(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4814599号
(P4814599)
(45)発行日　平成23年11月16日(2011.11.16)　(24)登録日　平成23年9月2日(2011.9.2)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675A

請求項の数 6　(全 19 頁)

(21)出願番号	特願2005-276336 (P2005-276336)
(22)出願日	平成17年9月22日 (2005.9.22)
(65)公開番号	特開2006-180460 (P2006-180460A)
(43)公開日	平成18年7月6日 (2006.7.6)
審査請求日	平成20年9月10日 (2008.9.10)
(31)優先権主張番号	特願2004-342945 (P2004-342945)
(32)優先日	平成16年11月26日 (2004.11.26)
(33)優先権主張国	日本国 (JP)
(31)優先権主張番号	特願2004-342946 (P2004-342946)
(32)優先日	平成16年11月26日 (2004.11.26)
(33)優先権主張国	日本国 (JP)

(73)特許権者　310021766
株式会社ソニー・コンピュータエンタテインメント
東京都港区港南１丁目７番１号
(74)代理人　110000154
特許業務法人はるか国際特許事務所
(72)発明者　佐々木　大
東京都港区南青山二丁目６番２１号　株式会社ソニー・コンピュータエンタテインメント内
(72)発明者　盛合　志帆
東京都港区南青山二丁目６番２１号　株式会社ソニー・コンピュータエンタテインメント内

最終頁に続く

(54)【発明の名称】認証装置及び認証対象装置、及び認証方法

(57)【特許請求の範囲】
【請求項１】
バッテリと、当該バッテリを認証する認証装置とを含む認証システムであって、
前記認証装置は、
前記バッテリに接続されるバッテリ接続部と、
外部電源に接続されたときに、当該外部電源からの電源供給を受け入れる受入部と、を具備し、
前記バッテリ接続部に接続されたバッテリを認証する認証処理を、繰返し期間の間、繰返して行い、前記受入部に対して外部電源から電源が供給されているか否かにより、認証処理の繰り返し期間を異ならせる認証装置であることを特徴とする認証システム。
【請求項２】
バッテリに接続するバッテリ接続部と、
外部電源に接続されたときに、当該外部電源からの電源供給を受け入れる受入部と、を具備し、
前記バッテリ接続部に接続されたバッテリを認証する認証処理を、繰返し期間の間、繰返して行う認証装置であって、
前記受入部に対して外部電源から電源が供給されているか否かにより、認証処理の繰り返し期間を異ならせることを特徴とする認証装置。
【請求項３】
請求項２に記載の認証装置であって、

前記受入部が、外部電源からの電源供給を受け入れているか否かにより、繰返し間隔及び繰返し回数を異ならせることを特徴とする認証装置。
【請求項４】
請求項３に記載の認証装置であって、
前記認証処理によるバッテリの認証に、前記繰返し回数だけ失敗した場合に、認証装置の電源をオフとする失敗処理を実行することを特徴とする認証装置。
【請求項５】
請求項２又は３に記載の認証装置であって、
前記認証処理によるバッテリの認証に失敗した場合に、認証装置の電源をオフとする失敗処理を実行することを特徴とする認証装置。
【請求項６】
バッテリに接続するバッテリ接続部と、
外部電源に接続されたときに、当該外部電源からの電源供給を受け入れる受入部と、を具備する認証装置に、前記バッテリ接続部に接続されたバッテリが正規品であるか否かの認証処理を、繰返し期間の間、繰返して行わせる制御方法であって、前記受入部が、外部電源からの電源供給を受け入れているか否かにより、認証処理の繰り返し期間を異ならせることを特徴とする認証装置の制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、バッテリに接続され、当該バッテリを認証する認証装置及び、他の装置に接続され、当該他の装置との間での認証を行う認証装置に関する。
【背景技術】
【０００２】
近年、様々な家電製品が高機能化しており、家電製品の本体に、周辺機器を接続して機能を拡張できるようになっているものも増えている。こうした製品においては、利用者が誤って他社製品を接続してしまうなどのトラブルを避けるため、周辺機器が正規品（純正品）であるか否かを判断したい場合があると考えられる。
【０００３】
そこで一般に、コンピュータシステムにおいて用いられている認証処理を、家電製品の本体と周辺機器との間で行い、正規品であるか否かの確認に応用することも考えられる。例えば、一般的なチャレンジ－レスポンス型の認証の例が、特許文献１に開示されている。
【０００４】
さらに近年、バッテリについても、純正外品（正規品以外）を提供するメーカーが現れており、その電気的定格の相違から、電源供給が不安定であるなどの問題が生じるケースが増えている。このため、バッテリについても正規品であるか否かを認証する必要性が高まっている。この目的のため、例えば特許文献２に開示されているバッテリの認証方法を採用することも考えられる。
【特許文献１】特開平１１－１６３８５３号公報
【特許文献２】特表２０００－５１７４８７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、家電製品は、情報機器とは異なり、動作中に大きな電気的ノイズを発生させるものなども存在する。そこで認証処理の確実性を増大させるため、認証を繰返し行うなどの方法が考えられる。
【０００６】
ところが、認証処理を繰返し行うこととすると、周辺機器と本体との間で授受するデータ量が大きくなって、通信負荷が増大する。家電製品などでは、家電製品そのものの機能

に係る処理を優先的に実行させる必要があるので、周辺機器との間で、当該家電製品の機能に直接関係しない通信の負荷を増大させることは、望ましくない。

【０００７】

本発明は上記実情に鑑みて為されたもので、認証のために授受するデータ量を低減させ、通信負荷を低減できる認証装置を提供することを、その目的の一つとする。

【０００８】

また、バッテリについても、上記従来のバッテリの認証方法では、バッテリが充電されていない状態など、バッテリ特有の問題に配慮していない。

【０００９】

本発明のまた別の目的の一つは上記実情に鑑みて為されたもので、バッテリに特有の問題に配慮した認証装置を提供することである。

【課題を解決するための手段】

【００１０】

上記従来例の問題点を解決するための本発明は、バッテリと、当該バッテリを認証する認証装置とを含む認証システムであって、前記認証装置は、前記バッテリに接続されるバッテリ接続部と、外部電源に接続されたときに、当該外部電源からの電源供給を受け入れる受入部と、を具備し、前記バッテリ接続部に接続されたバッテリを認証する認証処理を行い、前記受入部に対して外部電源から電源が供給されているか否かにより、認証処理の内容を異ならせる認証装置であることを特徴としている。

【００１１】

また、上記従来例の問題点を解決するための本発明は、バッテリに接続するバッテリ接続部と、外部電源に接続されたときに、当該外部電源からの電源供給を受け入れる受入部と、を具備し、前記バッテリ接続部に接続されたバッテリを認証する認証処理を行う認証装置であって、前記受入部に対して外部電源から電源が供給されているか否かにより、認証処理の内容を異ならせることを特徴としている。

【００１２】

これらにおいて、前記認証処理は、繰返し期間の間、繰返して行われ、前記受入部が、外部電源からの電源供給を受け入れているか否かにより、認証処理の繰返し期間を異ならせることとしてもよいし、また、前記認証処理は、繰返して複数回行われ、前記受入部が、外部電源からの電源供給を受け入れているか否かにより、繰返し間隔及び繰返し回数を異ならせることとしてもよい。この場合において、前記認証処理によるバッテリの認証に、前記繰返し回数だけ失敗した場合に、認証装置の電源をオフとする失敗処理を実行することとしてもよい。

【００１３】

また、前記認証処理によるバッテリの認証に失敗した場合に、認証装置の電源をオフとする失敗処理を実行することとしてもよい。

【００１４】

さらに本発明の一態様に係る制御方法は、バッテリに接続するバッテリ接続部と、外部電源に接続されたときに、当該外部電源からの電源供給を受け入れる受入部と、を具備する認証装置に、前記バッテリ接続部に接続されたバッテリが正規品であるか否かの認証処理を行わせる制御方法であって、前記受入部が、外部電源からの電源供給を受け入れているか否かにより、認証処理の内容を異ならせることを特徴としている。

