

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4832926号
(P4832926)

(45) 発行日 平成23年12月7日(2011.12.7)

(24) 登録日 平成23年9月30日(2011.9.30)

(51) Int. Cl.		F I			
GO6K	19/07	(2006.01)	GO6K	19/00	N
GO6F	21/24	(2006.01)	GO6F	12/14	530D
HO4L	9/32	(2006.01)	GO6F	12/14	540C
			HO4L	9/00	673E

請求項の数 8 (全 15 頁)

(21) 出願番号	特願2006-67672 (P2006-67672)	(73) 特許権者	390040187
(22) 出願日	平成18年3月13日(2006.3.13)		株式会社バッファロー
(65) 公開番号	特開2007-249263 (P2007-249263A)		愛知県名古屋市中区大須三丁目30番20号
(43) 公開日	平成19年9月27日(2007.9.27)	(74) 代理人	100096703
審査請求日	平成20年9月11日(2008.9.11)		弁理士 横井 俊之
		(72) 発明者	石徹白 敬
			名古屋市南区柴田本通四丁目15番地 株式会社バッファロー内
		審査官	関 博文

最終頁に続く

(54) 【発明の名称】 持ち運び可能なデータストレージデバイスおよびデータの読み出し制御方法

(57) 【特許請求の範囲】

【請求項1】

所定の制御に基づいてデータの書き込みと読み出しとが可能な記憶手段と、
外部との接続用インターフェイスを備えるとともに上記記憶手段に対する書き込みと読み出しとを制御する制御手段と、

外部の非接触型ICチップに対する情報の読み出しを実行する非接触型ICチップリーダとを備え、

上記制御手段は、上記接続用インターフェイスを介して外部機器に接続された状態で、
同外部機器からデータの読み出しの要求を受けると、上記非接触型ICチップリーダに外部の非接触型ICチップから非接触型ICチップの固有識別番号を読み出すことを指示し

10

上記非接触型ICチップリーダは、番号のうちの一部が所定の分類基準に基づいて共通性を有し且つ番号のうち他の部分が所定の分類基準に基づいて相互に異なる特異性を有する固有識別番号を、非接触型ICチップから読み出し、

上記制御手段は、上記読み出された固有識別番号における上記共通性を有する部分を認証情報として用いて所定の認証を行うとともに、認証が完了できたときは、上記読み出された固有識別番号における上記特異性を有する部分を暗号キーとし、上記データの読み出しの要求に対しては、同暗号キーを利用して、上記記憶手段から読み出されるデータの復号化を行なうことを特徴とする持ち運び可能なデータストレージデバイス。

【請求項2】

20

上記制御手段は、

上記接続用インターフェイスと、

所定の認証情報を記憶する認証情報保持回路と、

上記非接触型ＩＣチップリーダを介して外部の非接触型ＩＣチップに対する固有識別情報の読み出しを実行させるとともに、同読み出された固有識別情報に基づく上記認証情報と、上記認証情報保持回路に記憶されている認証情報とを比較して照合を確認する認証情報比較回路と、

この認証情報比較回路にて照合が確認できたときに上記非接触型ＩＣチップから読み出された固有識別情報に基づく上記暗号キーを出力する暗号キー生成回路と、

上記暗号キーに基づいて所定のデータの暗号化を行う暗号化回路と、

上記暗号キーに基づいて所定のデータの復号化を行う復号化回路と、

上記外部機器からのデータの書き込み又はデータの読み出しの要求に対応し、上記認証情報比較回路にて照合を実行させつつ、

照合が確認されたときに上記暗号キー生成回路が出力する暗号キーに基づいて、データの書き込み時には暗号化されてない所定のデータを同暗号キーにより上記暗号化回路にて暗号化を行わせ、暗号化されたデータを上記記憶手段に記憶させ、

データの読み出し時には上記記憶手段から読み出される暗号化データを同暗号キーにより上記復号化回路にて復号化を行わせて復号化されたデータを出力するリード/ライト制御回路とを具備することを特徴とする上記請求項１に記載のデータストレージデバイス

【請求項３】

上記認証情報保持回路は、所定の状況において上記非接触型ＩＣチップリーダを介して外部の非接触型ＩＣチップに対する固有識別情報の読み出しを実行させ、同読み出された固有識別情報に基づく上記認証情報を取得して保持することを特徴とする上記請求項２に記載のデータストレージデバイス。

【請求項４】

上記認証情報保持回路は、認証情報が保持されていないときに、上記接続用インターフェイスを介して上記外部機器に接続された状況において、上記読み出された固有識別情報に基づく上記認証情報を保持することを特徴とする上記請求項３に記載のデータストレージデバイス。

【請求項５】

上記記憶手段は、フラッシュメモリで構成され、

上記接続用インターフェイスは、ＵＳＢインターフェイスで構成されることを特徴とする上記請求項１～請求項４のいずれかに記載のデータストレージデバイス。

【請求項６】

上記非接触型ＩＣチップリーダは、短距離無線通信により上記非接触型ＩＣチップから情報を読み出すことを特徴とする上記請求項１～請求項５のいずれかに記載のデータストレージデバイス。

【請求項７】

上記非接触型ＩＣチップリーダは、ＲＦＩＤにより上記非接触型ＩＣチップから情報を読み出すことを特徴とする上記請求項１～請求項５のいずれかに記載のデータストレージデバイス。

【請求項８】

持ち運び可能であるとともに、外部の非接触型ＩＣチップに対する情報の読み出しを実行する非接触型ＩＣチップリーダを有し、接続用インターフェイスを介して外部機器と接続して内部の記憶手段に対してデータの書き込みと読み出しとを実行可能なデータストレージデバイスにおけるデータの読み出し制御方法であって、

上記接続用インターフェイスを介して外部機器に接続された状態で、同外部機器からデータの読み出しの要求を受けると、上記非接触型ＩＣチップリーダに外部の非接触型ＩＣチップから非接触型ＩＣチップの固有識別番号を読み出すことを指示し、

