(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2025-66236
(P2025-66236A)
(43)公開日　令和7年4月23日(2025.4.23)

(51)Int.Cl.			FI			テーマコード（参考）
H04L	9/08	(2006.01)	H04L	9/08	A	
H04L	9/32	(2006.01)	H04L	9/32	200Z	

審査請求 有　請求項の数 9　ＯＬ　（全 15 頁）

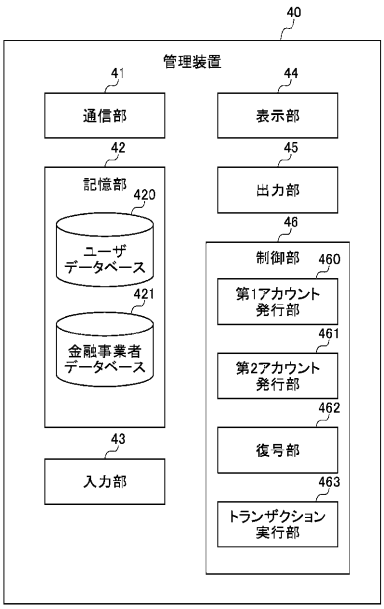
(21)出願番号　特願2023-175671(P2023-175671)
(22)出願日　令和5年10月11日(2023.10.11)

(71)出願人　514020389
ＴＩＳ株式会社
東京都新宿区西新宿八丁目１７番１号
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦
(74)代理人　100134120
弁理士　内藤　和彦
(72)発明者　藤田　匡彦
東京都新宿区西新宿８－１７－１　ＴＩＳ株式会社内

最終頁に続く

(54)【発明の名称】情報処理システム、情報処理方法、プログラム

(57)【要約】
【課題】より適切に秘密鍵を管理することが可能な情報処理システムを提供する。
【解決手段】情報処理システム１０は、記憶部４２と、トランザクション実行部４６３とを備える。記憶部４２には、セキュリティトークンのトランザクションを実行するための事業者用秘密鍵が暗号化された状態で記憶されている。トランザクション実行部４６３は、暗号化された事業者用秘密鍵を記憶部４２から読み込むとともに、暗号化された事業者用秘密鍵を復号して、復号化された事業者用秘密鍵を用いてブロックチェーン上でセキュリティトークンのトランザクションを実行する。
【選択図】図２



【特許請求の範囲】
【請求項１】
セキュリティトークンのトランザクションを実行するための第１秘密鍵が暗号化された状態で記憶される記憶部と、
取引者のログイン操作に基づいて、前記取引者のアカウントに対応した前記暗号化された第１秘密鍵を前記記憶部から読み込むとともに、前記暗号化された第１秘密鍵を復号して、復号化された第１秘密鍵を用いてブロックチェーン上で前記セキュリティトークンのトランザクションを実行するトランザクション実行部と、を備える
情報処理システム。
【請求項２】
前記記憶部には、前記第１秘密鍵を暗号化する際に用いられた第２秘密鍵が暗号化された状態で更に記憶されており、
前記第２秘密鍵を復号可能な復号部を更に備え、
前記トランザクション実行部は、前記取引者のログイン操作に基づいて、前記暗号化された第２秘密鍵を前記記憶部から読み込むとともに、前記暗号化された第２秘密鍵を前記復号部により復号して、復号化された第２秘密鍵を用いて、前記暗号化された第１秘密鍵を復号する
請求項１に記載の情報処理システム。
【請求項３】
前記取引者に対して前記セキュリティトークンの取り引きを依頼するユーザに対応したウォレットアドレス、及び前記ウォレットアドレスに対応した第３秘密鍵を発行する発行部と、
前記発行部により発行された前記第３秘密鍵を、当該第３秘密鍵の情報が残らないように出力する出力部と、を更に備える
請求項１に記載の情報処理システム。
【請求項４】
前記出力部は、前記第３秘密鍵の情報が残らないように、前記第３秘密鍵が印字された紙媒体を印刷して出力、又は前記第３秘密鍵を表示部に表示する
請求項３に記載の情報処理システム。
【請求項５】
前記記憶部には、前記ユーザのウォレットアドレスが前記ユーザの識別番号と関連付けられて更に記憶されている
請求項３に記載の情報処理システム。
【請求項６】
前記第３秘密鍵の情報をインターネットに接続されていない状態で保管可能な保管部を更に備える
請求項３に記載の情報処理システム。
【請求項７】
前記保管部は、前記第３秘密鍵が印字された紙媒体、又は前記第３秘密鍵が電子データとして記憶された記憶媒体を保管する
請求項６に記載の情報処理システム。
【請求項８】
セキュリティトークンのトランザクションを実行するための第１秘密鍵が暗号化された状態で記憶部に記憶されており、
コンピュータが、
取引者のログイン操作に基づいて、前記取引者のアカウントに対応した前記暗号化された第１秘密鍵を前記記憶部から読み込むとともに、前記暗号化された第１秘密鍵を復号して、復号化された第１秘密鍵を用いてブロックチェーン上で前記セキュリティトークンのトランザクションを実行する
情報処理方法。