【００１５】

上記従来例の問題点を解決するための本発明は、互いに共通の暗号鍵を保持する、認証要求側装置と認証対象装置とを含む認証システムであって、前記認証要求側装置が、コード関係情報を生成して前記認証対象装置に対して送信するとともに、当該コード関係情報に基づいてチャレンジコードを取得し、当該チャレンジコードを、前記暗号鍵で暗号化した比較用暗号化情報を生成し、前記認証対象装置が、当該コード関係情報を受け入れ、当該受け入れたコード関係情報に基づいて、チャレンジコードを取得し、当該取得したチャレンジコードを、前記暗号鍵で暗号化して、暗号化情報を生成し、当該生成した暗号化情

報に関係する暗号関係情報を、前記認証要求側装置に送信し、前記認証要求側装置が、当該暗号関係情報と、前記生成した比較用暗号化情報に関係する比較用暗号関係情報と、を比較することにより前記認証対象装置の認証処理を実行し、前記コード関係情報が前記チャレンジコードの一部であり、及び／又は、前記暗号関係情報が前記暗号化情報の一部であることを特徴としている。

【００１６】

また、本発明の一態様は、認証要求側装置に接続され、当該認証要求装置からの認証要求に応答して認証に係る情報を送信する認証対象装置であって、前記認証要求側装置からコード関係情報を受け入れる手段と、前記受け入れたコード関係情報に基づいて、チャレンジコードを取得するコード取得手段と、前記チャレンジコードを暗号化して、暗号化情報を生成する手段と、前記生成した暗号化情報に関係する暗号関係情報を、前記認証要求側装置に送信する手段と、を含み、前記コード関係情報が前記チャレンジコードの一部であり、及び／又は、前記暗号関係情報が前記暗号化情報の一部であることを特徴としている。

【００１７】

ここで前記コード関係情報は前記チャレンジコードの一部であり、前記コード取得手段は、認証要求側装置が保持しているものと共通の共通部分情報と、前記コード関係情報とを接合することにより、チャレンジコードを生成して取得することとしてもよい。

【００１８】

また、認証要求側装置を認証するために、第２のコード関係情報を生成して、前記認証要求装置に対して送信する手段と、第２のチャレンジコードを暗号化した暗号化情報の一部を、前記認証要求側装置から取得する手段と、前記第２のコード関係情報に基づいて、第２のチャレンジコードを取得する手段と、前記生成した第２のチャレンジコードを暗号化して、比較用暗号化情報を生成する手段と、前記比較用暗号化情報のうち、前記取得した暗号化情報の一部に対応する部分を比較用部分情報として抽出し、当該比較用部分情報と、前記取得した暗号化情報の一部とを比較する手段と、を含み、前記比較の結果、前記比較用部分情報と、前記取得した暗号化情報の一部とが、相異なる場合に、前記比較用部分情報に対して所定の第１の論理演算を行った結果に対応する値を送信し、前記比較用部分情報と、前記取得した暗号化情報の一部とが、一致する場合に、前記比較用部分情報に対して所定の第２の論理演算を行った結果に対応する値を送信することとしてもよい。

【００１９】

また、本発明の別の態様は、認証要求側装置に接続された装置における認証方法であって、前記認証要求側装置からコード関係情報を受け入れる工程と、前記受け入れたコード関係情報に基づいて、チャレンジコードを取得する工程と、前記チャレンジコードを暗号化して、暗号化情報を生成する工程と、前記生成した暗号化情報に関係する暗号関係情報を、前記認証要求側装置に送信する工程と、を含み、前記コード関係情報が前記チャレンジコードの一部であり、及び／又は、前記暗号関係情報が前記暗号化情報の一部であることを特徴としている。

【００２０】

さらに、上記従来例の問題点を解決するための本発明は、認証要求側装置であって、バッテリに接続するバッテリ接続部と、外部電源に接続されたときに、当該外部電源からの電源供給を受け入れる受入部と、を具備し、前記バッテリ接続部に接続されたバッテリを認証する認証処理を行う認証要求側装置であって、コード関係情報を生成して前記バッテリに対して送信するとともに、当該コード関係情報に基づいてチャレンジコードを取得し、当該チャレンジコードを、前記暗号鍵で暗号化した比較用暗号化情報を生成し、前記送信したコード関係情報に基づいて取得されるチャレンジコードを、前記バッテリ側にて前記暗号鍵で暗号化した暗号化情報を取得して、当該バッテリから取得した暗号関係情報と、前記生成した比較用暗号化情報に関係する比較用暗号関係情報と、を比較することにより前記バッテリの認証処理を実行し、前記コード関係情報が前記チャレンジコードの一部であり、及び／又は、前記暗号関係情報が前記暗号化情報の一部であることを特徴として

いる。

【００２１】

ここで前記受入部に対して外部電源から電源が供給されているか否かにより、認証処理の内容を異ならせてもよい。また、前記認証処理は、繰返し期間の間、繰返して行われ、前記受入部が、外部電源からの電源供給を受け入れているか否かにより、認証処理の繰返し期間を異ならせてもよい。

【００２２】

さらに前記認証処理は、繰返して複数回行われ、前記受入部が、外部電源からの電源供給を受け入れているか否かにより、繰返し間隔及び繰返し回数を異ならせてもよい。この場合、前記認証処理によるバッテリの認証に、前記繰返し回数だけ失敗した場合に、バッテリの電源をオフとする失敗処理を実行してもよい。

【００２３】

また、前記認証処理によるバッテリの認証に失敗した場合に、バッテリの電源をオフとする失敗処理を実行することとしてもよい。

【発明を実施するための最良の形態】

【００２４】

本発明の第１の実施の形態について図面を参照しながら説明する。本発明の第１の実施の形態に係る認証装置は、例えば家庭用ゲーム機であり、ＣＰＵ等の制御部１１と、記憶部１２と、操作部１３と、表示制御部１４と、通信部１５と、光ディスクドライブ１６と、電源制御部１７とを含んで構成され、バッテリ３に接続されている。

【００２５】

制御部１１は、記憶部１２に格納されているプログラムに従って動作する。この制御部１１は、ゲームに関係する処理を実行する。また本実施の形態では、この制御部１１が、認証装置としての処理を行う。制御部１１の認証装置としての具体的な処理の内容は後述する。

【００２６】

記憶部１２は、例えばＲＡＭなどであり、光ディスクドライブ１６から読み出されたゲームプログラムを保持する。また、この記憶部１２は、不揮発性の記憶素子を備え、認証要求側装置としてのプログラムを格納している。さらに記憶部１２は、制御部１１のワークメモリとしても動作する。

【００２７】

操作部１３は、ゲームコントローラであり、プレイヤの指示操作内容を制御部１１に出力する。表示制御部１４は、グラフィックボードであり、制御部１１から入力される指示に従って、液晶ディスプレイなどの表示装置に対してゲーム画面を表示出力する。通信部１５は、例えばシリアル通信ポート等であり、バッテリ３に接続され、情報の授受を行う。具体的にこの通信部１５は、制御部１１から入力される指示に従って、バッテリ３に対して情報を送信する。また、この通信部１５は、バッテリ３側から受信される情報を制御部１１に出力する。

【００２８】

光ディスクドライブ１６は、例えばＤＶＤ－ＲＯＭドライブやＢｌｕ－ｒａｙディスクドライブであり、ＤＶＤや、Ｂｌｕ－ｒａｙディスク等の記憶媒体から、プログラムなどの情報を読み取って制御部１１に出力する。

【００２９】

電源制御部１７は、バッテリ３に接続されており、図２に示すように、電源制御回路２１と、充電回路２２と、電源供給回路２３とを含んで構成される。電源制御回路２１は、バッテリ３や、電源供給回路２３から供給される電源の、制御部１１等の各部への供給を制御している。例えばこの電源制御回路２１は、プレイヤが電源を投入する操作を行うと、各部への電源供給を開始し、電源を切る操作が行われた場合、又は制御部１１から電源をオフとするべき旨の指示（電源断指示）があった場合に、各部への電源供給を停止する。

