

(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9月6日(06.09.2024)



(10) 国際公開番号

WO 2024/180903 A1

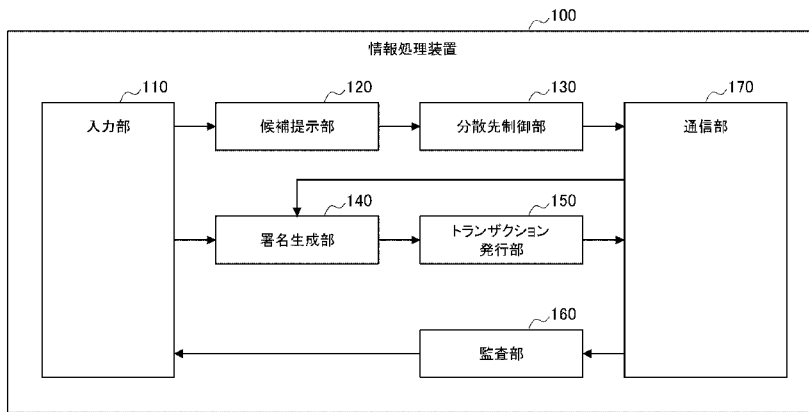
- (51) 国際特許分類:
H04L 9/32 (2006.01) H04L 9/08 (2006.01)
- (21) 国際出願番号: PCT/JP2024/000037
- (22) 国際出願日: 2024年1月5日(05.01.2024)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2023-028108 2023年2月27日(27.02.2023) JP
- (71) 出願人: ソニーグループ株式会社(SONY GROUP CORPORATION) [JP/JP]; 〒1080075 東京都港区港南1丁目7番1号 Tokyo (JP).
- (72) 発明者: 前田 勇作(MAEDA, Yusaku); 〒1080075 東京都港区港南1丁目7番1号 ソニーグループ株式会社内 Tokyo (JP). 丸山 信也(MARUYAMA, Shinya); 〒1080075 東京都港区港南1丁目7番1号 ソニーグループ株式会社内 Tokyo (JP).

- (74) 代理人: 伊藤 学, 外 (ITO, Manabu et al.); 〒1600023 東京都新宿区西新宿7-22-37 ストック西新宿413 協学国際特許事務所 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, 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,

(54) Title: INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD, AND PROGRAM

(54) 発明の名称: 情報処理装置、情報処理方法、及びプログラム

[図3]



100... Information processing device
110... Input unit
120... Candidate provision unit
130... Sharing destination control unit
140... Signature generation unit
150... Transaction issuance unit
160... Auditing unit
170... Communication unit

(57) Abstract: [Problem] To verify which share of a secret key is used in the generation of an electronic signature generated by the secret key. [Solution] This information processing device comprises: a sharing destination control unit that controls a plurality of sharing destinations respectively storing a plurality of shares obtained by secret-sharing a secret key on the basis of a user's selection; a signature generation unit that generates an electronic signature by the secret key using some of the plurality of shares stored in the plurality of sharing destinations; a transaction issuance unit that issues a transaction to which the electronic signature is affixed on a block chain; and an auditing unit that verifies which share among the plurality of shares is used in the generation of the electronic signature affixed to the transaction on the block chain.

[続葉有]



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)）

(57) 要約：【課題】秘密鍵によって生成された電子署名が秘密鍵のいずれの分散片を用いて生成されたかを検証する。【解決手段】秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分散先をユーザの選択に基づいて制御する分散先制御部と、前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、前記秘密鍵による電子署名を生成する署名生成部と、前記電子署名が付されたトランザクションをブロックチェーンに発行するトランザクション発行部と、前記ブロックチェーン上の前記トランザクションに付された前記電子署名が前記複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証する監査部と、を備える、情報処理装置。

明 細 書

発明の名称： 情報処理装置、情報処理方法、及びプログラム

技術分野

[0001] 本開示は、情報処理装置、情報処理方法、及びプログラムに関する。

背景技術

[0002] 近年、ブロックチェーン技術を用いた暗号資産の取引が活発化している。このような暗号資産の管理には、仮想的な財布の役割を担うウォレットが用いられる。ウォレットは、ユーザが所有する暗号資産のアドレスを管理すると共に、暗号資産を取引する際に用いられる電子署名を生成するための秘密鍵及び公開鍵を管理するシステムである。ウォレットは、秘密鍵の管理方法によって大きく2種類に分類される。

[0003] 例えば、Custodialなウォレットでは、ユーザは事業者秘密鍵の管理を一任することができる。Custodialなウォレットでは、ユーザは、事業者への信頼が必要となるものの、任意のデバイスから事業者のサービスにアクセスすることで、暗号資産を取引することができる。

[0004] 一方、Non-Custodialなウォレットでは、ユーザは自身で秘密鍵の管理を行うことになる。Non-Custodialなウォレットでは、ユーザは、第三者への信頼を前提とせずに暗号資産を取引することができるものの、任意のデバイスにて暗号資産を取引することが困難となる。

[0005] すなわち、一般的に、秘密鍵をより高い安全性で管理しようとするほど、秘密鍵の運用の柔軟性が低下することが知られている。そこで、ウォレットにおける秘密鍵の管理の安全性と、秘密鍵の運用の柔軟性とを両立させるために、例えば、秘密鍵の管理にMPC (Multi-Party Computation) 技術を用いることが検討されている（下記非特許文献1及び2参照）。

[0006] MPC技術は、互いに信頼していない複数の対象から入力された値を用いた計算結果を、各自の入力値を共有せずに導き出す暗号技術である。したがって、MPC技術を用いたウォレットでは、秘密鍵を複数の分散片に分割し

て分散管理し、電子署名を生成する際に分散先の各々から分散片を取得することで、秘密鍵を復元せずに電子署名に必要な計算結果を算出することができる。

先行技術文献

非特許文献

- [0007] 非特許文献1 : Yehuda Lindell, “Fast Secure Two-Party ECDSA Signing” , Journal of Cryptology, 2021, Volume 34, issue 4, Article:44
- 非特許文献2 : Rosario Gennaro and Steven Goldfeder, “Fast Multiparty Threshold ECDSA with Fast Trustless Setup” , CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, October 2018, p.1179-1194

発明の概要

発明が解決しようとする課題

- [0008] しかし、MPC技術では、設定によっては、秘密鍵のすべての分散片を集めずとも電子署名を生成することが可能である。そのため、分散片の分散管理の仕方によっては、ウォレットのユーザが関与していないところで電子署名が生成されてしまう可能性がある。
- [0009] そこで、分散片の紛失又は盗難を早期に発見するために、秘密鍵によって生成された電子署名が秘密鍵のいずれの分散片を用いて生成されたかを検証可能とする技術が求められていた。

課題を解決するための手段

- [0010] 本開示によれば、秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分散先をユーザの選択に基づいて制御する分散先制御部と、前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、前記秘密鍵による電子署名を生成する署名生成部と、前記電子署名が付されたトランザクションをブロックチェーンに発行するトランザクション発行部と、前記ブロックチェーン上の前記トランザクションに付された前記電子署名が前記

複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証する監査部と、を備える、情報処理装置が提供される。

[0011] また、本開示によれば、秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分散先をユーザの選択に基づいて制御することと、前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、前記秘密鍵による電子署名を生成することと、前記電子署名が付されたトランザクションをブロックチェーンに発行することと、前記ブロックチェーン上の前記トランザクションに付された前記電子署名が前記複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証することと、を含む、コンピュータによる情報処理方法が提供される。

[0012] さらに、本開示によれば、コンピュータを、秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分散先をユーザの選択に基づいて制御する分散先制御部と、前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、前記秘密鍵による電子署名を生成する署名生成部と、前記電子署名が付されたトランザクションをブロックチェーンに発行するトランザクション発行部と、前記ブロックチェーン上の前記トランザクションに付された前記電子署名が前記複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証する監査部と、として機能させるためのプログラムが提供される。

図面の簡単な説明

[0013] [図1]ブロックチェーン技術を用いた暗号資産の取引を示す説明図である。

[図2]MPC技術による秘密鍵の分散管理を説明する説明図である。

[図3]本開示の一実施形態に係る情報処理装置の内部構成を示すブロック図である。

[図4]秘密鍵の分散片を保管する分散先を選択させる画像の一例を示す説明図である。

[図5]ユーザが所有する他端末を分散片の分散管理に参加させるための画像の一例を示す説明図である。

[図6]第三者機関であるA A銀行のサーバを分散片の分散管理に参加させるための画像の一例を示す説明図である。

[図7]トランザクションに付された電子署名の検証結果を示す画像の一例を示す説明図である。

[図8]秘密鍵の分散片を生成する際の情報処理装置の動作を示すシーケンス図である。

[図9]トランザクションを発行する際の情報処理装置の動作を示すシーケンスである。

[図10]電子署名を検証する際の情報処理装置の動作を示すシーケンスである。

[図11]分散片を分散管理する分散先の信頼度を示す画像の一例を示す説明図である。

[図12]分散片を保管する分散先を他の分散先に切り替える際の情報処理装置の動作を示すシーケンスである。

[図13]本開示の一実施形態に係る情報処理装置のハードウェア構成例を示すブロック図である。

発明を実施するための形態

[0014] 以下に添付図面を参照しながら、本開示の好適な実施の形態について詳細に説明する。なお、本明細書及び図面において、実質的に同一の機能構成を有する構成要素については、同一の符号を付することにより重複説明を省略する。

[0015] なお、説明は以下の順序で行うものとする。

1. 本開示の背景技術
2. 情報処理装置の構成
3. 情報処理装置の動作
 3. 1. 分散片生成の際の動作
 3. 2. トランザクション発行の際の動作
 3. 3. 電子署名の検証の際の動作

4. 変形例

4. 1. 第1の変形例

4. 2. 第2の変形例

5. ハードウェア構成

[0016] <1. 本開示の背景技術>

まず、図1及び図2を参照して、本開示の一実施形態に係る情報処理装置100の背景技術について説明する。図1は、ブロックチェーン技術を用いた暗号資産の取引を示す説明図である。図2は、MPC技術による秘密鍵の分散管理を説明する説明図である。

[0017] 図1に示すように、暗号資産は、ネットワーク上に存在する複数の端末同士を直接接続することで構成された情報処理システム10にて分散的に管理される財産的価値である。情報処理システム10は、ネットワーク内で発生した暗号資産の取引履歴をブロックチェーンにて記録し、該ブロックチェーンを複数の端末で分散して管理する。

[0018] 例えば、情報処理装置100から暗号資産の取引を示すトランザクションTrが発行された場合、情報処理システム10の各ノードは、所定期間ごとに、発行されたトランザクションTrを検証し、検証されたトランザクションTrをブロックとしてまとめる。トランザクションTrをまとめたブロックが新しいブロックとしてブロックチェーンに連結されることにより、該ブロックに含まれる暗号資産の取引が成立する。

[0019] ここで、トランザクションTrには、トランザクションTrを発行したユーザによる電子署名ESが付される。電子署名ESは、トランザクションTrの内容に対する改ざんの有無を確認するために付される。電子署名ESは、電子署名ESを生成する際に用いられた秘密鍵と対応する公開鍵にて検証可能である。

[0020] トランザクションTrに付される電子署名ESを生成する秘密鍵は、例えば、情報処理装置100にインストールされたウォレットで管理され、情報処理装置100にてトランザクションTrを生成する際に使用される。した

がって、暗号資産を適切に管理するためには、電子署名ESを生成する秘密鍵を紛失したり、盗難されたりしないように適切に管理することが重要となる。

[0021] そこで、秘密鍵をより安全に管理するために、図2に示すように、MPC(Multi-Party Computation)技術を用いて秘密鍵SKを複数の分散片Frに分割して管理することが検討されている。秘密鍵SKを分割した複数の分散片Frは、例えば、ユーザのウォレットがインストールされた情報処理装置100、ユーザが所有する他端末101、暗号資産の取引に関するサービスを提供する事業者のサーバ200、又は第三者機関300などに分散して管理される。

[0022] 秘密鍵SKの分散片Frは、単独では電子署名ESを生成することができない。そのため、ユーザは、分散片Frを分散管理することで、分散片Frの紛失時又は盗難時に他者に電子署名ESを生成されるリスクを低減させることができる。一方で、MPC技術によれば、情報処理装置100は、秘密鍵SKの分散片Frのうち所定の数 of 分散片Frを集めることで、秘密鍵SKを復元することなく、秘密鍵SKによる電子署名ESを生成することができる。したがって、秘密鍵SKの分散片Frの各々を互いに異なる主体、又は互いに異なる端末の間で分散管理することで、秘密鍵SKの利便性を維持しつつ、秘密鍵SKの保管上のリスクを低減することができる。

