

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B1)

(11) 特許番号

特許第6353128号
(P6353128)

(45) 発行日 平成30年7月4日(2018.7.4)

(24) 登録日 平成30年6月15日(2018.6.15)

(51) Int.Cl.

F I

G 0 7 D 9/00 (2006.01)

G 0 7 D 9/00 4 5 6 F

G 0 7 D 9/00 4 6 1 Z

請求項の数 6 (全 27 頁)

(21) 出願番号 特願2017-122585 (P2017-122585)

(22) 出願日 平成29年6月22日(2017.6.22)

審査請求日 平成29年6月22日(2017.6.22)

早期審査対象出願

(73) 特許権者 000237639

富士通フロンテック株式会社
東京都稲城市矢野口1776番地

(74) 代理人 100074099

弁理士 大菅 義之

(72) 発明者 久岡 武志

東京都稲城市矢野口1776番地 富士通
フロンテック株式会社内

(72) 発明者 山崎 宏

東京都稲城市矢野口1776番地 富士通
フロンテック株式会社内

(72) 発明者 大木 徹

東京都稲城市矢野口1776番地 富士通
フロンテック株式会社内

最終頁に続く

(54) 【発明の名称】 自動取引装置

(57) 【特許請求の範囲】

【請求項1】

金融取引を行う自動取引装置であって、

カードの磁気データの読み取り並びに書き込み、および、ICデータの読み取りが可能なカード取扱部と、

前記カードの磁気データの読み取りを未実行の段階で、前記ICデータへのアクセスを実行し、前記ICデータが正常に読み取れた場合に、前記ICデータを用いた金融取引を実行する処理部と、

を備えることを特徴とする自動取引装置。

【請求項2】

金融取引を行う自動取引装置であって、

カードの磁気データの読み取り並びに書き込み、および、ICデータの読み取りが可能なカード取扱部と、

前記カードの磁気データの読み取りを未実行の段階で、前記ICデータへのアクセスを実行し、前記ICデータが正常に読み取れた場合であり、且つ前記カードが自行のカードである場合、前記ICデータを用いた金融取引を実行する処理部と、

を備えることを特徴とする自動取引装置。

【請求項3】

金融取引を行う自動取引装置であって、

カードの磁気データの読み取り並びに書き込み、および、ICデータの読み取りが可能

10

20

なカード取扱部と、

前記カードの磁気データの読み取りを未実行の段階で、前記ＩＣデータへのアクセスを実行し、前記ＩＣデータが正常に読み取れた場合であり、且つ前記カードが他行のカードである場合、前記磁気データの読み取り結果に基づく金融取引を実行する処理部と、
を備えることを特徴とする自動取引装置。

【請求項４】

金融取引を行う自動取引装置であって、
カードの磁気データの読み取り並びに書き込み、および、ＩＣデータの読み取りが可能なカード取扱部と、

前記カードの磁気データの読み取りを未実行の段階で、前記ＩＣデータへのアクセスを実行し、前記ＩＣデータが正常に読み取れた場合に、前記ＩＣデータを用いた金融取引を実行し、正常に読み取れた前記ＩＣデータに基づく情報を、前記磁気データに上書きする制御を行う処理部と、

を備えることを特徴とする自動取引装置。

【請求項５】

金融取引を行う自動取引装置であって、
カードの磁気データの読み取り並びに書き込み、および、ＩＣデータの読み取りが可能なカード取扱部と、

前記カードの磁気データの読み取りを未実行の段階で、前記ＩＣデータへのアクセスを実行し、前記ＩＣデータが正常に読み取れた場合であり、且つ前記カードが自らのカードである場合、前記ＩＣデータを用いた金融取引を実行し、正常に読み取れた前記ＩＣデータに基づく情報を、前記磁気データに上書きする制御を行う処理部と、

を備えることを特徴とする自動取引装置。

【請求項６】

金融取引を行う自動取引装置であって、
カードの磁気データの読み取り並びに書き込み、および、ＩＣデータの読み取りが可能なカード取扱部と、

前記カードの磁気データの読み取りを未実行の段階で、前記ＩＣデータへのアクセスを実行し、前記ＩＣデータが正常に読み取れた場合であり、且つ前記カードが他行のカードである場合、前記磁気データの読み取り結果に基づく金融取引を実行し、正常に読み取れた前記ＩＣデータに基づく情報を、前記磁気データに上書きせず前記カードの返却を行う処理部と、

を備えることを特徴とする自動取引装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、金融取引を行う自動取引装置に関する。

【背景技術】

【０００２】

金融機関等に設置されているＡＴＭ（Automatic Teller Machine：現金自動預払機）等の自動取引装置では、利用者は、金融取引操作時に、一般的に銀行カードを使用する。

【０００３】

銀行カードはＭＳ（Magnetic Stripe：磁気ストライプ）カードである場合もあり、ＭＳ＆ＩＣ（Integrated Circuit集積回路）チップ搭載カードである場合もある。ＭＳ＆ＩＣチップ搭載カードは、磁気ストライプおよびＩＣチップが搭載された銀行カードである。

【０００４】

近年、銀行カードは、ＭＳカードから、ＭＳ＆ＩＣチップ搭載カードに主流が変わってきている。ここで、ＭＳカードに対する処理との互換性を維持する等の目的で、ＡＴＭ装置は、ＭＳ＆ＩＣチップ搭載カードにおいても、まずＭＳデータ（磁気データ）の読取を行なう。その後、ＡＴＭ装置は、ＭＳ＆ＩＣチップ搭載カード上のＩＣチップに記録され

10

20

30

40

50

ているＩＣデータへのアクセスを行う。

【０００５】

関連する技術として、例えば、キャッシュカードのＩＣチップ搭載フラグの有無をチェックする技術が提案されている（例えば、特許文献１を参照）。上記ＩＣチップ搭載フラグは、カードに貼付される磁気ストライプにおけるデータフォーマットにある予備フィールド領域に立てられる。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】特開２００２－３２８３２号公報

10

【発明の概要】

【発明が解決しようとする課題】

【０００７】

上述したように、ＭＳ＆ＩＣチップ搭載カードであっても、ＡＴＭは、まずＭＳデータの読み取りを行ない、読み取られたＭＳデータに基づく処理を行なう。上述した特許文献１の場合、ＡＴＭは、まず、磁気ストライプのＩＣチップ搭載フラグの有無をチェックし、その後、業務処理を実行する。

【０００８】

ＭＳデータは、不正な情報に書き換えられることがある。例えば、ＭＳ＆ＩＣカードのＭＳデータに、ＩＣチップが搭載されていないことを示す不正な情報が書き込まれた場合、カードにＩＣチップが搭載されているにもかかわらず、ＩＣチップに記憶されるＩＣデータは読み取られない。このため、不正な情報が書き込まれたＭＳデータに基づく金融取引が行われる可能性がある。

20

【０００９】

１つの側面として、本発明は、磁気ストライプとＩＣチップとを有するカードを用いた自動取引装置の金融取引を行う際のセキュリティの向上を図ることを目的とする。

【課題を解決するための手段】

【００１０】

態様の一例では、金融取引を行う自動取引装置は、カードの磁気データの読み取り並びに書き込み、および、ＩＣデータの読み取りが可能なカード取扱部と、前記カードの磁気データの読み取りを未実行の段階で、前記ＩＣデータへのアクセスを実行し、前記ＩＣデータが正常に読み取れた場合に、前記ＩＣデータを用いた金融取引を実行する処理部と、を含む。

30

【発明の効果】

【００１１】

１つの側面によれば、磁気ストライプとＩＣチップとを有するカードを用いた自動取引装置の金融取引を行う際のセキュリティの向上を図ることができる。

【図面の簡単な説明】

【００１２】

【図１】本実施形態のＡＴＭの外観図である。

40

【図２】本実施形態のＡＴＭのハードウェア構成例を示す図である。

【図３】主制御部のハードウェア構成例を示す図である。

【図４】第１の例の処理の流れの一例を示すフローチャート（その１）である。

【図５】第１の検出処理の流れの一例を示すフローチャートである。

【図６】第１の例の処理の流れの一例を示すフローチャート（その２）である。

【図７】第１の例の処理の流れの一例を示すフローチャート（その３）である。

【図８】第２の例の処理の流れの一例を示すフローチャート（その１）である。

【図９】第２の例の処理の流れの一例を示すフローチャート（その２）である。

【図１０】第２の例の処理の流れの一例を示すフローチャート（その３）である。

【図１１】第３の例の処理の流れの一例を示すフローチャート（その１）である。

50

【図 1 2】第 3 の例の処理の流れの一例を示すフローチャート（その 2）である。
【図 1 3】第 3 の例の処理の流れの一例を示すフローチャート（その 3）である。
【図 1 4】第 4 の例の処理の流れの一例を示すフローチャート（その 1）である。
【図 1 5】第 4 の例の処理の流れの一例を示すフローチャート（その 2）である。
【図 1 6】第 4 の例の処理の流れの一例を示すフローチャート（その 3）である。
【図 1 7】第 5 の例の処理の流れの一例を示すフローチャート（その 1）である。
【図 1 8】第 2 の検出処理の流れの一例を示すフローチャートである。
【図 1 9】第 5 の例の処理の流れの一例を示すフローチャート（その 2）である。
【図 2 0】第 5 の例の処理の流れの一例を示すフローチャート（その 3）である。
【図 2 1】第 6 の例の処理の流れの一例を示すフローチャート（その 1）である。
【図 2 2】第 6 の例の処理の流れの一例を示すフローチャート（その 2）である。
【図 2 3】第 6 の例の処理の流れの一例を示すフローチャート（その 3）である。
【図 2 4】第 7 の例の処理の流れの一例を示すフローチャート（その 1）である。
【図 2 5】第 7 の例の処理の流れの一例を示すフローチャート（その 2）である。
【図 2 6】第 7 の例の処理の流れの一例を示すフローチャート（その 3）である。
【図 2 7】第 8 の例の処理の流れの一例を示すフローチャート（その 1）である。
【図 2 8】第 8 の例の処理の流れの一例を示すフローチャート（その 2）である。
【図 2 9】第 8 の例の処理の流れの一例を示すフローチャート（その 3）である。

【発明を実施するための形態】

【0013】

<実施形態の自動取引装置>

以下、図面を参照して、実施形態について説明する。実施形態の自動取引装置は、A T M（現金自動預払機）であることを想定するが、A T M以外の各種の取引装置に適用されてもよい。実施形態の自動取引装置は、M SカードとM S & I Cカードとを取り扱い可能なA T Mであるとする。

【0014】

M Sカードは、M S（磁気ストライプ）を有するが、I Cチップを有しないカードである。M S & I Cカードは、M SとI Cチップとを有するカードである。M SカードおよびM S & I Cカードは、自動取引装置で金融取引を行う際に用いられるカード（銀行カード等）であるとする。

【0015】

以下の実施形態において、自動取引装置に挿入されるカードは、M S & I Cカードであることを想定する。ただし、自動取引装置に挿入されるカードは、M Sカードであってもよい。例えば、I Cチップの読み取りに対応していない自動取引装置は、M S & I Cカードを取り使いの対象外とする。M S & I Cカードを、以下、カードと称することがある。

