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

特許第6029592号
(P6029592)

(45)発行日　平成28年11月24日(2016.11.24)　(24)登録日　平成28年10月28日(2016.10.28)

(51)Int.Cl.		F I	
G06F 21/62	(2013.01)	G06F	21/62
G06F 21/79	(2013.01)	G06F	21/79
G06K 17/00	(2006.01)	G06K	17/00
G06K 19/073	(2006.01)	G06K	19/073
G06K 19/10	(2006.01)	G06K	19/10

請求項の数 7　(全 10 頁)

(21)出願番号	特願2013-544158(P2013-544158)
(86)(22)出願日	平成24年9月3日(2012.9.3)
(86)国際出願番号	PCT/JP2012/072303
(87)国際公開番号	WO2013/073260
(87)国際公開日	平成25年5月23日(2013.5.23)
審査請求日	平成26年1月7日(2014.1.7)
審判番号	不服2015-16372(P2015-16372/J1)
審判請求日	平成27年9月4日(2015.9.4)
(31)優先権主張番号	特願2011-253368(P2011-253368)
(32)優先日	平成23年11月19日(2011.11.19)
(33)優先権主張国	日本国(JP)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
New Orchard Road, Armonk, New York 10504, United States of America
(74)代理人　100108501
弁理士　上野　剛史

最終頁に続く

(54)【発明の名称】記憶装置

(57)【特許請求の範囲】

【請求項１】

コンピュータに接続されると起動して通信可能となる記憶装置であって、

前記コンピュータとの通信を制御するインターフェイスと、

前記インターフェイスを介して前記コンピュータから受信したデータを保管するデータ記憶部と、

ＩＤ情報を含む無線信号を所定のタイミング毎に受信し、受信したＩＤ情報を認証する無線信号処理部と、

認証されたＩＤ情報をキーとして前記データを暗号化し、当該暗号化したデータを前記データ記憶部に送り、さらに、前記無線信号処理部が、最後に前記認証が成功した前記無線信号の受信の時から所定時間内において前記所定のタイミング毎に受信した前記無線信号の全ての前記認証に失敗した場合、前記インターフェイスにおける前記コンピュータとの通信を不能にする制御部と、を備える記憶装置。

【請求項２】

前記制御部は、前記無線信号処理部が前記所定時間内において前記所定のタイミング毎に受信した前記無線信号の少なくとも１つの前記認証に成功した場合に、前記コンピュータからデータ読み出し要求があった場合、当該読み出し要求に対応する暗号化されたデータを前記データ記憶部から読み出して、当該暗号化されたデータを前記認証されたＩＤ情報をキーとして復号化して、当該復号されたデータを前記インターフェイスを介して前記コンピュータに送る、請求項１の記憶装置。

