS 専用 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 GNS 放送局 5 C、具体的には 4 基の測位用衛星端末 5 C 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 5 C は既知の GNS 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 4 A の GNS 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 GNS 衛星 5 C が 180 秒以内に一回から数回送るなどしてもよい。

GNS のメッセージデータの長さが足りない場合には、GNS 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】

GNS 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 5 C (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 5 CC (コントロールセグメント) と GPS 受信機端末 4 A (ユーザーセグメント) が存在し、また端末 5 C や端末 5 CC と端末 4 A 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 3 A や端末 3 B 等と接続させ端末 5 C 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 5 C の原子時計を頼りにして Bn がすべての GNS 衛星端末 5 C 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 5 CC と衛星端末 5 C 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 GNS 衛星局 5 C と共有しブロックチェーン部を同期させる。

10

20

30

40

50

このとき端末 4 A は端末 5 C から受信した放送に含まれる B_nTOTP をブロックチェーンのノード端末 3 A の認証関数 3018 A を用いて認証し、正しい B_nTOTP が記録された 4 つの GPS 衛星の放送データを用いて端末 4 A 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 1500 bit を 30 秒、認証用データは 1 つの変数が 256 bit で 5 つある場合は 1280 bit なので 30 秒以内、両者を連結して順に放送する場合は 2780 bit を 60 秒にわたり放送する。ブロック番号 B_n 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 B_nTOTP 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 4 A が検出し、 B_nTOTP 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 5 C 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。

10

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 B_n 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 1280 bit 30 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 5 C と端末 4 A がネットワーク 20 から切断されている場合は、端末 5 C 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 3009 A を基に、ブロック番号 B_n と B_nTOTP を算出し、 B_n と B_nTOTP とメッセージデータとそれらの MAC 値を添付して端末 4 A 等ユーザーセグメント端末に放送する。

20

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

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

30

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

【0291】

ユーザー端末 4 A は複数（4 つ以上）の衛星端末 5 C が放送する測位用信号を端末 4 A の 42 A の 423 A もしくは 422 A 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 5 C の放送する B_nTOTP の OTP 認証処理に移行する。

40

【0292】

端末 5 C の放送する B_nTOTP の OTP 認証処理では、端末 4 A が受信している人工衛星端末 5 C の送付する測位用情報に添付されたブロック番号 B_n と B_nTOTP （または B_nTOTP 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 3018 A を用いて認証させ、認証関数の戻り値から端末 5 C の放送したデータの真偽・真贋を判断する。

【0293】

50

端末4 Aにおいて端末5 C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3 Aの端末5 Cの管理者が設定した認証関数3018 AにB n T O T P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B n、B n T O T Pを引数として渡して3018 Aを実行させ、その戻り値がO T Pが正しい時の戻り値であったとき(B n T O T Pが真の値であったとき)、放送局5 Cの放送が正しいことが期待されることを端末4 Aに記録し、ユーザーに通知・表示させる。

3018 Aの戻り値が正しくない戻り値であったとき(B n T O T Pが偽りの値であったとき)その放送局5 Cに関連する測位情報はO T P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5 Cの放送したデータ情報がO T P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G N S S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5 Cとは異なる新規のG N S S放送用衛星5 Cの信号を受信するよう待機し、新規の端末5 Cから受信した信号を認証し、認証された端末5 C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5 C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4 Aは4つ以上の端末5 Cから4 Aの本発明のO T P認証により認証された位置情報と時刻情報と4つの5 Cの放送するブロック番号B nおよびB n T O T Pに平文データに記録し、秘密鍵401 A等を用いて改ざん検知用の電子署名やH M A Cを平文データに行い、電子署名またはM A C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4 Aは4つ以上の端末5 Cから4 Aの本発明のO T P認証により認証された位置情報と時刻情報と4つの5 Cの放送するブロック番号B nおよびB n T O T P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401 A等を用いて改ざん検知用の電子署名やH M A Cを平文データに行い、電子署名またはM A C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4035 A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M A C値付きの改ざん検知可能な平文データ4035 Aとして作成できてもよく、前記4035 Aを秘密鍵401 Aに割り当てられたO T Pトークンによってソフトウェア403 Aを用いて暗号化する事が出来てもよい。

平文データ4035 A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4035 A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O T P認証システムにより簡易に証明する。

前記の4035 Aに記入するブロック番号B nはB n pであって、B n pはB n T O T Pを取得したときのB n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。

O T P認証コントラクトのO T P認証関数3018 Aや認証を検証する端末3 Dの認証関数3018 D Aには $B n T O T P = f h(A, T I D A, K C, B n p)$ の形で認証するための認証関数を備え、4035 Aにはユーザー識別子Aとトークン番号T I D Aが記入されていてもよい。

10

20

30

40

50

出版された 4 0 3 5 A の暗号化データ 4 0 3 4 A は流通し、それを復号するトークン番号 T I D B の O T P トークンと A K T B とソフトウェア 4 0 3 A を持つ顧客ユーザー U B がいる場合には平文データ 4 0 3 5 A が閲覧などされる。そして顧客ユーザーは平文データ 4 0 3 5 A に記録された B n p と B n T O T P とトークン番号 T I D A 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、O T P 認証関数にて $B n T O T P = f h (A , T I D A , K C , B n p)$ の形で計算を行えるよう A と T I D A と B n p 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 G N S S などを用いた正確な緯度経度を記したもので

10

【 0 2 9 6 】

< 放送局 5 C からのデータファイルの放送 >

放送局 5 C 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、音声を送信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 5 C であってもよい。

【 0 2 9 7 】

ここで文章、音声、動画ファイルの配信に放送局 5 C を用いる狙いは、O T P 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 4 0 3 4 A 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 2 0 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。

20

ただし災害など緊急時は、公共性のある放送局 5 C はソフトウェア 4 0 3 A 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 4 0 3 5 A 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 2 0 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 2 0 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。

30

【 0 2 9 8 】

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 5 C 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 5 C、送信所 5 C などの形で設置されている。ユーザー端末 4 A は最寄りの無線局 5 C の暗号データ放送を閲覧する O T P 生成トークンを取得する。

40

【 0 2 9 9 】

放送局 5 C は放送局 5 C に固有の共通鍵 T T K Y 4 0 3 3 A でラジオやテレビジョン番組のデータを暗号化し 4 0 3 4 A として、電波が届く最寄りのユーザー端末 4 A に放送局 5 C が暗号データ 4 0 3 4 A を送信する。そして放送された暗号化データ 4 0 3 4 A を復号し閲覧するソフトウェア 4 0 3 A にて、サーバー端末 3 A と端末 4 A をネットワーク 2 0 を介して接続させ B n T O T P の生成・認証を行い認証関数の戻り値 C T A U 4 0 3 1 A を得る。

ここで B n T O T P でなく O W P を取得できる O T P トークンを用いてソフトウェア 4 0 3 A にて O W P の生成と認証を行い戻り値 C T A U 4 0 3 1 A を得てもよい。 4 0 3 1

50

Aと必要に応じて4032Aと403A内部の鍵情報40302Aを用いてTTY4033Aを生成し、TTY4033A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。

10

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BnTOP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TTY4033A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。

20

【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TTY4033Aが変更される。OTPトークンは契約ができていないユーザー識別子(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。

30

【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BnTOP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OTP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によりブロック番号BnとCTAU4031AからTTY4033A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。

40

【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

50

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 C R H N 4 0 3 A 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。

【 0 3 0 5 】

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 5 C からの無線による信号が端末 4 A 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。

【 0 3 0 6 】

先の例ではアマチュア局一つの暗号化放送データ 4 0 3 4 A に対し T T K Y 4 0 3 3 A 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 4 0 3 5 A 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 O W P が割り当てられ T T K Y 4 0 3 3 A 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 O T P トークン、O W P、T T K Y 4 0 3 3 A 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 T T K Y 4 0 3 3 A を用い暗号化する場合は T T K Y 4 0 3 3 A 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 O T P トークン、ソフトウェア 4 0 3 の版、O W P ・ B n T O T P、T T K Y 4 0 3 3 A を使い分けることが好ましいかもしれない。）

【 0 3 0 7 】

< 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 4 0 3 A 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 2 0 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 3 C（サーバ端末 S V L o g i n）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。

【 0 3 0 8 】

ソフトウェア 4 0 3 A や端末 3 C 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 2 7 6 0 7 9 9 がある。また A E S 方式も利用されうる。端末 5 C 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。

【 0 3 0 9 】

< 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 O T P 認証用コードを T L S による暗号化通信（T L S ・ S S L による暗号化

10

20

30

40

50

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。

10

【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。

20

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。

30

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。

40

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CRYPTWEBPAGE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

50

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。

10

20

30

40

50

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。

10

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。

20

【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。

30

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。

40

（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

50

ザーの識別子にトークンを発行する。

またコントラクト 3 0 0 8 A や 3 0 0 8 A G や 3 0 0 8 A A や 3 0 0 8 D A の O T P 生成関数 3 0 0 9 A や O T P 認証関数 3 0 1 8 A や 3 0 1 8 D A の O T P 計算に用いるシークレットキー情報 K 値の K C 値 3 0 1 1 A や B C 値 3 0 1 3 A を関数 3 0 1 2 A や 3 0 1 2 D A 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 (K N B N) となる変数 3 0 2 4 A を変更できる。

注意すべきこととして本発明のワнта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 1 A がサーバ端末 3 C にアクセスするサービスやソフトウェア 4 0 3 A を用いる暗号化データの復号用途では、端末 1 A は 4 0 3 A のプログラムに従いネットワーク 2 0 を介してブロックチェーンのノード端末 3 A にアクセスし O T P (O W P 、 B n T O T P) を取得できる。

10

管理者端末 1 C のアクセスを端末 3 A が受け付け、K C 値 3 0 1 1 A の変更のトランザクションを端末 3 A は受信しブロックチェーンに連結することで K C 値の変更が行え、端末 3 A にアクセスする端末 1 A は端末 1 C が書き換えた K C 値を反映した O T P による認証ができる。一方で端末 3 D を用いるサービスでは K 値は K C 値 3 0 1 1 D A や B C 値 3 0 1 3 D A を書き換え更新する手段をコントラクト管理者 U C は提供する。

【 0 3 2 2 】

例としてユーザー U A が秘密鍵 1 0 1 A を用いてアクセスする O T P 生成関数と O T P 認証関数について、O T P 生成関数と O T P 認証関数が利用するワнтаイムパスワードのシード値 T I D A 、K C 、B n 、A の場合には K C 値 3 0 1 1 A を、O T P 生成関数と O T P 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нтаイムパスワード認証が行えなくなる。

20

【 0 3 2 3 】

K C 値 3 0 1 1 A 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 K C 値 3 0 1 1 A はコントラクトの管理者のみが変更することもできる。K C 値 3 0 1 1 A の取り扱いにはコントラクトの管理者による。K C 値 3 0 1 1 A 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 O W P の算出などで用いる B C 値 3 0 1 3 A と同じ役割を持つ変数とみなせる。

30

【 0 3 2 4 】

K C 値 3 0 1 1 A は本発明を用いるほかのスマートコントラクトと O T P トークンの O T P の値と衝突しにくくするために、例えば O T P 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 I S B N 等に基づいて計算される K C 値 3 0 1 1 A を使うことが好ましい。

K C 値が似通ったもの、例えば 2 5 6 b i t (符号なし整数値では 2 の 2 5 6 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 K C 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 2 5 5 (2 の 8 乗まで) 、さらには 0 から 1 0 までといった小さい整数の範囲で K C 値を記録するなどの運用を複数の O T P トークンのコントラクトで行われてしまうと O T P 値が衝突する恐れがある。

40

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 9 8 7 6 の O T P 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 O T P トークンの番号 9 8 7 6 であった時、両サービスの O T P トークンのコントラクトの K C 値が 1 2 3 などと設定されハッシュ関数も S H A - 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、O T P は $B n T O T P = f h$ (共通の A , $T I D A = 9 8 7 6$, $K C = 1 2 3$, 共通の B n) として計算され、結果として二つの異なるサービス用の O T P トークン間で一致した O T P が算出されてしまう。

これはウェブサイトログイン用の B n T O T P のみならず施錠用の O W P でも同様のこ

50

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。

10

【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。

20

【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。

30

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SHA256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。

40

【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。

50

$$\begin{aligned} \text{TOTP} &= \text{HOTP}(K, T) \\ &= \text{Truncate}(\text{HMAC-SHA-1}(K, T)) \end{aligned}$$

ここで Truncate は端数処理である。本発明では RFC 6238 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-SHA384、HMAC-SHA512）、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なし、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 RFC 6238 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 B_n 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 $B_n \text{TOTP}$ の算出式は以下ようになる。また n 桁の整数のパスワード $B_n \text{TOTP} - N$ も次に示す。

$$\begin{aligned} B_n \text{TOTP} &= fh(K, T) \\ &= fh(KC, TIDA, A, B_n) \quad \text{具体例。} \\ B_n \text{TOTP} - N &= \text{Truncate}(fh(K, T)) \\ &= \text{Uint}(fh(KC, TIDA, A, B_n)) \bmod 10^n \quad \text{具体例、} B_n \text{TOTP} \text{ を符号無し整数化して } 10 \text{ の } n \text{ 乗で割り算しその余りをパスワードとする場合。} \end{aligned}$$

ここで $\text{Uint}(X)$ は引数 X を符号なし整数に型変換する関数。

【0331】

< $B_n \text{TOTP}$ 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 T_m 値として、本発明のブロック番号 B_n を T_m として用いるワンタイムパスワード $B_n \text{TOTP}$ の算出式の一つの例は次のようになる。 T_m は TB と同じである。

$$\begin{aligned} B_n \text{TOTP} &= fh(K, T_m) \\ &= fh(KC, TIDA, A, B_n) \quad \text{例} \end{aligned}$$

一方、 T_m 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。

$$\begin{aligned} \text{OWP} &= fh(K, T_m) \\ &= fh(KC, TIDA, A, BC) \quad \text{例} \end{aligned}$$

【0332】

n 桁の整数のパスワード $\text{OWP} - N$ と $B_n \text{TOTP} - N$ を次に示す。

$$\begin{aligned} B_n \text{TOTP} - N &= \text{Uint}(fh(KC, TIDA, A, B_n)) \bmod 10^n \\ \text{OWP} - N &= \text{Uint}(fh(KC, TIDA, A, BC)) \bmod 10^n \end{aligned}$$

10ⁿ

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。

10

$$\text{OTPr} = m - qn$$

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。

20

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。

30

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OTP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】

40

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

50

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。

G N S S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るOWP型のパスワードを表示させ入場用のチケットや施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B n T O T P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 $O(\log(n))$ 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 $O(\log(n))$ 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のに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。

10

20

30

40

50

【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。

10

【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することも好ましい。

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。

20

【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OTPT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。

30

【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OTPTトークンの資産残高やOTPTトークンのURIなどOTPT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ー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OTPT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OTPTトークンの資産残高やOTPTトークンのURIなどOTPT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OTPTトークンの残高・残数データをユーザーUAらの端末に発行できることが好ましい。

40

【0345】

サービス提供者の意志に応じてOTPT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OTPTトークンとは異なるコントラクト識別子にOTPTトークンのコントラクトを新規にデプロイし、元のOTPT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

50

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。

10

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。

20

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。

30

【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においてユーザー端末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。

40

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。

50

参考として図 9 A は分散型台帳システム D L S 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 3 0 0 A を用いるときの O T P トークンによる認証システムの概要を説明しており、図 9 B は分散型台帳システム D L S に有向非巡回グラフ型 (D A G 型) のデータ構造を用いた分散型台帳記録部 3 0 0 A を用いるときの O T P 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 7 A では端末 1 C は S 1 1 0 から S 1 1 3 にかけて端末 3 A の D L S 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。S 1 1 4 と S 1 1 5 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 3 C やソフトウェア 4 0 3 A による暗号データの復号の用途等で、ネットワーク 2 0 と切断される恐れがある端末 3 D もネットワーク 2 0 に接続できるときは図 7 A 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 1 C が O T P トークンをユーザー識別子 A にトークン番号 T I D A としてトークンを発行し、また 1 C またはサービスはユーザー端末 1 A 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。

10

S 1 1 6 ではユーザー端末 1 A がサービスにアクセスし、図 6 X 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 1 A に O T P 認証を求め端末 1 A は端末 3 A にアクセスし S 1 1 7 から S 1 1 9 のシークエンスで O T P 生成関数 3 0 0 9 A から O T P を取得する。O T P はハッシュ関数に S H A 2 5 6 を用いたときは 3 2 バイト (符号なし整数にして 2 の 2 5 6 乗 - 1) のデータとして計算され出力される。

(3 0 0 9 A と 3 0 1 8 A に S H A 2 5 6 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 O T P としてもよい。例として 3 2 バイトのデータを符号なし整数に型変換しその 1 0 の N 乗の剰余 O T P r を N 桁の符号なし整数の O T P 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 O T P 生成関数 3 0 0 9 A と O T P 認証関数 3 0 1 8 A や端末 3 D に搭載する 3 0 1 8 D A も対となる O T P 生成関数と同じように O T P の計算を行い剰余によるパスワード O T P r を計算できなければ認証できない。)

20

そして S 1 2 0 ではサービスが接続中の 1 A 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。S 1 2 0 では O T P 認証を端末 1 A に要求しする。端末 1 A は S 1 2 1 から S 1 2 3 にかけて S 1 1 7 から S 1 1 9 で取得した値とユーザー識別子と O T P トークンのトークン番号を O T P 認証関数 3 0 1 8 A に入力し認証関数 3 0 1 8 A を実行させ S 1 2 3 にて認証結果 3 0 1 8 A 等の戻り値 C T A U を端末 3 A から得てサービスに認証関数の戻り値 C T A U を入力・出力する。端末 1 A の出力した認証関数の戻り値 C T A U が O T P 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。

30

S 1 2 5 ではログイン後も端末 1 A 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 O T P トークン番号 T I D A とユーザー識別子 A に対し異なる I P アドレスや位置情報や端末の I D 値そして端末のセンサ値が図 6 X 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 6 X 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。

40

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 O T P 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 6 X 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 6 X のデータ収集と監視を行わない。図 6 X 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。

50

【 0 3 4 8 】

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

コントラクト内部のシークレット変数 K C 、ブロック番号 B n 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 B C 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 G a s L i m i t 値を V として、

$f_h(A, T I D A, K C, B n, B C, V)$ を計算させ O T P 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 O T P 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 K C と B C のうち B C 値を更新できる O T P 認証システムを構築した。

10

【 0 3 4 9 】

実施例 1 では図 8 A のサーバ端末 3 A のブロックチェーン上のコントラクト 3 0 0 8 A と 3 0 0 8 A G と 3 0 0 8 A A は、コントラクト内部の変数 K C (図 3 A C の 3 0 1 1 A) または B C (図 3 A C の 3 0 1 3 A) と内部変数 K C または B C またはその両方を書き換えて更新できるセッター関数 f_{scb} (図 3 A C の 3 0 1 2 A) を備えている。

前記セッター関数 f_{scb} (図 3 A C の 3 0 1 2 A) はコントラクト管理者の端末 1 C が備える秘密鍵 P R V C (図 2 C の 1 0 1 C) 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 K C (図 3 A C の 3 0 1 1 A) または B C (図 3 A C の 3 0 1 3 A) と内部変数 K C または B C またはその両方を書き換えて更新できるよう関数 $f_{scb}(3012A)$ はプログラムされる。

20

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。

3 0 0 8 A は同一のコントラクトに内部変数 K C 値や B C 値が記録されているが、3 0 0 8 A G と 3 0 0 8 A A の二つのコントラクトを用いる場合には O T P の計算に用いる変数 K C (3 0 1 1 A) 、変数 B C (3 0 1 3 A) を関数 $f_{scb}(3012A)$ で書換更新し 3 0 0 8 A G と 3 0 0 8 A A の K C 値及び B C 値を一致させ同期させ、同期した状態を保つ必要がある。K C や B C の変数の個数やデータ型等は限定しないが、設定した K C や B C 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 K C や B C のほかに O T P 認証の待受け時間を変える関数及び変数 3 0 3 0 A や O T P r を求めるための O T P r 桁数変更用関数及び変数 3 0 3 1 A も 3 0 0 8 A G と 3 0 0 8 A A 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 O T P を計算するために必要なハッシュ関数 f_h の関数の種類を一致させなければならない。

30

ここで端末 3 C では 3 0 0 8 A G と 3 0 0 8 A A を用いるが、端末 3 D では 3 0 0 8 A または 3 0 0 8 A G と端末 3 D の認証関数 3 0 1 8 D A を用いるので端末 3 D に K C 値や B C 値や 3 0 3 0 A や 3 0 3 1 A を設定する場合には 3 0 0 8 A または 3 0 0 8 A G の変数・関数の記憶部と端末 3 D 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。

【 0 3 5 0 】

40

またコントラクトの管理者はその端末 1 C からコントラクトに O T P 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 K N B N (3 0 2 4 A) 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 3 0 2 4 A 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 (K N B N の書換は端末 1 C の秘密鍵 P R V C (1 0 1 C) を用いて行われる) 。

【 0 3 5 1 】

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 1 C の秘密鍵 P R V C (秘密鍵 1 0 1 C) 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 1 0

50

1 C 情報を入手し、その情報を複製し、端末からコントラクト 3 0 0 8 A 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 O T P 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 3 0 2 4 A や内部変数 3 0 1 1 A および 3 0 1 3 A 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に、コントラクト内部にあるトークン発行関数（図 3 0 4 3 A）や関数 f s c b（3 0 1 2 A）や 3 0 2 4 A 等に含まれるセッター関数を実行する際に秘密鍵 1 0 1 C 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 3 0 4 2 A を備えることができる。

【0352】

10

<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 3 0 4 2 A について説明する。

O T P 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 P R V C 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ー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 O T P 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。

