(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-200059
(P2014-200059A)
(43)公開日　平成26年10月23日(2014.10.23)

(51)Int.Cl.		F I			テーマコード（参考）
H04N 5/225	(2006.01)	H04N	5/225	F	5B035
G06F 21/34	(2013.01)	G06F	21/20	134	5C053
G06F 21/62	(2013.01)	G06F	21/24	165C	5C122
G06K 19/10	(2006.01)	G06K	19/00	R	
H04N 5/907	(2006.01)	H04N	5/907	B	

審査請求 未請求　請求項の数 4　ＯＬ　（全 13 頁）　最終頁に続く

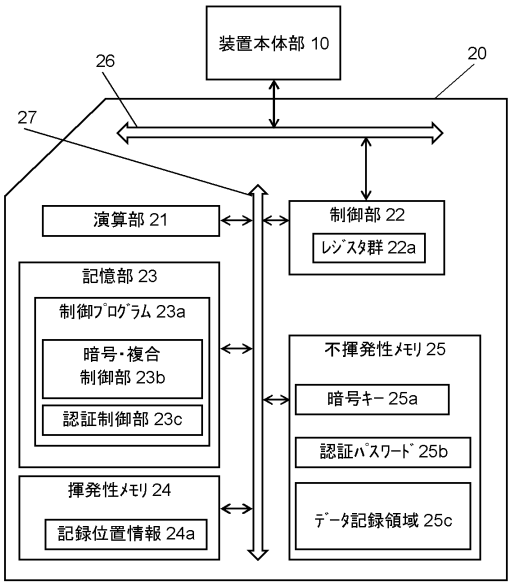
(21)出願番号　特願2013-259755 (P2013-259755)
(22)出願日　平成25年12月17日 (2013.12.17)
(31)優先権主張番号　特願2013-52848 (P2013-52848)
(32)優先日　平成25年3月15日 (2013.3.15)
(33)優先権主張国　日本国 (JP)

(71)出願人　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100109667
弁理士　内藤　浩樹
(74)代理人　100120156
弁理士　藤井　兼太郎
(74)代理人　100137202
弁理士　寺内　伊久郎
(72)発明者　三皷　正則
大阪府門真市大字門真１００６番地　パナソニック株式会社内

Ｆターム(参考)　5B035 AA02 AA13 BB09 CA38
5C053 FA27 LA01 LA14
5C122 EA07 EA69 GA16 GA24 GA31
HA23 HA27 HA32 HA60 HB01

(54)【発明の名称】記録媒体

(57)【要約】
【課題】セキュリティ機能を有する記録媒体おいて、電源を入れた後、すぐに撮影を開始できるという即時性を持つ動作と、記録されたデータの機密性を確保する動作を両立させることを目的とする。
【解決手段】装置本体部１０から伝送されるデータの暗号化及び復号化を行う暗号・復号制御部２３ｂと、装置本体部１０から送られる認証パスワードの認証処理を行う認証制御部２３ｃと、前記暗号・復号制御部で用いる暗号キー及び前記認証制御部で認証のために用いる認証パスワードを記憶し、暗号・復号制御部により暗号化されたデータの記録を行うデータ記録領域を有する不揮発性メモリ２５と、認証制御部による認証処理が行われていない未認証時に、前記不揮発性メモリのデータ記録領域に記録されたデータの記録位置情報２４ａを記憶する揮発性メモリ２４とを備える。
【選択図】図２



【特許請求の範囲】
【請求項１】
装置本体部に任意に取付け、取外し可能で、装置本体部に取付けることにより装置本体部から通電が行われる記録媒体であって、
装置本体部から伝送されるデータの暗号化及び復号化を行う暗号・復号制御部と、
装置本体部から送られる認証パスワードの認証処理を行う認証制御部と、
前記暗号・復号制御部で用いる暗号キー及び前記認証制御部で認証のために用いる認証パスワードを記憶し、暗号・復号制御部により暗号化されたデータの記録を行うデータ記録領域を有する不揮発性メモリと、
前記認証制御部による認証処理が行われていない未認証時に、前記不揮発性メモリの前記データ記録領域に記録された前記データの記録位置情報を記憶する揮発性メモリと、
を備えたことを特徴とする記録媒体。
【請求項２】
前記揮発性メモリは、認証済み、または未認証であることを示す認証フラグが記憶されることを特徴とする請求項１に記載の記録媒体。
【請求項３】
前記揮発性メモリは、認証済み、または未認証であることを示す認証フラグと、未認証時に前記不揮発性メモリの前記データ記録領域に記録された前記データの記録位置情報とが記憶され、前記認証フラグが未認証であることを示す場合は前記記録位置情報に基づき、前記不揮発性メモリの前記データ記録領域に記録された前記データを読み出すことを特徴とする請求項１に記載の記録媒体。
【請求項４】
前記揮発性メモリは、前記記録媒体を前記装置本体部から取出して通電を停止することにより、記憶された前記データが消去されるものである請求項１に記載の記録媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本技術は、撮影装置などに使用されるセキュリティ機能を有する記録媒体に関する。
【背景技術】
【０００２】
従来、撮影装置で撮影した画像データを暗号化して保存する記録媒体が実現されている。暗号化を実現するためには、平分データを暗号化する際の暗号鍵が必要である。勿論、暗号化されたデータを解読するには、復号鍵が必要である。暗号化方式によっては、暗号鍵と復号鍵は、一致することがある。これら暗号鍵及び復号鍵の一方、または両方は、第三者に漏洩することなく、安全に管理されなければならない。
【０００３】
これらの鍵データを安全に保管する手段として、記憶データの解読がソフトウェア上及びハードウェア上、困難なＩＣカードが有力視されている。鍵データをＩＣカードなどの記憶デバイスに秘匿して格納し、その鍵でデジタルデータを暗号化する撮影装置が特許文献１に記載されている。
【０００４】
また、セキュリティ機能を有する記録媒体として、認証処理が終了していない場合は、撮影画像データを暗号化して保存しないようにするか、撮影画像データを暗号化して保存するようにするかを選択できるようにしたものが知られている。
【０００５】
一方、報道などで使用される業務用の撮影装置においては、電源を入れた後、すぐに撮影を開始できるという即時性を持つ動作が求められるが、セキュリティ機能を有する記録媒体は、認証が完了しないと暗号化記録の動作を行うことができなく、また暗号化記録したコンテンツデータの確認も行えない。このため、業務用の撮影装置に使用されるセキュリティ機能を有する記録媒体においては、電源を入れた後、すぐに撮影を開始できるとい

