

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4751632号  
(P4751632)

(45) 発行日 平成23年8月17日(2011.8.17)

(24) 登録日 平成23年5月27日(2011.5.27)

(51) Int. Cl.	F I				
HO4N 1/00 (2006.01)	HO4N	1/00			C
GO3G 21/00 (2006.01)	GO3G	21/00	388		
GO6F 21/24 (2006.01)	GO6F	12/14	530C		
HO4L 9/08 (2006.01)	GO6F	12/14	540A		
HO4N 1/21 (2006.01)	HO4L	9/00	601A		
請求項の数 1 (全 19 頁) 最終頁に続く					

(21) 出願番号 特願2005-99104 (P2005-99104)  
 (22) 出願日 平成17年3月30日(2005.3.30)  
 (65) 公開番号 特開2006-279816 (P2006-279816A)  
 (43) 公開日 平成18年10月12日(2006.10.12)  
 審査請求日 平成20年1月11日(2008.1.11)

(73) 特許権者 000006747  
 株式会社リコー  
 東京都大田区中馬込1丁目3番6号  
 (74) 代理人 100090103  
 弁理士 本多 章悟  
 (74) 代理人 100067873  
 弁理士 樺山 亨  
 (72) 発明者 阪上 弘文  
 東京都大田区中馬込1丁目3番6号・株式会社リコー内  
 審査官 堀井 啓明

最終頁に続く

(54) 【発明の名称】 画像形成装置

(57) 【特許請求の範囲】

【請求項1】

入力されたデータを記憶する記憶装置と、  
 上記記憶装置内のデータを記録媒体に記録再生する情報記録再生装置と  
 を有する画像形成装置であって、  
 上記情報記録再生装置は、  
 上記記録媒体にデータを記録する時にデータを暗号化して上記記録媒体に記録させる暗号化手段と、  
 上記記録媒体からデータを再生する時に上記記録媒体から再生したデータを復号化する復号化手段と、  
 上記暗号化と上記復号化に使用する、上記情報記録再生装置に固有の暗号鍵を記憶する手段とを有し、  
 上記情報記録再生装置が  
破損した別の情報記録再生装置に固有の暗号鍵を記憶する記憶手段を有し、  
 上記別の情報記録再生装置に固有の暗号鍵をデータの復号化に使用し、  
 上記情報記録再生装置が  
 上記情報記録再生装置の製造番号を記憶する手段と、  
 上記情報記録再生装置に固有のデータを記憶する手段とを有し、  
 上記情報記録再生装置の製造番号と上記固有のデータを暗号化して上記記録媒体に記録し、

上記記録媒体に記録された暗号化された製造番号と固有のデータを復号化し、

上記復号化された製造番号と上記情報記録再生装置に記憶された製造番号とが一致し、かつ、上記復号化された固有のデータと上記情報記録再生装置に記憶された固有のデータとが一致した時に、上記記録媒体から再生されたデータを復号化して上記記憶装置に入力し、

上記破損した上記別の情報記録再生装置の固有の暗号鍵を上記記憶手段に追加して記憶し、上記記憶手段は上記固有の暗号鍵が複数個追加して記憶される

ことを特徴とする画像形成装置。

【発明の詳細な説明】

【技術分野】

10

【0001】

本発明は、内蔵するハードディスク装置等の記憶装置に記憶されたデータのバックアップが行える複写機、プリンタ、ファクシミリ等の画像形成装置に関する。

【背景技術】

【0002】

特許文献1には、内蔵したハードディスク装置内のデータをバックアップする時に、省エネルギー性を損なわないように、バックアップに要する時間を予測して、スリープモードへの移行タイミングから、予測時間分だけさかのぼってバックアップを開始する複写機が記載されている。

【0003】

20

特許文献2には、ドキュメントの取扱いルールを記述したセキュリティポリシーに基づいて、ドキュメントの管理を行えるように、セキュリティポリシーを保持する手段と、セキュリティポリシーを書換える手段と、セキュリティポリシーに従って動作を制御する手段とを有する画像形成装置が記載されている。

【0004】

【特許文献1】特開2004 148609

【特許文献2】特開2004 166241

【発明の開示】

【発明が解決しようとする課題】

【0005】

30

特許文献1記載の複写機では、バックアップされたデータの機密保持に関する記述が無く、容易に関係者以外にデータが漏洩する危険がある。

特許文献2記載の画像形成装置では、情報システム（画像形成装置）内のデータに関してはセキュリティポリシーに基づいた管理が行われるが、着脱可能な記録媒体に記録されたバックアップデータの機密保持に関する記述が無く、容易に関係者以外にデータが漏洩する危険がある。

【0006】

本発明の目的は、内蔵する記憶装置内のデータを、着脱可能な記録媒体に記録したバックアップデータの機密を保持することができる画像形成装置を提供することにある。

本発明の他の目的は、記録を行った情報記録再生装置でしかデータを再生できず、記録媒体に記録したバックアップデータの機密を保持することができる画像形成装置を提供することにある。

40

【0007】

本発明の他の目的は、別の情報記録再生装置が破損した場合等に該別の情報記録再生装置によって記録された記録媒体からデータを再生できる画像形成装置を提供することにある。

本発明の他の目的は、暗号が解読されてもバックアップデータの機密を保持することができる画像形成装置を提供することにある。

【課題を解決するための手段】

【0008】

50

上記目的を達成するため、請求項 1 に係る発明は、入力されたデータを記憶する記憶装置と、上記記憶装置内のデータを記録媒体に記録再生する情報記録再生装置とを有する画像形成装置であって、上記情報記録再生装置は、上記記録媒体にデータを記録する時にデータを暗号化して上記記録媒体に記録させる暗号化手段と、上記記録媒体からデータを再生する時に上記記録媒体から再生したデータを復号化する復号化手段と、上記暗号化と上記復号化に使用する、上記情報記録再生装置に固有の暗号鍵を記憶する手段とを有し、上記情報記録再生装置が破損した別の情報記録再生装置に固有の暗号鍵を記憶する記憶手段を有し、上記別の情報記録再生装置に固有の暗号鍵をデータの復号化に使用し、上記情報記録再生装置が上記情報記録再生装置の製造番号を記憶する手段と、上記情報記録再生装置に固有のデータを記憶する手段とを有し、上記情報記録再生装置の製造番号と上記固有のデータを暗号化して上記記録媒体に記録し、上記記録媒体に記録された暗号化された製造番号と固有のデータを復号化し、上記復号化された製造番号と上記情報記録再生装置に記憶された製造番号とが一致し、かつ、上記復号化された固有のデータと上記情報記録再生装置に記憶された固有のデータとが一致した時に、上記記録媒体から再生されたデータを復号化して上記記憶装置に入力し、上記破損した上記別の情報記録再生装置の固有の暗号鍵を上記記憶手段に追加して記憶し、上記記憶手段は上記固有の暗号鍵が複数個追加して記憶されることを特徴とするものである。

10

【発明の効果】

【0019】

本発明によれば、内蔵する記憶装置内のデータを、着脱可能な記録媒体に記録したバックアップデータの機密を保持することができる。

20

本発明によれば、記録を行った情報記録再生装置でしかデータを再生できず、記録媒体に記録したバックアップデータの機密を保持することができる。

本発明によれば、別の情報記録再生装置が破損した場合等に該別の情報記録再生装置によって記録された記録媒体からデータを再生できる。

本発明によれば、暗号が解読されてもバックアップデータの機密を保持することができる。

【発明を実施するための最良の形態】

【0020】

図 1 は、本発明の一実施形態である画像形成装置を示す。この実施形態では、書類を光学的に読み取るスキャナ 1 と、画像データを紙に印刷して出力するプリンタ 2 と、外部のコンピュータとネットワークで接続するためのネットワークインターフェース 3 と、電話回線に接続するモデム 4 と、スキャナ 1 で読み取ったデータを蓄積する記憶装置としてのハードディスク装置 5 と、このハードディスク装置 5 のデータを記録媒体としての光ディスク 6 に記録再生する光ディスク装置 7 と、本画像形成装置をユーザが操作するためのボタンやタッチパネル、文字や画像を表示するための液晶表示装置からなる操作部 8 と、本画像形成装置の動作を制御するための CPU (Central Processing Unit) 9 と、この CPU 9 がアクセスするデータを一時的に蓄積する RAM (Random Access Memory) 10 と、本画像形成装置の制御プログラムや固定データ等を記憶する ROM (Read Only Memory) 11 がシステムバス 12 に接続されている。これにより、本画像形成装置は、ファクシミリ、コピー機、スキャナ、プリンタ、データサーバとして機能する。

30

40

【0021】

例えば、操作部 8 からファクシミリの宛先番号を入力すると、CPU 9 は、ファクシミリ送信モードで、スキャナ 1 に送信原稿を読み取らせ、その読み取ったデータをハードディスク装置 5 によりハードディスクに保存した後にそのデータをモデム 4 を介して送信することにより、ファクシミリ送信を行う。CPU 9 は、ファクシミリ受信モードでは、モデム 4 で受信したファクシミリ受信データをハードディスク装置 5 によりハードディスクに保存し、プリンタ 2 で印刷出力することによりファクシミリ受信を行う。