【請求項３】
前記ＩＤ情報を保管するためのＩＤ情報記憶部と、
前記ＩＤ情報の認証スイッチと、を更に備え、
前記制御部は、前記認証スイッチがオンになっている場合に、前記無線信号処理部に対して受信したＩＤ情報を登録ＩＤ情報として前記ＩＤ情報記憶部に保管することを指示する、請求項１の記憶装置。
【請求項４】
前記無線信号処理部は、前記認証スイッチがオンになっている場合を除いて、受信したＩＤ情報が前記ＩＤ情報記憶部に保管されている登録ＩＤ情報に一致するか否かを判定することにより前記認証をおこなう、請求項３の記憶装置。
【請求項５】
前記ＩＤ情報には、当該ＩＤ情報を担持する媒体固有の第１のＩＤ番号と、当該第１のＩＤ番号に付随する第２のＩＤ番号とが含まれ、
前記制御部は、認証されたＩＤ情報中の前記第１のＩＤ番号および前記第２のＩＤ番号のいずれか一方あるいは双方を前記キーとして用いる、請求項１または２の記憶装置。
【請求項６】
前記無線信号処理部はＲＦＩＤのリーダ／ライタ（Ｒ／Ｗ）を含み、
前記ＩＤ情報は、前記Ｒ／Ｗと通信可能なＲＦＩＤタグとして前記媒体に担持される、請求項５の記憶装置。
【請求項７】
前記インターフェイスはＵＳＢインターフェイスからなり、前記データ記憶部は、半導体メモリおよび磁気メモリの少なくとも１つを含む、請求項１～６のいずれか１項の記憶装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、記憶装置に関し、より具体的には、コンピュータに接続されると起動して通信可能となる記憶装置における情報保護に関する。
【背景技術】
【０００２】
ＵＳＢ（フラッシュ）メモリ、ＵＳＢ接続のポータブルなＨＤＤ等のようなコンピュータに接続するためのＵＳＢインターフェイスを備える記憶装置は、小型で携帯可能であるために、紛失したり盗難にあう可能性が大きい。その紛失や盗難の際に、あるいはユーザがＵＳＢメモリが接続されたコンピュータから離れてしまった際に、ＵＳＢメモリ内の情報が漏えいすることを防ぐために、従来から各種方策が取られている。
【０００３】
例えば、ＵＳＢメモリ等の記憶装置に情報を書き込む際にパスワードを入力させ、そのパスワードを入力しないと記憶装置から情報を読み出せないようにすることが行われている。
【０００４】
また、公開特許公報の2009-042927号（特許文献１）には、情報記憶装置において、ＲＦＩＤカードからＩＤを受信するリーダ／ライタ（Ｒ／Ｗ）と、大容量ストレージとを備え、ＲＦＩＤカードから受信したＩＤに基づいて、大容量ストレージの端末からのアクセス可能な領域を変更し、あるいはＲ／Ｗへの端末からのアクセスを遮断することが開示されている。
【０００５】
公開特許公報の2005-267533号（特許文献２）には、記憶装置において、当該記憶装置が、情報処理装置から予め設定された設定距離以上離れた隔離状態となったことが検出された場合に、当該記憶装置に記録されたデータの一部又は全部のアクセスを禁止し、あるいは当該記憶装置に記録されたデータを暗号化することが開示されている。

【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００９－０４２９２７号公報
【特許文献２】特開２００５－２６７５３３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
従来のパスワードを入力させる方法では、予めコンピュータに情報保護のためのドライバやアプリケーションのソフトウェアを導入しておく必要がある。また、情報の書き込み、あるいは読み出しの際に毎回パスワードを入力しなければならず、さらにパスワードの定期的な更新等の管理も必要となる。
【０００８】
特許文献１の情報記憶装置では、ＲＦＩＤカードからＩＤを受信できない場合のデータ保護については考慮されておらず、またデータの暗号化についても何ら考慮していない。
【０００９】
特許文献２の記憶装置では、当該記憶装置が、情報処理装置から予め設定された設定距離以上離れた隔離状態にならない場合についてのデータ保護については考慮されておらず、またデータの暗号化もその隔離状態になった場合についてのみおこなうことしか考慮していない。
【００１０】
したがって、本発明の目的は、これらの従来技術の問題を解決あるいは軽減しつつ、コンピュータに接続されると起動して通信可能となる記憶装置における適切かつ効率的な情報保護をおこなうことである。
【課題を解決するための手段】
【００１１】
本発明は、コンピュータに接続されると起動して通信可能となる記憶装置を提供する。その記憶装置は、コンピュータとの通信を制御するインターフェイスと、インターフェイスを介してコンピュータから受信したデータを保管するデータ記憶部と、ＩＤ情報を含む無線信号を所定のタイミング毎に受信し、受信したＩＤ情報を認証する無線信号処理部と、認証されたＩＤ情報をキーとしてデータを暗号化し、当該暗号化したデータをデータ記憶部に送り、さらに、無線信号処理部が所定時間内に認証されたＩＤ情報を含む無線信号を受信しない場合、インターフェイスにおけるコンピュータとの通信を不能にする制御部と、を備える。
【００１２】
本発明によれば、受信したＩＤ情報を認証し、認証されたＩＤ情報をキーとしてデータを暗号化するので、データの暗号化に際してパスワードを入力する等の手間を省くことができる。また、本発明によれば、所定時間内に認証されたＩＤ情報を含む無線信号を受信しない場合、コンピュータとの通信を不能にするので、記憶装置を紛失などした場合、あるいはユーザが使用中のコンピュータから離れたような場合であっても記憶装置内のデータの保護を図ることができる。さらに、本発明によれば、基本的にコンピュータおよびそこで実行されるソフトウェアの介在なしに記憶装置単独でデータの保護を図ることができる。
【００１３】
本発明の一態様では、制御部は、無線信号処理部が所定時間内に認証されたＩＤ情報を含む無線信号を受信している間に、コンピュータからデータ読み出し要求があった場合、読み出し要求に対応する暗号化されたデータをデータ記憶部から読み出して、暗号化されたデータを認証されたＩＤ情報をキーとして復号化して、復号されたデータを前記インターフェイスを介して前記コンピュータに送る。
【００１４】