【0016】

カードのM Sには、M Sデータが記録される。M Sデータは、磁気データの一例である。I Cチップには、I Cデータが記録される。自動取引装置は、挿入されたカードから、M Sデータの読み取り並びに書き込み、およびI CチップのI Cデータの読み取りを行なうことができる。なお、自動取引装置はI CチップにI Cデータを書込み可能な構成としてもよい。自動取引装置には、カード出入口が設置され、該カード出入口にカードが挿入されると、カード処理部等により、挿入されたカードに対して所定の処理が行なわれる。実施形態の自動取引装置は、カードが挿入された際、カードのM Sデータの読み取りを実行する前、またはM Sデータを確認する前に、I CチップのI Cデータにアクセスする。

【0017】

I Cデータの読み込み処理の結果が正常な場合、M Sデータの読み込み結果に基づく金融取引処理ではなく、I CチップのI Cデータの読み込み結果に基づく金融取引処理が行われる。該金融取引処理は、例えば、出金処理等である。

【0018】

従って、自動取引装置は、まずカードのＩＣチップからＩＣデータを読み取り、読み取られたＩＣデータに基づいて、金融取引を行うことから、ＭＳデータに不正な情報が記録されていたとしても、正常な金融取引が行われる。

【００１９】

カードのＭＳデータに対して、ＩＣチップが搭載されていないことを示す不正な書き込みがされた場合、ＩＣデータの読み取りが行われることなく、不正な書き込みがされたＭＳデータに基づく金融取引が行われる。

【００２０】

実施形態の自動取引装置は、ＭＳデータより先にＩＣデータを読み取り、ＩＣデータの読み取り結果に基づいて、各種の処理を行なう。従って、不正な金融取引が行われることが抑制され、ＭＳとＩＣチップとを有するカードを用いた金融取引を行う際のセキュリティの向上が図られる。

10

【００２１】

また、実施形態の自動取引装置は、カードのＩＣチップから正常にＩＣデータを読み込んだ場合、１回の金融取引ごとに、またはＭＳデータが異常である場合に、読み込まれたＩＣデータに基づく情報を、カードのＭＳに上書きする。

【００２２】

従って、カードのＭＳに不正な情報が記録されている場合でも、該カードのＭＳには、上記ＩＣデータに基づく情報が上書きされるため、カードのＭＳから不正な情報は消失し、正常な情報がカードのＭＳに書き込まれる。よって、カードのＭＳデータを正常な状態に復元できる。

20

【００２３】

また、カードのＭＳデータに異常が生じることがある。例えば、カードのＭＳデータの情報は、外部の電磁的な影響等により変更または消失することがある。上述したように、自動取引装置は、正常に読み込まれたＩＣデータに基づく情報を、カードのＭＳに上書きするため、カードのＭＳデータは正常な状態に復元される。

【００２４】

図１は、本実施形態による自動取引装置をＡＴＭ１００に適用した場合の外観図である。ＡＴＭ１００の筐体１０１には、利用者操作パネル１０２、カード出入口１０３、通帳出入口１０４、紙幣出入口１０５、硬貨出入口１０６および生体認証装置１０７が備え付けられている。ＡＴＭ１００には、他の機構や装置等が設けられてもよいし、上記の各部のうち一部が設けられなくてもよい。

30

【００２５】

図２は、本実施形態によるＡＴＭのハードウェア構成例を示す図である。ＡＴＭ１００は、主制御部２０２、記憶装置２０３、利用者操作表示部２０４、カード／レシート処理部２０５、通帳処理部２０６、紙幣処理部２０７、硬貨処理部２０８、ジャーナル処理部２０９、および生体認証処理部２１０を備える。

【００２６】

主制御部２０２は、実施形態における各種の処理を実行する。記憶装置２０３は、ＡＴＭ１００を制御するプログラムを含む各種制御プログラムやデータ群を記憶する。記憶装置２０３には、他の情報が記憶されてもよい。

40

【００２７】

利用者操作表示部２０４は、主制御部２０２による利用者取引処理の実行時に、主制御部２０２と連携して、利用者取引処理に関する表示を行うとともに、利用者取引処理の指示を入力させるための、例えば、図１の利用者操作パネル１０２である。該利用者操作パネル１０２は、例えば、タッチパネルディスプレイである。

【００２８】

カード／レシート処理部２０５は、主制御部２０２による利用者取引処理の実行時に、主制御部２０２と連携して、利用者のキャッシュカードや売上金入金カード等の磁気カードやＩＣカード等のカード類の読み込みや書き込み等を行なう。

50

【 0 0 2 9 】

カード/レシート処理部 2 0 5 は、例えば、カードリーダー装置である。また、カード/レシート処理部 2 0 5 は、主制御部 2 0 2 による利用者取引処理の実行時に、主制御部 2 0 2 と連携して、レシートへの印字を行う印字装置である。

【 0 0 3 0 】

実施形態のカード/レシート処理部 2 0 5 は、カードの M S データの読み取り並びに書き込みを行い、I C データの読み取りを行なう。カード/レシート処理部 2 0 5 は、カード取扱部の一例である。

【 0 0 3 1 】

通帳処理部 2 0 6 は、主制御部 2 0 2 による利用者取引処理の実行時に、主制御部 2 0 2 と連携して、通帳への印字を行う印字装置である。

10

【 0 0 3 2 】

紙幣処理部 2 0 7 は、不図示の紙幣入出金機構、紙幣識別機構、および紙幣収納機構を備える。紙幣入出金機構は、利用者が入金口から挿入した紙幣を入金し、または出金口から利用者へ紙幣を出金する機構である。紙幣識別機構は、入出金された紙幣の真贋や金種を識別する機構である。紙幣収納機構はさらに、不図示の紙幣スタッカ、紙幣カセット、紙幣リジェクトカセット等を含む。

【 0 0 3 3 】

紙幣スタッカは、紙幣収納機構に固定された収納部であり、入出金のための紙幣を一時的に収納する。紙幣カセットは、紙幣スタッカに紙幣を補充したり、紙幣スタッカの紙幣を回収するために用いられるカセットである。紙幣リジェクトカセットは、再度流通させるのに適さない紙幣を収納する。

20

【 0 0 3 4 】

硬貨処理部 2 0 8 は、不図示の硬貨入出金機構、硬貨識別機構、および硬貨収納機構を備える。硬貨入出金機構は、利用者が入金口から挿入した硬貨を入金し、または出金口から利用者へ硬貨を出金する機構である。

【 0 0 3 5 】

硬貨識別機構は、入出金された硬貨の真贋や金種を識別する機構である。硬貨収納機構はさらに、不図示の硬貨スタッカ、硬貨カセット、硬貨リジェクトカセット等を含む（特には図示しない）。

30

【 0 0 3 6 】

硬貨スタッカは、硬貨収納機構に固定された収納部であり、入出金のための硬貨を一時的に収納する。硬貨カセットは、硬貨スタッカに硬貨を補充したり、硬貨スタッカの硬貨を回収するために用いられるカセットである。硬貨リジェクトカセットは、再度流通させるのに適さない硬貨を収納する。

【 0 0 3 7 】

ジャーナル処理部 2 0 9 は、取引情報を記録等するジャーナル処理を実行する。また、A T M 1 0 0 は、外部電源と接続されて供給された電力を変換して、A T M 1 0 0 の各部へ電力を供給する不図示の電源供給部等を備える。生体認証処理部 2 1 0 は、生体認証装置 1 0 7 に対応する処理部であり、指紋認証や手のひら認証等の所定の生体認証に関する処理を行なう。

40

【 0 0 3 8 】

図 3 は、図 2 のうち、主制御部 2 0 2 のハードウェア構成の一例を示す図である。図 3 の例に示すように、バス 2 5 0 に対して、C P U (Central Processing Unit) 2 5 1 と R A M (Random Access Memory) 2 5 2 と R O M (Read Only Memory) 2 5 3 とが接続される。また、該バス 2 5 0 に対して、記録媒体 2 5 4 と通信インタフェース 2 5 5 と入出力インタフェース 2 5 6 とが接続される。

【 0 0 3 9 】

C P U 2 5 1 は、プロセッサであり、R A M 2 5 2 に展開されたプログラムを実行する。実行されるプログラムとしては、実施形態の処理を行うプログラムが適用されてもよい

50

。ROM 253はRAM 252に展開されるプログラムを記憶する不揮発性の記憶装置である。

【0040】

記録媒体254は、例えば、可搬型記録媒体であって、可搬型のメモリ（例えば、半導体メモリ）や光学式ディスク（例えば、CD（Compact Disc）やDVD（Digital Versatile Disc(DVD)）等が適用されてもよい。該記録媒体254に、実施形態の処理を実行するプログラムが記録されてもよい。

【0041】

通信インタフェース255は、外部との通信を行うインタフェースであって、例えば、ホストコンピュータ211と通信を行う。入出力インタフェース256は、図2の各部（カード/レシート処理部205等）と接続される。

10

【0042】

処理部202Aは、金融取引に関する各種の処理を行なう。上書き制御部202Bは、カードのMSデータに対して、ICデータに基づく情報を上書きする制御を行う。該制御に基づいて、カード/レシート処理部205は、カードのMSに対して、情報を上書きする。処理部202Aは、上書き制御部202Bの機能を含んでもよい。

【0043】

RAM 252に展開されたプログラムを、CPU 251が実行することで、処理部202Aおよび上書き制御部202Bの機能が実現される。

【0044】

20

RAM 252、ROM 253、記録媒体254は、何れもコンピュータ読み取り可能な有形の記憶媒体の一例である。これらの有形な記憶媒体は、信号搬送波のような一時的な媒体ではない。

【0045】

<第1の例の処理の流れの一例を示すフローチャート>

図4乃至図7の例のフローチャートを参照して、第1の例の処理について説明する。ATM 100を利用する利用者は、カードを用いて、該ATM 100を用いた金融取引を開始する。

【0046】

ATM 100は、所定の操作が行われたことを検出することにより、金融取引の開始を認識する。図4のフローチャートにおいて、上記所定の操作は、第1の検出処理（ステップS301）として示される。図5のフローチャートを参照して、第1の検出処理について説明する。

30

【0047】

図5（A）の例では、利用者操作パネル102に表示されている「支払いキー」の押下操作が検出される（ステップS261）。例えば、利用者は、利用者操作パネル102に表示されている内容に応じて、「支払いキー」（出金取引）を押下する。

【0048】

「支払いキー」の押下操作が検出されると、例えば、主制御部202は、利用者操作パネル102に、カードの挿入を促す指示を表示させる。利用者は、利用者操作パネル102の表示内容に応じて、カードを挿入する。

40

【0049】

カード/レシート処理部205は、カードが挿入されたことを検出する（ステップS262）。カード/レシート処理部205は、カードが挿入されたことを検出すると、挿入されたカードのMSに記録されたMSデータ（MS磁気）を読み取る（ステップS263）。読み取られたMSデータの情報は、例えば、記憶装置203やRAM 252等に記憶される。記憶装置203またはRAM 252は、記憶部の一例である。

【0050】

図5（B）の例では、カードの挿入が検出され（ステップS271）、MSデータの読み取りが行われ（ステップS272）、利用者操作表示部204に表示されている「支払

50

いキー」が押下されたかが検出される（ステップS 2 7 1）。

【 0 0 5 1 】

図 5（A）と図 5（B）とでは、処理の順序が異なるだけであり、各処理の内容は同様である。第 1 の検出処理は、図 5（A）の順序で行なわれてもよいし、図 5（B）の順序で行なわれてもよい。