う即時性を持つ動作と、記録されたデータの機密性を確保する動作を両立させることは難しいという課題があった。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】特開２００１－３２０６６８号公報

【発明の概要】

【発明が解決しようとする課題】

【０００７】

本技術はこのような現状に鑑みなされたもので、業務用の撮影装置などに使用されるセキュリティ機能を有する記録媒体おいて、電源を入れた後、すぐに撮影を開始できるという即時性を持つ動作と、記録されたデータの機密性を確保する動作を両立させることを目的とする。

【課題を解決するための手段】

【０００８】

本技術の記録媒体は、装置本体部に任意に取付け、取外し可能で、装置本体部に取付けることにより装置本体部から通電が行われる記録媒体であって、装置本体部から伝送されるデータの暗号化及び復号化を行う暗号・復号制御部と、装置本体部から送られる認証パスワードの認証処理を行う認証制御部と、前記暗号・復号制御部で用いる暗号キー及び前記認証制御部で認証のために用いる認証パスワードを記憶し、暗号・復号制御部により暗号化されたデータの記録を行うデータ記録領域を有する不揮発性メモリと、前記認証制御部による認証処理が行われていない未認証時に、前記不揮発性メモリのデータ記録領域に記録されたデータの記録位置情報を記憶する揮発性メモリとを備えている。

【発明の効果】

【０００９】

本技術による記録媒体は、装置本体部に装填した状態、すなわち電源の供給を開始した段階で、直ぐに撮影したデータの書込み動作と読出し動作を行うことが可能で、即時性を持つ動作を持たせることができる。しかも、装置本体部から取出し、電源の供給を停止することにより、認証パスワードによる認証動作を行わずに記録されたデータの読出し動作が不可能になるため、記録情報の機密性も確保することが可能となる。

【図面の簡単な説明】

【００１０】

【図１】本技術による記録媒体を使用する撮影装置の概略構成を示すブロック図である。

【図２】本技術の一実施の形態による記録媒体の概略構成を示すブロック図である。

【図３】本技術による記録媒体において、書込み動作時において、認証パスワード設定コマンドを受信した場合の動作フローを示すフローチャートである。

【図４】本技術による記録媒体において、書込み動作時において、認証パスワード設定コマンドを受信しない場合の動作フローを示すフローチャートである。

【図５】本技術による記録媒体において、読出し動作時の動作フローを示すフローチャートである。

【発明を実施するための形態】

【００１１】

以下、本技術の一実施の形態によるセキュリティ機能を有する記録媒体について、図面を参照しながら説明する。但し、必要以上に詳細な説明は省略する場合がある。例えば、既によく知られた事項の詳細説明や実質的に同一の構成に対する重複説明を省略する場合がある。これは、以下の説明が不必要に冗長になるのを避け、当業者の理解を容易にするためである。

【００１２】

なお、発明者は、当業者が本技術を十分に理解するために添付図面及び以下の説明を提供するのであって、これらによって特許請求の範囲に記載の主題を限定することを意図す

るものではない。

【００１３】

本技術による記録媒体は、撮影装置に使用されるものであある。以下、業務用の撮影装置の概略構成について説明する。

【００１４】

図１は、本技術による記録媒体を使用する撮影装置の概略構成を示すブロック図である。

【００１５】

図１に示すように、撮影装置の装置本体部１０は、映像信号や音声信号の入出力を行う信号入出力部１１と、映像信号や音声信号のアナログ・デジタル変換や所定の信号フォーマットへの変換などの信号処理を行う信号処理部１２と、フラッシュメモリなどの記憶部１３と、液晶ディスプレイなどのモニタ１４と、外部機器との間で無線によりデータの送受信を行う無線通信部１５と、装置本体部１０と記録媒体２０との間でデータのやり取りを行うインターフェース部１６と、これらの各部を制御するための制御部１７とを有している。また、装置本体部１０の各部は、バス１８を介してデータのやり取りが行われる。