本発明の一態様によれば、データの暗号化のみならずその復号化においても認証されたＩＤ情報をキーとしてデータの復号をおこなうので、データの読み出し時におけるパスワード入力の手間を省くことができると同時に、データ保護のさらなる促進、強化を図ることが可能となる。

【００１５】

本発明の一態様では、記憶装置は、ＩＤ情報を保管するためのＩＤ情報記憶部と、ＩＤ情報の認証スイッチとを更に備え、制御部は、認証スイッチがオンになっている場合に、無線信号処理部に対して受信したＩＤ情報を登録ＩＤ情報としてＩＤ情報記憶部に保管することを指示する。

【００１６】

本発明の一態様によれば、ユーザの意図により、新たなＩＤ情報を新たな登録ＩＤ情報としてＩＤ情報記憶部に保管させることにより、記憶装置をその新たな登録ＩＤ情報でのみ機能する記憶装置として利用することが可能となる。これにより、データ保護機能を堅持しつつ記憶装置の再利用（繰り返し利用）が可能となる。

【００１７】

本発明の一態様では、無線信号処理部は、認証スイッチがオンになっている場合を除いて、受信したＩＤ情報がＩＤ情報記憶部に保管されている登録ＩＤ情報に一致するか否かを判定することにより認証をおこなう。

【００１８】

本発明の一態様によれば、記憶装置内で受信したＩＤ情報の認証が登録ＩＤ情報との比較によって自動的におこなわれるので、コンピュータの介在なしに暗号化のためのキーおよびそれを用いた認証の管理を行うことができる。

【００１９】

本発明の一態様では、ＩＤ情報には、当該ＩＤ情報を担持する媒体固有の第１のＩＤ番号と、第１のＩＤ番号に付随する第２のＩＤ番号とが含まれ、制御部は、認証されたＩＤ情報中の第１のＩＤ番号および第２のＩＤ番号のいずれか一方あるいは双方を暗号化または復号化のためのキーとして用いる。

【００２０】

本発明の一態様によれば、ＩＤ情報を担持する媒体固有の第１のＩＤ番号と、第１のＩＤ番号に付随する第２のＩＤ番号とのいずれか一方あるいは双方を暗号化または復号化のためのキーとして用いるので、さらに、通信するＩＤ情報を担持する媒体をその媒体固有のＩＤ番号により特定（限定）することができるので、データの保護をより強固なものとすることが可能となる。

