(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4701615号
(P4701615)

(45)発行日　平成23年6月15日(2011.6.15)　(24)登録日　平成23年3月18日(2011.3.18)

(51)Int.Cl.　　F I
G06F 21/24 (2006.01)　　G06F 12/14 530D
G06F 21/20 (2006.01)　　G06F 15/00 330B

請求項の数 1　(全 19 頁)

(21)出願番号　特願2004-16280(P2004-16280)
(22)出願日　平成16年1月23日(2004.1.23)
(65)公開番号　特開2005-209038(P2005-209038A)
(43)公開日　平成17年8月4日(2005.8.4)
審査請求日　平成18年12月25日(2006.12.25)

前置審査

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100067736
弁理士　小池　晃
(74)代理人　100096677
弁理士　伊賀　誠司
(74)代理人　100106781
弁理士　藤井　稔也
(74)代理人　100113424
弁理士　野口　信博
(74)代理人　100150898
弁理士　祐成　篤哉

最終頁に続く

(54)【発明の名称】情報記憶装置

(57)【特許請求の範囲】
【請求項１】
外部機器と接続するための所定のインターフェースと、上記外部機器からのアクセスが制限されている記憶手段とを備えるリムーバルな情報記憶装置において、
入力するパスワードを構成する情報を示す複数のコードから所望の１コードを選択操作手段の選択操作により選択し、上記選択操作手段の選択操作により選択された上記コードが決定操作手段の決定操作により上記パスワードを構成するパスワード構成コードとして決定し、上記決定操作手段の決定操作により上記パスワード構成コードが決定されたことを視覚的に表示手段により表示することによって、上記所定のインターフェースを介して接続された上記外部機器へ出力することなく、当該情報記憶装置のみに通知するパスワードを入力するパスワード入力手段と、
上記パスワード入力手段によって入力された上記パスワードを照合するパスワード照合手段と、
上記パスワード照合手段によって上記パスワードが照合されたことに応じて、上記所定のインターフェースを介して接続された上記外部機器からの上記記憶手段へのアクセスを許可するアクセス許可手段とを備え、
上記記憶手段は、上記所定のインターフェースを介して接続された上記外部機器からのアクセスが常時許可されている第１の記憶領域と、上記所定のインターフェースを介して接続された上記外部機器からのアクセスが制限されている第２の記憶領域とを備え、上記第１の記憶領域には、上記パスワード入力手段を用いてパスワードを入力する際に起動さ

せるパスワード入力用アプリケーションソフトウェアが格納されており、
上記パスワード照合手段は、上記パスワード入力用アプリケーションソフトウェアが起動され、上記パスワード入力用アプリケーションソフトウェアに従って上記パスワード入力手段によって入力された上記パスワードを照合し、
上記アクセス許可手段は、上記パスワード照合手段によって上記パスワードが照合されたことに応じて、上記記憶手段の第２の記憶領域に対するアクセスを許可すること
を特徴とする情報記憶装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、所定のインターフェースを介して外部機器と接続され、所定のファイルシステムによるデータの書き込み読み出しが可能なリムーバルな情報記憶装置に関し、詳しくは、当該情報記憶装置が備える情報記憶手段へアクセスする際のセキュリティ強度を高めた情報記憶装置に関する。
【背景技術】
【０００２】
ＰＣ（Personal Computer）などの外部機器と、所定のインターフェースを介して接続され、所定のファイルシステムによるデータの書き込み読み出しが可能な情報記憶手段を備えたリムーバルな情報記憶装置が普及している。この情報記憶装置は、情報記憶手段として大容量のフラッシュメモリといった半導体メモリを用いているため、従来まで非常に普及していた磁気ディスク記憶媒体などと比較して大容量で、且つ高速なデータアクセスが可能となっている。
【０００３】
このような、情報記憶装置では、正規のユーザ、例えば、当該情報記憶装置を購入したユーザ以外の者が使用することがないように、情報記憶手段のアクセス制御を行っている。従来までの情報記憶装置では、情報記憶手段へのアクセス制御を行うために、専用のアプリケーションソフトウェアを、当該情報記憶装置を使用するＰＣ全てにインストールし、パスワードを登録する必要があった。
【０００４】
例えば、ユーザは、上記情報記憶装置を購入した際には、情報記憶装置を接続して使用するＰＣ全てに対して、当該情報記憶装置が備える情報記憶手段へのアクセス制御を行うアプリケーションソフトウェアをインストールし、パスワードを登録する。そして、実際に情報記憶装置を使用する際には、ＰＣが備えるキーボードといった入力インターフェースを介してパスワードを入力することで、情報記憶手段へのアクセスを許可するといった制御を行っている（例えば、特許文献１参照。）。
【０００５】
一般に、ユーザが入力するパスワードを用いて、セキュリティシステムを構築した場合、高価なセキュリティデバイスや、高価なセキュリティアプリケーションソフトウェアといたものを必要としないため、セキュリティシステムを構築する上でのコストを抑えることができるといった利点がある。また、パスワードをユーザが覚えやすい数字や、文字などを用いることでユーザにとって利用しやすいとった利点もある。
【０００６】
しかしながら、このように、ユーザにとって利便性の高いパスワードは、ユーザにとって記憶しやすい文字列などとすることが大半であるため、不正利用者にとっても容易に推測可能となってしまうといった問題がある。例えば、ユーザは、生年月日といったユーザ自身と関連性の高い情報をパスワードとして設定することが多いため、不正利用者によって容易に推測されてしまうことになる。
【０００７】
また、パスワードは、ユーザの記憶しやすさから、パスワードの長さが、例えば４桁の数字などというように制限されてしまうことになる。パスワードの長さに、このような制

限があると、不正利用者によって、無制限にパスワードを生成して入力し、パスワードを解析するようなアプリケーションソフトウェアを使用された場合、短時間のうちに完全に解析されてしまうといった問題もある。

【０００８】

また、上述したように情報記憶装置を接続したＰＣのキーボードから、パスワードを入力することで情報記憶手段のアクセスを可能とするセキュリティシステムでは、ＰＣに、例えば、トロイジャン・ホースといったパスワードの不正取得を目的とするコンピュータウィルスを、注入されると、パスワードを簡単に盗み見られてしまうことになる。

【０００９】

このように、情報記憶装置の情報記憶手段へのアクセスを、当該情報記憶装置を接続したＰＣからのパスワード入力によって許可するようなセキュリティシステムは、セキュリティ強度の弱い、非常に脆弱なセキュリティシステムとなってしまうといった問題がある。

【００１０】

【特許文献１】特表２００３－５２４８４２号公報

【発明の開示】

【発明が解決しようとする課題】

【００１１】

そこで、本発明は、このような問題を解決するために案出されたものであり、パスワードを用いるセキュリティシステムのコストの低さと、ユーザ利便性を保持しつつ、セキュリティ強度を極めて強固にした情報記憶装置、セキュリティシステム、アクセス許可方法、ネットワークアクセス方法及びセキュリティ処理実行許可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】