【0022】

50

CPU9は、複写モードでは、スキャナ1で読み取った原稿画像データをハードディスク装置5によりハードディスクに保存し、その必要枚数分だけ、プリンタ2に繰返し出力して紙に印刷することにより、コピー機として機能させる。更に、データサーバモードでは、CPU9はスキャナ1で読み取った原稿画像データをハードディスク装置5によりハードディスクに保存し、その原稿画像データがネットワークインターフェース3を介して外部のコンピュータからダウンロードされたり、或いは、外部のコンピュータへ電子メールとして送信されたりすることにより、コンピュータ用のスキャナとして使用させる。

【0023】

また、外部コンピュータからネットワークインターフェース3を介して入力された画像や文書のデータはハードディスク装置5によりハードディスクに保存され、その後、そのデータがプリンタ2へ出力されて印刷されることにより、コンピュータ用のプリンタとして使用させる。更に、ハードディスク装置5によりハードディスクに保存されたデータは、ネットワークインターフェース3を介して外部の複数のコンピュータからアクセスできるので、オフィス等で業務データを共有するためのデータサーバとしても使用できる。そして、ハードディスク装置5のハードディスクに保存されたデータは、光ディスク装置7で光ディスク6に記録してバックアップを行う。

【0024】

図2は上記光ディスク装置7の構成を示す。情報を記録する記録媒体である光ディスク6には、らせん状又は同心円上のトラックが形成され、このトラックに沿ってデータを記録する。光ディスク6のトラックは、一定の周期でわずかに蛇行(wobble)し、その周波数変化や位相変化によって、光ディスク6の全面にわたるアドレスが前以て記録されている。光ディスク6はモータ13により回転させる。光ヘッド14は、レーザダイオードとレンズ等からなる光学系および光電変換素子が組込まれており、レーザダイオードからレンズ等を介して光ディスク6上にレーザ光を照射して光ディスク6にデータに対応するマークを記録し、その記録されたマークを上記レーザ光で走査してその反射光を光電変換素子で受光することにより電気信号を出力する。光ヘッド14から出力された電気信号は、演算増幅回路15で増幅され、光ディスク6上のマークに対応した再生信号や、レーザ光の焦点が光ディスク6の記録面に合っているかどうかを示すフォーカスエラー信号や、レーザ光が光ディスク6のトラックに沿って走査しているかどうかを示すトラッキングエラー信号や、トラックの蛇行に対応した信号等として出力される。

【0025】

サーボ回路16は、演算増幅回路15からのフォーカスエラー信号や、トラッキングエラー信号、トラックの蛇行に対応した信号により光ヘッド14内のレンズやモータ13を制御することで、レーザ光の焦点を光ディスク6の記録面に合わせ、レーザ光に正しくトラックを走査させ、光ディスク6を線速度一定又は、角速度一定で回転させる。尚、図示していないが、光ヘッド14を光ディスク6の半径方向に移動させ、光ディスク6上のデータをサーチする機構も備わっている。以上が、光ディスク6のトラックに対してマークの記録再生を行うための動作である。

【0026】

次に、上記光ディスク装置7の記録再生時のデータ処理について説明する。まず、バスインターフェース回路17は、光ディスク6へデータを記録するデータ記録時には、内蔵されているアドレスデコードによって、システムバス12から光ディスク装置7への入力データを検出して、これを暗号化復号化回路18に入力する。光ディスク6からデータを再生するデータ再生時には、バスインターフェース回路17は、暗号化復号化回路18から出力されたデータをシステムバス12へ出力する。

【0027】

暗号化復号化回路18は、光ディスク6へデータを記録するデータ記録時には、バスインターフェース回路17からの入力データを光ディスク装置7に固有の暗号鍵によって暗号化した後、誤り訂正符号化復号化回路19へ出力する。暗号化復号化回路18は、光ディスク6からデータを再生するデータ再生時には、データ記録時と同じ鍵を使用して誤り

10

20

30

40

50

訂正符号化復号化回路 19 からの暗号化されたデータを復号化してバスインターフェース回路 17 へ出力する。

【0028】

誤り訂正符号化復号化回路 19 は、光ディスク 6 へデータを記録するデータ記録時には、暗号化復号化回路 18 からの暗号化されたデータに誤り訂正を行うためのデータを付加して、変調復調回路 20 へ出力する。誤り訂正符号化復号化回路 19 は、光ディスク 6 からデータを再生するデータ再生時には、変調復調回路 20 からのデータに対してその付加されているデータを使用して誤り訂正復号化を行い、誤り訂正後のデータを暗号化復号化回路 18 へ出力する。

【0029】

変調復調回路 20 は、光ディスク 6 へデータを記録するデータ記録時には、記録信号の直流成分が少なくなり、かつ、信号の持つ周波数成分が所定の特性になるように、データの反転間隔が所定の規則に合うように誤り訂正符号化復号化回路 19 からのデータの変換を行うと同時に、そのデータに同期信号を挿入してレーザー駆動回路 21 へ出力する。ここでのデータの変換は、一般に、RLL (Run Length Limited) 変調と呼ばれる処理である。光ディスク 6 からデータを再生するデータ再生時には、データ検出回路 22 からの 2 値データに対して、データ検出回路 22 からの同期信号により、上記データの変換とは逆の変換 (復調) を行う。

【0030】

レーザー駆動回路 21 は、記録媒体としての光ディスク 6 上にレーザー光照射によって変調後の 2 値データに対応したマークとスペースを記録するために、変調復調回路 20 からのデータにより、光ヘッド 14 のレーザーダイオードを駆動する信号を生成する。光ディスク 6 からデータを再生するデータ再生時には、演算増幅回路 15 から出力された再生信号は、波形等化回路 23 によって波形等化が行われ、しきい値によって 2 値化する時のエラーを低減するように補正される。

【0031】

その後、波形等化回路 23 からの再生信号は、2 値化回路 24 にて所定のしきい値で 2 値化される。データ検出回路 22 は、2 値化回路 24 の出力信号から同期信号を検出し、更にデータ検出回路 22 に内蔵されている PLL 回路で、データに同期したクロック信号を生成する。データ検出回路 22 は、その生成したクロック信号によって 2 値化回路 24 からの 2 値化された信号を 0 と 1 の 2 値データとして検出して出力する。その後、データ検出回路 22 の出力信号は、変調復調回路 20 による復調、誤り訂正符号化復号化回路 19 による誤り訂正復号化、暗号化復号化回路 18 による暗号の復号化が行われ、バスインターフェース回路 17 を経て光ディスク装置 7 より出力される。

【0032】

上記で説明した光ディスク装置 7 の各回路は、光ディスク装置 7 の動作を制御するための CPU 25、RAM 26、ROM 27 と共にシステムバス 28 に接続されている。図 1 に示したシステムバス 12、CPU 9、RAM 10、ROM 11 は、画像形成装置内の構成部品である。光ディスク装置 7 には、これらとは別に、構成部品としてのシステムバス 28、CPU 25、RAM 26、ROM 27 がある。光ディスク 6 としては DVD+RW を使用し、光ヘッド 14 にはレーザー光の波長が 650nm であるレーザーダイオードを使用する。光ヘッド 14 には、より高密度記録ができる青レーザーを使用し、そのレーザー波長 (例えば、405nm) に対応した相変化型の光ディスクを使用しても良い。

【0033】

図 3 は、上記暗号化復号化回路 18 の内部構成を示す。暗号化復号化回路 18 は、暗号化回路 29 と、復号化回路 30 と、暗号化回路 29 に入力するデータを切替えるデータセレクタ 31 と、CPU 25 がシステムバス 28 を介して設定した種々のデータを保持する記憶装置としてのレジスタ 32 ~ 35、逆に CPU 25 が読み取るためのデータを保持する記憶装置としてのレジスタ 37、38 および、各レジスタ 32 ~ 35、37、38 のアドレスを検出するアドレスデコーダを内蔵し、CPU 25 と各レジスタ 32 ~ 35、37

10

20

30

40

50

、38の間のデータ転送を制御するバスインターフェース回路39から成る。

【0034】

暗号化および復号化に使用する暗号鍵は、ROM27やEEPROM等の不揮発性記憶手段に記憶されており、CPU25によってレジスタ32に設定される。暗号化回路29と復号化回路30は、レジスタ32に設定された暗号鍵が入力され、該暗号鍵によりデータの暗号化と復号化をそれぞれ行う。又、暗号鍵の他に、光ディスク装置7の製造番号と光ディスク装置7に固有のデータ(以下、固有データと呼ぶ)も、ROM27等の不揮発性記憶手段に記憶されて、それぞれをCPU25によってレジスタ33、34に設定できる。