【００１６】

また、装置本体部１０は、ユーザーが記録媒体２０を任意に取付け、及び取出し可能なアダプター（図示せず）を備えており、そのアダプターはインターフェース部１６に接続されている。記録媒体２０は、装置本体部１０のアダプターに取付けることにより、記録媒体２０に通電が行われる。これにより、記録媒体２０は、装置本体部１０で作成されたデータの暗号化記録と、暗号化記録されたデータを復号化して読み出す動作を行うことが可能となる。

【００１７】

信号入出力部１１は、撮像素子やマイクロフォンなどからの映像信号や音声信号を入力し、信号処理部１２により信号処理された信号を外部のモニタやスピーカーなどに出力する機能を有している。なお、この信号入出力部１１は、外部機器との間で映像信号や音声信号を通信でやり取りする通信手段を構成してもよい。

【００１８】

信号処理部１２は、エンコーダやデコーダなどの信号変換部、及びデータを一時保存するためのバッファも有している。

【００１９】

記憶部１３は、装置本体部１０の各種設定情報を保存するためのものであり、ユーザーが設定した各種設定情報を制御部１７がバス１８を介して、記憶部１３に記録する。設定情報にはコンテンツを暗号化記録するか否かの情報も含まれている。

【００２０】

無線通信部１５は、インターネットに接続するためのインターフェースモジュールであり、無線ＬＡＮモジュールなどにより構成される。無線通信部１５は、制御部１７からの指示により認証パスワードを管理する管理サーバに通信し、記録媒体２０のシリアル番号を基に認証パスワードを問い合わせる。管理サーバから記録媒体２０のシリアル番号に対応する認証パスワードを取得できた場合は、制御部１７のメモリに認証パスワードが保存される。

【００２１】

制御部１７は、一般的な演算プロセッサ、メモリ、及び演算プロセッサを動作させるためのプログラムを格納する記憶領域などを有している。また、制御部１７は、所望のデータを記録媒体２０にファイルとして記録するためのファイルシステムを搭載している。

【００２２】

信号入出力部１１から入力された映像信号や音声信号は、信号処理部１２で信号処理され、符号化されたデジタルデータに変換される。これらのデジタルデータはバッファに蓄えられ、制御部１７によって、インターフェース部１６を介してデータファイルとして記録媒体２０に記録される。このとき、制御部１７は、符号化されたデジタルデータの先頭

フレームのデータを、ビットマップ形式の画像ファイルであるサムネール画像として作成し、記録媒体２０に記録する。このサムネール画像データは、ユーザーが操作することにより、モニタ１４にサムネール一覧として表示されることが可能である。サムネール画像データは、所望の画像データを記録媒体２０から探しやすくしたりするものである。したがって、画像データは、例えば縦８０ピクセル、横６０ピクセル、１ピクセルあたり２４ビットの画像データに圧縮される。

【００２３】

また、制御部１７は、映像データや音声データのフレームレートやフレーム数、データのサイズをフレーム数で表したデュレーションなどの情報を管理したり、関連付けを行うためのクリップ管理情報を作成し、ＸＭＬ形式のデータファイルを作製する。クリップ管理情報もファイルシステムにより記録媒体２０に記録される。

【００２４】

図２は本技術の一実施の形態による記録媒体の概略構成を示すブロック図である。

【００２５】

図２に示すように、記録媒体２０は、演算部２１と、制御部２２と、不揮発性メモリとしてのＲＯＭ（リード・オンリー・メモリ）からなる記憶部２３と、ＲＡＭ（ランダム・アクセス・メモリ）からなる揮発性メモリ２４と、フラッシュメモリからなる不揮発性メモリ２５と、装置本体部１０と制御部２２との間でデータを伝送するためのバス２６と、演算部２１、制御部２２、記憶部２３、揮発性メモリ２４、及び不揮発性メモリ２５をデータ伝送可能に接続するバス２７とを有している。これにより、演算部２１は、レジスタ群２２ａを含む制御部２２、記憶部２３、揮発性メモリ２４及び不揮発性メモリ２５に対し、バス２７を介してアクセス可能に接続されている。さらに、記録媒体２０は、装置本体部１０から取出し、通電を停止した時点で、揮発性メモリ２４に記憶されているデータは消去されるが、記憶部２３、不揮発性メモリ２５に記憶されているデータは、通電停止後も消去されず、そのまま保持されている。

【００２６】

演算部２１は、バス２７に接続され、記憶部２３に格納されるファームウェアとしての制御プログラム２３ａを実行し、制御部２２の制御を行う。記憶部２３に格納されている制御プログラム２３ａには、装置本体部１０から伝送されるデータの暗号化及び復号化を行う暗号・復号制御部２３ｂと、装置本体部１０から送られる認証パスワードの認証処理を行う認証制御部２３ｃを含んでいる。

【００２７】

制御部２２は、レジスタ群２２ａを有し、装置本体部１０から送られる制御コマンドをバス２６を介して受信し、この受信した制御コマンドを解析して、コマンド番号、コマンド引数などをレジスタ群２２ａに保存する。演算部２１は、レジスタ群２２ａに保存された値を参照して、制御プログラム２３ａを実行する。

【００２８】

揮発性メモリ２４は、バス２７に接続され、演算部２１のワークメモリとしての機能を有するとともに、記録媒体２０において実行される処理に必要とされる種々のデータを記憶する。また、揮発性メモリ２４は、未認証時に暗号化されて記録されたデータの記録位置を保持するための記録位置情報２４ａを含んでいる。なお、未認証時とは、認証制御部２３ｃにおいて、認証パスワードによる認証処理が行われていない状態を意味している。また、揮発性メモリ２４は、記録媒体２０が装置本体部１０から取出されて通電が停止した時点で、内部に記憶されているデータは消去される。

