(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
2015 年 10 月 29 日(29.10.2015)

WIPO | PCT

(10) 国際公開番号
WO 2015/163340 A1

(51) 国際特許分類:
G07D 9/00 (2006.01) *G06Q 20/18* (2012.01)

(21) 国際出願番号: PCT/JP2015/062171

(22) 国際出願日: 2015 年 4 月 22 日(22.04.2015)

(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 2014-090861 2014 年 4 月 25 日(25.04.2014) JP

(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, CORPORATION) [JP/JP]; 〒 1418576 東京都品川区大崎一丁目６番３号 Tokyo (JP).

(72) 発明者: 柴田 雄介(SHIBATA Yusuke); 〒 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). 石川 智祥(ISHIKAWA Tomoyoshi); 〒 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). 岡部 公誠(OKABE Kosei); 〒 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). 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: 井上 学, 外(INOUE Manabu et al.); 〒 1008220 東京都千代田区丸の内一丁目６番１号 株式会社日立製作所内 Tokyo (JP).

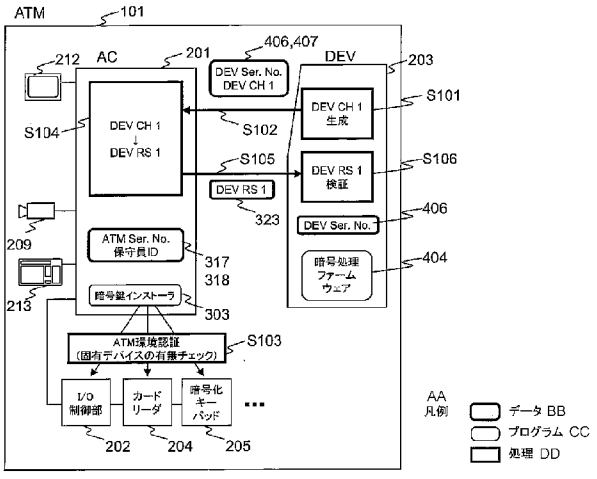
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, 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,

[続葉有]

(54) **Title**: AUTOMATIC TRANSACTION DEVICE AND AUTOMATIC TRANSACTION SYSTEM

(54) 発明の名称 : 自動取引装置及び自動取引システム

図6



202 I/O control unit
204 Card reader
205 Encryption key pad
303 Encryption key installer
317, 318 ATM Ser. No. maintenance person ID
404 Encryption firmware
S101 DEV CH1 generation
S103 ATM environment verification
(check for presence of unique device)
S106 DEV RS 1 verification
AA Legend
BB Data
CC Program
DD Processing

(57) **Abstract**: The present invention ensures safety and validity, during generation of encryption keys required for encrypted communication between an overall control unit for an automatic transaction device and an internal device. An automatic transaction device comprising a first device mounted internally and a control unit that controls devices sends and receives data between said first device and the control unit. The first device executes processing that generates a first code relating to the first device and sends same to the control unit and executes processing that verifies a second code received from the control unit and generates an encryption key in accordance with the verification results. The control unit executes: processing whereby, after the first code has been received, verification is made that the operation environment is within the automatic transaction device; and processing whereby, if a determination is made that the operation environment is within the automatic transaction device, a second code is generated and sent to the first device.

(57) 要約:

[続葉有]

WO 2015/163340 A1

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)）

自動取引装置の全体制御部と内部デバイスとの暗号通信に必要な暗号鍵の生成において、安全性及び正当性を保証する。 内部に搭載される第１のデバイスと、装置を制御する制御部とを備え、該第１のデバイスと該制御部との間でデータの送受信を行う自動取引装置であって、前記第１のデバイスは、該第１のデバイスに関する第１のコードを生成し、前記制御部に送信する処理と、前記制御部から受信した第２のコードを検証し、検証結果に応じて暗号鍵を生成する処理と、を実行し、前記制御部は、前記第１のコードを受信した後、動作環境が前記自動取引装置内であることを検証する処理と、前記動作環境が前記自動取引装置内であると判断された場合、前記第２のコードを生成し、該第２のコードを前記第１のデバイスに送信する処理と、を実行する。

明　細　書

発明の名称 ： 自動取引装置及び自動取引システム

技術分野

[0001] 本発明は、自動取引装置及び自動取引システムに関する。

背景技術

[0002] ＡＴＭ（Ａｕｔｏｍａｔｅｄ　Ｔｅｌｌｅｒ　Ｍａｃｈｉｎｅ）等の自動取引装置において、装置を構成する内部デバイスに対して不正なコマンドが送信されることにより、不正な処理が実行されることがある。例えば、紙幣の入出金を行う紙幣処理部に対し、取引とは関係の無い不正な出金命令を送られ、現金が引き出されてしまう。このような不正な処理を防止する対策として、自動取引装置の全体制御部と内部デバイスとの間の通信を保護するための暗号化処理が実行されている。

[0003] 暗号化処理には暗号鍵が必要となるが、暗号鍵が適切に管理されていない場合、第三者によって安全性を証明された暗号アルゴリズムを採用していたとしても、暗号機能による通信の保護は期待できない。従って、自動取引装置の全体制御部と内部デバイスとのそれぞれにおいて、暗号鍵管理（暗号鍵の設定等）の安全性が求められている。

[0004] 暗号鍵を自動取引装置に設定する方法として、特許文献１には、秘密鍵を自動取引装置に予め設定し、自動取引装置にネットワークを介して接続されたホストシステムで暗号化されたマスター鍵により暗号鍵を復号することが記載されている。

先行技術文献

特許文献

[0005] 特許文献1：米国特許第６７０５５１７号公報

発明の概要

発明が解決しようとする課題

[0006] 特許文献１に開示された構成を、ＡＴＭ制御部とＡＴＭの内部に搭載され

る内部デバイスとの間で適用する場合、内部デバイスに予め秘密鍵を設定し、ＡＴＭ制御部にて暗号化された通信暗号鍵を当該秘密鍵で復号する処理を実行することにより、ＡＴＭ制御部と内部デバイスとの間でのみ当該通信暗号鍵を共有し、ＡＴＭ制御部と内部デバイスとの間の通信の暗号化及び復号化が可能となる。

[0007] しかし、暗号化通信を実行する場合や、暗号鍵が一切設定されていない自動取引装置に対して、暗号化通信機能を用いて内部デバイスに対する通信を保護する場合において、自動取引装置の全体制御部と同一の環境を構築した外部端末（ノートパソコン等）が自動取引装置の内部デバイスに接続されると、外部端末側に内部デバイスとの暗号通信に必要な暗号鍵が作成、保存されてしまう。暗号鍵が保存された外部端末と運用中の自動取引装置の内部デバイスとを接続すると、外部端末から不正なコマンドを送信することが可能となり、不正な処理が実行されてしまうおそれがある。

[0008] 特に、物理的にセキュリティが保証された場所（入退室管理機能を備えた場所）以外に設置されているＡＴＭに対して暗号鍵を設定する際に、物理的にセキュリティが保証された場所までＡＴＭを運搬することは、工数、費用、サービス停止時間の面から現実的ではないため、ＡＴＭが設定された場所において暗号鍵を設定する必要がある。

[0009] 上記課題に対処するためには、暗号鍵を生成する環境の安全性や正当性が、正当なＡＴＭとして保証される必要がある。そこで、本発明では、自動取引装置の全体制御部と内部デバイスとの暗号通信に必要な暗号鍵の生成において、安全性及び正当性を保証することを目的とする。

課題を解決するための手段

[0010] 上記課題を解決するために、本発明では、内部に搭載される第１のデバイスと、装置を制御する制御部とを備え、該第１のデバイスと該制御部との間でデータの送受信を行う自動取引装置であって、前記第１のデバイスは、該第１のデバイスに関する第１のコードを生成し、前記制御部に送信する処理と、前記制御部から受信した第２のコードを検証し、検証結果に応じて暗号

鍵を生成する処理と、を実行し、前記制御部は、前記第１のコードを受信した後、動作環境が前記自動取引装置内であることを検証する処理と、前記動作環境が前記自動取引装置内であると判断された場合、前記第２のコードを生成し、該第２のコードを前記第１のデバイスに送信する処理と、を実行することを特徴とする。

発明の効果

[0011] 本発明によれば、自動取引装置の全体制御部と内部デバイスとの暗号通信に必要な暗号鍵の生成において、安全性及び正当性を保証することが可能になる。特に、暗号鍵が一切設定されていない自動取引装置に対して暗号鍵を新規に設定する場合において安全性及び正当性を確保することにより、外部端末からの不正な処理が実行されないようにすることが可能となる。

図面の簡単な説明

[0012] [図1]実施例１における、自動取引システムの全体構成図

[図2]実施例１における、ＡＴＭの機能ブロック図

[図3]ＡＴＭ制御部のソフトウェア・データ構成図

[図4]紙幣処理部のファームウェア・データ構成図

[図5]実施例１における、処理を示すフローチャート

[図6]実施例１における、処理のデータの流れを示す図

[図7]デバイスの接続状態や、ソフトウェアのステータスを管理する管理テーブル

[図8]ＡＴＭの環境認識の結果画面

[図9]実施例２の概念図

[図10]実施例２における、自動取引システムの全体構成図

[図11]実施例２における、ＡＴＭの機能ブロック図

[図12]携帯端末のソフトウェア・データ構成図

[図13]管理サーバのソフトウェア・データ構成図

[図14]管理サーバに格納する暗号鍵生成ログの格納データ項目リスト

[図15]実施例２における、処理を示すフローチャート

[図16]実施例２における、処理のデータの流れを示す図

[図17]実施例２における、保守用表示部に表示される認証画面を示す図

[図18]実施例２における、携帯端末に表示される認証画面を示す図

[図19]実施例２における、携帯端末に表示されるレスポンス受信画面を示す図

[図20]実施例２における、保守用表示部に表示されるレスポンス受信画面を示す図

[図21]自動取引システムの全体構成図（変形例）

[図22]保守用表示部に表示される認証画面を示す図（変形例）

発明を実施するための形態

[0013] （１）実施例１

通信相手が正当であるかを認証する手段として、「チャレンジ・レスポンス認証」と呼ばれる手法が用いられる。本実施例では、自動取引装置（以下、ＡＴＭとする）の制御部（以下、「ＡＴＭ制御部（ＡＣ）」とする）がＡＴＭの環境認識をすると共に、ＡＴＭ固有の内部デバイス（ＤＥＶ）（紙幣処理部、硬貨処理部、カードリーダ、暗号化キーパッド、レシートプリンタ、通帳プリンタ、ジャーナルプリンタ、監視カメラ等のハードウェア）がＡＴＭ制御部（ＡＣ）に対して、デバイス間での「チャレンジ・レスポンス認証」を実行する。デバイス間での「チャレンジ・レスポンス認証」により、ＡＴＭ制御部（ＡＣ）に紐付けられた秘密鍵を、内部デバイス（ＤＥＶ）紙幣処理部に予め設定しておくことが可能となる。これにより、ＡＴＭ制御部（ＡＣ）で暗号化された通信暗号鍵を前記秘密鍵で復号することにより、ＡＴＭ制御部（ＡＣ）と内部デバイスのみが前記通信暗号鍵を共有でき、以降の通信を暗号化および復号することが可能となる。

[0014] 一般的な「チャレンジ・レスポンス認証」は、サーバと装置との間における認証であって、ソフトウェアで実現可能であるため、ＡＴＭ制御部（ＡＣ）以外の外部端末（例えば、ノートパソコン）に認証プログラムをコピーしても認証可能である。外部端末における認証を防止するためには、ＡＴＭ制

御部（ＡＣ）が内部デバイス（ＤＥＶ）の接続状況を参照することにより、動作環境がＡＴＭ内の環境であるか否かの認識（環境認識）を行う。すなわち、一般的な「チャレンジ・レスポンス認証」とは異なり、デバイス間での「チャレンジ・レスポンス認証」となる。その上で、ＡＴＭ制御部（ＡＣ）がレスポンスコード（ＤＥＶ　ＲＳ）を送信し、内部デバイス（ＤＥＶ）において当該レスポンスコード（ＤＥＶ　ＲＳ）を検証する。このようなＡＴＭ制御部（ＡＣ）と内部デバイス（ＤＥＶ）との間のチャレンジ・レスポンス認証により、内部デバイス（ＤＥＶ）の接続環境がＡＴＭ内であることを検証することが可能となる。なお、本実施例における内部デバイス（ＤＥＶ）として、紙幣処理部を用いる場合について説明するが、他の内部デバイス（硬貨処理部、カードリーダ、暗号化キーパッド、レシートプリンタ、通帳プリンタ、ジャーナルプリンタ、監視カメラ等）でも同様の処理が可能である。

[0015] 以下、図１～図８を用いて、第１の実施例について説明する。図１は、自動取引システムの全体構成図である。自動取引システムＳ１は、ＡＴＭ１０１と、上位装置であるホストコンピュータ１０３と、これらを接続する金融取引ネットワーク１０２とから構成される。

[0016] ＡＴＭ１０１は、利用者の操作により、現金の入出金等の取引を行う装置である。金融取引ネットワーク１０２は、例えばＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）やＷＡＮ（Ｗｉｄｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）であるが、これに限られるものではない。ホストコンピュータ１０３は、複数のＡＴＭ１０１と接続されるコンピュータであり、ＡＴＭ１０１の利用者の口座や残高に関する情報などが記録されている。

[0017] 図２は、ＡＴＭ１０１の機能ブロック図である。ＡＴＭ１０１は、ＡＴＭ内のデバイスを制御するためのＡＴＭ制御部（ＡＣ）２０１と、ＡＴＭの前面パネルの表示ランプ制御や前面パネルの開閉検知を行うＩ／Ｏ制御部２０２と、入金された紙幣や出金される紙幣を取り扱う紙幣処理部２０３と、ＡＴＭでの取引に必要なキャッシュカード等のカードの情報を読取るカードリ

ーダ部２０４と、ＡＴＭでの取引における本人確認のための暗証番号を入力し、さらに、ホストコンピュータ１０３に送るための暗号化を内部で行う暗号化キーパッド２０５と、取引の明細票を印字するレシートプリンタ２０６と、通帳の読み取りと記帳を行う通帳プリンタ２０７と、ＡＴＭ取引のログを記録するジャーナルプリンタ２０８と、ＡＴＭ利用者の顔写真を撮影する等のＡＴＭセキュリティ維持のために活用する監視カメラ２０９と、ホストコンピュータ１０３と通信を行うための通信処理部２１０と、ＡＴＭ利用者に取引に必要な情報を表示するための表示部２１１と、ＡＴＭの保守員がＡＴＭの保守作業を行う際に、ＡＴＭの保守に関する情報を表示する保守用表示部２１２と、保守員がＡＴＭの保守作業のために操作するための保守用キーボード２１３と、を備える。また、入金された硬貨や出金される硬貨を取り扱う硬貨処理部（図示せず）を備えていても良い。

[0018] 図３は、ＡＴＭ制御部（ＡＣ）２０１内のメモリに格納されたプログラム及びデータ構成を示す図である。

[0019] プログラム領域３０１には、ＡＴＭ取引全体を制御するＡＴＭ取引アプリケーション３０２と、暗号処理に関わる２種類のソフト３０３及び３０４と、９種類のデバイス制御ソフト３０５～３１３と、ソフトウェア環境の設定ファイル３１４とが格納される。

[0020] 暗号鍵インストーラ３０３は、ＡＴＭ制御部（ＡＣ）２０１と紙幣処理部２０３との間の暗号通信に必要な暗号鍵生成に関わると共に、暗号鍵生成に必要な安全な環境がＡＴＭ内部で実現しているかを検証するソフトウェアである。なお、暗号鍵インストーラ３０３は、ＡＴＭを保守するソフトウェアの一部の機能であっても良い。暗号通信制御ソフト３０４は、暗号鍵インストーラ３０３によって生成、あるいは、設定された暗号鍵を用いて、内部デバイスと暗号通信を行うソフトウェアである。デバイス制御ソフト３０５～３１３は、それぞれ２０２～２１０の機能に対応するソフトウェアである。

[0021] データ領域３１５には、ＡＴＭ制御部（ＡＣ）２０１に関するデータ３１６～３１７と、紙幣処理部２０３に関するデータ３２１～３２３との２種類

のデータが格納されている。

[0022] 保守員ＩＤ３１６は、暗号鍵をＡＴＭ内に設定する作業者を識別するための情報（識別コード）である。ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）３１７は、個々のＡＴＭを識別するための情報であり、いわゆる製造ラインで割り当てられた製造番号や、金融機関がＡＴＭを識別するために製造番号とは別に与えた識別番号等である。

[0023] 内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１は、紙幣処理部２０３を識別するための情報であり、いわゆる製造ラインで割り当てられた製造番号や、製造番号とは別に保守会社等によって与えられた識別番号等である。また、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１は、紙幣処理部２０３から送信される。

[0024] ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２は、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１と共に、紙幣処理部２０３から送信されたデータであり、ＡＴＭ制御部（ＡＣ）２０１に対し、紙幣処理部２０３がチャレンジ・レスポンス認証を行うために用いられる。

[0025] ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３は、暗号鍵インストーラ３０３により、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２から所定の一方向変換アルゴリズムにより生成される。また、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３は、ＡＴＭ制御部（ＡＣ）２０１に対し、紙幣処理部２０３の正当性を検証するために生成される。

[0026] 図４は、紙幣処理部２０３内のメモリＭ２０３に格納されたプログラム及びデータ構成を示す図である。

[0027] プログラム領域４０１には、紙幣処理部２０３の紙幣搬送などの制御を行う内部デバイス（ＤＥＶ）制御ファームウェア４０２と、ＡＴＭ制御部（ＡＣ）２０１と通信を行うための通信制御ファームウェア４０３と、ＡＴＭ制御部（ＡＣ）２０１と紙幣処理部２０３との間の通信の暗号化を実行する暗号処理ファームウェア４０４とが格納される。

[0028] データ領域４０５には、３種類のデータ４０６～４０８が格納されている。内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６は、紙幣処理部２０３を識別するための情報である。ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７は、ＡＴＭ制御部（ＡＣ）２０１の正当性を検証するために、紙幣処理部２０３がチャレンジ・レスポンス認証を行う際に生成される。

[0029] 内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６と、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７とは、共にＡＴＭ制御部（ＡＣ）２０１に送信される。ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８は、上述のチャレンジ・レスポンス認証の際に用いられるデータであって、内部デバイス（ＤＥＶ）としての紙幣処理部紙幣処理部２０３で生成される。また、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８は、ＡＴＭ制御部（ＡＣ）２０１から送信されるＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３と一致しているか否かの比較対象となるデータである。

[0030] 以下、図５（ａ）及び図６を用いて、第１の実施例における全体処理の流れを説明する。紙幣処理部２０３において、暗号処理ファームウェア４０４の所定の乱数生成器により、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７が生成される（Ｓ１０１）。その後、例えば、保守員により保守用表示部２１２に表示された所定のキーが押下されたことを検知した等の予め定めた処理が発生した場合、通信制御ファームウェア４０３により、内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６と、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７とは、ＡＴＭ制御部（ＡＣ）２０１に送信される（Ｓ１０２）。

[0031] ＡＴＭ制御部（ＡＣ）２０１では、内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６とＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７とを受信し、データ領域３１５内の、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１及びＤＥＶチャレンジコ

ード１（ＤＥＶ　ＣＨ　１）３２２もそれぞれに格納する。さらに、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１は、暗号鍵生成のトレース情報として電子ジャーナルなどのログファイルに記録される。暗号鍵漏洩などの問題発生時に、このログファイルを参照することで、暗号鍵生成状況を確認することができる。このログファイルは改ざん防止などのセキュリティ対策を施されることが望ましい。

[0032] その後、暗号鍵インストーラ３０３は、ＡＴＭ制御部（ＡＣ）が動作している環境が外部端末（一般のノートパソコン等）ではなく、ＡＴＭ１０１の内部であることを検証するために、ＡＴＭの環境認識を行う（Ｓ１０３）。例えば、ＡＴＭ１０１に固有のデバイスである、Ｉ／Ｏ制御部２０２、カードリーダ２０４、暗号化キーパッド２０５等が、ＡＴＭ制御部（ＡＣ）２０１に接続されているか否かを判断する。当該判断は、例えば、ＡＴＭアプリケーション３０２が各デバイスに対して、デバイスの起動を指示し、起動した旨のレスポンスを確認することにより行われる。また、ＡＴＭの環境認識の精度を向上させるため、各デバイスが単に接続されているか否かを判断するだけでなく、インストールされているソフトウェア、環境設定パラメータ群、デバイスのエラー状態等も参照することにより、各デバイスが適切に動作しているか否かを判断しても良い。