【００２１】

本発明の一態様では、無線信号処理部はＲＦＩＤのリーダ／ライタ（Ｒ／Ｗ）を含み、ＩＤ情報は、Ｒ／Ｗと通信可能なＲＦＩＤタグとして前記媒体に担持される。

【００２２】

本発明の一態様によれば、ＲＦＩＤ技術を利用して無線信号処理部およびＩＤ情報を担持する媒体の小型化、省電力化を図ることができる。

【図面の簡単な説明】

【００２３】

【図１】本発明の記憶装置とその通信環境の構成例を示す図である。

【図２】本発明の記憶装置の構成例を示すブロック図である。

【図３】本発明の記憶装置の構成例と信号経路の例を示す図である。

【図４】本発明の無線信号処理部によるポーリング処理の流れを示す図である。

【発明を実施するための形態】

【００２４】

図面を参照しながら本発明の実施の形態を説明する。図１は、本発明の記憶装置およびその通信環境の構成例を示す図である。図１においては、コンピュータ１０と、ＵＳＢメモリ２０と、非接触型（無線式）のＩＤカード３０とにより、通信環境が構成される。な

お、コンピュータ１０は、図１のノート型に限られず、デスクトップ型、タブレット型、サーバー等その形態は任意に選択可能である。また、コンピュータ１０はネットワークに接続されたものでも、あるいはスタンドアローンのものでもよい。

【００２５】

記憶装置は、図１のＵＳＢメモリ２０に限定されず、基本的にコンピュータに接続されると起動して通信可能となる記憶装置であればなんでもよい。すなわち、ＵＳＢインターフェイス以外のインターフェイスを備える記憶装置であってもよい。また、ＵＳＢメモリ２０として、図１の半導体メモリ（フラッシュメモリ）タイプではなく、ＵＳＢ接続のＨＤＤ等であってもよい。図１において、ＵＳＢメモリ２０は、ＵＳＢインターフェイス（端子）２２を矢印Ａの方向からコンピュータ１０のＵＳＢインターフェイス１２に挿入することにより起動し、コンピュータ１０と通信可能な状態となる。ＵＳＢメモリ２０は、さらにＩＤカード３０と無線通信（Ｂ）する。

【００２６】

ＩＤカード３０は、ＵＳＢメモリ２０と無線通信するための回路（ＩＣ、ＩＣタグ）、アンテナ（コイル）、さらにＩＤ情報を格納するためのメモリを内蔵する。ＩＤカード３０は、図１のカード（平板）タイプに限定されず、円盤型、ペン型、名札型など任意の形態を選択することができる。ＩＤ情報には、ＩＤカード３０固有の第１のＩＤ番号（例えば、複数桁の数字からなる製品番号）と、第１のＩＤ番号に付随する第２のＩＤ番号（例えば、複数桁の英数字）とが含まれる。なお、ＩＤカード３０の複製防止のため、一定期間毎にＩＤカード３０に格納されるＩＤ情報と記憶装置内に格納される認証用の登録ＩＤ情報（後述）とを同時に更新する（同一の他のＩＤ情報に変更する）ことが望ましい。

【００２７】

図２は、本発明の記憶装置の構成例を示すブロック図である。図１の例では、ＵＳＢメモリ２０の構成例となる。各ブロックの要素は、通信経路（バス）２７０を介して相互に通信可能になっている。制御部２１０は、プロセッサ（ＣＰＵ）、レジスタ、メモリ等を含み、後述する各種制御をおこなう。無線信号処理部２２０は、ＩＤ情報を含む無線信号を所定のタイミング毎に受信し、受信したＩＤ情報を認証する。ＩＤ情報記憶部２３０は、ＩＤ情報を保管する。なお、ＩＤ情報記憶部２３０は、制御部２１０に内蔵あるいは制御部２１０内のメモリを兼用してもよい。