【００２９】

不揮発性メモリ２５は、バス２７に接続され、暗号・復号制御部２３ｂで用いる暗号キー２５ａ、及び認証制御部２３ｃで認証のために用いる認証パスワード２５ｂを記憶する領域と、暗号・復号制御部２３ｂにより暗号化されたデータの記録を行うためのデータ記録領域２５ｃとを有している。

【００３０】

暗号キー２５ａは、装置本体部１０から送られる制御コマンドにより認証パスワード２５ｂが設定されたときに、暗号・復号制御部２３ｂによりランダムに生成される。暗号キー２５ａは、装置本体部１０から書込コマンドを受信した場合に、装置本体部１０からレジスタ群２２ａの所定のアドレスに設定されたデータを、暗号・復号制御部２３ｂにより暗号化する際に使用される。また、暗号キー２５ａは、装置本体部１０から読込コマンドを受信した場合に、データ記録領域２５ｃから読み込んだデータを、暗号・復号制御部２３ｂにより復号化する際の復号キーとしても使用される。

【００３１】

認証パスワード２５ｂは、装置本体部１０から送られる認証パスワード設定コマンドにより設定される。認証パスワード２５ｂは、装置本体部１０から認証パスワード設定コマンドを受信した場合に、認証制御部２３ｃにおいて認証用のパスワードとして使用される。

【００３２】

認証制御部２３ｃは、装置本体部１０から認証パスワード設定コマンドを受信した場合に、認証パスワード設定コマンドの引数として受信したパスワードを認証パスワード２５ｂと比較し、一致した場合に認証が成功したことを揮発性メモリ２４に記録する。具体的には、認証制御部２３ｃは、受信した認証パスワードが不揮発性メモリ２５に記憶されている認証パスワード２５ｂと一致しているか否かを比較し、受信した認証パスワードが記憶されている認証パスワード２５ｂと一致し、認証が成功した場合は、揮発性メモリ２４に、認証済みであることを示す認証フラグ［１］を書込む。

【００３３】

一方、装置本体部１０から認証パスワードを受信せず、認証が成功しなかった場合、または受信した認証パスワードが記憶されている認証パスワード２５ｂと一致せず、認証が成功しなかった場合は、揮発性メモリ２４に、未認証であることを示す認証フラグ［０］を書込む。これにより、認証制御部２３ｃによる認証処理の結果として、認証済み、または未認証であることを示す認証フラグが揮発性メモリ２４に記憶される。なお、揮発性メモリ２４内の認証済みか否かの認証フラグ情報は、記録媒体２０への通電開始時、すなわち装置本体部１０に記録媒体２０を取付けた段階で、初期値として未認証状態に設定されている。

【００３４】

データ記録領域２５ｃは、装置本体部１０からのデータの保存、読出しを行うための領域で、装置本体部１０から書込コマンドを受信した場合、装置本体部１０からレジスタ群２２ａの所定のアドレスに設定されたデータを制御プログラム２３ａによりデータ記録領域２５ｃに記録する。この時、装置本体部１０から書込コマンドを受信した場合、装置本体部１０からレジスタ群２２ａの所定のアドレスに設定されたデータは、暗号・復号制御部２３ｂにより暗号化され、データ記録領域２５ｃに記録される。なお、未認証状態の場合は、装置本体部１０から書込コマンドを受信し、暗号・復号制御部２３ｂにより暗号化してデータ記録領域２５ｃにデータを記録したとき、揮発性メモリ２４にデータの記録位置である記録位置情報２４ａが書き込まれる。この記録位置情報２４ａとしては、不揮発性メモリ２５のファイルシステム管理情報が用いられる。

【００３５】

また、装置本体部１０から読込コマンドを受信した場合、装置本体部１０からレジスタ群２２ａの所定のアドレスに、制御プログラム２３ａによりデータ記録領域２５ｃから読み込んだデータを記録する。この時、装置本体部１０から読込コマンドを受信した場合、データ記録領域２５ｃから読み込んだデータは、暗号・復号制御部２３ｂにより復号化され、レジスタ群２２ａに記録される。なお、未認証状態の場合は、装置本体部１０から読込コマンドを受信したとき、揮発性メモリ２４の記録位置情報２４ａを参照し、その記録位置情報２４ａに記憶されているデータ記録領域２５ｃの位置からデータが読み出される。

【００３６】

上記本実施の形態においては、暗号・復号制御部２３ｂ及び認証制御部２３ｃはソフトウェアによって実現しているが、専用回路を設けハードウェアによって実現してもよい。

【００３７】

次に、本技術による記録媒体において、装置本体部１０から伝送されるデータの書込み動作について説明する。

【００３８】

図３は、書込み動作時において、認証パスワード設定コマンドを受信した場合の動作フローを示すフローチャートである。

【００３９】

まず、装置本体部１０から認証パスワードを入力することにより、記録媒体２０は、ステップＳ３０１において、認証パスワード設定コマンドを受信する。

【００４０】

次に、認証制御部２３ｃは、受信認証パスワードが不揮発性メモリ２５に記憶されている認証パスワード２５ｂと一致しているか否かを比較する（ステップＳ３０２）。受信した認証パスワードが記憶されている認証パスワード２５ｂと一致し、認証が成功した場合は、揮発性メモリ２４に、認証済みであることを示す認証フラグ［１］を書込む（ステップＳ３０３）。なお、揮発性メモリ２４内の認証済みか否かの認証フラグ情報は、記録媒体２０の電源立ち上げ時に、すなわち装置本体部１０に記録媒体２０を装填した段階で、初期値として未認証状態に設定されている。

