

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6181015号
(P6181015)

(45) 発行日 平成29年8月16日(2017.8.16)

(24) 登録日 平成29年7月28日(2017.7.28)

(51) Int.Cl. F I
G06F 21/34 (2013.01) G O 6 F 21/34
G06K 19/073 (2006.01) G O 6 K 19/073 O O 9

請求項の数 18 (全 35 頁)

<p>(21) 出願番号 特願2014-169419 (P2014-169419) (22) 出願日 平成26年8月22日 (2014.8.22) (65) 公開番号 特開2016-45699 (P2016-45699A) (43) 公開日 平成28年4月4日 (2016.4.4) 審査請求日 平成29年3月17日 (2017.3.17)</p>	<p>(73) 特許権者 000003078 株式会社東芝 東京都港区芝浦一丁目1番1号 (74) 代理人 110001634 特許業務法人 志賀国際特許事務所 (72) 発明者 谷口 敬太 東京都港区芝浦一丁目1番1号 株式会社 東芝内 審査官 宮司 卓佳</p>
--	---

最終頁に続く

(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

(57) 【特許請求の範囲】

【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、

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

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】

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、

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 IC カード。

【請求項 6】

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 5 に記載の IC カード。

【請求項 7】

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 6 に記載の IC カード。

【請求項 8】

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 6 又は請求項 7 に記載の IC カード。

10

20

30

40

50

【請求項 9】

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 5 から請求項 8 のいずれか一項に記載の IC カード。

【請求項 10】

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 11】

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、

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し、

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し、

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

10

20

30

40

50

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ＩＣカード。

【請求項 1 2】

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 1 1 に記載のＩＣカード。

【請求項 1 3】

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 1 4】

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 1 3 に記載のＩＣカード。

【請求項 1 5】

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一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一つを選択し、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 1 4 のいずれか一項に記載のＩＣカード。

【請求項 1 6】

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、

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
ＩＣモジュール。

【請求項 1 7】

請求項 1 から請求項 1 6 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、

10

20

30

40

50

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。

【請求項18】

ICカードと、

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ICカードは、

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生成部と、

前記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、

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。

【発明の詳細な説明】

【技術分野】

【0001】

本発明の実施形態は、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】

【0002】

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利用される可能性があった。

【先行技術文献】

【特許文献】

【0003】

10

20

30

40

50

【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】

【0004】

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】

【0005】

実施形態のICカードは、生成部と、認証部と、初期化処理部とを持つ。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。前記記憶部は、前記第2のパスワードの初期値を記憶する。初期化処理部は、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。

10

【図面の簡単な説明】

【0006】

【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。

20

【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。

30

【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】

【0007】

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。

40

【0008】

(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、I

50

C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。

【0009】

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。

10

【0010】

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。

【0011】

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。

20

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。

【0012】

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。

【0013】

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。

30

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。

【0014】

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。

40

【0015】

EEPROM8（記憶部の一例）は、例えば、電氣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。

【0016】

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

50

、 P I N 初期値記憶領域 8 3 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。

【 0 0 1 7 】

P I N 記憶領域 8 1 は、カードホルダーの正当性を認証する P I N を記憶する記憶領域である。P I N 記憶領域 8 1 が記憶する P I N 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 P I N と称することがある）を生成するための P I N（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、P I N 記憶領域 8 1 が記憶する P I N（以下、単に記憶 P I N と称することがある）は、認証用 P I N（第 2 のパスワード）としても使用される。

【 0 0 1 8 】

パラメータ記憶領域 8 2 は、カードホルダーの認証用 P I N 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 P I N 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 8 2 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。

【 0 0 1 9 】

P I N 初期値記憶領域 8 3 は、P I N の初期値を記憶する記憶領域である。ここで、P I N の初期値とは、I C カード 1 及び後述する I C カードシステム 2 0（図 3 参照）にカードホルダーを登録する際に、登録された P I N であり、I C カード 1 及び I C カードシステム 2 0 に最初に記憶された P I N である。

【 0 0 2 0 】

通信部 4 0 は、例えば、通信 I / F 部 4、C P U 5、及び R O M 6 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。

【 0 0 2 1 】

制御部 5 0 は、例えば、C P U 5 と、R A M 7 と、R O M 6 又は E E P R O M 8 とにより実現され、I C カード 1 を統括的に制御する。制御部 5 0 は、例えば、外部装置 2 から I C 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 5 0 は、例えば、P I N 記憶領域 8 1 が記憶する認証用 P I N 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 P I N を変更する。

また、制御部 5 0 は、P I N 生成部 5 1 と、認証部 5 2 と、パラメータ変更部 5 3 と、初期化処理部 5 4 とを備えている。

【 0 0 2 2 】

P I N 生成部 5 1（生成部の一例）は、予め E E P R O M 8（P I N 記憶領域 8 1）に記憶されている記憶 P I N（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 P I N 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、E E P R O M 8 が記憶する記憶 P I N 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 P I N 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 E E P R O M 8（パラメータ記憶領域 8 2）が記憶する加算値である。

【 0 0 2 3 】

P I N 生成部 5 1 は、例えば、P I N 記憶領域 8 1 が記憶する記憶 P I N と、パラメータ記憶領域 8 2 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 P I N を生成する。すなわち、P I N 生成部 5 1 は、記憶 P I N の値と、加算値とを加算した値を認証用 P I N として生成する。また、P I N 生成部 5 1 は、後述する認証部 5 2 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 P I N を生成し、認証用 P I N を記憶 P I N として、E E P R O M 8 の P I N に記憶させる。すなわち、P I N 生成部 5 1 は、例えば、記憶 P I N 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 P I N を生成

10

20

30

40

50

し、生成した認証用 P I N を記憶 P I N として、P I N 記憶領域 8 1 に記憶させる。

【 0 0 2 4 】

認証部 5 2 は、外部装置 2 から取得した取得 P I N (第 3 のパスワード)と、認証用 P I N 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 5 2 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 P I N と、P I N 記憶領域 8 1 が記憶する認証用 P I N とを照合する。認証部 5 2 は、取得 P I N と、認証用 P I N とが一致する場合(照合成功の場合)に、取得 P I N 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 5 2 は、取得 P I N と、認証用 P I N とが一致しない場合(照合失敗の場合)に、取得 P I N を外部装置 2 に入力したカードホルダーが正当でない(認証失敗)と判定する。

10

【 0 0 2 5 】

パラメータ変更部 5 3 (変更部の一例)は、認証部 5 2 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、E E P R O M 8 (パラメータ記憶領域 8 2)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 5 3 は、認証用 P I N 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 I C カード 1 が受信した際に、パラメータ記憶領域 8 2 が記憶する加算値を変更する。パラメータ変更部 5 3 は、認証部 5 2 が、認証用 P I N による認証が成功している場合に、パラメータ記憶領域 8 2 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 5 3 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 8 2 に記憶させる。また、パラメータ変更部 5 3 は、認証用 P I N 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。