20

3 0 4 2 A 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 3 0 4 2 A はトークン発行関数 3 0 4 3 A や関数 3 0 1 2 A 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>

30

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 P R V C と P R V C が漏洩した際に O T P トークンの発行等を停止するための秘密鍵 P R V B を用意し、P R V C 2 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 O T P トークンの発行関数やコントラクト内部変数（図 3 A C における 3 0 4 3 A や 3 0 2 4 A、3 0 3 0 A、3 0 3 1 A、3 0 1 1 A、3 0 1 3 A）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】

40

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 3 0 1 9 A 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 O T P 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 O T P を流通させ O T P 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。

50

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

10

20

30

40

50

る。

【0357】

シーケンス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】

シーケンス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付けられた値(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OTPの生成と認証を行う。)

【0359】

シーケンス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】

シーケンス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クサービス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随して発行される。

【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

10

20

30

40

50

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】

シーケンス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DL5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。

10

3Cはシーケンス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用途によってはPINや生体認証でもよい。)

20

【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。

30

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。

40

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OTP

50

C T (図 3 A C の 3 0 1 7 A) または O T P C T G (図 3 A B の 3 0 1 7 A G) 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 O T P 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 3 0 1 7 A または 3 0 1 7 A G の変数変化をサーバ端末 3 C の 3 1 1 4 C が検出し、不正利用があったことを通知する O T P 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 3 0 1 6 C 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。

O T P 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 O T P を生成する際に 3 0 1 7 A や 3 0 1 7 A G の数値の増加減少などの変化が発生し、サーバ端末 3 C はそれを検出してユーザーに通知できるほか、3 0 1 7 A や 3 0 1 7 A G 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 O T P 認証を行うための O T P を生成する段階で改ざん困難なブロックチェーン上に O T P 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。

【 0 3 6 5 】

ここで S 2 1 6 及び S 2 1 7 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 O T P 生成関数 3 0 0 9 A と認証関数 3 0 1 8 A をユーザー端末 1 A に実行させる。この時、端末 1 A 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 1 A に発行されたトークン番号 T I D A の情報が必要である。

端末 1 A からサーバ端末 3 C へアクセスするために用いたトークン番号と、ユーザー識別子と、端末 1 A の I P アドレスや位置情報やセンサ情報などの I P V 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 3 C の記憶部 3 0 C のアクセス検出及び監視用データベース 3 0 1 1 C に図 6 X 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 O T P を表示させるソフトウェアを端末 1 A の記憶装置 1 0 A の 1 0 2 A 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 T I D A 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。)

【 0 3 6 6 】

シーケンス S 2 1 9 においてサーバ 3 C は端末 1 A に対し、O T P トークンのトークン番号とユーザー識別子と O T P の入力を求め、その際にサーバ 3 C にログインに用いたトークン番号、ユーザー識別子、I P アドレスや位置情報やセンサ情報などの I P V 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 3 C から端末 1 A へ O T P 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 1 A 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 O T P を認証する際にユーザーのユーザー識別子やトークン番号等の入力値と、ユーザー端末の I P アドレスや位置情報や端末のセンサ値などを含む I P V 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 6 X 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 3 C へアクセスする場合は、図 6 X に記載の異なる I P V 値は記録されないはずである。

【 0 3 6 7 】

シーケンス S 2 2 0 及び S 2 2 1 では S 2 1 9 で配信されたウェブページの E C M A S c r i p t 等プログラムに応じて、ユーザー識別子 A とトークン番号 T I D A とユーザー端末 1 A に記録された秘密鍵 1 0 1 A を用いてブロックチェーンのノードの一つである 3 A にアクセスし、3 A にデプロイされた O T P 生成コントラクト 3 0 0 8 A または 3 0 0 8 A A の O T P 認証関数 (図 3 A C の 3 0 1 8 A) を実行する。

O T P 認証関数 3 0 1 8 A はユーザー識別子 A、トークン番号 T I D A、O T P を引数と

10

20

30

40

50

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 1 A に戻り値 $CTAU$ (図 3 AB の 3021 A) 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 6 C 又は図 6 D 又は図 6 E 又は図 6 F 又は図 6 G 又は図 6 H のフローチャート説明図に従って認証関数 3018 A は動作する)。

図 6 C または図 6 D に示すように OTP 認証関数 3018 A を実行した際に、3018 A の処理内部にその実行回数を記録する変数 $OTPC T$ (図 3 AC の 3017 A) または $OTPC T A$ (図 3 AB の 3017 AA) 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 3017 A または 3017 AA の変数の変化をサーバ端末 3 C の 3114 C 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)をユーザ識別子に対し送信することや、顧客情報データベース 3016 C に記載のユーザ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端末と不正に秘密鍵を入手したユーザ端末の区別を問わず、 OTP を生成する際に 3017 A や 3017 AG の数値の増加減少などの変化が発生し、サーバ端末 3 C はそれを検出してユーザに通知できるほか、3017 A や 3017 AG 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 認証回数が増加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】

シーケンス $S222$ では 3021 A 、3022 A 、3023 A 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。3022 A や 3023 A 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。3022 A 、3023 A 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 3 C 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 3022 A や 3023 A は利用されないことも考えられる。

【0369】

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

【0370】

シーケンス $S224$ では端末 1 A 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を行い

10

20

30

40

50

、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ケンスでもよい。

【0371】

シーケンス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。

10

シーケンス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。シーケンスS227はシーケンス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。

20

【実施例2】

30

【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。)

40

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OWP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わることがある。

【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

50

コントラクト管理者端末 1 C (図 2 C の 1 C) 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 O T P 認証システムによる認証を行うことの出来る端末 3 D (図 3 D の端末 3 D) とチケットなど有価紙葉を O T P トークンとしてを発券するサーバ端末 3 E がネットワーク 2 0 を通じて接続されている。

【 0 3 7 5 】

端末 3 D 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 3 D の記憶装置 3 0 D のブロックチェーン記録部 3 0 0 D または 3 0 1 0 A には、端末 3 A の O T P 生成コントラクトが生成する O W P 型 O T P を認証できる認証関数 3 0 1 8 A、3 0 1 8 D A が記録されていてもよい。認証関数 3 0 1 8 A、3 0 1 8 D A に用いる K C 値 3 0 1 1 A や B C 値 3 0 1 3 A や 3 0 3 0 A や 3 0 3 1 A といった O T P 計算に必要な変数情報を端末 3 D に記録していてもよい。

10

端末 3 D はネットワーク 2 0 には接続されていないがサーバ端末 3 A の O T P 生成トークンに関するコントラクト 3 0 0 8 A または 3 0 0 8 A G にて生成された O T P (O W P 型 O T P、O W P) を認証できる認証関数を 3 D の記憶部 3 0 D の 3 0 0 D や 3 0 1 0 D に備え、ブロックチェーン部を持つ 3 A とネットワーク 2 0 を通じて接続されていないオフライン状態であっても O W P などの認証情報を記録した紙のチケット等有価紙葉や N F C 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 2 0 等から端末 3 D 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。

20

そこで本発明では O T P トークンの発行・流通・O W P 型 O T P の生成はオンラインにおいて端末 1 A と端末 3 A と端末 3 E と端末 1 C がネットワーク 2 0 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 1 A と端末 3 A 間で O W P 型の生成を行い、生成された O W P と O W P 生成に用いたトークン番号とユーザ識別子を端末 1 A のプリンタ 1 5 2 A にて紙に印刷・印字し印刷物 1 8 A (図 2 A または図 8 B の 1 8 A) を製造し端末 3 D のカメラ 3 4 0 D に 1 8 A や 1 5 0 0 A 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 1 2 A と N F C タグ 1 9 A (図 2 A または図 8 B の 1 9 A) を通信させ N F C タグ 1 9 A に O W P と O W P 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 N F C タグ 1 9 A を電子的な入場券や解錠を行う鍵として端末 3 D と通信させ認証を行い入場または解錠などを行う。

30

ここでタグ 1 9 A は主に非接触式の N F C タグを想定するが接触式の I C タグや I C カード、通信端子を備えた外部記録端末 1 9 A でもよく、磁気ストライプを用いた 1 9 A でもよく、1 9 A は非接触式または接触式の通信を端末 3 D と行うことができる。

なお端末 3 D がネットワークに接続されている場合は、3 D に記録された認証関数 3 0 1 8 D A に限らず、端末 3 A に存在するブロックチェーン部の認証関数 3 0 1 8 A にアクセスし紙のチケットや N F C タグに記録された O W P を含む認証情報を持ちいて認証を行い、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。

40

【 0 3 7 6 】

< 紙のチケット等有価紙葉 1 8 A または N F C タグ 1 9 A の製造と利用 >

オフライン状態にある端末 3 D のカメラ 3 4 0 D にて紙の有価紙葉 1 8 A の印刷面の O W P と O W P 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、あるいは 3 D の N F C 通信装置 3 4 1 D にて N F C タグ 1 9 A 内部に記録された O W P と O W P 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、3 D の記録部 3 0 D の 3 0 0 D や 3 0 1 0 D に記録された認証関数 3 0 1 8 D A または 3 0 1 8 A と同様の処理 (図 6 F のフローチャートも参照) に従って紙や N F C タグの O W P 型 O T P を A r g O T P として、V e r i O T P と A r g O T P 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 3 5 0 A 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

50

装置であれば始動を行う。同時に 3 5 1 D と 3 5 2 D 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 3 D のカメラ 3 4 0 D に対し紙の情報 1 8 A の代わりに端末 1 A のディスプレイ 1 5 0 A の O W P 等認証情報表示画面 1 5 0 0 A を提示し読み取ることで認証してもよい。

【 0 3 7 7 】

< プリンタによる 1 8 A の製造 >

紙のチケット等の有価紙葉 1 8 A 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
10 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3 D プリンタなども利用できてよい。ここでプリンタは認証先となる端末 3 D のカメラやスキャナ 3 4 0 D 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・パターン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 O W P 等の認証情報を印刷・パターンニング・捺染・転写し有価紙葉 1 8 A 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
20 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 1 A 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 1 8 A 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
30 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 C V S などでも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 A T M や C V S 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 O W P 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。

【 0 3 7 8 】

< N F C タグ 1 9 A の製造 >

N F C タグ 1 9 A を用いる場合は端末 1 A の通信装置 1 2 A と 1 9 A が通信できれば良い。N F C タグでもよいし N F C カードでもよい。1 9 A は N F C 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。N F C タグ 1 9 A 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
40 端末といった製品に組み込まれた N F C タグ 1 9 A もしくは N F C タグ 1 9 A の機能付きのウェ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 N F C タグを内蔵してもよい。N F C タグ 1 9 A 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。

10

20

30

40

50

また端末 1 A が N F C 機能をもち端末 1 A そのものが持ち運びの出来る N F C タグ 1 9 A となっていてよい。その場合、端末 1 A の通信装置 1 2 A (端末の電子回路を含む) にて N F C タグ部分 1 9 A と制御装置 1 1 A や記憶装置 1 0 A が有線方式で接続される。タグ 1 9 A 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。1 9 A に備えられた接点又は端子を用いて端末 3 D に認証情報を読み込ませ 3 D 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。

I C を用いる 1 9 A も 1 6 A も端末 1 A 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。

10

【 0 3 7 9 】

実施例 2 における O T P の生成関数のフローチャートは図 6 A と図 6 B に記載し、O T P の認証フローチャートは図 6 D と図 6 F に記載する。図 6 D 及び図 6 F では引数となるユーザー識別子 A とトークン番号 T I D A と O W P が紙に印刷された情報または N F C 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 3 0 1 8 A (もしくは 3 0 1 8 D A) は入力された引数の情報に従い、認証関数 3 0 1 8 A の属するコントラクト 3 0 0 8 A A の内部シークレット変数 K C や B C と、引数として入力されたユーザー識別子 A とトークン番号 T I D A と O W P (O W P = A r g O T P として) から、検証用 O T P 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 3 D に記録された認証関数 3 0 1 8 D A を用いることもできる。

20

【 0 3 8 0 】

図 7 E は図 8 B に記載の装置と O T P 認証システムを用いて端末 3 D に対し認証を行う際のシーケンスの説明図である。図 7 E 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 7 E は図 7 B と類似する。

30

図 7 B はパスワード O W P を用いた O T P トークンの一般的な発行時のシーケンス図であり S 1 3 0 から S 1 3 5 までの一連の流れで O T P 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 D L S) のノード端末 3 A のに K C 値を k_1 、B C 値を c_1 として O T P 生成関数を含む O T P トークンのコントラクト (生成コントラクト、O T P 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 O W P による認証をできるように準備した後にユーザー端末 1 A の秘密鍵 1 0 1 A のユーザー識別子 A にトークン番号 T I D A 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 3 D や 3 C に O T P 認証関数 3 0 1 8 D A や 3 0 1 9 A A や 3 0 1 8 A に K C 値を k_1 、B C 値を c_1 として O T P 認証関数を設定しなければならない。この時点では端末 1 A のユーザーは $OWP = fh(A, TIDA, k_1, c_1)$ のパスワード O W P を生成して取得し認証に用いることができる。

40

S 1 4 4 においてある時間が経過した後、S 1 4 5 にて O T P トークンの O T P 生成関数を含むコントラクトと認証関数 3 0 1 8 D A の K C 値を k_2 、B C 値を c_2 へ書き換えることでユーザーの O T P トークンの生成する O T P を変えることができる。

端末 1 A 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 O W P 生成ソフトウェアまたは専用のウェブサイトを用い、S 1 3 7 から S 1 3 9 までの一連の流れで端末 3 A のブロックチェーン部の O W P 型の O T P トークンのコントラクトから O T P 生成関数を呼び出して O W P 型の O T P を取得する。その際の O W P は $OWP = fh(A, TIDA, k_2, c_2)$ で計算される。

端末 3 C や端末 3 D がネットワーク 2 0 を介して 3 A と接続されているとき S 1 4 1 から

50

S 1 4 3 にて O T P 認証関数 3 0 1 8 A を呼び出し、もしくは S 1 4 1 から S 1 4 3 と同様の工程を 3 A ではなく 3 D の O T P 認証関数 3 0 1 8 D A を呼び出し行って認証結果の戻り値 C T A U を得て、前記認証の戻り値 C T A U が認証ができたときの値（データ）の時に S 1 4 4 にて端末 3 D 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 3 5 0 D 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。

O W P 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 S 1 3 6 や S 1 4 0 のプロセスにて図 6 X 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、O W P を用いた N F C タグ 1 9 A 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 3 C（およびネットワークに接続できる 3 D）や 3 E や 3 F や 5 A で情報流出する事により顧客が購入した端末 3 D の設備やその所有者を危険にさらす恐れがあるときは S 1 3 6 や S 1 4 0 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。

10

S 1 4 6 では S 1 4 4 と同じくある任意の時間経過したのち S 1 4 5 と同様に、端末 1 C が O T P 生成側の 3 A と O T P 認証及びサービス側の 3 D や 3 C にて K C 値と B C 値を更新し一致させ O T P 計算ができるように設定することができる。K C 値を k 3、B C 値を c 3 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 K C 値 B C 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 N F C タグ 1 9 A で実現する場合には車検ごとに自動車の鍵となる O W P を書き換え偽造された N F C タグ 1 9 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 1 8 A 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。

20

【0381】

実施例 2 の O W P は $O W P = f h(A, T I D A, K C, B C)$ として算出され、A、T I D A、O W P の 3 つを記録させた N F C タグ 1 9 A（および A、T I D A、O W P の 3 つを印刷した有価紙葉 1 8 A）は K C 値や B C 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 3 0 0 8 A および 3 0 0 8 A G の生成関数と 3 D に認証関数に対し同一の K C 値、B C 値を設定した後に K C 値、B C 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）K C 値 B C 値を変更しない場合、N F C タグ中の A、T I D A、O W P の 3 つの情報が漏洩し O W P 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 O W P を更新したいときがあるかもしれない。その場合には O W P を生成する O T P トークンのコントラクトの管理者が数カ月、数年ごとに K C 値と B C 値をセッター関数 $f s c b$ で書き換えることで O T P トークンのシークレット変数を書き換え、O W P を任意の時間間隔で変更できる。更新された取得した O W P は更新前の複製されていたかもしれない O W P とは異なる。

30

ここでは N F C タグについて述べているが、紙のチケットなどでも O W P が更新され、O W P の更新前に印刷した紙のチケットは無効となる。K C 値 B C 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 N F C 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。K C 値や B C 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 1 8 A 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。1 8 A には好ましくは A、T I D A、O W P のほかに印刷時のブロック番号 B n や印刷時刻、サービス提供者の名称と連絡先、O T P 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。

40

【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 3 D をインターネットに接続させ認証関

50

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。

10

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や施錠装置が取り付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。

20

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。

30

【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。シーケンスS230、S231は実施例1と同様である。S230ではOTPを計算する際に $f_h(A, TIDA, KC, BC)$ といった、ブロック番号 B_n 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 $OWP = f_h(A, TIDA, KC, BC)$ 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。

40

【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。シーケンスS233では1C

50

は 1 A のユーザ識別子 A に対しトークン番号 T I D A のトークンを発行する。

【 0 3 8 9 】

< 有価紙葉の製造 >

S 2 3 4 から S 2 4 0 までの一連のシークエンスでは、端末 1 A に発行されたトークン番号 T I D A と端末 1 A に記録された秘密鍵 1 0 1 A を基に、発券サイト 3 E もしくは端末 1 A の記憶装置に記録された発券ソフトウェアを用いて 1 A をブロックチェーンシステムの O T P 生成コントラクト 3 0 0 8 A にアクセスさせ、S 2 3 0 にて 3 0 0 8 A 設定された O W P = f h (A , T I D A , K C , B C) を O T P として生成させる処理を開始する。

そして O W P を 3 E 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 O W P 等認証情報表示画面 1 5 0 0 A を 1 A 表示させ、また必要であれば 1 5 0 0 A の画面情報を端末 1 A のプリンタ 1 5 2 A を用いて印刷させ、O W P と A と T I D A を記入した有価紙葉 1 8 A を製造させる。

また O W P と A と T I D A を記入した N F C タグ 1 9 A を製造させる。N F C タグ 1 9 A についても有価紙葉 1 8 A と同様に、O W P と A と T I D A 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 1 9 A の記録装置に記録させることができる。

【 0 3 9 0 】

シークエンス S 2 3 5 では発券サーバ 3 E にアクセスし 1 5 0 0 A や 1 8 A に発券を行う際に図 6 X 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 S 2 4 2 や S 2 4 4 にて 1 5 0 0 A や 1 8 A や 1 9 A をサービス提供端末 3 D に提示した際に図 8 B の 3 4 2 D 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。(3 4 2 D 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 3 4 2 D を搭載しない場合も本発明では考えられる。)

【 0 3 9 1 】

シークエンス S 2 3 6 、S 2 3 7 、S 2 3 8 で端末 1 A は端末 3 A の O T P 生成コントラクトに O T P 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 3 E のウェブサイトではチケットを発行している場合には S 2 3 9 にて有価紙葉の情報 1 5 0 0 A を表示し、1 5 0 0 A の印刷を許可し有価紙葉 1 8 A を印刷させ N F C タグ 1 9 A に有価紙葉の情報を記録させる。また 1 A 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 S 2 4 0 にてソフトウェアを通じて有価紙葉の情報 1 5 0 0 A を表示し、1 5 0 0 A の印刷を許可し有価紙葉 1 8 A を印刷させ N F C タグ 1 9 A に有価紙葉の情報を記録させる。

【 0 3 9 2 】

< 有価紙葉の使用 >

シークエンス S 2 4 1 では 1 5 0 0 A を表示できる端末 1 A もしくは S 2 4 0 で製造した紙チケット 1 8 A 又は N F C タグ 1 9 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 3 D へ提示し入場や解錠を試みる。このとき 1 5 0 0 A または紙チケット 1 8 A を端末 3 D のカメラ 3 4 0 D に読取させる。また N F C タグ 1 9 A の O W P の認証に必要な入場口又は施錠設備の端末 3 D の通信装置 3 2 D を通じて読取させる。

【 0 3 9 3 】

シークエンス S 2 4 2 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 N F C タグチケットのデータ読み取り、

端末 3 D がネットワーク 2 0 と接続されていない場合 (オフラインの場合) 、 S 2 4 2

10

20

30

40

50

にてサービス部の端末装置 3 D 内部の 3 0 0 D や 3 0 1 0 D に記録された認証関数 3 0 1 8 D A にて O W P の検証、認証処理を行い認証関数から認証結果の戻り値 C T A U を得る。

端末 3 D がネットワーク 2 0 と接続されている場合（オンラインの場合）、S 2 4 3 にて D L S 上の認証関数 3 0 1 8 A にアクセスして O W P を認証し認証関数から認証結果の戻り値 C T A U を得る。S 2 4 3 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 3 D 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 3 D では保守点検用に 3 D の 3 0 0 D や 3 0 1 0 D に記録された認証関数 3 0 1 8 D A に用いる変数 K C や B C を変更できる通信用の端子や無線通信装置、N F C 装置を備えていると好ましい。

10

端末 3 D 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ネットワーク上の 3 A のブロックチェーン部を複製し同期させつつ、インターネットネットワークから遮断された場合でも端末 3 D にブロックチェーン部 3 0 0 D を構築できていることが好ましい。

【 0 3 9 4 】

シークエンス S 2 4 4 では端末 3 D は認証関数から認証結果の戻り値 C T A U 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 3 5 0 D を操作する。認証結果の戻り値 C T A U が正しく無い場合には再度認証を行うまで待機する。S 2 4 4 にて 3 5 0 D を操作すると同時に 3 5 1 D と 3 5 2 D 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。

20

また S 2 4 4 において入場口や駅の改札の端末 3 D などの時に開閉装置 3 5 0 D が無く人員によって入場者の制止などを行う場合は 3 5 0 D を備えていなくてもよく、3 5 0 D 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 3 5 1 D と 3 5 2 D 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。