【００３０】
充電回路２２は、電源供給回路２３から電源供給がある場合に、バッテリ３が接続されていれば、バッテリ３を充電する動作を行う。電源供給回路２３は、例えばレギュレータ等であり、外部電源として例えば家庭用コンセントからの電力に基づいて生成される、直流電源電圧の供給を受けて、電源制御回路２１や充電回路２２に出力する動作を行っている。この電源供給回路２３は本発明の受入部に相当する。
【００３１】
この電源制御部１７は、バッテリ３が接続され、電源供給回路２３が外部電源の供給を受けていないときには、バッテリ３から供給される電力を各部へ供給する。また、電源供給回路２３が外部電源の供給を受けていれば、当該外部電源により供給される電力を各部へ供給する。さらに、電源供給回路２３が外部電源の供給を受けているとき、バッテリ３が接続されていれば、当該バッテリ３を充電する。
【００３２】
バッテリ３は、図３に示すように、制御部３１と、記憶部３２と、通信部３３とを含んで構成されている。制御部３１は、ＣＰＵ等であり、記憶部３２に格納されているプログラムに従って動作する。この制御部３１は、電池に関する情報（電池残量や温度等）を提供するための処理を行う。また、この制御部３１は、認証の機能を実現する処理を行う。この制御部３１の認証機能を実現するための処理については、後に述べる。
【００３３】
記憶部３２は、フラッシュＲＯＭ（Read Only Memory）や、ＲＡＭ（Random Access Memory）などの記憶素子を含んで構成される。この記憶部３２は、制御部３１によって実行されるプログラムが格納されている。また、この記憶部３２は、制御部３１の処理の過程で必要となる種々のデータを格納するワークメモリとしても動作する。
【００３４】
通信部３３は、認証装置１側に接続される。この通信部３３は、例えばシリアル通信ポートである。通信部３３は、制御部３１から入力される指示に従って認証装置１に情報を送信する。また、この通信部３３は、認証装置１から受信される情報を制御部３１に出力する。
【００３５】
本実施の形態の認証装置１は、機能的には、図４に示すように、バッテリ認証部６１と、失敗カウンタ６２と、間隔値バッファ６３と、外部電源供給判断部６４とを含んで構成される。
【００３６】
バッテリ認証部６１は、間隔値バッファ６３に記憶されている時間間隔だけ待機して、バッテリを認証する処理を実行する。ここで認証は、例えば特許文献１に開示されているようなチャレンジ－レスポンス法のほか、パスワードを用いる方法など様々なものがあり、どれでも構わない。また、このバッテリ認証部６１は、認証に失敗したときには、失敗カウンタ６２をインクリメントし、外部電源供給判断部６４に認証に失敗したことを表す信号を出力する。また、バッテリ認証部６１は、認証に成功すると、失敗カウンタ６２を「０」にリセットし、間隔値バッファ６３に予め成功時に設定するべき値として定められている間隔値を記憶させる。
【００３７】
さらに、このバッテリ認証部６１は、失敗カウンタ６２の値が予め定めた回数閾値を超える場合に、失敗時処理を実行する。この処理については後に述べる。
【００３８】
失敗カウンタ６２は、当初は「０」にリセットされている。この失敗カウンタ６２は、バッテリ認証部６１の指示により値をインクリメントし、また、「０」にリセットする。間隔値バッファ６３は、間隔値を保持する。
【００３９】
外部電源供給判断部６４は、バッテリ認証部６１から認証に失敗したことを表す信号の

入力を受けて、電源制御部１７が外部電源の供給を受けているか否かを判断する。そして、外部電源の供給を受けていれば、外部電源が供給されているときの間隔値として予め定められている間隔値を、間隔値バッファ６３に格納する。また、外部電源の供給を受けていなければ、外部電源が供給されていないときの間隔値として予め定められている間隔値を、間隔値バッファ６３に格納する。

【００４０】

本実施の形態では、ソフトウエア的に上記機能が実現される。すなわち制御部１１の認証装置としての処理、並びにバッテリ３の制御部３１の認証機能を実現する処理の例について次に説明する。この認証の処理は、既に述べたように、例えば特許文献１に開示されているようなチャレンジ－レスポンス法のほか、パスワードを用いる方法など様々なものがあり、どれを用いてもよい。制御部１１は、認証の結果を表すフラグを記憶部１２に格納する。例えばこのフラグは、認証が成功した場合に「０」、認証に失敗した場合に「１」となるものとしておく。

【００４１】

本実施の形態の認証装置の制御部１１と、バッテリ３の制御部３１とは、認証が失敗した場合、上記認証の処理を再度実行する。また、認証が成功した場合にも、一定の時間をおいて上記認証の処理を再度行うこととしてもよい。

【００４２】

本実施の形態において特徴的なことの一つは、電源制御部１７が外部電源の供給を受けているか否かによって、制御部１１が、その認証処理の内容を異ならせていることである。具体的に制御部１１は、電源が投入されると、バッテリ３が接続されているか否かを調べ、バッテリ３が接続されていれば、図５に示す処理を開始する。なおここでは、記憶部１２に予め認証の連続失敗回数を保持する失敗カウンタを記憶する記憶領域が確保されているものとして説明するが、制御部１１として動作するＣＰＵのレジスタに失敗カウンタを記憶しておいてもよい。

【００４３】

そしてバッテリ３の認証の処理を行い（Ｓ１）、バッテリ３の認証に成功したか（バッテリ３は正規品であると判断されたか）否かを調べる（Ｓ２）。つまり認証に関するフラグが「１」（前回の認証失敗を表す値）となっているか否かを調べる。ここで認証が失敗したと判断された場合は、失敗カウンタを１つインクリメントする（Ｓ３）。そして電源制御部１７が外部電源の供給を受けているか否かを判断する（Ｓ４）。

【００４４】

ここで、電源制御部１７が外部電源の供給を受けていなければ、認証処理の繰返し間隔を第１の所定間隔値（例えば１００ミリ秒）に設定するとともに、認証失敗回数の回数閾値を第１閾値「３０回」に設定する（Ｓ５）。そして制御部１１は、失敗カウンタの値が、上記設定した回数閾値を超えたか否かを調べ（Ｓ６）、超えている場合は、失敗時処理を実行して（Ｓ７）、処理を終了する。つまり、設定された回数閾値（繰返し回数）だけ、連続的に失敗したときに失敗時処理を実行し、例えば装置の電源をオフとする。

【００４５】

一方、処理Ｓ６において、設定した回数閾値を超えていない場合は、認証処理の繰返し間隔に設定された時間だけ処理を中断し（Ｓ８）、認証処理の繰返し間隔に設定された時間が経過してから、処理Ｓ１に戻って処理を続ける。

【００４６】

また、処理Ｓ４において、電源制御部１７が外部電源の供給を受けている場合は、認証処理の繰返し間隔を第２の所定間隔値（例えば５００ミリ秒）に設定するとともに、認証失敗回数の回数閾値を第２閾値「６００回」に設定し（Ｓ９）、処理Ｓ６に移行して処理を続ける。

【００４７】

すなわち外部電源の供給を受けているか否かによって、所定間隔値（繰返し間隔）と、回数閾値（繰返し回数）とを異ならせ、認証処理の繰返し期間を異ならせているのである

。これは例えばバッテリ３が正規品であっても、残量がほとんどなく、制御部３１を稼働させることができない場合に配慮したものである。すなわち、制御部３１が稼働していなければ、認証装置１からバッテリ３へ乱数値を送信しても、バッテリ３から暗号化情報を送信することができず、認証装置１はバッテリ３の認証が失敗したものと判断してしまう。そこで、ここでは外部電源が供給され、バッテリ３が充電されている間は、認証の間隔を長めに設定するとともに、認証の繰返し回数を多めにして、当初バッテリ３が空であっても、制御部３１を稼働させることができる程度に充電がされるまで、認証処理の繰返し期間を延長させているのである。