【 0 0 5 2 】

上述したように、ステップ S 2 6 3 またはステップ S 2 7 2 において、M S データの読み取りが行なわれて、読み取られた M S データの情報が、記憶装置 2 0 3 または R A M 2 5 2 に記憶される。

【 0 0 5 3 】

ただし、読み取られた M S データは、カードの I C チップに記録された I C データが読み取られる前に、使用や参照等がされることはない。実施形態では、A T M 1 0 0 は、M S と I C チップとを有するカードが挿入された場合、I C チップの I C データの読み取り及び I C データの読み取り結果の確認を先に行い、その後、必要に応じて、M S データの読み取り結果の確認を行なう。

【 0 0 5 4 】

カード / レシート処理部 2 0 5 に挿入されたカードの読み取りは、1 度で成功するとは限らない。そこで、カード / レシート処理部 2 0 5 は、ステップ S 2 6 3 またはステップ S 2 7 2 の処理を、M S データの読み取りが成功するまで、所定回数繰り返してもよい。該所定回数には、所定の上限が設けられることが好ましい。M S の読み取り回数が多くなると、操作待ち時間が長くなることや M S の劣化度合いが進行するためである。

【 0 0 5 5 】

図 4 の例に示されるように、ステップ S 3 0 1 の第 1 の検出処理の後、処理部 2 0 2 A は、カード / レシート処理部 2 0 5 に対し、カードの I C チップからの I C データの読み込みの処理（アクセス）を実行させる（ステップ S 3 0 2）。ステップ S 3 0 2 の段階では、M S データは使用（または参照）されていない。

【 0 0 5 6 】

処理部 2 0 2 A は、カード / レシート処理部 2 0 5 での I C チップの読み取り結果が正常であるか、または異常であるかを判定する（ステップ S 3 0 3）。

【 0 0 5 7 】

処理部 2 0 2 A は、カードの I C チップを検知できなかった場合に、I C チップの読み取り結果が異常であると判定してもよい。また、I C チップから I C データが読み取られたとしても、該 I C データが、異常な情報であることを示す場合に、処理部 2 0 2 A は、I C チップの読み取り結果が異常であると判定してもよい。読み取られた I C データが異常な情報であることを示す場合、処理部 2 0 2 A は、カードを返却させる制御を行い、取引を終了させてもよい。

【 0 0 5 8 】

カード / レシート処理部 2 0 5 での I C チップの読み取り結果が正常であった場合には、処理部 2 0 2 A は、I C チップから読み取られた I C データで処理を継続する（ステップ S 3 1 1）。

【 0 0 5 9 】

ステップ S 3 0 2、S 3 0 3、S 3 1 1 と続く一連の処理は、M S データの読み取り結果ではなく、I C データの読み取り結果に基づく処理である。I C チップの I C データが利用できる場合は、A T M 1 0 0 は、カードの M S データを使用することなく、金融取引を継続することが可能となる。

【 0 0 6 0 】

従って、M S に不正な情報が記録されていたとしても、M S データよりも I C チップの I C データが先に使用される。該 I C データが正常に読み取られた場合には、M S データの情報が使用されることなく、I C データに基づく金融取引が行われる。

【 0 0 6 1 】

また、カードのMSに、ICチップがないことを示す不正な情報が記録されたとしても、MSデータよりも、ICデータが先に使用される。このため、カードのMSに、不正な情報が書き込まれたとしても、ICデータに基づく正常な金融取引が行われる。よって、セキュリティの向上が図られる。

【0062】

一方、上述したように、ICチップが検知されなかった場合等においては、ICチップの読み取り結果が異常と判定される。処理部202Aは、カード/レシート処理部205でのICチップの読み取り結果が異常であった場合、図4のステップS306からS310までの一連の処理等を実行する。

【0063】

ステップS306からS310までの一連の処理は、MSデータの読み取り結果に基づく処理である。例えば、各金融機関のATMの金融取引処理の共通仕様として、ステップS306からS310までの一連の処理（MSデータの読み取り結果に基づく処理）の仕様が適用されているとする。

【0064】

実施形態のATM100は、カードのICチップの読み取り結果に基づいて、上述したICデータの読み取り結果に基づく処理またはMSデータの読み取り結果に基づく処理の何れかを実行する。

【0065】

従って、ATM100において、各金融機関の共通仕様である「MSデータの読み取り結果に基づく処理」と、「ICデータの読み取り結果に基づく処理」とを両立させることができる。

【0066】

処理部202Aは、記憶装置203やRAM252等を参照して、第1の検出処理において、カード/レシート処理部205がMSデータを読取った結果が正常であったか異常であったかを判定する（ステップS306）。上述したように、ステップS301の第1の検出処理において、MSデータは、記憶装置203やRAM252等に記憶される。なお、MSデータの読み取り結果が異常とは、例えば、BCC等のデータ整合性チェックやMSデータ内（読み取りはできたとしても）のIC搭載フラグ等の情報が検出されない場合等も含み特に限定しない。また、MSデータ内（読み取りはできたとしても）のIC搭載フラグ等の情報が検出されない場合、MSデータの読み取りから、所定回数繰り返してもよい。

【0067】

処理部202Aは、記憶装置203やRAM252等に記憶されたMSデータの情報を参照して、ステップS306の判定を行なう。従って、第1の検出処理において、MSデータの読み取りが正常に行われていた場合には、ステップS306の時点で、改めて、MSデータの読み取りは行なわれない。このため、MSデータの読み取りを行なう時間が省かれる。

【0068】

MSデータの読み取り結果が正常であった場合には、処理部202Aは、カード/レシート処理部205でカードの逆挿入が検知されているか否かを判定する（ステップS307）。カードの挿入方向が、正常な方向と逆方向である場合、カードの読み取りが正常に行なわれないためである。

【0069】

カード/レシート処理部205でカードの逆挿入ではなく正常挿入が検知されている場合、処理部202Aは、MSデータに、挿入されているカードにICチップが搭載されているか否かを示すIC情報があるか否かを判定する（ステップS308）。

【0070】

上記IC情報がカードにない場合には、処理部202Aは、MSから読み取られたMSデータで処理を継続する（ステップS310）。これにより、ICチップが搭載されてい

10

20

30

40

50

ない旧型のカードにおいても、正常に金融取引を実行させることが可能となる。ステップ S 3 1 0 の後、処理は、ステップ S 3 1 5 に進む。

【 0 0 7 1 】

一方、上記 I C 情報がカードにある場合には、処理部 2 0 2 A は、カード / レシート処理部 2 0 5 に対して、カードに搭載されている I C チップの再読み取りを実行させる。処理部 2 0 2 A からの制御に基づいて、カード / レシート処理部 2 0 5 は、I C チップの再読み取りを行なう（ステップ S 3 0 8 - 1）。I C チップの再読み取りも、M S データの読み取りと同様、1 度で成功するとは限らない。そこで、カード / レシート処理部 2 0 5 は、I C チップからの I C データの読み取りが成功するまで、I C チップの読み取りを所定回数繰り返してもよい。

10

【 0 0 7 2 】

処理部 2 0 2 A は、カード / レシート処理部 2 0 5 で M S の読み取りと共に実行された I C チップの読み取り結果が正常であったか異常であったかを判定する（ステップ S 3 0 9）。なお、判定の結果が異常であった場合、I C チップからの I C データ読み取りから、所定回数繰り返してもよい。また、読み取り結果の異常についても M S データの異常と同様に特に限定しない。

【 0 0 7 3 】

カード / レシート処理部 2 0 5 による I C チップの再読み取り結果が正常であった場合には、処理部 2 0 2 A は、I C チップから読み取られた I C データに基づく金融取引の処理を継続する。従って、処理は、ステップ S 3 0 9 から S 3 1 1 に進む。

20

【 0 0 7 4 】

上述したように、ステップ S 3 0 3 の処理において、処理部 2 0 2 A は、I C チップの読み取り結果が正常であるか異常であるかを判定する。例えば、カード / レシート処理部 2 0 5 が I C チップを検知できなかった場合、I C チップの読み取り結果は異常であると判定される。

【 0 0 7 5 】

一方、カードの M S データに I C 情報があることを示す情報が記録されている場合、カードに I C チップは搭載されていることになる。従って、ステップ S 3 0 8 で、M S 内 I C 情報ありと判定された場合、カードの I C チップの再読み取りが行われる。

【 0 0 7 6 】

30

ステップ S 3 0 9 において、I C チップの再読み取りの結果が正常であると判定された場合、I C データに基づく金融取引の処理が継続する。従って、金融取引の際に、M S に記録されている M S データではなく I C チップに記録されている I C データが優先されるため、セキュリティの向上が図られる。

【 0 0 7 7 】

ステップ S 3 0 6 で M S データの読み取り結果が異常であると判定された場合、ステップ S 3 0 7 でカードが逆挿入されていると判定された場合、またはステップ S 3 0 9 で I C チップ再読み取り結果が以上であると判定された場合、処理は、ステップ S 3 1 2 に進む。

【 0 0 7 8 】

40

処理部 2 0 2 A は、カード / レシート処理部 2 0 5 に挿入されたカードを返却させると共に、利用者操作表示部 2 0 4 に、挿入されたカードが異常であるため窓口に出向くように促すことを表示させる（ステップ S 3 1 2）。

【 0 0 7 9 】

従って、M S カードと M S & I C カードとの互換性を維持しながら、I C チップ上の I C データが利用できる場合には、M S データを使用する前に、I C データを使用して金融取引を行うため、セキュリティの向上が図られる。

【 0 0 8 0 】

図 4 のステップ S 3 1 1 での I C データによる継続処理から、図 6 のステップ S 3 1 3 の処理が実行される。また、ステップ S 3 1 0 での M S データによる継続処理から、図 6

50

のステップS 3 1 5 の処理が実行される。

【 0 0 8 1 】

図 6 の例に示されるように、処理部 2 0 2 A は、ステップ S 3 1 1 での I C データによる継続処理を実行した場合には、I C データに生体認証のための静脈データが登録されていれば、図 1 の生体認証装置 1 0 7 による生体認証を実施する（ステップ S 3 1 3 ）。

【 0 0 8 2 】

利用者は、利用者操作表示部 2 0 4 に表示されたガイダンス表示に従って、生体認証装置 1 0 7 に登録した手のひらまたは指をかざす。これにより、生体認証が実施される。

【 0 0 8 3 】

次に、処理部 2 0 2 A は、I C チップ内に格納されている全銀 A P（アプリケーション）と通信できるか確認する（ステップ S 3 1 4 ）。

10

【 0 0 8 4 】

一方、処理部 2 0 2 A は、ステップ S 3 1 0 での M S データによる継続処理を実行した場合には、上述のステップ S 3 1 3 および S 3 1 4 の処理はスキップする。

【 0 0 8 5 】

次に、処理部 2 0 2 A は、利用者からの暗証番号の入力を待つ（ステップ S 3 1 5 ）。

利用者は、利用者操作表示部 2 0 4 から暗証番号を入力する。A T M 1 0 0 は、該暗証番号の入力を受け付ける。なお、ステップ S 3 1 3 での生体認証に成功している場合には、ステップ S 3 1 5 の処理はスキップしてもよい。

