

(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12月7日(07.12.2017)



(10) 国際公開番号

WO 2017/208445 A1

(51) 国際特許分類:
G06Q 20/18 (2012.01)

(21) 国際出願番号: PCT/JP2016/066630

(22) 国際出願日: 2016年6月3日(03.06.2016)

(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: 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

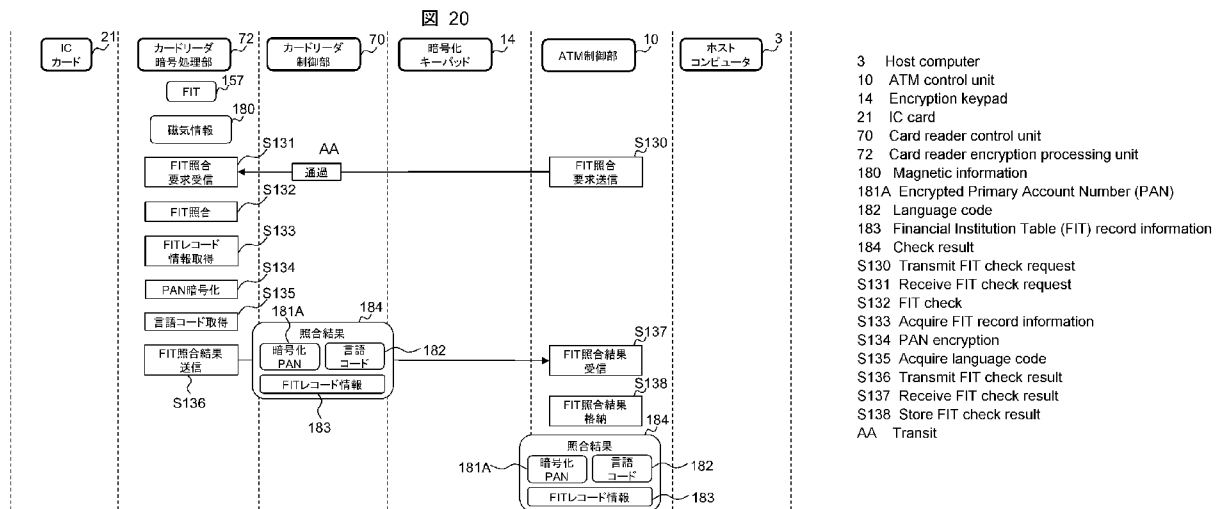
株式会社内 Tokyo (JP). 芳井 昌浩(YOSHII, Masahiro); 〒1418576 東京都品川区大崎一丁目6番3号 日立オムロンターミナルソリューションズ株式会社内 Tokyo (JP).

(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,

(54) Title: AUTOMATED TRANSACTION SYSTEM, METHOD FOR CONTROL THEREOF, AND CARD READER

(54) 発明の名称: 自動取引システム及びその制御方法並びにカードリーダー



(57) Abstract: [Problem] To recommend a highly reliable automated transaction system, method for control thereof, and card reader such that leakage of card information can be sufficiently avoided practically. [Solution] Provided is an automated transaction system, in which an automated transaction device has disposed thereupon: a card reader which reads first card information which has been recorded on a card medium inserted therein by a user; and a device control unit which generates a request message, transmits said message to a host device, and, on the basis of a response message from the host device, executes a control process for carrying out a transaction. The card reader: stores first card format information in which information which relates to a format of the first card information for each financial institution has been registered; refers to the first card format information so as to acquire prescribed confidential information from the first card information which has been read from the card medium, said prescribed confidential information including a card number; and encrypts the acquired confidential information for transmission to the device control unit. The device control

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:

- 一 国際調査報告 (条約第21条(3))

unit generates a request message which includes the encrypted confidential information which has been transmitted from the card reader, and transmits said request message to the host device.

(57) 要約: 【課題】 カード情報の漏洩を実用上十分に防止し得る信頼性の高い自動取引システム及びその制御方法並びにカードリーダを提案する。 【解決手段】 自動取引システムにおいて、利用者により装填されたカード媒体に記録された第1のカード情報を読み出すカードリーダと、要求電文を生成してホスト装置に送信し、ホスト装置からの応答電文に基づいて取引を行うための制御処理を実行する装置制御部とを自動取引装置に設け、カードリーダが、金融機関ごとの第1のカード情報のフォーマットに関する情報が登録された第1のカードフォーマット情報を保持し、第1のカードフォーマット情報を参照して、カード媒体から読み出した第1のカード情報からカード番号を含む所定の機密情報を取得し、取得した機密情報を暗号化して装置制御部に送信し、装置制御部が、カードリーダから送信されてきた暗号化された機密情報を含む要求電文を生成してホスト装置に送信するようにした。

明 細 書

発明の名称：

自動取引システム及びその制御方法並びにカードリーダー

技術分野

[0001] 本発明は、自動取引システム及びその制御方法並びにカードリーダーに関し、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カード情報と、利用者の操作とに基づいて入出金取引を行うＡＴＭ（Automated Teller Machine）と、当該入出金取引の承認等を行う勘定系ホストコンピュータとを有する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] 近年、急速な情報化社会の進展に伴い、企業や自治体等において個人情報や機密情報に対する管理意識が高まっている。また、これまで問題視されてこなかったＡＴＭ内の閉じたネットワークについてもマルウェアによる機密情報の詐取や不正取引が大きな問題となっている。

[0003] ＡＴＭで扱う機密情報としては、カード裏面に貼着された磁気テープに記録されている磁気情報やカード番号及び金融機関コードなどのカード情報がある（特許文献１）。磁気情報が漏洩した場合、その磁気情報を元に偽造カードが作成され、不正使用される可能性がある。またカード番号が有効期限等と併せて漏洩した場合には、その情報を利用してネットショッピングなどで不正使用される可能性がある。

[0004] このような情報漏洩を防止するための対策として、利用者によりＡＴＭに装填されたカードから読み取ったカード情報を、ＡＴＭの制御部において暗号化した上で、取引の承認等を行う勘定系ホストコンピュータに送信する方法が考えられる。

先行技術文献

特許文献

[0005] 特許文献１：特開平５－２７４３３１号公報

発明の概要

発明が解決しようとする課題

[0006] しかしながら、上述のようにＡＴＭの制御部が勘定系ホストコンピュータにカード情報を暗号化して送信するようにしたとしても、ＡＴＭの内部デバイス、特にＡＴＭ全体の動作制御を司り、勘定系ホストコンピュータとの間の通信を行うＡＴＭ制御部がマルウェアに感染した場合に、当該ＡＴＭ制御部を介してカード情報が外部に流出するおそれがある。

[0007] 本発明は以上の点を考慮してなされたもので、カード情報の漏洩を実用上十分に防止し得る信頼性の高い自動取引システム及びその制御方法並びにカードリーダ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

[0008] かかる課題を解決するため本発明においては、自動取引装置及びホスト装置を有し、前記自動取引装置に対する利用者の操作に応じた取引の要求電文を前記自動取引装置から前記ホスト装置に送信し、前記要求電文に対する前記ホスト装置からの応答電文に基づいて前記自動取引装置が前記取引を行う自動取引システムにおいて、前記自動取引装置に、前記利用者により装填された前記カード媒体に記録された第１のカード情報を読み出すカードリーダと、前記要求電文を生成して前記ホスト装置に送信し、前記ホスト装置からの前記応答電文に基づいて前記取引を行うための制御処理を実行する装置制御部とを設け、前記カードリーダが、金融機関ごとに固有な、前記第１のカード情報のフォーマットに関する情報が登録された第１のカードフォーマット情報を保持し、前記第１のカードフォーマット情報を参照して、前記カード媒体から読み出した前記第１のカード情報から前記カード番号を含む所定の機密情報を取得し、取得した前記機密情報を暗号化して前記装置制御部に送信し、前記装置制御部が、前記カードリーダから送信されてきた暗号化された前記機密情報を含む前記要求電文を生成して前記ホスト装置に送信するようにした。

[0009] また本発明においては、自動取引装置及びホスト装置を有し、前記自動取

引装置に対する利用者の操作に応じた取引の要求電文を前記自動取引装置から前記ホスト装置に送信し、前記要求電文に対する前記ホスト装置からの応答電文に基づいて前記自動取引装置が前記取引を行う自動取引システムの制御方法において、前記自動取引装置は、前記利用者により装填された前記カード媒体に記録された第1のカード情報を読み出すカードリーダーと、前記要求電文を生成して前記ホスト装置に送信し、前記ホスト装置からの前記応答電文に基づいて前記取引を行うための制御処理を実行する装置制御部とを有し、前記カードリーダーは、金融機関ごとに固有な、前記第1のカード情報のフォーマットに関する情報が登録された第1のカードフォーマット情報を保持し、前記カードリーダーが、前記第1のカードフォーマット情報を参照して、前記カード媒体から読み出した前記第1のカード情報から前記カード番号を含む所定の機密情報を取得する第1のステップと、前記カードリーダーが、取得した前記機密情報を暗号化して前記装置制御部に送信する第2のステップと、前記装置制御部が、前記カードリーダーから送信されてきた暗号化された前記機密情報を含む前記要求電文を生成して前記ホスト装置に送信する第3のステップとを設けるようにした。

[0010] さらに本発明においては、利用者の操作に応じた取引の要求電文を前記ホスト装置に送信し、前記要求電文に対する前記ホスト装置からの応答電文に基づいて前記取引を行う自動取引装置に設けられ、前記利用者により前記自動取引装置に装填されたカード媒体から当該カード媒体に記録されたカード情報を読み出すカードリーダーにおいて、前記自動取引装置に装填された前記カード媒体を搬送し、前記カード媒体から前記カード情報を読み取るカード搬送・読取部と、前記カード搬送・読取部により前記カード媒体から読み取られた前記カード情報を暗号化するカードリーダー暗号処理部とを設け、前記自動取引装置は、前記要求電文を生成して前記ホスト装置に送信し、前記ホスト装置からの前記応答電文に基づいて前記取引を行うための制御処理を実行する装置制御部を有し、前記カードリーダー暗号処理部が、金融機関ごとに固有な、前記第1のカード情報のフォーマットに関する情報が登録された第

1のカードフォーマット情報を保持し、前記第1のカードフォーマット情報を参照して、前記カード媒体から読み出した前記第1のカード情報から前記カード番号を含む所定の機密情報を取得し、取得した前記機密情報を暗号化して前記装置制御部に送信するようにした。

[0011] 本自動取引システム及びその制御方法並びにカードリーダーによれば、仮にATMの制御部がマルウェアに感染して第1のカード情報が外部に流出したとしても、機密情報が暗号化されているため、偽造カードの作成や不正なネットショッピングの利用に必要なカード番号の漏洩を防止することができる。

発明の効果

[0012] 本発明によれば、カード情報の漏洩を実用上十分に防止し得る信頼性の高い自動取引システム及びその制御方法並びにカードリーダーを実現できる。

図面の簡単な説明

[0013] [図1]第1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]ATM制御部の構成を示すブロック図である。

[図3A]カードリーダーの構成を示すブロック図である。

[図3B]カードリーダー制御部の構成を示すブロック図である。

[図3C]カードリーダー暗号処理部の構成を示すブロック図である。

[図4A]暗号化キーパッド部の構成を示すブロック図である。

[図4B]暗号化キーパッド部の構成を示すブロック図である。

[図5]ICカードの構成を示すブロック図である。

[図6]勘定系ホストコンピュータの構成を示すブロック図である。

[図7A]FITの構成を示す概念図である。

[図7B]FIT機密関連カードフォーマット情報の構成を示す概念図である。

[図8]認証局の構成を示すブロック図である。

[図9]ルート鍵ペア及びCR鍵ペアの初期設定の流れを示すフロー図である。

[図10]EPP鍵ペアの初期設定の流れを示すフロー図である。

[図11]ホスト鍵の初期設定の流れを示すフロー図である。

[図12]カードリーダー及び暗号化キーパッド間でのマスタ鍵交換の流れを示すフロー図である。

[図13]カードリーダー及び暗号化キーパッド間でのマスタ鍵交換の流れを示すフロー図である。

[図14]カードリーダー及び勘定系ホストコンピュータ間でのマスタ鍵交換の流れを示すフロー図である。

[図15]カードリーダー及び勘定系ホストコンピュータ間でのマスタ鍵交換の流れを示すフロー図である。

[図16]カードリーダー及び暗号化キーパッド間でのセッション鍵交換の流れを示すフロー図である。

[図17]カードリーダー及び勘定系ホストコンピュータ間でのセッション鍵交換の流れを示すフロー図である。

[図18]ＩＣカード取引処理のうちのＦＩＴ更新処理の流れを示すフロー図である。

[図19]ＩＣカード取引処理のうちのＩＣカードから磁気情報を読み取るカード読取処理の流れを示すフロー図である。

[図20]ＩＣカード取引処理のうちのＦＩＴ照合処理の流れを示すフロー図である。

[図21]ＩＣカード取引処理のうちのＩＣカードからＩＣ情報を読み取るカード読取処理の流れを示すフロー図である。

[図22]ＩＣカード取引処理のうちのＰＩＮ入力に関する処理の流れを示すフロー図である。

[図23]ＩＣカード取引処理のうちの取引金額の入力に関する処理の流れを示すフロー図である。

[図24]ＩＣカード取引処理のうち、ＡＴＭ制御部がＩＣカードからカード認証データを取得する処理の流れを示すフロー図である。

[図25]ＩＣカード取引処理のうち、ＡＴＭ制御部が勘定系ホストコンピュー

タに取引要求を送信する処理の流れを示すフロー図である。

[図26] ICカード取引処理のうち、ATM制御部が勘定系ホストコンピュータからの取引応答電文を取得する処理の流れを示すフロー図である。

[図27] ICカード取引処理のうち、イシュア認証及び出金処理の流れを示すフロー図である。

[図28] 第2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29] 第2の実施の形態の自動取引システムにおけるFIT更新処理の流れを示すフロー図である。

[図30] 第2の実施の形態の自動取引システムにおけるFIT照合処理の流れを示すフロー図である。

[図31] 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32] 第3の実施の形態の自動取引システムにおけるカードリーダ暗号処理部の構成を示すブロック図である。

[図33] 第3の実施の形態の自動取引システムにおける勘定系ホストコンピュータの構成を示すブロック図である。

[図34] 第3の実施の形態の自動取引システムにおけるルート鍵ペア及びCR鍵ペアの初期設定の流れを示すフロー図である。

[図35] 第3の実施の形態の自動取引システムにおけるホスト鍵の初期設定の流れを示すフロー図である。

[図36] 第3の実施の形態の自動取引システムにおけるカードリーダ及び勘定系ホストコンピュータ間でのマスタ鍵交換の流れを示すフロー図である。

[図37] 第3の実施の形態の自動取引システムにおけるカードリーダ及び勘定系ホストコンピュータ間でのマスタ鍵交換の流れを示すフロー図である。

発明を実施するための形態

[0014] 以下図面について、本発明の一実施の形態を詳述する。

[0015] (1) 第1の実施の形態

(1-1) 本実施の形態による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とがLAN (Local Area Network) 又はWAN (Wide Area Network) などの広域ネットワーク4を介して接続され、これらATM2及び勘定系ホストコンピュータ3とは別個に認証局5が設けられることにより構成されている。

[0016] ATM2は、利用者の操作に応じて現金の入出金等の取引を行う自動取引装置である。図1に示すように、ATM2は、当該ATM2全体の動作制御を司るATM制御部10と、ATM2の各種表示ランプ制御や扉開閉検知等を行うI/O制御部11と、ATM2の前面に設けられた入出金口内に投入された紙幣を計数して収納庫に搬送、保管し又は出金すべき紙幣を収納庫から取り出して入出金口内に搬送する紙幣処理部12と、ATM2での取引に必要なキャッシュカード等のカード媒体から当該カード媒体に記録されている情報を読み取るカードリーダ13と、取引金額や暗証番号等を入力するためのテンキーを有し、入力された暗証番号等の情報を暗号化する機能を有する暗号化キーパッド14と、取引明細票用のプリンタでなるレシートプリンタ15と、通帳用のプリンタでなる通帳プリンタ16と、ATM取引のログを記録するジャーナルプリンタ17と、ATM利用者の顔写真を撮影するセキュリティ用の監視カメラ18と、入金取引、出金取引などの取引に関する情報を表示する表示部19と、勘定系ホストコンピュータ3と通信を行う通信処理部20とを備えて構成される。なお、表示部19は、利用者からの操作を受け付ける表示操作部であってもよい。

[0017] ただしATM2は、入金された硬貨や出金する硬貨を取り扱う硬貨処理部(図示せず)を備えていてもよい。また、本実施の形態においては、カード媒体としてIC (Integrated Circuit Card) カード21が使用される例について説明する。

[0018] 図2は、ATM制御部10の概略構成を示す。この図2に示すように、A

ＴＭ制御部１０は、ＣＰＵ（Central Processing Unit）３０、メモリ３１等の情報処理資源を備えたマイクロコンピュータ構成を有する。ＣＰＵ３０は、ＡＴＭ制御部１０全体の動作制御を司るプロセッサである。メモリ３１は、例えば半導体メモリから構成され、プログラムやデータが格納される。

[0019] ＡＴＭ制御部１０のメモリ３１の記憶領域は、プログラム領域３１Ａ及びデータ領域３１Ｂに区分されて管理される。そしてプログラム領域３１Ａには、ＡＴＭ２の取引全体を制御するＡＴＭアプリケーション４０と、Ｉ／Ｏ（Input/Output）制御部１１、紙幣処理部１２、カードリーダ１３、暗号化キーパッド１４、レシートプリンタ１５、通帳プリンタ１６、ジャーナルプリンタ１７、監視カメラ１８、表示部１９及び通信処理部２０をそれぞれ制御するためのソフトウェア（Ｉ／Ｏ制御部制御ソフトウェア４１、紙幣処理部制御ソフトウェア４２、カードリーダ制御ソフトウェア４３、暗号化キーパッド制御ソフトウェア４４、レシートプリンタ制御ソフトウェア４５、通帳プリンタ制御ソフトウェア４６、ジャーナルプリンタ制御ソフトウェア４７、監視カメラ制御ソフトウェア４８及び通信処理ソフトウェア４９）と、ソフトウェア環境等の設定ファイルであるソフトウェア設定ファイル５０とが格納される。

[0020] またデータ領域３１Ｂには、ＡＴＭ２での入出金取引に必要なデータが格納される。例えば、カード番号６０、勘定系ホストコンピュータ３（図１）との取引電文のセキュリティを高めるために取引ごとに生成されるＡＴＣ（ＡＴｍ Controler）乱数６１、磁気情報などを含む取引電文データである取引データ６２、ＡＲＱＣ（Authentication Request Cryptogram）６３、取引を成立させてよいかどうかを判断した結果のデータである取引可否データ６４、ＡＲＰＣ（Authentication Response Cryptogram）６５、ＡＲＰＣの正当性を検証した結果であるＡＲＰＣ検証結果６６、ＩＣカード２１（図１）によって取引可否が検証された結果である取引検証結果６７、紙幣処理部１２（図１）に対して送信されるコマンドデータである紙幣処理部制御データ６８及び入金取引時において紙幣処理部１２（図１）がＡＴＭ２（図１）に投入

された紙幣を計数した合計金額である入金計数金額 6 9 などがデータ領域 3 1 B に格納される。

[0021] 図 3 A は、カードリーダ 1 3 (図 1) の概略構成を示す。この図 3 A に示すように、カードリーダ 1 3 は、カードリーダ制御部 7 0、カード搬送・読取部 7 1 及びカードリーダ暗号処理部 7 2 を備えて構成される。カードリーダ制御部 7 0 は、カード搬送・読取部 7 1 及びカードリーダ暗号処理部 7 2 を制御すると共に、これらカード搬送・読取部 7 1 及びカードリーダ暗号処理部 7 2 の間でデータのやり取りを行う機能を有するハードウェアユニットである。また、カード搬送・読取部 7 1 は、ATM 2 のカード挿入口 (図示せず) と、ATM 2 内部にあるカードリーダ 1 3 の読取部との間で IC カード 2 1 を搬送すると共に、IC カード 2 1 の接点を通じて IC カード 2 1 との間でデータの入出力を行う機能を有するハードウェアユニットである。さらにカードリーダ暗号処理部 7 2 は、カードリーダ 1 3 内でカード情報の暗号化などの暗号処理を行う機能を有するハードウェアユニットである。カードリーダ暗号処理部 7 2 として、SAM (Secure Access Module) 等、取り外し可能な暗号処理デバイスを用いることもできる。

[0022] カードリーダ制御部 7 0 は、図 3 B に示すように、カードリーダ制御部 7 0 全体の動作制御を司る CPU 8 0 と、例えば半導体メモリなどから構成されるメモリ 8 1 などの情報処理資源を備えて構成される。カードリーダ制御部 7 0 のメモリ 8 1 の記憶領域は、プログラム領域 8 1 A 及びデータ領域 8 1 B に区分されて管理されており、プログラム領域 8 1 A に、全体制御ファームウェア 8 2、IC カード通信制御ファームウェア 8 3 及び CSE (Card reader Secure Element) 制御ファームウェア 8 4 が格納され、データ領域 8 1 B に、全体制御用バッファ 8 5、IC カード通信用バッファ 8 6 及び CSE 通信用バッファ 8 7 が設けられる。

[0023] 全体制御ファームウェア 8 2 は、ATM 制御部 1 0 との間の通信を制御したり、カード搬送・読取部 7 1 (図 3 A) の搬送制御などを行う機能を有するソフトウェアであり、IC カード通信制御ファームウェア 8 3 は、IC カ

ード 21 との間でデータの入出力制御を行う機能を有するソフトウェアである。また CSE 制御ファームウェア 84 は、カードリーダ暗号処理部 72 (図 3A) を制御したり、当該カードリーダ暗号処理部 72 との間の通信制御を行うソフトウェアである。

[0024] また全体制御用バッファ 85 は、ATM 制御部 10 との通信用バッファも含む全体制御に使われるデータエリアであり、IC カード通信用バッファ 86 及び CSE 通信用バッファ 87 はそれぞれ、IC カード 21 又はカードリーダ暗号処理部 72 との通信制御用バッファである。

[0025] カードリーダ暗号処理部 72 は、図 3C に示すように、当該カードリーダ暗号処理部 72 全体の動作制御を司るプロセッサである CPU 90 と、例えば、半導体メモリなどから構成されるメモリ 91 となどの情報処理資源を備えて構成される。

[0026] カードリーダ暗号処理部 72 のメモリ 91 の記憶領域は、カードリーダ制御部 70 (図 3B) と同様に、プログラム領域 91A 及びデータ領域 91B に区分されて管理されている。

[0027] そしてプログラム領域 91A には、アプリケーション 92、通信制御ファームウェア 93 及び暗号処理ファームウェア 94 が格納される。アプリケーション 92 は、カードリーダ暗号処理部 72 全体の制御を行う機能を有するソフトウェアであり、通信制御ファームウェア 93 は、カードリーダ制御部 70 との間の通信制御を行う機能を有するソフトウェアである。また暗号処理ファームウェア 94 は、電子署名処理や暗号化などを行う機能を有するソフトウェアである。

[0028] またデータ領域 91B には、ルート検証鍵 95、CR 署名鍵 96、CR 検証鍵 97、CR 検証鍵署名 98、EPP 公開鍵 99、ホスト公開鍵 100、CR-EPP マスタ鍵 101、CR-EPP セッション鍵 102、CR-ホストマスタ鍵 103 及び CR-ホストセッション鍵 104 などが後述する各種処理の過程で適宜格納される。

[0029] 暗号化キーパッド (EPP) 14 は、図 4A に示すように、暗号化キーパ

ッド制御部 110 及びキーパッド 111 などを備えて構成される。暗号化キーパッド制御部 110 は、キーパッド 111 を制御すると共に、暗号化キーパッド制御部 110 及びキーパッド 111 の間でデータのやり取りを行う機能を有するハードウェアユニットであり、キーパッド 111 は、ATM2 の筐体上で顧客による操作を受け付けるように設置され、顧客による暗証番号や金額などの入力を受け付けるハードウェアユニットである。

[0030] 暗号化キーパッド制御部 110 は、図 4 B に示すように、暗号化キーパッド制御部 110 全体の動作制御を司る CPU 120 と、例えば半導体メモリなどから構成されるメモリ 121 などの情報処理資源を備えて構成される。

[0031] 暗号化キーパッド制御部 110 のメモリ 121 の記憶領域は、プログラム領域 121 A 及びデータ領域 121 B に区分されて管理されている。

[0032] そしてプログラム領域 121 A には、アプリケーション 122、通信制御ファームウェア 123 及び暗号処理ファームウェア 124 が格納される。アプリケーション 122 は、暗号化キーパッド制御部 110 全体の制御を行う機能を有するソフトウェアであり、通信制御ファームウェア 123 は、ATM 制御部 10 やカードリーダ 13 との間の通信制御を行う機能を有するソフトウェアである。また暗号処理ファームウェア 124 は、電子署名処理や暗号化などを行う機能を有するソフトウェアである。

[0033] またデータ領域 121 B には、全体制御用バッファ 125 及び通信用バッファ 126 が設けられるほか、ルート検証鍵 95、EPP 秘密鍵 105、EPP 公開鍵 99、EPP 公開鍵署名 106、CR 検証鍵 97、CR-EPP マスタ鍵 101 及び CR-EPP セッション鍵 102 などが後述する各種処理の過程で適宜格納される。

[0034] 図 5 は、IC カード 21 の概略構成を示す。IC カード 21 は、当該 IC カード 21 に搭載された IC チップにより構成される IC 領域 130 と、当該 IC カード 21 の裏面に貼着された磁気テープにより構成される磁気領域 140 とを備えている。

[0035] このうち IC 領域 130 は、CPU 131 及びメモリ 132 等の情報処理

資源を備えて構成される。CPU 131は、ICカード21のIC領域130の動作制御を司るプロセッサである。メモリ132は、例えば半導体メモリから構成される。

[0036] IC領域130のメモリ132の記憶領域は、プログラム領域132A及びデータ領域132Bに区分されて管理される。そしてプログラム領域132Aには、IC領域130の処理を制御するICアプリケーション133、通信制御ファームウェア134及び暗号処理ファームウェア135などが格納される。

[0037] ICアプリケーション133は、ICカード21全体の制御を行うソフトウェアであり、通信制御ファームウェア134は、カードリーダ13（図1）との間でのデータ通信を制御する機能を有するソフトウェアである。また暗号処理ファームウェア135は、メッセージ認証コードを生成したり、勘定系ホストコンピュータ3から送信されてくるメッセージ認証コードを検証したりする暗号処理機能をもつソフトウェアである。

[0038] またデータ領域132Bには、IC領域130での処理に必要なデータが格納される。具体的には、IC領域130の制御に必要な処理用バッファ136及び通信用バッファ137が設けられるほか、ICカード21を用いた取引に必要な取引データ138などが格納される。なお、取引データ138には、カード番号（以下、これをPAN（Primary Account Number）と呼ぶ）や、磁気領域140に格納されている後述の磁気情報とほぼ同じ内容の情報、及び、そのICカード21を発行した金融機関が自由に格納できる情報であるディスクレショナリ（discretionary）情報などが含まれる。

[0039] さらに磁気領域140には、磁気テープの各トラック（図5ではトラック1～トラック3）140Aにそれぞれ必要な磁気情報が格納される。この磁気情報には、そのICカード21を発行した金融機関に付与されたその金融機関に固有の識別子（金融機関ID）、その金融機関が定めている暗証番号（以下、これをPIN（Personal Identification Number）と呼ぶ）の最大桁数（最大PIN長）、その金融機関におけるPANの桁数（PAN長）、

そのＩＣカード２１に対応付けられた言語を表すコード（言語コード）などが含まれる。

[0040] 図６は、勘定系ホストコンピュータ３の概略構成を示す。勘定系ホストコンピュータ３は、ＡＴＭ２の利用者の口座や残高に関する情報などを記憶及び管理するコンピュータ装置であり、図６に示すように、ＣＰＵ１５０、メモリ１５１等の情報処理資源を備えて構成される。ＣＰＵ１５０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。またメモリ１５１は、例えば半導体メモリから構成される。

[0041] 勘定系ホストコンピュータ３のメモリ１５１の記憶領域は、プログラム領域１５１Ａ及びデータ領域１５１Ｂに区分されて管理される。そしてプログラム領域１５１Ａには、勘定系ホストコンピュータ３の処理全体を制御するホストアプリケーション１５２、通信制御ソフトウェア１５３及び暗号処理ソフトウェア１５４などが格納される。

[0042] ホストアプリケーション１５２は、勘定系ホストコンピュータ３全体の制御を行うソフトウェアである。また通信制御ソフトウェア１５３は、勘定系ホストコンピュータ３と各ＡＴＭ２との間でのデータ通信を制御する機能を有するソフトウェアである。暗号処理ソフトウェア１５４は、ＡＴＭ２から送信されてくるメッセージ認証コードを検証したり、新たなメッセージ認証コードを生成したりする暗号処理機能をもつソフトウェアである。

[0043] またデータ領域１５１Ｂには、勘定系ホストコンピュータ３での処理に必要なデータが格納される。具体的には、かかるデータ領域１５１Ｂには、勘定系ホストコンピュータ３全体の制御に必要な全体制御用バッファ１５５及び通信用バッファ１５６が設けられるほか、ルート検証鍵９５、ホスト秘密鍵１０７、ホスト公開鍵１００、ホスト公開鍵署名１０８、ＣＲ検証鍵９７、ＣＲ－ホストマスタ鍵１０３及びＣＲ－ホストセッション鍵１０４などが後述する各種処理の過程で適宜格納される。

[0044] また勘定系ホストコンピュータ３のメモリ１５１のデータ領域１５１Ｂには、ＩＣカード２１を利用した取引に必要なＦＩＴ（Financial Institution