[0023] 本実施形態に係る情報処理装置100は、ユーザの選択に基づいて、秘密鍵SKの分散片Frをそれぞれ保管する分散先を制御することが可能である。このような場合、情報処理装置100は、ユーザが信頼する分散先に分散片Frを分散管理することができるため、暗号資産の取引における安心感をより高めることができる。

[0024] また、本実施形態に係る情報処理装置100は、秘密鍵SKによって生成された電子署名ESが秘密鍵SKのいずれの分散片Frを用いて生成されたかを検証することが可能である。これによれば、情報処理装置100は、ユーザが把握していない電子署名ESの生成を検証することで、秘密鍵SKの

分散片 F r の紛失又は盗難を早期に発見することが可能である。したがって、情報処理装置 100 は、秘密鍵 S K の運用の安全性をより向上させることができる。

[0025] < 2. 情報処理装置の構成 >

続いて、図 3 を参照して、本実施形態に係る情報処理装置 100 の構成についてより詳細に説明する。図 3 は、本実施形態に係る情報処理装置 100 の内部構成を示すブロック図である。

[0026] 図 3 に示すように、情報処理装置 100 は、入力部 110 と、候補提示部 120 と、分散先制御部 130 と、署名生成部 140 と、トランザクション発行部 150 と、監査部 160 と、通信部 170 とを備える。

[0027] 入力部 110 は、例えば、マウス、キーボード、タッチパネル、ボタン、スイッチ、又はレバーなどのユーザからの入力を受け付ける装置である。入力部 110 は、秘密鍵 S K の分散片 F r を分散管理する分散先を指定する入力をユーザから受け付けることができる。また、入力部 110 は、暗号資産の取引内容の入力をユーザから受け付けることができる。

[0028] 候補提示部 120 は、秘密鍵 S K を分割した複数の分散片 F r をそれぞれ保管する分散先の候補をユーザに提示する。秘密鍵 S K の分散片 F r は、悪用、盗難、又は紛失のリスクを避けるためには、互いに異なる主体、又は互いに異なる端末の間で分散管理することが望ましい。そのため、候補提示部 120 は、秘密鍵 S K の分散片 F r を互いに独立して管理することが可能な主体又は端末が異なる分散先の候補をユーザに提示する。例えば、候補提示部 120 は、分散片 F r の分散先の候補として、情報処理装置 100、ユーザが所有する他端末、暗号資産の取引に関するサービスを提供する事業者のサーバ、又は第三者機関のサーバを提示してもよい。ユーザは、候補提示部 120 が提示した分散先の候補の中から所定の数 of 候補を選択することで、秘密鍵 S K の分散片 F r を保管する分散先を決定することができる。

[0029] なお、候補提示部 120 は、上記以外にも、ユーザの親族又は友人などが所有する端末を分散片 F r の分散先の候補として提示してもよい。候補提示

部 120 は、信頼できる人物が所有する端末、又は信頼できる機関のサーバであれば、上記以外にも他の分散先の候補をユーザに提示してもよい。

[0030] 例えば、候補提示部 120 は、図 4 に示す画像 500 を提示することで、秘密鍵 SK の分散片 F_r を保管する分散先の候補をユーザに提示してもよい。図 4 は、秘密鍵 SK の分散片 F_r を保管する分散先を選択させる画像 500 の一例を示す説明図である。

[0031] 図 4 に示す画像 500 には、秘密鍵 SK の分散片 F_r の分散先の選択肢として、選択肢画像 501、502、503、504、505 が表示されている。選択肢画像 501 は、秘密鍵 SK の分散片 F_r の分散先として情報処理装置 100 自体を選択する選択肢である。選択肢画像 502 は、秘密鍵 SK の分散片 F_r の分散先としてユーザが所有する他端末を選択する選択肢である。選択肢画像 503 は、秘密鍵 SK の分散片 F_r の分散先として暗号資産の取引に関するサービスを提供する事業者のサーバを選択する選択肢である。選択肢画像 504 は、秘密鍵 SK の分散片 F_r の分散先として第三者機関である AA 銀行のサーバを選択する選択肢である。選択肢画像 505 は、秘密鍵 SK の分散片 F_r の分散先として第三者機関である BB 銀行のサーバを選択する選択肢である。

[0032] また、図 4 に示す画像 500 では、ユーザが選択肢画像 501（情報処理装置 100）、選択肢画像 503（事業者のサーバ）、及び選択肢画像 505（第三者機関である BB 銀行のサーバ）を秘密鍵 SK の分散片 F_r の分散先として選択した例を示す。秘密鍵 SK の分散片 F_r の分散先が選択された場合、図 4 の画像 510 に示すように、分散片 F_r の分散先を確定するか否かが確認される。ユーザは、確定ボタン 511 を押下することで、提示された分散先の候補の中から分散片 F_r を保管する分散先を決定することができる。

[0033] 分散先制御部 130 は、ユーザの選択に基づいて、秘密鍵 SK の複数の分散片 F_r をそれぞれ分散管理する複数の分散先を制御する。具体的には、分散先制御部 130 は、ユーザによって分散片 F_r の分散先として選択された

端末又はサーバに分散片 F_r の分散管理への参加を要請し、要請を受諾した分散先と協働することで、秘密鍵 SK の分散片 F_r の生成プロセスを実行する。

[0034] 例えば、分散先制御部 130 は、図 5 に示す画像 520、及び図 6 に示す画像 530 を提示することで、分散片 F_r の分散先として選択された端末又はサーバに分散片 F_r の分散管理への参加を要請してもよい。図 5 は、ユーザが所有する他端末を分散片 F_r の分散管理に参加させるための画像 520 の一例を示す説明図である。図 6 は、第三者機関である AA 銀行のサーバを分散片 F_r の分散管理に参加させるための画像 530 の一例を示す説明図である。

[0035] 図 5 に示すように、ユーザが所有する他端末に分散片 F_r の分散管理への参加を要請する場合、分散先制御部 130 は、分散片 F_r の分散先を登録する web サイトの URL を示す二次元コード 521 を含む画像 520 を提示してもよい。ユーザは、提示された二次元コード 521 を分散片 F_r の分散先に決定した他端末に読み込ませることで、分散片 F_r の分散先として該他端末を登録することができる。

[0036] 図 6 に示すように、例えば、第三者機関のサーバに分散片 F_r の分散管理への参加を要請する場合、分散先制御部 130 は、画像 530 として第三者機関へログインするための web サイトを提示し、ユーザに第三者機関へログインを促してもよい。ユーザの第三者機関へのログインが確認された場合、分散先制御部 130 は、第三者機関のサーバに分散片 F_r の分散管理への参加を要請する。なお、ユーザの第三者機関へのログインが確認されなかった場合、分散先制御部 130 は、第三者機関のサーバが分散片 F_r の分散先として使用できない旨をユーザに伝達してもよい。

[0037] 秘密鍵 SK の分散片 F_r の生成プロセスでは、情報処理装置 100、及び要請を受諾した分散先は、公知の MPC 技術を用いてそれぞれ独立して演算を行い、演算結果を送受信し合うことで、秘密鍵 SK の分散片 F_r を生成する。これにより、秘密鍵 SK の分散片 F_r の生成プロセスに参加した分散先

の端末又はサーバでは、秘密鍵SKの分散片F_rがそれぞれ生成されるため、情報処理装置100は、秘密鍵SKの分散片F_rを分散先でそれぞれ分散管理することができる。

[0038] 署名生成部140は、複数の分散先にそれぞれ保管された複数の分散片F_rのうちの一部を用いて、秘密鍵SKによる電子署名ESを生成する。具体的には、署名生成部140は、複数の分散片F_rをそれぞれ保管する複数の分散先に秘密鍵SKによる電子署名ESの生成プロセスの実行を連絡し、応答した複数の分散先と協働することで、秘密鍵SKによる電子署名ESを生成する。

[0039] ただし、電子署名ESの生成プロセスでは、署名生成部140は、複数の分散先にそれぞれ保管された分散片F_rを受信するものの、秘密鍵SK自体を復元することはしない。署名生成部140は、MPC技術を用いることで、秘密鍵SKを復元することなく複数の分散片F_rから秘密鍵SKによる電子署名ESを生成することが可能である。

[0040] 秘密鍵SKによる電子署名ESは、秘密鍵SKのすべての分散片F_rのうち所定の数の分散片F_rが集まれば生成することが可能である。秘密鍵SKによる電子署名ESを生成するために必要な分散片F_rの数は、秘密鍵SKの分散片F_rの生成プロセスの実行の際に設定することが可能である。

[0041] トランザクション発行部150は、電子署名ESが付されたトランザクションTrを情報処理システム10のブロックチェーンに発行する。具体的には、トランザクション発行部150は、まず、ユーザからの入力に基づいて、情報処理システム10のブロックチェーンにて管理される暗号資産をあるアドレスから他のアドレスへ移動させるトランザクションTrを生成する。次に、トランザクション発行部150は、生成したトランザクションTrに秘密鍵SKによる電子署名ESを付した後、電子署名ESが付されたトランザクションTrを情報処理システム10のブロックチェーンに発行する。

[0042] ブロックチェーンに発行されたトランザクションTrは、情報処理システム10の各ノードで検証された後、所定期間ごとにブロックにまとめられる

。その後、トランザクションT_rを含むブロックが新しいブロックとしてブロックチェーンに連結されることにより、トランザクションT_rに示される暗号資産の移動が成立する。

[0043] なお、ブロックチェーンでは、スマートコントラクト技術を用いることにより、特定の分散片F_rを用いて生成された電子署名E_SのトランザクションT_rのみをブロックチェーンに追加するように制御することも可能である。具体的には、情報処理装置100は、特定の分散片F_rを含む電子署名E_Sのみを承認する旨の監査ルールをスマートコントラクトとしてブロックチェーンにあらかじめ設定することが可能である。このような場合、情報処理装置100は、例えば、情報処理装置100自体に保管された分散片F_rを用いて生成された電子署名E_SのトランザクションT_rのみをブロックチェーンに追加するように制御することが可能である。これによれば、ユーザは、ユーザが関与しないところで、ユーザに不利益をもたらすトランザクションT_rがブロックチェーンに発行されてしまうことを防止することができる。

[0044] 監査部160は、ブロックチェーン上のトランザクションT_rに付された電子署名E_Sがいずれの分散片F_rを用いて生成されたのかを検証する。具体的には、監査部160は、まず、情報処理システム10のブロックチェーンに組み込まれたトランザクションT_rに関する情報をブロックチェーンから取得する。次に、監査部160は、トランザクションT_rに付された電子署名E_Sを検証することで、電子署名E_Sの生成に用いられた分散片F_rを特定する。

[0045] 例えば、監査部160は、図7に示す画像540を提示することで、トランザクションT_rに付された電子署名E_Sの検証結果をユーザに提示してもよい。図7は、トランザクションT_rに付された電子署名E_Sの検証結果を示す画像540の一例を示す説明図である。

[0046] 図7に示す画像540には、検証したトランザクションT_rの情報を示すトランザクション情報テキスト541と、トランザクションT_rに付された

電子署名E Sの検証結果を示す検証結果テキスト5 4 2とが含まれる。

[0047] トランザクション情報テキスト5 4 1には、例えば、検証したトランザクションT rにて移動した暗号資産の額、暗号資産の移動元、及び暗号資産の移動先の情報が含まれてもよい。また、トランザクション情報テキスト5 4 1には、トランザクションT rを発行した日時情報がさらに含まれてもよい。検証結果テキスト5 4 2には、例えば、トランザクションT rに付された電子署名E Sを生成した分散片F rを保管する主体又は端末に関する情報が含まれてもよい。ユーザは、図7に示す画像5 4 0を参照することで、不審なトランザクションT rに付された電子署名E Sがいずれの分散片F rで生成されたかを検証することができる。よって、ユーザは、分散管理された分散片F rの悪用又は盗難を迅速に把握することが可能である。

[0048] 通信部1 7 0は、例えば、情報処理システム1 0のネットワークに接続するための通信インタフェースである。通信部1 7 0は、例えば、有線若しくは無線L A N (Local Area Network)、W i - F i (登録商標)、B l u e t o o t h (登録商標)、又はW U S B (Wireless USB) 用の通信カードなどであってもよい。情報処理装置1 0 0は、通信部1 7 0を介して、情報処理システム1 0のネットワークに暗号資産の取引を示すトランザクションT rを発行することができる。また、情報処理装置1 0 0は、通信部1 7 0を介して、情報処理システム1 0のネットワークから発行したトランザクションT rに関する情報を取得することができる。

[0049] 以上の構成を備える情報処理装置1 0 0は、暗号資産の取引に用いる秘密鍵S Kを複数の分散片F rに分割し、分割した分散片F rをユーザによって選択された分散先にそれぞれ保管することができる。これによれば、情報処理装置1 0 0は、ユーザがより信頼する分散先に分散片F rを分散管理することができるため、暗号資産の取引における安心感をより高めることができる。

