(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2007-4456
(P2007-4456A)
(43)公開日　平成19年1月11日(2007.1.11)

(51)Int.Cl.		F I			テーマコード（参考）
G06K 19/073	(2006.01)	G06K	19/00	P	5B017
G06F 21/06	(2006.01)	G06F	12/14	560E	5B035
H04L 9/10	(2006.01)	H04L	9/00	621Z	5J104

審査請求 未請求　請求項の数 16　ＯＬ　（全 13 頁）

(21)出願番号　特願2005-183465 (P2005-183465)
(22)出願日　平成17年6月23日 (2005.6.23)

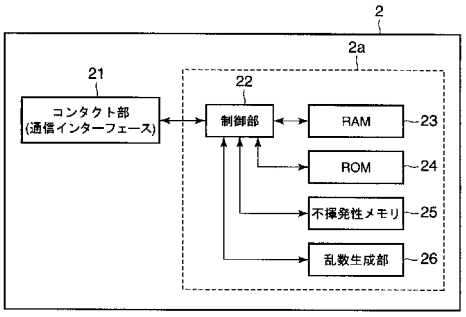
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】携帯可能電子装置及び携帯可能電子装置のデータ出力方法

(57)【要約】
【課題】処理プログラムが不正な処理を行った場合であっても、ＩＣカード内のデータを保護することができ、セキュリティ性の高いＩＣカードを実現することが可能となる。
【解決手段】データの出力を要求するコマンドに対応する種々の処理が全て正常に実行された場合に所定の値となるような初期値を監視フラグに設定し、データの出力を要求するコマンドに対応する種々の処理の実行状況に応じて監視フラグの値をセットし、データを出力するまでの各処理が完了すると、監視フラグの値に基づいて出力すべきデータをマスクし、マスクしたデータを出力する。
【選択図】図２

図２



【特許請求の範囲】
【請求項１】
外部からデータの出力を要求するコマンドが供給された場合に、当該コマンドに応じた処理を全て実行した状態で所定の値となる監視情報の初期値を設定する設定手段と、
この設定手段により初期値が設定された監視情報を実行した処理に応じて変更する変更手段と、
この変更手段により実行した処理に応じて変更された監視情報に基づいて出力すべきデータを保護する保護手段と、
この保護手段により保護されたデータを外部へ出力する出力手段と、
を有することを特徴とする携帯可能電子装置。
【請求項２】
前記設定手段、前記変更手段、前記保護手段および前記出力手段を具備するモジュールと、
前記モジュールが埋設された筐体と、を有する、
ことを特徴とする前記請求項１に記載の携帯可能電子装置。
【請求項３】
前記保護手段は、前記変更手段により実行した処理に応じて変更された監視情報に基づいて出力すべきデータに対して所定の演算処理を施し、
前記出力手段は、前記保護手段による演算処理の結果として得られたデータを外部へ出力する、
ことを特徴とする前記請求項１に記載の携帯可能電子装置。
【請求項４】
前記保護手段は、前記変更手段により実行した処理に応じて変更された監視情報と任意のデータとに基づいて出力すべきデータを保護する、
ことを特徴とする前記請求項１に記載の携帯可能電子装置。
【請求項５】
前記保護手段は、前記変更手段により実行した処理に応じて変更された監視情報と任意のデータとに基づいて出力すべきデータに対して所定の演算処理を施し、
前記出力手段は、前記保護手段による演算処理の結果として得られたデータを外部へ出力する、
ことを特徴とする前記請求項４に記載の携帯可能電子装置。
【請求項６】
さらに、乱数データを生成する乱数生成手段を有し、
前記保護手段は、前記変更手段により実行した処理に応じて変更された監視情報と前記乱数生成手段により生成した乱数データとに基づいて出力すべきデータを保護する、
ことを特徴とする前記請求項１に記載の携帯可能電子装置。
【請求項７】
前記保護手段は、前記変更手段により実行した処理に応じて変更された監視情報と前記乱数生成手段により生成された乱数データとに基づいて出力すべきデータに対して所定の演算処理を施し、
前記出力手段は、前記保護手段による演算処理の結果として得られたデータを外部へ出力する、
ことを特徴とする前記請求項６に記載の携帯可能電子装置。
【請求項８】
さらに、当該携帯可能電子装置に固有な固有データが記憶されているメモリを有し、
前記保護手段は、前記変更手段により実行した処理に応じて変更された監視情報と前記メモリに記憶されている固有データとに基づいて出力すべきデータを保護する、
ことを特徴とする前記請求項１に記載の携帯可能電子装置。
【請求項９】
前記保護手段は、前記変更手段により実行した処理に応じて変更された監視情報と前記