上記非接触型ＩＣチップリーダに、番号のうちの一部が所定の分類基準に基づいて共通

10

20

30

40

50

性を有し且つ番号のうちの他の部分が所定の分類基準に基づいて相互に異なる特異性を有する固有識別番号を、非接触型ＩＣチップから読み出させ、

上記読み出された固有識別番号における上記共通性を有する部分を認証情報として用いて所定の認証を行うとともに、認証が完了できたときは、上記読み出された固有識別番号における上記特異性を有する部分を暗号キーとし、上記データの読み出しの要求に対しては、同暗号キーを利用して、上記記憶手段から読み出されるデータの復号化を行なうこと
を特徴とするデータの読み出し制御方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、持ち運び可能なデータストレージデバイスおよびデータの読み出し制御方法に関し、特に、データを暗号化して記憶するデータストレージデバイスおよびデータの読み出し制御方法に関する。

【背景技術】

【０００２】

データの手軽な移動のためには持ち運び可能なデータストレージデバイスが便利であるが、移動中に同デバイスを喪失して内部の機密情報が他人に漏れてしまう懸念がある。

従来、他人にデータが漏洩しないようにするための技術として特許文献１または２に示すものが知られている。

【特許文献１】特開平１０－２４７９０６号公報

【特許文献２】特開２００３－２２３３６７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００３】

上記特許文献１～２には以下に示すような課題があった。

特許文献１は、指紋に基づいてコンピュータ内で暗号化ファイルを作成した後、同暗号化ファイルを記憶させている。

特許文献１に示すものでは、データを復号化するためには、コンピュータ内でデータを暗号化した際の暗号化プログラムに対応する復号化プログラムが必要であり、予めこのプログラムが用意されている環境でないと復号化できない。

特許文献２は、媒体とは別途用意されるキーデータがコンピュータ内に保持されている場合、同キーデータを利用して媒体から復号化されたデータを読み出すことができる。

所定のルートで配布されるキーデータがコンピュータ内に保存されていないと復号化されず、媒体を持ち出したときにデータを正常に読み出せない。

本発明は、上記課題にかんがみてなされたもので、データの漏洩を確実に防止しつつ、煩わしい管理や操作を必要としないようにすることが可能な持ち運び可能なデータストレージデバイスおよびデータの読み出し制御方法の提供を目的とする。

【課題を解決するための手段】

【０００４】

上記目的を達成するため、所定の制御に基づいてデータの書き込みと読み出しとが可能な記憶手段と、外部との接続用インターフェイスを備えるとともに上記記憶手段に対する書き込みと読み出しとを制御する制御手段と、外部の非接触型ＩＣチップに対する情報の読み出しを実行する非接触型ＩＣチップリーダとを備え、上記制御手段は、上記接続用インターフェイスを介して外部機器に接続された状態で、同外部機器からのデータの書き込みと読み出しの要求に対し、上記非接触型ＩＣチップリーダによって外部の非接触型ＩＣチップから情報を読み出し、所定の認証を行うとともに、認証が完了できたときは、所定の暗号キーの生成を行いつつ、同暗号キーを利用して、上記記憶手段に対するデータの暗号化・復号化を行って上記データの書き込みと読み出しの要求に対応する構成としてもよい。

【０００５】

10

20

30

40

50

上記構成においては、本データストレージデバイスを外部機器に接続した状態で同外部機器の側からデータの書き込みや読み出しを行う。データの書き込みや読み出しを行う場合、上記制御手段は、上記非接触型ICチップリーダによって外部の非接触型ICチップから情報を読み出し、所定の認証を行うとともに、認証が完了できたときは、所定の暗号キーの生成を行いつつ、同暗号キーを利用して、上記記憶手段に対するデータの暗号化・復号化を行って上記データの書き込みと読み出しの要求に対応する。

【0006】

このように、データの暗号化・復号化を行う際の暗号キーは外部の非接触型ICチップから取得する。このため、書き込みや読み出しに非接触型ICチップは必要であるが、非接触であるので煩わしい管理や操作も不要である。

むしろ、このような非接触型ICチップは、個別のものである必要はないので、ユーザが既に所有しているものを利用することができる。従って、全く所有していない場合を除き、既存の非接触型ICチップを利用して簡易かつ確実なデータ保護が可能となる。

非接触型ICチップからの情報の読み出しは汎用的な手段を利用可能である。

このため、上記非接触型ICチップリーダは、短距離無線通信により上記非接触型ICチップから情報を読み出す構成としたり、上記非接触型ICチップリーダは、RFIDにより上記非接触型ICチップから情報を読み出す構成としてもよい。

【0007】

短距離無線通信は、ニアフィールドコミュニケーションに代表され、例えば、13.56MHzの電波を使い、10cm程度のごく近距離で100~400kbpsの双方向通信を行なうものが知られている。また、RF-IDは、Radio Frequency Identificationと綴られるものであり、微小な無線ICチップを利用して商品物流などの物体の識別に利用されるものである。

【0008】

また、データストレージデバイスは、所定の制御に基づいてデータの書き込みと読み出しとが可能な記憶手段と、外部との接続用インターフェイスを備えるとともに上記記憶手段に対する書き込みと読み出しとを制御する制御手段と、外部の非接触型ICチップに対する情報の読み出しを実行する非接触型ICチップリーダとを備え、上記制御手段は、上記接続用インターフェイスを介して外部機器に接続された状態で、同外部機器からデータの読み出しの要求を受けると、上記非接触型ICチップリーダに外部の非接触型ICチップから非接触型ICチップの固有識別番号を読み出すことを指示し、上記非接触型ICチップリーダは、番号のうちの一部が所定の分類基準に基づいて共通性を有し且つ番号のうち他の部分が所定の分類基準に基づいて相互に異なる特異性を有する固有識別番号を、非接触型ICチップから読み出し、上記制御手段は、上記読み出された固有識別番号における上記共通性を有する部分を認証情報として用いて所定の認証を行うとともに、認証が完了できたときは、上記読み出された固有識別番号における上記特異性を有する部分を暗号キーとし、上記データの読み出しの要求に対しては、同暗号キーを利用して、上記記憶手段から読み出されるデータの復号化を行なう。