[0050] また、情報処理装置1 0 0は、暗号資産を管理するブロックチェーン上に発行されたトランザクションT rの電子署名E Sが秘密鍵S Kのいずれの分

分散片 F_r を用いて生成されたのかを検証することができる。これによれば、情報処理装置 100 は、不審なトランザクション T_r に付された電子署名 E_S がいずれの分散片 F_r で生成されたかを検証することができるため、分散管理された分散片 F_r の悪用又は盗難を迅速に把握することが可能である。

[0051] < 3. 情報処理装置の動作 >

次に、図 8～図 10 を参照して、本実施形態に係る情報処理装置 100 の動作について説明する。図 8 は、秘密鍵 SK の分散片 F_r を生成する際の情報処理装置 100 の動作を示すシーケンス図である。図 9 は、トランザクション T_r を発行する際の情報処理装置 100 の動作を示すシーケンス図である。図 10 は、電子署名を検証する際の情報処理装置 100 の動作を示すシーケンス図である。

[0052] (3. 1. 分散片生成の際の動作)

図 8 に示すように、まず、候補提示部 120 から提示された分散先の候補の中から、ユーザによって秘密鍵 SK の分散片 F_r の分散先が決定される ($S101$)。図 8 では、情報処理装置 100、第 1 の分散先、及び第 2 の分散先が秘密鍵 SK の分散片 F_r の分散先として決定されている。

[0053] 続いて、分散先制御部 130 は、決定された分散先 (第 1 の分散先、及び第 2 の分散先) に分散片 F_r の分散管理への参加を要請する ($S102$, $S104$)。これに対して、第 1 の分散先、及び第 2 の分散先の各々から要請を受諾する旨が返信される ($S103$, $S105$)。

[0054] その後、分散先制御部 130 は、第 1 の分散先、及び第 2 の分散先と協働することで、秘密鍵 SK の分散片 F_r の生成プロセスを実行する ($S106$)。具体的には、情報処理装置 100、第 1 の分散先、及び第 2 の分散先は、それぞれ演算を行うと共に、演算結果を互いに送受信し合うことで、情報処理装置 100、第 1 の分散先、及び第 2 の分散先の各々で分散片 F_r を生成する。

[0055] 生成された分散片 F_r は、情報処理装置 100、第 1 の分散先、及び第 2 の分散先でそれぞれ保存される ($S107$, $S108$, $S109$)。これに

より、情報処理装置100は、秘密鍵SKを分割した3つの分散片Frを情報処理装置100、第1の分散先、及び第2の分散先でそれぞれ分散管理することができる。

[0056] (3. 2. トランザクション発行の際の動作)

図9に示すように、まず、トランザクション発行部150は、ユーザからの入力に基づいて監査ルールを設定する(S201)。監査ルールは、電子署名ESの生成に用いられる分散片Frに制限を加えるものであってもよい。例えば、監査ルールは、トランザクションTrに付された電子署名ESの生成に情報処理装置100自体に保管された分散片Frが用いられることであってよい。

[0057] 続いて、トランザクション発行部150は、設定された監査ルールをブロックチェーンに送信し(S202)、ブロックチェーンにて監査ルールをスマートコントラクトとして実装する(S203)。

[0058] その後、ユーザからの入力に基づいて、ブロックチェーンにて管理される暗号資産の移動を指示するトランザクションTrの発行が決定される(S204)。このとき、まず、署名生成部140は、複数の分散片Frをそれぞれ保管する第1の分散先、第2の分散先、及び情報処理装置100と協働することで、秘密鍵SKによる電子署名ESの生成プロセスを実行する(S205)。これにより、秘密鍵SKによる電子署名ESが生成されるため、トランザクション発行部150は、電子署名ESが付されたトランザクションTrを生成することができる(S206)。

[0059] その後、トランザクション発行部150は、電子署名ESが付されたトランザクションTrをブロックチェーンに発行する(S207)。ブロックチェーンに発行されたトランザクションTrは、ブロックチェーンを管理する情報処理システム10の各ノードにて電子署名ES及び監査ルールを検証される(S208)。検証が終わったトランザクションTrは、所定期間ごとにブロックにまとめられた後、新たなブロックとしてブロックチェーンに連結される(S209)。これにより、発行されたトランザクションTrが指

示する暗号資産の移動が成立する。

[0060] (3. 3. 電子署名の検証の際の動作)

図10に示すように、例えば、暗号資産の不審な移動が見られた場合、監査部160は、該当する暗号資産の移動を指示するトランザクションTrの情報をブロックチェーンに照会する(S301)。

[0061] 続いて、監査部160は、ブロックチェーンからトランザクションTrの情報を取得し(S302)、取得したトランザクションTrに付された電子署名ESがいずれの分散片Frを用いて生成されたか検証する(S303)。具体的には、監査部160は、トランザクションTrに付された電子署名ESを演算することで、電子署名ESの生成に用いられた分散片Frを特定することができる。

[0062] これによれば、情報処理装置100は、不審なトランザクションTrに付された電子署名ESを検証することで、電子署名ESの生成に用いられた分散片Frの悪用又は盗難を迅速に把握することが可能である。

[0063] <4. 変形例>

(4. 1. 第1の変形例)

続いて、図11を参照して、本実施形態に係る情報処理装置100の第1の変形例について説明する。第1の変形例は、ユーザによって選択された分散先の組み合わせの信頼度をユーザにさらに提示する変形例である。図11は、分散片Frを分散管理する分散先の信頼度を示す画像550の一例を示す説明図である。

[0064] 図11に示すように、ユーザによって分散片Frの分散先が選択された場合、候補提示部120は、選択された分散先の組み合わせの信頼度を数値化してユーザに提示してもよい。具体的には、候補提示部120は、所定のルールに基づいて、選択された分散先の組み合わせの信頼度を数値として算出し、算出した信頼度の数値をユーザに提示してもよい。

[0065] 例えば、図11に示す画像550では、分散片Frの分散先として、選択肢画像551, 553, 554で示されるように、情報処理装置100(こ

の端末)、事業者のサーバ(ウォレット用サーバ)、及び第三者機関であるAA銀行のサーバ(AA銀行サーバ)が選択されている。このような場合、候補提示部120は、これらの分散先の組み合わせの信頼度の数値を信頼度画像556(80点)でユーザに提示してもよい。

[0066] 信頼度の数値は、例えば、秘密鍵SKを分割した分散片Frの分散数、及び秘密鍵SKによる電子署名ESを生成するために必要な分散片Frの数に基づいて算出されてもよく、分散先同士の結託の可能性(例えば、分散先の運営主体の共通性、又は分散先のサーバで使用するクラウドサービスの共通性)に基づいて算出されてもよく、分散先のセキュリティ強度に基づいて算出されてもよい。

[0067] 例えば、分散片Frの分散先の組み合わせの信頼度は、以下の項目を用いて所定の点数(例えば、100点など)からの減点方式で算出されてもよい。

- ・分散片Frの分散数よりも電子署名ESを生成するために必要な分散片Frの数が少ない：-20点
- ・共通の組織に属する分散先が存在する：-30点
- ・共通のクラウドサービスを使用している分散先が存在する：-10点
- ・セキュリティに関する監査が成されていない組織が分散先に含まれる：-10点
- ・重大なセキュリティインシデントを発生させた組織が分散先に含まれる：-20点

[0068] 分散片Frの分散先の組み合わせの信頼度を減点方式で算出する場合、候補提示部120は、減点の理由となったルール、及びルールの対象となった分散先をユーザに提示してもよい。これによれば、ユーザは、より信頼度が高い分散先の組み合わせを選択するための指針を得ることができるため、信頼度が高い分散先の組み合わせをより容易に選択することが可能となる。

[0069] なお、信頼度の数値は、上述した減点方式に替えて、所定の点数(例えば、0点など)からの加点方式を用いて算出されてもよい。また、信頼度の数

値は、減点方式と加点方式とを併用して算出されてもよい。

[0070] また、候補提示部 120 は、信頼度が高くなる分散先の候補を認証し、認証した分散先の候補を強調表現してユーザに提示してもよい。候補提示部 120 は、例えば、堅牢なセキュリティ対策を施している、又はセキュリティインシデントの発生数が少ないなどの所定の条件を満たす組織を信頼度が高くなる分散先の候補として認証してもよい。候補提示部 120 は、認証した分散先の候補を強調表現してユーザに提示することで、信頼度が高い分散先をユーザにより容易に選択させることができる。

[0071] さらに、候補提示部 120 は、信頼度が高くなる分散先の組み合わせをあらかじめテンプレートとして用意してもよい。候補提示部 120 は、あらかじめ用意した分散先の組み合わせをユーザに提示することで、分散片 F r の分散先の選択をより容易に行わせることが可能である。

[0072] (4. 2. 第2の変形例)

次に、図 12 を参照して、本実施形態に係る情報処理装置 100 の第2の変形例について説明する。第2の変形例では、情報処理装置 100 は、分散片 F r を保管する分散先を他の分散先に切り替える処理を行うことができる。図 12 は、分散片 F r を保管する分散先を他の分散先に切り替える際の情報処理装置 100 の動作を示すシーケンスである。

[0073] 図 12 に示すように、ユーザによって分散片 F r を保管する分散先の変更が入力されたとする (S401)。例えば、ユーザによって、分散片 F r の 1 つを保管する分散先を第2の分散先から第3の分散先に変更する入力が行われたとする。

[0074] このような場合、分散先制御部 130 は、分散片 F r の保管を第2の分散先から第3の分散先に切り替える要請を第2の分散先に送信する (S402)。要請を受信した第2の分散先は、保管していた分散片 F r を暗号化して第3の分散先に送信する (S403)。暗号化された分散片 F r を受信した第3の分散先は、受信した分散片 F r を復号して保管する (S404)。

[0075] その後、分散先制御部 130 は、切り替え前の分散先である第2の分散先

に保管された分散片 F_r の悪用を防止するための処理を行う。具体的には、分散先制御部 130 は、第 1 の分散先、及び第 3 の分散先と協働して、それぞれが保管する分散片 F_r の各々の乱数成分を再設定する (S405)。これにより、第 2 の分散先で保管されていた分散片 F_r が無効化されるため、第 2 の分散先で保管されていた分散片 F_r を用いた電子署名 E_S の生成ができなくなる。上記の処理では、秘密鍵 SK による電子署名 E_S の生成と同様に、秘密鍵 SK を復元することなく分散片 F_r の各々の乱数成分の再設定のみを行うことが可能である。

[0076] なお、分散先制御部 130 は、分散片 F_r の各々の乱数成分を再設定せずとも、切り替え前の分散先である第 2 の分散先に保管された分散片 F_r の悪用を防止することも可能である。

[0077] 一例として、分散先制御部 130 は、分散片 F_r を保管する分散先の切り替え数を制限してもよい。例えば、分散先制御部 130 は、一度に切り替え可能な分散先の数が電子署名 E_S の生成に必要な分散片 F_r の数よりも少なくなるように分散先の切り替え数を制限してもよい。これによれば、分散先制御部 130 は、切り替え前の分散先に保管されていた分散片 F_r のみを用いて電子署名 E_S が生成されることを防止することが可能である。

[0078] また、他の例として、分散先制御部 130 は、電子署名 E_S を生成する際に用いられる分散片 F_r を制限する監査ルールをスマートコントラクトにて設定してもよい。例えば、分散先制御部 130 は、分散片 F_r の分散先を切り替えていない第 1 の分散先又は情報処理装置 100 に保管されている分散片 F_r を必ず用いて電子署名 E_S を生成する旨の監査ルールをスマートコントラクトにて設定してもよい。より詳細には、分散先制御部 130 は、ユーザが所有する端末である情報処理装置 100 に保管されている分散片 F_r を必ず用いて電子署名 E_S を生成する旨の監査ルールをスマートコントラクトにて設定してもよい。これによれば、分散先制御部 130 は、切り替え前の分散先に保管されていた分散片 F_r のみを用いて電子署名 E_S が生成されることを防止することが可能である。

[0079] <5. ハードウェア構成>

図13を参照して、本実施形態に係る情報処理装置100のハードウェア構成について説明する。図13は、本実施形態に係る情報処理装置100のハードウェア構成例を示すブロック図である。

[0080] 本実施形態に係る情報処理装置100の機能は、ソフトウェアと、以下で説明するハードウェアとの協働によって実現され得る。候補提示部120、分散先制御部130、署名生成部140、トランザクション発行部150、及び監査部160の機能は、例えば、CPU901により実行されてもよい。入力部110の機能は、入力装置906により実行されてもよい。通信部170の機能は、例えば、接続ポート910、又は通信装置911により実行されてもよい。

