(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4965512号
(P4965512)
(45)発行日　平成24年7月4日(2012.7.4)　(24)登録日　平成24年4月6日(2012.4.6)

(51)Int.Cl.　F I
G06F 21/20 (2006.01)　G06F 21/20　144C

請求項の数 8　(全 21 頁)

(21)出願番号　特願2008-144420 (P2008-144420)
(22)出願日　平成20年6月2日 (2008.6.2)
(65)公開番号　特開2009-289242 (P2009-289242A)
(43)公開日　平成21年12月10日 (2009.12.10)
審査請求日　平成22年9月30日 (2010.9.30)

(73)特許権者　390040187
株式会社バッファロー
愛知県名古屋市中区大須三丁目３０番２０号
(74)代理人　110000028
特許業務法人明成国際特許事務所
(72)発明者　菰田　英明
名古屋市南区柴田本通４丁目１５番　株式会社バッファロー内

審査官　田中　慎太郎

最終頁に続く

(54)【発明の名称】認証システム、情報処理装置、記憶装置、認証方法及びそのプログラム

(57)【特許請求の範囲】
【請求項１】
情報処理装置と記憶装置とを備えた認証システムであって、
公開鍵暗号化方式の公開鍵と秘密鍵とを生成する鍵生成手段と、
前記記憶装置のユーザが入力する識別情報を受け付ける識別情報受付手段と、
前記識別情報受付手段により受け付けられた第１の識別情報をもとに第１の鍵を生成し、該第１の鍵を、前記鍵生成手段が生成した第１の公開鍵で暗号化した第２の鍵を生成し、前記第１の公開鍵と前記第２の鍵とを、前記記憶装置内の記憶媒体に記憶させる第１の初期設定手段と、
前記識別情報受付手段により受け付けられた第２の識別情報をもとに第３の鍵を生成し、該第３の鍵を前記記憶された第１の公開鍵で暗号化して、第４の鍵を生成し、該第４の鍵と前記記憶された第２の鍵とを照合して、前記ユーザが前記記憶媒体にアクセス可能とするためのユーザの認証を行う第１の認証手段と、
前記第２の識別情報をもとに生成された第３の鍵を、前記鍵生成手段が生成した第２の公開鍵と秘密鍵とのうち、該第２の公開鍵で暗号化して第５の鍵を生成し、該第２の公開鍵と第５の鍵とを前記記憶媒体に記憶させると共に、前記秘密鍵を前記情報処理装置にのみ記憶させる第２の初期設定手段と、
前記情報処理装置に接続される所定の記憶装置の登録指示を受け付け、該所定の記憶装置の登録のための動作を行う登録手段と、
前記情報処理装置に新たに記憶装置が接続されたとき、該接続された記憶装置が、前記

登録された記憶装置であるか否かを判断し、前記登録された記憶装置であると判断した場合に、前記記憶した秘密鍵を認証のために提供する秘密鍵提供手段と、
前記秘密鍵提供手段から前記秘密鍵を受け取って、前記記憶された第５の鍵を該秘密鍵で復号化して、第６の鍵を生成し、該第６の鍵を前記記憶された第１の公開鍵で暗号化して、第７の鍵を生成し、該第７の鍵と、前記記憶された第２の鍵とを照合して、前記ユーザが前記記憶媒体にアクセス可能とするためのユーザの認証を行う第２の認証手段と
を備えた認証システム。
【請求項２】
記憶装置と接続される情報処理装置であって、
前記記憶装置が生成した秘密鍵を該記憶装置から受け取って、記憶する記憶手段と、
前記情報処理装置に接続される所定の記憶装置の登録指示を受け付け、該所定の記憶装置の登録のための動作を行う登録手段と、
前記情報処理装置に、前記秘密鍵を有しない記憶装置が新たに接続されたとき、該接続された記憶装置が、前記登録された記憶装置であるか否かを判断し、前記登録された記憶装置であると判断した場合に、前記記憶した秘密鍵を、前記秘密鍵を有しない記憶装置に渡す秘密鍵提供手段と
を備えた情報処理装置。
【請求項３】
請求項２記載の情報処理装置であって、
前記記憶手段は、前記取得した秘密鍵を暗号化して記憶し、
前記秘密鍵提供手段は、前記暗号化した秘密鍵を復号化して、前記接続された記憶装置に渡す
情報処理装置。
【請求項４】
情報処理装置と接続される記憶装置であって、
公開鍵暗号化方式の公開鍵と秘密鍵とを生成する鍵生成手段と、
前記記憶装置のユーザが入力する識別情報を受け付ける識別情報受付手段と、
前記識別情報受付手段により受け付けられた第１の識別情報をもとに第１の鍵を生成し、該第１の鍵を、前記鍵生成手段が生成した第１の公開鍵で暗号化した第２の鍵を生成し、前記第１の公開鍵と前記第２の鍵とを記憶媒体に記憶させる第１の初期設定手段と、
前記識別情報受付手段により受け付けられた第２の識別情報をもとに第３の鍵を生成し、該第３の鍵を前記記憶された第１の公開鍵で暗号化して、第４の鍵を生成し、該第４の鍵と前記記憶された第２の鍵とを照合して、前記ユーザが前記記憶媒体にアクセス可能とするためのユーザの認証を行う第１の認証手段と、
前記第２の識別情報をもとに生成された第３の鍵を、前記鍵生成手段が生成した第２の公開鍵と秘密鍵とのうち、該第２の公開鍵で暗号化して第５の鍵を生成し、該第２の公開鍵と第５の鍵とを前記記憶媒体に記憶させると共に、前記秘密鍵を前記情報処理装置に渡し、該秘密鍵を前記記憶装置から消去する第２の初期設定手段と、
前記情報処理装置から前記秘密鍵を受け取って、前記記憶された第５の鍵を該秘密鍵で復号化して、第６の鍵を生成し、該第６の鍵を前記記憶された第１の公開鍵で暗号化して、第７の鍵を生成し、該第７の鍵と、前記記憶された第２の鍵とを照合して、前記ユーザが前記記憶媒体にアクセス可能とするためのユーザの認証を行う第２の認証手段と
を備えた記憶装置。
【請求項５】
請求項４記載の記憶装置であって、
前記記憶媒体は、予め用意した特定のプログラムでしかアクセスできない隠し領域を備え、
前記第１の初期設定手段は、前記第１の公開鍵と前記第２の鍵とを前記隠し領域に記憶させ、
前記第２の初期設定手段は、前記第２の公開鍵と第５の鍵とを前記隠し領域に記憶させ

る
記憶装置。
【請求項６】
請求項４または請求項５記載の記憶装置であって、
前記第２の初期設定手段は、前記鍵生成手段が、前記記憶装置に接続された情報処理装置ごとに生成した前記第２の公開鍵と前記秘密鍵とのうち、該第２の公開鍵で暗号化して第５の鍵を生成し、
前記記憶媒体は、予め位置が定められ、所定数に区画されて管理される区画記憶領域を備え、
前記第２の初期設定手段は、少なくとも前記第２の公開鍵と第５の鍵とを、前記接続された情報処理装置ごとに、前記区画記憶領域の１つに記憶させる
記憶装置。
【請求項７】
記憶装置と接続された情報処理装置が、該記憶装置のユーザの認証を行うためのコンピュータプログラムであって、
前記記憶装置が生成し、前記認証に用いる秘密鍵を該記憶装置から受け取って、記憶する記憶機能と、
前記情報処理装置に接続される所定の記憶装置の登録指示を受け付け、該所定の記憶装置の登録のための動作を行う登録機能と、
前記情報処理装置に、前記秘密鍵を有しない記憶装置が新たに接続されたとき、該接続された記憶装置が、前記登録された記憶装置であるか否かを判断し、前記登録された記憶装置であると判断した場合に、前記記憶した秘密鍵を、前記秘密鍵を有しない記憶装置に渡す秘密鍵提供機能と
をコンピュータに実現させるプログラム。
【請求項８】
情報処理装置と接続される記憶装置のユーザの認証を行う認証方法であって、
第１の初期設定として、第１の公開鍵を生成すると共に、前記記憶装置のユーザが入力する第１の識別情報をもとに第１の鍵を生成し、該第１の鍵を前記第１の公開鍵で暗号化した第２の鍵を生成し、前記第１の公開鍵と前記第２の鍵とを記憶媒体に記憶させ、
第２の初期設定として、前記ユーザが入力する第２の識別情報をもとに第３の鍵を生成し、第２の公開鍵と秘密鍵とを生成し、前記第３の鍵を該第２の公開鍵で暗号化して第４の鍵を生成し、該第２の公開鍵と第４の鍵とを前記記憶媒体に記憶させると共に、前記秘密鍵を前記情報処理装置に渡し、該秘密鍵を前記記憶装置から消去し、
前記情報処理装置と前記記憶装置とを新たに接続した際に、前記情報処理装置が、該新たに接続した記憶装置を、予め登録動作を行って登録した記憶装置であると判断した場合に渡す秘密鍵を受け取って、前記記憶された第４の鍵を該秘密鍵で復号化して、第５の鍵を生成し、該第５の鍵を前記記憶された第１の公開鍵で暗号化して、第５の鍵を生成し、該第５の鍵と、前記記憶された第２の鍵とを照合して、前記ユーザが前記記憶媒体にアクセス可能とするためのユーザの認証を行う
認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号化手段を用いた利用者の認証技術に関する。
【背景技術】
【０００２】
近年、ＩＴ技術の発展に伴い、フラッシュメモリ、ハードディスク、ＭＯ、ＤＶＤなど、種々の記憶媒体が普及している。こうした記憶媒体に機密情報等を記憶させる場合、記憶媒体の紛失、盗難などによる情報漏洩を防止するために、利用者認証に成功した場合にのみ、記憶媒体にアクセスできる装置が開発されている。