メモリに記憶されている固有データとに基づいて出力すべきデータに対して所定の演算処理を施し、
前記出力手段は、前記保護手段による演算処理の結果として得られたデータを外部へ出力する、
ことを特徴とする前記請求項８に記載の携帯可能電子装置。
【請求項１０】
さらに、前記出力手段によりデータを出力した場合に、前記保護手段により当該データを保護するために用いた前記監視情報を記憶するメモリを有し、
前記保護手段は、前記変更手段により実行した処理に応じて変更された監視情報と前記メモリに記憶されている監視情報とに基づいて出力すべきデータを保護する、
ことを特徴とする前記請求項１に記載の携帯可能電子装置。
【請求項１１】
前記保護手段は、前記変更手段により実行した処理に応じて変更された監視情報と前記メモリに記憶されている監視情報とに基づいて出力すべきデータに対して所定の演算処理を施し、
前記出力手段は、前記保護手段による演算処理の結果として得られたデータを外部へ出力する、
ことを特徴とする前記請求項１０に記載の携帯可能電子装置。
【請求項１２】
外部からデータの出力を要求するコマンドが供給された場合に、当該コマンドに応じた処理を全て実行した状態で所定の値となる監視情報の初期値を設定する第１のステップと、
この第１のステップにより初期値が設定された監視情報を実行した処理に応じて変更する第２のステップと、
この第２のステップにより実行した処理に応じて変更された監視情報に基づいて出力すべきデータを保護する第３のステップと、
この第３のステップにより保護されたデータを外部へ出力する第４のステップと、
を有する特徴とする携帯可能電子装置のデータ出力方法。
【請求項１３】
前記第３のステップは、前記第２のステップにより実行した処理に応じて変更された監視情報と任意のデータとに基づいて出力すべきデータを保護する、
ことを特徴とする前記請求項１２に記載の携帯可能電子装置のデータ出力方法。
【請求項１４】
さらに、乱数データを生成する乱数生成ステップを有し、
前記第３のステップは、前記第２のステップにより実行した処理に応じて変更された監視情報と前記乱数生成ステップにより生成した乱数データとに基づいて出力すべきデータを保護する、
ことを特徴とする前記請求項１２に記載の携帯可能電子装置のデータ出力方法。
【請求項１５】
前記第３のステップは、前記第２のステップにより実行した処理に応じて変更された監視情報と当該携帯可能電子装置に固有な固有データとに基づいて出力すべきデータを保護する、
ことを特徴とする前記請求項１２に記載の携帯可能電子装置のデータ出力方法。
【請求項１６】
さらに、前記第４のステップによりデータを出力した場合に、前記第３のステップにおいて当該データを保護するために用いた前記監視情報をメモリに記憶する第５のステップを有し、
前記第３のステップは、前記第４のステップにより実行した処理に応じて変更された監視情報と前記メモリに記憶されている監視情報とに基づいて出力すべきデータを保護する、

ことを特徴とする前記請求項１２に記載の携帯可能電子装置のデータ出力方法。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、例えば、外部装置との通信インターフェース、データを記憶しているメモリ、および処理プログラムを実行するＣＰＵなどを有するＩＣカードなどの携帯可能電子装置及び携帯可能電子装置のデータ出力方法に関する。

【背景技術】

【０００２】

従来、携帯可能電子装置としてのＩＣカードでは、外部機器からのデータの読み出しを要求する読み出しコマンドに応じて、メモリに記憶しているデータを出力するようになっている。従来のＩＣカードでは、外部から読み出しコマンドを受信すると、データを出力するために必要な種々の処理を実行する。この際、ＩＣカードでは、データを出力するために必要な種々の処理の実行状態を監視フラグにより監視している。従って、ＩＣカードでは、実際にデータを出力する前に、監視フラグをチェックする。このチェックの結果として監視フラグが正常であると判断した場合、当該ＩＣカードは、データを出力する。このように、従来のＩＣカードでは、監視フラグを用いて処理内容を監視している。これにより、従来のＩＣカードでは、不正にデータを出力することを抑えるようになっている。

【０００３】

しかしながら、上記のようなＩＣカードからデータを盗み出そうとする悪意のある者（不正アクセス者）は、ＩＣカードに対する様々なアタックにより、当該ＩＣカード内のデータを解読（読み出）しようとする。たとえば、不正アクセス者は、ＩＣカードに対して外部からノイズを加えてプログラムを誤動作させることがある。この場合、当該ＩＣカードは、上記のような処理における監視フラグのチェックが無効化され、当該ＩＣカード内のデータを出力してしまう可能性がある。つまり、従来のＩＣカードでは、外部からのノイズなどにより意図的にプログラムを誤動作させると、内部のデータを出力してしまう可能性があるという問題点がある。

【特許文献１】特開平１０－１５４９７６号公報

【発明の開示】

【発明が解決しようとする課題】

【０００４】

この発明の一形態では、外部へ出力するデータを保護することによりセキュリティ性を向上させることができ、安全性が高い携帯可能電子装置および携帯可能電子装置の制御方法を提供することを目的とする。

【課題を解決するための手段】

【０００５】

この発明の一形態としての携帯可能電子装置は、外部からデータの出力を要求するコマンドが供給された場合に、当該コマンドに応じた処理を全て実行した状態で所定の値となる監視情報の初期値を設定する設定手段と、この設定手段により初期値が設定された監視情報を実行した処理に応じて変更する変更手段と、この変更手段により実行した処理に応じて変更された監視情報に基づいて出力すべきデータを保護する保護手段と、この保護手段により保護されたデータを外部へ出力する出力手段とを有する。