[0081] 図13に示すように、情報処理装置100は、CPU(Central Processing Unit)901、ROM(Read Only Memory)902、及びRAM(Random Access Memory)903を含む。

[0082] また、情報処理装置100は、ホストバス904a、ブリッジ904、外部バス904b、インタフェース905、入力装置906、出力装置907、ストレージ装置908、ドライブ909、接続ポート910、又は通信装置911をさらに含んでもよい。情報処理装置100は、CPU901に替えて、又はCPU901と共に、DSP(Digital Signal Processor)、又はASIC(Application Specific Integrated Circuit)などの処理回路を有してもよい。

[0083] CPU901は、演算処理装置、又は制御装置として機能し、ROM902、RAM903、ストレージ装置908、又はドライブ909に装着されたリムーバブル記録媒体に記録された各種プログラムに従って、情報処理装置100内の動作を制御する。ROM902は、CPU901が使用するプログラム、及び演算パラメータなどを記憶する。RAM903は、CPU901の実行において使用するプログラム、及びその実行の際に使用するパラメータなどを一時的に記憶する。

- [0084] CPU 901、ROM 902、及びRAM 903は、高速なデータ伝送が可能なホストバス 904 aにより相互に接続される。ホストバス 904 aは、ブリッジ 904を介して、PCI (Peripheral Component Interconnect/Interface)バスなどの外部バス 904 bに接続され、外部バス 904 bは、インタフェース 905を介して種々の構成要素と接続される。
- [0085] 入力装置 906は、例えば、マウス、キーボード、タッチパネル、ボタン、スイッチ、又はレバーなどのユーザからの入力を受け付ける装置である。なお、入力装置 906は、ユーザの音声を検出するマイクロフォンなどであってもよい。入力装置 906は、例えば、赤外線、又はその他の電波を利用したリモートコントロール装置であってもよく、情報処理装置 100の操作に対応した外部接続機器であってもよい。
- [0086] 入力装置 906は、ユーザが入力した情報に基づいて生成した入力信号をCPU 901に出力する入力制御回路をさらに含む。ユーザは、入力装置 906を操作することによって、情報処理装置 100に対して各種データの入力、又は処理動作の指示を行うことができる。
- [0087] 出力装置 907は、情報処理装置 100にて取得又は生成された情報をユーザに対して視覚的、又は聴覚的に提示することが可能な装置である。出力装置 907は、例えば、LCD (Liquid Crystal Display)、PDP (Plasma Display Panel)、OLED (Organic Light Emitting Diode)ディスプレイ、ホログラム、又はプロジェクタなどの表示装置であってもよく、スピーカ又はヘッドホンなどの音出力装置であってもよく、プリンタ装置などの印刷装置であってもよい。出力装置 907は、情報処理装置 100の処理により得られた情報をテキスト又は画像などの映像、及び音声又は音響などの音として出力することができる。
- [0088] ストレージ装置 908は、情報処理装置 100の記憶部の一例として構成されたデータ格納装置である。ストレージ装置 908は、例えば、HDD (Hard Disk Drive)などの磁気記憶デバイス、半導体記憶デバイス、光記憶デバイス、又は光磁気記憶デバイスなどにより構成されてもよい。ストレージ装

置 908 は、CPU 901 が実行するプログラム、各種データ、又は外部から取得した各種データなどを格納することができる。

[0089] ドライブ 909 は、磁気ディスク、光ディスク、光磁気ディスク、又は半導体メモリなどのリムーバブル記録媒体の読み取り又は書き込み装置であり、情報処理装置 100 に内蔵、又は外付けされる。例えば、ドライブ 909 は、装着されているリムーバブル記録媒体に記録されている情報を読み出して RAM 903 に出力することができる。また、ドライブ 909 は、装着されているリムーバブル記録媒体に記録を書き込むことができる。

[0090] 接続ポート 910 は、外部接続機器を情報処理装置 100 に直接接続するためのポートである。接続ポート 910 は、例えば、USB (Universal Serial Bus) ポート、IEEE 1394 ポート、又は SCSI (Small Computer System Interface) ポートなどであってもよい。また、接続ポート 910 は、RS-232C ポート、光オーディオ端子、又は HDMI (登録商標) (High-Definition Multimedia Interface) ポートなどであってもよい。接続ポート 910 は、外部接続機器と接続されることで、情報処理装置 100 と外部接続機器との間で各種データの送受信を行うことができる。

[0091] 通信装置 911 は、例えば、通信ネットワーク 920 に接続するための通信デバイスなどで構成された通信インタフェースである。通信装置 911 は、例えば、有線若しくは無線 LAN (Local Area Network)、Wi-Fi (登録商標)、Bluetooth (登録商標)、又は WUSB (Wireless USB) 用の通信カードなどであってもよい。また、通信装置 911 は、光通信用のルータ、ADSL (Asymmetric Digital Subscriber Line) 用のルータ、又は各種通信用のモデムなどであってもよい。

[0092] 通信装置 911 は、例えば、インターネット、又は他の通信機器との間で、TCP/IP などの所定のプロトコルを用いて信号などを送受信することができる。また、通信装置 911 に接続される通信ネットワーク 920 は、有線又は無線によって接続されたネットワークであり、例えば、インターネット通信網、家庭内 LAN、赤外線通信網、ラジオ波通信網、又は衛星通信

網などであってもよい。

[0093] なお、コンピュータに内蔵されるCPU901、ROM902、及びRAM903などのハードウェアに上記の情報処理装置100と同等の機能を発揮させるためのプログラムも作成可能である。また、該プログラムを記録したコンピュータに読み取り可能な記録媒体も提供可能である。

[0094] 以上、添付図面を参照しながら本開示の好適な実施形態について詳細に説明したが、本開示の技術的範囲はかかる例に限定されない。本開示の技術分野における通常の知識を有する者であれば、請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであり、これらについても、当然に本開示の技術的範囲に属するものと了解される。

[0095] また、本明細書に記載された効果は、あくまで説明的または例示的なものであって限定的ではない。つまり、本開示に係る技術は、上記の効果とともに、または上記の効果に代えて、本明細書の記載から当業者には明らかな他の効果を奏しうる。

[0096] なお、以下のような構成も本開示の技術的範囲に属する。

(1)

秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分散先をユーザの選択に基づいて制御する分散先制御部と、

前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、前記秘密鍵による電子署名を生成する署名生成部と、

前記電子署名が付されたトランザクションをブロックチェーンに発行するトランザクション発行部と、

前記ブロックチェーン上の前記トランザクションに付された前記電子署名が前記複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証する監査部と、

を備える、情報処理装置。

(2)

前記署名生成部は、前記複数の分散片のうち所定の数の前記分散片を用いて、前記電子署名を生成する、前記（１）に記載の情報処理装置。

（３）

前記複数の分散先は、前記ユーザが所有する端末、前記トランザクションに関するサービスを提供する事業者が管理するサーバ、又は第三者機関が管理するサーバを含む、前記（１）又は（２）に記載の情報処理装置。

（４）

前記複数の分散先は、前記ユーザが所有する端末を少なくとも含み、
前記署名生成部は、前記ユーザが所有する端末に保管された前記分散片を少なくとも用いて、前記電子署名を生成する、前記（３）に記載の情報処理装置。

（５）

前記分散先制御部は、前記ユーザに選択された前記複数の分散先と協働することで、前記複数の分散片の生成プロセスを実行する、前記（１）～（４）のいずれか一項に記載の情報処理装置。

（６）

前記複数の分散先が変更される場合、前記分散先制御部は、前記複数の分散片の各々に含まれる乱数成分を再設定する、前記（１）～（５）のいずれか一項に記載の情報処理装置。

（７）

前記複数の分散先の候補を前記ユーザに提示する候補提示部をさらに備え、

前記ユーザは、提示された前記候補の中から前記複数の分散片の各々を保管する前記複数の分散先を選択する、前記（１）～（６）のいずれか一項に記載の情報処理装置。

（８）

前記候補提示部は、前記ユーザに選択された前記複数の分散先の組み合わせの信頼度を導出すると共に、導出した前記信頼度を前記ユーザにさらに提

示する、前記（７）に記載の情報処理装置。

（９）

前記信頼度は、前記組み合わせに含まれる前記分散先の数、前記分散先の互いの共通項、前記分散先の各々のセキュリティ強度、又は前記分散先の各々の過去実績の少なくとも１つ以上を参照する所定のルールに基づいて導出される、前記（８）に記載の情報処理装置。

（１０）

前記候補提示部は、前記信頼度の導出根拠を前記ユーザにさらに提示する、前記（９）に記載の情報処理装置。

（１１）

前記候補提示部は、前記複数の分散先の候補の推奨される組み合わせを前記ユーザにさらに提示する、前記（７）～（１０）のいずれか一項に記載の情報処理装置。

（１２）

秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分散先をユーザの選択に基づいて制御することと、

前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、前記秘密鍵による電子署名を生成することと、

前記電子署名が付されたトランザクションをブロックチェーンに発行することと、

前記ブロックチェーン上の前記トランザクションに付された前記電子署名が前記複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証することと、

を含む、コンピュータによる情報処理方法。

（１３）

コンピュータを、

秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分散先をユーザの選択に基づいて制御する分散先制御部と、

前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、
前記秘密鍵による電子署名を生成する署名生成部と、

前記電子署名が付されたトランザクションをブロックチェーンに発行する
トランザクション発行部と、

前記ブロックチェーン上の前記トランザクションに付された前記電子署名
が前記複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証
する監査部と、

として機能させるためのプログラム。

符号の説明

[0097]	1 0	情報処理システム
	1 0 0	情報処理装置
	1 1 0	入力部
	1 2 0	候補提示部
	1 3 0	分散先制御部
	1 4 0	署名生成部
	1 5 0	トランザクション発行部
	1 6 0	監査部
	1 7 0	通信部
	T r	トランザクション
	E S	電子署名
	S K	秘密鍵
	F r	分散片

請求の範囲

- [請求項1] 秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分散先をユーザの選択に基づいて制御する分散先制御部と、
- 前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、前記秘密鍵による電子署名を生成する署名生成部と、
- 前記電子署名が付されたトランザクションをブロックチェーンに発行するトランザクション発行部と、
- 前記ブロックチェーン上の前記トランザクションに付された前記電子署名が前記複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証する監査部と、
- を備える、情報処理装置。
- [請求項2] 前記署名生成部は、前記複数の分散片のうち所定の数の前記分散片を用いて、前記電子署名を生成する、請求項1に記載の情報処理装置。
- [請求項3] 前記複数の分散先は、前記ユーザが所有する端末、前記トランザクションに関するサービスを提供する事業者が管理するサーバ、又は第三者機関が管理するサーバを含む、請求項1に記載の情報処理装置。
- [請求項4] 前記複数の分散先は、前記ユーザが所有する端末を少なくとも含み、
- 前記署名生成部は、前記ユーザが所有する端末に保管された前記分散片を少なくとも用いて、前記電子署名を生成する、請求項3に記載の情報処理装置。
- [請求項5] 前記分散先制御部は、前記ユーザに選択された前記複数の分散先と協働することで、前記複数の分散片の生成プロセスを実行する、請求項1に記載の情報処理装置。
- [請求項6] 前記複数の分散先が変更される場合、前記分散先制御部は、前記複数の分散片の各々に含まれる乱数成分を再設定する、請求項1に記載の情報処理装置。

- [請求項7] 前記複数の分散先の候補を前記ユーザに提示する候補提示部をさらに備え、
- 前記ユーザは、提示された前記候補の中から前記複数の分散片の各々を保管する前記複数の分散先を選択する、請求項1に記載の情報処理装置。
- [請求項8] 前記候補提示部は、前記ユーザに選択された前記複数の分散先の組み合わせの信頼度を導出すると共に、導出した前記信頼度を前記ユーザにさらに提示する、請求項7に記載の情報処理装置。
- [請求項9] 前記信頼度は、前記組み合わせに含まれる前記分散先の数、前記分散先の互いの共通項、前記分散先の各々のセキュリティ強度、又は前記分散先の各々の過去実績の少なくとも1つ以上を参照する所定のルールに基づいて導出される、請求項8に記載の情報処理装置。
- [請求項10] 前記候補提示部は、前記信頼度の導出根拠を前記ユーザにさらに提示する、請求項9に記載の情報処理装置。
- [請求項11] 前記候補提示部は、前記複数の分散先の候補の推奨される組み合わせを前記ユーザにさらに提示する、請求項7に記載の情報処理装置。
- [請求項12] 秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分散先をユーザの選択に基づいて制御することと、
- 前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、前記秘密鍵による電子署名を生成することと、
- 前記電子署名が付されたトランザクションをブロックチェーンに発行することと、
- 前記ブロックチェーン上の前記トランザクションに付された前記電子署名が前記複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証することと、
- を含む、コンピュータによる情報処理方法。
- [請求項13] コンピュータを、
- 秘密鍵を秘密分散させた複数の分散片をそれぞれ保管する複数の分