【０００３】
【特許文献１】特開２００４－３６２５１６号公報
【特許文献２】特開２００７－１５６７７５号公報
【０００４】
しかしながら、記憶媒体にアクセスするたびにパスワードの入力等を行うことは、ユーザにとって面倒であった。
【発明の開示】
【発明が解決しようとする課題】
【０００５】
上述の問題を考慮し、本発明が解決しようとする課題は、利用者認証が必要な記憶装置において、セキュリティを一定程度保ちつつ、記憶媒体にアクセスする際の利用者の利便性を向上させることである。
【課題を解決するための手段】
【０００６】
本発明は、上述の課題の少なくとも一部を解決するためになされたものであり、以下の形態又は適用例として実現することが可能である。
【０００７】
［適用例１］情報処理装置と記憶装置とを備えた認証システムであって、
公開鍵暗号化方式の公開鍵と秘密鍵とを生成する鍵生成手段と、
前記記憶装置のユーザが入力する識別情報を受け付ける識別情報受付手段と、
前記識別情報受付手段により受け付けられた第１の識別情報をもとに第１の鍵を生成し、該第１の鍵を、前記鍵生成手段が生成した第１の公開鍵で暗号化した第２の鍵を生成し、前記第１の公開鍵と前記第２の鍵とを、前記記憶装置内の記憶媒体に記憶させる第１の初期設定手段と、
前記識別情報受付手段により受け付けられた第２の識別情報をもとに第３の鍵を生成し、該第３の鍵を前記記憶された第１の公開鍵で暗号化して、第４の鍵を生成し、該第４の鍵と前記記憶された第２の鍵とを照合して、前記ユーザが前記記憶媒体にアクセス可能とするためのユーザの認証を行う第１の認証手段と、
前記第２の識別情報をもとに生成された第３の鍵を、前記鍵生成手段が生成した第２の公開鍵と秘密鍵とのうち、該第２の公開鍵で暗号化して第５の鍵を生成し、該第２の公開鍵と第５の鍵とを前記記憶媒体に記憶させると共に、前記秘密鍵を前記情報処理装置にのみ記憶させる第２の初期設定手段と、
前記情報処理装置に接続される所定の記憶装置の登録指示を受け付け、該所定の記憶装置の登録のための動作を行う登録手段と、
前記情報処理装置に新たに記憶装置が接続されたとき、該接続された記憶装置が、前記登録された記憶装置であるか否かを判断し、前記登録された記憶装置であると判断した場合に、前記記憶した秘密鍵を認証のために提供する秘密鍵提供手段と、
前記秘密鍵提供手段から前記秘密鍵を受け取って、前記記憶された第５の鍵を該秘密鍵で復号化して、第６の鍵を生成し、該第６の鍵を前記記憶された第１の公開鍵で暗号化して、第７の鍵を生成し、該第７の鍵と、前記記憶された第２の鍵とを照合して、前記ユーザが前記記憶媒体にアクセス可能とするためのユーザの認証を行う第２の認証手段と
を備えた
認証システム。
【０００８】
かかる構成の認証システムは、ユーザの認証に用いる秘密鍵を生成し、これを情報処理装置のみに記憶する。情報処理装置は、当該秘密鍵を記憶しておき、新たに記憶装置が接続された際に、当該記憶装置が登録された記憶装置であると判断すれば、秘密鍵を認証のために提供し、これを用いて、ユーザの認証が行われる。したがって、ユーザは、パスワード等を入力することなく、ユーザの認証を行うことができる。また、ユーザの認証に用いる秘密鍵を、情報装置のみに記憶しておくので、記憶装置が第三者の手に渡った場合で

あっても、第三者は、容易に記憶装置の認証を行うことができず、セキュリティも確保できる。

【０００９】

なお、本願において、記憶装置とは、記憶媒体と記憶媒体へのデータの書き込み等を行う記憶媒体制御装置とを一体的に備えた装置、例えば、ＵＳＢフラッシュメモリ、外付けハードディスクドライブ、コンピュータ等の種々の装置と、記憶媒体と脱着可能に接続でき、当該記憶媒体へのデータ書き込み等を行う制御装置、例えば、ＣＤドライブ、ＤＶＤドライブ、ＭＯドライブ、ブルーレイドライブ、メモリカードリーダ等の種々の装置とを併せた総称である。

【００１０】

［適用例２］記憶装置と接続される情報処理装置であって、記憶装置が生成した秘密鍵を記憶装置から受け取って、記憶する記憶手段と、情報処理装置に接続される所定の記憶装置の登録指示を受け付け、所定の記憶装置の登録のための動作を行う登録手段と、情報処理装置に、秘密鍵を有しない記憶装置が新たに接続されたとき、接続された記憶装置が、登録された記憶装置であるか否かを判断し、登録された記憶装置であると判断した場合に、記憶した秘密鍵を、秘密鍵を有しない記憶装置に渡す秘密鍵提供手段とを備えた情報処理装置。

かかる構成の情報処理装置も、適用例１と同様の効果を奏する。

【００１１】

［適用例３］適用例２記載の情報処理装置であって、記憶手段は、取得した秘密鍵を暗号化して記憶し、秘密鍵提供手段は、暗号化した秘密鍵を復号化して、接続された記憶装置に渡す情報処理装置。

【００１２】

かかる構成の情報処理装置は、記憶装置から受け取った秘密鍵を暗号化して記憶しておくので、暗号化された秘密鍵が第三者の手に渡っても、第三者は、容易に記憶装置の認証を行うことができないので、セキュリティを高めることができる。

【００１３】

［適用例４］情報処理装置と接続される記憶装置であって、公開鍵暗号化方式の公開鍵と秘密鍵とを生成する鍵生成手段と、記憶装置のユーザが入力する識別情報を受け付ける識別情報受付手段と、識別情報受付手段により受け付けられた第１の識別情報をもとに第１の鍵を生成し、第１の鍵を、鍵生成手段が生成した第１の公開鍵で暗号化した第２の鍵を生成し、第１の公開鍵と第２の鍵とを記憶媒体に記憶させる第１の初期設定手段と、識別情報受付手段により受け付けられた第２の識別情報をもとに第３の鍵を生成し、第３の鍵を記憶された第１の公開鍵で暗号化して、第４の鍵を生成し、第４の鍵と記憶された第２の鍵とを照合して、ユーザが記憶媒体にアクセス可能とするためのユーザの認証を行う第１の認証手段と、第２の識別情報をもとに生成された第３の鍵を、鍵生成手段が生成した第２の公開鍵と秘密鍵とのうち、第２の公開鍵で暗号化して第５の鍵を生成し、第２の公開鍵と第５の鍵とを記憶媒体に記憶させると共に、秘密鍵を情報処理装置に渡し、秘密鍵を記憶装置から消去する第２の初期設定手段と、情報処理装置から秘密鍵を受け取って、記憶された第５の鍵を秘密鍵で復号化して、第６の鍵を生成し、第６の鍵を記憶された第１の公開鍵で暗号化して、第７の鍵を生成し、第７の鍵と、記憶された第２の鍵とを照合して、ユーザが前記記憶媒体にアクセス可能とするためのユーザの認証を行う第２の認証手段とを備えた記憶装置。

かかる構成の記憶装置も、適用例１と同様の効果を奏する。

【００１４】

［適用例５］適用例４記載の記憶装置であって、記憶媒体は、予め用意した特定のプログラムでしかアクセスできない隠し領域を備え、第１の初期設定手段は、第１の公開鍵と第２の鍵とを隠し領域に記憶させ、第２の初期設定手段は、第２の公開鍵と第５の鍵とを隠し領域に記憶させる記憶装置。

【００１５】

かかる構成の記憶装置は、ユーザの認証に関係する情報を隠し領域に記憶させるため、万が一、記憶装置が第三者の手に渡った場合であっても、これらの情報に簡単にアクセスすることができない。したがって、記憶装置のセキュリティを高めることができる。

【００１６】

［適用例６］適用例４または適用例５記載の記憶装置であって、第２の初期設定手段は、鍵生成手段が、記憶装置に接続された情報処理装置ごとに生成した第２の公開鍵と秘密鍵とのうち、第２の公開鍵で暗号化して第５の鍵を生成し、記憶媒体は、予め位置が定められ、所定数に区画されて管理される区画記憶領域を備え、第２の初期設定手段は、少なくとも第２の公開鍵と第５の鍵とを、接続された情報処理装置ごとに、区画記憶領域の１つに記憶させる記憶装置。

【００１７】

かかる構成の記憶装置は、第５の鍵と、接続される情報処理装置ごとに生成される第２の公開鍵とを、予め位置が定められ、所定数に区画されて管理される区画記憶領域の１つに記憶させる。したがって、記憶装置に接続される情報処理装置は、区画記憶領域を参照することで、第２の認証に用いる鍵の有無を容易に判断することができ、情報処理装置が、接続された記憶装置が第２の認証のために登録されたものであるか否かの判断に資する。

【００１８】

なお、本発明は、上述した認証システム、情報処理装置、記憶装置としての構成のほか、認証方法や、そのプログラムとしても構成することができる。

【発明を実施するための最良の形態】

【００１９】

本発明の実施例について説明する。

Ａ．認証システム２０の概略構成：

本発明の実施例としての認証システム２０は、ホストコンピュータＰＣと、ＵＳＢフラッシュメモリＵＭとにより構成される。なお、ホストコンピュータＰＣは、請求項の情報処理装置に、ＵＳＢフラッシュメモリＵＭは、請求項の記憶装置に該当する。

【００２０】

Ａ－１．ＵＳＢフラッシュメモリの概略構成：

図１は、本願の実施例としてのＵＳＢフラッシュメモリＵＭの概略構成を示す説明図である。ＵＳＢフラッシュメモリＵＭは、汎用入出力ポート３２、ＣＰＵ４０、ＲＯＭ３３、ＳＲＡＭ３４、暗号用回路３５、内部インタフェース３６、フラッシュメモリ５０、ＵＳＢコネクタ３８、電圧制御部３７を備えており、それぞれが内部バスで接続されている。