上記制御手段の一例として、上記制御手段は、上記接続用インターフェイスと、所定の認証情報を記憶する認証情報保持回路と、上記非接触型ICチップリーダを介して外部の非接触型ICチップに対する固有識別情報の読み出しを実行させるとともに、同読み出された固有識別情報に基づく上記認証情報と、上記認証情報保持回路に記憶されている認証情報とを比較して照合を確認する認証情報比較回路と、この認証情報比較回路にて照合が確認できたときに上記非接触型ICチップから読み出された固有識別情報に基づく上記暗号キーを出力する暗号キー生成回路と、上記暗号キーに基づいて所定のデータの暗号化を行う暗号化回路と、上記暗号キーに基づいて所定のデータの復号化を行う復号化回路と、上記外部機器からのデータの書き込み又はデータの読み出しの要求に対応し、上記認証情報比較回路にて照合を実行させつつ、照合が確認されたときに上記暗号キー生成回路が出力する暗号キーに基づいて、データの書き込み時には暗号化されてない所定のデータを同暗号キーにより上記暗号化回路にて暗号化を行わせ、暗号化されたデータを上記記憶手段

10

20

30

40

50

に記憶させ、データの読み出し時には上記記憶手段から読み出される暗号化データを同暗号キーにより上記復号化回路にて復号化を行わせて復号化されたデータを出力するリード/ライト制御回路とを具備する構成としてある。

【0009】

上記構成においては、認証情報比較回路は、上記非接触型ICチップリーダを介して外部の非接触型ICチップに対する情報の読み出しを実行させた後、同読み出された情報に基づく認証情報と、認証情報保持回路に記憶されている認証情報とを比較して照合を確認し、照合が確認できたときに暗号キー生成回路は上記非接触型ICチップから読み出された情報に基づいて暗号キーを生成し、データを書き込むときは、暗号化回路が上記暗号キーに基づいて所定のデータの暗号化を行い、データを読み出すときは、復号化回路が上記暗号キーに基づいて所定のデータの復号化を行うことができる。

10

【0010】

従って、リード/ライト制御回路は、上記外部機器からのデータの書き込みと読み出しの要求があった場合に、上記認証情報比較回路にて照合を実行させつつ、照合が確認されたときに上記暗号キー生成回路にて生成される暗号キーに基づいて、データの記憶時には暗号化されていない所定のデータを同暗号キーにより上記暗号化回路にて暗号化を行わせ、暗号化されたデータを上記記憶手段に記憶させ、また、データの読み出し時には上記記憶手段から読み出される暗号化データを同暗号キーにより上記復号化回路にて復号化を行わせて復号化されたデータを出力する。

【0011】

20

記憶手段の一例として、上記記憶手段は、フラッシュメモリで構成され、上記接続用インターフェイスは、USBインターフェイスで構成してある。

上記構成においては、暗号化されたデータはフラッシュメモリに記憶され、必要に応じて同暗号化されたデータをフラッシュメモリから読み出す。

利用する情報の一例として、上記非接触型ICチップリーダが、上記非接触型ICチップから読み出す情報は同非接触型ICチップの固有識別番号である構成としてある。

上記構成においては、非接触型ICチップの固有識別番号を非接触型ICチップリーダが読み出し、同情報を利用する。

非接触型ICチップには、固有識別番号が必ず記憶されており、この情報を利用するのであれば、敢えて専用の情報を書き込む必要がなくなる。また、固有であるため、利用の仕方

30

で情報の漏洩も防げる。むろん、かかる固有識別番号を利用することを前提とすれば専用の情報を書き込む手間がなくなるのであって、かかる固有識別番号以外の情報を利用することを妨げるものではない。

かかる固有識別番号を利用する好適な一例として、上記認証情報は、上記固有識別番号の一部で構成してある。

認証情報は完全に固有とすることにも意義があるが、共通性を適用する余地を残すことにも意義がある。共通性を残すという意味では、上記固有識別番号の一部とすることで実現できる。

また、上記非接触型ICチップは、上記固有識別番号のうち一部が所定の分類基準に基づいて共通となっており、上記認証情報は、同共通となっている部分であり、上記非接触型ICチップは、上記固有識別番号のうち一部が所定の分類基準に基づいて相互に異なる特異性のあるものとなっており、上記暗号キーは、同特異性のある部分で構成してある。

40

【0012】

より具体的には、固有識別番号のうち一部が所定の分類基準に基づいて共通となっている場合に、認証情報は、同共通となっている部分を利用する。例えば、非接触型ICチップがある会社の社員に配布されているとし、社員は、所属部署や身分によってクラス分けされているとする。認証情報を所属部署ごとに共通する部分の情報とすれば、同所属部署に属するものであれば同僚のストレージデバイスについては認証までは確認できることになる。その反対に、所属部署が異なれば認証すら実現できない。会社内でストレージデバ

50

イスを喪失した場合、所属部署までは特定できることになり、遺失者の特定に便利となる。

【 0 0 1 3 】

この場合、上記暗号キーは、上記固有識別番号の特異性のある一部で構成してあるから、所属部署が共通であるとしても、各個人ごとに異なる暗号キーで暗号化されることになり、認証は実現できてもデータを復号化して読み出すことは妨げられる。

なお、暗号キーが利用される前提として認証も行われるため、暗号キーは認証情報と組み合わせると特異性が実現できればよい。

認証情報を保持する手法は様々であり、上記認証情報保持回路は、所定の状況において上記非接触型ＩＣチップリーダを介して外部の非接触型ＩＣチップに対する情報の読み出しを実行させ、同読み出された情報に基づく認証情報を取得して保持する構成としてある。

10

【 0 0 1 4 】

上記構成においては、所定の状況において上記認証情報保持回路が上記非接触型ＩＣチップリーダを介して外部の非接触型ＩＣチップに対する情報の読み出しを実行させ、同読み出された情報に基づく認証情報を取得して保持する。

【 0 0 1 5 】

このようにすれば、外部の非接触型ＩＣチップの情報を読み出して認証情報として保持するため、ユーザーが所有している非接触型ＩＣチップを用意してその情報を認証情報として利用できることになる。

20

また、上記認証情報保持回路は、認証情報が保持されていないときに、上記接続用インターフェイスを介して上記外部機器に接続された状況において、上記読み出された情報に基づく認証情報を保持する構成としてある。

