(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
2016 年 2 月 25 日(25.02.2016)

WIPO | PCT

(10) 国際公開番号
WO 2016/027441 A1

(51) 国際特許分類:
G06F 21/34 (2013.01) *G06K 19/073* (2006.01)

(21) 国際出願番号: PCT/JP2015/004033

(22) 国際出願日: 2015 年 8 月 12 日(12.08.2015)

(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 2014-169419 2014 年 8 月 22 日(22.08.2014) JP

(71) 出願人: 株式会社 東芝 (KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目１番１号 Tokyo (JP).

(72) 発明者: 谷口 敬太(TANIGUCHI, Keita).

(74) 代理人: 美甘 徹也(MIKAMO, Tetsuya); 〒2100007 神奈川県川崎市川崎区駅前本町１２番１号東芝テクノセンター株式会社内 Kanagawa (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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

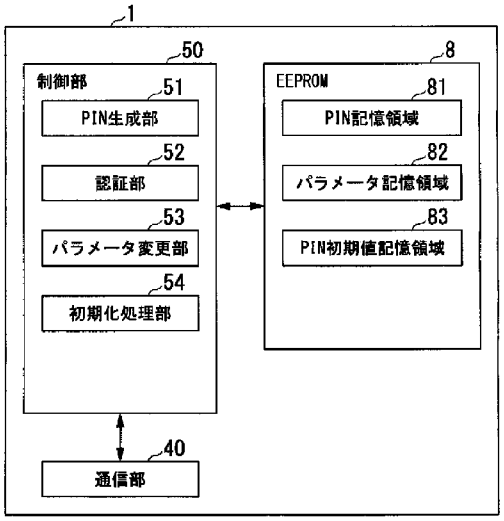
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR),

[続葉有]

(54) **Title**: IC CARD, IC MODULE, AND IC CARD SYSTEM

(54) 発明の名称 : ＩＣカード、ＩＣモジュール、及びＩＣカードシステム

[図2]



40... COMMUNICATION UNIT
50... CONTROL UNIT
51... PIN GENERATION UNIT
52... AUTHENTICATION UNIT
53... PARAMETER CHANGING UNIT
54... INITIALIZATION PROCESSING UNIT
81... PIN STORAGE AREA
82... PARAMETER STORAGE AREA
83... PIN INITIAL VALUE STORAGE AREA

(57) **Abstract**: Provided are an IC card, an IC module, and an IC card system by which it is possible to improve security. An IC card of an embodiment of the present invention has a generation unit and an authentication unit. On the basis of a first password stored in a storage unit in advance, prescribed parameters, and a prescribed algorithm, the generation unit generates a second password which is a password for card-user authentication. The authentication unit compares a third password obtained from an external device with the second password, and determines the validity of the card user on the basis of the comparison results.

(57) 要約: セキュリティを向上させることができるＩＣカード、ＩＣモジュール、及びＩＣカードシステムを提供することである。 実施形態のＩＣカードは、生成部と、認証部とを持つ。生成部は、予め記憶部に記憶されている第１のパスワードと、所定のパラメータと、所定のアルゴリズムとに基づいて、カード利用者の認証用のパスワードである第２のパスワードを生成する。認証部は、外部装置から取得した第３のパスワードと、前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する。

WO 2016/027441 A1

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

— 補正された請求の範囲（条約第 19 条(1)）

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

ＩＣカード、ＩＣモジュール、及びＩＣカードシステム

関連出願の引用

[0001] 本出願は、２０１４年８月２２日に出願した先行する日本国特許出願第２０１４－１６９４１９号による優先権の利益に基礎をおき、かつ、その利益を求めており、その内容全体が引用によりここに包含される。

技術分野

[0002] 本実施形態は、ＩＣカード、ＩＣモジュール及びＩＣカードシステムに関する。

背景技術

[0003] 近年、ＩＣチップを内蔵したＩＣカードが広く使用されている。従来のＩＣカードは、正当なカード所有者であるカードホルダーとの間で共有する秘密のパスワードを受信して、受信したパスワードと、ＩＣカードが記憶しているパスワードとを照合することにより、カードホルダーの正当性を認証する。しかしながら、従来のＩＣカードでは、パスワードとして静的データ（固定値）を使用するため、例えば、パスワードが漏洩すると、第三者がカードホルダーに成りすまして不正にそのＩＣカードが利用される可能性があった。

[0004] 下記文献は、上述した技術に関連しており、ここに内容全体を引用によりここに包含する。

[0005] 特許文献１：特開２００６－２６８７７９号公報

発明の概要

発明が解決しようとする課題

[0006] 本発明が解決しようとする課題は、セキュリティを向上させることができるＩＣカード、ＩＣモジュール及びＩＣカードシステムを提供することである。

課題を解決するための手段

[0007] 実施形態のＩＣカードは、生成部と、認証部とを持つ。生成部は、予め記憶部に記憶されている第１のパスワードと、所定のパラメータと、所定のアルゴリズムとに基づいて、カード利用者の認証用のパスワードである第２のパスワードを生成する。認証部は、外部装置から取得した第３のパスワードと、前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する。

図面の簡単な説明

[0008] [図1]第１の実施形態のＩＣカードのハードウェア構成例を示す図。

[図2]第１の実施形態のＩＣカードの機能構成例を示すブロック図。

[図3]第１の実施形態のＩＣカードシステムの一例を示すブロック図。

[図4]第１の実施形態のカード情報記憶部のデータ例を示す図。

[図5]第１の実施形態のＩＣカードの動作の一例を示すフローチャート。

[図6]第１の実施形態のＩＣカードの認証処理の一例を示す図。

[図7]第１の実施形態のＩＣカードのパラメータ変更処理の一例を示す図。

[図8]第１の実施形態のＩＣカードシステムのセンタ認証処理の一例を示す図。

[図9]第２の実施形態のＩＣカードの機能構成例を示すブロック図。

[図10]第２の実施形態のＩＣカードの動作の一例を示すフローチャート。

[図11]第２の実施形態のＩＣカードの回数情報の出力処理の一例を示す図。

[図12]第３の実施形態のＩＣカードの機能構成例を示すブロック図。

[図13]第３の実施形態のＩＣカードの動作の一例を示すフローチャート。

[図14]第３の実施形態のＩＣカードの認証処理の一例を示す図。

[図15]第４の実施形態のＩＣカードの機能構成例を示すブロック図。

[図16]第４の実施形態のＩＣカードの動作の一例を示すフローチャート。

[図17]第４の実施形態のＩＣカードの認証処理の一例を示す図。

[図18]第５の実施形態のＩＣカードの機能構成例を示すブロック図。

発明を実施するための形態

[0009] 以下、実施形態のＩＣカード、ＩＣモジュール、及びＩＣカードシステムを、図面を参照して説明する。

[0010] （第１の実施形態） 図１は、第１の実施形態のＩＣカード１のハードウェア構成例を示す図である。この図１に示すように、ＩＣカード１は、ＩＣモジュール１００を備えており、ＩＣモジュール１００は、コンタクト部３と、ＩＣチップ１０とを備えている。ＩＣカード１は、例えば、プラスチックのカード基材に、ＩＣモジュール１００を実装して形成されている。また、ＩＣカード１は、コンタクト部３を介して、外部装置２と通信可能である。ＩＣカード１は、例えば、外部装置２が送信したコマンド（処理要求）を、コンタクト部３を介して受信し、受信したコマンドに応じた処理（コマンド処理）を実行する。そして、ＩＣカード１は、コマンド処理の実行結果であるレスポンス（処理応答）を外部装置２にコンタクト部３を介して送信する。

[0011] なお、本実施形態によるＩＣカード１は、例えば、ＩＣカード１の所有者であるカードホルダーを認証するパスワードを、ＩＣカード１とカードホルダーとで共有する所定のアルゴリズムにより動的に変更して、カードホルダーの正当性を判定する。本実施形態では、所定のアルゴリズムの一例として、所定のパラメータとの加算処理を用いる例について説明する。 また、図１に示す例は、ＩＣカード１を外部装置２と接続して、例えば、オフライン処理を行う場合の構成例を示している。

[0012] 外部装置２は、ＩＣカード１と通信する上位装置であり、例えば、リーダ／ライタ装置などを含んだ端末装置などである。また、外部装置２は、ＩＣカード１にコマンドを出力して、コマンド処理を実行させる。例えば、外部装置２は、ＩＣカード１の所有者であるカードホルダー（カード利用者）からパスワード（例えば、ＰＩＮ（Personal Identification Number））を受け付けて、ＩＣカード１に送信して認証処理を実行させる。

[0013] ＩＣモジュール１００は、コンタクト部３と、ＩＣチップ１０とを備え、例えば、テープ上にＩＣモジュール１００が複数配置されたＣＯＴ（Chip On

Tape）などの形態で取引されるモジュールである。　コンタクト部３は、ＩＣカード１が動作するために必要な各種信号の端子を有している。ここで、各種信号の端子は、電源電圧、クロック信号、リセット信号などを外部装置２から供給を受ける端子、及び、外部装置２と通信するためのシリアルデータ入出力端子（ＳＩＯ端子）を有する。

[0014]　ＩＣチップ１０は、例えば、１チップのマイクロプロセッサなどのＬＳＩ（Large Scale Integration）である。ＩＣチップ１０は、通信Ｉ／Ｆ部４と、ＣＰＵ（Central Processing Unit）５と、ＲＯＭ（Read Only Memory）６と、ＲＡＭ（Random Access Memory）７と、ＥＥＰＲＯＭ（Electrically Erasable Programmable ROM）８とを備えている。

[0015]　通信Ｉ／Ｆ（Interface）部４は、ＩＣカード１と外部装置２との間の通信（コマンド／レスポンスの送受信）を行う。　ＣＰＵ５は、ＲＯＭ６又はＥＥＰＲＯＭ８に記憶されているプログラムを実行して、ＩＣカード１の各種処理を行う。ＣＰＵ５は、例えば、コンタクト部３を介して、通信Ｉ／Ｆ（Interface）部４が受信したコマンドに応じたコマンド処理を実行する。

[0016]　ＲＯＭ６は、例えば、マスクＲＯＭなどの不揮発性メモリであり、ＩＣカード１の各種処理を実行するためのプログラム、及びコマンドテーブルなどのデータを記憶する。ＲＡＭ７は、例えば、ＳＲＡＭ（Static RAM）などの揮発性メモリであり、ＩＣカード１の各種処理を行う際に利用されるデータを一時記憶する。

[0017]　ＥＥＰＲＯＭ８（記憶部の一例）は、例えば、電気的に書き換え可能な不揮発性メモリである。ＥＥＰＲＯＭ８は、後述するＰＩＮ情報、認証用のＰＩＮを生成するためのパラメータ、ＰＩＮの初期値などを記憶する。

[0018]　次に、図２を参照して、本実施形態によるＩＣカード１の機能構成例について説明する。図２は、本実施形態のＩＣカード１の機能構成例を示すブロック図である。この図２に示すように、ＩＣカード１は、ＥＥＰＲＯＭ８と、通信部４０と、制御部５０とを備えている。ＥＥＰＲＯＭ８は、ＰＩＮ記憶領域８１と、パラメータ記憶領域８２と、ＰＩＮ初期値記憶領域８３とを

備えている。　ここで、図２に示される各部は、図１に示されるハードウェアを用いて実現される。

[0019]　ＰＩＮ記憶領域８１は、カードホルダーの正当性を認証するＰＩＮを記憶する記憶領域である。ＰＩＮ記憶領域８１が記憶するＰＩＮは、カードホルダー（カード利用者）の認証用のパスワード（以下、単に認証用ＰＩＮと称することがある）を生成するためのＰＩＮ（第１のパスワード）として使用される。なお、本実施形態では、ＰＩＮ記憶領域８１が記憶するＰＩＮ（以下、単に記憶ＰＩＮと称することがある）は、認証用ＰＩＮ（第２のパスワード）としても使用される。

[0020]　パラメータ記憶領域８２は、カードホルダーの認証用ＰＩＮを生成する際に使用するパラメータを記憶する記憶領域である。なお、本実施形態では、認証用ＰＩＮを生成（変更）する所定のアルゴリズムは、加算処理（演算処理の一例）であり、パラメータ記憶領域８２は、例えば、加算処理のためのパラメータである加算値を記憶する。

[0021]　ＰＩＮ初期値記憶領域８３は、ＰＩＮの初期値を記憶する記憶領域である。ここで、ＰＩＮの初期値とは、ＩＣカード１及び後述するＩＣカードシステム２０（図３参照）にカードホルダーを登録する際に、登録されたＰＩＮであり、ＩＣカード１及びＩＣカードシステム２０に最初に記憶されたＰＩＮである。

[0022]　通信部４０は、例えば、通信Ｉ／Ｆ部４、ＣＰＵ５、及びＲＯＭ６に記憶されているプログラムにより実現され、コンタクト部３を介して、外部装置２との間でコマンド及びレスポンスの送受信を行う。

[0023]　制御部５０は、例えば、ＣＰＵ５と、ＲＡＭ７と、ＲＯＭ６又はＥＥＰＲＯＭ８とにより実現され、ＩＣカード１を統括的に制御する。制御部５０は、例えば、外部装置２からＩＣカードに送信された各種コマンドの処理（コマンド処理）を実行する。また、制御部５０は、例えば、ＰＩＮ記憶領域８１が記憶する認証用ＰＩＮによる認証処理を行うとともに、カードホルダーによって認識可能、あるいは記憶可能な所定のアルゴリズムを用いて、認証

用ＰＩＮを変更する。　また、制御部５０は、ＰＩＮ生成部５１と、認証部５２と、パラメータ変更部５３と、初期化処理部５４とを備えている。

[0024] ＰＩＮ生成部５１（生成部の一例）は、予めＥＥＰＲＯＭ８（ＰＩＮ記憶領域８１）に記憶されている記憶ＰＩＮ（第１のパスワード）と、所定のパラメータと、カードホルダーによって認識可能な所定のアルゴリズムとに基づいて、認証用ＰＩＮを生成する。ここで、所定のアルゴリズムとは、例えば、加算処理、減算処理、乗算処理、循環処理などの演算処理であり、上述したように、本実施形態では、一例として、ＥＥＰＲＯＭ８が記憶する記憶ＰＩＮと、所定のパラメータとの加算処理である例について説明する。また、所定のパラメータは、所定のアルゴリズムを用いて認証用ＰＩＮを生成する際に、使用するパラメータを示し、ここでは、一例としてＥＥＰＲＯＭ８（パラメータ記憶領域８２）が記憶する加算値である。

[0025] ＰＩＮ生成部５１は、例えば、ＰＩＮ記憶領域８１が記憶する記憶ＰＩＮと、パラメータ記憶領域８２が記憶する加算値との加算処理に基づいて、新しい認証用ＰＩＮを生成する。すなわち、ＰＩＮ生成部５１は、記憶ＰＩＮの値と、加算値とを加算した値を認証用ＰＩＮとして生成する。また、ＰＩＮ生成部５１は、後述する認証部５２が、カードホルダーが正当であると判定した場合に、認証用ＰＩＮを生成し、認証用ＰＩＮを記憶ＰＩＮとして、ＥＥＰＲＯＭ８のＰＩＮに記憶させる。すなわち、ＰＩＮ生成部５１は、例えば、記憶ＰＩＮによるカードホルダーの認証が成功した場合に、次回の認証用ＰＩＮを生成し、生成した認証用ＰＩＮを記憶ＰＩＮとして、ＰＩＮ記憶領域８１に記憶させる。

[0026] 認証部５２は、外部装置２から取得した取得ＰＩＮ（第３のパスワード）と、認証用ＰＩＮとを照合し、当該照合結果に基づいて、カード利用者の正当性を判定する。すなわち、認証部５２は、例えば、外部装置２を介してカードホルダーから入力された取得ＰＩＮと、ＰＩＮ記憶領域８１が記憶する認証用ＰＩＮとを照合する。認証部５２は、取得ＰＩＮと、認証用ＰＩＮとが一致する場合（照合成功の場合）に、取得ＰＩＮを外部装置２に入力した

カードホルダーが正当である（認証成功）と判定する。また、認証部５２は、取得ＰＩＮと、認証用ＰＩＮとが一致しない場合（照合失敗の場合）に、取得ＰＩＮを外部装置２に入力したカードホルダーが正当なでない（認証失敗）と判定する。

[0027] パラメータ変更部５３（変更部の一例）は、認証部５２によってカードホルダーが正当であると判定された場合（認証成功の状態である場合）に、所定のパラメータ（例えば、加算値）の変更要求に応じて、ＥＥＰＲＯＭ８（パラメータ記憶領域８２）が記憶する所定のパラメータを変更する。すなわち、パラメータ変更部５３は、認証用ＰＩＮによる認証が成功している場合に、所定のパラメータである加算値の変更を要求するコマンドを、外部装置２を介してＩＣカード１が受信した際に、パラメータ記憶領域８２が記憶する加算値を変更する。パラメータ変更部５３は、認証部５２が、認証用ＰＩＮによる認証が成功している場合に、パラメータ記憶領域８２が記憶する加算値を、例えば、外部装置２を介してカードホルダーから入力された新しい加算値に変更する。すなわち、パラメータ変更部５３は、カードホルダーから取得した加算値を、新しい加算値としてパラメータ記憶領域８２に記憶させる。また、パラメータ変更部５３は、認証用ＰＩＮによる認証が成功していない場合には、加算値を変更する処理を実行しない。

[0028] 初期化処理部５４は、認証部５２が、カードホルダーが正当であると判定した場合（認証成功の状態である場合）に、認証用ＰＩＮの初期化要求に応じて、ＥＥＰＲＯＭ８（ＰＩＮ記憶領域８１）が記憶する記憶ＰＩＮを、ＰＩＮ（認証用ＰＩＮ）の初期値に変更する。すなわち、初期化処理部５４は、認証用ＰＩＮによる認証が成功している場合に、認証用ＰＩＮを初期化するコマンドを、外部装置２を介してＩＣカード１が受信した際に、ＰＩＮ記憶領域８１が記憶する記憶ＰＩＮを、ＰＩＮ（認証用ＰＩＮ）の初期値に変更する。初期化処理部５４は、認証用ＰＩＮによる認証が成功している場合に、ＰＩＮ初期値記憶領域８３が記憶するＰＩＮの初期値を、ＰＩＮ記憶領域８１に記憶させる。また、初期化処理部５４は、認証用ＰＩＮによる認証

が成功していない場合には、認証用ＰＩＮを初期化する処理を実行しない。

[0029] 次に、図３を参照して、本実施形態によるＩＣカードシステム２０の構成例について説明する。 図３は、本実施形態のＩＣカードシステム２０の一例を示すブロック図である。 この図に示すように、ＩＣカードシステム２０は、認証センタ装置２００と、外部装置２と、ＩＣカード１とを備えている。

[0030] なお、この図に示す例は、ＩＣカード１を外部装置２と接続し、さらに、ネットワークＮＷを介して、認証センタ装置２００と接続して、例えば、オンライン処理を行う場合の構成例を示している。このようなオンライン処理する場合には、カードホルダーの認証処理を、認証センタ装置２００が行うことがあり、本実施形態によるＩＣカードシステム２０では、認証センタ装置２００がカードホルダーの認証を行うものとする。

[0031] 認証センタ装置２００は、ＩＣカード１に対して、登録されたカードホルダーの認証を、ネットワークＮＷを介してオンラインにより行い、ＩＣカード１を利用した各種処理（例えば、取引処理など）を行うコンピュータ装置である。認証センタ装置２００は、例えば、センタ通信部２１０と、センタ記憶部２２０と、センタ制御部２３０とを備えている。

[0032] センタ通信部２１０は、ネットワークＮＷを介して、外部装置２と通信する。 センタ記憶部２２０は、認証センタ装置２００が行う各種処理に利用する情報を記憶する。センタ記憶部２２０は、例えば、カード情報記憶部２２１を備えている。 カード情報記憶部２２１は、ＩＣカードシステム２０において利用されるＩＣカード１に関する情報を記憶する。カード情報記憶部２２１は、例えば、図４に示すように、少なくとも「カードＩＤ」と、「ＰＩＮ初期値」と、「ＰＩＮ」と、「ＰＡＲ」とを関連付けて記憶する。

[0033] ここで、「カードＩＤ」は、ＩＣカードシステム２０に登録されているＩＣカード１を識別する識別情報であり、「ＰＩＮ初期値」は、ＩＣカード１のカードホルダーが、登録したＰＩＮの初期値を示している。また、「ＰＩＮ」は、後述するＰＩＮ生成部２３１により生成され、変更された認証用Ｐ

ＩＮを示している。すなわち、「ＰＩＮ」は、現在のＰＩＮの値を示している。また、「ＰＡＲ」は、認証用ＰＩＮを生成する際に用いるパラメータ（例えば、加算値）を示している。例えば、図４に示した例では、「カードＩＤ」が“ＸＸＸＸＸ”であるＩＣカード１における「ＰＩＮ初期値」は、“００１５”であり、「ＰＩＮ」が“００２０”であることを示している。また、この場合に、「ＰＡＲ」は、“０００５”であることを示している。

[0034] 図３の説明に戻り、センタ制御部２３０は、例えば、ＣＰＵ（Central Processing Unit）などを含むプロセッサであり、認証センタ装置２００を統括的に制御する。センタ制御部２３０は、例えば、ＩＣカード１がＩＣカードシステム２０によりオンライン処理される場合に、上述したＩＣカード１と同様に、カードホルダーの認証処理、及び、認証用ＰＩＮの生成を行う。また、センタ制御部２３０は、カードホルダーから外部装置２を介して取得したパラメータの変更要求、及びＰＩＮの初期化要求により、上述したカード情報記憶部２２１が記憶する「ＰＡＲ」の変更処理、及び「ＰＩＮ」の初期化処理を行う。また、センタ制御部２３０は、例えば、カード情報記憶部２２１が記憶するＰＩＮに関する情報と、ＩＣカード１が記憶するＰＩＮに関する情報とが一致しない場合に、これらのＰＩＮに関する情報を同期させる処理を行う。センタ制御部２３０は、例えば、ＰＩＮ生成部２３１と、センタ認証部２３２と、パラメータ変更部２３３と、初期化処理部２３４と、同期処理部２３５とを備えている。