【００２１】

汎用入出力ポート３２は、ＵＳＢフラッシュメモリＵＭに図示しない指紋認証装置等の付加デバイスを接続する場合に利用するパラレルインタフェースである。

【００２２】

ＣＰＵ４０は、フラッシュメモリ５０やＲＯＭ３３に記憶されたＵＳＢフラッシュメモリＵＭの制御に関するプログラムをＳＲＡＭ３４に展開し、実行することで、利用者の認証や、フラッシュメモリ５０へのデータ書き込み等の機能部として動作する。また、ＣＰＵ４０は、フラッシュメモリ５０やＲＯＭ３３に記憶されたプログラムを実行することで、第１の初期設定部４１、第２の初期設定部４２、識別情報認証部４３、自動認証部４４としても機能する。これらの機能部の詳細については後述する。

【００２３】

ＲＯＭ３３は、不揮発性メモリであり、ＵＳＢフラッシュメモリＵＭをコンピュータＰＣに接続した際に、ＵＳＢフラッシュメモリＵＭを起動させるためのファームウェアが保存されている。

【００２４】

ＳＲＡＭ３４は、ＣＰＵ４０が各種処理を行う際に利用するバッファである。本実施例

では、単純化のために単一のバッファとして示しているが、各処理の高速化のために、例えば、フラッシュメモリ５０のためのバッファと暗号用回路３５のためのバッファからなる構成としてもよい。

【００２５】

暗号用回路３５は、フラッシュメモリ５０に入出力するデータや、ＵＳＢフラッシュメモリＵＭを利用可能とするための利用者認証を行うためのパスワード等を暗号化／復号化するための回路であり、公開鍵暗号と共通鍵暗号の両方式の回路を備えている。公開鍵暗号方式は、主にパスワード等の暗号化／復号化を、共通鍵暗号方式は、後述するセキュア領域のデータの暗号化／復号化に使われる。本実施例においては、公開鍵暗号はＲＳＡ方式、共通鍵方式はＡＥＳ方式を採用した。なお、本実施例においては、暗号化手段として暗号用回路３５を用いたが、暗号化ソフトウェアなど、別の方法を用いてもよい。

【００２６】

内部インタフェース３６は、フラッシュメモリ５０とデータをやり取りするためのインタフェースから成る。

【００２７】

フラッシュメモリ５０は、ブロック単位でデータの消去を行う不揮発性メモリであり、本実施例では、大容量化に適したＮＡＮＤ型のフラッシュメモリとした。

【００２８】

ＵＳＢコネクタ３８は、バスパワード電源の利用が可能なシリアルインタフェースであり、ＵＳＢポートを備えたホストコンピュータＰＣに接続される。

【００２９】

電圧制御部３７は、ＵＳＢコネクタ３８を介して接続されたホストコンピュータＰＣから供給される５Ｖのバスパワード電源を、例えば、３．３Ｖに調整し、各部へ供給する。

【００３０】

図２は、図１に示したフラッシュメモリ５０の内部領域を示す説明図である。フラッシュメモリ５０は、隠し領域５１、フリー領域５２、セキュア領域５３を備えている。また、フリー領域５２及びセキュア領域５３は、それぞれ、フリー領域用、または、セキュア領域用のマスターブートレコード領域、パーティション情報領域、ファイルシステム情報領域、データ情報領域（図中の６１～６４，６６～６９）を備えている。

【００３１】

隠し領域５１は、ファイルシステムの管理外の領域であり、ＣＰＵ４０が使用するプログラムや、フラッシュメモリ５０に保存するデータの暗号化に関する情報、後述する利用者認証に関する情報などを記憶する領域として確保されている。フリー領域５２は、利用者認証を行わずに、アクセスできる領域である。セキュア領域５３は、利用者認証に成功した場合のみアクセス可能となる領域である。

【００３２】

マスターブートレコード領域６１，６６は、ＵＳＢフラッシュメモリＵＭの起動時に最初に読み出される領域であり、ＵＳＢフラッシュメモリＵＭのドライバを起動させるための情報等を記憶する領域である。パーティション情報領域６２，６７は、上述の内部領域の位置や大きさなどを記録したパーティションテーブルを記憶する領域である。ファイルシステム情報領域６３，６８は、ファイルやディレクトリを管理する情報を記憶する領域である。データ情報領域６４，６９は、フラッシュメモリ５０に保存すべきデータを記憶する領域である。

【００３３】

上述の隠し領域５１は、専用のプログラムを用いてしか見ることができない領域である。したがって、ＵＳＢフラッシュメモリＵＭを接続したホストコンピュータＰＣのＯＳ上では、通常、見ることができない。本実施例では、ＣＰＵ４０は、論理デバイスとして扱う領域の外部に置かれた物理デバイスに対して、ファイルシステムを介さずに、直接的にアドレス指定するプログラムにより、隠し領域５１にアクセス可能としている。一方、フリー領域５２は、ＵＳＢフラッシュメモリＵＭをホストコンピュータＰＣに接続しただけ

で、ホストコンピュータＰＣのＯＳ上で見ることができる領域である。また、セキュア領域５３は、利用者認証が成功した後に見ることができる領域である。

【００３４】

このＵＳＢフラッシュメモリＵＭは、他人に知られたくない情報をフラッシュメモリ５０のセキュア領域用データ情報領域６９に記憶させる場合のセキュリティ機能として、暗号化機能と利用者認証機能を備えている。暗号化機能は、上述の暗号用回路３５を用いて、ＵＳＢフラッシュメモリＵＭと接続されたホストコンピュータＰＣが記憶するデータを暗号化してセキュア領域用データ情報領域６９に記憶させ、また、セキュア領域用データ情報領域６９に記憶した暗号化されたデータを復号化して、ホストコンピュータＰＣに出力させる機能である。利用者認証機能は、利用者がＵＳＢフラッシュメモリＵＭを利用する際に、利用者にパスワード等の情報を入力させて、予め利用を許された利用者であるか否かを確認し、予め利用を許された利用者であることが確認できた場合にのみＵＳＢフラッシュメモリＵＭのセキュア領域５３の使用が許可される機能である。

【００３５】

Ａ－２．ホストコンピュータＰＣの概略構成：

ホストコンピュータＰＣの概略構成を図３に示す。本実施例におけるコンピュータＰＣは、所定のプログラムがインストールされた汎用のパーソナルコンピュータであり、ＣＰＵ７０、ハードディスクドライブ８１、ＲＯＭ８２、ＲＡＭ８３、入力機構８４、ディスプレイ８５、ＵＳＢインタフェース８６を備えており、それぞれがバスで接続されている。

【００３６】

ＣＰＵ７０は、ハードディスクドライブ８１やＲＯＭ８２に記憶されたファームウェアやＯＳをＲＡＭ９３展開して実行することで、ホストコンピュータＰＣ全体の制御を司る。また、ＣＰＵ７０は、ハードディスクドライブ８１に記憶されたプログラムを実行することで、記憶部７１、登録部７２、秘密鍵提供部７４、暗号化部７５として機能する。これらの機能部の詳細については、後述する。

【００３７】

入力機構８４は、キーボード及びポインティングデバイスを備えている。ディスプレイ８５は、液晶式のディスプレイである。ＵＳＢインタフェース８６は、ホスト側のＵＳＢポートであり、ＵＳＢフラッシュメモリＵＭに接続される。

【００３８】

Ｂ．パスワード認証処理：

ＵＳＢフラッシュメモリＵＭのパスワード認証処理について説明する。パスワード認証処理とは、ユーザが入力するパスワードに基づいて、ＵＳＢフラッシュメモリＵＭのセキュア領域５３の利用についての利用者認証を行う処理である。

Ｂ－１．パスワード認証処理の初期設定：

パスワード認証処理を行うために必要となる初期設定について説明する。パスワード認証を行うための初期設定処理の手順を図４に示す。図示する一連の処理は、ＵＳＢフラッシュメモリＵＭのユーザが、ＵＳＢフラッシュメモリＵＭをホストコンピュータＰＣに接続し、ディスプレイ８５に表示される選択画面の中から「初期設定」を選択することで、ＵＳＢフラッシュメモリＵＭのＣＰＵ４０が、第１の初期設定部４１の処理として行う。この処理が開始されると、ＣＰＵ４０は、初期設定を行うユーザが入力機構８４を用いて入力する所望のパスワードＰＷ１を、ホストコンピュータＰＣを介して受け付ける（ステップＳ１００）。

【００３９】

次に、ＣＰＵ４０は、受け付けたパスワードＰＷ１から鍵Ａ１を生成する（ステップＳ１１０）。なお、本実施例においては、鍵Ａ１は、受け付けたパスワードＰＷ１の文字列をＵＮＩＣＯＤＥにより数値変換するものとしたが、これに限られるものではなく、入力されたパスワードから一意に求められる鍵を生成できる方法であればよい。例えば、疑似乱数生成器を用いてソルトを生成し、このソルトとパスワードＰＷ１から一方向ハッシュ

関数を用いて、鍵Ａ１を生成するなど、別の方法を用いてもよい。

【００４０】

鍵Ａ１を生成すると、ＣＰＵ４０は、暗号用回路３５を用いて、ＲＳＡ暗号の鍵ペアである公開鍵Ｂと秘密鍵Ｃを生成する（ステップＳ１２０）。

【００４１】

そして、ＣＰＵ４０は、上記ステップＳ１２０で生成した公開鍵Ｂで、上記ステップＳ１１０で生成した鍵Ａ１を暗号化し、鍵Ａ１Ｂを生成し（ステップＳ１３０）、この鍵Ａ１Ｂと公開鍵Ｂとをフラッシュメモリ５０の隠し領域５１に保存する（ステップＳ１４０，Ｓ１５０）。なお、鍵Ａ１Ｂ、公開鍵Ｂは、後述するパスワード認証処理に用いる情報であり、このような情報を上述のように隠し領域５１に保存すれば、万一、ＵＳＢフラッシュメモリＵＭが紛失等により第三者に渡った場合であっても、容易にパスワード認証を行うことができず、ＵＳＢフラッシュメモリＵＭに保存したデータの機密性を確保することができる。