【００２８】

インターフェイス（Ｉ／Ｆ）２４０は、コンピュータとの通信（入出力）を制御する。データ記憶部２５０は、インターフェイス（Ｉ／Ｆ）２４０を介してコンピュータから受信したデータを保管する。データ記憶部２５０は、上述したように、ＵＳＢメモリ２０の場合は、フラッシュメモリやＨＤＤ等からなる。認証スイッチ（ＳＷ）２６０は、新たにあるいは改めてＩＤ情報をＩＤ情報記憶部２３０に保管（登録）させる場合にユーザによってオンされるスイッチである。認証スイッチ（ＳＷ）２６０は、オン／オフでその位置が変わるボタン式あるいはスライド式のスイッチ等からなる。その実施形態は任意に選択することができる。また、ユーザがうっかり誤って認証ＳＷ２６０を押してしまう場合に、ＩＤ情報が更新されないようにするために、認証ＳＷ２６０を一定時間（例えば２、３秒）以上押し続けなければオン信号が出力されないようにすることが望ましい。さらに、認証ＳＷ２６０を押した場合、ＬＥＤのような小型の発光素子が点灯あるいは点滅してその新たなＩＤ情報の登録（更新）の開始およびその完了をユーザに視覚的に知らせるようにしてもよい。あるいは、認証ＳＷ２６０を押した場合、ビープ音等の音を発生させて、ユーザに聴覚的に新たなＩＤ情報の登録（更新）の開始およびその完了を知らせるようにしてもよい。

【００２９】

図３は、本発明の記憶装置の構成例の詳細と信号経路の例を示す図である。図３を参照しながら、主に本発明を構成する各要素の動作について説明する。無線信号処理部２２０は、Ｒ／Ｗ制御部２２１と、タイマ２２２と、アンテナ２２３とを含む。Ｒ／Ｗ制御部２２１は、例えばＲＦＩＤのリーダ／ライタ（Ｒ／Ｗ）からなる。ＲＦＩＤのＲ／Ｗの場合

は、ＲＦＩＤ用のＩＣ（ＩＤ）タグを内蔵するＩＤカードが用いられる。ＲＦＩＤのＲ／Ｗは、アンテナ２２３を介して電磁波である無線信号をＩＤカードに送り、すなわちポーリングし、ＲＦＩＤ用のＩＣタグを内蔵するＩＤカードを起動させて、ＩＤカードのメモリに格納されているＩＤ情報を無線信号（電磁波）として発信させる。Ｒ／Ｗ制御部２２１は、ＩＤカードからのＩＤ情報を含む無線信号を受信する。タイマ２２２は、ポーリング開始からの時間を計測する。タイマ２２２による計測時間は、後述するＩＤ情報の認証およびデータ保護のための制御に利用される。Ｒ／Ｗ制御部２２１は、受信したＩＤ情報を認証し、認証したＩＤ情報記憶部２３０に保管する。ポーリングおよびＩＤ情報の認証の制御についてはさらに後述する。

【００３０】

制御部２１０は、暗号化／復号化部２１１と、メモリ制御部２１２と、Ｉ／Ｆおよび認証の制御部２１３とを含む。暗号化／復号化部２１１は、認証されたＩＤ情報をキーとして、Ｉ／Ｆ２４０を介してコンピュータから送られるデータを暗号化し、その暗号化したデータをメモリ制御部２１２を介してデータ記憶部２５０に送る。暗号化／復号化部２１１は、暗号化の際に、上述したＩＤカード３０固有の第１のＩＤ番号（例えば、複数桁の数字からなる製品番号）と、第１のＩＤ番号に付随する第２のＩＤ番号（例えば、複数桁の英数字）のいずれか一方あるいは双方を暗号化または復号化のためのキーとして用いる。

【００３１】

メモリ制御部２１２は、データ記憶部２５０へのデータの書き込みおよびデータ記憶部２５０からのデータの読み出しの制御、データ記憶部２５０における書き込みおよび読み出しのアドレス制御等のいわゆるメモリ・コントローラとしての一般的な機能を備えている。

【００３２】

Ｉ／Ｆおよび認証の制御部２１３は、Ｒ／Ｗ制御部２２１から所定時間内に認証されたＩＤ情報を含む無線信号を受信していることを示す信号を受けている場合において、Ｉ／Ｆ２４０を介してコンピュータからデータ読み出し要求を受けた場合、メモリ制御部２１２に対して読み出し要求に対応するデータの読み出しを指示する。ここで言う所定時間は、予め設定され、例えば１０秒である。所定時間に至ったか否かは、Ｒ／Ｗ制御部２２１において、タイマ２２２によって計測されるポーリング開始後の経過時間を基に判断される。メモリ制御部２１２は、読み出し要求に対応する暗号化されたデータをデータ記憶部から読み出して、暗号化／復号化部２１１に送る。暗号化／復号化部２１１は、送られてきた暗号化されたデータを認証されたＩＤ情報をキーとして復号し、復号されたデータをＩ／Ｆ２４０を介してコンピュータに送る。