【 0 3 9 5 】

シークエンス S 2 4 5 ではコントラクト管理者端末 1 C がブロックチェーンのノード端末 3 A にアクセスし、O T P 生成コントラクトのシークレット変数 K C 値や B C 値を変更し、さらに端末 3 D の記憶装置の 3 0 0 D や 3 0 1 0 D に記録された認証関数の K C 値 B C 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 O W P が変更される。ネットワークに接続されていない端末 3 D は端末 3 D 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、N F C 装置が必要である。端末 3 D 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 K C 値や B C 値を変更する必要がある。

30

【 0 3 9 6 】

シークエンス S 2 4 5 において端末 3 A と端末 3 D の K C や B C を変更すると、ユーザーが製造した N F C 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（1 1 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 K C 値や B C 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、N F C 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。

40

【 0 3 9 7 】

シークエンス S 2 3 2、S 2 3 3 に関連して端末 3 D 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 3 D の R O M となる記憶装置に記録させてもよい。端末 3 D の認証関数は A、T I D A、O W P を N F C 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 3 D 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

50

の製造時に端末 3 D に組み込むことができる。

【 0 3 9 8 】

< 自動車の鍵 >

例として仮に O T P トークンとそのトークンが生成する O W P 型のパスワード等を N F C 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 O T P 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 3 D が製造番号に対応する自動車の施錠装置の端末 3 D や始動制御装置端末 3 D あるいは自動車のメインコンピュータ端末 3 D に搭載されうる。

自動車を所有している事は D L S 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、O W P 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 O W P を生成し N F C 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 , T I D A , O W P を持つ N F C 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 S 2 4 5 において定期的に 3 A を含むブロックチェーンシステムと自動車の端末 3 D の K C , B C を変更させ更新させる。

また端末 3 D 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 3 D に書き込んでよい。前記の例ではユーザー識別子 B が内部で端末 3 D に書き込まれて O T P 認証関数 3 0 1 8 D A の引数に固定されていれば端末 3 D は解錠時にユーザー識別子 B に由来する O W P 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 3 D がインターネットワークに接続できる場合には端末 3 D とサーバ端末 3 A での K C , B C の更新と同期は容易であるが、インターネットワーク 2 0 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 K C , B C の更新の対応ができる。また定期的な自動車検査の段階で自動車の端末 3 D の認証関数とそれを動かす N F C タグ 1 9 A 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 3 D もユーザーの求めに応じて保守点検や譲渡時に K C を B C を書換えて N F C タグと端末 3 D 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 R O M 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 R O M の形で）端末 3 D 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、自動車等の製品の所有者の履歴情報、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。

【 0 3 9 9 】

< 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 3 D に固有のトークン番号を端末 3 D の記憶装置 3 0 D の R O M に記録させ、ユーザーのもとへ端末 3 D を含む製品を流通させることができる。一方で 3 0 D の R O M 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 3 D 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 3 0 D にトークン番号を記録させる際に R O M ではなく不揮発性の R A M を使い、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 N F C 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 3 D 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 T I D A 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 3 D への接続用端子や N F C 等通信部を用いて、ユーザー端末 1 A などから記憶装置 3 0 D 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 T I D A に設定

する。そして端末 1 A の持っている秘密鍵 1 0 1 A を用いてサーバ 3 A より O W P を生成し、O W P とユーザ識別子 A (そしてトークン番号 T I D A) を N F C タグ 1 9 に記録させ、前記認証情報を記録した N F C タグ 1 9 にて端末 3 D で O W P による O T P 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 3 D においても自動車の場合と同じくユーザ識別子を端末 3 D に記録させてもよい。(装置にユーザ識別子という形でユーザの名義を記入してもよい。)

【0400】

< N F C タグの電源および入出力装置 >

N F C タグ 1 9 A 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。1 9 A 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 N F C 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 1 9 A は備え、なおかつ 1 9 A の O W P 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 1 9 A の入力装置は N F C 機能付きの I C カードやタグであるときは、入力装置が N F C 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)。1 9 A には N F C 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 N F C タグ 1 9 A 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。1 9 A 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 8 C 及び図 8 D は本発明のワンタイムパスワード認証システム(O T P 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 8 C はネットワーク 2 0 を経由して双方向に通信できるよう端末 4 A、端末 1 C、端末 3 A、端末 5 A、端末 5 B が接続されている。図 8 D は端末 4 A (および 4 A と同等の複数端末)が放送局端末 5 C 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 4 A の記録部にはソフトウェア C R H N の情報 4 0 3 A が記録され、4 0 3 A のプログラムを実行しソフトウェア C R H N を動作させ暗号化されたデータ E n c D a t a (図 4 B の 4 0 3 4 A)を本発明の認証システムから得られた鍵情報 C T A U 4 0 3 1 A や外部の鍵情報 A K T B 4 0 3 2 A を用いて復号に用いる鍵情報 T T K Y 4 0 3 3 A を作成し、4 0 3 3 A を用いて 4 0 3 4 A を復号し復号されたデータ D e c D a t a (図 4 B の 4 0 3 5 A)を得て 4 0 3 5 A を閲覧または視聴し、4 0 3 5 A がプログラムの場合は実行する。図 8 C と図 8 D 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 ではウェブサイトログイン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 B n 等ブロックチェーンの時刻情報を利用した B n T O T P を用いる。実施例で利用する B n T O T P は $B n T O T P = f h(A, T I D A, K C, B n)$ または $B n T O T P = f h(A, T I D A, K C, B n, V)$ または $B n T O T P = f h(A, T I D A, K C, B C, B n, V)$ であり、変数 K C と B C はコントラクト管理者によって関数 f s c b により変更され更新されることがある。

10

20

30

40

50

【 0 4 0 3 】

図 7 C A 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ケンスを示す。図 7 C B 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ケンスを示す。図 7 C C 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 O F B K M K を用いて暗号化ファイルを復号し閲覧する例を示す。

【 0 4 0 4 】

< 暗号化されたデータの作成 >

まずソフトウェア C R H N 4 0 3 A 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。

10

図 7 C B のシーケンス S 1 8 0 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。S 1 8 1 では平文データに添付する電子証明書 D e c C e r t など（電子証明書とコンテンツデータと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 C R H N 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るなら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 C R H N 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进行处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 C R H N 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。

20

【 0 4 0 5 】

S 1 8 1 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 5 A（C R H N c m）にリンクし接続させるための広告配信サイトの U R I を埋め込むことができる。

30

この端末 5 A の広告配信サイトへの U R I を平文データに埋め込むこと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 5 A 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 4 0 3 A 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 U R I を設定することもできる（基本的な U R I 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 U R I に対応する広告データを設定するなど）。

40

ここで設定する U R I 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 O T P 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 2 0 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 U R I は変更出来ない。

【 0 4 0 6 】

端末 5 A が配信する広告配信サイトへ接続するための U R I はソフトウェア C R H N 4 0 3 A にも設定でき、端末 4 A で 4 0 3 A 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 4 0 3 A が調べることもできる。広告に加えソフトウェア C R H N 4 0 3 A 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 4 0 3 A は広告

50

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TTY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における値であり、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TTY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TTY(4033A)を生成させた。

また実際にはこのほかにTTY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TTY(4033A)を生成する方法を考案した。実施例3ではCTAUとAKTBとCRKY

10

20

30

40

50

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はなく、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)を利用して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。

10

【0412】

CTAU(3021Aまたは4031A)に加えAKTB(4032A)が利用できる。4032Aは具体的に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。

20

【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DLSにデプロイする。

30

【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。

40

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。

50

【 0 4 1 5 】

また、端末 5 B 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 5 B 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 5 B 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 A K T B (4 0 3 2 A) 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 4 0 3 2 A の伝達を 4 0 3 2 A をユーザ識別子 A に内容を秘匿化できるトランザクションを用いて A K T B (4 0 3 2 A) 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 4 A の秘密鍵 4 0 1 A を基に別のブロックチェーン基盤を構築し秘密鍵 4 0 1 A A からユーザ識別子 A ではなくユーザ識別子 A A が計算される場合にユーザ識別子 A A に向けて 4 0 3 2 A 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 A A を示す秘密鍵 4 0 1 A を用い、OTP トークンの発行はイーサリアムを用い、A K T B (4 0 3 2 A) 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。

【 0 4 1 6 】

S 1 8 5 では広告機能を持つサーバ 5 A (S V C R H N c m) 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。

【 0 4 1 7 】

S 1 8 6 ではコントラクトの管理者端末 1 C 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 1 C の秘密鍵 1 0 1 C に対応するユーザ識別子 C に発行する。S 1 8 6 は端末 1 C 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 1 C に記録し、記録した暗号化データを配布するためのシーケンスである。

後に後述するが、S 1 5 5 では端末 5 B 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 5 B で購入される必要はなく、端末 1 C が注文や依頼を受ければ発行できる。たとえば端末 1 C 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識別子が必要である。

【 0 4 1 8 】

S 1 8 7 ではソフトウェア C R H N (4 0 3 A) を主に端末 5 B から取得する。端末 5 B 以外でも信頼できる 4 0 3 A 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）4 0 3 A 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 C R H N (4 0 3 A) を暗号化データと共に配布すればよい。

【 0 4 1 9 】

S 1 8 8 では設定読込・入力等を行う。4 0 3 A に秘密鍵を直接入力するか秘密鍵を管理する 4 0 3 A とは別のソフトウェアと連携させ秘密鍵情報を 4 0 3 A に入力する。

【 0 4 2 0 】

S 1 9 9 では 4 0 3 A 起動時、あるいは秘密鍵（図 7 C B では端末 1 C の秘密鍵 1 0 1 C ）の情報が 4 0 3 A に入力された時にユーザ識別子が計算され生成され、4 0 3 に埋め

10

20

30

40

50

込まれた端末 5 A の広告配信用 U R I 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 1 C に対しても図 6 X に示すような不正アクセスの監視を行うことができる。

【 0 4 2 1 】

S 1 8 9 では A K T B (4 0 3 2 A) を設定する。もしくはあらかじめ決めておいた A K T B (4 0 3 2 A) を端末 1 C の記録装置に記憶させる。S 1 8 9 は S 1 8 8 と同時に行ってもよい。A K T B (4 0 3 2 A) 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 A K T B (4 0 3 2 A) を設定して団体に所属するユーザー同士が A K T B (4 0 3 2 A) を知っており O T P 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。

10

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 A K T B (4 0 3 2 A) を設定しメールアドレスなどで A K T B (4 0 3 2 A) を通知してから、権利者は平文データを A に対応した A K T B (4 0 3 2 A) を用いて暗号化してもよい。

【 0 4 2 2 】

暗号化に関して、C T A U (3 0 2 1 A または 4 0 3 1 A) と任意設定し配布先に通知される A K T B (4 0 3 2 A) とソフトウェア C R H N (4 0 3 A) と 4 0 3 A の秘密鍵 C R K Y (4 0 3 0 2 A) を利用してユーザー識別子 A だけが知る A K T B (4 0 3 2 A) 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 5 B 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 2 0 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。

20

雑誌や書籍について顧客ごとに異なる A K T B (4 0 3 2 A) 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 A K T B (4 0 3 2 A) 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。

30

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 A K T B (4 0 3 2 A) 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、A K T B (4 0 3 2 A) 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 O T P トークンをブロックチェーンに所有し、A K T B (4 0 3 2 A) を知り、ソフトウェア C R H N (4 0 3 A) を持っているユーザがそのデータを手に入れば新聞を読めるようにすることもできる。

【 0 4 2 3 】

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 (4 0 3 4 A) を O T P トークン (O T P トークンの認証時に得られる C T A U (3 0 2 1 A)) と A K T B (4 0 3 2 A) とソフトウェア C R H N (4 0 3 A) と C R K Y (4 0 3 0 2 A) と秘密鍵 4 0 1 A がある場合に復号し、復号データ・平文データ (4 0 3 5 A) として閲覧できる。

40

閲覧時に暗号化データを復号できる鍵 T T K Y (4 0 3 3 A) が算出されそれを秘密鍵 4 0 1 A で暗号化し C T T K Y (4 0 3 6 1 A) とし、C T T K Y (4 0 3 6 1 A) をソフトウェア C R H N (4 0 3 A) に記録された C R K Y (4 0 3 0 2 A) で暗号化し A C T T K Y (4 0 3 6 0 A) を得て、O T P 認証済み証明書 4 0 3 6 A または閲覧済み証明書 O F B K M K (4 0 3 6 A) データ内部に記録する。O F B K M K はソフトウェア C R H N 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 T T K Y (4 0 3 3 A) を記録している。(O F B K M K はオフライン・ブック・マーク)

50

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。

10

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、 $300[\text{分}] \div 10 = 30[\text{分}]$ の間に限り、ソフトウェアCRHN(403A)にて閲覧可能などとして行うことができる。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。

20

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。

30

【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。

40

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

50

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。

10

(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。

20

【0426】

S190からS192までの一連のシーケンスは、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生成のシーケンスは実施例1や実施例2と同様である。

30

【0427】

S193からS195までの一連のシーケンスは、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。

40

【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(4034

50

A、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。

10

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。

20

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 packets 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よい。

30

【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。

40

【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

50

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。

【 0 4 3 4 】

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。

10

【 0 4 3 5 】

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。

20

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。

【 0 4 3 6 】

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。

30

【 0 4 3 7 】

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ー識別子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。

40

【 0 4 3 8 】

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５Ａに記録し図６Ｘのようなア

50

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S 1 5 9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。

【0 4 3 9】

S 1 6 0からS 1 6 5まではOTPの生成と認証の一連のシーケンスでありS 1 9 0からS 1 9 5までの一連のシーケ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S 1 6 0からS 1 6 5までのシーケンスはソフトウェアC R H N (4 0 3 A) 内部で自動的に行ってもよい。S 1 6 2からS 1 6 3のシーケ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4 0 3 A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。

10

S 1 6 2からS 1 6 3のシーケ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4 0 3 Aのプログラムを設定できる。

【0 4 4 0】

S 1 6 6は4 0 3 AにてC T A U (4 0 3 1 A) とA K T B (4 0 3 2 A) とC R K Y (4 0 3 0 A) からE n c D a t a (4 0 3 4 A) を復号する鍵情報T T K Y (4 0 3 3 A) を生成する。

【0 4 4 1】

S 1 6 7はS 1 6 6で生成された鍵情報T T K Y (4 0 3 3 A) を用いて暗号化データE n c D a t a (4 0 3 4 A) を復号し、平文データD e c D a t a (4 0 3 5 A) を得る。

20

【0 4 4 2】

S 1 6 8にてS 1 6 7で4 0 3 4 Aを復号して端末4 Aの記憶装置に得られた平文データ4 0 3 5 Aについて、端末4 Aの出力装置4 5 Aと入力装置4 4 Aを用いて平文データ4 0 3 5 A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4 0 3 5 A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。

30

実施例3ではウェブブラウザソフトが対応するH T M L 5とE C M A S c r i p tで処理できる米国アドビ社の文章データを管理するP D F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M P 3ファイル(拡張子は.mp3)、I S O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M P 4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C R H N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P D F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P D F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P D F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。)

40

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。

50

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。

【 0 4 4 3 】

ファイルの形式等に応じてソフトウェア C R H N (4 0 3 A) は平文データ 4 0 3 5 A の内容を読み取り、権利者が 4 0 3 5 A 設定したプログラムに応じてユーザーの端末 4 A でのプリンタ 4 5 2 A 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 4 5 0 A やスピーカー 4 5 1 A ヘッドマウントディスプレイ 4 5 3 A 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 4 5 A から出力させる。また入力装置 4 4 A 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。

10

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 4 5 0 A 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 4 5 0 A 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 4 5 0 A 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 4 5 3 A は用いず通常のディスプレイ 4 5 0 A のみを用い暗号化データをソフトウェア 4 0 3 A と分散型台帳システム D L S を用いた O T P 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 D L S による O T P 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。

20

ヘッドマウントディスプレイ 4 5 3 A 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 V R 、拡張現実 A R を実現する際の O T P 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 O T P トークンから計算される O T P 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 B n T O T P 型の O T P 認証コードを用いてもよい。 O T P を疑似ランダム用途に利用する場合は O T P 認証に用いるよりも少ない桁数の値、例えば本来 10 桁の O T P 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。

30

【 0 4 4 4 】

また S 1 6 8 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 4 4 A を用いて平文データの書き換えを行い端末 4 A の秘密鍵 4 0 1 A 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 B n 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 H M A C 等 M A C 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 4 0 1 A 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 4 A の O T P トークンを用い C T A U (4 0 3 1 A) と A K T B (4 0 3 2 A) と C R K Y (4 0 3 0 A) 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 T T K Y (4 0 3 3 A) 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 O T P 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 H M A C の M A C 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

40

50

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ケンスは図7C Bと図7C Cを組み合わせたものである。ユーザーU AとユーザーU Cがある団体に所属し機密文章をH M A CのM A C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C R H N (4 0 3 A) 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。

【 0 4 4 5 】

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S 1 6 8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、4 0 3 A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4 0 1 A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ィ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7C Bと図7C Cを組み合わせることで実現できる。

紙の教科書と比べO T P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4 A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O T P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C R H N (4 0 3) は音楽や動画といった権利者の存在する作品を復号し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。

【 0 4 4 6 】

S 1 6 9においてコンテンツに内蔵されたU R Iに対応する広告等サーバ5 A (S V C R H N c m) に接続させることができる。これはソフトウェアC R H N (4 0 3 A) に内蔵されたプログラムが、S 1 6 8にてS 1 6 7で4 0 3 4 Aを復号して端末4 Aの記憶装置に得られた平文データ4 0 3 5 A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4 0 3 Aはサーバ5 Aに接続できるU R Iが記載されている場合にそのU R Iの接続先から広告の配信を受ける。ここでU R I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U R I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。

S 1 6 9において端末4 Aのユーザー識別子、保有しているトークン番号、I Pアドレスや位置情報、端末のI Dやセンサ値などから図6 X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5 Aに記録させることもできる。プライバシー保護のために5 Aまたは5 A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。

10

20

30

40

50

S 1 6 9ではサーバ5 A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5 A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5 A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】

S 1 7 0では閲覧済みの証明書データOFB K M K (4 0 3 6 A)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4 0 3 Aにて行われる。S 1 7 0 Aで証明書データ(4 0 3 6 A)はT T K Y (4 0 3 3 A)を暗号化もしくは難読化し、なおかつO T P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4 0 3 3 A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できるようにしたものである。

10

何らかの形で4 0 3 3 Aを難読化・暗号化し端末4 Aのユーザーからは復号されない(復号が困難な)鍵情報4 0 3 6 0 Aとする。O T P認証時の時刻データ及びユーザー識別子等情報(4 0 3 6 2 A)と4 0 3 6 0 A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4 Aの秘密鍵4 0 1 Aまたは秘密鍵C R K Y (4 0 3 0 2 A)をキーとしたH M A C (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H M A C 値を算出し認証情報(4 0 3 6 3 A)とする。そして4 0 3 6 0 Aと4 0 3 6 2 Aと4 0 3 6 3 Aを連結し閲覧済み証明書データOFB K M K (4 0 3 6 A)とする

20

【0448】

S 1 7 0では閲覧済みの証明書データOFB K M K (4 0 3 6 A)はネットワークから端末4 A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C T A U 値(4 0 3 1 A)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OFB K M K (4 0 3 6 A)には暗号データを復号するT T K Y (4 0 3 3 A)の情報が含まれる。

4 0 3 6 Aに4 0 3 3 Aを記載してしまう事もできるが、その場合は4 0 3 3 A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C R H N (4 0 3 A)のプログラムに内蔵された秘密鍵C R K Y (4 0 3 0 2 A)のみを用い4 0 3 3 Aを暗号化することも可能であるが、その場合は同じ4 0 3 A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4 0 3 A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4 0 3 Aが出力した4 0 3 6 A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1 0 1 B)であったとき4 0 3 Aはそれを検知して閲覧を実行させないこともできる。)

30

そこで4 0 3 3 Aを端末4 Aの秘密鍵4 0 1 A (4 0 1 Aには端末4 Aの様々な有価なO T Pトークンが割り当てられている)を用いて暗号化しC T T K Y (4 0 3 6 1 A)とする。続いてC T T K Y (4 0 3 6 1 A)をソフトウェアC R H N (4 0 3 A)の秘密鍵(4 0 3 0 2 A)を用いて暗号化しA C T T K Y (4 0 3 6 0 A)とした。

40

秘密鍵4 0 1 Aの流出時や秘密鍵の不正な使いまわしは端末4 A等のユーザー端末が広告サーバ5 Aにアクセスした際に図6 X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4 0 3 6 Aは4 0 3 3 A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H M A Cを用いて算出したM A C 値を含むデータである。4 0 3 6 Aは内部情報の改ざんを検知できるH M A C から計算されるM A C 値を備えている。改ざん検知をさせる情報(4 0 3 6 3 A)には共通鍵やハッシュ関数に基づくH M A C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4 0 3 6 Aの改ざん検知ができれば良いのでH M A Cを用いた。

50

【 0 4 5 0 】

実施例 3 では T T K Y (4 0 3 3 A) を難読化もしくは暗号化し鍵情報 4 0 3 6 0 A にする方法として、4 0 3 3 A を端末 4 A の秘密鍵 4 0 1 A で暗号化した後ソフトウェア C R H N (4 0 3 A) の秘密鍵 C R K Y (4 0 3 0 2 A) で暗号化させ、端末 4 A の秘密鍵 4 0 1 A とソフトウェア C R H N (4 0 3 A) の秘密鍵 4 0 3 0 2 A が揃う場合でなければ T T K Y (4 0 3 3 A) 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、T T K Y (4 0 3 3 A) を秘密鍵 4 0 1 A を鍵に用いて共通鍵暗号化して C T T K Y (4 0 3 6 1 A) 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 O F B K M K (4 0 3 6 A) 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 T T K Y (4 0 3 3 A) を暗号化もしくは難読化させそれを復号し再度 T T K Y (4 0 3 3 A) として取得出来る方法であれば構わない。)

