

明 細 書

発明の名称：

携帯可能電子装置、ＩＣカードおよびＩＣカード処理装置

技術分野

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

背景技術

[0002] 近年、携帯可能電子装置としてのＩＣカードに対して外部から攻撃を加えることによって制御回路に不正な動作を実行させるセキュリティ攻撃が知られている。このような外部から攻撃によれば、ＩＣカードは、セキュリティの保持に必要な判定処理などの正規の処理の一部をスキップしてしまうような不正な動作を行う可能性がある。

[0003] しかしながら、従来のＩＣカードは、外部からの攻撃によってコマンドで要求される正規の処理の一部をスキップしても正常なレスポンスを出力する可能性があるという問題がある。このため、ＩＣカードとカードリーダーとからなるＩＣカード処理システムとしては、ＩＣカード内における判定処理などの正規の処理の一部がスキップされてしまうような不正を検知できるものが要望されている。

先行技術文献

特許文献

[0004] 特許文献1：日本国特開２０２０－００９３０５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、不正な動作を検知できる携帯可能電子装置、ＩＣカードおよびＩＣカード処理装置を提供する。

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有する。インターフェースは、外部装置と通信する。メモリは、外部装置がコマンドを送信してから前記コマンドに対するレスポンスを受信するまでの待機時間の下限値を設定するための待機時間の設定情報を記憶する。プロセッサは、メモリに記憶した待機時間の設定情報に基づく待機時間の下限値を特定するための待機時間情報を外部装置へ送信し、待機時間情報を送信した外部装置から受信するコマンドに応じた処理を実行し、コマンドに応じた処理の実行結果を含むレスポンスを外部装置へ送信する。

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カードのメモリに記憶される処理時間の設定情報の例を示す図である。

[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カードのメモリに記憶される処理時間の設定情報の例を示す図である。

[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カードのメモリに記憶される処理時間の設定情報に対する調整値の例を示す図である。

[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カードのメモリに記憶される処理時間の設定情報に対する調整値の例を示す図である。

[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カードに対するICカード処理装置による待機時間の上限および下限を説明するためのシーケンスである。

[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ICカード処理装置の動作例を説明するためのフローチャートである。

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、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。たとえば、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。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。

[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（携帯端末）

を形成する本体内にモジュール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、不揮発性メモリ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。

[0014] 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あるいは不揮発性メモリ14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。

[0015] 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。

[0016] 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。つまり、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。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。

[0017] 不揮発性メモリ14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。不揮発性メモリ14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。不揮発性メモリ 14 は、一部または全部の領域が耐タンパ性を有し、セキュアにデータが格納できる。不揮発性メモリ 14 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。不揮発性メモリ 14 は、所定の規格で規定されるファイル構造でデータが格納される。不揮発性メモリ 14 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制御プログラムや種々のデータが書き込まれる。

[0018] 例えば、国際的な標準規格である ISO/IEC 7816-4 に対応する IC カードの不揮発性メモリ 14 には、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。ISO/IEC 7816-4 に規定するファイル構造では、MF が最上階層にあり、MF の次の階層に、1 又は複数の DF が存在する。1 つの DF は、例えば、1 つのアプリケーションを実現するためのデータが格納される。また、DF の次の階層には、1 又は複数の EF が存在する。各 EF は、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。

[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、複数の通信方式（たとえば、接触通信と非接触通信）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。

[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２４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。

[0022] 次に、実施形態に係るＩＣカード処理装置２の構成について説明する。

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２４を介してＩＣカード１と通信する機能を有する上位装置である。ＩＣカード処理装置２は、たとえば、カードリーダー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、ＲＡＭ２６、ＲＯＭ２７、不揮発性メモリ２８、通信部２９およびタイマ３０などを有する。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。

[0024] プロセッサ２５は、ＲＯＭ２７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。ＲＡＭ２６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。ＲＯＭ２７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。タイマ３０は、経過時間を計時する。タイマ３０は、プロセッサ２５によって経過時間の計測の開始および停止が制御される。

- [0025] 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。
- [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、電源供給、クロック供給、リセット制御、データの送受信を行う。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 の活性化（起動）、種々のコマンドの送信、および送信したコマンドに対する応答の受信などを行う。
- [0028] 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 と IC カー