Table) 157も格納されている。

[0045] FIT 157は、金融機関ごとに固有な各種情報取が格納されたテーブルであり、図7Aに示すように、金融機関ごとの金融機関IDオフセット、金融機関ID、最大PIN長、PANオフセット、PAN長、言語コードオフセット及びPINブロックフォーマットなどの情報161～167がそれぞれ金融機関ごとにまとめられたレコード160の情報（以下、これをレコード情報と呼ぶ）としてそれぞれ格納されている。

[0046] このうち金融機関IDは、上述のように対応する金融機関に付与されたその金融機関に固有の識別子である。また金融機関IDオフセットは、その金融機関が発行したICカード21の裏面に貼着された磁気テープの記憶領域における、その金融機関の金融機関IDが格納されている先頭からのオフセット量を表す。さらに最大PIN長は、上述のようにその金融機関が定めているPIN（暗証番号）の最大長を表す。

[0047] またPANオフセットは、その金融機関が発行したICカード21の磁気テープの記憶領域における、PAN（カード番号）が格納されている先頭からのオフセット量を表し、PAN長は、その金融機関におけるカード番号の長さを表す。

[0048] さらに言語コードオフセットは、その金融機関が発行したICカード21の磁気テープの記憶領域における、言語コードが格納されている先頭からのオフセット量を表す。さらにPINブロックフォーマットは、利用者により入力されたPINを暗号化キーパッド14で暗号化する際のフォーマット（暗号化フォーマット）を表す。

[0049] 図8は、認証局5の概略構成を示す。認証局5は、必要な公開鍵に対して署名を付与するコンピュータ装置であり、CPU170及びメモリ171等の情報処理資源を備えて構成される。CPU170は、認証局5全体の動作制御を司るプロセッサである。またメモリ171は、例えば半導体メモリから構成される。

[0050] 認証局5のメモリ171の記憶領域は、プログラム領域171A及びデー

タ領域 171B に区分されて管理される。そしてプログラム領域 171A には、認証局 5 の処理全体を制御するアプリケーション 172、検証鍵の出力等を行うための通信制御ソフトウェア 173 及び暗号化に関する各種処理を実行する機能を有する暗号処理ソフトウェア 174 などが格納される。

[0051] またデータ領域 171B には、認証局 5 での処理に必要なデータが格納される。具体的に、データ領域 171B には、認証局 5 全体の制御に必要な処理用バッファ 175 及び通信制御に利用する通信制御用バッファ 176 が設けられ、さらにルート署名鍵 109 及びルート検証鍵 95 などが後述する各種処理の過程で適宜格納される。

[0052] (1-2) 本自動取引システムにおける各種処理の流れ

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各種処理の流れについて説明する。なお以下においては、各種処理の処理主体を ATM 制御部 10 (図 2)、カードリーダ制御部 70 (図 3B)、カードリーダ暗号処理部 72 (図 3C)、暗号化キーパッド制御部 110 (図 4B)、IC カード 21 (図 5)、勘定系ホストコンピュータ 3 (図 6)、認証局 5 (図 8) として説明するが、実際上は、これら ATM 制御部 10、カードリーダ制御部 70、カードリーダ暗号処理部 72、暗号化キーパッド制御部 110、IC カード 21、勘定系ホストコンピュータ 3 又は認証局 5 内の CPU 30, 80, 90, 120, 131, 150, 170 (図 2、図 3B、図 3C、図 4B、図 5、図 6、図 8) が対応するプログラムやソフトウェアに基づいてその処理を実行することは言うまでもない。

[0053] (1-2-1) 鍵設定の流れ

まず、本自動取引システム 1 においてセキュアな取引を実施するために必要な暗号鍵の設定の流れについて説明する。この鍵設定は、ATM 2 を利用者に利用可能とする前までに行われる。

[0054] (1-2-1-1) ルート鍵ペア及びカードリーダ鍵ペアの初期設定の流れ

図 9 は、ATM 2 のカードリーダ 13 (図 3A) と、認証局 5 (図 8) とを対象として実行される初期鍵 (ルート鍵ペア及びカードリーダ鍵ペア) の

設定手順の流れを示す。なお、以下においては、適宜、「カードリーダ」を「C R」とも呼ぶものとする。

[0055] かかる初期鍵の設定を行う場合、まず、本自動取引システム 1 におけるセキュアな取引の責任元（主に A T M ベンダを想定）がセキュアな環境である認証局 5 おいて、非対称暗号鍵であるルート鍵ペア（ルート署名鍵 1 0 9 及びルート検証鍵 9 5）を生成する（S 1）。そして認証局 5 は、このとき生成したこれらルート署名鍵 1 0 9 及びルート検証鍵 9 5 を認証局 5 のメモリ 1 7 1（図 8）のデータ領域 1 7 1 B に格納する（S 2）。

[0056] また、A T M 2 側では、カードリーダ 1 3（図 3 A）のカードリーダ暗号処理部 7 2 において、非対称暗号鍵である C R 鍵ペア（C R 署名鍵 9 6 及び C R 検証鍵 9 7）を生成する（S 3）。そしてカードリーダ暗号処理部 7 2 は、生成した C R 署名鍵 9 6 及び C R 検証鍵 9 7 をメモリ 9 1（図 3 C）のデータ領域 9 1 B（図 3 C）に格納する（S 4）。この後、カードリーダ暗号処理部 7 2 は、C R 検証鍵 9 7 に対してルート署名鍵 1 0 9 を用いて電子署名を付与するため、C R 検証鍵 9 7 を認証局 5 に送信する（S 5）。

[0057] 認証局 5 は、かかる C R 検証鍵 9 7 を受信すると（S 6）、ステップ S 1 で生成したルート署名鍵 1 0 9 を用いて C R 検証鍵 9 7 に電子署名（C R 検証鍵署名 9 8）を付与する（S 7）。また認証局 5 は、付与した C R 検証鍵署名 9 8 及びステップ S 1 で生成したルート検証鍵 9 5 をカードリーダ暗号処理部 7 2 に送信する（S 8）。

[0058] そしてカードリーダ暗号処理部 7 2 は、これら C R 検証鍵署名 9 8 及びルート検証鍵 9 5 を受信すると（S 9）、これらをメモリ 9 1（図 3 C）のデータ領域 9 1 B（図 3 C）に格納する（S 1 0）。

[0059] （1－2－1－2）暗号化キーパッド鍵ペアの初期設定の流れ

一方、図 1 0 は、暗号化キーパッド 1 4 と、認証局 5 との間で実行される暗号化キーパッド鍵ペアの設定の流れを示す。なお、以下においては、適宜、「暗号化キーパッド」を「E P P」とも呼ぶものとする。

[0060] 図 9 において上述したルート署名鍵 1 0 9 及びルート検証鍵 9 5 を認証局

5が生成後、暗号化キーパッド14が非対称暗号鍵であるEPP鍵ペア（EPP秘密鍵105及びEPP公開鍵99）を生成する（S20）。

[0061] そして暗号化キーパッド14（正確には暗号化キーパッド制御部110であり、以下、同様）は、生成したEPP秘密鍵105及びEPP公開鍵99を暗号化キーパッド制御部110のメモリ121（図4B）のデータ領域121B（図4B）に格納する（S21）。また暗号化キーパッド14は、生成したEPP公開鍵99を、ルート署名鍵109を用いて電子署名を付与するため、認証局5に送信する（S22）。

[0062] 一方、認証局5は、かかるEPP公開鍵99を受信すると（S23）、ルート署名鍵109を用いてこのEPP公開鍵99に電子署名を付与する（S24）。また、認証局5は、付与した電子署名であるEPP公開鍵署名106とルート検証鍵95とを併せて暗号化キーパッド14に送付する（S25）。

[0063] そして暗号化キーパッド14は、これらEPP公開鍵署名106及びルート検証鍵95を受信すると（S26）、これらEPP公開鍵署名106及びルート検証鍵95を暗号化キーパッド制御部110のメモリ121（図4B）のデータ領域121B（図4B）に格納する（S27）。

[0064] （1-2-1-3）暗号鍵（ホスト鍵）の初期設定の流れ

他方、図11は、勘定系ホストコンピュータ3に対してホスト鍵を設定するホスト鍵設定の流れを示す。

[0065] 図9について上述したルート署名鍵109及びルート検証鍵95を認証局5が生成後、まず、勘定系ホストコンピュータ3が非対称暗号鍵であるホスト鍵ペア（ホスト秘密鍵107及びホスト公開鍵100）を生成する（S30）。そして勘定系ホストコンピュータ3は、生成したホスト秘密鍵107及びホスト公開鍵100をメモリ151（図6）のデータ領域151B（図6）に格納する（S31）。

[0066] また勘定系ホストコンピュータ3は、ルート署名鍵109を用いて電子署名を付与するため、ホスト公開鍵100を認証局5に送信する（S32）。

[0067] 認証局 5 は、かかるホスト公開鍵 100 を受信すると (S33)、ルート署名鍵 109 を用いてホスト公開鍵 100 に電子署名を付与する (S34)。また認証局 5 は、このときホスト公開鍵 100 に付与した電子署名であるホスト公開鍵署名 108 及びルート検証鍵 95 を勘定系ホストコンピュータ 3 に送信する (S35)。

[0068] そして勘定系ホストコンピュータ 3 は、かかるホスト公開鍵署名 108 及びルート検証鍵 95 を受信すると (S36)、これらをメモリ 151 (図 6) のデータ領域 151B (図 5) に格納する (S37)。

[0069] (1-2-1-4) マスタ鍵交換 (CR-EPP 間)

本実施の形態の自動取引システム 1 では、カードリーダ 13 及び暗号化キーパッド 14 間と、カードリーダ 13 及び勘定系ホストコンピュータ 3 間とで機密情報をセキュアにやり取りするために当該機密情報をセッションキーを用いて暗号化する。このセッションキーをカードリーダ 13 及び暗号化キーパッド 14 間と、カードリーダ 13 及び勘定系ホストコンピュータ 3 間とでセキュアに共有するためにマスタキーを用いて暗号化する。

[0070] 以下、このマスタキーをカードリーダ 13 及び暗号化キーパッド 14 間とでセキュアに共有するための手順について、図 12 及び図 13 を参照して説明する。

[0071] この場合、まず、カードリーダ 13 のカードリーダ暗号処理部 72 (図 3C) が、CR 検証鍵 97 及び CR 検証鍵署名 98 を暗号化キーパッド 14 に送信する (S40)。

[0072] 暗号化キーパッド 14 は、これら CR 検証鍵 97 及び CR 検証鍵署名 98 を受信すると (S41)、CR 検証鍵署名 98 の署名の正当性をルート検証鍵 95 を用いて検証し (S42)、正当性が検証されればその CR 検証鍵 97 をメモリ 121 (図 4B) のデータ領域 121B (図 4B) に格納する (S43)。そして暗号化キーパッド 14 は、この後、EPP 公開鍵 99 及び EPP 公開鍵署名 106 をカードリーダ 13 のカードリーダ暗号処理部 72 に送信する (S44)。

[0073] カードリーダ暗号処理部 72 は、かかる E P P 公開鍵 99 及び E P P 公開鍵署名 106 を受信すると (S45)、E P P 公開鍵署名 106 の署名の正当性をルート検証鍵 95 を用いて検証し (S46)、正当性が検証されれば E P P 公開鍵 99 をメモリ 91 (図 3C) のデータ領域 91B (図 3C) に格納する (S47)。

[0074] 続いて、カードリーダ暗号処理部 72 は、図 13 に示すように、乱数により C R - E P P マスタ鍵 101 を生成し (S50)、生成した C R - E P P マスタ鍵 101 をメモリ 91 (図 3C) のデータ領域 91B (図 3C) に格納する (S51)。

[0075] またカードリーダ暗号処理部 72 は、この C R - E P P マスタ鍵 101 を E P P 公開鍵 99 を用いて暗号化し、さらに暗号化した C R - E P P マスタ鍵 101 (以下、これを暗号化 C R - E P P マスタ鍵と呼ぶ) に対して C R 署名鍵 96 を用いて電子署名を付与する (S52)。そしてカードリーダ暗号処理部 72 は、この後、この暗号化 C R - E P P マスタ鍵 101A 及び電子署名 101B を暗号化キーパッド 14 に送信する (S53)。

[0076] 暗号化キーパッド 14 は、これら暗号化 C R - E P P マスタ鍵 101A 及び電子署名 101B を受信すると (S54)、まず、その電子署名 101B の正当性を C R 検証鍵 97 を用いて検証する (S55)。そして、暗号化キーパッド 14 は、かかる正当性が検証されれば暗号化 C R - E P P マスタ鍵 101A を E P P 秘密鍵 105 を用いて復号し (S56)、復号した C R - E P P マスタ鍵 101 をメモリ 121 (図 4B) のデータ領域 121B (図 4B) に格納する (S57)。

[0077] (1-2-1-5) マスタ鍵交換 (C R - ホスト間)

次に、図 14 及び図 15 を参照して、カードリーダ 13 及び勘定系ホストコンピュータ 3 間でマスタキーを共有する手順について説明する。この場合、まず、カードリーダ暗号処理部 72 が、C R 検証鍵 97 及び C R 検証鍵署名 98 を勘定系ホストコンピュータ 3 に送信する (S60)。

[0078] 勘定系ホストコンピュータ 3 は、かかる C R 検証鍵 97 及び C R 検証鍵署

名 9 8 を受信すると (S 6 1)、C R 検証鍵署名 9 8 の署名の正当性をルート検証鍵 9 5 を用いて検証し (S 6 2)、正当性が検証されれば C R 検証鍵 9 7 をメモリ 1 5 1 (図 6) のデータ領域 1 5 1 B (図 6) に格納する (S 6 3)。また勘定系ホストコンピュータ 3 は、この後、ホスト公開鍵 1 0 0 及びホスト公開鍵署名 1 0 8 をカードリーダ暗号処理部 7 2 に送信する (S 6 4)。

[0079] カードリーダ暗号処理部 7 2 は、かかるホスト公開鍵 1 0 0 及びホスト公開鍵署名 1 0 8 を受信すると (S 6 5)、ホスト公開鍵署名 1 0 8 の署名の正当性をルート検証鍵 9 5 を用いて検証し (S 6 6)、正当性が検証されればホスト公開鍵 1 0 0 をメモリ 9 1 (図 3 C) のデータ領域 9 1 B (図 3 C) に格納する (S 6 7)。

[0080] またカードリーダ暗号処理部 7 2 は、図 1 5 で示すように、乱数により C R - ホストマスタ鍵 1 0 3 を生成し (S 7 0)、生成した C R - ホストマスタ鍵 1 0 3 をメモリ 9 1 (図 3 C) のデータ領域 9 1 B (図 3 C) に格納する (S 7 1)。

[0081] さらにカードリーダ暗号処理部 7 2 は、かかる C R - ホストマスタ鍵 1 0 3 をホスト公開鍵 1 0 0 を用いて暗号化すると共に、暗号化したホスト公開鍵 1 0 0 (以下、これを暗号化ホスト公開鍵と呼ぶ) に対して C R 署名鍵 9 6 を用いて電子署名を付与し (S 7 2)、この後、これらの暗号化 C R - ホストマスタ鍵及び電子署名を勘定系ホストコンピュータ 3 に送信する (S 7 3)。

[0082] そして勘定系ホストコンピュータ 3 は、これら暗号化 C R - ホストマスタ鍵及び電子署名を受信すると (S 7 4)、まず、その電子署名の正当性を C R 検証鍵 9 7 を用いて検証する (S 7 5)。そして勘定系ホストコンピュータ 3 は、かかる電子署名の正当性を検証できた場合、暗号化 C R - ホストマスタ鍵をホスト秘密鍵 1 0 7 を用いて復号し (S 7 6)、かくして得られた復号された C R - ホストマスタ鍵 1 0 3 をメモリ 1 5 1 (図 6) のデータ領域 1 5 1 B (図 6) に格納する (S 7 7)。

[0083] (1-2-1-6) セッション鍵交換 (CR-EPP)

次に、図16を参照して、カードリーダ13及び暗号化キーパッド14間で必要なカード情報を暗号化するためのセッション鍵 (CR-EPPセッション鍵102) を共有する手順について説明する。

[0084] まず、カードリーダ暗号処理部72が、乱数を用いてCR-EPPセッション鍵102を生成し (S80)、生成したCR-EPPセッション鍵102をメモリ91 (図3C) のデータ領域91B (図3C) に格納する (S81)。

[0085] またカードリーダ暗号処理部72は、このCR-EPPセッション鍵102をCR-EPPマスタ鍵101を用いて暗号化し (S82)、暗号化したCR-EPPセッション鍵102 (以下、これを暗号化CR-EPPセッション鍵102Aと呼ぶ) を暗号化キーパッド14に送信する (S83)。

[0086] 暗号化キーパッド14は、かかる暗号化CR-EPPセッション鍵102Aを受信すると (S84)、この暗号化CR-EPPセッション鍵102AをCR-EPPマスタ鍵101を用いて復号し (S85)、かくして得られた復号されたCR-EPPセッション鍵102をメモリ121 (図4B) のデータ領域121B (図4B) に格納する (S86)。

[0087] (1-2-1-7) セッション鍵交換 (CR-ホスト)

次に、図17を参照して、カードリーダ13と勘定系ホストコンピュータ3の間に必要なカード情報を暗号化するためのセッション鍵 (CR-ホストセッション鍵) を共有する手順について説明する。

[0088] まず、カードリーダ暗号処理部72が、乱数を用いてCR-ホストセッション鍵104を生成し (S90)、生成したCR-ホストセッション鍵104をメモリ91 (図3C) のデータ領域91B (図3C) に格納する (S91)。

[0089] またカードリーダ暗号処理部72は、かかるCR-ホストセッション鍵104をCR-ホストマスタ鍵103を用いて暗号化し (S92)、暗号化したCR-ホストセッション鍵104 (以下、これを暗号化CR-ホストセ

ション鍵１０４Ａと呼ぶ）を勘定系ホストコンピュータ３に送信する（Ｓ９３）。

[0090] 勘定系ホストコンピュータ３は、かかる暗号化ＣＲ－ホストセッション鍵１０４Ａを受信すると（Ｓ９４）、この暗号化ＣＲ－ホストセッション鍵１０４ＡをＣＲ－ホストマスタ鍵１０３を用いて復号し（Ｓ９５）、かくして得られた復号されたＣＲ－ホストセッション鍵１０４をメモリ１５１（図６）のデータ領域１５１Ｂ（図６）に格納する（Ｓ９６）。ここではセッション鍵の共有をマスタ鍵で暗号化して送付する方式で説明したが、ＤＵＫＰＴ（Derived Unique Key Per Transaction）等の鍵共有方式を利用しても同等の効果が得られる。

[0091] （１－２－２）本実施の形態における取引の流れ

次に、本実施の形態の自動取引システム１におけるＩＣカード２１（図１）を用いた取引の流れについて説明する。

[0092] （１－２－２－１）ＦＩＴ更新

図１８に示すように、ＦＩＴ１５７（図７Ａ参照）は勘定系ホストコンピュータ３にて用意されるが、更新された場合などはＡＴＭ２（図１）が持つＦＩＴ１５７を更新して同期を取る必要がある。この場合、ＣＲ－ホストセッション鍵１０４（図１７）を用いてＦＩＴ１５７を暗号化し（Ｓ１００）、暗号化したＦＩＴ（以下、これを暗号化ＦＩＴ１５７Ａと呼ぶ）をＡＴＭ制御部１０に送信する（Ｓ１０１）。またＡＴＭ制御部１０は、この暗号化ＦＩＴ１５７Ａをそのままカードリーダー１３（図１）に送付する。

[0093] カードリーダー１３側では、カードリーダー暗号処理部７２がこの暗号化ＦＩＴ１５７Ａを受信し（Ｓ１０２）、受信した暗号化ＦＩＴ１５７ＡをＣＲ－ホストセッション鍵１０４を用いて復号する（Ｓ１０３）。またカードリーダー暗号処理部７２は、かかる復号により得られた元のＦＩＴ１５７をメモリ９１（図３Ｃ）のデータ領域９１Ｂ（図３Ｃ）に格納する（Ｓ１０４）。

[0094] （１－２－２－２）カード読取（磁気情報）

利用者が取引開始のための所定操作を行い、ＩＣカード２１をＡＴＭ２に

装填すると、図 19 に示すように、ATM制御部 10 がカードリーダー 13 (図 1) のカードリーダー制御部 70 に対してカード読取要求を送信する (S 110)。

[0095] カードリーダー制御部 70 は、かかるカード読取要求を受信すると (S 111)、カード読取処理を開始して、利用者が装填した IC カード 21 を受け付ける (S 112)。またカードリーダー制御部 70 は、この後、IC カード 21 の裏面の磁気テープに記録されている磁気情報 180 をカード搬送・読取部 71 (図 3A) に読み取らせることにより、これを取得する (S 113)。そしてカードリーダー制御部 70 は、このようにして取得した磁気情報 180 をカードリーダー暗号処理部 72 に送信する (S 114)。

[0096] カードリーダー暗号処理部 72 は、かかる磁気情報 180 を受信すると (S 115)、この磁気情報 180 をメモリ 91 (図 3C) のデータ領域 91B (図 3C) に格納する (S 116)。またカードリーダー暗号処理部 72 は、この後、この磁気情報 180 に対するマスク化及び暗号化をそれぞれ行う (S 117, S 118)。なお、ここでの「マスク化」とは、磁気情報 180 のうちの PAN を含む特定の機密情報が格納されている部分の一部 (例えば、PAN の真ん中の数桁) 又は全部を「*」等の記号、他の文字又は数字に変換するなどして隠蔽することを意味し、例えば、トークン PAN のように最初の数桁以外の桁をランダムな数字に変換する処理も含む。また「暗号化」とは、磁気情報 180 のうちのかかる機密情報が格納されている部分を暗号化することを意味する。

[0097] この後、カードリーダー暗号処理部 72 は、かくして得られたマスク化された磁気情報 180 (以下、これをマスク化磁気情報 180A と呼ぶ) と、暗号化された磁気情報 180 (以下、これを暗号化磁気情報 180B と呼ぶ) とを ATM 制御部 10 にそれぞれ送信する (S 119)。

[0098] そして ATM 制御部 10 は、かかるマスク化磁気情報 180A 及び暗号化磁気情報 180B を受信すると (S 120)、これらをメモリ 31 (図 2) のデータ領域 31B (図 2) に格納する (S 121)。

[0099] (1-2-2-3) F I T 照合

続いて、A T M 制御部 1 0 は、図 2 0 に示すように、今回の取引に必要な情報を取得すべく、カードリーダ 1 3 に対して F I T 照合要求を送信する (S 1 3 0)。

[0100] カードリーダ暗号処理部 7 2 は、この F I T 照合要求を受信すると (S 1 3 1)、磁気情報 1 8 0 を F I T 1 5 7 と照合する F I T 照合処理を実行する (S 1 3 2)。そして、カードリーダ暗号処理部 7 2 は、この F I T 照合処理により、F I T 1 5 7 に登録されている各金融機関に関する情報のうちのその I C カード 2 1 を発行した金融機関を特定し、特定した金融機関に関するレコード 1 6 0 (図 7 A) のレコード情報 (以下、これをその金融機関の F I T レコード情報 1 8 3 と呼ぶ) を取得する (S 1 3 3)。

[0101] またカードリーダ暗号処理部 7 2 は、この F I T レコード情報 1 8 3 を使用して磁気情報 1 8 0 からその I C カード 2 1 の P A N を取得し、取得した P A N を暗号化すると共に (S 1 3 4)、かかる F I T レコード情報 1 8 3 を使用して磁気情報 1 8 0 からその I C カード 2 1 の言語コードを取得する (S 1 3 5)。

[0102] そしてカードリーダ暗号処理部 7 2 は、このようにして取得した暗号化した P A N (以下、これを暗号化 P A N 1 8 1 A と呼ぶ) と、言語コード 1 8 2 と、その他の F I T レコード情報 1 8 3 とを F I T 照合結果 1 8 4 として A T M 制御部 1 0 に送信する (S 1 3 6)。

[0103] また A T M 制御部 1 0 は、かかる F I T 照合結果 1 8 4 を受信すると (S 1 3 7)、受信した F I T 照合結果 1 8 4 をメモリ 3 1 (図 2) のデータ領域 3 1 B (図 2) に格納する (S 1 3 8)。

[0104] なお A T M 制御部 1 0 は、この後、このとき取得した F I T 照合結果 1 8 4 に含まれる言語コード 1 8 2 に基づいて、各種画面をその言語コード 1 8 2 に応じた言語で表示するよう表示部 1 9 (図 1) を制御する一方、F I T レコード情報 1 8 3 に含まれる P I N 長や P I N ブロックフォーマットなどの情報を暗号化キーパッド 1 4 に送信する。そして暗号化キーパッド 1 4 は

、このP I N長やP I Nブロックフォーマットに基づいて、取引時におけるP I Nの受付けや、P I Nの暗号化を行う。

[0105] (1-2-2-4) カード読取 (I C情報)

次に、図21に示すように、A T M制御部10がカードリーダ制御部70に対してI Cチップ読取要求を送信する (S140)。

[0106] カードリーダ制御部70は、このI Cチップ読取要求を受信すると (S141)、I Cカード21に実装されたI CチップからI C情報190をカード搬送・読取部71 (図3A)に読み取らせることにより、これを取得する (S142)。そしてカードリーダ制御部70は、このようにして取得したI C情報190のうち、機密にすべき情報 (P A N及び上述のディスクレシヨナリ (discretionary) 情報などであり、以下、これを機密I C情報と呼ぶ) 191をカードリーダ暗号処理部72に送信する (S143)。

[0107] カードリーダ暗号処理部72は、かかる機密I C情報191を受信すると (S144)、受信した機密I C情報191をメモリ91 (図3C)のデータ領域91B (図3C)に格納する (S145)。

[0108] そしてカードリーダ暗号処理部72は、この後、機密I C情報191のマスク化及び暗号化をそれぞれ行い (S146, S147)、かかるマスク化された機密I C情報191 (以下、これをマスク化機密I C情報191Aと呼ぶ) と、かかる暗号化された機密I C情報191 (以下、これを暗号化機密I C情報191Bと呼ぶ) とをA T M制御部10にそれぞれ送信する (S148)。なお、ここでの「マスク化」及び「暗号化」とは、上述した磁気情報180の「マスク化」及び「暗号化」と同様である。

[0109] そしてA T M制御部10は、かかるマスク化機密I C情報191A及び暗号化機密I C情報191Bを受信すると (S149)、これらをメモリ31 (図2)のデータ領域31B (図2)に格納する (S150)。

[0110] (1-2-2-5) P I N入力

次に、A T M制御部10は、図22に示すように、暗号化キーパッド14にP I N入力受付要求を送信する (S160)。そして、暗号化キーパッド

14は、このPIN入力受付要求を受信すると（S161）、PIN入力受付処理を開始して、利用者にPINを入力すべき旨の操作指示画面を表示部19（図1）に表示させ、その後、利用者が暗号化キーパッド14のキーパッド111（図4A）のキーを押下してPINを入力するのを待ち受ける。

[0111] そして暗号化キーパッド14は、利用者がキーパッド111のキーを押下するごとに、キーが押下された旨の情報（以下、これをキー押下情報と呼ぶ）200をATM制御部10に送信する（S162）。なお、このステップS162では、暗号化キーパッド14からはキーが押下されたという情報（以下、これをキー押下情報200と呼ぶ）のみがATM制御部10に通知され、どのキーが押されたかという情報はATM制御部10に通知されない。

[0112] また、このときATM制御部10は、かかるキー押下情報200を受信すると（S163）、必要に応じて利用者がPINを何桁目まで入力したかという情報をATM画面に表示させる。

[0113] そして暗号化キーパッド14は、やがてキーパッド111の確定キーが押下され又は入力されたPINが指定桁数に到達するなどにより利用者によるPINの入力が完了すると、PINの入力が完了した旨の通知（以下、これを入力完了通知と呼ぶ）をATM制御部10に送信する（S164）。かくしてATM制御部10は、この入力完了通知に基づいてPIN入力が完了したことを認識する（S165）。ただしATM制御部10が入力された桁数からPIN入力完了を判断するようにしてもよい。また暗号化キーパッド14は、この後、そのとき利用者が入力したPINをメモリ121（図4B）のデータ領域121B（図4B）に格納する（S166）。

[0114] ATM制御部10は、この後、暗号化したPINの転送を暗号化キーパッド14に要求（以下、この要求を暗号化PIN転送要求と呼ぶ）する（S167）。この際、PINの暗号化方式の中にはPANを必要とするものがあるため、暗号化PAN181Aをかかると暗号化PIN転送要求と併せて送付する。この暗号化PAN181Aは、図20について上述した処理のステップS138でATM制御部10がメモリ31（図2）のデータ領域31B（

図2)に格納しておいたF I T照合結果184(図20)に含まれているものである。

[0115] 暗号化キーパッド14側では、かかる暗号化P I N転送要求を受信すると(S168)、必要に応じて暗号化P A N181Aを復号し(S169)、復号したP A Nを使用してP I Nを暗号化する(S170)。そして暗号化キーパッド14は、暗号化したP I N(以下、これを暗号化P I Nと呼ぶ)201をA T M制御部10に送信する(S171)。

[0116] またA T M制御部10は、かかる暗号化P I N201を受信すると(S172)、この暗号化P I N201をメモリ31(図2)のデータ領域31B(図2)に格納する(S173)。

[0117] (1-2-2-6)取引金額入力

この後、A T M制御部10は、図23に示すように、暗号化キーパッド14に対して利用者取引金額を入力させるべき旨の金額入力要求を送信する(S180)。そして暗号化キーパッド14は、この金額入力要求を受信すると(S181)、金額入力処理を開始して、利用者取引金額を入力すべき旨の操作指示画面を表示部19(図1)に表示させ、その利用者がキーパッド111(図4A)のキーを押下して取引金額を入力するのを待ち受ける。