[0035] ＰＩＮ生成部２３１（センタ生成部の一例）は、センタ記憶部２２０が記憶する記憶ＰＩＮ（認証用ＰＩＮ）、及び所定のパラメータ（例えば、加算値）と、所定のアルゴリズムとに基づいて、認証用ＰＩＮを生成する。つまり、ＰＩＮ生成部２３１は、ＩＣカード１のオンライン処理において、例えば、上述したＰＩＮ生成部５１と同様の処理を実行する。

[0036] センタ認証部２３２は、外部装置２を介してカード利用者から取得した取得ＰＩＮと、カード情報記憶部２２１が記憶する認証用ＰＩＮとを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。つまり、セ

ンタ認証部２３２は、ＩＣカード１のオンライン処理において、例えば、上述した認証部５２と同様の処理を実行する。

[0037] パラメータ変更部２３３は、センタ認証部２３２によってカードホルダーが正当であると判定された場合（認証成功の状態である場合）に、所定のパラメータ（例えば、加算値）の変更要求に応じて、カード情報記憶部２２１が記憶する所定のパラメータを変更する。すなわち、パラメータ変更部２３３は、ＩＣカード１のオンライン処理において、例えば、上述したパラメータ変更部５３と同様の処理を実行する。なお、パラメータ変更部２３３は、カードホルダーによって外部装置２から要求された所定のパラメータの変更要求を、センタ通信部２１０を介して取得し、取得した変更要求に応じて、カード情報記憶部２２１の上述した「ＰＡＲ」を変更する。

[0038] 初期化処理部２３４は、センタ認証部２３２が、カードホルダーが正当であると判定した場合（認証成功の状態である場合）に、認証用ＰＩＮの初期化要求に応じて、カード情報記憶部２２１が記憶する記憶ＰＩＮを、ＰＩＮ（認証用ＰＩＮ）の初期値に変更する。すなわち、初期化処理部２３４は、ＩＣカード１のオンライン処理において、例えば、上述した初期化処理部５４と同様の処理を実行する。なお、初期化処理部２３４は、カードホルダーによって外部装置２から要求された認証用ＰＩＮの初期化要求を、センタ通信部２１０を介して取得し、取得した初期化要求に応じて、カード情報記憶部２２１の上述した「ＰＩＮ」を、ＰＩＮの初期値である「ＰＩＮ初期値」の値に変更する。

[0039] 同期処理部２３５は、センタ記憶部２２０に記憶されている「ＰＩＮ」及び「ＰＡＲ」をＩＣカード１と同期させる処理を行う。同期処理部２３５は、ＩＣカード１が記憶する記憶ＰＩＮ及び所定のパラメータと、当該ＩＣカード１に対応する「ＰＩＮ」及び「ＰＡＲ」とが一致しない場合に、同期処理を行う。すなわち、同期処理部２３５は、例えば、ＩＣカード１が記憶する記憶ＰＩＮ及び所定のパラメータと、当該ＩＣカード１に対応する「カードＩＤ」と関連付けられてセンタ記憶部２２０に記憶されている「ＰＩＮ」

及び「ＰＡＲ」とが一致しない場合に、同期処理を行う。つまり、同期処理部２３５は、センタ記憶部２２０に記憶されている「ＰＩＮ」及び「ＰＡＲ」を、ＩＣカード１が記憶する記憶ＰＩＮ及び所定のパラメータに変更する。

[0040] 次に、図面を参照して、本実施形態によるＩＣカード１及びＩＣカードシステム２０の動作について説明する。図５は、本実施形態によるＩＣカード１の動作の一例を示すフローチャートである。ここでは、ＩＣカード１が外部装置２に接続され、オフライン処理される場合の一例について説明する。

[0041] この図に示すように、ＩＣカード１は、まず、コマンドを受信したか否かを判定する（ステップＳ１０１）。すなわち、ＩＣカード１の通信部４０が、コンタクト部３及び通信Ｉ／Ｆ部４を介して、外部装置２からコマンドを受信したか否かを判定する。通信部４０は、コマンドを受信した場合（ステップＳ１０１：ＹＥＳ）に、処理をステップＳ１０２に進める。また、通信部４０は、コマンドを受信していない場合（ステップＳ１０１：ＮＯ）に、ステップＳ１０１の処理に戻し、処理を繰り返す。

[0042] ステップＳ１０２において、ＩＣカード１の制御部５０は、受信したコマンドに応じて、処理を分岐させる。この図に示す例では、制御部５０は、受信したコマンドがＰＩＮを照合するコマンドである場合（ＰＩＮ照合）に、処理をステップＳ１０３に進める。また、制御部５０は、受信したコマンドがパラメータの変更要求である場合（ＰＡＲ変更）に、処理をステップＳ１０７に進める。また、制御部５０は、受信したコマンドが認証用ＰＩＮの初期化要求である場合（ＰＩＮ初期化）に、処理をステップＳ１１０に進める。

[0043] ステップＳ１０３において、制御部５０の認証部５２は、ＰＩＮ照合処理を実行する。すなわち、認証部５２は、カードホルダーによって外部装置２に入力された取得ＰＩＮを取得し、当該取得ＰＩＮと、ＰＩＮ記憶領域８１が記憶する記憶ＰＩＮとを照合する。

[0044] 次に、認証部５２は、照合結果が照合成功であるか否かを判定する（ステ

ップＳ１０４）。認証部５２は、例えば、照合結果が取得ＰＩＮと記憶ＰＩＮとが一致している照合成功である場合（ステップＳ１０４：ＹＥＳ）に、例えば、ＲＡＭ７内に、照合成功を示す情報を記憶させて、処理をステップＳ１０５に進める。なお、認証部５２は、照合成功である場合に、カードホルダーが正当であると判定し、ＩＣカード１による各種取引処理が可能になる。また、認証部５２は、例えば、照合結果が取得ＰＩＮと記憶ＰＩＮとが一致していない（不一致である）照合失敗である場合（ステップＳ１０４：ＮＯ）に、処理をステップＳ１０６に進める。なお、認証部５２は、照合失敗である場合に、カードホルダーが正当でないと判定する。認証部５２は、カードホルダーが正当でない場合に、例えば、認証失敗の回数を示すＥＥＰＲＯＭ８のエラーカウンタ情報（不図示）をカウントアップし、さらに、エラーカウンタ情報が所定のカウント値に達した場合に、認証用ＰＩＮによる照合処理の実行を禁止してもよい。

[0045] ステップＳ１０５において、制御部５０のＰＩＮ生成部５１は、加算処理（ＰＩＮ＝ＰＩＮ＋ＰＡＲ）により、次回の照合に使用する認証用ＰＩＮを生成する。すなわち、認証部５２は、ＰＩＮ生成部５１に認証用ＰＩＮを生成させ、ＰＩＮ生成部５１は、例えば、ＰＩＮ記憶領域８１が記憶する記憶ＰＩＮ（ＰＩＮ）に、パラメータ記憶領域８２が記憶する加算値（ＰＡＲ）を加算して認証用ＰＩＮを生成する。ＰＩＮ生成部５１は、生成した認証用ＰＩＮを記憶ＰＩＮとして、ＰＩＮ記憶領域８１に記憶させる。

[0046] また、ステップＳ１０６において、制御部５０は、ＰＩＮ照合結果を送信させる。すなわち、制御部５０は、認証部５２が照合した照合結果（認証結果）を、通信部４０にレスポンスとして外部装置２に向けて送信させる。ステップＳ１０６の処理後に、制御部５０は、処理をステップＳ１０１に戻し、次のコマンド受信を待つ。

[0047] また、ステップＳ１０７において、制御部５０のパラメータ変更部５３は、利用者認証済（カードホルダーの認証済）であるか否かを判定する。パラメータ変更部５３は、例えば、ＲＡＭ７内に、上述した照合成功を示す情報

が記憶されているか否かにより、カードホルダーの認証済であるか否かを判定する。パラメータ変更部５３は、カードホルダーの認証済である場合（ステップＳ１０７：ＹＥＳ）に、処理をステップＳ１０８に進める。また、パラメータ変更部５３は、カードホルダーの認証済でない場合（ステップＳ１０７：ＮＯ）に、処理をステップＳ１０９に進める。

[0048] ステップＳ１０８において、パラメータ変更部５３は、パラメータ記憶領域８２が記憶する加算値（ＰＡＲ）を変更する。すなわち、パラメータ変更部５３は、パラメータ記憶領域８２が記憶する加算値を、例えば、外部装置２を介してカードホルダーから取得した新しい加算値に変更する。

[0049] また、ステップＳ１０９において、制御部５０は、ＰＡＲ変更結果を送信させる。すなわち、制御部５０は、パラメータ変更部５３が、例えば、加算値を変更した結果（ＰＡＲ変更結果）を、通信部４０にレスポンスとして外部装置２に向けて送信させる。ステップＳ１０９の処理後に、制御部５０は、処理をステップＳ１０１に戻し、次のコマンド受信を待つ。

[0050] また、ステップＳ１１０において、制御部５０の初期化処理部５４は、利用者認証済（カードホルダーの認証済）であるか否かを判定する。初期化処理部５４は、例えば、ＲＡＭ７内に、上述した照合成功を示す情報が記憶されているか否かにより、カードホルダーの認証済であるか否かを判定する。初期化処理部５４は、カードホルダーの認証済である場合（ステップＳ１１０：ＹＥＳ）に、処理をステップＳ１１１に進める。また、初期化処理部５４は、カードホルダーの認証済でない場合（ステップＳ１１０：ＮＯ）に、処理をステップＳ１１２に進める。

[0051] ステップＳ１１１において、初期化処理部５４は、ＰＩＮ記憶領域８１が記憶する認証用ＰＩＮ（記憶ＰＩＮ）を初期化する。すなわち、初期化処理部５４は、ＰＩＮ記憶領域８１が記憶する記憶ＰＩＮを、ＰＩＮ初期値記憶領域８３が記憶するＰＩＮの初期値に変更する。

[0052] また、ステップＳ１１２において、制御部５０は、ＰＩＮ初期化結果を送信させる。すなわち、制御部５０は、初期化処理部５４が、例えば、認証用

ＰＩＮ（記憶ＰＩＮ）を初期化した結果（ＰＩＮ初期化結果）を、通信部４０にレスポンスとして外部装置２に向けて送信させる。ステップＳ１１２の処理後に、制御部５０は、処理をステップＳ１０１に戻し、次のコマンド受信を待つ。

[0053] また、図６は、本実施形態によるＩＣカード１の認証処理の一例を示す図である。この図６において、ＩＣカード１は、「ＰＩＮ」（記憶ＰＩＮ）が“００１５”、「ＰＡＲ」（加算値）が“０００５”である状態であり、この図に示す例では、この状態を初期状態として認証処理を行う一例を説明する。なお、ここでの所定のアルゴリズムは、加算処理である。

[0054] 図６において、カードホルダーＵ１が、外部装置２において、ＩＣカード１を利用した取引処理を指定し、ＩＣカード１を外部装置２に接続した場合に、外部装置２は、カードホルダーＵ１に対して、ＰＩＮ入力要求を出力する（ステップＳ２０１）。外部装置２は、例えば、表示部（不図示）のメニュー画面に、カードホルダーＵ１にＰＩＮの入力を促す表示を出力する。

[0055] 次に、カードホルダーＵ１によって、外部装置２にＰＩＮ（例えば、“００１５”）が入力されると（ステップＳ２０２）、外部装置２は、ＩＣカード１に対して、ＰＩＮ照合要求を送信する（ステップＳ２０３）。すなわち、外部装置２は、取得ＰＩＮとして、例えば、“００１５”を含むＰＩＮ照合のコマンドを、ＩＣカード１に対して送信する。

[0056] 次に、ＩＣカード１は、ＰＩＮ照合のコマンドに応じて、ＰＩＮ照合処理（例えば、“００１５”の照合）を実行する（ステップＳ２０４）。ＩＣカード１の認証部５２は、例えば、取得ＰＩＮである“００１５”と、ＰＩＮ記憶領域８１が記憶する“００１５”とを照合する。なお、ここでは、認証部５２は、取得ＰＩＮである“００１５”と、ＰＩＮ記憶領域８１が記憶する“００１５”とが一致するので、照合成功と判定する。

[0057] 次に、ＩＣカード１のＰＩＮ生成部５１が、照合成功である場合に、ＰＩＮを変更し、照合失敗である場合に、ＰＩＮを変更しない（ステップＳ２０５）。なお、この例では、認証部５２が照合成功と判定しているので、ＰＩ

Ｎ生成部５１は、“００１５”に“０００５”を加算処理して、次回に使用する認証用ＰＩＮ“００２０”を生成する。ＰＩＮ生成部５１は、生成した認証用ＰＩＮ“００２０”をＰＩＮ記憶領域８１に記憶させる。

[0058] 次に、ＩＣカード１は、ＰＩＮ照合結果を外部装置２に送信する（ステップＳ２０６）。すなわち、ＩＣカード１の制御部５０は、認証部５２のＰＩＮ照合結果を通信部４０に送信させる。 このように、本実施形態によるＩＣカード１は、ＰＩＮ照合（カードホルダーＵ１の認証）が成功するごとに、認証用ＰＩＮを変更する。

[0059] 次に、図７を参照して、本実施形態によるＩＣカード１のパラメータ変更処理について説明する。図７は、本実施形態のＩＣカード１のパラメータ変更処理の一例を示す図である。この図７において、ＩＣカード１は、「ＰＩＮ」（記憶ＰＩＮ）が“００２０”、「ＰＡＲ」（加算値）が“０００５”である状態であり、図６に示す認証処理を行った後の状態を初期状態としてパラメータ変更処理を行う一例を説明する。すなわち、ＩＣカード１は、カードホルダーＵ１の認証済の状態で、記憶ＰＩＮが“００２０”である状態である。

[0060] 図７において、カードホルダーＵ１が、外部装置２において、パラメータ変更処理を指定した場合に、外部装置２は、カードホルダーＵ１に対して、変更する加算値入力要求を送信する（ステップＳ３０１）。外部装置２は、例えば、表示部（不図示）のメニュー画面に、カードホルダーＵ１に変更する加算値の入力を促す表示を出力する。

[0061] 次に、カードホルダーＵ１によって、外部装置２に加算値（例えば、“０００３”）が入力されると（ステップＳ３０２）、外部装置２は、ＩＣカード１に対して、パラメータ変更要求を送信する（ステップＳ３０３）。すなわち、外部装置２は、取得した加算値（例えば、“０００３”）を含む加算値変更のコマンドを、ＩＣカード１に対して送信する。

[0062] 次に、ＩＣカード１は、パラメータ変更のコマンドに応じて、カードホルダーＵ１の認証済である場合に、加算値を変更し、カードホルダーＵ１の認

証済でない場合に、加算値を変更しない（ステップＳ３０４）。なお、この例では、認証済であるので、パラメータ変更部５３は、加算値“０００５”を“０００３”に変更する。すなわち、パラメータ変更部５３は、パラメータ記憶領域８２が記憶する加算値“０００５”を取得した加算値“０００３”に変更する。

[0063] 次に、ＩＣカード１は、加算値変更結果を外部装置２に送信する（ステップＳ３０５）。すなわち、ＩＣカード１の制御部５０は、パラメータ変更部５３の加算値結果を通信部４０に送信させる。

[0064] なお、次に、ＰＩＮ照合処理が行われる場合には、図６に示すステップＳ２０１からステップＳ２０６の処理と同様のステップＳ３０６からステップＳ３１１の処理が実行される。ただし、ステップＳ３０６からステップＳ３１１の処理では、パラメータ記憶領域８２が記憶する加算値が“０００３”である。そのため、ステップＳ３１０において、ＰＩＮ生成部５１は、“００２０”に“０００３”を加算処理して、次回に使用する認証用ＰＩＮ“００２３”を生成する。

[0065] このように、ＩＣカード１のパラメータ変更部５３は、カードホルダーＵ１が正当であると判定された場合（認証成功の状態である場合）に、加算値変更のコマンドに応じて、パラメータ記憶領域８２が記憶する加算値を変更する。

[0066] 次に、図８を参照して、本実施形態によるＩＣカードシステム２０のオンライン処理によるセンタ認証処理について説明する。図８は、本実施形態のＩＣカードシステム２０のセンタ認証処理の一例を示す図である。この図８において、ＩＣカード１は、「ＰＩＮ」（記憶ＰＩＮ）が“００２０”、「ＰＡＲ」（加算値）が“０００３”である状態であり、認証センタ装置２００は、「ＰＩＮ」（記憶ＰＩＮ）が“００１５”、「ＰＡＲ」（加算値）が“０００５”である状態である場合について説明する。すなわち、ＩＣカード１と認証センタ装置２００との間で、ＰＩＮ情報が一致していない状態である。

[0067] 図８において、外部装置２は、ネットワークＮＷを介して認証センタ装置２００に接続されており、外部装置２は、まず、認証センタ装置２００にＰＩＮ同期要求を送信する（ステップＳ４０１）。次に、認証センタ装置２００は、ＰＩＮ同期要求に応じて、ＰＩＮ情報要求を、外部装置２を介して、ＩＣカード１に送信する（ステップＳ４０２）。すなわち、外部装置２は、認証センタ装置２００からの要求に応じて、ＰＩＮ情報を取得するコマンドをＩＣカード１に対して送信する。

[0068] 次に、ＩＣカード１は、ＰＩＮ情報を、外部装置２を介して、認証センタ装置２００に送信する（ステップＳ４０３）。すなわち、ＩＣカード１の制御部５０は、ＰＩＮ情報を取得するコマンドに応じて、ＰＩＮ記憶領域８１が記憶する記憶ＰＩＮ“００２０”と、パラメータ記憶領域８２が記憶する加算値“０００３”とを外部装置２に通信部４０に送信させ、外部装置２は、このＰＩＮ情報を認証センタ装置２００に送信する。 なお、ＩＣカード１は、例えば、認証センタ装置２００との間で共有するセンタキーによるキー照合（センタ認証）が成功している場合に、ＰＩＮ情報を送信するものとする。図８において図示を省略するが、ここでは、ＰＩＮ情報要求の前に、センタキーによるキー照合（センタ認証）が行われているものとする。

[0069] 次に、認証センタ装置２００は、ＰＩＮ情報の同期処理を実行する（ステップＳ４０４）。この例では、ＩＣカード１が記憶する記憶ＰＩＮ及び所定のパラメータと、当該ＩＣカード１に対応する「ＰＩＮ」及び「ＰＡＲ」とが一致しないので、認証センタ装置２００の同期処理部２３５は、同期処理を行う。すなわち、同期処理部２３５は、カード情報記憶部２２１のＩＣカード１に対応する「ＰＩＮ」を“００１５”から“００２０”に変更し、「ＰＡＲ」を“０００５”から“０００３”に変更する。

[0070] 次に、認証センタ装置２００は、同期結果を外部装置２に送信する（ステップＳ４０５）。 次に、外部装置２は、カードホルダーＵ１に対して、ＰＩＮ入力要求を出力する（ステップＳ４０６）。外部装置２は、例えば、表示部（不図示）のメニュー画面に、カードホルダーＵ１にＰＩＮの入力を促

す表示を出力する。

[0071] 次に、カードホルダーＵ１によって、外部装置２にＰＩＮ（例えば、“００２０”）が入力されると（ステップＳ４０７）、外部装置２は、認証センタ装置２００に対して、ＰＩＮ照合要求を送信する（ステップＳ４０８）。すなわち、外部装置２は、取得ＰＩＮとして、例えば、“００２０”を含むＰＩＮ照合要求を、認証センタ装置２００に対して送信する。

[0072] 次に、認証センタ装置２００は、ＰＩＮ照合要求に応じて、ＰＩＮ照合処理（例えば、“００２０”の照合）を実行する（ステップＳ４０９）。認証センタ装置２００のセンタ認証部２３２は、例えば、取得ＰＩＮである“００２０”と、カード情報記憶部２２１が記憶する“００２０”とを照合する。なお、ここでは、センタ認証部２３２は、取得ＰＩＮである“００２０”と、カード情報記憶部２２１が記憶する“００２０”とが一致するので、照合成功と判定する。

[0073] 次に、認証センタ装置２００のＰＩＮ生成部２３１が、照合成功である場合に、ＰＩＮを変更し、照合失敗である場合に、ＰＩＮを変更しない（ステップＳ４１０）。なお、この例では、センタ認証部２３２が照合成功と判定しているので、ＰＩＮ生成部２３１は、“００２０”に“０００３”を加算処理して、次回に使用する認証用ＰＩＮ“００２３”を生成する。ＰＩＮ生成部２３１は、生成した認証用ＰＩＮ“００２３”をカード情報記憶部２２１に記憶させる。

[0074] 次に、認証センタ装置２００は、ＰＩＮ照合結果を外部装置２に送信する（ステップＳ４１１）。すなわち、認証センタ装置２００のセンタ制御部２３０は、センタ認証部２３２のＰＩＮ照合結果をセンタ通信部２１０に送信させる。 このように、本実施形態による認証センタ装置２００は、オンライン処理において、ＰＩＮ照合（カードホルダーＵ１の認証）が成功するごとに、認証用ＰＩＮを変更する。