【0035】

暗号化回路29は、データセクタ31によって、ハードディスク装置5からシステムバス12、バスインターフェース回路17を経由して入力されるデータ(図3に示す入力データ)と、レジスタ33、34に設定された製造番号と固有データとが切換えて入力される。データセクタ31は、その切換を、CPU25がレジスタ35に設定したデータセクタ制御データにより行う。例えば、データセクタ31は、データセクタ制御データを2ビットのデータとして、該データセクタ制御データが“00”と“11”の時にはバスインターフェース回路17からの入力データを選択して暗号化回路29に入力し、データセクタ制御データが“01”の時には光ディスク装置7の製造番号を選択して暗号化回路29に入力し、データセクタ制御データが“10”の時には固有データを選択して暗号化回路29に入力する。これにより、暗号化回路29の入力データが切換えられる。

【0036】

復号化回路30は、光ディスク6からデータを再生するデータ再生時には、レジスタ32に設定された、データ記録時と同じ暗号鍵を使用して誤り訂正符号化復号化回路19からの暗号化されたデータや製造番号、固有データを復号化する。復号化回路30の出力データのうちの製造番号と固有データは、それぞれレジスタ37、38に保持される。これによって、CPU25が光ディスク6に記録された製造番号や固有データがレジスタ37、38から読み取られる。

なお、本実施形態では暗号化と復号化に同じ暗号鍵(共有の暗号鍵)を使用しているの  
で、暗号化回路29の暗号方式には一例として米国の標準暗号方式であるAES(Advanced Encryption Standard)を使用するとよい。

【0037】

図4は、本実施形態のハードディスク装置5からのデータを光ディスク6に記録してバックアップを行う時に、光ディスク6に記録したバックアップデータの機密を守るための暗号鍵の使用方を説明するための図である。まず、本実施形態の画像形成装置40a、40bにそれぞれ内蔵した光ディスク装置7(以下7a、7bという)には、それぞれ固有の暗号鍵をROM27やEEPROM等の不揮発性記憶手段に記憶させ、それぞれ光ディスク6(以下6a、6bという)への記録時には暗号化回路29でその暗号鍵を使用してデータを暗号化する。従って、光ディスク6a、6bの記録されているデータは、記録した光ディスク装置でのみ再生でき、他の光ディスク装置や他の画像形成装置に内蔵した光ディスク装置では再生できない。ここでは、この暗号鍵を記録再生用暗号鍵と呼ぶ。

【0038】

本来、バックアップは、特定の画像形成装置に内蔵したハードディスク装置のハードディスクから再生したデータを外部の記録媒体(ここでは光ディスク)に記録し、再びハードディスク装置のハードディスクに戻す(記録する)のが目的であるので、光ディスクに記録したデータは該データを記録した光ディスク装置以外の光ディスク装置では再生できなくとも支障は無い。これにより、光ディスクの記録データは記録した光ディスク装置以外の他の光ディスク装置では再生できないので、バックアップデータの機密が守れる。

しかし、光ディスク装置が破損するなどして、該光ディスク装置を別の光ディスク装置に置換えた場合、破損した光ディスク装置で破損前に記録した光ディスクの記録データは

10

20

30

40

50

、破損した光ディスク装置に置換えた光ディスク装置では再生できない。或いは、内蔵する光ディスク装置が破損した画像形成装置自体を該画像形成装置と同様な構成の新機種の画像形成装置に置換えた場合、その新機種の画像形成装置が内蔵している光ディスク装置は破損した光ディスク装置とは別の光ディスク装置になるので、破損した光ディスク装置で記録したバックアップデータを別の光ディスク装置では再生できない。

**【 0 0 3 9 】**

このような光ディスク装置や画像形成装置の置換え時に限って、破損した光ディスク装置 7 b 又は他の画像形成装置が内蔵する光ディスク装置 7 b の記録再生用暗号鍵を再生専用暗号鍵として、新機種の画像形成装置における光ディスク装置 7 a 又は他の画像形成装置 4 0 b から置換した光ディスク装置 7 a の記録可能な不揮発性記憶手段に追加して記憶する。記録可能な不揮発性記憶手段に追加できる再生専用鍵の個数は、1 個に限らず、複数個追加できるようにする。こうすることにより、置換える前の光ディスク装置で記録した光ディスク 6 のデータを、置換えた後の光ディスク装置で再生できる。置換える前の光ディスク装置は廃棄する。

10

**【 0 0 4 0 】**

図 4 では、光ディスク装置を置換えた後の画像形成装置、および破損して置換えた光ディスク装置が画像形成装置 4 0 a および光ディスク装置 7 a である。他の画像形成装置の置換前の光ディスク装置、及び他の画像形成装置が光ディスク装置 7 b および画像形成装置 4 0 b である。光ディスク装置 7 a、7 b は、それぞれの記録再生用暗号鍵 1、2 を不揮発性記憶手段に記憶している。この段階では、それぞれの光ディスク装置 4 0 a、4 0 b で光ディスク 6、6 a に記録したデータは、記録した光ディスク装置でしか再生できない。破損した光ディスク装置 7 b を置換で新機種の画像形成装置 4 0 a に移さない画像形成装置 4 0 b、破損して置換が行われない光ディスク装置 7 b を廃棄する時は、光ディスク装置 7 b 内の ROM 2 7 等の不揮発性記憶手段に記憶されていた記録再生用暗号鍵 2 を再生専用暗号鍵 1 として光ディスク装置 4 0 a 内の不揮発性記憶手段に追加する。こうすることにより、光ディスク 6 b の記録データを画像形成装置 4 0 a および光ディスク装置 7 a で再生できる。

20

**【 0 0 4 1 】**

図 5 は、光ディスク装置 7 の製造番号と光ディスク装置 7 に固有のデータを使用しない場合において記録再生用暗号鍵によって暗号化されたデータが記録された光ディスク 6 からデータを再生する時の処理フローを示す。まず、ステップ S 1 で光ディスク装置 7 内の ROM 2 7 に記憶された記録再生用暗号鍵で復号化回路 3 0 により誤り訂正符号化復号化回路 1 9 からの暗号化されたデータ（光ディスク 6 から再生したデータ）が復号化される。この時、CPU 2 5 が ROM 2 7 内の記録再生用暗号鍵をレジスタ 3 2 に設定し、復号化回路 3 0 がレジスタ 3 2 からの記録再生用暗号鍵を用いて誤り訂正符号化復号化回路 1 9 からの暗号化されたデータを復号化することで、光ディスク 6 に暗号化されて記録されたデータを復号化する。CPU 2 5 は、ステップ S 2、S 3 で、その復号化した一部のデータを図 1 におけるシステムバス 1 2 を経由して操作部 8 の液晶表示装置で表示させることで、そのデータをユーザに確認させる。

30

**【 0 0 4 2 】**

光ディスク 6 に記録されていた暗号化されたデータを復号化する時は、異なる暗号鍵を使用しても、復号化されたデータが異常であるか否かは機械的には検出できないので、復号化されたデータが異常であるか否かは操作部 8 の液晶表示装置の表示データから人間による目視確認を行う。この確認の結果、データが正常であれば、操作部 8 のタッチパネル等でユーザが「OK」等の表示ボタンを押す。データが異常であれば、ユーザが「NG」等の表示ボタンを押す。「OK」ボタンが押されれば、CPU 2 5 は、その「OK」ボタンからの入力信号により、ステップ S 4 で光ディスク装置 7 に対して光ディスク 6 からデータを再生させて復号化回路 3 0 からバスインターフェース回路 1 7 を介して出力させることで該データをハードディスク装置 5 に入力させてハードディスクに記録させ、処理を終了する。

40

50

## 【 0 0 4 3 】

「 N G 」 ボタンが押された場合は、 C P U 2 5 は、その「 N G 」 ボタンからの入力信号により、ステップ S 5 で光ディスク装置 7 内の R O M 2 7 等の不揮発性記憶手段に再生専用暗号鍵が記憶されているか否かを判断し、 C P U 2 5 は、再生専用暗号鍵が R O M 2 7 等の不揮発性記憶手段に記憶されていない場合には、ステップ S 1 0 で操作部 8 の液晶表示装置に「データを再生できません。」等の警告を表示して、処理を終了する。

## 【 0 0 4 4 】

C P U 2 5 は、 R O M 2 7 等の不揮発性記憶手段に再生専用暗号鍵が記憶されていれば、ステップ S 6 で、その再生専用暗号鍵をレジスタ 3 2 に設定し、再び誤り訂正符号化復号化回路 1 9 からの暗号化されたデータ（光ディスク 6 から再生されたデータ）を復号化回路 3 0 で復号化させる。 C P U 2 5 は、ステップ S 7、 S 8 で、その復号化したデータの一部のデータを、操作部 8 の液晶表示装置で表示させることで、ユーザに復号化されたデータが異常であるか否かを確認させる。その確認の結果、「 O K 」 ボタンが押されれば、 C P U 2 5 は、「 O K 」 ボタンからの入力信号により、ステップ S 4 に飛んで光ディスク装置 7 に対して光ディスク 6 からデータを再生させて復号化回路 3 0 からバスインターフェイス回路 1 7 を介して出力させることで該データをハードディスク装置 5 に入力させてハードディスクに記録させ、処理を終了する。

