

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2024年6月20日(20.06.2024)

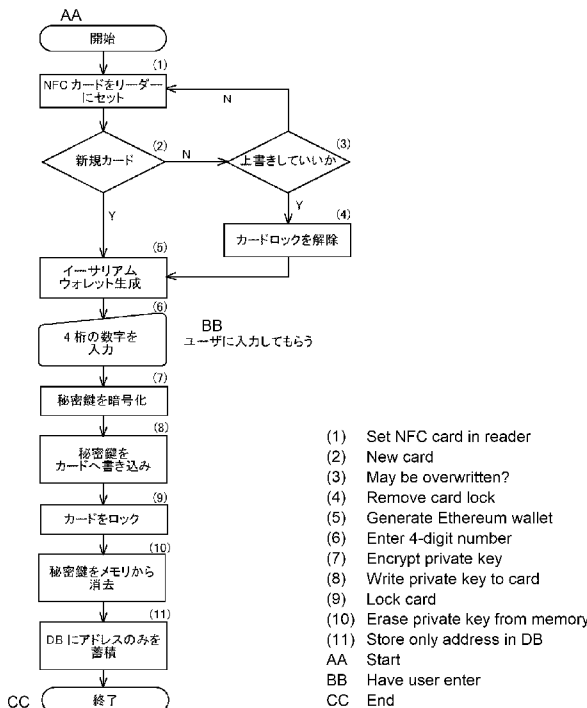


(10) 国際公開番号
WO 2024/128208 A1

- (51) 国際特許分類:
H04L 9/10 (2006.01) *G06Q 20/32* (2012.01)
- (21) 国際出願番号: PCT/JP2023/044356
- (22) 国際出願日: 2023年12月12日(12.12.2023)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2022-198251 2022年12月12日(12.12.2022) JP
- (71) 出願人: 株式会社 P B A D A O (PBADAO CO., LTD.) [JP/JP]; 〒1500034 東京都渋谷区代官山町13-5 代官山135ビル Tokyo (JP).
- (72) 発明者: 芳賀 真(HAGA, Tadashi); 〒1500034 東京都渋谷区代官山町13-5 代官山135ビル 株式会社 P B A D A O 内 Tokyo (JP). 堀井 紳吾(HORII, Shingo); 〒1500034 東京都渋谷区代官山町13-5 代官山135ビル 株式会社 P B A D A O 内 Tokyo (JP).
- (74) 代理人: 白 浜 秀 二 (SHIRAHAMA, Shuji); 〒1070052 東京都港区赤坂四丁目9番17号 赤坂第一ビル Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR,

(54) Title: NFT DISTRIBUTION SYSTEM AND WALLET CARD CREATION METHOD FOR NFT DISTRIBUTION SYSTEM, AND ACTIVATION PROCESSING METHOD FOR NFC CARD PROCESSING SYSTEM

(54) 発明の名称: N F T 配布システムおよび N F T 配布システムのウォレットカード作成方法および N F C カード処理システムのアクティベーション処理方法



(57) Abstract: The present invention addresses the problem of popularizing a card-type wallet that makes it possible to confirm, on a data terminal, information about an NFT and crypto asset in possession by a simple operation using an NFC card medium. Provided is a wallet card creation method for an NFT distribution system in which a predetermined

HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告 (条約第21条(3))

NFC card (3) and a data terminal (1) that performs near field communication with the NFC card (3) perform near field communication, the method being characterized by comprising: an encrypting step (7) for creating a private key for using the NFC card as a wallet for managing an NFT in possession, and encrypting the created private key; and control steps ((8) to (11)) in which, in a state in which the private key encrypted by the encrypting step has been written to a storage medium of the NFC card (3), the private key is erased from the storage medium and address information for trading the NFT is written to the storage medium.

(57) 要約: N F C カード媒体を利用して、所有する N F T の情報および暗号資産の情報を簡単な操作で、データ端末上で確認することができるカード型のウォレットを普及させること。所定の N F C カード (3) と、N F C カード (3) と近接無線通信するデータ端末 (1) とが近接無線通信する N F T 配布システムのウォレットカード作成方法であって、所有している N F T を管理するためのウォレットとして前記 N F C カードを使用するための秘密鍵を作成し、該作成した秘密鍵を暗号化する暗号化ステップ (7) と、暗号化ステップが暗号化した秘密鍵を N F C カード (3) の記憶媒体に書き込んだ状態で、秘密鍵を記憶媒体から消去して、N F T を取引するためのアドレス情報を記憶媒体に書き込む制御ステップ ((8) ~ (11)) とを備えることを特徴とする。

明 細 書

発明の名称：

N F T 配布システムおよびN F T 配布システムのウォレットカード作成方法およびN F C カード処理システムのアクティベーション処理方法

技術分野

[0001] 本発明は、暗号資産を利用するN F T の取引を行うデータ端末と、所定のN F C カードが無線通信してN F T カードウォレットを配布するN F T 配布システムおよびN F T 配布システムのウォレットカード作成方法およびN F C カード処理システムのアクティベーション処理方法に関するものである。

背景技術

[0002] 近年、暗号資産を取引するシステムで扱うコインの種類は、増加の傾向を示している。つまり、複数の暗号資産を取引する資産家も増え、暗号資産間においても公開されたレートで換金取引が可能となっている。

[0003] なお、暗号資産は、代替不可能なN F T とは異なり、代替が可能であり、例えば、暗号資産のビットコインを例に考えてみると、自分が持っている1ビットコインと、他人が持っている1ビットコインは、同じ価値を持っており、代替が可能である。ここで、暗号資産における秘密鍵の仕組みを考える。N F T や暗号資産で用いられているブロックチェーンの「公開鍵暗号方式」とは、公開鍵と秘密鍵という2種類の「鍵」を用いた暗号の仕組みを用いている。

[0004] 公開鍵とは、簡単にいうと、データを暗号化するための鍵であり、公開鍵については、あくまで暗号化するための鍵であるので、公開されてもセキュリティ上の問題はない。

[0005] 他方、秘密鍵とは、公開鍵によって暗号化されたデータを復号するための鍵であり、ブロックチェーンにデータを記録するときの電子署名にも利用される。秘密鍵については、第三者に知られてしまうと、その秘密鍵を利用して暗号化されたデータが復元されてしまうため、秘密鍵については、公開鍵

と異なり、漏洩を防いで安全に保管する必要がある。そのため、暗号資産を扱うウォレットでは、この秘密鍵をどのように保管しているかが重要になる。

[0006] また、ウォレットには、ホットウォレットと、コールドウォレットとがあり、ホットウォレットは、ネットワークに接続できるため、ユーザがオンラインで簡単にNFTや暗号資産を管理することができるという点がメリットとしてある。

[0007] 一方で、ネットワークに接続できることから、端末へのハッキングやウィルスの感染などにより秘密鍵の情報が流出したり、秘密鍵が使えなくなったりするというデメリットがある。

[0008] 一方、コールドウォレットは、ネットワークに接続されていないので、ネットワーク経由でのハッキングによる不正アクセスや、ウィルスに感染するリスクがないという点が、メリットとなる。

[0009] 一方、コールドウォレットは、ネットワークに接続されていないため、送金等の操作を行う際に追加の手続きが必要となり、時間がかかってしまうという課題があった。

[0010] なお、下記特許文献1にはブロックチェーンにデータを記録する際には、データ作成者が持つ秘密鍵により記録するデータに対して電子署名を作成する必要があるため、NFTを発行・売買する際には、ウォレットをNFTマーケットプレイスに接続する必要があること、また、NFTの取引には暗号資産が使われることが多いことから、ウォレットはNFT取引に必須となることが記載されている。

[0011] なお、暗号通貨には、異なる特徴を有する複数の種類の暗号通貨がある。このため、ユーザは、暗号通貨を使用するとき、用途に適した暗号通貨を選択して利用する。暗号通貨の種類には、例えば、ビットコイン（BTC：登録商標）、イーサリアム（ETH：登録商標）、ライトコイン（LTC）、及びモナコイン（MONA：登録商標）などがある。暗号通貨の用途には、例えば、価値の保存、商品の購入、及びブロックチェーン上に書き込まれる

データの管理手数料などがある。

- [0012] 暗号資産を扱うツールとしてのソフトウェアウォレットであるMe t a M a s k（商品名）をデータ端末にインストールすることで、データ端末を操作してイーサリアム（E T H：登録商標）やイーサリアムベースの暗号通貨およびN F Tの保管・管理・送受信やWe bブラウザまたはモバイルアプリの内蔵ブラウザによる分散型アプリケーション（D A p p s）への接続を行うことができる。また、複数の分散型取引所（D E X）との連携に対応し、最適な為替レートを検索してイーサリアム系トークンを交換することができる。
- [0013] さらに、急増するN F Tゲームやマーケットプレイスなど、多くのN F Tコンテンツへの接続に使用することもでき、Me t a M a s kウォレットは必須ツールとなっている。
- [0014] 一方、マルチ署名ブロックチェーンウォレットを使用して、集積回路決済カードを介して暗号通貨ブロックチェーン取引を実行するデバイスとして、下記特許文献2が公開されている。
- [0015] この特許文献2には、暗号通貨ブロックチェーン取引の構成として、「マルチ署名ブロックチェーンウォレットを使用して、集積回路決済カードを介して暗号通貨ブロックチェーン取引を実行するための方法は、決済カードの集積回路の記憶部内に、少なくとも、第1の暗号鍵ペアの第1の秘密鍵と取引口座番号とを格納することと、集積回路の受信器によって、販売時点情報管理装置からブロックチェーン取引を受信することであって、ブロックチェーン取引は、少なくとも、1つ以上の未使用取引出力額と、1つ以上の宛先アドレスと、1つ以上の宛先アドレスの各々に関する暗号通貨額と、第2の暗号鍵ペアの第2の秘密鍵を使用して生成された第1のデジタル署名と、を含む、ことと、集積回路のプロセッサによって、第1の秘密鍵を使用してブロックチェーン取引にデジタル署名して、第2のデジタル署名を生成することと、集積回路の送信器によって、第1のデジタル署名と第2のデジタル署名とを含むデジタル署名付きブロックチェーン取引を、販売時点情報管理装置に送信することと、を含む。」が記載されている。

先行技術文献

特許文献

[0016] 特許文献1：特許第7 1 3 7 0 3 2号公報

特許文献2：特表2 0 2 3－5 2 1 7 0 7号公報

発明の概要

発明が解決しようとする課題

[0017] 一方、暗号資産の取引を管理するためには、ブロックチェーンにデータを記録する必要があり、その際、データ作成者が持つ秘密鍵により記録するデータに対して電子署名を作成する必要がある。

[0018] そのため、N F Tを発行・売買する際には、暗号資産が使われることが多く、ウォレットをN F Tマーケットプレイスに接続する必要があるにもかかわらず、ウォレットとN F T取引とを連系するための扱い易い媒体が提案されていないため、データ端末装置が必須となってしまう、N F Tと暗号資産を利用する取引システムの改善が切望されていた。

[0019] 一方、仮想通貨ウォレットとして機能させるN F Cカードを使った新しいセキュリティ管理方法も盛んに提案されているが、これといった標準仕様が規定されておらず、汎用性や操作性に偏りが生じてしまうため、N F Tを簡単にN F Cカードと連系したシステムの開発が急務である。

[0020] 本発明は、上記事情に基づいてなされたもので、その目的とするところは、N F Cカード媒体を利用して、所有するN F Tの情報および暗号資産の情報を簡単な操作で、データ端末上で確認することができるN F T配布システムを提供することである。

[0021] さらに、1枚のN F Cカードを所有するだけで、複数の仮想通貨のいずれにも適応した共通のプロトコルに基づきN F Cカードを安全にアクティベーションできるN F Cカード処理システムのアクティベーション処理方法を提供することである。

課題を解決するための手段

[0022] 本発明に係るNFT配布システムは、所定のNFCカードと、前記NFCカードと近接無線通信するデータ端末とが近接無線通信するNFT配布システムであって、前記データ端末は、所有しているNFTを管理するためのウォレットとして前記NFCカードを使用するための秘密鍵を作成し、該作成した前記秘密鍵を暗号化する暗号化手段と、前記暗号化手段が暗号化した前記秘密鍵を前記NFCカードの記憶媒体に書き込んだ状態で、前記秘密鍵を前記記憶媒体から消去して、前記NFTを取引するためのアドレス情報を前記記憶媒体に書き込むように制御する制御手段と、を備えることを特徴とする。

[0023] 本発明に係るNFCカード処理システムのアクティベーション処理方法は、所定の通信媒体を介して、NFCカードと近接無線通信するデータ端末と、前記データ端末が読み取る前記NFCカードのアクティベーション処理を複数のシステム管理サーバと連携して行うNFCカード処理システムのアクティベーション処理方法であって、前記複数のシステム管理サーバのうち、いずれか1つのシステム管理サーバを介して前記NFCカードに対してプリアクティベーション処理を実行して前記NFCカードのUID（個体識別番号）をプリアクティベーションデータベースに登録する第1の登録ステップと、前記複数のシステム管理サーバのうち、いずれか1つのシステム管理サーバを介して前記NFCカードに対してプリアクティベーション処理が終了している処理済NFCカードに対してアクティベーション処理を実行してアクティベーションデータベースに生成される公開鍵と、UIDとを紐づけて登録する第2の登録ステップと、を備えることを特徴とする。

発明の効果

[0024] 本発明によれば、NFCカード媒体を利用して、所有するNFTの情報および暗号資産の情報を簡単な操作で、データ端末上で確認することができるカード型のウォレットを普及させることができる。