散先をユーザの選択に基づいて制御する分散先制御部と、

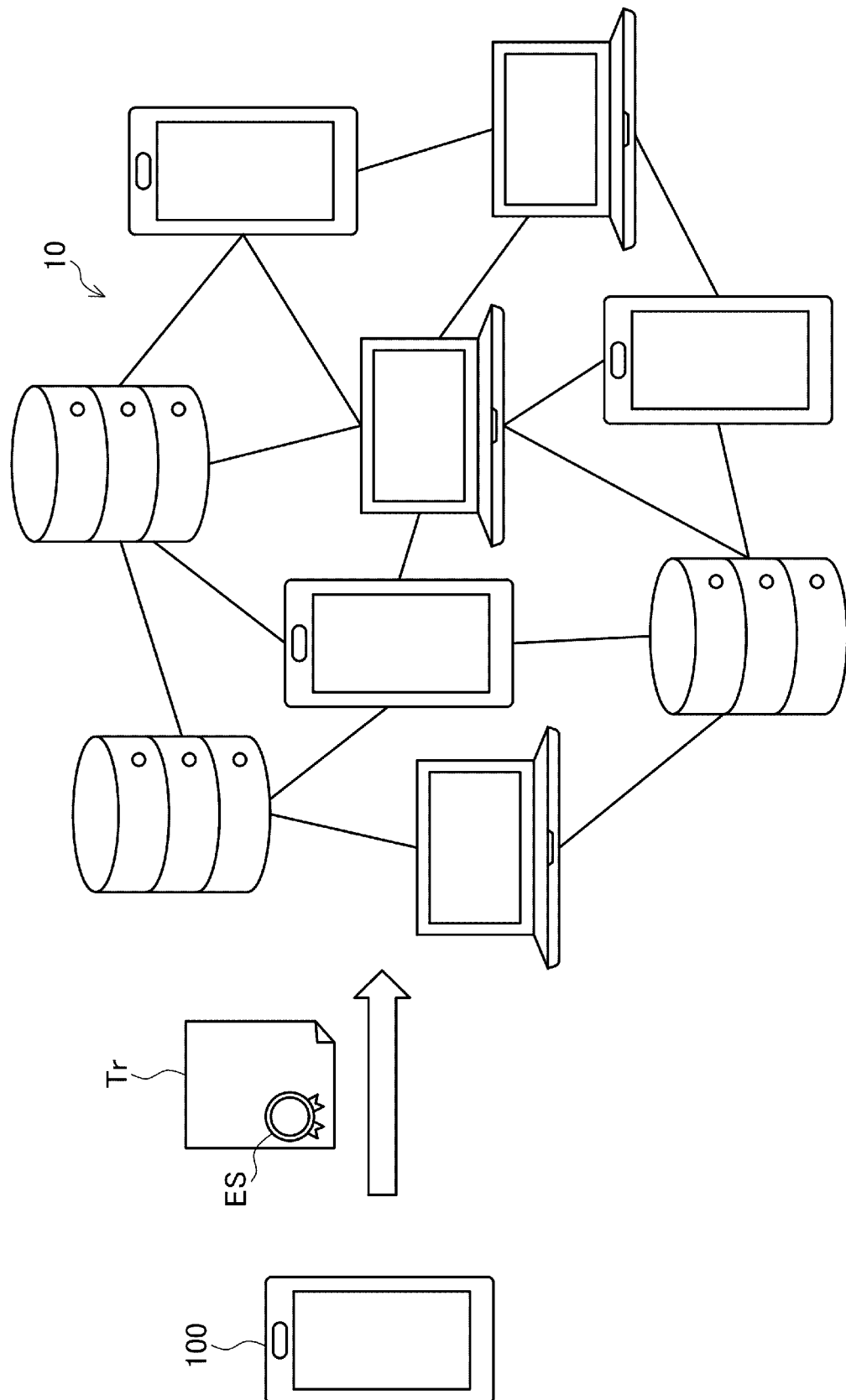
前記複数の分散先に保管された前記複数の分散片のうちの一部を用いて、前記秘密鍵による電子署名を生成する署名生成部と、

前記電子署名が付されたトランザクションをブロックチェーンに発行するトランザクション発行部と、

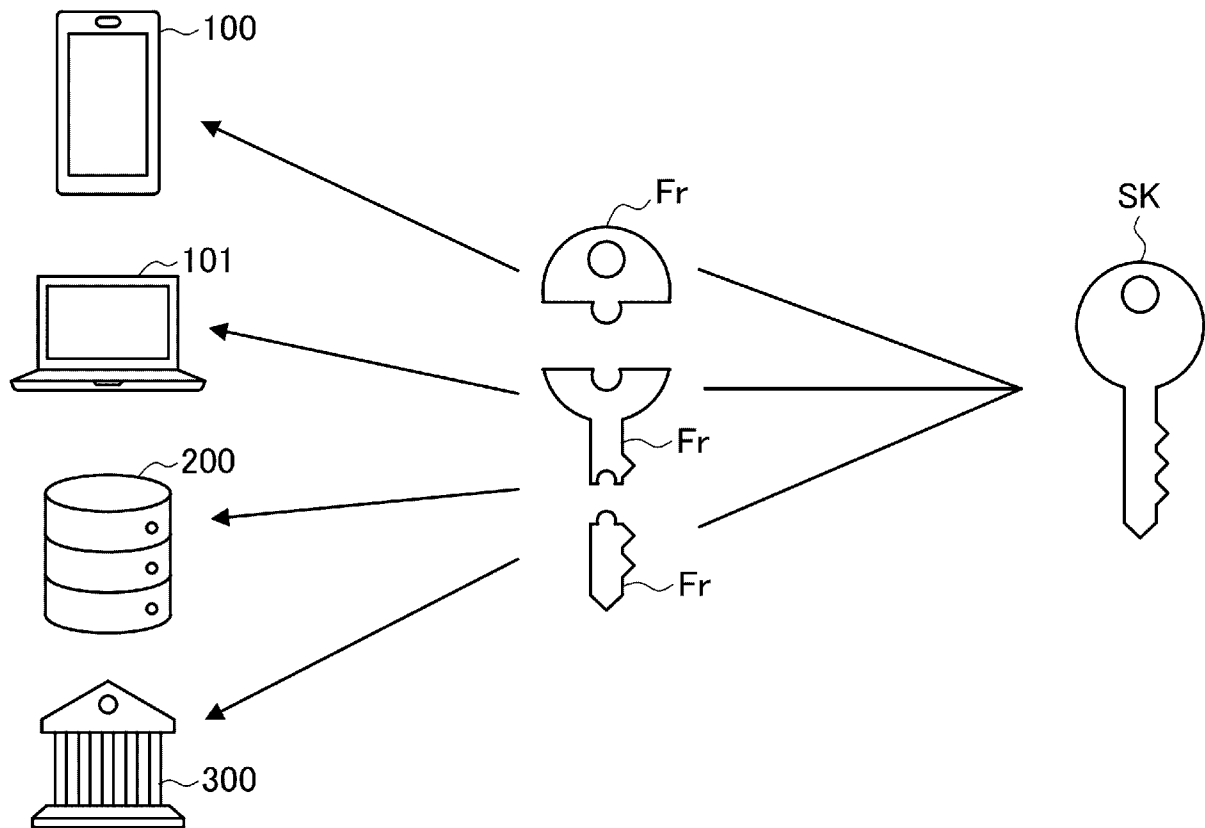
前記ブロックチェーン上の前記トランザクションに付された前記電子署名が前記複数の分散片のうちのいずれの分散片を用いて生成されたのかを検証する監査部と、

として機能させるためのプログラム。

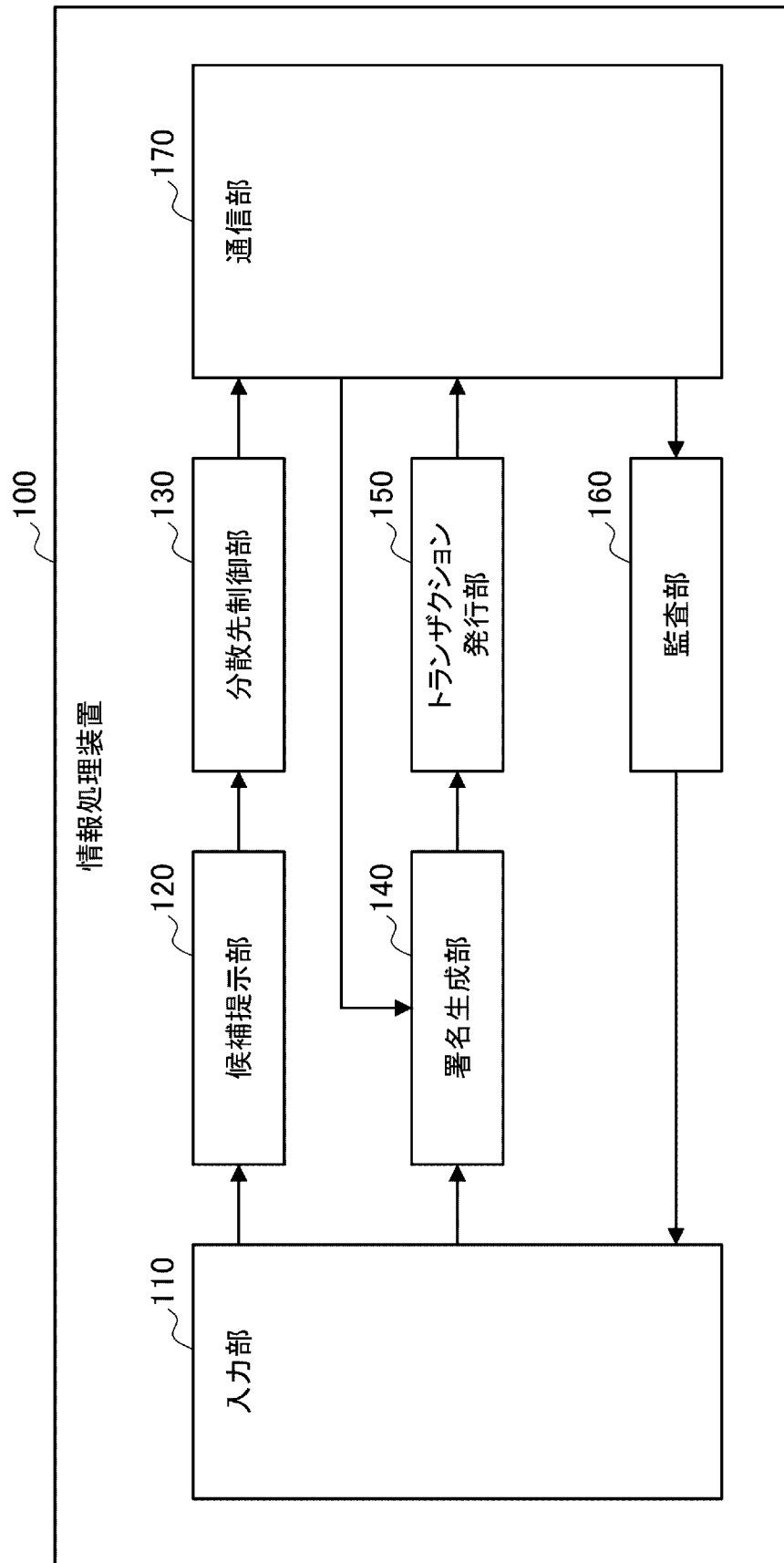
[図1]



