

明 細 書

発明の名称： 携帯可能電子装置およびＩＣカード

技術分野

[0001] 本発明の実施形態は、携帯可能電子装置およびＩＣカードに関する。

背景技術

[0002] 従来、携帯可能電子装置としてのＩＣカードとＩＣカード処理装置とからなる処理システムは、当該システムの運用方針に従って予め設定された処理方式で特定の処理を実行するように発行処理される。例えば、ＩＣカードは、予め設定された１つの暗号方式で暗号処理を実行するように発行処理される。一方、近年では、量子コンピュータなどの高度な計算力を備える計算機の登場に対応するために耐量子暗号などの新しい暗号方式による暗号処理が望まれる場面も多くなってきている。上述した従来の処理システムは、耐量子暗号などの新しい暗号方式での暗号処理を実施するためには、ＩＣカードだけでなく全てのＩＣカード処理装置を一斉に新暗号方式に対応するものに置き換える必要がある。

[0003] しかしながら、運用中の処理システム全体でＩＣカードおよびＩＣカード処理装置を一斉に新暗号方式に対応するものに置き換えるのは現実的に難しいと考えられる。このため、暗号処理に用いる暗号方式を既存の暗号方式から新しい暗号方式に移行するには、暗号処理を実行する暗号方式として既存暗号方式と新暗号方式とが共存する移行期間が必要となることが想定される。このような移行期間において、ＩＣカードは、既存暗号方式と新暗号方式との両方に対応するだけでなく、ＩＣカード処理装置が要求する暗号方式での暗号処理を円滑に実行できるようにすることが要望される。

先行技術文献

特許文献

[0004] 特許文献１：日本国特開２０２０－１０３９６号公報

発明の概要

発明が解決しようとする課題

[0005] 上記の課題を解決するために、本発明は、複数の処理方式から1つの処理方式を選択して特定の処理を実行することができる携帯可能電子装置、および、ICカードを提供する。

課題を解決するための手段

[0006] 実施形態によれば、携帯可能電子装置は、インターフェースとメモリとプロセッサとを備える。インターフェースは、外部装置と通信する。メモリは、特定の処理を実行するための複数の異なる処理方式ごとの設定情報を記憶する。プロセッサは、外部装置から供給される情報に応じて特定の処理を実行するための1つの処理方式を選択し、選択した処理方式によって特定の処理を実行する。

図面の簡単な説明

[0007] [図1]図1は、実施形態に係る携帯可能電子装置としてのICカードの構成例を示すブロック図である。

[図2]図2は、実施形態に係る携帯可能電子装置としてのICカードと通信するICカード処理装置の構成例を示すブロック図である。

[図3]図3は、実施形態に係る携帯可能電子装置としてのICカードにおけるNVMに複数の暗号方式ごとの設定情報（設定フラグ）を記憶する例を示す図である。

[図4]図4は、実施形態に係る携帯可能電子装置としてのICカードにおけるRAMに選択（設定）中の暗号方式を示す情報（識別フラグ）を記憶した例を示す図である。

[図5]図5は、実施形態に係る携帯可能電子装置としてのICカードによる第1の動作例を説明するためのフローチャートである。

[図6]図6は、実施形態に係る携帯可能電子装置としてのICカードによる第2の動作例を説明するためのフローチャートである。

[図7]図7は、実施形態に係る携帯可能電子装置としてのICカードによる第3の動作例を説明するためのフローチャートである。

[図8]図8は、実施形態に係る携帯可能電子装置としてのＩＣカードによる第4の動作例を説明するためのフローチャートである。

[図9]図9は、実施形態に係る携帯可能電子装置としてのＩＣカードによる第5の動作例を説明するためのフローチャートである。

[図10]図10は、実施形態に係る携帯可能電子装置としてのＩＣカードによる第6の動作例を説明するためのフローチャートである。

[図11]図11は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される署名検証コマンドの構成例を示す図である。

[図12]図12は、実施形態に係る携帯可能電子装置としてのＩＣカードによる第7の動作例を説明するためのフローチャートである。

[図13]図13は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される暗号方式を指定するパラメータを含む署名検証コマンドの例を示す図である。

[図14]図14は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される暗号方式を指定するパラメータを含む署名検証コマンドの例を示す図である。

[図15]図15は、実施形態に係る携帯可能電子装置としてのＩＣカードによる第8の動作例の流れを説明するためのフローチャートである。

[図16]図16は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される暗号方式ごとの署名検証コマンドの例を示す図である。

[図17]図17は、実施形態に係る携帯可能電子装置としてのＩＣカードに供給される暗号方式ごとの署名検証コマンドの例を示す図である。

実施形態

[0008] 以下、実施形態について、図面を参照しつつ説明する。

図1は、実施形態に係るＩＣカード1の構成例を概略的に示すブロック図である。実施形態に係る携帯可能電子装置としてのＩＣカード1は、外部装置としてのＩＣカード処理装置2と共にＩＣカード処理システムを構成する。ＩＣカード1は、ＩＣカード処理装置2から供給される電力により活

性化する（動作可能な状態になる）携帯可能な電子機器である。ＩＣカード１は、スマートカードとも称される。

[0009] なお、実施形態に係る携帯可能電子装置は、カード状の形状に限定されるものではなく、後述するＩＣカード１と同等な構成および処理機能を備える冊子状（たとえば、パスポートなどの手帳）のものであっても良い。また、実施形態に係る携帯可能電子装置は、後述するＩＣカード１と同等な構成および処理機能を備える携帯型の電子装置（たとえば、スマートフォン、携帯電話機、タブレットＰＣ、ドングルなど）であっても良い。

[0010] ＩＣカード１は、大別すると、接触型のＩＣカードと非接触型のＩＣカードとがある。接触型のＩＣカード１は、通信インターフェースとしてのコンタクト部を介してＩＣカード処理装置２からの動作電源および動作クロックの供給を受けて活性化する。たとえば、接触型のＩＣカード１は、ＩＳＯ／ＩＥＣ 7816-3に規定される規格に準拠するＩＣカードである。非接触型のＩＣカード１は、通信インターフェースとしてのアンテナおよび変復調回路などを介してＩＣカード処理装置２からの電波を受信し、その電波から動作電源および動作クロックを生成して活性化する。たとえば、非接触型のＩＣカード１は、ＩＳＯ／ＩＥＣ 14443-3に規定される規格に準拠するＩＣカードである。

[0011] 図１に示すように、ＩＣカード１は、本体Ｃを有する。本体Ｃは、プラスチックなどによりカード状に形成される。ＩＣカード１は、本体Ｃ内にモジュールＭを有する。モジュールＭは、１つまたは複数のＩＣチップＣaと通信の外部インターフェース（インターフェース）とが接続された状態で一体的に形成され、本体Ｃ内に埋設される。

[0012] なお、実施形態に係る携帯可能電子装置は、冊子状に形成される本体ＣにモジュールＭを備えるものであっても良いし、携帯型の電子装置を形成する本体Ｃ内にモジュールＭを備えるものであっても良い。

[0013] 図１に示す構成例において、ＩＣカード１のモジュールＭは、プロセッサ１１、ＲＡＭ１２、ＲＯＭ１３、ＮＶＭ（メモリ）１４、通信制御部１５お

よびインターフェース16などを有する。

プロセッサ11は、種々の処理を実行する回路を含む。プロセッサ11は、たとえば、CPU (Central Processing Unit) である。プロセッサ11は、ICカード1全体の制御を司る。プロセッサ11は、ROM13あるいはNVM14に記憶されているプログラムを実行することにより、種々の処理機能を実現する。ただし、後述するプロセッサ11が実行する各種の機能のうちの一部または全部は、ハードウェア回路により実現されるようにしても良い。

[0014] RAM12は、ワーキングメモリとして機能する揮発性のメモリである。また、RAM12は、プロセッサ11が処理中のデータなどを一時保管するバッファとしても機能する。たとえば、RAM12は、通信制御部15およびインターフェース16を介してICカード処理装置2との間で送受信するデータを一時保管する通信バッファとして機能する。

[0015] ROM13は、プログラムメモリとして機能する不揮発性のメモリである。ROM13は、予め制御用のプログラムおよび制御データなどが記憶される。ROM13は、製造段階で制御プログラムや制御データなどが記憶された状態でICカード1内に組み込まれるものである。ROM13に記憶される制御プログラムや制御データは、予め当該ICカード1の仕様に応じて組み込まれる。