【００３３】

Ｉ／Ｆおよび認証の制御部２１３は、さらに、Ｒ／Ｗ制御部２２１から所定時間内に認証されたＩＤ情報を含む無線信号を受信していないことを示す信号を受けた場合、Ｉ／Ｆ２４０におけるコンピュータとの通信を不能にする。ここで言う所定時間は、予め設定され、例えば１０秒である。コンピュータとの通信を不能にする方法は、例えば、Ｉ／Ｆ２４０においてデータラインのインピーダンスをハイ（Ｈｉ－Ｚ）またはロウ（Ｌｏｗ－Ｚ）にして、論理上コンピュータから切り離された状態（データ送受信不能状態）にする。この時、転送中のトランザクションは最後まで実行させ、少なくとも１パケット分の送受信は完了させるようにする。ただし、転送中のデータは完全な形で転送されないので、コンピュータとの通信再開後に再度転送し直す必要がある。コンピュータとの通信を再開させるには、改めて記憶装置２０を起動させる、すなわち例えば図１に例示されるＵＳＢメモリ２０にあっては、コンピュータ１０のＵＳＢインターフェイス（端子）２２から一旦抜いて、再度差し込む必要がある。

【００３４】

Ｉ／Ｆおよび認証の制御部２１３は、さらに、ＩＤ情報の認証スイッチ（ＳＷ）２６０がオンになった信号を受けて、Ｒ／Ｗ制御部２２１に対して受信したＩＤ情報を登録ＩＤ

情報としてＩＤ情報記憶部２３０に保管することを指示する。新たに保管された登録ＩＤ情報は、Ｒ／Ｗ制御部２２１における認証判断の基準となり、すなわち、登録ＩＤ情報に一致するか否かを判定することにより認証がおこなわれ、また暗号化／復号化部２１１における暗号化／復号化のためのキーとして利用される。これにより、ＩＤカードを紛失等した場合であっても、新たなＩＤカードに格納されるＩＤ情報を用いて、記憶装置２０の利用を継続することが可能となる。その際、ＩＤ情報が異なることから、前の（古い）ＩＤ情報をキーとして暗号化されたデータへのアクセスはできなくなり、情報（データ）漏洩を防止することが可能となる。また、新たにＩＤ情報が登録された際に、データ記憶部２５０をフォーマットすることにより、古いデータを消去してしまうことができる。これにより、完全に古いデータの漏洩を防止することが可能となる。

【００３５】

次に、図４を参照しながら、記憶装置によるポーリングおよびＩＤ情報の認証の制御について説明する。図４は、記憶装置（Memory）とＩＤカード（ID Card）との間のポーリングおよび認証処理の流れを示す図である。なお、図４におけるポーリングおよび認証制御は、既に述べたように、実際には記憶装置内の無線信号処理部２２０（Ｒ／Ｗ制御部２２１）によって実行される。図４の（ａ）はＩＤ情報の認証に成功する場合であり、（ｂ）は認証に失敗する場合の例である。