【００１２】

本発明は、外部機器と接続するための所定のインターフェースと、上記外部機器からのアクセスが制限されている記憶手段とを備えるリムーバルな情報記憶装置において、入力するパスワードを構成する情報を示す複数のコードから所望の１コードを選択操作手段の選択操作により選択し、上記選択操作手段の選択操作により選択された上記コードが決定操作手段の決定操作により上記パスワードを構成するパスワード構成コードとして決定し、上記決定操作手段の決定操作により上記パスワード構成コードが決定されたことを視覚的に表示手段により表示することによって、上記所定のインターフェースを介して接続された上記外部機器へ出力することなく、当該情報記憶装置のみに通知するパスワードを入力するパスワード入力手段と、上記パスワード入力手段によって入力された上記パスワードを照合するパスワード照合手段と、上記パスワード照合手段によって上記パスワードが照合されたことに応じて、上記所定のインターフェースを介して接続された上記外部機器からの上記記憶手段へのアクセスを許可するアクセス許可手段とを備え、上記記憶手段は、上記所定のインターフェースを介して接続された上記外部機器からのアクセスが常時許可されている第１の記憶領域と、上記所定のインターフェースを介して接続された上記外部機器からのアクセスが制限されている第２の記憶領域とを備え、上記第１の記憶領域には、上記パスワード入力手段を用いてパスワードを入力する際に起動させるパスワード入力用アプリケーションソフトウェアが格納されており、上記パスワード照合手段は、上記パスワード入力用アプリケーションソフトウェアが起動され、上記パスワード入力用アプリケーションソフトウェアに従って上記パスワード入力手段によって入力された上記パスワードを照合し、上記アクセス許可手段は、上記パスワード照合手段によって上記パスワードが照合されたことに応じて、上記記憶手段の第２の記憶領域に対するアクセスを許可することを特徴とする。

【発明の効果】

【００１９】

これにより、従来からの利便性の高いパスワードを使用しながらも、外部機器を介して

のパスワードの漏洩を完全に防止することができるため、非常に高いセキュリティで、上記記憶手段を保護することが可能となる。

【００２０】

また、本発明は、情報記憶装置にワンタイムパスワード生成手段を備えることによりワンタイムパスワードを用いて、ネットワークへアクセスをするシステムに適用され、端末装置からパスワードを入力することなくユーザ認証ができるため、非常に高いセキュリティでネットワークへアクセス可能となる。

【００２１】

また、本発明は、端末装置が備えるセキュリティチップに搭載した第１の暗号鍵と、全く同じ第２の暗号鍵を情報記憶装置の記憶手段に格納することで、上記セキュリティチップを搭載した端末装置におけるユーザ認証にも適用され、端末装置からパスワードを入力することなくユーザ認証ができるため、非常に高いセキュリティで、端末装置のセキュリティ処理を実行することが可能となる。

【発明を実施するための最良の形態】

【００２２】

以下、本発明に係る情報記憶装置、セキュリティシステム、アクセス許可方法、ネットワークアクセス方法及びセキュリティ処理実行許可方法の発明を実施するための最良の形態を図面を参照にして詳細に説明する。

【００２３】

｛第１の実施の形態｝

図１は、本発明を実施するための最良の形態として示すリムーバルな情報記憶装置である記憶メディア１０の使用形態を示した図である。

【００２４】

図１に示すように、記憶メディア１０は、外部機器であるＰＣ（Personal Computer）２１が備えるＵＳＢ（Universal Serial Bus）ジャック２２に当該記憶メディア１０が備えるＵＳＢプラグ１１を差し込むことで使用可能となる。このように、記憶メディア１０は、外部機器であるＰＣ２１に直接接続されることで、ＰＣ２１のデータストレージ、つまり外部メモリとして機能する。

【００２５】

この、記憶メディア１０が接続されるＰＣ２１は、所定のＯＳ（Operating System）の制御の元に動作する。また、ＰＣ２１は、当該ＰＣで実行処理した結果などを表示するためのモニタ２３を備えている。モニタ２３は、後述する記憶メディア１０のパスワード入力時において、パスワードを選択する際の候補を表示するためにも用いられることになる。

【００２６】

なお、記憶メディア１０は、外部機器であるＰＣ２１とＵＳＢインターフェースを介して接続されるＵＳＢ機器としているが、本発明はこのように接続インターフェースに限定されるものではなく、ＰＣ２１が備える接続インターフェースであれば、どのような接続インターフェースを備えていてもよい。

【００２７】

図１に示すように、記憶メディア１０は、ジョグダイヤル１２を備えており、このジョグダイヤル１２を用いて、後述するフラッシュメモリへのアクセス許可をとるためのパスワードを入力することになる。ジョグダイヤル１２は、矢印Ａで示す方向への回転操作と、矢印Ｂで示す方向への押下操作とが可能なメカニカルな入力手段である。例えば、ユーザは、このジョグダイヤル１２を矢印Ａ方向に回転操作することで、パスワードを構成する文字列の所望の１文字を選択し、ジョグダイヤル１２を矢印Ｂ方向に押下することで選択した１文字をパスワードの文字列の一つとして決定することになる。

【００２８】

なお、本発明は、記憶メディア１０のパスワード入力手段の種別、例えば、上述したジョグダイヤル１２に限定されるものではなく、当該記憶メディア１０に搭載可能な形状で

あり、且つ、パスワードを構成する文字列などの選択操作、決定操作が可能な入力機構を有するものであれば、どのような入力手段であってもかまわない。

【００２９】

また、図１に示すように、記憶メディア１０は、上記ジョグダイヤル１２によってパスワードが決定されたことを確認するための入力確認ランプ１３を備えている。この、入力確認ランプ１３は、例えば、赤色光を発光する発光ダイオードなどであり、ジョグダイヤル１２による、パスワードの構成要素を決定するための、上述したＢ方向への押下操作に応じて点灯する。

【００３０】

続いて、図２を用いて、記憶メディア１０の構成について説明をする。記憶メディア１０は、上述したＵＳＢプラグ１１と、ジョグダイヤル１２と、入力確認ランプ１３と、ＵＳＢコントローラ１４と、ジョグダイヤルコントローラ１５と、ＲＯＭ（Read Only Memory）１６と、ＲＡＭ（Random Access Memory）１７と、ＣＰＵ（Central Processing Unit）１８と、メモリコントローラ１９と、フラッシュメモリ２０とを備えている。ＵＳＢコントローラ１４と、ジョグダイヤルコントローラ１５と、ＲＯＭ１６と、ＲＡＭ１７と、ＣＰＵ１８と、メモリコントローラ１９とは、バス２５を介してそれぞれ接続されている。

【００３１】

ＵＳＢプラグ１１は、上述したように、外部機器のＵＳＢインターフェース、例えば、図１に示したＰＣ２１のＵＳＢジャック２２と接続するためのＵＳＢインターフェースである。ＵＳＢプラグ１１を介して、ＰＣ２１と接続された当該記憶メディア１０は、ＰＣ２１から電源供給を受けることで動作し、ＰＣ２１とデータ通信を行う。

【００３２】

ジョグダイヤル１２は、上述したように、矢印Ａ方向の回転操作と、矢印Ｂ方向の押下操作が可能な機構となっている。ジョグダイヤル１２は、矢印Ａ方向の回転操作に応じて変化する回転方向と、回転速度を検出する回転検出機構と、矢印Ｂ方向の押下操作を検出する押下検出機構を備えている。回転検出機構、押下検出機構は、それぞれが検出する検出値をジョグダイヤルコントローラ１５に出力することになる。

【００３３】

入力確認ランプ１３は、例えば、赤色光を発光する発光ダイオードであり、ジョグダイヤルコントローラ１５にジョグダイヤル１２の押下検出機構から押下操作信号が供給されたことに応じて点灯する。ユーザは、入力確認ランプ１３の点灯を目視することで、パスワードが正確に入力されたことを確認することができる。