認証情報を取り込むタイミングを専用のユーティリティなどで指示することも可能であるが、上記構成においては、認証情報が保持されておらず、かつ、上記接続用インターフェイスを介して上記外部機器に接続されたとき、上記認証情報保持回路は、外部の非接触型ＩＣチップの情報を読み出して認証情報を保持する。

【 0 0 1 6 】

従って、ユーザはまだ認証情報が記憶されていないストレージデバイスを外部機器に初めて接続した時点で外部の非接触型ＩＣチップを近づけさえすればその情報を認証情報と指定後使用できるようになる。

30

このように、非接触型ＩＣチップを利用してセキュリティを確保する手法は必ずしも実体のある装置に限られる必要はなく、その方法としても機能することは容易に理解できる。このため、持ち運び可能であるとともに、外部の非接触型ＩＣチップに対する情報の読み出しを実行する非接触型ＩＣチップリーダを有し、接続用インターフェイスを介して外部機器と接続して内部の記憶手段に対してデータの書き込みと読み出しとを実行可能なデータストレージデバイスにおけるデータの読み出し制御方法であって、上記接続用インターフェイスを介して外部機器に接続された状態で、同外部機器からデータの読み出しの要求を受けると、上記非接触型ＩＣチップリーダに外部の非接触型ＩＣチップから非接触型ＩＣチップの固有識別番号を読み出すことを指示し、上記非接触型ＩＣチップリーダに、番号のうちの一部が所定の分類基準に基づいて共通性を有し且つ番号のうちの他の部分が所定の分類基準に基づいて相互に異なる特異性を有する固有識別番号を、非接触型ＩＣチップから読み出させ、上記読み出された固有識別番号における上記共通性を有する部分を認証情報として用いて所定の認証を行うとともに、認証が完了できたときは、上記読み出された固有識別番号における上記特異性を有する部分を暗号キーとし、上記データの読み出しの要求に対しては、同暗号キーを利用して、上記記憶手段から読み出されるデータの復号化を行なう構成としてある。

40

【 0 0 1 7 】

すなわち、必ずしも実体のある装置に限らず、その方法としても有効であることに相違はない。

50

ところで、このようなストレージデバイスは単独で存在する場合もあるし、ある機器に組み込まれた状態で利用されることもあるなど、発明の思想としてはこれに限らず、各種の態様を含むものである。従って、ソフトウェアであったりハードウェアであったりするなど、適宜、変更可能である。

【 0 0 1 8 】

発明の思想の具現化例としてストレージデバイスのソフトウェアとなる場合には、かかるソフトウェアを記憶した記憶媒体上においても当然に存在し、利用されるといわざるをえない。

むろん、その記憶媒体は、磁気記憶媒体であってもよいし光磁気記憶媒体であってもよいし、今後開発されるいかなる記憶媒体においても全く同様に考えることができる。また、一次複製品、二次複製品などの複製段階については全く問う余地無く同等である。その他、供給方法として通信回線を利用して行なう場合でも本発明が利用されていることにはかわりない。

【 0 0 1 9 】

さらに、一部がソフトウェアであって、一部がハードウェアで実現されている場合においても発明の思想において全く異なるものではなく、一部を記憶媒体上に記憶しておいて必要に応じて適宜読み込まれるような形態のものとしてあってもよい。

本発明をソフトウェアで実現する場合、ハードウェアやオペレーティングシステムを利用する構成とすることも可能であるし、これらと切り離して実現することもできる。例えば、各種の演算処理といっても、その実現方法はオペレーティングシステムにおける所定の関数を呼び出して処理することも可能であれば、このような関数を呼び出すことなくハードウェアから入力することも可能である。そして、実際にはオペレーティングシステムの介在のもとで実現するとしても、プログラムが媒体に記憶されて流通される過程においては、このプログラムだけで本発明を実施できるものと理解することができる。

【 0 0 2 0 】

また、本発明をソフトウェアで実施する場合、発明がプログラムを記憶した媒体として実現されるのみならず、本発明がプログラム自体として実現されるのは当然であり、プログラム自体も本発明に含まれる。

【 発明の効果 】

【 0 0 2 1 】

以上説明したように本発明は、認証と暗号キーを利用するも、そのような情報は外部の非接触型 IC チップから非接触で取得することで、煩わしい管理や操作を不要としつつ、データの漏洩を確実に防止することが可能なデータストレージデバイスを提供することができる。

【 0 0 2 2 】

また、本発明によれば、USB インターフェイスで接続されるフラッシュメモリとして実現され、かつ、その際に外部機器の側では暗号化復号化のためのプログラムも不要であるため、広範囲に利用することが可能となる。

さらに、本発明によれば、非接触型 IC チップが必ず保持している固有識別番号を利用するので、かかるセキュリティ目的のために特別な情報を書き込むことが不要となり、利用するための準備等がなくなって使いやすくなる。

さらに、本発明によれば、認証情報に共通性を残し、グループ管理などを実現しつつも、セキュリティを確保することができ、管理の仕方により一層利便性が向上する。

さらに、本発明によれば、傍に置いた非接触型 IC チップから認証情報を取得するので、ユーザが鍵として利用したい非接触型 IC チップを選択でき、極めて便利である。

【 0 0 2 3 】

さらに、本発明によれば、例えば初めて利用する時点で非接触型 IC チップを傍に置いておきさえすれば特別な操作は一切不要となり、利便性がよい。

さらに、本発明によれば、既存の技術である短距離無線通信を利用することにより、ス

10

20

30

40

50

ストレージデバイスを利用するにあたって遠すぎない範囲の非接触型ＩＣチップだけを対象とさせ、周囲で並行して利用することを妨げず、ぴったりと接続させなければいけないといった厳格な位置管理までは必要としないので、利便性も保持することが可能となる。

【 0 0 2 4 】

さらに、本発明によれば、商品タグとして利用されることが期待される無線ＩＣチップを利用することにより、商品として購入される殆ど全てのものが備えていることになり、各ユーザが指定する全てのものをいわゆる鍵として利用でき、特別なものを一切不要とすることができる。

【 0 0 2 5 】

さらに、本発明によれば、同様の効果を奏するデータの読み出し制御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 】

