(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-14607
(P2012-14607A)
(43)公開日　平成24年1月19日(2012.1.19)

(51)Int.Cl.		F I		テーマコード（参考）
G06K 17/00	(2006.01)	G06K 17/00	F	5B017
G06K 19/07	(2006.01)	G06K 17/00	B	5B035
G06K 19/10	(2006.01)	G06K 17/00	T	5B058
G06F 21/24	(2006.01)	G06K 19/00	J	5K012
H04B 5/02	(2006.01)	G06K 19/00	R	

審査請求 未請求　請求項の数 6　ＯＬ　（全 16 頁）　最終頁に続く

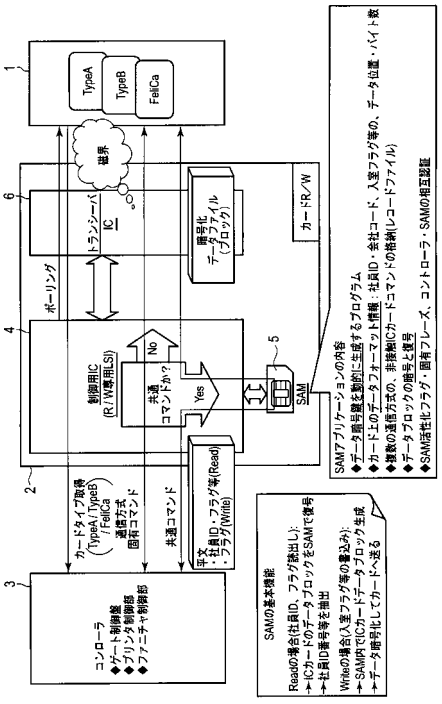
(21)出願番号　特願2010-152725 (P2010-152725)
(22)出願日　平成22年7月5日 (2010.7.5)

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号
(74)代理人　100111659
弁理士　金山　聡
(74)代理人　100135954
弁理士　深町　圭子
(74)代理人　100119057
弁理士　伊藤　英生
(74)代理人　100122529
弁理士　藤枡　裕実
(74)代理人　100131369
弁理士　後藤　直樹
(74)代理人　100164987
弁理士　伊藤　裕介

最終頁に続く

(54)【発明の名称】ＩＣカードリーダライタおよびそれに内蔵するＳＡＭ

(57)【要約】
【課題】　一台のＩＣカードリーダライタでデータフォーマットや通信方式の異なるＩＣカードの読み書きができ、しかも情報漏洩等に対するセキュリティ性が高く、仕様等の変更要求への対応を容易とする。
【解決手段】　複数の通信方式の非接触ＩＣカードへの読み書きが可能なＩＣカードリーダライタの中に、着脱可能なＳＡＭを内蔵し、そのＳＡＭの中に、ＩＣカードリーダーが読み書きする非接触ＩＣカードのデータフォーマット情報として、すくなくとも非接触ＩＣカードのメモリに設定されるデータブロックの名称、およびそのデータブロックに記憶するデータの項目とバイト数、データ項目の配列順の情報を格納する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ＩＣカードの読み書きにおけるデータ処理を行う制御部と、その制御部に対して着脱が可能かつ装着時にその制御部とのデータ通信が可能なＳＡＭを有するＩＣカードリーダライタであって、
前記制御部は、
前記データ処理の対象となるＩＣカードの通信方式を特定する通信方式特定手段と、
前記通信方式に適合するように必要に応じてコマンドとデータフォーマットの変換要求を前記ＳＡＭに対して行うデータ変換要求手段とを有し、
前記ＳＡＭは、
前記ＩＣカードの各々におけるメモリのデータフォーマット情報と、前記制御部において処理可能な共通コマンドと前記通信方式の異なるＩＣカードの各々において処理可能な固有コマンドとを対応させたコマンドリスト情報とを格納する固有情報メモリと、
前記変換要求を受付けて、前記固有情報メモリのデータフォーマット情報と前記コマンドリスト情報を参照し、コマンドとデータフォーマットの変換を行なうデータ変換応答手段とを有する、
ことを特徴とするＩＣカードリーダライタ。
【請求項２】
請求項１に記載のＩＣカードリーダライタであって、前記データフォーマットの情報は、すくなくともメモリに設定されるデータブロックの名称、およびそのデータブロックを構成するデータの項目とバイト数、その項目の配列順の情報であることを特徴とするＩＣカードリーダライタ。
【請求項３】
請求項１または２に記載のＩＣカードリーダライタであって、
前記制御部が前記データ処理を行うときの前記ＩＣカードに対するコマンドが共通コマンドであるときには、
前記制御部のデータ変換要求手段は、前記制御部の通信方式特定手段が特定した前記ＩＣカードの通信方式と、前記データ処理を実行する前記共通コマンドとその付加データとからなる変換要求データを前記ＳＡＭのデータ変換応答手段に送信することによって変換要求を行い、
前記ＳＡＭのデータ変換応答手段は、前記変換要求データの前記共通コマンドに対応する固有コマンドを前記ＳＡＭの固有情報メモリが格納するコマンドリスト情報から選択するとともに、前記共通コマンドの付加データと内容が同一でかつ前記ＩＣカードのデータフォーマットに形式が適合する付加データを前記固有情報メモリのデータフォーマット情報に基づいて生成し、さらにその生成した付加データを前記選択した固有コマンドに付加することによって変換応答データを生成し、その変換応答データを前記制御部に返信し、
前記制御部は、前記ＳＡＭから返信された変換応答データを、前記ＩＣカードの固有コマンドとして前記ＩＣカードへ送信する、
ことを特徴とするＩＣカードリーダライタ。
【請求項４】
請求項１～３のいずれかに記載のＩＣカードリーダライタに装着されるＳＡＭにおいて、前記ＩＣカードのメモリは暗号化したデータブロックを記憶するメモリであって、
前記制御部が前記ＩＣカードからリードコマンドにより読み取る暗号化データブロックを復号化して復号化データブロックを得る復号化手段と、
前記復号化データブロックを構成する項目の各々のデータを、前記データフォーマットの情報を参照して抽出するデータ抽出手段と、
前記抽出された項目の各々のデータを前記制御部において処理可能な所定の順番に配列したデータ列を編成するデータ再配列手段と、
を有することを特徴とするＳＡＭ。
【請求項５】