20

【 0 0 2 6 】

初期化処理部 5 4 は、認証部 5 2 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 P I N の初期化要求に応じて、E E P R O M 8 (P I N 記憶領域 8 1)が記憶する記憶 P I N を、P I N (認証用 P I N)の初期値に変更する。すなわち、初期化処理部 5 4 は、認証用 P I N による認証が成功している場合に、認証用 P I N を初期化するコマンドを、外部装置 2 を介して I C カード 1 が受信した際に、P I N 記憶領域 8 1 が記憶する記憶 P I N を、P I N (認証用 P I N)の初期値に変更する。初期化処理部 5 4 は、認証用 P I N による認証が成功している場合に、P I N 初期値記憶領域 8 3 が記憶する P I N の初期値を、P I N 記憶領域 8 1 に記憶させる。また、初期化処理部 5 4 は、認証用 P I N による認証が成功していない場合には、認証用 P I N を初期化する処理を実行しない。

30

【 0 0 2 7 】

次に、図 3 を参照して、本実施形態による I C カードシステム 2 0 の構成例について説明する。

図 3 は、本実施形態の I C カードシステム 2 0 の一例を示すブロック図である。

この図に示すように、I C カードシステム 2 0 は、認証センタ装置 2 0 0 と、外部装置 2 と、I C カード 1 とを備えている。

40

【 0 0 2 8 】

なお、この図に示す例は、I C カード 1 を外部装置 2 と接続し、さらに、ネットワーク N W を介して、認証センタ装置 2 0 0 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 2 0 0 が行うことがあり、本実施形態による I C カードシステム 2 0 では、認証センタ装置 2 0 0 がカードホルダーの認証を行うものとする。

【 0 0 2 9 】

認証センタ装置 2 0 0 は、I C 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 N W を介してオンラインにより行い、I C 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 2 0 0 は、例え

50

ば、センタ通信部 2 1 0 と、センタ記憶部 2 2 0 と、センタ制御部 2 3 0 とを備えている。

【 0 0 3 0 】

センタ通信部 2 1 0 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 2 2 0 は、認証センタ装置 2 0 0 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 2 2 0 は、例えば、カード情報記憶部 2 2 1 を備えている。

カード情報記憶部 2 2 1 は、IC カードシステム 2 0 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 2 2 1 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。

10

【 0 0 3 1 】

ここで、「カード ID」は、IC カードシステム 2 0 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 2 3 1 により生成され、変更された認証用 PIN 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。

20

【 0 0 3 2 】

図 3 の説明に戻り、センタ制御部 2 3 0 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 2 0 0 を統括的に制御する。センタ制御部 2 3 0 は、例えば、IC カード 1 が IC カードシステム 2 0 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 2 3 0 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 2 2 1 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 2 3 0 は、例えば、カード情報記憶部 2 2 1 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。

30

カード情報記憶部 2 2 1 は、例えば、PIN 生成部 2 3 1 と、センタ認証部 2 3 2 と、パラメータ変更部 2 3 3 と、初期化処理部 2 3 4 と、同期処理部 2 3 5 とを備えている。

【 0 0 3 3 】

PIN 生成部 2 3 1 (センタ生成部の一例) は、センタ記憶部 2 2 0 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 2 3 1 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 5 1 と同様の処理を実行する。

40

【 0 0 3 4 】

センタ認証部 2 3 2 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 2 2 1 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 2 3 2 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 5 2 と同様の処理を実行する。

【 0 0 3 5 】

パラメータ変更部 2 3 3 は、センタ認証部 2 3 2 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 2 2 1 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 2 3 3 は、IC カード 1 のオンライン処理において、例え

50

ば、上述したパラメータ変更部 5 3 と同様の処理を実行する。なお、パラメータ変更部 2 3 3 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 2 1 0 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 2 2 1 の上述した「P A R」を変更する。

【 0 0 3 6 】

初期化処理部 2 3 4 は、センタ認証部 2 3 2 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 P I N の初期化要求に応じて、カード情報記憶部 2 2 1 が記憶する記憶 P I N を、P I N（認証用 P I N）の初期値に変更する。すなわち、初期化処理部 2 3 4 は、I C 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 5 4 と同様の処理を実行する。なお、初期化処理部 2 3 4 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 P I N の初期化要求を、センタ通信部 2 1 0 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 2 2 1 の上述した「P I N」を、P I N の初期値である「P I N 初期値」の値に変更する。

10

【 0 0 3 7 】

同期処理部 2 3 5 は、センタ記憶部 2 2 0 に記憶されている「P I N」及び「P A R」を I C カード 1 と同期させる処理を行う。同期処理部 2 3 5 は、I C カード 1 が記憶する記憶 P I N 及び所定のパラメータと、当該 I C カード 1 に対応する「P I N」及び「P A R」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 2 3 5 は、例えば、I C カード 1 が記憶する記憶 P I N 及び所定のパラメータと、当該 I C カード 1 に対応する「カード I D」と関連付けられてセンタ記憶部 2 2 0 に記憶されている「P I N」及び「P A R」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 2 3 5 は、センタ記憶部 2 2 0 に記憶されている「P I N」及び「P A R」を、I C カード 1 が記憶する記憶 P I N 及び所定のパラメータに変更する。

20

【 0 0 3 8 】

次に、図面を参照して、本実施形態による I C カード 1 及び I C カードシステム 2 0 の動作について説明する。

図 5 は、本実施形態による I C 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、I C 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。

【 0 0 3 9 】

この図に示すように、I C 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 S 1 0 1）。すなわち、I C カード 1 の通信部 4 0 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 4 0 は、コマンドを受信した場合（ステップ S 1 0 1：Y E S）に、処理をステップ S 1 0 2 に進める。また、通信部 4 0 は、コマンドを受信していない場合（ステップ S 1 0 1：N O）に、ステップ S 1 0 1 の処理に戻し、処理を繰り返す。

30

【 0 0 4 0 】

ステップ S 1 0 2 において、I C カード 1 の制御部 5 0 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 5 0 は、受信したコマンドが P I N を照合するコマンドである場合（P I N 照合）に、処理をステップ S 1 0 3 に進める。また、制御部 5 0 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（P A R 変更）に、処理をステップ S 1 0 7 に進める。また、制御部 5 0 は、受信したコマンドが認証用 P I N の初期化要求である場合（P I N 初期化）に、処理をステップ S 1 1 0 に進める。

40

【 0 0 4 1 】

ステップ S 1 0 3 において、制御部 5 0 の認証部 5 2 は、P I N 照合処理を実行する。すなわち、認証部 5 2 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 P I N を取得し、当該取得 P I N と、P I N 記憶領域 8 1 が記憶する記憶 P I N とを照合する。

【 0 0 4 2 】

次に、認証部 5 2 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 S 1 0 4）。認証部 5 2 は、例えば、照合結果が取得 P I N と記憶 P I N とが一致している照合成

50

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タ値に達した場合に、認証用PINによる照合処理の実行を禁止してもよい。

10

【0043】

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。

【0044】

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。

20

【0045】

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。

30

【0046】

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。

【0047】

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。

40

【0048】

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。

【0049】

50

ステップS 1 1 1において、初期化処理部5 4は、P I N記憶領域8 1が記憶する認証用P I N（記憶P I N）を初期化する。すなわち、初期化処理部5 4は、P I N記憶領域8 1が記憶する記憶P I Nを、P I N初期値記憶領域8 3が記憶するP I Nの初期値に変更する。