【００３６】

図４（ａ）において、記憶装置が起動し（Power On）、ポーリングを所定のタイミングで開始する（Ｐ１）。ＩＤカードは、記憶装置と通信可能な状態にある場合、Ackを返し、同時にＩＤ情報を送信する（Ａ１）。記憶装置は、受信したＩＤ情報が登録ＩＤ情報と一致するか否かを判断し、一致して認証がＯＫな場合は、Valid Flagを出力する（Ｆ１）。以下、ポーリング毎に同様な動作が繰り返される。今、ｎ回目のポーリング（Ｐｎ）において、Ackが戻らずＩＤ情報が受信できないとする（Ａｎ）。記憶装置はＩＤ情報の認証に失敗し、Invalid Flagを出力する（Ｆｎ）。図４（ａ）では、この認証失敗が２回繰り返されるが、所定時間ΔＴ１内での認証失敗であるので、Valid Flag出力が維持されてＩＤ情報の認証継続となる。この所定時間ΔＴ１は、既に述べたように、例えば１０秒である。所定時間以上Valid Flag出力が維持される場合、既に述べたように、その状態を示す信号、すなわち所定時間内に認証されたＩＤ情報を含む無線信号を受信していることを示す信号がＲ／Ｗ制御部２２１からＩ／Ｆおよび認証の制御部２１３に送られる。

【００３７】

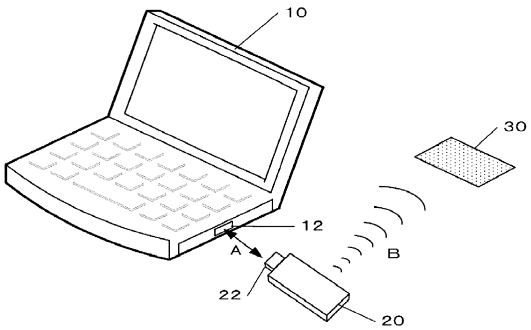
図４（ｂ）において、（ａ）の場合と同様に、ポーリングが所定のタイミングで行われており認証がされているとする（Ｐ１、Ａ１、Ｆ１）。その後のｎ回目のポーリング（Ｐｎ）において、Ackが戻らずＩＤ情報が受信できないとする（Ａｎ）。記憶装置はＩＤ情報の認証に失敗し、Invalid Flagを出力する（Ｆｎ）。（ｂ）では、（ａ）の場合と違って、この認証失敗がその後連続して発生し、所定時間ΔＴ１を超えて認証失敗を示すInvalid Flagが出力される。この場合、所定時間以上Invalid Flag出力が維持される状態を示す信号、すなわち所定時間内に認証されたＩＤ情報を含む無線信号を受信していないことを示す信号がＲ／Ｗ制御部２２１からＩ／Ｆおよび認証の制御部２１３に送られる。その結果、既に述べたように、Ｉ／Ｆ２４０におけるコンピュータとの通信が不能にされる（USB Release）。これにより、記憶装置に格納された情報（データ）へのアクセスが禁止され、その情報漏洩が防止される。

【００３８】

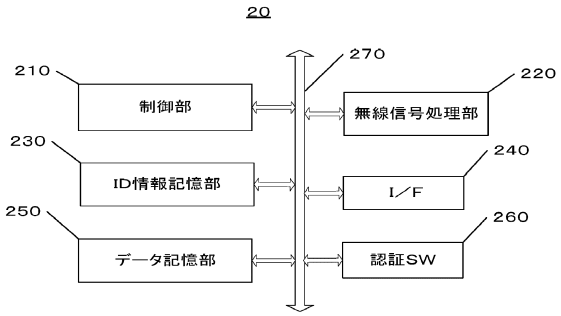
上述した認証の有無を判断するための所定時間を例えば１０秒に設定する理由は、以下の通りである。すなわち、（ａ）処理中のトランザクションを処理し終わるまでには十分な時間であること、（ｂ）電波状況によっては２～３回は続けて正常にＩＤ情報が受信できないケースもあること、（ｃ）数十ＭＢのファイルの転送ならば終えることができるので、必要以上に余計な転送中断は発生しなくて済むこと、さらに（ｄ）ＩＤカードが記憶装置から離れて１０秒以内で第三者が記憶装置内のファイル（データ）をコピーしていくことは難しいこと、がその理由である。