請求項４に記載のＳＡＭにおいて、前記制御部が前記ＩＣカードにライトコマンドにより書き込むデータブロックを暗号化して暗号化データブロックを得る暗号化手段を有することを特徴とするＳＡＭ。
【請求項６】
請求項４または５に記載のＳＡＭにおいて、前記ＳＡＭは活性化フラグを有し、その活性化フラグの値によって非活性化状態または活性化状態のいずれかの状態であって、
前記制御部は活性化指令手段を有し、その活性化指令手段は前記ＳＡＭから読み出した活性化フラグの値が非活性化状態であるときに、前記ＩＣカードリーダライタに固有のキーフレーズを付加データとして活性化コマンドをＳＡＭに送信し、
前記ＳＡＭは活性化遷移手段を有し、その活性化遷移手段は前記ＳＡＭのメモリに前記キーフレーズを書き込むとともに前記ＳＡＭの中の活性化フラグを活性化状態に遷移し、
前記制御部はキーフレーズ送信手段を有し、そのキーフレーズ送信手段は前記ＳＡＭから読み出した活性化フラグの値が活性化状態であるときに、前記キーフレーズを前記ＳＡＭに送信し、
前記ＳＡＭはキーフレーズ管理手段を有し、そのキーフレーズ管理手段は前記キーフレーズ送信手段から受信したキーフレーズと、前記ＳＡＭのメモリに書き込まれているキーフレーズとが一致するときにだけ前記ＳＡＭが前記制御部のコマンドを受付けるようにする、
ことを特徴とするＳＡＭ。
【発明の詳細な説明】
【技術分野】
【０００１】
ＩＣカードリーダライタとＩＣカードの技術分野に属する。特に、一台のＩＣカードリーダライタでデータフォーマットや通信方式の異なるＩＣカードの読み書きができるようにしたＩＣカードリーダライタおよびそれに内蔵するＳＡＭ（Secure Application Module）に関する。
【背景技術】
【０００２】
磁気カードなどのＩＤカードの記録部に書かれる会社名などの特定データについては、そのデータの記録場所や記録内容がデータフォーマットとして規定されている。このデータフォーマットは、カード発行者により様々である。したがって、一つのカード端末装置（コントローラ付カードリーダライタ）でデータフォーマットが異なるカードを取り扱えるようにするために、カード選択ボタンを押してカード種別を選択するなどの方法が採用されている。この方法においては、人手による手間がかかり、またカード利用者または係員が自身のカードの種別を記憶する必要があるため極めて操作が煩雑となるという問題があった（特許文献１）。
一方、非接触ＩＣカードには複数の通信方式が存在する。一台のカードリーダライタで複数の通信方式のＩＣカードの読み書きができるようにするためには、たとえば、通信方式ごとのＩＣカード検出信号を順番に送出し、カードからの応答信号が適正であるか否かによりＩＣカードの通信方式を特定することが行なわれる。通信方式が特定されると、以後、その通信方式に固定してＩＣカードの読み書き処理を行う技術が存在する（特許文献２）。しかし、通信方式が異なるカードでは、カードにデータを読み書きするためのコマンド体系が異なっている。そのため、上記のような仕組みを実現するためには、カードリーダライタの上位のコントローラは、各々の通信方式に対応したコマンドを保持して、通信方式に応じたコマンドを、カードリーダライタを通じてＩＣカードに送出しなければならないという問題があった。
【０００３】
上記のようなコントローラの負担を軽減するために、コントローラとカードリーダライタ間のコマンドとしては、コントローラとカードリーダライタで処理可能な共通形式のコマンド（共通コマンド）に一本化することが行なわれる。そして、カードリーダライタは

コントローラから送信された共通コマンドを特定された非接触ＩＣカードの通信方式にしたがって、カードリーダライタと非接触ＩＣカードで処理可能な固有形式のコマンド（固有コマンド）に変換する。さらに、カードリーダライタはＩＣカードから返信されるレスポンスについても、固有形式から共通形式に変換してコントローラに返信するという方法が考えられる。

しかし、この場合、カードリーダライタが、固有コマンドと共通コマンドとの変換を行うためには、通信方式によって異なるコマンド情報を保持する必要があり、リーダライタにおける処理負荷が大きくなるという問題がある。

更に、上記変換の際に、カード上のデータフォーマット（データの区切りなど）を知る必要がある場合があるが、カードのデータフォーマットは、本来、カードの発行者が極力秘匿したい情報であるため、このような共通コマンドで動作するカードリーダライタは、実際にはほとんど開発されていない。

【０００４】

また、ＩＣカード内で、データを暗号化して保管することは一般的に広く実施されているが（特許文献３）、複数の通信方式もしくは複数のデータフォーマットによって異なる暗号方式を、一つのカードリーダライタのＲＯＭなどに実装することは、情報漏洩の危険があり、ほとんど行われていない。

一方、暗号アルゴリズムや暗号鍵などを、耐タンパー性のある、セキュアアプリケーションモジュール（ＳＡＭ）に実装して、このＳＡＭをカードリーダライタやコントローラに装着して、外部プログラムがＳＡＭにアクセスして暗号計算を行わせたり、重要なファイルをＳＡＭに格納させることが行われている。

なお、ＳＡＭ内での暗号処理については特許文献４に、ＳＡＭ内に装置のコマンドを格納する技術については特許文献５に、それぞれ開示されている。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開平８－１３８００３

【特許文献２】特開２００１－３１２７０１

【特許文献３】特開２００３－２９６６９１

【特許文献４】特開２００４－２４６５６３

【特許文献５】特開２００８－１３４８８１

【発明の概要】

【発明が解決しようとする課題】

【０００６】

本発明は上記の問題を解決するために成されたものである。その目的は、一台のＩＣカードリーダライタでデータフォーマットや通信方式の異なるＩＣカードの読み書きができしかも情報漏洩等に対するセキュリティ性が高く、仕様等の変更要求への対応が容易なＩＣカードリーダライタとそれに内蔵するＳＡＭを提供することにある。

【課題を解決するための手段】

【０００７】

本発明の請求項１に係るＩＣカードリーダライタは、　ＩＣカードの読み書きにおけるデータ処理を行う制御部と、その制御部に対して着脱が可能かつ装着時にその制御部とのデータ通信が可能なＳＡＭを有するＩＣカードリーダライタであって、　前記制御部は、前記データ処理の対象となるＩＣカードの通信方式を特定する通信方式特定手段と、前記通信方式に適合するように必要に応じてコマンドとデータフォーマットの変換要求を前記ＳＡＭに対して行うデータ変換要求手段とを有し、　前記ＳＡＭは、　前記ＩＣカードの各々におけるメモリのデータフォーマット情報と、前記制御部において処理可能な共通コマンドと前記通信方式の異なるＩＣカードの各々において処理可能な固有コマンドとを対応させたコマンドリスト情報とを格納する固有情報メモリと、前記変換要求を受付けて、前記固有情報メモリのデータフォーマット情報と前記コマンドリスト情報を参照し、コマ

ンドとデータフォーマットの変換を行なうデータ変換応答手段とを有するようにしたものである。

また本発明の請求項２に係るＩＣカードリーダライタは、請求項１に係るＩＣカードリーダライタであって、前記データフォーマットの情報は、すくなくともメモリに設定されるデータブロックの名称、およびそのデータブロックを構成するデータの項目とバイト数、その項目の配列順の情報であるようにしたものである。

また、本発明の請求項３に係るＩＣカードリーダライタは、請求項１または２に係るＩＣカードリーダライタであって、前記制御部が前記データ処理を行うときの前記ＩＣカードに対するコマンドが共通コマンドであるときには、 前記制御部のデータ変換要求手段は、前記制御部の通信方式特定手段が特定した前記ＩＣカードの通信方式と、前記データ処理を実行する前記共通コマンドとその付加データとからなる変換要求データを前記ＳＡＭのデータ変換応答手段に送信することによって変換要求を行い、 前記ＳＡＭのデータ変換応答手段は、前記変換要求データの前記共通コマンドに対応する固有コマンドを前記ＳＡＭの固有情報メモリが格納するコマンドリスト情報から選択するとともに、前記共通コマンドの付加データと内容が同一でかつ前記ＩＣカードのデータフォーマットに形式が適合する付加データを前記固有情報メモリのデータフォーマット情報に基づいて生成し、さらにその生成した付加データを前記選択した固有コマンドに付加することによって変換応答データを生成し、その変換応答データを前記制御部に返信し、 前記制御部は、前記ＳＡＭから返信された変換応答データを、前記ＩＣカードの固有コマンドとして前記ＩＣカードへ送信するようにしたものである。

また、本発明の請求項４に係るＳＡＭは、請求項１～３のいずれかに係るＩＣカードリーダライタに装着されるＳＡＭにおいて、前記ＩＣカードのメモリは暗号化したデータブロックを記憶するメモリであって、 前記制御部が前記ＩＣカードからリードコマンドにより読み取る暗号化データブロックを復号化して復号化データブロックを得る復号化手段と、 前記復号化データブロックを構成する項目の各々のデータを、前記データフォーマットの情報を参照して抽出するデータ抽出手段と、 前記抽出された項目の各々のデータを前記制御部において処理可能な所定の順番に配列したデータ列を編成するデータ再配列手段とを有するようにしたものである。