【0050】

また、ステップS 1 1 2において、制御部5 0は、P I N初期化結果を送信させる。すなわち、制御部5 0は、初期化処理部5 4が、例えば、認証用P I N（記憶P I N）を初期化した結果（P I N初期化結果）を、通信部4 0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S 1 1 2の処理後に、制御部5 0は、処理をステップS 1 0 1に戻し、次のコマンド受信を待つ。

10

【0051】

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。

この図において、ICカード1は、「P I N」（記憶P I N）が“0015”、「P A R」（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。

【0052】

図6において、カードホルダーU 1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U 1に対して、P I N入力要求を出力する（ステップS 2 0 1）。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U 1にP I Nの入力を促す表示を出力する。

20

【0053】

次に、カードホルダーU 1によって、外部装置2にP I N（例えば、“0015”）が入力されると（ステップS 2 0 2）、外部装置2は、ICカード1に対して、P I N照合要求を送信する（ステップS 2 0 3）。すなわち、外部装置2は、取得P I Nとして、例えば、“0015”を含むP I N照合のコマンドを、ICカード1に対して送信する。

【0054】

次に、ICカード1は、P I N照合のコマンドに応じて、P I N照合処理（例えば、“0015”の照合）を実行する（ステップS 2 0 4）。ICカード1の認証部5 2は、例えば、取得P I Nである“0015”と、P I N記憶領域8 1が記憶する“0015”とを照合する。なお、ここでは、認証部5 2は、取得P I Nである“0015”と、P I N記憶領域8 1が記憶する“0015”とが一致するので、照合成功と判定する。

30

【0055】

次に、ICカード1のP I N生成部5 1が、照合成功である場合に、P I Nを変更し、照合失敗である場合に、P I Nを変更しない（ステップS 2 0 5）。なお、この例では、認証部5 2が照合成功と判定しているので、P I N生成部5 1は、“0015”に“0005”を加算処理して、次回に使用する認証用P I N“0020”を生成する。P I N生成部5 1は、生成した認証用P I N“0020”をP I N記憶領域8 1に記憶させる。

【0056】

次に、ICカード1は、P I N照合結果を外部装置2に送信する（ステップS 2 0 6）。すなわち、ICカード1の制御部5 0は、認証部5 2のP I N照合結果を通信部4 0に送信させる。

40

このように、本実施形態によるICカード1は、P I N照合（カードホルダーU 1の認証）が成功するごとに、認証用P I Nを変更する。

【0057】

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。

この図において、ICカード1は、「P I N」（記憶P I N）が“0020”、「P A

50

R」(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、記憶PINが“0020”である状態である。

【0058】

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。

【0059】

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。

10

【0060】

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。

20

【0061】

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。

【0062】

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。

30

【0063】

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。

【0064】

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。

40

この図において、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。

【0065】

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)。

50

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。

【0066】

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。

10

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。

【0067】

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。

20

【0068】

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。

【0069】

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。

30

【0070】

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。

40

【0071】

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ため、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。

【0072】

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23

50

2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。

【0073】

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、ICカード1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1に送信する。

【0074】

ICカード1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。

【0075】

次に、ICカード1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1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1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1との間でPIN情報を同期させる。

【0076】

以上説明したように、本実施形態によるICカード1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1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1は、セキュリティを向上させることができる。

【0077】

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。

【0078】

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

10

20

30

40

50

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。

【 0 0 7 9 】

また、本実施形態では、PIN 生成部 5 1 は、認証部 5 2 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、EEPROM 8 に記憶させる。そして、認証部 5 2 は、次回の照合をする際に、取得 PIN と、記憶 PIN として EEPROM 8 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、EEPROM 8 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、CPU 5 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、CPU 5 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。

【 0 0 8 0 】

また、本実施形態では、EEPROM 8 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 5 2 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、EEPROM 8 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 5 4 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。

【 0 0 8 1 】

本実施形態による IC モジュール 1 0 0 は、PIN 生成部 5 1 と、認証部 5 2 とを備えている。PIN 生成部 5 1 は、予め EEPROM 8（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 5 2 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 1 0 0 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。

【 0 0 8 2 】

また、本実施形態によれば、IC カードシステム 2 0 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 2 0 0 とを備えている。認証センタ装置 2 0 0 は、センタ記憶部 2 2 0 と、PIN 生成部 2 3 1（センタ生成部）と、センタ認証部 2 3 2 と、同期処理部 2 3 5 とを備えている。センタ記憶部 2 2 0 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 2 3 1 は、センタ記憶部 2 2 0 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 2 3 2 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 2 3 5 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 2 2 0 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 2 2 0 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。

【 0 0 8 3 】

これにより、本実施形態による IC カードシステム 2 0 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 2 0 0 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 2 0 は、例えば、

10

20

30

40

50

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 P I N 及びパラメータを適切に変更することができる。

【 0 0 8 4 】

上述した本実施形態では、P I N 生成部 5 1 は、認証処理が成功した場合に、次回に照合する認証用 P I N を生成し、E E P R O M 8 に次回に照合する認証用 P I N を記憶 P I N 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、P I N 生成部 5 1 は、認証処理の際に、E E P R O M 8 が記憶する記憶 P I N に基づいて、毎回認証用 P I N を生成し、生成した認証用 P I N による認証処理が成功した場合に、生成した認証用 P I N を記憶 P I N として記憶させてもよい。

【 0 0 8 5 】

(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 I C カード 1 a 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 P I N を忘れてしまった場合に、I C カード 1 a が、現在の認証用 P I N 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 I C カード 1 a 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。

【 0 0 8 6 】

図 9 は、本実施形態の I C カード 1 a の機能構成例を示すブロック図である。

この図に示すように、I C カード 1 a は、E E P R O M 8 a と、通信部 4 0 と、制御部 5 0 a とを備えている。E E P R O M 8 a は、P I N 記憶領域 8 1 と、パラメータ記憶領域 8 2 と、P I N 初期値記憶領域 8 3 と、回数情報記憶領域 8 4 とを備えている。また、制御部 5 0 a は、P I N 生成部 5 1 a と、認証部 5 2 a と、初期化処理部 5 4 a と、回数情報処理部 5 5 とを備えている。

ここで、図 9 に示される各部分は、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。

【 0 0 8 7 】

回数情報記憶領域 8 4 は、認証用 P I N を生成した回数を示す回数情報を記憶する。

認証部 5 2 a 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 5 2 a は、第 1 の認証処理において、取得 P I N と、認証用 P I N 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 5 2 a 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 P I N (第 4 のパスワード) と、認証用 P I N 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 5 2 a は、第 2 の認証処理において、P I N 初期値記憶領域 8 3 が記憶する P I N の初期値による認証処理を実行する。

【 0 0 8 8 】

P I N 生成部 5 1 a は、認証部 5 2 a 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 P I N を生成するとともに、E E P R O M 8 a (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、P I N 生成部 5 1 a は、回数情報記憶領域 8 4 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 8 4 に記憶させる。なお、P I N 生成部 5 1 a のその他の機能は、第 1 の実施形態の P I N 生成部 5 1 と同様である。