【請求項９】
セキュリティトークンのトランザクションを実行するための第１秘密鍵が暗号化された状態で記憶部に記憶されており、
コンピュータに、
取引者のログイン操作に基づいて、前記取引者のアカウントに対応した前記暗号化された第１秘密鍵を前記記憶部から読み込ませるとともに、前記暗号化された第１秘密鍵を復号して、復号化された第１秘密鍵を用いてブロックチェーン上で前記セキュリティトークンのトランザクションを実行させる
プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理システム、情報処理方法、及びプログラムに関する。
【背景技術】
【０００２】
下記の特許文献１に記載のシステムは、株式や債券等の有価証券をデジタル化したセキュリティトークンをブロックチェーン上で発行する。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０２１－１２４６０号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
特許文献１に記載のシステムでは、セキュリティトークンに関するトランザクションを実行するための秘密鍵の管理に関して改善の余地がある。
本発明は、こうした実情に鑑みてなされたものであり、その目的は、より適切に秘密鍵を管理することが可能な情報処理システム、情報処理方法、及びプログラムを提供することにある。
【課題を解決するための手段】
【０００５】
上記課題を解決する情報処理システムは、記憶部と、トランザクション実行部と、を備える。記憶部には、セキュリティトークンのトランザクションを実行するための第１秘密鍵が暗号化された状態で記憶される。トランザクション実行部は、取引者のログイン操作に基づいて、取引者のアカウントに対応した暗号化された第１秘密鍵を記憶部から読み込むとともに、暗号化された第１秘密鍵を復号して、復号化された第１秘密鍵を用いてブロックチェーン上でセキュリティトークンのトランザクションを実行する。
【０００６】
上記課題を解決する情報処理方法では、セキュリティトークンのトランザクションを実行するための第１秘密鍵が暗号化された状態で記憶部に記憶されており、コンピュータが、取引者のログイン操作に基づいて、取引者のアカウントに対応した暗号化された第１秘密鍵を記憶部から読み込むとともに、暗号化された第１秘密鍵を復号して、復号化された第１秘密鍵を用いてブロックチェーン上でセキュリティトークンのトランザクションを実行する。
【０００７】
上記課題を解決するプログラムでは、セキュリティトークンのトランザクションを実行するための第１秘密鍵が暗号化された状態で記憶部に記憶されており、コンピュータに、取引者のログイン操作に基づいて、取引者のアカウントに対応した暗号化された第１秘密鍵を記憶部から読み込ませるとともに、暗号化された第１秘密鍵を復号して、復号化された第１秘密鍵を用いてブロックチェーン上でセキュリティトークンのトランザクションを

実行させる。
【０００８】
この構成によれば、取引者のログイン操作に基づいて第１秘密鍵が記憶部から読み込まれるため、取引者自身で第１秘密鍵を管理する必要がない。また、第１秘密鍵は記憶部において暗号化された状態で記憶されている。よって、より適切に第１秘密鍵を管理することが可能となる。
【発明の効果】
【０００９】
本発明の情報処理システム、情報処理方法、及びプログラムによれば、より適切に秘密鍵を管理することが可能である。
【図面の簡単な説明】
【００１０】
【図１】実施形態の情報処理システムの概略構成を示すブロック図。
【図２】実施形態の管理装置の概略構成を示すブロック図。
【図３】（Ａ），（Ｂ）は、実施形態のユーザデータベース及び金融事業者データベースにそれぞれ記憶されているデータの一例を示す図表。
【図４】実施形態のトランザクション実行部の動作例を示すシーケンスチャート。
【図５】実施形態の情報処理システムの動作例を示すシーケンスチャート。
【図６】実施形態の情報処理システムの動作例を示すシーケンスチャート。
【図７】実施形態のコンピュータのハードウェア的な構成を示すブロック図。
【発明を実施するための形態】
【００１１】
以下、添付図面を参照して、本発明の情報処理システム、情報処理方法、及びプログラムの好適な実施形態（以下、「本実施形態」という）について説明する。なお、各図において、同一の符号を付したものは、同一又は同様の構成を有する。本実施形態において、「部」や「手段」、「装置」、「システム」とは、単に物理的手段を意味するものではなく、その「部」や「手段」、「装置」、「システム」が有する機能をソフトウェアによって実現する場合も含む。また、一つの「部」や「手段」、「装置」、「システム」が有する機能が２つ以上の物理的手段や装置により実現されてもよく、二つ以上の「部」や「手段」、「装置」、「システム」の機能が１つの物理的手段や装置により実現されてもよい。
【００１２】
＜実施形態＞
はじめに、本実施形態の情報処理システムの概要について説明する。
（情報処理システムの概要）
図１に示される本実施形態の情報処理システム１０は、取引者の秘密鍵を用いてブロックチェーン上でセキュリティトークンの発行を行うとともに、秘密鍵の管理を行うシステムである。
【００１３】
セキュリティトークンとは、有価証券等に基づく金融商品をデジタル化したものであって、電子情報処理組織を用いて移転することができる財産的価値に表示されるものをいう（「金融商品取引業等に関する内閣府令」第１条第４項第１７号等）。セキュリティトークンの適用対象は、例えば株式、社債、金銭債権等が含まれる。
【００１４】
取引者は、セキュリティトークンの取り引きを行う者である。取引者は、例えばユーザ、金融事業者、及びシステム提供事業者である。
ユーザは、例えばセキュリティトークンの取得、売却、及び預託等を所望する投資家である。
【００１５】
金融事業者とは、セキュリティトークンを発行する主体であって、例えば、資金を調達

する事業会社や投資運用業者（アセットマネジメント会社を含む）、及び金融商品取引業者（証券会社など）を含む。なお、本実施形態の金融事業者は、投資家等のユーザ以外の取引者を指す。

【００１６】

システム提供事業者とは、セキュリティトークンの取り引きを可能とするシステム（ここでは、情報処理システム１０）を提供又は運用する事業者であって、例えば、当該システムを構築し、ユーザ及び金融事業者に当該システムを利用可能にさせる事業者をいう。

秘密鍵は、情報処理システム１０において、ウォレットアドレスでセキュリティトークンの各種取り引き（例えば発行処理、強制移転処理、預託処理）を行うために必要な情報である。換言すると、秘密鍵は、ウォレットアドレスにおけるセキュリティトークンの取り引きを可能にする唯一の情報である。具体的には、秘密鍵は、ブロックチェーンで用いられている公開鍵暗号方式における鍵情報である。なお、本実施形態では、ブロックチェーンを用いた取り引きの際に、公開鍵暗号方式の一種である「電子署名」が用いられる場合を例に挙げて説明する。

【００１７】

電子署名とは、デジタル情報の作成者を証明する技術であり、秘密鍵を用いて電子署名をすることで、「データが署名者により作成されたこと」、及び「データが改ざんされていないこと」を証明できる仕組みである。