図面の簡単な説明

[0025] 図面は、本開示に係る本発明の特定の実施の形態を示し、発明の不可欠な

構成ばかりでなく、選択的及び好ましい実施の形態を含む。

[図1]本実施形態を示すN F T配布システムにおけるデータ処理装置の構成を説明する平面図。

[図2]図1に示したデータ端末のハードウェア構成を説明するブロック図。

[図3]本実施形態を示すN F T配布システムにおけるデータ処理装置のデータ処理手順の一例を示すフローチャート。

[図4]本実施形態を示すN F T配布システムにおけるデータ処理装置のデータ処理手順の一例を示すフローチャート。

[図5]本実施形態を示すN F Cカード処理システムの構成を説明するブロック図。

[図6]図5に示した所有確認サーバの機能処理を説明するブロック図。

[図7]図5に示した所有確認サーバによる所有確認シーケンスの一例を示すフローチャート。

[図8]図5に示したプリアクティベーションサーバの機能処理を説明するブロック図。

[図9]図5に示したプリアクティベーションサーバによるシーケンスの一例を示すフローチャート。

[図10]図5に示した動的Q Rサーバによる機能処理を説明するブロック図。

[図11]図5に示した動的Q Rサーバによる機能処理を説明するフローチャート。

[図12]図5に示したブロックチェーン巡回サーバが参照するデータベースの対応を説明するブロック図。

[図13]図5に示したブロックチェーン巡回サーバによる機能処理を説明するフローチャート。

[図14]本実施形態を示すN F Cカード処理システムにおけるアクティベーション処理手順を示すフローチャート。

[図15]本実施形態を示すN F Cカード処理システムにおけるアクティベーション処理手順を示すフローチャート。

[図16]本実施形態を示すNFCカード処理システムにおけるトークン送信処理サーバによるトークン取得処理手順を示すフローチャート。

[図17]本実施形態を示すNFCカード処理システムにおけるトークン送信処理サーバによるトークン取得処理手順を示すフローチャート。

発明を実施するための形態

[0026] <第1実施形態>

以下、図面を参照しながら本発明の第1実施形態について説明する。

[0027] 図1は、本実施形態を示すNFT配布システムにおけるデータ処理装置の構成を説明する平面図である。本例は、データ処理装置が所定の通信媒体を介して、暗号資産の取引を行う取引所システムと通信可能に構成されているものとする。

[0028] 図1において、1はデータ端末で、後述するハードウェア資源を備えて、所定の標準規格化されたNFCカードに対してデータの書き込み、データの読み出しの処理を行う。なお、本例はEthereumを例とするが、他の暗号資産を扱う取引所と通信可能である。2はカード載置部で、新規NFCカード、情報書き込み済の処理済NFCカードが載置される。3はNFCカード本体で、後述するハードウェア資源を備える。4はキー入力装置で、ユーザが数値情報、アルファベット情報をキー操作で暗証情報が入力される。

[0029] 5は表示デバイスで、カード載置部2に載置されたNFCカード3に入力すべき情報を表示したり、既にNFCカード3に記憶された情報の内容を表示したりする。なお、表示態様はリスト形式とするが、GUI機能を備えることで多種多様なアイコン表示も可能となる。

[0030] なお、NFCカード3の前面および／または背面に表示される識別情報、および接触パッドも含まれる。データ端末1などの他の通信デバイスとの接触を確立するように構成されている。NFCカード3は、所定の記憶部と、データ通信処理回路、アンテナ部を備える。

[0031] 図2は、図1に示したデータ端末1のハードウェア構成を説明するブロック図である。

[0032] 図2において、データ端末1は、CPU1A、ROM1B、RAM1C、入出力インタフェース回路1Dを備え、入出力インタフェース回路1Dは、キー入力装置4の入出力インタフェース回路4Bと通信してデータのやり取りを制御する。キーパッド部4Aには、数値キーと、文字キーとが割り当てられている。

[0033] 通信インタフェース（通信I/F）1Eは、WiFiポート10を介して所定のネットワークに接続して、例えば暗号資産を取り扱う取引所のデータ端末1と双方向に通信可能に構成されている。

[0034] 上記の様に構成されたNFT配布システムは、NFCカード3と、NFCカード3と近接無線通信するデータ端末1とが近接無線通信するNFT配布システムであって、データ端末1は、所有しているNFTを管理するためのウォレットとしてNFCカード3を使用するための秘密鍵を作成し、該作成した秘密鍵を暗号化する暗号機能と、該暗号機能で暗号化した秘密鍵をNFCカード3の記憶媒体に書き込んだ状態で、秘密鍵をNFCカード3の記憶部から消去して、NFTを取引するためのアドレス情報をNFCカード3の記憶部に書き込むように制御するコントローラと、を備えて、以下のフローチャートで示すデータ処理を行う。

[0035] [NFCカード作成処理]

図3は、本実施形態を示すNFT配布システムにおけるデータ処理装置のデータ処理手順の一例を示すフローチャートである。なお、各ステップは、CPU1AがROM1Bに記憶された制御プログラムをRAM1Cに展開して実行することで実現される。まず、NFCカード作成者は、データ端末1のカード載置部2にNFCカード3を載置して読取を指示する（1）。

[0036] CPU1Aは、カード載置部2に載置されたNFCカード3の書き換え可能部に記憶された識別情報の書き込み状態から、このカードが新規カードであるのか、すでにNFTを操作することのできる状態にあるか否かを判断する（2）。ここで、当該NFCカード3が新規カードでないと判断した場合は、当該NFCカード3の書き換え可能部のデータを上書きしてもよいかど

うかを問い合わせるメッセージを表示デバイス5に表示する。ここで、問合せに対してユーザがNOを指示したとCPU1Aが判断した場合、ステップ(1)へ戻る。

[0037] 一方、ステップ(3)で、CPU1Aが上書きしてもよいと判断した場合、当該NFCカード3の書き換え可能部に設定されたカードロックを解除するフラグを立てて、カードロック状態を解除して(4)、ステップ(5)へ進む。

[0038] 一方、ステップ(2)で、載置されたNFCカード3が新規カードであるとCPU1Aが判断した場合、図示しないアプリケーションを実行して、暗号資産の操作に必要な秘密鍵を生成する(5)。

[0039] 次に、キー入力装置4を操作して、例えば4桁の数字を入力する(6)。この数字は、暗号資産や、NFTを検索して表示するための秘密鍵を暗号化するために使用される。

[0040] 次に、CPU1Aは、ステップ(6)で入力された4桁の数字を利用して、所定のビット数で構成されるハッシュを発生させて、ステップ(5)で生成した秘密鍵を暗号化する(7)。

[0041] 次に、ステップ(7)で暗号化された秘密鍵を前記NFCカード3の不揮発性メモリ部に書き込みを行う(8)。

[0042] 次に、CPU1Aは、ステップ(6)で入力された4桁の数字を指定せずにNFCカード3のデータがアクセスされないよう、NFCカード3をロックする(9)。次に、一時的に保存しておいた、ステップ(5)で生成された秘密鍵と、ステップ(7)で暗号化された秘密鍵を不揮発性メモリ部RAM1Cから消去して(10)、データベース(DB)にNFTを参照するためのアドレス情報のみ蓄積して(11)、本処理を終了する。

[0043] 本処理によれば、暗号資産を操作可能なユーザであれば、新規NFCカード3をカード載置部2に載置する簡単な操作で、当該カードに暗号資産やNFTの操作を行う際に利用される秘密鍵を記録し、即座にウォレット機能を持ったNFCカード3を作成することができる。

[0044] また、暗号資産を操作可能なユーザは、上述した手順でNFCカード3を作成することで、秘密鍵のセキュリティを担保しつつ、ウォレットを操作性にすぐれたNFCカード3として所持、使用することが可能となる。

[0045] 〔秘密鍵取得処理〕

図4は、本実施形態を示すNFT配布システムにおけるデータ処理装置のデータ処理手順の一例を示すフローチャートである。なお、(21)～(26)は各ステップを示し、各ステップは、CPU1AがROM1Bに記憶された制御プログラムをRAM1Cに展開して実行することで実現される。まず、NFCカード所有者は、データ端末1のカード載置部2にNFCカード3を載置(セット)して読取を指示する(21)。

[0046] CPU1Aは、カード載置部2に載置されたNFCカード3の書き換え可能部に記憶された識別情報の書き込み状態から、このカードが新規カードであるのか、すでにNFTを操作することのできる状態にあるか否かを判断する(23)。ここで、当該NFCカード3が新規カードであるとCPU1Aが判断した場合、表示デバイス5に書き込み済のカードをセットしてくださいとメッセージを表示して(22)、ステップ(21)へ戻る。

[0047] 一方、ステップ(22)で、キー入力装置4を操作して、例えば4桁の数字を入力する(24)。

[0048] 次に、CPU1Aはステップ(24)で入力された数値情報を用い、NFCカード3に記録されている暗号化されている秘密鍵を復号化する処理を実行する(25)。次に、復号した秘密鍵を表示デバイス5に表示して(26)、本処理を終了する。

[0049] これにより、カード保持者は、秘密鍵の内容を何ら知得しておく必要がなく、暗証番号を入力することで確認できた秘密鍵を操作して、暗号資産の内容を確認するために設定された取引所のアカウントに接続すると、表示デバイス5を通して所有するNFTや暗号資産に対する操作を行うことができる。

[0050] 本実施形態によれば、NFCカード媒体を利用して、所有するNFTおよ

び暗号資産を簡単な操作で、データ端末1上で確認・操作することができるカード型のウォレットを普及させることができる。

[0051] なお、本システムにおいて、暗号資産は、ビットコイン（BTC：登録商標）、イーサリアム（ETH：登録商標）、ライトコイン（LTC）、及びモナコイン（MONA：登録商標）などいずれにも対応可能である。

[0052] <第1実施形態の効果>

本実施形態によれば、NFCカード媒体を利用して、所有するNFTおよび暗号資産を簡単な操作で、データ端末上で確認・操作することができる。

[0053] <第2実施形態>

図5は、本実施形態を示すNFCカード処理システムの構成を説明するブロック図である。本実施形態では、所定の通信媒体（ネットワークNET）を介して、第1の実施形態に一例を示すNFCカード3と近接無線通信するデータ端末1と、データ端末1が読み取る前記NFCカード3のアクティベーション処理を複数のシステム管理サーバと連携して行うNFCカード処理システムを例として、アクティベーション処理方法について詳述する。

[0054] また、本実施形態では、データ端末1として、NFCカード3を読み取り可能なICチップを備えるスマートフォンを例とするが、データ端末1は、これに限らず無線通信機能を備える各種のPADデバイスが含まれる。

[0055] 図5において、SB1はブロックチェーンサーバで、図示しない取引所が管理する複数の仮想通貨管理サーバから構成されている。仮想通貨例としては、Ethereum、Polygon、Asterがある。

[0056] SB2は所有確認サーバで、後述する手順に基づいてNFCカード3を所有するユーザに対して所有確認処理を実行する。

[0057] SB3は動的QRサーバで、後述する手順に基づいてQRコード（登録商標）を表示用端末上でQRコード（登録商標）で特定されるQRページを表示する処理を実行する。

[0058] SB4はブロックチェーン巡回サーバで、後述する手順に基づいてブロックチェーン巡回処理を実行する。

[0059] S B 5 はプリアクティベーションサーバで、N F C カード 3 の有効性を判断するための処理を実行する。

[0060] なお、ブロックチェーンサーバ S B 1、所有確認サーバ S B 2、動的 Q R サーバ S B 3、ブロックチェーン巡回サーバ S B 4、プリアクティベーションサーバ S B 5 は、コンピュータシステムとしてネットワークに接続して所定のデータ処理を実行するためのハードウェア資源（C P U、R A M、大容量メモリ、ネットワーク制御システム等）を備えるが、その詳細については省略する。なお、ブロックチェーンサーバ S B 1、所有確認サーバ S B 2、動的 Q R サーバ S B 3、ブロックチェーン巡回サーバ S B 4、プリアクティベーションサーバ S B 5、トークン送信処理サーバ S B 6、アクティベーションサーバ S B 7 は、システム管理サーバの一例である。

[0061] 図 6 は、図 5 に示した所有確認サーバ S B 2 の機能処理を説明するブロック図である。各部は、記憶部に記憶されたソフトウェアを実行することにより実現される。

[0062] 図 6 において、6 1 は所有データベース（所有 D B）で、N F C カード 3 の所有者が登録されている。6 2 は N F T 閲覧機能処理部で、所有データベース（所有 D B）6 1 に登録された N F C カード 3 の所有者に N F T 閲覧機能処理サービスを提供する。6 3 は N F T 表示機能処理部で、所有データベース（所有 D B）6 1 に登録された N F C カード 3 の所有者に N F T 表示機能処理サービスを提供する。

[0063] 図 7 は、図 5 に示した所有確認サーバ S B 2 による所有確認シーケンスの一例を示すフローチャートである。（7 1）～（7 5）は各ステップを示す。

[0064] ユーザが所有する N F C カード 3（第 1 実施形態で示した処理に基づいて作成される N F C カード）をユーザが操作するデータ端末 1 としてのスマートフォンの I C チップ読取部に翳すと（7 1）、データ端末 1 は、契約キャリアに従う無線ネットワークを介して所有確認サーバ S B 2 に接続するためのリンク先を表示ボタンとしてスマートフォンの画面に表示した状態で、ユ

ーザが表示ボタンをタップすると（７２）、ユーザが登録した所有情報ページの取得する要求が所有確認サーバＳＢ２に通知される。

[0065] これに所有確認サーバＳＢ２が応答し、ユーザが操作するデータ端末１から送られてきたリンクのアドレス情報に基づいてデータベースを検索し（７３）、ＮＦＴの所有情報ページを読み出してユーザが操作するデータ端末１に返却する（７４）。

