(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
2017 年 6 月 29 日(29.06.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/109994 A1

(51) 国際特許分類:
G07D 9/00 (2006.01)

(21) 国際出願番号: PCT/JP2015/086412

(22) 国際出願日: 2015 年 12 月 25 日(25.12.2015)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人: 日立オムロンターミナルソリューションズ株式会社 (HITACHI-OMRON TERMINAL SOLUTIONS, CORP.) [JP/JP]; 〒1418576 東京都品川区大崎一丁目６番３号 Tokyo (JP).

(72) 発明者: 水野　英治(MIZUNO, Eiji); 〒1418576 東京都品川区大崎一丁目６番３号　日立オムロンターミナルソリューションズ株式会社内 Tokyo (JP). 緒方　日佐男(OGATA, Hisao); 〒1418576 東京都品川区大崎一丁目６番３号　日立オムロンターミナルソリューションズ株式会社内 Tokyo (JP).

(74) 代理人: 大賀　眞司, 外 (OHGA, Shinji et al.); 〒1400002 東京都品川区東品川二丁目３番１２号 シーフォートスクエア　センタービルディング１６階　サンネクスト国際特許事務所 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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

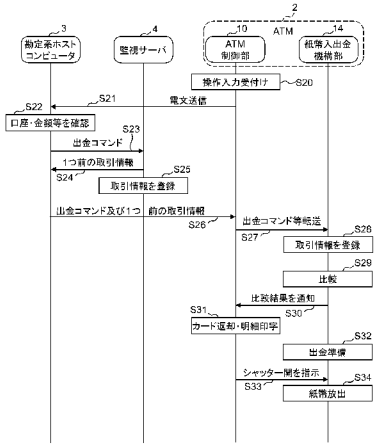
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨー

[続葉有]

(54) **Title**: AUTOMATED TRANSACTION SYSTEM

(54) 発明の名称 : 自動取引システム

図 4



3 Calculation system host computer
4 Monitoring server
10 ATM control unit
14 Paper currency deposit/withdrawal mechanism unit
S20 Accept operation input
S21 Transmit electronic message
S22 Verify account, amount, etc.
S23 Withdrawal command
S24 Information of immediately preceding transaction
S25, S28 Register transaction information
S26 Withdrawal command and information of immediately preceding transaction
S27 Transfer of withdrawal command, etc.
S29 Comparison
S30 Issue notification of comparison result
S31 Return card, print out statement
S32 Prepare for withdrawal
S33 Instruct shutter to open
S34 Discharge paper currency

(57) **Abstract**: [Problem] To provide a highly reliable automated transaction system which is capable of keeping damage due to malware to a minimum. [Solution] Provided is an automated transaction system in which a first storage unit which stores first transaction information is disposed in a paper currency transaction device and a second storage unit which stores the first transaction information is disposed in an external device. With regard to a second transaction which is a transaction which takes place after a first transaction: an ATM control unit transmits second transaction information which includes second amount information which is information which relates to the amount which is being handled in the second transaction; the external device transmits the first transaction information which is stored in the second storage unit; and the paper currency transaction device receives the first transaction information which the external device has transmitted and the second transaction information, determines whether the first transaction information which is stored in the first storage unit matches the first transaction information which the external device has transmitted, and if the respective instances of the first transaction information match, carries out a conveyance of paper currency on the basis of the second amount information which is included in the second transaction information.

(57) 要約:

[続葉有]

WO 2017/109994 A1

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, 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:

— 国際調査報告（条約第 21 条(3)）

【課題】 マルウェアによる被害を最小限に留め得る、信頼性の高い自動取引システムを提案する。
【解決手段】 自動取引システムにおいて、第１の取引情報を記憶する第１の記憶部を紙幣取引装置に設けると共に、第１の取引情報を記憶する第２の記憶部を外部の装置に設け、第１の取引後の取引である第２の取引において、ＡＴＭ制御部は、第２の取引で扱われる金額に関する情報である第２の金額情報を含む第２の取引情報を送信し、外部の装置は、第２の記憶部に記憶される第１の取引情報を送信し、紙幣取扱装置は、第２の取引情報と、外部の装置の送信した第１の取引情報とを受信し、第１の記憶部に記憶される第１の取引情報と、外部の装置の送信した第１の取引情報とが一致するか否かを判断し、一致した場合に、第２の取引情報に含まれる第２の金額情報に基づき、紙幣の搬送を行うようにした。

明　細　書

発明の名称 ： 自動取引システム

技術分野

[0001] 本発明は自動取引システムに関し、例えば、クレジットカードやキャッシュカードに記録された情報と利用者の操作とに基づいて入出金取引を行う自動取引システムに適用して好適なものである。

背景技術

[0002] 従来、ＡＴＭ（Automated Teller Machine）等の自動取引装置において実行された不正な取引を検出する方法として、特許文献１や特許文献２に開示された方法が知られている。具体的に、特許文献１には、店舗等にある入出金装置に保管された紙幣の売上集計の違算についてユーザの不正が関与していないかを確認する技術が述べられている。また、特許文献２には、取引のログデータと比較を行い、自動取引装置を利用するユーザの性質と比較して不審な形態の取引を自動的に検出し、それぞれに応じた対処を施す技術が述べられている。

先行技術文献

特許文献

[0003] 特許文献1：特開２０１３－１７１３１３号公報

特許文献2：特開２００７－１９９８８１号公報

発明の概要

発明が解決しようとする課題

[0004] ところで、自動取引装置の全体を制御するＡＴＭ制御部には、紙幣入出金機構部を制御するアプリケーションソフトや制御用のソフトウェアが組み込まれているが、これらのソフトウェアがマルウェアに乗っ取られた場合、不正な出金コマンドが紙幣入出金機構部に送信され、この出金コマンドに基づいて不正な出金処理が実行されるおそれがある。また入金取引の場合に、自動取引装置に投入された紙幣枚数以上に入金金額を増加させ、不正に口座残

高を増やすこともマルウェアにより可能になる。

[0005] 特に、近年、マルウェア（Malicious Software）の偽装技術は高度化され様々な情報機器産業に対して課題となっている。人為的管理ミスなどから防衛策をすり抜けてマルウェアの侵入を許してしまうことや、新たに作り出されたマルウェアの対策とシステムへの配備は時間を要するためにマルウェアの発見から対策までの間に被害が拡大してしまうケースを想定しておかなければいけない。

[0006] 本発明は以上の点を考慮してなされたもので、マルウェアによる被害を最小限に留め得る、信頼性の高い自動取引システムを提案しようとするものである。

課題を解決するための手段

[0007] かかる課題を解決するため本発明においては、紙幣を用いた取引を行う自動取引システムであって、第１の取引で扱われる金額に関する情報である第１の金額情報を含む第１の取引情報を送信するＡＴＭ制御部と、前記第１の取引情報を受信し、前記第１の取引情報に含まれる前記第１の金額情報に基づき紙幣の搬送を行う紙幣取扱装置と、前記紙幣取扱装置に設けられ、前記紙幣取扱装置の受信した前記第１の取引情報を記憶する第１の記憶部と、前記紙幣取扱装置の外部の装置に設けられ、前記外部の装置が受信した前記第１の取引情報を記憶する第２の記憶部とを設け、前記第１の取引後の取引である第２の取引において、前記ＡＴＭ制御部は、前記第２の取引で扱われる金額に関する情報である第２の金額情報を含む第２の取引情報を送信し、前記外部の装置は、前記第２の記憶部に記憶される前記第１の取引情報を送信し、前記紙幣取扱装置は、前記第２の取引情報と、前記外部の装置の送信した前記第１の取引情報とを受信し、前記第１の記憶部に記憶される前記第１の取引情報と、前記外部の装置の送信した前記第１の取引情報とが一致するか否かを判断し、一致した場合に、前記第２の取引情報に含まれる前記第２金額情報に基づき、紙幣の搬送を行うようにした。

[0008] 本発明の自動取引システムによれば、ＡＴＭ制御部がマルウェアに感染し

て不正な第２の取引情報を紙幣取扱装置に送信した場合においても、マルウェアは第１の取引情報を保持しないため、当該第２の取引情報に従って紙幣取扱装置が紙幣の搬送を行うことはない。またマルウェアが取引情報を傍受し記録する機能を有するものであっても、次の正常な取引の際に第１の記憶部に記憶されている第１の取引情報と、ＡＴＭ制御部から紙幣取扱装置に送信される第１の取引情報とに齟齬が生じるため、当該次の正常な取引までの間に不正な取引があったことを検出することができる。

発明の効果

[0009] 本発明によれば、マルウェアによる被害を最小限に留め得る、信頼性の高い自動取引システムを実現できる。

図面の簡単な説明

[0010] [図1]第１～第３の実施の形態による自動取引システムの全体構成を示すブロック図である。

[図2]第１～第３の実施の形態による取引情報テーブルの構成を示す概念図である。

[図3]初期設定処理の流れを示すシーケンス図である。

[図4]第１の実施の形態による出金取引処理の流れを示すシーケンス図である。

[図5]不正取引が行われた場合の説明に供する概念図である。

[図6]第２の実施の形態による不正コマンドの検出処理の流れを示すシーケンス図である。

[図7]第３の実施の形態の説明に供するフローチャートである。

[図8]第４の実施の形態による自動取引システムの全体構成を示すブロック図である。

[図9]第４の実施の形態による出金取引処理の流れを示すシーケンス図である。

[図10]第４の実施の形態による取引情報テーブルの構成を示す概念図である。

発明を実施するための形態

[0011] 以下図面について、本発明の一実施の形態を詳述する。

[0012] （１）第１の実施の形態

（１－１）本実施の形態の自動取引システムの構成

図１において、１は全体として本実施の形態による自動取引システムを示す。この自動取引システム１は、１又は複数のＡＴＭ２と、勘定系ホストコンピュータ３及び監視サーバ４とを備え、これらがＬＡＮ（Local Area Network）又はＷＡＮ（Wide Area Network）などの広域ネットワーク５を介して接続されることにより構成されている。

[0013] ＡＴＭ２は、利用者の操作に応じて入出金等の取引を行う自動取引装置である。ＡＴＭ２は、ＡＴＭ制御部１０、操作部１１、明細票機構部１２、カード機構部１３及び紙幣入出金機構部１４などの内部デバイスを備える。

[0014] ＡＴＭ制御部１０は、ＡＴＭ２全体の動作制御を司るハードウェアである。実際上、ＡＴＭ制御部１０は、ＣＰＵ（Central Processing Unit）、メモリ及び通信装置等の情報処理資源を備えたコンピュータ構成を有し、ＣＰＵがメモリに格納されたプログラムに基づいて操作部１１、明細票機構部１２、カード機構部１３及び紙幣入出金機構部１４等の内部デバイスを制御することによりＡＴＭ２全体としての各種処理が実行される。

[0015] 操作部１１は、例えばタッチパネルを有し、タッチパネルに表示した各種操作案内に従って行われた利用者の操作入力を受け付け、受け付けた操作入力をＡＴＭ制御部１０に通知する。明細票機構部１２は、ＡＴＭ制御部１０から通知される取引内容を明細票に印字してＡＴＭ２の前面部に設けられた図示しない明細票排紙部から排紙する機能を有する内部デバイスである。

[0016] カード機構部１３は、例えばカードリーダから構成され、ＡＴＭ２の前面部に設けられた図示しないカード挿入口に挿入されたキャッシュカード等のカード媒体をＡＴＭ２内部に取り込み、そのカード媒体から利用者の口座番号等の必要な情報を読み出してＡＴＭ制御部１０に通知したり、ＡＴＭ２内部に取り込んだカード媒体を上述のカード挿入口から排出する機能を有する

。

[0017] また紙幣入出金機構部１４は、紙幣を搬送して現金の入出金を行う紙幣取扱装置として機能する内部デバイスである。紙幣入出金機構部１４は、金庫１５内に配置されることにより保護されており、金庫１５には紙幣入出金機構部１４が取り扱う紙幣を出し入れする際に開閉する金庫扉１６が設けられている。紙幣入出金機構部１４には、金庫扉１６の開閉状態を検出する検知部としてのセンサ１７が設けられている。

[0018] なお本実施の形態の場合、紙幣入出金機構部１４には、半導体メモリやハードディスク装置などから構成される記憶部１８が設けられており、そのＡＴＭ２において実行された各取引の取引内容等を表すログ情報（以下、これを取引情報と呼ぶ）が登録された取引情報テーブル１９がこの記憶部１８に保持される。