情報処理システム１０では、ユーザ及びシステム提供事業者が秘密鍵をそれぞれ有している。ユーザの秘密鍵は、ネットワークに接続されていない状態、いわゆるコールドウォレットの状態で管理されている。システム提供事業者が有する秘密鍵は、暗号化された状態であって、且つネットワークに接続されている状態、いわゆるホットウォレットの状態で管理されている。以下では、ユーザの秘密鍵を「ユーザ用秘密鍵」と称し、システム提供事業者の秘密鍵を「事業者用秘密鍵」と称する。

【００１８】

情報処理システム１０では、ユーザから金融事業者に対してセキュリティトークンの各種取り引きの要求があった場合には、金融事業者が事業者用秘密鍵を用いてセキュリティトークンの各種取り引きを実行する。したがって、セキュリティトークンの各種取り引きにユーザ用秘密鍵が用いられることがないため、ユーザ用秘密鍵はコールドウォレットの状態で安全に保管されている。

【００１９】

（情報処理システムの構成）

図１に示されるように、情報処理システム１０は、ユーザ端末２０と、金融事業者端末３０と、管理装置４０と、システム端末５０とを備えている。ユーザ端末２０、金融事業者端末３０、及び管理装置４０は通信ネットワークＮを介して有線又は無線により互いに通信可能に接続されている。

【００２０】

ユーザ端末２０はユーザにより所持される。ユーザ端末２０は、ユーザの操作に基づいて、例えばセキュリティトークンの各種取り引きを金融事業者端末３０に対して要求する。

金融事業者端末３０は金融事業者により所持される。金融事業者端末３０は、ユーザ端末２０から送信されるセキュリティトークンの各種取り引きの要求を受信する。金融事業者の担当者は、金融事業者端末３０を操作して管理装置４０のプラットフォームにログインすることにより、ユーザ端末２０から要求されたセキュリティトークンの各種取り引きの実行を管理装置４０に対して指示することができる。

【００２１】

管理装置４０は、金融事業者により金融事業者端末３０を介して利用される装置である。管理装置４０はシステム提供事業者により管理されている。管理装置４０は、ユーザのウォレットアドレス及びユーザ用秘密鍵の生成、並びにセキュリティトークンの取り引きを実行可能なプラットフォームを提供する装置である。管理装置４０は、金融事業者端末

３０からセキュリティトークンの各種取り引きの実行が指示された場合、管理装置４０に記憶されている事業者用秘密鍵を用いて、ブロックチェーンＢＮ上のユーザのウォレットアドレスに対して、指示されたセキュリティトークンの各種取り引きを行うトランザクションを実行する。

【００２２】

ブロックチェーンＢＮとは、暗号化された通貨やセキュリティトークンの取り引きに用いられるシステムである。ブロックチェーンＢＮは、複数のノード（コンピュータ）により構成されており、台帳データを分散して管理している。分散台帳は、いわゆるブロックチェーンＢＮの仕組みにより改ざん困難に管理される。なお、本実施形態のブロックチェーンＢＮによる分散台帳管理の仕組みには一般的なものが採用されているため、ここでは詳細な説明を省略する。ブロックチェーンＢＮは例えばイーサリアムなどにより構築することができる。

【００２３】

システム端末５０はシステム提供事業者により所持される。システム端末５０は、例えば管理装置４０からの通知等を画面に表示することにより、当該通知をシステム提供事業者に知らせるための装置である。

情報処理システム１０には、通信ネットワークＮに接続されていない鍵保管装置６０が設けられている。鍵保管装置６０は、管理装置４０により生成されたユーザ用秘密鍵をコールドウォレットの状態で保管するための装置である。鍵保管装置６０としては、例えば金庫が用いられる。ユーザ用秘密鍵の管理としては、コールドウォレットのうち、例えばハードウェアウォレット方式が用いられる。この場合、管理装置４０では、例えば他の装置と通信可能に接続されていない外部記憶媒体にユーザ用秘密鍵が記憶される。外部記憶媒体としては、例えばＵＳＢ（Universal Serial Bus）型の記憶媒体や、カード型の記憶媒体が用いられる。鍵保管装置６０は、このユーザ用秘密鍵が記憶された外部記憶媒体を保管する。本実施形態では、鍵保管装置６０が保管部の一例である。

【００２４】

ユーザ端末２０、金融事業者端末３０、及びシステム端末５０は、例えばスマートフォン、携帯電話（フィーチャーフォン）、パーソナルコンピュータ（例えばデスクトップ、ラップトップ、タブレットなど）、メディアコンピュータプラットホーム（例えばケーブル、衛星セットトップボックス、デジタルビデオレコーダ）、ハンドヘルドコンピュータデバイス（例えばＰＤＡ（Personal Digital Assistant）、電子メールクライアントなど）、ウェアラブル端末（メガネ型デバイス、時計型デバイスなど）、他種のコンピュータ、又はコミュニケーションプラットホームである。

【００２５】

管理装置４０は、例えばクラウドコンピュータ、サーバコンピュータ、パーソナルコンピュータ（例えばデスクトップ、ラップトップ、タブレットなど）、メディアコンピュータプラットホーム（例えばケーブル、衛星セットトップボックス、デジタルビデオレコーダ）、ハンドヘルドコンピュータデバイス（例えば、ＰＤＡ、電子メールクライアントなど）、あるいは他種のコンピュータ、又はコミュニケーションプラットホームである。なお、管理装置４０における処理の少なくとも一部は、１以上のコンピュータ（例えば１以上のコンピュータにより構成されるクラウドコンピューティング）により実現されていてもよいし、そうでなくてもよい。

【００２６】

（管理装置の構成）

次に、図２を参照して、管理装置４０の具体的な構成について説明する。

図２に示されるように、管理装置４０は、通信部４１と、記憶部４２と、入力部４３と、表示部４４と、出力部４５と、制御部４６とを備えている。

【００２７】

通信部４１は、図１に示される通信ネットワークＮを介してユーザ端末２０、金融事業者端末３０、システム端末５０、及びブロックチェーンＢＮと各種通信を行う。

記憶部４２には、管理装置４０を動作させるための各種プログラムや各種データ等が記憶されている。例えば記憶部４２にはユーザデータベース４２０及び金融事業者データベース４２１が記憶されている。