## 【 0 0 4 5 】

C P U 2 5 は、「 N G 」 ボタンが押された場合には、ステップ S 9 で光ディスク装置 7 の R O M 2 7 等の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されているかを判断し、不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されていれば、ステップ S 6 に戻ってその再生専用暗号鍵をレジスタ 3 2 に設定して再び誤り訂正符号化復号化回路 1 9 からの暗号化されたデータを復号化回路 3 0 で復号化させる。

## 【 0 0 4 6 】

C P U 2 5 は、ステップ S 8 で更に「 N G 」 ボタンが押された場合には、ステップ S 9 で光ディスク装置 7 内の R O M 2 7 等の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されているかの判断を繰り返し、 R O M 2 7 等の不揮発性記憶手段に記憶されている再生専用暗号鍵がある限り「 O K 」 ボタンが押されるまで、ステップ S 6 に戻ってその再生専用暗号鍵をレジスタ 3 2 に設定して再び誤り訂正符号化復号化回路 1 9 からの暗号化されたデータを復号化回路 3 0 で復号化させる。 C P U 2 5 は、正常に復号化できる暗号鍵が光ディスク装置 7 内の R O M 2 7 等の不揮発性記憶手段に無い場合には、ステップ S 1 0 で操作部 8 の液晶表示装置に「データを再生できません。」等の警告を表示させて、処理を終了する。

## 【 0 0 4 7 】

こうすることにより、画像形成装置に内蔵したハードディスク装置 5 内のハードディスクの記録データを、光ディスク 6 へバックアップした時の光ディスク 6 に記録したバックアップデータの機密を守ることができる。又、他の光ディスク装置の記録再生用暗号鍵を再生専用暗号鍵として上記不揮発性記憶手段に記憶し、他の光ディスク装置で記録した光ディスクのデータも再生することができるので、画像形成装置や光ディスク装置の置換え時にも対応できる。

## 【 0 0 4 8 】

この場合、バックアップデータを記録した光ディスク 6 は、他の光ディスク装置では再生できないので、バックアップデータの機密を守ることができるが、画像形成装置から光ディスク装置が外されて、光ディスクと光ディスク装置とが盗まれると、バックアップデータが第三者に漏洩する。そこで、本実施形態の画像形成装置への光ディスク装置 7 の取付けと取外しには、機械的な鍵を併用すると良い。この鍵は、画像形成装置とは別の場所に保管する。又、機械的な鍵には無線タグを内蔵し、鍵と鍵穴の機構部とで暗号を送受信して鍵の解除と施錠を行うようにすれば、機械的に鍵を複製しても第三者が鍵を解除できなくなるので尚良い。

## 【 0 0 4 9 】



上記の場合では、光ディスクに記録するデータだけを暗号化したが、更に光ディスク装置7の製造番号も暗号化して光ディスク6に記録し、データ再生時に、光ディスク6から読み出した光ディスク装置7の製造番号と、再生を行っている光ディスク装置7の製造番号とを比較し、両者が一致する時のみデータを出力するようにして、バックアップデータの機密保守の安全性を向上させる場合について以下に説明する。この場合は、悪意のある第三者が、光ディスクを盗み、光ディスク装置7とは別の同機種の光ディスク装置を入手して、光ディスクの暗号鍵を解読した場合でも、盗んだ光ディスクのデータを再生できないようにする効果がある。

#### 【0050】

まず、光ディスク6に光ディスク装置7の製造番号を暗号化して記録する動作を説明する。CPU25は、図3に示すように、レジスタ33に光ディスク装置7の製造番号を設定し、データセクタ31が光ディスク装置7の製造番号を選択するためのデータセクタ制御データをレジスタ35に設定する。そして、レジスタ33に設定された光ディスク装置7の製造番号は、レジスタ35に設定されたデータセクタ制御データによりデータセクタ31で選択されて暗号化回路29で暗号化され、誤り訂正符号化復号化回路19へ出力されることで、光ディスク6に記録される。

10

#### 【0051】

CPU25は、バスインターフェース回路17からの入力データを暗号化して光ディスク6に記録する時には、データセクタ31からの入力データを選択するためのデータセクタ制御データをレジスタ35に設定する。したがって、バスインターフェース回路17からの入力データは、レジスタ35に設定されたデータセクタ制御データによりデータセクタ31で選択されて暗号化回路29で暗号化され、誤り訂正符号化復号化回路19へ出力されることで、光ディスク6に記録される。

20

#### 【0052】

又、図4において、画像形成装置40bの記録再生用暗号鍵2を画像形成装置40aの再生専用暗号鍵1として上記不揮発性記憶手段に追加する時には、画像形成装置40bの光ディスク装置7bの製造番号も光ディスク装置7aの不揮発性記憶手段に追加して記憶する。このように、光ディスク装置7aに固有の暗号鍵と製造番号を対で使用する。

#### 【0053】

図6は、光ディスク装置7aに固有の暗号鍵と製造番号を対で使用する場合において光ディスク6からバックアップデータを再生する時の処理フローを示す。まず、ステップS11で光ディスク装置7内のROM27に記憶された記録再生用暗号鍵で復号化回路30により誤り訂正符号化復号化回路19からの暗号化されたデータ(光ディスクから再生されたデータ)が復号化される。この時、CPU25はROM27内の記録再生用暗号鍵をレジスタ32に設定し、復号化回路30がレジスタ32からの記録再生用暗号鍵を用いて誤り訂正符号化復号化回路19からの暗号化された光ディスク装置7の製造番号を復号化し、その復号化した光ディスク装置7の製造番号がレジスタ37に保持される。次に、CPU25は、ステップS12で、レジスタ37に保持された光ディスク装置7の製造番号を光ディスク装置7の不揮発性記憶手段に記憶されている光ディスク装置7の製造番号と比較して両者が一致するか否かを判断し、両者が一致した場合にはステップS13で光ディスク装置7に対して光ディスク6からデータを再生させて復号化回路30からバスインターフェース回路17を介して出力させることで該データをハードディスク装置5に入力させてハードディスクに記録させ、処理を終了する。

30

40

#### 【0054】

CPU25は、両者が一致しない場合には、ステップS14で光ディスク装置7内の不揮発性記憶手段に再生専用暗号鍵が記憶されているか否かを判断し、CPU25は、再生専用暗号鍵が光ディスク装置7内の不揮発性記憶手段に記憶されていない場合には、ステップS18で操作部8の液晶表示装置に「データを再生できません。」等の警告を表示して、処理を終了する。

#### 【0055】

50

CPU25は、光ディスク装置7内の不揮発性記憶手段に再生専用暗号鍵が記憶されていれば、ステップS15で、その再生専用暗号鍵をレジスタ32に設定し、再び誤り訂正符号化復号化回路19からの(光ディスク6から再生された)光ディスク装置の製造番号を復号化回路30で復号化させる。CPU25は、ステップS16で、その復号化した光ディスク装置の製造番号が光ディスク装置7内の不揮発性記憶手段に記憶されている再生専用暗号鍵に対応する光ディスク装置の製造番号と一致するか否かを判断し、両者が一致すればステップS13に進んで光ディスク装置7に対して光ディスク6からデータを再生させて復号化回路30からバスインターフェース回路17を介して出力させることでデータをハードディスク装置5に入力させてハードディスクに記録させ、処理を終了する。

【0056】

更に、CPU25は、両者が一致しなければ、ステップS17で光ディスク装置7の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されているか否かを判断し、光ディスク装置7内の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されていれば、ステップS15に戻ってその再生専用暗号鍵をレジスタ32に設定して再び誤り訂正符号化復号化回路19からの暗号化された光ディスク装置の製造番号を復号化回路30で復号化させる。

【0057】

CPU25は、ステップS16で更に両者が一致しない場合には、ステップS17で光ディスク装置7内の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されているか否かの判断を繰返し、光ディスク装置7内の不揮発性記憶手段に記憶されている再生専用暗号鍵がある限りステップS16で更に両者が一致するまで、ステップS15に戻ってその再生専用暗号鍵をレジスタ32に設定して再び誤り訂正符号化復号化回路19からの暗号化された光ディスク装置の製造番号を復号化回路30で復号化させる。CPU25は、光ディスク装置の製造番号を正常に復号化できる暗号鍵が光ディスク装置7内の不揮発性記憶手段に無い場合には、ステップS18で操作部8の液晶表示装置に「データを再生できません。」等の警告を表示させて、処理を終了する。

【0058】

こうすることにより、暗号が解読されても、画像形成装置に内蔵したハードディスク装置5内のハードディスクの記録データを、光ディスク6へバックアップした時の光ディスク6に記録したバックアップデータの機密を守ることができる。又、他の光ディスク装置の記録再生用暗号鍵を再生専用暗号鍵として光ディスク装置7aの不揮発性記憶手段に記憶し、更に該他の光ディスク装置の製造番号も光ディスク装置7aの不揮発性記憶手段に記憶するので、他の光ディスク装置で記録した光ディスクのデータも再生でき、画像形成装置や光ディスク装置の置換え時にも対応できる。