【 0 0 2 6 】

以下、図面にもとづいて本発明の実施形態を説明する。

図 1 は、本発明の一実施形態にかかるデータストレージデバイスをブロック図により示している。

同図において、ストレージデバイス 1 0 は、いわゆる持ち運び可能な USB フラッシュメモリであり、USB コネクタ 1 1 を介して外部機器であるホスト（パーソナルコンピュータ）5 0 に接続される。非接触型ＩＣチップ 6 0 は短距離無線通信（ニアフィールドコミュニケーション：NFC）技術を利用して非接触で所定の情報を伝達する非接触ＩＣカードである。

【 0 0 2 7 】

なお、本実施例では、短距離無線通信を利用する非接触ＩＣカードを使用しているが、RFIDの技術を利用した非接触ＩＣカードを利用しても良い。むしろ、これらはカード形状であることが必須であるわけではない。

ストレージデバイス 1 0 は、その内部に、制御部（制御手段に相当する）2 0 と、メモリ 3 0 と、非接触型ＩＣチップリーダ 4 0 とを備えている。メモリ（記憶手段に相当する）3 0 は、不揮発性のフラッシュメモリであり、所定容量を有し、アドレスバスとデータバスとで指定される記憶エリアに対してデータの書き込みと読み出しが可能である。非接触型ＩＣチップリーダ 4 0 はNFCの規格に基づいて近傍に位置する非接触型ＩＣチップ 6 0 と交信し、同チップ 6 0 内に書き込まれているデータを読み出す。本実施例においては、読み出し機能だけが必要であるため、書き込み機能であるライタの機能は備えていないが、データを書き出す機能を備えたものであっても構わない。読み出す情報は特に限られるものではないが、本実施例では後述するように当該非接触型ＩＣチップ 6 0 の固有識別番号（ID）を利用するため、同固有識別番号は少なくとも取得可能となっている。

【 0 0 2 8 】

制御部 2 0 内には、リード/ライト制御回路 2 1 と、暗号化回路 2 2 と、復号化回路 2 3 と、暗号キー生成回路 2 4 と、認証情報比較回路 2 5 と、認証情報保持回路 2 6 とを備えている。

暗号化回路 2 2 は、リード/ライト制御回路 2 1 から指示される所定の暗号キーを利用してデータを暗号化する。また、復号化回路 2 3 は同じリード/ライト制御回路 2 1 から指示される暗号キーを利用して暗号化されているデータを復号する。リード/ライト制御回路 2 1 は、暗号キー生成回路 2 4 から入力される暗号キーを暗号化回路 2 2 と復号化回路 2 3 に指示するが、暗号時の暗号キーと復号時の暗号キーが一致するか否かを判断する必要はない。復号化回路 2 3 においては、暗号時の暗号キーと復号時の暗号キーが一致すれば暗号化する前のデータを復元できるのであり、一致しない場合は本来のデータに復元できないだけのこととなる。暗号化回路 2 2 も復号化回路 2 3 もそれぞれ暗号キーは暗号化作業および復号化作業中のみ保持し、作業終了後にクリアするようにしている。内部に不必要に保持されるとデータ漏洩の可能性が増すからである。なお、本実施例では、後述するIDの一部を認証情報とし、他の一部を暗号キーとして使用しているが、暗号キーに

10

20

30

40

50

認証情報をそのまま使用することも可能であり、その場合は暗号キー生成回路を省略することもできる。

【0029】

メモリ30には暗号化されたデータが記憶されるが、暗号化の有無でデータの質が変化するものではなく、メモリ30は暗号化の有無にかかわらず所定のビット長のデータを指示されたアドレスに書き込み、または読み出すことになる。なお、本実施例ではフラッシュメモリを利用するものとなっているが、暗号化・復号化をしてデータのセキュリティを図るためのデータストレージデバイスであればよいので、記憶部分とコントローラ部分とが存在する他の記憶デバイス、例えば、ハードディスク、SDメモリなども利用可能である。

10

【0030】

リード/ライト制御回路21は、USBコネクタ11を介してホスト50と制御コマンドとデータの送受信を行う。この意味で、リード/ライト制御回路21はUSBコネクタ11を含めて接続用インターフェイスを構成する。むろん、この接続用インターフェイスはUSBインターフェイスである。ホスト50がリード/ライト制御回路21に対してデータの書き込みや読み出しを指示すると、リード/ライト制御回路21は認証情報比較回路25に対して認証の実行を指示する。

【0031】

認証情報比較回路25は認証の要求があると、非接触型ICチップリーダ40に対して近傍にある非接触型ICチップ60から固有識別番号を読み取るように指示を出す。すると、非接触型ICチップリーダ40は規格に則ったプロトコルに従って近傍にある非接触型ICチップ60への交信を試みる。かかる交信は現実にはその前から実施しているとしても同様である。そして、近傍の非接触型ICチップ60と交信可能となっていれば、同チップ60に対して固有識別番号を求め、取得する。非接触型ICチップリーダ40は固有識別番号をそのまま認証情報比較回路25に出力するが、認証情報比較回路25はその一部を認証情報として認識する。

20

【0032】

次に、認証情報比較回路25は認証情報保持回路26に対して保持している認証情報を求める。認証情報保持回路26は後述するようにして予め認証情報を保持しており、認証情報比較回路25に対して出力する。

30

認証情報比較回路25は、非接触型ICチップリーダ40から得られた固有識別番号の一部である認証情報と、認証情報保持回路26から得られた認証情報とを比較し、一致していれば認証完了と判断する。認証を完了したら認証情報比較回路25は、非接触型ICチップリーダ40から得られた固有識別番号を暗号キー生成回路24に出力し、暗号キー生成回路24は同暗号キーをリード/ライト制御回路21に出力する。

【0033】

ここで、認証情報比較回路25にて認証が完了しなかった場合、認証が完了しなかった判断を暗号キー生成回路24を介してリード/ライト制御回路21に出力するか否かはどちらの対応も可能である。

認証が完了しなかった場合、固有識別番号は出力されず、暗号キー生成回路24は暗号キーを生成できない。暗号キー生成回路24は認証情報比較回路25から固有識別番号が与えられたらそれに基づく暗号キーを生成するが、暗号キーを出力したら、すぐに内部の記憶エリアをクリアする。そして、次に固有識別番号が与えられない限り、新たな暗号キーも従前の暗号キーも出力できない。