【００３４】

ＵＳＢコントローラ１４は、ＵＳＢプラグ１１を介して行われるＰＣ２１と、当該記憶メディア１０とのデータ転送をＵＳＢプロトコルに基づき制御する。

【００３５】

ジョグダイヤルコントローラ１５は、ジョグダイヤル１２が備える回転検出機構から検出された回転方向と回転速度の検出値から回転操作信号を生成する。また、ジョグダイヤルコントローラ１５は、同じくジョグダイヤル１２が備える押下検出機構によって検出された押下操作の検出値から押下操作信号を生成する。ジョグダイヤルコントローラ１５は、この回転操作信号と、押下操作信号とをＣＰＵ１８に供給する。

【００３６】

ＲＯＭ１６は、ＣＰＵ１８で実行するファームウェアや、ファイルシステムを格納しているメモリである。また、ＲＯＭ１６には、図３に示すような、パスワードテーブル３１が格納されている。パスワードテーブル３１は、ユーザがジョグダイヤル１２からパスワード選択するために用意された複数の文字コードからなる文字コード群３１ａと、ジョグダイヤル１２からパスワードを決定するために用意された終了コード３１ｂで構成されたテーブルである。

【００３７】

このＲＯＭ１６に格納されたパスワードテーブル３１は、ジョグダイヤルコントローラ１５からＣＰＵ１８に供給された回転操作信号、押下操作信号に応じて、ＣＰＵ１８によって、文字コード群３１ａから適切な文字コード或いは終了コード３１ｂが読み出されることになる。

【００３８】

パスワードテーブル３１は、ユーザによって登録されたパスワードが文字である場合を想定して用意されたテーブルであるが、本発明は、このようなパスワードの種別に限定されるものではない。

【００３９】

例えば、ユーザによって登録するパスワードを、ユーザが住居しているマンションの住人の名前を順に配列したデータとすると、ＲＯＭ１６に格納されるパスワードテーブルは、名前を示す複数のコードが格納されたテーブルとなる。

【００４０】

また、例えば、ユーザによって登録するパスワードを、ユーザが嗜好する酒の名前を順に配列したデータとすると、ＲＯＭ１６に格納されるパスワードテーブルは、酒名を示す複数のコードが格納されたテーブルとなる。

【００４１】

また、例えば、ユーザによって登録するパスワードを、一別して視認できるようなアイコンを配列、あるいは、単一のアイコンを用いたデータとすると、ＲＯＭ１６に格納されるパスワードテーブルは、アイコンを示す複数のコードが格納されたテーブルとなる。

【００４２】

ＲＡＭ１７は、ＣＰＵ１８のワーキング用のメモリである。

【００４３】

ＣＰＵ１８は、ＲＯＭ１６に格納されているファームウェアや、ファイルシステムを実行して、当該記憶メディア１０の動作を統括的に制御する。ＣＰＵ１８は、上記ファイルシステムに基づいてメモリコントローラ１９を制御し、ＰＣ２１からＵＳＢプラグ１１を介して転送されたデータを、フラッシュメモリ２０に書き込んで記憶させたり、記憶させたデータを読み出してＵＳＢプラグ１１を介してＰＣ２１に転送したりすることで、当該記憶メディア１０をデータストレージとして機能させる。

【００４４】

ＣＰＵ１８は、ジョグダイヤルコントローラ１５から供給される回転操作信号に応じて、ＲＯＭ１６に格納されている、例えばパスワードテーブル３１から文字コードを読み出す。当該記憶メディア１０が接続されたＰＣ２１は、ＣＰＵ１８に対して周期的に文字コードの送信を要求するポーリング（問い合わせ）を行っている。ＣＰＵ１８は、ＰＣ２１からのポーリングに応じて、読み出した文字コードをＵＳＢジャック１１を介してＰＣ２１に送信する。

【００４５】

ＰＣ２１に送信された文字コードは、ＰＣ２１で起動された所定のアプリケーションソフトウェアを介してＰＣ２１のモニタ２３上に文字として表示されることになる。ユーザは、このモニタ２３上に表示された文字を目視することで自分自身がジョグダイヤル１２を操作することで選択した文字コードを確認することができる。

【００４６】

また、ＣＰＵ１８は、ジョグダイヤルコントローラ１５から供給される押下操作信号に応じて、ＲＯＭ１６に格納されているパスワードテーブル３１から読み出した文字コードをパスワードの文字列として決定する。ＣＰＵ１８が読み出した文字コードを、押下操作信号に応じて、パスワードを構成する文字列であると決定した情報は、記憶メディア１０から外部へ、つまりＰＣ２１へ送信されない。

【００４７】

メモリコントローラ１９は、ＲＯＭ１６からＣＰＵ１８に読み出されたファイルシステムによって制御され、フラッシュメモリ２０に記憶するデータをファイルとして管理しな

がら、フラッシュメモリ２０へのデータの書き込み、フラッシュメモリ２０に記憶されたデータの読み出しを制御する。

【００４８】

フラッシュメモリ２０は、当該記憶メディア１０の記憶部であり、ＲＯＭ１６からＣＰＵ１８に読み出されたファイルシステムによって、メモリコントローラ１９でファイルとして管理されるデータを記憶する。また、フラッシュメモリ２０のメモリ領域は、当該記憶メディア１０をＰＣ２１に接続した場合に、直ちに、何の制限もなしにＰＣ２１からのアクセスが可能なオープンエリア２０ａと、ジョグダイヤル１２からのパスワード入力に応じてＰＣ２１からのアクセスが可能となるセキュリティエリア２０ｂとを備えている。

【００４９】

フラッシュメモリ２０のセキュリティエリア２０ｂは、ＰＣ２１からは、パスワードが認証された場合にのみアクセス可能となるが、当該記憶メディア１０のＣＰＵ１８からは、いつでもアクセスすることができる。例えば、このセキュリティエリア２０ｂには、当該記憶メディア１０の初期設定時にジョグダイヤル１２を操作することで登録されるパスワードが格納される。ＣＰＵ１８は、この登録されセキュリティエリア２０ｂに格納されたパスワードと、ジョグダイヤル１２を操作することで入力されるパスワードとを比較照合することで、パスワードの認証処理を行う。

【００５０】

フラッシュメモリ２０のオープンエリア２０ａは、当該記憶メディア１０において、ジョグダイヤル１２を用いてパスワードを入力する際に起動させるパスワード入力用アプリケーションソフトウェア（以下、パスワード入力用アプリケーションソフトウェアを、入力用アプリと省略して呼ぶ。）が格納されている。

【００５１】

ユーザは、記憶メディア１０をＰＣ２１に接続し、セキュリティエリア２０ｂを使用する場合に、まずこのオープンエリア２０ａにアクセスし、入力用アプリを起動させる。入力用アプリは、上述したように、ＣＰＵ１８でＲＯＭ１６のパスワードテーブル３０内から読み出された文字コードを、ＰＣ２１のモニタ２３に表示させるための文字に変換して出力表示させる。ユーザは、記憶メディア１０のジョグダイヤル１２を操作する毎に、ＰＣ２１で起動された入力用アプリがモニタ２３に表示させる文字を目視しながら、自分が現在選択している文字を確認することができる。

【００５２】

また、上述したＲＯＭ１６は、図３に示したような文字コード群３１ａを備えたパスワードテーブル３０ばかりだけではなく、図４に示すように、複数の文字コードからなるパスワードテーブル３１と、複数の名前からなるパスワードテーブル３２と、複数の酒名からなるパスワードテーブル３３と、パスワードテーブル３１，３２，３３を選択するためのカテゴリーテーブル３４とを備えていてもよい。