【００２８】

図３（Ａ）に示されるように、ユーザデータベース４２０には、例えば各ユーザの識別番号、氏名、メールアドレス、及びウォレットアドレス等の情報が含まれている。識別番号は、例えばユーザを一意に識別可能な番号である。ウォレットアドレスは、例えばブロックチェーンＢＮにおけるユーザのウォレットアドレスを示す情報である。

【００２９】

図３（Ｂ）に示されるように、金融事業者データベース４２１には、例えば各金融事業者の識別番号、名称、パスワード、事業者用秘密鍵、及びデータキーが記憶されている。金融事業者の識別番号は、例えば金融事業者を一意に識別可能な番号である。パスワードは、例えば金融事業者が管理装置４０のプラットフォームにログインする際に用いられる文字情報である。事業者用秘密鍵及びデータキーは、暗号化された状態で金融事業者データベース４２１に記憶されている。事業者用秘密鍵は、セキュリティトークンの取り引きの際に用いられる情報である。事業者用秘密鍵は、複数の金融事業者のそれぞれに対して個別に付与されている。データキーは、暗号化された秘密鍵を復号する際に用いられる。本実施形態では、事業者用秘密鍵が第１秘密鍵の一例である。また、データキーが第２秘密鍵の一例である。

【００３０】

入力部４３は、システム提供事業者の担当者による各種入力操作を受け付ける。入力部４３は、例えばシステム提供事業者の担当者によるユーザのウォレットアドレス及びユーザ用秘密鍵を新規に発行する操作を受け付ける。本実施形態では、ユーザ用秘密鍵が第３秘密鍵の一例である。

【００３１】

表示部４４は、システム提供事業者の担当者により視認可能な各種画面を表示する。表示部４４は、例えば新規に発行されたユーザの識別番号及びユーザ用秘密鍵を示す画面を表示する。

出力部４５は、外部記憶媒体にデータを出力させて記憶させる。出力部４５は、例えばユーザの識別番号及びユーザ用秘密鍵が表示されている表示部４４の画面がＰＤＦファイル等の電子データに変換されると、変換された電子データを外部記憶媒体に出力して記憶させる。

【００３２】

制御部４６は管理装置４０を制御する。制御部４６は、記憶部４２に記憶されているプログラムを実行することにより実現される機能的な構成として、第１アカウント発行部４６０と、第２アカウント発行部４６１と、復号部４６２と、トランザクション実行部４６３とを備えている。

【００３３】

（第１アカウント発行部）

第１アカウント発行部４６０はユーザのアカウントを発行する。例えば、金融事業者の担当者は、新規にユーザのアカウントの登録を依頼するための申込情報を金融事業者端末３０から管理装置４０に送信する。申込情報には、ユーザの氏名、及びメールアドレス等の情報が含まれている。第１アカウント発行部４６０は、ユーザの申込情報を受信すると、ユーザの識別番号を新たに発行するとともに、発行されたユーザの識別番号を氏名及びメールアドレス等に関連付けてユーザデータベース４２０に記憶させる。

【００３４】

このようにしてユーザの識別番号等がユーザデータベース４２０に記憶された後、第１アカウント発行部４６０は、ユーザの識別番号に対応したウォレットアドレス及びユーザ用秘密鍵を更に発行する。そして、第１アカウント発行部４６０は、発行されたウォレットアドレスとユーザの識別番号とを関連付けてユーザデータベース４２０に更に記憶させ

る。これにより、セキュリティトークンの取り引きを行うためのユーザのアカウントの発行が完了する。

【００３５】

（第２アカウント発行部）

第２アカウント発行部４６１は金融事業者のアカウントを発行する。例えば、金融事業者の担当者は、新規に金融事業者のアカウントの登録を依頼するための申込情報を金融事業者端末３０から管理装置４０に送信する。申込情報には、金融事業者の名称、パスワード、及びメールアドレス等の情報が含まれている。第２アカウント発行部４６１は、金融事業者の申込情報を受信すると、金融事業者の識別番号を新たに発行するとともに、新たに発行された金融事業者の識別番号を金融事業者の名称及びパスワード等と関連付けて金融事業者データベース４２１に記憶させる。これにより、セキュリティトークンの取り引きを行うための金融事業者のアカウントの発行が完了する。

【００３６】

（復号部）

復号部４６２は、トランザクション実行部４６３からの要求に基づいて、金融事業者データベース４２１に記憶されている、暗号化されたデータキーを復号する。具体的には、復号部４６２は、データキーを暗号化する際に用いられたマスタキーを有しており、当該マスタキーを用いて、暗号化されたデータキーを復号する。

【００３７】

（トランザクション実行部）

トランザクション実行部４６３は、金融事業者からの要求に基づいて、セキュリティトークンに関するトランザクションをブロックチェーンＢＮに対して実行する。図４は、トランザクション実行部４６３によるセキュリティトークンのトランザクションの実行手順を示したものである。