【００４１】

揮発性メモリ２４内記憶されている情報が認証済みの場合は、ステップＳ３０４において装置本体部１０から送られる書込みデータを暗号化する。書込みデータの暗号化動作は、暗号・復号制御部２３ｂにより、装置本体部１０から暗号書込コマンドを受信した場合に、装置本体部１０からレジスタ群２２ａの所定のアドレスに設定されたデータについて、暗号キー２５ａを用いて暗号化することにより行われる。そして、暗号化された書込みデータは、ステップＳ３０５において、不揮発性メモリ２５のデータ記録領域２５ｃに記録される。

【００４２】

ステップＳ３０６において、不揮発性メモリ２５のデータ記録領域２５ｃへの書込みデータの記録が終了した後、ステップＳ３０７において、記録媒体２０を装置本体部１０から取出す動作を行うと、揮発性メモリ２４に記憶されている認証済みであることを示す認証フラグが初期化される（ステップＳ３０８）。これにより、認証パスワード設定コマンドを受信し、認証が成功した場合の書込み動作が終了する。

【００４３】

一方、ステップＳ３０２において、受信した認証パスワードが記憶されている認証パスワード２５ｂと一致せず、認証が成功しなかった場合は、揮発性メモリ２４に、認証フラグ［０］を書込む（ステップＳ３０９）。また、揮発性メモリ２４は、未認証となった書込みデータの記録位置情報２４ａを書込む（ステップＳ３１０）。

【００４４】

その後は、認証済みの場合と同様、ステップＳ３０４において装置本体部１０から送られる書込みデータを暗号化し、暗号化された書込みデータは、ステップＳ３０５において、不揮発性メモリ２５のデータ記録領域２５ｃに記録される。不揮発性メモリ２５のデータ記録領域２５ｃへの書込みデータの記録が終了し（ステップＳ３０６）、記録媒体２０を装置本体部１０から取出す動作（ステップＳ３０７）を行うと、ステップＳ３０８において、揮発性メモリ２４に記憶されている認証フラグが初期化されるとともに、未認証となった書込みデータの記録位置情報２４ａのデータも消去される。これにより、認証パスワード設定コマンドを受信し、認証が成功しなかった場合の書込み動作が終了する。

【００４５】

このように書込み動作時において、認証パスワード設定コマンドを受信し、認証が成功した場合も、成功しなかった場合も書込みデータの記録が行われる。しかし、認証が成功

しなかった場合、記録媒体２０を装置本体部１０から取出す動作を行うことにより、書込みデータの記録位置情報２４ａが消去されているため、不揮発性メモリ２５のデータ記録領域２５ｃに記録された書込みデータの読出しは困難となる。

【００４６】

図４は、書込み動作時において、認証パスワード設定コマンドを受信しない場合の動作フローを示すフローチャートである。

【００４７】

この場合、装置本体部１０から認証パスワードの入力は行われなく、揮発性メモリ２４に記憶されている認証フラグが、認証済みであることを示す認証フラグ［１］であるか、認証フラグ［０］であるかの判断を実行する（ステップＳ４０１）。

【００４８】

揮発性メモリ２４内に記憶されている情報が認証済みの場合は、ステップＳ４０２において装置本体部１０から送られる書込みデータを暗号化する。書込みデータの暗号化動作は、暗号・復号制御部２３ｂにより、装置本体部１０から暗号書込コマンドを受信した場合に、装置本体部１０からレジスタ群２２ａの所定のアドレスに設定されたデータについて、暗号キー２５ａを用いて暗号化することにより行われる。そして、暗号化された書込みデータは、ステップＳ４０３において、不揮発性メモリ２５のデータ記録領域２５ｃに記録される。

【００４９】

ステップＳ４０４において、不揮発性メモリ２５のデータ記録領域２５ｃへの書込みデータの記録が終了した後、ステップＳ４０５において、記録媒体２０を装置本体部１０から取出す動作を行うと、揮発性メモリ２４に記憶されている認証済みであることを示す認証フラグが初期化される（ステップＳ４０６）。これにより、認証パスワード設定コマンドを受信し、認証が成功した場合の書込み動作が終了する。

【００５０】

一方、ステップＳ４０１において、揮発性メモリ２４内に記憶されている情報が認証フラグ［０］である場合は、揮発性メモリ２４は、未認証の書込みデータの記録位置情報２４ａを書込む（ステップＳ４０７）。