【０００６】

この発明の一形態としての携帯可能電子装置のデータ出力方法は、外部からデータの出力を要求するコマンドが供給された場合に、当該コマンドに応じた処理を全て実行した状態で所定の値となる監視情報の初期値を設定する第１のステップと、この第１のステップにより初期値が設定された監視情報を実行した処理に応じて変更する第２のステップと、この第２のステップにより実行した処理に応じて変更された監視情報に基づいて出力すべきデータを保護する第３のステップと、この第３のステップにより保護されたデータを外部へ出力する第４のステップとを有する。

【発明の効果】
【０００７】
この発明の一形態によれば、外部へ出力するデータを保護することによりセキュリティ性を向上させることができ、安全性が高い携帯可能電子装置および携帯可能電子装置の制御方法を提供できる。
【発明を実施するための最良の形態】
【０００８】
以下、この発明を実施するための最良の形態について図面を参照して詳細に説明する。

図１は、この発明の実施の形態に係る携帯可能電子装置としてのＩＣカード２との通信機能を有する外部装置としての端末システム（ＩＣカード処理装置）１の構成例を概略的に示すブロック図である。
図１に示すように、上記端末システム１は、端末装置１１、表示装置１２、キーボード１３、および、カードリーダライタ１４などを有している。
【０００９】
上記端末装置１１は、上記端末システム１全体の動作を制御するものである。上記端末装置１１は、ＣＰＵ、種々のメモリおよび各種インターフェースなどを有する。上記端末装置１１は、上記カードリーダライタ１４により上記ＩＣカード２へ処理命令としてのコマンドを送信する機能、上記ＩＣカード２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している。
【００１０】
たとえば、上記端末装置１１は、上記カードリーダライタ１４を介して上記ＩＣカード２にデータの書込みを要求する書込みコマンドを送信する。すると、この書込みコマンドを受けたＩＣカード２では、ＩＣカード２内のメモリにデータを書き込んむ処理を行う。また、上記端末装置１１は、上記カードリーダライタ１４を介して上記ＩＣカード２にデータの読み出しを要求する読出コマンドを送信する。すると、この読出コマンドを受けたＩＣカード２では、当該ＩＣカード２内のメモリに記憶されているデータを読み出し、読み出したデータを上記端末装置１１へ送信する処理を行う。
【００１１】
上記表示装置１２は、上記端末装置１１の制御により種々の情報を表示するディスプレイ装置である。上記キーボード１３は、当該端末システム１の操作員が操作する操作部である。上記キーボード１３は、操作員により種々の操作指示やデータなどが入力される。上記カードリーダライタ１４は、上記ＩＣカード２との通信を行うためのインターフェース装置である。上記カードリーダライタ１４では、上記ＩＣカード２に対する電源供給、クロック供給、リセット制御、データの送受信などを行うようになっている。つまり、上記カードリーダライタ１４は、上記端末装置１１による制御に基づいて上記ＩＣカード２を活性化（起動）させ、活性化させたＩＣカード２へ種々のコマンドを送信したり、送信したコマンドに対する応答を受信したりするようになっている。
【００１２】
上記ＩＣカード２は、上記ＩＣカード処理装置１などの上位機器から電力などの供給を受けた際、活性化される（動作可能な状態になる）ようになっている。例えば、上記ＩＣカード２が接触式通信により上記端末システム１と通信を行う場合、つまり、上記ＩＣカード２が接触式のＩＣカードで構成される場合、上記ＩＣカード２は、通信インターフェースとしてのコンタクト部２１を介してＩＣカード処理装置１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される。
【００１３】
また、ＩＣカード２が非接触式の通信方式により上記端末システム１と通信を行う場合、つまり、上記ＩＣカード２が非接触式のＩＣカードで構成される場合、上記ＩＣカード２の上記コンタクト部２１は、通信インターフェースとしてのアンテナおよび通信制御部等により構成される。この場合、上記ＩＣカード２は、通信インターフェースとしてのコ

ンタクト部２１のアンテナおよび通信制御部等を介してＩＣカード処理装置１からの電波を受信し、その電波から図示しない電源部により動作電源および動作クロックを生成して活性化するようになっている。

【００１４】

次に、上記ＩＣカード２の構成例について説明する。

図２は、上記ＩＣカード２の内部構成例を概略的に示すブロック図である。図２に示すように、上記ＩＣカード２は、コンタクト部２１、制御部２２、ＲＡＭ２３、ＲＯＭ２４、および不揮発性メモリ２５などを有してしている。上記制御部２２、ＲＡＭ２３、ＲＯＭ２４および不揮発性メモリ２５は、例えば、ＩＣチップ（図示しない）により構成され、ＩＣカード２の筐体内に埋設されている。