【００４８】

さらに、制御部１１は、処理Ｓ２においてバッテリ３の認証に成功したと判断された場合、失敗カウンタを「０」にリセットする（Ｓ１０）。そして認証処理の繰返し間隔を第３の所定間隔値（例えば３０秒）に設定し（Ｓ１１）、成功時処理を実行して（Ｓ１２）、処理Ｓ８に移行して処理を続ける。

【００４９】

なお、処理Ｓ７における失敗時処理は、例えば電源制御部１７に対して電源断を指示し、認証装置の電源をオフとする処理としてもよいし、表示制御部１４に対して「使用できません」のような表示をさせ、ゲームに係る処理を中止する処理としてもよい。

【００５０】

また処理Ｓ１２における成功時処理は、例えばゲーム処理の開始であってもよい。また、既にゲームの処理が開始されている場合は、この成功時処理において、何らかの処理を行う必要は必ずしもない。

【００５１】

さらにこの失敗カウンタの記憶領域は、記憶部１２の不揮発性メモリ上に確保することとして、電源が切られた場合もその内容が保持されるようにしてもよい。このようにすると、例えば外部電源を接続したり切離したりという操作や、ゲームを定期的に中断して電源を入れ直すといった操作を行うことで、失敗カウンタを途中でリセットさせ、ゲームを断続的にプレイし続けることをも防止できる。

【００５２】

本実施の形態によれば、電源を供給する主体としてのバッテリを認証するにあたり、バッテリが充電されていない状態で、バッテリの認証ができなくなることなど、バッテリの認証に特有の問題に配慮した処理とすることができる。

【００５３】

また、本発明の第２の実施の形態について図面を参照しながら説明する。本実施の形態に係る認証対象装置は、周辺機器４を用いて実現される。ここで周辺機器４は、図６に示すように、制御部４１と、記憶部４２と、通信部４３とを含んで構成され、本体５に接続される。なお、周辺機器４は、この他にも周辺機器としての機能を提供するための図示しない構成を有してもよい。

【００５４】

制御部４１は、ＣＰＵ等であり、記憶部４２に格納されているプログラムに従って動作する。この制御部４１は、周辺機器としての機能を実現する処理を実行する。例えば、周辺機器４がコントローラ等の操作装置であれば、この制御部４１は、利用者の指示操作に係る情報を本体５側に送信する処理を行う。また、メモリカード等の記憶装置であれば本体５側から受信される情報を保持する処理や、本体５側からの要求に応答して保持している情報を提供する処理などを行う。このほか、周辺機器４としては、通信装置、撮像装置、電力供給装置、音響装置その他、様々なものが相当する。

【００５５】

また、この制御部４１は、認証対象装置としての機能を実現する処理を行う。具体的に制御部４１は、認証対象装置としての機能を実現するため、チャレンジコードのもととなるコード関係情報の入力を受け入れて、チャレンジコードを取得し、このチャレンジコードを暗号化した暗号化情報を生成する処理を実行している。これら制御部４１の認証対象

装置の機能を実現するための処理については、後に詳しく述べる。

【００５６】

記憶部４２は、フラッシュＲＯＭ（Read Only Memory）や、ＲＡＭ（Random Access Memory）などの記憶素子を含んで構成される。この記憶部４２は、制御部４１によって実行されるプログラムが格納されている。また、この記憶部４２は、制御部４１の処理の過程で必要となる種々のデータを格納するワークメモリとしても動作する。

【００５７】

通信部４３は、本体５側に接続される。この通信部４３は、例えばシリアル通信ポートである。通信部４３は、制御部４１から入力される指示に従って本体５側に情報を送信する。また、この通信部４３は、本体５側から受信される情報を制御部４１に出力する。

【００５８】

本体５は、例えば家庭用ゲーム機であり、図７に示すように、ＣＰＵ等の制御部５１と、記憶部５２と、操作部５３と、表示制御部５４と、通信部５５と、光ディスクドライブ５６とを含んで構成されている。

【００５９】

制御部５１は、記憶部５２に格納されているプログラムに従って動作する。具体的にこの制御部５１は、ゲームに関係する処理を実行する。また本実施の形態では、この制御部５１が、認証要求側装置としての動作を行う。制御部５１の認証要求側装置としての具体的な処理の内容は後述する。

【００６０】

記憶部５２は、例えばＲＡＭなどであり、光ディスクドライブ５６から読み出されたゲームプログラムを保持する。また、この記憶部５２は、不揮発性の記憶素子を備え、認証要求側装置としてのプログラムを格納している。さらに記憶部５２は、制御部５１のワークメモリとしても動作する。

【００６１】

操作部５３は、ゲームコントローラであり、プレイヤの指示操作内容を制御部５１に出力する。表示制御部５４は、グラフィックボードであり、制御部５１から入力される指示に従って、家庭用テレビなどの表示装置に対してゲーム画面を表示出力する。通信部５５は、例えばシリアル通信ポート等であり、周辺機器４の通信部４３に接続され、情報の授受を行う。具体的にこの通信部５５は、制御部５１から入力される指示に従って、情報を周辺機器４へと送信する。また、この通信部５５は、周辺機器４側から受信される情報を制御部５１に出力する。

【００６２】

光ディスクドライブ５６は、例えばＤＶＤ－ＲＯＭドライブやＢｌｕ－ｒａｙディスクドライブであり、ＤＶＤや、Ｂｌｕ－ｒａｙディスク等の記憶媒体から、プログラムなどの情報を読み取って制御部５１に出力する。

【００６３】

ここで周辺機器４の制御部４１における認証対象装置の機能を実現するための処理について説明する。本実施の形態では、周辺機器４の記憶部４２に、予め複数の暗号化鍵候補k0，k1，…を格納している。

【００６４】

この制御部４１は、機能的には図８に例示するように、認証要求処理部７１と、本体側認証部７２とを含んで構成される。

【００６５】

ここで認証要求処理部７１は、認証要求側装置としての本体５側から、通信部４３を介してチャレンジコードの元となるコード関係情報の入力を受け入れる。またこの認証要求処理部７１は、暗号化鍵の一つを特定する暗号化鍵特定情報の入力を本体５側から受け入れて、当該暗号化鍵特定情報（例えば鍵番号N）によって特定される暗号化鍵kNを記憶部４２から読み出す。

【００６６】

なお、ここでコード関係情報は、チャレンジコードの一部であるとする。具体的にチャレンジコードとして１２８ビット長のチャレンジコードを用いる場合、本体５側は、コード関係情報として、１２８ビット長の前半（上位）に相当する６４ビットを送出する。認証要求処理部７１は、このコード関係情報に基づいてチャレンジコードを生成して取得する。

【００６７】

すなわち、本実施の形態では、複数の第１定数値群C10，C11，…を記憶部４２に格納しておき、暗号化鍵特定情報として受信される鍵番号Ｎに対応する第１定数値C1Nを記憶部４２から読み出し、受信したコード関係情報に当該読み出した第１定数値C1Nを連接して、チャレンジコードを生成する。上述のように１２８ビット長のチャレンジコードに対してコード関係情報が６４ビットである場合は、この第１定数値C10，C11，…は、いずれも６４ビット長の定数となる。この第１定数値が本発明における共通部分情報となる。

【００６８】

そして認証要求処理部７１は、記憶部４２から読み出した暗号化鍵kNを用いて、上記生成したチャレンジコードを暗号化した暗号化情報を生成する。

【００６９】

さらに認証要求処理部７１は、暗号化情報の予め定めた一部（例えば後半（下位）部分）を暗号関係情報として取り出す。そして、取り出した暗号関係情報を、本体５に対して送信する。具体的にチャレンジコードが１２８ビット長であるとし、また上記暗号化のアルゴリズムが、暗号化の対象となる情報の符号長を変えない暗号化方式に係るものであるとすると、暗号化情報もまた１２８ビット長となる。認証要求処理部７１は、この１２８ビット長の暗号化情報のうち、予め定めた一部、例えば後半６４ビット分を本体５側に送信することになる。

