(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2009-32003
(P2009-32003A)
(43)公開日　平成21年2月12日(2009.2.12)

(51)Int.Cl.		F I			テーマコード（参考）
G06K 19/10	(2006.01)	G06K	19/00	R	5B035
G06K 17/00	(2006.01)	G06K	17/00	T	5B058
H04L 9/32	(2006.01)	H04L	9/00	675A	5J104

審査請求 未請求　請求項の数 10　ＯＬ　（全 14 頁）

(21)出願番号　特願2007-194818 (P2007-194818)
(22)出願日　平成19年7月26日 (2007.7.26)

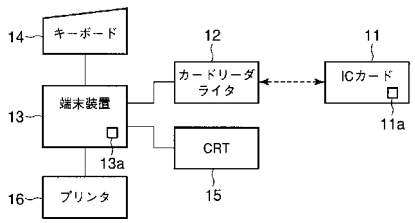
(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】携帯可能電子装置、端末装置、認証システム、及び認証方法

(57)【要約】
【課題】　セキュリティ性の高い携帯可能電子装置、端末装置、認証システム、及び認証方法を提供する。
【解決手段】　携帯可能電子装置１１は、携帯可能電子装置１１を処理する端末装置１３より乱数要求コマンドを受信した場合、乱数を生成し、生成した乱数を前記端末装置１３に送信する。前記携帯可能電子装置１１と前記端末装置１３は、予め記憶している複数の暗号鍵のうち１つを前記乱数に基づいて選択し、選択した前記暗号鍵を用いて相互に認証処理を行なう。
【選択図】　図１

図1



【特許請求の範囲】
【請求項１】
端末装置から送信されるコマンドに応じた処理を行なう携帯可能電子装置であって、
前記端末装置とデータの送受信を行なう送受信手段と、
複数の鍵データを記憶している記憶手段と、
前記端末装置より乱数要求コマンドを受信した場合、乱数を生成する乱数生成手段と、
前記乱数生成手段により生成した乱数を前記端末装置に送信する処理手段と、
前記乱数生成手段により生成した乱数に基づいて前記記憶手段に記憶されている複数の鍵データから１つの鍵データを選択する選択手段と、
前記選択手段により選択された鍵データに対応している鍵データを前記端末装置が持っているか否かにより前記端末装置を認証する認証手段と、
を具備することを特徴とする携帯可能電子装置。
【請求項２】
前記認証手段は、
前記乱数生成手段により生成された乱数を前記送受信手段により前記端末装置へ送信する手段と、
前記選択手段により選択された鍵データを用いて第１の認証用データを暗号化する暗号化手段と、
前記暗号化手段により暗号化された暗号化データを前記送受信手段により前記端末装置へ送信する手段と、
前記端末装置により暗号化データが復号化されたデータである第２の認証用データを前記送受信手段により受信する手段と、
前記第１の認証用データと前記端末装置より受信した第２の認証用データとを照合する照合手段と、
前記照合手段による照合結果を前記送受信手段により前記端末装置へ送信する手段と、
を具備することを特徴とする請求項１に記載の携帯可能電子装置。
【請求項３】
前記認証手段は、
前記乱数生成手段により生成された乱数を前記送受信手段により前記端末装置へ送信する手段と、
前記端末装置により第１の認証用データが暗号化されたデータである暗号化データを前記送受信手段により受信する手段と、
前記選択手段により選択された鍵データを用いて前記暗号化データを復号化する復号化手段と、
前記復号化手段により復号化された復号化データを第２の認証用データとして前記送受信手段により前記端末装置へ送信する手段と、
を具備することを特徴とする請求項１に記載の携帯可能電子装置。
【請求項４】
さらに、前記各手段を有するモジュールと、
前記モジュールが内蔵された本体と、
を具備することを特徴とする請求項１乃至３のいずれか１項に記載の携帯可能電子装置。
【請求項５】
携帯可能電子装置にコマンドを送信し処理を行なう端末装置であって、
前記携帯可能電子装置とデータの送受信を行なう送受信手段と、
前記携帯可能電子装置に記憶されている複数の鍵データに対応する複数の鍵データを記憶している記憶手段と、
前記携帯可能電子装置に乱数要求コマンドを前記送受信手段により送信し、前記コマンドに対するレスポンスとして前記携帯可能電子装置から受信した乱数に基づいて前記記憶手段に記憶されている複数の鍵データから１つの鍵データを選択する選択手段と、