【 0 0 8 9 】

回数情報処理部 5 5 は、認証部 5 2 a 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 8 4 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 8 4 が記憶する回数情報が判明すれば、カードホルダーは、P I N の初期値と、パラメータの値とにより、現在の認証用 P I N を算出することが可能になる。

【 0 0 9 0 】

10

20

30

40

50

初期化処理部 5 4 a は、認証部 5 2 a 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 P I N の初期化要求に応じて、E E P R O M 8 a が記憶する記憶 P I N を、認証用 P I N の初期値に変更する。そして、初期化処理部 5 4 a は、この初期化処理の際に、E E P R O M 8 a の回数情報記憶領域 8 4 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 5 4 a は、回数情報記憶領域 8 4 が記憶する回数情報として、例えば、“ 0 ”を記憶させる。

【 0 0 9 1 】

次に、図 1 0 を参照して、本実施形態による I C カード 1 a の動作の一例について説明する。

図 1 0 は、本実施形態の I C カード 1 a の動作の一例を示すフローチャートである。

この図において、ステップ S 5 0 1 及びステップ S 5 0 2 の処理は、図 5 に示すステップ S 1 0 1 及びステップ S 1 0 2 の処理と同様であるので、ここではその説明を省略する。

【 0 0 9 2 】

なお、ステップ S 5 0 2 のコマンド分岐の処理において、制御部 5 0 a は、受信したコマンドが P I N を照合するコマンドである場合（P I N 照合）に、処理をステップ S 5 0 3 に進める。また、制御部 5 0 a は、受信したコマンドが認証用 P I N の初期化要求である場合（P I N 初期化）に、処理をステップ S 5 0 8 に進める。また、制御部 5 0 a は、受信したコマンドが P I N の初期値を照合するコマンドである場合（初期 P I N 照合）に、処理をステップ S 5 1 2 に進める。また、制御部 5 0 a 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 S 5 1 4 に進める。

【 0 0 9 3 】

ステップ S 5 0 3 からステップ S 5 0 7 までの P I N 照合の処理（第 1 の認証処理）において、ステップ S 5 0 6 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 S 1 0 3 からステップ S 1 0 6 までの処理と同様である。

ステップ S 5 0 6 において、制御部 5 0 a の P I N 生成部 5 1 a 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、P I N 生成部 5 1 a は、回数情報記憶領域 8 4 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 8 4 に記憶させる。

【 0 0 9 4 】

また、ステップ S 5 0 8 からステップ S 5 1 1 までの P I N 初期化の処理は、ステップ S 5 1 0 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 S 1 1 0 からステップ S 1 1 2 までの処理と同様である。

ステップ S 5 1 0 において、制御部 5 0 a の初期化処理部 5 4 a は、回数情報を初期化する。すなわち、初期化処理部 5 4 a は、回数情報記憶領域 8 4 が記憶する回数情報として、例えば、“ 0 ”を記憶させる。

【 0 0 9 5 】

ステップ S 5 1 2 において、制御部 5 0 a の認証部 5 2 a は、第 2 の認証処理として、初期 P I N 照合処理を行う。認証部 5 2 a は、外部装置 2 から取得した取得初期 P I N と、認証用 P I N 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 5 2 a は、第 2 の認証処理において、P I N 初期値記憶領域 8 3 が記憶する P I N の初期値による認証処理を実行する。なお、認証部 5 2 a は、R A M 7 内に、照合結果を示す情報を記憶させる。また、認証部 5 2 a は、照合失敗の場合には、例えば、認証失敗の回数を示す E E P R O M 8 a 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タ値に達した場合に、初期 P I N による照合処理の実行を禁止してもよい。

【 0 0 9 6 】

ステップ S 5 1 3 において、制御部 5 0 a は、初期 P I N 照合結果を送信させる。すなわち、制御部 5 0 a は、認証部 5 2 a が照合した初期 P I N の照合結果（認証結果）を、

10

20

30

40

50

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 S 5 1 3 の処理後に、制御部 50 a は、処理をステップ S 5 0 1 に戻し、次のコマンド受信を待つ。

【 0 0 9 7 】

ステップ S 5 1 4 において、制御部 50 a の回数情報処理部 55 は、初期 P I N 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、R A M 7 内に、上述した初期 P I N 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 P I N 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 P I N の照合成功である場合（ステップ S 5 1 4 : Y E S ）に、処理をステップ S 5 1 5 に進める。また、回数情報処理部 55 は、初期 P I N の照合成功でない場合（ステップ S 5 1 4 : N O ）に、処理をステップ S 5 1 6 に進める。

10

【 0 0 9 8 】

ステップ S 5 1 5 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 8 4 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 S 5 1 5 の処理後に、制御部 50 a は、処理をステップ S 5 0 1 に戻し、次のコマンド受信を待つ。

【 0 0 9 9 】

ステップ S 5 1 6 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 P I N 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 S 5 1 6 の処理後に、制御部 50 a は、処理をステップ S 5 0 1 に戻し、次のコマンド受信を待つ。

20

【 0 1 0 0 】

次に、図 1 1 を参照して、本実施形態による I C カード 1 a の回数情報の出力処理について説明する。

図 1 1 は、本実施形態の I C カード 1 a の回数情報の出力処理の一例を示す図である。

この図において、I C カード 1 a は、「初期 P I N」（P I N の初期値）が“ 0 0 1 5 ”、「P I N」（記憶 P I N）が“ 0 0 2 0 ”、「P A R」（加算値）が“ 0 0 0 5 ”、「回数」（回数情報）が“ 0 1 ”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。

30

【 0 1 0 1 】

図 1 1 において、カードホルダー U 1 が、外部装置 2 において、P I N 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 U 1 に対して、初期 P I N 入力要求を出力する（ステップ S 6 0 1）。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 U 1 に初期 P I N の入力を促す表示を出力する。

【 0 1 0 2 】

次に、カードホルダー U 1 によって、外部装置 2 に初期 P I N（例えば、“ 0 0 1 5 ”）が入力されると（ステップ S 6 0 2）、外部装置 2 は、I C カード 1 a に対して、初期 P I N 照合要求を送信する（ステップ S 6 0 3）。すなわち、外部装置 2 は、取得 P I N として、例えば、“ 0 0 1 5 ”を含む初期 P I N 照合のコマンドを、I C カード 1 a に対して送信する。

40

【 0 1 0 3 】

次に、I C カード 1 a は、初期 P I N 照合のコマンドに応じて、初期 P I N 照合処理（例えば、“ 0 0 1 5 ”の照合）を実行する（ステップ S 6 0 4）。I C カード 1 a の認証部 5 2 a は、例えば、取得 P I N である“ 0 0 1 5 ”と、P I N 初期値記憶領域 8 3 が記憶する“ 0 0 1 5 ”とを照合する。なお、ここでは、認証部 5 2 a は、取得 P I N である“ 0 0 1 5 ”と、P I N 初期値記憶領域 8 3 が記憶する“ 0 0 1 5 ”とが一致するので、照合成功と判定する。