[0016] たとえば、ROM13には、ICカード処理装置2から受信するコマンドに応じた処理をプロセッサ11が実行するためのプログラムが記憶される。また、実施形態に係るICカードは、複数の処理方式としての複数の暗号方式に対応するため、ROM13には、対応する各暗号方式（新暗号方式および既存暗号方式）での暗号処理を行うためのプログラムが記憶される。

[0017] NVM14は、データの書き込みおよび書き換えが可能な不揮発性のメモリである。NVM14は、たとえば、EEPROM（登録商標）（Electrically Erasable Programmable Read Only Memory）あるいはフラッシュROMなどで構成する。

また、NVM14は、一部または全部の領域が耐タンパー性を有し、セキュアにデータが格納できる記憶領域を有する。

[0018] NVM14には、当該ICカード1の運用用途に応じたプログラムや種々のデータが書き込まれる。NVM14には、プログラムファイルあるいはデータファイルなどが定義され、それらのファイルにプログラムや種々のデータが書き込まれる。たとえば、NVM14は、複数の暗号方式ごとに暗号方式が有効か無効かを示す情報（有効性を示す情報）を格納する記憶領域が設けられる。また、NVM14は、複数の暗号方式ごとに暗号処理用のプログラムおよび鍵データなどの暗号処理用のデータを記憶するようにしても良い。また、NVM14は、ユーザデータ、外部のネットワークと通信するためのネットワーク認証用のデータ、および、各種の処理を実行するためのアプリケーションプログラムなどを記憶する。

[0019] 通信制御部15は、インターフェース16に接続する。インターフェース16は、外部装置に通信接続するためのインターフェースである。通信制御部15およびインターフェース16は、通信部を構成する。通信制御部15およびインターフェース16は、ICカード処理装置2のインターフェースに対応した通信方式による通信機能を実現する。また、通信制御部15およびインターフェース16は、接触通信である場合、又は、非接触通信である場合も、複数の通信方式（通信プロトコル）をサポートするものとして構成しても良い。

[0020] 当該ICカード1が接触型のICカードとして実現される場合、通信制御部15およびインターフェース16は、ICカード処理装置2と接触して通信する通信部を構成する。この場合、インターフェース16は、ICカード処理装置2のコンタクト部と物理的かつ電氣的に接触するコンタクト部により構成され、通信制御部15は、コンタクト部を介した信号の送受信を制御する回路などにより構成される。また、通信制御部15は、プロセッサ11が指定する通信方式（通信プロトコル）に従って通信を制御する。

[0021] また、当該ICカード1が非接触型のICカードとして実現される場合、

通信制御部 15 およびインターフェース 16 は、ＩＣカード処理装置 2 のカードリーダーライタと非接触（無線）で通信する通信部を構成する。この場合、インターフェース 16 は、電波の送受信を行うアンテナにより構成され、通信制御部 15 は、送信する電波を生成するための変調回路および受信した電波から信号を生成するための復調回路などにより構成される。また、非接触通信を行う通信制御部 15 は、プロセッサ 11 により指定される Type A や Type B などの通信方式（通信プロトコル）に従って通信を制御する。

[0022] 図 2 は、実施形態に係る ＩＣカード処理装置 2 の構成例を概略的に示すブロック図である。

図 2 に示す構成例において、ＩＣカード処理装置 2 は、カードリーダーライタ 24 を介して ＩＣカード 1 と通信する機能を有する装置（Ｒ／Ｗ）である。ＩＣカード処理装置 2 は、たとえば、カードリーダーライタ 24 をパーソナルコンピュータ（ＰＣ）などの制御装置に接続した装置であっても良い。

[0023] ＩＣカード処理装置 2 は、図 2 に示すように、制御部 21、表示部 22、操作部 23、カードリーダーライタ 24 などを有する。

制御部 21 は、ＩＣカード処理装置 2 全体の動作を制御する。制御部 21 は、プロセッサ（ＣＰＵ）25、ＲＡＭ 26、ＲＯＭ 27、不揮発性メモリ 28、通信部 29 などにより構成される。たとえば、制御部 21 は、パーソナルコンピュータにより構成される。プロセッサ 25 は、ＲＯＭ 27 または不揮発性メモリ 28 が記憶するプログラムを実行することにより種々の処理を実行する。ＲＡＭ 26 は、データを一時的に保持するワーキングメモリとして機能する。ＲＯＭ 27 は、プログラムや制御データなどを記憶する不揮発性のメモリである。不揮発性メモリ 28 は、書き換え可能な不揮発性のメモリである。通信部 29 は、外部装置と通信するためのインターフェースである。

[0024] 制御部 21 は、カードリーダーライタ 24 により ＩＣカード 1 へコマンドを送信する機能、ＩＣカード 1 から受信したデータを基に種々の処理を行う機

能などを有する。たとえば、制御部21は、カードリーダーライタ24を介してICカード1にデータの書き込みコマンドを送信することによりICカード1内の不揮発性メモリにデータを書き込む制御を行う。また、制御部21は、ICカード1に読み取りコマンドを送信することによりICカード1からデータを読み出す制御を行う。また、制御部21は、ICカード1にアプリケーション選択コマンドを送信することによりICカード1において選択されるアプリケーションを制御する。

[0025] また、本実施形態において、ICカード処理装置2の制御部21は、後述する各動作例で説明するようなコマンドなどの情報をICカード1に供給することによりICカード1が暗号処理に用いる暗号方式を指定する。

[0026] 表示部22は、制御部21の制御により種々の情報を表示する表示装置である。操作部23は、キーボード、テンキー、ポインティングデバイスなどにより構成する。操作部23は、ICカード処理装置2の操作員が種々の操作指示やデータなどを入力するためのものである。また、操作部23は、ICカード1の利用者の識別情報あるいはパスワードなどの認証情報を入力するための入力部としても機能する。

[0027] カードリーダーライタ24は、ICカード1との通信を行うための通信部（第2の通信部）である。カードリーダーライタ24は、ICカード1の通信方式に応じたインターフェースにより構成される。たとえば、ICカード1が接触型のICカードである場合、カードリーダーライタ24は、ICカード1のコンタクト部と物理的かつ電氣的に接続するための接触部などにより構成される。また、ICカード1が非接触型のICカードである場合、カードリーダーライタ24は、ICカード1との無線通信を行うためのアンテナおよび通信制御などにより構成される。カードリーダーライタ24は、ICカード1に対して、電源電力を供給したり動作用のクロックを供給したりする。カードリーダーライタ24は、制御部21による制御に基づいてICカード1へのコマンドの送信およびICカード1からのコマンドに対するレスポンス（応答）の受信などを行う。

[0028] 次に、実施形態に係るＩＣカード１のＮＶＭ１４においてデータを格納するためのファイルの構成について説明する。

ＩＣカード１におけるＮＶＭ１４は、例えば、ＩＣカードの国際的な標準規格であるＩＳＯ／ＩＥＣ ７８１６－４で規定されているファイル構造の各ファイルにデータを格納する。このような規定のファイル構造では、ＭＦ（Master File）、ＤＦ（Dedicated File）、および、ＥＦ（Elementary File）などからなる階層構造を有する複数のファイル群が定義される。

[0029] ＭＦは最上階層にあり、ＭＦの次の階層に１又は複数のＤＦが定義され、ＤＦの次の階層に１又は複数のＥＦが定義される。１つのＤＦは、例えば、当該ＩＣカード１が備える１つのアプリケーションを実現するためのデータ群が格納される。複数のアプリケーションによって複数の機能を実現しているＩＣカード１は、各アプリケーションに対応する複数のＤＦがＮＶＭ１４に設けられる。また、ＤＦの配下にある各ＥＦは、上位階層となるＤＦとしてのアプリケーションに用いる各種のデータを格納するためのデータファイルである。

[0030] 次に、実施形態に係るＩＣカード１が備える特定の処理を実行するための複数の異なる処理方式について説明する。

実施形態に係るＩＣカード１は、特定の処理としての暗号処理を実行するための複数の異なる処理方式（暗号方式）に対応する。ＩＣカード１は、複数の処理方式から選択した１つの処理方式によって特定の処理を実行する機能を有する。本実施形態では、携帯可能電子装置としてのＩＣカード１は、既存の暗号方式（既存暗号方式、第１の暗号方式）と既存暗号方式とは異なる暗号方式（新暗号方式、第２の暗号方式）とに対応するものとする。また、本実施形態に係るＩＣカード１は、複数の暗号方式としての既存暗号方式および新暗号方式から選択する何れか一方の暗号方式を用いて暗号処理を実行する機能を有する。