[0066] これを受けて、データ端末１のコントローラ部は、ユーザが操作するデータ端末１の画面に、所有確認サーバＳＢ２が記憶して管理しているＮＦＴの所有情報ページを表示する（７５）。

[0067] 図８は、図５に示したプリアクティベーションサーバＳＢ５の機能処理を説明するブロック図である。各部は、ハードウェア資源として構成されるコントローラが記憶部に記憶されたソフトウェア（プログラム）を実行することにより実現される。

[0068] 図８において、８１はプリアクティベーションデータベース（プリアクティベーションＤＢ）で、ＮＦＣカード３のプリアクティベーションに必要なカード有効化処理に必要な情報を記憶している。

[0069] ８２はデータベース管理機能処理部（ＤＢ管理機能処理部）で、プリアクティベーションＤＢ８１に登録されたプリアクティベーションページをユーザが操作するデータ端末１に提供するサービスを行う。

[0070] 図９は、図５に示したプリアクティベーションサーバＳＢ５によるシーケンスの一例を示すフローチャートである。（８１）～（８６）は各ステップを示す。

[0071] プリアクティベーションサーバＳＢ５は、所有確認サーバＳＢ２より、所有確認処理が終了した旨の通知を受けると、データ端末１を操作するユーザに対して、プリアクティベーションページを送信する（８１）。次に、ユーザは、プリアクティベーションサーバＳＢ５から通知されたプリアクティベーションページを開く操作を行うとともに（８２）、ＮＦＣカード３をデータ端末１のＩＣチップ読取部に翳すと（８３）、ＮＦＣカード３内に記憶さ

れたNFC情報がプリアクティベーションサーバSB5に送信される。

[0072] プリアクティベーションサーバSB5は、送信されたNFC情報を取得したら、NFC情報から抽出されるUID（固体識別番号）をプリアクティベーションDB81に保存する処理を実行し（84）、プリアクティベーションサーバSB5は、UID（固体識別番号）の保存の可否を判別した結果をユーザが操作するデータ端末1に送信する（85）。

[0073] これを受けて、ユーザが操作するデータ端末1のコントローラ部は、プリアクティベーションサーバSB5から送信された保存の成功／失敗のいずれかを表示する（86）。

[0074] これにより、プリアクティベーションが正常に終了したNFCカード3は、仮想通貨取引のためのカード媒体を有効化する処理がユーザの手元で完了する。

[0075] 図10は、図5に示した動的QRサーバSB3による機能処理を説明するブロック図である。各部は、記憶部に記憶されたソフトウェアを実行することにより実現される。

[0076] 図10において、101はQR画像生成機能処理部で、図5に示した動的QRサーバSB3は、後述するトークン送信処理サーバSB6によるトークン情報の受け取りに使用するQRコード（登録商標）を生成する処理を実行する。

[0077] 102は表示用端末で、動的QRサーバSB3により生成されたQRコード（登録商標）を表示する。表示用端末102は、ユーザが操作するデータ端末1の画面とするが、他の表示デバイスであってもよい。

[0078] 図11は、図5に示した動的QRサーバSB3による機能処理を説明するフローチャートである。なお、（111）～（113）は各ステップを示す。

[0079] NFCカード処理システムとして連携する動的QRサーバSB3は、プリアクティベーションが有効に完了したことをプリアクティベーションサーバSB5より通知を受けると、トークン送信処理に利用するQRコード（登録

商標)を即時生成して(111)、ネットワークNETを介して表示用端末102に送信する。これにより、QRページが表示用端末102に表示される(112)。次に、一定間隔でページを自動更新して(113)、ステップ(111)へ戻る。

[0080] 図12は、図5に示したブロックチェーン巡回サーバSB4が参照するデータベースの対応を説明するブロック図である。本実施形態では、クロールデータベース(クロールDB)1201と、所有データベース(所有DB)1202とを備える。

[0081] 図12において、クロールデータベース(クロールDB)1201には、ブロックチェーン上のデータをどこまで読み込んだかのデータが記録されている。

[0082] 具体的には、ブロックチェーンのデータの位置を一意に示すブロックナンバーという整数値が記録されている。これを参照することにより、ブロックチェーン巡回サーバSB4が所有データベース1202を更新する際に、全てのブロックチェーンを読むことなく未取得分データを取得することが可能になる。

[0083] 所有データベース1202には、どのユーザがどのトークンを保有しているかというデータが記録されている。

[0084] 具体的には、トークンを一意に示す文字列(アドレス)と整数値(トークンID)、そして、所有者のアドレス情報が記憶されている。

[0085] ブロックチェーン上には、すべてのトークンの所有者とその遷移が記録されているが、所有データベース1202には、ブロックチェーン上のデータをもとに作成された最終確認時点での所有情報のみが記録される。

[0086] 図13は、図5に示したブロックチェーン巡回サーバSB4による機能処理を説明するフローチャートである。なお、(1301)～(1305)は各ステップを示す。

[0087] ブロックチェーン巡回サーバSB4は、図12に示したクロールDB1201とブロックチェーン1201-1とから情報を取得し(1301)、最

最新のブロックまで読み取ったかどうかを判断し（１３０２）、最新のブロックまで読み取っていると判断した場合、（１３０５）へ進み、所定時間（例えば１分）待機した後（１３０５）、ステップ（１３０１）へ戻る。

[0088] 一方、ステップ（１３０２）で、最新のブロックまで読み取っていないと判断した場合、最新ブロックに到達するまで情報を読み込む処理を実行する（１３０３）。

[0089] 次に、所有ＤＢ１２０２に最新の情報を書き込む処理を実行して（１３０４）、ステップ（１３０５）へ進む。これにより、所有ＤＢには、ブロックチェーン上に記録されているものと同様の、最新のトークンの所有者情報が保存されることとなる。この所有ＤＢを参照することで、本システムおよび関連システムがトークンの所有者情報を参照する必要がある場合、ブロックチェーンを参照する場合と比べ、高速かつ低コストで最新のトークンの所有者情報を取得することができる。

[0090] 図１４、図１５は、本実施形態を示すＮＦＣカード処理システムにおけるアクティベーション処理手順を示すフローチャートである。なお、（１４０１）、（１４０２）はサーバ側のコントローラが実行する各ステップを示し、（１４２１）～（１４３０）はユーザ端末側のコントローラが実行するステップを示す。また、本処理におけるアクティベーションサーバＳＢ７は、アクティベーションサーバＳＢ５が機能処理を兼ねる構成としてもよい。

[0091] データ端末１は、ＮＦＣカード３に記憶されたＮＦＣタグの情報を読み取り（１４２１）、無線通信によりネットワークＮＥＴを介してＮＦＣ情報をアクティベーションサーバＳＢ７に送信する。

[0092] これを受けて、アクティベーションサーバＳＢ７は、図８に示したプリアクティベーションＤＢ８１に登録されたＵＩＤと一致するかどうかをチェックする（１４０１）。

[0093] そして、アクティベーションサーバＳＢ７は、ステップ（１４２１）で送信されたＮＦＣ情報に含まれるＵＩＤが登録済か否かの判断結果をデータ端末１側に送信する。

- [0094] 次に、データ端末1は、アクティベーションサーバSB7から送信された結果、ステップ(1421)で送信したNFC情報に含まれるUIDが既に登録されているか否か、すなわちプリアクティベーション済であるか否かを判断する(1422)。
- [0095] ここで、データ端末1は、ステップ(1421)で送信したNFC情報に含まれるUIDが既に登録されていないと判断した場合、データ端末1にプリアクティベーション失敗を表示して(1423)、処理を終了する。
- [0096] 一方、ステップ(1422)で、ステップ(1421)で送信したNFC情報に含まれるUIDが既に登録されていると判断した場合、データ端末1にインストールされているアクティベーションアプリケーションを起動して、鍵ペアを生成する(1424)。
- [0097] 次に、ユーザは、データ端末1の表示画面に表示されたパスワード入力表示に従い、所望のパスワード(8文字以上、大文字小文字英数記号を含む)を入力する(1425)。
- [0098] 次に、ステップ(1424)で生成されたNFCタグのセキュア領域に与えられたパスワードでロックして保存し、ステップ(1425)で生成されたパスワードをアプリ内のセキュア領域に保存する(1426)。次に、ステップ(1424)で生成された公開鍵(アドレス)とUIDを署名付きでプリアクティベーションサーバSB7に送信する(1427)。
- [0099] これを受けて、アクティベーションサーバSB7は、ステップ(1427)でユーザが操作するデータ端末1から送信された署名を検証し、UIDに公開鍵(アドレス)を紐づけてアクティベーションDB81-2に保存する処理を実行する(1402)。
- [0100] そして、アクティベーションサーバSB7は、ステップ(1427)でデータ端末1から送信された公開鍵、UIDをプリアクティベーションDB81-2に対して正常に保存処理が完了しているか、または正常に保存処理が完了していないかの成功、失敗を示すコードを結果として送信する。
- [0101] これを受けて、データ端末1では、アクティベーションサーバSB7から

送信された登録処理が成功しているか失敗しているか、すなわち成功を送信しているかどうかを判断し（１４２８）、送信を成功していると判断した場合は、データ端末１の画面にアクティベーション成功の旨を表示して（１４２９）、処理を終了する。

[0102] 一方、ステップ（１４２８）で、アクティベーションサーバＳＢ７から送信された登録処理が失敗していると判断した場合、データ端末１の画面にアクティベーション失敗の旨を表示して（１４３０）、処理を終了する。

[0103] これにより、サーバは、データ端末１で生成された公開鍵（アドレス）とＵＩＤを記録したアクティベーションDBを参照することで、ＵＩＤに対応するアドレスに対してトークンの送付等の操作を行うことができる。

また、データ端末１にサーバからアクティベーションの結果を送付することで、アクティベーションの結果によって、データ端末１の機能を切り替えることができる。

[0104] 具体的には、アクティベーション成功時は、所有するトークンの表示、アクティベーションが失敗時は、アクティベーションの再実行などである。

[0105] 図１６、図１７は、本実施形態を示すＮＦＣカード処理システムにおけるトークン送信処理サーバＳＢ６によるトークン取得処理手順を示すフローチャートである。なお、（１５１１）、（１５１２）はサーバ側の各ステップを示し、（１５０１）～（１５０８）はデータ端末１側のステップを示す。

[0106] データ端末１は、図５に示した動的ＱＲサーバＳＢ３から受け取るＱＲコード（登録商標）またはＮＦＣカード３に記憶されたＮＦＣタグを読み取る（１５０１）。ここで、データ端末１からトークン送信処理サーバＳＢ６にトークン情報を要求して取得したら（１５０２）、トークン送信処理サーバＳＢ６は、トークン情報ＤＢ１２０２－２から読み出すトークン情報をデータ端末１に返却する（１５１１）。

[0107] これを受けて、データ端末１は、ステップ（１５０２）で、トークン送信処理サーバＳＢ６から受け取るトークン情報を取得する。次に、受け取るトークン情報の中からＮＦＣタグを選択して、データ端末１にＮＦＣカード３

を翳す（１５０３）。

[0108] 次に、データ端末１は、アプリのセキュア領域に保存されているパスワードを読み取り、NFCタグのセキュア領域に保存されている秘密鍵を読み込む（１５０４）。

[0109] 次に、データ端末１のコントローラは、UIDおよびステップ（１５０２）でトークン送信処理サーバＳＢ６から受け取るトークン情報を秘密鍵による署名付きでトークン送信処理サーバＳＢ６に送信する（１５０５）。

[0110] これを受けて、トークン送信処理サーバＳＢ６は、データ端末１から送信された署名を検証し、対象アドレスにトークンを送信する処理を開始する（１５１２）。

[0111] これにより、トークン送信処理サーバＳＢ６は、ブロックチェーン１２０２－１または所有ＤＢ６１へのアクセスを行うことが可能となる。

[0112] 次に、データ端末１は、トークン送信処理サーバＳＢ６がブロックチェーン１２０２－１または所有ＤＢ６１から情報の読み出しが成功したかどうかを示す情報をトークン送信処理サーバＳＢ６から受信しているかどうかを判断し（１５０６）、データ端末１のコントローラは、成功していないと判断した場合、ブロックチェーン１２０２－１または所有ＤＢ６１から情報の読み出しを失敗した旨を表示して（１５０８）、処理を終了する。

[0113] 一方、ステップ（１５０６）で、データ端末１のコントローラは、成功していると判断した場合、ブロックチェーン１２０２－１または所有ＤＢ６１から情報の読み出しを成功した旨を表示して（１５０７）、処理を終了する。

[0114] ＜第２実施形態の効果＞

本実施形態によれば、図１５に示したステップ（１４２２）でプリアクティベーション済のカードかを確認することで、正規品以外のNFCを用いた本システムの利用を制限することができる。

[0115] また、図１５のステップ（１４２７）で署名を検証することで、秘密鍵所有者以外が不正に公開鍵（アドレス）をデータベースに登録することを防止

することができる。

[0116] さらに、図 1 3 に示したフローチャートで最新の所有情報を所有 D B に保管しておくことで、外部の取引所等の機能に依存することなく、ユーザが所有する N F T の数、最新の暗号資産の総額等を容易に確認することができる。

[0117] また、図 1 6 のステップ (1 5 1 2) で署名を検証することで、カードの所有者がトークンの受け取り者であることを確認することができる。

[0118] なお、上記実施形態では、複数のシステム管理サーバをシステム構成とする場合について説明したが、それぞれのシステム管理サーバが機能連携処理を行うサーバ構成とすることで、システム管理サーバの台数を減らすことも可能である。