前記選択手段により選択された鍵データに対応している鍵データを前記携帯可能電子装置が持っているか否かにより前記携帯可能電子装置を認証する認証手段と、
を具備することを特徴とする端末装置。
【請求項６】
前記認証手段は、
前記選択手段により選択された鍵データを用いて第１の認証用データを暗号化する暗号化手段と、
前記暗号化手段により暗号化された暗号化データを前記送受信手段により前記携帯可能電子装置へ送信する手段と、
前記携帯可能電子装置により暗号化データが復号化されたデータである第２の認証用データを前記送受信手段により受信する手段と、
前記第１の認証用データと前記携帯可能電子装置より受信した第２の認証用データとを照合する照合手段と、
を具備することを特徴とする請求項５に記載の端末装置。
【請求項７】
前記認証手段は、
前記携帯可能電子装置により第１の認証用データが暗号化されたデータである暗号化データを前記送受信手段により受信する手段と、
前記選択手段により選択された鍵データを用いて前記暗号化データを復号化する復号化手段と、
前記復号化手段により復号化された復号化データを第２の認証用データとして前記送受信手段により前記携帯可能電子装置へ送信する手段と、
を具備することを特徴とする請求項５に記載の端末装置。
【請求項８】
端末装置と携帯可能電子装置とを備える認証システムであって、
前記携帯可能電子装置は、
前記端末装置とデータの送受信を行なう第１の送受信手段と、
複数の鍵データを記憶している第１の記憶手段と、
前記端末装置より乱数要求コマンドを受信した場合、乱数を生成する乱数生成手段と、
前記乱数生成手段により生成した乱数を前記端末装置に送信する処理手段と、
前記乱数生成手段により生成した乱数に基づいて前記第１の記憶手段に記憶されている複数の鍵データから１つの鍵データを選択する第１の選択手段と、
前記選択手段により選択された鍵データに対応している鍵データを前記端末装置が持っているか否かにより前記端末装置を認証する第１の認証手段と、
を具備し、
前記端末装置は、
前記携帯可能電子装置とデータの送受信を行なう第２の送受信手段と、
複数の鍵データを記憶している第２の記憶手段と、
前記携帯可能電子装置に乱数要求コマンドを前記第２の送受信手段により送信し、前記コマンドに対するレスポンスとして前記携帯可能電子装置から受信した乱数に基づいて前記第２の記憶手段に記憶されている複数の鍵データから１つの鍵データを選択する第２の選択手段と、
前記第２の選択手段により選択された鍵データに対応している鍵データを前記携帯可能電子装置が持っているか否かにより前記携帯可能電子装置を認証する第２の認証手段と、
を具備することを特徴とする認証システム。
【請求項９】
端末装置とデータの送受信を行なう送受信手段を有する携帯可能電子装置に用いられる前記端末装置の認証方法であって、
前記端末装置より乱数要求コマンドを受信した場合、乱数を生成し、
生成した乱数を前記端末装置に送信し、

生成した乱数に基づいて複数の鍵データを記憶している記憶手段から１つの鍵データを選択し、
選択された鍵データに対応している鍵データを前記端末装置が持っているか否かにより前記端末装置を認証する、
ことを特徴とする認証方法。
【請求項１０】
携帯可能電子装置とデータの送受信を行なう送受信手段を有する端末装置に用いられる前記携帯可能電子装置の認証方法であって、
前記携帯可能電子装置に乱数要求コマンドを送信し、前記乱数要求コマンドに対するレスポンスとして前記携帯可能電子装置から受信した乱数に基づいて前記携帯可能電子装置に記憶されている複数の鍵データに対応する複数の鍵データを記憶している記憶手段から１つの鍵データを選択し、
選択された鍵データに対応している鍵データを前記携帯可能電子装置が持っているか否かにより前記携帯可能電子装置を認証する、
ことを特徴とする認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、例えば、通信インターフェースを備え、装置間で通信を行なう携帯可能電子装置、端末装置、認証システム、及び認証方法関する。
【背景技術】
【０００２】
一般的に、携帯可能電子装置としてのＩＣカードは、プラスチックなどで形成されたカード状の筐体内にＩＣチップが埋め込まれているものである。
たとえば、上記ＩＣカードは、エレクトリック・パース（電子貨幣、電子マネー）、電子商取引（エレクトリック・コマース）、及び企業内部のプライベートセキュリティシステム（ドアセキュリティシステム、ネットワーク上のアクセス管理など）に用いられている。これらのような用途においては、セキュリティが極めて重要となる。従来のＩＣカードには、不正利用を防止するため、不揮発性メモリに鍵情報などの認証用の情報が記憶されるものがある。このような認証用の情報が悪意のある者により特定されてしまった場合、当該ＩＣカードが不正使用される可能性があるという問題がある。そこで、ＩＣカードの保持している暗号鍵を用いてデータの暗号化及び復号化を行い、書き込み及び読出しを実行するＩＣカードシステムが提示されている（たとえば、特許文献１参照）。
【０００３】
しかしながら、上記した従来のＩＣカードシステムでは、ＩＣカードとＩＣカードのリダ装置とで、常に同一の１セットの暗号鍵がデータの暗号化及び復号化に用いられている。この場合、既知の暗号化前のデータ（元データ）と暗号化後のデータ（暗号化データ）の相関関係に着目することにより、暗号化データから未知の元データを解析することができる可能性があるという問題がある。また、暗号化処理の処理内容を解析して暗号鍵を推定することがされた場合、ＩＣカードが容易に不正使用することが可能となってしまうという問題がある。
【特許文献１】特開２００５－１２２４０２号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
そこで、本発明の一形態では、セキュリティ性の高い携帯可能電子装置、端末装置、認証システム、及び認証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】
上記目的を達成する為、本発明の一形態に係る携帯可能電子装置は、端末装置から送信