【 0 0 8 6 】

20

金融取引が出金取引の場合、処理部 2 0 2 A は、利用者による利用者操作表示部 2 0 4 からの出金金額の入力・確認操作を受け付ける（ステップ S 3 1 6 ）。以下、金融取引は、出金取引であるものとして説明するが、該金融取引は、出金取引以外であってもよい。

【 0 0 8 7 】

処理部 2 0 2 A は、図 4 のステップ S 3 1 1 から移行してきた場合のみ、カード上の I C チップにホストコンピュータ 2 0 1 と通信するための認証情報を要求し、その要求結果が正常であるか否かを判定する（ステップ S 3 1 7 ）。

【 0 0 8 8 】

上記要求結果が異常であった場合には、処理部 2 0 2 A は、カード / レシート処理部 2 0 5 に、挿入されているカードを返却させると共に、異常終了を利用者操作表示部 2 0 4 に表示させる（ステップ S 3 2 3 ）。そして、金融取引は終了する。

30

【 0 0 8 9 】

処理部 2 0 2 A は、図 4 のステップ S 3 1 1 から移行してきて上記要求結果が正常であった場合に、ホストコンピュータ 2 0 1 に、I C データに基づく支払要求の電文を送信する（ステップ S 3 1 8 ）。つまり、図 4 のステップ S 3 1 1 からステップ S 3 1 8 に処理が移行してきた場合、処理部 2 0 2 A は、I C データを用いた金融取引を実行する。

【 0 0 9 0 】

また、処理部 2 0 2 A は、図 4 のステップ S 3 1 0 からステップ S 3 1 8 に処理が移行してきた場合も、ホストコンピュータ 2 0 1 に、M S データに基づく支払要求の電文を送信する（ステップ S 3 1 8 ）。なお、図 4 のステップ S 3 1 1 から移行してきた場合には、上記電文には、ステップ S 3 1 7 で取得した認証情報が含まれる。

40

【 0 0 9 1 】

この結果、ホストコンピュータ 2 0 1 は、上記認証情報（図 4 のステップ S 3 1 1 から移行した場合）または暗証番号（図 4 のステップ S 3 1 0 から移行した場合）に基づく利用者認証を実施する。

【 0 0 9 2 】

ホストコンピュータ 2 0 1 は、認証 O K の場合には、支払許可の電文を A T M 1 0 0 に送信する。この結果、A T M 1 0 0 の処理部 2 0 2 A は、ホストコンピュータ 2 0 1 から支払許可を受信する（ステップ S 3 1 9 ）。

【 0 0 9 3 】

50

処理部 202A は、図 4 のステップ S 3 1 1 から移行してきた場合のみ、カード / レシート処理部 205 を介して、IC チップに上記支払許可の情報を通知し、その処理結果を取得する (ステップ S 3 2 0)。処理部 202A は、この処理結果が異常の場合には、ATM 100 の装置を休止させる (ステップ S 3 2 4)。そして、金融取引は終了する。

【0094】

処理部 202A は、図 4 のステップ S 3 1 1 から移行してきて上記処理結果が正常であった場合、または図 4 のステップ S 3 1 0 から移行してきた場合には、紙幣処理部 207 および硬貨処理部 208 に対して、支払現金を計数させる (ステップ S 3 2 1)。

【0095】

更に、処理部 202A は、カード / レシート処理部 205 に対してレシートへの支払金額の印字処理を実行させ、通帳が挿入されている場合には通帳処理部 206 に対して通帳への支払金額および残高の印字処理を実行させる (ステップ S 3 2 2)。処理部 202A は、ジャーナル処理部 209 にジャーナル処理を実行させてもよい。

【0096】

以上、図 6 の一連のステップによる金融取引処理が完了した後、処理部 202A は、ステップ S 3 2 5 以降の処理を実行する。図 7 を参照して、ステップ S 3 2 5 以降の処理について説明する。

【0097】

図 7 の各処理は、図 4 のステップ S 3 1 1 から移行した場合に主に実行される処理である。つまり、図 7 の各処理は、IC チップから読み込まれた IC データに基づく処理であり、ステップ S 3 1 0 から移行した場合、IC チップから IC データは読み込まれていない。従って、以下の処理において、処理部 202A は、カードの IC チップから既に IC データを読み込んでいる。

【0098】

処理部 202A は、IC チップから読み込まれた IC データに基づいて、カード / レシート処理部 205 に挿入されているカードが自行のカード (自行 IC カード) であるか否かを判定する (ステップ S 3 2 5)。

【0099】

例えば、IC データには、金融機関を識別するコード (金融機関コード) が含まれる。処理部 202A は、該金融機関コードに基づいて、挿入されたカードが、ATM 100 が属する金融機関 (自行) のカードであるか、自行以外の他の金融機関 (他行) のカードであるかを判定してもよい。

【0100】

処理部 202A が、挿入されたカードが自行のカードであると判定した場合 (ステップ S 3 2 5 で YES)、処理部 202A は、IC データに基づいて、挿入されたカードがクレジットカード一体型のカードであるか否かを判定する (ステップ S 3 2 6)。

【0101】

クレジットカード一体型のカードは、クレジットカードの機能を含む銀行カードである。例えば、IC データには、カードが、クレジットカード一体型のカードであるか否かを識別する情報が含まれている。処理部 202A は、該情報に基づいて、ステップ S 3 2 6 の判定を行ってもよい。

【0102】

上記カードがクレジットカード一体型のカードではないと判定された場合 (ステップ S 3 2 6 で NO)、上書き制御部 202B は、IC チップから読み取られた IC データから、MS データを生成する処理を実行する (ステップ S 3 2 7)。

【0103】

上書き制御部 202B は、カード / レシート処理部 205 に、ステップ S 3 2 7 で生成した MS データを、挿入されているカードの MS に上書きする制御を行う。該制御に基づいて、カード / レシート処理部 205 は、挿入されているカードの MS に、IC データの情報を上書きする (ステップ S 3 2 8)。

10

20

30

40

50

【 0 1 0 4 】

上書き制御部 2 0 2 B は、 I C データから読み取った情報に基づいて、ホストコンピュータ 2 1 1 と通信を行い、該ホストコンピュータ 2 1 1 から、 M S に上書きする情報を取得する制御を行ってもよい。

【 0 1 0 5 】

上記の場合、上書き制御部 2 0 2 B は、ホストコンピュータ 2 1 1 から取得した情報を、挿入されているカードの M S に上書きする制御を行う。該制御に基づいて、カード/レシート処理部 2 0 5 は、挿入されている M S に、ホストコンピュータ 2 1 1 から取得された情報を上書きする。

【 0 1 0 6 】

10

上書き制御部 2 0 2 B は、 1 回の金融取引が行われるごとに、挿入されているカードの M S に、 I C データの情報（またはホストコンピュータ 2 1 1 から取得された情報）を上書きする。

【 0 1 0 7 】

従って、カードの M S に不正な情報が記録されていたとしても、正常に読み取られた I C データの情報が、 1 回の金融取引ごとに、カードの M S に上書きされる。このため、カードの M S に記録されていた不正な情報は消失し、正常な情報がカードの M S に記録される。

【 0 1 0 8 】

従って、該カードを用いた次の金融取引を行う際には、カードの M S には正常な情報が上書きされているため、 A T M を用いた不正な情報に基づく金融取引が抑制される。例えば、 A T M の中には、 I C チップの読み取りに対応していない A T M も存在する。

20

【 0 1 0 9 】

上述したように、カードの M S に不正な情報が記録されたとしても、該不正な情報は、正常な情報に上書きされる。従って、 I C チップ非対応の A T M で、上記カードを用いた金融取引が行われたとしても、 M S には正常な情報が記録されているため、不正な情報に基づく金融取引が抑制される。

【 0 1 1 0 】

処理部 2 0 2 A は、ステップ S 3 2 8 での M S への書込処理結果が正常であったか異常であったかを判定する（ステップ S 3 2 9 ）。例えば、処理部 2 0 2 A は、カード/レシート処理部 2 0 5 に対して、挿入されたカードの M S から、再度、 M S データを読み出すように制御する。該制御に基づいて、カード/レシート処理部 2 0 5 は、挿入されたカードの M S から、再度、 M S データを読み出す。

30

【 0 1 1 1 】

そして、処理部 2 0 2 A は、再度、読み出された M S データが正常であるか否かに基づいて、ステップ S 3 2 9 の判定を行ってもよい。

【 0 1 1 2 】

M S への書込処理結果が正常であった場合、処理部 2 0 2 A は、カード/レシート処理部 2 0 5 に、挿入されているカードを返却させる（ステップ S 3 3 0 ）。

【 0 1 1 3 】

40

また、ステップ S 3 2 5 において、処理部 2 0 2 A が、挿入されたカードが自行 I C カードでないと判定した場合（ステップ S 3 2 5 で N O ）、処理は、ステップ S 3 3 0 に進む。また、ステップ S 3 2 6 において、処理部 2 0 2 A が、挿入されたカードがクレジット一体型カードであると判定した場合（ステップ S 3 2 6 で Y E S ）、処理は、ステップ S 3 3 0 に進む。

【 0 1 1 4 】

ステップ S 3 2 9 において、 M S への書込処理結果が異常であると判定された場合、処理部 2 0 2 A は、カード/レシート処理部 2 0 5 に、挿入されているカードを返却させる。

【 0 1 1 5 】

50

そして、処理部 202A は、利用者操作表示部 204 に、挿入されたカードに基づく金融取引は正常に完了したが、カードの MS データが異常であるため窓口に出向くように促すことを表示させる（ステップ S331）。

【0116】

金融取引が出金取引の場合、処理部 202A は、紙幣処理部 207 および硬貨処理部 208 から紙幣出入口 105 または硬貨出入口 106 に、現金を放出させて（ステップ S332）、出金取引を終了する。以上のステップ S301 ~ S332 までの処理により、1 回の金融取引が行なわれる。

【0117】

従って、MS と IC チップとを有するカードを用いた金融取引を行う際、カードの MS データが使用される前に（MS データが正常であるか異常であるかが未確認の段階で）、IC データが正常に読み取られたかが判定される。そして、IC データが正常に読み取られた場合に、IC データを用いた金融取引が行われる。

【0118】

カードの MS データに、IC チップがないことを示す不正な情報が記録されたとしても、処理部 202A は、MS データよりも先に、IC チップの IC データにアクセスし、該 IC データに基づいて、金融取引を行う。従って、MS と IC チップとを有するカードを用いた ATM の金融取引におけるセキュリティが向上する。

【0119】

また、上書き制御部 202B は、1 回の金融取引ごとに、正常に読み取られた IC データに基づく情報を、カードの MS に上書きする制御を行う。従って、カードの MS に、IC チップがないことを示す不正な情報が記録されていたとしても、カードの MS を正常な情報に復元できる。

【0120】

また、MS データが壊れていて正常な書込みができない場合であっても、利用者は通常通り金融取引を完了させることができ、時間があるときに銀行窓口に出向いてカードの更新を行えばよいため、利用者の利便性を損なうことがない。

【0121】

< 第 2 の例 >

次に、図 8 乃至図 10 のフローチャートを参照して、第 2 の例について説明する。第 2 の例は、第 1 の例のステップ S303 に続く処理として、ステップ S304 が追加された点で、第 1 の例と異なる。

【0122】

図 8 の例に示されるように、ステップ S303 において、処理部 202A は、IC チップの読み取り結果が正常であるか、異常であるかを判定する。IC チップの読み取り結果が正常であると判定された場合、処理部 202A は、挿入されたカードが自らのカードであるか、他行のカードであるかを判定する（ステップ S304）。