[0119] 以上の記載した本発明に関する開示は、少なくとも下記事項に要約することができる。

[0120] (1) 所定の N F C カードと、前記 N F C カードと近接無線通信するデータ端末とが近接無線通信する N F T 配布システムであって、前記データ端末は、所有している N F T を管理するためのウォレットとして前記 N F C カードを使用するための秘密鍵を作成し、該作成した前記秘密鍵を暗号化する暗号化手段と、前記暗号化手段が暗号化した前記秘密鍵を前記 N F C カードの記憶媒体に書き込んだ状態で、前記秘密鍵を前記記憶媒体から消去して、前記 N F T を取引するためのアドレス情報を前記記憶媒体に書き込むように制御する制御手段と、を備えることを特徴とする。

[0121] (2) 所定の N F C カードと、前記 N F C カードと近接無線通信するデータ端末とが近接無線通信する N F T 配布システムのウォレットカード作成方法であって、前記データ端末は、所有している N F T を管理するためのウォレットとして前記 N F C カードを使用するための秘密鍵を作成し、該作成した前記秘密鍵を暗号化する暗号化ステップと、前記暗号化ステップが暗号化した前記秘密鍵を前記 N F C カードの記憶媒体に書き込んだ状態で、前記秘密鍵を前記記憶媒体から消去して、前記 N F T を取引するためのアドレス情報

を前記記憶媒体に書き込むように制御する制御ステップと、を備えることを特徴とする。

[0122] (3) 所定の通信媒体を介して、N F Cカードと近接無線通信するデータ端末と、前記データ端末が読み取る前記N F Cカードのアクティベーション処理を複数のシステム管理サーバと連携して行うN F Cカード処理システムのアクティベーション処理方法であって、前記複数のシステム管理サーバのうち、いずれか1つのシステム管理サーバを介して前記N F Cカードに対してプリアクティベーション処理を実行して前記N F CカードのU I Dをプリアクティベーションデータベースに登録する第1の登録ステップと、前記複数のシステム管理サーバのうち、いずれか1つのシステム管理サーバを介して前記N F Cカードに対してプリアクティベーション処理が終了している処理済N F Cカードに対してアクティベーション処理を実行してアクティベーションデータベースに生成される公開鍵と、U I Dとを紐づけて登録する第2の登録ステップと、を備えることを特徴とする。

[0123] (4) 前記公開鍵は、前記データ端末で起動されるアプリケーションが生成することを特徴とする。

[0124] (5) 複数のシステム管理サーバは、前記N F Cカードに対するプリアクティベーション処理を行う第1のシステム管理サーバと、前記N F Cカードに対するアクティベーション処理を行う第2のシステム管理サーバと、仮想通貨の情報をブロックチェーンに紐づけて管理する第3のシステム管理サーバと、前記N F Cカードの所有情報を管理する第4のシステム管理サーバと、を含むことを特徴とする。

[0125] (6) 前記データ端末は、前記N F Cカードに対するアクティベーション処理を行う第2のシステム管理サーバと通信する際、前記N F Cカードが既にプリアクティベーション済であるかどうかを判断する判断ステップと、前記判断ステップで、前記N F Cカードが既にプリアクティベーション済であるかどうかを判断した場合、秘密鍵と前記公開鍵のペア鍵を生成する生成ステップと、所望のパスワードを入力する入力ステップと、前記秘密鍵をN F C

タグのセキュア領域に与えられた前記所望のパスワードでロックして保存するとともに、前記所望のパスワードをアプリケーション内のセキュア領域に保存する保存ステップと、前記公開鍵とU I Dを署名付きでいずれかのシステム管理サーバに送信する送信ステップと、を備えることを特徴とする。

符号の説明

- [0126] 1 データ端末
- 2 カード載置部
- 3 N F Cカード本体（N F Cカード）
- 4 キー入力装置
- 5 表示デバイス
- S B 1 ブロックチェーンサーバ
- S B 2 所有確認サーバ
- S B 3 動的Q Rサーバ
- S B 4 ブロックチェーン巡回サーバ
- S B 5 プリアクティベーションサーバ
- S B 6 トークン送信処理サーバ
- S B 7 アクティベーションサーバ

請求の範囲

- [請求項1] 所定のN F Cカードと、前記N F Cカードと近接無線通信するデータ端末とが近接無線通信するN F T配布システムであって、
- 前記データ端末は、
- 所有しているN F Tを管理するためのウォレットとして前記N F Cカードを使用するための秘密鍵を作成し、該作成した前記秘密鍵を暗号化する暗号化手段と、
- 前記暗号化手段が暗号化した前記秘密鍵を前記N F Cカードの記憶媒体に書き込んだ状態で、前記秘密鍵を前記記憶媒体から消去して、前記N F Tを取引するためのアドレス情報を前記記憶媒体に書き込むように制御する制御手段と、
- を備えることを特徴とするN F T配布システム。
- [請求項2] 所定のN F Cカードと、前記N F Cカードと近接無線通信するデータ端末とが近接無線通信するN F T配布システムのウォレットカード作成方法であって、
- 前記データ端末は、
- 所有しているN F Tを管理するためのウォレットとして前記N F Cカードを使用するための秘密鍵を作成し、該作成した前記秘密鍵を暗号化する暗号化ステップと、
- 前記暗号化ステップが暗号化した前記秘密鍵を前記N F Cカードの記憶媒体に書き込んだ状態で、前記秘密鍵を前記記憶媒体から消去して、前記N F Tを取引するためのアドレス情報を前記記憶媒体に書き込むように制御する制御ステップと、
- を備えることを特徴とするN F T配布システムのウォレットカード作成方法。
- [請求項3] 所定の通信媒体を介して、N F Cカードと近接無線通信するデータ端末と、前記データ端末が読み取る前記N F Cカードのアクティベーション処理を複数のシステム管理サーバと連携して行うN F Cカード

処理システムのアクティベーション処理方法であって、

前記複数のシステム管理サーバのうち、いずれか1つのシステム管理サーバを介して前記N F Cカードに対してプリアクティベーション処理を実行して前記N F CカードのU I Dをプリアクティベーションデータベースに登録する第1の登録ステップと、

前記複数のシステム管理サーバのうち、いずれか1つのシステム管理サーバを介して前記N F Cカードに対してプリアクティベーション処理が終了している処理済N F Cカードに対してアクティベーション処理を実行してアクティベーションデータベースに生成される公開鍵と、U I Dとを紐づけて登録する第2の登録ステップと、
を備えることを特徴とするN F Cカード処理システムのアクティベーション処理方法。

[請求項4] 前記公開鍵は、前記データ端末で起動されるアプリケーションが生成することを特徴とする請求項3に記載のN F Cカード処理システムのアクティベーション処理方法。

[請求項5] 複数のシステム管理サーバは、
前記N F Cカードに対するプリアクティベーション処理を行う第1のシステム管理サーバと、
前記N F Cカードに対するアクティベーション処理を行う第2のシステム管理サーバと、
仮想通貨の情報をブロックチェーンに紐づけて管理する第3のシステム管理サーバと、
前記N F Cカードの所有情報を管理する第4のシステム管理サーバと、
を含むことを特徴とする請求項3に記載のN F Cカード処理システムのアクティベーション処理方法。

[請求項6] 前記データ端末は、
前記N F Cカードに対するアクティベーション処理を行う第2のシ

システム管理サーバと通信する際、

前記N F Cカードが既にプリアクティベーション済であるかどうかを判断する判断ステップと、

前記判断ステップで、前記N F Cカードが既にプリアクティベーション済であるかどうかを判断した場合、秘密鍵と前記公開鍵のペア鍵を生成する生成ステップと、

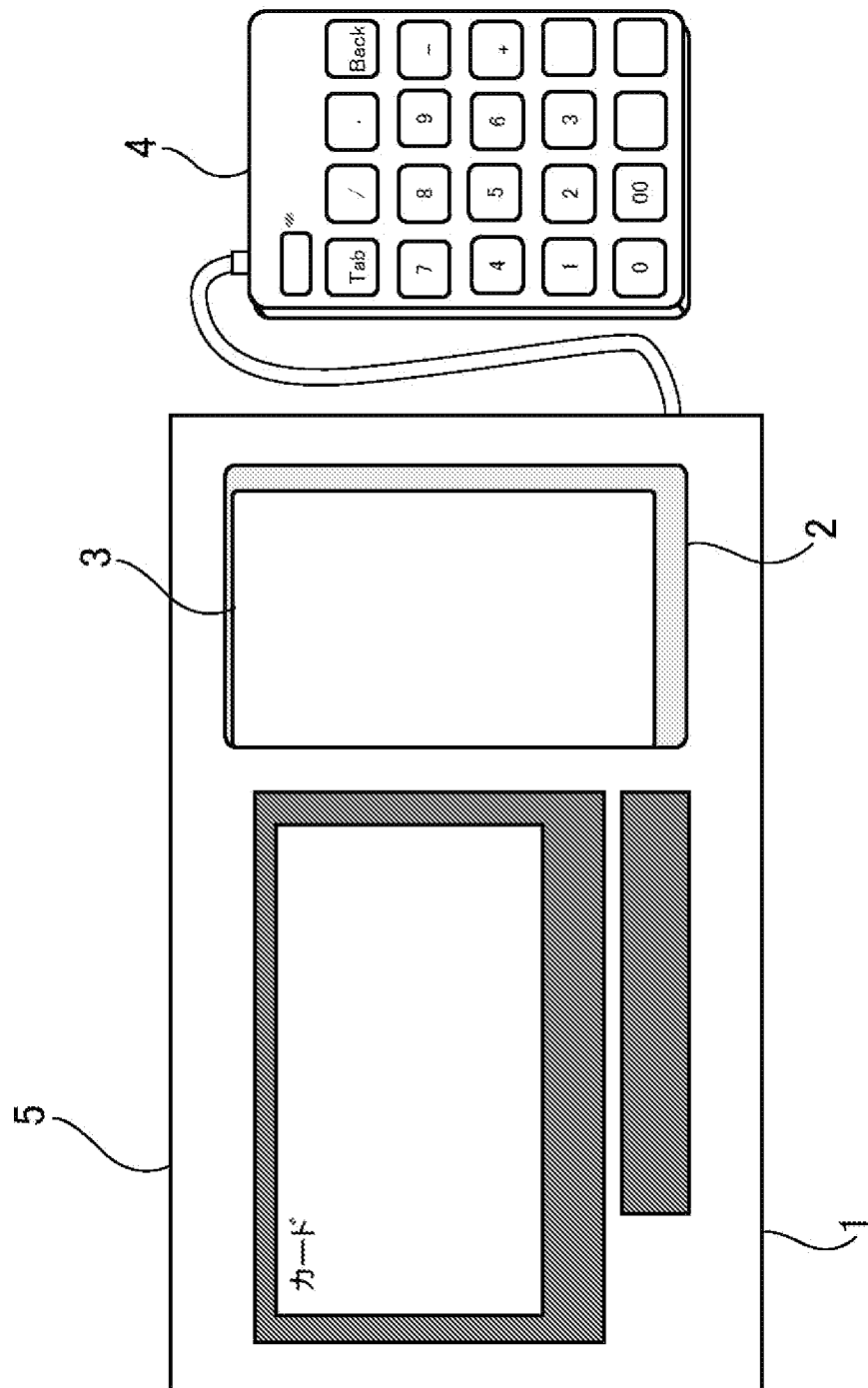
所望のパスワードを入力する入力ステップと、

前記秘密鍵をN F Cタグのセキュア領域に与えられた前記所望のパスワードでロックして保存するとともに、前記所望のパスワードをアプリケーション内のセキュア領域に保存する保存ステップと、

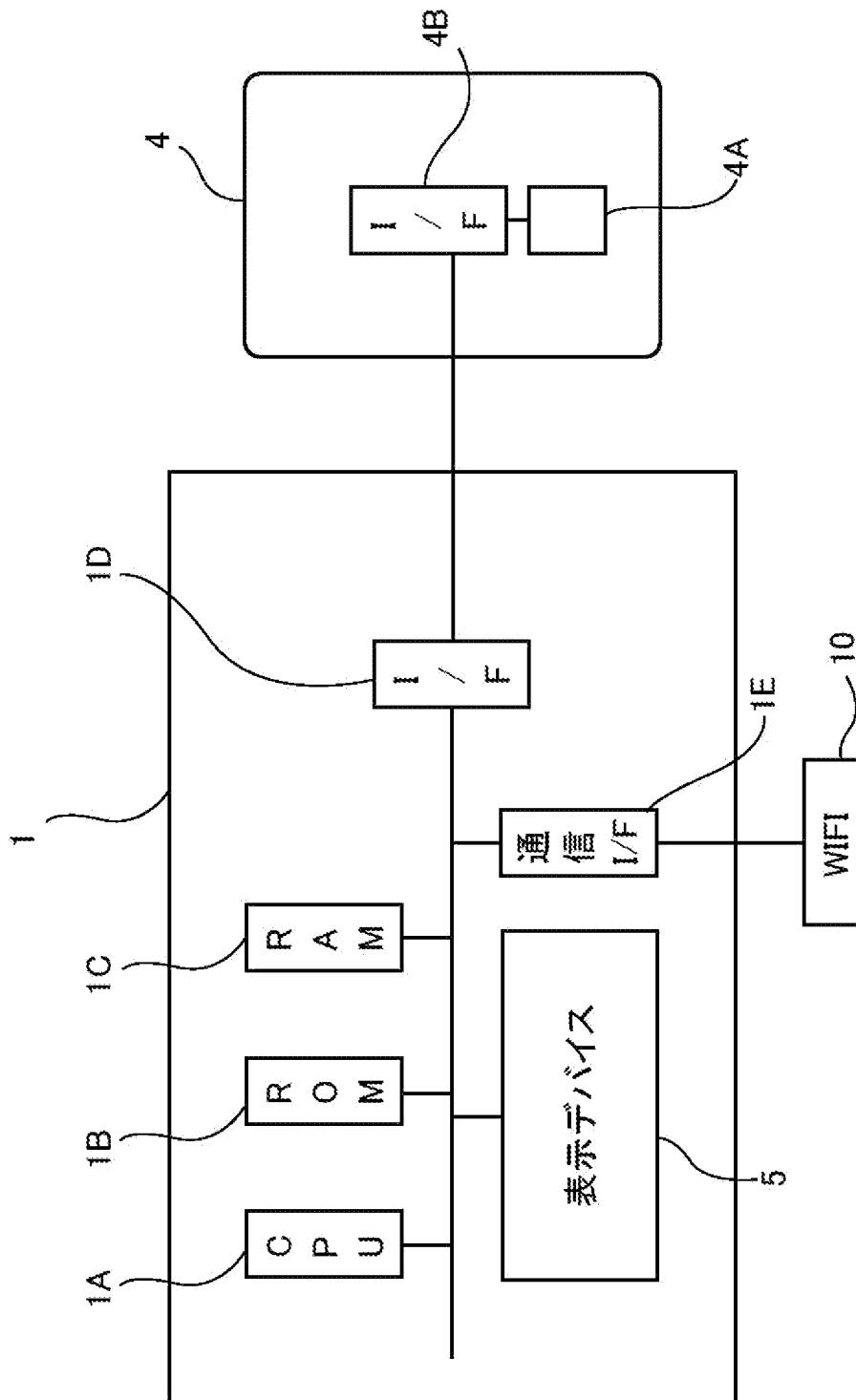
前記公開鍵とU I Dを署名付きでいずれかのシステム管理サーバに送信する送信ステップと、