【００３８】

図４に示されるように、金融事業者の担当者が金融事業者端末３０において金融事業者の識別番号及びパスワードを入力して管理装置４０のプラットフォームにログインする操作を行うと（ステップＳ１０）、トランザクション実行部４６３は、そのログイン操作を受け付けた後（ステップＳ２０）、金融事業者の担当者により入力された識別番号及びパスワードと、金融事業者データベース４２１に記憶されている金融事業者の識別番号及びパスワードとを照合することにより、金融事業者の認証処理を行う（ステップＳ２１）。トランザクション実行部４６３による認証が成立した後（ステップＳ２２）、金融事業者の担当者が、金融事業者端末３０を操作して、セキュリティトークンの取り引き内容に対応した更新処理の実行を要求すると（ステップＳ１１）、トランザクション実行部４６３はセキュリティトークンの更新処理を受信する（ステップＳ２３）。このとき、トランザクション実行部４６３は、金融事業者の識別番号に関連付けられている、暗号化された事業者用秘密鍵及びデータキーを金融事業者データベース４２１から読み込む（ステップＳ２４）。続いて、トランザクション実行部４６３は、暗号化されたデータキーを復号部４６２により復号する（ステップＳ２５）。さらに、トランザクション実行部４６３は、復号化されたデータキーを用いて、暗号化された事業者用秘密鍵を更に復号する（ステップＳ２６）。そして、トランザクション実行部４６３は、復号化された事業者用秘密鍵を用いて、更新処理に対応したトランザクションデータに電子署名するとともに、署名済みのトランザクションをブロックチェーンＢＮに対して実行する（ステップＳ２７）。以上により、金融事業者から管理装置４０に対して要求されたセキュリティトークンのトランザクションが完了する。

【００３９】

（情報処理システムの動作例）

次に、情報処理システム１０の動作例について説明する。まず、図５を参照して、管理装置４０におけるユーザのアカウントの発行手順について説明する。なお、ユーザが金融事業者においてアカウント情報を既に有している場合を例に挙げて説明する。

図５に示されるように、本実施形態の情報処理システム１０では、金融事業者の顧客である投資家等のユーザがセキュリティトークンの預託や購入等の取り引きを新規に行うことを金融事業者に対して申し込むと、金融事業者は、そのセキュリティトークンに対応したユーザのアカウントを作成する。

【００４０】

具体的には、図５に示されるように、金融事業者の担当者が、まず、金融事業者端末３０を操作して、ユーザの氏名及びメールアドレス等を含む申込情報を管理装置４０に送信すると（ステップＳ５０）、当該申込情報が管理装置４０の通信部４１により受信される（ステップＳ６０）。これにより、管理装置４０の第１アカウント発行部４６０は、ユーザの識別番号を発行する処理を実行するとともに（ステップＳ６１）、発行された識別番号をユーザの氏名及びメールアドレス等と関連づけてユーザデータベース４２０に記憶させる（ステップＳ６２）。また、第１アカウント発行部４６０は、ユーザのアカウントの一次登録が完了した旨の通知をシステム端末５０にメール等により送信する（ステップＳ６３）。システム提供事業者の担当者は、管理装置４０から送信される通知をシステム端末５０により閲覧すると、次の作業として、例えばユーザのウォレットアドレス及びユーザ用秘密鍵を管理装置４０においてセキュアルームＲｓ内で発行する。

【００４１】

具体的には、セキュアルームＲｓ内には管理装置４０の入力部４３、表示部４４、及び出力部４５が配置されている。システム提供事業者の担当者が、ユーザのウォレットアドレス及びユーザ用秘密鍵の発行を要求する操作を入力部４３に対して行うと（ステップＳ６４）、第１アカウント発行部４６０は、担当者の要求に基づいて、ユーザのブロックチェーン上のウォレットアドレスを作成するとともに、セキュリティトークンの取り引きに使用可能なユーザ用秘密鍵を発行する（ステップＳ６５）。続いて、第１アカウント発行部４６０は、発行されたウォレットアドレスをユーザの識別番号と関連付けてユーザデータベース４２０に記憶させる（ステップＳ６６）。これにより、ユーザのアカウントの発行が完了する。なお、この際、第１アカウント発行部４６０は、発行されたユーザ用秘密鍵を記憶部４２等の管理装置４０の記憶媒体に記憶させない。

【００４２】

続いて、第１アカウント発行部４６０は、発行されたユーザ用秘密鍵をユーザの識別番号と共に表示部４４の画面に表示させる（ステップＳ６７）。これにより、担当者は、ユーザの識別番号と、それに対応するユーザ用秘密鍵を表示部４４の画面で視認することができる。なお、第１アカウント発行部４６０は、ユーザ用秘密鍵を表示部４４に表示する際に、記憶部４２等の管理装置４０の記憶媒体にユーザ用秘密鍵の情報を一時的に記憶させてもよい。

【００４３】

続いて、担当者が、入力部４３を操作して、表示部４４に表示されている画面情報をＰＤＦファイル等の電子データに変換する操作を行った後（ステップＳ６８）、その電子データを外部記憶媒体に記憶させる操作を行うと、出力部４５は、変換された電子データを外部記憶媒体に出力して記憶させる（ステップＳ６９）。続いて、担当者が、出力部４５から外部記憶媒体を取り外した後、当該外部記憶媒体を鍵保管装置６０に保管する（ステップＳ７０）。これにより、ユーザ用秘密鍵の情報は、管理装置４０にデータとして残ることなく、鍵保管装置６０にのみに存在する状態で、すなわちコールドウォレットの状態で保管となる。

【００４４】

次に、図６を参照して、管理装置４０におけるユーザのセキュリティトークンの取り引きの処理手順について説明する。

図６に示されるように、ユーザがユーザ端末２０を操作して、セキュリティトークンの預託や購入等の取り引きを金融事業者に対して要求すると（ステップＳ８０）、その取引要求情報が金融事業者端末３０により受信される（ステップＳ９０）。これにより、金融事業者の担当者は、ユーザの取引要求情報に対応したセキュリティトークンの取引処理の

実行を管理装置４０に対して要求する。具体的には、金融事業者の担当者が金融事業者端末３０を操作することにより金融事業者の識別番号及びパスワードを入力して管理装置４０のプラットフォームにログインした後（ステップＳ９１）、ユーザの取り引き内容に対応した更新処理の実行を管理装置４０に要求すると（ステップＳ９２）、管理装置４０のトランザクション実行部４６３が、更新処理に対応したセキュリティトークンのトランザクションをブロックチェーンＢＮに対して実行する（ステップＳ１００）。このトランザクション処理の詳細は図４に示される通りであるため省略する。