【００５３】

例えば、ＰＣ２１のＵＳＢジャック２２に、記憶メディア１０のＵＳＢプラグ１１を差し込んでから、ジョグダイヤル１２を始めて回転操作した場合には、ＣＰＵ１８によって、カテゴリーテーブル３４が読み出され、回転操作信号に応じてパスワードをどのような種別にするのか、つまりパスワードテーブル３１，３２、３３のいずれを用いてパスワードを入力するのかを選択する。また、同様に、記憶メディア１０をＰＣ２１に差し込んでから、ジョグダイヤル１２を始めて押下操作した場合には、押下操作信号に応じて、ＣＰＵ１８によって、パスワードテーブル３１，３２，３３のいずれかが読み出され、どの種別のパスワードを入力するのかが決定される。

【００５４】

続いて、図５に示すフローチャートを用いて、記憶メディア１０におけるジョグダイヤル１２を用いたパスワードの入力動作について説明をする。なお、図５に示すフローチャートでの説明においては、ＲＯＭ１６には、パスワードテーブル３０が格納されているものとし、使用するパスワードを文字とする。

【００５５】
ステップＳ１において、まず、記憶メディア１０のＵＳＢジャック１１を、ＰＣ２１のＵＳＢプラグ２２に差し込んで記憶メディア１０をＰＣ２１に接続する。ＰＣ２１に記憶メディア１０が接続されると、ＰＣ２１のＯＳは、記憶メディア１０を周辺機器として認識し、例えば、図６に示すように、モニタ２３上のタスクバー２３ａに、記憶メディア１０が認識され、利用可能であることを示すアイコンＡを表示させる。
【００５６】
ステップＳ２において、ユーザは、ＰＣ２１を介して、記憶メディア１０が備えるフラッシュメモリ２０のオープンエリア２０ａにアクセスし、入力用アプリを起動させる。ＰＣ２１のＯＳは、入力用アプリを実行し、モニタ２３上に、例えば、図６に示すようなアプリケーション実行画面Ｂを表示させる。入力用アプリが実行されると、記憶メディア１０は、ジョグダイヤル１２の操作待ち状態となる。
【００５７】
ステップＳ３において、記憶メディア１０のＣＰＵ１８は、ジョグダイヤル１２が回転操作されたかどうかを、ジョグダイヤルコントローラ１５から供給される回転操作信号に応じて判断する。ＣＰＵ１８は、ジョグダイヤル１２が回転操作されたと判断した場合は、工程をステップＳ４へと進め、回転操作されていないと判断した場合には、ジョグダイヤル１２の操作待ち状態を継続する。
【００５８】
ステップＳ４において、ＣＰＵ１８は、ジョグダイヤルコントローラ１５から供給された回転操作信号に基づいて、ＲＯＭ１６に格納されているパスワードテーブル３０から文字コード又は終了コードを読み出す。
【００５９】
ステップＳ５において、ＣＰＵ１８は、ＰＣ２１の入力用アプリから、文字コード又は終了コードの送信要求をするポーリング（問い合わせ）があった際に、読み出した文字コード又は終了コードをＵＳＢジャック１１を介して送信する。
【００６０】
ステップＳ６において、ＰＣ２１で実行されている入力用アプリは、記憶メディア１０から送信された文字コード又は終了コードを、モニタ２３に表示可能なように文字又は終了メッセージへと変換し、モニタ２３上に表示させる。例えば、図６に示すように、モニタ２３上のアプリケーション実行画面Ｂの所定の領域には、記憶メディア１０から送信された文字コードが変換されて文字“Ｘ”が表示されている。
【００６１】
ステップＳ７において、記憶メディア１０のＣＰＵ１８は、ジョグダイヤル１２が押下操作されたかどうかを、ジョグダイヤルコントローラ１５から供給される押下操作信号に応じて判断する。ＣＰＵ１８は、ジョグダイヤル１２が押下操作されたと判断した場合は、工程をステップＳ８へと進め、押下操作されていないと判断した場合には、工程をステップＳ３へと戻し、ジョグダイヤル１２の操作待ち状態とする。
【００６２】
ステップＳ８において、ＣＰＵ１８は、モニタ２３に終了メッセージが表示されている状態、つまり、ＲＯＭ１６のパスワードテーブル３０から終了コードがＣＰＵ１８に読み出されている場合に、ジョグダイヤル１２が押下操作されジョグダイヤルコントローラ１５から押下操作信号が供給されたかどうかを判断する。ＣＰＵ１８は、終了メッセージではなくモニタ２３に表示された文字に対して押下操作されたと判断した場合は、工程をステップＳ９へと進め、終了メッセージに対して押下操作されたと判断した場合は、工程をステップＳ１０へと進める。
【００６３】
ステップＳ９において、ＣＰＵ１８は、モニタ２３に表示された文字に対して、ジョグダイヤル１２による押下操作がなされ、ジョグダイヤルコントローラ１５から押下操作信号を供給されたことに応じて、パスワードを構成する文字列のうちの１文字を決定する。

ステップＳ９の工程が終了すると、工程をステップＳ３へと戻し、再びジョグダイヤル１２の操作待ち状態となる。

【００６４】

ステップＳ１０において、ＣＰＵ１８は、モニタ２３に表示された終了メッセージに対して、ジョグダイヤル１２による押下操作がなされ、ジョグダイヤルコントローラ１５から押下操作信号が供給されたことに応じて、まだ、パスワードがフラッシュメモリ２０のセキュリティエリア２０ｂに登録されていない場合には、工程をステップＳ１１へと進め、パスワードの登録処理モードとする。既に、フラッシュメモリ２０のセキュリティエリア２０ｂに、パスワードが登録されている場合には、工程をステップＳ１２へと進めパスワードの認証処理モードとする。

【００６５】

ステップＳ１１において、ＣＰＵ１８は、メモリコントローラ１９を制御して、ジョグダイヤル１２によって入力された複数の文字列で構成されるパスワードを、フラッシュメモリ２０のセキュリティエリア２０ｂに格納する。

【００６６】

ステップＳ１２において、ＣＰＵ１８は、メモリコントローラを制御して、フラッシュメモリ２０のセキュリティエリア２０ｂにアクセスし、格納されている登録パスワードを読み出す。そして、ＣＰＵ１８は、読み出した登録パスワードと、新たにジョグダイヤル１２によって入力されたパスワードとを比較照合して、認証処理を行う。

【００６７】

ＣＰＵ１８は、入力されたパスワードと、登録パスワードとが一致し、入力されたパスワードが認証された場合には、フラッシュメモリ２０のセキュリティエリア２０ｂを解放して、ＰＣ２１からのＵＳＢプラグ１１を介したアクセスを許可する。

【００６８】

このように、ＰＣ２１に接続された記憶メディア１０は、パスワードを入力する際、ジョグダイヤル１２を回転操作してパスワードを選択する際の、文字コードをＰＣ２１に送信するものの、どの文字コードをパスワードとして決定したか通知する押下操作信号は、ＣＰＵ１８にのみ送信されるので、入力されたパスワードをＰＣ２１から知ることを不可能とする。また、ＰＣ２１からパスワードを入力することができないため、ＰＣ２１からの不正なアタックを排除することができる。