を備えることを特徴とする請求項3に記載のN F Cカード処理システムのアクティベーション処理方法。

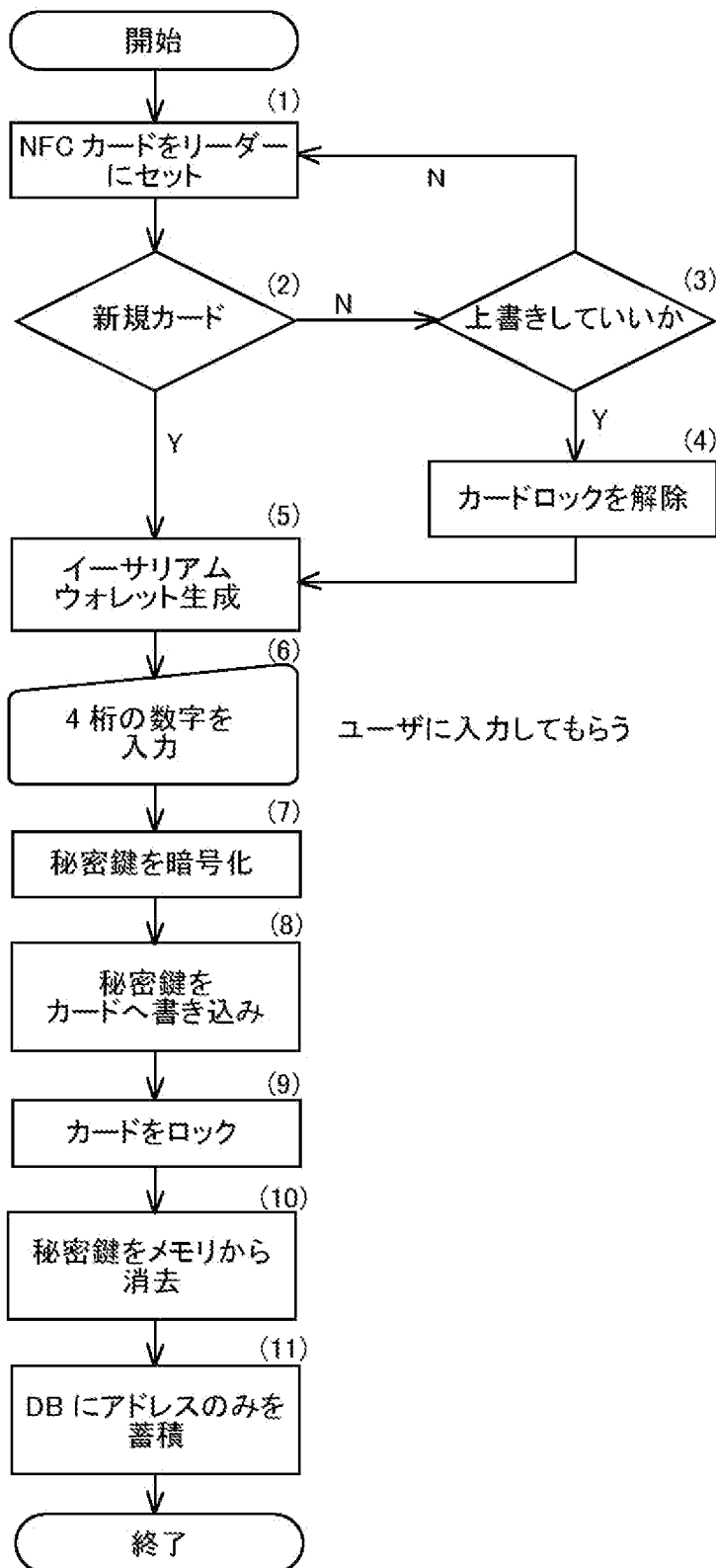
[図1]



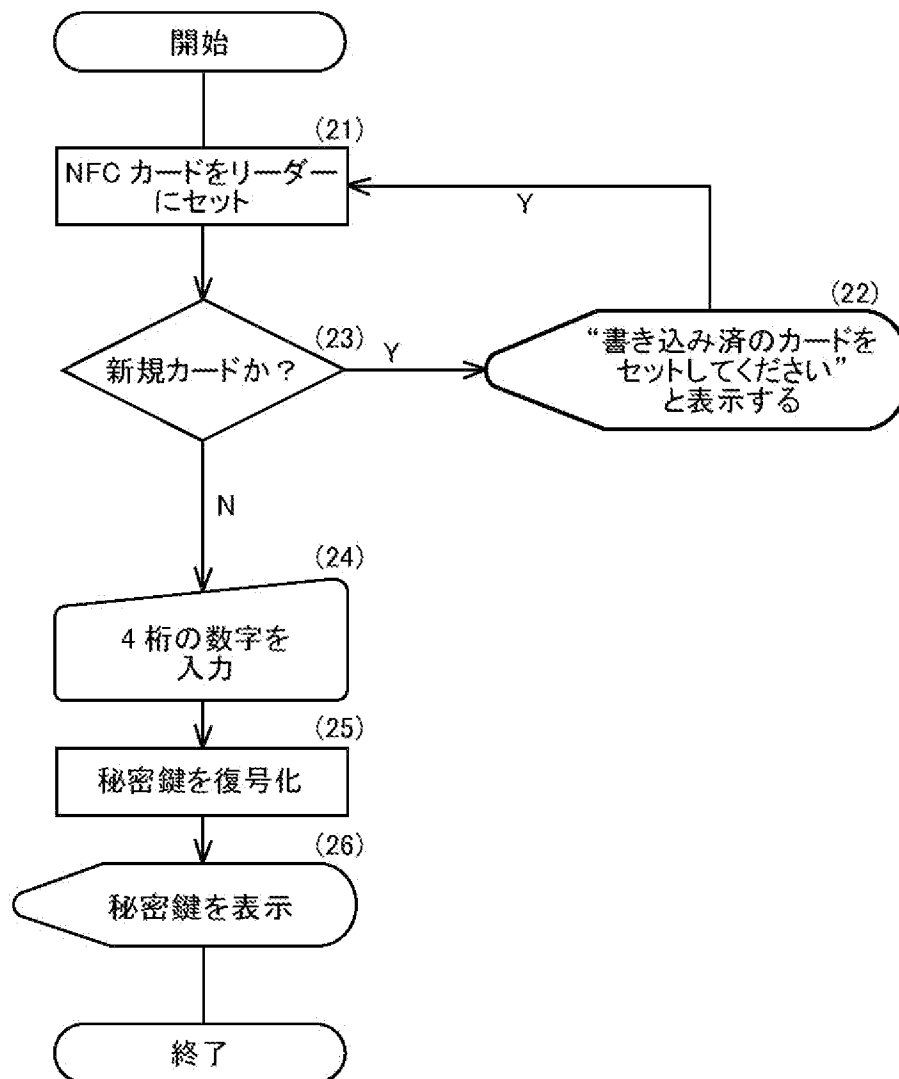
[図2]



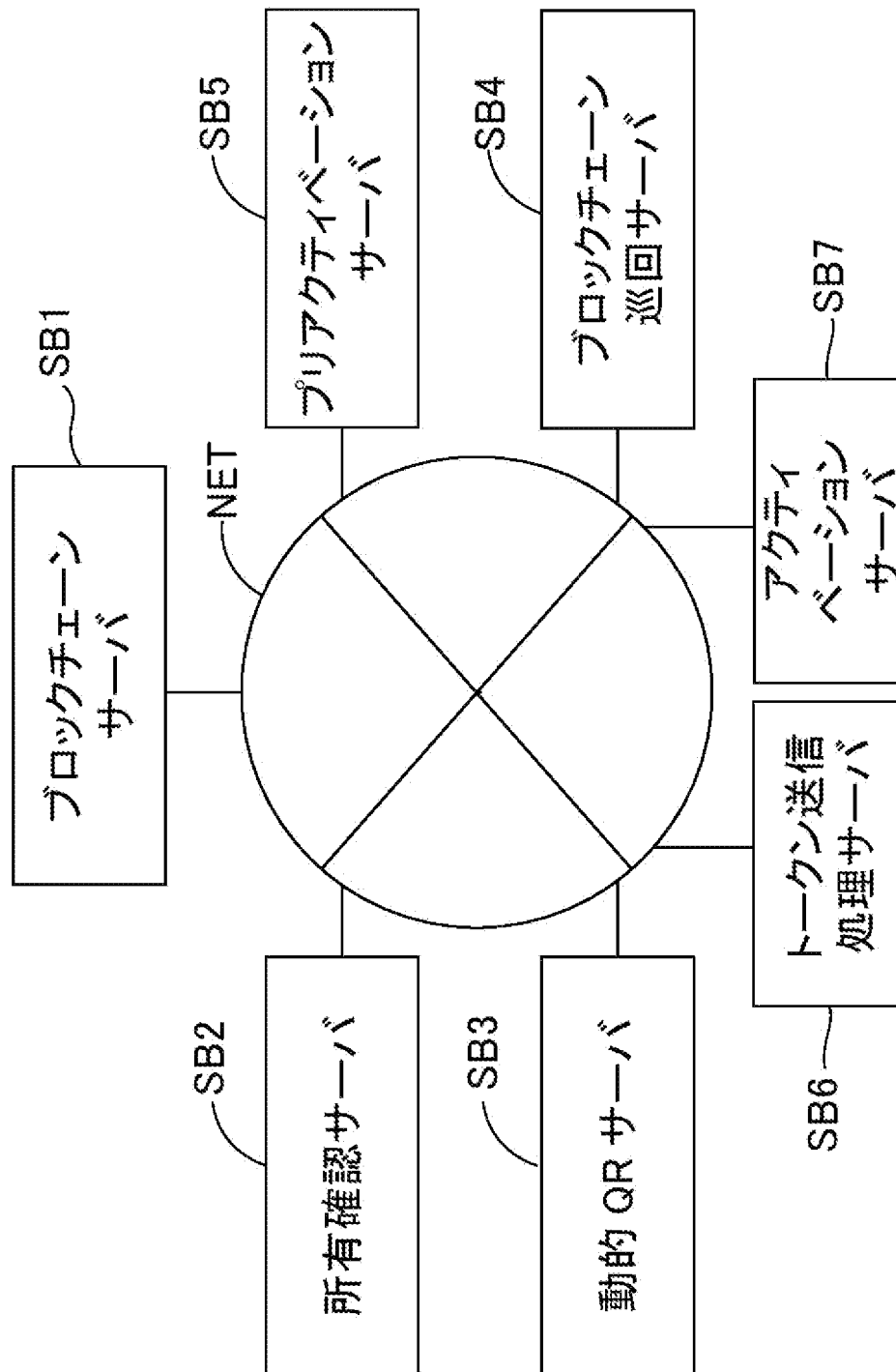
[図3]



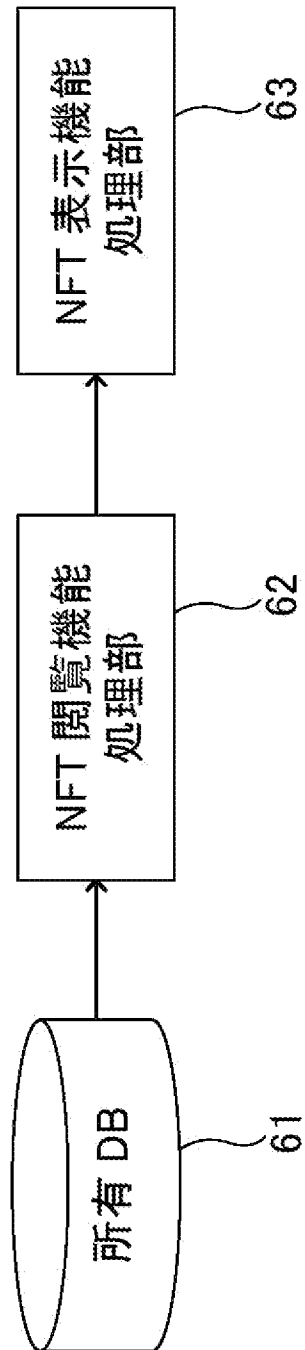
[図4]