【００１５】

上記コンタクト部２１は、上記端末システム１のカードリーダライタ１４との通信用のインターフェースとして機能する。当該ＩＣカード２が接触式のＩＣカードとして実現される場合、上記コンタクト部２１は、上記ＩＣカード処理装置１のカードリーダライタ１４と接触して信号の送受信を行うインターフェースとして構成される。また、当該ＩＣカード２が非接触式のＩＣカードとして実現される場合、上記コンタクト部２１は、上記ＩＣカード処理装置１のカードリーダライタ１４との電波の送受信を行うインターフェースとして構成される。

【００１６】

上記制御部２２は、当該ＩＣカード２全体の制御を司るものである。上記制御部２２は、上記ＲＯＭ２４あるいは不揮発性メモリ２５に記憶されている処理プログラムに基づいて動作する。上記ＲＡＭ２３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。上記ＲＡＭ２３は、上記制御部２２が処理中のデータなどを一時保管するバッファとして機能する。上記ＲＡＭ２３は、例えば、上記コンタクト部２１を介して上記ＩＣカード処理装置１から受信したデータを一時保管するようになっている。

【００１７】

上記ＲＯＭ２４は、予め制御用のプログラムや制御データなどが記憶されている不揮発性のメモリである。上記ＲＯＭ２４は、製造段階でＩＣカード２内に組み込まれるものである。上記ＲＯＭ２４に記憶されている制御プログラムは、予め当該ＩＣカード２の仕様に応じて組み込まれるものである。

【００１８】

上記不揮発性メモリ２５は、例えば、ＥＥＰＲＯＭあるいはフラッシュＲＯＭなどのデータの書込み及び書き換えが可能な不揮発性のメモリにより構成される。上記不揮発性メモリ２５には、当該ＩＣカード２の運用用途に応じてプログラムファイルやデータファイルなどが定義され、それらのファイルにデータが書き込まれる。また、上記不揮発性メモリ２５には、当該ＩＣカードを認証するための認証情報、あるいは、当該ＩＣカードに固有な固有データなども記憶されている。上記乱数生成部２６は、乱数データを生成するものである。

【００１９】

次に、上記のように構成されるＩＣカード２における処理について説明する。

図３は、上記ＩＣカード２における処理例を説明するためのフローチャートである。

まず、上記端末システム１では、上記カードリーダライタ１４によりＩＣカード２に対してデータの読み出しを要求する読出コマンドを出力する。これに対して、上記ＩＣカード２では、上記通信インターフェース２１により端末システム１からの読出コマンドを受信する（ステップＳ１１）。上記端末システム１からの読出コマンドを受信すると、当該ＩＣカード２の制御部２２は、受信したコマンドに応じた監視フラグ（監視情報）を設定（初期化）する（ステップＳ１２）。

【００２０】

上記監視フラグは、受信したコマンドに応じた処理の実行状況を監視するための情報である。つまり、上記監視フラグは、コマンドに対応する各種の処理が確実に実行されたか

否かを識別するための情報である。また、上記監視フラグは、当該ＩＣカード２内のメモリに設定される。たとえば、上記監視フラグは、制御部２２内の内部メモリ（図示しない）に記憶されるようにしても良いし、ＲＡＭ２３に記憶されるようにしても良いし、上記不揮発性メモリ２５に記憶されるようにしても良い。

【００２１】

このような監視フラグを初期化すると、上記ＩＣカード２の制御部２２は、受信したコマンドに応じた各種の処理を順次行い、それらの処理の実行に応じて所定のタイミングで監視フラグのセット（監視フラグの値の変更）を行う（ステップＳ１３～Ｓ２０）。つまり、受信した読出コマンドに応じた各処理が正常に実行された場合に、上記制御部２２は、上記監視フラグをセットする処理として監視フラグの値を変更する。

【００２２】

また、上記監視フラグの値（初期値）は、データを出力するまでの各種の処理を終了した時点（データを出力する直前）で所定の値（「０」）となるような値に設定される。また、上記ＩＣカード２では、受信したコマンドに応じて実行すべき種々の処理（処理内容）が決まる。このため、上記監視フラグには、受信したコマンドに応じた所定の初期値が設定される。また、上記監視フラグをセットするタイミング（処理チェックポイント）は、受信したコマンドに応じて予め設定されているものとする。

【００２３】

なお、図３では、データを暗号化して出力する場合における代表的な処理内容と、監視フラグをセットすべき複数のタイミングとの例を示している。ここでは、データを出力する処理の具体例の１つとして、図３に示すようなデータを暗号化して出力する処理について説明する。なお、本実施の形態では、監視フラグをセットすべきタイミングを処理チェックポイントとも称することとする。

【００２４】

すなわち、端末システム１からデータを暗号化して出力する旨のコマンドを受信した場合、上記制御部２２は、まず、当該コマンドに応じた処理チェックポイントの数に基づく監視フラグの初期値を設定する（ステップＳ１２）。なお、図３に示す例では、処理チェックポイントの数が４つである。このため、図３に示す例では、例えば、監視フラグの初期値として「４」が設定される。

【００２５】

上記監視フラグを初期化すると、上記制御部２２は、第１の処理としてセキュリティステータスのチェックを行う（ステップＳ１３）。このセキュリティステータスのチェックとは、セキュリティステータスとして設定されている事項をチェックする処理である。このセキュリティステータスのチェックとしては、たとえば、コマンドの送信元としての端末システム１の認証、あるいは、受信したコマンドの認証などの処理が行われる。