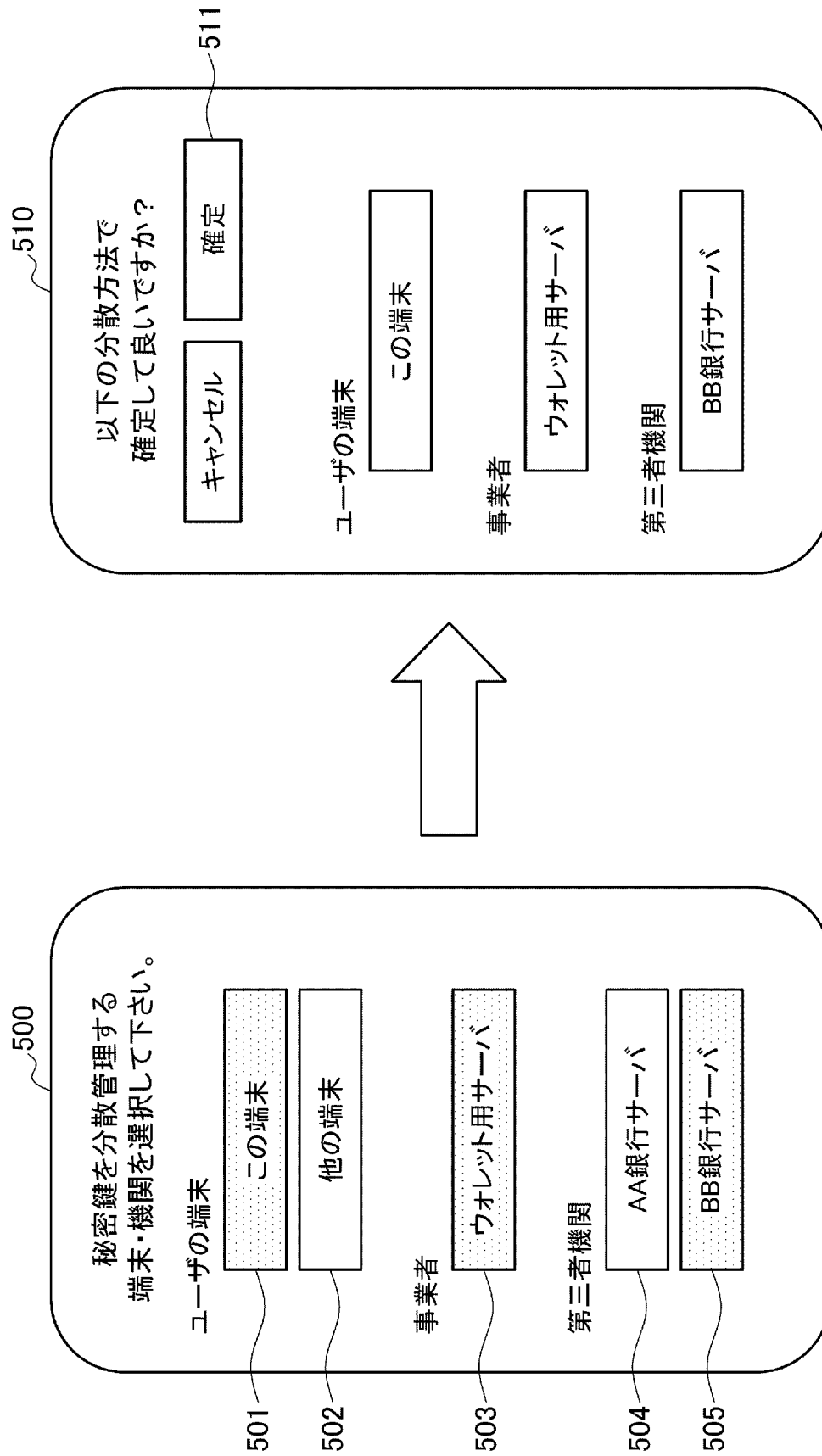
[図2]



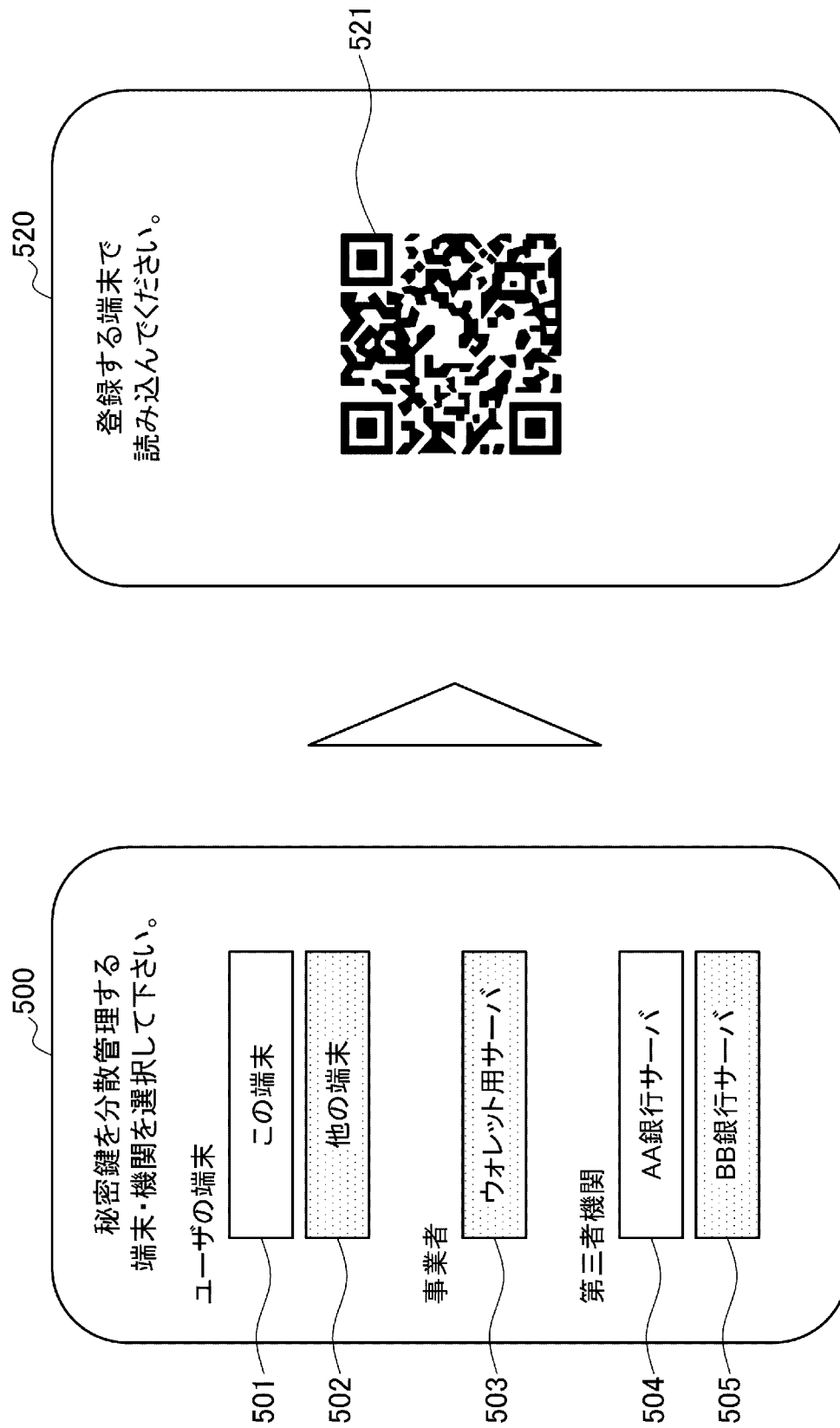
[図3]



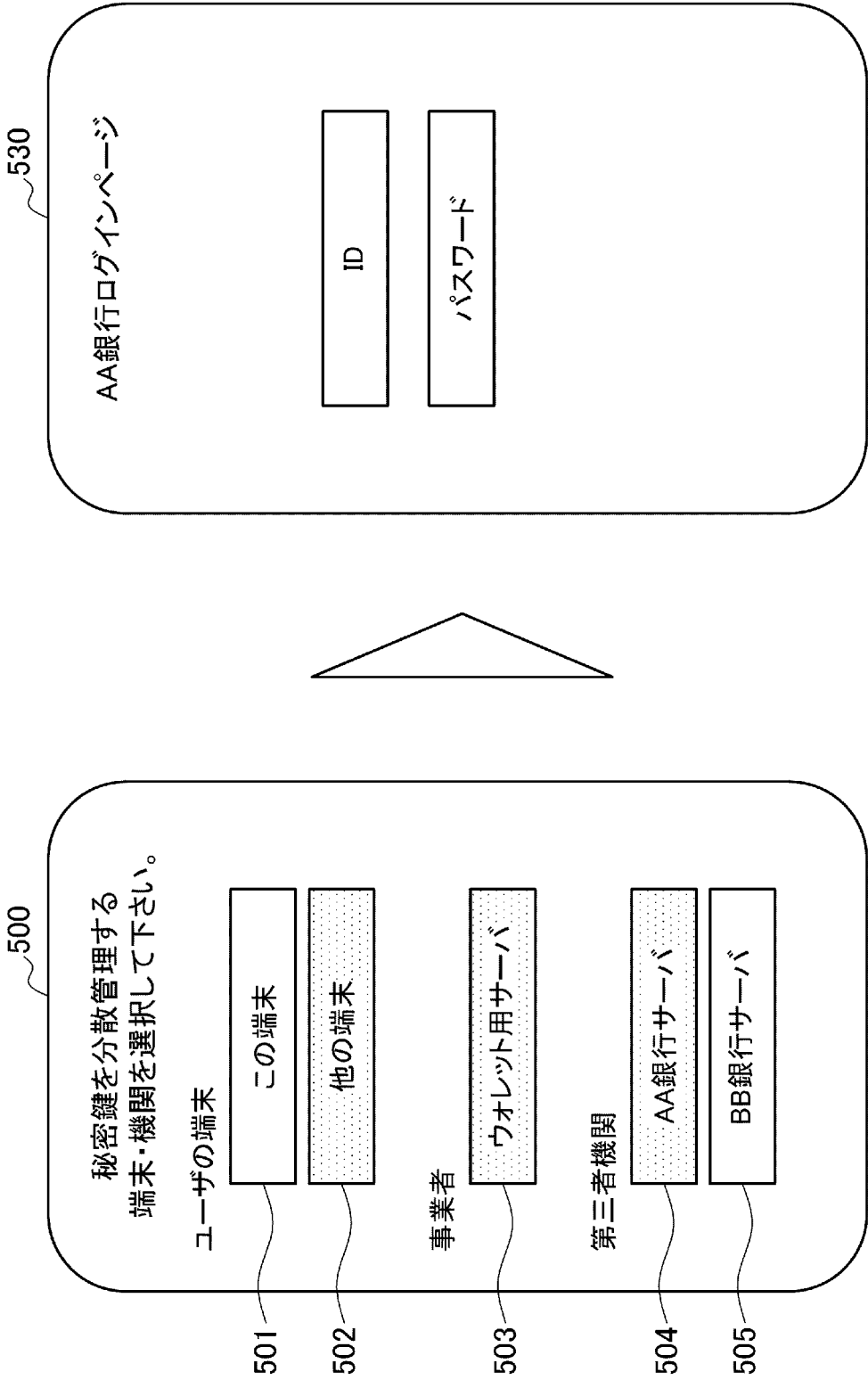
[図4]



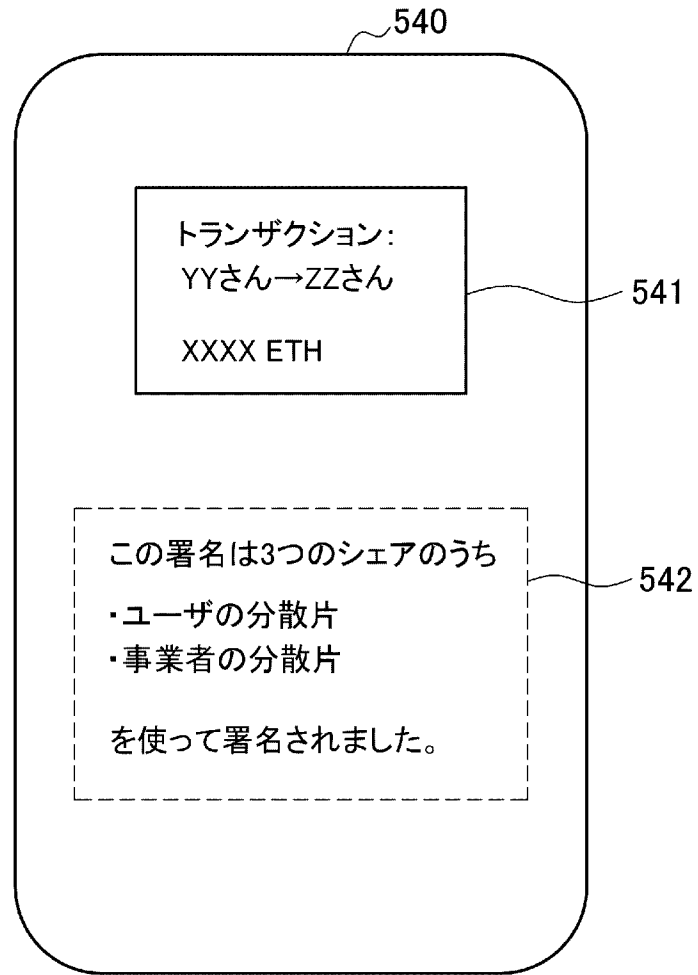
[図5]