【0123】

第 2 の例では、ステップ S303 で IC チップの読み取り結果が正常であると判定され、且つステップ S304 で挿入されたカードが自らのカードであると判定された場合に、処理は、ステップ S311 の「IC データで処理継続」に進む。

【0124】

上述したように、ステップ S302、S303、S111 と続く一連の処理は、IC データの読み取り結果に基づく処理である。一方、ステップ S306 から S310 までの一連の処理は、MS データの読み取り結果に基づく処理である。

【0125】

「MS データの読み取り結果に基づく処理」が各金融機関の共通仕様である場合、ステップ S303 の判定結果に基づいて、「IC データの読み取り結果に基づく処理」または「MS データの読み取り結果に基づく処理」の何れかに移行する。

【0126】

10

20

30

40

50

従って、ＡＴＭ１００において、各金融機関の共通仕様である「ＭＳデータの読み取り結果に基づく処理」と、「ＩＣデータの読み取り結果に基づく処理」とを両立させることができる。

【０１２７】

この際、金融機関によっては、ＡＴＭ１００に挿入されたカードが他行カードである場合には、各金融機関の共通仕様である「ＭＳデータの読み取り結果に基づく処理」を、ＡＴＭ１００に実行させることが好ましい場合がある。

【０１２８】

そこで、ステップＳ３０４において、挿入されたカードが、他行のカードであると判定された場合、処理部２０２Ａは、上記「ＭＳデータの読み取り結果に基づく処理」を実行させる。

10

【０１２９】

従って、ＡＴＭ１００に、「ＭＳデータの読み取り結果に基づく処理」と、「ＩＣデータの読み取り結果に基づく処理」との何れを実行させるかを、自行のカードであるか否かに基づいて決定できるため、ＡＴＭのシステムの柔軟な運用を実現できる。

【０１３０】

ステップＳ３０９において、ＩＣチップの再読み取りの結果が正常であると判定された場合、処理は、ステップＳ３１１に進む。従って、例えば、ＩＣチップが搭載されている他行のカードが挿入された場合であっても、ＭＳに記録されているＭＳデータよりもＩＣチップのＩＣデータを用いた金融取引を優先させることができる。

20

【０１３１】

ステップＳ３１０の処理が行われた場合、処理は、図９のステップＳ３１５に進む。ステップＳ３１１の処理が行われた場合は、処理は、図９のステップＳ３１３に進む。図９のフローチャートの各処理は、第１の例における図６のフローチャートの各処理と同様である。

【０１３２】

また、図９のステップＳ３２２の処理が終了すると、処理は、図１０のステップＳ３２５に進む。図１０のフローチャートの各処理は、第１の例における図７のフローチャートの各処理と同様である。

【０１３３】

30

< 第３の例 >

図１１乃至図１３のフローチャートを参照して、第３の例について説明する。第３の例は、第１の例における図７のステップＳ３２５の処理の後に、ステップＳ３２５－１の処理が追加された点で、第２の例と異なる。

【０１３４】

図１１のフローチャートの各処理は、第２の例における図８のフローチャートの各処理と同様である。ステップＳ３１０の処理が行われた場合は、処理は、図１２のステップＳ３１５に進む。ステップＳ３１１の処理が行われた場合は、処理は、図１２のステップＳ３１３に進む。図１２のフローチャートの各処理は、第１の例のける図６のフローチャートの各処理と同様である。

40

【０１３５】

図１３の例において、ステップＳ３２５の判定結果がＹＥＳである場合、処理部２０２Ａは、挿入されたカードのＭＳを読み取り、読み取り結果が正常であるか、異常であるかを判定する（ステップＳ３２５－１）。例えば、挿入されたカードのＭＳが損傷している場合、処理部２０２Ａは、読み取り結果が異常であると判定してもよい。

【０１３６】

また、図１１のステップＳ３０３において、ＩＣチップの読み取り結果が正常であると判定されたにもかかわらず、ステップＳ３２５－１で、カードのＭＳに、ＩＣチップがないことを示す情報が記録されている場合がある。この場合、カードのＭＳに不正な情報が記録されている可能性があり、処理部２０２Ａは、読み取り結果が異常であると判定して

50

もよい。なお、カードのMSデータは、第1の検出処理（ステップ301）で検出したデータを判定してもよいし、判定直前にカードのMSを読取ってから判定してもよい。さらに異常の場合、所定回数読取りと判定を繰り返してもよい。

【0137】

ステップS326の判定がNOである場合、ステップS328において、カードのMSデータは上書きされる。従って、上記のように、カードのMSに不正な情報が記録されている場合でも、カードのMSには、正常に読み取られたICデータの情報が上書きされる。従って、カードのMSから不正な情報は消失し、該カードのMSには正常な情報が上書きされることから、該カードを用いた金融取引を行う際のセキュリティが向上する。

【0138】

第3の例では、挿入されたカードのMSの読み取り結果が正常である場合には、カードのMSに上書きはされない。従って、上書きの必要がない場合に、カードのMSに上書きがされないため、カードのMSに対する書き込み回数を低減できる。従って、カードのMSの劣化度合いの進行を遅くすることができる。

【0139】

<第4の例>

図14乃至図16のフローチャートを参照して、第4の例について説明する。第4の例における図14のフローチャートの各処理は、第1の例における図4のフローチャートと同様である。

【0140】

ステップS310の処理が行われた場合は、処理は、図15のステップS315に進む。ステップS311の処理が行われた場合は、処理は、図15のステップS313に進む。図15のフローチャートの各処理は、第1の例における図6のフローチャートの各処理と同様である。第4の例における図16のフローチャートの各処理は、第3の例における図13のフローチャートの各処理と同様である。

【0141】

上述した第1の例～第4の例は、第5の例～第8の例を説明するための参考例である。

<第5の例>

図17乃至図20のフローチャートを参照して、第5の例について説明する。図17のフローチャートに示されるように、第5の例において、第2の検出処理が行なわれる（S301-1）。第2の検出処理について、図18のフローチャートを参照して、説明する。

【0142】

図18（A）の例では、利用者操作表示部204に表示されている「支払いキー」の押下操作が検出され（ステップS261）、カードの挿入が検出される（ステップS262）。図18（B）の例では、カードの挿入が検出され（ステップS271）、「支払いキー」の押下が検出される（ステップS272）。

【0143】

図18（A）または図18（B）の何れかの処理が行なわれると、金融取引が開始されたことが検出される（第2の検出処理）。第1の例で説明した第1の検出処理（図5）とは異なり、第2の検出処理では、カードのMSは読み取られない。

【0144】

図17のフローチャートに示されるように、第2の検出処理が行われた後、ICチップのICデータが読み取られる（ステップS302）。従って、カードのMSデータの読み取りが未実行の段階で、ICデータが読み取られる。

【0145】

ステップS303で、ICチップの読み取り結果が異常であると判定された場合、カード/レシート処理部205は、カードのMSデータを読み取る（ステップS305）。一方、ステップS303で、ICチップの読み取りが正常であると判定された場合、ステップS305の処理は実行されない。

10

20

30

40

50

【 0 1 4 6 】

第 1 の例～第 4 の例では、第 1 の検出処理において、カードの M S データは、I C データに対するアクセスよりも前に使用されることはないが、M S データの読み取りは行なわれる。一方、第 5 の例では、ステップ S 3 0 3 において、I C チップの読み取り結果が正常であると判定された場合、カードの M S データの読み取りは行なわれない。

【 0 1 4 7 】

上述したように、ステップ S 3 0 6 から S 3 1 0 までの一連の処理は、M S データの読み取り結果に基づく処理であり、例えば、所定の仕様に応じた処理である。一方、S 3 0 2、S 3 0 3、S 3 1 1 と続く一連の処理は、I C データの読み取り結果に基づく処理である。なお、ステップ S 3 0 6 の M S データの読み取り結果が異常な場合、ステップ S 3 0 5 のカードの M S データ読み取りから、所定回数繰り返してもよい。

10

【 0 1 4 8 】

処理部 2 0 2 A は、M S データの読み取り結果に基づく処理を行う際に、M S データの読み取りを行なうように制御し、I C データの読み取り結果に基づく処理を行う際には、M S データの読み取りを行なわないように制御する。

【 0 1 4 9 】

これにより、カードの M S に不正な情報が記録されていたとしても、I C データの読み取り結果に基づく処理が行われる場合には、A T M 1 0 0 は、上記不正な情報を読み込むことなく、金融取引を完了することができる。

【 0 1 5 0 】

20

図 1 7 のフローチャートにおける上述した処理以外の各処理は、第 1 の例における図 4 のフローチャートの各処理と同様である。ステップ S 3 0 3 の処理の後、挿入されたカードが自らのカードであるか、他行のカードであるかの判定は行われない。

【 0 1 5 1 】

ステップ S 3 1 0 の処理が行われた場合は、処理は、図 1 9 のステップ S 3 1 5 に進む。ステップ S 3 1 1 の処理が行われた場合は、処理は、図 1 9 のステップ S 3 1 3 に進む。図 1 9 のフローチャートの各処理は、第 1 の例における図 6 のフローチャートの各処理と同様である。図 2 0 のフローチャートの各処理は、第 1 の例における図 7 のフローチャートの各処理と同様である。

【 0 1 5 2 】

30

< 第 6 の例 >

図 2 1 乃至図 2 3 のフローチャートを参照して、第 6 の例について説明する。図 2 1 の例に示されるように、第 6 の例は、第 5 の例に、ステップ S 3 0 4 を追加した例である。該ステップ S 3 0 4 は、第 2 の例のステップ S 3 0 4 と同様である。

【 0 1 5 3 】

ステップ S 3 0 3 の判定が行なわれた後、ステップ S 3 0 4 において、挿入されたカードが、自らのカードであるか、他行のカードであるかが判定される。

【 0 1 5 4 】

第 6 の例では、ステップ S 3 0 4 で、挿入されたカードが他行のカードであると判定された場合、処理は、ステップ S 3 0 5 に進む。この場合、ステップ S 3 0 5 において、M S データの読み取りが行われる。

40

【 0 1 5 5 】

ステップ S 3 0 3 で、I C チップの読み取り結果が正常であると判定され、且つステップ S 3 0 4 で、挿入されたカードが自らのカードであると判定された場合、M S データの読み取りは行われない。

【 0 1 5 6 】

ステップ S 3 1 0 の処理が行われた場合は、処理は、図 2 2 のステップ S 3 1 5 に進む。ステップ S 3 1 1 の処理が行われた場合は、処理は、図 2 2 のステップ S 3 1 3 に進む。図 2 2 のフローチャートの各処理は、第 1 の例における図 6 のフローチャートの各処理と同様である。図 2 3 のフローチャートの各処理は、第 1 の例における図 7 のフローチャ

50

ートの各処理と同様である。

【 0 1 5 7 】

< 第 7 の例 >

図 2 4 乃至図 2 6 のフローチャートを参照して、第 7 の例について説明する。第 7 の例における図 2 4 のフローチャートの各処理は、第 5 の例における図 1 7 のフローチャートの各処理と同様である。

【 0 1 5 8 】

ステップ S 3 1 0 の処理が行われた場合は、処理は、図 2 5 のステップ S 3 1 5 に進む。ステップ S 3 1 1 の処理が行われた場合は、処理は、図 2 5 のステップ S 3 1 3 に進む。図 2 5 のフローチャートの各処理は、第 1 の例における図 6 のフローチャートの各処理と同様である。