[0031] 本実施形態において、新暗号方式は、既存暗号方式に比べて暗号強度が高

い暗号処理を実現できるものとする。例えば、新暗号方式としては、耐量子暗号が想定される。耐量子暗号は、量子コンピュータを用いても解読が困難であると考えられる暗号方式の総称である。耐量子暗号としては、例えば、格子暗号などがある。また、既存暗号方式としては、RSA、DES（Data Encryption Standard）などがある。RSAは、公開鍵暗号式によるデータ暗号化のアルゴリズムの1つである。DESは、共通鍵暗号式によるデータ暗号化のアルゴリズムの1つである。耐量子暗号、RSAおよびDESなどの暗号方式は、暗号処理を実行するために必要となる計算量などが異なる。一般に、耐量子暗号は、RSAおよびDESに比べて、暗号強度が強く（セキュリティレベルが高く）、暗号処理の処理負荷（計算量）が大きくなる。

[0032] 図3は、実施形態に係るICカード1が複数の暗号方式ごとの状態（有効性）を示す設定情報を記憶するNVM14の記憶領域を模式的に示す図である。また、図4は、実施形態に係るICカード1が選択（設定）中の暗号方式を示す設定情報（暗号方式識別フラグ）を記憶するRAM12の記憶領域を模式的に示す図である。

図3に示すように、ICカード1のNVM14には、既存暗号方式が有効か無効かを示す情報と新暗号方式が有効か無効かを示す情報を記憶する記憶領域を有する。例えば、既存暗号方式と新暗号方式とが共に有効である場合、NVM14は、暗号方式の設定情報（フラグ）として、既存暗号方式が有効であることを示す情報と新暗号方式が有効であることを示す情報とを記憶する。また、新暗号方式が有効なままで既存暗号方式が無効に設定された場合、NVM14は、既存暗号方式が無効で、新暗号方式が有効であることを示す設定情報を記憶する。

[0033] また、ICカード1のRAM12には、選択中の暗号方式を示す情報が暗号方式識別フラグとして記憶される。図4に示す例によれば、ICカード1は、暗号方式識別フラグが新暗号方式を示す状態（「11」）である場合には暗号方式として新暗号方式（新暗号方式での暗号処理）が選択されている

ことを示し、暗号方式識別フラグが既存暗号方式を示す状態（「２２」）である場合には暗号方式として新暗号方式（新暗号方式での暗号処理）が選択されていることを示す。

[0034] なお、既存暗号方式と新暗号方式との共存に期限がない場合は、何れかの暗号方式を無効とする必要がないので、上述したような何れかの暗号方式を無効にするような設定がなくても良い。例えば、ＩＣカード１がクレジットカードなどとして発行される場合、運用上の有効期限までに何れかの暗号方式を無効とするような運用計画が無ければ、当該ＩＣカード１は、何れかの暗号方式を無効にするような設定が無くても良い。

[0035] 次に、実施形態に係る携帯可能電子装置としてのＩＣカード１がＩＣカード処理装置２からのコマンドに応じて暗号方式を選択する処理を含む動作例（第１乃至第３の動作例）について説明する。

まず、実施形態に係る携帯可能電子装置としてのＩＣカード１による第１の動作例について説明する。

図５は、実施形態に係る携帯可能電子装置としてのＩＣカード１による第１の動作例の流れを説明するためのフローチャートである。

ＩＣカード１は、通信制御部１５によりインターフェース１６を介してＩＣカード処理装置２に接続する。ＩＣカード１のプロセッサ１１は、ＩＣカード処理装置２と接続すると、ＩＣカード処理装置２から供給される電力によって起動する。

[0036] ＩＣカード１のプロセッサ１１は、ＩＣカード処理装置２からのリセット要求（コマンド）に応じてリセットを実行する。ＩＣカード１のプロセッサ１１は、ＩＣカード処理装置２からの要求に応じて実行するリセットの種別を判別する（ステップＳＴ１１）。図５に示す例において、プロセッサ１１は、リセットがコールド（ＣＯＬＤ）リセットかウォーム（ＷＡＲＭ）リセットかを判別する。

[0037] ここで、コールドリセットは、各種メモリやプログラムなどの初期状態として起動（リセット）する動作である。ウォームリセットは、メモリが保持

する情報やプログラムを初期状態とすることなく起動（リセット）する動作である。例えば、コールドリセットは、電源がオフの状態からオンとなった直後に実行され、ウォームリセットは、電源がオンの状態においてメモリが保持する情報やプログラムの状態を維持したままで実行される起動動作である。例えば、ＩＣカード１におけるコールドリセットおよびウォームリセットは、ＩＳＯ／ＩＥＣ 7816-3に定義されるもので良い。

[0038] プロセッサ１１は、ＩＣカード処理装置２からコールドリセットが要求された場合（ステップＳＴ１１、ＹＥＳ）、コールドリセットを実行する（ステップＳＴ１２）。プロセッサ１１は、コールドリセットにおいて、暗号処理に用いる暗号方式として新暗号方式をセットする（ステップＳＴ１３）。例えば、プロセッサ１１は、ＲＡＭ１２に格納する暗号方式識別フラグとして新暗号方式を示すデータをセットする。プロセッサ１１は、コールドリセットが完了すると、コールドリセットが完了したことを示す応答（ＡＴＲ；Answer To Reset）をＩＣカード処理装置２へ送信する（ステップＳＴ１４）。

[0039] プロセッサ１１は、ＩＣカード処理装置２からウォームリセットが要求された場合（ステップＳＴ１１、ＮＯ）、ウォームリセットを実行する（ステップＳＴ１５）。ここで、ウォームリセットを要求するタイミングは、ＩＣカード処理装置２がＩＣカード１に対する処理に応じて要求する。プロセッサ１１は、ウォームリセットの動作において、暗号処理に用いる暗号方式として既存暗号方式をセットする（ステップＳＴ１６）。例えば、プロセッサ１１は、ＲＡＭ１２に格納する暗号方式識別フラグとして既存暗号方式を示すデータをセットする。プロセッサ１１は、ウォームリセットが完了すると、ウォームリセットが完了したことを示す応答（ＡＴＲ）をＩＣカード処理装置２へ送信する（ステップＳＴ１７）。

[0040] ＩＣカード１のプロセッサ１１は、リセット動作を実行した後、ＩＣカード処理装置２からの各種のコマンドを受け付ける（ステップＳＴ１８）。

[0041] また、プロセッサ１１は、コマンドを受信した場合には、コマンドに応じ

て処理（コマンド処理）を実行する（ステップS T 1 9）。ここで、コマンド処理については、後で詳細に説明するものとする。プロセッサ1 1は、コマンド処理の結果を示すレスポンスを送信し（ステップS T 2 0）、ステップS T 1 8へ戻り、コマンド待ちの状態とする。

- [0042] 上述したように、第1の動作例に係るI Cカードは、I Cカード処理装置から要求されるリセットの種別に応じて選択する暗号方式をリセット動作において設定する。例えば、I Cカードは、I Cカード処理装置からコールドリセットが要求された場合にはコールドリセットの動作において第2暗号方式としての新暗号方式をセットし、I Cカード処理装置からウォームリセットが要求された場合にはウォームリセットの動作において第1暗号方式としての既存暗号方式をセットする。
- [0043] なお、上述した第2暗号方式と第1暗号方式とは、上述した例とは逆にしても良い。すなわち、I Cカードは、I Cカード処理装置からコールドリセットが要求された場合にコールドリセットの動作において第2暗号方式としての既存暗号方式をセットし、I Cカード処理装置からウォームリセットが要求された場合にはウォームリセットの動作において第1暗号方式としての新暗号方式をセットするようにしても良い。
- [0044] このような第1の動作例によれば、I Cカードは、I Cカード処理装置から要求されるリセットの種別に応じて暗号方式を設定することができる。これに対応して、I Cカード処理装置としては、I Cカードに要求するリセットの種別によって暗号方式を指定することができる。
- [0045] 具体例として、I Cカードは、I Cカード処理装置からのコールドリセットの要求に応じてコールドリセット動作を行う場合に新暗号方式を設定し、I Cカード処理装置からのウォームリセットの要求に応じてウォームリセット動作を行う場合に既存暗号方式を設定するようにできる。言い換えると、I Cカード処理装置は、各種の情報がデフォルト状態となるコールドリセットにおいて耐量子暗号などの暗号強度が強い新暗号方式をI Cカードにセットすることができ、各種の情報が保持されたままで実行されるウォームリセ