【００４２】

以上の処理により、初期設定処理は終了となる。以降、ユーザは、後述するパスワード認証処理により、ＵＳＢフラッシュメモリＵＭのセキュア領域５３を利用可能となる。なお、上述の鍵Ａ１、鍵Ａ１Ｂは、それぞれ、請求項１の第１の鍵、第２の鍵に該当し、公開鍵Ｂは、請求項１の第１の公開鍵に該当する。

【００４３】

Ｂ－２．パスワード認証処理：

ユーザがＵＳＢフラッシュメモリＵＭのセキュア領域５３の利用を行う際のパスワードによる利用者認証の手順を図５に示す。図示する一連の処理は、上述の初期設定処理を実行した後、ユーザが、上述の初期設定が完了したＵＳＢフラッシュメモリＵＭをホストコンピュータＰＣに接続し、ホストコンピュータＰＣのディスプレイ８５に表示される選択画面の中から「セキュア領域の使用」を選択することで、ＵＳＢフラッシュメモリＵＭのＣＰＵ４０が、識別情報認証部４３として行う処理である。この処理が開始されると、ＵＳＢフラッシュメモリＵＭのＣＰＵ４０は、ユーザが、入力機構８４を用いて入力するパスワードＰＷ２を、ホストコンピュータＰＣを介して受け付ける（ステップＳ２００）。

【００４４】

次に、ＣＰＵ４０は、受け付けたパスワードＰＷ２から鍵Ａ２を生成する（ステップＳ２１０）。この処理は、上記ステップＳ１１０と同一の処理である。

【００４５】

鍵Ａ２を生成すると、ＣＰＵ４０は、フラッシュメモリ５０の隠し領域５１から、上記ステップＳ１５０で保存された公開鍵Ｂを読み出し、この公開鍵Ｂで、上記ステップＳ２１０で生成された鍵Ａ２を暗号化し、鍵Ａ２Ｂを生成する（ステップＳ２２０）。

【００４６】

鍵Ａ２Ｂを生成すると、ＣＰＵ４０は、上記ステップＳ２２０で生成された鍵Ａ２Ｂと、上記ステップＳ１４０でフラッシュメモリ５０の隠し領域５１に保存された鍵Ａ１Ｂとを照合する（ステップ２３０）。

【００４７】

その結果、両鍵が一致しなければ（ステップＳ２３０：ＮＯ）、ステップＳ２００で入力されたパスワードＰＷ２が正しくないということであり、ＣＰＵ４０は、ＵＳＢフラッシュメモリＵＭが接続されたホストコンピュータＰＣのディスプレイ８５にエラー表示をさせ（ステップＳ２４０）、処理を上記ステップＳ２００に戻す。

【００４８】

一方、両鍵が一致すれば（ステップＳ２３０：ＹＥＳ）、ステップＳ２００で入力されたパスワードＰＷ２が正しいということであり、ＣＰＵ４０は、鍵Ａ２をホストコンピュータＰＣのＲＡＭ８３に保存して（ステップＳ２５０）、セキュア領域５３のセキュア領域用データ情報領域６９を開く（ステップＳ２６０）。こうして、パスワード認証処理は終了する。なお、上記ステップＳ２５０で鍵Ａ２をホストコンピュータＰＣのＲＡＭ８３

に保存する構成としたが、ＵＳＢフラッシュメモリＵＭのＳＲＡＭ３４に保存する構成としてもよい。いずれの構成であっても、ＵＳＢフラッシュメモリＵＭをホストコンピュータＰＣから取り外した場合に、鍵Ａ２はＵＳＢフラッシュメモリＵＭ内に残留しないので、セキュリティを確保することができる。

【００４９】

なお、上記ステップＳ２１０で生成された鍵Ａ２は、請求項１の第３の鍵に該当し、上記ステップＳ２２０で生成された鍵Ａ２Ｂは、請求項１の第４の鍵に該当する。

【００５０】

Ｃ．自動認証処理：

ＵＳＢフラッシュメモリＵＭの自動認証処理について説明する。自動認証処理とは、予め登録したホストコンピュータＰＣとＵＳＢフラッシュメモリＵＭとの組合せにおいては、ユーザのパスワード入力を求めることなく、ＵＳＢフラッシュメモリＵＭをホストコンピュータＰＣに接続するだけで、利用者認証を行い、ユーザがセキュア領域５３を利用可能とする処理である。

【００５１】

Ｃ－１．自動認証処理の初期設定：

自動認証処理を行うために必要となる初期設定について説明する。自動認証処理の各種設定を行う設定モードの起動手順を図６に示す。この処理は、ユーザが、ＵＳＢフラッシュメモリＵＭをホストコンピュータＰＣに接続することで、ディスプレイ８５に、フリー領域用データ情報領域６４のＧＵＩ（Graphical User Interface）を表示させ、フリー領域用データ情報領域６４に記憶された所定のプログラムを起動させることで開始される。このプログラムは、ＵＳＢフラッシュメモリＵＭのＣＰＵ４０により実行される。この処理が開始されると、まず、ＣＰＵ４０は、ユーザが入力機構８４を用いて入力する、設定モードへの移行指示を受け付ける（ステップＳ３００）。

【００５２】

設定モードへの移行指示を受け付けると、ＣＰＵ４０は、パスワード認証処理を実行する（ステップＳ３１０）。この処理は、図５を用いて上述したパスワード認証処理のＳ２００～Ｓ２３０と同様の処理である。

【００５３】

そして、パスワード認証処理の認証に成功すると、ＣＰＵ４０は、ディスプレイ８５に、ＵＳＢフラッシュメモリＵＭの隠し領域５１に記憶されたホストコンピュータ登録一覧と、ハードディスクドライブ８１に記憶されたＵＳＢフラッシュメモリ登録一覧を表示させる（ステップＳ３２０）。ホストコンピュータ登録一覧とは、登録されたＵＳＢフラッシュメモリとの組合せにおいて自動認証処理を行うことができる、予め登録されたホストコンピュータの一覧であり、本実施例においては、ホストコンピュータの識別情報の一覧表示と、それぞれに対応する登録削除ボタンを備えている。また、ＵＳＢフラッシュメモリ登録一覧とは、上述の登録されたホストコンピュータとの組合せにおいて自動認証処理を行うことができる、予め登録されたＵＳＢフラッシュメモリの一覧であり、本実施例においては、ＵＳＢフラッシュメモリ名、製品名（型番）、登録日時の一覧表示と、それぞれに対応する登録削除ボタンを備えている。これらの登録方法は、後述する。かかる一覧を含む設定モードとしてのＧＵＩは、後述する登録処理の指示も併せて行うことができるが、登録数は、後述する通り登録制限数が設けられているので、ユーザは、当該ＧＵＩで登録状況を容易に把握しながら、登録制限の範囲内となるように登録・削除指示を行うことができ、ユーザの利便性が向上する。

【００５４】

一覧表示を行うと、ＣＰＵ４０は、設定モードへ移行させ（ステップＳ３３０）、処理を終了する。この設定モードでは、上述したホストコンピュータやＵＳＢフラッシュメモリの登録や登録削除を行うことができる。

【００５５】

Ｃ－２．登録処理：

自動認証処理を行うために必要となる、ホストコンピュータＰＣとＵＳＢフラッシュメモリＵＭとの登録処理の流れについて図７に示す。この処理は、ユーザが、上述した設定モードのＧＵＩを用いて、登録するＵＳＢフラッシュメモリについての所望の名称を入力し、登録指示を入力することで開始される。この処理が開始されると、ホストコンピュータＰＣのＣＰＵ７０は、まず、ユーザが入力したＵＳＢフラッシュメモリ名と登録指示とを受け付ける（ステップＳ４００）。

【００５６】

そして、ＣＰＵ７０は、ホストコンピュータＰＣのハードディスクドライブ８１を参照して、ＵＳＢフラッシュメモリＵＭが規定数登録済みであるかを判断すると共に、ＵＳＢフラッシュメモリＵＭの隠し領域５１を参照して、ホストコンピュータＰＣが規定数登録済みであるかを判断する（ステップＳ４１０）。なお、本実施例においては、登録情報の保存領域の効率的利用、後述する自動認証処理の高速化の観点から、ホストコンピュータＰＣの登録上限を３台、ＵＳＢフラッシュメモリＵＭの登録上限を１０台と定めているため、かかる判断が行われる。

【００５７】

その結果、ＵＳＢフラッシュメモリＵＭが規定数登録済みであれば、または、ホストコンピュータＰＣが規定数登録済みであれば（ステップＳ４１０：ＹＥＳ）、これ以上、登録はできないということであり、ＣＰＵ７０は、その旨をディスプレイ８５に表示させ（図示せず）、処理を上記ステップＳ４００に戻す。

【００５８】

一方、ＵＳＢフラッシュメモリＵＭの登録数が規定数未満であり、かつ、ホストコンピュータＰＣの登録数が規定数未満であれば（ステップＳ４１０：ＮＯ）、さらなる登録が可能であるということであり、ＣＰＵ７０は、処理を進め、上記ステップＳ４００で受け付けたＵＳＢフラッシュメモリ名について、同名の登録が既にされているか否かを判断する（ステップＳ４２０）。

【００５９】

その結果、同名の登録があれば（ステップＳ４２０：ＹＥＳ）、同名での複数台の登録により生じる識別の混乱を避ける必要があるので、ＣＰＵ７０は、その旨を表示させ（図示せず）、処理を上記ステップＳ４００に戻す。