【0059】

更に、光ディスクからデータを再生する時に、光ディスクから読み出した光ディスク装置の製造番号と再生を行っている光ディスク装置の製造番号とを比較し、両者が一致する時のみデータを出力するようにしているので、悪意のある第三者が、光ディスクを盗み、別の同機種的光ディスク装置を入手して、暗号鍵を解読した場合でも、盗んだ光ディスクのデータを再生できないようにする効果がある。

【0060】

上記の場合では、光ディスク装置の製造番号も暗号化して光ディスクに記録した。しかし、光ディスク装置の製造番号も第三者には分ってしまう恐れがある。そこで、個々の光ディスク装置に固有のデータを割当て、光ディスクにデータを暗号化して記録する時に、そのデータへ一定間隔毎に上記固有データを挿入する場合について説明する。この場合は、データ再生時に、光ディスクから読み出したデータに挿入された固有データと再生を行っている光ディスク装置の固有データとを比較し、両者が一致する時のみ光ディスクから読み出したデータを出力するようにして、バックアップデータの機密保守の安全性を向上させる。これは、悪意のある第三者が、光ディスクを盗み、光ディスク装置7とは別の同機種的光ディスク装置を入手して、暗号鍵と製造番号を解読した場合でも、盗んだ光ディスクのデータを再生できないようにする効果がある。

10

20

30

40

50

## 【 0 0 6 1 】

まず、光ディスク6に記録するデータに光ディスク装置7の固有データを挿入し、これを暗号化して光ディスク6に記録する動作を説明する。光ディスク装置7に固有のデータとしては、例えば、1と0から成る128ビットの乱数を発生し、これを個々の光ディスク装置に割当てて光ディスク装置7の不揮発性記憶手段に記憶させる。CPU25は、図3に示すように、光ディスク装置7の固有データを光ディスク装置7の不揮発性記憶手段から読み出してレジスタ34に設定する。そして、CPU25は、データセクタ31が入力を切換えることで、ハードディスク装置5からシステムバス28、バスインターフェース回路17を経由して入力されるデータに対して一定間隔毎に上記固有データを挿入するように、データセクタ制御データをレジスタ35に設定する。したがって、データセクタ31はハードディスク装置5からシステムバス28、バスインターフェース回路17を経由して入力されるデータに対して一定間隔毎にレジスタ34に設定された光ディスク装置の固有データを挿入する。データセクタ31の出力は、暗号化回路29によりレジスタ32に設定された暗号鍵で暗号化されて誤り訂正符号化復号化回路19へ出力されることで、光ディスク6に記録される。

10

## 【 0 0 6 2 】

又、図4に示すように、画像形成装置40bの記録再生用暗号鍵2を画像形成装置40aの再生専用暗号鍵1として光ディスク装置7aの不揮発性記憶手段に追加する時には、画像形成装置40bの光ディスク装置7bの固有データも光ディスク装置7aの不揮発性記憶手段に追加して記憶する。このように、光ディスク装置7に固有の暗号鍵と固有データを対で使用する。

20

## 【 0 0 6 3 】

図7は、光ディスク装置7に固有の暗号鍵と固有データを対で使用する場合において光ディスク6からバックアップデータを再生する時の処理フローを示す。まず、ステップS21で光ディスク装置7内の不揮発性記憶手段に記憶された記録再生用暗号鍵で復号化回路30により誤り訂正符号化復号化回路19からの暗号化されたデータが復号化される。この時、CPU25は光ディスク装置7内の不揮発性記憶手段内の記録再生用暗号鍵をレジスタ32に設定し、復号化回路30がレジスタ32からの記録再生用暗号鍵を用いて誤り訂正符号化復号化回路19からの光ディスク6の読み取りデータを復号化し、CPU25はその復号化したデータから光ディスク装置7に固有のデータを検出してレジスタ38に保持させる。

30

## 【 0 0 6 4 】

次に、CPU25は、ステップS22で、レジスタ38に保持された固有データを光ディスク装置7内の不揮発性記憶手段に記憶されている固有データと比較して両者が一致するか否かを判断し、両者が一致した場合にはステップS23で光ディスク装置7に対して光ディスク6からデータを再生させて復号化回路30からバスインターフェース回路17を介して出力させることで該データをハードディスク装置5に入力させてハードディスクに記録させ、処理を終了する。CPU25は、両者が一致しない場合には、ステップS24で光ディスク装置7内の不揮発性記憶手段に再生専用暗号鍵が記憶されているか否かを判断し、再生専用暗号鍵が光ディスク装置7内の不揮発性記憶手段に記憶されていないならば、ステップS28で操作部8の液晶表示装置に「データを再生できません。」等の警告を表示して、処理を終了する。

40

## 【 0 0 6 5 】

CPU25は、光ディスク装置7内の不揮発性記憶手段に再生専用暗号鍵が記憶されていれば、ステップS25に戻って、その再生専用暗号鍵をレジスタ32に設定し、再び誤り訂正符号化復号化回路19からの暗号化されたデータ(光ディスク6から再生されたデータ)を復号化回路30で復号化させ、その復号化したデータから固有データを検出する。CPU25は、ステップS26で、その復号化した固有データと、光ディスク装置7内の不揮発性記憶手段に記憶されている再生専用暗号鍵に対応する固有データとが一致するか否かを判断し、両者が一致すればステップS23に進んで光ディスク装置7に対して光

50

ディスク6からデータを再生させて復号化回路30からバスインターフェース回路17を介して出力させることで該データをハードディスク装置5に入力させてハードディスクに記録させ、処理を終了する。

【0066】

更に、CPU25は、両者が一致しなければ、ステップS27で光ディスク装置7の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されているか否かを判断し、光ディスク装置7内の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されていれば、ステップS25に戻ってその再生専用暗号鍵をレジスタ32に設定して再び誤り訂正符号化復号化回路19からの暗号化されたデータを復号化回路30で復号化させる。

【0067】

CPU25は、ステップS26で更に両者が一致しない場合には、ステップS27で光ディスク装置7内の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されているか否かの判断を繰返し、光ディスク装置7内の不揮発性記憶手段に記憶されている再生専用暗号鍵がある限りステップS26で更に両者が一致するまで、ステップS27からステップS25に戻ってその再生専用暗号鍵をレジスタ32に設定して再び誤り訂正符号化復号化回路19からの暗号化されたデータを復号化回路30で復号化させる。CPU25は、データを正常に復号化できる暗号鍵が光ディスク装置7内の不揮発性記憶手段に無い場合には、ステップS28で操作部8の液晶表示装置に「データを再生できません。」等の警告を表示させて、処理を終了する。

【0068】

こうすることにより、暗号が解読されても、画像形成装置に内蔵したハードディスク装置5内のハードディスクの記録データを、光ディスク6へバックアップした時の光ディスク6に記録したバックアップデータの機密を守ることができる。又、他の光ディスク装置の記録再生用暗号鍵を再生専用暗号鍵として不揮発性記憶手段に記憶し、更にその光ディスク装置の製造番号も記憶するので、他の光ディスク装置で記録した光ディスクのデータも再生でき、画像形成装置や光ディスク装置の置換え時にも対応できる。

【0069】

更に、光ディスクからデータを再生する時に、光ディスクから読み出した固有データと、再生を行っている光ディスク装置の固有データとを比較し、両者が一致する時のみデータを出力するようにしているので、悪意のある第三者が、光ディスクを盗み、別の同機種

【0070】

の光ディスク装置を入手して、暗号鍵を解読した場合でも、盗んだ光ディスクの記録データを再生できないようにする効果がある。

【0071】

上記の実施形態では、光ディスク装置の製造番号か固有データのどちらかを使用しているが、光ディスク装置の製造番号と固有データの両方を組合せると、更に光ディスクに記録したバックアップデータの機密保守の安全性を向上させることができる。以下に本実施形態において光ディスク装置の製造番号と固有データの両方を組合せて使用する場合について説明する。

【0071】

まず、光ディスク6に対して、光ディスク装置の固有データをデータに挿入し、更にそのデータと光ディスク装置の製造番号を暗号化して記録する動作を説明する。CPU25は、図3に示すように、レジスタ33に光ディスク装置7の製造番号を設定し、レジスタ34に光ディスク装置7の固有データを設定する。さらに、CPU25は、データセクタ31が光ディスク装置7の製造番号を選択するためのデータセクタ制御データをレジスタ35に設定し、レジスタ33に設定された光ディスク装置7の製造番号をデータセクタ31を介して暗号化回路29で暗号化させて誤り訂正符号化復号化回路19へ出力させることで、光ディスク6に記録させる。次に、CPU25は、ハードディスク装置5からシステムバス28、バスインターフェース回路17を経由して入力されるデータに対して一定間隔毎に上記固有データを挿入するように、データセクタ制御データをレジスタ35に設定する。したがって、データセクタ31はハードディスク装置5からシステム

10

20

30

40

50

バス 28、バスインターフェース回路 17 を経由して入力されるデータに対して一定間隔毎にレジスタ 34 に設定された光ディスク装置の固有データを挿入する。データセレクタ 31 の出力は、暗号化回路 29 によりレジスタ 32 に設定された暗号鍵で暗号化されて誤り訂正符号化復号化回路 19 へ出力されることで、光ディスク 6 に記録される。