[0118] そして暗号化キーパッド14は、利用者がキーパッド111のキーを押下するごとに、押下されたキーの値を押下キー情報210としてA T M制御部10に通知する(S182)。またA T M制御部10は、かかる押下キー情報210を受信すると(S183)、この押下キー情報210に基づいて、そのときまでに利用者が入力した取引金額を金額情報としてA T M画面に表示させる。

[0119] そして暗号化キーパッド14は、やがてキーパッド111の確定キーが押下されることにより利用者による取引金額の入力が完了すると、その旨の通知(入力完了通知)をA T M制御部10に通知する(S184)。かくしてA T M制御部10は、この入力完了通知に基づいて取引金額の入力が完了し

たことを認識する（S 1 8 5）。

[0120] そしてA T M制御部 1 0は、この後、利用者により入力された取引金額を金額情報 2 1 1としてメモリ 3 1（図 2）のデータ領域 3 1 B（図 2）に格納する（S 1 8 6）。

[0121] （1－2－2－7）カード認証データ要求

続いて、A T M制御部 1 0は、図 2 4に示すように、カードリーダ制御部 7 0経由でI Cカード 2 1に対してカード認証データを作成すべき旨のカード認証データ作成要求を送信する（S 1 9 0）。この際、A T M制御部 1 0は、かかるカード認証データの作成に必要な取引金額等の情報 2 2 0をカード認証データ作成要求と共にI Cカード 2 1に送信する。

[0122] I Cカード 2 1は、かかるカード認証データ作成要求を受信すると（S 1 9 1）、当該カード認証データ作成要求と共に送信されてきた情報 2 2 0を利用して、カード認証データ 2 2 1を作成する（S 1 9 2）。そしてI Cカード 2 1は、作成したカード認証データ 2 2 1をカードリーダ制御部 7 0経由でA T M制御部 1 0に送信する（S 1 9 3）。

[0123] またA T M制御部 1 0は、かかるカード認証データ 2 2 1を受信すると（S 1 9 4）、そのカード認証データ 2 2 1をメモリ 3 1（図 2）のデータ領域 3 1 B（図 2）に格納する（S 1 9 5）。

[0124] （1－2－2－8）取引要求

次いで、A T M制御部 1 0は、図 2 5に示すように、これまでの処理でメモリ 3 1のデータ領域 3 1 Bに格納されているマスク化磁気情報 1 8 0 A、暗号化磁気情報 1 8 0 B、マスク化機密I C情報 1 9 1 A、暗号化機密I C情報 1 9 1 B、金額情報 2 1 1及びカード認証データ 2 2 1などの情報から、勘定系ホストコンピュータ 3に対する取引要求電文 2 3 0を作成し（S 2 0 0）、作成した取引要求電文 2 3 0を勘定系ホストコンピュータ 3に送信する（S 2 0 1）。

[0125] また勘定系ホストコンピュータ 3は、かかる取引要求電文 2 3 0を受信すると（S 2 0 2）、受信した取引要求電文 2 3 0に含まれる暗号化磁気情報

180B及び暗号化機密IC情報191Bをそれぞれ復号し(S203)、かかる復号により得られた磁気情報180及びIC情報190などを用いて取引要求電文231を作成し直す(S204)。

[0126] そして勘定系ホストコンピュータ3は、作成し直した取引要求電文231を外部ネットワーク232経由でカードブランド・イシュア(図示せず)に送信する(S205)。

[0127] (1-2-2-9) 取引応答

この後、勘定系ホストコンピュータ3は、図26に示すように、外部ネットワーク232経由でカードブランド・イシュア(図示せず)から上述の取引要求電文231に対する取引応答電文240を受信する(S210)。この取引応答電文240には、金額情報241及びイシュア認証データ242等が含まれる。

[0128] そして勘定系ホストコンピュータ3は、かかる取引応答電文240を受信すると、その情報から、ATM制御部10に対する取引応答電文243を作成し直し(S211)、作成し直した取引応答電文243をATM制御部10に送信する(S212)。なお、この取引応答電文243には、金額情報241及びイシュア認証データ242が含まれる。

[0129] ATM制御部10は、かかる取引応答電文243を受信すると(S213)、当該取引応答電文243に含まれる金額情報241及びイシュア認証データ242等の電文情報をメモリ31(図2)のデータ領域31B(図2)に格納する(S214)。

[0130] (1-2-2-10) イシュア認証及び出金

この後、ATM制御部10は、図27に示すように、イシュア認証データ242と、イシュア認証を要求するイシュア認証要求とをカードリーダー制御部70経由でICカード21に送信する(S220)。

[0131] ICカード21は、かかるイシュア認証データ242及びイシュア認証要求を受信すると(S221)、イシュア認証を実施する(S222)。そしてICカード21は、実行したイシュア認証の認証結果をイシュア認証結果

244としてATM制御部10に送信する(S223)。

[0132] ATM制御部10は、かかるイシュア認証結果244を受信すると(S224)、イシュア認証が成功したか否かを判定し、イシュア認証が成功であった場合には、出金すべき金額を含む出金情報245及び出金要求を紙幣処理部12に送信する(S225)。そして紙幣処理部12は、かかる出金要求を受信すると、そのとき受信した出金情報に基づく金額を出金する(S226)。

[0133] (1-3) 本実施の形態の効果

以上のように本実施の形態の自動取引システム1では、カードリーダー13のカードリーダー暗号処理部72(図3C)がFIT157(図7A)を保持し、当該FIT157を参照して、ICカード21から読み取ったカード情報(磁気情報180(図19)及び機密IC情報191(図21))のうちのPANを含む機密情報を暗号化した上で、必要なカード情報をATM制御部10を介して勘定系ホストコンピュータ3に送信する。

[0134] 従って、本実施の形態によれば、仮にATM2のATM制御部10がマルウェアに感染してカード情報が外部に流出したとしても、機密情報が暗号化されているため、偽造カードの作成や不正なネットショッピングの利用に必要なPANの漏洩を防止することができ、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。

[0135] また本実施の形態によれば、ATM制御部10が暗号化されていないカード番号を取り扱わなくなるため、PCIDSS(Payment Card Industry Data Security Standards)の認定を受ける際の検査対象からATM制御部10を外すことができ、その分、ATM2がPCIDSSの認定を受け易くなるという効果をも得ることができる。

[0136] (2) 第2の実施の形態

第1の実施の形態では、FIT157(図7A)をカードリーダー暗号処理部72で処理する方式を説明した。FIT157が持つ金融機関番号が機密に該当しない桁のみに限定できるという条件で、ATM制御部10にFIT

157を持たせることができる。以下ではこのケースを第2の実施の形態として、ICカード21を用いて取引を実施する手順を第1の実施の形態と異なる箇所についてのみ説明する。

[0137] (2-1) 本実施の形態による自動取引システムの構成

図1との対応部分に同一符号を付して示す図28は、第2の実施の形態による自動取引システム250を示す。この自動取引システム250は、勘定系ホストコンピュータ251と、ATM252のATM制御部253及びカードリーダ254の一部処理に関する機能が異なる点を除いて第1の実施の形態による自動取引システム1(図1)と同様に構成されている。

[0138] この場合、勘定系ホストコンピュータ251は、そのCPU150(図6)がメモリ151に格納されたホストアプリケーション152(図6)に基づいて実行する図29について後述するFIT更新に関する処理の処理内容と、図30について後述するFIT照合に関する処理の処理内容とが異なる点を除いて第1の実施の形態の勘定系ホストコンピュータ3と同様の構成を有する。

[0139] またATM252は、ATM制御部253のCPU30(図2)がメモリ31に格納されたATMアプリケーション40(図2)に基づいて実行する図29及び図30について後述する処理の処理内容と、カードリーダ254のカードリーダ暗号処理部255(図29)のCPU90(図3C)がメモリ91(図3C)に格納されたアプリケーション92(図3C)に基づいて実行する図29及び図30について後述する処理の処理内容とが異なる点を除いて第1の実施の形態のATM2と同様の構成を有する。

[0140] (2-2) FIT更新

図29は、図18について上述した第1の実施の形態のFIT更新処理に代えて本実施の形態の自動取引システム250において実行されるFIT更新処理の処理手順を示す。本実施の形態の場合、図29に示すように、第1の実施の形態と同様、FIT157は勘定系ホストコンピュータ251(図28)にて用意されるが、FIT157が更新された場合などはATM25

2（図28）が持つF I T 1 5 7を更新して同期を取る必要がある。

[0141] そこで、本実施の形態において、勘定系ホストコンピュータ251は、更新されたF I T 1 5 7をA T M 2 5 2のA T M制御部253に送信する（S 2 5 0）。A T M制御部253は、このF I T 1 5 7を受信すると（S 2 5 1）、受信した更新後のF I T 1 5 7をメモリ31（図2）のデータ領域31B（図2）及び図示しないA T M 2 5 2内のハードディスク装置等からなる外部記憶装置に格納する（S 2 5 2）。

[0142] またA T M制御部253は、図7Bに示すように、このF I T 1 5 7に含まれる金融機関ごとに固有な各種情報のうちの機密情報に関連する項目（ここでは各金融機関のレコード160（図7A）のレコード情報のうち、金融機関IDオフセット、金融機関ID、PANオフセット、PAN長及び言語コードオフセット）の各情報161, 162, 164, 165, 166を金融機関ごとにそれぞれ抜粋してこれらそれぞれその金融機関のレコード160Aとすることにより、F I T 1 5 7のサブセットとなるF I T機密関連テーブル157Aを作成する（S 2 5 3）。そしてA T M制御部253は、このようにして作成したF I T機密関連テーブル157Aをカードリーダー254（図28）に送信する（S 2 5 4）。

[0143] カードリーダー254は、かかるF I T機密関連テーブル157Aをカードリーダー暗号処理部255がカードリーダー制御部70経由で受信し（S 2 5 5）、受信したF I T機密関連テーブル157Aをメモリ91（図3C）のデータ領域91B（図3C）に格納する（S 2 5 6）。

[0144] （2-3）F I T照合

一方、図30は、図20について上述した第1の実施の形態のF I T照合処理に代えて本実施の形態の自動取引システム250において実行されるF I T照合処理の処理手順を示す。

[0145] 本実施の形態の場合、A T M制御部253は、マスク化磁気情報180AをF I T 1 5 7と照合する（S 2 6 0）。照合結果より、該当する金融機関のレコード160の機密データ（ここではPAN及び言語コード）以外のレ

コード情報を取得する（S261）。またATM制御部253は、ステップS260の参照結果に基づいて、FIT157に登録された各金融機関のレコード160のうち、該当する金融機関のレコード160が何番目のレコードであるかを表す番号でなるテーブルインデックス300をカードリーダ254（図28）に送信し、該当するレコード160に含まれる機密データの取得を要求する（S262）。

[0146] カードリーダ254のカードリーダ暗号処理部255は、かかる要求をカードリーダ制御部70経由で受信すると（S263）、機密データの取得処理を開始し、まず磁気情報180をFIT機密関連テーブル157A（図7B）と照合することにより、FIT機密関連テーブル157A上のかかるテーブルインデックス300に対応するレコード160AからPANのオフセットの情報164（図7B）を取得する（S264）。またカードリーダ暗号処理部255は、取得したPANオフセットの情報164を用いて、磁気情報180上にあるPAN及び言語コードを取得し、取得したPANを暗号化することにより暗号化PAN181Aを生成する（S265）。

[0147] さらにカードリーダ暗号処理部255は、FIT機密関連テーブル157Aから取得した言語コードオフセットの情報166（図7B）を用いて、磁気情報180から言語コード182を取得する（S266）。そしてカードリーダ暗号処理部255は、このように生成又は取得した暗号化PAN181A及び言語コード182をATM制御部253に送信する（S267）。

[0148] ATM制御部253は、カードリーダ制御部70を介してこれらの暗号化PAN181A及び言語コード182を受信すると（S268）、受信した暗号化PAN181A、言語コード182、及びその他のFIT157及びFIT機密関連テーブル157Aを照合した結果259をメモリ31（図2）のデータ領域31B（図2）に格納する（S269）。

[0149] （2-4）本実施の形態の効果

以上のように本実施の形態の自動取引システム250では、カードリーダ254（図28）のカードリーダ暗号処理部255が、FIT157に代え

て、F I T 1 5 7に含まれる各種情報1 6 1～1 6 7のうち、機密情報を取得するための情報1 6 1, 1 6 2, 1 6 4～1 6 6のみを抜粋したF I T機密関連テーブル1 5 7 Aを保持し、このF I T機密関連テーブル1 5 7 Aに基づいてI Cカード2 1から読み出した磁気情報1 8 0からP A Nを取得し、取得したP A Nを暗号してA T M制御部2 5 3に送信する。また、A T M制御部2 5 3は、F I T 1 5 7を保持し、このF I T 1 5 7を参照してマスク化磁気情報1 8 0 Aから取得可能なカード情報を取得する。

[0150] この場合、F I T機密関連テーブル1 5 7 Aのデータ量は、F I T 1 5 7のデータ量と比べて格段的に少ない。従って、本実施の形態の自動取引システム2 5 0によれば、第1の実施の形態の自動取引システム1により得られる効果に加えて、カードリーダ2 5 4のカードリーダ暗号処理部2 5 5がI Cカード2 1からP A Nを取得する際に必要なテーブルを保持するためのメモリ9 1（図3 C）のメモリ容量を低減させることができるという効果をも得ることができる。

[0151] また本自動取引システム2 5 0では、上述のようにカードリーダ暗号処理部2 5 5からP A Nと言語コードのみを取得すれば良く、磁気情報1 8 0からカード情報を取得する処理をカードリーダ暗号処理部2 5 5と、A T M制御部2 5 3とで分担することになるため結果的に、カードリーダ暗号処理部2 5 5の処理負荷を低減し、カード情報の取得に関するカードリーダ暗号処理部2 5 5の処理時間を低減させることができる。

[0152] （3）第3の実施の形態

（3－1）本実施の形態による自動取引システムの概要及び構成

次に、図3 1～図3 7を参照して、本実施の形態による自動取引システム2 6 0（図3 1）について説明する。本実施の形態の自動取引システム2 6 0は、C R－ホストマスタ鍵1 0 3（図3 3）を勘定系ホストコンピュータ2 6 1で生成し、生成したC R－ホストマスタ鍵1 0 3を勘定系ホストコンピュータ2 6 1からA T M 2 6 2のカードリーダ2 6 3に送付する点を特徴とし、他の部分は第1の実施の形態の自動取引システム1（図1）と同様に

構成されている。

[0153] このため図3Cとの対応部分に同一符号を付して示す図32に示すように、本実施の形態のカードリーダ263のカードリーダ暗号処理部270は、後述する各種処理の過程において、図3Cのホスト公開鍵100に代えてホスト検証鍵271をメモリ91のデータ領域91Bに適宜保持すると共に、CR秘密鍵272及びCR公開鍵273をメモリ91のデータ領域91Bに適宜保持する。これ以外のカードリーダ263の構成は、図34～図37の処理に関するアプリケーション275（図32）の機能を除いて第1の実施の形態のカードリーダ13（図1）と同様である。

[0154] また本実施の形態の勘定系ホストコンピュータ261は、図6との対応部分に同一符号を付して示す図33に示すように、後述する各種処理の過程において、図6のホスト秘密鍵107、ホスト公開鍵100、ホスト公開鍵署名108及びCR検証鍵97に代えて、ホスト署名鍵280、ホスト検証鍵281及びホスト検証鍵署名282をメモリ151のデータ領域151Bに保持する。これ以外の勘定系ホストコンピュータ261の構成は、図34～図37の処理に関するアプリケーション283（図33）の機能を除いて第1の実施の形態の勘定系ホストコンピュータ3（図1）と同様である。

[0155] さらに認証局264（図31）のCPU170がメモリ171に格納されたアプリケーション172に基づいて実行する図34～図37の処理の処理内容の一部も第1の実施の形態と異なっているが、これ以外の処理内容は第1の実施の形態の認証局5と同様である。

[0156] （3-2）ルート鍵ペア及びCR鍵ペアの初期設定の流れ

図34は、図9に代えて本実施の形態の自動取引システム260（図31）において実行される初期鍵（ルート鍵ペア及びCR鍵ペア）の設定手順の流れを示す。

[0157] かかる初期鍵の設定を行う場合、まず、本自動取引システム260におけるセキュアな取引の責任元（主にATMベンダを想定）がセキュアな環境である認証局264において、非対称暗号鍵であるルート鍵ペア（ルート署名鍵

１０９及びルート検証鍵９５）を生成する（Ｓ２７０）。そして認証局２６４は、このとき生成したこれらルート署名鍵１０９及びルート検証鍵９５を認証局２６４のメモリ１７１（図８）のデータ領域１７１Ｂに格納する（Ｓ２７１）。

[0158] またＡＴＭ２６２（図３１）側では、カードリーダー２６３（図３１）のカードリーダー暗号処理部２７０（図３２）において、非対称暗号鍵であるＣＲ鍵ペア（ＣＲ秘密鍵２７２及びＣＲ公開鍵２７３）を生成する（Ｓ２７２）。そしてカードリーダー暗号処理部２７０は、生成したＣＲ秘密鍵２７２及びＣＲ公開鍵２７３をメモリ９１（図３２）のデータ領域９１Ｂ（図３２）に格納する（Ｓ２７３）。この後、カードリーダー暗号処理部２７０は、ＣＲ公開鍵２７３に対して、ルート署名鍵１０９を用いて電子署名を付与するため、ＣＲ公開鍵２７３を認証局２６４に送信する（Ｓ２７４）。

[0159] 認証局２６４は、かかるＣＲ公開鍵２７３を受信すると（Ｓ２７５）、ステップＳ２７０で生成したルート署名鍵１０９を用いてＣＲ公開鍵２７３に電子署名を付与する（Ｓ２７６）。また認証局２６４は、付与した電子署名であるＣＲ公開鍵署名２７４及びルート検証鍵９５をカードリーダー暗号処理部２７０に送信する（Ｓ２７７）。

[0160] そしてカードリーダー暗号処理部２７０は、これらＣＲ公開鍵署名２７４及びルート検証鍵９５を受信すると（Ｓ２７８）、これらをメモリ９１（図３２）のデータ領域９１Ｂ（図３２）に格納する（Ｓ２７９）。

[0161] （３－３）暗号鍵（ホスト鍵）の初期設定の流れ

一方、図３５は、図１１に代えて本実施の形態の自動取引システム２６０（図３１）において実行される初期鍵（ホスト鍵）の設定手順の流れを示す。

[0162] 図３４について上述したルート署名鍵１０９及びルート検証鍵９５を認証局２６４が生成後、まず、勘定系ホストコンピュータ２６１が非対称暗号鍵であるホスト鍵ペア（ホスト署名鍵２８０及びホスト検証鍵２８１）を生成する（Ｓ２８０）。そして勘定系ホストコンピュータ２６１は、生成したホ

スト署名鍵 280 及びホスト検証鍵 281 をメモリ 151 (図 33) のデータ領域 151B (図 33) に格納する (S281)。

[0163] また勘定系ホストコンピュータ 261 は、ルート署名鍵 109 を用いて電子署名を付与するため、ホスト検証鍵 281 を認証局 264 に送信する (S282)。

[0164] 認証局 264 は、かかるホスト検証鍵 281 を受信すると (S283)、ルート署名鍵 109 を用いてホスト検証鍵 281 に電子署名を付与する (S284)。また認証局 264 は、このときホスト検証鍵 281 に付与した電子署名であるホスト検証鍵署名 282 及びルート検証鍵 95 を勘定系ホストコンピュータ 261 に送信する (S285)。

[0165] そして勘定系ホストコンピュータ 261 は、かかるホスト検証鍵署名 282 及びルート検証鍵 95 を受信すると (S286)、これらをメモリ 151 (図 33) のデータ領域 151B (図 33) に格納する (S287)。

[0166] (3-4) マスタ鍵交換 (CR-ホスト)

図 36 及び図 37 は、図 14 及び図 15 に代えて本実施の形態による自動取引システム 260 (図 31) において、カードリーダー 263 及び勘定系ホストコンピュータ 261 間でマスタキーを共有するために実行される処理の流れを示す。この場合、まずカードリーダー暗号処理部 270 が、CR 公開鍵 273 及び CR 公開鍵署名 274 を勘定系ホストコンピュータ 261 に送信する (S290)。

[0167] 勘定系ホストコンピュータ 261 は、かかる CR 公開鍵 273 と CR 公開鍵署名 274 を受信すると (S291)、CR 公開鍵署名 274 の署名の正当性をルート検証鍵 95 を用いて検証し (S292)、正当性が検証されれば CR 公開鍵 273 をメモリ 151 (図 33) のデータ領域 151B (図 33) に格納する (S293)。また勘定系ホストコンピュータ 261 は、この後、ホスト検証鍵 281 及びホスト検証鍵署名 282 をカードリーダー暗号処理部 270 に送信する (S294)。

[0168] カードリーダー暗号処理部 270 は、かかるホスト検証鍵 281 及びホスト

検証鍵署名 282 を受信すると (S 295)、ホスト検証鍵署名 282 の署名の正当性をルート検証鍵 95 を用いて検証し (S 296)、正当性が検証されればホスト検証鍵 281 をメモリ 91 (図 32) のデータ領域 91 B (図 32) に格納する (S 297)。

[0169] この後、図 37 に示すように、勘定系ホストコンピュータ 261 は、乱数により CR-ホストマスタ鍵 103 を生成し (S 300)、生成した CR-ホストマスタ鍵 103 をメモリ 91 (図 32) のデータ領域 91 B (図 32) に格納する (S 301)。

[0170] さらに勘定系ホストコンピュータ 261 は、CR 公開鍵 273 を用いて CR-ホストマスタ鍵 103 を暗号化すると共に、暗号化した CR-ホストマスタ鍵 103 (以下、これを暗号化 CR-ホストマスタ鍵 103 A と呼ぶ) に対してホスト署名鍵 280 を用いて電子署名を付与し (S 302)、この後、これらの暗号化 CR-ホストマスタ鍵 103 A 及び電子署名をカードリーダー暗号処理部 270 に送信する (S 303)。

[0171] カードリーダー暗号処理部 270 は、暗号化 CR-ホストマスタ鍵 103 A 及び電子署名を受信すると (S 304)、まず、その電子署名の正当性をホスト検証鍵 281 を用いて検証する (S 305)。そしてカードリーダー暗号処理部 270 は、かかる電子署名の正当性を検証できた場合、暗号化 CR-ホストマスタ鍵 103 A を CR 秘密鍵 272 を用いて復号し (S 306)、かくして得られた復号された CR-ホストマスタ鍵 103 をメモリ 91 (図 32) のデータ領域 91 B (図 32) に格納する (S 307)。

[0172] 続くセッション鍵の生成についても、第 1 の実施の形態 (図 17) ではカードリーダー暗号処理部 72 にて CR-ホストセッション鍵を生成し、これをホストコンピュータ 3 に送信することで CR-ホストセッション鍵の共有を行っているのに対し、第 3 の実施の形態ではホストコンピュータ 261 にて CR-ホストセッション鍵を生成し、暗号化し、カードリーダー暗号処理部 270 に送信し、カードリーダー暗号処理部 270 にて復号化した CR-ホストセッション鍵を、メモリ 91 に記憶することで、図 17 と同様に CR-ホス

トセッション鍵を共有する。

[0173] (3-5) 本実施の形態の効果

以上のように本実施の形態の自動取引システム260によれば、ATM262のカードリーダ263のカードリーダ暗号処理部270と、勘定系ホストコンピュータ261とが通信を行う際の暗号化に利用するCR-ホストセッション鍵104を共有する際、当該CR-ホストセッション鍵104を暗号化するのに利用するCR-ホストマスタ鍵103を勘定系ホストコンピュータ261で生成するため、複数のATM262との間のCR-ホストマスタ鍵103を勘定系ホストコンピュータ261において一括管理することができる。

[0174] 従って、第1の実施の形態のようにかかるCR-ホストマスタ鍵103を各ATM2(図1)のカードリーダ13(図1)のカードリーダ暗号処理部72(図3C)で生成する場合と比べてその管理が容易であり、また端末である各ATM262においてCR-ホストマスタ鍵103を管理する場合と比べてハッキングを受けたときのリスクを低減することができる。

[0175] (4) 他の実施の形態

なお上述の第1～第3の実施の形態においては、自動取引装置としてのATM2, 252, 262を図1、図28又は図31のように構成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、この他種々の構成を広く適用することができる。また、ATM2, 252, 262の取引としては、入金取引、出金取引、送金取引、残高確認などのカード認証後に行う取引きであってよい。

[0176] また上述の第1～第3の実施の形態においては、カード媒体がICカード21である場合について述べたが、本発明はこれに限らず、カード媒体が磁気カードの場合でも本発明を適用することができる。

[0177] さらに上述の第1～第3の実施の形態においては、取引要求電文230(図25)を生成して勘定系ホストコンピュータ3(ホスト装置)に送信し、当該勘定系ホストコンピュータ3からの取引応答電文243(図26)に基

づいて取引を行うための制御処理を実行する装置制御部としてのA T M制御部10, 253を図2、図28のように構成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、この他種々の構成を広く適用することができる。

[0178] さらに、上述の第1～第3の実施の形態においては、F I T 157、F I T機密関連テーブル157Aをテーブルとして説明したがその形式はテーブルに限るものではなく、上述の処理を実行する上で必要となる情報を関連付けた情報（例えば、金融機関毎のカード情報のフォーマットに関する情報）であればよい。

[0179] さらに上述の第2の実施の形態においては、F I T機密関連テーブル157Aを、各金融機関のレコード160Aのレコード情報のうち、金融機関I Dオフセット、金融機関I D、P A Nオフセット、P A N長及び言語コードオフセットの各情報161, 162, 164, 165, 167を金融機関ごとにそれぞれ抜粋して作成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、これらの情報161, 162, 164, 165, 167以外の情報を含ませるようにしても良い。

産業上の利用可能性

[0180] 本発明は、カード情報と、利用者の操作とに基づいて入出金取引を行うA T Mと、当該入出金取引の承認等を行う勘定系ホストコンピュータとを有する自動取引システムに適用することができる。

符号の説明

[0181] 1, 250, 260……自動取引システム、2, 252, 262……A T M、3, 251, 261……勘定系ホストコンピュータ、5, 264……認証局、10, 253……A T M制御部、13, 254, 263……カードリーダー、14……暗号化キーパッド、21……I Cカード、30, 90, 120, 150, 170……C P U、72……カードリーダー暗号処理部、110……暗号化キーパッド制御部、130……I C領域、140……磁気領域、157……F I T、157A……F I T機密関連テーブル。

請求の範囲

[請求項1]

自動取引装置及びホスト装置を有し、前記自動取引装置に対する利用者の操作に応じた取引の要求電文を前記自動取引装置から前記ホスト装置に送信し、前記要求電文に対する前記ホスト装置からの応答電文に基づいて前記自動取引装置が前記取引を行う自動取引システムにおいて、

前記自動取引装置は、

前記利用者により装填された前記カード媒体に記録された第1のカード情報を読み出すカードリーダと、

前記要求電文を生成して前記ホスト装置に送信し、前記ホスト装置からの前記応答電文に基づいて前記取引を行うための制御処理を実行する装置制御部と

を備え、

前記カードリーダは、

金融機関ごとに固有な、前記第1のカード情報のフォーマットに関する情報が登録された第1のカードフォーマット情報を保持し、

前記第1のカードフォーマット情報を参照して、前記カード媒体から読み出した前記第1のカード情報から前記カード番号を含む所定の機密情報を取得し、

取得した前記機密情報を暗号化して前記装置制御部に送信し、

前記装置制御部は、

前記カードリーダから送信されてきた暗号化された前記機密情報を含む前記要求電文を生成して前記ホスト装置に送信する

ことを特徴とする自動取引システム。

[請求項2]

キーパッドを有し、前記キーパッドを介して前記利用者が入力した暗証番号を暗号化して前記装置制御部に送信する暗号化キーパッドを備え、

前記カードリーダは、

前記機密情報のうちの暗号化した前記カード番号を前記装置制御部を経由して前記暗号化キーパッドに送信する

ことを特徴とする請求項 1 に記載の自動取引システム。

[請求項3]

前記第 1 のカードフォーマット情報には、前記第 1 のカード情報のフォーマットに関する情報の一部が登録され、

前記第 1 のカードフォーマット情報に登録された前記第 1 のカード情報のフォーマットに関する情報の一部は、前記金融機関ごとの前記機密情報を前記第 1 のカード情報から取得するのに必要な情報であり、

前記カードリーダは、

前記カード媒体から読み出した前記第 1 のカード情報のうちの前記機密情報を暗号化して前記装置制御部に送信すると共に、前記第 1 のカード情報のうちの前記機密情報をマスク化し、他の情報をマスク化していない第 2 のカード情報を前記装置制御部に送信し、

前記装置制御部は、

前記金融機関ごとの前記カード情報のフォーマットに関する情報が登録された第 2 のカードフォーマット情報を保持し、当該第 2 のカードフォーマット情報を参照して、前記第 2 のカード情報の中から必要な情報を取得する

ことを特徴とする請求項 1 に記載の自動取引システム。

[請求項4]

前記ホスト装置は、

前記自動取引装置の前記カードリーダとの間で通信を行う際の暗号化に利用するセッション鍵を暗号化するためのマスタ鍵を生成し、

生成した前記マスタ鍵を前記カードリーダと共有する

ことを特徴とする請求項 1 に記載の自動取引システム。

[請求項5]

自動取引装置及びホスト装置を有し、前記自動取引装置に対する利用者の操作に応じた取引の要求電文を前記自動取引装置から前記ホスト装置に送信し、前記要求電文に対する前記ホスト装置からの応答電