[0019] 一方、勘定系ホストコンピュータ３は、ＡＴＭ２の上位装置として当該ＡＴＭ２の利用者の口座や残高に関する各種情報を記憶し管理する機能を有するコンピュータ装置であり、ＣＰＵ２０、記憶装置２１及び通信装置２２等の情報処理資源を備えて構成される。

[0020] ＣＰＵ２０は、勘定系ホストコンピュータ３全体の動作制御を司るプロセッサである。また記憶装置２１は、半導体メモリ及びハードディスク装置などから構成され、主としてプログラムや必要な情報を保持するために利用される。記憶装置２１に格納されたプログラムをＣＰＵ２０が実行することにより、勘定系ホストコンピュータ３全体としての各種処理が実行される。通信装置２２は、例えば、ＮＩＣ（Network Interface Card）などから構成され、広域ネットワーク５を介した各ＡＴＭ２や監視サーバ４との通信時におけるプロトコル制御を行う。

[0021] 監視サーバ４は、各ＡＴＭ２において実行された取引を監視する機能を有する汎用のサーバ装置であり、ＣＰＵ３０、記憶装置３１、通信装置３２及び表示装置３３等の情報処理資源を備えて構成される。ＣＰＵ３０、記憶装置３１及び通信装置３２の機能及び構成は、勘定系ホストコンピュータ３の

対応部位（ＣＰＵ２０、記憶装置２１又は通信装置２２）と同様であるため、ここでの説明は省略する。表示装置３３は、例えば液晶ディスプレイや有機ＥＬ（ElectroLuminescence）ディスプレイ等から構成され、各種情報を表示するために利用される。

[0022] 監視サーバ４の記憶装置３１には、後述のように勘定系ホストコンピュータ３が各ＡＴＭ２にそれぞれ許可した各取引（以下においては出金取引とする）の内容を表す取引情報がすべて登録された取引情報テーブル３４が格納される。この取引情報は、勘定系ホストコンピュータ３が出金を許可するコマンド（出金する紙幣の金種及びその枚数を含むコマンドであり、以下、これを出金コマンドと呼ぶ）をＡＴＭ２に送信する際に当該勘定系ホストコンピュータ３から通知された内容に基づくものであり、ＡＴＭ２の紙幣入出金機構部１４の記憶部１８に格納された取引情報テーブル１９に登録されている各取引情報と同じデータフォーマットを有する。

[0023] なお、かかるＡＴＭ２の紙幣入出金機構部１４の記憶部１８に格納された取引情報テーブル１９及び監視サーバ４の記憶装置３１に格納された取引情報テーブル３４の構成を図２に示す。これら取引情報テーブル１９，３４の各行がそれぞれ１つの取引の内容を表す取引情報に相当する。

[0024] 取引情報テーブル１９，３４は、店舗番号欄４０、装置ＩＤ（Identification）欄４１、取引番号欄４２、取引日時欄４３、取引種別欄４４、ハッシュ値欄４５及び金額欄４６を備えて構成される。

[0025] そして店舗番号欄４０には、対象とする取引が行われたＡＴＭ２が設置されている店舗に付与されたその店舗に固有の番号（店舗番号）が格納され、装置ＩＤ欄４１には、その取引を行ったＡＴＭ２に付与されたそのＡＴＭ２に固有の識別子（装置ＩＤ）が格納される。また取引番号欄４２には、取引毎に付与されるその取引に固有の番号（取引番号）が格納される。本実施の形態の場合、ＡＴＭ制御部１０からの処理要求に応じてその取引に対して勘定系ホストコンピュータ３が付与したトランザクション番号がその取引の取引番号として利用される。

[0026] 取引日時欄４３には、その取引が行われた日時（取引日時）が格納され、取引種別欄４４には、その取引の種別（取引種別）が格納される。なお、取引種別としては、「出金」、「回収リセット」及び「初期設定ログ」などがある。「出金」は出金取引を表し、「回収リセット」は、その取引情報がＡＴＭ２の金庫１５（図１）内の紙幣の回収が行われたときに登録されるダミーの取引情報であることを表す。また「初期設定ログ」は、その取引情報がＡＴＭ２の設置時や、ＡＴＭ２の紙幣入出金機構部１４（図１）の記憶部１８（図１）が故障等により交換されたときに登録されるダミーの取引情報であることを表す。

[0027] さらに金額欄４６には、そのとき国内において発行されている各紙幣の種類（金種）にそれぞれ対応させて金種欄４６Ａが設けられると共に、これら金種欄４６Ａにそれぞれ対応させて枚数欄４６Ｂが設けられ、金種欄４６Ａに対応する金種の金額が格納され、枚数欄４６Ｂに対応する取引において入出金された対応する金種の枚数が格納される。

[0028] さらにハッシュ値欄４５には、対応する取引の店舗番号、装置ＩＤ、取引番号、取引日時、取引種別及び金額などの各情報から生成されたハッシュ値が格納される。このハッシュ値は、後述のようにＡＴＭ２の紙幣入出金機構部１４や監視サーバ４において、例えば、ＳＨＡ（Secure Hash Algorithm）－１やＳＨＡ－２などの共通のハッシュ関数を利用してそれぞれ算出されたものである。因みに、取引種別が「初期設定ログ」や「回収リセット」の場合には金種及び枚数は存在しないためその情報は省略される。

[0029] なお、監視サーバ４の記憶装置３１に保持された取引情報テーブル３４には、本自動取引システム１内の各ＡＴＭ２がそれぞれ行った取引の取引情報がすべて蓄積されるが、図２は、このうちの１つのＡＴＭ２（図２の場合は装置ＩＤが「1234」のＡＴＭ２）についての取引情報のみを抜き出して表示したものとして理解されたい。

[0030] （１－２）本自動取引システムにおける取引監視機能

次に、本実施の形態の自動取引システム１において実行される取引監視機

能について説明する。まず、ＡＴＭ２のＡＴＭ制御部１０（図１）が何らかの原因によりマルウェアに感染し、当該マルウェアによってＡＴＭ制御部１０から紙幣入出金機構部１４（図１）に不正な出金コマンドが与えられて不正な出金取引が行われた場合について考える。

[0031] この場合、かかる不正な出金取引は勘定系ホストコンピュータ３からの出金コマンドに基づいて実行されものではないため、監視サーバ４の記憶装置３１（図１）に蓄積された各ＡＴＭ２においてそれぞれ実行された取引の取引情報と、紙幣入出金機構部１４の記憶部１８に蓄積されたそのＡＴＭ２において実行された各取引の取引情報との間に齟齬が生じる。

[0032] そこで、本自動取引システム１では、勘定系ホストコンピュータ３がＡＴＭ２に出金コマンドを送信する際、監視サーバ４の記憶装置３１に保持されているそのＡＴＭ２が勘定系ホストコンピュータ３からの出金コマンドに基づいて実行した１つ前の取引の取引情報を併せてそのＡＴＭ２に送信する。

[0033] そしてＡＴＭ２側では、紙幣入出金機構部１４において、受信したかかる１つ前の取引の取引情報と、記憶部１８に格納されている１つ前の取引の取引情報とを比較して、これらが一致した場合にのみ取引を実行し、これらが一致しない場合には、その取引を中止して外部に異常を通知するようになされている。

[0034] 以下、このような取引監視機能に関連して本自動取引システム１において実行される各種処理の内容について説明する。

[0035] （１－２－１）初期設定処理

図３は、例えば、新たに設置したＡＴＭ２を稼働させる前に実行される初期設定処理の処理手順を示す。

[0036] 係員は、新たなＡＴＭ２を設置後、まず、そのＡＴＭ２の操作部１１を介して初期設定を行う旨の操作入力を行う。そして、かかるＡＴＭ２のＡＴＭ制御部１０は、この操作入力が与えられると、その操作入力を受け付け（Ｓ１）、そのとき金庫１５（図１）の金庫扉１６（図１）が開いているか否かを紙幣入出金機構部１４に問い合わせる（Ｓ２）。

[0037] この確認は正当な権限を持った係員が初期設定に立ち会っていることを確認するために行われるものであり、本実施の形態においては、金庫１５内の現金にアクセスできる係員が、金庫１５内の紙幣管理者として、初期設定の権限をもつものとする。ただし、例えばパスワードなど別の手段で係員の権限を確認しても良い。

[0038] そしてＡＴＭ制御部１０は、かかる問合せに対する紙幣入出金機構部１４からの回答を受信すると（Ｓ３）、この回答に基づいて金庫１５の金庫扉１６の開閉状態を判定し（Ｓ４）、かかる金庫扉１６が閉じていると判断した場合には、初期設定の権限を持つ係員が不在と判断して、この初期設定処理を終了する。従って、この場合には、ＡＴＭ２の初期設定を行うことができない。

[0039] これに対してＡＴＭ制御部１０は、ステップＳ４において、金庫１５の金庫扉１６が開いていると判断した場合には、初期設定を実行することを勘定系ホストコンピュータ３に通知する（Ｓ５）。

[0040] そして、この通知を受信した勘定系ホストコンピュータ３は、初期設定時のダミーの取引情報（以下、これを初期設定情報と呼ぶ）を生成する。この初期設定情報は、図２において取引種別が「初期設定ログ」である行の取引情報のうちのハッシュ値を除く情報である。そして勘定系ホストコンピュータ３は、生成した初期設定情報を監視サーバ４に送信する（Ｓ６）。かくして、この初期設定情報を受信した監視サーバ４は、受信した初期設定情報（店舗番号、装置ＩＤ、取引番号、取引日時及び取引種別）のハッシュ値を算出し、算出したハッシュ値を含む初期設定情報を記憶装置３１の取引情報テーブル３４に登録する（Ｓ７）。

[0041] また勘定系ホストコンピュータ３は、かかる初期設定情報を、ステップＳ５で初期設定の実行を通知してきたＡＴＭ２にも送信する（Ｓ８）。かくして、かかるＡＴＭ２のＡＴＭ制御部１０は、この初期設定情報を受信すると、これを紙幣入出金機構部１４に転送する（Ｓ９）。また、この初期設定情報を受信した紙幣入出金機構部１４は、受信した初期設定情報のハッシュ値

を監視サーバ４と同じハッシュ関数を用いて算出し、算出したハッシュ値を含む初期設定情報を記憶部１８に格納されている取引情報テーブル１９に登録する（Ｓ１０）。

[0042] 以上により、この一連の初期設定処理が終了する。

[0043] （１－２－２）出金取引処理

一方、図４は、本自動取引システム１において、利用者によりＡＴＭ２に対して出金取引の操作が行われた場合に実行される出金取引処理の処理手順を示す。

[0044] 利用者がキャッシュカード等のカード媒体を装填し、操作部１１を操作して暗証番号及び取引金額等の必要事項を入力後に操作部１１に表示された確認ボタンにタッチすると、そのＡＴＭ２のＡＴＭ制御部１０は、かかる操作入力を受け付け（Ｓ２０）、そのときカード機構部１３によりカード媒体から読み出された利用者の口座番号や、取引金額などの出金取引に必要な情報を含む処理要求の電文を生成して勘定系ホストコンピュータ３に送信する（Ｓ２１）。

[0045] 勘定系ホストコンピュータ３は、かかる電文を受信すると、図示しないデータベースを参照して、その利用者の口座番号や取引後の残高などを確認し（Ｓ２２）、取引可能な場合には、図２について上述した店舗番号、装置ＩＤ、取引番号、取引日時及び取引種別と、要求された金額を出金する際の金種及びその枚数とを含む出金コマンドを生成して、これを監視サーバ４に送信する（Ｓ２３）。

[0046] この出金コマンドを受信した監視サーバ４は、かかる出金取引の操作が行われたＡＴＭ２において実行された１つ前の取引に関する取引情報を記憶装置３１に格納されている取引情報テーブル３４から読み出し、これを勘定系ホストコンピュータ３に送信する（Ｓ２４）。また監視サーバ４は、この後、かかる出金コマンドに含まれている店舗番号、装置ＩＤ、取引番号、取引日時及び取引種別と、要求された金額を出金する際の金種及びその枚数とに基づいて図２について上述したハッシュ値を算出し、当該ハッシュ値を含め

たこれら店舗番号及び装置ＩＤ等の情報を、そのとき実行される出金取引の取引情報としてかかる取引情報テーブル３４に登録する（Ｓ２５）。

[0047] 一方、上述のようにして監視サーバ４から１つ前の取引の取引情報を取得した勘定系ホストコンピュータ３は、その取引情報と、ステップＳ２３で監視サーバ４に送信した出金コマンドと同じ出金コマンドとをかかる出金取引の操作が行われたＡＴＭ２に送信する（Ｓ２６）。