40

【0034】

従って、認証が完了しなければ、暗号キー生成回路24は本来の暗号キーを生成できないし、その状態ではリード/ライト制御回路21は暗号キーが生成されないことに基づいて認証が完了しなかったものと判断できる。この結果、それ以降のホスト50からのデータの読み出しおよび書き込みの制御を拒否する。

【0035】

50

これに対して、認証が完了した場合は、固有識別番号が出力されて暗号キー生成回路 2 4 が正しい暗号キーを生成するのでリード/ライト制御回路 2 1 を介して同暗号キーを取得する暗号化回路 2 2 や復号化回路 2 3 はセキュリティを確保したデータの読み出しや書き込みが可能となる。

【 0 0 3 6 】

なお、後述するように認証情報をグループ管理することで認証だけは完了させることができるものの、正しい暗号キーを生成できないという状況を作り出すこともできる。この場合は、単に認証までは完了するものの正しい非接触型 IC チップ 6 0 でないので固有識別番号が異なっており、暗号キー生成回路 2 4 にて本来とは異なる暗号キーが生成され、リード/ライト制御回路 2 1 を介して暗号化回路 2 2 や復号化回路 2 3 に誤った暗号キーが出力される。データの読み出し自体はそのまま行うこととすれば正しくない暗号キーで復号化されたデータを読み出しても全く利用価値がない。データの書き込み自体は暗号化して行われるが、自分のものでないデータストレージに対してデータを書き込むこと自体が無意味である。従って、いずれにしても問題は生じない。

【 0 0 3 7 】

グループ管理は、非接触型 IC チップ 6 0 の固有識別番号の全部または一部を所定の分類基準に則って設定することにより行える。例えば、非接触型 IC チップ 6 0 が会社における身分証明書として利用する場合、ある部分の 5 桁を所属部署を表すものとして共通性をもたせ、別の 5 桁を各部署内で相互に異なるようにして各個人に割り当てる。このような分類基準を適用すれば、共通性のある 5 桁を認証情報に割り当て、特異性のある 5 桁を暗号キーに割り当てることで、部署が共通する社員の間では本データストレージデバイスの認証までは確認できるようにすることができる。ただし、各個人ごとに暗号キーの 5 桁には特性があるのでデータの読み出し等は行えない。

【 0 0 3 8 】

認証情報保持回路 2 6 が保持する認証情報は、最初に認証情報比較回路 2 5 から認証情報を求められた時点で、非接触型 IC チップリーダ 4 0 から読み取られた固有識別番号の一部を認証情報として記憶する。このようにすれば、ユーザは初めて使用するときに鍵として使用したい非接触型 IC チップ 6 0 を用意しておくだけで以後の使用において同非接触型 IC チップ 6 0 を認証情報および暗号キーの生成用の鍵のように利用できる。むしろ、他の手法で認証情報を書き込むようにしても良い。例えば、ホスト 5 0 に認証情報書き換え用のユーティリティプログラムをロードし、リード/ライト制御回路 2 1 を介して書き込むようにすることも可能である。かかるデータの書き込み時の制御が書き込み制御方法であり、同データの読み出し時の制御が読み出し制御方法となる。

【 0 0 3 9 】

次に、上記構成からなる本実施形態の動作を説明する。

図 2 は認証情報保持回路 2 6 が認証情報を保持していない時点での動作を示すフローチャートである。同図に示すように、ステップ S 1 0 2 にて認証情報保持回路 2 6 に認証情報がないと判断されるときには、ステップ S 1 0 4 にて非接触型 IC チップリーダ 4 0 から非接触型 IC チップ 6 0 の固有識別番号（以下、ID と呼ぶ）を読み取り、ステップ S 1 0 6 にて読み取った ID の一部を認証情報として認証情報保持回路 2 6 に書き込む。

【 0 0 4 0 】

図 3 は認証情報が認証情報保持回路 2 6 に保持されている状態でのデータの読み書き時の動作を示すフローチャートである。

ホスト 5 0 からデータの書き込みあるいは読み出しの要求があると、ステップ S 1 1 0 では非接触型 IC チップリーダ 4 0 にて近傍に位置する非接触型 IC チップ 6 0 から ID を読み出す処理を行う。すなわち、リード/ライト制御回路 2 1 がホスト 5 0 からの制御コマンドを受け、認証情報比較回路 2 5 に対して認証の実行を指示する。すると、同認証情報比較回路 2 5 は、非接触型 IC チップリーダ 4 0 に対して近傍にある非接触型 IC チップ 6 0 から ID を読み取るように指示を出し、非接触型 IC チップリーダ 4 0 は規格に則った プロトコル に従って近傍にある非接触型 IC チップ 6 0 への交信を試みる。近傍の

非接触型 IC チップ 60 と交信可能となっていれば、非接触型 IC チップリーダ 40 は同チップ 60 に対して ID を求め、得られた ID をそのまま認証情報比較回路 25 に出力し、認証情報比較回路 25 はその一部を認証情報として認識する。

【 0041 】

ステップ S 112 では、認証情報比較回路 25 が、非接触型 IC チップリーダ 40 から得られた ID の一部である認証情報と、認証情報保持回路 26 が保持する認証情報とを比較する。ステップ S 114 では、比較結果が一致したとき、すなわち認証が完了した場合にステップ S 116 に進み、ホスト 50 からの制御コマンドがデータライト（書き込み）であれば、ステップ S 118 にて ID の一部を暗号キーとしてホスト 50 から制御コマンドに続いて送り出されるデータを暗号化してメモリ 30 に書き込むし、ホスト 50 からの制御コマンドがデータリード（読み出し）であれば、ステップ S 120 にて上記 ID の一部を暗号キーとしてホスト 50 からの制御コマンドに対応するデータをメモリ 30 から読み出しつつ復号化してホスト 50 に送り出す。むろん、この際のデータの書き込みおよび読み出しのアドレスは別途規定の処理に基づいて特定されている。