また、本発明の請求項５に係るＳＡＭは、請求項４に係るＳＡＭにおいて、前記制御部が前記ＩＣカードにライトコマンドにより書き込むデータブロックを暗号化して暗号化データブロックを得る暗号化手段を有するようにしたものである。

また、本発明の請求項６に係るＳＡＭは、請求項４または５に係るＳＡＭにおいて、前記ＳＡＭは活性化フラグを有し、その活性化フラグの値によって非活性化状態または活性化状態のいずれかの状態であって、 前記制御部は活性化指令手段を有し、その活性化指令手段は前記ＳＡＭから読み出した活性化フラグの値が非活性化状態であるときに、前記ＩＣカードリーダライタに固有のキーフレーズを付加データとして活性化コマンドをＳＡＭに送信し、 前記ＳＡＭは活性化遷移手段を有し、その活性化遷移手段は前記ＳＡＭのメモリに前記キーフレーズを書き込むとともに前記ＳＡＭの中の活性化フラグを活性化状態に遷移し、 前記制御部はキーフレーズ送信手段を有し、そのキーフレーズ送信手段は前記ＳＡＭから読み出した活性化フラグの値が活性化状態であるときに、前記キーフレーズを前記ＳＡＭに送信し、 前記ＳＡＭはキーフレーズ管理手段を有し、そのキーフレーズ管理手段は前記キーフレーズ送信手段から受信したキーフレーズと、前記ＳＡＭのメモリに書き込まれているキーフレーズとが一致するときにだけ前記ＳＡＭが前記制御部のコマンドを受付けるようにしたものである。

【発明の効果】

【０００８】

本発明によれば、一台のＩＣカードリーダライタでデータフォーマットや通信方式の異なるＩＣカードの読み書きができ、しかも情報漏洩等に対するセキュリティ性が高く、仕様等の変更要求への対応が容易なＩＣカードリーダライタおよびそれに内蔵するＳＡＭ（Secure Application Module）が提供される。

【図面の簡単な説明】
【０００９】
【図１】本発明のＩＣカードリーダライタおよびＳＡＭにおける構成の一例を示す説明図である。
【図２】本発明のＩＣカードリーダライタおよびＳＡＭにおける構成の一例を示すブロック図である。
【図３】本発明のＩＣカードリーダライタおよびＳＡＭにおける固有コマンドをＩＣカードリーダライタが受信したときの動作の過程を示すフロー図である。
【図４】本発明のＩＣカードリーダライタおよびＳＡＭにおける共通コマンド（リード）をＩＣカードリーダライタが受信したときの動作の過程を示すフロー図である。
【図５】本発明のＩＣカードリーダライタおよびＳＡＭにおける共通コマンド（ライト）をＩＣカードリーダライタが受信したときの動作の過程を示すフロー図である。
【発明を実施するための形態】
【００１０】
次に、本発明の実施の形態について図を参照しながら説明する。本発明のＩＣカードリーダライタおよびＳＡＭにおける構成の一例を説明図として図１に、ブロック図として図２に示す。図１、図２において、１はＩＣカード、２はＩＣカードリーダライタ、３はコントローラ、４は制御部（制御用ＩＣ：Ｒ／Ｗ専用ＬＳＩ）、５はＳＡＭ（Secure Application Module）、６は通信部（トランシーバＩＣ）である。図２において、４１は通信方式特定手段、４２はデータ変換要求手段、４３は活性化指令手段、４４はキーフレーズ送信手段、５１は固有情報メモリ、５２は活性化フラッグ、５３はキーフレーズ、５０１はデータ変換応答手段、５０２は復号化手段、５０３はデータ抽出手段、５０４はデータ配列手段、５０５は暗号化手段、５０６は活性化遷移手段、５０７はキーフレーズ管理手段である。
【００１１】
ＩＣカード１は非接触ＩＣカードである。非接触ＩＣカードとして、通信距離が１０ｃｍ以下の近接型の非接触ＩＣカード、すなわちＴｙｐｅＡ，ＴｙｐｅＢ，ＴｙｐｅＣ（ＦｅｌｉＣａ）が知られている（図１参照）。ＴｙｐｅＡとＴｙｐｅＢの規格は同一のＩＳＯ／ＩＥＣ１４４４３であるが、変調方式（ＡＳＫ１００％、ＡＳＫ１０％）、符号化方式（Modified Miller、ＮＲＺ－Ｌ）において相違している。一方、同じ近接型のＴｙｐｅＣの規格はＦｅｌｉＣａであり、ＴｙｐｅＡ、ＴｙｐｅＢとは規格が相違する。このように、同じ近接型の非接触ＩＣカードであっても、ＴｙｐｅＡ，ＴｙｐｅＢ，ＴｙｐｅＣは互いに通信方式におい相違がある。さらに、通信方式が異なるカードでは、カードにデータを読み書きするためのコマンド体系においても相違がある。
また、ＩＣカード１としては、通信距離が２ｍｍ以下の密接型（ＩＳＯ／ＩＥＣ１０５３６）、通信距離が７０ｃｍ以下の近傍型（ＩＳＯ／ＩＥＣ１５６９３）の非接触ＩＣカードであってもよい。非接触ＩＣカードの周波数は、密着型が４．９１ＭＨｚ、近接型と近傍型が１３．５６ＭＨｚである。非接触ＩＣカードの通信速度は、密着型が９．６ｋｂｐｓ以上、近接型が１０６ｋｂｐｓ以上、近傍型が１０ｋｂｐｓ以下である。
なお、これらすべての非接触ＩＣカードに対して読み書きのできるＩＣカードリーダライタは、上記から明らかなように、ソフトウェアだけでなくハードウェアにおいてもそれぞれの型式の非接触ＩＣカードに対応している必要性がある。
ここでは、簡単のため、ＩＣカード１は近接型の非接触ＩＣカードであるものとして説明を行なう。他の形式の非接触ＩＣカードへの適用は、その説明から容易である。
【００１２】
ＩＣカードリーダライタ２は非接触ＩＣカードであるＩＣカード１のリーダライタである。ＩＣカードリーダライタ２は複数の通信方式の非接触ＩＣカード、たとえばＴｙｐｅＡ，ＴｙｐｅＢ，ＴｙｐｅＣ（ＦｅｌｉＣａ）のいずれの型式のＩＣカードに対しても読み書きを行うことができるＩＣリーダライタである。
ＩＣカードリーダライタ２は複数の通信方式のＩＣカードの読み書きができるようにす

るため、たとえば、通信方式ごとのＩＣカード検出信号を順番に送出し、カードからの応答信号があったときに、その応答信号が適正であるか否かによりＩＣカードの通信方式を特定することを行なう。通信方式が特定されると、一連の処理が終了するまでは、その通信方式に固定してＩＣカードの読み書き処理を行う。前記した特許文献２には、そのような処理についての記載がある。

ＩＣカードリーダライタ２は制御部４はさらにその細部の構成要素として、制御部（制御用ＩＣ：Ｒ／Ｗ専用ＬＳＩ）４、ＳＡＭ（Secure Application Module）５、通信部（トランシーバＩＣ）６を有する。制御部４とＳＡＭ５は協調した動作を行なうことによって、上述したＩＣカードの通信方式を特定する処理、ＩＣカードに対する読み書き処理、等のデータ処理を行う（詳細を後述する）。通信部６は、制御部４の制御下において、電磁波による送受信をＩＣカード１との間で行なう。その電磁波による送受信は複数の通信方式のＩＣカードに対応する形態で行なわれる。