[0048] この出金コマンド及び１つ前の取引の取引情報を受信したＡＴＭ２のＡＴＭ制御部１０は、受信したこれら出金コマンド及び１つ前の取引の取引情報を紙幣入出金機構部１４に転送する（Ｓ２７）。

[0049] そして、これら出金コマンド及び１つ前の取引の取引情報を受信した紙幣入出金機構部１４は、かかる出金コマンドに含まれている店舗番号、装置ＩＤ、取引番号、取引日時及び取引種別と、要求された金額を出金する際の金種及びその枚数とに基づいて、ステップＳ２５において監視サーバ４がハッシュ値を算出したときと同じハッシュ関数を用いて図２について上述したハッシュ値を算出し、算出したハッシュ値と、出金コマンドに含まれる店舗番号及び装置ＩＤ等の情報とを、そのとき実行する出金取引の取引情報として記憶部１８内の取引情報テーブル１９に登録する（Ｓ２８）。

[0050] また紙幣入出金機構部１４は、この後、かかる出金コマンドと共に送信されてきた１つ前の取引の取引情報に含まれるハッシュ値と、かかる取引情報テーブル１９に格納されているそのＡＴＭ２が実行した１つ前の取引の取引情報に含まれるハッシュ値とを比較し（Ｓ２９）、これらが一致するか否かの比較結果をＡＴＭ制御部１０に通知する（Ｓ３０）。また紙幣入出金機構部１４は、かかる２つのハッシュ値が一致した場合にのみ、出金コマンドにおいて指定された各金種の紙幣を当該出金コマンドで指定された枚数だけそれぞれ紙幣取出し口に排出する出金準備を行う（Ｓ３２）。

[0051] 一方、ＡＴＭ制御部１０は、紙幣入出金機構部１４からの比較結果が、かかる２つのハッシュ値が一致しなかった旨の内容であった場合には、今回の取引が不正な取引の可能性があると判断して、今回の取引を中止して外部に

異常を通知する。ここで、外部への異常の通知とは、監視サーバ４の記憶装置３１に格納されている取引情報と、紙幣入出金機構部１４の記憶部１８に格納されている対応する取引情報とが不一致であったことの利用者又は係員への通知であり、ブザーや異常ランプの点灯、監視サーバへの異常情報発信などを含む。以下においても同様である。

[0052] これに対して、ＡＴＭ制御部１０は、紙幣入出金機構部１４からの比較結果が、かかる２つのハッシュ値が一致した旨の内容であった場合には、カード機構部１３（図１）を制御することにより、そのとき装填された利用者のカード媒体を利用者に返却させると共に、明細票機構部１２（図１）を制御することにより、明細票に今回の取引内容を印字させる（Ｓ３１）。

[0053] さらにＡＴＭ制御部１０は、紙幣取出し口（図示せず）を閉塞しているシャッターを開くよう紙幣入出金機構部１４に指示を与える（Ｓ３３）。かくして、紙幣入出金機構部１４は、この指示に従ってシャッターを開くことにより紙幣を放出し（Ｓ３４）、この後、利用者により紙幣が取り出されるとかかるシャッターを閉じる。以上により、一連の出金処理が終了する。

[0054] （１－３）本実施の形態の効果

以上のように本自動取引システム１では、ＡＴＭ２で実行された各取引の取引情報を監視サーバ４の記憶装置３１及びそのＡＴＭ２の紙幣入出金機構部１４の記憶部１８に蓄積し、勘定系ホストコンピュータ３がＡＴＭ２に出金コマンドを送信する際に、監視サーバ４の記憶装置３１に格納されているそのＡＴＭ２が実行した１つ前の取引の取引情報を併せてそのＡＴＭ２に送信し、当該ＡＴＭ２の紙幣入出金機構部１４において、その取引情報に含まれるハッシュ値と、記憶部１８に格納されている１つ前の取引の取引情報に含まれるハッシュ値とを比較し、これらが一致しない場合には、その取引を中止して外部に異常を通知する。

[0055] ここで、例えば、図２の例において、ＡＴＭ２が取引番号「34504」までの間正常に稼動をした後に、何らかの事象でＡＴＭ制御部１０がマルウェア３５（図１）に感染してしまい、マルウェア３５が紙幣入出金機構部１４に詐

称した出金コマンドを発行できる状態になったものとする。

[0056] この場合、マルウェア３５が詐称した出金コマンドを発行して不正な出金取引を実行するためには、ＡＴＭ２が１つ前に実行した取引の取引情報が必要となるが、マルウェア３５はそのような取引情報を保持しない。このため、例えマルウェア３５が詐称した出金コマンドを紙幣入出金機構部１４に発行したとしても、紙幣入出金機構部１４において実行される２つのハッシュ値の比較（図４のステップＳ２９）において、これら２つのハッシュ値が一致しない旨の比較結果が得られることとなり、不正な出金取引が成立することはない。

[0057] また、何らかの方法によりマルウェア３５は、何らかの不正な方法で監視サーバ４が保持するハッシュ値を含む取引情報を入手する場合も想定できる。その場合には、マルウェア３５が１つ前の取引の取引情報と出金コマンドとを紙幣入出金機構部１４へ送信することにより、不正な出金取引が成立することになる。

[0058] しかしながら、この場合には、図５に示すように、かかる不正な出金取引に関する取引情報（取引日時が「2015/11/15 14:10:10」、取引番号が「34505」の取引情報とする）が紙幣入出金機構部１４側の取引情報テーブル１９に残されるため、この後、勘定系ホストコンピュータ３から正常な出金コマンド及び１つ前の取引の取引情報が送られてきたときに、勘定系ホストコンピュータ３から送られてきた１つ前の取引の取引情報（図５の例では取引日時が「2015/11/15 13:39:40」、取引番号が「34504」の取引情報）に含まれるハッシュ値と、紙幣入出金機構部１４が保持する取引情報テーブル１９に保存されている１つ前の取引の取引情報（不正な出金取引に関する取引情報であり、図５の取引日時が「2015/11/15 14:10:10」、取引番号が「34505」の取引情報）に含まれるハッシュ値とが一致せず、過去に不正な取引があったことを検出することができる。

[0059] 従って、本自動取引システム１によれば、ＡＴＭ２のＡＴＭ制御部１０がマルウェア３５に感染した場合においても、そのマルウェア３５によって不

正な取引が実行されるのを有効に防止でき、そのマルウェア３５が勘定系ホストコンピュータ３からの出金コマンドを記録し保持するタイプのものであっても、その後、実行される正常な取引の際に不正な取引が実行されたことを検出することができる。かくするにつき、本実施の形態によれば、マルウェア３５による不正処理の被害を最小限に留めることができる、信頼性の高い自動取引システムを実現することができる。

[0060] （２）第２の実施の形態

第１の実施の形態の自動取引システム１では、勘定系ホストコンピュータ３が出金コマンドをＡＴＭ２に送信する際、常にそのＡＴＭ２で実行された１つ前の取引の取引情報を併せて送信するため、勘定系ホストコンピュータ３及び各ＡＴＭ２間で行われる通信の既存の通信プロトコルに対する変更量が大きい。

[0061] 一方、ＡＴＭ２は、一般に数日～１週間に１度の頻度でその内部に保有している現金と、勘定系ホストコンピュータ３で記録している、そのＡＴＭ２が保有しているべき現金の精査（一致の確認）が行われる。この精査の際には、ＡＴＭ２から現金を取り出して計数機などを用いて現金の現物確認を行う。そのときにＡＴＭ２から取り出した現金と、勘定系ホストコンピュータ３で記録している現金とが一致していない場合には、不正により現金が抜き取られている可能性がある。

[0062] この場合において、ＡＴＭ２から取り出した現金と、勘定系ホストコンピュータ３で記録している現金との不一致は、マルウェア３５による不正コマンドの発行だけでなく、現物盗難によっても発生する可能性がある。このため、これらが不一致であるというだけではマルウェア３５による不正コマンドの発行を検出することはできない。しかしながら、監視サーバ４が保持する取引情報テーブル３４に登録されている取引情報と、紙幣入出金機構部１４が保持する取引情報テーブル１９に登録されている取引情報とを比較することで、第１の実施の形態と同様に、マルウェア３５による不正コマンドの発行が過去にあったか否かを容易に検証することができる。

[0063] 以上の点を勘案して、本実施の形態では、ＡＴＭ２の精査を行うタイミングで監視サーバ４が保持する取引情報テーブル３４に格納されているそのＡＴＭ２で実行された過去の取引の取引情報と、そのＡＴＭ２の紙幣入出金機構部１４が保持する取引情報テーブル１９に登録されている取引情報とを比較する。これにより既存の通信プロトコルに影響を与えることなく、マルウェア３５による不正な取引を検出することができる。

[0064] 以下、このような本実施の形態による取引監視機能が搭載された本実施の形態による自動取引システム５０（図１）について説明する。

[0065] まず、本実施の形態の自動取引システム５０における出金処理の流れについて、図４を参照して説明する。上述のように本自動取引システム５０では、勘定系ホストコンピュータ５１（図１）は、通常の取引時には１つ前の取引の取引情報をＡＴＭ５２（図１）に送信しないため、ステップＳ２６では出金コマンドのみが勘定系ホストコンピュータ５１からＡＴＭ５２に送信される。また、かかる出金コマンドを受信したＡＴＭ５２側では、ステップＳ２９及びステップＳ３０の処理が省略される。これ以外の処理の流れは、第１の実施の形態と同様である。

[0066] 次に、図６を参照して、ＡＴＭ５２の精査を行うタイミングで実行される不正コマンドの有無を検証する不正コマンド検証処理の内容について説明する。まず、ＡＴＭ５２の精査を行う係員は、操作部１１を所定操作することにより、紙幣入出金機構部５４の記憶部１８が保持する取引情報テーブル１９に登録されている取引情報を監視サーバ５５に送信するようそのＡＴＭ５２に指示を与える。

[0067] そして、この操作入力が与えられたＡＴＭ（精査対象のＡＴＭ）５２のＡＴＭ制御部５３は、紙幣入出金機構部５４に対して、記憶部１８（図１）に保持している取引情報テーブル１９（図１）に登録されている取引情報を監視サーバ５５に送信するよう指示を与える（Ｓ４０）。かくして、この指示を受領した紙幣入出金機構部５４は、かかる取引情報テーブル１９に登録されている取引情報のうち、最新の取引情報から過去に遡って最初の初期設定

情報が現れる期間（以下、これを検証対象期間と呼ぶ）までの取引情報を読み出し、これをＡＴＭ制御部５３を介して監視サーバ５５に送信する（Ｓ４１）。

[0068] この取引情報を受信した監視サーバ５５は、自己が管理する取引情報テーブル３４（図１）に登録されている取引情報の中から、その精査が行われている対象とするＡＴＭ（以下、これを対象ＡＴＭと呼ぶ）５２に関する取引情報であって、必要な取引情報を取得する（Ｓ４２）。

[0069] 具体的に、監視サーバ５５は、かかる取引情報テーブル３４に登録されている取引情報のうち、そのとき対象ＡＴＭ５２に関する取引情報をだけを選択し、さらに選択した取引情報のうち、そのとき対象ＡＴＭ５２から送信されてきた取引情報の検証対象期間内に実行された各取引に関する取引情報のみを選択する。

[0070] 続いて、監視サーバ５５は、ステップＳ４２で取得した各取引情報にそれぞれ含まれるハッシュ値を、ステップＳ４１で対象ＡＴＭ５２から送信されてきた取引情報のうちの対応する取引情報に含まれるハッシュ値と一致するか否かをそれぞれ順番に判定する（Ｓ４３）。

[0071] そして監視サーバ５５は、かかる判定の判定結果を表示すると共に当該判定結果を所定のファイルに記録する（Ｓ４４）。具体的に、監視サーバ５５は、かかる判定の結果、対象ＡＴＭ５２から送信されてきた各取引情報の内容がいずれも記憶部に蓄積されている対応する取引情報と一致した場合には、その検証対象期間内に不正コマンドが実行されていないと判断して、その検証対象期間内に不正がなかったことを表示及び所定ファイル等に記録する。

[0072] また監視サーバ５５は、かかる判定の結果、対象ＡＴＭ５２から送信されてきたいずれかの取引情報に含まれるハッシュ値が取引情報テーブル３４に登録されている対応する取引情報に含まれるハッシュ値と一致しなかった場合には、その検証対象期間内に不正コマンドが実行されたと判断して、警告を表示するなどして外部に異常を通知すると共にその旨を所定ファイル等に