文に基づいて前記自動取引装置が前記取引を行う自動取引システムの制御方法において、

前記自動取引装置は、

前記利用者により装填された前記カード媒体に記録された第1のカード情報を読み出すカードリーダと、

前記要求電文を生成して前記ホスト装置に送信し、前記ホスト装置からの前記応答電文に基づいて前記取引を行うための制御処理を実行する装置制御部とを有し、

前記カードリーダは、

金融機関ごとに固有な、前記第1のカード情報のフォーマットに関する情報が登録された第1のカードフォーマット情報を保持し、

前記カードリーダが、前記第1のカードフォーマット情報を参照して、前記カード媒体から読み出した前記第1のカード情報から前記カード番号を含む所定の機密情報を取得する第1のステップと、

前記カードリーダが、取得した前記機密情報を暗号化して前記装置制御部に送信する第2のステップと、

前記装置制御部が、前記カードリーダから送信されてきた暗号化された前記機密情報を含む前記要求電文を生成して前記ホスト装置に送信する第3のステップと

を備えることを特徴とする自動取引システムの制御方法。

[請求項6]

前記自動取引システムは、

キーパッドを有し、前記キーパッドを介して前記利用者が入力した暗証番号を暗号化して前記装置制御部に送信する暗号化キーパッドを含み、

前記第2のステップにおいて、前記カードリーダは、

前記機密情報のうちの暗号化した前記カード番号を前記装置制御部を経由して前記暗号化キーパッドに送信する

ことを特徴とする請求項5に記載の自動取引システムの制御方法。

[請求項7] 前記第1のカードフォーマット情報には、前記第1のカード情報のフォーマットに関する情報の一部が登録され、

前記第1のカードフォーマット情報に登録された前記第1のカード情報のフォーマットに関する情報の一部は、前記金融機関ごとの前記機密情報を前記第1のカード情報から取得するのに必要な情報であり、

前記第2のステップにおいて、前記カードリーダは、

前記カード媒体から読み出した前記第1のカード情報のうちの前記機密情報を暗号化して前記装置制御部に送信すると共に、前記第1のカード情報のうちの前記機密情報をマスク化し、他の情報をマスク化していない第2のカード情報を前記装置制御部に送信し、

前記装置制御部は、

前記金融機関ごとに固有な、前記カード情報のフォーマットに関する情報が登録された第2のカードフォーマット情報を保持し、

前記第3のステップにおいて、前記装置制御部は、

前記第2のカードフォーマット情報を参照して、前記第2のカード情報の中から必要な情報を取得する

ことを特徴とする請求項5に記載の自動取引システムの制御方法。

[請求項8] 前記ホスト装置は、

前記自動取引装置のカードリーダとの間で通信を行う際の暗号化に利用するセッション鍵を暗号化するためのマスタ鍵を生成し、

生成した前記マスタ鍵を前記カードリーダと共有する

ことを特徴とする請求項5に記載の自動取引システムの制御方法。

[請求項9] 利用者の操作に応じた取引の要求電文を前記ホスト装置に送信し、前記要求電文に対する前記ホスト装置からの応答電文に基づいて前記取引を行う自動取引装置に設けられ、前記利用者により前記自動取引装置に装填されたカード媒体から当該カード媒体に記録されたカード情報を読み出すカードリーダにおいて、

前記自動取引装置に装填された前記カード媒体から前記カード情報を読み取るカード読取部と、

前記カード読取部により前記カード媒体から読み取られた前記カード情報を暗号化するカードリーダ暗号処理部と

を備え、

前記自動取引装置は、

前記要求電文を生成して前記ホスト装置に送信し、前記ホスト装置からの前記応答電文に基づいて前記取引を行うための制御処理を実行する装置制御部を有し、

前記カードリーダ暗号処理部は、

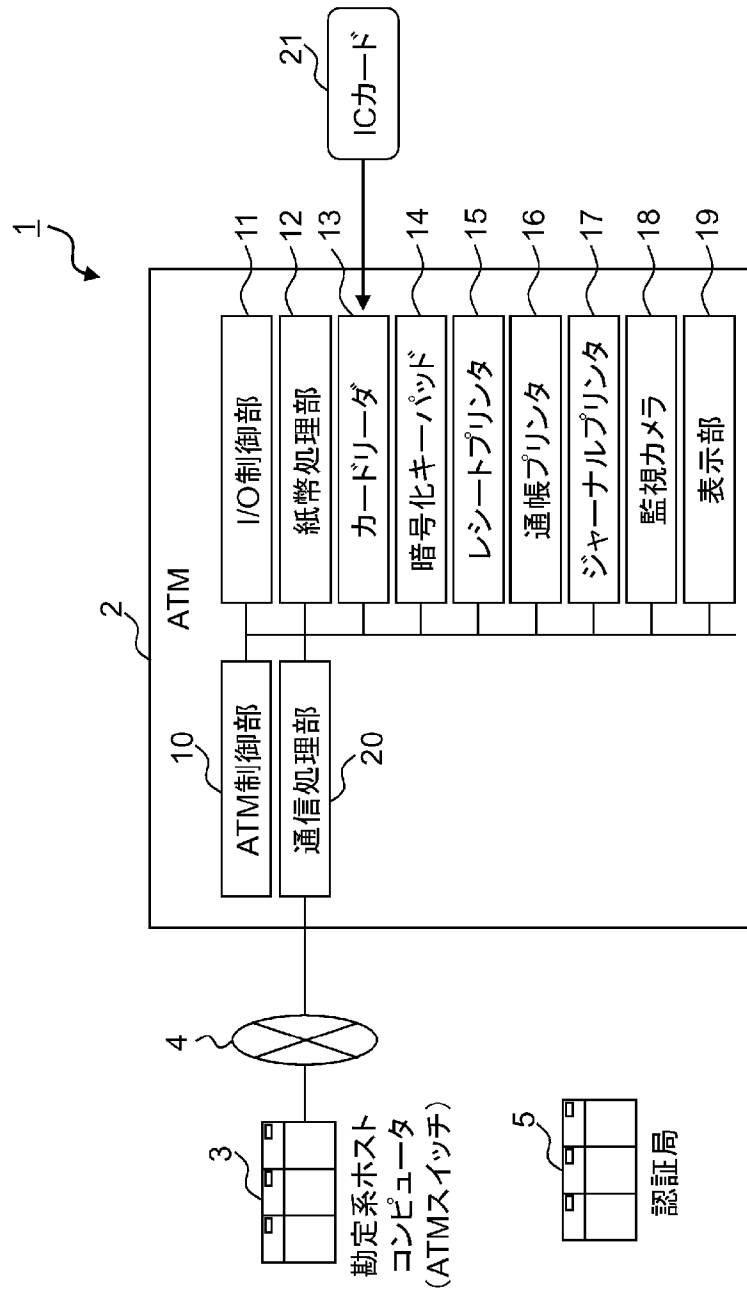
金融機関ごとに固有な、前記第1のカード情報のフォーマットに関する情報が登録された第1のカードフォーマット情報を保持し、

前記第1のカードフォーマット情報を参照して、前記カード媒体から読み出した前記第1のカード情報から前記カード番号を含む所定の機密情報を取得し、

取得した前記機密情報を暗号化して前記装置制御部に送信することを特徴とするカードリーダ。

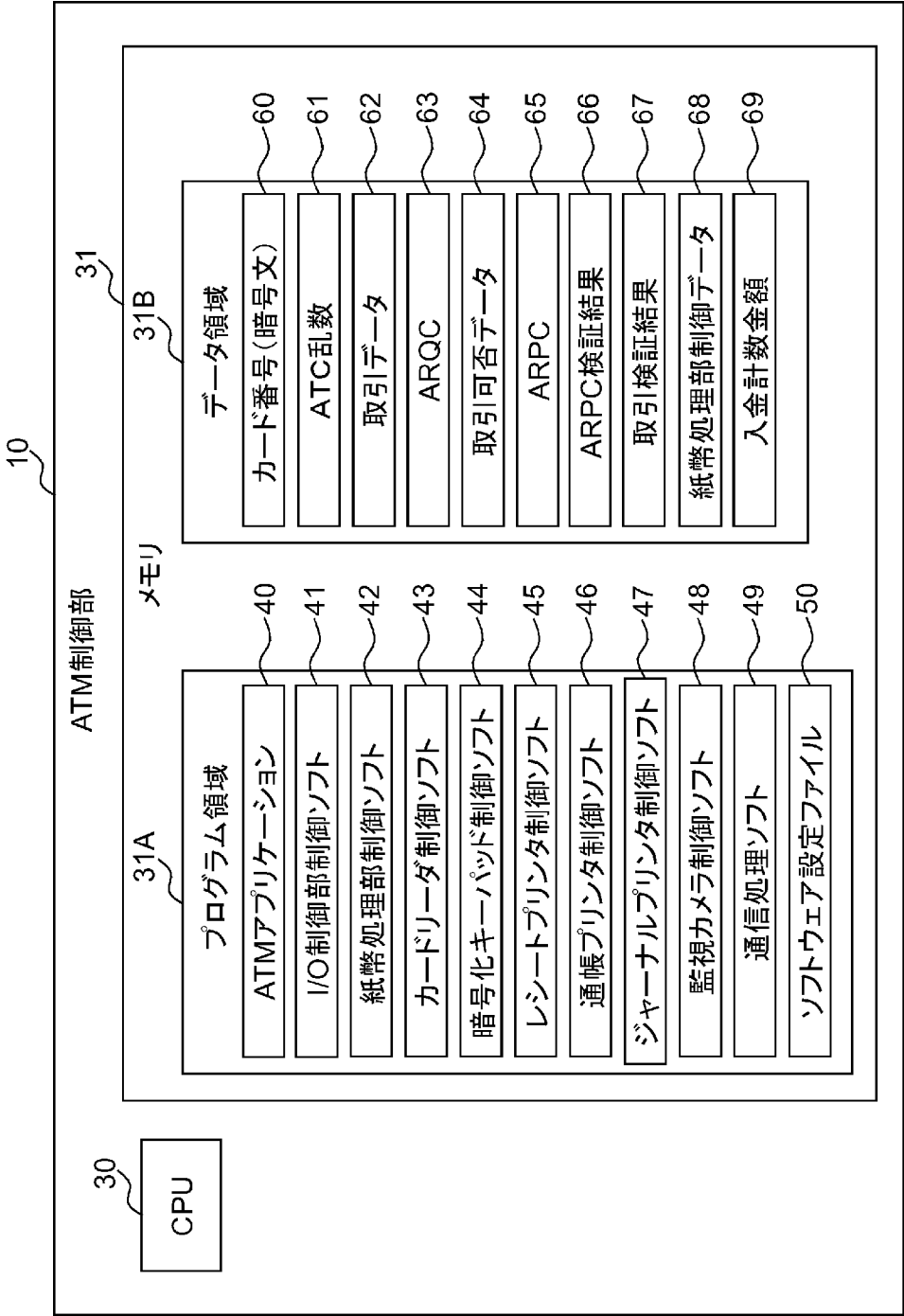
[図1]

図 1

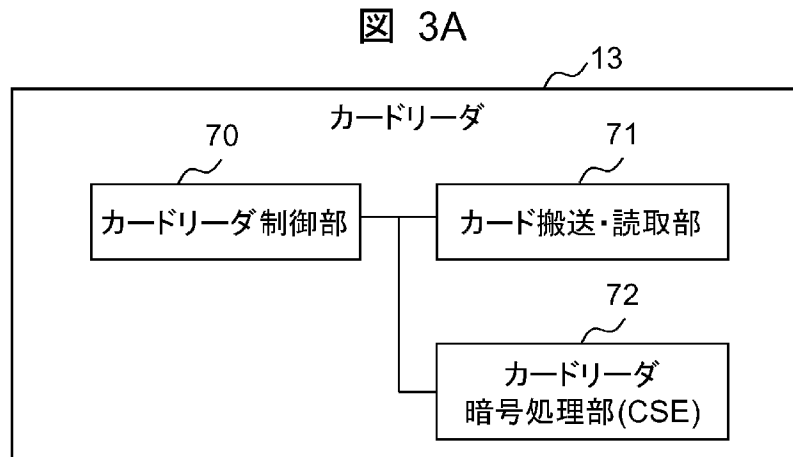


[図2]

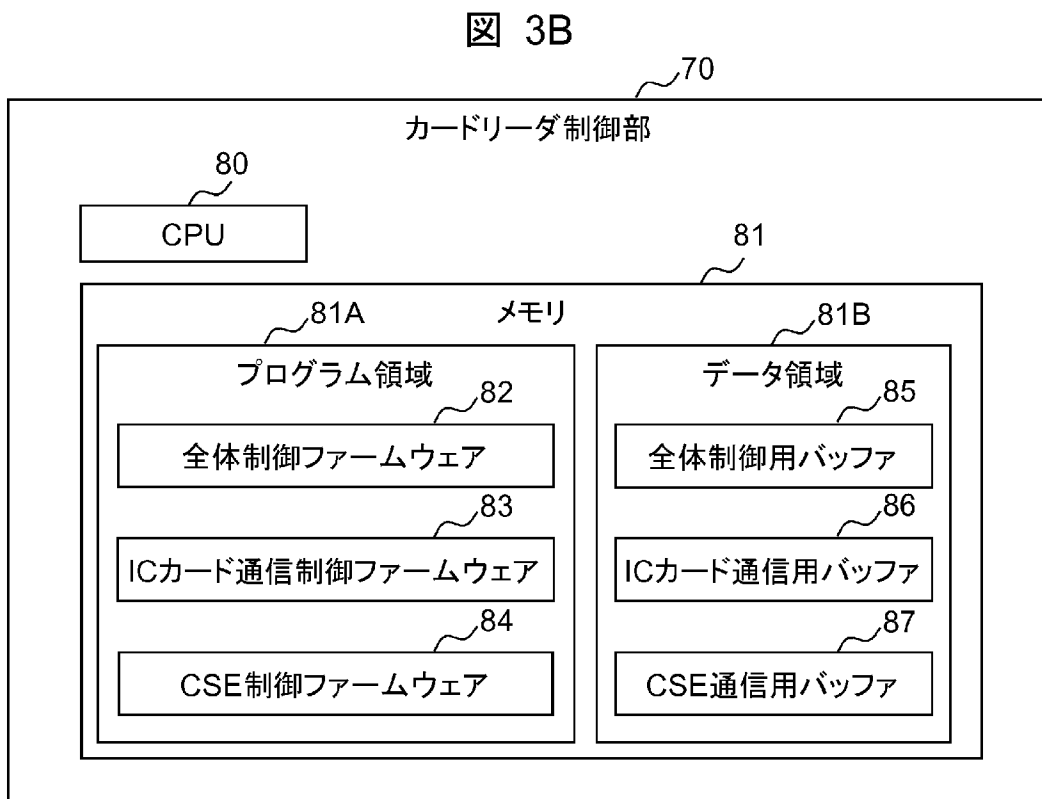
図 2



[図3A]

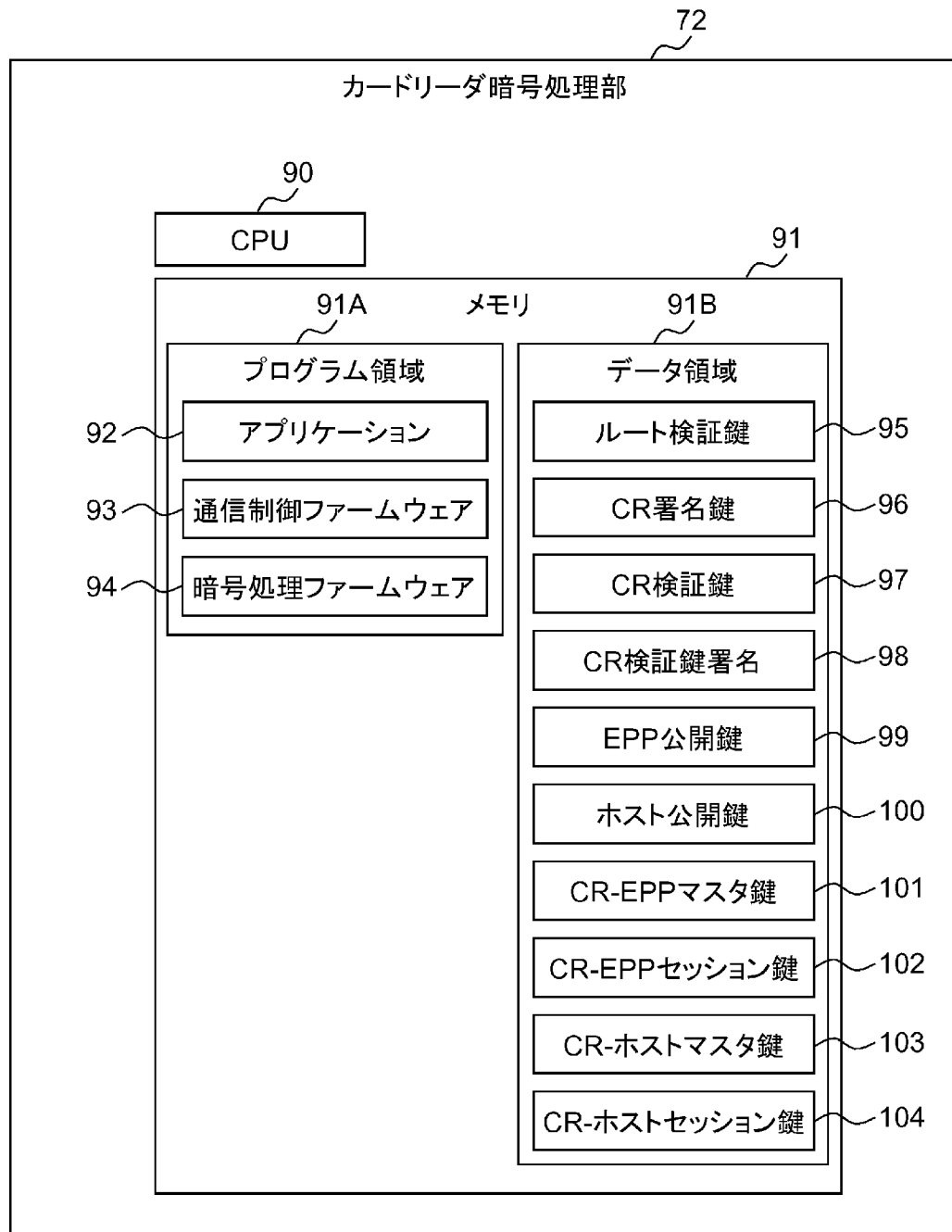


[図3B]



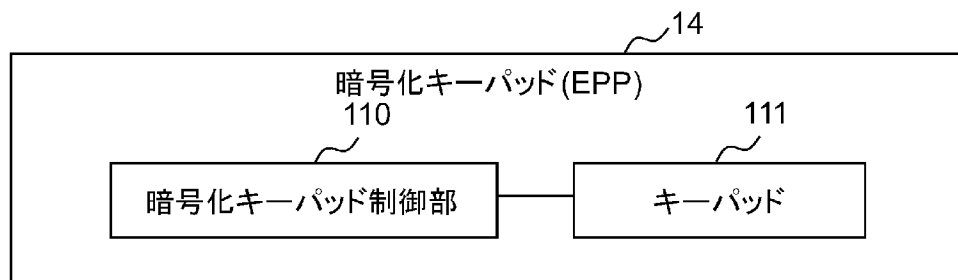
[図3C]

図 3C



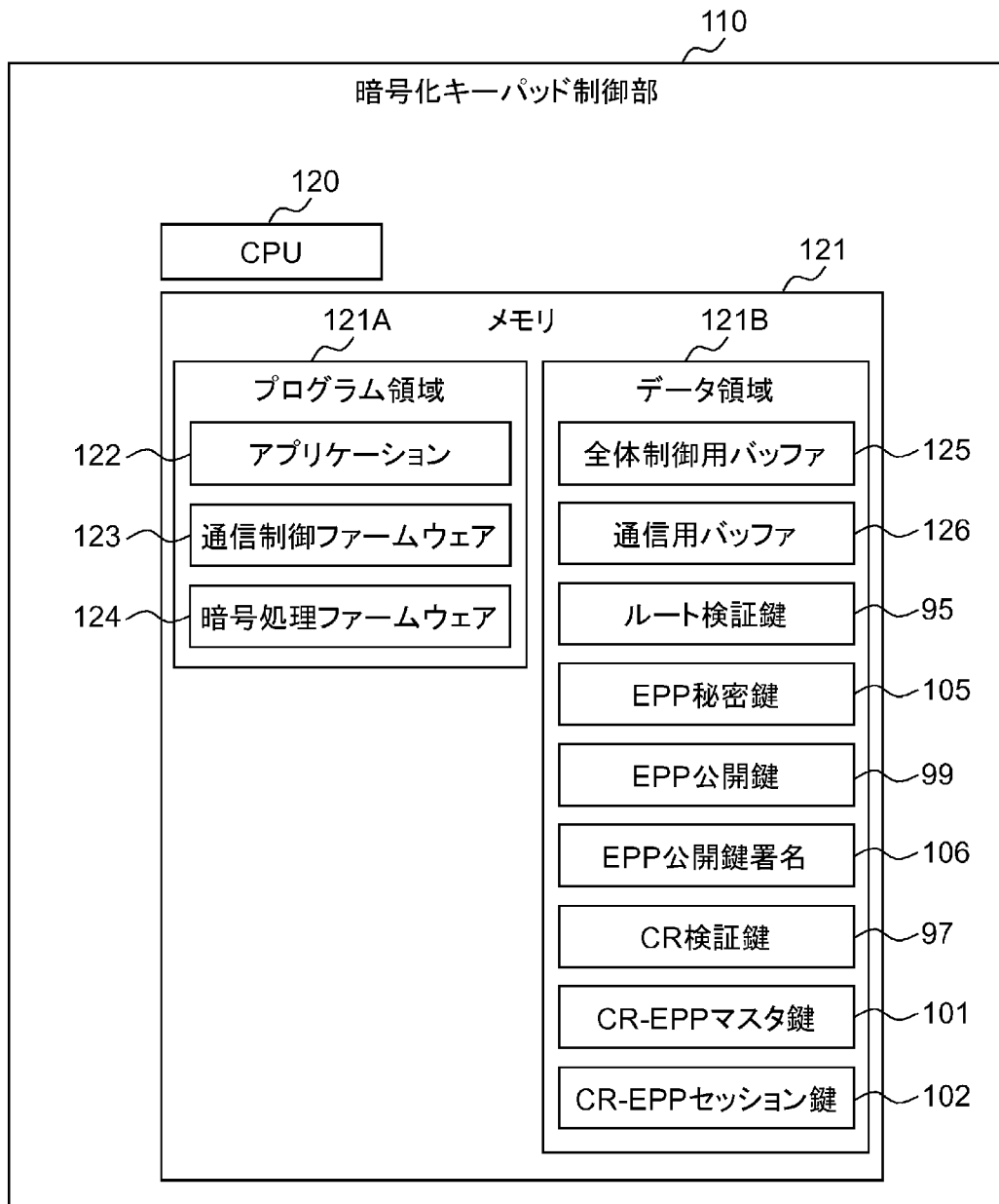
[図4A]

図 4A



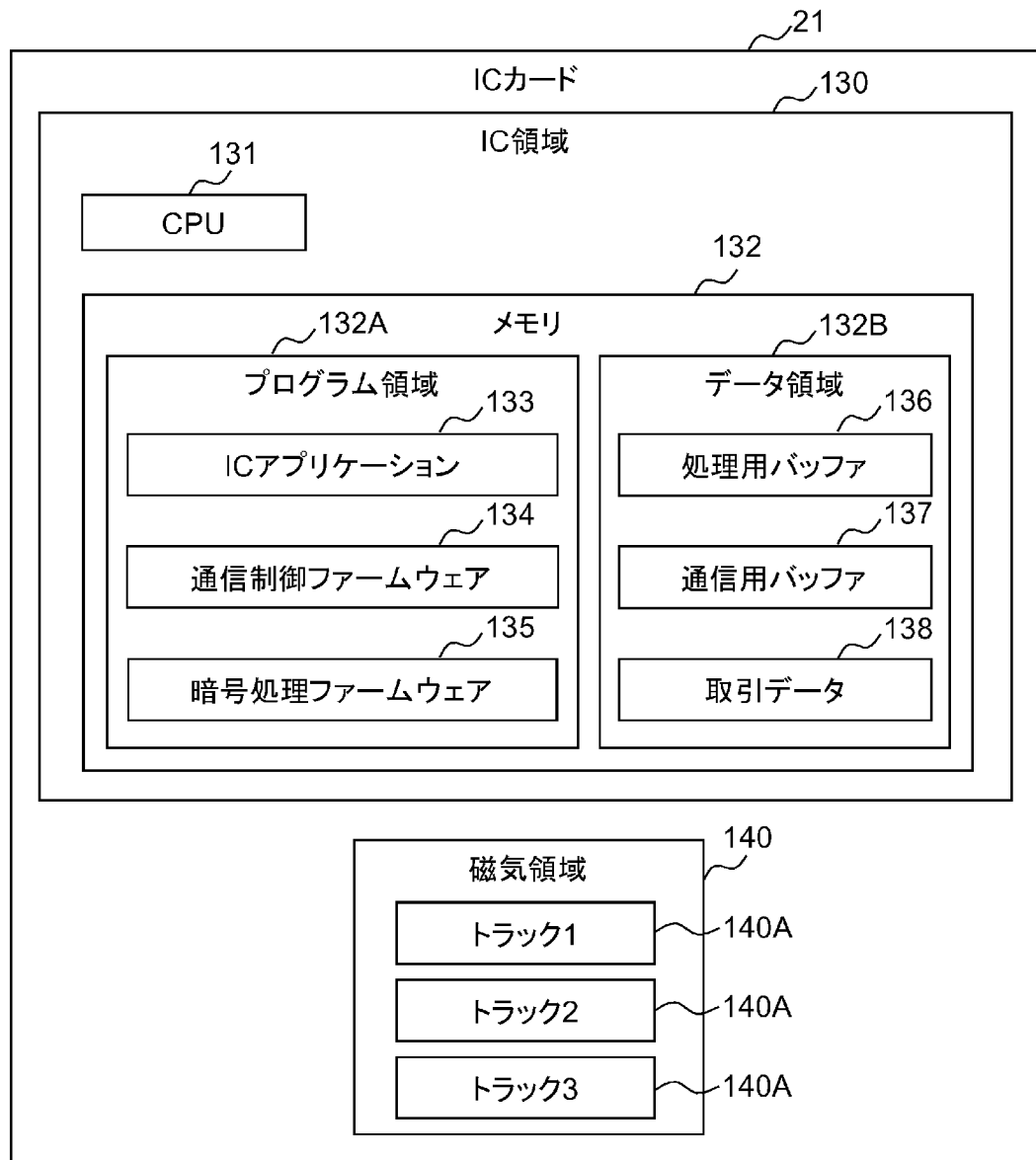
[図4B]

図 4B



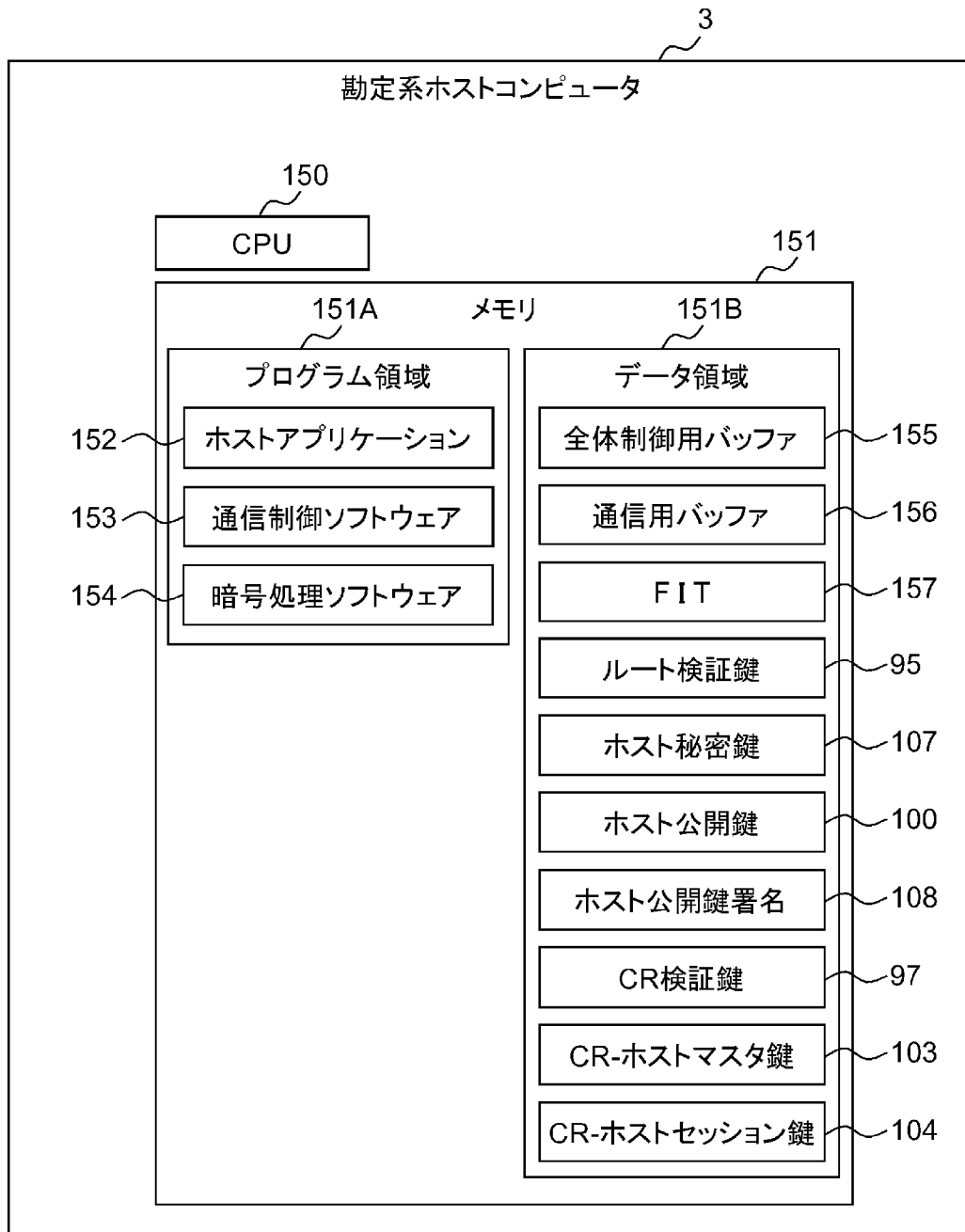
[図5]