ド処理装置 2 との通信処理について説明する。

ＩＣカード 1 は、カードリーダを含むＩＣカード処理装置 2 からのコマンドに応じた処理を実行し、コマンドに応じた処理の実行結果を含むレスポンスをＩＣカード処理装置 2 へ送信（応答）する。ＩＣカード 1 がＩＣカード処理装置 2 からコマンドに応じて実行する処理に要する処理時間は、正常に処理が実行される場合には予め推定可能な時間である。つまり、ＩＣカード 1 におけるコマンドに対する正常な処理時間の範囲が設定されると、ＩＣカード処理装置 2 がコマンドを送信してからレスポンスを受信するまでの待機時間の範囲（上限値および下限値）が設定できる。

[0029] 実施形態に係るＩＣカード 1 は、コマンドに応じた処理に要する正常な処理時間の範囲とする下限値および上限値が設定できる。処理時間に対する下限値および上限値は、ＩＣカード 1 の仕様などに応じて予め設定され、ＩＣカードの製造又は発行時などに内部データとして記憶される。例えば、処理時間に対する下限値および上限値を含む待機時間の設定情報としてＲＯＭ 13 又は不揮発性メモリ 14 などのメモリに記憶される。待機時間の設定情報は、アプリケーションごとに記憶しても良いし、コマンドごとに記憶しても良いし、ファイル（ＤＦ又はＥＦ）ごとに記憶しても良い。

[0030] 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 1 がアプリケーションごとに待機時間の設定情報を記憶する場合の構成例を示す図である。

図 3 では、ＩＳＯ／ＩＥＣ 7816-4:2020 の 12.2.4.2 で規定されるフォーマットを元に、正常な処理時間に対する下限を含む待機時間の設定情報を記憶するテーブルの構成例を示す。

図 3 に示す例において、待機時間の設定情報は、アプリケーションごとに、処理時間の上限値（ Tb_max ）、処理時間の下限値（ Tb_min ）、ユニットタイム（ Tu ）、および、オプションが設定される。

[0031] 「 Tb_max 」は、処理時間に対する上限の基準時間（例えば、 $Tb_max [ms]$ ）である。「 Tb_min 」は、処理時間に対する下限の基

準時間（例えば、 T_{b_min} [ms]）である。「 T_u 」は、単位データの送信時間（例えば、 T_u [ms/B]）である。ここで、通信データの長さを L_d （例えば、 L_d [B]）とすれば、通信時間は、「 $T_u \times L_d$ 」 ([ms]) として算出される。

[0032] ICカード処理装置2がICカード1にコマンドを送信してからレスポンスを受信するまでの時間（待機時間）は、ICカード1におけるコマンドに対する処理時間と通信時間とを含む。このため、待機時間の上限値（ T_{max} ）は、通信データの長さが L_d であれば、 $T_{max} = T_{b_max} + (T_u \times L_d)$ により算出される。また、待機時間の下限値（ T_{min} ）は、通信データの長さが L_d であれば、 $T_{min} = T_{b_min} + (T_u \times L_d)$ により算出される。

[0033] また、図3に示す待機時間の設定情報では、アプリケーションごとに、上限値又は下限値のいずれか一方を設定したり、上限値および下限値の両方を設定したり未設定としたりすることができる。具体例として、図3に示す例では、「Application1」には、処理時間の上限値が設定され、下限値が設定されない。この場合、ICカード1が処理時間の下限を指定しないため、ICカード処理装置2は、待機時間に対する下限のチェックを行わず、待機時間に対する上限のチェックを行う。

[0034] また、図3に示す例では、「Application2」には、処理時間の上限値が設定されず、下限値が設定される。この場合、ICカード1が処理時間の上限を指定しないため、ICカード処理装置2は、待機時間に対する上限のチェックを行わず、待機時間に対する下限のチェックを行う。また、図3に示す例では、「Application3」には、処理時間の上限値および下限値の両方が設定される。この場合、ICカードが処理時間の上限および下限を指定するため、ICカード処理装置2は、待機時間に対する上限および下限の両方のチェックを実施する。

[0035] また、図3に示す待機時間の設定情報では、アプリケーションごとに「オプション」が設定できる。待機時間の設定情報における「オプション」の設

定としては、例えば、ロジカルチャネル、セキュアセッション、優先順位などが指定できる。

ロジカルチャネルは、例えばISO/IEC 7816-4で規定される論理的に設定される通信チャネルである。待機時間の設定情報のオプションとしては、待機時間範囲の設定を有効とするロジカルチャネルと無効とするロジカルチャネルとを指定（設定）するようにしても良い。この場合、ICカード1は、オプションの設定に従って、ロジカルチャネルごとに待機時間範囲の設定を有効とするか無効とするかを切り替える。