記録する。

[0073] そして監視サーバ５５は、この後、初期設定を実行すべき旨の通知を勘定系ホストコンピュータ５１に送信する（Ｓ４５）。かくして、この通知に従って、図３のステップＳ６～ステップＳ１０と同様にして、勘定系ホストコンピュータ５１から監視サーバ５５及び対象ＡＴＭ５２に初期設定情報が送信され、当該初期設定情報が監視サーバ５５が保持する取引情報テーブル３４と、対象ＡＴＭ５２の紙幣入出金機構部５４が保持する取引情報テーブル１９とにそれぞれ登録される（Ｓ４６～Ｓ５０）。

[0074] 以上のように本実施の形態の自動取引システム５０では、通常の出金取引時には勘定系ホストコンピュータ５１からＡＴＭ５２に対して１つ前の取引の取引情報を送信せず、ＡＴＭ５２の精査を行うタイミングでそのＡＴＭ５２の紙幣入出金機構部５４が保持する一定の検証対象期間（そのＡＴＭ５２の金庫１５の金庫扉１６が開けられてから再び金庫扉１６が開けられるまでの期間）内の取引情報に含まれるハッシュ値と、監視サーバ５５が保持するその検証対象期間内のそのＡＴＭ５２で実行された取引の取引情報に含まれるハッシュ値とを比較して検証する。

[0075] 従って、本自動取引システム５０によれば、出金取引時における通信プロトコルの変更量を最小限としながら、かかる一定の検査対象期間内における不正コマンドによって現金の抜き取り行為が行われていないかを検証することができ、かくして信頼性の高い自動取引システムを実現することができる。

[0076] （３）第３の実施の形態

第１又は第２の実施の形態のＡＴＭ２，５２の紙幣入出金機構部１４，５４の記憶部１８に偶発故障が発生し、当該記憶部１８に格納されている取引情報を読み出すことができなくなった場合には、第１の実施の形態や第２の実施の形態について上述した方法によりマルウェア３５による不正な取引を検出することができなくなる。

[0077] また、かかる記憶部１８を新たなものに交換した場合には、交換後の記憶

部１８に過去の取引情報が記録されていないため、第１の実施の形態について上述した方法の取引や、第２の実施の形態について上述した方法の検証を行い得るようにするためには、図３について上述した初期設定処理を実行して取引の準備を完了させる必要がある。

[0078] これは、例えば第１の実施の形態について上述した方法の取引を再開するためには１つ前の取引の取引情報としてダミーの取引情報である初期設定情報を監視サーバ４の記憶装置３１及びＡＴＭ２の紙幣入出金機構部１４の記憶部１８にそれぞれ登録させる必要があり、また第２の実施に形態について上述した方法の検証を行うためには、最新の取引情報から過去に遡って最初の初期設定情報が現れるまでの検証期間内の取引情報がすべてＡＴＭ５２の紙幣入出金機構部５４の記憶部１８に蓄積されている必要があるからである。例えば、図２の場合、取引番号が「78901」の取引は初期設定であるため、新しく交換された記憶部１８によって比較検証すべき取引履歴は取引番号が「34501」～「34505」の取引は除外して新たに「78901」からの取引情報が対象になる。

[0079] このため、これらの事象を逆手にＡＴＭ２，５２の紙幣入出金機構部１４，５４の記憶部１８の交換や初期設定の実行が不正に行われると適切な過去の検証ができなくなってしまう。従って、かかる記憶部１８の交換や初期設定処理を実行する際に適切な権限を持つ係員が介在することを確認する手段が必要になる。そこでＡＴＭ２，５２として守るべき現金を保管しておく金庫１５の金庫扉１６を開けることができる係員が適切な権限を持つとして、初期設定処理時に金庫１５の金庫扉１６が開いてることを確認する手段を設ける。

[0080] 図７を参照しながら、ＡＴＭ２，５２の紙幣入出金機構部１４，５４の記憶部１８を交換する交換作業処理の手順について説明する。まず、ＡＴＭ２，５２の紙幣入出金機構部１４，５４の記憶部１８を交換するためにＡＴＭ２，５２の金庫１５（図１）の金庫扉１６を開ける（Ｓ６０）。次に、かかる記憶部１８を交換する（Ｓ６１）。

[0081] 新しく取り付けた記憶部１８には取引情報は蓄積されていないため、そのＡＴＭ２，５２の操作部１１（図１）を所定操作することにより、図３について上述した初期設定処理を実施させる（Ｓ６２）。なお、図３について上述したように初期設定処理では金庫１５の金庫扉１６が開いていることが必要となる。つまり金庫１５の金庫扉１６を開けることができる係員がかかる記憶部１８の交換と初期設定に立ち会っている状態であることが要求される。そして、この初期設定処理が完了した後に、金庫１５の金庫扉１６を閉める（Ｓ６３）。

[0082] 以上により、ＡＴＭ２，５２の紙幣入出金機構部１４，５４の記憶部１８の交換や初期設定を不正に実施されることなく、検証すべき取引情報の範囲（検証対象期間）を正しく設定することができる。

[0083] （４）第４の実施の形態

上述のように、第１の実施の形態の自動取引システム１では、勘定系ホストコンピュータ３が出金コマンドをＡＴＭ２に送信する際、常にそのＡＴＭ２で実行された１つ前の取引の取引情報を併せて送信するため、勘定系ホストコンピュータ３及び各ＡＴＭ２間で行われる通信の既存の通信プロトコルに対する変更量が大きい。

[0084] そこで、本実施の形態においては、図１との対応部分に同一符号を付した図８に示すように、ＡＴＭ６２のカード機構部６４に記憶部６５を設け、ＡＴＭ６２で実行された取引の取引情報をこの記憶部６５に蓄積し、当該記憶部６５に蓄積された取引情報と、紙幣入出金機構部６７の記憶部１８に蓄積された取引情報とを比較検証することにより、勘定系ホストコンピュータ６１との通信プロトコルへの影響なく取引情報の検証を行い得るようにする。

[0085] 実際上、本実施の形態による自動取引システム６０は、監視サーバ４（図１）が省略されている点と、ＡＴＭ６２のカード機構部６４内に記憶部６５が設けられ、この記憶部６５に取引情報テーブル６６が格納されている点と、カード機構部６４が取り扱うカード媒体としてＩＣ（Integrated Circuit）カードが適用される点とが第１の実施の形態の自動取引システム１と大き

く相違する。

[0086] 図９は、本実施の形態の自動取引システム６０において、利用者によりＡＴＭ６２に対して出金取引の操作が行われた場合に実行される出金取引処理の流れを示す。なお、以下の説明で登場する電子署名の取り扱いは、ＥＭＶ仕様に準拠したものとして、一般のＡＴＭ取引で扱われるものと同じであるため、以下においては、その詳細説明は省略する。

[0087] 図９において、ステップＳ７０～ステップＳ７２までの流れは、図４のステップＳ２０～ステップＳ２２と同様であるため、ここでの説明は省略する。ただし、本実施の形態においては、利用者がＡＴＭ６２に装填するカード媒体はＩＣカードである。

[0088] この後、勘定系ホストコンピュータ６１は、出金コマンドと、出金コマンドが正当なコマンドあるかを検証するための電子署名とを、そのとき対象としているＡＴＭ６２（ステップＳ７１で電文を送信してきたＡＴＭ６２）に送信する（Ｓ７３）。

[0089] この出金コマンド及び電子署名を受信したＡＴＭ６２のＡＴＭ制御部６３は、出金コマンドを紙幣入出金機構部６７に転送する（Ｓ７４）。かくして、紙幣入出金機構部６７は、この出金コマンドに含まれる今回の出金取引の取引情報を当該出金コマンドから抽出し、抽出した取引情報を記憶部１８に格納されている取引情報テーブル６８に登録する（Ｓ７６）。

[0090] またＡＴＭ制御部６３は、受信した出金コマンド及び電子署名をカード機構部６４に送信する（Ｓ７５）。そしてカード機構部６４は、このとき受信した電子署名をＩＣカードを使って検証し（Ｓ７７）、検証結果を出金コマンドに含まれる今回の出金取引の取引情報に追加して記憶部６５に格納されている取引情報テーブル６６に登録する。また、カード機構部６４は、この際、出金コマンドに含まれる店舗番号及び装置ＩＤ等の情報に基づいてその取引情報に対するハッシュ値を算出し、算出したハッシュ値も併せて取引情報テーブル６６に登録する（Ｓ７８）。なおハッシュ値の計算に際しては、電子署名や電子署名の検証結果を含ませるようにしても良い。

[0091] この後、カード機構部６４は、かかる取引情報テーブル６６に登録されているそのＡＴＭ６２が実行した１つ前の取引の取引情報と、ステップＳ７７において実行した検証処理の検証結果とをＡＴＭ制御部６３に送信する（Ｓ７９）。

[0092] ＡＴＭ制御部６３は、カード機構部６４から送信されてきた電子署名の検証結果に基づいて、かかる電子署名が正しくないとの検証結果であった場合には、今回の取引を中止して外部に異常を通知する。

[0093] これに対して、ＡＴＭ制御部６３は、かかる電子署名が正しい場合には、ステップＳ７３で勘定系ホストコンピュータ６１から送信されてきた出金コマンドと、ステップＳ７９でカード機構部６４から送信されてきた１つ前の取引の取引情報（電子署名の検証結果を含む）とを紙幣入出金機構部６７に送信する（Ｓ８０）。

[0094] そして紙幣入出金機構部６７は、ＡＴＭ制御部６３から送信されてきた出金コマンドに含まれる今回の取引の取引情報に基づいて、カード機構部６４と同じハッシュ関数を用いてカード機構部６４と同様にして今回の取引に対するハッシュ値を算出し、算出したハッシュ値と、電子署名の検証結果とを追加した新たな取引情報を記憶部１８に格納されている取引情報テーブル６８に登録する（Ｓ８１）。

[0095] また紙幣入出金機構部６７は、記憶部１８内の取引情報テーブル６６に登録されている１つ前の取引の取引情報に含まれるハッシュ値と、ステップＳ８０でＡＴＭ制御部６３から送信されてきた１つ前の取引の取引情報に含まれるハッシュ値とを比較してこれらが一致するか検証し（Ｓ８２）、検証結果をＡＴＭ制御部６３に通知する（Ｓ８３）。また紙幣入出金機構部６７は、かかる２つのハッシュ値が一致した場合にのみ、出金コマンドにおいて指定された各金種の紙幣を当該出金コマンドで指定された枚数だけそれぞれ紙幣取出し口（図示せず）に排出する出金準備を行う（Ｓ８５）。

[0096] 一方、ＡＴＭ制御部６３は、紙幣入出金機構部６７からの比較結果が、かかる２つのハッシュ値が一致しないというものであった場合には、今回の取

引を中止して外部に異常を通知する。

[0097] これに対して、ＡＴＭ制御部６３は、紙幣入出金機構部６７からの比較結果が、かかる２つのハッシュ値が一致するというものであった場合には、カード機構部６４を制御することにより、そのとき装填された利用者のカード媒体を利用者に返却させると共に、明細票機構部１２（図８）を制御することにより、明細票に今回の取引内容を印字させる（Ｓ８４）。

[0098] さらにＡＴＭ制御部６３は、紙幣取出し口（図示せず）を閉塞しているシャッターを開くよう紙幣入出金機構部６７に指示を与える（Ｓ８６）。かくして、紙幣入出金機構部６７は、この指示に従ってシャッターを開くことにより紙幣を放出し（Ｓ８７）、この後、利用者により紙幣が取り出されるとかかるシャッターを閉じる。以上により、一連の出金処理が終了する。

[0099] 図１０は、カード機構部６４の記憶部６５と、紙幣入出金機構部６７の記憶部１８とにそれぞれ保持される本実施の形態による取引情報テーブル６６，６８の構成を示す。この取引情報テーブル６６，６８は、店舗番号欄７０、装置ＩＤ（Identification）欄７１、取引番号欄７２、取引日時欄７３、取引種別欄７４、ハッシュ値欄７５、署名検証結果欄７６及び金額欄７７を備えて構成される。