【００２６】

第１の処理としてのセキュリティステータスチェックが正常に終了すると、上記制御部２２は、第１の処理チェックポイントであると判断する。上記第１の処理チェックポイントは、第１の処理に対応して監視フラグをセットするタイミングである。上記判断により第１の処理チェックポイントであると判断した場合、つまり、第１の処理としてのセキュリティステータスチェックが正常に終了したと判断した場合、上記制御部２２は、上記監視フラグをセットする処理を行う。たとえば、第１の処理チェックポイントで監視フラグを「１」づつ減算する場合、上記制御部２２は、現在の監視フラグの値（初期値）から「１」を減算することにより監視フラグのセットを行う。

【００２７】

上記第１の処理チェックポイントで監視フラグをセットすると、上記制御部２２は、第２の処理としての認証子データの検証処理を行う（ステップＳ１５）。この認証子データの検証処理とは、認証子データを正当性を検証する処理である。上記第２の処理としての認証子データの検証処理が正常に終了すると、上記制御部２２は、第２の処理チェックポイントであると判断する。上記第２の処理チェックポイントは、第２の処理に対応して監

視フラグをセットするタイミングである。

【００２８】

上記判断により第２の処理チェックポイントであると判断した場合、つまり、第２の処理としての認証子データの検証処理が正常に終了したと判断した場合、上記制御部２２は、上記監視フラグをセットする処理を行う（ステップＳ１６）。たとえば、第２の処理チェックポイントで監視フラグを「１」づつ減算する場合、上記制御部２２は、現在の監視フラグの値から「１」を減算することにより監視フラグのセットを行う。

【００２９】

上記第２の処理チェックポイントで監視フラグをセットすると、上記制御部２２は、第３の処理としての暗号化処理を行う（ステップＳ１７）。この暗号化処理では、出力すべきデータの暗号化を行う。上記第３の処理としての暗号化処理が正常に終了すると、上記制御部２２は、第３の処理チェックポイントであると判断する。上記第３の処理チェックポイントは、第３の処理に対応して監視フラグをセットするタイミングである。

【００３０】

上記判断により第３の処理チェックポイントであると判断した場合、つまり、第３の処理としての暗号化処理が正常に終了したと判断した場合、上記制御部２２は、上記監視フラグをセットする処理を行う（ステップＳ１８）。たとえば、第３の処理チェックポイントで監視フラグを「１」減算する場合、上記制御部２２は、現在の監視フラグの値から「１」を減算することにより監視フラグのセットを行う。

【００３１】

上記第３の処理チェックポイントで監視フラグをセットすると、上記制御部２２は、第４の処理としての認証子データ処理を行う（ステップＳ１９）。この認証子データ処理とは、暗号化した出力すべきデータに認証子データを付加する処理である。上記第４の処理としての認証子データ処理が正常に終了すると、上記制御部２２は、第４の処理チェックポイントであると判断する。上記第４の処理チェックポイントは、第４の処理に対応して監視フラグをセットするタイミングである。

【００３２】

上記判断により第４の処理チェックポイントであると判断した場合、つまり、第４の処理としての認証子データ処理が正常に終了したと判断した場合、上記制御部２２は、上記監視フラグをセットする処理を行う（ステップＳ２０）。たとえば、第４の処理チェックポイントで監視フラグを「１」減算する場合、上記制御部２２は、現在の監視フラグの値から「１」を減算することにより監視フラグのセットを行う。

【００３３】

図３に示す例では、第１、第２、第３および第４の処理がデータを出力するまでに実行すべき処理である。従って、上記第４の処理チェックポイントで監視フラグをセットすると、上記制御部２２は、受信した読み出しコマンドに応じて、データを出力するまでに実行すべき種々の処理が完了したものと判断する。データを出力するまでに実行すべき種々の処理が終了したと判断した場合、上記制御部２２は、マスクデータを生成する処理を行う（ステップＳ２１およびＳ２２）。

【００３４】

上記マスクデータは、出力すべきデータを保護するために用いられるデータである。本実施の形態では、後述するステップＳ２３において、上記マスクデータを用いて出力すべきデータに演算処理が施される。つまり、上記マスクデータは、監視フラグが所定の値である場合にマスクされるデータを変化させずに、監視フラグが所定の値でない場合にマスクされるデータを変化させるようになっている。

【００３５】

また、上記マスクデータは、たとえば、監視フラグの値を用いても良いし、監視フラグの値と乱数データ（任意のデータ）とに基づいて生成するようにしても良いし、監視フラグの値と当該ＩＣカードの固有データとに基づいて生成するようにしても良いし、過去の処理における監視フラグの値と今回の監視フラグの値とに基づいて生成するようにしても