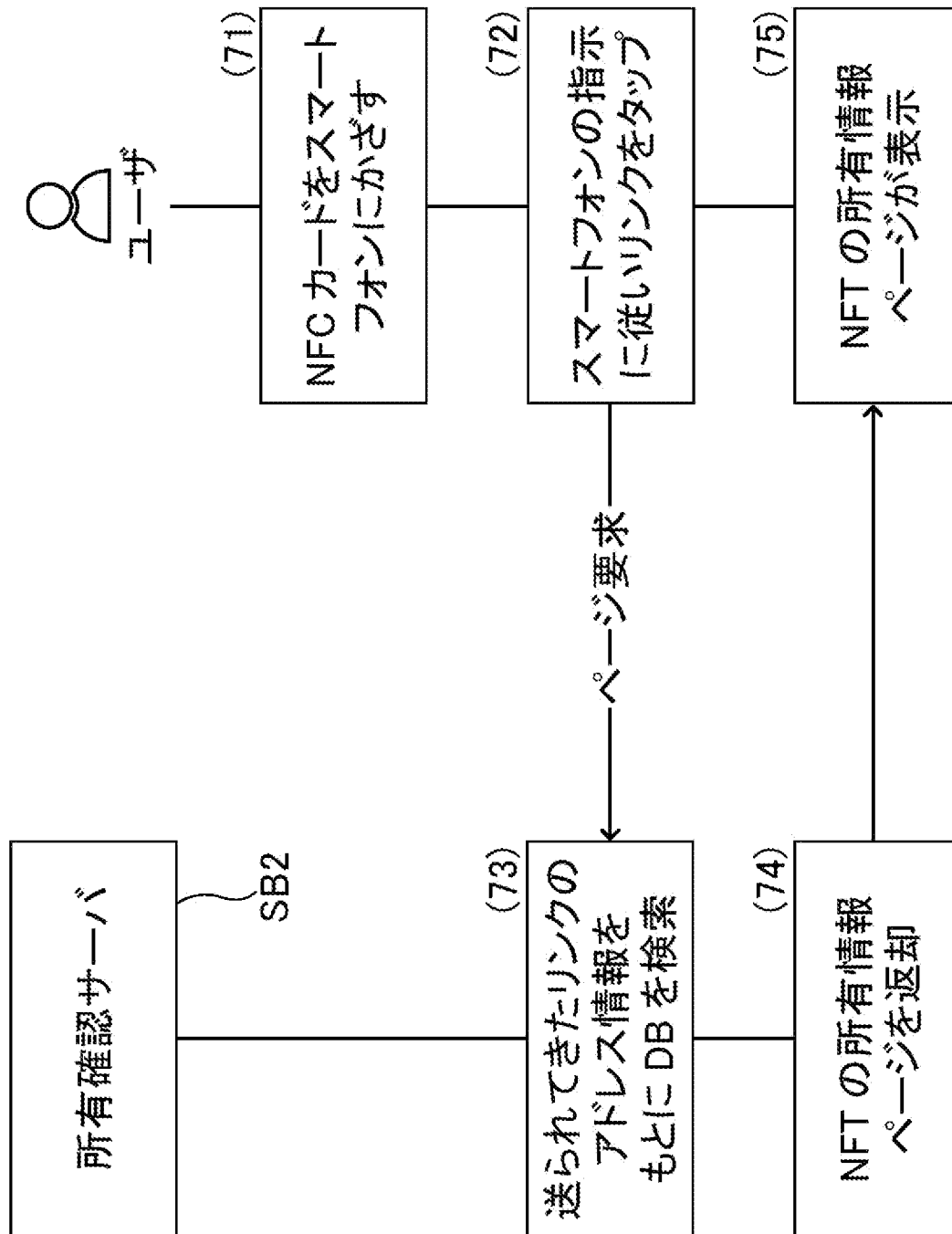
[図5]



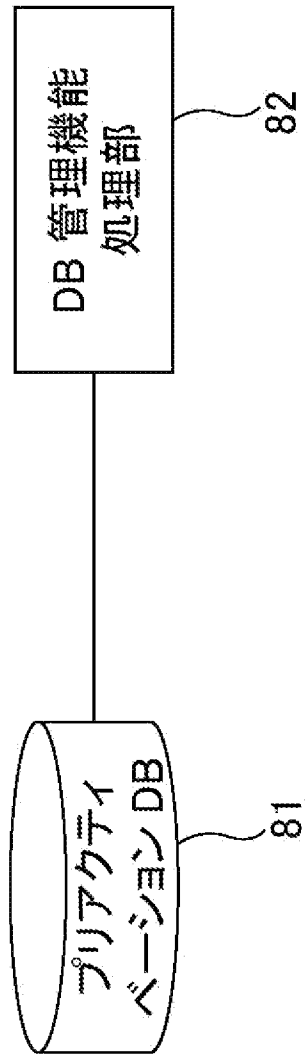
[図6]

SB2

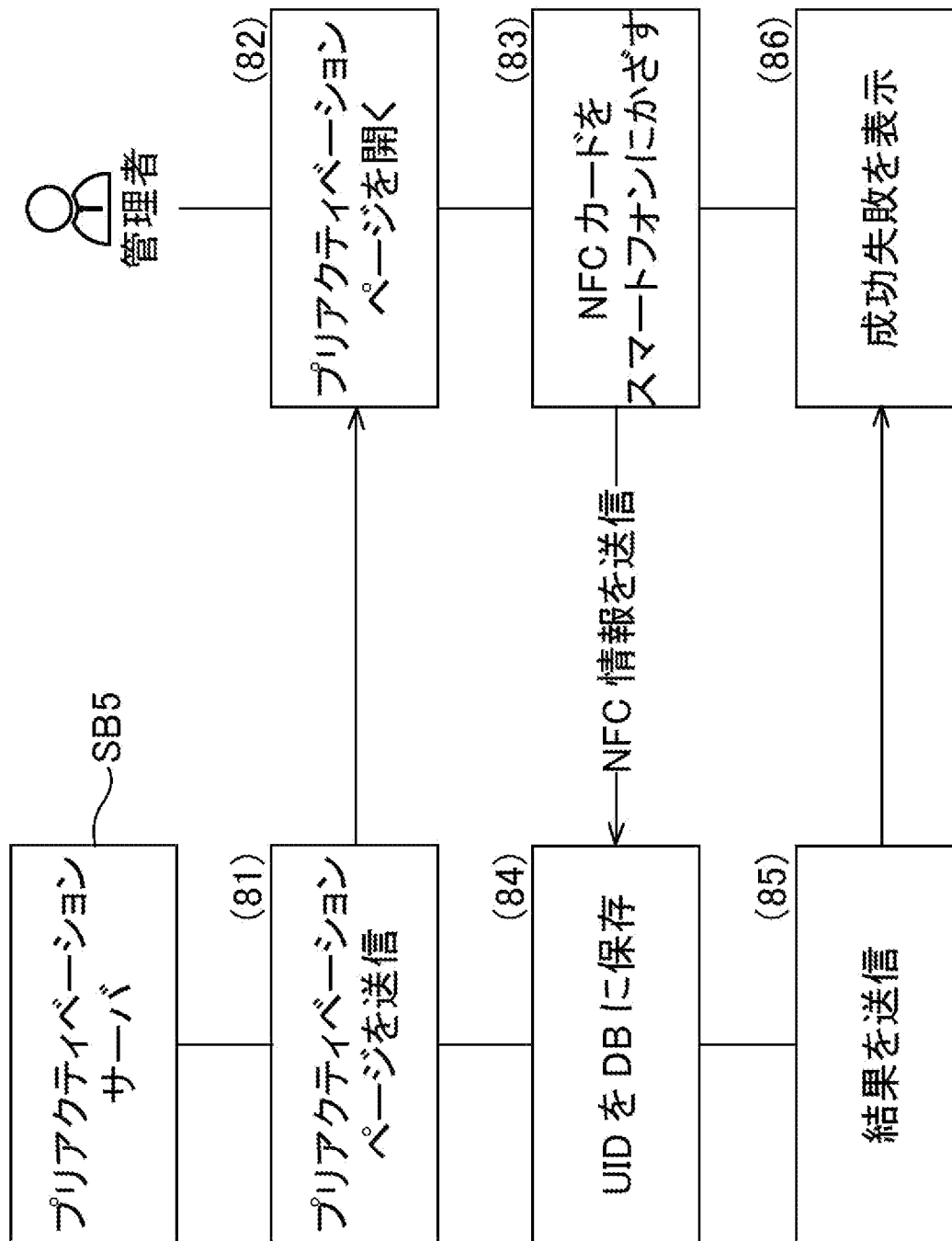
[図7]



[図8]

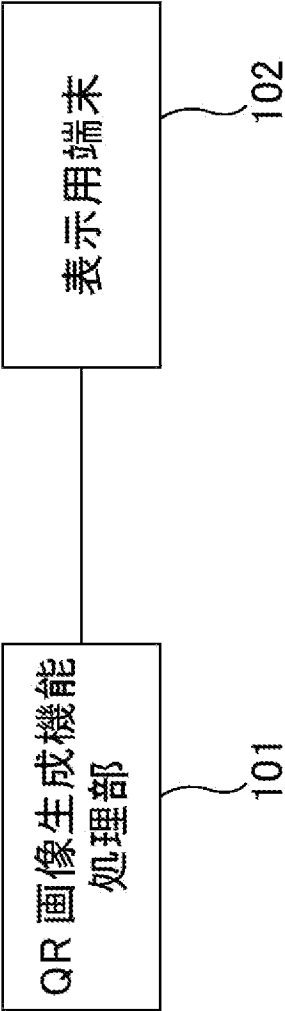
SB5

[図9]

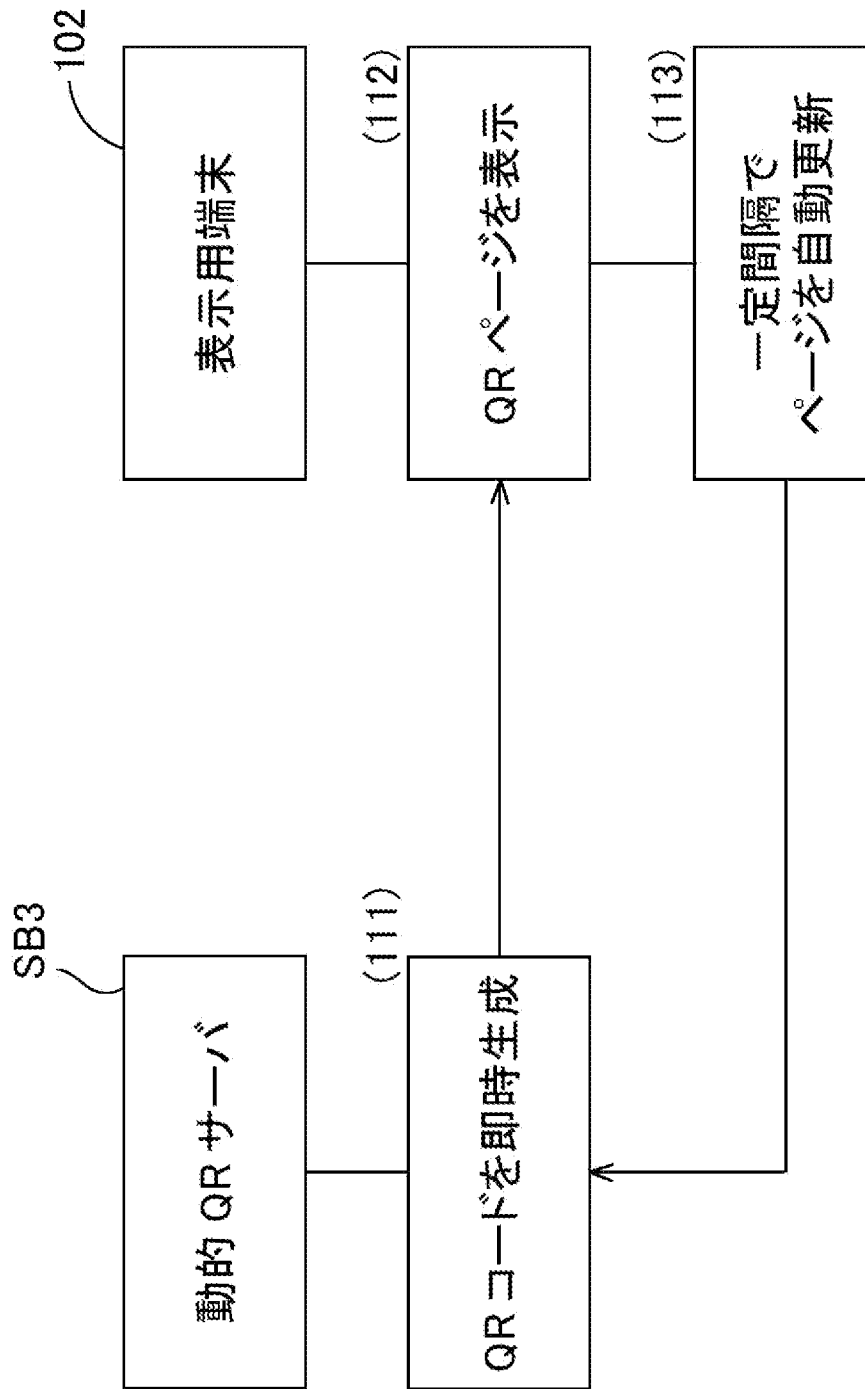


[図10]