[0075] 次に、認証センタ装置２００は、ＩＣカード１に対して、ＰＩＮ変更要求を送信する（ステップＳ４１２）。すなわち、認証センタ装置２００は、Ｉ

ＣカードＩとＰＩＮ情報を同期させるために、外部装置２を介して、変更された認証用ＰＩＮ“００２３”を含むＰＩＮ変更要求のコマンドをＩＣカードＩに送信する。

[0076] ＩＣカードＩの制御部５０は、ＰＩＮ変更要求のコマンドに応じて、ＰＩＮ情報の変更処理を行う（ステップＳ４１３）。すなわち、制御部５０は、ＰＩＮ記憶領域８１が記憶するＰＩＮ“００２０”を“００２３”に変更する。なお、制御部５０は、例えば、センタキーによるキー照合（センタ認証）が成功している場合に、ＰＩＮ情報の変更処理を行う。

[0077] 次に、ＩＣカードＩは、ＰＩＮ変更結果を、外部装置２を介して認証センタ装置２００に送信する（ステップＳ４１４）。すなわち、ＩＣカードＩの制御部５０は、ＰＩＮ変更結果を通信部４０に送信させる。このように、本実施形態によるＩＣカードシステム２０では、オンライン処理時に、認証センタ装置２００がＩＣカードＩと同様の認証処理を行い、さらに、認証センタ装置２００とＩＣカードＩとの間でＰＩＮ情報を同期させる。

[0078] 以上説明したように、本実施形態によるＩＣカードＩは、ＰＩＮ生成部５１と、認証部５２とを備えている。ＰＩＮ生成部５１は、予めＥＥＰＲＯＭ８（記憶部）に記憶されている記憶ＰＩＮ（第１のパスワード）と、所定のパラメータ（例えば、加算値）と、所定のアルゴリズム（例えば、加算処理）とに基づいて、カードホルダーの認証用ＰＩＮ（第２のパスワード）を生成する。認証部５２は、外部装置２から取得した取得ＰＩＮ（第３のパスワード）と、認証用ＰＩＮとを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。 これにより、本実施形態によるＩＣカードＩは、認証用ＰＩＮを動的データとして、認証処理ごとに変更するので、例えば、第三者がカードホルダーに成りすまして不正に利用される可能性を低減することができる。よって、本実施形態によるＩＣカードＩは、セキュリティを向上させることができる。

[0079] また、本実施形態では、ＥＥＰＲＯＭ８は、所定のパラメータ（例えば、加算値）を予め記憶し、所定のアルゴリズムは、記憶ＰＩＮと、所定のパラ

メータ（例えば、加算値）との所定の演算処理（例えば、加算処理）を含む。ＰＩＮ生成部５１は、記憶ＰＩＮと所定のパラメータ（例えば、加算値）との所定の演算処理（例えば、加算処理）に基づいて認証用ＰＩＮを生成する。　これにより、演算処理より認証用ＰＩＮするので、本実施形態によるＩＣカード１は、より簡易な手法により、認証用ＰＩＮを変更することができる。

[0080] また、本実施形態によるＩＣカード１は、パラメータ変更部５３を備えている。パラメータ変更部５３は、認証部５２によってカードホルダーが正当であると判定された場合に、所定のパラメータの変更要求（例えば、変更要求コマンド）に応じて、ＥＥＰＲＯＭ８が記憶する所定のパラメータ（例えば、加算値）を変更する。　これにより、カードホルダーが正当である場合（認証が成功した状態の場合）に、パラメータを変更するので、本実施形態によるＩＣカード１は、セキュリティを確保しつつ、パラメータを変更することができる。そのため、本実施形態によるＩＣカード１は、例えば、定期的に、所定のパラメータを変更することで、認証用ＰＩＮの生成アルゴリズムが第三者に判明する可能性を低減することができる。よって、本実施形態によるＩＣカード１は、よりセキュリティを向上させることができる。

[0081] また、本実施形態では、ＰＩＮ生成部５１は、認証部５２が、カード利用者が正当であると判定した場合に、所定のアルゴリズムに基づいて、次回に照合に使用する認証用ＰＩＮを生成し、認証用ＰＩＮを記憶ＰＩＮとして、ＥＥＰＲＯＭ８に記憶させる。そして、認証部５２は、次回の照合をする際に、取得ＰＩＮと、記憶ＰＩＮとしてＥＥＰＲＯＭ８に記憶されている認証用ＰＩＮとを照合する。これにより、本実施形態によるＩＣカード１は、ＥＥＰＲＯＭ８に記憶されている認証用ＰＩＮを使用して認証処理を行うので、毎回認証用ＰＩＮを生成する場合に比べて、ＣＰＵ５の処理量（演算量）を低減することができる。すなわち、本実施形態によるＩＣカード１は、ＣＰＵ５に負荷を掛けずに、セキュリティを向上させることができる。

[0082] また、本実施形態では、ＥＥＰＲＯＭ８は、認証用ＰＩＮの初期値を記憶

する。ＩＣカード１は、さらに、認証部５２によってカード利用者が正当であると判定された場合に、認証用ＰＩＮの初期化要求（例えば、初期化コマンド）に応じて、ＥＥＰＲＯＭ８が記憶する記憶ＰＩＮを、認証用ＰＩＮの初期値に変更する初期化処理部５４を備える。　これにより、本実施形態によるＩＣカード１では、セキュリティを確保しつつ、カードホルダーが現在の認証用ＰＩＮを初期値に戻すことができる。

[0083] 本実施形態によるＩＣモジュール１００は、ＰＩＮ生成部５１と、認証部５２とを備えている。ＰＩＮ生成部５１は、予めＥＥＰＲＯＭ８（記憶部）に記憶されている記憶ＰＩＮ（第１のパスワード）と、所定のパラメータ（例えば、加算値）と、所定のアルゴリズム（例えば、加算処理）とに基づいて、カードホルダーの認証用ＰＩＮ（第２のパスワード）を生成する。認証部５２は、外部装置２から取得した取得ＰＩＮ（第３のパスワード）と、認証用ＰＩＮとを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。これにより、本実施形態によるモジュール１００は、ＩＣカード１と同様に、セキュリティを向上させることができる。

[0084] また、本実施形態によれば、ＩＣカードシステム２０は、ＩＣカード１と、外部装置２を介してＩＣカード１と接続される認証センタ装置２００とを備えている。認証センタ装置２００は、センタ記憶部２２０と、ＰＩＮ生成部２３１（センタ生成部）と、センタ認証部２３２と、同期処理部２３５とを備えている。センタ記憶部２２０は、ＩＣカード１を識別するカード識別情報（例えば、カードＩＤ）と、記憶ＰＩＮ（次回の認証用ＰＩＮ）と、所定のパラメータとを関連付けて記憶する。ＰＩＮ生成部２３１は、センタ記憶部２２０が記憶する記憶ＰＩＮ及び所定のパラメータ（例えば、加算値）と、所定のアルゴリズム（例えば、加算処理）とに基づいて、認証用ＰＩＮを生成する。センタ認証部２３２は、外部装置２を介してカードホルダーから取得した取得ＰＩＮと、認証用ＰＩＮとを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。同期処理部２３５は、ＩＣカード１が記憶する記憶ＰＩＮ及び所定のパラメータ（例えば、加算値）と、当該

ＩＣカード１に対応するカードＩＤと関連付けられてセンタ記憶部２２０に記憶されている記憶ＰＩＮ及び所定のパラメータ（例えば、加算値）とが一致しない場合に、センタ記憶部２２０に記憶されている記憶ＰＩＮ及び所定のパラメータを、ＩＣカード１が記憶する記憶ＰＩＮ及び所定のパラメータに変更する。

[0085] これにより、本実施形態によるＩＣカードシステム２０は、上述したＩＣカード１と同様に、セキュリティを向上させることができる。また、ＩＣカード１が記憶する認証用ＰＩＮ及びパラメータと、認証センタ装置２００が記憶する認証用ＰＩＮ及びパラメータを、同期させることができるので、本実施形態によるＩＣカードシステム２０は、例えば、オフライン処理とオンライン処理が混在する場合であっても、認証用ＰＩＮ及びパラメータを適切に変更することができる。

[0086] 上述した本実施形態では、ＰＩＮ生成部５１は、認証処理が成功した場合に、次回に照合する認証用ＰＩＮを生成し、ＥＥＰＲＯＭ８に次回に照合する認証用ＰＩＮを記憶ＰＩＮとして、記憶させる例を説明したが、これに限定されるものではない。例えば、ＰＩＮ生成部５１は、認証処理の際に、ＥＥＰＲＯＭ８が記憶する記憶ＰＩＮに基づいて、毎回認証用ＰＩＮを生成し、生成した認証用ＰＩＮによる認証処理が成功した場合に、生成した認証用ＰＩＮを記憶ＰＩＮとして記憶させてもよい。

[0087] （第２の実施形態） 次に、図面を参照して、第２の実施形態によるＩＣカード１ａについて説明する。本実施形態では、例えば、カードホルダーが変更された認証用ＰＩＮを忘れてしまった場合に、ＩＣカード１ａが、現在の認証用ＰＩＮを生成するヒントとなる情報を出力する場合の一例について説明する。なお、本実施形態によるＩＣカード１ａのハードウェア構成は、図１に示す第１の実施形態と同様であるので、ここではその説明を省略する。

[0088] 図９は、本実施形態のＩＣカード１ａの機能構成例を示すブロック図である。この図９に示すように、ＩＣカード１ａは、ＥＥＰＲＯＭ８ａと、通信

部４０と、制御部５０ａとを備えている。ＥＥＰＲＯＭ８ａは、ＰＩＮ記憶領域８１と、パラメータ記憶領域８２と、ＰＩＮ初期値記憶領域８３と、回数情報記憶領域８４とを備えている。また、制御部５０ａは、ＰＩＮ生成部５１ａと、認証部５２ａと、初期化処理部５４ａと、回数情報処理部５５とを備えている。ここで、図９に示される各部は、図１に示されるハードウェアを用いて実現される。なお、この図において、図２に示す機能構成と同一の構成については同一の符号を付し、その説明を省略する。

[0089] 回数情報記憶領域８４は、認証用ＰＩＮを生成した回数を示す回数情報を記憶する。認証部５２ａは、以下の第１の認証処理と、第２の認証処理とを実行する。認証部５２ａは、第１の認証処理において、取得ＰＩＮと、認証用ＰＩＮとを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。また、認証部５２ａは、第２の認証処理において、外部装置２から取得した取得初期ＰＩＮ（第４のパスワード）と、認証用ＰＩＮの初期値とを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。すなわち、認証部５２ａは、第２の認証処理において、ＰＩＮ初期値記憶領域８３が記憶するＰＩＮの初期値による認証処理を実行する。

[0090] ＰＩＮ生成部５１ａは、認証部５２ａが、第１の認証処理によりカードホルダーが正当であると判定した場合に、認証用ＰＩＮを生成するとともに、ＥＥＰＲＯＭ８ａ（回数情報記憶領域８４）が記憶する回数情報を更新する。すなわち、ＰＩＮ生成部５１ａは、回数情報記憶領域８４が記憶する回数情報の値に“１”を加算して、再び回数情報記憶領域８４に記憶させる。なお、ＰＩＮ生成部５１ａのその他の機能は、第１の実施形態のＰＩＮ生成部５１と同様である。

[0091] 回数情報処理部５５は、認証部５２ａが、第２の認証処理によりカードホルダーが正当であると判定した場合に、回数情報記憶領域８４が記憶する回数情報を外部装置２に出力させる。なお、回数情報記憶領域８４が記憶する回数情報が判明すれば、カードホルダーは、ＰＩＮの初期値と、パラメータの値とにより、現在の認証用ＰＩＮを算出することが可能になる。

[0092] 初期化処理部５４ａは、認証部５２ａが、第１の認証処理によりカードホルダーが正当であると判定した場合に、認証用ＰＩＮの初期化要求に応じて、ＥＥＰＲＯＭ８ａが記憶する記憶ＰＩＮを、認証用ＰＩＮの初期値に変更する。そして、初期化処理部５４ａは、この初期化処理の際に、ＥＥＰＲＯＭ８ａの回数情報記憶領域８４が記憶する回数情報を初期化する。すなわち、初期化処理部５４ａは、回数情報記憶領域８４が記憶する回数情報として、例えば、“０”を記憶させる。

[0093] 次に、図１０を参照して、本実施形態によるＩＣカード１ａの動作の一例について説明する。図１０は、本実施形態のＩＣカード１ａの動作の一例を示すフローチャートである。この図１０において、ステップＳ５０１及びステップＳ５０２の処理は、図５に示すステップＳ１０１及びステップＳ１０２の処理と同様であるので、ここではその説明を省略する。

[0094] なお、ステップＳ５０２のコマンド分岐の処理において、制御部５０ａは、受信したコマンドがＰＩＮを照合するコマンドである場合（ＰＩＮ照合）に、処理をステップＳ５０３に進める。また、制御部５０ａは、受信したコマンドが認証用ＰＩＮの初期化要求である場合（ＰＩＮ初期化）に、処理をステップＳ５０８に進める。また、制御部５０ａは、受信したコマンドがＰＩＮの初期値を照合するコマンドである場合（初期ＰＩＮ照合）に、処理をステップＳ５１２に進める。また、制御部５０ａは、受信したコマンドが回数情報の出力を要求するコマンドである場合（回数情報要求）に、処理をステップＳ５１４に進める。

[0095] ステップＳ５０３からステップＳ５０７までのＰＩＮ照合の処理（第１の認証処理）において、ステップＳ５０６の処理が追加されている点を除いて、図５に示すステップＳ１０３からステップＳ１０６までの処理と同様である。ステップＳ５０６において、制御部５０ａのＰＩＮ生成部５１ａは、回数情報記憶領域８４が記憶する回数情報を更新する。すなわち、ＰＩＮ生成部５１ａは、回数情報記憶領域８４が記憶する回数情報の値に“１”を加算して、再び回数情報記憶領域８４に記憶させる。

[0096] また、ステップＳ５０８からステップＳ５１１までのＰＩＮ初期化の処理は、ステップＳ５１０の処理が追加されている点を除いて、図５に示すステップＳ１１０からステップＳ１１２までの処理と同様である。ステップＳ５１０において、制御部５０ａの初期化処理部５４ａは、回数情報を初期化する。すなわち、初期化処理部５４ａは、回数情報記憶領域８４が記憶する回数情報として、例えば、“０”を記憶させる。

[0097] ステップＳ５１２において、制御部５０ａの認証部５２ａは、第２の認証処理として、初期ＰＩＮ照合処理を行う。認証部５２ａは、外部装置２から取得した取得初期ＰＩＮと、認証用ＰＩＮの初期値とを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。すなわち、認証部５２ａは、第２の認証処理において、ＰＩＮ初期値記憶領域８３が記憶するＰＩＮの初期値による認証処理を実行する。なお、認証部５２ａは、ＲＡＭ７内に、照合結果を示す情報を記憶させる。また、認証部５２ａは、照合失敗の場合には、例えば、認証失敗の回数を示すＥＥＰＲＯＭ８ａのエラーカウンタ情報（不図示）をカウントアップし、さらに、エラーカウンタ情報が所定のカウント値に達した場合に、初期ＰＩＮによる照合処理の実行を禁止してもよい。

[0098] ステップＳ５１３において、制御部５０ａは、初期ＰＩＮ照合結果を送信させる。すなわち、制御部５０ａは、認証部５２ａが照合した初期ＰＩＮの照合結果（認証結果）を、通信部４０にレスポンスとして外部装置２に向けて送信させる。ステップＳ５１３の処理後に、制御部５０ａは、処理をステップＳ５０１に戻し、次のコマンド受信を待つ。

[0099] ステップＳ５１４において、制御部５０ａの回数情報処理部５５は、初期ＰＩＮの照合成功であるか否かを判定する。回数情報処理部５５は、例えば、ＲＡＭ７内に、上述した初期ＰＩＮの照合成功を示す情報が記憶されているか否かにより、初期ＰＩＮの照合成功であるか否かを判定する。回数情報処理部５５は、初期ＰＩＮの照合成功である場合（ステップＳ５１４：ＹＥＳ）に、処理をステップＳ５１５に進める。また、回数情報処理部５５は、

初期ＰＩＮの照合成功でない場合（ステップＳ５１４：ＮＯ）に、処理をステップＳ５１６に進める。

[0100] ステップＳ５１５において、回数情報処理部５５は、回数情報を外部装置２に送信する。すなわち、回数情報処理部５５は、回数情報記憶領域８４が記憶する回数情報を、通信部４０を介して外部装置２に出力させる。ステップＳ５１５の処理後に、制御部５０ａは、処理をステップＳ５０１に戻し、次のコマンド受信を待つ。

[0101] ステップＳ５１６において、回数情報処理部５５は、エラー応答を外部装置２に送信する。すなわち、回数情報処理部５５は、初期ＰＩＮによる照合が成功していないことを示すレスポンス（エラー応答）を、通信部４０を介して外部装置２に出力させる。ステップＳ５１６の処理後に、制御部５０ａは、処理をステップＳ５０１に戻し、次のコマンド受信を待つ。

[0102] 次に、図１１を参照して、本実施形態によるＩＣカード１ａの回数情報の出力処理について説明する。図１１は、本実施形態のＩＣカード１ａの回数情報の出力処理の一例を示す図である。この図１１において、ＩＣカード１ａは、「初期ＰＩＮ」（ＰＩＮの初期値）が“００１５”、「ＰＩＮ」（記憶ＰＩＮ）が“００２０”、「ＰＡＲ」（加算値）が“０００５”、「回数」（回数情報）が“０１”である状態であり、この１１図に示す例では、この状態を初期状態として回数情報の出力処理を行う一例を説明する。なお、ここでの所定のアルゴリズムは、加算処理である。

[0103] 図１１において、カードホルダーＵ１が、外部装置２において、ＰＩＮ変更の回数情報を表示させる指定をした場合に、外部装置２は、カードホルダーＵ１に対して、初期ＰＩＮ入力要求を出力する（ステップＳ６０１）。外部装置２は、例えば、表示部（不図示）のメニュー画面に、カードホルダーＵ１に初期ＰＩＮの入力を促す表示を出力する。

[0104] 次に、カードホルダーＵ１によって、外部装置２に初期ＰＩＮ（例えば、“００１５”）が入力されると（ステップＳ６０２）、外部装置２は、ＩＣカード１ａに対して、初期ＰＩＮ照合要求を送信する（ステップＳ６０３）

。すなわち、外部装置２は、取得ＰＩＮとして、例えば、“００１５”を含む初期ＰＩＮ照合のコマンドを、ＩＣカード１ａに対して送信する。

[0105] 次に、ＩＣカード１ａは、初期ＰＩＮ照合のコマンドに応じて、初期ＰＩＮ照合処理（例えば、“００１５”の照合）を実行する（ステップＳ６０４）。ＩＣカード１ａの認証部５２ａは、例えば、取得ＰＩＮである“００１５”と、ＰＩＮ初期値記憶領域８３が記憶する“００１５”とを照合する。なお、ここでは、認証部５２ａは、取得ＰＩＮである“００１５”と、ＰＩＮ初期値記憶領域８３が記憶する“００１５”とが一致するので、照合成功と判定する。

[0106] 次に、ＩＣカード１ａは、初期ＰＩＮ照合結果を外部装置２に送信する（ステップＳ６０５）。すなわち、ＩＣカード１ａの制御部５０ａは、認証部５２ａの初期ＰＩＮ照合結果を通信部４０に送信させる。 次に、外部装置２は、ＩＣカード１ａに対して、回数情報要求を送信する（ステップＳ６０５）。すなわち、外部装置２は、回数情報要求のコマンドを、ＩＣカード１ａに対して送信する。

[0107] 次に、ＩＣカード１ａは、回数情報要求のコマンドに応じて、回数情報を外部装置２に送信する（ステップＳ６０７）。すなわち、ＩＣカード１ａの回数情報処理部５５は、回数情報記憶領域８４が記憶する回数情報“０１”を、通信部４０を介して外部装置２に出力させる。次に、外部装置２は、ＩＣカード１ａが出力した回数情報を、カードホルダーＵ１に提示する（ステップＳ６０８）。すなわち、外部装置２は、ＩＣカード１ａから取得した回数情報“０１”を表示部に表示する。これにより、カードホルダーＵ１は、回数情報を取得し、予め認識しているアルゴリズム（ここでは、加算処理）と、パラメータである加算値と、当該回数情報により、現在の認証ＰＩＮを容易に算出することができる。

[0108] なお、上述した回数情報に関する処理が追加されている点を除いて、本実施形態のＩＣカード１ａの基本的な処理は、第１の実施形態のＩＣカード１と同様であるので、その他の処理についての説明を省略する。また、上述し

た本実施形態では、ＩＣカード１ａは、パラメータ変更部５３を備えない例を説明したが、第１の実施形態と同様に、パラメータ変更部５３を備えてもよい。なお、この場合、パラメータ変更部５３が、所定のパラメータ（例えば、加算値）を変更した際に、初期化処理部５４ａに、初期化処理をさせるようにしてもよい。また、本実施形態のＩＣカード１ａを用いたＩＣカードシステム２０は、回数情報の同期処理が追加になる点を除いて、第１の実施形態と同様であるので、ここではその説明を省略する。