【0072】

又、CPU 25 は、図 4 に示すように、画像形成装置 40b の記録再生用暗号鍵 2 を画像形成装置 40a の再生専用暗号鍵 1 として光ディスク装置 7a の不揮発性記憶手段に追加する時には、画像形成装置 40b の光ディスク装置 7b の製造番号と固有データも光ディスク装置 7a の不揮発性記憶手段に追加して記憶する。このように、光ディスク装置に固有の暗号鍵と製造番号と固有データを一組で使用する。

10

【0073】

図 8 は、光ディスク装置に固有の暗号鍵と製造番号と固有データを一組で使用する場合において光ディスクからバックアップデータを再生する時の処理フローを示す。まず、ステップ S31 で光ディスク装置 7 内の不揮発性記憶手段に記憶された記録再生用暗号鍵で復号化回路 30 により誤り訂正符号化復号化回路 19 からの暗号化されたデータ（光ディスク 6 から再生されたデータ）が復号化される。この時、CPU 25 は、光ディスク装置 7 の不揮発性記憶手段内の記録再生用暗号鍵をレジスタ 32 に設定し、復号化回路 30 がレジスタ 32 からの記録再生用暗号鍵を用いて、誤り訂正符号化復号化回路 19 から入力される、光ディスク 6 から再生された光ディスク装置の製造番号を復号化し、CPU 25 はその復号化した光ディスク装置の製造番号をレジスタ 37 に保持させる。更に、復号化回路 30 はレジスタ 32 からの記録再生用暗号鍵を用いて誤り訂正符号化復号化回路 19 からの光ディスク 6 の読み取りデータを復号化し、CPU 25 はその復号化したデータから光ディスク装置に固有のデータを検出してレジスタ 38 に保持させる。

20

【0074】

次に、CPU 25 は、ステップ S32 で、レジスタ 37 に保持された光ディスク装置 7 の製造番号を光ディスク装置 7 の不揮発性記憶手段に記憶されている光ディスク装置 7 の製造番号と比較して両者が一致するか否かを判断するとともに、レジスタ 38 に保持された固有データを光ディスク装置 7 の不揮発性記憶手段に記憶されている固有データと比較して両者が一致するか否かを判断し、光ディスク装置の製造番号、固有データの双方とも各々上記両者が一致した場合にはステップ S33 で光ディスク装置 7 に対して光ディスク 6 からデータを再生させて復号化回路 30 からバスインターフェース回路 17 を介して出力させることで該データをハードディスク装置 5 に入力させてハードディスクに記録させ、処理を終了する。CPU 25 は、光ディスク装置の製造番号、固有データのいずれか一方又は両方について各々上記両者が一致しない場合には、ステップ S34 で光ディスク装置 7 内の不揮発性記憶手段に再生専用暗号鍵が記憶されているか否かを判断し、再生専用暗号鍵が光ディスク装置 7 内の不揮発性記憶手段に記憶されていないければ、ステップ S38 で操作部 8 の液晶表示装置に「データを再生できません。」等の警告を表示して、処理を終了する。

30

【0075】

CPU 25 は、光ディスク装置 7 内の不揮発性記憶手段に再生専用暗号鍵が記憶されていれば、ステップ S35 で、その再生専用暗号鍵をレジスタ 32 に設定し、再び誤り訂正符号化復号化回路 19 からの暗号化されたデータ（光ディスク 6 から再生されたデータ）を復号化回路 30 で復号化させ、その復号化したデータから光ディスク装置 7 の製造番号、固有データを検出する。CPU 25 は、ステップ S36 で、その復号化した光ディスク装置 7 の製造番号を光ディスク装置 7 内の不揮発性記憶手段に記憶されている光ディスク装置の製造番号と比較して両者が一致するか否かを判断するとともに、その復号化した固有データと、光ディスク装置 7 内の不揮発性記憶手段に記憶されている再生専用暗号鍵に対応する固有データとを比較して両者が一致するか否かを判断し、光ディスク装置の製造番号、固有データの双方とも各々上記両者が一致すればステップ S33 に進んで光ディスク装置 7 に対して光ディスク 6 からデータを再生させて復号化回路 30 からバスインター

40

50

フェース回路 17 を介して出力させることで該データをハードディスク装置 5 に入力させてハードディスクに記録させ、処理を終了する。

【 0 0 7 6 】

更に、CPU 25 は、光ディスク装置 7 の製造番号、固有データのいずれか一方又は双方について上記両者が一致しなければ、ステップ S 37 で光ディスク装置 7 の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されているか否かを判断し、光ディスク装置 7 内の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されていれば、ステップ S 35 に戻ってその再生専用暗号鍵をレジスタ 32 に設定して再び誤り訂正符号化復号化回路 19 からの暗号化されたデータ（光ディスク 6 から再生されたデータ）を復号化回路 30 で復号化させる。

10

【 0 0 7 7 】

CPU 25 は、ステップ S 36 で更に光ディスク装置の製造番号、固有データのいずれか一方または双方とも各々上記両者が一致しない場合には、ステップ S 37 で光ディスク装置 7 内の不揮発性記憶手段に更に他の再生専用暗号鍵が記憶されているか否かの判断を繰返し、光ディスク装置 7 内の不揮発性記憶手段に記憶されている再生専用暗号鍵がある限りステップ S 36 で更に光ディスク装置の製造番号、固有データの双方とも各々上記両者が一致するまで、ステップ S 37 からステップ S 35 に戻ってその再生専用暗号鍵をレジスタ 32 に設定して再び誤り訂正符号化復号化回路 19 からの暗号化されたデータ（光ディスク 6 から再生されたデータ）を復号化回路 30 で復号化させる。CPU 25 は、データを正常に復号化できる暗号鍵が光ディスク装置 7 内の不揮発性記憶手段に無い場合には、ステップ S 38 で操作部 8 の液晶表示装置に「データを再生できません。」等の警告を表示させて、処理を終了する。

20

【 0 0 7 8 】

こうすることにより、暗号鍵が解読されても、光ディスク装置の製造番号と固有データとで二重にバックアップデータを保護しているので、画像形成装置に内蔵したハードディスク装置 5 のハードディスク内のデータを、光ディスク 6 へバックアップした時の光ディスク 6 に記録したバックアップデータの機密を守ることができる。又、他の光ディスク装置の記録再生用暗号鍵を再生専用暗号鍵として記憶し、更に該他の光ディスク装置の製造番号と固有データも記憶するので、他の光ディスク装置で記録した光ディスクの記録データも再生でき、画像形成装置や光ディスク装置の置換え時にも対応できる。

30

【 0 0 7 9 】

更に、光ディスクの記録データを再生する時に、光ディスクから読み出した製造番号と固有データと、再生を行っている光ディスク装置の製造番号と固有データとをそれぞれ比較し、これらが各々一致する時のみ光ディスク装置からデータを出力するようにしているので、悪意のある第三者が、光ディスクを盗み、別の同機種の光ディスク装置を入手して、暗号鍵を解読した場合でも、盗んだ光ディスクの記録データを再生できないようにする効果がある。

【 0 0 8 0 】

本実施形態によれば、着脱可能な記録媒体にハードディスク内のデータを記録再生する情報記録再生装置としての光ディスク装置 7 が、データを暗号化する手段としての暗号化回路 29 と、データを復号化する手段としての復号化回路 30 と、暗号化と復号化に使用する上記情報記録再生装置 7 に固有の暗号鍵を記憶する手段としての不揮発性記憶手段とを有し、記録した情報記録再生装置でしかデータを再生できないようにしているので、記録媒体に記録したバックアップデータの機密を保持できる画像形成装置を提供できる。

40

【 0 0 8 1 】

本実施形態によれば、さらに、上記情報記録再生装置 7 が別の情報記録再生装置に固有の暗号鍵を記憶する手段としての不揮発性記憶手段を有しているため、上記別の情報記録再生装置が破損した場合等に、上記別の情報記録再生装置によって記録媒体に記録されたデータを上記情報記録再生装置 7 で再生できる画像形成装置を提供できる。

【 0 0 8 2 】

50

本実施形態によれば、さらに、上記情報記録再生装置7が上記情報記録再生装置の製造番号を記憶する手段としての不揮発性記憶手段を有し、上記情報記録再生装置の製造番号を暗号化して上記記録媒体に記録するので、暗号が解読されても、製造番号が一致しないと上記情報記録再生装置からデータを出力できないようにして、バックアップデータの機密を保持できる画像形成装置を提供できる。

【0083】

本実施形態によれば、さらに、上記情報記録再生装置7が上記別の情報記録再生装置の製造番号を記憶する手段としての不揮発性記憶手段を有しているため、上記別の情報記録再生装置によって記録された記録媒体のデータを上記情報記録再生装置で再生する場合に、暗号が解読されても、解読後の製造番号が上記別の情報記録再生装置の製造番号と一致しないと上記情報記録再生装置からデータを出力できないようにして、バックアップデータの機密を保持できる画像形成装置を提供できる。