ットで既存暗号方式をＩＣカードにセットすることができる。

[0046] 次に、実施形態に係る携帯可能電子装置としてのＩＣカード１による第２の動作例について説明する。

図６は、実施形態に係る携帯可能電子装置としてのＩＣカード１による第２の動作例の流れを説明するためのフローチャートである。

ＩＣカード１は、通信制御部１５によりインターフェース１６を介してＩＣカード処理装置２に接続し、ＩＣカード処理装置２から供給される電力によって起動する。ＩＣカード１のプロセッサ１１は、ＩＣカード処理装置２からのリセット要求に応じてリセットを実行する（ステップＳＴ３１）。

[0047] プロセッサ１１は、リセット動作が完了すると、リセット応答（ＡＴＲ）をＩＣカード処理装置２へ送信する（ステップＳＴ３２）。例えば、プロセッサ１１は、ＩＣカード処理装置２からコールドリセットが要求された場合にはコールドリセットを実行してコールドリセットに対応したＡＴＲを送信し、ＩＣカード処理装置２からウォームリセットが要求された場合にはウォームリセットを実行してウォームリセットに対応したＡＴＲを送信する。

[0048] また、プロセッサ１１は、ＡＴＲを送信する場合、ＩＣカード処理装置２へ送信するＡＴＲに対応した通信レート（通信速度）を含む通信条件を設定し（ステップＳＴ３３）、当該ＩＣカード１のデフォルト設定の暗号方式である既存暗号方式をセットする（ステップＳＴ３４）。プロセッサ１１は、通信条件および暗号方式を設定すると、ＩＣカード処理装置２からの各種のコマンドを受け付ける。

[0049] プロセッサ１１は、ＩＣカード処理装置２からのコマンドとして通信レートなどの通信条件の設定（変更）要求を受信すると（ステップＳＴ３５、ＹＥＳ）、当該コマンドに応じて通信条件を変更する（ステップＳＴ３６）。例えば、接触式ＩＣカードの規格であるＩＳＯ／ＩＥＣ 7816-3によれば、ＩＣカード処理装置２は、ＩＣカード１に対してＰＰＳ request というコマンドによって通信レートの設定を要求する。これに対して、ＩＣカード１は、ＰＰＳ request で要求された通信レートに変更して

PPS responseという応答をICカード処理装置2へ返す。なお、ICカード1が非接触式ICカードである場合、ISO/IEC14443-4に規定されるPPS requestおよびPPS responseによって通信レートの変更が行える。

[0050] ICカード1のプロセッサ11は、通信条件を変更すると、新暗号方式が設定される通信条件に変更されたか否かを判断する（ステップST37）。例えば、新暗号方式を設定すべき通信レートなどの通信条件を示す設定情報はNVM14などに記憶される。プロセッサ11は、NVM14に記憶した設定情報に基づいて通信レートなどの通信条件が新暗号方式を設定すべき通信条件であるか否かを判断する。

[0051] プロセッサ11は、通信条件が新暗号方式を設定すべき通信条件に変更された場合（ステップST37、YES）、暗号処理に用いる暗号方式を新暗号方式にセットする（ステップST38）。また、プロセッサ11は、通信条件が新暗号方式を設定すべき通信条件でない場合（ステップST37、NO）、暗号処理に用いる暗号方式を既存暗号方式のままとする。

[0052] また、ICカード1のプロセッサ11は、ICカード処理装置2から通信レートの設定要求以外のコマンドを受信した場合（ステップST39）、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（ステップST40）。プロセッサ11は、コマンド処理を実行すると、コマンド処理の結果としてのレスポンスを送信し（ステップST41）、ステップST35へ戻り、コマンド待ち状態とする。

[0053] 上述したように、第2の動作例に係るICカードは、リセット動作においてデフォルト設定の既存暗号方式（第1の処理方式）を設定し、ICカード処理装置から要求（コマンド）に応じて変更した通信条件が新暗号方式（第2の処理方式）を設定すべき通信条件であれば、暗号処理に用いる暗号方式を新暗号方式に変更する。

[0054] このような第2の動作例によれば、ICカードは、ICカード処理装置から要求される通信設定に応じて暗号方式を設定することができ、ICカード

処理装置からの通信設定の変更に応じて暗号方式を切り替えるようにすることができる。これに対応して、ＩＣカード処理装置としては、任意のタイミングでＩＣカードに要求する通信条件（通信レート）によってＩＣカードの暗号方式を指定できる。

[0055] 具体例として、ＩＣカードは、ＩＣカード処理装置からの要求に応じて通信レートを高速化する場合に、コマンド処理で暗号処理に用いる暗号方式を新暗号方式に切り替えることができる。新暗号方式は、暗号に必要なデータが大きくなることが想定されるため、高速通信で実施することにより利便性が向上する。また、ＩＣカードは、デフォルト状態で既存暗号方式が設定されるようにすることで、既存暗号方式を用いて処理を行う既存のシステムがそのまま利用できる。

[0056] 次に、実施形態に係る携帯可能電子装置としてのＩＣカード１による第３の動作例について説明する。

図７は、実施形態に係る携帯可能電子装置としてのＩＣカード１による第３の動作例の流れを説明するためのフローチャートである。

ここで、図７に示す第３の動作例に係るＩＣカード１は、複数の通信方式（通信プロトコル）に対応し、ＩＣカード処理装置２からの要求に応じて何れかの１つの通信方式を切り替える機能があるものとする。例えば、ＩＳＯ／ＩＥＣ 14443-3で規定される非接触式ＩＣカードでは、通信方式として「Type A」、「Type B」などがある。ＩＣカード処理装置２は、少なくとも１つ以上の通信方式をサポートし、処理対象とするＩＣカードと通信を行う。

[0057] ＩＣカード１のプロセッサ１１は、ＩＣカード処理装置２から通信方式（通信プロトコル）のリクエストを受信した場合（ステップＳＴ５１、ＹＥＳ）、ＩＣカード処理装置２からのリクエストに応じてサポート可能な通信条件を示すレスポンスを送信する（ステップＳＴ５２）。例えば、ＩＣカード処理装置２は、「Type B」の場合にはREQB（REQUEST command, Type B）というコマンドをＩＣカード１へ送信する。

これに対して、ＩＣカード１のプロセッサ１１は、ＡＴＱＢ（Ａｎｓｗｅｒ
ｔｏ Ｒｅｑｕｅｓｔ, Ｔｙｐｅ Ｂ）というレスポンスを返信する。
ここで、ＡＴＱＢのレスポンスでは、ＩＣカード処理装置２とＩＣカード１
との間でサポート可能な複数の通信速度、および、通信データのバッファサ
イズ等の通信条件が示される。

[0058] また、ＩＣカード１のプロセッサ１１は、ＩＣカード処理装置２から通信
条件を指定するコマンドを受信し、指定された通信条件での通信設定を行う
（ステップＳＴ５３）。例えば、ＩＣカード処理装置２は、ＩＣカード１か
らの上述したようなＡＴＱＢで示される複数の通信速度から通信条件として
のパラメータ（通信速度、バッファサイズなど）を選択し、選択した通信条
件を指定するＡＴＴＲＩＢ（ＰＩＣＣ ｓｅｌｅｃｔｉｏｎ ｃｏｍｍａｎｄ, Ｔｙｐｅ Ｂ）コマンドをＩＣカードへ送信する。ＩＣカード１のプロ
セッサ１１は、ＩＣカード処理装置２からのＡＴＴＲＩＢで指定される通
信条件を設定し、Ａｎｓｗｅｒ ｔｏ ＡＴＴＲＩＢ ｃｏｍｍａｎｄでレ
スポンスする。これにより、ＩＣカード１は、ＩＣカード処理装置２に指定
されたパラメータ（通信速度、バッファサイズなど）で通信を行う。

[0059] ＩＣカード１のプロセッサ１１は、ＩＣカード処理装置２が指定する通信
条件を設定すると、設定した通信方式および通信条件に応じた暗号方式を選
択する（ステップＳＴ５４）。例えば、ＩＣカード１のプロセッサ１１は、
ＡＴＴＲＩＢコマンドで指定されたパラメータ（例えば、通信速度、バッ
ファサイズなど）により既存暗号方式又は新規暗号方式の何れかを選択する。