そして C T T K Y (4 0 3 6 1 A) をソフトウェア C R H N (4 0 3 A) のプログラムに内蔵された秘密鍵 C R K Y (4 0 3 0 2 A) を鍵に用いて暗号化し A C T T K Y (4 0 3 6 0 A) として、A C T T K Y にブロック番号 B n 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 O T P 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 4 0 1 A と H M A C を利用し電子署名を行い証明書データ O F B K M K (4 0 3 6 A) を作成する。H M A C のハッシュ関数は例えば S H A - 2 の S H A 2 5 6 を利用できる。

【 0 4 5 1 】

< 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 4 0 1 A 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 4 0 1 A 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 S V C R H N c m に I P アドレスや端末装置のシリアル番号、端末の入力装置 4 4 A の入力センサ 4 4 4 A の情報が規約で同意されている場合はサーバ 5 A に通知されサーバ 5 A に図 6 X に示すユーザー識別子と O T P トークンのトークン番号と I P V 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 3 C、実施例 2 では端末 3 D、実施例 3 では端末 5 A にアクセスする端末に対し図 6 X に示すユーザー識別子と O T P トークンのトークン番号と I P V に収集され記憶される。

もしオフラインの場合は G N S S や J J Y、N I T Z といった時刻情報を受信できる場合には、4 0 3 6 A 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 4 0 3 6 A で復号せず、ネットワークにて悪意を持って 4 0 1 A 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 C R H N (4 0 3 A) や書籍のデータに埋め込まれた広告サイトへの U R I を経由し端末 5 A に図 6 X 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 I P アドレスなどをハッシュ化しない様に規約を設定し I P アドレスを記録し図 6 X のようなアクセスの監視を端末 5 A で行うことを規約に明記して O T P 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 4 0 3 A 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 4 0 1 A 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

10

20

30

40

50

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。

10

【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。

20

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。

30

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】

40

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】

50

S 1 7 1ではコントラクト管理者が端末 1 Cを用いてコントラクトの K C 値や B C 値といった O T P 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 4 Aは本発明の O T P 認証時にインターネットワークに接続され B n T O T P もしくは O W P は常に最新のシード値を用いて認証が行える。また O T P トークンの名前や連絡先などを記載した看板情報 K N B N（3 0 2 4 A）も書換えることができる。その利用例として、O T P 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 B n T O T P のほかに O W P を用いてもよい。

【0 4 5 5】

< 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 >

10

紙の書籍はネットワーク 2 0 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 2 0 の存在を前提としてネットワーク 2 0 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 2 0 から切断された端末 4 Aにおいて、端末 4 Aに記録された O T P 認証を行って暗号化データを閲覧した時（シークエンス S 1 7 0 の時）に作成される証明書データ O F B K M K（4 0 3 6 A）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 7 C C にネットワーク 2 0 から端末 4 A 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。

20

本発明では実施例 3において図 7 C C に示すようにネットワーク 2 0 に接続されていない端末 4 A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 4 0 3 6 A に暗号化データの復号に用いる T T K Y（4 0 3 3 A）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 O T P 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 4 0 3 6 2 Aを含み、4 0 3 6 Aと4 0 3 6 2 A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 H M A C にて M A C 値（4 0 3 6 3 A）を算出し4 0 3 6 Aと4 0 3 6 2 Aと4 0 3 6 3 Aを連結して4 0 3 6 Aとする事を利用した。

30

4 0 3 6 Aに必要な情報は暗号化データの復号に用いる T T K Y（4 0 3 3 A）の算出に結びつく情報と、ネットワーク 2 0 に接続していた際に図 7 C A の S 1 5 6 から S 1 7 0 において O T P 認証を行い T T K Y（4 0 3 3 A）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 4 0 3 6 2 Aを結合し、端末 4 Aの秘密鍵 4 0 1 Aやソフトウェア C R H N（4 0 3 A）に内蔵された秘密鍵（4 0 3 0 2 A）または4 0 3 0 2 A以外のソフトウェア内部変数を基に H M A C にて算出した M A C 値（4 0 3 6 3 A）があれば本発明の証明書データを構成できる。

【0 4 5 6】

< 暗号化データ 4 0 3 4 A 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 4 0 3 A の内部に持つ場合 >

40

実施例 3の別の 4 0 3 6 Aの実施形態として図 4 C に記載の端末 4 Aのソースコードが難読化・暗号化されたソフトウェア 4 0 3 A の内部の 4 0 3 0 A に平文データ 4 0 3 5 A が内蔵されている実施例が実施できる。（4 0 3 A 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 4 0 3 0 A にソフトウェア用の秘密鍵 4 0 3 0 2 A と共に平文データ 4 0 3 5 A を組み込む場合である）。

この場合にはソフトウェア 4 0 3 A の秘密鍵 4 0 3 0 2 A とユーザー用秘密鍵 4 0 1 A がある時、ソフトウェア 4 0 3 A の 4 0 3 0 A にあるシークレット変数 K 4 0 3（4 0 3 0 3 K A）を用いて

4 0 1 A から計算できるユーザー識別子 A の情報と O T P 認証時の時刻情報 T 4 0 3 と K 4 0 3 を連結させた情報のハッシュ値 H T 4 0 3 を求め、前記ハッシュ値 H T K 4 0 3 と

50

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

10

20

30

40

50

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TTY(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TTY(4033A)が必要ないので、暗号化データを復号する鍵TTY(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】

10

20

30

40

50

S 2 0 3では4 0 3 6 AのA C T T K Y 4 0 3 6 0 AをC R K Y 4 0 3 0 2 A等にて復号しC T T K Y 4 0 3 6 1 Aを得る。

C T T K Y 4 0 3 6 1 Aを端末4 Aの秘密鍵を用いて復号しT T K Y 4 0 3 3 Aを生成する。

【0 4 6 8】

S 2 0 4ではT T K Y 4 0 3 3 Aにて暗号化データ4 0 3 4 Aを復号し平文データ4 0 3 5 Aを得る。

【0 4 6 9】

S 2 0 5ではソフトウェアC R H N 4 0 3 Aのプログラムに従い、証明書データ4 0 3 6に含まれる4 0 3 6 3 Aから証明書が改ざんされていないことを確認し、4 0 3 6 Aに含まれるO T P認証時及び平文データの閲覧時刻情報4 0 3 6 2 Aの時刻情報を取得し、端末4 Aの時刻情報と4 0 3 6 2 Aの時刻情報から閲覧可能な時刻を算出する。

10

【0 4 7 0】

S 2 0 6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D AのG N S S受信器や、N I T Z、J J Y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C R H N 4 0 3 Aのプログラムや、平文データ4 0 3 5 A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。S 2 0 6では4 0 3 6 2 A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4 0 3 A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。

20

【0 4 7 1】

S 2 0 7ではS 2 0 6で4 0 3 6 2 A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4 Aで経過したときを示す。S 2 0 8ではS 2 0 7に示す時刻になったときソフトウェア4 0 3 A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。

【0 4 7 2】

また図7 C Cのネットワークに接続されていない場合において、端末4 Aが図4 Cに示す構成(ソフトウェア4 0 3 Aの4 0 3 0 Aに平文データ4 0 3 5が内蔵され暗号化もしくは難読化されている場合)ではS 2 0 3やS 2 0 4のシーケンスを除いたシーケンス図となる。

30

【0 4 7 3】

実施例3のソフトウェアC R H N (4 0 3 A) には、

- 1 . E n c D a t a から D e c D a t a への変換のみができるものC R H N R e a d e r 、
- 2 . D e c D a t a から E n c D a t a への変換をするものC R H N W r i t e r 、
- 3 . D e c D a t a と E n c D a t a の相互変換を行えるものC R H N R e a d e r W r i t e r

の3種類が考えられる。

40

C R H N R e a d e r W r i t e r 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E n c D a t aとして保持し、ユーザーがE n c D a t aを復号して変更する際にD e c D a t a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B n T O T P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C R H N R e a d e r W r i t e r 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

50

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にもできる。

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。

10

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。

20

【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。

30

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 >

40

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

50

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ことから、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。

10

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。

20

<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ことができる。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。

30

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。

40

【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

50

ンテンツのレーティングを付与したことを示す監査証明書 *A u d i t R a t* 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 *A u d i t R a t* 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 *D e c C e r t* も利用されない。

暗号化ファイルに *E n c D a t a* にそのデータのハッシュ値と内容を保証する *E n c C e r t* 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 *C R H N 4 0 3 A* 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 *C R H N 4 0 3 A* 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。 *4 0 3 A* 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 *4 0 3* 用の物と、業務用の *4 0 3* 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 *C R H N 4 0 3 A* 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、*C R H N* がコンピュータの *B I O S* に相当する基本ソフトウェア部分を持っていたてもよい。

【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 *S o l i d i t y* 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 B_n が一つ増加する。ブロック番号 B_n 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 B_n 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、 $B_n \times 15 [sec]$ 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 *P R V A*（101A）はユーザー *U A* 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 D W A L T 1 6 0 3 A に記録されていもよい。D W A L T 1 6 0 3 A は接触式 I C カード型、非接触式 I C 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（N F C タグ型）でもよい。また紙や板などの記録された秘密鍵 P R V A 1 6 0 8 A 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
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 U A や U C 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 B n T O T P 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
P などからサーバ端末 3 F 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。サーバ端末 3 F を代表として端末 3 E や端末 5 B 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 3 F の記憶部 3 0 F の 3 0 1 F 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 3 F 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 3
F 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 O T P トークンのコントラクト識別子やサービ
ス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 3 A 等
にアクセスが集中することなく 3 F にて検索のアクセスを受け付けその情報を配信で
きる。3 0 1 F には 3 1 1 F の記憶が書き込まれているとともに 3 0 1 F は 3 1 1 F により制
御される。

端末 3 F がサーバ端末 3 A や 3 B 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（S S D ）
などに頻度の高い O T P 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 S S D 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 O T P 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 O T P トークンがあり、人々がその O T P トークンの名前や O T P トークンの発
行者（出版社名など）、O T P 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）、O T P 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）、O T P トークンは譲渡制
限があるかどうか、O T P トークンの看板情報 K N B N に記載のレーティング情報や出版
社連絡先・O T P 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。

10

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。

20

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。

30

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。

40

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

50

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。

10

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でも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>

20

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。

30

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。

40

【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

50

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等を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が利用できる。

10

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。

20

【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。

30

【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。

40

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

50

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。

10

【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ー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。

20

【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、Ｓｏｌｉｄｉｔｙ、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。

30

【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。

40

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

50

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f h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設するといった際に、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44A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、どのような情報を収集し、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

10

20

30

40

50

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。

10

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。

D L T (Distributed Ledger Technology) 分散型台帳技術のこと。

20

D L S (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D A G型システムの略号にD L Sを用いた。

U R I (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 D L S 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・D L S 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。

30

秘密鍵 P R V A 等 D L S 上で利用する秘密鍵。秘密鍵とD L S が無ければO T P 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D L S 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。

U A 端末1Aのユーザ。

U B 端末1Bのユーザ。

U C 端末1Cのユーザ。

U P 端末4Aのユーザ。

B n T O T P ブロックチェーンなどのD L S 上でブロック番号B n とコントラクト内部のシード値K C 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。

40

O W P コントラクト管理者(O w n e r) が分散型台帳システムD L S のコントラクト内部変数K C やB C を任意時間、任意数位に書き換えることで、疑似的なO T P を生成する際のパスワードの略称。

B I O S 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。

E F I Extensible Firmware Interfaceの略。特許出願時点で利用されている最新のB I O S の規格。

50

R O M Read Only Memory。データの書き込み後、読取のみできる記憶装置。
 R A M Random Access Memory。データの消去、書換が可能な記憶装置。
 C P U 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。
 S o C System on Chip。C P Uとグラフィック処理装置、G N S S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。
 M C U Micro Control Unitの略称。マイクロコントロールユニット。
 N F C Near Field Communicationの略称。近距離無線通信。
 N I T Z ネットワーク i dおよびタイムゾーン。
 G N S S Global Navigation Satellite System / 全球測位衛星システム。
 J J Y 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D L Sにおいて、D L S上で最新の時刻Tにおいて変化する情報T B（もしくはT m）のうち、ブロック番号B n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B n T O T P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D L S上で最新の時刻Tにおいて変化する情報T Bをワンタイムパスワード認証システムに關与するコントラクトのシード値B CやK C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T I D AのパスワードO W P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B n T O T Pについてシード値K C、B C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B n T O T P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B S Zを擬似乱数の元となる値としてB n T O T P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B n T O T P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】

< B n T O T P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。

< O W Pによる用途 >

チケットなど有価紙葉1 8 Aや施錠を解錠するN F Cタグ1 9 Aに用いられる。

パスワードO W P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T I D AとパスワードO W Pを紙などに文字列またはバーコードとして印刷し1 8 Aとし、あるいはN F Cタグ1 9 A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O W P、ユーザー識別子A、トークン番号T I D A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

10

20

30

40

50

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。

10

N F C タグ 1 9 A に O W P とユーザー識別子 A とトークン番号 T I D A を記録した場合は、N F C タグ 1 9 A を読み取ることの出来る施錠を管理する端末 3 D に A と T I D A と O W P を読み込ませ認証処理を端末 3 D 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。

【 0 5 0 6 】

< O W P などの認証情報を記録した N F C タグ >

紙よりも認証の高速化が期待できるのは N F C タグ 1 9 A などデジタル機器による認証である。N F C タグ 1 9 A 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、I C 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、N F C タグ 1 9 A 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 2 0 に接続できる端末と N F C 端末 1 9 A 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)。N F C タグでなくとも、財布や衣服、靴などの服飾品に O W P 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。

20

【 0 5 0 7 】

< O W P を用いたタグによる製品の真贋鑑定 >

本発明では O W P 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 O T P トークンのコントラクト識別子、製造番号と O T P 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、O W P 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 N F C タグか、製品の表面に目に見える形で取り付けられた布製・紙製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。

30

被服に N F C タグを搭載した場合、自らどのような N F C 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 N F C 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 N F C タグと比べ布などに O W P 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、無線により読み取ることがないので個人情報保護に役立つ。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 O W P 認証用情報のタグをつけることができる。

40

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ンニング、刻印、印字し、肉眼では判別

50

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。

ウェ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。

10

【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。

20

【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。

30

【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。

40

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OW

50

Pの概念を導入した。

【0512】

< B n T O T P と O W P の関連性 >

O W P 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、B n T O T P 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 B C 等をブロック番号 B n のようにブロック番号が変わるごとに変更するよう D L S 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 B n T O T P を O W P 方式でも実現できる。したがって、本発明では O W P のようにコントラクト管理者が B n T O T P の算出に用いるシード値を変更できることが好ましい。

10

D L S 上のスマートコントラクトにおいて、O W P 方式と B n T O T P 方式の考え方として、時計の秒針が自動で動く場合 (B n T O T P) と手動で動かす場合 (O W P) 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 D L S のスマートコントラクトで生成できる (D L S 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 B n T O T P と比べ O W P 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。

20

本発明では O W P 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。

O W P 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 D L S に利用されるブロック番号などのデータに着目し O W P 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 B n を追加して B n T O T P 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 D L S 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】

30

< O T P トークンのスマートコントラクト上での利用可能性 >

図 9 A にブロックチェーン型の分散型台帳システム、図 9 B に有方向非巡回 D A G 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 6 X 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 9 A の形態の他、図 9 B 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 O T P 生成関数と O T P 認証関数を用い、O T P 認証システムを提供しうる。

【0514】

< O T P トークンの利用可能性 >

本発明の B n T O T P もしくは O W P を生成する O T P 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。

40

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】

< O T P 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 N F C

50

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。

10

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。

20

【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。

30

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ログインするOTPトークンとして利用でき、ウェブサイトログインした後も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。

40

【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。

50

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。

$KCU[TIDA]$ 、 $KCU[TIDB]$ 、 $KCU[\text{トークン番号}]$ 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 $KCU[\text{トークン番号}]$ 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。

10

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 $KCU[\text{トークン番号}]$ 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。

20

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 >

30

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。

40

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 $CRHN403A$ 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

50

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O T P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O T Pトークンとして流通する。

O T P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、O T P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3 A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O T Pトークンの所有情報は保存される。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C R H N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。

10

【0520】

< O T P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O T P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。

20

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。

30

【0521】

< O T Pトークンを用いてG N S S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G N S Sなどの測位用人工衛星端末5Cから放送されたG N S S測位信号に、本発明のB n T O T P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、G N S Sの測位信号のなりすましを判断できる。

G N S S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、G N S S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B n T O T P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B n T O T P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。

40

そしてB n T O T P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B n T O T P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H M A CのM A C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】

50

このGNSS信号にBnT OTP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、BnT OTP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BnT OTP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。

10

例として電子書籍やコンピュータ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。

20

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。

30

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。

40

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

50

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。

10

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。

20

【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疑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。

30

【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。

40

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

50

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。

10

【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TKY(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。

20

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。

30

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 >

40

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

50

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。

10

【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。

20

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。

30

【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。

40

【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

50

平文のデータに $A, TIDA, B_n, B_nTOTP$ 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 $A, TIDA, B_n, B_nTOTP$ 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 B_n 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 B_nTOTP を計算して OTP の生成と認証を行う場合を考える。

$$B_nTOTP = fh(A, TIDA, KC, B_n, V)$$

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 ($A, TIDA, B_n, V$) となる。

この時、前記 B_nTOTP 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 B_n 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 B_nTOTP を取得する。そして端末 $1A$ は平文のデータに $A, TIDA, B_n, V, B_nTOTP$ 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 $A, TIDA, B_n, V, B_nTOTP$ 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 B_n 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として用いることでそのデータや文章が端末 $1A$ が B_nTOTP 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 $A, TIDA, B_n, V$ 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部の OTP 生成コントラクトにアクセスし、 $A, TIDA, B_n, V$ 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 $A, TIDA, B_n, V, B_nTOTP$ 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】

< B_nTOTP 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 >

B_nTOTP 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 $A, TIDA, B_n, B_nTOTP$ や、 $A, TIDA, B_n, V, B_nTOTP$ 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 B_n 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 B_nTOTP 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 $B_nTOTP = fh(A, TIDA, KC, B_n)$ としたとき、生成関数から取得した OTP とブロック番号 B_n 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 $A, TIDA, B_n, B_nTOTP$ 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 $A, TIDA, B_n, B_nTOTP$ の4つの情報を書き込んでもよい。

【符号の説明】

10

20

30

40

50

【 0 5 3 8 】

1 A ユーザー U A の端末となる端末 D A 、端末 1 A (電子計算機 D A 、電子計算機 1 A 。)

1 0 A 端末 1 A の記憶部 (記録装置、記録部、ROM や RAM を含む)

1 0 1 A 端末 1 A に記録されたユーザーの秘密鍵 P R V A

1 0 1 A 2 端末 1 A に記録されたユーザーの秘密鍵 P R V A 2

1 0 2 A 端末 1 A 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 1 0 1 A の秘密鍵 P R V A 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 1 0 2 A 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 、チェーン ID 等を含む) と、

アクセス先ノードとなるサーバ端末 3 A を示す U R I 情報を含むこともできる。

1 1 A 端末 1 A の制御部

1 1 0 A 端末 1 A のブロックチェーンへアクセスする制御処理部

1 2 A 端末 1 A 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)

1 2 0 A 端末 1 A の近距離無線通信 (N F C 装置)

1 2 1 A 端末 1 A の無線通信装置

1 2 2 A 端末 1 A の有線通信装置 (必要な場合)

1 2 3 A 端末 1 A の放送受信装置 (必要な場合。G N S S 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)

1 3 A 端末 1 A の制御および演算装置

1 4 A 端末 1 A の入力装置

1 4 0 A 端末 1 A キーボード

1 4 1 A 端末 1 A 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)

1 4 2 A 端末 1 A 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)

1 4 3 A 端末 1 A のマイク (音センサ)

1 4 4 A 端末 1 A 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。センサのうち種類または複数種類を用いてもよい)

1 4 4 0 A 端末 1 A 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)

1 4 4 1 A 端末 1 A 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)

1 4 4 2 A 端末 1 A のモーションセンサ (加速度計またはジャイロセンサ)

1 4 4 3 A 端末 1 A 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。)

1 5 A 端末 1 A の出力装置

1 5 0 A 端末 1 A のディスプレイ

1 5 0 0 A 端末 1 A のディスプレイに表示されたチケット、有価紙葉 1 8 A の画像、O T P 認証用情報

1 5 1 A 端末 1 A のスピーカー

1 5 2 A 端末 1 A のプリンタ (プリンター)

1 6 A 端末 1 A 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

1 6 0 0 A 端末 1 A の I C カードの読出し装置 (接触式 I C カードリーダ、非接触式 I C カードリーダ)

1 6 0 1 A 端末 1 A の接触式または非接触式の I C カード、非接触式 I C タグ

1 6 0 2 A 端末 1 A の I C に内蔵された秘密鍵 1 0 1 A 等

1 6 0 3 A 端末 1 A の無線ないし有線により D A と接続される記録装置 D W A L T

10

20

30

40

50

(外部接続型ハードウェアウォレット D W A L T、I C カード型、 dongle 型など含む)

1 6 0 4 A 端末 1 A の D W A L T 1 6 0 3 A に記録された秘密鍵 1 0 1 A、もしくは秘密鍵 1 0 1 A を含んだソフトウェア

1 6 0 5 A 端末 1 A の D W A L T 1 6 0 3 A に記録された秘密鍵処理ソフトウェア

1 6 0 6 A 端末 1 A の D W A L T 1 6 0 3 A の制御演算装置、処理装置 (D W A L T を制御する I C チップ群、M C U など)