[0109] 以上説明したように、本実施形態によるＩＣカード１ａでは、ＥＥＰＲＯＭ８ａは、認証用ＰＩＮの初期値と、認証用ＰＩＮを生成した回数を示す回数情報とを記憶する。そして、本実施形態の認証部５２ａは、第１の認証処理と、第２の認証処理とを実行する。認証部５２ａは、第１の認証処理において、取得ＰＩＮと、認証用ＰＩＮとを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。また、認証部５２ａは、第２の認証処理において、外部装置２から取得した取得初期ＰＩＮ（第４のパスワード）と、認証用ＰＩＮの初期値とを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。ＰＩＮ生成部５１ａは、認証部５２ａによる第１の認証処理によりカードホルダーが正当であると判定された場合に、第２のパスワードを生成するとともに、ＥＥＰＲＯＭ８ａが記憶する回数情報を更新する。さらに、ＩＣカード１ａは、認証部５２ａによる第２の認証処理によりカードホルダーが正当であると判定された場合に、回数情報を外部装置２に出力させる回数情報処理部５５を備える。

[0110] これにより、本実施形態によるＩＣカード１ａでは、セキュリティを確保しつつ、認証用ＰＩＮを生成した回数を示す回数情報をカードホルダーに知らせることができるので、カードホルダーが現在に認証ＰＩＮを忘れてしまった場合であっても、カードホルダーが独自に認証用ＰＩＮを生成することができる。本実施形態によるＩＣカード１ａは、カードホルダーが現在において認証ＰＩＮを忘れてしまった場合であっても、認証用ＰＩＮによる認証処理を可能にすることができるので、利便性を向上させることができる。

[0111] また、本実施形態では、ＩＣカード１ａは、初期化処理部５４ａを備える。初期化処理部５４ａは、認証部５２ａによる第１の認証処理によりカードホルダーが正当であると判定された場合に、認証用ＰＩＮの初期化要求（例えば、初期化コマンド）に応じて、ＥＥＰＲＯＭ８ａが記憶する記憶ＰＩＮを、認証用ＰＩＮの初期値に変更する。さらに、初期化処理部５４ａは、認証用ＰＩＮの初期化要求に応じて、ＥＥＰＲＯＭ８ａが記憶する回数情報を初期化する。これにより、本実施形態によるＩＣカード１ａでは、セキュリティを確保しつつ、カードホルダーが現在の認証用ＰＩＮ及び回数情報を初期値に戻すことができる。

[0112] （第３の実施形態） 次に、図面を参照して、第３の実施形態によるＩＣカード１ｂについて説明する。本実施形態は、上述した第２の実施形態の変形例を示す実施形態である。第２の実施形態では、認証処理が成功するごとに変更される認証ＰＩＮであって、記憶ＰＩＮとしてＥＥＰＲＯＭ８ａに記憶されている認証ＰＩＮにより認証処理を行う例を説明した。これに対して、本実施形態では、回数情報と、認証ＰＩＮの初期値とに基づいて毎回生成した認証ＰＩＮにより認証処理を行う一例について説明する。なお、本実施形態によるＩＣカード１ｂのハードウェア構成は、図１に示す第１の実施形態と同様であるので、ここではその説明を省略する。

[0113] 図１２は、本実施形態のＩＣカード１ｂの機能構成例を示すブロック図である。この図１２に示すように、ＩＣカード１ｂは、ＥＥＰＲＯＭ８ｂと、通信部４０と、制御部５０ｂとを備えている。ＥＥＰＲＯＭ８ｂは、ＰＩＮ記憶領域８１と、パラメータ記憶領域８２と、回数情報記憶領域８４とを備えている。また、制御部５０ｂは、ＰＩＮ生成部５１ｂと、認証部５２ｂと、初期化処理部５４ｂと、回数情報処理部５５とを備えている。ここで、図１２に示される各部は、図１に示されるハードウェアを用いて実現される。なお、この図において、図２及び図９に示す機能構成と同一の構成については同一の符号を付し、その説明を省略する。

[0114] 本実施形態のＥＥＰＲＯＭ８ｂは、ＰＩＮ初期値記憶領域８３を備えない

代わりに、ＰＩＮ記憶領域８１が、認証用ＰＩＮの初期値を記憶する。認証部５２ｂは、第１の認証処理と、第２の認証処理とを実行する。ＰＩＮ生成部５１ｂは、第１の認証処理において、取得ＰＩＮと、ＰＩＮ生成部５１ｂが毎回生成する認証用ＰＩＮとを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。また、ＰＩＮ生成部５１ｂは、第２の認証処理において、外部装置２から取得した取得初期ＰＩＮ（第４のパスワード）と、ＰＩＮ記憶領域８１が記憶する認証用ＰＩＮの初期値とを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。

[0115] ＰＩＮ生成部５１ｂは、ＰＩＮ記憶領域８１が記憶する認証用ＰＩＮの初期値と、パラメータ記憶領域８２が記憶する所定のパラメータ（例えば、加算値）と、所定の演算処理（例えば、加算処理）と、回数情報記憶領域８４が記憶する回数情報とに基づいて、認証用ＰＩＮを生成する。また、ＰＩＮ生成部５１ｂは、認証部５２ｂが、第１の認証処理によりカードホルダーが正当であると判定した場合に、回数情報記憶領域８４が記憶する回数情報を更新する。なお、ＰＩＮ生成部５１ｂは、認証部５２ｂが第１の認証処理を実行するごとに毎回、認証用ＰＩＮの初期値と、所定のパラメータ（例えば、加算値）と、回数情報とに基づいて認証用ＰＩＮを生成する。

[0116] 初期化処理部５４ｂは、認証部５２ｂが、第１の認証処理によりカードホルダーが正当であると判定した場合に、回数情報の初期化要求（回数情報の初期化コマンド）に応じて、ＥＥＰＲＯＭ８ｂ（回数情報記憶領域８４）が記憶する回数情報を初期化する。すなわち、初期化処理部５４ｂは、回数情報記憶領域８４が記憶する回数情報として、例えば、“０”を記憶させる。

[0117] 次に、図１３を参照して、本実施形態によるＩＣカード１ｂの動作の一例について説明する。図１３は、本実施形態のＩＣカード１ｂの動作の一例を示すフローチャートである。この図１３において、ステップＳ７０１及びステップＳ７０２の処理は、図１０に示すステップＳ５０１及びステップＳ５０２の処理と同様であるので、ここではその説明を省略する。

[0118] なお、ステップＳ７０２のコマンド分岐の処理において、制御部５０ｂは

、受信したコマンドがＰＩＮを照合するコマンドである場合（ＰＩＮ照合）に、処理をステップＳ７０３に進める。また、制御部５０ｂは、受信したコマンドが回数情報の初期化要求である場合（回数情報初期化）に、処理をステップＳ７０８に進める。また、制御部５０ｂは、受信したコマンドがＰＩＮの初期値を照合するコマンドである場合（初期ＰＩＮ照合）に、処理をステップＳ７１１に進める。また、制御部５０ｂは、受信したコマンドが回数情報の出力を要求するコマンドである場合（回数情報要求）に、処理をステップＳ７１３に進める。

[0119] ステップＳ７０３において、制御部５０ｂのＰＩＮ生成部５１ｂは、回数情報に基づいて、認証用ＰＩＮを生成する。例えば、所定のアルゴリズムが加算処理であり、所定のパラメータが加算値である場合には、ＰＩＮ生成部５１ｂは、下記の式（１）により、認証用ＰＩＮを生成する。

[0120] 認証用ＰＩＮ＝認証用ＰＩＮの初期値＋加算値×回数情報の値 ・・・（１）

次に、制御部５０ｂの認証部５２ｂは、第１の認証処理として、取得ＰＩＮと、ＰＩＮ生成部５１ｂが生成した認証用ＰＩＮとを照合する（ステップＳ７０４）。次に、制御部５０ｂの認証部５２ｂは、照合結果が照合成功であるか否かを判定する（ステップＳ７０５）。認証部５２ｂは、照合成功である場合（ステップＳ７０５：ＹＥＳ）に、例えば、ＲＡＭ７内に、照合成功を示す情報を記憶させて、処理をステップＳ７０６に進める。また、認証部５２ｂは、照合失敗である場合（ステップＳ７０５：ＮＯ）に、処理をステップＳ７０７に進める。なお、認証部５２ｂは、照合失敗である場合に、カードホルダーが正当でないと判定する。認証部５２ｂは、カードホルダーが正当でない場合に、例えば、認証失敗の回数を示すＥＥＰＲＯＭ８ｂのエラーカウンタ情報（不図示）をカウントアップし、さらに、エラーカウンタ情報が所定のカウント値に達した場合に、認証用ＰＩＮによる照合処理の実行を禁止してもよい。

[0121] ステップＳ７０６において、ＰＩＮ生成部５１ｂは、回数情報記憶領域８

４が記憶する回数情報を更新する。すなわち、ＰＩＮ生成部５１ｂは、回数情報記憶領域８４が記憶する回数情報の値に“１”を加算して、再び回数情報記憶領域８４に記憶させる。次のステップＳ７０７の処理は、図１０に示すステップＳ５０７の処理と同様であるので、ここではその説明を省略する。

[0122] また、ステップＳ７０８からステップＳ７１０までの処理は、図１０に示すステップＳ５０８からステップＳ５１１までの処理からステップＳ５０９の処理を除いた処理と同様であるので、ここではその説明を省略する。なお、本実施形態の初期化処理部５４ｂは、認証用ＰＩＮの初期化を行う必要がなく、ステップＳ７０９において、回数情報の初期化を行う。また、ステップＳ７１０において、制御部５０ｂは、ＰＩＮ初期化結果の代わりに、回数情報の初期化結果を、通信部４０に送信させる。

[0123] また、ステップＳ７１１からステップＳ７１５までの処理は、図１０に示すステップＳ５１２からステップＳ５１６までの処理と同様であるので、ここではその説明を省略する。

[0124] 次に、図１４を参照して、本実施形態によるＩＣカード１ｂの認証処理について説明する。図１４は、実施形態のＩＣカード１ｂの認証処理の一例を示す図である。この図１４において、ＩＣカード１ｂは、「初期ＰＩＮ」（認証用ＰＩＮの初期値）が“００１５”、「ＰＡＲ」（加算値）が“０００５”、「回数」（回数情報）が“０１”である状態であり、この図１４に示す例では、この状態を初期状態として認証処理を行う一例を説明する。なお、ここでの所定のアルゴリズムは、加算処理である。

[0125] 図１４において、カードホルダーＵ１が、外部装置２において、ＩＣカード１ｂを利用した取引処理を指定し、ＩＣカード１ｂを外部装置２に接続した場合に、外部装置２は、カードホルダーＵ１に対して、ＰＩＮ入力要求を出力する（ステップＳ８０１）。外部装置２は、例えば、表示部（不図示）のメニュー画面に、カードホルダーＵ１にＰＩＮの入力を促す表示を出力する。

[0126] 次に、カードホルダーＵ１によって、外部装置２にＰＩＮ（例えば、“００２０”）が入力されると（ステップＳ８０２）、外部装置２は、ＩＣカード１ｂに対して、ＰＩＮ照合要求を送信する（ステップＳ８０３）。すなわち、外部装置２は、取得ＰＩＮとして、例えば、“００２０”を含むＰＩＮ照合のコマンドを、ＩＣカード１ｂに対して送信する。

[0127] 次に、ＩＣカード１ｂは、ＰＩＮ照合のコマンドに応じて、認証用ＰＩＮを生成する（ステップＳ８０４）。すなわち、ＰＩＮ生成部５１ｂは、認証用ＰＩＮの初期値と、所定のパラメータ（例えば、加算値）と、回数情報とに基づいて認証用ＰＩＮを生成する。ここでは、ＰＩＮ生成部５１ｂは、認証用ＰＩＮとして“００２０”を生成する。

[0128] 次に、ＩＣカード１ｂは、ＰＩＮ照合処理（例えば、“００２０”の照合）を実行する（ステップＳ８０５）。ＩＣカード１ｂの認証部５２ｂは、例えば、取得ＰＩＮである“００２０”と、生成した認証用ＰＩＮ“００２０”とを照合する。なお、ここでは、認証部５２ｂは、取得ＰＩＮである“００２０”と、生成した認証用ＰＩＮ“００２０”とが一致するので、照合成功と判定する。

[0129] 次に、ＩＣカード１ｂのＰＩＮ生成部５１ｂが、照合成功である場合に、回数情報を更新し、照合失敗である場合に、回数情報を更新しない（ステップＳ８０６）。なお、この例では、認証部５２ｂが照合成功と判定しているので、ＰＩＮ生成部５１ｂは、回数情報を“０１”から“０２”に変更して、回数情報記憶領域８４に記憶させる。

[0130] 次に、ＩＣカード１ｂは、ＰＩＮ照合結果を外部装置２に送信する（ステップＳ８０７）。すなわち、ＩＣカード１ｂの制御部５０ｂは、認証部５２ｂのＰＩＮ照合結果を通信部４０に送信させる。

[0131] 以上説明したように、本実施形態によるＩＣカード１ｂでは、ＥＥＰＲＯＭ８ｂは、認証用ＰＩＮの初期値を記憶ＰＩＮとして記憶するとともに、認証用ＰＩＮを生成した回数を示す回数情報を記憶する。認証部５２ｂは、第１の認証処理と、第２の認証処理とを実行する。認証部５２ｂは、第１の認

証処理において、取得ＰＩＮと、認証用ＰＩＮとを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。また、認証部５２ｂは、第２の認証処理において、外部装置２から取得した取得初期ＰＩＮと、認証用ＰＩＮの初期値とを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する。ＰＩＮ生成部５１ｂは、認証用ＰＩＮの初期値と、所定のパラメータ（例えば、加算値）と、所定の演算処理（例えば、加算処理）と、ＥＥＰＲＯＭ８ｂが記憶する回数情報とに基づいて、認証用ＰＩＮを生成する。また、ＰＩＮ生成部５１ｂは、認証部５２ｂが、第１の認証処理によりカードホルダーが正当であると判定した場合に、ＥＥＰＲＯＭ８ｂが記憶する回数情報を更新する。これにより、本実施形態によるＩＣカード１ｂは、認証用ＰＩＮを動的データとして、認証処理ごとに変更するので、第１及び第２の実施形態と同様に、セキュリティを向上させることができる。

[0132] また、本実施形態では、ＩＣカード１ｂは、認証部５２ｂによる第２の認証処理によりカードホルダーが正当であると判定された場合に、回数情報を外部装置２に出力させる回数情報処理部５５を備えている。これにより、本実施形態によるＩＣカード１ｂは、第２の実施形態と同様に、カードホルダーが現在に認証ＰＩＮを忘れてしまった場合であっても、カードホルダーが独自に認証用ＰＩＮを生成することができる。

[0133] また、本実施形態では、ＩＣカード１ｂは、認証部５２ｂによる第１の認証処理によりカード利用者が正当であると判定された場合に、回数情報の初期化要求に応じて、ＥＥＰＲＯＭ８ｂが記憶する回数情報を初期化する初期化処理部５４ｂを備える。これにより、本実施形態によるＩＣカード１ｂでは、セキュリティを確保しつつ、カードホルダーが現在の認証用ＰＩＮを初期値に戻すことができる。

[0134] （第４の実施形態） 次に、図面を参照して、第４の実施形態によるＩＣカード１ｃについて説明する。本実施形態は、認証用ＰＩＮを変更するための所定のパラメータとして、外部装置２から供給される供給情報を用いる場合の一例について説明する。また、本実施形態では、所定のアルゴリズムの

一例として、置換処理を用いる一例を説明する。　なお、本実施形態によるＩＣカード１ｃのハードウェア構成は、図１に示す第１の実施形態と同様であるので、ここではその説明を省略する。

[0135]　図１５は、本実施形態のＩＣカード１ｃの機能構成例を示すブロック図である。この図１５に示すように、ＩＣカード１ｃは、ＥＥＰＲＯＭ８ｃと、通信部４０と、制御部５０ｃとを備えている。ＥＥＰＲＯＭ８ｃは、ＰＩＮ記憶領域８１と、置換情報記憶領域８５とを備えている。また、制御部５０ｃは、ＰＩＮ生成部５１ｃと、認証部５２ｃと、置換情報変更部５６とを備えている。ここで、図１５に示される各部は、図１に示されるハードウェアを用いて実現される。

[0136]　ＰＩＮ記憶領域８１は、上述した第３の実施形態と同様に、認証用ＰＩＮの初期値を記憶する。置換情報記憶領域８５は、置換処理情報を記憶する。ここで、置換処理情報には、認証用ＰＩＮのうちの所定の位置、供給情報の種類、及び供給情報に基づいて生成された所定の置換値の生成方法のうちの少なくとも１つを示す。また、供給情報は、ＩＣカード１ｃの取引を行う際に、外部装置２から供給される情報であり、供給情報の種類には、例えば、取引日付、取引時間帯、取引曜日、及び取引金額などが含まれる。

[0137]　ＰＩＮ生成部５１ｃは、外部装置２から供給された供給情報を所定のパラメータとして、当該供給情報と、所定のアルゴリズム（例えば、置換処理）と、認証用ＰＩＮの初期値とに基づいて、認証用ＰＩＮを生成する。ＰＩＮ生成部５１ｃは、例えば、認証用ＰＩＮの初期値の下位１桁と、供給情報である取引日付の下位１桁とを置換して認証用ＰＩＮを生成する。

[0138]　置換情報変更部５６（変更部の一例）は、認証部５２ｃが、カード利用者が正当であると判定した場合に、置換処理情報の変更要求に応じて、ＥＥＰＲＯＭ８ｃ（置換情報記憶領域８５）が記憶する置換処理情報を変更する。

[0139]　次に、図１６を参照して、本実施形態によるＩＣカード１ｃの動作の一例について説明する。図１６は、本実施形態のＩＣカード１ｃの動作の一例を示すフローチャートである。この図１６において、ステップＳ９０１及びス

テップＳ９０２の処理は、図５に示すステップＳ１０１及びステップＳ１０２の処理と同様であるので、ここではその説明を省略する。

[0140] なお、ステップＳ９０２のコマンド分岐の処理において、制御部５０ｃは、受信したコマンドがＰＩＮを照合するコマンドである場合（ＰＩＮ照合）に、処理をステップＳ９０３に進める。また、制御部５０ｃは、受信したコマンドが置換処理情報の変更要求である場合（置換情報変更）に、処理をステップＳ９０６に進める。

[0141] ステップＳ９０２において、制御部５０ｃのＰＩＮ生成部５１ｃは、置換処理情報に基づいて、認証用ＰＩＮを生成する。ＰＩＮ生成部５１ｃは、例えば、認証用ＰＩＮの初期値の下位１桁と、供給情報である取引日付の下位１桁とを置換して認証用ＰＩＮを生成する。

[0142] 次に、制御部５０ｃの認証部５２ｃは、取得ＰＩＮと、ＰＩＮ生成部５１ｃが生成した認証用ＰＩＮとを照合する（ステップＳ９０４）。次に、制御部５０ｃは、ＰＩＮ照合結果を送信させる（ステップＳ９０５）。すなわち、制御部５０ｃは、認証部５２ｃが照合した照合結果（認証結果）を、通信部４０にレスポンスとして外部装置２に向けて送信させる。ステップＳ９０４の処理後に、制御部５０ｃは、処理をステップＳ９０１に戻し、次のコマンド受信を待つ。

[0143] また、ステップＳ９０６において、制御部５０ｃの置換情報変更部５６は、利用者認証済（カードホルダーの認証済）であるか否かを判定する。置換情報変更部５６は、例えば、ＲＡＭ７内に、照合成功を示す情報が記憶されているか否かにより、カードホルダーの認証済であるか否かを判定する。置換情報変更部５６は、カードホルダーの認証済である場合（ステップＳ９０６：ＹＥＳ）に、処理をステップＳ９０７に進める。また、置換情報変更部５６は、カードホルダーの認証済でない場合（ステップＳ９０６：ＮＯ）に、処理をステップＳ９０８に進める。

[0144] ステップＳ９０７において、置換情報変更部５６は、置換情報記憶領域８５が記憶する置換処理情報を変更する。すなわち、パラメータ変更部５３は

、置換情報記憶領域８５が記憶する置換処理情報を、例えば、外部装置２を介してカードホルダーから取得した新しい置換処理情報に変更する。例えば、置換情報変更部５６は、カードホルダーから供給情報を取引日付から取引金額に変更する要求を取得した場合には、置換情報変更部５６は、認証用ＰＩＮを生成する供給情報を取引日付から取引金額に変更する情報を、置換処理情報として、置換情報記憶領域８５に記憶させる。

[0145] また、ステップＳ９０８において、制御部５０ｃは、置換情報変更結果を送信させる。すなわち、制御部５０ｃは、置換情報変更部５６が、置換処理情報を変更した結果（置換情報変更結果）を、通信部４０にレスポンスとして外部装置２に向けて送信させる。ステップＳ９０８の処理後に、制御部５０ｃは、処理をステップＳ９０１に戻し、次のコマンド受信を待つ。

[0146] 次に、図１７を参照して、本実施形態によるＩＣカード１ｃの認証処理について説明する。図１７は、実施形態のＩＣカード１ｃの認証処理の一例を示す図である。この図１７において、ＩＣカード１ｃは、「ＰＩＮ」（認証用ＰＩＮの初期値）が“００１５”であり、「取引日付」が“$Y_1Y_2Y_3Y_4M_1M_2D_1D_2$”である供給情報が既に供給されている状態である。この図１７に示す例では、この状態を初期状態として認証処理を行う一例を説明する。なお、ここでの所定のアルゴリズムは、置換処理である。

[0147] 図１７において、カードホルダーＵ１が、外部装置２において、ＩＣカード１ｃを利用した取引処理を指定し、ＩＣカード１ｃを外部装置２に接続した場合に、外部装置２は、カードホルダーＵ１に対して、ＰＩＮ入力要求を出力する（ステップＳ１００１）。外部装置２は、例えば、表示部（不図示）のメニュー画面に、カードホルダーＵ１にＰＩＮの入力を促す表示を出力する。