[0033] また、ＡＴＭの環境認識の例として、ＡＴＭ制御部（ＡＣ）２０１内のプログラムや設定が正当なものであるか、例えば電子署名や所定のツールなどを用いて検証することも可能である。

[0034] このようなＡＴＭの環境認識にあたり、図７に示すような、デバイスの接続状態（立上状態）や、ソフトウェアのステータスを管理する管理テーブル１５００を用いて処理を実行しても良い。１５０１は、ＡＴＭ内に実装されているデバイス／ソフトウェア名称であり、１５０２は、各デバイスが正常に立ち上がったか否かを示す状態データであり、１５０３は、各デバイスの立ち上げが異常である場合における、異常の種類を示すエラーコードなどの具体的異常状態を示すデータである。データ１５０４～１５１２は、それぞ

れ図３に示すＩ／Ｏ制御部制御ソフト３０５、紙幣処理部制御ソフト３０６、カードリーダ制御ソフト３０７、暗号化キーパッド制御ソフト３０８、レシートプリンタ制御ソフト３０９、通帳プリンタ制御ソフト３１０、ジャーナルプリンタ制御ソフト３１１、監視カメラ制御ソフト３１２、通信処理ソフト３１３の動作状態にそれぞれ対応する。また、データ１５１３は、図３に示すＡＴＭアプリケーション３０２の完全性検証状態に対応するが、暗号鍵インストーラ３０３又は暗号通信制御ソフト３０４の完全性検証状態を含めても良い。また、データ１５１４は、図３に示すソフトウェア設定ファイル３１４の完全性検証状態に対応する。ここで、完全性（ｉｎｔｅｇｒｉｔｙ）検証とは、データの改竄や破壊が無いことを検証する処理である。

[0035] このとき、ＡＴＭが立ち上がる過程で、各デバイスの接続状態（立上状態）を予め管理テーブル１５００に格納する。そして、ＡＴＭの環境認識において、暗号鍵インストーラ３０２が本テーブルを参照し、各デバイスが正常立上げであるか、または各ソフトウェアの完全性が検証されているか、を確認する。

[0036] ＡＴＭの環境認識の結果は、保守用表示部２１２に表示される。図８は、ＡＴＭの環境認識の結果画面の一例である。ＡＴＭの環境認識の結果画面１６００は、デバイスのステータスを表示するデバイスステータス領域１６０１と、ソフトウェアのステータスを表示するソフトウェアステータス領域１６０２と、「続行」キー１６０３と、「再実行」キー１６０４と、「キャンセル」キー１６０５とを備える。

[0037] デバイスステータス領域１６０１には、図７で示したデータ１５０４～１５１２に対応するデータが表示される。また、ソフトウェアステータス領域１６０２には、図７で示したデータ１５１３、１５１４に対応するデータが表示される。

[0038] 各データの接続状態（立上状態）が正常であり、保守員により「続行」キー１６０３が押下されたことを検出した場合は、次のステップ以降の処理を実行する。一方、異常があるデータを検出した場合は、保守員により該当す

るデバイスやソフトウェアの状態を確認する必要がある。その後、保守員により「再実行」キー１６０４が押下されたことを検出した場合は、再度環境認識を実行する。一方、異常があるデータを検出した場合であり、保守員により「キャンセル」キー１６０５が押下されたことを検出した場合は、処理を停止する。なお、異常があるデータを検出した場合は、「続行」キー１６０３を表示しなかったり、「続行」キー１６０３の押下を検出しないようにすることが望ましい。

[0039] ＡＴＭの環境認識に失敗した場合、ＡＴＭ制御部（ＡＣ）２０１は、正当なＡＴＭ環境ではないと判断し、ＡＴＭの環境認識の失敗結果をログファイルに記録する。このログファイルは、暗号化などにより改ざんに対して保護されていることが望ましい。その後、紙幣処理部２０３に対して、正当なＡＴＭ環境ではない旨を示すデータを送信する。紙幣処理部２０３は、当該データを受信し、正当なＡＴＭ環境ではない旨を記録し、更なるセキュリティ対策を施すことも可能である。例えば、正当なＡＴＭ環境ではない旨を記録した累積回数、または、正当なＡＴＭ環境ではない旨を記録した連続回数が所定値を超えた場合に、ＡＴＭではなく外部端末（ノートパソコン等）から不正なアクセスがされていると見做し、紙幣処理部２０３の暗号鍵生成動作を閉塞させることも可能である。

[0040] ＡＴＭの環境認識に成功した場合、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１及びＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２から、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３が生成される（Ｓ１０４）。生成されたＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３は、紙幣処理部２０３に送信される（Ｓ１０５）。

[0041] 紙幣処理部２０３では、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３を受信すると、所定の変換アルゴリズムを用いて、内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６とＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７とから、ＤＥＶレスポンスコード１（ＤＥＶ

ＲＳ　１）４０８を生成する。ここで、所定の変換アルゴリズムとは、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１とＡＴＭ制御部（ＡＣ）２０１のＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２から、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３を生成する変換アルゴリズムと同一の変換アルゴリズムである。

[0042] 次に、受信したＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３と、生成されたＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８とが一致するかを検証する（Ｓ１０６）。

[0043] このように、紙幣処理部２０３における変換アルゴリズムは、ＡＴＭ制御部（ＡＣ）２０１と共有されている。その結果、内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６が、ＡＴＭ制御部（ＡＣ）２０１のログファイルに登録されたかを、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３とＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８との一致を検証することにより、紙幣処理部２０３側で確認することが可能となる。この一致検証により、紙幣処理部２０３は、安全なＡＴＭ運用環境であると判断し、その後暗号鍵生成コマンドを受信した場合に暗号鍵生成処理を実行する。

[0044] ここで、紙幣処理部２０３は、安全なＡＴＭ運用環境であると判断した後に、暗号鍵生成コマンドを受信するまでの間に時間の上限を設けることも可能である。時間制限を設けることにより、保守員がＡＴＭ１０１を操作中に現場から離れてしまった場合に、第三者が暗号鍵生成コマンドを部デバイス（ＤＥＶ）としての紙幣処理部２０３に送信して、不正に暗号鍵を生成されるリスクが回避される。

[0045] 受信したＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３と、生成されたＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８とが一致しない場合は、暗号鍵を生成する適切な環境にないとして、紙幣処理部２０３は、後に暗号鍵生成コマンドを受信したとしても処理を拒絶する。なお、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３とＤＥＶレスポンスコー

ド１（ＤＥＶ　ＲＳ　１）４０８との不一致が所定の回数以内であれば、Ｓ１０１から再度処理を実行しても良い。この場合、所定の回数を超えて不一致となったときは、紙幣処理部２０３に対して不正なアクセスがされていると見做し、所定の期間Ｓ１０１の処理を拒絶する。また、処理の拒絶の他に、ＡＴＭ制御部（ＡＣ）と紙幣処理部２０３との通信を遮断しても良い。

[0046] 第１の実施例によれば、内部デバイスと通信する相手であるＡＴＭ制御部（ＡＣ）において、暗号鍵を生成するソフトウェアの動作環境が外部端末ではなく、ＡＴＭ内の環境であることの環境認識を行う。すなわち、ＡＴＭ制御部（ＡＣ）が内部デバイスの接続状況を参照すると共に、レスポンスコード（ＤＥＶ　ＲＳ）を送信し、内部デバイスでそれを検証することにより、内部デバイスの接続環境を検証する。これにより、暗号化通信を実行する場合や、暗号鍵が一切設定されていない自動取引装置に対して暗号鍵を新規に設定する場合において、暗号鍵を生成するソフトウェアが、ＡＴＭ以外の外部端末で動作していないことを検証することが可能となる。

[0047] また、耐タンパ性を持つセキュアチップのような安全なハードウェアを用いて、暗号鍵をそのハードウェア内部で生成する場合であっても、安全な環境であることを確認することは有効である。ハードウェア内部で暗号鍵を生成する場合は、暗号鍵生成命令を送るためのアクセスコントロールが必要となる。その場合、アクセスコントロールにパスワード認証などが使われるが、パスワードが漏洩すると、例えば、秘密鍵・公開鍵が勝手にハードウェア内部で生成され、公開鍵が不必要にそのハードウェアから取り出されることがある。このように意図しない暗号鍵の取り出しは脆弱性につながるのでハードウェアであっても環境の安全性は重要である。

[0048] なお、本実施例では、内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６が、ＡＴＭ制御部（ＡＣ）２０１のログファイルに登録されたかを、紙幣処理部２０３が検証できるようにするために、Ｓ１０４において、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１とＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２との２つの

情報から、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３を生成する。しかし、ＡＴＭ制御部（ＡＣ）２０１のログファイルへの登録を、紙幣処理部２０３がＳ１０６のレスポンスコード検証を通じて確認する必要がなければ、Ｓ１０４では、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２の１つの情報から、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３を生成してもよい。その場合、Ｓ１０６での検証も同様に、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７の一つの情報から、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８を生成することになる。

[0049] また、本実施例では、内部デバイス（ＤＥＶ）において、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）を検証する例について説明したが、例えば、不正な内部デバイス（ＤＥＶ）が接続されている可能性がある場合は、ＡＴＭ制御部（ＡＣ）においてレスポンスコードを生成、検証するようにしても良い。

[0050] この場合、図５（ｂ）に示すように、最初にＡＴＭ制御部（ＡＣ）２０１は、動作環境が前記自動取引装置内であることを検証する処理を実行し（Ｓ１１１）、前記動作環境が前記自動取引装置内であると判断された場合、ＡＣチャレンジコード１（ＡＣ　ＣＨ　１）を生成し（Ｓ１１２）、ＡＣシリアルナンバー（ＡＣ　Ｓｅｒ．Ｎｏ．）とＡＣチャレンジコード１（ＡＣ　ＣＨ　１）とを、内部デバイス（ＤＥＶ）に送信する（Ｓ１１３）。その後、内部デバイス（ＤＥＶ）は、ＡＣシリアルナンバー（ＡＣ　Ｓｅｒ．Ｎｏ．）及びＡＣチャレンジコード１（ＡＣ　ＣＨ　１）から、ＡＣレスポンスコード１（ＡＣ　ＲＳ　１）を生成し（Ｓ１１４）、ＡＴＭ制御部（ＡＣ）２０１に送信する（Ｓ１１５）。３２３が生成される（Ｓ１０４）。生成されたＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３は、内部デバイス（ＤＥＶ）に送信される（Ｓ１０５）。最後に、ＡＴＭ制御部（ＡＣ）２０１は、内部デバイス（ＤＥＶ）から受信したＡＣレスポンスコード１（ＡＣ　ＲＳ　１）と、ＡＴＭ制御部（ＡＣ）２０１において、受信したＡＣレスポンスコード１（ＡＣ　ＲＳ　１）と、ＡＣシリアルナンバー（ＡＣ　Ｓ

ｅｒ．Ｎｏ．）及びＡＣチャレンジコード１（ＡＣ　ＣＨ　１）から生成されたＡＣレスポンスコード１（ＡＣ　ＲＳ　１）とが一致するかを検証する（Ｓ１１６）。上記説明ではＡＣシリアルナンバー（ＡＣ　Ｓｅｒ．Ｎｏ．）及びＡＣチャレンジコード１（ＡＣ　ＣＨ　１）を一緒に送信して、その両者からＡＣレスポンスコード１（ＡＣ　ＲＳ　１）を生成する例を示したが、ＡＣチャレンジコード１（ＡＣ　ＣＨ　１）のみを送信し、ＡＣチャレンジコード１（ＡＣ　ＣＨ　１）からＡＣレスポンスコード１（ＡＣ　ＲＳ　１）を生成してもよい。

[0051] なお、本実施例は、ＡＴＭ制御部（ＡＣ）と内部デバイス（ＤＥＶ）との間において、チャレンジコード、レスポンスコードを用いるチャレンジ・レスポンス認証を例にして説明したが、他の認証形式でも良い。例えば、使い捨て方式のパスワードである、ワンタイムパスワード（Ｏｎｅ　Ｔｉｍｅ　ＰＷ）を用いた方式が挙げられる。ワンタイムパスワード方式でも複数の方式がありうるが、例えば、認証する側とされる側で時刻を共有しておき、その時刻に対応するパスワードを同じ適当なアルゴリズムを用いて互いに生成して検証する方式について、図５（ｃ）を用いて説明する。なお、内部デバイス（ＤＥＶ）にも時計が実装されていることが前提である。

[0052] まず、内部デバイス（ＤＥＶ）では、内蔵されている時計を参照して、時刻データを取得する（Ｓ１２１）。得られた時刻データから、適当なアルゴリズムを用いてワンタイムパスワード（ＤＥＶ　Ｏｎｅ　Ｔｉｍｅ　ＰＷ）が生成される（Ｓ１２２）。その後、内部デバイス（ＤＥＶ）はＡＴＭ制御部（ＡＣ）に対し、ＡＣワンタイムパスワード（ＡＣ　Ｏｎｅ　Ｔｉｍｅ　ＰＷ）の送信要求を送信する（Ｓ１２３）。

[0053] ＡＴＭ制御部（ＡＣ）の暗号鍵インストーラ３０３は、ステップＳ１０３と同様の手順に基づき、ＡＴＭの環境認識を行う（Ｓ１２４）。ＡＴＭの環境認識が成功した場合は、ＡＴＭ制御部（ＡＣ）２０１内に組み込まれている時計を参照し、時刻データ（ＡＣ時刻データ）を取得する（Ｓ１２５）。そして、得られた時刻データから、内部デバイス（ＤＥＶ）と同じアルゴリ

ズムを用いて、ワンタイムパスワード（ＡＣ　Ｏｎｅ　Ｔｉｍｅ　ＰＷ）を生成し（Ｓ１２６）、ＡＣワンタイムパスワード（ＡＣ　Ｏｎｅ　Ｔｉｍｅ　ＰＷ）を内部デバイス（ＤＥＶ）に送信する（Ｓ１２７）。内部デバイス（ＤＥＶ）は、ＤＥＶワンタイムパスワード（ＤＥＶ　Ｏｎｅ　Ｔｉｍｅ　ＰＷ）とＡＣワンタイムパスワード（ＡＣ　Ｏｎｅ　Ｔｉｍｅ　ＰＷ）とが一致しているかを検証し（Ｓ１２８）、検証結果に応じて暗号鍵生成処理の実行等の処理を実行する。

[0054] このように、共有されている時刻データを用いたワンタイムパスワード方式を用いて、内部デバイス（ＤＥＶ）はＡＴＭ制御部（ＡＣ）２０１を認証することが可能である。

[0055] （２）実施例２

以下、図２、図４、図９～２０を用いて、第２の実施例について説明する。

図９は、第２の実施例の概念、すなわち、第２の実施例における処理手順の基本的な考え方について示した図である。

[0056] 例えば、保守用の倉庫にＡＴＭが保管されている場合（すなわちＡＴＭが運用されていない場合）、運用に必要なソフトウェア群をＡＴＭ制御部（ＡＣ）上にコピーして、その状態で暗号鍵を生成することが可能になる。この場合、ＡＴＭは運用されていないため、ソフトウェアの構成が変更された上で、暗号鍵が生成された際にメモリダンプが行われると、暗号鍵が不正に取得されてしまう。

[0057] このような不正を防止するためには、第１の実施例において説明した、内部デバイス（ＤＥＶ）の接続環境がＡＴＭ内であることの検証（（ａ）参照）に加え、ＡＴＭが運用中であるか否かを更に検証することが必要である。ＡＴＭが運用中であることは、ＡＴＭがホストコンピュータに接続されていることが一つの判断材料になる。しかし、暗号鍵をＡＴＭに設定する際は、通常の取引を実行する運用モードとは別のモードである保守モードでＡＴＭを動作させるため、ホストコンピュータへの接続は切断されていることが一

般的であり、ＡＴＭ１０１とホストコンピュータ１０３との間の通信状態を基に、運用中のＡＴＭであることを検証することは困難である。そのため、運用中のＡＴＭであるか否かを判断するためには、ホストコンピュータ１０３との接続以外の手段で判断する必要がある。

[0058] そこで、（ｂ）に示すように、内部デバイス（ＤＥＶ）は、ＡＴＭの外部に設置された管理サーバに対して、暗号鍵生成のトレーサビリティに必要な情報（内部デバイス（ＤＥＶ）のシリアルナンバー、ＡＴＭのシリアルナンバー、日時、作業者のＩＤ等）を送信し、当該管理サーバで当該情報を保管する処理が考えられる。仮に、不正な暗号鍵生成が行われた場合、当該トレーサビリティ情報を用いて、不正行為者等の追跡調査ができるので、運用されていないＡＴＭを用いた不正な暗号鍵生成を抑止できる。

[0059] 暗号鍵生成のトレーサビリティに必要な情報が管理サーバに確実に保管されたか否かは、内部デバイス（ＤＥＶ）においてチャレンジ・レスポンス認証を用いて検証される。例えば、管理サーバは、内部デバイスが生成したチャレンジコードと、トレーサビリティに必要な情報とから、一方向関数などの所定の変換アルゴリズムを用いて、レスポンスコードを生成する。内部デバイス（ＤＥＶ）において、管理サーバから送信されたレスポンスコードを正しく検証できれば、管理サーバに暗号鍵生成のトレーサビリティに必要な情報が確実に登録されたことを確認することが可能である。

[0060] このように、トレーサビリティに必要な情報が管理サーバに確実に登録されたことを、内部デバイス（ＤＥＶ）において検証することにより、保守モードであるか否かによらず、運用中のＡＴＭに接続されていることを確認することが可能である。

[0061] また、暗号鍵が生成される際に、内部デバイス（ＤＥＶ）だけでなく、ＡＴＭ制御部（ＡＣ）も、運用中のＡＴＭの環境であることを検証する必要がある。そこで、（ｃ）に示すように、ＡＴＭ制御部（ＡＣ）も、ＡＴＭの外部に設置された管理サーバに対して、暗号鍵生成のトレーサビリティに必要な情報を送信し、当該管理サーバで当該情報を保管する処理が考えられる。

そして、暗号鍵生成のトレーサビリティに必要な情報が管理サーバに確実に保管されたか否かは、ＡＴＭ制御部（ＡＣ）においてチャレンジ・レスポンス認証を用いて検証される。

[0062] 以上（ａ）～（ｃ）で説明した概念を組み合わせることにより、暗号鍵の不正漏洩があった場合に、認証用のサーバに登録された履歴情報を参照することで、問題のあったＡＴＭのトレースが可能になり、結果として暗号鍵生成に伴う不正行為を抑止することが可能となる。すなわち、（ａ）（ｃ）に示すＡＴＭ制御部（ＡＣ）が同一であり、かつ（ｂ）（ｃ）に示す管理サーバが同一かつ正当な通信相手であることの情報を用いて、内部デバイスにおいて、運用中のＡＴＭに接続されていることを精度良く検証することが可能となる。本実施例では、（ａ）～（ｃ）で説明した概念である（ｄ）を実現する構成や処理について、詳細に説明する。

[0063] 図１０は、自動取引システムの全体構成図である。自動取引システムＳ２は、第１の実施例で述べたＡＴＭ１０１、金融取引ネットワーク１０２、ホストコンピュータ１０３の他に、携帯情報端末１０４と、金融取引ネットワーク１０２とは別のネットワークである、保守用ネットワーク１０５と、管理サーバ１０６と、ストレージ１０７とを備える。ＡＴＭ１０１は、携帯情報端末１０４を介し、保守用ネットワーク１０５に接続され、管理サーバ１０６と情報のやり取りを行う。ストレージ１０７は、管理サーバ１０６に接続され、携帯情報端末１０４経由でＡＴＭ１０１から送信される暗号鍵生成のトレース情報を格納する格納部である。

[0064] ＡＴＭ１０１の機能ブロック図は、第１の実施例と同様であるため（図２を参照）、詳細な説明を省略する。

[0065] 図１１は、ＡＴＭ制御部（ＡＣ）２０１内のメモリに格納されたプログラム・データ構成を示す図である。プログラム領域３０１は、第１の実施例と同様であるため、詳細な説明を省略する。