[0100] この場合、店舗番号欄７０、装置ＩＤ（Identification）欄７１、取引番号欄７２、取引日時欄７３、取引種別欄７４、ハッシュ値欄７５及び金額欄７７にそれぞれ格納される情報は、図２について上述した第１の実施の形態の取引情報テーブル１９，３４の対応する欄に格納される情報と同様であるため、ここでの説明は省略する。また署名検証結果欄７６には、対応する取引においてカード機構部６４において実行された電子署名の検証（ステップＳ７７）の検証結果が格納される。

[0101] 以上のように電子署名を検証するカード機構部６４の記憶部６５に取引情報を記録することで、改ざんされることなく正しい取引情報を記録することが可能であり、その取引情報と紙幣入出金機構部６７への取引情報とを比較検証することで、勘定系ホストコンピュータ６１が介在しなくてもＡＴＭ６

２内部で十分に信頼性のある検証が可能になる。なお、より安全性を高めるために取引情報に電子署名の確認結果だけでなく電子署名を記録・検証しても良い。

[0102] （５）他の実施の形態

なお上述の第１～第４の実施の形態においては、取引が出金取引の場合についてのみ説明したが、本発明はこれに限らず、入金取引や振込み取引などについても同様に不正を検出することが可能であり特に区別するものではない。この場合、取引情報テーブル１９，２４，６６には出金取引、入金取引及び振込取引などのすべての取引が登録されるため、「１つ前の取引」は、勘定系ホストコンピュータ３，５１又は監視サーバ４，５５に接続された複数のＡＴＭ２のうち、特定の１つのＡＴＭ２で実行されたすべての取引のうちの１つ前に実行された取引を指すものとなる。

[0103] また上述の第１～第４の実施の形態においては、監視サーバ４，５５の記憶部３１やカード機構部６４の記憶部６５に記憶保持されている過去の取引の取引情報と、紙幣入出金取引部１４，５４，６７の記憶部１８に記憶保持されている過去の取引情報とを比較する際の対象として、１つ前の取引の取引情報を適用するようにした場合について述べたが、本発明はこれに限らず、２つ前以上の取引の取引情報を適用するようにしても良い。また、比較する際の対象として、１つの過去の取引情報だけではなく、複数の過去の取引情報を適用してもよい。

[0104] さらに上述の第１～第３の実施の形態においては、各取引情報のハッシュ値を監視サーバ４，５５と、ＡＴＭ２，５２の紙幣入出金機構部１４，５４とで共通のハッシュ関数を用いてそれぞれ算出し、これらのハッシュ値を比較することで取引情報の内容が同じであるか否かを判定するようにした場合について述べたが、本発明はこれに限らず、例えば、勘定系ホストコンピュータ３，５１においてハッシュ値を算出するようにしても良く、また取引情報の内容が同じであるか否かの判定を、ハッシュ値ではなく取引情報全体を比較して内容が同じであるか否かを判定するようにしても良い。また、ハッ

シュ値の生成に関しては、紙幣入出金機構部１４や監視サーバ４、又は勘定系ホストコンピュータ３，５１が、取引の店舗番号、装置ＩＤ、取引番号、取引日時、取引種別及び金額の一部の情報を用いてハッシュ値を生成するものであってよい。

産業上の利用可能性

[0105] 本発明は、紙幣を取り扱う種々の構成の自動取引システムに広く適用することができる。

符号の説明

[0106] １，５０，６０……自動取引システム、２，５２，６２……ＡＴＭ、３，５１，６１……勘定系ホストコンピュータ、４，５５……監視サーバ、１０，５３，６３……ＡＴＭ制御部、１３，６４……カード機構部、１４，５４，６７……紙幣入出金機構部、１５……金庫、１６……金庫扉、１７……センサ、１８，６５……記憶部、１９，３４，６６，６８……取引情報テーブル、３１……記憶装置。

請求の範囲

[請求項1] 紙幣を用いた取引を行う自動取引システムであって、

第１の取引で扱われる金額に関する情報である第１の金額情報を含む第１の取引情報を送信するＡＴＭ制御部と、

前記第１の取引情報を受信し、前記第１の取引情報に含まれる前記第１の金額情報に基づき紙幣の搬送を行う紙幣取扱装置と、

前記紙幣取扱装置に設けられ、前記紙幣取扱装置の受信した前記第１の取引情報を記憶する第１の記憶部と、

前記紙幣取扱装置の外部の装置に設けられ、前記外部の装置が受信した前記第１の取引情報を記憶する第２の記憶部と

を備え、

前記第１の取引後の取引である第２の取引において、

前記ＡＴＭ制御部は、前記第２の取引で扱われる金額に関する情報である第２の金額情報を含む第２の取引情報を送信し、

前記外部の装置は、前記第２の記憶部に記憶される前記第１の取引情報を送信し、

前記紙幣取扱装置は、

前記第２の取引情報と、前記外部の装置の送信した前記第１の取引情報とを受信し、

前記第１の記憶部に記憶される前記第１の取引情報と、前記外部の装置の送信した前記第１の取引情報とが一致するか否かを判断し、一致した場合に、前記第２の取引情報に含まれる前記第２の金額情報に基づき、紙幣の搬送を行うことを特徴とする自動取引システム。

[請求項2] 請求項１に記載の自動取引システムであって、

前記紙幣取扱装置及び前記外部の装置は、それぞれ前記第１の取引情報に含まれる共通の情報に基づき、共通のハッシュ関数を用いてハッシュ値を計算し、

前記外部の装置により計算されたハッシュ値は、前記第２の取引に

おいて、前記外部の装置の送信した前記第１の取引情報に含まれ、

前記紙幣取扱装置により計算されたハッシュ値は、前記第１の記憶部に記憶された対応する前記第１の取引情報に含まれることを特徴とする自動取引システム。

[請求項3] 請求項１又は２に記載の自動取引システムであって、

前記第１の取引情報及び前記第２の取引情報を含む取引情報は、取引毎に付与される取引番号、取引の日時である取引日時、取引の種別である取引種別、及び取引で扱われる紙幣金種毎の紙幣の枚数の少なくとも１つを含むことを特徴とする自動取引システム。

[請求項4] 請求項１乃至３のいずれか一項に記載の自動取引システムであって、

前記第２の取引において、前記第１の記憶部に記憶される前記第１の取引情報と、前記外部の装置の送信した前記第１の取引情報とが一致しなかった場合に、不一致であったことを利用者又は係員に通知する通知手段を備えることを特徴とする自動取引システム。

[請求項5] 請求項１乃至４のいずれか一項に記載の自動取引システムであって、

前記ＡＴＭ制御部及び前記紙幣取扱装置は、利用者の操作入力に応じて入出金取引を行う自動取引装置内に設けられ、

前記自動取引装置の上位の装置であるホストコンピュータを備え、

前記ホストコンピュータは、前記ＡＴＭ制御部からの前記第１又は第２の取引の処理要求に応じてトランザクション番号を含む前記第１又は第２の取引情報を生成して前記外部の装置及び前記ＡＴＭ制御部に送信することを特徴とする自動取引システム。

[請求項6] 請求項１乃至４の何れか一項に記載の自動取引システムであって、

前記ＡＴＭ制御部及び前記紙幣取扱装置は、利用者の操作入力に応じて入出金取引を行う自動取引装置内に設けられ、

前記自動取引装置の上位の装置であるホストコンピュータを備え、

前記ホストコンピュータは、前記ＡＴＭ制御部からの前記第１又は第２の取引の処理要求に応じて前記第１又は第２の取引情報を生成して前記外部の装置及び前記ＡＴＭ制御部に送信し、

前記外部の装置は、前記自動取引装置とは別個に設けられた監視サーバであることを特徴とする自動取引システム。

[請求項7] 請求項１乃至４のいずれか一項に記載の自動取引システムであって、

前記外部の装置は、ＩＣカードを用いて、前記ＡＴＭ制御部の上位の装置から送信された前記第１の取引に関する第１の電子署名を検証するカード機構部であって、

前記第１の取引において、

前記カード機構部は、前記第１の電子署名の検証結果が正しい場合に、前記カード機構部が受信した前記第１の取引情報を前記第２の記憶部に記憶し、

前記紙幣取扱装置は、前記カード機構部による前記第１の電子署名の検証結果を受信し、前記１の電子署名の検証結果が正しい場合に前記紙幣取扱装置が受信した前記第１の取引情報を前記第１の記憶部に記憶することを特徴とする自動取引システム。

[請求項8] 請求項７に記載の自動取引システムであって、

前記カード機構部は、ＩＣカードを用いて、前記ＡＴＭ制御部の上位の装置から送信された前記第２の取引に関する第２の電子署名を検証し、

前記紙幣取扱装置は、前記第２の取引において、前記カード機構部により前記第２の電子署名の検証結果が正しいと判断されていた場合に、前記カード機構部の送信した前記第１の取引情報を受信し、前記第１の記憶部に記憶された前記第１の取引情報と、前記カード機構部の送信した前記第１の取引情報とが一致するか否かを判断することを特徴とする自動取引システム。

[請求項9] 請求項１に記載の自動取引システムであって、

前記紙幣取扱装置は、紙幣を保管する金庫と、前記金庫の扉の開閉状態を検知する検知部を備え、

前記ＡＴＭ制御部は、前記金庫の扉が開である場合に、上位の装置であるホストコンピュータに初期設定の実行を通知し、

前記ホストコンピュータは、当該通知に応じてダミーの取引情報である第３の取引情報を生成して前記外部の装置及び前記ＡＴＭ制御部に送信し、

前記外部の装置は、受信した前記第３の取引情報を前記第２の記憶部に記憶し、

前記ＡＴＭ制御部は、受信した前記第３の取引情報を前記紙幣取扱装置に送信し、

前記紙幣取扱装置は、前記第１の記憶部が新しい記憶部である第３の記憶部に交換されていた場合に、受信した前記第３の取引情報を前記第３の記憶部に記憶することを特徴とする自動取引システム。

[請求項10] 請求項１に記載の自動取引システムであって、

前記紙幣取扱装置は、紙幣を保管する金庫と、前記金庫の扉の開閉状態を検知する検知部とを備え、

前記ＡＴＭ制御部は、前記金庫の扉が開である場合に、上位の装置であるホストコンピュータに初期設定の実行を通知し、

前記ホストコンピュータは、当該通知に応じてダミーの取引情報である第３の取引情報を生成して前記外部の装置及び前記ＡＴＭ制御部に送信し、

前記外部の装置は、受信した前記第３の取引情報を前記第２の記憶部に記憶し、

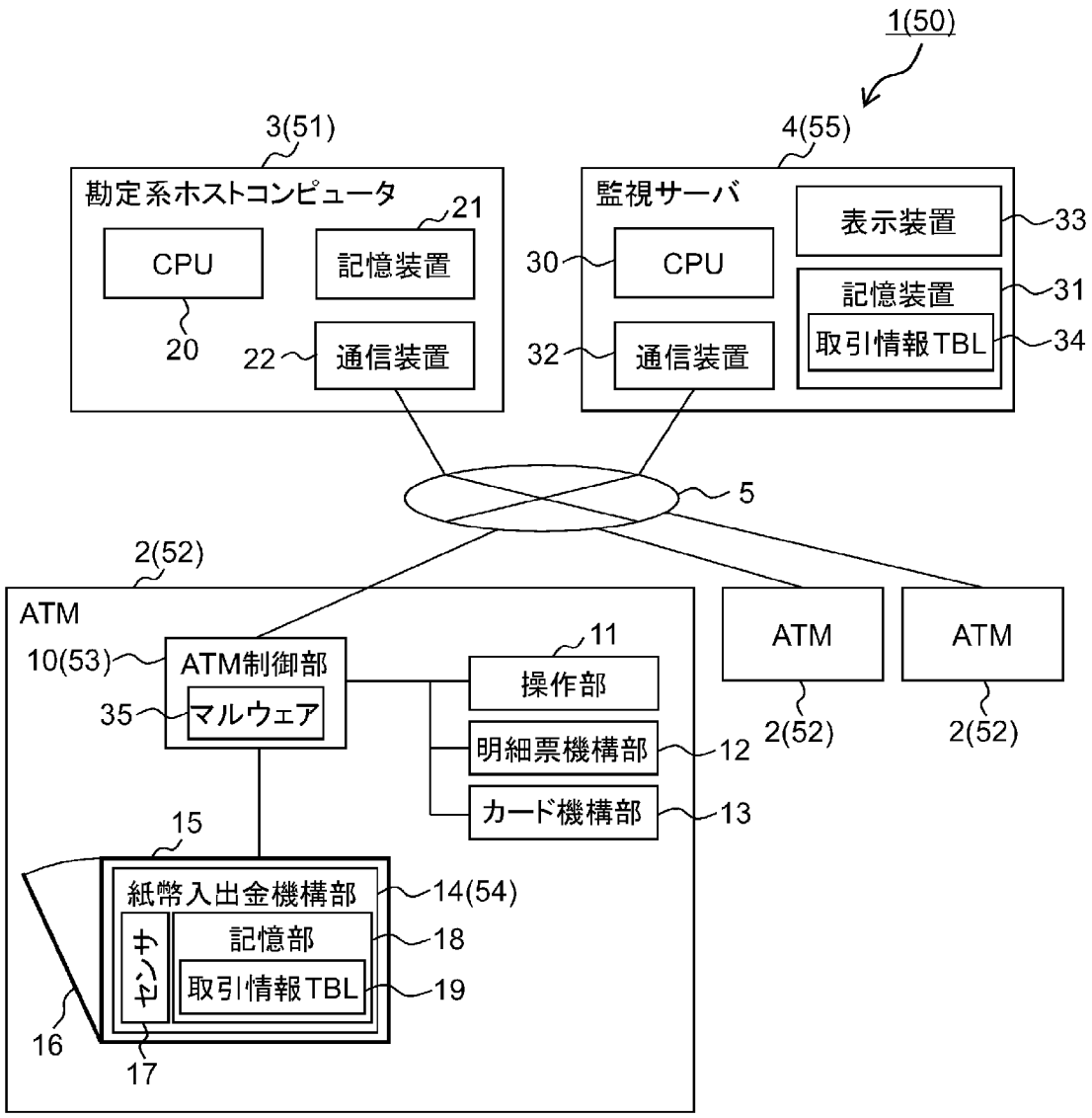
前記紙幣取扱装置は、受信した前記第３の取引情報を前記第１の記憶部に記憶することを特徴とする自動取引システム。