【 0 1 0 4 】

次に、I C カード 1 a は、初期 P I N 照合結果を外部装置 2 に送信する（ステップ S 6

50

05)。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。

【0105】

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。

【0106】

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。

【0107】

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。

【0108】

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。

【0109】

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

10

20

30

40

50

定された場合に、認証用 P I N の初期化要求（例えば、初期化コマンド）に応じて、E E P R O M 8 a が記憶する記憶 P I N を、認証用 P I N の初期値に変更する。さらに、初期化処理部 5 4 a は、認証用 P I N の初期化要求に応じて、E E P R O M 8 a 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 I C カード 1 a 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 P I N 及び回数情報を初期値に戻すことができる。

【 0 1 1 0 】

（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 I C カード 1 b 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 P I N であって、記憶 P I N として E E P R O M 8 a に記憶されている認証 P I N 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 P I N の初期値とに基づいて毎回生成した認証 P I N 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 I C カード 1 b 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。

【 0 1 1 1 】

図 1 2 は、本実施形態の I C カード 1 b の機能構成例を示すブロック図である。

この図に示すように、I C カード 1 b は、E E P R O M 8 b と、通信部 4 0 と、制御部 5 0 b とを備えている。E E P R O M 8 b は、P I N 記憶領域 8 1 と、パラメータ記憶領域 8 2 と、回数情報記憶領域 8 4 とを備えている。また、制御部 5 0 b は、P I N 生成部 5 1 b と、認証部 5 2 b と、初期化処理部 5 4 b と、回数情報処理部 5 5 とを備えている。

ここで、図 1 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。

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。

【 0 1 1 2 】

本実施形態の E E P R O M 8 b は、P I N 初期値記憶領域 8 3 を備えない代わりに、P I N 記憶領域 8 1 が、認証用 P I N の初期値を記憶する。

認証部 5 2 b は、第 1 の認証処理と、第 2 の認証処理とを実行する。P I N 生成部 5 1 b は、第 1 の認証処理において、取得 P I N と、P I N 生成部 5 1 b が毎回生成する認証用 P I N 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、P I N 生成部 5 1 b 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 P I N（第 4 のパスワード）と、P I N 記憶領域 8 1 が記憶する認証用 P I N 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。

【 0 1 1 3 】

P I N 生成部 5 1 b は、P I N 記憶領域 8 1 が記憶する認証用 P I N の初期値と、パラメータ記憶領域 8 2 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 8 4 が記憶する回数情報とに基づいて、認証用 P I N を生成する。また、P I N 生成部 5 1 b は、認証部 5 2 b 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 8 4 が記憶する回数情報を更新する。なお、P I N 生成部 5 1 b は、認証部 5 2 b が第 1 の認証処理を実行するごとに毎回、認証用 P I N 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 P I N を生成する。

【 0 1 1 4 】

初期化処理部 5 4 b は、認証部 5 2 b 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、E E P R O M 8 b（回数情報記憶領域 8 4）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 5 4 b は、回数情報記憶領域 8 4 が記憶する回数情報として、例えば、“ 0 ” を記憶させる。

10

20

30

40

50

【 0 1 1 5 】

次に、図 1 3 を参照して、本実施形態による IC カード 1 b の動作の一例について説明する。

図 1 3 は、本実施形態の IC カード 1 b の動作の一例を示すフローチャートである。

この図において、ステップ S 7 0 1 及びステップ S 7 0 2 の処理は、図 1 0 に示すステップ S 5 0 1 及びステップ S 5 0 2 の処理と同様であるので、ここではその説明を省略する。

【 0 1 1 6 】

なお、ステップ S 7 0 2 のコマンド分岐の処理において、制御部 5 0 b は、受信したコマンドが P I N を照合するコマンドである場合 (P I N 照合) に、処理をステップ S 7 0 3 に進める。また、制御部 5 0 b 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 S 7 0 8 に進める。また、制御部 5 0 b は、受信したコマンドが P I N の初期値を照合するコマンドである場合 (初期 P I N 照合) に、処理をステップ S 7 1 1 に進める。また、制御部 5 0 b 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 S 7 1 3 に進める。

10

【 0 1 1 7 】

ステップ S 7 0 3 において、制御部 5 0 b の P I N 生成部 5 1 b は、回数情報に基づいて、認証用 P I N 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、P I N 生成部 5 1 b は、下記の式 (1) により、認証用 P I N を生成する。

20

【 0 1 1 8 】

認証用 P I N = 認証用 P I N の初期値 + 加算値 × 回数情報の値 . . . (1)

【 0 1 1 9 】

次に、制御部 5 0 b の認証部 5 2 b は、第 1 の認証処理として、取得 P I N と、P I N 生成部 5 1 b が生成した認証用 P I N とを照合する (ステップ S 7 0 4) 。

次に、制御部 5 0 b の認証部 5 2 b 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 S 7 0 5) 。認証部 5 2 b は、照合成功である場合 (ステップ S 7 0 5 : Y E S) に、例えば、RAM 7 内に、照合成功を示す情報を記憶させて、処理をステップ S 7 0 6 に進める。また、認証部 5 2 b は、照合失敗である場合 (ステップ S 7 0 5 : N O) に、処理をステップ S 7 0 7 に進める。なお、認証部 5 2 b 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 5 2 b 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 E E P R O M 8 b 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タ値に達した場合に、認証用 P I N による照合処理の実行を禁止してもよい。

30

【 0 1 2 0 】

ステップ S 7 0 6 において、P I N 生成部 5 1 b 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、P I N 生成部 5 1 b は、回数情報記憶領域 8 4 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 8 4 に記憶させる。

次のステップ S 7 0 7 の処理は、図 1 0 に示すステップ S 5 0 7 の処理と同様であるので、ここではその説明を省略する。

40

【 0 1 2 1 】

また、ステップ S 7 0 8 からステップ S 7 1 0 までの処理は、図 1 0 に示すステップ S 5 0 8 からステップ S 5 1 1 までの処理からステップ S 5 0 9 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 5 4 b は、認証用 P I N の初期化を行う必要がなく、ステップ S 7 0 9 において、回数情報の初期化を行う。

また、ステップ S 7 1 0 において、制御部 5 0 b は、P I N 初期化結果の代わりに、回数情報の初期化結果を、通信部 4 0 に送信させる。

【 0 1 2 2 】

50

また、ステップS 7 1 1からステップS 7 1 5までの処理は、図10に示すステップS 5 1 2からステップS 5 1 6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。

【0123】

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。

10

【0124】

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S 8 0 1）。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。

【0125】

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S 8 0 2）、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S 8 0 3）。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。

20

【0126】

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S 8 0 4）。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。

【0127】

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S 8 0 5）。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。

30

【0128】

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S 8 0 6）。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。

【0129】

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S 8 0 7）。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。

40

【0130】

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PI

50

N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。P I N生成部51bは、認証用P I N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、E E P R O M 8 bが記憶する回数情報とに基づいて、認証用P I Nを生成する。また、P I N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、E E P R O M 8 b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I Cカード1bは、認証用P I N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。

【0131】

また、本実施形態では、I C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I C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P I N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P I Nを生成することができる。