[0066] データ領域３１５には、ＡＴＭ制御部（ＡＣ）２０１に関するデータ３１６～３２０と、内部デバイス（ＤＥＶ）に関するデータ３２１～３２５との

２種類のデータが格納されている。

[0067] 時刻データ３１６は、管理サーバ１０６にデータを送信する時刻を表すデータである。保守員ＩＤ３１７は、暗号鍵をＡＴＭ内に設定する作業者を識別するための識別コードである。ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）３１８は、個々のＡＴＭを識別するための情報であり、いわゆる製造ラインで割り当てられた製造番号や、金融機関がＡＴＭを識別するために製造番号とは別に与えた識別番号等である。

[0068] ＡＣチャレンジコード（ＡＣ　ＣＨ）３１９は、ＡＴＭ制御部（ＡＣ）２０１が管理サーバ１０６の正当性を検証する際に、チャレンジ・レスポンス認証を行うために生成される。すなわち、ＡＣチャレンジコード（ＡＣ　ＣＨ）３１９は、ＡＴＭ制御部（ＡＣ）２０１が、管理サーバ１０６を認証すると共に、当該管理サーバ１０６でトレーサビリティ用の登録データが適切に保存されたかを検証するために生成される。ＡＣレスポンスコード（ＡＣ　ＲＳ）３２０は、チャレンジ・レスポンス認証のために用いられるデータであって、ＡＴＭ制御部（ＡＣ）２０１によって生成される。また、ＡＣレスポンスコード（ＡＣ　ＲＳ）３２０は、管理サーバ１０６から送信されるＡＣレスポンスコード（ＡＣ　ＲＳ）７１１（図１３参照）と一致しているか否かの比較対象となるデータである。

[0069] 内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１は、紙幣処理部２０３を識別するための情報であり、いわゆる製造ラインで割り当てられた製造番号や、製造番号とは別に保守会社等によって与えられた識別番号等である。また、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１は、紙幣処理部２０３から送信されたデータであり、暗号鍵生成のトレース情報の一部として管理サーバ１０６に送信される。

[0070] ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２は、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１と共に、紙幣処理部２０３から送信されたデータであり、ＡＴＭ制御部（ＡＣ）２０１

に対し、紙幣処理部２０３がチャレンジ・レスポンス認証を行うために用いられる。また、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２は、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１が管理サーバ１０６に確実に送信されたことを、紙幣処理部２０３が検証する際にも用いられる。

[0071] ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３は、暗号鍵インストーラ３０３により、後述するＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）３２４から所定の一方向変換アルゴリズムにより生成される。また、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３は、ＡＴＭ制御部（ＡＣ）２０１と管理サーバ１０６との両者に対し、紙幣処理部２０３の正当性を検証するために生成される。さらに、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３により、暗号鍵トレース情報として、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１が管理サーバ１０６に確実に届いたことも検証することが可能となる。

[0072] ＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）３２４は、暗号鍵インストーラ３０３により、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２から一方向変換を行うことにより生成される。また、ＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）３２４は、紙幣処理部２０３により、管理サーバ１０６の正当性が検証される際に用いられ、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１と共に管理サーバ１０６に送信される。なお、管理サーバ１０６に送信されるデータは、これに限るものではなく、暗号鍵生成のトレースに寄与できるデータであれば、どのようなデータでもよい。

[0073] ＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）３２５は、管理サーバ１０６によって生成されたレスポンスコードである。すなわち、適切な一方向変換によって、紙幣処理部製造番号３２１とＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）と２つのデータから、ＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）３２５が管理サーバ１０６上で生成される。ＤＥＶレスポンス

コード２（ＤＥＶ　ＲＳ　２）３２５は、紙幣処理部２０３により、管理サーバ１０６の正当性を検証するために生成される。

[0074] 紙幣処理部２０３内のメモリに格納されたプログラム及びデータ構成は、第１の実施例と同様であるため（図４を参照）、詳細な説明を省略する。

[0075] 図１２は、ＡＴＭ１０１からの入出力データを管理サーバ１０６と送受信するために用いられる携帯端末１０４内の、メモリＭ１０４に格納されたプログラム・データ構成を示す図である。

[0076] プログラム領域５０１には、４種類のソフトウェア５０２～５０５が格納される。通信制御ソフトウェア５０２は、無線ネットワーク１０５を介して通信を行うためのソフトウェアである。データ送信ソフトウェア５０３は、データを管理サーバ１０６に送信するためのソフトウェアであり、例えば、ショートメッセージや電子メールソフトウェアである。データ入力ソフトウェア５０４は、ＡＴＭ１０１の保守用表示部２１２に表示されたデータを携帯端末１０４に入力するためのソフトウェアであり、例えば、二次元コードを読み取るソフトウェアである。データ表示ソフトウェア５０５は、携帯端末１０４の情報をＡＴＭ１０１に入力するためにデータの表示形式を変換するためのソフトウェアであり、例えば、バーコードや二次元コードの生成や表示をするソフトウェアである。

[0077] データ領域５０６には、管理サーバ１０６に対して送信されるデータと、管理サーバ１０６から受信されるデータとが格納される。すなわち、ＡＴＭ１０１の保守用表示部２１２に表示され、携帯端末１０４内に取り込まれ、管理サーバ１０６に送信されるデータと、管理サーバ１０６から受信され、ＡＴＭ１０１に入力されるデータとが格納される。

[0078] 具体的には、データ領域５０６には、８種類のデータ５０７～５１２、６０１、６０２が格納される。時刻データ５０７、保守員ＩＤ　５０８、ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）５０９、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）５１０、ＡＣチャレンジコード（ＡＣ　ＣＨ）５１１及びＤＥＶチャレンジコード２（ＤＥＶ　Ｃ

Ｈ　２）５１２は、ＡＴＭ制御部（ＡＣ）２０１のデータ領域３１５に格納されているデータ３１８、３１６、３１７、３２１、３１９及び３２４にそれぞれ対応するデータ。また、ＡＣレスポンスコード（ＡＣ　ＲＳ）６０１及びＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）６０２は、ＡＴＭ制御部（ＡＣ）２０１のデータ領域３１５に格納されているデータ３２０及び３２５にそれぞれ対応する。

[0079] 図１３は、管理サーバ１０６内のメモリＭ１０６に格納されたプログラム・データ構成を示す図である。

[0080] プログラム領域７０１には、２種類のソフトウェア７０２～７０３が格納される。ＡＴＭ暗号鍵生成管理ソフトウェア７０２は、ＡＴＭ暗号鍵生成のログ管理や、受信したＡＣチャレンジコード（ＡＣ　ＣＨ）やＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）から、ＡＣレスポンスコード（ＡＣ　ＲＳ）やＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）を生成すると共に、ストレージ１０７に暗号鍵トレース情報を格納するソフトウェアである。通信制御ソフトウェア７０３は、ネットワーク１０５を介して携帯端末１０４と通信を行うためのソフトウェアである。

[0081] データ領域７０４には、ログとして保存するデータとして、８種類のデータ７０５～７１２が格納される。これらのデータの内、時刻データ７０５、保守員ＩＤ７０６、ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）７０７、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）７０８、ＡＣチャレンジコード（ＡＣ　ＣＨ）７０９及びＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）７１０は、携帯端末１０４から受信したデータであり、それぞれデータ５０７～５１２に対応する。

[0082] ＡＣレスポンスコード（ＡＣ　ＲＳ）７１１は、ＡＴＭ暗号鍵生成管理ソフトウェア７０２によって生成されたデータである。ＡＣレスポンスコード（ＡＣ　ＲＳ）７１１を生成する際に、ＡＴＭ暗号鍵生成管理ソフトウェア７０２は、入力された時刻データ７０５、保守員ＩＤ７０６、ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）７０７及びＡＣチャレンジコード（

ＡＣ　ＣＨ）７０９を用いて、適切な一方向変換処理（ハッシュ計算等）を実行する。

[0083] ＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）７１２は、ＡＣレスポンスコード（ＡＣ　ＲＳ）７１１と同様に、ＡＴＭ暗号鍵生成管理ソフトウェア７０２によって生成されたデータである。ＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）７１２を生成する際に、ＡＴＭ暗号鍵生成管理ソフトウェア７０２は、入力された内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）７０８及びＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）７１０を用いて、適切な一方向変換処理（ハッシュ計算等）を実行する。

[0084] 図１４は、ストレージ１０７に格納される暗号鍵生成ログ（トレース情報）のデータ項目名を示した図である。項目８０１～８０８は、管理サーバ１０６内のメモリＭ１０６に格納されたデータ７０５～７１２にそれぞれ対応する。

[0085] 以下、図１５及び図１６を用いて、第２の実施例における全体処理の流れを説明する。紙幣処理部２０３において、暗号処理ファームウェア４０４の所定の乱数生成器により、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７が生成される（Ｓ２０１）。その後、例えば、保守員により保守用表示部２１２に表示された所定のキーが押下されたことを検知した等の予め定めた処理が発生した場合、通信制御ファームウェア４０３により、内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６と、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７とは、ＡＴＭ制御部（ＡＣ）２０１に送信される（Ｓ２０２）。ＡＴＭ制御部（ＡＣ）２０１では、内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６とＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７とを受信し、データ領域３１５内の、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１及びＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２としてそれぞれに格納する。その後、暗号鍵インストーラ３０３は、ＡＴＭ制御部（Ａ

Ｃ）が動作している環境が外部端末（一般のノートパソコン等）ではなく、ＡＴＭ１０１の内部であることを検証するために、ＡＴＭの環境認識を行う（Ｓ２０３）。

[0086] Ｓ２０１～Ｓ２０３の処理は、第１の実施例におけるＳ１０１～Ｓ１０３の処理と同様である。但し、第２の実施例の場合、ＡＴＭアプリケーション３０２により、ＡＴＭ１０１とホストコンピュータ１０３とが、金融取引ネットワーク１０２を介して接続されているか否かを判断することにより、正常な運用がされているＡＴＭであることも確認可能である。ＡＴＭ１０１に暗号鍵を設定する際には、保守モードでＡＴＭ１０１を起動し、通常の取引サービス提供を停止する必要がある。保守モードである場合、ＡＴＭ１０１とホストコンピュータ１０３とが接続されているか否かを判断することは、一般的に不可能である。このような場合は、ＡＴＭ１０１内のログデータに含まれる、電子ジャーナルなどの時刻を含むデータを参照し、ホストコンピュータ１０３と接続され、正常な運用がされているＡＴＭであることを確認しても良い。

[0087] ＡＴＭの環境認識に失敗した場合の処理は、第１の実施例と同様であるため、説明を省略する。

[0088] ＡＴＭの環境認識に成功した場合、所定の乱数生成器を用いて、ＡＣチャレンジコード（ＡＣ　ＣＨ）３１９が生成される（Ｓ２０４）。その後、ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２から、所定の変換アルゴリズムを用いてＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）３２４を生成する（Ｓ２０５）。当該変換アルゴリズムは、ＡＴＭ制御部（ＡＣ）２０１と紙幣処理部２０３との間で共有されているものとし、例えば、紙幣処理部２０３から送られてきた管理サーバ１０６への登録データである、内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６を、変換アルゴリズムの入力の一つにしても良い。

[0089] その後、保守員ＩＤ３１６、ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）３１７、時刻データ３１８、ＡＣチャレンジコード（ＡＣ　ＣＨ）

３１９、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１及びＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）３２４を、管理サーバ認証用データとして保守用表示部２１２に表示する（Ｓ２０６）。

[0090] 保守用表示部２１２に表示される、管理サーバへの認証画面の例を図１７に示す。１７０１～１７０６は、それぞれ図１１に示す時刻データ３１８、保守員ＩＤ３１６、ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）３１７、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１、ＡＣチャレンジコード（ＡＣ　ＣＨ）３１９及びＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）３２４に対応する。１７０７は、１７０１～１７０６の情報を格納した２次元コードである。このように、保守用表示部２１２への表示は、テキスト形式による表示の他、所定のリーダで読取ることが可能であれば、バーコードまたは２次元コードのようなコード形式による表示でも良い。これにより、保守員は、管理サーバ認証用データを自らが保有している携帯端末１０４に入力することが可能となる。なお、管理サーバ認証用データは、無線の他の手段によりＡＴＭ１０１の外部に出力しても良い。

[0091] また、保守用表示部２１２に表示された２次元コード１７０７が外光などの悪条件により携帯端末の読取装置で読み取りづらい場合は、プリンタから印字された２次元コードを読み取ることで処理を継続しても良い。この場合、１７０８に表示された「印刷」キーが押下されたときに、ＡＴＭに実装されているいずれかの印字手段を用いて、２次元コードを印字する。さらに、無線通信等の手段により、管理サーバ認証用データをＡＴＭ１０１の外部に出力しても良い。

[0092] 携帯端末１０４は、管理サーバ認証用データが入力されたことを確認し、データ領域５０６内のデータ５０７～５１２に前述の情報を格納する（Ｓ２０７）。管理サーバ認証用データの携帯端末１０４への入力は、例えば、データ入力ソフトウェア５０４が、バーコードリーダや２次元コードリーダを

備えている場合、当該リーダを用いてＡＴＭ１０１の保守用表示部２１２に表示されたコード情報を読み取るようにしても良い。携帯端末１０４の表示部に表示される、管理サーバへの認証画面の表示例を図１８に示す。１８０１～１８０６は、それぞれ図１１に示す時刻データ３１８、保守員ＩＤ３１６、ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）３１７、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）３２１、ＡＣチャレンジコード（ＡＣ　ＣＨ）３１９及びＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）３２４（すなわち、図１７に示す１７０１～１７０６）に対応する。

[0093] その後、「送信」キー１８０７の押下が検出されると、データ送信ソフトウェア５０３は、通信ネットワーク１０５を介して、管理サーバ１０６にデータ５０７～５１２を送信する（Ｓ２０８）。

[0094] 管理サーバ１０６は、携帯端末１０４より送信されたデータ５０７～５１２を受信し、ＡＴＭ暗号鍵生成管理ソフトウェア７０２により、データ領域７０４上のデータ７０５～７１０として格納する（Ｓ２０９）。その後、ＡＴＭ暗号鍵生成管理ソフトウェア７０２は、所定の変換アルゴリズムを用いて、時刻データ７０５、保守員ＩＤ706、ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）７０７及びＡＣチャレンジコード（ＡＣ　ＣＨ）７０９から、ＡＣレスポンスコード（ＡＣ　ＲＳ）７１１を生成する。同様に、ＡＴＭ暗号鍵生成管理ソフトウェア７０２は、所定の変換アルゴリズムを用いて、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）７０８及びＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）７１０から、ＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）７１２を生成する（Ｓ２１０）。

[0095] 所定の変換アルゴリズムとは、例えば、チャレンジコード（ＡＣ　ＣＨ、ＤＥＶ　ＣＨ２）とそれ以外の入力データとを結合した上で、それに所定の一方向変換関数を掛けてレスポンスコードを生成するような関数が考えられる。このように、管理サーバ１０６とＡＴＭ制御部（ＡＣ）２０１の間で、

または管理サーバ１０６と紙幣処理部２０３の間でそれぞれ共有された変換アルゴリズムを用いると共に、レスポンスコード（ＡＣ　ＲＳ、ＤＥＶ　ＲＳ　２）の生成の際に、チャレンジコードとそれ以外の入力データとを含めることにより、レスポンスコードを検証するＡＴＭ制御部（ＡＣ）２０１や、紙幣処理部２０３は、送信したデータが確実に管理サーバ１０６に届いたことを確認することが可能となる。

[0096] ＡＴＭ暗号鍵生成管理ソフトウェア７０２は、携帯端末１０４より受信したデータと生成された２種類のレスポンスコードとを、図１４に示す暗号鍵生成ログ（トレース情報）として、ストレージ１０７に格納する（Ｓ２１１）。その後、ＡＴＭ暗号鍵生成管理ソフトウェア７０２は、ＡＣレスポンスコード（ＡＣ　ＲＳ）７１１とＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ２）７１２とを、携帯端末１０４に対して送信する（Ｓ２１２）。

[0097] Ｓ２０９～Ｓ２１２の処理を実行している際に、携帯端末１０４より送信されたデータ５０７～５１２の全部または一部が同一であるデータを、一定時間内に繰り返し管理サーバ１０６で受信した場合、管理サーバ１０６、ＡＴＭ１０１、または紙幣処理部２０３に対して不正なアクセスがされていると見做し、携帯端末１０４に対するデータの送信を中止する。すなわち、携帯端末１０４より送信されたデータ５０７～５１２の全部または一部が同一であるデータに対する連続受信回数や一定期間内の受信回数に上限を設け、その上限を超えた場合に、ストレージ１０７にその旨の記録を行い、管理サーバ１０６の管理者に対して警告を発する。または、不正なアクセスがあった旨の情報をＡＣレスポンスコード（ＡＣ　ＲＳ）７１１及びＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）７１２に含めることも可能である。これにより、レスポンスコードを受信したＡＴＭ制御部（ＡＣ）２０１や、紙幣処理部２０３は、管理サーバ１０６に対する不正のアクセスがあったことを判断することが可能となる。その結果、適切なＡＴＭの運用環境ではない（またはＡＴＭ制御部（ＡＣ）や紙幣処理部が攻撃されていると検知している）と判断して、その後の暗号鍵生成処理を拒絶することが可能となる。

[0098] ＡＣレスポンスコード（ＡＣ　ＲＳ）７１１とＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）７１２とを受信した携帯端末１０４は、これらのレスポンスコードを、データ領域５０６のＡＣレスポンスコード（ＡＣ　ＲＳ）６０１、ＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）６０２として格納する（Ｓ２１３）。その後、データ表示ソフトウェア５０５は、当該６０１及びＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）６０２を、例えばバーコードや２次元コード、あるいは、テキストの形で携帯端末の表示部に表示する（Ｓ２１４）。携帯端末の表示部に表示される、管理サーバのレスポンス受信画面の表示例を図１９に示す。１９０１及び１９０２は、それぞれ、図１３に示すＡＣレスポンスコード（ＡＣ　ＲＳ）７１１及びＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）７１２に対応する。１９０３は、１９０１及び１９０２の情報を格納した２次元コードである。

[0099] 表示されたバーコードや２次元コードは、監視カメラ２０９によって読取られるたり、テキストは保守員により保守用キーボード２１３を介して入力され、その結果を保守用表示部２１２に表示する。保守用表示部２１２に表示される、管理サーバのレスポンス受信画面の表示例を図２０に示す。２００１及び２００２は、それぞれ、図１３に示すＡＣレスポンスコード（ＡＣ　ＲＳ）７１１及びＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）７１２（すなわち、図１９に示す１９０１及び１９０２）に対応する。「２次元コード読み込み」キー２００３は、携帯端末１０４の表示部に表示された２次元コード１９０３を、監視カメラ２０９で読み込むためのキーである。２００４は、ＡＣレスポンスコード（ＡＣ　ＲＳ）を検証するためのキーである。

[0100] 管理サーバから送られてきたレスポンスコード（ＡＣ　ＲＳ、ＤＥＶ　ＲＳ　２）の内、ＡＣレスポンスコード（ＡＣ　ＲＳ）は、ＡＴＭ制御部（ＡＣ）２０１が正当性を検証する。具体的には、「検証」キー２００４への押下が検出されると、暗号鍵インストーラ３０３は、Ｓ２１０で説明した変換アルゴリズムと同一の変換アルゴリズムを用いて、ＡＣレスポンスコード（

ＡＣ　ＲＳ）３２０の妥当性を検証する（Ｓ２１５）。すなわち、データ３１６～３１９が変換アルゴリズムに入力されることにより生成されたＡＣレスポンスコード（ＡＣ　ＲＳ）３２０が、携帯端末１０４より受信されたＡＣレスポンスコード６０１と一致するか否かが検証される。これにより、ＡＴＭ制御部（ＡＣ）２０１は、通信相手が適切な管理サーバ１０６であることを検証すると共に、送信した登録データが管理サーバに確実に保存されたことを確認することが可能となる。

[0101] 一致していない場合、携帯端末１０４による通信不良や、保守員による操作ミスがあったと判断し、保守員に操作ミスの確認を促す。その結果、図１９に示す、携帯端末１０４の管理サーバのレスポンス受信画面のＡＣレスポンスコード（ＡＣ　ＲＳ）１９０１及びＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）１９０２と、図２０に示すＡＴＭの管理サーバのレスポンス受信画面のＡＣレスポンスコード（ＡＣ　ＲＳ）２００１及びＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）２００２と、が一致している場合は、操作ミスではなく通信不良と判断される。そして、データ３１６～３１９、３２１、３２４のデータを管理サーバ１０６に再度送信するべく、Ｓ２０６（またはＳ２０８）以降の処理を再度実行する。