図 5



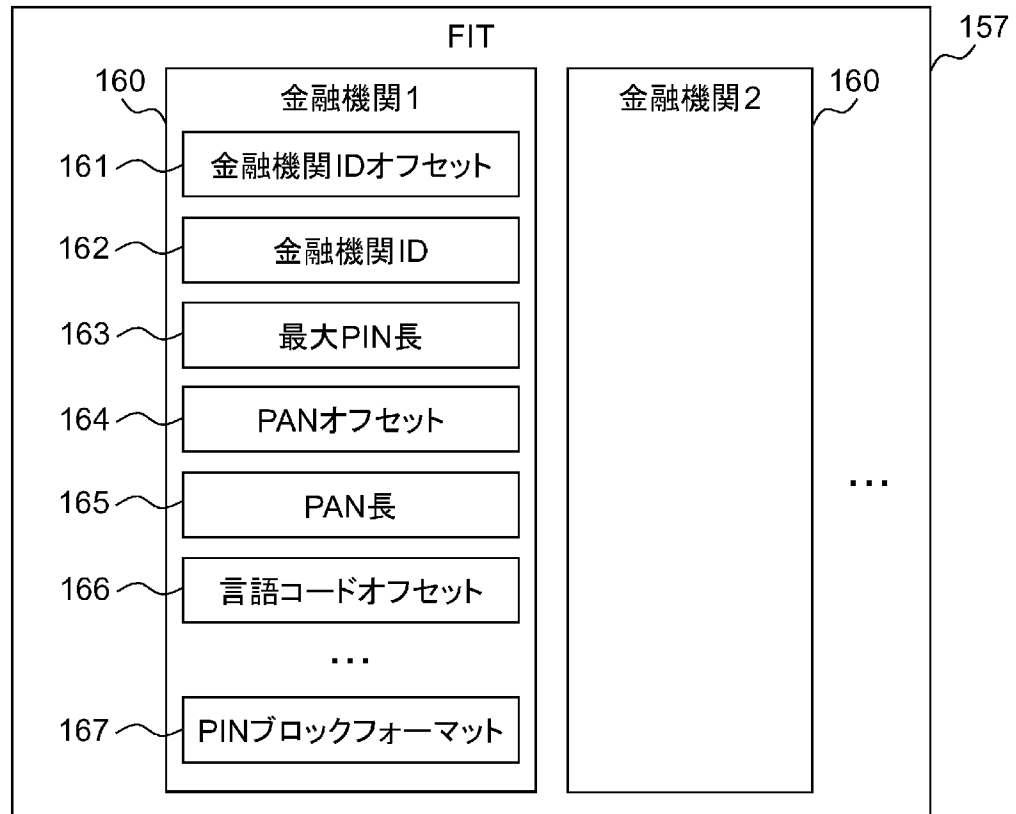
[図6]

図 6



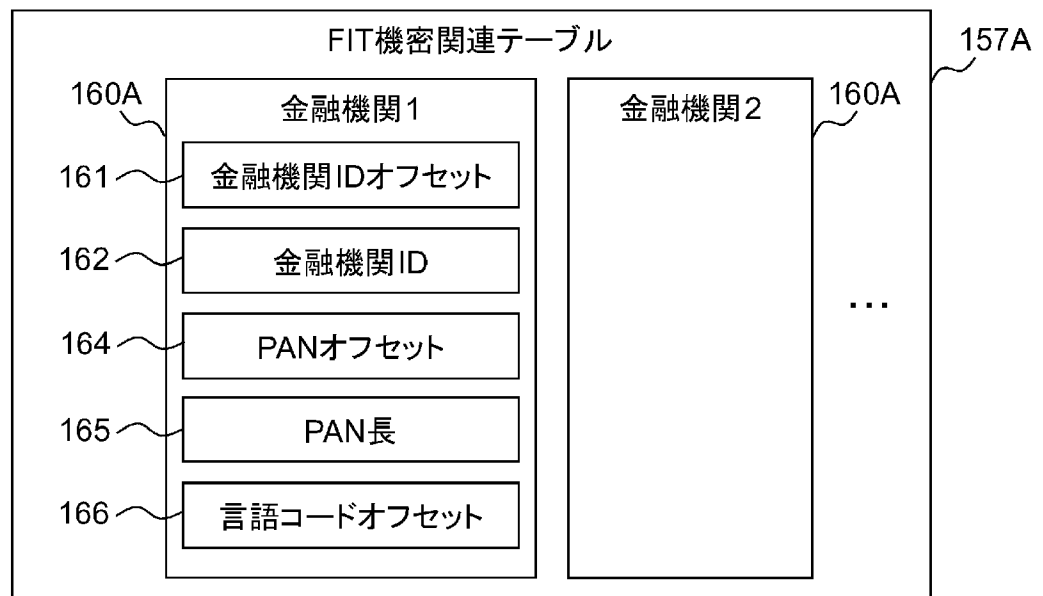
[図7A]

図 7A



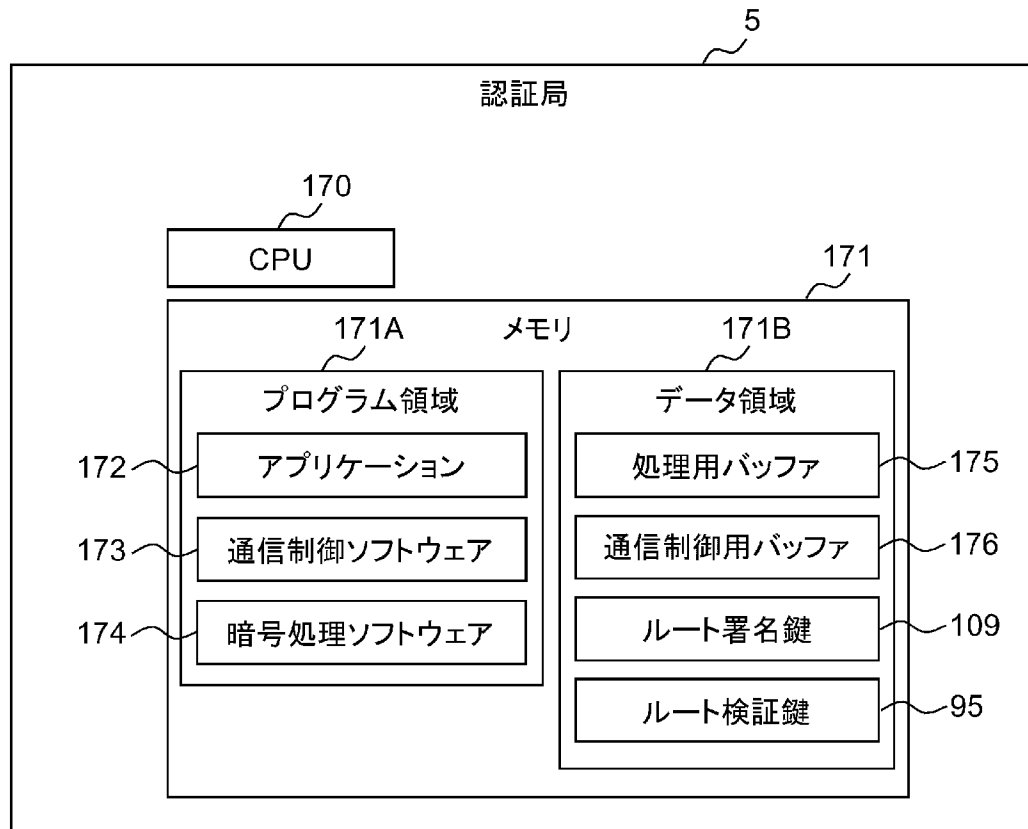
[図7B]

図 7B

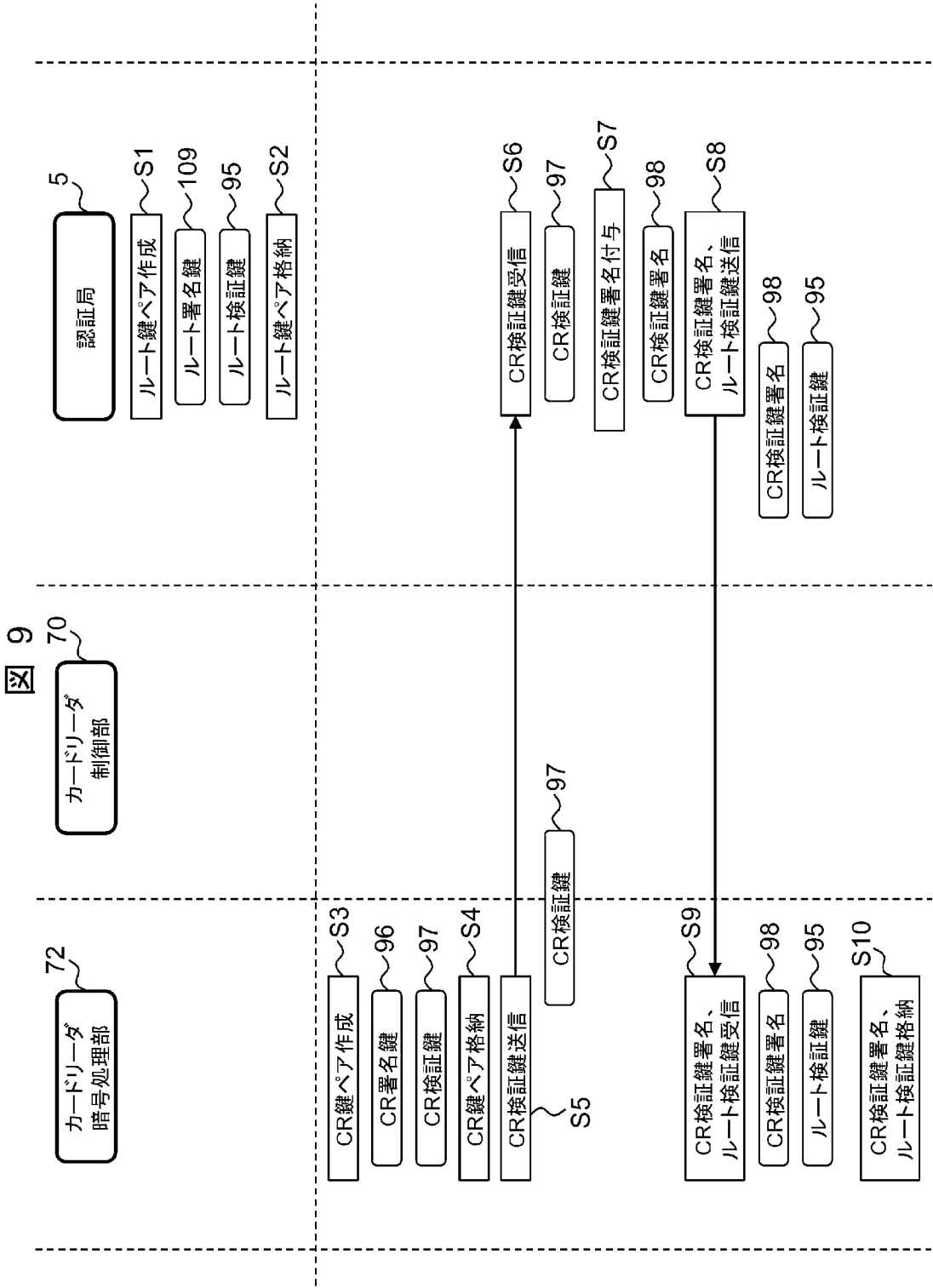


[図8]

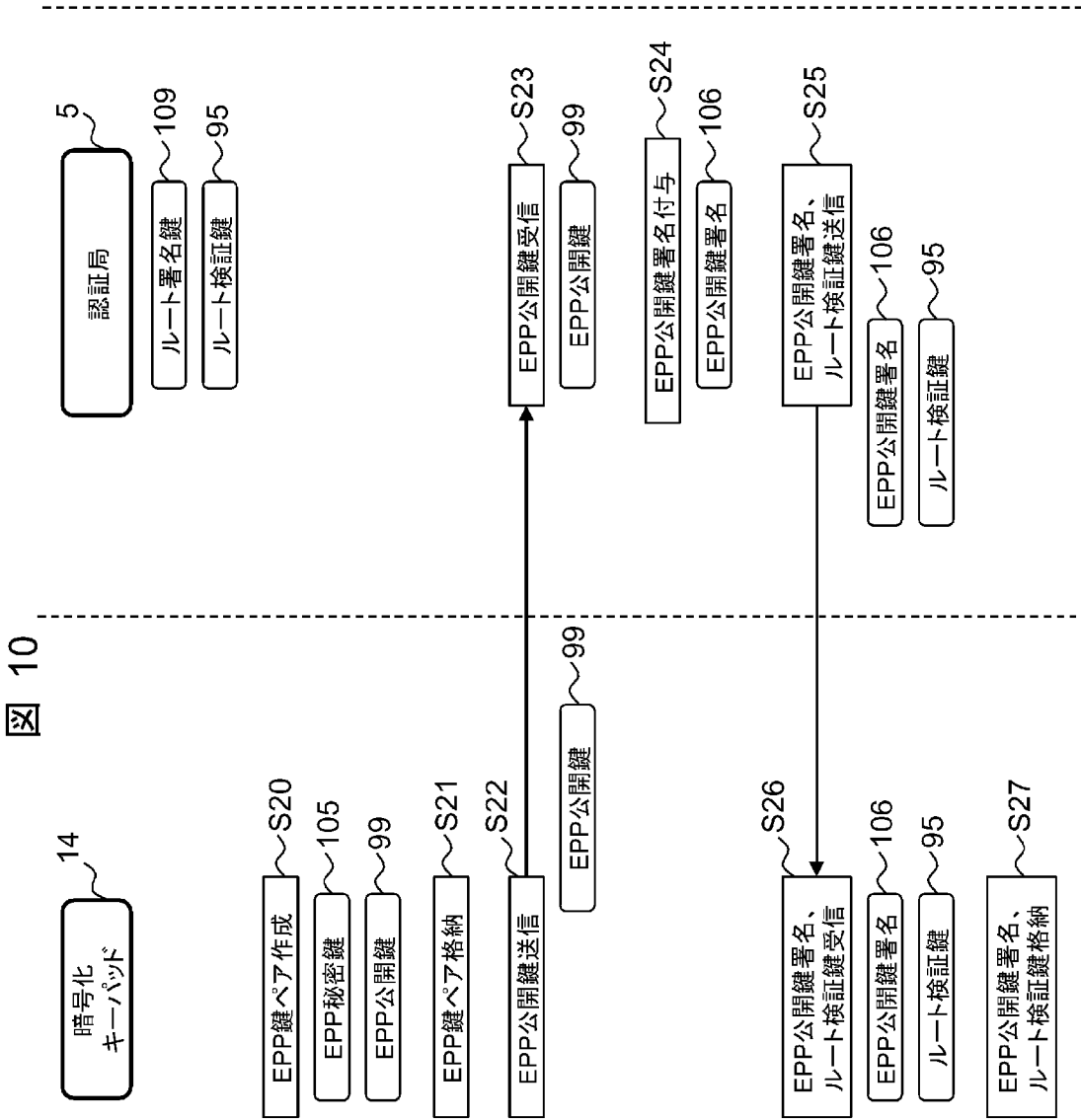
図 8



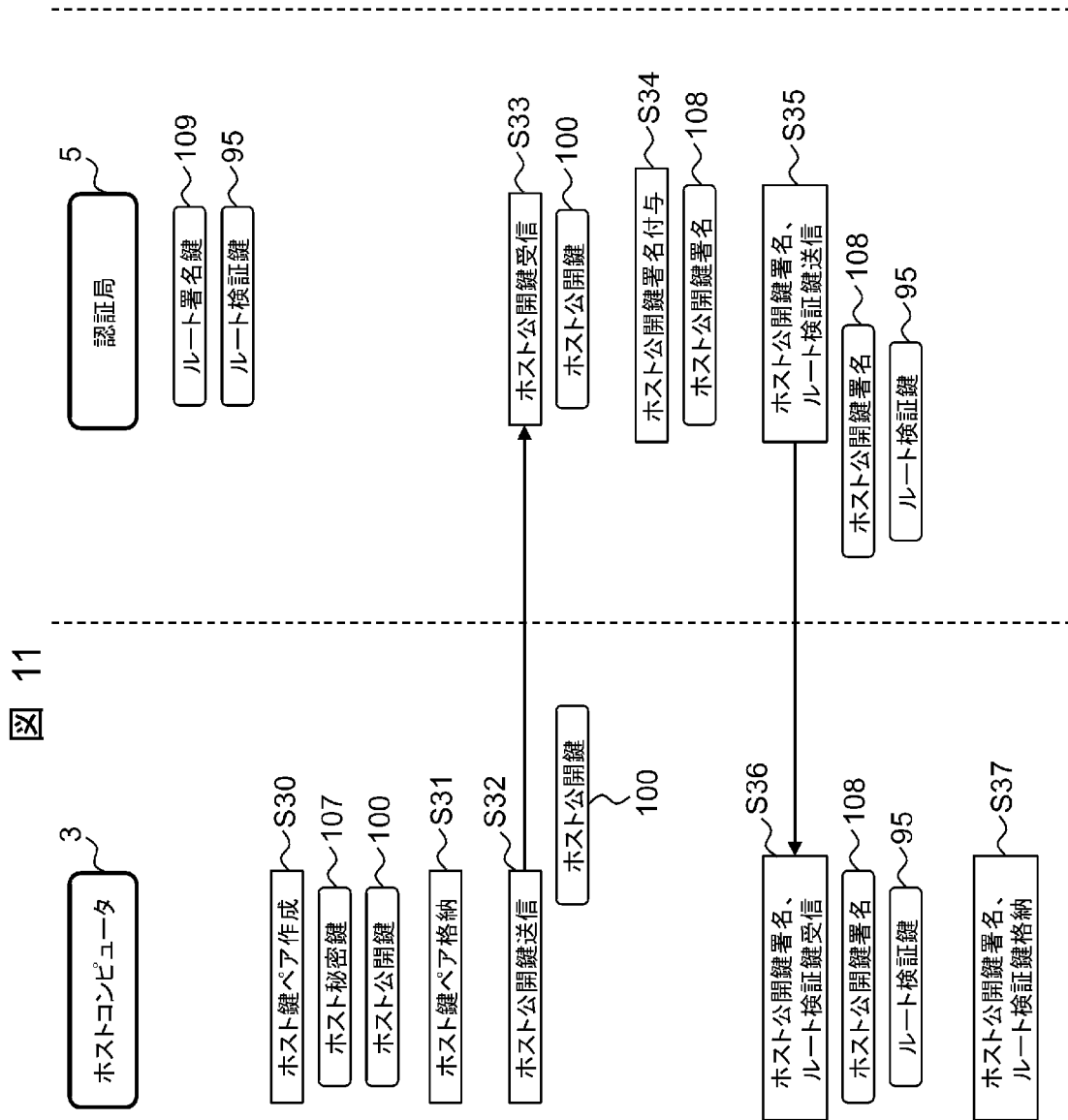
[図9]

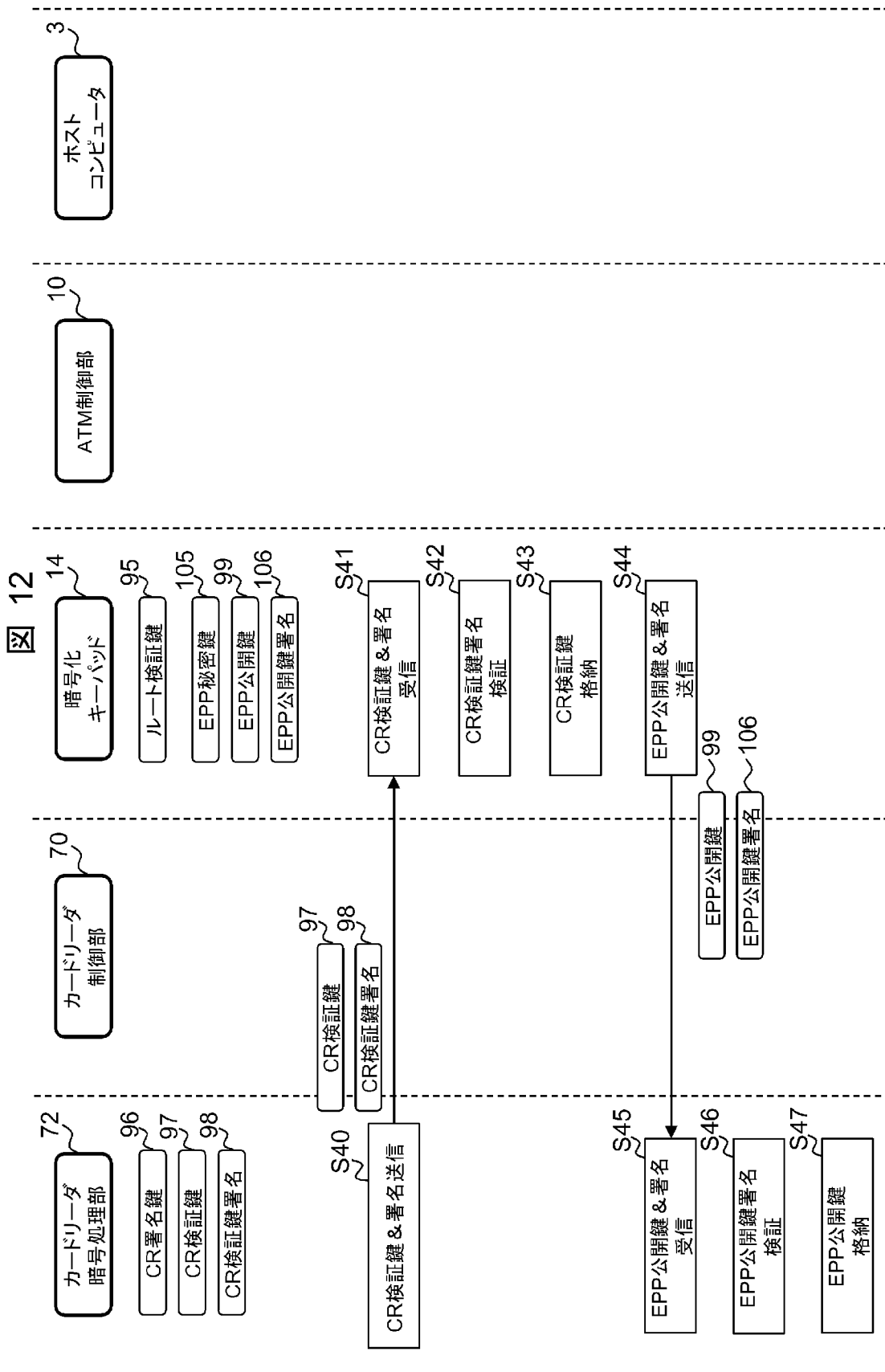


[図10]

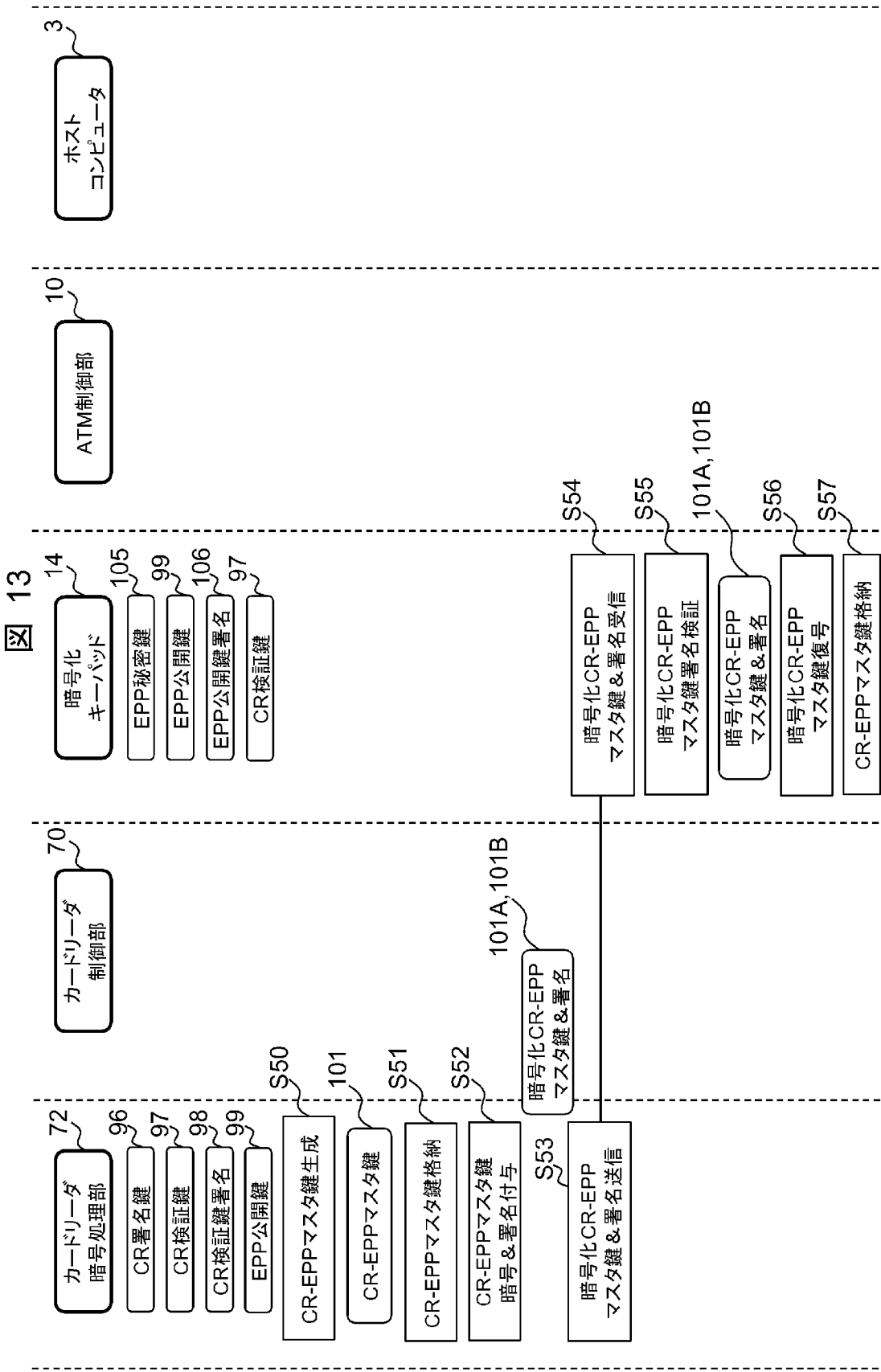


[図11]