良い。ここでは、上記マスクデータが監視フラグの値と乱数データとに基づいて生成される場合を想定して説明する。

【００３６】

この場合、上記マスクデータを生成する処理として、上記制御部２２は、上記乱数生成部２６により乱数データを生成する（ステップＳ２１）。上記乱数生成部２６により乱数データを生成すると、上記制御部２２は、生成した乱数データと監視フラグの値とによりマスクデータを生成する（ステップＳ２２）。ここでは、上記制御部２２は、乱数データと監視フラグの値との所定の演算処理により上記マスクデータを生成する。上記マスクデータの生成処理の具体例としては、生成した乱数データに対して監視フラグの数値分のビットシフト演算を行い、その演算結果と乱数データとの排他的論理和を演算する。

【００３７】

上記マスクデータを生成すると、上記制御部２２は、生成したマスクデータにより出力すべきデータをマスク（保護）する処理を行う（ステップＳ２３）。具体的には、上記制御部２２は、生成したマスクデータと出力すべきデータとの所定の演算処理を行う（ステップＳ２３）。つまり、上記制御部２２は、出力すべきデータを保護するために、上記マスクデータを用いて出力すべきデータに演算処理を施す。たとえば、マスクデータを用いた出力すべきデータに対する演算処理として、上記制御部２２は、マスクデータと出力すべきデータとの排他的論理和を演算する。また、上記ステップＳ２３の演算処理としては、マスクデータと出力すべきデータとを、論理和演算、加算、あるいは、シフト演算などを施すようにしても良い。

【００３８】

上記マスクデータを用いて出力すべきデータをマスクすると、上記制御部２２は、受信した読出コマンドに対する応答として、上記マスクデータによりマスクされた出力すべきデータを上記通信インターフェース２１により上記端末システム１へ出力する（ステップＳ２５）。これにより、上記端末システム１では、送信した読出コマンドに対応する応答として当該ＩＣカードからデータを取得する。

【００３９】

上記のようなステップＳ２２～Ｓ２４の具体例として、上記ステップＳ２２で、乱数データを用いて監視フラグの数値分をシフトしたデータと乱数データとの排他的論理和演算を行い、上記ステップＳ２３で、マスクデータと出力すべきデータとの排他的論理和演算を行う場合について説明する。

【００４０】

この場合、監視フラグが「０」であれば、乱数データの値に関らず、上記ステップＳ２２の演算結果としてのマスクデータは、「０」となる。このように、マスタデータが「０」であれば、出力すべきデータは、上記ステップＳ２３の演算処理で改ざんされない。従って、監視フラグが「０」であればマスクデータも「０」となる。このため、上記ステップＳ２４では、出力すべきデータが正常なデータのまま出力される。

【００４１】

これに対して、監視フラグが「０」でなければ、上記ステップＳ２２の演算結果としてのマスクデータは、「０」でなくなる。このように、マスタデータが「０」でなければ、出力すべきデータは、上記ステップＳ２３の演算処理で改ざんされる。すなわち、監視フラグが「０」であればマスクデータも「０」でなくなる。このため、上記ステップＳ２４では、出力すべきデータを改ざんした異常なデータが出力される。

【００４２】

上記のように、本実施の形態のＩＣカードは、データの出力を要求するコマンドに対応する種々の処理の実行状況を監視する監視フラグを全ての処理が正常に実行された場合に所定の値となるような初期値に設定し、実行した処理に応じて監視フラグの値を変更（セット）し、データの出力処理の前までの各処理が完了した段階において監視フラグの値に基づいて出力すべきデータをマスクし、マスクしたデータを出力する。

【００４３】

これにより、上記ＩＣカードでは、監視フラグのチェックが不要となるとともに、正常な処理が行われなければ、正常なデータを出力しないようにすることができる。たとえば、外乱によりプログラムが誤動作して特定の処理過程がスキップされると、監視フラグは正常な値にならない。このため、監視フラグに基づいてマスキングされる出力データは、正常なデータではなくなる。従って、上記のような実施の形態によれば、ＩＣカード内のデータを保護することができ、セキュリティ性の高いＩＣカードを実現することが可能となる。

【００４４】

さらに、上記ＩＣカードは、出力すべきデータに対して、上記マスクデータとの、排他的論理和演算、論理和演算、加算演算、あるいは、シフト演算などの所定の規則に基づいた演算を施し、その演算結果を出力データとして出力する。これにより、監視フラグが所定の値でなければ、実際に出力されるデータは、出力すべきデータとは異なる異常なデータとなる。この結果、ＩＣカード内のデータを保護することが可能となる。

【００４５】

さらに、上記監視フラグにより監視すべき全ての処理が終了すると、上記ＩＣカードは、上記監視フラグの値と乱数データとによりマスクデータを生成し、生成したマスクデータに基づいて出力すべきデータをマスクして出力する。これにより、上記ＩＣカードでは、出力すべきデータを乱数性を持たせてマスクすることができる。この結果、マスクされたデータ（出力されるデータ）の傾向から正しいデータを予測することもできないようにすることができ、セキュリティ性の高いＩＣカードを実現することが可能となる。