1 6 0 7 A 端末 1 A の D W A L T 1 6 0 3 A の入出力装置、通信装置

1 6 0 8 A 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 1 0 1 A。(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。)

1 7 A 端末 1 A 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。)

1 8 A 端末 1 A のプリンタで紙などに印刷されたチケット、有価紙葉

1 8 0 A 1 8 A 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

1 8 1 A 1 8 A 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 T I D A の情報

1 8 2 A 1 8 A 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 O W P の情報

1 8 3 A 1 8 A 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

1 8 4 A 1 8 A 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。

1 9 A 有線通信型又は近距離無線通信型の I C カード、I C 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 N F T タグ、N F C カード型チケット)

1 9 0 A 1 9 A に記載の記憶装置

1 9 1 A 1 9 A に記載の制御処理装置

1 9 2 A 1 9 A に記載の通信装置

1 9 3 A 1 9 A に記載の制御演算装置

1 9 4 A 1 9 A に記載の入力装置

1 9 5 A 1 9 A に記載の出力装置

1 9 7 A 1 9 A に記載の電源装置

1 B ユーザー U B の端末 D B、端末 1 B。1 B はスマートフォン等の携帯可能な端末でもよい。端末 D B は D A 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。

1 0 B 端末 1 B の記憶装置

1 0 1 B 端末 1 B に記録されたユーザーの秘密鍵 P R V B

1 0 2 B 端末 1 B 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 1 0 1 A の秘密鍵 P R V B を用いてアクセスするためのプログラム。

ここで 1 0 2 B 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 I D、チェーン I D 等を含む) と、

アクセス先ノードとなるサーバ端末 3 A を示す U R I 情報を含むこともできる。

1 1 B 端末 1 B の制御部

1 1 0 B 端末 1 B のブロックチェーンへアクセスする制御処理部

1 2 B 端末 1 B の通信装置

1 3 B 端末 1 B 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

10

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、チェーン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

20

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）

30

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、一对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ならない。）

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）

40

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

50

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

10

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のみが変更す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に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

20

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OTPC T(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OTPC Tを用いた)

3017AG 300Aに記録されたOTPC TG(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OTPC TA(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。)

30

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)

40

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

50

関数

- 3 0 4 2 A 3 0 0 A に記録されたコントラクト管理者秘密鍵漏洩対策部分
- 3 0 1 A サーバ端末 3 A のサーバの基礎的な制御プログラム記録部
- 3 1 A サーバ端末 3 A のサーバ制御部 (サーバ P の制御装置)
- 3 1 0 A サーバ端末 3 A 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 D A G 型分散型台帳制御処理部)
- 3 1 1 A サーバ端末 3 A のサーバの基礎的な制御部
- 3 2 A サーバ端末 3 A の通信装置、通信制御装置 (サーバ P の通信装置)
- 3 3 A サーバ端末 3 A 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) 10
- 3 4 A サーバ端末 3 A の入力装置 (サーバ P の入力装置)
- 3 5 A サーバ端末 3 A の出力装置 (サーバ P の出力装置)
- 3 7 A サーバ端末 3 A 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)
- 3 B サーバ端末 3 B (サーバ端末 B)、およびサーバ端末 3 B やサーバ端末 3 A 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
- 3 0 B サーバ端末 3 B のサーバの記憶部 (記憶部はサーバ 3 A と同じ 3 0 0 A を持つ)
- 3 1 B サーバ端末 3 B のサーバの制御部 (制御部はサーバ 3 A と同じ 3 1 0 A を持つ) 20
- 3 2 B サーバ端末 3 B の通信装置
- 3 3 B サーバ端末 3 B の制御および演算装置
- 3 4 B サーバ端末 3 B の入力装置
- 3 5 B サーバ端末 3 B の出力装置
- 3 7 B サーバ端末 3 B の電源装置
- 3 C サーバ S V L o g i n、サーバ端末 3 C (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。)
- 3 0 C サーバ端末 3 C の記録部
- 3 0 0 C 端末 3 C のブロックチェーン記録部 (必要な場合。3 0 0 A と 3 0 0 C は同じ) 30
- 3 0 1 C 端末 3 C のサービス用プログラム及び記録部
- 3 0 1 0 C 端末 3 C の S V L o g i n 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)
- 3 0 1 1 C 端末 3 C 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 6 X 参照。ログイン時の時刻、ユーザー・トークン情報、I P V 値、現在のサービス状態を随時記憶し監視する。)
- 3 0 1 2 C 端末 3 C の不正アクセス検出プログラム
- 3 0 1 3 C 端末 3 C 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。)
- 3 0 1 4 C 端末 3 C の O T P C T 変化検出部 (必要な場合。O T P 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)
- 3 0 1 5 C 端末 3 C の O T P C T 変化通知部 (必要な場合。O T P 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)
- 3 0 1 6 C 端末 3 C 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。)
- 3 1 C 端末 3 C のサーバ制御部
- 3 1 0 C 端末 3 C のブロックチェーン制御部 (必須ではない。3 1 0 A と 3 1 0 C 50

は同じ)

3 1 1 C 端末 3 C のログイン及びサービス制御部

3 1 1 0 C 端末 3 C の S V L o g i n 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)

3 1 1 1 C 端末 3 C 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 6 X 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。)

3 1 1 2 C 端末 3 C 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)

3 1 1 3 C 端末 3 C 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。)

3 1 1 4 C 端末 3 C の O T P C T 変化検出部 (必要な場合。O T P 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)

3 1 1 5 C 端末 3 C の O T P C T 変化通知部 (必要な場合。O T P 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)

3 1 1 6 C 端末 3 C 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。)

3 2 C 端末 3 C の通信装置、通信制御装置

3 3 C 端末 3 C の制御および演算装置

3 4 C 端末 3 C の入力装置

3 5 C 端末 3 C の出力装置

3 7 C 端末 3 C の電源装置

3 D サーバ S V L o g 、端末 3 D (1 9 A や 1 8 A と 1 5 0 0 A を認証する端末。アクセス制御端末 3 D。3 D 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)

3 0 D 端末 3 D のサーバ記憶部 (3 0 D には O T P 認証関数と O T P 認証関数の計算に用いる変数や関数が記録される)

3 0 0 D 端末 3 D のブロックチェーン記録部 (必要な場合。3 0 0 A と 3 0 0 D は同じ)

3 0 1 D 端末 3 D のサービス用プログラム及び記録部

3 0 1 0 D 端末 3 D の S V L o g 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)

3 0 1 1 D 端末 3 D 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)

3 0 1 2 D 端末 3 D の不正アクセス検出プログラム (必要な場合。3 0 1 1 D に入場者の風貌等情報や解錠者の N F C 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)

3 0 1 3 D 端末 3 D の不正アクセス通知プログラム (必要な場合。3 D 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)

3 0 1 4 D 端末 3 D の O T P C T 変化検出部 (必要な場合。O T P 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 3 D の備えられた金庫や自動車では解錠の回数を記録する)

3 0 1 5 D 端末 3 D の O T P C T 変化通知部 (必要な場合。O T P 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。3 D 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)

3 0 1 6 D 端末 3 D 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

10

20

30

40

50

- 、利用資格のあるユーザー識別子やトークン番号を記録)
- 3 0 1 0 D A 3 0 D に記録されたハッシュ関数 f h
- 3 0 1 1 D A 3 0 D に記録されたシークレット変数 K C
- 3 0 1 2 D A 3 0 D に記録された変数 K C または変数 B C のどちらかまたは両方を変更し更新するセッター関数 f s c b (端末 3 D の管理者によりアクセスされる)
- 3 0 1 3 D A 3 0 D 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 B C
- 3 0 1 7 D A 3 0 D に記録された O T P 認証関数の実行回数又は数値記録部 (認証時の O T P 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。)
- 3 0 1 8 D A 端末 3 D の 3 0 D に記録された O T P 認証関数 (ノード 端末 3 A で生成する O T P と等しい O T P を計算できる変数と関数と処理方法を備える)
- 3 0 2 1 D A O T P 認証関数の戻り値又はデータ C T A U
- 3 0 2 2 D A 3 0 D に記録された O T P 認証時の処理内容
- 3 0 2 3 D A 3 0 D に記録された O T P 認証時の処理にて書き換える変数またはデータベース、
- 3 1 D 端末 3 D のサーバ制御部
- 3 1 0 D 端末 3 D のブロックチェーン制御部 (必須ではない。 3 1 0 A と 3 1 0 D は同じ)
- 3 1 1 D 端末 3 D のログイン及びサービス制御部
- 3 1 1 0 D 端末 3 D の S V L o g 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)
- 3 1 1 1 D 端末 3 D 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 6 X 参照。ログイン時の時刻、ユーザー情報、トークン番号、 I P V 値、現在のサービス状態を随時記憶しモニタリングする。)
- 3 1 1 2 D 端末 3 D の不正アクセス検出プログラム (必要な場合。)
- 3 1 1 3 D 端末 3 D 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ランザクションを送り異常を知らせる。)
- 3 1 1 4 D 端末 3 D の O T P C T 変化検出部 (必要な場合。 O T P 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)
- 3 1 1 5 D 端末 3 D の O T P C T 変化通知部 (必要な場合。 O T P 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)
- 3 1 1 6 D 端末 3 D 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。)
- 3 2 D 端末 3 D の通信装置、通信制御装置
- 3 3 D 端末 3 D の制御および演算装置
- 3 4 D 端末 3 D の入力装置
- 3 4 0 D 端末 3 D 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)
- 3 4 1 D 端末 3 D の N F C タグの信号受信部 (3 2 D と共有)
- 3 4 2 D 端末 3 D 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。)
- 3 5 D 端末 3 D の出力装置
- 3 5 0 D 端末 3 D 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)
- 3 5 1 D 端末 3 D 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。)
- 3 5 2 D 端末 3 D 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

10

20

30

40

50

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)

10

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

20

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

30

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。)

40

(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

50

- 3 0 1 6 F 端末 3 F のブロックチェーン検索情報データベース
- 3 1 F 端末 3 F のサーバ制御部
- 3 1 0 F 端末 3 F のブロックチェーン制御部（必要な場合。3 0 0 A と 3 1 0 F は同じ）
- 3 1 1 F 端末 3 F 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
- 3 1 1 0 F 端末 3 F の監視部
- 3 1 1 1 F 端末 3 F の状態変化検出部
- 3 1 1 2 F 端末 3 F の状態変化通知部
- 3 1 1 3 F 端末 3 F の状態変化通知先登録部
- 3 1 1 4 F 端末 3 F のブロックチェーン情報検索部 10
- 3 1 1 5 F 端末 3 F のブロックチェーン検索情報表示部
- 3 1 1 6 F 端末 3 F のブロックチェーン検索情報データベース処理部
- 3 2 F 端末 3 F の通信装置
- 3 3 F 端末 3 F の制御および演算装置
- 3 4 F 端末 3 F の入力装置
- 3 5 F 端末 3 F の出力装置
- 3 7 F 端末 3 F の電源装置
- 4 A ユーザー U P の端末となるコンピュータ D P、端末 4 A（P：プレイヤー、再生機を備えたユーザー端末）
- 4 0 A 端末 4 A の記録部（コンピュータ D P の記憶装置） 20
- 4 0 1 A 端末 4 A に記録されたユーザーの秘密鍵 P R V P（ここで P R V P は P R V A と同じくユーザー識別子 A を示す秘密鍵）
- 4 0 2 A 端末 4 A 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 3 A へアクセスする U R I などが記録されていてもよい）
- 4 0 3 A 端末 4 A の記録部 4 0 A 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 C R H N の情報、ソフトウェア C R H N のプログラムと関連データ。
- 4 0 3 0 A 端末 4 A の 4 0 3 A のソフトウェア C R H N 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。4 0 3 0 A に含まれる変数も難読化または暗号化されている） 30
- （ブロックチェーンのノード端末 3 A へアクセスする U R I などが 4 0 3 0 A 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）
- 4 0 3 0 1 A 4 0 3 A 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 A P K Y
- 4 0 3 0 2 A 4 0 3 A に記載の内蔵した秘密鍵 C R K Y（ブロックチェーン部 D L S にアクセスできる公開鍵暗号の秘密鍵でもよい。4 0 3 0 2 A は 4 0 3 0 A に内蔵され難読化または暗号化されている） 40
- 4 0 3 0 3 A 4 0 3 A 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 C A P K Y（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）
- 4 0 3 0 3 K A 4 0 3 A に記載のソフトウェア内部のシークレット変数 K 4 0 3（K 4 0 3 は難読化または暗号化されている）
- 4 0 3 1 A ブロックチェーンから取得した O T P 認証関数の戻り値 C T A U の端末 4 A における記憶部（C T A U は認証関数の戻り値の管理者により変更されうる）
- 4 0 3 2 A ブロックチェーンおよびソフトウェア C R H N 4 0 3 A の外部で設定されるパスワード A K T B の端末 4 A 内の記憶部（A K T B は平文データ管理者により変更 50

されうる)

4 0 3 3 A 4 0 3 A に記載の暗号化及び復号に用いる鍵情報 T T K Y の記憶部 (少なくとも C T A U を含み、そして A K T B を用い、さらに C R K Y を用い算出される鍵情報。)

4 0 3 4 A 4 0 3 A に用いるソフトウェア C R H N で復号する暗号されたデータまたはファイル E n c D a t a (4 0 3 4 A は 4 0 A に含まれていればよい。)

4 0 3 4 0 A 4 0 3 4 A の暗号化データ本体 E t D a t a

4 0 3 4 1 A 4 0 3 4 A の平文データ発行者の暗号化データ 4 0 3 4 A に対して付与した電子証明書 E n c C e r t (電子署名も含まれていてよい。 M A C 値が含まれていてもよい。無くともよい。)

10

4 0 3 5 A 4 0 3 A に用いるソフトウェア C R H N で暗号化したい平文のデータまたはファイル D e c D a t a (4 0 3 5 A は 4 0 A に含まれていればよい。 D e c D a t a はアクセス制御される。)

4 0 3 5 0 A 4 0 3 5 A の平文データ本体 C t D a t a

4 0 3 5 1 A 4 0 3 5 A の平文データ発行者の電子証明書 D e c C e r t (電子署名も含まれていてよい。無くともよい。)

4 0 3 5 2 A 4 0 3 5 A の平文データ監査証明書 A u d i t R a t (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ーティング。あることが好ましい)

4 0 3 6 A 4 0 A に記録された閲覧済みの証明書データ O F B K M K (O T P 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。 4 0 3 6 A は 4 0 A に含まれていればよい。)

20

4 0 3 6 0 A 4 0 3 6 A に記録された C T T K Y を C R H N のプログラムに内蔵した秘密鍵 C R K Y 等で暗号化した A C T T K Y

4 0 3 6 1 A 4 0 3 6 A に記録された T T K Y を秘密鍵 P R V A で暗号化したデータ C T T K Y (4 0 3 6 A 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。)

4 0 3 6 2 A 4 0 3 6 A 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

4 0 3 6 3 A 4 0 3 6 A に記録された H M A C など認証用情報

4 0 3 6 2 K A 4 0 A に記録された証明書の本文データ C H T 4 0 3

30

4 0 3 6 3 K A 4 0 A に記録された 4 0 3 6 2 K A をメッセージとした H M A C など認証用情報

4 0 4 A 4 0 A に記録されたソフトウェア C R H N 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

4 0 5 A 4 0 A に記録されたコンピュータ D P 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)

4 1 A 端末 4 A の制御部

4 1 0 A 端末 4 A のブロックチェーンへアクセスする制御処理部

4 1 1 A 端末 4 A のソフトウェア C R H N の制御処理部

4 2 A 端末 4 A の通信装置

40

4 2 0 A 通信装置 4 2 A の近接無線通信装置 (必要な場合)

4 2 1 A 通信装置 4 2 A の無線通信装置

4 2 2 A 通信装置 4 2 A の有線通信装置 (必要な場合)

4 2 3 A 通信装置 4 2 A の放送受信装置 (必要な場合。時刻取得のため N I T Z 、 J J Y 、時刻及び位置情報測位用の G N S S の受信機、暗号化データ放送受信装置を含む。)

4 3 A 端末 4 A の制御および演算装置

4 4 A 端末 4 A の入力装置

4 4 0 A 端末 4 A のキーボード

4 4 1 A 端末 4 A 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

50

-)
- 4 4 2 A 端末 4 A のカメラもしくはスキャナ
- 4 4 3 A 端末 4 A のマイク
- 4 4 4 A 端末 4 A 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)
- 4 4 4 0 A 端末 4 A 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)
- 4 4 4 1 A 端末 4 A 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)
-)
- 4 4 4 2 A 端末 4 A のモーションセンサ (加速度計またはジャイロセンサ) 10
- 4 4 4 3 A 端末 4 A 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)
- 4 5 A 端末 4 A の出力装置
- 4 5 0 A 端末 4 A のディスプレイ (暗号化された動画データを表示する)
- 4 5 1 A 端末 4 A 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)
- 4 5 2 A 端末 4 A 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。)
- 4 5 3 A 端末 4 A のヘッドマウントディスプレイ (H M D、頭部装着ディスプレイ 20。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)
- 4 5 3 0 A 端末 4 A の H M D に付属の生体認証センサ。
- 4 5 3 0 A 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
- 4 5 3 0 A は 4 4 4 3 A に記載のセンサと機能を共有していてもよい。
- (ここで 4 5 3 0 A のセンサは 4 5 3 A 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。) 30
- (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 H M D 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 H M D 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。)
- (4 5 3 0 A 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。)
- (H M D 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 5 A 等のサービス用サーバに通知されることがある。) 40
- 4 6 A 端末 4 A 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。)
- 4 7 A 端末 4 A の電源装置
- 5 A 端末 5 A のサーバ S V C R H N c m (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)
- 5 0 A 端末 5 A のサーバ記録部
- 5 0 0 A 端末 5 A の S V C R H N c m 動作プログラム (ソフトウェア C R H N に指 50

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に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に対応付けた情報。

アクセス者情報はハッシュ化などされて個人情報保護を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CRHN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CRHN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

10

20

30

40

50

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。)

5 0 2 B 端末 5 B 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)

5 0 3 B 端末 5 B 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)

5 0 4 B 端末 5 B の鍵情報 A K T B 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 S M S サービスと連携してもよい。鍵通知は端末 5 B の外で行ってもよい)

10

5 0 5 B 端末 5 B の A K T B により暗号化されたファイルの U R I 等配信先の通知部 (A K T B を鍵の 1 つとして利用して生成した鍵 T T K Y で暗号化されたファイルの U R I を通知するメール通知部)

5 0 6 B 端末 5 B 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 O T P 生成トークン共に販売する際に利用。決済機能と連携)

5 0 7 B 端末 5 B の O T P 生成及び認証用の O T P トークン発行部 (必要な場合。5 0 6 B の決済の完了を確認しデータの復号を行える O T P トークンを発行するプログラム。端末 1 C に発行指示)

20

5 0 8 B 端末 5 B 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 6 X と同じ。)

5 0 9 B 端末 5 B 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 O T P トークンの売買をする際に 5 B に搭載する事が好ましい。)

5 0 0 0 B 端末 5 B の任意のブロックチェーン記憶部 (必要な場合。3 0 0 A と 5 0 0 0 B は同じ)

5 1 B 端末 5 B のサーバ制御部

5 1 0 B 端末 5 B のサービス制御部 (プログラム 5 0 0 B、5 0 1 B、5 0 2 B、5 0 3 B、5 0 4 B、5 0 5 B、5 0 6 B、5 0 7 B、5 0 8 B、5 0 9 B に従い制御する部分)

30

5 1 0 0 B 端末 5 B の任意のブロックチェーン制御部 (必要な場合。3 1 0 A と 5 1 0 0 B は同じ)

5 2 B 端末 5 B の通信装置

5 3 B 端末 5 B の制御および演算装置

5 3 B 端末 5 B の入力装置

5 4 B 端末 5 B の出力装置

5 7 B 端末 5 B の電源装置

5 C 放送局となるサーバ S V C R H N b r o a d c a s t e r、端末 5 C、放送局
端末 5 C

40

5 0 C 端末 5 C のサーバ記録部

5 0 1 C 端末 5 C のブロックチェーンアクセス用秘密鍵

5 0 2 C 端末 5 C の秘密鍵 5 0 1 C 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

5 0 3 C 端末 5 C の放送用ソフトウェア (ソフトウェア 4 0 3 A を含んでもよい。G N S S による測位情報を放送するソフトウェアを含んでもよい。)

5 0 0 0 C 端末 5 C の任意のブロックチェーンの記憶部 (必要な場合。3 0 0 A と 5 0 0 0 C は同じ。特に人工衛星型端末 5 C では 5 0 0 0 C を備えてもよい。)

5 0 3 4 C 端末 5 C の放送する暗号化データ (5 0 3 5 C を 4 0 3 A で復号できる

50

鍵 T T K Y で暗号化し放送するデータ)

5 0 3 5 C 端末 5 C 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 5 0 C に保持してもよい。)

5 1 C 端末 5 C のサーバ制御部

5 1 0 C 端末 5 C の制御部

5 1 0 0 C 端末 5 C 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。3 1 0 A と 5 1 0 0 C は同じ)

5 2 C 端末 5 C の通信装置

5 2 0 C 端末 5 C の放送用無線装置

10

5 2 1 C 端末 5 C の無線通信装置 (5 C を制御する端末 5 C との連絡用)

5 2 2 C 端末 5 C の有線通信装置 (必要な場合。端末 5 C が地上局の際には利用される。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。)

5 2 0 0 C 端末 5 C の放送用空中線

5 2 1 C 端末 5 C 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。)