【００６９】

つまり、記憶メディア１０は、ユーザがパスワードを入力する際に、入力するパスワードを目視して確認するためだけにＰＣ２１のモニタ２３を利用しているため、従来までのように、ＰＣ２１に直接入力したパスワードが、当該ＰＣ２１に残ってしまうことによるパスワードの漏洩を完全に回避することを可能とする。

【００７０】

また、図示しないが、記憶メディア１０に小型の液晶ディスプレイを搭載させ、ＰＣ２１のモニタ２３で行っていたパスワード入力時の文字又は終了メッセージの表示機能を、組み込むようにしてもよい。この場合、記憶メディア１０の製造コストは、液晶ディスプレイ分だけ増加することになるが、当該記憶メディア１０だけで、完全に独立したセキュリティシステムを構築することができる。

【００７１】

｛第２の実施の形態｝

続いて、第２の実施の形態として、この記憶メディア１０をワンタイムパスワードを生成するワンタイムパスワード生成器として用いる場合について説明をする。ワンタイムパスワードとは、ネットワーク上において、端末装置などからアクセスしたユーザが正当なユーザであるかどうか認証する認証処理に使用されるパスワードである。このワンタイムパスワードは、ユーザがネットワークへのアクセスを行う毎に、毎回異なるパスワードになるため、盗み見、盗聴に非常に強いといった利点を有している。ワンタイムパスワードは、毎回、異なるパスワードを、ユーザが入力することになるため、利便性を考え、ワン

タイムパスワードを自動的に生成するワンタイムパスワード生成器を用いるのが一般的になっている。

【００７２】

図７に、ワンタイムパスワード生成機能を備えた記憶メディア４０を示す。記憶メディア４０は、図２を用いて説明した記憶メディア１０に、ワンタイムパスワード生成部４１を与えた以外は、全く同じ構成であるため、重複する個所は、同符号を付し説明を省略する。

【００７３】

ワンタイムパスワード生成部４１は、ネットワーク上の認証サーバ（ＲＡＤＩＵＳサーバ）との間でのみ規定されている所定のアルゴリズムにしたがって、ユーザのネットワーク上へのアクセスがある毎に、ワンタイムパスワードを生成する。

【００７４】

記憶メディア４０のフラッシュメモリ２０は、セキュリティエリア２０ｂに、暗号キーＵｋを格納している。この暗号キーＵｋは、上述したジョグダイヤル１２を用いたパスワードの入力によりセキュリティエリア２０ｂへのアクセスが可能となることで使用可能となる。セキュリティエリア２０ｂに格納された暗号キーＵｋは、当該記憶メディア４０の製造時に製造者によって格納され、ワンタイムパスワードによる認証処理におけるチャレンジレスポンス時に使用されることになる。

【００７５】

このワンタイムパスワード生成部４１を備える記憶メディア４０は、具体的には、図８に示すような、いわゆるＲＡＤＩＵＳ（Remote Authentication Dial In User Service）認証システムにて使用することができる。ＲＡＤＩＵＳ認証システムとは、クライアント・サーバ型の認証システムであり、特に、リモートアクセスの規模が大きくなり、アクセスポイントを複数持つようなネットワークシステムにおけるユーザ情報の管理を一元的に行う場合などに適用することができる。

【００７６】

図８に示すように、ＲＡＤＩＵＳ認証システムでは、まず、クライアント端末であるＰＣ２１は、リモートアクセスサーバ５１へダイヤルインする。このリモートアクセスサーバ５１は、ＲＡＤＩＵＳサーバ５２に対して認証要求を行い、ＲＡＤＩＵＳサーバ５２は、認証の可否を、再びリモートアクセスサーバ５１を介してクライアント端末であるＰＣ２１に送ることになる。ＲＡＤＩＵＳサーバ５２は、認証処理に使用することになる登録ユーザの認証情報を格納した認証データベース５２ａと、認証処理結果に応じて実際のネットワークサービス時の課金処理を行うためのアカウントデータベース５２ｂを備えている。

【００７７】

このようなＲＡＤＩＵＳ認証システムは、例えば、音楽配信サービス、ソフトウェア配信サービス、電子商取引などを行う場合に適用されることになる。

【００７８】

図９に示すフローチャートを用いて、このようなＲＡＤＩＵＳ認証システムにおける認証処理について説明をする。

【００７９】

まず、ステップＳ２１において、図５に示すフローチャートを用いて説明をしたのと全く同じ動作で、記憶メディア４０からパスワードを入力する。パスワードの認証がなされると、フラッシュメモリ２０のセキュリティエリア２０ａへのアクセスが可能となり、暗号化キーＵｋが使用可能となる。

【００８０】

ステップＳ２２において、パスワードの認証がなされ、フラッシュメモリ２０のセキュリティエリア２０ａへのアクセスが可能となったことに応じて、図１０に示すタイミングチャートのようにチャレンジレスポンスが開始される。なお、図１０においては、説明のため記憶メディア４０と、ＲＡＤＩＵＳサーバ５２のみのタイミングチャートを示してい

るが、図８に示すように、記憶メディア４０は、ＰＣ２１に接続され、リモートアクセスサーバ５１を介して、ネットワーク上のＲＡＤＩＵＳサーバ５２に接続されていることが前提である。

【００８１】

図１０に示すように、ステップＳ３１において、まず、記憶メディア４０から、ユーザは、あらかじめ登録されているＩＤをＲＡＤＩＵＳサーバ５２に送信する。このときのＩＤの入力手法は、ジョグダイヤル１２を用いたパスワードの入力手法と全く同じである。

【００８２】

ステップＳ３２において、これを受けたＲＡＤＩＵＳサーバ５２は、チャレンジコードＣ１を記憶メディア４０に送信する。ＲＡＤＩＵＳサーバ５２は、記憶メディア４０からＩＤが送られる毎に、異なるチャレンジコードを送信することになる。このチャレンジコードは、例えば、乱数などである。

【００８３】

ステップＳ３３において、記憶メディア４０のＣＰＵ１８は、アクセス可能となったフラッシュメモリ２０のセキュリティエリア２０ｂから、暗号キーＵｋを読み出し、読み出した暗号キーＵｋをワンタイムパスワード生成部４１に供給する。

【００８４】

ワンタイムパスワード生成部４１は、この暗号化キーＵｋを用い、所定のアルゴリズムに基づいて、ＲＡＤＩＵＳサーバ５２から送信されたチャレンジコードＣ１を暗号化する。ワンタイムパスワード生成部４１において、暗号キーＵｋで暗号化されたチャレンジコードＣ１を、ワンタイムパスワード、ＥｎｃＵｋ（Ｃ１）とする。記憶メディア４０は、このＥｎｃＵｋ（Ｃ１）を、ＲＡＤＩＵＳサーバ５２に送信する。

【００８５】

ステップＳ３４において、ＲＡＤＩＵＳサーバ５２は、送信されたＥｎｃＵｋ（Ｃ１）を復号する。復号した結果、チャレンジコードＣ１が得られた場合は、記憶メディア４０にＩＤを入力して送信したユーザが、正当なユーザであることが認証されることになる。

【００８６】

再び、図９に示すフローチャートに戻る。

【００８７】

ステップＳ２３において、上述したステップＳ２２におけるチャレンジレスポンスの結果、ユーザ認証されなかった場合は工程をステップＳ２４へと進め、ユーザ認証された場合は工程をステップＳ２５へと進める。