[0148] カードホルダーＵ１は、「取引日付」が“$Y_1Y_2Y_3Y_4M_1M_2D_1D_2$”であるので、例えば、この「取引日付」の最下位１桁の“D_2”をＰＩＮの初期値の最下位１桁と置換して認証用ＰＩＮを生成する。すなわち、カードホルダーＵ１によって、外部装置２にＰＩＮ（例えば、“００１D_2”）が入力さ

れると（ステップＳ１００２）、外部装置２は、ＩＣカード１ｃに対して、ＰＩＮ照合要求を送信する（ステップＳ１００３）。すなわち、外部装置２は、取得ＰＩＮとして、例えば、“００２１D_2”を含むＰＩＮ照合のコマンドを、ＩＣカード１ｃに対して送信する。

[0149] 次に、ＩＣカード１ｃは、ＰＩＮ照合のコマンドに応じて、認証用ＰＩＮを生成する（ステップＳ１００４）。すなわち、ＰＩＮ生成部５１ｃは、認証用ＰＩＮの初期値と、すでに供給されている「取引日付」の最下位１桁の“D_2”とに基づいて認証用ＰＩＮを生成する。ここでは、ＰＩＮ生成部５１ｃは、認証用ＰＩＮの初期値の最下位１桁と、「取引日付」の最下位１桁の“D_2”とを置換処理して、認証用ＰＩＮとして“００１D_2”を生成する。

[0150] 次に、ＩＣカード１ｃは、ＰＩＮ照合処理（例えば、“００１D_2”の照合）を実行する（ステップＳ１００５）。ＩＣカード１ｃの認証部５２ｃは、例えば、取得ＰＩＮである“００１D_2”と、生成した認証用ＰＩＮ“００１D_2”とを照合する。なお、ここでは、認証部５２ｃは、取得ＰＩＮである“００１D_2”と、生成した認証用ＰＩＮ“００１D_2”とが一致するので、照合成功と判定する。

[0151] 次に、ＩＣカード１ｃは、ＰＩＮ照合結果を外部装置２に送信する（ステップＳ１００６）。すなわち、ＩＣカード１ｃの制御部５０ｃは、認証部５２ｃのＰＩＮ照合結果を通信部４０に送信させる。このように、本実施形態によるＩＣカード１ｃは、供給情報が変化に応じて、認証用ＰＩＮを変更することができる。

[0152] なお、上述した本実施形態では、所定のパラメータとして、取引日付を用いる例を説明したが、取引日付の代わりに、例えば、取引金額、曜日、時刻（時間帯）などを用いてもよい。また、所定のパラメータには、置換位置を示す情報や置換値の生成方法、供給情報の種類などを含めてもよい。また、所定のパラメータに、曜日や時刻（時間帯）を使用する場合には、ＰＩＮ生成部５１ｃは、曜日や時間帯と置換値とを対応付けた対応テーブルに基づいて、置換値を決定してもよい。また、ＰＩＮ生成部５１ｃは、取引金額の範

囲に応じて、置換値を決定してもよい。

[0153] 以上説明したように、本実施形態によるＩＣカード１ｃでは、所定のパラメータは、外部装置２から供給される供給情報を含み、所定のアルゴリズムは、第１のパスワードのうちの所定の位置の値と、供給情報に基づいて生成された所定の置換値とを置換する置換処理を含む。ＰＩＮ生成部５１ｃは、この置換処理に基づいて認証用ＰＩＮを生成する。これにより、本実施形態によるＩＣカード１ｃは、認証用ＰＩＮを動的データとして、認証処理を行うので、第１の実施形態と同様に、セキュリティを向上させることができる。

[0154] また、本実施形態では、ＥＥＰＲＯＭ８ｃは、所定の位置、供給情報の種類、及び所定の置換値の生成方法のうちの少なくとも１つを示す置換処理情報を記憶する。ＩＣカード１ｃは、さらに、認証部５２ｃによってカード利用者が正当であると判定された場合に、置換処理情報の変更要求に応じて、ＥＥＰＲＯＭ８ｃが記憶する置換処理情報を変更する置換情報変更部５６を備える。これにより、本実施形態によるＩＣカード１ｃは、例えば、定期的に、置換処理情報を変更することで、認証用ＰＩＮの生成アルゴリズムが第三者に判明する可能性を低減することができる。よって、本実施形態によるＩＣカード１ｃは、よりセキュリティを向上させることができる。

[0155] （第５の実施形態） 次に、図１８を参照して、第５の実施形態によるＩＣカード１ｄについて説明する。本実施形態は、ＩＣカード１ｄが、認証用ＰＩＮを生成（変更）するための所定のアルゴリズムを複数有しており、複数の所定のアルゴリズムのうちの１つを選択して、認証用ＰＩＮとして用いる場合の一例について説明する。なお、本実施形態によるＩＣカード１ｄのハードウェア構成は、図１に示す第１の実施形態と同様であるので、ここではその説明を省略する。

[0156] 図１８は、本実施形態のＩＣカード１ｄの機能構成例を示すブロック図である。この１８図に示すように、ＩＣカード１ｄは、ＥＥＰＲＯＭ８ｄと、通信部４０と、制御部５０ｄとを備えている。ＥＥＰＲＯＭ８ｄは、ＰＩＮ

記憶領域８１と、パラメータ記憶領域８２と、ＰＩＮ初期値記憶領域８３と、選択情報記憶領域８６とを備えている。また、制御部５０ｄは、ＰＩＮ生成部５１ｄと、認証部５２と、パラメータ変更部５３、初期化処理部５４とを備えている。ここで、図１８に示される各部は、図１に示されるハードウェアを用いて実現される。また、この図において、図２に示す機能構成と同一の構成については同一の符号を付し、その説明を省略する。

[0157] 選択情報記憶領域８６は、種類の異なる複数の所定のアルゴリズムのうちの１つを選択する選択情報を記憶する。選択情報記憶領域８６は、例えば、所定のアルゴリズムが加算処理である場合に“０１”を記憶し、所定のアルゴリズムが減算処理である場合に“０２”を記憶し、所定のアルゴリズムが置換処理である場合に“０３”を記憶する。なお、本実施形態のパラメータ記憶領域８２は、複数の所定のアルゴリズムのそれぞれに対応するパラメータを記憶する。

[0158] ＰＩＮ生成部５１ｄは、ＥＥＰＲＯＭ８ｄ（選択情報記憶領域８６）が記憶する選択情報に基づいて選択し、選択された当該所定のアルゴリズムに基づいて、認証用ＰＩＮを生成する。例えば、選択情報記憶領域８６が記憶する選択情報が“０１”である場合に、所定のアルゴリズムとして加算処理を選択し、加算処理により、認証用ＰＩＮを生成する。

[0159] 以上説明したように、本実施形態によるＩＣカード１ｄでは、ＥＥＰＲＯＭ８ｄは、種類の異なる複数の所定のアルゴリズムのうちの１つを選択する選択情報を記憶する。そして、ＰＩＮ生成部５１ｄは、ＥＥＰＲＯＭ８ｄが記憶する選択情報に基づいて複数の所定のアルゴリズムのうちの１つを選択し、選択した当該所定のアルゴリズムに基づいて、認証用ＰＩＮを生成する。これにより、複数の所定のアルゴリズムのうちから、認証用ＰＩＮを生成するアルゴリズムを選択できるので、本実施形態によるＩＣカード１ｄは、認証用ＰＩＮの生成アルゴリズムが第三者に判明する可能性を低減することができる。よって、本実施形態によるＩＣカード１ｄは、よりセキュリティを向上させることができる。

[0160] なお、本実施形態では、ＩＣカード１ｄは、認証部５２によってカードホルダーが正当であると判定された場合に、アルゴリズムの変更要求（例えば、アルゴリズム変更コマンド）に応じて、ＥＥＰＲＯＭ８ｄが記憶する選択情報を変更する変更部を備えるようにしてもよい。これにより、定期的に、所定のアルゴリズムを変更するこができるので、本実施形態によるＩＣカード１ｄは、さらにセキュリティを向上させることができる。

[0161] 上記の各実施形態において、各実施形態を単独で実施する場合の例を説明したが、各実施形態を組み合わせて実施してもよい。また、上記の各実施形態において、ＩＣカード１（１ａ～１ｄ）は、書き換え可能な不揮発性メモリとして、ＥＥＰＲＯＭ８（８ａ～８ｄ）を備える構成としたが、これに限定されるものではない。例えば、ＩＣカード１（１ａ）は、ＥＥＰＲＯＭ８（８ａ～８ｄ）の代わりに、フラッシュＥＥＰＲＯＭ、ＦｅＲＡＭ（Ferroelectric Random Access Memory：強誘電体メモリ）などを備えてもよい。また、上記の各実施形態において、ＩＣカード１（１ａ～１ｄ）は、コンタクト部３を介して外部装置２と通信する例を説明したが、コイルなどを用いたコンタクトレスインターフェースを介して外部装置２と通信するように構成してもよい。

[0162] 以上説明した少なくともひとつの実施形態によれば、は、予めＥＥＰＲＯＭ８（８ａ～８ｄ）に記憶されている記憶ＰＩＮと、所定のパラメータと、所定のアルゴリズムとに基づいて、カードホルダーの認証用ＰＩＮを生成するＰＩＮ生成部５１（５１ａ～５１ｄ）と、外部装置２から取得した取得ＰＩＮと、認証用ＰＩＮとを照合し、当該照合結果に基づいて、カードホルダーの正当性を判定する認証部５２（５２ａ～５２c）とを持つことにより、セキュリティを向上させることができる。

[0163] なお、実施形態におけるＩＣカード１（１ａ～１ｄ）及び認証センタ装置２００が備える各構成の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより上述したＩＣカー

ド１（１ａ～１ｄ）及び認証センタ装置２００が備える各構成における処理を行ってもよい。ここで、「記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行する」とは、コンピュータシステムにプログラムをインストールすることを含む。ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものとする。　また、「コンピュータシステム」は、インターネットやＷＡＮ、ＬＡＮ、専用回線等の通信回線を含むネットワークを介して接続された複数のコンピュータ装置を含んでもよい。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。このように、プログラムを記憶した記録媒体は、ＣＤ－ＲＯＭ等の非一過性の記録媒体であってもよい。

[0164]　また、記録媒体には、当該プログラムを配信するために配信サーバからアクセス可能な内部又は外部に設けられた記録媒体も含まれる。なお、プログラムを複数に分割し、それぞれ異なるタイミングでダウンロードした後にＩＣカード１（１ａ～１ｄ）及び認証センタ装置２００が備える各構成で合体される構成や、分割されたプログラムのそれぞれを配信する配信サーバが異なっていてもよい。さらに「コンピュータ読み取り可能な記録媒体」とは、ネットワークを介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。また、上記プログラムは、上述した機能の一部を実現するためのものであってもよい。さらに、上述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

[0165]　本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら実施形態は、その他の様々な形態で実施されることが可能であり、発明の

要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれると同様に、特許請求の範囲に記載された発明とその均等の範囲に含まれるものである。

符号の説明

[0166] １，１ａ，１ｂ，１ｃ，１ｄ…ＩＣカード、２…外部装置、３…コンタクト部、４…通信Ｉ／Ｆ部、５…ＣＰＵ、６…ＲＯＭ、７…ＲＡＭ、８，８ａ，８ｂ，８ｃ，８ｄ…ＥＥＰＲＯＭ、１０…ＩＣチップ、２０…ＩＣカードシステム、４０…通信部、５０，５０ａ，５０ｂ，５０ｃ，５０ｄ…制御部、５１，５１ａ，５０ｂ，５１ｃ，５１ｄ，２３１…ＰＩＮ生成部、５２，５２ａ，５２ｂ，５２ｃ…認証部、５３，２３３…パラメータ変更部、５４，５４ａ，５４ｂ，２３４…初期化処理部、５５…回数情報処理部、５６…置換情報変更部、８１…ＰＩＮ記憶領域、８２…パラメータ記憶領域、８３…ＰＩＮ初期値記憶領域、８４…回数情報記憶領域、８５…置換情報記憶領域、８６…選択情報記憶領域、１００…ＩＣモジュール、２００…認証センタ装置、２１０…センタ通信部、２２０…センタ記憶部、２２１…カード情報記憶部、２３０…センタ制御部、２３２…センタ認証部、２３５…同期処理部、ＮＷ…ネットワーク、Ｕ１…カードホルダー

請求の範囲

[請求項1] 予め記憶部に記憶されている第１のパスワードと、所定のパラメータと、所定のアルゴリズムとに基づいて、カード利用者の認証用のパスワードである第２のパスワードを生成する生成部と、

外部装置から取得した第３のパスワードと前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する認証部と

を備えるＩＣカード。

[請求項2] 前記所定のアルゴリズムは、前記第１のパスワードと前記所定のパラメータとの演算処理を含み、

前記生成部は、前記第１のパスワードと前記所定のパラメータとの前記演算処理によって前記第２のパスワードを生成する

請求項１に記載のＩＣカード。

[請求項3] 前記記憶部は、前記所定のパラメータを予め記憶し、

前記認証部によって前記カード利用者が正当であると判定された場合に、前記所定のパラメータの変更要求に応じて、前記記憶部が記憶する前記所定のパラメータを変更する変更部を備える

請求項２に記載のＩＣカード。

[請求項4] 前記生成部は、前記認証部によって前記カード利用者が正当であると判定された場合に、前記所定のアルゴリズムに基づいて、次回に照合に使用される前記第２のパスワードを生成し、生成した当該第２のパスワードを前記第１のパスワードとして、前記記憶部に記憶させる

請求項２又は請求項３に記載のＩＣカード。

[請求項5] 前記記憶部は、前記第２のパスワードの初期値を記憶し、さらに、前記認証部によって前記カード利用者が正当であると判定された場合に、前記第２のパスワードの初期化要求に応じて、前記記憶部が記憶する前記第１のパスワードを、前記第２のパスワードの初期値に変更する初期化処理部を備える

請求項４に記載のＩＣカード。

[請求項6] 前記記憶部は、前記第２のパスワードの初期値と、前記第２のパスワードを生成した回数を示す回数情報とを記憶し、

前記認証部は、

前記第３のパスワードと、前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する第１の認証処理と、

前記外部装置から取得した第４のパスワードと、前記第２のパスワードの初期値とを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する第２の認証処理と

を実行し、

前記生成部は、前記認証部によって前記第１の認証処理により前記カード利用者が正当であると判定された場合に、前記第２のパスワードを生成するとともに、前記記憶部が記憶する前記回数情報を更新し、

さらに、前記認証部によって前記第２の認証処理により前記カード利用者が正当であると判定された場合に、前記回数情報を前記外部装置に出力させる回数情報処理部を備える

請求項１から請求項４のいずれか一項に記載のＩＣカード。

[請求項7] 前記認証部によって前記第１の認証処理により前記カード利用者が正当であると判定された場合に、前記第２のパスワードの初期化要求に応じて、前記記憶部が記憶する前記第１のパスワードを、前記第２のパスワードの初期値に変更するとともに、前記記憶部が記憶する前記回数情報を初期化する初期化処理部を備える

請求項６に記載のＩＣカード。

[請求項8] 前記記憶部は、前記第２のパスワードの初期値を前記第１のパスワードとして記憶するとともに、前記第２のパスワードを生成した回数を示す回数情報を記憶し、

前記認証部は、

前記第３のパスワードと、前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する第１の認証処理と、

前記外部装置から取得した第４のパスワードと、前記第２のパスワードの初期値とを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する第２の認証処理と、

を実行し、

前記生成部は、

前記第２のパスワードの初期値と、前記所定のパラメータと、前記演算処理と、前記記憶部が記憶する前記回数情報とに基づいて、前記第２のパスワードを生成するとともに、前記認証部による前記第１の認証処理により前記カード利用者が正当であると判定された場合に、前記記憶部が記憶する前記回数情報を更新する

請求項２又は請求項３に記載のＩＣカード。

[請求項9] 前記認証部による前記第２の認証処理により前記カード利用者が正当であると判定された場合に、前記回数情報を前記外部装置に出力させる回数情報処理部と、

前記認証部による前記第１の認証処理により前記カード利用者が正当であると判定された場合に、前記回数情報の初期化要求に応じて、前記記憶部が記憶する前記回数情報を初期化する初期化処理部と

を備える請求項８に記載のＩＣカード。

[請求項10] 前記所定のパラメータは、前記外部装置から供給される供給情報を含み、

前記所定のアルゴリズムは、前記第１のパスワードのうちの所定の位置の値と、前記供給情報に基づいて生成された所定の置換値とを置換する置換処理を含み、

前記生成部は、前記置換処理に基づいて前記第２のパスワードを生

成する

請求項１に記載のＩＣカード。

[請求項11] 前記記憶部は、前記所定の位置、前記供給情報の種類、及び前記所定の置換値の生成方法のうちの少なくとも１つを示す置換処理情報を記憶し、

さらに、前記認証部によって前記カード利用者が正当であると判定された場合に、前記置換処理情報の変更要求に応じて、前記記憶部が記憶する前記置換処理情報を変更する変更部を備える

請求項１０に記載のＩＣカード。

[請求項12] 前記記憶部は、種類の異なる複数の前記所定のアルゴリズムのうちの１つを選択する選択情報を記憶し、

前記生成部は、前記記憶部が記憶する前記選択情報に基づいて前記複数の所定のアルゴリズムのうちの１つを選択し、選択した当該所定のアルゴリズムに基づいて、前記第２のパスワードを生成する

請求項１から請求項１１のいずれか一項に記載のＩＣカード。

[請求項13] 予め記憶部に記憶されている第１のパスワードと、所定のパラメータと、所定のアルゴリズムとに基づいて、カード利用者の認証用のパスワードである第２のパスワードを生成する生成部と、

外部装置から取得した第３のパスワードと前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する認証部と

を備えるＩＣモジュール。

[請求項14] 請求項１から請求項９のいずれか一項に記載のＩＣカードと、

前記外部装置を介して前記ＩＣカードと接続される認証センタ装置と、

を備え、

前記認証センタ装置は、

前記ＩＣカードを識別するカード識別情報と、前記第１のパスワー

ドと、前記所定のパラメータとを関連付けて記憶するセンタ記憶部と、

前記センタ記憶部が記憶する前記第１のパスワード及び前記所定のパラメータと、前記所定のアルゴリズムとに基づいて、前記第２のパスワードを生成するセンタ生成部と、　前記外部装置を介して前記カード利用者から取得した前記第３のパスワードと、前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定するセンタ認証部と、

前記ＩＣカードが記憶する前記第１のパスワード及び前記所定のパラメータと、当該ＩＣカードに対応する前記カード識別情報と関連付けられて前記センタ記憶部に記憶されている前記第１のパスワード及び前記所定のパラメータとが一致しない場合に、前記センタ記憶部に記憶されている前記第１のパスワード及び前記所定のパラメータを、前記ＩＣカードが記憶する前記第１のパスワード及び前記所定のパラメータに変更する同期処理部と

を備えるＩＣカードシステム。

補正された請求の範囲
[2015年12月14日 (14.12.2015) 国際事務局受理]

[請求項１]（補正後）第１のパスワードを記憶する記憶部と、
前記予め記憶部に記憶されている第１のパスワードと、所定のパラメータと、所定のアルゴリズムとに基づいて、カード利用者の認証用のパスワードである第２のパスワードを生成する生成部と、
外部装置から取得した第３のパスワードと前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する認証部と、
前記認証部によって前記カード利用者が正当であると判定された場合に、前記生成部により生成された第２のパスワードを前記記憶に記憶させる変更部と
を備えるＩＣカード。

[請求項２] 前記所定のアルゴリズムは、前記第１のパスワードと前記所定のパラメータとの演算処理を含み、
前記生成部は、前記第１のパスワードと前記所定のパラメータとの前記演算処理によって前記第２のパスワードを生成する
請求項１に記載のＩＣカード。

[請求項３] 前記記憶部は、前記所定のパラメータを予め記憶し、前記認証部によって前記カード利用者が正当であると判定された場合に、前記所定のパラメータの変更要求に応じて、前記記憶部が記憶する前記所定のパラメータを変更する変更部を備える
請求項２に記載のＩＣカード。

[請求項４]（削除）

[請求項５]（補正後）前記記憶部は、前記第２のパスワードの初期値を記憶し、さらに、
前記認証部によって前記カード利用者が正当であると判定された場合に、前記第２のパスワードの初期化要求に応じて、前記記憶部が記憶する前記第１のパスワードを、前記第２のパスワードの初期値に変更する初期化処理部を備える
請求項１に記載のＩＣカード。

[請求項６] 前記記憶部は、前記第２のパスワードの初期値と、前記第２のパスワードを生成した回数を示す回数情報とを記憶し、
前記認証部は、
前記第３のパスワードと、前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する第１の認証処理と、
前記外部装置から取得した第４のパスワードと、前記第２のパスワードの初期値とを照合し、

当該照合結果に基づいて、前記カード利用者の正当性を判定する第２の認証処理とを実行し、
前記生成部は、前記認証部によって前記第１の認証処理により前記カード利用者が正当であると判定された場合に、前記第２のパスワードを生成するとともに、前記記憶部が記憶する前記回数情報を更新し、
さらに、前記認証部によって前記第２の認証処理により前記カード利用者が正当であると判定された場合に、前記回数情報を前記外部装置に出力させる回数情報処理部を備える
請求項１から請求項４のいずれか一項に記載のＩＣカード。

[請求項７] 前記認証部によって前記第１の認証処理により前記カード利用者が正当であると判定された場合に、前記第２のパスワードの初期化要求に応じて、前記記憶部が記憶する前記第１のパスワードを、前記第２のパスワードの初期値に変更するとともに、前記記憶部が記憶する前記回数情報を初期化する初期化処理部を備える
請求項６に記載のＩＣカード。