10

【 0 1 5 9 】

図 2 6 のフローチャートにおいて、ステップ S 3 2 5 の後、ステップ S 3 2 5 - 1 において、MS 読み取り結果が正常であるか、異常であるかが判定される。図 2 6 のフローチャートは、第 3 の例における図 1 3 のフローチャートと同様である。

【 0 1 6 0 】

< 第 8 の例 >

図 2 7 乃至図 2 9 のフローチャートを参照して、第 8 の例について説明する。第 8 の例における図 2 7 のフローチャートの各処理は、第 6 の例における図 2 1 のフローチャートの各処理と同様である。

20

【 0 1 6 1 】

ステップ S 3 1 0 の処理が行われた場合は、処理は、図 2 8 のステップ S 3 1 5 に進む。ステップ S 3 1 1 の処理が行われた場合は、処理は、図 2 8 のステップ S 3 1 3 に進む。図 2 8 のフローチャートの各処理は、図 6 のフローチャートの各処理と同様である。

【 0 1 6 2 】

図 2 9 のフローチャートにおいて、ステップ S 3 2 5 の後、ステップ S 3 2 5 - 1 において、MS 読み取り結果が正常であるか、異常であるかが判定される。図 2 9 のフローチャートは、第 3 の例における図 1 3 のフローチャートと同様である。

【 符号の説明 】

【 0 1 6 3 】

30

- 1 0 0 A T M
- 1 0 1 A T M 筐体
- 1 0 2 利用者操作パネル
- 1 0 3 カード出入口
- 1 0 4 通帳出入口
- 1 0 5 紙幣出入口
- 1 0 6 硬貨出入口
- 1 0 7 生体認証装置
- 2 0 2 主制御部
- 2 0 2 A 処理部
- 2 0 2 B 上書き制御部
- 2 0 3 記憶装置
- 2 0 4 利用者操作表示部
- 2 0 5 カード / レシート処理部
- 2 0 6 通帳処理部
- 2 0 7 紙幣処理部
- 2 0 8 硬貨処理部
- 2 0 9 ジャーナル処理部
- 2 1 0 生体認証処理部
- 2 1 1 ホストコンピュータ

40

50

250	バス
251	CPU
252	RAM
253	ROM
254	記録媒体
255	通信インタフェース
256	入出力インタフェース

【要約】

【課題】磁気ストライプとＩＣチップとを有するカードを用いた金融取引を行う際のセキュリティの向上を図ることを目的とする。

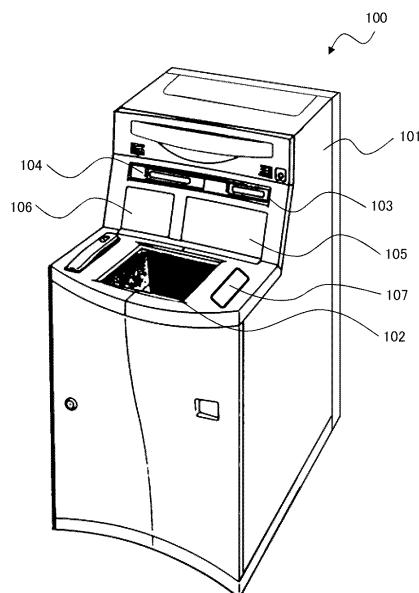
10

【解決手段】金融取引を行う自動取引装置は、カードの磁気データの読み取り並びに書き込み、および、ＩＣデータの読み取りが可能なカード／レシート処理部と、前記カードの磁気データの読み取りを未実行の段階で、前記ＩＣデータへのアクセスを実行し、前記ＩＣデータが正常に読み取れた場合に、前記ＩＣデータを用いた金融取引を実行する各処理部と、を含む。

【選択図】図２

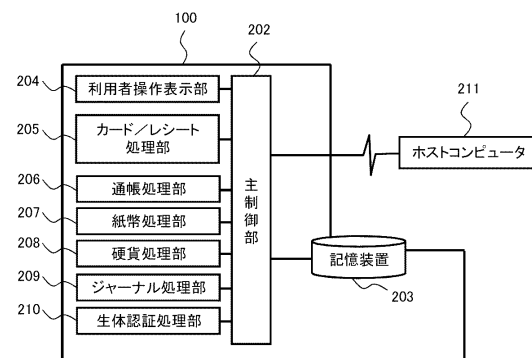
【図１】

本実施形態のATMの外観図



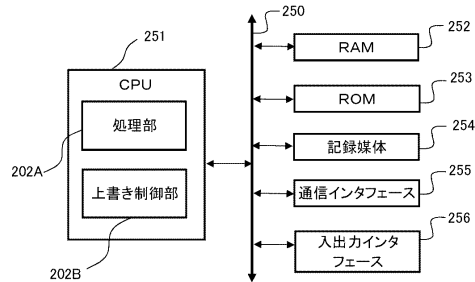
【図２】

本実施形態のATMのハードウェア構成例を示す図

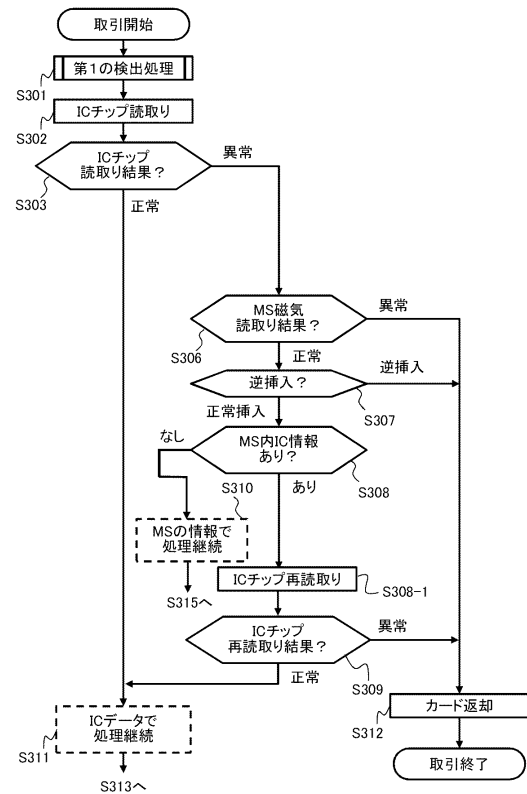


【図 3】

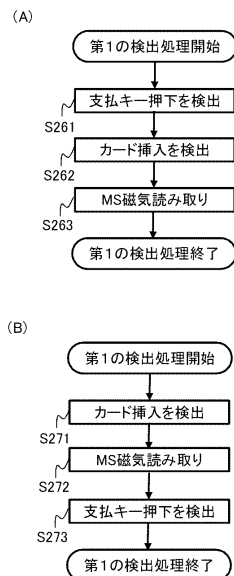
主制御部のハードウェア構成例を示す図



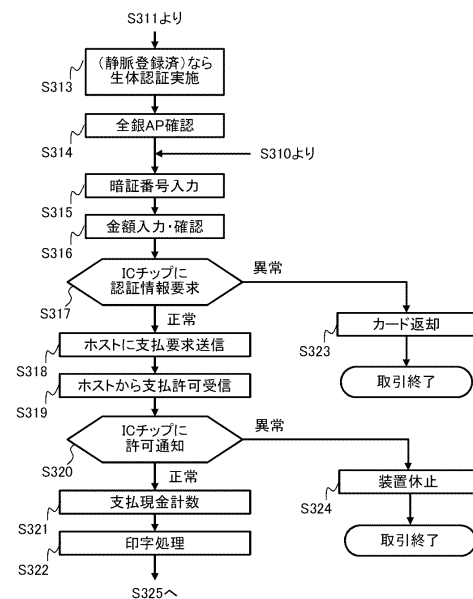
【図 4】

第1の例の処理の流れの一例を示す
フローチャート（その1）

【図 5】

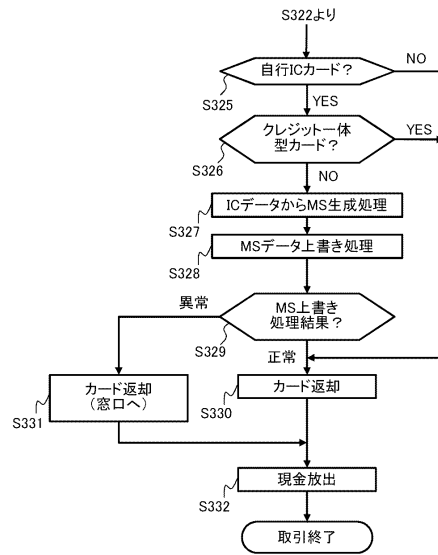
第1の検出処理の流れの
一例を示すフローチャート

【図 6】

第1の例の処理の流れの一例を示す
フローチャート（その2）

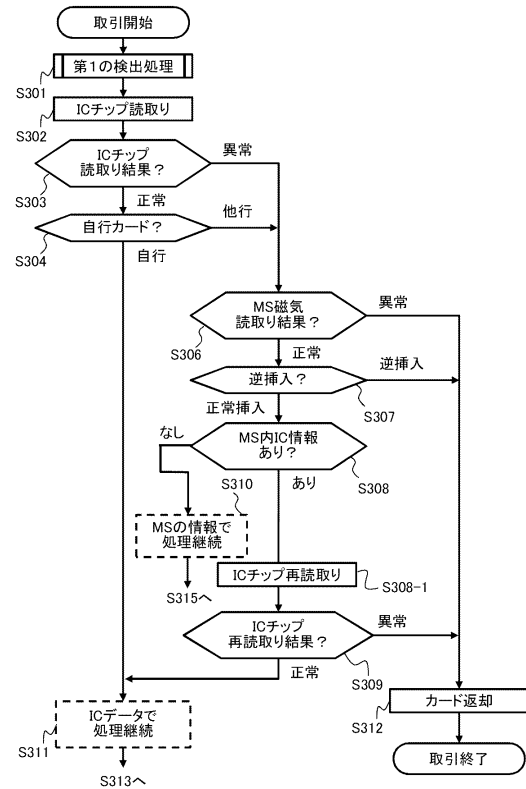
【図 7】

第1の例の処理の流れの一例を示す
フローチャート(その3)



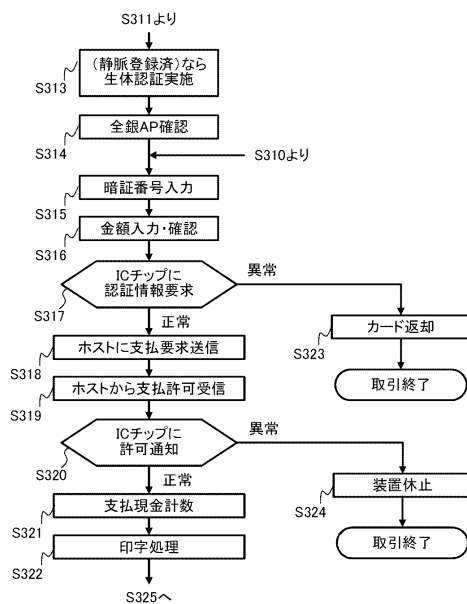
【図 8】

第2の例の処理の流れの一例を示す
フローチャート(その1)