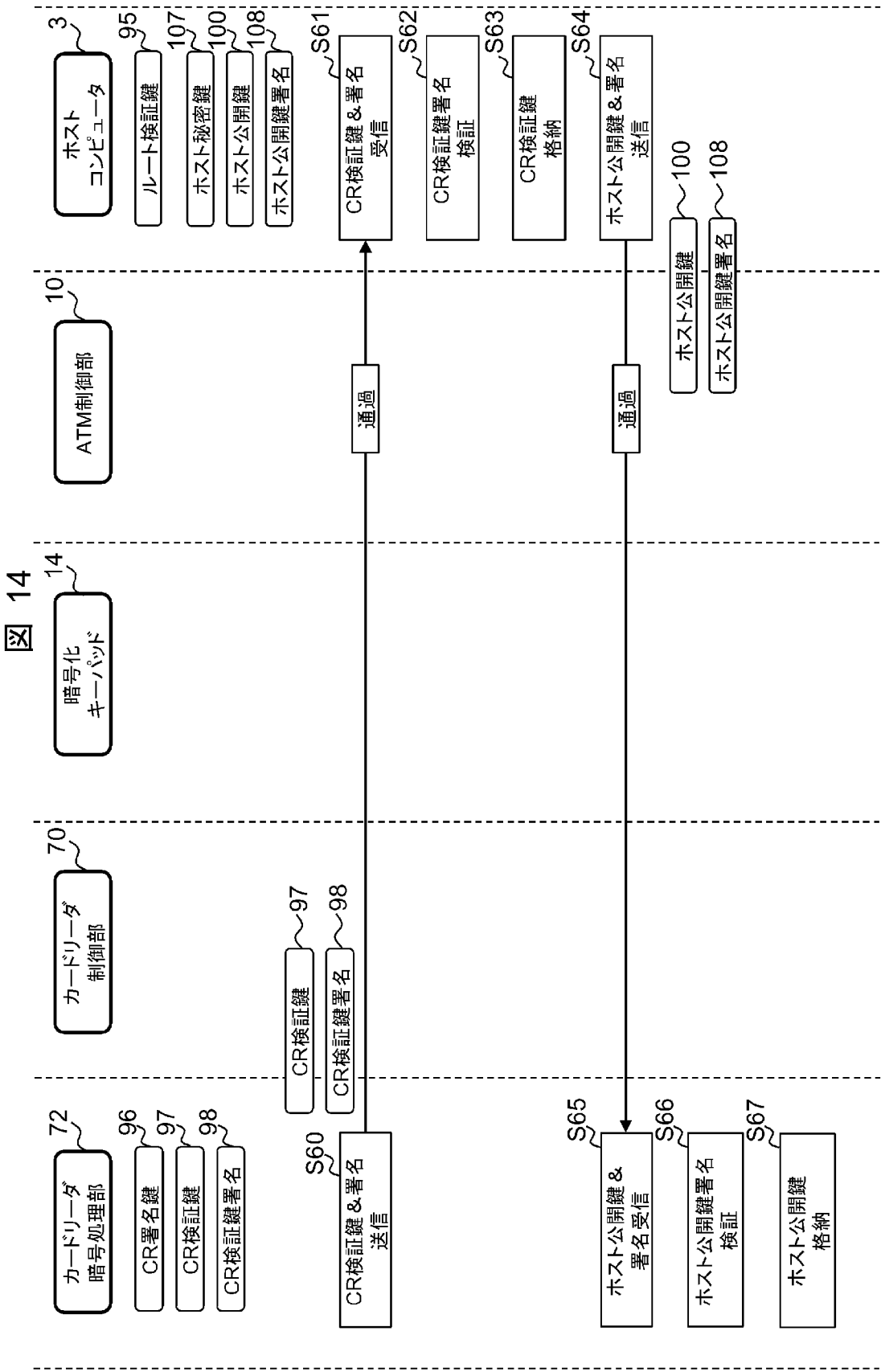




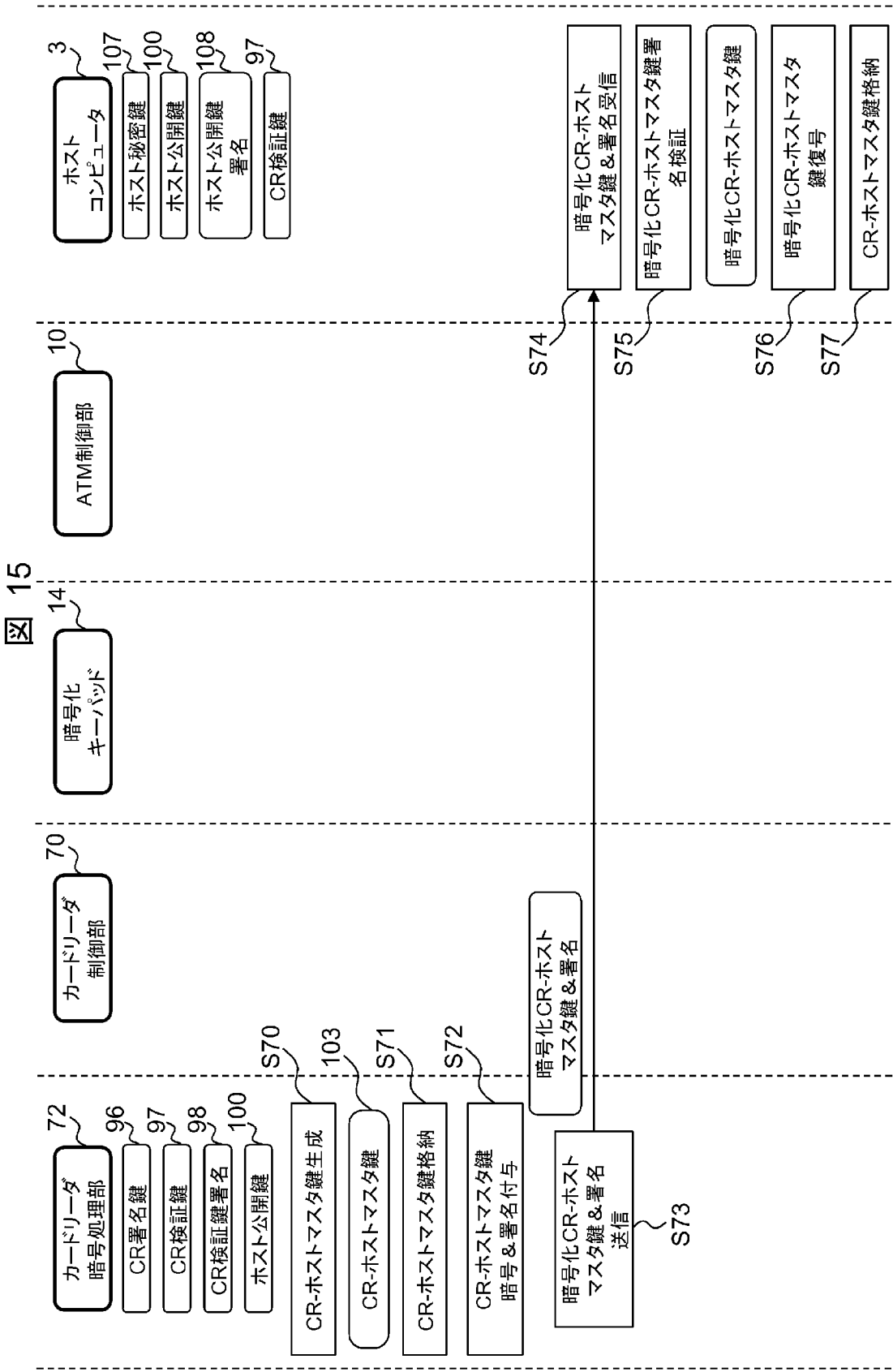
[図13]

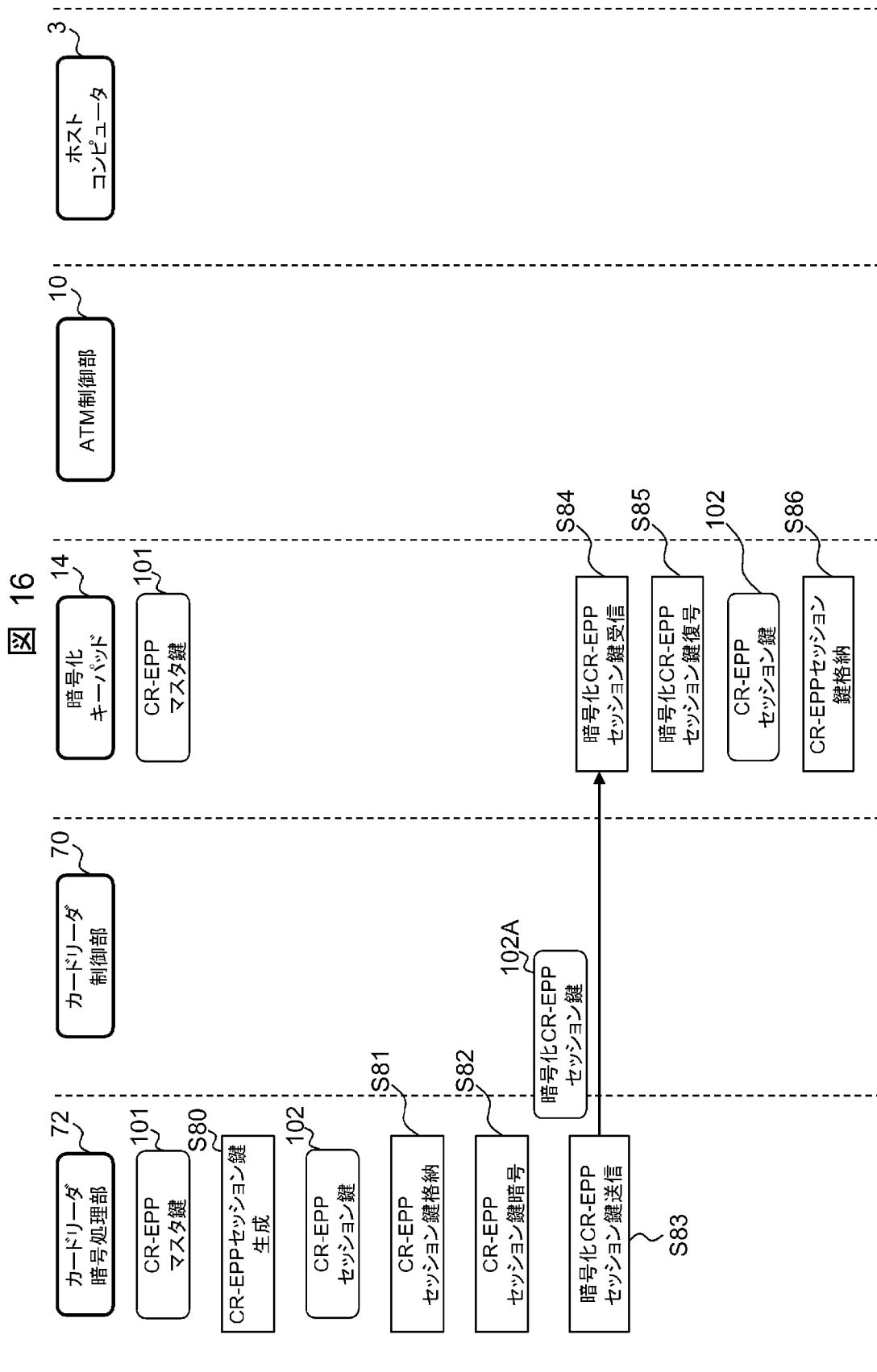


[図14]

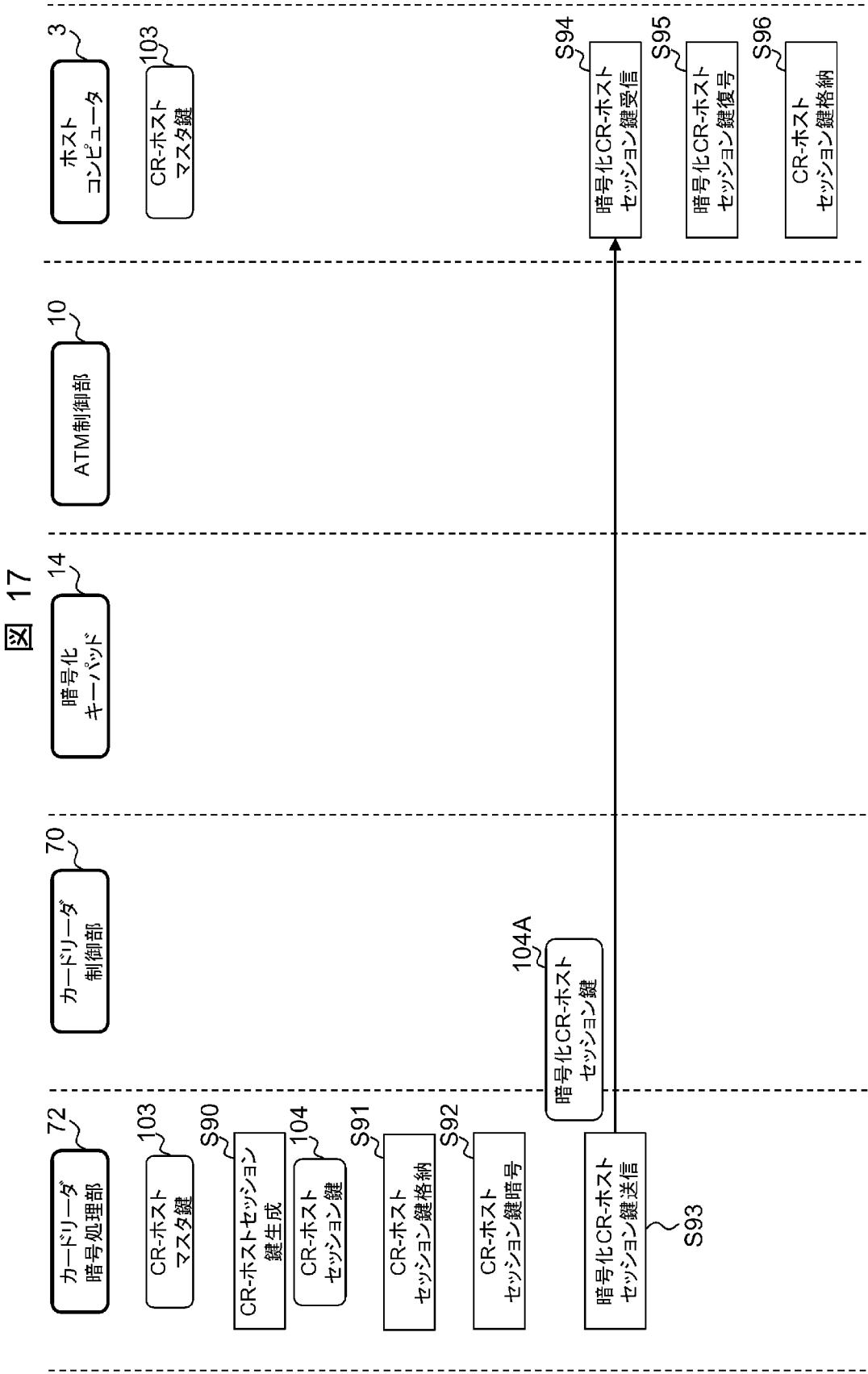


[図15]

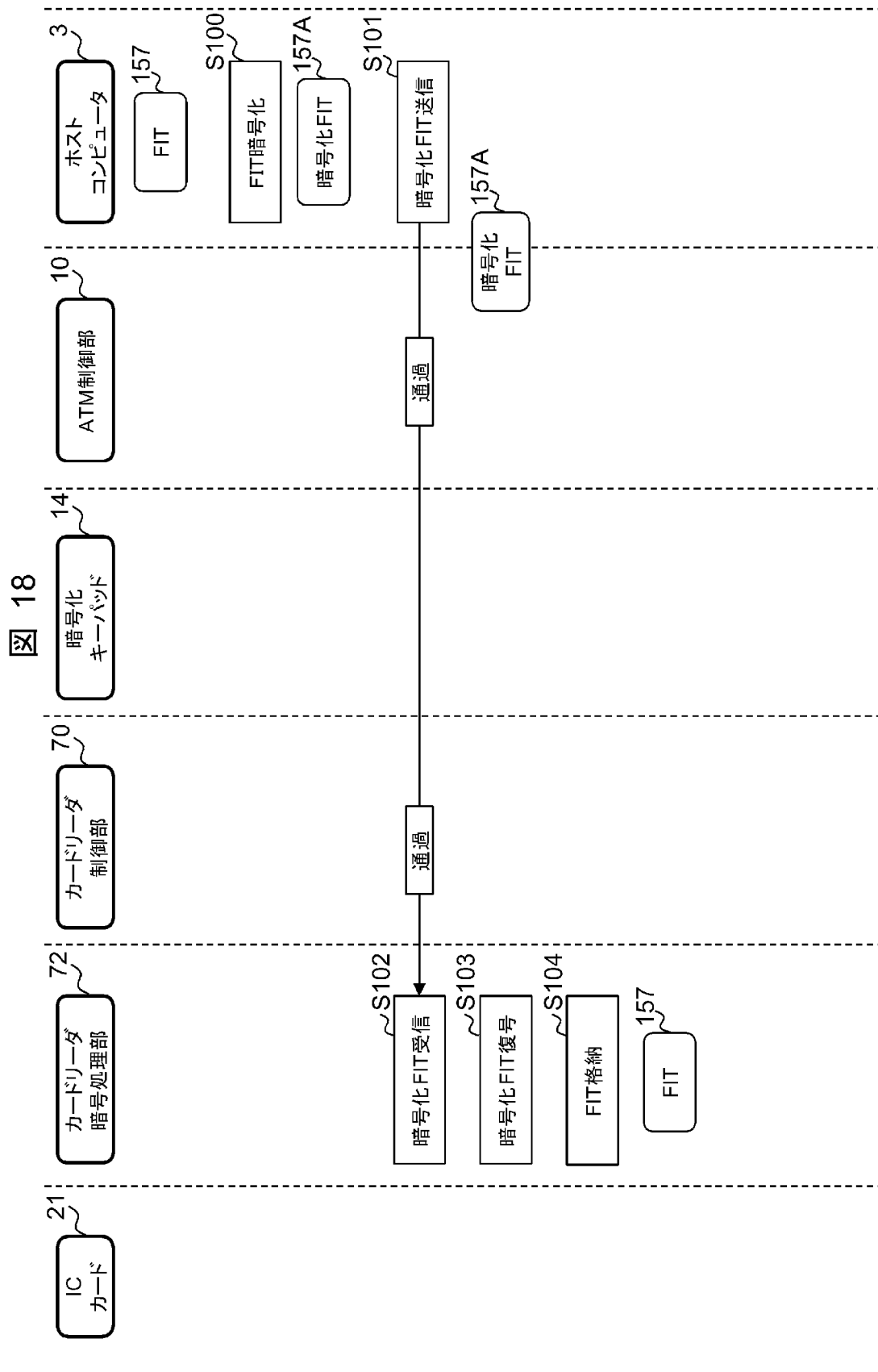




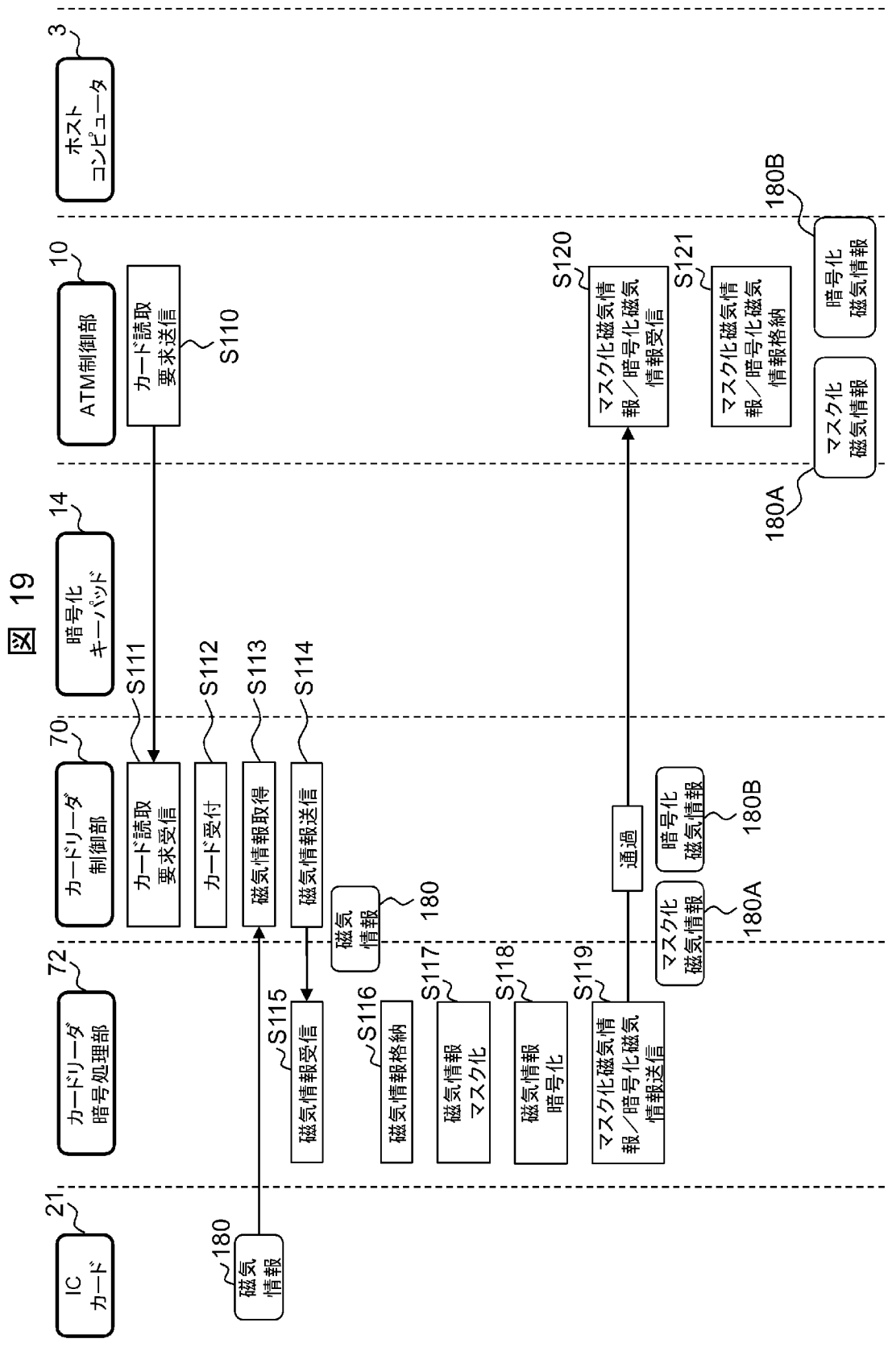
[図17]



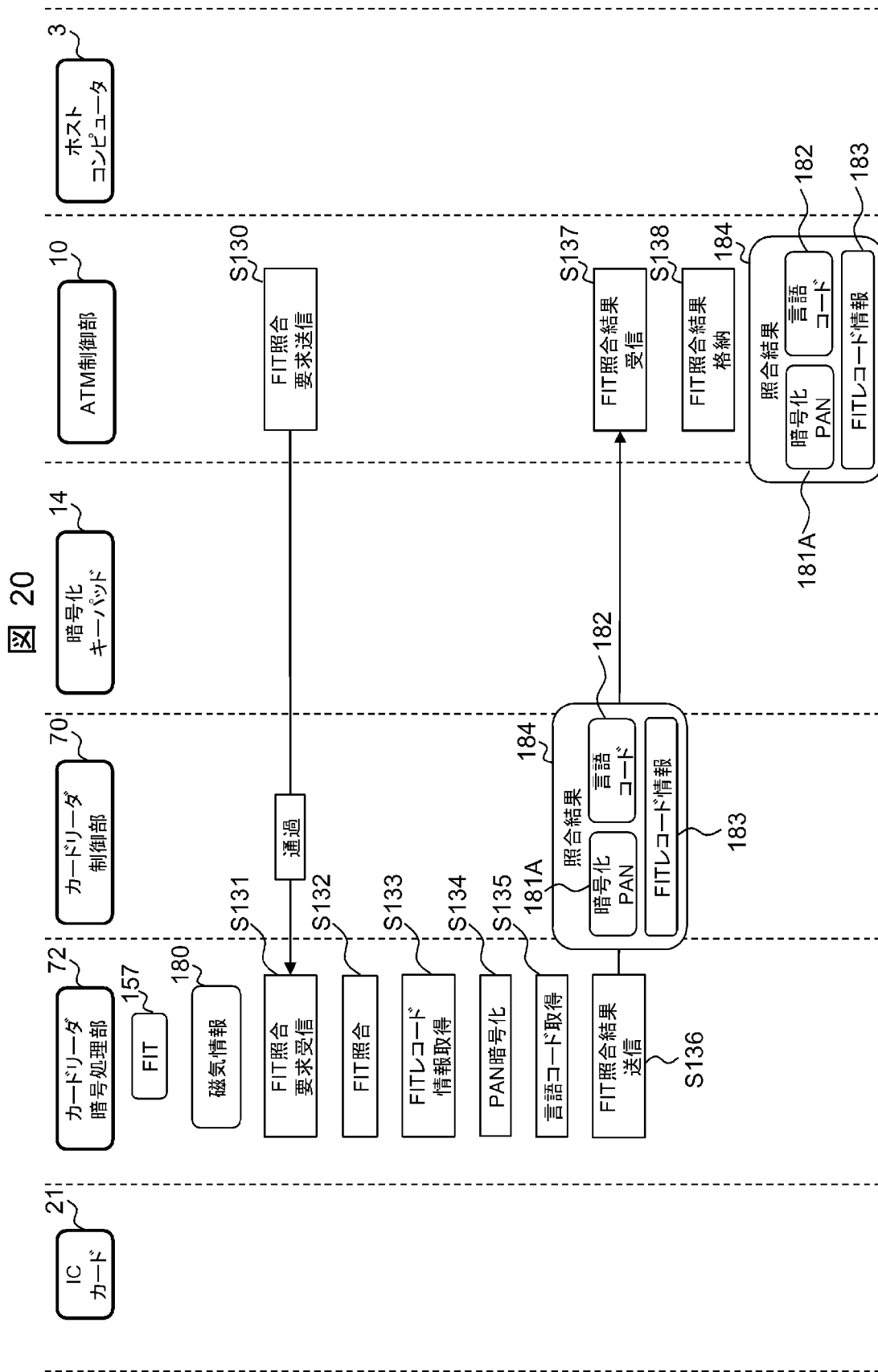
[図18]



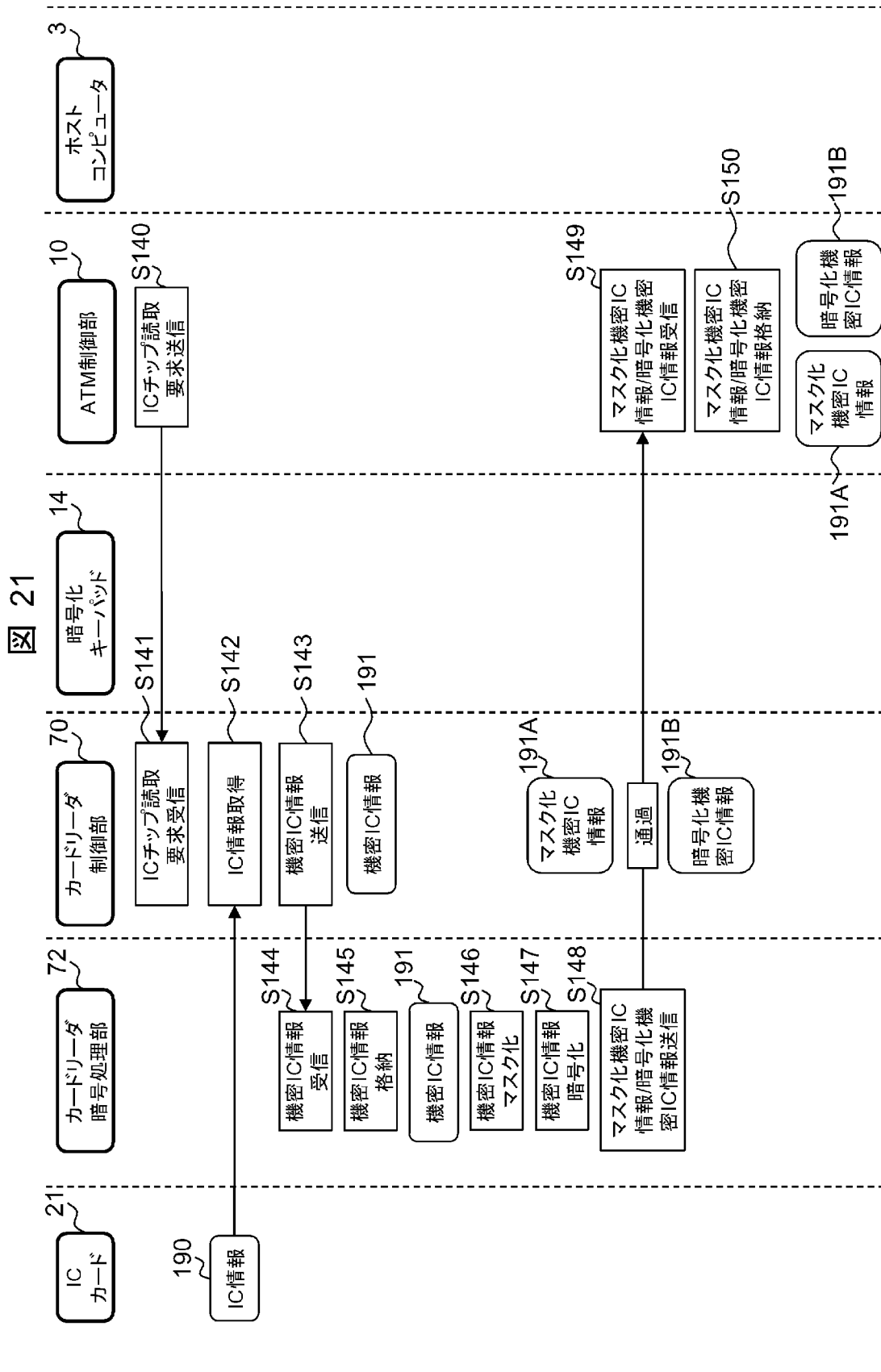
[図19]