[請求項８] 前記記憶部は、前記第２のパスワードの初期値を前記第１のパスワードとして記憶するとともに、前記第２のパスワードを生成した回数を示す回数情報を記憶し、
前記認証部は、
前記第３のパスワードと、前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する第１の認証処理と、
前記外部装置から取得した第４のパスワードと、前記第２のパスワードの初期値とを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する第２の認証処理と、
を実行し、
前記生成部は、
前記第２のパスワードの初期値と、前記所定のパラメータと、前記演算処理と、前記記憶部が記憶する前記回数情報とに基づいて、前記第２のパスワードを生成するとともに、前記認証部による前記第１の認証処理により前記カード利用者が正当であると判定された場合に、前記記憶部が記憶する前記回数情報を更新する
請求項２又は請求項３に記載のＩＣカード。

[請求項９] 前記認証部による前記第２の認証処理により前記カード利用者が正当であると判定された場合に、前記回数情報を前記外部装置に出力させる回数情報処理部と、
前記認証部による前記第１の認証処理により前記カード利用者が正当であると判定された場合に、前記回数情報の初期化要求に応じて、前記記憶部が記憶する前記回数情報を初期化する初期化処理部と
を備える請求項８に記載のＩＣカード。

[請求項１０] 前記所定のパラメータは、前記外部装置から供給される供給情報を
含み、

前記所定のアルゴリズムは、前記第１のパスワードのうちの所定の位置の値と、前記供給情報に基づいて生成された所定の置換値とを置換する置換処理を含み、
前記生成部は、前記置換処理に基づいて前記第２のパスワードを生成する
請求項１に記載のＩＣカード。

[請求項１１]（補正後） 前記記憶部は、前記所定の位置、前記供給情報の種類、及び前記所定の置換値の生成方法のうちの少なくとも１つを示す置換処理情報を記憶し、
前記変更部はさらに、前記認証部によって前記カード利用者が正当であると判定された場合に、前記置換処理情報の変更要求に応じて、前記記憶部が記憶する前記置換処理情報を変更する変更部を備える
請求項１０に記載のＩＣカード。

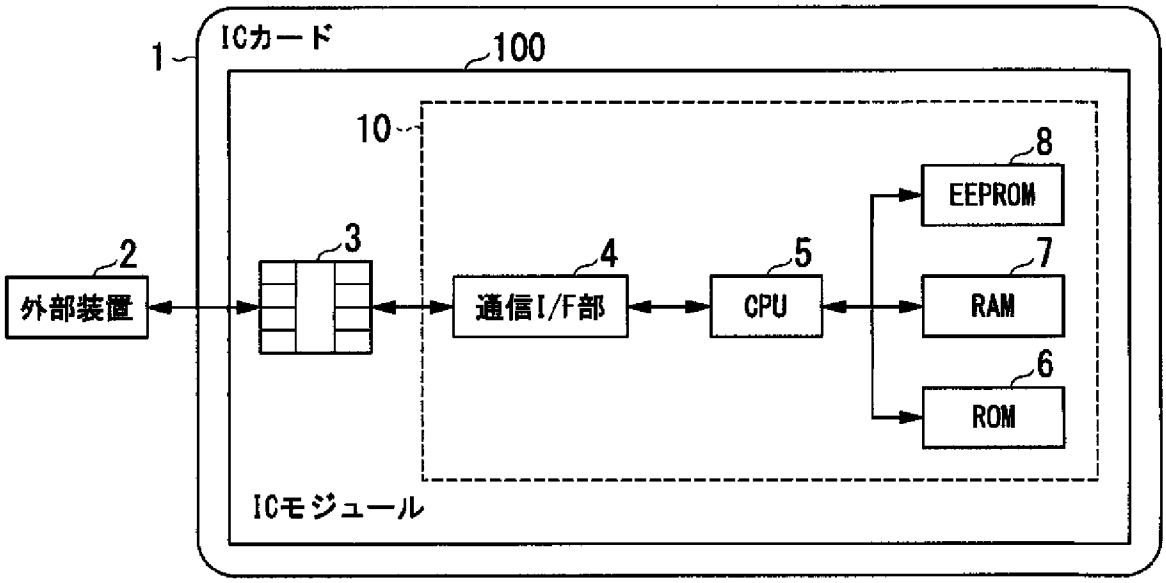
[請求項１２] 前記記憶部は、種類の異なる複数の前記所定のアルゴリズムのうちの１つを選択する選択情報を記憶し、
前記生成部は、前記記憶部が記憶する前記選択情報に基づいて前記複数の所定のアルゴリズムのうちの１つを選択し、選択した当該所定のアルゴリズムに基づいて、前記第２のパスワードを生成する
請求項１から請求項１１のいずれか一項に記載のＩＣカード。

[請求項１３] 予め記憶部に記憶されている第１のパスワードと、所定のパラメータと、所定のアルゴリズムとに基づいて、カード利用者の認証用のパスワードである第２のパスワードを生成する生成部と、
外部装置から取得した第３のパスワードと前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定する認証部と
を備えるＩＣモジュール。

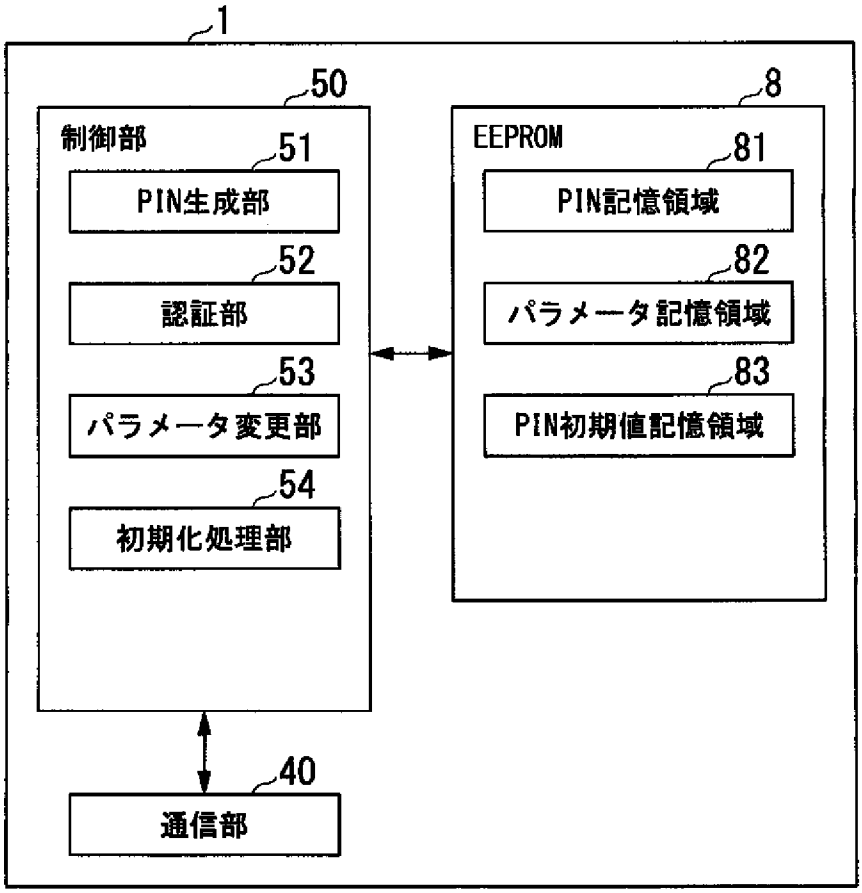
[請求項１４] 請求項１から請求項９のいずれか一項に記載のＩＣカードと、前記外部装置を介して前記ＩＣカードと接続される認証センタ装置と、
を備え、
前記認証センタ装置は、
前記ＩＣカードを識別するカード識別情報と、前記第１のパスワードと、前記所定のパラメータとを関連付けて記憶するセンタ記憶部と、
前記センタ記憶部が記憶する前記第１のパスワード及び前記所定のパラメータと、前記所定のアルゴリズムとに基づいて、前記第２のパスワードを生成するセンタ生成部と、前記外部装置を介して前記カード利用者から取得した前記第３のパスワードと、前記第２のパスワードとを照合し、当該照合結果に基づいて、前記カード利用者の正当性を判定するセンタ認証部と、
前記ＩＣカードが記憶する前記第１のパスワード及び前記所定のパラメータと、当該ＩＣカ

ードに対応する前記カード識別情報と関連付けられて前記センタ記憶部に記憶されている前記第１のパスワード及び前記所定のパラメータとが一致しない場合に、前記センタ記憶部に記憶されている前記第１のパスワード及び前記所定のパラメータを、前記ＩＣカードが記憶する前記第１のパスワード及び前記所定のパラメータに変更する同期処理部と
を備えるＩＣカードシステム。

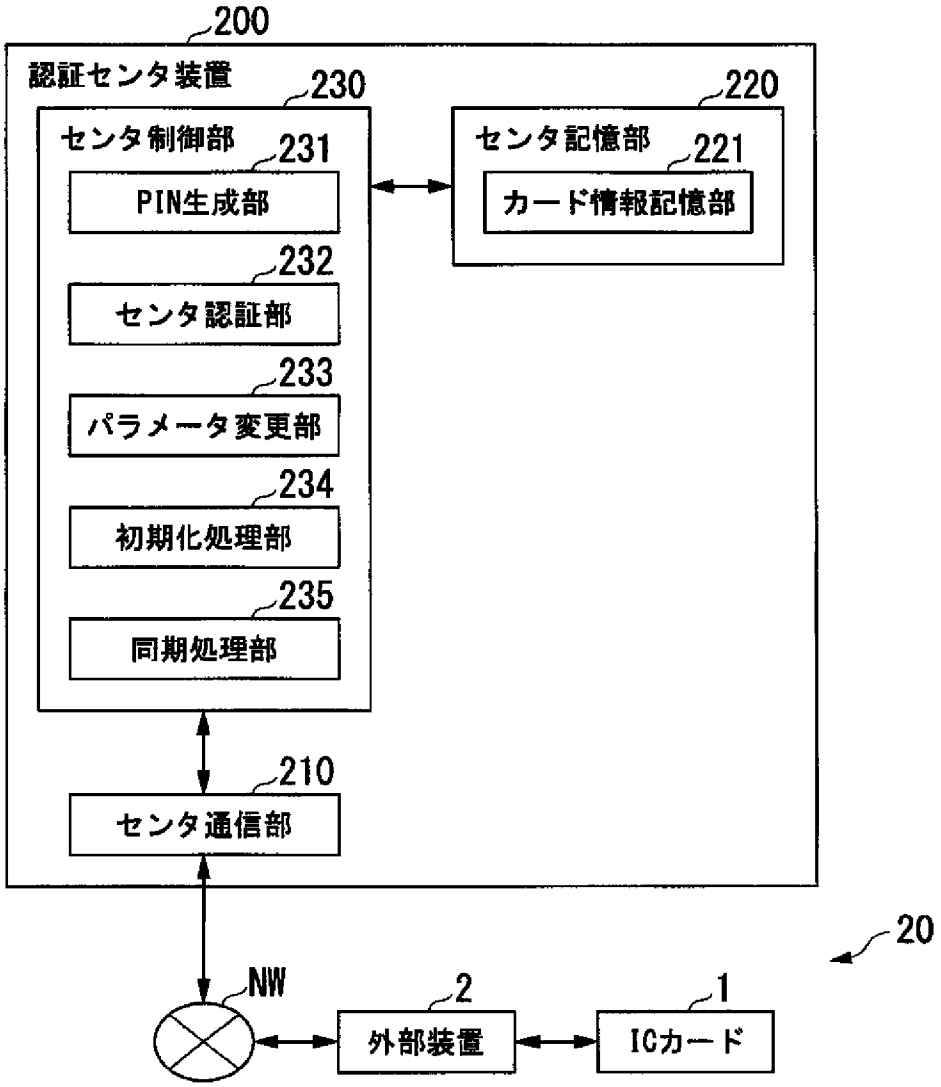
[図1]


1
ICカード
100
10
8
EEPROM
2
外部装置
3
4
通信I/F部
5
CPU
7
RAM
6
ROM
ICモジュール

[図2]


1
50
制御部
51
PIN生成部
52
認証部
53
パラメータ変更部
54
初期化処理部
8
EEPROM
81
PIN記憶領域
82
パラメータ記憶領域
83
PIN初期値記憶領域
40
通信部

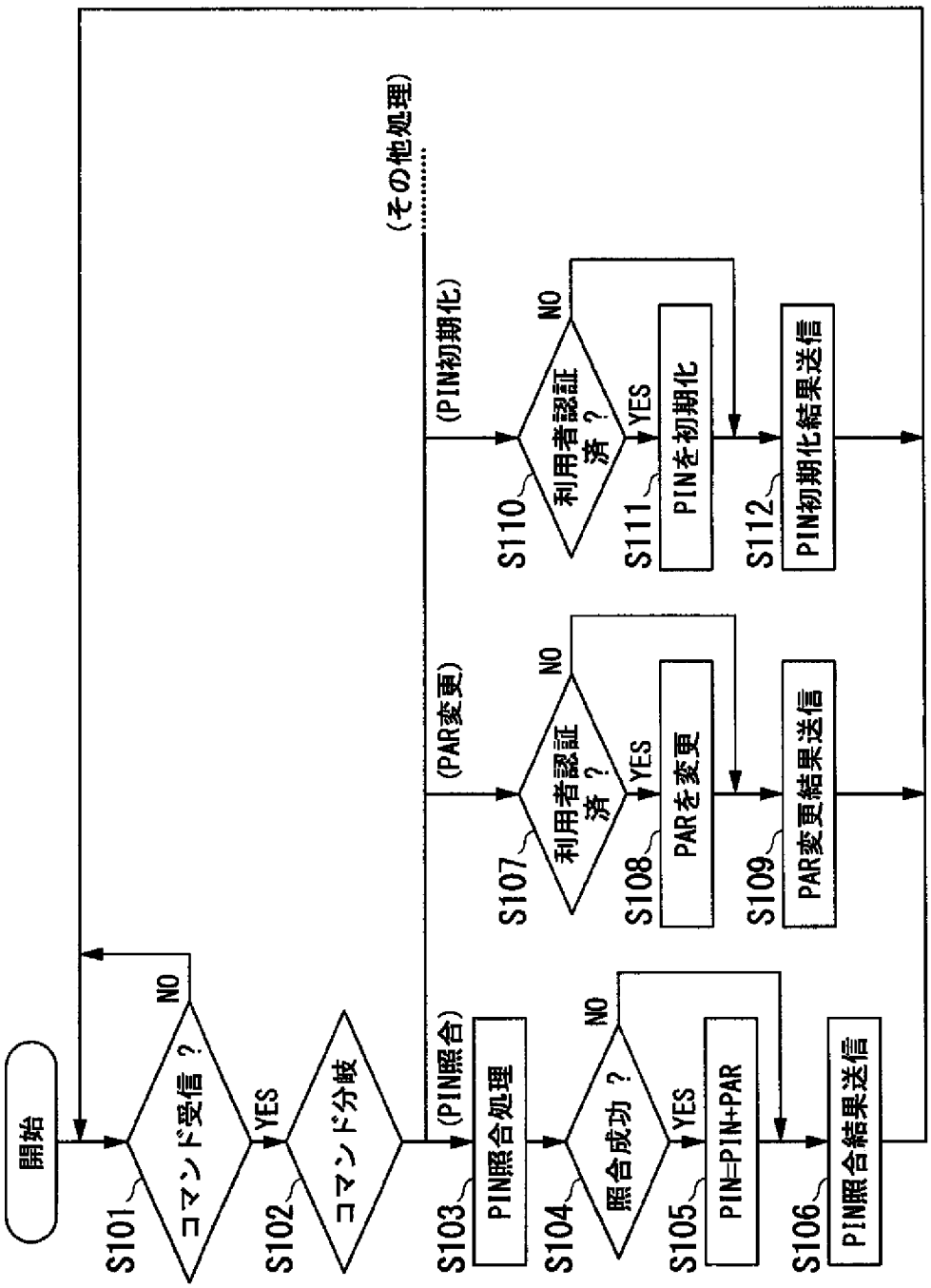
[図3]



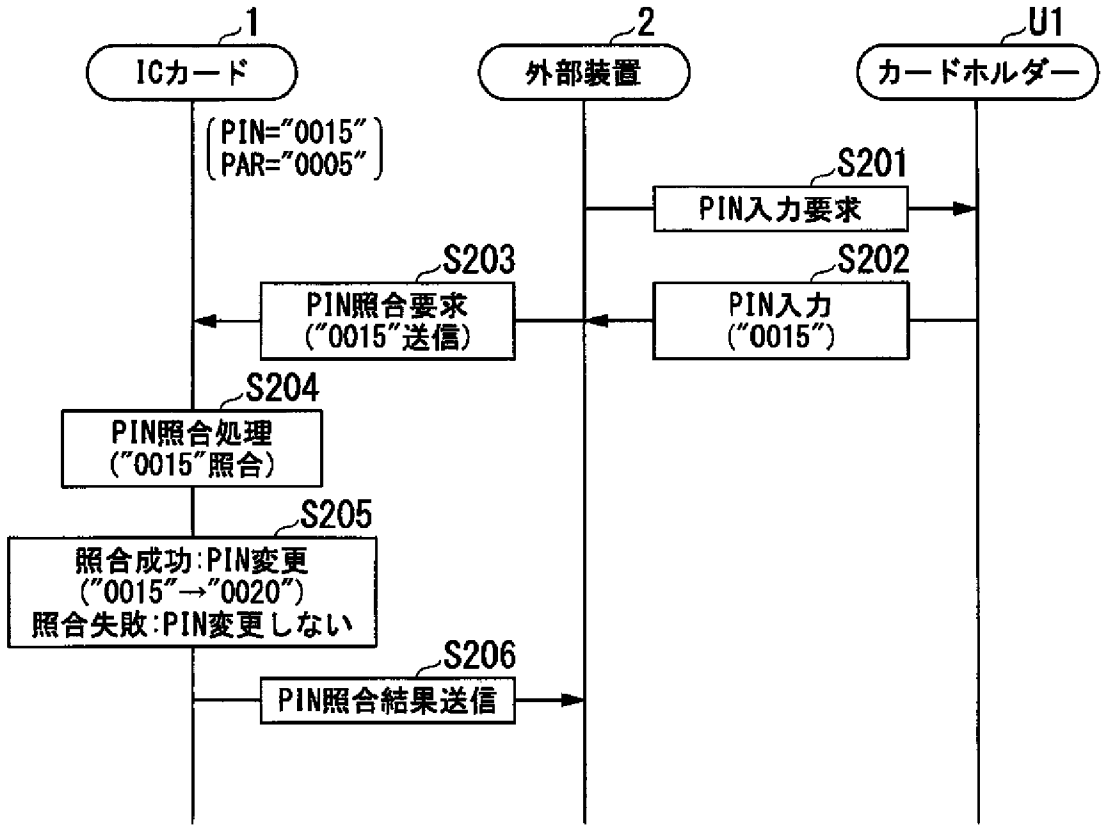
[図4]

カードID	PIN初期値	PIN	PAR	…
XXXXX	0015	0020	0005	…
⋮	⋮	⋮	⋮	⋮

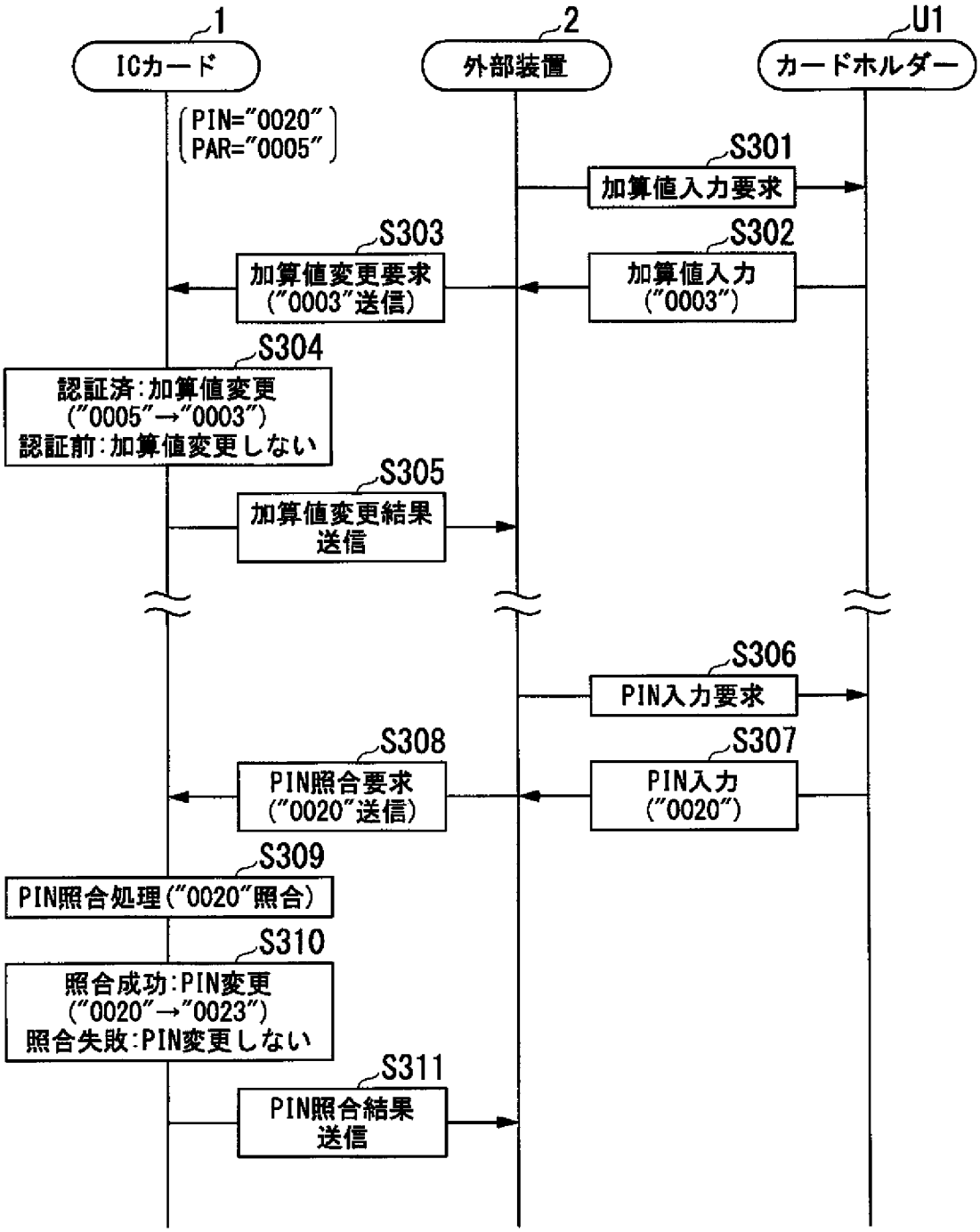
[図5]