【００５１】

その後は、認証済みの場合と同様、ステップＳ４０２において装置本体部１０から送られる書込みデータを暗号化し、暗号化された書込みデータは、ステップＳ４０３において、不揮発性メモリ２５のデータ記録領域２５ｃに記録される。不揮発性メモリ２５のデータ記録領域２５ｃへの書込みデータの記録が終了し（ステップＳ４０４）、記録媒体２０を装置本体部１０から取出す動作（ステップＳ４０５）を行うと、ステップＳ４０６において、揮発性メモリ２４に記憶されている認証フラグが初期化されるとともに、未認証の書込みデータの記録位置情報２４ａのデータも消去される。これにより、未認証の場合の書込み動作が終了する。

【００５２】

このように書込み動作時において、認証パスワード設定コマンドを受信しなかった場合において、記録媒体２０が認証済みか、未認証状態かにかかわらず書込みデータの記録が行われる。しかし、未認証状態の場合、記録媒体２０を装置本体部１０から取出す動作を行うことにより、書込みデータの記録位置情報２４ａが消去されているため、不揮発性メモリ２５のデータ記録領域２５ｃに記録された書込みデータの読出しは困難となる。

【００５３】

次に、本技術による記録媒体において、記録媒体に記録されているデータの読出し動作について説明する。

【００５４】

図５は、読出し動作時の動作フローを示すフローチャートである。

【００５５】

装置本体部１０から読出しコマンドが入力されると、まず、制御プログラム２３ａが揮

発性メモリ２４のステータスを参照する。すなわち、揮発性メモリ２４に記憶されている認証フラグが、認証済みであることを示す認証フラグ［１］であるか、認証フラグ［０］であるかの判断を実行する（ステップＳ５０１）。

【００５６】

揮発性メモリ２４内に記憶されている情報が認証済みの場合は、データの読出しが可能なため、不揮発性メモリ２５のデータ記録領域２５ｃからのデータの読出し（ステップＳ５０２）、読出しデータの復号化動作（ステップＳ５０３）が実行され、データの読出し動作が終了する（ステップＳ５０４）。データの復号化は、ステップＳ５０３において、記憶部２３の暗号・復号制御部２３ｂにより、暗号キー２５ａを復号キーとして実行する。複合化したデータは、制御プログラム２３ａによりレジスタ群２２ａの所定のアドレスに記録し、装置本体部１０にデータ伝送可能な状態とする。

【００５７】

揮発性メモリ２４内に記憶されている情報が認証フラグ［０］で、未認証の場合は、揮発性メモリ２４に記録位置情報２４ａが存在するか否かを確認するためにステップＳ５０５に進む。ステップＳ５０５において、記録位置情報２４ａが存在する場合、次のステップＳ５０６において、その記録位置情報２４ａのデータ読出し動作を実行する。その後は、記録位置情報２４ａに基づき、認証済みの場合と同様に、不揮発性メモリ２５のデータ記録領域２５ｃからのデータの読出し（ステップＳ５０２）、読出しデータの復号化動作（ステップＳ５０３）が実行され、データの読出し動作が終了する（ステップＳ５０４）。ステップＳ５０５において、記録位置情報２４ａが存在しない場合はエラー終了となる。

【００５８】

なお、記録位置情報２４ａが存在するか否かの確認は、制御プログラム２３ａにより、記録位置情報２４ａにおいて、装置本体部１０からの読込みコマンドの引数として設定された読込みアドレスのセクタに相当するビットの値を参照することで行う。該当ビットが［１］の場合は、記録位置情報ありと判定して、ステップＳ５０６に進む。該当ビットが［０］の場合は、記録位置情報なしと判定し、レジスタ群２２ａにおいて、エラーを通知するためのレジスタを設定し、装置本体部１０にエラーを通知し、終了する。

【００５９】

また、揮発性メモリ２４内に記憶されている情報が認証フラグ［０］の場合であっても、書込み動作において、認証パスワード設定コマンドを受信し、認証が成功した場合に書き込まれたデータは読出しが可能なため、認証パスワードの判定を行うステップＳ５０７に進む。

【００６０】

ステップＳ５０７においては、書込み動作時と同様に、装置本体部１０から認証パスワードを受信する。その後、ステップＳ５０８において、入力された認証パスワードが一致するか否かの判断を行い、認証パスワードが一致した場合は、認証済みの場合と同様、データの読出し（ステップＳ５０２）、読出しデータの復号化動作（ステップＳ５０３）が実行され、データの読出し動作が終了する（ステップＳ５０４）。認証パスワードが一致しない場合は、データの読出し動作が行われず、終了となる。

【００６１】

このように読出し動作において、揮発性メモリ２４に記憶されている認証フラグが、認証済みであることを示すフラグか否かの判定を行い、認証済みでない場合であっても、揮発性メモリ２４に記録位置情報２４ａが存在する場合は不揮発性メモリ２５のデータ記録領域２５ｃに書き込まれたデータを読み出すことが可能である。勿論、未認証の状態であっても、書込み動作において、認証が成功した場合に書き込まれたデータは、認証パスワードが一致した場合は読出しが可能となる。

【００６２】

以上のように本技術による記録媒体は、暗号化されたデータを記録する不揮発性メモリ２５と、認証パスワードによる認証済みか否かを示す認証フラグ、及び認証フラグが未認

証であることを示す場合に不揮発性メモリ２５に記録したデータの記録位置情報２４ａを記憶する揮発性メモリ２４とを有している。これにより、認証パスワードを取得できなかった場合も、揮発性メモリ２４に記録位置情報２４ａを記憶しておくことにより、不揮発性メモリ２５にデータを暗号化して記録することができるとともに、揮発性メモリ２４の記録位置情報２４ａを参照することにより暗号化されたデータを復号化して読み出すことが可能となる。したがって、記録媒体２０を装置本体部１０に装填した状態であれば、パスワード認証を行わなくても、装置本体部１０から伝送されるデータの書込み動作、及び読出し動作を行うことができる。