5 3 C 端末 5 C の制御および演算装置

5 3 C 端末 5 C の入力装置

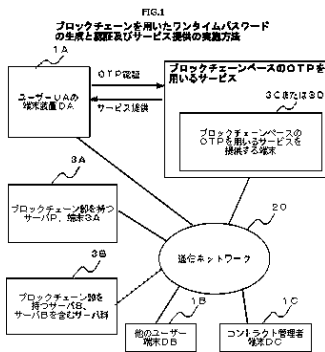
5 4 C 端末 5 C の出力装置

20

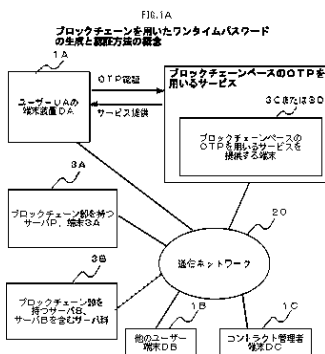
5 7 C 端末 5 C の電源装置 (人工衛星の場合は二次電池や太陽電池を含む)、

5 C C 端末 5 C 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 5 C が人工衛星局の時、5 C C は地上局で 5 C は 5 C C と通信し 5 C C 経由でネットワーク 2 0 に接続される。)

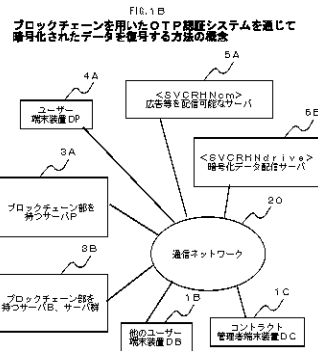
【図 1】



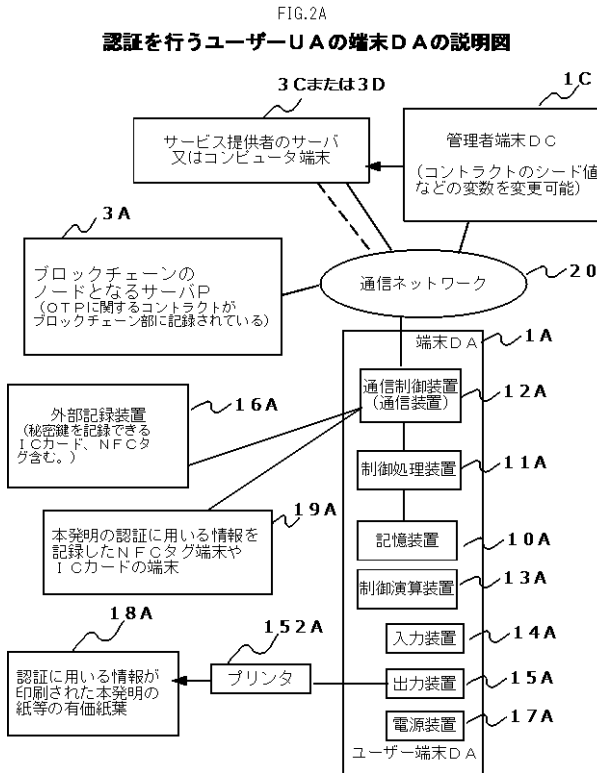
【図 1 A】



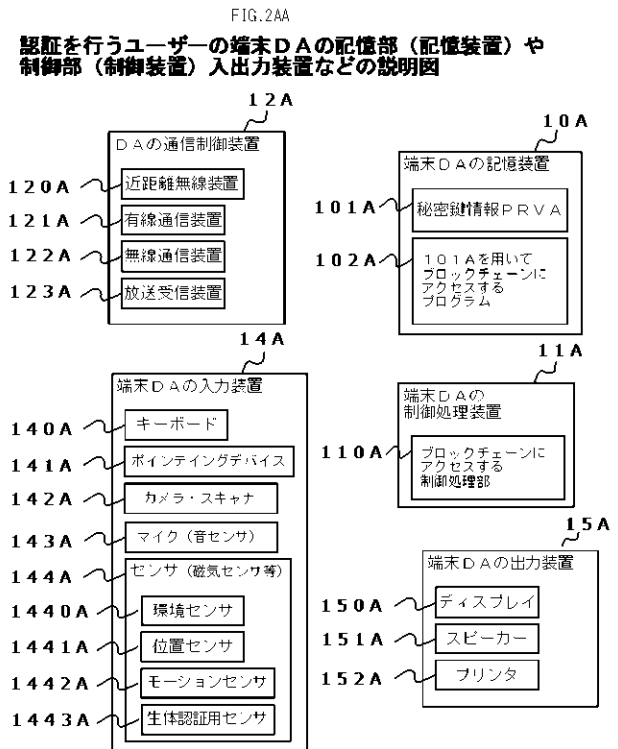
【図 1 B】



【図 2 A】

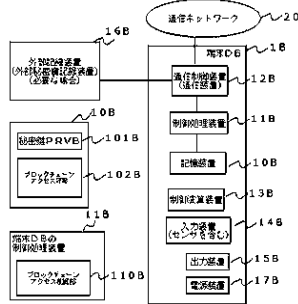


【図 2 A A】



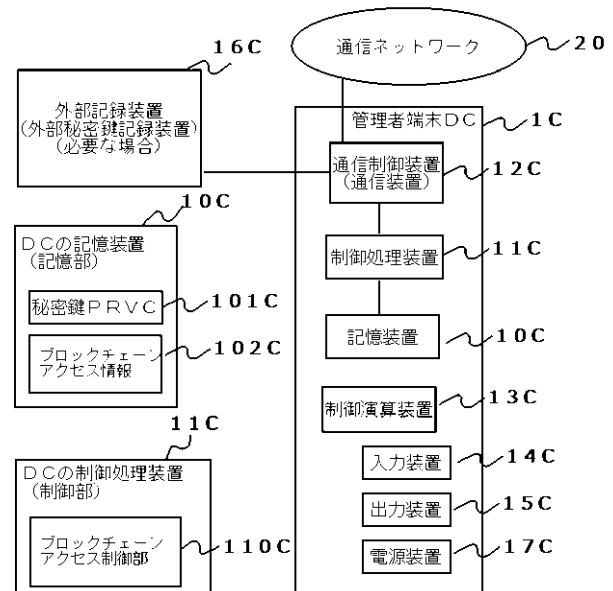
【図 2 B】

FIG. 2B
ユーザーUBの端末DBの説明図
端末DAと端末DBの機能は同等で秘密鍵が異なる



【図 2 C】

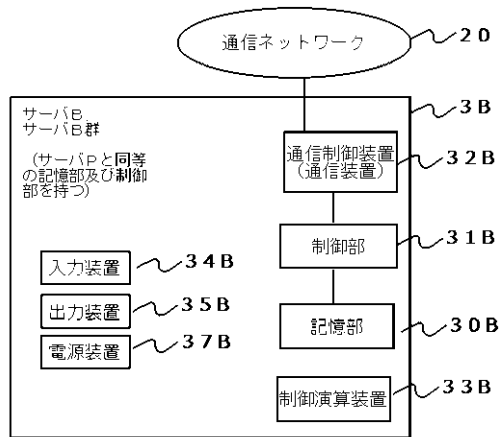
FIG.2C
ブロックチェーン部にコントラクトをデプロイし管理するユーザーUCの端末DCの説明図。端末DAと端末DCの機能は同等で秘密鍵が異なる。



【図 3 B】

FIG.3B

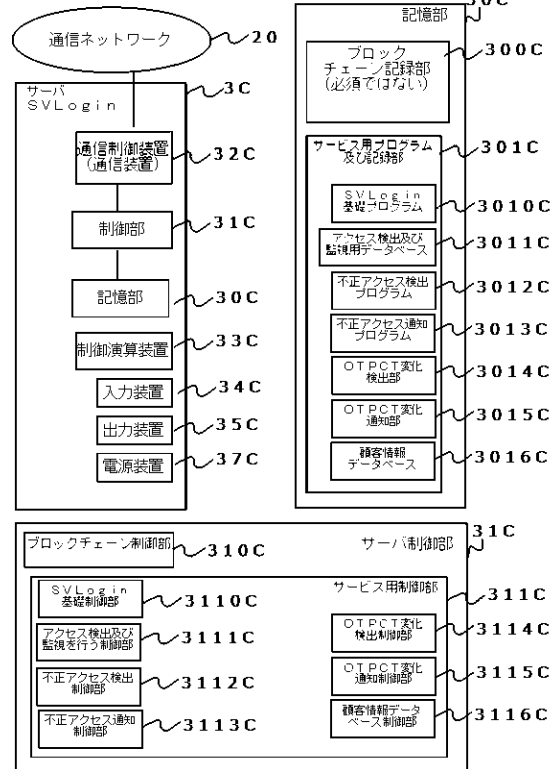
サーバP (3A) と同じブロックチェーン部を持ちネットワーク20上で分散台帳システムDL Sを構成するノードとなる端末3Bの説明図



【図 3 C】

FIG.3C

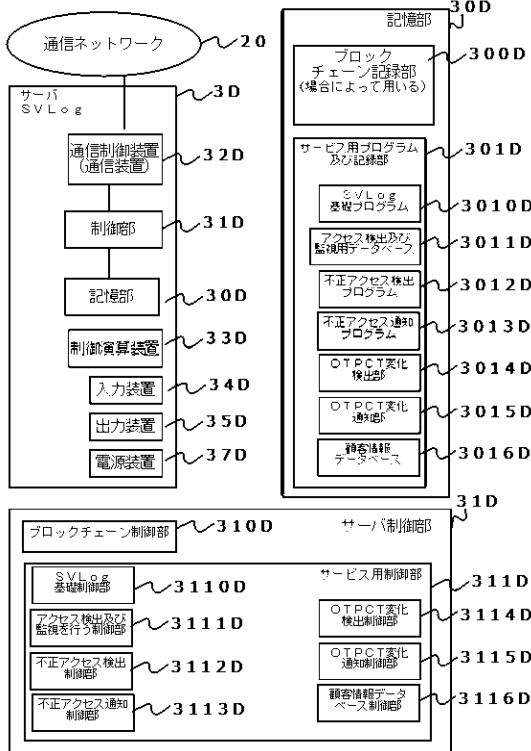
ウェブサイト (ウェブページ、ウェブアプリ) へのログイン等で認証を行う場合のサーバ端末3Cの説明図



【図 3 D】

FIG.3D

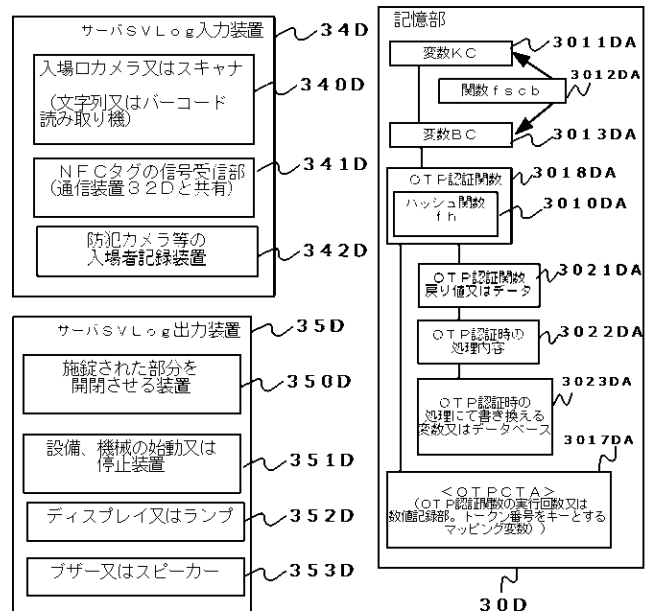
印刷物や表示画面及びNFCタグに記録された本発明の認証情報を読み取り認証を行いサービスを行うサーバ端末3Dの説明図



【図 3 D A】

FIG.3DA

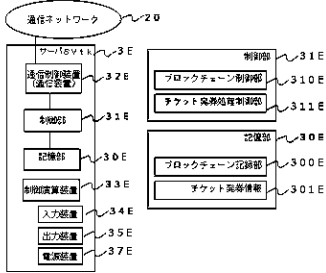
サーバSVLog (端末3D) の記憶部と入出力装置 (34D、35D) に関する説明図



【 図 3 E 】

FIG. 3E

OTPトークンの購入または紙及びRFIDタグに対しOTP認証情報を出力し、有価証券を発行するサービスを行うサーバ側SEの説明図



【 図 3 F 】

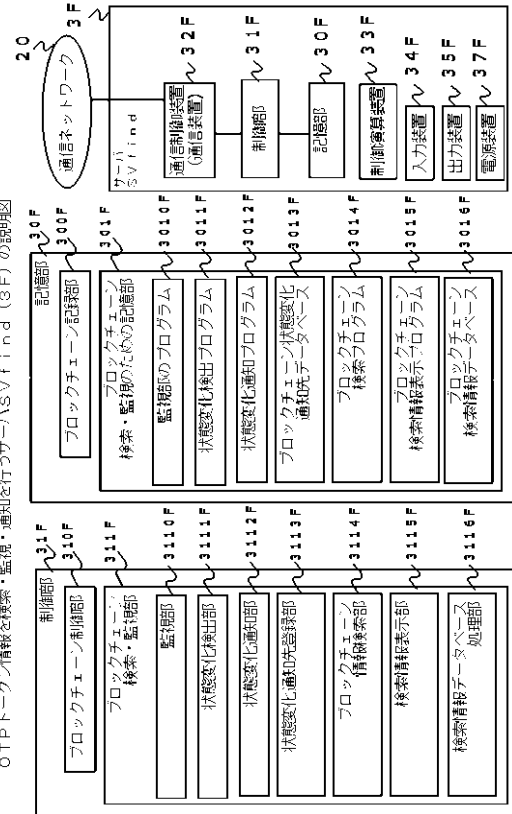


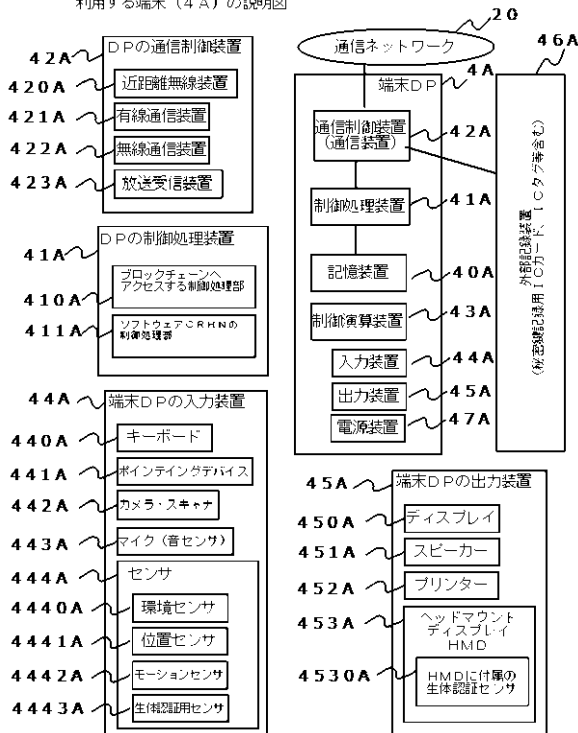
FIG. 3F

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OTTPトークン情報を検索・監視・通知を行うサーバSvfind (3F) の説明図

【 図 4 A 】

FIG.4A

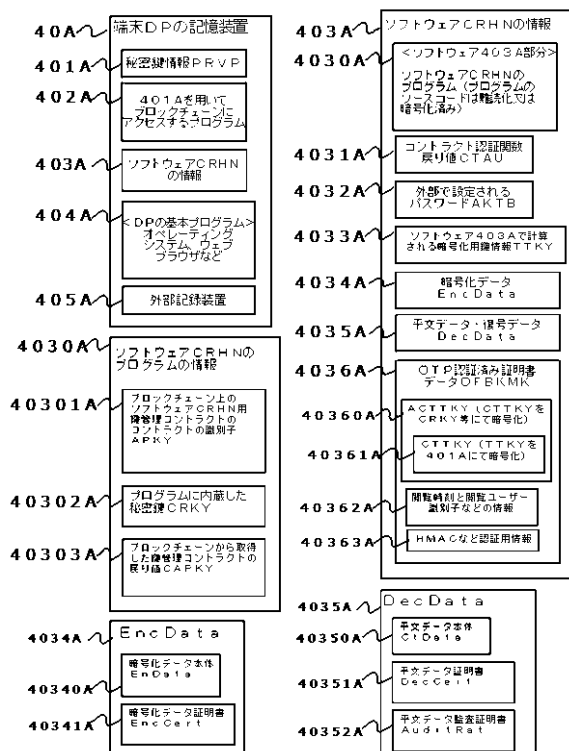
認証システムを用いて暗号化データを復号し閲覧視聴または
利用する端末（４Ａ）の説明図



【 図 4 B 】

FIG.4B

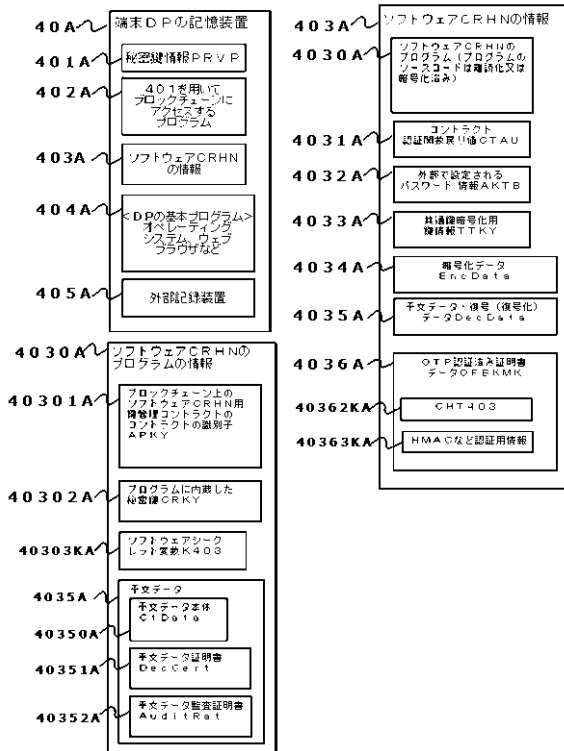
認証システムを用いて暗号化データを復号し閲覧視聴または利用する
端末（４Ａ）の記憶装置に関する説明図



【図 4 C】

FIG. 4C

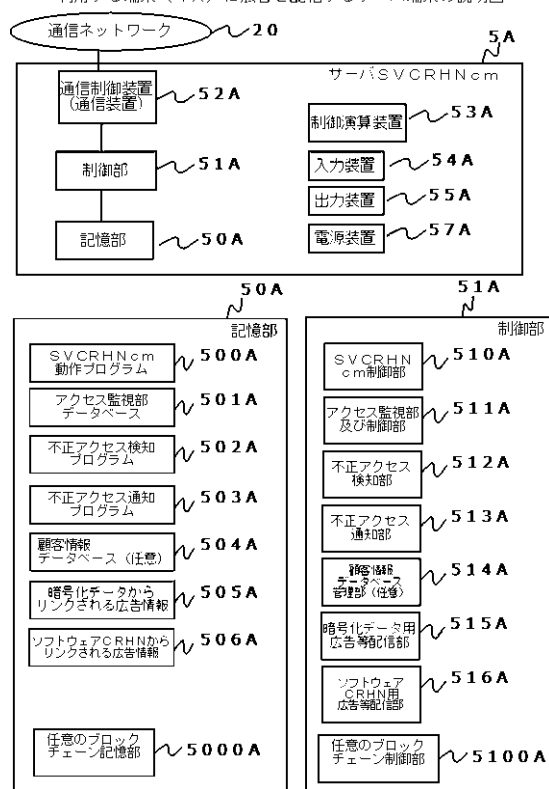
図 4 B において端末 4 A の記憶装置に平文データが暗号化もしくは難読化されてソフトウェア 4 0 3 A の 4 0 3 0 A に内蔵されるとき説明図



【図 5 A】

FIG. 5A

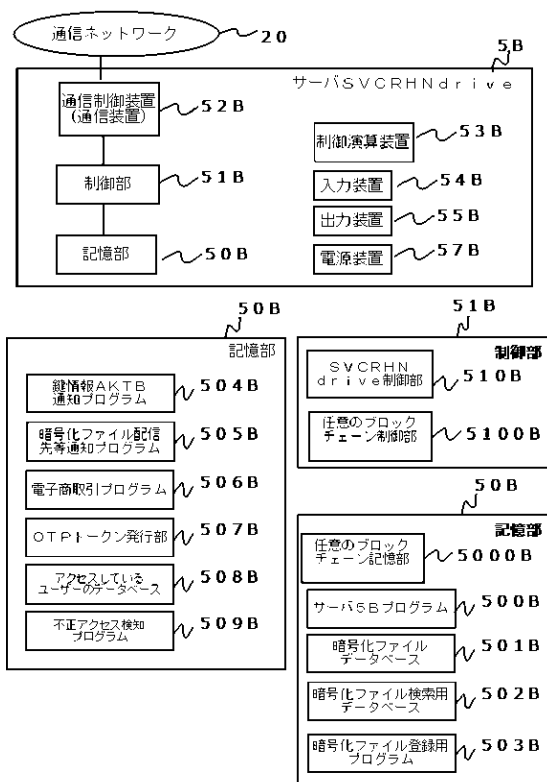
認証システムを用いて暗号化データを復号し閲覧視聴または利用する端末 (4 A) に広告を配信するサーバ端末の説明図