[0036] セキュアセッションは、例えばISO/IEC 7816-4で規定される暗号化複合化を含むセキュアな通信モードである。待機時間の設定情報のオプションとしては、セキュアセッションである場合に待機時間範囲の設定を有効とし、セキュアセッションでない場合に無効とするように設定しても良い。この場合、ICカード1は、オプションの設定に従ってセキュアセッションであるか否かにより待機時間範囲の設定を有効とするか無効とするかを切り替える。

[0037] また、待機時間の設定情報のオプションとしては、優先順位を設定できる。オプションにおける優先順位は、例えば、後述するような別の条件で設定された待機時間の設定情報がある場合にどの設定情報を優先するか決定するための設定情報である。すなわち、異なる条件で設定された複数の待機時間の設定情報がある場合、ICカード1は、オプションとして設定する優先順位に基づいて適用する待機時間の設定情報を特定するようにできる。

[0038] 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1がコマンドごとに待機時間の設定情報を記憶する場合の構成例を示す図である。

図4は、ISO/IEC 7816-4で規定されるフォーマットを元に、正常な処理時間に対する下限値を含む待機時間の設定情報を記憶するテーブルの構成例を示す。図4に示す待機時間の設定情報では、コマンドごとに、処理時間の上限値（ T_{b_max} ）、処理時間の下限値（ T_{b_min} ）、ユニットタイム（ T_u ）、および、オプションが設定される。図3に示す

例と同様に、処理時間の上限値 (Tb_max) は、正常な処理時間に対する上限の基準時間であり、処理時間の下限値 (Tb_min) は、正常な処理時間に対する下限の基準値である。

[0039] 図4に示す待機時間の設定情報によれば、待機時間の上限値 ($Tmax$) は、図3に示す例と同様に、通信データの長さが Ld であれば、 $Tmax = Tb_max + (Tu \times Ld)$ により算出される。待機時間の下限値 ($Tmin$) は、通信データの長さが Ld であれば、 $Tmin = Tb_min + (Tu \times Ld)$ により算出される。

[0040] 図4に示す待機時間の設定情報では、コマンドごとに、上限値又は下限値のいずれか一方を設定したり、上限値および下限値の両方を設定したり未設定としたりすることができる。具体例として、図4に示す例では、「`read binary`」には、ICカードにおける正常な処理時間に対する上限値 (Tb_Max) が設定され、下限値 (Tb_min) が設定されない。この場合、ICカード1が待機時間の下限を指定しないため、ICカード処理装置2は、待機時間に対する下限のチェックを行わない。

[0041] また、図4に示す例では、「`Update binary`」には、ICカードにおける正常な処理時間に対する上限値 (Tb_Max) が設定されず、下限値 (Tb_min) が設定される。この場合、ICカードが待機時間の上限を指定しないため、ICカード処理装置2は、待機時間に対する上限のチェックを行わない。また、図4に示す例では、「`read record`」には、ICカードにおける正常な処理時間に対する上限値 (Tb_Max) および下限値 (Tb_min) の両方が設定される。この場合、ICカード1が待機時間の上限および下限を指定するため、ICカード処理装置2は、待機時間に対する上限および下限の両方のチェックを実施する。また、図4に示す例では、「`Update record`」には、ICカードにおける正常な処理時間に対する上限値 (Tb_Max) および下限値 (Tb_min) の両方が設定される。この場合、ICカード1が待機時間の上限および下限を指定するため、ICカード処理装置2は、待機時間に対する上限

および下限の両方のチェックを実施する。

[0042] 図4に示すように、コマンドごとの待機時間の設定情報における「オプション」としては、図3に示す例と同様に、ロジカルチャネル、セキュアセッション、優先順位などを設定できる。

[0043] また、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、ファイルごとに処理時間範囲の上限および下限などを示す待機時間の設定情報をメモリに記憶するようにしても良い。