【００７０】

本体側認証部７２は、認証要求側装置としての本体５を認証するため、本体５を認証するためのチャレンジコード（第２のチャレンジコード）に係る第２のコード関係情報を生成する。具体的には乱数ルーチンによって所定ビット長の数値を発生させ、当該乱数値を第２のコード関係情報として、通信部４３を介して本体５側に送信する。

【００７１】

本体側認証部７２はさらに、発生させたコード関係情報に基づいて第２のチャレンジコードを生成する。本実施の形態では、複数の第２定数値群C20，C21，…を記憶部４２に格納しておき、先に暗号化鍵特定情報として受信した鍵番号Ｎに対応する第２定数値C2Nを記憶部４２から読み出す。そして、この第２定数値C2Nを、発生させたコード関係情報に連接して、第２のチャレンジコードを生成する。このように第２のチャレンジコードの一部をランダムに決定し、残りの部分を定数値としておくことで、第２のチャレンジコードの送受信に係る通信量を低減できる。

【００７２】

本体側認証部７２は、認証装置としての処理を行う際に受信した、暗号鍵特定情報によって特定される暗号化鍵kNを用いて、記憶部４２に格納した第２のチャレンジコードを暗号化して、比較用暗号化情報を生成しておく。

【００７３】

さらに本体側認証部７２は、本体５側で第２チャレンジコードを暗号化した情報の一部と、そして比較用暗号化情報の予め定められた一部とを比較する。上に述べた例のように、予め定められた一部として、後半６４ビット分を抽出することとしている場合、本体側認証部７２は、比較用暗号化情報の後半部分６４ビットを抽出し、当該抽出した６４ビット長の情報と、本体５側から受信した暗号関係情報（６４ビット長）とを比較する。

【００７４】

そしてこれらが一致していれば、本体側認証部７２は、本体５が承認された本体、例えば純正の本体であると判断し、その旨を本体５側に報知する。また、本体側認証部７２が、比較用暗号化情報の予め定められた一部と、本体５側から受信した暗号関係情報とが一

致していないと判断した場合、つまり本体５が承認されていない機器であると判断される場合にも、その旨を本体５側に報知する。

【００７５】

次に、認証要求側装置として動作する、本体５の制御部５１の動作について説明する。なお、本体５の記憶部５２には、暗号化鍵kNを格納しておく。この暗号化鍵は、認証装置としての周辺機器４側の記憶部４２に格納されている複数の暗号化鍵のうちの一つと同一のものとしておく。また、周辺機器４側において当該暗号化鍵を特定するために必要な情報である、暗号鍵特定情報（例えば鍵番号Ｎ）を、記憶部５２に保持しておく。

【００７６】

本体５の制御部５１によって実行される処理は、機能的には図９に示すように、周辺機器認証部７５と、認証要求処理部７６とを含んで構成される。

【００７７】

周辺機器認証部７５は、チャレンジコードの元となるコード関係情報を生成する。具体的には乱数ルーチンによって所定ビット長の乱数値を発生させ、当該乱数値をコード関係情報として、通信部５５を介して周辺機器４側に送信する。また周辺機器認証部７５は、暗号化鍵kNを特定する暗号化鍵特定情報（例えば鍵番号Ｎ）を、周辺機器４側に送信する。

【００７８】

周辺機器認証部７５はさらに、発生させたコード関係情報に基づいてチャレンジコードを生成する。本実施の形態では、周辺機器４側で利用する第１定数値C1iを記憶部５２に格納しておく。ここでの例では、周辺機器４では、暗号鍵特定情報（鍵番号Ｎ）によって特定される第１定数値C1Nを用いるので、記憶部５２に第１定数値C1Nを保持させておく。

【００７９】

周辺機器認証部７５は、発生させたコード関係情報に、記憶部５２に格納されている第１定数値C1Nを連接して、チャレンジコードを生成する。このようにチャレンジコードの一部をランダムに決定し、残りの部分を定数値としておくことで、チャレンジコードの送受信に係る通信量を低減できる。

【００８０】

周辺機器認証部７５は、生成したチャレンジコードを、記憶部５２に格納されている暗号化鍵kNで暗号化して、比較用暗号化情報を生成しておく。

【００８１】

また周辺機器認証部７５は、暗号関係情報として、周辺機器４側にて、暗号化鍵kNを用いて暗号化した結果の所定一部を、周辺機器４側から受信する。そして比較用暗号化情報の予め定められた一部と、周辺機器４側から受信した暗号関係情報とを比較する。上に述べた例のように、予め定められた一部として、後半６４ビット分を抽出することとしている場合、周辺機器認証部７５は、比較用暗号化情報の後半部分６４ビットを抽出し、当該抽出した６４ビット長の情報と、周辺機器１側から受信した暗号関係情報（６４ビット長）とを比較する。

【００８２】

そしてこれらが一致していれば、周辺機器４は承認された周辺機器、例えば純正の周辺機器であると判断する。

【００８３】

また、本体５側では、周辺機器４側で用いる第２定数値C2Nを保持しておく。そして認証要求処理部７６は、周辺機器４の本体側認証部７２から受信した第２のコード関係情報に、第２定数値C2Nを連接して第２のチャレンジコードを生成して取得する。

【００８４】

認証要求処理部７６は、記憶部５２から暗号化鍵kNを読み出し、この暗号化鍵ｋNを用いて、上記生成した第２のチャレンジコードを暗号化して、暗号化情報を生成する。さらに認証要求処理部７６は、暗号化情報の予め定めた一部（例えば後半部分）を暗号関係情報として取り出し、取り出した暗号関係情報を、周辺機器４に対して送信する。

【００８５】
なお、ここでは周辺機器４を認証する処理と周辺機器４が本体５を認証する処理との双方が行なわれる場合について説明したが、本体５が周辺機器４を認証する処理を行なうだけで十分な場合は、それでもよい。この場合、周辺機器４における本体側認証部７２や本体５における認証要求処理部７６は必ずしも必要でない。
【００８６】
すなわち、制御部４１は、認証要求側装置としての本体５側から、通信部４３を介してチャレンジコードの元となるコード関係情報の入力を受け入れる。また、制御部４１は、本体５側から暗号化鍵の一つを特定する、暗号化鍵特定情報の入力を受け入れて、当該暗号化鍵特定情報（例えば鍵番号N）によって特定される暗号化鍵kNを記憶部４２から読み出す。
【００８７】
なお、ここでコード関係情報は、チャレンジコードの一部であるとする。具体的にチャレンジコードとして１２８ビット長のチャレンジコードを用いる場合、本体５側は、コード関係情報として、１２８ビット長の前半（上位）に相当する６４ビットを送出する。制御部４１は、このコード関係情報に基づいてチャレンジコードを生成して取得する。
【００８８】
すなわち、本実施の形態では、複数の第１定数値群C10，C11，…を記憶部４２に格納しておき、暗号化鍵特定情報として受信される鍵番号Ｎに対応する第１定数値C1Nを記憶部４２から読み出し、受信したコード関係情報に当該読み出した第１定数値C1Nを連接して、チャレンジコードを生成する。上述のように１２８ビット長のチャレンジコードに対してコード関係情報が６４ビットである場合は、この第１定数値C10，C11，…は、いずれも６４ビット長の定数となる。この第１定数値が本発明における共通部分情報となる。
【００８９】
制御部４１は、記憶部４２から読み出した暗号化鍵kNを用いて、上記生成したチャレンジコードを暗号化した暗号化情報を生成する。
【００９０】
制御部４１は、暗号化情報の予め定めた一部（例えば後半（下位）部分）を暗号関係情報として取り出す。そして、取り出した暗号関係情報を、本体５に対して送信する。具体的にチャレンジコードが１２８ビット長であるとし、また上記暗号化のアルゴリズムが、暗号化の対象となる情報の符号長を変えない暗号化方式に係るものであるとすると、暗号化情報もまた１２８ビット長となる。制御部４１は、この１２８ビット長の暗号化情報のうち、予め定めた一部、例えば後半６４ビット分を本体５側に送信することになる。
【００９１】
また、本体５の制御部５１の動作は次のようになる。本体５の記憶部５２には、暗号化鍵kNを格納しておく。この暗号化鍵は、認証対象装置としての周辺機器４側の記憶部４２に格納されている複数の暗号化鍵のうちの一つと同一のものとしておく。また、周辺機器４側において当該暗号化鍵を特定するために必要な情報である、暗号鍵特定情報（例えば鍵番号Ｎ）を、記憶部５２に保持しておく。
【００９２】
制御部５１は、チャレンジコードの元となるコード関係情報を生成する。具体的には乱数ルーチンによって所定ビット長の乱数値を発生させ、当該乱数値をコード関係情報として、通信部５５を介して周辺機器４側に送信する。また制御部５１は、暗号化鍵kNを特定する暗号化鍵特定情報（例えば鍵番号Ｎ）を、周辺機器４側に送信する。
【００９３】
制御部５１はさらに、発生させたコード関係情報に基づいてチャレンジコードを生成する。本実施の形態では、周辺機器４側で利用する第１定数値C1iを記憶部５２に格納しておく。ここでの例では、周辺機器４では、暗号鍵特定情報（鍵番号Ｎ）によって特定される第１定数値C1Nを用いるので、記憶部５２に第１定数値C1Nを保持させておく。
【００９４】