【００４６】

なお、上記ＩＣカードでは、全ての処理が正常に行われた場合に「０」となるような初期値を監視フラグに設定し、特定の各処理が実行されるごとに監視フラグの値を減算するようにしても良い。この場合、上記監視フラグにより監視すべき全ての処理が正常に終了すると、上記ＩＣカードは、上記監視フラグの値が「０」となる。このため、マスク処理としては、監視フラグの値が「０」であれば、出力すべきデータが変化しないような演算処理を施すようにする。これにより、上記ＩＣカードでは、全ての処理が正常に終了すると、出力すべきデータをマスクしてもデータが変化しないようにでき、セキュリティ性を高めることができる。

【００４７】

また、上記ＩＣカードには、上記ステップＳ２４でデータを出力するごとに不揮発性メモリ等に当該ＩＣカードに固有な固有データを保持しておき、上記ステップＳ２１～Ｓ２３において、固有データと監視フラグの値とによりマスクデータを生成するようにしても良い。この場合、上記監視フラグにより監視すべき全ての処理が終了すると、上記ＩＣカードは、上記監視フラグの値と当該ＩＣカードの固有データとによりマスクデータを生成し、生成したマスクデータに基づいて出力すべきデータをマスクして出力する。これにより、上記ＩＣカードでは、出力すべきデータを各ＩＣカードの固有データに応じてマスクすることができ、セキュリティ性を向上させることが可能となる。

【００４８】

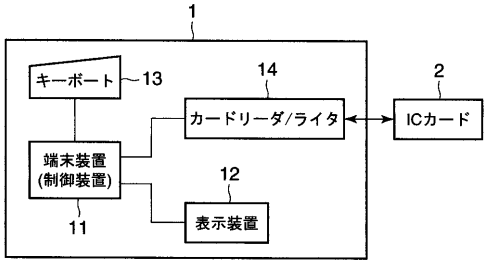
また、上記ＩＣカードには、上記のような処理を行う毎（上記ステップＳ２４でマスクしたデータを出力する毎）に当該出力データをマスクするために用いた監視フラグの値を不揮発性メモリ２５に保存しておき、上記ステップＳ２１～Ｓ２３において、前回の監視フラグの値と今回の監視フラグの値とによりマスクデータを生成するようにしても良い。この場合、上記監視フラグにより監視すべき全ての処理が終了すると、当該ＩＣカードでは、今回の監視フラグの値と不揮発性メモリに保存している前回の監視フラグの値とを加算し、乱数データを用いて加算した数値分をシフトしたデータと乱数データとによりマスクデータを生成し、生成したマスクデータに基づいて出力すべきデータをマスクして出力する。これにより、監視フラグの値を保存しておくことで、毎回同じ箇所でプログラムが誤動作する場合に対しても、セキュリティ性を向上させることをが可能となる。

【００４９】

次に、上記したような処理の変形例について説明する。
図４は、上記ＩＣカード２における処理例を説明するためのフローチャートである。
なお、図４は、図３の処理の変形例を説明するためのフローチャートである。このため、図４に示す処理例の説明としては、図３に示す各ステップと同様な処理ステップについては、同一箇所に同一符号を付して詳細な説明を省略するものとする。図４に示すフローチャートでは、図３に示すフローチャートにステップＳ３１およびＳ３２が付加されたものとなっている。
【００５０】
すなわち、データを出力する処理の前までに実行すべき種々の処理（第１、第２、第３および第４の処理）が完了したものと判断した場合、上記制御部２２は、監視フラグの値が所定の値（例えば、「０」）であるか否かを判断する（ステップＳ３１）。この判断により監視フラグが所定の値でないと判断した場合、上記制御部２２は、エラーステータスを出力し（ステップＳ３２）、当該処理を終了する。また、上記判断により監視フラグが所定の値であると判断した場合、上記制御部２２は、上記ステップＳ２１へ進む。
【００５１】
従って、図４に示す変形例では、監視フラグが所定の値（「０」）でないと判断すれば、上記制御部２２は、データを出力することなく、エラーステータスを出力して当該読出コマンドに対する処理を終了する。また、監視フラグの値が所定の値（「０」）であると判断すれば、上記制御部２２は、マスクデータの生成し、マスクデータによりマスクしたデータを出力する。
【００５２】
つまり、このような変形例によれば、監視フラグのチェックによって監視フラグが所定の値でないと判断した場合にはデータを出力せずにエラーであることを通知でき、監視フラグのチェックがスキップされてしまった場合であっても出力すべきデータを監視フラグの値に基づくマスクデータによってマスクすることができる。
【００５３】
言い換えれば、通常のエラーによって監視フラグの値が所定の値でなくなった場合、ＩＣカードは、エラーが発生した旨を通知でき、不正に監視フラグのチェックがスキップされた場合には、監視フラグの値が所定の値でなければ、出力すべきデータを改ざんして出力することができる。
【図面の簡単な説明】
【００５４】
【図１】この発明の実施の形態に係る携帯可能電子装置としてのＩＣカードとＩＣカードとの通信を行う外部装置としてのＩＣカード処理装置の構成例を概略的に示すブロック図。
【図２】ＩＣカードの構成例を示すブロック図。
【図３】データの読み出しを要求する読出コマンドを受信した場合の処理を説明するためのフローチャート。
【図４】図３の処理の変形例を説明するためのフローチャート。
【符号の説明】
【００５５】
１…端末システム（ＩＣカード処理装置）、２…ＩＣカード（携帯可能電子装置）、１１…端末装置、１２…表示装置、１３…キーボード、１４…カードリーダライタ、２１…コンタクト部、２２…制御部、２３…ＲＡＭ、２４…ＲＯＭ、２５…不揮発性メモリ、２６…乱数生成部