[0044] 例えば、不揮発性メモリ14には、上述したように、MF、DFおよびEFなどからなる複数階層のファイル構造で管理されるファイルにアプリケーションのデータを格納するものとする。この場合、待機時間の設定情報は、DF又はEFなどのファイルごとに設定しても良い。ファイルごとの待機時間の設定情報は、図3又は図4に示す例と同様に、処理時間の上限、処理時間の下限、ユニットタイム、および、オプションなどの設定情報をファイルごとに設定した設定情報である。また、ファイルごとの待機時間の設定情報では、ファイルごとに、上限値又は下限値のいずれか一方を設定したり、上限値および下限値の両方を設定したり未設定としたりすることができる。

[0045] 次に、実施形態に係るICカード1における待機時間の設定情報における処理時間の上限値および下限値の調整について説明する。

実施形態に係るICカード1における正常な処理時間の範囲は、ICカードの状態によって変動する可能性がある。このため、実施形態に係るICカード1は、待機時間の設定情報における処理時間の上限値および下限値をICカードの状態によって調整する機能を有する。例えば、ICカード1は、通信状態、又は、メモリの状態などによって、処理時間の上限値および下限値の調整を行うことができる。

[0046] 図5は、ICカード1が通信状態に応じて処理時間の上限値および下限値を調整するための調整用パラメータの設定例を示す図である。

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って動作するため、通信状態によってコマンドに応じた処理時間が変わる可能である

。例えば、接触式のインターフェースによりＩＣカード処理装置（カードリーダーライター）２と通信接続する場合、ＩＣカード１は、ＩＣカード処理装置２から供給される印可電圧に依存して処理時間が変わる。

[0047] また、非接触式のインターフェースによりＩＣカード処理装置２と通信接続する場合、ＩＣカード１は、ＩＣカード処理装置（カードリーダーライター２４）２からの磁界強度などのコンタクトレス通信環境によって処理時間が変わる。例えば、磁界強度は、ＩＣカード１のインターフェース１６とＩＣカード処理装置２のカードリーダーライター２４との距離などによって変動する。このため、非接触式のインターフェースを介して通信するＩＣカード１は、コンタクトレス通信環境が頻繁に変動する可能性がある。

[0048] ＩＣカード１は、通信状態に応じた調整用パラメータとして、処理時間の上限および下限に対する調整値をＲＯＭ１３又は不揮発性メモリ１４などのメモリに記憶する。図５に示す例では、通信状態（印可電圧又は磁界の強度）のレベルに応じて調整値が設定されている。また、通信状態に応じた調整値は、処理時間の上限値および下限値に対する係数又はオフセットの値として設定される。

[0049] 例えば、調整値が処理時間の上限値および下限値に対する係数として設定される場合、処理時間の上限値および下限値は、調整値を乗算することにより調整される。具体的には、通信状態がレベル１で係数としての調整値が「ＡＡ」であれば、「 Tb_max 」は「 Tb_max 」×「ＡＡ」として調整され、「 Tb_min 」は「 Tb_min 」×「ＡＡ」として調整される。

[0050] また、調整値が処理時間の上限値および下限値に対するオフセットとして設定される場合、処理時間の上限値および下限値は、調整値を加算することにより調整される。具体的には、通信状態がレベル１でオフセットとしての調整値が「ＡＡ」であれば、「 Tb_max 」は「 Tb_max 」＋「ＡＡ」として調整され、「 Tb_min 」は「 Tb_min 」＋「ＡＡ」として調整される。

[0051] 図5に示すような通信状態に応じた調整用パラメータが設定されていれば、ＩＣカード１は、ＩＣカード処理装置２との通信が開始された場合に通信状態に応じたレベルを特定する。ＩＣカード１は、通信状態のレベルを特定すると、特定したレベルに応じた調整値を係数又はオフセットの値として調整した処理時間に対する上限値および下限値を算出する。ＩＣカード１は、調整後の処理時間に対する上限値および下限値を規格などで規定される所定のタイミングでＩＣカード処理装置２へ送信する。

[0052] 図6は、ＩＣカード１におけるデータ書き込み用のメモリ（例えば不揮発性メモリ１４）の状態に応じた調整値の設定例を示す図である。

ＩＣカード１における不揮発性メモリ１４は、データの書き込みを要求するコマンドに応じて、データが書き込まれるデータ記憶領域を有する。データ記憶領域を構成する記憶素子は性能が劣化する可能性がある。例えば、不揮発性メモリ１４（データ記憶領域）は、データの書き込みを頻繁に実施すると、通常の処理時間となる処理（通常の１回の処理）ではデータの消去および書き込みが完全に行えない可能性がある。