【００１３】

コントローラ３はＩＣカードリーダライタ２を端末とする本体システムにおいてＩＣカードリーダライタ２を制御する等のデータ処理を行う本体システムのコントローラ（データ処理部）である。すなわち、コントローラ３はＩＣカードリーダライタ２に対してコマンドを送信する機能を有している。コントローラ３は、たとえばゲート制御盤、プリンタ制御部、ファニチャ制御部である（図２参照）。コントローラ３の動作の一例を以下に説明する。

コントローラ３がゲート制御盤であるときには、〔１〕コントローラ３はＩＣカードリーダライタ２から「カード検出」を受信し、〔２〕コントローラ３はＩＣカードリーダライタ２に「ＩＤ情報読出」のコマンドを送信し、〔３〕コントローラ３はＩＣカードリーダライタ２がＩＣカード１から得た「ＩＤ情報」をＩＣカードリーダライタ２から受信し、〔４〕コントローラ３はその「ＩＤ情報」がコントローラ３のメモリにゲートの開錠を許可するＩＤとして登録されているか否かの判定を行ない、〔５〕コントローラ３はそのＩＤが登録されているときにはゲートの電気錠に対して開錠指令信号を出力する。

コントローラ３がプリンタ制御部であるときには、〔１〕最初にユーザがパーソナルコンピュータにおいて印刷指令を入力すると、印刷ジョブがプリンタに送信され、プリンタはそのメモリに印刷ジョブを保存する。〔２〕続いてコントローラ３はＩＣカードリーダライタ２から「カード検出」を受信し、〔３〕コントローラ３はＩＣカードリーダライタ２に「ＩＤ情報読出」のコマンドを送信し、〔４〕コントローラ３はＩＣカードリーダライタ２がＩＣカード１から得た「ＩＤ情報」をＩＣカードリーダライタ２から受信し、〔５〕コントローラ３はその「ＩＤ情報」に紐付けされている印刷ジョブがメモリに保存されているか否かの判定を行ない、〔６〕コントローラ３は、その印刷ジョブが保存されているときには、印刷部に対してその印刷ジョブの紙への印刷指令信号を出力する。

コントローラ３がたとえばＩＣカード認証キャビネットのファニチャ制御部であるときには、上記のゲート制御盤と同様である。ＩＣカードリーダライタ２がＩＣカード１から読み出した「ＩＤ情報」がコントローラ３のメモリに登録されているときにはキャビネットの電気錠に対して開錠指令信号を出力する。

【００１４】

制御部４はＩＣカードリーダライタ２において制御に係わるデータ処理、ＩＣカード１の読み書きに係わるデータ処理、等を行うＩＣカードリーダライタ２のデータ処理部である。図１、図２において、制御部、制御用ＩＣ、Ｒ／Ｗ専用ＬＳＩは呼称としては相違するが物としては同一である。制御部４はさらにその細部の構成要素として、通信方式特定手段４１、データ変換要求手段４２、活性化指令手段４３、キーフレーズ送信手段４４を有する。

通信方式特定手段４１はデータ処理の対象となるＩＣカードの通信方式を特定する。

データ変換要求手段４２は通信方式に適合するように必要に応じてコマンドとデータフォーマットの変換要求をＳＡＭ５に対して行う（詳細を後述する）。

活性化指令手段４３は、ＩＣカードリーダライタに固有のキーフレーズを付加データと

して活性化コマンドをＳＡＭ５に送信することにより、ＳＡＭ５を活性化状態にする。ＳＡＭは活性化フラグを有し、その活性化フラグの値によって非活性化状態または活性化状態のいずれかの状態となっている。非活性化状態は使用開始手続前の使用不可能な状態であり、活性化状態は使用開始手続後の使用可能な状態である。固有のキーフレーズは、たとえば、ＩＣカードリーダライタの製造シリアル番号である。

キーフレーズ送信手段４４はキーフレーズをＳＡＭ５に送信する。そのキーフレーズを受信したＳＡＭ５のキーフレーズ管理手段５０７はその受信したキーフレーズとＳＡＭのメモリに書き込まれているキーフレーズとが一致するか否かを判定し、一致するときにだけ、ＳＡＭが制御部のコマンドを受付けるようにする。

【００１５】

ＳＡＭ５は固有情報メモリ５１とデータ変換応答手段５０１を有する。固有情報メモリ５１はＩＣカード１の各々におけるメモリのデータフォーマット情報と、制御部４において処理可能な共通コマンドと通信方式の異なるＩＣカードの各々において処理可能な固有コマンドとを対応させたコマンドリスト情報とを格納する。そのデータフォーマット情報には、すくなくともメモリに設定されるデータブロックの名称、およびそのデータブロックを構成するデータの項目とバイト数、その項目の配列順の情報が含まれている。

制御部４から、データ処理の対象となるＩＣカードの通信方式に適合するように必要に応じてコマンドとデータフォーマットの変換要求が、ＳＡＭ５に対して行われたときには、その変換要求を受付けて、ＳＡＭ５は固有情報メモリのデータフォーマット情報とコマンドリスト情報を参照し、コマンドとデータフォーマットの変換を行なう。

【００１６】

その過程は、たとえば次のような過程である。

制御部４がＩＣカード１の読み書きに係わるデータ処理を行うときのＩＣカードに対するコマンドが共通コマンドであるときには、制御部４はデータの変換要求を行なう。制御部４のデータ変換要求手段４２は、制御部４の通信方式特定手段４１が特定したＩＣカード１の通信方式と、そのデータ処理を実行する共通コマンドとその付加データとからなる変換要求データをＳＡＭ５のデータ変換応答手段５０１に送信する。これにより制御部４によるデータの変換要求が行なわれる。

その変換要求に対して、ＳＡＭ５のデータ変換応答手段５０１は変換要求データの共通コマンドに対応する固有コマンドをＳＡＭ５の固有情報メモリ５１が格納するコマンドリスト情報から選択する。さらに、ＳＡＭ５のデータ変換応答手段５０１は共通コマンドの付加データと内容が同一でかつＩＣカード１のデータフォーマットに形式が適合する付加データを固有情報メモリのデータフォーマット情報に基づいて生成する。さらに、ＳＡＭ５のデータ変換応答手段５０１はその生成した付加データを選択した固有コマンドに付加することによって変換応答データを生成する。そして、ＳＡＭ５のデータ変換応答手段５０１はその変換応答データを制御部４に返信する。

制御部４は、ＳＡＭ５から返信された変換応答データを、ＩＣカード１の固有コマンドとしてＩＣカード１へ送信する（詳細を後述する）。

このような固有情報メモリ５１とデータ変換応答手段５０１をＳＡＭ５が有することから、仕様等の変更要求への対応は、ＩＣカードリーダライタのプログラム変更等を必要とせず、ＳＡＭ５を更新することで済ませることができるため容易である。

【００１７】

ＳＡＭ５は、固有情報メモリ５１とデータ変換応答手段５０１だけでなく、さらにその細部の構成要素として、復号化手段５０２、データ抽出手段５０３、データ配列手段５０４、暗号化手段５０５、活性化遷移手段５０６、キーフレーズ管理手段５０７、使用許可手段５０８を有する。

復号化手段５０２は制御部４がＩＣカード１からリードコマンドにより読み取る暗号化データブロックを復号化して復号化データブロックを生成する。

データ抽出手段５０３は復号化データブロックを構成する項目の各々のデータを、データフォーマットの情報を参照して抽出する。

データ配列手段５０４は出された項目の各々のデータを制御部４において処理可能な所定の順番に配列したデータ列に編成する。

暗号化手段５０２は制御部４がＩＣカード１にライトコマンドにより書き込むデータブロックを暗号化して暗号化データブロックを生成する。

これらデータ処理によって、ＩＣカード１のメモリが記憶する暗号化されたデータブロックを制御部４において解釈することができるようになる。また、このようにデータブロックの暗号化と復号化によって情報漏洩等に対するセキュリティ性を高いものとすることができる。