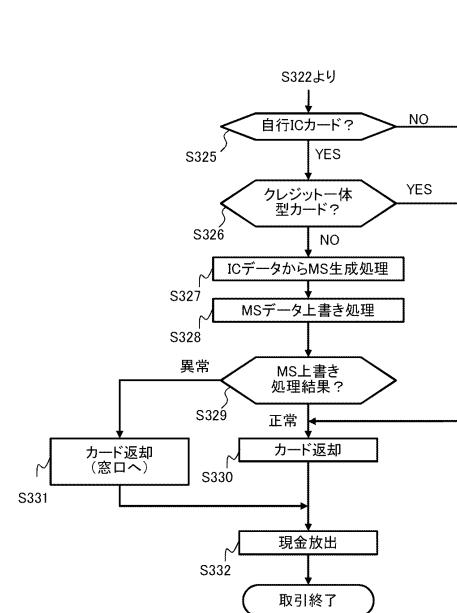
【図 9】

第2の例の処理の流れの一例を示す
フローチャート(その2)



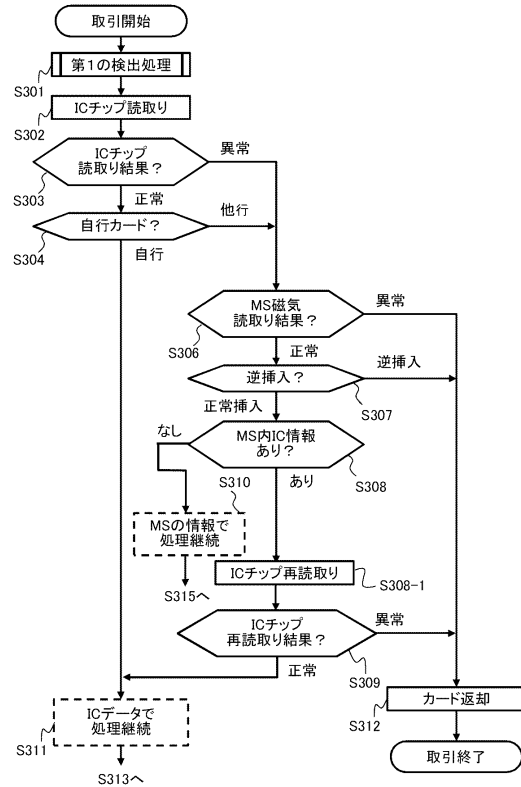
【図 10】

第2の例の処理の流れの一例を示す
フローチャート(その3)



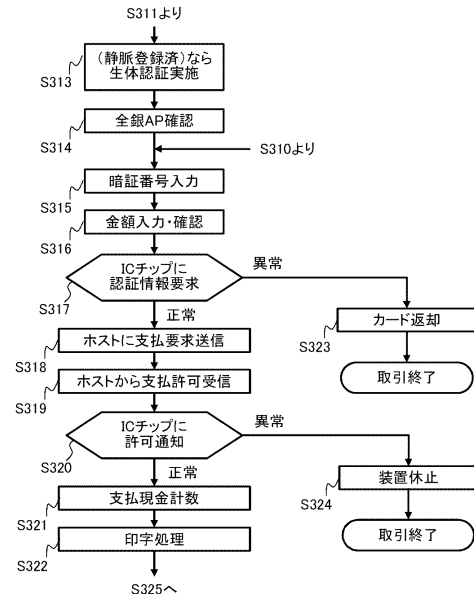
【図 1 1】

第3の例の処理の流れの一例を示す
フローチャート(その1)



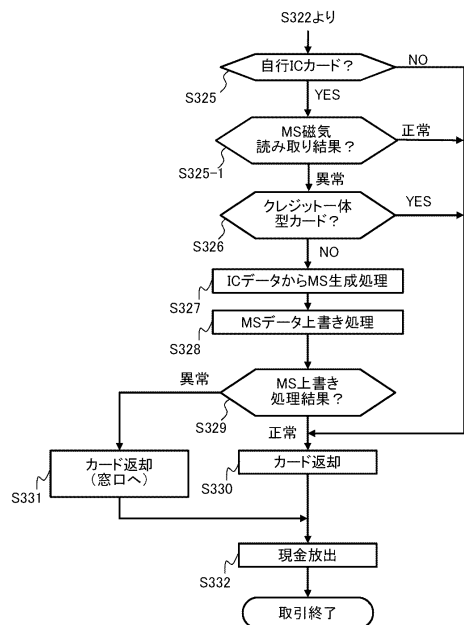
【図 1 2】

第3の例の処理の流れの一例を示す
フローチャート(その2)



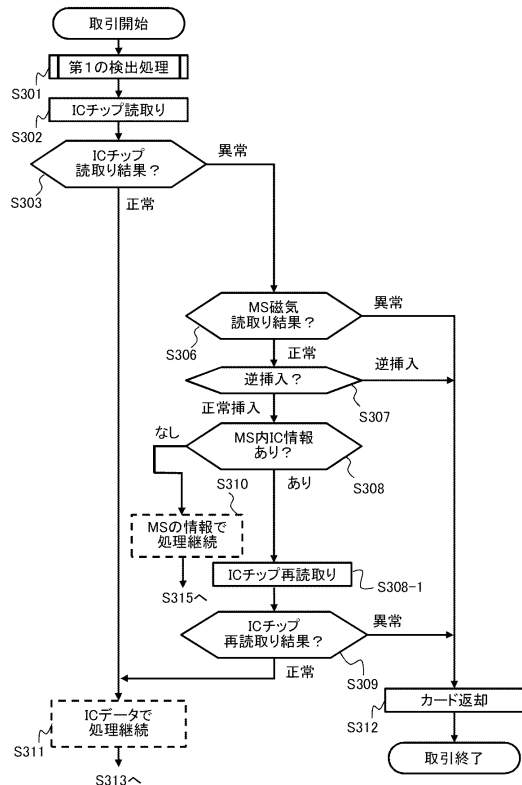
【図 1 3】

第3の例の処理の流れの一例を示す
フローチャート(その3)



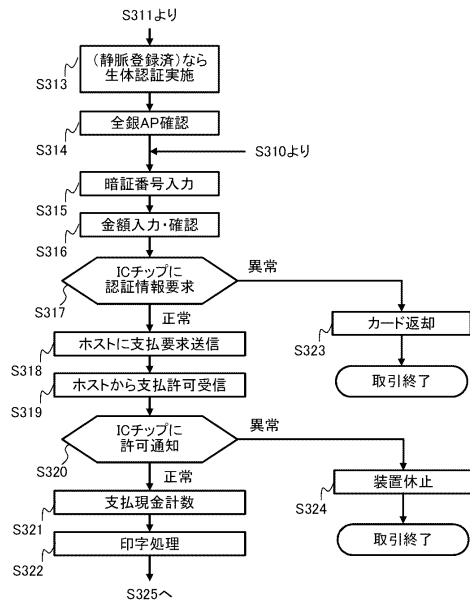
【図 1 4】

第4例の処理の流れの一例を示す
フローチャート(その1)



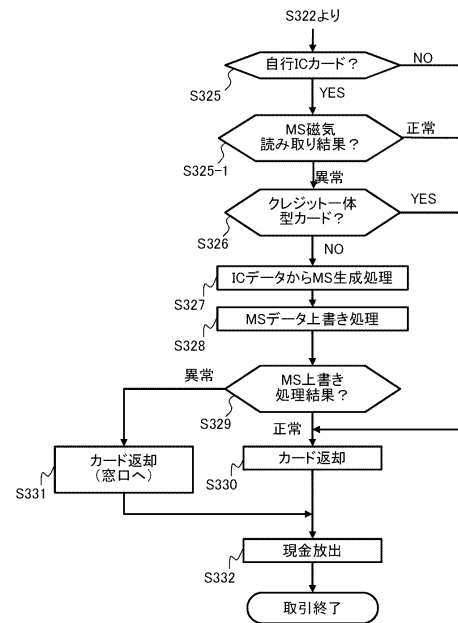
【図 15】

第4の例の処理の流れの一例を示す
フローチャート(その2)



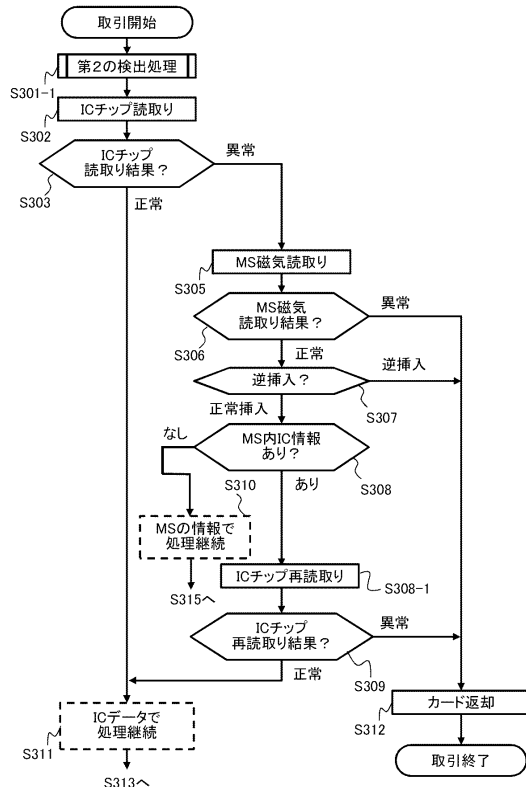
【図 16】

第4の例の処理の流れの一例を示す
フローチャート(その3)



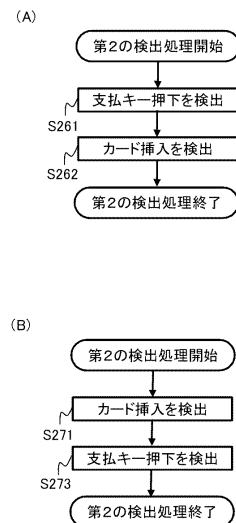
【図 17】

第5の例の処理の流れの一例を示す
フローチャート(その1)



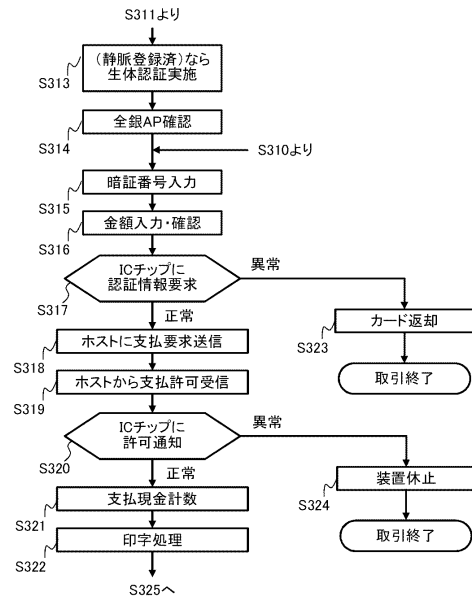
【図 18】

第2の検出処理の流れの
一例を示すフローチャート



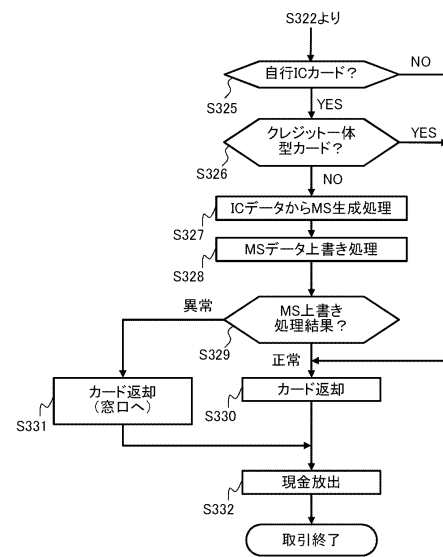
【図 19】

第5の例の処理の流れの一例を示す
フローチャート(その2)