10

【 0042 】

より具体的には、書き込み時は、上記非接触型 IC チップリーダ 40 から得られた ID を暗号キー生成回路 24 に出力し、暗号キー生成回路 24 は ID の一部を暗号キーとしてリード/ライト制御回路 21 に出力する。リード/ライト制御回路 21 は同暗号キーを暗号化回路 22 に出力した後、ホスト 50 から送られてくるデータを暗号化回路 22 に出力し、同暗号化回路 22 が上記暗号キーに基づいて暗号化するとともに、メモリ 30 に出力し、順次書き込んでいく。また、読み出し時は上記非接触型 IC チップリーダ 40 から得られた ID に基づいて暗号キー生成回路 24 がリード/ライト制御回路 21 に出力する暗号キーを復号化回路 23 に出力し、同復号化回路 23 はメモリ 30 から順次読み出されるデータを復号化して出力し、同復号化されたデータがリード/ライト制御回路 21 を介してホスト 50 に出力されていく。

20

【 0043 】

ここで、もし、不正にデータストレージを入手したものが自分のパーソナルコンピュータに接続して読み出しを試みようとした場合、本来の非接触型 IC チップがない限り認証が完了しない。すなわち、ステップ S 114 では認証情報が不一致と判断され、ステップ S 122 にてエラーリードライト不可となって処理を終了することになる。

30

【 0044 】

図 4 ~ 図 6 はほぼ同様の目的を実現するための別の実施例を示している。

図 4 は概略の動作を示しており、ステップ S 202 にてデータストレージ（デバイス）をホスト 50 の USB コネクタに挿入すると、ステップ S 204 にて認証情報保持回路の認証情報の有無に基づき、認証情報有りと判断されるとステップ S 206 に進んで通常動作を実行するし、認証情報無しと判断されるとステップ S 208 に進む。

【 0045 】

認証情報が無い場合の動作として、この実施例では三つの対応を示しており、1) 通常の暗号化や復号化ができない USB フラッシュデバイスとして動作させるか、2) 全く動作させないか、3) 認証情報の自動登録画面をホスト 50 に起動させるかの対応を可能としている。暗号化は復号化ができない USB フラッシュデバイスとしての動作を実現するには、暗号キーを与えずに暗号化や復号化を行わせると全く暗号化や復号化をしないように暗号化回路 22 や復号化回路 23 を構成することで実現可能である。全く動作させない処理は認証情報が無いときにリード/ライト制御回路 21 がそれ以降の処理を実施しないようにして実現可能である。認証情報の自動登録画面をホスト 50 に起動させる場合は、予めホスト 50 で実行するためのプログラムをデータストレージ内に記憶しておき、ホスト 50 にロードさせて実行させることで実現可能である。

40

【 0046 】

図 5 は通常動作のうち、データ書き込み時のデータの流れと処理を示している。同図において、ホスト 50 がステップ S 212 にてデータ書き込みを要求する。同要求に基づき

50

、ステップS 2 1 4にて制御部2 0はID取得要求を行う。同要求に基づき、ステップS 2 1 6にて非接触型ICチップリーダ4 0は近傍の非接触型ICチップ6 0からIDを取得する。ステップS 2 1 8では制御部2 0が上記取得されたIDの一部を認証情報とし、認証情報保持回路の認証情報と照合する。照合ができなかった(NG)場合はステップS 2 2 0にてエラーを通知する。この実施例では、アクセスキー(認証情報)が不正であることを表示して動作しない対応と、データ領域に対するアクセスを拒否する対応との二種類のいずれかを実施可能としている。

【0 0 4 7】

一方、認証が完了した(OK)場合は、ホスト5 0はステップS 2 2 2にて非暗号化データを順次書き出し、制御部2 0ではステップS 2 2 4にて暗号化回路2 2が上記IDの一部を暗号キーとして使用してデータの暗号化を行い、ステップS 2 2 6にてメモリ3 0に暗号化されたデータが書き込まれていく。

10

【0 0 4 8】

次に、図6は通常動作のうち、データ読み出し時のデータの流れと処理を示している。同図において、ホスト5 0がステップS 2 3 2にてデータ読み出しを要求する。同要求に基づき、ステップS 2 3 4にて制御部2 0はID取得要求を行う。同要求に基づき、ステップS 2 3 6にて非接触型ICチップリーダ4 0は近傍の非接触型ICチップ6 0からIDを取得する。ステップS 2 3 8では制御部2 0が上記取得されたIDの一部を認証情報とし、認証情報保持回路の認証情報と照合する。照合ができなかった(NG)場合はステップS 2 4 0にてエラーを通知する。この実施例では、アクセスキー(認証情報)が不正であることを表示してデータアクセスを拒否するなどの対応と、暗号化データの復号化をしない対応との二種類のいずれかを実施可能としている。

20

【0 0 4 9】

一方、認証が完了した(OK)場合は、メモリ3 0はステップS 2 4 2にて暗号化されているデータを読み出し、制御部2 0ではステップS 2 4 4にて復号化回路2 3が上記IDの一部を暗号キーとして使用してデータの復号化を行い、ホスト5 0にはステップS 2 4 6にて復号化されたデータが読み出されていくことになる。

【0 0 5 0】

このように、データの書き込み時や読み出し時に非接触型ICチップリーダ4 0を介して鍵となる非接触型ICチップ6 0から固有識別番号を読み出し、同固有識別番号に基づいて認証情報比較回路2 5にて認証を行いつつ、認証が完了した場合には暗号化回路2 2にて暗号化、復号化回路2 3にて復号化を行い、ホスト5 0から書き込まれる暗号化されていないデータを暗号化しつつメモリ3 0に書き込むとともに、同暗号化されたデータをメモリ3 0から読み出して復号化してからホスト5 0に出力する。