【００１８】

活性化遷移手段５０６はＳＡＭ５のメモリにキーフレーズを書き込むとともにＳＡＭ５の中の活性化フラグ５２を活性化状態に遷移させる。活性化遷移手段５０６は、ＳＡＭ５から読み出した活性化フラグの値が非活性化状態であって、制御部４の活性化指令手段４３がキーフレーズを付加データとして活性化コマンドをＳＡＭに送信したときに動作する。すなわち、その活性化コマンドに対応して、活性化遷移手段５０６はＳＡＭ５のメモリにキーフレーズを書き込むとともにＳＡＭ５の中の活性化フラグ５２を活性化状態に遷移させる。

キーフレーズ管理手段５０７はキーフレーズ送信手段４４から受信したキーフレーズと、ＳＡＭ５のメモリに書き込まれているキーフレーズとが一致するときにだけＳＡＭ５が制御部４のコマンドを受付けるようにする。

このような活性化遷移とキーフレーズ管理によって、特定のＳＡＭ５は特定のＩＣカードリーダライタ２によってだけ使用することが可能となり情報漏洩等に対するセキュリティ性を高いものとすることができる。

【００１９】

以上、構成について説明した。次に、本発明のＩＣカードリーダライタおよびそれに内蔵するＳＡＭにおける動作について説明する。最初に、コマンドが固有コマンドであるときの動作の一例を説明する。固有コマンドはそのままでＩＣカードにおいてデータ処理が可能なコントローラからのコマンドである。ＩＣカードの固有コマンドをＩＣカードリーダライタがコントローラから受信したときの本発明における動作の一例をフロー図として図３に示す。

まず、図３のステップＳ１において、コントローラ３はＩＣカードリーダライタ２へコマンド（Ａ）を送信する（発信する）。

次に、ステップＳ２において、ＩＣカードリーダライタ２はコマンド（Ａ）がＩＣカード１の固有コマンドであるか否かを判定する。固有コマンドでないときには共通コマンドを処理するフローへ進む（詳細を後述する）。固有コマンドであるときには、ステップＳ３へ進む。

【００２０】

次に、ステップＳ３において、ＩＣカードリーダライタ２はＩＣカード１のポーリングを開始する。ＩＣカードリーダライタ２は複数の通信方式のＩＣカード１に対する読み書きが可能である。ＩＣカードリーダライタ２はコマンド（Ａ）を実行する対象のＩＣカード１が存在するか否かをポーリングによって確認する。

次に、ステップＳ４において、ＩＣカード１はＩＣカードリーダライタ２のポーリングに対して応答を行なう。

次に、ステップＳ５において、ＩＣカードリーダライタ２はＩＣカード１からの応答を待機しており、その応答を受けるとステップＳ６へ進む。

これら、ステップＳ３～Ｓ５の過程は制御部４の通信方式特定手段４１によって行なわれ、ＩＣカード１の存在が確認されたときには同時にそのＩＣカード１の通信方式も特定される。

【００２１】

次に、ステップＳ６において、ＩＣカードリーダライタ２はコマンド（Ａ）をそのままＩＣカード１へ送信する（転送する）。

次に、ステップＳ７において、ＩＣカード１はコマンド（Ａ）を受信し、コマンド（Ａ）に対応するデータ処理を行なう。そして、ＩＣカードリーダライタ２のコマンド（Ａ）に対する応答を行なう。

次に、ステップＳ８において、ＩＣカードリーダライタ２はＩＣカード１からの応答を待機しており、その応答を受けるとステップＳ９へ進む。

次に、ステップＳ９において、ＩＣカードリーダライタ２はカード１からの応答をそのままコントローラ３へ送信する（返信する）。

次に、ステップＳ１０において、コントローラ３はＩＣカードリーダライタ２からの応答を待機しており、ＩＣカードリーダライタ２からのその応答を受信する。その応答を受信すると、コントローラ３はＩＣカードリーダライタ２へコマンド（Ａ）を送信してからの（ステップＳ１からの）一連の処理を終了する。

【００２２】

以上、コマンドが固有コマンドであるときの動作の一例を説明した。次に、コマンドが共通コマンドのリードコマンドであるときの動作の一例を説明する。共通コマンドはそのままでＩＣカードリーダライタにおいてはデータ処理が可能であるがＩＣカードにおいてはデータ処理が不可能なコントローラからのコマンドである。共通コマンドのリードコマンドをＩＣカードリーダライタがコントローラから受信したときの本発明における動作の一例をフロー図として図４に示す。

まず、図４のステップＳ１０１において、コントローラ３はＩＣカードリーダライタ２へリードコマンド（Ａ）を送信する（発信する）。リードコマンド（Ａ）は共通コマンドである。共通コマンドは、たとえばＩＳＯ／ＩＥＣ７８１６で規定されたＡＰＤＵ形式で定義される。すなわち、共通コマンドは「ＣＬＡ」＋「ＩＮＳ」＋「Ｐ１」＋「Ｐ２」＋「Ｌｃ」＋「Ｄａｔａ」＋「Ｌｅ」という構成を有する（図４参照）。ここで、「ＣＬＡ」はクラスコード、「ＩＮＳ」は命令コード、「Ｐ１」はパラメータ１、「Ｐ２」はパラメータ２、「Ｌｃ」は以下のデータのバイト数、「Ｄａｔａ」はデータ、「Ｌｅ」は応答として期待するバイト数である。

次に、ステップＳ１０２において、ＩＣカードリーダライタ２はリードコマンド（Ａ）がＩＣカード１の固有コマンドであるか否かを判定する。固有コマンドであるときには固有コマンドを処理するフローへ進む（図３とその説明を参照）。固有コマンドでないときすなわち共通コマンドのときには、ステップＳ１０３へ進む。

【００２３】

次に、ステップＳ１０３において、ＩＣカードリーダライタ２はＩＣカード１のポーリングを開始する。ＩＣカードリーダライタ２は複数の通信方式のＩＣカード１に対する読み書きが可能である。ＩＣカードリーダライタ２はコマンド（Ａ）を実行する対象のＩＣカード１が存在するか否かをポーリングによって確認する。

次に、ステップＳ１０４において、ＩＣカード１はＩＣカードリーダライタ２のポーリングに対して応答を行なう。

次に、ステップＳ１０５において、ＩＣカードリーダライタ２はＩＣカード１からの応答を待機しており、その応答を受けるとステップＳ１０６へ進む。

これらステップＳ１０３～Ｓ１０５の過程は制御部４の通信方式特定手段４１によって行なわれる。通信方式特定手段４１は、図４に示す一例において、ＩＣカード１からの応答によりＩＣカード１がタイプＹのＩＣカードであることを検出する。

【００２４】

次に、ステップＳ１０６において、タイプＹであるＩＣカード１がリードコマンド（Ａ）を実行することができるように、制御部４のデータ変換要求手段４２はＳＡＭ５に対して、共通コマンドであるリードコマンド（Ａ）をそれに対応するタイプＹであるＩＣカード１の固有コマンドに変換する要求を行なう。

次に、ステップＳ１０７において、ＳＡＭ５は共通コマンドであるリードコマンド（Ａ）に対応する固有コマンドであるリードコマンド（Ａ’）を、固有情報メモリ５１を参照して抽出する。さらにリードコマンド（Ａ）のデータフォーマットをリードコマンド（Ａ