制御部５１は、発生させたコード関係情報に、記憶部５２に格納されている第１定数値C1Nを連接して、チャレンジコードを生成する。このようにチャレンジコードの一部をランダムに決定し、残りの部分を定数値としておくことで、チャレンジコードの送受信に係る通信量を低減できる。

【００９５】

制御部５１は、生成したチャレンジコードを、記憶部５２に格納されている暗号化鍵kNで暗号化して、比較用暗号化情報を生成しておく。

【００９６】

また制御部５１は、暗号関係情報として、周辺機器４側にて、暗号化鍵kNを用いて暗号化した結果の所定一部を、周辺機器４側から受信する。そして比較用暗号化情報の予め定められた一部と、周辺機器４側から受信した暗号関係情報とを比較する。上に述べた例のように、予め定められた一部として、後半６４ビット分を抽出することとしている場合、制御部５１は、比較用暗号化情報の後半部分６４ビットを抽出し、当該抽出した６４ビット長の情報と、周辺機器４側から受信した暗号関係情報（６４ビット長）とを比較する。

【００９７】

そしてこれらが一致していれば、周辺機器４は承認された周辺機器、例えば純正の周辺機器であると判断する。

【００９８】

また、ここでは本体５が、周辺機器４を認証する処理例について説明したが、さらに上記処理に続けて、周辺機器４が本体５を認証する処理を行ってもよい。この場合、周辺機器４の制御部４１は、認証要求側装置としての本体５を認証するため、本体５を認証するためのチャレンジコード（第２のチャレンジコード）に係る第２のコード関係情報を生成する。具体的には乱数ルーチンによって所定ビット長の数値を発生させ、当該乱数値を第２のコード関係情報として、通信部４３を介して本体５側に送信する。

【００９９】

制御部４１はさらに、発生させたコード関係情報に基づいて第２のチャレンジコードを生成する。本実施の形態では、複数の第２定数値群C20，C21，…を記憶部４２に格納しておき、先に暗号化鍵特定情報として受信した鍵番号Ｎに対応する第２定数値C2Nを記憶部４２から読み出す。そして、この第２定数値C2Nを、発生させたコード関係情報に連接して、第２のチャレンジコードを生成する。このように第２のチャレンジコードの一部をランダムに決定し、残りの部分を定数値としておくことで、第２のチャレンジコードの送受信に係る通信量を低減できる。

【０１００】

制御部４１は、認証対象装置としての処理を行う際に受信した、暗号鍵特定情報によって特定される暗号化鍵kNを用いて、記憶部４２に格納した第２のチャレンジコードを暗号化して、比較用暗号化情報を生成しておく。

【０１０１】

本体５の制御部５１では、周辺機器４側で用いる第２定数値C2Nを保持しておく。そして受信した第２のコード関係情報に、第２定数値C2Nを連接して第２のチャレンジコードを生成して取得する。

【０１０２】

制御部５１は、記憶部５２から暗号化鍵kNを読み出し、この暗号化鍵ｋNを用いて、上記生成した第２のチャレンジコードを暗号化して、暗号化情報を生成する。さらに制御部５１は、暗号化情報の予め定めた一部（例えば後半部分）を暗号関係情報として取り出し、取り出した暗号関係情報を、周辺機器４に対して送信する。

【０１０３】

周辺機器４側の制御部４１は、当該本体５が送信した暗号関係情報を受信する。そして比較用暗号化情報の予め定められた一部と、本体５側から受信した暗号関係情報とを比較する。上に述べた例のように、予め定められた一部として、後半６４ビット分を抽出することとしている場合、制御部４１は、比較用暗号化情報の後半部分６４ビットを抽出し、

当該抽出した６４ビット長の情報と、本体５側から受信した暗号関係情報（６４ビット長）とを比較する。

【０１０４】

そしてこれらが一致していれば、周辺機器４は、本体５が承認された本体、例えば純正の本体であると判断し、その旨を本体５側に報知する。また、制御部４１が、比較用暗号化情報の予め定められた一部と、本体５側から受信した暗号関係情報とが一致していないと判断した場合、つまり本体５が承認されていない機器であると判断される場合にも、その旨を本体５側に報知する。

【０１０５】

本実施の形態において特徴的なことの一つは、認証の成立と不成立とを、比較用暗号化情報の予め定められた一部を用いたデータによって報知することである。具体的に、本体５を認証した旨の報知は、比較用暗号化情報の所定一部を認証成立データとして、そのまま本体５側に送信することによって行う。また、本体５の認証ができなかった旨の報知は、比較用暗号化情報の所定一部の各ビットを論理否定したデータを認証不成立データとし、この認証不成立データを本体５側に送出することで行う。なお、論理否定とは、「１」となっているビットを「０」とし、「０」となっているビットを「１」とする演算をいう。ここで、データの各ビットをそのままとする論理演算が、本発明の第２の論理演算に相当し、データの各ビットを論理否定する論理演算が、本発明の第１の論理演算に対応する。

【０１０６】

本体５側では、受信した認証成立データと、送信済みの暗号関係情報とを比較し、一致していれば、認証されたものと判断することになる。

【０１０７】

すなわち、認証成立データや認証不成立データとしては、全ビットを「１」としたり、「０」としたりするなど、それぞれ予め定められた定数値を用いてもよい。しかしながら、定数値を用いた場合は、不正に製造したＭＯＤチップで、例えば認証成立データの定数値を送信することで、本体側を認証したとする情報を送出することができるようになってしまう。こうしたセキュリティ上の脆弱性を防止するため、ここでは定数値に代えて、認証の処理ごとに異なる値となる情報である、比較用暗号化情報の予め定められた一部を用いて認証成立データと認証不成立データとを生成しているのである。

【０１０８】

本実施の形態によると、チャレンジコードや、当該チャレンジコードを暗号化した暗号化情報の全体を送受信せず、これらの一部を送受信することとしているので、認証のために授受するデータ量を低減でき、通信負荷の低減に資することができる。

【０１０９】

次に、本発明の認証対象装置及び認証要求側装置としての周辺機器４及び本体５の動作を、図１０を参照しながら説明する。図１０は、周辺機器４及び本体５の間の通信の流れを示す流れ図である。当初、本体５の記憶部５２には、暗号化鍵、第１定数値、第２定数値として、それぞれ、暗号化鍵特定情報Ｎ＝０に対応する暗号化鍵k0と、第１定数値C10と、第２定数値C20とが格納されている。

【０１１０】

本体５は、周辺機器４が接続されると、６４ビット長の乱数値R1を発生させ（Ｓ２１）、暗号化鍵k0を特定する暗号化鍵特定情報（ここでは鍵番号である「０」）と、コード関係情報となる当該乱数値R1とを、周辺機器４側に送信する（Ｓ２２）。