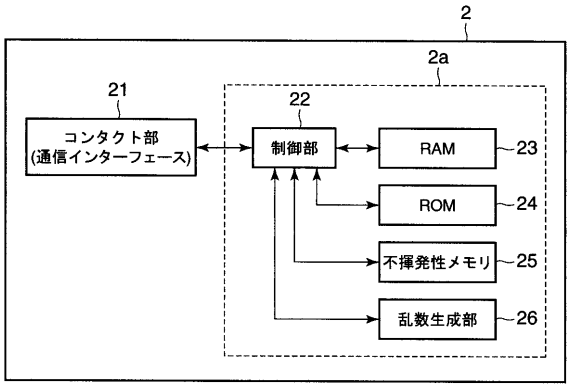
【図１】

図１



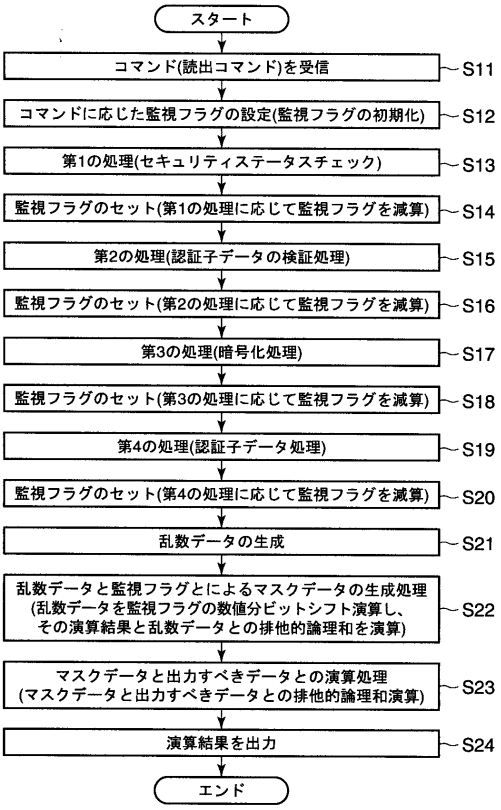
【図２】

図２



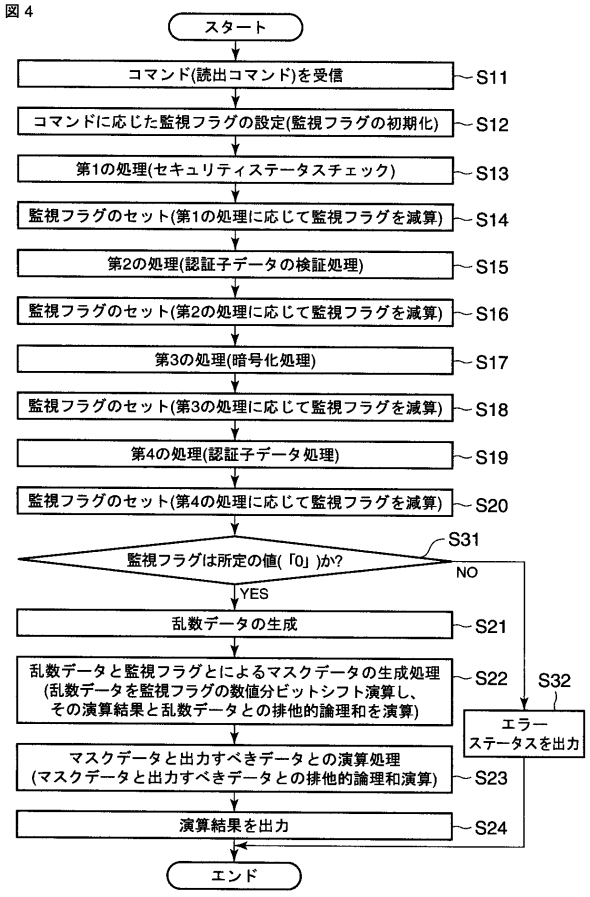
【図３】

図３



【図４】

図４



フロントページの続き

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 柳田 将
東京都青梅市新町３丁目３番地の５ 東芝デジタルメディアエンジニアリング株式会社内
(72)発明者 江尻 正仁
東京都青梅市新町３丁目３番地の５ 東芝デジタルメディアエンジニアリング株式会社内

Ｆターム(参考) 5B017 AA03 BB05 BB09 CA14
5B035 AA13 BB09 CA11 CA31 CA38
5J104 AA01 AA12 AA16 AA32 AA44 AA47 EA04 EA15 EA16 JA03
NA02 NA27 NA35 NA40 NA42 PA14