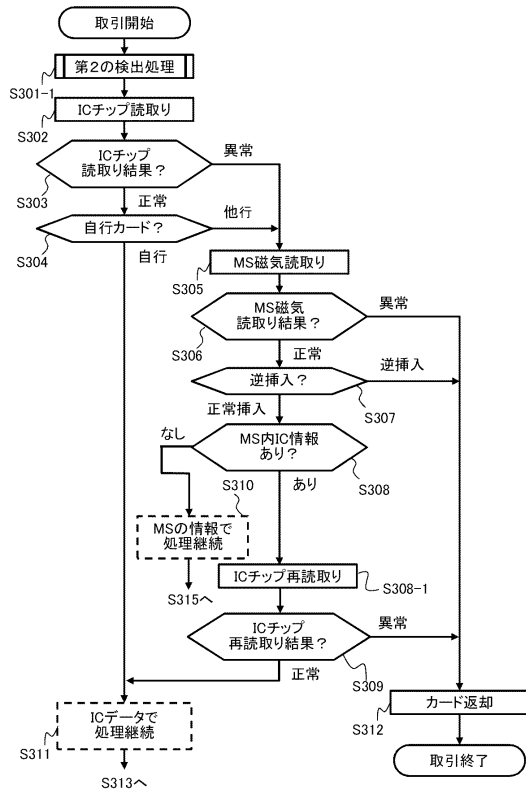
【図 20】

第5の例の処理の流れの一例を示す
フローチャート(その3)



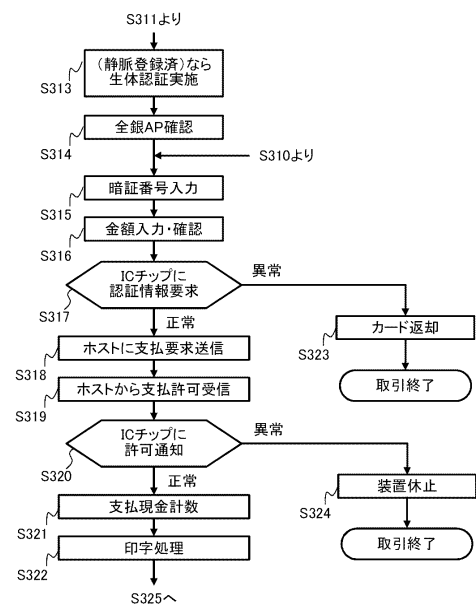
【図 21】

第6の例の処理の流れの一例を示す
フローチャート(その1)



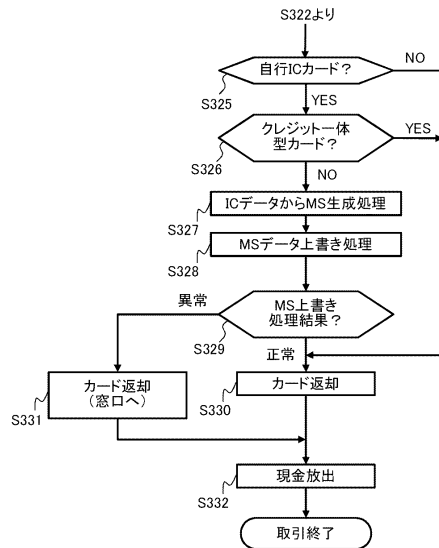
【図 22】

第6の例の処理の流れの一例を示す
フローチャート(その2)



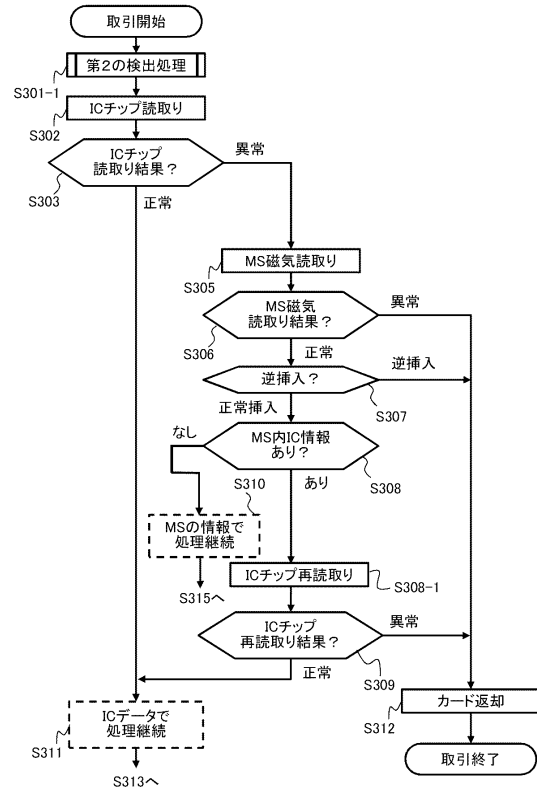
【図 2 3】

第6の例の処理の流れの一例を示す
フローチャート(その3)



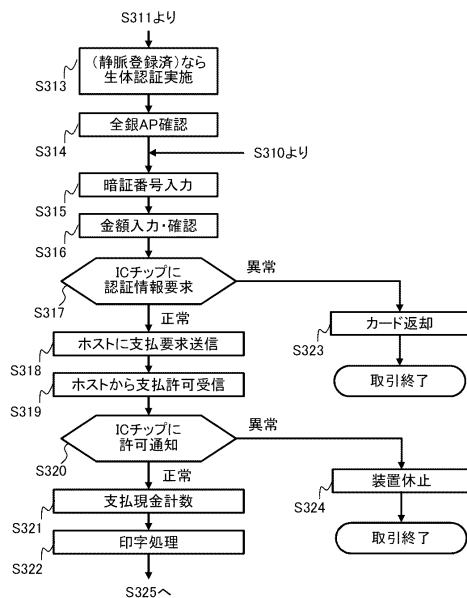
【図 2 4】

第7の例の処理の流れの一例を示す
フローチャート(その1)



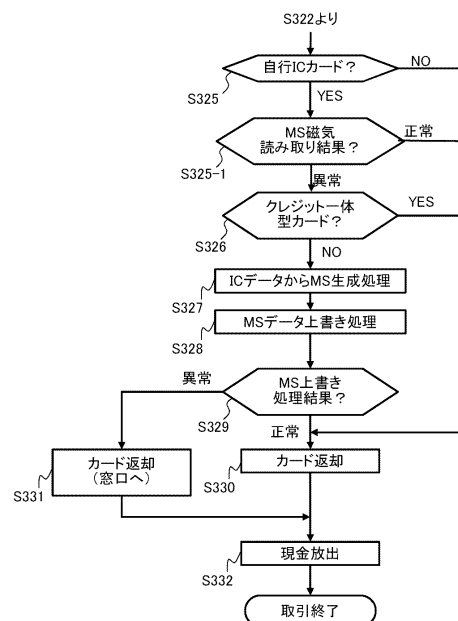
【図 2 5】

第7の例の処理の流れの一例を示す
フローチャート(その2)



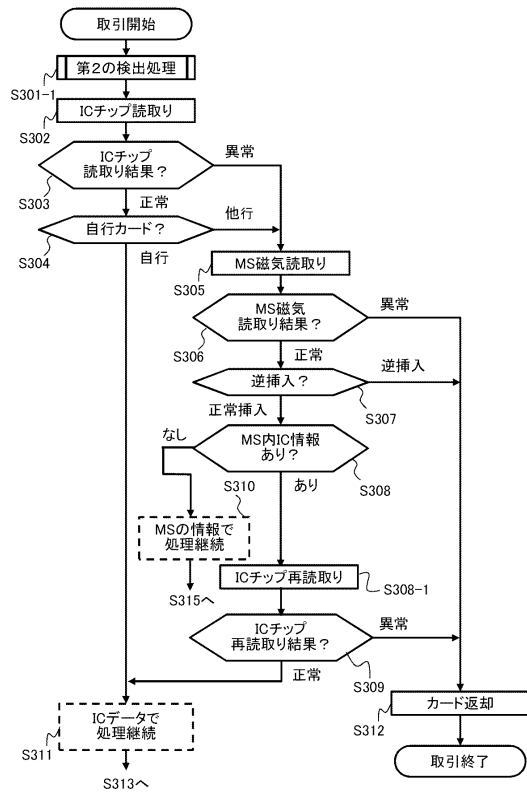
【図 2 6】

第7の例の処理の流れの一例を示す
フローチャート(その3)



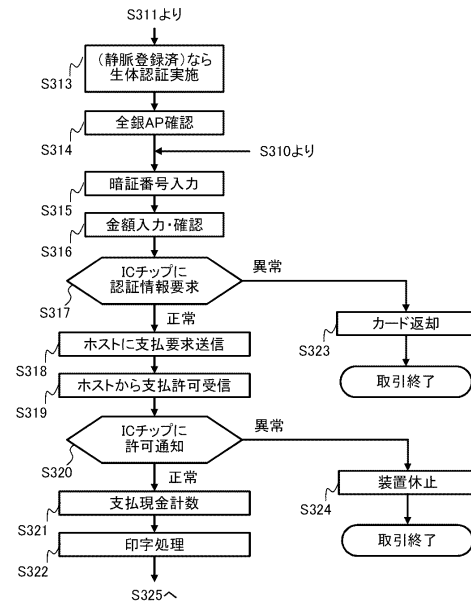
【図 27】

第8の例の処理の流れの一例を示す
フローチャート(その1)



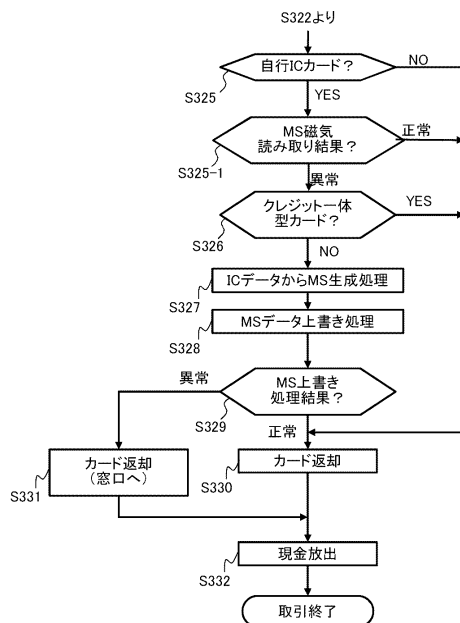
【図 28】

第8の例の処理の流れの一例を示す
フローチャート(その2)



【図 29】

第8の例の処理の流れの一例を示す
フローチャート(その3)



フロントページの続き

審査官 安井 寿儀

(56)参考文献 特開 2 0 1 3 - 2 0 6 3 1 1 (J P , A)
特開 2 0 1 3 - 0 1 6 0 9 2 (J P , A)

(58)調査した分野(Int.Cl. , D B 名)
G 0 7 D 9 / 0 0