【００８８】

ステップＳ２４において、ユーザ認証されなかったため、ＲＡＤＩＵＳ認証システムへのログインが不可となるため、ＲＡＤＩＵＳサーバ５２で提供される各種アプリケーションサービスを受けることができない。

【００８９】

ステップＳ２５において、ユーザ認証されたことに応じて、ＲＡＤＩＵＳ認証システムへのログインが可能となる。

【００９０】

ステップＳ２６において、ユーザは、ＲＡＤＩＵＳサーバ５２が提供する各種アプリケーションサービスを実行する。

【００９１】

このようにして、ワンタイムパスワード生成部４１を備える記憶メディア４０は、例えば、ＲＡＤＩＵＳ認証システムにおいて、ワンタイムパスワードを用いた非常に強固な認証処理を展開することが可能となり、パスワードの盗み見などのリスクを大幅に低減することができる。また、記憶メディア１０と同様に、記憶メディア４０でも、入力したパスワードがＰＣ２１へ残ることを排除することができる。

【００９２】

｛第３の実施の形態｝

続いて、第３の実施の形態として、記憶メディア１０を接続するＰＣ２１に、ＴＣＧ（Trusted Computing Group）によって規定されたセキュリティチップを搭載させることでセキュリティ機能を高めたＰＣとした場合に、記憶メディア１０を用いる使用手法について説明をする。

【００９３】

セキュリティチップは、正式にはＴＰＭ（Trusted Platform Module）と呼ばれ、セキュリティやプライバシーを実現するための基本機能のみを提供するもので、上述したＴＣＧの規定する仕様書に定義されている。ＰＣに搭載されたセキュリティチップは、あらかじめ搭載されている上記ＰＣ以外に移行させることはできず、このセキュリティチップを取り外した場合は、ＰＣは起動できなくなってしまうように構成されている。

【００９４】

図１１に、セキュリティチップ５０を搭載したＰＣ２１を示す。セキュリティチップ５０は、例えば、ＥＥＰＲＯＭ（Electrically Erasable Programmable Read Only Memory）といったメモリ５１を備えており、セキュリティチップ５０を搭載したＰＣ２１におけるセキュリティ処理のコアの鍵となる暗号キーＣｋを格納している。メモリ５１に格納された暗号キーＣｋは、セキュリティチップ５０内にあるため、不正なアクセスからの被害を受けにくく、当該セキュリティチップ５０から直接読み出すコマンドも存在しないため、不正に読み出されることはない。

【００９５】

この暗号キーＣｋは、ＰＣ２１におけるアプリケーションを利用する際の暗号鍵を暗号化するため、これらのアプリケーションを利用するには、必ず暗号キーＣｋが要求されることになる。このようなセキュリティチップ５０を備えるＰＣ２１は、セキュリティチップ５０内のメモリ５１に格納された暗号キーＣｋを用いて、ユーザ認証や、ファイルの暗号化、電子証明の保護を行うことで、当該ＰＣ２１以外では、使用できないセキュリティ機能を提供することができる。

【００９６】

このように、セキュリティチップ５０を搭載したＰＣ２１においても、不正なユーザによる使用を排除するため、ユーザ認証をする必要がある。上述したように、ＰＣ２１からキーボードなどによりパスワードを入力すると、ＰＣ２１に残されたパスワードが不正に取得されるなどといった問題が発生するため、記憶メディア１０を用いてパスワードを入力するようにする。

【００９７】

このとき、記憶メディア１０が備えるフラッシュメモリ２０のセキュリティエリア２０ｂに、ＰＣ２１のセキュリティチップ５０内のメモリ５１に格納させた暗号キーＣｋと全く同じ鍵を格納させておく。ＰＣ１０は、この暗号キーＣｋを用いて、図１２に示すようにネットワーク上にＰＣ２１と接続された認証サーバ６０との間で、チャレンジレスポンスを実行してユーザ認証を行うことになる。

【００９８】

図１３に示すフローチャートを用いて、このようなユーザ認証システムにおける認証処理について説明をする。

【００９９】

まず、ステップＳ４１において、図５に示すフローチャートを用いて説明をしたのと全く同じ動作で、記憶メディア１０からパスワードを入力する。パスワードの認証がなされると、フラッシュメモリ２０のセキュリティエリア２０ａへのアクセスが可能となり、暗号キーＣｋが使用可能となる。

【０１００】

ステップＳ４２において、パスワードの認証がなされ、フラッシュメモリ２０のセキュリティエリア２０ａへのアクセスが可能となったことに応じて、図１４に示すタイミングチャートのようにチャレンジレスポンスが開始される。なお、図１４においては、説明のため記憶メディア１０と、認証サーバ６０のみのタイミングチャートを示しているが、図

１２に示すように、記憶メディア１０は、ＰＣ２１に接続され、ネットワーク上の認証サーバ６０に接続されていることが前提である。

【０１０１】

図１４に示すように、ステップＳ５１において、まず、記憶メディア１０から、ユーザは、あらかじめ登録されているＩＤを認証サーバ６０に送信する。このときのＩＤの入力手法は、ジョグダイヤル１２を用いたパスワードの入力手法と全く同じである。

【０１０２】

ステップＳ５２において、これを受けた認証サーバ６０は、チャレンジコードＣ２を記憶メディア１０に送信する。認証サーバ６０は、記憶メディア１０からＩＤが送られる毎に、異なるチャレンジコードを送信することになる。このチャレンジコードは、例えば、乱数などである。

【０１０３】

ステップＳ５３において、記憶メディア１０のＣＰＵ１８は、アクセス可能となったフラッシュメモリ２０のセキュリティエリア２０ｂから、暗号キーＣｋを読み出す。

【０１０４】

ＣＰＵ１８は、この暗号キーＣｋを用い、所定のアルゴリズムに基づいて、認証サーバ６０から送信されたチャレンジコードＣ２を暗号化する。ＣＰＵ１８において、暗号キーＣｋで暗号化されたチャレンジコードＣ２を、暗号化チャレンジコード、ＥｎｃＣｋ（Ｃ２）とする。記憶メディア１０は、このＥｎｃＣｋ（Ｃ２）を、認証サーバ６０に送信する。

【０１０５】

ステップＳ５４において、認証サーバ６０は、送信されたＥｎｃＣｋ（Ｃ２）を復号する。復号した結果、チャレンジコードＣ２が得られた場合は、記憶メディア１０にＩＤを入力して送信したユーザが、正当なユーザであることが認証されることになる。

【０１０６】

再び、図１３に示すフローチャートに戻る。

【０１０７】

ステップＳ４３において、上述したステップＳ４２におけるチャレンジレスポンスの結果、ユーザ認証されなかった場合は工程をステップＳ４４へと進め、ユーザ認証された場合は工程をステップＳ４５へと進める。

【０１０８】

ステップＳ４４において、ユーザ認証されなかったため、ＰＣ２１におけるセキュリティチップ５０を介したセキュリティ処理を伴うアプリケーションの実行をするためのログインが不可となる。

【０１０９】

ステップＳ４５において、ユーザ認証されたことに応じて、ＰＣ２１におけるセキュリティチップ５０を介したセキュリティ処理を伴うアプリケーションを実行するためのログインが可能となる。

【０１１０】

ステップＳ４６において、ユーザは、ＰＣ２１におけるセキュリティチップ５０を介してセキュリティ処理を伴う各種アプリケーションサービスを実行する。

【０１１１】

このようにして、記憶メディア１０でジョグダイヤル１２によって入力したパスワードが照合されたことに応じて利用可能となる、セキュリティエリア２０ｂに格納された暗号キーＣｋによってユーザ認証をするため、非常にセキュリティの高い認証処理を展開することが可能となる。また、パスワードの盗み見などのリスクを大幅に低減することができると共に、パスワードがＰＣ２１へ残ることを排除することができる。