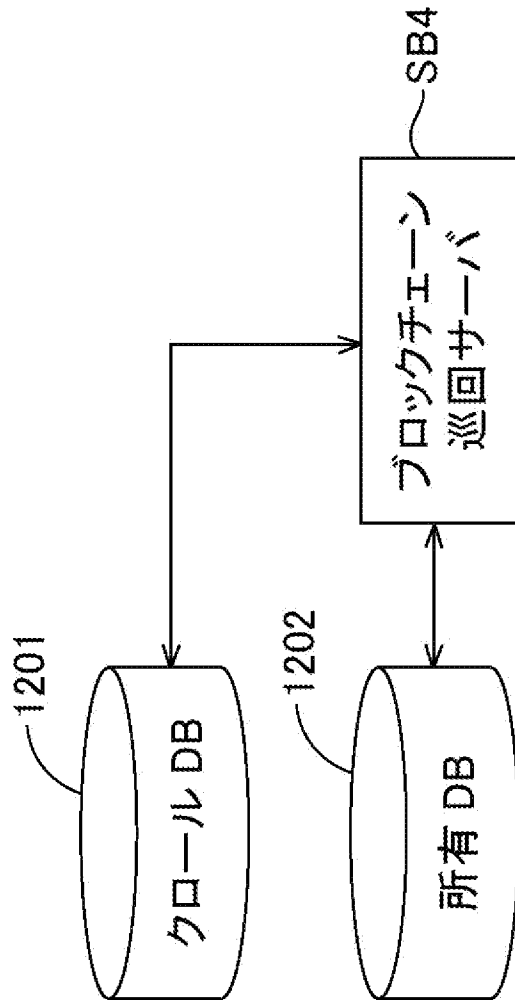
SB3



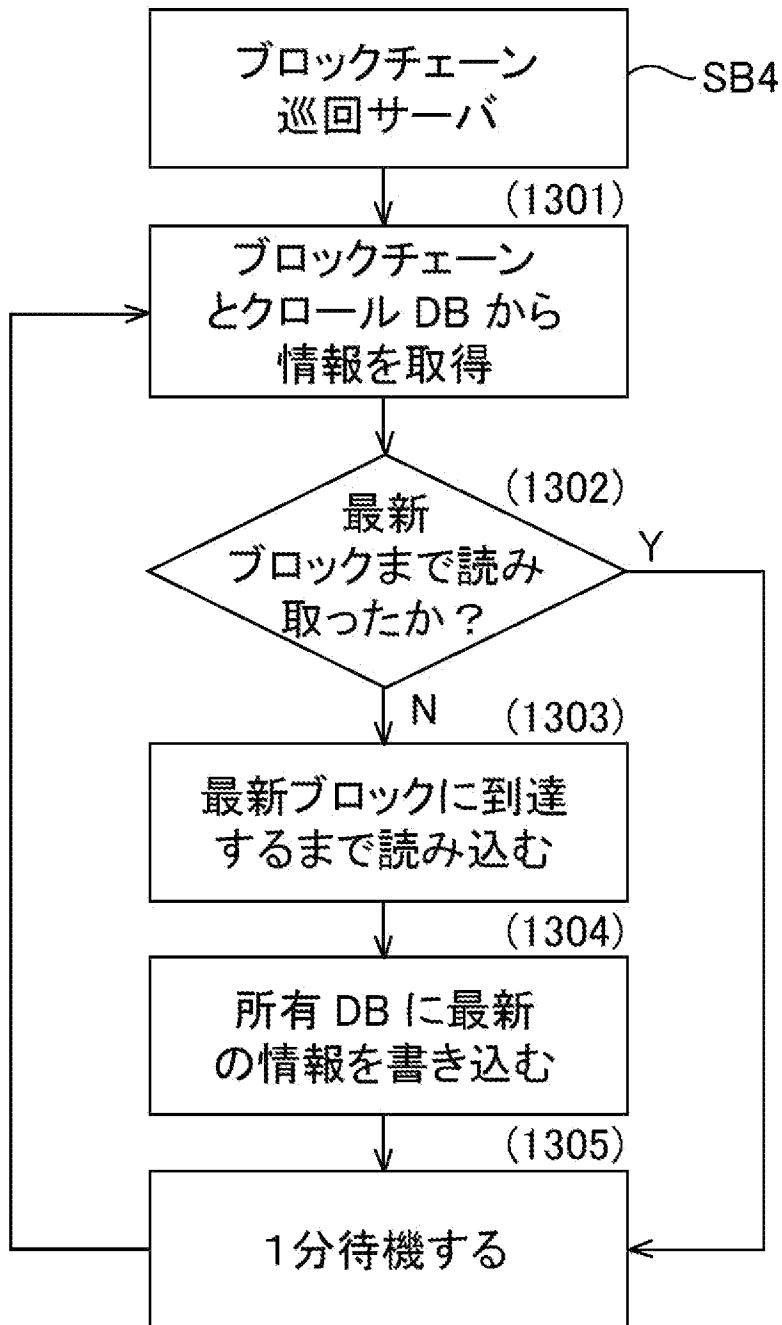
[図11]



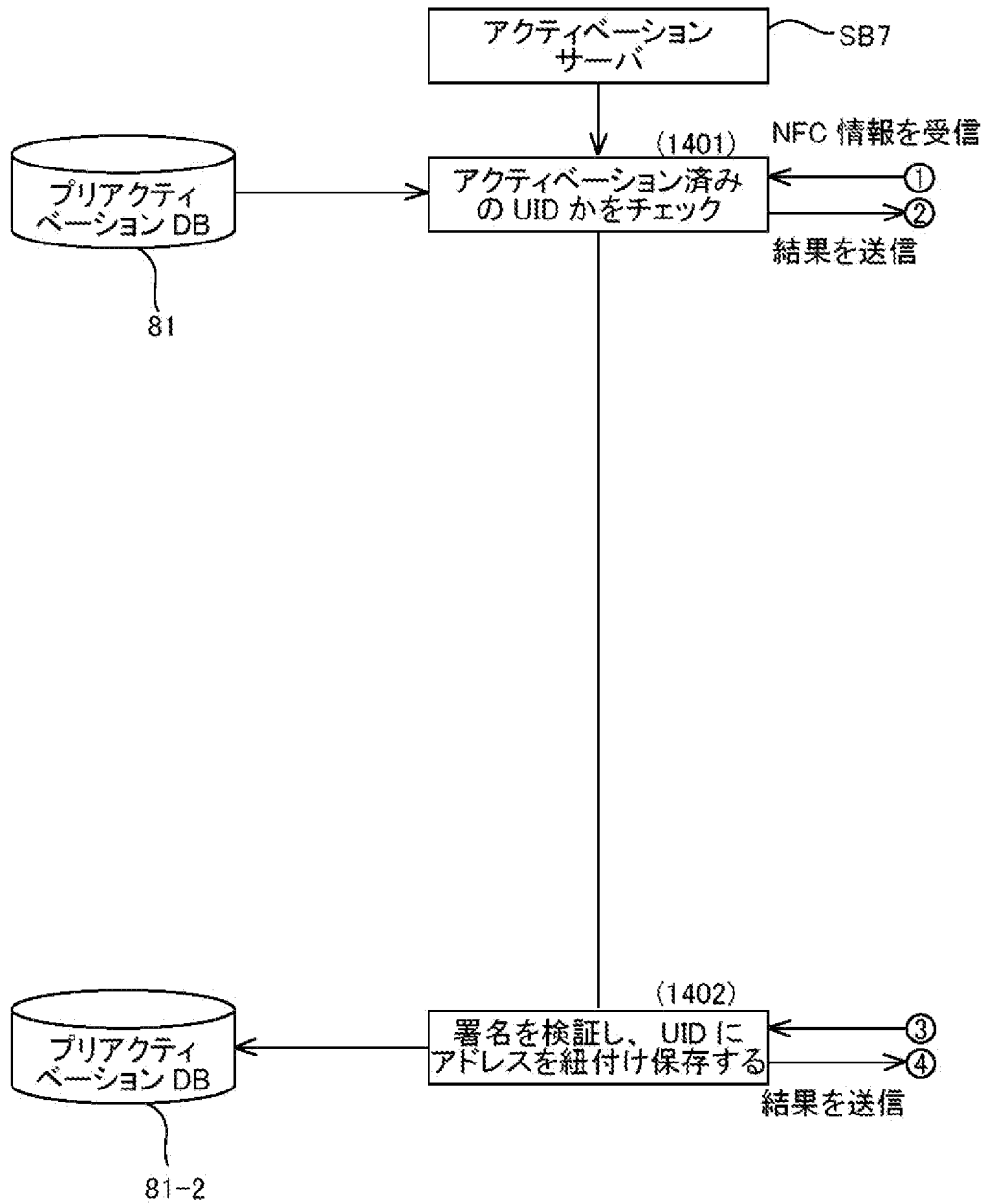
[図12]



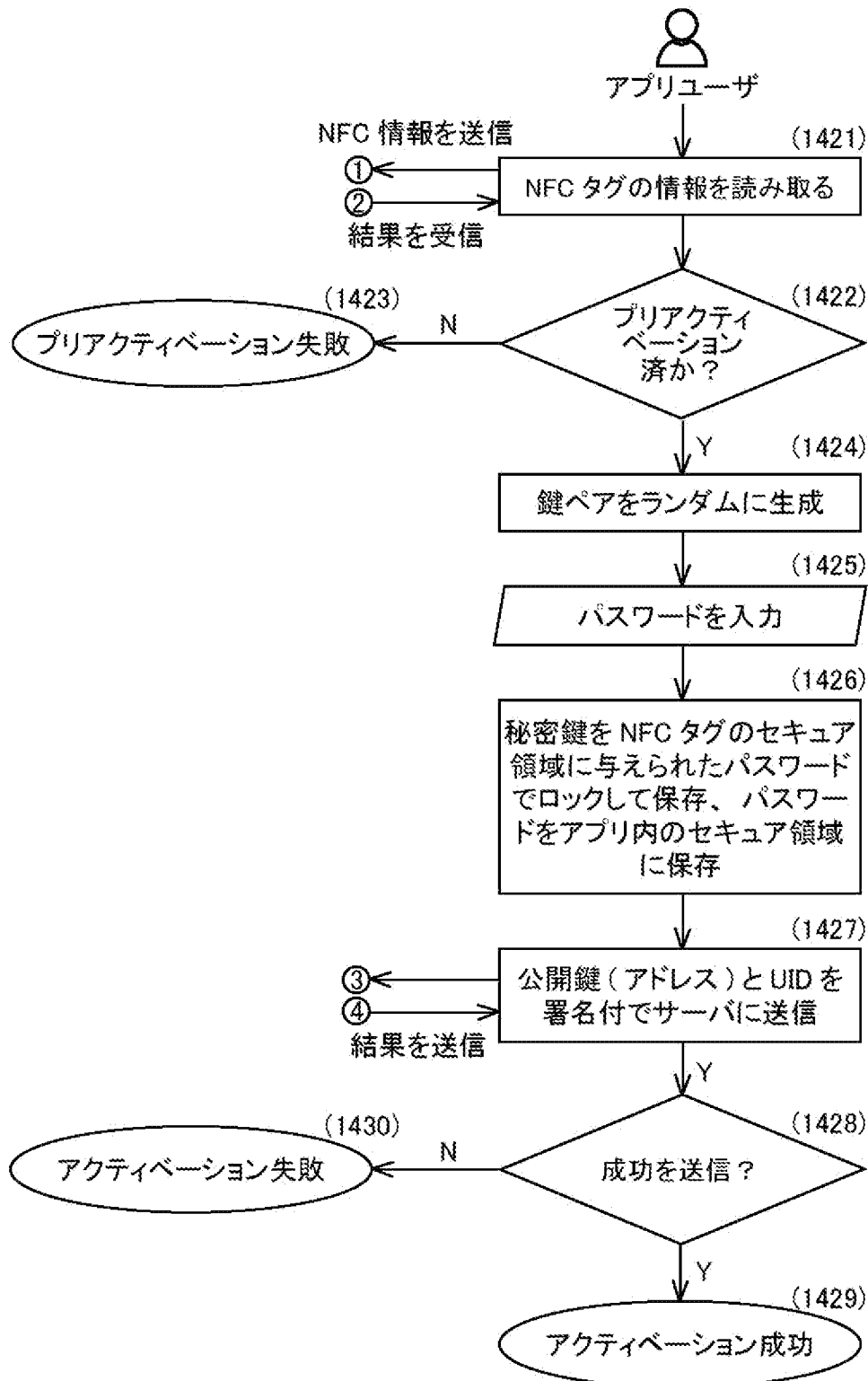
[図13]