[0053] ＩＣカード１は、通常の１回の処理でデータの消去および書き込みが行えない場合、複数回のデータの消去および書き込みを行ったり、１回のデータの消去および書き込みにかける時間を長くしたりするなどの対応が必要になる。すなわち、ＩＣカード１は、不揮発性メモリ１４の記憶領域に対するデータの書き込みを繰り返すと、データの書き込みの処理が遅くなってくることがある。

[0054] このため、ＩＣカード１は、データ書き込み処理の遅延に対応する調整値としてメモリの状態に応じた調整用のパラメータ（遅延調整用パラメータ）を設定する。遅延調整用パラメータとしては、待機時間の設定情報における処理時間の上限値および下限値に対する調整値をメモリの状態に対応づけてＲＯＭ１３又は不揮発性メモリ１４などのメモリに記憶する。

[0055] 図6に示す遅延調整用パラメータでは、メモリの状態を示すレベルに応じた調整値が設定される。メモリの状態を示すレベルは、記憶領域の使用頻度

又は実際に検出する処理時間の遅延によって特定される。例えば、使用頻度を示す指標値としては、例えば、不揮発性メモリ 14 における記憶領域ごとのデータの書き込み回数を記憶する。この場合、使用頻度がレベルごとに設定する閾値以上となったか否かによりメモリの状態を示すレベル（メモリレベル）を判定する。また、実際に検出する処理時間の遅延を示す指標値としては、例えば、コマンドを受信してからレスポンスを送信するまでに IC カード処理装置 2 から送信される WTX の回数を記憶する。この場合、実際に検出した処理時間の遅延に応じてメモリの状態を示すレベルを判定する。

[0056] IC カード 1 は、上述したように、使用頻度又は実際に検出した処理時間の遅延などからメモリの状態を示すレベル（メモリレベル）を特定する。IC カード 1 は、メモリの状態を示すレベルを特定すると、特定したレベルに応じた調整値を係数又はオフセットの値として調整した処理時間に対する上限値および下限値を算出する。IC カード 1 は、調整後の処理時間に対する上限値および下限値を規格などで規定される所定のタイミングで IC カード処理装置 2 へ送信する。

[0057] 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 と通信する IC カード処理装置 2 による待機時間の上限および下限のチェック動作について説明する。

図 7 は、実施形態に係る IC カード処理装置 2 による待機時間の上限および下限のチェックを含む動作を説明するためのシーケンスである。

IC カード 1 は、IC カード処理装置 2 との通信を開始すると、上述したような設定情報に基づく処理時間の下限値および上限値などを示す待機時間情報を IC カード処理装置 2 へ提示（送信）する。IC カード処理装置 2 は、IC カード 1 から提示された待機時間情報を保存した後、IC カード 1 に所望の処理を実行させるコマンドを送信する。IC カード処理装置 2 は、コマンドを送信するとき、IC カードからのレスポンスを受信するまでの経過時間の計測を開始する。

[0058] IC カード処理装置 2 は、IC カード 1 から提示された待機時間情報によ

って算出される待機時間の下限値および上限値を設定する。ＩＣカード処理装置２は、図７に示すように、コマンドを送信してからの経過時間が待機時間の下限値に達する前にＩＣカード１からレスポンスを受信すると、当該ＩＣカードに対する処理を中止する。これにより、ＩＣカードにおいて不正に処理をスキップされたことをＩＣカード処理装置２がレスポンスを受信するまでの待機時間によって検出することができる。

[0059] また、ＩＣカード処理装置２は、待機時間の下限値だけでなく、待機時間情報から待機時間の上限値も設定することができる。すなわち、ＩＣカード処理装置２は、適正な待機時間範囲内でＩＣカードからのレスポンスを受信できない場合に、ＩＣカードが正常な動作でコマンドに対する処理を実施しないと判定することができる。この結果、携帯可能電子装置としてのＩＣカードの不正な動作を検知でき、外部からの攻撃などによる不正な使用を防止することができる。

[0060] 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の動作について説明する。

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の動作例を説明するためのフローチャートである。

ＩＣカード１のプロセッサ１１は、ＩＣカード処理装置２から供給される電力によって起動し、ＩＣカード処理装置２との初期設定を含む初期通信を行う。プロセッサ１１は、初期通信が完了すると、ＲＯＭ１３又は不揮発性メモリ１４に保存している待機時間の設定情報を確認する（ステップＳＴ１１）。