【０１１２】

なお、上述した第１乃至第３の実施の形態として示した記憶メディア１０，４０に、例えば、指紋照合などといった、バイオメトリクス機能を搭載させ、このバイオメトリクス

機能によって、ユーザ認証処理を行うようにしてもよい。

【図面の簡単な説明】

【０１１３】

【図１】本発明の第１の実施の形態として示す記憶メディアの使用形態について説明するための図である。

【図２】同記憶メディアの構成について説明するための図である。

【図３】同記憶メディアに格納されたパスワードテーブルについて説明するための図である。

【図４】同記憶メディアに格納された複数のパスワードテーブルについての説明及び当該パスワードテーブルの使用方法の一具体例を説明するための図である。

【図５】同記憶メディアにおけるパスワード入力時の動作について説明するためのフローチャートである。

【図６】同記憶メディアにおけるパスワード入力時において、当該記憶メディアが接続されたＰＣ（Personal Computer）で起動させるパスワード入力用アプリケーションソフトウェアの表示画面の一例を示した図である。

【図７】本発明の第２の実施の形態として示す記憶メディアの構成について説明するための図である。

【図８】同記憶メディアの使用形態について説明するための図である。

【図９】同記憶メディアを用い、ワンタイムパスワード生成してユーザ認証処理をする際の動作について説明をするためのフローチャートである。

【図１０】図９のフローチャートで示すユーザ認証処理におけるチャレンジレスポンスの動作について説明するためのタイミングチャートである。

【図１１】本発明の第３の実施の形態として示す記憶メディアを接続するＰＣが備えるセキュリティチップについて説明するための図である。

【図１２】同記憶メディアの使用形態について説明するための図である。

【図１３】同記憶メディアを用い、ユーザ認証処理をする際の動作について説明するためのフローチャートである。

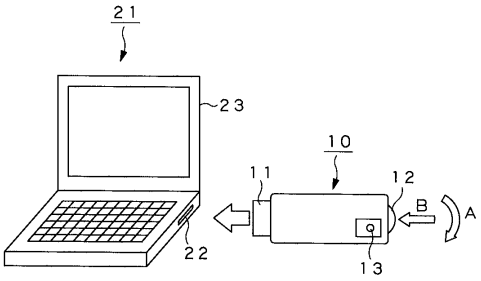
【図１４】図１３のフローチャートで示すユーザ認証処理におけるチャレンジレスポンスの動作について説明するためのタイミングチャートである。

【符号の説明】

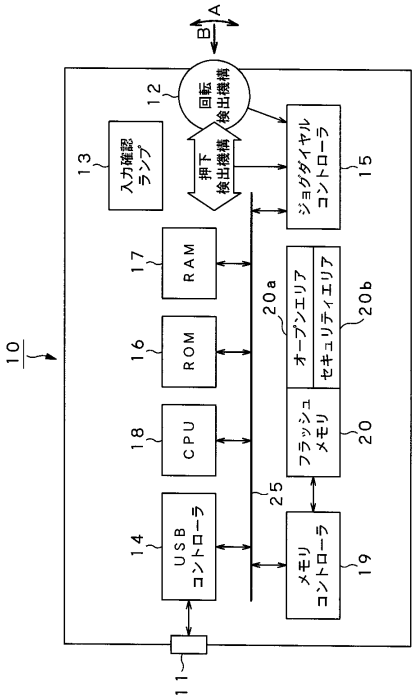
【０１１４】

１０，４０　記憶メディア、１１　ＵＳＢ（Universal Serial Bus）ジャック、１２　ジョグダイヤル、１３　入力確認ランプ、１４　ＵＳＢコントローラ、１５　ジョグダイヤルコントローラ、１６　ＲＯＭ（Read Only Memory）、１７　ＲＡＭ（Random Access Memory）、１８　ＣＰＵ（Central Processing Unit）、１９　メモリコントローラ、２０　フラッシュメモリ、２０ａ　オープンエリア、２０ｂ　セキュリティエリア、４１　ワンタイムパスワード生成部

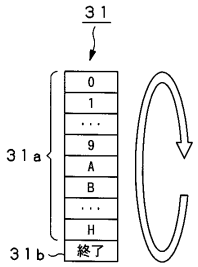
【図１】


21
23
10
11
12
B
A
22
13

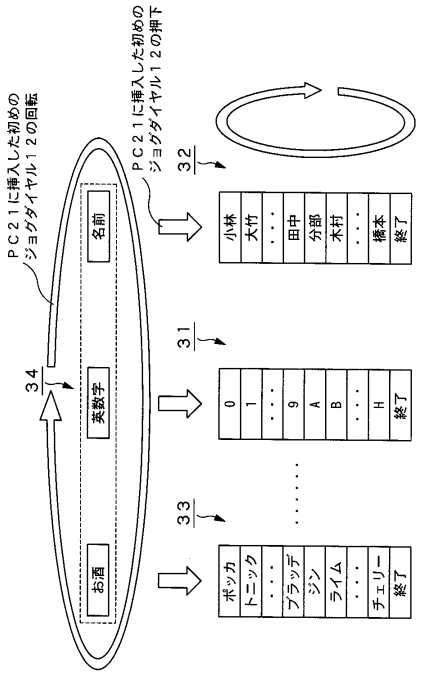
【図２】


A
B
回転検出機構
12
入力確認ランプ
13
押下検出機構
ジョグダイヤルコントローラ
15
RAM
17
ROM
16
CPU
18
USBコントローラ
14
メモリコントローラ
19
フラッシュメモリ
20
オープンエリア
20a
セキュリティエリア
20b
25
10
11

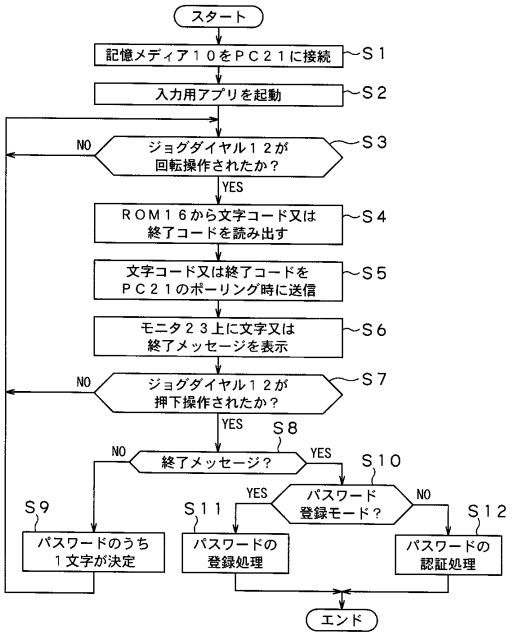
【図３】


31
0
1
9
A
B
H
終了
31a
31b

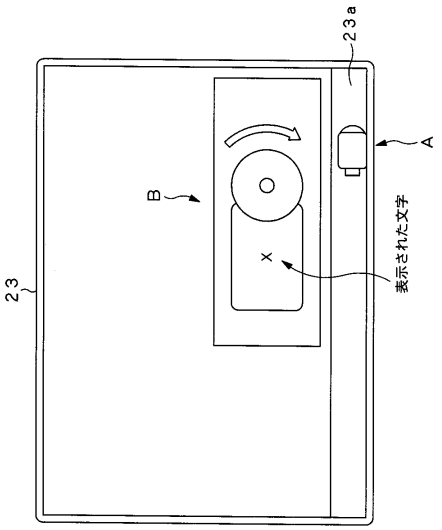
【図４】


PC21に挿入した初めのジョグダイヤル12の回転
PC21に挿入した初めのジョグダイヤル12の押下
名前
英数字
お酒
34
31
32
33
小林
大竹
田中
分部
木村
橋本
終了
0
1
9
A
B
H
終了
ボッカ
トニック
ブラッデ
ジン
ライム
チェリー
終了