’）のデータフォーマットに変換する。この変換においてはヘッダ、フッタ、等の付加データも変換付加される。固有情報メモリ５１にはカードタイプごとに規定されたコマンド形式が格納されている。たとえば、タイプＸのあるコマンドは「コマンド」＋「ブロックＮｏ．」＋「Ｐ１」＋「Ｐ２」＋「Ｌｅ」という構成を有し、タイプＹのあるコマンドは「コマンド」＋「セクタＮｏ．」＋「ブロック位置」＋「Ｐ１」という構成を有する（図４参照）。そして、ＳＡＭ５はそのリードコマンド（Ａ’）を制御部４へ送信する（返信する）。ステップＳ１０７におけるデータ変換はＳＡＭ５のデータ変換応答手段５０１によって行なわれる。

【００２５】

次に、ステップＳ１０８において、ＩＣカードリーダライタ２はヘッダ、フッタ、を除いてコマンド（Ａ’）をＩＣカード１へ送信する（転送する）。

次に、ステップＳ１０９において、ＩＣカード１は固有コマンドであるコマンド（Ａ’）を受信し、コマンド（Ａ’）に対応するデータ処理を行なう。そして、ＩＣカード１はＩＣカードリーダライタ２のコマンド（Ａ’）に対する応答（Ｒ１）を行なう。

次に、ステップＳ１１０において、ＩＣカードリーダライタ２はＩＣカード１からの応答を待機しておりその応答（Ｒ１）を受けると、その応答（Ｒ１）をＳＡＭ５に送信し、復号とデータ抽出を指令する。

次に、ステップＳ１１１において、ＳＡＭ５は応答（Ｒ１）を復号して得た平文から、データ項目を抽出し、所定の順番にデータ列を編成し制御部４に返答する。編成したデータ列は、たとえば、「タグ１」＋「ＩＤ番号」＋「タグ２」＋「組織コード」＋「タグ３」＋「性別」という構成を有する（図４参照）。ここにおける、応答（Ｒ１）の復号は復号化手段５０２によって、データ項目を抽出はデータ抽出手段５０３によって、データ列の編成はデータ配列手段５０４によって行なわれる。

【００２６】

次に、ステップＳ１１２において、制御部４はＳＡＭ５からの応答を待機しており、その応答を受けるとステップＳ１１３へ進む。

次に、ステップＳ１１３において、制御部４はカード１からの応答をそのままコントローラ３へ送信する（返信する）。

次に、ステップＳ１０において、コントローラ３はＩＣカードリーダライタ２からの応答を待機しており、ＩＣカードリーダライタ２からのその応答を受信する。その応答を受信すると、コントローラ３がＩＣカードリーダライタ２へコマンド（Ａ）を送信してからの（ステップＳ１からの）一連の処理を終了する。

【００２７】

以上、共通コマンドがリードコマンドであるときの動作の一例を説明した。次に、共通コマンドがライトコマンドであるときの動作の一例を説明する。共通コマンドのライトコマンド（部分書換コマンド（Ｂ））をＩＣカードリーダライタがコントローラから受信したときの本発明における動作の一例をフロー図として図５に示す。

まず、図５のステップＳ２０１において、コントローラ３は部分書き換えの対象となるデータブロックに対するリードコマンド（Ａ）をあらかじめ完了しておく（図４とその説明を参照）。その結果、部分書き換えの対象となるデータブロックはＳＡＭ５のメモリに保存されている。そのデータブロックは、たとえば、「入館情報」＋「建物Ｎｏ」＋「県コード」＋「国コード」という構成を有する（図５参照）。

次に、ステップＳ２０２において、コントローラ３はＩＣカードリーダライタ２へ部分書換コマンド（Ｂ）を送信する（発信する）。部分書換コマンド（Ｂ）は共通コマンドである。共通コマンドは、たとえばＩＳＯ／ＩＥＣ７６７１で規定されたＡＰＤＵ形式で定義される。部分書換コマンド（Ｂ）によって、たとえば「入館情報」＋「建物Ｎｏ」＋「県コード」＋「国コード」という構成を有するデータブロックの「建物Ｎｏ」の部分を「建物Ｎｏ’」に書き換えを行なう（図５参照）。

次に、ステップＳ２０３において、ＩＣカードリーダライタ２は部分書換コマンド（Ｂ）がＩＣカード１の固有コマンドであるか否かを判定する。固有コマンドであるときには

固有コマンドを処理するフローへ進む（図３とその説明を参照）。固有コマンドでないときすなわち共通コマンドのときには、ステップＳ２０４へ進む。

【００２８】

次に、ステップＳ２０４において、ＩＣカードリーダライタ２はＩＣカード１のポーリングを開始する。ＩＣカードリーダライタ２は複数の通信方式のＩＣカード１に対する読み書きが可能である。ＩＣカードリーダライタ２は部分書換コマンド（Ｂ）を実行する対象のＩＣカード１が存在するか否かをポーリングによって確認する。

次に、ステップＳ２０５において、ＩＣカード１はＩＣカードリーダライタ２のポーリングに対して応答を行なう。

次に、ステップＳ２０６において、ＩＣカードリーダライタ２はＩＣカード１からの応答を待機しており、その応答を受けるとステップＳ２０７へ進む。

これらステップＳ２０４～Ｓ２０６の過程は制御部４の通信方式特定手段４１によって行なわれる。通信方式特定手段４１は、図５に示す一例において、ＩＣカード１からの応答によりＩＣカード１がタイプＹのＩＣカードであることを検出する。

【００２９】

次に、ステップＳ２０７において、タイプＹであるＩＣカード１が部分書換コマンド（Ｂ）を実行することができるように、制御部４のデータ変換要求手段４２はＳＡＭ５に対して、共通コマンドである部分書換コマンド（Ｂ）をそれに対応するタイプＹであるＩＣカード１の固有コマンドに変換する要求を行なう。このとき、どのバイトをどんな値に書き換えるのかの情報を含めて要求する。

次に、ステップＳ２０８において、ＳＡＭ５は、部分書き換えの対象としてＳＡＭ５のメモリに保存されているデータブロックの構成の内で、部分書換コマンド（Ｂ）で書き換えを指定された部分のバイトを書き換える。たとえば、「建物Ｎｏ」の部分を「建物Ｎｏ’」に書き換える。そして、全体を暗号化して部分書換コマンド（Ｂ’）を生成する。この書き換え（データ変換）はＳＡＭ５のデータ変換応答手段５０１によって行なわれ、暗号化はＳＡＭ５の暗号化手段５０５によって行なわれる。

次に、ステップＳ２０９において、ＳＡＭ５は部分書換コマンド（Ｂ’）に対応する固有コマンドである部分書換コマンド（Ｂ”）を、固有情報メモリ５１を参照して抽出する。さらに部分書換コマンド（Ｂ’）のデータフォーマットを部分書換コマンド（Ｂ”）のデータフォーマットに変換する。この変換においてはヘッダ、フッタ、等の付加データも変換付加される。固有情報メモリ５１にはカードタイプごとに規定されたコマンド情報とデータフォーマット情報が格納されている。そして、ＳＡＭ５はその部分書換コマンド（Ｂ”）を制御部４へ送信する（返信する）。このステップＳ２０９におけるデータ変換はＳＡＭ５のデータ変換応答手段５０１によって行なわれる。

【００３０】

次に、ステップＳ２１０において、ＩＣカードリーダライタ２はヘッダ、フッタ、を除いて部分書換コマンド（Ｂ”）をＩＣカード１へ送信する（転送する）。

次に、ステップＳ２１１において、ＩＣカード１は固有コマンドである部分書換コマンド（Ｂ”）を受信し、部分書換コマンド（Ｂ”）に対応するデータ処理を行なう。そして、ＩＣカード１はＩＣカードリーダライタ２の部分書換コマンド（Ｂ”）に対する応答（Ｒ２）を行なう。