【００３９】
本発明の実施形態について、図を参照しながら説明をした。しかし、本発明はこれらの実施形態に限られるものではない。本発明はその趣旨を逸脱しない範囲で当業者の知識に基づき種々なる改良、修正、変形を加えた態様で実施できるものである。
【符号の説明】
【００４０】
１０　コンピュータ（ＰＣ）
１２、２２　ＵＳＢインターフェイス（Ｉ／Ｆ）
２０　記憶装置（ＵＳＢメモリ）
２７０　通信経路（バス）

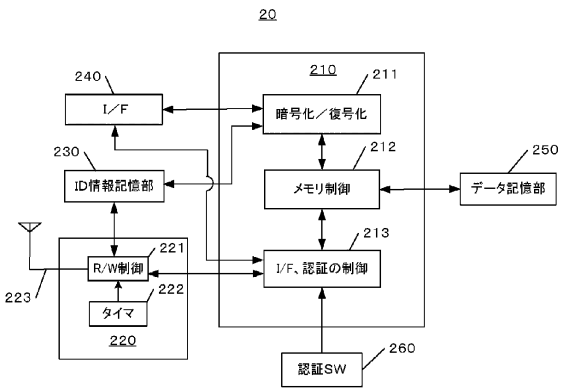
【図１】



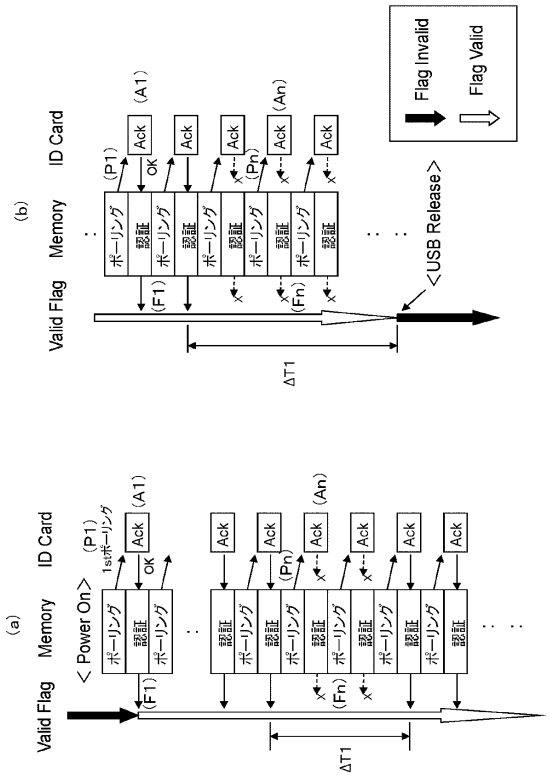
【図２】



【図３】



【図４】


(b)
Valid Flag
Memory
ID Card
Flag Invalid
Flag Valid
(P1)
(A1)
Ack
OK
ポーリング
認証
(F1)
(Pn)
(An)
(Fn)
<USB Release>
ΔT1
(a)
< Power On>
1stポーリング

フロントページの続き

(74)代理人 100112690
弁理士 太佐 種一
(72)発明者 松芝 卓二
東京都江東区豊洲五丁目６番５２号 ＮＢＦ豊洲キャナルフロント 日本アイ・ビー・エム株式会社 ＩＢＭ東京ラボラトリー内
(72)発明者 高山 雅夫
東京都江東区豊洲五丁目６番５２号 ＮＢＦ豊洲キャナルフロント 日本アイ・ビー・エム株式会社 ＩＢＭ東京ラボラトリー内

合議体
審判長 辻本 泰隆
審判官 須田 勝巳
審判官 高木 進

(56)参考文献 特開２００７－２４９２６３（ＪＰ，Ａ）
特開２００９－４２９２７（ＪＰ，Ａ）
特開２００９－１２９４１３（ＪＰ，Ａ）
特開２００７－３２９７２０（ＪＰ，Ａ）
特開２０１０－２０７５１（ＪＰ，Ａ）
米国特許出願公開第２００２／００４２８８３（ＵＳ，Ａ１）
特開２００４－２０８１６９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/00
H04L 9/00