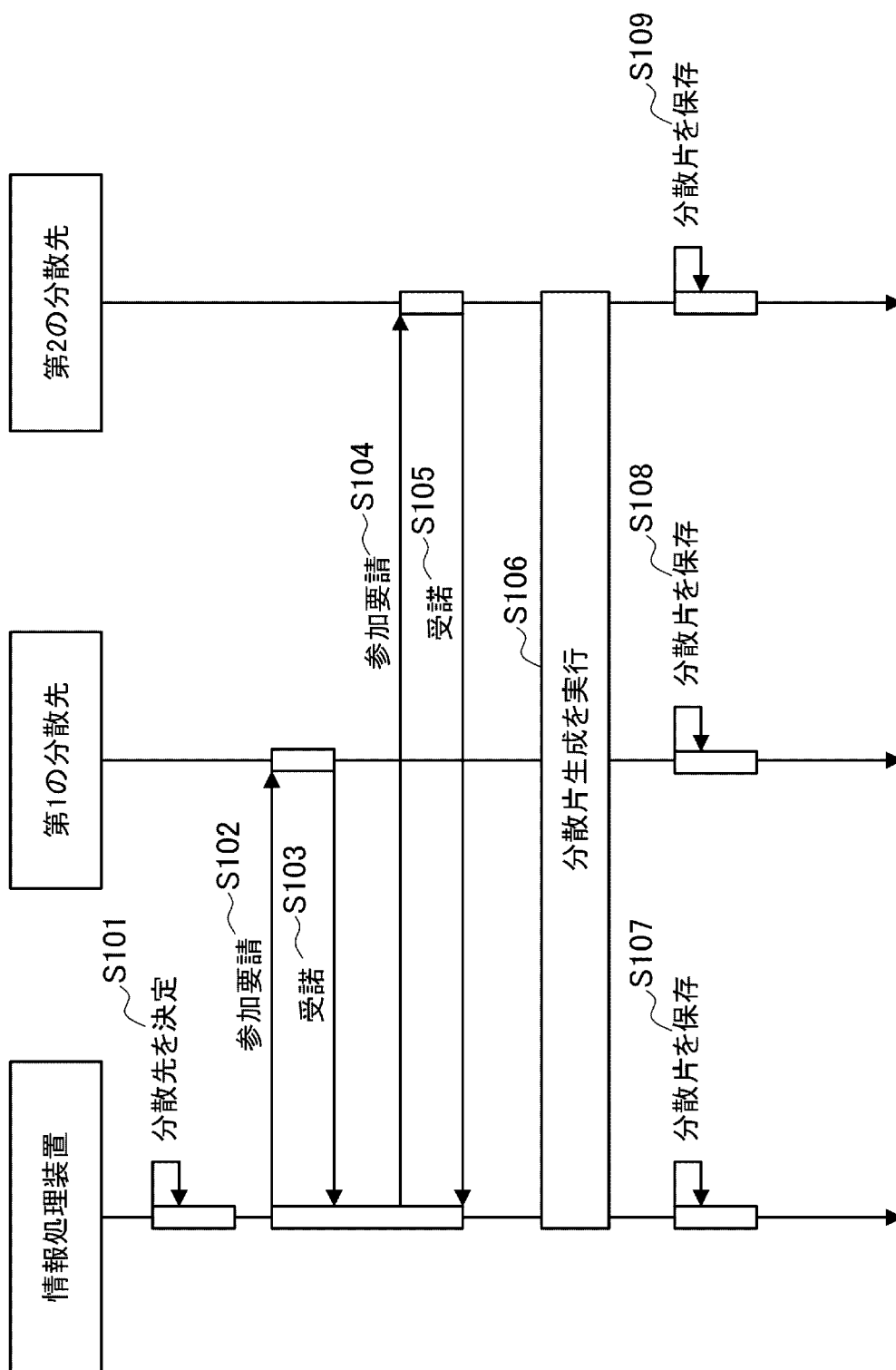
[図6]



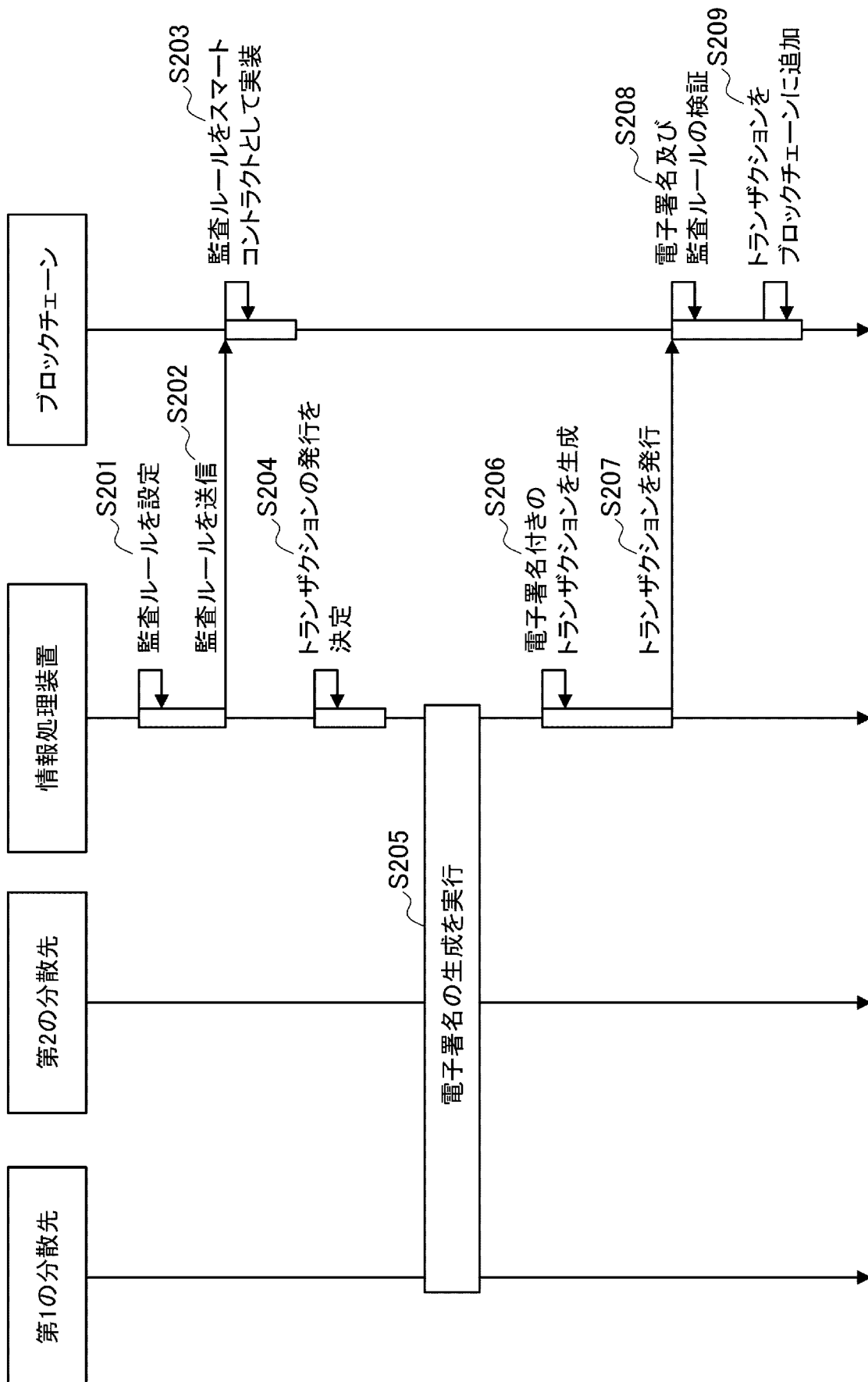
[図7]



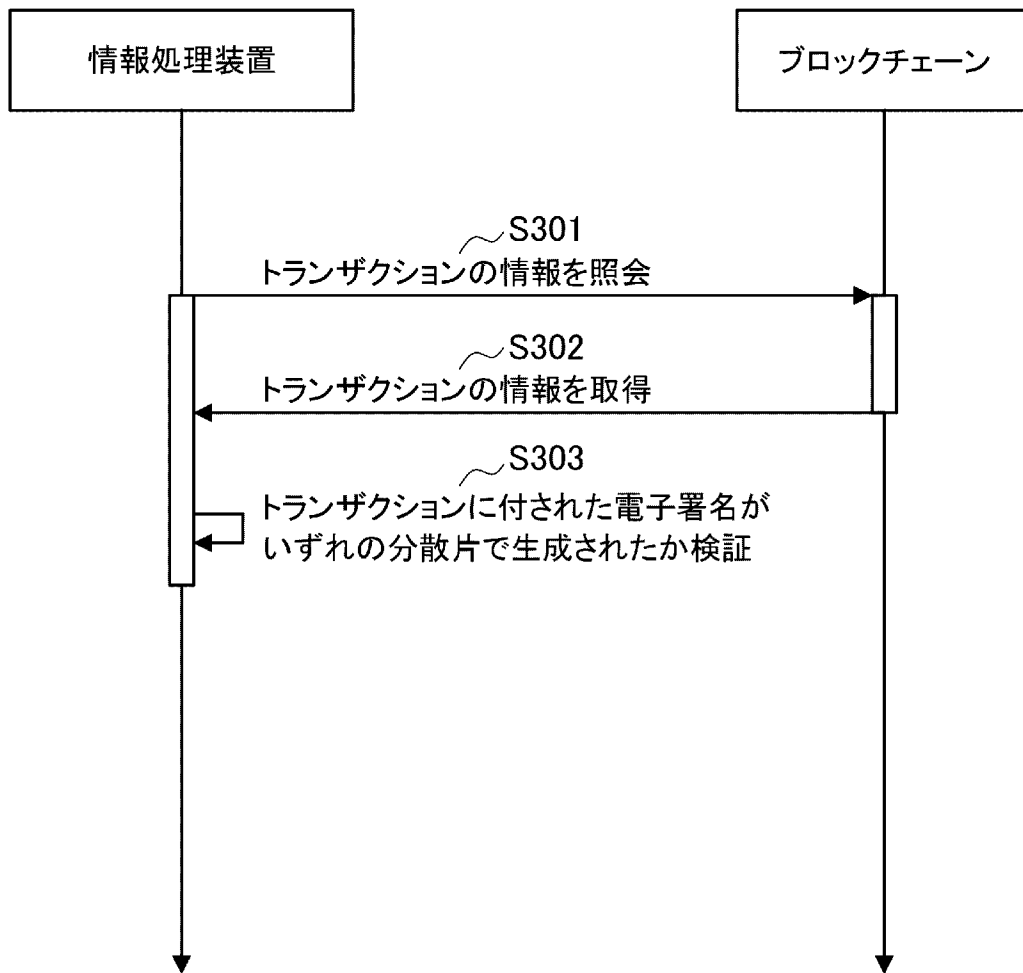
[図8]



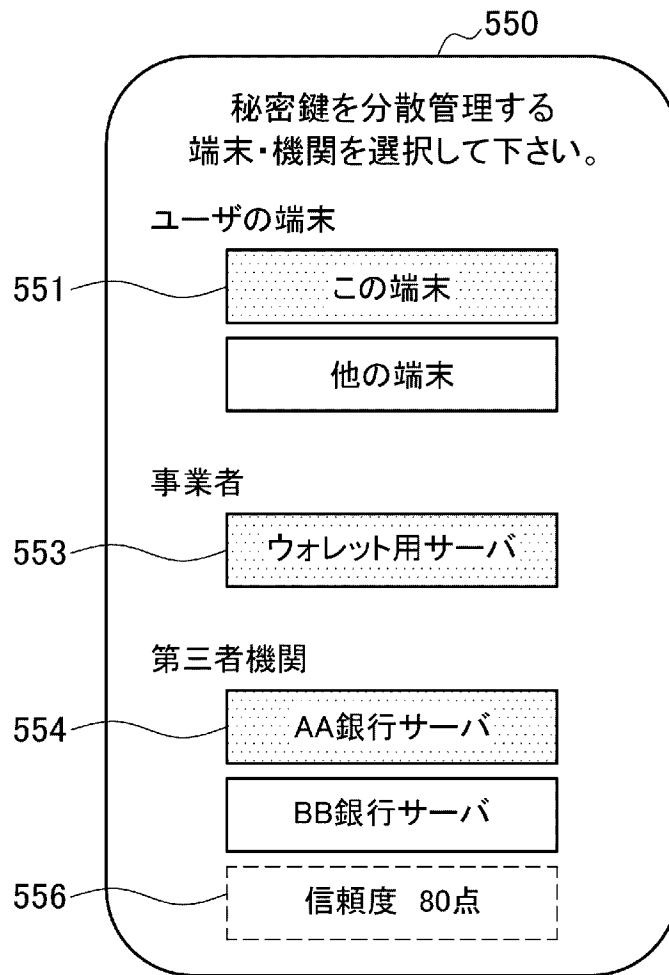
[図9]