次に、ステップＳ２１２において、ＩＣカードリーダライタ２はＩＣカード１からの応答を待機しておりその応答（Ｒ２）を受けるとステップＳ２１３へ進む。

次に、ステップＳ２１３において、制御部４はカード１からの応答をそのままコントローラ３へ送信する（返信する）。

次に、ステップＳ１０において、コントローラ３はＩＣカードリーダライタ２からの応答を待機しており、ＩＣカードリーダライタ２からのその応答を受信する。その応答を受信すると、コントローラ３がＩＣカードリーダライタ２へコマンド（Ａ）を送信してからの（ステップＳ１からの）一連の処理を終了する。

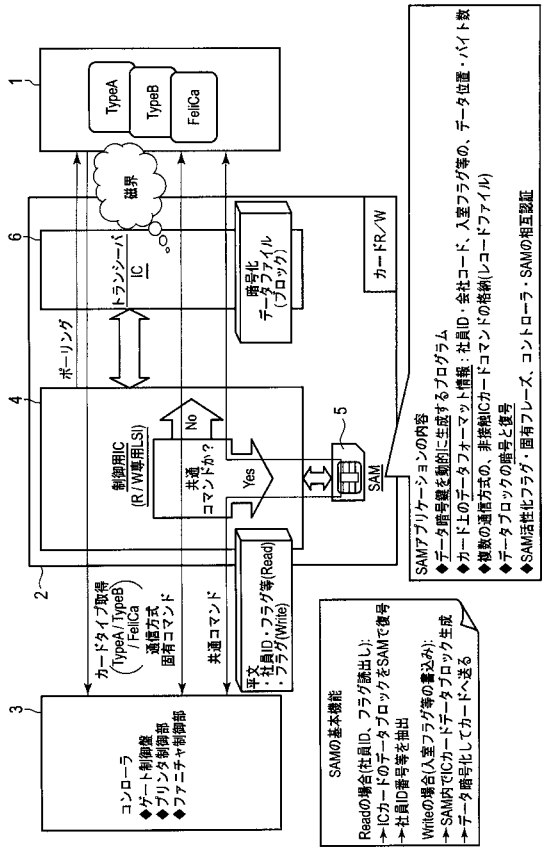
【産業上の利用可能性】

【００３１】
複数の形式のＩＣカードに対応するとともに、情報漏洩等に対するセキュリティ性が高く、仕様等の変更要求への対応が容易であることが求められるＩＣカードリーダライタ等において利用可能である。

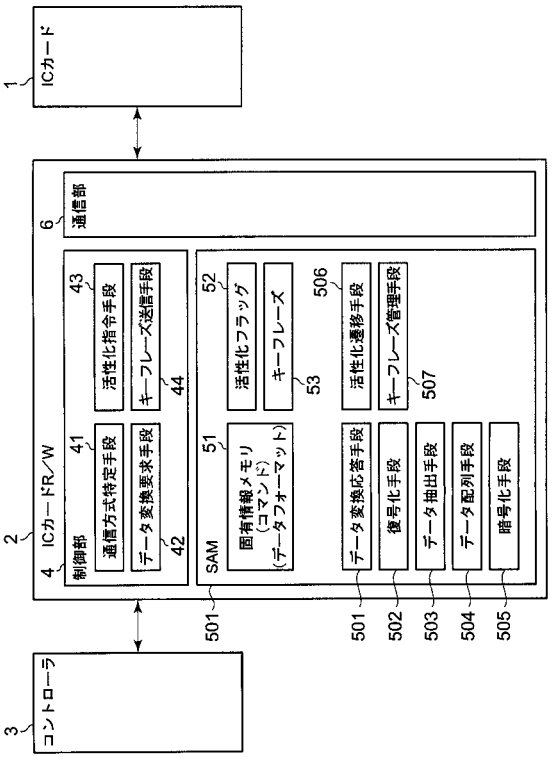
【符号の説明】

【００３２】
１　ＩＣカード
２　ＩＣカードリーダライタ
３　コントローラ
４　制御部（制御用ＩＣ：Ｒ／Ｗ専用ＬＳＩ）
５　ＳＡＭ（Secure Application Module）
６　通信部（トランシーバＩＣ）
４１　通信方式特定手段
４２　データ変換要求手段
４３　活性化指令手段
４４　キーフレーズ送信手段
５１　固有情報メモリ
５２　活性化フラッグ
５３　キーフレーズ
５０１　データ変換応答手段
５０２　復号化手段
５０３　データ抽出手段
５０４　データ配列手段
５０５　暗号化手段
５０６　活性化遷移手段
５０７　キーフレーズ管理手段

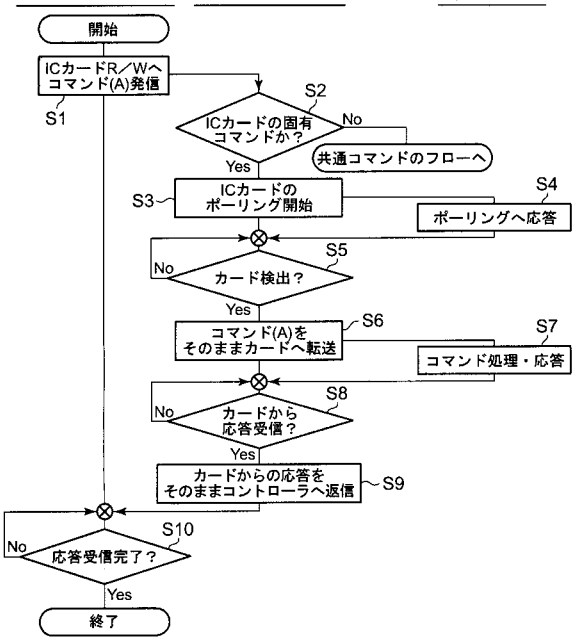
【図１】


TypeA
TypeB
FeliCa
磁界
トランシーバIC
ポーリング
暗号化データファイル(ブロック)
カードR/W
制御用IC(R/W専用SI)
共通コマンドか?
No
Yes
SAM
SAMアプリケーションの内容
◆データ暗号鍵を動的に生成するプログラム
◆カード上のデータフォーマット情報(社員ID・会社コード、入室フラグ等の、データ位置・バイト数
◆複数の通信方式の、非接触ICカードコマンドの格納(レコードファイル)
◆データブロックの暗号と復号
◆SAM活性フラグ・固有フレーズ、コントローラ・SAMの相互認証
カードタイプ取得(TypeA/TypeB/FeliCa)
通信方式
固有コマンド
共通コマンド
平文:社員ID・フラグ等(Read)
暗号:フラグ等(Write)
コンローラ
◆ゲート制御盤
◆プリンタ制御部
◆ファニチャ制御部
SAMの基本機能
Readの場合(社員ID、フラグ読出し):
→ICカードのデータブロックをSAMで復号
→社員ID番号等を抽出
Writeの場合(入室フラグ等の書込み):
→SAM内でICカードデータブロック生成
→データ暗号化してカードへ送る