開始
S101
コマンド受信 ?
NO
YES
S102
コマンド分岐
(PIN照合)
S103
PIN照合処理
S104
照合成功 ?
NO
YES
S105
PIN=PIN+PAR
S106
PIN照合結果送信
(PAR変更)
S107
利用者認証済 ?
NO
YES
S108
PARを変更
S109
PAR変更結果送信
(PIN初期化)
S110
利用者認証済 ?
NO
YES
S111
PINを初期化
S112
PIN初期化結果送信
(その他処理)

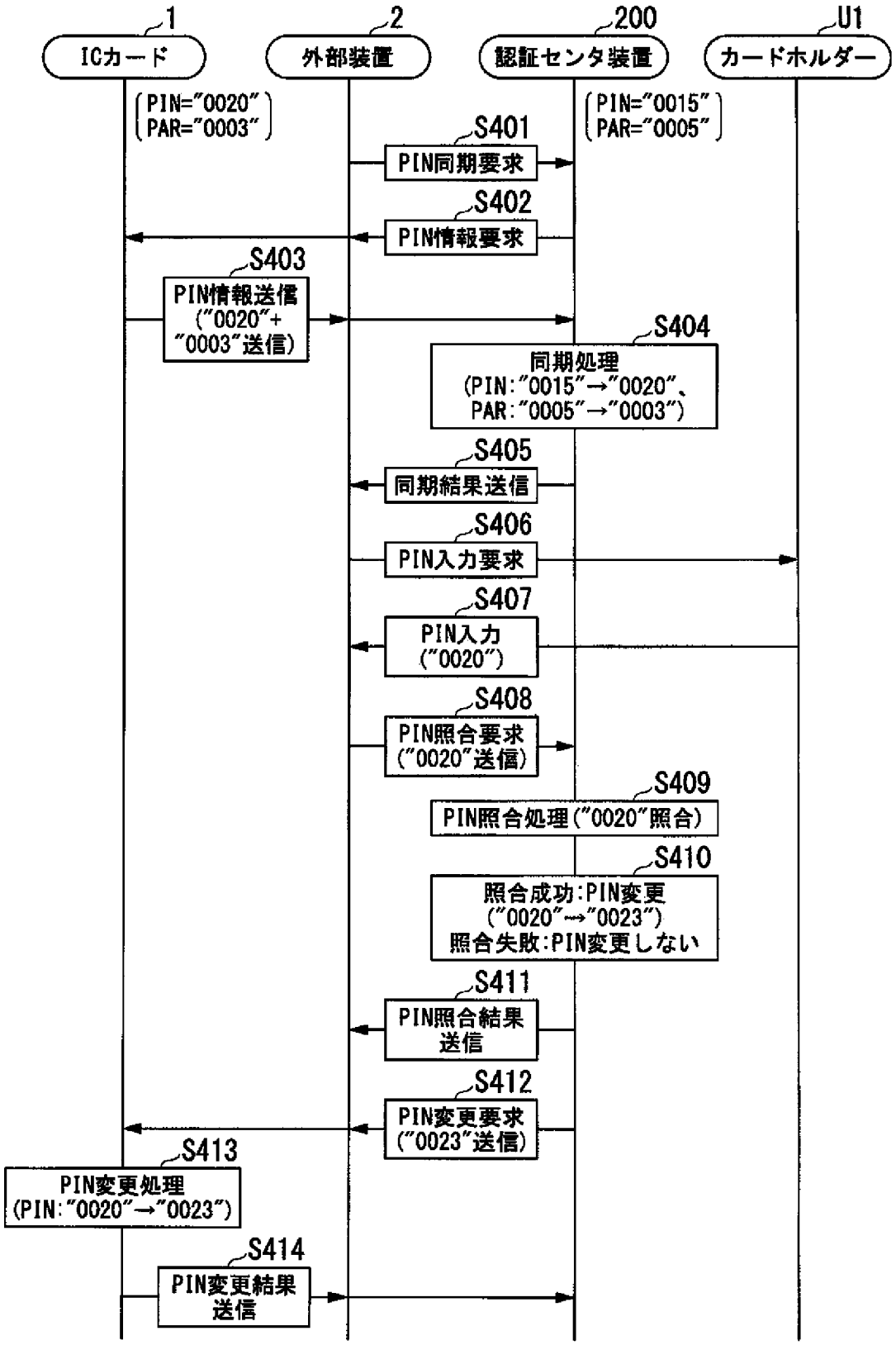
[図6]


1
ICカード
2
外部装置
U1
カードホルダー
PIN="0015"
PAR="0005"
S201
PIN入力要求
S203
PIN照合要求
("0015"送信)
S202
PIN入力
("0015")
S204
PIN照合処理
("0015"照合)
S205
照合成功:PIN変更
("0015"→"0020")
照合失敗:PIN変更しない
S206
PIN照合結果送信

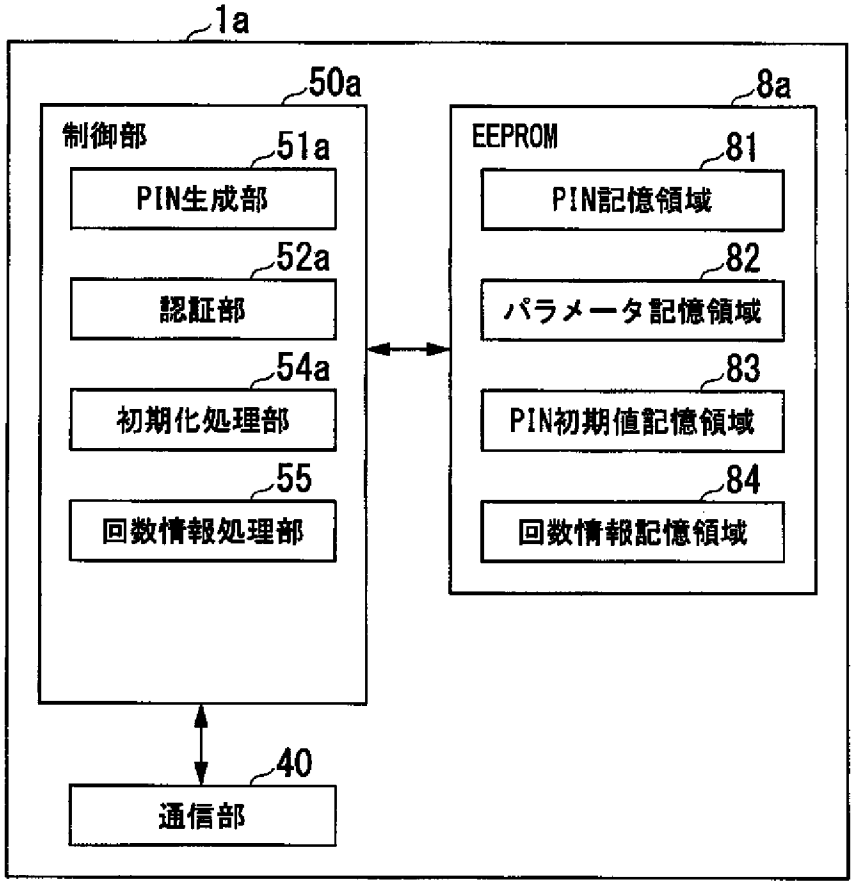
[図7]


1
ICカード
2
外部装置
U1
カードホルダー
PIN="0020"
PAR="0005"
S301
加算値入力要求
S303
加算値変更要求
("0003"送信)
S302
加算値入力
("0003")
S304
認証済:加算値変更
("0005"→"0003")
認証前:加算値変更しない
S305
加算値変更結果
送信
S306
PIN入力要求
S308
PIN照合要求
("0020"送信)
S307
PIN入力
("0020")
S309
PIN照合処理("0020"照合)
S310
照合成功:PIN変更
("0020"→"0023")
照合失敗:PIN変更しない
S311
PIN照合結果
送信

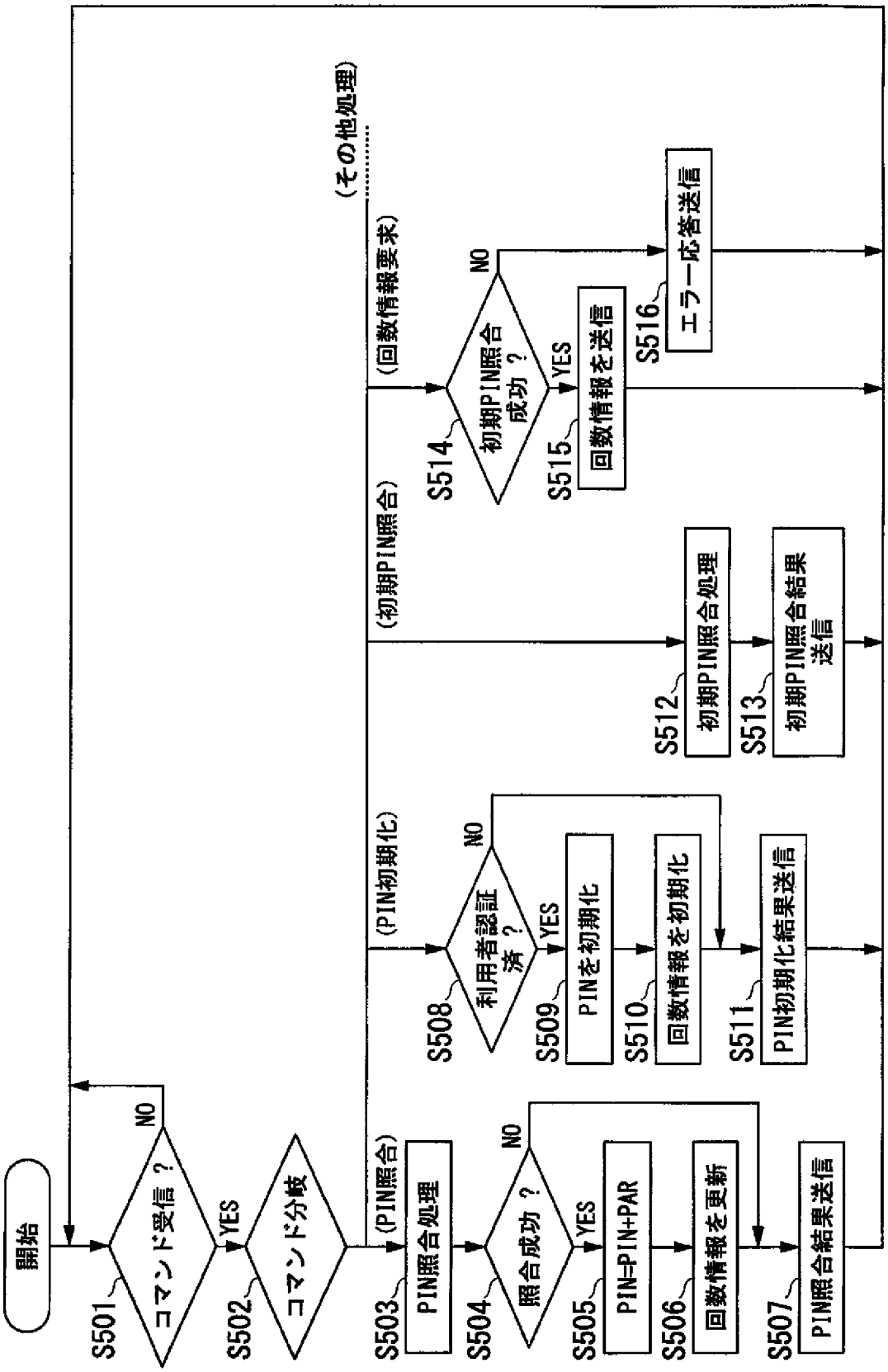
[図8]


1
ICカード
2
外部装置
200
認証センタ装置
U1
カードホルダー
(PIN="0020"
PAR="0003")
(PIN="0015"
PAR="0005")
S401
PIN同期要求
S402
PIN情報要求
S403
PIN情報送信
("0020"+
"0003"送信)
S404
同期処理
(PIN:"0015"→"0020"、
PAR:"0005"→"0003")
S405
同期結果送信
S406
PIN入力要求
S407
PIN入力
("0020")
S408
PIN照合要求
("0020"送信)
S409
PIN照合処理("0020"照合)
S410
照合成功:PIN変更
("0020"→"0023")
照合失敗:PIN変更しない
S411
PIN照合結果
送信
S412
PIN変更要求
("0023"送信)
S413
PIN変更処理
(PIN:"0020"→"0023")
S414
PIN変更結果
送信

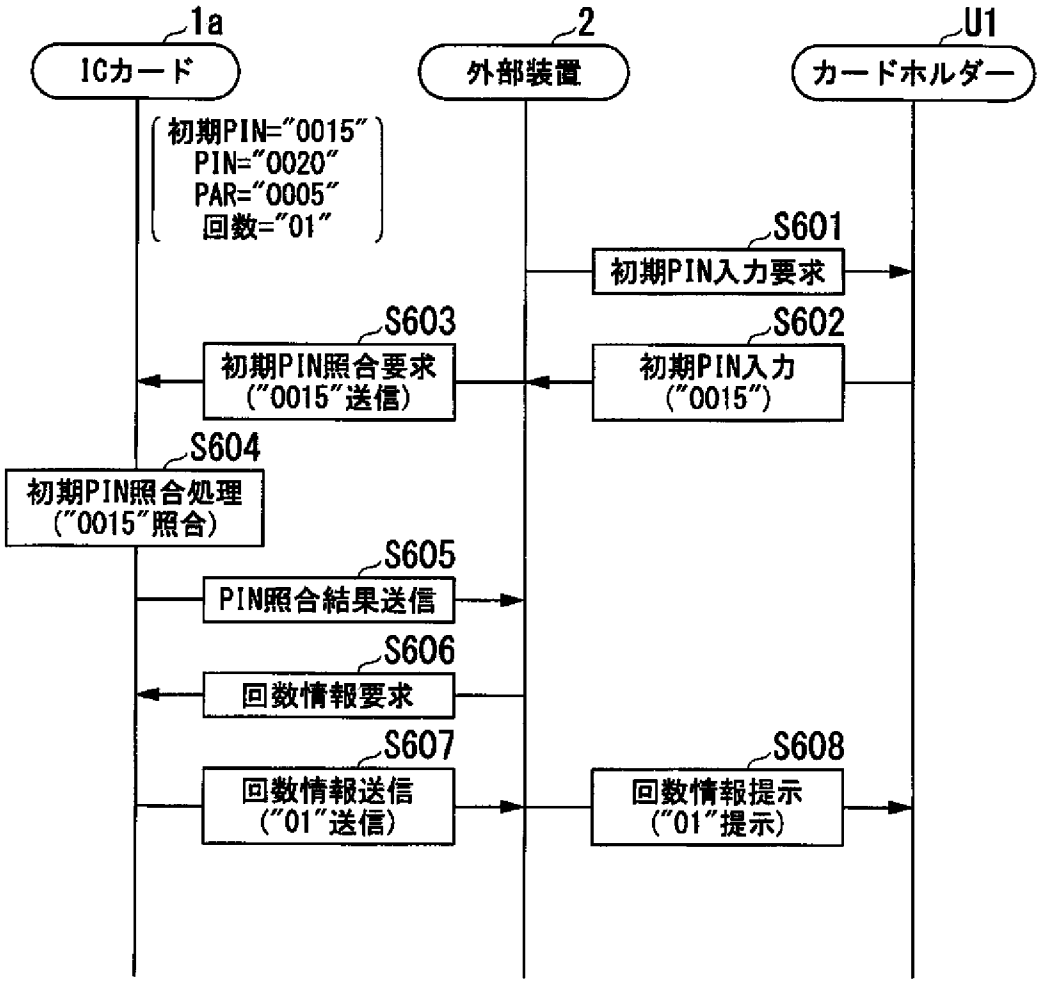
[図9]


1a
50a
制御部
51a
PIN生成部
52a
認証部
54a
初期化処理部
55
回数情報処理部
40
通信部
8a
EEPROM
81
PIN記憶領域
82
パラメータ記憶領域
83
PIN初期値記憶領域
84
回数情報記憶領域

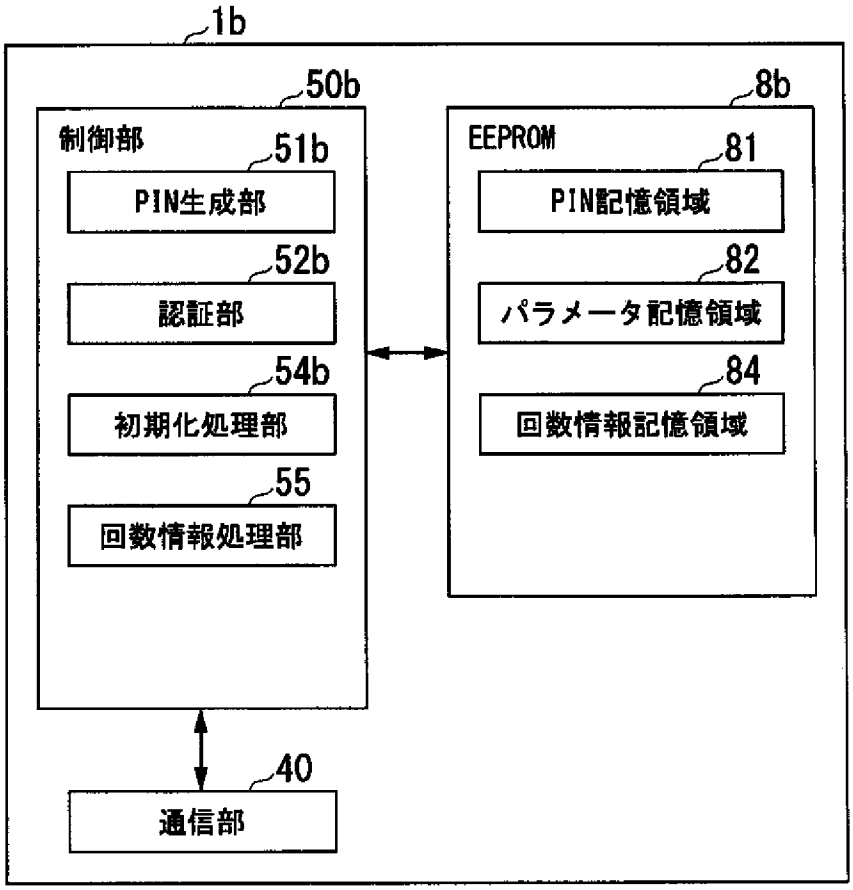
[図10]


開始
S501
コマンド受信 ？
NO
YES
S502
コマンド分岐
(PIN照合)
S503
PIN照合処理
S504
照合成功 ？
NO
YES
S505
PIN=PIN+PAR
S506
回数情報を更新
S507
PIN照合結果送信
(PIN初期化)
S508
利用者認証済 ？
NO
YES
S509
PINを初期化
S510
回数情報を初期化
S511
PIN初期化結果送信
(初期PIN照合)
S512
初期PIN照合処理
S513
初期PIN照合結果送信
(回数情報要求)
S514
初期PIN照合成功 ？
NO
YES
S515
回数情報を送信
S516
エラー応答送信
(その他処理)