されるコマンドに応じた処理を行なう携帯可能電子装置であって、前記端末装置とデータの送受信を行なう送受信手段と、複数の鍵データを記憶している記憶手段と、前記端末装置より乱数要求コマンドを受信した場合、乱数を生成する乱数生成手段と、前記乱数生成手段により生成した乱数を前記端末装置に送信する処理手段と、前記乱数生成手段により生成した乱数に基づいて前記記憶手段に記憶されている複数の鍵データから１つの鍵データを選択する選択手段と、前記選択手段により選択された鍵データに対応している鍵データを前記端末装置が持っているか否かにより前記端末装置を認証する認証手段とを具備する。

【０００６】

また、本発明の一形態に係る端末装置は、携帯可能電子装置にコマンドを送信し処理を行なう端末装置であって、前記携帯可能電子装置とデータの送受信を行なう送受信手段と、前記携帯可能電子装置に記憶されている複数の鍵データに対応する複数の鍵データを記憶している記憶手段と、前記携帯可能電子装置に乱数要求コマンドを前記送受信手段により送信し、前記コマンドに対するレスポンスとして前記携帯可能電子装置から受信した乱数に基づいて前記記憶手段に記憶されている複数の鍵データから１つの鍵データを選択する選択手段と、前記選択手段により選択された鍵データに対応している鍵データを前記携帯可能電子装置が持っているか否かにより前記携帯可能電子装置を認証する認証手段とを具備する。

【０００７】

また、本発明の一形態に係る認証システムは、端末装置と携帯可能電子装置とを備える認証システムであって、前記携帯可能電子装置は、前記端末装置とデータの送受信を行なう第１の送受信手段と、複数の鍵データを記憶している第１の記憶手段と、前記端末装置より乱数要求コマンドを受信した場合、乱数を生成する乱数生成手段と、前記乱数生成手段により生成した乱数を前記端末装置に送信する処理手段と、前記乱数生成手段により生成した乱数に基づいて前記第１の記憶手段に記憶されている複数の鍵データから１つの鍵データを選択する第１の選択手段と、前記選択手段により選択された鍵データに対応している鍵データを前記端末装置が持っているか否かにより前記端末装置を認証する第１の認証手段とを具備し、前記端末装置は、前記携帯可能電子装置とデータの送受信を行なう第２の送受信手段と、複数の鍵データを記憶している第２の記憶手段と、前記携帯可能電子装置に乱数要求コマンドを前記第２の送受信手段により送信し、前記コマンドに対するレスポンスとして前記携帯可能電子装置から受信した乱数に基づいて前記第２の記憶手段に記憶されている複数の鍵データから１つの鍵データを選択する第２の選択手段と、前記第２の選択手段により選択された鍵データに対応している鍵データを前記携帯可能電子装置が持っているか否かにより前記携帯可能電子装置を認証する第２の認証手段とを具備する。

【０００８】

また、本発明の一形態に係る認証方法は、端末装置とデータの送受信を行なう送受信手段を有する携帯可能電子装置に用いられる前記端末装置の認証方法であって、前記端末装置より乱数要求コマンドを受信した場合、乱数を生成し、生成した乱数を前記端末装置に送信し、生成した乱数に基づいて複数の鍵データを記憶している記憶手段から１つの鍵データを選択し、選択された鍵データに対応している鍵データを前記端末装置が持っているか否かにより前記端末装置を認証する。

【０００９】

また、本発明の一形態に係る認証方法は、携帯可能電子装置とデータの送受信を行なう送受信手段を有する端末装置に用いられる前記携帯可能電子装置の認証方法であって、前記携帯可能電子装置に乱数要求コマンドを送信し、前記乱数要求コマンドに対するレスポンスとして前記携帯可能電子装置から受信した乱数に基づいて前記携帯可能電子装置に記憶されている複数の鍵データに対応する複数の鍵データを記憶している記憶手段から１つの鍵データを選択し、選択された鍵データに対応している鍵データを前記携帯可能電子装置が持っているか否かにより前記携帯可能電子装置を認証する。