[0102] また、通信不良などにより、ＡＣレスポンスコード（ＡＣ　ＲＳ）６０１が得られない場合は、一時的な暗号鍵生成状態に移行する。すなわち、ＡＣレスポンスコード（ＡＣ　ＲＳ）３２０の妥当性が正しく検証された場合と同様に、その後の処理において、ＡＴＭ制御部（ＡＣ）２０１と、紙幣処理部２０３との間の暗号通信に必要な暗号鍵を生成するモードに移行する。但し、生成された暗号鍵に対して、有効期限を設け、適切なＡＣレスポンスコード（ＡＣ　ＲＳ）６０１が、有効期限内に暗号鍵インストーラ３０３に入力される必要がある。有効期限内に適切なＡＣレスポンスコード（ＡＣ　ＲＳ）６０１が入力されなかった場合は、生成された暗号鍵は無効となり、ＡＴＭ制御部（ＡＣ）２０１と、紙幣処理部２０３との間の暗号通信を禁止するように、暗号鍵インストーラ３０３は設定を変更する。

[0103] Ｓ２１５の処理が終了すると、暗号鍵インストーラ３０３は、所定の変換アルゴリズムを用いて、ＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）３２５から、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３を生成する（Ｓ２１６）。当該変換アルゴリズムは、ＡＴＭ制御部（ＡＣ）２０１と、紙幣処理部２０３との間で共有されている。また、前述した一時的な暗号鍵生成状態に移行しているか否かにより、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３を生成する変換アルゴリズムを変更してもよい。そして、生成されたＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３は、紙幣処理部２０３に送信される（Ｓ２１７）。

[0104] 紙幣処理部２０３では、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３を受信すると、所定の変換アルゴリズムを用いて、内部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６とＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）４０７とから、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８を生成する。そして、受信したＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３と、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８とが一致するか否かを検証する（Ｓ２１８）。

[0105] ここで、所定の変換アルゴリズムとは、（１）ＡＴＭ制御部（ＡＣ）２０１のＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）３２２から、ＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）３２４を生成する変換アルゴリズムと、（２）管理サーバ１０６における、内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）７０８とＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）７１０とからＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）７１２を生成する変換アルゴリズムと、（３）ＡＴＭ制御部（ＡＣ）２０１のＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）３２５からＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３を生成する変換アルゴリズムと、の３つの変換アルゴリズムを結合したアルゴリズムである。

[0106] このように、紙幣処理部２０３の変換アルゴリズムは、ＡＴＭ制御部（ＡＣ）２０１及び管理サーバ１０６と部分的に共有されている。その結果、内

部デバイスシリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）４０６が、ＡＴＭ制御部（ＡＣ）２０１経由で、管理サーバ１０６のストレージ１０７に確実に登録されたかを、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３と、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８との一致を検証することにより、紙幣処理部２０３は確認することが可能となる。この一致検証により、紙幣処理部２０３は、安全なＡＴＭ運用環境であると判断し、その後暗号鍵生成コマンドを受信した場合に暗号鍵生成処理を実行する。

[0107] ここで、紙幣処理部２０３は、安全なＡＴＭ運用環境であると判断した後に、暗号鍵生成コマンドを受信するまでの間に時間の上限を設けることも可能である。時間制限を設けることにより、保守員がＡＴＭを操作中に現場から離れてしまった場合に、第三者が暗号鍵生成コマンドを、紙幣処理部２０３に送信して、不正に暗号鍵を生成されるリスクが回避される。

[0108] ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３と、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８とが一致しない場合は、暗号鍵を生成する適切な環境にないとして、紙幣処理部２０３は、その後、暗号鍵生成コマンドを受信したとしても処理を拒絶する。または、携帯端末１０４の管理サーバのレスポンス受信画面の１９０１及び１９０２と、ＡＴＭの管理サーバのレスポンス受信画面の２００１及び２００２とが一致していることによりネットワーク１０５の通信不良と判断された場合や、保守員による操作ミスがあったと判断された場合において、一定回数以内であれば、Ｓ２０１以降の処理を再度実行する。一定回数を超えた場合、紙幣処理部２０３に対して不正なアクセスがされていると見做し、一定期間Ｓ２０１以降の処理の再実行を拒絶する。

[0109] ＡＴＭ制御部（ＡＣ）２０１が一時的な暗号鍵生成状態の場合、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３は、その状態に応じた変換アルゴリズムで生成されているため、紙幣処理部２０３は、その変換アルゴリズムを用いてＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８を生成する。そして、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）３２３と一

致するか検証し、一致すれば、一時的な暗号鍵生成状態と判断して、その後、暗号鍵生成コマンド受信した場合は暗号鍵を生成する。

[0110] 管理サーバ１０６に対する不正なアクセスが検知されている場合、ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）４０８に、当該情報が含まれているため、紙幣処理部２０３が当該情報の有無を検証することにより、管理サーバ１０６に対する不正なアクセスを確認することが可能となる。その場合、紙幣処理部２０３が適切なＡＴＭの運用環境でない（またはＡＴＭ制御部（ＡＣ）や紙幣処理部が攻撃されていると検知している）と判断して、その後に暗号鍵生成コマンドを受信した場合でも暗号鍵生成処理を、無期限、あるいは、一定期間拒絶する。

[0111] 本実施例は、暗号鍵が一切設定されていない自動取引装置に対して暗号鍵を新規に設定する場合において、紙幣処理部２０３の通信相手である管理サーバ（図９（ｂ）に示す管理サーバ）と、ＡＴＭ制御部（ＡＣ）２０１の通信相手である管理サーバ（図９（ｃ）に示す管理サーバ）とが同一の管理サーバであることを前提として説明したが、異なる管理サーバとしても良い。この場合、ＡＴＭ制御部（ＡＣ）２０１を経由して、紙幣処理部２０３が、図９（ｂ）に示す管理サーバ（すなわち、紙幣処理部２０３に接続された管理サーバ）に情報を送信する処理となる。

[0112] なお、本実施例では、ＡＴＭ外部の管理サーバと通信を行うことを前提として説明したが、管理サーバの代わりにＡＴＭ内部の暗号化キーパッドを用いてもよい。暗号化キーパッドは、ホストコンピュータ１０３と通信を行う機能があるため、暗号化キーパッドとホストとの通信の有無により、当該ＡＴＭが運用中のＡＴＭであるか否かを判断してもよい。

[0113] また、本実施例では、保守モードにおいて、ＡＴＭ１０１とホストコンピュータ１０３との接続は切断されていることが一般的であると説明したが、ＡＴＭ１０１とホストコンピュータ１０３とが接続されていても良い。

[0114] また、本実施例では、携帯端末１０４を備えた自動取引システムＳ２について説明したが、図２１に示すように、ＡＴＭ１０１と管理サーバ１０６と

が、いずれも保守用ネットワーク１０５に接続された自動取引システムＳ３としても良い。このとき、図２２に示すように、管理サーバへの認証画面に、管理サーバへのアクセスキー１７０９を追加しても良い。このような画面にすることにより、携帯端末を備えていなくても、ＡＴＭ１０１と管理サーバ１０６との間で情報の送受信を実行することが可能となる。

符号の説明

[0115] １０１：自動取引装置、１０２：金融取引ネットワーク、１０３：ホストコンピュータ、１０４：携帯情報端末、１０５：保守用ネットワーク、１０６：管理サーバ、１０７：ストレージ、２０１：ＡＴＭ制御部（ＡＣ）、２０３：内部デバイス（ＤＥＶ）としての紙幣処理部、３１８、５０７、７０５：時刻データ、３１６、５０８、７０６：保守員ＩＤ、３１７、５０９、７０７：ＡＴＭシリアルナンバー（ＡＴＭ　Ｓｅｒ．Ｎｏ．）、３１９、５１１、７０９：ＡＣチャレンジコード（ＡＣ　ＣＨ）、３２０、６０１、７１１：ＡＣレスポンスコード（ＡＣ　ＲＳ）、３２１、４０６、５１０、７０８：内部デバイス（ＤＥＶ）シリアルナンバー（ＤＥＶ　Ｓｅｒ．Ｎｏ．）、３２２、４０７：ＤＥＶチャレンジコード１（ＤＥＶ　ＣＨ　１）、３２３、４０８：ＤＥＶレスポンスコード１（ＤＥＶ　ＲＳ　１）、３２４、５１２、７１０：ＤＥＶチャレンジコード２（ＤＥＶ　ＣＨ　２）、３２５、６０２、７１２：ＤＥＶレスポンスコード２（ＤＥＶ　ＲＳ　２）

請求の範囲

[請求項1] 内部に搭載される第１のデバイスと、装置を制御する制御部とを備え、該第１のデバイスと該制御部との間でデータの送受信を行う自動取引装置であって、

前記第１のデバイスは、

該第１のデバイスに関する第１のコードを生成する処理と、

前記第１のコードと、前記制御部から受信した第２のコードとを検証し、検証結果に応じて暗号鍵を生成する処理と、を実行し、

前記制御部は、

前記第１のコードを受信した後、動作環境が前記自動取引装置内であることを検証する処理と、

前記動作環境が前記自動取引装置内であると判断された場合、前記第２のコードを生成し、該第２のコードを前記第１のデバイスに送信する処理と、を実行することを特徴とする、自動取引装置。

[請求項2] 請求項１に記載の自動取引装置であって、

前記制御部は、前記第１のコードから前記第２のコードを生成する処理を実行する、自動取引装置。

[請求項3] 請求項１に記載の自動取引装置であって、

前記制御部は、

前記第１のコードから第３のコードを生成し、該制御部に関する第４のコードを生成し、該第３のコードと該第４のコードとを出力する処理と、

サーバにおいて前記第４のコードから生成された、第５のコードを検証し、検証結果に応じて、前記サーバにおいて前記第３のコードから生成された前記第６のコードから、前記第２のコードを生成する処理と、を実行する、自動取引装置。

[請求項4] 請求項１に記載された自動取引装置であって、

前記第１のデバイスは、紙幣を取り扱う紙幣処理部、硬貨を取り扱

う硬貨処理部、カードの情報を読取るカードリーダ部、暗号化を行う暗号化キーパッド、明細票を印字するレシートプリンタ、通帳の読み取りと記帳を行う通帳プリンタ、取引のログを記録するジャーナルプリンタ、または利用者の顔写真を撮影するカメラのいずれかである、自動取引装置。

[請求項5] 請求項１に記載された自動取引装置であって、

前記第１のデバイスとは異なる、内部に搭載される第２のデバイスを備え、

前記動作環境が前記自動取引装置内であることを検証する処理は、前記制御部に前記第２のデバイスが接続されているか否かの判断を実行する処理を含む、自動取引装置。

[請求項6] 請求項５に記載された自動取引装置であって、

前記第１のデバイス及び第２のデバイスは、Ｉ／Ｏ制御部、紙幣を取り扱う紙幣処理部、硬貨を取り扱う硬貨処理部、カードの情報を読取るカードリーダ部、暗号化を行う暗号化キーパッド、明細票を印字するレシートプリンタ、通帳の読み取りと記帳を行う通帳プリンタ、取引のログを記録するジャーナルプリンタ、または利用者の顔写真を撮影するカメラのいずれかである、自動取引装置。

[請求項7] 請求項１に記載された自動取引装置であって、

前記動作環境が前記自動取引装置内でないと判断された場合、

前記制御部は、前記動作環境が前記自動取引装置内でない旨を示すデータを送信し、 前記第１のデバイスは、前記動作環境が前記自動取引装置内でない旨を示すデータの受信回数に応じて、暗号鍵生成処理を中断する、自動取引装置。

[請求項8] 請求項１に記載された自動取引装置であって、

前記第１のデバイスは、該第１のデバイスに固有の情報を前記制御部に送信する処理を実行し、

前記制御部は、前記第１のコードを生成する処理を実行するときに

、前記第１のデバイスに固有の情報を用いる、自動取引装置。

[請求項9] 請求項８に記載された自動取引装置であって、

前記第１のデバイスは、前記制御部から受信した第２のコードを検証する処理において、

該受信した第２のコードと、前記第１のデバイスにおいて、前記第１のコードと前記第１のデバイスに固有の情報とから生成した第２のコードとを比較する処理を実行する、自動取引装置。

[請求項10] 内部に搭載される第１のデバイスと、装置を制御する制御部とを備え、該第１のデバイスと該制御部との間でデータの送受信を行う自動取引装置であって、

前記制御部は、

動作環境が前記自動取引装置内であることを検証する処理と、

前記動作環境が前記自動取引装置内であると判断された場合、前記第１のコードを生成し、前記第１のデバイスに送信する処理と、

前記第１のコードと、前記第２のコードを検証する処理と、

前記第２のコードの検証結果に応じて暗号鍵を生成する処理と、を実行し、

前記第１のデバイスは、

前記第１のチャレンジ第２のコードを生成する処理と、

前記第２のコードから前記第２のコードを生成し、該第２のコードを、前記制御部に送信する処理と、を実行する、

ことを特徴とする、自動取引装置。

[請求項11] 内部に搭載される第１のデバイスと、装置を制御する制御部と、保守に関する情報を表示する表示部とを備え、該第１のデバイスと該制御部との間でデータの送受信を行う自動取引装置であって、

前記制御部において動作環境が前記自動取引装置内であると判断された場合、前記表示部は、前記制御部において、前記第１のデバイスに関するコードより生成される第１のコードと、前記制御部に関する

第２のコードと、を表示する、

ことを特徴とする自動取引装置。

[請求項12] 請求項１１に記載された自動取引装置であって、

前記表示部は、

前記サーバにおいて生成され、前記制御部で検証される第３のコードと、

前記サーバにおいて生成され、前記制御部において前記第３のコードを検証した結果、に応じて、前記第２のコードを生成する際に用いられる第４のコードと、を表示する、自動取引装置。

[請求項13] 内部に搭載される第１のデバイスと、装置を制御する制御部と、保守に関する情報を表示する表示部とを備え、該第１のデバイスと該制御部との間でデータの送受信を行う自動取引装置と、携帯端末と、サーバとを備える自動取引システムであって、

前記第１のデバイスは、

該第１のデバイスに関する第１のコードを生成し、前記制御部に送信する処理と、

前記制御部から受信した第２のコードを検証し、検証結果に応じて暗号鍵を生成する処理と、を実行し、

前記制御部は、

前記第１のコードを受信した後、動作環境が前記自動取引装置内であることを検証する処理と、

前記動作環境が前記自動取引装置内であると判断された場合、前記第１のコードから第３のコードを生成し、該制御部に関する第４のコードを生成し、該第３のコード及び該第４のコードに関する情報を前記表示部に表示する処理と、

前記携帯端末に表示された、第５のコード及び第６のコードに関する情報を読み取る処理と、

前記第５のコードを検証し、検証結果に応じて、前記第６のコー

ドから前記第２のコードを生成し、該第２のコードを前記第１のデバイスに送信する処理と、を実行し、

前記携帯端末は、

前記表示部に表示された前記第３のコード及び前記第４のコードに関する情報を読み取り、送信する処理と、

前記サーバから送信された前記第５のコード及び前記第６のコードを受信する処理と、

前記第５のコード及び前記第６のコードに関する情報を表示する処理と、を実行し、　前記サーバは、

前記第３のコードから前記第６のコードを生成する処理と、

前記第４のコードから前記第５のコードを生成する処理と、を実行する

ことを特徴とする自動取引システム。

[請求項14] 請求項１３に記載された自動取引システムであって、

前記制御部は、

前記第３のコード及び前記第４のコードに関する情報と共に、該情報を送信する時刻を表すデータ、作業者の識別情報、前記自動取引装置の識別情報又は前記第１のデバイスの識別情報を表示する処理を実行し、

前記携帯端末は、

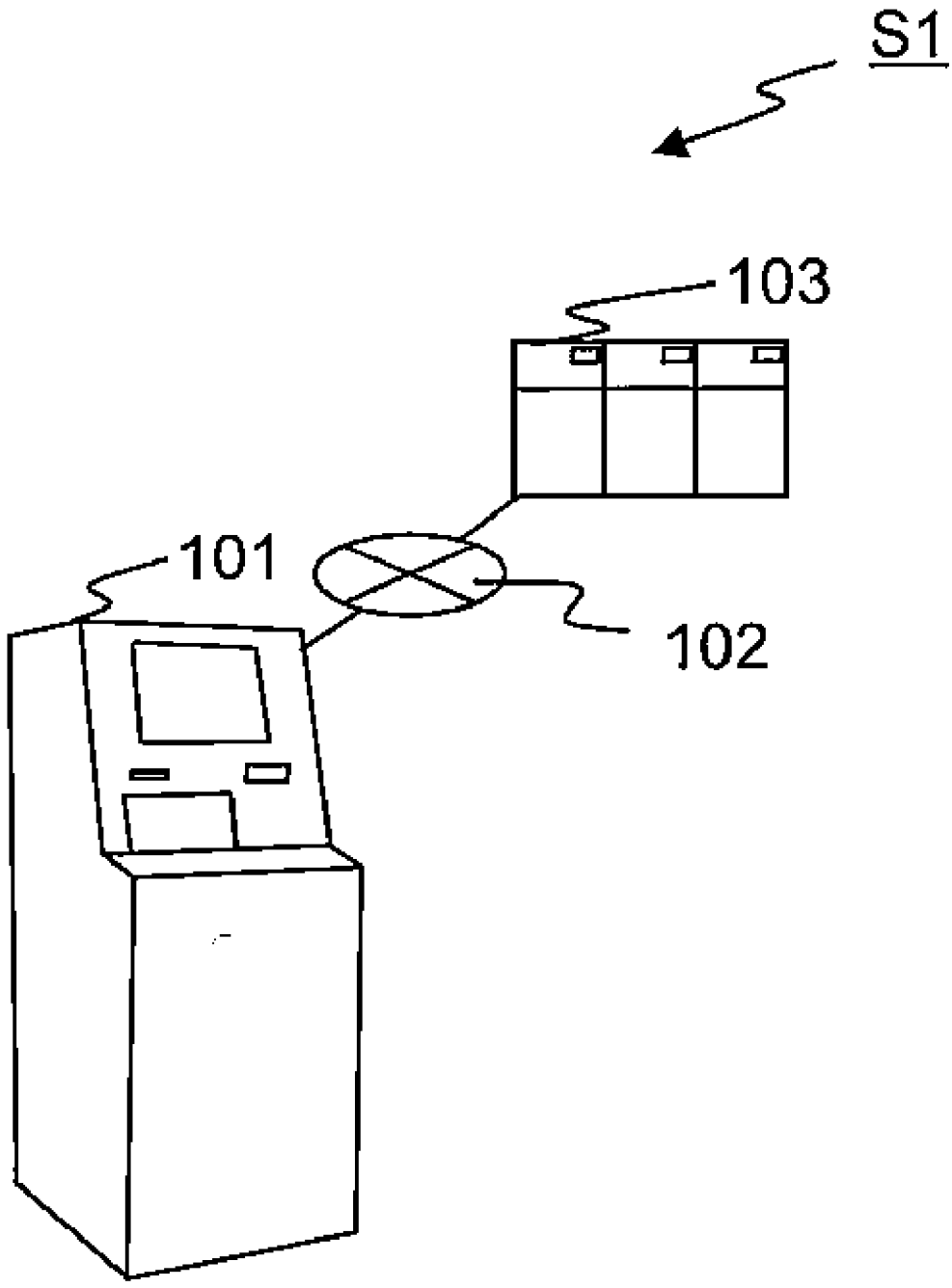
前記表示部に表示された、情報を送信する時刻を表すデータ、作業者の識別情報、前記自動取引装置の識別情報又は前記第１のデバイスの識別情報を読み取り、送信する処理を実行し、

前記サーバは、

前記第３のコード及び前記第４のコードに関する情報と、情報を送信する時刻を表すデータ、作業者の識別情報、前記自動取引装置の識別情報又は前記第１のデバイスの識別情報とを格納部に格納する処理を実行する自動取引システム。