[請求項11] 請求項１０に記載の自動取引システムであって、

前記ＡＴＭ制御部は、前記紙幣取扱装置の前記検知部が前記金庫の扉の開を検知している場合にのみ、前記初期設定の実行を前記ホストコンピュータに通知することを特徴とする自動取引システム。

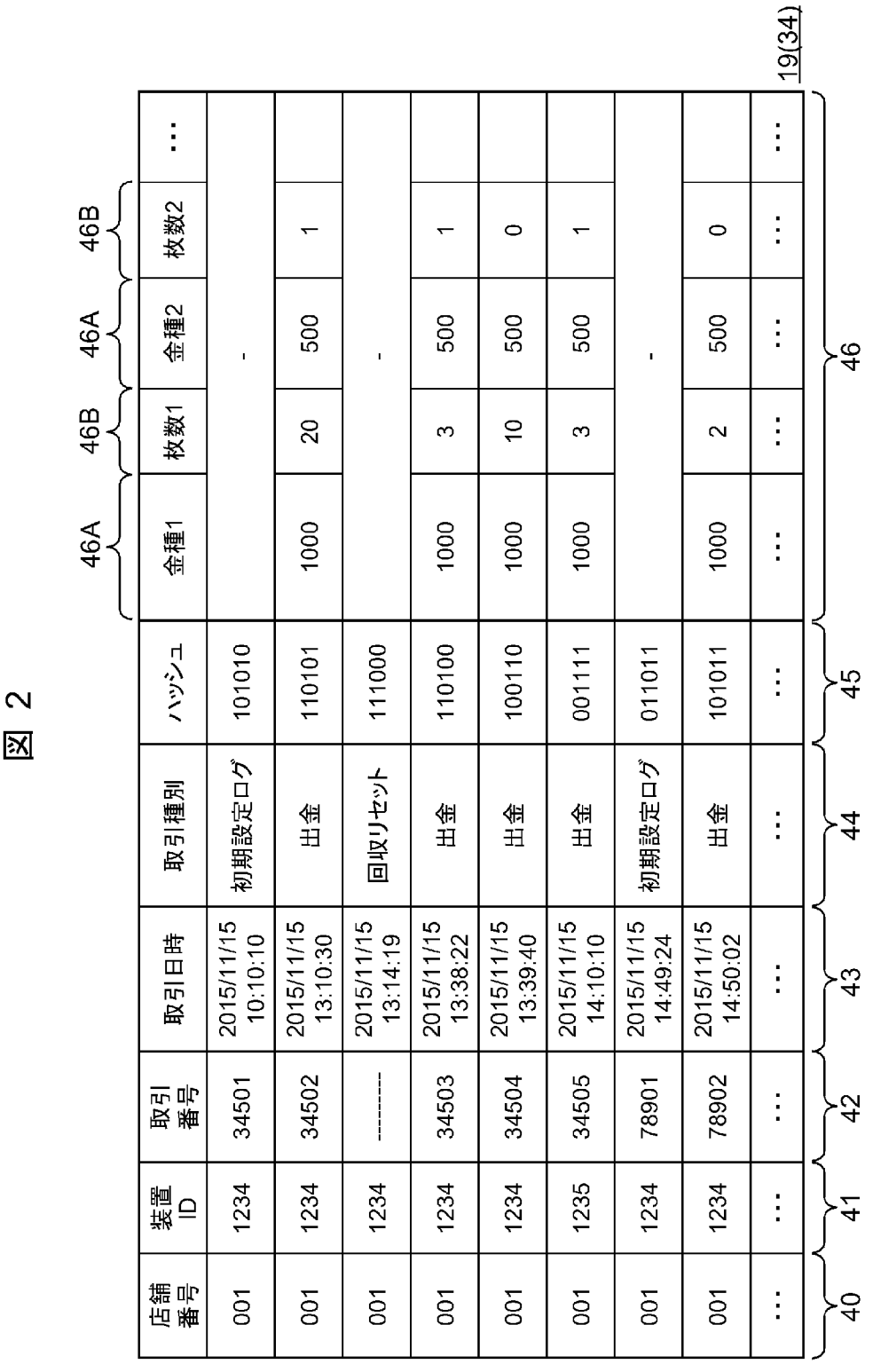
[図1]

図 1


1(50)
3(51)
4(55)
勘定系ホストコンピュータ
CPU
20
記憶装置
21
通信装置
22
監視サーバ
30
CPU
32
通信装置
表示装置
33
記憶装置
31
取引情報TBL
34
5
2(52)
ATM
10(53)
ATM制御部
35
マルウェア
11
操作部
明細票機構部
12
カード機構部
13
15
紙幣入出金機構部
14(54)
記憶部
18
取引情報TBL
19
16
17
ATM
2(52)
ATM
2(52)

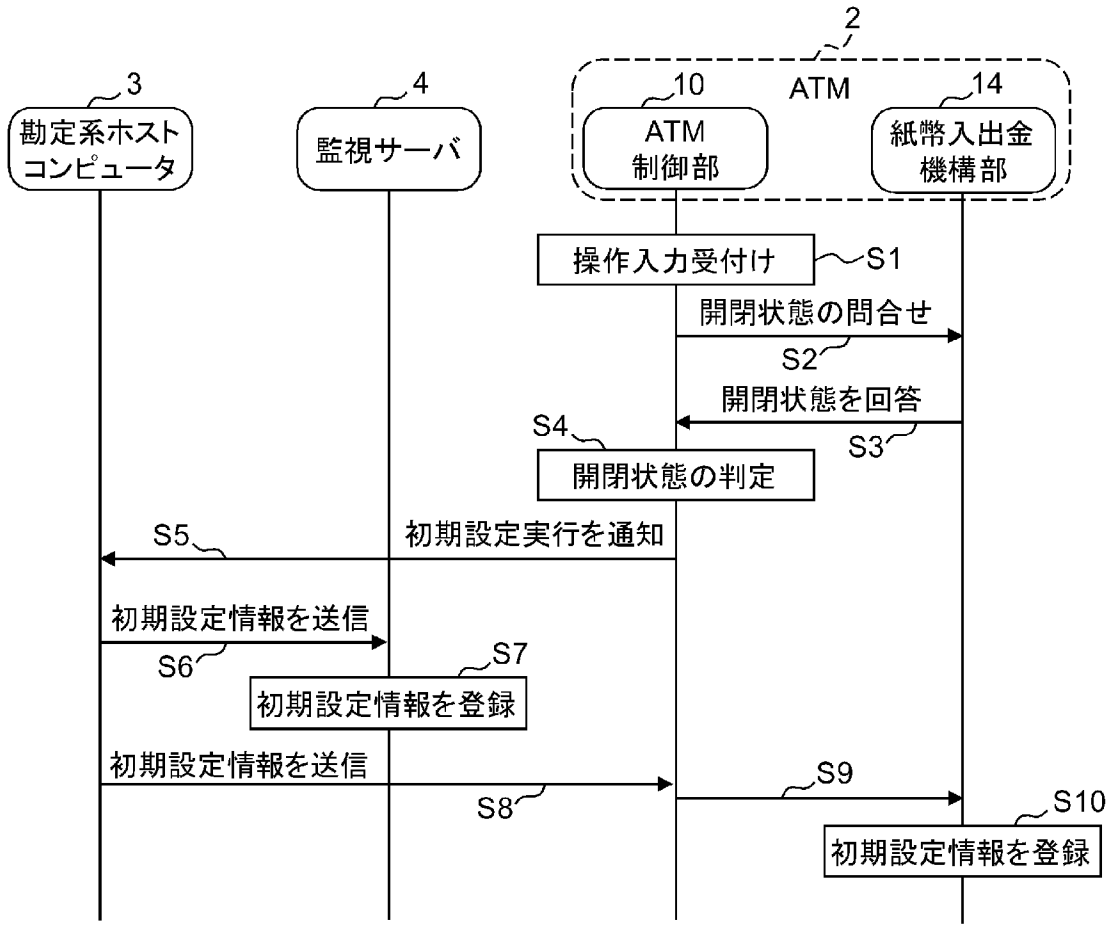
[図2]

図 2


46A
46B
46A
46B
店舗番号
装置ID
取引番号
取引日時
取引種別
ハッシュ
金種1
枚数1
金種2
枚数2
…
001 1234 34501 2015/11/15 10:10:10 初期設定ログ 101010 - …
001 1234 34502 2015/11/15 13:10:30 出金 110101 1000 20 500 1 …
001 1234 -------- 2015/11/15 13:14:19 回収リセット 111000 - …
001 1234 34503 2015/11/15 13:38:22 出金 110100 1000 3 500 1 …
001 1234 34504 2015/11/15 13:39:40 出金 100110 1000 10 500 0 …
001 1235 34505 2015/11/15 14:10:10 出金 001111 1000 3 500 1 …
001 1234 78901 2015/11/15 14:49:24 初期設定ログ 011011 - …
001 1234 78902 2015/11/15 14:50:02 出金 101011 1000 2 500 0 …
… … … … … … … … … … …
40 41 42 43 44 45 46
19(34)