【発明の効果】
【００１０】
この発明の一形態によれば、セキュリティ性の高い携帯可能電子装置、端末装置、認証システム、及び認証方法を提供することができる。
【発明を実施するための最良の形態】
【００１１】
以下、図面を参照しながら、本発明の一実施形態に係る携帯可能電子装置、端末装置、認証システム、及び認証方法について詳細に説明する。
【００１２】
まず、携帯可能電子装置と端末装置とから構成される携帯可能電子装置の認証システムについて説明する。
【００１３】
図１は、本発明の実施の形態に係る携帯可能電子装置（ＩＣカード）１１と端末装置１３の構成例を概略的に示すブロック図である。
端末装置１３は、カードリーダライタ１２、キーボード１４、ＣＲＴ１５、及び、プリンタ１６などに接続されている。
【００１４】
端末装置１３は、ＣＰＵ、種々のメモリ及び各種インターフェースなどを有する。また、端末装置１３は、カードリーダライタ１２によりＩＣカード１１とデータの送受信を行なう機能、ＩＣカード１１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。
たとえば、端末装置１３は、カードリーダライタ１２を介してＩＣカード１１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１１内の不揮発性メモリにデータを書き込む。また、端末装置１３は、ＩＣカード１１に読み取りコマンドを送信することによりＩＣカード１１からデータを読み出す。これにより、ＩＣカード１１に記憶されているデータが正当なものであるか否かを認証する認証処理を行なうこともできる。通常、認証処理は、暗号鍵を用いて暗号化したデータ、及び復号化したデータなどを端末装置１３とＩＣカード１１との間で通信を行い、照合することにより実行される。端末装置１３は、認証処理の為の複数の暗号鍵を記憶する暗号鍵記憶部１３ａをさらに備えている。端末装置１３は、暗号鍵記憶部１３ａに記憶されている暗号鍵を用いて、データの暗号化及び復号化を行なうことができる。
【００１５】
カードリーダライタ１２は、ＩＣカード１１との通信を行うためのインターフェース装置である。カードリーダライタ１２では、ＩＣカード１１に対する電源供給、クロック供給、リセット制御、データの送受信が行われるようになっている。このような機能によってカードリーダライタ１２は、端末装置１３による制御に基づいてＩＣカード１１の活性化（起動）、種々のコマンドの送信、及び送信したコマンドに対する応答の受信などを行なう。
【００１６】
キーボード１４は、端末装置１３の操作員が操作する操作部として機能し、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。ＣＲＴ１５は、端末装置１３の制御により種々の情報を表示する表示装置である。プリンタ１６は、端末装置１３による処理結果などを印刷する出力手段である。
【００１７】
次に、ＩＣカード１１について説明する。
ＩＣカード１１は、端末装置１３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、ＩＣカード１１が接触式通信により端末装置１３と接続される場合、つまり、ＩＣカード１１が接触式のＩＣカードで構成される場合、ＩＣカード１１は、通信インターフェースとしての通信インターフェース　を介して端末装置１３からの動作電源及び動作クロックの供給を受けて活性化さ

れる。

【００１８】

また、ＩＣカード１１が非接触式の通信方式により端末装置１３と接続される場合、つまり、ＩＣカード１１が非接触式のＩＣカードで構成される場合、ＩＣカード１１は、通信インターフェースとしてのアンテナ及び通信制御部などを介して端末装置１３からの電波を受信し、その電波から電源回路により動作電源及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。

【００１９】

ＩＣカード１１は、端末装置１３とデータの送受信を行なうことにより認証処理を行なうことができる。即ち、ＩＣカード１１は、認証処理の為の暗号鍵を複数記憶する暗号鍵記憶部１１ａをさらに備えている。

【００２０】

次に、ＩＣカード１１の構成例について説明する。

【００２１】

図２は、本第１の実施の形態に係るＩＣカード１１の構成例を概略的に示すブロック図である。ＩＣカード１１は、本体１１１を構成する筐体内にモジュール１１２が内蔵されている。モジュール１１２は、１つまたは複数のＩＣチップ１１３と通信用の外部インターフェース（通信インターフェース）とが接続された状態で一体的に形成され、ＩＣカード１１の本体１１１内に埋設されている。また、ＩＣカード１１のモジュール１１２は、図２に示すように、制御素子１０１、不揮発性メモリ１０２、揮発性メモリ１０３、プログラムメモリ１０４、電源回路１０５、電圧検出回路１０６、及び通信インターフェース１０７を有してしている。

【００２２】

制御素子１０１は、当該ＩＣカード１１全体の制御を司るものである。制御素子１０１は、プログラムメモリ１０４あるいは不揮発性メモリ１０２に記憶されている制御プログラムや制御データに基づいて動作することにより、種々の処理手段として機能する。

【００２３】

不揮発性メモリ１０２は、例えば、ＥＥＰＲＯＭあるいはフラッシュＲＯＭなどの、データの書き込み及び書換えが可能な不揮発性のメモリにより構成される。不揮発性メモリ１０２には、当該ＩＣカード１１の運用用途に応じて制御プログラムや種々のデータが書込まれる。たとえば、不揮発性メモリ１０２では、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制御プログラムや種々のデータが書き込まれる。また不揮発性メモリ１０２は、複数の暗号鍵が記憶される暗号鍵記憶部１１ａを備えている。即ち、不揮発性メモリ１０２は、記憶手段として機能する。

【００２４】

揮発性メモリ１０３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、揮発性メモリ１０３は、制御素子１０１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。例えば、揮発性メモリ１０３は、通信インターフェース１０７を介して端末装置１３から受信したデータを一時保管するようになっている。

【００２５】

プログラムメモリ１０４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。プログラムメモリ１０４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１１内に組み込まれるものである。つまり、プログラムメモリ１０４に記憶されている制御プログラムや制御データは、予め当該ＩＣカード１１の仕様に応じて組み込まれる。