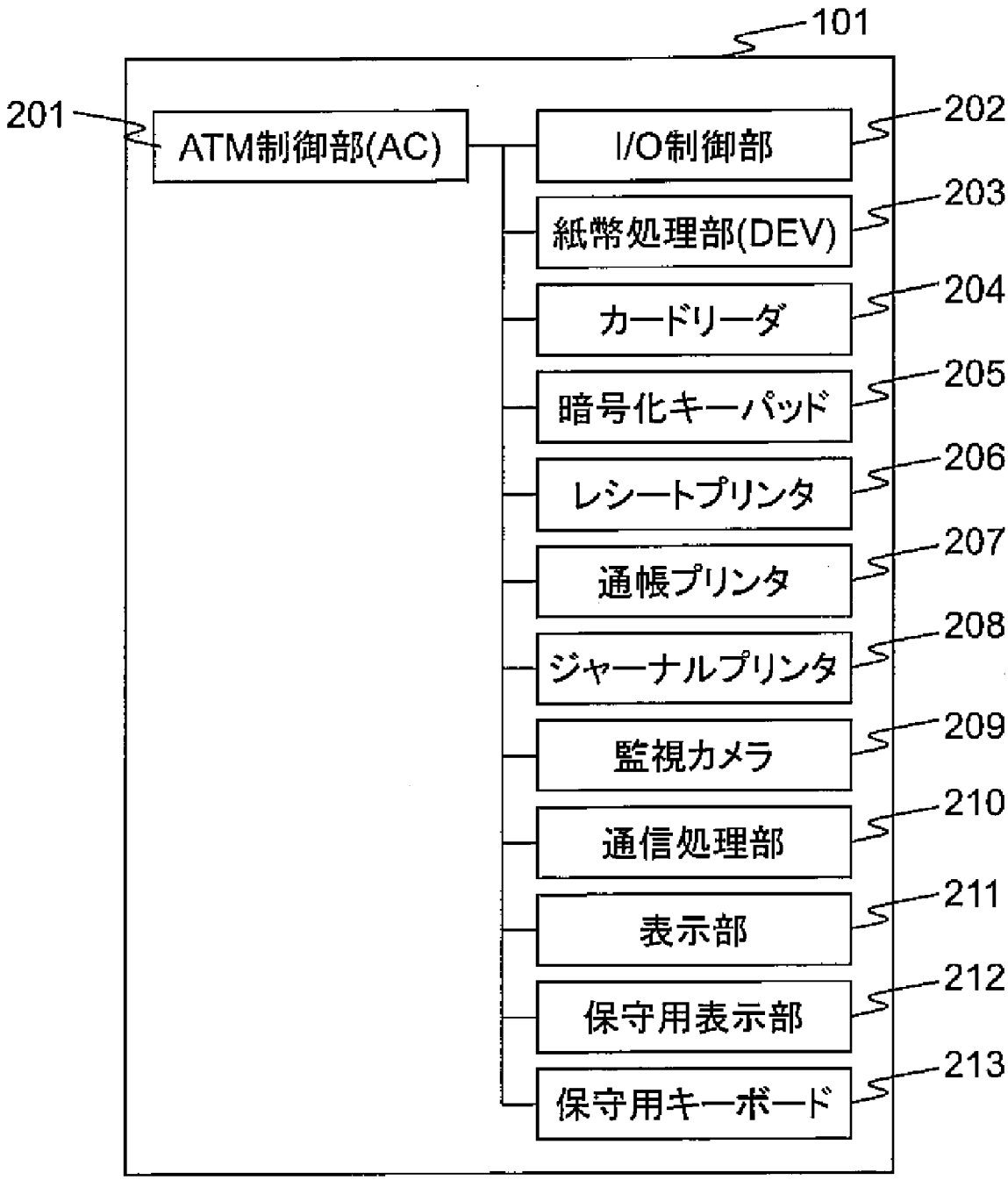
[図1]

図1



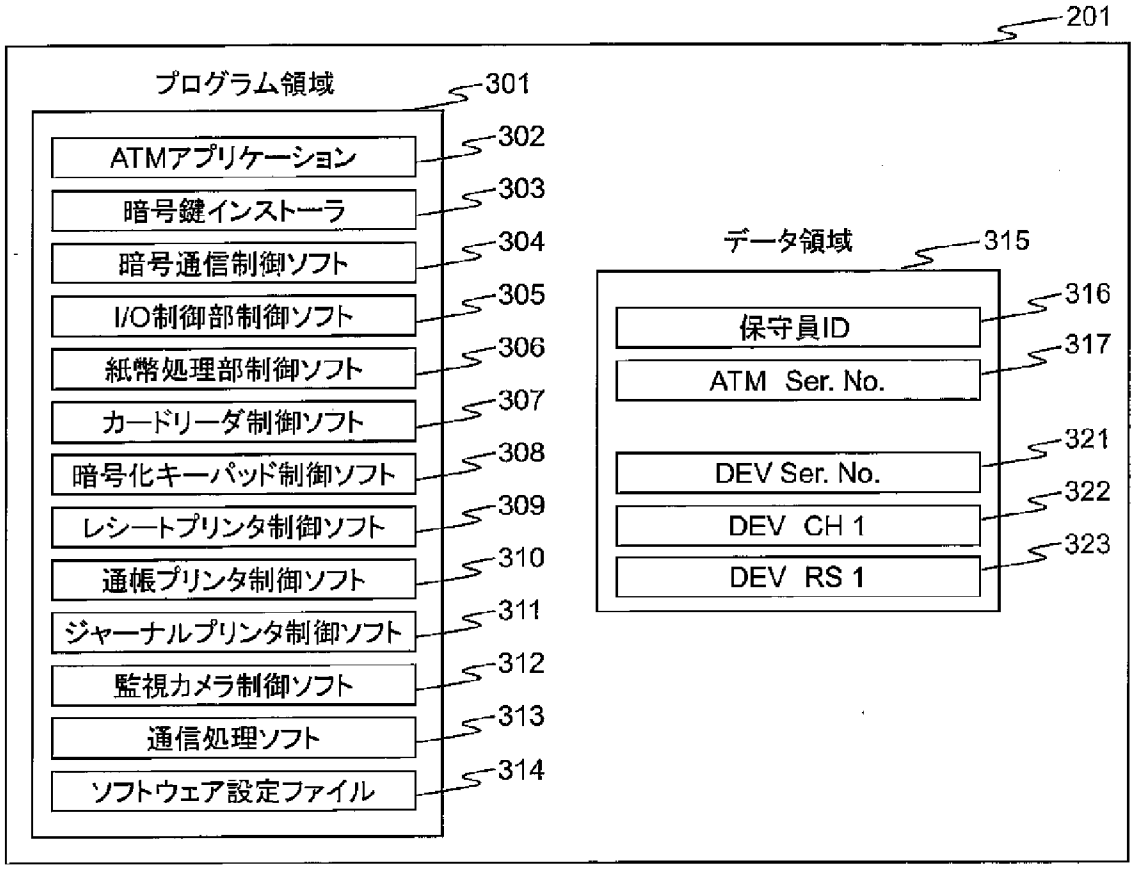
[図2]

図2


101
201
ATM制御部(AC)
I/O制御部
202
紙幣処理部(DEV)
203
カードリーダ
204
暗号化キーパッド
205
レシートプリンタ
206
通帳プリンタ
207
ジャーナルプリンタ
208
監視カメラ
209
通信処理部
210
表示部
211
保守用表示部
212
保守用キーボード
213

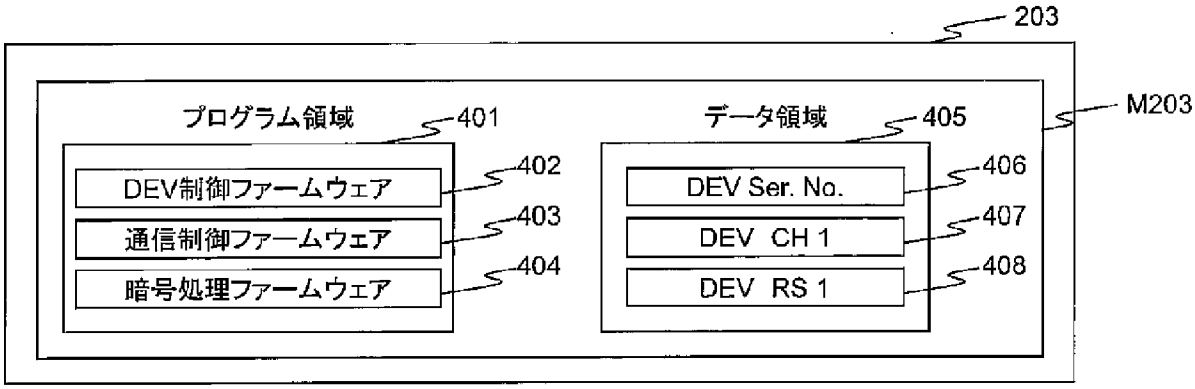
[図3]

図3


201
プログラム領域
301
ATMアプリケーション
302
暗号鍵インストーラ
303
暗号通信制御ソフト
304
I/O制御部制御ソフト
305
紙幣処理部制御ソフト
306
カードリーダ制御ソフト
307
暗号化キーパッド制御ソフト
308
レシートプリンタ制御ソフト
309
通帳プリンタ制御ソフト
310
ジャーナルプリンタ制御ソフト
311
監視カメラ制御ソフト
312
通信処理ソフト
313
ソフトウェア設定ファイル
314
データ領域
315
保守員ID
316
ATM Ser. No.
317
DEV Ser. No.
321
DEV CH 1
322
DEV RS 1
323

[図4]

図4


203
M203
プログラム領域
401
DEV制御ファームウェア
402
通信制御ファームウェア
403
暗号処理ファームウェア
404
データ領域
405
DEV Ser. No.
406
DEV CH 1
407
DEV RS 1
408

[図5]

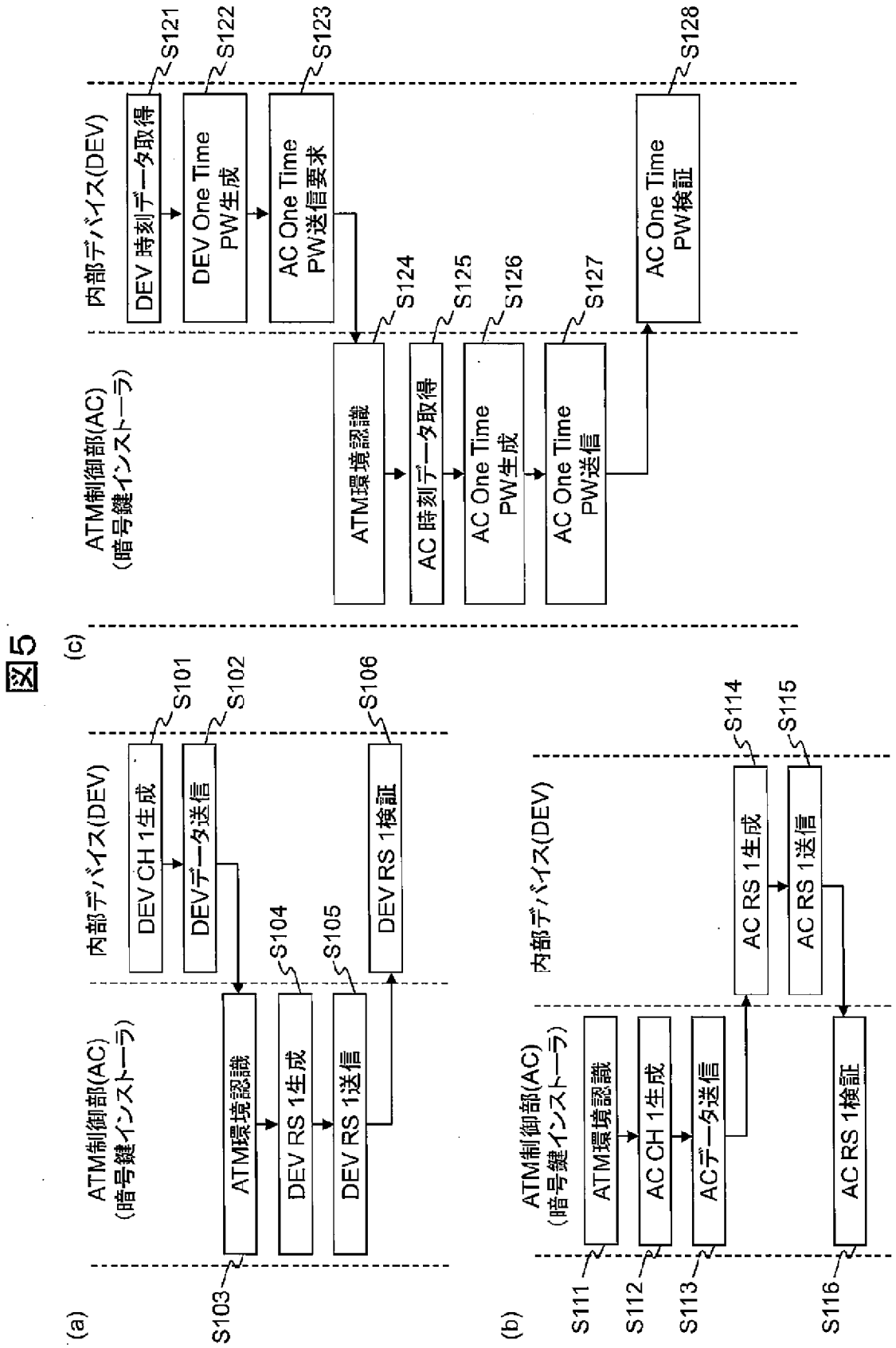
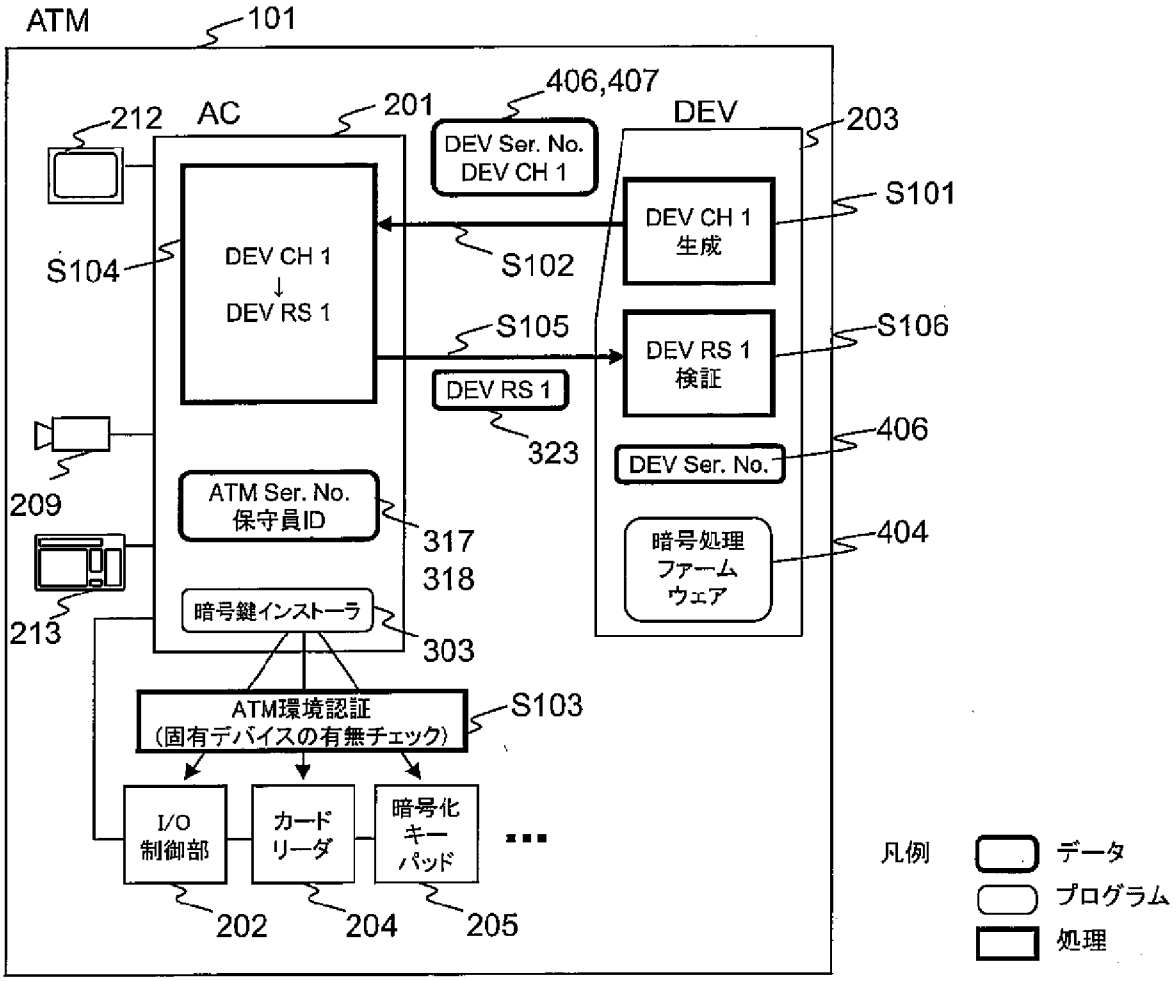


図5
(a)
ATM制御部(AC)
(暗号鍵インストーラ)
内部デバイス(DEV)
DEV CH 1生成
DEVデータ送信
ATM環境認識
DEV RS 1生成
DEV RS 1送信
DEV RS 1検証
S101
S102
S103
S104
S105
S106
(b)
ATM制御部(AC)
(暗号鍵インストーラ)
内部デバイス(DEV)
ATM環境認識
AC CH 1生成
ACデータ送信
AC RS 1生成
AC RS 1送信
AC RS 1検証
S111
S112
S113
S114
S115
S116
(c)
ATM制御部(AC)
(暗号鍵インストーラ)
内部デバイス(DEV)
DEV 時刻データ取得
DEV One Time PW生成
AC One Time PW送信要求
ATM環境認識
AC 時刻データ取得
AC One Time PW生成
AC One Time PW送信
AC One Time PW検証
S121
S122
S123
S124
S125
S126
S127
S128

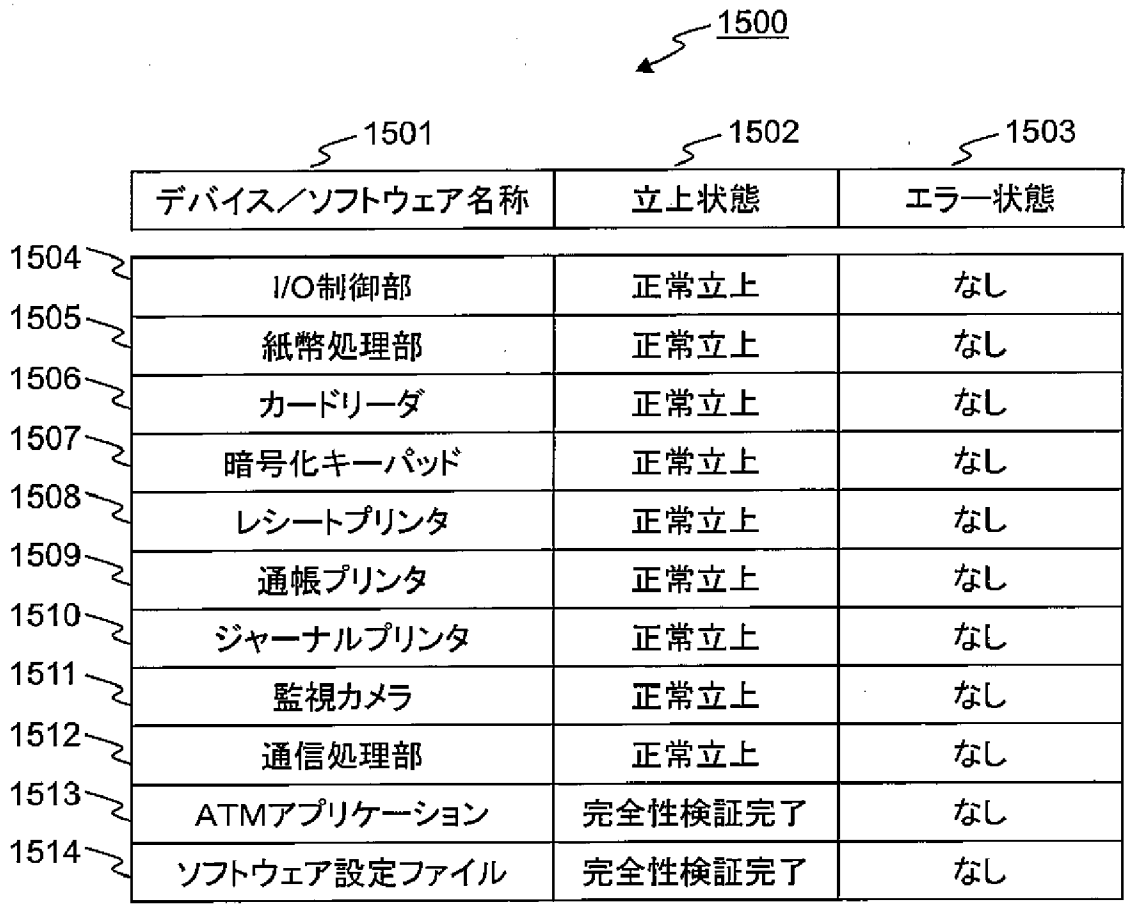
[図6]