30

【図面の簡単な説明】

【0 0 5 1】

【図1】本発明の一実施形態にかかるデータストレージの概略構成を示すブロック図である。

【図2】第一の実施例にかかるデータストレージデバイスにおける認証情報を認証情報保持回路に保持させる際のフローチャートである。

40

【図3】第一の実施例にかかるデータストレージデバイスにおけるデータの書き込みと読み出し時のフローチャートである。

【図4】第二の実施例にかかるデータストレージデバイスにおける動作の全体的なフローチャートである。

【図5】第二の実施例にかかるデータストレージデバイスにおけるデータの書き込み時のフローチャートである。

【図6】第二の実施例にかかるデータストレージデバイスにおけるデータの読み出し時のフローチャートである。

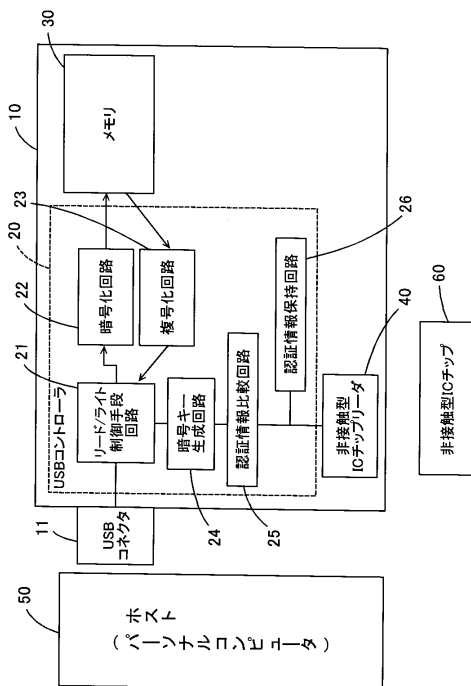
【符号の説明】

【0 0 5 2】

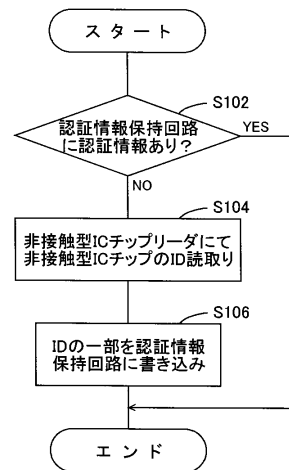
50

- 10 ... データストレージデバイス
- 20 ... 制御部
- 30 ... メモリ
- 40 ... 非接触型 IC チップリーダ
- 50 ... ホスト
- 60 ... 非接触型 IC チップ

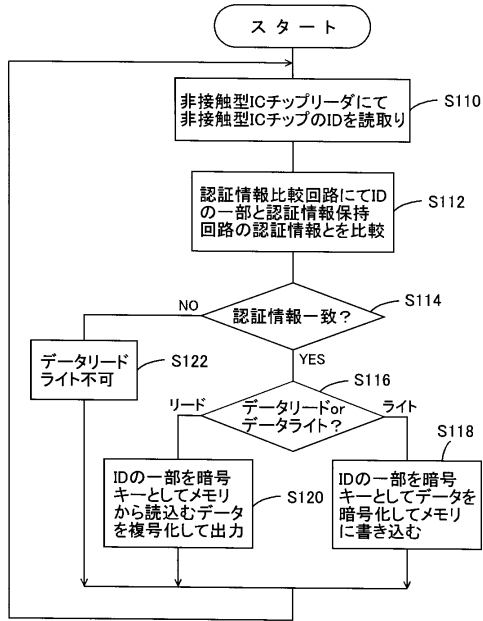
【図 1】



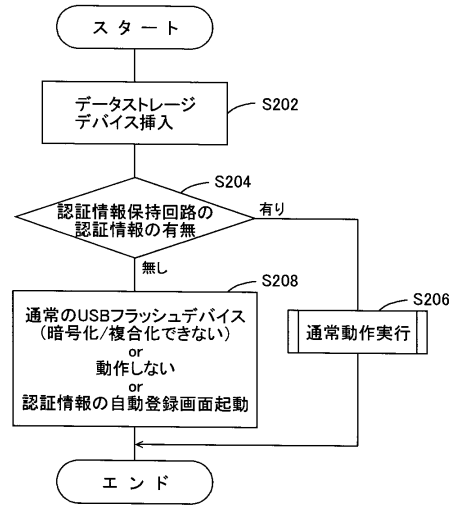
【図 2】



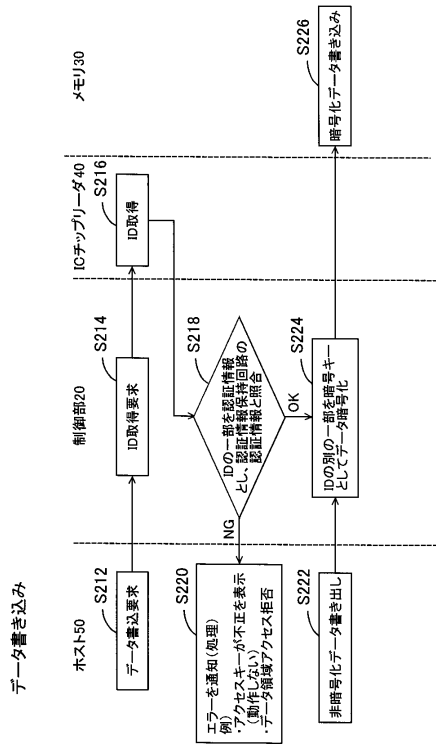
【図3】



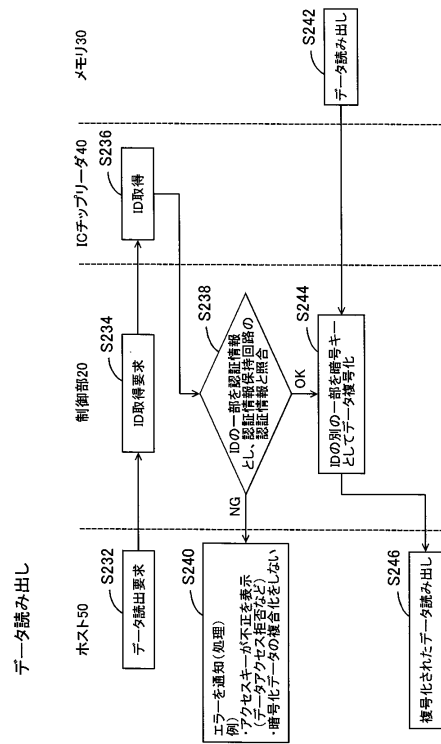
【図4】



【図5】



【図6】



フロントページの続き

(56)参考文献 特開2005-346263(JP,A)
特開2002-288372(JP,A)
特開2005-276025(JP,A)
特開2006-293943(JP,A)
特開2004-110382(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06K 19/07
G06F 21/24
H04L 9/32