【００２６】

また、プログラムメモリ１０４は、乱数を生成するための乱数生成プログラムを記憶している。制御素子１０１は、図１に示す端末装置１３より乱数データ要求コマンドを受信した場合、この乱数生成プログラムを実行することにより、乱数を生成する乱数生成手段として機能する。生成された乱数は、端末装置１３に、乱数データ要求コマンドのレスポ

ンスとして送信される。また、プログラムメモリ１０４は、暗号復号化プログラムを複数記憶している。制御素子１０１は、暗号鍵を用いてこの暗号復号化プログラムを実行することにより、データの暗号化及び復号化を行なう。

【００２７】

電源回路１０５は、ＩＣカード１１が非接触式通信を行う場合、図１に示すカードリーダライタ１２から受信した電波から動作電源及び動作クロックを生成してモジュール１１２内の各部に供給する。電圧検出回路１０６は、制御素子１０１に供給される電圧を監視する制御素子１０１のリセット回路として機能する。

【００２８】

通信インターフェース１０７は、送受信手段として機能し、図１に示すカードリーダライタ１２との通信を行うためのインターフェースである。当該ＩＣカード１１が接触式のＩＣカードとして実現される場合、通信インターフェース１０７は、カードリーダライタ１２と接触して信号の送受信を行うための通信制御部と外部インターフェースとしてのコンタクト部とにより構成される。また、当該ＩＣカード１１が非接触式のＩＣカードとして実現される場合、通信インターフェース１０７は、カードリーダライタ１２との無線通信を行うための通信制御部と外部インターフェースとしてのアンテナとにより構成される。

【００２９】

図３は、ＩＣカード１１の暗号鍵記憶部１１ａに記憶されている暗号鍵の一例を示す説明図である。

暗号鍵記憶部１１ａには、暗号鍵としての鍵データＡと鍵データＢが記憶されている。鍵データＡは、「０」に対応付けられている。また鍵データＢは、「１」に対応付けられている。即ち、図２に示す制御素子１０１が乱数生成プログラムを実行することにより生成された乱数の先頭ビットが「０」の場合鍵データＡ、先頭ビットが「１」の場合鍵データＢを選択するように乱数と鍵データとが対応付けられている。

【００３０】

図４は、端末装置１３の暗号鍵記憶部１３ａに記憶されている暗号鍵の一例を示す説明図である。

暗号鍵記憶部１３ａには、ＩＣカード１１の暗号鍵記憶部１１ａに記憶されている鍵データＡとペアである暗号鍵としての鍵データＡｐと、鍵データＢとペアである鍵データＢｐとが記憶されている。鍵データＡｐは、「０」に対応付けられている。また鍵データＢｐは、「１」に対応付けられている。即ち、図１に示す端末装置は、ＩＣカード１１より受信した乱数の先頭ビットが「０」の場合鍵データＡ、先頭ビットが「１」の場合鍵データＢを選択するように乱数と鍵データとが対応付けられている。

【００３１】

制御素子１０１は、プログラムメモリ１０４に複数記憶されている暗号復号化プログラムから、選択した鍵データに対応するプログラムを実行し、暗号化、若しくは復号化を行なう。なお、鍵データＡと、鍵データＡｐとは、例えば公開鍵暗号方式のように、鍵データＡを用いて暗号化したデータを鍵データＡｐを用いて復号化すると元のデータになる、という関係を有している。また、逆に、鍵データＡと、鍵データＡｐとは、鍵データＡｐを用いて暗号化したデータを鍵データＡを用いて復号化すると元のデータになる、という関係を有している。この関係は、鍵データＢと、鍵データＢｐにおいても同様である。

【００３２】

これにより、ＩＣカード１１と端末装置１３とは、異なる鍵データを用いて暗号化、若しくは復号化を行なう。この為、鍵データ（暗号鍵）を見破られるリスクが軽減する。

【００３３】

次に、上記した認証システムにおける認証方法について説明する。

【００３４】

図５は、図１に示す認証システムの各構成における処理を説明するためのシーケンスである。

端末装置１３は、カードリーダライタ１２によりＩＣカード１１を検知すると（ステップＳ１１）、ＩＣカード１１に、図６に示す乱数データ要求コマンドを送信する（ステップＳ１２）。乱数データ要求コマンドは、図２に示すＩＣカード１１の制御素子１０１に乱数生成プログラムを実行させるためのコマンドである。

【００３５】

ＩＣカード１１の制御素子１０１は、端末装置１３より乱数データ要求コマンドを受信すると、乱数生成プログラムを実行し、図６に示す８バイトの乱数データを生成する（ステップＳ１３）。制御素子１０１は、生成した乱数データを揮発性メモリ１０３に一時的に記憶し（ステップＳ１４）、さらに、生成した乱数データを乱数データ要求コマンドのレスポンスとして端末装置１３に送信する（ステップＳ１５）。ここで生成された乱数データは、ＩＣカード１１及び端末装置１３に暗号鍵を選択させる為の先頭ビットが設定されている。