図6


ATM
101
212
AC
201
406,407
DEV
203
DEV Ser. No.
DEV CH 1
DEV CH 1
生成
S101
S104
DEV CH 1
↓
DEV RS 1
S102
S105
DEV RS 1
検証
S106
DEV RS 1
323
406
DEV Ser. No.
209
ATM Ser. No.
保守員ID
317
318
暗号処理
ファーム
ウェア
404
213
暗号鍵インストーラ
303
ATM環境認証
(固有デバイスの有無チェック)
S103
I/O
制御部
カード
リーダ
暗号化
キー
パッド
202
204
205
凡例
データ
プログラム
処理

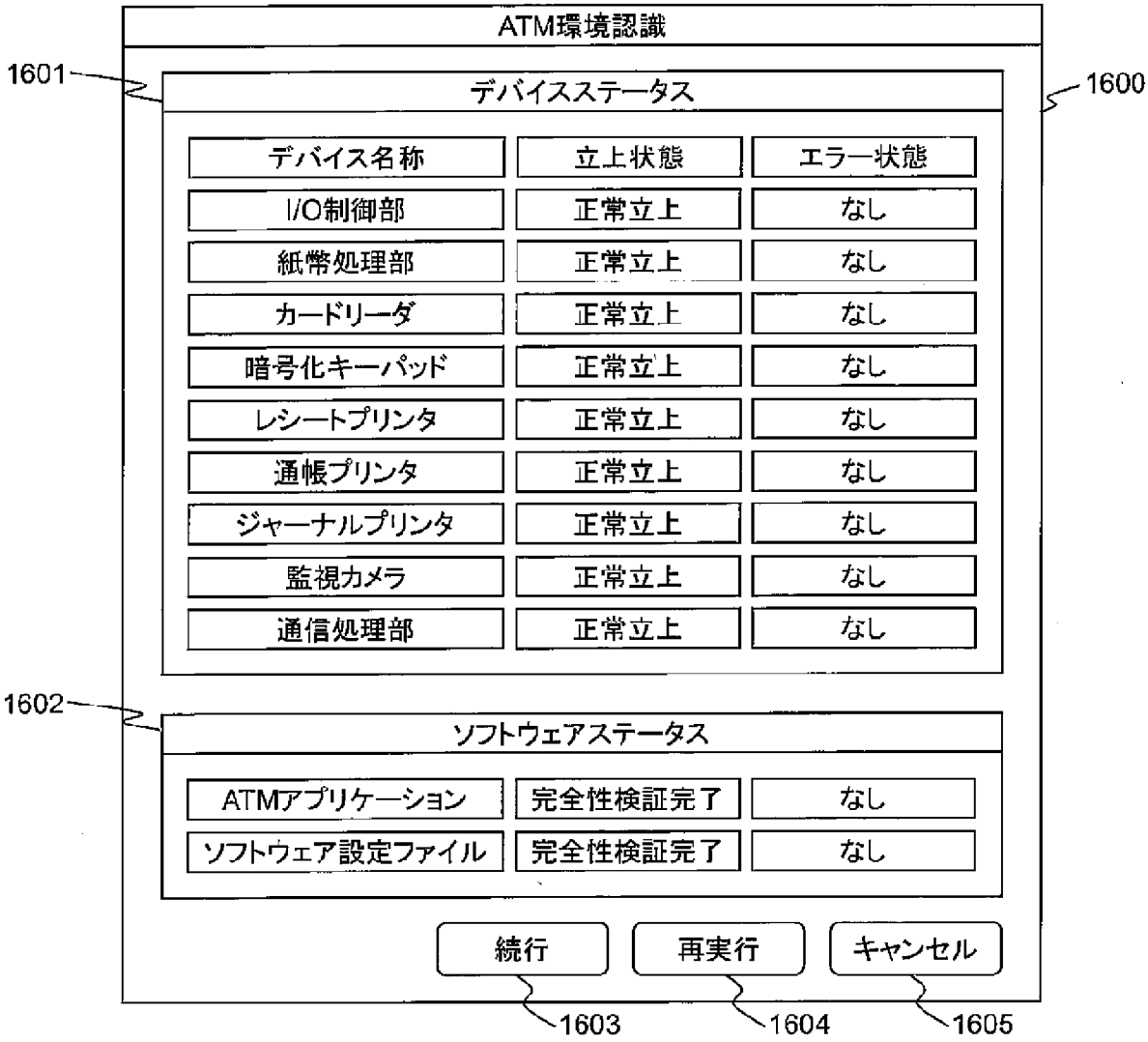
[図7]

図7


1500
1501
1502
1503
デバイス／ソフトウェア名称
立上状態
エラー状態
1504
I/O制御部
正常立上
なし
1505
紙幣処理部
正常立上
なし
1506
カードリーダ
正常立上
なし
1507
暗号化キーパッド
正常立上
なし
1508
レシートプリンタ
正常立上
なし
1509
通帳プリンタ
正常立上
なし
1510
ジャーナルプリンタ
正常立上
なし
1511
監視カメラ
正常立上
なし
1512
通信処理部
正常立上
なし
1513
ATMアプリケーション
完全性検証完了
なし
1514
ソフトウェア設定ファイル
完全性検証完了
なし

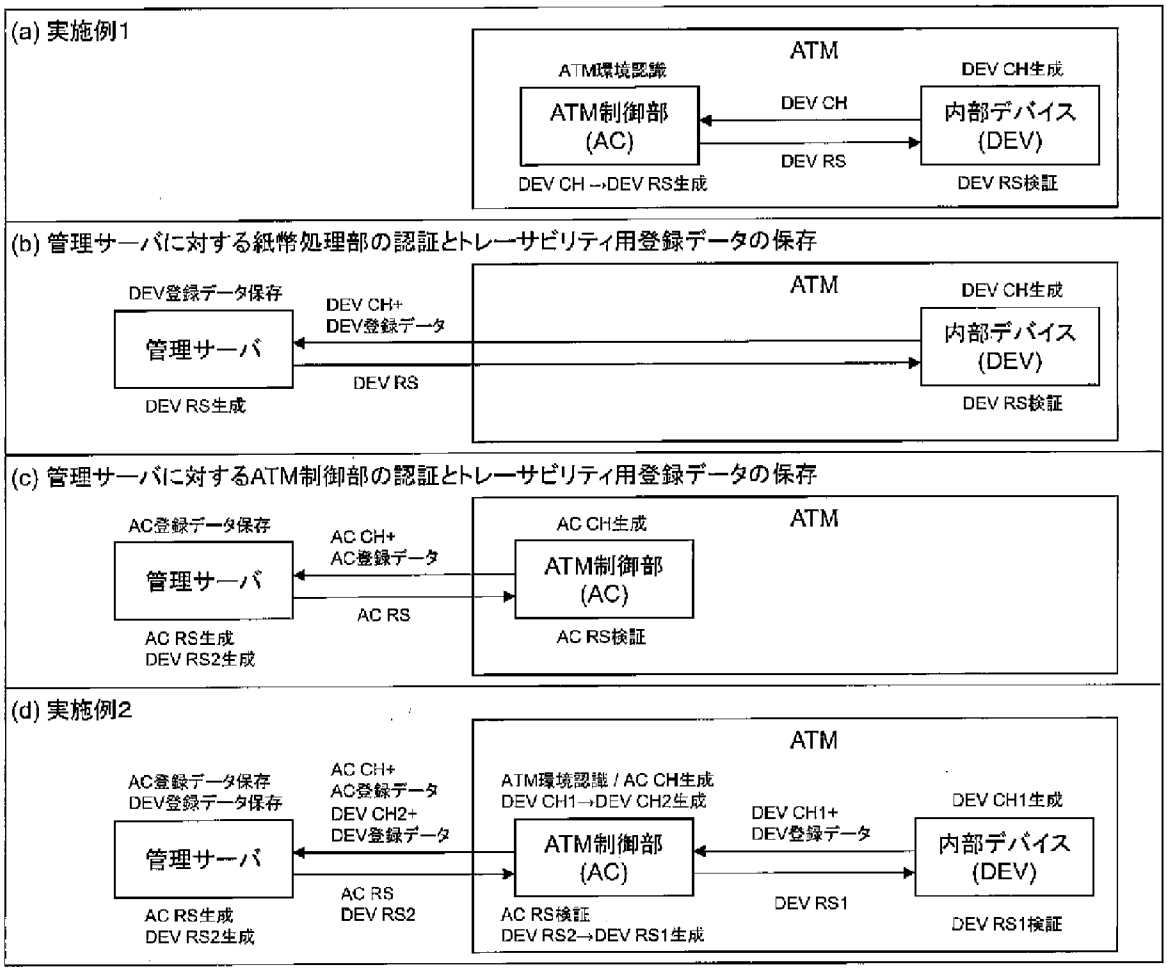
[図8]

図8


ATM環境認識
1601
デバイスステータス
1600
デバイス名称
立上状態
エラー状態
I/O制御部
正常立上
なし
紙幣処理部
正常立上
なし
カードリーダ
正常立上
なし
暗号化キーパッド
正常立上
なし
レシートプリンタ
正常立上
なし
通帳プリンタ
正常立上
なし
ジャーナルプリンタ
正常立上
なし
監視カメラ
正常立上
なし
通信処理部
正常立上
なし
1602
ソフトウェアステータス
ATMアプリケーション
完全性検証完了
なし
ソフトウェア設定ファイル
完全性検証完了
なし
続行
再実行
キャンセル
1603
1604
1605

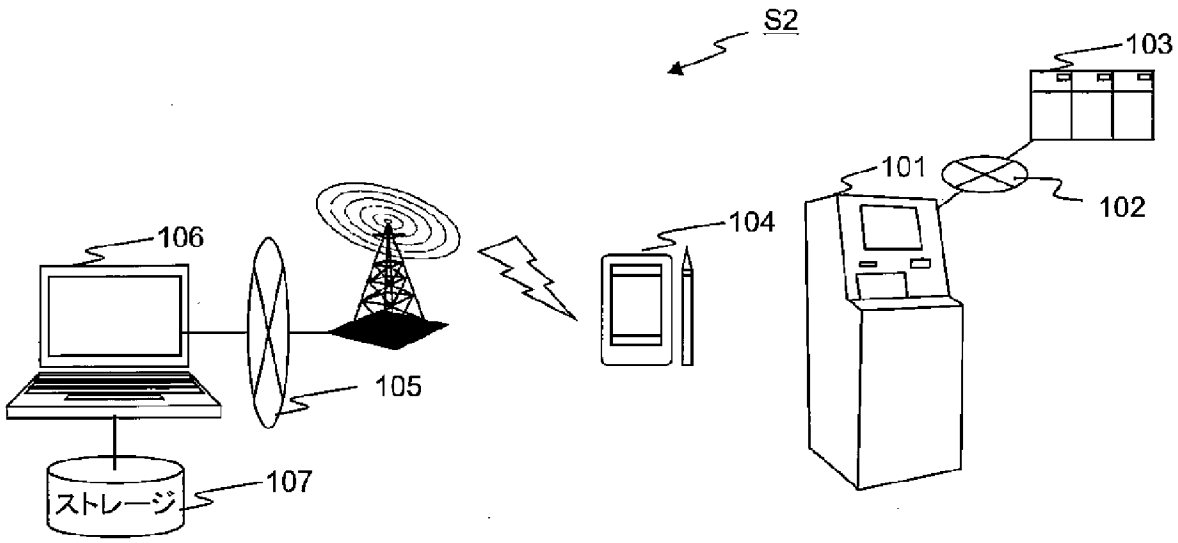
[図9]

図9


(a) 実施例1
ATM
ATM環境認識
DEV CH生成
ATM制御部
(AC)
DEV CH
内部デバイス
(DEV)
DEV RS
DEV CH→DEV RS生成
DEV RS検証
(b) 管理サーバに対する紙幣処理部の認証とトレーサビリティ用登録データの保存
DEV登録データ保存
DEV CH+
DEV登録データ
管理サーバ
DEV RS
DEV RS生成
ATM
DEV CH生成
内部デバイス
(DEV)
DEV RS検証
(c) 管理サーバに対するATM制御部の認証とトレーサビリティ用登録データの保存
AC登録データ保存
AC CH+
AC登録データ
管理サーバ
AC RS
AC RS生成
DEV RS2生成
AC CH生成
ATM
ATM制御部
(AC)
AC RS検証
(d) 実施例2
ATM
AC登録データ保存
DEV登録データ保存
AC CH+
AC登録データ
DEV CH2+
DEV登録データ
管理サーバ
AC RS
DEV RS2
AC RS生成
DEV RS2生成
ATM環境認識 / AC CH生成
DEV CH1→DEV CH2生成
DEV CH1+
DEV登録データ
ATM制御部
(AC)
DEV RS1
AC RS検証
DEV RS2→DEV RS1生成
DEV CH1生成
内部デバイス
(DEV)
DEV RS1検証

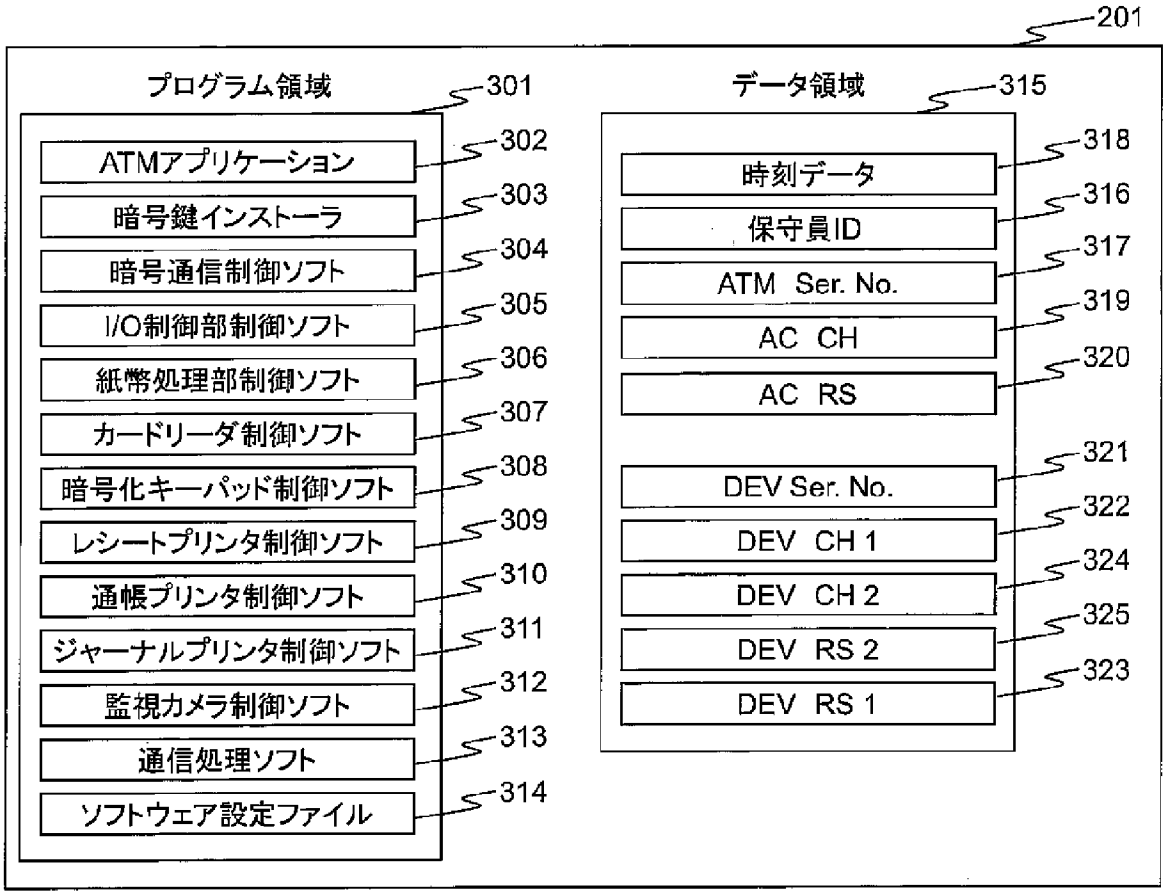
[図10]

図10


S2
103
101
102
104
106
105
ストレージ
107

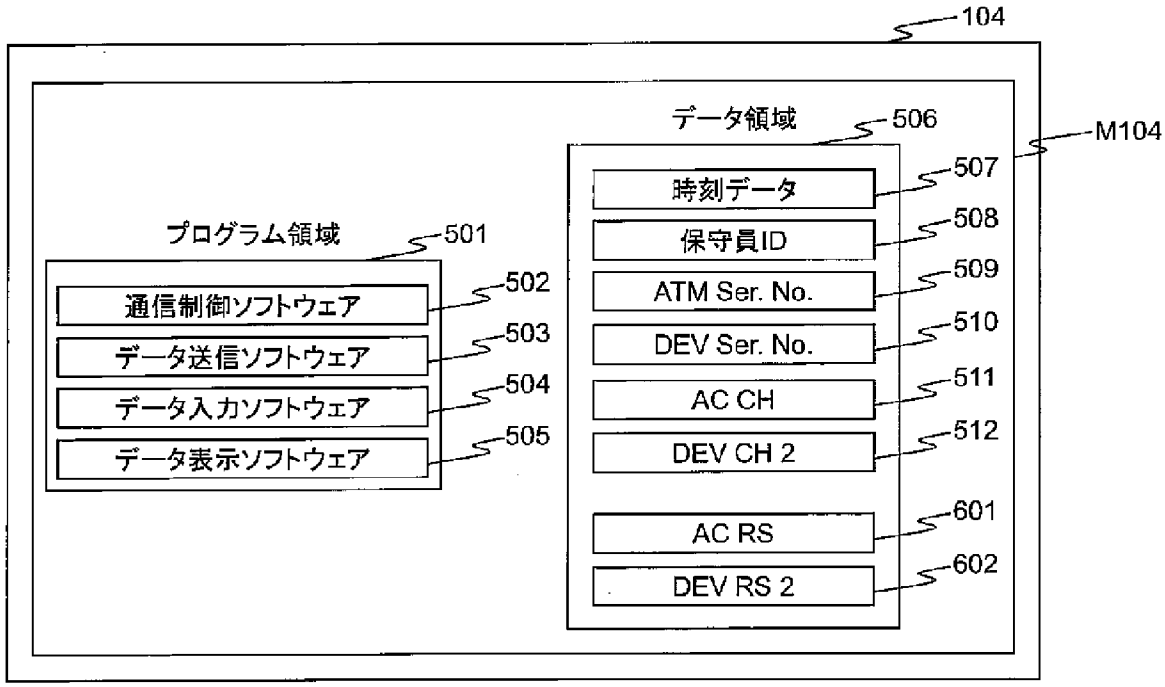
[図11]