【図 5 B】

FIG. 5B

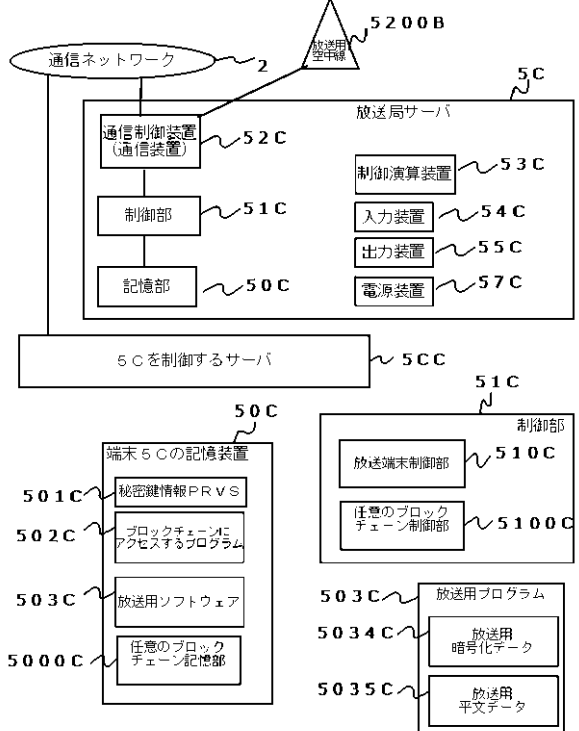
端末 (4 A) に暗号化データをネットワークを通じて配信するサーバ端末 5 B の説明図



【図 5 C】

FIG. 5C

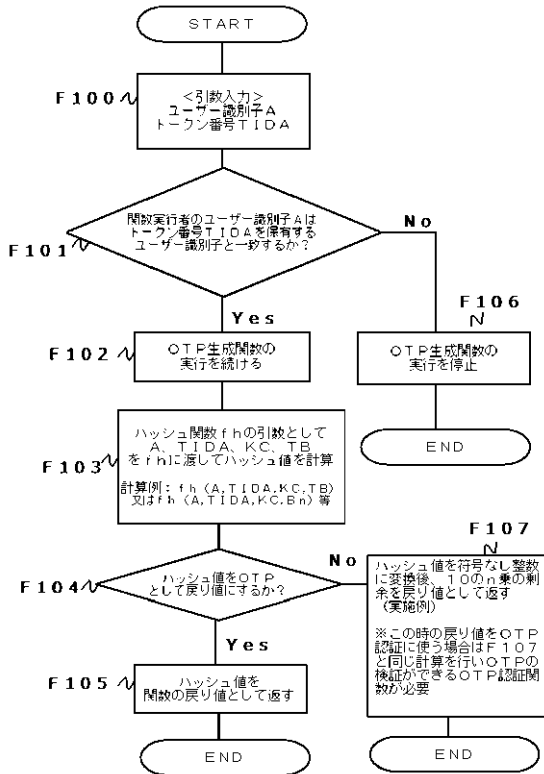
端末 (4 A) に暗号化データを放送によって送付するサーバ端末 5 C の説明図



【図 6 A】

FIG.6A

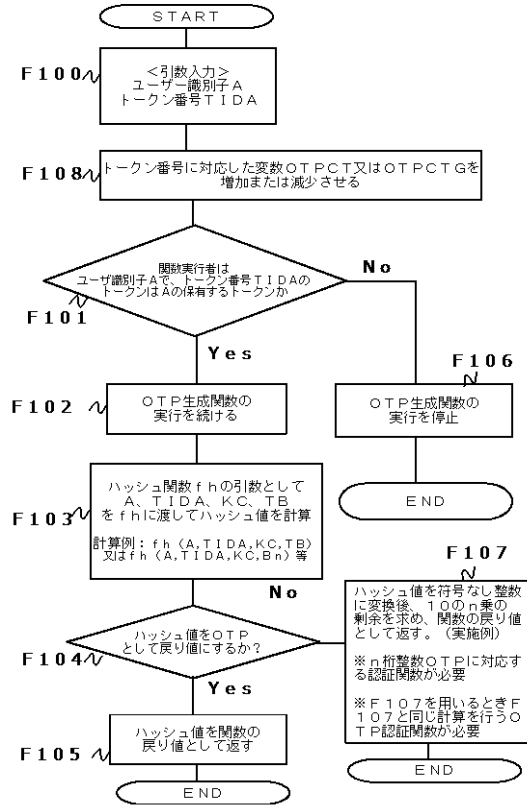
OTPを生成する関数の処理を示したフローチャート図



【図 6 B】

FIG.6B

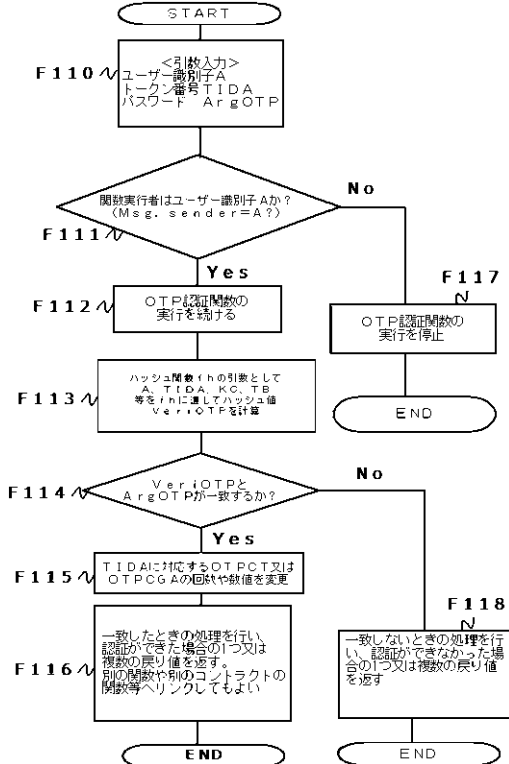
OTP生成回数記録機能を備えたOTPを生成する関数の処理を示したフローチャート図



【図 6 C】

FIG.6C

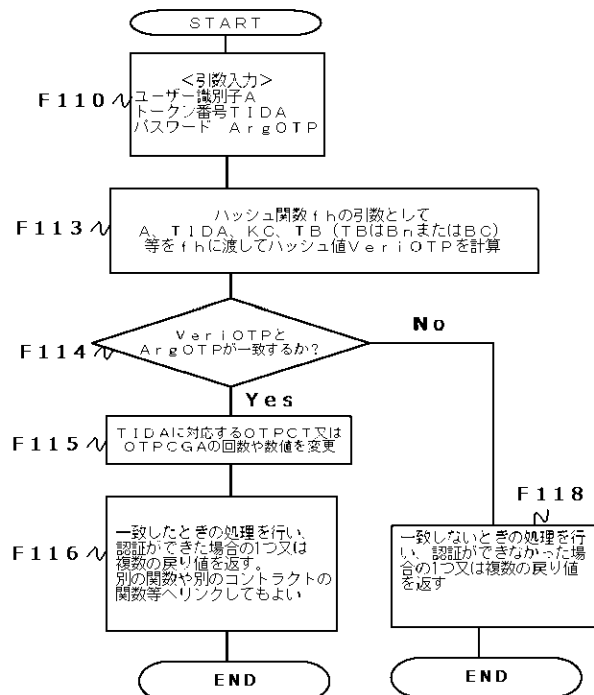
OTP認証回数等記録機能を備えた認証するアクセス者をトークン保有者のユーザー識別子に限定する場合のOTPを認証する関数のフローチャート図



【図 6 D】

FIG.6D

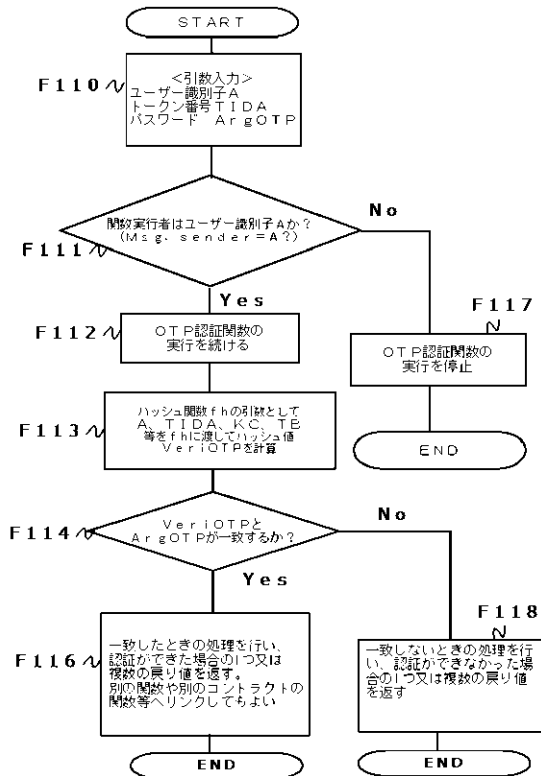
OTP認証回数等記録機能を備えた認証するアクセス者を限定しない場合のOTPを認証する関数のフローチャート図



【図 6 E】

FIG.6E

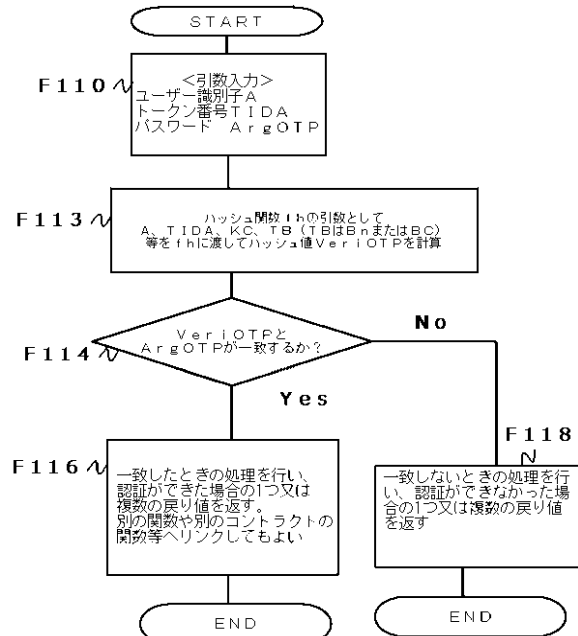
図 6 C から OTP 認証回数等記録機能を除いた場合の OTP を認証する関数のフローチャート図



【図 6 F】

FIG.6F

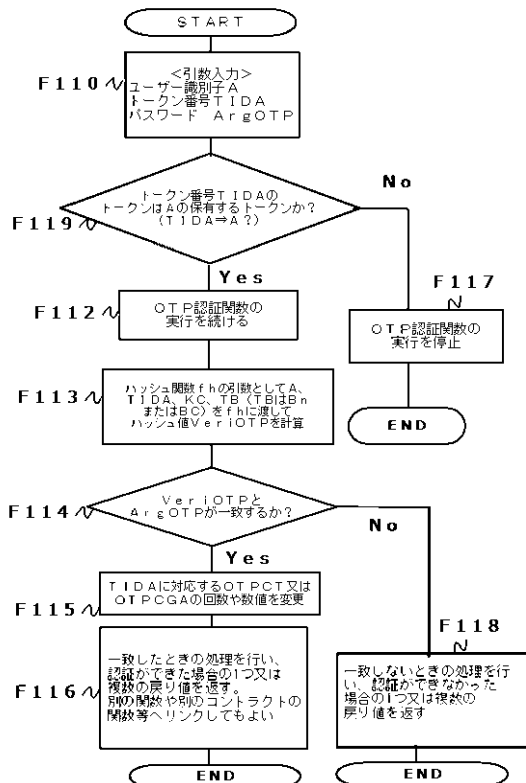
認証するアクセス者を限定しない場合の OTP を認証する関数のフローチャート図



【図 6 G】

FIG.6G

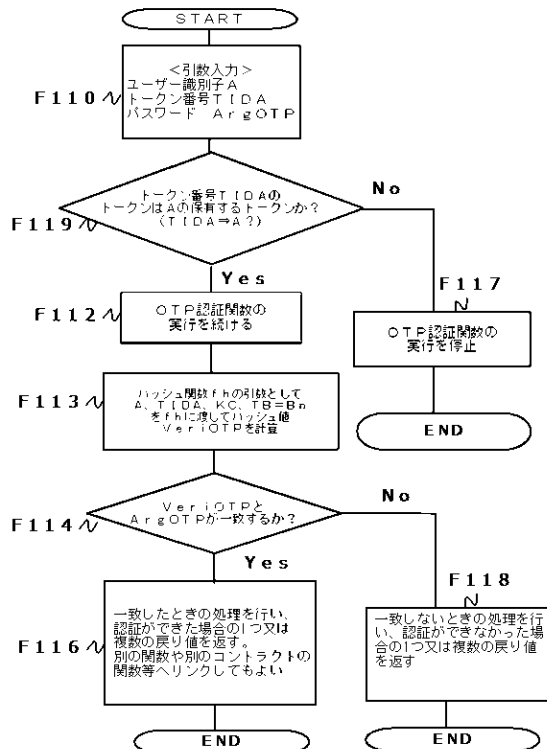
OTP 認証回数等記録機能を備えた OTP トークンの保有者のアクセスが判断して認証する関数の処理を示したフローチャート図



【図 6 H】

FIG.6H

OTP トークンの保有者のアクセスが判断して OTP を認証する関数の処理を示したフローチャート図



【図 6 X】

FIG. 6X

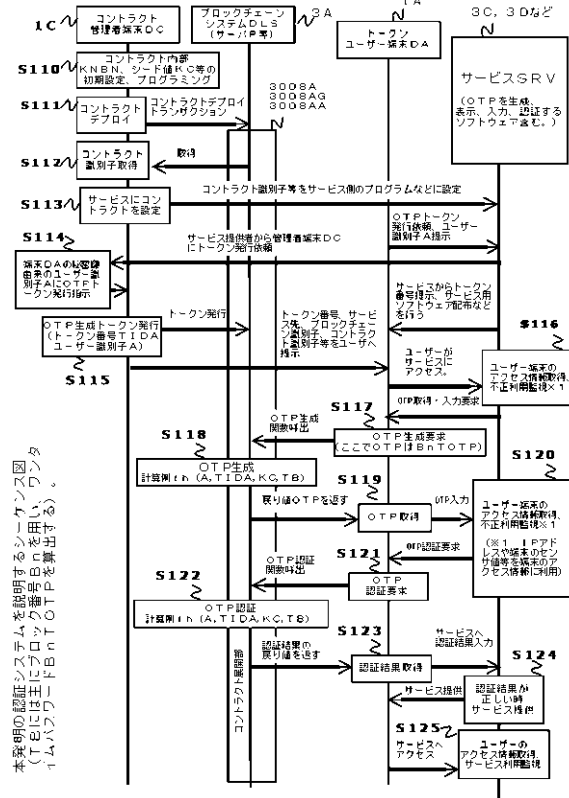
本発明の認証システムを利用するサービスを行うサーバ端末（3C、3D、3E、3F、5A、5B）にユーザ端末（DAなど）がアクセスした際に記録されるデータ構造

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？	履歴情報（ログイン履歴、アクセル回数等のログイン履歴データ）
		IPアドレス	位置情報	端末センサ値 ※1		
0x714009083C ※4※5	12345	111.11.11.1	東経111°北緯45°	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0x1100FF...
0x71400908D0	12346	121.11.11.2	非開示	非開示	正常	2020年11月11日11時11分ログイン、回数1234、状態0x1100FF...
0x71400908EE	54321	131.11.11.3	西経111°南緯51°	ID: A123BC, X=156, Y=345, Z=568	異常検知 ※2	2020年12月12日13時12分ログイン、回数1010、状態0x506011...
0x71400909EE	54321	131.11.11.3	西経111°南緯51°	ID: A123BC, X=156, Y=345, Z=123	異常検知 ※2	2020年12月12日13時12分ログイン、回数1010、状態0x506011...
0x71400908FF	12347	非開示	非開示	非開示	正常	2020年12月12日22時22分ログイン、回数1010、状態0x1100FF...
...

※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：同じユーザ識別子のアクセラ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：ログイン履歴データは一例、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。

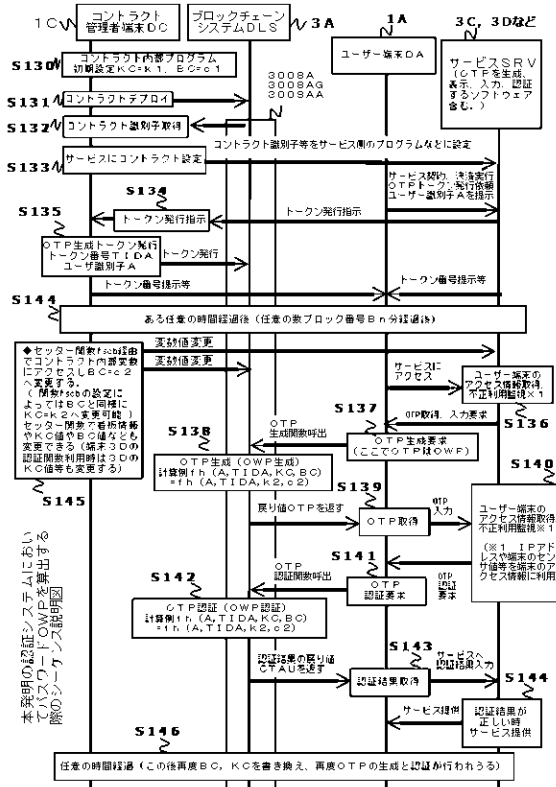
【図 7 A】

FIG. 7A



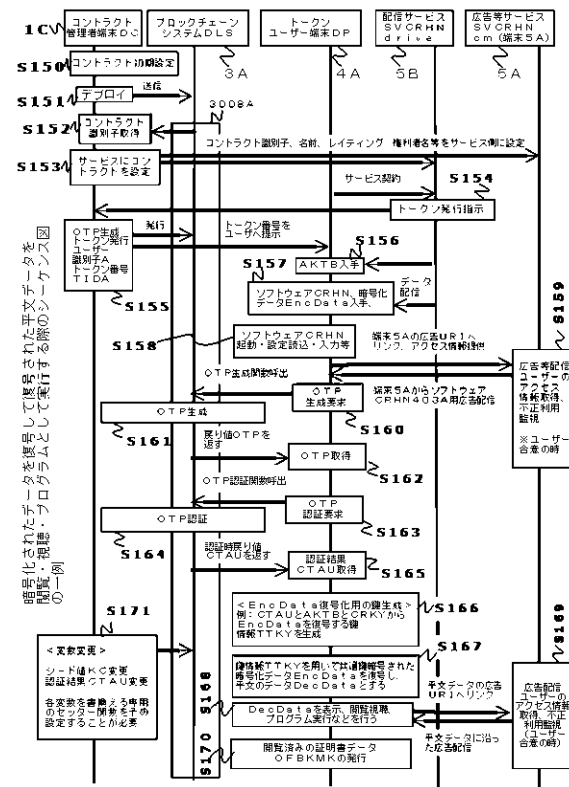
【図 7 B】

FIG. 7B

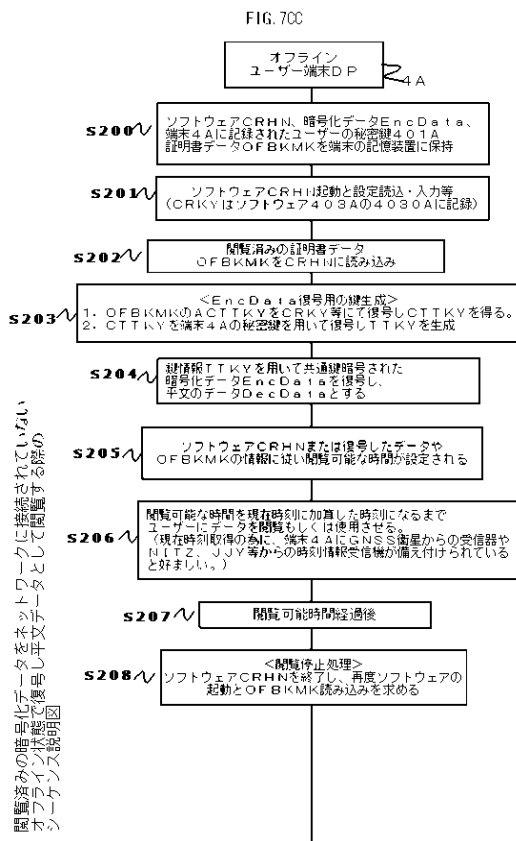
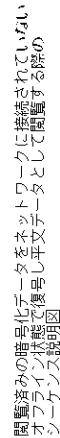