10

【0084】

本実施形態によれば、さらに、上記情報記録再生装置7が、上記情報記録再生装置に固有のデータを記憶する手段としての不揮発性記憶手段を有し、上記固有のデータを暗号化して上記記録媒体に記録するので、暗号が解読されても、固有のデータが一致しないと上記情報記録再生装置からデータを出力できないようにして、バックアップデータの機密を保持できる画像形成装置を提供できる。

【0085】

本実施形態によれば、さらに、上記情報記録再生装置7が上記別の情報記録再生装置に固有のデータを記憶する手段としての不揮発性記憶手段を有しているため、上記別の情報記録再生装置によって記録された記録媒体のデータを上記情報記録再生装置で再生する場合に、暗号が解読されても、解読後の固有のデータが上記別の情報記録再生装置の固有のデータと一致しないと上記情報記録再生装置からデータを出力できないようにして、バックアップデータの機密を保持できる画像形成装置を提供できる。

20

【0086】

本実施形態によれば、さらに、上記情報記録再生装置7が上記情報記録再生装置7の製造番号を記憶する手段としての不揮発性記憶手段と、上記情報記録再生装置に固有のデータを記憶する手段としての不揮発性記憶手段とを有し、上記情報記録再生装置の製造番号と上記固有のデータを暗号化して上記記録媒体に記録するので、暗号が解読されても、製造番号と固有のデータが一致しないと上記情報記録再生装置からデータを出力できないようにして、バックアップデータの機密を保持できる画像形成装置を提供できる。

30

【0087】

本実施形態によれば、さらに、上記情報記録再生装置7が上記別の情報記録再生装置の製造番号を記憶する手段としての不揮発性記憶手段と、上記別の情報記録再生装置に固有のデータを記憶する手段としての不揮発性記憶手段とを有しているため、上記別の情報記録再生装置によって記録された記録媒体のデータを上記情報記録再生装置で再生する場合に、暗号が解読されても、解読後の製造番号と固有のデータが上記別の情報記録再生装置の製造番号と固有のデータに一致しないと、上記情報記録再生装置からデータを出力できないようにして、バックアップデータの機密を保持できる画像形成装置を提供できる。

40

【0088】

本実施形態によれば、さらに、上記記録媒体に記録された暗号化された製造番号を復号化し、上記復号化された製造番号と上記情報記録再生装置7の記憶装置（レジスタ37）に記憶された製造番号とが一致した時に、上記記録媒体のデータを復号化したデータを上記記憶装置に入力しているため、暗号が解読されても、解読後の製造番号が上記情報記録再生装置の不揮発性記憶手段に記憶された製造番号と一致しないと上記情報記録再生装置からデータを出力できないようにして、バックアップデータの機密を保持できる画像形成装置を提供できる。

【0089】

本実施形態によれば、さらに、上記記録媒体に記録された暗号化された固有のデータを

50

復号化し、上記復号化された固有のデータと上記情報記録再生装置 7 の記憶装置（レジスタ 3 8 ）に記憶された固有のデータとが一致した時に、上記記録媒体のデータを復号化したデータを上記記憶装置に入力しているため、暗号が解読されても、解読後の固有のデータが上記情報記録再生装置に記憶された固有のデータと一致しないと上記情報記録再生装置からデータを出力できないようにして、バックアップデータの機密を保持できる画像形成装置を提供できる。

【 0 0 9 0 】

本実施形態によれば、上記記録媒体に記録された暗号化された製造番号と固有のデータを復号化し、上記復号化された製造番号と上記情報記録再生装置 7 の記憶装置（レジスタ 3 7 ）に記憶された製造番号とが一致し、上記復号化された固有のデータと上記情報記録再生装置 7 の記憶装置（レジスタ 3 8 ）に記憶された固有のデータとが一致した時に、上記記録媒体のデータを復号化したデータを上記記憶装置に入力するので、暗号が解読されても、解読後の製造番号と固有データが上記情報記録再生装置の記憶装置に記憶された製造番号と固有データに一致しないと上記情報記録再生装置からデータを出力できないようにして、バックアップデータの機密を保持できる画像形成装置を提供できる。

【図面の簡単な説明】

【 0 0 9 1 】

【図 1】本発明の一実施形態を示すブロック図である。

【図 2】同実施形態の光ディスク装置を示すブロック図である。

【図 3】同光ディスク装置の暗号化復号化回路の内部構成を示すブロック図である。

【図 4】同実施形態のハードディスク装置からのデータを光ディスクに記録してバックアップを行う時に、光ディスクに記録したバックアップデータの機密を守るための暗号鍵の使用方法を説明するための図である。

【図 5】同実施形態における光ディスク装置の製造番号と固有のデータを使用しない場合において記録再生用暗号鍵によって暗号化されたデータが記録された光ディスクからデータを再生する時の処理フローを示すフローチャートである。

【図 6】同実施形態における光ディスク装置に固有の暗号鍵と製造番号を対で使用する場合において光ディスクからバックアップデータを再生する時の処理フローを示すフローチャートである。

【図 7】同実施形態における光ディスク装置に固有の暗号鍵と固有データを対で使用する場合において光ディスクからバックアップデータを再生する時の処理フローを示すフローチャートである。

【図 8】同実施形態における光ディスク装置に固有の暗号鍵と製造番号と固有データを一組で使用する場合において光ディスクからバックアップデータを再生する時の処理フローを示すフローチャートである。