【０１１１】

本体５側では、処理Ｓ１で発生させたコード関係情報である乱数値R1に、第１定数値C10を連接して、チャレンジコードを生成する（Ｓ２３）。ここでは、連接を記号として、「||」なる記号を用いる。つまり、チャレンジコードは、「R1||C10」となる。

【０１１２】

本体５は、生成したチャレンジコード「R1||C10」を、暗号化鍵k0で暗号化して、比較

用暗号化情報を生成する（Ｓ２４）。ここで対象となるデータｄを暗号化鍵ｋで暗号化することを、ENC(k,d)と表記することとすると、比較用暗号化情報は、ENC(k0, (R1||C10))となる。

【０１１３】

周辺機器４側では、本体５側から受信したコード関係情報R1と、暗号化鍵特定情報である鍵番号「０」との入力を受け入れて、当該暗号化鍵特定情報によって特定される暗号化鍵k0と、第１定数値C10とを記憶部４２から読み出す。そしてコード関係情報R1と第１定数値C10とを連接してチャレンジコード「R1||C10」を生成する（Ｓ２５）。

【０１１４】

周辺機器４は、暗号化鍵k0を用いて、上記生成したチャレンジコード「R1||C10」を暗号化し、暗号化情報、ENC(k0, (R1||C10))を生成する。

【０１１５】

周辺機器４は、暗号化情報ENC(k0, (R1||C10))の所定一部（例えば下位６４ビット部分）を暗号関係情報として取り出す（Ｓ２６）。そして取り出した暗号関係情報を、本体５に対して送信する（Ｓ２７）。

【０１１６】

本体５は、この暗号関係情報を受信する。そして処理Ｓ２４で生成した比較用暗号化情報の所定一部（下位６４ビット部分）と、受信した暗号関係情報とが一致しているか否かを調べ、周辺機器４側を認証する（Ｓ２８）。

【０１１７】

周辺機器を不正に製造する側には、一般に、暗号化鍵k0や第１定数値C10が不知であるので、チャレンジコードが生成できず、また、暗号化情報を生成することもできない。従って、一般には処理Ｓ２８において比較用暗号化情報の所定一部（下位６４ビット部分）と、受信した暗号関係情報とが一致せず、周辺機器４側が不正なものと判断できる。

【０１１８】

さらに周辺機器４では、本体５を認証するためのチャレンジコード（第２のチャレンジコード）に係る第２のコード関係情報を生成してもよい（Ｓ２９）。具体的に、ここでは乱数ルーチンによって６４ビット長の乱数値R2を発生させ、当該乱数値R2を第２のコード関係情報として、処理Ｓ２７において暗号関係情報とともに送信する。

【０１１９】

周辺機器４側では、第２のコード関係情報R2に基づいて第２のチャレンジコードを生成する。ここでは処理Ｓ２２にて送信された暗号化鍵特定情報である鍵番号「０」に対応する第２定数値C20を記憶部４２から読み出す。そして、この第２定数値C20を、第２のコード関係情報R2に連接して、第２のチャレンジコード「R2||C20」を生成する（Ｓ３０）。

【０１２０】

周辺機器４は、暗号鍵特定情報である鍵番号「０」によって特定される暗号化鍵k0を用いて、第２のチャレンジコードを暗号化して、比較用暗号化情報ENC(k0, (R2||C20))を生成しておく（Ｓ３１）。

【０１２１】

本体５側では、処理Ｓ２７にて送信された第２のコード関係情報R2に、第２定数値C20を連接して第２のチャレンジコード「R2||C20」を生成して取得する（Ｓ３２）。本体５は、暗号化鍵k0を用いて、上記生成した第２のチャレンジコードを暗号化し、暗号化情報ENC(k0,(R2||C20))を生成する。そして本体５は、この暗号化情報の所定一部（下位６４ビット部分）を暗号関係情報として取り出し（Ｓ３３）、取り出した暗号関係情報を、周辺機器４に対して送信する（Ｓ３４）。

【０１２２】

周辺機器４は、当該本体５が送信した暗号関係情報を受信し、処理Ｓ３１で生成した比較用暗号化情報の所定一部（下位６４ビット部分）と、本体５側から受信した暗号関係情報とが一致しているか否かを判断する（Ｓ３５）。そして、その判断の結果を本体５に対して送信する（Ｓ３６）。

【０１２３】
既に述べたように、処理Ｓ３１で生成した比較用暗号化情報の所定一部（下位６４ビット部分）と、本体５側から受信した暗号関係情報とが一致した場合は、処理Ｓ３１で生成した比較用暗号化情報の所定一部を認証成立データとして、そのまま本体５側に送信する。

【０１２４】
また、処理Ｓ３１で生成した比較用暗号化情報の所定一部（下位６４ビット部分）と、本体５側から受信した暗号関係情報とが一致しなかった場合は、処理Ｓ３１で生成した比較用暗号化情報の所定一部の各ビットを論理否定したデータを認証不成立データとし、この認証不成立データを本体５側に送出する。

【０１２５】
本体５では、処理Ｓ３６にて送信された判断の結果を基づいて、本体５自身が認証されたか否かを調べる（Ｓ３７）。具体的に、本体５は処理Ｓ３３で送信した暗号化情報の所定一部と、処理Ｓ３６にて送信された判断結果に係る情報とを比較し、一致していれば本体５自身が認証されたものと判断する。また、処理Ｓ３３で送信した暗号化情報の所定一部の各ビットを論理否定したデータと、処理Ｓ３６にて送信された判断結果に係る情報とが一致していれば、本体５自身が認証されなかったものと判断する。

【０１２６】
仮に、暗号化鍵k0等が漏洩した場合は、本体５を回収して、記憶部５２に格納されている暗号化鍵等を、例えば鍵番号「１」で特定される暗号化鍵k1、第１定数値C11、第２定数値C21（これらはいずれも予め周辺機器４側には保持されている）に変更して上書きする。そして暗号化鍵特定情報を「１」に変更する。これにより、本体５よりも数多く流通する周辺機器４を回収することなく、暗号化鍵などの更新を行うことができるようになる。

【０１２７】
本体５と周辺機器４とは、相互に接続されている間は、図１０に示した通信を所定のタイミングごとに繰返し行うこととしてもよい。また、本体５は、処理Ｓ２８にて認証ができなかった場合は、処理Ｓ２１に戻って処理を繰返してもよい。同様に本体５は、処理Ｓ３７にて本体５自身が認証されなかったと判断した場合、処理Ｓ２１に戻って処理を繰返してもよい。

【０１２８】
さらにここまでの説明では、認証の処理に用いるチャレンジコードと暗号化情報との双方について、それぞれの一部を送受信することとしているが、これらのうちいずれか一方については、その全体を送信することとしてもよい。このように、いずれか一方について全体を送信する場合は、通信量についてはその分、負担が増大するが、例えば暗号化情報の全体を送信して一致／不一致を判断させればセキュリティレベルを高めることができる。

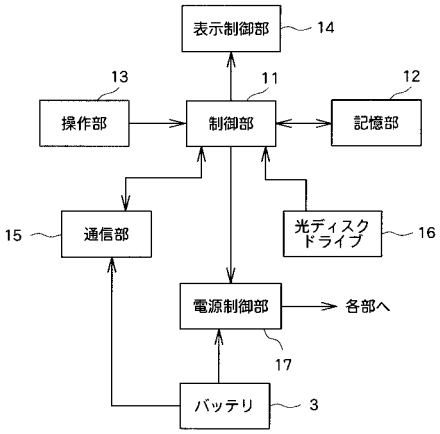
【０１２９】
また、コード関係情報として、チャレンジコードの一部を送信した場合において、コード関係情報Rと定数値Cとの接合の順序は、上述のように「R||C」の順序に限られず、「C||R」としてもよい。さらに本体５が周辺機器４を認証する処理（図１０の処理Ｓ２１からＳ２８に相当する処理）における接合の順序と、周辺機器４が本体５を認証する処理（図１０の処理Ｓ２９からＳ３７に相当する処理）における接合の順序とが異なっていてもよい。