[0061] 例えば、アプリケーションごとに待機時間の設定情報が保存されている場合、プロセッサ１１は、選択中のアプリケーションに対応する設定情報から処理時間の上限値および下限値などの設定情報を特定する。また、コマンドごとの待機時間の設定情報が保存されている場合、プロセッサ１１は、各コマンドに対する処理時間の上限値および下限値などの設定情報を特定する。さらに、ファイルごとに待機時間の設定情報が保存されている場合、プロセ

ッサ 11 は、選択されているファイルに対応する処理時間の上限値および下限値などの設定情報を特定する。

[0062] また、プロセッサ 11 は、ROM 13 又は不揮発性メモリ 14 に保存する自動調整用パラメータに基づいて処理時間の上限値および下限値を調整する（ステップ ST 12）。例えば、プロセッサ 11 は、図 5 に示すような自動調整用パラメータを参照し、インターフェース 16 を介して通信接続する IC カード処理装置 2 との通信状態に応じたレベル（通信レベル）を判断する。

[0063] プロセッサ 11 は、IC カード処理装置 2 との通信状態のレベルを特定すると、通信状態のレベルに応じた調整値を自動調整用パラメータから特定する。プロセッサ 11 は、通信状態に応じた調整値を特定すると、上述したように、通信状態に応じた調整値を係数又はオフセットとすることにより処理時間の上限値および下限値を調整する。なお、自動調整用パラメータが設定されていない場合、プロセッサ 11 は、通信状態による調整を省略する。

[0064] さらに、プロセッサ 11 は、ROM 13 又は不揮発性メモリ 14 に保存する書き込みによる遅延調整用パラメータに基づいて書き込み処理に対する処理時間の上限値および下限値を調整する（ステップ ST 13）。例えば、プロセッサ 11 は、図 6 に示すような遅延調整用パラメータを参照し、データ記憶領域としての不揮発性メモリ 14 の状態に応じたメモリレベルを特定する。

[0065] プロセッサ 11 は、メモリレベルを特定すると、メモリレベルに応じた調整値を遅延調整用パラメータから特定する。プロセッサ 11 は、メモリレベルに応じた調整値を特定すると、上述したように、メモリレベルに応じた調整値を係数又はオフセットとすることによりデータの書き込み処理に対する処理時間の上限値および下限値を調整する。なお、遅延調整用パラメータが設定されていない場合、プロセッサ 11 は、メモリの状態による遅延調整を省略する。

[0066] プロセッサ 11 は、待機時間の設定情報における処理時間の上限値および

下限値に対する調整が終了すると、調整した処理時間の上限値および下限値を含む待機時間情報をＩＣカード処理装置２へ送信する（ステップＳＴ１４）。プロセッサ１１は、待機時間情報を送信した後、ＩＣカード処理装置２からのコマンドを受け付ける（ステップＳＴ１５）。

[0067] 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ＳＴ１５、ＹＥＳ）、受信したコマンドに応じた処理を実行する（ステップＳＴ１６）。プロセッサ１１は、コマンドに応じた処理が完了すると、コマンドの処理結果を含むレスポンスをＩＣカード処理装置２へ送信する（ステップＳＴ１７）。

[0068] レスポンスを送信した後にトランザクション終了（中止）の通知を受けなければ（ステップＳＴ１８、ＮＯ）、プロセッサ１１は、ステップＳＴ１５へ進み、次のコマンドの受信待ちとなる。また、プロセッサ１１は、レスポンスを送信した後にＩＣカード処理装置２からトランザクションの終了通知を受信した場合（ステップＳＴ１８、ＹＥＳ）、ＩＣカード処理装置２との一連の通信処理を終了する。

[0069] 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と通信するカードリーダーライタを備えるＩＣカード処理装置２の動作について説明する。

図９は、実施形態に係るＩＣカード処理装置２の動作例を説明するためのフローチャートである。

ＩＣカード処理装置２の制御部２１は、カードリーダーライタ２４に接続されたＩＣカード１へ電力を供給し、ＩＣカード１を起動させる。制御部２１のプロセッサ２５、カードリーダーライタ２４を介して通信接続したＩＣカード１が起動すると、ＩＣカード１との初期設定を含む初期通信を行う。