【００３６】

端末装置１３は、ＩＣカード１１より受信した乱数データを図示しない記憶部に一時的に記憶する（ステップＳ１６）。さらに、端末装置１３は、記憶した乱数データに応じて暗号鍵記憶部１３ａに記憶されている鍵データを選択する（ステップＳ１７）。即ち、端末装置１３は、乱数データの先頭ビットを参照し、先頭ビットが「０」の場合鍵データＡｐ、先頭ビットが「１」の場合鍵データＢｐを選択する。ここで、端末装置１３は、ＩＣカード１１に、選択した鍵データにより暗号化が施された暗号化データを要求するコマンドを送信する。

【００３７】

制御素子１０１は、コマンドを受信すると、揮発性メモリ１０３に記憶した乱数データに応じて暗号鍵記憶部１１ａに記憶されている鍵データを選択する（ステップＳ１８）。即ち、制御素子１０１は、乱数データの先頭ビットを参照し、先頭ビットが「０」の場合鍵データＡ、先頭ビットが「１」の場合鍵データＢを選択する。

【００３８】

次に、ＩＣカード１１及び端末装置１３は、認証処理を行なう。即ち、まず、ＩＣカード１１の制御素子１０１は、認証処理用の所定のデータを選択した鍵データとその選択した鍵データに対応する暗号復号化プログラムを用いて暗号化する（ステップＳ１９）。制御素子１０１は、所定のデータを暗号化した暗号化データを端末装置１３に送信する（ステップＳ２０）。

【００３９】

端末装置１３は、ＩＣカード１１より受信した暗号化データを選択した鍵データとその選択した鍵データに対応する暗号復号化プログラムを用いて復号化する（ステップＳ２１）。端末装置１３は、暗号化データを復号化した復号化データをＩＣカード１１に送信する（ステップＳ２２）。

【００４０】

ＩＣカード１１の制御素子１０１は、認証処理用の所定のデータと端末装置１３より受信した復号化データとが一致するか否か照合する（ステップＳ２３）。制御素子１０１は、照合結果を端末装置１３に送信する（ステップＳ２４）。ここでは、ＩＣカード１１は、例えば、所定のデータと復号化データが一致する場合、ＯＫの照合結果を端末装置１３に送信し、所定のデータと復号化データが一致しない場合、ＮＧの照合結果を端末装置に送信する。端末装置１３は、受信した照合結果に応じて、ＩＣカード１１が正当なカードであるか否かを判定する。

【００４１】

なお、制御素子１０１が乱数生成プログラムにより生成する乱数データのサイズは８バイトとしたが、任意のサイズの乱数データを生成するようにしてもよい。

【００４２】

認証処理の照合処理をＩＣカード１１でするとしたが、通常、続けて、端末装置１３でも認証処理を行う。この場合、まず、端末装置１３は、認証処理用の所定のデータを選択

した鍵データとその選択した鍵データに対応する暗号復号化プログラムを用いて暗号化する。端末装置１３は、所定のデータを暗号化した暗号化データを端末装置１３に送信する。

【００４３】

ＩＣカード１１の制御素子１０１は、端末装置１３より受信した暗号化データを選択した鍵データとその選択した鍵データに対応する暗号復号化プログラムを用いて復号化する。制御素子１０１は、暗号化データを復号化した復号化データを端末装置１３に送信する。

【００４４】

端末装置１３は、認証処理用の所定のデータとＩＣカード１１より受信した復号化データとが一致するか否かを照合する　。

【００４５】

なお、暗号鍵を選択する為に乱数データの先頭ビットの値を参照するとしたが、参照するビットの位置は、ＩＣカード１１と端末装置１３とで同じ位置であれば何ビット目を参照してもよい。

【００４６】

また、乱数データ要求コマンドに乱数データの中の参照すべきビットの位置を特定する値（ビット特定値）を加えることにより、鍵データを選択する為のビットを指定してもよい。この場合、図５に示すステップ１２及びステップ１５において、図７に示すデータが送受信される。即ち、端末装置１３は、ビット特定値が加えられた乱数データ要求コマンドをＩＣカード１１に送信する。ＩＣカード１１は、乱数データを生成し、ビット特定値が加えられた乱数データを端末装置１３に送信する。ＩＣカード１１および端末装置１３は、乱数データのうちのビット特定値により指定された位置のビットの値を参照し、鍵データを特定する。例えば、図７に示すように、ビット特定値が「５」である場合、ＩＣカード１１および端末装置１３は、乱数データの先頭ビットから数えて５番目のビットの値を鍵データを特定するための値として参照する。

【００４７】

また、上記した実施形態では、暗号鍵記憶部１１ａおよび１３ａに記憶されている暗号鍵はそれぞれ２つである例を示したが、２つ以上でもよい。例えば、暗号鍵記憶部１１ａおよび１３ａに記憶されている暗号鍵がそれぞれ４つである場合、鍵データを特定するための値は必然的に２ビット必要となる。即ち、ＩＣカード１１および端末装置１３は、図８に示すように、２ビットの組み合わせを、鍵データを選択する為の値として扱う。