【図面の簡単な説明】
【０１３０】
【図１】本発明の第１の実施の形態に係る認証装置の例を表す構成ブロック図である。
【図２】本発明の第１の実施の形態に係る電源制御部の一例を表す構成ブロック図である。
【図３】本発明の第１の実施の形態に係るバッテリの例を表す構成ブロック図である。

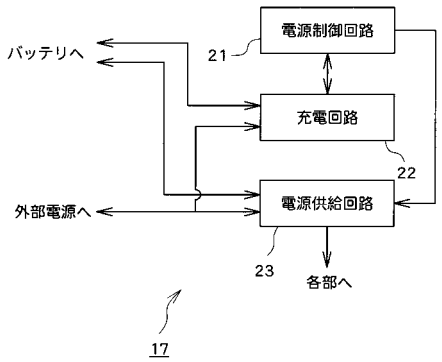
【図４】本発明の第１の実施の形態に係る認証装置の例を表す機能ブロック図である。
【図５】本発明の第１の実施の形態に係る認証装置の動作例を表すフローチャート図である。
【図６】本発明の第２の実施の形態に係る周辺機器４の概要例を表す構成ブロック図である。
【図７】本発明の第２の実施の形態に係る本体５の一例を表す構成ブロック図である。
【図８】本発明の第２の実施の形態に係る周辺機器４の例を表す機能ブロック図である。
【図９】本発明の第２の実施の形態に係る本体５の例を表す機能ブロック図である。
【図１０】本発明の第２の実施の形態に係る周辺機器４及び本体５の間の通信の流れを示す流れ図である。

【符号の説明】
【０１３１】
３　バッテリ、４　周辺機器、５　本体、１１，３１，４１，５１　制御部、１２，３２，４２，５２　記憶部、１３，５３　操作部、１４，５４　表示制御部、１５，３３，４３，５５　通信部、１６，５６　光ディスクドライブ、１７　電源制御部、２１　電源制御回路、２２　充電回路、２３　電源供給回路、６１　バッテリ認証部、６２　失敗カウンタ、６３　間隔値バッファ、６４　外部電源供給判断部、７１　認証要求処理部、７２　本体側認証部、７５　周辺機器認証部、７６　認証要求処理部。

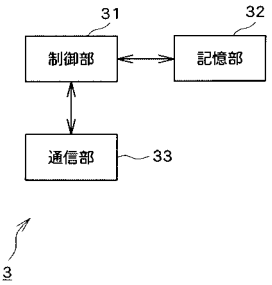
【図１】



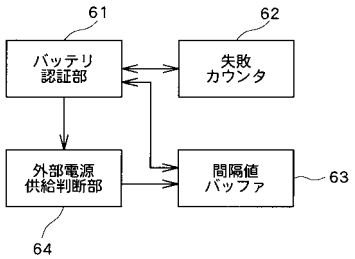
【図２】



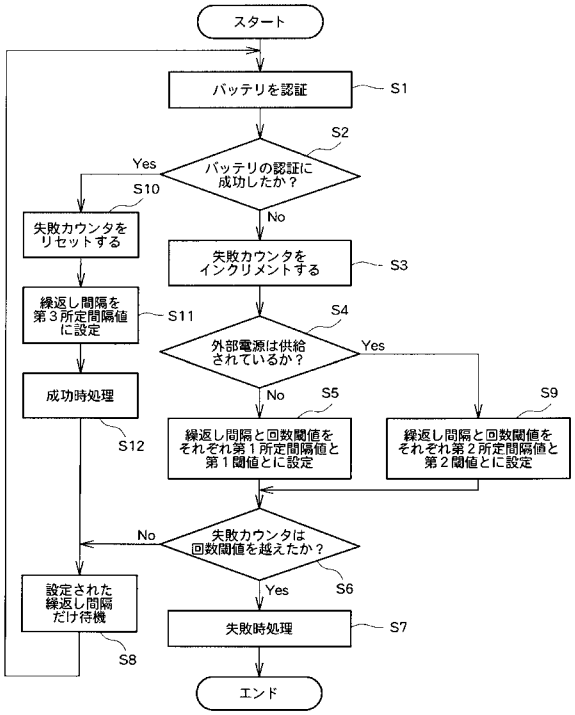
【図３】



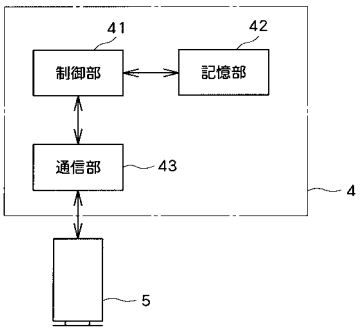
【図４】



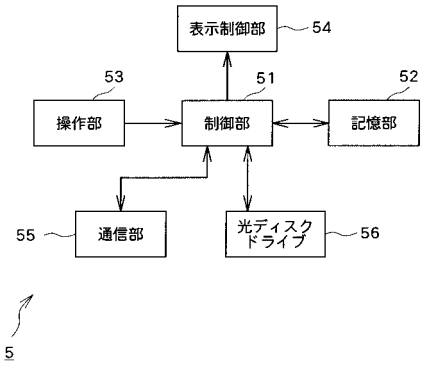
【図５】



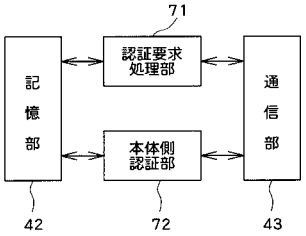
【図６】



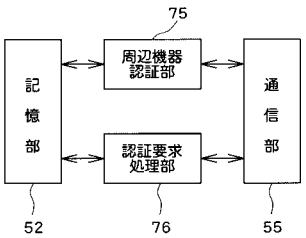
【図７】



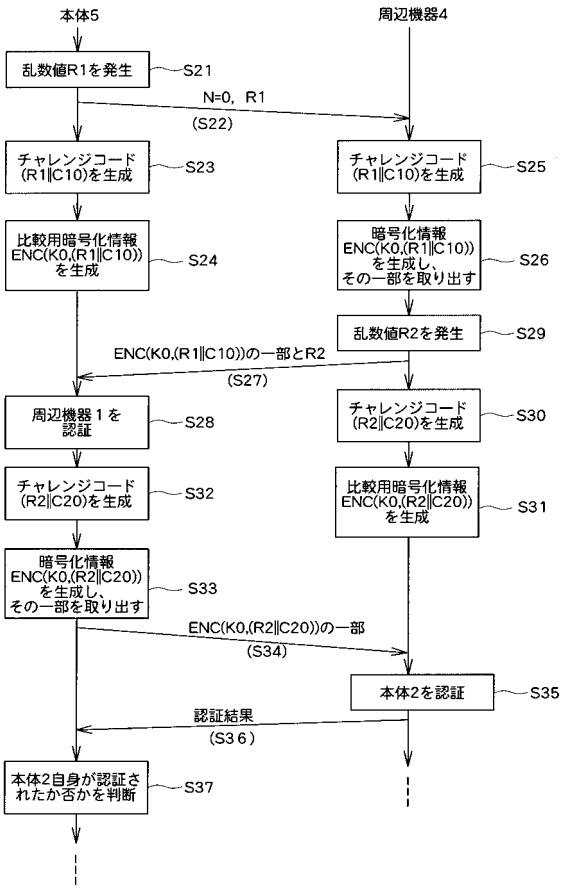
【図８】



【図９】



【図１０】



フロントページの続き

審査官　新田　亮

(56)参考文献　特開２００４－１２６７６５（ＪＰ，Ａ）
特開２００４－１５７７９０（ＪＰ，Ａ）
特開２００５－９４０８９（ＪＰ，Ａ）
特開２００５－１１０３４７（ＪＰ，Ａ）
特開２００５－１５１３６８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２