【００６０】

一方、同名の登録がなければ（ステップＳ４２０：ＮＯ）、識別の混乱は生じないので、ＣＰＵ７０は、処理を進め、ホストコンピュータＰＣに接続しているＵＳＢフラッシュメモリＵＭが、既に登録済みのＵＳＢフラッシュメモリＵＭであるか否かを判断する（ステップＳ４３０）。本実施例においては、この判断は、ＵＳＢフラッシュメモリＵＭが登録されることにより、ホストコンピュータＰＣのハードディスクドライブ８１に記憶される登録日時と、ホストコンピュータＰＣの識別情報が登録されることにより、ＵＳＢフラッシュメモリＵＭの隠し領域５１に記憶される登録日時とを読み込んで、両者が一致する組合せがある場合には、登録済みのＵＳＢフラッシュメモリＵＭであると判断する構成とした。なお、この判断は、ホストコンピュータＰＣが、登録されたＵＳＢフラッシュメモリＵＭの識別情報（シリアルナンバなど）を記憶しておき、その一致性に基づいて行ってもよい。

【００６１】

その結果、登録済みのＵＳＢフラッシュメモリＵＭであれば（ステップＳ４３０：ＹＥＳ）、再度登録する必要はないので、ＣＰＵ７０は、その旨を表示させ（図示せず）、処理を上記ステップＳ４００に戻す。

【００６２】

一方、登録済みのＵＳＢフラッシュメモリＵＭでなければ（ステップＳ４３０：ＮＯ）、ＣＰＵ７０は、ＵＳＢフラッシュメモリＵＭに対して、自動認証用鍵の作成指示を送出する（ステップＳ４４０）。

【００６３】

これを受けて、ＵＳＢフラッシュメモリＵＭでは、ＣＰＵ４０が、暗号用回路３５を用いて、自動認証用鍵として、ＲＳＡ暗号の鍵ペアである公開鍵Ｄと秘密鍵Ｅを生成すると共に、ホストコンピュータＰＣに対して、生成した秘密鍵Ｅを送出する（ステップＳ５００）。なお、ＣＰＵ４０は、秘密鍵Ｅの送出後、秘密鍵Ｅを消去し、ＵＳＢフラッシュメモリＵＭ側では、記憶しない構成としたが、ＳＲＡＭ３４にのみ記憶し、ＵＳＢフラッシュメモリＵＭがホストコンピュータＰＣから取り外された際に、秘密鍵Ｅが消去される構成としてもよい。また、公開鍵Ｄは、請求項１の第２の公開鍵に該当し、秘密鍵Ｅは、請求項１の秘密鍵に該当する。

【００６４】

これを受けて、ホストコンピュータＰＣでは、ＣＰＵ７０が、秘密鍵Ｅを受け取り、暗号化部７５の処理として、ホストコンピュータＰＣで使用できる固有の情報Ｆで秘密鍵Ｅを暗号化し、鍵ＥＦを生成する（ステップＳ４５０）。本実施例では、固有の情報Ｆとして、ホストコンピュータＰＣのＭＡＣアドレスＦを用いた。そして、ＣＰＵ７０は、記憶部７１の処理として、生成した鍵ＥＦと、上記ステップＳ４００で受け付けたＵＳＢフラッシュメモリ名と、現在の日時（登録日時）と、ＵＳＢメモリの製品名とを関連付けて、ハードディスクドライブ８１に登録すると共に、ホストコンピュータＰＣの識別情報（以下、ＰＣ識別情報という。ここではＭＡＣアドレス）、登録日時及びＵＳＢフラッシュメモリ名をＵＳＢフラッシュメモリＵＭに対して送出する（ステップＳ４６０）。なお、上記ステップＳ４００～Ｓ４６０は、特に注記した場合を除き、登録部７２の処理として行われる。

【００６５】

一方、ＵＳＢフラッシュメモリＵＭでは、ステップＳ５００で公開鍵Ｄ及び秘密鍵Ｅを生成すると、ＲＡＭ８３から読み込んだ鍵Ａ２を公開鍵Ｄで暗号化し、鍵Ａ２Ｄを生成する（ステップＳ５１０）。そして、ＣＰＵ４０は、ホストコンピュータＰＣから、ＰＣ識別情報、登録日時、上記Ｓ４００で受け付けたＵＳＢフラッシュメモリ名を受け取って、公開鍵Ｄ及び鍵Ａ２Ｄと共に、隠し領域５１に記憶する（ステップＳ５２０）。このように、隠し領域５１に記憶するのは、万一、ＵＳＢフラッシュメモリＵＭが紛失等により第三者に渡った場合であっても、容易にパスワード認証を行うことができず、ＵＳＢフラッシュメモリＵＭに保存したデータの機密性を確保することができるからである。

【００６６】

こうして、ホストコンピュータＰＣと、ＵＳＢフラッシュメモリとの間で、共通の情報を共有することにより、登録処理は終了となる。なお、上記ステップＳ５００～Ｓ５２０の処理は、第２の初期設定部４２の処理として行われる。また、鍵Ａ２Ｄは、請求項１の第５の鍵に該当する。

【００６７】

Ｃ－３．自動認証処理：

自動認証処理の流れについて、図８を用いて説明する。この処理は、前述の初期設定処理（図４）及び登録処理（図７）を実行した後、ユーザが、新たにＵＳＢフラッシュメモリＵＭをホストコンピュータＰＣに接続し、ホストコンピュータＰＣのディスプレイ８５に表示される選択画面の中から「自動認証」を選択し、所定のプログラムを起動させることで、ホストコンピュータＰＣのＣＰＵ７０と、ＵＳＢフラッシュメモリＵＭのＣＰＵ４０とで行われる処理である。ＵＳＢフラッシュメモリＵＭがホストコンピュータＰＣに挿入されたことを検知し、「自動認証」のプログラムを起動するということを別のプログラムで代行させてもよい。なお、ＣＰＵ４０は、自動認証部４４の処理として、この処理を行う。この処理が開始されると、ホストコンピュータＰＣのＣＰＵ７０は、自動認証用鍵（公開鍵Ｄ）が、ＵＳＢフラッシュメモリＵＭの隠し領域５１に記憶されているか否かを判断する（ステップＳ６１０）。

【００６８】

なお、本実施例においては、図９に例示するように、隠し領域５１は、区画記憶領域ＭＡを備えている。区画記憶領域ＭＡは、予め位置が定められており、所定数（ここでは、

ホストコンピュータＰＣの登録上限数である１０）の区画エリアＭＡ１～ＭＡ１０に区画されて管理されている。この例では、各区画エリアＭＡｉ（ｉ＝１～１０）は、公開鍵Ｄ用の領域１２８バイト、鍵Ａ２Ｄ用の領域６４バイト、ＰＣ識別情報用の領域１６バイト、ＵＳＢフラッシュメモリ名用の領域１６バイト、登録日時用の領域４バイト、ホストコンピュータＰＣのハードディスクドライブ８１の位置情報用の領域１バイト（合計２２９バイト）が、それぞれ所定位置に確保されている。また、各区画エリアＭＡｉ（ｉ＝１～１０）の先頭には、当該区画エリアのデータの有無を示すフラグビットが確保されており（図示せず）、上記ステップＳ６１０においては、ＣＰＵ７０は、区画記憶領域ＭＡのフラグビットを参照して、自動認証用鍵の有無を判断するものとした。このような構成とすることで、ＣＰＵ７０は、容易に自動認証用の鍵の有無を判断することができる。

【００６９】

その結果、自動認証用の鍵があれば（ステップＳ６１０：ＹＥＳ）、ＣＰＵ７０は、自己のＰＣ識別情報と一致するＰＣ識別情報が区画記憶領域ＭＡに記憶されているか否かを判断する（ステップＳ６２０）。本実施例では、上述のように、自動認証用の鍵の有無と、一致するＰＣ識別情報の有無とを用いて、登録されたＵＳＢフラッシュメモリＵＭであるか否かの判断を効率的に行う構成としている。

【００７０】

その結果、ＰＣ識別情報が一致するものがあれば（ステップＳ６２０：ＹＥＳ）、接続されたＵＳＢフラッシュメモリＵＭは、自動認証用に登録されたＵＳＢフラッシュメモリＵＭであるということであり、ＣＰＵ７０は、暗号化部７５の処理として、一致するＰＣ識別情報と関連付けられて隠し領域５１に記憶されたＵＳＢフラッシュメモリ名に対応する鍵ＥＦをＭＡＣアドレスＦで復号化し、秘密鍵Ｅを生成すると共に、当該秘密鍵ＥをＵＳＢフラッシュメモリＵＭに渡す（ステップＳ６３０）。なお、上記ステップＳ６１０～Ｓ６３０の処理は、特に注記した場合を除き、秘密鍵提供部７４の処理として行う。

【００７１】

なお、上記ステップＳ６１０において、自動認証用の鍵がなければ（ステップＳ６１０：ＮＯ）、あるいは、上記ステップＳ６２０において、ＰＣ識別情報が一致しなければ（ステップＳ６２０：ＮＯ）、接続されたＵＳＢフラッシュメモリＵＭは、自動認証用に登録されたＵＳＢフラッシュメモリＵＭではないということであり、処理を終了する。

【００７２】

なお、上記ステップＳ６２０において、ＰＣ識別情報が一致しない場合（ステップＳ６２０：ＮＯ）には、同様の判断を規定回数繰り返し、その全てにおいて、ＰＣ識別情報が一致しないと判断した場合に、処理を終了する構成としてもよい。こうすれば、判断の確度を向上させることができる。

【００７３】

一方、ＵＳＢフラッシュメモリＵＭでは、ホストコンピュータＰＣから秘密鍵Ｅを受け取ると（ステップＳ７００）、ＣＰＵ４０が、受け取った秘密鍵Ｅで、隠し領域５１に記憶した鍵ＡＤ２を復号化し、鍵Ａ３を生成する（ステップＳ７１０）。鍵Ａ３を生成すると、ＣＰＵ４０は、隠し領域５１に記憶した公開鍵Ｂで、生成した鍵Ａ３を暗号化し、鍵Ａ３Ｂを生成する（ステップＳ７２０）。