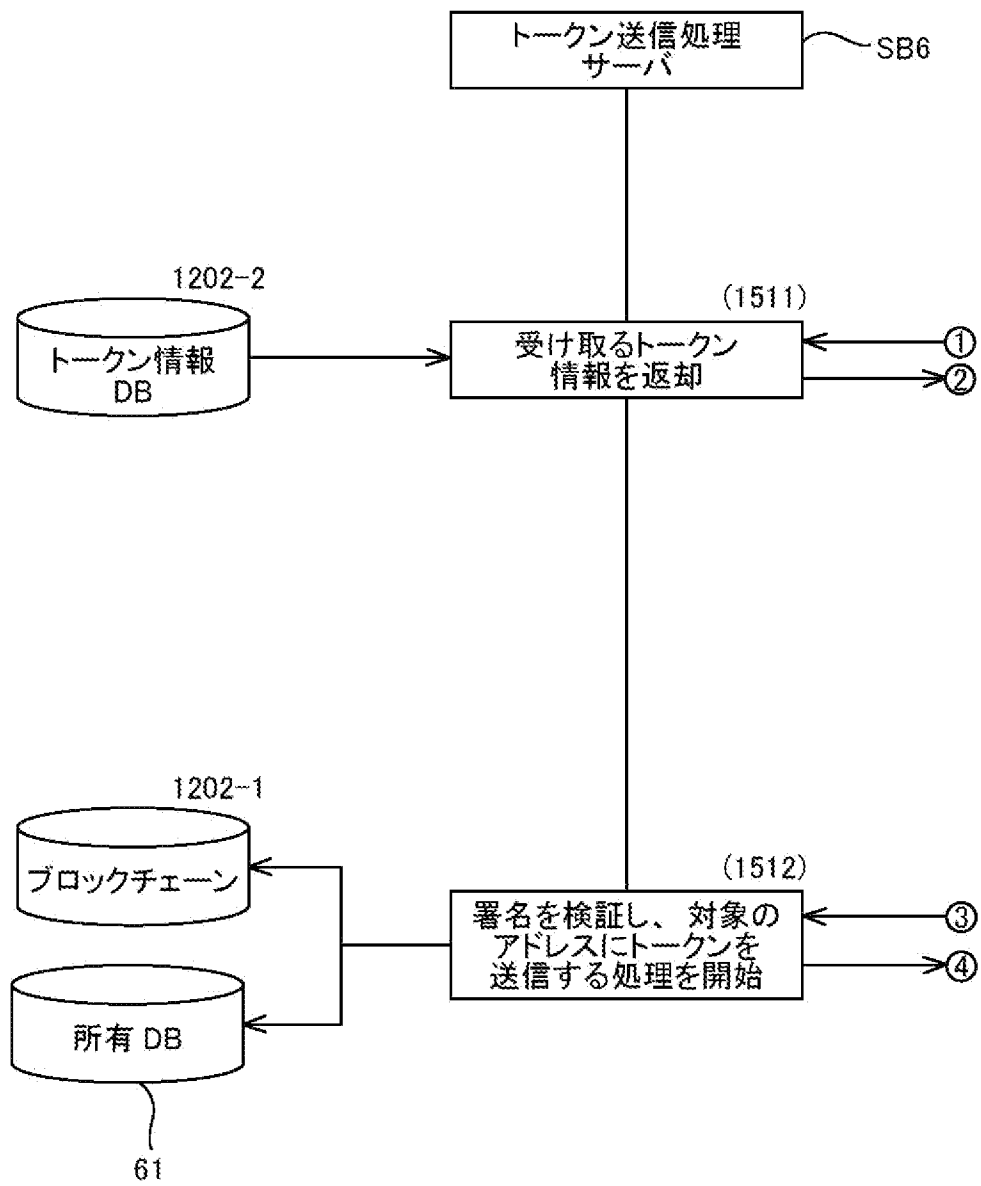
[図14]



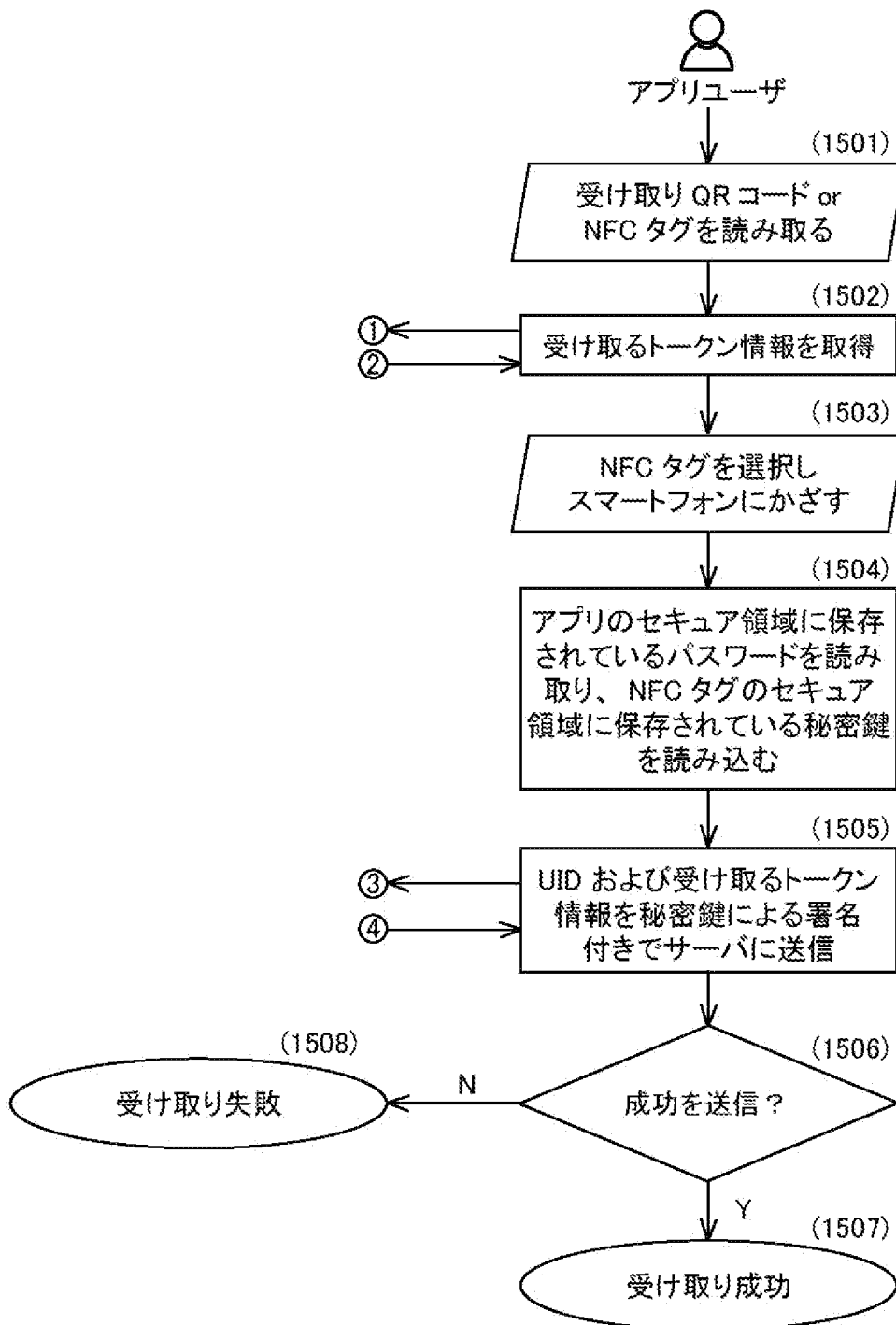
[図15]



[図16]



[図17]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2023/044356

A. CLASSIFICATION OF SUBJECT MATTER**H04L 9/10**(2006.01)i; **G06Q 20/32**(2012.01)i

FI: H04L9/10 A; G06Q20/32 330

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L9/10; G06Q20/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan 1922-1996
 Published unexamined utility model applications of Japan 1971-2024
 Registered utility model specifications of Japan 1996-2024
 Published registered utility model applications of Japan 1994-2024

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2022/0383295 A1 (DISNEY ENTERPRISES, INC.) 01 December 2022 (2022-12-01) paragraphs [0024]-[0037], fig. 1A-1B	1-2, 5
Y	JP 2012-065123 A (FUJI ELECTRIC RETAIL SYSTEMS CO LTD) 29 March 2012 (2012-03-29) paragraph [0060]	1-2
Y	WO 2014/196174 A1 (NIHON UNISYS LTD.) 11 December 2014 (2014-12-11) paragraphs [0012]-[0038], fig. 1-4	3-6
Y	JP 2006-148492 A (KABUSHIKI KAISHA TOSHIBA) 08 June 2006 (2006-06-08) paragraphs [0015]-[0049], fig. 1-5	3-6

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance
 “D” document cited by the applicant in the international application
 “E” earlier application or patent but published on or after the international filing date
 “L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 “O” document referring to an oral disclosure, use, exhibition or other means
 “P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

30 January 2024

Date of mailing of the international search report

13 February 2024

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
 3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915
 Japan

Authorized officer

Telephone No.

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

(Invention 1) Claims 1-2

Claims 1-2 have the special technical feature of a “control means that performs control to remove the secret key from a storage medium in a state in which the secret key encrypted by the encryption means is written in the storage medium of the NFC card and write address information for transacting the NFT in the storage medium,” and are thus classified as invention 1.

(Invention 2) Claims 3-6

Claims 3-6 share, with claim 1 classified as invention 1, the common technical feature of a “data terminal that performs proximity wireless communication with an NFC card.” However, said technical feature does not make a contribution over the prior art in light of the disclosure of document 1, and thus cannot be said to be a special technical feature. There are no other same or corresponding special technical features between these inventions.

Claims 3-6 are not dependent on claim 1. Claims 3-6 are not substantially identical to or similarly closely related to any of the claims classified as invention 1.

Therefore, claims 3-6 cannot be classified as invention 1.

Claims 3-6 have the special technical feature of a “second registration step for executing activation processing on a processed NFC card for which pre-activation processing on the NFC card ends via one of the plurality of system management servers and registering a public key generated in an activation database and UID in association with each other,” and are thus classified as invention 2.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2023/044356

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2022/0383295	A1	01 December 2022	(Family: none)			
JP	2012-065123	A	29 March 2012	(Family: none)			
WO	2014/196174	A1	11 December 2014	JP	2014-235683	A	
JP	2006-148492	A	08 June 2006	TW	200734373	A	

A. 発明の属する分野の分類（国際特許分類（IPC）） H04L 9/10(2006.01)i; G06Q 20/32(2012.01)i FI: H04L9/10 A; G06Q20/32 330		
B. 調査を行った分野 調査を行った最小限資料（国際特許分類（IPC）） H04L9/10; G06Q20/32 最小限資料以外の資料で調査を行った分野に含まれるもの 日本国実用新案公報 1922 - 1996年 日本国公開実用新案公報 1971 - 2024年 日本国実用新案登録公報 1996 - 2024年 日本国登録実用新案公報 1994 - 2024年 国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）		
C. 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	US 2022/0383295 A1 (DISNEY ENTERPRISES, INC.) 01.12.2022 (2022 - 12 - 01) 段落[0024]-[0037], Figs. 1A-1B	1-2, 5
Y	JP 2012-065123 A (富士電機リテイルシステムズ株式会社) 29.03.2012 (2012 - 03 - 29) 段落[0060]	1-2
Y	WO 2014/196174 A1 (日本ユニシス株式会社) 11.12.2014 (2014 - 12 - 11) 段落[0012]-[0038], 図1-4	3-6
Y	JP 2006-148492 A (株式会社東芝) 08.06.2006 (2006 - 06 - 08) 段落[0015]-[0049], 図1-5	3-6
☐ C欄の続きにも文献が列挙されている。 ☒ パテントファミリーに関する別紙を参照。		
* 引用文献のカテゴリー “A” 特に関連のある文献ではなく、一般的技術水準を示すもの “D” 国際出願で出願人が先行技術文献として記載した文献 “E” 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの “L” 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す） “O” 口頭による開示、使用、展示等に言及する文献 “P” 国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献 “T” 国際出願日又は優先日後に公表された文献であって出願と抵触するものではなく、発明の原理又は理論の理解のために引用するもの “X” 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの “Y” 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの “&” 同一パテントファミリー文献		
国際調査を完了した日 30.01.2024	国際調査報告の発送日 13.02.2024	
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 青木 重徳 5S 4229 電話番号 03-3581-1101 内線 3546	

第Ⅲ欄 発明の単一性が欠如しているときの意見（第1ページの3の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

（発明1）請求項1-2

請求項1-2は、[前記暗号化手段が暗号化した前記秘密鍵を前記NFCカードの記憶媒体に書き込んだ状態で、前記秘密鍵を前記記憶媒体から消去して、前記NFTを取引するためのアドレス情報を前記記憶媒体に書き込むように制御する制御手段]という特別な技術的特徴を有しているので、発明1に区分する。

（発明2）請求項3-6

請求項3-6は、発明1に区分された請求項1と、[NFCカードと近接無線通信するデータ端末]という共通の技術的特徴を有している。しかしながら、当該技術的特徴は、文献1の開示内容に照らして、先行技術に対する貢献をもたらすものではないから、当該技術的特徴は、特別な技術的特徴であるとはいえない。また、これらの発明の間には、他に同一の又は対応する特別な技術的特徴は存在しない。

さらに、請求項3-6は、請求項1の従属請求項ではない。また、請求項3-6は、発明1に区分されたいずれの請求項に対しても実質同一又はそれに準ずる関係にはない。

したがって、請求項3-6は発明1に区分できない。

そして、請求項3-6は、[前記複数のシステム管理サーバのうち、いずれか1つのシステム管理サーバを介して前記NFCカードに対してプリアクティベーション処理が終了している処理済NFCカードに対してアクティベーション処理を実行してアクティベーションデータベースに生成される公開鍵と、UIDとを紐づけて登録する第2の登録ステップ]という特別な技術的特徴を有しているので、発明2に区分する。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

追加調査手数料の異議の
申立てに関する注意

- ☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。
- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。
- ☐ 追加調査手数料の納付はあったが、異議申立てはなかった。

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2023/044356

引用文献			公表日	パテントファミリー文献			公表日
US	2022/0383295	A1	01.12.2022	(ファミリーなし)			
JP	2012-065123	A	29.03.2012	(ファミリーなし)			
WO	2014/196174	A1	11.12.2014	JP	2014-235683	A	
JP	2006-148492	A	08.06.2006	TW	200734373	A	