【００６３】

しかも、記録媒体２０を装置本体部１０から取出すことにより、揮発性メモリ２４に記憶された認証フラグが初期化されるとともに、記録位置情報２４ａも消去される。これにより、認証パスワードを取得していない状態で記録媒体２０の不揮発性メモリ２５に記録されたデータは読出し動作が行えないため、認証パスワードによるセキュリティ機能も持たせることが可能である。

【００６４】

報道などで使用される業務用の撮影装置に使用される記録媒体おいては、電源を入れた後、すぐに撮影を開始できるという即時性を持つ動作と、記録されたデータの機密性を確保する動作が求められている。本技術による記録媒体は、装置本体部１０に装填した状態、すなわち電源の供給を開始した段階で、直ぐに撮影したデータの書込み動作と読出し動作を行うことが可能で、即時性を持つ動作を持たせることができる。しかも、装置本体部１０から取出し、電源の供給を停止することにより、認証パスワードによる認証動作を行わずに記録されたデータの読出し動作が不可能になるため、記録情報の機密性も確保することが可能となる。

【００６５】

以上のように、本開示における技術の例示として、実施の形態を説明した。そのために、添付図面及び詳細な説明を提供した。したがって、添付図面及び詳細な説明に記載された構成要素の中には、課題解決のために必須な構成要素だけでなく、上記技術を例示するために、課題解決のためには必須でない構成要素も含まれ得る。そのため、それらの必須ではない構成要素が添付図面や詳細な説明に記載されていることをもって、直ちに、それらの必須ではない構成要素が必須であるとの認定をするべきではない。

【００６６】

また、上述の実施の形態は、本開示における技術を例示するためのものであるから、請求の範囲またはその均等の範囲において種々の変更、置き換え、付加、省略などを行うことができる。

【産業上の利用可能性】

【００６７】

以上のように本技術にかかる記録媒体は、業務用の撮影装置などのように即時性を持つ動作と、記録されたデータの機密性を確保する動作が求められる機器に使用する記録媒体として有用な発明である。

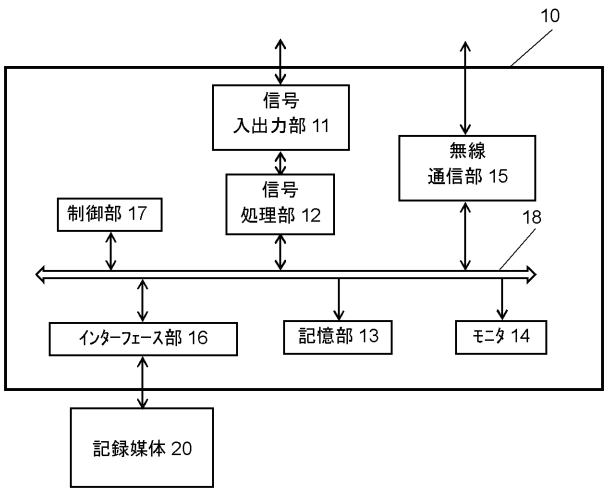
【符号の説明】

【００６８】

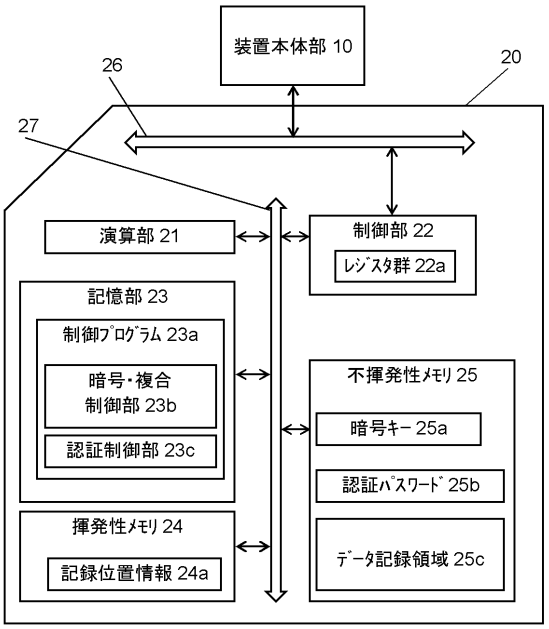
１０　装置本体部
１１　信号入出力部
１２　信号処理部
１３　記憶部
１４　モニタ
１５　無線通信部
１６　インターフェース部
１７　制御部
１８，２６，２７　バス

２０　記録媒体
２１　演算部
２２　制御部
２２ａ　レジスタ群
２３　記憶部
２３ａ　制御プログラム
２３ｂ　暗号・復号制御部
２３ｃ　認証制御部
２４　揮発性メモリ
２４ａ　記録位置情報
２５　不揮発性メモリ
２５ａ　暗号キー
２５ｂ　認証パスワード
２５ｃ　データ記録領域