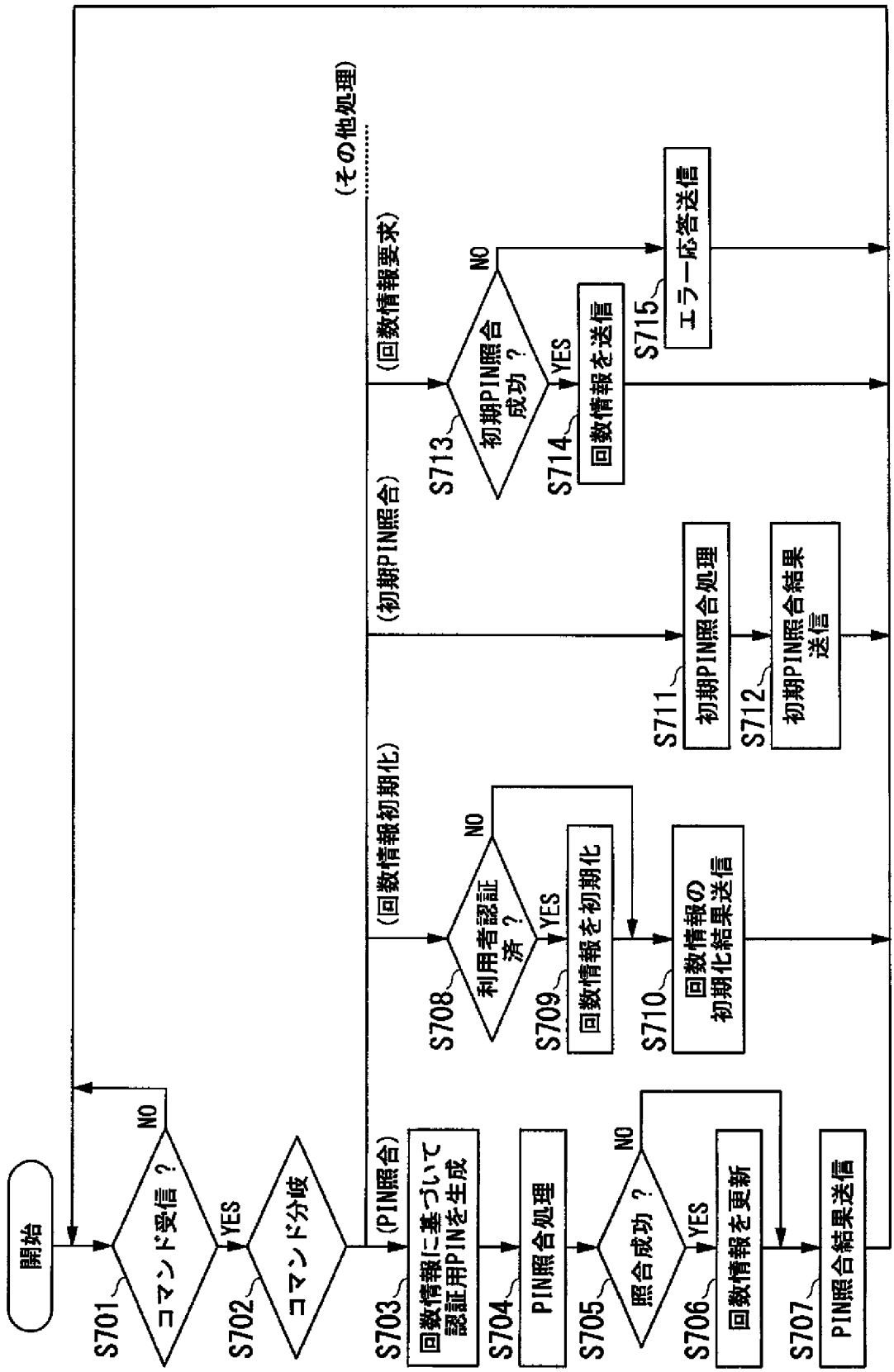
[図11]


1a
ICカード
2
外部装置
U1
カードホルダー
初期PIN="0015"
PIN="0020"
PAR="0005"
回数="01"
S601
初期PIN入力要求
S603
初期PIN照合要求
("0015"送信)
S602
初期PIN入力
("0015")
S604
初期PIN照合処理
("0015"照合)
S605
PIN照合結果送信
S606
回数情報要求
S607
回数情報送信
("01"送信)
S608
回数情報提示
("01"提示)

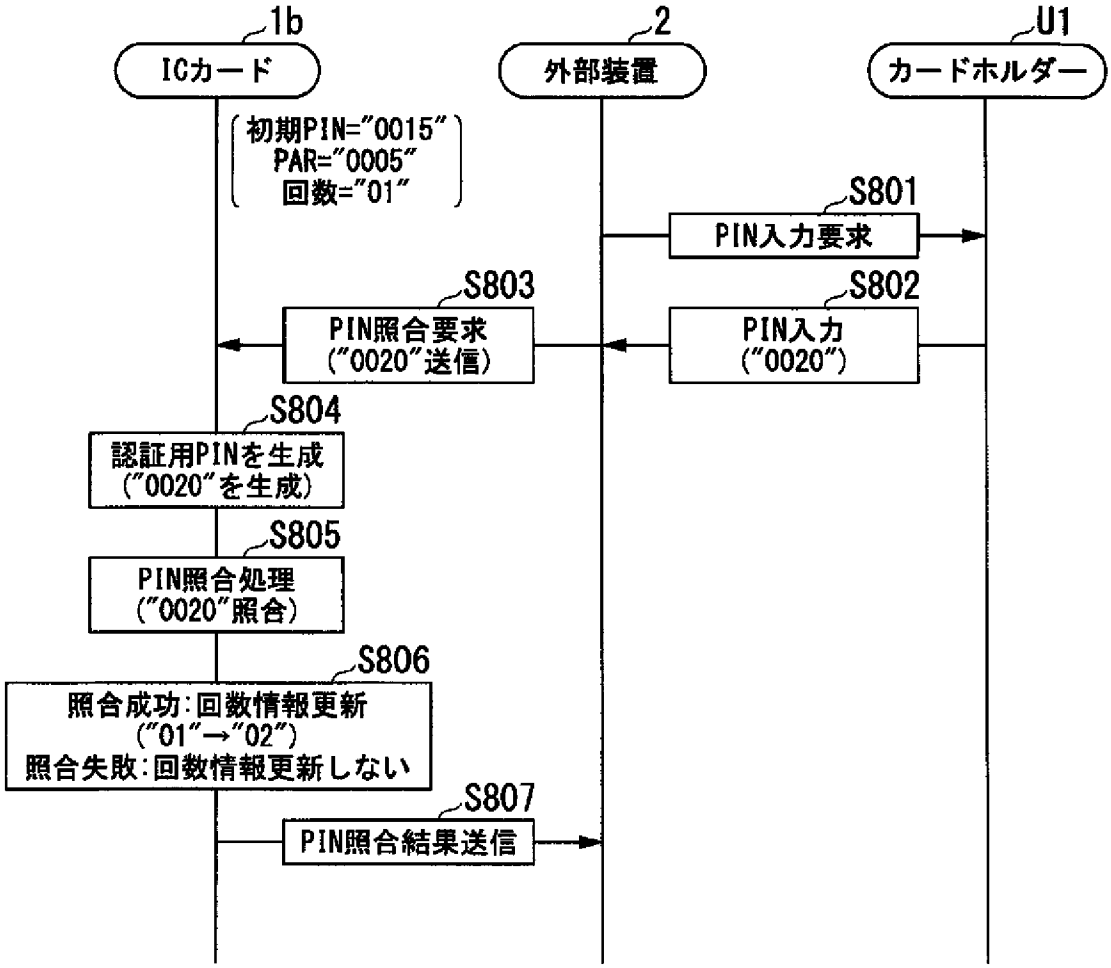
[図12]


1b
50b
制御部
51b
PIN生成部
52b
認証部
54b
初期化処理部
55
回数情報処理部
40
通信部
8b
EEPROM
81
PIN記憶領域
82
パラメータ記憶領域
84
回数情報記憶領域

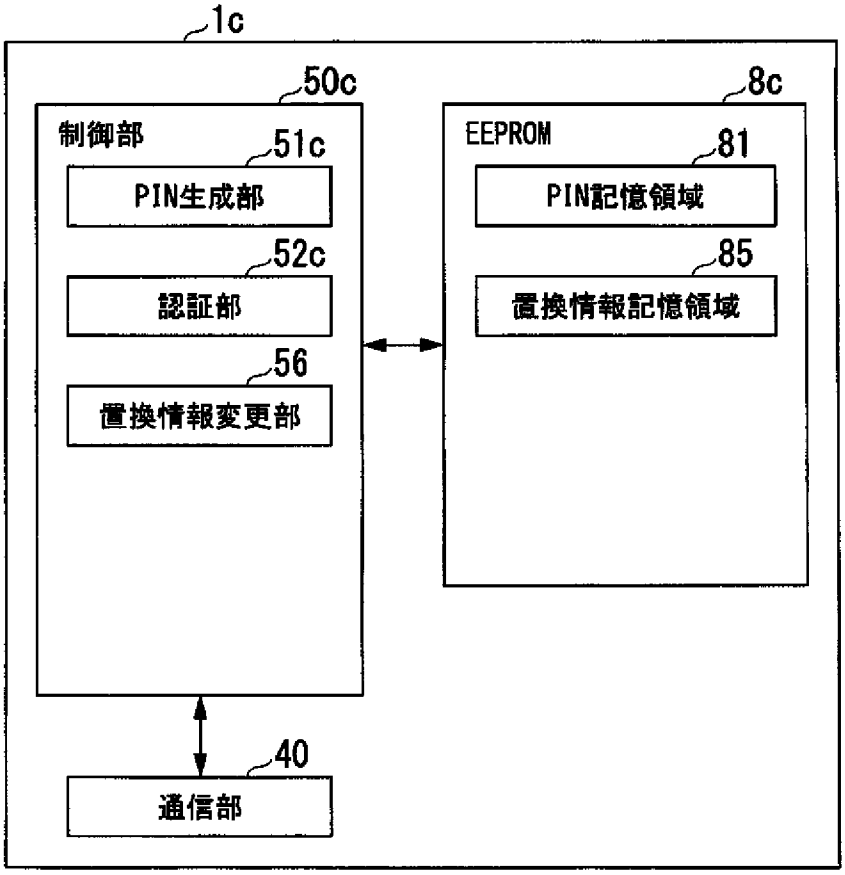
[図13]


開始
S701
コマンド受信 ?
NO
YES
S702
コマンド分岐
(PIN照合)
S703
回数情報に基づいて認証用PINを生成
S704
PIN照合処理
S705
照合成功 ?
NO
YES
S706
回数情報を更新
S707
PIN照合結果送信
(回数情報初期化)
S708
利用者認証済 ?
NO
YES
S709
回数情報を初期化
S710
回数情報の初期化結果送信
(初期PIN照合)
S711
初期PIN照合処理
S712
初期PIN照合結果送信
(回数情報要求)
S713
初期PIN照合成功 ?
NO
YES
S714
回数情報を送信
S715
エラー応答送信
(その他処理)

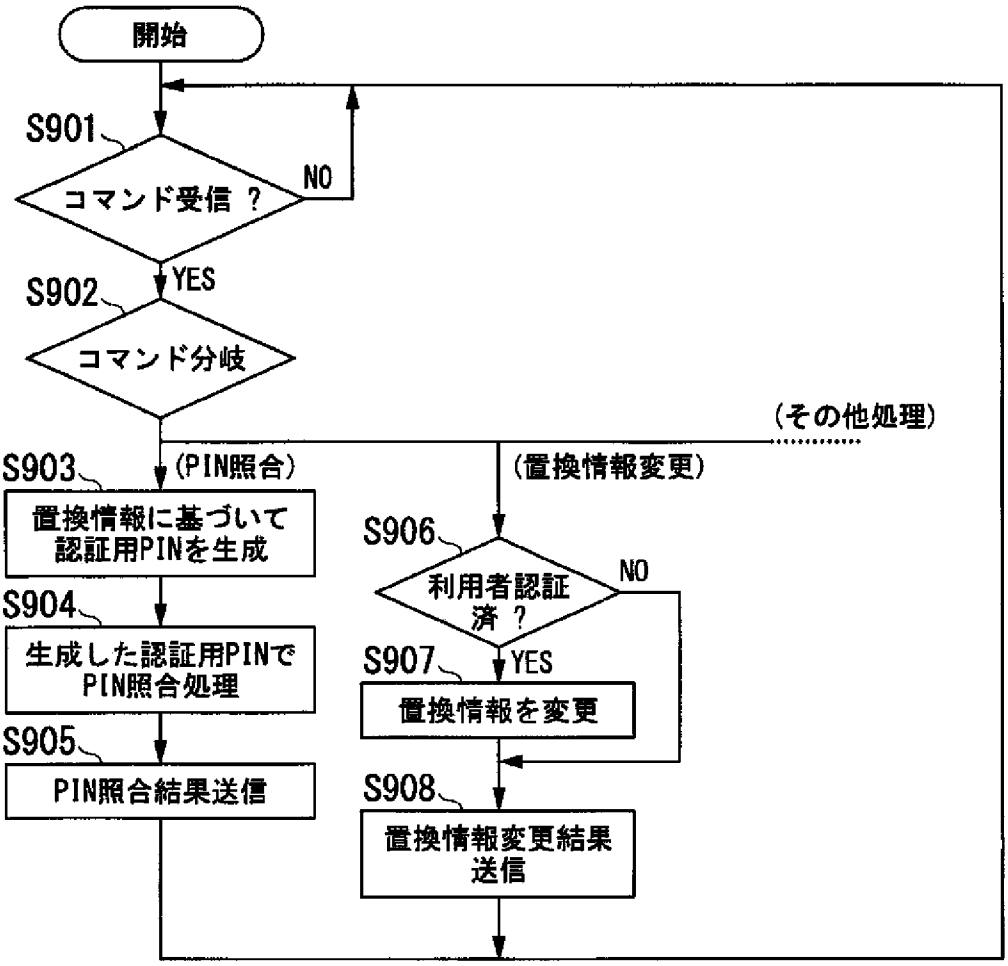
[図14]


1b
ICカード
2
外部装置
U1
カードホルダー
初期PIN="0015"
PAR="0005"
回数="01"
S801
PIN入力要求
S803
PIN照合要求
("0020"送信)
S802
PIN入力
("0020")
S804
認証用PINを生成
("0020"を生成)
S805
PIN照合処理
("0020"照合)
S806
照合成功:回数情報更新
("01"→"02")
照合失敗:回数情報更新しない
S807
PIN照合結果送信

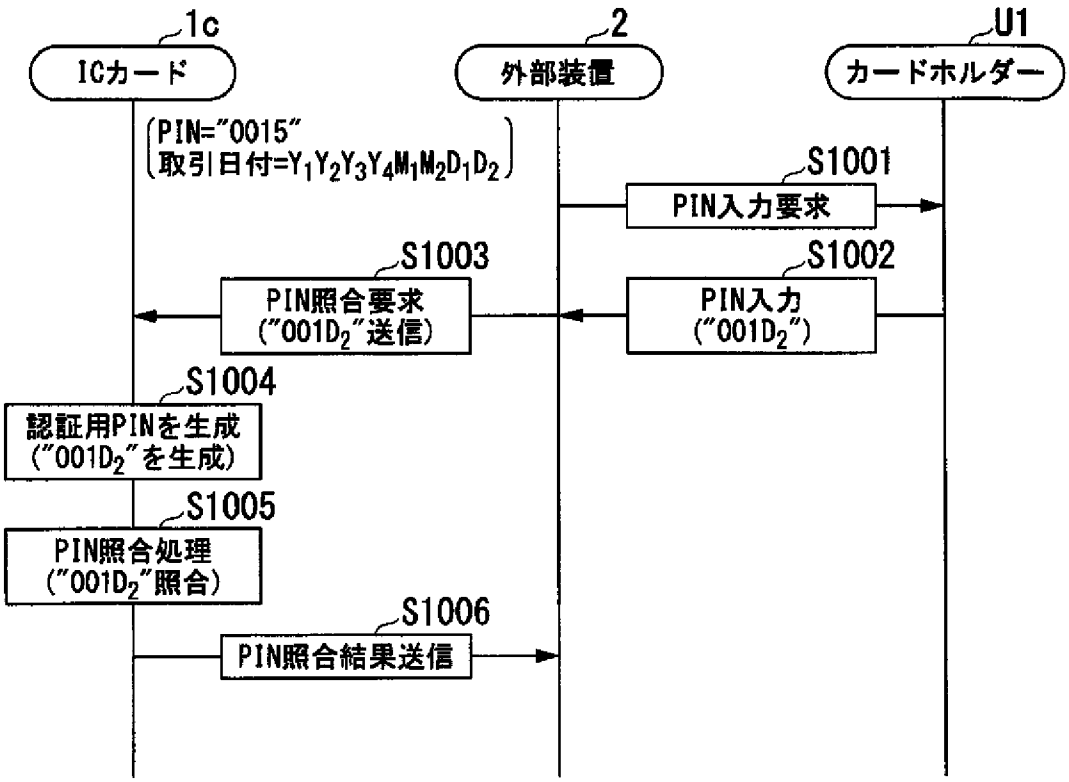
[図15]


1c
50c
制御部
51c
PIN生成部
52c
認証部
56
置換情報変更部
8c
EEPROM
81
PIN記憶領域
85
置換情報記憶領域
40
通信部

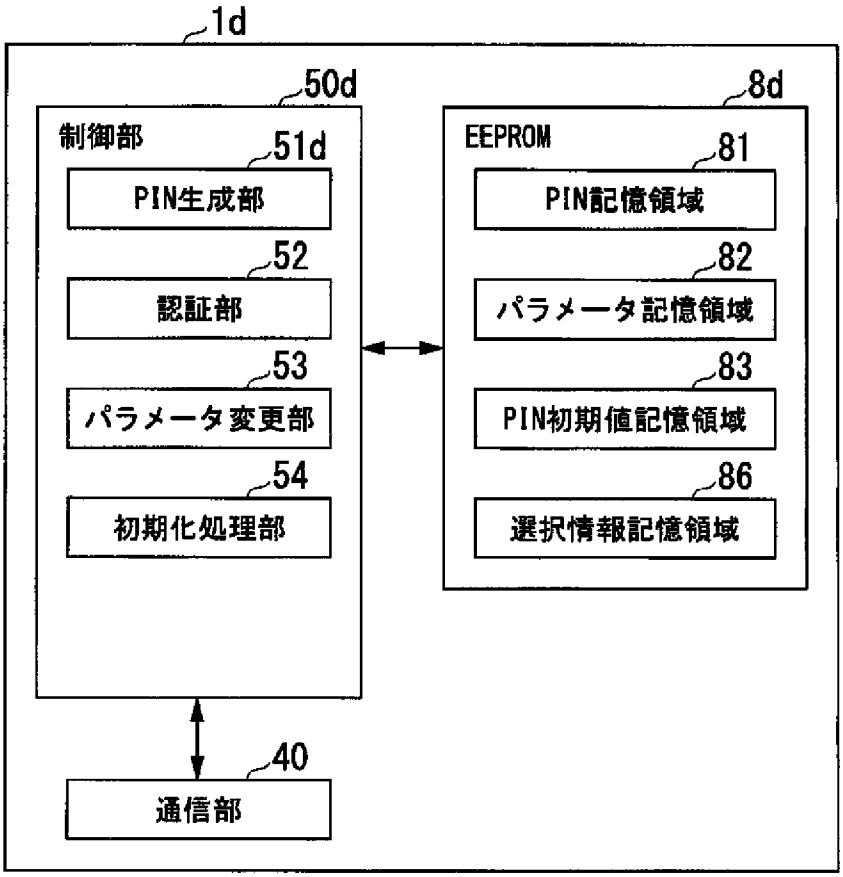
[図16]


開始
S901
コマンド受信 ?
NO
YES
S902
コマンド分岐
(その他処理)
(PIN照合)
(置換情報変更)
S903
置換情報に基づいて認証用PINを生成
S904
生成した認証用PINでPIN照合処理
S905
PIN照合結果送信
S906
利用者認証済 ?
NO
YES
S907
置換情報を変更
S908
置換情報変更結果送信

[図17]


1c
ICカード
2
外部装置
U1
カードホルダー
(PIN="0015"
取引日付=$Y_1Y_2Y_3Y_4M_1M_2D_1D_2$)
S1001
PIN入力要求
S1003
PIN照合要求
("001D_2"送信)
S1002
PIN入力
("001D_2")
S1004
認証用PINを生成
("001D_2"を生成)
S1005
PIN照合処理
("001D_2"照合)
S1006
PIN照合結果送信

[図18]


1d
50d
制御部
51d
PIN生成部
52
認証部
53
パラメータ変更部
54
初期化処理部
40
通信部
8d
EEPROM
81
PIN記憶領域
82
パラメータ記憶領域
83
PIN初期値記憶領域
86
選択情報記憶領域

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2015/004033

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/34(2013.01)i, *G06K19/073*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/34, G06K19/073

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.
X A	JP 2005-85071 A (Dainippon Printing Co., Ltd.), 31 March 2005 (31.03.2005), paragraphs [0021] to [0023]; fig. 4 to 6 (Family: none)	1,2,4,12,13 3,5-11,14
X A	JP 2005-78165 A (The Bank of Tokyo-Mitsubishi Ltd.), 24 March 2005 (24.03.2005), paragraphs [0015] to [0047]; fig. 1 to 6 (Family: none)	1-3,8,10-13 4-7,9,14
A	JP 2003-91712 A (Dainippon Printing Co., Ltd.), 28 March 2003 (28.03.2003), abstract (Family: none)	1-14

☒ 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
22 October 2015 (22.10.15)	02 November 2015 (02.11.15)

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/JP2015/004033

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/0249503 A1 (Bernardo Nicolas Sanchez), 09 December 2004 (09.12.2004), claim 1 & WO 2003/032264 A2 & CA 2358753 A1	1-14

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１５／００４０３３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/34(2013.01)i, G06K19/073(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/34, G06K19/073

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
X A	JP 2005-85071 A (大日本印刷株式会社) 2005.03.31, [0021]-[0023], 図 4-図 6 (ファミリーなし)	1, 2, 4, 12, 13 3, 5-11, 14
X A	JP 2005-78165 A (株式会社東京三菱銀行) 2005.03.24, [0015]-[0047], 図 1-図 6 (ファミリーなし)	1-3, 8, 10-13 4-7, 9, 14
A	JP 2003-91712 A (大日本印刷株式会社) 2003.03.28, 要約 (ファミリーなし)	1-14

☑　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
２２．１０．２０１５	０２．１１．２０１５

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）　５Ｓ　９５５５
宮司　卓佳
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	US 2004/0249503 A1 (Bernardo Nicolas Sanchez) 2004.12.09, claim.1 & WO 2003/032264 A2 & CA 2358753 A1	1-14