[0060] 例えば、ＩＣカード１のプロセッサ１１は、ＮＶＭ１４などのメモリに記
憶した通信方式ごとの設定情報に基づいて通信条件に暗号方式を選択する。
具体例として、Ｔｙｐｅ Ｂでは、通信速度が１０６ｋｂｐｓであれば既存暗
号方式をセットし、１０６ｋｂｐｓ以外であれば新規暗号方式をセットする
ような設定情報をＮＶＭ１４に記憶する。このような設定情報が記憶された
ＩＣカード１は、ＡＴＴＲＩＢでの通信速度の指定が１０６ｋｂｐｓであれ
ば既存暗号方式をセットし、１０６ｋｂｐｓ以外であれば新規暗号方式をセ

ットする。

- [0061] すなわち、プロセッサ 11 は、通信方式および通信条件に応じて新暗号方式を選択する場合（ステップ S T 5 4、Y E S）、暗号処理を実行するための暗号方式として新暗号方式をセットする（ステップ S T 5 5）。また、プロセッサ 11 は、通信方式および通信条件に応じて既存暗号方式を選択する場合（ステップ S T 5 4、N O）、暗号処理を実行するための暗号方式として既存暗号方式をセットする（ステップ S T 5 6）。
- [0062] また、I C カード 1 のプロセッサ 11 は、I C カード処理装置 2 から通信方式のリクエスト以外のコマンドを受信した場合（ステップ S T 5 7、Y E S）、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（ステップ S T 5 8）。プロセッサ 11 は、コマンド処理を実行すると、コマンド処理の結果を示すレスポンスを送信し（ステップ S T 5 9）、ステップ S T 5 1 へ戻り、通信設定要求又はそれ以外のコマンドを受信待ちとする状態になる。
- [0063] 上述したように、第 3 の動作例に係る I C カードは、通信方式（通信プロトコル）ごとに暗号方式を選択するための通信条件を示す設定情報を保持し、通信方式が設定された（切り替えられた）場合に通信方式ごとの設定情報に基づいて処理方式（暗号方式）を設定する。I C カード処理装置としては、I C カードの通信方式を指定する場合に指定した通信方式での通信条件によって当該 I C カードにセットする処理方式を指定する。
- [0064] このような第 3 の動作例によれば、I C カードは、I C カード処理装置から要求される通信方式ごとに通信条件に応じて特定の処理を実行するための処理方式を設定することができ、通信方式ごとに設定する設定情報によって処理方式を切り替えることができる。また、I C カード処理装置としては、通信方式ごとの通信条件によって I C カードの処理方式を指定できる。
- [0065] 次に、実施形態に係る携帯可能電子装置としての I C カード 1 が I C カード処理装置 2 に自身が対応する暗号方式を通知する処理を含む動作例（第 4 の動作例）について説明する。

図8は、実施形態に係る携帯可能電子装置としてのICカード1による第4の動作例の流れを説明するためのフローチャートである。

第4の動作例は、ICカード1が有効となっている暗号方式（実行可能な暗号方式）をICカード処理装置2に通知する処理を含む動作の例である。

[0066] 図8に示す例において、まず、ICカード1のプロセッサ11は、ICカード処理装置2から電力が供給された直後にリセット（コールドリセット）の要求を受信するものとする。プロセッサ11は、ICカード処理装置2からコールドリセットが要求された場合（ステップST61、YES）、コールドリセットを実行する（ステップST62）。プロセッサ11は、コールドリセットにおいて暗号処理に用いる暗号方式として新暗号方式をセットする（ステップST63）。プロセッサ11は、コールドリセットが完了すると、コールドリセットが完了したことを示す応答（ATR）をICカード処理装置2へ送信する（ステップST64）。

[0067] ICカード1のプロセッサ11は、リセット動作を実行した後、ICカード処理装置2からの各種のコマンドを受け付ける（ステップST69）。プロセッサ11は、ICカード処理装置2からリセット要求以外のコマンドを受信した場合（ステップST70、YES）、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（ステップST71）。

[0068] プロセッサ11は、コマンド処理を実行すると、既存暗号方式（デフォルト（コールドリセット）でセットされる新暗号方式とは別の暗号方式）が有効であるか否かを判定する（ステップST72）。例えば、プロセッサ11は、NVM14に記憶する暗号方式設定フラグを示す情報に基づいて既存暗号方式が有効か無効かを判定する。

[0069] プロセッサ11は、既存暗号方式が有効である場合（ステップST72、YES）、コマンド処理の結果を示すレスポンスデータに既存暗号方式が有効であることを示す情報をセットする（ステップST73）。プロセッサ11は、既存暗号方式が有効であることを示すデータをセットしたレスポンスデータをICカード処理装置2へ送信し（ステップST75）、ステップS

T 6 9 へ戻り、コマンド待ちの状態となる。なお、既存暗号方式が有効であることを示す情報は、コマンド処理の結果を示すステータスワードに既存暗号方式が有効であることを示す情報を含めても良いし、レスポンスデータに既存暗号方式が有効であることを示すデータを設定しても良い。

[0070] また、プロセッサ 1 1 は、既存暗号方式が有効でない場合（ステップ S T 7 2、N O）、コマンド処理の結果を示すレスポンスデータに既存暗号方式が無効であることを示すデータをセットする（ステップ S T 7 4）。プロセッサ 1 1 は、既存暗号方式が無効であることを示すデータをセットしたレスポンスデータを I C カード処理装置 2 へ送信し（ステップ S T 7 5）、ステップ S T 6 9 へ戻り、コマンド待ちの状態となる。

[0071] ただし、プロセッサ 1 1 は、ステップ S T 7 3－S T 7 5 の処理として、既存暗号方式が有効性でかつコマンド処理の結果が異常である場合は、通常の異常を意味するレスポンスデータを送信し、既存暗号方式が有効性でかつコマンド処理の結果が正常である場合は、処理結果は正常で既存暗号方式が有効であることを意味するようなレスポンスデータを送信するようにして良い。

[0072] なお、上述した第 4 の動作例は、第 1 の動作例で説明したようなりセットの種別に応じて暗号方式をセットする動作において、コマンドに対する応答で暗号方式の有効性を通知する例について説明したが、図 8 に示す動作例において、セットする暗号方式を選択する動作は、第 2 の動作例又は第 3 の動作例で説明した動作を適用しても良い。つまり、リセット種別に応じて暗号方式をセットする動作を通信レートなどの通信条件に応じて暗号方式をセットする動作に置き換えて実施しても良い。

[0073] また、上述した第 4 の動作例では、I C カード 1 は、コールドリセット（デフォルト状態）でセットされる暗号方式が新暗号方式であること前提に説明している。このため、I C カード 1 は、ステップ S T 7 2－7 4 の処理（コマンドに対する応答処理）において、デフォルト状態（コールドリセット）でセットされる新暗号方式とは別の暗号方式である既存暗号方式が有効で

あるか否かを示す情報を含むコマンド応答をＩＣカード処理装置２へ送信する。

[0074] このような第４の動作例は、変形例として、ＩＣカード１がデフォルト状態で既存暗号方式がセットされる運用とする場合にも適用できる。すなわち、ＩＣカード１がデフォルト状態で既存暗号方式がセットされる運用とする場合、ＩＣカード１は、ステップＳＴ７２－７４のコマンドに対する応答処理において、デフォルト状態でセットされる既存暗号方式とは別の暗号方式である新暗号方式が有効であるか否かを示す情報を含むコマンド応答をＩＣカード処理装置２へ送信するようにしても良い。

[0075] さらに変形例として、上述した第４の動作例は、ＩＣカード１がデフォルト状態でセットする暗号方式によらず、コマンドの処理結果を示す応答において当該ＩＣカード１が対応する各暗号方式（新暗号方式および既存暗号方式）の有効性を示す情報を含むコマンド応答を出力するようにしても良い。すなわち、第４の動作例は、ステップＳＴ７２－７４の処理を、各暗号方式（新暗号方式および既存暗号方式）の有効性を示す情報を含むコマンド応答を出力する処理に置き換えて実施しても良い。