図11



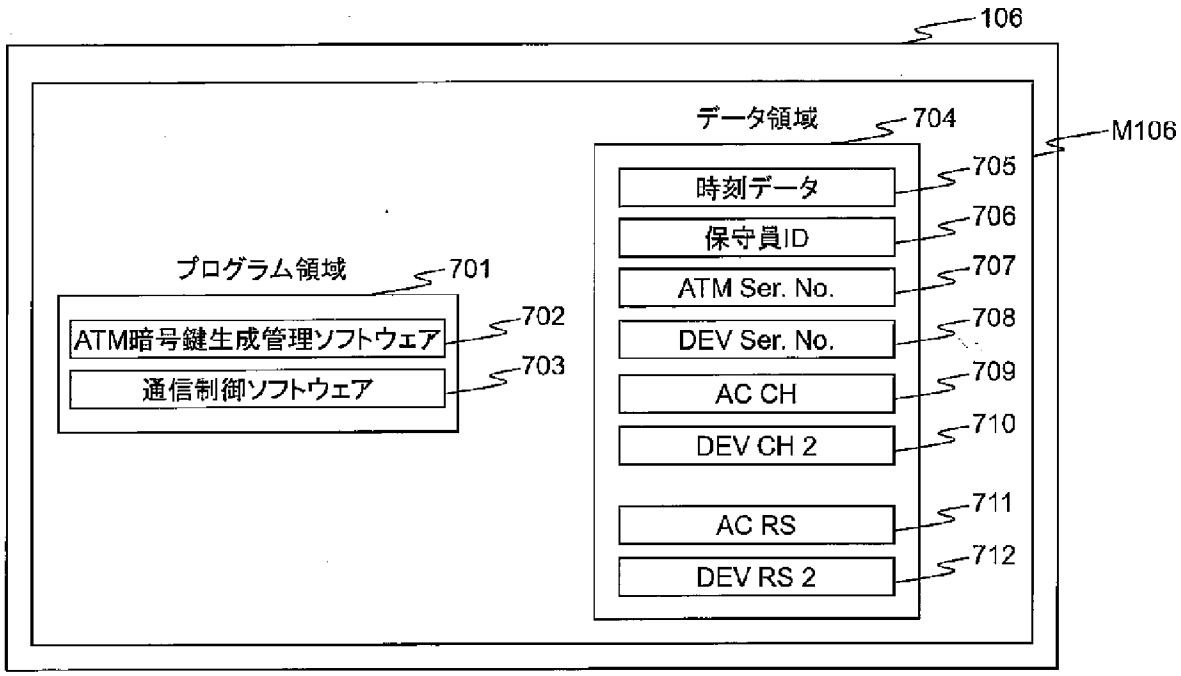
[図12]

図12



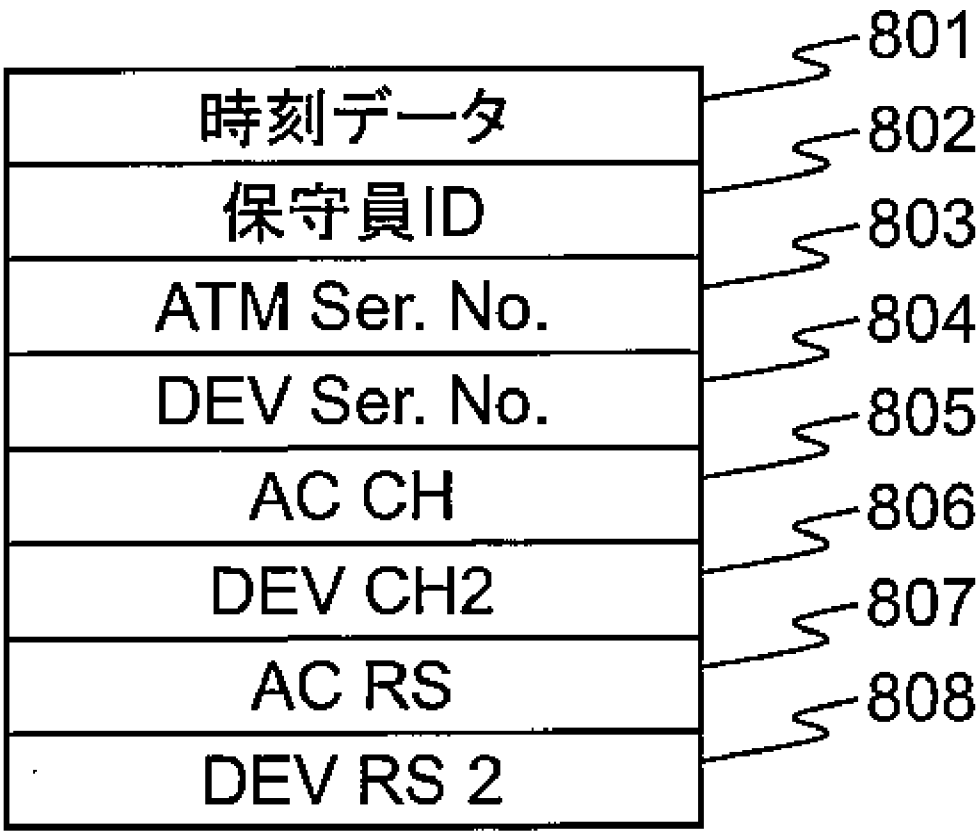
[図13]

図13


106
M106
データ領域
704
時刻データ
705
保守員ID
706
ATM Ser. No.
707
DEV Ser. No.
708
AC CH
709
DEV CH 2
710
AC RS
711
DEV RS 2
712
プログラム領域
701
ATM暗号鍵生成管理ソフトウェア
702
通信制御ソフトウェア
703

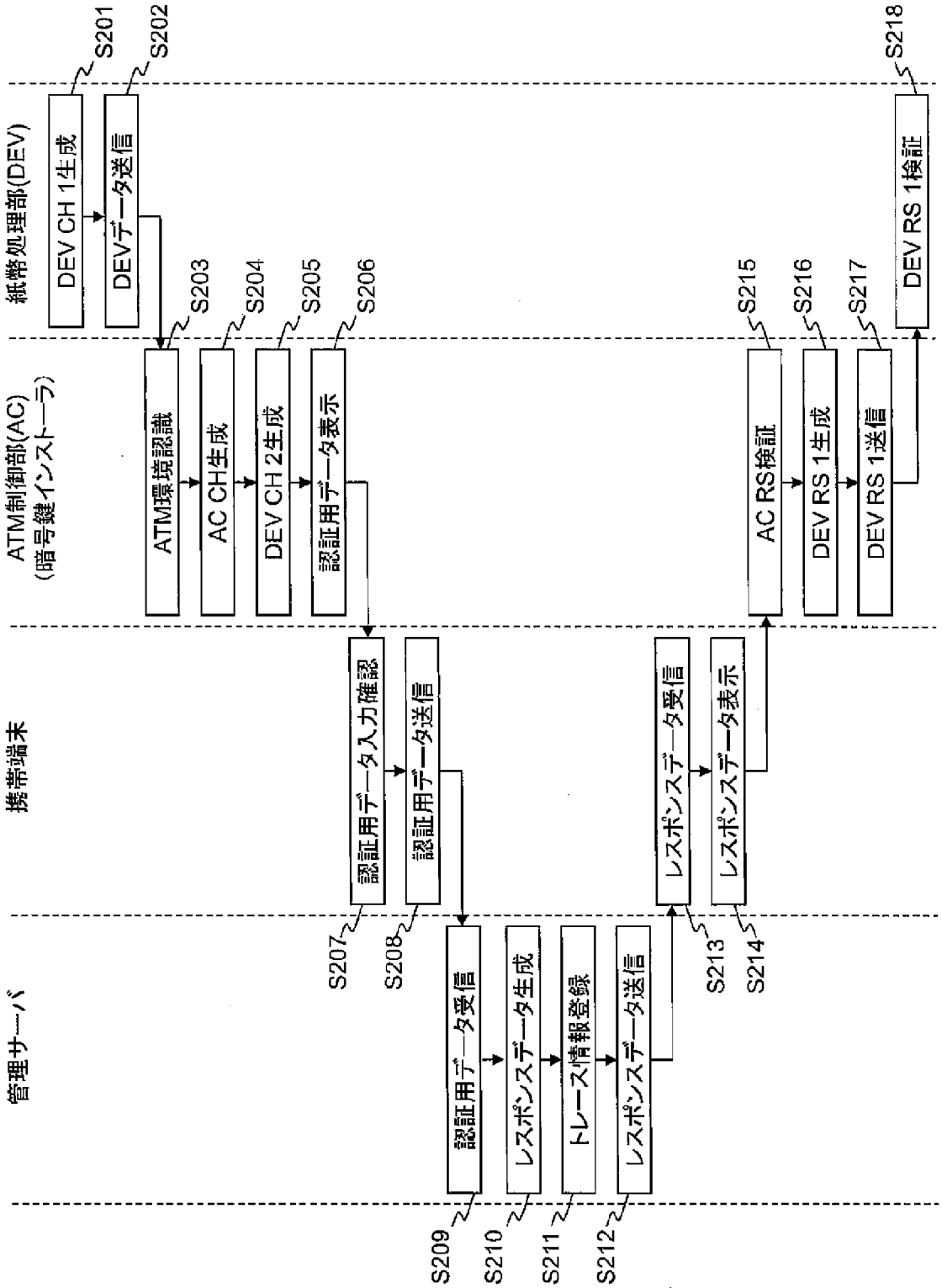
[図14]

図14


時刻データ
保守員ID
ATM Ser. No.
DEV Ser. No.
AC CH
DEV CH2
AC RS
DEV RS 2
801
802
803
804
805
806
807
808

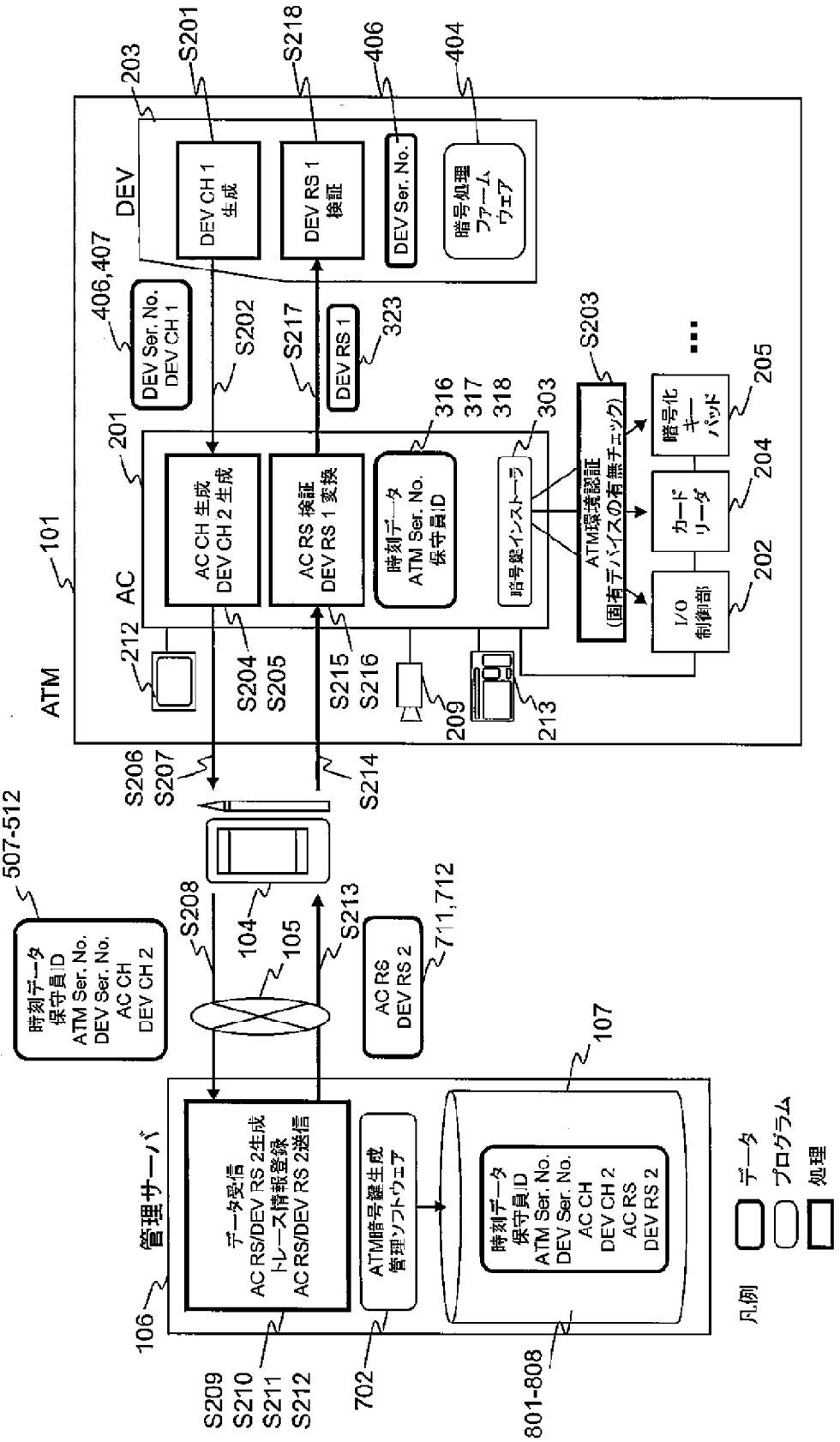
[図15]

図15


紙幣処理部(DEV)
ATM制御部(AC)
(暗号鍵インストーラ)
携帯端末
管理サーバ
DEV CH 1生成
DEVデータ送信
ATM環境認識
AC CH生成
DEV CH 2生成
認証用データ表示
認証用データ入力確認
認証用データ送信
認証用データ受信
レスポンスデータ生成
トレース情報登録
レスポンスデータ送信
レスポンスデータ受信
レスポンスデータ表示
AC RS検証
DEV RS 1生成
DEV RS 1送信
DEV RS 1検証
S201
S202
S203
S204
S205
S206
S207
S208
S209
S210
S211
S212
S213
S214
S215
S216
S217
S218

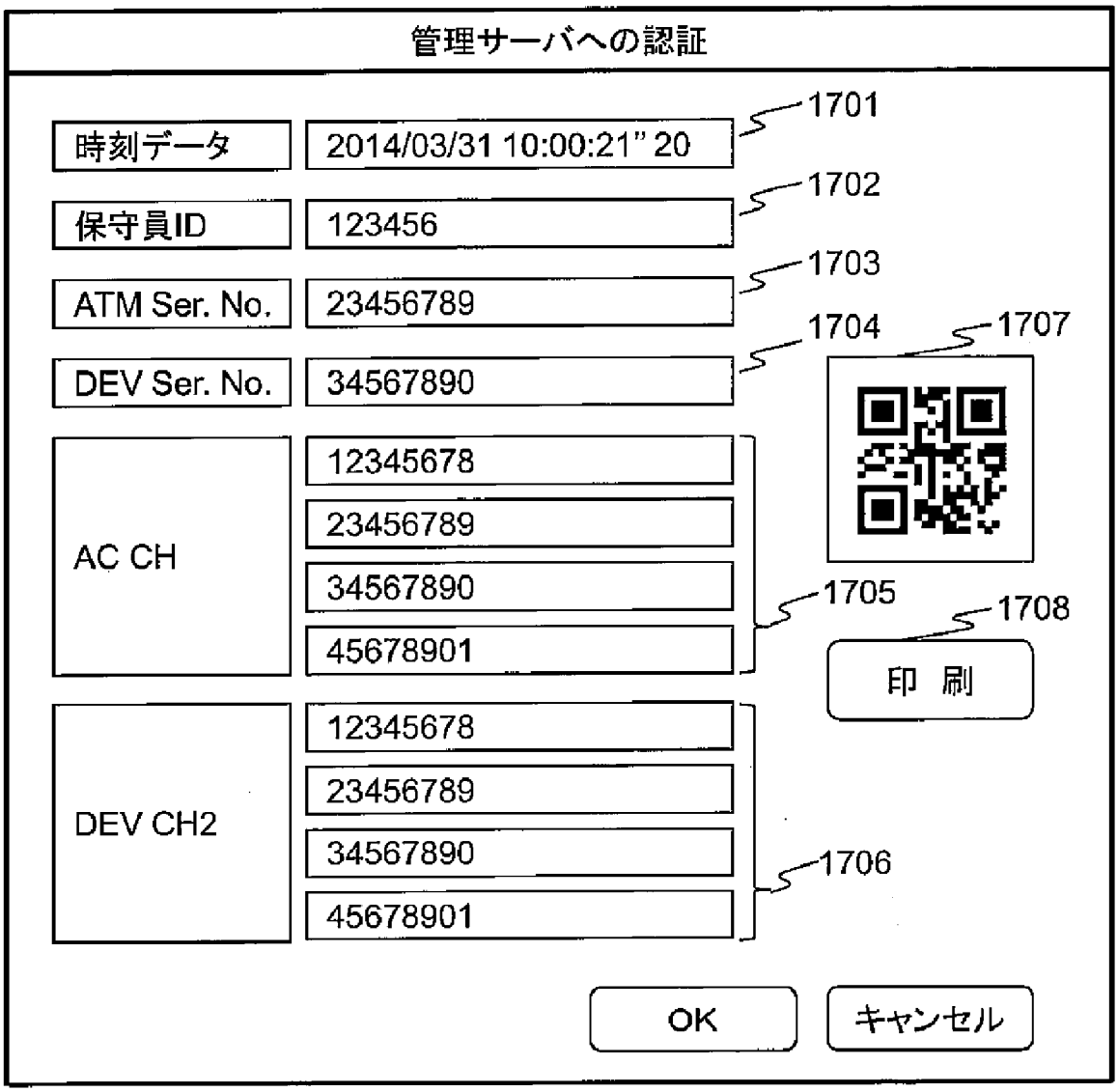
[図16]

図16


ATM
101
AC
201
DEV
203
406,407
404
406
DEV CH 1 生成
DEV RS 1 検証
DEV Ser. No.
暗号処理ファームウェア
DEV Ser. No. DEV CH 1
DEV RS 1
323
S201
S202
S217
S218
AC CH 生成 DEV CH 2 生成
AC RS 検証 DEV RS 1 変換
時刻データ ATM Ser. No. 保守員ID
暗号鍵インストーラ
316
317
318
303
S203
ATM環境認証 (固有デバイスの有無チェック)
暗号化キーパッド
カードリーダ
I/O制御部
205
204
202
212
209
213
S204
S205
S215
S216
S206
S207
S214
507-512
時刻データ 保守員ID ATM Ser. No. DEV Ser. No. AC CH DEV CH 2
S208
104
105
S213
AC RS DEV RS 2
711,712
107
管理サーバ
106
データ受信 AC RS/DEV RS 2生成 トレース情報登録 AC RS/DEV RS 2送信
ATM暗号鍵生成管理ソフトウェア
時刻データ 保守員ID ATM Ser. No. DEV Ser. No. AC CH DEV CH 2 AC RS DEV RS 2
S209
S210
S211
S212
702
801-808
凡例
データ
プログラム
処理