【0132】

また、本実施形態では、I C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、E E P R O M 8 b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I C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P I Nを初期値に戻すことができる。

【0133】

（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I Cカード1cについて説明する。

本実施形態は、認証用P I N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I C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。

【0134】

図15は、本実施形態のI Cカード1cの機能構成例を示すブロック図である。

この図に示すように、I Cカード1cは、E E P R O M 8 cと、通信部40と、制御部50cとを備えている。E E P R O M 8 cは、P I N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、P I N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。

【0135】

P I N記憶領域81は、上述した第3の実施形態と同様に、認証用P I N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P I N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、I C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。

【0136】

P I N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P I Nの初期値とに基づいて、認証用P I Nを生成する。P I N生成部51cは、例えば、認証用P I N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P I Nを

10

20

30

40

50

生成する。

【0137】

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。

【0138】

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。

【0139】

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。

【0140】

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。

【0141】

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。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。

【0142】

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。

【0143】

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。

【0144】

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

10

20

30

40

50

ド受信を待つ。

【0145】

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“Y₁Y₂Y₃Y₄M₁M₂D₁D₂”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。

【0146】

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。

【0147】

カードホルダーU1は、「取引日付」が“Y₁Y₂Y₃Y₄M₁M₂D₁D₂”であるので、例えば、この「取引日付」の最下位1桁の“D₂”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、“001D₂”）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、“002D₂”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。

【0148】

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“D₂”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“D₂”とを置換処理して、認証用PINとして“001D₂”を生成する。

【0149】

次に、ICカード1cは、PIN照合処理（例えば、“001D₂”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“001D₂”と、生成した認証用PIN“001D₂”とを照合する。なお、ここでは、認証部52cは、取得PINである“001D₂”と、生成した認証用PIN“001D₂”とが一致するので、照合成功と判定する。

【0150】

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。

【0151】

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。

10

20

30

40

50

【 0 1 5 2 】

以上説明したように、本実施形態による IC カード 1 c 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 5 1 c 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 1 c 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。

【 0 1 5 3 】

また、本実施形態では、EEPROM 8 c 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 1 c は、さらに、認証部 5 2 c 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、EEPROM 8 c が記憶する置換処理情報を変更する置換情報変更部 5 6 を備える。

これにより、本実施形態による IC カード 1 c 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 1 c は、よりセキュリティを向上させることができる。

【 0 1 5 4 】

(第 5 の実施形態)

次に、図 1 8 を参照して、第 5 の実施形態による IC カード 1 d について説明する。

本実施形態は、IC カード 1 d 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 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 1 d 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。

【 0 1 5 5 】

図 1 8 は、本実施形態の IC カード 1 d の機能構成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 1 d は、EEPROM 8 d と、通信部 4 0 と、制御部 5 0 d とを備えている。EEPROM 8 d は、PIN 記憶領域 8 1 と、パラメータ記憶領域 8 2 と、PIN 初期値記憶領域 8 3 と、選択情報記憶領域 8 6 とを備えている。また、制御部 5 0 d は、PIN 生成部 5 1 d と、認証部 5 2 と、置換情報変更部 5 6 とを備えている。

ここで、図 1 8 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。

【 0 1 5 6 】

選択情報記憶領域 8 6 は、種類の異なる複数の所定のアルゴリズムのうち 1 つを選択する選択情報を記憶する。選択情報記憶領域 8 6 は、例えば、所定のアルゴリズムが加算処理である場合に“0 1”を記憶し、所定のアルゴリズムが減算処理である場合に“0 2”を記憶し、所定のアルゴリズムが置換処理である場合に“0 3”を記憶する。

なお、本実施形態のパラメータ記憶領域 8 2 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。

【 0 1 5 7 】

PIN 生成部 5 1 d は、EEPROM 8 d (選択情報記憶領域 8 6) 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 8 6 が記憶する選択情報が“0 1”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。

【 0 1 5 8 】

以上説明したように、本実施形態による IC カード 1 d では、EEPROM 8 d は、種

10

20

30

40

50

類の異なる複数の所定のアルゴリズムのうちの一つを選択する選択情報を記憶する。そして、P I N生成部5 1 dは、E E P R O M 8 d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一つを選択し、選択した当該所定のアルゴリズムに基づいて、認証用P I N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P I N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I Cカード1 dは、認証用P I N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I Cカード1 dは、よりセキュリティを向上させることができる。

【0159】

なお、本実施形態では、I Cカード1 dは、認証部5 2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、E E P R O M 8 d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。

10

これにより、定期的に、所定のアルゴリズムを変更することができるので、本実施形態によるI Cカード1 dは、さらにセキュリティを向上させることができる。

【0160】

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る実施してもよい。

また、上記の各実施形態において、I Cカード1(1 a~1 d)は、書き換え可能な不揮発性メモリとして、E E P R O M 8(8 a~8 d)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、I Cカード1(1 a)は、E E P R O M 8(8 a~8 d)の代わりに、フラッシュE E P R O M、F e R A M(Ferroelectric Random Access Memory: 強誘電体メモリ)などを備えてもよい。

20

また、上記の各実施形態において、I Cカード1(1 a~1 d)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。

【0161】

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E E P R O M 8(8 a~8 d)に記憶されている記憶P I N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P I Nを生成するP I N生成部5 1(5 1 a~5 1 d)と、外部装置2から取得した取得P I Nと、認証用P I N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5 2(5 2 a~5 2 c)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。

30

【0162】

なお、実施形態におけるI Cカード1(1 a~1 d)及び認証センタ装置2 0 0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I Cカード1(1 a~1 d)及び認証センタ装置2 0 0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、O Sや周辺機器等のハードウェアを含むものとする。

40

また、「コンピュータシステム」は、インターネットやW A N、L A N、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、R O M、C D - R O M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、C D - R O M等の非一過性の記録媒体であってもよい。