[0070] 制御部２１のプロセッサ２５は、初期通信が終了した後、カードリーダーライタ２４によりＩＣカード１から待機時間情報を受信する（ステップＳＴ３１）。例えば、制御部２１において、プロセッサ２５は、ＩＣカード１を処理するためのアプリケーションを起動する。ＩＣカード１を処理するための

アプリケーションを起動すると、プロセッサ25は、待機時間情報を含む通信設定情報をICカード1に要求し、要求に応じてICカード1が送信する待機時間情報を含む通信設定情報を受信する。

[0071] 制御部21のプロセッサ25は、ICカード1から待機時間情報を含む情報を受信すると、ICカード1から受信した情報に含まれる待機時間情報を不揮発性メモリ28又はRAM26などのメモリに保存する（ステップST32）。制御部21のプロセッサ25は、待機時間情報を保存すると、ICカード1に対して要求する処理を実行させるためのコマンドをカードリーダーライタ24から送信する（ステップST33）。

[0072] プロセッサ25は、ICカード1へコマンドを送信すると、タイマ30による経過時間の計時を開始する（ステップST34）。プロセッサ25は、タイマ30により経過時間を計測しながら、ICカード1からのレスポンス待ちとなる（ステップST35）。プロセッサ25は、ICカード1からのレスポンスがなければ（ステップST35、NO）、タイマ30による経過時間の計測を継続する。

[0073] ICカード1からのレスポンスを受信した場合（ステップST35、YES）、プロセッサ25は、タイマ30による計時を停止し（ステップST36）、コマンドを送信してからレスポンスを受信するまでの時間（待機時間）を確定する。プロセッサ25は、待機時間が確定すると、確定した待機時間が待機時間情報によって指定される待機時間範囲外であるか否かを判定する（ステップST37）。

[0074] プロセッサ25は、確定した待機時間が待機時間情報によって指定される待機時間範囲外ではない（待機時間範囲内である）と判定した場合（ステップST38、NO）、ステップST33へ戻り、上述した処理を繰り返し実施する。

[0075] 確定した待機時間が待機時間情報によって指定される待機時間範囲外であると判定した場合（ステップST38、YES）、プロセッサ25は、当該ICカード1に対する処理を終了（中止）し、トランザクション終了をIC

カード1に通知する（ステップST39）。つまり、プロセッサ25は、確定した待機時間が待機時間の下限値よりも短い場合、又は、確定した待機時間が待機時間の上限値よりも長い場合、ICカード1の処理を中止する。

[0076] 例えば、確定した待機時間が待機時間の下限値よりも短い場合、プロセッサ25は、待機時間が短すぎるために、ICカード1の処理を中止する。これにより、ICカード1においてセキュリティ攻撃などによって規定の処理ステップが省略された場合、ICカード処理装置2は、ICカード1からのレスポンスの内容が正常であっても、不正として検知してICカード1における処理を中止させることが可能となる。この場合、ICカード処理装置2のプロセッサ25は、表示部22に処理のスキップによる不正の可能性があるために、処理を中止したことを表示（報知）するようにしても良い。

[0077] なお、上述した動作例では、レスポンスを受信したときまでの待機時間が待機時間範囲外であるか否かを判定するものとして説明したが、コマンドを送信してからの経過時間が待機時間の上限値を超えた場合にトランザクションを終了するようにしても良い。すなわち、プロセッサ25は、レスポンスの受信待ちの状態においてタイマ30が計時する経過時間が待機時間の上限値を超えたか否かをチェックする。プロセッサ25は、タイマ30が計時する経過時間が待機時間の上限値を超えた場合、待機時間範囲外であると判断し、ステップST39へ進むようにしても良い。

[0078] 以上のように、実施形態に係る携帯可能電子装置としてのICカードは、メモリに記憶した待機時間の設定情報に基づいて、コマンドを送信してからレスポンスを受信するまでの待機時間に対する下限値を示す待機時間情報をICカード処理装置に提供する。

[0079] これにより、ICカード処理装置は、コマンドを送信してからレスポンスを受信するまでの待機時間が当該ICカードによって指定される待機時間の下限値より短い時間である場合、ICカードからのレスポンスの内容にかかわらず当該ICカードによる処理を中止させることができる。この結果、実施形態に係る携帯可能電子装置としてのICカードは、規定の処理をスキ