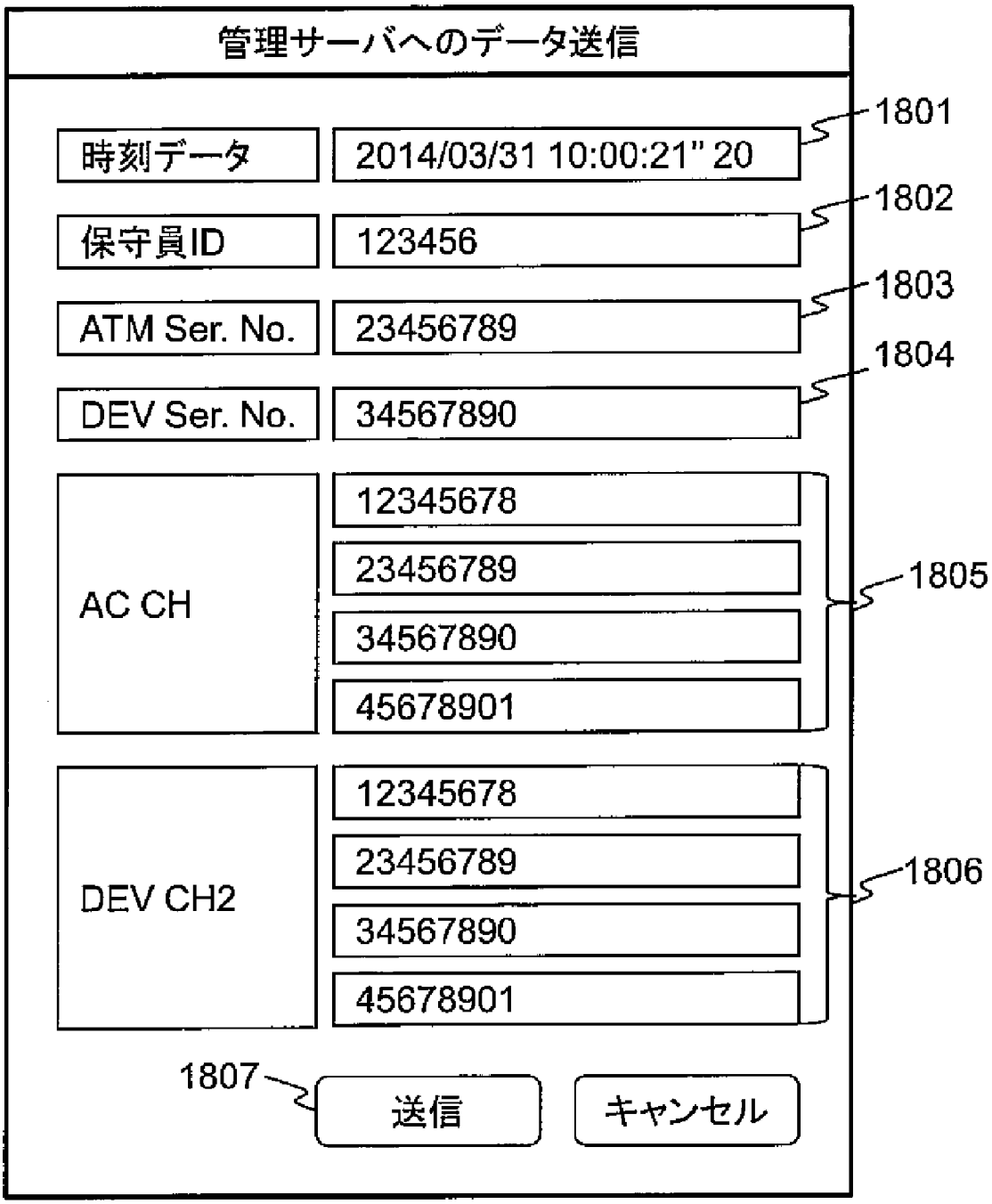
[図17]

図17


管理サーバへの認証
時刻データ
2014/03/31 10:00:21" 20
1701
保守員ID
123456
1702
ATM Ser. No.
23456789
1703
DEV Ser. No.
34567890
1704
1707
AC CH
12345678
23456789
34567890
45678901
1705
1708
印 刷
DEV CH2
12345678
23456789
34567890
45678901
1706
OK
キャンセル

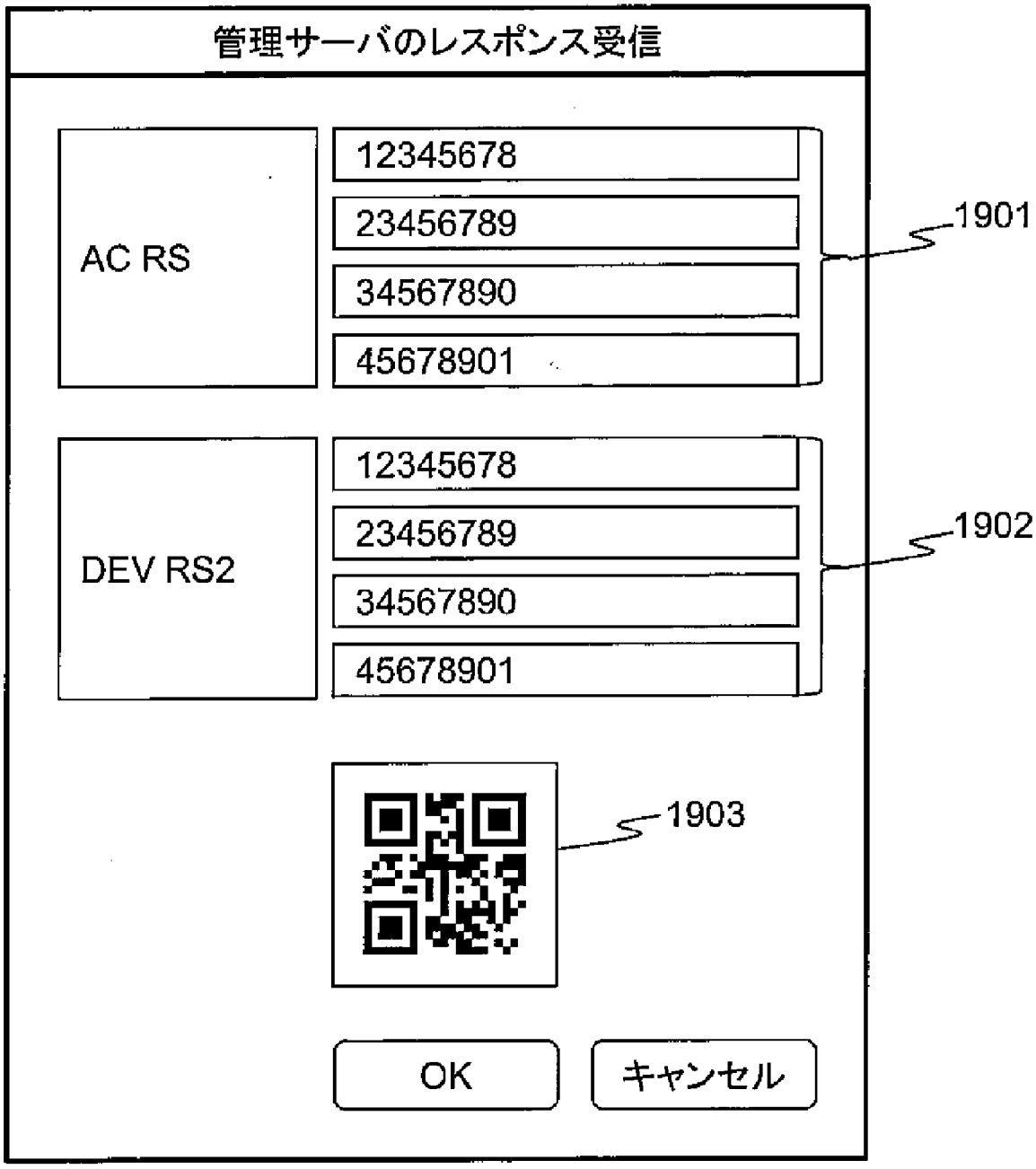
[図18]

図18


管理サーバへのデータ送信
時刻データ
2014/03/31 10:00:21" 20
1801
保守員ID
123456
1802
ATM Ser. No.
23456789
1803
DEV Ser. No.
34567890
1804
AC CH
12345678
23456789
34567890
45678901
1805
DEV CH2
12345678
23456789
34567890
45678901
1806
1807
送信
キャンセル

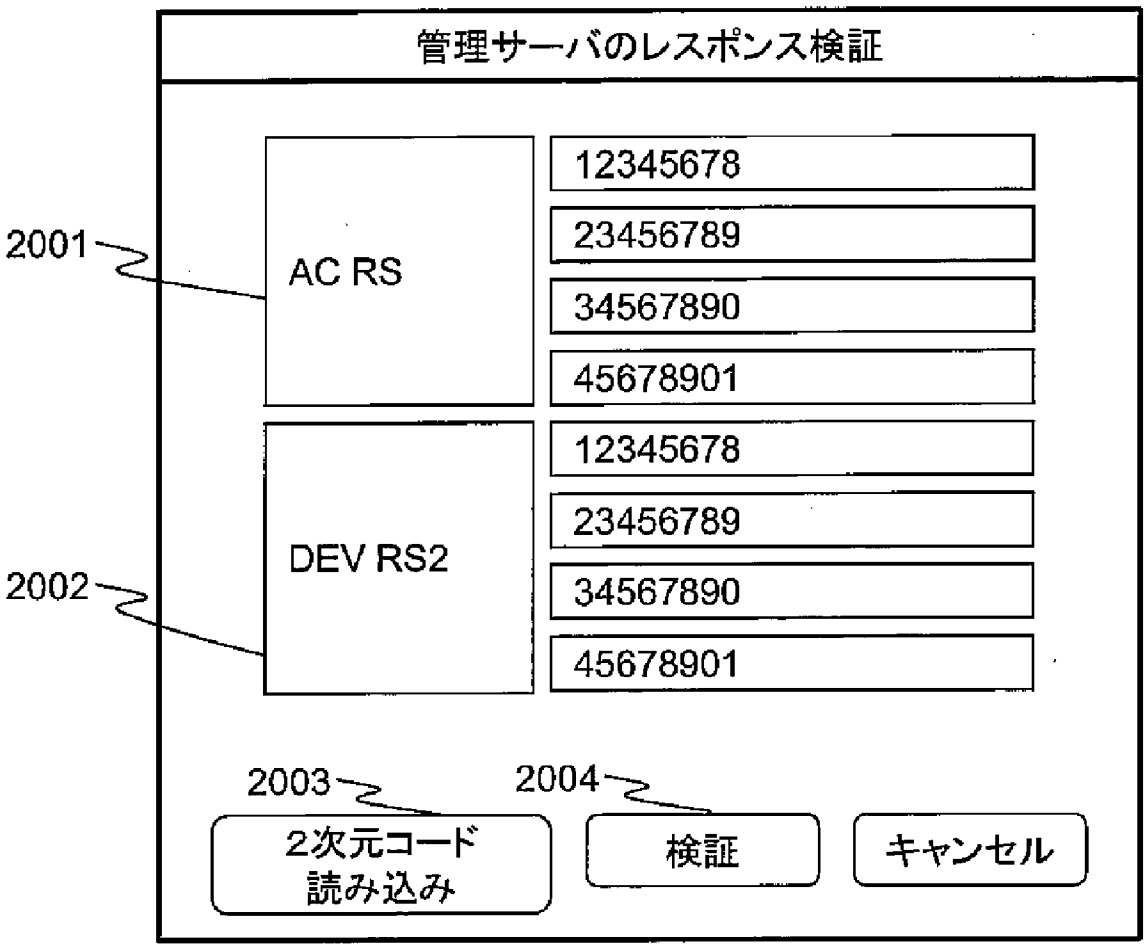
[図19]

図19


管理サーバのレスポンス受信
AC RS
12345678
23456789
34567890
45678901
1901
DEV RS2
12345678
23456789
34567890
45678901
1902
1903
OK
キャンセル

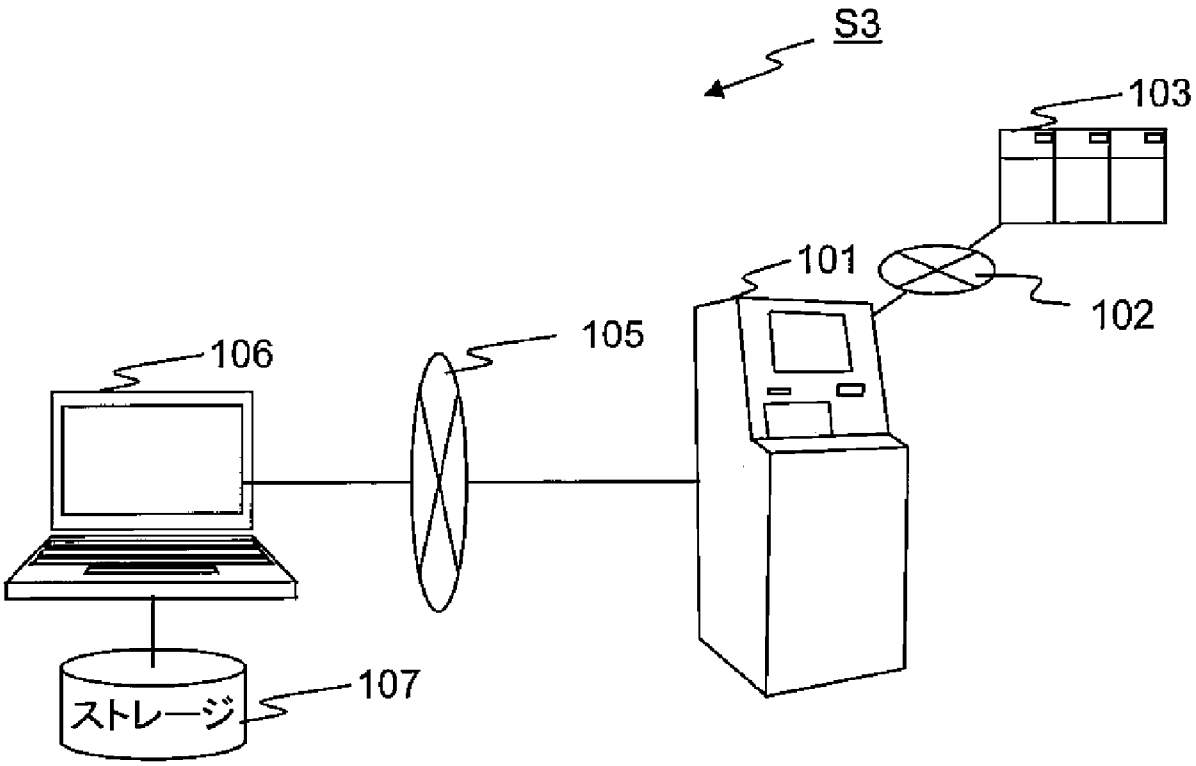
[図20]

図20


管理サーバのレスポンス検証
2001
AC RS
12345678
23456789
34567890
45678901
2002
DEV RS2
12345678
23456789
34567890
45678901
2003
2004
2次元コード
読み込み
検証
キャンセル

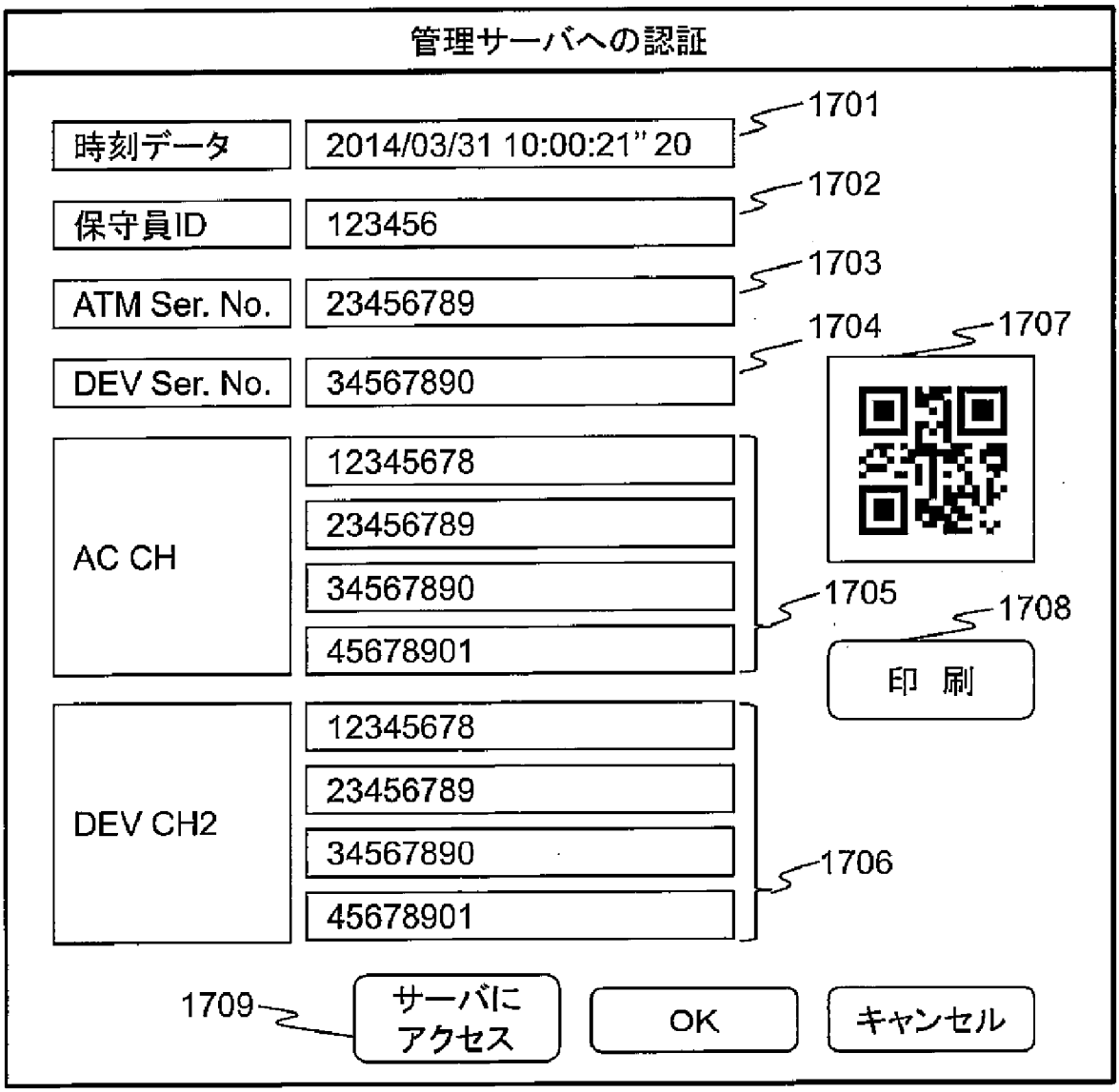
[図21]

図21



[図22]

図22


管理サーバへの認証
時刻データ
2014/03/31 10:00:21" 20
1701
保守員ID
123456
1702
ATM Ser. No.
23456789
1703
DEV Ser. No.
34567890
1704
1707
AC CH
12345678
23456789
34567890
45678901
1705
1708
印 刷
DEV CH2
12345678
23456789
34567890
45678901
1706
1709
サーバに
アクセス
OK
キャンセル

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/062171

A. CLASSIFICATION OF SUBJECT MATTER
G07D9/00(2006.01)i, *G06Q20/18*(2012.01)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, G06Q20/18

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	1996-2015
Kokai Jitsuyo Shinan Koho	1971-2015	Toroku Jitsuyo Shinan Koho	1994-2015

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 A	JP 2001-126098 A (Fujitsu Ltd.), 11 May 2001 (11.05.2001), paragraphs [0014], [0024] to [0054], [0077] to [0088]; fig. 1 to 5, 10 to 12 & US 6253997 B1 & EP 1096450 A2	1-2,4-6,10 3,7-9,11-14
Y	JP 2006-72775 A (Fuji Electric Retail Systems Co., Ltd.), 16 March 2006 (16.03.2006), paragraphs [0021] to [0029]; fig. 3 (Family: none)	1-2,4-6,10
Y	JP 2005-346423 A (Hitachi-Omron Terminal Solutions, Corp.), 15 December 2005 (15.12.2005), paragraphs [0023] to [0025]; fig. 1 to 5 (Family: none)	1-2,4-6,10

☒ 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
"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
04 August 2015 (04.08.15)	11 August 2015 (11.08.15)

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/JP2015/062171

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 2001-117873 A (Hitachi, Ltd.), 27 April 2001 (27.04.2001), paragraphs [0067] to [0074]; fig. 16 to 17 (Family: none)	1-14
A	EP 1898349 A1 (SIEMENS AG), 12 March 2008 (12.03.2008), entire text; all drawings (Family: none)	13-14

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／０６２１７１

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, G06Q20/18(2012.01)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, G06Q20/18

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	１９７１－２０１５年
日本国実用新案登録公報	１９９６－２０１５年
日本国登録実用新案公報	１９９４－２０１５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 A	JP 2001-126098 A (富士通株式会社) 2001.05.11, 段落 [0014], [0024] - [0054], [0077] - [0088], [図 1] - [図 5], [図 10] - [図 12] & US 6253997 B1 & EP 1096450 A2	1-2, 4-6, 10 3, 7-9, 11-14
Y	JP 2006-72775 A (富士電機リテイルシステムズ株式会社) 2006.03.16, 段落 [0021] - [0029], [図 3] (ファミリーなし)	1-2, 4-6, 10
Y	JP 2005-346423 A (日立オムロンターミナルソリューションズ株式会社) 2005.12.15, 段落 [0023] - [0025], [図 1] － [図 5] (フ	1-2, 4-6, 10

☑　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
０４．０８．２０１５	１１．０８．２０１５

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　３９４３
望月　寛
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
	ファミリーなし）	
A	JP 2001-117873 A（株式会社日立製作所）2001.04.27，段落［0067］－［0074］，［図16］－［図17］（ファミリーなし）	1-14
A	EP 1898349 A1（SIEMENS AKTIENGESELLSCHAFT）2008.03.12，全文，全図（ファミリーなし）	13-14