[0076] 上述したように、第４の動作例に係るＩＣカードは、ＩＣカード処理装置からのコマンドに対するコマンド処理を実行した場合に当該ＩＣカードにおける各暗号方式の有効性を示す情報を含むレスポンスを出力する。このような第４の動作例によれば、ＩＣカードは、コマンド処理に対する応答において当該ＩＣカードが実行可能な暗号方式を示す情報をＩＣカード処理装置へ送信できる。

[0077] また、上述した第４の動作例に係るＩＣカードは、デフォルト状態でセットされる暗号方式とは別の暗号方式が有効か否かを示す情報を含むコマンド処理の結果を示す応答を出力する。このような第４の動作例によれば、ＩＣカードは、コマンド処理に対する応答においてデフォルト状態で設定される暗号方式とは別の暗号方式が有効であるか否かを示す情報をＩＣカード処理装置へ送信できる。

[0078] 次に、実施形態に係る携帯可能電子装置としてのＩＣカード１がコマンド処理として特定の暗号方式を無効化する処理の動作例（第５の動作例）について説明する。

図９は、実施形態に係る携帯可能電子装置としてのＩＣカード１による第５の動作例の流れを説明するためのフローチャートである。

図９は、図５乃至図８におけるコマンド処理の１つとして実行される特定の暗号方式を無効化する処理の例を第５の動作例として説明するためのフローチャートである。第５の動作例において、ＩＣカード１は、対応する複数の暗号方式のうちＩＣカード処理装置２が指定する特定の暗号方式を無効化する処理を行う。

ＩＣカード１のプロセッサ１１は、上述した図５乃至８に示す処理においてＩＣカード処理装置２からのコマンドを受信すると、コマンド処理を実行する。

[0079] プロセッサ１１は、ＩＣカード処理装置２からコマンドを受信すると、受信したコマンドが暗号方式の無効化を要求するコマンドであるか否かを判断する（ステップＳＴ８１）。例えば、プロセッサ１１は、受信したコマンドが後述する図１１などに示すようなフォーマットである場合、コマンドの識別情報である「ＣＬＡ／ＩＮＳ」に暗号方式の無効化を要求することを示すデータがセットされているか否かにより受信したコマンドが暗号方式の無効化を要求するか否かを判断する。具体例として、ＩＣカード処理装置２は、ＩＣカード１の既存暗号方式を無効化する場合に既存暗号方式の無効化を要求するコマンドをＩＣカード１へ送信する。これにより、ＩＣカード１のプロセッサ１１は、既存暗号方式の無効化を要求するコマンドを受信する。

[0080] プロセッサ１１は、特定の暗号方式の無効化を要求するコマンドを受信した場合（ステップＳＴ８１、ＹＥＳ）、受信したコマンドで指定される暗号方式を無効化する処理を行う（ステップＳＴ８２）。例えば、プロセッサ１１は、コマンドで指定された暗号方式の無効を示す情報をＮＶＭ１４に記憶することにより指定された暗号方式を無効化する。具体例として、既存暗号

方式の無効化を要求するコマンドを受信した場合、ＩＣカード１のプロセッサ１１は、図３に示すようなＮＶＭ１４における暗号方式設定フラグを既存暗号方式の無効を示す情報に更新することにより既存暗号方式を無効化する。

- [0081] プロセッサ１１は、コマンドで指定された暗号方式を無効化すると、コマンド処理の結果を示すデータとして、指定された暗号方式を無効化したことを示す情報を含むレスポンスデータを生成する（ステップＳＴ８４）。プロセッサ１１は、レスポンスデータを生成すると、図５乃至８で示すように、コマンド処理の結果を示すレスポンスデータをＩＣカード処理装置２へ送信する。これにより、コマンドの送信元であるＩＣカード処理装置２は、ＩＣカード１において指定の暗号方式が無効化されたことを確認する。
- [0082] また、プロセッサ１１は、暗号方式の無効化を要求するコマンド以外のコマンドを受信した場合（ステップＳＴ８１、ＮＯ）、受信したコマンドに応じた処理（コマンド処理）を実行し（ステップＳＴ８３）、コマンド処理の結果を示すレスポンスデータを生成する（ステップＳＴ８４）。
- [0083] 上述したように、第５の動作例に係るＩＣカードは、ＩＣカード処理装置から要求されるコマンドに応じて指定された暗号方式を無効化する。これにより、複数の暗号方式に対応するＩＣカードは、ＩＣカード処理装置からのコマンドによって特定の暗号方式を無効化することができる。この結果、複数の暗号方式が実行可能なＩＣカードを発行処理した後であっても脆弱性が発見された特定の暗号方式をＩＣカード処理装置からのコマンドで無効化することができる。
- [0084] 例えば、第５の動作例に係るＩＣカードは、ＩＣカード処理装置から既存暗号方式の無効化が要求するコマンドを受信した場合、受信したコマンドに応じて既存暗号方式を無効化する。これにより、既存暗号方式から新暗号方式へ移行期間において既存暗号方式と新暗号方式とが実行可能なＩＣカードを発行した場合であっても、移行期間が終了した後に既存暗号方式を無効化する運用が可能となる。この結果、移行時間後に暗号強度が弱い既存暗号方

式による暗号方式を無効化することができ、既存暗号方式と新暗号方式とを並存させる移行期間での運用と移行期間終了後の運用とを円滑に実施することが可能となる。

[0085] また、上述した第5の動作例によれば、新暗号方式と既存暗号方式とに対応するICカードがICカード処理装置からのコマンドに応じて新暗号方式よりも暗号強度の弱い既存暗号方式を無効化するようにもできる。この結果、ICカードは、ICカードとICカード処理装置とを有するシステム全体が既存暗号方式から新暗号方式に移行する移行期間において既存暗号方式と新暗号方式とから選択する何れかの暗号方式を用いて暗号処理を実施し、移行期間が終了した場合に暗号強度が弱い既存暗号方式を無効化するという運用が可能となる。

[0086] 次に、実施形態に係る携帯可能電子装置としてのICカード1が暗号処理を含む処理を要求するコマンド処理の一例である署名検証コマンドを受信した場合の処理を含む動作例（第6の動作例）について説明する。

図10は、実施形態に係る携帯可能電子装置としてのICカード1による第6の動作例の流れを説明するためのフローチャートである。

第6の動作例は、ICカード1が複数の暗号方式から1つの暗号方式を設定しておき、暗号処理を含む処理のコマンドを受信した場合には設定されている暗号方式で暗号処理を含む処理を実行する。言い換えると、第6の動作例において、暗号処理を含む処理のコマンド（署名検証コマンド）は、どの暗号方式が設定されている場合であっても同じ内容（同じデータもしくは同じデータに相当するデータをセットしたコマンド）であるものとする。

[0087] 図10に示す動作例において、ICカード1のプロセッサ11は、まず、ICカード処理装置2からのリセット要求に応じてリセットを実行する（ステップST90）。プロセッサ11は、リセット動作が完了すると、リセット応答（ATR）をICカード処理装置2へ送信する（ステップST91）。また、プロセッサ11は、ATRを送信する場合、ICカード処理装置2へ送信するATRに対応した通信レートなどを含む通信条件を設定する（ス

テップST92)。プロセッサ11は、通信条件を設定すると、ICカード処理装置2からの各種のコマンドを受け付ける（ステップST93）。

[0088] ICカード1のプロセッサ11は、コマンドを受信すると（ステップST93、YES）、受信したコマンドが暗号処理を含む処理を要求するコマンドであるか否かを判断する（ステップST94）。暗号処理を含む処理を要求するコマンドの一例が署名検証コマンドである。ここでは、図10に示すように暗号処理を含む処理を要求するコマンドが署名検証コマンドであることを想定して説明するものとする。

[0089] 図11は、暗号処理を含む処理を要求するコマンドの一例である署名検証コマンドのフォーマットの構成例を示す図である。

図11に示すようなコマンドのフォーマットは、コマンドの識別情報である「CLA/INS」とパラメータである「P1P2」とを含む。図11は、署名検証コマンドの例を示すものであり、署名検証コマンドは「CLA/INS」に「0088」がセットされる例を示す。つまり、「CLA/INS」が「0088」のコマンドは、署名検証コマンドを示す。第6の動作例では、暗号方式によらずに、図11に示すような署名検証コマンドが用いられる。言い換えると、第6の動作例では、署名検証コマンドは、図11に示すような既存暗号方式および新暗号方式で共通のコマンドとなる。