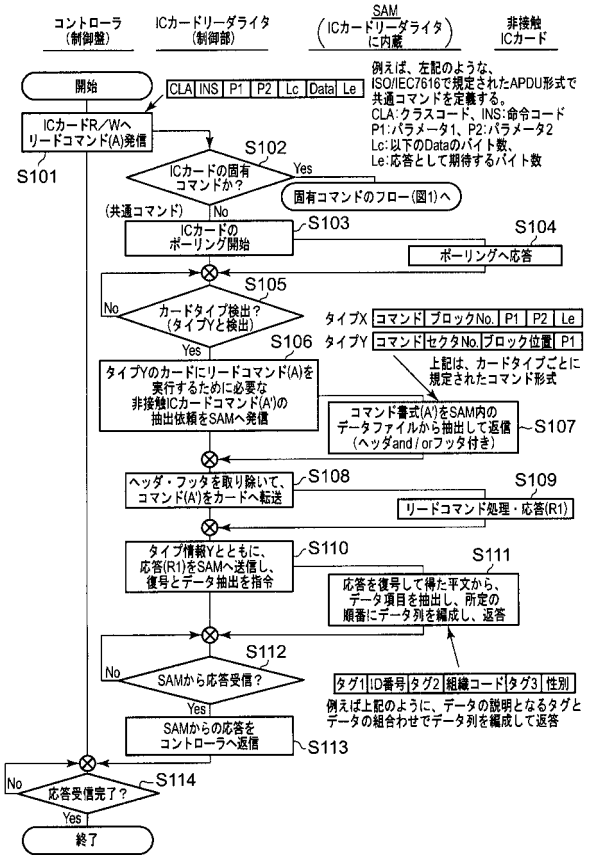
【図２】


ICカード
通信部
ICカードR/W
制御部
通信方式特定手段
データ変換要求手段
活性化指令手段
キーフレーズ送信手段
SAM
固有情報メモリ(コマンド)(データフォーマット)
活性化フラグ
キーフレーズ
活性化遷移手段
キーフレーズ管理手段
データ変換応答手段
復号化手段
データ抽出手段
データ配列手段
暗号化手段
コントローラ

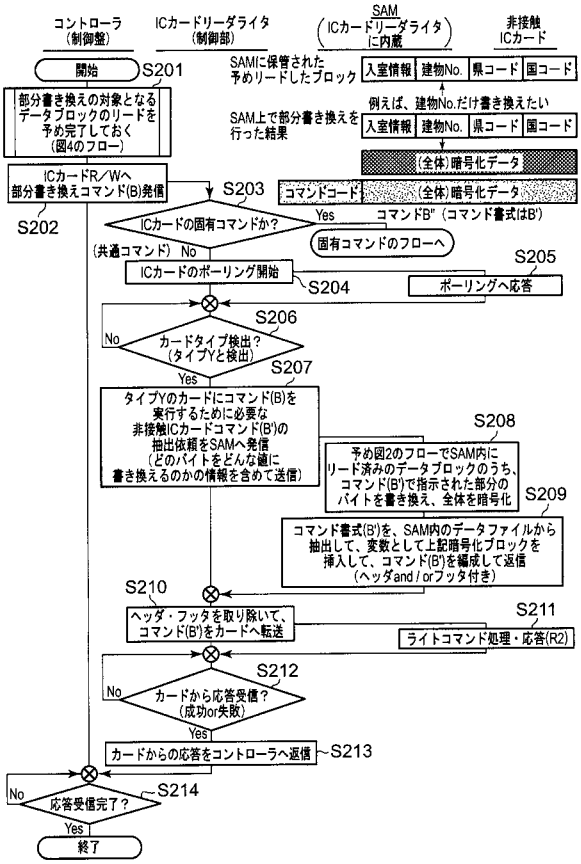
【図３】


コントローラ（制御盤）
ICカードリーダライタ
非接触ICカード
開始
ICカードR/Wへコマンド(A)発信
S1
ICカードの固有コマンドか?
S2
No
Yes
共通コマンドのフローへ
ICカードのポーリング開始
S3
ポーリングへ応答
S4
カード検出?
S5
コマンド(A)をそのままカードへ転送
S6
コマンド処理・応答
S7
カードから応答受信?
S8
カードからの応答をそのままコントローラへ返信
S9
応答受信完了?
S10
終了

【図４】


コントローラ(制御盤)
ICカードリーダライタ(制御部)
SAM(ICカードリーダライタに内蔵)
非接触ICカード
開始
ICカードR/Wへリードコマンド(A)発信
S101
CLA INS P1 P2 Lc Data Le
例えば、左記のような、ISO/IEC7616で規定されたAPDU形式で共通コマンドを定義する。
CLA:クラスコード、INS:命令コード
P1:パラメータ1、P2:パラメータ2
Lc:以下のDataのバイト数、
Le:応答として期待するバイト数
ICカードの固有コマンドか?
S102
Yes
固有コマンドのフロー(図1)へ
(共通コマンド)
No
ICカードのポーリング開始
S103
ポーリングへ応答
S104
カードタイプ検出?(タイプYと検出)
S105
タイプX コマンド ブロックNo. P1 P2 Le
タイプY コマンド セクタNo. ブロック位置 P1
上記は、カードタイプごとに規定されたコマンド形式
タイプYのカードにリードコマンド(A)を実行するために必要な非接触ICカードコマンド(A')の抽出依頼をSAMへ発信
S106
コマンド書式(A')をSAM内のデータファイルから抽出して返信(ヘッダand/orフッタ付き)
S107
ヘッダ・フッタを取り除いて、コマンド(A')をカードへ転送
S108
リードコマンド処理・応答(R1)
S109
タイプ情報Yとともに、応答(R1)をSAMへ送信し、復号とデータ抽出を指令
S110
応答を復号して得た平文から、データ項目を抽出し、所定の順番にデータ列を編成し、返答
S111
SAMから応答受信?
S112
タグ1 ID番号 タグ2 組織コード タグ3 性別
例えば上記のように、データの説明となるタグとデータの組合わせでデータ列を編成して返答
SAMからの応答をコントローラへ返信
S113
応答受信完了?
S114
終了

【図５】


コントローラ（制御盤）
ICカードリーダライタ（制御部）
SAM（ICカードリーダライタに内蔵）
非接触ICカード
開始
S201
SAMに保管された予めリードしたブロック
入室情報
建物No.
県コード
国コード
部分書き換えの対象となるデータブロックのリードを予め完了しておく（図4のフロー）
例えば、建物No.だけ書き換えたい
SAM上で部分書き換えを行った結果
(全体)暗号化データ
ICカードR／Wへ部分書き換えコマンド(B)発信
S202
S203
コマンドコード
ICカードの固有コマンドか？
Yes
コマンドB''（コマンド書式はB'）
（共通コマンド）No
固有コマンドのフローへ
ICカードのポーリング開始
S204
S205
ポーリングへ応答
S206
No
カードタイプ検出？（タイプYと検出）
Yes
S207
タイプYのカードにコマンド(B)を実行するために必要な非接触ICカードコマンド(B')の抽出依頼をSAMへ発信（どのバイトをどんな値に書き換えるのかの情報を含めて送信）
S208
予め図2のフローでSAM内にリード済みのデータブロックのうち、コマンド(B')で指示された部分のバイトを書き換え、全体を暗号化
S209
コマンド書式(B')を、SAM内のデータファイルから抽出して、変数として上記暗号化ブロックを挿入して、コマンド(B')を編成して返信（ヘッダand / orフッタ付き）
S210
ヘッダ・フッタを取り除いて、コマンド(B')をカードへ転送
S211
ライトコマンド処理・応答(R2)
S212
No
カードから応答受信？（成功or失敗）
Yes
カードからの応答をコントローラへ返信
S213
No
応答受信完了？
S214
Yes
終了

フロントページの続き

(51)Int.Cl.	FI	テーマコード（参考）
	Ｇ０６Ｆ　12/14　５４０Ａ	
	Ｈ０４Ｂ　5/02	

(72)発明者　蜂木　茂男
東京都新宿区市谷加賀町一丁目１番１号　大日本印刷株式会社内
(72)発明者　矢野　義博
東京都新宿区市谷加賀町一丁目１番１号　大日本印刷株式会社内

Ｆターム(参考) 5B017 AA03 BA07 CA14
5B035 AA06 AA13 BB09 CA29
5B058 CA13 CA17 CA23 CA27 KA08 KA21 KA35
5K012 AB05 AB18 BA02 BA07