【0163】

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

50

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。

10

【0164】

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】

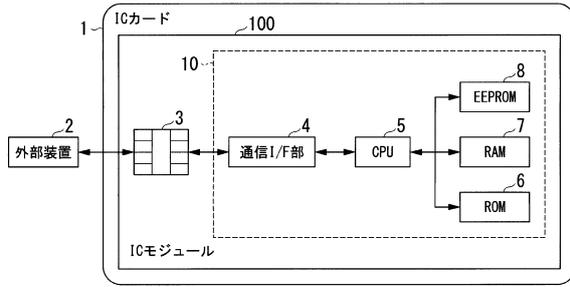
【0165】

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

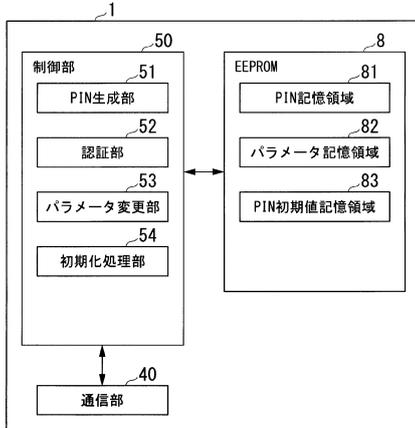
20

30

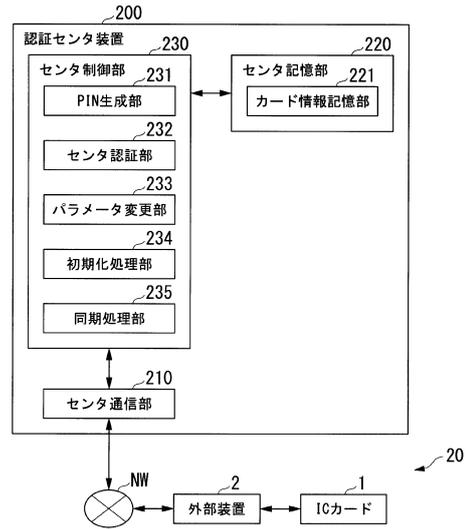
【図1】



【図2】



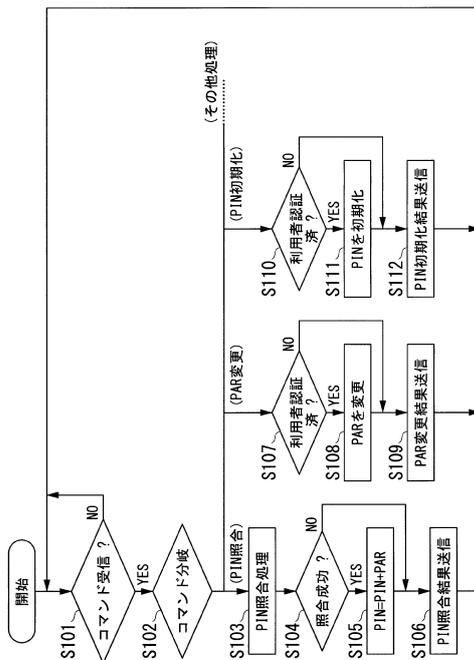
【図3】



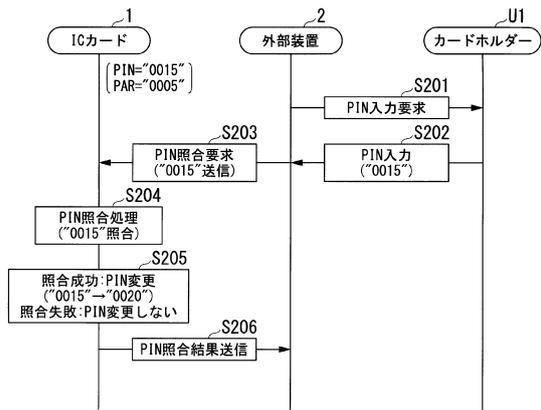
【図4】

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

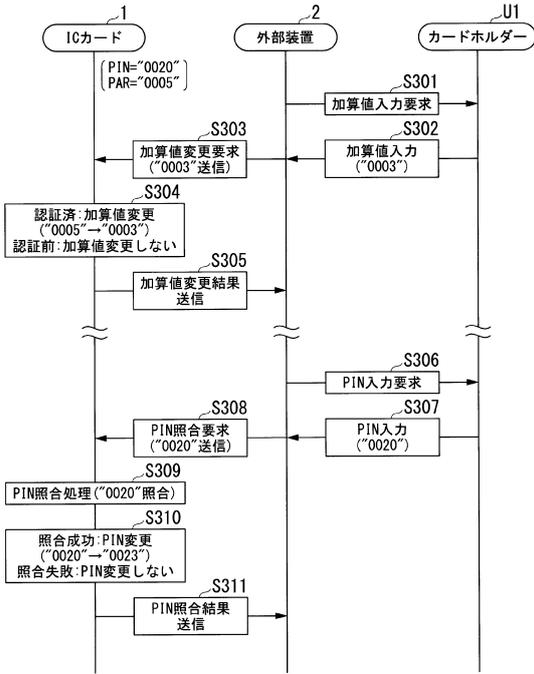
【図5】



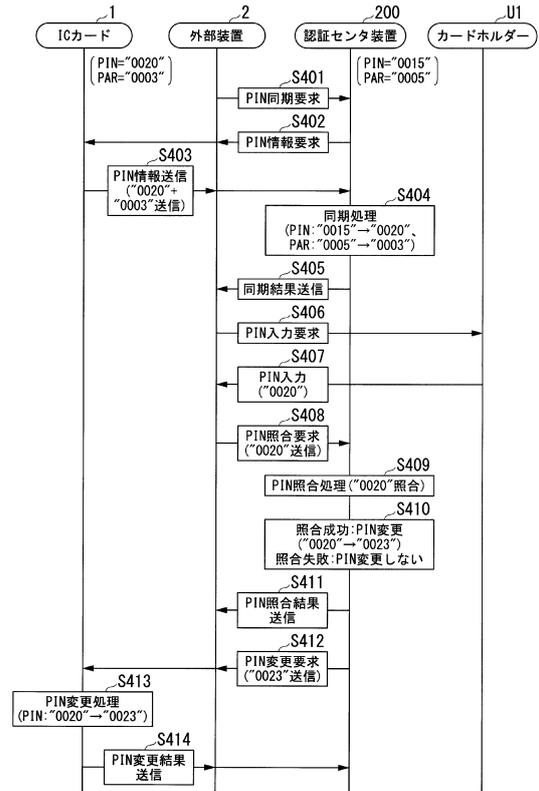
【図6】