[0090] プロセッサ11は、受信したコマンドが暗号処理を含む処理を要求するコマンド（署名検証コマンド）である場合（ステップST94、YES）、当該ICカード1が通信条件に応じて選択する暗号方式が新暗号方式であるか既存暗号方式であるかを判断する（ステップST95）。プロセッサ11は、通信条件に応じて選択する暗号方式が新暗号方式である場合（ステップST95、YES）、署名検証コマンドに応じて新暗号方式による暗号処理を含む処理としての署名検証の処理を実行する（ステップST96）。プロセッサ11は、新暗号方式による暗号処理を含む署名検証を実行すると、署名検証の処理結果を示すレスポンスデータをICカード処理装置2へ送信する（ステップST99）。

- [0091] また、プロセッサ11は、当該ICカード1にセットされている暗号方式が既存暗号方式である場合（ステップST95、NO）、署名検証コマンドに応じて既存暗号方式による暗号処理を含む処理としての署名検証の処理を実行する（ステップST98）。プロセッサ11は、既存暗号方式による暗号処理を含む署名検証を実行すると、署名検証の処理結果を示すレスポンスデータをICカード処理装置2へ送信する（ステップST99）。
- [0092] また、プロセッサ11は、受信したコマンドが暗号処理を含む処理を要求するコマンド（署名検証コマンド）以外のコマンドを受信した場合（ステップST94、NO）、受信したコマンドに応じた処理を実行し（ステップST97）、コマンド処理の結果を示すレスポンスデータをICカード処理装置2へ送信する（ステップST99）。
- [0093] 上述したように、第6の動作例に係るICカードは、ICカードに設定済み（選択中）の暗号方式で暗号処理を実行する。これにより、ICカードは、暗号処理を含む処理を要求するコマンドから暗号処理に用いる暗号方式を特定（識別）する必要なく、ICカード処理装置は、暗号処理に用いる暗号方式を指定するためにコマンドのデータを変更する必要がない。例えば、第6の動作例に係るICカードは、第1の動作例と組み合わせ実施すれば、リセット動作において暗号方式を設定すればよく、暗号処理を要求するコマンドにおいて暗号方式を指定することが不要となる。
- [0094] 次に、実施形態に係る携帯可能電子装置としてのICカード1が暗号処理を含む処理を要求するコマンドの一例である署名検証コマンドを受信した場合の動作例（第7の動作例）について説明する。

図12は、実施形態に係る携帯可能電子装置としてのICカード1による第7の動作例の流れを説明するためのフローチャートである。

第7の動作例は、ICカード1は、暗号処理を含む処理のコマンド（一例として署名検証コマンドとする）におけるパラメータで指定される暗号方式で暗号処理を実行する。言い換えると、第7の動作例のICカードは、暗号処理を含む処理のコマンドにおけるパラメータによって暗号処理にどの暗号

方式を使用するかを特定するものである。

[0095] 図12に示す動作例において、ICカード1のプロセッサ11は、まず、ICカード処理装置2からのリセット要求に応じてリセットを実行する（ステップST100）。プロセッサ11は、リセット動作が完了すると、リセット応答（ATR）をICカード処理装置2へ送信する（ステップST101）。また、プロセッサ11は、ATRを送信する場合、ICカード処理装置2へ送信するATRに対応した通信レートなどを含む通信条件を設定する（ステップST102）。プロセッサ11は、通信条件を設定すると、ICカード処理装置2からの各種のコマンドを受け付ける（ステップST103）。

[0096] ICカード1のプロセッサ11は、ICカード処理装置2からのコマンドを受信すると（ステップST103、YES）、受信したコマンドが暗号処理を含む処理を要求するコマンド（署名検証コマンド）であるか否かを判断する（ステップST104）。プロセッサ11は、署名検証コマンド以外のコマンドを受信した場合（ステップST104、NO）、受信したコマンドに応じたコマンド処理を実行し（ステップST105）、そのコマンド処理の結果を示すレスポンスデータをICカード処理装置2へ送信する（ステップST111）。

[0097] また、プロセッサ11は、受信したコマンドが署名検証コマンドである場合（ステップST104、YES）、当該署名検証コマンドのパラメータにセットされているデータが新暗号方式を指定するか既存暗号方式を指定するかを判断する。すなわち、プロセッサ11は、受信した署名検証コマンドのパラメータに基づいて署名検証の暗号処理に用いる暗号方式を特定する。

[0098] 図13は、署名検証コマンドのパラメータに既存暗号方式を指定するデータをセットした例を示す図である。図14は、署名検証コマンドのパラメータに新暗号方式を指定するデータをセットした例を示す図である。

図13および図14に示す署名検証コマンドの例において、パラメータとしての「P1」および「P2」は、以下のように定義されるものとする。

「P 2」は、暗号方式を指定する。例えば、「P 2」が「0 1」である場合は既存暗号方式を指定するものとする。また、「P 2」が「0 2」である場合は新規暗号方式を指定するものとする。また、「P 1」は署名データに使用する鍵の識別子が示されるものとする。この場合、「P 1」が「0 1」であれば「0 1」というIDの鍵データを使用することを示す。「P 1」が「0 2」であれば「0 2」というIDの鍵データを使用することを示す。なお、鍵データは、ICカード1内のNVMなどのメモリに識別子と共に格納されているものとする。

[0099] 具体例として、図13に示す例では、署名検証コマンドのパラメータ「P 1」「P 2」にセットされているデータが「0 1」「0 1」であるため、暗号方式が既存暗号方式であり、鍵データのIDが「0 1」であることを示す。また、図14に示す例では、署名検証コマンドのパラメータ「P 1」「P 2」にセットされているデータが「0 3」「0 2」であるため、暗号方式が新暗号方式であり、鍵データのIDが「0 3」であることを示す。

[0100] プロセッサ11は、当該署名検証コマンドのパラメータが新暗号方式である場合（ステップST106、YES）、署名検証コマンドに応じて新暗号方式による暗号処理を含む処理としての署名検証の処理を実行する（ステップST107）。プロセッサ11は、新暗号方式による暗号処理を含む署名検証を実行すると、署名検証の処理結果を示すレスポンスデータをICカード処理装置2へ送信する（ステップST111）。

[0101] また、プロセッサ11は、当該署名検証コマンドのパラメータが新暗号方式でない場合（ステップST106、NO）、当該署名検証コマンドのパラメータが既存暗号方式であるか否かを判断する（ステップST108）。プロセッサ11は、当該署名検証コマンドのパラメータが既存暗号方式である場合（ステップST108、YES）、署名検証コマンドに応じて既存暗号方式による暗号処理を含む処理としての署名検証の処理を実行する（ステップST109）。プロセッサ11は、既存暗号方式による暗号処理を含む署名検証を実行すると、署名検証の処理結果を示すレスポンスデータをICカ

ード処理装置2へ送信する（ステップST111）。

[0102] また、プロセッサ11は、当該署名検証コマンドのパラメータが新暗号方式でも既存暗号方式でもない場合（ステップST108、NO）、当該署名検証コマンドのパラメータがエラー（異常値）であるとする（ステップST110）。プロセッサ11は、受信した署名検証コマンドのパラメータがエラーである場合、署名検証コマンドのパラメータが異常であることを示すレスポンスデータをICカード処理装置2へ送信する（ステップST111）。

[0103] 上述したように、第7の動作例に係るICカードは、受信した署名検証コマンドのパラメータによって暗号方式を特定し、パラメータで指定される暗号方式を用いた暗号処理を含む署名検証を実行する。これにより、ICカードは、暗号処理を含む処理を要求するコマンドのパラメータで暗号処理に用いる暗号方式を特定することができる。ICカード処理装置は、暗号処理を含む処理を要求するごとに、コマンドのパラメータで暗号処理に用いる暗号方式を指定できる。

[0104] 次に、実施形態に係る携帯可能電子装置としてのICカード1が暗号処理を含む処理を要求するコマンド処理の一例である署名検証コマンドを受信した場合の処理を含む動作例（第8の動作例）について説明する。

図15は、実施形態に係る携帯可能電子装置としてのICカード1による第8の動作例の流れを説明するためのフローチャートである。

第8の動作例は、暗号方式ごとに署名検証コマンドの識別情報（CLA/INS）が定義される場合の動作例である。ICカード1は、ICカード処理装置2から受信するコマンドの識別情報によって既存暗号方式での署名検証コマンドか新暗号方式での署名検証コマンドかを判断する。言い換えると、第8の動作例のICカードは、暗号方式ごとに署名検証コマンドが定義されるため、署名検証コマンドの識別情報によって暗号処理に用いる暗号方式を特定するものである。