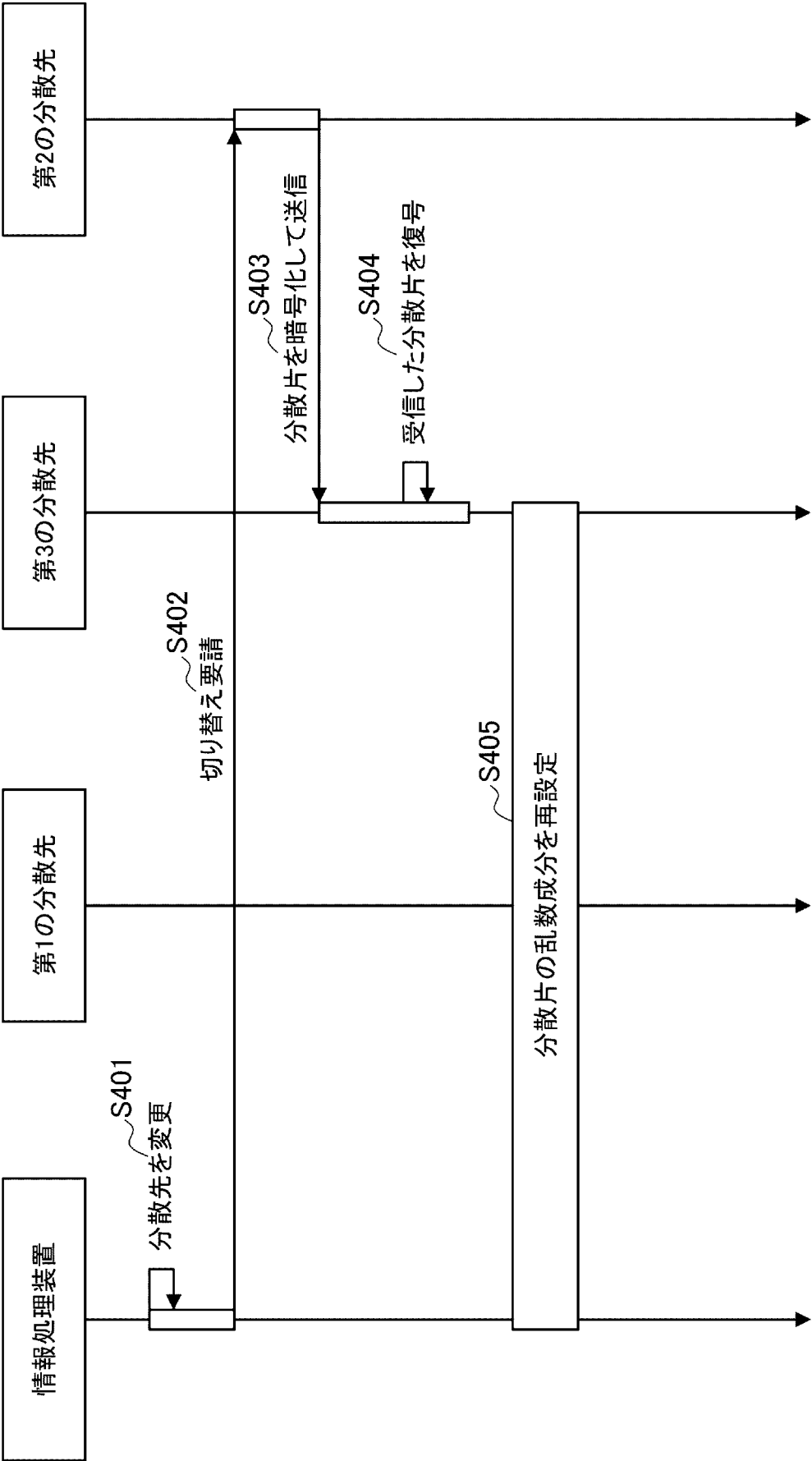
[図10]



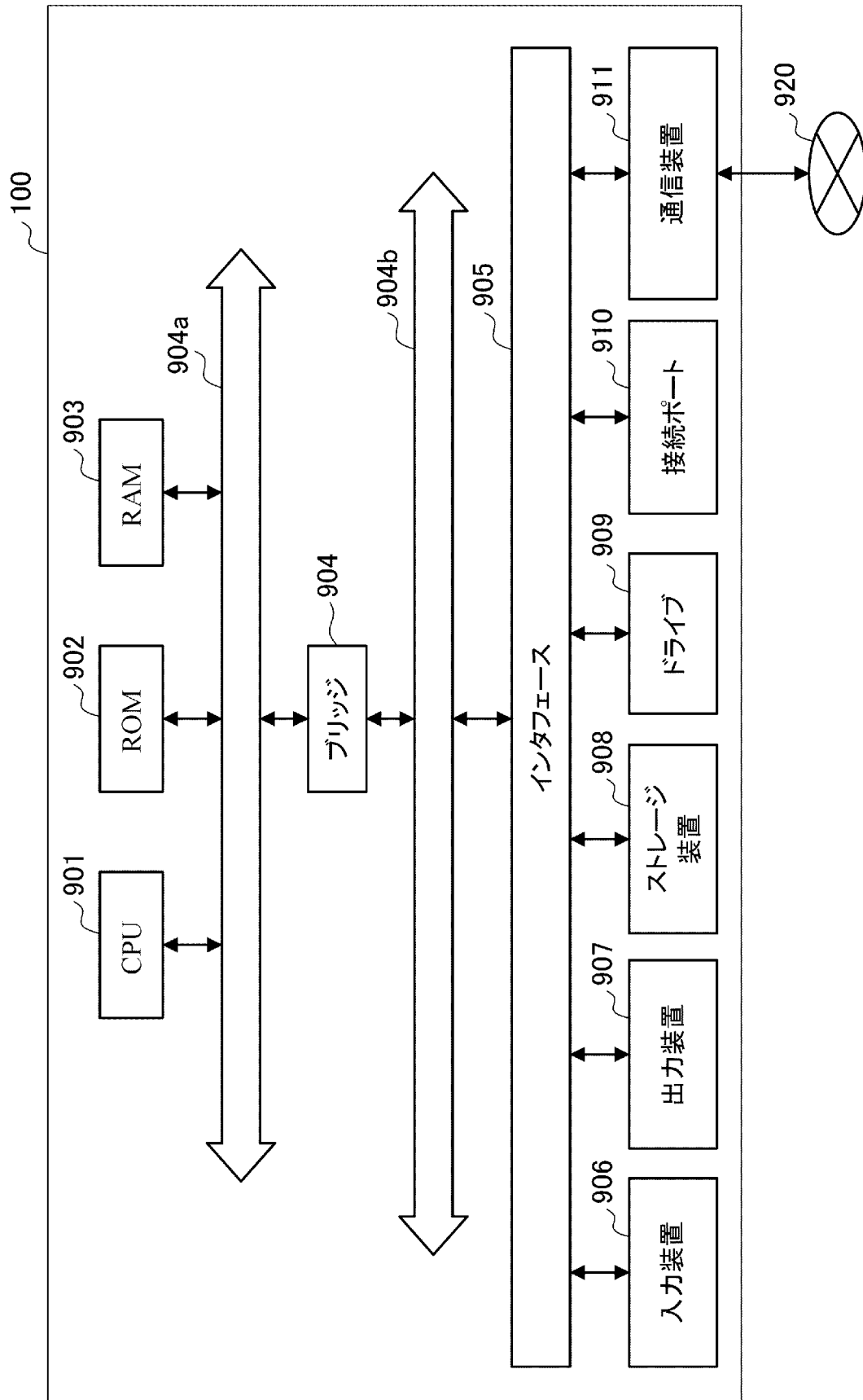
[図11]



[図12]



[図13]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2024/000037

A. CLASSIFICATION OF SUBJECT MATTER H04L 9/32 (2006.01)i; H04L 9/08 (2006.01)i FI: H04L9/32 200B; H04L9/08 A 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) H04L9/32; H04L9/08 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) JSTPlus/JMEDPlus/JST 7580 (JDreamIII); Science Direct; IEEE Xplore threshold signature, traceability		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 2022/0239509 A1 (SAMSUNG ELECTRONICS CO., LTD.) 28 July 2022 (2022-07-28) paragraphs [0075]-[0119], [0225]-[0240]	1-7, 11-13 8-10
Y	VAN DER MERWE, J. DAWOUD, D. S. and MCDONALD, S. A Fully Distributed Proactively Secure Threshold-Multisignature Scheme. IEEE Transactions on Parallel and Distributed Systems. April 2007, vol. 18 no. 4, pp. 562-575 see all pages	1-7, 11-13
Y A	WO 2022/037869 A1 (NCHAIN LICENSING AG) 24 February 2022 (2022-02-24) p. 2, line 22 to p. 3, line 2, p. 26, line 11 to p. 32, line 20, p. 44, line 15 to p. 49, line 6	1-7, 11-13 8-10
☒ 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 07 March 2024		Date of mailing of the international search report 19 March 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.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	HWANG, M. -S. and CHANG, T. -Y. Threshold Signatures: Current Status and Key Issues. International Journal of Network Security, [online]. 01 November 2005, vol. 1, no. 3, pp. 123-137, retrieved from the Internet: <URL:http://ijns.jalaxy.com.tw/contents/ijns-v 1-n 3.html>, [retrieved on 11 March 2024] pp. 125-126 (t, n) Threshold Signature with Traceability/Untraceability	1-13
A	BONEH, D. and KOMLO, C. Threshold Signatures with Private Accountability. Cryptology ePrint Archive, Paper 2022/1636 ver:20221124:151741, [online]. November 2022, pp. 1-35, retrieved from the Internet: <URL:https://eprint.iacr.org/archive/2022/1636/20221124:151741>, [retrieved on 11 March 2024] abstract, 1 Introduction, 3.3 Accountable Therseshold Schemes(ATS), 5.1 A review of the Schnorr ATS schemes	1-13

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/JP2024/000037

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2022/0239509	A1	28 July 2022	WO	2021/075867	A1	
				KR	10-2021-0046357	A	

WO	2022/037869	A1	24 February 2022	JP	2023-539432	A	
				US	2023/0308287	A1	
				EP	4169206	A1	
				CN	115885498	A	

A. 発明の属する分野の分類（国際特許分類（IPC））

H04L 9/32(2006.01)i; H04L 9/08(2006.01)i

FI: H04L9/32 200B; H04L9/08 A

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））

H04L9/32; H04L9/08

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）

JSTPlus/JMEDPlus/JST7580 (JDreamIII); Science Direct; IEEE Xplore threshold signature, traceability

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 2022/0239509 A1 (SAMSUNG ELECTRONICS CO., LTD.) 28.07.2022 (2022-07-28)	1-7, 11-13
A	段落[0075]-[0119], [0225]-[0240]	8-10
Y	VAN DER MERWE, J., DAWOUD, D. S. and MCDONALD, S., A Fully Distributed Proactively Secure Threshold-Multisignature Scheme, IEEE Transactions on Parallel and Distributed Systems, 2007.04, Vol.18 No.4, pp.562-575	1-7, 11-13
	全頁を参照	
Y	WO 2022/037869 A1 (NCHAIN LICENSING AG) 24.02.2022 (2022-02-24)	1-7, 11-13
A	2頁22行-3頁2行, 26頁11行-32頁20行, 44頁15行-49頁6行	8-10
A	HWANG, M. -S. and CHANG, T. -Y., Threshold Signatures: Current Status and Key Issues, International Journal of Network Security, [online], 2005.11.01, Vol.1, No.3, pp.123-137, retrieved from the Internet: <URL:http://ijns.jalaxy.com.tw/contents/ijns-v1-n3.html>, [retrieved on 2024.03.11]	1-13
	pp.125-126 (t, n) Threshold Signature with Traceability/Untraceability	

☒ 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

07.03.2024

国際調査報告の発送日

19.03.2024

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）

中里 裕正 5S 9364

電話番号 03-3581-1101 内線 3546

様式 PCT/ISA/210（第2ページ）（2022年7月）

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
A	BONEH, D. and KOMLO, C., Threshold Signatures with Private Accountability, Cryptology ePrint Archive, Paper 2022/1636 ver:20221124:151741, [online], 2022.11, pp.1-35, retrieved from the Internet: <URL:https://eprint.iacr.org/archive/2022/1636/20221124:151741>, [retrieved on 2024.03.11] Abstract, 1 Introduction, 3.3 Accountable Threshold Schemes(ATS), 5.1 A review of the Schnorr ATS schemes	1-13

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/JP2024/000037

引用文献			公表日	パテントファミリー文献			公表日
US	2022/0239509	A1	28.07.2022	WO	2021/075867	A1	
				KR	10-2021-0046357	A	

WO	2022/037869	A1	24.02.2022	JP	2023-539432	A	
				US	2023/0308287	A1	
				EP	4169206	A1	
				CN	115885498	A	