【００７４】

そして、ＣＰＵ４０は、隠し領域５１に記憶している鍵Ａ１Ｂと、生成した鍵Ａ３Ｂとを照合する（ステップＳ７３０）。その結果、両鍵が一致しなければ（ステップＳ７３０：ＮＯ）、受け取った秘密鍵Ｅが正しくないということであり、ＣＰＵ４０は、処理を終了する。

【００７５】

一方、両鍵が一致すれば（ステップＳ７３０：ＹＥＳ）、受け取った秘密鍵Ｅが正しいということであり、ＣＰＵ４０は、セキュア領域５３のセキュア領域用データ情報領域６９を開く（ステップＳ７４０）。こうして、自動認証に成功すると、自動認証処理を終了する。なお、上述の鍵Ａ３は、請求項１の第６の鍵に該当し、鍵Ａ３Ｂは、請求項１の第

７の鍵に該当する。

【００７６】

Ｃ－４．登録削除処理：

認証システム２０における登録削除処理の流れについて図１０に示す。登録削除処理とは、図７で示した登録処理で行ったホストコンピュータＰＣ及びＵＳＢフラッシュメモリＵＭの登録を削除する処理である。この処理は、ユーザが、図６に示した処理で移行した設定モードのＧＵＩを用いて、ホストコンピュータＰＣのハードディスクドライブ８１に記憶されたＵＳＢフラッシュメモリＵＭの登録の一覧、または、ＵＳＢフラッシュメモリＵＭの隠し領域５１に記憶されたホストコンピュータＰＣの登録の一覧のうち、削除を所望する機器に対応する削除ボタンをクリックすることで開始される。この処理が開始されると、ホストコンピュータＰＣのＣＰＵ７０は、まず、ユーザが入力した削除指示を受け付ける（ステップＳ８００）。

【００７７】

登録削除指示を受け付けると、ＣＰＵ７０は、当該指示が、ホストコンピュータＰＣに記憶されたＵＳＢフラッシュメモリＵＭの登録を削除するものであるか否かを判断する（ステップＳ８１０）。その結果、ホストコンピュータＰＣに記憶されたＵＳＢフラッシュメモリＵＭの登録を削除するものであれば、（ステップＳ８１０：ＹＥＳ）、ＣＰＵ７０は、選択されたＵＳＢフラッシュメモリＵＭは、ホストコンピュータＰＣに接続されているＵＳＢフラッシュメモリＵＭであるか否かを判断する（ステップＳ８２０）。本実施例においては、接続されているＵＳＢフラッシュメモリＵＭの隠し領域５１に記憶されているＵＳＢフラッシュメモリ名及び登録日時が、ホストコンピュータＰＣのハードディスクドライブ８１に既に登録されていれば、選択されたＵＳＢフラッシュメモリＵＭは、ホストコンピュータＰＣに接続されているＵＳＢフラッシュメモリＵＭであると判断するものとした。

【００７８】

その結果、選択されたＵＳＢフラッシュメモリＵＭは、接続されているＵＳＢフラッシュメモリＵＭであれば（ステップＳ８２０：ＹＥＳ）、ＣＰＵ７０は、接続されたＵＳＢフラッシュメモリＵＭの隠し領域５１から、自己のＰＣ識別情報に対応するＵＳＢフラッシュメモリＵＭの登録データ（公開鍵Ｄ、鍵ＡＤ２、ＰＣ識別情報、登録日時、ＵＳＢフラッシュメモリ名）を削除する（ステップＳ８３０）。

【００７９】

ＵＳＢフラッシュメモリＵＭの登録データを削除すると、または、上記ステップＳ８２０の判断において、選択されたＵＳＢフラッシュメモリＵＭが接続されていなければ（ステップＳ８２０：ＮＯ）、ＣＰＵ７０は、ホストコンピュータＰＣのハードディスクドライブ８１から、対応するＵＳＢフラッシュメモリＵＭの登録データ（鍵ＥＦ、登録日時、ＵＳＢフラッシュメモリ名、製品名）を削除する（ステップＳ８４０）。

【００８０】

また、上記ステップＳ８１０の判断において、ホストコンピュータＰＣに記憶されたＵＳＢフラッシュメモリＵＭの登録を削除するものでなければ、すなわち、ＵＳＢフラッシュメモリＵＭに記憶されたホストコンピュータＰＣの登録を削除するものであれば（ステップＳ８２０：ＮＯ）、ＣＰＵ７０は、選択された登録が自身のものであるか否かを判断する（ステップＳ８５０）。この判断は、本実施例においては、ＵＳＢフラッシュメモリＵＭの隠し領域５１に記憶されたＵＳＢフラッシュメモリ名及び登録日時が、ハードディスクドライブ８１に既に登録されていれば、選択された登録は、自身のものであると判断するものとした。

【００８１】

その結果、選択された登録が自身のものであれば（ステップＳ８５０：ＹＥＳ）、ＣＰＵ７０は、ハードディスクドライブ８１から、接続されているＵＳＢフラッシュメモリＵＭに関する登録データ（鍵ＥＦ、ＵＳＢフラッシュメモリ名、登録日時、製品名）を削除する（ステップＳ８６０）。

【００８２】
ハードディスクドライブ８１の登録データを削除すると、または、上記ステップＳ８５０の判断において、選択された登録が自身のものでなければ（ステップＳ８５０：ＮＯ）、ＣＰＵ７０は、ＵＳＢフラッシュメモリＵＭの隠し領域５１から、自身のＰＣ識別情報を含む登録データ（公開鍵Ｄ、鍵ＡＤ２、ＰＣ識別情報、登録日時、ＵＳＢフラッシュメモリ名）を削除する（ステップＳ８７０）。こうして、登録削除処理は終了となる。
【００８３】
かかる構成の認証システム２０において、ＵＳＢフラッシュメモリＵＭは、ユーザの認証に用いる秘密鍵Ｅを生成し、これをホストコンピュータＰＣに渡すと共に、自らはこれを保持せずに消去する。ホストコンピュータＰＣは、受け取った秘密鍵Ｅを記憶しておき、新たにＵＳＢフラッシュメモリＵＭが接続された際に、当該ＵＳＢフラッシュメモリＵＭが、予め登録されたＵＳＢフラッシュメモリＵＭであるか否かの判断を行い、登録されたものであれば、記憶していた鍵ＥＦを復号化して秘密鍵Ｅを得、ＵＳＢフラッシュメモリＵＭに渡す。一方、ＵＳＢフラッシュメモリＵＭは、受け取った秘密鍵Ｅを用いて、ユーザの認証を行う。したがって、ユーザは、パスワード等を入力することなく、容易にユーザの認証を行うことができるので、ユーザの利便性が向上する。また、秘密鍵Ｅが暗号化した鍵ＥＦを、ホストコンピュータＰＣにのみ記憶しておくので、ＵＳＢフラッシュメモリＵＭが第三者の手に渡った場合であっても、第三者は、容易にユーザの認証を行うことができず、セキュリティも確保できる。
【００８４】
Ｄ．変形例：
上述の実施例の変形例について説明する。
Ｄ－１．変形例１：
実施例では、図７に示した登録処理において、ホストコンピュータＰＣは、ＵＳＢフラッシュメモリＵＭから受け取った秘密鍵Ｅを暗号化する固有の情報Ｆとして、ＭＡＣアドレスを用いた（ステップＳ４５０）が、固有の情報Ｆは、特に限定するものではない。例えば、暗号化ソフトウェアで生成した鍵などであってもよい。
【００８５】
また、図８で示した自動認証処理において、ホストコンピュータＰＣに接続されたＵＳＢフラッシュメモリＵＭが、登録されたＵＳＢフラッシュメモリＵＭであるか否かを判断するためのＰＣ識別情報として、ＭＡＣアドレスを用いたが（ステップＳ６２０）、ＰＣ識別情報は、特に限定するものではない。例えば、ホストコンピュータＰＣのシリアルナンバなど、ホストコンピュータＰＣを識別できる情報であればよい。
【００８６】
Ｄ－２．変形例２：
実施例では、図７に示した登録処理において、ホストコンピュータＰＣは、ＵＳＢフラッシュメモリＵＭから受け取った秘密鍵Ｅを暗号化してハードディスクドライブ８１に記憶し（ステップＳ４５０，Ｓ４６０）、図８に示した自動認証処理において、暗号化して記憶した鍵ＥＦを復号化して、秘密鍵Ｅを生成し、当該秘密鍵ＥをＵＳＢフラッシュメモリＵＭに渡す（ステップＳ６３０）構成とした。このように、ホストコンピュータＰＣが、秘密鍵Ｅを暗号化して記憶することにより、暗号化された秘密鍵Ｅが第三者の手に渡っても、第三者は、容易に秘密鍵Ｅを復号化することができないので、セキュリティを高めることができるからである。ただし、かかる構成は、必須ではなく、ホストコンピュータＰＣは、秘密鍵Ｅを暗号化せずに記憶してもよい。
【００８７】
Ｄ－３．変形例３：
実施例においては、図４に示した初期設定処理において、ＵＳＢフラッシュメモリＵＭが、公開鍵Ｂ及び秘密鍵Ｃを生成し、公開鍵Ｂで鍵Ａ１を暗号化する構成としたが、当該鍵の生成及び／または暗号化は、ホストコンピュータＰＣ側が備える暗号化手段により行う構成としてもよい。例えば、ホストコンピュータＰＣが、公開鍵Ｂ及び秘密鍵Ｃを生成

し、公開鍵ＢをＵＳＢフラッシュメモリＵＭに渡し、ＵＳＢフラッシュメモリＵＭが、受け取った公開鍵Ｂを用いて、鍵Ａ１を暗号化する構成としてもよい。同様に、図７に示した登録処理において、ＵＳＢフラッシュメモリＵＭが、公開鍵Ｄ及び秘密鍵Ｅを生成し、公開鍵Ｄで鍵Ａ２を暗号化する構成としたが、当該鍵の生成及び／または暗号化は、ホストコンピュータＰＣ側が備える暗号化手段により行う構成としてもよい。例えば、ホストコンピュータＰＣが、公開鍵Ｄ及び秘密鍵Ｅを生成し、公開鍵ＤをＵＳＢフラッシュメモリＵＭに渡し、ＵＳＢフラッシュメモリＵＭが、受け取った公開鍵Ｄを用いて鍵Ａ２を暗号化する構成としてもよい。