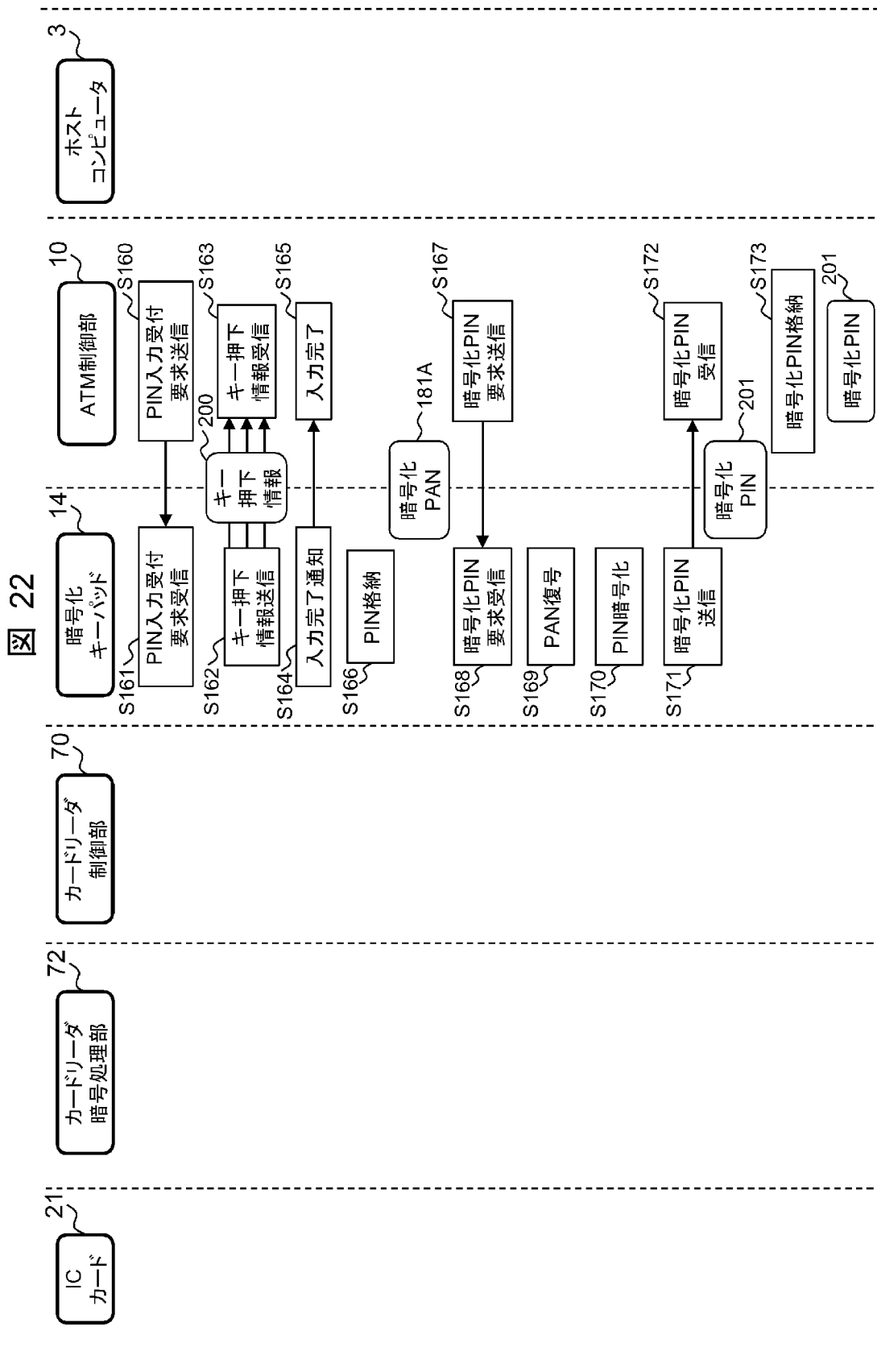
[図20]



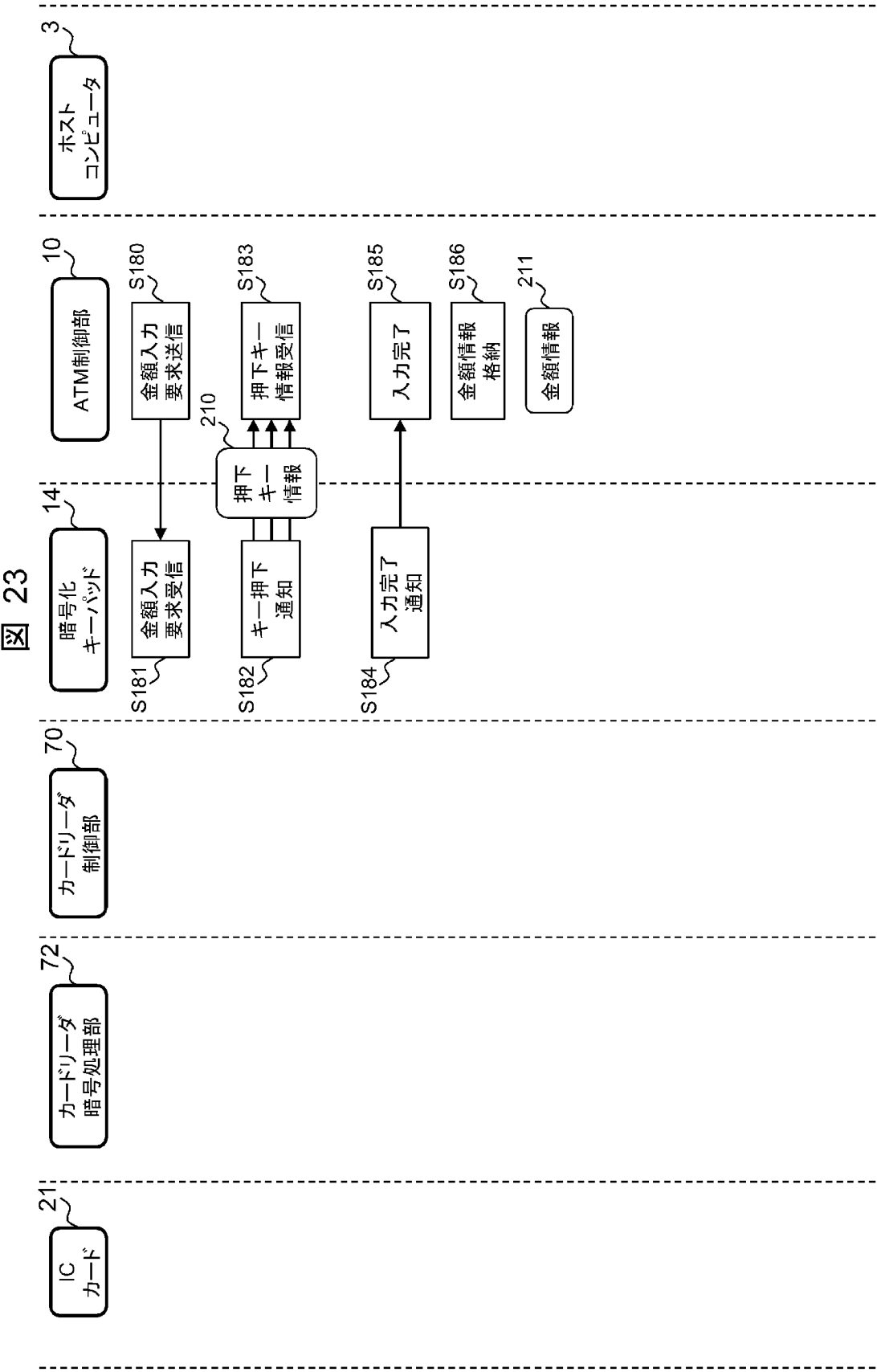
[図21]



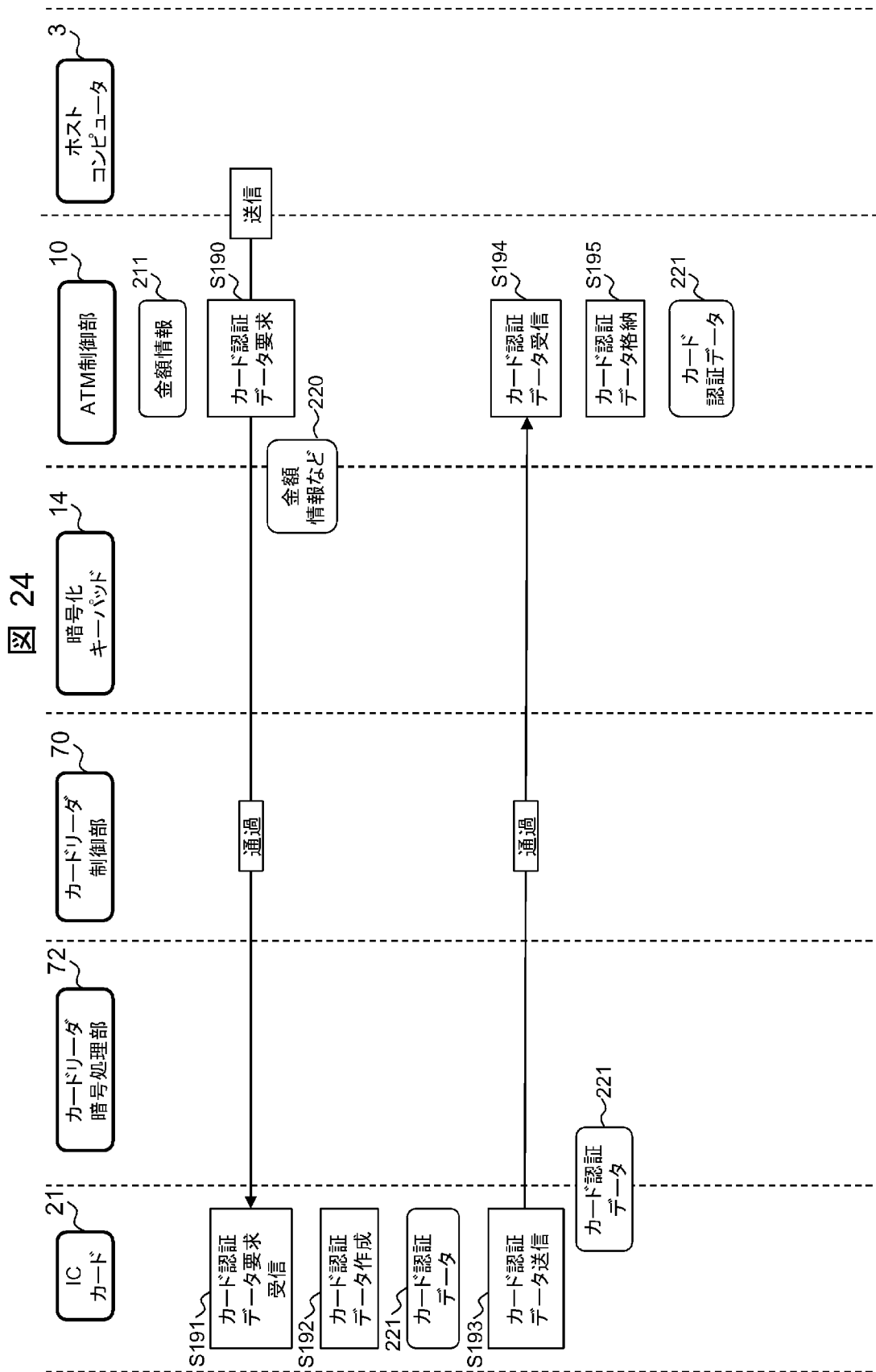
[図22]



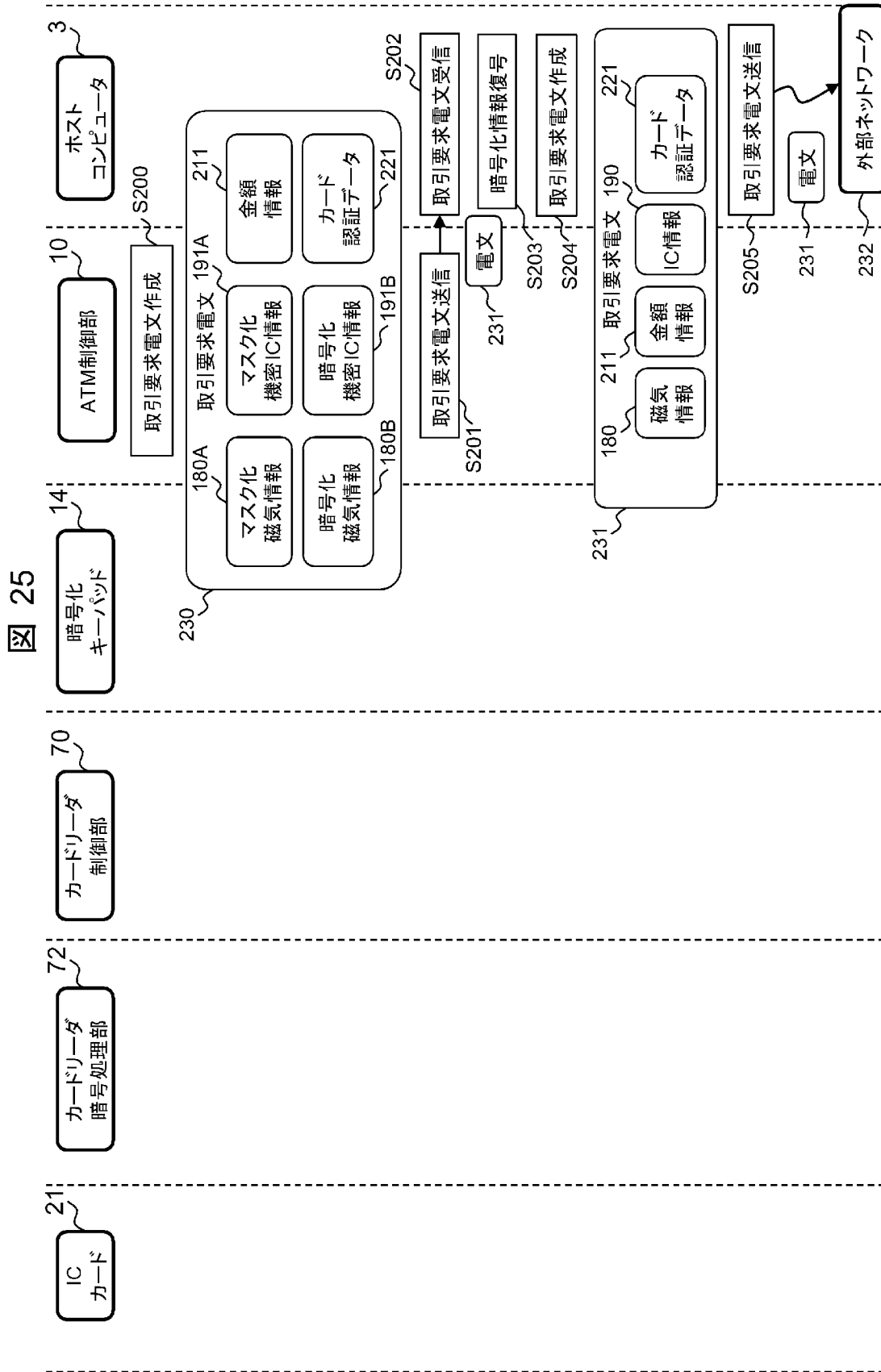
[図23]



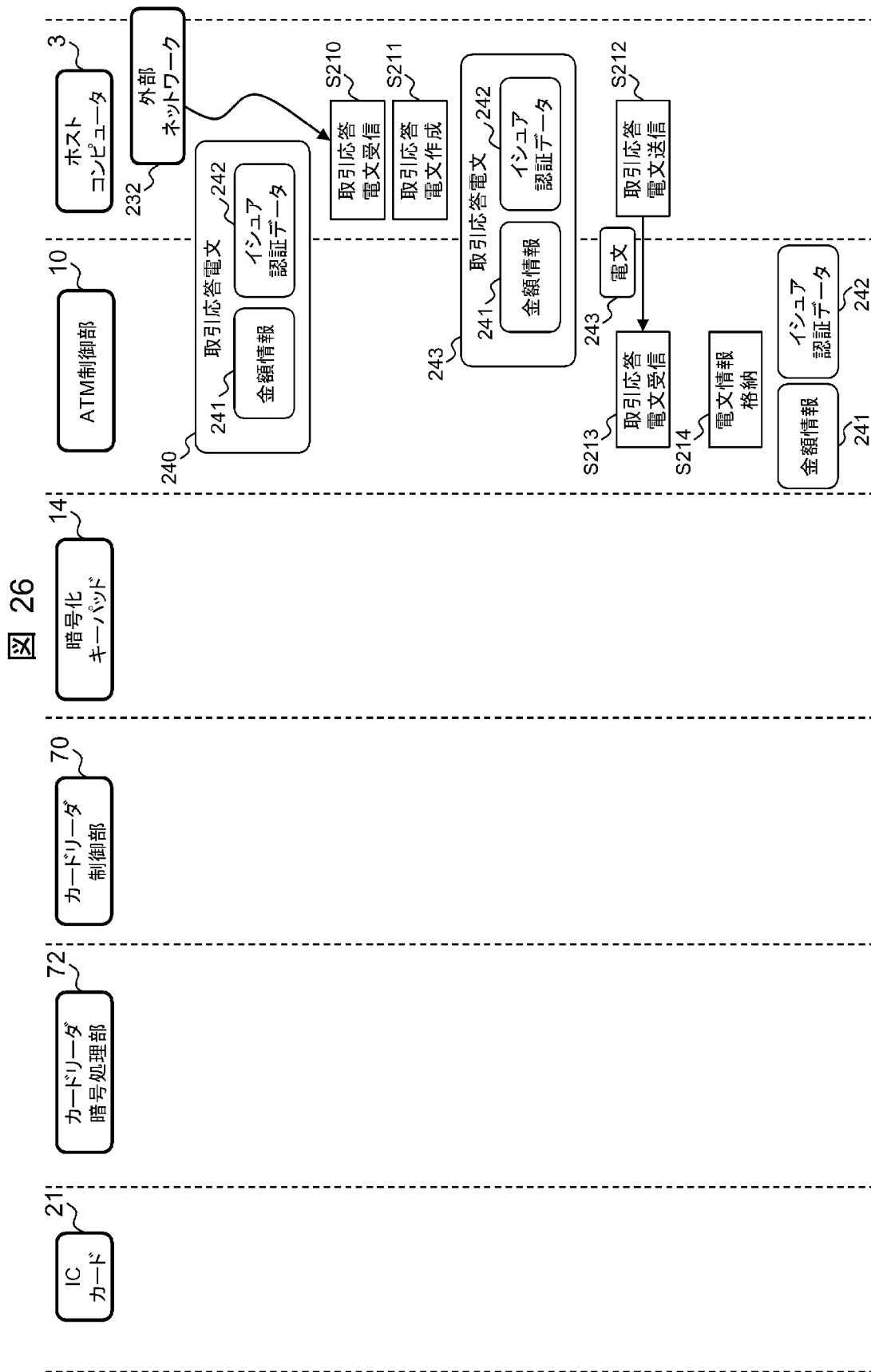
[図24]



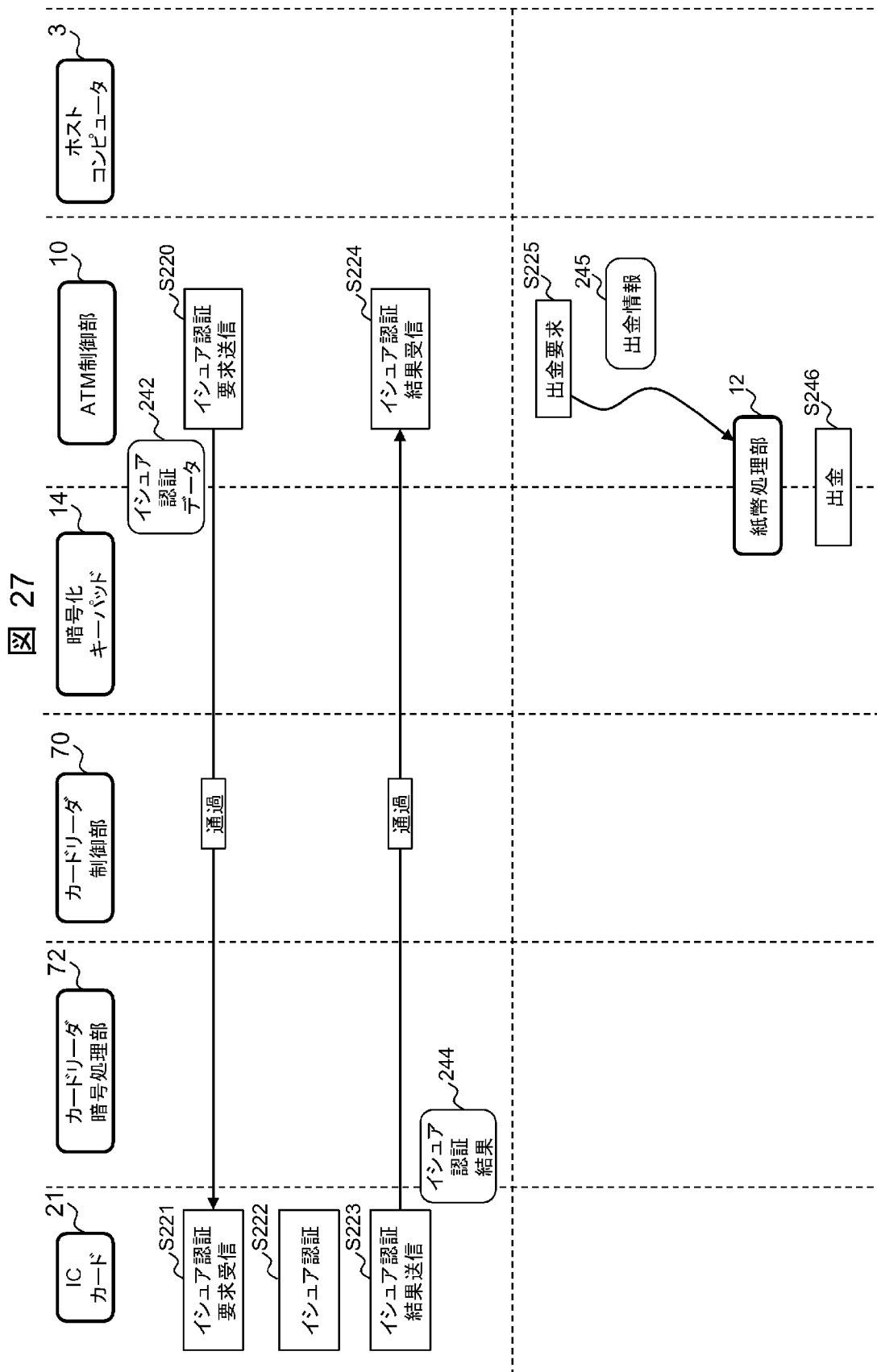
[図25]



[図26]

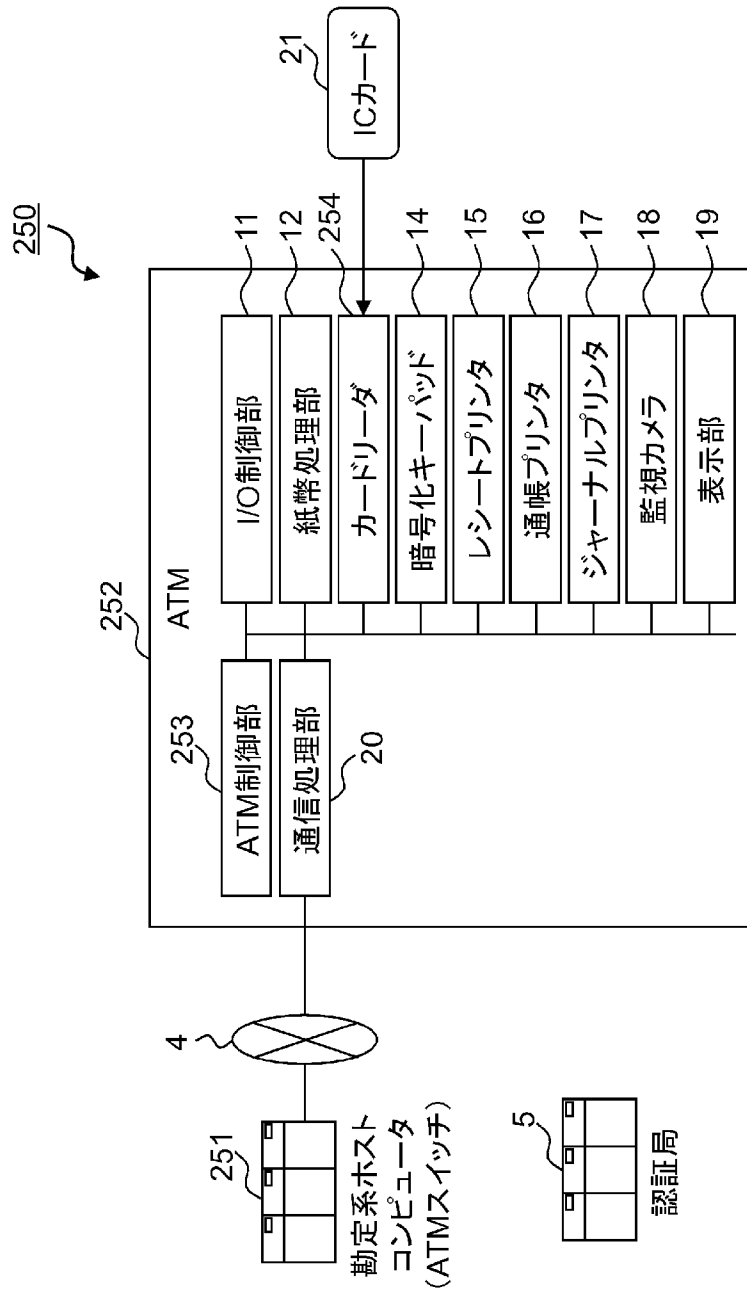


[図27]

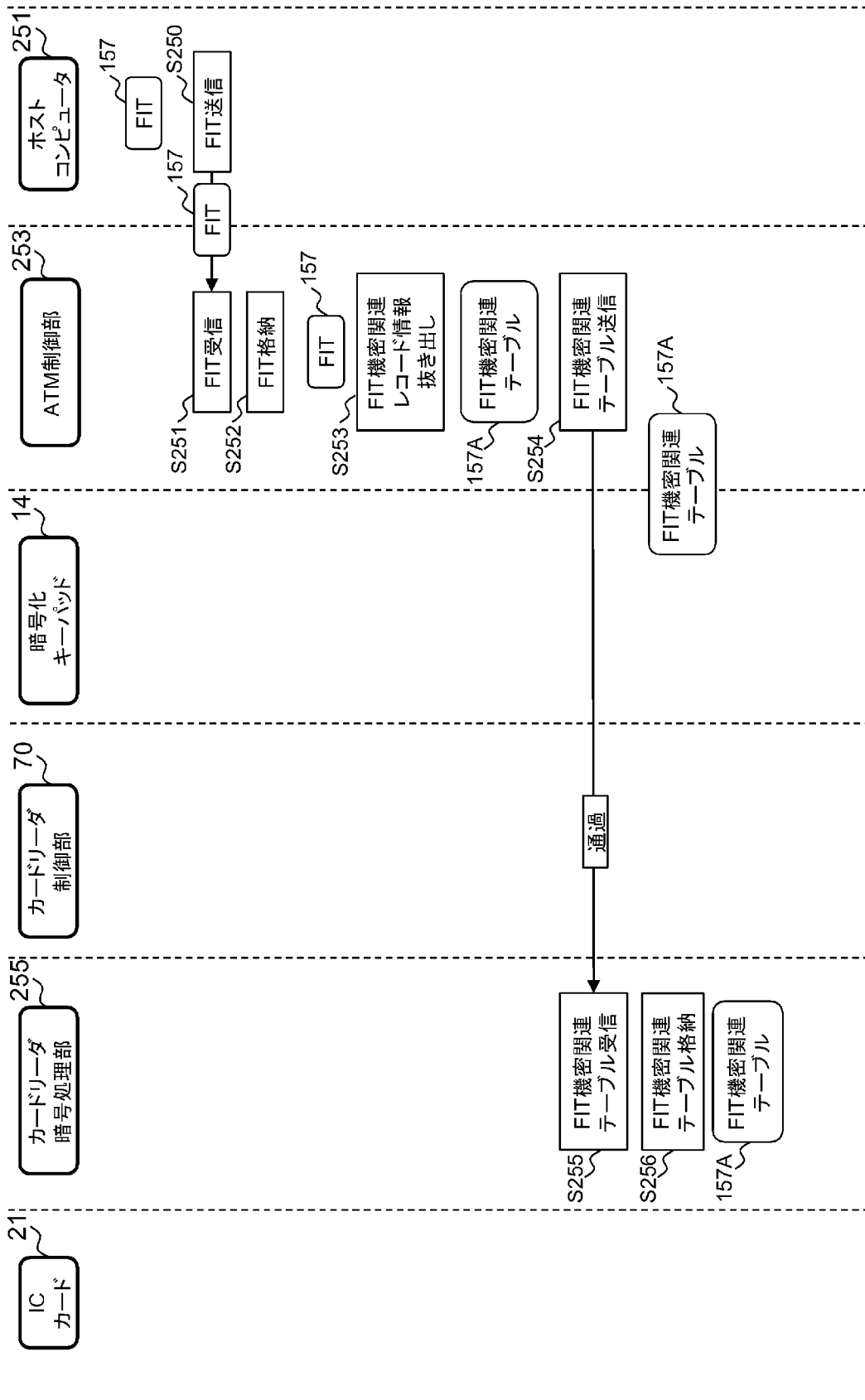


[図28]