【００４８】

図９は、ＩＣカード１１の暗号鍵記憶部１１ａに記憶されている暗号鍵の一例を示す説明図である。暗号鍵記憶部１１ａには、鍵データＡ、Ｂ、Ｃ、及びＤが記憶されている。鍵データＡ、Ｂ、Ｃ、及びＤは、それぞれ「００」、「０１」、「１０」、「１１」に対応付けられている。即ち、Ｉカードの制御素子１０１は、図８に示す鍵データを選択する為の値が「００」の場合鍵データＡ、「０１」の場合鍵データＢ、「１０」の場合鍵データＣ、「１１」の場合鍵データＤを選択し、認証処理に用いる。

【００４９】

図１０は、端末装置の暗号鍵記憶部１３ａに記憶されている暗号鍵の一例を示す説明図である。暗号鍵記憶部１３ａには、図９に示す鍵データＡ、Ｂ、Ｃ、及びＤとそれぞれペアとなる鍵データＡｐ、Ｂｐ、Ｃｐ、及びＤｐが記憶されている。鍵データＡｐ、Ｂｐ、Ｃｐ、及びＤｐは、それぞれ「００」、「０１」、「１０」、「１１」に対応付けられている。即ち、端末装置１３は、図８に示す鍵データを選択する為の値が「００」の場合鍵データＡｐ、「０１」の場合鍵データＢｐ、「１０」の場合鍵データＣｐ、「１１」の場合鍵データＤｐを選択し、認証処理に用いる。

【００５０】

上記したように、ＩＣカード１１に予め複数の暗号鍵を記憶し、ＩＣカード１１を処理する端末装置１３にＩＣカード１１に記憶されている複数の暗号鍵とペアとなる複数の暗

号鍵を記憶する。ＩＣカード１１を検知した場合、端末装置１３は、ＩＣカード１１に乱数データ要求コマンドを送信する。ＩＣカード１１は乱数を生成し、生成した乱数データを端末装置１３にレスポンスとして送信する。ＩＣカード１１および端末装置１３は、乱数データの先頭のビットの値を参照し、記憶している複数の暗号鍵のうちの１つをそれぞれ選択する。ＩＣカード１１および端末装置１３は、選択した暗号鍵を用いて互いに認証処理を行なう。

【００５１】

このような構成によれば、ＩＣカードとＩＣカードを処理する端末装置とで異なる暗号鍵が用いられる為、暗号鍵の推定を困難にすることができる。また、常に同じ暗号鍵を用いるのではなく、複数組の暗号鍵のうちの１組を乱数に基づいて決定するため、元データ及び暗号鍵の推定をより困難にすることができる。この結果として、よりセキュリティ性の高い携帯可能電子装置、端末装置、認証システム、及び認証方法を提供することができる。

【００５２】

なお、この発明は、上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具現化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。更に、異なる実施形態に亘る構成要素を適宜組み合わせてもよい。

【００５３】

本実施形態では携帯可能電子装置はＩＣカードとして説明した。しかし、携帯可能電子装置はこれに限らず、例えば、ＩＣタグ、パスポート、クレジットカード、キャッシュカード、ＩＤカード、及び携帯電話など、外部機器との通信手段とＩＣとを備えるものであれば、本発明は適用され得る。

【図面の簡単な説明】

【００５４】

【図１】本実施形態に関わるＩＣカードと端末装置の構成例を示すブロック図。

【図２】図１に示すＩＣカードの内部の構成例を示すブロック図。

【図３】図１に示すＩＣカードに記憶されている暗号鍵の一例を示す説明図。

【図４】図１に示す端末装置に記憶されている暗号鍵の一例を示す説明図。

【図５】図１に示すＩＣカードと端末装置における処理を説明するためのシーケンス。

【図６】図１に示すＩＣカードと端末装置との間で通信されるデータの例を示す説明図。

【図７】図１に示すＩＣカードと端末装置との間で通信されるデータの他の例を示す説明図。

【図８】図１に示すＩＣカードと端末装置との間で通信されるデータのさらに他の例を示す説明図。

【図９】図１に示すＩＣカードに記憶されている暗号鍵の他の例を示す説明図。

【図１０】図１に示す端末装置に記憶されている暗号鍵の他の例を示す説明図。

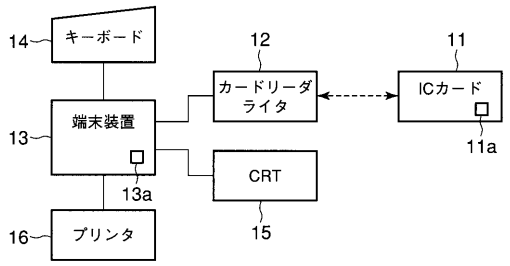
【符号の説明】

【００５５】

１１…ＩＣカード、１１ａ…暗号鍵記憶部、１２…カードリーダライタ、１３…端末装置、１３ａ…暗号鍵記憶部、１０１…制御素子、１０２…不揮発性メモリ、１０３…揮発性メモリ、１０４…プログラムメモリ、１０７…通信インターフェース、１１１…本体、１１２…モジュール、１１３…ＩＣチップ。