ップさせるようなセキュリティ攻撃による待機時間の下限値よりも早すぎるレスポンスを検知でき、ＩＣカードにおける不正な動作を含む処理を中止させることができる。

[0080] また、実施形態に係る携帯可能電子装置としてのＩＣカードは、アプリケーション毎、コマンド毎、又は、ファイル毎に待機時間の設定情報を設定でき、さらに、待機時間の設定情報において待機時間の下限と上限とをそれぞれ設定できる。これにより、実施形態に係る携帯可能電子装置としてのＩＣカードは、特定のアプリケーション、コマンド、ファイルごとに、待機時間の下限だけを設定したり、上限だけを設定したり、下限と上限との両方を設定したりするなどの運用に応じた詳細な設定が行える。

[0081] また、実施形態に係る携帯可能電子装置としてのＩＣカードは、待機時間の設定情報で設定される処理時間の下限値および上限値を通信状態に応じて調整できる。また、実施形態に係る携帯可能電子装置としてのＩＣカードは、待機時間の設定情報で設定される処理時間の下限値および上限値をデータが書き込まれるメモリの態に応じて調整することもできる。これらのカード状態に応じた処理時間の下限および上限の設定によって、実施形態に係る携帯可能電子装置としてのＩＣカードおよびＩＣカード処理装置は、待機時間による不正な動作の高精度に検知することができる。

[0082] なお、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。

[0083] 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

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、
前記外部装置がコマンドを送信してから前記コマンドに対するレスポンスを受信するまでの待機時間の下限値を設定するための待機時間の設定情報を記憶するメモリと、
前記メモリに記憶した待機時間の設定情報に基づく前記待機時間の下限値を特定するための待機時間情報を前記外部装置へ送信し、前記待機時間情報を送信した前記外部装置から受信するコマンドに応じた処理を実行し、前記コマンドに応じた処理の実行結果を含むレスポンスを前記外部装置へ送信するプロセッサと、
を有する携帯可能電子装置。
- [請求項2] 前記待機時間の設定情報は、コマンドに応じた処理に要する処理時間の下限値を含み、前記メモリは、さらに、通信状態に応じた調整値を示す情報を記憶し、
前記プロセッサは、前記インターフェースによる前記外部装置との通信状態を特定し、通信状態に応じた調整値によって調整した前記処理時間に対する下限値を含む待機時間情報を前記外部装置へ送信する、
請求項1に記載の携帯可能電子装置。
- [請求項3] 前記待機時間の設定情報は、前記メモリにおけるデータ記憶領域に対するデータの書き込み処理に要する処理時間の下限値を含み、
前記メモリは、さらに、前記データ記憶領域の状態に応じた遅延調整値を記憶し、
前記プロセッサは、前記データ記憶領域の状態を特定し、前記データ記憶領域の状態に応じた遅延調整値によって調整した前記処理時間に対する下限値を含む待機時間情報を前記外部装置へ送信する、
請求項1に記載の携帯可能電子装置。
- [請求項4] 前記メモリは、アプリケーションごとに前記待機時間の設定情報を

記憶する、

請求項 1 に記載の携帯可能電子装置。

[請求項5] 前記メモリは、コマンドごとに前記待機時間の設定情報を記憶する

、

請求項 1 に記載の携帯可能電子装置。

[請求項6] 前記メモリは、所定のファイル構造で管理されるファイルに格納するデータを記憶し、ファイルごとに前記待機時間の設定情報を記憶する、

請求項 1 に記載の携帯可能電子装置。

[請求項7] 外部装置と通信するインターフェースと、前記外部装置がコマンドを送信してから前記コマンドに対するレスポンスを受信するまでの待機時間の下限値を設定するための待機時間の設定情報を記憶するメモリと、前記メモリに記憶した待機時間の設定情報に基づく前記待機時間の下限値を特定するための待機時間情報を前記外部装置へ送信し、前記待機時間情報を送信した前記外部装置から受信するコマンドに応じた処理を実行し、前記コマンドに応じた処理の実行結果を含むレスポンスを前記外部装置へ送信するプロセッサと、を有するモジュールと、

前記モジュールを有する本体と、

を有する I C カード。

[請求項8] I C カードと通信する通信部と、

前記 I C カードから取得する待機時間情報を保存するメモリと、

前記 I C カードへコマンドを送信してからの経過時間が前記メモリに記憶した前記待機時間情報から特定する待機時間の下限値に達する前に前記コマンドに対するレスポンスを受信した場合、前記 I C カードによる処理を中止するプロセッサと、

を有する I C カード処理装置。