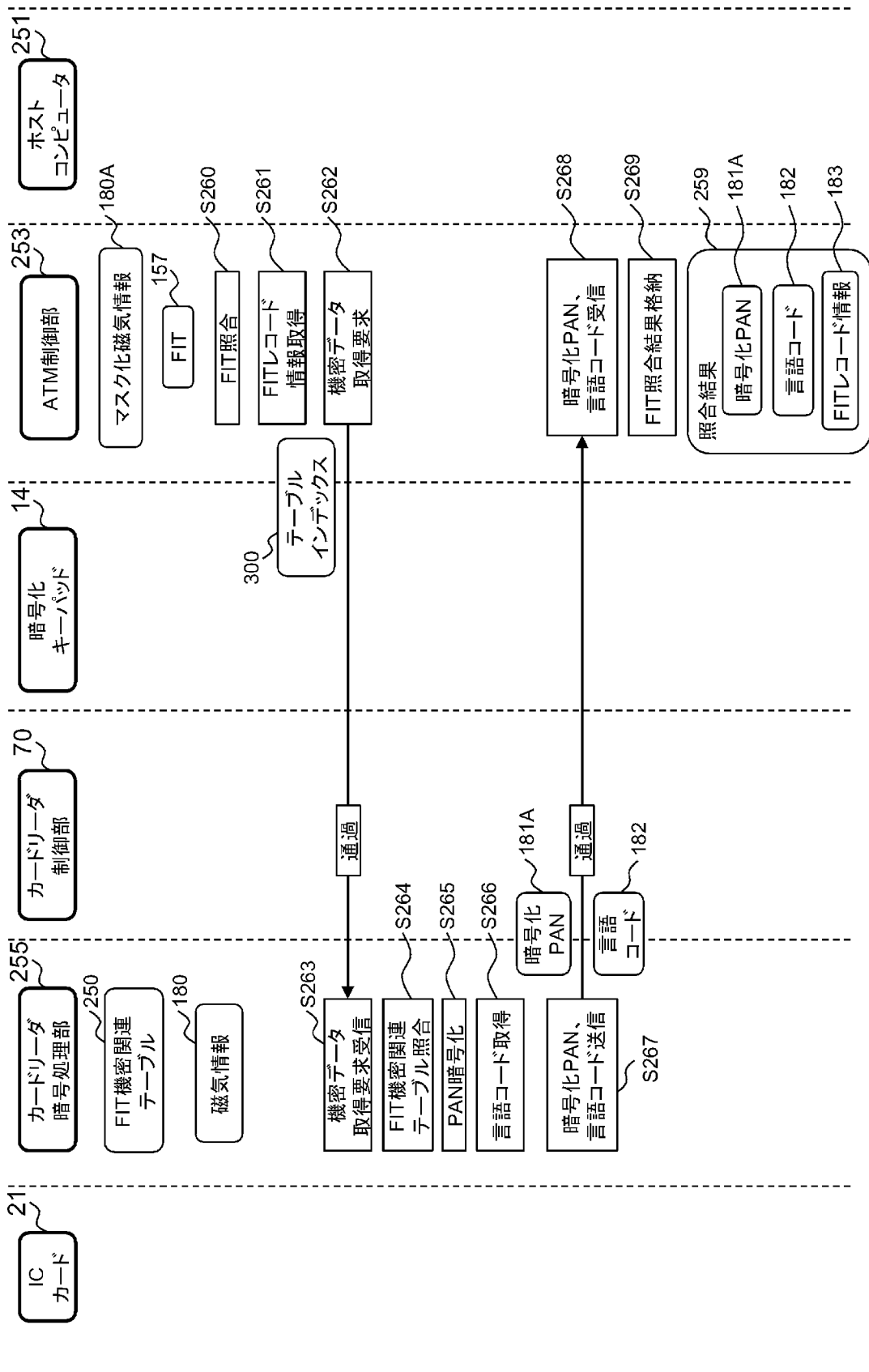
図 28



29

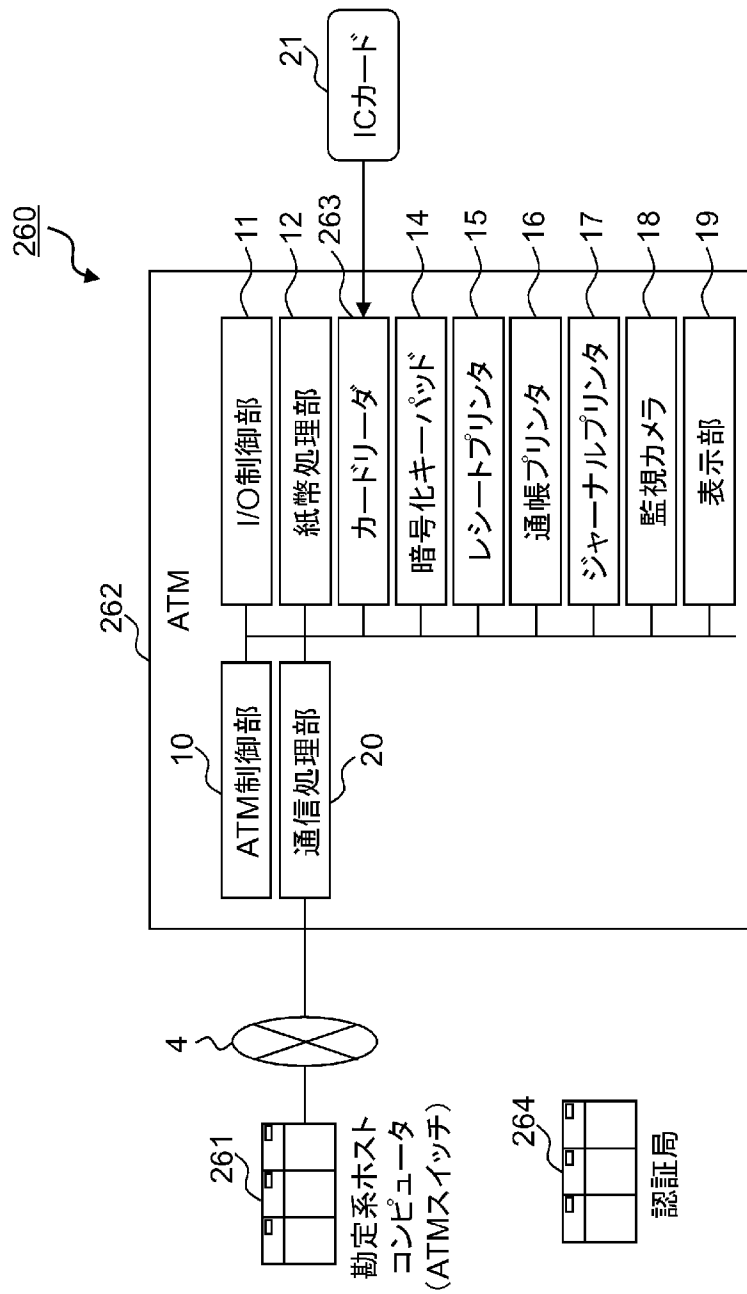


30



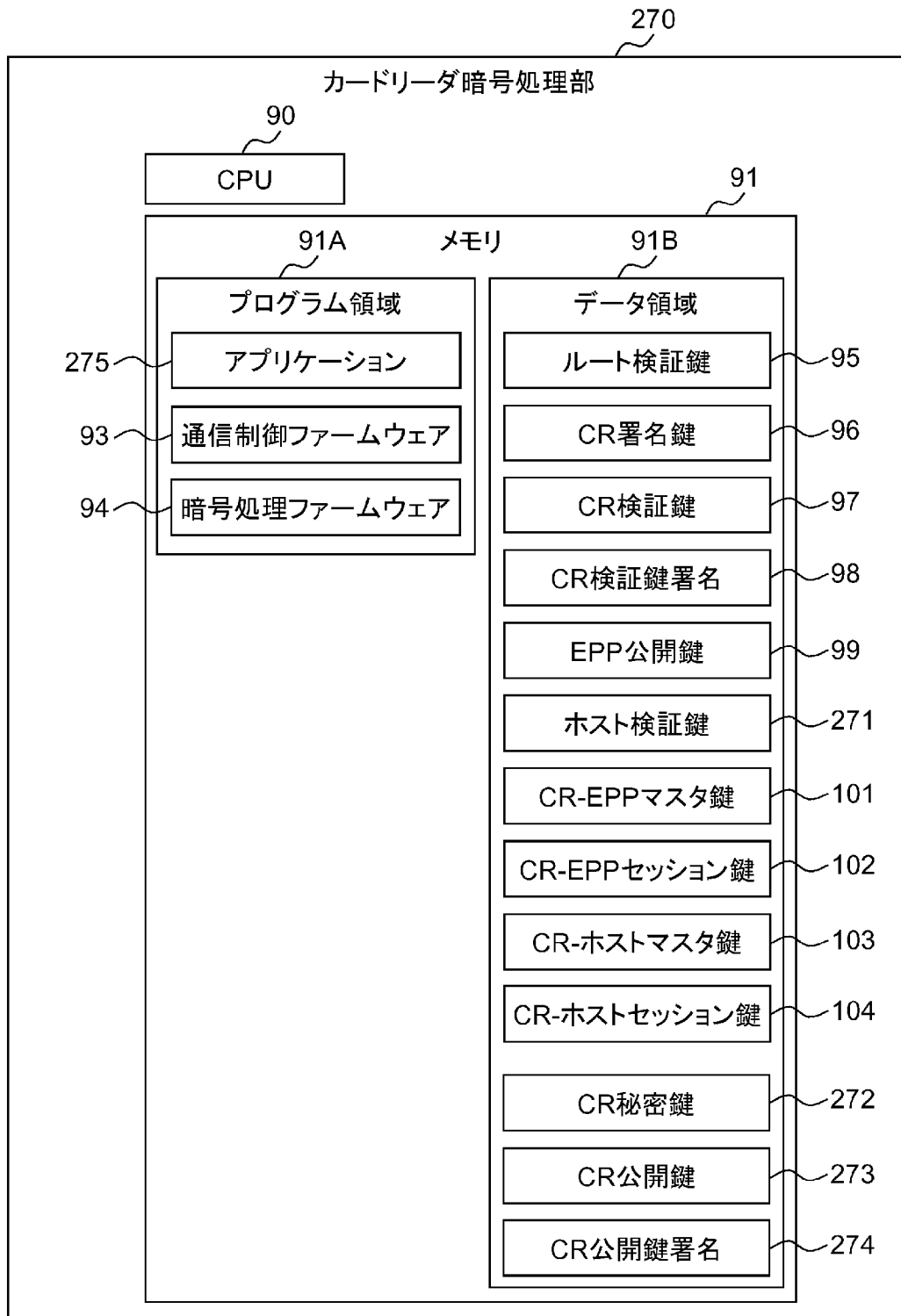
[図31]

図 31



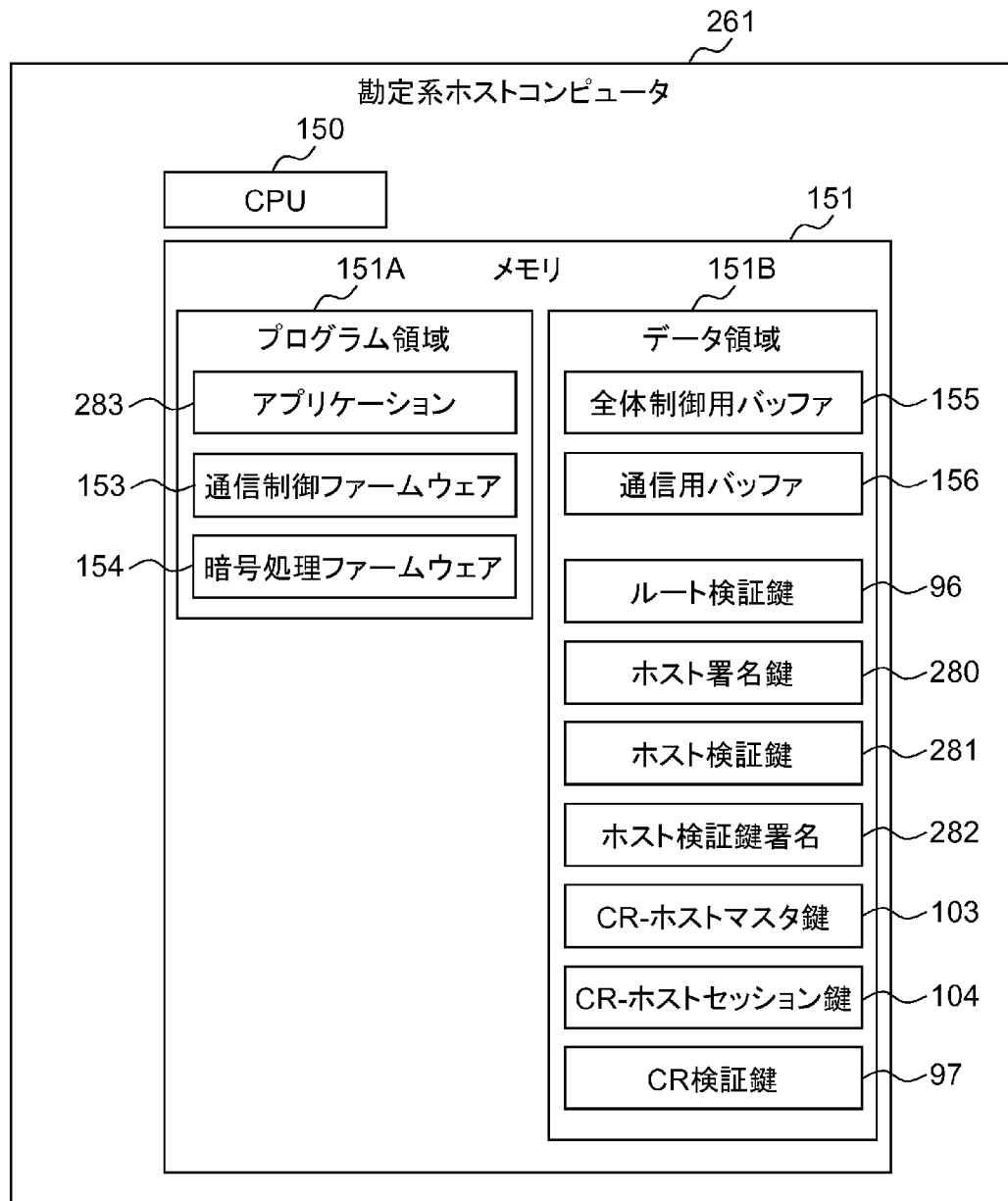
[図32]

図 32

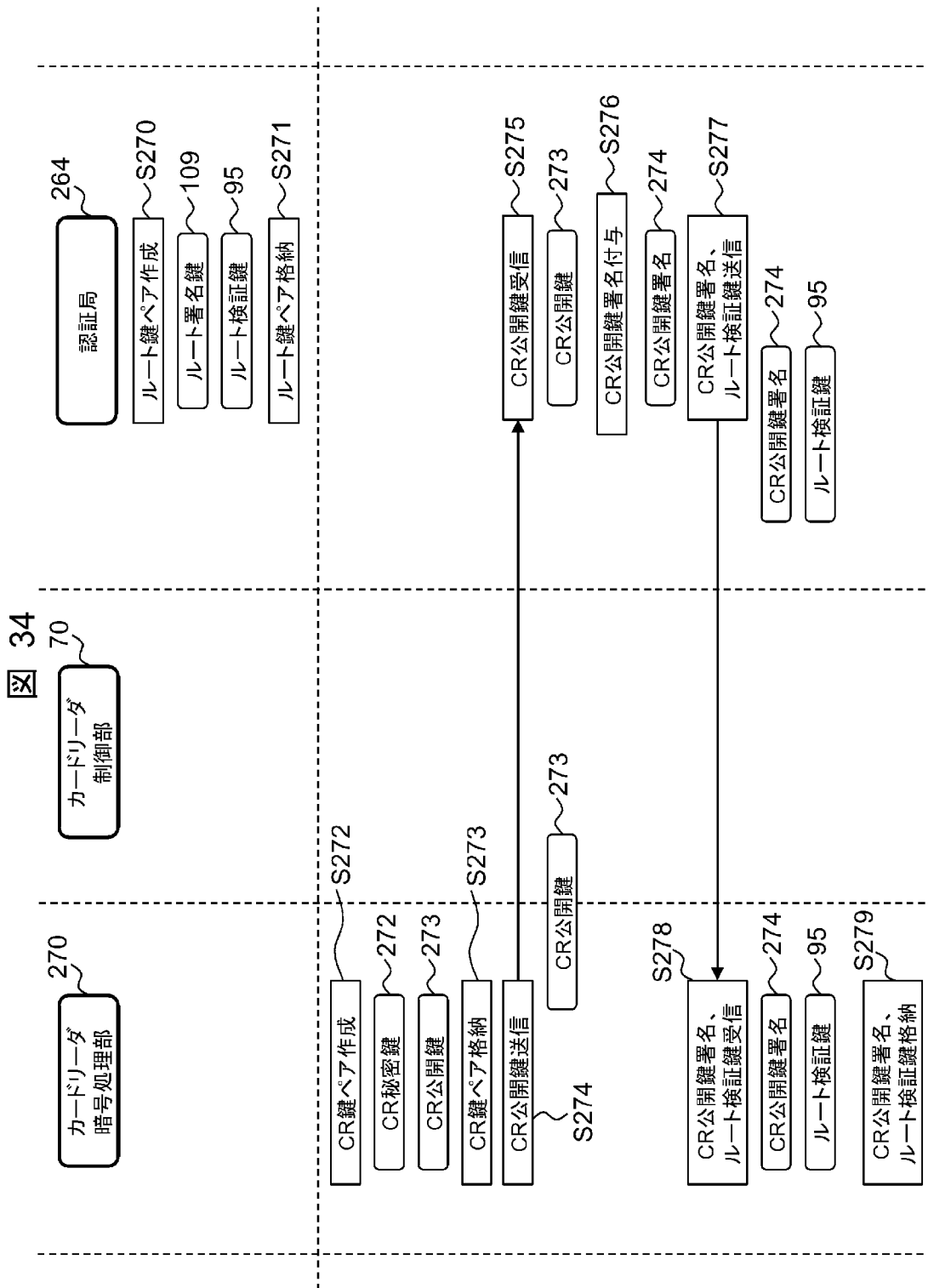


[図33]

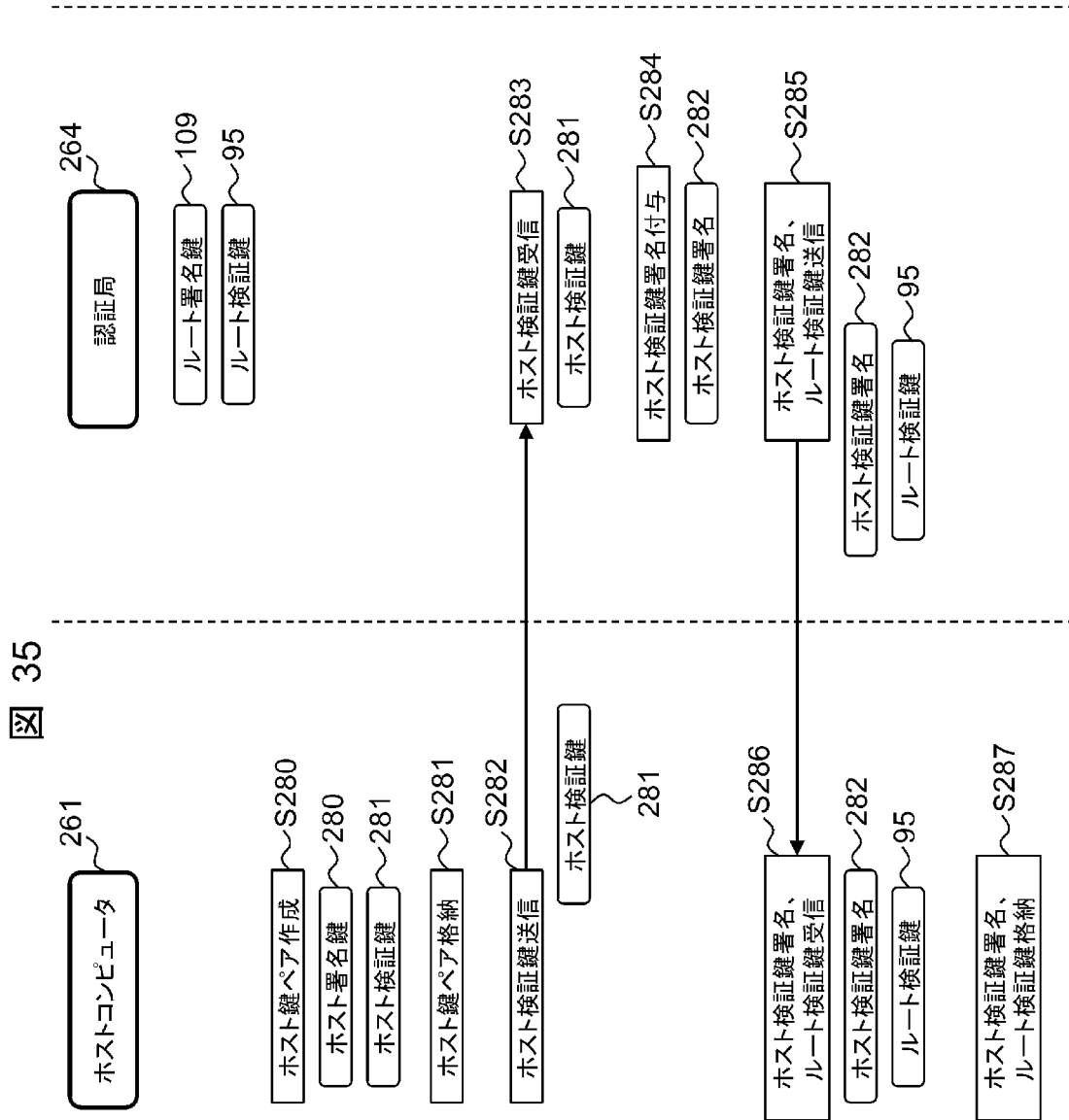
図 33



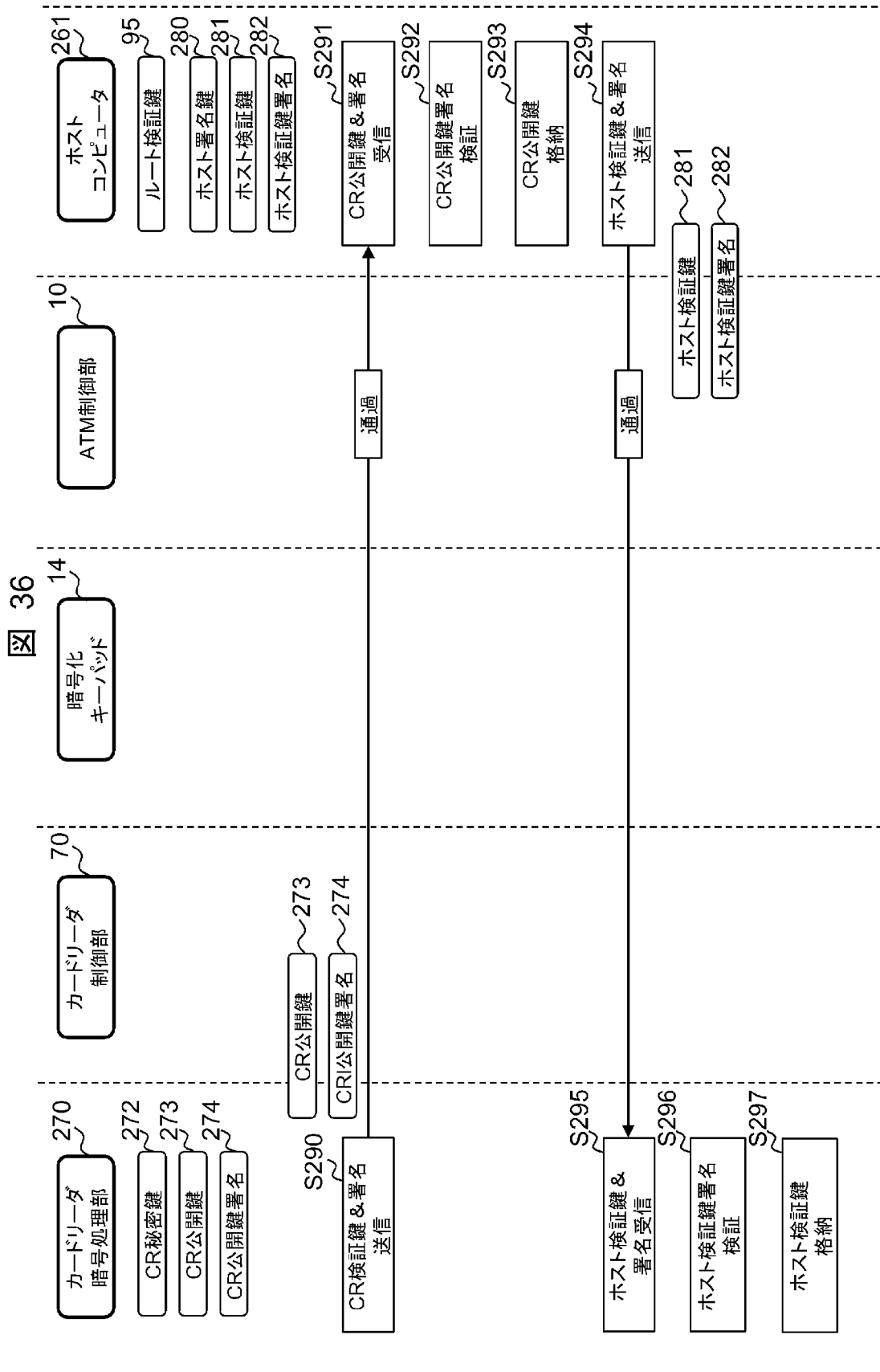
[図34]



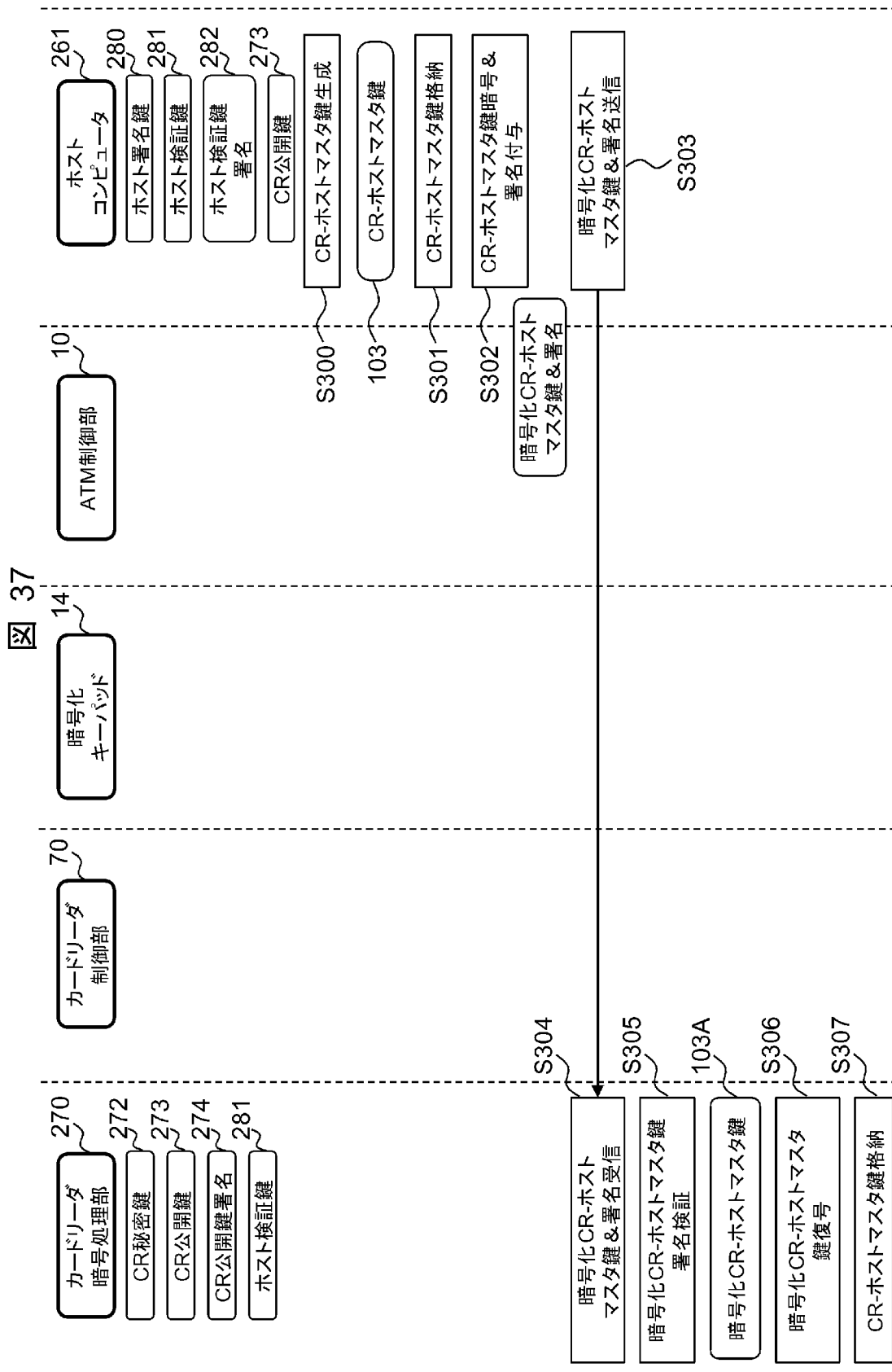
[図35]



[図36]



[図37]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/066630

A. CLASSIFICATION OF SUBJECT MATTER

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)

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	1996-2016
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.
Y	JP 2002-259866 A (NEC Communication Systems, Ltd.), 13 September 2002 (13.09.2002), paragraphs [0012] to [0042] (Family: none)	1-9
Y	JP 2010-20402 A (Oki Electric Industry Co., Ltd.), 28 January 2010 (28.01.2010), paragraph [0022] (Family: none)	1-9
Y	JP 2016-91132 A (Canon Marketing Japan Inc.), 23 May 2016 (23.05.2016), paragraphs [0008], [0067] to [0070] (Family: none)	3, 7

☒ 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
05 August 2016 (05.08.16)

Date of mailing of the international search report
16 August 2016 (16.08.16)

Name and mailing address of the ISA/
Japan Patent Office
3-4-3, Kasumigaseki, Chiyoda-ku,
Tokyo 100-8915, Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/066630

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-171717 A (Matsushita Electric Industrial Co., Ltd.), 26 June 1998 (26.06.1998), paragraph [0002] (Family: none)	4, 8

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl. 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. 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	1971-2016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
Y	JP 2002-259866 A（日本電気通信システム株式会社）2002.09.13, 【0012】 - 【0042】（ファミリーなし）	1-9
Y	JP 2010-20402 A（沖電気工業株式会社）2010.01.28, 【0022】（フ ァミリーなし）	1-9
Y	JP 2016-91132 A（キャノンマーケティングジャパン株式会社） 2016.05.23, 【0008】, 【0067】 - 【0070】（ファミリーなし）	3, 7

☒ 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

05.08.2016

国際調査報告の発送日

16.08.2016

国際調査機関の名称及びあて先

日本国特許庁（ISA/J P）

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）

山内 裕史

5 L

4064

電話番号 03-3581-1101 内線 3562

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
Y	JP 10-171717 A (松下電器産業株式会社) 1998. 06. 26, 【0002】 (ファミリーなし)	4, 8