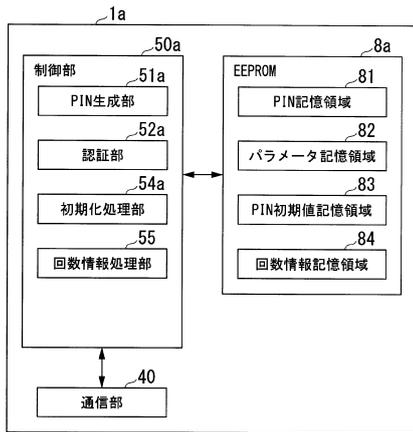
【図7】



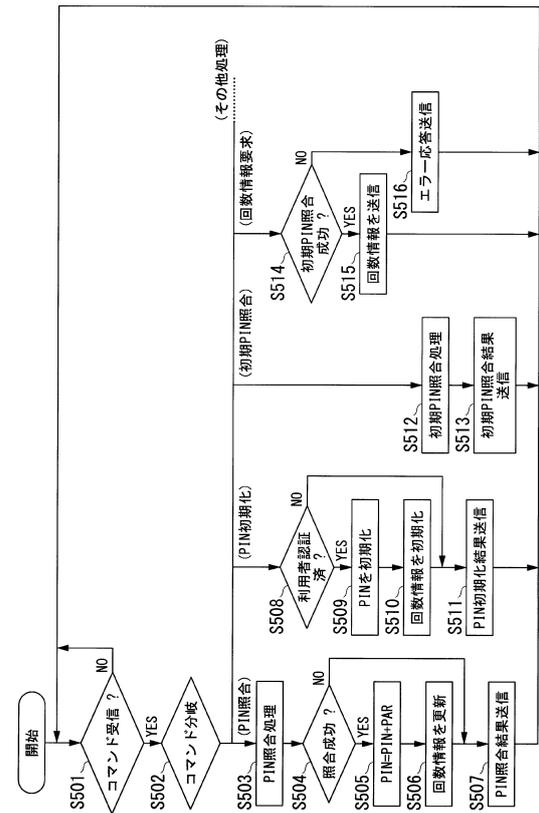
【図8】



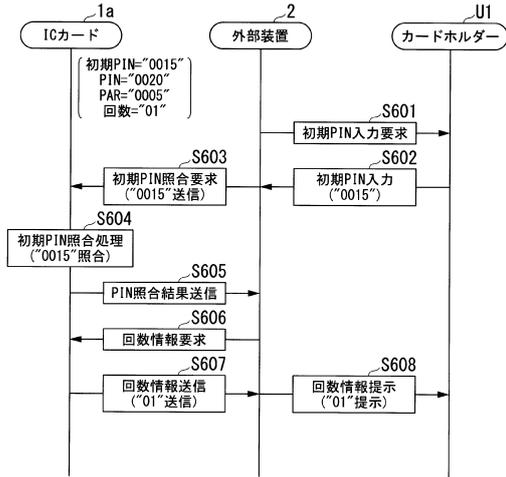
【図9】



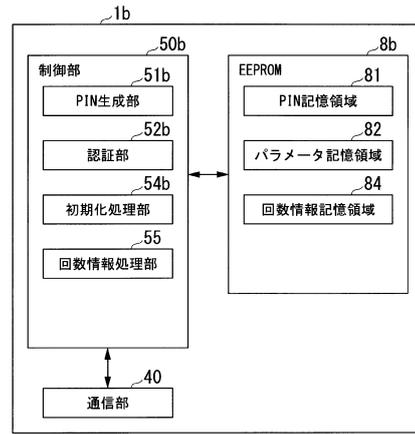
【図10】



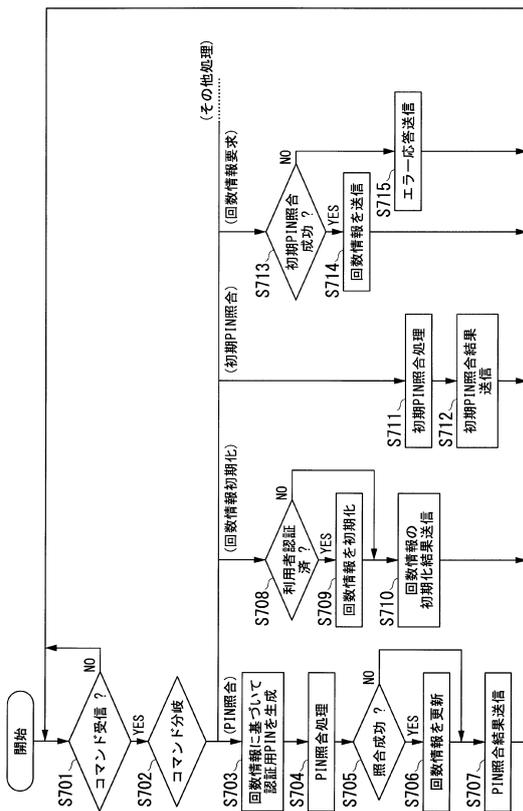
【図11】



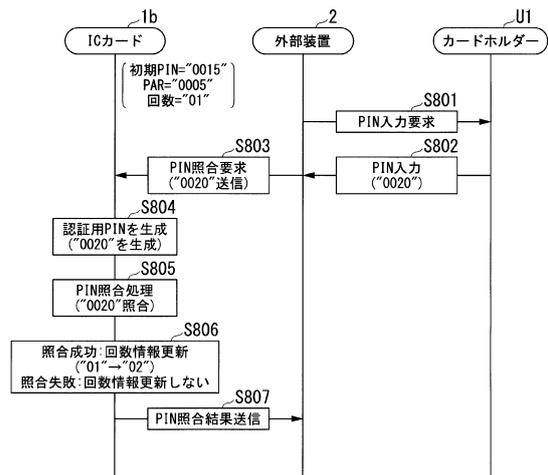
【図12】



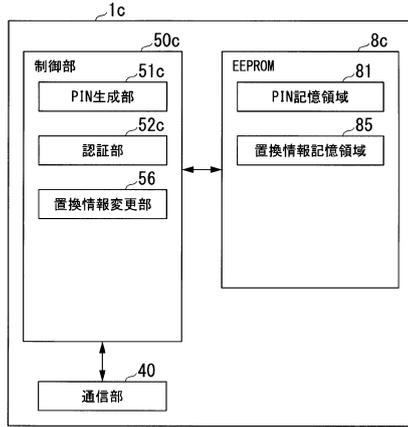
【図13】



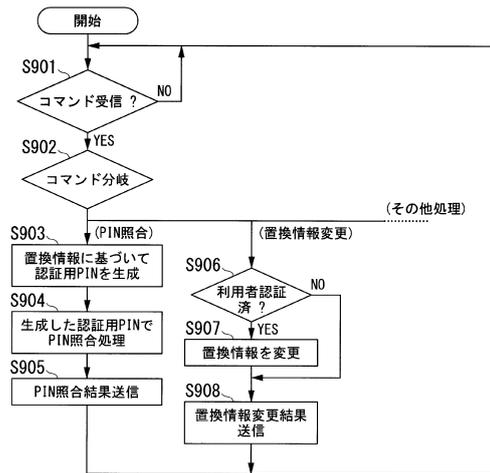
【図14】



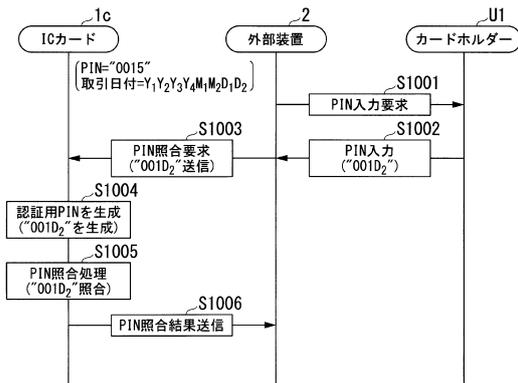
【図15】



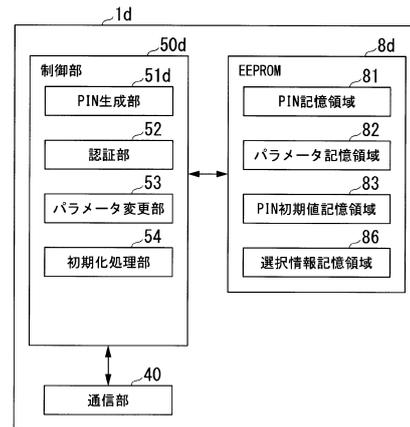
【図16】



【図17】



【図18】



フロントページの続き

- (56)参考文献 特開2005-085071(JP,A)
特開2005-078165(JP,A)
特開2003-091712(JP,A)
米国特許出願公開第2004/0249503(US,A1)

- (58)調査した分野(Int.Cl., DB名)
G06F 21/34
G06K 19/073