【００４５】

（ハードウェア的な構成）

次に、図７を参照して、ユーザ端末２０、金融事業者端末３０、管理装置４０、及びシステム端末５０をコンピュータにより実現する場合のハードウェア構成の一例を説明する。図７は、コンピュータのハードウェア構成の一例を示す図である。

【００４６】

図７に示されるように、コンピュータ１０００は、プロセッサ１００１と、メモリ１００２と、記憶装置１００３と、入力Ｉ／Ｆ部１００４と、データＩ／Ｆ部１００５と、通信Ｉ／Ｆ部１００６と、表示装置１００７とを含む。

プロセッサ１００１は、メモリ１００２に記憶されているプログラムを実行することによりコンピュータ１０００における各種の処理を制御する制御部である。

【００４７】

メモリ１００２は、例えばＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等の記憶媒体である。メモリ１００２は、プロセッサ１００１によって実行されるプログラムのプログラムコードや、プログラムの実行時に必要となるデータを一時的に記憶する。

記憶装置１００３は、例えばハードディスクドライブ（ＨＤＤ）やフラッシュメモリ等の不揮発性の記憶媒体である。記憶装置１００３は、オペレーティングシステムや、上記各構成を実現するための各種プログラムを記憶する。

【００４８】

入力Ｉ／Ｆ部１００４は、ユーザからの入力を受け付けるためのデバイスである。入力Ｉ／Ｆ部１００４の具体例としては、キーボードやマウス、タッチパネル、各種センサー、ウェアラブル・デバイス等が挙げられる。入力Ｉ／Ｆ部１００４は、例えばＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）等のインターフェースを介してコンピュータ１０００に接続されていても良い。

【００４９】

データＩ／Ｆ部１００５は、コンピュータ１０００の外部からデータを入力するためのデバイスである。データＩ／Ｆ部１００５の具体例としては、各種記憶媒体に記憶されているデータを読み取るためのドライブ装置等がある。データＩ／Ｆ部１００５は、コンピュータ１０００の外部に設けられることも考えられる。その場合、データＩ／Ｆ部１００５は、例えばＵＳＢ等のインターフェースを介してコンピュータ１０００へと接続される。

【００５０】

通信Ｉ／Ｆ部１００６は、コンピュータ１０００の外部の装置と有線又は無線により、通信ネットワークＮを介したデータ通信を行うためのデバイスである。通信Ｉ／Ｆ部１００６は、コンピュータ１０００の外部に設けられることも考えられる。その場合、通信Ｉ／Ｆ部１００６は、例えばＵＳＢ等のインターフェースを介してコンピュータ１０００に接続される。

【００５１】

表示装置１００７は、各種情報を表示するためのデバイスである。表示装置１００７の具体例としては、例えば液晶ディスプレイや有機ＥＬ（Ｅｌｅｃｔｒｏ－Ｌｕｍｉｎｅｓｃｅｎｃｅ）ディスプレイ、ウェアラブル・デバイスのディスプレイ等が挙げられる。表示装置１００７は、コンピュータ１０００の外部に設けられても良い。その場合、表示装置１００７は、例えばディスプレイケーブル等を介してコンピュータ１０００に接続され

る。また、入力Ｉ／Ｆ部１００４としてタッチパネルが採用される場合には、表示装置１００７は、入力Ｉ／Ｆ部１００４と一体化して構成することが可能である。

【００５２】

（実施形態の情報処理システムの作用及び効果）

以上説明したように、本実施形態の情報処理システム１０は、記憶部４２と、トランザクション実行部４６３とを備える。記憶部４２には、セキュリティトークンのトランザクションを実行するための事業者用秘密鍵（第１秘密鍵）が暗号化された状態で記憶されている。トランザクション実行部４６３は、金融事業者（取引者）のログイン操作に基づいて、金融事業者のアカウントに対応した、暗号化された事業者用秘密鍵を記憶部４２から読み込むとともに、暗号化された事業者用秘密鍵を復号して、復号化された事業者用秘密鍵を用いてブロックチェーンＢＮ上でセキュリティトークンのトランザクションを実行する。

この構成によれば、金融事業者のログイン操作に基づいて事業者用秘密鍵が記憶部４２から読み込まれるため、金融事業者自身で事業者用秘密鍵を管理する必要がない。よって、より適切に事業者用秘密鍵を管理することができる。また、事業者用秘密鍵は記憶部４２において暗号化された状態で記憶されているため、セキュリティ性を確保することもできる。

【００５３】

記憶部４２には、事業者用秘密鍵を暗号化する際に用いられたデータキー（第２秘密鍵）が暗号化された状態で更に記憶されている。情報処理システム１０は、データキーを復号可能な復号部４６２を更に備える。トランザクション実行部４６３は、金融事業者のログイン操作に基づいて、暗号化されたデータキーを記憶部４２から読み込むとともに、暗号化されたデータキーを復号部４６２により復号して、復号化されたデータキーを用いて、暗号化された事業者用秘密鍵を復号する。

この構成によれば、記憶部４２には、事業者用秘密鍵を復号可能なデータキーが暗号化された状態で更に記憶されているため、データキー及び事業者用秘密鍵が第三者に流出し難くなる。よって、セキュリティ性を更に高めることができる。

【００５４】

本実施形態の情報処理システム１０は、第１アカウント発行部４６０と、出力部４５とを更に備える。第１アカウント発行部４６０は、金融事業者に対してセキュリティトークンの取り引きを依頼するユーザに対応したウォレットアドレス、及びウォレットアドレスに対応したユーザ用秘密鍵（第３秘密鍵）を発行する。出力部４５は、第１アカウント発行部４６０により発行されたユーザ用秘密鍵を、ユーザ用秘密鍵の情報が残らないように出力する。具体的には、出力部４５は、ユーザ用秘密鍵の情報が残らないように、ユーザ用秘密鍵を表示部４４に表示する。