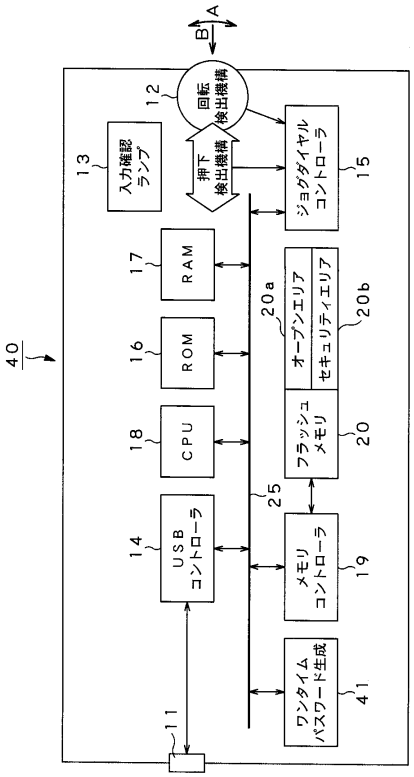
【図５】


スタート
記憶メディア１０をＰＣ２１に接続
S1
入力用アプリを起動
S2
NO
ジョグダイヤル１２が回転操作されたか？
S3
YES
ＲＯＭ１６から文字コード又は終了コードを読み出す
S4
文字コード又は終了コードをＰＣ２１のポーリング時に送信
S5
モニタ２３上に文字又は終了メッセージを表示
S6
NO
ジョグダイヤル１２が押下操作されたか？
S7
YES
S8
NO
終了メッセージ？
YES
S10
YES
パスワード登録モード？
NO
S9
パスワードのうち１文字が決定
S11
パスワードの登録処理
S12
パスワードの認証処理
エンド

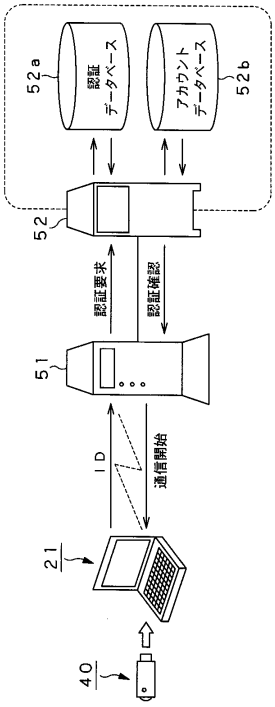
【図６】


23a
A
B
23
表示された文字

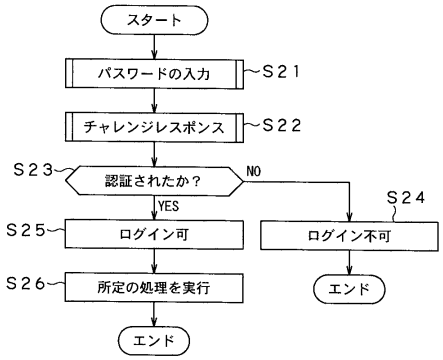
【図７】


A
B
回転検出機構
12
押下検出機構
入力確認ランプ
13
ジョグダイヤルコントローラ
15
RAM
17
ROM
16
CPU
18
USBコントローラ
14
オープンエリア
セキュリティエリア
20a
20b
フラッシュメモリ
20
メモリコントローラ
19
ワンタイムパスワード生成
41
25
11
40

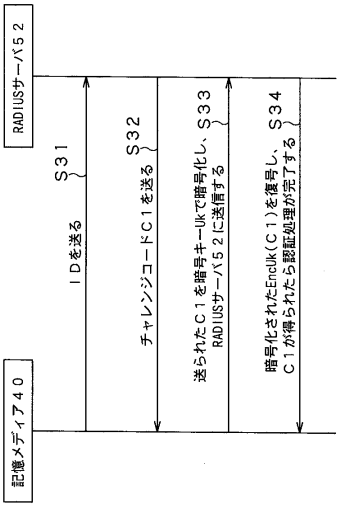
【図８】


認証データベース
52a
アカウントデータベース
52b
52
認証要求
認証確認
51
ID
通信開始
21
40

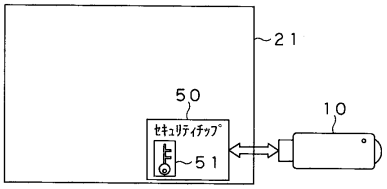
【図９】



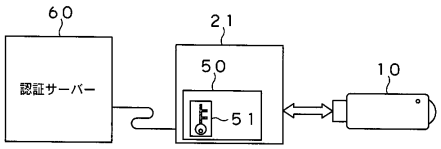
【図１０】



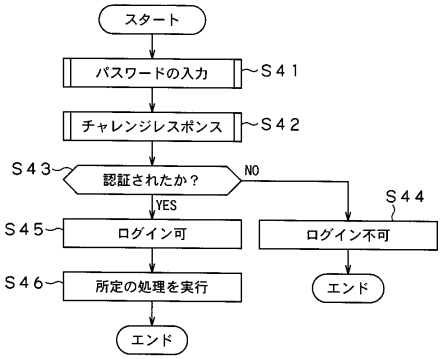
【図１１】



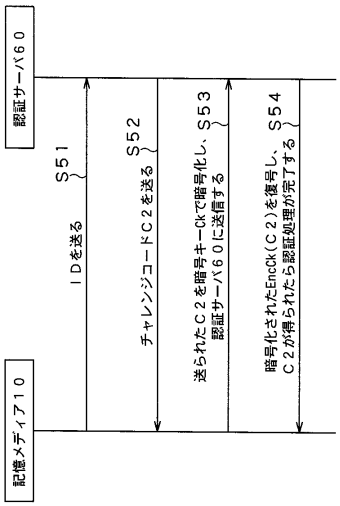
【図１２】



【図１３】



【図１４】


認証サーバ６０
記憶メディア１０
ＩＤを送る
Ｓ５１
チャレンジコードＣ２を送る
Ｓ５２
送られたＣ２を暗号キーＣｋで暗号化し、
認証サーバ６０に送信する
Ｓ５３
暗号化されたEnc_Ck(Ｃ２)を復号し、
Ｃ２が得られたら認証処理が完了する
Ｓ５４

フロントページの続き

(72)発明者　船橋　武
東京都品川区北品川６丁目７番３５号　ソニー株式会社内
(72)発明者　長戸　佐起子
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　児玉　崇晶

(56)参考文献　特表２００２－５３５７４６（ＪＰ，Ａ）
特開２００４－０２１５８１（ＪＰ，Ａ）
特開２００３－０４４４３６（ＪＰ，Ａ）
特開２００２－０４１２２８（ＪＰ，Ａ）
特開２００１－２０９６１５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４
Ｇ０６Ｆ　２１／２０