【図 7 C A】

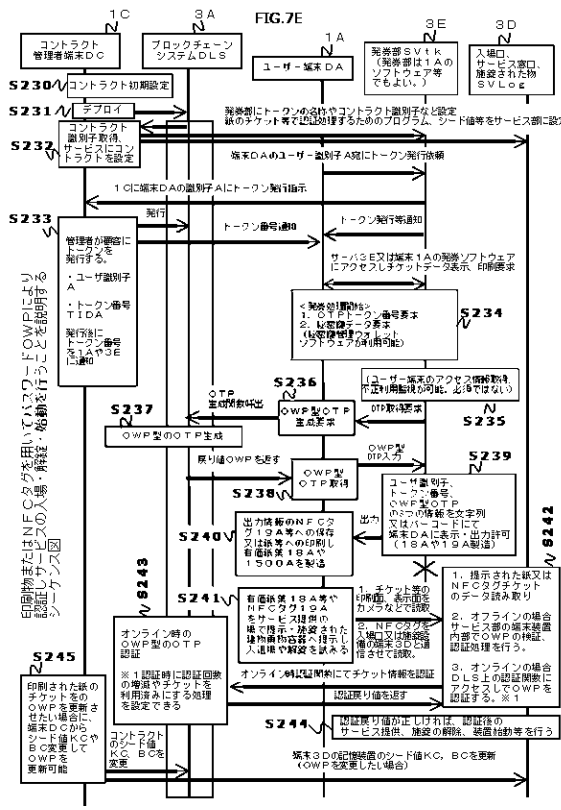
FIG. 7CA



【 図 7 C C 】



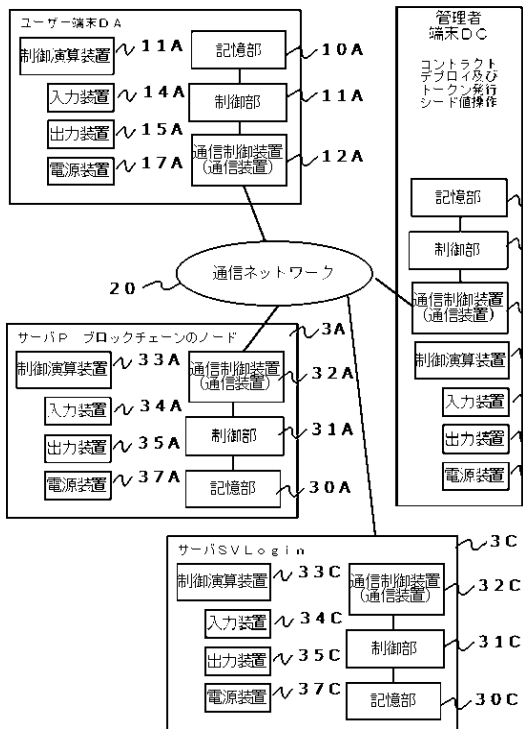
【図 7 E】



【図 8 A】

FIG. 8A

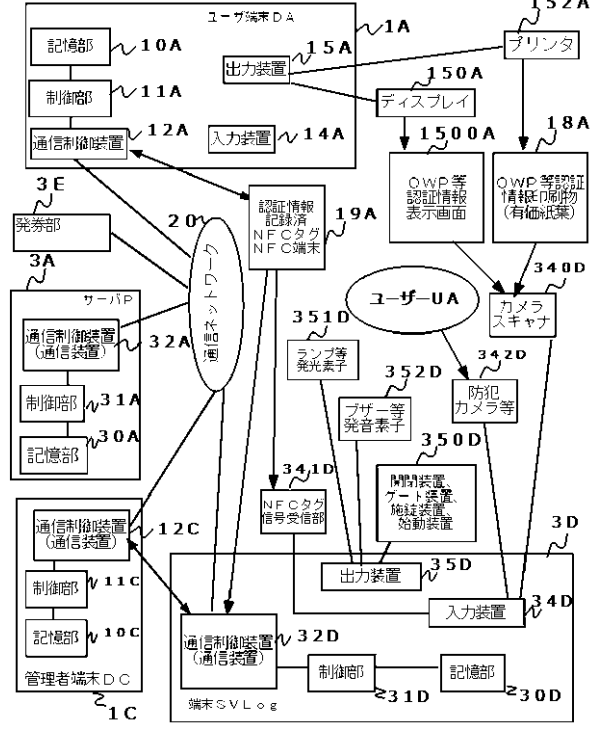
ウェブサイトログイン時の端末の接続



【図 8 B】

FIG. 8B

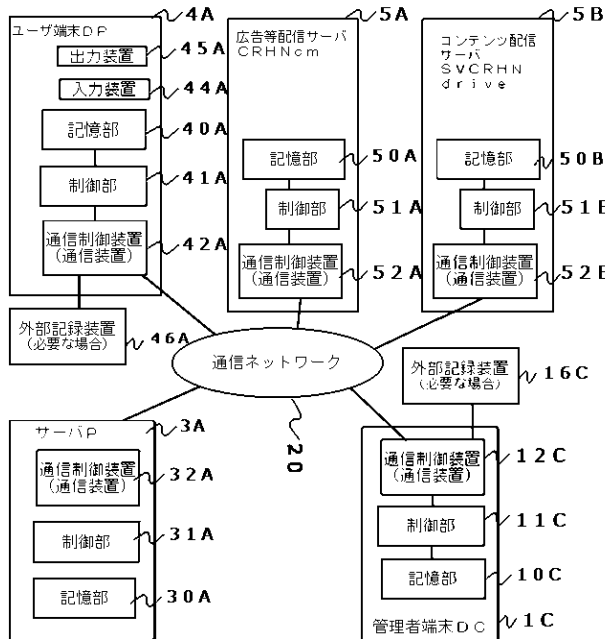
印刷物及びNFCタグによる有価紙葉または鍵利用時の端末の接続



【図 8 C】

FIG. 8C

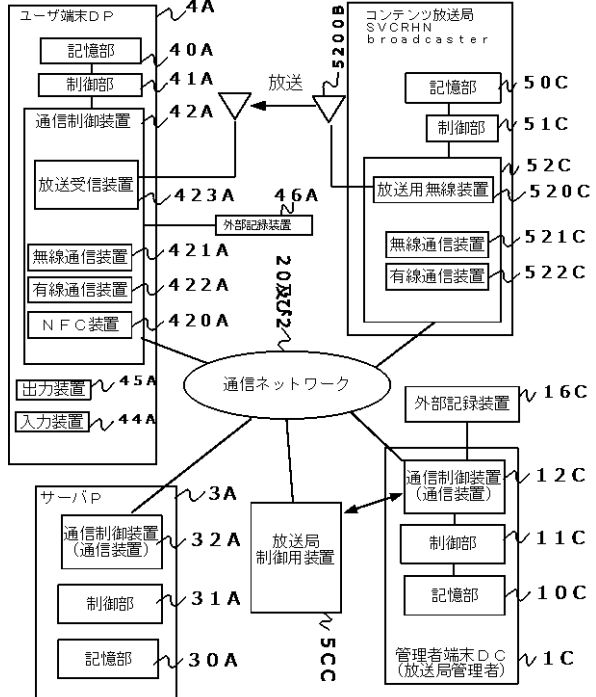
通信ネットワークを通じて暗号化データを配信（配布）する場合においてソフトウェアCRHN（403A）を利用する端末の接続



【図 8 D】

FIG. 8D

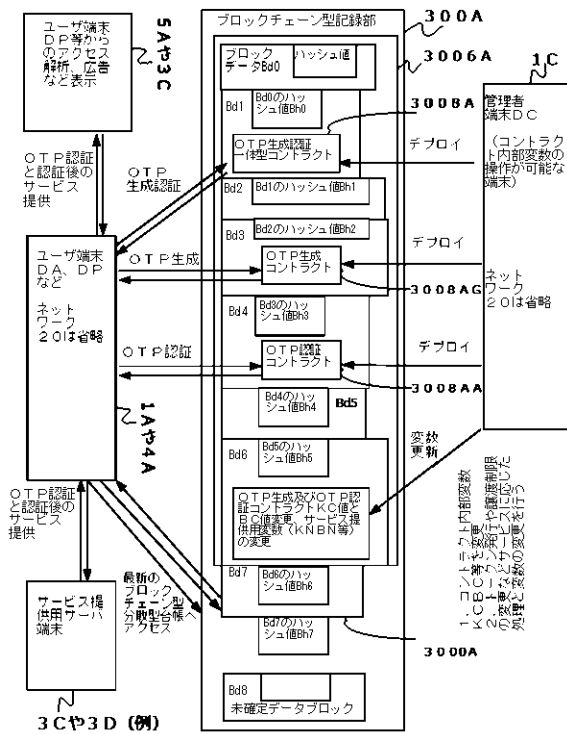
データ放送により暗号化データを放送する場合においてソフトウェアCRHN（403A）を利用する端末の接続



【図 9 A】

FIG. 9A

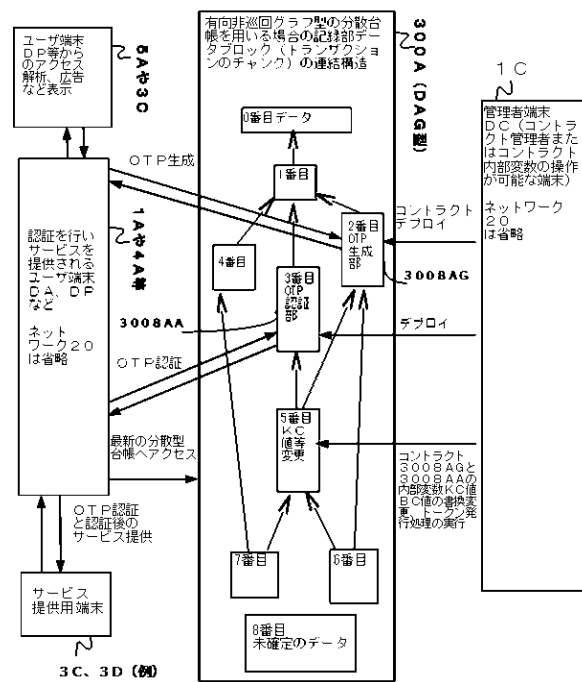
分散型台帳システムDLSにブロックチェーン型のデータ構造を用いたOTPトークンによる認証システムの概要を説明する図



【図 9 B】

FIG. 9B

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



【手続補正書】

【提出日】令和4年3月6日(2022.3.6)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

或る時刻において変化可能な変数TBを用いる動的なパスワードVPをワンタイムパスワードまたはOTPとして計算または生成するOTP生成関数またはOTP生成部またはVP生成部を備えたスマートコントラクトを備える分散型台帳システムのノードとなる端末3Aと、

ユーザ端末1Aを、前記ネットワーク20を介して接続させたコンピュータネットワークシステムにおいて、

前記パスワードVPの認証を行う前記OTP認証関数またはOTP認証部またはVP認証部を、OTP認証端末またはサービス提供端末3D、または前記ノードとなる端末3A若しくは他の前記ノード端末3Bのスマートコントラクト部に備え、

前記OTP認証関数またはOTP認証部は、前記スマートコントラクトの前記OTP生成関数またはOTP生成部にて計算される前記OTPと同じまたは等しいOTPを計算する処理部を備えており、

前記ユーザ端末1Aが前記OTP生成関数またはOTP生成部より前記OTPを生成又は取得し、前記OTPを前記OTP認証関数またはOTP認証部に入力することによりOTP認証を行うコンピュータネットワークシステムであって、

前記OTP生成関数またはOTP生成部と前記OTP認証関数またはOTP認証部のパス

ワードVPの計算をハッシュ関数fhを用いて行う場合に、
 前記ハッシュ関数fhの引数にトークン番号TIDAと、
 前記OTP生成関数またはOTP生成部と前記OTP認証関数またはOTP認証部を備える端末に記憶された変数KCと、
 ある時刻において変更される変数TBと、
 ユーザー端末の秘密鍵もしくはシードとなる情報から計算されるユーザー識別子Aのうち3つ以上の変数を基にして、
 前記ハッシュ関数fhの引数に利用するキー値もしくはシード値として備えハッシュ値を計算し前記OTPの算出に用いるコンピュータネットワークシステム。

【請求項2】

10

セッターとなる関数または変数変更手段と、
 前記関数または前記変数変更手段を用い任意の時刻またはブロック番号において書き換えることの出来る変数KC、
またはOTPの計算に用いるハッシュ関数、
またはOTPの計算に用いる変数または関数を、
 前記OTP生成関数またはOTP生成部を備える端末と、前記OTP認証関数またはOTP認証部を備える端末に備え、
 任意の時刻またはブロック番号Bnにおいて、
 前記変数KCまたは、
またはOTPの計算に用いるハッシュ関数、
またはOTPの計算に用いる変数または関数を、
 前記変数変更手段または前記関数を用いて変更または更新することによって、変更または更新された前記パスワードVPを生成しOTP認証または動的パスワード認証を行う、
 請求項1に記載のコンピュータネットワークシステム。

20

【請求項3】

前記分散型台帳システムはブロックチェーンを用い、
 前記パスワードVPの計算を行う時に前記OTP生成関数またはOTP生成部と前記OTP認証関数またはOTP認証部の前記ハッシュ関数fhの引数に前記ブロックチェーンの最新のブロック番号BnまたはブロックナンバーBnを前記変数TBの代わりに用い、
 時間が変化することによって前記ブロックチェーンの前記ブロック番号Bnが変化することにより前記動的なパスワードVPを生成しOTP認証を行う請求項1に記載のコンピュータネットワークシステム。

30

【請求項4】

前記パスワードVPの計算に用いる変数に前記変数KC、
またはOTPの計算に用いるハッシュ関数、
またはOTPの計算に用いる変数または関数、
 を備え、
 前記関数または前記変数変更手段を用いて前記変数KC
OTPの計算に用いる変数または関数を1つ以上書換えることができる、
 前記動的なパスワードVPを生成しOTP認証を行う
 請求項3に記載のコンピュータネットワークシステム。

40

【請求項5】

前記変数TBまたは前記ブロック番号Bnを前記パスワードVPの計算に用いる場合について、
 整数の変数Mを前記OTP生成関数を備える端末と前記OTP認証関数を備える端末に備え、
 前記変数Bnもしくは前記変数TBを変数Mで割った剰余r、
 すなわち $r = Bn \bmod M$ を計算し、
 前記Bnまたは前記変数TBからrを減算することで算出される値Bnrを前記TBまたは前記Bnの代わりに用いパスワードVPを計算する、
 請求項1から請求項4の何れかに記載のコンピュータネットワークシステム。

50

【請求項 6】

前記OTP生成関数を備える端末と前記OTP認証関数を備える端末に整数Yと、1以上の整数Nを備え、

前記パスワードVPを符号なし整数型に変換した値mを被除数mとし、
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を整数値のパスワードVPrとして用いる

請求項 1 から請求項 5 の何れかに記載のコンピュータネットワークシステム。

【請求項 7】

前記パスワードVPの生成と認証を行うOTP生成関数またはOTP生成部、またはOTP認証関数またはOTP認証部の関数実行時に用いる変数として、

前記OTP生成関数の実行回数もしくは前記OTP認証関数の実行回数を記録するトークン番号を検索のキーとする変数、

又は前記OTP生成関数の実行回数もしくは前記OTP認証関数の実行回数、

又は前記OTP生成関数もしくは前記OTP認証関数の関数実行により変化する変数を前記スマートコントラクトまたはOTP認証端末またはサービス提供端末に備え、

前記OTP生成関数またはOTP生成部、

もしくは前記OTP認証関数またはOTP認証部のいずれか、

もしくは両方について前記関数が実行されるたびに前記実行回数を記録する変数の値を増加もしくは減少させる処理を行うことの出来る制御部と記憶部を備えた、

請求項 1 から請求項 6 の何れかに記載のコンピュータネットワークシステム。

【請求項 8】

前記OTP認証関数またはOTP認証部を実行できる前記ユーザー識別子を限定する処理部を備える、

請求項 1 から請求項 7 の何れかに記載のコンピュータネットワークシステム。

【請求項 9】

前記分散型台帳システムを構成するノード間で、データブロックを連結する際にブロックチェーンまたは分散型台帳システムを構成するノード間で利用される変数をノード間の投票または合意により決定する際に前記投票または合意により決定した変数Vを、

前記パスワードVPを計算するシード値に用い、前記パスワードVPを計算する、

請求項 1 から請求項 8 の何れかに記載のコンピュータネットワークシステム。

【請求項 10】

前記変数Vはブロックチェーンのデータブロックのデータサイズである変数BSZ、またはBlockGasLimitである

請求項 9 に記載のコンピュータネットワークシステム。

【請求項 11】

トークン送信関数tfを備えるスマートコントラクトにおいて、

前記関数tfを実行する際に必要な変数または関数実行の認否を決定する変数を備え、

前記関数tfを実行する際に必要な前記変数はセッターとなる関数または変数変更手段より変更され、

前記関数tfを実行する際に必要な前記変数の値によって前記送信関数tfの実行は制御され、

異なるユーザー識別子間で前記OTPトークンの送信と譲渡を前記管理者が停止または制御できる機能を持つ前記スマートコントラクトを用いることを特徴とする、

請求項 1 から請求項 10 の何れかに記載のコンピュータネットワークシステム。

【請求項 12】

前記OTP生成関数またはOTP生成部を備えた前記OTPトークンのスマートコントラクトから前記OTPを計算して生成し前記ユーザー端末の記憶装置に取得し、

前記記憶装置に記憶され取得された前記OTPと前記ユーザー識別子または前記トークン番号またはその両方を、

ログインサービスを提供するサービス提供端末が提供するウェブサービスプログラムに含まれる前記OTP認証関数またはOTP認証部、
もしくは前記ウェブサービスプログラムからアクセス又は参照できるスマートコントラクトに含まれる前記OTP認証関数またはOTP認証部へ入力し、
前記OTP認証関数またはOTP認証部を実行し、OTP認証を行う、
請求項1から請求項11の何れかに記載のコンピュータネットワークシステム。

【請求項13】

前記ユーザ識別子A、前記トークン番号TIDA、前記パスワードVPを、文字列または二次元バーコードとして紙等あるいはユーザ端末のディスプレイといった記録手段に記録または表示させ、

10

あるいは認証用データである前記ユーザ識別子Aと前記トークン番号TIDAと前記パスワードVPの情報を、ユーザの所持する磁気ストライプカードまたはICカード端末やNFC端末またはNFCカードまたはNFCタグ、またはスマートフォン端末もしくはウェアラブルコンピュータ端末を含む前記ユーザ端末といったデータとして記憶または記録する記録手段に記憶または記録させて、

前記記録手段を作成または作製または生成または製造し、

前記記録手段が紙等あるいはユーザ端末のディスプレイといった記録手段または有価紙葉の形態で用いられる場合には、前記記録手段に記録された変数を、サービスを提供するサービス提供端末の備えるカメラもしくはスキャナを用いて読み取り、前記OTP認証関数を含む前記スマートコントラクトもしくは前記サービス提供端末の前記OTP認証関数またはOTP認証部の引数に入力し、前記OTP認証関数またはOTP認証部を実行させ、
前記OTP認証関数またはOTP認証部の前記戻り値CTAUを得て、ユーザに対しサービス提供を行うコンピュータネットワークシステムであり、

20

前記記録手段が前記データとして記憶または記録する記録手段の場合には、前記サービス提供端末を用いて前記記録手段に記録された認証用データとして読み取り、前記サービス提供端末に備えられた前記OTP認証関数またはOTP認証部の引数に入力し、前記OTP認証関数またはOTP認証部を実行させ、前記OTP認証関数またはOTP認証部の戻り値CTAUを得て、ユーザに対しサービス提供を行う、

請求項1から請求項11の何れかに記載のコンピュータネットワークシステム。

【請求項14】

30

前記OTP認証関数またはOTP認証部から得られる前記戻り値CTAUを暗号化データを復号するための鍵情報に用いて暗号化されたデータを復号するソフトウェアCRHNをユーザ端末に備える請求項1から請求項11の何れかに記載のコンピュータネットワークシステム。

【請求項15】

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UAの秘密鍵に基づくユーザ識別子Aと前記トークン番号TIDAまたはその両方と、

前記ユーザ端末のIPアドレスまたは位置情報または端末識別子または端末センサ値、

40

もしくは前記IPアドレスまたは前記位置情報または前記端末識別子または前記端末センサ値のハッシュ値、

もしくは前記IPアドレスまたは前記位置情報または前記端末識別子または前記端末センサ値の何れかを直接もしくは仮名化または匿名化して含む値IPV、

もしくは前記IPアドレスまたは前記位置情報または前記端末識別子または前記端末センサ値の何れかを直接もしくは仮名化または匿名化して含む値IPVのハッシュ値を、

前記ユーザ端末より前記サービス提供端末に収集し記録させ、

同一のユーザ識別子Aもしくはトークン番号TIDAもしくはその両方に対し、異なる前記IPアドレスまたは前記位置情報または前記端末識別子または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もしくは前記値IPVのハッシュ値からのアクセスが

50

行われたか否かを検出する処理部または制御部と記憶部をサービス提供端末に備える、
請求項 1 から請求項 1 1 および請求項 1 2 と請求項 1 4 の何れかに記載のコンピュータネ
ットワークシステム。

【請求項 1 6】

前記パスワード V P を含む前記 O T P 認証関数またはOTP認証部の引数となる認証情報を

紙面または有価紙葉や N F C タグ端末といった記録手段に記録させ物のタグまたはデータ

のタグとして添付又は貼付又は記録し、
もしくは物の表面に添付して、前記物のタグに記録されたパスワード V P を前記 O T P 認
証関数またはOTP認証部に入力し認証する請求項 1 から請求項 1 1 の何れかに記載のコン
ピュータネットワークシステム。

10

【請求項 1 7】

パスワード V P を含む前記 O T P 認証関数またはOTP認証部の引数となる認証情報を、デ
ータ通信端末または配信端末および放送局端末の放送データ又は配信データ又は送信する
データに添付し、前記放送データ又は配信データ又は送信するデータに添付されたパsw
ード V P を前記 O T P 認証関数またはOTP認証部に入力し認証し、

または、

前記パスワード V P の取得時の前記変数 T B またはブロック番号 B n と前記パスワード V P
を含む前記 O T P 認証関数またはOTP認証部の引数となる認証情報を、物のタグまたはデ
ータのタグとして添付又は貼付又は記録し、

20

前記タグに記録された前記パスワード V P と、前記パスワード V P の取得時の前記変数 T B
または前記ブロック番号 B n を前記 O T P 認証関数またはOTP認証部へ入力し認証する、
請求項 1 から請求項 1 1 の何れかに記載のコンピュータネットワークシステム。

【請求項 1 8】

前記放送データが全球測位衛星システム衛星端末より放送される測位用信号または測位用
データである請求項 1 7 に記載のコンピュータネットワークシステム。

【請求項 1 9】

トークン番号 T I D A の前記 O T P トークンを付与されたユーザ識別子 A のユーザが設定または書
換または変更出来るシード値 V U [T I D A] を前記パスワード V P の前記ハッシュ関数
f h の引数に利用する、

30

請求項 1 から請求項 1 8 の何れかに記載のコンピュータネットワークシステム。

フロントページの続き

特許法第30条第2項適用申請有り 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項適用申請有り 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.etherscan.io/address/0x0f398803BE4319B98F164cae47589797aC5cF906>、<https://rinkeby.etherscan.io/address/0x0f398803BE4319B98F164cae47589797aC5cF906>。