この構成によれば、ユーザ用秘密鍵の情報が管理装置４０に残ることがない。よって、ユーザ用秘密鍵のセキュリティ性を向上させることができる。

【００５５】

情報処理システム１０は、ユーザ用秘密鍵の情報をインターネットに接続されていない状態で保管可能な鍵保管装置６０（保管部）を更に備える。鍵保管装置６０は、ユーザ用秘密鍵が電子データとして記憶された外部記憶媒体を保管する。

この構成によれば、ユーザ用秘密鍵をコールドウォレットの状態で保管することができるため、より適切にユーザ用秘密鍵を管理することが可能となる。

【００５６】

＜他の実施形態＞

本開示は上記の具体例に限定されるものではない。

【００５７】

例えば情報処理システム１０では、事業者用秘密鍵に代えて、複数のセキュリティトークンのそれぞれの発行体に対して個別に付与されている発行体用秘密鍵を用いてもよい。この場合、トランザクション実行部４６３は、例えば所定の金融事業者から複数のセキュ

リティトークンの更新処理の実行が要求された場合、複数のセキュリティトークンにそれぞれ対応した複数の発行体用秘密鍵を用いてブロックチェーンＢＮに対してトランザクションを実行する。この場合、所定の金融事業者とは別の金融事業者からセキュリティトークンの更新処理の実行が要求された場合、トランザクション実行部４６３は、セキュリティトークンの種類が同一であれば、同一の発行体用秘密鍵を用いてブロックチェーンＢＮに対してトランザクションを実行することになる。すなわち、この変形例と上記実施形態とを比較すると、この変形例では同一のセキュリティトークンであれば同一の発行体用秘密鍵が用いられるのに対し、上記実施形態では同一の金融事業者であれば同一の事業者用秘密鍵が用いられるという点で異なる。

【００５８】

出力部４５は、ユーザの識別番号及びユーザ用秘密鍵の情報を外部記憶媒体に記憶するものに限らず、例えばユーザの識別番号及びユーザ用秘密鍵が印字された紙媒体を印刷する印刷装置等であってもよい。この場合、鍵保管装置６０には、ユーザの識別番号及びユーザ用秘密鍵が印字された紙媒体が保管されることになる。

【００５９】

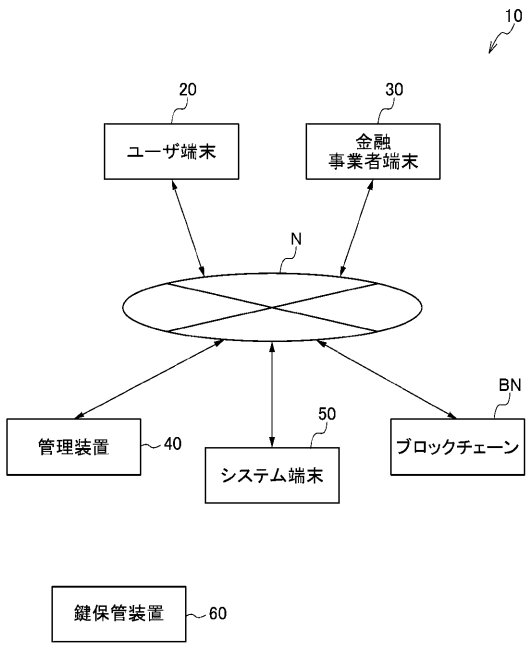
上記の具体例に、当業者が適宜設計変更を加えたものも、本開示の特徴を備えている限り、本開示の範囲に包含される。前述した各具体例が備える各要素、及びその配置、条件、形状等は、例示したものに限定されるわけではなく適宜変更することができる。前述した各具体例が備える各要素は、技術的な矛盾が生じない限り、適宜組み合わせを変えることができる。

【符号の説明】

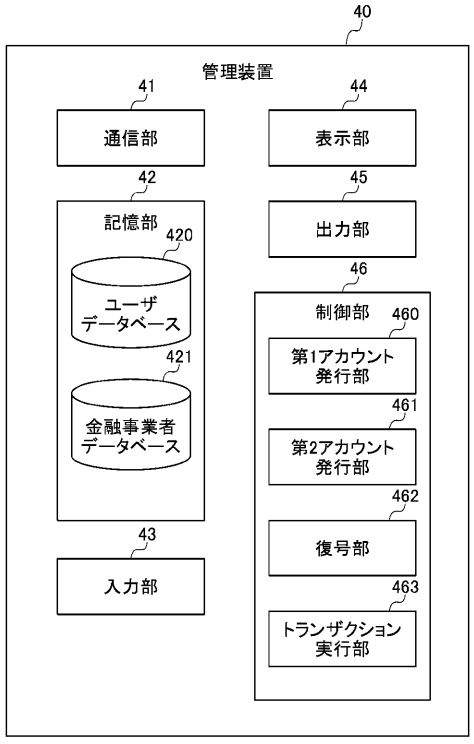
【００６０】

１０：情報処理システム、４２：記憶部、４４：表示部、４５：出力部、６０：鍵保管装置（保管部）、４６０：第１アカウント発行部、４６２：復号部、４６３：トランザクション実行部、１０００：コンピュータ。

【図１】



【図２】



【図３】

(A)