【符号の説明】

【 0 0 9 2 】

7 光ディスク装置

1 8 暗号化復号化回路

2 5 CPU

2 7 ROM

2 9 暗号化回路

3 0 復号化回路

3 1 データセレクタ

3 2 ~ 3 8 レジスタ

10

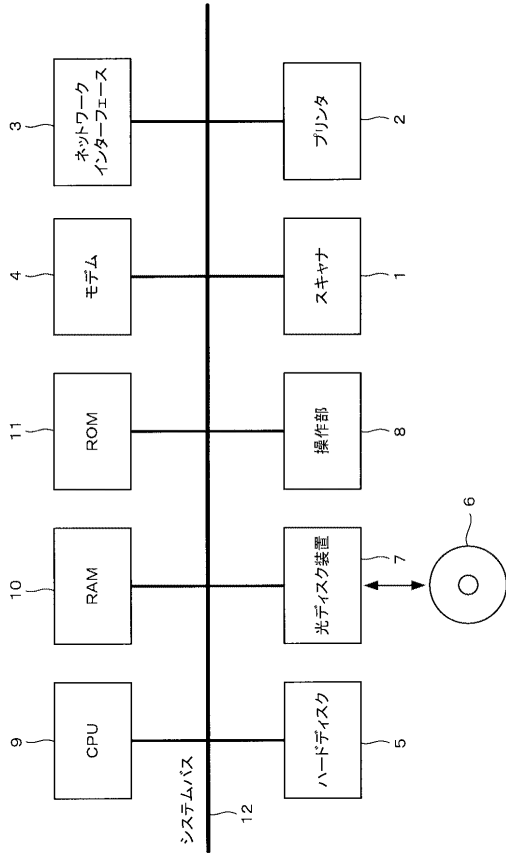
20

30

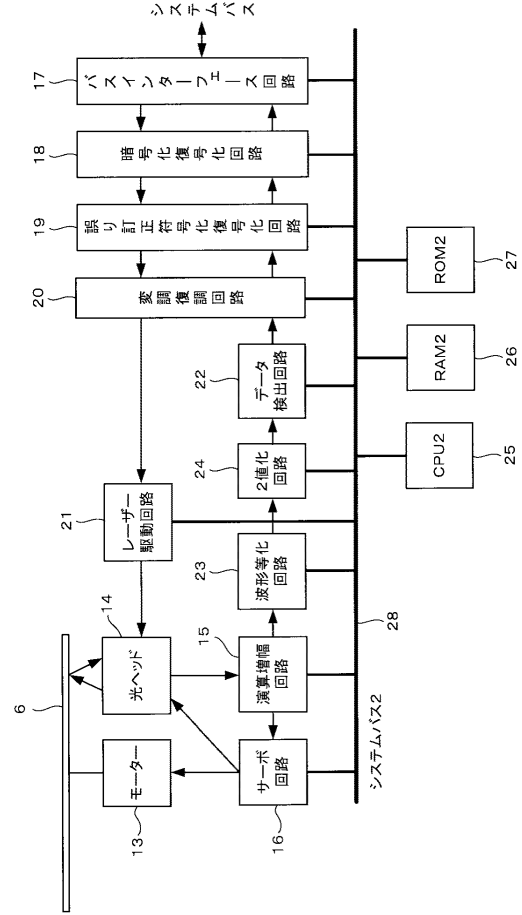
40



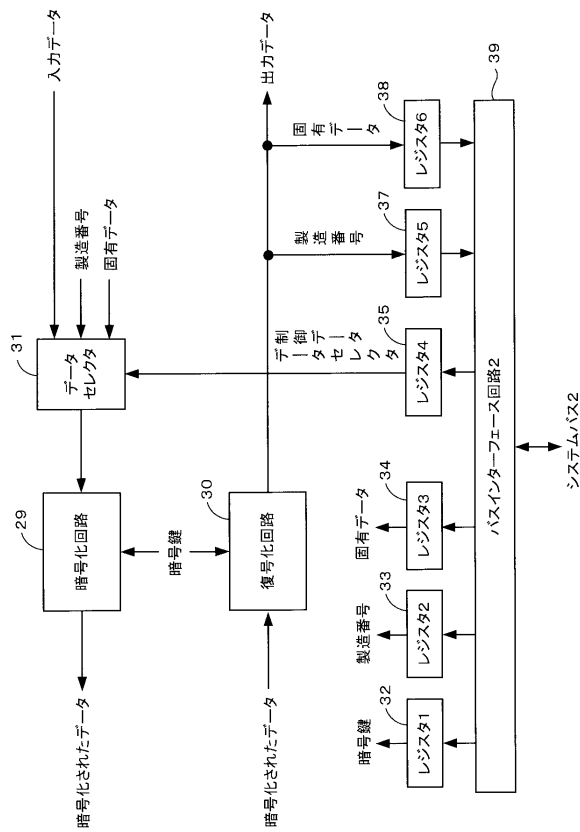
【図1】



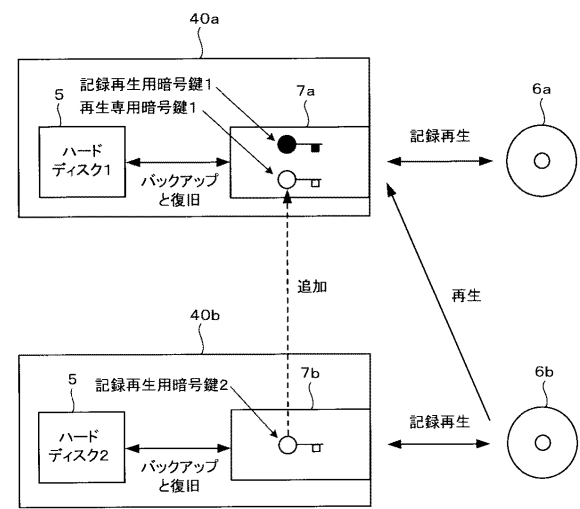
【図2】



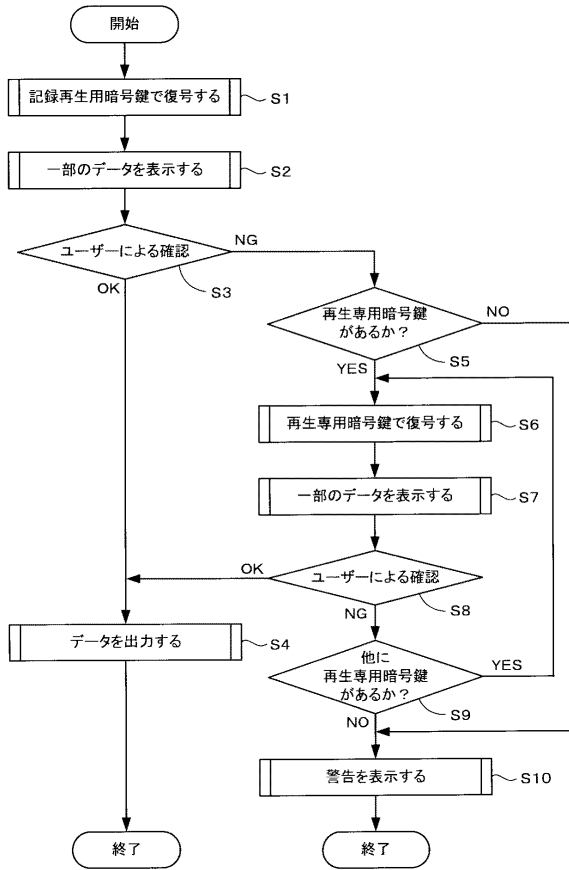
【図3】



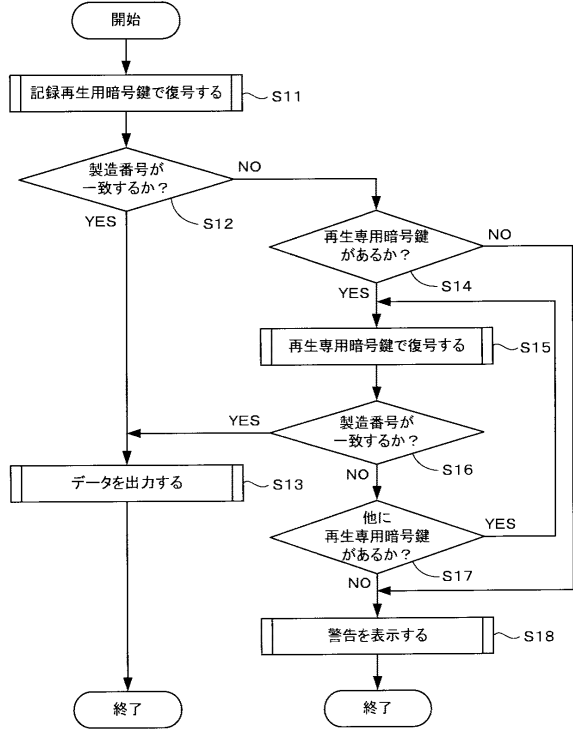
【図4】



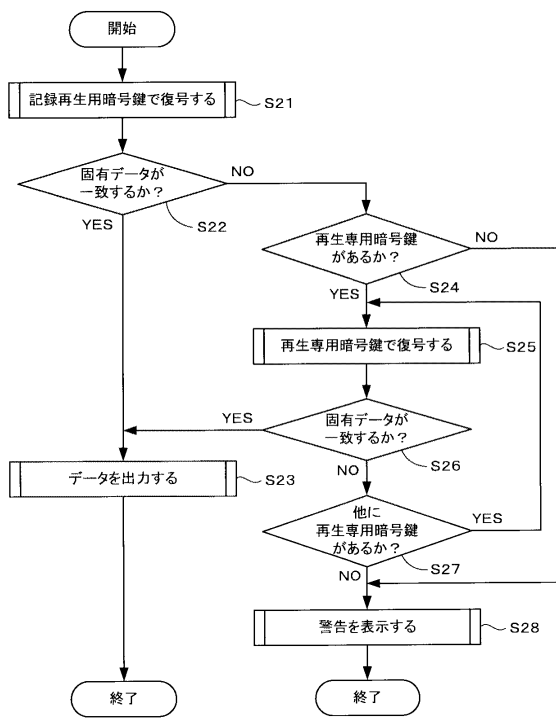
【図5】



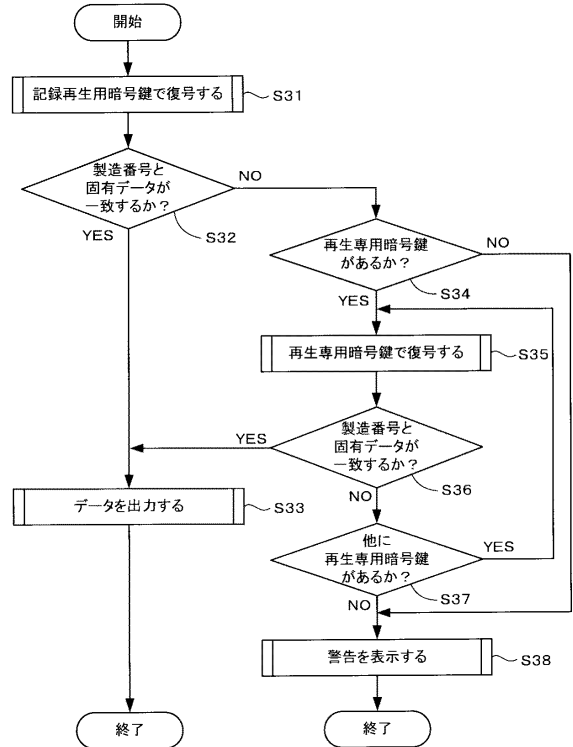
【図6】



【図7】



【図8】



---

フロントページの続き

(51)Int.Cl. F I  
H 0 4 L 9/00 6 0 1 E  
H 0 4 N 1/21

(56)参考文献 特開2003-255832(JP,A)  
特開2005-063068(JP,A)  
特開2003-333519(JP,A)  
特開2002-287919(JP,A)  
特開2003-179850(JP,A)  
特開平11-352881(JP,A)  
特開2002-260327(JP,A)  
特開2004-265006(JP,A)

(58)調査した分野(Int.Cl., DB名)  
H 0 4 N 1 / 0 0 - 1 / 0 0 1 0 8  
H 0 4 N 1 / 3 2 - 1 / 3 6  
H 0 4 N 1 / 4 2 - 1 / 4 4  
H 0 4 N 1 / 2 1  
G 0 3 G 2 1 / 0 0  
G 0 6 F 3 / 0 9 - 3 / 1 2  
B 4 1 J 2 9 / 6 8