【００８８】

もとより、上述の鍵の生成については、ＵＳＢフラッシュメモリＵＭやホストコンピュータＰＣで行う構成に限るものではなく、他で生成した鍵を用いる構成としてもよい。例えば、ホストコンピュータＰＣとネットワークを介して接続されたサーバが鍵を生成し、ホストコンピュータＰＣが、ネットワークを介して当該鍵を取得して用いる構成としてもよいし、ＵＳＢフラッシュメモリの製造段階において、予め鍵を生成して、隠し領域５１などに記憶させておいてもよい。こうすれば、ホストコンピュータＰＣやＵＳＢフラッシュメモリＵＭは、鍵生成手段を備える必要がないので、低コスト化ならびに処理の効率化に資する。

【００８９】

また、実施例においては、図５に示したパスワード認証処理と、図８に示した自動認証処理とは、ＵＳＢフラッシュメモリＵＭ側で行う構成としたが、これらの処理の両方、もしくは、いずれか一方、または、それらの一部を、ホストコンピュータＰＣ側で行ってもよい。例えば、ホストコンピュータＰＣのＣＰＵ７０が、図８のステップＳ７００～Ｓ７４０までの処理を行う構成としてもよいし、ＣＰＵ７０がステップＳ７００～Ｓ７２０までの処理を行い、ステップＳ７３０～Ｓ７４０の処理は、ＵＳＢフラッシュメモリが行う構成としてもよい。

【００９０】

Ｄ－４．変形例４：

実施例においては、本発明の記憶装置の実施形態として、ＵＳＢフラッシュメモリＵＭとしての構成を例示したが、本発明の記憶装置は、ＵＳＢフラッシュメモリに限るものではなく、外付けハードディスクドライブ、ＣＤドライブ、ＤＶＤドライブ、ＭＯドライブ、ブルーレイドライブ、メモリカードリーダ等、種々の記憶装置として実現することができる。

【００９１】

また、実施例においては、本発明の情報処理装置の実施形態として、パーソナルコンピュータとしての構成を例示したが、本発明の情報処理装置は、パーソナルコンピュータに限るものではなく、上述の機能をハードウェア資源により実現可能であれば、ＰＤＡ（Personal Digital Assistant）、携帯電話、各種デジタル家電など、種々の情報処理装置として実現することができる。

【００９２】

以上、本発明の実施例について説明したが、本発明はこうした実施例に限られるものではなく、本発明の要旨を脱しない範囲において、種々なる態様で実施できることは勿論である。例えば、本発明は、自動認証方法や、そのプログラム、当該プログラムを読み取り可能に記録した記憶媒体などの形態でも実現が可能である。

【図面の簡単な説明】

【００９３】

【図１】ＵＳＢフラッシュメモリＵＭの概略構成を示す説明図である。

【図２】フラッシュメモリ５０の内部領域を示す説明図である。

【図３】ホストコンピュータＰＣの概略構成を示す説明図である。

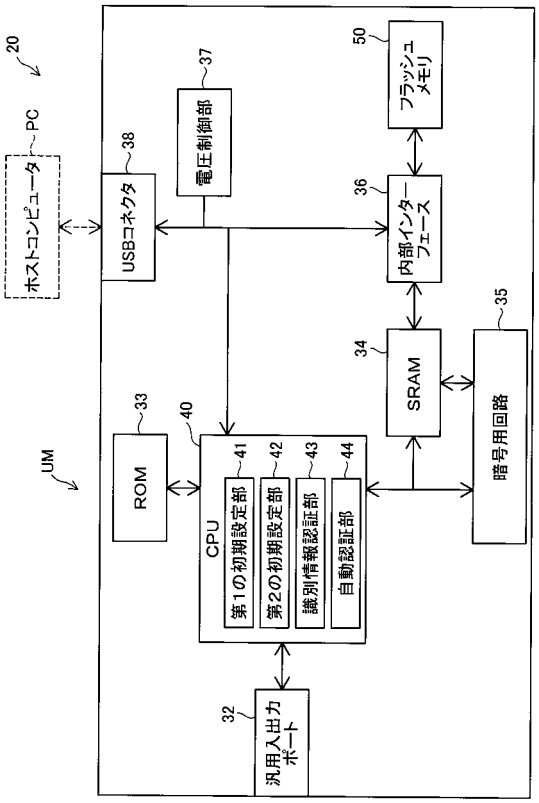
【図４】ＵＳＢフラッシュメモリＵＭのパスワード認証を行うための初期設定の手順を示すフローチャートである。

【図５】パスワード認証処理の手順を示すフローチャートである。
【図６】自動認証処理の各種設定を行う設定モードの起動手順を示すフローチャートである。
【図７】ＵＳＢフラッシュメモリＵＭの自動認証処理を行うための登録処理の手順を示すフローチャートである。
【図８】ＵＳＢフラッシュメモリＵＭの自動認証処理の手順を示すフローチャートである。
【図９】フラッシュメモリ５０の隠し領域５１の内部領域を示す説明図である。
【図１０】登録処理により登録された情報を削除する登録削除処理の手順を示すフローチャートである。

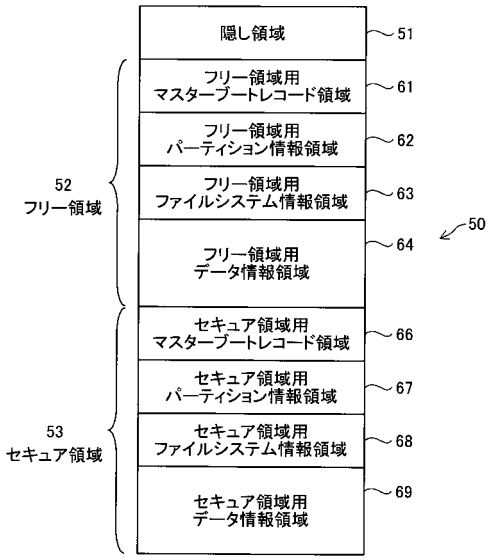
【符号の説明】
【００９４】
２０…認証システム
３２…汎用入出力ポート
３３…ＲＯＭ
３４…ＳＲＡＭ
３５…暗号用回路
３６…内部インタフェース
３７…電圧制御部
３８…ＵＳＢコネクタ
４０…ＣＰＵ
４１…第１の初期設定部
４２…第２の初期設定部
４３…識別情報認証部
４４…自動認証部
５０…フラッシュメモリ
５１…隠し領域
５２…フリー領域
５３…セキュア領域
６１…フリー領域用マスターブートレコード領域
６２…フリー領域用パーティション情報領域
６３…フリー領域用ファイルシステム情報領域
６４…フリー領域用データ情報領域
６６…セキュア領域用マスターブートレコード領域
６７…セキュア領域用パーティション情報領域
６８…セキュア領域用ファイルシステム情報領域
６９…セキュア領域用データ情報領域
７０…ＣＰＵ
７１…記憶部
７２…登録部
７４…秘密鍵提供部
７５…暗号化部
８１…ハードディスクドライブ
８２…ＲＯＭ
８３…ＲＡＭ
８４…入力機構
８５…ディスプレイ
８６…ＵＳＢインタフェース
ＭＡ…区画記憶領域
ＭＡ１～ＭＡ１０…区画エリア

ＰＣ…ホストコンピュータ
ＵＭ…ＵＳＢフラッシュメモリ

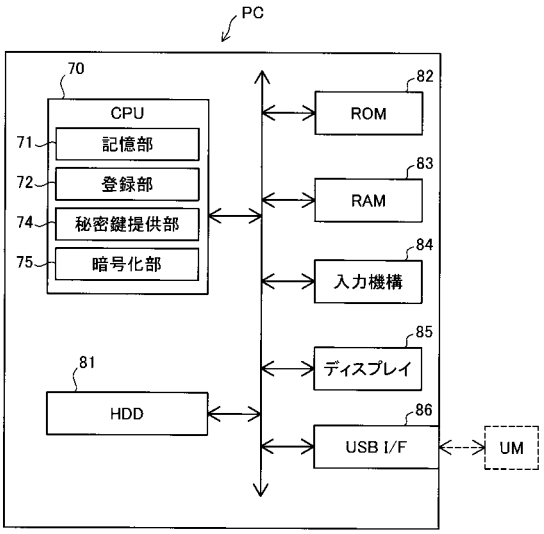
【図１】



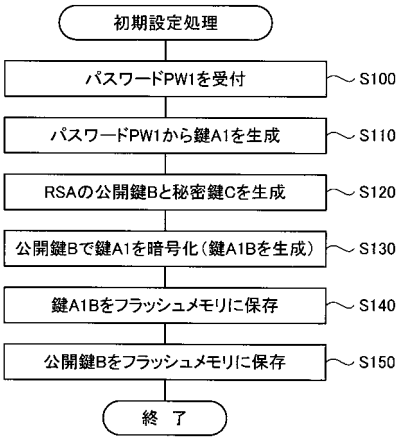
【図２】



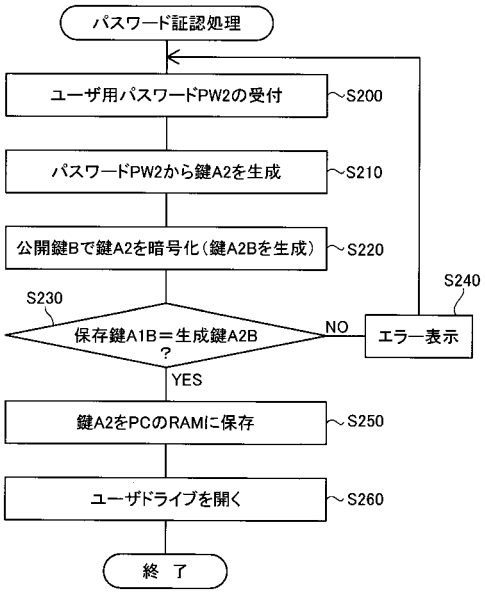
【図３】


PC
70
CPU
71
記憶部
72
登録部
74
秘密鍵提供部
75
暗号化部
81
HDD
82
ROM
83
RAM
84
入力機構
85
ディスプレイ
86
USB I/F
UM