420

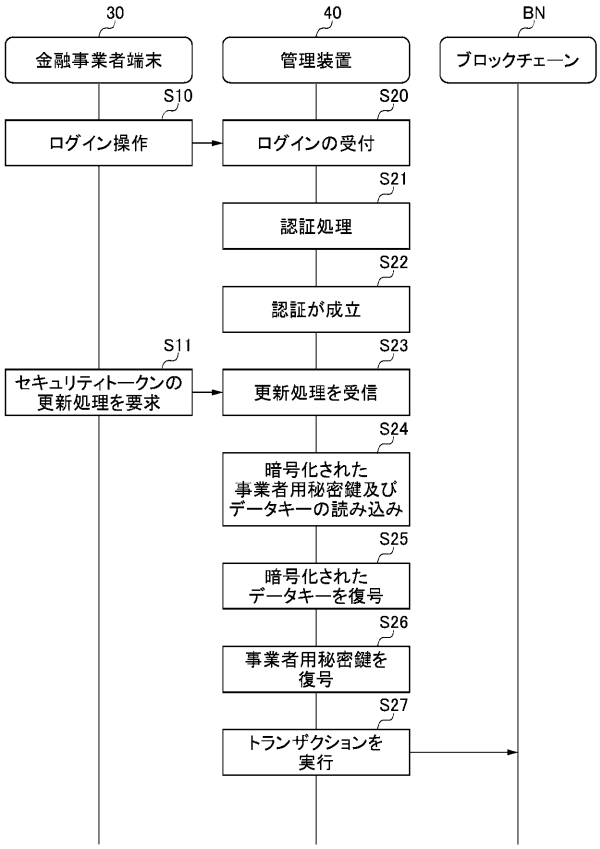
ユーザ識別番号	ユーザ氏名	メールアドレス	ウォレットアドレス
0001	山田花子	abcd@ef.com	1HL1zFK…
0002	山田太郎	ghij@kl.com	Dx7c7a…
・・・	・・・	・・・	・・・

(B)

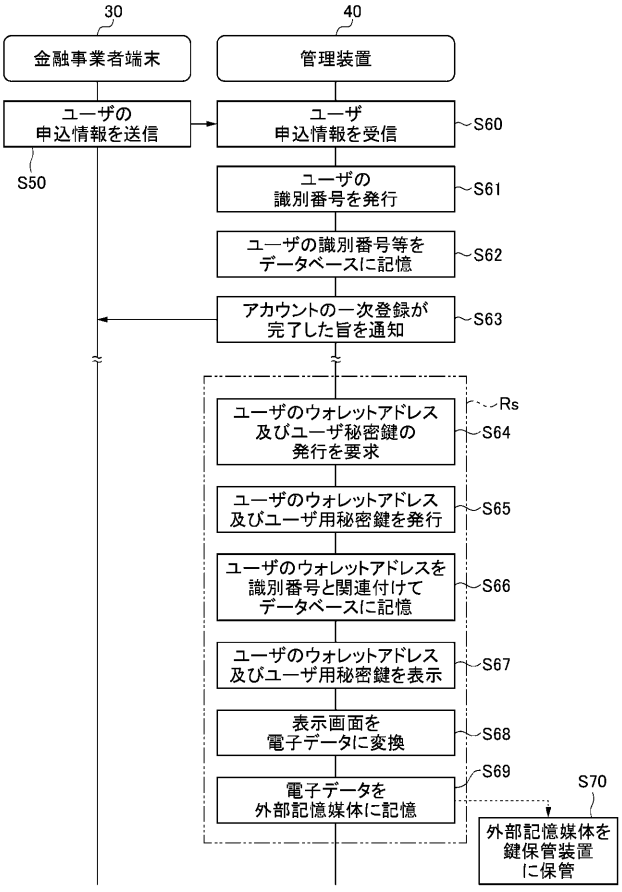
421

金融事業者識別番号	金融事業者名称	パスワード	事業者用秘密鍵	データキー
1001	甲証券	AAA	o9dZN2…	Dnbouu…
1002	乙証券	BBB	GBRcmW…	ELhNRu…
・・・	・・・	・・・	・・・	・・・

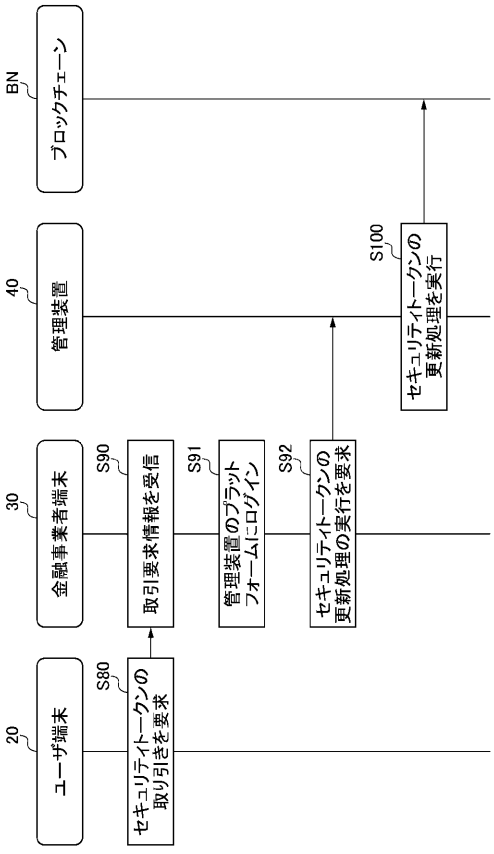
【図４】



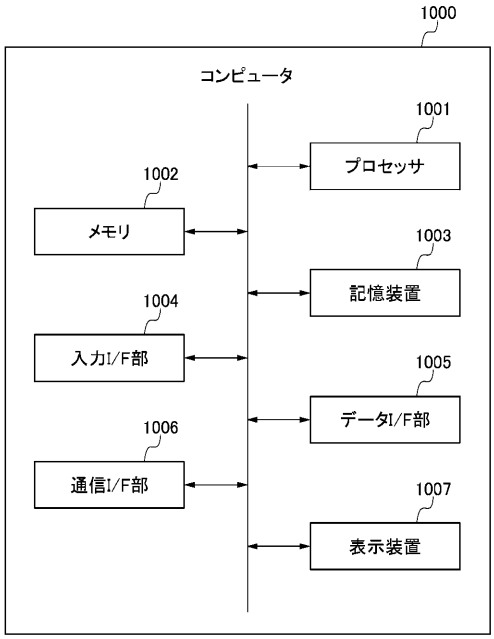
【図５】



【図６】



【図７】


1000
コンピュータ
1001
プロセッサ
1002
メモリ
1003
記憶装置
1004
入力I/F部
1005
データI/F部
1006
通信I/F部
1007
表示装置

フロントページの続き

(72)発明者　中島　和哉
東京都新宿区西新宿８－１７－１　ＴＩＳ株式会社内