[0105] 例えば、図16は、既存暗号方式を指定する署名検証コマンドの例を示す

図である。図 1 7 は、新暗号方式を指定する署名検証コマンドの例を示す図である。

図 1 6 および図 1 7 に示す署名検証コマンドでは、コマンドの識別情報である「CLA/INS」のデータ（値）が異なっている。図 1 6 に示すコマンドは、「CLA/INS」が「008A」となっている。図 1 6 に示すように、「CLA/INS」が「008A」のコマンドが既存暗号方式による署名検証コマンドと定義される。また、図 1 7 に示すコマンドは、「CLA/INS」が「008C」となっている。図 1 7 に示すように、「CLA/INS」が「008C」のコマンドが新暗号方式による署名検証コマンドと定義される。

[0106] 図 1 5 に示す動作例において、IC カード 1 のプロセッサ 1 1 は、まず、IC カード処理装置 2 からのリセット要求に応じてリセットを実行する（ステップ ST 1 2 0）。プロセッサ 1 1 は、リセット動作が完了すると、リセット応答（ATR）を IC カード処理装置 2 へ送信する（ステップ ST 1 2 1）。また、プロセッサ 1 1 は、ATR を送信する場合、IC カード処理装置 2 へ送信する ATR に対応した通信レートなどを含む通信条件を設定する（ステップ ST 1 0 2）。プロセッサ 1 1 は、通信条件を設定すると、IC カード処理装置 2 からの各種のコマンドを受け付ける（ステップ ST 1 2 3）。

[0107] IC カード 1 のプロセッサ 1 1 は、IC カード処理装置 2 からコマンドを受信すると、受信したコマンドが新暗号方式による暗号処理を含む署名検証を要求するコマンド（署名検証コマンド）であるか否かを判断する（ステップ ST 1 2 4）。上述した図 1 6 に示す例によれば、プロセッサ 1 1 は、受信したコマンドの「CLA/INS」が「008C」であるか否かによって新暗号方式を指定する署名検証コマンドであるか否かを判断する。

[0108] プロセッサ 1 1 は、受信したコマンドが新暗号方式を指定する署名検証コマンドである場合（ステップ ST 1 2 4、YES）、当該コマンドに応じて新暗号方式による暗号処理を含む署名検証の処理を実行する（ステップ ST

125)。プロセッサ11は、新暗号方式による暗号処理を含む署名検証を実行すると、署名検証の処理結果を示すレスポンスデータをICカード処理装置2へ送信する(ステップST129)。

[0109] また、プロセッサ11は、受信したコマンドが新暗号方式を指定する署名検証コマンドでない場合(ステップST124、NO)、当該コマンドが既存暗号方式を指定する署名検証コマンドであるか否かを判断する(ステップST126)。プロセッサ11は、受信したコマンドが既存暗号方式を指定する署名検証コマンドである場合(ステップST126、YES)、当該コマンドに応じて既存暗号方式による暗号処理を含む署名検証の処理を実行する(ステップST127)。プロセッサ11は、既存暗号方式による暗号処理を含む署名検証を実行すると、署名検証の処理結果を示すレスポンスデータをICカード処理装置2へ送信する(ステップST129)。

[0110] また、プロセッサ11は、受信したコマンドが既存暗号方式を指定する署名検証コマンドでない場合、つまり、受信したコマンドが署名検証コマンドでない場合(ステップST126、NO)、受信したコマンドに応じたコマンド処理を実行し(ステップST128)、そのコマンド処理の結果を示すレスポンスデータをICカード処理装置2へ送信する(ステップST129)。

[0111] 上述したように、第8の動作例に係るICカードは、受信したコマンドの識別情報によってどの暗号方式を用いる署名検証コマンドであるかを識別し、指定された暗号方式による暗号処理を含む署名検証を実行する。具体例として、ICカードは、既存暗号方式を指定する署名検証コマンドを受信した場合には既存暗号方式を用いた暗号処理を含む署名検証を実行し、新暗号方式を指定する署名検証コマンドを受信した場合には新暗号方式を用いた暗号処理を含む署名検証を実行する。

[0112] これにより、ICカードは、暗号方式ごとに定義されるコマンドによって暗号処理に用いる暗号方式を特定することができ、指定された暗号方式での暗号処理を含む処理を実行することができる。また、ICカード処理装置は

、暗号方式ごとに定義される複数種類のコマンドから所望の暗号方式を指定するコマンドを選択することにより暗号処理に用いる暗号方式をコマンドで指定することができる。

[0113] なお、上述した各動作例は、適宜組み合わせて実施することができる。例えば、第1乃至3の動作例は、第4乃至第8の動作例と組み合わせて実施することができ、第6乃至8の動作例は、第1乃至第5の動作例と組み合わせて実施することができる。また、第4および第5の動作例は、他の動作例を組み合わせたものにさらに組み合わせて実施することも可能である。

[0114] また、上述の各実施の形態で説明した機能は、ハードウェアを用いて構成するに留まらず、ソフトウェアを用いて各機能を記載したプログラムをコンピュータに読み込ませて実現することもできる。また、各機能は、適宜ソフトウェア、ハードウェアのいずれかを選択して構成するものであっても良い。

[0115] 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。これら新規な実施形態は、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ともに、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。

請求の範囲

- [請求項1] 外部装置と通信するインターフェースと、
特定の処理を実行するための複数の異なる処理方式ごとの設定情報を記憶するメモリと、
前記外部装置から供給される情報に応じて前記特定の処理を実行するための1つの処理方式を選択し、選択した処理方式によって前記特定の処理を実行するプロセッサと、
を有する携帯可能電子装置。
- [請求項2] 前記特定の処理は、暗号処理であり、
前記処理方式は、暗号方式である、
請求項1に記載の携帯可能電子装置。
- [請求項3] 前記暗号方式には、耐量子暗号の暗号方式と耐量子暗号以外の暗号方式とを含む、
請求項2に記載の携帯可能電子装置。
- [請求項4] 前記プロセッサは、前記外部装置から要求されるリセットの種別に応じて1つの暗号方式を選択する、
請求項2に記載の携帯可能電子装置。
- [請求項5] 前記プロセッサは、前記外部装置から指定される通信条件に応じて1つの暗号方式を選択する、
請求項2に記載の携帯可能電子装置。
- [請求項6] 前記プロセッサは、前記外部装置から指定される通信レートに応じて1つの暗号方式を選択する、
請求項5に記載の携帯可能電子装置。
- [請求項7] 前記プロセッサは、前記外部装置から指定される通信方式を設定し、設定した通信方式ごとの通信条件に応じて1つの暗号方式を選択する、
請求項5に記載の携帯可能電子装置。
- [請求項8] 前記プロセッサは、前記外部装置からのコマンドに応じたコマンド

処理を実行した場合に実行可能な暗号方式を示す情報を前記外部装置へ送信する、

請求項2に記載の携帯可能電子装置。

[請求項9] 前記プロセッサは、前記外部装置から特定の暗号方式の無効化を要求するコマンドを受信した場合に前記特定の暗号方式を無効化する、
請求項2に記載の携帯可能電子装置。

[請求項10] 前記プロセッサは、選択中の暗号方式を示す情報を保持し、前記外部装置から暗号処理を含む処理を要求するコマンドを受信した場合に選択中の暗号方式を用いて暗号処理を実行する、
請求項2に記載の携帯可能電子装置。

[請求項11] 前記プロセッサは、前記外部装置から暗号処理を含む処理を要求するコマンドを受信した場合に当該コマンドのパラメータに基づいて暗号処理に用いる暗号方式を選択する、
請求項2に記載の携帯可能電子装置。

[請求項12] 前記プロセッサは、前記外部装置から暗号処理を含む処理を要求するコマンドを受信した場合、当該コマンドが指定する暗号方式を選択する、
請求項2に記載の携帯可能電子装置。

[請求項13] ICカード処理装置と通信するインターフェースと、複数の暗号方式ごとに各暗号方式での暗号処理を実行するためのデータを記憶する記憶領域を設けたメモリと、前記複数の暗号方式から1つの暗号方式を選択し、選択した暗号方式を前記ICカード処理装置と共有し、前記ICカード処理装置と共有した暗号方式による暗号処理を用いた処理を実行するプロセッサと、を有するモジュールと、
前記モジュールを有する本体と、
を備えるICカード。