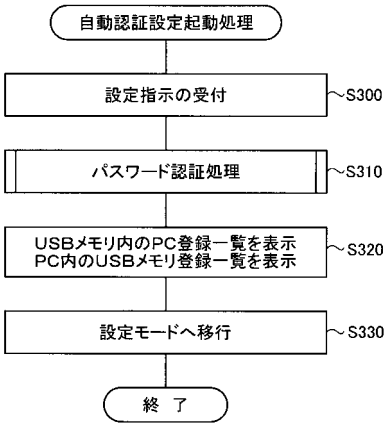
【図４】


初期設定処理
パスワードPW1を受付
S100
パスワードPW1から鍵A1を生成
S110
RSAの公開鍵Bと秘密鍵Cを生成
S120
公開鍵Bで鍵A1を暗号化（鍵A1Bを生成）
S130
鍵A1Bをフラッシュメモリに保存
S140
公開鍵Bをフラッシュメモリに保存
S150
終 了

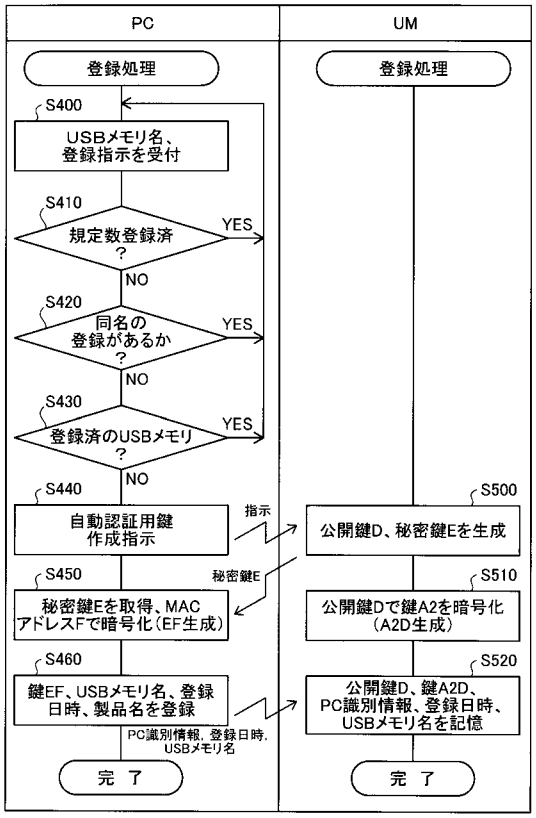
【図５】


パスワード証認処理
ユーザ用パスワードPW2の受付
S200
パスワードPW2から鍵A2を生成
S210
公開鍵Bで鍵A2を暗号化（鍵A2Bを生成）
S220
S230
保存鍵A1B＝生成鍵A2B
？
NO
S240
エラー表示
YES
鍵A2をPCのRAMに保存
S250
ユーザドライブを開く
S260
終 了

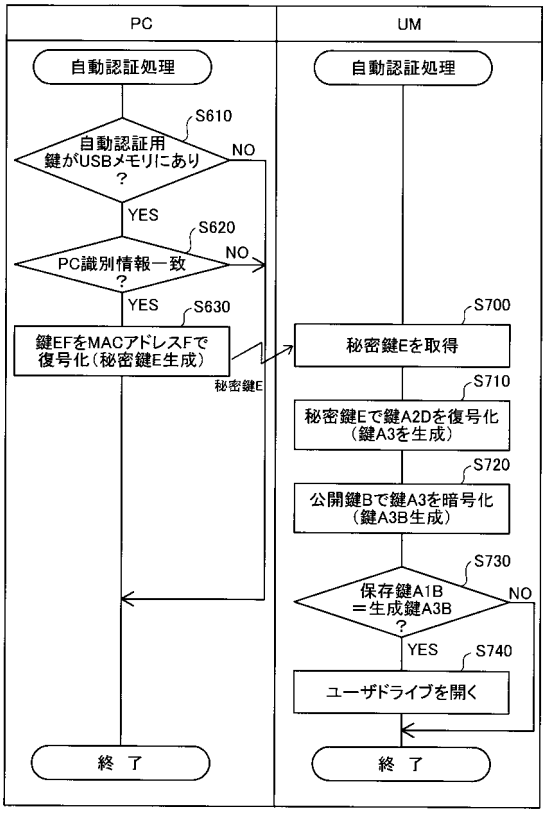
【図６】


自動認証設定起動処理
設定指示の受付
S300
パスワード認証処理
S310
USBメモリ内のPC登録一覧を表示
PC内のUSBメモリ登録一覧を表示
S320
設定モードへ移行
S330
終 了

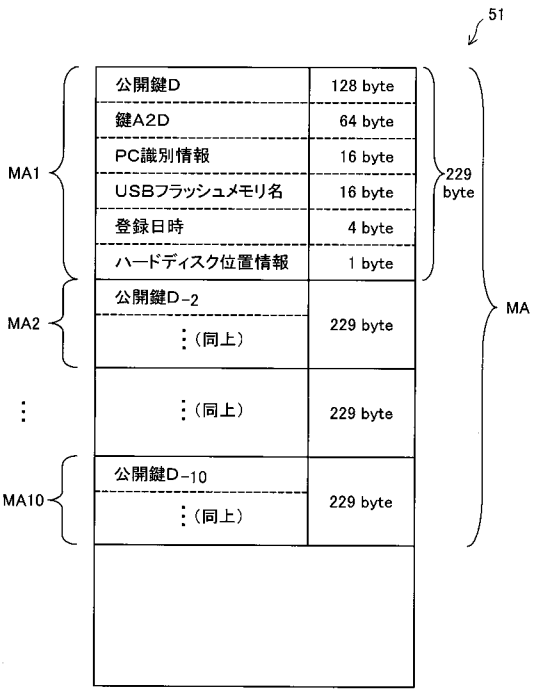
【図７】


PC
UM
登録処理
登録処理
S400
USBメモリ名、
登録指示を受付
S410
規定数登録済
？
YES
NO
S420
同名の
登録があるか
？
YES
NO
S430
登録済のUSBメモリ
？
YES
NO
S440
自動認証用鍵
作成指示
指示
S500
公開鍵D、秘密鍵Eを生成
S450
秘密鍵Eを取得、MAC
アドレスFで暗号化（EF生成）
秘密鍵E
S510
公開鍵Dで鍵A2を暗号化
（A2D生成）
S460
鍵EF、USBメモリ名、登録
日時、製品名を登録
S520
公開鍵D、鍵A2D、
PC識別情報、登録日時、
USBメモリ名を記憶
PC識別情報、登録日時、
USBメモリ名
完 了
完 了

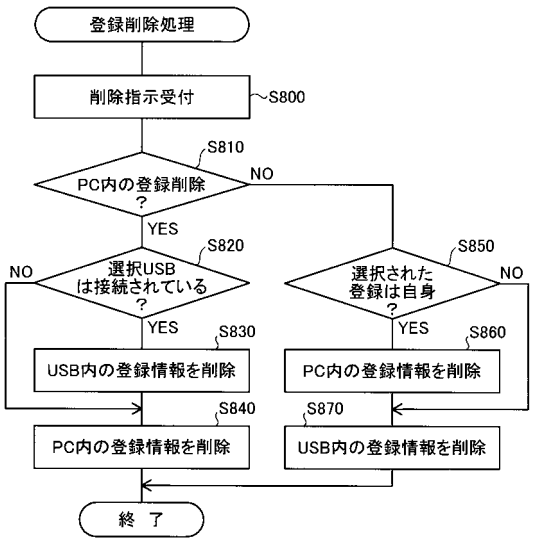
【図８】


PC
UM
自動認証処理
自動認証処理
S610
自動認証用
鍵がUSBメモリにあり
？
NO
YES
S620
PC識別情報一致
？
NO
YES
S630
鍵EFをMACアドレスFで
復号化（秘密鍵E生成）
秘密鍵E
S700
秘密鍵Eを取得
S710
秘密鍵Eで鍵A2Dを復号化
（鍵A3を生成）
S720
公開鍵Bで鍵A3を暗号化
（鍵A3B生成）
S730
保存鍵A1B
＝生成鍵A3B
？
NO
YES
S740
ユーザドライブを開く
終 了
終 了

【図９】


51
公開鍵D
128 byte
鍵A2D
64 byte
PC識別情報
16 byte
USBフラッシュメモリ名
16 byte
登録日時
4 byte
ハードディスク位置情報
1 byte
229
byte
MA1
MA2
公開鍵D-2
⋮（同上）
229 byte
⋮
⋮（同上）
229 byte
MA10
公開鍵D-10
⋮（同上）
229 byte
MA

【図１０】


登録削除処理
削除指示受付
S800
S810
PC内の登録削除
？
NO
YES
S820
選択USB
は接続されている
？
NO
YES
S830
USB内の登録情報を削除
S840
PC内の登録情報を削除
S850
選択された
登録は自身
？
NO
YES
S860
PC内の登録情報を削除
S870
USB内の登録情報を削除
終 了

フロントページの続き

(56)参考文献 特開２００９－７５６９３（ＪＰ，Ａ）
特開２００８－４０５９７（ＪＰ，Ａ）
特開２００２－３００１５５（ＪＰ，Ａ）
特開２００８－２９９６８３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０