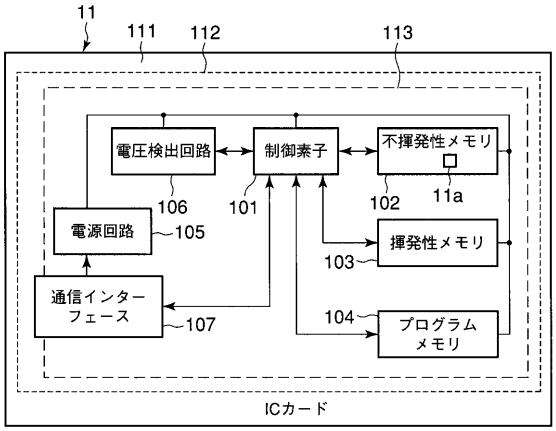
【図１】

図１



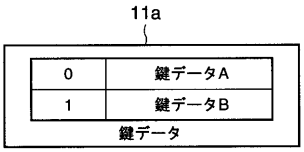
【図２】

図２



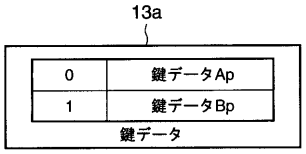
【図３】

図３



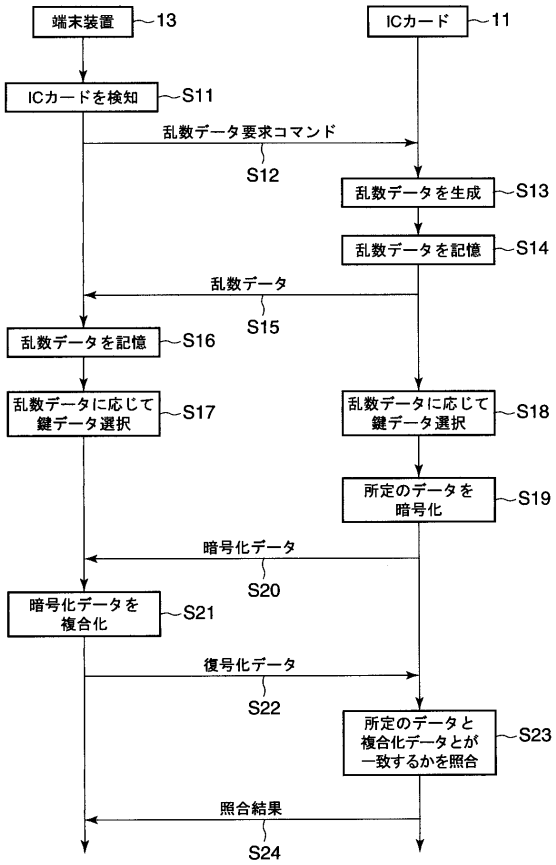
【図４】

図４



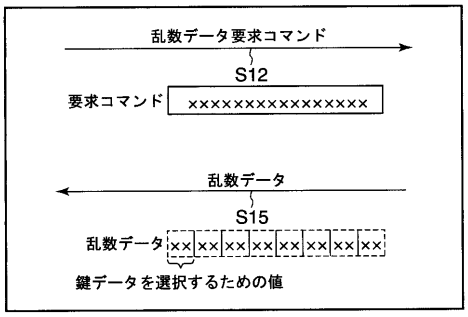
【図５】

図５



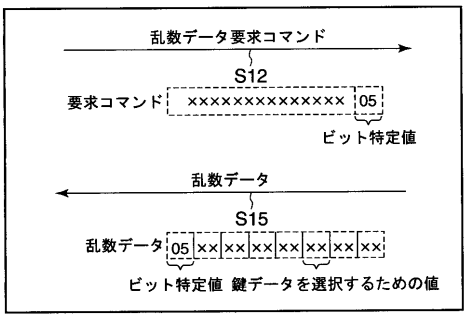
【図６】

図６



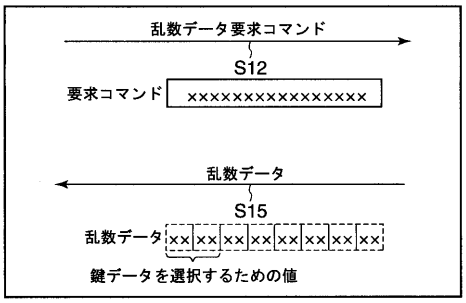
【図７】

図７



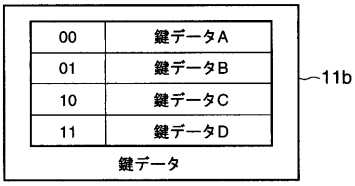
【図８】

図 8



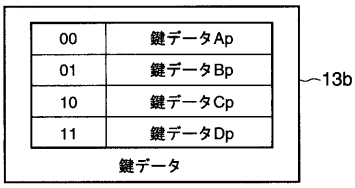
【図９】

図 9



【図１０】

図 10



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 小松 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) 5B035 AA13 BB09 CA11 CA38
5B058 CA27 KA33 KA35
5J104 AA07 GA05 KA02 KA04 KA06 NA02 NA35 NA37 NA38