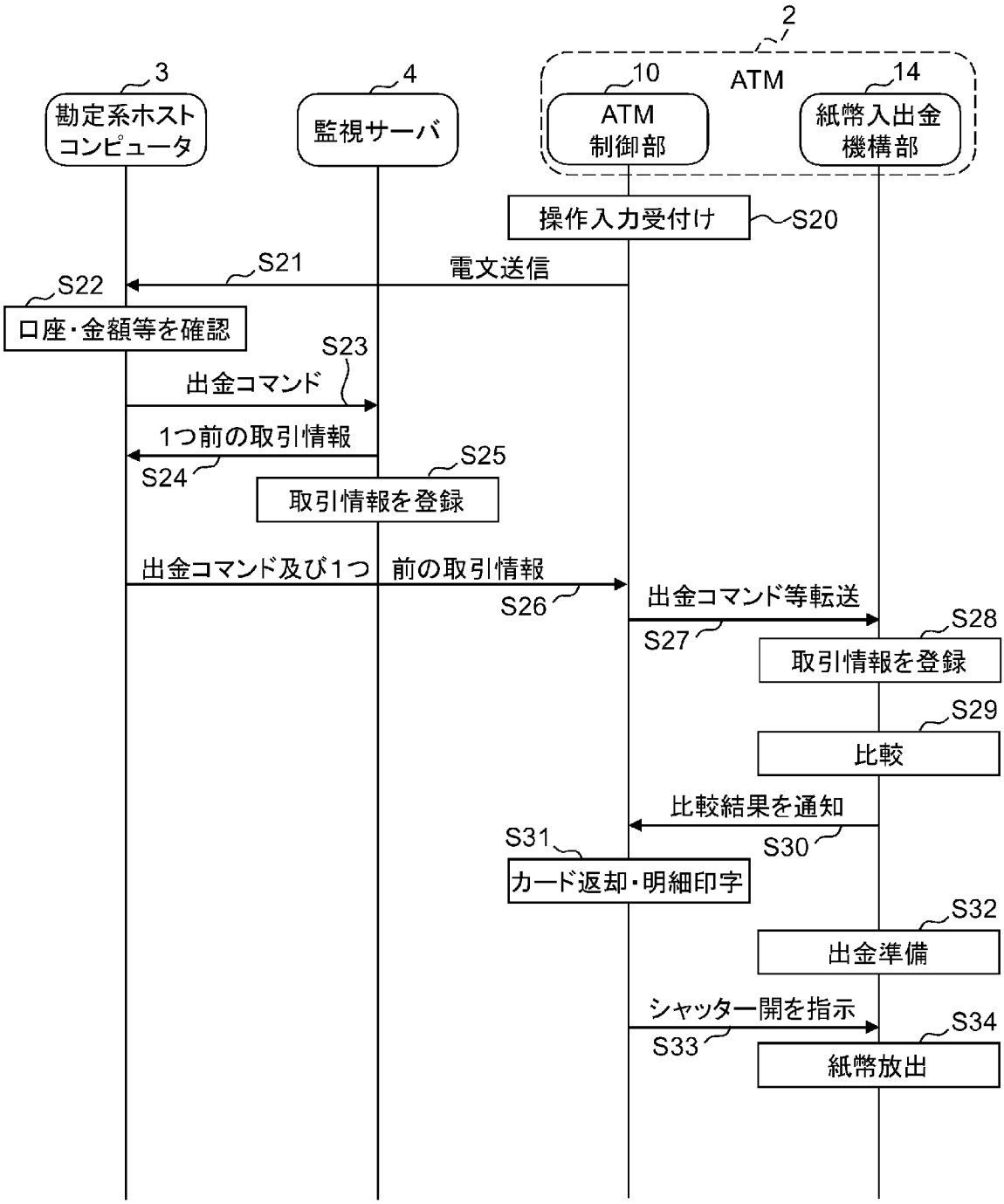
[図3]

図 3


2
3
勘定系ホスト
コンピュータ
4
監視サーバ
10
ATM
制御部
ATM
14
紙幣入出金
機構部
操作入力受付け
S1
開閉状態の問合せ
S2
開閉状態を回答
S3
S4
開閉状態の判定
S5
初期設定実行を通知
初期設定情報を送信
S6
S7
初期設定情報を登録
初期設定情報を送信
S8
S9
S10
初期設定情報を登録

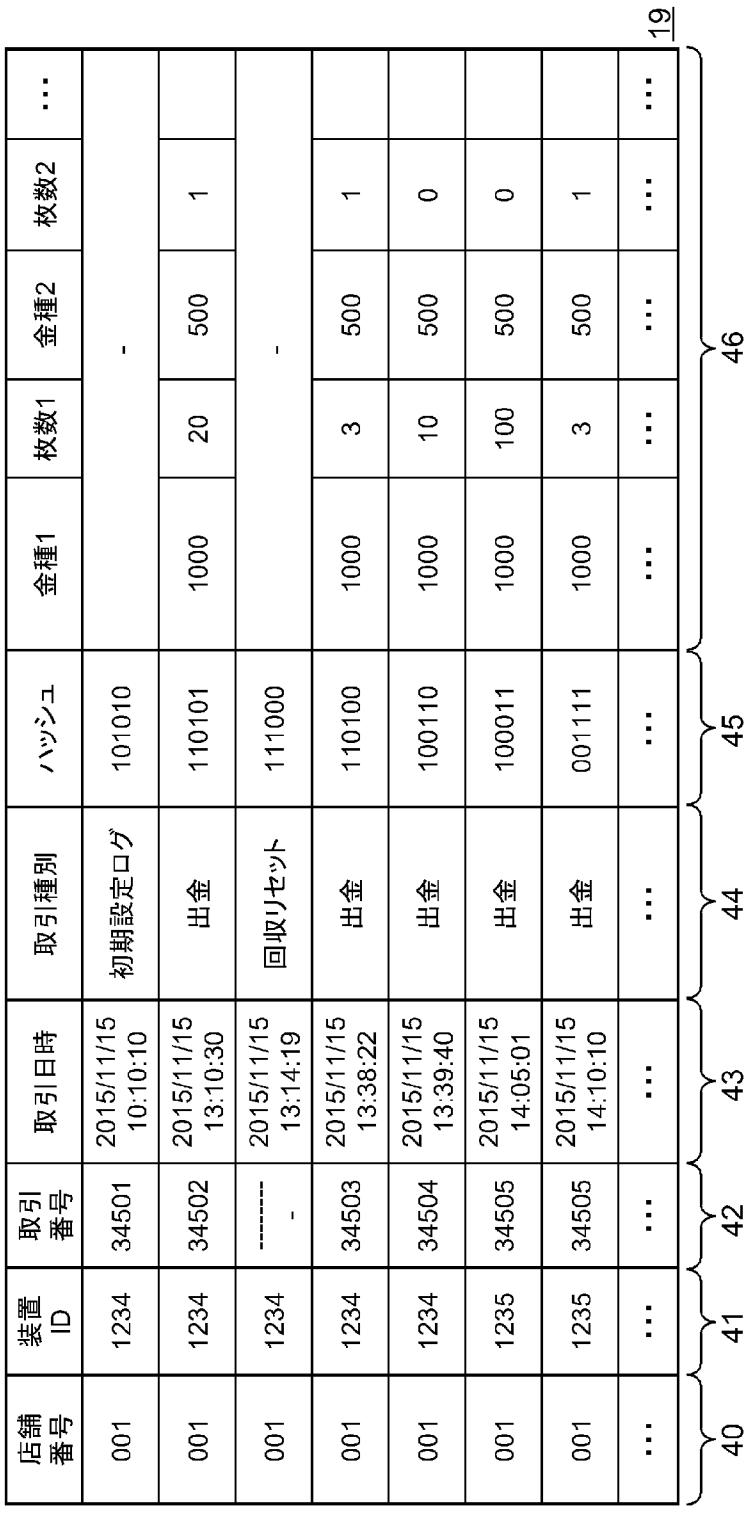
[図4]

図 4


2
ATM
3
勘定系ホスト
コンピュータ
4
監視サーバ
10
ATM
制御部
14
紙幣入出金
機構部
操作入力受付
S20
S21
電文送信
S22
口座・金額等を確認
S23
出金コマンド
1つ前の取引情報
S24
S25
取引情報を登録
出金コマンド及び1つ
前の取引情報
S26
出金コマンド等転送
S27
S28
取引情報を登録
S29
比較
比較結果を通知
S30
S31
カード返却・明細印字
S32
出金準備
シャッター開を指示
S33
S34
紙幣放出

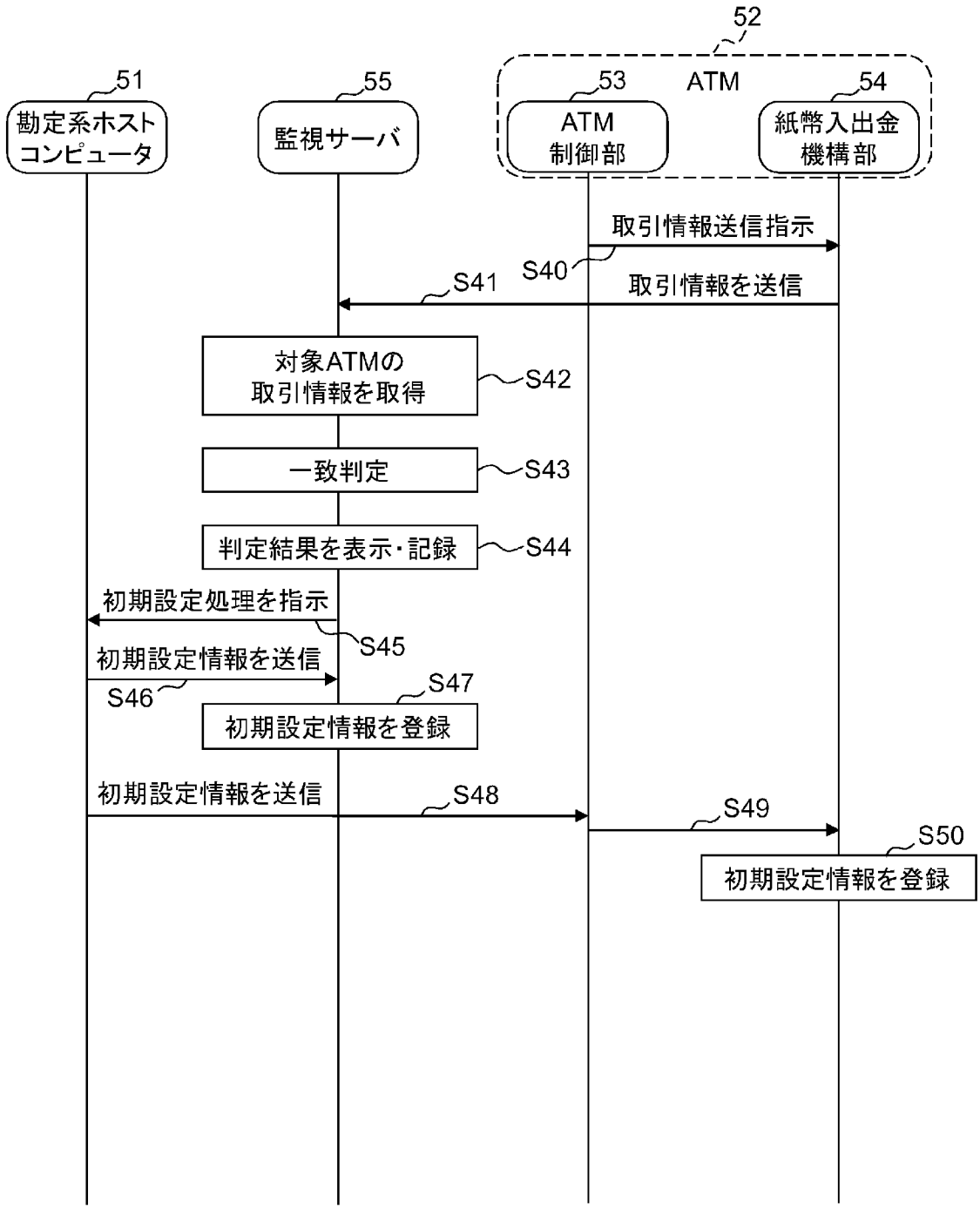
[図5]

図 5


46A
46B
46A
46B
店舗番号
装置ID
取引番号
取引日時
取引種別
ハッシュ
金種1
枚数1
金種2
枚数2
…
001 1234 34501 2015/11/15 10:10:10 初期設定ログ 101010 - …
001 1234 34502 2015/11/15 13:10:30 出金 110101 1000 20 500 1
001 1234 ------ - 2015/11/15 13:14:19 回収リセット 111000 -
001 1234 34503 2015/11/15 13:38:22 出金 110100 1000 3 500 1
001 1234 34504 2015/11/15 13:39:40 出金 100110 1000 10 500 0
001 1234 34505 2015/11/15 14:05:01 出金 100011 1000 100 500 0
001 1235 34505 2015/11/15 14:10:10 出金 001111 1000 3 500 1
… … … … … … … … … …
40
41
42
43
44
45
46
19

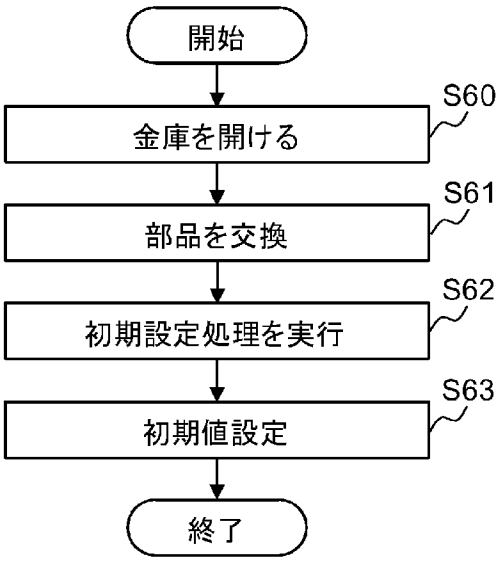
[図6]