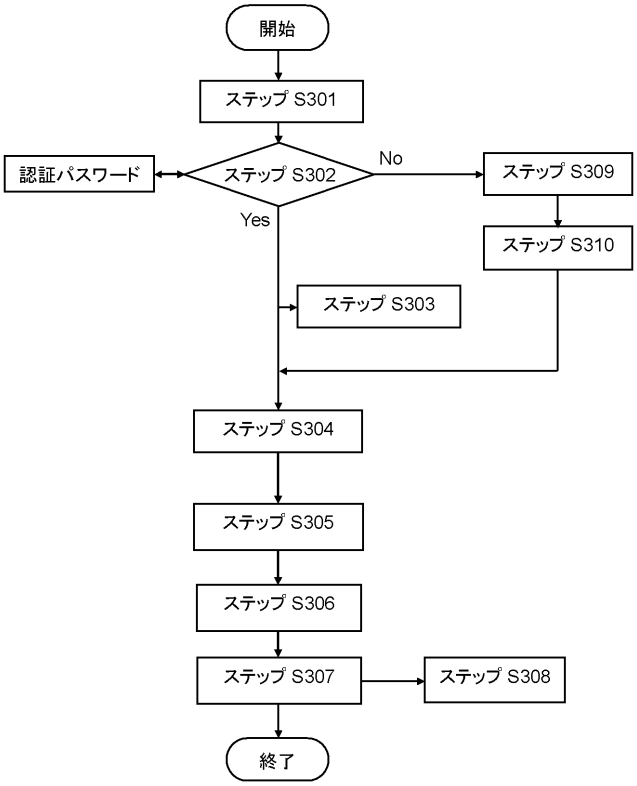
【図１】



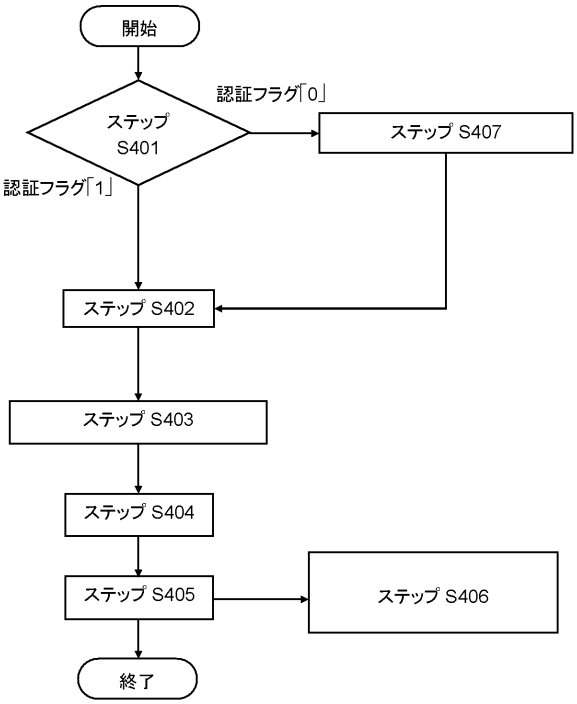
【図２】



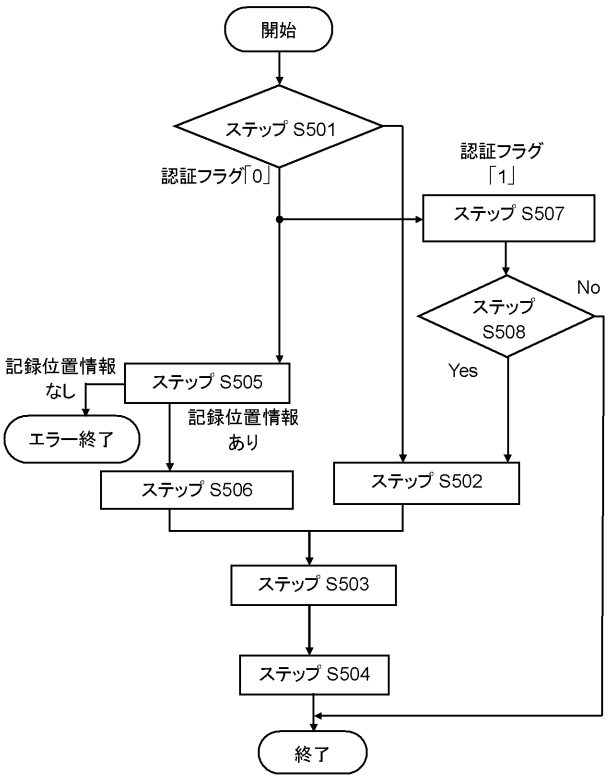
【図３】


開始
ステップ S301
認証パスワード
ステップ S302
No
ステップ S309
Yes
ステップ S310
ステップ S303
ステップ S304
ステップ S305
ステップ S306
ステップ S307
ステップ S308
終了

【図４】


開始
ステップ S401
認証フラグ「0」
ステップ S407
認証フラグ「1」
ステップ S402
ステップ S403
ステップ S404
ステップ S405
ステップ S406
終了

【図５】


開始
ステップ S501
認証フラグ「0」
認証フラグ「1」
ステップ S507
ステップ S508
No
Yes
記録位置情報なし
ステップ S505
エラー終了
記録位置情報あり
ステップ S506
ステップ S502
ステップ S503
ステップ S504
終了

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
Ｈ０４Ｎ　5/91	***(2006.01)***	Ｈ０４Ｎ	5/91	Ｚ