図 6


52
ATM
51
勘定系ホスト
コンピュータ
55
監視サーバ
53
ATM
制御部
54
紙幣入出金
機構部
取引情報送信指示
S40
S41
取引情報を送信
対象ATMの
取引情報を取得
S42
一致判定
S43
判定結果を表示・記録
S44
初期設定処理を指示
S45
初期設定情報を送信
S46
S47
初期設定情報を登録
初期設定情報を送信
S48
S49
S50
初期設定情報を登録

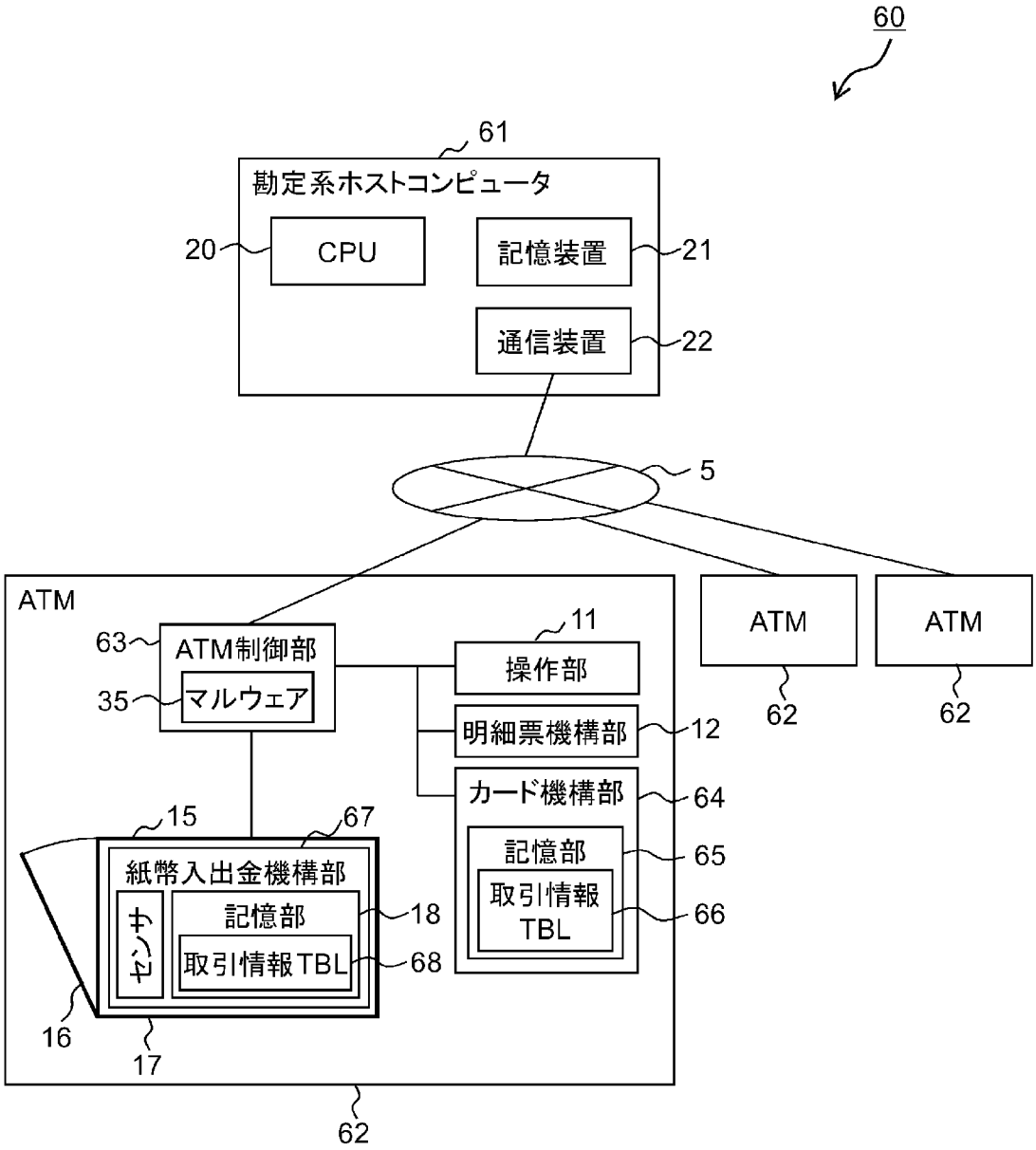
[図7]

図 7



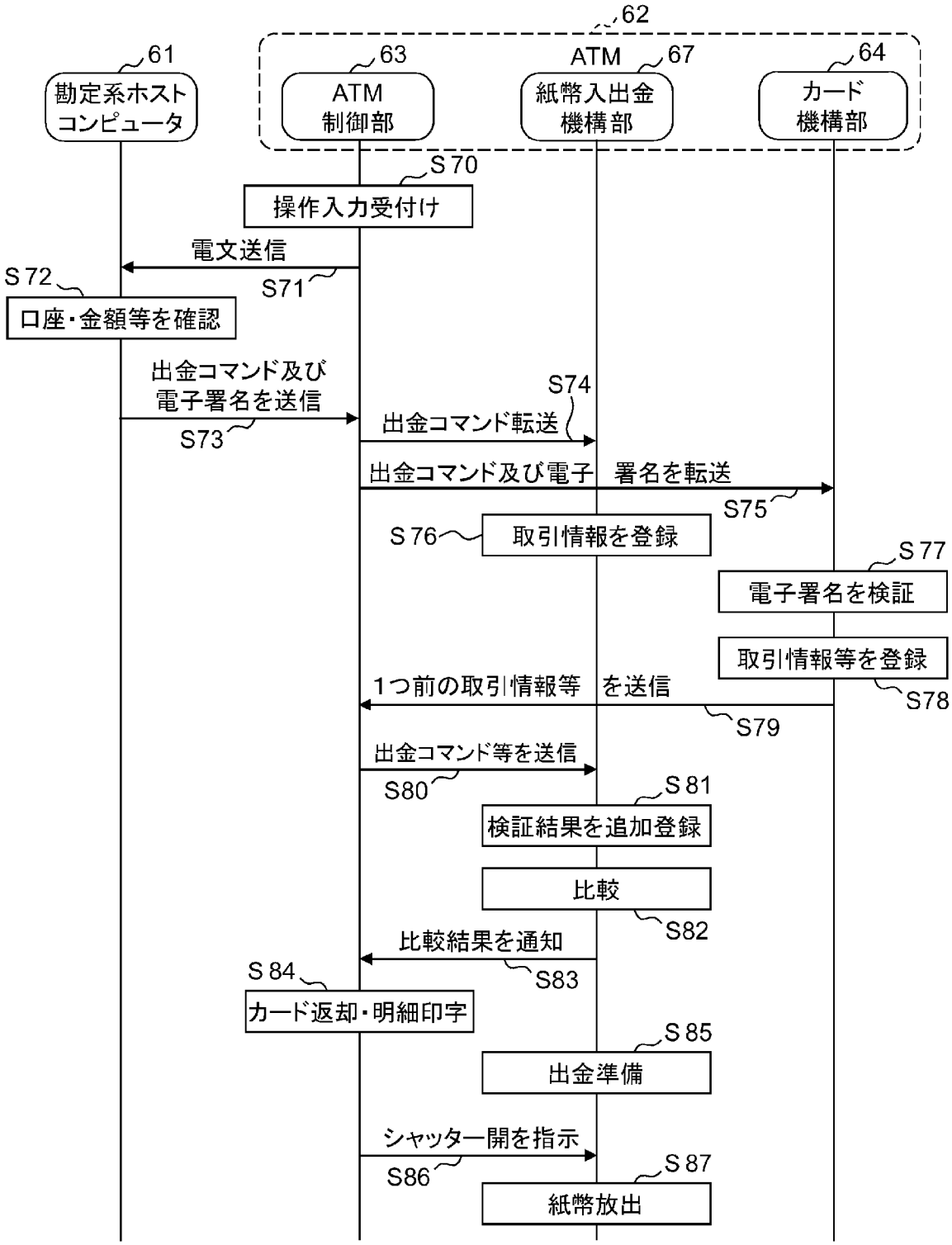
[図8]

図 8


60
61
勘定系ホストコンピュータ
20
CPU
記憶装置
21
通信装置
22
5
ATM
63
ATM制御部
35
マルウェア
11
操作部
明細票機構部
12
カード機構部
64
記憶部
65
取引情報TBL
66
15
67
紙幣入出金機構部
センサ
記憶部
18
取引情報TBL
68
16
17
62
ATM
62
ATM
62

[図9]

図 9


62
61
63
ATM
67
64
勘定系ホスト
コンピュータ
ATM
制御部
紙幣入出金
機構部
カード
機構部
S70
操作入力受付け
電文送信
S71
S72
口座・金額等を確認
出金コマンド及び
電子署名を送信
S73
S74
出金コマンド転送
出金コマンド及び電子
署名を転送
S75
S76
取引情報を登録
S77
電子署名を検証
取引情報等を登録
S78
1つ前の取引情報等
を送信
S79
出金コマンド等を送信
S80
S81
検証結果を追加登録
比較
S82
比較結果を通知
S83
S84
カード返却・明細印字
S85
出金準備
シャッター開を指示
S86
S87
紙幣放出

[図10]

図 10

店舗番号	装置ID	取引番号	取引日時	取引種別	ハッシュ	署名検証結果	金種1	枚数1	金種2	枚数2	…
001	1234	34501	2015/11/15 10:10:10	初期設定ログ	101010		-				
001	1234	34502	2015/11/15 13:10:30	出金	110101	OK	1000	20	500	1	
001	1234	------- -	2015/11/15 13:14:19	回収リセット	111000		-				
001	1234	34503	2015/11/15 13:38:22	出金	110100	OK	1000	3	500	1	
001	1234	34504	2015/11/15 13:39:40	出金	100110	OK	1000	10	500	0	
001	1235	34505	2015/11/15 14:10:10	出金	001111	OK	1000	3	500	1	
001	1234	78901	2015/11/15 14:49:24	初期設定ログ	011011		-				
001	1234	78902	2015/11/15 14:50:02	出金	101011	OK	1000	2	500	0	
…	…	…	…	…	…		…	…	…	…	…

66(68)

70 71 72 73 74 75 76 77

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/086412

A. CLASSIFICATION OF SUBJECT MATTER
G07D9/00(2006.01)i

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)
G07D9/00

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2016
Kokai Jitsuyo Shinan Koho	1971-2016	Toroku Jitsuyo Shinan Koho	1994-2016

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.
A	JP 2015-210613 A (Hitachi-Omron Terminal Solutions, Corp.), 24 November 2015 (24.11.2015), fig. 1 to 21 & WO 2015/163340 A1	1-11
A	JP 2001-126098 A (Fujitsu Ltd.), 11 May 2001 (11.05.2001), fig. 1 to 14 & US 6253997 B1 fig. 1 to 14 & EP 1096450 A2 & ES 2313872 T	1-11

☒ 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
"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	Date of mailing of the international search report
08 February 2016 (08.02.16)	16 February 2016 (16.02.16)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/086412

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-72775 A (Fuji Electric Retail Systems Co., Ltd.), 16 March 2006 (16.03.2006), fig. 1 to 4 (Family: none)	1-11
A	JP 2007-249781 A (Fujitsu Ltd.), 27 September 2007 (27.09.2007), fig. 1 to 12 (Family: none)	1-11

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／０８６４１２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G07D9/00(2006.01)i

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））

Int.Cl.　G07D9/00

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	１９７１－２０１６年
日本国実用新案登録公報	１９９６－２０１６年
日本国登録実用新案公報	１９９４－２０１６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
A	JP 2015-210613 A（日立オムロンターミナルソリューションズ株式会社）2015.11.24, 図１－２１ & WO 2015/163340 A1	1-11
A	JP 2001-126098 A（富士通株式会社）2001.05.11, 図１－１４ & US 6253997 B1 FIG.1-14 & EP 1096450 A2 & ES 2313872 T	1-11
A	JP 2006-72775 A（富士電機リテイルシステムズ株式会社）2006.03.16, 図１－４（ファミリーなし）	1-11

☑　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
「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矛盾するものではなく、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	国際調査報告の発送日
０８．０２．２０１６	１６．０２．２０１６

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　３Ｒ　９４３３
大谷　謙仁
電話番号　０３－３５８１－１１０１　内線　３３７２

C（続き）．　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	JP 2007-249781 A（富士通株式会社）2007.09.27, 図１－１２（ファミリーなし）	1-11